サイバーセキュリティ関係法令
Q&A ハンドブック

Ver. 3.0

令和 8 年 10 月

内閣官房国家サイバー統括室（ＮＣＯ）

「サイバーセキュリティ関係法令 Q&A ハンドブック」の公開に当たって

この度、関係者の自発的かつ精力的な努力と相互の協力により、「サイバーセキュリティ関係法令 Q&A ハンドブック」をお届けできるのは、作業に当たった全員の喜びであります。また私個人にとっても、サイバーセキュリティ戦略本部員を辞した後に、このサブワーキンググループ（サイバーセキュリティ戦略本部の普及啓発・人材育成専門調査会の中のサブワーキンググループとなります）の主査を仰せつかい、ボランティア精神に富んだ皆さんとご一緒できたのは、格別の思い出となりました。

この企画のアイディアは、副主査を務められた岡村久道氏の経験と発案に多くを負っています。同氏は、経済産業省が平成 21 年にとりまとめた「情報セキュリティ関連法令の要求事項集」（以下「要求事項集」）の編集を手掛けられ、その後、現在までの間にサイバーセキュリティ基本法をはじめとしたセキュリティに関係する重要な法律が多くなってきたことを踏まえて、その発展形として今回のような資料集刊行の必要性を強く主張されました。なぜなら、ドッグ・イヤーの比喩に従えば、この間に 70 人間イヤー相当の時間が経過したわけで、事実「想定外」の事例が多数発生していたからです。

私も岡村さんとは幾分違った観点から、このような資料集の必要性を感じていました。というのも、学者として「情報法」という法分野が存在し得ることを直感し、幾分でもその体系化に寄与することを志していましたので、「情報セキュリティ六法」のようなものができること自体が、この分野の学問の発展に資するものだと思ったからです。また実務的に言えば、官僚の皆さんの仕事は「法の原則に基づいて」行われねばなりませんから、多くの仕事は「○○六法」のような法令集と首っ引きでなされるのが通例です。サイバーセキュリティの重要性が増した現在では、「六法」のようなものを机上において作業する時代になったのではないか、と考えたのです。

かくして出来上がった本書は、作成側からすれば、次の 3 つの特徴を持っていると自負しています。まず、サイバーセキュリティに関連すると思われる法令を、なるべく広範に網羅するよう努めたことです。参考にした「要求事項集」は主として経済産業省所管の範囲をカバーするものでしたが、本書は関係省庁の協力を得て幅広く関連事項を収録しています。

第 2 点は、これらの法令の最新版を集めたことです。IT の展開はドッグ・イヤーと呼ばれるほど早いので、法的な対応もそれに従わざるを得ません。そこで、法律など正規の手続きを経たハード・ローよりも、ソフト・ローと呼ばれるガイドラインや技術標準などが、事実上の規範となっている場合があります。ところが、これらの規範はごく少数の関

係者は知っているとしても、一般にはいつ改定されたかが分かりにくい宿命があります。本書の編集作業により、とりあえず現時点での最新情報をお届けできたかと思います。

第 3 点は、ソフト・ローを収録したことから当然の要請ともいえますが、「法令」だけでなく、その「解説」をも重視したことです。そのためには「解説者」が必要になりますので、サブワーキンググループの下に更に「タスクフォース」を設け、新進気鋭の弁護士を中心に、なるべく客観的な記述に努めてもらいました。参加して下さった方々は多忙にもかかわらず、「縁の下の力持ち」的な仕事をボランティア精神で遂行されたことに感謝しています。

このようにして、ようやく形を整えるに至ったドキュメントを見ると、ある種の感慨を覚えます。しかし、これが終点ではありません。本書に掲載したものは、現時点で解釈まで含めて一定の方向性が出ている法令を主な対象としており、重要性が高いとしても未確定な部分があるものについては、次回以降の改訂に際しての課題となると考えています。

サイバーセキュリティの実務に携わり、本書の主たる利用者である方々には、ぜひ「改訂版」へのご要望を伝えていただければ、と思います。また、学者として本書を利用する私たちは、これを素材にして、「情報法」や「サイバーセキュリティ法」の体系化を試みていければ、と思います。

参加者一同、「現時点では精一杯努力した」という満足感はありますが、「これで満点」などとは到底思えません。また、仮に現時点で満足度が高いにしても、ドッグ・イヤーの時代にはすぐに時代遅れになる恐れがあります。今後、利用者の皆さんの後押しをいただいて、「六法」が毎年発行されるのと同じように改訂を重ねていくことができれば、「叩き台」である初版に関与した私たちの努力も、報われるのではないかと期待しています。

令和 2 年 2 月 26 日
関係者を代表して　林　紘一郎

前文

【Ver.1.0】

サイバー空間と実空間の一体化、事業のグローバル化等に伴い、サイバーセキュリティに関係する法令が増えており、事業者が適切なサイバーセキュリティ対策を講じていく上で、サイバーセキュリティに関係する法令の知識が不可欠である。

一方で、サイバーセキュリティの関係法令は体系的に存在するものではなく、これらを取りまとめ、解説を施した資料は少ない。経済産業省が平成 21 年に「情報セキュリティ関連法令の要求事項集」（以下「要求事項集」という。）[1]をとりまとめているが、その後サイバーセキュリティに関係する法令として、サイバーセキュリティ基本法等が新たに成立し、また、個人情報の保護に関する法律や不正競争防止法が改正される等、法制度に関する状況が変化している。

このような状況を踏まえ、サイバーセキュリティ戦略（平成 30 年 7 月 27 日閣議決定）においては、企業がサイバーセキュリティ対策の実施において参照すべき法制度に関する整理を行うこととされ、サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会は、平成 30 年 10 月 10 日、サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ（以下「サブ WG」という。）を設置した（オブザーバーとして関係省庁も参加）。

サブ WG は、平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、近年増加する情報の取扱いに関する法令や、情勢の変化、技術の進展に伴い生じている法的課題等について、平易な表記による解説を付して取りまとめた関係法令集を作成することを目的とし、林紘一郎名誉教授（情報セキュリティ大学院大学）を主査、岡村久道弁護士（英知法律事務所・京都大学）を副主査として検討を進め、要求事項集をベースとしつつ、必要に応じて内容をアップデートし、また、新たに検討が必要となる法的論点を加え、解説を付すこととした。この方針を踏まえた具体的な執筆に際しては、サブ WG の下部にタスクフォースを設置し、必要に応じて有識者等にヒアリングを実施した。当該ドラフトはサブ WG に提出され、サブ WG において検討を加え、本書を取りまとめた。

読み手としては、経営層、企業においてサイバーセキュリティ対策を企画、立案し、経営層に必要な説明や助言を行う「戦略マネジメント層」及び法令対応を行う法務部門を想定し、現場で広く利用頂けるよう可能な限り平易な表現を心がけた。

本書は、基本的に、一般的なものと考えられる公刊物の内容を踏まえて作成したものであるが、個別具体的な事例において現行法がどのように解釈・適用されるかは、それぞれの状況を勘案した上で、最終的には裁判所において判断されるものであることは言うまでもない。

いずれにせよ、本書が企業実務上の参考として、効率的・効果的なサイバーセキュリティ対策・法令遵守の促進への一助になることを期待している。

---

[1] https://warp.da.ndl.go.jp/info:ndljp/pid/12166597/www.meti.go.jp/policy/netsecurity/secgov-documents.html で閲覧可能。

なお、本書については、サイバーセキュリティに関する法令について今後も大きな変化が予想されることを踏まえ、継続的に必要な論点の検討を行いつつ、必要に応じ改訂・拡充等を行っていく予定である。

【Ver.2.0】

本ハンドブック Ver.1.0 の策定以降、サイバーセキュリティを巡る情勢は一層その厳しさを増している。特に、本年に入り、ウクライナ情勢を巡って多くのサイバーセキュリティ関連の報道がなされ、また、Emotet の活動再開や、ランサムウェア被害の増加など、サイバーセキュリティを巡る話題は枚挙にいとまがない。

このような状況に対応すべく、サイバーセキュリティに係る制度も、随時、整備・改正等が行われており、法令対応を行う各組織の法務部門をはじめ、経営層や経営層をサポートする戦略マネジメント層等に対しては、できる限り最新の状況を提供することが必要となっている。

この点について、Ver.1.0 の策定の際に、既に本ハンドブックを継続的に改訂・拡充等を行っていくことが想定されていた。そこで、「サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ」においてあらためて検討を開始し、Ver. 1.0 策定に携わった専門家が集結し、時宜にかなったハンドブックとすべく、法制面の大所高所から、必要な検討を行った。また、原案の策定にあたっては、NISC の委託事業の下、Ver. 1.0 のドラフトを起草した若手の弁護士陣が再び筆をとり、記載内容の充実を図った。さらに、本サブワーキンググループ前主査である林紘一郎名誉教授（情報セキュリティ大学院大学）には、改訂にあたり、サイバーセキュリティ法制全般にわたる後見人的お立場から、ご指導を賜った。

今回の改訂では、関係法令やガイドライン等の成立・改正等を踏まえた情報の更新とともに、サイバーセキュリティの実務において扱われているトピック（例：インシデント対応、ランサムウェア対応、サイバー保険等）を多数追加している。また、本ハンドブックが必要な人に届き、活用されるよう、今後、書籍化やウェブサイト掲載にあたっての HTML 化など、利便性の向上にも務めることとしている。

本書が、2021 年 9 月に閣議決定された「サイバーセキュリティ戦略」に掲げる「Cybersecurity for All～誰も取り残さないサイバーセキュリティ～」実現の一助として、法令への理解を深めたい方々のお手元に置かれ、日々の業務に活かされれば、関係者一同にとって望外の喜びであり、我が国のサイバーセキュリティは向上していくものと確信している。

なお、本ハンドブックは、基本的に 2023 年 1 月 1 日時点の法令等を基準としているが、適宜サイバーセキュリティ関係法令等の制定・改廃の動きに合わせ、今後も、本ハンドブックの改訂を実施していくこととしたい。

【Ver.3.0】

本ハンドブック Ver.2.0 の策定以降、巧妙化・高度化したサイバー攻撃事案が相次ぎ、外国国家の関与が疑われるサイバー攻撃キャンペーンが顕在化するなど、我が国を取り巻くサイバー脅威の情勢は一層深刻化し、国民生活・経済活動、ひいては国家安全保障に深刻な影響を与え得る重大な懸念となっている。

このような脅威の高まりを受け、我が国のサイバーセキュリティ政策は大きな転換点を迎えた。2025 年 5 月、能動的サイバー防御の導入を可能とする「重要電子計算機に対する不正な行為による被害の防止に関する法律」（サイバー対処能力強化法）及び関係法律の整備等に関する法律が成立した。同年 7 月には、その一部施行に伴い、サイバーセキュリティ戦略本部の改組及び機能強化が行われ、また、本ハンドブックを策定・公表してきた内閣サイバーセキュリティセンター（NISC）が発展的に改組され、官民を通じたサイバーセキュリティの確保に関する司令塔として国家サイバー統括室（NCO）が発足した。この新たな体制の下で、2025 年 12 月に新たなサイバーセキュリティ戦略が策定され、2026 年 10 月にはサイバー対処能力強化法の本格施行を迎えるに至った。

また、生成 AI をはじめとする AI 技術は、高性能化が急速に進み、サイバー攻撃に悪用されることで攻撃手法の高速化・自動化を促し、脅威の質と量の双方を押し上げることが想定されるところ、サイバーセキュリティ対策の重要性は日々高まっている状況にある。

今回の Ver.3.0 への改訂では、こうした時勢を踏まえ、サイバーセキュリティ関連制度についての様々な変化を適切に反映すべく、内容の拡充と全体構成の見直しを行った。内容面では、サイバー対処能力強化法等をはじめ国内外の関係法令・ガイドラインの制定・改正を取り上げ、解説を新たに作成した。構成面では、法令等の趣旨目的や利用主体に着目して目次を体系化し、項目の統廃合・再構成を行った。加えて、関係法令・ガイドライン等を体系的に整理した「サイバーセキュリティ法体系マッピング」を作成し、同マッピングから関連する解説項目を逆引きできる資料を付録として収録した。

サイバーセキュリティ戦略が掲げる「幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上」の実現に向け、本ハンドブックが実務に携わる全ての方々に広く活用されるよう、今後も利便性の向上に努めるとともに、関係法令等の制定・改廃に合わせて改訂を継続していくこととしたい。

【留保事項】

- 本ハンドブックは、NCO が収集したサイバーセキュリティ関係法令に関する知見について、実務者に資する情報発信・普及啓発を行うことを目的とし、法学者・弁護士等に編纂を依頼して取りまとめた、サイバーセキュリティ関係法令の解釈・適用等についての一つの考え方を示すものである（巻末「関係者一覧」参照）。
- なお、本ハンドブックには、政府の施策内容のみならず、実務者の視点から有用と思われる知見や外国法令の内容等に言及した箇所が含まれるが、これらは法的助言や NCO を含む政府機関の公式見解を示すものではなく、また、日本法以外の外国法の専門家による確認を経たものではない。
- また、本ハンドブック Ver.3.0 は、原則として**2026 年 1 月 1 日時点**の法令等に基づいている。同日以降（公表日まで）の関係法令等の制定・改廃についても可能な範囲で言及しているが、国内外のサイバーセキュリティ関係法令や関連制度は刻一刻と改正等されている。したがって、本ハンドブックの記載内容だけでなく、関係法令の原典、各制度の根拠文書、所管当局等の公式ウェブサイト等を併せて参照し、常に最新情報を確認する必要があることに注意いただきたい。

本書の目次構成

第 1. サイバーセキュリティ確保のための基本的な枠組み

Q1 サイバーセキュリティの定義 1

タグ：サイバーセキュリティ基本法、サイバーセキュリティの定義

Q2 サイバーセキュリティ基本法の概要 3

タグ：サイバーセキュリティ基本法、サイバーセキュリティ戦略本部、政府機関等統一基準群、重要インフラ統一基準、重要インフラ行動計画、GSOC

Q3 能動的サイバー防御に関する法律 11

タグ：能動的サイバー防御、サイバー対処能力強化法及び同整備法、特定重要電子計算機、インシデント報告、通信情報、アクセス・無害化、サイバー通信情報監理委員会

Q4 地方公共団体のサイバーセキュリティ 20

タグ：地方自治法、地方公共団体、安全管理体制、リスク管理体制、サイバーセキュリティ基本法、地方公共団体情報システムの標準化に関する法律、地方公共団体情報システム標準化基本方針

第 2. 企業・組織のセキュリティガバナンス

2-1. 会社法・情報開示関連

Q5 内部統制システムとサイバーセキュリティとの関係 26

タグ：会社法、内部統制システム、リスク管理体制、事業継続計画（BCP）、グループ・ガバナンス・システム、CSIRT、モニタリング

Q6 サイバーセキュリティと取締役等の責任 33

タグ：会社法、個情法、損害賠償責任

Q7 サイバーセキュリティ体制の適切性を担保するための監査等 36

タグ：会社法、内部監査、情報セキュリティ監査、システム監査、情報開示、内部通報、CSIRT

Q8 サイバーセキュリティと情報開示 41

タグ：会社法、金融商品取引法、有価証券報告書、コーポレート・ガバナンス報告書、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、統合報告書

2-2. サイバーセキュリティに関する規格・資格・認証制度等

Q9 サイバーセキュリティに関する規格等と NIST SP800 シリーズ 47

タグ：ISO/IEC 27000、JIS Q 15001、プライバシーマーク、NIST、FISMA、FIPS、SP800 シリーズ、

NIST CSF、NIST PF

Q10 情報処理安全確保支援士 53

タグ：情促法、情報処理安全確保支援士、情報セキュリティサービス基準

Q11 技術情報管理認証制度について 57

タグ：産業競争力強化法、技術情報管理認証制度、技術等情報漏えい防止措置、重要技術マネジメント、現地審査を含む認証、情報セキュリティ、第三者認証

Q12 DX 認定・DX 銘柄とサイバーセキュリティ 60

タグ：DX 銘柄、DX 認定、デジタルガバナンス・コード、プライバシーガバナンスガイドブック、情促法、IPA

第 3. 情報・データ等の保護

3-1. 個人情報保護法関連

Q13 個情法の安全管理措置義務とサイバーセキュリティの関係 65

タグ：個情法、個人データ、安全管理措置、保有個人データ、ISO/IEC27001、JIS Q 15001、P マーク

Q14 個人データの取扱いの委託と安全管理 71

タグ：個情法、個人データ、委託、監督、監査、外的環境の把握

Q15 クラウドサービスの活用と個情法 75

タグ：個情法、安全管理措置、委託先の監督、クラウドサービス、外国にある第三者、外的環境の把握

Q16 官民における個人情報に関する安全管理措置の相違 78

タグ：個情法、行個法、独個法、個人情報保護条例、安全管理措置、個人情報の定義、漏えい等

Q17 個人データの加工と法令上の安全管理 82

タグ：個情法、安全管理措置義務、統計情報、仮名加工情報、匿名加工情報

Q18 クレジットカード情報の取扱い 90

タグ：割賦販売法、クレジットカード情報、PCI DSS、非保持化、クレジットカード・セキュリティガイドライン

Q19 労働者の心身の状態に関する情報の取扱い 94

タグ：労働安全衛生法、じん肺法、個情法、労働契約法、労働者、メンタルヘルス、健康診断

Q20 マイナンバーの取扱い 98

タグ：番号利用法、個情法、マイナンバー、個人番号、安全管理措置

3-2. 不正競争防止法・知的財産法関連

Q21 営業秘密の要件 101

タグ：不正競争防止法、営業秘密、情報管理、営業秘密保有者、秘密管理性、有用性、非公知性、従業員、委託、リスクマネジメント

Q22 限定提供データとサイバーセキュリティ 106

タグ：不正競争防止法、限定提供データ、限定提供性、相当量蓄積性、電磁的管理性、営業秘密

Q23 技術的手段の回避行為・無効化行為の法的責任 109

タグ：不正競争防止法、著作権法、刑法、不正アクセス禁止法、技術的制限手段、技術的保護手段、技術的利用制限手段、技術的手段

Q24 データの知的財産権法規定による保護方法 113

タグ：不正競争防止法、著作権法、著作権、特許権、実用新案権、意匠権、営業秘密，限定提供データ

Q25 ソフトウェアのリバースエンジニアリング 117

タグ：著作権法、リバースエンジニアリング、マルウェア、柔軟な権利制限、複製権、翻案権、同一性保持権

3-3. 情報管理の手法

Q26 暗号の利用と情報管理等 123

タグ：個情法、不正競争防止法、著作権法、電波法、電子署名法、暗号、CRYPTREC、危殆化、技術的制限手段、技術的利用制限手段、技術的保護手段

Q27 データの消去、データが記録された機器・電子媒体の廃棄 128

タグ：個情法、安全管理措置、秘密情報、消去、削除、廃棄、暗号化消去、秘密保持契約、ハードディスク

3-4. 雇用上の情報管理措置

Q28 セキュリティ上必要となる雇用関係上の措置と誓約書の取得 132

タグ：労働基準法、労働組合法、労働契約法、民法、個情法、不正競争防止法、従業員、就業規則、誓約書、秘密保持義務、懲戒処分

Q29 従業員のモニタリングに関する留意点 141

タグ：民法、個情法、モニタリング、GPS、プライバシー権

Q30 業務用端末の私的利用・私物端末の業務利用等に関する諸問題 149

タグ：労働契約法、私用メール、SNS、労働契約、就業規則、職務専念義務、解雇・懲戒処分、労働基

準法、私物 PC、業務用データの社外持ち出し

Q31 テレワークにおけるセキュリティ 155

タグ：テレワーク、VPN、テレワークセキュリティガイドライン

Q32 派遣労働者及び特定受託事業者に対するセキュリティに関する義務付け 160

タグ：民法、労働者派遣法、派遣労働者、フリーランス、誓約書、教育訓練

Q33 退職後の競業避止義務と違反時の退職金減額・不支給及び情報漏えい防止のための秘密保持契約 163

タグ：民法、不正競争防止法、競業避止義務、競業避止義務契約、労働基準法、退職金、労働契約法、就業規則、秘密保持契約、秘密保持義務

Q34 退職後の海外での秘密保持義務違反行為について 172

タグ：不正競争防止法、民事訴訟法、法の適用に関する通則法、秘密保持義務、競業避止義務、情報漏えい、人材を通じた技術流出

第 4. 製品・サービス等のセキュリティ保護

Q35 IoT 機器のセキュリティに関する法的対策 179

タグ：電気通信事業法、国立研究開発法人情報通信研究機構法、IoT セキュリティガイドライン ver1.0、IoT セキュリティ総合対策、電気通信事業法に基づく端末機器の基準認証に関するガイドライン、米国カリフォルニア州 IoT セキュリティ法、IoT 機器、NOTICE

Q36 IoT 製品のセキュリティ適合性に関する認証制度（JC-STAR） 185

タグ：IoT 機器、JC-STAR、適合ラベル、端末設備等規則

Q37 IoT 機器からのデータ漏えいにおける製造者の責任 190

タグ：民法、製造物責任法、IoT 機器、データ漏えい、製造者責任、NIST

Q38 ドローンとサイバーセキュリティ 196

タグ：航空法、登録制度、リモート ID、機体認証制度、操縦ライセンス制度、政府機関等における無人航空機の調達等に関する方針について

Q39 モビリティとサイバーセキュリティ 201

タグ：自動運転、道路運送車両法、道路交通法、WP29

Q40 スマホソフトウェア競争促進法 207

タグ：スマホソフトウェア競争促進法、スマートフォン、アプリ、ソフトウェア

Q41 5G 促進法とサイバーセキュリティ 213

タグ：5G 促進法、特定高度情報通信技術活用システムの開発供給等の促進に関する指針、開発供給計

画、導入計画、Society 5.0

Q42 クラウドサービスとサイバーセキュリティ 219

タグ：民法、個情法、不正競争防止法、クラウド、定型約款

Q43 AI のサイバーセキュリティ 232

タグ：AI、リスク管理体制、モニタリング

Q44 Web サービスにおける本人確認とサイバーセキュリティ 239

タグ：個情法、公的個人認証法、犯収法、出会い系サイト規制法、古物営業法、携帯電話不正利用防止法、本人確認ガイドライン、認証、認可、アクセス制御、本人確認、顔認証、安全管理措置、eKYC、なりすまし

第 5. 重要インフラ分野における規律

Q45 重要インフラ分野における規律の概要 246

タグ：重要インフラ、重要インフラ統一基準、重要インフラ行動計画、安全管理、保安規定、事故報告、報告徴求

Q46 電気通信事業分野における規律（電気通信事業法に基づく登録・届出） 251

タグ：電気通信事業法、外国法人等が電気通信事業を営む場合における電気通信事業法の適用に関する考え方、電気通信事業参入マニュアル、電気通信事業参入マニュアル［追補版］、電気通信事業参入マニュアル（追補版）ガイドブック

Q47 電気通信事業分野における規律（電気通信事業者に関する規律の概要） 256

タグ：電気通信事業法、通信の秘密、同意取得の在り方に関する参照文書、通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針、電気通信事業における個人情報等の保護に関するガイドライン、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会、重要インフラ、電気通信事業法の消費者保護ルールに関するガイドライン

Q48 医療分野におけるサイバーセキュリティ 263

タグ：医療法、医療情報システムの安全管理に関するガイドライン、医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律（次世代医療基盤法）、医療情報、匿名加工医療情報、仮名加工医療情報

Q49 金融分野におけるサイバーセキュリティ 270

タグ：金融分野におけるサイバーセキュリティに関するガイドライン、金融分野におけるサイバーセキュリティ強化に向けた取組方針、金融分野のサイバーセキュリティレポート、銀行法、保険業法、金融商品取引業者等向けの総合的な監督指針、主要行等向け監督指針、フィッシングに耐性のある多要素認証

第 6. 取引・通商

6-1. 契約関連（電子署名・システム開発等）

Q50 電子契約と電子署名法 277

タグ：電子署名法、電子署名法施行規則、民事訴訟法、電子帳簿保存法、電子帳簿保存法施行規則、電子契約、文書の成立の真正

Q51 データ取引に関する契約におけるサイバーセキュリティ関連法令上のポイント 284

タグ：民法、不正競争防止法、データ取引、AI・データの利用に関する契約ガイドライン 1.1 版

Q52 データ漏えいに関するシステム開発ベンダの責任とモデル契約 289

タグ：民法、SQL インジェクション、重過失、モデル契約、セキュリティ仕様

Q53 サプライチェーン・リスク対策 295

タグ：独占禁止法、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）、リスクマネジメント、サプライチェーン・リスク、委託、優越的地位の濫用、IT 調達

6-2. 輸出管理・対内直接投資・経済安全保障

Q54 サイバーセキュリティと輸出管理 303

タグ：外為法、輸出貿易管理令、外国為替令、貨物等省令、貿易外省令、役務通達、輸出管理、ワッセナー・アレンジメント、侵入プログラム関連品目

Q55 サイバーセキュリティ事業者への投資 309

タグ：外国為替及び外国貿易法、国家安全保障、対内直接投資、コア業種、CFIUS、FIRRMA

Q56 経済安全保障（経済安保推進法、セキュリティ・クリアランス） 313

タグ：経済安全保障推進法、基幹インフラ、セキュリティ・クリアランス、特定秘密保護法、重要経済安保情報保護活用法

第 7. サイバーセキュリティに関するインシデント対応

7-1. インシデント発生時の対応と法的責任

Q57 サイバーセキュリティインシデント発生時の当局等対応 323

タグ：個情法、番号利用法、電気通信事業法、金融商品取引法、銀行法施行規則、漏えい等、報告義務、有価証券上場規程、認定個人情報保護団体、プライバシーマーク、不正競争防止法、刑事訴訟法、営業秘密、限定提供データ

Q58 インシデントレスポンスと関係者への対応 335

タグ：インシデント対応、デジタル・フォレンジック、サイバー保険、EC サイト、脅威インテリジェンスサービス

Q59 デジタル・フォレンジック 340

タグ：刑法、不正競争防止法、著作権法、児童ポルノ禁止法、金融商品取引法、デジタル・フォレンジック、証拠保全、個情法

Q60 ランサムウェア対応 349

タグ：ランサムウェア、会社法、善管注意義務、経営判断原則、個情法、適時開示、テロ資金提供処罰法

Q61 サイバー攻撃による情報喪失 354

タグ：民法、消費者契約法、電気通信事業法、情報消失、寄託、免責規定、責任制限規定、過失相殺

Q62 電子メールの誤送信 358

タグ：不正競争防止法、民法、営業秘密を示された者、電子メール、誤送信

7-2. インシデント発生時の損害

Q63 データ漏えい時の損害賠償額の算定 361

タグ：民法、不正競争防止法、損害賠償額

Q64 データを紛失・消失した場合における損害額 368

タグ：民法、データ、紛失、消失、滅失、損害賠償額

Q65 インシデント対応における費用負担及びサイバー保険 370

タグ：ランサムウェア、サイバー保険、保険業法

7-3. インシデント発生時の紛争解決手続

Q66 デジタルデータの証拠利用について 373

タグ：民事訴訟法、証拠能力、デジタル・フォレンジック

Q67 営業秘密等の漏えい事実（情報管理体制含む）及び不正使用行為の立証 377

タグ：不正競争防止法、民事訴訟法、営業秘密侵害訴訟、営業秘密、限定提供データ、技術上の秘密、不正使用行為により生じた物、推定規定

Q68 ドメイン名の不正使用への対抗措置 382

タグ：不正競争防止法、サイバースクワッティング、統一ドメイン名紛争処理方針（UDRP）、JP ドメイン名紛争処理方針（JP-DRP）

Q69 発信者情報開示 389

タグ：情報流通プラットフォーム対処法、不正競争防止法、発信者情報開示請求、削除請求

7-4. インシデントに関する情報の取扱い

Q70 サイバーセキュリティと情報共有・公表 394

タグ：サイバーセキュリティ基本法、個情法、不正競争防止法、金融商品取引法、刑法、情報共有、サイバーセキュリティ協議会、CISTA、J-CSIP、JC3、セプター、サイバーセキュリティ対処調整センター、ISAC

Q71 脅威インテリジェンスサービス 403

タグ：脅威インテリジェンス、ダークウェブ、個情法、不正競争防止法、刑法

Q72 脆弱性情報の取扱いについて 408

タグ：情促法、脆弱性、脆弱性情報ハンドリング、JVN

第 8. 刑事法（サイバー犯罪の防止）

Q73 不正プログラムと刑事罰 412

タグ：刑法、不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪、コンピュータ・ウイルス、不正プログラム、不正指令電磁的記録、マルウェア

Q74 電磁的記録不正作出罪 420

タグ：刑法、私電磁的記録不正作出罪、公電磁的記録不正作出罪

Q75 電子計算機使用詐欺罪 424

タグ：刑法、電子計算機使用詐欺罪

Q76 スキミング 428

タグ：刑法、割賦販売法、スキミング、デビットカード、偽造、IC 化

Q77 情報の不正入手・漏えい 431

タグ：刑法、著作権法、個情法、番号利用法、不正競争防止法、国家公務員法、地方公務員法、電気通信事業法、有線電気通信法、電波法、不正アクセス禁止法、割賦販売法、情報の不正入手、漏えい

Q78 不正アクセス 436

タグ：不正アクセス禁止法、アクセス制御機能、識別符号

Q79 フィッシング 441

タグ：不正アクセス禁止法、割賦販売法、フィッシング、識別符号、クレジットカード、フィッシング対策協議会

Q80 フェイクニュース対策 446

タグ：刑事法、偽情報、誤情報、悪意のある情報、フェイクニュース、発信者情報開示、不正アクセス

Q81 越境リモートアクセス 452

タグ：刑事訴訟法、リモートアクセス、記録命令付差押え、サイバー犯罪条約

第 9. 海外法令（米国、EU・英国、その他地域）

Q82 海外における主な個人データ保護関係法令 456

タグ：欧州一般データ保護規則（GDPR）、データ保護オフィサー（DPO）、データ保護影響評価（DPIA）、カリフォルニア州消費者プライバシー法（CCPA）、CPRA、データ侵害通知法、SHIELD Act、データ安全法、ネットワーク安全法、中国民法典

Q83-1 米国における主なサイバーセキュリティ法令 472

タグ：ランサムウェア、OFAC、FinCEN、Cyber Trust Mark プログラム、NIST SP 800-213、CIRCIA

Q83-2 EU・英国における主なサイバーセキュリティ法令 479

タグ：NIS2 指令、基幹サービス運営者、デジタルサービス提供者、EU サイバーセキュリティ法、EU サイバーレジリエンス法、EU データ法

Q83-3 中国における主なサイバーセキュリティ法令 492

タグ：中国個人情報保護法、データ安全法、ネットワーク安全法、民法典、ネットワーク安全審査規則、ネットワークデータ安全管理条例、国家ネットワークセキュリティインシデント報告管理弁法

Q84 データローカライゼーション規制の概要 495

タグ：データローカライゼーション、越境移転、ネットワーク安全法、中国個人情報保護法、重要データ、個人データ、重要情報インフラ運営者、ネットワーク運営者、ネットワークデータ安全管理条例、データ越境移転セキュリティ評価弁法、データ越境流動の促進及び規範規定

Q85 国際捜査共助・協力に関する条約・協定 502

タグ：証拠収集、外交ルート、サイバー犯罪条約、刑事共助条約（協定）、MLAT、ICPO、24 時間コンタクトポイント

付録 サイバーセキュリティ法体系マッピング及び関連する Q 一覧 506

関係者一覧（全て敬称略） 516

凡例・略称

- 本書は、原則として令和 8 年 1 月 1 日時点の法令等を基準としている。
  ただし、それ以降の法令でも、記載した方がよいと判断したものは適宜掲載している。
- 引用している URL の最終アクセス日は原則として令和 8 年 3 月 6 日時点である。
- 年月日の表示については原則として和暦を用いる。　例：令和 3 年 4 月 12 日
- 法令、判例・判例集等の書籍等、その他関係文書等の略称は慣例による。
- 裁判例の表示については、最高裁大法廷は「最大」、その他最高裁は「最」、高裁は「高」、地裁は「地」と略し、判決は「判」、決定は「決」と略すこととする。支部の場合は「支」と略すこととする。
  例：最判昭和 54 年 7 月 10 日民集 32 巻 4 号 1222 頁
  　　横浜地川崎支判昭和 45 年 10 月 10 日

【法令の略称】

略称	正式名称
独占禁止法	私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）
情促法	情報処理の促進に関する法律（昭和 45 年法律第 90 号）
不正アクセス禁止法	不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
電子署名法	電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
情報流通プラットフォーム対処法（旧：プロバイダ責任制限法）	特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（平成 13 年法律第 137 号） ※令和 7 年 4 月「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律の一部を改正する法律」（令和 6 年法律第 25 号）が施行され、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（プロバイダ責任制限法）から名称変更。
個情法	個人情報の保護に関する法律（平成 15 年法律第 57 号）
行個法	行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）※令和 4 年 4 月 1 日、デジタル社会形成整備法の施行に伴い廃止され、個情法に統合された。
独個法	独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）※令和 4 年 4 月 1 日、デジタル社会形成整備法の施行に伴い廃止され、個情法に統合された。

略称	正式名称
番号利用法	行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
個情法施行規則	個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）
デジタル基本法	デジタル社会形成基本法（令和 3 年法律第 35 号）
デジタル社会形成整備法	デジタル社会の形成を図るための関係法律の整備に関する法律（令和 3 年法律第 37 号）
サイバー対処能力強化法	重要電子計算機に対する不正な行為による被害の防止に関する法律（令和 7 年法律第 42 号）
サイバー対処能力強化法整備法	重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和 7 年法律第 43 号）
令和 6 年改正地方自治法	地方自治法の一部を改正する法律（令和 6 年法律第 65 号）により改正された地方自治法（昭和 22 年法律第 67 号）

【関係文書の略称】

略称	正式名称
サイバーセキュリティ 2026	サイバーセキュリティ戦略本部「サイバーセキュリティ 2026（2025 年度年次報告・2026 年度年次計画）」（令和 8 年 7 月 31 日）
政府機関等統一基準群	以下から構成される基準群 ・サイバーセキュリティ戦略本部「政府機関等のサイバーセキュリティ対策のための統一規範（令和 7 年度版）」 ・サイバーセキュリティ戦略本部「政府機関等のサイバーセキュリティ対策のための統一基準（令和 7 年度版）」 ・NCO「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」
重要インフラ行動計画	サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」
個情法ガイドライン（通則編）	個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月、令和 7 年 6 月一部改正）
個情法ガイドライン（仮名加工情報・匿名加工情報編）	個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）」（平成 28 年 11 月、令和 6 年 12 月一部改正）

略称	正式名称
個情法 QA	個人情報保護委員会「「個人情報の保護に関する法律についてのガイドライン」に関する Q&A」（平成 29 年 2 月 16 日、令和 7 年 7 月更新）
経営ガイドライン	経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」（令和 5 年 3 月 24 日）
逐条不正競争防止法	経済産業省知的財産政策室「逐条解説 不正競争防止法 令和 6 年 4 月 1 日施行版」
営業秘密管理指針	経済産業省「営業秘密管理指針」（令和 7 年 3 月 31 日最終改訂）
限定提供データ指針	経済産業省「限定提供データに関する指針」（令和 4 年 5 月最終改訂）
秘密情報の保護ハンドブック	経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」（令和 4 年 5 月最終改訂）
グループガイドライン	経済産業省「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」（令和元年 6 月 28 日策定）
電子商取引準則	経済産業省「電子商取引及び情報財取引等に関する準則」（令和 4 年 4 月、令和 7 年 2 月改訂）

【裁判例集の略称】

略称	正式名称
民集（刑集）	最高裁判所民事（刑事）判例集
集民（集刑）	最高裁判所裁判集民事（刑事）
知財集	知的財産権関係民事・行政裁判例集（法曹会）
無体集	無体財産権関係民事・行政裁判例集（法曹会）
労裁集	労働関係民事事件裁判集（法曹会）
労民	労働関係民事裁判例集（法曹会）
労刑	労働関係刑事事件判決集（法曹会）
判時	判例時報（判例時報社）
判タ	判例タイムズ（判例タイムズ社）
判自	判例地方自治（ぎょうせい）
労判	労働判例（産業労働調査所）
労経速	労働経済判例速報（経団連事業サービス）

【その他組織等の略称】

略称	正式名称
NCO	内閣官房国家サイバー統括室
NISC	内閣官房内閣サイバーセキュリティセンター （令和 7 年 7 月、国家サイバー統括室（NCO）に改組）
NICT	国立研究開発法人情報通信研究機構
IPA	独立行政法人情報処理推進機構
JPCERT/CC	一般社団法人 JPCERT コーディネーションセンター

Q1 サイバーセキュリティの定義

法令上「サイバーセキュリティ」はどのように定義されているか。

タグ：サイバーセキュリティ基本法、サイバーセキュリティの定義

１．概要

サイバーセキュリティ基本法（平成 26 年法律第 104 号。以下、本項において「基本法」という。）第 2 条において、サイバーセキュリティが定義されている[1]。保護すべき客体として情報、情報システム、情報通信ネットワークの 3 つを挙げており、外部からのサイバー攻撃への対応に限らないものとなっている。また、いわゆる情報の CIA（機密性、完全性、可用性）も定義の中に実質的に含まれている。

２．解説

基本法第 2 条は、サイバーセキュリティについて、「電磁的方式[2]により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下、本項において「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」と定義している。

保護すべき客体（措置対象）に着目して整理すると、①情報、②情報システム、③情報通信ネットワークについて必要な措置が講じられ、それが適切に維持管理されていること、ということができる。

（１）情報の安全管理のために必要な措置

措置の対象となる「情報」は、「電磁的方式により記録され、又は発信され、若しくは受信される情報」と規定されており、例えば、口頭での情報伝達は含まれない。

---

[1] デジタル基本法第 33 条、サイバー対処能力強化法第 2 条第 1 項、令和 6 年改正地方自治法第 244 条の 5 第 2 項、地方公共団体情報システムの標準化に関する法律（令和 3 年法律第 40 号）第 2 条第 2 項、及び番号利用法第 29 条の 2 は、「サイバーセキュリティ」とは、サイバーセキュリティ基本法第 2 条に規定するサイバーセキュリティをいうと規定しており、他にも同条を引用する法令が多く、同条は我が国の法令における一般的な定義といえよう。警察法（昭和 29 年法律第 162 号）施行規則第 8 条、電気通信事業法（昭和 59 年法律第 86 号）施行規則第 29 条、金融庁組織規則（平成 10 総理府令第 81 号）第 1 条等のように、「情報セキュリティ」という用語を用いる規則も少なくない。

[2] 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。

また、必要な措置については、「漏えい、滅失又は毀損の防止」と、いわゆる情報の CIA を定義の中に実質的に組み込んでいるが、これに限定せず、「その他の当該情報の安全管理のために必要な措置」と広く規定しており、外部からのサイバー攻撃に対する対策に限らず、内部不正に対する対策等も含まれることとなる。

（２）情報システム及び情報通信ネットワークの安全性・信頼性の確保に必要な措置

ここにいう安全性の確保には、情報システム又は情報通信ネットワークについて外部からの侵入が防止された状態にあることが含まれており、信頼性の確保には、情報システム又は情報通信ネットワークが、災害等により障害が起こっても迅速に復旧することが含まれている。このように、情報システム又は情報通信ネットワークの安全性・信頼性の確保に必要な措置については、外部からのサイバー攻撃への対策に限られない。

（３）情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動

情報システム及び情報通信ネットワークの安全性・信頼性の確保に必要な措置については、「情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動[3]による被害の防止のために必要な措置を含む」としている。

サイバー攻撃は、一般的に情報通信ネットワークを通じたものが想定されるが、本定義においては、「電磁的記録媒体を通じた」ものも含まれており、例えば、ネットワークと連結していない制御系のシステムを標的とし、USB メモリ等の外部記録媒体に保存された不正なプログラムを作用させて制御システムを乗っ取ることも、「電磁的記録媒体を通じた電子計算機に対する不正な活動」にあたる。

なお、いわゆるフィッシング[4]については、電子計算機そのものに対して不正な活動を行っているわけではないので、「電子計算機に対する」不正な活動にはあたらないが、フィッシング対策のための措置については、一般に、情報の安全管理のために必要な措置、又は、情報システム及び情報通信ネットワークの安全性及び信頼性の確保のための措置に含まれると考えられる。

３．参考資料（法令・ガイドラインなど）

・サイバーセキュリティ基本法第 2 条

４．裁判例

特になし

[3] ここにいう「電子計算機に対する不正な活動」は、具体例としてサイバー攻撃を念頭に置いている。

[4] 詳細については Q79 を参照されたい。

Q2 サイバーセキュリティ基本法の概要

サイバーセキュリティ基本法にはどのような規定があり、サイバーセキュリティ戦略本部及びその事務を担う NCO はどのような事務を行っているのか。

タグ：サイバーセキュリティ基本法、サイバーセキュリティ戦略本部、政府機関等統一基準群、重要インフラ統一基準、重要インフラ行動計画、GSOC

１．概要

サイバーセキュリティ基本法（以下、本項において「基本法」という。）は、サイバーセキュリティ戦略本部の設置や本部長の権限をはじめ、我が国におけるサイバーセキュリティに関する基本的施策等について規定しており、同本部及びその事務を担う NCO においても、同法の規定に基づき様々な取組がなされている。

２．解説

基本法は、デジタル社会形成基本法[1]と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進するもの（同法第 1 条）であり、総則（基本理念や関係者の責務等）、サイバーセキュリティ戦略、基本的施策、サイバーセキュリティ戦略本部に関する規定等から構成されている。

以下、同法の規定と関連するサイバーセキュリティ戦略本部及び NCO の事務に焦点を当てて概説する。

（１）サイバーセキュリティ戦略本部

基本法第 24 条は、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部を設置することを規定している。

同本部は、内閣総理大臣を本部長、内閣官房長官及びサイバーセキュリティ戦略本部に関する事務を担当する国務大臣を副本部長、本部長及び副本部長以外の全ての国務大臣を本部員とし、NCO が事務を担う（基本法第 35 条、第 36 条、内閣官房組織令第 4 条の 2）。

同本部の所掌事務として具体的に列記されているものは、以下のとおりである（同法第 25 条第 1 項各号）。

① サイバーセキュリティ戦略の案の作成及び実施の推進に関すること（第 1 号）

[1] 従来は高度情報通信ネットワーク社会形成基本法（平成 12 年法律第 144 号）が引用されていたが、同法は、令和 3 年にデジタル社会形成基本法の制定とともに廃止された。それに伴い、サイバーセキュリティ基本法第 1 条の文言も改正された。また、「情報通信技術」の定義についてデジタル社会形成基本法第 2 条を引用しており、AI、IoT、クラウドなどの先端的な技術を含む概念として「情報通信技術」を用いていることが明確化された。

② 国の行政機関、独立行政法人及び指定法人[2]におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること（第 2 号）

③ 重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュリティの確保の状況の調査を含む。）及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること（第 3 号）

④ 国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティの確保の状況の評価（情報システムに対する不正な活動であって情報通信ネットワーク又は電磁的記録媒体を通じて行われるものの監視及び分析並びにサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）を含む。）に関すること（第 4 号）

⑤ 前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること（第 5 号）

（２）サイバーセキュリティ戦略

基本法第 12 条は、サイバーセキュリティに関する施策の基本的な方針等を定めるものとして、政府がサイバーセキュリティ戦略を定める旨を規定している。なお、上記（１）のとおり、その案についてはサイバーセキュリティ戦略本部が作成する（基本法第 25 条第 1 項第 1 号）。

直近では、令和 7 年 12 月 23 日に、新たなサイバーセキュリティ戦略[3]が閣議決定されている。同戦略では、サイバー空間を取り巻く情勢認識として、厳しさを増す国際情勢と外国国家の関与が疑われるサイバー攻撃の顕在化、社会全体のデジタル化の進展とサイバー脅威の増大、AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影

[2] 「指定法人」とは、「特殊法人及び認可法人･･･のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するもの」と定義される（基本法第 13 条）。また、「特殊法人」とは、「法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成 11 年法律第 91 号）第 4 条第 1 項第 9 号の規定の適用を受けるもの」をいい、「認可法人」とは、「法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人」をいう（いずれも基本法第 13 条）。現在、「サイバーセキュリティ基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人」（令和 7 年 2 月 5 日サイバーセキュリティ戦略本部決定）に基づき、地方公共団体情報システム機構（J-LIS）、共済組合関係 7 法人、日本年金機構及び国立健康危機管理研究機構の合計 10 法人が指定されている。

[3] https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf

響等を示した上で、我が国が直面するこうした現状を踏まえて、サイバー空間を取り巻く課題として以下の 3 つを挙げている。

・我が国の国民生活・経済活動、ひいては国家安全保障に深刻な影響を与えるサイバー脅威への対応
・デジタル化の進展・浸透等とそれに伴い拡大するリスクに対応した、社会全体のサイバーセキュリティ及びレジリエンスの確保
・我が国のサイバー対応を支える人材・技術の確保と先端技術への対応

同戦略は、こうした課題認識の下、サイバー空間を取り巻く切迫した情勢、社会全体への DX の浸透や技術革新等に的確に対応し、「自由、公正かつ安全なサイバー空間」を確保し、もって基本法の目的に掲げられた「経済社会の活力向上・持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安全の確保」、「我が国の安全保障」の達成を図るためには、以下の 3 つの方向性に基づき、施策を推進する必要があるとしている。

・深刻化するサイバー脅威に対する防御・抑止
・幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上
・我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

その上で、同戦略では、これら 3 つの大きな施策軸の下、今後 5 年間に実施すべき諸施策の目標や実施方針が具体的に示されている。

（3）国の行政機関等における対策の基準の作成及び当該基準に基づく監査

サイバーセキュリティ戦略本部は、国の行政機関、独立行政法人及び指定法人[4]におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく監査等を行う（基本法第 25 条第 1 項第 2 号）。

本規定に基づくものとして、政府機関等統一基準群[5]が定められており、これは、国の行政機関、独立行政法人及び指定法人における情報セキュリティ水準を向上させるための統一的な枠組みであり、政府機関等における情報セキュリティのベースラインを定めている。

また、監査に関しては、サイバーセキュリティ戦略本部「サイバーセキュリティ対策を強化するための監査に係る基本方針」（平成 27 年 5 月 25 日戦略本部決定、令和 8 年 9 月 14 日改定（同年 10 月 1 日施行））に基づき、①マネジメント監査（政府統一基準群等に基づく施策の取組状況について、組織全体として PDCA サイクルが機能しているかとい

[4] 従来は国の行政機関、独立行政法人のみを対象としていたが、平成 28 年の基本法の改正により、指定法人が対象として加わった。
[5] 政府機関等統一基準群は、①「政府機関等のサイバーセキュリティ対策のための統一規範」、②「政府機関等のサイバーセキュリティ対策のための統一基準」、③「政府機関等の対策基準策定のためのガイドライン」から構成されている。なお、①及び②についてはサイバーセキュリティ戦略本部が、③については NCO が決定している。

う観点から検証)、②ペネトレーションテスト（情報システムに対する擬似的攻撃により侵入の可否やセキュリティ対策状況を検証)、③レッドチームテスト（情報システムに対する擬似的攻撃によりインシデント検知能力や対応プロセスまでを組織・システム・人的側面を含めて多面的に評価）の 3 つの方法により監査を実施することとされている。

（4）重要インフラ防護に関する施策の基準の作成及び当該基準に基づく施策の評価

基本法第 25 条第 1 項第 3 号は、「重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成……及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること」をサイバーセキュリティ戦略本部の所掌事務としている。

ここにいう「重要社会基盤事業者」とは、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」（基本法第 3 条第 1 項）と定義されており、いわゆる重要インフラ事業者を指す。また、「重要社会基盤事業者等」は、重要社会基盤事業者及びその組織する団体並びに地方公共団体を指す（基本法第 12 条第 2 項第 3 号)。

重要インフラの防護については、「任務保証[6]」の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現するため、官民の共通の重要インフラのサイバーセキュリティに係る行動計画として、サイバーセキュリティ戦略本部が「重要インフラのサイバーセキュリティに係る行動計画」（令和 4 年 6 月 17 日戦略本部決定、令和 8 年 7 月 31 日改定）を策定している。同行動計画においては、①安全基準等の整備・浸透、②情報共有体制の強化、③障害対応体制の強化、④リスクマネジメント及び対処態勢の整備、⑤防護基盤の強化という 5 つの施策群に基づいて、重要インフラ事業者等の自主的な取組を推進している。

他方で、国家を背景とした攻撃キャンペーンの発生等、深刻化するサイバー脅威に対し、重要インフラ事業者等におけるサイバーセキュリティの一層の確保を図るためには、重要インフラ事業者等が分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）を底上げし、各分野におけるリスクベースの取組の内容・水準を向上させる必要があることから、基本法第 25 条第 1 項第 3 号に基づき、重要インフラ事業者等におけるサイバーセキュリティの確保に係る国の行政機関が実施する施策についての統一的な基準であるサイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティ対策の

[6] 重要インフラ行動計画によれば、サイバーセキュリティ戦略において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方」を意味すると説明されている。

ための統一基準[7]」（令和 8 年 7 月 31 日戦略本部決定、令和 8 年 10 月 1 日施行）が策定された。当該基準に基づき、政府機関では、重要インフラ分野として指定されている 16 の分野[8]を対象に、各分野の実施計画の策定、各分野の重要インフラ事業者等におけるセキュリティ対策への反映、サイバーセキュリティ戦略本部による評価等を踏まえた実施計画の改善等によって、重要インフラ事業者等におけるサイバーセキュリティの一層の確保を図る。

（５）国の行政機関等におけるサイバーセキュリティの確保の状況の評価

サイバーセキュリティ戦略本部は、基本法第 25 条第 1 項第 4 号に基づき、「国の行政機関、独立行政法人及び指定法人[9]におけるサイバーセキュリティの確保の状況の評価…に関すること」を所管事務としており、具体的には、①「情報システムに対する不正な活動であって情報通信ネットワーク又は電磁的記録媒体を通じて行われるものの監視及び分析」や、②「サイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）」等の事務を遂行する。

上記①に関して、NCO はサイバーセキュリティの確保の状況の評価の一環として、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC[10]）を運用している。当該状況評価に当たっては、「サイバーセキュリティの確保の状況の評価に係る方針」（令和 7 年 7 月 1 日戦略本部決定）に基づき、GSOC においては、24 時間 365 日体制でサイバー攻撃等の不審な通信の横断的な監視、不正プログラムの分析や脅威情報の収集を実施し、各組織へ情報提供を行うとともに、年度ごとに状況評価について取りまとめている。

上記②に関して、原因究明調査等の対象となる国の行政機関等のサイバーセキュリティに関する重大な事象（特定重大事象）は、サイバーセキュリティ戦略本部「サイバーセキュリティ戦略本部重大事象施策評価規則」（平成 27 年 2 月 10 日戦略本部決定、令和 7 年 6 月 27 日改定）において、以下のとおり列挙されている。

① 国の行政機関、独立行政法人又は指定法人が運用する情報システムにおける障害を伴う事象であって、当該国の行政機関、独立行政法人又は指定法人が実施する事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの

---

[7] 「重要インフラのサイバーセキュリティ対策のための統一基準」の概要については、Q45 を参照されたい。

[8] 情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、港湾及び郵便という 16 の分野が指定されている。

[9] 従来は国の行政機関のみを対象としていたが、平成 28 年の基本法の改正により、独立行政法人及び指定法人が対象として加わった。

[10] Government Security Operation Coordination team の略。なお、基本法第 13 条に基づく監視の対象は、従来は国の行政機関のみであったが、平成 28 年の基本法改正により、独立行政法人、指定法人にも拡大された。当該法改正も踏まえ、NCO において政府機関に対する横断監視・即応調整チーム（第一 GSOC）、NCO の監督の下、IPA において独立行政法人及び指定法人に対する横断監視・即応調整チーム（第二 GSOC）が設けられている（サイバーセキュリティ 2021・12 頁参照）。下記 NCO サイトも参照されたい。
https://www.cyber.go.jp/policy/group/general/policy.html

② 情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの
③ 上記(i)及び(ii)のほか、我が国のサイバーセキュリティに対する国内外の信用を著しく失墜させ、又は失墜させるおそれがある事象

（６）横断的施策

ア 研究開発の推進

基本法第 20 条は、サイバーセキュリティに関する研究開発について規定している。研究開発の推進については、サイバーセキュリティ戦略においても、「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」の一環として、我が国の対応能力の基礎となるサイバーセキュリティ関連技術に関する研究開発等、新たな技術・サービスを生み出すエコシステムの形成、AI・量子技術を含む先端技術に対する対応・取組等の推進について記載されている。

イ 人材育成・確保

基本法第 21 条は、サイバーセキュリティに関する人材の確保等について規定している。人材育成・確保については、サイバーセキュリティ戦略においても、サイバーセキュリティ分野における多様な職務ごとに必要な知識・スキル等を体系的に整理した人材フレームワークを整備し、これを軸として、様々な施策を有機的に連携させながら、効率的・効果的な人材育成を進めること等が記載されている。

令和 7 年度に NCO の下で「サイバーセキュリティ人材フレームワークに関する検討会」が開催され、令和 8 年 4 月に、「サイバーセキュリティ人材フレームワーク 2026」が策定・公表されている[11]。

ウ 教育及び学習の振興・普及啓発

基本法第 22 条は、サイバーセキュリティに関する教育及び学習の振興と、普及啓発について規定している。

サイバーセキュリティ人材の育成に資する教育・学習の振興については、サイバーセキュリティ戦略において、基礎的素養（情報リテラシー）から高度な専門性まで段階的に習得できる場の整備を図り、産学官が連携を強化して実践的スキルや最新知見の学習機会を確保することや、これらの取組と人材フレームワークとの有機的な接続を図る方針等が記載されている。

また、サイバーセキュリティに関する普及啓発については、NCO において、サイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、更に安全・安心にインターネット

[11] https://www.cyber.go.jp/council/csjinzai/index.html 参照。

を利活用してもらうことを目的として、「インターネットの安全・安心ハンドブック」[12]を公開している。

（７）多様な主体の連携

基本法第 16 条は、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者[13]等の多様な主体による相互連携について規定している。同条を具体化する形で、平成 30 年に改正されたサイバーセキュリティ基本法に基づき組織されたのが、同法第 17 条に規定するサイバーセキュリティ協議会であった。

同協議会は、サイバー対処能力強化法整備法の施行により廃止され、同法に基づき特定不正行為（サイバー攻撃）による被害の防止のため、重要電子計算機を使用する者等を構成員とする協議会が設置された（同法第 45 条）。詳細については、Q3 を参照されたい。

（８）サイバー関連事業者・情報システム等供給事業者の責務

基本法第 7 条第 1 項には、従前、「サイバー関連事業者その他の事業者」について、自主的・積極的なサイバーセキュリティの確保及び国・地方公共団体のサイバーセキュリティ施策への協力に関する努力義務が規定されているが、サイバー対処能力強化法整備法に基づく改正により、これらに加えて、情報システム等[14]の供給者に関する規定が追加された。すなわち、情報システム等の供給者は、サイバーセキュリティに対する脅威により自らが供給した情報システム等に被害が生ずることを防ぐため、情報システム等の利用者がその安全性及び信頼性の確保のために講ずる措置に配慮した設計及び開発、適切な維持管理に必要な情報の継続的な提供その他の情報システム等の利用者がサイバーセキュリティの確保のために講ずる措置を支援する取組を行うよう努めるものとするとされている（基本法第 7 条第 2 項）。

また、NCO 及び経済産業省は、基本法第 7 条第 1 項及び第 2 項を踏まえ、情報システム等の供給者としてソフトウェア[15]の開発・供給・運用を行う事業者を「サイバーインフラ事業者」と称し、その役割等について整理・解説するとともに、当該事業者やその顧客がサイ

---

12 令和 7 年 3 月 11 日に Ver5.10 が公開されている。
https://security-portal.cyber.go.jp/guidance/handbook.html

13 「サイバー関連事業者」とは、インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう（基本法第 7 条第 1 項）。

14 「情報システム等」とは、情報システム若しくはその一部を構成する電子計算機若しくはプログラム、情報通信ネットワーク又は電磁的記録媒体をいう（基本法第 7 条第 2 項）。

15 ここでいう「ソフトウェア」には、製品として顧客に提供されるソフトウェアのほか、クラウドサービス等のソフトウェアサービス、IT/OT/IoT 機器等のハードウェア製品として提供される組み込みソフトウェア・ファームウェア、システム・サービスの構成要素として提供されるソフトウェアも含まれる。

バーセキュリティ対策の実効性を確保するための参考となる考え方を示した「サイバーインフラ事業者に求められる役割等に関するガイドライン」を策定・公表している[16]。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[16] https://www.cyber.go.jp/policy/group/kihon-2/policy.html#yakuwari

Q3 能動的サイバー防御に関する法律

能動的サイバー防御を含む措置を定めたサイバー対処能力強化法・同整備法にはどのような規定があり、事業者に対して、どのようにしてサイバー対処能力を強化するよう求めているのか。

タグ：能動的サイバー防御、サイバー対処能力強化法及び同整備法、特定重要電子計算機、インシデント報告、通信情報、アクセス・無害化、サイバー通信情報監理委員会

１．概要

昨今、厳しさを増す国際的な安全保障環境の中で平素より国家を背景として、重要インフラの機能停止や機微情報の窃取等を目的としたサイバー攻撃が行われており、サイバー分野における安全保障の確保が切迫した課題となっている。この状況は近年、一層深刻化し、攻撃の巧妙化・高度化が進むとともにサイバー攻撃関連通信数も増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大している。加えて、社会全体のデジタル化やサプライチェーンの複雑化が進展することで、あらゆる主体がサイバー攻撃のリスクに晒されるとともに、一主体に対する攻撃による被害の影響が社会全体にまで波及するおそれをはらんでおり、サイバー脅威は国民生活・経済活動を脅かすまさに災害のような存在となっている。

令和 4 年 12 月 16 日に閣議決定された国家安全保障戦略[1]では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることとし、具体的には、武力攻撃に至らないものの、国や重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合に未然に排除し、サイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入することとした。当該戦略は、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとされている。その体制整備のため、①官民連携の強化、②通信情報の利用、③攻撃者のサーバ等への侵入・無害化、④NISC の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置等の実現に向け検討を進めるとされていたところ、これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和 6 年 6 月 7 日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年 11 月 29 日に提言が取りまとめられた。

この提言を踏まえ、令和 7 年 2 月 7 日に関係法案が閣議決定され、その後国会での審議・修正を経て、サイバー対処能力強化法（以下、本項において「強化法」という。）及

[1] https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html

びサイバー対処能力強化法整備法（以下、本項において「整備法」という。）が同年 5 月 16 日に成立、同月 23 日に公布された。

こうした制定に至る経緯から、強化法では、①官民連携の強化、②通信情報の利用、及び③分析情報・脆弱性情報の提供等について定め、整備法では、④アクセス・無害化措置、及び⑤組織・体制整備について定めている。このうち、⑤に係る規定は令和 7 年 7 月 1 日に、①、③及び④に係る規定は令和 8 年 10 月 1 日に施行されている。

また、強化法第 3 条では、①重要電子計算機に対する特定不正行為（不正アクセス行為等を指す。以下同じ。同法第 2 条第 4 項参照）による被害の防止に関すること、②当事者協定の締結に関すること、③通信情報保有機関[2]における通信情報の取扱いに関すること、④情報の整理及び分析に関すること、⑤総合整理分析情報の提供に関すること、及び⑥協議会の組織に関すること等の基本的事項を定める基本方針を定めることとされており、この基本方針は、サイバー対処能力強化法の施行等に関する有識者会議の了承を経て、令和 7 年 12 月 23 日に閣議決定された[3]。

２．解説

（１）官民連携の強化

ア　特別社会基盤事業者による資産届出

強化法のもと、特別社会基盤事業者（特定社会基盤事業者[4]（いわゆる基幹インフラ事業者）のうち、「特定重要電子計算機[5]」を使用するもの。同法第 2 条第 3 項）は、特定重要電子計算機を導入した場合、製品名や製造者名等を所管大臣に届け出なければならない（同法第 4 条）。届出対象となる「特定重要電子計算機」は、重要電子計算機に対する不正な行為による被害の防止に関する法律施行令（令和 8 年政令第 47 号。以下、本項において「政令」という。）において、①経済安保推進法第 50 条第 1 項に定める「特定重要設備[6]」そのものである電子計算機又は特定重要設備の一部を構成する電子計算機（同政令第 1 条第 3 項第 1 号）、②特定重要設備と直接又は間接に接続されている電子計算機（同条項第 2 号）、③USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機（同条項第 3 号）の 3 種類に大別されている。上記②及び③について

---

2 通信情報の提供等を受けた行政機関を指す（強化法第 2 条第 9 項）。

3 https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf

4 特定社会基盤事業者は、経済安全保障推進法（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号））に基づき指定される（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html）。なお、特定社会基盤事業者に対する経済安全保障推進法に基づく特定重要設備導入の事前届出義務等に関しては、Q56 を参照されたい。

5 具体的には、特定社会基盤事業者が使用する電子計算機のうち、そのサイバーセキュリティが害された場合に、特定重要設備の機能が停止し、又は低下するおそれがあるものとして政令で定めるものを指す（強化法第 2 条第 2 項第 2 号）。

6 経済安保推進法上の「特定重要設備」については、Q56 も参照されたい。

は、主務省令（重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令。以下、本項において「省令」という。）において、さらに対象となる電子計算機が、大要、以下のとおり類型化されている。

主務省令に基づく類型（政令との対応）	補足
A. インターネットとの接続口（②及び③）	グローバル IP アドレスが割り当てられている機器
B. 特定社会基盤役務の提供に係るシステムの認証を提供する機器等（②及び③）	特定重要設備に対し、当該特定重要設備の機能に影響を与える電磁的記録を送信することができる機器の認証・認可機能を有する機器
C. 特定重要設備を含むセグメントの DMZ その他当該セグメントにアクセス可能な機器（②）	いわゆる制御 DMZ（レベル 3.5）に該当するセグメントの機器
D. 特定重要設備を含むセグメントへのアクセスを制御する機器（②）	類型 E の機器（特定重要設備及び特定重要設備と同一セグメントの機器）から直接接続するファイアウォール等
E. 特定重要設備と同一セグメントの機器（②）	特定重要設備及び特定重要設備と同一のセグメントの機器（同一の L3 スイッチ配下の機器）
F. 上記 A.~E.の特定重要電子計算機に関する重要データを保存している機器（②）	特定重要電子計算機のサイバーセキュリティを確保する観点から重要な以下の情報（ネットワーク構成図、認証情報）を保存している機器： (1) ネットワーク構成図：特定重要電子計算機の総体にかかるもののうち、IP アドレスが記載されているものであって、一時的に保存されるもの以外のもの (2) 認証情報①ある電子計算機の識別符号の全部を保存しているものであって②一時的に保存されるもの以外のもの

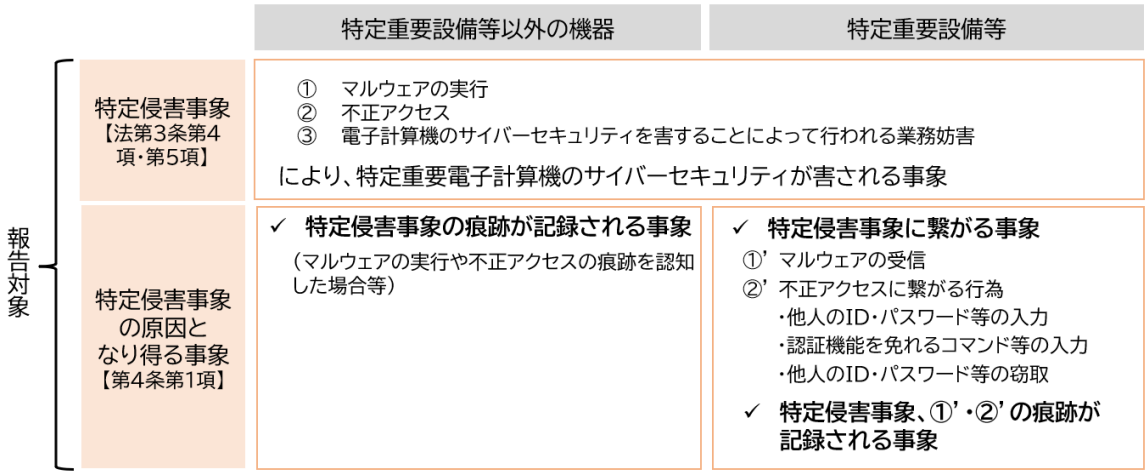
特別社会基盤事業者は、特定重要電子計算機のうち、(1) アプライアンス[7]に係るハードウェア、又は (2) アプライアンス以外の特定重要電子計算機に組み込まれたオペレーションシステム、ミドルウェア及びアプリケーションのいずれかに該当するものについて、当該特定重要電子計算機を導入した日又は変更した日から原則 4 か月以内に、所定の様式による資産届出を行う義務を負う（省令第 2 条・第 3 条）。

[7] 「アプライアンス」とは、特定の用途に供されるプログラムが組み込まれた特定重要電子計算機であって、当該プログラム以外のプログラムが通常組み込まれないものを指す（省令第 2 条第 1 項第 1 号）。

イ　特別社会基盤事業者によるインシデント報告

特別社会基盤事業者は、特定重要電子計算機に係る①「特定侵害事象[8]」又は②「特定侵害事象の原因となり得る事象として主務省令で定めるもの」のいずれかの発生を認知した場合には、所管大臣及び内閣総理大臣に報告する義務を負う（強化法第 5 条）[9]。

具体的にインシデント報告が必要となる事象の概要は、下図のとおりである（強化法第 2 条第 4 項・第 5 項、省令第 4 条第 1 項各号）。



※ 特定重要設備等の機器で発生した③については、DDoS攻撃等によって実際に業務への影響が生じた場合のみ報告を求める。【第4条第2項第3号】
※ 基幹インフラ事業者の指定を受けた日から6月以内に発生した事象等については、報告不要とする経過措置を置く。【第4条第2項第1号及び第2号】

上記①又は②の事象を認知した特別社会基盤事業者は、当該認知後、(1) 速やかに速報を、(2) 30 日以内に詳報を、所定の様式により提出しなければならない（省令第 4 条第 2 項・第 3 項）。

ウ　新協議会の設置

従来の基本法に基づくサイバーセキュリティ協議会は廃止され、強化法第 45 条に基づき、2026 年 10 月 1 日、重要電子計算機の使用者等を構成員とする官民共同の協議会

---

8 「特定侵害事象」とは「重要電子計算機に対する特定不正行為により、当該重要電子計算機のサイバーセキュリティが害されること」を指す（強化法第 2 条第 5 項）。

9 インシデント報告については、既存の業法や個人情報保護法においても報告義務が課されているものがあることから、事業者の負担を軽減する必要がある旨の指摘を受けて、強化法の成立後に策定された「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和 7 年 5 月 28 日関係省庁申合せ）において、官公署への報告等に際して利用できる共通様式を整備し、さらに官民連携基盤の整備により、これらの報告の窓口を一元化するよう所要の調整を進めるとされている（https://www.cyber.go.jp/pdf/policy/general/ref_moushiawase.pdf）。本申合せを踏まえて、令和 7 年 10 月 1 日からは、ランサムウェア攻撃と DDoS 攻撃事案におけるインシデント報告についての共通様式が決定され、運用が開始された（https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html）。

が設置された[10]。この協議会において構成員は、重要電子計算機に対する不正な行為による被害の防止に資する情報を共有し、被害の防止のための対策に関する事項及び被害防止情報を適正に管理するために必要な措置に関する事項等について協議を行う（同条第 3 項）。また協議会は、協議を行うため必要があると認めるときは、その構成員に対し、重要電子計算機に対する不正な行為による被害の防止に関し必要な情報に関する資料の提出、意見の開陳、説明その他の協力を求めることができ、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない（同条第 5 項）。なお、構成員は、共有された情報については適正管理の義務を負い、協議会事務従事者は当該情報の中でも秘密に相当するものの守秘の義務を負う（同条第 4 項、第 7 項）[11]。

また、構成員以外の者に対しても広くサイバーセキュリティ対策を促す観点から、準会員的位置づけの「協議会フレンズ」を協議会に設け、国がプッシュ型の情報提供を行うことが予定されている。

エ　罰則等

強化法違反の罰則等に関して、行政職員及び協議会構成員等による秘密の漏えい・盗用の行為については、2 年以下の拘禁刑又は 100 万円以下の罰金が科される（同法第 82 条）。また、特別社会基盤事業者がインシデント報告等を行わず、是正命令を受けてもなお対応しない場合には 200 万円以下の罰金が、特別社会基盤事業者がインシデント報告等に関連し、資料提出等を求められても対応しない場合には 30 万円以下の罰金が科される（同法第 83 条、第 84 条、第 86 条）。

（２）通信情報の利用

ア　協定（同意）に基づく通信情報の取得

強化法に基づき、内閣総理大臣は、特別社会基盤事業者等との協定に基づき、当該特別社会基盤事業者等を通信の当事者とする通信情報の提供を受け（強化法第 15 条）、当該取得通信情報に係る選別後当事者通信情報（当該提供を受けて取得した取得通信情報に自動選別を行い得られた情報）を用いて、当該特別社会基盤事業者等が使用する電子計算機のサイバーセキュリティの確保を図るために必要な分析を行った結果及びこれ

---

10 新協議会については、Q70 も参照されたい。

11 サイバー安全保障分野での対応能力の向上に向けた提言（https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf）では、「情報共有を行う場合には……攻撃の背景や目的に関する情報などのうち、特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティ・クリアランス制度を活用する等、適切な情報管理と情報共有を両立する仕組みを構築すべきである」とされており、重要経済安保情報の保護及び活用に関する法律（令和 6 年法律第 27 号。いわゆる「重要経済安保情報保護活用法」）の活用も示唆されており、この協議会が定める規約等（強化法第 45 条第 8 項）において、関連する運用ルール等が定められる可能性があると考えられる。

に関連する情報を、当該特別社会基盤事業者等に提供するものとされている（強化法第16条第1項）。

内閣総理大臣及び特別社会基盤事業者は、相互に、相手方に対し、協定を締結することについて協議を求めることができる。この場合、正当な理由がない限り、協議に応じなければならない（強化法第11条第2項）。なお、協定の締結は任意である。

イ　協定（同意）によらない通信情報の取得

強化法においては、通信情報の利用に伴う通信の秘密に対する制約を、公共の福祉との関係でやむを得ない限度にとどめるため、協定によらない通信情報の取得に係る措置を講ずるための要件及び取得した通信情報の取扱いに関する規律等を厳格に規定している。

内閣総理大臣は、外外通信（国内を経由し伝送される国外から国外への通信）であって、国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難であり、かつ、他の方法によっては当該実態の把握が著しく困難であるものに関係するものが、特定の国外関係電気通信設備を用いて提供される事業電気通信役務が媒介する国外関係通信に含まれると疑うに足りる場合において、必要と認めるときは、サイバー通信情報監理委員会（後述）の承認を受けて、当該国外関係通信により送受信が行われる媒介中通信情報の一部を取得することができる（強化法第17条、第18条）。また、外内通信（国外から国内への通信）又は内外通信（国内から国外への通信）であって、重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の外国設備を送信元又は送信先とする通信等（特定外内通信又は特定内外通信）の分析をしなければ当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難であり、かつ、他の方法によっては当該特定外内通信又は特定内外通信の分析が著しく困難であって、必要と認めるときは、サイバー通信情報監理委員会の承認を受け、国外関係電気通信事業者の設置する特定の国外関係電気通信設備であって当該国外関係電気通信設備を用いて媒介される国外関係通信に当該特定外内通信又は特定内外通信が含まれると疑うに足りるものにより送受信が行われる媒介中通信情報を取得することができる（強化法第32条、第33条）。

ウ　情報の自動選別、非識別化措置等

内閣総理大臣は、取得した取得通信情報について、何人にも閲覧等をされない自動的な方法により、コミュニケーションの本質的な内容ではない情報（機械的情報（強化法第2条第8項））であって調査すべきサイバー攻撃に関係があるもののみを選別し、記録する措置（自動選別）が終了したときは、直ちに当該措置により得られた取得通信情報（選別後通信情報）を除く取得通信情報の全て（コミュニケーションの本質的な内容

である情報等）を消去しなければならず（強化法第 22 条、第 35 条）、また、メールアドレス（ドメイン名以外の部分）その他の特定の個人を識別することができることとなるおそれが大きいと認められる情報を取り扱う際には、特定の個人を識別することができないようにするための措置（非識別化措置）を講じる必要がある（同法第 24 条第 1 項）。

さらに、強化法では、自動選別後の通信情報について、強化法に規定する一定の例外を除き、一定のサイバー攻撃による被害を防止する目的以外の目的のための利用又は提供を禁止しているほか（強化法第 23 条）、取得通信情報の安全管理措置を講ずること（第 26 条）等を定めている。また、サイバー通信情報監理委員会が、通信情報保有機関に対して法の規定に基づく検査（同法第 63 条）等を行うこととし、通信情報保有機関における法の規律の遵守を確保することとしている。

エ　罰則

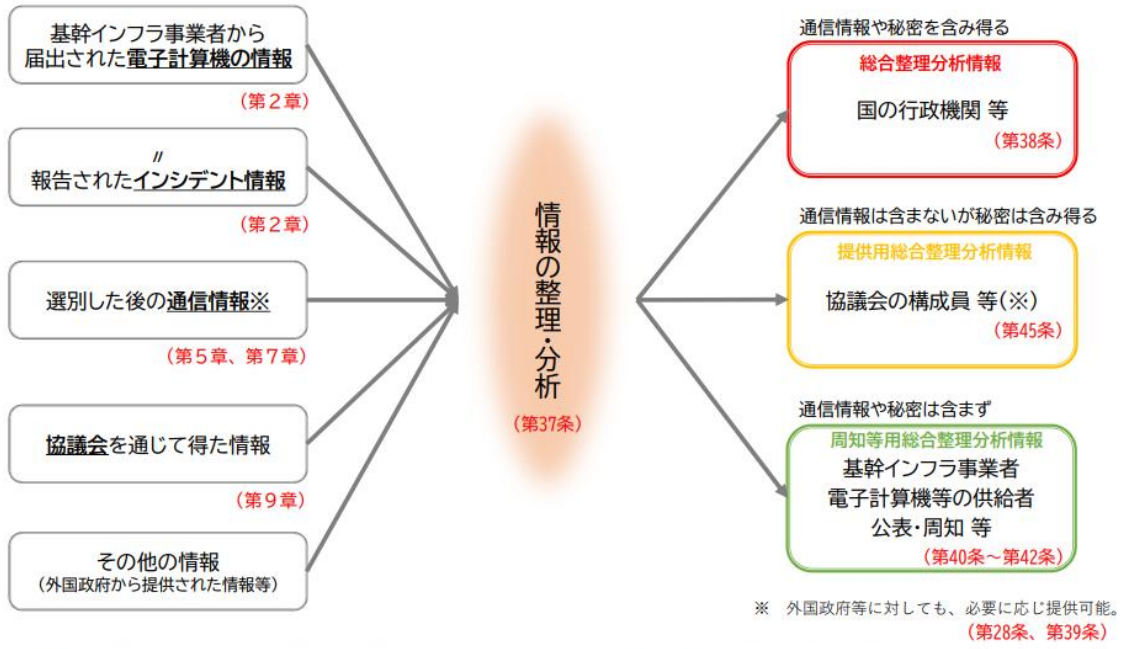
通信情報保有機関やサイバー通信情報監理委員会の職員等が、正当な理由なく業務上取り扱った取得通信情報のデータベースを提供した場合、4 年以下の拘禁刑又は 200 万円以下の罰金が科される（強化法第 79 条）。また、通信情報保有機関又はサイバー通信情報監理委員会の管理を害する行為により取得通信情報を入手した者は 3 年以下の拘禁刑又は 150 万円以下の罰金が科される（同法第 80 条第 1 項）。さらに、秘密漏えいや盗用を行った者は 3 年以下の拘禁刑又は 100 万円以下の罰金が科される（同法第 81 条）。

（３）分析情報・脆弱性情報の提供

ア　分析情報の提供

内閣総理大臣は、取得した各種の情報（電子計算機の情報、インシデント情報、通信情報、協議会を通じて得た情報等）を、重要電子計算機に対する特定不正行為による被害の防止のために整理・分析する（強化法第 37 条）。

整理・分析が行われた情報については、情報の守秘性に応じて、①「総合整理分析情報」（強化法第 37 条に基づく整理・分析が行われた情報。選別後通信情報や秘密を含み得る。）、②「提供用総合整理分析情報」（選別後通信情報は含まないが、秘密は含み得る。）、③「周知等用総合整理分析情報」（選別後通信情報や秘密を含まない。）の 3 つに大別され、それぞれに定める提供先に応じて、国の行政機関、電気通信事業者、協議会の構成員、外国の政府や国際機関等、特別社会基盤事業者及び電子計算機等の供給者等に対して提供される（強化法第 38 条、第 40 条～第 42 条、第 45 条。下図を参照）。



イ　脆弱性対応の強化

内閣総理大臣又は電子計算機等供給事業所管大臣は、総合整理分析情報その他の情報により電子計算機等における脆弱性を認知したときは、必要に応じ、電子計算機等のベンダ等に対して当該脆弱性に関する情報を提供するとともに、当該情報又は当該脆弱性への対応方法について、公表その他の方法により周知できる（強化法第 42 条第 1 項）。

また、所管大臣が、特定重要電子計算機として用いられる電子計算機又は当該電子計算機に組み込まれるプログラムにおける脆弱性を認知した場合には、当該特定電子計算機又はプログラムの供給者に対し、特定不正行為による被害を防止するために必要な措置を講ずるよう要請できる[12]（強化法第 42 条第 2 項）。

（４）アクセス・無害化措置

整備法に基づく改正により、警察官職務執行法（昭和 23 年法律第 136 号）に第 6 条の 2 第 2 項が新設され、警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃等を認めた場合であって、法定の緊急の必要があるときは、原則としてサイバー通信情報監理委員会の承認を得た上で、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる一定の措置を命じ、又は自らその措置をとることができることとされた。また、サイバー攻撃の送信元

[12] なお、整備法による改正後のサイバーセキュリティ基本法第 7 条第 2 項により、情報システム若しくはその一部を構成する電子計算機若しくはプログラム、情報通信ネットワーク又は電磁的記録媒体の供給者には、利用者のサイバーセキュリティ確保のための設計、開発、情報の継続的な提供等に努めるものとする規定が置かれた。

等である電子計算機が国内に設置されている相当な理由がない場合には、あらかじめ外務大臣との協議をすることとされた。同様に自衛隊法（昭和 29 年法律第 165 号）第 81 条の 3 も新設され、内閣総理大臣は、一定の重要電子計算機に対する攻撃であって、本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われ、自衛隊が対処する特別の必要があるときは、当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができることとされた。

（５）組織・体制整備

サイバーセキュリティについての組織体制を強化するため、整備法に基づき改正されたサイバーセキュリティ基本法では、サイバーセキュリティ戦略本部は、これまで内閣官房長官を本部長として一部の国務大臣のみを本部員としていたが、内閣総理大臣を本部長、本部長及び副本部長以外の全ての国務大臣を本部員とする体制に改組され、また、有識者から構成されるサイバーセキュリティ推進専門家会議が設置された（同法第 27 条、第 29 条、第 30 条)。また、政府が取得する通信情報の自動選別・非識別化等の適正性を監督し、検査・勧告・国会報告を通じて透明性を確保する独立機関として、サイバー通信情報監理委員会が設置された。さらに、戦略本部の所掌事務として、①重要インフラ事業者等のサイバーセキュリティ確保に関する国の基準の作成、②国の行政機関、独立行政法人等におけるサイバーセキュリティの確保の状況の評価が追加された（同法第 26 条)。

３．参照資料（法令・ガイドラインなど）

・サイバー対処能力強化法
・サイバー対処能力強化法整備法
・重要電子計算機に対する不正な行為による被害の防止に関する法律施行令
・内閣官房「サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など)」[13]
・重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令
・重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針

４．裁判例

特になし

[13] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

Q4 地方公共団体のサイバーセキュリティ

地方自治法は、地方公共団体におけるサイバーセキュリティの確保に関し、どのような内容を定めているのか。このほかに、地方公共団体におけるサイバーセキュリティ確保に関係する法令やガイドラインには、どのようなものがあるか。

タグ：地方自治法、地方公共団体、安全管理体制、リスク管理体制、サイバーセキュリティ基本法、地方公共団体情報システムの標準化に関する法律、地方公共団体情報システム標準化基本方針

１．概要

令和 6 年改正地方自治法は、普通地方公共団体に対し、その事務の処理に係る情報システムの利用に当たってサイバーセキュリティの確保、個人情報の保護その他の当該情報システムの適正な利用を図るために必要な措置を講ずることを求めている[14]。また、普通地方公共団体の議会及び長その他の執行機関に対し、それぞれその管理する情報システムの利用に当たってのサイバーセキュリティを確保するための方針を定め、必要な措置を講じ[15]、方針を定めた場合には遅滞なく公表することを定めている[16]。また、総務大臣に対しては、地方公共団体が方針を策定するに当たっての指針を示し、必要な助言を行うことを定めている[17]。これに基づいて「地方公共団体におけるサイバーセキュリティを確保するための方針の策定または変更に関する指針」（以下、本項において「総務大臣指針」という。）が策定され、令和 8 年 4 月 1 日に発出された。従来から総務省はサイバーセキュリティ基本法の責務規定に基づいて「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 8 年 3 月版）」[18]（以下、本項において「自治体セキュリティポリシーガイドライン」という。）を策定・公表してきた[19]。

このほか、地方公共団体情報システムの標準化に関する法律及び同法に基づく地方公共団体情報システム標準化基本方針がある。

以上が、地方公共団体におけるサイバーセキュリティ確保に関係する法令及び関係ガイドラインである。

---

14 地方自治法第 244 条の 5 第 2 項
15 地方自治法第 244 条の 6 第 1 項
16 地方自治法第 244 条の 6 第 2 項
17 地方自治法第 244 条の 6 第 3 項
18 平成 13 年 3 月 30 日策定・令和 8 年 3 月 27 日最終改定（https://www.soumu.go.jp/main_content/001064404.pdf）。
19 総務省は「地方公共団体における情報セキュリティ監査に関するガイドライン」（https://www.soumu.go.jp/main_content/001001338.pdf）も策定・公表してきた。

２．解説

（１）地方自治法におけるサイバーセキュリティの確保等に関する規定の創設

ア　令和 6 年改正前

令和 6 年改正前の地方自治法においては、地方公共団体で用いられる情報システムのサイバーセキュリティの確保等に関する規定は存在しなかった。

もっとも、地方公共団体のサイバーセキュリティについては、総務省による技術的助言として、自治体セキュリティポリシーガイドラインが策定・公表されている。このガイドラインには、地方公共団体における情報セキュリティに関する基本的な考え方、情報セキュリティポリシーの策定方法等の基本的な事項、及び情報セキュリティポリシーの策定例・解説が含まれている。

これを参照することにより、地方公共団体はそれぞれ、情報セキュリティポリシーを定めてきた。例えば、地方公共団体が策定及び公表している情報セキュリティポリシーとしては、「東京都サイバーセキュリティ基本方針」（令和 7 年 4 月 1 日）[20]が挙げられる。

なお、社会的基盤を構築する重要なインフラについてサイバーセキュリティを確保するための政府による行動計画である重要インフラ行動計画では、当該行動計画の適用対象となる重要インフラ事業者等に地方公共団体も含まれており、地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有するとされている[21]。また、特に重要インフラである水道分野については、水道のサイバーセキュリティ対策のために国土交通省によって「水道分野における情報セキュリティ確保に係る安全ガイドライン」が定められている[22]。

イ　令和 6 年改正の概要

地方制度調査会の答申において、国・地方公共団体等のネットワークを通じた相互接続が進展する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要等の提言があったことを踏まえ[23]、前述のとおり、令和 6 年改正地方自治法では、情報システムに関する規定として、新たに「第十一章 情報システム」が新設され、地方公共団体においてサイバーセキュリティを確保するための方針を策定すること等が定められた[24]（令和 8 年 4 月 1 日施行）。

---

[20] https://www.digitalservice.metro.tokyo.lg.jp/documents/d/digitalservice/cyber_security
[21] 重要インフラ行動計画（https://www.cyber.go.jp/pdf/policy/infra/cip_policy_2025.pdf）3.3(2)
[22] 国土交通省「水道分野における情報セキュリティ確保に係る安全ガイドライン」（令和 7 年 3 月 5 日）（https://www.mlit.go.jp/mizukokudo/watersupply/content/001869135.pdf）
[23] 前掲注 5・1 頁
[24] 地方自治法第 244 条の 6

これにより、既に情報セキュリティポリシーを策定済みの場合であっても、全ての地方公共団体が、令和 8 年 4 月 1 日までに、「サイバーセキュリティを確保するための方針」を策定・公表することが求められた[25]。

なお、地方自治法が参照しているサイバーセキュリティ基本法の詳細については、Q2 を参照されたい。

（2）標準化法とサイバーセキュリティ

ア　標準化法の概要

地方公共団体情報システムの標準化に関する法律（以下、本項では「標準化法」という。）は、「地方公共団体情報システムの標準化」[26]の推進及び実施を目的とする。すなわち、同法は、地方公共団体で共通する業務について地方公共団体ごとに独自に情報システムのカスタマイズがなされていたために、情報システムの維持管理や制度改正に対応するための改修等について地方公共団体ごとに対応しなければならないことや、情報システムの調整をすることが負担となってクラウド利用といった住民サービスを向上させるために必要な取組が円滑に進まないこと等の課題に対応するために、地方公共団体における情報システムの標準化を図るべく制定された法律である[27]。

標準化法は、地方公共団体が統一的な標準化基準に適合した標準準拠システムの利用といった地方公共団体情報システムの標準化を実施する責務を定める（同法第 4 条第 2 項）。標準準拠システムの利用対象となる事務は、政令において、20 項目に整理されている[28]。

このような標準準拠システムへの円滑かつ安全な移行によって、オンライン申請等を全国に普及させるためのデジタル化の基盤構築が進められている[29]。

イ　標準化法におけるサイバーセキュリティに関係する事項

標準化法におけるサイバーセキュリティに関係する事項は、次のとおりである。

---

[25] なお、これまで情報セキュリティポリシーを策定している地方公共団体等においては、既存の情報セキュリティポリシーの基本方針について、指針を十分に踏まえて必要に応じて見直しを行ったものの策定をもって、地方自治法第 244 条の 6 第 1 項に規定する方針に位置付けることとして差し支えないとしている。

[26] 標準化法第 2 条第 3 項

[27] デジタル庁「地方公共団体の基幹業務システムの統一・標準化」（令和 8 年 8 月 20 日最終更新）（https://www.digital.go.jp/policies/local_governments）

[28] 児童手当、子ども・子育て支援、住民基本台帳、戸籍の附票、印鑑登録、選挙人名簿管理、固定資産税、個人住民税、法人住民税、軽自動車税、戸籍、就学、健康管理、児童扶養手当、生活保護、障害者福祉、介護保険、国民健康保険、後期高齢者医療、及び、国民年金の 20 項目である（地方公共団体情報システムの標準化に関する法律第二条第一項に規定する標準化対象事務を定める政令（令和 4 年政令第 1 号））。

[29] 総務省「自治体情報システムの標準化・共通化」（https://www.soumu.go.jp/main_content/000971906.pdf）

① 標準化法は、政府の役割として、地方公共団体情報システムの標準化の推進を図るための基本的な方針を定めることを求めている（標準化法第 5 条第 1 項）。

そこで、デジタル庁による主導の下、「地方公共団体情報システム標準化基本方針」（令和 6 年 12 月。以下、本項において「標準化基本指針」という。）[30]が策定された。

この標準化基本指針では、地方公共団体の基幹業務システムの統一・標準化の意義及び目標、政府の推進方針、共通標準化基準に関する基本的な事項（データ要件・連携要件、サイバーセキュリティ、共通機能、ドキュメントの版管理等）、標準化基準の策定方法・時期、ガバメントクラウドの利用に関する事項（調達、利用、責任分界、品質保証、賠償責任等）等が示されている。

② 標準化基本指針におけるサイバーセキュリティに係る事項（標準化法第 5 条第 2 項第 3 号ロ～ニ）としては、（ⅰ）サイバーセキュリティ等に関する標準化基準、（ⅱ）地方公共団体が利用する標準準拠システム等の整備及び運用におけるセキュリティ対策に関係するガイドライン等[31]、及び、（ⅲ）ガバメントクラウド上に構築される標準準拠システム等についての考え方が示されている[32]。

③ 地方公共団体は、国が整備した全国的なクラウド環境（ガバメントクラウド）[33]の利用に努めることとされている（標準化法第 10 条）。

ガバメントクラウドは、クラウドサービスの利点を最大限に活用し、迅速、柔軟、かつセキュアでコスト効率の高いシステムとして導入されるものであり、デジタル庁が調達し、地方公共団体へ提供される[34]。デジタル庁がガバメントクラウドに求める技術要件は、国内企業と外国企業問わず、「最新かつ最高レベルの情報セキュリティを確保できること」や「データ保存の安全性を確保できること」等の基準を満たすことなどである。

---

[30] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/6a6cf2e1/20241224_policies_local_governments_doc_04.pdf

[31] 具体的には、自治体セキュリティポリシーガイドライン、地方公共団体を含めた官民共通の枠組みである重要インフラ行動計画、及び、今後策定予定の令和 6 年改正地方自治法第 244 条の 6 第 3 項に規定する総務大臣指針の 3 つが挙げられている（標準化基本指針 11 頁）。

[32] 標準化基本指針 11 頁

[33] 「ガバメントクラウド」とは、デジタル基本法第 29 条に規定する「全ての地方公共団体が官民データ活用推進基本法第二条第四項に規定するクラウド・コンピューティング・サービス関連技術に係るサービスを利用することができるようにするための国による環境の整備」として、「デジタル庁が調達し、整備するものであって、地方公共団体が標準準拠システム等を利用できるよう、地方公共団体に対し提供するクラウドサービス及びこれに関連するサービス」をいう（標準化基本指針 2.1、6.1.1）。

[34] デジタル庁「ガバメントクラウド」（令和 8 年 3 月 27 日最終更新）（https://www.digital.go.jp/policies/gov_cloud））

（３）地方公共団体におけるサイバーセキュリティに関する取組について

ア　地方公共団体におけるサイバーセキュリティ対策

総務省の調査によれば、地方公共団体のサイバーセキュリティ（情報セキュリティ）対策[35]は、下表のように、セキュリティ階層を以下の三層に分離することを基本とし、階層ごとの対策を実施する運用がされてきた[36]。

階層	対策
個人番号利用事務系 （宛名、既存住基、税、社会保障等）	端末からの情報持ち出し不可設定等を通じて、住民情報流出を徹底して防止する。
LGWAN 接続系[37] （人事給与、庶務、文書管理等）	LGWAN 接続系とインターネット接続系を分割し、LGWAN 環境のセキュリティを確保する。
インターネット接続系 （情報収集、メール、ホームページ等）	都道府県と市区町村が協力して自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施する。

また、自治体セキュリティポリシーガイドラインにおいては、策定･導入（Plan）、運用（Do）、評価（Check）、見直し（Action）の 4 段階（PDCA）サイクルを定期的に繰り返すことによって情報セキュリティの確保及び情報セキュリティ対策の水準の向上を図ることが望ましいとされている[38]。

---

[35] 自治体セキュリティポリシーガイドラインにおいては、「情報セキュリティ」という用語が用いられているが、これはサイバーセキュリティを中心としつつ、地方公共団体が職務において大量に取り扱う紙の書類等についてもセキュリティを図る必要があることから、これをセキュリティの保護対象から除外していないことによる。なお、令和 6 年改正地方自治法によって新設された「第十一章 情報システム」においては、「サイバーセキュリティ」という用語が用いられている。

[36] 総務省地域力創造グループ「新たな自治体情報セキュリティ対策の抜本的強化に向けて ～自治体情報セキュリティ対策検討チーム報告～（概要版）」（平成 27 年 11 月 24 日）4 頁（https://www.soumu.go.jp/main_content/000387560.pdf）、地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会「自治体情報セキュリティ対策の経緯について」（2021 年 9 月 27 日）2 頁（https://www.soumu.go.jp/main_content/000777002.pdf）。

[37] 「LGWAN 接続系」とは、LGWAN（Local Government Wide Area Network）に接続された情報システム及びその情報システムで取り扱うデータをいい、マイナンバー利用事務系は除かれる（自治体セキュリティポリシーガイドライン第 1 章 2.（9））。また、LGWAN とは、地方公共団体の組織内ネットワーク（庁内 LAN）を相互に接続し、地方公共団体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とする、高度なセキュリティを維持した行政専用ネットワークをいう（J-LIS「LGWAN について」（https://www.j-lis.go.jp/lgwan/about/cms_15039.html））。

[38] 自治体セキュリティポリシーガイドライン第 2 章 3

イ　J-LIS

国と地方公共団体が共同で管理する法人である J-LIS（地方公共団体情報システム機構）[39]は、情報共有サイトにおけるセキュリティ情報の提供、メールマガジン（J-LIS Security News＋）の発行、情報セキュリティインシデント対応訓練ツールの提供、インシデント発生時 CSIRT[40]対応訓練支援、サイバー攻撃検知通報等の活動を通じて、地方公共団体における情報セキュリティ対策を支援している[41]。

ウ　個人情報保護法

情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。

例えば、個情法上、地方公共団体は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置（安全管理措置）を講じなければならず[42]、地方公共団体の委託先、指定管理者、これらの者からの再委託先も地方公共団体と同等の安全管理措置を講じる義務を負うことなどが定められている[43] [44]。

３．参考資料（法令・ガイドラインなど）

・地方自治法
・サイバーセキュリティ基本法
・地方公共団体情報システムの標準化に関する法律
・地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 8 年 3 月版）
・地方公共団体における情報セキュリティ監査に関するガイドライン
・クラウドサービス提供における情報セキュリティ対策ガイドライン
・地方公共団体情報システム標準化基本方針
・重要インフラ行動計画
・水道分野における情報セキュリティ確保に係る安全ガイドライン

４．裁判例

特になし

---

[39] 地方公共団体情報システム機構法（平成 25 年法律第 29 号）を根拠法とする法人である。なお、J-LIS については、Q44 2.(5)も参照されたい。
[40] Computer Security Incident Response Team の略。
[41] J-LIS「情報セキュリティ対策支援」（https://www.j-lis.go.jp/spd/security/cms_12.html）
[42] 個情法第 66 条第 1 項
[43] 個情法第 66 条第 2 項第 1 号・第 2 号・第 5 号
[44] 自治体セキュリティポリシーガイドライン第 2 章 1

Q5 内部統制システムとサイバーセキュリティとの関係

内部統制システムとサイバーセキュリティの関係はどのようなものか。

タグ：会社法、内部統制システム、リスク管理体制、事業継続計画（BCP）、グループ・ガバナンス・システム、CSIRT、モニタリング

１．概要

会社その他の組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。取締役・理事等の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれる。

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各組織が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各組織において決定されるべきである。また、取締役会・理事会等は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定すればよい。

２．解説

（１）内部統制システムの概念とサイバーセキュリティ

後掲の各裁判例によれば、内部統制システムとは「会社が営む事業の規模、特性等に応じたリスク管理体制」と定義される。大会社[1]、監査等委員会設置会社及び指名委員会等設置会社においては、取締役会（取締役）は、内部統制システムの構築に関する事項を決定しなければならないこととされている（会社法（平成 17 年法律第 86 号）第 348 条第 3 項第 4 号、第 4 項、第 362 条第 4 項第 6 号、第 5 項、第 399 条の 13 第 1 項第 1 号ハ、第 416 条第 1 項第 1 号ホ）。それ以外の会社であっても、内部統制システムの構築に関する事項を決定しない場合に、そのことが、取締役の善管注意義務、忠実義務違反となる場合がある。会社の事業継続にとってサイバーインシデントが及ぼす影響が看過できない状況下においては、この「リスク」の中に、サイバーセキュリティに関するリスクが含まれ得るため、リスク管理体制の構築には、サイバーセキュリティを確保する体制の構築が含まれ得ると考えられる[2]。

---

[1] 「大会社」とは、直近事業年度末の資本金額が 5 億円以上の株式会社、又は負債総額が 200 億円以上の株式会社をいう（会社法第 2 条第 6 号）。上場会社の場合には、この要件を満たさない会社であっても、大会社と同等の体制を構築することが、上場規則によって要請されている。

[2] グループガイドライン 92 頁においては、「サイバーセキュリティについては、内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れたセキュリティ対策の在り方について検討されるべきである。」、経営ガイドライン 7 頁においては、「企業活動の多くをデジタル環境に依存する現在、会社法の

同体制の構築に当たっては、サイバーインシデントを未然に防止するための方策や方針（セキュリティポリシー）の策定に加え、事業継続に関する悪影響を最小化するための事業継続計画（BCP[3]）を策定する[4]ことも考えられる。特に、サイバー攻撃によるリスクとしては、情報漏えいリスクのほか、ネットワークや情報システムの停止、破壊等に起因する事業継続リスクが生じるケース（特にランサムウェア攻撃等）もあることから、BCP策定においては、（自然災害等といった典型的なシステムリスクのみならず）サイバー攻撃によるシステムリスク・事業継続リスクについても想定しておくことが重要である。

（２）会社法の内部統制システム

会社法は、大会社、監査等委員会設置会社及び指名委員会等設置会社について、内部統制システムの構築の基本方針を取締役又は取締役会が決定すべきことを明文の義務としている（会社法第 348 条第 3 項第 4 号・4 項、第 362 条第 4 項第 6 号・5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ）。これらの規定は、善管注意義務から要求される内部統制システム構築の基本方針決定義務を明文化したものである。決定すべき内部統制システムは、類型に分けて列挙されている。その中には、①法令等遵守体制、②損失危険管理体制、③情報保存管理体制、④効率性確保体制、⑤企業集団内部統制システム等が含まれる（前記引用の会社法各条及び会社法施行規則第 98 条第 1 項、第 2 項、第 100 条第 1 項、第 110 条の 4 第 2 項、第 112 条第 2 項）。サイバーセキュリティに関するリスクが、会社に重大な損失をもたらす危険がある場合には、②の損失危険管理体制（損失の危険の管理に関する規程その他の体制をいう。）に該当するため、取締役はその基本方針を決定しなければならない。

また、サイバーセキュリティインシデントに伴って漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）の対象となる情報の保存と管理に関するセキュリティは③の情報保存管理体制（取締役の職務の執行に係る情報の保存及び管理に関する体制をいう）の問題となるほか、個情法など法令が情報の安全管理を要求しているような場合には、①の法令等遵守体制（取締役及び使用人の職務の執行が法令及び定款に適合することを確保するための体制をいう。）の問題にも該当するだろう。

求める内部統制システムの構築……において、サイバーセキュリティに関するリスクを考慮しなければ実態に即したものにはならず、サイバーセキュリティを包含するエンタープライズリスクマネジメントの実践が求められている。」と記載されている。

[3] Business Continuity Plan の略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCP のうち情報（通信）システムについて記載を詳細化したものが IT-BCP（ICT-BCP）である（サイバーセキュリティ 2025 別添 8 用語解説 2 頁参照）。

[4] サイバーセキュリティ基本法におけるサイバーセキュリティの定義には、情報システムの安全性及び信頼性の確保のために必要な措置も含まれる（Q1 参照）ため、同法におけるサイバーセキュリティの確保の観点からは、サイバー攻撃への対応等はもちろん、天災等への対応も含めた情報システム運用継続計画（IT-BCP）を策定することも考えられる。

この点に関して、持株会社の子会社から顧客等の個人情報の管理について委託を受けていた持株会社の他の子会社の再委託先の従業員が当該個人情報を不正に取得して売却した情報流出事故に関して、持株会社の株主が、内部統制システムの構築等に係る取締役としての善管注意義務違反があったなどと主張して、持株会社の取締役に対し、会社法第 423 条第 1 項に基づく損害賠償金を支払うよう求めた株主代表訴訟がある。当該訴訟において、広島高裁は、持株会社及びその子会社からなる「グループにおいては、事業会社経営管理規程等の各種規程が整備され、それらに基づき、人事や事業計画への関与、グループ全体のリスク評価と検討、各種報告の聴取等を通じた一定の経営管理をし、法令遵守を期していたものであるから、企業集団としての内部統制システムがひととおり構築され、その運用がなされていたといえる。そして、会社法は内部統制システムの在り方に関して一義的な内容を定めているものではなく、あるべき内部統制の水準は実務慣行により定まると解され、その具体的内容については当該会社ないし企業グループの事業内容や規模、経営状態等を踏まえつつ取締役がその裁量に基づいて判断すべきものと解される」等と判示した[5]。

なお、上記の会社法上の規律は、大会社等の株式会社に適用されるものであるが、前述のとおり大会社等でない株式会社についても、また持分会社、一般社団法人・一般財団法人、医療法人、社会福祉法人その他の法人・団体においても、業務執行機関・理事等は、民法（明治 29 年法律第 89 号）上の善管注意義務（民法第 644 条）や一般社団法人及び一般財団法人に関する法律等に基づき、事業の継続や第三者の権利利益保護の観点から、必要なリスク管理体制を整備すべき責任を負っていることから、サイバー攻撃に起因する情報漏えいや業務停止等のリスクに対応する体制整備は、株式会社に限らず幅広い組織において内部統制上の重要な対応事項となり得ると考えられる。

（３）取締役会が決定すべき事項

会社法は、「業務の適正を確保するための体制の整備」について取締役会が決すべきものとしているが[6]、当該体制の具体的な在り方は、一義的に定まるものではなく、各会社が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各会社において決定されるべき事項である。

また、取締役会が決めるのは「目標の設定、目標達成のために必要な内部組織及び権限、内部組織間の連絡方法、是正すべき事実が生じた場合の是正方法等に関する重要な事項（要綱・大綱）[7]」でよいと解されている。

サイバーセキュリティに関していえば、当該体制の整備としては、「情報セキュリティ規程」、「個人情報保護規程」等の規程の整備や、CSIRT(Computer Security Incident

[5] 広島高判令和元年 10 月 18 日（平成 30 年（ネ）第 201 号）（請求棄却、控訴棄却）
[6] 会社法第 348 条第 3 項第 4 号、会社法第 362 条第 4 項第 6 号等
[7] 相澤哲ほか「論点解説新・会社法」（商事法務、平成 18 年）335 頁

Response Team)などのサイバーセキュリティを含めたリスク管理を担当する部署の構築等が考えられる。

これらのサイバーセキュリティ体制の整備に当たっては、経済産業省及び IPA が公表する経営ガイドラインを参照することが有用である。同ガイドラインは、経営者が認識すべき三原則及び「重要 10 項目」を提示し、国内外の拠点やビジネスパートナー、委託先を含むサプライチェーン全体を視野に入れたサイバーセキュリティリスク管理の方向性を示すものであり、リスク管理体制や法令等遵守体制等の内部統制システムをサイバーセキュリティの観点から具体化する際の指針となり得る。

さらに、中小企業については、IPA が公表する「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」（令和 8 年 3 月 27 日公表）において、中小企業の経営者が認識すべき三原則と「重要 7 項目」、具体的な対策の進め方や情報セキュリティ基本方針・関連規程等のひな形が提示されており、専門人材やコストに制約のある組織であっても、内部統制システムの一部として必要なサイバーセキュリティ体制を段階的に構築するための実務的な手掛かりとなる。

これらのガイドラインはいずれも法的拘束力を有するものではないが、例えば、経済産業省が公表するコーポレート・ガバナンス関連指針であるグループガイドライン（93 頁）においても参照が促されていることから、取締役会がサイバーセキュリティに関する基本方針や具体的な整備方針を検討する際の代表的な参照枠組みとして位置付けられる。

（4）企業集団における内部統制システム

会社法は、内部統制システムについて、会社単位での構築に加え、当該会社並びにその親会社及び子会社から成る企業集団（グループ）単位での構築を規定しており（会社法第 348 条第 3 項第 4 号、第 362 条第 4 項第 6 号、第 399 条の 13 第 1 項第 1 号ハ、第 416 条第 1 項第 1 号ホ、及び会社法施行規則第 98 条第 1 項第 5 号、第 100 条第 1 項第 5 号、第 110 条の 4 第 2 項第 5 号、第 112 条第 2 項第 5 号等）、すなわち、親会社の取締役（会）は、グループ全体の内部統制システムの構築に関する当該親会社における基本方針を決定することが求められており、子会社における①親会社への報告体制、②損失危機管理体制、③効率性確保体制、④法令等遵守体制等を含め、業務執行の中でその構築・運用が適切に行われているかを監視・監督する義務を負っている。

サイバーセキュリティに関していえば、親会社の取締役会において、子会社を含めたグループ全体を考慮に入れたセキュリティ対策について検討されるべきである[8]。特に、海外の子会社については、サイバーリスクの内容、現地の法規制及び対応実務が異なることも少なくないため、これらを考慮に入れた検討が必要となる。

[8] グループガイドライン 92 頁

（５）内部統制システムのモニタリング

取締役の善管注意義務には、上述のとおり内部統制システムの構築だけでなく、構築した後も環境変化を踏まえて内部統制システムが適切に機能しているか否かを継続的にモニタリングし、適時にアップデートすることも、その内容として含まれていると考えられている。平成 26 年の会社法改正の際には、その旨を明確化するため、内部統制システムの運用状況の概要を、事業報告の記載内容とすることが定められた（会社法施行規則第 118 条第 2 号）。

内部統制システムの運用状況をモニタリングする手段として、取締役（会）は内部監査の結果を活用することも考えられる（サイバーセキュリティに関する内部監査の役割については Q7 を参照されたい。）。

（６）金融商品取引法の内部統制

金融商品取引法（昭和 23 年法律第 25 号）は、上場会社等について、財務報告に係る内部統制の有効性の評価に関する報告書（内部統制報告書）の作成及び開示を義務付けている（いわゆる J-SOX）[9]。当該財務報告に係る内部統制は、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全という 4 つの目的を有するが[10]、IT への対応については、組織の業務内容が IT に大きく依存している場合や組織の情報システムが IT を高度に取り入れている場合において、内部統制の目的を達成するために不可欠な要素として、内部統制の有効性に係る判断の規準とされ、①IT 環境への対応と②IT の利用及び統制の 2 つの観点から対応することが求められている[11]。

（７）投資家と企業の対話ガイドライン

金融庁は、令和 3 年 6 月に、スチュワードシップ・コード及びコーポレートガバナンス・コードが求める持続的な成長と中長期的な企業価値の向上に向けた機関投資家と企業の対話において重点的に議論することが期待される事項を取りまとめた「投資家と企業の対話ガイドライン」[12]の改訂版を公表した。当該ガイドラインの 1-3 では、重点的に議論することが期待される事項として、SDGs などと並んで、「サイバーセキュリティ対応の必要性･･･等の事業を取り巻く環境の変化が、経営戦略・経営計画等において適切に反映されているか」が挙げられている。

３．参考資料（法令・ガイドラインなど）

・会社法第 348 条第 3 項第 4 号・第 4 項、第 362 条第 4 項第 6 号・第 5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ

---

[9] 金融商品取引法第 24 条の 4 の 4
[10] 企業会計審議会「財務報告に係る内部統制の評価及び監査の基準」Ⅰ.1
[11] 企業会計審議会「財務報告に係る内部統制の評価及び監査の基準」Ⅰ.2(6)
[12] https://www.fsa.go.jp/news/r2/singi/20210611-1/01.pdf

・会社法施行規則第 98 条第 1 項・第 2 項、第 100 条第 1 項、第 110 条の 4 第 2 項、第 112 条第 2 項、第 118 条第 2 号
・金融商品取引法第 24 条の 4 の 4、第 25 条第 1 項第 6 号、第 193 条の 2 第 2 項
・グループガイドライン
・金融庁「投資家と企業の対話ガイドライン」
・企業会計審議会「財務報告に係る内部統制の評価及び監査の基準」
・経営ガイドライン
・IPA「中小企業の情報セキュリティ対策ガイドライン」

４．裁判例

本文中に記載したもののほか、

・大阪地判平成 12 年 9 月 20 日判時 1721 号 3 頁・判タ 1047 号 86 頁
　米国国債の無断売却等により巨額損失が発生した事案。取締役には会社の規模・事業特性に応じたリスク管理体制（内部統制）の構築義務と、構築状況の監視義務があり、体制未整備・監視不十分が任務懈怠として広く認定され、損害賠償責任が認められた。
・金沢地判平成 15 年 10 月 6 日判時 1898 号 145 頁・労判 867 号 61 頁
　会社解散に伴う整理解雇等が主要争点であり、経営判断の相当性や労働法的枠組みが検討された事案。内部統制は直接の中心論点ではないが、品質問題等の背景事情が会社運営体制の適否の判断材料とされた。
・名古屋高金沢支判平成 17 年 5 月 18 日判時 1898 号 130 頁・労判 905 号 52 頁
　前掲・金沢地判平成 15 年 10 月 6 日の第二審。事実経過と会社対応を精査し、労働法上の基準で相当性を判断した。内部統制は中心論点ではないが、品質問題等の背景事情が会社運営体制の適否の判断材料とされた。
・東京地判平成 16 年 12 月 16 日判時 1888 号 3 頁・判タ 1174 号 150 頁
　デリバティブ取引で巨額損失が発生した事案。社内の取引限度・チェック手続の実効性を具体的に検証し、担当取締役らの内部統制の構築・運用義務違反を中心に責任が認められた。
・東京高判平成 20 年 5 月 21 日資料版商事法務 291 号 116 頁
　前掲・東京地判平成 16 年 12 月 16 日の第二審。非担当・社外等の取締役の監視義務について、特段の疑義・警鐘事情がない限り、一律に広範な責任を負わないと整理しつつ、担当取締役らには内部統制の構築・運用・報告体制の不備があれば責任が及ぶ旨が示された。
・大阪地判平成 16 年 12 月 22 日判時 1892 号 108 頁・判タ 1172 号 271 頁
　不祥事対応での報告・是正措置の不作為等を任務懈怠として問う枠組みが示され、法令遵守体制の整備・適正運用の必要性が強調された事案。
・大阪高判平成 18 年 6 月 9 日判時 1979 号 115 頁・判タ 1214 号 115 頁

違法原材料問題の認識後に「積極的に公表しない」対応を採った役員らに広く責任を認定。内部統制の構築のみならず、不祥事発覚後の是正・公表等の運用（モニタリング・損害拡大防止）義務違反が認定された事案。

・最判平成 21 年 7 月 9 日判時 2055 号 147 頁

従業員による架空売上の計上により有価証券報告書に虚偽記載が生じた事案。最高裁は、大会社取締役には通常想定される不正行為を防止し得る程度のリスク管理体制を構築すべき義務があるとしつつ、その具体的水準は事業内容・規模、過去の同種不正の有無、リスク管理体制の機能状況等を総合考慮して判断すべきであり、本件では管理体制に著しい不備や特別の予見可能性はないとして、代表取締役の任務懈怠責任を否定した。

Q6 サイバーセキュリティと取締役等の責任

会社が保有する情報の漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）によって会社又は第三者に損害が生じた場合、会社の役員（取締役・監査役）は、どのような責任を問われ得るか。

タグ：会社法、個情法、損害賠償責任

１．概要

取締役（会）が決定したサイバーセキュリティ体制が、当該会社の規模や業務内容に鑑みて適切でなかったため、会社が保有する情報が漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）（以下、本項において「漏えい等」という。）されたことにより会社に損害が生じた場合、体制の決定に関与した取締役は、会社に対して、任務懈怠（けたい）に基づく損害賠償責任（会社法第 423 条第 1 項）を問われ得る。また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、取締役・監査役（監査等委員・監査委員である取締役を含む。以下、本項において「取締役・監査役等」という。）がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である[1]。

なお、サイバーセキュリティ体制の構築・運用に当たっては、経済産業省及び IPA が公表する経営ガイドラインや、IPA が公表する「中小企業の情報セキュリティ対策ガイドライン」などの公的ガイドラインが取りまとめられており、企業の規模・事業特性に応じた対策水準を検討する際の参考とすることができる。

個人情報の漏えい等によって第三者が損害を被ったような場合、取締役・監査役等に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

他方、刑事責任についていうと、サイバーセキュリティインシデントに起因して、会社が保有する情報の漏えい等が生じた場合、当該会社の役員は、原則として、刑事責任を負うことはない。ただし、個人データに関して、その安全管理措置を怠ったため漏えい等が発生した場合など個情法の規定に違反した場合は、個人情報保護委員会による勧告・命令の対象になるほか、命令に違反した場合には、刑事罰の対象となり得る。

[1] 相澤哲ほか「論点解説新・会社法」（商事法務、平成 18 年）335 頁。

２．解説

（１）会社法上の責任

取締役は、内部統制システムの構築義務の一環として、サイバーセキュリティ体制を構築する義務を負うと解される（Q5 参照[2]。）。

取締役（会）が決定した内部統制システムが、当該会社の規模や業務内容に鑑みて、株式会社の業務の適正を確保するために不十分であった場合には、その体制の決定に関与した取締役は、善管注意義務（会社法第 330 条・民法第 644 条）違反に基づく任務懈怠責任（会社法第 423 条第 1 項）を問われ得る[3]。

また、内部統制システムは適切なものであったが、その内部統制システムが実際には遵守されておらず、取締役・監査役等がそれを知り、又は注意すれば知ることができたにも関わらず、それを長期間放置しているような場合にも、善管注意義務違反に基づく任務懈怠責任を問われ得る[4]。このとき、全員が同じ民事責任を負うのではなく、各取締役・監査役等が事件当時に置かれていた状況（役職、危険の兆候の把握の有無など）に照らして個別に判断される。

以上のとおり、サイバーセキュリティ体制の構築又はその運用に欠陥があり、情報の漏えい等によって会社に損害が生じたときは、取締役・監査役等は責任を負うことがあり得る[5]。

また、取締役・監査役等が職務を行うについて悪意又は重過失があったときは、それにより第三者に生じた損害についても賠償責任を負う（会社法第 429 条第 1 項）。

したがって、取締役・監査役等が、悪意・重過失により、適切なサイバーセキュリティ体制を構築せず、又は体制が適切に運用されていないのにこれを是正するのを怠り、個人情報の漏えい等によって第三者が損害を被ったときは、取締役・監査役等は、当該第三者に対しても責任を負うことがあり得る。

（２）その他留意すべき法令

会社が取扱う個人情報の漏えい等が生じた場合には、個情法が問題となる[6]。

個情法は、個人情報取扱事業者に対して個人情報（又は個人データ、保有個人データ）の取扱いについての義務を規定するところ、例えば、個人情報取扱事業者である会社が、個人データに係る安全管理措置（個情法第 23 条）を怠った結果、個人データが漏えい等

---

[2] 取締役の内部統制システム構築義務違反が争点となった主な裁判例のうち、サイバーセキュリティ体制そのものが直接争点となった事例としては、Q5 の 2.(2)のとおり広島高判令和元年 10 月 18 日（平成 30 年（ネ）第 201 号）。

[3] 相澤哲ほか・前掲注 1、大阪地判平成 12 年 9 月 20 日判タ 1047 号 86 頁。

[4] 相澤哲ほか・前掲注 1。

[5] それにもかかわらず、「2024 年度中小企業等実態調査結果」（https://www.ipa.go.jp/pressrelease/2024/press20250214.html）では、約 7 割の中小企業が組織的なセキュリティ体制が整備されていない状況が報告されている。

[6] 個人データの漏えい等があった場合の対応について Q57・Q58 を参照されたい。

した場合は、個人情報保護委員会による勧告・命令の対象となる（同法第 148 条）。この命令に違反をした者に対しては、1 年以下の懲役又は 100 万円以下の罰金が科され（同法第 178 条）、法人の代表者、使用人その他の従事者が、その法人の業務に関して命令違反行為を行った場合は、当該行為者を罰するほか、法人も罰金刑（1 億円以下）の対象となる（同法第 184 条第 1 項）。

したがって、個人情報の漏えい等に関して、個情法に定める義務違反がある場合には、会社の役員は、刑事罰の対象となり得る。

３．参考資料（法令・ガイドラインなど）

・会社法第 330 条、第 423 条第 1 項、第 429 条第 1 項
・民法第 644 条
・個情法第 23 条、第 148 条、第 178 条、第 184 条第 1 号
・経営ガイドライン
・IPA「中小企業の情報セキュリティ対策ガイドライン」

４．裁判例

本文中に記載のとおり

Q7 サイバーセキュリティ体制の適切性を担保するための監査等

社内のサイバーセキュリティ体制が適切であることを担保するためにどのような方策を実施することが考えられるか。

タグ：会社法、内部監査、情報セキュリティ監査、システム監査、情報開示、内部通報、CSIRT

１．概要

社内のサイバーセキュリティ体制が適切であることを担保するための方策としては、内部監査、情報セキュリティ監査、システム監査等の各種監査、内部通報、情報開示、CSIRT の設置といった方策が考えられる。

２．解説

（１）監査

ア　内部監査

会社法は、大会社、監査等委員会設置会社及び指名委員会等設置会社について、取締役（会）が内部統制システムの構築の基本方針を決定すべきことを明文の義務としているところ[1]、この内部統制システムには、会社におけるサイバーセキュリティに関する体制も含まれる（Q5 参照）。

内部統制システムに対する評価を行う仕組みとして内部監査が挙げられる。

内部監査とは、「組織体の経営目標の効果的な達成に役立つことを目的として、合法性と合理性の観点から公正かつ独立の立場で、ガバナンス・プロセス、リスクマネジメントおよびコントロールに関連する経営諸活動の遂行状況を、内部監査人としての規律遵守の態度をもって評価し、これに基づいて客観的意見を述べ、助言・勧告を行うアシュアランス業務、および特定の経営諸活動の支援を行うアドバイザリー業務」[2]とされている[3]。

サイバーセキュリティに関する体制を内部監査の対象とすることで、社内のサイバーセキュリティ体制の適切さの担保を図ることが期待できる。

---

[1] 会社法第 348 条第 3 項第 4 号・4 項、第 362 条第 4 項第 6 号・5 項、第 399 条の 13 第 1 項 1 号ハ、第 416 条第 1 項第 1 号ホ。

[2] 一般社団法人日本内部監査協会「内部監査基準」（平成 26 年改訂）2 頁。

[3] 令和 6 年 7 月 5 日、一般社団法人日本内部監査協会「グローバル内部監査基準」（日本語版）が公表された（令和 7 年 1 月 9 日より適用）。同基準は、内部監査の専門職的実施の国際フレームワーク（International Professional Practices Framework＝IPPF）の中核を成し、内部監査の品質を評価・向上させる基礎として位置付けられ、5 つのドメイン（Ⅰ～Ⅴ）と 15 原則で構成され、各原則について要求事項・実施上の考慮事項・適合していることの証拠の例が記載されている。また、同基準は、各主体において自己評価・外部評価の指針となるものであり、最新のリスク動向を踏まえた対応が促されている。

イ 情報セキュリティ監査

社内の情報資産を対象とした監査として、情報セキュリティ監査がある。これは、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと[4]を目的とした監査である。

情報セキュリティ監査は、一般的に経済産業省が定める「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」に則って実施される。情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール（管理策）を整備・運用するための実践的な規範として定められた基準であり、情報セキュリティマネジメントに関する国際規格[5]との整合をとるための改正も行われている。

情報セキュリティ監査は、社内の内部監査部門によって実施される場合は内部監査の一環として位置付けることができ、他方で、専門性の高い外部の監査機関によって実施されることもある。

なお、情報セキュリティ監査の技法を活用する形でサイバーセキュリティ体制を含めて監査を実施する場合には、リスク評価について、情報の機密性・完全性・可用性が損なわれるリスクはもちろん、企業の事業継続をはじめとした、経営レベルへの影響も重視の上、監査を行うこととなると考えられる[6]。

ウ システム監査

社内の情報システム体系を対象とした監査としてシステム監査がある。これは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて IT システムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものであり、システムの信頼性等を確保し、企業等に対する信用を高める重要な取組[7]である。

システム監査は、一般的に経済産業省が定める「システム管理基準」及び「システム監査基準」に則って実施される。

情報セキュリティ監査と同様、システム監査が、社内の内部監査部門によって実施される場合は、内部監査の一環として位置付けることができ、他方で、専門性の高い外部の監査機関によって実施されることもある。

---

[4] 経済産業省「情報セキュリティ監査基準」（令和 7 年改正）2 頁参照。
[5] ISO/IEC 27001(JIS Q 27001)及び ISO/IEC 27002(JIS Q 27002)。情報セキュリティマネジメントシステムに関する規格等については Q9 を参照されたい。
[6] この点については、経営ガイドラインも参照されたい。
[7] 経済産業省「システム監査基準」（令和 5 年 4 月）1 頁参照。

なお、システム監査基準において「システム監査は各種目的あるいは各種形態をもって実施されることから、他のガイドラインや組織体独自の諸規程・マニュアル等を、システム監査上の判断尺度として用いることもできる。特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」を参照することが望ましい」とされているとおり、情報システム監査とシステム監査については、双方が重なる部分もある[8]。

エ　監査証跡の重要性

上記のような監査を実効的に行うためには、システムの利用状況や管理状況、情報システムを構成するハードウェア、ソフトウェアに関連する各種ログ情報を含め、監査証跡[9]を残しておくことが重要である。そのために、様々なログ集積・管理のためのソリューション[10]を活用することも考えられる。このような証跡は、サイバーセキュリティインシデント発生時のフォレンジック調査などにも非常に有用である。

（２）情報開示

サイバーセキュリティに関する企業の情報を開示することは、開示の内容が過度に具体的である場合にはサイバー攻撃を誘発するおそれがあるものの、適度の開示を行うことで、サイバーセキュリティ体制の強化につながることが期待できる。情報開示に耐えるだけのサイバーセキュリティ体制の構築が必要となるからである。

現在のところ、サイバーセキュリティに特化した情報開示に関する法的な根拠や具体的な指針は存在しないものの、企業としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

詳細は Q8 のとおりであるが、既存の制度開示としては、事業報告（会社法第 435 条第 2 項）、有価証券報告書（金融商品取引法第 24 条）[11]、半期報告書（金融商品取引法第 24 条の 5)、コーポレート・ガバナンスに関する報告書（有価証券上場規程（東京証券取引

[8] この点については、経済産業省「情報セキュリティ管理基準参照表」も参照されたい。
[9] 監査証跡とは、システム監査を行う際の資料として用いられるログデータをいう。具体的には、システム監査人が追跡するために時系列に沿って操作や起きた事象、その結果行われる処理を保存し、記録することで、情報システムの信頼性や安全性、効率性、有効性などが確保されていることが証明される。
[10] 例えば、サーバやネットワーク機器、セキュリティ関連機器、アプリケーション等から集められたログ情報に基づいて、異常があった場合に管理者に通知したり対策を知らせたりする仕組みである SIEM（Security Information and Event Management）などが挙げられる。
[11] 令和 5 年 3 月 31 日以後に終了する事業年度から、サステナビリティに関する事項が開示項目に追加された（企業内容等の開示に関する内閣府令第 8 条第 1 号に定める第二号様式（記載上の注意）(30-2)）。当該サステナビリティ開示において記載すべき内容は法令上具体的に定められておらず、同項目においてサイバーセキュリティに関して記載することが全ての主体において必須ではないものの、各主体のガバナンス・リスク管理体制その他の事情を考慮し適切に記載する必要がある。Q8 も参照されたい。

所）第 204 条第 12 項第 1 号等)、適時開示（有価証券上場規程（東京証券取引所）第 402 条等）が存在する。また、任意開示として、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、統合報告書、情報セキュリティ基本方針等が挙げられる。

総務省は、令和元年 6 月に「サイバーセキュリティ対策情報開示の手引き」を公表し、情報開示の手段及び開示の在り方をまとめているため、詳細については同手引きも参照されたい。

（３）CSIRT の設置

CSIRT（シーサート）とは、Computer Security Incident Response Team の略称であり、企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと[12]をいう。

CSIRT は事業の規模、種類によって構成も形式も異なるため、その権限や活動範囲も各社によって異なるものの、最小構成の CSIRT であっても、CSIRT としての使命、サービス、活動範囲の 3 要素を定義づけることが重要である。また、組織内外の関係者と連携するためには、「PoC (Point of Contact)：信頼できる窓口」が必要である。

CSIRT は組織全体で考慮すべきであり、内部統制としてのリスク管理、事業継続マネジメントの一環として CSIRT を構築する流れが望ましいとされている。専門性の高い CSIRT の設置により、サイバーセキュリティ体制の実効性の担保を図ることが期待できる。

（４）内部通報制度

内部監査と同様、法令遵守体制の一内容としての内部通報制度の活用が挙げられる。例えば、社内における個情法に違反する態様での個人データの管理状況について、従業員が不利益を被るおそれなしにその事実を通報できる制度を整備することにより、サイバーセキュリティ体制の適切性を担保することが期待できる。

３．参考資料（法令・ガイドラインなど）

・情報セキュリティ監査基準（平成 15 年経済産業省告示第 114 号）
・情報セキュリティ管理基準（平成 28 年経済産業省告示第 37 号）
・経済産業省「システム監査基準」（令和 5 年 4 月 26 日改訂）
・経済産業省「システム管理基準」（令和 5 年 4 月 26 日改訂）
・経済産業省「情報セキュリティ管理基準参照表」

[12] サイバーセキュリティ 2025・215 頁参照。

４．裁判例

特になし

Q8 サイバーセキュリティと情報開示

企業は、サイバーセキュリティに関してどのような情報開示を行うことが望ましいか。

タグ：会社法、金融商品取引法、有価証券報告書、コーポレート・ガバナンス報告書、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、統合報告書

１．概要

サイバーセキュリティに特化した情報開示に関する法令や具体的な指針は存在しない。

もっとも、サイバーセキュリティに関する企業の情報を開示することは、開示の内容が過度に具体的である場合にはサイバー攻撃を誘発するおそれがあるものの、適度の開示を行うことで、企業の社会への説明責任を果たすとともに、経営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。また、自社のサイバーセキュリティ対策の強化につながることも期待できる。

そこで、企業としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

既存の制度開示としては、事業報告（会社法第 435 条第 2 項）、有価証券報告書（金融商品取引法第 24 条）、半期報告書（金融商品取引法第 24 条の 5）、コーポレート・ガバナンスに関する報告書（有価証券上場規程（東京証券取引所）第 204 条第 12 項第 1 号等）、適時開示（有価証券上場規程（東京証券取引所）第 402 条等）が存在する。

また、任意開示として、情報セキュリティ報告書、CSR 報告書、サステナビリティ報告書、統合報告書、情報セキュリティ基本方針等が挙げられる。

これらのほか、サイバー攻撃等に起因して損害等が発生する場合には、適時開示や臨時報告書（金融商品取引法第 24 条の 5 第 4 項）の提出が必要となる可能性もある。

なお、企業のサイバーセキュリティに関する情報開示の意義を踏まえ、総務省は、令和元年 6 月に「サイバーセキュリティ対策情報開示の手引き」を公表し、情報開示の手段及び開示の在り方をまとめている[1]ため、詳細については同手引きも参照されたい。

1 総務省「サイバーセキュリティ対策情報開示の手引き」（令和元年）13 頁等（https://www.soumu.go.jp/main_content/000630516.pdf）。

２．解説

（１）サイバーセキュリティに関する情報開示の重要性

現在のところ、サイバーセキュリティに特化した情報開示に関する法令や具体的な指針は存在しない。サイバーセキュリティに関する情報開示は、基本的には企業の任意の取組に位置付けられる。

もっとも、企業にとってサイバー攻撃が看過できないリスクとなりつつある状況において、企業のサイバーセキュリティへの取組は社会にとって重大な関心事である。企業としては、社会への説明責任の一環としてサイバーセキュリティに関する認識及び取組状況に関する情報を開示することが期待されるとともに、経営上の重要課題としてセキュリティ対策に取り組んでいることを積極的に開示することでステークホルダーから正当な評価を受けることが可能となる。また、サイバーセキュリティに関する情報を開示することは、自社のセキュリティ対策の現状を正しく認識した上で適正に運用する契機となるとともに、かつ、他社の状況との比較を通じて、さらに具体的な対策を検討・導入することで、自社のサイバーセキュリティ対策の強化につながることが期待できる。

そこで、企業としては、以下に例示する既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

（２）事業報告

会社法第 435 条第 2 項に基づき、株式会社は事業報告の作成が義務付けられている。

株式会社は、内部統制システムに関する決定又は決議をしたときは、その決定又は決議の内容の概要及び当該システムの運用状況の概要を事業報告に記載しなければならないところ（会社法施行規則第 118 条第 2 号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として決議し、その内容を事業報告に記載することによって開示することが考えられる（サイバーセキュリティと内部統制システムとの関係については Q5 を参照されたい。）。

（３）有価証券報告書・半期報告書

金融商品取引法第 24 条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項等について、内閣総理大臣に提出することが義務づけられている。

令和 5 年 3 月 31 日以後に終了する事業年度から、サステナビリティに関する事項が有価証券報告書の開示項目に追加されており、「サステナビリティに関する考え方および取組」の欄において、ガバナンス、リスク管理、戦略、指標・目標の 4 つの枠組みに沿って記載することが求められる（企業内容等の開示に関する内閣府令（昭和 48 年大蔵省令第 5 号）第 8 条第 1 号に定める第 2 号様式（記載上の注意）(30-2)）。サステナビリティに関して具体的にどのような内容を記載するかは法令上定められていないものの、データ

セキュリティやサイバーセキュリティに関する事項も「サステナビリティ」に含まれると考えられる[2]。その上で、同項目においてサイバーセキュリティに関して記載することが全ての主体において必須ではないものの、各主体のガバナンス・リスク管理体制その他の事情を考慮し、重要性及び記載の要否を判断する必要がある[3]。

事業等のリスクは、半期報告書においても記載することが求められている（企業内容等の開示に関する内閣府令第 18 条第 1 項第 1 号に定める第 4 号の 3 様式（記載上の注意）(7)）ことから、半期報告書においてもサイバーセキュリティに関するリスクを開示することが考えられる。

（４）内部統制報告書（J-SOX）

金融商品取引法は、上場会社等について、事業年度ごとに、財務報告に係る内部統制の有効性の評価に関する報告書（内部統制報告書）の作成及び開示を義務付けている[4]。

内部統制報告書の作成に際し、財務計算に関する書類その他の情報の適性を確保するための体制に関する内閣府令（内部統制府令）に定めのない事項は、「一般的に公正妥当と認められる財務報告に係る内部統制の評価の基準」に従うものとされており[5]、金融庁企業会計審議会が公表している「財務報告に係る内部統制の評価及び監査の基準」及び「財務報告に係る内部統制の評価及び監査に関する実施基準」（実施基準）等の基準が該当すると考えられるところ、同実施基準においては、サイバーリスクの高まり等を踏まえた情報システムに係るセキュリティの確保が重要であるとされている[6]。

（５）コーポレート・ガバナンスに関する報告書

金融商品取引所（証券取引所）による開示制度の一つに、コーポレート・ガバナンスに関する報告書が挙げられる。

有価証券上場規程（東京証券取引所）第 204 条第 12 項第 1 号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する基本的な考え方などを記載したコーポレート・ガバナンスに関する報告書を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている（有価証券上場規程（東京証券取引所）第 419 条）。

コーポレート・ガバナンスに関する報告書では、内部統制システムに関する基本的な考え方及びその整備状況を記載することとされているところ（有価証券上場規程施行規則第

---

[2] 金融庁「記述情報の開示に関する原則（別添）―サステナビリティ情報の開示について―」（令和 4 年）注 1 参照（https://www.fsa.go.jp/news/r4/sonota/20230131/07.pdf）。
[3] 具体例については金融庁「記述情報の開示の好事例集 2024」（https://www.fsa.go.jp/news/r6/singi/20250324-2.html）を参照のこと。
[4] 金商法第 24 条の 4 の 4 第 1 項。
[5] 内部統制府令第 1 条第 1 項。
[6] 企業会計審議会は、令和 5 年 4 月 7 日、実施基準の改訂を公表しており、当該改訂によりサイバーセキュリティの確保が重要である旨が追記された。

211 条第 4 項第 5 号)、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる。

なお、金融庁は、令和 3 年 6 月に、スチュワードシップ・コード及びコーポレートガバナンス・コードが求める持続的な成長と中長期的な企業価値の向上に向けた機関投資家と企業の対話において重点的に議論することが期待される事項を取りまとめた「投資家と企業の対話ガイドライン」[7]の改訂版を公表したところ、当該ガイドラインにおいては「サイバーセキュリティ対応の必要性……等の事業を取り巻く環境の変化が、経営戦略・経営計画等において適切に反映されているか」(1－3) について重点的に議論することが期待されるとされている。また、令和 8 年 7 月 21 日付で公表されたコーポレートガバナンス・コード (2026 年 7 月版) [8]では、「原則 4-4 取締役会の責務 III」の解釈指針において、取締役会が継続的に監督すべきリスクの一種として「サイバーセキュリティリスク」を具体的に記載する改訂が実施されている。

（６）適時開示

上場会社は、有価証券上場規程第 402 条等に基づき、剰余金の配当、株式移転、合併の決定を行った場合や災害に起因する損害又は業務遂行の過程で生じた損害が発生した場合等においては、直ちにその内容を開示することとされている[9]。

サイバー攻撃に起因して損害が発生する場合、その損害の規模や内容によっては「業務遂行の過程で生じた損害」(有価証券上場規程第 402 条第 2 号 a) として損害・損失の内容や今後の見通しを開示する必要が生じる。また、サイバー攻撃に起因して発生する損害等に照らして、「上場会社の運営、業務若しくは財産又は当該上場株券等に関する重要な事実であって投資者の投資判断に著しい影響を及ぼすもの」(有価証券上場規程第 402 条第 2 号 x) (いわゆるバスケット条項) に該当するかを検討する必要が生じることに留意されたい。

（７）臨時報告書

サイバー攻撃に起因して損害が発生する場合において、その損害の規模や内容等によって当該事象が「提出会社の財政状態、経営成績及びキャッシュ・フローの状況に著しい影響を与える事象」(企業内容等の開示に関する内閣府令第 19 条第 2 項第 12 号) に該当するとき、臨時報告書 (金融商品取引法第 24 条の 5 第 4 項) の提出が必要となる。

---

[7] https://www.fsa.go.jp/news/r2/singi/20210611-1/01.pdf
[8] https://www.jpx.co.jp/equities/listing/cg/tvdivq0000008jdy-att/nlsgeu000005lnul.pdf
[9] 実際に適時開示を行うに当たっては、東京証券取引所編「会社情報適時開示ガイドブック」が参考になる。

（８）情報セキュリティ報告書

平成 19 年 9 月に経済産業省が「情報セキュリティ報告書モデル」[10]を公表しており、企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指している。同モデルにおいては、①報告書の発行目的といった基礎情報、②経営者の情報セキュリティに関する考え方、③情報セキュリティガバナンス、④情報セキュリティ対策の計画・目標、⑤情報セキュリティ対策の実績・評価、⑥情報セキュリティに係る主要注力テーマ、⑦（取得している場合の）第三者評価・認証等を基本構成としている。

（９）CSR 報告書、サステナビリティ報告書

CSR（企業の社会的責任）報告書は、環境や社会問題などに対して企業は倫理的な責任を果たすべきであるとする CSR の考え方に基づいて行う企業の社会的な取組をまとめた報告書であり、サステナビリティ（持続可能性）報告書とも呼ばれている[11]。環境、労働、人権、社会貢献などに関する情報や、事業活動に伴う環境負荷などが幅広く公表されている。

この中にサイバーセキュリティに関する情報を含めて公表することも考えられる。

（10）統合報告書

統合報告書は、平成 25 年に国際統合報告評議会（IIRC）が公表した「国際統合報告フレームワーク」に基づき、財務情報を非財務情報と連動して開示するものである。同フレームワークでは、統合報告を「財務資本の提供者に対し、組織がどのように長期にわたり価値を創造するかを説明すること」と位置づけており、この中にサイバーセキュリティ対策に関する情報を含めることも考えられる。

（11）情報セキュリティ基本方針

情報セキュリティ基本方針は、企業や組織の内部において実施する情報セキュリティ対策の方針や行動指針であり、社内規程といった組織全体のルールから、どのような情報資産を、どのような脅威から、どのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するものである。

---

10 経済産業省「情報セキュリティ報告書モデル」https://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf

11 これらの報告書は、基本的に法令上の要請に基づくものではないが、ISO 26000（Social responsibility）等といった企業の社会的責任に関する国際的な規格に準拠した形で作成される例が多い。

３．参考資料（法令・ガイドラインなど）

・会社法第 435 条第 2 項
・会社法施行規則第 118 条第 2 号
・金融商品取引法第 24 条、第 24 条の 5
・企業内容等の開示に関する内閣府令第 8 条第 1 号において定められる第 2 号様式、第 15 条第 1 項第 1 号及び同号において定められる第 3 号様式、第 17 条の 15 第 1 項第 1 号及び同号において定められる第 4 号の 3 様式、第 19 条第 2 項第 12 号
・有価証券上場規程（東京証券取引所）第 204 条第 12 項第 1 号等、第 402 条等、第 419 条
・有価証券上場規程施行規則（東京証券取引所）第 211 条第 4 項各号
・総務省「サイバーセキュリティ対策情報開示の手引き」
・経済産業省「情報セキュリティ報告書モデル」
・金融庁「投資家と企業の対話ガイドライン」

４．裁判例

特になし

Q9 サイバーセキュリティに関する規格等と NIST SP800 シリーズ

サイバーセキュリティに関する規格等としてどのようなものがあるか。また、米国国立標準技術研究所（NIST）が公開している SP800 シリーズとは何か。サイバーセキュリティ対策に関してどのようなものがあるのか。

タグ：ISO/IEC 27000、JIS Q 15001、プライバシーマーク、NIST、FISMA、FIPS、SP800 シリーズ、NIST CSF、NIST PF

１．概要

サイバーセキュリティに関係する規格として、ISO/IEC27000 シリーズや、JIS Q 15001 等が挙げられる。後者については、一般財団法人日本情報経済社会推進協会（JIPDEC）がプライバシーマーク制度を運用している。

米国 NIST は、サイバーセキュリティの関係でも、技術仕様やベスト・プラクティス等をまとめたレポートを数多く公表している。NIST が公表しているレポートのうち、実務上特に重要なものとして、例えば、SP800-53、SP800-171、NIST CSF 及び NIST PF が挙げられる。

２．解説

（１）ISO/IEC27000 シリーズ

情報セキュリティに関する国際規格として、ISO/IEC27000 シリーズがある。これは、情報セキュリティマネジメントシステム（ISMS: Information Security Management System）に関する規格群であり、JIS としても、JIS Q 27000 シリーズとして制定されている。主なものとして以下の規格がある。

ISO/IEC27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary	ISO/IEC27000 シリーズにおける用語の定義等
ISO/IEC27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	ISMS の構築に対して組織が遵守すべき要求事項を定めたもの
ISO/IEC27002	情報セキュリティマネジメントを実施するためのベストプラクティス

Information security, cybersecurity and privacy protection — Information security controls	
ISO/IEC27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC27002 に基づき、クラウドサービスのための情報セキュリティ管理策の実践の規範を定める規格
ISO/IEC27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	ISO/IEC 27001 及び ISO/IEC 27002 の拡張規格。プライバシー保護のための要求事項とガイドラインを規定。

このうち、要求事項を定める ISO/IEC27001 は、組織が所有する情報資産を機密性・完全性・可用性の観点から適切管理するための包括的な枠組みを提供している。この要求事項に関する認証を取得することも可能であり、一般に、法人単位ではなく、法人内の部署において認証を取得することも可能である。

（２）プライバシーマーク

JIS Q 15001 は、個人情報保護マネジメントシステム（PMS: Personal information protection Management System）の要求事項を定める JIS であり、事業者が所有する個人情報を特定し、その入手から廃棄に至る一連の個人情報の取扱いを適切管理するための包括的な枠組みを提供している。

プライバシーマーク制度は、JIS Q 15001 をベースとした審査基準に適合した体制を整備しているかどうかという観点から事業者を評価し、その旨を示すプライバシーマークの使用を認めるという仕組みであり、JIPDEC が運営している。なお、プライバシーマークは法人単位で付与されることとなるため、ISMS 認証と異なり、法人の一部の部署のみで認証を受けることはできない。

PMS、ISMS ともに、これらは、「マネジメント」のシステムであって、テクノロジーに関する要求事項を定めているわけではないことに留意が必要である。マネジメントシステムであるため、サイバーセキュリティに関する技術的な対策を一通りカバーするものではない。したがって、ISMS、PMS の要求事項を遵守していれば、それ以上のサイバーセキュリティ対策が不要になるとまではいえない。

（３）米国国立標準技術研究所（NIST）について

米国国立標準技術研究所（NIST[1]）は、産業競争力のベースとなる計測技術基盤を強化するために、米国議会が 1901 年に設立した国立規格基準局（National Bureau of

[1] National Institute of Standards and Technology

Standards）を前身とし、現在は米国商務省の傘下で科学技術分野における研究を行う政府機関であり、情報セキュリティ分野においても、技術仕様やベスト・プラクティス等をまとめたレポートを数多く公表している。

米国では、平成 13 年 9 月 11 日の同時多発テロ事件を受け、連邦情報セキュリティマネジメント法（FISMA[2]）が制定された。FISMA は、NIST に対して、連邦政府機関の情報セキュリティ強化のための規格やガイドラインの開発を義務付けており、上記 NIST が公表しているレポートの一部は、FISMA に基づくものである。

（４）NIST が公表しているレポート

NIST が公表しているレポートは、以下のように分類される。

ア FIPS

NIST が FISMA の規定に基づき策定した、情報セキュリティの規格に係るレポートが、連邦情報処理標準（FIPS[3]）である。代表的な規格として、連邦政府が扱う情報や情報システムのセキュリティレベル、及びセキュリティ脅威の影響度に関する分類規格である FIPS199、連邦政府の情報や情報システムに対する最低限のセキュリティ要件を定めた規格である FIPS200 がある。

イ SP シリーズ

SP（Special Publications）シリーズは、FIPS の実践に役立つガイドライン、技術仕様、推奨策及び参照資料等をまとめたレポートである。

（ア）SP500 シリーズ

SP 500 シリーズは、基本的な情報システムの取扱いについてのレポートである。

（イ）SP800 シリーズ

SP 800 シリーズは、情報セキュリティ全般にわたるガイド、推奨、技術仕様、NIST 活動報告に関するレポートである。

（ウ）SP1800 シリーズ

SP1800 シリーズは、実用的で使用可能なサイバーセキュリティソリューションに関するレポートである。ベストプラクティスが記載されている等、実践的な文書であり、SP 800-53 やフレームワーク等との対応も記載される。

ウ NISTIR（NIST Interagency/Internal Report）

NISTIR は、FIPS や SP シリーズの策定に関する技術研究や仕様検討等の報告を行うレポートである。

---

[2] Federal Information Security Management Act of 2002
[3] Federal Information Processing Standards

エ フレームワーク

上記のほか、NIST は、より包括的・汎用的な枠組を示すドキュメントとしていくつかフレームワークを公開している。サイバーセキュリティに関係するフレームワークとして、NIST サイバーセキュリティ・フレームワーク（Framework for Improving Critical Infrastructure Cybersecurity Version 1.1。以下、本項において「NIST CSF」という。）及び NIST プライバシー・フレームワーク（NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 2.0。以下、本項において「NIST PF」という。）が挙げられる。

（５）NIST が公表しているレポートの概要の紹介

NIST が公表しているレポートのうち、実務上特に重要と考えられるものについて、以下のとおり概要を紹介する。

ア SP800-53（Revision5）[4]

SP800-53（Revision5）は、脅威やリスクから資産、個人、組織及び国家を守ることを目的として、情報システムのセキュリティ及びプライバシーの対策についてまとめたものである。米国連邦政府機関の情報システムでは、FISMA 等により、SP800-53 の管理策を使用することが義務付けられている。

従前は政府機関のみを対象としていたが、Revision5 では民間組織も対象に追加し、20 のカテゴリー[5]において 1000 を越える多様な管理策が記載されている。

イ SP800-161（Revision1）[6]

SP 800-161 （Revision 1）は、組織がサプライチェーン全体におけるサイバーリスクを特定・評価・軽減するための包括的な枠組みを示した文書であり、サプライチェーン・サイバーセキュリティリスク管理（C-SCRM）を企業レベルのリスクマネジメント活動に統合する方法を解説している。設計・取得・運用など複数のレベルにわたり、製品やサービスの供給者を含む多様なステークホルダーを対象とした多層的アプローチを採用し、SP 800-53 Rev. 5、SP 800-37 Rev. 2、SP 800-30 Rev. 1 など既存のリスク管理フレームワークと整合しているほか、米国大統領令 14028 や Federal Acquisition Supply Chain Security Act（FASCSA）とも連動し、連邦政府調達の契約要件への対応を意識した内容となっている。実務での適用を支援するためのテンプレートや付録（FASCSA

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[5] 20 のカテゴリーとは、①アクセス制御、②意識向上及びトレーニング、③監査及び説明責任、④アセスメント、認可及び監視、⑤構成管理、⑥緊急時対応計画、⑦識別及び認証、⑧インシデント対応、⑨メンテナンス、⑩媒体保護、⑪物理的及び環境的保護、⑫計画、⑬プログラムマネジメント、⑭職員のセキュリティ、⑮個人情報の取扱い及び透明性、⑯リスクアセスメント、⑰システム及びサービスの取得、⑱システム及び通信の保護、⑲システム及び情報の完全性、⑳サプライチェーンのリスクマネジメント、である。
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

対象機関や EO 関連の追加ガイダンス等）も収載され、組織が容易に導入できるよう工夫されている。

ウ SP800-171（Revision3）[7]

SP800-171（Revision3）は、非連邦政府組織及びシステムにおいて、管理すべき重要情報（CUI: Controlled Unclassified Information）について推奨されるセキュリティの要件を定めている。

エ NIST CSF2.0[8]

