サイバーセキュリティ関係法令 Q&A
ハンドブック

Ver1.0

令和２年３月２日

内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）

「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「〇〇六法」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

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うえで、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。

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。

---

[1] 平成 21 年 6 月にまとめた後に検討を行った平成 23 年 4 月版のものも参考として公開されている。

目次

総説

１．サイバーセキュリティと法制度

（１）サイバーセキュリティ基本法の制定前の状況について

サイバーセキュリティという概念は、法制度の領域から生成・発展した概念ではなく、サイバーセキュリティ基本法が制定されるまでは、わが国の法令において「セキュリティ」という単語を用いたものはなかった。ただ、平成 12 年に制定された IT 基本法第 22 条における「高度情報通信ネットワークの安全性及び信頼性」という文言の中に、情報セキュリティを読み取ることが可能であった。

情報セキュリティとは、一般に「情報の機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability）の 3 要素を維持すること」ということができ、この 3 要素の各々の頭文字を取って「情報の CIA」ということもある。

機密性とは、情報に関して正当な権限を持った者だけが、情報にアクセスできることをいう。機密性が損なわれた場合の典型例として不正アクセス等が挙げられる。

完全性とは、情報に関して破壊、改ざん又は消去されていないことをいう。完全性が損なわれた場合の典型例として情報の不正改ざん等が挙げられる。

可用性とは、情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできることをいう。可用性が損なわれた場合の典型例としてシステム障害による利用不能等が挙げられる。

このような CIA の概念を用いたものとしては、1992 年に経済協力開発機構（OECD[1]）が採択した「情報システムセキュリティガイドライン（Guidelines for the Security of Information Systems）」（以下「1992 年ガイドライン」という。）が挙げられる。同ガイドラインにおいては、情報セキュリティの目的について、「情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護すること」と定義している[2]。

これを踏まえ、情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO/IEC 27001:2005・同 27002:2005、これを日本工業規格化した JIS Q 27001: 2006・同 27002:2006 にも情報セキュリティに関する同様の定義が置かれている[3]。

---

[1] Organisation for Economic Co-operation and Development

[2] なお、1992 年ガイドラインは、2002 年に採択された「情報システム及びネットワークのセキュリティのためのガイドライン : セキュリティ文化の普及に向けて（Gudelines for the Security of Information Systems and Networks :Towards a Culture of Security）」によって改訂された。タイトルのとおり、情報システムのみならずネットワークにも重点が置かれている。また、同ガイドラインは、2015 年の理事会勧告「Degital Security Risk Management for Economic and Social Prosperity」によって改訂された。タイトルのとおり、リスクベースアプローチに重点が置かれている。

[3] ISO/IEC 27001 及び 27002 は、ISO/IEC 27001:2013（JIS Q 27001:2014）及び、ISO/IEC 27002:2013（JIS Q 27002:2014）に改訂されている。

（２）サイバーセキュリティ基本法

平成 26 年にサイバーセキュリティ基本法が制定された。具体的な内容については後述するが、情報、情報システム、情報通信ネットワークという 3 つの客体に着目して「サイバーセキュリティ」が定義されていることをはじめ、わが国のサイバーセキュリティ政策を推進するための様々な規定が置かれた基本法としての役割を有している。

ただし、同法は基本的に民間の企業等に対する具体的な権利・義務等を定めるものではなく、また、同法は、IT 基本法と相まって、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）であるが、現状において、これらの法律も含め、サイバーセキュリティに関して民間の企業等に対する権利・義務等を通則的に適用する法令が存在しているものではない。

一方で、個別の法令においては、サイバーセキュリティに関わる規定が存在しており、特に情報の安全管理に関する規定を置く法令が増加する傾向にある。本書においては、個別に存在するサイバーセキュリティに関する法令について解説を加えていく。

（３）サイバーセキュリティ対策と法令・ガイドライン

サイバー攻撃が複雑化・巧妙化する今日において、各々の企業がサイバーセキュリティ対策をとることの重要性は増加している。各々の企業は、企業の規模や業態、時代背景、取り扱う情報の種類と適用される法令等に基づき、必要なサイバーセキュリティ対策をとることとなる。

サイバーセキュリティに関しては、関係する法令を遵守する必要があることはもちろん、その他、国内外を問わず、様々な政府機関、民間の団体や企業等による様々なガイドライン等が発出されている。また、前述のとおり関係する国際規格も存在する。これらも参考にしながら各々の企業において必要とされる具体的なサイバーセキュリティ対策を行うことが望ましい。

２．本書で取り上げる主な法律について

○　**サイバーセキュリティ基本法**（平成 26 年法律第 104 号）

「サイバーセキュリティ」の定義を置くとともに、基本法として、わが国のサイバーセキュリティ政策を推進するための様々な規定を定めている。

○　**民法**（明治 29 年法律第 89 号）

契約に関する規律や、不法行為に基づく損害賠償請求等を規定している。

○　**会社法**（平成 17 年法律第 86 号）

取締役に対し、サイバーセキュリティを確保するための体制を含む内部統制システム構築義務を課している。

○　**個人情報の保護に関する法律**（平成 15 年法律第 57 号）

個人情報の取扱いに関する基本法と個人情報取扱事業者に対する義務等を定める。当該義務の中に個人データの安全管理措置義務が含まれる。また、個人番号を含む個人情報（特定個人情報）については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）が規律を定めている。

○　**不正競争防止法**（平成 5 年法律第 47 号）

不正競争の防止を目的の一つとしており、営業秘密や限定提供データの保護や、技術的制限手段の無効化、回避の禁止等を定める。

○　**著作権法**（昭和 45 年法律第 48 号）

プログラムを含む著作物の保護と複製権をはじめとする著作権等について規定している。

○　**労働基準法**（昭和 22 年法律第 49 号）

労働基準を定める法律であり、企業の就業規則に関する規定などを置いている。その他、労働契約に関する基本的な事項を定める労働契約法（平成 19 年法律第 128 号）等がある。

○　**電気通信事業法**（昭和 59 年法律第 86 号）

サイバー空間における活動の基盤となるインターネットサービス等の電気通信事業に関する諸規定や、通信の秘密等を規定している。

○　**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）

一定の条件を満たす電子署名を手書き署名や押印と同等に通用する旨等を規定している。

○　**情報処理の促進に関する法律**（昭和 45 年法律第 90 号）

情報処理安全確保支援士に関する規定や、独立行政法人情報処理推進機構（IPA）の業務としてサイバーセキュリティに関する講習や調査等を措置している。

○　**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）

国立研究開発法人情報通信研究機構（NICT）の業務を定めるとともに、時限的な業務として IoT 機器の調査を行う「NOTICE」に関する規定を措置している。

○　**刑法**（明治 40 年法律第 45 号）

不正指令電磁的記録に関する罪（いわゆるウィルス罪）をはじめとするサイバー犯罪を処罰する規定を含む刑罰が規定されている。

○　**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）

不正ログインといった不正アクセス行為や、いわゆるフィッシング行為を処罰する旨が規定されている。

３．本書の構成について

Q1,2 は、サイバーセキュリティに関する基本法として、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」の定義及び同法の概要を解説するものである。