NIST CSF は、標題は重要インフラをターゲットとしているものであるが、このドキュメントで言及されている対策は、重要インフラであるかどうかや業種を問わずに、汎用的かつ体系的なフレームワークとして参照されている。NIST CSF は、コア（Core）、ティア（Tier）及びプロファイル（Profile）から構成されている。コアは、組織の種類や規模を問わない共通のサイバーセキュリティ対策の一覧であり、ティアは、組織のサイバーセキュリティ対策がどの段階にあるのかを評価する基準であり、プロファイルは、組織のサイバーセキュリティ対策の現在の姿と目指すべき姿をまとめたものである。NIST CSF は、令和 6 年 2 月 26 日、Ver2.0 が公開され、大きな改訂としてフレームワークの適応範囲の拡大、オンラインコンテンツの拡充に加えて、コアのサイバーセキュリティ対策について、従来の「特定」、「防御」、「検知」、「対応」及び「復旧」の 5 段階に加えて「統治」の 6 段階目が追加された。「統治」は、「組織のコンテキスト」、「リスクマネジメント戦略」、「役割、責任及び権限」、「方針」、「監督」及び「サイバーセキュリティサプライチェーンリスクマネジメント」の 6 カテゴリーから構成されており、組織の経営層がコーポレート・ガバナンスの一つとしてサイバーセキュリティリスクの管理を行うことを求めているものである。

オ NIST PF[9]

NIST PF は、サイバー攻撃に加えて、個人データの処理に関するプライバシーリスクへの対応についても解説を加えたドキュメントである。NIST PF も、NIST CSF と同様、コア、ティア及びプロファイルから構成されているが、コアは、「特定」、「統治」、「制御」、「通知」及び「防御」の 5 段階で構成されている。「統治」、「制御」、「通知」は、NIST CSF では対応できないプライバシーリスクへの対処を補完するものであり、言及されていない「検知」、「対応」「復旧」は、NIST CSF により対応することが想定されている。

---

7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
8 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
9 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

カ　その他のレポート

その他、実務上重要性が高いと考えられる NIST のレポートとその内容は、以下のとおりである。

文書名	内容
SP800-18	連邦情報システムのためのセキュリティ計画作成
SP800-30	リスクアセスメント
SP800-61	インシデントレスポンス
SP800-63	電子認証[10]
SP800-70	IT 機器
SP800-82	産業制御システム
SP800-144～146、210	クラウドコンピューティング
SP800-207	ゼロトラストアーキテクチャ

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf

Q10 情報処理安全確保支援士

「情報処理安全確保支援士」とはどのような資格か。サイバーセキュリティとどのような関係があるのか。

タグ：情促法、情報処理安全確保支援士、情報セキュリティサービス基準

１．概要

情報処理安全確保支援士は、平成 28 年に創設されたサイバーセキュリティに関する専門人材の国家資格である。情報処理安全確保支援士になるためには、試験に合格するなどにより登録資格を得た上で、登録手続きをする必要があり、令和 8 年 4 月 1 日時点で 26,453 人が登録されている。情報処理安全確保支援士には、守秘義務等の義務が課されることとなるが、登録者は他の資格取得に当たって優遇を得られることがある。

２．解説

（１）意義、役割について

平成 28 年に情促法が改正され、国家資格として情報処理安全確保支援士（以下、本項において「登録セキスペ」という。）[11]制度が創設された。登録セキスペは、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業務としている。また、セキュリティの専門家のみならず、IT 及びセキュリティを専門としない人にも説明・連携するという役割が求められている。

具体的には、企業の事業リスクのうち、情報セキュリティリスクについて、経営層、事業部門に対して平易な説明を行い、必要な支援、協力、連携を取り付けることや、セキュリティ事故が発生した際にも、必要な専門家と連携しながら、早期に回復できるように、経営層、事業部門、情シス部門相互間の橋渡しの推進を行うことなどが期待されている。

（２）登録セキスペとなるための要件について

登録セキスペになるためには、毎年春期と秋期に実施される情報処理安全確保支援士試験に合格するなどにより登録資格を得た上で、登録手続を行う必要がある。令和 8 年 4 月時点で 26,453 名が登録されている。

[11] 通称として「登録セキスペ（登録情報セキュリティスペシャリスト）」、英語名として「RISS（Registered Information Security Specialist）」がある。

（３）法令上の義務等

ア　法令上の義務

① 信用失墜行為の禁止義務（情促法第 21 条）
登録セキスペは、その信用を傷つけるような行為をしてはならない。

② 秘密保持義務（情促法第 22 条）
登録セキスペは、正当な理由がなく、その業務に関して知り得た秘密を漏らし、又は盗用してはならない。登録セキスペでなくなった後においても同様である。

③ 講習の受講義務（情促法第 23 条）
登録セキスペは、オンライン講習を毎年 1 回、集合講習を 3 年に 1 回受講しなければならない。

これらの義務に違反した場合、登録の取消し、又は名称の使用停止処分の対象となり（情促法第 16 条第 2 項）、秘密保持義務に違反した場合は、これに加え刑事罰の対象となる（情促法第 76 条第 1 項）。なお、これは、告訴がなければ公訴を提起することができない親告罪である（同条第 2 項）。

イ　名称独占（情促法第 24 条）

登録セキスペでない者は、「情報処理安全確保支援士」という名称を用いてはならない。逆に言えば、登録セキスペのみが、「情報処理安全確保支援士」という資格名称を名刺や論文等に掲示することができる。これに違反した場合、30 万円の罰金が科される（情促法第 78 条第 2 号）。

ウ　登録の更新（情促法 12 条 2 項）

登録セキスペの有効期限は、登録日又は更新日から起算して 3 年であり、3 年ごとに、義務付けられた講習を全て修了した上で更新手続をしなければ効力を失う（令和 2 年情促法改正により導入）ため、その点留意が必要である。

（４）登録セキスペとなることのメリット

IPA は、情報処理に関する業務を行うために必要な専門の知識及び技能を有する者を養成し、及びその資質の向上を図ることを業務の 1 つとしており、登録セキスペとなった者は、毎年の講習による知識の最新化や、集合講習などの場での登録セキスペ同士のつながりなどで、継続的に知識・スキルを習得することができる。

また、経済産業省は、登録者数 5 万人を目指しており、登録簿及び検索サービスを設置して就業機会等における資格活用のチャンス拡大を図っている。

さらに、登録セキスペについては、関連資格取得についての優遇措置があり、現在、情報セキュリティ監査人の業務に携わるための資格取得の優遇制度[12]がある。

なお、令和元年 8 月には、登録セキスペの自己研鑽や相互共助によるスキル維持及びスキル向上の場の提供や、登録セキスペ同士のつながりを広げ深めるための交流活動などを目的とした情報処理安全確保支援士会（JP-RISSA）が任意団体として発足した。

（5）登録セキスペを社内に持つことの意義

ア　IT ベンダの場合

IT ベンダ企業の場合、登録セキスペを社員としていることで、顧客視点でのセキュリティ要求事項の理解が進むこととなる。

また、情報セキュリティサービス（情報セキュリティ監査サービス、脆弱性診断サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービス、機器検証サービスのいずれか又は全てのサービス）に関する一定の基準を設けることで、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的として経済産業省が策定した「情報セキュリティサービス基準第 4.1 版」（令和 7 年 4 月 1 日）においては、情報セキュリティサービスの提供に辺り、専門性を有する者の在籍状況を技術要件としているところ、脆弱性診断サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービス、機器検証サービスの提供に必要な専門性を満たす資格者として、登録セキスペが挙げられている。

イ　ユーザ企業の場合

IT を利活用する企業、組織においては、登録セキスペを社員として情報セキュリティ関連部門に配置することで、経営層と一体となったセキュリティ対策を推進することができ、例えば、セキュリティポリシーの策定、サイバーセキュリティリスクの把握及びこれに対応するために必要となる対策の検討など、自社において、対応が可能となる。

加えて、登録セキスペはセキュリティの専門家であることから、システム調達先やセキュリティベンダと密に連携を取ることができ、サイバーセキュリティリスクを許容できる程度まで低減させる対策が可能となる。

3．参考資料（法令・ガイドラインなど）

・情促法第 3 条から第 25 条
・経済産業省「情報セキュリティサービス基準第 4.1 版」（令和 7 年 4 月 1 日）

[12] 特定非営利活動法人日本セキュリティ監査協会(JASA)「高度情報セキュリティ資格特例制度」（https://jasa.jp/qualification/acquisition/info_secure_supporter/）。

４．裁判例

特になし

Q11 技術情報管理認証制度について

「技術情報管理認証制度」は、どのような制度か。

タグ：産業競争力強化法、技術情報管理認証制度、技術等情報漏えい防止措置、重要技術マネジメント、現地審査を含む認証、情報セキュリティ、第三者認証

１．概要

この制度は、事業者が保有する技術等情報（技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報）について、事業者の適切な管理を担保するため、産業競争力強化法（平成 25 年法律第 98 号）に基づき、技術等情報を適切に管理している事業者を国が認定した第三者機関（認定技術等情報漏えい防止措置認証機関。以下、本項において「認証機関」という。）が審査し、認証する制度（以下、本項において「本認証制度」という。）である。

２．解説

（１）背景・経緯

事業者にとって重要な技術等情報の管理（守り方）については、専門家等による意見も踏まえて、経済産業省が「重要技術管理ガイドライン」（平成 29 年 4 月公表）[1]を作成したところ、事業者から、ガイドライン遵守についての認証制度創設の要望が聞かれた[2]。

加えて、信頼できる取引先等との技術等情報の共有の円滑化がイノベーション促進の観点等から重要とされる中、日本経済の基盤を支え、国内企業数の 99%を占める中小企業等における技術等情報の管理を適確に進めていくことが不可欠であるものの、情報セキュリティの自己評価に関するアンケートを中小企業に対して実施したところ、情報セキュリティ体制を整えるだけのリソースがない、どの情報が重要なのか分からない、重要情報をどのように管理すればいいか分からない等の理由から、情報セキュリティの取組を全く行っていないと答えた企業が 3 割程度あった[3]。

---

[1] 経済産業省製造産業局「製造産業における重要技術の情報の適切な管理に関する基準となる考え方の指針（ガイドライン）（初版）」（平成 29 年 4 月）（https://warp.da.ndl.go.jp/info:ndljp/pid/11554520/www.meti.go.jp/policy/mono_info_service/mono/technology_management/guideline0.pdf）。

[2] 株式会社三菱総合研究所「平成 30 年度中小企業等の技術情報管理状況等調査事業報告書」（平成 31 年 3 月 29 日）技術等情報漏えい防止措置に係る検討会資料 1-4-1 技術等の情報の管理に係る認証機関の認定制度の創設（https://warp.da.ndl.go.jp/info:ndljp/pid/11663694/www.meti.go.jp/meti_lib/report/H30FY/000010.pdf）。

[3] 株式会社三菱総合研究所「平成 30 年度中小企業等の技術情報管理状況等調査事業報告書」（平成 31 年 3 月 29 日）5 頁、22 頁（https://warp.da.ndl.go.jp/info:ndljp/pid/11663694/www.meti.go.jp/meti_lib/report/H30FY/000010.pdf）。

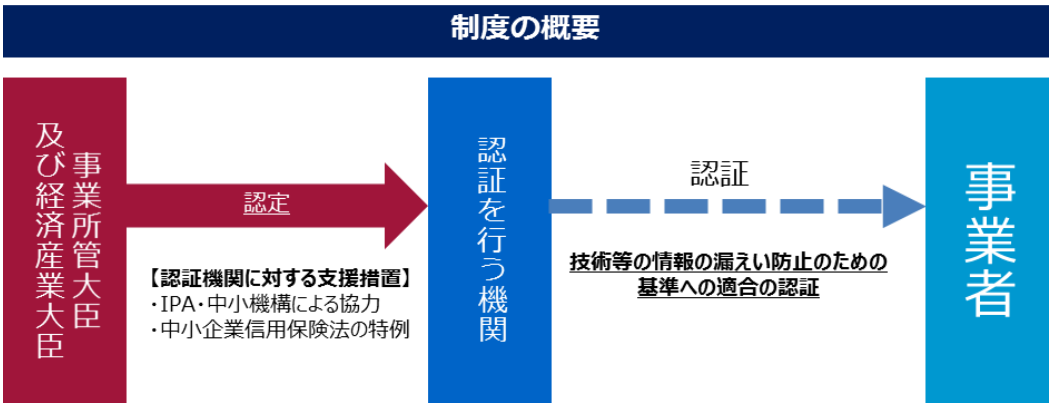
（２）要旨

本認証制度は、上記背景を踏まえ、技術等情報について、事業者の適切な管理を担保するため、事業者の情報セキュリティ対策の取組が国で示した「守り方」に即していることを、国が認定した認証機関の審査によって確認されれば、認証を受けられる制度である。

下記のとおり、国に認定された認証機関が事業者を認証するという仕組みとなっており、令和８年４月末時点で、６機関が認証機関として認定されている。

本認証制度による認証を取得することにより、自社が適切な情報セキュリティ対策の取組を行っていることを対外的に示すことができるとともに、取引先から実際の確認（監査）を行うことなく情報管理レベルを把握してもらうことができ、取引先との関係で一定の信頼性を確保することができる。

図　技術情報管理認証制度の概要[4]



また、「守り方」については、事業者、有識者の意見やパブリックコメントを踏まえて、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」（認証基準）が告示として制定され、示されている[5]。認証基準は、サイバーセキュリティだけではなく、物理的対策・人的対策をカバーしている点が特徴。また、社会環境の変化に対応するため、「自工会・部工会のサイバーセキュリティガイドライン」のレベル１項目を網羅するとともに、「ISO27001」の一部項目を取り入れる改正を令和６年８月に実施した。

[4] 経済産業省技術情報管理認証制度ポータルサイト（https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html）。
[5] https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf

なお、経済産業省は、認証基準をもとに自社の情報セキュリティ対策の状況確認に活用できる「技術情報管理 自己チェックリスト」[6]を公表しており参考になる。

（３）情報セキュリティマネジメントシステム（ISMS）認証との違い

本認証制度は、法律に基づく制度であるほか、自社のレベルに合わせて実際に導入する情報セキュリティ対策を選択できる制度として設計されており、また、認証機関による指導・助言が認められるなど、情報セキュリティ体制の構築が難しい比較的規模が小さい事業者でも認証を取得することができ、ISMS 認証[7]を取得するためのリソースが十分にない事業者でも活用することができる。

３．参考資料（法令・ガイドラインなど）

・産業競争力強化法第 2 条第 26 項・第 27 項、第 67 条～第 79 条[8]
・技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準（認証基準）[9]
・技術等情報漏えい防止措置の実施の促進に関する指針（促進指針）[10]
・「技術情報管理認証制度」ポータルサイト[11]

４．裁判例

特になし

[6] https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html
[7] ISMS については Q9 を参照。
[8] 平成 25 年法律第 98 号（https://laws.e-gov.go.jp/law/425AC0000000098）。
[9] 令和 6 年 8 月 16 日内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第 1 号（https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf）。
[10] 平成 30 年 9 月 25 日内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第 5 号（https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/02.pdf）。
[11] 「技術情報管理認証制度」ポータルサイト（https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html）。

Q12 DX 認定・DX 銘柄とサイバーセキュリティ

デジタルガバナンス・コードに基づく DX 認定、DX 銘柄とは何か。認定に際してサイバーセキュリティはどのような位置づけになっているのか。

タグ：DX 銘柄、DX 認定、デジタルガバナンス・コード、プライバシーガバナンスガイドブック、情促法、IPA

１．概要

DX 認定制度とは、日本における DX の遅れを踏まえて、各事業者に、ただのデジタル化ではなく、経営戦略としてデジタル技術の活用を前提としてビジネスモデル等を抜本的に変革し、新たな成長・競争力強化につなげていく「デジタルトランスフォーメーション（DX）」に取り組み、新しい価値を創造するインセンティブを与えるため、令和 2 年 5 月 15 日に施行された改正情促法に基づく認定制度である。経済産業省が策定したデジタルガバナンス・コードの認定基準等を踏まえ、当該認定がなされる。

また、DX 銘柄とは、経済産業省、東京証券取引所及び情報処理推進機構が企業価値向上につながる、「デジタルトランスフォーメーション（DX）」を推進するための仕組みを社内に構築し、優れたデジタル活用の実績が表れている企業を選定して紹介するものであり、これも令和 2 年から始まった。「DX 銘柄」の選定においては、DX 認定制度やデジタルガバナンス・コードと有機的に連動するように評価基準が設けられている。

２．解説

（１）DX 認定制度の背景

DX とは、「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」をいうとされている[1]。これは、ただ情報・各種プロセスを電子化する、データを利活用する、人力作業を AI や RPA（Robotic Process Automation）で代替することで効率化・コストダウンを図るのみではなく、経営戦略として、データ・デジタル技術を利用し、情報・各種プロセス・人的物的リソース・サービスを有機的につなぎ、これまで効率化や人的物的リソースの投入だけでは実現できなかった、ビジネスモデルの刷新やユーザ視点での新しい価値の創造・質の向上、組織における変革を起こすことを指す。

[1] 経済産業省商務情報政策局情報技術利用促進課「DX 認定制度の概要及び申請のポイントについて」（令和 3 年 8 月 6 日）（https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/0806_dx-certification_point.pdf）。

日本においては、デジタル化が進んでいないと指摘されているが、経営陣も巻き込んだ経営戦略としてデータ・デジタル技術を活用する DX はさらに進んでいないとも言え、このような状況を踏まえると、ユーザのニーズに応えられていないだけでなく、海外企業との競争という観点からも厳しい状況にあると考えられる。

（２）DX 認定

上記（１）のような状況を踏まえ、日本における DX を促進するため、DX 認定制度が創設された。

ア　具体的なプロセス

申請対象となるのは全ての事業者であり、これには、法人（会社のほか、公益法人等を含む。）及び個人が含まれる。これらの事業者が DX 認定を受けるに当たっては、概ね、以下のようなプロセスを経ることが想定されている[2]。なお、申請は通年可能であり、令和 8 年 9 月現在、2,275 の事業者が DX 認定を受けている[3]。

① データ活用やデジタル技術の進化による、社会及び競争環境の変化の影響も踏まえた経営ビジョン及び経営ビジョンの実現に向けたビジネスモデルの策定
② 経営ビジョンに基づくビジネスモデルを実現するため、データとデジタル技術を活用した既存ビジネスモデルの変革や、新規ビジネスモデルの創出に向けた方策のほか、必要な体制・組織のあり方や、その構築に向けた人材育成・確保に関する方策、IT システム環境の整備に向けた方策等を盛り込んだ DX 戦略を策定
③ 取締役会等において、①及び②について承認の上、その内容を公表
④ DX 戦略の達成度を測る指標を設定し、内容を公表
⑤ 経営者による効果的な戦略の推進等を図るために必要な情報発信

上記プロセスを経た後、当該事業者は、IPA に対して認定の申請を行う。後述するデジタルガバナンス・コードに基づく IPA の審査結果を踏まえ、経済産業省によって認定される。

イ　メリット

DX 認定を受けることより、以下のようなメリットが挙げられる。

まず、上記のような DX 認定のためのプロセスを通じ、DX を推進することで、当該事業者における業務効率化や新規事業の創出等による企業価値の向上が図られることになる。

---

[2] https://www.ipa.go.jp/digital/dx-nintei/shinsei.html
[3] 詳細は、IPA ウェブサイト「DX 認定制度 認定事業者の一覧」を参照（https://disclosure.dx-portal.ipa.go.jp/p/dxcp/top）。

加えて、当該事業者が中小企業である場合には、日本政策金融公庫による融資の際に基準金利よりも低い利率での融資を受けることが可能であり[4]、また、民間金融機関からの融資を受ける際の信用保証協会による信用保証について、追加保証や保証枠の拡大を受けることが可能となる[5]。

さらに、人材育成の訓練に対する支援措置として、訓練経費や訓練期間中の賃金の一部等について助成を受けることができる[6]ほか、ものづくり・商業・サービス生産性向上促進補助金を申請した際に、審査において加点を受けることができる[7]。

また、国から「DX 推進の先進的な取組を行う事業者である」との公的な認定が与えられ、その旨が IPA のウェブサイトにも掲載されるとともに、DX 認定制度ロゴマークの利用が可能になる。DX 認定を受けた事業者は、これらを用いて自社のブランディングを図ることによって、人材の募集等に役立てることができるほか、顧客や取引先の獲得にもつながり得る。

（3）デジタルガバナンス・コード

経済産業省は、企業価値向上に向けて経営者が実践すべき事柄をデジタルガバナンス・コードとして取りまとめ、令和 6 年には改訂版となる「デジタルガバナンス・コード 3.0」を公表した[8]。

当該コードは、全体像を「DX 経営に求められる 3 つの視点・5 つの柱」と整理し、概ね、各柱について、（1）①柱となる考え方、②認定基準、（2）望ましい方向性を説明している。

3 つの視点と 5 つの柱は以下のとおり。

柱① 経営ビジョン・ビジネスモデルの策定
　　視点① 経営ビジョンと DX 戦略の連動
柱② DX 戦略の策定
柱③ DX 戦略の推進
　　視点②As is-To be ギャップの定量把握・見直し
柱④ 成果指標の設定・DX 戦略の見直し
　　視点③ 企業文化への定着
柱⑤ ステークホルダーとの対話

---

[4] https://www.jfc.go.jp/n/finance/search/11_itsikin_m_t.html
[5] https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html
[6] 厚生労働省「人材開発助成金 人への投資促進コースのご案内(詳細版)」(令和 8 年 8 月 3 日)（https://www.mhlw.go.jp/content/11800000/001731974.pdf)。
[7] 経済産業省「ものづくり・商業・サービス生産性向上補助金総合サイト 公募要領」(令和 8 年 2 月 6 日)（https://portal.monodukuri-hojo.jp/about.html)。
[8] 経済産業省「デジタルガバナンス・コード 3.0」（令和 6 年 9 月 19 日）（https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc3.0.pdf)。

特に、3.0 の改訂においては、以下のポイントが強調された。

・経営におけるデータ活用やデータ連携の重要性
・デジタルスキル標準を参照した社員のスキル可視化や経営者を含めた役員・管理職の意識改革、キャリア形成支援等の重要性
・第三者監査やサプライチェーン保護に向けた対策等の重要性

また、サイバーセキュリティに関連して、柱となる考え方は、「経営者が事業実施の前提となるサイバーセキュリティリスクに対して適切に対応を行う。」としており、認定基準は、「DX 戦略の実施の前提となるサイバーセキュリティ対策を推進していること。」としている。認定にあたっての判断は、経営ガイドライン等に基づき対策を行い、セキュリティ監査（内部監査を含む）を行っていることの説明文書等の提出をもって確認することとしている。

関連して、経済産業省及び総務省は、Society5.0 の時代における企業の役割、プライバシーの考え方や企業のプライバシーガバナンスの重要性を前提に、令和 2 年 8 月に「DX 時代における企業のプライバシーガバナンスガイドブック ver1.0」を公開し、令和 5 年 4 月には、参考となる具体的な事例を更新した ver1.3 を公開しており[9]、DX を推し進める企業がプライバシーガバナンスを検討する上で参考になると思われる。

（4）DX 銘柄

経済産業省は、企業の戦略的 IT 利活用の促進に向けた取組の一環として、東京証券取引所と共同で、中長期的な企業価値の向上や競争力の強化のために、経営革新、収益水準・生産性の向上をもたらす積極的な IT 利活用に取り組んでいる企業を、「攻めの IT 経営銘柄」として平成 27 年から選定してきた。令和 2 年からは、デジタル技術を前提として、ビジネスモデル等を抜本的に変革し、新たな成長・競争力強化につなげていく「デジタルトランスフォーメーション（DX）」に取り組む企業を「デジタルトランスフォーメーション銘柄（DX 銘柄）」として選定している[10]。

「DX 銘柄」の選定においては、「企業価値貢献」、「ステークホルダーとの対話」及び「DX 実現能力」に着眼して評価を行っている。さらに、令和 8 年の選定においては、デジタルガバナンス・コードの「望ましい方向性」を踏まえつつ、AI の急速な技術進歩をとらえ、機動的・抜本的に、変革の範囲を拡充し、その質・スピードを高める企業をより一層評価した。

---

[9] 総務省「DX 時代における 企業のプライバシーガバナンスガイドブック ver1.3」（令和 5 年）（https://www.soumu.go.jp/main_content/000877678.pdf）。

[10] 詳細は、経済産業省作成の右記ウェブサイト参照（「DX 銘柄／攻めの IT 経営銘柄」（https://www.meti.go.jp/policy/it_policy/investment/keiei_meigara/dx_meigara.html））。

３．参考資料（法令・ガイドラインなど）

・情促法

・デジタルガバナンス・コード

・経営ガイドライン

・DX 時代における企業のプライバシーガバナンスガイドブック ver1.3

４．裁判例

特になし

Q13 個情法の安全管理措置義務とサイバーセキュリティの関係

企業が個人情報を取り扱うに当たって、個情法が要求する安全管理措置を講ずるための具体的な対応はどのようなものか。企業が取り扱う個人情報について、保存・消去、本人からの訂正・消去等請求への対応における注意点は何か。
また、企業におけるサイバーセキュリティ対策と個情法への対応の関係性はどのようなものか。

タグ：個情法、個人データ、安全管理措置、保有個人データ、ISO/IEC27001、JIS Q 15001、P マーク

１．概要

個情法上、個人情報取扱事業者は、個人データの安全管理のために「必要かつ適切な」措置を講ずる必要があるところ、当該措置は、個人データの漏えい、滅失又は毀損（以下、本項において「漏えい等」という。）をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。現況調査のためには、データの棚卸とその結果に基づくリスク分析評価が有益である[1]。

また、個人データの漏えい等を防止するためには、保有する個人データの正確性、最新性を確保しつつ、利用する合理的な必要性が直ちには存在しない個人データを保持せず、なおかつ、利用する必要がなくなった個人データを遅滞なく消去することも重要である。

２．解説

（１）はじめに

企業が個人情報を取り扱うに当たっては、原則として個情法が適用される。そこで、各々の企業は、同法が要求する安全管理措置義務とはどのようなものであるかを把握した上で具体的な対応を行うことが求められる。

個情法第 23 条では、安全管理措置として「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と規定しており、「その他の個人データの安全管理のために必要かつ適切な措置」には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを

[1] 「データマッピング・ツールキット」について、下記サイトを参照されたい（https://www.ppc.go.jp/personalinfo/independent_effort/）。

予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれるとされている（個情法ガイドライン（通則編）3-4-2）。

同規定は、取り扱う個人情報の内容、規模及び個人情報の取扱い態様に関わらず、個人情報取扱事業者に対して一律に課されるものであることから、実際に個人情報を取り扱う現場における「必要かつ適切」であると言えるための安全管理の水準設定と、具体的な措置内容を精査し、判断することが必要となる。

ここにいう「個人データ」とは、個人情報データベース等[2]を構成する個人情報のことをいう（個情法第 16 条第 1 項、第 3 項）。例えば、名刺が束のまま未整理の状態（他人には容易に検索できない独自の分類方法により分類された状態を含む）で保管されている場合は、名刺に記載された情報は、個人情報には当たるが個人データには当たらない。一方で、名刺の情報が名刺管理ソフト等で入力・整理されている場合は、特定の個人情報を検索することができるよう体系的に構成されているとして、名刺に記載された情報[3]は、個人データに該当する[4]。

以下では、企業が個人データの安全管理措置義務に対応するため、また、対応の実施に際して必要となる内部規程・ガイドライン等の策定、体制整備、技術的対策等の具体的な措置について確認する。また、これらに関連するものとして、個人情報の保存・消去、本人からの訂正・消去等の請求について確認しつつ注意点に触れることとする。

（２）個情法における安全管理措置

個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならない。個情法ガイドライン（通則編）は、「個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。」としており、また、同ガイドラインにある手法例については、必ずしも全てに対応する必要はなく、また、適切な手法はこれらの例示の内容に限られないとしている（同ガイドライン「10（別添）講ずべき安全管理措置の内容」参照）。

同ガイドラインでは、具体的な措置として、①基本方針の策定、②個人データの取扱いに係る規律の整備、③組織的安全管理措置、④人的安全管理措置、⑤物理的安全管理措置、

---

[2] 特定の個人情報をコンピュータを用いて検索することができるよう体系的に構成した、個人情報を含む情報の集合物、又は、コンピュータを用いてない場合であっても、紙面で処理した個人情報を一定の規則で整理・分類し、特定の個人情報を容易に検索することができるように目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものも該当する。

[3] 例えば、多数の個人情報が保存されているデータベースから 1 人分の個人情報を紙面に出力したとしても、当該紙面に記載された個人情報は個人データに該当する（個情法ガイドライン（通則編）2-6 も参照されたい。）。

[4] 詳細は個情法ガイドライン（通則編）2-4、2-6 を参照されたい。

⑥技術的安全管理措置を列挙している。さらに、令和 2 年の個情法改正を踏まえたガイドラインの改正により、安全管理措置の内容として⑦「外的環境の把握」が追加された。安全管理措置は、組織的に取り組むことが肝要であるところ、具体的な措置を講じる前提として、①基本方針の策定を行うことが重要であり、同ガイドラインでは、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等を含めた基本方針を策定することが挙げられている[5]。

②個人データの取扱いに係る規律の整備を行うに当たっては、組織的安全管理措置（③）、人的安全管理措置（④）、物理的安全管理措置（⑤）及び技術的安全管理措置（⑥）の内容を織り込むことが重要である。

③組織的安全管理措置を行うに当たっては、組織体制の整備（責任者の設置及び責任の明確化等）、個人データの取扱いに係る規律に従った運用、個人データの取扱状況を確認するための手段の整備、漏えい等の事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直しといった措置を講じることが求められる。

④人的安全管理措置を行うに当たっては、従業者に対して適切な教育を行うことが求められる。

⑤物理的安全管理措置としては、個人データを取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止、個人データの削除及び機器、電子媒体等の廃棄が求められる。

⑥技術的安全管理措置としては、アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報システムの仕様に伴う漏えい等の防止が求められる。

⑦外的環境の把握としては、外国において個人データを取り扱う場合、当該外国の個人情報保護制度を把握した上で、安全管理措置を講じることが求められる。

具体的な手法の例については、同ガイドラインのほか、個情法 QA「1-10 講ずべき安全管理措置の内容」（Q10-1～Q10-25）等を参照されたい[6]。また、個人情報保護委員会においては、四半期ごとに監視・監督権限の行使状況を公表し、漏えい等事案の概要及び指導事項等を示している[7]。

---

[5] また、上記の安全管理措置を講ずるための前提として、企業内のデータの取り扱いの現況を把握することが肝要であり、実務上は、いわゆるデータの棚卸作業を行うケースがある。データの棚卸とは、手順等が確立しているものではないが、一般的に、当該企業において取り扱っているデータ及び当該データの利用態様を把握するために、各部署へ質問票を配布し、実際にデータを取り扱っている担当者に質問票の記入を求め、適宜必要な調整を行っていくという手法である。

[6] 個情法ガイドライン（通則編）において、従業員の数が 100 人以下の中小規模事業者については、取り扱う個人データの数量及び個人データを取り扱う従業員数が一定程度にとどまること等を踏まえ、講ずべきとされている安全管理措置について、円滑に義務を履行しうるような手法の例が示されている。

[7] https://www.ppc.go.jp/personalinfo/activity/

（３）漏えい発生時の対応

個人情報取扱事業者は、個情法規則で定める、個人データの漏えい等が発生し、又は発生したおそれがある事態（報告対象事態）が生じたときは、個人情報保護委員会への報告及び本人通知を行う必要がある（個情法第 26 条）。

なお、報告対象事態のうち個情法施行規則第 7 条第 3 号（不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データの漏えい等又はそのおそれ）の対象は、「個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予想されているものを含む。）」とされるため、例えば、個人情報取扱事業者のウェブサイトの入力ページが第三者に改ざんされ、ユーザが当該ページに入力した個人情報が当該第三者に送信された場合であり、かつ、当該個人情報取扱事業者が、当該ページに入力される個人情報を個人情報データベース等へ入力することを予定していたときは、報告対象事態に該当するとされている[8]。

（４）保有個人データに関する安全管理措置の公表等

保有個人データとは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データをいい、取り扱う情報がこの保有個人データに該当する場合には、事業者は、本人の求めに応じて遅滞なく回答する場合も含め、一定の事項を本人の知り得る状態に置かなければならない（以下、本項において「公表等」という。）。令和 2 年個情法改正に伴い、どのような安全管理措置が講じられているかについて、本人が把握できるようにする観点から、公表等すべき事項が一部追加され、保有個人データの安全管理のために講じた措置（上記（２）の①～⑦）についても公表等すべきこととなった（個情法第 32 条第 1 項第 4 号、同法施行令第 10 条第 1 号。ただし、保有個人データの安全管理のために講じた措置のうち、公表等することにより保有個人データの安全管理に支障を及ぼすおそれがあるものは、同号括弧書により、公表等の対象から除かれている。）。①～⑦の中で、特に⑦の「外的環境の把握」との関係については留意すべきであり、外国において個人データを取り扱う場合、当該外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を公表等する必要がある[9]。

「本人の知り得る状態」とは、本人が知ろうとすれば知ることができる状態に置くことをいい、常にその時点での正確な内容を知り得る状態に置かなければならないと考えら

[8] 個情法施行規則第 7 条第 3 号、個情法ガイドライン（通則編）3-5-3-1。
[9] 例えば、外国にある支店・営業所に個人データを取り扱わせる場合、外国にある第三者に個人データの取扱いを委託する場合、外国に所在するクラウドサービス提供事業者の管理するサーバに個人データを保存する場合、外国に所在するサーバに個人データを保存する場合等には、当該外国の制度等を把握した上で安全管理措置を講じる必要がある（詳細は、個情法 QA10-22～10-25）。

れている。そのため、必ずしもウェブサイトへの掲載や事務所等の窓口等へ掲示すること等が継続的に行われることまで必要ではないが、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

上記のとおり、「公表等」は、必ずしもウェブサイトへの掲載を求められるものではないが、実務上は、自社ウェブサイトに設置しているプライバシーポリシーにおいて公表する例が多いため、安全管理措置についてもここで公表することが考えられる。なお、公表等すべき事項の一部をウェブサイトに掲載して公表し、残りの事項は本人の求めに応じて遅滞なく回答する、という対応も可能である。

（５）個人データの保存・消去、本人からの訂正・消去等の請求

個人データの漏えい等を防止するためには、保有する個人データの正確性、最新性を確保しつつ、利用する合理的な必要性が直ちには存在しない個人データを保持しないことが重要である。個情法上も、個人データは、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならず、また、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならないとされており（個情法第 22 条）、遅滞なく消去することは、個人データの漏えい等を防止する観点からも重要である。

なお、本人は、個人情報取扱事業者に対して、当該本人が識別される「保有個人データ」（個情法第 16 条第 4 項）[10]の開示を請求することができる（同法第 33 条第 1 項）。

加えて、保有個人データについては、その内容が事実でない場合、利用目的の達成に必要な範囲内において、本人からの訂正等の請求に応じる義務もある（同法第 34 条第 1 項、第 2 項）。

このほか、本人は、個人情報取扱事業者に対し、個情法に規定された事由（目的外利用、不正取得等）がある場合に、保有個人データの利用停止等又は第三者への提供の停止を請求することができる。令和 2 年個情法改正により、そのような事由として、保有個人データを利用する必要がなくなった場合、保有個人データに係る報告対象事態（Q57 参照）が生じる場合、その他本人の権利又は正当な利益が害されるおそれがある場合が追加されている（個情法第 35 条第 5 項）。

（６）サイバーセキュリティ対策との関係

サイバーセキュリティ基本法第 2 条にいう「サイバーセキュリティ」の定義（Q1 参照）には、情報の安全管理のための措置をとり、それが適切に維持管理されていることが含まれており、その点では個情法に基づく個人データの安全管理措置義務と法文上類似する。

[10] 個人データのうち、個人情報取扱事業者が、本人等から請求される開示等に応じることができる権限を有するもの。詳細は個情法ガイドライン（通則編）2-7 を参照されたい。

ただし、サイバーセキュリティは、個人データに限らず、不正競争防止法（平成 5 年法律第 47 号）にいう営業秘密や価値あるデータ（限定提供データ）など、「情報」を全般的に対象とするものである。また、サイバーセキュリティの定義には、情報の安全管理のみならず、情報システム及び情報通信ネットワークの安全性・信頼性も明示的に定義に含んでいる点で、個情法に基づく個人データの安全管理措置義務とは異なるといえる。

なお、企業等におけるサイバーセキュリティ対策の実効性担保のため仕組み[11]としては、情報セキュリティマネジメントの規格として、ISMS[12]要求事項を記した ISO/IEC27001（JIS Q 27001）を挙げることができる。また、個人情報を対象とする日本産業規格として、JIS Q 15001（個人情報保護マネジメントシステムー要求事項）があり、一般財団法人日本情報経済社会推進協会（JIPDEC）は、当該要求事項に基づく個人情報保護マネジメントシステムを定めていること等を条件としてプライバシーマーク（P マーク）を付与する制度を運営している。さらに、PIA[13]については、国際標準として、ISO/IEC 29134 が、PIA の実施プロセス及び PIA 報告書の構成・内容についてのガイドラインを提供しており、これの日本産業規格として、JIS X 9251 がある。

３．参考資料（法令・ガイドラインなど）

・個情法
・個情法ガイドライン（通則編）
・個情法 QA

４．裁判例

特になし

[11] Q7 も参照されたい。
[12] Information Security Management System の略。
[13] プライバシー影響評価(Privacy Impact Assessment)。個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法を指す。個人情報保護委員会の下記ページも参照されたい。https://www.ppc.go.jp/personalinfo/independent_effort/

Q14 個人データの取扱いの委託と安全管理

委託先に個人データを取り扱わせる場合、委託元にどのような監督責任が生じるのか。

タグ：個情法、個人データ、委託、監督、監査、外的環境の把握

１．概要

個情法では、個人データの取扱いを委託する場合に、委託先において当該個人データについて安全管理措置が適切に講じられるよう、委託先に対し必要かつ適切な監督を行うことが求められる。具体的には、①適切な委託先の選定、②委託契約の締結、③委託先における個人データの取扱状況の把握などが考えられる。

２．解説

（１）考え方

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託[1]する場合は、委託先において当該個人データについて安全管理措置が適切に講じられるよう、委託先に対し必要かつ適切な監督を行わなければならない（個情法第 25 条）。

「全部又は一部を委託」とされているとおり、一部を委託する場合、すなわち委託元の個人データの取扱いの一部を委託先に処理させる場合はもちろん、取扱いの全部を委託する場合でも、委託元には委託先への監督責任が生じる。

具体的には、個人情報取扱事業者は、個情法第 23 条に基づき自らが講ずべき安全管理措置（個人データの漏えい、滅失、又は毀損の防止等）と同等の措置が講じられるよう、必要かつ適切な監督を行うものとされている。

なお、個人データの第三者提供に当たっては原則として本人の事前同意が必要だが（個情法第 27 条第 1 項）、個人データの取扱いの委託に伴って当該個人データを委託先に提供する場合には、委託先は「第三者」に該当しないとされるため、本人の事前同意を得ることなく委託先に個人データを提供することが可能である（同法第 27 条第 5 項第 1 号）[2]。

[1] 個人データの取扱いの委託とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いを行わせることをいい、具体的には、個人データの入力、編集、分析、出力等の処理を行うことを委託することが想定される。

[2] ただし、「外国にある第三者」の場合は、国内にある第三者とは異なる制限が設けられている。詳しくは、Q15 を参照されたい。

（２）委託先を監督する責任の内容

委託先の監督責任の内容は、個情法ガイドライン（通則編）3-4-4 によれば、委託業務の内容に対して必要のない個人データを提供しないことをはじめとして、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい、滅失又は毀損（以下、本項において「漏えい等」という。）をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に起因するリスクに応じた、必要かつ適切な措置を講じることとされている。

具体的には、①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握等が考えられる。

（３）適切な委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも個情法第 23 条及び個情法ガイドライン（通則編）において委託元に求められるものと同等であることを確認するため、同ガイドライン「10（別添）講ずべき安全管理措置の内容」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない。

（４）委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい。

（５）委託先における個人データの取扱状況の把握

委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

また、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱方法等について、委託先から事前報告を受けること又は承認を行うこと、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が個情法第 23 条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様である。

個情法ガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」において明確に委託に言及しているものとして、以下のものが挙げられる。

・組織的安全管理措置のうち、個人データの取扱いに係る規律に従った運用の手法例として、「個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。）」が挙げられている。
・物理的安全管理措置について、「個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。」とされている。

（６）委託先の監督責任に関する留意点

委託先の監督責任に関しては、上記のとおり個情法第 25 条が問題となるが、それ以外の法令が問題となる場合があるため、同法はもちろん、他の法令に適合しない対応にならないよう注意すべきである。

例えば、具体的には、優越的地位にある者が委託元の場合、委託先に不当な負担を課す場合や、従業者等から取得する個人情報に関する誓約書において損害賠償額の予定や違約金を定めることなどが労働基準法第 16 条に違反する場合等が挙げられる。また、いわゆるサプライチェーン・リスク対策に関しては Q53 も参照されたい。

（７）外国における個人データの取扱い

個人情報取扱事業者は、外国において個人データを取り扱う場合[3]には、「外的環境の把握」として、当該外国の個人情報保護制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない（個情法第 23 条、個情法ガイドライン（通則編）10-7）。

委託先（再委託先を含む）が外国において個人データを取り扱う場合も同様であって、委託元は、当該外国の個人情報保護に関する制度等を把握した上で、委託先の監督その他の安全管理措置を講じる必要がある。その上で、「保有個人データの安全管理のために講じた措置」として、当該外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要がある（個情法 QA10-24）。

３．参考資料（法令・ガイドラインなど）

・個情法第 23 条、第 25 条
・個情法ガイドライン（通則編）3-4-4

[3] なお、外国において個人データを取り扱う場合の留意点としては、本トピックが対象としている安全管理措置との関係以外に、第三者提供との関係がある。これについては、Q15 を参照されたい。

４．裁判例

特になし

Q15 クラウドサービスの活用と個情法

クラウドサービスを活用している場合に、個情法上どのような点に留意すべきか。

タグ：個情法、安全管理措置、委託先の監督、クラウドサービス、外国にある第三者、外的環境の把握

１．概要

第三者の提供するクラウドサービスを利用し 、その管理するサーバに個人データを保存する場合において、クラウドサービスを提供する事業者（以下、本項において「クラウドサービス提供事業者」という。）が当該個人データを取り扱わないこととなっている場合には、当該クラウドサービスを利用する事業者（以下、本項において「クラウドサービス利用事業者」という。）は、クラウドサービス提供事業者に当該個人データを「提供」したことにはならないため、個情法第 27 条第 1 項、第 28 条第 1 項に基づく事前同意の取得は不要であり、また、個情法第 25 条に基づきクラウドサービス提供事業者を監督する義務は負わない。ただし、かかる場合であっても、クラウドサービス利用事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。

他方、クラウドサービス提供事業者が個人データを取り扱うこととなる場合、クラウドサービス提供事業者に当該個人データを「提供」したことになるため、原則として、個情法第 27 条第 1 項、第 28 条第 1 項に基づき事前同意を得る必要がある。

２．解説

（1）クラウドサービス提供事業者が個人データを取り扱わないこととなっている場合

第三者の提供するクラウドサービスを利用してその管理するサーバに個人データを保存する場合において、クラウドサービス提供事業者が個人データを取り扱わないこととなっている場合、クラウドサービス利用事業者は個人データを「提供」したことにはならないため、個情法第 27 条第 1 項、第 28 条第 1 項に基づく事前同意の取得は不要であり、また、同法第 25 条に基づく委託先の監督義務も課されないこととなる（個情法 QA7-53 参照）。

個情法 QA7-53 は、クラウドサービス提供事業者が個人データを取り扱わないこととなっている場合について、「契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」が考えられるとしている[1]。

[1] クラウドサービス提供事業者が提供する業務システムが不正アクセス被害を受け、クラウド環境で管理されていた多数のクラウドサービス利用者の顧客の従業員の個人データが暗号化され、漏えい等のおそれが生じた事案をふまえて個人情報保護委員会が公表した注意喚起では、当該事案においてクラウドサービス提供事業者がクラウドサービス利用者から個人デ

ただし、クラウドサービス利用事業者は、かかる場合であっても、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある（個情法 QA7-54 参照）。特に、外国において個人データを取り扱うこととなる場合（外国に所在する第三者の提供するクラウドサービスを利用する場合、外国に所在するサーバに個人データが保存されることとなる場合）には、当該外国の個人情報の保護に関する制度等を把握した上で安全管理措置を講じる必要がある（外的環境の把握）ため、その点についても注意が必要である（個情法 QA10-25。外的環境の把握については Q13、Q14 を参照されたい）。

（2）クラウドサービス提供事業者が個人データを取り扱う場合

クラウドサービス提供事業者が個人データを取り扱うこととなる場合、クラウドサービス利用事業者は、クラウドサービス提供事業者に対して当該個人データを「提供」したこととなるため、原則として、個情法第 27 条第 1 項、第 28 条第 1 項に基づき事前同意を得る必要がある。

すなわち、まず、日本国内に所在する第三者への個人データの提供となる場合、原則として、個情法第 27 条第 1 項に基づき、本人の事前同意を得る必要があるが、個情法第 27 条第 1 項各号の例外に該当する場合、個情法第 27 条第 5 項各号に基づき提供する場合（個人データの取扱いの委託に伴って提供する場合等）には、本人の事前同意を得る必要はない。

次に、外国に所在する第三者への個人データの提供となる場合、原則として、個情法第 28 条第 1 項に基づき、「外国にある第三者」への提供を認める旨の本人の事前同意を得る必要がある。この点に関して、前述の個情法第 27 条第 5 項各号に該当する場合（個人データの取扱いの委託に伴って提供する場合等）であっても、本人の事前同意を得る必要がある（個情法第 28 条には、第 27 条第 5 項に相当する規定がないため）ことに注意を要する。また、当該同意取得に先立ち、①移転先の外国の名称、②適切かつ合理的な方法で確認された当該外国の個人情報保護に関する制度に関する情報、③移転先の第三者が講ずる個人情報の保護のための措置に関する情報を提供する必要がある（同条第 2 項、個情法施行規則第 17 条第 2 項）[2]。

他方、個情法第 27 条第 1 項各号に該当する場合には本人同意を得る必要はない（個情法第 28 条第 1 項において、「前条第 1 項各号に掲げる場合を除くほか、あらかじめ外国

ータの取扱いの委託を受け、個人データを取り扱っていたと判断した考慮要素として、利用規約において、クラウドサービス提供事業者が特定の場合にクラウドサービス利用者の個人データを使用等できることとなっていたこと、クラウドサービス提供事業者が保守用 ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態であり、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと、クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていたことが挙げられている。

[2] 提供すべき情報の詳細については、個人情報の保護に関する法律ガイドライン（外国にある第三者への提供編）5-2 を参照されたい。

にある第三者への提供を認める旨の本人の同意を得なければならない」と明記されている。)。また、以下の①又は②に該当する場合には、個情法第 28 条第 1 項の適用はないため（個情法第 28 条第 1 項括弧書)、個情法第 27 条の規律に従えば足りることとなる。

① 提供先が EU・英国に所在する場合

提供先の第三者が、EU・英国（我が国と同等の水準にあると認められる個人情報保護制度を有している外国として個情法施行規則で定める国）に所在する場合には、個情法第 27 条の規律に従えば足りる。

② 提供先が基準適合体制を整備している場合

提供先の第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として個情法施行規則で定める基準に適合する体制を整備している場合、個情法第 28 条第 1 項は適用されない。

具体的には、第一に、適切かつ合理的な方法によって、個情法第 4 章第 2 節の規定の趣旨に沿った措置の実施が確保されている場合であり（個情法施行規則第 16 条第 1 号)、例えば、委託契約や、提供元・提供先に共通して適用される内規によって当該措置の実施を確保する場合などが挙げられる。

第二に、外国にある第三者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けている場合であり（個情法施行規則第 16 条第 2 号)、例えば、当該第三者が、APEC の CBPR システムの認証を取得している場合、が挙げられる。

なお、提供先が基準適合体制を整備していることを根拠として外国に所在する第三者に個人データを提供する場合、個人情報取扱事業者は、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供する必要がある（個情法第 28 条第 3 項）[3] 。

３．参考資料（法令・ガイドラインなど）

・個情法第 23 条、第 25 条、第 27 条、第 28 条
・個人情報の保護に関する施行規則第 15 条、第 16 条、第 17 条、第 18 条
・個情法ガイドライン（通則編）
・個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）
・個情法 QA

４．裁判例

特になし

[3] 個情法第 28 条第 3 項、個情法施行規則第 18 条。必要措置及び提供すべき情報の詳細については、個人情報の保護に関する法律ガイドライン（外国にある第三者への提供編）6-2 を参照されたい。

Q16 官民における個人情報に関する安全管理措置の相違

個人情報の適正な取扱いに関して法令上求められる安全管理措置は、個人情報を取り扱う主体に関わらず同じなのか。同じではないとしてどのように異なるのか。

タグ：個情法、行個法、独個法、個人情報保護条例、安全管理措置、個人情報の定義、漏えい等

１．概要

個人情報の適正な取扱いに関して適用される法令は、従来官民で適用される法令が異なっていたところ、令和 3 年に成立したデジタル社会形成整備法に基づく個情法の改正により、個情法に統合する形で一本化された。ただし、官民で全く同じ規律が適用されるわけではなく、個情法が定める安全管理措置義務の対象となる個人情報の範囲は、個人情報を取り扱う主体によって異なる。具体的には、民間企業を含む個人情報取扱事業者については「個人データ」、国の行政機関、独立行政法人等、地方公共団体又は地方独立行政法人については「保有個人情報」が対象となる。なお、国立大学法人や国立研究開発法人等の個人情報の取扱いに関して民間部門と差を設ける必要性の乏しい法人や業務における個人情報の取扱い等については大部分において個人情報取扱事業者と同一の規律が適用されるなど、法令の適用関係は複雑である。

いずれにせよ、個人データや保有個人情報の漏えい、滅失又は毀損（以下、本項において「漏えい等」という。）があった場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データや保有個人情報の取扱状況（取り扱う個人データや保有個人情報の性質及び量を含む。）、個人データや保有個人情報を記録した媒体の性質等に起因するリスクに応じて、適切な安全管理措置を実施することが求められる。

２．解説

（１）従来の法体系

我が国の個人情報保護法制は、個人情報を取り扱う主体によって、適用される法令が異なっていた。具体的には、個人情報取扱事業者については、個情法の具体的な義務規定、国の行政機関については行個法、独立行政法人等については独個法、地方公共団体及び地方独立行政法人については各々の地方公共団体が定める個人情報保護に関する条例（以下、本項において「個人情報保護条例」という。）が適用されていた。したがって、個人情報を取り扱う上では、まずは適用対象となる法令が何かという点に留意する必要があった。

そのため、個人情報を取り扱う主体が法令に基づき必要となる安全管理措置義務を講じるためにも、まずは適用対象となる法令が何かを特定する必要があった。

（２）令和 3 年改正後の情報の安全管理に関する規定について

令和 3 年に成立したデジタル社会形成整備法により、個情法、行個法、独個法とバラバラであった個人情報の適正な取扱いに関する法制が、個情法に統合される形で一本化され、法所管も個人情報保護委員会に一本化された。また、地方公共団体の機関及び地方独立行政法人についても、個人情報保護条例ではなく、国の行政機関や独立行政法人等と同じ規律が適用されることとなった。なお、学術研究分野に関しては、規制を統一するため、国公立の病院、大学等に原則として民間の個人情報取扱事業者と同等の規律が適用されることとなった。

ただし、官民で全く同じ規律が適用されるというわけではなく、個情法の中に民間事業者向けの規律と行政機関等向けの規律の双方が置かれている。例えば、個人情報の安全管理に関する規定については、個人情報取扱事業者には「個人データ」についての安全管理措置義務（個情法第 23 条）が課される[4]一方で、国の行政機関、独立行政法人等、地方公共団体の機関及び地方独立行政法人（以下、本項において「行政機関等」という。）には「保有個人情報」についての安全管理措置義務が課される（個情法第 66 条第 1 項）[5] [6]。保有個人情報とは、行政機関等の職員が職務上作成し、又は取得した個人情報であって、当該行政機関等の職員が組織的に利用するものとして当該行政機関等が保有しているもののうち、行政文書等[7]に記録されているものをいう（個情法第 60 条第 1 項）。したがって、データベース化などされておらず散在する個人情報（いわゆる散在情報）も、安全管理措置義務の対象となる保有個人情報に該当し得る。

一方で、個人情報取扱事業者については、散在情報に関する安全管理措置義務は課されていない。ただし、散在情報の漏えい等が発生した場合、同法が定める安全管理措置義務違反にはならないとしても、同法に関する各業種別のガイドラインに反する場合がある

---

[4] この点について Q13 も参照されたい。

[5] 行政機関等から個人情報の取扱いの委託を受けた者、指定管理者、個情法第 58 条第 1 項又は第 2 項に規定される者については、一部業務を行う場合、行政機関等に課される保有個人情報に関する安全管理措置が準用される（個情法第 66 条第 2 項第 1 号、同第 2 号、同第 3 号、同第 4 号）。上記の者から当該業務について委託を受けた者（二以上の段階にわたる委託を含む。）についても同様である（個情法第 66 条第 2 項第 5 号）。このように、民間事業者等についても、行政機関等に課される保有個人情報に関する安全管理措置が準用されることがある。

[6] なお、地方議会は、明文上、原則的に地方公共団体の機関から除外されており、「行政機関等」に含まれない（個情法第 2 条第 11 項第 2 号）。地方議会における個人情報の取扱いは、その自律的な対応に委ねられることとなる。

[7] 行政機関情報公開法（平成 11 年法律第 42 号）第 2 条第 2 項に規定する行政文書、独立行政法人等情報公開法（平成 13 年法律第 140 号）第 2 条第 2 項に規定する法人文書（同項第 4 号に掲げるものを含む。）をいい、令和 5 年度以降は、地方公共団体等行政文書（地方公共団体の機関又は地方独立行政法人の職員が職務上作成し、又は取得した文書、図画及び電磁的記録であって、当該地方公共団体の機関又は地方独立行政法人の職員が組織的に用いるものとして、当該地方公共団体の機関又は地方独立行政法人が保有しているもの（行政機関情報公開法第二条第二項各号に掲げるものに相当するものとして政令で定めるものを除く。）も含まれている（個情法第 60 条第 1 項）。

ほか、それらの情報が個人のプライバシーに属する情報に該当する場合には、不法行為法上の責任を負う可能性がある。

（３）具体的な安全管理措置の手法

個人情報取扱事業者は、個情法ガイドライン（通則編）に記載された安全管理措置の手法の例などを参照しながら、個人データの安全管理措置を実施する必要がある[8]。加えて、令和 2 年の個情法ガイドライン（通則編）の改正により、個人情報取扱事業者は、外国において個人データを取り扱う場合、安全管理措置の一環として、外的環境の把握[9]が必要となり、また、保有個人データの安全管理のために講じた措置の内容を本人の知り得る状態に置かなければならないこととなった（詳細は Q13、Q14 を参照されたい。）。

一方で、行政機関等は、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」や、「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」[10]を参照しながら保有個人情報に関する安全管理措置を実施することとなる[11]。デジタル化の進展とともに、安全管理措置を適切に講じるためにサイバーセキュリティの確保が重要であるとされ、サイバーセキュリティ基本法第 26 条第 1 項第 2 号で掲げられたサイバーセキュリティに関する対策の基準等、すなわち、サイバーセキュリティ戦略本部及び NCO が定める政府機関等統一基準群を参考として、適正な水準を確保する必要があるとされている。

（４）漏えい等発生時の対応

個人情報取扱事業者は、一定の条件を満たす個人データ[12]の漏えい等又はそのおそれのある事案が発生した場合（報告対象事態）に、個人情報保護委員会への報告及び本人通知を行う必要がある（個情法第 26 条）。

---

8 「その他の保有個人情報の安全管理のために必要かつ適切な措置」（個情法第 66 条第 1 項）には、行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものの漏えい等を防止するために必要かつ適切な措置も含まれる（個人情報の保護に関する法律についてのガイドライン（行政機関等編）23 頁及び個人情報の保護に関する事務対応ガイド（行政機関向け）73 頁）。

9 当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じることを指す。

10 特に、「4-3 安全管理措置等」、「4-8 （別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」。

11 「その他の保有個人情報の安全管理のために必要かつ適切な措置」（個情法第 66 条第 1 項）には、行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものの漏えい等を防止するために必要かつ適切な措置も含まれる（個人情報の保護に関する法律についてのガイドライン（行政機関等編）5-3-1(1)及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）4-3-1-1）。

12 当該個人情報取扱事業者に対し不正の目的をもって行われたおそれがある行為による個人データの漏えい等が発生し、又はそのおそれがある場合において、「個人データ」には当該個

行政機関等においても、デジタル社会形成整備法による改正により、一定の条件を満たす保有個人情報[13]の漏えい等又はそのおそれのある事案が発生した場合に個人情報保護委員会への報告と本人通知を行う義務が措置された（個情法第 68 条)。個人情報取扱事業者に対する義務との主な相違点として、以下のものが挙げられる。

まず、漏えい等発生時に対応が必要となるのは、個人データではなく保有個人情報であり、安全管理措置と同様、散在情報も含まれている。

次に、個人情報保護委員会への報告等が必要となる事態について、民間では、事態の一つとして、1,000 人を超える個人データの漏えい等が発生し又はそのおそれがある場合が定められているが（個情法施行規則第 7 条第 3 号)、行政機関等においては、100 人を超える保有個人情報の漏えい等又はそのおそれが発生した場合には報告等が必要となる（同規則第 43 条第 4 号)。

なお、令和 5 年度より、地方公共団体の機関又は地方独立行政法人も個情法の適用対象となっているところ、これらについては、条例要配慮個人情報[14]が含まれる保有個人情報の漏えい等が発生し、又は発生したおそれがある事態も報告対象となる（同規則第 43 条第 5 号）。

３．参考資料（法令・ガイドラインなど）

・個情法第 23 条、第 26 条、第 66 条、第 68 条
・個情法ガイドライン（通則編）
・個人情報の保護に関する法律についてのガイドライン（行政機関等編）（令和 4 年 4 月 1 日施行、令和 8 年 9 月一部改正）
・個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）（令和 4 年 4 月 1 日施行、令和 8 年 9 月一部改正）

４．裁判例

特になし

人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む（個情法施行規則第 7 条第 3 号)。

[13] 不正の目的をもって行われたおそれがある当該行政機関の長等の属する行政機関等に対する行為による保有個人情報（当該行政機関の長等の属する行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態を含む（個情法施行規則第 43 条第 1 項第 3 号)。

[14] 地方公共団体の機関又は地方独立行政法人が保有する個人情報（要配慮個人情報を除く。）のうち、地域の特性その他の事情に応じて、本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして地方公共団体が条例で定める記述等が含まれる個人情報をいう（個情法第 60 条第 5 項)。

Q17 個人データの加工と法令上の安全管理

個人データを安全管理のため、又は利活用のために加工する場合に、法令上どのような措置が必要となるか。

タグ：個情法、安全管理措置義務、統計情報、仮名加工情報、匿名加工情報

１．概要

個人データを加工する場合、①安全管理のため氏名等を削除するなどの加工を施す、②仮名加工情報へ加工する、③匿名加工情報へ加工する、④統計情報へ加工するケースが考えられる。

①の場合、個人データ該当性は失われないため、個情法第 23 条に基づく安全管理措置など、個情法上の個人データの取扱いに係る規律を遵守する必要がある。

②の場合、個情法上の仮名加工情報の取扱いに係る規律を遵守する必要がある。例えば、仮名加工情報の安全管理措置、削除情報等の安全管理措置、識別行為の禁止、本人への連絡等の禁止等の規律を遵守する必要がある。

③の場合、個情法上の匿名加工情報の取扱いに係る規律を遵守する必要がある。例えば、匿名加工情報の安全管理措置（努力義務）、加工方法等情報の安全管理措置、匿名加工情報の作成時の公表、識別行為の禁止等の規律を遵守する必要がある。

④の場合、個情法に基づく規律はかからないが、適切に管理することが重要であると考えられる。

２．解説

（１）データの加工について

企業が保有する個人データ[1]を含むデータについては、データベースから一定の条件を満たすデータ等を抽出し、加工を施す等して社内外で利活用することも考えられる。

このうち、個人データを加工するという場合、①安全管理のため氏名等を削除するといった加工を施すケース、②仮名加工情報へ加工するケースや、③匿名加工情報へ加工するケース、④統計情報へ加工するケースが考えられる[2]。

いずれの場合も、事業者が保有する個人データを元に加工を行うこととなるが、データの加工に当たっては、個情法ガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」を踏まえ、データ加工に関する手続等を含め、個人データの取扱いにかかる規律

[1] 個人データ等、個情法における定義については Q13 を参照されたい。
[2] なお、データを加工して社外へ提供するという場合には、データ取引に係る契約を締結するケースが多いと考えられる。データ取引に関する契約については Q51 を参照されたい（特に「派生データ」について）。

の整備などの措置を講じる必要がある。また、②の仮名加工情報及び③の匿名加工情報の場合には、個情法ガイドライン（仮名加工情報・匿名加工情報編）及び個人情報保護委員会事務局「個人情報保護委員会事務局レポート：仮名加工情報・匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」（以下、本項において「事務局レポート」という。）により、仮名加工情報・匿名加工情報の作成・利活用をサポートする情報発信がなされており、これらを踏まえて適切に加工を行う必要がある。

（２）安全管理のための加工

名簿等の個人データから、安全管理のために氏名等を削除する等の加工を施す場合がある。

個情法においては、当該情報単体で特定の個人を識別できる場合はもちろん、「他の情報と容易に照合することができ、それにより特定の個人を識別することができる」（同法第 2 条第 1 項第 1 号）場合も個人情報に該当するため、加工前のデータをはじめ、他の情報と容易に照合でき、それにより特定の個人を識別することができるのであれば、加工後のデータの個人データ該当性を失われず、加工後のデータについても、同法第 23 条に基づく安全管理措置義務が課されることとなる。

当該安全管理措置については、「個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容」[3]とすることが必要である。

（３）仮名加工情報への加工

ア　仮名加工情報制度の趣旨

近年、個人データに上記（２）で述べたような氏名を削除等する等の加工を施し利活用するニーズが高まっていたところ、このような加工を施しても、加工後のデータも個人情報に該当する場合もあり、そのような場合には、通常の個人情報としての取扱いに係る義務が一律に課されていた。一方で、このような加工がされた個人情報は、本人と紐づいて利用されることのない限り、個人の権利利益が侵害されるリスクを相当程度低下する。これらの観点から、事業者内部で個人情報を様々な分析に活用できるよう、令和 2 年の個情法改正で「仮名加工情報」が設けられた。

イ　仮名加工情報の定義や性質

仮名加工情報とは、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報をいう（個情法第 2 条第 5 項）。ここにいう「他の情報と照合しない限り特定の個人を識別することができない」とは、

[3] 個情法ガイドライン（通則編）3-4-2 参照。

加工後の情報それ自体により特定の個人を識別することができないような状態にすることを求めるものであり、当該加工後の情報とそれ以外の他の情報を組み合わせることによって特定の個人を識別することができる状態にあることを否定するものではない[4]。

仮名加工情報取扱事業者[5]において、仮名加工情報の作成の元となった個人情報や当該仮名加工情報に係る削除情報等[6]を保有している等により、当該仮名加工情報が「他の情報と容易に照合することができ、それにより特定の個人を識別することができる」状態にある場合には、当該仮名加工情報は、「個人情報」に該当する。他方、委託や共同利用、事業承継等に伴って仮名加工情報の提供を受けた場合（同法第 27 条第 5 項各号）等、当該仮名加工情報の作成の元となった個人情報や当該仮名加工情報に係る削除情報等を保有していない等により、当該仮名加工情報が「他の情報と容易に照合することができ、それにより特定の個人を識別することができる」状態にない場合には、当該仮名加工情報は個人情報に該当しない[7]。

仮名加工情報については、一定のルールに従った取扱いが求められている。まず、仮名加工情報を作成する個人情報取扱事業者は、①適正な加工、②削除情報等の安全管理措置が求められ（同法第 41 条第 1 項、同条第 2 項）、個人情報である仮名加工情報を取り扱うに当たっては、③利用目的による制限・公表、④利用する必要がなくなった場合の消去、⑤第三者提供の禁止、⑥識別行為の禁止、⑦本人への連絡等の禁止、が求められる（同条第 3 項から第 8 項まで）[8]。

他方で、仮名加工情報については、個人情報、個人データ又は保有個人データに該当する場合であっても、利用目的の変更の制限（同法第 17 条第 2 項）、個人データに関する漏えい等の報告及び本人通知（同法第 26 条）、保有個人データに関する事項の公表等及び保有個人データの開示・訂正等・利用停止等への対応等（同法第 32 条から第 39 条まで）の規定は適用されない（同法第 41 条第 9 項）。

特に、利用目的の変更の制限がかからないことが仮名加工情報制度のポイントの一つであり、仮名加工情報は、当初の利用目的には該当しない目的や、該当するか判断が難しい新たな目的での内部分析を行うケース等での利用が想定されている。また、仮名加工情報は、事業者内部での利活用が想定されており、法令に基づく場合や、委託、事業

---

4 個情法ガイドライン（仮名加工情報・匿名加工情報編）2-1-1(1)参照。
5 仮名加工情報データベース等（仮名加工情報を含む情報の集合物であって、特定の仮名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の仮名加工情報を容易に検索することができるように体系的に構成したものとして個情法施行令で定めるもの。）を事業の用に供している者を指す（個情法第 16 条第 5 項。ただし、同条第 2 項各号に掲げる者を除く。）。
6 削除情報等とは、仮名加工情報の作成に用いられた個人情報から削除された記述等及び個人識別符号並びに個情法第 41 条第 1 項の規定により行われた加工の方法に関する情報をいう（同条第 2 項括弧書）。
7 個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-1 参照。
8 個人情報に該当でない仮名加工情報を取り扱うに当たっては、上記⑤⑥⑦と同様の義務に加えて、安全管理措置義務等の義務が課される（同法第 42 条第 3 項）。

承継又は共同利用の場合を除き、第三者提供は認められない（上記⑤。個情法第 41 条第 6 項・第 27 条第 5 項各号、同法第 42 条第 2 項・第 27 条第 5 項各号）[9]。

ウ　仮名加工情報の適正な加工

個人情報取扱事業者は、仮名加工情報を作成するときは、他の情報と照合しない限り特定の個人を識別することができないようにするために、個情法施行規則第 31 条各号に定める基準[10]に従って、個人情報を加工しなければならない（個情法第 41 条第 1 項、同法施行規則第 31 条）。

仮名加工情報を「作成するとき」とは、仮名加工情報として取り扱うために、当該仮名加工情報を作成するときのことを指し、例えば、上記（2）のように、安全管理措置の一環として氏名等の一部の個人情報を削除することは、仮名加工情報を「作成するとき」には該当しない[11]。

エ　仮名加工情報に関する安全管理措置義務

仮名加工情報に関する安全管理措置義務としては、削除情報等の安全管理措置義務（個情法第 41 条第 2 項、同法施行規則第 32 条）及び仮名加工情報自体の安全管理措置義務（同法第 23 条、同法第 42 条第 3 項）が挙げられる。

削除情報等の安全管理措置については、同規則 32 条に定める基準に従い、必要な措置を講じなければならず、当該措置の内容は、対象となる削除情報等が漏えいした場合における個人の権利利益の侵害リスクの大きさを考慮し、当該削除情報等の量、性質等に応じた内容としなければならない[12]。同条においては、①削除情報等を取り扱う者の権限及び責任の明確化、②削除情報等の取扱いに関する規程類の整備及び当該規程類に従った削除情報等の適切な取扱い並びに削除情報等の取扱状況の評価及びその結果に基づき改善を図るために必要な措置の実施、③削除情報等を取り扱う正当な権限を有しない者による削除情報等の取扱いを防止するために必要かつ適切な措置の実施が求められている[13]。

次に、仮名加工情報それ自体については、当該仮名加工情報が個人データ（個人情報）である場合には、個人データ全般に係る同法第 23 条に基づき安全管理措置義務が課され、当該仮名加工情報が個人情報でない場合には、同法第 42 条第 3 項により準用される同法第 23 条に基づき安全管理措置義務が課される。講ずべき安全管理措置の内容は、

---

9 仮名加工情報を作成する前に本人の同意を得ていた場合であっても、仮名加工情報を第三者に提供することはできない（個情法 QA14-17 参照）。
10 詳細については、個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-2-1 を参照されたい。
11 個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-2-1 参照。
12 個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-2-2 参照。
13 具体例については、個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-2-2 を参照されたい。

仮名加工情報が個人情報であるかどうかに関わらず通常の個人情報と同様と考えられるが、仮名加工情報には（通常の個人情報とは異なり）識別行為の禁止義務や本人への連絡等の禁止義務が課されている（上記イ）ことから、これらの義務に違反することがないよう、仮名加工情報に該当することを明確に認識できるようにしておくことが重要であり、仮名加工情報を取り扱う者にとってその情報が仮名加工情報である旨が一見して明らかな状態にしておくことが望ましい[14]。

（４）匿名加工情報への加工

ア　匿名加工情報制度の趣旨

「匿名加工情報」は、個人情報を特定の個人を識別できないように加工した情報について、一定のルールの下で本人の同意を得ることなく目的外利用及び第三者提供を可能とすることにより、安全性を確保しつつ、事業者間におけるデータ取引やデータ連携を含むパーソナルデータの利活用を促進しようとするものである[15]。匿名加工情報の利活用による事例としては、例えば、ポイントカードの購買履歴や交通系 IC カードの乗降履歴等を複数の事業者間で分野横断的に利活用することにより、新たなサービスやイノベーションを生み出す可能性などが挙げられている[16]。

イ　匿名加工情報の定義や性質

匿名加工情報とは、特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう（個情法第 2 条第 6 項）。ここにいう「特定の個人を識別することができないように」「復元することができないように」とは、あらゆる手法によって特定することができないよう（復元することができないよう）技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として、当該情報を通常の方法により特定できない（復元できない）ような状態にすることを求めるとされている[17]。

匿名加工情報については、一定のルールに従った取扱いが求められており、匿名加工情報を作成する個人情報取扱事業者には、個情法第 43 条に基づき、①適正加工、②加工方法等情報[18]の安全管理措置、③作成した際の情報項目の公表、④第三者提供に当たっ

---

14 個情法ガイドライン（仮名加工情報・匿名加工情報編）2-2-4-2(1)参照。
15 事務局レポート 3 頁、9 頁参照。
16 事務局レポート 9 頁参照。
17 個情法ガイドライン（仮名加工情報・匿名加工情報編）3-1-1 参照。
18 匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに同法第 43 条第 1 項の規定により行った加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る）をいう（同法施行規則第 35 条第 1 号）。なお、氏名等を仮 ID に置き換えた場合における氏名と仮 ID の対応表は、匿名加工情報と容易に照合することができ、それにより匿名加工情報の作成の元となった個人情報の本人を識別することができるものであることから、匿名加工情報の作成後は破棄しなければならず、氏名等の仮

ての情報項目等の公表及び匿名加工情報であることの明示、⑤識別行為の禁止、⑥匿名加工情報の安全管理措置等が求められる（⑥については努力義務）。また、匿名加工情報の提供を受けて取り扱う匿名加工情報取扱事業者[19]には、個情法第 44 条から第 46 条までに基づき、上記④から⑥までと同様の義務が課せられる[20]。

匿名加工情報は、特定の個人を識別することができないもので、かつ、作成の元となる個人情報を復元することができないように適正に加工されたものであり、さらに、個人情報に係る本人を識別することを禁止する等の制度的な担保がなされていることから、作成の元となった個人情報を通常の業務における一般的な方法で照合することができる状態にある（すなわち容易照合性がある）とはいえず、個人情報に該当しないとされており[21]、例えば、同法第 27 条第 1 項に基づく第三者提供に当たっての本人の同意は不要となる。

ウ　匿名加工情報の適正な加工

個人情報取扱事業者は、匿名加工情報を作成するときは、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、個人情報保護法施行規則第 34 条各号に定める基準に従って、個人情報を加工しなければならない（個情法 43 条第 1 項、同法施行規則第 34 条）。

匿名加工情報を「作成するとき」とは、匿名加工情報として取り扱うために、当該匿名加工情報を作成するときのことを指し、例えば、上記（2）のように、安全管理措置の一環として氏名等の一部の個人情報を削除することは、匿名加工情報を「作成するとき」には該当しない[22]。

ID への置き換えに用いた置き換えアルゴリズムと乱数等のパラメータの組み合わせを保有している場合には、当該置き換えアルゴリズム及び当該乱数等のパラメータを用いて再度同じ置き換えを行うことによって、匿名加工情報とその作成の元となった個人情報とを容易に照合でき、それにより匿名加工情報の作成の元となった個人情報の本人を識別することができることから、匿名加工情報の作成後は、氏名等の仮 ID への置き換えに用いた乱数等のパラメータを破棄しなければならない（個情法ガイドライン（仮名加工情報・匿名加工情報編）3-2-3-1 参照）。

[19] 匿名加工情報データベース等（匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして個情法施行令で定めるものを事業の用に供している者を指す（個情法第 16 条第 6 項。ただし、同条第 2 項各号に掲げる者を除く。）。

[20] なお、匿名加工情報取扱事業者は、⑤に関して加工方法等情報の取得も禁止されている。

[21] 事務局レポート 4.1.4.2 参照。

[22] 個情法ガイドライン（仮名加工情報・匿名加工情報編）3-2-2 参照。

エ　匿名加工情報に関する安全管理措置

匿名加工情報に関する安全管理としては、加工方法等情報の安全管理措置（個情法第 43 条第 2 項）及び匿名加工情報自体の安全管理措置義務の努力義務（同条第 6 項、同法第 46 条）が挙げられる。

加工方法等情報の安全管理については、個情法施行規則第 35 条に定める基準に従い、必要な措置を講じなければならず、当該措置の内容は、対象となる加工方法等情報が漏えいした場合における復元リスクの大きさを考慮し、当該加工方法等情報の量、性質に応じた内容としなければならない[23]。同施行規則においては、①加工方法等情報を取り扱う者の権限及び責任を明確に定めること、②加工方法等情報の取扱いに関する規程類を整備し、当該規程類に従って加工方法等情報を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講ずること、③加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置が求められている[24]。

次に、匿名加工情報それ自体については、個人情報と同様の取扱いを求めるものではないが、それも参考にしつつ、具体的には、事業の性質、匿名加工情報の取扱状況、取り扱う匿名加工情報の性質、量等に応じて、合理的かつ適切な措置を講ずることが望ましいとされている[25]。

（５）統計情報への加工

統計情報とは、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られるデータであり、集団の傾向又は性質などを数量的に把握するものである。

したがって、統計情報は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当せず、個情法の規制の対象外と整理されている[26]。

したがって、例えば、第三者提供における本人同意（個情法第 27 条第 1 項）が不要であるなど、データの利活用を推進することが可能となり、また、同法第 23 条に基づく安全管理措置義務も課されない。

ただし、法的な義務がないからといって何らの対策も行わなくてよいものではなく、こうしたデータが漏えい等した場合に、企業に対する風評被害が生じるなど社会的責任を問われる可能性や、当該漏えい等に関して損害賠償責任等の法的責任を問われる可能性があるため、統計情報についても、適切な管理を行うことが重要であると考えられる。

---

[23] 個情法ガイドライン（仮名加工情報・匿名加工情報編）3-2-3-1 参照。
[24] 具体例については、個情法ガイドライン（仮名加工情報・匿名加工情報編）3-2-3-1 を参照されたい。
[25] 個情法ガイドライン（仮名加工情報・匿名加工情報編）3-2-3-2 参照。
[26] 個情法ガイドライン（仮名加工情報・匿名加工情報編）3-1 参照。

３．参考資料（法令・ガイドラインなど）

・個情法第 2 条、第 23 条、第 27 条、第 4 章第 3 節、第 4 章第 4 節
・個情法施行規則第 31 条、第 32 条、第 34 条、第 35 条
・個情法ガイドライン（通則編）、個情法ガイドライン（仮名加工情報・匿名加工情報編）
・個情法 QA
・個人情報保護委員会事務局「個人情報保護委員会事務局レポート：仮名加工情報・匿名加工情報パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」

４．裁判例

特になし

Q18 クレジットカード情報の取扱い

クレジットカード情報を取り扱うに当たって、セキュリティ上どのような点に留意すべきか。

タグ：割賦販売法、クレジットカード情報、PCI DSS、非保持化、クレジットカード・セキュリティガイドライン

１．概要

クレジットカードによる決済は、利用可能な店舗等が拡大しており、現在社会的なインフラとなっている。また、キャッシュレス化の推進に伴い、クレジットカード決済のより一層の進展が見込まれている。一方、クレジットカード情報の漏えいやクレジットカード情報の不正利用も発生しており、割賦販売法（昭和 36 年法律第 159 号）では、安全・安心なクレジットカード利用環境を整備するため、クレジットカードを発行する事業者（クレジットカード等購入あっせん業者）、加盟店に立替払いを行う事業者（立替払取次業者）、決済代行業者、コード決済事業者、コード決済事業者の受託者、決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者、及び加盟店に対して、クレジットカード情報の漏えい等の事故を防止するための適正管理を義務付けるとともに、加盟店に対してはクレジットカード情報の不正利用を防止するための措置を義務付けている。

これらの措置については、「クレジットカード・セキュリティガイドライン」（以下、本項において「ガイドライン」という。）を実務上の指針としており、ガイドラインに掲げる措置又はそれと同等以上の措置を講じている場合には、法令に基づく措置を講じていると認められることとしている。

２．解説

（１）クレジットカードに関するセキュリティ確保の重要性

クレジットカードによる決済は、利用可能な店舗等が拡大しており、現在社会的なインフラ[1]となっており、キャッシュレス化の推進に伴い、クレジットカード決済のより一層の進展が見込まれている。一方、クレジットカード情報の漏えいやクレジットカード情報の不正利用も発生しており、こうした不正利用に対する対策の必要性に鑑み、割賦販売法は、クレジットカード番号等の適切な管理に関する規定や、クレジットカード番号等の不正な利用の防止に関する規定を置いている。

[1] 重要インフラに関する取組の概要について Q45 を参照されたい。

（２）クレジットカード番号等の適切な管理

割賦販売法では、クレジットカード等購入あっせん業者、立替払取次業者、決済代行業者、コード決済事業者、コード決済事業者の受託者、加盟店及び EC モール事業者等の決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者等（これらを併せて以下、本項において「クレジットカード情報取扱事業者」という。）に対して、割賦販売法施行規則に定められた基準に従い、クレジットカード番号の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置を講ずることを求めている（割賦販売法第 35 条の 16 第 1 項）。

具体的な基準は、以下のとおりである（割賦販売法施行規則第 132 条第 1 号～第 5 号）。

① クレジットカード番号等の漏えい、滅失、毀損その他のクレジットカード番号等の管理に係る事故（以下、本項において「漏えい等の事故」という。）を防止するため必要かつ適切な措置を講ずること。

② 漏えい等の事故が発生し、又は発生したおそれがあるときは、直ちに事故の状況を把握し、事故の拡大を防止するとともに、その原因の究明のために必要な調査（当該事故に係るクレジットカード番号等の特定を含む。）を行うこと[2]。

③ 漏えい等の事故が発生し、又は発生したおそれがあるときは、当該事故の対象となったクレジットカード番号等を利用者に付与したクレジットカード等購入あっせん業者は、不正利用されることを防止するために必要な措置を講ずること。

④ 漏えい等の事故が発生し、又は発生したおそれがあるときは、類似の漏えい等の事故の再発防止のために必要な措置を講ずること。

⑤ クレジットカード番号等をクレジットカード取引の健全な発達を阻害し、又は利用者若しくは購入者等の利益の保護に欠ける方法により取り扱わないこと。

また、クレジットカード情報取扱事業者は、クレジットカード情報の取扱いを委託した事業者（以下、本項において「受託業者」という。）に対して、クレジットカード番号等の適切な管理が図られるよう、受託業者に対する指導その他の適切な措置を講じなければならない（割賦販売法第 35 条の 16 第 3 項）。

これらの措置に関しては、ガイドラインを実務上の指針としており、このガイドラインに掲げる措置又はそれと同等以上の措置を講じている場合には、法令上の基準となる「必要かつ適切な措置」を満たしているとされている[3]。

---

[2] 個情法の観点からは、Q13 で述べたとおり、ウェブサイトの入力ページが第三者に改ざんされ、ユーザが当該ページに入力したカード情報等の個人情報が当該第三者に送信された場合であり、かつ、当該個人情報取扱事業者が、当該ページに入力される個人情報を個人情報データベース等へ入力することを予定していたときは、報告対象事態として個人情報保護委員会への報告及び本人通知を行う必要があることに留意しなければならない。

[3] 経済産業省プレスリリース「『クレジットカード・セキュリティガイドライン』が改訂されました」（令和 7 年 3 月 5 日）（https://www.meti.go.jp/press/2024/03/20250305002/20250305002.html）。

ガイドラインにおいては、クレジットカード番号等の漏えい防止措置として、クレジットカード等購入あっせん業者、立替払取次業者、決済代行業者及びコード決済事業者等に対して、国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が定めたクレジットカード情報についてのセキュリティの国際基準である PCI DSS（Payment Card Industry Data Security Standard）[4]の準拠が求められている。また、加盟店については、クレジットカード決済の際にクレジットカード情報を通過・保持しない方法（非保持化）を推奨しており、クレジットカード番号等を保持する場合には PCI DSS 準拠が求められている。ただし、非保持化を実現した場合であっても、ウェブサイトの開発・運用段階での対応が不十分であるとクレジットカード情報が漏えいするリスクがあることから、自社システムの定期的な点検や追加的な対策の実施等が重要である。また、不正犯の攻撃手口も巧妙化していることから、新たな攻撃手口への速やかな対応が必要となる。同ガイドラインは、令和 8 年 3 月に 6.1 版が公表されており、加盟店について、上記、クレジットカード情報の非保持又は PCI DSS に加えて、脆弱性対策として、①システム管理画面のアクセス制限と管理者の ID/パスワード管理、②データディレクトリの露見に伴う設定不備への対策、③Web アプリケーションの脆弱性対策、④マルウェア対策としてのウイルス対策ソフトの導入、運用、⑤悪質な有効性確認、クレジットマスターへの対策等を講じることが求められているので、留意を要する。

経済産業大臣は、クレジットカード等購入あっせん業者、立替払取次業者、決済代行業者又はコード決済事業者等が講じるクレジットカード番号等の適切管理に係る措置が法令上の基準に適合しないと認めるときは業務改善命令を発出することができる（割賦販売法第 35 条の 17）。

（３）クレジットカード番号等の不正な利用の防止

加盟店は、施行規則に定められた基準に従って、クレジットカード番号等の不正な利用を防止するために必要な措置を取らなければならない（割賦販売法第 35 条の 17 の 15）。

具体的な基準は、以下のとおりである（割賦販売法施行規則第 133 条の 14）。

① クレジットカード番号等の通知を受けたとき、当該通知が正当な利用者によるものかについての適切な確認その他の不正利用を防止するために必要かつ適切な措置を講ずること。

② 加盟店において不正利用されたときは、その発生状況を踏まえ、類似の不正利用を防止するために必要な措置を講ずること。

これらの措置の実務上の指針であるガイドラインにおいては、対面加盟店における偽造カードによる不正利用防止策として、クレジットカードの IC 化及び加盟店の決済端末の IC 対応を求めており、また、非対面加盟店におけるなりすまし等による不正利用防止

[4] 詳細については、PCI SSC（Payment Card Industry Security Standards Council）ウェブサイトを参照されたい。
https://ja.pcisecuritystandards.org

策として、パスワードによる本人認証（EMV 3-D セキュア）、セキュリティコードによる券面認証、不正検知システムによる不正取引判断等の措置をリスクに応じて多面的・重層的に導入することを求めている。

（4）クレジットカード番号の漏えい等に係る責任

裁判例として、クレジットカードの発行会社について、カード保持者でない者が有効なカード番号と有効期間の組合せを不正に作出してカード保持者になりすますというカードの悪用等の事態が生ずることを防止するために必要な手立てを講ずる信義則上の義務を負うものではないと判示した事案(東京地判平成 21 年 11 月 11 日判時 2073 号 64 頁)、また、クレジットカード番号の管理に係るシステムの構築についてのベンダの責任について、債務不履行責任が認められた事案[5]及び認められなかった事案[6]がある。

３．参考資料（法令・ガイドラインなど）

・割賦販売法第 35 条の 16、第 35 条の 17、第 35 条の 17 の 15
・割賦販売法施行規則第 132 条、第 133 条の 14
・クレジット取引セキュリティ対策協議会「クレジットカード・セキュリティガイドライン 6.1 版」

４．裁判例

本文中に記載のとおり

[5] ウェブサイトにおける商品の受注システムを利用した顧客の情報が流出した場合に同システムを導入したユーザに対する同ユーザから同システムの設計・保守等を受託していたベンダの同システムの構築に係る債務不履行責任が認められた事案（東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁）がある。

[6] 通販サイト、サーバ及びウェブアプリケーション等からなるシステムに、脆弱性を含むオープンソースソフトウェアを使っていたところ、当該サイトの運営・保守をベンダに委託し、その中で顧客のクレジットカード情報が漏えいしたという事案において、ベンダに対してセキュリティ対策まで委託していないと認定し、債務不履行責任を否定した事案（東京地判令和元年 12 月 20 日（平成 29 年（ワ）第 6203 号））、及び、ウェブサイトからクレジットカード情報が漏えいした事件について、サイトの構築・保守を委託したベンダに対し債務不履行に基づく損害賠償請求を行ったものの、クレジットカード情報を保持しない仕様にする義務、及び技術水準に沿ったセキュリティ対策を行う義務を否定し、債務不履行の成立を否定した事案（東京地判令和 2 年 10 月 13 日（平成 28 年（ワ）第 10775 号））がある。

Q19 労働者の心身の状態に関する情報の取扱い

労働者の心身の状態に関する情報を取り扱う際のセキュリティ対策を含めた留意点は何か。

タグ：労働安全衛生法、じん肺法、個情法、労働契約法、労働者、メンタルヘルス、健康診断

１．概要

事業者は、労働安全衛生法（昭和 47 年法律第 57 号）の規定に基づく定期健康診断の実施等の健康確保措置や任意に行う労働者の健康管理等を通じて労働者の心身の状態に関する情報の収集等を行うこととなる。当該情報は、労働者の健康確保の観点から事業者が取り扱う必要があるものである一方で、労働者側からみれば雇用管理において自身にとって不利益な取扱いを受けることが懸念されるものでもある。

そのため、労働安全衛生法において、事業者に対し適正な取扱いが求められている。また、同時に個情法における個人情報であり、要配慮個人情報であることも多い。そこで、労働者の心身の状態に関する情報の適切な取扱いのために事業者が講ずべき措置に関する指針の内容を踏まえ、個情法や労働安全衛生法によって規定されている情報の取扱いの定めに従う必要がある。具体的には、労使関与の下で事業所ごとに取扱規程を定め、労働者の健康確保の実施や事業者が負う民事上の安全配慮義務の履行の目的の範囲で適正に取扱い、情報の収集に当たっては適切な説明を行うこと、必要に応じて労働者本人の同意を取得すること、労働者を不利益に取扱わないこと、情報の取扱者を制限することなどの措置をとることが必要である。

２．解説

（１）「労働者の心身の状態に関する情報」と個情法

事業者（個人情報取扱事業者）は、事業活動を行うために労働者を雇用し、その雇用する労働者について、氏名、年齢、性別など基本的な情報に加え、給与の額、勤務状況、勤務成績など多くの情報を保有している。これらの労働者の情報は、個人情報（個情法第 2 条第 1 項）に該当し、個情法に基づいた取扱いを行わなければならない。また、労働者の情報には、労働者の病歴や健康診断の結果、健康診断の結果に基づき医師から指導等を受けたこと、すなわち労働者の心身の状態に関する情報も含まれる。このような労働者の心身の状態に関する情報のほとんどが、要配慮個人情報（個情法第 2 条第 3 項）に該当し得る。個人情報保護委員会・厚生労働省「雇用管理分野における個人情報のうち健康情報

を取り扱うに当たっての留意事項」（平成 29 年 5 月 29 日）[1]（以下、本項において「留意事項」という。）によれば、例えば、労働安全衛生法の諸規定に基づく健康診断の結果やストレスチェックの結果等が要配慮個人情報にあたるとされている。要配慮個人情報に該当する場合には、その取得に当たって原則として本人同意を得る必要がある（同法第 20 条第 2 項）、オプトアウトによる第三者提供は認められない（同法第 27 条第 2 項）など、要配慮個人情報としての取扱いに係る規律に留意しなければならない。要配慮個人情報に該当する具体例を含め、個情法に基づく具体的な取扱いの方法については、留意事項を参照されたい。

（２）「労働者の心身の状態に関する情報」と労働安全衛生法

事業者は労働者に対して安全配慮義務を負っており、この履行として労働者の健康管理活動を行う必要がある（労働契約法（平成 19 年法律第 128 号）第 5 条、最判昭和 50 年 2 月 25 日民集 29 巻 2 号 143 頁）。また、労働安全衛生法は、労働者の安全と健康を確保するとともに、快適な職場環境の形成を促進する目的で、事業者に様々な労働者の健康管理措置を行うことを求めている（労働安全衛生法第 66 条以下）。同法にいう事業者とは、「事業を行う者で、労働者を使用するものをいう。」と定義されており（同法第 2 条第 3 号）、業種や分野、法人格の有無を問わない。法人企業であれば当該法人（法人の代表者ではない。）、個人企業であれば事業経営主を指し、事業経営の利益の帰属主体そのものを義務主体としている[2]。

したがって、労働者の健康管理活動や健康確保措置を行うため、事業者は労働者の心身の状態に関する情報を取得する必要がある。もっとも、労働者側としては自身の心身の状態についての情報により不利益な取扱いを受けるという懸念があり、自身の心身の情報について、事業者に対して、取得、利用、管理のそれぞれの場面に応じた適切な管理を望んでいる。

このような観点から、労働安全衛生法は、事業者は、労働者の心身の状態の情報を収集、保管、又は使用するに当たっては、労働者の健康の確保に必要な範囲内で収集し、当該収集の目的の範囲内でこれを保管し、使用しなければならないとしている（同法第 104 条第 1 項）。加えて、労働者の心身の状態に関する情報を適正に管理するために必要な措置を講じなければならないとしている（同条第 2 項）[3]。

---

[1] https://www.ppc.go.jp/personalinfo/legal/ryuuijikou_health_condition_info/ 都道府県労働局長宛て個人情報保護委員会事務局長・厚生労働省労働基準局長通知「雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項について（通知）」（平成 29 年 5 月 29 日付個情第 749 号・基発 0529 第 3 号）も参照されたい。

[2] 都道府県労働基準局長宛て労働事務次官通達「労働安全衛生法の施行について」（昭和 47 年 9 月 18 日発基第 91 号）。

[3] 労働者の心身の状態に関する情報の取扱いについては、同様の規定がじん肺法（昭和 35 年法律第 30 号）第 35 条の 3 にも設けられている。

このように「労働者の心身の状態に関する情報」には、健康診断の結果などの要配慮個人情報も含まれ、さらに労働安全衛生法によっても事業者に適切な取扱いが要請される情報でもある。したがって、その取扱いに当たっては、個情法や労働安全衛生法との関係に留意することが必要である。このうち、要配慮個人情報を含む個人情報の取扱いに関しては、留意事項を、また、労働者安全衛生法による労働者の心身の状態に関する情報の取扱いについては、「労働者の心身の状態に関する情報の適正な取扱いのために事業者が講ずべき措置に関する指針」（以下、本項において「指針」という。労働安全衛生法第 104 条第 3 項参照）を参照されたい。

（３）労働者の心身の状態に関する情報の適正な取扱いのために事業者が講ずべき措置に関する指針

労働者の心身の状態の情報をどのように取扱うかについては、指針において具体的に示されている。

指針においては、まず、心身の状態の情報の取扱いに関する原則として、①取扱いの目的は労働者の健康確保や安全配慮義務の履行のためであり、そのために必要な情報を適正に収集し、活用すること、②事業者による労働者の健康確保措置が十全に行われるよう事業所における取扱規程を定めること、③心身の状態の情報を取扱う目的や取扱い方法、取扱者、取扱う情報の範囲などを取扱規程に定めること、④取扱規程については、労使関与の下で定めるとともに労働者へ周知すること、⑤情報取扱者の制限や情報の加工など適正な取扱いのための体制を整備すること、⑥情報の収集に当たって本人同意の取得や利用目的、取扱い方法の周知を行うこと、⑦労働者に対する不利益な取扱いを防止することなどが定められている。

また、同様に、心身の状態の情報の適正管理（労働安全衛生法第 104 条第 2 項関係）の方法についても示されている。具体的には、①心身の状態の情報の適正管理のための規程として、心身の状態の情報の正確性の確保、安全管理措置、適切な消去等について、事業場ごとに取扱規程に定めること、②労働者からの開示請求、訂正等に適切に対応することなどが定められている。

（４）健康診断等の事務を実施した者の守秘義務等について

その他、労働安全衛生法に基づく労働者の心身の状態に関する情報の取扱いに関しては、同法第 105 条にも留意を要する。同条は、同法に基づく健康診断、面接指導、ストレスチェック等の実施事務に従事した者に対して、その実施に関して知り得た労働者の秘

密を漏らしてはならない旨を規定するものであり、これに違反した者に対しては、6 月以下の懲役又は 50 万円以下の罰金が科せられる（同法第 119 条第 1 号）[4] [5]。

これに関連して、個人の健康診断結果や服薬歴等の健診等情報（Personal Health Record、以下、本項において「PHR」という。）を電子記録として本人や家族が正確に把握するための仕組みについて、適切に民間 PHR サービスが利活用されるための民間 PHR 事業者におけるルール整備等が必要であるとされたことを受け、PHR サービスを提供する民間事業者が遵守すべき事項について、総務省、厚生労働省、経済産業省から、「PHR サービス提供者による健診等情報の取扱いに関する基本的指針」が公表された。同指針は、令和 7 年 4 月に改定されているところ、PHR サービス提供者が健診等情報を取り扱うに当たって、①情報セキュリティを確保するために講じなければならない対策の内容やその具体例、②個人情報の取扱いに関する法規制及び同指針に基づき遵守しなければならない事項の内容等が示されている。また、別紙には、同指針に係るチェックリストも付属しており、参考になる。

３．参考資料（法令・ガイドラインなど）

・労働安全衛生法第 104 条、第 105 条、じん肺法第 35 条の 3、第 35 条の 4
・個人情報保護委員会、厚生労働省「雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項」（平成 29 年 5 月 29 日）
・労働者の心身の状態に関する情報の適正な取扱いのために事業者が講ずべき措置に関する指針（平成 30 年 9 月 7 日　労働者の心身の状態に関する情報の適正な取扱い指針公示第 1 号）
・厚生労働省「事業場における労働者の健康情報等の取扱規程を策定するための手引き」（平成 31 年 3 月）
・総務省、厚生労働省、経済産業省「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」（令和 3 年 4 月 23 日策定、令和 4 年 4 月一部改定）

４．裁判例

本文中に記載のとおり

[4] なお、罰則付きの守秘義務については、Q77 も参照されたい。
[5] 守秘義務については、刑法（明治 40 法律第 45 号）第 134 条 1 項、保健師助産師看護師法（昭和 23 年法律第 203 号）第 42 条の 2、臨床検査技師等に関する法律（昭和 33 年法律第 76 号）第 19 条及びじん肺法第 35 条の 4 などにも規定されている。

Q20 マイナンバーの取扱い

企業がマイナンバーを取り扱う上で、その安全管理を含め留意しなければならない点は何か。

タグ：番号利用法、個情法、マイナンバー、個人番号、安全管理措置

１．概要

マイナンバー（個人番号）については、その制度趣旨に鑑み、利用主体や利用範囲の限定、厳格な本人確認、提供等の制限等の個情法における個人情報には見られない対応が求められる。

２．解説

（１）マイナンバー制度の趣旨と個人情報との相違

マイナンバー制度は、行政運営の効率化と国民の利便性の向上を図り、公平・公正な社会を実現する基盤となるものである（番号利用法第 1 条参照）が、全ての住民に指定される個人識別のための番号である（同法第 2 条第 5 項参照）ことから、安全かつ適正な取扱いを担保するため、企業がマイナンバーを取り扱う際には、以下のとおり、個情法に規定する「個人情報」[1]には見られない対応が求められる。

（２）利用主体や利用範囲を法律で限定

マイナンバーは、番号利用法に定められた、①社会保障・税・災害対策等分野[2]の行政事務（個人番号利用事務。番号利用法第 2 条第 11 項参照）、②個人番号利用事務に関して行われている事務（個人番号関係事務。番号利用法第 2 条第 12 項参照。以下、個人番号利用事務と総称して、本項において「個人番号利用事務等」という。）の範囲内に限り、利用が認められる。本人の同意を得たとしても、この範囲を超えて利用することはできない。

---

[1] なお、番号利用法は、「個人情報」の定義について個情法を引用している。従来は、番号利用法において、個人情報とは、「行個法に規定する個人情報であって行政機関が保有するもの」、「独個法に規定する個人情報であって独立行政法人等が保有するもの」又は「個情法に規定する個人情報であって行政機関及び独立行政法人等以外の者が保有するもの」である旨規定していたが、デジタル社会整備法による改正に伴い個人情報の定義が統合されたことに伴い、番号利用法における個人情報の定義も改正された（現行の番号利用法第 2 条第 3 項において、「この法律において「個人情報」とは、個人情報保護法第二条第一項に規定する個人情報をいう。」と規定されている）。

[2] 理容師・美容師、小型船舶操縦士及び建築士等の国家資格等、自動車登録、在留資格に係る許可等に関する事務においてもマイナンバーの利用は可能である（番号利用法別表（第 9 条関係）参照）。

企業においては、例えば、雇用保険被保険者資格取得届や源泉徴収票の作成等の個人番号関係事務に必要な限度で、個人番号関係事務実施者として、マイナンバーの利用が認められる。

（３）厳格な本人確認

個人番号利用事務実施者[3]及び個人番号関係事務実施者[4]は、本人からマイナンバーの提供を受けるときは、なりすましを防止するため、本人確認（番号確認と身元確認）措置をとらなければならない（番号利用法第 16 条参照）。

企業においては、例えば、雇用保険被保険者資格取得届や源泉徴収票の作成等の個人番号関係事務に当たり、従業員等本人からマイナンバーの提供を受けるときは、マイナンバーカード等による本人確認を行う必要がある。

（４）提供等の制限

マイナンバーを含む個人情報は、番号利用法上、「特定個人情報」と定義される（番号利用法第 2 条第 9 項）。特定個人情報については、番号利用法で定められた一定の場合を除き、提供の求め・提供・収集・保管が禁止される（番号利用法第 15 条、第 19 条、第 20 条参照）。本人の同意を得たとしても、番号利用法で定められた場合に該当しない限り、提供等は認められない。

また、（２）の事務（個人番号利用事務・個人番号関係事務）を第三者に委託することは可能であるが、再委託に当たっては、委託元の許諾が必要となる（番号利用法第 10 条第 1 項参照）。

（５）安全管理措置

個人番号利用事務等の全部又は一部の委託をする者は、当該委託に係る個人番号利用事務等において取り扱う特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなければならない（番号利用法第 11 条）。また、個人番号関係事務実施者又は個人番号利用事務実施者である事業者は、個人番号及び特定個人情報（以下、本項において「特定個人情報等」という。）の漏えい、滅失又は毀損の防止その他の特定個人情報等の管理のために、必要かつ適切な措置を講じなければならない（番号利用法第 12 条、個情法第 23 条）。

[3] 個人番号利用事務を処理する者及び個人番号利用事務の全部又は一部の委託を受けた者をいう（番号利用法第 2 条第 13 項）。
[4] 個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者をいう（番号利用法第 2 条第 14 項）。

個人番号利用事務等の全部又は一部の委託の場合は委託先に安全管理措置を遵守させるために委託先との契約において一定の事項を盛り込むこととされており[5]、また、安全管理措置の具体的な内容については、個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の「（別添１）特定個人情報に関する安全管理措置（事業者編）」が参考になる。特定個人情報の漏えい等が発生した場合の個人情報保護委員会への報告等については、Q57 を参照。

（６）マイナンバーの利用制限とマイナンバーカード

マイナンバーの利用範囲は、番号利用法において、行政機関等に限定されているが、マイナンバーカード自体については番号利用法上、基本的に利用範囲に制限がなく、民間企業もこれを利用することができる。

すなわち、マイナンバーカードの利用とマイナンバーそのものの利用とは法的性質を異にする。マイナンバーカードは、裏面にマイナンバーが記載されているものの、カードの利用は、マイナンバーそのものを利用しない限りは、マイナンバーの利用とはみなされない。マイナンバーそのものを利用するとは、①マイナンバーの提示書類としての機能のように、マイナンバーカードに記載されたマイナンバーの確認、コピー、又はマイナンバーカードの IC チップ内に記録されたマイナンバーの読み取り等を指す。これに対して、②顔写真付き本人確認書類、③オンラインでの確実な本人確認（公的個人認証サービスによる電子証明書[6]）の場合は、マイナンバーそのものを確認・取得等することなく、マイナンバーカードを利用しているだけであるので、マイナンバーの利用にはあたらない。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[5] 個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」第 4-2-(1)。

[6] https://www.soumu.go.jp/kojinbango_card/kojinninshou-01.html

Q21 営業秘密の要件

不正競争防止法上の「営業秘密」としての法的保護は、サイバーセキュリティとの関係でどのように位置づけられるか。

タグ：不正競争防止法、営業秘密、情報管理、営業秘密保有者、秘密管理性、有用性、非公知性、従業員、委託、リスクマネジメント

１．概要

不正競争防止法の「営業秘密」に該当する情報を不正に取得、開示又は使用する「不正競争」により営業上の利益を侵害され、又は侵害されるおそれがある者は、同法に基づいてその営業上の利益を侵害する者又は侵害するおそれがある者に対し差止請求を、また、営業上の利益を侵害されたときは、同法等に基づき損害賠償請求を、それぞれ行い得る。さらに、同法が定める構成要件に該当すれば、不正取得等の行為をした者は営業秘密侵害罪により処罰の対象となる。このように不正競争防止法に基づく営業秘密の法的保護は、サイバーインシデント発生後に営業秘密保有者が採り得る法的手段の一つとして機能するとともに、侵害予防請求や罰則による威嚇的効果により、その発生を未然に防止する機能も営む。

２．解説

（１）「営業秘密」の定義及び法的保護の内容

「営業秘密」とは、不正競争防止法第 2 条第 6 項が定める三要件（秘密管理性・有用性・非公知性）を全て満たす情報をいう。「営業秘密」に該当する情報について不正競争（不正な取得・開示・使用）がなされた場合、同法が定めるその他の要件に該当すれば、当該情報は、次の手段による法的保護を受けることができる。

・民事上の措置：差止請求（第 3 条）、損害賠償請求（第 4 条、民法第 709 条[1]）
・刑事罰：一定の不正取得・使用・開示行為が対象（第 21 条、第 22 条）
・水際措置：営業秘密侵害品の輸入差止（関税法第 69 条の 11 第 1 項第 10 号等）

なお、秘密保持契約書や社内規程で定められる「秘密情報」や「機密情報」、「企業秘密」は、企業同士における契約や組織内の規程において用いられる呼称にすぎず、必ずしも「営業秘密」に該当し不正競争防止法上の保護を受けられるとは限られない。

[1] 厳密には、損害賠償を定めた第 4 条は、「不正競争」による営業上の利益の侵害が民法第 709 条の要件を充足することを確認的に規定したものである（逐条不正競争防止法 170 頁）。

また、不正競争防止法は、取引の安全等の観点から一定の場合には同法による法的保護を受けられない旨（適用除外・第 19 条）を定めているため、ある情報が当該法的保護を受けるには適用除外規定に該当しないことも必要となる。

（２）「営業秘密」として認められるための三要件（2 条 6 項）

① 秘密管理性

保有者の秘密管理意思（特定の情報を秘密として管理しようとする意思）が、保有者が実施する具体的状況に応じた経済合理的な秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保されていることをいう[2]。

営業秘密は、そもそも情報自体が無形で、その保有・管理形態も様々であること、また、特許権等のように公示を前提とできないことから、営業秘密たる情報の取得、使用又は開示を行おうとする従業員等にとって、当該情報が同法により保護される営業秘密であることを容易に知り得ない状況が想定される。本要件の趣旨は、このような営業秘密の性質を踏まえ、企業が秘密として管理しようとする対象が明確化されることによって、当該営業秘密に接した者が事後に不測の嫌疑を受けることを防止し、従業員等の予見可能性、ひいては経済活動の安定性を確保することにある。裁判例上は、情報の性質・種類・内容・価値、保有形態、企業の規模、従業員に対する指導監督及び侵害した相手方との関係等に応じて総合的に合理性を有する秘密管理措置が実施されていたか否かが考慮される。

② 有用性

当該情報が、営業秘密を保有する事業者の事業活動に使用・利用されているのであれば、当該情報が公序良俗に反するなど保護の相当性を欠くような場合でない限り有用性の要件は充足される。必ずしも現に事業活動に使用・利用されていることを要するものではなく、直接ビジネスに活用されている情報に限らず、間接的な（潜在的な）価値がある場合も含む[3]。

③ 非公知性

当該情報が、一般的に知られた状態になっていない状態、又は容易に知ることができない状態であることをいい、具体的には、当該情報が合理的な努力の範囲内で入手可能な刊行物に記載されていない、公開情報や一般に入手可能な商品等から容易に推測・分析されない等、営業秘密保有者の管理下以外では一般的に入手できない状態をいう[4]。

---

[2] 営業秘密管理指針 8 頁。
[3] 前掲注 2・20 頁。
[4] 前掲注 2・22 頁。

（３）従業員や取引相手先との関係について

秘密管理性要件が満たされるためには、営業秘密保有者の秘密管理意思（特定の情報を秘密として管理しようとする意思）が、具体的状況に応じた経済合理的な秘密管理措置によって、従業員に明確に示され、結果として、従業員が当該秘密管理意思を容易に認識できる（換言すれば、認識可能性が確保される）必要がある。具体的に必要な秘密管理措置の内容・程度は、企業の規模、業態、従業員等の職務、情報の性質その他の事情の如何によって異なるものであり、企業における営業秘密の管理単位における従業員等がそれを一般的に、かつ容易に認識できる程度のものである必要がある。取引相手先に対する秘密管理意思の明示についても、基本的には、従業員と同様に考えることができる。

秘密管理措置の対象者は、当該情報に合法的に、かつ、現実に接することができる従業員等である。

従業員や委託先企業が作成や取得に関与した情報については、雇用企業又は委託元企業の秘密管理意思が具体的状況に応じた経済合理的な秘密管理措置によって明確に示されており、従業員又は委託先企業において当該秘密管理意思を容易に認識できる場合には、雇用企業又は委託元企業が、営業秘密を保有する事業者として「営業秘密保有者」に該当し得るものと考えられる。

また、このような場合、当該従業員又は委託先企業は、営業秘密保有者から営業秘密を「示された」者に該当すると解され得る。

よって、雇用企業又は委託元企業においては、従業員又は委託先企業との間で情報を特定した秘密保持契約を締結するなどして「営業秘密」の要件を満たすような情報管理をすることにより、当該情報にサイバーインシデントが生じたときに、攻撃者等に対して民事上の措置を講じたり、刑事罰を求めて告発したりすることができる。

なお、従業員との関係においては、転職の自由に留意しつつ、具体的に企業秘密に接する時期に、秘密として管理すべき情報を特定した上で、秘密保持義務を負わせることが望ましいと考えられる。また、委託先企業との関係においては、秘密保持契約における制限が公正競争阻害性を有したり、片務的な秘密保持契約が優越的地位の濫用行為に該当したりしないよう、留意が必要である。

（４）営業秘密として法的保護を受けるための情報管理と、サイバーセキュリティ対策としての情報管理の異同

いずれも情報に関するリスクマネジメントである点で共通するが、上記のとおり、営業秘密として法的保護を受けるための情報管理は、企業が秘密として取り扱いたい情報が漏えいした後に当該情報について不正競争防止法に基づく民事上の措置や刑事罰といった法的保護を受けることを目的とした情報管理であり、サイバーセキュリティ対策としての情報管理は、企業が保有する様々な情報の漏えい・滅失・毀損の可能性を事前に回避・

低減等することを目的とした情報管理であるという点で異なる。相違点の概要は、以下のとおりである。

	営業秘密管理	サイバーセキュリティ対策
対象となる情報の範囲	「営業秘密」（第 2 条第 6 項）の三要件に該当する情報	機微情報・個人情報・機器制御情報など、サイバーセキュリティリスクが懸念される情報
対策内容	主に情報の漏えいを防ぐもの	情報の漏えい、滅失又は毀損を防ぐもの
アプローチ（事後か事前か）	不正競争（行為）に対して事後的に法的保護を受けることを目的とした情報管理	被害を未然に防ぐための情報管理

3．参考資料（法令・ガイドラインなど）

・営業秘密管理指針
・秘密情報の保護ハンドブック
・経済産業省知的財産政策室「秘密情報の保護ハンドブックのてびき；情報管理も企業力」
・経営ガイドライン
・公正取引委員会「知的財産の利用に関する独占禁止法上の指針」（平成 19 年 9 月 28 日（最終改正平成 28 年 1 月 21 日））
・公正取引委員会「製造業者のノウハウ・知的財産権を対象とした優越的地位の濫用行為等に関する実態調査報告書」（令和元年 6 月）

4．裁判例

・大阪地裁令和 2 年 10 月 1 日（平成 28 年（ワ）第 4029 号）
　原告会社の元従業員が、在職中に原告会社のリフォーム事業に関する営業秘密を不正取得・開示し、被告会社がこれを利用したとして、不正競争が認められた事例。
・知財高判令和 3 年 6 月 24 日金融・商事判例 1629 号 26 頁
　従業員間で共有を図られていたと推察される顧客カルテの施術履歴部分は、秘密管理性を欠き「営業秘密」に該当しない等と判断された事例。
・札幌地判平成 6 年 7 月 8 日（平成 6 年（モ）第 725 号）
　顧客情報は、オフィスコンピュータに入力されデータベースとして統一的に管理されており、入力作業は女性職員一名に担当させ、他には一切担当させないなど、従業員によるアクセスをも不可能としていた場合に、秘密管理性が認められた事例。
・東京地判平成 14 年 2 月 5 日判時 1802 号 145 頁・判タ 1114 号 279 頁

被告が、原告から仕入れた原告商品の仕入価格を明示してその仕入価格で販売するという原価セールを行ったことに関連して、被告の開示した原告からの仕入価格は、営業秘密には当たらないとされた事例。

・東京高判平成 15 年 3 月 31 日（平成 14 年（ラ）第 1302 号）

申立人の会員情報は保有者である申立人から被申立人に示されたものではないため、営業秘密の取得に当たらないとされた事例。

・東京高判平成 16 年 9 月 29 日判タ 1173 号 68 頁

被告が継続的に購入している医薬品についての原告からの仕入価格は、原告から開示を受けたものではないとして、不正競争行為はないとされた事例。

・知財高判平成 18 年 2 月 27 日（平成 17 年（ネ）第 10007 号）

商品の仕入価格は、売買契約の当事者との合意によって形成されるものであり、これが売主から買主に営業秘密を「示された」とみることは適切でないとして、買主が仕入価格を開示した行為は不正競争に当たるということはできないとされた事例。

・知財高裁平成 24 年 7 月 4 日（平成 23 年（ネ）第 10084 号・平成 24 年（ネ）第 10025 号）

元従業員らが、原告会社グループの顧客情報を退職後に利用して管理委託契約の顧客を引き抜き、さらに倒産の虞があるなどの虚偽を告知して信用を毀損した行為が不正競争に該当すると判断された事例。

・大阪地裁平成 30 年 3 月 5 日（平成 28 年（ワ）第 648 号）

原告が医薬品配置事業を譲り受けたことに伴い、必須となる顧客情報も原告に譲渡されており、事業譲渡日以降、原告が保有者となった当該顧客情報は有用性、非公知性、秘密管理性が認められる営業秘密に該当すると判断された事例。

Q22 限定提供データとサイバーセキュリティ

平成 30 年不正競争防止法改正により新たに導入された「限定提供データ」は、どのような制度であり、サイバーセキュリティインシデントにどのように対応できるのか。

タグ：不正競争防止法、限定提供データ、限定提供性、相当量蓄積性、電磁的管理性、営業秘密

１．概要

平成 30 年に不正競争防止法が改正され、「限定提供データ」の不正取得、不正使用又は不正開示といったサイバーセキュリティインシデントに対して差止請求又は損害賠償請求をなし得るようになった。「限定提供データ」にこのような法的保護を与えたのは、データの利活用を促進するための環境を整備するためである[1]。

また、限定提供データとしての法的保護を受けるために行う電磁的管理が、サイバーセキュリティ対策に通ずる場合もある。

２．解説

（１）「限定提供データ」とは

「限定提供データ」とは、「業として特定の者に提供する情報として電磁的方法……により相当量蓄積され、及び管理されている技術上又は営業上の情報（営業秘密を除く。）」と定義される（不正競争防止法第 2 条第 7 項）。

各要件は概要以下のとおりであるが、詳細な解説については、限定提供データに関する指針を参照されたい。

・業として特定の者に提供する情報であること（限定提供性）
・電磁的方法により相当量蓄積されていること（相当量蓄積性）
・電磁的方法により管理されていること（電磁的管理性）

なお、限定提供データが無償で公衆に利用可能となっている情報（オープンなデータ）と同一の情報である場合には、当該情報の不正取得・使用・開示行為については不正競争に該当しない（不正競争防止法第 19 条第 1 項第 9 号ロ[2]）ので留意が必要である。

---

[1] 経済産業省「不正競争防止法平成 30 年改正の概要（限定提供データ、技術的制限手段等）」（平成 30 年）（https://www.meti.go.jp/policy/economy/chizai/chiteki/H30_kaiseigaiyoutext.pdf）。なお、中間報告や新旧対照表は、右記ウェブサイトにまとめられている（「平成 30 年改正（限定提供データの不正取得等を不正競争行為として追加、技術的制限手段に係る規律強化）」https://www.meti.go.jp/policy/economy/chizai/chiteki/kaisei_recent.html）。

[2] 不正競争防止法第 19 条第 1 項第 9 号ロに該当すると、不正競争防止法が適用されないことになるので、このロの事由のことを適用除外事由という。

（２）法的保護の内容

限定提供データの不正取得・使用・開示のうち「不正競争」に該当する行為に対しては、差止請求又は損害賠償請求をなし得る（不正競争防止法第 3 条、第 4 条参照）。

刑事罰については、「まだ事例の蓄積も少ない中で、事業者に対して過度の萎縮効果を生じさせ」かねないことから設けられていない（限定提供データ指針 6 頁）。

また、限定提供データと同じ不正競争防止法に規定される営業秘密の場合は、営業秘密侵害品の譲渡等も不正競争の対象とされている（不正競争防止法第 2 条第 1 項第 10 号）のに対し、限定提供データの場合は、不正取得等された限定提供データを使用して生み出された物品の流通を不正競争として規制する規定はない。よって、「取得したデータを使用して得られる成果物（データを学習させて生成された学習済みモデル、データを用いて開発された物品等）がもはや元の限定提供データとは異なるものと評価される場合には、その使用、譲渡等の行為は不正競争には該当しない」ことになる（限定提供データ指針 21 頁）。

なお、法適用の場面において、営業秘密と限定提供データの 2 つの制度による保護が重複して及ばないことを意味することを明確にすべく、不正競争防止法の令和 5 年改正により、限定提供データの定義条項（第 2 条第 7 項）における「秘密として管理されているものを除く」という要件が、上記のとおり「営業秘密を除く」に改められた。

（３）サイバーセキュリティインシデントにどのように対応できるか

データの管理・利用においてサイバーセキュリティを確保しようとすると、自ずと、限定提供データの電磁的管理性の要件も満たされることが多いものと思われる。

逆に、「限定提供データ」としての法的保護を受けることを予定してデータを管理することは、サイバーセキュリティ対策の実施にもなり得る。例えば、電磁的管理性として、認証技術とともに対象となるデータを暗号化していた場合（限定提供データ指針 12 頁～13 頁）には、サイバー攻撃によりデータが不正に取得されたとしても、データの内容の流出（漏えい）を防ぎ得るし、ID・パスワードによるユーザ認証によってアクセスを制限していた場合（限定提供データ指針 13 頁）には、データの不正取得自体を防ぎ得る。

もっとも、限定提供データの法的保護は、限定提供データの不正取得等の不正行為が生じた後に又は生じようとしているときに、当該不正行為を行った者・行う者に対して差止請求又は損害賠償請求をすることができるという制度であるから、当該不正行為を行う者・行おうとする者（いわゆる被疑侵害者）をある程度特定できなければ、そのようなサイバーセキュリティインシデントに対して限定提供データの制度を利用した対応を取ることはできない。

３．参考資料（法令・ガイドラインなど）

・不正競争防止法第 2 条第 1 項第 11 号～第 16 号、第 2 条第 7 項、第 3 条、第 4 条、第 19 条第 1 項第 9 号ロ
・限定提供データに関する指針
・営業秘密管理指針

４．裁判例

特になし

Q23 技術的手段の回避行為・無効化行為の法的責任

企業内の秘密情報や従業員情報、顧客情報等のコピーや改変の禁止のために、若しくは当該情報が格納されたサーバやクラウドへのアクセスの禁止のために、又はアプリやソフトウェアの認証（アクティベーション方式）のために、技術的な手段が施されている場合に、そのような技術的手段を回避したり無効化したりする行為について、法律上、どのような責任が発生するのか。

タグ：不正競争防止法、著作権法、刑法、不正アクセス禁止法、技術的制限手段、技術的保護手段、技術的利用制限手段、技術的手段

１．概要

技術的手段を回避したり無効化したりする行為については、著作権法（昭和 45 年法律第 48 号）又は不正競争防止法に基づく民事上又は刑事上の法的責任が生じ得るが、一般論として、サイバーセキュリティ技術の開発目的又は当該技術の試験・研究目的による場合には、これら二つの法律に基づく法的責任は生じないと考えられる。

その他、刑法や不正アクセス禁止法等への抵触についても留意が必要である。

２．解説

（１）技術的手段とは

実務上、著作権法の「技術的保護手段」（第 2 条第 1 項第 20 号）及び「技術的利用制限手段」（同項第 21 号）、並びに不正競争防止法の「技術的制限手段」（第 2 条第 8 項）[1]をまとめて、「技術的手段」と呼ぶ[2] [3]。

（２）著作権法上の技術的保護手段・技術的利用制限手段の保護と不正競争防止法上の技術的制限手段の保護の相違点について

いずれも技術的手段に民事的措置及び刑事的措置（刑事罰）による保護を与えている点等多くの点で共通するが、著作権法と不正競争防止法における技術的手段の保護に関する主な相違点をまとめると、以下のとおりである。

---

[1] 平成 30 年不正競争防止法改正により、技術的制限手段の保護範囲が拡大され、アクティベーション方式も技術的制限手段に含まれることを明確化するために、「影像、音若しくはプログラムとともに」という要件が削除され、また、シリアルコード等の「指令符号」の提供等及びプロテクト破り代行サービス等の「役務」も「不正競争」として規制対象に加えられた。

[2] 逐条不正競争防止法 126 頁・注 1。なお、著作権法第 29 条に規定される「技術的手段」とは異なる意味である。

[3] Technological Measures や Technical Protection Measures に相当する用語であり、後者の略称の TPM と呼ばれることもある。

	著作権法上の技術的保護手段・技術的利用制限手段の保護	不正競争防止法上の技術的制限手段の保護
保護の対象物[4]	著作物、実演、レコード、放送又は有線放送	著作物性は問わず、影像、音、プログラムその他の情報
技術的手段の用途	営業上用いられるか否かは問わない。	営業上用いられる技術的制限手段に限られる。
回避行為・無効化行為後の対象物の利用	私的使用目的であっても、技術的保護手段が回避された対象物を回避されたことを知りながら複製等する行為は複製権侵害となり得る(著作権法第 30 条第 1 項第 2 号)。	不正競争防止法違反とはならない。
取り得る措置	回避装置等についての水際措置（税関における輸出入差止め手続）はない（もっとも、コピーコントロール技術を外して違法にコピーされた著作物等であれば、水際措置の対象となり得る)。	無効化装置等についての水際措置（税関における輸出入差止め手続）がある。

（3）技術的手段の回避行為・無効化行為に関する法的責任

著作権法と不正競争防止法における技術的手段の回避行為・無効化行為に関する法的責任をまとめると、以下のとおりである。

	著作権法			不正競争防止法
	技術的保護手段の回避行為	技術的利用制限手段の回避行為	技術的保護手段及び技術的利用制限手段の回避を行うための指令符号の提供等	技術的制限手段の無効化装置等の提供等の行為
民事上の責任	回避行為そのものは規制対象ではない。 ただし、回避行為後に回避されたことを知りながら行う私的使用目的の複製行為は著作権	一定の場合を除き、回避行為がみなし侵害行為（第 113 条第 6 項）	指令符号の提供等がみなし侵害行為(第 113 条第 7 項)	不正競争として差止め請求・損害賠償請求（第 2 条第 1 項第 17 号・第 18 号、第 3 条、第 4 条） なお、無効化行為そのものは規制対象ではないが、無効化するサービスの提供は規制対象である。

[4] 有体物に限る意味ではなく、無体物も含む意味で「対象物」と記載するものである。

	侵害になり得る（第 30 条第 1 項第 2 号）。			
刑事上の責任	－ 以下の行為について、拘禁刑 3 年以下若しくは罰金 300 万円以下又は併科 ・ 回避する機能を有する装置・プログラムの複製物の公衆への譲渡等、公衆への譲渡等目的の製造行為等、当該プログラムの公衆送信等（第 120 条の 2 第 1 号） ・ 業として公衆からの求めに応じて回避する行為（第 120 条の 2 第 2 号） ・ 技術的保護手段及び技術的利用制限手段の回避を行うための指令符号の提供等（第 120 条の 2 第 4 号） － 上記いずれの行為の場合も罰金 300 万円以下の法人両罰あり（第 124 条第 1 項第 2 号）			－ 上記行為について、拘禁刑 5 年以下若しくは罰金 500 万円以下又は併科（第 21 条第 3 項第 4 号） ・ 「不正の利益を得る目的で、又は営業上技術的制限手段を用いている者に損害を加える目的」が必要 ・ 罰金 3 億円以下の法人両罰あり（第 22 条第 1 項第 3 号）

（4）技術・開発目的、試験・研究目的について

ア 著作権法について

サイバーセキュリティに関する技術の開発のために行う技術的手段への攻撃行為（回避行為・無効化行為）については、著作権法上、「技術的利用制限手段に係る研究又は技術の開発の目的上正当な範囲内で行われる場合その他著作権者等の利益を不当に害しない場合」には、みなし侵害行為は成立しない[5]（第 113 条第 6 項）。また、刑事罰については、回避装置等の「公衆」への譲渡等、「公衆」への譲渡等目的での回避装置等の製造行為等、回避プログラムの公衆送信等、又は「公衆からの求めに応じて」の回避行為が規制対象とされている（第 120 条の 2 第 1 号・第 2 号）。著作権法上、「公衆」とは、不特定者のみならず、特定かつ多数の者を含むとされる（第 2 条第 5 項）ことから、例えば、自分が使用する目的や特定少数に譲渡する目的で回避装置等を製造する場合や、特定少数の求めに応じて回避行為を行うことは、刑事罰の対象外となると考えられる。

イ 不正競争防止法について

不正競争防止法の技術的制限手段の無効化行為についても、試験・研究目的で行う場合を規制の対象外としている（不正競争防止法第 19 条第 1 項第 10 号）。

（5）その他の法令への抵触の可能性について

不正なプログラムを作成等して技術的手段を回避・無効化した場合には、不正指令電磁的記録に関する罪により処罰され得るほか、電子計算機損壊等業務妨害罪や電磁的記録

[5] また、上記（3）記載のとおり、技術的保護手段の回避行為自体に関して民事上の責任は生じない。

毀棄罪などにより処罰され得る。また、技術的手段を回避・無効化して、①データを改ざんするなどした場合には、電磁的記録不正作出罪などにより、②情報を不正に入手した場合には、営業秘密侵害罪や通信の秘密侵害罪などにより、③情報を漏えいさせた場合には、個人情報データベース等提供罪や秘密漏示罪などにより、また、④不正にログインなどをした場合には、不正アクセス禁止法違反により、処罰され得る。その他、場合によっては、電算機使用詐欺罪などで処罰され得る（詳細は Q73～Q79 を参照されたい。）。

３．参考資料（法令・ガイドラインなど）

・著作権法第 2 条第 1 項第 20 号・第 21 号、第 2 条第 5 項、第 30 条第 1 項第 2 号、第 113 条第 6 項・第 7 項、第 120 条の 2 第 1 号・第 2 号・第 4 号、第 124 条第 1 項第 2 号
・不正競争防止法第 2 条第 1 項第 17 号・第 18 号、第 2 条第 8 項、第 3 条、第 4 条、第 19 条第 1 項第 10 号、第 21 条第 3 項第 4 号、第 22 条第 1 項第 3 号

４．裁判例

・東京地判平成 21 年 2 月 27 日（平成 20 年（ワ）第 20886 号・平成 20 年（ワ）第 35745 号）最高裁ウェブサイト

原告製品の仕組みが「技術的制限手段」に該当するか、被告製品の技術的制限手段を無効化する機能のみを有するといえるかについて争点となった事案。

・東京地判平成 25 年 7 月 9 日（平成 21 年（ワ）第 40515 号、同 22 年（ワ）第 12105 号、同第 17265 号）最高裁ウェブサイト、知財高裁平成 26 年 6 月 12 日（平成 25 年（ネ）第 10067 号）最高裁ウェブサイト

被告製品が、原告製品におけるプログラムの実行を営業上用いられている技術的制限手段の効果を妨げることにより可能とする機能のみを有するプログラムを記録した記録媒体に当たると認定し、その譲渡等により原告らの営業上の利益の侵害又はそのおそれを認め、差止め請求を認容した事案。

・大阪地判平成 28 年 12 月 26 日（平成 28 年（ワ）第 10425 号）最高裁ウェブサイト

原告製品の実行は、原告製品のライセンス取得者以外の者に原告製品の実行をさせないために営業上用いている技術的制限手段であるライセンス認証システムにより制限されていたところ、被告が、原告製品の実行を当該技術的制限手段の効果を妨げることにより可能とする機能を有する被告プログラムを電気通信回線を通じて提供した行為につき、不法行為に基づく損害賠償請求が認容された事案。

・最高裁判令和 3 年 3 月 1 日刑集 75 巻 3 号 273 頁

電子書籍の視聴制限を技術的に回避するプログラムが、「技術的制限手段の効果を妨げることにより影像の視聴を可能とする機能を有するプログラム」に当たるとされた事案。

Q24 データの知的財産権法規定による保護方法

企業や組織において保有する秘密情報やビッグデータなどの価値ある重要なデータについて、情報漏えい等が生じた場合に、不正競争防止法に基づく営業秘密又は限定提供データとしての保護以外に、他の知的財産権法規定による保護方法として有用なものはあるか。

タグ：不正競争防止法、著作権法、著作権、特許権、実用新案権、意匠権、営業秘密，限定提供データ

１．概要

秘密情報の保護については、そもそも、権利を取得するためには公開が必要となる特許権や実用新案権、権利取得後に権利内容の公開が必要となる意匠権といった産業財産権は適していない。なお、設計図、模型、写真、製造マニュアルといった形式の秘密情報については、これらに著作物性が認められる場合、著作権法で保護される可能性があるが、著作権法は表現を保護の対象としており、アイデア自体を保護するものではないため、秘密情報の表現ではなくて中身が利用された場合、保護が及ばないと考えられる。

構造を有するデータなどのプログラム等の特許権も、データそのものが保護されるものではない。また、データの選択又は体系的な構成によって創作性を有するデータベースは著作物として保護されるが、データベースを構成する個々の秘密情報やデータを保護するものではない。

このように、秘密情報の保護や価値ある重要なデータの保護として、産業財産権や著作権による保護は十分ではない。そこで、秘密情報の保護としては不正競争防止法による営業秘密としての保護が重要となるし（Q21 参照）、（営業秘密ではない）事業者等が取引等を通じて第三者に提供するデータの保護については平成 30 年の不正競争防止法改正により導入された限定提供データとしての保護が重要となる（Q22 参照）。なお、価値ある重要なデータについては、不正競争防止法による保護とは別途、適切な内容のデータ取引契約を締結することによる保護を図ることも重要となる。

２．解説

（１）特許法、実用新案法、意匠法又は著作権法による秘密情報の保護

ア　特許権又は実用新案権による保護について

特許権や実用新案権は、権利を取得するためには特許庁に出願して一般に公開しなければならない[6]ため、特許権や実用新案権では、秘密情報を秘密のまま保護することはできない。

なお、構造を有するデータは、プログラムに準ずるものと解釈される場合があり、プログラム等の特許権（特許法第 2 条第 4 項）として保護の対象となり得るが、データそのものを保護するものではなく、あくまでもデータ構造全体として特定された発明を保護するものに過ぎない。

イ　意匠権による保護について

権利取得後に権利内容の公開が必要となる意匠権は、秘密意匠制度を利用することにより、意匠登録の日から最長 3 年間、意匠を記載した図面などを秘密にすることが可能であるが、意匠を秘密とする期間が経過した後に、改めて図面などを掲載した公報が発行されるため、意匠法で秘密情報を秘密のまま保護できる期間は限定的である。

ウ　著作権による保護について

①　秘密情報の著作物該当性について

設計図、模型、写真、製造マニュアル、ソースコード、顧客データベースといった秘密情報について、著作物性が認められる場合には、著作権法による保護が考えられるが、以下のとおり、極めて限定的であるといわざるを得ない。

まず、著作権法上の「著作物」とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものをいうから（著作権法第 2 条第 1 項第 1 号）、著作権法の保護を受けるためには、当該秘密情報が創作的に表現されたものである必要がある。また、情報の選択又は体系的な構成によって創作性を有するデータベースは、著作物として保護される（同法第 12 条の 2 第 1 項）。

したがって、例えば、重要な顧客データベースであったとしても、それが顧客の住所、電話番号を五十音順に並べたものなど、ありふれた構成でデータベースの著作物としての創作性が認められない場合には、著作権法の保護を受けることはできない。データベースの著作物としての創作性が否定された例としては、自動車データベース

[6] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）に基づき、令和 6 年 5 月 1 日から、特許出願非公開制度が実施されている。これは、特許出願の明細書等に国家及び国民の安全を損なう事態を生ずるおそれが大きい発明が記載されている場合に保全指定により出願公開等を留保するものである。

の創作性について争われた事例で、東京地判平成 13 年 5 月 25 日判時 1774 号 132 頁（中間判決）、東京地判平成 14 年 3 月 28 日判時 1793 号 133 頁がある[7]。

他方、データベースの著作物としての創作性が肯定された例としては、旅行業者向けシステムのリレーショナル・データベース（データベースの情報の単位であるレコードを別のレコードと関連付ける処理機能を持つ）の創作性について争われた事案で、知財高判平成 28 年 1 月 19 日（平成 26 年（ネ）第 10038 号）最高裁ウェブサイト[8]がある。

② 著作権法に基づく保護の内容について

秘密情報が著作物として保護される場合、著作者は、公表権をはじめとする著作者人格権（同法第 18 条～第 20 条）、複製権をはじめとする著作権（財産権）（同法第 21 条～第 28 条）を享有し、これらの権利を侵害する者に対し、差止請求（同法第 112 条、第 116 条）、損害賠償請求、名誉回復措置請求（同法第 115 条、第 116 条）等が可能である。このため、情報漏えい等が生じた場合には、かかる権利行使により保護を図ることも考えられる。

しかしながら、著作権法は著作物の創作的な表現を保護する法律であって、アイデアを保護するものではないため、著作物に含まれるアイデア自体を使用する行為（例えば製造マニュアルを読んでそこに書かれているアイデアを利用して製造する行為）は著作権侵害とはならない。さらに、他人の営業秘密である機械の設計図に基づき、第三者が無断で機械を製作しても、機械に著作物性が認められない以上、設計図の著作権侵害にならないとされる（大阪地判平成 4 年 4 月 30 日判時 1436 号 104 頁）。

また、データベースを構成する個々のデータを不正に取得・利用された場合には、データベースそのものの複製でない限り、データベースの著作物に係る複製権侵害とはならないと考えられる。

（2）価値ある重要なデータの保護

平成 30 年の不正競争防止法改正において、商品として広く提供されるデータや、コンソーシアム内で共有されるデータなど、事業者等が取引等を通じて第三者に提供するデータを念頭においた、「限定提供データ」（不正競争防止法第 2 条第 7 項）の概念が導入され、限定提供データの不正取得・使用・開示行為等の不正競争も規制されることになった。当該制度については、Q22 を参照されたい。

---

[7] ただし、当該データベースの複製行為が不法行為に該当すると認定していることに注意。もっとも、その後の最判平成 23 年 12 月 8 日民集 65 巻 9 号 3275 頁において、著作権法所定の著作物に該当しない著作物の利用行為については、「同法が規律の対象とする著作物の利用による利益とは異なる法的に保護された利益を侵害するなどの特段の事情がない限り、不法行為を構成するものではない」として、不法行為の成立が否定されている。

[8] 原審：東京地判平成 26 年 3 月 14 日（平成 21 年（ワ）第 16019 号）最高裁ウェブサイト

（3）契約による保護

特許法等による保護は限定的であるため、企業や組織において保有する秘密情報やビッグデータなどの価値ある重要なデータについては、契約による保護を図ることが重要である。これについては Q51 において解説する。

3．参考資料（法令・ガイドラインなど）

・著作権法第 2 条第 1 項第 1 号（著作物の定義）、第 10 条（著作物の例示）、第 12 条の 2（データベースの著作物）
・特許法第 2 条第 4 項
・不正競争防止法第 2 条第 6 項（営業秘密）、同条第 7 項（限定提供データ）

4．裁判例

本文中に記載したもののほか、

・東京高判昭和 58 年 6 月 30 日無体例集 15 巻 2 号 586 号
　原告が創作したと主張する技術的思想や原理は、文章や図面などの表現形式を伴わない限り、著作権法上の保護対象ではなく、同様の技術的思想を文書に記載していたとしても、それは著作物の「引用」には当たらず、著作権侵害には該当しないとされた事案。
・東京地判平成 12 年 3 月 17 日判時 1714 号 128 頁
　電話番号情報を職業別に分類したデータベースがデータベースの著作物と認められた事案。
・東京地判平成 17 年 11 月 17 日判時 1949 号 95 頁
　空調設備等に排水等が溜まりやすい箇所を簡便に見出すために使用する図表の著作物性を否定した事案。
・大阪地判平成 16 年 11 月 4 日判時 1898 号 117 頁
　自然科学に関する論文と著作物性が争われた事案。

Q25 ソフトウェアのリバースエンジニアリング

マルウェア対策のために当該マルウェアを解析する場合やサイバーセキュリティ対策として不正行為に用いられるソフトウェアの構造等を解析する場合に、当該マルウェアや当該ソフトウェアの複製や一部改変を行うことは、著作権法上、問題ないのか。
マルウェアに感染等したソフトウェア、又はマルウェアの感染等から守られるべきソフトウェアについて、サイバーセキュリティ対策の目的で当該ソフトウェアを解析する際にこれを複製することは、著作権法上、問題ないのか。

タグ：著作権法、リバースエンジニアリング、マルウェア、柔軟な権利制限、複製権、翻案権、同一性保持権

１．概要

たとえサイバーセキュリティを脅かす不正行為に供されるソフトウェアやマルウェア[1]であっても、プログラムの著作物として著作権による保護を否定することはできないと考えられる。しかし、このようなサイバーセキュリティ対策目的やプログラムの調査解析目的で行われる当該プログラムの複製や改変等のいわゆるリバースエンジニアリング[2]や、生成 AI 以外の AI（認識、識別、人の判断支援等を行う AI）を開発する学習のための著作物の利用、技術開発・実用化試験のための著作物の利用については[3]、同法第 30 条の 4 に規定される権利制限の対象となる場合には、著作権侵害にはならないと考えられる。

２．解説

（１）プログラムの著作物について

マルウェアや不正行為に用いられるソフトウェア（以下、本項において「不正目的ソフトウェア」という。）であっても、通常は、著作権法上のプログラムの著作物（著作権法第 2 条第 1 項第 10 号の 2、第 10 条第 1 項第 9 号）[4]に該当するものは多いと考えられ

[1] malicious software の短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェア（サイバーセキュリティ 2025・227 頁）。
[2] 文化庁著作権課「デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方（著作権法第 30 条の 4、第 47 条の 4 及び第 47 条の 5 関係）」（令和元年 10 月 24 日）11 頁参照（https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_17.pdf）。
[3] 生成 AI のみならず、技術革新に伴う著作物の新たな利用態様に柔軟に対応できる権利制限規定として設けられたものとされている（文化庁 文化審議会著作権分科会法制度小委員会「AI と著作権に関する考え方について」（令和 6 年 3 月 15 日）17~18 頁 5.(1)ア(イ)（https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf））。
[4] 知財高判平成 18 年 12 月 26 日（平成 18 年（ネ）第 10003 号）最高裁ウェブサイトは、プログラムに著作物性があるといえるためには、「指令の表現自体、その指令の表現の組合せ、その表現順序からなるプログラムの全体に選択の幅が十分にあり、かつ、それがありふれた

る。このため、これらの不正目的ソフトウェアであっても、それを構成するプログラムについては著作権が発生し、著作権法上の保護が及ぶことになる。もちろん、マルウェアに感染等したソフトウェア、又はマルウェアの感染等から守られるべきソフトウェア（以下総称して、本項において「対象ソフトウェア」という。）についても、著作権法上のプログラムの著作物に該当するものは多いと考えられる。

したがって、プログラムの著作物に関するリバースエンジニアリングについては、たとえマルウェア対策等の目的の解析を行う場合であっても、権利者に許諾なく複製や一部を改変する行為が生じている以上は、平成 30 年の著作権法改正前までは、同改正前著作権法第 30 条の 4 や第 47 条の 3 等の権利制限規定に該当しない限り、複製権や翻案権の侵害となる可能性を否定できなかった。

（２）著作権法第 30 条の 4 について

社会におけるデジタル化・ネットワーク化の進展等に伴う著作物の利用環境の変化等に対応するべく、著作物等の公正な利用を図るとともに著作権等の適切な保護に資するため、平成 30 年に著作権法が改正[5]され、改正内容の一つとして、柔軟な権利制限規定が新設された。

このうち、同法第 30 条の 4 は、「著作物に表現された思想又は感情の享受を目的としない行為については、著作物の表現の価値を享受して自己の知的又は精神的欲求を満たすという効用を得ようとする者からの対価回収の機会を損なうものではなく、著作権法が保護しようとしている著作権者の利益を通常害するものではないと考えられるため、当該行為については原則として権利制限の対象とすることが正当化できる」[6]ことを趣旨として設けられたものである。

同条は、通常権利者の利益を害しないと考えられる行為類型に該当するものとして、著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合（以下、本項において「非享受目的」という。）には、その必要と認められる限度において利用できる旨を規定している。

同条にいう「『享受』とは、一般的には『精神的にすぐれたものや物質上の利益などを、受け入れ味わいたのしむこと』を意味することとされており、ある行為が本条に規定する『著作物に表現された思想又は感情』の『享受』を目的とする行為に該当するか否か」は、「立法趣旨及び『享受』の一般的な語義を踏まえ、著作物等」の利用を通じて、利用によ

表現ではなく、作成者の個性が表れているものであることを要する」としており、「プログラムの表現に選択の余地がないか、あるいは、選択の幅が著しく狭い場合には、作成者の個性の表れる余地もなくなり、著作物性を有しないことになる」と判示している。

[5] 著作権法の一部を改正する法律（平成 30 年法律第 30 号）による改正。同法は、一部を除き平成 31 年 1 月 1 日に施行された。

[6] 前掲注 2・6 頁参照。

る「知的又は精神的欲求を満たすという効用を得ることに向けられた行為であるか否か[7]という観点から判断」される[8]。

同条は、このような非享受目的の著作物利用を柱書において権利制限の対象[9]としつつ、同条各号において非享受目的として典型的に想定される場合を例示列挙している。

（3）プログラムの著作物の享受について

プログラムの著作物は、「表現と機能の複合的性格を有して」いることから、「プログラムの著作物に『表現された思想又は感情』とは、当該プログラムの機能を意味すると考えられるところ、その『表現された思想又は感情』の『享受』に該当するか否かは、当該プログラムを実行等することを通じて、その機能に関する効用を得ることに向けられた行為であるかという観点から判断されるものと考えられる。プログラムの著作物について対価回収の機会が保障されるべき利用は、プログラムの実行等を通じて、プログラムの機能に関する効用を得ることに向けられた利用行為であると考えられる」としている[10]。

したがって、プログラムの著作物に関しては、当該プログラムの実行等を通じて、プログラムの機能に関する効用を得ることを目的としていない場合は、非享受目的として著作権法第 30 条の 4 を適用することが同条の趣旨に合致すると考えられる。

（4）リバースエンジニアリングについて[11]

マルウェア対策やサイバーセキュリティ対策の目的で、いわゆるリバースエンジニアリングの一環として不正目的ソフトウェア又は対象ソフトウェアを解析に伴い複製する場合や、構造等を複製、改変して解析する場合は、不正目的ソフトウェア又は対象ソフトウェアの実行等を通じて、その機能を享受することに向けられた利用行為ではないと評価できる、すなわち、非享受目的による利用行為であるといえるため、著作権法第 30 条の 4 の規定に基づき、必要と認められる限度において方法を問わず不正目的ソフトウェア又は対象ソフトウェアを構成するプログラムの著作物を利用できることとなり、この場合には、著作権侵害の問題は生じないことになる。

---

7 前掲注 2・39 頁によれば、「本条では『享受』の目的がないことが要件とされているため、仮に主たる目的が『享受』のほかにあったとしても、同時に『享受』の目的もあるような場合には、本条の適用はないものと考えられる」とされている点については留意が必要である。

8 詳細は、前掲注 2・6 頁～8 頁を参照。なお、当該資料は、文化庁としての基本的な考え方が示されたものであり、司法判断を拘束するものではなく、「享受」の意味や個別具体的な事案における著作権法第 30 条の 4 の権利制限規定への該当性については、最終的には司法の場で判断されるものである点に留意が必要である。

9 なお、本権利制限規定は著作権を対象とするものであり、同一性保持権などの著作者人格権を対象としていない点については留意が必要である。

10 前掲注 2・39～42 頁。

11 前掲注 2・11 頁及び 37～42 頁参照。

その他具体的な利用方法として、以下のような行為が、非享受目的の利用に該当すると考えられている[12]。

① プログラムのオブジェクトコードをソースコードに変換するだけでなく、それをまたオブジェクトコードに変換し直す場合
② プログラムの解析を困難にする機能が組み込まれているマルウェアプログラムの当該機能部分を除去する場合
③ プログラムの解析の訓練・研修のために調査解析を行う場合
④ プログラムを実行しつつ調査解析する場合や調査解析中の当該プログラムがアセンブリ言語に変換された画面を資料化（紙媒体への印刷、PDF 化）する場合であって、そのプログラムの実行や資料化がその機能を享受することに向けられていない場合

実務的には、上記の行為がプログラムの機能の享受に向けられたことでないことを担保し、立証できるようにしておくことが望ましく、具体的な方策として、「例えば、調査解析専用のパソコンを用意してそれで実行したり、調査解析の過程や結果をレポートに記録したりする」[13]といったことが挙げられている。

（５）利用規約とリバースエンジニアリングの関係について[14]

通常、ソフトウェアを利用する場合には、利用規約等においてディスアセンブル、デバッグ、リバースエンジニアリング等の解析行為を禁止する条項が規定されているが、以下のように、このような条項は、独占禁止法上の違法性が私法上の効力に影響を与える可能性がある。また、著作権法上権利制限規定がある部分について利用制限を課す契約条項の効力については様々な考え方があり得るため留意が必要である。

ア　独占禁止法上違法となる契約条項

独占禁止法上違法となる契約条項については、民法第 90 条（公序良俗違反）に基づき、私法上の効力も無効となる場合があり、リバースエンジニアリングを禁止する条項は、市場における公正な競争を阻害するおそれがある場合においては、無効となる可能性がある[15]。

---

12 前掲注 2・11 頁。
13 前掲注 2・11 頁。
14 電子商取引準則 247 頁以下参照。
15 ソフトウェアと独占禁止法に関する研究会「ソフトウェアライセンス契約等に関する独占禁止法上の考え方」（平成 14 年 3 月 20 日）（http://warp.ndl.go.jp/info:ndljp/pid/247419/www.jftc.go.jp/pressrelease/02.march/020320.pdf）によれば、「プラットフォーム機能を持つソフトウェアのように，当該ソフトウェアとインターオペラビリティを持つソフトウェアやハードウェアを開発するために」「①当該ソフトウェアのインターフェース情報が必要であり、②ライセンサーがインターフェース情報を提供しておらず、③ライセンシーにとって、リバースエンジニアリングを行うことが、当該ソフトウェア向けにソフトウェアやハードウェアを開発するために必要不可欠な手段となっているような場合においては、リバー

イ　権利制限規定がある部分について利用制限を課すライセンス契約の条項

著作権法で保護されている著作物であっても、同法の規定により著作権が制限されている部分（著作権法第 30 条から第 49 条まで）が存在する。この部分は著作権法によって著作権者の許諾なく著作物の利用が認められている部分である。この著作権が制限されている部分について利用制限を課す契約条項の効力については、有効・無効様々な考え方があり得るため、留意する必要がある[16]。

なお、平成 30 年の著作権法改正以前の事案として、プログラムに関するリバースエンジニアリングの可否が争点となった裁判例が存在する（原審：大阪地判平成 21 年 10 月 15 日、控訴審：知財高判平成 22 年 4 月 27 日）。原審は、リバースエンジニアリングのみを理由として著作権侵害を主張し、損害賠償請求をすることは権利の濫用（民法第 1 条第 3 項）に当たり許されないとして原告の請求を棄却した。また、控訴審は、被告プログラムが原告プログラムの複製物又は翻案物であったとしても原告に財産的又は非財産的損害が発生したということはできないとして、被告による控訴を棄却している。上記（4）記載のとおり、リバースエンジニアリングが許容されることは著作権法の改正によって明確になったが、契約上リバースエンジニアリングが禁止されることは引き続き想定されるため、同判例は依然として先例としての価値があると考えられる。