Q3~Q6 は、会社法を中心に、経営体制の観点から取締役が負う義務（内部統制システム構築義務）や、当該体制が適切であることを担保するための監査や情報開示について解説するものである。

Q7~Q16 は、個人情報の保護に関する法律等を中心に、個人データの安全管理措置を軸として様々な論点を解説するとともに、クレジットカード情報、労働者の心身の状態に関する情報、マイナンバーについて解説を加えるものである。

Q17~Q22 は、不正競争防止法を中心に、営業秘密の保護、限定提供データ、技術的手段の回避行為・無効か行為に関する解説を行い、その他知的財産法について補足を加えるものである。

Q23～35 は、労働関係法令を中心に、企業においてサイバーセキュリティ対策を行うにあたっての組織的対策・人的対策について解説するものである。

Q36~Q38 は、サイバー空間を支える情報通信ネットワークの関係で、電気通信事業者に対する規律や、IoT 機器に関する法的論点について解説するものである。

Q39~Q43 は、契約を軸としつつ、電子署名、データ取引、システム開発、クラウドサービス、サプライチェーンなど、サイバーセキュリティに関わる様々な論点について解説するものである。

Q44,Q45 は、サイバーセキュリティに関する資格等を対外的に示す法的な仕組み（情報処理安全確保支援士、技術等情報の適切な管理に係る認証）を解説するものである。

Q46~Q49 は、上記に分類しづらいサイバーセキュリティに関わる各論を解説するものである（リバースエンジニアリング、暗号、輸出管理、情報共有）。

Q50~Q58 は、サイバーセキュリティに関するインシデントが発生した場合の事後的な対応等（デジタル・フォレンジック等を含む）について解説するものである。

Q59~Q64 は、サイバーセキュリティに関する紛争が民事訴訟となった場合に留意すべき手続等について解説するものである。

Q65~Q71 は、サイバーセキュリティに関係する刑事実体法について解説するものである。

Q72,Q73 は、わが国の事業者がサイバーセキュリティ対策を行う上で留意すべき主な海外法令について簡単な解説を加えたものである。

凡例・略称

- 本書は、令和 2 年 2 月 26 日時点の法令等を基準としている。
- 引用している URL の最終アクセス日は令和 2 年 2 月 26 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：平成 30 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以下による。
- 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）
IT 基本法	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）
プロバイダ責任制限法	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（平成 13 年法律第 137 号）
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）
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）
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）

【関係文書の略称】

略称	正式名称
サイバーセキュリティ 2019	サイバーセキュリティ戦略本部「サイバーセキュリティ 2019（2018 年度報告・2019 年度計画）」（令和元年 5 月）

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、平成 31 年 1 月一部改正）
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」及び「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」に関するＱ＆Ａ」（平成 29 年 2 月 16 日、令和元年 11 月 12 日更新）
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 Ver2.0」（平成 29 年 11 月 16 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 令和元年 7 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」（平成 31 年 1 月 23 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」（平成 31 年 1 月 23 日）
秘密情報保護ハンドブック	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～」（平成 28 年 2 月）
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」（令和元年 12 月）

【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
NISC	内閣官房内閣サイバーセキュリティセンター
公取委	公正取引委員会
個情委	個人情報保護委員会
厚労省	厚生労働省
農水省	農林水産省
経産省	経済産業省
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。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[1]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「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、または発信され、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。

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

[1] 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

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（以下「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[2]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[3]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、または、情報システム及び情報通信ネットワークの安全性およ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

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

[3] 詳細については Q71 を参照されたい。

Q2 サイバーセキュリティ基本法について

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局である NISC 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、政府機関等の情報セキュリティ対策のための統一基準群、重要インフラの情報セキュリティ対策に係る第４次行動計画、GSOC、サイバーセキュリティ協議会

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、同本部及び事務局を務める NISC 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、平成 26 年に成立し、平成 28 年、平成 30 年にそれぞれ改正が行われている。同法は、IT 基本法と相まって、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 NISC 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について

基本法第 25 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、関係閣僚及び有識者により構成されており、内閣官房内閣サイバーセキュリティセンター（NISC）が事務局を務める（基本法第 35 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明記されている主なものを抜粋すると、以下のとおりである（同法第 26 条第１項各号）。

①サイバーセキュリティ戦略の案の作成

②国の行政機関、独立行政法人及び指定法人[1]におけるサイバーセキュリティに関する対

[1] 基本法第 13 条は、指定法人について、「特殊法人（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）及び認可法人（特別の法律に

策の基準の作成及び当該基準に基づく監査

③国の行政機関、独立行政法人及び指定法人で発生したサイバーセキュリティに関する重大な事象に対する原因究明調査

④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

⑤その他サイバーセキュリティに関する重要施策に関する、企画に関する調査審議、施策の実施の推進及び総合調整

（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 26 条第 1 項第 1 号)。

現在、平成 30 年に閣議決定されたサイバーセキュリティ戦略が最新のものであり、持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステムの実現）を目指す姿とし、①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働を観点としつつ、基本法第 13 条から第 24 条までに規定する我が国におけるサイバーセキュリティに関する様々な基本的施策に関する事項が盛り込まれている。

なお、同戦略は、「今後 3 年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となる」とされているとおり、定期的な改定を想定したものとなっている。

（３）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[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監査を行う（基本法第 26 条第 1 項第 2 号)。

本規定に基づくものとして、「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」

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）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」と定義しており、現在、サイバーセキュリティ戦略本部「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」（平成 28 年決定）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、日本年金機構の合計 9 法人が指定されている。

[2] 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。

[3]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 年決定、平成 31 年一部改定）に基づき、①マネジメント監査（セキュリティ向上のための体制・制度が機能しているかの検証による評価（監査））、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る評価（監査））の二つにより監査を実施[4]することとされている。

（４）重大な事象に関する原因究明調査

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[5]で発生したサイバーセキュリティに関する重大な事象に対する原因究明調査を行う（基本法第 26 条第 1 項第 3 号）。本号に基づく事務を適切に遂行するため、サイバーセキュリティ戦略本部は「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 年決定、平成 31 年一部改定）を定めており、同規則においては、基本法第 26 条第 1 項第 3 号にいう「国の行政機関、独立行政法人又は指定法人で発生した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）を以下のとおり挙げている。

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

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 ①、②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

（５）情報システムに対する不正な活動の監視及び分析

基本法第 13 条は、国が講ずる施策として、「情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の

---

[3] 統一基準群は、①「政府機関等の情報セキュリティ対策のための統一規範」、②「政府機関等の情報セキュリティ対策の運用等に関する指針」、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」、④「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、①～③についてはサイバーセキュリティ戦略本部が、④については NISC が決定している。

[4] 監査事務については、サイバーセキュリティ戦略本部が NISC に実施させることとされており、独立行政法人及び指定法人における監査事務の一部については、基本法第 31 条第 1 項第 1 号の規定に基づき IPA に委託されている。

[5] 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。

監視及び分析」を挙げており、当該規定を踏まえ、内閣官房組織令第 4 条の 2 第 1 号は、「情報通信ネットワーク又は電磁的記録媒体…を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること」を NISC の所掌事務としている。

本規定に基づき、NISC は、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[6]）を運用しており、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っている。

（６）重要インフラ防護の推進に係る取組

上記（１）のサイバーセキュリティ戦略には、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におけるサイバーセキュリティの確保の促進に関する事項を定める必要がある（基本法第 12 条第 2 項第 3 号)。

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。

重要インフラの防護については、「任務保証[7]」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、サイバーセキュリティ戦略本部が「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成 29 年決定、令和 2 年改定）を策定している。同行動計画においては、重要インフラ分野として 14 の分野[8]が指定されており、当該分野に属する事業を営む者等のうち、対象となる重要インフラ事業者等[9]が挙げられているところ、①安全基準等の整備・浸透[10]、②情報共有体制の強化、③障害対応体制の強化、

---

[6] 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、NISC 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)、NISC 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 2019・29 頁参照)。

[7] 「重要インフラの情報セキュリティ対策に係る第４次行動計画」においては、「機能保証」という文言を用いている。平成 27 年にサイバーセキュリティ戦略本部が決定した旧サイバーセキュリティ戦略においては、「機能保証（任務保証)」としていたが、趣旨は「重要インフラ事業者等が果たすべき役割を確実に遂行することが重要」ということであり、「機能保証」とここにいう「任務保証」は同じ趣旨である。

[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

[9] 例えば、電力分野については「一般送配電事業者、主要な発電事業者」とされ、「主要な」という限定が付されている一方、金融分野についてはそのような限定はなく、対象となる事業者は分野により異なる。その他詳細については、同行動計画「別紙１　対象となる重要インフラ事業者等と重要システム例」における「対象となる重要インフラ事業者等」を参照されたい。

[10] サイバーセキュリティ戦略本部「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版)」（平成 30 年決定、令和元年改定）も参照。

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 つの施策群に基づく取組を推進している。

（7）横断的施策

ア　研究開発の推進

基本法第 21 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、横断的施策として、サイバー空間におけるイノベーションの進展とそれに対するサイバー攻撃の脅威を踏まえた実践的な研究開発の必要性と、中長期的な技術・社会の非連続的進化[11]を視野に入れた対応の必要性などが記載されている。

イ　人材育成・確保

基本法第 22 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、横断的施策として、あらゆる活動がサイバー空間に依存し、サイバー攻撃の脅威が広がっていく現状においては、一部の専門家がサイバーセキュリティの確保に取り組むのではなく、それぞれの役割を遂行する観点から主体的に取り組むことが求められること[12]などが記載されている。

ウ　教育及び学習の振興・普及啓発

基本法第 23 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戦略における主な観点の一つとして「参加・連携・協働」が挙げられていることも踏まえ、普及啓発に関しては、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、サイバーセキュリティ戦略本部「サイバーセキュリティ意識・行動強化プログラム」が平成 31 年に策定されている。

また、NISC においては、サイバーセキュリティの普及啓発活動の一環として、一般向けに身近な話題からサイバーセキュリティに関する基本的な知識を紹介する「インターネットの安全・安心ハンドブック」[13]を、そして、小規模な事業者や、セキュリティ担当者を置くことが難しい企業及び NPO 向けにサイバーセキュリティを解説した「小さな中小企業と NPO 向け情報セキュリティハンドブック Ver1.00」（平成 31 年 4 月）を公開している。

---

11 サイバーセキュリティ戦略本部「サイバーセキュリティ研究開発戦略」（平成 29 年）も参照。

12 サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」（平成 29 年）及び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「サイバーセキュリティ人材育成取組方針の決定について」（平成 30 年）も参照。

13 現在、令和元年 6 月 18 日に公開された Ver4.03 が最新版である。

（８）多様な主体の連携及びサイバーセキュリティ協議会

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[14]等の多様な主体による相互連携に関することを規定している。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る。

同協議会は、官民様々な主体を構成員とし、サイバーセキュリティに関する情報共有を行うことによって、サイバー攻撃による被害の予防及び被害拡大の防止を目的としている法定の情報共有体制である。詳細については、Q49 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

[14] 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）。

Q3 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

会社におけるサイバーセキュリティに関する体制は、その会社の内部統制システムの一部といえる。取締役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得る。

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である。また、取締役会は、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ることでもよい。

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、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おり（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、その事情いかんによっては、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、忠実義務違反となり得る場合がある。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。

同体制の構築にあたっては、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[1]）を策定する[2]ことも考えられる

---

[1] 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 2019・356 頁参照。

[2] 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およ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

このように、サイバーセキュリティを確保する体制は、内部統制システムに含まれ得るといえる。

（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念のために明文にしたものである。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のある場合には、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）に含まれる。

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）の問題ともなり得るほか、個人情報保護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）の問題にもなることがある。

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

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。

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[3]。

（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、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）[4]」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 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。

（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 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 号など）、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法令等遵守体制などを含め、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[5]。

（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趣旨からも、内部統制システムの運

[3] 広島高判令和元年 10 月 18 日判例集未登載
[4] 相澤哲ほか『論点解説新・会社法』（商事法務、平成 18 年）335 頁
[5] グループガイドライン 92 頁

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 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 Q5 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。

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
・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

４．裁判例

内部統制システムの整備義務に関して、
・大阪地判平成 12 年 9 月 20 日判時 1721 号 3 頁・判タ 1047 号 86 頁
・金沢地判平成 15 年 10 月 6 日判時 1898 号 145 頁・労判 867 号 61 頁
・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
・東京地判平成 16 年 12 月 16 日判時 1888 号 3 頁・判タ 1174 号 150 頁
・東京高判平成 20 年 5 月 21 日資料版商事法務 291 号 116 頁
・大阪地判平成 16 年 12 月 22 日判時 1892 号 108 頁・判タ 1172 号 271 頁
・大阪高判平成 18 年 6 月 9 日判時 1979 号 115 頁・判タ 1214 号 115 頁
・最判平成 21 年 7 月 9 日判時 2055 号 147 頁
・広島高判令和元年 10 月 18 日判例集未登載

Q4 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）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]。

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、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、取締役は、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、個情委による勧告・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。