3．参考資料（法令・ガイドラインなど）

・著作権法第 2 条第 1 項第 10 号の 2、第 10 条第 1 項第 9 号、第 30 条の 4
・文化庁著作権課「著作権法の一部を改正する法律（平成 30 年改正）について（解説）」
http://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_11.pdf
・文化庁著作権課「デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方（著作権法第 30 条の 4、第 47 条の 4 及び第 47 条の 5 関係）」（令和元年 10 月 24 日）

スエンジニアリングを禁止することは，ソフトウェアにノウハウが含まれる場合があり，また，仮に外形上又は形式的には著作権法上の権利の行使とみられる行為であるとしても，著作権法上の権利の行使と認められる行為とは評価されず，独占禁止法が適用されるものと考えられる。」「このような場合において，ライセンサーがライセンシーに対して，リバースエンジニアリングを行うことを禁止することは，このような制限が課されることにより，ソフトウェアの製品市場又は技術市場におけるライセンシーの研究開発活動が阻害されるなど，当該ソフトウェアで利用可能な他のソフトウェア若しくはハードウェアの製品市場又はシステムインテグレーターなどが提供する当該ソフトウェアに関連したサービス市場における公正な競争が阻害される場合には，不公正な取引方法に該当し，違法となると考えられる（一般指定第 13 項（※）〔拘束条件付取引〕に該当）。」とされている。（※）現行一般指定 12 項。

[16] 前掲注 15・250 頁参照。

https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_17.pdf

・電子商取引準則 247 頁以下

・ソフトウェアと独占禁止法に関する研究会「ソフトウェアライセンス契約等に関する独占禁止法上の考え方」（平成 14 年 3 月 20 日）
https://warp.ndl.go.jp/web/20070426101636/www.jftc.go.jp/pressrelease/02.march/020320.pdf

４．裁判例

本文中に記載のとおり

Q26 暗号の利用と情報管理等

暗号の利用は情報の管理を求める法令等に関してどのような役割を果たすか。また、関連する法制度としてどのようなものがあるか。

タグ：個情法、不正競争防止法、著作権法、電波法、電子署名法、暗号、CRYPTREC、危殆化、技術的制限手段、技術的利用制限手段、技術的保護手段

１．概要

暗号技術を利用することにより、情報の内容を第三者に秘匿することができる。このため、法律上情報の安全管理が求められている場合（個情法）や情報の秘匿を行っていることにより法的な保護を受けることができる場合（不正競争防止法、著作権法）には、暗号が利用される。また、暗号を応用した技術により電磁的記録の改ざんの検知や情報発信の否認を防止することができる。この技術を利用し、電磁的記録の作成の真正を技術的に担保することができる（電子署名法）。

暗号を利用するに当たっては、適切な強度の暗号を選択すること、復号するための鍵について適切に管理すること、危殆化が生じている暗号を利用しないことが必要である。

２．解説

（１）サイバーセキュリティと暗号[1]

暗号技術（暗号を応用した技術を含む。）を利用することにより、情報の内容を第三者に秘匿すること、情報の改ざんを発見すること、発信の否認を防止すること、正当な利用者のみアクセスさせることができる。そのため、保管データや通信の秘匿など情報の秘匿化、認証によるアクセスコントロール、改ざんの検知（電子署名）などにおいて広く利用されている。

暗号を生成するアルゴリズムには、基礎理論の違い、解析の容易性・困難性、利用の際のハードウェアへの負荷の程度の軽重などに応じて種々のものがある。そのため、一定の目的を達成するために暗号を利用する場合には、その利用方法と達成する目的を勘案した上で、適切な強度の暗号を選択し、利用するよう留意しなければならない。

また、一度暗号化された情報を再度意味内容が理解できるようにすることを復号というが、復号に当たっては、復号鍵が必要である。情報を暗号化したとしても、復号鍵が流出してしまうと、その流出した復号鍵を利用して第三者が復号することが可能になるな

[1] 暗号については、例えば「暗号とは一定の規則に従って文章・数などを他の表現に変えて、その規則を知らない人には元が何かは判らなくするためのものです。」（IPA「暗号技術 Q&A」（https://www.ipa.go.jp/archive/security/crypto/qa.html））などとされている。暗号に関する技術の解説についても同ページが参考となる。

ど、情報を暗号化した意味がなくなってしまう。そこで、復号鍵の適切な管理も重要であり、復号鍵の適切な管理のためには、管理手順を定めることが有用である。

さらに、暗号自体の問題として、暗号アルゴリズムが開発された時点では暗号理論上、十分な堅牢性を持っている場合であっても、計算速度の向上など日々の技術の進歩により、容易に破られるようになってしまう（暗号の危殆化）[2]。そこで、暗号の実装に当たっては、このように危殆化した暗号を排斥し、安全で信頼できる暗号を利用する必要があり、また、一度実装した暗号であっても時の経過により危殆化した場合には、新たな暗号アルゴリズムに置き換える、鍵長を長くするなどの対応が必要である。安全で信頼できる暗号アルゴリズムのリストとしては、CRYPTREC[3]の電子政府推奨暗号リスト[4]やISO/IEC18033 シリーズがある。なお、特に近年は、量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性が低下することが懸念されており、量子計算機への耐性を有する「耐量子計算機暗号（PQC）」への移行に向けた関心が国内外で高まっている。

以上のとおり、暗号を利用する場合には、その利用方法と達成する目的を勘案した上で、適切な強度の暗号を選択し、また、技術の進歩による暗号の危殆化についても情報を継続的に入手した上で、利用する暗号アルゴリズムを更新すること、復号鍵を適切に管理することが重要である[5]。

（２）暗号と法制度

暗号は、法制度との関係では、情報の秘匿性が実現できるという観点から、①一定の情報について法律上、セキュリティ義務が課せられている場合の利用、②一定の情報については、セキュリティ確保が法的保護を受けるための条件となっているところ、当該セキュ

---

[2] 平成 25 年 3 月時点の電子政府推奨暗号リストにおいては、共通鍵暗号について 64 ビットブロック暗号の 3-key Triple DES やストリーム暗号の 128 ビット RC4、ハッシュ関数について SHA1 などは、互換性維持以外の目的での利用が非推奨とされている。

[3] CRYPTREC は Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT 及び IPA が共同で運営する暗号技術評価委員会及び暗号技術活用委員会等で構成される。

[4] CRYPTREC は活動を通して電子政府で利用される暗号技術の評価を行っており、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」を策定している。そのリストの中で、安全性及び実装性能が確認され、市場における利用実績が十分であるか今後の普及が見込まれると判断されて利用を推奨する暗号技術のリストを「電子政府推奨暗号リスト」としてまとめている（https://www.cryptrec.go.jp/list.html）。当該「電子政府推奨暗号リスト」は、「現行暗号リスト」と、現行暗号の解読に利用可能な水準の量子計算機（CRQC: Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術からなる「耐量子計算機暗号（PQC）リスト」の 2 つから構成される。

[5] 暗号の評価、導入、管理について、NCO「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」（令和 8 年 6 月一部改訂）431 頁「7.1.5 暗号・電子署名」（https://www.cyber.go.jp/policy/group/general/kijun.html）が参考になる。

リティ確保のための利用がある。また、情報改ざん検知、発信の否認防止ができるという観点から、③一定の法制度の基礎技術としての利用がある。

ア　サイバーセキュリティに関する義務の履行としての利用

事業者に一定の情報についてセキュリティ義務を課している法律は多く、そのセキュリティ義務の履行の方法として暗号が利用される。

個人情報取扱事業者は、個人データに対して安全管理措置（個情法第 23 条）を講ずる必要があるが、個情法ガイドライン（通則編）においても、 安全管理措置のうち、技術的安全管理措置として、個人データを含む通信の経路又は内容を暗号化することが手法の例示の一つとして挙げられている[6]。同様に、行政機関の長等は、保有個人情報について安全管理措置を講ずる必要があり（個情法第 66 条第 1 項）、また、総務大臣等は、特定個人情報の提供システムについて秘密管理として適切な方法を取らなければならないが（番号利用法第 24 条）、これらの方法としても暗号化がその方法の一つとして利用される。

ただし、暗号化はあくまでも安全管理措置の一環として行われるものであり、個人情報（個情法第 2 条第 1 項）を暗号化しても、暗号化された情報は非個人情報となるわけでない[7]。

その他個情法との関係では、要配慮個人情報が含まれる個人データの漏えい等一部の類型の漏えい等事案（報告対象事態）が生じた場合、個人情報保護委員会への報告及び本人への通知が必要となる（個情法第 26 条、個情法施行規則第 7 条）ところ、漏えい等した個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合には、上記個人情報保護委員会への報告及び本人への通知を行う必要がないとされている[8]。

ここにいう「高度な暗号化等の秘匿化がされている場合」とは、漏えい等事案が生じた時点の技術水準に照らして、漏えい等した個人データについて、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されている場合をいう。そして、第三者に見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、電子政府推奨暗号リストや ISO/IEC18033 シリーズ等に掲載されている暗号技術が用いられ、それが適切に実装されていることをいい、また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離した上で、復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠

6 個情法ガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」参照。
7 個情法ガイドライン（通則編）2-1。
8 個情法施行規則第 7 条。

隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかを満たすことが必要である[9]。

イ　法的保護の前提としてのセキュリティ確保のための利用

事業者が一定の情報についてセキュリティ等を確保している場合、当該情報が法的に保護を受け得ることがあるが、その方法として暗号が利用される。

一定の情報が不正競争防止法における営業秘密（不正競争防止法第 2 条第 6 項）や限定提供データ（同法第 2 条第 7 項）に該当する場合、民事上、営業秘密の場合は刑事上の保護も受け得る[10]。この際、営業秘密や限定提供データと認められるためには、それぞれ秘密管理性や電磁的管理性などの要件を満たす必要があり、対象情報を暗号化し、特定の者のみがアクセスすることができるようにすることも、これらの要件を満たすための方法の一つである[11]。

また、技術的制限手段（同法第 2 条第 8 項）として暗号が利用されており、技術的制限手段を回避する装置やプログラム等を譲渡等することは不正競争に該当し得る（同法第 2 条第 1 項第 17 号、第 18 号）。

さらに、著作物についても、技術的利用制限手段（著作権法第 2 条第 1 項第 21 号）や技術的保護手段（同項第 20 号）に当たるものの一つとして暗号方式によるものが規定されている。技術的利用制限手段を回避する行為や、技術的保護手段の回避又は技術的制限手段を回避する装置やプログラム等を公衆に譲渡等する行為は、一定の場合を除き、これらの手段に係る著作権、出版権又は著作隣接権を侵害する行為とみなされる（同法第 113 条第 6 項、第 7 項）。また、私的使用のために複製する行為については著作権が制限されているが（同法第 30 条第 1 項本文）、その場合であっても、技術的保護手段によってコントロールされた著作物について、その技術的手段が回避されたことを知って複製を行う場合には、同規定の対象外とされている（同項第 2 号）[12]。

最後に、電波法（昭和 25 年法律第 131 号）は、暗号通信という概念を設定しており、無線通信が暗号化されている場合には、その内容を漏えいし、又は窃用する目的で、無線通信を復号する行為が罰則の対象となる（電波法第 109 条の 2 第 1 項、第 2 項）。

ウ　一定の法制度の基礎技術としての利用

電磁的記録に記録された情報について本人による電子署名が行われているときは、真正に成立したものと推定される（電子署名法第 3 条）。また、電子署名法上の電子署名に該当するためには、電磁的記録に記録することができる情報について行われる措置であ

[9] 個情法 QA 6-19。
[10] ただし、限定提供データについては、刑事上の保護は規定されていない。
[11] Q21、Q22 も参照されたい。
[12] Q23 も参照されたい。

って、①当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること、②当該情報について改変が行われていないかどうかを確認することができるものであることの二つの要件を満たす必要がある（同法第 2 条第 1 項）。また、電子署名法上の特定認証業務による電子署名の要件を技術的に満たす方法として、暗号を応用した技術が使われている（同法施行規則第 2 条各号）[13]。

3．参考資料（法令・ガイドラインなど）

・デジタル庁、総務省、経済産業省「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」(令和 5 年 3 月 30 日(最終更新:令和 8 年 3 月 30 日))
・個情法
・個情法施行規則
・番号利用法第 24 条
・不正競争防止法第 2 条第 1 項第 17 号、第 18 号、第 8 項
・著作権法第 2 条第 1 項第 20 号、第 21 号
・電波法第 109 条の 2
・電子署名法第 2 条、同法施行規則第 2 条
・NCO「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」

4．裁判例

特になし

[13] Q50 も参照されたい。

Q27 データの消去、データが記録された機器・電子媒体の廃棄

データを消去したり、データが記録された機器・電子媒体等を廃棄したりする場合に、どのような点に留意する必要があるか。

タグ：個情法、安全管理措置、秘密情報、消去、削除、廃棄、暗号化消去、秘密保持契約、ハードディスク

１．概要

データの消去や、データが記録された機器・電子媒体等の廃棄に際しては、データを完全に消去せずに機器・媒体を廃棄した場合、データが復元される危険もあるため、このような不完全な消去等によって個人データや他社の秘密情報等のデータが漏えいしないように十分留意する必要がある。消去等の作業を行うに当たっては、複数のガイドライン・資料が公表されており参考になる。また、外部の事業者にデータ消去を委託する場合は、適切な委託先を選定し、情報の漏えいに関して規定した契約を締結した上で情報が適正に抹消されたことを証明する資料の提出を求める、スタッフ等による立ち合いを行う等、委託先での履行状況を確認することが重要である。

２．解説

（１）総論

データを消去したり、データが記録された機器・電子媒体等を廃棄したりする場合（以下「データの消去等」という。）には、不完全なデータの消去等によって個人データや他社の秘密情報等のデータの漏えいが生じないように十分留意する必要がある。

個人データについては、個情法第 23 条に基づき安全管理措置義務を講じる必要があり、具体的な安全管理措置の内容及びその実践手法の例については個情法ガイドライン（通則編）の「10（別添）講ずべき安全管理措置の内容」に定められている。そのうち、安全管理措置の一環としての物理的安全管理措置としては、個人データを消去等する場合は、復元不可能な手段で行わなければならないこと、また、個人データを消去等した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要であるとされている。同ガイドラインでは、より具体的な措置の手法の例として、個人データが記載された書類等を廃棄する際に、焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用すること、個人データの消去等に際して、情報システム（PC 等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用すること、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用することが挙げられている。

他社の秘密情報については、まず秘密保持契約の有無を確認し、そのような契約がある場合には、契約上の義務に十分留意する必要がある。例えば、秘密保持契約に、データの消去義務や返却義務が規定されているケースが多く、消去の方法の指定や、消去したことの証明を提出しなければならないこと等が規定されているケースもある。このような条項がない場合であっても、データの消去等に際して、不完全なデータの消去等によって他社の秘密情報を漏えいさせた場合には、取引に関する契約に基づく責任や不法行為に基づく責任が生じる可能性があるため留意が必要である。

（２）データの消去等における留意点

データが記録されている機器・媒体を廃棄するに当たって、データを完全に消去せずに廃棄した場合、廃棄された機器・媒体からデータが復元され、情報が流出する危険がある。実際に、令和元年 11 月、神奈川県がリースを受けて使用していたハードディスクをリース会社に返却したところ、当該リース会社からデータ消去作業を受託した会社の従業員が、当該ハードディスクを消去の作業前に盗んでオークションサイトに出品し、全て落札され、県の内部情報ではないかという連絡を受けたことで事案が発覚したことがあった[1]。

データの消去に関しては、以下のような資料が参考になる。

ア NIST SP800-88

米国国立標準技術研究所（NIST[2]）が発表しているガイドラインである「NIST Special Publication 800-88 Revision 1」[3]は、記録媒体のサニタイズ（消去や破壊）に関する内容をまとめたもので、消去や破壊を行う機器やソフトウェアにて処理方法の基準となっており、主に大容量のハードディスクをソフトウェア消去（上書き方式）する場合の標準方式として参照されている。

同ガイドラインの改訂版である「NIST Special Publication 800-88 Revision 2」[4]が、2025 年 9 月に公開されている。Revision 2 への改訂では、情報の機密性に応じた消去方法のフローに大幅な変更はないが、デバイス毎の消去方法に関しては IEEE 2883（電子機器のデータ消去に関する国際標準規格）を参照する構成への変更、暗号化消去に関する留意事項の追加等が行われた。

---

[1] 本件では、当該従業員につき刑事事件となり、令和 2 年 6 月 9 日、東京地裁において懲役 2 年執行猶予 5 年の刑が言い渡されている。
[2] National Institute of Standards and Technology
[3] IPA が翻訳版を公表している。下記リンクを参照。なお、SP800 シリーズについては Q9 を参照（https://www.ipa.go.jp/security/crypto/gmcbt80000005u4j-att/SP800-88rev1.pdf）。
[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf

イ　地方公共団体における情報セキュリティポリシーに関するガイドライン

総務省が公表した「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 8 年 3 月版）」[5]は、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものとなっている。同ガイドラインでは、「情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。」という記載がある。また、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行う際の「機器の廃棄等の方法」及び「確実な履行を担保する方法」を整理している。

ウ　政府機関等統一基準群

政府機関等統一基準群の一つである NCO「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」[6]では、「『ファイル削除』の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。」として、電磁的記録媒体に記録されている情報を抹消するための方法を次のように列挙している。

- データ抹消ソフトウェア（もとのデータに異なるランダムなデータを 1 回以上上書きすることでデータを抹消するソフトウェア[7]）によりファイルを抹消する方法
- 暗号化消去を行う方法
- ATA コマンドの「Enhanced SECURITY ERASE UNIT」コマンドを使用する方法
- SCSI コマンドの「SCSISANITIZE」コマンドや「SCSIFormat」コマンドを使用する方法
- NVMe（PCIe）コマンドの「NVMExpressFormat」コマンドや「NVMExpressSANITIZE」コマンドを使用する方法
- ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
- 媒体を物理的に破壊する方法

---

[5] 平成 13 年 3 月 30 日策定・令和 8 年 3 月 27 日最終改定（https://www.soumu.go.jp/main_content/001064404.pdf）

[6] https://www.cyber.go.jp/policy/group/general/kijun.html

[7] ソリッドステートドライブ（SSD）や USB 等のフラッシュメモリタイプの電磁的記録媒体は、その構造上、データ抹消ソフトウェアによる上書きが 1 回のみの場合には消去すべき情報が残っている可能性があるため、2 回以上の上書きを行うソフトウェアを用いる必要がある。

上記のうち、「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法と定義されており、暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などが挙げられている。暗号化消去は、同ガイドラインの令和 3 年改正時に新たに加わったものであり、この方法による消去も積極的に検討されるべきである。

なお、前掲のハードディスクが盗まれオークションサイトに流出した事例では、ハードディスクのデータの消去に関して委託を受けた業者の従業員が一連の行為を行っている。企業のスタッフ自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を企業内で実施することや情報の抹消を外部の事業者等へ業務委託することは合理的であるが、外部事業者にデータの消去を委託する場合には、適切な事業者を選定し、情報の漏えいに関して規定した契約を締結した上で、情報が適正に抹消されたことを証明する資料の提出を求める、スタッフ等による立ち合いを行う等、委託先での履行状況を確認することが重要である[8]。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

本文中に記載のとおり

[8] 本事例を踏まえて、令和 2 年 5 月 22 日、総務省自治行政局地域情報政策室長から自治体の情報セキュリティ担当部長宛に、「情報システム機器の廃棄等時におけるセキュリティの確保について」（総行情第 77 号）が出されている。なお、民間企業向けには、一般社団法人電子情報技術産業協会（JEITA）が、「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項（2018 年 10 月改訂）」を公表している。
https://home.jeita.or.jp/page_file/20181025154114_OcyNEMuIAs.pdf

Q28 セキュリティ上必要となる雇用関係上の措置と誓約書の取得

企業は、従業員がサイバーセキュリティ上の事故を発生させる事態を未然に防止し、また、こうした事態が発生した場合に適切な対応をとるために、雇用関係上どのような措置を講じておくべきか。

タグ：労働基準法、労働組合法、労働契約法、民法、個情法、不正競争防止法、従業員、就業規則、誓約書、秘密保持義務、懲戒処分

１．概要

サイバーセキュリティの観点から遵守すべき事項について、明確な服務規律の定めを設けて周知徹底を図ることが望ましい。重要になるのが、就業規則上の規定の整備である。特に、企業が従業員に対して懲戒処分を行うに当たっては、あらかじめ就業規則上の懲戒の種別及び事由を定めておくことなどが必要となる。

また、従業員が在職中及び退職後に負う秘密保持義務を明確化することや、サイバーセキュリティに関する法令上の義務を履行するため、情報資産の守秘に関する誓約書を従業員から取得することも必要となる。誓約書の対象となる情報の範囲は具体的に特定するべきであり、誓約書の取得時期は、プロジェクトへの参加時など、具体的に企業秘密に接する時期がより適切であるといえる。

２．解説

（１）就業規則上の規定の整備

ア　考え方

企業が従業員との関係でサイバーセキュリティ体制を確立する上では、サイバーセキュリティをめぐる企業と従業員との関係を明確にしておくことが重要である。このような体制の構築は、労働法制に適合した形で行われる必要があるが、その際、特に就業規則を適切な形で作成することが重要になる。

イ　従業員との関係において構築すべきサイバーセキュリティ体制

企業がサイバーセキュリティを確保する観点から、従業員との関係において講じておくべき措置としては、まず、従業員が職務遂行に当たってサイバーセキュリティの観点から遵守すべき事項を、従業員の服務上の義務（服務規律）としてあらかじめ定めておくことが挙げられる。こうした事項の遵守は、個別の業務命令等によってもある程度対応は可能であるが、サイバーセキュリティ体制を確立するという観点からは、明確な服務規律の定めを設けて周知徹底を図ることが望ましい。

また、こうした服務上の義務の履行を確実なものとするためには、従業員が義務に違反し、サイバーセキュリティ上の問題を生じさせた（あるいはそのおそれがある）場合には事実関係を確認し、違反の事実が確認された場合には迅速に是正するとともに、必要に応じて従業員に対して懲戒処分等の制裁を課すことが可能な体制を整えておくことが重要である。こうした観点からも、事実関係の調査や懲戒処分との関係で、あらかじめ関連する規定を整備しておくことが必要になる。

以上のようなサイバーセキュリティ体制の構築に当たって、特に重要になるのが、就業規則上の規定の整備である。

ウ　サイバーセキュリティとの関係での就業規則の意義及び運用上の留意点

（ア）就業規則の意義

適法に作成、運用される就業規則には、サイバーセキュリティの観点からは、次に挙げるような意義が認められる。

第 1 に、就業規則には、①その内容が合理的であることと、②従業員に対して周知させる手続が取られていることを要件として、当該就業規則の適用を受ける労働者の労働契約内容を定める効力が認められる（労働契約法第 7 条）。

なお、上記の 2 要件のうち②周知については、問題となる従業員（労働者）が所属する事業場において周知がなされている必要がある。また、この場面での周知は労働基準法第 106 条に基づく就業規則等の周知義務[1]と異なり、従業員が就業規則の内容を知り得る状態にあれば、その方法は問われないというのが通説的理解であるが、同条による周知義務が課せられている以上、企業としては同条所定の方法による周知を行うべきである。

したがって、企業がサイバーセキュリティの観点から、在職中の秘密保持義務など、従業員が遵守すべき事項を就業規則に定めてこれを従業員に周知させた場合、その内容がサイバーセキュリティ確保の手段として合理的なものである限り、これを遵守すべき従業員の義務の存在が認められ、従業員に遵守を求める使用者の対応は法的根拠を伴ったものとなる（ただし、秘密保持義務については、下記（2）、退職後の秘密保持義務については、Q33 も参照されたい。）。

第 2 に、判例[2]によれば、企業が従業員に対して懲戒処分を行うためには、就業規則上の懲戒の種別及び事由を定めておくことが必要である。したがって、サイバーセキュリティ上の問題を生じさせた従業員に対し、制裁として懲戒処分を課すに当たっては、あらかじめ就業規則上の根拠規定の整備が不可欠となる。ただし、実際に懲

[1] ①常時各作業場の見やすい場所へ掲示する、又は備え付ける、②書面で労働者に交付する、③磁気テープ、磁気ディスクその他これらに準ずる物に記録し、かつ、各作業場に労働者が当該記録の内容を常時確認できる機器を設置する、のいずれかの方法により周知する必要がある。

[2] 最判平成 15 年 10 月 10 日労判 861 号 5 頁。

戒処分を行うに当たっては、就業規則所定の懲戒処分事由への該当性、懲戒権濫用の有無などが問題になる。

さらに、サイバーセキュリティに関する規程は、①基本方針（ポリシー）、②対策基準（スタンダード）、③実施手順（プロシージャー）の 3 階層構造で体系的に整備されることが一般的であるとされている[3]が、サイバーセキュリティに関する規程のうち、どの範囲を就業規則上遵守すべきものとするかについて、検討が必要となる。すなわち、サイバーセキュリティに関する規程は柔軟に変更していく必要性があるが、就業規則の対象とした場合には不利益変更などの問題（労働契約法第 9 条）が生じてしまうことからすると、上記③のうち従業員に対して遵守を求める事項のみを対象とするなど、対象範囲が適切となるような検討が必要である。

一方で、あらかじめ就業規則上明確に規定しておくべき場合として、例えば、サイバーセキュリティインシデントが発生した場合における調査協力義務が挙げられる。企業が行う従業員による企業秩序違反行為の調査について他の従業員の協力義務が問題となった判例は、従業員の調査協力義務を肯定しつつも、それが「労働者の職務遂行にとって必要かつ合理的なものでなくてはならない」としている[4]。

そこで、サイバーセキュリティインシデントが発生した場合、当該インシデントを解明するのに必要かつ合理的な範囲での調査に関して、従業員はこれに協力する義務を負うと考えられるが、インシデント発生の場合に調査があり得る旨をあらかじめ就業規則において明確にしておくことが望ましいと考えられる。

（イ）就業規則に基づく処分

従業員が在職中に発生させるサイバーセキュリティインシデントのうち、これまでの裁判例において最も多く問題にされてきたのは、営業上の秘密の漏えい行為等である。企業の従業員（労働者）は、労働契約に付随する義務として、その在職中、秘密保持義務を負っていると解されていることから、こうした漏えい行為等は原則として当該義務の違反となる。

こうした場合、企業は、当該行為を行った従業員に対し、解雇、懲戒処分、損害賠償請求等を行い得る。ただし、解雇及び懲戒処分については、それぞれの労働契約法上の枠組みに依拠して具体的な効力が判断されることになる（懲戒解雇の場合には双方の枠組みに沿った判断がなされる。）。

すなわち、解雇については、解雇権濫用（労働契約法第 16 条）が主要な問題となり、従業員の行為態様、問題となった行為の重大性等に照らして解雇の効力が判断される。懲戒処分については、あらかじめ就業規則に設けられた根拠規定に基づいて処

[3] IPA ウェブサイト「情報セキュリティマネジメントと PDCA サイクル」参照（https://warp.ndl.go.jp/info:ndljp/pid/11334363/www.ipa.go.jp/security/manager/protect/pdca/policy.html）。
[4] 最判昭和 52 年 12 月 13 日民集 31 巻 7 号 1037 頁。

分を行うことが必要であるほか、権利濫用の成否が問題となり（労働契約法第 15 条）、処分の根拠とされた行為の重大性に比して重すぎる処分でないか、他の同種事案に対する扱いと均衡を失していないか、等の点が問題になる。

このほか、従業員の営業上の秘密の漏えい行為等によって企業に損害が生じた場合、労働契約上の債務不履行若しくは不法行為に基づく損害賠償請求の対象となることもある。

裁判例における具体的な判断としては、退職直前の従業員自らが関与した設計書類、設計計算書等を自宅に持ち出した行為について、当該書類記載の情報を利用して退職後に競業行為に及ぶ意図が推認できるなどとして懲戒解雇を有効とし、退職金を支給しないことも適法であるとした例（大阪地判平成 13 年 3 月 23 日労経速 1768 号 20 頁）、新商品に関するデータ漏えい行為について、懲戒解雇に相当するものと認め、退職金を支給しないことも適法であるとしたほか、データ保存費用等、当該商品の開発・情報管理のために企業が支出した費用の一部に相当する額の損害賠償請求を認めた例（東京地判平成 14 年 12 月 20 日労判 845 号 44 頁）などがある。

一方、従業員に対する制裁が認められなかった例としては、従業員が、会社との間の雇用関係上の紛争に関連する資料として弁護士に会社の顧客情報を渡した行為について、当該情報を渡した経緯や相手方を考慮すると守秘義務違反に該当するとはいえないなどとして、懲戒解雇を無効とした例（東京地判平成 15 年 9 月 17 日労判 858 号 57 頁）などが存在する。

また、裁判例上の事例は少数であるが、情報の改ざんや正確な情報の記録を怠ることについて、具体的行為態様に照らして労働契約上の義務違反が認められる場合もある。

具体例としては、農協職員による貸付金の担保に関する資料の改ざんを理由とした懲戒解雇を有効とした例（大阪地決平成 13 年 7 月 23 日労経速 1783 号 18 頁）、先物取引会社の従業員について、会社に対して自己の担当顧客の真実の氏名・住所等を告知する義務の存在を認め、当該告知を怠ったことによって生じた回収不能差損金相当額の損害賠償を認めた例（東京地判平成 11 年 11 月 30 日労判 782 号 51 頁）などが存在する。

（ウ）運用上の留意点

こうした就業規則規定の違反に対して現実に懲戒処分を行う場面としては、サイバーセキュリティ上のルール違反によりインシデントが発生した場合と、単にルール違反が生じている段階で処分を行う場合が考えられるが、このうち事前のインシデント予防策として懲戒処分を行う場合（後者の場合）、懲戒処分事由（ルール違反行為）の重大さの評価は、一般的にいえば具体的なインシデントが生じた場合に比して低いものとなる。

このため、適法・有効な懲戒処分を行うという観点（主として懲戒権濫用の成否が問題となる）からは、処分内容の選択や処分に至る過程において留意が必要となる。懲戒処分を課すことの可否や、どの程度重い処分までが許容されるかは、ルール違反がインシデントを惹起する蓋然性、想定されるインシデントの重大性、従業員の職種・地位（サイバーセキュリティに対して特に高い意識が求められるものかどうか）、平素におけるルールの周知・徹底のあり方、過去における同種事案への対応事例など、当該事案における様々な事情に左右される。実務上の指針となる公刊裁判例は必ずしも多くないが、基本的には、発見されたルール違反に対し、懲戒処分事由に該当する行為である点を指摘しつつ注意を与えて是正を促した上で、なお従業員の態度が改まらずに違反が繰り返される場合に、比較的軽い処分を行うことは許容され得るものと考えておくべきであろう。

また、インシデントが発生した場合であっても、そうでない場合であっても、従業員に対し、顛末書ないし始末書を求める場合があり得る。

その内容が事実関係の報告や状況説明に過ぎないものであれば、状況説明としての具体的内容として、反省点を列挙させたり、今後気をつけていくべきことや心構え等について書かれた顛末書を提出させることは、業務命令権の範囲内の行為として命じることができると考えられる[5]。

これに対して、顛末書等による事実確認を経た上で、その内容に「謝罪の言葉を述べること」が含まれる文書の提出を求める場合には、懲戒の一類型としての始末書の提出（譴責処分）となると考えられるため、これを義務付ける就業規則上の規定が必要と考えられる[6]。

なお、「謝罪の言葉を述べること」を求める、すなわち、「謝らせる」という行為は、従業員の良心、思想、信条等と微妙にかかわる内的意思の表明を求めるものであると考えられることから、反省を強要することにもなり、個人の良心・内面の自由の観点から問題となる可能性がある[7]。

さらに、従業員によるインシデントを防止するため、教育訓練を実施することがあり得る。教育を実施する権利は、労働契約から派生し、特に長期雇用システムにおいては幅広い教育訓練の実施の権限が企業にはあると考えられる。しかし、内容が業務遂行と関係がなく、過度の苦痛を伴うなど不適切な制裁を含むような場合などは、権

[5] 事実関係の報告を目的とした始末書（顛末書）の提出が労務指揮権の範囲内と認められるとする見解として、石嵜信憲ほか「懲戒処分の基本と実務」（中央経済社、令和元年）16 頁。
[6] 前掲注 5・16 頁は、「事実関係をきちんと確認し、それが譴責処分に該当すると判断されれば、そのとき初めて懲戒として始末書の提出を命じる」べきであるとする。
[7] 例えば、水町勇一郎「詳解　労働法　第 3 版」（東京大学出版会、令和 5 年 9 月）601～602 頁は、「事実関係の報告にとどまらず、本人の謝罪・反省の意思の表明を命令するものについては、労働者本人の自由意思に委ねるべきものであるから、その不提出・不記載を理由にさらに懲戒処分を科すことはできないと解すべき」とする。

利濫用となる。セキュリティ啓発教育に関しても、この点の問題が生じていない限り、命令することは、可能である。

（２）守秘に関する誓約書の取得

ア　誓約書を取得する意義

（ア）在職中、退職後の秘密保持義務の明確化

労働契約は、賃貸借契約等と同様に継続的性格を有することから労使双方の信頼関係が重視される。そのため、労使はともに相手方の利益を不当に侵害しないことが求められる（労働契約法第 3 条第 4 項、民法第 1 条第 2 項）。

このことから、従業員は、仮に労働契約において特別に定めがなくても、企業秘密を保持する義務を負うと考えられている。しかし、責任の範囲などが必ずしも明確とはいえないことから、契約上の特約又は就業規則上の条項によって秘密保持を定めておくことが有効であると考えられている。もっとも、就業規則に秘密保持に関する規定があっても、抽象的な規定に留まらざるを得ないため、どの程度の義務を負うかが明確でないという点が問題となりうる。そこで、義務の内容を具体化する観点からも、誓約書を取得することには意味がある。従業員としても自らの負う秘密保持義務の内容を明確に知ることになるため、予測可能性が高まり、注意喚起的な効果も認めることができる。

加えて、退職後には、営業秘密としての保護がある場合など、法律上の保護がある場合を除き、原則として在職中負っていた労働契約の信義則上の秘密保持義務が退職により消滅すると考えられるので、退職後も秘密保持義務を課す誓約書を取得しておくことが望ましい（退職後の秘密保持義務については Q33 を参照されたい。）。

（イ）サイバーセキュリティの確保

守秘の対象となる情報資産が個人情報の含まれるデータベースであった場合、個人情報取扱事業者となる使用者側は、従業員が当該データベースを取り扱うにあたり、必要かつ適切な管理措置を行わなければならない（個情法第 24 条）。

また、例えば情報資産が技術情報であり、当該情報資産が、営業秘密として保護を受ける必要があるのであれば、当該情報資産を秘密として管理する必要がある（秘密管理性・不正競争防止法第 2 条第 6 項）。さらに、契約上も機密情報とされる情報の適切な管理が求められることがある。

こうしたサイバーセキュリティ関連法令の義務を履行するための方法の一つとして、従業員との間で秘密保持契約を締結し、又は誓約書を取得する方法が考えられる。

イ　誓約書を取得する際に考慮すべき事項

誓約書を取得する際に考慮すべきなのは、法令上要求されている情報資産の管理という目的の達成と、従業員に課される義務とのバランスをとることである[8]。

（ア）誓約書の対象情報

誓約書の対象となる情報については、情報資産の管理という観点から決定されるべきであるが、特に営業秘密として保護をする場合には対象を具体的に特定することが必要である[9]。また、従業員の予測可能性を高めるという観点からもできるだけ特定し具体化することが望ましいといえる。もっとも、守秘すべき必要性が乏しい情報を含めて広く誓約書を取得することは、後に誓約書の内容が争いになった場合、誓約書の有効性が否定されるおそれがあるため、望ましいとはいえない。例えば、従業員本人が当該職種における一般的な仕事の中で自然に身につけることができるスキルのような情報に制約を課すことができないとした裁判例[10]がある。

（イ）誓約書を取得する時期

誓約書を取得するタイミングとして、従業員の退職時、あるいは退職後に誓約書を取得することも考えられないわけではない。しかし、退職時あるいは退職後には従業員がこれに応じないことも少なくないと考えられる。また、入社時に徴収した誓約書では、抽象的な内容とならざるを得ないため、その有効性には限界がある（このような問題は、後から誓約書が有効か否かをめぐって争いになる。）。そこで、義務を具体化するといった観点から、企業秘密に接する段階において守秘すべき情報を特定した上でかかる情報に関する守秘について合意する旨の誓約書を当該従業員から取得することなどが考えられよう。なお、従業員の退職後に競業避止義務、秘密保持義務を課す場合の留意点については、Q33、Q34 を参照されたい。

ウ　従業員が誓約書への署名に応じない場合の措置

誓約書への署名については労働契約上使用者が有する業務命令権が及ぶとは考えられないため、業務命令の対象とすることはできない。したがって、従業員が署名を拒否したことを業務命令違反として懲戒処分を行うことはできない。また、誓約書に署名しないという行為が、企業秩序を侵しているとまでいえないため、この観点からも懲戒処分はできない。もっとも、誓約書を提出しない従業員をプロジェクトに参加させないことは、人事権の行使の範囲内にあたる限り認められる。誓約書を提出しない従業員に対しては、このような人事権の行使で対処することになろう。

---

[8] 秘密保持誓約書の例として、秘密情報保護ハンドブック 187 頁以下に誓約書例が記載されている。
[9] この点については、Q21 も参照されたい。
[10] 奈良地判昭和 45 年 10 月 23 日判時 624 号 78 頁。

エ　誓約書に違反した場合の懲戒処分の可否

誓約書に違反したからといって、常に懲戒処分が有効とされるわけではないことに注意を要する。すなわち、上記（1）ウ（ア）で述べたとおり、懲戒処分を科すためには、就業規則に列挙された懲戒事由に該当し、かつ、懲戒権濫用（労働契約法第 15 条）に該当しないことが必要である。

3．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

4．裁判例

本文中に記載したもののほか、

・奈良地判昭和 45 年 10 月 23 日判時 624 号 78 頁

退職後の競業禁止は、労働者の職業選択の自由や競争を不当に制限し得るため、合理的必要性の立証がない限り公序良俗に反し無効となるが、顧客情報や製法などの営業上・技術上の秘密は使用者の保護法益であり、当該秘密にアクセスする者に対し、秘密保持を実効化する範囲で一定期間の競業避止を課すことは有効となり得るとして、会社の技術的秘密を知る被用者の退職後における競業行為を禁止する旨の特約を有効と認めた事例。

・大阪高判昭和 53 年 10 月 27 日労判 314 号 65 頁

誓約書の内容に妥当性を欠くものが含まれており、また誓約書の提出の強制は個人の良心の自由に関わる問題を含んでいるから、誓約書を提出しないこと自体を企業秩序を乱す行為としたり、特に悪い情状とみたりすることは相当ではないとして、誓約書の不提出を理由とする諭旨解雇が懲戒権の濫用とされた事例。

・東京地判平成 15 年 10 月 17 日労経速 1861 号 14 頁

元従業員が労働契約上の競業避止義務及び退職時の契約に反し、会社を設立して競合する業務を行なっているとして損害賠償請求を行ったが、元従業員の行為は、自由競争社会において当然容認される経済活動の範囲を逸脱するものとはいえないとして、不法行為責任を問うことはできないとした事例。

・東京高判平成 29 年 3 月 21 日判タ 1443 号 80 頁

情報システムの開発等の業務に従事し、その顧客情報にアクセスする権限を付与されていた者が、その顧客情報を領得し、その一部を名簿業者に開示したという不正競争防止法違反の事案において、情報セキュリティ研修の実施状況や上記システムの内容等の事実関係の下では、本件顧客情報が会社の事業活動に活用される営業戦略上重要な情報であって機密にしなければならない情報であることを容易に認識することができたといえ、一定のアクセス制限の措置が取られていたことを併せ考えると、不正競争

防止法２条６項にいう「営業秘密」の要件である秘密管理性は満たされていたということができるとした事例。

Q29 従業員のモニタリングに関する留意点

企業が従業員に提供する業務用の PC やスマートフォン等の端末について、従業員による個人データや営業秘密の流出・漏えいの未然防止、早期発見のために、企業が、従業員の電子メールのモニタリングや端末画面のスクリーンショット等、又は GPS を用いて従業員の位置を管理すること等について、法律上問題点になる点、留意すべき点は何か。また、従業員の私物である PC やスマートフォン等の端末の場合はどうか。

タグ：民法、個情法、モニタリング、GPS、プライバシー権

１．概要

企業が従業員に提供する PC やスマートフォン端末は、従業員の私的な通信など、私的な目的でも利用されることが少なくない実態があるため、企業が行う電子メール等のモニタリングは、従業員に対するプライバシー侵害の問題や個情法への抵触を生じさせる可能性がある。

そこで、企業としては、業務用の PC やスマートフォン端末の利用に関する規程を設け、その中で、私的利用についてのルールを明確化するとともに、個人情報保護法制に適合的な形でモニタリングについて規定し、従業員への周知徹底を図るべきである。その上で、モニタリングを行う際には、モニタリングを必要とする個別具体的な事情も考慮しつつ、社会的に相当な範囲を逸脱する監視と評価されることがないよう注意を払うべきである。

近年は、EDR（Endpoint Detection and Response）や SOC（Security Operation Center）を活用する例も増えているが、これらを活用する場合にも、プライバシー侵害や個情法への抵触が問題となり得るため、電子メール等のモニタリングと同様若しくはそれ以上に注意を払う必要がある。

なお、企業が、従業員の私用メール等や、業務用 PC やスマートフォン端末の私的利用を禁止することには、服務規律上の根拠が認められるが、一方で過度に渡らない私用メール等が許容されるべきことは社会通念として一定の定着をみていると考えられるため、そのことへの配慮が必要となる。

さらに、近年、従業員が私物の PC やスマートフォン端末を業務に利用する事例も増えてきている。かかる私物端末について端末管理ソフト等を導入する場合には、事前に、個別の同意書面を取得する必要がある。

２．解説

（１）PC やスマートフォン端末等のモニタリングをめぐる問題点

一般に、内部不正の早期発見及び事後対策の観点から、ログや証跡を記録して保存することはこの重要性は高いと考えられ、また、そうしてログ・証跡の保存を行っている事実を従業員に通知することは、内部不正の発生を抑止する上で効果的な方法とされている[1]。一方で、企業が従業員の利用する PC やスマートフォン端末等をモニタリングすることには、次に挙げるように、従業員に対するプライバシー侵害と、個情法の観点から、法的な問題が生じ得る。

ア　プライバシーに関する問題点と裁判例の状況

まず、企業が PC やスマートフォン端末等のモニタリングを通じて、私的利用に伴う従業員の私的な情報を知ることは、従業員のプライバシーを侵害する違法な行為とされる可能性がある。この点についての代表的な裁判例（東京地判平成 13 年 12 月 3 日労判 826 号 76 頁、東京地判平成 14 年 2 月 26 日労判 825 号 50 頁、東京地判平成 16 年 9 月 13 日労判 882 号 50 頁など）において示された考え方は、概ね次のようなものである。

① まず、電子メール等の私的利用について、これを禁止する服務規律上の定めが存在しないか、存在しても、その実効性確保に向けた取組が十分でない場合、社会通念に照らして過度にわたらない私的利用が許容されているものと解される。

② このように、電子メール等の私的利用が一定範囲で許容されている場合、私的利用に伴う従業員の私的情報はプライバシーによる保護の対象となり得る。ただし、このような場合にも、企業が行うモニタリングが直ちにプライバシー侵害として違法になるわけではない（裁判例の中には、このことに関連して、電子メール等の私的利用の場合には使用者が管理する領域（サーバ上のファイル等）に情報が残ることなどから、私用電話のようなケースに比べるとプライバシーによる保護の程度は弱いものとなる旨を述べるものもある。前掲・東京地判平成 13 年 12 月 3 日）。

③ 具体的にプライバシー侵害が成立するかどうかの判断は、モニタリングの目的が企業運営上必要かつ合理的なものか、その手段・態様は相当か、従業員の人格や自由に対する行き過ぎた支配や拘束にならないか、従業員の側に監視を受けることも止むを得ないような具体的事情が存在するか、等の要素を総合的に考慮し、モニタリング行為が社会通念上相当として許容される範囲を逸脱するかどうかを判断するという枠組みの下で行われ、これが肯定される場合にプライバシー侵害が成立する。

なお、このようなプライバシー侵害の問題は、基本的には被監視者とされた従業員に対して企業が不法行為（民法第 709 条、第 715 条）に基づく損害賠償責任を負うことに

[1] IPA「組織における内部不正防止ガイドライン」第 5 版、令和 4 年 4 月、（https://www.ipa.go.jp/security/guide/hjuojm0000005l0-att/ps6vr7000000jvcb.pdf）68~70 頁 4-5.原因究明と証拠確保　（18）情報システムにおけるログ・証跡の記録と保存。

なるかという問題であるが、プライバシー侵害の程度が重大である場合には、そのような違法性の強いモニタリング等の行為によって得られた情報は従業員に対する懲戒処分等の不利益を課す根拠となし得ないものとされる可能性もある（結論としては否定したが、このような処理の可能性を認めた例として、前掲・東京地判平成 16 年 9 月 13 日）。

また、GPS を用いた従業員の位置情報の監視に関する裁判例として、東京地判平成 24 年 5 月 31 日労判 1056 号 19 頁がある。同裁判例は、「GPS 衛星の電波を受信することによって携帯電話又はパソコン（親機）から、本件ナビシステムに接続した携帯電話（子機）の位置を常時確認することができる」機能を持つ、電話会社の提供する「本件ナビシステム」を用いた従業員の位置情報の監視の不法行為該当性が論点の一つとなった事案である。同裁判例は、「原告が労務提供が義務付けられる勤務時間帯及びその前後の時間帯において、被告が本件ナビシステムを使用して原告の勤務状況を確認することが違法であるということはできない。」としつつも、「反面、早朝、深夜、休日、退職後のように、従業員に労務提供義務がない時間帯、期間において本件ナビシステムを利用して原告の居場所確認をすることは、特段の必要性のない限り、許されない」とし、結論として、本件ナビシステムを用いた被告による原告の監視は不法行為を構成すると判断した。

イ　個情法上の問題点と関連する規定等

次に、個情法との関係では、企業が行う PC やスマートフォン端末等のモニタリングに対して同法の規制が及ぶ可能性がある。

すなわち、従業員による PC やスマートフォン端末等の利用に関する情報（メールの文面、アクセス履歴等）は、当該情報それ自体から、あるいは他の情報と容易に照合することにより、特定の個人を識別することができる場合には、同法第 2 条第 1 項にいう個人情報に該当する。そして、このような個人情報を企業が PC やスマートフォン端末等のモニタリングを通じて取得することは、従業員の個人情報の取得に該当する。このため企業がモニタリングを行う際には、個人情報の利用目的の特定及びその通知等（同法第 17 条第 1 項、第 21 条）、目的外利用の原則禁止（同法第 18 条）、不適正利用の禁止（同法第 19 条）、適正取得（同法第 20 条）、さらに、個人データ（同法第 16 条第 3 項）に該当する場合には、第三者提供規律（同法第 27 条)などの同法が定める事項を遵守しなければならない。

以上のほか、同法との関係では、個情法ガイドライン（通則編）及び個情法 QA の記載も、企業が PC やスマートフォン端末等のモニタリングを行う際に留意すべき点を検討する上で参考になる。

例えば、個情法 QA5-7 は、個人データの取扱いに関する従業者の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリングを実施する場合は、以下のようにすることが望ましいとしている。

① モニタリングの目的をあらかじめ特定した上で、社内規程等に定め、従業者に明示すること。
② モニタリングの実施に関する責任者及びその権限を定めること。
③ あらかじめモニタリングの実施に関するルールを策定し、その内容を運用者に徹底すること。
④ モニタリングがあらかじめ定めたルールに従って適正に行われているか、確認を行うこと。

また、個情法 QA5-7 は、モニタリングに関して、個人情報の取扱いに係る重要事項等を定めるときは、あらかじめ労働組合等に通知し必要に応じて協議を行うことが望ましく、また、その重要事項等を定めたときは、従業者に周知することが望ましいとしている。

（2）PC やスマートフォン端末等のモニタリングについて企業が講ずべき措置

以上のような裁判例・法令等の状況を前提とすると、企業は、PC やスマートフォン端末等のモニタリングを行う際には、従業員に対するプライバシー侵害等の法的リスクの回避・軽減を図るという観点から、以下のような措置を講ずべきである。

ア　モニタリングに関する規程の整備

まず、業務用の PC やスマートフォン端末の利用方法に関する規程を整備し、その中で、PC やスマートフォン端末等のモニタリングについての規定を置くべきである。このような規定を置き、それに従ってモニタリングを行うことは、モニタリング行為の手段・方法の相当性を肯定する要素となるなど、前述した、プライバシー侵害の成否についての判断において、侵害のリスクを回避・軽減することにつながる。また、個情法との関係では、このような規程の中でモニタリングによって収集した従業員の個人情報の利用目的を示すことで、利用目的の特定・通知等という同法上の要求事項を満たすことになる。

こうした規程は、事業場の全従業員を対象としたものであるときには、就業規則に記載することが労働基準法上要求される（労働基準法第 89 条第 10 号）。また、事業場の全従業員を対象としていない場合及び使用者に就業規則の作成義務がない場合（同法第 89 条参照。これらの場合、就業規則に記載する法律上の義務はない。）にも、対象となる事項がサイバーセキュリティ上の重要な事項であることからすると、社内規程に記載しておくことは望ましいといえる。作成した社内規程は、就業規則として作成したかどうかに関わらず、対象となる従業員に周知する必要がある（就業規則の周知については、同法第 106 条、労働契約法第 7 条、第 10 条参照。就業規則の形をとらない場合にも、上述した法的リスクの回避・軽減を実現するためには従業員への周知が不可欠である。）。

規程中でモニタリングに関する事項として規定しておくべき事項としては、次のようなものが挙げられる。

① モニタリング対象となる機器等の私的利用（私用メール等）に関するルール（私的利用の許容範囲等）
② モニタリングを実施する権限と責任の所在（権限・責任が帰属する職制・部署等）
③ モニタリングを実施する目的（収集情報の利用目的）
④ モニタリングの具体的実施方法（調査の対象となる媒体等及び調査の手法、事前予告の有無等の調査実施手続）

このほか、収集した情報の保存期間、収集情報の第三者提供を原則として行わないこと（個情法第 27 条参照）、モニタリングの適正を確保するための監査に関する事項などについての規定を置くことも考えられる。

いくつかの点に説明を補足すると、まず、私的利用の許容範囲等に関する定めは、これをどのように設定するかによって、モニタリングとの関係で保護の対象となる従業員のプライバシーの範囲に影響を及ぼす。この点について、理論上は、私的利用を一切禁止するとともに、電子メール等がモニタリングによる閲覧の対象となることを事前に明らかにしておけば、プライバシー侵害の問題は生じなくなるといえるが、このような取扱い（特に私的利用を一切禁止すること）が許容されるかについては検討を要する（下記「(3) PC やスマートフォン端末等の私的利用の禁止について」）を参照）。

次に、モニタリングの実施目的については、情報流出・漏えいの防止、電子メール等の業務目的外利用の防止等の、企業運営上の必要性・服務規律の観点から合理的なものであることを要する。

モニタリングの実施方法については、従業員のプライバシー侵害を生じさせないことへの留意が必要となる。基本的には、上述したモニタリングの目的を達成する上で合理的であり、かつ、従業員のプライバシーその他の人格的利益を必要以上に侵害しないよう配慮した内容を定めるべきであるが、次のイで述べるように、プライバシー侵害を生じさせないものとして許容されるモニタリング手法の範囲は、具体的状況に応じて変化し得るため、イで述べる内容を踏まえつつ、具体的な状況に応じた柔軟な対応の余地を残すような定め方とすることが望ましいといえよう。

イ　モニタリング実施時の留意点

次に、具体的にモニタリングを実施する際の留意点であるが、基本的には、上記アで述べた規程の整備がなされていることを前提として、当該規程の定めに沿う形で実施すべきものである。ただし、モニタリングがプライバシー侵害となるかどうかは、最終的には、個別具体的な事案に即して判断されることになるので、実施に際しては、実施の具体的必要性（情報流出等が現に発生しているか又はまさに発生しようとしている具体的なおそれ）の有無・内容、実施しようとする手法が従業員に及ぼす不利益の内容・程度等を個別に考慮して、許容限度を超えた従業員の権利・利益の侵害と評価されることのないよう留意することが必要である。

こうした具体的留意点は、個々の事案ごとに判断されるという性質上、一般的に記述することに限界があり、また、現時点の裁判例から得られる示唆も限られたものではあるが、概ね次のようなことがいえるであろう。

① 情報流出等の具体的なおそれが生じていない段階で行われるモニタリングは、「広く、浅く」を旨とすべきであり、特定従業員に対象を絞って集中的にモニタリングを行うのは、当該従業員から情報流出等が生じている具体的な疑いが生じた後とすべきと思われる。

② 事前にモニタリング等の実施について十分な予告を行わない抜き打ち的な検査や、（使用者が管理するサーバ等ではなく）従業員が日常的に使用する端末等、従業員が通常管理する領域を対象として行う検査は、それを必要とする（より穏当な手段ではモニタリングの目的を達成することができない。）事情が具体的に存在していることが必要と思われる。

ウ EDR・SOC を活用する場合の留意点

近年、セキュリティ強化を目的として、EDR（Endpoint Detection and Response）や SOC（Security Operation Center）を活用する企業が増加している。

EDR とは、組織内のネットワークに接続されている PC やスマートフォン端末等（＝エンドポイント）における操作や通信内容等のログデータを収集・解析し、不審な挙動やサイバー攻撃を検知した場合に、管理者に通知するセキュリティ・ソリューションである。EDR を導入した場合においては、電子メールに関するデータのみならず、エンドポイント端末に係る様々な情報を収集・解析することになるため、従業員のプライバシー侵害を生じさせないことへの留意がより一層重要となる。また、EDR において収集するデータは、それ自体だけでは特定の個人を識別することが出来なくとも、導入企業においては、通常、「他の情報と容易に照合することができ、それにより特定の個人を識別することができ」、それゆえ個人情報に該当する（個情法第 2 条第 1 項第 1 号）と考えられる。したがって、EDR を導入する際には、上記（1）イで述べたような個情法上の義務を遵守することも必要となる。

特に、グローバル展開している企業に関しては、日本に所在する子会社のエンドポイント端末を外国の親会社が監視する場合等には、個人データの越境移転規制（同法第 28 条）が問題となり得る[2]。逆に、日本に本社が所在しており、外国子会社のエンドポイン

[2] なお、個人データの提供先が、「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国」（例えば、EU 加盟国）に所在する場合や、「個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している」場合は、個情法第 28 条第 1 項の規定は適用されないが、その場合であっても、同法第 27 条の第三者提供制限の規律は適用されるため、留意する必要がある。

ト端末を一括して監視する場合等には、外国支社に適用される各国の個人情報保護法令上問題がないかどうか（越境移転規制など）が問題となり得る。

SOC とは、24 時間 365 日体制で企業のネットワークや端末を監視し、サイバー攻撃の検出や分析等を行う組織であり、企業が SOC サービス・プロバイダに対してネットワーク等の監視を委託するケースが多い。SOC による監視においても、EDR と同様、様々なデータが収集されるため、やはり従業員のプライバシー侵害を生じさせないことへの留意が必要である。また、SOC により収集されるデータも、EDR により収集されるデータと同様、通常は容易照合性を満たし個人情報に該当すると考えられる。そのため、委託者である企業は、受託者である SOC サービス・プロバイダを監督する義務を負い（同法第 25 条）、また、SOC サービス・プロバイダが外国事業者である場合には個人データの越境移転規制（同法 28 条）が問題となり得る点に留意する必要がある。他方、受託者である SOC サービス・プロバイダにとっては、収集したデータが個人情報に該当しない場合も少なくないと考えられるものの、個人情報に該当する可能性がある情報を含めて収集データを取り扱う以上、同法の規制には常に注意を払う必要がある。

（3）PC やスマートフォン端末等の私的利用の禁止について

上述した問題のうち、従業員のプライバシー侵害をめぐる問題においては、前述した裁判例の判断枠組みに照らすと、会社の提供する PC やスマートフォン端末等について、私的な目的での利用が一定の範囲内で許容されることが、プライバシー侵害が成立する前提になっているといえる（私的利用の禁止の可否については Q30 を参照されたい。）。

（4）従業員の私物である PC やスマートフォン端末等を対象とした検査

以上の検討は、モニタリングの対象となる業務用の PC やスマートフォン端末等を企業が提供することを前提としたものであった。

これと異なり、従業員が私物の PC やスマートフォン端末を業務に利用している場合には、そこに保存されたデータについて従業員のプライバシーを保護する必要性は企業が提供する PC の場合に比して著しく大きいものとなる。このため、従業員から、事前に、個別の同意書面を取得する必要がある。同意書面には、端末管理ソフトを導入する目的、取得するデータの範囲、取得の方法、取得したデータの利用態様などを明記するほか、リモートでデータを削除する場合等の条件などを明記し、従業員に十分その内容を理解させる必要がある。なお、一般に、従業員は企業に従属する関係にあり、仮に同意したくない場合であっても代替的な選択肢がほとんど存在しないことから、従業員の自由な意思により同意をしたとは評価しにくい実情があるため、留意が必要であり、同意の有効性が問題となる場合があるので、留意が必要である。

さらに、上記の従業員から個別に取得する同意書面は、個人情報保護法上の（第三者提供等に係る）同意を兼ねる場合が多いと思われるところ、このような同意の取得にあたっては、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない[3]。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

文中に記載のとおり

[3] 個情法ガイドライン（通則編）2-16。

Q30 業務用端末の私的利用・私物端末の業務利用等に関する諸問題

企業が従業員に貸与する端末やメールアドレスを私的に利用することや従業員が私物端末を業務に利用すること等を巡っては様々な問題があるが、次のようなケースではどのようなことを考慮すべきか。

① 私用メールの禁止・制限
② SNS の利用禁止・制限
③ 私物端末の社内持込及び業務用データの社外持ち出しの禁止・制限
④ ①～③に違反した場合の懲戒・解雇処分の可否

タグ：労働契約法、私用メール、SNS、労働契約、就業規則、職務専念義務、解雇・懲戒処分、労働基準法、私物 PC、業務用データの社外持ち出し

１．概要

① 業務用メールアドレスの私的利用の禁止・制限

企業が従業員の業務用メールアドレスの私的利用（以下、本項において「私用メール」という。）その他業務用 PC の私的利用を禁止又は制限することについては、禁止を原則としつつ例外を認めること等柔軟な制度設計を行うことが考えられる。

② SNS の利用禁止・制限

企業が一定の場合に SNS の利用を禁止又は制限する規程を設けることには合理的理由がある。ただし、必要かつ合理的な限度の範囲においてのみ社会通念上許容されるものである。

③ 私物端末の社内持込及び業務用データの社外持ち出しの禁止・制限

企業は、従業員が遵守すべき事項を、従業員の服務上の義務（服務規律）としてあらかじめ定め、周知徹底を図る必要がある。さらに、当該服務規律について、就業規則上で、従業員に対して遵守を求め、違反がある場合には懲戒処分を実施できるようにしておくべきである。

私物 PC 等の社内持込及び利用禁止を実施する際、会社は従業員に持込及び利用の禁止を命ずることができる。私物 PC 等の社内持込及び利用を認める場合には、所有者の意思に反して調査することは原則的にできないことに注意すべきである。

また、使用者は、就業規則に定めを置き、業務用の情報の社外持ち出しを規制することができる。

④ ①～③に違反した場合の懲戒・解雇処分の可否

上記の行為は、解雇や懲戒処分の対象となり得る。ただし、こうした処分を実際に行うに当たっては、あらかじめこれらの行為に関する禁止や制限を定めた規程を作成し、就業規則上でこれらに関する服務上の規律の遵守を求めた上で、従業員に周知す

る等の形で当該服務規律が徹底されていることが重要である。このような徹底がなされていない場合、解雇や懲戒処分の許容性は大きく減殺される。

２．解説

（１）業務用メールアドレスの私的利用の禁止・制限

企業が業務遂行のために従業員に提供する業務用 PC 等の機器・設備及びメールアドレス（以下、本項において「PC 等」という。）を私的な目的を含む業務外の目的で利用することは、これらを提供する趣旨に反する。そして、私用メールが就業時間内に行われる場合には、当該行為は従業員が労働契約上負っている職務専念義務への違反となり得る。さらに、業務上取り扱う情報を外部に転送すること等で、情報流出のおそれはもちろん、その他守秘義務違反、競業行為等の問題が生じ得るほか、企業が提供する PC 等がストーキングや脅迫に用いられることで、企業の評判が害されるおそれがあるという名誉・信用の問題、そして、PC 等の私的利用を許すことで、ウイルス感染のリスクが高まるという問題も生じ得る。こうした問題を抑止する観点から、業務用の PC 等端末の私的利用の禁止が正当化され得る。

他方において、PC 等の私的利用が会社における職務の遂行の妨げとならず、また、私的利用を許容することで発生しうる会社の経済的負担（メールサーバの負荷、PC のメンテナンスコスト等）もきわめて軽易なものである場合には、必要かつ合理的な範囲内における過度に渡らない私用メール等が許容されるべきことは社会通念として一定の定着をみていると考えられるため、全面的に禁止することは難しいと考えられる。

以上から、企業が従業員に対して業務用 PC 等の私的利用を禁止したい場合には、就業規則等の諸規程において、合理的な理由がある場合に限定的に禁止するなど柔軟な規定を設けて制度設計を行うことが考えられる。

加えて、従業員がこれを理解し、実行し得るものとなるよう、必要に応じてガイドラインを設けるなどしておくことが望ましい。

なお、私用メール等を禁止する規定を設けているとしても、事実上私用メール等が黙認される等の実態がある場合には、当該規定の有効性が問題となることがあり得るため、規定を設けるだけでなく、規定に沿った実運用を図る必要がある。

（２）SNS の利用禁止・制限

企業内において、人事情報、知的財産、営業秘密等のセンシティブな情報を取り扱う従業員については、私的な SNS アカウントの利用を許すことで、これらのセンシティブな情報を流出するおそれがあり、その他の従業員についても、SNS を用いて企業の評価を害するような発信を行うおそれがある。

このため、企業としては、一定の場合に SNS の利用を禁止し、又は制限する規定を設けることが認められると考えられる。

ただし、こうした規定は、必要かつ合理的な限度の範囲においてのみ社会通念上許容されるものと考えられることから、SNS の利用に関する規程ないしガイドラインを設け、禁止又は制限の対象となる部署、発信内容、対象となる SNS 等について明確化することが考えられる。

（3）私物端末の社内持込及び業務用データの社外持ち出しの禁止・制限

ア　服務規律の作成[1]

企業は、私物 PC 等の社内持込及び利用禁止、業務用データの社外持ち出し、テレワークなど社外における業務を認めるに当たっては、従業員が遵守すべき事項を、従業員の服務上の義務（服務規律）としてあらかじめ定め、周知徹底を図る必要がある。そして、企業は、就業規則上で、当該服務規律の遵守を求め、違反がある場合には従業員に対する懲戒処分を実施できるようにしておくべきである。

イ　私物 PC 等の社内持込及び利用禁止を実施する際の考慮事項

私物 PC 等の社内持込及び利用は、企業秘密漏えいの可能性があるため、会社は、従業員に持込及び利用の禁止を命ずることができる。私物 PC は、当然のことながら会社には所有権がないため、所有者の意思に反して調査することは原則的にできないと考えるべきである。調査は、現に秘密漏えい事故があり、当該従業員にその漏えいの疑いを持つことに合理的な根拠があるなどの高度の必要性がある例外的な場合に限定されよう。また、私物 PC には多くのプライバシー情報が含まれる点も留意しなければならない。

ウ　業務用データの社外持ち出しを認める場合の考慮事項

従業員は労働契約上、企業の利益を不当に害しないようにする信義則上の義務（労働契約法第 3 条第 4 項）の履行として、秘密保持義務を負っているため、使用者は業務用の情報の社外持ち出しを規制することができる。また、業務上の情報を含む物品に関し、会社は所有権を有するため、これをどこで使用させるかについて会社には管理権限により決定することができる。企業は、業務上、情報を含む物品を社外に持ち出さないという規則を定める権限があり、従業員は、労働契約上の企業秩序遵守義務から当該規則に従う義務を負っている。特に、従業員の義務の内容に関しては、就業規則に根拠規定を置いた社内規程等において、禁止の範囲などを明確に定めておかなければならない。この際、企業の外から、企業の管理するアカウントを利用して、企業に管理権限がある情

[1] 私物端末の社内持込及び業務データの社外持ち出しに限らず、企業と従業員との関係でサイバーセキュリティ体制を確立するためには、就業規則上の規定の整備が重要であることについて、Q28 を参照されたい。

報にアクセスすることも業務用データの社外持ち出しに該当することに注意する必要がある。

（４）上記（１）～（３）に違反した場合の懲戒・解雇処分の可否

私用メール等を理由とした解雇や懲戒処分の効力も、一般的な解雇・懲戒処分の判断と同様の枠組で判断される。

すなわち、解雇については就業規則等で定められた解雇事由への該当性、解雇権濫用の成否（労働契約法第 16 条）などが、懲戒処分については就業規則上の根拠規程の存否、就業規則上の懲戒処分事由への該当性、懲戒権濫用の成否（労働契約法第 15 条）などが、それぞれ問題となる。

上記のとおり、PC 等の私的利用、SNS の利用や私物 PC 等に関する規定を設け、また、その違反行為を就業規則上の懲戒処分事由として明確化し、解雇・懲戒の対象とした場合であっても、裁判上、解雇・懲戒の効力が否定されることはあり得る。

例えば、軽微な違反の場合に解雇・懲戒を行った場合は、裁判においてその効力が否定されることがあり、また、就業規則等に PC 等の私的利用等について単純に全面禁止である旨を規定するのみでは、裁判においてそのとおりの効力が認められず合理的限定解釈の対象となり得る。

さらに、規定はあるものの、従業員に周知されていないなど、運用面で実態と乖離している場合も、当該規定の効力が否定され得る。

以上のとおり、上記（１）～（３）に関する制限については、全面禁止の規定を設けたとしても、従業員と争いとなる場面ではその効力の全部又は一部が否定されることがあり得る。このため、少なくともガイドラインの制定による基準の設定、規程・ガイドラインの内容の周知を行うことによって、規程と実態の乖離を防ぎ、当該規程の効力の有効性を担保することが考えられる。

３．参考資料（法令・ガイドラインなど）

・労働契約法第 3 条第 4 項、第 15 条、第 16 条など

４．裁判例

・東京地判平成 13 年 12 月 3 日労判 826 号 76 頁

社内ネットワークシステムを用いた私的電子メールの送受信につき、日常の社会生活を営む上で通常必要な外部との連絡の着信先として用いること、さらに、職務遂行の妨げとならず、会社の経済的負担もきわめて軽微なものである場合には、外部からの連絡に適宜即応するために必要かつ合理的な限度の範囲内において、発信に用いることも社会通念上許容されていると解すべきであるとした事例。従業員が社内ネットワークシステムを用いて電子メールを私的に使用する場合に期待し得るプライバシーの保

護の範囲は、通常の電話装置の場合よりも相当程度低減されることを甘受すべきであり、監視の目的、手段及びその態様等を総合考慮し、監視される側に生じた不利益と比較衡量の上、社会通念上相当な範囲を逸脱した監視がなされた場合に限りプライバシー権の侵害となると解するのが相当であると判断された事例。

・東京地判平成 14 年 2 月 26 日労判 825 号 50 頁

メールファイルの点検は、事情聴取により本人が送信者である疑いをぬぐい去ることができず、また、本人の多量の業務外の私用メールの存在が明らかになった以上行う必要があるとし、その内容は業務に必要な情報を保存する目的で会社が所有し管理するファイルサーバ上のデータ調査であることから、社会的に許容し得る限界を超えて原告の精神的自由を侵害した違法な行為とはいえないとされた事例。

・東京地判平成 15 年 9 月 22 日労判 870 号 83 頁

会社の送信するメールに機密文書であることを示す英文が付されているからといって、その内容が常に会社にとって実質的な営業上の機密にあたるものとは断定できず、むしろ、昇格人事については、従業員のメール送信以前に既に実施されており、外部に対しても早晩明らかになるべき事項であると考えられるから、会社にとって実質的な営業上の機密にはあたらないとした事例。

・札幌地判平成 17 年 5 月 26 日労判 929 号 66 頁

会社の備品であるパソコンを使用した私的メールの交信は懲戒処分の事由には該当するが、減給処分は懲戒処分として重すぎて不当であり、懲戒権の濫用に当たるとした事例。

・福岡高判平成 17 年 9 月 14 日労判 903 号 68 頁

専門学校の教職員が、勤務先から貸与された業務用パソコンを使用して、出会い系サイトに登録し、勤務中に大量の私用メールのやり取りを行ったことを理由に懲戒解雇とされたことにつき、同懲戒解雇は、解雇権の濫用にあたらないとされた事例。

・東京高判平成 17 年 11 月 30 日労判 919 号 83 頁

従業員が自己の扱う金融商品の営業成績に影響を及ぼす第三者の発表に対抗して行った個人的な訴訟の提起等の一連の行為について、それが従業員の全く私的な行為と認められるのでない限り、使用者の事業活動の一環として行われるものとして、使用者の指揮命令権限が及ぶというべきであり、就業規則等による規制の対象ともなるとされた事例（原判決は、東京地判平成 17 年 4 月 15 日労判 895 号 42 頁）。

・東京地判平成 19 年 6 月 22 日労経速 1984 号 3 頁

原告は就業中に IP メッセンジャー等で私的連絡を多数（6 か月で約 1700 件）行い、業務用として限定された機器の私的利用は服務規律・職務専念義務違反となるが、職場では一定範囲の私用が黙認される実情があり、本件の頻度は通常限度をやや超えるものの極端とはいえず、利用基準や指導・懲戒の実績が乏しく、顧客トラブルも生じていないことからすれば、当該事由により解雇は認められないとした事例。

・東京地判平成 19 年 9 月 18 日労判 947 号 23 頁

従業員の就業時間中の私用メールの送信頻度は 1 か月につき 2～3 通であり、その内容も、取引先の関係者からの世間話や母校の後輩からの就職相談、社員からの懇親会の打合せなどといったものであり、社会通念上許容される範囲を超えたものではないとして、私用メールの送信を就業規則違反に問うことはできないとされた事例。

Q31 テレワークにおけるセキュリティ

テレワークなど社外における業務を認める場合にはどのようなことを考慮すべきか。

タグ：テレワーク、VPN、テレワークセキュリティガイドライン

１．概要

新型コロナウイルス感染症の拡大によりテレワークの導入が加速したが、テレワークは、オフィスにおける勤務に比して類型的にセキュリティリスクが高く、実際、テレワークが普及したことを狙ったと思われるサイバー攻撃が多数発生している。

テレワークの実施に当たっては、経営者、システム・セキュリティ管理者、テレワーク勤務者がそれぞれの立場からセキュリティの確保に関して必要な役割を認識し、適切に担っていくことが重要である。

２．解説

（１）テレワークの拡大とセキュリティリスク

新型コロナウイルス感染症の拡大によりテレワークの導入が加速し、組織内外のコミュニケーション手段としてウェブ会議システムの利用が普及した。テレワークとは、労働者が情報通信技術を利用して行う事業場外勤務をいい、①労働者の自宅で業務を行う在宅勤務、②労働者の属するメインのオフィス以外に設けられたオフィスを利用するサテライトオフィス勤務、③ノートパソコンや携帯電話を活用して臨機応変に選択した場所で業務を行うモバイル勤務などの類型がある[1]。また、長期滞在先や旅行先などでテレワークを行う「ワーケーション」も注目を浴び、勤務の場所や状況を選ばない点で業務の効率化に役立っている。

他方、テレワークには、業務にインターネットを利用すること、従業員以外の第三者が立ち入る場所で執務をすること、セキュリティ設定が甘い無線 LAN（Wi-Fi）を利用する可能性があること、私物の端末を使用する場合があること等、特有のリスクがあり、テレワークは、オフィスにおける勤務に比して、類型的にセキュリティリスク（情報漏えいリスク[2]や情報システムリスク[3]等）が高い。実際、テレワークが普及したことを狙ったと思

[1] 厚生労働省「テレワークの適切な導入及び実施の推進のためのガイドライン」（https://www.mhlw.go.jp/content/000759469.pdf）１頁参照。
[2] テレワークにおける情報漏えいリスクの具体例として、例えば、インターネットを通じて業務データを社外で利用している際のマルウェア感染、第三者によるのぞき込み、ウェブ会議システムにおける機密情報の写り込み等が考えられる。
[3] テレワークにおける情報システムリスクの具体例として、例えば、インターネットを通じて業務データを社外で利用している際のマルウェア感染等により情報システムの全部又は一部を停止せざるを得なくなり、業務継続に支障が生じること等が考えられる。

われるサイバー攻撃が実際に多数発生している。近時では、複数の VPN 製品の脆弱性を突いた不正アクセス事案やランサムウェア事案も多発している。

脆弱性が原因と思われるサイバー攻撃については、国内外で様々な機関が注意喚起を行っており、IPA が公開した「情報セキュリティ 10 大脅威 2025」でも、「リモートワーク等の環境や仕組みを狙った攻撃」が組織向けの脅威の第 6 位となっている。

テレワークに係るセキュリティ対策を検討・実施するに当たっては、例えば、総務省が公表している「テレワークセキュリティガイドライン」や「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）第 3 版」、NCO が発出している注意喚起、IPA が公表している「テレワークを行う際のセキュリティ上の注意事項」等が参考になる。また、テレワークの実施に際しては、必然的に労務管理上の問題も生じることとなるが、これについては、厚生労働省が公表している「テレワークの適切な導入及び実施の推進のためのガイドライン」等が参考になる。以下、これらの概要を説明する。

（2）テレワークセキュリティガイドライン（総務省）

総務省「テレワークセキュリティガイドライン（第 5 版）」[4]（以下、本項において「テレワークセキュリティガイドライン」という。）は、テレワークの実施に当たっては、経営者、システム・セキュリティ管理者、テレワーク勤務者がそれぞれの立場からセキュリティの確保に関して必要な役割を認識し、適切に担っていくことが重要とし、それぞれの立場について、期待される役割と具体的に実施すべき事項を説明している[5]。

また、特に中小企業等については、予算やセキュリティ体制等が必ずしも十分ではないことから、中小企業等においても、実現可能性が高く優先的に実施すべきセキュリティ対策を判断するため、総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）第 3 版」[6]を活用することも考えられる。

ア　経営者の役割・実施すべき事項

経営者の基本的な役割は、事業の効率的かつ健全な発展と、当該事業に影響を及ぼすセキュリティリスクへの対応という両側面から、組織としてのあるべき姿を大局的な立場から検討し、その方針を示し、システム・セキュリティ管理者に作業を指示することである。具体的には、①テレワークセキュリティに関する脅威と事業影響リスクの認識、②テレワークに対応したセキュリティポリシーの策定、③テレワークにおける組織的なセキュリティ管理体制の構築、④テレワークでのセキュリティ確保のための資源（予算・人員）確保、⑤テレワークにより生じるセキュリティリスクへの対応方針決定と対応計

---

[4] https://www.soumu.go.jp/main_content/000752925.pdf
[5] 「テレワークセキュリティガイドライン」は、それぞれの役割や実施すべき事項を考える前提として、セキュリティ対策は、「最も弱いところが全体のセキュリティレベルになる」という特徴があり、「ルール」「人」「技術」のバランスが取れた対策が必要性であるとしている。
[6] https://www.soumu.go.jp/main_content/000752925.pdf

画策定、⑥テレワークにより対応が必要となるセキュリティ対策のための体制構築、⑦情報セキュリティ関連規程やセキュリティ対策の継続的な見直し、⑧テレワーク勤務者に対するセキュリティ研修の実施と受講の徹底、⑨セキュリティインシデントに備えた計画策定や体制整備、⑩サプライチェーン全体での対策状況の把握を実施することが重要である[7]。

イ　システム・セキュリティ管理者の役割・実施すべき事項

システム・セキュリティ管理者の基本的な役割は、経営者が示した方針や指示を情報セキュリティに関するルール（情報セキュリティ関連規程）の作成により具体化し、当該ルールを従業員に遵守させるとともに、当該ルールに沿った対策の企画・実施を行うことである。具体的には、①テレワークに対応した情報セキュリティ関連規程[8]やセキュリティ対策の見直し、②テレワークで使用するハードウェア・ソフトウェア等の適切な管理、③テレワーク勤務者に対するセキュリティ研修の実施、④セキュリティインシデントに備えた準備と発生時の対応、⑤セキュリティインシデントや予兆情報の連絡受付、⑥最新のセキュリティ脅威動向の把握を実施することが重要である。

ウ　テレワーク勤務者の役割・実施すべき事項

テレワーク勤務者の基本的な役割は、システム・セキュリティ管理者が作成した「ルール」を認識・理解し、これを遵守することである。具体的には、①情報セキュリティ関連規程の遵守、②テレワーク端末の適切な管理、③認証情報（パスワード・IC カード等）の適切な管理、④適切なテレワーク環境の確保、⑤セキュリティ研修への積極的な参加、⑥セキュリティインシデントに備えた連絡方法の確認、⑦セキュリティインシデント発生時の速やかな報告を実施することが重要である。

---

7 なお、②⑤⑦⑧⑨の全部又は一部については、本来は経営者が実施すべき事項であるものの、その具体的作業をシステム・セキュリティ管理者に任せることが想定されている。

8 テレワークの実施に当たっては、日頃は企業内部で厳密に保管されている情報を紙媒体で持ち帰って、あるいは、自宅等外部から共有ドライブにアクセスして業務を遂行することも生じ得るところ、営業秘密に関しては、営業秘密管理指針でも明記されたとおり、テレワーク環境などにおいて外部クラウドを利用して営業秘密を保管・管理する場合であっても、秘密管理性を失わないように扱う必要がある点に留意が必要である。この点に関して、経済産業省知的財産政策室が公表している「テレワーク時における秘密情報管理のポイント（Q&A 解説）」（令和 2 年 5 月 7 日）（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf）は、重要情報の自宅持ち帰り、私物端末での利用、ウェブ会議の留意点と営業秘密に関する事項が Q&A 方式でまとめられており参考になる。営業秘密の管理については、Q21 も参照されたい。

（３）テレワークの導入に関連する注意喚起

NCO は、テレワークの実施に伴い、テレワークに関連したサイバー攻撃やサポート詐欺などのリスクが高まることから、テレワークの導入に関連する注意喚起を複数発出している。

例えば、令和 2 年 4 月に発出された NCO（発出当時：NISC）「テレワークを実施する際にセキュリティ上留意すべき点について」[9]は、テレワークの開始に当たって、導入目的の明確化、対象範囲の決定、導入計画の策定、職員への説明等を行い、必要に応じ、セキュリティポリシーの改訂、それに伴う各種ルールの策定、ICT 環境の確認・整備を行うことが必要とした上で、テレワークの実施に際して留意すべき事項[10]について説明を行っている。同注意喚起は、テレワーク勤務者が留意すべき 7 つの項目[11]も指摘しており、参考になる。

また、令和 2 年 6 月に発出された NCO（発出当時：NISC）「テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について」[12]では、テレワークの導入後、これを継続的に実施するために留意すべき事項として、①情報セキュリティリスクの再評価、②情報セキュリティ関連規程の確認と必要に応じた改定、③利用端末・関連機器等の確認、④遠隔会議システムの利用状況の確認等が挙げられている。

（４）テレワークを行う際のセキュリティ上の注意事項（IPA）

IPA は、令和 2 年 4 月に公表した「テレワークを行う際のセキュリティ上の注意事項」[13]（令和 3 年 7 月更新）において、テレワーク勤務者に向けたセキュリティ上の注意事項を説明している。

情報漏えい防止の観点で、テレワーク時に特に気をつけるべき注意事項として、①テレワークで使用する PC 等は、できる限り他人と共有して使わず、共有で使わざるを得ない場合は、業務用のユーザアカウントを別途作成すること、②ウェブ会議のサービス等を新たに使い始める際は、事前にそのサービス等の初期設定の内容を確認し、特にセキュリティ機能は積極的に活用すること、③自宅のルータは、メーカーのサイトを確認の上、最新のファームウェアを適用すること、④カフェ等の公共の場所で PC 等を使用するときは画

---

9 https://www.ipa.go.jp/security/anshin/measures/ug65p9000000nk14-att/telework20200414.pdf

10 例えば、SNS に投稿したテレワークの写真に、機密性の高い文書や業務情報が映り込む事例が発生しており、テレワーク実施時には特に不用意な機密情報の漏洩に留意する必要があるとされている。

11 ①複雑なパスワードや多要素認証を使うこと、②端末や機器を最新のものにアップデートすること、③業務を装ったりするメールや不審なメールに注意すること、④通信を暗号化すること、⑤端末の盗難、紛失への注意（データの暗号化等）、⑥社外での留意点（他者からの盗み見（ショルダーハッキング）等への注意、無線 LAN のセキュリティ設定の注意）、⑦事故が生じた場合の連絡手順を確認することの 7 つである。

12 https://www.ipa.go.jp/security/anshin/measures/ug65p9000000nk14-att/telework20200611.pdf

13 https://www.ipa.go.jp/security/anshin/measures/telework.html

面をのぞかれないように注意すること、⑤公共の場所でウェブ会議を行う場合は、話し声が他の人に聞こえないように注意すること、⑥公衆 Wi-Fi を利用する場合は、PC のファイル共有機能をオフにすること、⑦公衆 Wi-Fi を利用する場合は、必要に応じて信頼できる VPN サービスを利用すること、⑧デジタルデータ／ファイルだけではなく、紙の書類等の管理にも注意することが挙げられている。

（５）テレワークの適切な導入及び実施の推進のためのガイドライン（厚生労働省）

厚生労働省は、使用者が適切に労務管理を行い、労働者が安心して働くことができる良質なテレワークを推進するため、テレワークの導入及び実施に当たり、労務管理を中心に、労使双方にとって留意すべき点、望ましい取組等を明らかにするため、「テレワークの適切な導入及び実施の推進のためのガイドライン」[14]を公表している。

同ガイドラインは、労務管理を中心に、①テレワークの導入に際しての留意点、②労務管理上の留意点[15]、③テレワークのルールの策定と周知、④さまざまな労働時間制度の活用、⑤テレワークにおける労働時間管理の工夫、⑥テレワークにおける安全衛生の確保、⑦テレワークにおける労働災害の補償、⑧テレワークの際のハラスメントへの対応、⑨テレワークの際のセキュリティへの対応について説明している。上記⑨においては、情報セキュリティの観点から全ての業務を一律にテレワークの対象外と判断するのではなく、関連技術の進展状況等を踏まえ、解決方法の検討を行うことや業務ごとに個別に判断することが望ましいとされ、また、企業・労働者が情報セキュリティ対策に不安を感じないよう、テレワークセキュリティガイドライン等を活用した対策の実施や労働者への教育等を行うことが望ましいとされている。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[14] 前掲注 1 参照。
[15] 「テレワークに要する費用負担の取扱い」について、「テレワークを行うことによって労働者に過度の負担が生じることは望ましくない。」といった記述もある（5 頁）。

Q32 派遣労働者及び特定受託事業者に対するセキュリティに関する義務付け

派遣先企業は秘密情報流出防止の目的で派遣社員の秘密漏えい防止の誓約書提出を義務付けることができるか。また、セキュリティ対策のための教育訓練を行うことができるか。また、派遣労働者以外に、フリーランス等について留意すべき点はあるか。

タグ：民法、労働者派遣法、派遣労働者、フリーランス、誓約書、教育訓練

１．概要

派遣労働者の秘密漏えい防止については、派遣元企業と派遣先企業との間の労働者派遣契約の中でそれを条件とするなど、労働者派遣契約（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和 60 年法律第 88 号。以下「労働者派遣法」という。）第 26 条に規定する労働者派遣契約をいう。以下同じ。）の中で検討すべき事項である。

セキュリティ対策のための教育訓練に関しては、派遣労働者が派遣契約上負う職務を遂行する上で必要な範囲のものであれば、派遣先企業は、当該派遣労働者に対して教育訓練を行うことが可能である。

請負契約等（業務委託契約を含む。以下同じ。）の形式をとっている場合であったとしても、発注者と受託者の労働者との間に指揮命令関係があると評価される場合には、労働者派遣法違反となる。なお、請負契約等の形式をとる場合、発注者は、情報セキュリティ措置等を受託者との契約に盛りこむことによりサイバーセキュリティを確保することが考えられる。

併せて、令和 6 年 11 月 1 日から、特定受託事業者に係る取引の適正化等に関する法律（令和 5 年法律第 25 号）が施行され、同法に規定する特定受託事業者（以下、本項において「フリーランス」という。）との取引における情報管理についてもあらかじめ検討しておく必要がある。

２．解説

（１）労働契約に付随する秘密保持義務等

従業員は、労働契約に付随する義務として秘密保持義務を負っている。しかし、派遣先企業と派遣労働者との間には労働契約が存在しないため、派遣先企業において派遣労働者に秘密保持義務を直接負わせることはできない。派遣労働者の守秘義務に関しては、あくまでも雇用関係のある派遣元企業と派遣労働者の間で義務付けがなされるべき事項である。

したがって、派遣労働者に派遣先企業の業務に関する秘密保持を義務付けるためには、基本的には派遣元企業との労働者派遣契約において、派遣元企業・派遣労働者間で派遣先の業務に関する秘密保持契約を締結させることを条件としておくことが考えられる。そして、派遣労働者が派遣元企業に対して誓約書を提出すること及び当該誓約書の写しを派遣先に提出することも派遣の条件としておくとよいであろう。また、派遣労働者が秘密を漏えいした場合には、派遣元企業が派遣先企業に対して損害賠償額の支払の責任を負う旨を定めておく等の措置も考えられる。

（２）労働者派遣法上の秘密保持義務

ところで、労働者派遣法第 24 条の 4 は「派遣元事業主及びその代理人、使用人その他の従業者は……その業務上取り扱ったことについて知り得た秘密を漏らしてはならない。派遣元事業主及びその代理人、使用人その他の従業者でなくなった後においても、同様とする。」と定めている。この条文にいう「従業者」とは派遣元企業において勤務する従業者のほか、派遣労働者も含むため、派遣労働者は労働者派遣法上「秘密を守る義務」を負うということになる。しかし、この義務は、労働者派遣法の性質から、該当する者が国に対して負っている義務（公法的な義務）であって、派遣労働者が派遣先企業に対してこの義務を負うものではない。したがって、やはり上記のように労働者派遣契約の中での対応が必要となるといえる。

（３）セキュリティ対策のための教育訓練等

派遣先企業は、派遣労働者の就業に際して、派遣先企業において秘密としている事項又は一般の従業員が負っている秘密保持の内容について、派遣労働者に周知すべきである。そして、秘密保持について教育訓練が必要になる場合には、派遣先企業はこれを実施することができる。派遣労働者は、派遣先企業の指揮命令下で使用されるため、派遣先企業で指揮命令を受けて職務を遂行する上で必要な教育訓練であれば、派遣先企業は当該派遣労働者に教育訓練を命ずることができるからである。

したがって、セキュリティ対策のための教育訓練に関しては、派遣労働者が労働者派遣契約上負う職務を遂行する上で必要な範囲のものであれば、派遣先企業は当該派遣労働者に教育訓練を行うことは可能である。このことについても、できる限り労働者派遣契約において明確化しておいた方がより適切であると考えられる。

（４）偽装請負

偽装請負とは、契約上、形式的には請負契約等としつつも、発注者が受託者の労働者に対して業務の遂行方法や勤務時間等について直接指揮命令を行っており、実態は受託者による発注者への労働者派遣事業であるものをいい、これは労働者派遣法に違反するも

のである。（労働者派遣事業と請負により行われる事業との区別に関する考え方については、厚生労働省「労働者派遣・請負を適正に行うためのガイド[1]」を参照）。

サイバーセキュリティ確保との関係では、例えば、請負契約等に基づき、発注者の事業所内で受託者の従業員が作業をしているケースにおいて、発注者が、受託者の従業員に対し、サイバーセキュリティ確保のために必要な行動を直接指示しているといった事情がある場合には、偽装請負と評価され得るのではないかが問題となり得る。このような場合、サイバーセキュリティを確保するためには、情報セキュリティ措置等（緊急時の対応に関する事項を含む。）を発注者と受託者との契約に盛りこむことが考えられる。

（５）フリーランスへの対応

他方で、フリーランスについては、派遣労働者とは異なり、公法的な義務も定められておらず、企業からも独立した主体であるため、何らの対策も採らなければ、企業との関係において、秘密保持義務を負う関係にはない。したがって、企業は、フリーランスとの関係においては、業務委託契約において秘密保持義務を定めることや、秘密保持に関する誓約書を取得しておく必要がある。

さらに、フリーランスであっても、場合によっては、委託元企業が保有する機密情報に触れたり、委託元企業の PC 等の端末を利用したりすることもあり得るため、そこからの情報流出リスクに対応する必要がある。この点の対策として、企業としては、フリーランスにどの程度の情報へのアクセスを認めるのかを、社内ルールを作成するなどして、事前に取り決めておき、その内容を従業員に対し周知徹底し、そもそもフリーランスが無用な機密情報にアクセスし得る環境を排除する必要がある。

３．参考資料（法令・ガイドラインなど）

・民法第 709 条
・労働者派遣法第 24 条の 4、第 26 条
・秘密情報の保護ハンドブック
・労働者派遣・請負を適正に行うためのガイド

４．裁判例

特になし

[1] https://www.mhlw.go.jp/content/001704228.pdf

Q33 退職後の競業避止義務と違反時の退職金減額・不支給及び情報漏えい防止のための秘密保持契約

秘密情報の流出を防止する目的で、従業員に退職後の競業避止義務を課すことを定める就業規則規定や個別合意の効力について、従業員の職業選択の自由との関係でどのような問題が生じるか。また、秘密情報流出防止を目的として競業避止義務を従業員に課した場合、これに違反したことを理由とする退職金の減額・不支給は認められるか。退職者が在職中に知り得た秘密情報を使用又は第三者に開示することを防ぐためには、いつどのような方法で秘密保持義務を負わせることが有効であるか。

タグ：民法、不正競争防止法、競業避止義務、競業避止義務契約、労働基準法、退職金、労働契約法、就業規則、秘密保持契約、秘密保持義務

１．概要

退職後の従業員に競業避止義務や秘密保持義務を負わせる就業規則上の規定や個別合意については、それが退職した従業員の職業選択の自由を過度に制約するものとして、公序良俗違反（民法第 90 条）によりその全部又は一部が無効になるのではないかが問題になる。

この点につき、裁判例の傾向は、①企業側の守るべき利益及びそれを踏まえた競業避止義務契約の内容の合理性、②従業員の地位、③地域的な限定の有無、④競業避止義務の存続期間、⑤禁止される競業行為の範囲への制限、⑥代償措置の有無等の要素に基づいて判断するという点では概ね一致しているが、裁判例は個別具体的な判断であるため、どのような規定ぶりであれば有効かということは一概には言えない。

また、秘密情報流出防止を目的として競業避止義務を従業員に課した場合、これに違反したことを理由とする退職金の減額・不支給は基本的に認められる。ただし、賃金の後払い的性格の強い退職金制度の場合、退職金の減額･不支給ができない場合がある。

企業としては、従業員との間の契約関係において、従業員が退職後に会社の秘密情報を流出させる行為、あるいはこれにつながり得る行為に制約を加えるための整備をしておくことが望ましい。このような定めとしては、以下のものが例として挙げられる。

① 退職後の従業員に競業避止義務を課す定め
② 退職後の従業員に秘密保持義務を課す定め

これらは、常に有効と判断されるとは限らない。各々の定めの有効性等は、それぞれ異なる枠組みの下で判断され、認められ得る効力も異なる。

２．解説

（１）退職後の情報漏えい防止のための競業避止義務

ア　退職後の従業員の競業避止義務を定める約定の効力を判断する枠組み

退職後の従業員に競業避止義務を課すためには、その旨を明示的に定める就業規則上の規定、個別合意等の根拠が必要であるが、これらの定めについては、適法な手続に則った就業規則の作成・周知や合意の成立が認められたとしても、さらにそれが退職した従業員の職業選択を過度に制約するものとして公序良俗違反によりその全部又は一部が無効になるのではないかが問題になる。この点について裁判例は、その細部においては必ずしも確立した傾向を示すとはいえないが、①企業側の守るべき利益及びそれを踏まえた競業避止義務契約の内容の合理性、②従業員の地位、③地域的な限定の有無、④競業避止義務の存続期間、⑤禁止される競業行為の範囲への制限、⑥代償措置の有無等の要素に基づいて判断するという点では概ね一致しているといえる。

以下では、各々の考慮要素について、秘密情報の保護ハンドブック参考資料 5 に沿って概要を解説する。

イ　裁判例における具体的判断

（ア）企業側の守るべき利益

裁判例において、企業側の守るべき利益としては、不正競争防止法上の「営業秘密」はもちろん、個別の判断においてそれに準じて取り扱うことが妥当な情報やノウハウについても、守るべき企業側の利益として判断されている（めっき加工や金属表面処理加工について、めっき技術訓練学校の教科書の記述やめっき事業者各社のホームページの記載等と比較して、法的保護に値する独自のノウハウが存することを主張して、一応の疎明がなされていると判断された事案として、大阪地決平成 21 年 10 月 23 日労判 1000 号 50 頁等参照）。営業秘密に準じるほどの価値を有する営業方法や指導方法等に係る独自のノウハウについては、営業秘密として管理することが難しいものの、競業避止によって守るべき企業側の利益があると判断されやすい傾向がある。

また、裁判例の中には、顧客との人的関係等について判断を行ったものも見られ、多数回にわたる訪問、地道な営業活動を要する場合であって、人的関係の構築が企業の業務としてなされている場合には、企業側の利益があると判断されやすい。

（イ）従業員の地位

従業員の地位について判断を行った裁判例では、合理的な理由なく従業員全てを対象とした規定はもとより、特定の職位にあることをもって判断されるというよりは、企業が守るべき利益を保護するために競業避止義務を課す必要がある従業員かどうかという観点から判断されていると考えられる。

例えば、形式的に執行役員という高い地位にある者を対象とした競業避止義務であっても、企業が守るべき機密性のある情報に接していなければ否定的な判断が行われることがある（東京地判平成 24 年 1 月 13 日労判 1041 号 82 頁等参照）。

（ウ）地域的限定

地域的限定について判断を行っている裁判例はそれほど多くはない。地理的な限定がないことを他の要素と併せて競業避止義務契約の有効性を否定する要素としている裁判例も散見されるが、地理的な限定が付されていない場合であっても、企業の事業内容（特に事業展開地域）や、職業選択の自由に対する制約の程度、特に禁止行為の範囲との関係等を総合的に考慮して競業避止義務契約を有効とした裁判例もあり、単に地理的な制限がないことをもって契約の有効性を否定するものではないと考えられる。

例えば、使用者が全国規模で事業を行っていることを理由に挙げて、地理的な制限がないとしても禁止範囲が過度に広範であるということもないとした裁判例がある（東京地判平成 19 年 4 月 24 日労判 942 号 39 頁参照）。

（エ）競業避止義務期間

退職後に競業避止義務が存続する期間についても、形式的に何年以内であれば認められるというものではなく、労働者の不利益の程度を考慮した上で、業種の特徴や企業の守るべき利益を保護する手段としての合理性等が判断されているものと考えられる。裁判例の傾向として、期間が短期、特に 1 年以内のものについては、肯定的に捉えられている裁判例も多いが、長期のもの、特に 2 年以上の期間となっているものについては、否定的な判断がなされている例もみられる。

（オ）禁止行為の範囲

禁止される行為の範囲についても、企業側の守るべき利益との整合性が判断される傾向にある。例えば、約定で禁止される行為の内容が、競業行為の自営や競業企業への就職を全面的に禁止するものでなく、上記（ア）で挙げた企業の利益を侵害するおそれが大きい行為に絞り込まれている場合、従業員の職業選択の自由に及ぼす制約が小さくなることから、約定の効力は認められやすくなる。例えば、東京地判平成 14 年 8 月 30 日労判 838 号 32 頁は、退職後 2 年間、在職中の営業担当地域及びこれに隣接する地域における（転職先からの）使用者の顧客への営業活動を禁止する内容の定めが置かれた事案であり、このように禁止する行為の内容が絞り込まれていたことから、代償措置がなくとも当該定めは有効と認められると判示されている。

このように、禁止対象となる活動内容や職種を限定する場合においては、必ずしも個別具体的に禁止されている業務内容や取り扱う情報を特定することまでは求められていないものと考えられる。

なお、これに関連して、競業行為の自営や競業企業への就職を一般的に禁止する約定の効力について、使用者たる企業側の利益を侵害するおそれが多い行為を禁止す

る限度で肯定する合理的限定解釈を行う裁判例もみられる（合理的限定解釈を行った上で、その限度で差止めを認めた例として、東京地決平成 16 年 9 月 22 日判時 1887 号 149 頁、合理的限定解釈を行った結果義務違反を否定した例として、東京地判平成 17 年 2 月 23 日判タ 1182 号 337 頁）。

（カ）代償措置

代償措置、すなわち、競業行為を規制される従業員に対して、その代償として金銭の支払等を行うことについては、他の要素に比して競業避止義務契約の有効性について直接的な影響を与えている例も少なくなく、裁判所が重視していると思われる要素である。裁判例の中には、代償措置と呼べるものが何らなされていないことを理由の一つとして当該契約の有効性を否定する例もある。

しかし、主流な考え方は、複数の要因を総合的に考慮する考え方であり、代償措置の有無のみをもって当該契約の有効性の判断が行われているわけではない。代償措置がない場合であっても約定の効力を認める例（前掲・東京地判平成 14 年 8 月 30 日）や、代償措置が明確な形で講じられていない場合にも、従業員に支払われた賃金が比較的高額である場合に、そのことを代償措置としての性質も有するものとして柔軟に考慮する例（前掲・東京地決平成 16 年 9 月 22 日、東京地判平成 19 年 4 月 24 日など）も存在する。

もっとも、代償措置が明確な形で講じられていない場合に約定の効力を認めた事案の多くは、禁止される行為の内容が絞り込まれた形で約定がなされていたか、合理的限定解釈により、裁判所が禁止される行為の内容を絞り込んだ上でその効力を認めた事案である。

ウ　小括

以上をまとめると、競業避止義務契約締結に際して考慮すべき点を以下のとおり挙げることができる。

（ア）競業避止義務契約締結に際して最初に考慮すべきポイント

- 企業側に営業秘密等の守るべき利益が存在する。
- 上記守るべき利益に関係していた業務を行っていた従業員等特定の者が対象

（イ）競業避止義務契約の有効性が認められる可能性が高い規定のポイント

- 競業避止義務期間が短期間（1 年以内）となっている。
- 禁止行為の範囲につき、業務内容や職種等によって限定を行っている。
- 代償措置（高額な賃金等「みなし代償措置」といえるものを含む）が設定されている。

（ウ）有効性が認められない可能性が高い規定のポイント

- 業務内容等から競業避止義務が不要である従業員と契約している。
- 職業選択の自由を阻害するような広汎な地理的制限をかけている。

- 競業避止義務期間が長期間（2 年超）にわたっている。
- 禁止行為の範囲が、一般的・抽象的な文言となっている。
- 代償措置が設定されていない。

（エ）労働関係法令との関係におけるポイント

- 就業規則上の規定、個別合意等の根拠を整備すること。
- 当該就業規則について、入社時の「就業規則を遵守します」等といった誓約書を通じて従業員の包括同意を得るとともに、十分な周知を行う。

エ　義務違反がある場合の差止め要件

上述した判断枠組みにしたがって、義務違反が認められる場合、従業員の義務違反行為に対する差止め又は義務違反によって生じた損害の賠償の請求が認められ得る。ただし、裁判例の中には、このうち前者の差止めについて、元使用者の営業上の利益が侵害されるか、そのおそれがある場合に限って認められるという要件を課しているもの（東京地決平成 7 年 10 月 16 日労判 690 号 75 頁等参照）も存在する。

オ　競業避止義務違反による退職金の減額不支給

判例は、企業が労働者（従業員）に対し退職後の同業他社への就職をある程度の期間制限することをもって直ちに労働者の職業の自由等を不当に拘束するものとは認められず、したがって、会社がその退職金規程において、競業制限に反して同業他社に就職した退職従業員に支給すべき退職金につき、その点を考慮して、退職金の減額する規定にも合理性があるとしている。これは、退職金が賃金の後払い的性格を持つとともに、功労報償的性格をあわせ持つと解されるため、功労を抹消するような行為について退職金を減額・不支給（没収）する条項も合理性があると考えられているためである。

ただし、このような退職金の減額・不支給は、同業他社への就職を制約するものであるため、労働者の職業選択の自由との関係が問題となる。すなわち、退職金の減額・不支給が適用になるのは、競業規制の内容（競業規制の期間、態様、減額率）について合理的な範囲に限定されるのである[1]。合理的でない場合には、条項が無効とされよう。

また、理論的には、支払済みの場合退職金返還請求も可能である。もっとも、退職金減額・不支給のメリットとしては、あらかじめ退職金を押さえてしまうことで、損害賠償請求を行う手間を省けるところにあるので、一度支払ってしまった退職金を取り戻すことができると考えることにどれほどのメリットがあるか疑問ではある。したがって、特に秘密に触れる業務に従事する従業員が退職を申し出たような場合には、退職金を支払う前に当該従業員に関し十分慎重に調査するなどの対応が求められよう。その対策の一例としては、秘密を取り扱う企業である場合、十分調査できるように支給日に余裕をもたせた退職金制度を設計しておくなどの方法も考えられよう（また、退職金相当額の

[1] 菅野和夫・山川隆一『労働法』（弘文堂、第 13 版、令和 6 年）183 頁等参照。

違約金の約定を取り付けておく等の対策も検討されるべきである。なお、この場合、労働契約の不履行に対する違約金の定めではないので労働基準法第 16 条の問題は生じない)。

なお、退職金の不支給･減額が認められない場合として、業務実績に応じて額が機械的に積算されるような方式（ポイント式退職金制度）や、退職金相当額を毎月前払で支払ってもらうか退職時に積み立てた額を支払ってもらうか従業員が選択する方式（退職金前払選択制度）が採用されている場合が挙げられる。このような制度の下では、賃金後払い的性格が強く功労報償的性格は認められないとして、退職金の減額・不支給は否定されるとする裁判例がある。また、選択的な制度を採用している企業において退職一時金を選択した従業員に対してのみ、制裁措置として退職金を減額･不支給にすることは、公平さを欠き許されないと考えられる。

（２）退職後の情報漏えい防止のための秘密保持義務

ア　退職後の秘密保持義務

就業規則により退職後の秘密保持義務を負わせることは、一定の合理性が認められる範囲では有効と解される余地がある。一方で就業規則では従業員の退職後の法律関係を定めることはできないという見解も有力であり、裁判実務上確立していない中で、退職後の従業員の秘密保持義務を就業規則にのみ依拠することは少なからず法的リスクを伴うことになる。また、就業規則に退職後の従業員の秘密保持義務を定める規定を置いた場合には、従業員との間の個別合意によって、就業規則の定めよりも従業員に不利益となるような義務を課すことができなくなる（労働契約法第 12 条)。さらに、就業規則規定の新設や変更により、既に退職した後の従業員に対し、新たに義務を課したり、義務の内容を従業員側の不利益に変更したりすることについては、許容されないと解される。そこで、退職者が在職中に知り得た企業の秘密情報を第三者に開示させないためには、仮に就業規則でその旨を設ける場合であっても、さらに、個別の秘密保持契約により、当該退職者に企業に対する秘密保持義務を負わせることが有効と考えられる。

また、企業に対する契約上の秘密保持義務は、営業秘密の要件である秘密管理性を充足するための重要な要素の一つと考えられている。そして、秘密情報が不正競争防止法における営業秘密としての保護を受けるためには、秘密保持の対象となる情報が具体的に特定されている必要があると考えられている[2]ため、営業秘密としての保護を受けるためには、対象となる秘密情報を特定した上で契約を締結することが望ましい（秘密管理性の意義について、Q21 を参照されたい。)。

秘密保持契約を締結する場合には、その締結時期に留意する必要がある。入社時において、秘密保持契約を個別に締結する場合には、秘密保持の対象とする具体的な秘密情報の特定が困難であり、秘密情報を特定しない包括的な秘密保持義務を定めることにな

[2] 東京地判平成 17 年 2 月 25 日判時 1897 号 98 頁参照。

らざるを得ない。他方、退職時に秘密保持契約を締結しようとしても、退職者が秘密保持契約の締結を拒否する場合があり、この場合には契約の締結を強要することはできない。

そこで、従業員に秘密情報を開示する段階で、退職後も秘密保持義務を継続的に負うことを明示した秘密保持契約を締結することが有効と考えられる。この場合、労働契約終了後も守秘義務を継続的に負担させる合意の効力が問題となるが、裁判例[3]は、「使用者にとって営業秘密が重要な価値を有し、労働契約終了後も一定の範囲で営業秘密保持義務を存続させることが、労働契約関係を成立、維持させる上で不可欠の前提でもあるから、労働契約関係にある当事者において、労働契約終了後も一定の範囲で秘密保持義務を負担させる旨の合意は、その秘密の性質・範囲、価値、当事者（労働者）の退職前の地位に照らし、合理性が認められるときは、公序良俗に反せず無効とはいえないと解するのが相当である。」としている。

また、秘密保持義務の定めを実効的なものにするためには、秘密保持義務違反に対する違約金を定めておくことも考えられる。なお、秘密保持義務違反に対する違約金の定めは労働基準法第 16 条との関係でその有効性について議論があるところ、企業としては、同条に違反するとの評価を受けるリスクがある点を踏まえて違約金の定めを置くことの是非を検討する必要がある。

イ　秘密保持義務、競業避止義務等の比較

秘密保持義務の定めによる方法は、従業員による情報漏えいそれ自体を禁止対象としているのに対し、競業避止義務の定めによる方法は、情報漏えいにつながり得る行為を広く禁止対象としている。このように、後者の手法は前者の手法と比べて禁止対象が広く、それだけ従業員の退職後の職業選択の自由に対する制約の度合いが大きいため、定めの有効性の判断が、より厳格なものとなる。すなわち、一般的にいえば、前者の手法の方が、後者の手法よりも、その有効性を認められやすい（より一般的にも、禁止される行為の範囲が絞り込まれていた方が、定めの有効性を認められやすいといえる。）。

次に、退職金の減額等による方法は、退職した従業員の行為を直接的に禁止する（差止める）効果をもたらすものではないが、その反面、定めの効力等が認められた場合、企業側には従業員の行為によって被った具体的損害の額に関わりなく一定の額の金銭を従業員に請求できる（あるいは一定の範囲で退職金支払を免れる）というメリットがある。企業としては、このような各手法の特質及びその相違を考慮しつつ、自企業においてどのような定めを設けるべきかを判断すべきである。なお、これらの手法のうち複数のものを併用することは差し支えなく、実際にもそのような例は多い。

[3] 東京地判平成 14 年 8 月 30 日労判 838 号 32 頁。

３．参考資料（法令・ガイドラインなど）

・労働契約法第 7 条、第 9 条、第 10 条、第 12 条など
・民法第 90 条
・秘密情報の保護ハンドブック　参考資料 5 競業避止義務契約の有効性について
・労働基準法第 16 条、第 24 条、第 89 条第 3 号の 2
・不正競争防止法第 2 条第 1 項第 7 号、第 21 条第 2 項第 1 号・第 3 号・第 4 号
・秘密情報の保護ハンドブック

４．裁判例

退職後の競業避止義務の効力については、本文中に記載したもののほか、

・福岡高判令和 2 年 11 月 11 日労判 1241 号 70 頁

退職後の競業避止義務については、労働者と使用者の間で合意が成立していたとしても、その合意どおりの義務を労働者が負うと直ちに認めることはできず、労働者が負う競業避止義務による不利益の程度、使用者の利益の程度、競業避止義務が課される期間、労働者への代償措置の有無等の事情を考慮し、競業避止義務に関する合意が公序良俗に反して無効であると解される場合や、合意の内容を制限的に解釈して初めて有効と解される場合があるというべきであるとされた事例。

競業避止義務違反による退職金の減額不支給については以下のとおり

・最判昭和 52 年 8 月 9 日労経速 958 号 25 頁

会社が営業担当社員に退職後の同業他社への就職をある程度期間制限することが直ちに社員の職業選択の自由を不当に拘束するとは認められず、退職金規定でその制限に違反し、同業他社に就職した場合の退職金を半額と定めることも功労報酬的な退職金の性格を併せ有することに鑑みれば、合理性のない措置とすることはできないとした事例。

・名古屋高判平成 2 年 8 月 31 日労判 569 号 37 頁

退職金支給規定に退職後六か月以内に同業他社に就職した場合には退職金を支給しない旨の不支給条項がある場合において、退職従業員に会社に対する顕著な背信性は認められないとして、右従業員に対する右不支給条項の適用を否定した事例。

・大阪高判平成 10 年 5 月 29 日労判 745 号 42 頁

就業規則の変更に際しての周知手続がとられていないこと、すでに退職願を出している労働者に報復的な意図の下に退職金の支給義務を免れようとしたこと、既得権である退職予定者の退職金請求権を奪うもので合理的な変更といえず、労働者には効力がないとして、重大な背信行為の有無を問わず退職金不支給規定は適用されないとした事例。

・名古屋地判平成 6 年 6 月 3 日労判 680 号 92 頁

Q33 退職後の競業避止義務と違反時の退職金減額・不支給及び情報漏えい防止のための秘密保持契約

求人票に外交員の仕事としてパン類の宅配業務と記載されており、従業員らは、単に被告会社の販売員になるとの認識を有していたこと、従業員らは、会社のパン類の販売業務の一端を担う外交員として作業に従事してきたこと、外交員の売上手数料及び退職慰労金が労働の対償であることなどを理由として、従業員の契約が業務委託契約ではなく、労働契約であったと判断した上で、所定の販売手数料（賃金）及び退職慰労金（退職金）の支払い請求を認容した事例。

Q34 退職後の海外での秘密保持義務違反行為について

元従業員・元役員による海外における秘密情報の不正使用・不正開示行為については、どのような対策があり得るか。退職後の秘密情報流出防止を目的とした秘密保持義務契約は有効か。また、当該義務違反時にどのような措置を取り得るか。

タグ：不正競争防止法、民事訴訟法、法の適用に関する通則法、秘密保持義務、競業避止義務、情報漏えい、人材を通じた技術流出

１．概要

企業から退職等した元従業員・元役員が、当該企業の秘密情報を海外において不正に使用する行為や不正に開示する行為については、秘密保持義務契約（守秘義務契約）違反若しくは不正競争防止法違反を主張して争う、又は営業秘密侵害罪の被害に関して警察等に相談するという措置を取り得る。

もっとも、海外における裁判の利用には様々な論点が存在するため、秘密保持義務契約を反故にされても、技術的又は物理的に秘密情報が使用されたり漏えいしたりしないようにするためのサイバーセキュリティ対策が重要といえる。

２．解説

（１）海外における秘密保持義務違反行為とは

かねてより人を通じた技術流出が指摘されている。特に近時は、経済安全保障の観点から、重要な技術情報（秘密情報）の海外流出の防止の重要性が高まっており、情報の窃取の手法としても、SNS を通じた手法、在籍していた役員・従業員の転職・退職を利用した手法、産業スパイを利用した手法など、きわめて多様化している[1]。そこで、企業では、このような秘密情報の流出の防止を目的として、退職後の秘密情報の使用・開示を禁止する内容の、就業規則（包括的合意）を規定したり、誓約書等（個別の合意）を従業員・役員に提出させたりする場合がある[2]。

本項においては、このように就業規則や誓約書等を通じて秘密保持義務契約を締結した従業員・役員が企業を退職・退任又は解雇・解任された後、海外で秘密保持義務の対象となっている秘密情報の不正使用・不正開示を行った場合について解説する。

[1] 具体例については、「技術流出対策ガイダンス 第１版」（経済産業省貿易経済安全保障局 技術調査・流出対策室）（https://www.meti.go.jp/policy/economy/economic_security/guidance.pdf）などが参考になる。
[2] なお、誓約書の徴収については Q28 参照。また、退職後の秘密保持義務及び競業避止義務の効力については、Q33 を参照されたい。

（２）海外における秘密保持義務違反行為のパターンについて

元従業員・元役員が海外（仮に A 国とする）において従前所属し又は勤めた企業の秘密情報を不正に使用・開示する場合を整理すると、以下のようなパターンに分類される。それぞれのパターンごとに、どの国の法律が適用されるのか、どの国に裁判管轄があるかなど、検討する必要がある。

	従前の所属先	秘密保持契約の締結者	契約の締結時期
1	日本（日本本社勤務）	日本本社	退職前
2			退職後
3	海外支店（B 国）	日本本社	退職前
4			退職後
5	海外子会社（B 国）	海外子会社（B 国）	退職前
6			退職後

（３）国際私法（抵触法）及び準拠法について

このような場合、どの国・地域の裁判所が管轄権を有するのかという国際裁判管轄の問題[3]に加えて、日本の法令が適用されるのか、A 国の法令が適用されるのか、又は B 国の法令が適用されるのかといったような、どの国・地域の法令によるべきかという問題が生じる。

このような渉外的私法関係に適用すべき私法を指定する法規が国際私法である[4]。そして、渉外的私法関係に適用すべく指定される実質法のことを準拠法という[5]。

我が国における代表的な国際私法としては、法の適用に関する通則法（平成 18 年法律第 78 号。以下、本項において「法適用通則法」という。）[6]が挙げられる。

（４）設例に関する検討

ア　A 国において争う場合について

秘密情報が実際に使用されている A 国において、元従業員・元役員による秘密情報の開示行為又は使用行為を差し止めたり損害賠償を請求したりしようとする場合、①A 国

[3] 我が国においては、民事紛争のうち財産権上の訴えについては、民事訴訟法（平成 8 年法律第 109 号）及び民事保全法（平成元年法律第 91 号）に国際裁判管轄に関する規定が設けられている（法務省民事局総務課長小出邦夫編著「逐条解説 法の適用に関する通則法〔増補版〕」（商事法務、平成 26 年 12 月）449 頁）。

[4] 山田鐐一「国際私法 第 3 版」2 頁（有斐閣、平成 16 年 12 月）2 頁。なお、法律の抵触を解決する法という意味で、国際私法は往々抵触法とも呼ばれ、また、狭義の国際私法と、国際民事訴訟法ないし国際手続法を含めた広義の国際私法という概念がある（同 3 頁）。

[5] 前掲注 4・2 頁。

[6] 法適用通則法は、外国法、慣習法、判例法などを含む私法一般という意味で「法」という文言にかえられている（櫻田嘉章＝道垣内正人「注釈国際私法 第 1 巻 §§1～23」（有斐閣、平成 23 年）66 頁）。

の裁判所又は裁判外紛争手続を利用する、②日本の裁判所で得た判決を A 国で承認してもらい執行する、という 2 つの選択肢が考えられる。

また、請求の相手方としては、元従業員・元役員のみならず、不正開示先又は不正使用先（例えば、元従業員・元役員の再就職先や自らが設立した企業など）を相手方とすることも考えられる。留意すべきは、秘密保持義務契約の相手方は元従業員・元役員であるため、秘密保持義務違反に基づく主張は、元従業員・元役員を相手方とする場合に限られることである。不正開示先・不正使用先を相手方にしようとするときは、日本の不正競争防止法違反、又は A 国・当該地域の営業秘密に関する法令や不法行為を規定する法令等の違反を主張する必要がある。

（ア）A 国の裁判所を利用するとき

まず、A 国の裁判所を利用しようとするときには、当該裁判所の管轄権の有無が判断されなければならない。

その上で、元従業員・元役員を相手方とするならば、秘密保持義務違反で争うことが考えられる。この場合、A 国の国際私法に則って、準拠法が判断された上、秘密保持義務契約の有効性が判断されることになる。そこで、仮に、秘密保持義務契約において準拠法を日本国法とする旨の準拠法の指定に関する合意がなされていたとしても、A 国の国際私法によれば、秘密保持義務契約における準拠法の指定は許されないと判断される可能性もある。

加えて、準拠法は A 国又は該当地域の法令であると判断された場合に、A 国・当該地域の法令に基づくと従業員・役員との秘密保持義務契約は無効と判断されることもある。

次に、元従業員・元役員又は不正開示先・不正使用先を相手方として、日本の不正競争防止法違反、又は A 国・当該地域の営業秘密に関する法令違反を主張して争うことが考えられる。

A 国の裁判所等において日本の不正競争防止法違反を主張できるかは、A 国の国際私法によることとなる。

また、A 国・当該地域の営業秘密に関する法令違反を主張する場合には、当該法令の調査・検討を要することとなる。

（イ）日本の裁判所で得た判決を A 国で執行しようとするとき

まず、日本の裁判所で判決を得る必要があるが、この場合の論点等については、下記イ（ア）及び（イ）を参照されたい。

その上で、日本国の判決が A 国において承認され執行されるかという国際手続法に関する検討が必要となる（下記イ（ウ）と同じ論点である。）。

イ　日本において争う場合

日本の裁判所において、秘密保持義務違反又は不正競争防止法違反を主張して争い、そこで得た判決をもってA国において執行しようとする場合については、以下の論点が考えられる。

（ア）秘密義務契約違反を主張する場合

日本の裁判所の管轄権の有無は、民事訴訟法第3条の3第1号に基づき判断されると考えられる[7]。

仮に管轄権が日本の裁判所にあると判断された場合、次に、準拠法が問題となる。準拠法については、上記（3）のとおり、日本においては法適用通則法が規定している。具体的には、同法は、「法律行為の成立及び効力」についての準拠法を規定しているところ、元従業員・元役員に対し秘密保持義務違反に基づいてA国における秘密情報の不正使用・不正開示を差し止めたり、損害賠償請求をしたりできるかという点については、「法律行為の……効力」の問題と考えられる。

法律行為の効力に関する準拠法について、同法は、まずは当事者の選択によることとしており（同法第7条）、当事者の選択がない場合についての基準も定めている（同法第8条）。そして、法律行為のうち消費者契約と労働契約については、それぞれ特例を定めている（同法第11条及び第12条）。

そこで、従業員・役員との間の秘密保持義務契約については、法適用通則法第12条の労働契約の特例により準拠法が決定されるのかという問題が生じる。すなわち、退職等する前に秘密保持義務契約を締結していたとしても、既に退職等しているのであれば、秘密保持契約は「労働契約」[8]に該当しないのではないかが問題となる。

この点、秘密保持義務契約ではないものの、競業避止義務契約については、学説上、労働契約の終了後に関するものであり、厳密な意味での労働契約には該当しないものの、労働契約と密接に関連し、当該合意を行う時点で当事者間の交渉力格差も認められることから、法適用通則法第12条の適用又は類推適用がなされると解されている[9]。

他方、会社法上の役員については、そもそも企業に雇用されているのではなく委任契約であり（会社法第330条）、「労働契約」とはいえないため、法適用通則法第12条ではなく、当事者が準拠法の選択をしているか否か（第7条及び第8条）の問題

[7] 民事訴訟法第3条の3第1号は、「契約上の債務の履行の請求を目的とする訴え……契約上の債務の不履行による損害賠償の請求その他契約上の債務に関する請求を目的とする訴え」については、「契約において定められた当該債務の履行地が日本国内にあるとき、又は契約において選択された地の法によれば当該債務の履行地が日本国内にあるとき」は、日本の裁判所に提起することができる旨を規定する。

[8] 法適用通則法上、「労働契約」の定義が明示されていないものの、「労働契約」とは、労働者が使用者に使用されて労働し、使用者がこれに対して賃金を支払うことを約する契約と解されるとされる（前掲注6・275頁）。

[9] 前掲注6・277頁。

となると考えられる。すなわち、秘密保持義務契約において準拠法の指定がなければ、「当該法律行為に最も密接な関係がある地の法による」（法適用通則法第 8 条第 1 項）こととなる。

しかし、秘密保持義務違反に基づく差止請求における「当該法律行為に最も密接な関係がある地」はどこなのか、秘密保持義務契約の締結自体は、上記（2）に記載のとおり大きく 6 パターンに分けられるが、契約違反行為自体は A 国で生じているため、「当該法律行為に最も密接な関係がある地」をどのように解すべきかという問題が生じると考えられる。また、秘密保持義務違反に基づく損害賠償請求については、契約違反に基づく損害賠償請求が「法律行為において特徴的な給付を当事者の一方のみが行うものである」といえるのであれば[10]、「その給付を行う当事者の常居所地法」が当該法律行為に最も密接な関係がある地の法と推定されると考えられる（法適用通則法第 8 条第 2 項）。なお、秘密保持義務違反に基づく損害賠償請求が不法行為に基づく損害賠償請求の要件も満たす場合には、同法第 20 条の「当事者間の契約に基づく義務に違反して不法行為が行われたこと」に該当し、結局、契約の準拠法によることとなると解される[11]。

（イ）不正競争防止法違反を主張する場合

A 国において元従業員･元役員により開示･使用されている秘密情報が「営業秘密」に該当するのであれば、元従業員・元役員又は不正開示先・不正使用先に対して不正競争防止法違反の主張をすることが考えられる。

不正競争防止法第 19 条の 2 は、日本国内で事業を行う企業の、日本国内で管理体制を敷いて管理している営業秘密に関する民事訴訟であれば、海外での侵害行為も日本の裁判所で日本の不競法に基づき提訴できる旨を明確化した。ただし、同条は、当該営業秘密が専ら日本国外において事業の用に供されるものである場合を除外しており、この場合の日本の裁判所の管轄権の有無が問題となるが、不正競争防止法は不法行為の特則であるから、日本の裁判所の管轄権の有無は、民事訴訟法第 3 条の 3 第 8 号に基づき判断されると考えられる[12]。

仮に管轄権が日本の裁判所にあると判断された場合、次に、上記（ア）同様、準拠法が問題となる。不正競争の準拠法決定は、不正競争における被侵害利益が多様であ

[10] 「特徴的給付の理論」とは、ある契約を他の種類の契約から区別する（特徴付ける）基準となる特徴的な給付を当事者の一方のみがする場合に、その当事者の所在地をその契約と最も密接に関係する地とする考え方である（前掲注 3・108～109 頁）。
[11] 前掲注 3・232～237 頁。
[12] 民事訴訟法第 3 条の 3 第 8 号は、「不法行為に関する訴え」については、「不法行為があった地が日本国内にあるとき（外国で行われた加害行為の結果が日本国内で発生した場合において、日本国内におけるその結果の発生が通常予見することのできないものであったときを除く。）」は、日本の裁判所に提起することができる旨を規定する。

ることを理由に法適用通則法の立法時に見送られたため[13]、法適用通則法には明文の規定がない。

そこで、法適用通則法第 17 条説、第 20 条（最密接関係地がある場合の例外）説又は条理に基づく市場地法による説といった解釈論が展開されている[14] [15]。また、裁判例としては、法適用通則法第 17 条によるもの、明文の規定ではなく条理によるもの、根拠を示すことなく日本法を適用したものに分類されるという[16] [17]。

（ウ）A 国において判決を執行する場合

上記（ア）又は（イ）の各論点をクリアして日本国の判決を得た場合、日本国の判決が A 国において承認され執行されるかという国際手続法に関する検討が必要となる[18]。

（５）刑事的措置について

平成 27 年不正競争防止法改正により、国外犯処罰の規定について、従前「日本国内において管理されていた営業秘密」との定めが「日本国内において事業を行う営業秘密保有者の営業秘密」と改正され[19]、対象となる営業秘密の範囲が明確化ないし拡大されたとともに、国外における不正取得行為も対象行為として追加され、国外犯処罰規定の範囲が拡大された（不正競争防止法第 21 条第 8 項）。また、海外重罰規定も設けられた（不正競争防止法第 21 条第 4 項及び第 5 項。）。

そこで、これら規定の被害に関して、警察・検察に相談するという手段もある[20]。

---

[13] 前掲注 6・450 頁。
[14] 前掲注 6・450～451 頁。
[15] 法規欠缺の場合の裁判事務処理の方法として、まず慣習により、慣習なきときは条理によるとされる（前掲注 6・51 頁）。
[16] 嶋拓哉「日本法人保有の情報の使用及び開示の差止等請求と不競法」（私法判例リマークス、59～142 頁）。
[17] なお、近時の裁判例としては、海外で不正開示された営業秘密を海外で取得した日本法人に対して（不競法第 2 条第 1 項第 8 号）、当該営業秘密の日本における使用・開示の差止め等を求めた日本法人間の事案において、知財高判平成 30 年 1 月 15 日判タ 1452 号 80 頁があるが、日本法人の日本での使用・開示が問題になった事案であり、本項の設例のように、海外での使用・開示が問題となった事案ではない。
[18] なお、上記設例とは逆であるが、日本において技術の不正開示・使用をされたことを理由とする不法行為に基づく損害賠償請求及び当該不正使用行為等の差止請求を認容した米国判決を日本で執行しようとした場合については、最決平成 26 年 4 月 24 日民集 68 巻 4 号 329 頁を参照されたい。
[19] 正確には、平成 27 年改正では、「日本国内において事業を行う保有者の営業秘密」との改正内容であったところ、「限定提供データ保有者」という定義規定が創設された平成 30 年改正によって、「日本国内において事業を行う営業秘密保有者の営業秘密」と「営業秘密」が加えられたものである。
[20] 都道府県警本部には、営業秘密保護対策官が置かれている。また、全国都道府県警察営業秘密侵害事犯窓口については、右記資料 19 頁参照（経済産業省知的財産政策室「秘密情報の保護ハンドブックのてびき；情報管理も企業力」（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf））。

（６）サイバーセキュリティ対策について

上記のとおり、退職後にも秘密保持義務を負わせる契約が従業員・役員と締結されていた場合であっても、海外における元従業員・元役員による秘密情報の不正使用・不正開示を裁判等において差し止めるためには様々な論点に対応する必要が生じ得る。

そこで、例えば、元従業員・元役員に付与していた秘密情報への電磁的なアクセス権限を直ちに停止する、退職等の前に秘密情報の不正な持ち出しがないか技術的に確認するといったようなサイバーセキュリティ対策が重要であるといえる。加えて、従業員・役員に対し、秘密情報を持ち出していないか、企業に対して不満がないか等について在職中に定期的に確認する、退職予定者に対しインタビューするといったような対策も有用であるといえる。

３．参考資料（法令・ガイドラインなど）

・法適用通則法第 7 条、第 8 条、第 12 条、第 17 条、第 20 条
・民事訴訟法第 1 編第 2 章第 2 節
・不正競争防止法第 21 条第 4 項・第 5 項、第 21 条第 8 項

４．裁判例

本文中に記載のとおり

Q35 IoT 機器のセキュリティに関する法的対策

IoT 機器のセキュリティに関する法的対策として、どのような取組があるか。

タグ：電気通信事業法、国立研究開発法人情報通信研究機構法、IoT セキュリティガイドライン ver1.0、IoT セキュリティ総合対策、電気通信事業法に基づく端末機器の基準認証に関するガイドライン、米国カリフォルニア州 IoT セキュリティ法、IoT 機器、NOTICE

１．概要

平成 31 年 2 月から、脆弱な ID・パスワード設定等のためサイバー攻撃に悪用されるおそれのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取組である「NOTICE」[1]が実施されている。電気通信事業法（昭和 59 年法律第 86 号。以下、本項において「事業法」という。）の技術基準関係では、IoT 機器の技術基準において、セキュリティ対策が規定されている。電波法については Q38、電気用品安全法（昭和 36 年法律第 234 号）については Q37、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和 35 年法律第 145 号）ついては Q48 を参照されたい。

２．解説

（１）IoT 機器特有の性質について

IoT の進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT 特有の性質と想定されるリスクを踏まえたセキュリティ対策を行うことが必要とされている。一般的な IoT 機器特有の性質は次のとおりである[2]。

① 脅威の影響範囲・影響度合いが大きいこと

IoT 機器がひとたび攻撃を受けると、IoT 機器単体に留まらずネットワークを介して関連する IoT システム・サービス全体へ影響が波及する可能性が高い。

② IoT 機器のライフサイクルが長いこと

長期にわたって使用されるものも多く、構築・接続時に適用したセキュリティ対策が時間経過とともに危殆化した状態で、ネットワークに接続され続ける可能性がある。

③ IoT 機器に対する監視が行き届きにくいこと

IoT 機器の多くは画面がないため、利用者には IoT 機器に問題が発生していることがわかりづらく、勝手にネットワークにつながりマルウェアに感染する可能性がある。

④ IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること

[1] National Operation Towards IoT Clean Environment の略。
[2] IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン ver1.0」（平成 28 年 7 月）（https://www.soumu.go.jp/main_content/000428393.pdf）。

IoT 機器側とネットワーク側のそれぞれが有する業態の環境や特性が相互間で十分に理解されていないと、所要の安全や性能を満たすことができなくなる可能性がある。

⑤ IoT 機器の機能・性能が限られていること

センサー等のリソースが限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合がある。

⑥ 開発者が想定していなかった接続が行われる可能性があること

これまで外部につながっていなかったモノがネットワークに接続されることで、IoT 機器メーカーやシステム、サービスの開発者が当初想定していなかった問題が発生する可能性がある。

これらの性質と想定されるリスクがあることから、IoT 機器のセキュリティに関する法的な対策として、次に取り上げるものを中心とした取組が行われている。

（２）サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査

平成 31 年 2 月より、総務省、NICT 及びインターネット・サービス・プロバイダが連携し、サイバー攻撃に悪用されるおそれのある機器を調査し、利用者への注意喚起を行う取組である「NOTICE」が実施されている。

これは、国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号。以下、本項において「NICT 法」という。）第 14 条第 1 項第 7 号ロに基づき、サイバーセキュリティの確保のための措置を十分に講じていないと認められる電気通信設備の管理者その他の関係者に対して必要な助言及び情報を提供する業務として行われるものであり[3]、既に市場に出ている機器に関する対策として、具体的には、次の①～④の運用がされている[4]。

① 機器調査：NICT は、インターネット上の IoT 機器に対して、容易に推測されるパスワード等[5]を入力し、特定アクセス行為[6]を行うことができるかを確認すること

[3] NICT 法に基づく特定アクセス行為等の業務は令和 6 年 3 月 31 日までの期限であったが、令和 5 年 12 月に改正され、期限が撤廃された。

[4] NOTICE ウェブサイト参照（https://notice.go.jp/）。

[5] NICT 法第 18 条第 7 項第 1 号により、「不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさない」識別符号とされており、当該基準については、「特定アクセス行為等実施計画及び識別符号の基準に関する省令」（令和六年総務省令第十一号）第 3 条により、(1) 字数 8 以上であること、(2) これまで送信型対電気通信設備サイバー攻撃のために用いられたもの、同一の文字のみ又は連続した文字のみを用いたものその他容易に推測されるもの以外であることのいずれも満たすこととされている。当該基準を満たさないものとして、具体的には、①送信型対電気通信設備サイバー攻撃の実績のあるマルウェア（亜種含む）で利用されている識別符号、②同一の文字のみの暗証符号を用いているもの、③連続した文字のみの暗証符号を用いているもの、④連続した文字のみを繰り返した暗証符号を用いているもの、⑤機器の初期設定の識別符号（機器固有の識別符号が付与されていると確認されたものを除く。）が挙げられる。

[6] NICT 法第 18 条第 7 項第 1 号に定義されている。なお、同法に基づく NICT の業務として行われる特定アクセス行為については、不正アクセス禁止法に基づく不正アクセス行為から除外されている（不正アクセス禁止法第 2 条第 4 項第 1 号）。

などにより、サイバー攻撃[7]に悪用されるおそれのある機器を調査し、当該機器の情報をインターネット・サービス・プロバイダに通知する。総務省は、令和 2 年 9 月に、調査の取組強化として、特定アクセス行為において入力する識別符号（ID・パスワード）の追加、特定アクセス行為の送信元の IP アドレスの追加を認可している。

② 注意喚起：インターネット・サービス・プロバイダは、NICT から受け取った情報を元に該当機器の利用者を特定し、電子メールなどにより注意喚起を行う。

③ 設定変更等：注意喚起を受けた利用者は、注意喚起メールや NOTICE サポートセンターサイトの説明などに従い、パスワード設定の変更、ファームウェアの更新など適切なセキュリティ対策を行う。

④ ユーザサポート：総務省が設置する NOTICE サポートセンターは、ウェブサイトや電話による問合せ対応を通じて利用者に適切なセキュリティ対策等を案内する。

なお、NICT は、当該業務を行う場合、その一部として次に掲げる業務を行おうとするときは、総務大臣の認可を受けなければならない[8]。

① 特定アクセス行為を行うこと。

② 通信履歴等の電磁的記録を作成すること。

③ 特定アクセス行為に係る電気通信の送信先の電気通信設備が次に掲げる者の電気通信設備であるときは、それぞれに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと。

・電気通信事業者の電気通信設備：当該電気通信事業者へ通知

・電気通信事業者（事業法第 116 の 2 第 2 項第 1 号イに該当するものに限る。）の利用者の電気通信設備：当該電気通信事業者へ通知

NICT は、認可の申請に先立ち、特定アクセス行為等実施計画を作成し、総務大臣へ提出する義務を負い、当該計画には、実施期間、実施体制（委託時の選定基準・手続含む。）、

[7] 事業法第 116 条の 2 第 1 項第 1 号においては、「送信型対電気通信設備サイバー攻撃」（①設備攻撃（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち、送信先の電気通信設備の機能に障害を与える電気通信の送信（当該電気通信の送信を行う指令を与える電気通信の送信を含む。）により行われるもの）、又は②攻撃先設備探査（設備攻撃の送信先となる電気通信設備の探査のうち、電気通信事業者がその業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録により、設備攻撃に先立って行われる当該探査を目的とする電気通信の送信（当該電気通信の送信を行う指令を与える電気通信の送信を含む。）であることを合理的に特定できるものとして総務省令で定める電気通信の送信により行われるもの）に該当するもの）とされている。具体的には、DDoS 攻撃等を想定したものである。

[8] NICT 法第 18 条第 1 項各号。

用いる設備・識別符号、取得情報の適正取扱い確保措置（委託先での措置を含む。）等を記載しなければならない[9]。

（３）電気通信事業法の技術基準関係

利用者[10]は、電話機、FAX、モデム等の端末機器を電気通信事業者のネットワーク（電気通信回線設備）に接続し使用する場合、原則として、総務省令で定める技術基準（端末設備等規則（昭和 60 年郵政省令第 31 号））に適合しているもの（適合表示端末機器）を使用する必要がある。（事業法第 52 条及び第 69 条等）。

この技術基準は、①電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること、②電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること、③電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすること（事業法第 52 条第 2 項各号）の各事項が確保されるものとして、定められている[11]。

令和 2 年 4 月から、端末設備等規則に IoT 機器の技術基準にセキュリティ基準が追加された。新たに技術基準に位置づけられた具体的な内容は次のとおりである。インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、セキュリティ基準として、①アクセス制御機能、②アクセス制御の際に使用する ID/パスワードの適切な設定を促す等の機能、③ファームウェアの更新機能、又は①～③と同等以上の機能を具備すること、を追加した。なお、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ基準の対象外とされている。また、電気通信回線設備に直接接続して使用されない機器は認定等の対象外である。総務省は、端末設備等規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第 3 版）」[12]を策定・公表しているので、詳細については同ガイドラインも参照されたい。

さらに、上述のセキュリティ基準施行から 5 年が経過したことを踏まえ、端末設備等規則の見直しが令和 7 年 12 月に情報通信審議会から一部答申として示された。当該一部答申を踏まえ、端末設備等規則の一部改正等（大要、下表のとおり。）について、総務省

---

9 NICT 法第 18 条第 2 項及び第 3 項各号。なお、特定アクセス行為等実施計画の記載事項や識別符号の基準の詳細は、特定アクセス行為等実施計画及び識別符号の基準に関する省令（令和 6 年総務省令第 11 号）にて具体化されている。

10 「利用者」とは、電気通信事業者との間に電気通信役務の提供を受ける契約を締結する者をいう。エンドユーザのほか、電気通信事業者である者を含む（多賀谷一照監修「電気通信事業法逐条解説」（情報通信振興会、再訂増補版、令和 6 年）389 頁参照）。

11 以上①から③について、総務省ウェブサイト「端末機器に関する基準認証制度について」参照（https://www.soumu.go.jp/main_sosiki/joho_tsusin/tanmatu/index.html）。

12 https://www.soumu.go.jp/main_content/001033053.pdf

は、情報通信行政・郵政行政審議会に諮問を行い、令和 8 年 7 月 28 日、適当である旨の答申を受けた（令和 8 年 9 月 24 日公布、令和 9 年 4 月 1 日施行）。

主な見直し・検討事項	一部改正の概要・方向性
アクセス制御の際に使用する ID/パスワードの設定機能	・デフォルト ID/パスワードの設定及び当該 ID/パスワードからの変更にあたり「第三者から容易に推測されない」ものを設定・変更するよう技術基準に規定 ・デフォルト ID/パスワードの「変更を促す」という文言を「変更させる」に変更
ファームウェアの更新機能	・更新に関する具体的な基準・指標を総務大臣告示により規定
不要なインターフェースへの物理/論理アクセスに関する機能（現行規定なし）	・インターフェースへのアクセスに対しては、製造者が提供する意図を持つ通信機能以外について無効化しておくことを技術基準とする規定を新規追加
セキュリティ基準が適用される対象機器の範囲	・対象機器の範囲は、従前同様、「電気通信回線設備に直接接続される端末機器」。但し、間接的に接続される機器への適用要否も、今後の状況を踏まえた検討事項とする。
制度改正前に技術等適合認定等を受けた端末機器に対する経過措置	・従前同様の経過措置（制度改正前に認定等を受けた機器については再度認定等を受けることを求めない）を設けることを基本とし、周知活動等により置き換えを推進 ・既存機器のセキュリティリスクを継続的に注視し、特にリスクの高い機器が判明した場合等には個別に対策・対応を実施

（4）参考：米国カリフォルニア州 IoT セキュリティ法

米国カリフォルニア州では、IoT 機器のセキュリティ対策に関する法律[13]が 2018 年 9 月に成立し、2020 年 1 月から施行されている（詳細は Q83-1 参照）。同法では、接続される装置がローカルエリアネットワークの外部に認証手段を備えている場合、IoT 機器には、ユーザが IoT 機器に初めてアクセスする時に、ユーザが新しい認証手段を生成しなければならないようにするか、1 台ずつ固有のパスワードを設定して出荷するようにしなければならないというセキュリティ機能を含むことが必要とされている。日本の企業であっても、米国カリフォルニア州で販売されることとなる機器を製造する場合には、同法の対象となり得るので、注意が必要である。

3．参考資料（法令・ガイドラインなど）

・電気通信事業法

[13] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.91.05.&lawCode=CIV

・端末設備等規則
・端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）
・国立研究開発法人情報通信研究機構法
・IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン ver1.0」（平成 28 年 7 月）
・総務省「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第 3 版)」（令和 7 年 10 月 1 日）
・米国カリフォルニア州 IoT セキュリティ法

４．裁判例

特になし

Q36 IoT 製品のセキュリティ適合性に関する認証制度（JC-STAR）

IoT 製品のセキュリティ適合性に関する制度である JC－STAR の目的と JC－STAR による適合ラベルが付与される IoT 製品の対象範囲はどのようなものか。

タグ：IoT 機器、JC-STAR、適合ラベル、端末設備等規則

１．概要

JC-STAR（Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）は、日本の IoT 製品に対する適合基準への適合性を確認・可視化するため、令和 6 年に経済産業省が公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」[1]に基づき構築された制度である。インターネットに接続可能な IoT 製品を幅広く対象として、製品に具備されているセキュリティ機能を共通の物差しで評価・可視化することで消費者が容易にセキュリティ対策の施された製品を識別できるようにし、安全な製品選択を促進すること、及び日本における IoT 機器のセキュリティ水準の向上と国際的な整合性を図ることを目的としている。

２．解説

（１）制度運用について

JC-STAR は、IoT 製品のセキュリティ適合性を評価し、ラベルを付与する日本独自の制度である[2]。IPA が運営し、令和 7 年 3 月から運用が開始されている。

本制度の狙いは、IoT 製品の脆弱性対策（例：容易に推測できるパスワードの防止、セキュアなアップデートメカニズムの確保）を促進し、調達者や消費者がセキュリティ要件を満たした安全な製品を選びやすくすることである。評価レベルは★1 から★4 までの 4 段階が設定されており、★1・★2 は製品ベンダの自己適合宣言（自己評価方式）、★3・★4 は第三者機関による評価及び認証を基本とする。

[1] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf

[2] 制度としては日本独自のものだが、内容は欧州の標準規格である ETSI EN 303 645 や、米国の NISTIR8425 といった国際的な規格とも整合するものとして定められている。なお、同制度に基づく対応を講じることによって、製造物責任等の法的責任を問われなくなるという関係にはないため、留意されたい。

レベル	位置づけ	評価方式
★1	全 IoT 製品に共通の最低限のセキュリティ要件を定めている。チェックリストに基づく低コストな自己評価。	自己適合宣言
★2	★1 に要件を追加したもの。製品類型ごとの特徴（例：ネットワークカメラ、通信機器など）を考慮している。	自己適合宣言
★3 ／ ★4	政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定める。	第三者による評価・認証

これにより、IoT 製品ベンダへのインセンティブ付与や、諸外国の類似制度との国際連携、相互承認の推進も目指している。

本制度の対象となる製品には、適合基準への適合を示す目印として適合ラベルが付与される。ラベルには、適合するレベルに応じた 1 から 4 つの★と URL を埋め込んだ二次元バーコードが掲載されており、二次元バーコードを読み込むことで製品ごとの情報提供ページを閲覧できる。これにより、調達者や利用者は、適合ラベルの情報とセキュリティ情報・問い合わせ先等を一元的に確認することができる。

（２）適合ラベルが付与される IoT 製品の対象範囲

本制度における「IoT 製品」とは、「供給者による販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の IoT 機器、又は IoT 機器と必須付随サービスとで構成される一式」と定義されている[3]。また、「IoT 機器」とは「インターネットプロトコル（IP）を使用したデータの送受信機能を持つ、インターネットに接続可能な機器又は内部ネットワークに接続可能な機器（他の「インターネットに接続可能な機器」や「内部ネットワークに接続可能な機器」に接続し、IP を使用してデータを送受信する機能を持つ機器）であって、利用者自身によって、当該 IoT 機器本体に対してソフトウェア製品のインストール等により容易にセキュリティ対策を追加することが困難であるもの」を指し、「必須付随サービス」とは「IoT 製品が意図した目的を提供するために、IoT 機器と一体で提供することが必須となるデジタルサービス。当該 IoT 機器本体だけでは、当該 IoT 製品が意図した目的を提供できない場合に、当該 IoT 機器に付随して提供する」サービスを指す[4]。

上記の定義をまとめると、本制度の対象となる「IoT 製品」とは、以下のような製品が対象となる。

---

[3] IPA「セキュリティ要件適合評価及びラベリング制度の基本規程」（令和 7 年 7 月）1.4 参照（https://www.ipa.go.jp/security/jc-star/begoj90000003563-att/JSS-01.pdf）。

[4] 前掲注 3 参照。

① 機器が含まれていること（機器に対してラベルが付与される）
- ソフトウェアやクラウドサービスのみでは対象外となる。
- 必須付随サービス単体でも対象外である。

② インターネットプロトコル（IP）を使用したデータの送受信機能を持つこと

③ 直接・間接を問わず、インターネットにつながる（可能性がある／否定できない）こと
- インターネット側からの攻撃ができる可能性がある製品が対象となる。
- 論理的な制御（アクセスコントロール）によって分離されていても「インターネットにつながる可能性がある／否定できない」と判断される場合は対象となる。
- 物理的分離、又は完全な論理的切断による分離であれば、「インターネットにつながる可能性がない」と判断でき、ベンダが対象／対象外を判断できる。

④ 購入時に具備されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意志で）後からセキュリティ機能を追加することが困難／できないこと
- 利用者は購入時点で IoT 製品に具備されているセキュリティ機能を利用することになるため、必要なセキュリティ機能があらかじめ具備されていることを求めることが主眼である。
- 容易にセキュリティ機能を追加できる汎用 PC、スマートフォン、タブレット等は対象外となる。なお、汎用 OS を搭載した IoT 製品については、利用者が製品本体に容易にセキュリティ対策を追加できない場合は対象となる。

適合基準を満たせば、コンポーネントやモジュールでも理論的にラベルの取得は可能である。また、PC・タブレットベースの独自 IoT 製品も、特定の条件（セキュリティ機能のインストール制御、汎用 PC/タブレットとしての利用防止対策、汎用 OS ベンダ提供の脆弱性対応の適切なコントロール）を満たせばラベル取得が可能である。

また、電気通信回線設備に直接接続する端末機器に関する技術基準（セキュリティ基準）を定めた端末設備等規則との違いは、大要、以下のとおりである。

	端末設備等規則	JC-STAR
対象機器	・インターネットプロトコルを使用（データ通信） ・電気通信回線設備に直接接続	・インターネットプロトコルを使用（データ通信） ・インターネットに接続（直接・間接を問わない）
位置づけ	・強制規格（技術基準適合認定等に必須）	・任意規格、自己宣言（★1・2）

	端末設備等規則	JC-STAR
趣旨	・電気通信回線設備に障害を与えない ・他の利用者に迷惑を及ぼさない等	・IoT 製品として共通して求められる最低限のセキュリティ要件（★1・2）を備えさせること等
セキュリティ項目	・アクセス制御機能 ・ID/PW の適切な設定を促す等の機能 ・ファームウェアの更新機能	・左記項目（一部の項目では、より詳細な規定） ・インターフェースへの論理アクセス ・IoT 機器内のデータ保護 ・製品ベンダーに関する適合基準