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（Q3 参照）。

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[2]。

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

[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] 相澤哲ほか・同、及び大阪地判平成 12 年 9 月 20 日判タ 1047 号 86 頁

されておらず、取締役（・監査役）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[3]。

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）は責任を負うことがあり得る。

また、取締役（・監査役）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）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）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

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、取締役は原則として、刑事責任を負うことはない。ただし、会社が保有する情報のうち個人情報に関する漏えい等が生じた場合には、個情法が問題となる[4]。

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）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 20 条）を怠った結果、個人データが漏えいした場合は、個情委による勧告・命令の対象となる（同法第 42 条）。この命令に違反をした者に対しては、6 月以下の懲役または 30 万円以下の罰金が科され（同法第 84 条）、法人の代表者、使用人その他の従事者（以下本項において「代表者等」という。）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、法人も罰金刑の対象となる（同法第 87 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、代表者等は、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 20 条、第 42 条、第 84 条、第 87 条第 1 項

４．裁判例

特になし

---

[3] 相澤哲ほか・同
[4] 個人データの漏えいがあった場合に望ましい行動について Q50 参照。

Q5 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得る（Q3 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部門による監査（以下「内部監査」という。）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。

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。

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

[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）

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[3]を目的とした監査である。

情報セキュリティ監査は、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[4]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うえ、監査を行うこととなると考えられる[5]。

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総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査[6]である。

システム監査は、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。

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[7]。

---

[3] 情報セキュリティ監査基準・2 頁参照
[4] ISO/IEC 27001:2013（JIS Q 27001:2014）及び ISO/IEC 27002:2013（JIS Q 27002:2014）
[5] この点については、経営ガイドラインも参照されたい。
[6] システム監査基準 1 頁参照
[7] この点については、経産省「情報セキュリティ管理基準参照表」も参照されたい。

（２）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、社内における個人情報保護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）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、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 Q6 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）、コーポレート・ガバナンス報告書（有価証券上場規程（平成 19 年 11 月 1 日東京証券取引所）第 204 号第 12 項第 1 号等）、適時開示（有価証券上場規程第 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、情報セキュリティ基本方針等が挙げられる。

（４）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[8]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。

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）

[8] サイバーセキュリティ 2019・357 頁参照

・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）
・経産省「システム監査基準」（平成 30 年 4 月 20 日改訂）
・経産省「システム管理基準」（平成 30 年 4 月 20 日改訂）
・経産省「情報セキュリティ管理基準参照表」

４．裁判例

特になし

Q6 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

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的な根拠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、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も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）、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（平成 19 年 11 月 1 日東京証券取引所）第 204 号第 12 項第 1 号等）、適時開示（有価証券上場規程第 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、情報セキュリティ基本方針等が挙げられる。

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、「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、詳細についてはそちらも参照されたい。

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的な根拠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

[1] 総務省「サイバーセキュリティ対策情報開示の手引き」13 頁など
https://www.soumu.go.jp/main_content/000630516.pdf

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のうえ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を作成すること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 Q3 を参照されたい。）。

（３）有価証券報告書

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。

その他事業の内容に関する重要な事項の中には、事業等のリスクが含まれるところ（企業内容等の開示に関する内閣府令第 15 条第 1 項第 1 号に定める第 3 号様式）、サイバーセキュリティに関するリスクをこの事業等のリスクとして開示することが考えられる。

（４）コーポレート・ガバナンスに関する報告書

証券取引所による開示制度の一環として、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。

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 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ステムの一部として

開示することが考えられる。

（５）適時開示

有価証券上場規程第 402 条等に基づき、上場会社は、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。

サイバー攻撃に起因して損害が発生する場合には、この災害に起因する損害又は業務遂行の過程で生じた損害として損害・損失の内容や今後の見通しを開示することが考えられる。

（６）情報セキュリティ報告書

平成 19 年 9 月に経産省が「情報セキュリティ報告書モデル」[2]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。

（７）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。環境、労働、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が考えらえる。

（８）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、社内規定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。

---

[2] 経産省「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

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
・企業内容等の開示に関する内閣府令第 15 条第 1 項第 1 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
・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」
・経産省「情報セキュリティ報告書モデル」

４．裁判例

特になし

Q7 個人情報保護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

個情法は個人データの取扱いにあたって、「必要かつ適切な」安全管理のための措置を講ずると規定するところ、具体的な措置については各社がその実情に応じて決定する必要がある。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。

保存・消去、本人請求への対応に関しては、まず、不要不急な個人情報の取扱いがなされないような対応が求められる。請求については、これに応じ得る組織的・技術的措置を講ずるとともに、他方でアクセス制御等によって不当な保有個人データの取扱いを防止することが求められる。

２．解説

（１）はじめに

企業が個人情報を取り扱うにあたっては、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うえで具体的な対応を行うことが求められる。

個情法第 20 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、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[1]を構成する個人情報のことを

[1] 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

いう（個情法第 2 条第 4 項、同条第 6 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[2]は、個人データに該当することとなる[3]。

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、滅失又は毀損（以下「漏えい等」という。）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「8（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、⑥技術的安全管理措置を列挙している。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[4]。②個人データの取扱いに係る規律の整備を行うにあたっては、組織的安全管理措

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（個情法第 2 条第 5 項、個情法施行令第 3 条第 2 項）。

[2] 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）。

[3] 詳細は個情法ガイドライン（通則編）2-4、2-6 を参照。

[4] 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およ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

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あたっては、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あたっては、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、電子媒体等と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。

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 QA1-7「講ずべき安全管理措置の内容」等を参照されたい[5]。

（３）個人情報の保存・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、不要・不急な個人情報を保持しないことが重要である。そこで、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（個情法第 19 条）。

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 2 条第 7 項）[6]の開示を請求することができる（同法 28 条 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 29 条第 1 項、第 2 項）。

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。

[5] なお、平成27年の個情法改正（平成29年施行）前は、事業に用いる個人情報データベース等の対象者が5000人を超えない場合は、個人情報取扱事業者に該当しなかったため、安全管理措置その他の個情法上の義務は生じなかったが、同改正により、事業に用いる個人情報データベース等の対象者が5000人を超えない場合であっても、個人情報取扱事業者に該当し、安全管理措置その他の各種義務を履行する義務が課されることとなった。ただし、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。

[6] 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。

（４）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。

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。

加えて、サイバーセキュリティ対策は、各々の企業が経営管理の観点からリスクマネジメントを行い、具体的な対策を実施していくものである。個情法に基づく安全管理措置義務は、個人情報の有用性を図りつつ本人の権利利益を保護するという法目的を実現するための法的義務であり、これに違反した場合は、個人情報保護委員会による指導や勧告がなされうる（個情法第 41 条、42 条）点で異なる。

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[7]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[8]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。

３．参考資料（法令・ガイドラインなど）

・個情法第 2 条、第 19 条、第 20 条、第 28 条、第 29 条
・個情法ガイドライン（通則編）
・個情法QA

４．裁判例

特になし

[7] Q5 も参照。
[8] Information Security Management System の略。

Q8 個人データの委託と安全管理

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

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、当該個人データの安全管理が図られるよう、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、取扱いを委託された個人データの安全管理が図られるよう、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（個情法第 22 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、全部の取扱い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 20 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同意が必要だが（個情法第 23 条第 1 項）、委託に伴う個人データの提供は、委託する内容が、委託元が特定した当該個人データの利用目的の達成に必要な範囲を超えない限りにおいて、個人データの第三者提供には該当しないとされている（同法第 23 条第 5 項第 1 号）。

（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）3-3-4 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、本人の個人データが漏えい、滅失又は毀損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、事業の性質及び個人データの取扱状況（取り扱う

[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。

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について、必要かつ適切な措置を講じなければならない。

（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 20 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「8（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 20 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）「8（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 22 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・リスクに関しては Q43 も参照されたい。

３．参考資料（法令・ガイドラインなど）

・個情法第 20 条、第 22 条
・個情法ガイドライン（通則編）3-3-4

４．裁判例

特になし

Q9 クラウドサービスの活用と個人情報保護法

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

１．概要

クラウドサービスの利用に伴って個人データが取り扱われる場合、クラウドサービスを利用しようとする企業には、安全管理措置（個情法第 20 条）のほか、クラウドサービス提供事業者が個人データの取扱いを行っているか否かによって、クラウドサービス提供事業者に対する監督義務（同法第 22 条）の適用の有無が変わる。

クラウドサービス提供事業者が海外の事業者である場合、個情法第 24 条の例外事由にあたるかどうかを検討する必要がある。

２．解説

（１）クラウドサービスと個情法

ア　はじめに

企業が個人データの取扱いに伴ってクラウドサービスを利用する場合、必然的に個人データが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。）に移転する。

このため、原則として個人データの第三者提供の制限に対応して同意を取得することが必要となる（個情法第 23 条第 1 項）が、個人データの取扱いの委託として整理しうる場合には、「第三者」への提供ではないとして、同意が不要となる（同条第 5 項）。

また、そもそも個人データの「取扱い」に該当しないとして、クラウドサービス提供事業者への移転は第三者提供にあたらないとされる場合があり得る（個情法 QA5-33,34 参照）。

また、クラウドサービス提供事業者が外国にある第三者（外国法人など）の場合には、外国にある第三者への個人データの提供を認める旨の本人同意が必要である。

イ　クラウドサービスと「個人情報の取扱い」の有無

個情法 QA5-33 は、「保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準となります。」としている。

ウ　「個人情報の取扱い」に該当しない場合の対応

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、「個人データを提供したことにはならない」ため、個情法第 23 条第 1 項に基づく同意の取得は不要であり、また、同法第 22 条に基づく委託先の監督義務も課されないこととなる。

個人情報を取り扱わないこととなっているといえる場合について、個情法 QA5-33 は、

「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。

ただし、個人データを取り扱わないこととなっており、個情法第 23 条第 1 項に基づく本人の同意を得る必要がないとしても、当該クラウドサービスを利用する企業は、自らが同法第 20 条に基づき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 QA5-34 参照）とされている点に留意が必要である。

エ　「個人情報の取扱い」に該当する場合の対応

クラウドサービス提供事業者による個人情報の取扱いに該当する場合、当該クラウドサービスを利用する企業としては、クラウドサービス提供事業者が「外国にある第三者」か否かを検討する必要がある。

まず、クラウドサービスを海外の事業者が運営している場合であっても、サーバが国内にある場合であり、当該サーバに保存された個人データを国内で取り扱っていると認められる場合には、当該サーバの運営事業者は個人情報取扱事業者に該当するため、当該事業者への個人データの提供は、外国にある第三者への提供に該当しないとされている（個情法 QA9-6 参照）。

次に、外国にある第三者への個人データの提供となる場合、個情法においては、国内にある第三者とは異なる制限が設けられており、以下の 3 つの例外を除き、個情法上の委託によることができず、あらかじめ「外国にある第三者」への提供を認める旨の同意を取得する必要がある（個情法第 24 条）。

①「外国」の例外

当該第三者が、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国として、個情法施行規則で定める国にある場合であり、具体的には EU が該当する[1]。

②「第三者」の例外

当該第三者が、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であり、具体的には、アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システムの認証を取得した第三者である場合[2]、また、提供元の事業者が CBPR システムの認証を取得しており、当該事業者に代わって個人情報を取り扱う海外の事業者等に対して提供する場合など[3]が挙げられる。

---

1 個情法施行規則第 11 条第 1 項、「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等」（平成 31 年個人情報保護委員会告示第 1 号）第 2 項参照。なお、同施行規則第 11 条第 2 項は、外国を定める場合において我が国における個人の権利利益を保護するために必要があると認めるときは必要な条件を付することができるとしているところ、現在は欧州一般データ保護規則に服するものであることと、見直しを行うことが定められているのみである。以上のことから、基本的に EEA 域内に所在する事業者に対しては、国内にある第三者と同様の対応を行えばよいものと考えられる。

2 個情法施行規則第 11 条の 2 第 2 号

3 個情法施行規則第 11 条の 2 第 1 号、個人情報の保護に関する法律ガイドライン（外国にあ

③個情法第 23 条第 1 項各号に該当する場合

以上 3 つの例外のいずれかに該当しない場合、外国にある第三者への提供については、同法第 23 条が適用されない、すなわち、個人データの取扱いの委託、事業承継に伴う個人データの提供、共同利用等の例外規定（同法第 23 条第 5 項各号）は適用されず、「外国にある第三者」への提供を認める旨の同意を取得する必要がある。

一方で、国内にある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、または、上記①～③の例外に該当する外国の事業者に対する個人データの提供については、個情法第 23 条の適用を受けることとなる。この場合、同法第 23 条に基づき本人同意が不要となる例外規定が適用される余地がある。

３．参考資料（法令・ガイドラインなど）

・個情法第 20 条、第 22 条、第 23 条、第 24 条
・個人情報の保護に関する施行規則第 11 条、第 11 条の 2
・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

る第三者への提供編）4-1。その他、同号に定める「個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第 4 章第 1 節の規定の趣旨に沿った措置の実施が確保されていること」の詳細については、同ガイドライン（外国にある第三者への提供偏）4-1、4-2 を参照されたい。

Q10 個人情報保護法制

個人情報の保護に関して法令上求められる安全管理の措置は、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、安全確保措置、個人情報の定義

１．概要

法令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情法に規定する「個人データ」、国の行政機関又は独立行政法人等については、行個法又は独個法に規定する「保有個人情報」が対象となる。また、地方公共団体の場合、各地方公共団体の条例ごとに安全管理措置の対象が異なる可能性があり、さらにいえば個人情報の定義自体も異なる可能性がある。