（３）現在の運用状況と今後の展望

本書基準日時点においては、★1 の申請受付と適合製品の公開が始まっている。今後、本制度に関する各業界団体やワーキンググループにおける検討を踏まえて、★2 以降の基準についても、製品区分ごとに順次整備予定である（令和 7 年 11 月、通信機器及びネットワークカメラそれぞれについて、★3 の要件・適合基準案について意見公募を実施し、令和８年２月にセキュリティ要件を公開）。セキュリティ要件に応じたラベルを付与することで、IoT 製品ベンダーへのインセンティブ、IoT 製品の付加価値向上に繋げるべく、政府機関等、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高く確かな制度利用が見込まれる組織の IoT 製品の調達要件の中にラベルが付与された製品の選定を含める方向で取組が進められている。

（４）関連する諸外国の制度

以上のような日本のセキュリティ適合を示す認証制度と同趣旨の制度として、米国の Cyber Trust Mark、NIST SP800-213、EU の Cyber Resilience Act（CRA）、ドイツの IT セキュリティラベル、英国の Product Security and Telecommunications Infrastructure Act 2022（PSTI）等が挙げられる。

制度間の手続簡略化、JC-STAR の国際的な認知度向上、適切なセキュリティ対策が講じられている IoT 製品の国際的な普及等を目的として、JC-STAR と諸外国の制度との相互承認の取組も進められており、2026 年 1 月には英国の Product Security and Telecommunications Infrastructure Act 2022（PSTI）と、2026 年 6 月にはシンガポールの Cybersecurity Labelling Scheme(CLS)との相互承認制度の運用がそれぞれ開始されている。こうした類似制度との相互承認を通じ、制度間の相互運用性を高め、グローバル企業にとってのサイバーセキュリティ製品認証取得のインセンティブを高め、適切な

セキュリティ基準を講じた IoT 製品の国際的な普及等への貢献が期待される。これらの制度の詳細については、Q83-1、Q83-2、Q83-3 を参照されたい。

３．参照資料（法令・ガイドラインなど）

・経済産業省商務情報政策局サイバーセキュリティ課「IoT 製品に対するセキュリティ適合性評価制度構築方針」（令和 6 年 8 月）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf
・IPA「セキュリティ要件適合評価及びラベリング制度の基本規程」（令和 7 年 7 月）
https://www.ipa.go.jp/security/jc-star/begoj90000003563-att/JSS-01.pdf
・IPA「IoT 製品のセキュリティ確保に向けて ～セキュリティ要件適合評価及びラベリング制度(JC-STAR)の紹介～」（令和 6 年）
https://www.ipa.go.jp/security/jc-star/begoj9000000gg60-att/JC-STARsetumeikai_1.pdf
・IPA「JC-STAR 制度に対するよくある質問について」（令和 6 年）
https://www.ipa.go.jp/security/jc-star/begoj9000000gg60-att/JC-STARsetumeikai_2.pdf
・IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」（最終更新日：令和 7 年 3 月 28 日）
https://www.ipa.go.jp/security/jc-star/detail.html
・情報通信技術分科会 IP ネットワーク設備委員会「『ネットワークの IP 化に対応した電気通信設備に係る技術的条件』（平成 17 年 10 月 31 日付諮問第 2020 号）のうち『端末機器の技術基準等への適合性に係る セキュリティ基準の見直し』の検討開始について」
https://www.soumu.go.jp/main_content/001012910.pdf
・IPA「申請手続き・報告手続き」
https://www.ipa.go.jp/security/jc-star/shinsei/index.html
・IPA「英国 PSTI 法適合の相互承認申請について」（最終更新日：令和 8 年 6 月 1 日）
https://www.ipa.go.jp/security/jc-star/shinsei/psti.html
・IPA「シンガポール CLS 適合の相互承認申請について」（最終更新日：令和 8 年 7 月 1 日）
https://www.ipa.go.jp/security/jc-star/shinsei/cls.html

４．裁判例

特になし

Q37 IoT 機器からのデータ漏えいにおける製造者の責任

IoT 機器からデータが漏えいした場合、同機器の製造者はデータ漏えいの被害者に対して、どのような責任を負うおそれがあるか。

タグ：民法、製造物責任法、IoT 機器、データ漏えい、製造者責任、NIST

１．概要

IoT 機器にデータ漏えいの原因があった場合、同機器の製造者は、データ漏えいの被害者に対して、不法行為又は債務不履行に基づく責任のほか、製造物責任を負う可能性がある。

第三者又は利用者に原因があった場合、同機器の製造者は、原則として責任を負わないと考えられる。なお、製造者でも、初めての利用時に、パスワード変更が必要な仕様とするなど、利用者保護のための対策を講じることが望ましい。

２．解説

（１）IoT 機器の特徴

IoT 機器はネットワークにつながっているため、従来の機器に比べると、データ漏えいが生じるリスクが高く、かつ漏えいが生じた場合にその影響が広範囲に及ぶ可能性もある。さらに、ネットワークにつながることで、データ漏えいの原因が解明しづらくなることから、製造者だけではなく、IoT 機器を利用したサービスを提供する第三者を含む多数の者が当該漏えいによる被害者から責任追及され得るという特徴がある。

IoT 機器からデータが漏えいした場合、① IoT 機器に原因があった場合、② IoT 機器を利用したサービスを提供する第三者に原因があった場合、③ 利用方法が不適切であったなど利用者に原因があった場合、④ ①～③の原因が複合的にあった場合に大きく分類できる。以下、それぞれの場合に分けて、IoT 機器の製造者がデータ漏えいの被害者に対して負う可能性がある民事上の責任について検討する。なお、データ漏えい時における損害額については、Q63 を参照されたい。

（２）IoT 機器の製造者がデータ漏えいの被害者に対して負う可能性がある民事上の責任

ア　IoT 機器に原因があった場合

製造者は、被害者から、不法行為（民法第 709 条）又は債務不履行（民法第 415 条）に基づく損害賠償責任を負う可能性がある。

被害者が不法行為責任（民法第 709 条）を追及する場合、製造者に故意又は過失があったことなどの要件を証明する必要がある。もっとも、製造物責任法（平成 6 年法律第

85 号）第 3 条では、「製造業者等[1]は、その製造……した製造物であって、その引き渡したものの欠陥により他人の生命、身体又は財産を侵害したときは、これによって生じた損害を賠償する責めに任ずる」とし、被害者は、製造物に欠陥があることを証明すれば足り、製造者（同法上では、製造業者等）に故意又は過失があったことを証明する必要まではないとされている。

ここで、「製造物」とは、製造又は加工された動産をいい（製造物責任法第 2 条第 1 項）、「欠陥」とは、当該製造物の特性、その通常予見される使用形態、その製造業者等が当該製造物を引き渡した時期その他の当該製造物に係る事情を考慮して、当該製造物が通常有すべき安全性を欠いていることをいうとされている（同条第 2 項）。IoT 機器に欠陥があり、これを原因としてデータ漏えいがあり、損害が生じた場合には、製造物責任法上の製造物責任を負う可能性がある[2]。

被害者は、上記の不法行為責任（民法第 709 条）のほかに、債務不履行責任（民法第 415 条）による責任を追及することも考えられるが、被害者と製造業者との間に直接的な契約関係の存在が必要とされることなどからすると、不法行為責任に基づく責任追及が一般的と考えられる。

もっとも、製造物責任法は、①被害者又はその法定代理人が損害及び損害賠償義務者を知った時から 3 年間行使しないとき又は②その製造業者等が当該製造物を引き渡した時から 10 年を経過したときには、損害賠償の請求権が時効によって消滅する（製造物責任法第 5 条第 1 項）ため、注意が必要である。ただし、人の生命又は身体を侵害した場合における損害賠償の請求権の消滅時効においては、上記①について、被害者又はその法定代理人が損害及び損害賠償義務を知った時から 5 年間行使しないときとされている（同条第 2 項）[3]。

---

[1] 製造物責任法では、「製造業者等」とは、次のいずれかに該当する者をいうとされている（製造物責任法第 2 条第 3 項）。
① 当該製造物を業として製造、加工又は輸入した者（以下単に「製造業者」という。）
② 自ら当該製造物の製造業者として当該製造物にその氏名、商号、商標その他の表示（以下「氏名等の表示」という。）をした者又は当該製造物にその製造業者と誤認させるような氏名等の表示をした者
③ 前号に掲げる者のほか、当該製造物の製造、加工、輸入又は販売に係る形態その他の事情からみて、当該製造物にその実質的な製造業者と認めることができる氏名等の表示をした者

[2] 製造物責任法上の責任が生じる要件として「人の生命、身体又は財産を侵害したとき」（製造物責任法第 3 条）に該当する必要があるところ、クレジットカード情報のような情報の漏えいによって不正利用がされる等により財産的被害が発生した場合には同要件に該当する可能性があるものの、単なる個人データの漏えいの場合に、同要件を充足するか否かは個別具体的な事情に即した検討を要すると考えられる。

[3] なお、参考として、電気用品（電気事業法（昭和 39 年法律第 170 号）にいう一般電気工作物の部分となり、又はこれに接続して用いられる機械、器具又は材料をいう。例えば、電気温水器、電気マッサージ器、電気冷蔵庫などがこれにあたる）については、電気用品安全法が適用される。

イ　IoT 機器を利用したサービスを提供する第三者に原因があった場合

第三者（サービスプロバイダやアプリケーション開発者・提供者）が IoT 機器を利用したサービスを提供している場合に、IoT 機器自体ではなく、サービスの内容が原因で、データが漏えいしたケース、例えば、IoT 機器からデータが送信される先におけるサーバのセキュリティ設定が適切ではなく、外部にデータが流出してしまったケースである。データ漏えいの被害者との関係では、当該第三者が、不法行為（民法第 709 条）又は債務不履行（同法第 415 条）に基づく損害賠償責任を負う可能性がある。この場合、IoT 機器の製造者は、IoT 機器に関する当該第三者への説明に過誤があったなどの特別な事情がない限り、責任を負わないと考えられる。

ウ　利用者に原因があった場合

利用者が容易に予測可能なパスワードを使用利用していた（当該利用者のみに漏えいが生じた）場合など、利用者のみに漏えいの原因があった場合には、利用者に責任があることとなり、この時には、IoT 機器の製造者は法的な責任は負わないと考えられる。もっとも、IoT 機器に固有のパスワードが振られていてユーザが変更できないなど、利用者にだけ漏えいの原因があったと直ちにはいえない場合には、製造者が責任を負う可能性がある。製造者においても、利用者が初めて利用をする際にパスワード変更が必要な仕様とするなど、利用者保護のための対策を講じることが望ましい[4]。

エ　ア～ウの原因が複合的に存在した場合

上記アからウのいずれか一つだけでなく、複合的な原因でデータ漏えいするケースも考えられる。この場合、利用者に原因があったことは、過失相殺（民法第 418 条、第 722 条第 2 項）の対象となる。なお、訴訟提起などの段階でデータ漏えいの原因が明確になっているとは限らず、被害者は、上記アからウのいずれの場合においても、IoT 機器自体にも欠陥があったとして、製造者やサービス提供者に対して、共同不法行為（民法第 719 条）などに基づく損害賠償を請求する可能性があるので、注意が必要である。

（3）（参考）英国における 13 項目のベストプラクティス

英国政府（当時のデジタル・文化・メディア・スポーツ省（DCMS））は、2018 年 10 月に IoT 製品を利用する消費者のセキュリティに関する負担を軽減するデザイン（セキュア・バイ・デザイン）とすることを目的として、製造者等が IoT 製品の開発、製造及び販売の段階で安全を確保するために実践すべき対策について、「Code of Practice for Consumer IoT Security」を公表し、製造・開発・販売等を行う各事業者が遵守すべき 13

[4] IoT 機器がインターネット回線に直接つながる場合には、Q35 の 2(3)電気通信事業法の技術基準関係を参照。

項目のベストプラクティスを示した[5]。具体的な項目は次のとおりであるが、参考に当たっては法制などの違いについても留意する必要がある。

① デフォルトパスワードを使用しない	⑧ 個人データの保護を徹底する
② 脆弱性の情報公開ポリシーを策定する	⑨ 機能停止時の復旧性を確保する
③ ソフトウェアを定期的に更新する	⑩ システムの遠隔データを監視する
④ 認証情報とセキュリティ上重要な情報を安全に保存する	⑪ 消費者が個人データを容易に削除できるように配慮する
⑤ 安全に通信する	⑫ デバイスの設置とメンテナンスを容易にできるように配慮する
⑥ 攻撃対象になる場所を最小限に抑える	⑬ 入力データを検証する
⑦ ソフトウェアの整合性を確認する	

その後、Code of Practice for Consumer IoT Security をベースに、欧州の標準化機関（European Telecommunications Standards Institute（ETSI））が消費者向け IoT のセキュリティ・ベースラインを規定する欧州規格（ETSI EN 303 645）を策定した[6]。

さらに、英国は Product Security and Telecommunications Infrastructure Act 2022（PSTI 法）[7]と、その委任にもとづく 2023 年規則（SI 2023/1007）[8]により、消費者向けコネクタブル製品（relevant connectable products）について、①共通・既定パスワードの禁止（推測容易なデフォルトは不可）、②脆弱性報告の連絡窓口の公表（受領・対応のための連絡先明示）、③セキュリティ更新の提供期間に関する情報の公表（最低何年更新されるか等の明示）という 3 つの最低限のセキュリティ要件を法制化した[9]。これらは、Code of Practice for Consumer IoT Security 及び欧州規格のコア部分に対応する法的なベースラインとして位置づけられる。

日本の IoT 機器メーカーが英国市場（越境 EC や英国向け OEM 含む。）に製品を供給する場合、上記の最低限の 3 要件への対応は法的な義務であり、設計（初期パスワード仕様）、開示（更新期間・連絡窓口の表示）、体制（脆弱性受付・対応プロセス）について、当該要件に合わせて準備する必要がある。また、英国市場向けの輸出・販売事業者（商社・小売・越境 EC 運営者等）は、輸入業者・流通業者としての義務（適合声明、調査、記録

[5] Department for Digital, Culture,Media & Sport, Guidance Code of Practice for consumer IoT security（https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security）

[6] なお、英国政府は、「Code of Practice for Consumer IoT Security」と ETSI EN 303 645 を英国の最低基準の根拠として並列に位置づけている（GOV UK「Secure by design」（https://www.gov.uk/government/collections/secure-by-design））。

[7] Legislation.GOV.UK「Product Security and Telecommunications Infrastructure Act 2022」（https://www.legislation.gov.uk/ukpga/2022/46/contents）

[8] Legislation.GOV.UK「The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023」（https://www.legislation.gov.uk/uksi/2023/1007/contents）

[9] GOV UK「Regulations: consumer connectable product security」（https://www.gov.uk/guidance/regulations-consumer-connectable-product-security）

保持、是正等）を理解し、メーカーから適合に必要な情報の提供を受け、表示・記録を整備する必要がある。

なお、EU では、2024 年 12 月 8 日付の製造物責任指令（Directive (EU) 2024/2853）（Product Liability Directive）[10]改正により、業務目的で使用されることのない「データ」の「損壊（destruction）」又は「破損」（corruption）は損害賠償請求の対象として規定された。しかし、データの「漏洩」は、「損壊」や「破損」とは区別され、同指令の対象として規定されていない。

（４）（参考）米国国立標準技術研究所（NIST）の NIST Cybersecurity for IoT Program

米国国立標準技術研究所（NIST）は、IoT に対する信頼を醸成するとともにスタンダード、ガイダンス及び関連するツールを通じてグローバルスケールのイノベーションを可能とすることを目的として「NIST Cybersecurity for IoT Program」[11]を確立している。

かかるプログラムにおいては、多数のガイドラインやベースラインを公表しており、例えば、以下のようなものがある。なお、2024 年 9 月には、米国の連邦通信委員会（FCC）による「Cybersecurity Labeling for Internet of Things」[12]が発効されており、そこでは「Profile of the IoT Core Baseline for Consumer IoT Products」（NISTIR 8425）が適合性基準として用いられるものとされている。

- SP 800-213 – IoT Device Cybersecurity Guidance for the Federal Government Establishing IoT Device Cybersecurity Requirements[13]
- SP 800-213A – IoT Device Cybersecurity Guidance for the Federal Government[14]
- NISTIR 8259B – IoT Non-Technical Supporting Capability Core Baseline[15]
- NISTIR 8425 – Profile of the IoT Core Baseline for Consumer IoT Products[16]

３．参考資料（法令・ガイドラインなど）

・民法第 415 条、第 418 条、第 709 条、第 719 条、第 722 条第 2 項
・製造物責任法（平成 6 年 7 月 1 日法律第 85 号）第 2 条、第 3 条

---

[10] Directive (EU) 2024/2853（https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng）
[11] NIST Cybersecurity for IoT Program（https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program）
[12] Cybersecurity Labeling for Internet of Things（https://www.federalregister.gov/documents/2024/07/30/2024-14148/cybersecurity-labeling-for-internet-of-things）
[13] IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (nist.gov)
[14] IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog (nist.gov)
[15] NISTIR 8259B – IoT Non-Technical Supporting Capability Core Baseline（https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259B.pdf）
[16] NISTIR 8425 – Profile of the IoT Core Baseline for Consumer IoT Products（https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf）

・経済産業省商務情報政策局サイバーセキュリティ課「『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性」（令和元年 8 月）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/index.html

４．裁判例

特になし

Q38 ドローンとサイバーセキュリティ

ドローンの活用が拡大する中で法規制も整備されているが、サイバーセキュリティの関係でどのような点に留意すべきか。

タグ：航空法、登録制度、リモート ID、機体認証制度、操縦ライセンス制度、政府機関等における無人航空機の調達等に関する方針について

１．概要

ドローンの飛行は航空法（昭和 27 年法律第 231 号）、重要施設の周辺地域の上空における小型無人機等の飛行の禁止に関する法律（平成 28 年法律第 9 号。以下、本項において「小型無人機等飛行禁止法」という。）及び電波法等による規制を受ける。

ドローンについても、ユーザが意図しないプログラムの更新や飛行・撮影情報の外部漏えい、他人による機体制御乗っ取り等のサイバーセキュリティ上のリスクが指摘されている。

２．解説

（１）ドローンを規制する法律の概要

ア　航空法

平成 27 年 4 月 22 日に首相官邸に落下したドローンが発見された事件を契機として、ドローンに関する規制の必要性が認識されたことにより、平成 27 年 12 月に航空法が改正された。当該改正により、「無人航空機」（航空法第 2 条第 22 項）の定義が創設され、その飛行禁止空域（当該空域の飛行には国土交通大臣の許可が必要）及び飛行の方法に関する規制（当該方法によらない飛行には国土交通大臣の承認が必要）が導入された。

さらに、令和 2 年の航空法改正により、「無人航空機」の登録制度が導入され、令和 4 年 6 月 20 日より当該登録制度に基づく登録が義務化された（義務化に先立ち令和 3 年 12 月 20 日から事前登録が開始された。）。

かかる登録制度において、登録を受けた無人航空機の所有者は、その登録記号を当該無人航空機に表示するなど、登録記号が識別できるような措置を講じる必要がある。具体的には、機体表面への物理的な表示及びリモート ID 機能の搭載の両方の措置を講じることが原則として求められる（航空法施行規則第 236 条の 6 第 1 項）。このうち、リモート ID 機能とは、登録記号を識別するための信号を、電波を利用して送信することにより、遠隔で無人航空機の識別をその飛行中常時可能とする機能をいい（航空法施行規則第 236 条の 3 第 1 項第 13 号）、リモート ID 機能による遠隔識別を確実に行うため、リモート ID 機器の製造及び開発にあたり従うべき要件が「リモート ID 技術規格書」に定められている。

さらに、令和 3 年の航空法改正により以下のカテゴリー区分及び制度が新たに導入された。

（ア）カテゴリー区分

飛行のリスクに応じて、リスクの高いものから、「カテゴリーIII」、「カテゴリーII」及び「カテゴリーI」という 3 つのカテゴリーが設定されている。

「カテゴリーIII」は、飛行ごとに許可・承認を要する空域及び飛行方法での飛行（以下、本項において「特定飛行」という。）（航空法第 132 条の 87）であって、操縦者及び操縦補助者以外の立入りを管理する措置（以下、本項において「立入管理措置」という。航空法第 132 条の 85 第 1 項）を講じない飛行（レベル 4 相当の第三者上空の飛行）をいい、後述する第一種機体認証（航空法第 132 条の 13 第 2 項第 1 号）及び一等無人航空機操縦士のライセンス（同法第 132 条の 42 第 1 号）が必要となり、飛行ごとに許可・承認が必要となる（同法第 132 条の 85 第 2 項、第 132 条の 86 第 3 項）。

「カテゴリーII」は、飛行ごとに許可・承認を要する「特定飛行」であって、「立入管理措置」を講じる飛行をいい、後述する第二種機体認証（航空法第 132 条の 13 第 2 項第 2 号）及び二等無人航空機操縦士のライセンス（同法第 132 条の 42 第 2 号）があれば、一定の要件のもとで飛行ごとの許可・承認が不要とされている（同法第 132 条の 85 第 2 項、第 132 条の 86 第 3 項）。

「カテゴリーI」は、航空法上、許可・承認が不要とされる飛行（「特定飛行」に該当しない飛行）をいう。

（イ）機体認証制度

機体認証は、申請により国土交通大臣が行い（航空法第 132 条の 13 第 1 項）、第一種機体認証及び第二種機体認証に区分される（同条第 2 項）。第一種機体認証は、カテゴリーIII の飛行を行うことを目的とする無人航空機を対象とするものであり（同項第 1 号）、他方、第二種機体認証は、カテゴリーII の飛行を行うことを目的とする無人航空機を対象とする（同項第 2 号）。

（ウ）操縦ライセンス制度

機体認証制度とともに操縦ライセンス制度として「無人航空機操縦者技能証明」制度が導入された。無人航空機操縦者技能証明は、無人航空機を飛行させるために必要な技能について、申請により国土交通大臣が行い（航空法第 132 条の 40）、一等無人航空機操縦士及び二等無人航空機操縦士に区分される（同法第 132 条の 42）。一等無人航空機操縦士は、カテゴリーIII の飛行に必要な技能を対象とするものであり（同条第 1 号）、他方、二等無人航空機操縦士は、カテゴリーII の飛行に必要な技能を対象とする（同条第 2 号）。

イ　小型無人機等飛行禁止法

平成 27 年の航空法改正と同様に、首相官邸にドローンが落下した事件を契機として、小型無人機等飛行禁止法が制定され、平成 28 年 4 月から施行されている。

同法は、国会議事堂、内閣総理大臣官邸その他の国の重要な施設等、外国公館等、防衛関係施設（令和元年の改正で追加）、空港（令和 2 年の改正で追加）及び原子力事業所を「対象施設」（同法第 2 条第 1 項）と定め、当該対象施設の敷地又は区域及びその周囲おおむね 1,000m（令和 8 年の改正で 300m から拡大）の地域を、「対象施設周辺地域」（同条第 2 項）として指定し、その上空におけるドローンを含む小型無人機等の飛行を原則として禁止している（同法第 10 条第 1 項）。警察庁ウェブサイト「小型無人機等飛行禁止法関係」[1]では、対象施設の一覧や対象施設周辺地域の範囲、飛行禁止の例外に当たる場合に必要な通報手続等が公表されている。

ウ　電波法

ドローンの飛行においては電波の利用は不可欠であることから、電波法の規制にも服する。

電波法上、電波を発する無線設備の使用（無線局の開設）には、原則として総務大臣の免許が必要となる（電波法第 4 条）。ただし、発射する電波が著しく微弱な無線局や、特定の用途に用いる小電力の無線局等については、例外的に免許は不要とされており（電波法第 4 条但書、電波法施行規則第 6 条）、市販のホビー用ドローンに使用される無線設備は、基本的にかかる免許不要の場合に該当する。他方で、産業用ドローンについては、平成 28 年の電波法施行規則等の改正により導入されたロボット用の電波（無人移動体画像伝送システム）が用いられることが多く、かかる電波を使用する場合には、免許が必要となる。詳細については総務省ウェブサイト「ドローン等に用いられる無線設備について」[2]を参照されたい。

（２）ドローンのサイバーセキュリティに関する留意点

ドローンの中には、スマートフォン等を介して外部データセンターとの飛行・撮影情報のやり取りや、プログラム更新を行う機種が存在し、また、ドローンは一般的に無線回線で機体が制御されている。そのため、ユーザが意図しないプログラムの更新や飛行・撮影情報の外部漏えい、他人による機体制御乗っ取り等のサイバーセキュリティ上のリスクが指摘されている（内閣官房「ドローンに関するセキュリティリスクへの対応について」

[1] 警察庁「小型無人機等飛行禁止法関係」（https://www.npa.go.jp/bureau/security/kogatamujinki/index.html）。
[2] 総務省電波利用ポータル「ドローン等に用いられる無線設備について」（https://www.tele.soumu.go.jp/j/sys/others/drone/）。

（令和 2 年 9 月 14 日）[3]。そこで、内閣官房は、令和 2 年 9 月 14 日、関係省庁で申合せを行った「政府機関等における無人航空機の調達等に関する方針について」[4]を公表し、以下の業務に用いられるドローンについては、令和 3 年度以降の新規調達に当たって、サプライチェーン・リスクの少ない製品を採用するために、セキュリティ上の疑義に留意した「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」[5]と同様の措置を講ずることとした。

① カメラやセンサーから収集される情報の窃取や飛行記録データ（時間・場所）の窃取により、活動内容が推測され得ることで、公共の安全と秩序維持に関する業務の円滑な遂行に支障が生じるおそれがある業務（例：防衛、領土・領海保全、犯罪捜査・警備等）

② カメラやセンサーから収集される情報の窃取により、公共の安全と秩序維持等に支障が生じるおそれがある業務（例：国民保護法の生活関連等施設の脆弱性に関する情報を収集する業務（点検等）等）

③ 人命に直結する業務であって、無人航空機の適時適切な飛行が妨げられる（例：無人航空機が突然動かなくなる）ことで、その遂行に支障が生じるおそれがある業務（救難、救命等の緊急対応業務等）

なお、ドローンのセキュリティに関して、IPA 産業サイバーセキュリティセンターは、令和 3 年 6 月、ドローンの歴史や基礎的な機能・仕様、法規制、利活用シーン、ドローンの事故攻撃と防御事例の紹介を踏まえて、ドローンに対するサイバー攻撃（脆弱性）とその対策を検証し、安全に利活用するための勘どころについて取りまとめた「ドローンサイバーセキュリティハンドブック～安全なドローン利活用の勘どころ～」[6]を公表しており参考になる。

また、経済産業省及び国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）は、ドローン等の無人航空機システムの情報漏えい対策が求められていることを受け、令和 4 年 3 月に、「無人航空機分野サイバーセキュリティガイドライン」[7]を公表している。本ガイドラインは、無人航空機システムが活用される用途と扱われる情報の特性を踏まえつつ、機体メーカーやサービス事業者からユースケースごとの情報資産やセキュリテ

---

[3] 内閣官房「ドローンに関するセキュリティリスクへの対応について」（https://www.kantei.go.jp/jp/singi/kogatamujinki/dai10/siryou1.pdf）。

[4] 政府機関等における無人航空機の調達等に関する方針について（https://www.kantei.go.jp/jp/singi/kogatamujinki/pdf/siryou15.pdf）。

[5] この申合せについては Q53 を参照。「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（https://www.cyber.go.jp/pdf/policy/general/ref_moushiawase.pdf）。

[6] ドローンサイバーセキュリティハンドブック～安全なドローン利活用の勘どころ～（https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002jq9-att/000092207.pdf）。

[7] 経済産業省及び国立研究開発法人新エネルギー・産業技術総合開発機構「無人航空機分野サイバーセキュリティガイドライン Ver.1.0 非耐空性の領域における情報セキュリティの対応指針」（令和 4 年 3 月）（https://www.nedo.go.jp/content/100944342.pdf）。

ィ要件等をヒアリングした結果を反映することで、より実務的・実践的な情報セキュリティ上の対策がまとめられており、参考になる。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

Q39 モビリティとサイバーセキュリティ

移動サービスが多様化している中、法令上、どのようなサイバーセキュリティ対策が求められているか。

タグ：自動運転、道路運送車両法、道路交通法、WP29

１．概要

自動運転をはじめとする先進的なモビリティサービス[1]の普及への期待が高まる中で、自動運転に向けた法整備が進みつつある。道路運送車両法（昭和 26 年法律第 185 号）の令和元年改正により、道路運送車両の保安基準の対象装置に自動運行装置が追加されるとともに、その施行に併せて、国際基準に沿う形で自動車の電気装置に関するサイバーセキュリティ確保のための技術基準やサイバーセキュリティ業務管理システムが適合すべき技術基準も設けられた。

その後、国際基準（UN Regulation No.155）が正式に発効されたことを受けて、サイバーセキュリティに関する保安基準は、国際基準を直接引用する形式に改正されるとともに、その適用対象は、自動運転車以外の従来の自動車全般にも拡大されることとなった。

２．解説

我が国においては、地方では超高齢に伴う地域の交通サービスの縮小や交通手段の確保が課題となっており、都市部では道路混雑や交通による環境負荷が課題となっている。そこで、このような社会課題を背景に、自動運転をはじめとする先進的なモビリティサービスの普及への期待が高まっている。

本項では、モビリティサービスの中でも、自動車の自動運転に向けた法整備及び自動車のサイバーセキュリティに関する法整備について解説する。

（１）自動運転に向けた法整備について

ア　自動運転について

米国の SAE（Society of Automotive Engineers（自動車技術会））による運転自動化レベルはレベル 0 からレベル 5 まで定義されている。レベル 3（条件付自動運転）は、場所（高速道路のみ等）、天候（晴れのみ等）、速度などの特定条件下においてシステムが運転を実施するもの（当該条件を外れる等、作動継続が困難な場合は、システムの介入要求等に対して運転者が適切に対応することが必要）、レベル 4（特定条件下における

[1] 例えば、他にも MaaS 等が挙げられる。MaaS（Mobility as a Service）とは、地域住民や旅行者一人一人のトリップ単位での移動ニーズに対応して、複数の公共交通やそれ以外の移動サービスを最適に組み合わせて検索・予約・決済等を一括で行うサービスをいう。

完全自動運転）は、特定条件下においてシステムが運転を実施するもの（作動継続が困難な場合もシステムが対応）、レベル 5（完全自動運転）は、常にシステムが運転を実施するものとされている[2]。

国内では、自動車の運転者のミスに起因する交通事故の大幅な削減が期待するものとして[3]、自動運転の実現に向けて、道路運送車両法及び道路交通法（昭和 35 年法律第 105 号）[4]の改正が行われている[5]。

イ　道路運送車両法の改正

令和元年 5 月、自動運転車等の安全性を確保するため、道路運送車両法の改正法が公布され、道路運送車両の保安基準（昭和 26 年運輸省令第 67 号。以下、本項において「保安基準」という。）[6]の対象装置に自動運行装置が追加された（道路運送車両法第 41 条第 1 項第 20 号。令和 2 年 4 月 1 日施行）。自動運行装置とは、国土交通省が付する条件（走行環境条件）で使用する場合において、運転者の操作に係る認知、予測、判断、操作に係る能力の全部を代替する機能を有するものをいう[7]。自動車は、その装置が保安基準に適合するものでなければ運行の用に供してはならないため（同法第 41 条）、自動運転のための装置を備える自動車は、自動運行装置に関する保安基準に適合する必要がある。

併せて、サイバーセキュリティに関する保安基準も定められたが、これについては下記（２）で解説する。

ウ　道路交通法の改正

道路運送車両法の改正と同時になされた、道路交通法令和元年改正により、①自動運行装置の定義等に関する規定の整備、②自動運行装置を使用する運転者の義務に関する

---

[2] 国土交通省「自動運転車の定義及び政府目標」（https://www.mlit.go.jp/report/press/content/001371533.pdf）。

[3] デジタル庁「AI 時代における自動運転車の社会的ルールの在り方について」（(https://www.cao.go.jp/consumer/iinkai/2024/442/doc/20240807_shiryou1-1.pdf)。

[4] 道路運送車両法は、自動車の車体の規格等（車両の安全基準）を定めているのに対し、道路交通法は自動車の運転に関して遵守すべき規律（交通ルール）を定めている。

[5] なお、国土交通省が設置した自動運転における損害賠償責任に関する研究会による報告書では、ハッキングにより引き起こされた事故の損害（自動車の保有者が運行供用者責任を負わない場合）の責任の所在等について、①ハッキングにより第三者が保有者に無断で車両を操縦した場合、保有者の運行支配・運行利益は原則失われ、保有者は運行供用者責任を負わないこと、②被害者救済は政府保障事業（自動車損害賠償保障法（昭和 30 年法律第 97 号）第 72 条）で行うこと、③ハッキングが自動運転システムの欠陥に起因する場合、政府は填補後にメーカー等へ求償し得ること、④保守点検等の義務懈怠があれば保有者が責任を負う可能性があること等が示されている（国土交通省自動車局「自動運転における損害賠償責任に関する研究会 報告書」2－2（論点②）（https://www.mlit.go.jp/common/001226365.pdf））。

[6] 道路運送車両法第 3 章においては、自動車の構造・装置について、安全確保及び環境保全上の技術基準を省令に定める旨が規定されており、当該省令を道路運送車両の保安基準という。

[7] 国土交通省 自動車局 技術・環境政策課「自動運行装置の保安基準の概要」（https://www.npa.go.jp/bureau/traffic/council/jidounten/R03nendo/2021dai1kaishiryou2.pdf）。

規定の整備、及び③作動状態記録装置による記録等に関する規定の整備が行われ[8]（令和 2 年 4 月 1 日施行）、これによって SAE レベル 3 の自動運転車が公道を走行するための規定が整備された。

また、限定地域における遠隔監視のみの無人自動運転移動サービス（SAE レベル 4）の実用化を念頭に、令和 4 年 4 月 19 日に、SAE レベル 4 に相当する、運転者がいない状態での自動運転である特定自動運行の許可制度[9]の創設等を内容とする道路交通法の一部を改正する法律[10]（令和 4 年法律第 32 号）が成立した。

なお、道路交通に関する国際的動向として、我が国は、道路交通に関する条約、いわゆる 1949 年ジュネーブ条約を批准しており、これにより国際運転免許証の恩恵等に与れている。近年、自動運転と国際条約との関係の整理等に関し、国際場裡で議論が行われているところ、我が国も議論に参画している。

（２）サイバーセキュリティに関する法整備について

ア　国際基準策定の取組

我が国は、国連自動車基準調和世界フォーラム（WP29）において、共同議長又は副議長等として自動運転に関する国際基準に係る議論を主導している。2020 年 6 月に開催された WP29 において、サイバーセキュリティ対策等を含む自動運行装置の国際基準が成立し、2021 年 1 月に、国際基準（UN Regulation No.155）として正式に発効した[11][12]。

イ　国内基準の動向

国内では、サイバーセキュリティの要件として、道路運送車両法の令和元年改正法の施行日（令和 2 年 4 月 1 日）に、自動車の電気装置に関する保安基準において、サイバーセキュリティを確保できるものとして、性能に関し告示で定める基準に適合するものでなければならない（第 17 条の 2 第 3 項）とされ、その告示で定める基準として、「サイバーセキュリティシステムの技術基準」[13]が設けられた。

また、同日に、自動車のサイバーセキュリティを確保することを目的として、国土交通大臣による、申請者のサイバーセキュリティを確保するための業務管理システム（CSMS[14]。リスクアセスメントの実施などに関する組織的な管理体制・方法等）の適合

---

8 道路交通法の一部を改正する法律（概要）（https://www.npa.go.jp/laws/kaisei/houritsu/190605/gaiyou.pdf）。
9 警察庁「自動運転」（https://www.npa.go.jp/bureau/traffic/selfdriving/index.html）。
10 警察庁「国会提出法案」（https://www.npa.go.jp/laws/kokkai/index.html）。
11 UN Regulation No. 155（https://unece.org/sites/default/files/2021-03/R155e.pdf）。
12 UN Regulation No.155 は 1958 年協定に基づく協定規則であり、1998 年協定に基づく世界統一技術規則（UNGTR）においても、UN Regulation No.155 と同様の要件が、2022 年に承認される予定であったが、現時点では正式承認に関する明確な情報が確認されていない。
13 道路運送車両の保安基準の細目を定める告示（平成 14 年国土交通省告示第 619 号）の別添 120。
14 Cyber Security Management System の略。

証明の制度及び適合証明書の交付手続きを定めるサイバーセキュリティ業務管理システムの適合証明に関する規程（令和 2 年国土交通省告示第 464 号）が施行された。

これらの国内基準は、上記の国際基準に先行して定められたが、その内容は国際基準に沿う形で定められたものであるため、2021 年 1 月に、国際基準（UN Regulation No.155）が正式に発効されたことを受けて、国内基準は、国際基準（UN Regulation No.155）を直接引用する形式に改正された。また、サイバーセキュリティに関する国内基準の適用対象は、従前は自動運転車に限られていたが、自動運転車以外の従来の自動車全般にも拡大されることとなった[15]。これにより、令和 4 年 7 月 1 日以降の自動運転車又は無線によるソフトウェアアップデートに対応している車両の新型車から、順次、国際基準（UN Regulation No.155）が適用され、継続生産車は令和 6 年 7 月 1 日から、無線によるソフトウェアアップデートに対応していない車両の新型車は令和 6 年 1 月 1 日から、継続生産車は令和 8 年 9 月 1 日から、それぞれ適用される[16]。

ウ　国際基準（UN Regulation No.155）の概要[17]

サイバーセキュリティに関する国際基準（UN Regulation No.155）は、他の技術要件と異なり、自動車メーカーの組織が取るべき対策（組織要件）と、車両への対策（型式要件）で構成される。組織要件では、自動車メーカーにおいて、サイバーセキュリティの適切さを担保するための業務管理システム（CSMS）を確保しているかが審査される。車両のセキュリティを確実なものにしても、管理者（自動車メーカー）の管理がずさんであれば、全体として意味をなさないためである。

2025 年 1 月に国際基準（UN Regulation No.155）の改訂が採択され、合わせて日本国内においても省令等の改正が行われた。この改正により、二輪自動車、三輪自動車等のカテゴリ車両も新たに規制対象に追加され、新型車は令和 11 年 7 月 1 日から、継続生産車は令和 13 年 9 月 1 日から適用される[18]。

---

15 国土交通省「道路運送車両の保安基準等の一部を改正する省令及び道路運送車両の保安基準の細目を定める告示等の一部を改正する告示について」（https://www.mlit.go.jp/report/press/content/001379922.pdf）。

16 第 2 回車両安全対策検討会「4-3. サイバーセキュリティ及びプログラム等改変システムに係る基準」（https://www.mlit.go.jp/jidosha/content/001844079.pdf）。

17 国際基準（UN Regulation No.155）の詳細については、新国哲也「国連自動車基準調和世界フォーラム（WP29）における自動車のサイバーセキュリティ基準の解説」（自動車技術会論文集 vol52,No.1,January 2021）を参照されたい。https://www.jstage.jst.go.jp/article/jsaeronbun/52/1/52_20214056/_pdf/-char/ja

18 国土交通省「道路運送車両の保安基準等の一部を改正する省令及び道路運送車両の保安基準の細目を定める告示等の一部を改正する告示について」（https://www.mlit.go.jp/report/press/content/001854946.pdf）。

（ア）組織要件

自動車メーカーが構築すべき CSMS として、大要、以下のプロセスを実行することが求められている。なお、CSMS では、自動車メーカーのみならず関連するサプライチェーンなどの外部組織との連携も考慮されなければならない。

- セキュリティを管理するためのプロセス
- 審査対象となる車両型式のシステムにおける固有のリスクを特定するためのプロセス
- 特定されたリスクを評価、分類しさらにそのリスクを低減させるためのプロセス
- 特定されたリスクが拡大しないような措置を講じるためのプロセス
- 車両型式のシステムにおけるセキュリティ評価のためのプロセス
- （新たな脅威を考慮しつつ）リスク評価を最新の状態に保つプロセス
- セキュリティ上の脅威や実際の攻撃、車両型式のシステムにおける脆弱性の監視、検出等を行うためのプロセス、またその監視、検出結果に照らし、車両型式のシステムにおけるセキュリティ評価を行うためのプロセス
- セキュリティ上の攻撃を分析するために使用されるプロセス

上記プロセスの審査に当たっては、下記の点をポイントとして検証することが必要とされている。

- CSMS に係る組織の体制の提示
- CSMS により設定される業務手順書などのルールの制定、運用、改正方法等の確認
- 制定されているルールが組織構成員に周知徹底されていることの確認

CSMS への要件の適合性が確認されれば、CSMS 適合証明書が発行される。

（イ）型式要件

自動車の型式に対する主な要件は、以下のとおりである。

- 審査対象車両に関する有効な CSMS 適合証明書を持っていること
- 車両に搭載されるシステムにおける重要な要素（例えば、車両を制御する上で重要なパラメータなど）を特定し、それに対するリスク（サプライヤーに関連のあるリスクを含む。）評価や管理を行うこと
- 特定されたリスクから車両を保護するために、技術的な対策を行い、その有効性を検証するための適切かつ十分な試験を実施すること
- 車両の使用段階で利用されるサービスのために適切な対策を講じる。また、サイバー攻撃を検出し、防止する対策を講じること。

3．参考資料（法令・ガイドラインなど）

本文中に記載したもののほか、

・自動走行ビジネス検討会報告書「自動走行の実現及び普及に向けた取組報告と方針 Version7.0」（2023 年 4 月 28 日）
https://www.meti.go.jp/policy/mono_info_service/mono/automobile/jido_soko/20230428_report.html
・自動走行ビジネス検討会「自動走行システムにおけるサイバーセキュリティ対策」（2019 年 6 月 26 日）
https://www.meti.go.jp/policy/mono_info_service/mono/automobile/jido_soko/pdf/sanko_03.pdf

４．裁判例

特になし

Q40 スマホソフトウェア競争促進法

スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律はどのような法律か。また、サイバーセキュリティを確保するための取組についてはどのように扱われるのか。

タグ：スマホソフトウェア競争促進法、スマートフォン、アプリ、ソフトウェア

１．概要

スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律（令和 6 年法律第 58 号。以下、本項において「スマホソフトウェア競争促進法」という。）は、スマートフォンの利用に特に必要な特定ソフトウェア（基本動作ソフトウェア、アプリストア、ブラウザ及び検索エンジン）の提供等を多数のユーザーに行う事業者に対し、特定ソフトウェアの提供等を行う事業者としての立場を利用して自ら提供する商品又は役務を競争上優位にすること及び特定ソフトウェアを利用する事業者の事業活動に不当な不利益を及ぼすことの禁止等について定めることにより、特定ソフトウェアに係る公正かつ自由な競争の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的として制定された法律である。

そのため、スマホソフトウェア競争促進法の義務は、特定ソフトウェアの提供等を多数のユーザーに行う指定事業者（本法の規制対象事業者として公正取引委員会から指定された事業者）のみに課される。

そして、スマホソフトウェア競争促進法の一定の禁止行為については、スマートフォンの利用に係るサイバーセキュリティの確保等のために必要な行為を行う場合であって、他の行為によってその目的を達成することが困難であるときは、いわゆる「正当化事由」に該当し、例外的に違反とならない（スマホソフトウェア競争促進法第 7 条但書、第 8 条但書）。スマートフォンの利用者が多様なアプリストア及びアプリストアで配布される個別ソフトウェア（アプリ）を安心して利用できるようにするために、指定事業者によるサイバーセキュリティを確保するための取組について正当化事由が認められるか否かは、サイバーセキュリティの確保と競争の促進のバランスにも配慮しながら判断を行うことが重要であるとされている。

指定事業者の義務に関して、指定事業者が適切に対処するために必要な指針として同法に基づいて公正取引委員会が策定し、公表した「スマホソフトウェア競争促進法に関する指針」[1]（以下、本項において「本指針」という。）には、サイバーセキュリティの確保

[1] スマホソフトウェア競争促進法に関する指針（令和 7 年 8 月 20 日／公正取引委員会）（https://www.jftc.go.jp/file/shishin2.pdf）。

のための正当化事由に関する想定例が記載されている。ただし、これらの想定例はあくまで仮想的な事例を列挙したものであり、スマホソフトウェア競争促進法の適用に当たっては、個別具体的な事情を踏まえて判断することになるものとされている。

２．解説

（１）スマホソフトウェア競争促進法の規制対象となる指定事業者

スマホソフトウェア競争促進法の規制対象となる「指定事業者」は、特定ソフトウェア（検索エンジンについては、それを用いた検索サービス）の提供を行う事業者のうち、年度における各月平均での国内利用者（エンドユーザー）の数が 4000 万人以上であるものを公正取引委員会が指定するものと規定されている（スマホソフトウェア競争促進法第 3 条第１項、スマホソフトウェア競争促進法施行令第１条）。

令和８年３月末現在、Apple Inc.、iTunes 株式会社及び Google LLC が指定されており、スマホソフトウェア競争促進法の義務は、これらの事業者に対して課されている。

規制対象である 指定事業者	指定に係る 特定ソフトウェアの種類	（参考）提供する特定ソフトウェア
Apple Inc.	基本動作ソフトウェア	iOS
	アプリストア	App Store
	ブラウザ	Safari
iTunes 株式会社	アプリストア	App Store
Google LLC	基本動作ソフトウェア	Android OS
	アプリストア	Google Play
	ブラウザ	Google Chrome
	検索エンジン	Google 検索

（注）Apple Inc.と iTunes 株式会社は、共同してアプリストアを提供している。

（２）第７条第１号

ア　禁止行為

基本動作ソフトウェアに係る指定事業者が、当該基本動作ソフトウェアを通じて提供されるアプリストアを当該指定事業者又はその子会社等（以下、本項において「基本動作ソフトウェア指定事業者等」という。）が提供するものに限定することのほか、他の事業者が当該基本動作ソフトウェアを通じて代替アプリストア（基本動作ソフトウェア指定事業者等以外の事業者が提供するアプリストアをいう。以下、本項において同じ。）を提供すること等を妨げることが禁止されている。ただし、サイバーセキュリティを確保するための指定事業者の行為が、スマホソフトウェア競争促進法の定める正当化事由に

該当する場合には、当該行為によって代替アプリストアの提供等を妨げたとしても例外的に違反とならない。

イ　正当化事由に関する想定例

① 正当化事由が認められ、違反とならない例

指定事業者が、その指定に係る基本動作ソフトウェアにおいて利用される代替アプリストアに対して、サイバーセキュリティの確保等の観点から必要な基準に照らした審査等を行い、当該アプリストアが当該基準を満たしていない場合には、当該基本動作ソフトウェアにおける当該代替アプリストアの提供を禁止すること。【本指針の想定例 35】

② 正当化事由が認められず、違反となる例

スマートフォンの利用者が代替アプリストアのダウンロード及びインストールを行おうとする際に、いずれの代替アプリストアに対しても審査等を行うことなく一律に、指定事業者が、当該代替アプリストアはサイバーセキュリティの確保等の観点から安全ではないことから利用を控えるように促す旨の警告表示を行うこと。【本指針の想定例 39】

（3）第 7 条第 2 号

ア　禁止行為

基本動作ソフトウェアに係る指定事業者が、基本動作ソフトウェアにより制御される音声を出力する機能その他のスマートフォンの動作に係る機能であって、基本動作ソフトウェア指定事業者等がアプリの提供に利用するもの（以下、本項において「本 OS 機能」という。）について、同等の性能で他のアプリ事業者がアプリの提供に利用することを妨げることが禁止されている。ただし、サイバーセキュリティを確保するための指定事業者の行為が、スマホソフトウェア競争促進法の定める正当化事由に該当する場合には、当該行為によって他のアプリ事業者が本 OS 機能を同等の性能で利用できないとしても例外的に違反とならない。

イ　正当化事由に関する想定例

① 正当化事由が認められ、違反とならない例

サイバーセキュリティの確保等の観点から懸念がある特定の本 OS 機能であって、当該本 OS 機能をアプリの提供に利用できる他の事業者を限定しなければ当該懸念を解消することが困難であるものについて、他の事業者に対し、当該観点から必要な基準に照らした審査等を行い、当該他の事業者が当該基準を満たしていない場合には、当該本 OS 機能の利用を制限すること。【本指針の想定例 61】

② 正当化事由が認められず、違反となる例

特定の本 OS 機能について、多数の他の事業者に対しては、サイバーセキュリティの確保等の観点から必要な基準に照らした審査等を行い、当該基準を満たす者に当該本 OS 機能を同等の性能でアプリの提供に利用できるようにしているにもかかわらず、サイバーセキュリティの確保等の目的のために必要であるとして、特定の他の事業者に対してのみ、当該審査等を行うことなく、当該本 OS 機能の利用を認めないこと。【本指針の想定例 64】

（4）第 8 条第 1 号

ア　禁止行為

アプリストアに係る指定事業者が、当該アプリストアに関し、当該指定事業者又はその子会社等（以下、本項において「アプリストア指定事業者等」という。）が提供する支払管理役務以外の支払管理役務（以下、本項において「代替支払管理役務」という。）を個別アプリ事業者が利用しないことを当該アプリストアの利用条件とすることのほか、代替支払管理役務をアプリ事業者が利用すること等を妨げることが禁止されている。ただし、サイバーセキュリティを確保するための指定事業者の行為が、スマホソフトウェア競争促進法の定める正当化事由に該当する場合には、当該行為によって代替支払管理役務の利用が妨げられたとしても例外的に違反とならない。

イ　正当化事由に関する想定例

① 正当化事由が認められ、違反とならない例

代替支払管理役務等（代替支払管理役務又はアプリ事業者が支払管理役務を利用せずにスマートフォンの利用者に対して用いることができるようにする支払手段をいう。以下、本項において同じ。）がスマートフォンの利用に係るサイバーセキュリティの確保等のための的確な対策を講じておらず、当該代替支払管理役務等を利用することによって、スマートフォンの利用者のクレジットカード情報等の漏洩が生じると認められる場合に、指定事業者が、スマートフォンの利用に係るサイバーセキュリティの確保等の観点で、アプリストアにおいて、当該代替支払管理役務等を利用するアプリ事業者のアプリの提供を認めないこと。【本指針の想定例 78】

② 正当化事由が認められず、違反となる例

指定事業者が、アプリ事業者が代替支払管理役務等を利用する場合に、サイバー攻撃によるクレジットカード情報の漏えいのリスクが上昇するというサイバーセキュリティの確保等の観点からの問題を理由に、アプリ事業者による代替支払管理役務等の利用について、審査等を行うことなく一律に禁止すること。【本指針の想定例 79】

（５）第 8 条第 2 号

ア　禁止行為

アプリストアに係る指定事業者が、当該アプリストアに関し、アプリ事業者がその提供するアプリ（以下、本項において「本アプリ」という。）の作動中に、ウェブページ又は本アプリ以外のアプリ（以下、本項において「関連ウェブページ等」という。）を通じて提供される商品又は役務の価格その他の情報（以下、本項において「外部誘導情報」という。）の表示を行わないことや、アプリからアプリの外のウェブページに遷移するリンク（以下、本項において「リンクアウト」という。）を含めないことを、当該アプリストアを通じてアプリを提供する際の条件とすること等が禁止されている。ただし、サイバーセキュリティを確保するための指定事業者の行為が、スマホソフトウェア競争促進法の定める正当化事由に該当する場合には、当該行為によって外部誘導情報の表示を制限するなどしても例外的に違反とならない。

イ　正当化事由に関する想定例

① 正当化事由が認められ、違反とならない例

指定事業者が、基本動作ソフトウェア及びアプリストアを提供する立場から、スマートフォンの利用者がリンクアウトの提供を受ける場合に、当該リンクアウト経由で外部のウェブサイトに遷移した後に、本物のウェブサイトに似せることでスマートフォンの利用者を欺く又は当該利用者に誤解を与えるウェブサイトに遷移するリスクについて指定事業者により制御することができないことから、当該リスクについての注意喚起及び遷移後は指定事業者による制御の範囲から離れる旨を説明するポップアップを表示すること。【本指針の想定例 93】

② 正当化事由が認められず、違反となる例

外部誘導情報として表示する内容及びリンクアウトから遷移する外部のウェブサイトの内容に何ら制限がなければ、アプリ事業者が、外部のウェブサイトにおける商品又は役務の価格と異なる価格情報（販売価格のほか、値引額、値引率を含む。）を外部誘導情報として表示したり、スマートフォンの利用者が意図するものとは異なる商品又は役務の決済画面に当該スマートフォンの利用者を誘導したりするリスクがあるという理由で、指定事業者が、本アプリにおける外部誘導情報に価格情報を含めることやリンクアウトから遷移する先のウェブページとして決済画面を個別アプリ事業者が設定することを、個別アプリ事業者に対する審査等を行うことなく一律に禁止すること。【本指針の想定例 95】

（6）第 8 条第 3 号

ア　禁止行為

アプリストアに係る指定事業者が、当該アプリストアに関し、アプリストア指定事業者等が提供するブラウザエンジン（HTML 等のプログラム言語で書かれたウェブサイトを閲覧可能な表示に変換・処理する、ブラウザの中核的なソフトウェア）をアプリ事業者がそのアプリの構成要素とすることを当該アプリストアの利用条件とすることのほか、代替ブラウザエンジン（指定事業者等が提供するブラウザエンジン以外のブラウザエンジンをいう。）をアプリ事業者がそのアプリの構成要素とすることを妨げることが禁止されている。ただし、サイバーセキュリティを確保するための指定事業者の行為が、スマホソフトウェア競争促進法の定める正当化事由に該当する場合には、当該行為によって代替ブラウザエンジンの利用が制限されたとしても例外的に違反とならない。

イ　正当化事由に関する想定例

① 正当化事由が認められ、違反とならない例

アプリストアを経由してブラウザ以外のアプリを配布する事業者が極めて多数に上ることから、指定事業者が、それらのアプリ経由でウェブページを表示するためのブラウザエンジンを原則として指定事業者等のブラウザエンジンに統一することとしつつ、代替ブラウザエンジンを採用しようとするアプリ事業者に対しては、サイバーセキュリティの確保等の観点から一定の要件（例えば、指定事業者と同等の脆弱性対応を行っているか否か、ペアレンタルコントロール機能が機能するか否か）を設け、当該要件を満たすか否かの審査等を事前に行った上で、当該代替ブラウザエンジンの採用の可否を判断すること。【本指針の想定例 103】

② 正当化事由が認められず、違反となる例

ブラウザエンジンを自ら開発し、指定事業者と同等の脆弱性対応を行っているアプリ事業者のアプリについて、サイバーセキュリティの確保等の観点からの懸念について、指定事業者等のブラウザエンジンを採用したアプリの場合と差異はないにもかかわらず、当該個別アプリ事業者が自らのブラウザエンジンを自らのアプリに採用することについて、指定事業者が、サイバーセキュリティの確保等の観点からの問題があるとして認めないこと。【本指針の想定例 104】

3．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

4．裁判例

特になし

Q41 5G 促進法とサイバーセキュリティ

いわゆる「5G 促進法」とは、どのような法律か。また、同法は、誰に対して、どのようにしてサイバーセキュリティを確保するよう求めているのか。

タグ：5G 促進法、特定高度情報通信技術活用システムの開発供給等の促進に関する指針、開発供給計画、導入計画、Society 5.0

１．概要

特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律(令和 2 年法律第 37 号。以下、本項において「5G 促進法」という。）は、サイバーセキュリティ等を確保しつつ、第 5 世代移動通信システム（5G）及びドローンの普及を図る目的で制定された法律であり、同法に基づいて一定の計画を認定する際に参照される、特定高度情報通信技術活用システムの開発供給等の促進に関する指針（令和 2 年総務省・財務省・経済産業省告示第 1 号。以下、本項において「本指針」という。）には、サイバーセキュリティの確保に関する要件が含まれる。

２．解説

（１）背景

5G 促進法は、Society 5.0 の実現に不可欠な社会基盤となる特定高度情報通信技術活用システム（5G 及びドローン）のサイバーセキュリティ等を確保しながら、その適切な開発供給及び導入を促進するための措置を講じて、5G 及びドローンの普及を図ることを目的として制定され、令和 2 年 8 月 31 日より施行されている。

なお、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律及び国立研究開発法人新エネルギー・産業技術総合開発機構法の一部を改正する法律（令和 4 年 3 月 1 日施行）による改正により、5G 促進法に特定半導体（5G 情報通信システムに不可欠な大量の情報を高速度での処理を可能とするもので、国際的に生産能力が限られている等の事由により国内で安定的に生産することが特に必要なもの）の生産施設整備等計画の認定制度及び認定事業者に対する支援措置が追加されている。

（２）概要

ア　特定高度情報通信技術活用システムの定義

5G 促進法第 2 条は、「特定高度情報通信技術活用システム」のうち 5G 及びドローンについて、以下のとおり定義している。

① 情報通信の業務を一体的に行うよう構成された無線設備及び交換設備等並びにプログラムの集合体であって、政令で定める周波数の電波を使用することにより

大量の情報を高速度で送受信することを可能とするものその他の高度な技術を活用した情報通信を実現するもの（以下、本項において「1 号システム」という。）

② 国、地方公共団体若しくは重要社会基盤事業者の事業又はこれに類する事業に係る点検、測量その他の政令で定める業務を一体的に行うよう構成された小型無人機、撮影機器その他機器及びこれらに係るプログラムの集合体（以下、本項において「2 号システム」という。）

このうち、①については 5G が想定されており、5G には携帯電話事業者が全国展開するサービス（全国 5G）に加え、地域や産業の個別のニーズに応じて活用されるローカル 5G も含まれる。他方、②についてはドローン及びドローンにおいて利用される撮影機器等を含むシステムが想定されている。

また、②の「重要社会基盤事業者」とは、サイバーセキュリティ基本法第 3 条第 1 項に定める重要社会基盤事業者を指し（5G 促進法第 2 条第 1 項第 2 号）、「重要社会基盤事業者の事業」とは、重要インフラ行動計画において指定される 15 の重要インフラ分野[1]に属する事業を指すと解されている。なお、「これに類する事業」として、農業、林業、漁業、建設業、鉄鋼業、郵便業及び警備業が指定されている（特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律施行令第 1 条第 2 項）。

イ　特定高度情報通信技術活用システムの開発供給等の促進に関する指針の策定

主務大臣は、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する指針を定めるものとされており（5G 促進法第 6 条）、これに基づき、令和 2 年 8 月 28 日、本指針が公布された。

ウ　特定高度情報通信技術活用システムの開発供給・導入に係る計画の認定

特定高度情報通信技術活用システムの開発供給事業者（ベンダ）又は当該システムの導入事業者（通信キャリア、製造事業者等）は、開発供給計画又は導入計画を作成して、主務大臣に対して申請することができる。主務大臣が、当該計画が本指針に照らして適切なものであること等について適合するものであることを認めた場合、計画の認定を受けることができ、この認定を受けた計画はその概要が公表される[2]（5G 促進法第 7 条～第 10 条）。

[1] 詳細については Q2 を参照されたい。
[2] 経済産業省のウェブサイトにおいて公表されている（https://www.meti.go.jp/policy/mono_info_service/joho/laws/5g_drone.html）。

エ　認定された開発供給計画及び導入計画に係る支援措置

認定開発供給事業者及び認定導入事業者は、以下の①～③の支援措置を受けることができる（5G 促進法第 13 条～第 28 条)。ただし、このうち①については、特定高度情報通信技術活用システムのうち、5G のみが対象であり、ドローンは対象外である。

① 日本政策金融公庫の業務の特例（ツーステップローン）: 認定計画に従って開発供給等を行うために必要な資金の貸付けを公庫から受けられる
② 中小企業投資育成株式会社法（昭和 38 年法律第 101 号）の特例：中小企業者が認定計画に従って開発供給等を行う場合、中小企業投資育成株式会社の新規投資の対象となるための要件が緩和される
③ 中小企業信用保険法（昭和 25 年法律第 264 号）の特例：計画の認定を受けた中小企業者が、民間金融機関を利用して信用保証付き融資を受ける際、一般枠とは別枠の保証等の措置を受けられる

（３）5G 促進法におけるサイバーセキュリティの確保

ア　5G 促進法の基本理念

5G 促進法は、その基本理念の中で、特定高度情報通信技術活用システムの開発供給及び導入が、サイバーセキュリティを確保しつつ適切に行われることを基本とすることを明記し（同法第 3 条)、特定高度情報通信技術活用システムの開発供給等を行う事業者は、同法第 3 条の基本理念にのっとり、国が実施する特定高度情報通信技術活用システムの開発供給等の促進に関する施策に協力するよう努めるものと定める(同法第 5 条)。

イ　本指針において規定されるサイバーセキュリティの確保

開発供給計画及び導入計画の認定を受けるに当たっては、当該計画が本指針に照らし適切なものであることの確認がなされるところ（同法第 7 条第 3 項第 1 号、第 9 条第 3 項第 1 号)、本指針においては、サイバーセキュリティの確保に関し、以下の要件が規定されている。

（ア）1 号システムの開発供給内容に関する要件

開発供給を行う 1 号システムの安全性及び信頼性確保のための対策が、下記①から④までのいずれにも該当すること（本指針第二・一・1）

① 開発供給を行う事業者において、サイバーセキュリティを確保するための規程を策定した上で、開発供給を行う 1 号システムのサイバーセキュリティに係る脆弱性の評価を行い、適切な対策が講じられていること
② 開発供給を行う事業者において、開発供給した 1 号システムの導入を行う事業者が当該システムのサイバーセキュリティを持続的に確保することを支援するために必要な体制が整備されていること

③ 「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」[3]、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ（平成 30 年 12 月 10 日関係省庁申合せ）」[4]並びに「第 5 世代移動通信システムの導入のための特定基地局の開設に関する指針（平成 31 年総務省告示第 24 号）」及び「ローカル 5G 導入に関するガイドライン（令和元年 12 月総務省策定）」[5]等に留意し、サプライチェーン・リスク対応を含むサイバーセキュリティ対策が講じられていること

④ 国際的な取組（プラハ 5G セキュリティ会議[6]等）の考え方に基づき、開発供給を行う事業者の信頼性を確保するため、(a)開発供給を行う事業者の所有関係及びガバナンスの透明性が確保されていること、(b)開発供給を行う事業者が、過去 3 年間の実績を含め、国際的に受け入れられた基準に反していないこと、及び(c)外国の法的環境等により開発供給の適切性が影響を受けるものでないことのいずれにも該当すること

（イ）1 号システムの導入内容に関する要件

導入を行う 1 号システムの安全性及び信頼性確保のための対策が、下記①から③までのいずれにも該当すること（本指針第二・三・1）

① サイバーセキュリティ上の事案が発生した場合に、1 号システム導入計画に係る事業を所管する省庁に対し、速やかに報告を行うための体制が整備されていること

② サイバーセキュリティ上の事案が発生した場合に、関係主体に対して適切な情報共有を行うための体制が整備されていること

③ 全国 5G システムにあっては、「第五世代移動通信システムの導入のための特定基地局の開設計画」の認定を受けて「第五世代移動通信システムの導入のための特定基地局の開設に関する指針」に留意し、ローカル 5G システムにあっては、「ローカル 5G 導入に関するガイドライン」[7]に留意し、サプライチェーン・リスク対応を含むサイバーセキュリティ対策が講じられていること

---

[3] 令和 3 年度、令和 5 年度、令和 7 年度に更新され、名称も「政府機関等のサイバーセキュリティ対策のための統一基準群」に変わっている。過去のものも含めて、右記ウェブサイトを参照されたい（https://www.cyber.go.jp/policy/group/general/kijun.html）。

[4] https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf この申合せに関しては、Q53 も参照されたい。

[5] https://www.soumu.go.jp/main_content/000659870.pdf

[6] 2019 年 5 月 3 日、当該会議において、サイバー攻撃等のリスク回避に向けて各国が連携を深めるとする議長声明（プラハ提案）が採択された。

[7] 前掲注 5 参照。

（ウ）2 号システムの開発内容に関する要件

開発供給を行う 2 号システムの安全性及び信頼性確保のための対策が、下記①から④までのいずれにも該当すること（本指針第二・五・1）

① 開発供給を行う事業者において、サイバーセキュリティを確保するための規程を策定した上で、開発供給を行う 2 号システムのサイバーセキュリティに係る脆弱性の評価を行い、適切な対策が講じられていること

② 開発供給を行う事業者において、開発供給した 2 号システムの導入を行う事業者が当該システムのサイバーセキュリティを持続的に確保することを支援するために必要な体制が整備されていること

③ 「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」[8]におけるサプライチェーン・リスク対策の内容と同等の対応を含むサイバーセキュリティ対策が講じられていること

④ 開発供給を行う事業者の信頼性を確保するため、(a)開発供給を行う事業者の所有関係及びガバナンスの透明性が確保されていること、(b)開発供給を行う事業者が、過去 3 年間の実績を含め、国際的に受け入れられた基準に反していないこと、及び(c)外国の法的環境等により開発供給の適切性が影響を受けるものでないことのいずれにも該当すること

（エ）2 号システムの導入内容に関する要件

導入を行う 2 号システムの安全性及び信頼性確保のための対策が、下記①から③までのいずれにも該当すること（本指針第二・七・1）

① サイバーセキュリティ上の事案が発生した場合に、2 号システム導入計画に係る事業を所管する省庁に対し、速やかに報告を行うための体制が整備されていること

② サイバーセキュリティ上の事案が発生した場合に、関係主体に対して適切な情報共有を行うための体制が整備されていること

③ 「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」[9]におけるサプライチェーン・リスク対策の内容と同等の対応を含むサイバーセキュリティ対策が講じられていること

（4）その他

生成 AI の利活用の急速な拡大に伴う計算需要の大幅な増加に対応するため、半導体・データセンター等のハードウェアと生成 AI 等のソフトウェアが相互に連携の上、高度化していくエコシステムを構築するとともに、生成 AI 等のデジタル技術の利活用促進を牽

[8] 前掲注 3 参照。
[9] 前掲注 3 参照。

引するデジタル人材の育成を進めるための措置を講じることを目的として、情報処理の促進に関する法律の一部改正が行われており、令和 7 年 8 月 4 日付で施行されている。

ドローンのサイバーセキュリティに関する留意点については Q38 及び IPA が公表する「ドローンサイバーセキュリティハンドブック～安全なドローン利活用の勘どころ～（2021 年 6 月）」[10]も参照されたい。また、ドローンのサイバーセキュリティに関する守るべき要件等については、経済産業省と国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）で策定した「無人航空機分野サイバーセキュリティガイドライン（2022 年 3 月 31 日）」[11]も合わせて参照されたい。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[10] https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002jq9-att/000092207.pdf
[11] https://www.meti.go.jp/policy/mono_info_service/mono/robot/drone_cybersecurity.html

Q42 クラウドサービスとサイバーセキュリティ

クラウドサービスを利用するに当たって、サイバーセキュリティの観点から留意すべき点は何か。

タグ：民法、個情法、不正競争防止法、クラウド、定型約款

１．概要

クラウドサービスについては、IT の基盤部分のコントロールが外部のクラウドサービスを提供する事業者（以下、本項において「クラウドサービス提供事業者」という。）にあること、複数のベンダが関与する形でサービスが提供されることから、その利用に際してサイバーセキュリティの観点を考慮するに当たっても、クラウドサービスの特色を踏まえた検討が必要である。

クラウドサービスのユーザは、クラウドサービスにおいて管理する情報資産の性質を踏まえたセキュリティレベルを決定し、クラウドサービス提供事業者から開示されたサービス内容やセキュリティレベルの内容が、決定されたセキュリティのレベルに対応しているのかを検討する。クラウドサービス提供事業者から開示されたサービス内容やセキュリティのレベルについては、法的拘束力を持つ形で合意できるのかについても確認する必要がある。

２．解説

（１）クラウドサービスの特徴

ア　外部リソースの利用[1]

クラウドコンピューティングとは、「共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーションなど）について、ユーザの要求に応じて適宜・適切に配分してネットワークを通じて提供することを可能とする情報処理形態」であるとされる[2]。インターネットの発達を背景にクラウドサービスが提供されるようになってきたが、近時では、通信速度の向上、携帯端末の高機能化を背景に、世界的規模の事業者により大規模な設備投資が行われ、従前はオンプレミスの環境において提供されていたサービスがクラウド化するなど、IT サービスの一層のクラウド環境への移行が見られるようにな

[1] 本項の議論につき、経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013 年度版）」（以下、本項において「クラウドサービス利用ガイドライン」という。）4 頁以下。

[2] クラウドサービス利用ガイドライン 8 頁。なお、法令においては、官民データ活用推進基本法（平成 28 年法律第 103 号）が、「クラウド・コンピューティング・サービス関連技術」について、「インターネットその他の高度情報通信ネットワークを通じて電子計算機（入出力装置を含む。……）を他人の情報処理の用に供するサービスに関する技術」と定義している。

ってきている。ユーザ側でも、自前で環境を整備するよりも、クラウドサービスを利用したほうが簡易であり、初期投資も安価であることから、利用が進んでいる。

このようなクラウドサービスの最大の特徴としては、外部リソースの利用であることが挙げられる。社内において情報資産を管理するに当たっては、情報の重要性や機密性に応じて、例えば、ファイアウォールの設定、IDS 等のサイバーセキュリティに関連する機器の選定といったシステムをどのように構築するかという技術的な点から、情報システムに関わる組織体制の整備や従業員に対する教育といった組織的な点まで、自社でコントロールすることができる。しかし、外部のクラウドサービスを利用する場合、このように自社で全て管理することができていたリソースの一部を外部に切り出し、外部のクラウドサービス提供事業者が管理する情報システムからサービスの提供を受ける形になる。そのため、クラウドサービスを利用する部分のセキュリティについては、外部のクラウドサービス提供事業者に委ねることになることに留意が必要である。なお、ユーザがクラウドサービスを利用し、クラウドサービス上に構築するシステムにおいて利用するデータ等の情報資産については、ユーザが保有する情報資産であることに留意する必要がある。

イ　クラウドサービスの提供形態の複雑化[3]

また、クラウドサービスの特徴として、サプライチェーンが複雑になることが多いという点が挙げられる。従前は単独の事業者が提供していたクラウドサービスについても、その利用が拡大するにしたがって、巨額な投資を必要とするインフラ側のベンダ（IaaS[4]、PaaS[5]、データセンター）と少額の投資で構築可能であるが多様なサービスが提供されているアプリケーション側のベンダ（SaaS[6]）への分化が見られる。例えば、クラウドサービスの利用者が、SaaS 事業者が提供しているサービスを利用している場合、その SaaS 事業者は他のクラウドサービス事業者の PaaS を利用しているため、クラウドサービス利用者が SaaS 事業者にしか預けていないと認識している情報が PaaS 事業者に渡っている場合がある。サプライチェーンの構造としては、①複数の SaaS が連携してサービ

[3] 本項の議論につき、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」（以下、本項において「クラウドサービス提供ガイドライン」という。）26 頁以下。

[4] 「Infrastructure as a Service」の略。利用者に CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるサービス形態を指す。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。

[5] 「Platform as a Service」の略。IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるサービス形態を指す。利用者は、基本機能等を組み合わせることにより情報システムを構築する。

[6] 「Software as a Service」の略。利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等が提供されるサービス形態を指す。

スを提供する、②一つのプラットフォーマーが提供するサービスの上で複数の SaaS がサービスを提供する、③ユーザの ID などを連結点としてデータの連携を行う（ID 連携）などの形態が現れてきている。さらに、クラウドサービス提供事業者がユーザを獲得するために代理店に販路開拓を依頼することもあり、クラウドサービスの提供ルートは複雑になっている。

（２）クラウドサービスの利用に当たってセキュリティの観点から留意すべき点

クラウドサービスを利用するに当たっては、①クラウドサービスを利用しようと考えているユーザ内部の情報資産を検討し、必要なセキュリティのレベルを確定すること、②クラウドサービス提供事業者側から開示される情報をもとに、クラウドサービスを利用することによって必要なセキュリティのレベルを確保することができるかを検討することが重要である。また、③クラウドサービス提供事業者の提供するサービスが実際に開示されたセキュリティのレベルを維持しているのかをどのように確認するのかも検討する必要がある。さらに、④責任共有モデル（Shared Responsibility Model）を前提として、クラウドサービス提供事業者間やクラウドサービス提供事業者とユーザの間でセキュリティの責任分界がどこにあるのかについて理解することも重要である。

ア　ユーザ内部の情報の検討

クラウドサービスを利用するに当たり、ユーザ側がまず検討すべき事項は、ユーザがクラウドサービスを利用して管理しようとしている情報資産の範囲を確定し、その情報資産について必要とされるセキュリティの内容、レベルを明らかにするということである。必要なセキュリティの内容が明らかになっていれば、クラウドサービス提供事業者側からの開示事項を検討することにより、オンプレミスの環境におけるセキュリティレベルと同レベルの環境を維持し得る。

また、クラウドサービス上で利用する情報資産の内容によっては、以下のとおり法的にどのように考えるのかを検討しておく必要がある。

（ア）個情法との関係

個情法においては、個人情報の利用目的の特定及びその通知等（同法第 17 条第 1 項、第 21 条）、目的外利用の原則禁止（同法第 18 条）、不適正利用の禁止（同法第 19 条）、適正取得（同法第 20 条）の規律がある。さらに、個人データ（同法第 16 条第 3 項）に該当する場合には、個人データについて、安全管理措置を行い（同法第 23 条）、また、委託先に対して必要かつ適切な監督を行わなければならない（同法第 25 条）とされている。クラウドサービスにおいてユーザが取り扱うデータに個人情報が含まれている場合、クラウドサービスを利用することが、クラウドサービス提供事業者に対する個人データの「提供」に該当するかを検討し、対応しなければならない（Q15 参照）。

また、クラウドサービスにおいては、複数の事業者が関与し、クラウドサービス提供事業者間で API（Application Programming Interface）連携や ID 連携によって情報の交換を行っていることがあるが、提供又は受領する情報の中に個人データが含まれていて個人データを取り扱うこととなる場合、各事業者において、個人データの第三者提供に係る本人同意を得る等、個情法の規律を遵守してサービスを利用する必要がある[7]。

（イ）不正競争防止法との関係

クラウドサービスは外部リソースの利用ではあるが、クラウドサービスにより営業秘密の管理を行っていたとしても、そのこと自体で、営業秘密と認められるための要件である秘密管理性が失われることはない[8]。もっとも、クラウドサービスに従業員全員がアクセスできるような場合には、適切なアクセス管理がなされておらず、秘密管理性が失われることがある。

（ウ）ライセンス、守秘義務契約等

ユーザがクラウドサービスにおいて利用するデータ等については、別の企業やベンダとの間で締結したライセンス契約や守秘義務契約の対象となっており、当該ライセンス契約等に第三者への開示の禁止や、委託の禁止等の利用制限条項が入っている場合がある。

クラウドサービスを利用することが当該ライセンス契約等の対象となっているデータの第三者への開示や委託に該当するか否かは、当該契約の解釈によるため、明確ではない場合には、契約の締結に当たって解釈を確認することが必要である。

（エ）リージョン（地理的範囲）

クラウドサービスを利用する際に、どのリージョンのサーバが使われるのかについても法的に重要である。海外のサーバを利用してデータを処理する場合、特に公法については、原則として属地的にそのサーバが所在するリージョンの法律が適用される可能性がある[9]。

---

[7] 個情法との関係についても触れていて、クラウド利用にも参考になるものとして、NCO「クラウドを利用したシステム運用に関するガイダンス」（令和 5 年 7 月）がある（https://www.cyber.go.jp/policy/group/infra/cloud_guidance.html）。

[8] 営業秘密管理指針 14 頁。

[9] 適用法令は、私法と公法を分けて識別することが望ましい。例えば、私人間に適用される法は「当事者が当該法律行為の当時に選択した地の法による」（法の適用に関する通則法第 7 条）とされる。つまり、契約時に準拠法を定めるのが一般的であるため、契約当事者間の適用法令が問題になることは少ない。一方、国家が関わるわる公法の適用は、原則として属地的に定まる。外国法人でも日本国内において事業を行う限り、原則として国内法の適用を受け、逆に日本法人でも外国において事業を行う限り、外国法の適用を受けることがある。例えば、データセンターが外国にあっても我が国で事業を営む企業は、我が国の捜査機関の捜査を受け、外国のサーバ内の情報が差し押えられることがあり、逆にデータセンターが国内にあっても外国で事業を営む企業は、その国の捜査機関の捜査を受け、我が国のサーバ内の情報が差し押えられることがある（クラウドサービス利用ガイドライン 77 頁）。

また、個人データについては、越境移転の規制があり（個情法第 28 条）、海外リージョンのクラウドサービスを利用する場合には、越境移転に該当するか、越境移転に該当する場合、同条の要件を満たしているのかについて検討することが必要である（個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編））。また、仮に越境移転に該当しない場合についても、安全管理措置の一環としての外的環境の把握に注意が必要である（以上について、Q15 参照）。

さらに、クラウドサービスのリージョンが海外にある場合、海外のサーバを利用してデータを処理することが外為法にいう技術移転とされる可能性があるため、外為法の規制対象とならないかの確認も必要である（Q54 参照）。

イ　クラウドサービス提供事業者の開示情報の精査

クラウドサービス提供事業者からは、クラウドサービスの内容や、セキュリティについてのホワイトペーパーなどが開示されている。そこで、ユーザは、それらの開示情報を精査するなどして、提供されるサービス内容がクラウドサービスを利用する目的と合致しているか、また、クラウドサービスを利用して管理する情報資産のセキュリティレベルと合致しているかを確認することが必要である。確認又は検討すべき事項については、各種の基準やガイドラインで示されているセキュリティに関する事項[10]に加えて、法的には以下のような点が挙げられる。

（ア）契約当事者

上記のとおりクラウドサービスの提供は複数のクラウドサービス提供事業者の共同によって行われていることも多く、また、代理店による販売も一般的に行われている。そこで、クラウドサービスの導入について検討するに当たっては、交渉の相手方が、ベンダの立場となるのか、それとも代理店の立場となるのかについて確認し、相手方の立場に応じた契約内容を選択する必要がある。

また、クラウドサービスについては、サービス自体の提供者と保守、運用を行っている窓口が異なっていることも多い。このような場合にも、適切な相手方を選択し、適切な契約形態を選択しなければならない。

（イ）責任分界

クラウドサービスは第三者の提供するサービスをユーザが利用することになるため、クラウドサービス提供事業者とユーザとの間で、どちらがどこまで責任を持つのかについてあらかじめ決められているかを確認することが重要である。

また、クラウドサービスの提供形態の複雑化により、複数のクラウドサービス提供事業者が関与してクラウドサービスを提供しているケースがあり、これらのクラウ

[10] クラウドサービス利用におけるセキュリティの検討事項についての規格としては、ISO/IEC27017（JIS Q 27017）がある。また、ユーザ向けのガイドラインとして、クラウドサービス利用ガイドライン、クラウドサービス提供ガイドラインも参照されたい。

ドサービス提供事業者間の責任分界が決められているかについても確認することが重要である。

（ウ）クラウドサービス提供事業者間での情報共有

複数のクラウドサービス提供事業者が関与してサービスを提供している場合には、ユーザの情報資産がクラウドサービス提供事業者間で共有されるのかを確認することも重要である。複数の事業者間で共有される場合、前述した個情法やライセンス関係の制限があり、改めて別の契約を締結する必要があるなど、手当てを行う必要が生じることがある。

（エ）サービスの内容やサービスレベル

クラウドサービスのうち、インフラ系のクラウドサービスについては、サービスの内容が比較的定型的であり、稼働率や平均復旧時間などの指標が開示されていることがある。したがって、サービス内容の把握については比較的容易であるといえる。しかし、一方で SaaS 等のアプリケーション寄りのクラウドサービスについては、提供されるサービスが不定型であるという特色があり、また、サービス内容についても、機能の追加などが予定されていることが少なくない。そこで、そのサービス内容について明確に記述することが難しいこともあり、どこまでのサービスが提供されるのかを明確に把握することが難しいことがある。

（オ）事故時の対応

情報漏えい等のインシデント時にどのような対応が行われるかについても確認しておくことが重要である。具体的には、サイバーセキュリティインシデントが発生した場合の報告義務、報告の方法、賠償責任の範囲などを確認することになる。

セキュリティレベルを高く設定していたとしても、クラウドサービスで利用しているデータについては、セキュリティ事故により消失してしまったり、利用が一部できなくなったりする可能性がある。そこで、データをバックアップすることが必要であるが、バックアップがクラウドサービスの標準サービスとして設定されているのかについて確認しておく必要がある。

（カ）データポータビリティ

ユーザがクラウドサービスの利用を開始した後に、サービスを乗り換えたい、初期の目的を達成したために解約したい、サービス提供事業者が倒産した等、契約を終了する局面が発生することが予想される。そこで重要となるのが、契約が終了した場合にユーザがクラウドサービス上に入力、集計、加工したデータやアプリケーションを回収できるか、その後他の環境で再利用できるか（データのポータビリティ、アプリケーションの相互運用性）という点である。これらのデータやアプリケーションをユーザが契約終了時に出力して受領する権利の有無と条件、データ形式の種類に応じた出力の可否（ユーザ自身の環境又は他のサービス提供事業者のサービスにおいて

移行・再利用可能な形式かどうか)、その容易性はどうか等の点が、どのように定められているかについて、検討しておく必要がある。

（キ）データの消去

クラウドサービスは仮想化された環境で提供されることが多く、クラウドサービス契約が終了した場合には、別のユーザがその環境を利用することになる。クラウドサービス上にデータを残しておくと、何らかのサイバーセキュリティインシデントが発生して、情報の漏えいが生じる可能性がある。そこで、終了したサービス上からデータが確実に削除されるかという問題がある。また、削除はクラウドサービス提供事業者側で行われるので、削除がなされたことについてどのように担保するかという問題がある。そこで、契約終了時及びサービス終了時にデータ消去がなされるかどうか、また消去がなされるとして、作業が行われたことの担保はどのように行われるかを確認しておく必要がある。

（ク）サポート

クラウドサービスの利用方法が不明な場合のみならず、サイバーセキュリティインシデントが発生したような場合にも、クラウドサービス提供事業者側からのサポートが確実に受けられるかを確認することが必要である。特に、クラウドサービス提供形態の複雑化により、窓口になっているクラウドサービス提供事業者とクラウドサービスを提供しているクラウドサービス提供事業者が異なることがある。また、クラウドサービスが、国外のクラウドサービス提供事業者によって提供されている場合には、サポートが日本語で提供されているかが重要になることがある。

（ケ）初期設定

クラウドサービスは初期設定のまま利用されることが少なくないが、利用の方法によっては、初期設定ではセキュリティが十分ではないこともある。そのため、クラウドサービスにおける初期設定はどのようになっているか、権限設定の不備がないかを確認する必要がある。

ウ　第三者による監査・認証

クラウドサービスのセキュリティについても、どのようなセキュリティポリシーを定めているのか、人的管理をどのように行っているのか、アクセス制御を行うのか、情報資産の保存に暗号を利用するのかなど、オンプレミスの環境についての情報セキュリティと同様の問題がある。もっとも、クラウドサービスについては、物理的に外部リソースを利用することになるため、情報セキュリティについてもクラウドサービス提供事業者側に委ねざるを得ない。そこで、実際に情報セキュリティが確保されているかについて、監査をすることが必要となるが、コストや能力の観点からユーザ側では実効性のある監査をなし得ないことが多く、第三者が行ったセキュリティ監査の結果を確認することも選択肢となる。第三者認証としては、ISO/IEC27017（JIS Q 27017)、日本公認会

計士協会が実務指針を公開している「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」[11]などがある[12]。

エ　責任共有モデル（Shared Responsibility Model）の理解

クラウドサービスを利用するに当たっては、責任共有モデル（Shared Responsibility Model）について理解していることが前提となる。責任共有モデルとは、ユーザ及びクラウドサービス提供事業者が、上記イ（イ）の責任分界点を定めるだけでなく、運用責任を共有し合っているという考え方である[13]。各クラウドサービス提供事業者やクラウドサービスによって責任共有モデルの考え方が異なる場合があるものの、いかなるクラウドサービスであっても、組織としての活用の目的や指針、設定や接続する端末の安全性の確保、クラウドサービスにより管理又は生成されるデータ等の取扱いは基本的にユーザ側の責任であることを認識する必要がある。また、上記のとおり、クラウドサービスの提供は複数のクラウドサービス提供事業者の共同によって行われることも多く、また、代理店による販売も一般的に行われるなど、クラウドサービスには多数のステークホルダーが関与しており、一般的にユーザ側に責任がある領域についても外部に委託している場合や外部からの支援を受けている場合があることから、責任共有モデルはこれらのステークホルダーを踏まえた上で理解する必要がある。

（３）クラウドサービスに関する契約

以上のとおり検討したクラウドサービスの内容については、契約として法的拘束力を持たせておくことが望ましい。契約関係については、上記の検討事項に加えて、以下の点の検討が重要である。

ア　定型約款への該当性

クラウドサービスは多数のユーザに対して画一的に安価にサービスを提供することに特徴がある。一方で、特に事業者間の契約においては、契約内容について交渉が行われることもある。そこで、クラウドサービス契約を締結する場合には、その契約がひな型であり、修正が可能であるのか、それとも定型約款[14]となるのかについて検討することが必要である。

---

11 日本公認会計士協会「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」（https://jicpa.or.jp/specialized_field/20190401gff.html）。

12 その他、米国公認会計士協会により実務指針が策定されているサービス・オーガニゼーション・コントロール報告書（SOC、SOC1、SOC2）がある。また、業界ごとの認証として PCI DSS（Payment Card Industry Data Security Standard）（Q18 参照）等がある。

13 前掲注 4・NCO「クラウドを利用したシステム運用に関するガイダンス」（令和 5 年 7 月）11 頁。

14 民法第 548 条の 2 第 1 項によれば、定型約款とは、定型取引（ある特定の者が不特定多数の者を相手方として行う取引であって、その内容の全部又は一部が画一的であることがその

定型約款に該当する場合、当該クラウドサービス契約については、原則として民法の定型約款に関する規定（同法第 548 条の 2 から第 548 条の 4）の適用を受ける。

イ　契約締結の相手方の選択

クラウドサービス提供の複雑化により、複数のクラウドサービス提供事業者の共同によってクラウドサービスが行われていることも多く、また、代理店による販売も一般的に行われている。そこで、契約を締結しようとしている相手方が契約の当事者として適切なのかどうか、他の当事者とも契約を締結するべきではないかの検討が必要である。

ウ　法的拘束力が及ぶ範囲

前記したクラウドサービス締結に当たって検討した点については、努力目標として定められているものなのか、又はクラウドサービス提供事業者とユーザとの間の合意として法的拘束力がある形となるのか否か[15]を確認し、必要に応じて法的拘束力を持たせる形で契約を締結するため交渉をすることを検討する。

エ　取り扱う情報の性質

クラウドサービスにおいて管理されている情報資産については、情報セキュリティを確保するに当たって、クラウドサービス提供事業者側も技術的にアクセスできることが多い。情報資産について、個人データが含まれていたり、営業秘密として管理していた情報であったりする場合、その性質に応じ、秘密保持条項や監査条項により管理を行わなければならないことがある。

オ　責任制限

クラウドサービス契約においては、クラウドサービス提供事業者側の責任を免除したり、一部制限したりする条項が置かれることがある。責任免除条項や責任制限条項については、事業者と消費者との間の契約であれば消費者契約法（平成 12 年法律第 61 号）による規制があるほか（消費者契約法第 8 条第 1 項）、事業者間の契約であっても、当該契約が民法第 548 条の 2 にいう定型約款に該当すれば、不当条項規制（民法第 548 条の 2 第 2 項）の適用を受けることとなる可能性があるため、その点検討が必要である（Q61 参照）。

双方にとって合理的なもの）において、契約の内容とすることを目的としてその特定の者により準備された条項の総体とされている。

[15] 電子商取引準則 260 頁～「Ⅲ-6 SaaS・ASP のための SLA（Service Level Agreement）」も参照されたい。

（4）クラウドサービスのアクセス管理者が複数の場合の不適切なアクセス

クラウドサービスは、提供事業者によってその利用形態には様々なものが存在し、当該サービスの明確な分類が困難な状況になっている。これらのクラウドサービスは、形態によって多数の者が関与することとなり、例えば、クラウドサービスを提供する事業者（クラウド事業者)、クラウドサービスの販売事業者、クラウドサービスの利用事業者、クラウドサービスを含めて構築されたシステムの運用を支援する運用事業者等があり得る。これらの者の中には、アクセス管理者に該当する者が複数存在することもある。

クラウド事業者が提供するサービスにおいて、複数のアクセス管理者が存在する場合、アクセス管理者 A が外部者等からのアクセスを意図していないにもかかわらず、アクセス管理者 B の行為によって外部からアクセスできてしまった場合に、当該アクセスをした者は、アクセス管理者 A が意図していないアクセスをしたという意味では不適切なアクセスといえるが、当該行為が不正アクセス行為に該当するのかが問題となる。

この点、アクセス管理者は、特定電子計算機の動作を管理する者をいい、クラウドサービスへのアクセスを誰に認めるかという動作の管理をする権原を有していれば、アクセス制御機能による特定利用を制限することが可能なアクセス管理者となり得る。そのため、前述のとおり、このようなクラウドサービスにおいては、複数の管理者が存在することとなる。この場合において、個々の管理者の権原、つまり、アクセス制御機能による特定利用を制限する範囲が相互に排他的であれば大きな問題は生じないと考えられる。すなわち、アクセス管理者 A が外部者等からのアクセスを意図しておらずアクセス制御機能による特定利用を制限している一方で、アクセス管理者 B が外部者等からのアクセスに対してアクセス制御機能による特定利用を制限していない場合、外部からアクセス管理者 B の管理範囲にアクセスしたとしても、特定利用の制限を免れたとはいえず、不正アクセス行為には該当しないと考えられる。

他方、複数の管理者が存在し、個々の管理者としてアクセス制御機能による特定利用を制限する範囲が相互に重なり合う場合には問題が生じ得る。このような場合に、アクセス管理者の有する権原の範囲は、クラウドサービスにおける管理形態や利用規約、管理者間の関係等に依存し得るため、一律にクラウドサービスにおける当該特定利用の制限をしたのは、どの管理者であるかを決することが困難になる。

よって、複数の管理者が存在し、個々の管理者として有する権原の範囲が相互に重なり合う場合には、外部からアクセスした者の行為が不正アクセス行為に該当するか否かを直ちに判断できるわけではない点に留意すべきである。

しかし、不正アクセス行為に該当するかどうかにかかわらず、クラウドサービス等においては、アップデートに伴うサービスの仕様変更・設定変更等に起因して、あるアクセス管理者が意図していない情報にアクセスされるというデータの機密性に関わる問題が生じ得る。過去にそれが大きく問題となった事案もあった。同様の不適切なアクセス行為を防止するためにも、クラウド事業者は、不適切なアクセスが可能となり得る仕様変更を実

施する場合には、クラウドサービスの運用事業者を含めた利用事業者らに対して繰り返し注意喚起を行い、運用事業者らはクラウドサービスのアップデート等がなされた際には必ずアクセス制御機能の設定等について確認する運用にすることが望ましい。

（５）（参考１）政府情報システムのためのセキュリティ評価制度

政府機関等におけるクラウドサービスの導入にあたり情報セキュリティ対策が十分に行われているサービスを調達できるようにすべく、令和 2 年 6 月に NCO（旧 NISC）、デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）、総務省及び経済産業省の連携の下、「政府情報システムのためのセキュリティ評価制度」（Information system Security Management and Assessment Program、以下、本項において「ISMAP」という。）を立ち上げた。

ISMAP の基本的な枠組みは、国際標準等を踏まえて策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、クラウドサービスを登録する制度である。

政府機関は、原則として ISMAP 等クラウドサービスリスト[16]に掲載されたサービスから調達を行うところ、令和 3 年 3 月に初回の ISMAP クラウドサービスリストの登録及び公開が行われ、政府機関による本制度の利用を開始した。また、令和 4 年 11 月には、ISMAP の枠組みのうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みである「ISMAP-LIU」の運用を開始した。なお、ISMAP 等クラウドサービスリストは、IPA が運用する ISMAP ポータルサイト[17]にて公開されている。

統一的なセキュリティ要求基準に基づき安全性が評価されたクラウドサービスは ISMAP 等クラウドサービスリストへの追加登録が継続的に行われており、政府機関における ISMAP の利用が推進されている。なお、ISMAP の運用状況を踏まえ、統一的なセキュリティ要求基準等の見直しが行われることが予定されている。

ISMAP 等クラウドサービスリストは、民間においても参照することで、クラウドサービスの適切な活用が推進されることが期待されている。

（６）（参考２）自治体におけるクラウド利活用

地方自治体の関係では、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説した総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」がある。

同ガイドラインでは、情報セキュリティ基本方針と情報セキュリティ対策基準から構成される情報セキュリティポリシーの例文や例文に対応する解説を付しており、クラウ

---

16 ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト
https://www.ismap.go.jp/csm?id=cloud_service_list
https://www.ismap.go.jp/csm?id=cloud_service_list_liu

17 https://www.ismap.go.jp/csm

ドサービスの利用に関しても、情報セキュリティ対策基準の例文として、①取り扱う情報の格付及び取扱制限を踏まえて業務に係る影響度等を検討した上でクラウドサービスの利用を検討する、②クラウド上の情報に対して海外法令が適用されるリスクを評価して委託先を選定し、必要に応じて準拠法・裁判管轄を指定する、③クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討する、④クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるようにセキュリティ設計を行い、セキュリティ要件を定める、⑤クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価する旨が定められている。

３．参考資料（法令・ガイドラインなど）

・サイバーセキュリティ戦略本部「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」
https://www.cyber.go.jp/pdf/policy/general/wakugumi2021.pdf
・デジタル社会推進会議幹事会決定「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和 5 年 9 月 29 日）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf
・ISO/IEC27017、JIS Q 27017
・総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」（令和 3 年 9 月）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html
・総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」（令和 4 年 10 月）
https://www.soumu.go.jp/main_content/000843318.pdf
・総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 8 年 3 月版）」
https://www.soumu.go.jp/main_content/001064404.pdf
・経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（2013 年度版）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf
・The cloud security alliance「クラウドコンピューティングのためのセキュリティガイダンス」（日本語版 ver5.0）
・電子商取引準則
・NCO「クラウドを利用したシステム運用に関するガイダンス」（令和 7 年 5 月）
https://www.cyber.go.jp/policy/group/infra/cloud_guidance.html

４．裁判例

特になし

Q43 AI のサイバーセキュリティ

人工知能関連技術の研究開発及び活用の推進に関する法律（いわゆる AI 法）及び AI 事業者ガイドライン（第 1.2 版）はどのような内容を定めているのか。また、それらは AI システムのサイバーセキュリティ確保として何を望ましいと位置づけ、事業者にどのような対応を期待しているか。

タグ：AI、リスク管理体制、モニタリング

１．概要

人工知能関連技術の研究開発及び活用の推進に関する法律（令和 7 年法律第 53 号。令和 7 年 5 月 28 日成立、令和 7 年 9 月 1 日施行。以下、本項において「AI 法」という。）は、人工知能に関する技術（人工知能関連技術）が我が国の経済社会の発展の基盤となる技術であることに鑑み、当該技術の研究開発及び活用の推進に関する施策について、基本理念並びに基本的な計画の策定その他の施策の基本となる事項を定めるとともに、人工知能戦略本部を設置することにより、人工知能関連技術の研究開発及び活用の推進に関する施策の総合的かつ計画的な推進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とするものである。

AI 法では、同法第 13 条において、国際的な規範の趣旨に即した指針を国が整備することとされており、2025 年 12 月に AI 戦略本部において「人工知能関連技術の研究開発及び活用の適正性確保に関する指針」が取りまとめられた。この中では、サイバーセキュリティについて、事業者をはじめとする各主体が研究開発、活用する AI の特性、用途、目的や、自身の立場、社会的役割等を踏まえて自主的に取組を進める上で考慮すべき主な要素の一つとして、不正な操作による AI の意図しない動作や停止をはじめとする AI のセキュリティ上のリスクを低減させるよう、AI のセキュリティを適切に確保する旨が明示されている。

また、AI 事業者ガイドラインは、AI 開発・提供・利用に当たって必要と考えられる取組についての基本的な考え方を示すことにより、事業活動において AI を活用する者が AI のリスクを正しく認識すること等を通じ、イノベーションの促進と AI のライフサイクルにわたるリスクの緩和を両立する枠組みを政府と AI 事業者とで共創することを目指すものであり、法的拘束力はない。従前の総務省主導の「国際的な議論のための AI 開発ガイドライン案」及び「AI 利活用ガイドライン～AI 利活用のためのプラクティカルリファレンス～」と、経済産業省主導の「AI 原則実践のためのガバナンス・ガイドライン Ver.1.1」

を統合・見直したものである。令和 6 年 4 月 19 日に第 1.0 版として策定、令和 7 年 3 月 28 日に第 1.1 版、令和 8 年 3 月 31 日に第 1.2 版が公表され、適宜更新されている[1]。

２．解説

（１）AI 法の概説

AI 法は、人工知能関連技術について、各主体の責務等を定める。

「人工知能関連技術」とは、人工的な方法により人間の認知、推論及び判断に係る知的な能力を代替する機能を実現するために必要な技術並びに入力された情報を当該技術を利用して処理し、その結果を出力する機能を実現するための情報処理システムに関する技術と定義されている（AI 法第 2 条）。

AI 法が責務等を定める各主体は、国、地方公共団体、研究開発機関[2]、活用事業者[3]及び国民である。

もっとも、AI 法は、活用事業者に対し、AI の開発や利活用におけるサイバーセキュリティ確保の責務を具体的に定めるものではないため、活用事業者は、AI 事業者ガイドライン等を参照し、サイバーセキュリティの確保に関して具体的に定める事項を参考にすることが期待される。

（２）AI 事業者ガイドラインの解説

ア　用語

AI 事業者ガイドラインにおける主要な用語[4]は、以下のとおりである。

- 「AI」については、現時点で確立された定義はなく、広義の人工知能の外延を厳密に定義することは困難であるとしつつ、本ガイドラインにおいては、「AI システム自体又は機械学習をするソフトウェア若しくはプログラムを含む抽象的な概念」とされている。
- 「AI システム」とは、「活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム（機械、ロボット、クラウドシステム等)」とされている。

---

[1] 総務省及び経済産業省・IPA/AISI による共管。総務省：https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html、経済産業省・IPA/AISI：https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/index.html

[2] 科学技術・イノベーション創出の活性化に関する法律（平成 20 年法律第 63 号）第二条第九項に規定する研究開発法人その他の人工知能関連技術の研究開発を行う機関をいう（AI 法第 6 条)。

[3] 人工知能関連技術を活用した製品又はサービスの開発又は提供をしようとする者その他の人工知能関連技術を事業活動において活用しようとする者をいう（AI 法第 7 条)。

[4] AI 事業者ガイドライン第 1 部。

イ　AI 事業者ガイドラインの位置づけ等

AI 事業者ガイドラインに法的拘束力はなく、AI 開発・提供・利用に当たってのリスク及びリスク対策の方向についての基本的な考え方を示すものであり、活用事業者としては、サイバーセキュリティ含め、自主的に具体的な取組を推進することが期待されている。

また、AI の利用は、その分野と利用形態によっては、社会に対して大きなリスクを生じさせる可能性がある一方で、過度な対策を講じることは AI 活用によって得られる便益を阻害する可能性がある。これを踏まえ同ガイドラインでは、当該利用分野における利用形態に伴って生じうるリスクの大きさ（危害の大きさ及びその蓋然性）を把握したうえで、その対策の程度をリスクの大きさに対応させる「リスクベースアプローチ」が重要であるとしている。

ウ　AI 事業者ガイドラインの構成

AI 事業者ガイドラインの第 3 部～第 5 部では、事業活動を担う主体を AI 開発者（AI Developer）、AI 提供者（AI Provider）、AI 利用者（AI Business User）の 3 つに区分し[5]、これらの主体ごとにリスクやその対応の方針が記載されている。これら 3 つの主体は、AI 活用の場面において相互に関連性を有して活動することが想定されるため、自らが該当する主体以外の記載も参照することにより、自らの AI 活用の取組に活かすことも期待されている。

（3）AI 事業者ガイドラインにおけるサイバーセキュリティ確保に関する事項

AI 事業者ガイドラインは、AI の事業活動を担う主体が取り組むべき事項を 10 の「共通の指針」として整理しており、「セキュリティ確保」についてもその 1 つに含まれている。各主体が AI のライフサイクル全体で実装すべき方向性を「①AI システム・サービスに影響するセキュリティ対策」及び「②最新動向への留意」の二つに分けた上で、具体的に示している。

特に、上記①として、AI システム・サービスの「機密性(Confidentiality)」、「完全性(Integrity)」、「可用性(Availability)」（CIA）を維持しつつ、開発・提供・利用の各時点の技術水準に照らした合理的対策を継続的に講じることが明示されている[6]。

加えて、主体ごとに、ライフサイクルごとの「セキュリティ確保」に関する事項も示されている。例えば、AI 開発者については、AI 開発時に「セキュリティ対策のための仕組みの導入」として「AI システムの開発の過程を通じて、採用する技術の特性に照らし適切にセキュリティ対策を講じる（セキュリティ・バイ・デザイン）」という考え方や、AI

[5] なお、事業活動以外で AI を利用する者又は AI を直接事業で利用せずに AI システム・サービスの便益を享受する、場合によっては損失を被る者（業務外利用者）は、本ガイドラインの名宛人には含まれない。
[6] AI 事業者ガイドライン第 2 部 C.(5)①。

開発後においては「最新動向への留意」として「AI システムに対する攻撃手法は日々新たなものが生まれており、これらのリスクに対応するため、開発の各工程で留意すべき点を確認する」といった考え方が示されている。

さらに、「高度な AI システムを開発する開発者」については、AI のライフサイクル全体にわたってサイバーセキュリティを含む「強固なセキュリティ管理に投資し、実践する」という考え方が追加的に示されている。

なお、令和 7 年 12 月の総務省「AI セキュリティ分科会」による取りまとめ[7]を踏まえて、AI 開発者及び AI 提供者を想定読者とした「AI のセキュリティ確保のための技術的対策に係るガイドライン」が令和 8 年 3 月 27 日付で公表されている[8]。当該ガイドラインは、大規模言語モデル（LLM）及び LLM を搭載したシステムを主な対象とし、不正操作による機密情報の漏えい、AI システムの意図せぬ変更や停止が生じないような状態に対する脅威への対策を主な対象としている。

（４）民間事業者が国などの政府機関から業務を受託する際の留意点

民間事業者が国又は独立行政法人等から情報システム（生成 AI 等を含む）に関連する業務を受託する場合は、政府機関等統一基準群[9]に規定する外部委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。そのため、当該民間事業者において、当該業務を受託し、受託業務の中で AI 等を活用することが想定される場合には、要求され得る条件を適切に把握しておく必要がある。

統一基準群においては、AI 又は生成 AI を明示的に対象とした記載はまだ存在しないものの、AI を含む高度情報処理システム・自動化システム・クラウドサービス・ソフトウェア供給網などについてはリスク管理の対象となる。

具体的には、民間事業者としては、以下の点などに留意する必要がある。

ア　クラウドサービスの利用について

生成 AI 等のサービスについては、クラウド上でサービスを展開しているものが多く、サービス利用に当たっては定型約款や規約等への同意のみで利用が可能となることが多い。もっとも、このような生成 AI サービスについては、セキュリティ対策やデータの取扱いなどについて個別に特別な扱いを求めることができない場合が多い。そのため、

---

[7] AI セキュリティ分科会取りまとめ（令和 7 年 12 月）（https://www.soumu.go.jp/main_content/001051814.pdf）。

[8] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00282.html

[9] 凡例・略称のとおり、政府機関等統一基準群を構成する文書は以下のとおりである（https://www.cyber.go.jp/policy/group/general/kijun.html）。
・政府機関等のサイバーセキュリティ対策のための統一規範（令和 7 年度版）
・政府機関等のサイバーセキュリティ対策のための統一基準（令和 7 年度版）（以下、本項において「統一基準」という。）
・政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）

原則として要機密情報（機密性 2 情報及び機密性 3 情報をいう[10]。）を取り扱うことができない点について留意が必要である[11]。なお、要機密情報を取り扱わない場合であっても、利用するサービスの定型約款、その他の提供条件等を踏まえ、受託業務に利用することが可能か、検討することが必要である。

また、政府調達におけるクラウド利用は、要機密情報を取り扱う場合、統一的なセキュリティ要求基準（ISMAP 管理基準）に基づいたセキュリティ対策を実施していることが第三者（ISMAP 登録監査機関）により確認されたサービスが登録されている ISMAP 等クラウドサービスリストに登録済みのサービスから選定することが原則である。生成 AI の推論 API や学習用 SaaS を採用する場合も、対象サービスが ISMAP（又は ISMAP-LIU）に登録されているかを確認し、サービス名・版・掲載日を記録する。登録されていないサービスを採用する場合は、発注者の例外承認や代替管理策の提示が実務上求められる[12]。

イ　国外のデータセンター等にサーバ装置を設置している場合

生成 AI 等のサービスにおいては、国外のデータセンター等にサーバを設置してサービスを提供している場合がある。この場合、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性があり、国等においては当該リスクを受容するか又は低減するための措置を講ずることが可能かを検討した上で、利用可能な業務の範囲を定めることになる。そのため、民間事業者においては、要求される調達基準に利用する生成 AI サービスの仕様が適合しているか、検討する必要がある。また、国外のデータセンター等にサーバを設置してサービスを提供している生成 AI を利用する場合には、必然的にデータの越境移転が生じることとなる。そのため、委託者との契約のほか、委託者及び受託者に対して個人情報保護法その他のデータ関連法令が適用されるかどうか、及び当該法令が要求する規制を遵守できる体制を構築しているかは、検討する必要がある。

また、政府における生成 AI の利活用促進とリスク管理に関するガバナンス、各府省庁における調達・利活用時のルールを定める観点から、デジタル社会推進会議幹事会による「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」[13]が決定・公表されている。同ガイドラインでは、例えば生成 AI の調達・利活用のルールにつ

---

10 統一基準 3 頁。
11 統一基準 31 頁。
12 NCO「政府情報システムのためのセキュリティ評価制度（ISMAP）」（https://www.cyber.go.jp/policy/group/general/ismap.html）
13 デジタル社会推進会議幹事会「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」（令和 7 年 5 月 27 日）（以下、本項において「AI 調達・利活用ガイドライン」という。）（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/80419aea/20250527_resources_standard_guidelines_guideline_01.pdf）

いて、企画・調達・開発・構築・リリース前準備や[14]、生成 AI システム特有のリスクケースへの対応というライフサイクル全体をカバーし[15]、調達チェックシート・契約チェックシート・高リスク判定シートなど具体的ツールを用いて運用する構成が示されている[16]。そのため、民間事業者としてもこのような運用ルールについて理解を深めておくことが望ましい。

加えて、地方公共団体が取り扱う情報システムについては、「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 8 年 3 月版）」[17]が公表されている。同ガイドライン中では AI に関して特有の言及はないものの、民間事業者としては、地方公共団体の業務に関わるシステム全体を通じて、当該システムが ISMAP 登録されるなどによりセキュリティ対策が講じられているものか、サービス提供事業者の所在国やサーバの設置場所等を踏まえて当該システムにどの国の法令が適用されるか確認されているかなど、各地方公共団体の情報セキュリティポリシーとの関係を踏まえた対応が必要になる[18]。詳細は Q4 を参照されたい。

（５）（参考）人工知能基本計画（AI 基本計画）

令和 8 年 7 月 14 日、第 2 期「人工知能基本計画」[19]が閣議決定された。AI ガバナンスの観点から、「不具合の連鎖による大規模障害といった技術的リスク、責任の所在の曖昧化、雇用への影響といった社会的リスク、自律型のサイバー攻撃といった安全保障上のリスクが懸念され、適時適切の対応が一層求められる。特にサイバーセキュリティ上の脅威は、ＡＩによる自律型攻撃により未知の脆弱性の発見がされるなどの形で顕在化している。これらの脅威に対応し「信頼できる AI」を実現するためにも、サイバー防御の強化が不可欠である。」（14 頁）など、AI とサイバーセキュリティの関係性に関しても言及されている。

（６）（参考）Project YATA-Shield

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況である。こうした喫緊の課題に対して、令和 8 年 5 月 18 日に国家サイバー統括室が中心となり、関係省庁・関係機関の緊密な連携の下、政府一体となって対応するため、

[14] AI 調達・利活用ガイドライン 6.3
[15] AI 調達・利活用ガイドライン 6.7
[16] AI 調達・利活用ガイドライン 6.1.2、別紙 1、別紙 3、別紙 4 等
[17] 平成 13 年 3 月 30 日策定・令和 8 年 3 月 27 日最終改定（https://www.soumu.go.jp/main_content/001064404.pdf）。
[18] 同ガイドライン第 2 章 3(2)②
[19] https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html

AI 性能の高度化を踏まえたサイバーセキュリティ対策パッケージ「Project YATA-Shield」をとりまとめた[20]。

重要インフラ事業者等への対応と脆弱性の発見・修正等に関する対応の 2 つの観点から、我が国のサイバー対処能力の更なる強化を目指している。

３．参考資料（法令・ガイドラインなど）

・人工知能関連技術の研究開発及び活用の推進に関する法律
・「人工知能関連技術の研究開発及び活用の推進に関する法律（AI 法）の概要」[21]
・「人工知能関連技術の研究開発及び活用の推進に関する法律案に対する附帯決議」（第 217 回国会閣法第 29 号　衆議院附帯決議）[22] [23]
・AI 事業者ガイドライン（第 1.2 版）
・「AI 事業者ガイドライン（第 1.2 版）」別添（付属資料）
・「AI のセキュリティ確保のための技術的対策に係るガイドライン」本編
・「AI のセキュリティ確保のための技術的対策に係るガイドライン 別添（付属資料）」
・「AI 事業者ガイドライン案」に対するご意見及びその考え方
・「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」
・「地方公共団体における情報セキュリティポリシーに関するガイドライン」

４．裁判例

特になし

[20] https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf
[21] https://www8.cao.go.jp/cstp/ai/ai_hou_gaiyou.pdf
[22] https://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikaku2C59590D86DDF9A049258C73000C0C74.htm
[23] https://www8.cao.go.jp/cstp/ai/ai_hou_sangiin_futai.pdf

Q44 Web サービスにおける本人確認とサイバーセキュリティ

「本人確認」とはどのような概念か。また、本人確認を求める法制度としてどのようなものがあり、なりすましが起きた際の法的問題はどのようなものがあるか。

タグ：個情法、公的個人認証法、犯収法、出会い系サイト規制法、古物営業法、携帯電話不正利用防止法、本人確認ガイドライン、認証、認可、アクセス制御、本人確認、顔認証、安全管理措置、eKYC、なりすまし

１．概要

デジタル庁は、デジタル社会推進標準ガイドライン「DS-511」（以下「本人確認ガイドライン」）において、本人確認の基本的な枠組み（身元確認、当人認証、フェデレーション）や想定される脅威に応じた対策基準等を整理している[1]。当該整理によれば、本人確認は、窓口手続やサービスの初回登録時等に行う「身元確認」と登録済みサービスへのログイン時等に行う「認証（当人認証）」に大別され、特に後者に関してインターネットにおける特定の機能の利用等の権限やアクセス権を付与する仕組みとして、認証、認可、アクセス制御といったものが挙げられる。また、法令上本人確認が求められていることがあるが、本人確認における脅威の一つとして、存在する別の利用者としてサービスを利用する、なりすましが挙げられ、民事上、刑事上問題となり得る。

２．解説

（１）本人確認の構成要素

デジタル技術の普及・浸透を背景として、本人確認においてデジタルアイデンティティ[2]を取り扱う機会が急速に拡大しており、諸外国でも、デジタルアイデンティティに関するガイドライン等の見直しや新規制定が進められている[3]。このような環境の変化等を踏まえ、デジタル庁は、行政手続等での本人確認におけるデジタルアイデンティティの取扱いを最新の脅威・技術等に適応させるべく、本人確認ガイドラインを整備している。

---

[1] 本人確認ガイドライン P9-10 参照。
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/12cb1a6c/20250930_resources_standard_guideline_identityverification_01.pdf

[2] 「デジタルアイデンティティ」は、ある主体(Entity)をデジタル空間に置いて表現するための属性の集合のことを指す（本人確認ガイドライン 1 頁）。

[3] 例えば、米国国立標準技術研究所(NIST)が発行する米国連邦政府向けのデジタルアイデンティティガイドラインである SP 800-63 や、欧州デジタルアイデンティティ規則と称される eIDAS 2.0 等が代表的である。

同ガイドラインでは、本人確認について、サービスの初回登録時等に行う「身元確認(Identity Proofing)」と登録済みサービスへのログイン時等に行う「当人認証(Authentication)」に大別し、さらに、身元確認や当人認証を他者（信用できる ID・パスワードプロバイダ）に依拠して実現する手法として「フェデレーション（Federation)」を定義している[4]。

（２）身元確認（Identity Proofing）

身元確認は、申請者の属性情報を収集することで申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認することをいうとされている[5]。

身元確認における代表的な脅威として、①重複登録、②別人との誤紐づけ、③本人確認書類の偽造・改ざん、④本人確認書類の複製、⑤本人確認書類の盗用、⑥本人確認書類の貸し借り等が想定されるところ、①及び②の脅威には「属性情報の収集」のプロセスで、③及び④の脅威には「本人確認書類の検証」のプロセスで、⑤及び⑥の脅威には「申請者の検証」のプロセスで、それぞれ適正な手法を選択・実施すべきであり、本人確認ガイドラインでは、その具体的な手法とリスク度合いに応じた対策基準について整理されている[6]。

（３）認証（authentication）と認可（authorization）

認証とは、インターネット上においては、対象サービスを利用しようとする者が、身許確認時に登録された者と同一の人物であること(当人性)を確認すること[7]とされている。認証は、一般に「認証の 3 要素」と呼ばれる「知識情報（パスワードや暗証番号等、利用者本人のみが知り得る情報)」、「所持情報（秘密鍵を格納した IC カードやスマートフォン、ワンタイムパスワード生成器など、利用者本人のみが所持する物に関する情報)」及び「生体情報（顔、指紋、虹彩、静脈等、本人のみがもつ生体的特徴に関する情報)」のうち 1 つ以上を用いて行われる。1 つの要素を用いるものを「単要素認証」、複数の要素を組み合わせて用いるものを「多要素認証」という[8]。

---

[4] 詳細は、本人確認ガイドライン 9 頁以下を参照されたい。
[5] 本人確認ガイドライン 13 頁。
[6] 本人確認ガイドライン 13-27 頁参照。
[7] 本人確認ガイドライン 9 頁、28 頁以下。
[8] 具体的な実装方法や昨今増加している「リアルタイムフィッシング」と呼ばれる攻撃手法への耐性の有無については、デジタル庁　デジタル社会推進標準ガイドライン「DS-512 行政手続等での本人確認におけるデジタルアイデンティティの取扱に関するガイドライン 解説書」（以下、本項において、「本人確認ガイドライン解説書」という。）を参照。
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/c7edc43c/20260224_resources_standard_guideline_identityverification_1.pdf

そして、認可とは、特定の条件の下、利用者に特定の機能の利用の権限（アクセス権限）を付与することを指す[9]。例えば、SNS において、利用者がログインした場合、当該利用者に、当該 SNS の利用者のアカウントでの投稿を許可する場合などを指す。

そして、認証と認可を組み合わせて、正当に承認されている人を認証した上でその人にだけ特定の情報やリソースについてのアクセス権を付与し、主体を制限することをアクセス制御という。

なお、生体認証に関して、例えば顔認証では、顔画像等から生存する特定の個人を識別できれば個人情報に該当する。また、認証用に抽出した顔の特徴情報は、個人識別符号として個人情報に該当する。そのため、これらの情報の取扱いに当たっては、利用目的を特定した上で通知又は公表を行うなど、個情法に基づく取扱いが必要である。

（４）認証の活用

上記のように、認証機能を利用することで、誰にどの情報やどのリソースにアクセスさせるのかを管理し、情報についての機密性を確保することができる。そのため、個情法ガイドライン（通則編）においても、安全管理措置（個情法第 23 条）のうち、技術的安全管理措置として、個人データを取り扱う情報システムを使用する従業員を認証し、アクセス制御することが手法の例示の一つとして挙げられている。また、情報についての機密性を確保することができることから、営業秘密の要件である秘密管理性の確保にも活用することができる。

（５）当人認証手法の具体例

主要な当人認証の手法の１つとして、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号。以下、本項において「公的個人認証法」という。）に基づき、地方公共団体情報システム機構（Japan Agency for Local Authority Information Systems）[10]により運営されている「公的個人認証サービス」（Japanese Public Key Infrastructure：以下、本項において「JPKI」という。）を導入する方法がある[11]。

JPKI を利用した当人認証手法には、実物のマイナンバーカードに格納された電子証明書（利用者証明用電子証明書）やスマートフォンのマイナンバーカードに格納された電子

---

[9] 認可(Authorization)等の用語については、NIST SP 800-53, Rev 5（特に Appendix A）等も参照されたい。

[10] 地方公共団体情報システム機構法（平成 25 年法律第 29 号）に基づき、国と地方公共団体が共同で運営管理する法人であり、公的個人認証サービスの運営主体である。なお、Q4 2.(3)イも参照されたい。

[11] 公的個人認証サービスを利用している民間事業者は 1,246 社（令和 8 年 4 月 30 日時点）あり（https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction/mynumbercard-user-list）、公的個人認証サービスを含むマイナンバーカードの普及や利用拡大に向けた取組みは、政府全体で強力に推進されている。

証明書（移動端末設備用利用者証明用電子証明書）を用いるものがある[12]。これらの電子証明書を用いることで Web サイト等へのログイン時において、公開鍵認証による当人認証を行うことができ、どちらの手法においても実装において適切なフィッシング対策を講じることで[13]、フィッシング攻撃への耐性等の厳格な脅威耐性[14]を確保した多要素認証による当人認証を実現できる[15]。

民間事業者が JPKI を導入する場合は、公的個人認証法に基づき主務大臣認定を受けて自社が認定事業者になる方法と、認定事業者に利用者証明検証業務を委託して利用する方法の 2 つの方法があり、いずれの方法によっても、公的個人認証法等を遵守することが求められる。JPKI の導入を通じて、顧客サービス向上や事務コスト削減等の効果が期待される。

（６）本人確認等を具体的に要請する法令・制度

各種法令には、本人確認又は本人の属性の確認が義務とされているものがある。

まず、犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号。以下、本項において「犯収法」という。）第 4 条において、特定取引[16]を行う際に取引時確認を実施すべきことが義務づけられているところ、オンライン上だけで完結する確認方法も認められている（犯罪による収益の移転防止に関する法律施行規則（平成 20 年内閣府、総務省、法務省、財務省、厚生労働省、農林水産省、経済産業省、国土交通省令第 1 号。以下、本項において「犯収法規則」という。）第 6 条第 1 項）。その具体的な方法としては、同項の要件を充足する運転免許証等の写真付き本人確認書類の画像と容貌の画像で確認することが考えられる[17]。

このほかに、以下のような法令で本人確認又は本人の属性の確認が求められている。

---

[12] 利用者証明用電子証明書による当人認証は、マイナンバーカードを利用することによる所有物認証と利用者証明用暗証番号を入力することによる知識認証を組み合わせた多要素認証となり、移動端末設備用利用者証明用電子証明書による当人認証は、スマートフォンのマイナンバーカードを利用することによる所有物認証とスマートフォンで実行される当人認証（顔認証、指紋認証等）を組み合わせた多要素認証となる。

[13] フィッシング耐性を確保するためには、mTLS による相互認証やアクセス先ドメインの制限等の適切な実装が必要となる。

[14] フィッシング攻撃への耐性、暗号鍵の不正な取り出し・複製への耐性、オンライン上でのパスワードの推測への耐性、盗聴・リプレイ攻撃への耐性。

[15] これらの当人認証手法における脅威耐性と留意事項、またその他の当人認証手法については、本人確認ガイドライン解説書　別紙２　当人認証手法の具体例を参照されたい。

[16] 犯収法別表及び犯罪による収益の移転防止に関する法律施行令（平成 20 年政令第 20 号）第 7 条及び第 9 条を参照。例えば、銀行が行う預貯金契約の締結が一例である。

[17] なお、令和 9 年 4 月 1 日施行予定の犯収法規則では、本人確認書類の偽造等によるなりすまし等のリスクが高いと考えられる令和 8 年 8 月 6 日施行の犯収法規則における「ホ方式」・「リ方式」の廃止や、住民基本台帳法が適用されない海外在住者等を対象とした「ワ方式」・「カ方式」の新設等が予定されている。

① マッチングサイトなどの出会い系サイト事業者による、利用者が児童でないことを確認するための本人の年齢確認（出会い系サイト規制法[18]第 11 条）
② 古物営業による、古物取引の相手方の本人確認（古物営業法（昭和 24 年法律第 108 号）第 15 条第 1 項）
③ 携帯電話の販売業者等による、携帯電話の悪用を防ぐための、携帯電話等の契約・譲渡時の取引相手方の本人確認（携帯電話不正利用防止法[19]第 3 条第 1 項）

また、法令ではないが、決済事業者等とクレジットカードの連携に係る本人認証等についてのガイドライン[20]があり、決済事業者等がクレジットカードと連携させる場合は、当該ガイドラインに沿って本人確認のための認証等を実施する必要がある。

（7）なりすまし

上記のとおり、様々な場面で活用される認証に対する脅威の一つ[21]として、本人になりすますことが挙げられる。以下で、なりすましが起きた際の法的問題について紹介する。

ア　なりすましについての民事的論点

民事上の論点としては、本人になりすました者による意思表示の効果がなりすまされた本人に帰属するかという点がある。

まず、本人以外の者が本人になりすまして行った意思表示の効果は本人に帰属しないのが原則である。ただし、例外的に、表見代理（民法第 109 条、第 110 条、第 112 条）の規定は、本人の帰責性等の一定の要件の下、代理行為の効果の本人への帰属を認めている。表見代理制度は、あくまでも、相手方に、代理権がある旨を誤認した場合の制度であり、なりすましの場合に直接適用されるものではないが、判例において、代理人が直接本人名義で権限外行為を行い、相手方が当該行為を本人自身の行為と信じたことに正当事由がある場合に、民法第 110 条の類推適用を認めたものがある（最判昭和 44 年 12 月 19 日民集 23 巻 12 号 2539 頁）。

一方で、一定の方式に基づく認証がなされた利用者による意思表示の効果が本人に帰属する旨の事前同意がある場合は、原則として、同意した方法で認証された利用者による意思表示を本人による意思表示とみなし、契約が成立すると考え得るが、以下のような考慮が必要である。

---

18 正式名称は、「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」（平成 15 年法律第 83 号）。
19 正式名称は、「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」（平成 17 年法律第 31 号）。
20 一般社団法人日本クレジット協会「資金決済業者等とクレジットカードとの連携に係る本人認証等セキュリティガイドライン」（令和 3 年 3 月 24 日制定）（https://www.j-credit.or.jp/download/news20210330c1.pdf）
21 その他の本人確認に対する脅威については、本人確認ガイドライン「3. 本人確認における脅威と対策」を参照されたい。

まず、対等な当事者間（例：事業者間取引）において、上記のような本人確認方式について合意した場合は、契約自由の原則（民法第 521 条）の下、当該本人確認方式の効力が認められ、契約が成立すると考えられる。もっとも、定型約款（民法第 548 条の 2 第 1 項）の個別条項として事前合意される場合は、その内容如何によっては、民法第 548 条の 2 第 2 項により、定型約款の合意内容から排除されることがあるので留意が必要である。

次に、利用者が消費者であり、一方当事者が消費者ではない場合は、消費者契約法に基づく考慮も必要である。ID・パスワードを使ってログイン等した利用者を常に本人とみなし、事業者に帰責性がある場合でも利用者の行為が本人に効果が帰属する旨を本人との間で合意した場合、そのような合意は、消費者の利益を一方的に害するものとして無効となり得る（消費者契約法第 10 条）。例えば、インターネット通販におけるクレジットカードのなりすましによる利用については、本人ではない者がクレジットカード番号等を入力して商品を購入したとしても、現行の主なクレジットカード会員規約からすると、本人に帰責性がない限り、本人が支払義務を負わないとするケースが多い[22]。

イ　なりすましについての刑事的論点

例えば SNS で他の誰かになりすまして何らかの投稿をすると、著作権侵害や、名誉毀損で刑事罰を科される可能性がある。そして、なりすまして得た営業秘密を使用又は開示する行為については、営業秘密侵害罪に該当する可能性がある（不正競争防止法 21 条 1 項 1 号、2 号）。また、なりすましに必要な、ID やパスワード等を販売、公開する行為は、不正アクセス行為の禁止等に関する法律第 5 条により、同法に規定する識別符号の不正な提供であるとして刑事罰を科される可能性がある。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

本文中に記載したもののほか、

・最判昭和 44 年 12 月 19 日民集 23 巻 12 号 2539 頁

代理人が本人名で権限外の行為をした場合、相手方が本人の行為と信じ、その信頼に「正当な理由」があれば民法第 110 条を類推適用し本人に帰責させ得ると判示した事例。

・最判平成 15 年 4 月 8 日民集 57 巻 4 号 337 頁

盗難通帳と暗証番号が用いられ ATM で払戻しが行われた事案において、最高裁が、民法第 478 条の枠組みを前提に、銀行が免責されるには機械払いシステム全体の設置・

[22] 以上の詳細については、電子商取引準則 I-3-1「なりすましによる意思表示のなりすまされた本人への効果帰属」を参照されたい。

管理につき、無権限払戻しを可能な限度で排除する注意義務を尽くしたことが必要と判示した事例。

・最判平成 5 年 7 月 19 日集民 169 号 255 頁

真正なキャッシュカードと正しい暗証番号による ATM 払戻しについて、銀行の免責特約を原則有効とし、銀行側に暗証番号管理上の不備など「特段の事情」がない限り免責を認めた事例。

Q45 重要インフラ分野における規律の概要

各々の重要インフラ分野においては、サイバーセキュリティに関してどのような義務が課せられているか。法令上、どのような規定に着目すべきか。

タグ：重要インフラ、重要インフラ統一基準、重要インフラ行動計画、安全管理、保安規定、事故報告、報告徴求

１．概要

重要インフラ分野に属する事業者がサイバーセキュリティ対策を行うに当たっては、各々に適用される業法を始め、どのような規定があるかに着目すべきである。特に、サイバーセキュリティに関する情報の安全管理や保安規定の有無、事故の報告に関する規定の有無、所管省庁による報告徴求規定の有無について把握しておくことが肝要である。これらを把握するためには、重要インフラ統一基準、重要インフラ行動計画や関係する文書が参考になる。

２．解説

（１）重要インフラ分野

わが国の重要インフラ防護に関して、「重要インフラ」とは、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に、国民生活又は経済活動に多大な影響を及ぼすおそれが生じるもの」をいい、「重要インフラのサイバーセキュリティ対策のための統一基準」（重要インフラ統一基準）により、重要インフラ分野として、情報通信、金融、航空、空港、鉄道、電力、ガス、行政サービス、医療、水道、物流、化学、クレジット、石油、港湾及び郵便の合計 16 の分野が指定されている[1]。

また、分野に属する事業を営む者全てが重要インフラ事業者となるわけではなく、重要インフラ所管省庁において対象となる事業者等を特定することとされている。なお、どの事業者等が特定されているのかは、重要インフラ防護の観点から公表されていない。

なお、令和 4 年 5 月 11 日に可決成立した経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）は、その柱の一つとして、「基幹インフラ」役務の安定的な提供の確保に関する制度[2]を導入しているが、「重要インフラ」はサイバーセキュリティ基本法に基づくものであり[3]、それぞれ根拠とする法律が異なり、同一のものではないため注意が必要である。もっとも、重要インフラ統一基準においては、

[1] NCO「重要インフラ対策関連」（https://www.cyber.go.jp/policy/group/infra/policy.html）
[2] 詳細は、Q56 を参照。
[3] 詳細は、Q2 を参照。

基幹インフラの対象範囲については、原則、重要インフラの防護範囲に含めるとの方針が示されている。

（2）総説

重要インフラ防護の目的とは、重要インフラにおいて、任務保証の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することにある。

重要インフラ防護のための基本的な考え方は以下のとおりである。

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

（3）重要インフラ統一基準

令和 7 年に改正されたサイバーセキュリティ基本法に基づき、政府は、重要インフラ事業者等におけるサイバーセキュリティの確保に関して政府機関が実施する施策の基準として、「重要インフラのサイバーセキュリティ対策のための統一基準」（重要インフラ統一基準）を策定した（令和 8 年 7 月 31 日サイバーセキュリティ戦略本部決定）。重要インフラ統一基準は重要インフラ事業者等を直接規律するものではないが、政府機関は、重要インフラ統一基準に基づき各分野の施策を推進するための実施計画を策定し、施策の実施を通して重要インフラ事業者等におけるセキュリティ対策に反映することとされている。

また、各重要インフラ事業者等は、所管省庁や業界団体等が策定した「安全基準等」[4]を踏まえてサイバーセキュリティ対策に取り組むことになるが、重要インフラ統一基準

[4] 各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類。具体的には、①関係法令に基づき政府機関が定める「強制基準」、②関係法令に準じて政府機関が定める「推奨基準」及び「ガイドライン」、③関係法令や国民からの期待に応えるべき業界団体等

の「第 3 部　安全基準等において規律されるべき事項」では、安全基準等の策定に当たって参照する事項を記載している。具体的には、①「閉域網だから安全」との考え方の刷新、②サプライチェーン・リスクへの対応、③ランサムウェア攻撃等の被害を低減するためのレジリエンス向上、④技術・脅威の動向等を踏まえた対策、⑤官民双方向でのコミュニケーションの強化、が取り組むべき主な対策として記載されている。この第 3 部の詳細事項については、「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」に記載されている。

重要インフラ統一基準では、全ての分野・事業者を対象とした「重要インフラ・サイバーセキュリティ・セルフアセスメント」（CI-CSA）を実施することとされ、重要インフラ事業者等は、質問調査への自身の回答を通じて自己評価を行い、自組織のセキュリティ対策の実施状況を客観的に把握すること（成熟度モデル）を通じて、現段階におけるセキュリティ対策の実施状況と、求められるセキュリティ要件との差異を分析、改善すべき対策の優先順位を明確化し、継続的なセキュリティ水準の向上を図ることが期待されている。

（4）重要インフラ行動計画

重要インフラ防護に係る基本的な枠組みとして、政府と重要インフラ事業者等の共通の行動計画である「重要インフラのサイバーセキュリティに係る行動計画」（重要インフラ行動計画）がある。

重要インフラ行動計画は、関係主体の責務・取組や目指すべき将来性を提示し、自主的かつ積極的な取組を促進するものであり、主な取組として、「障害対応体制の強化」、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「リスクアセスメントの活用」及び「防護基盤の強化」の 5 つの施策が掲げられている。

なお、重要インフラ統一基準は、政府機関を対象として、PDCA サイクルの実施により重要インフラのサイバーセキュリティ強化の実効性を確保することを目的としているのに対し、重要インフラ行動計画は、政府機関のみならず、重要インフラ事業者等、セプター事務局、サイバーセキュリティ関係機関、サイバー空間関連事業者等といった多様な関係主体を対象として、官民連携の下、自主的な取組を促進することを目的としており、重要インフラ統一基準と重要インフラ行動計画は、対象となる主体や目的は異なるものの、相補的な関係として位置づけられている。この点、重要インフラ事業者等としては、重要インフラ行動計画に基づき 5 つの施策に取り組むことが期待されるが、その際、安全基準等の策定・改善に当たっては重要インフラ統一基準第 3 部を参照することになり、取組の継続的改善に当たっては CI-CSA を活用することが期待される。

が定める業界横断的な「業界標準」及び「ガイドライン」、④関係法令や国民・利用者等からの期待に応えるべき重要インフラ事業者等が自ら定める「内規」等の 4 分類が想定される。

（５）その他の重要インフラ分野に適用のある法令等

重要インフラ分野においては、重要インフラ事業者等に一般的に適用される法律のほか、それぞれ分野ごとに、適用される業法がある。例えば、情報通信であれば電気通信事業法、電力であれば電気事業法などが適用される。重要インフラ事業者等がサイバーセキュリティ対策を行うに当たっては、業法の中で、サイバーセキュリティに関する安全管理や保安規定の有無（データの保管場所を含む。）、事故の報告に関する規定の有無、所管省庁による報告徴求規定の有無について把握しておくことが肝要である。

ア　サイバーセキュリティに関する規定

重要インフラ事業者は、サイバーセキュリティ基本法第 6 条において、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めることが求められている。地方公共団体に関しては、同法第 5 条において、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有するとされている。

また、同法第 33 条第 2 項において、サイバーセキュリティ戦略本部は、重要インフラ事業者及びその組織する団体の代表者に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができるとされており、当該求めを受けた者は、その求めに応じるよう努めるものとされている。地方公共団体に関しては、同条第 1 項に基づき、正当な理由のある場合を除き、その求めに応じなければならないとされている。

なお、基幹インフラ事業者である重要インフラ事業者については、サイバー対処能力強化法の対象となるところ、同法に基づく届出・報告義務等については Q3 を参照されたい。

イ　情報の安全管理に関する規定

重要インフラのみならず、事業者に通則的に適用される法令として個情法を挙げることができ、個人データの安全管理措置が定められている（Q13 参照）。同法は、消費者向けの事業により消費者の個人情報を収集・利用していないとしても、取引先の担当者の個人情報や自社の従業員等の個人情報を取り扱っていれば適用されることに注意する必要がある。

その他、特に消費者向けの事業を行う分野の業法の場合には、法人を含む利用者に関する情報の保護を定めている例がある。例えば、情報通信分野では、電気通信事業法第 4 条第 1 項が通信の秘密（Q47 参照）の保護を定めており、金融分野では、銀行法（昭和 56 年法律第 59 号）第 12 条の 2 第 2 項が顧客情報の適正な取扱いを定め、同法施行規則第 13 条の 6 の 5 が個人顧客情報の安全管理措置を規定している。

ウ　情報漏えい等の事故報告に関する規定

情報漏えいが発生した場合又は重大な事故が発生した場合に、所管省庁等に報告する旨を定めている場合がある（Q57 参照）。

エ　重要インフラ分野ごとの規定

業法によっては、サイバーセキュリティ対策を行う旨を明確に定めている場合がある。

例えば、電力分野においては、電気設備に関する技術基準を定める省令（平成 9 年通商産業省令第 52 号）第 15 条の 2 に基づき、一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供する電気工作物の運転を管理する電子計算機におけるサイバーセキュリティの確保が義務として明記されている。また、電気通信分野においても、事業用電気通信設備規則（昭和 60 年郵政省令第 30 号）第 6 条が、事業用電気通信設備についてサイバーセキュリティ対策を含む防護措置を取らなければならない旨を定めている（Q47 参照）。

また、必要に応じて、所管省庁が事業者に対して資料の提出や報告を求めることができる旨が定められている場合がある。許認可や届出が必要となる事業に関する業法の多くがこの定めを置いていると考えられる。この報告徴求規定を根拠として、報告に関する規則を定めている例もあり、例えば、電気通信分野では電気通信事業報告規則（昭和 63 年郵政省令第 46 号）、電力分野では電気関係報告規則（昭和 40 年通商産業省令第 54 号）が定められている。

重要インフラ分野のうち、医療分野に関しては Q48 を、金融分野に関しては Q49 を、クレジット分野に関しては Q18 を、電気通信分野に関しては Q47 をそれぞれ参照されたい。

3．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

4．裁判例

特になし

Q46 電気通信事業分野における規律（電気通信事業法に基づく登録・届出）

どのような事業を行うと電気通信事業者に該当するか。

タグ：電気通信事業法、外国法人等が電気通信事業を営む場合における電気通信事業法の適用に関する考え方、電気通信事業参入マニュアル、電気通信事業参入マニュアル［追補版］、電気通信事業参入マニュアル（追補版）ガイドブック

１．概要

情報通信ネットワークを構築するための通信インフラは、サイバー空間における活動を支える基盤である。今日において、いかなる事業も多かれ少なかれ通信インフラを利用している。電気通信事業法（「事業法」という。以下本項において同じ。）は、電気通信事業の公共性に鑑み、その運営を適正かつ合理的なものとするとともに、その公正な競争を促進することにより、電気通信役務の円滑な提供を確保するとともにその利用者等の利益を保護し、もって電気通信の健全な発達及び国民の利便の確保を図るものであり、電気通信事業を営もうとする者は、原則として総務大臣の登録又は届出が必要となる。とりわけ外国法人等（外国の法人及び団体並びに外国に住所を有する個人をいう。以下本項において同じ。）については、総務省「外国法人等が電気通信事業等を営む場合における電気通信事業法の適用に関する考え方」[1]（令和 3 年 2 月 12 日）に基づき、外国から日本国内にある者（訪日外国人を含む。以下２（２）において同じ。）に対して電気通信役務の提供の意図を有していることが明らかなときも、同法の適用対象となる。また、外国法人等が登録又は届出を行う際には、国内代表者又は国内代理人を定める必要がある。以下では、外国法人等に関する取扱い、登録・届出の要否、適用除外の整理等について、順に解説する。

２．解説

（１）電気通信事業を営む場合

電気通信事業（事業法第 2 条第 4 号）を営もうとする者は、同法第 9 条の規定による登録を受け、又は同法第 16 条第 1 項の規定による届出を行う必要がある旨を定める。同法第 9 条の登録を受けた者及び同法第 16 条第 1 項の規定による届出をした者を電気通信事業者という（同法第 2 条第 5 号）。

[1] https://www.soumu.go.jp/main_content/000733072.pdf

（２）外国法人等が電気通信事業を営む場合

総務省は「外国法人等が電気通信事業等を営む場合における電気通信事業法の適用に関する考え方」（令和 3 年 2 月 12 日）を公表しており、外国法人等が営む電気通信事業に対する事業法の適用に関する解釈を示している。

具体的には、同法は、外国法人等が、①日本国内において電気通信役務を提供する電気通信事業を営む場合のほか、②外国から日本国内にある者に対して電気通信役務を提供する電気通信事業を営む場合に適用されること、さらに、②については、外国から日本国内にある者に対する電気通信役務の提供の意図を有していることが明らかであることを指し、例えば、a サービスを日本語で提供している場合、b 有料サービスにおいて決済通貨に日本円がある場合、c 日本国内におけるサービスの利用について広告や販売促進等の行為を行っている場合には、当該意図を有していることが明らかと判断され得るという解釈が示されている。なお、外国法人等が電気通信事業の登録又は届出を行う際には、国内における代表者又は国内における代理人を定める必要がある（同法第 10 条第 1 項第 2 号）。

（３）登録又は届出を行うことを要する場合

次の①から④の全てに該当する場合は、事前に登録（事業法第 9 条）又は届出（同法第 16 条第 1 項）を行うことを要する。なお、登録、届出のいずれの手続が必要かを含め、詳しい内容は総務省ホームページに掲載されている「電気通信事業参入マニュアル［追補版］」及び「電気通信事業参入マニュアル（追補版）ガイドブック」を参照されたい[2]。

① 提供する役務が「電気通信役務」に該当すること

電気通信役務とは、a 電気通信設備を用いて b 他人の通信を媒介し、その他 c 電気通信設備を他人の通信の用に供することをいう（同法第 2 条第 3 号）。

a 「電気通信設備」とは、電気通信（有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けること。）（同法第 2 条第 1 号）を行うための機械、器具、線路その他の電気的設備をいう（同法第 2 条第 2 号）。

b 「他人の通信を媒介する」とは、他人の依頼を受けて、情報をその内容を変更することなく伝送・交換し、隔地者間の通信を取次ぎ、又は仲介してそれを完成させることをいう。

c 「電気通信設備を他人の通信の用に供する」とは、広く電気通信設備を他人の通信のために運用することをいう。

② 事業が「電気通信事業」に該当すること

[2] 「電気通信事業参入・変更手続の案内」（https://www.soumu.go.jp/menu_seisaku/ictseisaku/denkitsushin_suishin/tetsuzuki/）

電気通信事業とは、電気通信役務を d 他人の需要に応ずるために提供する e 事業（放送法（昭和 25 年法律第 132 号）第 118 条第 1 項に規定する放送局設備供給役務に係る事業を除く。）をいう（同法第 2 条第 4 号）。

d 「他人の需要に応ずるため」とは、電気通信役務の提供について自己の需要のために提供していることではなく、他人の需要に応ずることを目的とすることをいう。

e 「事業」とは、主体的・積極的意思、目的をもって同種の行為を反復継続的に遂行することをいう。

③ 「事業法の適用除外」に該当しないこと

次の場合、「適用除外となる電気通信事業」（同法第 164 条第 1 項）に該当する。

・専ら一の者に電気通信役務（当該一の者が電気通信事業者であるときは、当該一の者の電気通信事業の用に供する電気通信役務を除く。）を提供する電気通信事業（同項第 1 号）
・その一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は建物内である電気通信設備その他総務省令で定める基準（設置する線路のこう長の総延長が 5km）に満たない規模の電気通信設備により電気通信役務を提供する電気通信事業（同項第 2 号）
・他人の通信を媒介しない電気通信役務（ドメイン名電気通信役務、検索情報電気通信役務、媒介相当電気通信役務（後二者にあっては、当該電気通信役務を提供する者として総務大臣が総務省令で定めるところにより指定する者により提供されるものに限る。）を除く。）を電気通信回線設備を設置することなく提供する電気通信事業（同項第 3 号）

このうち、同項第 3 号により適用除外となる電気通信事業には、以下のものが含まれる（総務大臣が総務省令で定めるところにより指定する者による検索情報電気通信役務又は媒介相当電気通信役務を提供する電気通信事業は除く。）[3]。

a 電子メールマガジンの配信（企業等から提供された製品 PR やイベント開催案内等に関する情報を元に電子メールマガジンを作成し、あらかじめ登録した購読者等に対して送信するもの）

b 各種情報のオンライン提供（電気通信設備（サーバ等）を用いて、天気予報やニュース等の情報を、インターネットを経由して利用者に提供するもの）

[3] 総務省「電気通信事業参入マニュアル［追補版］」（平成 17 年 8 月 18 日策定（令和 5 年 1 月 30 日改定）4.「主な事例と考え方」

c　Web サイトのオンライン検索（広範な Web サイトのデータベースを構築し、検索語を含む Web サイトの URL 等を、インターネットを経由して利用者に提供するもの）

d　ソフトウェアのオンライン提供（クラウド上にアプリケーションソフトウェアを構築し又はアプリケーションソフトウェアをインストールしたサーバ等を設置し、インターネット等を経由して当該ソフトウェアを企業や個人等に利用させるもの）

e　オンラインストレージ（利用者がデータを保存することを目的として、サーバ等を設置して、インターネット等を経由して利用者のデータ等を受信して保存するもの）

f　オープン・チャット（インターネット経由で不特定多数の利用者がリアルタイムで文字ベースの会話を行うことができる「場」を提供するもの）

g　EC モール/ネットオークション/フリマアプリの運営（インターネット経由で複数の店舗でネットショッピングを行うことができる又は複数の出品者の商品等を購入できる「場」を提供するもの）

ただし、特定の利用者間におけるダイレクトメッセージ機能の提供は、「他人の通信を媒介」する役務（同法第 2 条第 3 号）に該当するため、同法第 164 条第 1 項第 3 号の規定に該当せず、適用除外となる電気通信事業には当たらない。したがって、当該電気通信事業を営む場合には、登録又は届出が必要となる。

なお、適用除外となる電気通信事業である場合でも、同法第 3 条（検閲の禁止）及び同法第 4 条（通信の秘密の保護）は当該電気通信事業を営む者の取扱中に係る通信については、適用されるので（同法第 164 条第 3 項）、注意が必要である。また、適用除外となる電気通信事業を行う者についても、電気通信事業における個人情報等の保護に関するガイドライン（令和 4 年個人情報保護委員会・総務省告示第 4 号（最終改正令和 7 年個人情報保護委員会・総務省告示第 2 号））[4]が適用される[5]ことにも注意が必要である。

④　「電気通信事業を営むこと」に該当すること

「電気通信事業を営む」とは、利用者に対して、電気通信役務を反復継続して提供して、その対価として料金を徴収することにより電気通信事業自体で利益を上げようとすることを意味する。

[4] 詳しくは「電気通信事業における個人情報等の保護に関するガイドライン（令和 4 年個人情報保護委員会・総務省告示第 4 号（最終改正令和 7 年個人情報保護委員会・総務省告示第 2 号））の解説」（令和 4 年 3 月（令和 8 年 6 月更新）　個人情報保護委員会・総務省）を参照されたい。

[5] 事業法に規定する「電気通信事業者」と、電気通信事業における個人情報等の保護に関するガイドラインの適用対象として定義される「電気通信事業者」とでは定義・範囲が異なっている。

（４）登録又は届出を要する電気通信事業者の例示

「電気通信事業参入マニュアル［追補版］」には、電気通信事業について、登録又は届出を要する事例と登録又は届出を要しない事例が例示されているので参照されたい。もっとも、事業の内容によっては異なる判断となる場合があるので、個別かつ具体的な検討が必要である。また、いわゆる「クラウド」、「プラットフォーム」、「スーパーアプリ」、「ポータルサイト」等、様々なサービスが複合的に提供されている場合は、それぞれのサービスごとに、登録又は届出の要否を判断することとなる。

３．参考資料（法令・ガイドラインなど）

・電気通信事業法（昭和 59 年法律第 86 号）
・総務省「電気通信事業参入マニュアル」
https://www.soumu.go.jp/main_content/000739290.pdf
・総務省「電気通信事業参入マニュアル［追補版］」
https://www.soumu.go.jp/main_content/000477428.pdf
・総務省「電気通信事業参入マニュアル（追補版）ガイドブック」
https://www.soumu.go.jp/main_content/000799137.pdf
・総務省「外国法人等が電気通信事業を営む場合における電気通信事業法の適用に関する考え方」
https://www.soumu.go.jp/main_content/000733072.pdf
・電気通信事業における個人情報等の保護に関するガイドライン
https://www.soumu.go.jp/main_content/001032808.pdf
・電気通信事業における個人情報等の保護に関するガイドラインの解説
https://www.soumu.go.jp/main_content/001064462.pdf

４．裁判例

特になし

Q47 電気通信事業分野における規律（電気通信事業者に関する規律の概要）

電気通信事業者に対する電気通信事業法上の義務としてどのようなものがあるか。

タグ：電気通信事業法、通信の秘密、同意取得の在り方に関する参照文書、通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針、電気通信事業における個人情報等の保護に関するガイドライン、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会、重要インフラ、電気通信事業法の消費者保護ルールに関するガイドライン

１．概要

電気通信事業者は、電気通信事業法（以下、本項において「事業法」という。）や電気通信事業法施行規則（昭和 60 年郵政省令第 25 号。以下、本項において「施行規則」という。）等の関係法令の規定を遵守する必要があり、「検閲の禁止」（事業法第 3 条）や「通信の秘密の保護」（事業法第 4 条）といった規律をはじめ、参入に関する規律、登録・届出事項の変更や事業の休廃止等に関する規律、消費者保護に関する規律、電気通信設備に関する規律、報告等に関する規律等が適用される。

２．解説

（１）電気通信事業者に係る規律

電気通信事業者に対する全般的な規律として、検閲の禁止（事業法第 3 条）、通信の秘密の保護（事業法第 4 条）、利用の公平（事業法第 6 条）、重要通信の確保（事業法第 8 条）、業務の停止等の報告（事業法第 28 条）、電気通信設備の維持（事業法第 41 条）がある。

また、利用者の利益に及ぼす影響が大きい電気通信役務を提供する事業者として総務大臣に指定された場合[1]、特定利用者情報を適正に取り扱うべき電気通信事業者として、その情報の取扱規程の策定・届出[2]、情報取扱方針の策定・公表[3]等の義務が課されることとなる。

（２）通信の秘密の保護

まず、事業法が定める通信の秘密の保護の大要を説明する。

[1] 事業法第 27 条の 5。
[2] 事業法第 27 条の 6。
[3] 事業法第 27 条の 8。

日本国憲法第 21 条第 2 項後段は、「通信の秘密は、これを侵してはならない」と定めるところ、同規定は、プライバシー権の観念が発展した現在において、その一局面を取り上げて通信の秘密を保護する規定であるとともに、電気通信事業者に特別の位置づけを与えることを通じて、国民の自由なコミュニケーション、すなわち通信の自由を保障する規定であると解される[4]。同規定を受けて、事業法第 4 条第 1 項では、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」との定めが置かれ、同法第 179 条では違反した場合の罰則も定められている。

同法第 4 条第 1 項の趣旨は、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、日本国憲法第 21 条第 2 項後段の規定を受けて思想表現の自由の保障を実行たらしめること及び個人の私生活の自由を保護し、個人生活の安寧を保護すること（プライバシー保護）にとどまらず、国家権力が自ら通信を侵害しないのみならず、自然による侵害から通信の秘密を保護すること、国民が安全・安心に通信を利用できるよう通信制度を保障することにより、国民の通信の自由を確保することにあると考えられる。

「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号等の当事者の識別符号等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれる。

「通信の秘密」を侵害する行為は、一般に、通信当事者以外の第三者（電気通信事業者とそれ以外の全ての者を含む。）による行為を念頭に、以下の①から③の 3 類型に大別されている。知得や窃用には、機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る。

① 知　得：積極的に通信の秘密を知ろうとする意思のもとで知ること[5]
② 窃　用：発信者又は受信者の意思に反して利用すること
③ 漏えい：他人が知り得る状態に置くこと

通信当事者の「有効な同意」がある場合、通信当事者の意思に反しない利用であり、通信の秘密の侵害に当たらないが、一般的に「有効な同意」は「個別具体的かつ明確な同意」であることが必要と解されていることに注意が必要である[6]。

---

[4] 渡辺康行・宍戸常寿・松本和彦・工藤達朗「憲法Ⅰ　基本権 第 2 版」（日本評論社、平成 28 年）270 頁。

[5] 電気通信事業者が電気通信事業を行うために通信の秘密に当たる情報を知得することも、形式上通信の秘密侵害に該当する（構成要件該当性がある）が、正当業務行為として違法性が阻却される場合には許容される。

[6] 「有効な同意」の有無は個別事案ごとに判断する必要があるが、規律を明確化することで事業者における予見可能性を高めることを目的として、総務省は、令和 3 年 2 月 25 日、同意取得の在り方に関する論点について整理・検討した「同意取得の在り方に関する参照文書」を公表した。また、「同意取得の在り方に関する参照文書」の公表にあわせて、総務省は、事業法第 29 条第 1 項第 1 号に基づく「通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針」を公表している。これは通信の秘密の確保に関する考え方を明らかにし、

また、通信当事者の同意を得ることなく通信の秘密を侵した場合であっても、①正当防衛（刑法第 36 条）、②緊急避難（刑法第 37 条）（例：人命保護の観点から緊急に対応する必要のある電子掲示板等での自殺予告事案について、インターネット・サービス・プロバイダが警察機関に発信者情報を開示する場合）、③正当行為（刑法第 35 条）に当たる場合[7]（例：電気通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為）等違法性阻却事由がある場合には、例外的に通信の秘密を侵しても違法とはならない[8]。

（３）通信の秘密の保護とサイバー攻撃への適正な対処の在り方

総務省は、サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるように、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を開催している。同研究会における議論を取りまとめた結果については、これまでに、第一次取りまとめが平成 26 年 4 月に、第二次取りまとめが平成 27 年 9 月に、第三次取りまとめが平成 30 年 9 月に、第四次取りまとめ[9]が令和 3 年 11 月にそれぞれ公表されているので、サイバー攻撃との詳しい関係については、同取りまとめを参考にされたい。

このうち、第四次とりまとめにおいては、①インターネット・サービス・プロバイダがサイバー攻撃に予防的に対処するため、平時から自らのネットワーク内の通信トラフィックに係るデータを収集・蓄積・分析し、C&C サーバ[10]である可能性が高い機器の検知を行うことは、必要最低限の範囲でフロー情報[11]を収集・蓄積し、当該情報を C&C サー

各事業者の取組が十分機能していないとして業務改善命令を発動する基準や事例を指針として類型的に示すことにより透明性・予見可能性を高めることを目的として策定されたものである が、本指針においても、「有効な同意」の判断に関わる項目が示されている。同意取得方法について検討する際には、「同意取得の在り方に関する参照文書」及び「通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針」（令和 3 年 2 月）をあわせて参照することが有効である。

7 正当業務行為として違法性が阻却されるためには、電気通信役務の円滑な提供の確保の観点から、業務の目的が正当であり、当該目的を達成するための行為の必要性及び手段の相当性が認められる行為である必要がある（個人情報保護委員会・総務省「電気通信事業における個人情報等の保護に関するガイドライン（令和 4 年個人情報保護委員会・総務省告示第 4 号（最終改正令和 6 年個人情報保護委員会・総務省告示第 4 号））の解説」令和 4 年 3 月（令和 8 年 6 月更新）参照）。

8「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第一次取りまとめ」（平成 26 年 4 月）（https://www.soumu.go.jp/main_content/000283608.pdf）。

9「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次取りまとめ」（令和 3 年 11 月）（https://www.soumu.go.jp/main_content/000779208.pdf）。

10 Command and Control（指揮統制）サーバの略称。C2（シーツー）サーバということもある。マルウェアに感染した PC をネットワーク経由で操作し、情報の収集や攻撃の命令を出すサーバのこと。

11 「フロー情報」とは、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IP アドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報をいう（第四次取りまとめ第 1 章(2)）。

バ検知以外で使用しない場合に限り、正当業務行為として違法性が阻却されること、②各インターネット・サービス・プロバイダがサイバー攻撃に対処できるようにする観点から、一のインターネット・サービス・プロバイダが自らの電気通信ネットワーク内のフロー情報の収集・蓄積・分析によって検知した C&C サーバに関する IP アドレス及びポート番号のリストの情報のみを、サイバーセキュリティ対策を行うために必要最小限の情報として、適切な事業者団体等に提供することは、通信の秘密の保護規定に直ちに抵触するとまではいえないと考えられることが示されている。

（４）電気通信設備に関する規律

サイバーセキュリティ基本法におけるサイバーセキュリティの定義の中に情報通信ネットワークの安全性・信頼性を含んでいることからも明らかなとおり、情報通信ネットワークを構築するための通信インフラは、サイバー空間における活動を支える基盤であり、重要インフラ行動計画においても、電気通信を含む情報通信分野は、重要インフラ分野[12]の１つとして、セキュリティ強化の取組が求められている。

電気通信サービスを提供する上での基盤となる電気通信設備に対する規律として、事業法第 41 条において、電気通信回線設備を設置する電気通信事業者、基礎的電気通信役務を提供する電気通信事業者及び利用者の利益に及ぼす影響が大きい電気通信役務を提供する電気通信事業者等に対し、その電気通信事業の用に供する電気通信設備（以下、本項において「事業用電気通信設備」という。）について、電気通信役務の確実かつ安定的な提供を確保するため、技術基準への適合維持義務を課している。このうち、サイバーセキュリティ対策については、電気通信事業者は、事業用電気通信設備について、サイバーセキュリティ対策を含む防護措置を取らなければならないと事業用電気通信設備規則第 6 条に定められており、当該措置等の具体的な内容については、事業法第 42 条において、電気通信設備の使用を開始しようとするときには、当該電気通信設備が技術基準に適合することを自ら確認し、その結果を電気通信設備の使用の開始前に、届け出なければならないことが規定されている。

同法第 44 条において、事業用電気通信設備の技術基準適合維持義務が適用される電気通信事業者は、電気通信役務の確実かつ安定的な提供を確保するため、当該設備について、電気通信事故の事前防止や発生時に必要な取組のうち、技術基準等で画一的に定めることが必ずしも適当でなく、電気通信事業者ごとの特性に応じた自主的な取組により確保すべき管理の方針・体制・方法等の事項について管理規程を定め、事業の開始前に届け出なければならないことが規定されている。このうち、サイバーセキュリティ対策については、事業用電気通信設備の情報セキュリティの確保のための方針と情報セキュリティ対策の内容について、管理規程に記載をしなければならないとされている[13]。

---

[12] 重要インフラに係る取組について Q2、Q45 参照。
[13] 施行規則第 29 条及び平成 27 年総務省告示第 67 号。

さらに、同法第 44 条の 3 において、電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方針・体制・方法に関する事項に関する業務を統括管理させるため、事業運営上の重要な決定に参画する管理的地位にあり、かつ、電気通信設備の管理に関する一定の実務の経験等の要件を備える者のうちから、電気通信設備統括管理者を選任すること、及び、同法第 45 条において、事業用電気通信設備の工事・維持・運用に関する事項を監督させるため、電気通信主任技術者を選任することが規定されている。

（５）通信の秘密の漏えい等の重大事故に関する報告及び四半期報告に関する規律

電気通信事業者は、電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えい、特定利用者情報の漏えいその他総務省令で定める重大な事故（電気通信役務の提供を停止又は品質を低下させた事故で、継続時間及び影響利用者数が一定の基準を満たすもの等）が生じたときは、速やかにその発生日時及び場所、概要、理由又は原因、措置模様等について報告するとともに、30 日以内にその詳細について報告しなければならない（事業法第 28 条、施行規則第 57 条、第 58 条）。

また、電気通信事業者は、電気通信役務の提供を停止又は品質を低下させた事故で、影響利用者数 3 万人以上又は継続時間 2 時間以上のものや、電気通信設備に関する情報であって、電気通信役務の提供に支障を及ぼすおそれのある情報が漏えいした事故等が発生した場合には、毎報告年度経過後 2 か月以内に、その発生状況について報告しなければならない（電気通信事業報告規則第 7 条の 3）。

事故に関する報告等の適用関係については、「電気通信事故に係る電気通信事業法関係法令の適用に関するガイドライン（第 5 版）」（令和 2 年 1 月 27 日）が参考になる。

（６）外部送信規律

近年、SNS、動画共有、ニュース配信等のサービスによる情報の流通が、スマートフォン等を経由して行われているところ、利用者が認識しないまま、端末から第三者に情報が送信される、いわゆる「外部送信」が行われる場合がある。この不透明な状況を解消し、安心してサービスを利用できるよう電気通信事業者[14]は、タグや情報収集モジュール等により外部送信を指示する際、送信される利用者に関する情報の内容等を事前に通知又は

[14] 例えば、メッセージ媒介サービス、SNS、検索サービス、ニュースサイト、まとめサイト等各種情報のオンライン提供サービスの提供事業者が対象として想定されている。他方で、企業等のホームページ、自社商品等をオンライン販売しているホームページの運営事業者、個人ブログの運営者は対象として想定されていない。

公表（利用者が容易に知り得る状態に置く）する義務を負う（事業法第 27 条の 12、外部送信規律）[15, 16]。

（７）その他の規律（参入などの各場面に関する規律）

上記のほか、参入などの各場面に関する規律として、次のものがある。特に、消費者保護に関する規律の詳しい内容は、総務省総合通信基盤局が公表している「電気通信事業法の消費者保護ルールに関するガイドライン」（平成 28 年（2016 年）3 月（令和 4 年 2 月最終改正）を参照されたい。

【そのほか、電気通信事業者における参入などの各場面に関する規律】

参入に関する規律	電気通信事業の登録（事業法第 9 条）、電気通信事業の届出（事業法第 16 条第 1 項）、事業法第 9 条違反への罰則（事業法第 177 条）、事業法第 16 条第 1 項違反への罰則（事業法第 185 条）
登録・届出事項の変更や事業の休廃止等に関する規律	変更登録等（事業法第 13 条）、届出事項の変更（事業法第 16 条第 2 項、3 項）、事業の承継（事業法第 17 条）、事業の休廃止・法人の解散（事業法第 18 条）、電気通信役務等の変更報告（施行規則第 10 条）
消費者保護に関する規律	提供条件の説明（事業法第 26 条）、書面の交付（事業法第 26 条の 2）、書面による解除（初期契約解除）（事業法第 26 条の 3）、業務の休廃止の周知（事業法第 26 条の 4）、苦情等の処理（事業法第 27 条）、電気通信事業者等の禁止行為（事業法第 27 条の 2 及び第 27 条の 3）、媒介等業務受託者に対する指導（事業法第 27 条の 4）
報告等に関する規律	業務の改善命令（事業法第 29 条）、報告及び検査（事業法第 166 条）、法令等違反行為を行った者の氏名等の公表（事業法第 167 条の 2）

３．参考資料（法令・ガイドラインなど）

・電気通信事業法（昭和 59 年法律第 86 号）
・同意取得の在り方に関する参照文書
https://www.soumu.go.jp/main_content/000734726.pdf
・通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針
https://www.soumu.go.jp/main_content/000734725.pdf

[15] 総務省「外部送信規律について ウェブサイトやアプリケーションを運営している皆様、御確認ください！」（令和 5 年 2 月）（https://www.soumu.go.jp/main_content/000862755.pdf）。
[16]「電気通信事業における個人情報等の保護に関するガイドライン（令和 6 年 3 月 12 日版）」も参照（https://www.soumu.go.jp/main_content/001032808.pdf）。

・個人情報保護委員会・総務省「電気通信事業における個人情報等の保護に関するガイドライン（令和 4 年個人情報保護委員会・総務省告示第 4 号（最終改正令和 7 年個人情報保護委員会・総務省告示第 2 号））の解説」令和 4 年 3 月（令和 7 年 12 月更新）
https://www.soumu.go.jp/main_content/001032808.pdf
・「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第一次取りまとめ」（平成 26 年 4 月）
https://www.soumu.go.jp/main_content/000283608.pdf
・「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第二次取りまとめ」（平成 27 年 9 月）
https://www.soumu.go.jp/main_content/000376396.pdf
・「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第三次取りまとめ」（平成 30 年 9 月）
https://www.soumu.go.jp/main_content/000575399.pdf
・「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次取りまとめ」（令和 3 年 11 月）
https://www.soumu.go.jp/main_content/000779208.pdf
・総務省総合通信基盤局「電気通信事業法の消費者保護ルールに関するガイドライン」平成 28 年 3 月（令和 4 年 2 月最終改正）
https://www.soumu.go.jp/main_content/000794752.pdf
・総務省「外部送信規律についてウェブサイトやアプリケーションを運営している皆様、御確認ください！」（令和 5 年 2 月）
https://www.soumu.go.jp/main_content/000862755.pdf

4. 裁判例

・東京地判平成 14 年 4 月 30 日（平成 11 年（刑わ）第 3255 号）
　電気通信事業者の社員が、特定の団体の動向を把握する目的で自社システムから加入電話の契約者名・設置場所・請求先・支払状況等を出力・持出した行為について、事業法第 4 条の「通信の秘密」は通話内容のみならず日時・回数等の外形的事項も含むものの、本件で問題となっている行為で取得された情報は個々の通信と無関係に蓄積された加入者・料金情報であり、「通信の秘密」に該当せず、同法違反について無罪と判断した事例。

Q48 医療分野におけるサイバーセキュリティ

医療機関においては、サイバーセキュリティを確保するために、どのような措置を講ずる必要があるか。
また、次世代医療基盤法上の匿名加工医療情報や仮名加工医療情報の取扱いに当たり、サイバーセキュリティの観点から留意すべき点は何か。

タグ：医療法、医療情報システムの安全管理に関するガイドライン、医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律（次世代医療基盤法）、医療情報、匿名加工医療情報、仮名加工医療情報

１．概要

昨今、医療機関に対するサイバー攻撃が増加しており、サイバー攻撃により診療が停止する事案が発生したこと、また、サイバー攻撃により医療に関する患者の個人情報が窃取されるなどの甚大な被害がもたらされる可能性があること等を踏まえ、医療機関におけるサイバーセキュリティ対策に関する取組の実効性を高める必要が生じている。

医療機関等は、厚生労働省による監督のもと、インシデント発生時の報告、医療分野におけるサイバーセキュリティの取組を行っている[1]。

また、令和 5 年 4 月に医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項が新設され、病院、診療所又は助産所の管理者が遵守すべき事項として、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じることが追加された。

他方で、医療情報は保護の重要性とともに、利活用することで医療の発展に寄与するなど、公益に資することから、医療情報利活用をめぐる政策もさまざま展開されている。本項では、セキュリティの観点から、かかる政策の 1 つである、医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律（平成 29 年法律第 28 号。以下、本項において「次世代医療基盤法」という。）についても併せて説明する。

２．解説

（１）総論

厚生労働省は、医療機関等におけるサイバーセキュリティ対策の充実は喫緊の課題であるという認識の下で、平成 30 年に地方自治体向けに、「医療機関等におけるサイバー

[1] その他、日本医師会によるサイバーセキュリティ関連の取組として、「日本医師会サイバーセキュリティ支援制度」（https://www.med.or.jp/doctor/sys/cybersecurity/001566.html）や「医療機関におけるサイバーセキュリティ対策チェックリストの実践ガイド」（https://www.med.or.jp/nichiionline/article/011545.html）などが挙げられる。

セキュリティ対策の強化について（通知）」を発出し、関係ガイドラインの周知徹底、インシデント発生時の報告、医療分野におけるサイバーセキュリティの取組との連携等について通知を行っている。

ア　情報の安全管理

医療分野においては、医師法（昭和 23 年法律第 201 号）、医療法（昭和 23 年法律第 205 号）などが関係するが、これらの法律においては、情報の安全管理を直接義務づける規定はない[2]。しかし、医療機関が取り扱う医療情報は、個情法に規定される要配慮個人情報に該当するものがほとんどであり、機微性の高い情報であることから、安全管理を行う重要性は高い。

イ　医療分野のサイバーセキュリティに関係するガイドライン（サイバーセキュリティに関する規定）

医療分野においては、厚生労働省が「医療情報システムの安全管理に関するガイドライン 第 6.0 版」[3]を策定しており、医療機関等における医療情報システムの安全管理など、サイバーセキュリティの観点から医療機関等が遵守すべき事項等を定めている。

また、総務省及び経済産業省は、医療情報を取り扱う情報システム・サービスを提供する事業者向けのガイドラインとして、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版」[4]を公開している。これは、医療機関等との契約に基づいて情報システム・サービスを提供する事業者向けのガイドラインであるところ、様々な要求事項を定めている。リスクベースアプローチを採用しており、リスクに応じて適切な安全管理措置を選択して実施することを求めている（法令等で義務付けられているものについては、一律に対応の必要があるとしている）。

この 2 つのガイドラインを総称して「3 省 2 ガイドライン」ということがある。なお、データの保管場所に関して Q84 を参照されたい。

---

[2] ただし、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（以下、本項において「薬機法」という。）第 8 条第 3 項において、「薬局の管理者が行う薬局の管理に関する業務及び薬局の管理者が遵守すべき事項については、厚生労働省令で定める。」とされているところ、これを受けた医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項が令和 5 年 3 月に改正された。同項第 1 号では、「保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従事者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じ、その他その薬局の業務につき、必要な注意をすること。」とされている（同年 4 月 1 日施行）。医療法施行規則第 14 条第 2 項については後述する。

[3] https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

[4] https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20250328_rev1.pdf

ウ　事故報告に関する規定

医師法及び医療法においては、サイバーセキュリティインシデント発生時の当局報告に関する法律上の規定は特に定められていないが、上記厚生労働省「医療情報システムの安全管理に関するガイドライン 第 6.0 版（企画管理編）」においては、「サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、……所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。」とされている[5]。

エ　報告徴求規定

医療法第 25 条第 1 項は、「都道府県知事、保健所を設置する市の市長又は特別区の区長は、必要があると認めるときは、病院、診療所若しくは助産所の開設者若しくは管理者に対し、必要な報告を命じ……ることができる」としている。

オ　参考：医療機器に関するサイバーセキュリティ

医療機関等が業務において取り扱う医療機器についても、その安全な使用を確保するため、サイバーセキュリティの確保が必要である。薬機法に基づき定められる基準[6]（以下、本項において「基本要件基準」という。）においては、サイバーセキュリティリスクを含むリスクマネジメントが求められている。これに基づき、厚生労働省は、平成 27 年[7]、平成 30 年[8]にそれぞれ医療機器におけるサイバーセキュリティの確保に関するガイダンスを公開している。

また、令和 2 年には、国際医療機器規制当局フォーラム（International Medical Device Regulators Forum：IMDRF）において、医療機器サイバーセキュリティガイダンス N60「Principles and Practices for Medical Device Cybersecurity（医療機器サイバーセキュリティの原則及び実践）」がとりまとめられ、厚生労働省がその周知を図る通知を発出している[9]。これを受けて、厚生労働省は、令和 3 年 12 月に、医療機器のサイバーセキ

---

5 厚生労働省「医療情報システムの安全管理に関するガイドライン 第 6.0 版（企画管理編）1.2」。

6 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準（厚生労働省告示第 122 号）。

7 厚生労働省「医療機器におけるサイバーセキュリティの確保について」（平成 27 年）（https://www.pmda.go.jp/files/000204891.pdf）

8 厚生労働省「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成 30 年）（https://www.pmda.go.jp/files/000225426.pdf）

9 厚生労働省「国際医療機器規制当局フォーラム（IMDRF）による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」（令和 2 年）（https://www.pmda.go.jp/files/000235089.pdf）

ュリティの確保及び徹底に係る手引書（以下、本項において「製販業者向け手引書」という。）を公開した[10]。さらに、厚生労働省は、基本要件基準の改正[11]、製販業者向け手引書の改訂[12]及び医療機関における医療機器のサイバーセキュリティ導入に関する手引書の発出[13]を行っている。

（２）医療法施行規則改正

医療法施行規則第 14 条第 2 項

> 病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）[14]を確保するために必要な措置を講じなければならない。

医療法施行規則第 14 条第 2 項は、医療法 17 条に規定する医療機関の管理者が遵守すべき具体的事項として、サイバーセキュリティの確保について必要な措置を講じることを定めたものである。

病院、診療所及び助産所においては、規則第 14 条第 2 項に規定する「必要な措置」として、厚生労働省が作成した「医療情報システムの安全管理に関するガイドライン」（以下、本項において「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行う必要がある。

安全管理ガイドラインの最新版である第 6.0 版では、同ガイドラインの目的や対象、全体構成について解説する概説編に加え、対象読者ごとに、経営管理編、企画管理編、システム運用編が作成されており、医療機関等のそれぞれの立場を踏まえ、必要な箇所を参照して対策を行う必要がある。

---

10 厚生労働省「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」（令和 3 年）
（https://www.mhlw.go.jp/web/t_doc?dataId=00tc6374&dataType=1&pageNo=1）

11 薬事法第 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件（令和 5 年厚生労働省告示第 67 号）

12 医療機器のサイバーセキュリティ導入に関する手引書の改訂について
（https://www.mhlw.go.jp/content/11120000/001167217.pdf）

13 医療機関における医療機器のサイバーセキュリティ確保のための手引書について
（https://www.mhlw.go.jp/content/11120000/001094637.pdf）

14 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること（サイバーセキュリティ基本法 2 条）。

また、安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省において別途チェックリスト[15]が作成されており、医療機関において求められるサイバーセキュリティの基準を把握するに当たり参考になる。過去には、インシデント発生時の初動対応について十分に協議されておらず、証拠保全が不十分となり、被害範囲の特定ができなかったり、ランサムウェアによる攻撃の際に、バックアップが適切に確保できておらず、復旧が難航したりという事案が発生しており、診療の継続を含め、医療機関の機能に重大な影響が生じたこともある。そのような背景から、チェックリスト上、医療機関ではサイバー攻撃を想定した事業継続計画（BCP）を策定することが求められており、「サイバー攻撃は完全に排除できない」ことを大前提としつつ、診療業務の中断が発生しないよう（又は、短期間で再開できるよう）に、平常時にインシデント発生時の医療情報システムの復旧の手順等を定めておくなど、サイバー攻撃を受けても事業を継続できる体制を整備しておく必要がある。

（３）次世代医療基盤法

ア　概要

医療分野における IT 化の進展により、医療情報を扱う機会は飛躍的に増加したものの、従来の我が国では医療情報に関する統一的な規格が存在せず、個人の医療情報は医療機関や研究機関ごとに分散的に管理されていたため、症例研究や創薬などに必要となる大規模な医療情報の収集・解析が容易でなかった。こうした課題に対応するため、健康・医療分野における先端的な研究開発や新産業の創出を推進することを目的として、個人の権利利益の保護に配慮しつつ、医療情報を大規模に収集・利活用できる仕組みを整備すべく、医療情報の匿名加工や仮名加工に関する特例等を定める法律として次世代医療基盤法が制定された。同法は、匿名加工医療情報や仮名加工医療情報の制度を設けることにより、医療情報を保有・管理する医療機関等が安心して情報を提供できるようにし、また製薬企業や研究機関が研究開発に必要な医療情報へ円滑にアクセスできる環境を整備するという点で、重要な意義を有している。

イ　定義（医療情報・匿名加工医療情報・仮名加工医療情報）

次世代医療基盤法は、「医療情報」、「匿名加工医療情報」及び「仮名加工医療情報」という 3 つのカテゴリーを設け、それぞれの取り扱いについて規定している。

① 医療情報：特定の個人の病歴その他の当該個人の心身の状態に関する情報であって、当該心身の状態を理由とする当該個人又はその子孫に対する不当な差別、偏

[15] 医療機関におけるサイバーセキュリティ対策チェックリスト（令和 6 年 5 月）（https://www.mhlw.go.jp/content/10808000/001253950.pdf）

見その他の不利益が生じないようにその取扱いに特に配慮を要するものが含まれる個人に関する情報（次世代医療基盤法第 2 条第 1 項）

② 匿名加工医療情報：医療情報の区分に応じて一定の措置を講じ、特定の個人を識別することができないように医療情報を加工して得られる個人に関する情報（次世代医療基盤法第 2 条第 3 項）

③ 仮名加工医療情報：医療情報の区分に応じて当該各号に定める措置を講じて他の情報と照合しない限り特定の個人を識別することができないように医療情報を加工して得られる個人に関する情報（次世代医療基盤法第 2 条第 4 項）

個人情報保護法上の「個人情報」が「生存する個人」の情報に限定されているのとは異なり、次世代医療基盤法上の「医療情報」は「生存する個人」の情報に限定されておらず、死者に関する情報も含まれる。

また、同じく個人情報保護法において規定されている「匿名加工情報」及び「仮名加工情報」とは異なり、匿名加工医療情報及び仮名加工医療情報は、医療情報を加工して得られる個人に関する情報に限定されている。

ウ　次世代医療基盤法の特色

次世代医療基盤法には、医療情報を大規模に収集・利活用するための仕組みとして、代表的には以下のような個人情報保護法との違いがある。

まず、医療情報は個人情報であり個人情報保護法が適用されるが、次世代医療基盤法はその特別法として、個人情報保護法では認められていないオプトアウト方式[16]での医療情報の提供が認められている（次世代医療基盤法第 52 条第 1 項、第 57 条第 1 項）。これにより、次世代医療基盤法に基づく大臣認定を取得した認定作成事業者において、より多くの医療情報を収集し、加工の上、提供できるスキームとなっている。

また、仮名加工医療情報は、個人情報保護法上の仮名加工情報と同様に第三者への提供が制限されるものの、仮名加工情報とは異なって、医薬品の製造販売の承認等を受けるために提供する必要がある場合には、厚生労働大臣、独立行政法人医薬品医療機器総合機構（PMDA）、薬機法に規定する登録認証機関、欧州医薬品庁（EMA）、英国医薬品医療製品規制庁（MHRA）及び米国食品医薬品局（FDA）に仮名加工医療情報を提供することができる（次世代医療基盤法第 43 条第 1 項第 2 号、同規則第 40 条第 1～4 号）。

なお、認定匿名（仮名）加工医療情報作成事業者、連結可能匿名加工医療情報利用者、認定仮名加工医療情報利用事業者は、それぞれ安全管理措置を講じることが求められているところ、安全管理措置の具体的な内容は次世代医療基盤法ガイドラインを参照されたい。

---

16 医療分野の研究開発に資するための匿名加工医療情報又は仮名加工医療情報の作成の用に供するものとして、認定作成事業者に提供すること等についてあらかじめ本人に通知した場合、当該本人又は遺族から停止の求めがない限り、個別の同意がなくとも医療情報の提供を可能とする方式のこと（次世代医療基盤法第 52 条第 1 項、第 57 条第 1 項）。

３．参考資料（法令・ガイドラインなど）

・医療法施行規則の一部を改正する省令について
https://www.mhlw.go.jp/content/10808000/001075881.pdf
・医療情報システムの安全管理に関するガイドライン 第 6.0 版
https://www.mhlw.go.jp/content/10808000/001102570.pdf
・令和 7 年度版 医療機関におけるサイバーセキュリティ対策チェックリスト
https://www.mhlw.go.jp/content/10808000/001253950.pdf
・令和 7 年度版 医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関等・事業者向け～
https://www.mhlw.go.jp/content/10808000/001490741.pdf
・サイバー攻撃を想定した事業継続計画（BCP）策定の確認表
https://www.mhlw.go.jp/content/10808000/001261299.pdf
・サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き
https://www.mhlw.go.jp/content/10808000/001261301.pdf
・医療機関におけるサイバーセキュリティ対策チェックリストの実践ガイド
https://www.mie.med.or.jp/hp/doctor/joho/joho4.pdf
・よくわかる次世代医療基盤法
https://www8.cao.go.jp/iryou/gaiyou/pdf/zentaizou.pdf
・医療分野の研究開発に資するための 匿名加工医療情報及び仮名加工医療情報に関する法律についてのガイドライン（次世代医療基盤法ガイドライン）
https://www8.cao.go.jp/iryou/hourei/pdf/guideline.pdf

４．裁判例

特になし

Q49 金融分野におけるサイバーセキュリティ

重要インフラ分野の中でも、類型的に機微性の高い個人情報を含む情報を取り扱う分野であり、ガイドライン等についても多く公開されている金融分野においては、サイバーセキュリティに関してどのような義務が課せられているか。法令上、どのような規定に着目すべきか。
また、金融分野におけるサイバーセキュリティに関するガイドラインは、金融機関等に対して、どのようなサイバーセキュリティ対応を求めているのか。

タグ：金融分野におけるサイバーセキュリティに関するガイドライン、金融分野におけるサイバーセキュリティ強化に向けた取組方針、金融分野のサイバーセキュリティレポート、銀行法、保険業法、金融商品取引業者等向けの総合的な監督指針、主要行等向け監督指針、フィッシングに耐性のある多要素認証

１. 概要

金融分野に属する事業者がサイバーセキュリティ対策を行うに当たっても、重要インフラ分野に属する事業者と同様に、各々に適用される業法にどのような規定があるかに着目して検討すべきである。金融分野においては、ガイドライン等も多く公開されており、それぞれのガイドライン等におけるサイバーセキュリティに関する情報の安全管理や保安規定の有無、事故の報告に関する規定の有無、金融庁による報告徴求規定の有無について把握しておくことが肝要である。

特に、金融分野におけるサイバーセキュリティに関するガイドライン（以下、本項において「本ガイドライン」という。）は、金融機関等に対して、事業環境、経営戦略及びリスクの許容度等を踏まえてサイバーセキュリティ対策を講ずることを求めている。その中では、①サイバーセキュリティ管理態勢の構築、②サイバーセキュリティリスクの特定、③サイバー攻撃の防御、④サイバー攻撃の検知、⑤サイバーインシデント対応及び復旧、⑥サードパーティリスク管理といった点が中心的な対応事項とされている。

２. 解説

（１）業法上の対応事項

金融庁は、金融分野のサイバーセキュリティの確保が金融システム全体の安定のための喫緊の課題であるとの認識の下、平成 27 年に公開し、令和 4 年 2 月にアップデートした、「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）」に基づき、官民一体となって金融分野のサイバーセキュリティ強化に向けた取組を実施してい

る。そして、その中で把握された実態や課題等について取りまとめた「金融分野のサイバーセキュリティレポート」を令和 2 年 6 月 30 日に公表している[1]。

ア　情報の安全管理

金融分野では、銀行法第 12 条の 2 第 2 項が顧客情報の適正な取扱いを定め、同法施行規則第 13 条の 6 の 5 が個人顧客情報の安全管理措置を規定している。その他、保険分野においても、保険業法（平成 7 年法律第 105 号）第 100 条の 2 に顧客情報の適正な取扱い、同法施行規則第 53 条の 8 に個人顧客情報の安全管理措置が定められている。一口に金融といっても、銀行、生命保険、損害保険、証券と様々な業態があり、それぞれ適用される法令も異なるが、概ね銀行法等と同趣旨の規定が置かれている（以下についても同様である。）。

イ　主要行等向け監督指針（サイバーセキュリティ対策に関する規定）

主要行等の検査・監督を担う職員向けの手引書として、検査・監督に関する基本的考え方、事務処理上の留意点、監督上の評価項目等を体系的に整理した「主要行等向け監督指針」[2] [3]においては、主要行等監督上の評価項目として、システムリスクが挙げられており（III－3-7）、その中で、仮に主要行等において、システム障害や「サイバーセキュリティ事案」[4]が発生した場合は、利用者の社会経済生活、企業等の経済活動、ひいては、我が国経済全体にもきわめて大きな影響を及ぼすおそれがあるほか、その影響は単に一銀行の問題にとどまらず、金融システム全体に及びかねないことから、システムが安全かつ安定的に稼動することは決済システム及び銀行に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化はきわめて重要である旨指摘されている。また、当該評価項目における着眼点として、「サイバーセキュリティ管理」が挙げられており、例えば次のような項目が挙げられている。

① サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

② サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、サイバーセキュリティ管理態勢（サイバー攻撃に対する監視体制、サイバー攻撃を受

[1] 金融庁は、金融分野におけるサイバーセキュリティ対策を、金融庁ウェブサイト「金融分野におけるサイバーセキュリティ対策について」において取りまとめている。
[2] https://www.fsa.go.jp/common/law/guide/city/index.html
[3] 監督指針は、その他、保険会社向け、金融商品取引業者向け等のものがある。
[4] 「サイバーセキュリティ事案」とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行や DDoS 攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。

けた際の報告及び広報体制、組織内 CSIRT 等の緊急時対応及び早期警戒のための体制、情報共有機関等を通じた情報収集・共有体制等）の整備を図っているか。

③ サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

④ サイバー攻撃を受けた場合に被害の拡大を防止するために、攻撃元の IP アドレスの特定と遮断、DDoS[5]攻撃に対して自動的にアクセスを分散させる機能、システムの全部又は一部の一時的停止等の措置を講じているか。

⑤ システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

⑥ サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

ウ　事故報告に関する規定

銀行法においては、個情法に基づく個人データの漏えい等に関する報告等を補完する規定が置かれている。例えば、銀行法施行規則第 13 条の 6 の 5 の 2 では、個人顧客に関する個人データの漏えい等が発生した場合には、金融庁長官等に速やかに報告することその他の適切な措置を講じなければならない旨が規定されている。

また、主要行等向け監督指針において、顧客等に関する情報管理体制に関する主な着眼点の一つとして、「顧客等に関する情報の漏えい等が発生した場合に、適切に責任部署へ報告され、二次被害等の発生防止の観点から、対象となった顧客等への説明、当局への報告及び必要に応じた公表が迅速かつ適切に行われる体制が整備されているか。」が挙げられている[6]。

さらに、サイバーセキュリティインシデントが不祥事件（銀行法第 53 条、同法施行規則第 35 条）に該当する場合は、銀行法に基づく届出が必要となる。

エ　報告徴求規定

銀行法第 24 条に定めがある。

（2）本ガイドライン上の対応事項

ア　サイバーセキュリティ管理態勢の構築

本ガイドラインは、サイバーセキュリティ管理態勢を構築するために、経営陣に対して、サイバーセキュリティリスクを組織全体のリスク管理の一部と位置付け、サイバーセキュリティ管理の基本方針を策定するとともに、これに基づいてサイバーセキュリテ

[5] Distributed Denial of Service attack の略。
[6] 主要行等向け監督指針 III-3-3-3-2(1)④。

ィ管理体勢の整備・見直しや予算・人材等を適切に確保し、資源配分することを求めている。さらに、サイバーセキュリティに係る戦略や取組計画を策定し、年次及び重要な変更が生じた時点で、見直しを行うことも必要とされている。

また、一般的な 3 線防衛態勢（業務部門、リスク管理部門及び内部監査部門）の下、サイバーセキュリティに関する各部門の役割分担の明確化や外部専門家を利用した検証の仕組みを構築することを含め、サイバーセキュリティに関する十分な知識を利用できる体制の整備も推奨されている。

さらに、整備したサイバーセキュリティ管理態勢やサイバーセキュリティに係る規程及び業務プロセスについて、少なくとも年１回見直すべきとしている。

本ガイドラインは、経営陣だけでなく、リスク管理部門に対しては、業務部門等から独立した立場から監視・牽制を行い、必要に応じて経営陣に対する報告を行うことを、内部監査部門に対しては、サイバーセキュリティに係る内部監査計画を策定し、これに基づいて内部監査を実施し、重要な指摘事項について遅滞なく経営陣に報告するとともに、その改善状況を的確に把握することを要求している。

イ　サイバーセキュリティリスクの特定

本ガイドラインでは、サイバーセキュリティリスクの特定のためには、まず保有する情報資産（①情報システム及び外部システムサービス、②その構成要素であるハードウェア・ソフトウェア等及び保管される情報（データ）、並びに③ネットワークを指す。）を把握・分類し、その重要度や脆弱性等に応じて適切に管理する必要があるとされている。具体的には、情報資産を台帳等により管理し、リスク評価を定期的に実施した上で、分類に応じたアクセス制御や保護措置を講じる必要がある。また、新たな情報資産が追加された場合や業務変更があった場合には、管理対象や方法の見直しを行い、最新の状態に維持することが重要である。

また、リスクを管理するという観点からは、脅威情報及び脆弱性情報を収集・分析し、自組織の事業・情報資産に与える影響を評価した上で、定められた手順に従い、サイバーセキュリティリスクを少なくとも１年に１回評価することが必要であるとされている。そして、リスク評価の結果に基づき優先順位付けを行い、リスク対応計画（リスク回避、リスク軽減、リスク受容、リスク移転）を策定し、継続的な改善活動を実施することが求められている。

さらに、ハードウェア・ソフトウェア等の脆弱性管理に係る手続等を策定した上で、入手した脆弱性情報は、当該手続等に基づき対応の要否を検討し、深刻度に応じて迅速に対応を講じることが求められる。なお、管理対象は重要なサードパーティ（自組織として業務運営上重要と認識しているサードパーティをいう。）が保有するシステムにも及ぶことに注意が必要である。

脆弱性診断やペネトレーションテストを定期的に実施し、システムの脆弱性やセキュリティの問題点を把握・評価することも重要である。また、サイバー攻撃やインシデント発生時に適切に対応できるよう、関係者を含めた演習・訓練を定期的に実施し、サイバーインシデント対応計画及びコンティンジェンシープランの有効性を定期的に検証の上、演習・訓練で得られた課題や教訓等を踏まえ見直すことも求められている。

ウ　サイバー攻撃の防御

本ガイドラインは、サイバー攻撃を防ぐためには、多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じることが必要であるとした上で、認証・アクセス権付与の方針策定と見直し、システム権限についての、正当な業務上の要請があり、承認され、適切に教育・研修を受け、管理されている個人に対してのみへの付与、ID・認証情報の適切管理、アクセス権限の適切性の検証、認証要件の決定、不正行為防止策の実施、システム間認証の機密性、完全性及び真正性等の確保、重要区域への物理的アクセス管理・保護・記録といった対応を求めている。

また、経営陣を含む全ての役職員に対して、役割と責任に応じたサイバーセキュリティの意識向上に係る教育・研修を定期的に実施することも必要である。

さらに、データ保護の観点からは、情報の重要度と、使用される技術環境における固有のリスクに応じて、データの管理方針を策定し、管理方針に従ってデータを保護すること、ライフサイクル全体を通じて、データを適切に管理することも必要となる。

加えて、システム全体に対して多層的かつ網羅的なセキュリティ対策を講じることが求められる。具体的には、ログ管理、セキュリティ・バイ・デザインの実践、物理的セキュリティ・ネットワークセキュリティの確保、クラウドサービス利用時の対策等を含め、平時からの備えと継続的な改善により、脅威への対応力を高める必要がある。

セキュリティ・バイ・デザインとの関係では、令和 7 年に発生した証券口座の不正アクセス事案を受けて、「金融商品取引業者等向けの総合的な監督指針」が改正され、ログイン、出金、出金先銀行口座の変更等の重要な操作時におけるフィッシングに耐性のある多要素認証[7]や、認証に連続して失敗した場合、ログインを停止するアカウント・ロックの自動発動機能といった仕組みの実装が必須のものとされている点にも留意が必要である。

[7] インターネット取引に関して、「ログイン、出金、出金先銀行口座の変更など、重要な操作時におけるフィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定）」を求めている（III-2-8-2-2）。同監督指針は、金融商品取引業者等向けのものであるが、金融商品取引業者等以外であってもかかる対応を講じることの重要性については同様に当てはまると考えられる。主要行等向け監督指針等でも、令和 8 年 2 月 27 日から適用された最新版において同様の記載が盛り込まれた（III-3-8-2(2)）。

エ　サイバー攻撃の検知

サイバー攻撃を早期に検知するため、ネットワークやシステムの監視体制を整備し、異常を自動的に把握できる仕組みを構築することが求められる。特に、攻撃の初期段階に検知するための仕組みを導入したり、常時監視を行うこと等が推奨されている。

オ　サイバーインシデント対応及び復旧

本ガイドラインでは、インシデント発生時に備え、まずインシデント対応計画及びコンティンジェンシープランを、サイバー攻撃の種別ごとに策定することが求められている。

その際、(i)初動対応や(ii)攻撃の手口や原因・経路、システムへの影響、現在発生している業務影響及び今後発生し得る業務影響等についての分析、(iii)顧客対応・組織内外の連携・広報といった対応の実施、(iv)サイバー攻撃による被害拡大を防止するための対応（封じ込め）、(v)サイバー攻撃により被害が発生した原因の除去、(vi)復旧計画といった事項を盛り込むべきである。

カ　サードパーティリスク管理

さらに、金融機関等のサードパーティへの依存が増大するとともに、金融機関等のサプライチェーンは拡大・複雑化し、サプライチェーンに由来するサイバーインシデントにより、金融機関等が多大な影響を受ける事例が発生していることから、サプライチェーンのサイバーセキュリティリスクを適切に管理する必要があるとされている。また、金融機関等にサービス等を提供するサードパーティは、金融機関等によるサイバーセキュリティリスクの適切な管理のために、必要な支援を実施すべきとされている。

すなわち、サイバーセキュリティ戦略・計画策定に際し、サプライチェーン全体とサードパーティを含む業務プロセスを対象に管理態勢を整備することが求められる。具体的には、リスク管理方針・体制・規程を策定し、サードパーティの特定・リスク評価・台帳管理を行う。取引開始時にはデューデリジェンスを実施し、契約や SLA に役割分担・監査権限・再委託手続・インシデント対応・データ取扱い等を明記する必要がある。さらに、重要なサードパーティについては管理態勢や計画の評価を行い、契約履行やリスクを継続的にモニタリングし、取引終了時にはデータ廃棄やアクセス遮断を実施することが求められる。

3．参照資料（法令・ガイドラインなど）

・金融分野におけるサイバーセキュリティに関するガイドライン
・金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針
・金融機関における個人情報保護に関する Q&A

・金融商品取引業者等向けの総合的な監督指針

４．裁判例

特になし

Q50 電子契約と電子署名法

近年、契約業務の電子化が進んでいるが、電子契約は可能か。また電子契約を行うにあたり関連する法令はどのようなものであり、また、企業はどのような点に留意すべきか。

タグ：電子署名法、電子署名法施行規則、民事訴訟法、電子帳簿保存法、電子帳簿保存法施行規則、電子契約、文書の成立の真正

１．概要

電子的な契約が可能だが、民事訴訟において証拠として利用できるようにするためには、電子署名が重要となる。電子署名法第 3 条の要件を満たす電子署名が付された電子契約は、その電磁的記録の真正な成立の推定が働くことから、文書作成者の印章による押印がある紙の契約書と同様の効力を有する。他方、電子署名法第 3 条の要件を満たさない電子署名が付された電子契約は、その電磁的記録の真正な成立の推定は働かない。しかしながら、自ら、当該電子署名の本人性と非改ざん性が担保されていることを立証できれば、結果として、紙の契約書と同様の効力を有する。

また、電子契約の保存との関係において、電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（平成 10 年法律第 25 号。以下、本項において「電子帳簿保存法」という。）の規定に留意する必要がある。電子契約において、時刻認証業務認定事業者のタイムスタンプが付されない場合には、「電子取引データの訂正及び削除の防止に関する事務処理規程」を定め、当該規程に沿った運用を行うことが必要になる。また、関係書類の備付け、見読性の確保及び検索機能の確保の要件を満たす必要がある。

２．解説

（１）電子契約

契約は、一般に、口頭でも契約可能であり、書面の契約書がなければ契約が成立しないわけではない（民法第 522 条第 2 項）。売買契約を例にすると、店頭で商品を購入する際は、契約書を交わさない場合がほとんどである。

もっとも、何か問題が発生した場合等には、契約が成立しているかどうか、どのような条件で契約が成立しているのか等に争いが生じることもあり、契約書面で確定していることが重要となってくる。そこで実務上、重要な契約では書面の契約書を交わすことが多い。ただし、契約は書面ではなく ICT を利用して電子的に契約することも可能である。

（２）文書証拠の形式的証拠力

民事裁判において文書を証拠とするためには、その文書の成立が真正であること、すなわち、その文書が作成者の意思に基づいて作成されたことが必要である（民事訴訟法第228条第1項）。これを形式的証拠力という。

契約書等の私文書に関しては、私文書に顕出された印影と作成名義人の印章が一致することが立証されれば、当該印影は、当該作成名義人の意思に基づき押印されたものと事実上推定される（最判昭和39年5月12日民集18巻4号597頁）。そして、私文書の作成者が、その意思に基づいて当該私文書に署名又は押印をした場合には、当該私文書全体がその意思に基づいて作成されたものと推定される（同条第4項）。この二段階の推定を、二段の推定という[1]。

もっとも、署名及び押印がない等の理由により二段の推定が働かない場合でも、文書の成立の真正を他の方法により直接立証することが可能である（大判昭和6年1月31日）。

（３）電子データの形式的証拠力

民事裁判において電子データの意味内容を証拠資料とする場合にも、その成立の真正（＝本人の意思に基づき作成されたこと）を証明する必要がある。これは契約を電子的に行った場合に契約内容を証拠としたい場合に限らず、あらゆる電子データについてあてはまる。一定の要件を満たす電子署名が行われた電子データについては、真正に成立したものと推定される（電子署名法第3条）。つまり、同条の要件を満たす電子署名がなされていれば、文書に署名又は押印があるのと同様の効果が得られる[2]。

もっとも、同条の要件を満たさない場合であっても、電子データの成立の真正を他の方法により直接立証することも可能と考えられる。

（４）電子契約の有効性と電子署名法

ア　電子署名法第3条の要件を満たす電子署名と電子契約

（ア）電子署名法第3条の要件

デジタル庁・法務省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法第3条関係）」[3]（以下、本項において「3条QA」という。）によれば、電子署名法第3条の規定が適用されるためには、次の要件が満たされる必要がある。

①　電子文書に同条に規定する電子署名が付されていること。

---

[1] これらに関して、内閣府・法務省・経済産業省「押印についてのQ&A」（令和2年6月19日）も参照されたい（https://www8.cao.go.jp/kisei-kaikaku/kisei/imprint/document/20061 9document01.pdf）。

[2] なお、タブレット等に手書きで名前を書く、いわゆる電子サインは、同条の要件を満たさない。

[3] 令和6年1月9日付で一部改定がなされた。

② 上記電子署名が本人（電子文書の作成名義人）の意思に基づき行われたものであること。

そして、上記①を満たすためには、(a)当該電子署名が同法第 2 条に規定する電子署名に該当するものであることに加え、(b)当該電子署名「を行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」に該当するものでなければならない。

（イ）電子署名法第 2 条に規定する電子署名（上記①(a)）

電子署名法第 2 条第 1 項は、「電子署名」を、電磁的記録に記録することができる情報について行われる措置であって、以下の要件のいずれにも該当するものをいうと定めている。

(i) 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること（本人性）

(ii) 当該情報について改変が行われていないかどうかを確認することができるものであること（非改ざん性）

近時、電子契約の締結においては、「サービス提供事業者が利用者の指示を受けてサービス提供事業者自身の署名鍵による電子署名を行う電子契約サービス」（総務省・法務省・経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A」（以下、本項において「2 条 1 項 QA」という。））（以下、このような形態のサービスを本項において「利用者指示型サービス」という。）[4]の利用が拡大している。利用者指示型サービスは、利用者が「当該措置を行った者」（上記(i)）と評価できるのかが問題となるところ、2 条 1 項 QA によれば、「当該措置を行った者」に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではないとしている。利用者指示型サービスであっても、技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されているものであり、かつサービス提供事業者が電子文書に行った措置について付随情報を含めて全体を 1 つの措置と捉え直すことによって、当該措置が利用者の意思に基づいていることが明らかになる場合には、「当該措置を行った者」はサービス提供事業者ではなく、利用者と考えられる。

（ウ）電子署名「を行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」（上記①(b)）

3 条 QA によれば、電子署名「を行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」の要件が設けられているのは、電子署名法第 3 条の推定効を生じさせる前提として、暗号化等の措置を行う

[4] 利用者指示型サービスは、3 条 QA では「サービス提供事業者が利用者の指示を受けてサービス提供事業者自身の署名鍵による暗号化等を行う電子契約サービス」と表現されている。

ための符号について、他人が容易に同一のものを作成することができないと認められること（以下、本項において「固有性の要件」という。）が必要だからであり、利用者指示型サービスが上記要件を満たすためには、利用者とサービス提供事業者の間で行われるプロセス[5]及び当該プロセスにおける利用者の行為を受けてサービス提供事業者内部で行われるプロセス[6]のいずれにおいても十分な水準の固有性が満たされている必要がある。

（エ）電子署名が本人（電子文書の作成名義人）の意思に基づき行われたものであること（上記②）

3 条 QA によれば、上記②の要件は、電子署名法第 3 条が「本人による」電子署名であることを要件としていることから導かれるものである。電子署名についても、文書に関する二段の推定の一段目の推定[7]と同様、電子署名の一致[8]があれば、電子署名が電子文書の作成名義人の意思に基づき行われたものであることが推定されるのかどうかが問題となるところ、この点について裁判例はなく、確立された見解はない。

また、同条の推定効の主張が認められるためには、電子契約サービスの利用者と電子文書の作成名義人が同一であることを立証する必要がある。そのため、サービス提供事業者が電子契約サービスの利用者と電子文書の作成名義人の同一性を確認する（いわゆる利用者の身元確認を行う）ことは、電子署名法第 3 条の要件となっていないものの、電子契約サービスの利用者と電子文書の作成名義人が同一であることの有効な立証手段となり得る。

イ　電子署名法第 3 条の要件を満たさない電子署名と電子契約

電子署名が電子署名法第 3 条の要件を満たすものではない場合でも、作成された電磁的記録の真正な成立の推定が否定されるにとどまり、これにより、当該電子署名が行われた電子契約の証拠としての有効性が否定されるものではない。同条の要件を満たさな

---

[5] 3 条 QA によれば、例えば、利用者が 2 要素による認証を受けなければ措置を行うことができない仕組み（利用者が、あらかじめ登録されたメールアドレス及びログインパスワードの入力に加え、スマートフォンへの SMS 送信や手元にあるトークンの利用等当該メールアドレスの利用以外の手段により取得したワンタイム・パスワードの入力を行うことにより認証するもの等）が備わっている場合には、十分な水準の固有性が満たされていると認められ得る。

[6] 3 条 QA によれば、サービス提供事業者が当該事業者自身の署名鍵により暗号化等を行う措置について、暗号の強度や利用者毎の個別性を担保する仕組み（例えばシステム処理が当該利用者に紐付いて適切に行われること）等に照らし、電子文書が利用者の作成に係るものであることを示すための措置として十分な水準の固有性が満たされていると評価できるものである場合には、固有性の要件を満たすと認められ得る。

[7] 私文書に顕出された印影と作成名義人の印章が一致することが立証されれば、当該印影は、当該作成名義人の意思に基づき押印されたものと事実上推定される（上記（2）参照）。

[8] いわゆる RSA 方式の電子署名の場合、ファイルから生成されたハッシュ値と、添付された電子署名に対し署名者の復号鍵（公開鍵）で復号して得られたハッシュ値とが一致していれば「電子署名の一致」があると評価されると考えられる。

い電子署名が行われている電子契約であっても、その真正な成立を直接立証することができれば、その契約内容を訴訟資料とすることが可能である[9]。

（５）電子保存と電子帳簿保存法

電子契約を電子保存する場合には、税法上の帳簿書類の保存義務との関係で、電子帳簿保存法の要件を満たす必要がある。

電子契約は、「電子取引」（同法第 2 条第 1 項第 5 号）[10]とされ、所得税を納税する個人事業者や法人税を納税する企業が電子取引を行った場合、財務省令で定めるところにより、その電磁的記録を保存しておく必要がある（同法第 7 条）。

そして、「財務省令」とは同法施行規則を指すが、同施行規則第 4 条第 1 項が、電磁的記録を保存するに当たって充足すべき要件をまとめている。その内容は以下のとおりである。

① 以下のいずれかの措置を行う

(ア) タイムスタンプ[11]が付された後、当該取引情報の授受を行う（同項第 1 号）。

(イ) 取引情報の授受後、速やかに（又はその業務の処理に係る通常の期間を経過した後、速やかに）[12]タイムスタンプを付す（同項第 2 号）。

(ウ) 記録事項について訂正・削除を行った場合に、これらの事実及び内容を確認できるシステム又は記録事項の訂正・削除を行うことができないシステムで取引情報の授受及び保存を行う（同項第 3 号）。

(エ) 記録事項について正当な理由がない訂正・削除の防止に関する事務処理規程を定め、その規程に沿った運用を行う（同項第 4 号）。

---

[9] 3 条 QA によれば、身元確認が取引開始時に行われていなかった場合であっても、契約当事者における当該電子文書の成立過程を裏付ける証拠等が提出できれば、それらも電子文書の成立の申請の有効な立証手段となり得る。真正な成立を直接立証する手段を確保するための方策として、①取引先とのメールのメールアドレス・本文及び日時等、送受信記録の保存（継続的な取引関係がある場合）、②契約締結前段階での本人確認情報（氏名・住所等及びその根拠資料としての運転免許証など）の記録・保存（新規に取引関係に入る場合）、③電子署名や電子認証サービスの活用（利用時のログイン ID・日時や認証結果などを記録・保存できるサービスを含む）等が考えられる（内閣府・法務省・経済産業省「押印に関する Q&A」Q6 参照）。

[10] 「取引情報（取引に関して受領し、又は交付する注文書、契約書、送り状、領収書、見積書その他これらに準ずる書類に通常記載される事項をいう。以下同じ。）の授受を電磁的方式により行う取引をいう。」と定義される。

[11] 「タイムスタンプ」とは、一般に、データファイルの作成日時、更新日時、最終アクセス日などのデータの総称として用いられることがあるが、ここにいうタイムスタンプは、時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）にいう時刻認証業務において電子データに付与される時刻情報等の総体であって、当該電子データがある時刻に存在していたことを示すためのものであり、かつ当該電子データについて改変が行われていないかどうか確認することができるものを指す。本規程に基づき、総務大臣による時刻認証業務認定制度が令和 3 年 4 月より開始されている。

[12] 最長では、電子取引の取引情報に係る電磁的記録を授受してから 2 か月と概ね 7 営業日以内にタイムスタンプを付与すれば足りる（国税庁「電子帳簿保存法一問一答 【電子取引関係】」（令和 7 年 6 月）問 62）。

② 当該電磁的記録の備付け及び保存に併せて、施行規則所定の関係書類の備え付けを行う。

③ 当該電磁的記録の備付け及び保存の場所に、PC、プログラム、ディスプレイ、プリンタ及びこれらのマニュアルを備え付け、当該電磁的記録をディスプレイ画面及び書面に、整然とした形式及び明瞭な状態で、速やかに出力することができるようにする。

④ 当該電磁的記録について検索機能（同規則第 2 条第 6 項第 5 号）[13]を確保する[14]。

上記①(エ)に関して、正当な理由がない訂正・削除の防止に関する事務処理規程の例が、国税庁「電子帳簿保存法一問一答 【電子取引関係】」（令和 7 年 6 月）問 33 に掲載されているため参照されたい。

（６）外国における電子契約制度

外国企業との取引において電子契約を用いる場合等、企業が外国法に準拠して電子契約を締結することも少なくない。多くの国では既に法令上電子契約の使用が認められているが、実際に外国法に準拠して電子契約を締結する際には、当該外国法の内容を慎重に検証する必要がある。

例えば、EU における電子契約に関する主な法規制として、2014 年 7 月に成立し、2016 年 7 月に発効した、eIDAS（electronic Identification, Authentication and trust Services）規則があり、eIDAS 規則は、現在、EU における電子署名及び電子シール[15]等に関する最も重要な法的枠組みとして機能している。

eIDAS 規則では、一定の要件を満たすデバイスを使用して生成され、かつ一定の要件を満たす証明書による裏付けがなされた「適格電子署名」[16]は「手書署名と同じ法的効力を有する」[17]。ただし、手書署名の法的効力は加盟国ごとに異なり得るため、「適格電子署名」が EU で統一的な効力を持つとは限らない点に注意が必要である。また、eIDAS 規

---

[13] 原則として、(ⅰ)取引年月日、取引金額、取引先により検索できること、(ⅱ)日付又は金額の範囲指定により検索できること、(ⅲ)2 つ以上の任意の記録項目を組み合わせた条件により検索できることが必要であるが、税務調査時においてダウンロードの求めに応じることができるようにしている場合には、(ⅱ)及び(ⅲ)は不要となる。

[14] 保存義務者が小規模な事業者であり、税務調査時においてダウンロードの求めに応じることができるようにしている場合には、検索機能は不要となる。

[15] 日本においては、企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明する技術である e シールについて、「デジタル社会の実現に向けた重点計画」（令和 5 年 6 月 9 日閣議決定。以下、本項において「重点計画」という。）において「e シールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む」こととされ、総務省から「e シールに係る指針（第 2 版）」（令和 6 年 4 月）が公表され、e シールに係る認証業務の認定に関する規程を定める件（令和 7 年総務省告示第 113 号）が令和 7 年 3 月から施行されている。

[16] eIDAS 規則第 3 条第 12 号。

[17] eIDAS 規則第 25 条第 2 項。もっとも、「適格電子署名」以外の電子署名の法的有効性も否定されない。

則は、電子署名の証明力について規定していないため、証明力も加盟国法ごとに異なり得る点にも注意が必要である。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

本文中に記載のとおり

Q51 データ取引に関する契約におけるサイバーセキュリティ関連法令上のポイント

AI 技術を利用したソフトウェアやサービスの開発・利用など、データの流通・利用を目的とする取引（データ取引）において、サイバーセキュリティ関連法令上のどのようなポイントに留意して、データの流通・利用に関する契約（データ契約）を取り決めるべきか。

タグ：民法、不正競争防止法、データ取引、AI・データの利用に関する契約ガイドライン 1.1 版

１．概要

データの法的性質及び近時のデータに関する法制度整備の状況を踏まえ、従前の有体物に関する契約や秘密保持義務に関する契約とは異なる観点からの検討を行い、取引の目的に適った実効性のあるデータ契約を取り決めることが望ましい。

２．解説

（１）背景

デジタル技術の急激な発達や IoT デバイスの急速な普及により[1]、多量・多種・リアルタイムなデータ（ビッグデータ）の活用が指摘されるようになって久しい。この間、平成 26 年に「企業が壁を越えてデータを共有・活用し、新たな付加価値を生む取組として“データ駆動型（ドリブン）イノベーション”」という考え方が示され[2]、平成 28 年には、官民データ活用推進基本法（平成 28 年法律第 103 号）が公布・施行された。また、第三次 AI ブームといわれてしばらく経ち、回帰や分類、クラスタリングなどのタスクを統計的に行う機械学習やディープラーニングも社会実装が進み日常生活に浸透している。

こうして、データを対象とした取引やデータの利用・活用を目的とした取引が認知され増えるにあたり、データ取引については、往時からの有体物（民法第 85 条）を対象とした取引とは異なるため、また、従来からの秘密情報に関する秘密保持義務の合意（契約）

[1] 総務省「令和 7 年版情報通信白書」（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00231）によれば、世界の IoT デバイス数は、令和元年に 230.7 億であったが、令和 6 年には 420.4 億に伸びており、令和 9 年には 583.9 億にまで達するという予測があるとのことである（高成長が予想されているのは、デジタルヘルスケアの市場が拡大する「医療」、スマート家電や IoT 化された電子機器が増加する「コンシューマー」、スマート工場やスマートシティが拡大する「産業用途」（工場、インフラ、物流）、コネクテッドカーの普及により IoT 化の進展が見込まれる「自動車・宇宙航空」。）。

[2] 経済産業省ニュースリリース平成 26 年 6 月 9 日「データ駆動型(ドリブン)イノベーション創出戦略協議会を設立します」（http://warp.da.ndl.go.jp/info:ndljp/pid/10217941/www.meti.go.jp/press/2014/06/20140609004/20140609004.html）

や成果物に関する合意（契約）では対応しきれないため、どのような法的リスクがあり、どのような事項を合意すべきなのかということが議論されるようになった[3]。

例えば、平成 30 年 6 月には、経済産業省が、ユースケース（事例）に基づいて検討を展開した「AI・データの利用に関する契約ガイドライン」（以下、本項において「契約ガイドライン」という。）を策定し、令和元年 12 月にはアップデート版として契約ガイドライン 1.1 版がリリースされた[4]。また、令和 3 年 3 月には、経済産業省が、データ提供側とデータ受信側が実務面で直面する課題について、契約雛形を基に論点を整理・解説し、考え方を示すことでデータ提供・活用の促進を目的とした「AI・データサイエンス人材育成に向けたデータ提供に関する実務ガイドブック」（以下、本項において「AI 人材育成ガイドブック」という。）を策定した[5]。続いて、令和 7 年 2 月には、当事者間の適切な利益及びリスクの配分を目指し、ひいては AI の利活用を促すことを目的とした「AI の利用・開発に関する契約チェックリスト」を策定した[6]。

（２）データ取引とは

データ取引とは、法令上の用語ではない。一般的に、データの創出、取得、収集、譲渡、使用許諾、加工、統合、分析や管理といったデータの流通又は利用を目的とする取引のことを指す意味で用いられている。第四次産業革命や Society5.0 といわれる前から行われている取引類型である、顧客に関するデータの分析の委託や市場に関するデータの収集も、データ取引といえる。また、AI 技術を利用したソフトウェアやサービスの開発の受委託なども、データ取引といえる。

---

[3] 例えば、経済産業省及び IoT 推進コンソーシアムは、平成 29 年 5 月に「データの利用権限に関する契約ガイドライン Ver1.0」を策定した（経済産業省ニュースリリース平成 29 年 5 月 30 日「『データの利用権限に関する契約ガイドライン Ver1.0』を策定しました」（https://warp.da.ndl.go.jp/info:ndljp/pid/11646345/www.meti.go.jp/press/2017/05/20170530003/20170530003.html））。

[4] 経済産業省ニュースリリース令和元年 12 月 9 日「『AI・データの利用に関する契約ガイドライン 1.1 版』を策定しました」（https://warp.da.ndl.go.jp/info:ndljp/pid/12685722/www.meti.go.jp/press/2019/12/20191209001/20191209001.html）

[5] 経済産業省ニュースリリース令和 3 年 3 月 1 日「『AI・データサイエンス人材育成に向けたデータ提供に関する実務ガイドブック』を策定しました」（https://warp.ndl.go.jp/info:ndljp/pid/13120268/www.meti.go.jp/press/2020/03/20210301004/20210301004.html）
経済産業省「『AI・データサイエンス人材育成に向けた データ提供に関する実務ガイドブック』について」（https://www.meti.go.jp/policy/it_policy/jinzai/AIdataguide.html）

[6] 経済産業省ニュースリリース令和 7 年 2 月 18 日「『AI の利用・開発に関するチェックリスト』を取りまとめました」（https://www.meti.go.jp/press/2024/02/20250218003/20250218003.html）

（３）データ契約の意義について

データすなわち電磁的に記録された情報[7]は、有体物ではないため、我が国法制度上、所有権の対象とはならない。つまり、原則としてデータの使用・収益・処分をする権利は債権的地位に過ぎず、データの使用・収益・処分をする排他的権利は、法制度上の保証は与えられていないと考えられる（契約ガイドライン・データ編第 3-1-(1)及び(2)）。

言いかえれば、①刑法や不正アクセス禁止法に違反する行為によりデータを取得する場合、②個人情報が含まれるデータを取り扱う場合、③秘密情報や限定提供データ（不正競争防止法第 2 条第 7 項に定義されるデータをいう。詳細は Q22 参照）を取り扱う場合、④肖像権やプライバシー権を考慮しなければならない場合や、⑤外為法に抵触し得る場合（詳細は Q54 参照）などの制約（以下、本項においてまとめて「法的制約等」という。）がある場合を除いて、原則、誰でも自由にデータを利用できるといえる。

加えて、データ自体が知的財産権の対象となる場合も限られることから（Q24 参照）、データ取引においては、当事者間でデータの取扱いについて合意すること、すなわちデータ契約の重要性が指摘される（契約ガイドライン・データ編第 3-2-(1)）[8]。

（４）データ契約におけるサイバーセキュリティ関連法令上のポイント

データ契約（データの取扱いに関する取り決め）を行うに当たってのポイントは、まずデータ契約を交渉・締結しようとするデータ取引において、取引対象とするデータを特定した上で、どのような法的制約等があり得るかを調査し、把握して、契約上の手当てをすることである。

そして、把握した法的制約等の存否・内容を踏まえつつ、データが物権の対象ではないことを念頭に、取引の対象としようとするデータのライフサイクル（データが生成され利用・保管されて消去されるまで）の各段階に応じた契約当事者間のデータの利用権限を検討・交渉・合意することとなる（契約ガイドライン参照）。

このようなデータ契約の交渉・合意に当たってのサイバーセキュリティ関連法令上のポイントとしては、例えば、以下が挙げられる。

ア　取り扱うデータや取り扱うことができる者の範囲・取扱い態様の内容について

①　各契約当事者について（当事者内でのアクセス権の付与範囲など）

---

[7] 官民データ活用推進基本法において、「官民データ」は「電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録をいう……）に記録された情報……」と定義されている（同法第 2 条第 1 項）。

[8] なお、企業において、有体物の取引に関する職務権限は内規などに定められているものの、データ取引については、各種データの流通・利用における取扱いに関する職務権限が明らかではないためにデータ契約の交渉、合意や実行に至らないとの問題点がある。この点、データ取引に当たっての社内体制の検討・整備に関する参考資料も提供されている（経済産業省「データ利活用のポイント集」（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/datapoint.pdf）128 頁～141 頁・参考）。

② 契約当事者以外の第三者（委託先等）における取扱いについて
③ 例えば、データの並べ替え（ソート）について、加工と取り扱うのか、また加工後のデータ（契約ガイドラインにおいては「派生データ」と呼んでいる）の取扱いについても合意の対象とするのか、対象とするのであればどのような取り決めをすべきかといった論点が生じ得る。

イ　秘密保持義務・電磁的管理性の保持義務について

① 秘密情報とは別の取扱いを取り決めるか、データも秘密情報に含めるか。
② 特に、データ取引においては、情報の「開示」や「知得」と認識し難い場面、また秘密である旨が明示された情報とはいえない場面もあり得るため、データを秘密情報に含めるとしても、典型的な秘密保持義務に関する条項の書き方で捕捉でき得るかについては検討を要する[9]。

ウ　セキュリティのレベル又はデータの管理体制に関する合意について

① 内部不正などのサイバーセキュリティインシデントが生じたときなどに、営業秘密（Q21 参照）又は限定提供データ（Q22 参照）であると主張して争う予定があるか、争う予定があるのであればどのような管理をすべきかという観点からも考慮を要する。
② セキュリティのレベル又はデータの管理体制について合意するとして、当該レベル・体制の対象とするデータの範囲をどうするか（上記ア同様、どういった基準で「派生データ」を設定し、どのような「派生データ」も対象範囲に含めるのかという考慮も要する。）、当該レベル・体制についての監査条項を加えたいとしても当該データの範囲や特性を踏まえるとそもそも実効性のある監査を行える手段があるのか、あるとしてもコストはどれくらいか、といった観点からも考慮を要する。

エ　保証／非保証条項・免責条項について

① 安全性（ウイルスに感染していないこと）又は完全性について、保証又は免責の対象とするか。
② 保証・非保証や免責については、対象とするデータの特性及びデータ取引の目的に応じた考慮を要する。例えば、データに基づいて生じた成果物の安全性又は完全性について保証又は免責の対象とするかを検討するに当たっては、AI 技術を利用したソフトウェアの開発委託の場合であれば従来型のソフトウェアの開発以上にユーザとベンダ双方の積極的な関与が必要であり責任の分配についても検討を要する（契約ガ

[9] 例えば、データ取引の目的として生じるデータやデータ取引に派生したり副産物的に生じたりするデータと、データ取引に当たって「開示」したデータとの同一性を認めることが困難な場合には、どの範囲のデータを秘密情報として捕捉するかにつき検討や工夫を要することとなる。

イドライン AI 編第 3-4 及び第 4-3-(4)）など、対象とする成果物の特性に応じた考慮が必要となる。

オ　遵守すべき内容について

① 対象とするデータの内容や特性、また取引自体の内容や特性に応じて、どのような遵守義務を課し、違反時の効果（損害賠償、違約金、中途解約、解除、紛争解決の方法、紛争解決費用の負担等）をどのように設けるか。

② そもそも、遵守できているのか、又は遵守義務に違反したかについて、技術的に認知、確認、検証等できるのか。できるとして、どのような基準に基づいて義務違反と判断すべきか。

なお、契約ガイドライン[10]は、サイバーセキュリティに限らず、データ取引の事例を紹介・検討しているほか、モデル契約の紹介・解説も掲載している。また、AI 人材育成ガイドブックも、AI 人材の育成に資する取組のうち、三者以上の関係者間でのデータの授受を伴うものにおけるデータ契約の枠組みを 4 つ提示し[11]、それぞれの枠組みにおける留意点を検討し、モデル契約の紹介・解説を掲載しているので、参考となる。

３．参考資料（法令・ガイドラインなど）

・経済産業省「AI・データの利用に関する契約ガイドライン 1.1 版」
https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization.html

・経済産業省「AI・データサイエンス人材育成に向けた データ提供に関する実務ガイドブック」
https://www.meti.go.jp/policy/it_policy/jinzai/AIdataguide.html

・経済産業省「データ利活用のポイント集」
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/datapoint.pdf

・経済産業省「AI の利用・開発に関する契約チェックリスト」
https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20250218003-ar.pdf

４．裁判例

特になし

---

10 契約ガイドラインは、(a)一方当事者が既存データを保持しているという事実状態が明確であるか否か、(b)複数当事者が関与して従前存在しなかったデータが新たに創出されるか否か、(c)プラットフォームを利用したデータの共用か否かという観点からデータ契約を整理し、①データ提供型、②データ創出型、③データ共用型という 3 つの類型を取り扱う。

11 AI 人材育成ガイドブックが提示する 4 つのデータ契約の枠組みは、データ提供型（従来の基本的な枠組み）に加えて、ハッカソン型、有償コンサル型、及び共同研究型である。詳細については、同ガイドブックを参照されたい。

Q52 データ漏えいに関するシステム開発ベンダの責任とモデル契約

システム開発ベンダは、個人情報等を取り扱うウェブシステムの開発に際して、開発当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供する義務を負うか。契約内容に記載されていない場合についてはどうか。

タグ：民法、SQL インジェクション、重過失、モデル契約、セキュリティ仕様

１．概要

システム開発ベンダは、個人データやクレジットカード情報など流出すれば個人やシステムの発注者に損害が生じるシステムの開発に際しては、別段の合意がない限り、適切なセキュリティ対策が採られたアプリケーションを提供する義務がある。

システム開発の業務委託契約書や発注仕様にセキュリティ対策について記述されている場合はもちろんのこと、記述されていない場合でも、開発当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示に合意されていたとされ、特段の事情もなく既知の脆弱性についてセキュリティ対策を講じなかった場合、発注者に生じた損害の賠償義務を負う。

２．解説

（１）ベンダの債務の内容としてのセキュリティ対策

開発する情報システムの性質にもよるが、個人データ等を取り扱うウェブシステムについては、その流出を防ぐために、必要なセキュリティ対策を施したプログラムの提供が契約上の債務の内容となる。

システム開発の業務委託契約書や発注仕様にセキュリティ対策についての記述がない場合でも、既知の代表的なセキュリティ攻撃手法について、行政機関が対策の必要性及び対策の具体的方法を公表している場合、これに従ったプログラムの提供をしなければシステム開発ベンダが債務不履行責任を問われ得る（東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁）[1]。

もっとも、行政機関が単に「望ましい」と指摘するにすぎないセキュリティ対策については、契約で特別に合意していない場合は当然に実施すべきものではない。

[1] なお、SQL インジェクションが「既知の脆弱性と位置付けられ、これに対する対策を行うことが（筆者注：仕様書に）明記されていた」場合において、エスケープ処理の入れ忘れについて過失による不法行為責任（民法第 715 条）が問われ、情報漏えいが発生していない段階であっても損害賠償請求が認容された事案もある（東京地判平成 30 年 10 月 26 日（平成 29 年（ワ）第 40110 号））。

具体的には、平成 21 年のオンラインショップのウェブシステムの開発に当たり、平成 18 年に経済産業省が発行した SQL インジェクション攻撃に対する注意喚起文書[2]を受け、平成 19 年に IPA が発行した文書[3]に明示された SQL インジェクション攻撃に対するバインド機構の使用及びエスケープ処理という対策については、多大な労力や費用がかかるものでもなく、ベンダの当然の債務となるとされたが、IPA の前述の文書において「望ましい」旨を記述されたデータベースの暗号化等については、ベンダの当然の債務とはいえないとされた（上記・東京地判平成 26 年 1 月 23 日）。

また、ベンダにおいては、サイバーセキュリティに対する脅威により自らが供給したシステムに被害が生ずることを防ぐため、システムの利用者がその安全性及び信頼性の確保のために講ずる措置に配慮した設計及び開発、適切な維持管理に必要な情報の継続的な提供その他のシステムの利用者がサイバーセキュリティの確保のために講ずる措置を支援する取組を行うよう努めることが求められている[4]。

（２）ウェブシステムのセキュリティに関する発注者の責務

契約書や発注書に記載がなくても開発当時のセキュリティ水準を採用したシステムの開発がベンダの当然の義務とされるからといって、発注者が発注するシステムのセキュリティ水準について無関心であることは望ましくない。個人データの流出が懸念されるウェブシステムの開発を委託する場合、当該システムにセキュリティ対策を講じなければ、システムの利用者にどのような危害・損失が発生するのか、それを未然に防ぐためには、どのような対策が望ましいのか、たとえ情報システムに関する詳しい知見がなかったとしても、開発を委託するベンダとの間で十分な協議（リスクコミュニケーション）を行い、ベンダが必要な対策を講じることができるよう、セキュリティ対策のための合理的なコストの負担を検討することが必要となる。

前述のウェブシステム開発ベンダが責任を問われた事件でも、発注者のシステム担当者が、顧客のクレジットカード情報のデータがデータベースにあり、セキュリティ上はクレジットカード情報を保持しない方が良いことを認識し、ベンダからシステム改修の提案を受けていながら、何ら対策を講じずにこれを放置したことについて、クレジットカード情報流出の一因となったとして、発注者に生じた損害の 3 割の過失相殺を相当としている。

---

[2] 経済産業省「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」（平成 18 年 2 月 20 日）
（https://www.meti.go.jp/policy/it_policy/privacy/kanki.html）

[3] IPA「平成 18 年度調査研究報告書 大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策～」（平成 19 年 3 月）
（https://warp.ndl.go.jp/collections/info:ndljp/pid/11117513/www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/index.html）

[4] サイバーセキュリティ基本法第 7 条第 2 項

（３）重過失

ベンダにシステム開発に関する専門的知見があり、これを信頼して発注者が契約を締結し、ベンダに求められる注意義務の程度が高度なものである場合であって、世間で頻発するセキュリティ攻撃に関して行政機関が注意喚起しているなど、セキュリティ攻撃への対策を講じなかった場合の結果が予見することが容易であり、また、対策そのものに多大な労力や費用がかかるものではないような場合、対策を怠ったベンダの債務不履行責任は、重大な過失があったものとされることがある。

ベンダが賠償すべき損害額の上限に関する規定など、システム開発契約における免責条項の有効性に関して、上記・東京地判平成 26 年 1 月 23 日は、一律に責任を一定額に制限する旨の免責条項について、被告が「権利・法益侵害の結果について故意を有する場合や重過失がある場合……にまで同条項によって被告の損害賠償義務の範囲が制限されるとすることは、著しく衡平を害するものであって、当事者の通常の意思に合致しない」ため、被告に故意又は重過失がある場合には適用されないと解するのが相当であると判示しているため、免責条項の有効性については留意が必要である（データ消失時の責任と当該責任の免責条項の有効性について Q61 参照）。

（４）IPA モデル契約

IPA は、令和 2 年 12 月 22 日に、「情報システム・モデル取引・契約書」（受託開発（一部企画を含む）、保守運用）の第二版[5]（以下、本項において「IPA モデル契約」という。）を公開した。第二版では、①セキュリティ、②プロジェクトマネジメント義務及び協力義務、③契約における「重大な過失」の明確化、④システム開発における複数契約の関係、⑤システムの再構築対応という 5 つの論点に関する検討・見直しが行われた。

セキュリティに関しては、ユーザとベンダとは、それぞれの立場に応じて必要な情報を示しつつ、リスクやコスト等について相互に協議することにより、セキュリティ対策についてソフトウェアに具体的に具備する機能である「セキュリティ仕様」を決めることが必要であるとされ、その観点から、以下の見直しが行われている。

① 条項の見直し（定義条項、責任者条項、セキュリティ条項）
② セキュリティの実装プロセスに関する解説の加筆
③ セキュリティ検討 PT による「セキュリティ仕様関連文書」の策定

セキュリティ仕様の決定に当たっては、ベンダとユーザの間で、必要な情報を相互に出し合い、公的機関や業界団体、セキュリティ関連企業等が提供する参照情報によってセキュリティの脅威を把握し、リスク評価を行い、対策の実装の有無を決定、合意し、それを仕様書に反映するというプロセスが示されている。

IPA モデル契約のセキュリティ条項（第 50 条）は、セキュリティ仕様についてクリアすべき基準及び開発プロジェクトを進める上での提案や合意に関する手順が確立されて

[5] https://www.ipa.go.jp/digital/model/model20201222.html

いない場合を A 案、確立されている場合を B 案として区別している（B 案では簡素な規定となっている）ところ、以下では A 案について概説する。

（５）IPA モデル契約のセキュリティ条項

ア　セキュリティ仕様の確定・書面化等

ユーザ及びベンダは、協議の上で、開発業務開始前までにセキュリティ仕様を確定し、書面化する必要がある（第 50 条第 1 項）。ただし、セキュリティ仕様の確定後でも、その後新たなセキュリティ脅威が生じた等の場合には、IPA モデル契約書に定められた変更管理手続によれば、当該セキュリティ使用を変更することができる（同条第 3 項）。

イ　セキュリティガイドラインの参照（オプション）

第 50 条第 2 項と第 3 項の間に、オプションとして、ガイドラインの参照に関する規定がある。当該規定は、セキュリティ仕様を作成する際に、両当事者が何らかのセキュリティガイドラインを参照することに合意した場合、当該ガイドラインの名称とバージョンだけではなく、当該ガイドラインを参照して適用すべき事項（実装する対策）をセキュリティ仕様に個別に記載すべきこと等を定めている。そして、実装しない対策のうち、軽微とはいえないセキュリティ上の影響が懸念されるリスク受容項目については、その影響そのものについて議事録に記載することを定めており、この議事録がユーザとベンダのリスクコミュニケーションの証憑になるとしている。

ウ　情報提供義務

ユーザは、ベンダに対して、セキュリティ仕様を確定するために必要な情報を適時に提供する義務を負う（第 50 条第 2 項）。ユーザが提供した情報に誤りがあったことに起因してセキュリティインシデントが生じ、セキュリティ仕様に従った対策が奏功しなかった場合には、原則としてベンダは免責される。

ユーザ及びベンダのいずれも、セキュリティ仕様の確定後から納入までの間に確定したセキュリティ仕様では対応できない脅威や脆弱性（個別契約の目的を達することができないものに限る。）について知ったときは、相手方に対して書面で通知する義務を負う（第 50 条第 4 項）。

エ　セキュリティ仕様の不備等に関する責任

ベンダは、セキュリティ仕様で対応できないセキュリティ上の脅威又は脆弱性に関する情報を収集する義務を負わない（第 50 条第 7 項前段）。ただし、個別契約の目的を達成できない脅威又は脆弱性があることを知りながらユーザに通知しなかった場合（重大な過失によって知らなかったときを含む。）には、義務違反となる（同第 7 項後段）。

ここにいう「重大な過失」に関しては、(a)脅威又は脆弱性が単に既知であること（例えば IPA が運営する脆弱性対策情報のデータベース JVN iPedia[6]に登録されている状態）では足りず、(b)当該脆弱性に関するセキュリティ攻撃が頻発するなどの事態を受けて、国が一般的な方法で広く周知活動を行うなど、当該脅威又は脆弱性が広くベンダに知られるものとなっており、(c)加えて結果回避が容易である場合（特別な技術や多大なコストを要しない対策が広く知られているなど）には、重過失が認められる余地があるとの解釈が示されていることに留意が必要である（前掲・東京地判平成 26 年 1 月 23 日判例時報 2221 号 71 頁を参考としたもの）。

また、ベンダはセキュリティ仕様に従ってソフトウェアのセキュリティ対策を講じる義務は負うが、セキュリティインシデントが生じないことを保証するものではないことが明記されている（第 50 条第 6 項）。

３．参考資料（法令・ガイドラインなど）

・民法第 415 条
・民法第 715 条
・IPA　情報システム・モデル取引・契約書第二版

４．裁判例

・東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁
　概要は本文に記載のとおり。
・東京地判平成 30 年 10 月 26 日（平成 29 年（ワ）第 40110 号）
　ウェブサイト上で提供するシステムの制作をベンダに発注し、納品を受けたところ、SQL インジェクションを含む複数の脆弱性が発見された。ベンダとの契約書上 SQL インジェクション対策が明記されていたという事実関係のもとで、債務不履行が認められた事案。
・東京地判令和元年 12 月 20 日（平成 29 年（ワ）第 6203 号）
　通販サイト、サーバ及びウェブアプリケーション等からなるシステムに、脆弱性を含むオープンソースソフトウェアを使っていたところ、当該サイトの運営・保守をベンダ

[6] IPA は、日本国内で利用されているソフトウェア製品又は主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーションに係る脆弱性関連情報が発見された場合、その届出の受付機関となっており（情報処理の促進に関する法律施行規則第 47 条、ソフトウェア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号））、メーカー等との調整を経て、脆弱性を公開している。また、令和 6 年 6 月の改正によって、IPA は、対策方法が作成された日から脆弱性情報公表日までの間であって、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に脆弱性に起因する重大な影響が及ぶおそれがあると認められるときは、調整機関及び調整機関を経由して製品開発者と協議をした上で、政府機関や当該設備を用いる事業者等（脆弱性情報等を適切に管理できる者に限る。）に当該脆弱性情報等をあらかじめ通知することができるようになった（ソフトウェア製品等の脆弱性関連情報に関する取扱規程第 2 の 2(2)ア(ｸ)）。

に委託し、その中で顧客のクレジットカード情報が漏えいしたという事案において、ベンダに対してセキュリティ対策まで委託していないと認定し、債務不履行責任を否定した事案。

・東京地判令和 2 年 10 月 13 日（平成 28 年（ワ）第 10775 号）

ウェブサイトからクレジットカード情報が漏えいした事件について、サイトの構築・保守を委託したベンダに対し債務不履行に基づく損害賠償請求を行ったものの、クレジットカード情報を保持しない仕様にする義務、及び技術水準に沿ったセキュリティ対策を行う義務を否定し、債務不履行の成立を否定した事案。

・東京地判令和 4 年 1 月 12 日（令和 3 年（ワ）第 23709 号）

ホームページの制作、オンラインショップ機能の組込み等の業務を委託していたが、制作されたホームページの管理画面への外部からの侵入が可能な状態となっていたことから、顧客のクレジットカード情報を流出する被害が生じ、その原因がベンダの作成したホームページに問題があったことによるとして、ベンダに対しては上記業務委託契約の不履行に基づき、損害賠償責任を認めた事案。

Q53 サプライチェーン・リスク対策

サプライチェーン・リスク対策を実施・推進するにあたり、ビジネスパートナーや委託先等との関係において、どのような法律上の事項に留意すべきか。

タグ：独占禁止法、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）、リスクマネジメント、サプライチェーン・リスク、委託、優越的地位の濫用、IT 調達

１．概要

一定のサイバーセキュリティ対策を実施していることを取引の条件とすることや、一定のサイバーセキュリティ対策を実施することを取引先に求めることは、社会全体のサイバーセキュリティ対策に資するものであり、原則として、我が国の何らかの法令に抵触するおそれはないが、優越的地位の濫用及び取適法に留意すべき場合もある。

以下では製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（昭和 31 年法律第 120 号）（以下、本項において「取適法」という。）を解説しているが、取適法は令和 8 年 1 月 1 日に「下請代金支払遅延等防止法」（下請法）が改正・改称された法律である。

２．解説

（１）サプライチェーン・リスクとは

サプライチェーンとは、一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのことをいう。これらに加え、IT 分野では、情報システム・IT サービスの設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることもある。

サプライチェーン・リスクとは、従来、自然災害等何らかの要因からサプライチェーンに障害が発生し、結果として事業の継続に支障を来すおそれがあるというリスクを主に想定していたが、近年、新たなサイバーセキュリティリスクとして、サプライチェーン・リスクへの懸念が生じている[1]。すなわち、サプライチェーンのいずれかの段階において、①サイバー攻撃等によりマルウェア混入・情報流出・部品調達への支障等が発生する可能性、②悪意のある機能等が組み込まれ、機器やサービスの調達に際して情報窃取・破壊・情報システムの停止等を招く可能性についても想定する必要がある[2]。以下では、サプライチェーン・リスクのうちサイバーセキュリティに関する事項として、例えば、①取引に

[1] 総務省「令和 2 年版情報通信白書」1-3-4-4-1（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134410.html）参照。
[2] サイバーセキュリティ 2025・223 頁参照。

使用する自社の情報システムやビジネスパートナーが使用する情報システムにセキュリティインシデントが生じるおそれや、②サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうおそれ、③サプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されるおそれ、さらに④その結果、他社の二次被害を誘発し、加害者となるおそれなどのリスクを想定する[3]。

（２）サプライチェーン・リスク対策の現状について

ア　サプライチェーン・リスク対策の必要性

サプライチェーン・リスク対策については、国内外のサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえ、サプライチェーン全体を通じた対策の推進の必要性が高まっている[4]。

実務においても、一例として、システム管理等の委託先や、取引等に用いる IT サービスの選定時に、与信、業務体制や契約条件の各審査に加えて、セキュリティ体制やセキュリティ対策状況も審査する対策例がある。このときの審査方法としては、外部機関による監査の結果や認証等の取得状況を提供・開示してもらう、取引（候補）先にチェックリスト形式でセキュリティ体制やセキュリティ対策状況を報告してもらう、自社のセキュリティ部門・部署がヒアリング・インタビュー等をする、場合によっては外部専門家に審査してもらうといった方法がある。委託先においてサイバーセキュリティ対策の担保が求められるようになり、異なる委託元から様々な対策水準を要求される一方、委託元は外部から各委託先の対策状況を判断することが難しいといった課題が存在する。こうした課題に対応するため、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつその対策状況を可視化する仕組みである「サプライチェーン強化に向けたセキュリティ対策評価制度」（SCS 評価制度）の構築が進められており、令和 8 年度末頃の制度開始が目指されている[5]。令和 8 年 3 月、経済産業省及び NCO から「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」が策定・公表された[6]。

また、サプライチェーン上での対策の底上げとして、サイバーセキュリティお助け隊等の中小企業向け施策を活用するなども考えられる[7]。

---

[3] 経営ガイドライン 29 頁参照。
[4] 経営ガイドライン 3 頁参照。
[5] サイバーセキュリティ戦略Ⅲ.2(3)②。最新のサイバーセキュリティ戦略については Q2 を参照されたい。
[6] https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf
[7] 経営ガイドライン 30 頁参照。

その他の対策例としては、取引を開始したときには、契約上の監査条項に基づいて実地監査をする、委託取引の場合は委託先に対してサイバーセキュリティに関する教育・研修を実施するといった方法が考えられる。なお、外部監査等も、大きく分けると、セキュリティ体制自体を監査しているものと、製品・サービスのセキュリティレベル等を監査しているものとがあるため、サプライチェーン・リスクの内容・程度に応じて、いずれを参考とすべきかについて留意を要する[8]。

イ　経営者と担当幹部との関係において

経営ガイドラインにおいては、「自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要」（同 12 頁）として、経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部に対して以下の指示をすることが必要としている。（同 29 頁）。

① サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。

② ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

ウ　再委託先について

再委託を行うに当たっては、サプライチェーン・リスク対策として、委託先による再委託先の監督を求めることや、委託先に求められる水準と同等のセキュリティ水準を再委託先においても確保することを条件とすることが考えられる。

具体的には、委託先からの再委託・再々委託を何次までと制限する、再委託先を通知してもらい事前承諾を要求するといった対策例が考えられる。また、SCS 評価制度開始後にあっては、同制度で定める評価の取得又は同制度で用いる評価の取得を再委託先の選定に際して求める、といった活用が考えられる[9]。

[8] 例えば、前者については、ISMS が知られており、後者については、SOC 2（Service and Organization Controls 2）報告書の開示を受ける、ペネトレーションテストや脆弱性診断の結果を秘密保持義務を負った上で開示してもらう、ISMAP クラウドサービスリスト（詳細は Q42 参照）を参考にするといった方法が考えられる。

[9] 制度開始前にあっても、同制度の制度構築方針において要求項目・評価基準が公表されているため、当該基準への準拠を再委託先に対して求める、といった活用も考えられる。

エ　認証・評価・保証報告書の取得について

上記アのとおり、取引先から取引条件として求められることから、又は、取引先のサイバーセキュリティ対策の状況確認のコストの低減につながることから、情報セキュリティマネジメントシステム（ISMS）に関する認証を取得する企業もある（なお、技術等情報の適切な管理に係る認証制度については Q11 参照）。

また、SCS 評価制度開始後にあっては、同制度の評価を取得することで、発注企業等に対するセキュリティ対策に係る説明の説得力向上や、セキュリティサービスの標準化による選択肢拡大・コスト低減等の効果が期待される。

その他第三者機関に自社のサイバーセキュリティ対策を含めた内部統制を評価してもらい、その結果を取引（予定）先に報告してもらうというサービスを利用することも考えられる。

（３）法律上の留意点について

サプライチェーン・リスク対策は、その一環として、取引先に対してサイバーセキュリティ対策を求めることも含まれていることから、独占禁止法に抵触しないかが懸念される。

具体的には、不公正な取引方法のうち、①その他の取引拒絶、若しくは②優越的地位の濫用、又は③取適法に抵触しないかが問題となる[10]。

ア　その他の取引拒絶

（ア）基準

その他の取引拒絶とは、「不当に、ある事業者に対し取引を拒絶し若しくは取引に係る商品若しくは役務の数量若しくは内容を制限し、又は他の事業者にこれらに該当する行為をさせること」とされている。

「流通・取引慣行ガイドライン」[11]は、単独の直接取引拒絶について、「事業者がどの事業者と取引するかは、基本的には事業者の取引先選択の自由の問題である。事業者が、価格、品質、サービス等の要因を考慮して、独自の判断によって、ある事業者と取引しないこととしても、基本的には独占禁止法上問題となるものではない。しかし、事業者が単独で行う取引拒絶であっても、例外的に、独占禁止法上違法な行為の実効を確保するための手段として取引を拒絶する場合には違法となり、また、競争者を市場から排除するなどの独占禁止法上不当な目的を達成するための手段として取引を拒絶する場合には独占禁止法上問題となる」（同 35 頁）との考え方を示した上で、市場における有力な事業者が競争者を市場から排除するなどの独占禁止法上不

[10] 経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」第 3 の 2 が参考となる。（https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html ）

[11] 公正取引委員会事務局「流通・取引慣行に関する独占禁止法上の指針」（https://www.jftc.go.jp/dk/guideline/unyoukijun/ryutsutorihiki.html）

当な目的を達成するための手段として取引を拒絶し、これによって取引を拒絶される事業者の通常の事業活動が困難となるおそれがある場合には独占禁止法上問題となるとしている。

（イ）検討

事業者が、真にサプライチェーン・リスク対策を目的として、独自の判断で、取引先に一定のサイバーセキュリティ対策を求め、当該対策ができない場合に取引を拒絶するなど、サプライチェーン・リスク対策に向けて合理的な範囲で行われる単独の取引拒絶は、独占禁止法上問題とならない。

イ　優越的地位の濫用

（ア）基準

優越的地位の濫用とは、独占禁止法第 2 条第 9 項第 5 号に定義されるように、「自己の取引上の地位が相手方に優越していることを利用して、正常な商慣習に照らして不当に」、（イ）「継続して取引する相手方（新たに継続して取引しようとする相手方を含む。ロにおいて同じ。）に対して、当該取引に係る商品又は役務以外の商品又は役務を購入させること」、（ロ）「継続して取引する相手方に対して、自己のために金銭、役務その他の経済上の利益を提供させること」、又は（ハ）「取引の相手方からの取引に係る商品の受領を拒み、取引の相手方から取引に係る商品を受領した後当該商品を当該取引の相手方に引き取らせ、取引の相手方に対して取引の対価の支払を遅らせ、若しくはその額を減じ、その他取引の相手方に不利益となるように取引の条件を設定し、若しくは変更し、又は取引を実施すること」をいう。

「優越的地位濫用ガイドライン」[12]によれば、正常な商慣習に照らして不当である場合とは、「公正な競争を阻害するおそれ」（公正競争阻害性）がある場合をいう。この公正競争阻害性については、「問題となる不利益の程度、行為の広がり等を考慮して、個別の事案ごとに判断することになる。例えば、①行為者が多数の取引の相手方に対して組織的に不利益を与える場合、②特定の取引の相手方に対してしか不利益を与えていないときであっても、その不利益の程度が強い、又はその行為を放置すれば他に波及するおそれがある場合には、公正な競争を阻害するおそれがあると認められやすい」とのことである。

（イ）検討

よって、自社が優越的な地位にある場合には、取引先に対して一定のサイバーセキュリティ対策を求めることが、正常な商慣習に照らして不当に、継続して取引する相手方に、自己の指定する事業者が供給する商品又は役務、つまり、当該取引に係る商品又は役務以外の商品又は役務を購入させること（独占禁止法第 2 条第 9 項第 5 号

[12] 公正取引委員会「優越的地位の濫用に関する独占禁止法上の考え方」（https://www.jftc.go.jp/hourei_files/yuuetsutekichii.pdf）。

イ参照）に該当しないか、又は、一方的に、取引の条件を設定し、若しくは変更し、又は取引を実施する場合に、当該取引の相手方に正常な商慣習に照らして不当に不利益を与えること（同号ハ参照）に該当しないかという点に留意する必要があるといえる。

例えば、取引の相手方に対し、有償のセキュリティサービスの利用やセキュリティの認証の取得を要請したにもかかわらず、コスト上昇分の取引価格への反映の必要性について、価格の交渉の場において明示的に協議することなく、従来どおりに取引価格を据え置くことは独禁法上問題となるおそれがあるといえる[13]。

ウ　取適法

（ア）基準

取適法は、事業者の資本金規模・従業員規模と取引の内容により規制対象を画するものである[14]。取引の内容としては、①製造委託、②修理委託、③情報成果物作成委託、④役務提供委託及び⑤特定運送委託の 5 種類が対象となる。

そして、資本金規模・従業員規模と取引の内容が取適法の定める要件に該当する場合には、取適法上の委託事業者又は中小受託事業者に該当し、委託事業者に対して、給付の内容等を書面又は電磁的方法による明示義務等が課せられ、加えて、取適法第 5 条第 1 項各号及び第 2 項各号に規定される行為が禁止される。

委託事業者の禁止行為としては、受領拒否、下請代金の支払遅延、下請代金の減額、返品、買いたたき、購入・利用強制、報復措置、有償支給原材料等の対価の早期決済、不当な経済上の利益の提供要請、不当な給付内容の変更及び不当なやり直し、並びに、協議に応じない一方的な代金決定の 11 種類がある。

このうち、「買いたたき」とは、発注する物品・役務等に通常支払われる対価に比べ著しく低い代金を不当に定めることを、「購入・利用強制」とは、「正当な理由がないのに、指定する物品や役務を強制して購入、利用させること」により、中小受託事業者にその対価を負担させることを、「不当な経済上の利益の提供要請」とは自己のために、中小受託事業者に金銭や役務等を不当に提供させることをいう。

（イ）検討

委託事業者は、中小受託事業者に対し、中小受託事業者に生じるコスト上昇分を考慮することなく、著しく低い代金の額を不当に定めた場合には、取適法上の「買いたたき」（取適法第 5 条第 1 項第 5 号）に該当し得る。中小受託事業者に対して自己の指定するサイバーセキュリティ対策に関する物品の購入又は役務の利用を強制する場合には、正当な理由がないと、「購入・利用強制」（取適法第 5 条第 1 項第 6 号）

---

[13] 前掲注 10・経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」第 3 の 2(1)。

[14] 公正取引委員会ウェブサイト「取適法の概要」（https://www.jftc.go.jp/file/toriteki_leaflet.pdf）。

に、中小受託事業者の利益を不当に害する場合には「不当な経済上の利益の提供要請」（取適法第 5 条第 2 項第 2 号）にそれぞれ該当し得るため、留意する必要があるといえる。

（４）（参考１）サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説

発注者側である大企業が取引先である中小企業等に対してサイバーセキュリティ対策の実施要請をするに当たって、一定のサイバーセキュリティ対策を実施していることを取引の条件とすること等について、上記（３）で検討したような、独占禁止法や取適法の適用関係を明確にするため、経済産業省及び公正取引委員会では、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を公表し、一定の考え方を示していたところ[15]、令和 7 年 12 月 26 日、経済産業省及び公正取引委員会は、同文書を補足することを目的に、独占禁止法や取適法との関係を整理し、「問題とならない」ケースを想定した事例[16]と、想定事例の内容を補足するための解説文書[17]として、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説」を策定・公表した。

（５）（参考２）政府機関等におけるサプライチェーン・リスク対策

国の行政機関・独立行政法人・サイバーセキュリティ基本法に定める指定法人（以下、本項において「政府機関等」という。）においては、平成 30 年 12 月に、各府省庁間で「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（令和 7 年 7 月最新改正）[18]がなされ、これに基づきサプライチェーン・リスク対策が実施されている。

同申合せに基づき、政府機関等は、IT 調達のうち、下記 5 つの重要性の観点から、より一層サプライチェーン・リスクに対応することが必要であると判断されるものについては、価格面のみならず、総合評価落札方式等の総合的な評価を行う契約方式を採用し、原則として、NCO の助言を求めることとなっている。

① 国家安全保障及び治安関係の業務を行うシステム
② 機密性の高い情報を取り扱うシステム並びに情報の漏えい及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱うシステム
③ 番号制度関係の業務を行うシステム等、個人情報をきわめて大量に取り扱う業務を行うシステム
④ 機能停止等の場合、各省庁における業務遂行に著しい影響を及ぼす基幹業務システム、LAN 等の基盤システム、

---

15 前掲注 10 参照。
16 https://www.meti.go.jp/press/2025/12/20251226001/20251226001-f.pdf
17 partnership_soueijireikaisetu_.pdf
18 https://www.cyber.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf

⑤　運営経費がきわめて大きいシステム

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

Q54 サイバーセキュリティと輸出管理

サイバーセキュリティに関する物の輸出や技術提供を行う場合において、輸出管理に関する法令上、どのような点に留意すべきか。

タグ：外為法、輸出貿易管理令、外国為替令、貨物等省令、貿易外省令、役務通達、輸出管理、ワッセナー・アレンジメント、侵入プログラム関連品目

１．概要

輸出管理制度においては、規制対象リストに掲載されている貨物の輸出及び技術の提供を行う際には、原則として経済産業大臣の許可が必要となる。規制対象となる行為の範囲は広く、電子メールで当該技術のデータを送付することも対象行為となり得る。

サイバーセキュリティに関しては、武器や軍事転用可能な貨物や技術について、輸出管理における国際的な枠組み（輸出管理レジーム）の一つであるワッセナー・アレンジメントで検討され、侵入プログラム関連品目等が規制対象とされている。

侵入プログラム関連品目の中には、それに関わる脆弱性関連情報や、マルウェアに関する情報が含まれ得るが、セキュリティの脆弱性の開示に係るもの又はサイバー攻撃の対応に係るものは規制対象から除かれることが多く、サイバーセキュリティの実務への影響が低くなるよう配慮されている。

２．解説

（１）輸出管理制度

武器や軍事転用可能な貨物や技術が、我が国を含む国際的な平和及び安全の維持を脅かすおそれのある国家やテロリスト等、懸念活動を行うおそれのある者に渡り、大量破壊兵器等や通常兵器の開発等に転用されることを未然に防ぐため、国際的な枠組み（輸出管理レジーム）による輸出管理が推進されている。

我が国においては、外国為替及び外国貿易法（昭和 24 年法律第 228 号）（以下、本項において「外為法」という。）によって、輸出管理（貨物の輸出及び技術の提供の管理）を行っており、具体的には、規制対象となる貨物の輸出（外為法第 48 条第 1 項及び輸出貿易管理令（昭和 24 年政令第 378 号））や技術の提供（外為法第 25 条第 1 項、第 3 項及び外国為替令（昭和 55 年政令第 260 号））について経済産業大臣の許可を必要としている。

ア　規制対象について

外為法に基づく規制対象については、政省令で定める品目（武器、機微な汎用品など）に該当する貨物の輸出又は技術の提供を規制する「リスト規制」と、「リスト規制」に該当しない貨物又は技術であっても、その用途や需要者において、大量破壊兵器等や通常兵器の開発等に用いられるおそれがある場合などに貨物の輸出又は技術の提供を規制する「キャッチオール規制」がある。

イ　貨物の輸出と技術の提供

（ア）貨物の輸出

どのような場合に貨物の「輸出」にあたるかについて、法令上の定義は置かれていないが、その範囲は広い。典型的には、商取引に基づいて海外へ商品を送付することが想起されるが、その他、輸入した商品の返品等のための返送や、海外子会社への装置や部品の送付、個人が業としてではなく手荷物で海外に持ち出す場合等、かなり広範な行為が外為法上の「輸出」に該当する。

（イ）技術の提供

「技術」については、典型的には、リスト規制に該当する貨物の「設計」、「製造」又は「使用」に係る技術が規制対象となる。

技術の提供については、規制対象となる行為が外為法第 25 条第 1 項に規定されているところ、規制の対象となる外国為替令別表の中欄に掲げる技術（プログラムを含む。以下、本項において「特定技術」という。）を外国において提供することを目的とする取引（例えば、海外子会社において技術指導を行う場合や、電子データを外国へ送信する場合など）、居住者が非居住者に対して提供することを目的とする取引（例えば、日本居住者が外国から来た研修員に技術指導を行う場合）といった行為が規制対象とされている。

また、令和 4 年 5 月 1 日からは、居住者への技術提供であっても、雇用契約や経済的利益等に基づき外国政府や外国法人（非居住者）の強い影響を受けている状態（特定類型）に該当する居住者への技術提供については、「みなし輸出」管理の対象であることを明確化した（「みなし輸出」管理の運用明確化）。

ここにいう「取引」とは、経済産業省貿易経済協力局通達「外国為替及び外国貿易法第 25 条第 1 項及び外国為替令第 17 条第 2 項から第 4 項までの規定に基づき許可を要する技術を提供する取引又は行為について」[1]（以下、本項において「役務通達」という。）によれば、有償無償にかかわらず、取引当事者双方の合意に基づくものをいい、「提供することを目的とする取引」とは、特定国において又は特定国の非居住者に対して技術を提供することを内容とする取引をいう。例えば、サイバー攻撃など

[1] https://www.meti.go.jp/policy/anpo/law_document/tutatu/t10kaisei/ekimu_tutatu.pdf

によって規制対象となる技術が漏えいした場合は、当事者双方の合意がないため「取引」に該当しないと考えられる。

次に、ここにいう「提供」とは、役務通達によれば、「他者が利用できる状態に置くこと」と定義されているところ、いわゆるクラウドコンピューティングサービスの利用についても規制対象となり得る。例えば、役務通達別紙 1-2「いわゆるクラウドコンピューティングサービスの解釈」[2]によれば、クラウドストレージサービスなどの利用により、国外に設置されたサーバに情報が保管される場合に当該サーバに情報を保管する行為が技術の「提供」にあたるかどうかについて、ストレージサービスを利用するための契約は、サービス利用者が自ら使用するためにサービス提供者のサーバに情報を保管することのみを目的とする契約である限りにおいて、サービス利用者からサービス提供者に情報を提供することを目的とする取引に当たらないため、外国に設置されたサーバに特定技術が保管される場合であっても、原則として[3]外為法第 25 条第 1 項又は外為令第 17 条第 2 項に規定する役務取引に該当しないとされており、したがって外為法第 25 条第 3 項の対象にも該当しない。

また、サーバ上に存在するプログラム（アプリケーションソフトウェア等）を、インターネットを介して、他者がダウンロードすることなく利用できる状態にするサービス（SaaS 等）を提供することは、プログラムをサービス利用者にとって利用できる状態に置くことを目的とする取引であり、「提供」を目的とする取引に当たるため、当該プログラムが特定技術であれば、外為法第 25 条第 1 項又は外為令第 17 条第 2 項に定める役務取引に該当する[4]とされている。

（2）サイバーセキュリティに関する輸出管理

サイバーセキュリティの分野においては、サイバー攻撃に転用される懸念のあるツールについて、国家によるサイバー攻撃やテロリストに転用されることを防止する事を目的として、いくつかの品目が規制リストに追加されている。

---

[2] クラウドサービスに関しては、役務通達別紙 1-2 のほか、経済産業省安全保障貿易管理のウェブサイト「技術関連」の Q&A（https://www.meti.go.jp/policy/anpo/qanda25.html）において、Q3-1 から Q3-8 にかけて詳細に解説されているためそちらも参照されたい。なお、「クラウドコンピューティングサービスについては、サービスの形態や使用技術が日々進歩し変化しているため、諸外国の規制の動向等も踏まえつつ、必要に応じて通達及び Q&A を改正していく予定」（Q3-1）とされているため、その点留意が必要である。

[3] サービス提供者が保管された情報を閲覧、取得、利用できることを知りながらサービス利用契約を締結する場合や、契約開始後、サービス提供者が保管された情報を閲覧、取得、利用していることが判明したにもかかわらず契約関係を継続している場合には、実質的にサービス利用者からサービス提供者等に特定技術を提供することを目的とする取引とみなすとされている。

[4] ただし、貿易関係貿易外取引等に関する省令第 9 条第 2 項第 14 号イ（いわゆる市販プログラム特例）の要件を満たすプログラムについては、役務取引許可は不要である。

サイバーセキュリティに関して何を規制対象リストに加えるかについては、ワッセナー・アレンジメント[5]で議論されており、平成 26 年に外為法関連法令において、ワッセナー・アレンジメント合意内容を反映した侵入プログラム関連品目が規制対象リストに追加された。

なお、侵入プログラム関連品目の中には、侵入プログラムを製造するための脆弱性情報、マルウェアによる動作、被害、ふるまい等の情報や、類似するマルウェアに関する対策情報等が含まれ得るが、これらについては、「セキュリティの脆弱性の開示又はサイバー攻撃の対応に係るもの」として規制対象外となることが多いと考えられ、サイバーセキュリティに関する実務への影響が少ないよう配慮された規定となっている（詳細は後述）[6]。

（３）侵入プログラム関連品目

「侵入プログラム」については、役務通達別紙 1「外為令別表（貨物等省令を含む。）中解釈を要する語」によれば、電子計算機又は電気通信回線に接続する機能を有する機器の監視ツールによる検出を回避し、又は防御手段を無効化するように設計又は改造されたプログラムであって、①電子計算機又は電気通信回線に接続する機能を有する機器からデータ又は情報の抽出を行うこと、若しくはシステムや利用者のデータを変更すること、又は②外部からの命令の実行を可能とするため、プログラム又はプロセスの標準的な実行パスを改造すること、のいずれかの操作を実行するものと定義されている。

侵入プログラム関連の規制については、貨物の輸出及び技術の提供双方についてリスト規制が存在するが、侵入プログラムそのものを規制の対象としていない点に留意が必要である。

ア　規制対象となる貨物について

輸出貿易管理令別表第 1 の 8 の項において、「電子計算機若しくはその附属装置又はこれらの部分品……であつて、経済産業省令で定める仕様のもの」と規定されており、これに基づき、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令（平成 3 年通商産業省令第 49 号）（以下、本項において「貨物等省令」という。）第 7 条第 5 号において、「電子計算機若しくはその附属装置又はこれらの部分品であって、侵入プログラムの作成、指揮統制又は配信を行うように特に設計又は改造されたもの」と規定されている。

---

[5] Wassenaar Arrangement (http://www.wassenaar.org)

[6] なお、他国から日本へ輸出されたものを日本からさらに他国へ再輸出する場合に、元の輸出国の規制が適用される場合がある。例えば、米国に関しては、米国輸出管理規則（EAR: Export Administration Regulations）により、米国から日本へ輸出されたものを他国へ輸出する場合、日本の外為法に加えて EAR が適用される。EAR においても、2022 年に、ワッセナー・アレンジメントに基づき、侵入プログラム関連品目に関する規制が追加されたが、日本と同様、脆弱性の開示又はサイバー攻撃への対応を目的とする場合には規制の対象外である。

典型的にはいわゆる C&C サーバ[7]や、侵入プログラムのビルダーがこれに該当するが、「特に設計又は改造されたもの」でなければならないため、一般的に使用されている PC やサーバは該当しない。

イ　規制対象となるプログラム及び技術について

外国為替令別表の 8 の項において、「(一)　輸出貿易管理令別表第一の八の項の中欄に掲げる貨物の設計、製造又は使用に係る技術であつて、経済産業省令で定めるもの（四の項の中欄に掲げるものを除く。)」、「(二)　電子計算機若しくはその附属装置又はこれらの部分品の設計、製造又は使用に係る技術であつて、経済産業省令で定めるもの（(一)及び四の項の中欄に掲げるものを除く。)」と規定されており、これに基づき、貨物等省令第 20 条第 1 項及び第 2 項において、規制対象となるプログラム及び技術（プログラムを除く。）が規定されている。主たるものを抜粋すると以下のとおりである。

① プログラム関係
- a 上記アの貨物を含む貨物等省令第 7 条 1 号から第 5 号まで又は第 7 号のいずれかに該当するものを設計し、若しくは製造するために設計したプログラム（貨物等省令第 20 条第 1 項第 2 号）
- b 侵入プログラムの作成、指揮統制又は配信を行うように設計若しくは改造されたプログラム（貨物等省令第 20 条第 2 項第 6 号）

② 技術（プログラムを除く。以下 a から c において同じ。）関係
- a 上記①a のプログラムの設計、製造若しくは使用に必要な技術（貨物等省令第 20 条第 1 項第 2 号）
- b 上記①b のプログラムの設計、製造若しくは使用に必要な技術（貨物等省令第 20 条第 2 項第 5 号、同条同項第 6 号）
- c 侵入プログラムの設計に必要な技術（貨物等省令第 20 条第 2 項第 7 号）

ウ　セキュリティの脆弱性の開示又はサイバー攻撃の対応に係る例外

上記イの①、②、プログラムを除く技術については、セキュリティの脆弱性の開示に係るもの又はサイバー攻撃の対応に係るものは規制対象から除かれる。

役務通達別紙 1「外為令別表（貨物等省令を含む。）中解釈を要する語」によれば、「セキュリティの脆弱性の開示に係るもの」とは、「脆弱性を解決する目的のプロセスであって、脆弱性を特定するもの、報告するもの、対策を行い、若しくは調整する責任がある個人若しくは組織に伝達するもの又はこれらの個人若しくは組織と分析するもの」をい

[7] Command and Control（指揮統制）サーバの略称であり、C2（シーツー）サーバということもある。マルウェアに感染した PC をネットワーク経由で操作し、情報の収集や攻撃の命令を出すサーバのことを指す。

い、脆弱性関連情報の取扱いプロセス（Q72 参照）を念頭に置いているものと考えられる。

また、「サイバー攻撃の対応に係るもの」とは、「サイバーセキュリティ攻撃に対処するための対策を行い、又は調整する責任がある個人又は組織とサイバーセキュリティ攻撃に関する情報を交換するプロセス」をいうとされている。

上記イの規制は、海外のサイバー攻撃者や組織に対し、攻撃に転用されるおそれがあるツールや技術情報が渡らないようにするための規制であるが、サイバーセキュリティ分野において迅速な防御活動を行うためには、日々複雑化・巧妙化する攻撃手法や新たなソフトウェアの脆弱性に対応するため、海外のセキュリティベンダ等との連携や情報収集が不可欠である一方で、形式的には、マルウェアを製造するための脆弱性関連情報や、マルウェアによる動作・被害・振舞い等の侵入プログラムのビルダーや C&C サーバに関わる情報などを電子メールで海外に送信することが「技術の提供」として規制の対象になるおそれがあった。海外との情報交換のために逐一経済産業大臣の許可を取得する必要があるとなると、許可を取得する間にサイバー攻撃の被害が拡大するおそれもあり、そのような事態を招くのは本末転倒となるため、上記のとおり、セキュリティの脆弱性の開示に係るもの又はサイバー攻撃の対応に係るものを例外としたものである。

3．参考資料（法令・ガイドラインなど）

・ワッセナー・アレンジメント概要（外務省ウェブサイト）
https://www.mofa.go.jp/mofaj/gaiko/arms/wa/index.html
・外為法
・輸出貿易管理令
・外国為替令
・輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令
・経済産業省貿易経済協力局通達「外国為替及び外国貿易法第 25 条第 1 項及び外国為替令第 17 条第 2 項から第 4 項までの規定に基づき許可を要する技術を提供する取引又は行為について」
・経済産業省安全保障貿易管理ウェブサイト Q&A「技術関連」
https://www.meti.go.jp/policy/anpo/qanda25.html
・経済産業省安全保障貿易管理ウェブサイト「みなし輸出管理の運用明確化」
https://www.meti.go.jp/policy/anpo/anpo07.html

4．裁判例

特になし

Q55 サイバーセキュリティ事業者への投資

外国投資家が、サイバーセキュリティに関する事業を営む日本の上場会社の議決権を取得することについて何らかの法令上の制限があるのか。

タグ：外国為替及び外国貿易法、国家安全保障、対内直接投資、コア業種、CFIUS、FIRRMA

１．概要

近時、サイバー攻撃が、国民の安全・安心、国家や民主主義の根幹を揺るがすような重大な事態を生じさせ、国家安全保障上の課題へと発展していくリスクは増大しており、サイバーセキュリティの強化は、安全保障等の観点から不可欠となっている。外国投資家が、サイバーセキュリティに関する事業を営む日本の上場会社の議決権を取得することについては、外為法により、一定の場合に事前届出並びに財務大臣及び事業所管大臣による審査を経る必要がある。

諸外国においても、国家安全保障を目的とする対内直接投資の規制強化がなされており、例えば、日本から米国内のサイバーセキュリティに関する事業を営む企業への投資については、対米外国投資委員会（CFIUS）による審査の対象となる場合もあると考えられる。

２．解説

（１）安全保障等の観点におけるサイバーセキュリティの重要性

サイバー空間が社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となり、サイバー空間と実空間の一体化が進展している一方で、重要インフラの機能停止、国民情報や知的財産の窃取、民主プロセスへの干渉など国家の関与が疑われるものをはじめとする組織化・洗練化されたサイバー攻撃の脅威が増大しており、サイバー攻撃が、国民の安全・安心、国家や民主主義の根幹を揺るがすような重大な事態を生じさせ、国家安全保障上の課題へと発展していくリスクも増大している。こうしたリスクに対処するため、サイバーセキュリティの強化は、安全保障等の観点から不可欠となっている。

平成 25 年 12 月に閣議決定された「国家安全保障戦略」[1]において、我が国がとるべき国家安全保障上の戦略的アプローチの 1 つとして、サイバーセキュリティの強化が挙げ

[1] 令和 4 年 12 月 16 日付国家安全保障会議決定及び閣議決定（以下、本項において「令和 4 年決定という。」（https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf）により平成 25 年 12 月 17 日付国家安全保障会議決定及び閣議決定は廃止されたものの、令和 4 年決定においても引き続きサイバーセキュリティの強化については言及されている（令和 4 年決定Ⅵ2(4)ア等）。

られており、令和 3 年 9 月に閣議決定された「サイバーセキュリティ戦略」[2]においても、サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、サイバー攻撃に対する防御力等の向上等を一層強化するとされている。

（２）外国から日本への投資に対する規制

外国投資家[3]が、サイバーセキュリティに関する事業を営む日本の上場会社の議決権を取得することについては、外国為替及び外国貿易法（以下、本項において「外為法」という。）により一定の規制がなされている。

ア　外為法に基づく対内投資に関する規制の概要

外為法は、「外国為替、外国貿易その他の対外取引が自由に行われることを基本とし、対外取引に対し必要最小限の管理又は調整を行うことにより、対外取引の正常な発展並びに我が国又は国際社会の平和及び安全の維持を期し、もって国際収支の均衡及び通貨の安定を図るとともに我が国経済の健全な発展に寄与することを目的と」し（同法第 1 条）、外国為替、外国貿易その他の対外取引を総合的に対象としている法律であり、日本の対外取引の基本法となっている。同法による規制の 1 つに、対内直接投資規制がある。すなわち、同法は、対外取引の原則自由という基本的考え方に立ちつつ、経済協力開発機構（OECD）の資本移動自由化コード等の国際的な投資ルールの範囲内で、国の安全等の観点から対内直接投資規制を導入している。

具体的には、①外国投資家が行う国内の会社の株式又は議決権の取得等のうち一定の要件を満たすもの[4]を「対内直接投資等」（外為法第 26 条第 2 項、対内直接投資等に関する政令（昭和 55 年政令第 261 号）第 2 条第 16 項第 1 号～第 7 号）として原則として事後報告を義務付ける（同法第 55 条の 5 第 1 項）。特に、②「国の安全」、「公の秩序」、「公衆の安全」、「我が国経済の円滑な運営」の観点から、一部の指定業種に係る対内直接投資等に限定して、事前届出並びに財務大臣及び事業所管大臣による審査を要求している（同法第 27 条第 1 項、同令第 3 条第 2 項）[5]。

イ　サイバーセキュリティ業に係る対内直接投資等に関する規制

以下に述べるとおり、サイバーセキュリティに関する事業は、令和元年 5 月に指定業種に追加されたため、②の規制の対象となった（下記（ア）参照）。なお、同年 11 月の同法改正では、事前届出免除制度（同法第 27 条の 2）が新設されたものの、サイバーセ

---

[2] https://www.cyber.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf
[3] 外国投資家については、外為法第 26 条において定義されている。
[4] 上場企業の株式の 1%（下記イ（イ）のとおり、従前は 10%であったが、令和元年外為法改正により、1%に引き下げられた。）以上を取得する場合や、非上場企業の株式取得を取得する場合等が含まれる。
[5] なお、②の要件を満たし事前届出及び審査が要求される「対内直接投資等」については、①の事後報告は免除される（外為法第 55 条の 5 第 1 項但書）。

キュリティに関する事業の一部は、この免除制度が利用できないコア業種となっているため、この免除制度のメリットを享受することはできない（下記（イ）参照）。

そのため、外国投資家が、サイバーセキュリティに関する事業を営む日本の上場会社の議決権を取得する場合、それが「対内直接投資」の要件を満たせば、原則として事前届出並びに財務大臣及び事業所管大臣による審査を経る必要がある。

（ア）サイバーセキュリティ業の指定業種への追加

サイバーセキュリティの確保の重要性等を踏まえ、安全保障上の重要な技術の流出や、日本の防衛生産・技術基盤の毀損等、日本の安全保障に重大な影響を及ぼす事態を生じることを適切に防止する観点から、指定業種には、情報処理関連機器等の製造業やソフトウェア開発業、IT 関連サービス業等のサイバーセキュリティに関する事業が含まれている。

（イ）令和元年外為法改正によるサイバーセキュリティ業のコア業種への指定

近時、投資を通じた機微技術へのアクセスに対する関心の高まり等を背景に[6]、諸外国において、国家安全保障を目的とする対内直接投資の規制強化がなされている[7]。このような状況を踏まえ、経済の健全な発展につながる対内直接投資を一層促進するとともに、国の安全等を損なうおそれがある投資に適切に対応することにより、メリハリのある対内直接投資制度を目指す観点から、令和元年 11 月に外為法が改正され、事前届出免除制度の導入（同法第 27 条の 2、第 28 条の 2）、上場会社等の株式取得等の閾値の 10%から 1%への引下げ（同法第 26 条第 2 項第 3 号、同項第 4 号）等が行われた。

事前届出免除制度については、国家の安全等の観点から、原則として免除制度を利用できない業種（＝コア業種）が指定されており（対内直接投資等に関する命令（昭和 55 年総理府・大蔵省・文部省・厚生省・農林水産省・通商産業省・運輸省・郵政省・労働省・建設省令第 1 号）第 3 条の 2 第 3 項、対内直接投資等に関する命令第 3 条の 2 第 3 項の規定に基づき、財務大臣及び事業所管大臣が定める業種を定める

---

[6] 平成 31 年 3 月に OECD が公表したレポート（Acquisition-and ownership-related policies to safeguard essential security interest）においては、安全保障上の利益を保護するため、会社の資産買収を管理する伝統的な領域から、投資を通じた会社への影響力の行使（技術やデータへのアクセス等）を管理する領域へと、投資管理の対象範囲が拡大していることが指摘されており、この中では、対内直接投資に関する新たな懸念領域として、①重要インフラ（鉄道、水道、電力等）の支配に対する懸念の増大、②デジタル化の進展による個人情報の安全保障上重要な資産への変容、③先進技術へのアクセスの増加、④サイバーセキュリティに関する懸念の増大、⑤サプライチェーン上の重要企業に対する支配の増大が挙げられている。

[7] 例えば、米国では、対米外国投資委員会（The Committee on Foreign Investment in the United States）の権限を拡大する外国投資リスク審査現代化法（the Foreign Investment Risk Review Modernization Act）が 2018 年 8 月に成立し、EU では、2019 年 3 月に、欧州議会・理事会規則（Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union）によって、加盟国間及び欧州委員会の間の情報交換を含む対内直接投資審査に関する枠組みが新たに制定された。

件[8])、サイバーセキュリティ業のうち、重要インフラのために特に設計されたプログラム等の提供に係るサービス業等が、コア業種に指定されている[9]。

（３）日本から米国への投資に対する規制

米国では、日本を含む米国外から米国内への投資を、国家安全保障の確保の観点から審査する対米外国投資委員会（CFIUS[10]）の権限を、審査対象となる取引の拡充[11]、一部取引に対する事前申告の義務付け[12]等により拡大する外国投資リスク審査現代化法（FIRRMA[13]）が、2018 年 8 月に成立し、2020 年 2 月から施行されている。

FIRRMA は、CFIUS の審査における考慮要素の 1 つとして「サイバーセキュリティへの影響」を挙げており（FIRRMA1702(c)）、例えば、日本企業が、サイバーセキュリティに関する事業を営む米国企業を特定懸念国[14]に売却する場合等には、CFIUS による承認が得られず売却等を断念せざるを得ないケースも生じ得ると考えられる。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

---

[8] https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/publicnotice_core.pdf

[9] 令和元年外為法改正にあわせて指定業種の見直しが行われ、コア業種に該当せず、かつ、①自らが営む指定業種に該当しない事業に付随してソフトウェア業、情報処理サービス業若しくはインターネット利用サポート業を行う場合又は②指定業種に該当しない業種を営むグループ会社のためにソフトウェア業、情報処理サービス業若しくはインターネット利用サポート業を行う場合が、指定業種の対象から除外され、事前届出が不要とされている。詳細については、日本銀行国際局国際収支課外為法手続グループ「外為法 Q&A（対内直接投資・特定取得編）」（令和 7 年 5 月改定）（https://www.boj.or.jp/about/services/tame/faq/data/tn-qa.pdf）Q78 を参照されたい。

[10] The Committee on Foreign Investment in the United States

[11] 従前は、外国人が米国事業の支配を獲得することになる投資のみが審査対象となる取引であったが、重要技術・重要インフラ・機微個人データに関する米国事業に対する投資のうち一定のものについて、(非支配的な投資であっても) 審査対象となる取引に含まれることとなった。

[12] 外国政府による相当程度の影響力がある者（国有企業等）による、重要インフラ・重要技術・機微個人データに関する米国事業に対する投資のうち一定のものが、事前申告の対象となっている。

[13] the Foreign Investment Risk Review Modernization Act

[14] FIRRMA1702(c)は、「重要な技術・重要インフラの獲得を戦略的な目標として掲げる特定懸念国による投資」も考慮要素として挙げているが、「特定懸念国」が具体的にどの国を想定しているのかは明らかにされていない。

Q56 経済安全保障（経済安保推進法、セキュリティ・クリアランス）

経済安全保障推進法に基づき、基幹インフラ事業者にはどのようなサイバーセキュリティへの対策が求められているか。日本のセキュリティ・クリアランス制度（特定秘密保護法及び重要経済安保情報保護活用法）はどのような仕組みとなっているか。

タグ：経済安全保障推進法、基幹インフラ、セキュリティ・クリアランス、特定秘密保護法、重要経済安保情報保護活用法

１．概要

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号。以下、本項において「経済安全保障推進法」という。）は、安全保障の確保に関する経済施策を総合的かつ効果的に推進するために創設された法であるが、特に、基幹インフラ事業者に対するサイバーセキュリティの確保に関連する制度が設けられている。

セキュリティ・クリアランス制度とは、一般に、政府等が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者に対し、その者がそれらの情報を漏らすおそれがないかを調査・確認した上でアクセスを認める制度をいう。日本のセキュリティ・クリアランス制度を構成する法律として、まず、特定秘密の保護に関する法律（平成 25 年法律第 108 号。以下、本項において「特定秘密保護法」という。）がある。特定秘密保護法は、日本の安全保障に関する情報のうち特に秘匿することが必要であるものを保護するための法律であるが、これに加えて、重要な経済基盤に関する情報を適切に保護し、活用することを目的として、重要経済安保情報の保護及び活用に関する法律（令和 6 年法律第 27 号。以下、本項において「重要経済安保情報保護活用法」という。）が制定された。

２．解説

（１）経済安全保障推進法

ア　経済安全保障推進法の概要

経済安全保障推進法は、国際情勢の複雑化や社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることから、安全保障の確保に関する経済施策を総合的かつ効果的に推進するために創設された法である。

経済安全保障推進法は、①重要物資の安定的な供給の確保に関する制度、②基幹インフラ役務の安定的な提供の確保に関する制度、③先端的な重要技術の開発支援に関する制度、④特許出願の非公開に関する制度の 4 つの制度から構成される[1] [2]。

① 「重要物資の安定的な供給の確保に関する制度」は、国民の生存に必要不可欠な又は広く国民生活・経済活動が依拠している重要な物資を「特定重要物資」として指定し、その安定供給確保に取り組む民間事業者等を支援することを通じて、特定重要物資のサプライチェーンの強靭化を図る制度である。

② 「基幹インフラ役務の安定的な提供の確保に関する制度」は、基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、国が基幹インフラ事業を定め、一定の基準に該当する事業者を指定し、国が定めた重要設備の導入・維持管理等の委託をしようとする際に、事前に届出を行い、審査を受ける制度である。

③ 「先端的な重要技術の開発支援に関する制度」は、将来の国民生活・経済活動の維持にとって重要なものとなり得る先端的な技術のうち、その技術が外部に不当に利用された場合において国家・国民の安全を損なう事態を生ずるおそれがあるものなどを「特定重要技術」と定義し、これらの技術に関し、特定重要技術の研究開発の促進とその成果の適切な活用を図る制度である。

④ 「特許出願の非公開に関する制度」は、特許出願の明細書等に、公にすることにより外部から行われる行為によって国家及び国民の安全を損なう事態を生ずるおそれが大きい発明が記載されていた場合には、「保全指定」という手続により特許手続を留保するとともに、その間、公開を含む発明の内容の開示全般やそれと同様の結果を招くおそれのある発明の実施を原則として禁止し、かつ、特許出願の取下げによる離脱も禁止する制度である。

上記の 4 つの制度のうち、サイバーセキュリティとの関係で特に重要となるのは、②基幹インフラ役務の安定的な提供の確保に関する制度（以下、本項において「基幹インフラ制度」という。）である。

---

[1] 経済安全保障上の観点から、技術流出やサプライチェーンリスクへの対策に取り組む企業等の実例を紹介するものとして経済産業省貿易経済安全保障局技術調査・流出対策室「経済安全保障上の課題への対応 （民間ベストプラクティス集） —第 2.0 版—」（https://www.meti.go.jp/policy/economy/economic_security/best_practice2.0.pdf）も参照されたい。

[2] 令和 8 年 1 月 23 日、経済産業省は、企業が経済安全保障対応を進めていく中で、経済安全保障上のリスクに起因する損失を中長期的に抑え、企業価値の維持・向上も見据えた経営戦略を考える上の推奨事項として、「経済安全保障経営ガイドライン（第 1 版）」を取りまとめ、公表した（https://www.meti.go.jp/press/2025/01/20260123004/20260123004.html）。サイバーセキュリティとの関係では、同ガイドラインは、「自律性確保の取組」の観点から、「サイバー攻撃等によりネットワークが遮断されることで、IT・ソフトウェア産業におけるサプライチェーンの混乱に繋がる事態も発生していることにも留意が必要である。」といった点や、サプライチェーン構築に関して「コスト最適化だけでなく、製品・サービスの供給安定性やセキュリティの堅牢性等も重要であることを認識」すべきといった点を指摘している（9～10 頁）。

イ　基幹インフラ制度とサイバーセキュリティ

（ア）基幹インフラ制度の概要

基幹インフラ制度は、基幹的なインフラサービスが安定的に提供されることを確保するため、基幹的なインフラ事業を行う事業者（特定社会基盤事業者）を指定し、特定社会基盤事業者が、特定重要設備の導入又は重要維持管理等の委託をしようとする際には、事前に国（事業所管大臣）に届出を行い、審査を受けなければならないこととした[3]。

（イ）特定社会基盤事業者

基幹的なインフラ事業（特定社会基盤事業）として、電気・ガス・石油・水道・鉄道・貨物自動車運送・外航貨物・港湾運送・航空・空港・電気通信・放送・郵便・金融・クレジットカードの 15 業種が挙げられている（経済安全保障推進法第 50 条第 1 項各号）。

これらの種類の事業のうち、特定社会基盤役務（国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの）の提供を行うものとして、経済安全保障推進法施行令（令和 4 年政令第 394 号）で定めるものが、特定社会基盤事業にあたる。電気事業であれば、一般送配電事業・送電事業・配電事業・発電事業・特定卸供給事業が特定社会基盤事業に該当する[4]。

特定社会基盤事業を行う事業者のうち、事業ごとに事業所管大臣が主務省令で定める基準に該当する者が特定社会基盤事業者として個別に指定される（経済安全保障推進法 50 条 1 項）[5]。

（ウ）特定重要設備の導入・重要維持管理等の委託

特定社会基盤事業者が「特定重要設備」の導入又は「重要維持管理等」の委託をしようとする際に事前審査を要する（経済安全保障推進法第 52 条第 1 項）。

「特定重要設備」とは、特定社会基盤事業の用に供される設備、機器、装置又はプログラムのうち、特定社会基盤役務を安定的に提供するために重要であり、かつ、わが国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして主務省令で定めるものをいう。具体例とし

[3] 基幹インフラと混同しやすいものとして、重要インフラ（重要社会基盤事業者）がある。重要インフラについては、Q2 及び Q45 を参照されたい。
[4] 経済安全保障推進法施行令第 9 条第 1 号。
[5] 特定社会基盤事業者として指定された事業者は、基幹インフラ制度に関するウェブサイト（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html）で確認できる。令和 7 年 7 月 31 日時点で計 245 社が特定社会基盤事業者として指定されている。

て、一般送電事業における特定重要設備については、中央給電指令所における需給制御システムや系統制御所における系統制御システムが該当するとされている[6]。

そして「重要維持管理等」とは、他の事業者に委託して特定重要設備の維持管理若しくは操作を行うもののうち[7]、当該特定重要設備の機能を維持するため又は当該特定重要設備に係る特定社会基盤役務を安定的に提供するために重要であり、かつ、これらを通じて当該特定重要設備が我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして主務省令で定めるものをいう。具体例として、一般送電事業における特定重要設備の重要維持管理等には、需給制御システムにおける需給演算サーバ又は監視制御サーバの大部分を交換する行為等が該当するとされている[8]。

（エ）届出・審査の概要

特定社会基盤事業者は、①特定重要設備の導入を行う場合、又は、②他の事業者に委託して特定重要設備の重要維持管理等を行わせる場合に、主務大臣に対し、あらかじめ法定の事項を記載した計画書（導入等計画書）を届け出なければならない。導入等計画書には、①特定重要設備の導入に関しては特定重要設備の供給者はもちろん、「構成設備」の供給者まで、②特定重要設備の重要維持管理等の委託に関しては、重要維持管理等の委託先全てに関する情報の届出が必要である。「構成設備」とは、特定重要設備の一部を構成する設備、機器、装置又はプログラムのうち、特定妨害行為[9]の手段として使用されるおそれがあるものとして主務省令で定めるものをいう。

なお、構成設備が ISMAP（なお、ISMAP については、Q42 を参照されたい。）の登録を受けているクラウドサービスである場合は、一部の記載を省略することができる。重要維持管理等の再委託先についても例外的に、一定の要件を満たすこと及び

---

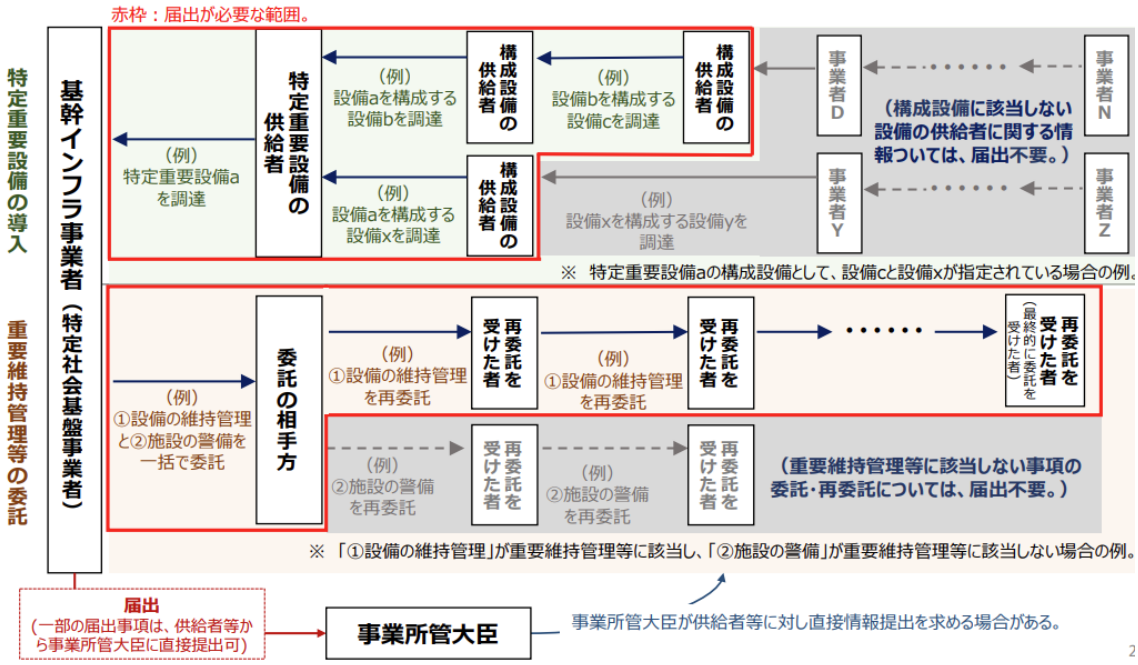
6 経済産業省「電気事業における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」（https://www.meti.go.jp/policy/economy/economic_security/denki.pdf）

7 「維持管理」とは、特定重要設備の機能を維持する（特定重要設備の機能を正常な状態に保つ）ため、その保守点検、機器の修理・部品の交換、プログラムの変更を行うこと等を指し、「操作」とは、特定重要設備を運用し、制御する操作を行うこと等を指す（「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」Q12）。

8 前掲注 6 参照。

9 「特定妨害行為」とは、特定重要設備の導入又は重要維持管理等の委託に関して我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為をいう（経済安全保障推進法第 52 条第 2 項第 2 号ハ）。例えば、供給者又は委託を受けた者から特定重要設備の脆弱性に関する情報を入手し、その情報を用いて特定重要設備をウイルスに感染させ、機能を停止・低下させる行為や脆弱性に関する情報を用いて特定重要設備に不正にアクセスして操作を行うことや、情報の滅失・改ざん等を通じて、特定社会基盤事業者が本来意図した動作とは異なる動作をさせる行為等が該当するとされている（「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」Q2）。

それを証する書類を添付することにより、一部事項の省略が可能である。図式化すると、以下のとおりとなる[10]。



また、導入等計画書には、特定妨害行為を防止するための措置（リスク管理措置）についても記載しなければならない。これらのリスク管理措置は、供給者の支配関係・製造過程の改ざん防止・重要維持管理の代替手当・再委託の統制・外国法的環境の影響確認といった事項を対象に、設備の導入から維持管理まで全体を統制するものであるため、サプライチェーン・リスク対策の一環と評価できる。

特定重要設備の導入や、特定重要設備の重要維持管理等の委託について、特定重要設備が特定妨害行為の手段として使用されるおそれを低減させるためには、特定社会基盤事業者が自らリスクを評価し、そのリスクの内容及び程度に応じて適切にリスク管理措置を講ずることが有効である（全ての項目を常に実施することを求めるものではない。）。導入等計画書においては、様式にしたがい、実施したリスク管理措置の項目にチェックを付して届け出る必要がある。

原則として、導入計画書の審査期間は 30 日間であり、審査期間中は導入等や重要維持管理等の委託を行ってはならないこととされている（経済安全保障推進法第 52 条第 3 項）。もっとも、「緊急やむを得ない場合」には、導入計画書の事前届出を行う

10 内閣府 政策統括官（経済安全保障担当）「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について（令和 7 年 8 月 1 日時点）」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf）

ことなく、特定重要設備の導入や重要維持管理等の委託を行うことが許容されている（経済安全保障推進法第 52 条第 1 項但書）[11]。

（オ）罰則

基幹インフラ制度に関する罰則は、事業者が特定重要設備の導入や重要維持管理等の委託を行う際の事前届出義務の違反、審査中の待機違反、勧告不受諾に続く命令違反、及び導入後等の報告義務違反を定め、いずれも 2 年以下の拘禁刑又は 100 万円以下の罰金（併科可）を科すこととなっている（経済安全保障推進法第 92 条第 1 項第 1 号乃至第 5 号）。また、両罰規定も定められており、法人の代表者・代理人・使用人その他の従業者が法人の業務に関して第 92 条第 1 項各号の違反行為をしたときは、行為者の処罰に加えて当該法人にも各本条の罰金刑を科すと規定している（経済安全保障推進法第 97 条）。

（2）セキュリティ・クリアランス制度

ア　特定秘密保護法と重要経済安保情報保護活用法の相違

日本のセキュリティ・クリアランス制度を構成する法律として、特定秘密保護法と重要経済安保情報保護活用法が定められている。両法は、適性評価において、安全保障上重要な情報を漏らすおそれがないと認められた者でなければ、政府等が保有する安全保障上重要な情報として指定された情報にアクセスできないという点で共通している。また、両法ともに指定された情報を取り扱う者が過失により漏えいした場合であっても処罰の対象となり得ることが特徴的である。

特定秘密保護法において、「特定秘密」として指定の対象となり得るのは、①防衛、②外交、③特定有害活動（スパイ行為等）の防止、④テロリズムの防止の 4 分野の情報に限定されている。しかし、安全保障の概念が防衛や外交といった伝統的な領域から経済・技術分野に拡大する中、経済安全保障分野における情報保全強化の必要性が生じ、重要経済安保情報保護活用法が制定されることとなった。このように重要なインフラや重要な物資のサプライチェーンに関する一定の情報についても「重要経済安保情報」として指定し、保護の対象とすることで、より経済安全保障に資するものとなっている。

特定秘密保護法と重要経済安保情報保護活用法の主な相違は以下のとおりである。

情報の秘匿度：特定秘密保護法においては「安全保障に著しい支障を与えるおそれ」がある情報を指定することと定められているが、重要経済安保情報保護活用法においては、「安全保障に支障を与えるおそれ」と定められ、保護すべき情報の秘匿度に差がある。

[11] 特定重要設備の導入等を行うことが緊急やむを得ない場合として導入等計画書を事前届出することなく導入等を行うこととした場合には、遅滞なく緊急導入等届出書を提出する必要がある。

適性評価の調査の実施機関：特定秘密保護法においては、適性評価は調査も含めて各行政機関の長が実施するのに対し、重要経済安保情報保護活用法においては、適性評価の調査は内閣府により一元的に行われる。

・民間事業者への提供：特定秘密保護法において、民間事業者に特定秘密を保有させ、又は提供することができるのは、当該事業者に保有又は提供しなければ、当該行政機関の所掌事務の遂行が立ちゆかないような、いわば非代替性が認められる場合に限定しているのに対し、重要経済安保情報保護活用法においては、重要経済安保情報の活用という法の趣旨を踏まえ、民間事業者への提供範囲をより具体的かつ広く定めている。

・罰則：特定秘密の取扱いの業務を行う者がこれを漏えいした場合、10 年以下の拘禁刑若しくは 1000 万円以下の罰金又はこれを併科であるのに対して、重要経済安保情報の取扱いの業務を行うものがこれを漏えいした場合、5 年以下の拘禁刑若しくは 500 万円以下の罰金又はこれを併科となっている。重要経済安保情報保護活用法においては法人の両罰規定も定められている。

イ　重要経済安保情報保護活用法の制度概要

（ア）重要経済安保情報の指定

行政機関の所掌事務に係る①重要経済基盤保護情報[12]であって、②公になっていないもののうち、③その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを、重要経済安保情報として指定する（重要経済安保情報保護活用法第 3 条第 1 項）。重要経済安保情報の具体例としては、重要なインフラ事業者の活用を妨げるようなサイバー攻撃が実施された場合を想定した政府の対応案の詳細に関する情報や重要物資の安定供給の障害となるサプライチェーンの脆弱性に関する情報、日本政府と外国政府で実施する安全保障に関わる革新的な技術の国際共同研究開発において外国政府から提供された情報といった情報が挙げられる。

重要経済安保情報に指定される情報とは、行政機関が保有する情報であることが前提であるが、事業者等から提供された情報であっても、上記①乃至③の要件に該当するものであれば、重要経済安保情報に指定されることもある。ただし、要件該当性

[12] 「重要経済基盤保護情報」とは、重要経済基盤（我が国の国民生活又は経済活動の基盤となる公共的な役務であってその安定的な提供に支障が生じた場合に我が国及び国民の安全を損なう事態を生ずるおそれがあるものの提供体制並びに国民の生存に必要不可欠な又は広く我が国の国民生活若しくは経済活動が依拠し、若しくは依拠することが見込まれる重要な物資（プログラムを含む。）の供給網をいう。）に関する情報であって次に掲げる事項に関するものをいう（重要経済安保情報保護活用法第 2 条第 3 項及び第 4 項）。
① 外部から行われる行為から重要経済基盤を保護するための措置又はこれに関する計画若しくは研究
② 重要経済基盤の脆弱性、重要経済基盤に関する革新的な技術その他の重要経済基盤に関する重要な情報であって安全保障に関するもの
③ ①の措置に関し収集した外国の政府又は国際機関からの情報
④ ②③に掲げる情報の収集整理又はその能力