２．解説

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る旨を規律している。

このうち、個情法は、理念等を規定する第一章から第三章までについては、すべての主体を対象とした基本法的機能を有しているものの、同法は、具体的な義務規定等については、民間部門における個人情報取扱事業者のみを対象としている。

一方で、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が適用される。また、地方公共団体については、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、「個人情報保護条例」という）が適用される。但し、これらの場合であっても、行個法第 6 条第 2 項のように、例外的に民間部門に適用される条項もある。

したがって、法令に基づき求められる安全管理措置については、個人情報を取り扱う主体によって異なることとなる。

なお、個情法第 20 条は、個人情報取扱事業者に対し、「個人データ」についての安全管理措置義務を課している[1]。データベース化などされておらず散在する個人情報については、法律上の安全管理措置義務は課されない。

次に、行個法第 6 条及び独個法第 7 条は、国の行政機関と独立行政法人等に対し、「保有個人情報」についての安全確保措置義務（個人情報保護法上の安全管理措置義務に相当するもの）を課している。保有個人情報とは、行政機関の職員（独立行政法人等の場合は、独立行政法人等の役員又は職員）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

[1] この点について Q7 も参照されたい。

関の職員（独立行政法人等の場合は、当該独立行政法人等の役員又は職員）が組織的に利用するものとして、当該行政機関（当該独立行政法人等）が保有しているものをいう。ただし、行政文書[2]に記録されているものに限られる。

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であっても、上記保有個人情報としての要件を充足する限り安全確保措置義務が課されることとなる。

また、地方公共団体については、上記のとおり、各地方公共団体が定める個人情報保護条例が適用となるため、どのような情報に対してどのような義務が課されるかは条例によって異なる。例えば、そもそもの「個人情報」の定義についても、個情法、行個法、独個法がいずれも「生存する個人に関する情報」を要件としており死者の情報を含まない一方で、地方公共団体の条例の中には、「生存する」が定義に含まれておらず、死者の情報も「個人情報」として保護されている場合がある。

このように、個人情報保護制度上は、個人情報を取り扱う主体ごとに適用される法令に基づき安全管理措置義務の対象となる個人情報の範囲が異なるため、個人情報を取り扱う上では、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る。

なお、個人情報保護法上の安全管理措置義務の対象とならない個人情報については、安全管理措置を怠ったことを原因として情報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該当しないとしても、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ほか、それらの情報が個人のプライバシーに係る情報に該当する場合には、過失により当該個人のプライバシー権を侵害したものとして法的な責任を負う可能性がある。

３．参考資料（法令・ガイドラインなど）

・個情法ガイドライン（通則編）
・行政機関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について（平成 16 年 9 月 14 日総務省行政管理局長通知［最終改正］平成 30 年 10 月 22 日）
・独立行政法人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について（平成 16 年 9 月 14 日総務省行政管理局長通知［最終改正］平成 30 年 10 月 22 日））

４．裁判例

特になし

[2] 行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）第 2 条第 2 項に規定する行政文書（独立行政法人等の場合は、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号）第 2 条第 2 項に規定する法人文書）

Q11 国立大学、私立大学及び企業の共同研究と個人情報保護

国立大学と企業、私立大学と企業がそれぞれ共同研究を行う場合のように、様々な主体が共同で個人情報を取り扱う場合に、法令上どのような点に留意すべきか。

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、研究開発、適用除外

１．概要

我が国の個人情報保護法制は、民間部門と公的部門で規律する根拠法令が異なる。また、個情法が適用される私立大学が学術研究の用に供する目的で個人情報を取り扱うことについては、個人情報取扱事業者の義務等が適用除外とされている（個情法第 76 条）。

安全管理については、対象範囲に齟齬はあるものの、個情法及び独個法は、いずれも安全管理のために実態に即した措置を講ずるものとされており、基本的に講ずべき措置に相違はない。

２．解説

（１）はじめに

我が国の個人情報保護法制は、民間部門と公的部門で適用される法令が異なるところ（Q10 参照）、国立大学、公立大学、私立大学ではそれぞれ適用法令が異なる。適用関係は、次のとおりである。

主体	適用法令
国立大学法人 研究開発法人	独個法
公立大学	地方公共団体が定める個人情報保護条例
私立大学 民間研究機関	個情法 なお、同法第 76 条は、大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者による学術研究の用に供する目的での個人情報の取扱いについて、個人情報取扱事業者又は匿名加工情報取扱事業者の義務を適用除外としている。
民間企業	個情法 なお、同法 43 条は、学問の自由を妨げないよう個人情報保護委員会による権限行使の制限を規定しており、特に、適用除外のケースで個人情報又は匿名加工情報を提供する場合は権限行使しないものとされている。

以上のとおり、主体によって適用される法令が異なり、民間部門においては研究機関について適用除外が設けられているため、企業や私立病院が大学と共同研究を行ったり協力したりするケースにおいて、適用除外又は権限行使の制限がなされるか等は、ケース・バ

イ・ケースである。よって、実際に研究を行う場面では、適法性担保の検討が必要である。

（２）適用法令の異なる主体間での共同研究と注意点

適用法令、適用条文が異なることによって、研究開発場面では次の点を注意する必要がある。

① 適用法令の確認
② 適用法令における差分の確認と追加対応の要否
③ 私立大学が含まれる場合の適用除外の射程の確認

まずは、共同研究を行う主体を確定し、それぞれの適用法令を確認する必要がある。そのうえで、義務等に差分がないか、追加対応を必要としないかを検討する。

例えば、個人情報の定義については、個情法はそれ単体では特定の個人を識別することができない情報についても他の情報と容易に照合することができこれによって特定の個人を識別することができる情報を個人情報としているところ（第 2 条第 1 項第 1 号）、独個法は他の情報との照合に当たり「容易性」の要件を付していない（同法第 2 条第 2 項第 1 号）。すなわち、理論上、国立大学法人や研究開発法人の方が、個人情報として法の適用を受け得る範囲が広い。

さらに、私立大学と企業が共同研究を行う場合や、企業が設立した研究機関が研究を行う場合等、個情法の適用除外規定の適用があるかどうかについては、個情法 QA8-3、8-4 等に照らして判断する必要がある。その際、主体と利用目的双方が個情法に定める要件を満たしているか等について吟味する必要がある。

なお、同法第 76 条が適用されない、すなわち、同法第 4 章の規定が適用される場合であっても、複数の主体の間で個人データのやり取りができないというものではなく、例えば、公衆衛生の向上に特に必要がある場合で本人の同意を得ることが困難であるときは、あらかじめ本人の同意を得ることなく個人データを第三者に提供することができるほか（同法第 23 条第 1 項第 3 号）、学術研究機関が学術研究の目的で個人情報等を取り扱う場合に、その者に対して個人情報等を提供する行為については、個人情報保護委員会は権限を行使しない旨が規定されている（同法第 43 条第 2 項）。

（３）安全管理措置

安全管理については、対象となる個人情報の範囲は適用される法令により異なりうる（Q10 参照）ものの、基本的な措置に相違はない。すなわち、個情法は個人データについて「漏えい、滅失又はき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。」（同法第 20 条）とし、独個法は保有個人情報について「漏えい、滅失又は毀損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない」としている（同法第 7 条第 1 項）。いずれも個人情報の内容、利用目的等の情報取扱いの実態に即した安全管理のための措置を講ずるよう義務付けるもので

あると考えられる。

なお、独個法第 7 条第 2 項は、委託先に対して「第 7 条第 1 項の規定は、独立行政法人等から個人情報…の取扱いの委託を受けた者が受託した業務を行う場合について準用する。」と定めを設けており、この点は個情法と異なる。

３．参考資料（法令・ガイドラインなど）

・個情法第 2 条、第 20 条、第 43 条、第 76 条
・独個法第 2 条、第 7 条
・個情法ガイドライン（通則編）
・個情法 QA

４．裁判例

特になし

Q12 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、法令上どのような安全管理が必要となるか。

タグ：個情法、安全管理措置義務、統計情報、匿名加工情報

１．概要

個人データを加工する場合、①安全管理上、氏名等を削除するといった加工を施す場合、②統計情報へ加工する場合、③匿名加工情報へ加工する場合が考えられる。

①の場合、個人データ該当性を失わないため、個情法第 20 条に基づく安全管理措置義務が課される。②の場合、個情法に基づく規律はかからないが、適切な管理が必要であると考えられる。③の場合、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 36 条に基づき、加工方法等情報に関する安全管理措置義務が課され、匿名加工情報に関する安全管理措置の努力義務が課される。

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社内で利用するために、安全管理上、氏名等を削除するといった加工を施す場合と、個人情報及びプライバシーの保護を前提としつつ、データの積極的な利活用を社内外で行うために②統計情報又は③匿名加工情報へ加工するといった場合が考えられる[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、データの加工にあたっては、個情法ガイドライン（通則編）「８（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の整備などの措置を講じる必要がある。また、③の匿名加工情報の場合には、個情委「個人情報の保護に関する法律ガイドライン（匿名加工情報編）」（以下本項において「個情法ガイドライン（匿名加工情報編）」という。）及び個情委事務局「個人情報保護委員会事務局レポート：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「事務局レポート」という。）により、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いる。

---

[1] 個人情報、個人データ等、個情法における定義については Q7 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関して Q40 を参照されたい（特に「派生データ」について）。

（２）安全管理のための加工

企業が社内で活用するために、名簿等の個人データから、安全管理のために氏名を削除する等の加工を施す場合がある。

しかし、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、加工した後のデータは個人データ該当性を失わず、加工後の情報についても、個情法第 20 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]とすることが求められている。

（３）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[4]。

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 23 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、個情法第 20 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、こうしたデータが過失により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、適切な管理を行う必要があると考えられる。

（４）匿名加工情報への加工

ア　匿名加工情報制度の趣旨

平成 27 年の個情法改正により、「匿名加工情報」の類型が新設された。これは、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

[3] 個情法ガイドライン（通則編）3-3-2 参照。
[4] 個情法ガイドライン（匿名加工情報編）2-1 参照

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[5]。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[6]。

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 9 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[7]。

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 36 条に基づき、①適正加工、②加工方法等情報[8]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には、個情法第 37 条から第 39 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[9]。

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あり、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、作成の基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[10]、例えば、同法第 23 条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。

---

[5] 事務局レポート 3 頁、9 頁参照
[6] 事務局レポート 9 頁参照
[7] 個情法ガイドライン（匿名加工情報編）2-1 参照。
[8] 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個情法第 36 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（個情法施行規則第 20 条第 1 号)。「その情報を用いて当該個人情報を復元できるもの」としては、例えば、氏名等を仮 ID に置き換えた場合における置き換えアルゴリズムに用いられる乱数等のパラメータ又は氏名と仮 ID の対応表の等のような加工の方法に関する情報が該当するとされている（個情法ガイドライン（匿名加工情報編）3-3-1 参照)。
[9] なお、匿名加工情報取扱事業者には、⑤に関して加工方法等情報の取得も禁止されている。
[10] 事務局レポート 3.4.2 参照。

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、本人の権利・利益保護の観点から、個情委が定める加工の基準[11]に従い適正に加工しなければならない（個情法 36 条第 1 項、同法施行規則第 19 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）、（3）のように、安全管理の一環としての氏名等の一部の個人情報の削除や、統計情報の作成のための加工については、匿名加工情報を「作成するとき」には該当しない[12]。

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 36 条第 2 項、同法第 38 条）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 39 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 20 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[13]。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[14]。

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[15]。

３．参考資料（法令・ガイドラインなど）

・個情法第 2 条、第 20 条、第 4 章第 2 節
・個情法施行令第 1 条
・個情法施行規則第 2 条、第 3 条、第 4 条、第 19 条、第 20 条
・個情法ガイドライン（通則編）

---

11 詳細については、個情法ガイドライン（匿名加工情報編）及び事務局レポートを参照されたい。
12 個情法ガイドライン（匿名加工情報編）3-2 参照
13 個情法ガイドライン（匿名加工情報編）3-3-1 参照。
14 具体例については、個情法ガイドライン（匿名加工情報編）3-3-1 を参照。
15 個情法ガイドライン（匿名加工情報編）3-3-2 参照。

・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（匿名加工情報編）」
・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：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

Q13 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あたって留意すべき点は何か。

タグ：割賦販売法、クレジットカード情報、PCI DSS、非保持化、重要インフラ分野

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）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」（以下「実行計画」という。）を実務上の指針としており、実行計画に掲げられ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。サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第４次行動計画」においても、クレジット分野は、重要インフラ分野[1]の一つとして位置付けられており、セキュリティ強化の更なる取組が求められている。

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。

（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、立替払取次業者及び加盟店（こ

[1] 重要インフラに関する取組の概要について Q2 参照。

れらを併せて以下「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 号ないし第 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カード番号等の管理に係る事故（以下「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、その原因を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。

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「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、2016 年から毎年見直しがなされている実行計画を実務上の指針としており、実行計画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、法令上の基準を満たしているとされている[2]。

2019 年に発表された実行計画 2019 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）[3]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

[2] 経産省プレスリリース「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」を取りまとめました」（平成 31 年 3 月 4 日）
https://www.meti.go.jp/press/2018/03/20190304004/20190304004.html