の判断に当たっては、特に、②の非公知性と③の秘匿の必要性の該当性との関係において留意が必要とされる。事業者等から提供された情報を単に重要経済安保情報に指定するだけでは、当該情報を提供した事業者等には法の規定は及ばず、当該事業者等は適性評価を受けずとも引き続き当該情報を扱うことが可能で、漏えいに対して罰則が及ぶこともないからである[13]。

（イ）適合事業者に対する重要経済安保情報の提供

行政機関の長は、適合事業者に重要経済安保情報を利用させる必要があると認めたときは、当該適合事業者との契約に基づき、当該適合事業者に当該重要経済安保情報を提供することができる（重要経済安保情報保護活用法第 10 条第 1 項）。「適合事業者」とは、我が国の安全保障の確保に資する活動を行う事業者であって重要経済安保情報の保護のために必要な施設設備を設置していること等の政令で定める基準に適合する事業者である。

また、行政機関の長は、適合事業者の同意を得て当該事業者に調査・研究等の活動を行わせる場合において、当該活動により重要経済安保情報の要件に該当する情報が生成されることが見込まれる場合には、あらかじめ当該情報を重要経済安保情報として指定し、当該事業者との契約に基づき、当該情報を重要経済安保情報として保有させることができる（同条第 2 項）。

適合事業者は、事業者からの申請に基づき、事業者が定める規程に従って重要経済安保情報を保護するために必要な措置を講じていることを中心に、事業者の意思決定に関して外国の影響がないか等の考慮要素を含めて、審査の上認定される。詳細は、「重要経済安保情報保護活用法の運用基準」[14]や「重要経済安保情報保護活用法の運用に関するガイドライン　（適合事業者編）」[15]を参照されたい。

（ウ）重要経済安保情報の取扱者の制限

重要経済安保情報の取扱者は、当該業務を行わせる行政機関の長が実施した適性評価（10 年以内に受けたもの）において重要経済安保情報を「漏らすおそれがない」と認められた者に限定されている（重要経済安保情報保護活用法第 11 条）。

重要経済安保情報保護活用法における適性評価は、特定秘密保護法における適性評価と同様、評価対象者の同意を前提として実施され、その調査内容は、①重要経済基盤毀損活動との関係、②犯罪及び懲戒の経歴、③情報の取扱いに係る非違の経歴、④薬物の濫用及び影響、⑤精神疾患、⑥飲酒についての節度、⑦信用状態その他の経済的な状況の 7 事項であり（重要経済安保情報保護活用法第 12 条第 2 項）、これ以外の事項の調査は禁止されている。さらに、評価対象者本人に対する質問だけではな

---

13 内閣府「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準」（https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/kijun.pdf）

14 前掲注 13 参照。

15 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/jigyousyagl.pdf

く、国及び地方の行政機関、信用情報機関、医療機関その他の公務所又は公私の団体への質問・照会も行われることがある。

（エ）罰則

重要経済安保情報保護活用法に関する主な罰則は、以下のとおりである。

行為類型	行為の内容	法定刑	未遂	過失犯	関連条文
① 取扱者による漏えい	「取扱いの業務に従事する者」が業務により知り得た重要経済安保情報を漏らすこと（取扱業務終了後の漏えいも含む）	5 年以下の拘禁刑又は 500 万円以下の罰金（併科可）	処罰あり	1 年以下の拘禁刑又は 30 万円以下の罰金	第 23 条第 1 項、第 3 項、第 4 項
② 提供・提示先での二次漏えい	公益上の必要等により提供・提示された情報を知り得た者の漏えい	3 年以下の拘禁刑又は 300 万円以下の罰金（併科可）	処罰あり	6 か月以下の拘禁刑又は20 万円以下の罰金	第 23 条第 2 項、第 3 項、第 5 項
③ 不正取得	外国利益の図利等の目的で、暴行・脅迫・詐欺・窃取・侵入・通信傍受・不正アクセス等により重要経済安保情報を取得すること	5 年以下の拘禁刑又は 500 万円以下の罰金（併科可）	処罰あり	―	第 24 条第 1 項、第 2 項

上記の罰則の対象となる行為の遂行に係る共謀、教唆、又は煽動は独立に処罰される（同法第 25 条）。これらの各罪は国外で行われた場合でも成立する旨の国外犯規定が置かれ（同法第 27 条）、過失犯を除き両罰規定が適用されるため、行為者に加えて法人等にも各罰則規定の罰金刑が及ぶ（同法第 28 条）。

3．参考資料（法令・ガイドラインなど）

・経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律施行令
・特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針
・経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説

・重要経済安保情報の保護及び活用に関する法律施行令
・重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準
・重要経済安保情報保護活用法の運用に関するガイドライン（行政機関編）
・重要経済安保情報保護活用法の運用に関するガイドライン（適合事業者編）
・適性評価に関する Q&A

４．裁判例

特になし

Q57 サイバーセキュリティインシデント発生時の当局等対応

企業が保有するデータの漏えいをはじめとするサイバーセキュリティインシデントにあった場合に法的義務又はそれに準じるものとして必要な対応は何か。また、必ずしも法的義務ではないが、対応したほうがよい事項としてどのようなものがあるか。

タグ：個情法、番号利用法、電気通信事業法、金融商品取引法、銀行法施行規則、漏えい等、報告義務、有価証券上場規程、認定個人情報保護団体、プライバシーマーク、不正競争防止法、刑事訴訟法、営業秘密、限定提供データ

１．概要

データの漏えいをはじめとするサイバーセキュリティインシデントが発生した場合には、法的義務又はそれに準じて対応が必要な事項（下記 2.（1））と、その他対応を検討すべき事項（下記 2.（2））の 2 種類の検討が必要になる。

前者の法的義務又はそれに準じて対応が必要な事項としては、一定の条件を満たす個人データの漏えい、滅失、毀損（以下、本項において「漏えい等」という。）があれば、個人情報取扱事業者は、個情法第 26 条に基づき、個人情報保護委員会への報告をしなければならず、また、本人に対して、当該事態が生じた旨を通知しなければならない（下記 2.（1）ア）[1, 2]。

さらに海外法令が適用される場合には、適用される海外法令に基づき、当局対応等が求められることがあり得る点にも留意が必要である[3]。

---

[1] 令和 4 年 3 月 31 日以前は、告示に基づく努力義務又は望ましい措置とされていたが、個情法改正により令和 4 年 4 月 1 日以降、法的な義務となった。

[2] なお、民間事業者だけではなく、行政機関の長等（行政機関の長、地方公共団体の機関、独立行政法人等及び地方独立行政法人をいう（個情法第 63 条括弧書）。）も、個人情報保護委員会への報告、本人への通知義務が課されている（同第 68 条）。
ただし、個情法別表第二に記載されている法人（個情法第 2 条第 11 項第 3 号括弧書において「独立行政法人等」から除かれている。）や、地方独立行政法人で試験研究を主たる目的とするもの又は大学等の設置及び管理及び病院事業の経営を目的とするもの（個情法第 58 条第 1 項第 2 号。これらは個情法第 2 条第 11 項第 4 号括弧書において「地方独立行政法人」の定義から除かれている。）は、個人情報取扱事業者に該当することになる（「独立行政法人等」「地方独立行政法人」から除かれる結果、個情法第 16 条第 2 項柱書きにより個人情報取扱事業者に該当する。）ため、個人データの漏えい等の個人情報保護委員会への報告・本人への通知については、個情法第 26 条が適用されることになる。また、地方公共団体の機関が、病院、診療所、大学の運営の業務を行う場合（個情法第 58 条第 2 項第 1 号）、独立行政法人労働者健康安全機構が、病院の運営を行う場合（個情法第 58 条第 2 項第 2 号）、これらの業務における個人データの漏えい等の個人情報保護委員会への報告・本人への通知については、個情法第 58 条第 2 項柱書きのみなし規定により、個情法第 26 条が適用されることになっている。このように、適用関係には留意する必要がある（詳しくは、Q16 参照）。

[3] 経済産業省が令和 2 年 12 月に公開した「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」においても、ランサムウェア攻撃が行われた場合の対応策として、「警察、個人情

また、各重要インフラ分野においては、各々に適用される業法に基づき、サイバーセキュリティインシデント発生時の事故報告が求められることがある（下記 2.（1）イ、ウ）。

このほか、有価証券上場規程第 402 条等に基づく適時開示、金融商品取引法第 24 条の 5 第 4 項に基づき臨時報告書の提出が必要となる場合もある（下記 2.（1）エ。詳細は Q8 参照）。

後者のその他対応を検討すべき事項としては、実際に発生した事案に応じ、犯罪が成立し得る事案であれば警察等への相談等（下記 2.（2）ア）、不正アクセス等の技術的な問題のある事案であればセキュリティ機関に対する相談や対応依頼、各種ガイドラインに基づく届出等があり得る（下記 2.（2）イ）。

その他、漏えいした情報が法的に保護される営業秘密や限定提供データ、インサイダー情報であれば、警察への被害届の提出のほか、差止請求や損害賠償請求、開示を検討すべきである（下記 2.（2）ウ、エ）。

２．解説

（１）法的義務又はそれに準じるものとして必要な対応

ア　個人データの漏えい等に関して必要となる対応

（ア）個情法に基づく個人データ漏えい等の対応（第 26 条）

概要を述べると、個人データの漏えい等又はそのおそれのある事案（以下、本項において「漏えい等事案」という。）が発生した場合、被害拡大防止、事実関係調査等の一定の対応が必要であり、個人の権利利益を害するおそれが大きい事態（以下、本項において「報告対象事態」という。）が発生した場合は個人情報保護委員会への報告、本人への通知が必要となる。以下、詳述する。

まず、漏えい等事案について述べると、個人データの「漏えい」とは、個人データが外部に流出することをいい、例えば社内の別の部署への誤送信は漏えいにあたらない。次に、「滅失」とは、個人データの内容が失われることをいい、個人データが格納された記録媒体の紛失などがこれに当たる（コピーがある場合は該当しない。）。「毀損」とは、個人データの内容が意図せず変更されたり利用不能になったりすることをいい、例えばランサムウェアによる暗号化がこれに当たる（バックアップからデータを復元できる場合は該当しない。）。

報保護委員会、所管省庁等への報告・届出の実施。特に報告義務のある事案については、正確かつ迅速な報告が求められる。」「事業形態や漏えいしたデータによっては、欧州の GDPR や米国のカリフォルニア州消費者プライバシー法（CCPA）など海外の法制度の報告対象になる場合があることにも留意すること。」と述べられている（11 頁参照）。

漏えい等事案が発生した場合、その内容に応じて、個情法ガイドライン（通則編）上、以下の措置を講じなければならないとされている[4] [5]。

①事業者内部における報告及び被害の拡大防止
責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。
②事実関係の調査及び原因の究明
漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。
③影響範囲の特定
上記②で把握した事実関係による影響の範囲を特定する。
④再発防止策の検討及び実施
上記②の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を速やかに講ずる。

次に、報告対象事態について述べると、個情法第 26 条及び個情法施行規則第 7 条では、次のケースが報告対象事態にあたるとされている。

①要配慮個人情報が含まれる個人データ[6]の漏えい等
②不正利用により財産的被害が発生するおそれがある個人データの漏えい等（クレジットカード番号など）
③不正の目的をもって行われたおそれがある個人データの漏えい等（サイバー攻撃や従業員による情報持ち出し、フィッシング詐欺[7]により個人データの漏えいが生じた場合等）
④1,000 人を超える個人データの漏えい等
⑤①～④の「おそれ」

[4] 個情法ガイドライン（通則編）3-5-2。なお、これらは、令和 4 年 3 月 31 日以前は、「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」（以下、本項において「旧漏えい等告示」という。）に基づき、望ましい措置とされていた。

[5] また、①～④の措置に加えて、「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましい。」とされている（個情法ガイドライン（通則編）3-5-2(5)）。

[6] 高度な暗号化その他の個人の権利利益を保護するために必要な措置が講じられているものを除く。②～④について同じ。なお、「個人データ」の意義については、個情法 QA6-1 を参照されたい。

[7] 但し、いわゆるフィシングサイトに関する事案が報告対象事態に該当するかどうかは、個別具体的な事情による点には留意されたい（個情法 QA6-7, 6-8 参照）。例えば、偽装したウェブサイトに本人が入力した情報（ID やパスワード等）を利用して、第三者が本人になりすまし、個人データが表示される当該個人情報取扱事業者の正規のウェブサイトにログインした場合、一般的には、「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ…の漏えい等が発生し、又は発生したおそれがある事態」が生じたものとして、報告対象となると考えられる（個情法 QA6-8）。

報告対象事態が発生した場合の個人情報保護委員会への報告は、速報と確報の二段階に分けて実施する必要がある。

速報は、報告対象事態を知った後、速やかに（個情法ガイドライン（通則編）によれば概ね 3～5 日以内）、概要や漏えい等した個人データの数などの報告事項[8]（個情法施行規則第 8 条、第 10 条参照）のうち、その時点で把握しているものを報告しなければならない。報告期限の起算点となる「知った」時点については、いずれかの部署が当該事態を知った時点を基準とするとされている。

確報は、報告対象事態を知った日から 30 日以内（サイバー攻撃等の場合は 60 日以内）に、報告事項を報告しなければならない。もっとも、サイバー攻撃等の場合には 60 日以内であっても確報を行うことが難しいケースも多いと考えられ、個情法ガイドライン（通則編）によれば、確報を行う時点において、合理的努力を尽くしたものの全ての事項を報告することができない場合は、確報を行った後で追完することも可能とされている。

次に、本人への通知については、状況に応じて速やかに行うこととされている。ただし、事案がほとんど判明しておらず、通知をしても本人のためにならず、かえって混乱が生じるような場合は、その時点では通知をしなくてもよいとされている。通知内容は、個人情報保護委員会への報告事項の一部であり、通知の方法は、文書の郵送、電子メールの送信等の様式に決まりはないが、本人に分かりやすい形での通知が望ましいとされている。また、ランサムウェアによる暗号化等のため、本人への通知が困難である場合は、本人の権利利益を保護するために必要な代替措置を講ずることによる対応が認められる[9]。

このような代替措置の例として、実務上、事案の公表、問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすることがあり得る（個情法ガイドライン（通則編）3-5-4-5）。

（イ）各分野における留意点

報告対象事態については、原則として個人情報保護委員会へ報告する必要があるが、分野や業種によっては、個人情報保護委員会から権限の委任を受けている府省庁に対する報告が必要となる[10]。

また、業法、分野別のガイドラインに基づく対応が必要となることもあり得る。例えば、金融分野の事業者については、顧客情報の保護の観点から、金融分野の業法（銀行法第 12 条の 2・銀行法施行規則第 13 条の 6 の 5 の 2 等）に基づき、その取り扱う個人

---

[8] 概要（漏えい等の発生日、発覚日など）、漏えい等した（おそれのある）個人データの項目（住所、電話番号、メールアドレス等）、漏えい等した（おそれのある）個人データに係る本人の数、原因、二次被害又はそのおそれの有無及びその内容、本人への対応の実施状況（本人への通知を含む。）、公表の実施状況、再発防止のための措置、その他参考となる事項

[9] なお、被害者の損害に関する金銭的対応については Q63 を参照されたい。

[10] 個人情報保護委員会から権限の委任を受けている府省庁については、下記のサイトを参照されたい。https://www.ppc.go.jp/personalinfo/legal/kengenInin/

顧客に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、金融庁長官等に速やかに報告する必要があるとされている。具体的な対応は、①金融分野における個人情報保護に関するガイドライン、②金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針、③金融機関における個人情報保護に関する Q&A に規定されている。

（ウ）特定個人情報（個人番号をその内容に含む個人情報）の漏えい等

特定個人情報の漏えい等についても、番号利用法等により、個人データの漏えい等と同様、個人情報保護委員会への報告や本人への通知が必要となる報告対象事態が規定されており、例えば、①情報提供ネットワークシステム等に記録された特定個人情報又は個人番号利用事務・個人番号関係事務（これらについては Q20 を参照）を処理するために使用する情報システムで管理される特定個人情報の漏えい等、②不正の目的をもって行われたおそれのある行為による特定個人情報の漏えい等、③特定個人情報が、電磁的方法により不特定多数の者に閲覧された事態、④100 人を超える特定個人情報の漏えい等が報告対象事態にあたるとされている（番号利用法第 29 条の 4、行政手続における特定の個人を識別するための番号の利用等に関する法律第 29 条の 4 第 1 項及び第 2 項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成 27 年特定個人情報保護委員会規則第 5 号）第 2 条参照）。もっとも、報告対象事態に該当しない場合であっても、個人情報保護委員会に報告するよう努めることとされている（特定個人情報の適正な取扱いに関するガイドライン（事業者編）別添 2 3B 参照）。

なお、特定個人情報の漏えい等事案が発覚した場合の、講ずべき措置や個人情報保護委員会への報告及び本人への通知については、個人データの漏えい等事案が発覚した場合と同様である。なお、クラウドサービス提供事業者が、特定個人情報を取り扱わないこととなっている場合において、報告対象となる特定個人情報の漏えい等が発生したときには、クラウドサービスを利用する事業者が報告義務を負うが、クラウドサービスを利用する事業者としては、自らが負う報告義務に基づく報告を、クラウドサービス提供事業者に代行させることができる[11]。

（エ）認定個人情報保護団体の対象事業者

認定個人情報保護団体とは、個人情報保護委員会の認定を受け、業界・事業分野ごとの個人情報等の適正な取扱いの確保を目的として所定の業務を行う法人であり、業界の特性に応じた自主的なルールとして、対象事業者に適用する個人情報保護指針を作成するよう努めなければならないとされている（個情法第 54 条）。例えば、後述するプライバシーマークの運用を担う一般財団法人日本情報経済社会推進協議会（JIPDEC）は、

11 「「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関する Q&A」Q17-17。

プライバシーマーク付与事業者をその対象事業者とする認定個人情報保護団体であり、個人情報保護指針も公表している[12]。

認定個人情報保護団体は、対象事業者において発生した漏えい等事案について自主的取組として、対象事業者から漏えい等事案の情報を受け付けることは有効であるとされている。また、必要に応じて、漏えい等事案の報告を受け付ける体制を確立し、実効的な指導・助言等を行うことが望ましいとされている[13]。ただし、個人情報保護委員会等への報告義務の対象となる漏えい等事案については、報告事項を個人情報保護委員会等が求める内容とできる限り一致させるなど、対象事業者の過度な負担とならないよう努める必要があるとされている（個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編））。

このように、認定個人情報保護団体の対象事業者である場合は、当該団体の個人情報保護指針に基づき、漏えい等事案が発生した場合に当該団体に報告する必要が生じる可能性がある点に注意が必要である。

（オ）プライバシーマーク付与事業者

個人データの漏えい等が発生した事業者がプライバシーマーク（P マーク）付与事業者（Q9 も参照）である場合、プライバシー付与に関する規約第 11 条に基づき、契約上の義務として、事故等の発生に際して、可及的速やかに JIPDEC 等の関係審査機関に報告しなければならない。同規約にいう「事故等」の範囲は、不正・不適正取得、目的外利用、不正利用といったものも含まれており、漏えい等に限られないため留意が必要である。なお、電気通信回線設備を設置する電気通信事業者等も報告義務を負う。

（カ）海外法令

以上のほか、事業者が取り扱っている個人データについて海外法令が適用される場合には、当該法令に基づく当局対応が必要となる。例えば、GDPR が適用される場合は、個人データ侵害に関する監督機関への通知義務及び本人への通知義務が課される（Q82 も参照）。

イ　セキュリティインシデントにおける事故報告制度[14]

データ漏えいをはじめとするサイバーセキュリティインシデントが発生した場合には、業法に基づく事故報告が必要となる場合がある。例えば、電気通信事業者の場合には、①非常事態が発生したこと等により電気通信業務の一部を停止したとき、②電気通信業務に関し、通信の秘密の漏えい、特定利用者情報（第 27 条の 5 第 2 号に掲げる情

[12] 認定個人情報保護団体の一覧及び指針については下記サイトを参照されたい。
https://www.ppc.go.jp/personalinfo/nintei/list/

[13] 令和 4 年 4 月 1 日より前は、旧漏えい等告示に基づき、認定個人情報保護団体の対象事業者において個人データの漏えい等事案が発生した場合は、認定個人情報保護団体に報告を行うこととされていた。

[14] 重要インフラ分野における事故報告制度等については Q45 も参照されたい。

報であって総務省令で定めるものに限る。）の漏えい、若しくはその他総務省令で定める重大な事故が生じたとき、又は③上記①・②の事故が生ずるおそれがあると認められる事態として総務省令で定めるものが生じたと認めたときは、総務大臣に対して遅滞なく報告しなければならない（電気通信事業法第 28 条及び同法施行規則第 58 条の 2）。

このように、業法においては、情報の漏えいを含む事故の発生時に所管省庁に対する報告義務が定められている場合がある。サイバーセキュリティインシデントが明文に含まれていないとしても、当該インシデントによって要件を充足する場合には報告が必要となる点に注意が必要である。

また、事業者による自発的な報告義務が定められていない場合であっても、特に許認可が必要となる事業に関しては、所管省庁が報告徴収の権限を有する法令が多い。このような場合、所管省庁が特定の事業者におけるサイバーセキュリティインシデントの発生を認識した場合には、報告を求めたり資料の提出を要求したりすることがあり得る。

なお、この報告徴収の権限を根拠として省令・規則が定められるケースがある。例えば、電気通信事業に関して、総務省令として電気通信事業報告規則が定められており、電気事業に関して、経済産業省令として電気関係報告規則が定められている。

ウ　重要インフラ行動計画

重要インフラ事業者は、上記（1）イの業法に基づく報告のほか、重要インフラ行動計画に基づき、重要インフラサービス障害を含むシステムの不具合等に関する情報のうち、以下のいずれかのケースに該当する場合には、所管省庁を通じて NCO に対する情報連絡を行うこととされている[15]。

① 法令等で重要インフラ所管省庁への報告が義務付けられている場合
② 関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合
③ そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合

エ　適時開示等

上場会社がサイバーセキュリティインシデントにあった場合には、有価証券上場規程第 402 条等に基づく適時開示、金融商品取引法第 24 条の 5 第 4 項に基づき臨時報告書の提出も検討する必要がある。これらについては Q8 を参照されたい。

[15] 情報連絡の方法については、NCO が「『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書」を公開している（https://www.cyber.go.jp/pdf/policy/infra/tebikisho.pdf）。

（２）その他インシデント発生時に対応を検討すべき事項

ア　警察等への相談等

外部からのサイバー攻撃や従業員による機密情報の持ち出しなどの事案が発生した場合における警察への通報や相談は、これを義務づける法令はないものの、積極的に行うことが望ましい[16]。例えば、外部からのサイバー攻撃を受けたという場合は、攻撃者は不正アクセス禁止法等の法令に違反している可能性があり（Q73～79 参照）、また、従業員等によるデータの持ち出しの場合、不正競争防止法等の法令に違反する可能性もある（下記（4）参照）。

特に外部からのサイバー攻撃の場合、攻撃者を特定することが難しいケースが多いが、例えば令和 3 年 4 月には、JAXA に対するサイバー攻撃事案について、警視庁が被疑者を検察庁に書類送致するなど、攻撃者の特定につながるケースもあり得る。なお、令和 4 年 4 月 1 日に施行された警察法の一部を改正する法律（令和 4 年法律第 6 号）に基づき、サイバー事案について捜査指導、解析、情報集約・分析、対策等を一元的に所掌するサイバー警察局が新設された。

警察との連携のあり方としては、①必要な情報を提供するなどして相談する、②被害届を提出する、③告訴・告発を行う、などの手続があり得る。警察では、被疑者の検挙に向けた捜査を実施することに加えて、捜査で判明した犯罪の手口等を関係機関に提供してさらなる被害を防止するなどの取組を行っている。特に外部からのサイバー攻撃の場合は、まずは警察に相談した上で、最終的な対応を決定することも可能であるため、情報収集や対応方針の決定が完了するまで警察への通報や相談を控えるのではなく、早期に警察に連絡することが重要である。警察への通報や相談は、基本的に、最寄りの警察署又は都道府県警察本部サイバー犯罪相談窓口[17]に行うこととされている。

警察に対してだけでなく、それ以外の行政機関にも相談を行う選択肢もあり得る。例えば、所管省庁が存在する事業者は、当該業法において、情報の漏えいを含む事故の発生時に所管省庁に対する報告義務が定められている場合があることは上記（1）で述べたとおりである。また、昨今のサイバー攻撃事案のリスクの高まりを踏まえ、様々な機会において、関係省庁が合同でサイバーセキュリティ対策の強化を呼びかけるケースが増えており、不審な動き等を検知した場合の所管省庁への情報提供・相談を推奨している[18]。

---

16 サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和 5 年 3 月 8 日）Q18 を参照されたい（https://www.soumu.go.jp/main_content/000867112.pdf）。

17 都道府県警察本部のサイバー犯罪相談窓口（https://www.npa.go.jp/bureau/cyber/soudan.html）

18 例えば、以下の例がある。

- 経済産業省・金融庁・総務省・厚生労働省・国土交通省・警察庁・NCO（旧 NISC）「サイバーセキュリティ対策の強化について（注意喚起）」（https://www.cyber.go.jp/pdf/press/20220301NISC_press.pdf）

なお、一部のサイバー保険では、所轄警察署や公的機関への届出を保険金の受給要件として明示している場合もあり、留意が必要である。

イ　不正アクセスを受けた場合等における対応

コンピュータウイルス・不正アクセスを検知した場合には、IPA が、「コンピュータウイルス対策基準」（平成 7 年通商産業省告示第 429 号）及び「コンピュータ不正アクセス対策基準」（平成 8 年通商産業省告示第 362 号）に基づき、コンピュータウイルスの感染被害の届出及び不正アクセス被害の届出を受け付けているので、これらの届出を行うことが望ましい。なお、IPA では企業組織向けサイバーセキュリティ相談窓口を設けられている。

また、ソフトウェア又はそれを組み込んだハードウェアであって汎用性を有する製品の脆弱性（コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所）を発見した者は、IPA にその旨を届け出ることが望ましい（Q72 参照）。

加えて、サイバーセキュリティに関する官民の各種情報共有の仕組み[19]に対して情報提供を行うことも検討すべきである。こうした情報共有体制に対する情報提供を行うことで、何らかのフィードバックを得ることができ、インシデントの原因究明等に資するケースも多い。

専門機関の JPCERT/CC[20]は、インシデントに関するコーディネーション[21]依頼や調査・解析、セカンドオピニオン依頼を受け付けているため、対応を依頼する、又は相談することが考えられる[22]。

なお、不正アクセスにより窃取された情報の中に取引先の機密情報が含まれていた場合には、取引先との機密保持契約に違反するものとして、債務不履行責任を問われるおそれがあるため、取引先に対して適切に情報の開示を行うことも検討すべきである。ま

- 経済産業省・総務省・警察庁・NCO（旧 NISC）「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」
（https://www.cyber.go.jp/pdf/press/20220324NISC_press.pdf）

[19] 例えば、JPCERT/CC 運営の情報共有プラットフォーム「CISTA」、IPA によるサイバー情報共有イニシアティブ「J-CSIP」などがある。各活動や情報共有全般については、「サイバー攻撃被害に係る情報の共有・公表 ガイダンス」（Q70 を参照）を参照されたい。

[20] 一般社団法人 JPCERT コーディネーションセンター。インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内に関するインシデント等の報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言等を技術的な立場から行う民間の専門機関を指す。
https://www.jpcert.or.jp/

[21] ここでいう「コーディネーション」とは、不正なウェブサイトやサーバの停止や第三者の被害に関する情報の伝達など、被害組織や発見者以外の国内外の組織に対して対応依頼や情報提供に係る調整を行うことを指す。

[22] 状況次第では、攻撃行為の停止のための調整活動として、JPCERT/CC に対して、該当サーバ等のテイクダウンを含む対応について相談等することも考えられる。

た、発生したインシデントが企業の業績等に大きな影響を与えると見込まれる場合、開示対応及び契約に基づく監査法人に対する報告の要否を検討すべきである。

ウ　営業秘密・限定提供データの漏えい

営業秘密の漏えいが発生した場合は（秘密として管理する顧客情報が漏えいした場合、漏えいした情報が個人データでもあると同時に営業秘密でもある場合などが考えられる。）、営業秘密を開示・取得した者等の行為が、不正競争防止法上の営業秘密侵害罪（同法第 21 条等）や、不正アクセス禁止法違反の罪（同法第 11 条）、背任罪（刑法第 247 条）、横領罪（同法第 252 条）等に該当する可能性があることを踏まえた対応が必要になる場合があり得る。

具体的には、漏えいが発覚した場合は、速やかに事実関係の調査と原因を分析し証拠を保全した上で、これらの犯罪が成立する可能性がある場合は、早急に警察への被害届や告訴（刑事訴訟法（昭和 23 年法律第 131 号）第 230 条）を検討すべきである。

加えて、営業秘密の漏えいにより、企業に多大な損害が発生するおそれもあることから、営業秘密の開示者・取得者等に対して差止（不正競争防止法第 3 条）及び仮の差止を求めることや、既に損害が発生している場合については損害賠償請求（同法第 4 条）を行うことも考えられる。

また、営業秘密の要件を満たさない情報であっても限定提供データ（同法第 2 条第 7 項）に該当する情報であれば、不正取得した限定提供データの開示・使用等の行為について差止請求ができ（同法第 3 条）、また損害が発生した場合は損害賠償請求（同法第 4 条）を行うことが可能である。

そのため、営業秘密が漏えいした場合と同様に、被害の拡大防止措置や事実関係の調査、原因の究明をした上で、限定提供データの不正取得等が認められた場合には、早急に民事保全手続きによる仮の差止を求めることや、損害賠償請求を行うことも考えられる。

なお、限定提供データに関しては、不正競争防止法上では不正取得者等に対して刑事罰の規定は設けられていない。もっとも、営業秘密を取得した者等の行為に該当し得るその他の犯罪（不正アクセス禁止法違反、電子計算機使用詐欺罪）については成立する余地があることから、該当する場合には、速やかに事実関係の調査と原因を分析し証拠を保全した上で、早急に警察への相談を検討すべきである（電子計算機使用詐欺罪については Q75、情報の不正入手や漏えいについては Q77、不正アクセスについては Q78 を参照）。

さらに、企業に在籍している従業員により営業秘密・限定提供データの漏えいが発生した場合については、企業内において当該従業員に対する処分（懲戒解雇、降格等）を行うことも考えられる。

エ　情報漏えい等があったという事実とインサイダー取引

上場会社等がサイバー攻撃を受け、大規模な損害の発生が想定される場合、情報漏えいがあったという事実そのものが当該上場会社等の業務等に関する重要事実（金融商品取引法第 166 条。以下、本項において「インサイダー情報」という。）に該当し得る。

この場合、当該情報を知った会社関係者等が当該事実の公表前に株式の売買等を行うことは、インサイダー取引として課徴金（同法第 175 条第 1 項）及び刑事罰の対象となり得るほか（同法第 197 条の 2 第 1 項第 13 号）、会社も刑事罰の対象となり得る（両罰規定。同法第 207 条 1 項 2 号）。

ただし、上場会社等の役員等が上場会社等の計算でインサイダー取引を行った場合のうち、自己株式取得が行われた場合において、同法第 177 条に定める課徴金に関する調査のための処分がなされる前に、自主的に証券取引等監視委員会に報告すれば、課徴金額が減額される（同法第 185 条の 7 第 14 項）。

そこで、会社関係者は、課徴金の減額が可能な場合には適時に証券取引委員会にインサイダー取引の事実を報告するほか、会社としても速やかに事実関係の調査と原因を分析した上で、捜査機関の調査に協力することが望ましい。

また、漏えいした情報の内容にインサイダー情報が含まれているという場合、漏えいの結果当該情報を基に不公正な取引が行われるおそれが高まることから、当該不公正な取引を防止するため、当該情報の公表を検討すべきである。

（３）（参考）セキュリティインシデント報告一元化に向けた動き

我が国全体のサイバーセキュリティを強化するためには、官民双方向の情報共有を促すことが必要不可欠である一方、サイバー攻撃による被害報告件数は増加の一途を辿っており、また、報告先となる官公署も多いことから、サイバー攻撃を受けた被害組織に過度な報告負担がかかっている旨の指摘がなされていた。

このような状況を踏まえ、サイバー攻撃による被害発生時の被害組織の報告負担軽減と政府の対応迅速化を図るため、令和 7 年 5 月 28 日に、関係省庁間で「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」[23]が行われた。

これにより、官公署への報告等に際して利用できる共通様式を整備し、さらに官民連携基盤の整備により、これらの報告の窓口を一元化するよう所要の調整が進められることになる。

本申合せを踏まえて、令和 7 年 10 月 1 日からは、ランサムウェア攻撃と DDoS 攻撃事案におけるインシデント報告についての共通様式が決定され、運用が開始された[24]。

[23] https://www.cyber.go.jp/pdf/policy/infra/ref_moushiawase0925.pdf
[24] https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

Q58 インシデントレスポンスと関係者への対応

企業においてサイバーセキュリティインシデントが発生した際には、どのような流れで対応する必要があるか。法令やガイドラインに基づく対応以外に、例えば契約等に基づいて連絡する必要がある相手方としてどのような者が挙げられるか。

タグ：インシデント対応、デジタル・フォレンジック、サイバー保険、EC サイト、脅威インテリジェンスサービス

１．概要

サイバーセキュリティインシデント発生時の対応としては、大要、インシデントの検知・認識、トリアージ、初動対応・調査（初期調査、詳細調査）、対外対応、再発防止策、プレスリリース等が必要になる。自社だけで対応が困難である場合には、外部の事業者に対応を依頼することが必要になる。その他、取引先や委託先、保険会社への連絡が必要となる場合もある。さらに、脅威インテリジェンスサービスの活用が二次被害の防止に寄与する可能性もあるので検討に値する。

２．解説

（１）インシデント対応の一般的な流れ

インシデント発生時には、大きく以下のような対応が必要になる。ア：インシデントの検知・認識、イ：トリアージ、ウ：初動対応・調査（初期調査、詳細調査）、エ：対外対応、オ：再発防止策。さらに、プレスリリースをすべきか等の検討も必要になる場合も多い。JPCERT/CC が公開する「インシデントハンドリングマニュアル」は、インシデント対応における各作業について解説を加えており参考になる。

ア　検知・認識

インシデントへの対応は、インシデントを検知・認識することから始まる。検知の契機は、システムやネットワークの監視を行う担当者等からの連絡や、外部の業者等からの指摘などがあるが、大まかには、自ら検知するか、外部業者等の第三者からの連絡を受ける形で認識することとなる。

自ら検知することは難しいケースも多いため、検知・認識の機会を増やすためには、外部からの連絡を適切に受け付けることができるようにしておくことが肝要である。例えば、ウェブサイトを運営している場合には、問合せ窓口を整備する、又は、ドメイン情報を Whois サービスで検索した場合に表示される技術連絡担当者の連絡先を適切にメンテナンスしておくべきである。

なお、個情法ガイドライン（通則編）においては、サイバー攻撃事案において個人データの漏えい等のおそれがある事態に該当し得る事例として、「不正検知を行う公的機

関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合」が挙げられているため、外部からの連絡には注意が必要である。

イ　トリアージ

トリアージは、インシデントを検知・認識した後、限られたリソースの中でどのように対応するか、優先順位等をどうするか等を決定する作業である。トリアージの過程で、インシデントの検知が誤りであったことがわかれば、当該インシデント対応としては、その場で終了ということになる。どのように対応すべきか方針を決定するためには、事実関係の整理が重要である。つまり、いつ、どこで、何が、どのように起こったのか、また、当事者や関係者が誰かという点を整理し、判断に必要な事実関係を的確に把握しなければならない。

トリアージの流れは一般的には次のとおりである[1]。

① 得られた情報に基づいて、事実関係を確認し、その情報を得た CSIRT が対応すべきインシデントか否かを判断する。その際には、必要に応じて、インシデントの報告者等と情報をやり取りして詳細を確認する。

② CSIRT が対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織のポリシーなどに照らして可能な範囲で詳細に、報告者に回答したり、情報をやり取りした関係者に報告したりする。

③ CSIRT が対応する、しないにかかわらず、関係者に速やかな対応を依頼すべき、又は情報提供すべきと判断した場合は、注意喚起などの情報発信を行なう。

④ CSIRT が対応すべきと判断した場合には、インシデントを「インシデント対応」の対象とする。

ウ　初動対応・調査（初期調査、詳細調査）

トリアージの結果、インシデント対応部署において対応を行うことを決定した場合には、インシデント対応をスタートさせることになる。まずは事実関係の詳細を整理し、とりまとめを行い、被害原因及び被害範囲を調査し、被害の拡大を防止するための措置を速やかに講じる必要がある。

被害の拡大防止措置としては、例えば、ある端末において不正プログラムの感染が疑われる場合に、当該端末を社外及び社内のネットワークから切り離すなどの措置等が挙げられる。初動対応においては、インシデントによる被害の拡大防止のために、封じ込めを行うことも重要である。必要に応じて情報システムの全部又は一部を一時的に停止するという業務継続に影響を及ぼす判断を下すこともあり得るため、その判断権限を有する者をインシデント対応チームに含めておく必要がある。

[1] JPCERT/CC「インシデントハンドリングマニュアル」10～11 頁。

被害の原因を特定し、調査・解析を行うに当たっては、ログの保全やマルウェア感染端末の確保等を行い、デジタル・フォレンジック[2]を実施し、必要な証拠を保全等することが重要である。例えば、不正プログラムの感染が疑われるコンピュータを再起動すると、揮発性メモリに保存されているデータが失われることがあるので注意を要する。デジタル・フォレンジックについては、自社において実施することが困難である場合には、外部事業者に委託することになる。外部委託に当たっては、IPA が公開する「情報セキュリティサービス適合サービスリスト」[3]中、「デジタルフォレンジックサービス」に掲載されている事業者及びサービスが参考になる。

また、被害範囲の特定のために、脅威インテリジェンスサービス（Q71 参照）などのウェブモニタリングサービスを活用することも考えられる。漏えいした情報が、どこかのサーフェスウェブやダークウェブにアップロードされている可能性もあるため、このようなサービスを活用することで、自社から漏えいした情報の流通・拡散状況を可能な範囲でモニタリングし、被害範囲を特定した上で必要な対策をとることができる。例えば、漏えいした個人情報がダークウェブ上に流通していることが判明すれば、それを本人に伝えて ID やパスワードの変更等を促し、二次被害の防止につなげることも可能である。

エ　対外対応

対外対応について、対応すべきステークホルダーには、①関係行政機関、②警察などの法執行機関、③攻撃者又は加害者、④関連する契約の相手方、⑤情報漏えいが発生した場合の被害者等が挙げられる。本項では、④について紹介し、残りは Q57 を参照されたい。対外対応に関連して、インシデントに関する情報を公表するかどうか、また、公表するとしてどのような情報をどのタイミングで公表するかについても検討が必要である。

オ　再発防止策

最後に再発防止策についてであるが、今後、同種のインシデントの発生を防止するために、その原因を究明し、再発防止策を実施することも重要である。加えて、インシデント対応終了後の総括として、インシデントの経緯、対応策、反省点や改善点に関する詳細を記録として残しておくことが重要である。このような記録が、今後のサイバーセキュリティ対策の参考となるためである。

---

[2] デジタル・フォレンジックについては Q59 を参照されたい。
[3] 経済産業省が策定した「情報セキュリティサービス基準」に適合するものとして審査機関によって認められた事業者のサービスをリストとして公開したものである。

（２）インシデント発生時の関連する契約の相手方への対応について

サイバーセキュリティインシデントの発生により情報の漏えい等が発生してしまった場合には、委託関係を含む取引先との契約等に基づいた行動をとることが必要となる。

ア　取引先への連絡

取引先との契約に基づき提供・開示を受けたデータについて漏えい等が発生した場合、当該取引先との契約において、秘密情報の守秘に関する条項が定められている場合には、漏えい等が発生した場合に当該条項に違反する可能性が考えられるため、契約内容をよく確認することが重要である。契約によっては、開示時に「秘密」と明示していなければ「秘密情報」に該当しないなど、「秘密情報」がかなり狭義に定められているものもあり、このような場合には漏えい等した情報が秘密情報に該当しないと整理することも可能であろう。また、契約相手に対する報告義務についても、規定内容は多岐にわたっており、例えば、秘密情報の漏えい等が発生した場合の報告義務が定められている場合もあれば、広くサイバーセキュリティインシデント発生時（又はそのおそれの発生時）の報告義務が定められている場合もある。

イ　委託先への連絡と調査依頼等

企業が、情報システムの開発や保守運用を委託先に行わせることも多い。このように委託先を利用している場合には、サイバーセキュリティインシデントが発生した際には、委託先に連絡して調査依頼をすることとなる。調査の結果、サイバーセキュリティインシデントの発生原因が委託先に起因することが判明した場合には、当該委託先との契約等に基づき、責任追及をすべきか否か等も検討する必要が生じる。

このほか、上記(1) ウの調査で紹介したデジタル・フォレンジックを行うために、外部事業者にフォレンジック調査を委託することが必要となる場合も多いと思われる。

また、サイバー保険に加入している場合には、保険会社への連絡も必要である（サイバー保険に関しては、Q65 を参照）。

ウ　委託元への報告

企業が、第三者から個人データの取扱いの委託を受けている場合において、委託先で漏えい等事案が発生した場合には、委託契約に基づいて委託元への報告が義務付けられていることが多いため、契約内容を把握し、報告その他の必要な対応を取る必要がある。

また、個人データの取扱いを委託している場合、原則として委託元と委託先の双方が個人情報保護委員会に対する報告義務を負う。この報告は、委託元及び委託先の連名で行うことができる。なお、個情法第 26 条第 1 項但書及び個情法施行規則第 9 条に従って、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知した場合には、委託先は報告義務を免除される。

エ　クレジットカード情報の漏えい等

クレジットカード情報の漏えい等が発生した場合には、クレジットカード会社との関係についても留意が必要である。例えば、EC サイトを運営する事業者においてクレジットカード情報が漏えい等したケース[4]を想定すると、まず、クレジットカード会社が、モニタリングシステムを通じて情報の漏えい元と判断した EC サイトに対して連絡することを契機として、インシデント対応が始まり、原則としてフォレンジック機関（場合により、PCISSC が認定する機関）によるフォレンジック調査が行われる。そして、クレジットカード会社がクレジットカードのユーザに対して不正利用された金額の補償等を行っている場合、クレジットカード会社と EC サイト運営事業者の間で、当該補填金額を最終的に誰が負担するかという観点で協議等を行う必要がある（その他クレジットカード情報の取り扱いについては、Q18 を参照）。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[4] EC サイトを狙った不正アクセスが多発しており、個人情報保護委員会へも、EC サイトへの不正アクセスによる個人データ漏えい等の事案が多く報告されている（個人情報保護委員会「EC サイトへの不正アクセスに関する実態調査」（令和 4 年 3 月 16 日）。もっとも、割賦販売法の平成 30 年改正により、クレジットカード情報保護対策として原則「カード情報の非保持化」をすることが求められており、今後は EC サイトを運営する事業者からのクレジットカード情報の漏えい事案は減少すると見込まれる。

Q59 デジタル・フォレンジック

デジタル・フォレンジックとは何か。どのような場面で使われるのか。また、デジタル・フォレンジックを活用する上で留意すべき法的な問題点としてどのようなものがあげられるか。

タグ：刑法、不正競争防止法、著作権法、児童ポルノ禁止法、金融商品取引法、デジタル・フォレンジック、証拠保全、個情法

１．概要

デジタル・フォレンジックについては、明確な定義があるものではないが、例えば、サイバーセキュリティ 2025・225 頁においては、「不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称」と定義されている。その他、特定非営利活動法人デジタル・フォレンジック研究会（以下、本項において単に「デジタル・フォレンジック研究会」という。）の定義では、「インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等をいう。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」とされ、警察庁の定義では、「犯罪の立証のための電磁的記録の解析技術及びその手続」とされている（警察庁「令和 7 年版警察白書」15 頁参照）。

デジタル・フォレンジックは様々な場面での活用が期待されている。例えば、民事訴訟において、証拠として提出されたデータについて成立の真正を証明するために活用されることや、刑事事件において、被疑事件を解明し、被疑者を特定し、公判の証拠として提出するために活用されることもある。他にも、企業の不祥事が発覚した場合に、第三者委員会が構成され、調査過程において削除されたメールやファイル等のデータを抽出又は復元することや、e-Discovery において Litigation Hold（訴訟に関連する情報・証拠を保全するための手続）を適切に実施するためにも活用されている。

２．解説

（１）デジタル・フォレンジック

デジタル・フォレンジックの定義は、前述したとおりであるが、サイバーセキュリティ戦略本部、デジタル・フォレンジック研究会、警察庁とでその定義が異なっているのは、次の理由によるものである。警察庁の場合は、デジタル・フォレンジックは、犯罪の立証

のために実施するものであるため、刑事事件を念頭に置いた定義になっている。一方、サイバーセキュリティ戦略本部及びデジタル・フォレンジック研究会の場合は、民事訴訟も念頭に、インシデントレスポンスの対応も視野に入れた定義になっているためにやや広くなっている。

デジタル・フォレンジックの大きな流れとしては、電磁的記録が保存されている電子計算機等の端末の収集又は特定、当該端末に対する電磁的記録の保全、電磁的記録の解析、解析結果報告書の作成[1]がある。

ア　端末の収集又は特定

収集又は特定は、被害端末又は攻撃端末を特定する作業、すなわち、収集した様々なアクセスログや端末を解析し、被害に遭った端末はどれか、攻撃に用いられた端末はどれかというように、電磁的記録が保存されている電磁的記録媒体を特定する作業である。

イ　端末に対する電磁的記録の保全

保全は、特定したデジタル・フォレンジックの対象となる HDD や SSD、USB メモリ、SD カード等の電磁的記録媒体に保存されている電磁的記録をコピーする作業であるが、これらの電磁的記録を物理的に全てコピーすること（完全（物理）複製）が通常である。ただし、削除されたデータや破損されたデータ等の復元までは不要であれば、ファイルシステムによって管理されているファイルごとにコピーする論理コピーを実施する。

電磁的記録媒体の完全（物理）複製において、不良セクター等により読み込みができない部分については、代替セクターが使用されるため、この代替セクターがコピーされることになる。しかし、読み込みができない部分に過去の重要なデータが含まれている可能性があるため、この読み込みができない部分も保全することが有益であると考えられる。また、コピーによって保全した場合は、コピー元、コピー先のハッシュ値を取得して同一になっているかを確認することが重要である。コピー元のハッシュ値とコピー先のハッシュ値が同一であれば、両者の電磁的記録の同一性も担保されるからである。なお、ハッシュ値とは、ファイルやイメージデータから一定の計算手順により求められた、規則性のない固定長の値のことをいう。MD5 は 128 ビットであり、全てのファイルやイメージデータは 16 進数表記 32 文字で表され、SHA1 は 160 ビットであり、16 進数表記 40 文字で表される。

このようなハッシュ値の活用は、HDD を丸ごと複写して保全した場合にも活用でき、HDD 全体が改ざんされていないことを立証する手法としても役立つ。

[1] 詳細については、デジタル・フォレンジック研究会「証拠保全ガイドライン　第 10 版」（令和 7 年）等を参照。

もっとも、前述した保全は電源を停止させるか電磁的記録が変更されないことを前提に行われることになるが、昨今のシステムでは停止できないものも存在するため、ある瞬間においての電磁的記録を保全することになる。この場合は、取得したコピー先のハッシュ値しか取得することができないため、写真や動画撮影、保全現場の立会等による適正な保全手続を実施することによって同一性を担保することになる。

ウ　電磁的記録の解析

解析は、保全作業により保全したデータから必要なデータを抽出し、可視化又は可読化する作業である。具体的には、削除されたデータの復元、暗号化されたファイルやフォルダの復号、仮想マシンのイメージファイルなどからの抽出、キャッシュファイルからのキャッシュデータの抽出、ブラウザによる閲覧履歴、メールの送受信履歴、時刻とプログラムが動作したタイムラインによる挙動の抽出等を行う。

このような解析は、手続の正当性、解析の正確性、第三者検証性を重視して実施する必要がある。手続の正当性とは、厳格な管理下で、電磁的記録が保存された電磁的記録媒体が取り扱われ、第三者によって内容が改変等されることなく同一性が保たれていることである。原則としてハッシュ値の同一性によって内容の同一性も担保されるが、前述したようにエラー等によって読み込みができたりできなかったりする場合は、ハッシュ値が異なる可能性がある。このような場合には、ハッシュ値の同一性だけでは内容の同一性を担保できないため、手続の正当性によって内容の同一性を担保することになる。解析の正確性とは、論理的にも技術的にも正確な方法を用いた解析を実施し、電磁的記録から得られた情報を抽出して、可視化又は可読化することである。一部の解析から得られた結果だけではなく、できる限り広範囲に解析した結果を照合し、複数の解析から同一の解析結果が得られることが望ましいといえる。第三者検証性とは、検証した結果が別の第三者が実施したとしても同一の解析結果が得られる再現性のことである。解析を担当した者の解析方法が正確であるかを確認することができるように、同一の解析結果となる業界内で標準的に使用されている解析ツール等を用いることが望ましいといえる。

エ　解析結果報告書の作成

作成は、解析した結果を正確かつ平易で分かりやすく記載し、認識した事実を客観的に記載すべきである。

ハッシュ値に関しては、以下の 2 つの参考となる裁判例がある。

（ア）東京地判平成 29 年 4 月 27 日（平成 26 年特（わ）第 927 号等）

不正アクセス禁止法違反等被告事件において東京地裁は「パソコンが感染した『Xfile.exe』のファイルと、……パソコンから発見された『syouhingazou7.exe』のファイルのハッシュ値……が、SHA-1 と MD5 という 2 種類の計算方法で一致した。

ハッシュ値が同一であるのにファイルが異なる確率は、比較的重複する可能性がある MD5 という計算方法でも、約 1800 京分の 1 の確率である。そうすると、……発見されたファイルと……送信されたファイルは、同一のファイルであると認められる」と判示しており、ハッシュ値が一致することの信頼性を認めている。

（イ）大分地判平成 27 年 2 月 23 日（平成 21 年（行ウ）第 3 号等）

同一と考えられたファイルのハッシュ値が異なったとしても実際に内容を確認した上で判断するため、問題がない場合もあり得る。教員採用決定取消処分取消請求等事件において大分地裁は「解析に用いることが予定されていない……ハードディスクへのアクセスがあり、ファイルの最終アクセス日時が変動しているからといって、……ハードディスク内に保存されていたデータを改変した事実をにわかに推認することはできない。

また、被告が復元したファイルと鑑定人が復元したファイルとの間に……同一名称のファイルでありながらハッシュ値が異なるとしても、鑑定嘱託の結果は、被告が特定したファイルの内容と一致しており、被告の特定したファイルの信用性を左右するものではない。なおファイルのハッシュ値は、ファイルのバイナリデータの僅か 1 ビットの変動でも異なってくるものであるから、ハッシュ値の違いのみから、被告の解析結果の信用性を判断するのは全く相当でないと思慮する。」と判示しており、ハッシュ値が異なったとしてもファイルの内容を実質的に判断していることから、単にハッシュ値が異なるからといって、ファイルの内容の同一性まで一律に否定されるわけではないことを述べている。

（2）デジタル・フォレンジックの民事的活用[2]

民事訴訟において電磁的記録を証拠として提出する場合、当事者は、当該記録が作成者の意思に基づき真正に成立したものであることを証明しなければならない。

電磁的記録が、例えば電子商取引でやり取りされたものであれば、電子署名の方法が法定されており、これにより成立の真正を証明することが考えられる[3]。ところが損害賠償請求訴訟では、このようなデータ等が整っていることは少なく、訴訟の相手方が争った場合に、成立の真正を証明する方法が問題となる。そこで、電磁的記録の意味内容を証拠資料とするためには、その電磁的記録としてのファイルがいつできたのか、最後に修正を加えられたのがいつかを明らかにするためのタイムスタンプや、修正履歴を記録しておくことが考えられる。また、こうした電磁的記録を特定し、成立の真正を証明するためには、デジタル・フォレンジック技術の活用が有用である。

---

[2] その他、解析結果報告書等のフォレンジック結果については、ベンダとの契約に基づき、利用目的が限定（第三者への提供禁止や裁判上の証拠としての利用禁止等）されることもあり得るため、想定する利用の態様によってベンダへの相談が必要となる点に留意が必要である。

[3] 電子署名については、Q50 を参照されたい。

具体的には、電磁的記録が作成された電子計算機等において当該電磁的記録としてのファイルが作成、変更等がされたのか、クラウド上に保存された痕跡が存在するか、あるいは、電磁的記録内に保存されるメタデータの整合性や同ファイルが他にコピーされた場合のハッシュ値の比較などが考えられる。

（３）デジタル・フォレンジックの刑事的活用

サイバーセキュリティの侵害が行われた場合、犯罪の立証に電磁的記録は不可欠な状況になってきている。デジタル・フォレンジックの大きな流れは前述したとおりであるが、留意すべき点としては保全と解析である。保全と解析が適切でないときは、電磁的記録、あるいはその解析結果の証明力が否定され得るからである。

（４）調査委員会による不正調査におけるデジタル・フォレンジックの活用

企業において不正や不祥事が発覚すると、その調査を実施する調査委員会が設置されることが多い。調査委員会には、社内調査委員会、外部調査委員会、第三者委員会等がある。これらの調査委員会で全容解明や類似不正の有無の確認等を目的として、電子計算機内に保存された電磁的記録や電子メール等が調査対象になることがあり、これらの調査にデジタル・フォレンジックが用いられる。

このような調査において重要な電磁的記録は、作成されたファイルや電子メールである。ファイルや電子メールによって、不正の動機や手口、期間、関与者の範囲、隠語、俗語、対象物品、金額等を把握し、その後に関係者に対して聞き取り調査を行う。さらに、昨今解析対象として重要になってきているのはコミュニケーションツールである。コミュニケーションツールには、LINE や X（旧 Twitter）、Facebook、WeChat、Slack や Teams 等があり、やり取りされた過去の履歴等が PC やスマートフォン等に保存されていることがあるため、解析対象となる。

大量のファイルや電子メールを全て網羅的に調査対象にすることは、不要なファイルや電子メールが数多く含まれていることから非常に非効率となる。そのため、実務上は、特定のキーワードによってヒットした検索結果のみの調査や AI を用いた調査を行い、効率化を図ることが多い。

（５）e-Discovery におけるデジタル・フォレンジックの活用

米国の民事訴訟においては、電子保存情報（Electronically Stored Information）を対象とするディスカバリー[4]である e-Discovery が、2006 年 12 月に施行された連邦民事訴訟規則（FRCP）改正により導入された。e-Discovery の対象である電子保存情報には、保存されたあらゆる種類のデータ及びコンテンツが含まれる。e-Discovery に関する規定

[4] ディスカバリーとは、連邦民事訴訟において、当事者の要請等に基づき、訴訟に関連する情報を当事者及び第三者から強制的に開示させる手続きをいう。

やルールに違反した場合には、事実の推定、訴えの全部又は一部の却下、法廷侮辱罪に基づく制裁金又は拘禁等、幅広い内容の制裁が科される。e-Discovery の違反に対する制裁例は多数存在しており、違反をした当事者の請求を棄却したものや、違反をした当事者に対して高額な金銭的制裁（2500 万ドルの支払い）を加えたもの等が存在する[5]。

e-Discovery を含むディスカバリーに関連して、当事者は、（訴訟係属前であったとしても）訴訟を合理的に予期できるに至った時点から[6]、情報保全義務（Duty To Preserve Information）を負い、当該時点で存在する訴訟に関連する情報、証拠を保全し、かつそれ以降に作成された訴訟に関連する情報、証拠を保全しなければならない。そして、情報保全義務を履行する手段として、Litigation Hold と呼ばれる、訴訟に関連する情報・証拠を保全するための手続を実施することが一般的である。Litigation Hold を実施するに際しては、少なくとも、①関連する情報、証拠の廃棄を止めるよう求める社内通達の交付、②キープレイヤーとなる従業員の特定、③電子データや紙媒体の資料の保全、④電子メール自動消去プログラムの停止、⑤元従業員の資料の保全、⑥（必要に応じて）バックアップデータの保全を検討することが必要となる。

Litigation Hold のうち、上記③の電子データの保全を適切に実施するためには、デジタル・フォレンジック技術の活用が有用である。

（６）デジタル・フォレンジックを行う際の法的課題

以下のとおり、デジタル・フォレンジックを行うに際しては、種々の法的課題が生じ得るため、注意する必要がある。

ア　著作権

デジタル・フォレンジックの保全作業には、電磁的記録媒体を全て物理コピー等する場合がある。しかし、この場合、対象となる電磁的記録媒体にインストールされた OS やプログラム等も丸ごとコピーすることになる。この際、著作権との関係が問題になるが、マルウェア等の被害に遭った電磁的記録媒体の OS やプログラム等について、被害当時の状況を保全するためにコピーし、第三者に調査解析を行わせるなどの場合、プログラムの実行等によってその機能を享受することに向けられた利用行為ではないと評価できれば、著作権法第 30 条の 4（著作物に表現された思想又は感情の享受を目的としない利用）に該当し、著作権侵害には該当しないと解される可能性がある（Q25 参照）。また、裁判手続のために必要と認められる場合であれば、その必要と認められる限度に

[5] なお、e-Discovery の違反に対する制裁は、訴訟当事者だけでなく、代理人弁護士や社内弁護士に対しても課せられることがあるため、留意が必要である。

[6] いつの時点から「合理的に予期」できるかは、具体的な事情によるため一義的に確定することはできないが、例えば、被告側であれば警告状を受領した時点、原告側であれば警告状の送付準備を開始した時点で「合理的に予期」できると評価される場合も少なくないと考えられる。

おいて OS やプログラム等を複製等したとしても著作権侵害には該当しないと考えられる（同法第 41 条の 2 第 1 項)。ただし、いずれの場合も著作権との関係とは別に、当該 OS やプログラム等における利用規約との関係については注意する必要がある。

イ　プライバシー権

企業が内部不正者に対するデジタル・フォレンジックを実施する際、対象者のプライバシーを著しく侵害しないように留意すべきである。企業が、企業防衛という名目で、対象者らを監視、調査等を行うため、対象者の尾行やロッカー内の私物の写真撮影等を行った事件について、最高裁は、「上告人は、被上告人らにおいて……企業秩序を破壊し混乱させるなどのおそれがあるとは認められないにもかかわらず、……退社後同人らを尾行したりし、……ロッカーを無断で開けて私物……を写真に撮影したりした」ことに対して、このような行為は、「プライバシーを侵害するものでもあって、同人らの人格的利益を侵害する」とし、これら一連の行為は不法行為を構成すると判断した（最判平成 7 年 9 月 5 日労働判例 680 号、関西電力事件。なお、Q29 も参照されたい。)。

ウ　個人情報

デジタル・フォレンジックの対象となるデータに個人情報が含まれる場合には、個情法も問題となる。

電子メール等の電磁的記録は、その量が膨大となりやすいため、デジタル・フォレンジックを外部事業者に委託する場合も多い。このような外部委託に関連して、例えば、デジタル・フォレンジックを委託した日本の外部事業者が、外国に所在するサーバを用いたクラウドサービスで電子メールの分析等を行う場合は、個人データの安全管理措置（同法第 23 条）の一環として外的環境の把握が必要になると考えられる。また、外国に所在する事業者にデジタル・フォレンジックを委託することに伴い、個人データを含む電磁的記録を提供する場合は、越境移転規制（同法第 28 条）も問題となる[7]。この点、提供先の事業者が EU・英国に所在する場合、又は、提供先の事業者が基準適合体制を整備している場合には、個人データの取扱いの委託（同法第 27 条第 5 項第 1 号）を法的根拠とすることが考えられるが、これらに該当しない場合には、個人データの取扱いの委託を法的根拠とすることはできない。他方、電子メール等の電磁的記録はその関係者が膨大であり、また、不正調査においては、本人が同意することが期待できない場合もあるところ、同条第 1 項第 2 号といった例外事由に該当する場合には、これを法的根拠として本人の事前同意を得ることなく提供することが可能である。

[7] 外的環境の把握及び越境移転規制については、Q15 を参照されたい。

エ　違法な電磁的記録

デジタル・フォレンジックを依頼された第三者が解析した結果、違法な電磁的記録を抽出した場合も問題が生じ得る。例えば、児童ポルノは、所持、提供等が児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律（平成 11 年法律第 52 号）により犯罪とされており（同法第 7 条第 1 項・第 2 項等)、デジタル・フォレンジック事業者等の第三者が児童ポルノに該当する電磁的記録を抽出した場合、その後の所持や提供には留意が必要である。また、マルウェアを抽出した場合、正当な理由なくその後も保管し続け、他人の PC 等の使用者の意図とは無関係に勝手に実行されるようにする目的を満たせば、不正指令電磁的記録保管罪（刑法第 168 条の 3）に該当し得る。また、デジタル・フォレンジック事業者等の第三者が他社の営業秘密に該当する電磁的記録を抽出した場合、不正に取得されたものであることを知るなどすれば、当該営業秘密に関するデータを使用、又は開示することができない（不正競争防止法第 2 条第 1 項第 9 号）ことになる。そのため、デジタル・フォレンジックの結果、得られた違法な電磁的記録をそのまま委託者に提出するのか、提供せずに削除するのかは契約関係や信義則に基づいて慎重に検討すべきであろう。また、デジタル・フォレンジック事業者等の第三者は、解析の正確性を検証することや再度の解析のため、バックアップを保存しておくことも考えられるが、このような違法な電磁的記録が含まれている可能性もあるため、早期に削除すること及びこれを契約内容として盛り込んでおくことが望ましい。

オ　インサイダー取引

デジタル・フォレンジック事業者がサイバー攻撃の被害に遭った上場企業からデジタル・フォレンジックを依頼された場合、当該依頼に基づいてサイバー攻撃の被害事実を知ることになるため、この被害事実が当該上場企業の投資者の投資判断に著しい影響を及ぼす場合には、当該事実の公表前に、当該事業者の役員等が当該上場企業の株取引を行えば、インサイダー取引規制に該当するおそれがある点に留意すべきである（金融商品取引法第 166 条第 1 項第 4 号、第 5 号等)。

（7）情報セキュリティサービス基準

経済産業省は、情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準を設けている。そして、デジタルフォレンジックサービスを提供しようとする者は、技術要件として、専門性を有する者の在籍状況やサービス仕様を明らかにしていること、品質管理要件として、品質管理者の割当状況や品質管理マニュアル等の整備、品質の維

持・向上に関する手続等の導入状況を明らかにしていることを充足しているかを確認し、これを満たしているサービス名がリスト化[8]されて公開されている。

デジタル・フォレンジックを第三者に依頼する必要が生じた場合には、このリストを参考にすることも選択肢の一つとして挙げられる。

３．参考資料（法令・ガイドラインなど）

・刑法第 168 条の 3
・不正競争防止法第 2 条第 1 項第 9 号
・児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律第 3 条の 2
・金融商品取引法第 166 条第 1 項第 4 号、第 5 号等
・デジタル・フォレンジック研究会「証拠保全ガイドライン第 10 版」
https://digitalforensic.jp/wp-content/uploads/2025/04/shokohozenGL10.pdf
・経済産業省「情報セキュリティサービス基準第 4 版」

４．裁判例

本文中に記載のとおり

[8] https://www.ipa.go.jp/security/service_list.html リストについては情報セキュリティサービス基準審査登録委員会ウェブサイトも参照されたい（https://sss-erc.org/digital）。

Q60 ランサムウェア対応

ランサムウェア攻撃を受けた場合、どのような法律に留意すべきか。

タグ：ランサムウェア、会社法、善管注意義務、経営判断原則、個情法、適時開示、テロ資金提供処罰法

１．概要

近時、ランサムウェア攻撃の手口としては、令和 4 年以降、いわゆる標的型ランサムによるものが高水準で推移しており、「二重の脅迫」を行うケースが多くの割合を占めている。また、大企業に対する攻撃件数も 3 割程度存在し、耳目を集めることが増えてきている。

ランサムウェア攻撃によって個人データの漏えい等又はそのおそれが発生した場合、対象となる個人データの内容や件数に関係なく、個情法上、原則として当局への報告対象である点に留意が必要である。ランサムウェア攻撃により身代金を要求された場合においては、支払いの是非を慎重に判断することが求められ、取締役などの役員が安易な身代金の支払いを決定すると、善管注意義務違反を構成し得ると考えられる。その他、適時開示も問題となり得る。

２．解説

（1）ランサムウェア攻撃とは

サイバー攻撃の一類型として、ランサムウェアと呼ばれるウイルスを使用し、攻撃先の端末上のデータを暗号化するなどして、その復元と引き換えに（身代金[1]として）金銭を脅し取ろうとする類型（以下、本項において「ランサムウェア攻撃」という。）がある[2]。

ランサムウェアとは、PC 等の端末及びネットワーク接続された共有フォルダ等に保管されたファイルを、利用者の意図に沿わず暗号化して使用を不可能にし、又は画面ロック等により操作を不可能にするマルウェアの総称である[3]。

---

[1] 「身代金」とは、通常、人質などと引き換えに渡す金銭のことであり、ランサムウェアの場合には、人間ではなく、データが問題となっているため、「身代金」という表現は必ずしも適切ではないという見方もあり得るものの、ランサムウェアの場合でも「身代金」と表現することが一般的であるため、本稿ではそのように表現する。

[2] 近時、ランサムウェア攻撃による被害は拡大しており、IPA が公開している「情報セキュリティ 10 大脅威 2025」では、ランサムウェアによる被害が、10 年連続で組織向け脅威の第 1 位となっている。

[3] 復旧と引き換えに身代金を支払うよう促す脅迫メッセージを表示するソフトウェアであることから、「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、ランサムウェアと呼ばれている。

近時、ランサムウェア攻撃の手口としては、令和 4 年以降、いわゆる標的型ランサム[4]によるものが高水準で推移しており、暗号化前にデータを窃取し、ランサムウェアにより暗号化したデータの復元に対する身代金に加えて、窃取したデータを公開しないことに対する身代金を要求する「二重の脅迫」を行うケースが多くの割合を占めている。また、データを暗号化することなく、データを窃取した上で企業・団体等に対価を要求する手口（ノーウェアランサム）も確認されている。

（２）ランサムウェア攻撃と個人データの「漏えい等」

令和 2 年個情法改正により、個人データの漏えい等に関する報告等を義務付ける規制が新たに導入された（同法第 26 条。詳細について Q57 を参照されたい。）ため、ランサムウェア攻撃を受けた場合には、報告等の要否を検討する必要がある。

「漏えい等」とは、「漏えい、滅失若しくは毀損」を指すところ、ランサムウェアによって個人データが暗号化され復元できなくなった場合には、個人データの「毀損」に該当するとともに、ランサムウェアによる暗号化に際して個人データが窃取されている場合には、「漏えい」にも該当する。

そして、ランサムウェア攻撃による個人データの漏えい等は、報告対象事態の１類型である「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等」（個情法施行規則第 7 条第 3 号）に該当するため、漏えい等した個人データの内容や件数に関係なく、個人情報保護委員会への報告及び本人への通知が必要となる点に留意が必要である。

（３）身代金の支払いと関連法令

ランサムウェア攻撃を受けた場合の対応において、実務上重要な論点は、要求された身代金を支払うことの是非である。以下のとおり、ランサムウェア攻撃で要求された身代金を支払うことを直接禁止する法令はないが、身代金の支払いには様々な問題が生じ得る[5]ことから、一般的な対応として、ランサムウェア攻撃者に対する金銭支払いを可能な限り

[4] ウイルスを添付したメールを機械的にばらまく手口ではなく、標的型サイバー攻撃と同様の方法、つまり、①攻撃者自身が様々な攻撃手法を駆使して、企業・組織のネットワークへひそかに侵入し、侵入後の侵害範囲拡大等を行った上で、②事業継続に関わるシステムや、機微情報等が保存されている端末やサーバを探し出してランサムウェアに感染させたり、管理サーバを乗っ取って、一斉に組織内の端末やサーバをランサムウェアに感染させたりする攻撃方法である。

[5] 例えば、サイバー攻撃者集団に対する資金提供行為は、具体的な状況次第では、テロ資金提供処罰法（公衆等脅迫目的の犯罪行為等のための資金等の提供等の処罰に関する法律）、犯罪収益移転防止法（犯罪による収益の移転防止に関する法律）、外為法（外国為替及び外国貿易法）等、様々な法令に抵触する可能性がある点には留意が必要である。

回避し、他の方法（当局への報告、専門家への相談、代替策の検討等）で脅威に対処することを強く推奨するのが国際的な動向といえる[6]。

ア　善管注意義務違反（会社法など）

身代金の支払いは、企業に身代金相当額の損失を発生させるものであるため、支払いを決定した取締役などの役員が、善管注意義務（会社法第 330 条、民法第 644 条）違反に基づく損害賠償責任（会社法第 423 条第 1 項、第 429 条第 1 項）を負わないかが問題となる。

ランサムウェア攻撃において要求された身代金を支払うかどうかは、多くの要素[7]を複合的に考慮した上での判断が必要となる。こうした判断は、一義的な回答があるわけではなく、一般的には、経営上の専門判断になじむ事項と考えられるところ、そうした経営判断は、判例上、「その決定の過程、内容に著しく不合理な点がない限り、取締役としての善管注意義務に違反するものではない」とされている（最判平成 22 年 7 月 15 日判タ 1332 号 50 頁参照）。他方で、取締役が、反社会的勢力等である株主からの株主の地位を濫用した不当な要求に応じて金銭的利益の供与を行った事案において、取締役は「暴力団関係者等会社にとって好ましくないと判断される者……から、株主の地位を濫用した不当な要求がされた場合には、法令に従った適切な対応をすべき義務を有する」と判示した判例も存在する（最判平成 18 年 4 月 10 日民集 60 巻 4 号 1273 頁）。

近時、コンプライアンスや犯罪組織への資金供給の防止に係る企業への要請がより一層高まっていること等に照らせば、株主の地位を濫用した不当な要求がされた場合と同様、ランサムウェア攻撃により身代金を要求された場合においても、支払いの是非を慎重に判断することが求められ、安易な身代金の支払いは善管注意義務違反を構成し得ると考えられる。

---

[6] 例えば、ランサムウェアの脅威への対処に関する国際連携等について議論するために毎年開催される Counter Ransomware Initiative (CRI)においては、2023 年の第 3 回会合で、ランサムウェアによる金銭支払いを避けることを強く勧めること等を内容とする共同声明が発出され（https://www.cyber.go.jp/pdf/press/press_cri_statement_20231102.pdf）、2024 年の第 4 回会合で、ランサムウェア・インシデント発生時に、身代金支払いを検討する前に組織が講じるべき手順のガイダンスが作成・公表されている（https://www.cyber.go.jp/pdf/press/press_cri_statement_20241003.pdf）。

[7] ①身代金を支払わずに復旧可能か、②（復旧可能な場合）復旧にかかるコスト、③身代金の金額と支払いによって得られると期待される効果のバランス、④身代金を支払ったとしても、攻撃者がデータの暗号化を解除し又は公表を中止する保証はないこと、⑤支払った身代金が攻撃者（犯罪者）の資金源となり、支払いの事実がランサムウェア攻撃が思惑どおりに機能していることを実証すること、⑥身代金の支払いは、間接的ではあるが攻撃者（犯罪者）に協力することを意味するため、当局等からそのような評価を受ける可能性があること、⑦身代金を支払った場合、攻撃者の「カモリスト」入りし、更なるランサムウェア攻撃を受ける可能性があること等が考えられる。

経済産業省が令和 2 年 12 月に公表した「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」[8]においても、身代金への対応が「経営者が判断すべき経営問題そのものであるということを強く認識する必要がある」と、対応が経営問題であることを強調しつつ、身代金の支払いは、「犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない[9]。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。」とされている。

イ　適時開示

要求された身代金の金額次第では、身代金を支払うこと又は支払わないことを決定した事実は、「投資者の投資判断に著しい影響を及ぼすもの」（有価証券上場規程（東京証券取引所）第 402 条第 1 号 at）として適時開示が必要となり得る[10]。また、身代金の支払に伴う損害の規模や内容等によって当該事象が「提出会社の財政状態、経営成績及びキャッシュ・フローの状況に著しい影響を与える事象」（企業内容等の開示に関する内閣府令第 19 条第 2 項第 12 号）に該当するとき、臨時報告書（金融商品取引法第 24 条の 5）の提出が必要となる。

ウ　OFAC 規制

米国財務省外国資産管理局（the U.S. Department of the Treasury's Office of Foreign Assets Control。以下、本項において「OFAC」という。）が実施・執行する、いわゆる OFAC 規制[11]には、米国企業等と制裁対象者である特定のサイバー犯罪グループ等との直接的又は間接的な取引を禁じる規制等が含まれる。そして、ランサムウェア攻撃の攻撃者が制裁対象者の場合等には、ランサムウェア攻撃を受けた者による身代金の支払い

---

[8] https://warp.ndl.go.jp/info:ndljp/pid/13345036/www.meti.go.jp/press/2020/12/20201218008/20201218008.html

[9] 例えば、一般財団法人日本情報経済社会推進協会（以下「JIPDEC」という。）の「企業 IT 利活用動向調査 2026」によれば、2026 年 1 月に実施された調査の対象企業となった 1107 社のうち、ランサムウェア感染の被害経験のある企業は 45.8%（507 社）であり、そのうち、身代金を支払った割合は 20.1%（222 社）、支払わなかった割合は 25.7%（285 社）、さらに、身代金を支払った企業（222 社）のうち、システム・データの復旧に成功したのは 7.5%（83 社）、復旧できなかったのは 12.6%（139 社）とのことであり、身代金を支払ってもシステム・データの復旧が必ずしも保証されない実態が窺われる。

[10] 加えて、ランサムウェア攻撃の被害を受けた事実自体も、これによって暗号化又は窃取・公表されたデータの量・内容等の事情次第で、適時開示が必要となり得る。

[11] 一般的に、OFAC が、米国の外交政策・安全保障上の目的から講じている、一定の国・地域や特定の個人・団体等を対象とする取引制限や資産凍結等の経済制裁を、OFAC 規制という。

が上記規制に違反し、規制違反となることを知らなくとも、厳格責任に基づく制裁金の対象となり得ると考えられる[12, 13, 14]。OFAC 規制については、Q83-1 も参照されたい。

（４）身代金の支払いとサイバー保険

仮にランサムウェア感染の被害にあった企業が身代金を支払った場合に、サイバー保険の補償対象となるか否かは、当該保険の補償の内容・条件次第であるが、現在、少なくとも日本の保険会社が提供するサイバー保険では、身代金として支払った金銭はサイバー保険の補償対象にならない、とする取扱いが一般的である（Q65（４）も参照）。

（５）参考ウェブサイトなど

実際にランサムウェア攻撃を受けてしまった場合には、上記のような法的な考慮以外にも様々な対応が必要となるところ、例えば以下のウェブサイトが参考になる。

① NCO： ランサムウェア特設ページ STOP! RANSOMWARE（各セキュリティ機関におけるランサムウェア攻撃に関するウェブページへのリンク集）
https://www.cyber.go.jp/tokusetsu/stopransomware/index.html

② JPCERT/CC： 侵入型ランサムウェア攻撃を受けたら読む FAQ（ランサムウェア攻撃の被害に遭った場合の対応ポイントや留意点を FAQ 形式で記載）
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

本文中に記載のとおり

---

12 OFAC が 2021 年 9 月 21 に公表した、ランサムウェアの支払いの促進についての潜在的制裁リスクについてのアップデート版の勧告（Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）（https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf）を参照されたい。

13 なお、企業に法令違反行為をさせることに役員の裁量は認められず、役員が、企業に法令違反行為をさせることとなる行為をした場合は、直ちに「任務を怠ったとき」に該当すると解され（最判平成 12 年 7 月 7 日民集 54 巻 6 号 1767 号参照）、当該役員は、法令違反について善意無重過失でない限り会社法第 423 条 1 項第 1 項に基づく損害賠償責任を負い、法令違反について悪意又は重過失の場合には同法 429 条 1 項に基づく損害賠償責任を負うと考えられる。したがって、身代金の支払いが OFAC 規制に違反し、かつ役員がそのことを認識していたにもかかわらず、当該役員が身代金の支払いを決定した場合には、当該役員は上記損害賠償責任を免れられないと考えられる。

14 このほか、外為法に基づく措置によって、指定された一定の対象者に対する支払いが許可制となっている点にも留意する必要がある。

Q61 サイバー攻撃による情報喪失

受託して管理していた情報がサイバー攻撃等により消失した場合、受託事業者はどのような法的責任を負うか。同様に、受託事業者が故意又は重過失による操作ミスにより消失した場合はどうか。

タグ：民法、消費者契約法、電気通信事業法、情報消失、寄託、免責規定、責任制限規定、過失相殺

１．概要

データの管理・保管を受託した事業者は、依頼者に対し、当該データを損壊又は消滅させないように注意すべき義務を負う。そのため、その注意義務に反した場合には、債務不履行責任を負うことになる。これは、サイバー攻撃等によるか受託事業者の故意又は重過失による操作ミスによるかにかかわらず、上記注意義務に反したかどうかによって法的責任を負うかどうかが決まる。保管を委託したデータについてユーザ側にもバックアップをしておくべき注意義務がある場合には、ユーザがバックアップをしていないことについて過失相殺がなされる可能性がある。

また、データを管理する事業者が電気通信事業者に該当する場合には、当該データが通信の秘密の保護対象であれば、消失したことは通信の秘密の漏えいと判断され得る。当該漏えいが過失により生じた場合には、電気通信事業法（以下、本項において「事業法」という。）第 29 条第 1 項第 1 号に基づき、データ管理事業者は総務大臣による業務改善命令の対象となることがある。また、当該漏えいに故意が認められるものであるならば、通信の秘密の侵害罪にあたり、刑事責任を負うことになる（同法第 179 条第 2 項、第 190 条第 2 号)。

さらに、このようなサービスの利用規約（約款）には、データ消失による損害についての責任制限や免責が定められていることが通常であるが、ユーザが消費者の場合は、消費者契約法により、責任の完全な免除や故意又は重過失に対する責任の一部免除を定める条項は無効になる（同法第 8 条第 1 項)。他方、ユーザが事業者の場合は、同法の適用がなく、ユーザとデータ受託事業者との間で責任の完全な免除や責任の一部免除を定める条項は、基本的には有効であるが、データ受託事業者に故意がある場合は無効に、重過失がある場合は、無効又は制限的に解釈される可能性があると考えられる。ユーザとデータ受託事業者との間で SLA（Service Level Agreement）の契約条項が存在する場合には、その限度で受託事業者は責任を負う。

２．解説

（１）データを受託して管理している事業者の注意義務

データを受託して管理している事業者は、「一般に、物の保管を依頼された者は、その依頼者に対し、保管対象物に関する注意義務として、それを損壊又は消滅させないように注意すべき義務を負う。この理は、保管の対象が有体物ではなく電子情報から成るファイルである場合であっても、特段の事情のない限り、異ならない。確かに電子情報は容易に複製可能であるから、依頼者の側で保管対象と同一内容のファイルを保存する場合が少なくないとしても、そのことをもって一般的に保管者の上記注意義務を否定することは妥当でない」（東京地判平成 13 年 9 月 28 日（平成 12 年（ワ）第 18753 号・平成 12 年（ワ）第 18468 号））とされており、ユーザから保管を委託されたデータを損壊又は消滅させないように注意すべき義務を負っている。

一方、データ管理事業者（クラウドサービス提供事業者）とユーザとの間に別の事業者が介在し、クラウドサービス提供事業者とユーザとの間に直接の契約関係がない場合について、東京地裁は、サーバに保存されたプログラムやデータの保管について寄託契約的性質があるとはいえず、契約関係にない第三者に対する関係で当然にはサーバに保管された記録について善管注意義務や記録の消失防止義務を負うことはできないとしている。また、クラウドサービス提供事業者は利用規約に責任制限規定や免責規定を設け、これを前提として料金を設定して契約者から料金の支払を受けて共用サーバホスティングサービスを提供している一方、ユーザはプログラムやデータの消失防止策を容易に講ずることができたのであるから、ユーザ及びクラウドサービス提供事業者双方の利益状況に照らせば、サーバを設置及び管理するクラウドサービス提供事業者に対し、ユーザの記録を保護するためにその消失防止義務まで負わせる理由も必要もないと判示した（東京地判平成 21 年 5 月 20 日判タ 1308 号 260 頁）。

（２）免責規定・責任制限規定

データを保管するサービスの利用規約（約款）には、データ消失による損害についての責任制限や免責が定められている条項が付されていることが通常であるが、ユーザが消費者の場合には、消費者契約法第 8 条第 1 項により、責任の完全な免除や故意又は重過失に対する責任の一部免除を定める条項は無効になる。一方、ユーザが事業者の場合は、消費者契約法の適用がなく、ユーザとデータ受託事業者との間で責任の完全な免除や一部免除を定める条項は、原則として有効である。

ただし、システム開発に関する裁判例（Q52 参照）として、東京地裁は、一律に責任を免除する規定について、被告が「権利・法益侵害の結果について故意を有する場合や重過失がある場合（その結果についての予見が可能かつ容易であり、その結果の回避も可能かつ容易であるといった故意に準ずる場合）にまで同条項によって被告の損害賠償義務の範囲が制限されるとすることは、著しく衡平を害するものであって、当事者の通常の意思

に合致しない」と判示しており（東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁）、当該裁判例に照らすと、データ管理事業者に故意又は重過失がある場合でも、一律に責任を免除する旨の免責規定は無効とされる可能性がある。

当該免責規定の有効性については、その他の裁判例[15]も踏まえると、当事者間の信義誠実の原則及び公平の原則に照らし、責任制限規定の趣旨や内容、契約に至る経緯等の個別的事情を総合的に考慮した上で判断することとなると考えられる[16]。

なお、SLA（Service Level Agreement）が設定されている場合には、SLA が充足されなかった場合の責任規定があれば、その内容に従って補償される。このような SLA のデータ管理の規定には、通常、バックアップの方法、バックアップデータの保存期間といったデータ管理の項目が設定されている。なお、SLA を設定するには SLO（Service Level Objective）[17]を考慮して決定することになる。

（３）過失相殺

データを委託したユーザが、自身で容易にバックアップを取得できる場合には、バックアップをしなかったことによってデータ受託事業者の下でデータが消失した場合にデータを復元できなかったことについて、ユーザにも一定の過失が認められるため、過失相殺により損害賠償額が減額される可能性がある。

東京地裁は、「原告は、本件ファイルの内容につき容易にバックアップ等の措置をとることができ、それによって……損害の発生を防止し、又は損害の発生をきわめて軽微なものにとどめることができたにもかかわらず、本件消滅事故当時、原告側で本件ファイルのデータ内容を何ら残していなかったものと認められる」とした上で、「本件においては、被告の損害賠償責任の負担額を決するに当たり、この点を斟酌して過失相殺の規定を適用することが、損害賠償法上の衡平の理念に適うというべきである」（前掲・東京地判平成 13 年 9 月 28 日）と判示した。

また、同裁判例では、ユーザ（原告）の予見可能性について、「過失相殺を適用するに当たっては、原告に本件ファイルの消滅という結果発生に対する予見可能性が認められれば十分であって、その結果に至る因果経過として、被告の本件注意義務違反により本件ファイルが消滅したことに対する予見可能性までは必要ないと解すべきである。……原

---

[15] 損害賠償額の上限を定める責任制限規定について、信義誠実の原則及び公平の原則に照らし、当該規定を適用せず相当な損害賠償額を認定した裁判例（東京地判平成 16 年 4 月 26 日（平成 14 年（ワ）第 19457 号））等がある。

[16] また、受託者との間で約款を用いて契約を締結している場合には民法における定型約款の規定（同法第 548 条の 2 から第 548 条の 4 まで）の適用について留意する必要がある（Q42 参照）。

[17] SLO はサービス目標値ともいわれ、サービス提供事業者が設定した SLA を履行するために、サーバやネットワーク等の性能、セキュリティ、データ管理等の項目ごとにサービス目標値を表したものである。例えば、性能の項目として、SLA を月間稼働率 99%以上としていた場合、SLO も月間稼働率 99%以上の数値目標を設定していなければ意味がないことになる。セキュリティの項目の SLO としては、公的認証取得や脆弱性対応等が挙げられる。

告代表者Bは、ホームページにハッカー等が侵入する危険について認識していたことが明らかであり、また、原告は、インターネット通信には情報の改変、破壊の危険があり、その危険は予見可能であったことを認めているのであるから、原告は、インターネット通信固有の原因により本件ファイルが消滅する危険は予見していたと判断され、本件ファイルの消滅という結果発生に対する予見可能性が十分に肯定され、過失相殺の適用を肯定する上での支障は到底認められない」と判断している。その上で、「原告の過失……の内容及び程度に、被告の過失の内容及びその程度、原告の損害の額、その他本件に表れた諸般の事情を斟酌すれば、過失相殺として原告の損害……の 2 分の 1 を減額するのが相当である」と判示した。

（4）行政規律、罰則等

データ管理事業者が電気通信事業者に該当する場合、当該データは事業法第 4 条第 1 項に規定する通信の秘密の保護対象となり得、その消失については通信の秘密の漏えいと判断され得る。漏えいが発生した際、データ管理事業者の業務の方法に関して、通信の秘密の保護に支障があるなどの過失が認められる場合には、同法第 29 条第 1 項第 1 号の規定に基づき、当該データ管理事業者は、業務の方法の改善その他の措置をとるべきことを命じられることがある。この命令に従わない場合には、200 万円以下の罰金に処せられる（同法第 186 条第 3 号、第 190 条第 2 号）。

また、この漏えいが、電気通信事業者たるデータ管理事業者の従業員等が故意に行ったと認められる場合には、事業法第 179 条第 2 項の規定に基づき、3 年以下の拘禁刑又は 200 万円以下の罰金に処せられ、当該事業者も 200 万円以下の罰金に処せられる（同法第 190 条第 2 号）。なお、故意による漏えいは、未遂も処罰の対象である（同法第 179 条第 3 項）。

3．参考資料（法令・ガイドラインなど）

本文中に記載したもののほか、

- 民法第 400 条、第 665 条、第 648 条第 1 項、第 709 条
- 商法第 512 条、第 593 条
- 経済産業省「SaaS 向け SLA ガイドライン」平成 20 年
- 電子商取引準則 324 頁以下

4．裁判例

本文中に記載のとおり

Q62 電子メールの誤送信

電子メールの誤送信や郵送送付先の誤り等、送信者側の過失により情報漏えいした場合、漏えい対策として、受信者に対して一定の要請（返却要請、削除要請、削除確認、現物確認等）を行うが、このような要請を受信者が拒否したため漏えい対策がとれずに二次被害が出た場合又はそのおそれがある場合、受信者に対して取り得る法的措置はあるか。

タグ：不正競争防止法、民法、営業秘密を示された者、電子メール、誤送信

１．概要

初動対応として、まずは誤送信先に直ちに連絡し、送付した電子メールの削除等を求めることが重要である。誤送信した電子メールの受信者に対して、誤って送信された場合の「電子メール守秘文言」は、当事者間の合意ではなく一方的な条件等であるため、強制力を持たせることはできないことに留意が必要である。

誤送信された情報が不正競争防止法上の営業秘密に該当するときは、当該情報について信義則上許されない使用や開示が行われた場合は、当該受信者に不法行為責任が発生する可能性があるほか、誤送信電子メールの文面や受信者の業務等を総合的に考慮する必要はあるものの、受信者が、当該情報が送信者の営業秘密であることを認識した上で、当該情報を自ら使用し若しくは第三者に開示した場合又はそのおそれがある場合には、送信者は、不正競争防止法に基づき、受信者に対して、差止請求や損害賠償請求等の措置を講じられる可能性がある。

２．解説

（１）電子メールの誤送信と個人データの漏えい等について

一般論として、電子メールを誤送信してしまった場合の初動対応としては、誤送信先に直ちに連絡を行い、誤送信した電子メールの削除を求めるなどすることが重要である。

特に個情法との関係では、電子メールの誤送信があり、そこに個人データが含まれていた場合[1]、誤送信した相手方から、メールに含まれる個人データを閲覧せずに削除した旨の申告を受けるなどして、相手方が当該メールを削除するまでの間に当該個人データを閲覧していないことを確認した場合は、そもそも「漏えい」に該当しないと解されている（個情法ガイドライン（通則編）3-5-1-2、個情法 QA6-2 参照）。したがって、誤送信先に対して直ちに連絡を行い、誤送信した電子メールの削除を求めるなどして漏えいの有無を確認することが重要といえる。

[1] 企業が保有する情報が漏えいした場合の対応については、Q57 を参照されたい。

（２）電子メール守秘文言

電子メール守秘文言とは、電子メールの誤送信があった場合に備えて、送信する電子メールに以下のような文言を本文の末尾に追記することである。

> この電子メール（添付ファイル等を含む）は、宛先として意図した特定の相手に送信したものであり、秘匿特権の対象になる情報を含んでいます。もし、意図した相手以外の方が受信された場合は、このメールを破棄していただくとともに、このメールについて、一切の開示、複写、配布、その他の利用、又は記載内容に基づくいかなる行動もされないようにお願いします。

契約は原則として当事者間の合意をもって成立するため、電子メールを一方的に送付し、末尾に追記した守秘文言に記載された内容に強制力を持たせることはできない。誤送信先の受信者が、その情報を保有する行為自体に違法性はないため、削除等を強制することはできず、任意の協力が得られない限り、誤送信した電子メールを削除することは困難である。ただし、誤送信された情報が営業秘密等に該当する情報であることを認識した場合には、後述するように信義則上の義務が生じると解する余地があるため、その限りにおいて有効であると考えられる。

（３）営業秘密侵害

営業秘密を保有する事業者（以下、本項において「営業秘密保有者」という。）からその営業秘密を示された者が、不正の利益を得る目的又は損害を加える目的で、営業秘密を使用する又は第三者に開示する行為は、不正競争行為となる（不正競争防止法第 2 条第 1 項第 7 号）。ここで、「営業秘密を示された」とは、「その営業秘密を不正取得以外の態様で営業秘密保有者から取得する場合」をいうと解されており[2]、「具体的には、営業秘密保有者から営業秘密を口頭で開示された場合や手交された場合、営業秘密へのアクセス権限を与えられた場合、営業秘密を職務上使用している場合などをいう」とされている[3]。

「営業秘密を示された」ことについて、上記具体例のほか広く解することにより、誤送信によって保有者から営業秘密の開示を受けた場合も「営業秘密を示された」に当たるとする余地はあると考えられるが、一方で、偶発的かつ一方的に誤送信メールを送信されたことにより、はじめて営業秘密であることを認識した者に対して営業秘密に関連する規律を課すことの妥当性も考慮する必要がある。

したがって、誤送信電子メールの受信者が、当該メールに送信者の営業秘密が含まれていることを認識した上で、当該営業秘密を自ら使用し若しくは第三者に開示した場合又はそのおそれがある場合に、それを不正競争防止法における営業秘密侵害行為として法的措置をとることができるか否かについては、当該メールを受信した者が「営業秘密を示された者」にあたるかどうかを含め、当該メールの文面や受信者の業務等の各種事情を総

[2] 逐条不正競争防止法 104 頁以下参照。
[3] 逐条不正競争防止法 104 頁以下参照。

合的に考慮した上で個別具体的に判断する必要があるが、当該メールの送信者としては、不正競争防止法に基づき、受信者に対して、差止請求や損害賠償請求等の措置を講じることができる可能性がある。

なお、誤送信電子メールの受信者が不正競争防止法における営業秘密の侵害行為に該当しない場合であっても、当該受信者が誤送信された情報を営業秘密であると認識した場合には、その情報を使用開示して送信者に損害を加えてはならないことについての信義則上の義務が発生すると解する余地がある。この場合、当該受信者が、企業に対して損害が及ぶことを認識しつつ、営業秘密を使用したり、第三者に開示したり、不特定多数の者が閲覧できるようにインターネット上に公開したりすれば、当該受信者に対して不法行為責任を問い得る。

企業としては、営業秘密を誤送信してしまった場合に、受信者に対して当該企業に損害を加えてはならないとする信義則上の義務が発生するように、送信された情報が送信者の営業秘密であると認識できる状態にしておくことが重要であると考えられる。その上で、営業秘密が誤送信された事実が明らかになった段階で、受信者に対して速やかに削除要請をするとともに、当該情報は送信者の営業秘密であるから受信者は当該情報を使用し又は第三者に開示しないように申し入れる必要があろう。

なお、電子メールにファイルを添付する方法においては人為的ミスによる誤送信が発生するリスクは避けがたいため、例えば、ファイル共有サービス等を利用することも検討に値する。

（4）情報記録媒体物の返還請求

誤配送された書類等の情報記録媒体については、送信者にその所有権がある場合には、送信者は受信者に対して、所有権に基づき情報記録媒体の返還を請求する権利を有する。

3. 参考資料（法令・ガイドラインなど）

・不正競争防止法第 2 条第 1 項第 7 号
・民法第 709 条
・逐条不正競争防止法 104 頁以下

4. 裁判例

特になし

Q63 データ漏えい時の損害賠償額の算定

重要なデータ等の漏えいが起こった場合の損害賠償額はどのように算出されるのか。

タグ：民法、不正競争防止法、損害賠償額

１．概要

個人情報漏えい事案の場合、漏えいした個人情報の主体たる本人から、個人情報の管理者に対して、プライバシー権侵害に基づく損害賠償請求が行われることが想定される。損害額の算定に当たっては、プライバシー侵害の程度、すなわち、①漏えいした個人情報の内容と、②漏えいの態様によって、金額が変動してくると考えられる。なお、もちろん、クレジットカード情報漏えい等に伴い、カード不正使用による実損害が生じた場合等においては、当該実損害も損害額となる。

また、営業秘密等漏えい事案の場合、漏えいした営業秘密の主体たる企業から、営業秘密の漏えい者に対して、不正競争防止法に基づく損害賠償請求が行われることが想定されるが、漏えいによる損害の立証に困難が伴うことから、不正競争防止法第 5 条は、損害額の算定・推定に関して「侵害品の譲渡数量又は侵害者により提供された役務の数量のうち被侵害者の販売又は提供の能力に応じた数量に、被侵害品等の単位数量当たりの利益額を乗じて得た額及び当該侵害に係る商品等表示の使用等により受けるべき金銭の額に相当する額を損害額とする算定方法」、「侵害者の利益を被侵害者の損害額と推定する方法」、「使用料相当額を損害額とする方法」の 3 つを設けている。

なお、委託先企業が情報漏えいを行った場合、委託元企業は、委託先企業に対して、契約違反を理由とした損害賠償責任の追及が可能である。その場合、損害賠償請求の内訳としては、①委託元企業が情報漏えいの被害者に対して支払った損害賠償額、②情報漏えいに関する事故対応費用、③委託元企業自体の信用毀損による損害、④その他、委託先企業の情報漏えい行為に起因する損害が考えられる。

２．解説

（１）問題の所在

個人情報、営業秘密及び限定提供データ等の重要なデータの漏えいが起こった場合の損害賠償額がどのように算出されるのかが問題となる。

（２）個人情報漏えい事案

個人情報漏えい事案の場合、漏えいした個人情報の主体たる本人から、個人情報の管理者に対して、プライバシー権侵害に基づく損害賠償請求が行われることが想定される。当該請求において想定される損害としては精神的損害が考えられるが、その損害額算定方

法を検討するに当たっては、実際に精神的損害の金額評価が争われた以下の 4 つの事件についての裁判例が参考になる。

ア　大阪高判平成 13 年 12 月 25 日判自 265 号 11 頁（原審：京都地判平成 13 年 2 月 23 日 判自 265 号 17 頁）

被告（京都府宇治市）が、その管理する住民基本台帳のデータを使用して乳幼児健診システムを開発することを企画し、その開発業務を民間業者に委託したところ、再々委託先のアルバイト従業員が住民約 22 万人の住民基本台帳データを不正にコピーしてこれを名簿販売業者に販売し、同名簿販売事業者がこれをさらに販売した事案である。漏えいデータは、住民番号、住所、氏名、性別、生年月日、転入日、転出先、世帯主名、世帯主との続柄等であり、これらの各データは個人ごとに整理されたものであった。宇治市の住民数名が、当該データの流出によって精神的苦痛を被ったと主張して、宇治市に対し、プライバシー権侵害を理由として損害賠償（慰謝料及び弁護士費用）の支払を求めた。請求額は、1 人当たり、慰謝料 30 万円、弁護士費用 3 万円であった。

大阪高裁は、宇治市の損害賠償責任を認め、損害額は、1 人当たり 1 万 5000 円（慰謝料 1 万円、弁護士費用 5000 円）とされた。

イ　最判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁

大学主催の講演会の参加申込者が申込に際して事前登録した氏名、住所、及び電話番号（学生は氏名と学籍番号）につき、大学側が警視庁から警備のために提出要請を受け、本人の同意なしに提出していた事実が発覚した事案である。学生が、大学に対し、プライバシー権侵害を理由に、損害賠償（慰謝料及び弁護士費用）を求め提訴した。請求額は、1 人当たり、慰謝料 30 万円、弁護士費用 3 万円であった。

最高裁は大学の情報提供行為を違法と認定し、その差戻審で、損害額は、1 人当たり 5,000 円（慰謝料 5,000 円、弁護士費用は否定）とされた。

ウ　大阪高判平成 19 年 6 月 21 日（平成 18 年（ネ）1704 号）（原審：大阪地判平成 18 年 5 月 19 日判タ 1230 号 227 頁）

インターネットポータルサイトの運営者とその業務委託先である被告らが、リモートメンテナンスサーバに顧客データベースを保管していたところ、業務委託先の元関係者が、外部から当該顧客データベースに不正アクセスし、約 1100 万件の会員の氏名、住所、電話番号、メールアドレス、ID 等の個人データを流出させた事案である。会員の一部が、被告らに対して損害賠償請求をした裁判で、大阪地裁は、被告らの責任を認め、損害額は、1 人当たり 6,000 円（慰謝料 5,000 円、弁護士費用 1,000 円）とされた。

エ　東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁（原審：東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁）

被告経営のエステティックサロンが、そのウェブサイトにおいて実施したアンケート等を通じて取得した氏名、住所、電話番号、メールアドレス等の個人情報が、インターネット上において第三者による閲覧が可能な状態に置かれ、実際に第三者がそれにアクセスして個人情報を流出させた事案である。なお、流出後、漏えいした個人情報の主体たる本人に対して迷惑メールが送信されるなどの 2 次被害が発生した。原告らは 1 人当たり慰謝料 100 万円及び弁護士費用 15 万円並びに遅延損害金を請求した。

裁判所は、被告の責任を認め、2 次被害を受けた原告には 1 人当たり慰謝料 3 万円と弁護士費用 5,000 円を、2 次被害が認められずかつ被告から既に 3,000 円の支払いを受けたと認められた原告には慰謝料 1 万 7,000 円と弁護士費用 5,000 円を認めた。

オ　大阪高判令和元年 11 月 20 日判時 2448 号 28 頁（最判平成 29 年 10 月 23 日の差戻審）

通信教育等を目的とする企業において、その管理していた年少者の個人情報等が業務委託先の従業員による不正の持ち出しによって流出したことについて、その親が、自らの個人情報が流出したものであるとして当該企業に対して不法行為に基づく損害賠償を求めた。

裁判所は当該企業の責任を認め、1 人当たり慰謝料 1,000 円を認めた。

各裁判例を見る限り、個人情報漏えい事案において精神的損害の金額が争われる場合、被害者らのプライバシー侵害の程度、すなわち、a）漏えいした個人情報の内容と b）漏えいの態様によって、損害額が変動すると考えられる。

まず、a）漏えいした個人情報の内容については、例えばイ、ウの事案のように、氏名、住所、生年月日、性別といった情報が漏えいした場合、各情報は、既に公となっていることも多く、また、本人自ら各情報を公表する機会も多いため、プライバシー侵害の程度としては比較的低いと判断される傾向にある。他方、④の事案のように、エステを受けようとしていることやエステの施術コースといった、通常第三者が知り得ない情報まで漏えいした場合、プライバシー侵害の程度は高いと判断される傾向にある。犯罪歴や病歴等の要配慮個人情報が漏えいした場合には、プライバシー侵害の程度はさらに高いものと判断される可能性がある。

また、b）漏えいの態様については、情報入手者数が多いほど、また、漏えいの態様それ自体の悪質性が高いほど、当該情報漏えいによるプライバシー侵害の程度は高いと判断される傾向にあるものと考えられる。また、例えば、個人情報が保存された記録媒体が他人に売却されたが、当該個人情報が他の媒体に複製される前に当該記録媒体が回収された場合等、漏えいした個人情報を完全に回収できた場合には、プライバシー侵害の程度は低いと判断されるものと考えられるが、当該情報が複製され、メールや SNS、ウ

ェブサイト上で頒布された場合には、もはや当該個人情報の回収自体不可能であることから、プライバシー侵害の程度は高いと判断されるものと考えられる。さらに漏えいした個人情報を利用した嫌がらせメールの送信等の 2 次被害が発生した場合にもプライバシー侵害の程度は高いと判断され、損害賠償額は高くなるものと考えられる。

個人情報漏えい事案における損害賠償額は、これらの各要素を総合的に勘案の上、個々の事例ごとに具体的に決せられることになるものと考えられる。

なお、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）の「インシデント損害額調査レポート　2021 年版」は、2016 年～2018 年のデータに基づく個人情報漏えい時における 1 人当たりの 3 か年平均想定損害賠償額につき 28,308 円としている。また、同じく JNSA の「2018 年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～（速報版）」では、2018 年のデータに基づく個人情報漏えい時における一件当たり平均想定損害賠償額につき 6 億 3,767 万円との試算を公表している。かかる金額は、あくまで JNSA「情報セキュリティインシデントに関する調査報告書別紙第 1.0 版」において示されている算定モデルに従い試算された想定上の数字であり、現実に争われた結果として認められた損害賠償額を反映したものではない点には注意する必要がある。もっとも、同算定モデルは、前掲ア、ウ及びエの裁判例も参考に作成されたものであり、企業において、情報漏えい時に現実的に想定される損害額を検討するに当たってのひとつの目安として参考になる。

（3）営業秘密等の漏えい事案

営業秘密等漏えい事案の場合、漏えいした営業秘密の主体たる企業から、営業秘密の漏えい者に対して、不正競争防止法第 4 条に基づく損害賠償請求が行われることが想定される[1]。当該請求において想定される損害としては逸失利益が考えられるところ、その損害賠償額算定に当たっては、営業秘密等の漏えいの事実と、漏えいした営業秘密等の主体たる企業における売上減少等との間の相当因果関係及びその損害額の立証が必要になる。しかしながら、損害額の立証責任はその請求を行う被害者の側にあるのが原則であり、かつ、営業秘密等の漏えいの事実と営業上の利益の侵害による損害との間の相当因果関係及びその損害額の立証は、一般的にかなり困難である。

そこで、不正競争防止法第 5 条は、被害者の立証の負担を軽減するため、一定の不正競争行為類型に関する損害額について、その推定規定を設けている。営業秘密等の漏えいに関するものとしては、具体的には以下のとおりである。

① 侵害品の譲渡数量に被侵害品の単位数量当たりの利益額を乗じて得た額を損害額とする算定方法（不正競争防止法第 5 条第 1 項[2]）

[1] なお、不正競争防止法第 4 条の規定は、民法第 709 条に基づく損害賠償請求を排除するものではないため、民法第 709 条に基づく損害賠償請求を行うことも許容される。

[2] 営業秘密に係る不正競争行為のうち技術上の秘密に関するもの（不正競争防止法第 2 条第 1 項第 4 号～第 9 号及び第 10 号）が漏えいしたケース、又は、限定提供データに係る不正競

侵害者が営業秘密侵害行為に係る物又は役務を譲渡・提供したときは、その譲渡・提供した物・役務の数量（以下、本項において「譲渡等数量」という。）のうち被侵害者の販売又は提供の能力に応じた数量（その全部又は一部に相当する数量を被侵害者が販売又は提供をすることができないとする事情があるときは、当該事情に相当する数量）に、被侵害者がその侵害行為がなければ販売することができた物又は提供することができた役務の単位数量当たりの利益の額を乗じて得た額及び以下の区分に応じてそれぞれの行為に対して受けるべき金銭の額に相当する額を、被侵害者が受けた損害の額とすることができる。

イ） 第 2 条第 1 項第 1 号又は第 2 号に掲げる不正競争　当該侵害に係る商品等表示の使用

ロ） 第 2 条第 1 項第 3 号に掲げる不正競争　当該侵害に係る商品の形態の使用

ハ） 第 2 条第 1 項第 4 号から第 9 号までに掲げる不正競争　当該侵害に係る営業秘密の使用

ニ） 第 2 条第 1 項第 11 号から第 16 号までに掲げる不正競争　当該侵害に係る限定提供データの使用

ホ） 第 2 条第 1 項第 22 号に掲げる不正競争　当該侵害に係る商標の使用

② 侵害者の利益を被侵害者の損害額と推定する算定方法（不正競争防止法第 5 条第 2 項[3]）

侵害者が当該侵害行為により利益を得ているときは、その利益の額は、被侵害者が受けた損害の額と推定する。

③ 使用料相当額を損害額とする算定方法（不正競争防止法第 5 条第 3 項[4]）

当該侵害に係る営業秘密又は限定提供データの使用に対して受けるべき金額に相当する金額（ライセンス料相当額）を、自己が受けた損害の額とする。

また、経済産業省は、ウェブページ「営業秘密~営業秘密を守り活用する~」において営業秘密に関係する基本資料を取りまとめている。その中の経済産業省知的財産政策室「営業秘密の保護・活用について」（平成 29 年 6 月）において、営業秘密の漏えいにより数百億円規模の訴訟が提起された事例が挙げられている。具体的には、日本の大手鉄鋼メーカーの元従業員と、外国競合企業が共謀して、高級鋼板の製造技術といった営業秘密を、当該競合企業が不正に取得したとして、当該鉄鋼メーカーが当該競合企業に対して約 1,000 億円の損害賠償請求（300 億円の和解金で解決）を行ったケースや、大手電機メーカーの業務提携先の元技術者が、無断複製したフラッシュメモリに関する営業秘密を、外

争行為（不正競争防止法第 2 条第 1 項第 11 号～第 16 号）により限定提供データが漏えいしたケース。

[3] 営業秘密に係る不正競争行為及び限定提供データに係る不正競争行為による情報漏えい全て。

[4] 営業秘密に係る不正競争行為（不正競争防止法第 2 条第 1 項第 4 号～第 9 号）及び限定提供データに係る不正競争行為（不正競争防止法第 2 条第 1 項第 11 号～第 16 号）による情報漏えい全て。

国競合企業に対して提供したとして、当該電機メーカーが当該競合企業に対して約 1,100 億円の賠償請求(330 億円の和解金で解決)したケース等がある。ここからわかるように、営業秘密が漏えいした場合には、巨額の損害を招くことが想定される。

（4）委託先に対する損害賠償請求

委託先企業が情報漏えいを行った場合、委託元企業は、委託先企業に対して、契約違反を理由とした損害賠償責任の追及が可能である。その場合、損害賠償請求の内訳としては以下のものが考えられる。

① 委託元企業が、情報漏えいの被害者（営業秘密等の漏えい事案においては被害企業等）に対して支払った損害賠償額
② 上記①に関連して訴訟手続等が行われた場合の合理的な訴訟費用
③ 情報漏えいインシデント対応費用（プレスリリース、苦情対応、謝罪等）
④ 委託元企業自体の信用毀損による損害
⑤ その他、委託先企業の情報漏えい行為に起因する損害

委託元企業が、情報漏えいを行った委託先企業に対して損害賠償請求を行い、これが認められた事例として、東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁が著名である(Q52 も参照)。本件は、ウェブサイト上で通信販売を営んでいる原告（委託元企業）が、被告（委託先企業）との間で、原告のウェブサイトにおける商品の受注システムの設計、保守等の委託契約を締結したところ、被告が製作したアプリケーションが脆弱であったことにより、外部から「SQL インジェクション」というアプリケーションの不備を利用してデータベースを不正に操作する攻撃を受け、上記ウェブサイトで商品の注文をした顧客のクレジットカード情報が流失し、原告による顧客対応等が必要となったために損害を被ったとして、被告に対し損害の賠償を求めた事案である。判決は、その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたとし、被告は、当該個人情報の漏えいを防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていたところ、これを怠ったとして、被告の損害賠償責任を認めた。

このような委託先に対する損害賠償請求事案においては、委託先企業は、特定のセキュリティ対策は債務の内容ではなかったという主張のほか、委託元企業自身による義務違反等もあったとして過失相殺（民法第 418 条）等を主張することが考えられる。また、①情報漏えいの被害者に対して払った損害賠償額の合理性、③情報漏えいインシデント対応費用の合理性や、④情報漏えいと委託元企業自体の信用毀損による損害との相当因果関係の有無等については争いになることも多い。

3．参考資料（法令・ガイドラインなど）

・民法第 416 条、第 709 条、第 710 条、第 715 条

・不正競争防止法第 4 条、第 5 条
・JNSA「2018 年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～（速報版）」
・JNSA セキュリティ被害調査ワーキンググループ「情報セキュリティインシデントに関する調査報告書別紙第 1.0 版」（平成 29 年 5 月 17 日）
・JNSA セキュリティ被害調査ワーキンググループ「インシデント損害額調査レポート 2021 年版 Version1.02」（令和 3 年 9 月 10 日）

４．裁判例

本文中に記載のとおり

Q64 データを紛失・消失した場合における損害額

他者のデータを紛失・消失した場合、損害賠償額はどのように算出されるのか。

タグ：民法、データ、紛失、消失、滅失、損害賠償額

１．概要

情報媒体に関する保守契約などに損害額を制限する旨の定めがある場合でも、データを紛失・消失した者に故意・重過失があれば、当該定めは適用されない可能性があるので注意が必要である。裁判例には、データ修復に要する費用を算出して損害額を算定したものがある。

２．解説

情報媒体が債務不履行・不法行為等によって滅失・損傷した場合に、責任が成立すると認められると、「通常生ずべき損害」及び、「特別の事情によって生じた損害であって……当事者がその事情を予見すべきであった」損害について損害賠償責任を負担することになる（民法第 416 条）。これらの「損害」を考える上では、情報媒体の価値をどのようにして算定するかが問題になる。

なお、情報媒体に関する保守契約などには損害額を制限する旨の定めが置かれていることが多いが、データを紛失・消失した者に故意・重過失があれば、損害額は制限されないと判断され得ること（Q52、Q61 参照）、また、当該情報についてバックアップを取っていなかったことを理由として過失相殺がなされ得ること（Q61 参照）に留意が必要である。

理論的に考えると、認められるべき損害賠償額は、①媒体の価値であるという考え方と、②①に加えて情報の価値を考慮する考え方があり得る。

裁判例には、運送人が情報媒体を滅失した場合の損害賠償責任に関して、データ修復作業の経済的価値を損害額として認めたものがある。これは、②の考え方に立つことを前提として、情報の価値はそれ自体としては算定できないため、失われた情報を復元する作業のためのコストによって算定したものと思われる。そして、当該コストは「通常生ずべき損害」として認められている。

このような裁判例は、一般論として、①の考え方を排除するものではないであろう。例えば、滅失・損傷したデータが媒体に収納された状態で取引の対象となるような場合（例えば、汎用ソフトウェアの CD-ROM による販売）は、その取引価格を鑑定等の方法によって認定し、損害額とすることもあり得ると思われる。

なお、フロッピーディスクが運送中に紛失したという事案で、データ修復作業のコストが損害賠償額と認められた結果、かえって、フロッピーディスクが高価品とされ、運送人

が明告を欠いていたこと（商法第 575 条、第 576 条、第 577 条、国際海上物品運送法第 8 条参照）を理由として責任を免れることになったという裁判例がある。

３．参考資料（法令・ガイドラインなど）

本文中に記載したもののほか、

・民法第 415 条、第 709 条

４．裁判例

・神戸地判平成 2 年 7 月 24 日判時 1381 号 81 頁・判タ 743 号 204 頁

運送中にデータを記録したフロッピーディスクを紛失した場合において、運送人に高価品である旨の明告がなされていないとしても、運送人に過失があれば不法行為に基づく損害賠償請求ができると判断した事例。

・広島地判平成 11 年 2 月 24 日判タ 1023 号 212 頁

PC のディスク内の情報を誤って削除された場合において、情報のバックアップを怠ったことにつき過失相殺を認めた事例。

・東京地判平成 13 年 9 月 28 日（平成 12 年（ワ）第 18753 号・平成 12 年（ワ）第 18468 号）

保管の対象が有体物ではなく電子情報から成るファイルである場合であっても、保管者は、サーバにおいて当該ファイルを消滅させないように注意すべき義務を負うと判断した事例。

・岡山地判平成 14 年 11 月 12 日（平成 13 年（ワ）第 967 号）

引越業者が、研究解析資料等の入った PC、MO 等を破損させたことについて、引越業者に損害賠償責任を認めた事例。

・東京地判平成 21 年 5 月 20 日判タ 1308 号 260 頁

レンタルサーバ業者の提供する共用サーバホスティングサービスを、契約者を介して利用してホームページを開設した第三者が、サーバの故障によりプログラム等を喪失した場合において、第三者のレンタルサーバ業者に対する不法行為に基づく損害賠償請求が認められなかった事例。

・東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁

ウェブサイトによる商品の受注システムを利用した顧客のクレジットカード情報が流出した事故につき、システムの設計、製作、保守等の受託業者の債務不履行に基づく謝罪・問合せ等の顧客対応費用、売上損失等の損害賠償責任が肯定された事例。

Q65 インシデント対応における費用負担及びサイバー保険

サイバー攻撃を受けた場合、どのような損害や費用が発生するか。また、サイバー保険ではどのような費用がカバーされるか。

タグ：ランサムウェア、サイバー保険、保険業法

１．概要

サイバー攻撃を受けた場合、主に以下のような損害・費用が発生する。

損害：①工場等の停止に伴う逸失利益、②個人情報の漏えいに伴う損害賠償、③情報管理義務又は秘密保持義務違反等を理由とする取引先等からの損害賠償

費用：④被害原因の調査（デジタル・フォレンジック等）のための専門家費用、⑤情報流出に関する説明・対応等（広報、コールセンター設置等）に関する費用、⑥当局対応その他の訴訟のための専門家（弁護士等）費用、⑦復旧費用、⑧再発防止策の策定・実行に係る費用

これらの損害・費用等をカバーする保険として、保険会社から「サイバー保険」と呼ばれる保険商品が提供されているところ、その補償項目は、概ね以下のとおりである。

・損害賠償補償（第三者からの賠償請求を補償）
・費用損害補償（被保険者に生じた費用を補償）
・利益損害補償（事故がなければ被保険者が得ていたであろう利益（逸失利益）の補償）

２．解説

（１）サイバー攻撃を受けた場合の損害

サイバー攻撃のインシデント発生時には、主に、以下のような損害の発生が想定される。

まず、サイバー攻撃を原因とする当該企業における逸失利益が挙げられる。例えば、サイバー攻撃によって工場等の操業が停止した場合、製品等を製造し、販売することによって得られたであろう利益を得ることができなくなる。工場等の操業の停止のほか、倉庫・配送システム・その他の事業に関するシステム等の停止等によって事業活動に係る機能が停止した場合において、その機能が停止していなければ得られたはずである利益も同様であり、これらは逸失利益に該当する。

次に、サイバー攻撃により、攻撃を受けた企業が保有する個人情報が漏えいした場合、漏えいした個人情報の本人等から当該会社に対する損害賠償請求が行われる可能性がある。サイバー攻撃を受けた企業は、本来被害者の立場ではあるものの、個人情報の管理等について過失があり、それが原因で情報漏えいが発生してしまったという場合は、賠償責任を負うことになる。個人情報を含むデータ漏えい時の損害賠償額に関しては Q63 を参照されたい。

（２）サイバー攻撃を受けた場合の費用

一般的に、サイバー攻撃等のインシデントの発生時には、以下のような費用が生じ得る。

まず、Q58 のとおり、サイバー攻撃の原因調査等のためには、デジタル・フォレンジックによる調査が必要となることが多く、専門性・迅速性等の観点からも、外部の専門業者にその対応を依頼することも多いため、これらの費用が生じる。

次に、サイバー攻撃によって個人情報等が漏えいした場合においては、Q57 のとおり、漏えいした個人情報の本人への連絡や、具体的な態様等によっては当該内容の公表が必要となる場合もある。これらの情報流出に関する説明・対応等に係る費用（広報、コールセンター設置等）も生じ得る。

さらに、個人情報の漏えいが生じた場合には、Q57 のとおり、個人情報保護委員会をはじめとする当局等に対する報告や、その後の対応等について協議等を行う必要が生じる。なお、一般的には、このような対応の要否やその内容の検討に当たっては、弁護士等の専門家に相談することが多いと考えられる。また、上記で述べたような、逸失利益の考え方、個人情報の漏えいに伴う損害賠償請求及び取引先等からの損害賠償請求への対応についても、弁護士等の専門家に助力を求めることが通常と思われ、これらの対応のための専門家に対する委託費用・相談費用等も発生する。

上記に加え、システム等の復旧に費用を要するほか、Q58 のとおり、インシデントへの対応の一環として、同様の事態の発生を防ぐ観点から、再発防止策を策定し、実施する必要があるところ、当該再発防止策の策定・実施に際しては、専門家の関与のほか、各種システム等の購入改修・交換等が必要となる場合も多いため、その費用も発生する。

（３）サイバー保険について

上記（１）、（２）において述べた損害や費用に備えることを目的に、多くの保険会社から、いわゆる「サイバー保険」と呼称される保険商品が提供されている。それぞれの保険商品における補償範囲、補償額及び補償条件は、各商品に係る約款等によって異なるものの、その補償の対象となる項目は、主に以下の 3 つに分類が可能である。

一つ目は、「損害賠償補償」である。これは、被保険者（補償の対象者）が法律上負担する損害賠償金を補償する保険である。（１）の漏えいした個人情報の本人等に対する損害賠償、取引先等との契約関係にある法人に対する損害賠償等の賠償額を填補するものである。

二つ目は、「費用損害補償」である。これは、サイバー攻撃等のインシデントに起因して生じた費用のうち、一定期間内に生じた費用を補償することをその内容とする。具体的には、（２）の原因調査等のための専門家費用や情報流出に関する説明・対応等に係る費用がこれに該当する。なお、個別の保険商品の設計によるものの、弁護士費用（訴訟費用）を、損害賠償補償として填補するものもある。

三つ目は、「利益損害補償」である。これは、当該事故が無ければ被保険者が得ていたであろう利益（逸失利益）を補償するものである。具体的には、（1）の工場が停止して製造・販売できなくなったことで生じた損害や、倉庫や冷蔵庫の機能が停止し、生鮮食品等が売り物にならなくなった場合の損害がカバーされることになる。

なお、インシデント発生時には外部のデジタル・フォレンジック事業者や弁護士といった専門家によるインシデント対応支援が重要となるところ、各社が提供するサイバー保険の中には、これらの外部事業者の紹介サービスが付帯しているものもあり、こうした要素もサイバー保険選択のポイントとなり得る。

（4）サイバー保険とランサムウェアとの関係

ランサムウェア攻撃については、近時、暗号化の前に企業が保有する様々なデータを窃取しておき、その後データの暗号化を行い、データの復号及び窃取したデータの公開取りやめと引き換えに身代金を要求する、いわゆる「二重の脅迫」のパターンが増加している（詳細は Q60 を参照）。被害企業の規模により、数千万円から数億円と高額な身代金が設定される例もあるところ、それをサイバー保険で補填することができるかどうかが問題となり得る。

少なくとも日本の保険会社が提供するサイバー保険においては、ランサムウェアの被害に遭い、データの復旧のために身代金を支払った場合において、その金銭はサイバー保険の補償対象にならないとされており、保険適用外と明示している事例も存在する。一般社団法人日本損害保険協会が公開するウェブサイトでは、「※ランサムウェアの被害によって支払った身代金はサイバー保険の対象になりません。」と言及されている[1]。

3. 参考資料（法令・ガイドラインなど）

本文中に記載のとおり

4. 裁判例

本文中に記載のとおり

[1] https://www.sonpo.or.jp/sme_insurance/cyber-hoken/

Q66 デジタルデータの証拠利用について

IT 関連の損害賠償等に関する民事訴訟において証拠を保全・提出するために留意すべき点にはどのようなものがあるか。

タグ：民事訴訟法、証拠能力、デジタル・フォレンジック

１．概要

民事訴訟法上は、原則としてどのようなものでも証拠とすることができるが、裁判官が書証として証拠調べをするためには、その文書が外観上見読可能なものでなければならない。また、証拠が要証事実を立証するに足る実質的な証拠価値を有すると評価されるためには、その前提として、当該文書が、挙証者が作成者であると主張する者（以下、本項において単に「作成者」という。）の意思に基づいて作成され、他の者により偽造又は改ざんされたものではないことを示す必要がある。

文書ファイルが、プリントアウトするなどして見読可能な状態で証拠として提出される場合、相手方が当該ファイルに収録された情報内容とプリントアウトされた文書の記載内容が異なるなどとして争う場合に備えて、プリントアウトされた文書と元の文書ファイルの記載内容が合致していること、元の文書ファイルが偽造又は改ざんされたものではないことを証明するため、オリジナルデータのコピーなどを保全しておくことが必要である。

２．解説

（１）問題の所在

IT 関連の損害賠償請求訴訟では、事件の性質上、紙媒体の文書や証人など従来型の証拠のほかに、デジタルデータの収録された磁気ディスク等を証拠として提出することが想定される。そのような場合に、従来型の証拠と違ってコピーや改ざんが容易であるという特性があり、またデジタルデータそのままでは読む及び見るということができない（見読性がない）。そこで、どうすれば裁判の証拠とできるかが問題となる。

（２）民事訴訟で提出できる証拠について

民事訴訟においては、原則として証拠能力に制限がないとされている。すなわち、原則としてどのようなものであっても証拠とすることができる。したがって、コンピュータに内蔵されたデータであっても、その意味内容を証拠化することは可能である。

しかし、一般的にデジタルデータを文書ないし準文書（民事訴訟法第 231 条）として証拠化することが可能であるとしても、訴訟上の証拠資料として事実認定の用に供する

ためには、裁判官がその証拠の内容を理解するに足る見読可能性を備えなければならず、さらに、要証事実を裁判官が認定するに十分な証明力を当該証拠が有することが必要である。デジタルデータの意味内容を証拠資料とする場合は、そのいずれについても注意が必要である。

（３）デジタルデータを取り調べる方法

デジタルデータは、そのままでは見読性がなく、情報内容を証拠資料とするためには、何らかの形で裁判官が認識できるようにしなければならない。いわゆる文書ファイルであれば、デジタル情報として記録されている文書の内容をエディタソフトやワープロソフト、表計算ソフト、プレゼンテーションソフトなど、いわゆるビューア・ソフトにより見読可能にして、モニターやプリンタ等に出力する。裁判官は、デジタルデータの収録された磁気ディスク等の情報記録媒体自体が証拠として提出された場合には、モニターに表示された情報を取り調べることになり、プリントアウトされた紙媒体が証拠として提出された場合には、これを取り調べる。

前者の情報記録媒体自体が証拠として提出された場合、当事者は情報記録媒体を準文書（民事訴訟法第 231 条参照）として提出することになる。この場合、裁判所や相手方の求めがあるときは、情報内容を説明した書面を提出しなければならない（民事訴訟規則第 149 条参照）。後者のプリントアウトされた紙媒体が証拠として提出された場合、当事者はプリントアウトされた紙媒体を文書として提出することになり、相手方が情報記録媒体の複製物の交付を求めたときは、複製物を相手方に交付しなければならない（民事訴訟規則第 144 条参照）。

なお、情報記録媒体の内容が言語により表現されている文書ファイルであれば、これを表示し又はプリントアウトすることにより取り調べることが可能だが、ソフトウェアやメタデータのような場合は、プリントアウト等したとしても、それだけで裁判官が理解できるものとはならない。この場合、証拠を提出する当事者は、証拠説明書を裁判所に提出するとともに、証拠の内容及びその意味を説明した書面、場合によっては陳述書などの書証を提出することが考えられる。

（４）デジタルデータの成立の真正を証明するための留意点

デジタルデータを証拠として提出する場合、当事者は、当該データが作成者の意思に基づき真正に成立したものであることを証明しなければならない。

デジタルデータが、例えば電子商取引でやりとりされたものであれば、電子署名法に基づき電子署名の方法が法定されており、これにより成立の真正を証明することが考えられる（Q50 参照）。

しかし、民事訴訟の局面において、提出されるデジタルデータの全てに電子署名が付されていることは少なく、訴訟の相手方が争った場合に、成立の真正を証明する方法が問題となる。

そのような場合に備えて、オリジナルデータのコピーなどを保全しておくことが必要であることはもちろん、当該データの意味内容を証拠資料とするためには、そのデータファイルがいつできたのか、最後に修正を加えられたのがいつかを明らかにするためのタイムスタンプや、修正履歴を記録しておくことが考えられる。

また、上記データが改ざんされていないことを証明し、成立の真正を証明するためには、デジタル・フォレンジック技術[1]を活用することも有用である。

（５）米国の e-Discovery 対策

上記の関連で米国連邦民訴規則における e-Discovery のための証拠保存義務は、渉外取引を行う企業にとってはきわめて重要である。本来存在するはずの文書や電子データを破棄したことが明らかになれば、不利な事実認定のほか、懲罰賠償を含む金銭的制裁及び刑事上の司法妨害罪の対象となりかねないため、注意が必要である。

（６）（参考１）民事裁判の IT 化について

令和 4 年 5 月 18 日、民事訴訟法等の一部を改正する法律が可決成立した（令和 4 年法律第 48 号。以下、本項において「改正民事訴訟法」という。）。これは、民事訴訟手続を全面的に IT 化すること等を内容とするものであり、法制審議会民事訴訟法（IT 化関係）部会において同年 1 月 28 日にとりまとめられた「民事訴訟法（IT 化関係）等の改正に関する要綱案」（同年 2 月 14 日の法制審議会において原案のとおり採択）に基づくものである。同法の施行日は、公布日（同年 5 月 25 日）から起算して 4 年を超えない範囲内において政令日で定める日とされており、一部事項については先行して施行されている。

同法には、「電磁的記録に記録された情報の内容に係る証拠調べ」の規律（改正民事訴訟法第 231 条の 2、第 231 条の 3）が含まれており、これが施行されれば、デジタルデータの情報内容を証拠とするための方法として、（３）に記載のほか、電子データそのものを、インターネットを使用して提出する方法が認められることになる。具体的には、デジタルデータを記録する USB などを記録媒体として提出及び裁判所が定める電子情報システムを利用した提出が認められることになる（改正民事訴訟法第 231 条の 2 第 1 項・第 2 項）。また、文書提出命令に係る規定（民事訴訟法第 220 条乃至第 228 条、及び第 230 条）も準用される（改正民事訴訟法第 231 条の 3 第 1 項）。さらに、文書提出命令が出た

[1] 安冨潔・上原哲太郎編著、特定非営利活動法人デジタル・フォレンジック研究会著「基礎から学ぶデジタル・フォレンジック」（日科技連、2019 年）。デジタル・フォレンジックについては、Q59 を参照されたい。

場合及び裁判所からの嘱託に応じる場合にも、記録媒体の提出及び裁判所が定める電子情報システムを利用した提出が認められる（改正民事訴訟法第 231 条の 3 第 2 項）。

（7）（参考２）弁護士情報セキュリティ規程の策定

上記のような民事訴訟手続の IT 化に伴って、弁護士が事件に関する情報を基本的に電子データとして保有することになることから、日本弁護士連合会において「弁護士情報セキュリティ規程」（会規第 117 号）が策定され、令和 6 年 6 月 1 日から施行されている。

同規程は、「情報セキュリティ」と「取扱情報」の定義を規定し、各弁護士に対して「取扱情報の情報セキュリティを確保するための基本的な取扱方法」を策定する義務を課している。

３．参考資料（法令・ガイドラインなど）

・民事訴訟法第 231 条
・民事訴訟規則第 144 条、第 149 条
・民事訴訟法第 220 条乃至第 228 条、第 230 条
・改正民事訴訟法第 231 条の 2 第 1 項・第 2 項、第 231 条の 3 第 1 項・第 2 項

４．裁判例

デジタルデータの証拠調べが問題となった例として、

・大阪高決昭和 53 年 3 月 6 日高民集 31 巻 1 号 38 頁
　コンピュータ用磁気テープが旧民訴法第 312 条にいう「文書」に該当するとして、文書提出命令の対象になると認められた事例。

Q67 営業秘密等の漏えい事実（情報管理体制含む）及び不正使用行為の立証

被疑侵害者（被告）が特定でき、営業秘密侵害訴訟を提起しようとする場合、営業秘密や限定提供データの不正使用・漏えいに関し、①不正使用・漏えいの事実をどのように立証すべきか、②立証を容易にするために平時からどのような情報管理体制を構築すべきか。

タグ：不正競争防止法、民事訴訟法、営業秘密侵害訴訟、営業秘密、限定提供データ、技術上の秘密、不正使用行為により生じた物、推定規定

１．概要

営業秘密の不正使用については、技術上の秘密を使用する行為等の推定規定、具体的態様の明示義務、訴訟記録の閲覧等制限の申立て、文書提出命令、文書提出命令制度におけるインカメラ手続、秘密保持命令、尋問の公開停止等を活用した立証活動をすることが考えられる。

また、情報漏えいについては、漏えいの事実を把握するために、営業秘密や限定提供データを物理的・技術的に隔離して管理し、当該情報の複製や外部への持ち出しを、客観的に把握できる手段を確保しておくことが望ましい。さらに、漏えいした情報が営業秘密や限定提供データであることを立証するために、あらかじめ、営業秘密や限定提供データの要件該当性を立証できる資料を用意しておくことが望ましい。

２．解説

（１）不正使用及び漏えいの立証について

営業秘密に対する侵害があった場合には、営業秘密侵害訴訟を提起することが考えられる。営業秘密侵害訴訟とは、営業秘密を保有する事業者、すなわち営業秘密保有者（不正競争防止法第 2 条第 1 項第 7 号）が、営業秘密に関する不正競争（同条第 1 項第 4 号～第 10 号）をした、又はしようとすることが疑われる相手方（以下、本項において「被疑侵害者」という。）に対して、不正取得・不正使用・不正開示の差止めを求める訴訟（不正競争防止法第 3 条）、又は不正取得・不正使用・不正開示により生じた損害の賠償を求める訴訟（不正競争防止法第 4 条）をいう。

不正取得・不正開示の立証に向けて、営業秘密を管理・保管していたサーバへのアクセスログの解析や、営業秘密にアクセスし得る端末のイベントログの解析、営業秘密が保管されている鍵付きキャビネットの鍵の保管状況の調査等を行うことが考えられる。また、不正競争の要件として、図利加害目的等の主観的要件が要求されている類型（不正競争防

止法第 2 条第 1 項第 5 号～第 9 号）[1]については、例えば、周囲にインタビューをして被疑侵害者の言動に関する証言を集めたり、被疑侵害者のメールのやり取りをフォレンジックによって解析したりする等して、客観的な証拠を集めて被疑侵害者の主観の立証を試みる（デジタル・フォレンジックの詳細については、Q59 を参照されたい。なお、被疑侵害者が従業員である場合のモニタリングに関する留意点等については、Q29 も参照されたい。）。

また、不正アクセスなどに対しては、コンピュータを解析して証拠を収集するデジタル・フォレンジックを行うことにより証拠を確保することも可能である（詳細については、Q59 を参照されたい。）。さらに、情報を漏えいさせている者が特定できている場合には、捜査当局の協力を得て具体的な流出経路を特定して証拠を確保することも考えられる。

他方、不正使用については、不正取得・不正開示と異なり、「使用」は相手方の支配領域内で行われることから、営業秘密保有者にとっては、相手方が使用したか否かの証拠を収集し難い類型であるといえる。

（２）不正使用に関する推定規定について

そこで、不正競争防止法の平成 27 年改正により、営業秘密の不正使用等の推定に関する規定（第 5 条の 2 第 1 項）（以下、本項において「本推定規定」という。）が新しく設けられ、さらに令和 5 年度改正によって、対象となる行為類型が拡大した（第 5 条の 2 第 2 項乃至第 4 項）。

ア　趣旨

本推定規定の趣旨は、不正使用の証拠を収集し難いことに加え、「技術上の営業秘密」を不正に取得した者については、当該営業秘密を使用することが通常であるとの経験則に基づくものである[2]。

イ　内容

営業秘密保有者（原告）が下記前提事実（①～③の 3 つ全て）の立証に成功した場合、被疑侵害者（被告）による営業秘密の不正使用行為が推定されることによって、立証責任が被告に転換され、被告において当該営業秘密を使用していないことを立証しない限り、不正使用についての責任を負うこととなる。

---

[1] 「不正競争の要件として、主観的要件が要求されている類型（不正競争防止法第 2 条第 1 項第 5 号～第 9 号）」として、第 10 号（営業秘密侵害品の譲渡等行為）を除いているのは、同号の「その譲り受けた時に当該物が不正使用行為により生じた物であることを知らず、かつ、知らないことにつき重大な過失がない者に限る。」という要件が、請求原因事実であるのか、それとも抗弁事実であるのかについて判示した裁判例が見当たらないためである。

[2] 逐条不正競争防止法 186 頁。

① 対象となる情報が営業秘密保有者（原告）の営業秘密であり、生産方法等の技術上の情報であること
② 以下のいずれかを充足すること
(i) 被疑侵害者（被告）による第 2 条第 1 項第 4 号、第 5 号又は第 8 号に該当する不正取得行為があったこと（第 5 条の 2 第 1 項）
(ii) 営業秘密をその営業秘密保有者から示された後に、図利加害目的で、その営業秘密に係る任務に背いて領得したこと（第 5 条の 2 第 3 項）
(iii) 営業秘密を取得した後にその営業秘密について営業秘密不正開示行為が介在等したことを知って、又は重大な過失により知らないで、その営業秘密に係る技術秘密記録媒体等を保有する一定の行為があったこと（第 5 条の 2 第 2 項・第 4 項）
③ 被疑侵害者（被告）が営業秘密保有者（原告）の営業秘密を用いて生産することのできる物を生産等していること

（３）情報漏えいの事実立証のための管理体制

情報漏えいの兆候を把握し、漏えいの疑いを速やかに確認できる体制を整備・実施した上で、情報漏えいの事実そのものに関する証拠を確保する必要がある。そのためには、営業秘密等を物理的・技術的に隔離して管理しておき、情報漏えいの事実を把握しやすくしておく必要がある。このような物理的・技術的管理は、下記（４）の営業秘密の秘密管理性（詳細は Q21）の要件、又は限定提供データの限定提供性及び電磁的管理性を満たすためにも必要な措置である。

具体的な管理方法としては、保管場所の隔離・施錠、アクセス権者の制限、電子データの複製の制限、不正アクセスの防御措置、外部ネットワークからの遮断、保管媒体の持出禁止等の営業秘密に関する裁判例において示された管理方法が挙げられる。

また、不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策ではなく漏えい防止ないし漏えい時に推奨される（高度なものも含めた）包括的対策を示した経済産業省の秘密情報の保護ハンドブックにおいて掲げられているものが参考となる（秘密情報の保護ハンドブックの概要については、Q21 も参照されたい。）。

例えば、秘密情報の保護ハンドブックにおいては、①ルールに基づく適切なアクセス権の付与・管理（社内規程等において、秘密情報の分類ごとに、アクセス権の設定に関するルール（どのような手続きで誰が設定するのかなど）を明確にした上で、当該ルールに基づき、適切にアクセス権の範囲を設定）、②情報システムにおけるアクセス権者の ID 登録（①で決定されたアクセス権者だけが、利用することが許可された電子データ等にアクセスできるように、あらかじめ、従業員等に対して情報システム上の ID を付与し、その ID を認証する（ID を使用する者が本人であることを確認する）ためのパスワード等を設定）、③分離保管による秘密情報へのアクセスの制限（秘密情報が記録された書類・ファ

イルや記録媒体については、保管する書棚や区域（倉庫、部屋など）を分離し、電子データについては格納するサーバやフォルダを分離した上で、アクセス権を有しない者が、その秘密情報を保管する領域にアクセスできないようにする）といった方法が、主として、情報漏えいを防止するための「接近の防御」に資する対策として紹介されており、これらの対策を実施することにより、情報漏えいが生じた際の原因の特定が容易になるので、かかる対策は、事後的に情報漏えいの事実を立証する上でも有用な管理策であると考えられる。

その他、営業秘密の不正取得等を立証するために有効な資料例として以下のものが紹介されている。これらを参考に、平時から、情報漏えい事案発生時に備えた記録を行っておくことが望ましい。

① 漏えいが疑われる者の立場（アクセス権の保有者であったか、会議等で資料を配付された者であったか、外部者であるか）に関する社内記録
② 漏えいが疑われる者が自社従業員である場合には、どのような秘密保持に係る任務を負っていたかが分かる就業規則、秘密保持誓約書
③ 漏えいが疑われる者が委託先である場合、委任契約書、秘密保持契約書
④ 情報持出しの具体的行為態様が分かるアクセスログ、メールログ、入退室記録、複製のログ（なお、従業員に対するモニタリング等に関する留意点等については、Q29 参照。）
⑤ 漏えいが疑われる者の行為目的が窺える他社とのメールや金銭のやりとりに関する書面
⑥ 情報漏えいの発覚の経緯を、社内調査等に基づき時系列的にまとめた文書

また、このような予防措置に加え、情報が外部に流出した場合に備え、情報漏えいの兆候を把握できる手段、すなわち秘密情報の複製や外部への持ち出しを、客観的に把握できる手段を確保しておくことが必要である。例えば、管理場所における監視カメラの設置、電子データの複製履歴の保存、電子メールのモニタリングや過去の送受信メールの保存等の情報漏えい時に流通経路を特定することが可能なシステムの設置などを行うことが考えられる。

さらに、秘密情報の保護ハンドブックにおいては、①秘密情報が記録された媒体の管理等、②コピー機やプリンタ等における利用者記録・枚数管理機能の導入、③印刷者の氏名等の「透かし」が印字される設定の導入、④秘密情報の保管区域等への入退室の記録・保存とその周知、⑤不自然なデータアクセス状況の通知（深夜帯や休日に、複数分野の業務にわたる様々なデータにアクセスし、大量のダウンロードがなされているなど、不自然な時間帯・アクセス数・ダウンロード量を検知した場合に上司等に通知）、⑥PC やネットワーク等の情報システムにおけるログの記録・保存とその周知、⑦秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査が、「視認性の確保」のうち、「事後的に検知されやすい状況を作り出す対策」として紹介されており、参考になる。

その他、秘密情報の保護ハンドブックの第 2 章及び第 3 章にも、保有する情報の把握・評価、秘密情報の決定、秘密情報の分類、対策の選択及びそのルール化について紹介されているので参照されたい。

（4）営業秘密や限定提供データの要件該当性立証のための管理体制

併せて、漏えいした情報が営業秘密や限定提供データに該当することに関する証拠を確保する必要がある。この点、前述のとおり、営業秘密等を物理的・技術的に隔離する管理方法は、営業秘密の秘密管理性の要件を満たすためにも必要な措置である。また、限定提供データの限定提供性（例えば、特定の法人・個人へのアカウントの付与等）及び電磁的管理性（アクセス制限）の要件も、かかる管理方法により確保されることになると考えられる。

その他、秘密情報の保護ハンドブックにおいては、営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料例として以下のものを挙げている。これらを参考に、平時から、情報漏えい事案発生時に備えた記録を行っておくことが望ましい。

情報の管理水準が分かる資料（就業規則、情報管理規程、管理状況に関する社内文書等）

① 漏えいが疑われる者と自社との間で交わされた秘密保持誓約書
② 情報の取扱いに関する社内研修等の実施状況に関する社内記録
③ 特定の情報に対するマル秘マークの付記、アクセス制限、施錠等の情報の管理状況に関する社内記録（教育マニュアル等）
④ 漏えいが疑われる者が、漏えいに係る情報が秘密であることを認識できたことを裏付ける陳述書（社内における実際の管理状況、口頭での情報管理に係る注意喚起の状況、示談文書等）

3．参考資料（法令・ガイドラインなど）

・不正競争防止法第 2 条第 1 項第 4 号～第 10 号、第 2 条第 6 項、第 2 条第 7 項、第 2 条第 11 項、第 3 条、第 4 条、第 5 条の 2、第 6 条、第 7 条、第 10 条、第 13 条、第 21 条第 1 項・第 2 項
・不正競争防止法施行令第 1 条、第 2 条
・民事訴訟法第 92 条、第 223 条第 6 項
・逐条不正競争防止法
・秘密情報の保護ハンドブック
・限定提供データ指針

4．裁判例

特になし

Q68 ドメイン名の不正使用への対抗措置

第三者に、自社の商標やブランド名を含むドメイン名を勝手に使用されている場合などにおいて、企業が取り得る措置はあるか。

タグ：不正競争防止法、サイバースクワッティング、統一ドメイン名紛争処理方針（UDRP）、JP ドメイン名紛争処理方針（JP-DRP）

１．概要

第三者が自社の商標やブランド名を含むドメイン名を勝手に使用する行為は、一般的にサイバースクワッティングと呼ばれる。これは、不正競争防止法第 2 条第 1 項第 19 号に定めるドメイン名に関する不正競争行為に該当し、同法に基づく当該行為の差止請求、行為者に対する損害賠償請求、信用回復措置請求が可能である。しかしながら、不正競争防止法上の解決手段は、ドメイン名の自己への移転請求は認めていないこと、裁判手続による必要があり時間と費用がかかること、行為者が海外所在の場合の執行困難性があることといった問題がある。

そこで、裁判外紛争処理手続として、例えば、UDRP（Uniform Domain Name Dispute Resolution Policy；統一ドメイン名紛争処理方針）や、JP-DRP（JP- Domain Name Dispute Resolution Policy ；JP ドメイン名紛争処理方針）に基づく仲裁手続での解決を図ることが考えられる。また、裁判手続における仮処分にあたる手続である、URS（Uniform Rapid Suspension；統一早期凍結）を活用することも考えられる。

２．解説

（１）問題の所在

自社のロゴマーク・商品名・サービス名などの商標と同様、自社の商標やブランド名を含むドメイン名は企業の重要財産であり、その管理は、ブランド保護戦略上、商標の管理と同様の重要性を持つ。特に、ドメイン名登録は、先願主義・無審査で行われることから、これを悪用して、後で高く売りつけるために他人の商標や名称と同一又は類似のドメイン名を取得するサイバースクワッティングと呼ばれる行為が行われることがある。これにより、正当な権利者のブランドの評判、顧客からの信頼や収益性は危険にさらされ、多額のマーケティング・ブランディング投資の効果が大きく弱体化される結果となり得る。

このような、第三者に、自社の商標やブランド名を含むドメイン名を勝手に使用されている場合などにおいて、企業が取り得る手続の種類・内容が問題となる[1]。

（２）不正競争防止法

サイバースクワッティングに対しては、国内法上、不正競争防止法の規定が抑止力になり得る。具体的には、同法第 2 条第 1 項第 19 号が、「不正の利益を得る目的で、又は他人に損害を加える目的で、他人の特定商品等表示（人の業務に係る氏名、商号、商標、標章その他の商品又は役務を表示するものをいう。）と同一若しくは類似のドメイン名を使用する権利を取得し、若しくは保有し、又はそのドメイン名を使用する行為」を禁止している。

不正競争防止法は、「不正の利益を得る目的」又は「他人に損害を加える目的」（いわゆる図利加害目的）を主観的要件として要求するが、前者は、公序良俗、信義則に反する形で自己又は他人の利益を不当に図る目的を、後者は、他者に対して財産上の損害、信用の失墜といった有形無形の損害を加える目的を、それぞれ指すものと考えられている。いかなる場合に図利加害目的が認められるかについては、個別具体的な事例における裁判所の判断に委ねられることとなるものの、当該目的が認められる行為の例としては、①ある特定商品等表示の正当な権利者に対して、不当な高額で買い取らせることを目的として、当該表示と同一又は類似のドメイン名を先に取得・保有する行為や、②他人の特定商品等表示を希釈化・汚染する目的で当該表示と同一又は類似のドメイン名のもとアダルトサイト等を開設する行為などが当たると考えられる。

また、不正競争防止法は、「他人の特定商品等表示」と「同一若しくは類似」のドメイン名であることを客観的要件として要求するが、この「同一若しくは類似」性の判断についても、個別具体的な事例における過去の裁判例が参考になる。例えば、富山地判平成 12 年 12 月 6 日判時 1734 号 3 頁（名古屋高金沢支判平 13 年 9 月 10 日（平成 12 年（ネ）第 244 号・平成 13 年（ネ）第 130 号）でも判断維持）では、「『JACCS』と『jaccs』とを対比すると、アルファベットが大文字か小文字かの違いがあるほかは、同一である。そして、実際上、小文字のアルファベットで構成されているドメイン名がほとんどであることに照らせば、大文字か小文字かの違いは重要ではないというべきである」と判示された。また、東京地判平成 13 年 4 月 24 日判時 1755 号 43 頁（東京高判平成 13 年 10 月 25 日でも判断維持）では、「被告が本件ウェブサイト上に表示した本件表示は、『J-PHONE』、『ジェイフォン』、『J-フォン』を横書きにしたものであって、本件ウェブサイト上の前記の『J-PHONE』と同一ないし類似するものである」と判示された。

[1] その他、近時は、企業等がドメイン名を廃止した後で、そのドメイン名が関係のない第三者に登録され詐欺サイト等に悪用される可能性が問題となっており、注意喚起等（https://jprs.jp/registration/suspended/）がなされている。

以上の要件を満たす「ドメイン名を使用する権利を取得し、若しくは保有し、又はそのドメイン名を使用する行為」に対しては、不正競争防止法第 3 条に基づくドメイン名の使用差止請求、同法第 4 条に基づく損害賠償請求、同法第 14 条に基づく信用回復措置請求等が可能である。

しかしながら、不正競争防止法に基づく請求においては、差止めの内容としてドメイン名の登録抹消も求め得ると考えられるものの、ドメイン名の自己への移転請求は認められていない。また、一般的に、裁判手続は時間と費用を要し、特に、被告たるドメイン名登録者が海外に所在する場合等には判決を取得してもその執行が困難なケースもあり、必ずしも有効ではない場合があることには留意が必要である。

（３）UDRP 及び JP-DRP

そこで、裁判手続の代替手段として、裁判外紛争処理制度の利用、例えば、UDRP（Uniform Domain Name Dispute Resolution Policy；統一ドメイン名紛争処理方針）や、JP-DRP（JP- Domain Name Dispute Resolution Policy；JP ドメイン名紛争処理方針）に基づく仲裁手続での解決が考えられる[2]。

UDRP は、ICANN（The Internet Corporation for Assigned Names and Numbers）が採択した統一ドメイン名紛争処理方針であり、「.com、.net、.org、.biz、.info、.name」等の gTLD（generic TLD；分野別トップレベルドメイン）及び「.jp .kr .cn .us .uk .fr .ca .au」等の ccTLD（country code TLD；国別トップレベルドメイン）に適用される紛争処理方針である。仲裁機関としては、WIPO（World Intellectual Property Organization；世界知的所有権機関）の仲裁調停センターや、NAF（The National Arbitration Forum；全米仲裁協会）、ADNDRC（Asian Domain Name Dispute Resolution Center；アジアドメイン名紛争解決センター）などがある。

他方、JP-DRP は、JPNIC（一般社団法人日本ネットワークインフォメーションセンター）が採択した JP ドメイン名紛争処理方針であり、「.jp」ドメインに適用される、UDRP 処理方針を日本にローカライズして作成された紛争処理方針である。仲裁機関としては、日本知的財産仲裁センターがある。

以下、UDRP 手続の中でも、WIPO 仲裁調停センターにおける UDRP 手続につき、内容を解説する[3]。なお、JP-DRP の内容も非常に類似している[4]。

---

[2] 沿革としては、当初、ICANN や JPNIC による裁判外紛争処理制度が整備され、紛争の処理が行われていたところ、実体法の整備が必要との意見が各方面から出されたため、平成 13 年の不正競争防止法の改正により、ドメイン名の不正取得等を不正競争の一類型として新たに規制することとなったものである（逐条不正競争防止法 142～145 頁参照）。

[3] なお、WIPO は日本語で情報提供をしているので、参考にされたい（「トップレベル・ドメイン名（ｇTLD ｓ）のための紛争処理手続」（https://www.wipo.int/amc/ja/domains/gtld/udrp/index.html））。

[4] JP-DRP の内容は、日本知的財産仲裁センターの「JP ドメイン名紛争処理」（https://www.ip-adr.gr.jp/business/domain/）を参照されたい。

ア UDRP 手続の特徴

UDRP 手続の特徴としては、簡易・迅速・低費用・非拘束という点が挙げられる。UDRP 手続においては、審理は全て提出書類のみに基づいて行われ、当事者の出席を要する審問等は原則として行われない。また、手続期間としては、WIPO 仲裁調停センターが申立書を受領した日から起算して、通常、3 か月程度で裁定が下される。そして、申立費用についても、例えば、1 つのドメイン名に関して 1 名のパネルでの審理を求める場合には、令和 2 年 2 月現在、1,500 米ドルである。ただし、パネルによる裁定結果に不服の場合には、別途裁判所への提訴が可能となっている点には留意が必要である。

イ UDRP の流れ

UDRP における紛争処理手続の流れは、概要、次のとおりである。なお、申立書や答弁書の提出、その他 WIPO 仲裁調停センターとの各種連絡はメールを通じて行うことが可能である。

（ア）申立書の提出

申立書には、請求内容、当事者名、申立対象たるドメイン名、当該ドメイン名のレジストラ[5]、希望するパネリストの数、申立の根拠などを記載する必要がある。申立人は、申立の根拠として、特に、次の 3 点を主張することが必須であり、かつ、これらの各点を立証する証拠を別途送付する必要がある。

① 申立対象のドメイン名が、申立人の有する商標と同一又は混同を引き起こすほど類似していること
② 登録者が、そのドメイン名登録について権利又は正当な理由がないこと
③ 登録者のドメイン名が悪意で登録かつ使用されていること

どのような場合に「③登録者のドメイン名が悪意で登録かつ使用されている」と認定されるかについては、UDRP 処理方針において、次の事項が例示列挙されている。

- 正当な権利者に対して登録実費金額を越える対価で転売等することを目的として当該ドメイン名を登録しているとき
- 正当な権利者による当該ドメイン名の使用を妨害するために登録し、そのような妨害行為が複数回行われているとき
- 正当な権利者の事業を混乱させることを主たる目的として、当該ドメイン名を登録しているとき
- ユーザによる正当な権利者と登録者との誤認混同をねらって、当該ドメイン名を登録・使用しているとき

WIPO 仲裁センターは申立書のひな形や UDRP の過去の裁定結果を公表しているため、申立書の作成・提出に当たっては、事案に応じた各論点の要件立証のための要

[5] レジストラとは、ドメイン名登録機関のことである。

素を検討する上で、これらの資料を十分に分析することが重要である。なお、UDRP の手続言語は、原則として、登録者とレジストラとの間の登録合意書の言語となる。

申立書は、WIPO 仲裁調停センターと、登録者たる被申立人及びそのレジストラに対して提出される必要がある。

（イ）手数料納付

申立書提出後、10 日以内に、銀行振込・クレジットカード又は WIPO アカウントからの引落しの方法により料金を支払う。なお、料金の詳細は WIPO のウェブサイトを参照されたいが、前述のとおり、ドメイン名 1 つにつきパネリスト 1 名での実施を求める場合、本稿作成日現在は 1,500 米ドルとされる。

（ウ）登録者たる被申立人への申立通知

申立書が提出されると、WIPO が申立書等の方式審査を実施し、申立書に不備がないこと及び手数料納付が完了していることを確認する。仮に申立書に不備がある場合には 5 日以内に補正する必要があるが、特段問題がない場合には、WIPO から登録者たる被申立人に対して正式に申立通知が行われる。

（エ）答弁書の提出

申立通知から 20 日以内に、登録者たる被申立人は、自らによるドメイン名登録が不正の目的で行われたものではないこと等、申立書に対する見解を主張した答弁書を WIPO 仲裁センターに対して提出するとともに、申立人に対しても送付する必要がある。仮に登録者からの答弁書が提出されない場合、このことを前提に判断がなされる。

（オ）パネリストの指名

UDRP 手続における審理・裁定は、WIPO 仲裁調停センターによって指名されたパネリストで構成されるパネルにより行われる。パネリスト候補者は、世界各国の弁護士・弁理士・大学教授等の有識者から構成され、その一覧は、WIPO 仲裁調停センターのウェブサイトで公表されている。パネリストの人数は 1 名又は 3 名であり、両当事者によりその人数が決定されるが、1 名構成のパネルで審理される事案が多数である。

（カ）パネルによる審理・裁定

パネリスト指名から 14 日以内に、パネルによる審理の結果として、ドメイン名の移転・取消・登録維持の裁定が下される。UDRP 手続における救済内容はドメイン名登録の移転・取消に限定されており損害賠償請求は認められていないため、金銭賠償を求めたい場合には、別途、訴訟提起を検討する必要がある。

（キ）裁定結果の通知と裁定実施

パネルによる裁定結果はドメイン名のレジストラへ通知され、当該レジストラによって裁定実施がなされる。ただし、裁定結果の通知から 10 日間は、裁定実施は保

留される。この保留期間内に、登録者たる被申立人から裁判所への提訴が行われなければ裁定を実施し、提訴の連絡があれば裁定実施を見送る運用である。

ウ UDRP 手続のポイント

UDRP 手続の利用に当たっては、申立書作成に先立って、対象ドメイン名情報（対象ドメイン名、レジストラ、登録者、登録日、適用される紛争処理方針）と UDRP 手続による移転・取消請求認容の見込みを検討する必要がある。これに当たっては、WHOIS 検索の活用、並びに WIPO における申立書雛形[6]及び過去の裁定例検索[7]の活用が望まれる。

（４）URS

また、裁判手続における仮処分にあたる手続である、URS（Uniform Rapid Suspension; 統一早期凍結）を活用することも考えられる。URS とは、UDRP 同様、ICANN が採択した手続であり[8]、2013 年に追加された新 gTLD（New Generic Top-Level Domain）と呼ばれるドメイン名について、これを保護するために活用が可能である。URS は、明確な侵害に対して、従来の UDRP と比較してもさらに安価に、かつ迅速に解決できる正当権利者にとっての救済措置とされる。

URS 申立ての要件は、UDRP と同様であり、ドメインの不正目的による登録・使用が行われていることの主張立証が必要になる。

URS と UDRP の違いは、UDRP はドメイン名の移転・取消を求めることができるが、URS はドメイン名の一定期間の凍結のみを求めることができる点である。ドメイン名の移転や取消を求めることができない代わりに、URS では、申立受領後の事務的なチェックが済み次第、迅速にドメイン名の登録内容がロックされ、ドメイン名の移転やレジストラ変更等ができない状態になり、かつ、その後迅速に裁定が行われ、申立人の主張が認められれば、ドメイン名の使用の差止が実現できる（具体的には、当該ドメイン名を持つウェブサイトなどにアクセスしても差止中である旨表示する紛争処理機関のウェブサイトにリダイレクトされるようになる）。

仲裁機関としては、本稿作成日現在、前述の NAF（全米仲裁協会）と ADNDRC（アジアドメイン名紛争解決センター）に加え、MFSD srl（イタリアの知的財産紛争解決機関）がある。

３．参考資料（法令・ガイドラインなど）

・不正競争防止法第 2 条第 1 項第 19 号、第 3 条、第 4 条、第 14 条
・Uniform Domain Name Dispute Resolution Policy

---

[6] WIPO 申立書雛形（http://www.wipo.int/amc/en/domains/complainant/）
[7] Search WIPO Cases and WIPO Panel Decisions（https://www.wipo.int/amc/en/domains/search/）
[8] https://newgtlds.icann.org/en/applicants/urs/

・JP ドメイン名紛争処理方針
・Uniform Rapid Suspension

４．裁判例

本文中に記載したもののほか、

・東京高判平成 14 年 10 月 17 日（平成 14 年（ネ）第 3024 号）最高裁ウェブサイト
JPNIC が定めていた「JP ドメイン名紛争処理方針」第 4 条 c に基づき、JP ドメイン名を使用する正当な権利を有するかどうかが争われた事例。

・知財高判平成 29 年 9 月 27 日（平成 29 年（ネ）第 10051 号）最高裁ウェブサイト
控訴人がドメイン名を使用する行為について、不正競争防止法第 2 条第 1 項第 13 号に定める「不正の利益を得る目的」があったと認定した事例。

・知財高裁中間判決令和元年 5 月 30 日（平成 30 年（ネ）第 10081 号・平成 30 年（ネ）第 10091 号）最高裁ウェブサイト
周知又は著名な商品名等の高い顧客吸引力を利用して、不当に利益を上げる目的で、当該商品名に類似したドメイン名を使用することが、不正競争防止法第 2 条第 1 項第 13 号所定の不正競争行為に該当すると判断した事例。

Q69 発信者情報開示

営業秘密などの企業が保有する情報がインターネット上で公開されてしまった場合、どのような対処を行うことができるか。

タグ：情報流通プラットフォーム対処法、不正競争防止法、発信者情報開示請求、削除請求

１．概要

公開された情報が不正競争防止法上の営業秘密に該当するときは、当該企業は、当該情報をインターネット上に公開した者（以下、本項において「発信者」という。）に対して、不正競争防止法に基づき差止めを請求し得る。また、この場合には、発信者の当該情報の開示行為により損害を被った場合は、損害賠償を請求し得る。

ただし、インターネットの匿名性から発信者が不明な場合は、まず、発信者を特定するための情報の開示請求をした上で、発信者を特定することにより、発信者に対する上記各請求をすることが可能となる。

また、発信者に対する差止請求又は発信者の特定を待っては、損害が拡大する場合には、一次的に当該情報が公開されているウェブサイト等を提供するプロバイダ等に対して、当該情報の送信防止措置を講ずるよう依頼のうえ、インターネット上に公開された情報を非公開にすることが有効となる。

２．解説

（１）営業秘密侵害

営業秘密を保有する事業者（以下、本項において「営業秘密保有者」という。）からその営業秘密を示された者が、不正の利益を得る目的又は損害を加える目的で、営業秘密を使用する又は第三者に開示する行為は、不正競争行為となる（不正競争防止法第 2 条第 1 項第 7 号)。

したがって、インターネット上で公開されてしまった営業秘密保有者の情報が秘密管理性、有用性、非公知性の要件（Q21 参照）を満たしている場合には、その発信者が、不正の利益を得る目的又は損害を加える目的で当該情報を開示する行為は、不正競争防止法第 2 条第 1 項第 7 号の不正競争行為に該当し、営業秘密保有者は発信者に対して損害賠償請求や差止請求等の請求をすることが考えられる。

なお、発信者の開示行為に不正の利益を得る目的や損害を加える目的が認められるかという点については、インターネット上に公開した情報が営業秘密保有者の営業秘密であることを認識した上で、当該情報を営業秘密保有者に無断で開示した場合には、少なくとも発信者には損害を加える目的が存在すると認められることが多いと考えられる。

（２）発信者情報開示請求

発信者が不明である場合は、営業秘密保有者が損害賠償請求や差止請求等の請求をする相手方自体が不明であることから、まず、その発信者を特定する必要がある。

インターネット上のウェブサイト等に掲載されることにより自己の権利を侵害された者は、①「当該開示の請求に係る侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき」であって、②「当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき」は、その情報を流通させた特定電気通信の役務提供者に対して、当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるもの[1]をいう（情報流通プラットフォーム対処法第 2 条第 10 号）。ただし、特定発信者情報の開示を請求する場合には、さらに補充的な要件を満たす必要がある。）の開示を請求することができる（情報流通プラットフォーム対処法第 5 条第 1 項）[2]。なお、情報流通プラットフォーム対処法における「権利の侵害」とは、同法において独自に定義されるものではなく、個人法益の侵害として、民事上の不法行為等の要件としての権利侵害に該当するものとされており[3]、裁判例の存在は確認されていないが、営業秘密の開示による不正競争行為についても、その対象となると考えられる。したがって、営業秘密保有者は、営業秘密が掲載されたウェブサイトを提供するプロバイダ等に対して、発信者情報の開示請求をすることができると考えられる。

①の「明らか」とは、権利の侵害がなされたことが明白であるという趣旨であり、不法行為等の成立を阻却する事由の存在をうかがわせるような事情が存在しないことまでを意味する[4]。もっとも、名誉毀損、プライバシー侵害、著作権等侵害、商標権侵害については、情報流通プラットフォーム対処法に関連するプロバイダ等の行動基準を明確化するためのガイドラインが公表されているが、不正競争行為については同様のガイドライ

---

[1] 令和 3 年 4 月の情報流通プラットフォーム対処法改正（令和 3 年法律第 27 号）が、令和 4 年 10 月 1 日から施行されたことに伴い、従前の省令である「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令」（平成 14 年総務省令第 57 号）が廃止され、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律施行規則」（令和 4 年総務省令第 39 号）が施行され、令和 7 年 4 月に「特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律施行規則」に改称されている。

[2] 前掲注 1 で述べた、令和 3 年 4 月の情報流通プラットフォーム対処法改正により、特定発信者情報以外の発信者情報の開示に加えて、特定発信者情報の開示も一定の補充的な要件を満たしたときには認められるようになっている（情報流通プラットフォーム対処法第 5 条第 1 項後段）。「特定発信者情報」とは、発信者情報であって専ら侵害関連通信に係るものとして総務省令で定めるものをいい（情報流通プラットフォーム対処法第 5 条第 1 項柱書き）、SNS サービス等にログインした際の IP アドレス等が念頭に置かれている。総務省「プロバイダ責任制限法 Q&A」問 9 も参照されたい。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_04.html

[3] 総務省情報流通行政局情報流通振興課情報流通適正化推進室「情報流通プラットフォーム対処法」（第一法規、令和 7 年）28 頁。

[4] 前掲注 3 112 頁。

ン等が存在しないため、プロバイダ等における権利侵害の判断が困難となる可能性があることに留意が必要である。

②の「発信者情報の開示を受けるべき正当な理由があるとき」とは、開示請求者が発信者情報を入手することの合理的な必要性が認められることを意味し、この必要性の判断には、開示請求を認めることにより制約される発信者の利益（プライバシー等）を考慮した「相当性」の判断をも含むものである[5]が、発信者に対して損害賠償請求や差止請求等の請求を行う予定であるときは、正当な理由があると認められるものと考えられる。

前掲注 1 でも述べたとおり、令和 3 年 4 月に情報流通プラットフォーム対処法の改正が行われたところ、従来の裁判手続とは別に新たな裁判手続として発信者情報開示命令事件に関する裁判手続が創設された。SNS 等を運営する情報・サービス提供事業者（以下、本項において「コンテンツプロバイダ」という。）は、権利侵害を行った発信者の氏名・住所等の情報を有していないことが多いため、従来、裁判外で開示がなされない場合には、①発信者が権利侵害の投稿等の発信をした際の IP アドレス及びタイムスタンプ等の開示請求（仮処分の手続によることが多い。）を行い、②その結果判明した、ユーザに対してインターネット接続サービスを提供する事業者（以下、本項において「アクセスプロバイダ」という。）に対して、発信者の氏名、住所等の開示請求（訴訟手続による）を行うというように、多くの場合、発信者を特定するために 2 段階の裁判手続を経る必要があった。令和 3 年の法改正では、上記一連の手続を 1 つの裁判手続で完結させることができるようになった[6]。具体的な手続として、以下の流れが想定されている。

① 申立人からコンテンツプロバイダに対して開示命令（情報流通プラットフォーム対処法第 8 条。申立人に対する発信者情報の開示の命令）・提供命令（同法第 15 条。(a)申立人に対してアクセスプロバイダの名称等の情報を提供すること、(b)申立人が③の申立てを行ったことをコンテンツプロバイダに通知した場合（④）に、コンテンツプロバイダが保有する発信者情報をアクセスプロバイダに対して提供することの命令）を申立て
② ①(a)の提供命令により申立人に対してアクセスプロバイダの情報の提供（同法第 15 条第 1 項第 1 号イ）
③ 申立人からアクセスプロバイダに対する開示命令（同法第 8 条。申立人に対する発信者情報の開示の命令）・消去禁止命令（同法第 16 条。発信者情報開示命令申立事件が終了するまでの間、保有する発信者情報を消去してはならないことの命令）を申立て

[5] 前掲注 3・114 頁。
[6] 発信者情報開示請求によってコンテンツプロバイダから発信者の電話番号の開示を受けることが可能であることから、発信者の電話番号の開示を受けた後、弁護士会照会制度（弁護士法第 23 条の 2）を用いることによって、当該電話番号を基に電話会社に対して当該電話番号に係る契約者の氏名及び住所等の回答を求めることも可能である。

④ 申立人が③の申立てを行ったことをコンテンツプロバイダに対して通知（同法第 15 条第 1 項第 2 号）

⑤ ①（b）の提供命令により、コンテンツプロバイダが保有する発信者情報がアクセスプロバイダに提供され、①及び③の開示命令により、発信者情報が申立人に開示

なお、法改正によって創設された新たな裁判手続は、従来の訴訟手続とは異なり、非訟手続であることから、迅速な審理が行われることが期待される。また、これらの発信者情報開示命令事件に関する決定について不服がある場合、不服がある当事者は 1 か月の不変期間内に異議の訴えを提起することができ（同法第 14 条第 1 項）、この期間内に異議の訴えが提起されない場合には当該決定は確定判決と同一の効力を有するものとされている（同法第 14 条第 5 項）。

令和 3 年 4 月の改正法の内容も含め、総務省ウェブサイト「インターネット上の違法・有害情報に対する対応（情報流通プラットフォーム対処法）」[7]も参照されたい。

（３）削除請求

さらに、営業秘密保有者は、営業秘密が掲載されたウェブサイトを提供するプロバイダ等に対して、当該情報の送信を防止する措置を講ずるよう依頼をすることが考えられる。

特に、発信者に対する差止請求又はプロバイダ等による発信者情報の開示を待っては、損害が拡大するような場合には、プロバイダ等に対して一次的に送信を防止する措置を依頼することにより公開された情報を非公開にすることが有効となる。

なお、かかる依頼を受けたプロバイダ等は、送信を防止する措置を講じなかったことについて、当該情報の流通により権利を侵害されたとする営業秘密保有者との関係で損害賠償責任（不法行為責任）が生じる場合があり得る。情報流通プラットフォーム対処法第 3 条第 1 項は、損害賠償責任を負い得る場合の要件として、①当該情報の流通によって他人の権利が侵害されていることを知っていたとき、又は、②当該情報が流通していることを知っていた場合であって当該情報の流通によって他人の権利が侵害されていることを知ることができたと認めるに足りる相当な理由があるときと規定している。

他方、情報流通プラットフォーム対処法第 3 条第 2 項は、プロバイダ等が送信を防止する措置を講じた場合において、当該措置の対象情報の発信者に損害が生じた場合であっても、当該措置が当該情報の不特定の者に対する送信を防止するために必要な限度において行われたものである場合で、①当該情報の流通によって他人の権利が侵害されていると信じるに足りる相当の理由があったとき、又は、②当該情報の発信者に対し当該措置を講ずることに同意するかどうかを照会し、当該発信者が当該照会を受けた日から 7 日を経過しても当該発信者から同意しない旨の申出がなかったときは、プロバイダ等の発信者に対する損害賠償責任が制限される旨を規定している。

[7] https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html

なお、上記とは別途、令和 7 年 4 月 1 日に施行された情報流通プラットフォーム対処法改正（令和 6 年法律第 25 号）により、「大規模特定電気通信役務提供者」として指定された SNS 事業者等は、削除対応の迅速化に係る義務として、被害者からの削除申出を受け付ける方法を公表し（同法第 22 条）、当該方法に従った削除申出があった場合には、必要な調査を行った上で（同法第 23 条）、その結果及び理由を総務省令で定める一定期間以内に通知する義務等を負う旨が規定された（同法第 25 条）。

３．参考資料（法令・ガイドラインなど）

・不正競争防止法第 2 条第 1 項第 7 号
・情報流通プラットフォーム対処法第 3 条第 1 項・第 2 項、第 5 条第 1 項
・特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律施行規則

４．裁判例

特になし

Q70 サイバーセキュリティと情報共有・公表

サイバーセキュリティに関する情報を第三者に共有しようとする場合に、法令上どのような点に留意すべきか。また、セキュリティインシデント発生時には、何を目的としてどのような情報を共有又は公表すべきか。

タグ：サイバーセキュリティ基本法、個情法、不正競争防止法、金融商品取引法、刑法、情報共有、サイバーセキュリティ協議会、CISTA、J-CSIP、JC3、セプター、サイバーセキュリティ対処調整センター、ISAC

１．概要

サイバーセキュリティ対策は自組織で行うことが原則だが、サイバー攻撃の複雑化・巧妙化に伴い、情報共有の重要性が高まっており、現在、複数の情報共有体制が活動を行っている。サイバーセキュリティに関する情報を共有するに当たっては、他者に対して情報を提供することとなるため、情報の内容によって、個情法、不正競争防止法、金融商品取引法、刑法、独占禁止法といった法令や秘密保持契約など自社が締結している契約上の秘密保持義務に注意が必要であり、万が一これらの法令等に抵触した場合には、法令上の罰則その他の処分を受ける可能性があり、また、レピュテーションリスクが生じることにも留意する必要がある。

また、セキュリティインシデント発生時には情報共有及び公表の要否及び適否について検討する必要がある。

２．解説

（１）情報共有の意義及び重要性

サイバーセキュリティは、本来、各々の組織において取り組むべきものであるが、攻撃が複雑化し、脅威の変化が早い現状においては、一組織の対応では限界があり、また、被害を受けた組織等から迅速な情報共有が行われなければ、攻撃手口や対策手法等を他組織が知ることができず、同様の手口によるサイバー攻撃の被害がいたずらに拡大するおそれがある。そのため、情報を相互に共有することで自組織の取組を一層高度化したいといった意識が高まり、サイバーセキュリティに関する情報を一定のコミュニティで共有する動きが一層活発化している。

経営ガイドラインにおいても、サイバーセキュリティ対策を実施する上で、経営者が責任者に指示すべき 10 項目の一つとして「サイバーセキュリティに関する情報の収集、共有及び開示の促進」が挙げられている。

前提として、「共有」と「公表」は峻別する必要がある。共有とは、一定の目的を果たすために、必要な情報を特定の相手方に提供することということができ、公表とは、同じ

く一定の目的を果たすために、ウェブサイト等を通じて不特定多数が閲覧できる状態に置くことということができる。

このうち、「共有」については、さらに、法令や契約に基づいて相手方に報告する場合（Q57 及び Q58 など参照）と、必要に応じて情報共有体制に共有する場合という 2 つに分けることができるが、本項では、後者の情報共有を中心に述べることとする。

サイバーセキュリティに関する情報共有のための体制は、現時点においても複数存在しているところ、代表的なものをいくつか紹介する。

ア　サイバーセキュリティ協議会

平成 30 年のサイバーセキュリティ基本法の改正により組織された法定の情報共有体制であり、内閣サイバーセキュリティセンター（NISC）及び政令指定法人 JPCERT/CC[1]が事務局を務めていた。情報共有を行う上で阻害要因となっていた事項について法律改正等により改善を図り、既存の情報共有体制の活動を補完し、これらと有機的に連携しつつ、従来の枠を超えた情報共有・連携体制を構築することを目標としている（詳細は後述）。なお、NISC は令和 7 年 7 月 1 日付で改組され、内閣官房組織令（昭和 32 年政令第 219 号）第 1 条に基づき、国家サイバー統括室（NCO[2]）が新たに設置された[3]。また、サイバー対処能力強化法整備法により、本協議会は廃止され、新たな会議体の設置が予定されている[4]。

イ　サイバーセキュリティ戦略本部

サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティ基本法第 24 条に基づき設置された組織であり、サイバーセキュリティ戦略案の作成及び実施の推進、国の行政機関等におけるサイバーセキュリティに関する対策基準の作成及び当該基準に基づく施策の評価・監査、サイバーセキュリティの確保の状

---

[1] 従来、サイバーセキュリティ戦略本部の事務として、サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整に関する事務（基本法旧第 26 条第 1 項第 5 号）が規定され、当該事務の一部を政令で定める法人に委託することができる（同法旧第 31 条第 1 項第 3 号）とされていたところ、当該政令で委託する法人として、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）が指定されていた（サイバーセキュリティ基本法施行令旧第 6 条）。しかし、サイバー対処能力強化法整備法により基本法旧第 26 条第 1 項第 5 号及び旧第 31 条第 3 号が削除されたことで、旧第 31 条第 3 号中の「政令で定める法人」を規定する施行令第 6 条を設けておく必要がなくなり、同条を削除する施行令の改正が行われた（施行日：令和 8 年 10 月 1 日）。

[2] National Cybersecurity Office の略。

[3] https://www.cyber.go.jp/about/history/index.html

[4] 同法第 45 条、内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法及び同整備法について」（令和 7 年 5 月）9 頁参照。

況の評価等の事務を所掌する[5]。また、令和 7 年、サイバーセキュリティ戦略本部の下に、サイバーセキュリティ戦略推進会議等を開催することが決定された[6]。

ウ　情報共有プラットフォーム「CISTA[7]」

JPCERT/CC は、国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織におけるセキュリティ関連部署又は組織内 CSIRT に向けて、サイバーセキュリティに関する脅威情報やそれらの分析・対策情報を CISTA を介して提供している[8]。

エ　重要インフラ行動計画に基づく情報共有体制

重要インフラ行動計画における 5 つの施策群の一つとして、「情報共有体制の強化」が挙げられており、NCO は、重要インフラ所管省庁、情報セキュリティ関係省庁等と相互にシステムの不具合等に関する情報の共有を行うこととされている。

オ　サイバー情報共有イニシアティブ「J-CSIP[9]」（ジェイシップ）

IPA は、平成 23 年、サイバー情報共有イニシアティブ「J-CSIP」を発足し、重工や重電等、重要インフラで利用される機器の製造業者を中心として、標的型メール攻撃に関する情報共有を実施している。

カ　日本サイバー犯罪対策センター（JC3[10]）による情報共有

平成 26 年に業務を開始した一般財団法人日本サイバー犯罪対策センター（JC3）においては、産学官（セキュリティ関係等の産業界、学術機関、警察庁等）の情報や知見を集約・分析し、その結果等を還元することで、脅威の大元を特定し、これを軽減及び無効化することにより、以後の事案発生の防止を図ることとしている。

キ　セプター及びセプターカウンシル

NCO は、重要インフラ事業者等の情報共有・分析機能を担う組織である「CEPTOAR（セプター）[11]」及び各セプターの代表で構成された協議体である「セプターカウンシル」の運営及び活動を支援している。

---

[5] サイバーセキュリティ基本法第 24 条、第 25 条 1 項各号。
[6] 令和 7 年 7 月 1 日付サイバーセキュリティ戦略本部長決定「サイバーセキュリティ戦略推進会議の開催について」（https://www.cyber.go.jp/pdf/policy/kihon-s/250701cs_conference_opening.pdf）
[7] Collective Intelligence Station for Trusted Advocates の略。
[8] https://www.jpcert.or.jp/wwinfo/
[9] Initiative for Cyber Security Information sharing Partnership of Japan の略。
[10] Japan Cybercrime Control Center の略。
[11] Capability for Engineering of Protection Technical Operation, Analysis and Response の略、令和 7 年 9 月現在、15 分野 21 セプターが存在している。

ク ISAC（アイザック）

民間の各業界において、自主的な情報共有を行う組織である「ISAC[12]」が徐々に増加している。主要なものを挙げると、「ICT-ISAC」（通信事業者等）、「金融 ISAC」（金融事業者）、「電力 ISAC」（電力事業者）、「交通 ISAC」（交通・運輸事業者等）、「J-Auto-ISAC」（自動車関係事業者等）、「Software ISAC」（ソフトウェア産業等）などがある。

（２）情報共有において留意すべき法令等

サイバーセキュリティを確保するために有用な情報の中には、攻撃手法に関する情報、マルウェアに関する情報など様々なものが含まれ得るが、それを他者との間で共有する場合には、情報の性質等に応じて、以下の法令等に留意しなければならない。

ア 個情法

共有しようとする情報の中に個人データ（個情法第 16 条第 3 項）[13]が含まれている場合には、原則として本人の同意なく第三者提供ができない（同法第 27 条第 1 項）。

ただし、法令に基づく場合など、同法第 27 条第 1 項各号のいずれかに当たる場合は、本人の同意は不要である。

イ 不正競争防止法

仮に共有しようとする情報の中に営業秘密や限定提供データが含まれている場合、当該情報を他者と共有することで、営業秘密にあっては「秘密として管理されている」、又は「公然と知られていない」（不正競争防止法第 2 条第 6 項）という要件、限定提供データにあっては「業として特定の者に提供する情報として」、又は「電磁的方法により……管理され」（同条第 7 項）という要件が失われ、当該情報が営業秘密、又は限定提供データとしての法的保護を受けられなくなるという事態を招かないよう留意しなければならない。

営業秘密において適切な管理状況を保つための対応としては、提供に当たって営業秘密を特定した秘密保持契約を締結する等して自社の秘密管理意思を明らかにすることなどが考えられる。

ウ 金融商品取引法

上場会社等における会社関係者が業務に関する重要事実を職務等に関して知りながら当該重要事実が公表される前に株式の売買等を行うことは、いわゆるインサイダー取引として禁止される（金融商品取引法第 166 条第 1 項）。これに違反した者は、個人に

[12] Information Sharing and Analysis Center の略。
[13] 個人情報データベース等を構成する個人情報（詳細は Q13 を参照されたい）。

ついては 5 年以下の拘禁刑又は 500 万円以下の罰金（同法第 197 条の 2 第 1 項第 13 号）、当該個人が代表者又は代理人、使用人、その他の従業者である法人に対しては、5 億円以下の罰金が科される（同法第 207 条第 1 項第 2 号）。

例えば、サイバーセキュリティに関する情報共有を行うに当たっては、自社がサイバー攻撃を受け、情報漏えいが疑われているという事実を含めて情報を伝達することもあり得る。当該事実は、公表されれば会社の株価に影響を及ぼし得る情報として、上記にいう「重要事実」に該当し得る。

また、ここにいう「会社関係者」には、上場会社等の役員、代理人、使用人その他の従業者（以下、本項において「役員等」という。）のほか、当該上場会社等と契約を締結している者又は締結の交渉をしている者（法人の場合はその役員等）も含まれる（同法第 166 条第 1 項第 4 号、第 5 号）。

サイバーセキュリティに関する情報共有体制は、当該体制が持つ規約といった内規を守る旨を合意することを前提に各々のメンバーが当該体制に加入し、当該内規に基づき情報を共有することとなる。また、メンバーには上場している会社も含むため、当該体制に加入しているメンバーが上場会社等と各々相互に情報共有の契約を締結していると評価することも可能である。この場合、当該体制に加入し、情報共有活動を行っているメンバー会社及び当該活動に従事している者が全て「会社関係者」に該当することとなる。

なお、情報共有体制が上場会社等と契約を締結していると評価できない場合であっても、会社関係者から情報伝達を受けた者はインサイダー取引規制の対象となる（同法第 166 条第 3 項）[14]。

情報共有体制において情報共有活動を行うに当たっては、外形的な情報共有又は情報伝達行為のみをもってインサイダー取引を疑われないよう、当該情報をサイバーセキュリティの確保目的以外に利用してはならないといった利用目的の制限、情報共有体制に加入している上場会社がサイバー攻撃の被害に遭った場合には、加入メンバー会社及び当該活動に従事している者は、被害会社の株取引を禁止すること、このような取決めに違反した場合にはサンクションを課す等の対応を行うことが考えられる。

---

[14] 上場会社等から情報共有を受ける者が「会社関係者」と評価できない場合、当該情報共有を受けた者は、上場会社等から情報伝達を受けることになるが、情報伝達行為の一部も規制の対象である。会社関係者は、重要事実について、他人に対し、公表前に有価証券等に係る売買等により他人に利益を得させ、又は当該他人の損失の発生を回避させる目的をもって、当該重要事実を伝達をしてはならない（同法第 167 条の 2 第 1 項）。これに違反し、情報の伝達を受けた者が当該重要事実の公表前に株式の売買等を行った場合には、上記インサイダー取引と同様の罰則が科される（同法第 197 条の 2 第 1 項第 14 号、第 207 条第 1 項第 2 号）。サイバーセキュリティに関する情報共有を行うに当たっての情報伝達は、「他人に利益を得させ、又は当該他人の損失の発生を回避させる目的」にあたらないため、基本的にはインサイダー取引規制の対象ではないと考えられる。

エ　刑法（不正指令電磁的記録に関する罪）[15]

サイバーセキュリティに関する情報共有を行うに当たっては、マルウェアの挙動の解析や対応策の発見など、対策のためにマルウェアそのものを共有することも考えられる。

このような場合、外形的には不正指令電磁的記録の提供（刑法第 168 条の 2 第 1 項）又は供用（同条第 2 項）に当たり得るため、他人の電子計算機の実行の用に供されることのないよう、情報の提供側と受領側でマルウェアの授受を行う旨を合意することを前提として、提供者・受領者ともに、外部に当該マルウェアが送られることがないよう、厳格に管理しながらやりとりするなどの対応を行うことが考えられる。

オ　独占禁止法

競合事業者同士の価格、供給数量等の重要な競争手段である取引条件に関する情報交換は独占禁止法上のカルテル規制（同法第 3 条）との関係で問題となる可能性がある。そのため、共有体制において情報共有活動を行うに当たってはこれらの情報が交換されないよう十分に留意する必要がある。

カ　秘密保持契約等の自社が締結している契約上の秘密保持義務

自社が締結している秘密保持契約その他の契約の秘密保持義務の対象となっている情報を契約の相手方の同意を得ることなく第三者に共有した場合、秘密保持義務に抵触する可能性がある。そのため、情報共有活動を行うに当たっては、共有する情報が自社の締結している契約における秘密保持義務の対象となっていないか確認する必要がある。

（3）セキュリティインシデント発生時の情報共有と公表について

セキュリティインシデント発生時の情報共有については、何を目的に共有を行うかという観点から、どのような情報をどのタイミングで誰に共有するかを検討する必要がある。この点に関しては、JPCERT/CC が総務省サイバーセキュリティタスクフォース第 33 回資料として公表した「サイバー攻撃被害情報の共有と公表のあり方について(公開版)」[16]が参考になる。

この文書においては、共有（及び報告）と公表を区別し、また、共有すべきサイバー攻撃被害を示す情報として、「技術情報」と「コンテクスト情報」を区別している。技術情報とは、攻撃に使用されたマルウェアや不正通信先の情報など、必ずしも被害を受けた組織に固有の情報ではないものであり、コンテクスト情報とは、被害を受けた個別組織名や対応経緯、被害内容など、被害組織に固有の情報を指す。

以下では、目的別に、共有及び公表の是非及びそのタイミングについて概説する。

---

15 構成要件などの詳細については Q73 を参照されたい。
16 https://www.soumu.go.jp/main_content/000762951.pdf

ア　攻撃の全容解明及び被害企業自身の二次被害防止目的

サイバー攻撃を受けた被害企業においては、自社がどういった攻撃を受けているのか、また、どのような対応を行えば脅威を除去できるのかがわからないケースも多く見られる。これに対処し、被害の原因調査及び根本的な原因への対応を行うためには、早期の段階での情報共有が重要となる。このとき、専門機関に対して技術情報を共有し、専門機関を含む他組織が保有する情報のフィードバックを受けることで、まずは、自組織が受けた攻撃を一定程度の確度をもって一次判定を行い、初期対応を行うことができる。また、攻撃の全容解明につなげるとともに、脅威を除去して被害企業自身の二次被害を防止する目的を果たすことができる。

この場合にコンテクスト情報を広く共有又は公開することは推奨されない。被害企業のネットワーク内に攻撃者が未だに潜伏している可能性があるため、コンテクスト情報を含めて広く公開を行うことは、攻撃者による被害企業への更なる攻撃を招くおそれがある。

イ　同種の攻撃による他の企業の被害拡大防止目的

同種の攻撃による他の企業の被害拡大防止を目的とする場合にも、公表等を行う前の早期の段階における情報共有が重要となり得る。専門機関や情報共有体制に対して技術情報を共有することで、専門機関や情報共有体制において当該技術情報のうち重要なエッセンスを抽出し、対策情報として展開することで被害拡大の防止という目的を果たすことができる。

この場合にコンテクスト情報を広く共有又は公開することは、自社が特定されることによる二次被害が生じる可能性がある一方で、被害拡大防止への寄与度が大きく変わるものではないため、その意義は乏しいと評価することができる。また、そのような情報を外部に出すためには、社内調整及び関係者との調整を経るためのハードルが高くなるところ、調整をしている間に、情報が陳腐化する、又は同種の攻撃による被害の拡大を招く結果となりかねない。

ウ　漏えいした情報の関係者の二次被害防止目的

例えば個人データが漏えいした場合には、漏えいした個人データが悪用されるなどして本人に対する二次被害が発生する可能性がある。本人に対して直接連絡することができれば、一定程度二次被害の防止に資すると考えられるが、本人の連絡先が古いなどによって直接の連絡ができない場合には、その代替措置としての公表を検討する必要が生じる。

この場合、個人データの本人に対して説明責任を果たす、又は信頼関係を維持するために、一定程度コンテクスト情報を連絡内容又は公表内容の中に盛り込む必要が出てくると考えられる。

エ　レピュテーションリスク対策目的

サイバー攻撃を受けた際には、自社以外の第三者からサイバー攻撃を受けたことが露呈する場合がある。例えば、ランサムウェア攻撃の場合は、攻撃者がリークサイトに情報を公開する、又は自らメディアを含めて広く情報を流すケースなどが挙げられる。また、一定の範囲で流通しているマルウェアの中に攻撃対象に関する情報が含まれていることで、当該攻撃対象に対するサイバー攻撃が行われた事実が推定されるケースもある。

この場合に、何らの情報も公表しなければ、サイバー攻撃を受けたことを隠蔽しているのではないかという誤解を与え、企業のレピュテーションを毀損する可能性がある。そこで、レピュテーションリスク対策としての公表を検討する必要が生じる。

この場合も、上記ウと同様、企業としての説明責任を果たしつつ、隠蔽という誤解を解くために、一定程度コンテクスト情報を公表内容の中に盛り込む必要が出てくると考えられる。

オ　法令に基づく義務を果たす目的

サイバー攻撃を受けた際に、法令又はガイドライン等に基づき当局等への対応が必要となる場合がある（詳細については Q57 及び Q58 を参照されたい。）。

このとき、法令に基づく義務を果たさない場合には、違法行為として当局から法執行を受けるリスクがあるため、少なくとも、その義務を果たす為に必要な範囲で、情報共有又は公表を行う必要が生じる。

サイバー攻撃被害組織等において、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいかの検討を行うにあたり、実務上参考となるガイダンス文書を策定するために、令和 4 年 4 月 20 日、サイバーセキュリティ協議会の運営委員会の下で、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」を開催することが決定され、令和 5 年 3 月 8 日に、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が公表されている[17]。

（4）官民、国及び地方公共団体等の連携

冒頭でも述べたように、サイバー攻撃が巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数が増加傾向にあることを踏まえ、国家及び国民の安全をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備するものとして、サイバー対処能力強化法及びサイバー対処能力強化法整備法が制定されている。サイバー対処能力

[17] https://www.cyber.go.jp/council/cs/kyogikai/guidancekentoukai.html

強化法においては、基幹インフラ事業者がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への情報共有・対処支援等により、事案の未然防止、対処支援強化を図る旨が定められている。また、内閣総理大臣は、サイバーインシデント防止のための情報共有及び対策に関する協議会を組織することとされている[18]。

また、令和 8 年 4 月 1 日に施行された改正地方自治法において、地方公共団体は、事務の種類・内容に応じて情報システムを有効に利用するとともに、他の地方公共団体又は国と協力し、その利用の最適化を図るよう努めることが求められている。また、地方公共団体は、サイバーセキュリティの確保等の情報システムの適正な利用を図るために必要な措置を講じなければならず、総務大臣は、これらの対応に関する指針を示すことが求められている。地方自治法に関する改正の詳細は、Q4 を参照されたい。

３．参考資料（法令・ガイドラインなど）

・サイバーセキュリティ基本法第 17 条
・サイバーセキュリティ協議会「サイバーセキュリティ協議会規約」（令和 7 年 7 月 1 日一部改正）
https://www.cyber.go.jp/pdf/council/cs/kyogikai/kyogikai_kiyaku.pdf
・経営ガイドライン
・個情法ガイドライン（通則編）
・一般社団法人 JPCERT コーディネーションセンター「サイバー攻撃被害情報の共有と公表のあり方について（公開版）」（2021 年 3 月）
https://www.soumu.go.jp/main_content/000762951.pdf
・サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和 5 年 3 月 8 日）
https://www.cyber.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

４．裁判例

特になし

[18] サイバー対処能力強化法第 2 章・第 9 章。

Q71 脅威インテリジェンスサービス

脅威インテリジェンスサービス（特にダークウェブからの情報収集を行っているサービス）を提供するに当たって、どのような点に留意すべきか。

タグ：脅威インテリジェンス、ダークウェブ、個情法、不正競争防止法、刑法

１．概要

DX の加速により、個人情報や営業秘密の漏えい、不正アクセス、サイバー攻撃など、デジタルにおける脅威・リスクが増している。そのような中、攻撃者からの脅威の検知・分析・対応・予防、サイバーセキュリティの向上に活用するため、サーフェスウェブのみならず、通常の方法ではアクセスが容易ではなく、アクセス自体に危険が伴うことがあるダークウェブやダークマーケットからも情報を収集し、加工・分析した上で、攻撃者の脅威の兆候などの有用な情報等を提供するサービス、すなわち、脅威インテリジェンスサービスが脚光を浴びている。

ダークウェブやダークマーケットでの情報収集は、それ自体の適法性も問題となる。そのため、違法行為を前提とする脅威インテリジェンスサービスの利用はコンプライアンスやレピュテーションに関して問題となり得る上、当該違法行為の幇助・教唆も問題となり得るので、適切な知識を持った上で、利用する必要がある。

２．解説

（１）脅威インテリジェンスサービスとは

脅威インテリジェンスサービスとは、明確な定義があるわけではないが、サイバーセキュリティ上の脅威に関する情報等（マルウェアや攻撃インフラ等に関する情報、いわゆる IoC（Indicator of Compromise）情報等）を収集し、その情報を分析又は集約し、評価、分析結果等の付加価値を加えて顧客に提供するという形態をとるサービスが多い。

情報の収集先は、一般公開されているニュースサイトや SNS などのいわゆるサーフェスウェブのみならず、通常の方法ではアクセスが容易ではなく、アクセス自体にも危険が伴うことがあるダークウェブやダークマーケットから情報を収集する脅威インテリジェンスサービスも近時増加しつつある。そうしたサービスでは、ダークウェブやダークマーケットにアクセスし、サイバー攻撃者のやりとりの内容、取引されている情報といった、サイバー攻撃の兆候となる情報を収集し、時には AI を駆使して専門家が加工・分析した上で、顧客との関連性が高い脅威情報を抽出して提供している。

こうしたサービスが増加している背景には、デジタルリスクが高まっていることや、特定の事業者や組織を狙う「標的型攻撃」の脅威が高まっていること、サイバー攻撃の巧妙化に伴い、これまでとは違った予防策を実施する必要が高まっていることが挙げられる。

加えて、サイバー攻撃が複雑化・巧妙化する中、日々刻々と様々なセキュリティ関連の企業や団体が脅威に関する情報発信を行っているため、情報過多となり、事業者にとって必ずしも必要な脅威情報に効率的にアクセスできないケースもある。

脅威インテリジェンスサービスを提供するための情報収集として、違法取引の温床となっているダークウェブやダークマーケットに潜入し、一定の活動や取引をすることが法令に違反しないかが問題となる。そのような状況を踏まえて、例えば米国では、米国司法省サイバーセキュリティユニットが、2020 年 3 月に、脅威インテリジェンスについてのガイダンスを発表している[1]。

日本においては、脅威インテリジェンスサービスの普及を目的として、IPA から、令和 6 年 7 月に、「脅威インテリジェンス導入・運用ガイドライン」が公表されている[2]。本ガイドラインは、脅威インテリジェンスサービスの導入・運用を主導するセキュリティ部門の担当者を主たる読者として想定し、具体的な導入・運用方法を提示することで、脅威インテリジェンスサービスの普及と組織のセキュリティ強化を図るものである。

本ガイドラインにおいて、「脅威インテリジェンス」とは、サイバーセキュリティに関する脅威情報を収集・加工し、分析で得たインテリジェンスに基づいて組織のセキュリティ対応における意思決定を回すライフサイクルを指すものと定義されている[3]。より具体的には、「脅威」とは、システムや組織に対し、害を与えるあるいは望まないインシデントを発生させる潜在的原因であり、「意図」「機会」「能力」の 3 要素から構成され、それぞれ以下の意味を有するとされている[4]。

- 意図：脅威アクターがターゲット組織を狙う目的・動機
- 機会：ターゲット組織内に、攻撃実行を可能にする環境・条件が揃っている状態
- 能力：目的を達成するために必要な脅威アクターが使う攻撃手法、及び攻撃手法を実現するために必要な脅威アクターのリソース・スキル

また、本ガイドラインでは、脅威インテリジェンスのライフサイクルを①方針策定、②収集・加工、③分析、④配布、⑤評価の 5 つのフェーズに分類し、それぞれのライフサイクル別に実施事項を示している[5]。

---

[1] Cybersecurity Unit Computer Crime & Intellectual Property Section Criminal Division U.S. Department of Justice "Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources"
（https://www.justice.gov/criminal-ccips/page/file/1252341/download）

[2] IPA「脅威インテリジェンス導入・運用ガイドライン」（令和 6 年 7 月）（https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003510-att/f55m8k000000358r.pdf）

[3] 脅威インテリジェンス導入・運用ガイドライン 2.1.1。

[4] 脅威インテリジェンス導入・運用ガイドライン 2.1.2。

[5] 脅威インテリジェンス導入・運用ガイドライン 2.1.3。

さらに、フレームワーク遵守に偏重しがちなコンプライアンスベース型アプローチ[6]だけでは現実の脅威に機動的に追随しにくいとの問題意識を踏まえ、脅威ベース型アプローチ[7]を採り入れて、脅威の発生頻度・影響度・攻撃可能性・自組織の対策状況に基づく優先順位付け、プロアクティブな準備、インシデント対応力の向上、経営判断を支える戦略的インテリジェンスの確立を図ることが提案されている。経営提案の素材から現場運用の手順まで一貫して活用できる実践的ガイドラインと位置づけられる。

（２）法的論点

以下では、日本法の観点から、脅威インテリジェンスサービスに関連する法的論点を解説する。

ア　ダークウェブ上で流通する個人情報を閲覧又はダウンロードすることの適法性

ダークウェブ上で流通する情報を収集するタイプの脅威インテリジェンスサービスにおいても、どのような情報を収集するかはさまざまである。例えば、ダークウェブ上で、不正アクセスにより窃取されたと思われるユーザ ID・ユーザ名・パスワードのリスト等が取引されている場合に、どのようなデータなのかという抽象的な情報のみを取り扱うサービスもあれば、実際に取引されているデータをダウンロードして取り扱うサービスもある。

特に後者については、ダークウェブ上で取引されている個人情報を含むデータをダウンロード等することがあり得るため、これが、偽りその他不正の手段による個人情報の取得を禁ずる個情法第 20 条第 1 項に反しないかが問題となる。

個情法ガイドライン（通則編）によれば、まず、「取得」について、個人情報を含む情報がインターネット等により公にされている場合であって、単にこれを閲覧するにすぎず、転記等を行わない場合は、個人情報の「取得」にあたらないとされている[8]。一方で、個人情報に該当するデータをダウンロード含め転記等する行為は、個人情報の「取得」に当たると考えられる。

そして、同ガイドラインでは、個情法第 20 条第 1 項違反に当たる事例として、同「法第 27 条第 1 項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、個人情報を取得する場合」や「不正の手段で

---

6 「コンプライアンスベース型アプローチ」とは、フレームワークや法規制などをベースとしてセキュリティ成熟度の基準やあるべき姿に対して現時点での状態を分析し、そのギャップを洗い出す手法をいう（脅威インテリジェンス導入・運用ガイドライン 1.1）。

7 「脅威ベース型アプローチ」とは、ビジネス環境・特性に注目し、自組織を対象とし得る攻撃グループ、脅威にフォーカスを当て特定脅威に関する事業への影響や攻撃可能性などをもとに対策の優先順位を判断する手法をいう（脅威インテリジェンス導入・運用ガイドライン 1.1）。

8 個情法ガイドライン（通則編）3-3-1。

個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合」が示されている[9]。

ダークウェブ上で掲載・取引されている個人情報は、掲載した者が偽りその他不正の手段により取得した個人情報である蓋然性が高く、また、掲載した者が個情法第 27 条第 1 項に違反してこれをダークウェブ上で提供している蓋然性が高い。このため、個人情報取扱事業者が、ダークウェブ上で掲載・取引されている個人情報を当該ダークウェブからダウンロード等により取得することは、偽りその他不正の手段による個人情報の取得に該当するものとして、個情法第 20 条第 1 項に違反するおそれがあると考えられる。

ただし、個別の事案ごとに判断することとなるが、例えば、人（法人を含む。）の生命、身体又は財産の保護のために個人情報をダークウェブから取得してこれを取り扱う必要がある場合、社会的に影響のあるサイバー攻撃の解析等のために研究機関等が必要最小限の範囲で個人情報をダークウェブから取得してこれを取り扱う必要がある場合には、個情法第 20 条第 1 項には違反しないものと考えられる（ただし、その取得したデータに上記の取扱いの必要性が認められない個人情報も含まれていた場合には、直ちにこれを削除する必要がある）。他方、みだりに個人情報を含むデータをダークウェブから取得する場合には、個情法第 20 条第 1 項に違反するおそれがあると考えられる[10]。

加えて、当該個人情報が特定個人情報に当たる場合は、番号利用法で認められていない目的での情報の取得は、同法に違反する可能性もあるので、注意が必要である。

イ　ダークウェブ上で流通する営業秘密及び限定提供データを閲覧又はダウンロードすることの適法性（不正競争防止法第 21 条）

営業秘密及び限定提供データのダウンロードは、窃取、詐欺、強迫その他の不正な手段による取得についての不正競争には当たらないと考えられる（不正競争防止法第 2 条第 1 項第 4 号・第 11 号）。しかし、不正取得行為が介在したことを知って、取得している場合には、不正競争に当たる（同法第 2 条第 1 項第 5 号・第 12 号）。ただし、営業上の利益の侵害等がなければ、同法上の差止請求及び損害賠償請求の対象にはならない（同法第 3 条・第 4 条）。なお、限定提供データに関しては刑事責任に関する規定がなく、営業秘密についても、「不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的」がなければ、営業秘密の取得についても、刑事責任を負うことはないと考えられる（同法第 21 条第 1 項第 3 号・第 4 号）。

---

[9] 個情法ガイドライン（通則編）3-3-1。

[10] 個情法 QA4-5。この QA4-5 は、令和 5 年 3 月 31 日の更新により追加されたものである。同日に更新された箇所の一覧については、下記を参照されたい。
個人情報保護委員会「個人情報の保護に関する法律についてのガイドラインに関する Q&A の更新」（令和 5 年 3 月 31 日）（https://www.ppc.go.jp/files/pdf/2304_APPI_QA_tsuikakoushin.pdf）

ウ　ダークウェブ上で流通するマルウェアをダウンロードすることの適法性

正当な理由がなく、人の電子計算機における実行の用に供する目的で、不正指令電磁的記録を取得又は保管する行為は、不正指令電磁的記録取得又は同保管罪（刑法第 168 条の 3）が成立する場合がある（Q73 参照。）。マルウェアは、この不正指令電磁的記録に該当し得るため、マルウェアのダウンロードについては、同罪に注意する必要がある。ただし、例えば、脅威インテリジェンスサービスの提供目的であれば、「正当な理由がないのに」及び「人の電子計算機における実行の用に供する目的」という要件を欠き、同罪は成立しないと考えられるが、ダウンロード及び保管する際には正当な理由及び目的があることを明らかにできるよう準備しておく必要がある。

エ　ダークウェブ上で流通する ID・パスワード等の識別符号をダウンロードすることの適法性

何人も、不正アクセス行為の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならず（不正アクセス禁止法第 4 条）、同目的でそれを保管してはならない（同法第 6 条）。

ダークウェブ上で流通している ID やパスワードは、同法に規定する識別符号に該当する可能性があるため、これをダウンロードし、保管する行為は、同法上問題となり得る。ただし、これらの罪が成立するのは、あくまで「不正アクセス行為の用に供する目的」が肯定される場合である。そのため、脅威インテリジェンスサービスの提供のために他人の識別符号を取得・保管する行為について、「不正アクセス行為の用に供する目的」という要件を欠く場合には、同罪は成立しないが、ダウンロード及び保管する際には、正当な理由及び目的があることを明らかにできるよう準備しておく必要がある。

3．参考資料（法令・ガイドラインなど）

- 個情法第 20 条第 1 項、同法第 27 条第 1 項、同法第 30 条第 1 項及び第 3 項
- 不正競争防止法第 21 条
- 刑法第 168 条の 3
- 個情法ガイドライン（通則編）
- 個情法 QA
- IPA「脅威インテリジェンス導入・運用ガイドライン」（令和 6 年 7 月）
  https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k000003510-att/f55m8k000000358r.pdf

4．裁判例

特になし

Q72 脆弱性情報の取扱いについて

利用しているソフトウェア製品等に脆弱性が発見された場合、どのような対応を行う必要があるか。

タグ：情促法、脆弱性、脆弱性情報ハンドリング、JVN

１．概要

脆弱性が発見された場合、対応を求めるべくそれを公開することが必要だが、どのように対策すればよいかという対策情報とセットで公開しなければ、悪意ある者のサイバー攻撃を誘発するおそれがあるため、脆弱性情報の取扱いには慎重な対応が必要である。

そこで、脆弱性の取扱いについては、法令及び経済産業省告示において、推奨される行動が定められている。具体的には、脆弱性を発見した場合には、IPA に脆弱性関連情報を届け出る等の対応が推奨される。

関係者との調整が終わるなど所定の手続を経た脆弱性対策情報については、ポータルサイト（JVN[1]）において公開される。

２．解説

（１）はじめに

ソフトウェア製品又はソフトウェアが組み込まれたハードウェアの中には、脆弱性が存在することがある。脆弱性とは、「コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所」[2]をいい、特に、汎用品として様々な企業等で広く利用されているソフトウェア等に脆弱性が発見された場合、それを放置すれば、当該ソフトウェア等を利用する不特定多数の者に対して大きな被害が発生するおそれがある。

一方で、脆弱性に対処するには、ソフトウェアのアップデートやその他回避策を取る等の対応が必要となるところ、そのような対策なく脆弱性に関する情報を公開すると、攻撃者が当該脆弱性を用いてサイバー攻撃等を行うおそれがあるため、脆弱性の情報の取扱いには慎重な対応が必要である。

そこで、脆弱性に関連する情報の取扱いについては、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」[3]（平成 29 年経済産業省告示第 19 号。以下、本項において「本規程」という。）が、ソフトウェア製品（ソフトウェア又はそれを組み込んだハードウェ

[1] Japan Vulnerability Notes の略。
[2] ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号）第 1 の 3(3)。
[3] 令和 6 年 6 月 18 日一部改正（令和 6 年経済産業省告示第 93 号）。

アであって、汎用性を有する製品）及びウェブアプリケーション（インターネット上のウェブサイトで稼働する固有のシステム）に係る脆弱性関連情報等を取り扱う際に推奨される行為等を定めている。

なお、本規程は、日本国内で利用されているソフトウェア製品又は日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーションに係る脆弱性であって、その脆弱性に起因する影響が不特定又は多数の者におよぶおそれがあるものを適用範囲としているため、汎用性を有しないソフトウェア製品、例えば、システム開発契約等に基づきオーダーメードで作成されるソフトウェア等に脆弱性が発見された場合については、同規程は適用されず契約等に基づく対応が必要となる（Q52 参照）。

また、基幹インフラ事業者が不正アクセス行為等を受けた場合の報告や、重要電子計算機として用いられる電子計算機又は当該電子計算機に組み込まれるプログラムにおける脆弱性情報の官民連携の仕組み等については、サイバー対処能力強化法において定められている（Q3 参照）。

（２）本規程の制定経緯

平成 28 年の情促法改正により、IPA の業務に、サイバーセキュリティに関する調査を行った場合、必要に応じて、その結果に基づき、事業者等のサイバーセキュリティの確保のため講ずべき措置の内容を公表するものとする業務が追加されるとともに、その公表の手続及び方法は経済産業省令で定めることとされた（情促法第 51 条第 1 項第 7 号、同条第 3 項、同条第 4 項）。これに基づき、経済産業省令においては、公表の方法として、インターネットの利用その他適切な手段により一般的に公表する方法とされ、その他の公表の方法及び手続に必要な事項は、経済産業大臣が定めることとされた（情促法施行規則第 47 条、第 48 条）。

そして、情促法施行規則第 48 条の規定に基づき、及び情促法を実施するため、ソフトウエア等脆弱性関連情報取扱基準（平成 26 年経済産業省告示第 110 号）を廃止するとともに本規程が新たに制定された。本規程における脆弱性関連情報の届出を受け付ける機関として IPA、脆弱性の発見者やソフトウェア製品の開発者等と協力しながら脆弱性対策情報の公表日の決定等の調整を担う機関として JPCERT/CC が指定されている（平成 31 年経済産業省告示第 19 号）。なお、本規程は、令和 6 年 6 月 18 日付で一部改正がされており、従前は調整機関のみが優先情報提供を実施することとされていたが、調整機関だけでなく、受付機関からも優先情報提供を行うことを可能とされた。

（３）本規程に基づく制度の概要

本規程は、ソフトウェア製品に係る脆弱性関連情報の取扱い及びウェブアプリケーションに係る脆弱性関連情報の取扱いに関する手続を定めている。各々の概要は、以下のとおりである。

ア ソフトウェア製品について

① 脆弱性情報を発見又は取得した発見者（開発者を除く）は、IPA に対して脆弱性関連情報を届け出る。

② JPCERT/CC は、IPA が受理した脆弱性関連情報の通知を受け、当該情報を製品開発者に対して通知するとともに、当該製品開発者に対し脆弱性検証の結果の報告を求める。

③ JPCERT/CC は、脆弱性情報を公表する日（以下、本項において「脆弱性情報公表日」という。）を定める。

④ 製品開発者は、脆弱性情報公表日までに、対策方法を講じる。

⑤ IPA 及び JPCERT/CC は、脆弱性情報公表日に、脆弱性情報、脆弱性検証の結果、対策方法及び対応状況について、インターネット等を通じて公表する。

⑥ ⑤にかかわらず、IPA 又は JPCERT/CC は、製品開発者から自ら開発等を行ったソフトウェア製品に係る脆弱性関連情報及び対策方法の通知を受けたときは、脆弱性情報公表日を定め、脆弱性情報及び当該対策方法について、インターネット等を通じて公表する。公表に先立って、JPCERT/CC は、製品開発者から脆弱性情報公表日に係る意見を聴取する。

なお、JPCERT/CC は、この業務を「脆弱性情報ハンドリング」と呼び[4]、脆弱性関連情報は必ずその対策方法とともに公表されなければならず、また、複数製品が影響を受ける脆弱性の場合には、情報の公表に当たって、関係者間で一定の足並みをそろえることが重要であるという「公表日一致の原則」を掲げ、関係者との調整を行っている。

調整がなされた脆弱性に関しては、IPA と JPCERT/CC が共同で運営する脆弱性対策情報ポータルサイト「JVN」[5]において公開されている。

イ ウェブアプリケーションについて

① 発見者（対象ウェブサイトの運営者を除く。）は、IPA に脆弱性関連情報を届け出る。

② IPA は、届出を受理したときは、ウェブサイト運営者に脆弱性関連情報を速やかに通知するとともに、当該ウェブサイト運営者に脆弱性検証の結果の報告を求める。

③ ウェブサイト運営者は、受付機関から脆弱性関連情報の通知を受けたときは、脆弱性を修正する。

３．参考資料（法令・ガイドラインなど）

・情促法第 51 条第 1 項第 7 号、第 3 項、第 4 項
・情促法施行規則第 47 条、第 48 条

[4] https://www.jpcert.or.jp/vh/index.html
[5] Japan Vulnerability Notes（https://jvn.jp/index.html）

・ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号（最終改正令和 6 年経済産業省告示第 93 号））
・平成 31 年経済産業省告示第 19 号（調整機関、受付機関を定める告示）
・IPA など「情報セキュリティ早期警戒パートナーシップガイドライン」（令和 6 年 5 月）

４．裁判例

特になし

Q73 不正プログラムと刑事罰

いわゆるコンピュータウイルスによって企業活動を阻害する行為は、どのような場合に、刑法上、処罰の対象となり得るか。

タグ：刑法、不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪、コンピュータウイルス、不正プログラム、不正指令電磁的記録、マルウェア

１．概要

いわゆるコンピュータウイルスなどの不正なプログラムによって企業活動を阻害する行為が、不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪[1]又は電磁的記録毀棄罪等の構成要件に該当する場合、これらの罪により処罰の対象となり得る。

２．解説

（１）企業活動を阻害する行為

企業活動を阻害する目的で、コンピュータウイルス[2]などの不正なプログラムを作成したり、他人のコンピュータの実行の用に供したりする等の行為が、不正指令電磁的記録に関する罪（刑法第 168 条の 2、第 168 条の 3）の構成要件に該当する場合、これらにより処罰され得る。また、他にも、企業活動が阻害されるおそれのある行為が、電子計算機損壊等業務妨害罪（同法第 234 条の 2）や電磁的記録毀棄罪（同法第 259 条）等の罪の構成要件に該当する場合、これらの罪により処罰され得る。

（２）不正指令電磁的記録に関する罪が新設された背景

電子計算機（典型的にはパーソナルコンピュータや携帯電話、スマートフォン等のことを指す。以下、本項において「コンピュータ」という。）は、広く社会に普及、浸透し、人々の社会生活に欠かせない存在になってきており、重要な社会的機能を有している。このような社会生活に必要不可欠なコンピュータに対し、不正な指令を与えるプログラムが実行されれば、コンピュータによる情報処理のために実行すべきプログラムに対する

[1] 情報通信技術の進展等に対応するための刑事訴訟法等の一部を改正する法律（令和 7 年 6 月 12 日施行）により新設された罪（刑法第 95 条の 2）。

[2] 「コンピュータウイルス対策基準」（通商産業省告示第 952 号）によると、コンピュータウイルスとは、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり」、①自己伝染機能（自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能）、②潜伏機能（発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能）、③発病機能（プログラム、データ等のファイルの破壊を行う、設計者の意図しない動作をする等の機能）のうち、一つ以上の機能を有するものをいう。

信頼が損なわれ、ひいては、社会的基盤となっているコンピュータによる情報処理が円滑に機能しないこととなる。そこで、平成 23 年の刑法改正によって、正当な理由がないのに、他人のコンピュータにおける実行の用に供する目的で、他人がコンピュータを使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正なプログラム（不正指令電磁的記録）を作成、提供、供用、取得又は保管する行為を処罰できるようにするため、不正指令電磁的記録に関する罪が新設された。

このように、不正指令電磁的記録に関する罪の保護法益は、コンピュータのプログラムに対する社会一般の者の信頼という社会的法益であるとされている[3]。

（３）不正指令電磁的記録に関する罪

不正指令電磁的記録に関する罪（刑法第 168 条の 2、第 168 条の 3）は、コンピュータウイルス等のコンピュータに不正な指令を与えるプログラムが、刑法第 168 条の 2 第 1 項各号に定める「不正指令電磁的記録」（以下、本項において「不正プログラム」という。）に該当する場合に、正当な理由がないのに、他人のコンピュータにおける実行の用に供する目的で当該不正プログラムを作成又は提供する行為、他人のコンピュータにおいて当該不正プログラムを実行の用に供する行為[4]、他人のコンピュータにおける実行の用に供する目的で当該不正プログラムの取得又は保管する行為を処罰対象としている。

いわゆるコンピュータウイルスには、他のプログラムに寄生して自己の複製を作成し感染する従来の形態のものに限らず、トロイの木馬[5]、ワーム[6]、スパイウェア[7]と呼ばれるものなど様々な種類のものがあるが、いずれについても、不正プログラムに該当すれば、刑法第 168 条の 2 又は第 168 条の 3 による処罰の対象となり得る。

刑法第 168 条の 2 第 1 項

1 号　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
2 号　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

[3] 以上について、前田雅英ら編「条解刑法（第四版）」（弘文堂、令和 2 年）490 頁以下。
[4] なお、実行の用に供する行為（供用行為）については、刑法第 168 条の 2 第 1 項第 1 号に該当する不正プログラムの供用のみが処罰対象とされている（刑法第 168 条の 2 第 2 項）。
[5] 無害プログラム等であるかのように見せかけてコンピュータの使用者が気付かないうちに侵入し、データ消去やファイルの外部流出、他のコンピュータの攻撃等の破壊活動やデータの流出等を行うプログラムのことをいう。
[6] 他のプログラムに寄生せず、単体で自身を複製して他のコンピュータに拡散する自己増殖機能を持ったプログラムのことをいう。
[7] コンピュータの使用者が気付かないうちにインストールされ、情報を収集するプログラムのことをいう。

不正プログラムの定義は、刑法第 168 条の 2 第 1 項第 1 号及び第 2 号に規定されている[8]。同項第 1 号は、「意図に沿うべき動作をさせず、又はその意図に反する動作をさせる」（反意図性）べき「不正な指令を与える」（不正性）電磁的記録が不正プログラムに該当することを定めている。

反意図性は、コンピュータのプログラムに対する社会一般の信頼を害するものであるか否かという観点から規範的に判断され、不正性は、反意図性が認められるプログラムであっても、社会的に許容し得るものが例外的に含まれ得ることから、このようなプログラムを処罰対象から除外するために付された要件であるとされている[9]。

反意図性が否定される具体例として、例えば、市販されているソフトウェアについては、使用者が、そのプログラムの指令によってコンピュータが行う基本的な動作については認識している上、それ以外の詳細な機能についても、通常は使用説明書等によって認識し得るのであるから、仮に使用者がその機能を現実には認識していなくても、当該ソフトウェアには反意図性が認められないであろうとされている。

不正性が否定される具体例として、例えば、ソフトウェアの製作会社が不具合を修正するプログラムをユーザのコンピュータに無断でインストールした場合が挙げられるであろう[10]。

反意図性と不正性の要件については、近時、最高裁判所による判断が示されたところであり、この点については下記（4）で解説する。上記（2）のとおり、刑法上、不正プログラムを作成、提供、供用、取得又は保管する行為について処罰の対象とされているところ、本問においては、関係する不正指令電磁的記録作成罪、同提供罪及び同供用罪（いずれも刑法第 168 条の 2）について解説する。

ア　不正指令電磁的記録作成罪及び同提供罪（刑法第 168 条の 2 第 1 項）

不正指令電磁的記録作成罪又は同提供罪が成立するためには、正当な理由がないのに他人のコンピュータにおける実行の用に供する目的で不正プログラムを作成又は提供することが必要であるところ、ここにいう「実行の用に供する目的」とは、不正プログラムを、コンピュータの使用者にはこれを実行しようとする意思がないのに実行され得

---

[8] なお、2 号にいう、「同号（1 号）の不正な指令を記述した電磁的記録その他の記録」とは、内容的には不正な指令を与えるものとして実質的に完成しているものの、そのままでは電子計算機において動作させ得る状態にないものをいう。本号の電磁的記録としては、例えば、そのような不正な指令を与えるプログラムのソースコードを記録した電磁的記録等がこれに当たり、その他の記録としては、そのようなソースコードを紙媒体に印刷したもの等がこれに当たる。以上について、前掲注 3・前田ら編 493 頁。

[9] 前掲注 3・前田ら編 492 頁。
法務省「いわゆるコンピュータ・ウイルスに関する罪について」
（http://www.moj.go.jp/content/001267498.pdf）（平成 23 年）3・4 頁
なお、後述の最判令和 4 年 1 月 20 日刑集 76 巻 1 号 1 頁も参照。

[10] 以上について、前掲注 3・前田ら編 492 頁。

る状態に置く目的のことをいい、不正プログラムを作成又は提供した時点でこの目的がなければ各罪は成立しない。

プログラムを作成した者がいる場合に、その者について不正指令電磁的記録作成罪が成立するか否かは、その者が人のコンピュータにおける「実行の用に供する目的」でこのプログラムを作成したか否か等によって判断するため、ある者が正当な目的で作成したプログラムが他人に悪用されて不正プログラムとして用いられたとしても、プログラムの作成者に不正指令電磁的記録作成罪は成立しない。

「正当な理由がないのに」とは、「違法に」という意味である。

例えば、専ら自己のコンピュータで、あるいは、他人の承諾を得てそのコンピュータで作動させるものとして不正プログラムの作成を行ったとしても、このような場合には他人のコンピュータにおいて実行の用に供する目的が欠けることとなるが、さらに、このような場合に不正指令電磁的記録に関する罪が成立しないことを一層明確にする趣旨で、「正当な理由がないのに」との要件が規定されたものである。

本罪の法定刑は、3 年以下の拘禁刑又は 50 万円以下の罰金である。

イ　不正指令電磁的記録供用罪（刑法第 168 条の 2 第 2 項）

不正指令電磁的記録供用罪が成立するためには、正当な理由がないのに不正プログラムを他人のコンピュータにおける実行の用に供することが必要である。例えば、不正プログラムの実行ファイルを電子メールに添付して送付し、そのファイルを、事情を知らず、かつ、そのようなファイルを実行する意思のない使用者のコンピュータ上でいつでも実行できる状態に置く行為や、不正プログラムの実行ファイルをウェブサイト上でダウンロード可能な状態に置き、事情を知らない第三者にそのファイルをダウンロードさせるなどして、そのようなファイルを実行する意思のない者のコンピュータ上でいつでも実行できる状態に置く行為等がこれに当たり得る[11]。

なお、不正指令電磁的記録供用罪において供用行為が処罰の対象となるプログラムは、他人のコンピュータにおける実行の用に供する目的で作成されたプログラムに限定されていないため、不正プログラム[12]の作成者が、当該不正プログラムの作成時にはこうした目的ではなかったとしても、正当な理由がないのに、当該不正プログラムを他人のコンピュータにおける実行の用に供した場合には、本罪が成立し得る。

本罪の法定刑は、3 年以下の拘禁刑又は 50 万円以下の罰金であり、未遂犯も処罰される（同条第 3 項）。

---

[11] 前掲注 3・前田ら編 491 頁、前掲注 9・法務省「いわゆるコンピュータ・ウイルスに関する罪について」10 頁。

[12] 不正指令電磁的記録強要罪において供用行為が処罰の対象となるプログラムは、刑法第 168 条の 2 第 1 項第 1 号に該当する不正プログラムに限られる。

（４）近時の判例

ア　最判令和 4 年 1 月 20 日刑集 76 巻 1 号 1 頁

不正指令電磁的記録に関する罪における不正プログラムの該当性については、前述のとおり、最判令和 4 年 1 月 20 日において、最高裁判所が判断を示したところである[13]。

本件の事案は、ウェブサイト X（以下、本項において「X」という。）の運営者が、X の閲覧者のコンピュータにおいて仮想通貨（暗号資産）の取引履歴の承認作業等を行わせてそれによる報酬を取得しようと考え、X の閲覧者の同意を得ることなく、閲覧者のコンピュータを使用して前述承認作業等を行わせるプログラムコード（以下、本項において「本件プログラムコード」という。）を、サーバコンピュータ内の X に係るファイル内に蔵置して保管したというものである。

最高裁判所は、本件プログラムコードが不正プログラムに該当するかどうかを判断するに当たって、反意図性の要件について、「当該プログラムについて一般の使用者が認識すべき動作と実際の動作が異なる場合に肯定されるものと解するのが相当であり、一般の使用者が認識すべき動作の認定に当たっては、当該プログラムの動作の内容に加え、プログラムに付された名称、動作に関する説明の内容、想定される当該プログラムの利用方法等を考慮する必要がある」と判示した上で、本件プログラムコードについて、閲覧者から前述承認作業等について同意を得る仕様になっておらず、前述承認作業等に関する説明やこれが行われていることの表示もなかったことなどの事情を踏まえて、反意図性を認めた。

一方で、最高裁判所は、不正性の要件について、「電子計算機による情報処理に対する社会一般の信頼を保護し、電子計算機の社会的機能を保護するという観点から、社会的に許容し得ないプログラムについて肯定されるものと解するのが相当であり、その判断に当たっては、当該プログラムの動作の内容に加え、その動作が電子計算機の機能や電子計算機による情報処理に与える影響の有無・程度、当該プログラムの利用方法等を考慮する必要がある」と判示した上で、本件プログラムコードについて、以下の事情を踏まえ、不正性を認めなかった。

- コンピュータの機能やコンピュータによる情報処理に与える影響は、X 閲覧中に閲覧者のコンピュータの中央処理装置を一定程度使用することにとどまり、その使用の程度も、閲覧者のコンピュータの消費電力が若干増加したり中央処理装置の処理速度が遅くなったりするものの、閲覧者がその変化に気付くほどのものではなかったこと
- 本件プログラムコードは、ウェブサイトの運営者が閲覧を通じて利益を得る仕組みとして社会的に受容されている広告表示プログラムと比較しても、閲覧者のコ

[13] 最判令和 4 年 1 月 20 日刑集 76 巻 1 号 1 頁（コインハイブ事件）
（https://www.courts.go.jp/assets/hanrei/hanrei-pdf-90869.pdf）
本件に関する調査官解説として、池田知史・法曹時報 75 巻 8 号 164 頁がある。

ンピュータに与える影響において有意な差異は認められず、事前の同意を得ることなく実行され、閲覧中に閲覧者のコンピュータを一定程度使用するという利用方法等も同様であって、これらの点は社会的に許容し得る範囲内といえるものであること

- 仮想通貨の承認手続を行わせるなどの本件プログラムコードの動作の内容は、仮想通貨の信頼性を確保するための仕組みであり、社会的に許容し得ないものとはいい難いこと

その上で、最高裁判所は、本件プログラムコードが不正プログラムに該当しないと結論付けたが、この判断は飽くまでも最高裁判所が判示した反意図性と不正性についての判断の枠組みを前提として、具体的な事実関係に即した事例判断であり、必ずしも同種の動作を行うプログラムコード一般について、その動作が電子計算機の機能や電子計算機による情報処理に与える影響の有無・程度、当該プログラムの利用方法等の如何を問わず不正プログラムに該当しないことまで述べたものではないことに留意する必要がある。

イ　東京高判令和元年 12 月 17 日高等裁判所刑事裁判速報集（令 1）号 362 頁

不正指令電磁的記録に関する罪における不正プログラムの該当性については、前述最判令和 4 年 1 月 20 日のほか、スマートフォンに不正なアプリケーションをダウンロードさせた事案について、東京高等裁判所が判断を示している[14]。

本件の事案は、被告人が、他人の携帯電話機（端末）にインストールされると、同端末の持ち主に知られることなく、遠隔操作で、同端末に記録された LINE メッセージ、通話履歴、電話帳データ、端末位置情報等を、インターネット回線を通じて特定のサーバコンピュータに送信させるソフトウェア（以下、本項において「本件ソフトウェア」という。）を開発・販売したというものである。

東京高等裁判所は、不正プログラム該当性の判断基準について、「不正指令電磁的記録作成等罪における不正指令電磁的記録に該当するためには、プログラムに悪用の可能性があるというだけでは足りず、当該プログラムが実行者の意図に反する動作をさせる指令を与えると、客観的、一般的に想定される必要があると解される。しかし、プログラム自体からそのように想定されない場合でも、プログラム作成当時の客観的事情に照らし、その供用先としてどのような電子計算機が想定されるかを考慮して、当該プログラムが指令を与える電子計算機の使用者のうち例外的とはいえない範囲の者が、実行する意思がない状態で当該プログラムを実行させられることが想定される場合には、当該プログラムは、実行者の意図に反する動作をさせる指令を与えると客観的、一般的に想定されると認められ、不正指令電磁的記録に当たると解される。」と判示し、本件ソフトウ

[14] 東京高判令和元年 12 月 17 日高等裁判所刑事裁判速報集（令 1）号 362 頁（アンドロイドアナライザー事件）。

ェアについて、「主に浮気調査の目的を有する者に提供されることが予定された、浮気調査に適した機能を有するプログラムであり、購入者が、第三者の合意を得ずに、当該第三者が使用する……端末に……インストールして、当該第三者が知らないうちに実行することが一般に予想され、それがインストールされた……端末の使用者のうちの例外的とはいえない範囲の者が、実行する意思がない状態でそれを実行させられることが想定されるから、……実行者の意図に反する動作をさせる指令を与えると客観的、一般的に想定される」として、不正プログラムに該当する旨判断した原判決の認定を是認した。

（５）その他

不正指令電磁的記録に関する罪以外にも、コンピュータウイルスなどの不正なプログラムの使用等が、以下の各罪が定める構成要件を満たす場合には処罰の対象となり得る。

罪名	法定刑
私電磁的記録不正作出罪（刑法第 161 条の 2 第 1 項）	5 年以下の拘禁刑又は 50 万円以下の罰金
公電磁的記録不正作出罪（刑法第 161 条の 2 第 2 項）	10 年以下の拘禁刑又は 100 万円以下の罰金
不正作出電磁的記録供用罪（刑法第 161 条の 2 第 3 項）	対象となる電磁的記録が私電磁的記録の場合には 5 年以下の拘禁刑又は 50 万円以下の罰金、公電磁的記録の場合には 10 年以下の拘禁刑又は 100 万円以下の罰金
電子計算機損壊等業務妨害罪（刑法第 234 条の 2）	5 年以下の拘禁刑又は 100 万円以下の罰金
電子計算機使用詐欺罪（刑法第 246 条の 2）	10 年以下の拘禁刑
私電磁的記録毀棄罪（刑法第 259 条）	5 年以下の拘禁刑
公電磁的記録毀棄罪（刑法第 258 条）	3 月以上 7 年以下の拘禁刑

３．参考資料（法令・ガイドラインなど）

・刑法第 161 条の 2、第 168 条の 2、第 168 条の 3、第 234 条の 2、第 246 条の 2、第 258 条、第 259 条
・法務省ホームページ「いわゆるコンピュータ・ウイルスに関する罪について」
http://www.moj.go.jp/content/001267498.pdf
・大塚仁・河上和雄・中山善房・古田佑紀編「大コンメンタール刑法第三版第 8 巻」（青林書院、第三版、平成 26 年）

・杉山徳明・吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について　上」法曹時報 64 巻 4 号
・前田雅英ら編「条解刑法（第 4 版）」（弘文堂、令和 2 年）

4．裁判例

本文中に記載のとおり

Q74 電磁的記録不正作出罪

ウェブサイトに登録されたユーザデータを権限なく変更するなど不正にデータを改ざんする行為について、刑法上どのような罰則があるか。

タグ：刑法、私電磁的記録不正作出罪、公電磁的記録不正作出罪

１．概要

ウェブサイトに登録されたユーザデータ等の電磁的記録を変更するなどして不正にデータを改ざんする行為が、刑法第 161 条の 2 の構成要件に該当する場合には、電磁的記録不正作出罪が成立し得る。同罪の客体は、人の事務処理の用に供する権利、義務又は事実証明に関する電磁的記録である。ここで、「電磁的記録」とは、刑法第 7 条の 2 において「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。」と定義されており、ハードディスクや USB メモリ、DVD-R などに保存された記録が電磁的記録に該当する。

「人の事務処理」とは、財産上、身分上その他の人の社会生活に影響を及ぼし得ると認められる事柄の処理をいうとされている。また、権利、義務に関する電磁的記録とは、権利、義務の発生、存続、変更、消滅の要件となる電磁的記録のみならず、その原因となる事実について証明力のある電磁的記録を含むと考えられており、事実証明に関する電磁的記録とは、実社会生活に交渉を有する事項を証明するに足りる電磁的記録をいうとされている。例えば、サーバコンピュータ内に保存されている顧客に関する情報などがこれに該当し得る。

さらに、電磁的記録文書等（文書等として表示されて行使されることとなる電磁的記録）の偽造等の罪が創設[15]され、刑法第 155 条以下（文書偽造の罪）の枠組みの中で、文書等として表示されて行使されることとなる電磁的記録についても紙媒体の文書と同様に刑罰法規による保護の対象とされている。

２．解説

（１）私電磁的記録不正作出罪

刑法第 161 条の 2 第 1 項

人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、5 年以下の拘禁刑又は 50 万円以下の罰金に処する。

[15] 情報通信技術の進展等に対応するための刑事訴訟法等の一部を改正する法律（令和 7 年 6 月 12 日施行）により、偽造等の対象に電磁的記録文書等が追加された。

本罪は、刑法等の一部を改正する法律（昭和 62 年法律第 52 号）によって刑法に新設された。本罪は、文書偽造の罪（刑法第 2 編第 17 章）の一つとして規定され、電子計算機によって収集、処理、記録された情報が、文書に代わり、社会的に重要なものとなってきたことを踏まえ、電磁的記録を勝手に作り出したり、勝手に作り出した電磁的記録を事務処理の用に供したりするような、その当罰性等において文書偽変造、同行使罪に匹敵する反社会的行為を処罰するため本条を新設し、電磁的記録にふさわしい刑法上の保護を図ることとしたものである。

「人の事務処理を誤らせる目的」とは、不正に作られた電磁的記録を用いて他人の事務処理を誤らせる目的のことである。「事務処理」とは、財産上、身分上その他の人の社会生活に影響を及ぼし得ると認められる事柄の処理を意味し、業務性を有するか、法律的事務か、財産上の事務かという点は問わないとされている。

権利、義務に関する電磁的記録とは、権利、義務の発生、存続、変更、消滅の要件となる電磁的記録等をいい、例えば、オンライン化された銀行の元帳ファイルの記録、乗車券の磁気ストライプ部分等が当たり得る。また、例えば IC カードを利用した入館証について、その脆弱性を利用するなどしてカード自体又は記録されているデータを複製したり改ざんしたりした場合にも、本罪が成立する可能性がある。

事実証明に関する電磁的記録とは、実社会生活に交渉を有する事項を証明するに足りる電磁的記録をいい、裁判例では、パソコン通信サービスを提供する会社のホストコンピュータ内の顧客データベースファイル（京都地判平成 9 年 5 月 9 日判時 1613 号 157 頁）、ネットオークション運営会社が管理するサーバコンピュータ内の会員情報に関する記録（大阪高判平成 19 年 3 月 27 日判タ 1252 号 174 頁）がこれに当たるとされている。

「不正に作」るとは、事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を権限なく又は権限を濫用して[16]作ることをいい、記録をはじめから作り出す場合のほか、既存の記録を部分的に改変、抹消することによって新たな電磁的記録を存在するに至らしめる場合も含むとされている。

（２）公電磁的記録不正作出罪

刑法第 161 条の 2 第 2 項

前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、10 年以下の拘禁刑又は 100 万円以下の罰金に処する。

[16] 本罪は、「不正に作」ることを処罰するものであって、内容虚偽の電磁的記録を作出することを一般的に処罰の対象とするものではない。例えば、記録の内容を自由に決定できる者の記録の作出にあっては、内容に虚偽があっても、本罪には該当しない。

刑法第 161 条の 2 第 2 項は、同条第 1 項よりも重い処罰が規定されている。これは、公電磁的記録は私電磁的記録よりもその信用性が高く、社会的に重要な機能を果たしているためにこれを厚く保護する必要があるからである。同項の客体は、「公務所又は公務員により作られるべき」電磁的記録であり、公務所又は公務員の職務遂行として作出されることとされているものをいう。具体例として、自動車登録ファイルや運転者管理ファイルの記録、住民基本台帳ファイルの記録、航空運送貨物の税関手続の特例等に関する法律に基づく電子情報処理組織における申告の記録等が当たり得る。

（３）電磁的記録文書等偽造等の罪の創設

本罪は、情報通信技術の進展等に対応するための刑事訴訟法等の一部を改正する法律（令和 7 年法律第 39 号）による刑法改正において新設されたものであり、令和 7 年 6 月 12 日から施行されている。

同法律による刑事訴訟法の改正後は、電子データによる令状の発付や執行が可能となるところ、それに伴い、電子データによる令状を偽造して悪用する事案の発生が懸念される。また、それ以外でも、私人にもスマートフォンが普及しており、私人がスマートフォンの画面に作成権限がないのに作成したデータを表示して行使するという事案も考えられる。さらに、私人が公務所や著名人などの他人になりすまして虚偽の内容の電子データを作成し、インターネット上で悪用する行為についても、問題となっている。

そこで、文書等と同様の機能を営む電子データに対する社会的信頼を文書等と同様に保護する観点から、本罪が新設されたものである。

処罰の対象となる行為は、従来の文書偽造罪と同様、行使の目的で、公務所又は公務員の作成すべき電磁的記録文書等を偽造する行為や、行使の目的で、権利、義務若しくは事実証明に関する電磁的記録文書等を偽造する行為である。また、印章偽造罪に対応するものとして電磁的記録印章等（印章等として表示されることとなる電磁的記録）偽造等の罪が、虚偽診断書等作成罪に対応するものとして虚偽電磁的記録診断書等作成の罪が、公記号偽造の罪に対応するものとして公電磁的記録記号（記号として表示されることとなる電磁的記録）偽造等の罪が、それぞれ新設されている。

（４）裁判例

前述の各裁判例のほか、例えば、A 社が開発した衛星放送を視聴するための A カードに記録されたデータを改変する行為につき本罪が成立するかどうかが争われた事案において、「A カードに記録された電磁的記録は、衛星放送事業者から送信される事業者ごとの視聴契約情報に基づき、当該カードを所持しその使用権限を有する一般視聴者の衛星放送受信権限について、衛星放送ごとに受信権限の有無及びその期限を記録することによって、受信権限のある者による受信を可能にし、受信権限のない者による受信は不能にするものであるから、視聴契約に基づく受信権限の有無により個別の受信機による当該

衛星放送受信の可否、ひいてはその視聴の可否を管理するという、衛星放送事業者の財産上又は社会的責務上の事務処理の用に供する電磁的記録であるとともに、衛星放送事業者との視聴契約に基づく受信権限に関する電磁的記録である」、「被告人が本件各 A カードに記録された電磁的記録を改変した行為は、被告人が、受信権限のない衛星放送を受信して視聴するため、上記電磁的記録を、あたかも被告人に当該受信権限があるかのように当該衛星放送事業者の許諾を得ることなく書き換えるものであるから、同事業者の上記事務処理を誤らせる目的で、同事業者の上記事務処理の用に供している、同事業者との視聴契約に基づく受信権限に関する電磁的記録の不正作出に当たるということができる」として本罪の成立を認めたものがある（大阪高判平成 26 年 5 月 22 日（平成 26 年（う）第 121 号））。

また、暗号資産（仮想通貨）取引所を運営していた会社の代表取締役であった被告人が、サーバコンピュータ内の暗号資産取引の仲介を行うシステムに設けた被告人のアカウントの米ドル口座の残高が増加した旨の虚偽情報を作出し、前述サーバコンピュータに記録保存させた私電磁的記録不正作出、同供用の事案につき、「本件各行為は、被告人に許された権限を濫用し、会社の意思に反するものであり、架空の暗号資産についての取引を行うためのものであるから、利用規約上予定されていない事務処理であって、会社の事務処理を誤らせる目的であったことも明らかである」とした原判決の認定を是認して、控訴を棄却したものがある（東京高裁令和 2 年 6 月 11 日（令和元年（う）第 948））。

３．参考資料（法令・ガイドラインなど）

・刑法第 7 条の 2、第 161 条の 2、第 163 条の 2
・大塚仁・河上和雄・中山善房・古田佑紀編「大コンメンタール刑法第三版第 8 巻」（青林書院、第三版、平成 26 年）234 頁以下
・第 217 回国会　法務委員会　第 8 号会議録

４．裁判例

本文中に記載のとおり

Q75 電子計算機使用詐欺罪

例えばインターネットバンキングなどにおいて他人になりすまし、別の銀行口座へ送金するような行為について、刑法上どのような罰則があるか。

タグ：刑法、電子計算機使用詐欺罪

１．概要

インターネットバンキングにおいてIDやパスワードを不正入手して他人になりすましてログイン[1]し、別の銀行口座に送金するなどの行為が、「人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた」と認められる場合には、電子計算機使用詐欺罪が成立し得る。さらに、近時では、いわゆる「サポート詐欺[2]」により、被害者に「端末を修復するため」などと称してオンラインバンキングのアカウント情報やワンタイムパスワードを提供させ、それを用いて犯人が不正送金を行う事例も報告されており、このような場合も、電子計算機使用詐欺罪に該当し得る。

２．解説

刑法第246条の2

前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、10年以下の拘禁刑に処する。

（１）「前条に規定するもののほか」

電子計算機使用詐欺罪は、電子計算機の発展により、事務処理に電子計算機が利用されるようになり、財産権の得喪、変更の事務が、人を介さず電磁的記録に基づいて自動的に処理されるようになってきたことに鑑み、人を介した取引であれば詐欺罪に当たるような不正な行為であって電子計算機によって機械的に行われるものについて、その処罰を可能にするために創設された規定である。

[1] なお、ID やパスワードを不正に入手してログインする行為については、不正アクセス禁止法における不正アクセス行為に該当し得る。詳細については Q78 を参照。

[2] サポート詐欺とは、PC でインターネットを閲覧中に、突然、ウイルス感染したかのような嘘の画面を表示させたり、警告音を発生させるなどして、ユーザの不安を煽り、画面に記載されたサポート窓口に電話をかけさせ、サポートの名目で金銭を騙し取しとったり、遠隔操作ソフトをインストールさせたりする手口をいう。

本条は「前条に規定するもののほか」と規定し、本罪が詐欺罪を補充する規定である旨が明示され、本罪に外観上該当する行為であっても、事務処理の過程に人に対する欺く行為が存在し、前条の詐欺罪が成立すると認められる場合には同罪が適用される。

（２）「人の事務処理」

「人の事務処理」とは、一般的には、他人の財産上、身分上その他の人の生活関係に影響を及ぼし得る事柄の処理をいうとされ、（４）に後述するとおり、本罪の場合には、事柄の性質上、財産権の得喪、変更に係る事務に限定される。

（３）「虚偽の情報若しくは不正な指令を与えて」

「虚偽の情報」とは、電子計算機を使用する当該事務処理システムにおいて予定されている事務処理の目的に照らし、その内容が真実に反する情報をいう（東京高判平成 5 年 6 月 29 日高刑集 46 巻 2 号 189 頁）。

この点に関して、窃取したクレジットカードを利用して、インターネットを介し電子マネーを購入した事案について、「本件クレジットカード名義人による電子マネーの購入申込みがないにもかかわらず、本件電子計算機に同カードに係る番号等を入力送信して名義人本人が電子マネーの購入を申し込んだとする」情報が「虚偽の情報」に当たるとした最高裁判例がある（最決平成 18 年 2 月 14 日刑集 60 巻 2 号 165 頁）。クレジットカードの名義人でない者が名義人になりすまして同カードの使用権限があるかのように装い、加盟店の店員を欺き、物品を購入する行為が詐欺罪に該当する（最決平成 16 年 2 月 9 日刑集 58 巻 2 号 89 頁）とされており、人ではなく、電子計算機を介してのクレジットカード決済を経た行為について電子計算機使用詐欺罪が成立するとした前掲・最決平成 18 年 2 月 14 日は、本罪の立法趣旨に適うといえるとされている。

他にも、銀行のオンラインシステムの端末を操作して、振替入金の事実がないのに、同システムの電子計算機に対して、自己の預金口座等に振替入金があったとする虚偽の情報を与えて同計算機に接続されている記憶装置の磁気ディスクに記録された同口座の預金残高を書き換えた事例（大阪地判昭和 63 年 10 月 7 日判時 1296 号 151 頁）などがある。

さらに、近時問題となっているサポート詐欺において、被害者から詐取した ID・パスワード・ワンタイムパスワードを用いてログイン・送金操作をする場合には、「正規利用者がその意思に基づいて送金した」との虚偽の情報を与えた構造となり、本要件に該当し得る。また、被害者を誤信させ、送金操作と気付かせないまま送金操作をさせた場合、被害者を介して電子計算機に虚偽の情報を与えたと評価し得る（大阪高判平成 28 年 7 月 13 日・高刑速平 28 年 8 号 195 頁）。

加えて、暗号資産の不正取引を行った事案について、最高裁は、「不正に入手した秘密鍵で署名した上で（暗号資産）の移転行為に係るトランザクション情報を（暗号資産）の

ネットワークに送信した行為は、正規に秘密鍵を保有する者が（暗号資産）の取引をするものであるとの『虚偽の情報』を（暗号資産）のネットワークを構成する NIS ノード（サーバ）に与えたものというべきである。」と判示し、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律違反の前提犯罪である、電子計算機使用詐欺罪の「虚偽の情報」の送信に当たると判断した（最判令和 6 年 7 月 16 日）。

また、「不正な指令」とは、当該事務処理の場面において与えられるべきではない指令のことをいう。

（４）「財産権の得喪若しくは変更に係る不実の電磁的記録」

「財産権の得喪若しくは変更に係る」電磁的記録とは、財産権の得喪、変更の事実又はその得喪、変更を生じさせるべき事実を記録した電磁的記録であって、一定の取引場面において、その作出、更新により事実上当該財産権の得喪、変更が生じることとなるようなものをいう。

本罪は、電磁的記録不正作出等罪（刑法第 161 条の 2・詳細は Q74（電磁的記録不正作出）を参照。）の条文の文言と異なり、「……関する電磁的記録」ではなく、「……係る電磁的記録」と規定されており、記録の作出等と事実上の財産権の得喪、変更との間に直接的あるいは必然的な関連性を要するとされている[3]。裁判例では、金融機関のオンラインシステムにあって事務センターのコンピュータに接続された磁気ディスク等（元帳ファイル）に記憶、蓄積された預金残高の記録（前掲・大阪地判昭和 63 年 10 月 7 日、東京地八王子支判平成 2 年 4 月 23 日判時 1351 号 158 頁等）がこのような電磁的記録に当たるとされ、売掛金等の請求や、買掛金、給与の支払の事務処理の目的で作成される企業内のファイルのうちで自動引落し用に作成された記録、自動改札に用いられる切符の磁気面の日付、金額、発車駅コード等の記録などがこれに当たり得るものとされている。なお、一定の資格を証明するための記録は、財産権の得喪、変更に「関する」記録ではあるが、財産権の得喪、変更に「係る」電磁的記録には該当しない[4]。

「不実の電磁的記録」とは、真実に反する内容の電磁的記録のことをいう。前述最高裁決定は、「虚偽の情報を与え、名義人本人がこれを購入したとする財産権の得喪に係る不実の電磁的記録を作」ったと判示した（前掲・最決平成 18 年 2 月 14 日）。

（５）「財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して」

「財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して」とは、行為者が真実に反する財産権の得喪、変更に係る電磁的記録を他人の事務処理に使用される電子計算機において用い得る状態に置くことをいうとされている。

---

[3] 米澤慶治編「刑法等一部改正法の解説」（立花書房、昭和 63 年）118 頁参照。
[4] 前掲注 3・米澤編 121 頁参照。

（６）「財産上不法の利益を得、又は他人にこれを得させた」

本罪は、「財産上不法の利益を得」たか「他人にこれを得させた」場合に既遂に達する。本罪の対象は、電子計算機の不正利用による不法利得行為の全てではなく、財産上の得喪、変更の事務が電磁的記録に基づいて自動的に処理される場面での不法利得行為のみを対象としている。また、財物は本罪の客体には該当しない。

「財産上不法の利益を得」るとは、財物以外の財産上の利益を不法な手段、方法で得ることをいい、不実又は虚偽の電磁的記録に基づき預金債権があるものとしてその引出、振替を行うことができる地位を得るなど、事実上財産を自由に処分できるという利益を得ること、機械的に料金の計算及び請求が行われることとなる課金ファイルの記録を改変して料金の請求を免れることなどがある。「他人にこれを得させ」るとは、他人にこのような財産上の利益を不法に得させることをいう。

（７）電子計算機使用詐欺罪の犯罪地

刑法は、「日本国内において罪を犯したすべての者」（国内犯）に適用される（同法第 1 条第 1 項）[5]。そして、構成要件該当事実の一部が日本国内で発生した場合には、国内犯として処罰の対象となると解されている。すなわち、行為が国内で行われれば結果が国外で発生しても（大判明治 44 年 6 月 16 日刑録 17 輯 1202 頁）、また、行為が国外で行われても結果が国内で発生すれば、国内犯であると解されている。この点について、裁判例では、特定の暗号資産について、当該暗号資産の得喪又は変更は、サーバによる承認を経て、ブロックチェーンに組み込まれた情報が各サーバに共有されることによってその権利関係が確定するものであるため、サーバのうち少なくとも 1 台が日本に所在しているなどの事実関係の下では、日本国内において「財産権の得喪若しくは変更に係る不実の電磁的記録を作」ったといえ、日本で構成要件の一部である結果が発生したと認定したものがある（東京地判令和 3 年 3 月 24 日、東京地判令和 3 年 7 月 8 日）。

３．参考資料（法令・ガイドラインなど）

本文中に記載したもののほか、

- 大塚仁・河上和雄・中山善房・古田佑紀編「大コンメンタール刑法第三版第 8 巻」（青林書院、第三版、平成 26 年）
- 前田雅英ら編「条解刑法（第 4 版）」（弘文堂、2020）802 頁
- 米澤慶治編「刑法等一部改正法の解説」（立花書房、1988）

４．裁判例

本文中に記載のとおり

[5] 電子計算機使用詐欺罪を含む一定の罪は、日本国籍を有する行為者が日本国外で罪を犯した場合にも適用される（同法第 3 条）。

Q76 スキミング

スキミングとはどのような手口なのか。刑法上どのような罰則があるか。

タグ：刑法、割賦販売法、スキミング、デビットカード、偽造、IC 化

１．概要

スキミング（skimming）とは、キャッシュカードやクレジットカードの磁気情報を瞬時にコピーする手口のことである。犯人は、不正にコピーした情報を元に偽造カードを作成し、本人に成りすまして、銀行預金を下ろしたり、買い物をしたりする。情報だけがコピーされるので、本人が偽造カードを作成されたことに気付きにくく、被害が大きくなりやすい。

例えば、不正にクレジットカードを作成したり、それで買い物をしたりするといったような行為やキャッシュカードやクレジットカードの磁気情報を不正にコピーする行為等については、罰則規定に該当すれば、処罰され得る。

スキミングを防ぐには、日頃から危機意識を持つことや不要なカードを作らないこと、残高確認を定期的に行うことなど、自衛的な手段も大切である。

２．解説

（１）スキミングの手口及び対策について

カード犯罪といえば、かつては、紛失したカードや盗難カードをそのまま不正に使用するケースが中心だったが、2000 年代になり、「スキマー」と呼ばれる機械を使ってカードの磁気情報を不正にコピーし、その情報を元に大量偽造するスキミング（skimming、吸い取り）と呼ばれる手法が使われるようになった。また、近年では、EC サイト上の入力フォームに不正な JavaScript 等を埋め込み、利用者が入力したカード情報・氏名・住所等を攻撃者に直接送信させて窃取する、いわゆる Web スキミングという手法もみられるようになっている。さらに、平成 25 年 12 月には、フィッシングメールを端緒として、攻撃対象企業に空調機器システムを提供していた会社から、攻撃対象企業のネットワークへ侵入できる暗証番号を不正入手した上、攻撃対象企業の POS 端末にマルウェアを送信するというサイバー攻撃が行われ、4,000 万件のクレジットカード情報と約 7,000 万件の個人情報が漏えいする事態も確認された。これは、攻撃対象企業ではなく、セキュリティの手薄な関連企業から攻撃を仕掛けるという高度な手口であり、重大な損害につながり得るものであるといえる[6]。

[6] 経済産業省情報処理振興課「情報セキュリティ分野の人材ニーズについて」（平成 27 年 3 月）（https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/joho_keizai/it_jinzai/pdf/002_03_00.pdf）

なお、フィッシング詐欺によるクレジットカード等の不正使用については、Q79 を参照されたい。

カードを利用する場合は、通常、加盟店の方で当該カードが事故カード等でないかを確認するため、CAT 端末（与信照会端末）や POS 端末（販売情報管理端末）から磁気情報がカード会社に送信され、カード会社の承認が返信される。磁気情報としては、会員氏名、会員番号、有効期限などが記録されており、さらに偽造を防止するための偽造防止コード（暗号）が記録されている。

しかし、磁気情報の暗号化は、磁気情報を丸ごとコピーして偽造カードに貼り付けてしまうスキミングの前ではほとんど意味がない。カードの外観上から本物であることを証明する、カード会社の虹色のロゴホログラムも偽造可能である。デジタル情報はオリジナルとコピーの判別が原理的に不可能であるから、このような方法で偽造されたカードは、視覚によるチェックをくぐり抜けて、完全に本物のカードとして通用する。

このような偽造カードによる不正利用を防止するため、平成 28 年に割賦販売法が改正され、令和 2 年 3 月末までに、クレジットカードの IC 化 100%とともに、加盟店の店頭に設置するクレジット決済端末の IC 対応を完了することが目指されてきた（詳細については Q18 を参照されたい。）[7]。

また、平成 12 年からデビットカードのサービスも開始している。これは金融機関のキャッシュカードでそのまま店舗などでの支払を可能とするものである。店舗のカードリーダーにカードを通し、キャッシュカードと同じ暗証番号を入力すると、即座に利用者の口座から店舗に代金が支払われる。現在、非接触型のデビットカードも多く普及しているが、非接触型についてもスキミングが行われ得るため、デビットカードについても、IC 化が図られてきている。

（２）処罰対象行為について

スキミングにより偽造されたクレジットカードを使って買い物などする場合は、詐欺罪（刑法第 246 条）や電子計算機使用詐欺罪（同法第 246 条の 2）などの規定に該当すれば、処罰され得る。

また、平成 13 年に刑法の一部改正が行われ、支払用カード電磁的記録に関する罪（第 2 編第 18 章の 2）が新設された。キャッシュカードやクレジットカードの磁気情報を不正にコピーする行為等は、これらの規定に該当すれば、処罰され得る。すなわち、支払用カードを構成する電磁的記録の不正作出（同法第 163 条の 2 第 1 項）、不正作出に係る支払用カードを構成する電磁的記録の供用（同条第 2 項）、同電磁的記録をその構成部分とするカードの譲渡し・貸渡し・輸入（同条第 3 項）は、10 年以下の拘禁刑又は 100 万円以下の罰金に、同電磁的記録をその構成部分とするカードの所持（同法第 163 条の 3）

[7] 経済産業省ウェブサイト・割賦販売法（https://www.meti.go.jp/policy/economy/consumer/credit/11kappuhanbaihou.html）

は、5 年以下の拘禁刑又は 50 万円以下の罰金に、同法第 163 条の 2 第 1 項の罪の準備罪としての支払用カードを構成する電磁的記録の情報の取得・提供（同法第 163 条の 4 第 1 項）、保管（同条第 2 項）、器械・原料の準備（同条第 3 項）は、3 年以下の拘禁刑又は 50 万円以下の罰金に、それぞれ処することとされた。

このうち、同法第 163 条の 2 及び第 163 条の 4 第 1 項の罪については、未遂犯も処罰の対象である（同法第 163 条の 5）。

なお、電磁的記録の不正作出については Q74（電磁的記録不正作出）を、また、なりすましによるクレジットカード等の不正使用に関連して、電子計算機使用詐欺罪の詳細については Q75（電子計算機使用詐欺罪）を参照されたい。

（3）クレジット決済端末の 100%IC 対応化について

カード犯罪対策は技術との闘いである。技術的なセキュリティを常に高めることが必要である。そこで、上記（1）のとおり、カードそのものに小型のコンピュータである IC チップを組み込んだ IC カードに対応するクレジット決済端末への完全移行が進められてきた。IC カードは独自の演算機能をもち、磁気カードに比べ記憶容量が飛躍的に増すため、きわめて高度で複雑なセキュリティ・システムを実現することができ、現在の技術では偽造が不可能と言われているが、今後の偽造被害等の状況を注視していく必要はある。

3．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

4．裁判例

特になし

Q77 情報の不正入手・漏えい

情報の不正入手及び漏えいに関して、どのような罰則があるか。

タグ：刑法、著作権法、個情法、番号利用法、不正競争防止法、国家公務員法、地方公務員法、電気通信事業法、有線電気通信法、電波法、不正アクセス禁止法、割賦販売法、情報の不正入手、漏えい

１．概要

情報の不正入手や漏えいについては、情報一般を対象として処罰する規定はなく、様々な法律の中に情報の侵害の態様に応じて個別的な処罰規定が置かれているにすぎない。

情報の不正入手については、営業秘密侵害罪などがある。また、著作権法上、違法にインターネット上に掲載された著作物（以下、本項において「侵害コンテンツ」という。）のダウンロードが一定の要件の下で違法とされ、海賊版であることを知りながら有償著作物の侵害コンテンツ著作物を継続的に又は反復してダウンロードを行った場合は刑罰が科される可能性がある。

また、情報の漏えいについては、個人情報データベース等提供罪や秘密漏示罪などがある。情報の不正入手及び漏えいの双方を処罰対象として含むものとしては、通信の秘密侵害罪がある。その他、情報の不正入手や漏えいに付随する行為に罰則が設けられていることも多い。

なお、国家の安全保障に関する情報の保護について定める特定秘密の保護に関する法律及び重要経済安保情報の保護及び活用に関する法律については Q56 を参照されたい。

２．解説

（１）情報の不正入手や漏えいについての一般的な保護と罰則

コンピュータによる情報処理が一般的に行われるようになったことを受け、昭和 62 年に「電磁的記録」の定義規定（刑法第 7 条の 2）、電磁的公正証書原本不実記録罪関係（刑法第 157 条、第 158 条）、電磁的記録不正作出罪関係（刑法第 161 条の 2）、電子計算機損壊等業務妨害罪関係（刑法第 234 条の 2）、電子計算機使用詐欺罪関係（刑法第 246 条の 2）、電磁的記録毀棄罪関係（刑法第 258 条、第 259 条）などの処罰規定が整備された。その際、情報の不正入手についても一般的な処罰規定を設けることが議論されたが、保護すべき情報の範囲や保護の程度などについて議論が分かれ、将来の課題とされた。情報は、同じ内容であっても人によって価値が異なり、時間の経過によってもその価値が変動する。このような客体に対して、一律に刑罰による保護を設定することには無理があり、個別的に保護せざるを得ないためである。

このように、情報の不正入手や漏えいについては、一律に保護されているわけではなく、個別的な保護がなされている[1]。

（２）個人情報データベース等不正提供等罪

個人情報取扱事業者若しくはその従業者又はこれらであったものが、業務で取り扱っている個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供（第三者が利用できる状態に置くこと）し、又は盗用（盗み利用すること）した場合には罰則が科される（個情法第 179 条）。現に役員や従業員である者のみならず、役員や従業員であった者についても処罰対象とされる。行為者のみならず、当該行為者を使用人その他の従業者とする法人等についても罰則の対象となる（同法第 184 条）[2]。

また、個人情報取扱事業者は、個人情報の適正な取得（同法第 20 条）等が義務づけられており、違法行為に関する個人情報保護委員会による命令に違反した場合には、罰則の対象（同法第 178 条）となる。なお、行政機関の職員等についても個情法第 179 条と類似の罰則がある（同法第 180 条、また、個人の秘密が記録された個人情報ファイルの提供について第 176 条）。

その他個情法以外の個人情報の適正な取扱いに関する主な法令においては、例えば、番号利用法第 49 条、第 57 条にも個情法第 179 条と類似の罰則が設けられている。

（３）営業秘密侵害罪

不正競争防止法は、営業秘密の不正取得・使用・開示行為（不正競争行為）のうち、特に違法性が高い行為について、営業秘密侵害罪として 10 年以下の拘禁刑又は 2,000 万円以下の罰金（又はその併科）を科すこととしており（不正競争防止法第 21 条第 1 項第 1 号ないし第 5 号、同条第 2 項第 1 号ないし第 5 号）、正当に示された営業秘密を不正に使用等する行為以外については、行為者を使用人、従業者とする法人についても 5 億円以下の罰金という高額の罰金を科すこととしている（同法第 22 条第 1 項第 2 号）。営業秘密侵害罪については、退職者や従業者、転得者への処罰範囲の拡大が行われ、また、法定刑の引き上げも行われるなど、段階的に改正されており、平成 27 年改正では、非親告罪化及び海外重罰規定の導入がなされた（後者の詳細については、Q34 を参照されたい。）。

いずれの行為も、「不正の利益を得る目的」又は「営業秘密保有者に損害を加える目的」（図利加害目的）で行う行為が刑事罰の対象であり、公益の実現を図る目的で不正情報を内部告発する行為は図利加害目的で行う行為に当たらない。また、日本国内において事業

[1] なお、個情法においては、「偽りその他不正の手段」による個人情報の取得が禁止されている（同法第 20 条第 1 項）。

[2] この点については、個人情報保護委員会から、適用事例等を踏まえた注意喚起が出されている（個人情報保護委員会事務局「個人情報データベース等不正提供等罪の適用事例等を踏まえた安全管理措置及び漏えい等の報告に関する留意点について（注意喚起）」（令和 5 年 11 月 16 日））（https://www.ppc.go.jp/files/pdf/231116_alert_fuseiteikyou.pdf）。

を行う営業秘密保有者の営業秘密については、日本国外で不正に取得・使用・開示した場合についても処罰の対象となる。

近時、ランサムウェア等のサイバー攻撃により窃取された営業秘密がダークウェブ上に掲載される事案が見られるが、「非公知性」の要件との関係では、ダークウェブへの掲載は一般の検索等では到達困難な領域で行われることが多く、その一事をもって直ちに「非公知性」を喪失するものではなく、「秘密管理性」と「有用性」の要件が充足されれば営業秘密性が認められると考えられる[3]。

また、秘密管理性の判断は営業秘密の管理単位で判断されるものであることから、ダークウェブにおいて掲載された場合であっても、秘密管理実態が維持されている限り、掲載後であっても営業秘密として認められ得る。

さらに、ダークウェブ上のサイトから営業秘密を「取得」するだけで直ちに営業秘密侵害罪の構成要件を充足するわけではなく、「不正の利益を得る目的」又は「営業秘密保有者に損害を加える目的」（図利加害目的）が必要となることは、前述のとおりである。

（４）侵害コンテンツの違法ダウンロードに対する刑事罰

著作権法は、音楽・映像だけでなく、漫画・書籍・論文・コンピュータプログラムなど著作物全般について、私的使用目的であっても、一定の場合には違法にアップロードされた著作物をダウンロードすることを著作権の制限の対象外とし（同法第 30 条第 1 項第 4 号）、さらに、このうち正規版が有償で提供されている著作物を反復・継続してダウンロードした場合に 2 年以下の拘禁刑又は 200 万円以下の罰金（又はその併科）を科す対象としている（同法第 119 条第 3 項第 2 号）。

（５）秘密漏示罪

情報を扱う一定の者に守秘義務を課し、漏えいがあった場合に、その義務違反という形で刑事責任が問われる。典型的なものとしては、公務員に対して職務上知り得た秘密を漏らす行為を処罰する、国家公務員法（昭和 22 年法律第 120 号）や地方公務員法（昭和 25 年法律第 261 号）に基づく守秘義務違反の罪（国家公務員法第 100 条第 1 項、同法第 109 条第 12 号、地方公務員法第 34 条第 1 項、同法第 60 条）や、医師や弁護士などによる秘密漏示罪（刑法第 134 条）が挙げられる。他にも、様々な職種において守秘義務違反の罪が規定されている。

（６）通信の秘密侵害罪

「電気通信事業者の取扱中にかかる通信」（電気通信事業法第 4 条第 1 項）、「有線電気通信」（有線電気通信法（昭和 28 年法律第 96 号）第 9 条）、「特定の相手方に対して行われる無線通信」（電波法第 59 条）については何人であってもその秘密を侵害する行為は

[3] 営業秘密管理指針 22 頁。

処罰される（電気通信事業法第 179 条第 1 項、有線電気通信法第 14 条第 1 項、電波法第 109 条第 1 項）。電気通信事業者、有線電気通信の業務に従事する者、無線通信の業務に従事する者が、それぞれ通信の秘密を侵害した場合には、重く処罰される（通信の秘密については、Q47 を参照されたい。）。

（７）識別符号の不正取得・漏えい

ログイン ID・パスワードなどの他人の識別符号の不正取得及び不正アクセスを助長する当該識別符号の提供行為については刑事罰が科される（不正アクセス禁止法第 4 条、第 5 条。Q78 も参照されたい。）。

（８）クレジットカード番号の不正取得・漏えい

不正アクセス行為によってクレジットカード番号を取得すること（割賦販売法第 49 条の 2 第 2 項第 2 号）及び正当な理由なく有償でクレジットカード番号の提供を受ける行為（同条第 3 項）については刑事罰が科される。

（９）その他付随する行為に対する刑事罰

情報の不正入手の付随行為が、現実空間で発生した場合には、その付随行為について刑法における窃盗罪や住居侵入罪等で処罰される場合がある。また、情報の不正入手がネットワークに接続したサイバー空間で発生し、不正アクセス行為が行われたなどの場合は、不正アクセス禁止法により処罰され得る。

いわゆるスタンドアロンのコンピュータの場合は不正アクセス禁止法の適用が困難だが（Q78 参照）、例えばコンピュータを一時的に外に持ち出すなどして、いったん自己の支配下に置いた上で、中の情報をコピーし、そのコンピュータを元の場所に戻すような場合は、そのコンピュータに関する窃盗罪や横領罪が成立し得る。

３．参考資料（法令・ガイドラインなど）

・著作権法第 30 条第 1 項第 4 号、第 119 条第 3 項第 2 号
・個情法第 20 条、第 174 条、第 179 条
・番号利用法第 49 条、第 51 条、第 57 条
・不正競争防止法第 21 条第 1 項第 1 号～第 5 号、同条第 2 項第 1 号～第 5 号
・電気通信事業法第 179 条
・有線電気通信法第 14 条
・電波法第 109 条、第 109 条の 2
・不正アクセス禁止法第 4 条、第 5 条
・割賦販売法第 49 条の 2

４．裁判例

・最判昭和 55 年 11 月 29 日最高裁判所判例解説刑事篇（昭和 55 年度）315 頁

電波法 109 条 1 項における「窃用」とは「無線局の取扱中に係る無線通信の秘密を発信者又は受信者の意思に反して利用すること」と判示した事例。

・最判平成 30 年 12 月 3 日判時 2407 号 106 頁

営業秘密侵害罪について、転職直前に勤務先の営業秘密を私物 HDD に複製した事案について、不正の利益を得る目的を認定した事例。

Q78 不正アクセス

いわゆる不正アクセスに関して、不正アクセス禁止法上どのような行為が禁止されているか。

タグ：不正アクセス禁止法、アクセス制御機能、識別符号

１．概要

不正アクセス禁止法は、ネットワーク（電気通信回線）を通じて他人の識別符号を入力すること等により、アクセス制御機能により制限されている特定利用（ネットワークに接続している電子計算機（以下、本項において「特定電子計算機」という。）の利用）をし得る状態にさせる行為を不正アクセス行為としてとらえ、これを禁止及び処罰している。

「不正アクセス行為」というためには、特定電子計算機に対して、アクセス管理者がアクセス制御機能（特定電子計算機にアクセスをしようとするユーザを ID・パスワード等の識別符号により自動的に識別、認証するため、アクセス管理者によって付加される機能）を付加し、当該特定電子計算機に対してネットワークを通じて別のユーザがアクセスする際に、アクセス制御機能により制限することが必要である。

不正アクセス禁止法では、上記の不正アクセス行為を禁止しているほか、不正アクセス行為の予備的行為を禁止している。

なお、一般的に、識別符号を入力してもしなくとも同じ特定利用ができ、アクセス管理者が特定利用を誰にでも認めている場合には、アクセス制御機能による制限はないものと解されることとなり、同法は適用されない。

２．解説

（１）不正アクセス禁止法

不正アクセス禁止法は、不正アクセス行為等を禁止するとともに、これについての罰則及び再発防止のための都道府県公安委員会による援助措置等を定めることにより、ネットワークを通じて行われる特定電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的としている（不正アクセス禁止法第１条）。不正アクセス禁止法は、特定電子計算機に対して、アクセス管理者が「アクセス制御機能」を付加している場合に、ネットワークを通じて他人の識別符号を入力したりすることや、アクセス制御機能による制限を回避できる情報(識別符号であるものを除く。) 又は指令を入力したりすることで、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為を不正アクセス行為としてとらえ、これを禁止及び処罰している。

（２）アクセス制御機能

アクセス制御機能（不正アクセス禁止法第 2 条第 3 項）とは、特定利用を正規の利用権者やアクセス管理者以外の者ができないように制限するために、アクセス管理者が特定電子計算機や特定電子計算機とネットワークで接続されている他の特定電子計算機に付加している機能のことをいう。具体的には、特定電子計算機の特定利用をしようとする者にネットワークを経由して識別符号の入力を求め、入力された情報が識別符号に当たる場合にのみ特定利用の制限を自動的に解除し、識別符号に当たらない場合には利用を拒否する機能をいう。

（３）アクセス管理者

アクセス管理者とは、特定電子計算機の特定利用につき当該特定電子計算機の動作を管理する者（不正アクセス禁止法第 2 条第 1 項)、すなわち、特定電子計算機を誰に利用させるか、特定利用をさせる場合にはどの範囲とするかを決定する権限を有する者をいう。

（４）識別符号

識別符号（不正アクセス禁止法第 2 条第 2 項）とは、特定電子計算機の特定利用をすることについてアクセス管理者の許諾を得た利用権者及びアクセス管理者ごとに定められ、アクセス管理者が他の利用権者及びアクセス管理者と区別して識別することができるよう付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

1 号　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

ウェブサイト等にログインする際によく用いられる ID・パスワードのうちパスワードがこの代表例である。ID とパスワードの両方が使用される場合、パスワードのみでは識別符号として使用できず、ID と「組み合わせた」（同法第 2 条第 2 項柱書）識別符号となる。この場合、ID は、本号の符号に該当する符号（パスワード）と組み合わせて用いられる「その他の符号」にあたる[1]。

2 号　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

「身体の全部若しくは一部の影像」としては、指紋、虹彩、網膜等が挙げられる[2]。

本号の場合も、単体で識別符号となるものもあれば、他の符号（ID など）を組み合わせて識別符号となるものもある。

---

[1] 不正アクセス対策法制研究会「逐条不正アクセス行為の禁止等に関する法律」（立花書房、第 2 版、平成 24 年）46 頁参照。
[2] 前掲注 1・45 頁参照。

3 号　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

署名の形状やその筆圧、動態等から特徴を取り出して数値化し符号化したようなものを指す。

本号の場合も、単体で識別符号となるものもあれば、他の符号（ID など）を組み合わせて識別符号となるものもある。

（５）不正アクセス行為

不正アクセス行為は、ネットワークを通じて他人の ID・パスワード等の識別符号を入力することや、アクセス制御機能による制限を回避できる情報（識別符号であるものを除く。）又は指令を入力することで、特定利用の制限を解除する行為である（不正アクセス禁止法第 2 条第 4 項各号）。

同法第 3 条により不正アクセス行為が禁止されており、これに違反した場合、3 年以下の拘禁刑又は 100 万円以下の罰金が科される（同法第 11 条）。

したがって、不正アクセスがあった場合に不正アクセス禁止法違反を問えるかどうかは、アクセス制御機能により制限された状態にあったか否かという点が重要な要素となる。

また、他サイト等から流出・収集された ID・パスワードの「リスト」を多数のサービスで自動的に試行する、いわゆる「リスト型アカウントハッキング（アカウントリスト攻撃）」は、典型的には他人の識別符号の入力により特定利用を可能にする行為として不正アクセス行為に該当し得る[3]。

なお、不正アクセス行為の定義（同法第 2 条第 4 項）に「電気通信回線を通じて」とあるとおり、不正アクセス行為はネットワークを通じて行われる必要があるため、いわゆるスタンドアロンのコンピュータに関して同法違反を問うことはできない。

（６）その他不正アクセス行為の予備的行為について[4]

不正アクセス禁止法は、不正アクセス行為のほか、同行為の予備的行為のうち、「識別符号」に関する次の行為を禁止している。

① 不正アクセス行為の用に供する目的でアクセス制御機能に係る他人の識別符号を取得すること（同法第 4 条）

② 業務その他正当な理由による場合を除き、アクセス制御機能に係る他人の識別符号を第三者に提供すること（同法第 5 条）

[3] 関連して、識別符号の提供・保管等を伴う場合には、助長・保管等の予備的行為も問題となり得る（第 5 条、第 6 条）。

[4] これらの他、いわゆるフィッシング行為の禁止等については Q79 を参照されたい。

③　不正アクセスの用に供する目的で不正に取得されたアクセス制御機能に係る他人の識別符号を保管すること（同法第 6 条）

上記②のうち「業務その他正当な理由による場合」とは、社会通念上、正当と認められるような場合をいい、例えば、以下の行為が該当する。

- 情報セキュリティ事業者がインターネット上に流出している識別符号のリストを契約している企業に提供する行為
- インターネット上に流出している他人の識別符号を発見した者がこれを情報セキュリティ事業者や公的機関に届け出る行為
- 情報セキュリティに関するセミナーの資料等において、ID・パスワードのインターネット上への流出の実態を示すために実際に流出した ID・パスワードのリストを掲載する行為
- よく用いられがちな単純な ID・パスワードを設定すべきでないものとして示す行為
- アクセス管理者自らが行う提供行為やアクセス管理者の承諾を得て行う提供行為（利用権者が複数のウェブサイトに同一の識別符号を設定して使い回している状況を背景に、あるアクセス管理者が、他のアクセス管理者が管理するウェブサイトに対する不正アクセス行為に用いられることを知りながら自らが管理する識別符号を提供するような場合は「業務その他正当な理由による場合」には該当しない。）
- 利用権者の承諾を得て当該利用権者の識別符号を提供する提供行為

（7）裁判例（東京地判平成 17 年 3 月 25 日判時 1899 号 155 頁・判タ 1213 号 314 頁）

ネットワークコンピュータのファイル格納領域に保存されている秘密ファイル F にアクセスする方法として、アクセス制御機能による制限がある x という通信方法のほかに、（プログラムの瑕疵や設定の不備により、アクセス制御機能による制限がない）y という通信方法も存在しており、y を経由して、F にアクセスすることが「不正アクセス行為」となるのかが問題となった事案について、東京地裁は、アクセス制御機能の有無については、（個々の通信プロトコル[5]ごとに判断するのではなく）特定電子計算機ごとに判断するのが相当であり、管理者が特定電子計算機の特定利用を誰にでも認めている場合を除き、特定利用のうち一部がアクセス制御機能によって制限されている場合であっても、その特定電子計算機にはアクセス制御機能があると解すべきであるとした。

さらに、識別符号を入力してもしなくても同じ特定利用ができ、アクセス管理者が当該特定利用を誰にでも認めている場合には、アクセス制御機能による特定利用の制限はないと解すべきであるが、プログラムの瑕疵や設定上の不備があるため、識別符号を入力する以外の方法によってもこれを入力したときと同じ特定利用ができることをもって、直ちに識別符号の入力により特定利用の制限を解除する機能がアクセス制御機能に該当しなくなるわけではないと解すべきであるとした。

[5] ネットワーク上で通信するための手順や規約を指す。

３．参考資料（法令・ガイドラインなど）

・不正アクセス禁止法第 1 条、第 2 条第 3 項、第 2 条第 2 項各号、第 2 条第 4 項各号、第 3 条～第 6 条、第 11 条～第 13 条

４．裁判例

本文中に記載したもののほか、

・東京地判平成 29 年 4 月 27 日（平成 26 年特（わ）第 927 号・平成 27 年刑（わ）第 2373 号等）

フィッシングメール等を利用して複数企業のインターネットバンキングの識別番号を不正に取得し，不正アクセス行為を行った事案。

Q79 フィッシング

フィッシングとはどのような手口か。法令上どのような行為が禁止されているか。

タグ：不正アクセス禁止法、割賦販売法、フィッシング、識別符号、クレジットカード、フィッシング対策協議会

１．概要

一般に、フィッシング（Phishing）とは、実在する金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのウェブサイトとそっくりの偽サイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為を指す[1]。

一般にフィッシングと呼ばれる上記のような行為のうち、不正アクセス禁止法で禁止されている処罰対象の行為は、同法第 7 条各号で規定されている行為である。具体的には、正規のアクセス管理者であると誤認させ、ID・パスワード等の識別符号を取得するためのウェブサイトの公開や、HTML で作成された電子メール等により識別符号を入力させようとする行為を処罰の対象としている。

クレジットカード番号等の情報を入力させる行為は、同条各号で禁止する行為ではなく割賦販売法第 49 条の 2 第 2 項本文において規制されている不正取得に該当し得る。ただし、そのような種類の情報の入力を求めるサイトの公開や当該サイトへ誘導する電子メールの送信などの準備行為の段階では処罰対象ではなく、そのような種類の情報を実際に不正に取得した場合に処罰対象となる。

近時は、ID・パスワードによる認証後に送付されたワンタイムパスワード等をリアルタイムに詐取して二要素認証を突破する「リアルタイムフィッシング」や、SMS を悪用してフィッシングサイトに誘導する「スミッシング（Smishing)」、音声通話を悪用する「ヴィッシング（Vishing)」など多様化が進んでいる。また、EC サイト改ざんにより入力されたカード情報を盗む「ウェブスキミング」[2]、カード番号の規則性等を用いて有効な番号の組合せを機械的に突き止める「クレジットマスター攻撃」も関連手口として被害拡大要因となっている。これらのうち、識別符号（ID・パスワード等）の詐取を目的とするものは不正アクセス禁止法 7 条により、クレジットカード番号等の不正取得は割賦販売法第 49 条の 2 によりそれぞれ処罰され得る。

[1] サイバーセキュリティ 2025・226 頁。
[2] 詳細については、Q76 を参照されたい。

２．解説

（１）不正アクセス禁止法第 7 条各号が禁止する行為

不正アクセス禁止法第 7 条

> 何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。
>
> 1 号　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為
>
> 2 号　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）第 2 条第 1 号に規定する電子メールをいう。）により当該利用権者に送信する行為

一般にフィッシングと呼ばれる行為のうち、不正アクセス禁止法第 7 条及び第 12 条第 4 号に基づき処罰の対象となっているのは、アクセス管理者（同法第 2 条第 1 項）が公開したウェブサイト又はアクセス管理者が送信した電子メールであると利用権者に誤認させて、アクセス管理者が ID・パスワード等の識別符号（識別符号については Q78 参照。）の入力を求める旨の情報を閲覧させようとすることである。

このように、同法は、不正アクセス行為の前提となる ID・パスワード等の識別符号を入手するための行為を禁止している。

ア　サイト構築型

不正アクセス禁止法第 7 条第 1 号は、識別符号を入力することを求める旨の情報を表示させたサイトを公開することを手口とする行為を禁止している。正規のアクセス管理者が公開したと誤認させるものであり、アクセス管理者の名称やロゴを使用して公開されたウェブサイトなどが該当し得る。また、他人の ID・パスワード等の識別符号の入力を求める旨の情報が必要になるため、ウェブサイト上に ID・パスワード等の識別符号を入力するよう求める文章、入力欄及び送信用ボタンが表示されている場合などが該当する。

イ　メール送信型

不正アクセス禁止法第 7 条第 2 号は、電子メールによって ID・パスワード等の識別符号を入力させて詐取しようとする行為を禁止している。正規のアクセス管理者が送信したと誤認させるものであり、アクセス管理者の名称やロゴを使用して送信された電子

メールなどが該当し得る。また、他人の ID・パスワード等の識別符号の入力を求める旨の情報が必要になるため、HTML を用いて電子メールの本文欄に ID・パスワード等の識別符号を入力するよう求める文章、入力欄及び送信ボタンが表示されている場合などが該当する。

（2）クレジットカード番号等のカード情報の不正取得

インターネット上でクレジットカード情報を利用するための本人認証サービス（3D セキュア[3]）として入力されるパスワードは識別符号に該当する場合があるため、これを不正取得するウェブサイトの構築・公開は不正アクセス禁止法第 7 条第 1 号（サイト構築型）に該当する場合がある。しかし、クレジットカード番号、有効期限、セキュリティコードなどの券面情報は識別符号ではないため、当該情報を不正に取得するためにウェブサイトを構築・公開し、当該情報を取得した場合には、割賦販売法違反によって処罰され得る（割賦販売法第 49 条の 2 第 2 項本文）。

割賦販売法第 49 条の 2

1 項　クレジットカード番号等取扱業者若しくはクレジットカード番号等取扱受託業者又はこれらの役員若しくは職員若しくはこれらの職にあつた者が、その業務に関して知り得たクレジットカード番号等を自己若しくは第三者の不正な利益を図る目的で、提供し、又は盗用したときは、3 年以下の拘禁刑又は 50 万円以下の罰金に処する。

2 項　人を欺いてクレジットカード番号等を提供させた者も、前項と同様とする。クレジットカード番号等を次の各号のいずれかに掲げる方法で取得した者も、同様とする。

1 号　クレジットカード番号等が記載され、又は記録された人の管理に係る書面又は記録媒体の記載又は記録について、その承諾を得ずにその複製を作成すること。

2 号　不正アクセス行為（不正アクセス禁止法第 2 条第 4 項に規定する不正アクセス行為をいう。）を行うこと。

3 項　正当な理由がないのに、有償で、クレジットカード番号等を提供し、又はその提供を受けた者も、第一項と同様とする。正当な理由がないのに、有償で提供する目的で、クレジットカード番号等を保管した者も、同様とする。人を欺いてクレジットカード番号等を提供させた者も、前項と同様とする。

4 項　前三項の規定は、刑法その他の罰則の適用を妨げない。

[3] 「3D セキュア」とは、カード会員のみが知るカード会社（イシュアー）に事前に登録したパスワード等を、カード利用時に当該カード会社（イシュアー）が照合することにより、本人が取引を行っていることを確認するものであり、国際ブランドが推奨する本人確認手法である（クレジット取引セキュリティ対策協議会「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 2019」（2019 年）39 頁　https://www.j-credit.or.jp/security/pdf/plan_2019.pdf）。

（３）フィッシング行為の処罰

これまで解説したように、ID・パスワード等の識別符号を入力させて詐取するためにフィッシングサイトを公開するなどした場合は不正アクセス禁止法第 7 条及び第 12 条第 4 号により、また、クレジットカード番号等の情報を窃取した場合は割賦販売法 49 条の 2 第 2 項本文により処罰され得る。

（４）フィッシング対策の取組

以上のとおり、一般にいうフィッシング行為の一部は処罰の対象となっているが、一方で、フィッシングの手口は年々高度化、巧妙化しており、フィッシングサイトの数も増加傾向にある。フィッシングサイトを放置すればそれだけ被害が拡大することとなるため、社名やサービス名などブランドを不正に騙られることにより被害を受けるおそれがある事業者としては、フィッシングへの対策を行うことが肝要である。

平成 17 年に設立されたフィッシング対策協議会は、フィッシング被害が発生する前に心がけておくべき事業者の対策を「フィッシング対策ガイドライン 2025 年度版」[4]としてとりまとめており、ウェブサイトの運営者がフィッシング被害の発生を抑制するための対策として、以下の 5 つの項目を挙げ、合計 10 の要件を設けている。

① 利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること
② 利用者に送信する SMS においては、国内の携帯キャリアに直接接続される送信サービスを利用し、事前に発信者番号等を Web サイトなどで告知すること
③ 多要素認証を要求すること
④ ドメイン名は自己ブランドと認識して管理し、利用者に周知すること
⑤ フィッシングについて利用者に注意喚起すること

フィッシングサイトの閉鎖（テイクダウン）は自社で対応することも可能だが、海外でホストされているケース等においては、専門機関に対する対応要請を行うとともに、フィッシング対策協議会への相談が推奨されている。なお、フィッシング対策協議会は、JPCERT/CC に対してフィッシングサイトをテイクダウンするための調整依頼を行っている。

加えて、一般財団法人日本サイバー犯罪対策センター（JC3）は、フィッシングサイト等の削除依頼（ABUSE 報告）を容易にする独自ツール「Predator」を開発し、ボランティアや会員企業等に提供してテイクダウン活動を推進している。定期的に「フィッシングサイト撲滅チャレンジカップ／チャレンジマラソン」等のイベントが開催され、集中的な

[4] https://www.antiphishing.jp/report/antiphishing_guideline_2025.pdf

削除要請が実施されているため、事業者の対処オプションとして把握しておくと有用である[5]。

（５）フィッシングサイトによりデータ漏えいが起こった場合の報告要否

個人情報取扱事業者の正規のウェブサイトに偽装したウェブサイト（いわゆるフィッシングサイト）に本人が入力した場合の取扱いについて、個別の事案ごとに判断される。例えば、以下のように考えられる。

① 本人が事業者の正規サイトを経由せずに偽サイトへ自発的にアクセスして入力しただけでは、当該事業者における「漏えい等」の報告対象にはならない。

② 正規サイトや正規メール内のリンクが改ざんされ、偽サイトへ誘導された場合には、事業者が『取得しようとしている』情報の漏えいに該当し、報告対象となり得る。

③ 偽サイトで詐取した ID・パスワードにより第三者が本人になりすましてログインし個人データを閲覧した場合、一般に報告対象となる。

３．参考資料（法令・ガイドラインなど）

本文中に記載したもののほか、

・「不正アクセス禁止法改正 Q&A」
https://www.npa.go.jp/bureau/cyber/pdf/6_QA.pdf

・サイバーセキュリティ 2025・226 頁

・フィッシング対策協議会 技術･制度検討ワーキンググループ「フィッシングレポート」

４．裁判例

・東京地判平成 29 年 4 月 27 日（平成 26 年特（わ）第 927 号・刑（わ）第 2373 号等）
フィッシングメール等を利用して複数企業のインターネットバンキングの識別番号を不正に取得し，不正アクセス行為を行った事案。

[5] 日本サイバー犯罪対策センター「フィッシングサイト撲滅への取組」（https://www.jc3.or.jp/activity-report/challengecup.html）

Q80 フェイクニュース対策

偽・誤情報（フェイクニュース）を利用したサイバー攻撃を規制する法令と罰則はどのようなものがあるか。企業として偽・誤情報対策を講じるに当たって、留意すべきポイントは何か。

タグ：刑事法、偽情報、誤情報、悪意のある情報、フェイクニュース、発信者情報開示、不正アクセス

１．概要

フェイクニュースは、主としてインターネット上で発信・拡散される、内容が真実ではない情報を指すものであり、政策的な対応の検討に当たっては、①誤情報（Misinformation：意図せず誤った情報を拡散）、②偽情報（Disinformation：意図的・計画的に虚偽情報を流布）、③悪意のある情報（Mal-information：真実の断片や漏えい情報を悪意の文脈で用いる）といった定義による分類が存在する[1]。

また、近年は生成 AI 等を利用し、特定の人物の顔や声などを本物そっくりに他の音声や映像と合成するディープフェイクという手法も見られ、より本物との見分けが困難なフェイクニュースが作られることもある。

これらのフェイクニュースは、例えば①偽情報で利用者を特定サイトへ誘導しマルウェア感染・資格情報搾取（フィッシング／クレデンシャル・スタッフィング）に結びつける行為、②SNS や掲示板で虚偽の風説を大量流布し、企業・市場・公共安全に混乱を生じさせる行為、③組織や従業員個人に対する名誉・信用の侵害を通じた業務妨害等として現れる。

また、SNS 上での偽情報の拡散については、特に災害時におけるデマの拡散速度・被害が増大し、政府は「デマ対策」として SNS 上の情報分析・事実確認・打消し情報の即時発信体制の構築を求めている[2]（首都直下地震対策検討 WG 資料、内閣府防災）。

なお、選挙時の SNS における偽・誤情報対策の強化を目的として、令和 8 年 7 月 17 日、公職選挙法及び情報流通プラットフォーム対処法の一部を改正する法律[3]が成立し、公布された（令和 9 年 3 月 1 日施行）。

---

[1] 国立国会図書館「諸外国・地域のフェイクニュース対策（参考資料）」（令和 7 年）（https://www.shugiin.go.jp/internet/itdb_kenpou.nsf/html/kenpou/2170410_2kokkaitosyokan-siryou.pdf/$File/2170410_2kokkaitosyokan-siryou.pdf）

[2] 内閣府（防災）：首都直下地震対策検討 WG「首都直下地震発生時の国内外への情報発信について」（https://www.bousai.go.jp/jishin/syuto/taisaku_wg_02/5/pdf/sanko_siryo3.pdf）

[3] 総務省「公職選挙法及び情報流通プラットフォーム対処法の一部改正について」（https://www.soumu.go.jp/senkyo/senkyo_s/news/senkyo/seiken_housou/000191240.html）参照。改正公職選挙法は、生成 AI を用いて作成・改変した画像・動画等へのその旨の表示義務、候補者に関する虚偽情報をインターネット上に流布させて選挙の公正を害するこ

２－１．解説

（１）フェイクニュースを利用したサイバー攻撃を規制する法令の具体例

フェイクニュースを含むインターネット上の偽・誤情報の流通や拡散に適用され得る法制度としては、まず情報の発信者に対して、刑事罰の適用、民事上の請求（損害賠償請求や差止請求等）及び行政処分（不当景品類及び不当表示防止法（昭和 37 年法律第 134 号）に基づく表示規制等）があり得る。また、そのような情報を伝送・流通させた者に対しても、発信者同様に刑事罰の適用（共同正犯又は幇助犯等）、民事上の請求、行政機関等による削除等の要請等の対応がなされる場合がある。

自社に関するフェイクニュースにより権利侵害が生じた場合には、被害企業は SNS 運営者や通信事業者に対し削除要請を行うことができる。併せて、発信者情報開示命令（非訟手続）を利用して、SNS 運営者や通信事業者に対し投稿時又はログイン時の IP アドレス等の情報の開示を一体的かつ迅速に求めることができる（特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（以下、本項において「情プラ法」という。）第 5 条）。

以下では、特に刑事罰の適用があり得る攻撃類型及び成立し得る犯罪等について例を示す。

（２）不正アクセス行為の禁止等に関する法律違反（不正アクセス禁止法）

偽情報により偽サイトに誘導した上、ID・パスワード等を入力させて詐取する方法（フィッシング）等によって他人の ID・パスワード等を不正に取得し、このような他人の識別符号を用いてアクセス権限のない認証領域にアクセスするといった行為は「不正アクセス行為」に当たる場合がある。法定刑は 3 年以下の拘禁刑又は 100 万円以下の罰金である（不正アクセス禁止法第 11 条）。

（３）信用毀損・偽計業務妨害罪（刑法第 233 条）

SNS 等において、虚偽の風説の流布や偽計により企業の信用を毀損し、又は業務を妨害した行為に適用される場合がある。法定刑は「3 年以下の拘禁刑又は 50 万円以下の罰金」である。

（４）名誉毀損罪（刑法第 230 条）

SNS 等で虚偽の事実を摘示して特定の個人又は法人の社会的評価を低下させた場合には、名誉毀損罪に当たる場合がある。法定刑は 3 年以下の拘禁刑又は 50 万円以下の罰金である。

との禁止等を内容とする。改正情報流通プラットフォーム対処法は、SNS 提供事業者に、偽・誤情報の拡散が選挙に与える悪影響の軽減措置を講じる義務等を課す内容である。

適用事例として、インターネット上の掲示板において、特定の事件と無関係の会社名等を同事件の犯人と関係があるかのように書き込んだ事例について名誉毀損罪を認定した事例[4]や、アダルトビデオに女性芸能人の顔を合成したディープフェイク動画を作成してインターネット上に掲載した者に対して、名誉毀損罪及び著作権法違反の成立を認めた事例がある[5]。

（５）金融商品取引法第 158 条（風説の流布・偽計）

株価や相場の変動を図る目的で虚偽情報を流布・拡散した場合には、金融商品取引法が禁止する風説の流布又は偽計に該当する場合がある。刑事罰は 10 年以下の拘禁刑又は 1,000 万円以下の罰金（併科可）である。法人が関与した場合には、両罰規定（金融商品取引法第 207 条第 1 項第 1 号）の適用もあり得る。

２－２．企業の対策のポイント

（１）自社以外のフェイクニュースに誘導されることへの対策

第一に、インターネット上の情報について信用性を検証し、適切に取捨選択をできるような社員研修の実施が必要である。

総務省は、偽情報に関する取組について公開し[6]、フェイクニュースへの対策として、インターネット上の偽・誤情報等への対策技術の開発・実証事業を実施したり[7]、メディア情報リテラシー向上の総合的な推進に資する目的で、メディア情報リテラシー向上施策の現状と課題等に関する調査を実施するとともに、偽・誤情報対策のための啓発教育教材とその効果検証手法を開発し、これらを用いた講座を公開している[8]。

また、内閣府は災害時デマを含む誤・偽情報の拡散危険に言及し、SNS 監視・打消し情報発信の仕組み構築を推奨している[9]。

これに伴い、社内でも①メール・Web フィルタリング、②添付隔離・サンドボックス、③参照する情報のファクトチェックを標準対策として実装することが考えられる。

また、非営利組織である日本ファクトチェックセンターによるファクトチェック講座を利用することも考えられる[10]。

---

4 福岡地判令和 2 年 12 月 10 日 LLI/DB 判例番号 L07550996。
5 東京地判令和 3 年 9 月 2 日 LLI/DB 判例番号 L07631177。
6 総務省：偽情報対策に関する総務省の取組について（https://www.soumu.go.jp/main_content/000882504.pdf）
7 総務省：インターネット上の偽・誤情報等への対策技術の開発・実証事業（https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/taisakugijutsu.html）
8 総務省：上手にネットと付き合おう！安心・安全なインターネット利用ガイド（https://www.soumu.go.jp/use_the_internet_wisely/special/nisegojouhou/）
9 内閣府（防災）：首都直下地震対策検討 WG「首都直下地震発生時の国内外への情報発信について」（https://www.bousai.go.jp/jishin/syuto/taisaku_wg_02/5/pdf/sanko_siryo3.pdf）
10 日本ファクトチェックセンターホームページ（https://www.factcheckcenter.jp/）

（２）自社のフェイクニュースを拡散されることへの対策

自社のフェイクニュースが拡散されないよう、フェイクニュースを認知した場合の社内対応フロー及び対策部署の整備について定め、これを社内に十分周知しておくことが望ましい。

自社に関するフェイクニュースの拡散を最小化するためには、監視ツールや通報窓口によって虚偽情報を早期に把握、迅速な対応をすることが重要となる。対応の基本は、公式 Web サイトや公式 SNS に統一見解を掲載し、速やかに周知することである[11]。公開する統一見解では、具体的事実と根拠資料を示して正確な情報を明瞭に提示し、当該流言が虚偽である旨を明確に指摘し、誤情報の再拡散を控えるよう呼びかけることが重要である。

この体制を実効化するためには、虚偽性を迅速かつ正確に立証できる体制を平時から維持することが重要であり、社内記録や情報を適切に管理することが必要となる。また、外部の通報窓口やプラットフォーム連絡先、警察・監督当局・弁護士の緊急連絡網を用意し、緊急時に即時発動できる状態を維持することや、これらの平時の整備と訓練により、虚偽情報の発見から公式の統一見解の発信、二次被害の抑止、必要な法的救済の着手までを迅速に完遂する体制を確立する必要がある。

さらに、自社に関するフェイクニュースについて、プラットフォーム事業者に対する削除依頼や発信者情報開示請求等、法的救済を見据えた対応を行うことも重要である。情プラ法は、発信者情報の開示請求や侵害情報送信防止措置の制度を定めており、権利侵害を受けた者が、当該プラットフォーム事業者等に対して、発信者情報の開示や削除依頼を行うことができる旨が規定されている。

具体的な削除依頼の方法については、総務省委託事業である違法・有害情報相談センターが、掲示板・ブログ等の作成者又は管理人、サイト管理者・サービス提供者、これらと連絡が取れない場合には当該サイトが利用するプロバイダの順に、当該投稿が表示されているページの URL を明記した上で削除依頼を行う手順を示しているほか、「侵害情報の通知書兼送信防止措置依頼書」の様式が公開されており、これを用いて権利侵害情報の削除を依頼することができる旨が示されている[12]。したがって、企業としては、社内で事実関係及び権利侵害の内容を整理した上で、これらの公表様式を参考に、どの権利がどのような条文・判例に基づき侵害されているのかを特定して記載し、プラットフォーム事業者の定める通報フォーム又は指定窓口を通じて送信防止措置を求める必要がある。

また、同法は、大規模特定電気通信役務提供者について、侵害情報送信防止措置の実施手続の迅速化及び送信防止措置の実施状況の透明化に関する義務を課している。そのた

---

[11] 公式 Web サイトや公式 SNS に統一見解を掲載するためには、事前に公式 Web サイトや公式 SNS を開設しておく必要がある。ただし、統一見解を掲載するためだけに開設した場合には、その後の管理が不十分になる可能性もあるため、運用体制も整備しておく必要がある。

[12] 違法・有害情報相談センター：削除依頼の流れについて（https://ihaho.jp/guide/reqdelflow.html）。

め、被害企業としても、当該プラットフォーム事業者が公表している削除ポリシー・ガイドラインを踏まえつつ、情プラ法上の制度趣旨を明示しながら削除申出を行い、一定期間内の対応・結果通知を求めることが考えられる。

自社に関するフェイクニュースが拡散された場合、削除依頼や発信者情報開示、さらには損害賠償請求・刑事告訴等の法的措置を検討するに先立ち、証拠保全を速やかに行う必要がある。警察庁は、誹謗中傷等の掲載を把握した場合には、プロバイダやサイト管理者等への削除依頼や関係機関への相談、警察への通報・相談の際に必要となることから、当該サイトや SNS のページを印字し、サイト名称、URL、書き込み者、書き込み日時、内容等を記録しておくよう明示している[13]。そのため、企業としても、問題となる投稿や記事について、画面全体が分かるスクリーンショットの取得及び印刷・PDF 保存、投稿が掲載されている URL、アカウント名、投稿日時、閲覧日時、フォロワー数・拡散状況等を可能な限り客観的な形で記録しておくことが求められる。

違法・有害情報相談センターの FAQ でも、誹謗中傷を受けた場合、まず誹謗中傷を証拠とするため印刷その他の方法で保存することが推奨されている[14]。

したがって、フェイクニュースによる権利侵害が疑われる場合には、削除依頼や通報を行う前の段階で、画面のキャプチャ、印刷、利用者のアクセスログ等の保存を行い、後に改ざんが疑われないよう、電子データについてはタイムスタンプ付与や社内システムへの保管、紙媒体については作成日・作成者の記録等の方法により真正性の確保に努めることが望ましい。

さらに、一般社団法人セーファーインターネット協会が運営する誹謗中傷ホットラインでは、法的措置を検討する場合の前提として、該当投稿のスクリーンショット、投稿日時及び URL 等を保存することに加え、必要に応じて削除要請に先立ちログ保全要請を行うことも検討すべき旨が示されている[15]。発信者情報開示命令や民事訴訟等に進む場合、特に IP アドレスやログイン記録は一定期間経過後には保有期間経過により消去される可能性があるため、企業としては、フェイクニュースによる被害の深刻性・再発の蓋然性を踏まえ、プラットフォーム事業者に対してログの保全を求める通知を行うか否かを早期に検討し、必要に応じて弁護士と連携して、削除依頼と並行してログ保全要請・発信者情報開示手続に着手する体制を整えておくことが重要となる。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

---

[13] 警察庁：インターネット上の誹謗中傷等への対応（https://www.npa.go.jp/bureau/cyber/countermeasures/defamation.html）。

[14] 違法・有害情報相談センター：ネット利用者の FAQ、Q6（https://ihaho.jp/faq/netuser.html#a6）。

[15] 一般社団法人セーファーインターネット協会：誹謗中傷ホットラインへの連絡（https://www.saferinternet.or.jp/bullying/）。

４．裁判例

本文中に記載のとおり

Q81 越境リモートアクセス

リモートアクセス、越境リモートアクセスとは何か。これらに関する我が国の現状はどのようなものか。

タグ：刑事訴訟法、リモートアクセス、記録命令付差押え、サイバー犯罪条約

１．概要

リモートアクセスとは、コンピュータを用いてこれと電気通信回線で接続している記録媒体（サーバ）にアクセスすることをいい、差押えに伴うリモートアクセスについては、平成23年の刑事訴訟法改正により、捜査機関は、電磁的記録に係る証拠を収集する際に、リモートアクセスを行い、記録媒体に保管されている電磁的記録をコンピュータ等に複写した上で、当該コンピュータ等を差し押さえることができることとされた(同法第99条第2項、第218条第2項)。

このうち、越境リモートアクセスとは、リモートアクセスの対象となる記録媒体が国外に所在する場合のリモートアクセスをいうところ、外国に所在する記録媒体に保管されているデータに当該外国の同意を得ることなくアクセスするに当たっては、当該外国の主権との関係を考慮する必要があり、この点に関連して、令和 3 年に最高裁判所が判断を示したところである（「２．解説」（２）イ参照)。

また、「情報通信技術の進展等に対応するための刑事訴訟法等の一部を改正する法律」により、新たに「電磁的記録提供命令」(刑訴法第102条の2等）が創設されるとともに、「記録命令付差押え」(刑訴法第99条の２等）が廃止された。電磁的記録提供命令は、捜査機関が、裁判官の発する令状により、電磁的記録を記録媒体に記録させ又は移転させて提出させる方法又は電気通信回線を通じて、命令発出者の管理する記録媒体に記録させ又は移転させる方法で、必要な電磁的記録の提供を命ずるものである。

２．解説

（１）リモートアクセスについて

リモートアクセスとは、コンピュータを用いてこれと電気通信回線で接続している記録媒体（サーバ）にアクセスすることをいう。

コンピュータ・ネットワークが高度に発展した現代において、コンピュータの利用はネットワークに接続した形態が一般的となり、コンピュータによる情報処理の用に供されるデータは、当該コンピュータ自体への保管にとどまらず、これと電気通信回線で接続している記録媒体に保管されることが、一般化している。

そのため、捜査に当たっては、必要なデータが保管されている記録媒体を特定することが困難な場合も多い上、仮にこれを特定することができたとしても、データが様々な場所にある多数の記録媒体に分散して保管されている場合もある。

こうした状況に鑑み、平成 23 年の刑事訴訟法改正により、捜査機関は、差押え対象物がコンピュータであるときは、当該コンピュータに電気通信回線で接続している記録媒体に保管されているデータを当該コンピュータ又は他の記録媒体に複写した上、これを差し押さえることができることとされ、リモートアクセスを行うための規定が整備された（同法第 99 条第 2 項、第 218 条第 2 項）。（以上の内容について、杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について　下」法曹時報 64 巻 5 号 95 ないし 96 頁参照）

（２）越境リモートアクセスについて

越境リモートアクセスとは、リモートアクセスの対象となる記録媒体が国外に所在する場合のリモートアクセスをいい、捜査機関が、当該記録媒体が所在する国の同意を得ることなく当該記録媒体にアクセスするに当たっては、当該外国の主権との関係を考慮する必要がある。

この点に関し、関係する国際約束であるサイバー犯罪に関する条約と、諸外国における越境リモートアクセスの取扱いを紹介した上で、我が国における現状について解説する。

ア　サイバー犯罪に関する条約等

サイバー犯罪に関する条約（平成 24 年条約第 7 号）（以下、本項において「サイバー犯罪条約」という。）は、欧州評議会が採択した世界初のサイバー犯罪対策条約であり、サイバー犯罪と効果的に戦うため、締約国に対し、刑事に関する実体法及び手続法の整備並びに国際協力のための措置を義務付けており、平成 24 年 11 月に我が国について効力が発生した。令和 8 年 5 月時点で、同条約の締約国は 82 か国（全ての G7 諸国を含む。）、署名済み未締結国等 15 か国である[1]。

日本は、サイバー犯罪条約の締約国等が参加するサイバー犯罪条約委員会会合等の国際会議に参加し、サイバー空間における脅威に関する情報共有を行っている。

---

[1] 外務省：サイバー犯罪に対する国際社会と日本の取組（https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html）。
なお、我が国は、協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書を締結済みだが（令和 5 年 8 月 10 日受託書寄託）、同議定書は令和 8 年 5 月時点で未発効（https://www.mofa.go.jp/mofaj/ila/st/page24_002143.html）。
この中には、「インターネット・サービス・プロバイダが保有する情報の開示」の項目もあるが、加入者情報の開示に関し、インターネット・サービス・プロバイダとの直接協力を規定する一部の規定は、個人情報や通信の秘密の保護等の観点から現行国内法と整合性を保つため、議定書が定める留保規定に基づき留保している（https://www.mofa.go.jp/mofaj/files/100476214.pdf）。

サイバー犯罪条約第 32 条は、一定の場合におけるリモートアクセスに関する規定を設けているところ、締約国は、他の締約国の許可なしに、以下を実施することができるとされている。

① 公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所の如何を問わない。）

② 自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。

越境リモートアクセスに係る諸外国の対応は様々であるが、国内法を制定するなどして対処している国も複数存在する。

イ　我が国における現状

我が国においては、前記のとおり、平成 23 年の刑事訴訟法改正により新設された同法第 99 条第 2 項及び第 218 条第 2 項において、コンピュータの差押えに際してリモートアクセスを行うことができる旨定められたものであるが、越境リモートアクセスが許されるか否かについては、刑事訴訟法の条文上明示されていない。

この点に関し、近年、最高裁判所による判断が示され（最決令和 3 年 2 月 1 日刑集 75 巻 2 号 123 頁[2]）、最高裁判所は、「刑訴法 99 条 2 項、218 条 2 項の文言や、これらの規定がサイバー犯罪に関する条約（平成 24 年条約第 7 号）を締結するための手続法の整備の一環として制定されたことなどの立法の経緯、同条約 32 条の規定内容等に照らすと、刑訴法が、上記各規定に基づく日本国内にある記録媒体を対象とするリモートアクセス等のみを想定しているとは解されず、電磁的記録を保管した記録媒体が同条約の締約国に所在し、同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に、国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許されると解すべきである」として、刑事訴訟法上、越境リモートアクセスが許容され得ることを明らかにするとともに、越境リモートアクセスを行うことができる一場面についても判示した[3]。

---

[2] 本件に関する調査官解説として、吉戒純一・ジュリスト 1562 号（令和 3 年）98 頁がある。

[3] 同決定に関し、三浦守裁判官の補足意見は以下のとおりである。
「リモートアクセスをして記録媒体から電磁的記録を複写するなどして収集した証拠の証拠能力について補足する。
電磁的記録を保管した記録媒体が外国に所在する場合に、同記録媒体へのリモートアクセス及び同記録の複写を行うことは、当該外国の主権との関係で問題が生じ得るが、法廷意見が説示するとおり、その記録媒体がサイバー犯罪に関する条約の締約国に所在し、同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に、国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許されると解される。

（３）電磁的記録提供命令について

電磁的記録提供命令は、捜査機関等が犯罪の捜査をするために、裁判官の発する令状により、電磁的記録を保管する者又は利用する権限を有する者に対し、サーバやクラウド上のデータの提供を命じることができる制度である。また、捜査機関は、電磁的記録提供命令をする場合において、必要があるときは、裁判官の許可を受けて、当該電磁的記録提供命令を受ける者に対し、1 年を超えない期間を定めて、みだりに当該電磁的記録提供命令を受けたこと及び当該電磁的記録提供命令により提供を命じられた電磁的記録を提供し又は提供しなかったことを漏らしてはならない旨を命ずることができる（秘密保持命令）[4]。

この強制処分は、記録命令付差押えと異なり、オンライン上でデータを移転又は記録させる方法でのデータ提供を命じることも可能となっている。正当な理由なく命令を拒否したり、秘密保持命令に違反したりした者には罰則が定められている（両罰規定も定められている。）ことから、企業等の当該電磁的記録提供命令を受ける者には適切な対応が求められる。

３．参考資料（法令・ガイドラインなど）

・刑事訴訟法第 99 条の 2、第 102 条の 2、第 218 条第 1 項、第 2 項
・サイバー犯罪条約第 32 条
・杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について　下」法曹時報 64 巻 5 号

４．裁判例

本文中に記載のとおり

本件においては、（略）リモートアクセスの対象である記録媒体は、日本国外にあるか、その蓋然性が否定できないものであって、同条約の締約国に所在するか否かが明らかではないが、このような場合、その手続により収集した証拠の証拠能力については、上記の説示をも踏まえ、権限を有する者の任意の承諾の有無、その他当該手続に関して認められる諸般の事情を考慮して、これを判断すべきものと解される。」

[4] 令和 7 年 5 月 16 日に成立、同年 5 月 23 日に公布された改正刑事訴訟法に基づく制度であり、公布の日から起算して 1 年を超えない範囲内において政令で定める日に施行される。

Q82 海外における主な個人データ保護関係法令

海外における主な個人データ保護関係法令としてどのようなものがあるか。その際に日本企業が留意すべき個人データのセキュリティに関するポイントとしてどのようなものがあげられるか。

タグ：欧州一般データ保護規則（GDPR）、データ保護オフィサー（DPO）、データ保護影響評価（DPIA）、カリフォルニア州消費者プライバシー法（CCPA）、CPRA、データ侵害通知法、SHIELD Act、データ安全法、ネットワーク安全法、中国民法典

１．概要

まず、欧州においては、欧州の一般データ保護規則（GDPR）に注意が必要である。日本企業であっても、個人データの取扱いの実態によっては、GDPR の適用を受け得る。このため、適用範囲（第 2 条、第 3 条）を精査し、同法の要請に応じた措置を講ずる必要がある。このとき、安全管理に関連して、詳細な規制があることに注意を要する。

次に、米国においては、連邦法レベルでは包括的な個人データ保護に関する法律は制定されていないものの、分野ごとに個別に法律が存在する。州法では、複数の州において包括的な法律が存在しており、例えば、カリフォルニア州では、カリフォルニア州消費者プライバシー法（the California Consumer Privacy Act。以下、本項において「CCPA」という。）及びその改正法であるカリフォルニア州プライバシー権法（the California Privacy Rights Act。以下、本項において「CPRA」という。）が存在し、カリフォルニア州以外でも州レベルでの包括的な個人情報保護法の制定が相次いでいる。また、このほか、各州においてデータ侵害通知法が制定されている。

そして、中国においては、個人情報保護に関係する法令として、「個人情報保護法」（原文「个人信息保护法」、以下、本項において「中国個人情報保護法」という。）、「ネットワーク安全法（サイバーセキュリティ法）」（原文「网络安全法」）、「データ安全法（データセキュリティ法）」（原文「数据安全法」）のデータ三法、及び「民法典」（以下、本項において「中国民法典」という。）、「刑法」、「輸出管理規制法」（原文「出口管制法」）や「消費者権益保護法」等が存在する。また、現在も意見募集稿段階の法令や、改正や制定について議論段階の法令も多数存在する。様々な法令・ガイドラインにまたがって個人情報の保護がなされており、改正・制定も順次なされている。

２．解説

２－１．欧州

（１）はじめに

EU[1]における一般データ保護規則（General Data Protection Regulation。以下、本項において「GDPR」という。）は、個人データの取扱いと関連する自然人の保護に関する規定及び個人データの自由な移動に関する規定を定めるものである（GDPR 第 1 条第 1 項）。我が国の個人情報保護法である個情法に相当するものということができる。また、英国においては、EU 離脱後に GDPR を国内法化した英国一般データ保護規則（General Data Protection Regulation。以下、本項において「UK GDPR」という。）及び 2018 年データ保護法（Data Protection Act 2018）が適用されているほか、英国データ（利用及びアクセス）法（Data (Use and Access) Act 2025）が 2025 年に成立しており、施行後には現行の英国におけるデータ保護規制に一部変更が生じることになる[2]。

以下のとおり、日本企業であっても GDPR 及び UK GDPR の適用を受けることがあるため、日本企業のグローバル展開と、グローバル・コンプライアンス体制の構築に伴い、GDPR 及び UK GDPR を課題とする企業は少なくないと考えられる。現時点では、個人データに関連する主な規律は GDPR と UK GDPR で基本的に同様であるところ、本項においては、GDPR を対象にその適用範囲、そしてセキュリティ対策に関連する主な規定について概要を紹介する[3]。

（２）適用範囲

GDPR は、個人データの取扱いが EU 域内で行われるものであるか否かを問わず、EU 域内の管理者又は処理者の拠点における活動の過程における個人データの取扱いについ

---

[1] 厳密には、欧州連合（European Union）加盟国及び欧州経済領域（EEA: European Economic Area）協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含むが、本文では、以下、便宜上 EU との用語を使用している。

[2] 主な変更点は、①個人データに係る自動意思決定の制限の緩和、②データ主体の権利についての追加規定（アクセス権対応に係る期限についての明確化や管理者への苦情申立手続の要件の追加等）、③データ移転規制における判断基準の変更（十分性認定基準について、「大幅に低い」（materially lower）か否かという基準への変更）、④デジタル認証サービス（Digital verification services：DVS）の導入（施行時期を含む詳細は、二次立法により具体化される予定）、⑤クッキー関連規制の変更（本人同意の例外拡大とその一方での制裁金の引上げ等）、⑥データ保護機関の改組（ICO（Information Commissioner's Office）から IC（Information Commission）への変更）と権限の全般的強化、⑦正当な利益（UK GDPR6 条 1 項 f 号）についての「認められた正当な利益」（recognized legitimate interest）の明文化、⑧目的外利用が認められる場合の明確化、⑨スマートデータスキーム（データの活用を促進するための新たな枠組み）の創設、⑩閣内大臣に対する UK GDPR 独自の「特別な種類の個人データ」を追加する権限の付与、等。既に一部の条項は同日施行されているが、大部分は今後成立する二次立法により施行される予定である。

[3] UK GDPR の規律としては、本項における GDPR の規定に関して、例えば、「EU 域内」を「英国国内」、「所轄監督機関」を「ICO（IC）」へとそれぞれ読み替えるべきこととなる。

て適用される[4]（GDPR 第 3 条第 1 項）。また、EU 域内に拠点が認められない場合であっても①有償無償を問わず、EU 域内のデータ主体に対する物品又はサービスの提供、又は②EU 域内におけるデータ主体の行動の監視を行う場合には、GDPR の適用があるとされる（同条第 2 項）。

このため、日本企業であっても、EU 域内で安定的な仕組みを通じて行われる実効的かつ現実的な活動（GDPR 前文第 22 項は「拠点」の意義をこのように説明する。）を行っている場合であって、この活動の過程でなされる個人データの取扱いについては、GDPR の適用を受ける。また、EU 域内にそのような拠点がないとしても、①又は②に該当すれば GDPR の適用を受け、一定の場合を除き、EU 域内における代理人を指名しなければならない（GDPR 第 27 条第 1 項）。

（３）安全管理に関する主な規定

GDPR 第 5 条は、個人データの取扱いと関連する基本原則を定めている。この中では、「無権限による取扱い若しくは違法な取扱いに対して、並びに、偶発的な喪失、破壊又は損壊に対して、適切な技術上又は組織上の措置を用いて行われる保護を含め、個人データの適切な安全性を確保する態様により、取扱われる。（「完全性及び機密性」）」（同条第 1 項(f)号）と定められている。これを受けて、様々な義務が設けられているところ、適切な技術上・組織上の措置を明示するものとしては、次のアのほか、管理者の責任（同第 24 条）、データ保護バイデザイン及びデータ保護バイデフォルト（同第 25 条）、処理者（同第 28 条）、監督機関及びデータ主体に対する個人データ侵害の通知・連絡（同第 33 条及び第 34 条）がある。その他、データ保護責任者（DPO）の選任等（同第 37 条から第 39 条）、データ保護影響評価（DPIA）の実施（同第 35 条）など、完全性・機密性に関連すると考えられる規定を含め、主なものの概要を紹介する[5]。

ア　適切な技術的・組織的措置の実施

GDPR 第 32 条第 1 項は「最新技術、実装費用、取扱いの性質、範囲、過程及び目的並びに自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮に入れた上で、管理者及び処理者は、リスクに適切に対応する一定のレベルの安全性を確保するために、特に、以下のものを含め、適切な技術上及び組織上の措置をしかるべく実装す

[4] 本文中では地理的適用範囲について記載しているところ、その他「本規則は、その全部又は一部が自動的な手段による個人データの取扱いに対し、並びに、自動的な手段以外の方法による個人データの取扱いであって、ファイリングシステムの一部を構成するもの、又は、ファイリングシステムの一部として構成することが予定されているものに対し、適用される。」等、実体的適用範囲についても定められている（GDPR 第 2 条）。

[5] 本文で述べた以外にも、安全管理に関しては、例えば、GDPR 第 28 条第 3 項は、処理者による取扱いについて、一定の事項を契約等で規定することを求めており、欧州委員会は 2021 年 6 月 4 日に当該契約についての EU/EEA 内の管理者及び処理者間の Standard Contractual Clauses を公表している。

る。」として安全管理措置の実施を求める。注意喚起しつつ例示列挙された「以下のもの」とは、①個人データの仮名化又は暗号化、②取扱システム及び取扱サービスの現在の機密性、完全性、可用性及び回復性を確保する能力、③物的又は技術的なインシデントが発生した際、適時な態様で、個人データの可用性及びそれに対するアクセスを復旧する能力、④取扱いの安全性を確保するための技術上及び組織上の措置の有効性の定期的なテスト、評価及び評定のための手順である。

各企業が実際にこれへの対応を実施するに際しては、実態に即することが求められるところ、データマッピングの結果に基づくことが肝要である。また、フランスのデータ保護機関である情報処理及び自由に関する国家委員会（CNIL[6]）が公表する「Practice guide GDPR - Security of personal data 2024」が参考となる。

イ　個人データ侵害への対応

GDPR 第 33 条は、「個人データ侵害が発生した場合、管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも 72 時間以内に、第 55 条に従って所轄監督機関に対し、その個人データ侵害を通知しなければならない。」とし（同条第 1 項）、また、「処理者は、個人データ侵害に気づいた後、不当な遅滞なく、管理者に対して通知しなければならない。」としている（同条第 2 項）。特に、処理者に個人データの取扱いを委託している場合、処理者から適切な情報共有がなされるようにすることが求められることに注意が必要である。また、GDPR 第 34 条は、「個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合」にデータ主体への連絡をしなければならないとしている（同条第 1 項）。

所轄監督機関[7]への通知及びデータ主体への連絡については、2021 年 1 月に公表された「個人データ侵害通知に関するガイドライン[8]」が、具体的な事例を挙げてその要否の判断基準や 72 時間の時間制限の開始時点等に関する検討を行っており、また、これを

---

[6] Commission nationale de l'informatique et des libertes の略。

[7] 複数の EU 加盟国内のデータ主体に影響を与えるような越境取扱いについてのデータ侵害が生じた場合、GDPR 上、原則として、通知はワンストップショップ・システムにより主監督機関に対して行うこととなる（この場合、2023 年 3 月に策定・公表された「管理者又は処理者の主監督機関の特定に関するガイドライン」を参考にしつつ、データの取扱いを含む事業活動を決定する場や決定権限（経営陣等）の所在地等を踏まえて、主たる拠点を確定した上で、当該拠点を管轄する監督機関を「主監督機関」として扱うことになる）が、個人データ侵害通知に関するガイドラインでは、EU 域内に拠点のない事業者については、ワンストップショップ・システムは適用されず、影響を受けるデータ主体が居住する加盟国の全ての監督機関に対して通知される必要があるとしている。

[8] https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

補完するものとして「個人データ侵害通知の事例に関するガイドライン[9]」も策定・公表されており参考になる。

ウ　DPO の選任等

（ア）データ保護オフィサー（DPO）の選任

管理者及び処理者は、一定の場合にデータ保護オフィサー（DPO[10]）を選任しなければならない（GDPR 第 37 条）。一定の場合とは、①公的機関又は公的組織によって個人データの取扱いが行われる場合、②管理者又は処理者の中心的業務が、その取扱いの性質、範囲及び又は目的のゆえに、データ主体の定期的かつ系統的な監視を大規模に要する取扱業務によって構成される場合、③管理者又は処理者の中心的業務が、第 9 条による特別な種類のデータ及び第 10 条で定める有罪判決及び犯罪行為と関連する個人データの大規模な取扱いによって構成される場合をいう[11]。

企業にとって問題となる要件は②又は③であるところ「データ保護オフィサー（DPO）に関するガイドライン[12]」では、具体例を含めた検討がなされている。例えば、大規模であるか否かについては、データ主体の数、個人データの量・種類、処理の期間・永続性、処理の地理的範囲を考慮して総合判断するとされ、定期的であるか否かは、現在継続し又は一定期間内に一定の間隔で発生するか、定期的に繰り返されるか、常時又は周期的に発生するか否かいずれかに該当するかによって判断するとされる。

DPO は、必ずしも EU 域内において選任する必要はなく、日本国内で自社の従業員や外部の専門家を選任することも差し支えない。また、企業グループは、DPO が各拠点から容易にアクセス可能な場合に限り、1 名の DPO を選任することができる（GDPR 第 37 条第 2 項）。企業ごとに監査の方法も異なることなどコンプライアンスの体制もそれぞれであるところ、選任に際して GDPR に係る専門的、実務的な知見の有無を判断するとともに、企業内部等関係主体との意思疎通が容易であるか等の要素から、機能する体制を構築することが望ましい。

（イ）DPO の業務

DPO は、少なくとも①管理者又は処理者及び取扱いを行う従業者に対し、本規則及びそれ以外の EU 若しくは加盟国のデータ保護条項による義務を通知し、かつ、助言すること、②取扱業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、本規則の遵守、それ以外の EU 又は加盟国の個人データ保

---

[9] https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

[10] Data Protection Officer の略。

[11] ただし、加盟国が内国施行法において独自の要件を設定している場合があるため、各国の法令を確認する必要がある（例：ドイツ）。

[12] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100

護条項遵守、並びに、個人データ保護と関連する管理者又は処理者の保護方針の遵守を監視すること、③要請があった場合、第 35 条によるデータ保護影響評価に関して助言を提供し、その遂行を監視すること、④監督機関と協力すること、⑤取扱いと関連する問題に関し、監督機関の連絡先として行動すること（第 36 条に規定する事前協議、適切な場合、それ以外の関連事項について協議することを含む。）をその職務として行わなければならない。なお、DPO に関しては、GDPR 第 38 条第 3 項において、管理者及び処理者は、DPO が、上記職務の遂行に関し、いかなる指示も受けないように確実を期すことが義務付けられているということにも留意が必要である。

エ　データ保護影響評価（DPIA）の実施

取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならないとされる（GDPR 第 35 条第 1 項）。この評価をデータ保護影響評価（DPIA[13]）という。

高いリスクを発生させるおそれがあり（「データ保護影響評価（DPIA）及び取扱いが 2016/679 規則の適用上、『高いリスクをもたらすことが予想される』か否かの判断に関するガイドライン」[14]III. B. a）に掲げられる 9 つの基準）、かつ適用除外事由に（同ガイドライン III. B. b）に掲げられる 5 つの類型）に該当しない場合は DPIA の実施をしなければならず、実施によって高いリスクがあることが示され、リスク軽減措置を講ずることができない場合、データ保護監督機関との事前協議を要する（GDPR 第 36 条第 1 項）。

（４）事例

GDPR 及び UK GDPR に関しては、近時でも、安全管理措置を問題とした事例であって、多額の制裁金を課すことを検討するケースが見られる。

EU における執行事例としては、例えば、以下の 2 件が挙げられる。

① DPC（アイルランドデータ保護委員会）が、2024 年 9 月に Meta Platforms Ireland Limited に対して 2 億 5,100 万ユーロの制裁金を科した事例

Meta Platforms Ireland Limited が、約 2,900 万人のユーザの個人データを漏えいさせ、データ侵害の通知及び侵害事実と対応措置に関する文書化の懈怠、並び

[13] Data Protection Impact Assessment の略。
[14] 原題は Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679（https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711）。

にデータ保護バイデザイン及びデータ保護バイデフォルト違反があったとして 2 億 5,100 万ユーロの制裁金が科された[15]。

② GPDP（イタリアのデータ保護機関）が 2024 年 2 月に Enel Energia 社に対し約 7,910 万ユーロの制裁金を科した事例

Enel Energia 社が、顧客データに関する情報システムに深刻なセキュリティ不備があったこと等の複数の違反を認定され、イタリアにおける国内過去最高額となる約 7,910 万ユーロの制裁金が科された[16]。

英国のデータ保護機関である英国情報コミッショナーズオフィス（ICO[17]）における執行事例としては、例えば以下の 2 件が挙げられる。

① ICO が Advanced Computer Software Group Limited 社に対し 2025 年 3 月に 307 万ポンドの制裁金を科した事例

Advanced Computer Software Group Limited 社が医療機関に提供していたソフトウェアサービスに対するランサムウェア攻撃によって約 8 万件の個人データが影響を受け、多要素認証の未導入等のセキュリティ対策の不備があったとして 307 万ポンドの制裁金が科された[18]。

② ICO が 23andMe 社に対し 2025 年 6 月に 231 万ポンドの制裁金を課した事例

23andMe 社において顧客に関する約 16 万件の個人データが不正アクセスを受け、追加認証措置の不備等のセキュリティ対策の不備があったとして、231 万ポンドの制裁金が科された[19]。

２－２．米国

（１）連邦法と州法の関係等

米国では、連邦政府及び州政府それぞれに立法権が認められている。そして、連邦政府が制定した連邦法は、全ての州に適用され、また、州法に優先する（米国合衆国憲法第 6 章第 2 項）。サイバーセキュリティについては、連邦法及び州法のいずれのレベルにおいても、包括的な法律は制定されていなかったが、2024 年 3 月、重要インフラのサイバーインシデントについて CISA（the Cybersecurity and Infrastructure Security Agency: サイバーセキュリティ・インフラストラクチャーセキュリティ庁）への報告を義務付ける

[15] Data Protection Commission（https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million）
[16] GPDP（https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9988921）
[17] Information Commissioner's Office の略。上記(1)のとおり、英国データ（利用及びアクセス）法により、Information Commissioner's Office から Information Commission に改組されることとなる。
[18] ICO（https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/）
[19] ICO（https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/?utm_source=chatgpt.com）

法律である「2022 年重要インフラ向けサイバーインシデント報告法」（CIRCIA）[20]の施行規則案が公告された。同規則案は、2026 年 5 月までに最終化される予定である[21]。

データ保護については、連邦レベルでは、CCPA の制定以降包括的な連邦データ保護法制定の機運は高まっているものの、現在のところ、データ保護に関する包括的な法律は制定されていない。一方で、州法レベルでは、後述のとおり、カリフォルニア州等、包括的な個人情報保護法が制定している州が増加している。

なお、連邦レベルにおいても、銀行等の金融機関に適用されるグラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）（以下、本項において「GLBA」という。）や医療関係についての医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）（以下、本項において「HIPAA」という。）等、分野ごとに個別のデータ保護に関する連邦法が存在する。

（２）データ保護に関する州法

ア　CCPA 及び CPRA

CCPA は、2018 年 6 月 28 日に制定されたカリフォルニア州における包括的な個人情報保護法であり、同州の自然人である住民（消費者）の個人情報を保護することを目的とするものであり、2020 年 1 月 1 日から施行されている。日本企業でカリフォルニア州に拠点を有しない場合であっても、カリフォルニア州において事業を行っており[22]、総売上が 2,500 万ドル以上であるなど、その他の要件を満たす場合には、CCPA が適用される。CCPA に違反した場合、州司法長官より違反行為の差止め又は制裁金（最大 2,500 ドル（故意の違反については最大 7,500 ドル））を求めた提訴（CCPA 1798.155(b)）を受ける可能性がある。さらに、合理的セキュリティ措置を取る義務の違反により、暗号化されていない、特定の情報が流出等した場合には、消費者には 1 件あたり 100 ドル以上 750 ドル以下の法定損害賠償又は実損額のいずれか大きいほうの金額について私人提訴権（クラスアクションも可能）（1798.150(a)(1)）が認められており、実際にクラスアクションが提起されている事例も存在する（例：Benjamin Karter v. Epiq Systems, Inc.）。

また、カリフォルニア州においては、2020 年 11 月 3 日に CCPA の改正法である CPRA が制定され、その大部分の規定は、2023 年 1 月 1 日から施行された。CPRA においては、違反した場合の制裁金の上限が、故意の違反、又は、故意の有無にかかわらず、16 歳未満であると認識している場合の未成年の個人情報に関する違反の場合には 7,500 ドルへと増額されている。また、私人提訴権の対象となる情報が、CCPA においては、氏

[20] Cyber Incident Reporting for Critical Infrastructure Act of 2022(CIRCIA)（https://www.congress.gov/bill/117th-congress/house-bill/2471/text）

[21] An official website of the United States government （https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202504&RIN=1670-AA04）

[22] なお、「カリフォルニア州において事業を行っている」（does business in the State of California）については、CCPA 上定義は存在せず、どのような場合に「カリフォルニア州において事業を行っている」と判断されるかは明らかではない。

名等を含む一定の個人情報に限られていたが、CPRA においては、新たに E メールアドレスと組み合わされた、アカウントへのアクセスを可能とするパスワード又はセキュリティ質問及びその回答の情報も対象として追加されている。

さらに、CCPA 制定後、カリフォルニア州以外でも州レベルでの包括的な個人情報保護法の制定が相次ぎ、米国全体で包括的な個人情報保護法を有する州は 2026 年 1 月 1 日時点で 20 州[23]に到達した。これらの州法は概ね似た内容となっているが、州ごとに適用範囲や義務規定に独自の特徴がみられることもある。

イ　データ侵害通知法及び SHIELD Act

データ侵害通知法は、個人情報の漏えいが発生した場合に、事業者に対し、漏えいの対象となった個人に対して漏えいの通知を義務付けるとともに、一定の場合に州当局への報告も義務付けるものであり、米国の各州において制定されている。

例えば、カリフォルニア州のデータ侵害通知法（Cal. Civ. 1798.82）においては、事業者は、システムセキュリティの侵害が発生した場合には、個人情報が漏えい等の対象となったカリフォルニア州の住民に対する通知を行わなければならず（Cal. Civ. 1798.82(a)）、さらに、500 名以上のカリフォルニア州の住民に対し当該通知を行う場合には、州司法長官に対し住民に対する通知書のサンプルを提出しなければならない（Cal. Civ. 1798.82（f））。

2019 年 7 月にニューヨーク州で制定されたハッキング禁止及び電子データセキュリティ改善に関する法律（Stop Hacks and Improve Electronic Data Security Act）（以下、本項において「SHIELD Act」という。）は、同州のデータ侵害通知法の個人情報の範囲を拡大する等の改正を定めている（N.Y. Gen. Bus. Law §899-aa 1 (b)(i)(ii)）。さらに、SHIELD Act は、ニューヨーク州の住民の個人情報を含む電子化データを保有等している事業者等に対し、当該個人情報を保護するための合理的セキュリティ措置を取るよう求めている（N.Y. Gen. Bus. Law §899-bb 2 (a)）。

（３）データ保護に関する連邦法

連邦レベルでは、現在のところ、データ保護に関する包括的な法律は制定されていないが、FTC 法（Federal Trade Commission Act）第 5 条の「unfair or deceptive acts or practices」の禁止に基づいて、プライバシーポリシー等に反した個人情報の漏えいについては高額の制裁金が科される[24]。また、分野ごとに個別の連邦法は存在し、例えば、HIPAA

[23] カリフォルニア州、バージニア州、コロラド州、コネチカット州、ユタ州、オレゴン州、モンタナ州、テキサス州、フロリダ州、アイオワ州、デラウェア州、テネシー州、インディアナ州、ニュージャージー州、ニューハンプシャー州、ケンタッキー州、ネブラスカ州、メリーランド州、ミネソタ州、ロードアイランド州

[24] 近時の執行事例としては、例えば、FTC が 2024 年 10 月に Marriott 及びその子会社との間で、不適切な情報セキュリティシステムが原因でデータ漏えいが複数回発生したとして、各顧客に対して個人情報の削除を要請する機会を与えること等を合意しまた、同社らが、州

は、電子化された医療情報を扱う病院や医療保険会社等を対象とし、保護健康情報（protected health information）について、会社の規模、技術的インフラ、コスト及びリスクの大きさ等に応じて、合理的かつ適切なセキュリティ措置（管理的措置、物理的措置、技術的措置及び組織的措置）を取ることを求めている[25]。また、GLBA は、金融機関に対し、顧客の非公開個人情報（nonpublic personal information）の保護について、特定の要素を含むセキュリティプログラムの実施を義務付けている[26]。

また、2023 年 7 月、米国証券取引委員会（SEC）は、上場企業によるサイバーセキュリティリスク管理、戦略、ガバナンス、インシデント開示に関する規則[27]を採択し、サイバーセキュリティインシデントの開示ルールを強化した。上場企業は、重大なサイバーインシデントが発生したと判断してから 4 営業日以内に開示し、インシデントの性質、範囲、時期及び影響を明示する義務がある。また、年次報告書ではリスク管理体制や取締役会の関与などを開示する必要がある[28]。

２－３．中国

（１）各法令の関係性

中国においては、まず、2017 年にネットワーク空間管理の基本法といえるネットワーク安全法（以下、本項において「サイバーセキュリティ法」ということがある。）が施行され、2021 年にはデータ安全法（以下、本項において「データセキュリティ法」ということがある。）と中国個人情報保護法が施行され、これら三法（以下、本項において「データ三法」ということがある。）を主要な法律として、横断的にネットワークデータ[29]の保護が図られている。

加えて、データ三法の下位法令に位置づけられる、ネットワークデータ安全管理条例が 2025 年 1 月 1 日より施行され、個人情報を含むネットワークデータの取扱い及び監督管理につきデータ三法を詳細化する。さらに、下位法令等で定められていない事項については、国家推奨標準である「情報安全技術個人情報安全規範」等の法的拘束力のない標準・ガイドライン等を参照する必要がある。また、2021 年 1 月 1 日に施行された中国民法典においても、個人情報及びプライバシー権が明記され、一定の義務等が規定されており、

の消費者保護法及び個人情報保護法等に基づき、49 州及びワシントン D.C.に合計 5,200 万ドルの和解金を支払った事例（https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches）がある。その他 FTC による執行事例（https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement）

[25] 42 U.S.C. §1302(a)及び 45 C.F.R. § 164.306, 308, 310, 312, 314

[26] 15 U.S.C. §6801(b)及び 16 C.F.R. §314.3, 314.4

[27] Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure（https://www.sec.gov/files/rules/final/2023/33-11216.pdf）

[28] SEC によるプレスリリース（https://www.sec.gov/newsroom/press-releases/2023-139）

[29] ネットワークを通じて取り扱われ、生成される各種の電子データ（ネットワークデータ安全管理条例第 62 条第 1 項）

この他にも、2025 年 11 月 1 日に施行された国家ネットワークセキュリティインシデント報告管理弁法はネットワークセキュリティインシデント発生時の対応を定めている。

下記に詳説するとおり、データ三法は、保護法益・適用対象について、重複する部分はあるものの法目的などの大枠は異なっている。他方で、中国個人情報保護法における個人情報の定義[30]と、ネットワーク安全法における個人情報の定義[31]は書きぶりは異なるものの、自然人の識別可能性を基準に個人情報の範囲を画するという点については同様と考えられる。

なお、今後も、後発の法令によって、適用対象、義務・規制が上乗せされることがありうるため、法令の制定の動向に注意が必要である。以上を踏まえ、以下ではデータ三法における保護法益・適用対象を紹介すると共に、（2）以下では、主に中国個人情報保護法のうち、サイバーセキュリティにかかわる部分の概要を紹介する。

ア　ネットワーク安全法

ネットワーク安全法は、Q83-3 で紹介するとおり、ネットワークの安全管理に関連する事項を全般的に規定したサイバーセキュリティの基本法となっている。中国国内においてインターネットを建設・運営・維持・使用する場合、又はインターネットの安全を監督管理する場合に適用されるため、中国国外に所在する企業であっても中国国内で事業を行う場合には適用される可能性がある。適用対象主体は「ネットワーク運営者」で、特に「重要情報インフラ運営者」に当たる場合は、個人情報・重要データの国内保存義務・国外移転規制が課されることとなる。ネットワーク安全法においても個人情報保護に関する規定が存在するが、原則的・概括的な規定に留まる。中国個人情報保護法の施行前は、ネットワーク安全法における個人情報保護に関する規定の重要性は高かったが、中国個人情報保護法の施行とともに、その規定の意義は薄れたといえる。

イ　データ安全法

次に、データ安全法は、Q83-3 で紹介するとおり、データセキュリティに関する責任主体及びデータセキュリティ保護義務等について規定した基本法である。中国国内にお

[30] 電子的又は他の方式により記録され、既に識別された又は識別可能な、自然人と関連する各種の情報であり、匿名化処理された情報は含まない（中国個人情報保護法第 4 条第 1 項）。

[31] 「電子的方式又はその他の方式によって記録され、単独で又はその他の情報と組み合わせて、特定の自然人を識別することができる各種情報をいい、自然人の氏名、生年月日、身分証明書番号、生体認証情報、住所、電話番号、電子メール、健康情報、行動履歴情報等を含む。」（ネットワーク安全法第 76 条第 5 号）。なお、中国民法典においてもこの個人情報の定義が用いられている（中国民法典第 1034 条第 2 項）。

ける個人データに限られない「データ」[32]の「取扱行為」[33]に適用される。また、同法は域外適用され得る（同法第 2 条第 2 項）。

ウ　中国個人情報保護法

そして、中国個人情報保護法は、GDPR に類似する内容を規定しており、包括的な個人情報の保護についての基本法となっている。個人情報を取り扱う「個人情報取扱者」は、中国国内における自然人の個人情報の取扱行為のみならず、中国国外における中国国内の自然人の個人情報の取扱行為についても、①国内の自然人に対する製品もしくは役務の提供を目的とする場合、②国内の自然人の行為を分析し、評価する場合、又は③法律、行政法規に定めるその他の事由のいずれかに該当する場合は、適用を受ける（同法第 3 条第 2 項）。また、後述する機微な個人情報についても規定がある。

エ　その他

ネットワークデータ安全管理条例は、ネットワークデータ取扱者[34]によるネットワークデータ取扱活動[35]を適用対象とし、中国国内の事業者のみならず、データ安全法第 2 条第 2 項及び中国個人情報保護法第 3 条第 2 項に基づき域外適用を受ける、中国国外の事業者にも適用される（同条例第 2 条）。

（２）機微な個人情報

上記のとおり、中国個人情報保護法は、機微な個人情報について規定する。機微な個人情報とは、「一旦漏洩され、又は不法に使用されると、自然人の人格の尊厳が侵害を受け、又は人身、財産の安全が害されやすい個人情報であり、生体認証、宗教信仰、特定の身分、医療健康、金融口座、行動履歴等の情報や、14 歳未満の未成年者の個人情報が含まれる」をいう（同法第 28 条第 1 項）。

機微な個人情報を取得する場合、同法が規定する個人情報の取扱行為前の本人の同意に加え、別途の本人同意を取得する必要がある（同法第 29 条）。また、一般的な事前告知事項に加え、機微な個人情報の取扱いの必要性及び個人の権益への影響を告知しなければならない（同法第 30 条）。その他、機微な個人情報を取り扱う場合は、（３）イで後述する個人情報影響評価を実施しなければならない（同法第 55 条）。

---

[32] いずれかの電子的又はその他の方式によって情報を記録したもの（データ安全法第 3 条第 1 項）。
[33] データの収集、保存、使用、加工、伝送、提供、公開等が含まれる（データ安全法第 3 条第 2 項）。
[34] ネットワークデータ取扱活動において、取扱の目的及び方法を独自に決定する個人又は組織（ネットワークデータ安全管理条例第 62 条第 3 項）。
[35] ネットワークデータの収集、保存、利用、処理、伝送、提供、開示、削除等の活動（ネットワークデータ安全管理条例第 62 条第 2 項）。

（３）安全管理に関する主な規定

ア　一般的な義務

中国個人情報保護法では、個人情報の安全管理に関わる個人情報取扱者の一般的な義務として、以下の①～⑥の措置義務が規定されている（同法第 51 条）。なお、ネットワーク安全法第 42 条第 2 項も、個人情報の安全管理措置として、技術的管理措置等を実施しなければならない旨を規定する[36]。

① 内部の管理制度及び操作規程の制定義務
② 個人情報に対する分類管理の実施義務
③ 適切な暗号化、非識別化等の然るべき安全技術の措置義務
④ 個人情報取扱の操作権限を合理的に確定し、かつ定期的に従業員に対して安全教育及び研修を実施する義務
⑤ 個人情報の安全に関わる事象に対する緊急対応策の制定・実施義務
⑥ 法律、行政法規に定めるその他義務

また、中国個人情報保護法は、取り扱う個人情報が国のネットワーク情報部門の定める数量に達している個人情報取扱者に対して、個人情報保護責任者の指定を要求している（第 52 条）。当該「国のネットワーク情報部門の定める数量」について、2025 年 1 月 1 日に施行された個人情報保護コンプライアンス監査管理弁法第 12 条第 1 項及び 2025 年 7 月 18 日に公表された「個人情報保護責任者の報告業務の実施に関する公告」によれば、100 万人以上とされているため、個人情報取扱者が 100 万人以上分の個人情報を取り扱う場合は、個人情報保護責任者を指定し、ネットワーク情報部門に報告することが必要となる。

イ　個人情報影響評価

さらに、中国個人情報保護法では、個人情報取扱者は、以下の①～⑤のいずれかに該当する場合、個人情報影響評価[37]を行わなければならない（同法第 55 条）。

① 機微な個人情報を取り扱う場合
② 個人情報を利用した自動化された意思決定を行う場合

---

[36] なお、電気通信事業及びインターネット情報サービス提供者については、電気通信及びインターネット利用者の個人情報の保護に関する規定（原文「电信和互联网用户个人信息保护规定」）第 13 条により、個人情報の安全管理措置として必要な措置を実施しなければならない旨の規定がある。この規定は、「国務院部門規章」であり、狭義の「法律」ではないが、法的拘束力を有する「法令」に位置づけられる。

[37] 個人情報影響評価には、①個人情報の取扱目的、取扱方法等が合法的、正当かつ必要なものであるか、②個人の権益に対する影響及び安全リスク、③講じる保護措置が合法的かつ有効であるか、かつリスクの程度に見合ったものであるかといった内容を含めなければならず、個人情報保護影響評価報告及び取扱状況の記録を少なくとも 3 年間保存しなければならないとされているが、具体的にどのように個人情報影響評価を実施しなければならないか等の細則について、本法には規定されていない（同法第 56 条）。

③　個人情報の取扱の委託、その他の個人情報取扱者への個人情報の提供及び個人情報の公開を行う場合
④　個人情報の国外提供を行う場合
⑤　その他個人の権益に重大な影響を与える個人情報取扱行為を行う場合

ウ　個人情報の取扱いの委託等

また、中国個人情報保護法では、個人情報取扱者が、個人情報の取扱いについて委託する場合は、取扱委託の目的、期間、取扱方法、個人情報の種類、保護措置、双方の権利及び義務等について約定した上で、委託者は受託者を監督しなければならないと規定されているため、注意が必要である（同法第 21 条第 1 項）。

加えて、同法では、個人情報取扱者が、合併、分割、解散、破産宣告等の原因により個人情報を移転する必要がある場合、本人に受領者の名称又は氏名及び連絡先情報を告知しなければならないとされている点も注意が必要である（同法第 22 条）。

（4）個人情報の漏えい等[38]

中国個人情報保護法は、個人情報の漏えい等のインシデントが発生した又は発生する可能性が生じた際の、個人情報取扱者における、改善措置の実施、監督機関や本人に対する特定事項[39]の通知に関する義務を規定する（同法第 57 条第 1 項）。また、一定の場合、本人への通知が不要になる旨の一般的規定も設けられている（同条第 2 項）[40]。

また、これら中国個人情報保護法の規定に基づき、ネットワークデータ安全管理条例は、ネットワークデータに関するセキュリティインシデントが発生した際にネットワークデータ取扱者が履行すべき具体的義務として、緊急対応策の発動、被害拡大の防止措置の実施、セキュリティ上のリスクの排除、電話・ショートメッセージ・チャットツール・電子メール・公告等の手段による本人その他利害関係者へ通知等を定めている。

さらに、2025 年 11 月 1 日に施行された国家ネットワークセキュリティインシデント報告管理弁法では、個人情報漏えいを含むネットワークセキュリティインシデント[41]が発

---

[38] 中国個人情報保護法の制定前は、個人情の報漏えい等のインシデントが発生した又は発生する可能性が生じた際の義務については、ネットワーク安全法第 42 条第 2 項で、救済措置、本人への通知及び関係所管機関に対する報告について抽象的な義務が定められていた。

[39] ①個人情報の漏えい、改ざん、又は損失の種類、理由、及び考えられる危害が発生したこと、又は発生する可能性があること、②個人情報取扱者が講じた是正措置、及び個人が危害を軽減するために講じることができる措置、③個人情報取扱者の連絡先

[40] 情報漏えい、改ざん、紛失による危害を効果的に回避するための措置を講じた場合は本人への通知が不要とされているが、監督機関が害を及ぼす可能性があると判断した場合は、本人への通知を要求される。なお、具体的な措置の内容については現時点では不明である。

[41] 国家ネットワークセキュリティインシデント報告管理弁法の別紙として付されている「ネットワークセキュリティインシデント分級ガイドライン」において、ネットワークセキュリティインシデントは、「人的原因、ネットワークへの攻撃、ネットワークにおける脆弱性、ソフトハードウェアの欠陥や故障、不可抗力等の要因により、ネットワーク及び情報システム又はその中のデータや業務アプリケーションに対して危害をもたらし、国家、社会、経済に

生した場合の監督機関への報告に関する具体的な手続[42]や、ネットワークセキュリティインシデントの分類ガイドライン等を定めている。

３．参考資料（法令・ガイドラインなど）

・個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679 （一般データ保護規則）
　前文の参考仮訳 https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf
　条文の参考仮訳 https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf
・GDPR の地理的適用範囲（第 3 条）に関するガイドライン バージョン 2.1 の参考仮訳 https://www.ppc.go.jp/files/pdf/chiritekitekiyouhanni_guideline2.1.pdf
・データ保護オフィサー（DPO）に関するガイドラインの参考仮訳 https://www.ppc.go.jp/files/pdf/dpo_guideline.pdf
・データ保護影響評価（DPIA）及び取扱いが 2016/679 規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドラインの参考仮訳 https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf
・Handbook on Security of Personal Data Processing https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
・THE CNIL'S GUIDES-2018 EDITION SECURITY OF PERSONAL DATA https://www.cnil.fr/sites/default/files/atoms/files/guide_security-personal-data_en.pdf
・中国ネットワーク安全法
・中国データ安全法
・中国個人情報保護法
・中国民法典
・ネットワークデータ安全管理条例
・個人情報保護コンプライアンス監査管理弁法
・ネットワークセキュリティインシデント報告管理弁法・情報安全技術個人情報安全規範

対してネガティブな影響を与える事件」と定義されており、①特に重大なもの、②重大なもの、③比較的重大なもの、④一般的なものの 4 つに分類されている。

[42] 特に重大、重大、若しくは比較的重大なサイバーセキュリティインシデント（①～③）が生じた場合には、監督機関への報告が求められる。このうち、重要情報インフラの運営者は事件発生後 1 時間以内、中央及び国家機関の各部門並びにこれらに直接所属する事業者は事件発生後 2 時間以内、その他のネットワーク運営者は事件発生後 4 時間以内に、それぞれの監督機関に報告する必要がある。

４．裁判例

本文中に記載のとおり

Q83-1 米国における主なサイバーセキュリティ法令

米国における主なサイバーセキュリティ関連法令としてどのようなものがあるか。その際に日本企業が留意すべきポイントとしてどのようなものがあげられるか。

タグ：ランサムウェア、OFAC、FinCEN、Cyber Trust Mark プログラム、NIST SP 800-213、CIRCIA

１．概要

米国においては、連邦法及び州法のいずれのレベルにおいてもサイバーセキュリティに係る包括的な法律は制定されていないが、サイバーセキュリティに関して一定の対応を求める法律は存在する。また、近時のランサムウェア攻撃による被害の増加を受けて、米国財務省外国資産管理局（the U.S. Department of the Treasury's Office of Foreign Assets Control）（以下、本項において「OFAC」という。）や金融犯罪取締網（Financial Crimes Enforcement Network）（以下、本項において「FinCEN」という。）が勧告を公表する等、規制を強化している。

２．解説

（１）包括的なサイバーセキュリティに関する連邦法の有無

米国においては、連邦法及び州法のいずれのレベルにおいてもサイバーセキュリティに係る包括的な法律は制定されていない。もっとも、以下のとおり、サイバーセキュリティに関して一定の対応を求める法律は存在する。

（２）サイバーセキュリティに関する義務・禁止を定める法令

全事業者に向けてサイバーセキュリティに係る包括的な対応を求めるものではないものの、以下のように、各事業者において公正な取引慣行の一環としてサイバーセキュリティ対策を求めたり、また一部の事業者に対してサイバーインシデントに係る報告義務等を課すなど、サイバーセキュリティに関する義務・禁止を定める法令は存在する。

ア　連邦取引委員会法

連邦取引委員会法（Federal Trade Commission Act）（以下、本項において「FTC 法」という。）は、連邦取引委員会（Federal Trade Commission）に対し、執行権限と調査権限を付与する根拠法であり、不公正な競争方法及び欺瞞的取引慣行の排除や消費者保護及び自由な市場競争の維持、企業行動の監視と是正を通じた健全な経済秩序の確立を目的とした法律である。

FTC 法は、米国において営利目的で商取引を行う企業全般に対して、商取引において、不公正又は欺瞞的な行為や慣行を行ってはならないことを義務付けている。近年では、

不十分なサイバーセキュリティ対策も「不公正な取引慣行」として扱われ[1]、企業に合理的なセキュリティ措置の実施を求める法的根拠とされている。実際に、事業者が収集した個人情報を保護するための容易に可能なセキュリティ対策を講じなかったことを要因として第三者による不正アクセスにより大量の個人情報を漏えいさせてしまった事案において、連邦取引委員会が事業者に対して合理的なセキュリティ対策を講じることを求めた執行事例も複数存在する。

イ　重要インフラ・サイバーインシデント報告法

Cyber Incident Reporting for Critical Infrastructure Act of 2022（CIRCIA）[2]は、米国の重要インフラ事業者に対し、重大なサイバーインシデントやランサムウェア支払いに関する報告を義務付ける連邦法である。これにより、米国政府がサイバー攻撃の全体像を把握し、防御策を強化することを目的としている。2024 年 3 月、CIRCIA の施行規則案が公告され、同規則案は、2026 年 5 月までに最終化される予定である[3]。

同法は、米国政府が「重要インフラ」と分類するシステムを所有又は運用する企業（医療、エネルギー、通信、金融サービス等）に加えて、重要インフラを直接運用していなくても、特定のセクターにとって重要なシステムを運用する企業（サービスプロバイダ等）が対象となる。対象事業者は、重大なサイバーインシデントが発生したと合理的に判断した場合、72 時間以内にサイバーセキュリティ・インフラセキュリティ庁（以下、本項において「CISA」という。）に報告しなければならず、ランサムウェア攻撃により身代金を支払った場合、支払い後 24 時間以内に CISA に報告しなければならない。

ウ　コンピュータ詐欺と濫用に関する法律

Computer Fraud and Abuse Act（CFAA）は、不正アクセスやサイバー犯罪を連邦レベルで処罰するための中核的法律である。当初は国家安全保障を目的に 1986 年に制定されたが、後に企業や個人の情報システムも対象に含め、幅広いコンピュータ犯罪（ハッキング、マルウェア配布、情報窃取、詐欺など）に対する刑事罰と民事救済を規定する法律として発展している。

---

[1] FTC によるブログ記事（https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/security-principles-addressing-vulnerabilities-systematically）は、不適切なサイバーセキュリティ対応が「不公正な取引慣行」に該当し得ることを前提に、代表的な脆弱性に対する既知の予防策を設計段階から組み込む必要性等を解説している。

[2] Cyber Incident Reporting for Critical Infrastructure Act of 2022(CIRCIA)（https://www.congress.gov/bill/117th-congress/house-bill/2471/text）

[3] OFFICE of INFORMATION and REGUKATORY AFFAIRS OFFICE of MANAGEMENT and BUDGET（https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202504&RIN=1670-AA04）

コンピュータ又はネットワークにアクセスする全ての個人及び組織に対して、不正アクセスによって詐欺を実行し金銭等を取得することやコンピュータに損害を与えること、他人のパスワード等を詐欺目的で不正に流通・販売すること等を禁じている。

エ　データセキュリティプログラム

2024 年 2 月に「懸念国による米国人の機微な個人データ及び米国政府関連データへのアクセス防止に関する大統領令」（大統領令第 14117 号）が発行され、同大統領令を受けて、「データセキュリティプログラム」が策定された。データセキュリティプログラムは、懸念国に関係する事業者又は個人による米国政府関連データ又は大量の機微な個人データへのアクセス・利用が、米国の国家安全保障を損なう脅威となり得ることに対処することを目的としている。

データセキュリティプログラムは、米国人（U.S.Person）に対して、懸念国又は規制対象者との間でのデータ取引等を禁止している。対象となるデータは、米国政府関連データに加えて、大量の機微な個人データである。具体的には、ヒトゲノム情報、生体認証情報、正確な位置情報、個人の健康情報、個人の財務情報等が挙げられており、各カテゴリごとに、規制対象となるか否かの閾値が定められている。

（３）ランサムウェアに関する規制

OFAC の規制の中には、外交政策・安全保障上の目的から特定の国・地域及び制裁対象者リスト（Specially Designated Nationals and Blocked Persons List）（以下、本項において「SDN リスト」という。）に記載された個人・団体等を対象として取引制限や資産凍結等の措置を講じているものがある。そして、OFAC 規制は、主に米国人・米国法人を対象とする措置（一次的制裁）と非米国人・非米国法人を対象とする措置（二次的制裁）に分類されるが、このうち一次的制裁は制裁金のみならず、刑事罰の対象となる上に、米国との接点がある限り、非米国人・非米国法人であっても域外適用される可能性がある。

近年、米国においてランサムウェア攻撃による被害が急増していることを受けて、2021 年 9 月 21 日、OFAC は、ランサムウェア支払いの助長についての潜在的制裁リスクについてのアップデート版の勧告（Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）（以下、本項において「OFAC 勧告」という。）[4]を公表し、同年のうちに複数の暗号資産取引所を SDN リストに追加している。

OFAC 勧告では、ランサムウェアの支払いへの協力は OFAC 規制に違反し、厳格責任に基づく制裁金の対象となりうることを明記するとともに、制裁遵守プログラム（Sanctions Compliance Program）の存在、性質及び適切性や、CISA の「ランサムウ

[4] U.S. DEPARTMENT OF THE TREASURY Office of Foreign Assets Control (https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf)

ェアガイド 2020 年 9 月」（Ransomware Guide September 2020）[5]において強調されているサイバーセキュリティプラクティスの採用又は改良を通じたリスク軽減のステップが、制裁の決定に際して、制裁緩和の要素として考慮されるとしている。さらに、OFAC 勧告においては、ランサムウェアの支払いを被害者に代わって行うことに関与する企業は、金融犯罪取締網（Financial Crimes Enforcement Network）（以下、本項において「FinCEN」という。）の規制を遵守する義務があるか否かに留意すべきである旨記載し、脚注において FinCEN の 2020 年 10 月 1 日付勧告（Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments[6]）（以下、本項において「FinCEN 勧告」という。なお、FinCEN 勧告は 2021 年 11 月 8 日付でアップデートされている[7]。）を引用している。

FinCEN 勧告は、金融機関が、銀行秘密法（Bank Security Act）に定める義務を遵守することを通じて、米国の金融システムをランサムウェアの脅威から守ることについて重要な役割を果たすとしつつ、金融機関は、ランサムウェア事案を扱う場合には、疑わしい取引報告（Suspicious Activity Reporting）（以下、本項において「SAR」という。）を行うことの要否・適否について決定すべきであるとしている。

さらに、換金可能な暗号資産の交換業者（CVC exchanges）を含む金融機関が、ランサムウェア攻撃に関連する疑わしい取引を特定し、SAR の義務を果たすことの重要性に照らし、FinCEN 及び法執行機関は、ランサムウェア攻撃に関する疑わしい取引は、「即時の注意が要求される違反に関する事態」[8]に該当する（金融機関による即時の通知が必要となる）と考える旨表明し、金融機関に対して、疑わしい取引の報告義務の履行を求めている。

（４）米国における IoT についての動向

ア　概要と目的

「U.S. Cyber Trust Mark プログラム」（以下、本項において「本プログラム」という。）は、消費者向け IoT 製品のセキュリティを強化するための制度であり、メーカー企業が自社製品のセキュリティ評価を行い、サイバーセキュリティ基準を満たした消費者向け IoT 製品に対し、「U.S. Cyber Trust Mark」というラベルを付すというものとなっている。

本プログラムはあくまで任意の取組であり、示されたセキュリティ要件を満たさなかったからといって罰則等の制裁が科されるわけではないが、本プログラムに準拠する製

[5] MS-ISAC「RANSOMWARE GUIDE」（2020 年）（https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf）
[6] 「FinCEN ADVISORY」（2020 年）（https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf）
[7] 「FinCEN ADVISORY」（2021 年）（https://www.fincen.gov/sites/default/files/2021-11/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf）
[8] 例えば、31 C.F.R. § 1020.320(b)(3)。

造業者が、自社製品に組み込む製品コンポーネントの製造業者に対して、その取引契約等において、プログラム要件への適合を求めるようになる可能性がある。

この制度により、消費者が十分な情報を得た上で購入を決定できるようなり、市場で信頼できる製品を差別化し、メーカー企業がより高いサイバーセキュリティ基準を満たすためのインセンティブを生み出すことにつながることが期待されている。

イ　適用対象

本プログラムの対象は、現時点では、「消費者向け IoT 製品（Consumer IoT Products）」とされている（§8.202(b)参照。）。

「消費者向け（Consumer）」とは、文字どおり消費者向け製品が対象であり、製造、ヘルスケア、産業制御その他の企業向けアプリケーションでの使用を主な目的とした製品は含まれない趣旨とされている（前文第 21 項参照。）。

「IoT 製品（IoT Products）」とは、無線通信によってインターネットに接続可能な機能を有する機器及びこれを構成するような一部分を意味するとされており、「IoT デバイス（IoT Devices）」よりも広い概念となっている（前文第 8 項、第 13 項参照。）。具体的には、スマート冷蔵庫、スマート電子レンジ、スマートテレビ、スマート空調システム、スマート・フィットネス・トラッカーなどが含まれる（§8.202(i)、第 13 項）。

ウ　プログラムの内容

本プログラムにおけるラベルの付与は、①認証機関（Cybersecurity Label Administrator）が認めた試験機関（例：(i)独立系の CyberLAB、(ii)企業が認定を受けて設立する社内 CyberLab（In-House Testing Lab）、(iii)認証機関が運営する CyberLab（CLA-Run Testing Lab））による製品試験と②認証機関（Cybersecurity Label Administrator）によるラベル認証という 2 段階の手続を経て行われる（前文第 71 項）。

ラベルの付与を受けるためには、まず CyberLAB による製品試験を受ける必要がある。製品試験は、ラベル認証を受けるために適合する必要があるセキュリティ要件（以下、本項において「プログラム要件」という。）への適合の有無について評価及び試験を実施し、試験結果の報告書を提供するものである（前文第 61 項参照。）。

ラベル認証の申請を受けた認証機関は、申請書と添付文書を審査の上、当該 IoT 製品がプログラム要件に適合している場合、ラベルを付与する（§8.205）。本プログラムにおけるプログラム要件は、NISTIR 8425 を基礎とし（前文第 89 項）、本プログラムに対応したセキュリティ基準・試験手順が定められることが想定されている（前文第 92 項）が、現時点でかかるセキュリティ基準・試験手順は策定・公表されていない。

なお、NISTIR 8425 は、(i)資産の識別、(ii)製品構成、(iii)データ保護、(iv)インターフェースアクセス制御、(v)ソフトウェアの更新及び(vi)セキュリティ状態認識という 6

つの技術的要件と、(i)ドキュメント作成、(ii)情報及び問合せ対応、(iii)情報公開及び(iv)教育・啓発という、4 つの非技術的要件から構成されている。

ラベルには、U.S. Cyber Trust Mark とともに QR コードが付されており、QR コードを読み取ることによって、製品登録制度に基づき登録された当該 IoT 製品の詳細な情報を確認することができる仕様となることが想定されている（前文第 95 項、第 98 項）。ラベルの使用を許可された製造業者は、製品登録制度を通じ、消費者に製品の情報を開示する必要がある。

製造業者は、ラベルの付与を受けた IoT 製品がプログラム要件に適合しているかどうかを継続的に確認し、ラベルの使用許可を更新する義務を負う（前文第 111 項）。また、認証機関が、当該 IoT 製品がプログラム要件に適合していないと判断した場合、直ちに被付与者と統括認証機関に対して書面で通知し、被付与者は 20 日以内に不備を是正するために講じた措置を記載した報告書を認証機関に対して提出する必要がある。そして、20 日以内に不備が是正されない場合、被付与者は使用許可を喪失することになる（前文第 116 項）。

（５）IoT 機器の政府調達に関する規制

NIST SP800-213 は、連邦政府機関が IoT 機器を利用する際にベンダに対して何を求めるべきか記載されたガイドラインである。

もっとも NIST SP800-213 には、具体的なセキュリティ対策についての記載がないため、IoT 機器製造企業は NISTIR 8259（IoT 機器製造企業が、実施すべきセキュリティ関連活動の推奨事項が記載）、NISTIR 8259A（IoT 機器が実装すべきセキュリティ機能の詳細）、NISTIR 8259B（IoT 機器製造時や製造後に導入すべきフローやサービスの詳細）を参照する必要がある。NISTIR 8259 では、IoT 機器の市販前フェーズにおいては、(i) 想定顧客／ユーザを特定し、想定ユースケースを定義する、(ii) 顧客のサイバーセキュリティへのニーズと目標を調査する、(iii) 顧客のニーズと目標に取り組む方法を決定する、及び(ix) 顧客のニーズと目標を適切に支援するための計画を策定する、といった 4 つの活動項目が挙げられている。また、IoT 機器の市販後フェーズにおいては、(i) 顧客とコミュニケーションするアプローチを定義する、及び(ii) 顧客とコミュニケーションする内容とそれをコミュニケーションする方法を決定するといった 2 つの活動項目が挙げられている。そして、NISTIR 8259A では技術的な要件として「デバイス識別」「安全な構成」「データ保護」「論理アクセス制御」「ソフトウェア更新」「サイバーセキュリティ状態認識」といった内容が、NISTIR 8259B では非技術的な要件として「文書提供」「通知・教育」「脆弱性報告対応」「セキュリティサポート体制」といった内容がそれぞれ定められている。

また、SP 800-213 の補足文書として NIST SP 800-213A があり、IoT 機器に求められるサイバーセキュリティ能力と非技術的支援能力をカタログ形式で整理しており、SP

800-213 の枠組みを前提とし、各能力（デバイス識別、設定、データ保護、論理アクセス、ソフトウェア更新、状態認識、機器セキュリティ等）及び支援能力（設計文書、通知、脆弱性情報対応、教育・啓発など）を定義し、それぞれの細目要件を示している。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

Q83-2 EU・英国における主なサイバーセキュリティ法令

EU・英国における主なサイバーセキュリティ関連法令としてどのようなものがあるか。その際に日本企業が留意すべきポイントとしてどのようなものがあげられるか。

タグ：NIS2 指令、基幹サービス運営者、デジタルサービス提供者、EU サイバーセキュリティ法、EU サイバーレジリエンス法、EU データ法

１．概要

欧州連合（EU）においては、ネットワーク・情報システムの安全に関する指令[1]（以下、本項において「NIS2 指令」という。）が、EU 加盟国が遵守すべきセキュリティ対策規範を定めており、NIS 指令[2]に代わって 2023 年 1 月 16 日から施行されている。また、EU 域内における統一的なサイバーセキュリティ認証制度の整備を目指して、EU サイバーセキュリティ法（EU Cybersecurity Act[3]）が 2019 年 6 月 27 日から施行されていることに加えて、EU 域内でのデータ流通を目的として、EU データ法（Data Act）が一部規定を除き 2025 年 9 月 12 日から施行されている。

英国においては、PSTI 法が 2022 年 12 月 6 日に成立し、2024 年 4 月 29 日に発効した。

２．解説

２－１．EU

（１）NIS2 指令

ア　NIS2 指令の概要

NIS2 指令は、欧州連合（EU）加盟国が遵守すべきセキュリティ対策規範を定めるものであり、EU 加盟国は、NIS2 指令が定める要求事項を各国法において定める必要がある。NIS2 指令は、2022 年 12 月 14 日に欧州議会及び欧州理事会で採択され、NIS 指令を廃止し、2023 年 1 月 16 日に発効した。

---

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

イ　NIS2 指令の目的

NIS2 指令の目的は大きく以下のとおりに分類される。

① 各国はサイバーセキュリティ国家戦略策定や、Computer Security Incident Response Team 設置を含めたサイバーセキュリティインシデント対応の国家的枠組みを構築すること

② 各国はサイバーセキュリティ関連の情報共有等の国家的枠組みを構築すること

③ 各国は主要エンティティ及び重要エンティティに対するインシデント届出義務等を課すセキュリティ法制を定めること

ウ　NIS2 指令の適用対象となる民間事業者

NIS2 指令の適用対象となる民間事業者は、主要エンティティ（Essential Entities）及び重要エンティティ（Important Entities）である。EU 加盟国は、2025 年 4 月 17 日までに、主要エンティティ及び重要エンティティのリストを作成する義務が課されている（NIS2 指令第 3 条第 3 項）。

① 主要エンティティ

主要エンティティ（Essential Entities）については、エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICT サービスマネジメント、公的サービス又は宇宙の 11 の事業分類（sector）ごとに種類（type of entity）が列記されている（NIS2 指令 Annex Ⅰ）。

② 重要エンティティ

重要エンティティ（Important Entities）については、郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）、デジタルプロバイダー及び研究の 6 つの事業分類ごとに種類が列記されている（NIS2 指令 AnnexⅡ）。

エ　NIS2 指令との関係において民間事業者に課される義務の内容

NIS2 指令は、EU 加盟国に対し、国内法において主要エンティティ及び重要エンティティに対し、大要、以下の義務を課すことを要求する。

① EU 域内提供サービスに使用するネットワーク及びシステムのリスクを管理するための適切な技術的かつ組織的な措置を講じること（NIS2 指令第 21 条第 1 項～第 4 項）

② EU 域内提供サービスに使用するネットワーク及びシステムに対するインシデントによる影響を防止・最小化するための適切な技術的かつ組織的な措置を講じること

③ 提供するサービスの継続性に重大な影響を及ぼすインシデントについて、24 時間以内に管轄官庁又は CSIRT に対し通知し、72 時間以内にインシデントの重大性や影響に関する評価を通知し、1 か月以内にそれらの詳細な説明を含む最終報告書を提出すること（NIS2 指令第 23 条第 1 項～第 4 項）

主要エンティティに対しては定期的な監査や監督が可能であるのに対し、重要エンティティに対しては NIS2 指令に違反しているとの証拠や情報があった場合の事後的な監督措置が基本となっている等、主要エンティティは重要エンティティに比較して厳格な規制に服する。

さらに、NIS2 指令は、EU 加盟国に対し、NIS2 指令に基づき採択された国内規定への違反があった場合に適用可能な罰則規定を定め、その実施を確保するための適切な措置を講じることを要求する（NIS2 指令第 36 条）。

（２）EU サイバーセキュリティ法

EU サイバーセキュリティ法は、欧州サイバーセキュリティ庁（European Union Agency for Cybersecurity、ENISA）の目的、役割、組織、権限等について定めるとともに、EU 域内における ICT 製品、ICT サービス及び ICT プロセスに関する統一的なサイバーセキュリティ認証制度である欧州サイバーセキュリティ認証フレームワーク（European cybersecurity certification framework）の確立を目的とする法律であり、2019 年 4 月 17 日に成立し、同年 6 月 27 日に施行された。2023 年 4 月 18 日には、ICT 製品、ICT サービス及び ICT プロセスに加えてマネジメントセキュリティサービスも認証制度の対象とする提案がなされ、改正案が 2025 年 1 月 15 日に採択されている[4]。

EU 加盟国は、EU サイバーセキュリティ法に基づき、EU 域内で製造・販売される ICT 製品、ICT サービス及び ICT プロセスのセキュリティ認証の規格統一を目指しており、2025 年 2 月 27 日に適用開始となった EUCC をはじめ、今後 ICT 製品、ICT サービス及び ICT プロセスのタイプや類型ごとに認証基準が順次作成されることが予定されている。また、欧州委員会は、ENISA の権限、欧州サイバーセキュリティ認証フレームワーク、ICT サプライチェーンのセキュリティ課題への対応の観点から同法の見直しを検討している[5]。

[4] European Commission EU Cybersecurity Act（https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act?utm.com）

[5] European Commission Commission opens consultation on revising EU Cybersecurity Act（https://digital-strategy.ec.europa.eu/en/news/commission-opens-consultation-revising-eu-cybersecurity-act）

（３）EU サイバーレジリエンス法

ア　法律の目的と概要

EU サイバーレジリエンス法（Cyber Resilience Act: CRA）は、2024 年 10 月 10 日に欧州理事会で採択され、同年 12 月 10 日に発効した EU の規則である。EU 市場で流通するデジタル製品をサイバーセキュリティの観点から規制し、共通のサイバーセキュリティルールを導入することで、サイバー攻撃のリスクを軽減し、安全なデジタル環境を実現することに加えて、CRA の定めるサイバーセキュリティ要件を満たさないデジタル製品を EU 市場から排除し、消費者が安全な製品を選択できるようにすることを目的としている。

CRA は、EU 市場に上市されるデジタル要素を含む製品（IoT 機器、スマートデバイス、通信機器、商用 SaaS、オープンソースソフトウェア等）に適用される。日本企業であっても EU 市場に製品を供給する場合には適用対象となり得る点に留意が必要である[6]。

イ　適用対象となる製品の範囲

CRA は、「デジタル要素を含む製品」（products with digital elements）であって、意図された目的又は合理的に予見可能な使用がデバイス又はネットワークへの直接的又は間接的な論理的又は物理的データ接続を含むものに適用される（CRA 第 2 条第 1 項[7]）。

「デジタル要素を含む製品」とは、主にソフトウェア又はハードウェア製品、及びその遠隔データ処理ソリューションをいい、別個に上市されるソフトウェア・ハードウェアコンポーネントを含む[8] [9]。

---

[6] EU 各加盟国においても個別の関連する取組が存在する場合がある。例として、ドイツの消費者向け IoT 製品対象セキュリティラベリング制度が挙げられる。同制度は、ドイツ連邦情報セキュリティ庁が 2021 年 12 月から運用を開始した制度で、消費者が IT 製品のセキュリティ特性を一目で理解できるようにする仕組みである。また同制度は、シンガポールにおける IoT 製品のセキュリティレベル向上に向けた同様の取組であるサイバーセキュリティラベリングスキーム（CLS：Cybersecurity Labelling Scheme:）と相互承認を実施している。これにより、例えば、ドイツの IT セキュリティラベルが発行されたスマートコンシューマー製品は、シンガポールのサイバーセキュリティラベル制度のレベル 2 を満たしていると Cyber Security Agency Singapore（CSA)によって認定され、CLS レベル 2 以上の製品はドイツの IT セキュリティラベルの要件を満たしていると認定される。

[7] 以下特に断らない限りいずれも条文は CRA のものを指す。

[8] 例えば、PC、スマートフォン、スマートロボット、IC カード、スマートホーム製品、モバイルアプリ、ビデオゲーム等、幅広いソフトウェア又はハードウェア製品と、これらのコンポーネントが含まれる。

[9] また、クラウドソリューションに関しては、遠隔データ処理ソリューションに該当する場合にのみ、CRA の適用を受ける。「遠隔データ処理」とは、製造業者自身により、又は製造業者の責任の下で設計・開発されたソフトウェアによる遠隔地でのデータ処理であって、それがなければデジタル要素を含む製品がその機能の一部を実行できなくなるものをいう（第 3 条第 2 項）。例えば、スマートホーム製品の製造業者が提供するクラウド対応機能で、ユーザが遠隔地からデバイスを制御できるようにするものは、「遠隔データ処理ソリューション」

「意図された目的又は合理的に予見可能な使用がデバイス又はネットワークへの直接的又は間接的な論理的又は物理的データ接続を含むもの」には、IoT 機器のようにネットワーク接続を前提とした製品や、他の機器やシステムに組み込まれる製品等のデジタル製品が幅広く含まれる。一方で、スタンドアロンで動作し、外部との接続を想定していない製品であれば、この要件を満たさず、CRA の適用対象から除外されると考えられる。

他方で CRA には、以下を含む特定の製品に関して適用除外規定が設けられている。

- 医療機器規則、体外診断用医療機器規則、自動車型式認証規則等の個別法が適用される製品（第 2 条第 2 項）
- 民間航空分野における一般規則（Regulation (EU) 2018/1139）に則って認証されているデジタル製品（第 2 条第 3 項）
- 国家安全保障・軍事目的、機密情報を処理するために特別に設計されたデジタル製品（第 2 条第 7 項）
- 商業活動外で提供されるオープンソースソフトウェア等（前文第 12 項、第 18 項）

ウ　義務主体の種類・範囲

CRA の義務主体として、「デジタル要素を含む製品」のライフサイクル・チェーンに関与する全ての経済事業者（economic operator）、すなわち、製造業者（manufacturer）、輸入業者（importer）、流通業者（distributor）等が想定されている（第 3 条第 12 号）。そのため、CRA は、EU 域内の事業者のみならず、外部との接続を予定した「デジタル要素を含む製品」を EU 向けに製造する日本の事業者、及び当該製品を EU 市場で入手できるように流通させる日本の事業者に対しても域外適用されることになる。

エ　適用開始時期

CRA は 2024 年 12 月 10 日に発効済みだが、各義務の適用開始時期は、以下のとおり、当局及びユーザへの脆弱性・インシデントの報告・通知義務（以下本項において、便宜上単に「報告義務」という。）とそれ以外の義務とで異なる。

まず報告義務以外の義務については、2027 年 12 月 11 日から適用され、原則として、同日以降に「上市された（have been placed on the market）」対象製品のみが適用を受ける[10]。

に該当する。他方で、デジタル要素を含む製品の機能をサポートしないウェブサイトや、デジタル要素を含む製品の製造業者の責任外で設計・開発されたクラウドサービスは、「遠隔データ処理ソリューション」にあたらず、CRA の適用を受けない（前文第 12 項）。

[10] ここでいう「上市（placing on the market）」とは、商業活動の過程において、EU 市場における頒布又は使用のために、対象製品を供給（supply）する最初の機会をいう(第 3 条第 21 号・第 22 号)。

次に、報告義務に関しては、2026 年 9 月 11 日から適用され、EU 市場におかれた対象製品である限り、2027 年 12 月 11 日より前に供給されたものであったとしても、報告義務の適用を受ける。すなわち、報告義務に関しては、報告義務以外の義務とは異なり、EU 市場への供給の時期とは関係なく適用があり、EU 市場に供給している対象製品に関して、2026 年 9 月 11 日以降、当局やユーザへの脆弱性・インシデントの報告・通知を実施する必要がある[11]。

オ　主体別の義務内容

各適用対象主体に課される義務は概要以下のとおりである。

（ア）製造業者

a. 報告義務以外の義務

(a) 上市前の義務

製造業者に対しては、報告義務以外の義務のうち、上市前の義務として、以下の義務が課される。

- 必須サイバーセキュリティ要件への準拠確保（第 13 条第 1 項、ANNEX 1）
- サイバーセキュリティリスク評価の実施・文書化（第 13 条第 2 項・第 3 項）
- 技術文書の作成（第 13 条第 12 項、第 31 条）
- 適合性評価手続の実施（第 13 条第 12 項、第 32 条）
- EU 適合宣言書の作成（第 13 条第 12 項、第 28 条）
- CE マークの貼付（第 13 条第 12 項、第 29 条、第 30 条）
- 第三者コンポーネントのデュー・ディリジェンス実施（第 13 条第 5 項）等

(b) 上市後の義務

上市後の義務としては、以下の義務が課される。

- デジタル製品を上市する際にデジタル製品と共に型式やシリアル番号等の一定の情報を提供する義務（第 13 条第 15 項、第 16 項、第 18 項、第 19 項、ANNEX II）
- 最低 5 年間のサポート期間の設定とサイバーセキュリティリスク評価結果のアップデート（第 13 条第 8 項）
- 脆弱性対処のためのポリシー・手順の整備（第 13 条第 7 項）
- デジタル製品がセキュリティ要件に適合した状態を維持するための手続の確保（第 13 条第 14 項）等

b. 報告義務

製造業者は、対象製品に関して「実際に悪用されている脆弱性（actively exploited vulnerability）」を認識した場合（第 14 条第 1 項）又は「対象製品のセキュリティに影

[11] もっとも、後述のとおり、輸入業者と流通業者の報告義務に関しては、製造業者の報告義務とは異なり、2027 年 12 月 11 日以降でなければ適用が開始されない。

響を及ぼす重大なインシデント（severe incident having an impact on the security of the product with digital elements）」（同条第 3 項）を認知した場合に、各加盟国によりコーディネーターとして指定された CSIRT[12]及び ENISA[13]に報告する必要がある[14]。

（イ）輸入業者

a. 報告義務以外の義務

輸入業者に対しては、報告義務以外の義務として、以下の義務が課される。

- 対象製品を市場におく際、事前に、対象製品が必須サイバーセキュリティ要件に準拠しているかを確認する義務（第 19 条第 1 項・第 2 項）
- 対象製品自体又は対象製品のパッケージ若しくは付属文書において、(i) 輸入業者の名称、登録商号又は登録商標、(ii) 郵便番号、メールアドレス又はその他の電磁的な連絡先及び（iii）（存在する場合）輸入業者に連絡できるウェブサイトの情報を記載する義務（第 19 条第 4 項）、EU 適合宣言書の写しを一定期間[15]保管する義務（第 19 条第 6 項）等

b. 報告義務

輸入業者は、報告義務として、サイバーセキュリティリスクをもたらす一定の場合に、製造業者や当局への報告を行う必要がある（第 19 条第 3 項・第 5 項）。

（ウ）製造業者

a. 報告義務以外の義務

流通業者に対しては、報告義務以外の義務として、以下の義務が課される。

- CRA で定められた各種要件に関して相当の注意（due care）を払う義務（第 20 条第 1 項）
- 対象製品に CE マーク及び型番等が付されていること、並びに製造業者・輸入業者が CRA に基づいてユーザへの情報提供を行っていることを確認する義務（同条第 2 項）等

b. 報告義務

[12] CSIRT とは、Computer Security Incident Response Team の略称であり、各 EU 加盟国において設立又は指定された組織を指す。また、「コーディネーターとして指定された CSIRT」とは、各 EU 加盟国が、NIS2 指令（Directive（EU）2022/2555）12 条 1 項に基づき、脆弱性に関する対応を調整するために指定した CSIRT をいう（第 3 条第 51 号）。

[13] ENISA とは、欧州全域でのサイバーセキュリティの共通水準を高めることを目的とした EU の機関である European Union Agency for Cybersecurity を指す。

[14] 脆弱性又はインシデントを発見してから 24 時間以内に早期警告報告を行い、72 時間以内にデジタル製品に関する一般的情報、悪用及び脆弱性についての性質、講じられた是正措置、ユーザが講じられる是正措置、（該当する場合）製造業者による通知された情報の機微の程度といった情報について報告する必要がある。

[15] 10 年間又はサポート期間のいずれか長い期間である。

流通業者は、サイバーセキュリティリスクをもたらす一定の場合に、製造業者や当局への報告を行う必要がある[16] [17]（第 20 条第 3 項・第 4 項）。

カ　罰則

製造業者が各義務に違反した場合、最高 1,500 万ユーロ又は全世界年間総売上高の 2.5%のいずれか高い方の金額を上限として行政罰が科される（第 64 条第 2 項）。

輸入業者又は流通業者が各義務に違反した場合、最高 1,000 万ユーロ又は全世界年間総売上高の 2%のいずれか高い方の金額を上限として行政罰が科される（同条第 3 項）。

キ　関連する諸外国の制度

CRA と同趣旨の制度として、日本には JC-STAR（Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）制度が存在する。現在、CRA と JC-STAR 制度との間で相互認証に向けた交渉が行われている[18]。

JC-STAR 制度の詳細については、Q36 を参照されたい。

（４）EU データ法

ア　EU データ法の概要

EU データ法（Data Act, Regulation (EU) 2023/2854）は、データへの公平なアクセス及びその利用について定めた EU の包括的な規則である。EU データ法は、大きく、①総則（目的・定義）②EU データ法の適用対象及びその対象が負う義務③執行・制裁で構成されている。一部の規制を除き、2025 年 9 月 12 日から施行されており、欧州データ戦略の中核として作用することが見込まれている。

イ　EU データ法の目的

近年、データ駆動型の技術は経済に大きな変革をもたらしており、高品質で相互運用可能なデータは、競争力とイノベーションを高め、持続可能な経済成長につながることが期待されている[19]。しかし、データ共有の障壁が残存すると、社会全体にとって最適なデータの活用を妨げる懸念がある[20]。そこで、こうした課題に対応し、経済のニーズに沿ってデータ共有を促進するためには、誰がどのような条件や根拠でデータを利用で

---

16 一定の場合に「製造業者」とみなされ製造業者に対する報告義務を自らの義務として負うことになる点は輸入業者と同様である（第 21 条）。
17 輸入業者と同様、流通業者の報告義務も、2027 年 12 月 11 日以降でなければ適用が開始されない（第 71 条第 2 項）。
18 IPA JC-STAR 活用に向けた取り組み（https://www.ipa.go.jp/security/jc-star/leverage.html）。
19 EU データ法前文第 1 項。
20 EU データ法前文第 2 項。

きるかを明確に定める、EU 域内で調和された枠組みが必要であるため、EU データ法が制定された[21]。

ウ　適用場面及び主体

EU データ法の適用が想定される場面及び適用される主体は、それぞれ以下のとおりである。

① コネクティッド製品又は関連サービスからデータが生成される場面
- EU 域内で上市されるコネクティッド製品の製造者及び関連サービスの提供者（いずれも設立地を問わない）
- EU 域内で上市されるコネクティッド製品又は関連サービスの利用者（EU 域内の者に限る）

② 事業者間でデータを利用可能にする場面
- EU 域内のデータ受領者にデータを利用可能にするデータ保有者（設立地を問わない）
- データを利用可能になるデータ受領者（EU 域内の者に限る）

③ 公的機関の要求に応じてデータを利用可能にする場面
- 公益のために行われる業務の遂行のためにデータが例外的に必要な場合であって、データ保有者に対してデータを利用可能にするよう要求する公的機関、欧州委員会、欧州中央銀行、EU の機関
- 上記の要求に対してデータを提供するデータ保有者

④ データ処理サービスを提供する場面
- EU 内の顧客に対してデータ処理サービスを提供する提供者（設立地を問わない）

⑤ データスペースに参加する場面
- データスペースの参加者

⑥ スマートコントラクトを利用又は配備する場面
- スマートコントラクト（一連の電子データ記録を利用し、その完全性と時系列順序の正確性を確保した、契約又はその一部の自動的な締結に利用されるコンピュータプログラム）を利用するアプリケーションの提供者
- 契約締結の過程において他人のためにスマートコントラクトを配備する取引、事業又は職業を営む者

エ　事業者の義務

以下では実務上民間企業に適用される例の多い、コネクティッド製品又は関連サービスからデータが生成される場面における規律を概説する。

[21] EU データ法前文第 4 項。

① 製品データ及び関連サービスデータを利用者に利用可能にする規律

・ 利用者がデータに直接アクセスできるように設計・製造・提供する義務

製品データ及び関連サービスデータが、容易に、安全に、無償で、包括的かつ構造化され、一般的に利用される機械が判読可能な形式で、かつ、適切かつ技術的に可能な場合には、利用者が直接アクセスできるような方法で、コネクティッド製品が設計及び製造され、また、関連サービスが設計及び提供されなければならない（第 3 条第 1 項）。

・ 利用者の要求に基づいて利用者がデータにアクセスできるようにする義務

データ保有者は、利用者がデータに直接アクセスできない場合、利用者の要求に基づいて、容易に利用可能なデータ、及びそれらのデータを解釈し利用するために必要な関連するメタデータを、データ保有者が利用可能なものと同じ品質で、容易に、安全に、無償で、包括的かつ構造化され、一般的に利用される機械判読可能な形式で、かつ、適切かつ技術的に可能な場合は、継続的に、かつ、リアルタイムで、利用者がアクセスできるようにしなければならない（第 4 条第 1 項）。

・ コネクティッド製品及び関連サービスの契約前説明義務

コネクティッド製品の購入、レンタル又はリース契約を締結する前に、法定の 4 項目を、関連サービスの提供に関する契約を締結する前に、法定の 9 項目を、利用者に対し、明確かつ理解しやすい方法で情報提供しなければならない（第 3 条第 2 項、第 3 項）。

② 利用者の要求に応じてデータを第三者に利用可能にする規律

データ保有者は、利用者又は利用者の代理を務める関係者から要求があった場合、容易に利用可能なデータ、及びそれらのデータを解釈し利用するために必要な関連するメタデータを、データ保有者が利用可能なものと同じ品質で、容易に、安全に、無償で、包括的にかつ構造化され、一般的に利用される機械判読可能な形式で、かつ、適切かつ技術的に可能な場合には、継続的に、かつ、リアルタイムで、第三者に提供するものとする（第 5 条第 1 項）。

③ 利用者の要求によってデータを受領する第三者の処理に関する規律

・ 第三者におけるデータの処理制限

第三者は、利用者の要求によって利用可能となったデータを、利用者と合意した目的及び条件の下でのみ処理しなければならず、個人データに関しては、個人データの保護に関する EU 法及び国内法に従って処理しなければならない（第 6 条第 1 項前段）。

・ 第三者におけるデータの消去義務

第三者は、非個人データに関して利用者と別段の合意がない限り、合意された目的に必要でなくなった時点で当該データを消去しなければならない（第 6 条第 1 項後段）。

２－２．英国[22]

（１）PSTI 法の概要

PSTI 法は、スマートベビーモニターやスマートスピーカー等の IoT 製品等の市場が急速に成長しており、また、消費者はこれらの製品が安全であると大多数が思い込んでいるにも関わらず、これらの製品におけるサイバーセキュリティ対策は不十分であるという問題に対処するために策定されたものであり、2022 年 12 月 6 日に成立し、2024 年 4 月 29 日に発効した。

当該問題への対処として、PSTI 法は、英国における一定の IoT 製品等の製造業者等にサイバーセキュリティ要件遵守等の義務を課しているところ、英国の消費者が手に取る可能性のある IoT 製品等の製造業者に広く適用される設計となっているため、英国の消費者に向けた IoT 製品を製造している製造業者は特に注意が必要である。

（２）対象となる製品

PSTI 法は、①インターネット接続製品（internet-connectable product）又はネットワーク接続製品（network-connectable product）であって、②対象除外製品（excepted product）に該当しないものに適用される（PSTI 法第 4 条。以下本項において、①②ともに該当するものを「PSTI 法対象製品」という。）。具体的には、スマート家電、スマートスピーカー、ウェアラブルデバイス等、多岐にわたる IoT 製品が PSTI 法対象製品に含まれる。また、PSTI 法対象製品の範囲は製造時期により限定されず、過去に製造された既存製品であっても、販売・供給時点で要件を満たす場合には本法の適用対象となる。

なお、対象除外製品は、PSTI 規則で特定される製品とされ、具体的には、北アイルランドで供給される製品、電気自動車チャージポイント、医療機器、スマートメーター製品、コンピュータ（デスクトップ、ラップトップ及び携帯ネットワーク接続機能を持たないタブレット）が列挙されている（PSTI 法第 6 条、PSTI 規則第 6 条・別紙 3）。

（３）対象事業者

PSTI 法の義務主体は、PSTI 法対象製品の製造業者（manufacturer）、輸入業者（importer）、流通業者（distributor）を規制対応の主体としており、それぞれの主体の

[22] 英国では、PSTI 法のほか、必須サービス及びデジタルサービスの提供に向けたネットワーク・情報システムのセキュリティ水準を向上させるための法的措置を定める NIS 規則（The Network and Information Systems Regulations 2018）が定められているが、同規則については、現在、同規則を改正・拡充する法案（The Cyber Security and Resilience (Network and Information Systems) Bill）が提案・審議されている。

類型ごとに、規制の内容が定められている（PSTI 法第 7 条）。そして、製造業者については、英国内の対象事業者のみでなく、PSTI 法対象製品を英国の消費者が入手することを意図している又は入手するであろうと認識している製造業者についても、PSTI 法の対象としている（PSTI 法第 8 条、第 54 条）。

（４）PSTI 法が定める義務

PSTI 法は、製造業者に対して、次のような義務を課している。なお、PSTI 法は、輸入業者や流通業者にも、同様の義務を課している。

- 次に掲げる事項への対応義務
  - セキュリティ要件の充足
  - 適合性宣言書又はその要約の添付
  - コンプライアンス違反の可能性の調査
  - コンプライアンス違反の製品を英国の顧客が入手することを防ぐこと、及びコンプライアンス違反の是正
  - コンプライアンス違反調査、及び違反の記録を保持する義務
- 通知義務
  - 当局へのコンプライアンス違反の通知
  - 当該製品の他の製造業者へのコンプライアンス違反の通知
  - 当該製品を供給した輸入業者又は流通業者へのコンプライアンス違反の通知
  - （一定の場合）当該製品を供給した顧客へのコンプライアンス違反の通知

（５）罰則

PSTI 法に違反した場合の罰則としては、①製品安全基準局（Office for Product Safety and Standards、以下、本項において「OPSS」という。）による販売停止及び/又はリコールの命令、②1,000 万ポンド又は全世界売上高の 4%のいずれか大きい額を上限とする罰金、③違反及びこれに対する執行措置の対外公表といったところが挙げられる。

（６）相互承認

2026 年 1 月より我が国のセキュリティ要件適合評価及びラベリング制度 JC-STAR との間で相互承認制度の運用が開始されている。本制度においては、JC-STAR★１適合ラベルと PSTI 法適合宣言書が相互承認の対象となっている。詳細は、独立行政法人情報処理推進機構（IPA)のウェブサイト（IPA「英国 PSTI 法適合の相互承認申請について」（最終更新日：令和 8 年 4 月 1 日））で確認できる。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

Q83-3 中国における主なサイバーセキュリティ法令

中国における主なサイバーセキュリティ関連法令としてどのようなものがあるか。その際に日本企業が留意すべきポイントとしてどのようなものがあげられるか。

タグ：中国個人情報保護法、データ安全法、ネットワーク安全法、民法典、ネットワーク安全審査規則、ネットワークデータ安全管理条例、国家ネットワークセキュリティインシデント報告管理弁法

１．概要

中国においては、ネットワーク安全法、中国個人情報保護法及びデータ安全法のいわゆるデータ三法が施行されている。このうち、サイバーセキュリティに関するものとしては、ネットワーク安全法及びデータ安全法が挙げられ、事業者に対する様々な義務を規定している。さらに、2022 年 2 月 15 日に施行された「ネットワーク安全審査規則」においても、所定の場合における安全審査義務が規定されている。

２．解説

（１）主要な法律

Q82 のとおり、中国においては、2017 年にネットワーク空間管理の基本法といえるネットワーク安全法（サイバーセキュリティ法）が、2021 年にはデータ安全法（データセキュリティ法）と中国個人情報保護法が施行され、これら三法を主要な法律として横断的にサイバーセキュリティの監督・管理を含むデータの保護を図っている（中国個人情報保護法については Q82 を参照されたい。）。

加えて、上記の三法の下位法令に位置づけられる、ネットワークデータ安全管理条例が 2025 年 1 月 1 日より施行され、ネットワークデータ及び重要データのセキュリティ管理等に関する要求事項を詳細化している。さらに、国家ネットワークセキュリティインシデント報告管理弁法が 2025 年 11 月 1 日に施行され、サイバーセキュリティインシデント発生時の対応を定めている（これらに関してはいずれも Q82 を参照されたい。）。

（２）ネットワーク安全法（サイバーセキュリティ法）

ア　ネットワーク運営者の義務

Q82 で詳説したとおり、ネットワーク安全法の適用対象は、「ネットワーク運営者」（中国国内におけるネットワークの所有者、管理者及びネットワークサービス提供者。同法第 76 条第 1 項第 3 号）である。ネットワーク運営者は、サイバーセキュリティ等級別保護制度の要件に基づき安全保護義務を履行しなければならない（ネットワーク安全法第 21 条、ネットワークデータ安全管理条例第 9 条）。サイバーセキュリティインシデント緊急対応プランを制定し、インシデント発生時には直ちにそのプランを発動して

救済措置を講じるとともに、関連の主管部門に報告する義務を負う（ネットワーク安全法第 25 条､国家ネットワークセキュリティインシデント報告管理弁法第 4 条､第 8 条)。

イ　重要情報インフラ運営者の義務

ネットワーク安全法は、重要情報インフラ運営者に対して、ネットワーク運営者に対する義務に加えて厳格な義務を課す。ここにいう「重要情報インフラ」とは、2021 年 9 月 1 日に施行された「重要情報インフラ安全保護条例」第 2 項によれば、「公共通信および情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務、国防科学技術工業等の重要な業界及び分野、並びにその他一旦その機能が破壊され、喪失し、又はデータが漏えいすると国の安全、国の経済、人民の生活、公共の利益に重大な危害が及ぶおそれのある重要なネットワーク施設及び情報システム等」とされている。同条例によれば、重要情報インフラは、当局主管部門が認定のための規則を制定し、認定結果を通知することとされているが、現時点では未制定である。

重要情報インフラ運営者には、安全性・リスク要因について年 1 回以上の検査評価を行う義務や、データローカライゼーション規制（Q84 参照。）が課せられる。

（３）データ安全法（データセキュリティ法）

安全法は、中国国内で「データ取扱行為」を行う場合に適用される（同法第 2 条第 1 項)。「データ取扱行為」とは、データの収集、保存、使用、加工、伝達、提供、開示等をいう（同法第 3 条第 2 項)。また、「データ」については、一般データ、重要データ及び国家核心データという 3 つの類型分けがなされている。中国国内でデータ取扱行為を行う者は、「データ取扱者」として、データセキュリティに関する責任を負う。

域外適用については、中国国外で行われるデータ取扱行為によって中国の国家安全、公共利益又は公民、組織の合法的な権益を害した場合、民事責任又は刑事責任を追及され得る（同法第 2 条第 2 項、第 52 条)。

データ取扱者[23]に対する主な義務には、まず、データセキュリティ保護義務（データ安全保護義務）である。データ取扱者は、データセキュリティ体制整備（同法第 27 条第 1 項など）を行い、法令の規定に基づく「全過程のデータ安全管理制度」を確立・整備し、教育研修の実施を手配し、相応の技術措置等を取らなければならない（同法第 27 条)。

次に、データ取扱者は、データ取扱行為において、リスクモニタリングを強化し、安全上の欠陥、脆弱性等のリスクを発見した場合の対応や、インシデント発生時の処置（ユーザ及び関連主管部門への告知・報告も含む）を講じなければならない（同法第 29 条)。

[23] 「データ処理者」の定義はないが、「ネットワークデータ処理者」の定義を踏まえると、データ処理活動において処理目的及び処理方法を自ら決定する個人又は組織を指すものと考えられる。

重要データの取扱いにおいては、データ安全責任者・管理機構の明確化（同法第 27 条 2 項）や定期的なリスク評価の実施と関連主管部門への報告（同法第 30 条）といった義務が加わる。

（4）ネットワーク安全審査規則[24]

「ネットワーク安全審査規則」によれば、重要情報インフラ運営者によるネットワーク製品もしくはサービスの調達、又はネットワーク・プラットフォーム運営者によるデータ取扱行為が、国家の安全に影響を及ぼし得る場合には、重要情報インフラ運営者又はネットワーク・プラットフォーム運営者がネットワーク安全審査を行わなければならない（同規則第 2 条第 1 項）。

また、重要情報インフラ運営者は、ネットワーク製品又はサービスを調達する場合、当該製品又はサービスによる国家安全リスクを事前に自ら判断しなければならず、国家の安全に影響を及ぼし得るときには、ネットワーク安全審査弁公室に対しネットワーク安全審査を申告しなければならない（同規則第 5 条）。

さらに、100 万を超えるユーザの個人情報を保有するネットワーク・プラットフォーム運営者は、国外で上場する場合、ネットワーク安全審査弁公室に対し、ネットワーク安全審査を申告しなければならない（同規則第 7 条）。

３．参考資料（法令・ガイドラインなど）

本文中に記載のとおり

４．裁判例

特になし

[24] サイバーセキュリティ法第 35 条及びデータセキュリティ法第 24 条に定める安全審査制度に基づき制定された下位法令である。

Q84 データローカライゼーション規制の概要

データローカライゼーションとはどのような内容の規制なのか。また、データローカライゼーション規制の適用がある場合の法的留意点はいかなるものか。

タグ：データローカライゼーション、越境移転、ネットワーク安全法、中国個人情報保護法、重要データ、個人データ、重要情報インフラ運営者、ネットワーク運営者、ネットワークデータ安全管理条例、データ越境移転セキュリティ評価弁法、データ越境流動の促進及び規範規定

１．概要

データローカライゼーションとは、重要データや個人データなど一定のデータを国内で保管することを義務付ける法規制をいう。中国のネットワーク安全法、ベトナムサイバーセキュリティ法、ロシア連邦個人情報保護法などが、かかるデータローカライゼーション規制を有する。

データローカライゼーション規制の適用がある場合には、その具体的な規制内容に応じたコンプライアンス対応が求められる。例えば、中国のネットワーク安全法は、重要情報インフラ運営者に対し、中国国内において収集・生成する個人情報及び重要データについては、重要性の高い情報の国外流出を防止するという観点も踏まえ、中国国内において保管しなければならないとし、業務上の必要から、中国国外へと越境移転することが確実に必要である場合には、一定の要件に従ったセキュリティ評価を行わなければならないとする。このため、重要情報インフラ運営者は、中国国内へのデータセンター設置や、中国国外へのデータ移転に対してのセキュリティ評価プロセスの構築が必要になる。一方、一般のネットワーク運営者がかかる義務を履行する必要があるか否かについては、未だ法令により明確にされていないため、弁法[1]やガイドラインの制定動向に注目する必要がある。

日本では、データローカライゼーション規制は実施されていないが、医療情報のような一部の類型の情報や政府の情報システムの情報の保管場所について、ガイドライン等で要求事項があることに留意すべきである。

２．解説

（１）問題の所在

近年、サイバーセキュリティと法令の文脈において「データローカライゼーション」と称する規制が注目されているが、これはどのような内容の規制であり、また、データロー

[1] 法律の下位規則にあたる行政法規等を意味する。

カライゼーション規制の適用がある場合の法的留意点はいかなるものであるのかが問題となる。

（2）データローカライゼーション規制の概要

データローカライゼーション規制とは、重要データや個人データなど一定のデータを国内で保管することを義務付ける法規制をいう。2017 年 6 月 1 日施行の中華人民共和国網絡安全法（中華人民共和国サイバーセキュリティ法、以下、本項において「ネットワーク安全法」という。）が、かかるデータローカライゼーション規制を制定し、当該規制に関して国際的に広い関心を集めるきっかけとなった。その他にも、ベトナムサイバーセキュリティ法やロシア連邦個人情報保護法などが、かかるデータローカライゼーション規制を有する。データローカライゼーション規制の適用がある場合には、その具体的な規制内容に応じたコンプライアンス対応が求められる。

なお、EU の General Data Protection Regulation（EU 一般データ保護規則。以下、本項において「GDPR」という。）などにおいては、個人データの国外移転に当たって一定の条件を求めているが、個人データの国内保管そのものを義務付けるものではない。このような、いわゆる個人データの越境移転規制については、データローカライゼーション規制には含まないものとして整理する。

以下、中国のネットワーク安全法の内容を中心に、データローカライゼーション規制の概要と、同規制の適用がある場合の法的留意点を説明する。

（3）中国のネットワーク安全法とデータローカライゼーション規制

ア　適用範囲

ネットワーク安全法においては、第 37 条において、いわゆるデータローカライゼーション規制が規定されている。すなわち、重要情報インフラの運営者（重要インフラ運営者の定義については Q83-3 を参照。）は、中国国内での事業運営において収集及び発生した個人情報及び重要データを、中国国内で保存しなければならず、また業務の必要により中国国外に提供する必要がある場合には、国家インターネット情報部門が国務院の関係部門と共に制定した規則に従ってセキュリティ評価を行わなければならない（第 37 条）。

また、データローカライゼーションの対象となる「個人情報」とは、「電子又はその他の方式で記録した単独又はその他の情報と組み合わせて自然人（個人）の身分を識別することができる、自然人の氏名、生年月日、身分証番号、個人の生体認証情報、住所、電話番号等を含むがこれらに限らない各種情報をいう。」（第 76 条第 1 項第 5 号）とされ、また、「重要データ」とは、特定の分野、特定の集団、特定の区域における、又は一定の精度及び規模に達している、一旦改ざん、破壊、漏えい又は違法取得、違法利用等

がされると、国家安全、経済運行、社会安定、公共の健康と安全等を害する可能性のあるデータをいう（ネットワークデータ安全管理条例第 62 条第 4 号）。

なお、ネットワーク安全法の条文上は、重要情報インフラの運営者のみがデータローカライゼーション規制の義務主体とされるが、データ越境流動の促進及び規範規定（2024 年 3 月 22 日施行）及びデータ越境移転セキュリティ評価弁法（2022 年 9 月 1 日施行）において、かかる義務主体が、重要情報インフラの運営者だけではなく、「中国国外に重要データを提供するデータ処理者」に拡大されることとなった[2]。

イ　規制内容

ネットワーク安全法の条文上の規制内容は、上記アのとおり、中国国内での運営において収集及び発生した個人情報及び重要データを中国国内で保存すること、また、業務の必要により中国国外に提供する必要がある場合には国家インターネット情報部門が国務院の関係部門と共に制定した規則に従ってセキュリティ評価を行うことである。

そして、後者のセキュリティ評価については、実施すべき事項につきネットワーク安全法の条文からはその具体的内容が明らかではないが、前述の、ネットワーク安全法の義務主体を拡大しているデータ越境移転セキュリティ評価弁法及びデータ越境流動の促進及び規範規定において具体的内容が示されている。

データ越境移転セキュリティ評価弁法及びデータ越境流動の促進及び規範規定によれば、セキュリティ評価においては、主に以下のプロセスを実施する必要がある。

① データ処理者[3]自身が、セキュリティ評価を申請する前に、データの越境移転に係るリスク自己評価を実施し、データ越境移転リスク自己評価報告書を作成する。
② データ処理者は、自己評価報告書等の書類をもって省レベルのネットワーク情報部門に対してセキュリティ評価を申請し、同部門による審査を受ける。
③ ネットワーク情報部門が書類の受理審査及びセキュリティ評価を実施する。
④ ネットワーク情報部門が、受理通知を発出してから原則として 45 営業日以内にデータ処理者に対してセキュリティ評価の結果を通知する。
⑤ セキュリティ評価の有効期間は、セキュリティ評価に通過したという評価結果が発行された日から 3 年間であるため、セキュリティ評価の有効期間が満了する場合において、データ越境移転を継続する必要があり、かつセキュリティ評価の再申請が必要となる事由が発生していないときには、データ処理者は、有効期間満

[2] 重要情報インフラの運営者による中国国外への重要データ又は個人情報の提供に加え、重要情報インフラの運営者以外のデータ処理者が中国国外に重要データを提供する場合にも、ネットワーク情報部門にセキュリティ評価の申請を行わなければならないと規定されている（データ越境流動の促進及び規範規定第 7 条第 1 項第 2 号、データ越境移転セキュリティ評価弁法第 4 条第 1 項）。

[3] 「データ処理者」の定義はないが、「ネットワークデータ処理者」の定義を踏まえると、データ処理活動において処理目的及び処理方法を自ら決定する個人又は組織を指すものと考えられる。

了前の 60 営業日までにネットワーク情報部門に有効期間延長を申請しなければならない。同部門の承認を得た場合に限り、評価結果の有効期間は 3 年間延長される。

また、データ越境移転セキュリティ評価弁法では、データ処理者がデータの越境移転に係るリスク自己評価を実施する際に、重点的に評価すべき事項として、以下の事項が列挙されている（同法第 5 条）。

① データの越境移転及び中国国外の受領者によるデータの取扱いの目的、範囲、方法等の合法性、正当性、必要性
② 越境移転データの規模、範囲、種類、機微度、データの越境移転により中国の安全、公共の利益及び個人又は組織の合法的権益に及ぼされる可能性のあるリスク
③ 中国国外の受領者が承諾する責任義務、責任義務の履行に係る管理、技術措置、能力等がデータの越境移転に係るセキュリティを保障できるか否か
④ データの越境移転中及び移転後における改ざん、破壊、漏えい、紛失、移転又は違法取得、違法利用等のリスク、個人情報権益を保護するルートの円滑さ等
⑤ 中国国外の受領者と締結する予定の、データ越境移転に関する契約又はその他の法律文書においてデータセキュリティ保護責任義務が十分合意されているか否か
⑥ その他データ越境移転のセキュリティに影響を与える可能性のある事項

また、国家ネットワーク情報部門がセキュリティ評価を実施するにあたって重点的に評価すべき事項は、以下のとおりである（同法第 8 条）。

① データの越境移転の目的、範囲、方法等の適法性、正当性、必要性
② 中国国外の受領者の所在国又は地域におけるデータセキュリティ保護政策法規及びサイバーセキュリティ環境の越境移転したデータのセキュリティに対する影響、中国国外の受領者のデータ保護水準が中国の法令及び強制国家基準の定める要求に達しているか否か
③ 越境移転するデータの規模、範囲、種類、センシティブ性、データの越境移転中及び移転後に改ざん、破壊、漏えい、紛失、移転又は違法取得、違法利用等が生じるリスク
④ データセキュリティ及び個人情報権益保護への十分かつ有効な保障の有無
⑤ 中国国外の受領者と締結する予定の、データ越境移転に関する契約又はその他の法律文書においてデータセキュリティ保護責任義務が十分合意されているか否か
⑥ 中国の関係法令の遵守状況等
⑦ 国家ネットワーク情報部門が評価すべきと認めるその他の事項

なお、重要情報インフラの運営者又は重要データを越境移転するデータ処理者が、セキュリティ評価に関する規定に違反して、中国国外でデータを保存した場合又は中国国外にデータを提供した場合は、関連の主管部門が是正を命じ、警告を行い、違法所得を没収し、5 万元以上 50 万元以下の罰金を科すとともに、関連業務の一時停止、営業停

止、ウェブサイトの閉鎖、関連業務許可の取消し又は営業許可の取消しを命じることができる（ネットワーク安全法第 66 条、データ越境移転セキュリティ評価弁法第 18 条）。営業停止や関連業務・営業許可の取消しを含む罰則は、他の立法例にはあまり見られず、データ処理者にとっては重い法的負担となり得る。

（４）中国個人情報保護法とデータローカライゼーション規制

個人情報については、2021 年 8 月 20 日に公布され、同年 11 月 1 日から施行された中国個人情報保護法において、個人情報取扱者が個人情報を国外に移転させる場合には、①国家ネットワーク情報部門によるセキュリティ評価の実施、②国家ネットワーク情報部門の規定に基づいて専門機構が行う個人情報保護に係る認証の取得、又は③国家ネットワーク情報部門が制定する標準契約に従い国外の情報受領者との間で契約を締結し、双方の権利及び義務を約定すること、④法律、行政法規は国家ネットワーク情報部門が定めるその他の条件に該当することのいずれかを満たす必要があるとされており（中国個人情報保護法第 38 条）、法令の適用を受ける全ての事業者に対して越境移転規制が適用される。

その上で、データローカライゼーション規制としては、従前からネットワーク安全法に基づき当該規制の対象となっていた「重要情報インフラ」の運営者、また、これに加えてデータ越境流動の促進及び規範規定及びデータ越境移転セキュリティ評価弁法に基づき規制対象となった「中国国外に重要データを提供するデータ処理者」、すなわち、取扱う個人情報が国家ネットワーク情報部門の定める数量（年間で累計 100 万人以上の個人情報（センシティブ個人情報を除く）又は 1 万人以上のセンシティブ個人情報を提供する場合とされている[4]。）に達している個人情報取扱者は、中国国内において収集し、及び生成される個人情報を、中国国内で保存しなければならず、中国国外に提供する必要が確実にある場合は、国家ネットワーク情報部門が行うセキュリティ評価に合格しなければならない。

（５）その他の法令とデータローカライゼーション規制

中国以外では、例えば、ベトナム、ロシアなどにおいて、データローカライゼーション規制が存在する。また、韓国においても、詳細地図情報の国外持ち出しを禁止する法制度の存在により、Google Maps 等のサービスが韓国国内では他国同様に展開することができない。データローカライゼーション規制を設ける目的は国や分野により様々だが、①自国内の産業保護、②安全保障の確保、③法執行／犯罪捜査などの要素が複雑に関連していることが指摘されている。

[4] データ越境流動の促進及び規範規定第 7 条第 1 項第 2 号

他方で、広範なデータローカライゼーション規制の拡大は、国際的な電子商取引を拡大していく上での障壁として機能するため、正当な公共政策上の理由を有さない同種の規制を抑止するための国際協力体制の構築も進められてきている。

（６）（参考）日本の状況

日本では、データローカライゼーションに関する法規制はないが、一部の類型のガイドライン等において、情報の保管場所に関する要求事項があることに留意すべきである。

例えば、医療分野においては、「医療情報システムの安全管理に関するガイドライン第 6.0 版（企画管理編）」27~28 頁においては、医療機関等が、データセンター等の外部事業者に委託して情報を保存する場合の要求として、外部保存の委託先事業者の選定に当たっては、少なくとも、①医療情報等の安全管理に係る基本方針・取扱規程等の整備状況、②医療情報等の安全管理に係る実施体制の整備状況、③不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況、④実績等に基づく個人データ安全管理に関する信用度、⑤財務諸表等に基づく経営の健全性、⑥プライバシーマーク認定又は ISMS 認証の取得、⑦「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す認証等により、適切な外部保存に求められる技術及び運用管理能力の有無、⑧医療情報を保存する情報機器が設置されている場所（地域、国）、及び⑨委託先事業者に対する国外法の適用可能性について確認するべきとされており、また、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版」56 頁においても、同様に、「法令で定められた医療機関等に対する義務や行政手続の履行を確保するために、医療情報及び当該情報に係る医療情報システム等が国内法の執行の及ぶ範囲にあることを確実とすること」とされている。

また、国の行政機関、独立行政法人及び指定法人を対象に、サイバーセキュリティに関する対策基準の策定及び実施に際しての考え方等を解説等している「政府機関等の対策基準策定のためのガイドライン」（令和 7 年度版）においても、「委託業務で取り扱われる情報に対して国外の法令等が適用される場合があり、国内であれば不適切と判断されるアクセス等が行われる可能性があることに注意が必要である。」という記述（144 頁）がある。そして、外部サービスの利用に当たっては、適切な外部サービス提供者を選定することにより、「クラウドサービスに保存する情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることに伴うリスク」等を低減することが要求されている（172 頁）。

３．参考資料（法令・ガイドラインなど）

・ネットワーク安全法
・中国個人情報保護法

・ネットワークデータ安全管理条例
・データ越境流動の促進及び規範規定
・データ越境移転セキュリティ評価弁法
・医療情報システムの安全管理に関するガイドライン第 6.0 版
・医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版
・政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）

４．裁判例

特になし

Q85 国際捜査共助・協力に関する条約・協定

国際捜査共助・協力とは何か。どのような場合に使われ、どういった根拠／手続に基づき行われるのか。

タグ：証拠収集、外交ルート、サイバー犯罪条約、刑事共助条約（協定）、MLAT、ICPO、24 時間コンタクトポイント

１．概要

国境を越えて行われるサイバー犯罪については、外国に所在する証拠を収集するため、外国の捜査機関の協力を求める必要があるところ、日本国は、国際捜査共助・協力の枠組みを活用している。国際捜査共助には、①国際礼譲に基づき外交ルートでこれを実施する場合と、②多数国間又は二国間の条約（協定）に基づきこれを実施する場合がある。国際捜査協力の枠組みとしては、①ICPO ルート、②24 時間コンタクトポイントがある。証拠の収集以外の情報提供や交換については、国際捜査協力において実施している。

国際捜査共助のうち、①の外交ルートで実施する場合は、我が国は、要請国からの共助の要請において捜査の対象とされている犯罪（共助犯罪）に係る行為が要請を受けた国において行われたとした場合において、その行為が当該国の法令によれば罪に当たるものでないときには共助を実施することができないが（双罰性）、②の条約（協定）に基づいて国際捜査共助を実施する場合には、根拠となる条約（協定）において、双罰性が緩和されている場合がある。

２．解説

（１）国際捜査共助の概要

国境を越えて行われるサイバー犯罪については、外国に所在する証拠を収集するため、外国の捜査機関の協力を求める必要があるところ、日本国は、その枠組みとして国際捜査共助を活用している。国際捜査共助には、以下に述べるとおり、①国際礼譲に基づき外交ルートでこれを実施する場合と、②多数国間又は二国間の条約（協定）に基づきこれを実施する場合がある。

このうち、①の外交ルートで国際捜査共助を実施する場合は、要請国からの共助の要請において捜査の対象とされている犯罪（共助犯罪）に係る行為が要請を受けた国において行われたとした場合において、その行為が当該国の要請によれば罪に当たるものではな

いときには共助を実施することができず（双罰性）、また、政治犯罪については取扱うことができない[1]という原則がある。

日本の捜査機関が外国において直接捜査を行うことは、当該外国の国家主権を侵害することになるため原則として認められない。そこで、国際捜査共助を利用して外国から捜査資料や証拠等を収集することとなる。

ア　外交ルート

外交ルートは、警察や検察といった捜査機関から外務省を通じて相手国に対して捜査共助の実施を要請する方法である。外国に対する捜査共助の要請は、一国の中で他の主権の行使を認めることができないとする主権国家の在り方を前提に、他国がその刑罰権の行使のために必要とする措置をその国のために実施することにより、主権の衝突と他国の刑罰権の適正な行使の実現の要請との調和を図るためのものであり、国家を当事者とする国家間の行為であって、外交的な側面を有する問題であるから、日本の捜査機関から要請するのではなく、外交に関する事務を所管する外務大臣から行うこととなる。

外国から日本国に対して捜査共助の要請があった場合、日本国としては、国際捜査共助等に関する法律に従って対応することとなる。同法に基づき、共助に必要な証拠の収集に際し、検察官及び司法警察員が関係者に出頭を求めてこれを取り調べること、鑑定を嘱託すること、実況見分、通信履歴の電磁的記録の必要なものを特定してこれを消去しないように求めることができることに加え、必要があると認めるときは、裁判官による令状により差押え、捜索、検証を実施することができる。

外交ルートでは、日本国から外国に対して捜査共助を要請し、その承諾を得るまでに数か月の時間を要することが多いため、サイバー犯罪に関してはあまり有効な手段ではないとの指摘[2]もある。

イ　刑事共助条約（協定）

国際捜査共助は、国家間において条約等を締結している場合には、日本の中央当局から相手国の中央当局に対して直接、捜査共助要請を行うことが可能である。現在、日本

---

[1] 国際捜査共助等に関する法律（昭和 55 年法律第 69 号）は、外国からの要請による国際捜査共助の手続等について規定しており、同法第 2 条は、共助をすることができない場合を規定する。同条第 1 号は「共助犯罪が政治犯罪であるとき、又は共助の要請が政治犯罪について捜査する目的で行われたものと認められるとき」について、同条第 2 号は「条約に別段の定めがある場合を除き、共助犯罪に係る行為が日本国内において行われたとした場合において、その行為が日本国の法令によれば罪に当たるものでないとき」について、共助をすることができない旨を定めている。

[2] 中野目善則「サイバー犯罪の捜査と捜査権の及ぶ範囲―プライヴァシーの理解の在り方、法解釈の在り方、他国へアクセスの及ぶ範囲等の観点からの検討―」警察政策 22 巻 130 号（令和 2 年）133 頁。

は、米国、韓国、中国、香港、EU、ロシア、及びベトナムとの間で二国間刑事共助条約を、EU との間で刑事共助協定を締結している[3]。

例えば、日本が米国と締結している刑事共助条約[4]では、裁判官が請求された共助の実施に必要な令状を発することや、証言、供述、証拠となる書類、記録を取得する際、必要があれば強制措置を採ることができること等が規定されており、日本の捜査機関は外務省を経由することなく、上記アで述べた外交ルートと同じような内容の捜査共助を要請できる。

また、サイバー犯罪条約等の多数国間条約にも、日本の中央当局から相手国の中央当局に対して直接捜査共助要請を行うことを可能とする旨の規定を含むものがある。

ウ　国際捜査共助が活用された件数[5]

		H29 年	H30 年	R1 年	R2 年	R3 年	R4 年	R5 年
捜査共助等を要請した件数	検察庁の依頼によるもの	8	24	12	13	7	4	5
	警察等の依頼によるもの	110	156	186	169	199	208	332
捜査共助等の要請を受託した件数		54	94	64	81	113	70	88

（２）その他の国際捜査協力の概要

ア　ICPO ルート

日本国が ICPO（International Criminal Police Organization：国際刑事警察機構又はインターポールという。）から捜査協力の要請を受けた場合、国家公安委員会は、国際捜査共助等に関する法律第 18 条に基づいて対応することになる。同条第 2 項では、共助の制限を定めた同法第 2 条第 1 号・第 2 号が準用されており、ICPO ルートに

[3] 警察庁「治安に関係する国際約束の締結」（https://www.npa.go.jp/bureau/soumu/kokusai/yakusoku.html）

[4] 詳細は、外務省「刑事に関する共助に関する日本国とアメリカ合衆国との間の条約」（https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_3.html）を参照されたい。

[5] 法務省「第 2 編第 6 章第 3 節　捜査・司法に関する国際協力 1 捜査共助」「令和 6 年版犯罪白書－詐欺事犯者の実態と処遇－」2-6-3-1 表 捜査共助等件数の推移（https://hakusyo1.moj.go.jp/jp/71/nfm/n71_2_2_6_3_1.html）

おいても、前述の（1）国際捜査共助の概要の箇所で述べた双罰性及び政治犯罪でないことが要件となっている。

もっとも、ICPO ルートは本来的に証拠の収集を目的とするものではないと解されているため、ICPO からの捜査協力の要請に基づく措置として採り得るのは任意の措置に限られ、捜索・押収等の強制処分を行うことはできない。

なお、ICPO に関しては、IGCI（INTERPOL Global Complex for Innovation）等のサイバー犯罪捜査・対策に関するトレーニング施設を設置する等、加盟国のサイバー犯罪捜査の支援に特化した部局が設置されており、今後、ICPO を通じた国際捜査共助の展開が注目される。

イ　24 時間コンタクトポイント

24 時間コンタクトポイントは、平成 9 年（1997 年）12 月の G8 司法内務閣僚会合で策定された「ハイテク犯罪と闘うための原則と行動計画」等に基づき設置された。国際的なサイバー犯罪に対する適時・効果的な対応を確保するために、この分野に精通した職員からなるコンタクトポイントを通じて、迅速かつ信頼できる通信手段により連絡をとることを想定したものである。令和 2 年 10 月現在、88 の国及び地域に設置されている。日本国では、警察庁に 24 時間コンタクトポイントを設置し、国際的な対応を必要とする事件への対応の円滑化を図るとともに、二国間での情報交換を積極的に行うなど、サイバー犯罪の取り締まりに関する国際的な捜査協力を推進している。

3．参考資料（法令・ガイドラインなど）

・国際捜査共助等に関する法律
・刑事に関する共助に関する日本国とアメリカ合衆国との間の条約
・サイバー犯罪条約

令和 6 年版警察白書
https://www.npa.go.jp/hakusyo/r06/pdf/06_dai3sho.pdf
第 3 章第 2 節第 4 項「国際連携の推進」

4．裁判例

特になし

付録 サイバーセキュリティ法体系マッピング及び関連するQ一覧

以下の表の「関係法令の分類」及び「法令等の名称」は、令和7年度サイバーセキュリティ法曹懇談会において作成した「サイバーセキュリティ法体系マッピング」を引用したものであり、「関連する本ハンドブックのQ」は、各法令等に関係するQを位置づけたものである。

1. サイバーセキュリティ確保のための基本的な枠組み

関係法令の分類	法令等の名称	関連する本ハンドブックのQ
基本理念・基本方針の策定等	・サイバーセキュリティ基本法 ・サイバー対処能力強化法 ・デジタル社会形成基本法 ・AI法	Q1 サイバーセキュリティの定義 Q2 サイバーセキュリティ基本法の概要と政府機関等のサイバーセキュリティ Q3 能動的サイバー防御に関する法律 Q4 地方公共団体のサイバーセキュリティ

2. 公的部門を対象とした法制度

(1) サイバーセキュリティ確保を促進する制度

関係法令の分類	法令等の名称	関連する本ハンドブックのQ
サイバーセキュリティ確保の要求	・政府機関等のサイバーセキュリティ対策のための統一基準群(令和7年度版) ・地方自治法 ・地方公共団体における情報セキュリティポリシーに関するガイドライン	Q1 サイバーセキュリティの定義 Q2 サイバーセキュリティ基本法の概要と政府機関等のサイバーセキュリティ Q3 能動的サイバー防御に関する法律 Q4 地方公共団体のサイバーセキュリティ
民間部門に対する支援施策	・サイバーセキュリティ基本法	
官民連携・国際協力の促進	・サイバー対処能力強化法	

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
公的部門によるサイバーセキュリティ対策強化・確保	・情報処理の促進に関する法律【IPA】 ・国立研究開発法人情報通信研究機構法【NICT】 ・電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律【J-LIS】	Q9 サイバーセキュリティに関する規格等と NIST SP800 シリーズ Q10 情報処理安全確保支援士 Q11 技術情報管理認証制度について Q12 DX 認定・DX 銘柄とサイバーセキュリティ

(2) 情報・データ等の保護を求める制度

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
個人情報の保護	・個人情報保護法 ・マイナンバー法	Q13 個情法の安全管理措置義務とサイバーセキュリティの関係 Q14 個人データの取扱いの委託と安全管理 Q15 クラウドサービスの活用と個情法 Q16 官民における個人情報に関する安全管理措置の相違 Q17 個人データの加工と法令上の安全管理 Q18 クレジットカード情報の取扱い Q19 労働者の心身の状態に関する情報の取扱い Q20 マイナンバーの取扱い Q82 海外における主な個人データ保護関係法令
情報全般の保護	・不正競争防止法【営業秘密等】	Q21 営業秘密の要件 Q22 限定提供データとサイバーセキュリティ Q23 技術的手段の回避行為・無効化行為の法的責任 Q24 データの知的財産権法規定による保護方法

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
		Q25 ソフトウェアのリバースエンジニアリング
	・特定秘密の保護に関する法律 ・重要経済安保情報の保護及び活用に関する法律	Q54 サイバーセキュリティと輸出管理 Q55 サイバーセキュリティ事業者への投資 Q56 経済安全保障（経済安保推進法、セキュリティ・クリアランス）
公文書に関する制度	・公文書管理法 ・情報公開法	―

(3) DX 推進のための制度

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
DX推進等	・デジタル手続法 ・AI 法	Q43 AI のサイバーセキュリティ

3. 民間部門を対象とした法制度

(1) サイバーセキュリティ確保を促進する制度

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
サイバーセキュリティ確保の要求	・産業競争力強化法【技術情報管理認証制度】	Q11 技術情報管理認証制度について
	・5G 促進法【開発供給計画・導入計画におけるサイバーセキュリティ確保】	Q41 5G 促進法とサイバーセキュリティ
	・重要インフラのサイバーセキュリティに係る	Q45 重要インフラ分野における規律

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
	行動計画【安全基準等、情報連絡等】 ・重要インフラのサイバーセキュリティ確保に係る安全基準等策定指針	
	・経済安保推進法【特定重要設備の導入計画書に係るリスク管理措置】	Q56 経済安全保障（経済安保推進法、セキュリティ・クリアランス）
	・サイバー対処能力強化法【特定重要電子計算機の届出、インシデント報告等】 ・サイバーセキュリティ経営ガイドライン Ver3.0 ・中小企業の情報セキュリティ対策ガイドライン ・個人情報保護法【安全管理措置、インシデント報告等】	Q57 インシデント発生時の当局等対応 Q58 インシデントレスポンスと関係者への対応 Q59 デジタル・フォレンジック Q60 ランサムウェア対応 Q61 サイバー攻撃による情報喪失 Q62 電子メールの誤送信 Q63 データ漏えい時の損害賠償額の算定 Q64 データを紛失・消失した場合における損害額 Q65 インシデント対応における費用負担及びサイバー保険 Q66 デジタルデータの証拠利用について Q70 サイバーセキュリティと情報共有・公表 Q71 脅威インテリジェンスサービス Q72 脆弱性情報の取扱いについて
	不正競争防止法	Q67 営業秘密等の漏えい事実（情報管理体制含む）及び不正使用行為の立証 Q68 ドメイン名の不正使用への対抗措置
	情報流通プラットフォーム対処法	Q69 発信者情報開示
	海外関係法令	Q83-1 米国における主なサイバーセキュリティ法令

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
		Q83-2 EU・英国における主なサイバーセキュリティ法令 Q83-3 中国における主なサイバーセキュリティ法令 Q84 データローカライゼーション規制の概要
サイバーセキュリティ確保を含み得る一般的な制度	・会社法【内部統制システム構築義務、内部監査等】 ・金融商品取引法【内部統制報告書】	＜会社法・情報開示関連＞ Q5 内部統制システムとサイバーセキュリティとの関係 Q6 サイバーセキュリティと取締役等の責任 Q7 サイバーセキュリティ体制の適切性を担保するための監査等 Q8 サイバーセキュリティと情報開示
	・労働基準法、労働契約法、労働者派遣法、労働安全衛生法、職業安定法その他の労働関係法令【守秘義務等】	Q28 セキュリティ上必要となる雇用関係上の措置と誓約書の取得 Q29 従業員のモニタリングに関する留意点 Q30 業務用端末の私的利用・私物端末の業務利用等に関する諸問題 Q31 テレワークにおけるセキュリティ Q32 派遣労働者及び特定受託事業者に対するセキュリティに関する義務付け Q33 退職後の競業避止義務と違反時の退職金減額・不支給及び情報漏えい防止のための秘密保持契約 Q34 退職後の海外での秘密保持義務違反行為について

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
製品・サービス等の安全を求める制度（ネットワーク製品や IoT 機器、生成 AI、クラウドサービス）	・セキュリティ要件適合評価及びラベリング制度（JC-STAR） ・AI 事業者ガイドライン（第 1.2 版） ・クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版） ・クラウドサービス利用・提供における適切な設定のためのガイドライン	Q35 IoT 機器のセキュリティに関する法的対策 Q36 IoT 製品のセキュリティ適合性に関する認証制度（JC－STAR） Q37 IoT 機器からのデータ漏えいにおける製造者の責任 Q38 ドローンとサイバーセキュリティ Q39 モビリティとサイバーセキュリティ Q40 スマホソフトウェア競争促進法 Q41 5G 促進法とサイバーセキュリティ Q42 クラウドサービスとサイバーセキュリティ Q43 AI のサイバーセキュリティ Q44 Web サービスにおける認証/本人確認に関するサイバーセキュリティ
業界特有の制度（通信分野、医療分野、金融分野）	・電気通信事業法 ・電気通信事業における個人情報等の保護に関するガイドライン	Q46 電気通信事業分野における規律（電気通信事業法に基づく登録・届出） Q47 電気通信事業分野における規律（電気通信事業者に関する規律の概要）
	・医療法施行規則 ・医療情報システムの安全管理に関するガイドライン 第 6.0 版 ・医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版 ・医薬品、医療機器等の品質、有効性及び安全性の確保等に	Q48 医療分野におけるサイバーセキュリティ

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
	関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準	
	・金融庁監督指針 ・金融分野におけるサイバーセキュリティに関するガイドライン ・金融分野における個人情報保護に関するガイドライン ・信用分野における個人情報保護に関するガイドライン ・割賦販売法【クレジットカード番号等の適切な管理】	Q49 金融分野におけるサイバーセキュリティ

(2) 情報・データ等の保護を求める制度

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
個人情報の保護	・個人情報保護法【安全管理措置、インシデント報告】 ・マイナンバー法	Q13 個情法の安全管理措置義務とサイバーセキュリティの関係 Q14 個人データの取扱いの委託と安全管理 Q15 クラウドサービスの活用と個情法 Q16 官民における個人情報に関する安全管理措置の相違 Q17 個人データの加工と法令上の安全管理 Q18 クレジットカード情報の取扱い Q19 労働者の心身の状態に関する情報の取扱い

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
		Q20 マイナンバーの取扱い Q82 海外における主な個人データ保護関係法令
情報全般の保護	・不正競争防止法【営業秘密等】 ・特許法 ・著作権法	Q21 営業秘密の要件 Q22 限定提供データとサイバーセキュリティ Q23 技術的手段の回避行為・無効化行為の法的責任 Q24 データの知的財産権法規定による保護方法 Q25 ソフトウェアのリバースエンジニアリング Q26 暗号の利用と情報管理等 Q27 データの消去、データが記録された機器・電子媒体の廃棄

(3) 企業取引等のルール策定

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
電子契約、電子署名、データ取引、本人確認等	・民法 ・民事訴訟法 ・電子署名及び認証業務に関する法律 ・e-文書法 ・電子帳簿保存法 ・犯罪による収益の移転防止に関する法律 ・出会い系サイト規制法 ・古物営業法 ・携帯電話不正利用防止法	Q50 電子契約と電子署名法 Q51 データ取引に関する契約におけるサイバーセキュリティ関連法令上のポイント Q52 データ漏えいに関するシステム開発ベンダの責任とモデル契約 Q53 サプライチェーン・リスク対策
輸出入、クロスボーダー取引等	・外国為替及び外国貿易法【輸出管理】 ・法の適用に関する通則法	Q54 サイバーセキュリティと輸出管理 Q55 サイバーセキュリティ事業者への投資

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
ステークホルダー（投資家等）の保護	・会社法【事業報告】 ・金融商品取引法【重要情報の開示義務】	Q5 内部統制システムとサイバーセキュリティとの関係 Q6 サイバーセキュリティと取締役等の責任 Q7 サイバーセキュリティ体制の適切性を担保するための監査等 Q8 サイバーセキュリティと情報開示

(4) 利用者等を保護するための制度

関係法令の分類	法令等の名称	関連する本ハンドブックの Q
利用者保護	・製造物責任法 ・消費生活用製品安全法 ・サイバーインフラ事業者に求められる役割等に関するガイドライン	Q37 IoT 機器からのデータ漏えいにおける製造者の責任
消費者保護・青少年保護	・消費者契約法 ・電子消費者契約法 ・特定商取引法 ・青少年インターネット環境整備法	Q61 サイバー攻撃による情報喪失
公正な競争の確保	・私的独占の禁止及び公正取引の確保に関する法律 ・下請代金支払遅延等防止法 ・スマホソフトウェア競争促進法	＜製品・サービス等のセキュリティ保護＞ Q40 スマホソフトウェア競争促進法 ＜契約関連（電子署名・システム開発等）＞ Q53 サプライチェーン・リスク対策

4. サイバー犯罪の防止

関係法令の分類		法令等の名称	関連する本ハンドブックの Q
サイバー犯罪に関する実体法	情報システムへの攻撃の禁止	・不正アクセス行為の禁止等に関する法律	Q73 不正プログラムと刑事罰

関係法令の分類		法令等の名称	関連する本ハンドブックの Q
		・刑法（不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪、器物損壊罪、業務妨害罪）	Q74 電磁的記録不正作出罪 Q75 電子計算機使用詐欺罪 Q76 スキミング Q77 情報の不正入手・漏えい Q78 不正アクセス Q79 フィッシング Q80 フェイクニュース対策
	サイバースペースでの犯罪行為の禁止	・著作権法 ・不正競争防止法 ・個人情報保護法（個人情報データベース等不正提供罪）	
サイバー犯罪に関する手続法	サイバー犯罪捜査の手続	・刑事訴訟法 ・通信傍受法	Q81 越境リモートアクセス
	国際的な捜査協力と法執行	・国際捜査共助等に関する法律	

関係者一覧（全て敬称略）

【Ver.3.0】（2026 年 10 月時点）

◇サイバーセキュリティ法曹懇談会

主　査	岡村　久道	国立情報学研究所客員教授・英知法律事務所弁護士
副主査	大谷　和子	株式会社日本総合研究所アドバイザー
副主査	湯淺　墾道	明治大学公共政策大学院ガバナンス研究科長
委　員	大杉　謙一	中央大学大学院法務研究科教授
委　員	奥邨　弘司	慶應義塾大学大学院法務研究科教授
委　員	小向　太郎	中央大学国際情報学部教授
委　員	星　周一郎	東京都立大学法学部教授
委　員	丸山　満彦	PwC コンサルティング合同会社パートナー
委　員	横田　明美	明治大学法学部専任教授

事務局

内閣官房国家サイバー統括室

TMI 総合法律事務所

寺門峻佑弁護士、臼倉尭史弁護士、岡部公志弁護士、田山翔弁護士、森田祐行弁護士、川上貴寛弁護士、杉浦翔太弁護士、柿山佑人弁護士、川口大喜弁護士、林知宏弁護士、澤中きらら弁護士、刀祢館菜摘弁護士、芥川詩門弁護士、金井秀隆弁護士、榊原颯子弁護士、林里奈弁護士、篠原峻弁護士、鈴木基浩弁護士、芹澤杏子弁護士、飛田紘佑弁護士、橋本大智弁護士、牧昂平弁護士、宮下大樹弁護士、飯田浩貴弁護士、井上智喜弁護士、岩渕芳人弁護士、梅本翔太弁護士、梶原大暉弁護士、梶原尚樹弁護士、滝川航生弁護士、坪広大弁護士、渡辺智裕弁護士、須田真綺弁護士、浅水菜穂子弁護士、田貝真紀弁護士、Maria Gonçalves 弁護士（以下「TMI チーム」という。）

◇サイバーセキュリティ関係法令 Q&A ハンドブックタスクフォース

構成員	寺門　峻佑	TMI 総合法律事務所弁護士
構成員	安藤　広人	ファイ法律事務所弁護士
構成員	有本　真由	アレシア国際法律事務所弁護士
構成員	蔦　　大輔	森・濱田松本法律事務所弁護士

構成員	早川　健	長島・大野・常松法律事務所弁護士
構成員	日置　巴美	長島・大野・常松法律事務所弁護士
構成員	北條　孝佳	西村あさひ法律事務所弁護士
構成員	水町　雅子	宮内・水町 IT 法律事務所弁護士
構成員	山岡　裕明	八雲法律事務所弁護士
構成員	渡邊　涼介	光和総合法律事務所弁護士

事務局

内閣官房国家サイバー統括室

TMI チーム

◇ヒアリング等協力（五十音順・敬称略）

※所属等はヒアリング当時

○　一般社団法人金融 ISAC

谷合　通宏

○　一般財団法人安全保障貿易情報センター（CISTEC）及び賛助会員

池田　誠一　　池田　伸生　　上田　広之　　田川　卓司　　徳山　弘毅

桃井　元士

○　特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）

片倉　悠暉　　倉持　浩明　　田原　祐介　　永野　憲次郎　　三国　貴正

○　一般社団法人 ICT-ISAC

石田　慶樹　　木内　直人　　近藤　和弘　　水越　一郎

○　独立行政法人情報処理推進機構（IPA）セキュリティセンター

小野塚　直人　　神田　雅透　　小山　明美　　佐藤　栄城　　高橋　将

中島　尚樹

○　公益社団法人日本医師会

長島　公之

【Ver.2.0】（2023 年 9 月時点）

◇サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ（第 2 期）

主　査	岡村　久道	国立情報学研究所客員教授・英知法律事務所弁護士
副主査	大谷　和子	株式会社日本総合研究所執行役員法務部長
委　員	大杉　謙一	中央大学大学院法務研究科教授
委　員	奥邨　弘司	慶應義塾大学大学院法務研究科教授
委　員	小向　太郎	中央大学国際情報学部教授
委　員	星　周一郎	東京都立大学法学部教授
委　員	丸山　満彦	PwC コンサルティング合同会社パートナー
委　員	宮川　美津子	TMI 総合法律事務所パートナー弁護士
委　員	湯淺　墾道	明治大学公共政策大学院ガバナンス研究科教授

オブザーバー

警察庁、個人情報保護委員会事務局、金融庁、デジタル庁、総務省、法務省、文化庁、厚生労働省、経済産業省

事務局

内閣官房内閣サイバーセキュリティセンター　基本戦略第２グループ

◇サイバーセキュリティ関係法令検討会　（ドラフトの検討）
※サイバーセキュリティ関係法令に関する調査研究受託事業として実施

主　査	蔦　　大輔	森・濱田松本法律事務所弁護士
構成員	阿久津匡美	弁護士法人内田・鮫島法律事務所弁護士
構成員	安藤　広人	ファイ法律事務所弁護士
構成員	寺門　峻佑	TMI 総合法律事務所弁護士
構成員	日置　巴美	三浦法律事務所弁護士
構成員	北條　孝佳	西村あさひ法律事務所弁護士
構成員	水町　雅子	宮内・水町 IT 法律事務所弁護士
構成員	山岡　裕明	八雲法律事務所弁護士
構成員	渡邊　涼介	光和総合法律事務所弁護士

オブザーバー
内閣官房内閣サイバーセキュリティセンター基本戦略第 2 グループ

検討会事務局
森・濱田松本法律事務所
林浩美弁護士、湯川昌紀弁護士、蔦大輔弁護士、清水池徹弁護士、嶋村直登弁護士、小川智史弁護士、大段徹次弁護士、本嶋孔太郎弁護士、塩崎耕平弁護士、城戸賢仁弁護士

◇ヒアリング等協力（五十音順・敬称略）
○　一般社団法人金融 ISAC
坊野　良英
○　一般社団法人 JPCERT コーディネーションセンター
佐々木　勇人　　真鍋　敬士
○　一般社団法人日本自動車工業会（JAMA）
青山　昌寛　　川名　茂之
○　一般社団法人日本損害保険協会
井川　文作　　教学　大介　　菅原　英美　　水谷　優里　　宮寺　翼
○　株式会社東京証券取引所
須賀　裕哉　　野村　旭　　門田　耕一郎
○　一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会（NCA）
法制度研究 WG
池田　香苗　　鳥越　真理子　　萩原　健太　　林　基樹

【Ver.1.0】（2020 年 3 月 2 日時点）

◇サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ

主　査	林　紘一郎	情報セキュリティ大学院大学　名誉教授
副主査	岡村　久道	英知法律事務所　弁護士
		京都大学大学院　医学研究科　講師
委　員	大杉　謙一	中央大学大学院　法務研究科　教授
委　員	大谷　和子	株式会社日本総合研究所　法務部長
委　員	奥邨　弘司	慶應義塾大学大学院　法務研究科　教授
委　員	小向　太郎	日本大学　危機管理学部　教授
委　員	星　周一郎	首都大学東京　法学部　教授
委　員	丸山　満彦	デロイト トーマツ サイバー合同会社　執行役員
委　員	宮川　美津子	ＴＭＩ総合法律事務所　弁護士
委　員	湯淺　墾道	情報セキュリティ大学院大学　教授

オブザーバー

警察庁、個人情報保護委員会事務局、総務省、法務省、厚生労働省、経済産業省

◇サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ
タスクフォース　（ドラフト起草担当）

構成員	阿久津　匡美	弁護士法人北浜法律事務所東京事務所　弁護士
構成員	安藤　広人	ファイ法律事務所　弁護士
構成員	寺門　峻佑	ＴＭＩ総合法律事務所　弁護士
構成員	日置　巴美	三浦法律事務所　弁護士
構成員	北條　孝佳	西村あさひ法律事務所　弁護士
構成員	水町　雅子	宮内・水町ＩＴ法律事務所　弁護士
構成員	山岡　裕明	八雲法律事務所　弁護士
構成員	渡邊　涼介	光和総合法律事務所　弁護士
オブザーバー	大谷　和子	株式会社日本総合研究所　法務部長
事務局（編著担当）	蔦　大輔	内閣官房内閣サイバーセキュリティセンター 上席サイバーセキュリティ分析官

◇ヒアリング等協力（五十音順・敬称略）

○ 一般財団法人安全保障貿易情報センター（CISTEC）
池田　伸生　　青木　眞夫[i]　加藤　智也　　佐藤　朋司　　千葉　晴夫
村井　則彦　　山田　尚文

○ 一般社団法人日本クラウドセキュリティアライアンス（CSA）
渥美　俊英　　高橋　郁夫　　成田　和弘　　諸角　昌宏

○ 一般社団法人日本内部監査協会
南部　芳子　　吉武　一

○ S&K Brussels 法律事務所
杉本　武重

○ 国立情報学研究所（NII）
佐藤　一郎　　高橋　克巳

○ システム監査学会（JSSA）
石島　隆

○ 特定非営利活動法人デジタル・フォレンジック研究会（IDF）
安冨　潔

○ 特定非営利活動法人日本セキュリティ監査協会（JASA）
永宮　直史

○ 独立行政法人日本貿易振興機構（JETRO）
島田　英樹　　長﨑　勇太

○ 日本シーサート協議会（NCA）法制度研究 WG
池田　香苗　　萩原　健太　　林　基樹

◇事務局

内閣官房内閣サイバーセキュリティセンター
基本戦略第１グループ・基本戦略第２グループ

[i] 独立行政法人情報処理推進機構（IPA）J-CRAT/サイバーレスキュー隊から協力