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

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。

経済産業大臣は、クレジットカード等購入あっせん業者又は立替払取次業者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実行計画2019においては、対面加盟店における偽造カード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策として、パスワードによる本人認証、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。

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、同第35条の17、同第35条の17の15
・割賦販売法施行規則第132条、同第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」

４．裁判例

・東京地判平成21年11月11日判時2073号64頁
・東京地判平成26年1月23日判時2221号71頁

Q14 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扱う際の留意点は何か。

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、労働者側からは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、同時に個人情報保護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、情報の収集にあ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）に該当しうる。個情委・厚労省「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、以下本項において「留意事項」という。[1]）によれば、例えば、労働安全衛生法の諸規定に基

[1] 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

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、その取得には原則として同意を要する（同法第 17 条第 2 項）、第三者提供にあたってオプトアウトによる方法が認められない（同法第 23 条第 2 項）など要配慮個人情報としての取扱い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、同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、平成 30 年改正労働安全衛生法は、事業者は、労働者の心身の状態の情報を収集、保管、または使用するにあたっては、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（労働安全衛生法第 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]。

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

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。

[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第 35 条の 3 にも設けられている。

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情報の収集にあ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]。

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（昭和 35 年法律第 30 号）第 35 条の 3、第 35 条の 4
・個情委、厚労省「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）

[4] なお、罰則付きの守秘義務については、Q69 も参照。
[5] 守秘義務については、じん肺法第 35 条の 4 にも規定されている。

https://www.ppc.go.jp/files/pdf/koyoukanri_ryuuijikou.pdf

・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）

・厚労省「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）

４．裁判例

本文中に記載のとおり

Q15 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、すべ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・災害対策等分野の行政事務（個人番号利用事務。番号利用法第 2 条第 10 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 11 項参照。）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。

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及び個人番号関係事務実施者は、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

[1] なお、番号利用法における「個人情報」については、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また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と定義されている（番号利用法第 2 条第 3 項）。この点に関連して Q10、Q11 も参照。

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[2]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)。

３．参考資料（法令・ガイドラインなど）

・番号利用法第 2 条、第 9 条、第 10 条、第 11 条、第 12 条、第 15 条、第 16 条、第 19 条、第 20 条
・個情委「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)」

４．裁判例

特になし

[2] 番号利用法第 2 条第 8 項は、マイナンバー（個人番号）をその内容に含む個人情報を「特定個人情報」と定義している。

Q16 マイナンバーカード

民間企業がマイナンバーカードを活用することは可能か。

タグ：番号利用法、マイナンバーカード、本人確認、身分証明証、公的個人認証、通知カード

１．概要

マイナンバーを利用できる主体は行政機関などに限られているが、①マイナンバーの提示書類、②顔写真付き身分証明書、③電子的な身分証明書という 3 つの機能を有しているところ、マイナンバー自体を利用しなければマイナンバーカードは企業も利用することができる。

２．解説

（１）マイナンバーカード

マイナンバーカード（個人番号カード）とは、券面に氏名、生年月日、性別、住所及びマイナンバーが記載されたプラスチック製のICカードである。申請した者に対して、市町村長が厳格な本人確認を実施した上で交付している。

マイナンバーカードには、①マイナンバーの提示書類、②顔写真付き身分証明書、③電子的な身分証明書という３つの機能がある。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は企業も利用することができる。

（２）マイナンバーカードの活用方法①　マイナンバーの提示書類

マイナンバーカードは、マイナンバーを使う手続の際に必要となるマイナンバーの確認と身元確認を１枚で行うことができる唯一のカードである。

なお、マイナンバーの証明自体は、交付済の通知カード[1]やマイナンバーが記載された住民票の写しなどによっても行うことができるが、その場合は身元確認のため顔写真付き身分証明書などの提示が必要になる。

（３）マイナンバーカードの活用方法②　顔写真付き身分証明書

②顔写真付き身分証明書としての機能とは、会員登録や銀行口座の開設など本人確認が

[1] 情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律（令和元年法律第 16 号）に基づく番号利用法の改正により、マイナンバーカードの取得促進を目的として、通知カードによる個人番号の通知（番号利用法第 7 条）が廃止されることとなった。本改正は、令和元年 5 月 31 日から 1 年以内の範囲で政令で定める日から施行される。

求められる様々な場面でマイナンバーカードを利用できることを指す。

ただし、身分証明書として利用すると偽って、カード裏面のマイナンバーを盗み見たり、書き取ったりすることは違法である。身分証明書を確認する際に、例えば、運転免許証であれば、運転免許証番号を別途メモ等にとることがあるが、マイナンバーカードの場合はマイナンバーを別途メモ等にとることはできない点に注意する必要がある。

（４）マイナンバーカードの活用方法③　電子的な本人確認

③電子的な本人確認としての機能とは、いわば身分証明書のデジタル版である。

申請した者のマイナンバーカードには、電子証明書（署名用電子証明書・利用者証明用電子証明書）が搭載される。電子証明書は、例えば、Web 上の電子申請、Web のログイン手段等に活用することができる。

電子証明書は以下の 2 種類である。

・署名用電子証明書

作成された電子文書をインターネット等で送信する際（例：e-Tax の確定申告など）に利用するものであり、当該電子文書の作成・送信者が送信者本人であることを証明することができる。

・利用者証明用電子証明書

インターネットサイトにログイン等する際（例：マイナポータルへのログイン、コンビニ交付サービスの利用など）に利用するものであり、オンラインサービスの利用者が特定の利用者であることを証明することができる。

なお、マイナンバーカードの IC チップの空き領域を活用し、カードアプリケーションを搭載することにより、例えば、物理的な入退室管理カード、チケット購入、ポイント付与等に活用することも可能である[2]。

３．参考資料（法令・ガイドラインなど）

・番号利用法

・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（公的個人認証法）

４．裁判例

特になし

[2] 詳細については、総務省自治行政局住民制度課「民間事業者による個人番号カードの空き領域の活用について」を参照されたい。

Q17 どのように情報を管理していれば「営業秘密」として認められるのか

サイバーセキュリティインシデントが発生し、企業が秘密として取扱いたい情報が漏えいした場合に、民事裁判において当該情報の使用・開示の停止・中止を求める、もしくは損害賠償を請求する、または刑事告訴して厳正に対処するためには、当該情報が不正競争防止法上の「営業秘密」に該当する必要がある。どのように秘密情報を管理していれば、「営業秘密」として認められるのか。

タグ：不正競争防止法、刑事訴訟法、関税法、営業秘密、秘密管理性、有用性、非公知性

１．概要

企業において秘密として取扱い情報が漏えいしたときに、当該情報を不正に開示した者や取得した者などを相手に当該情報の使用・開示の停止・中止や損害賠償を求めて裁判をするなどの法的保護を受けようとするのであれば、「営業秘密」の 3 要件を満たすように当該情報を管理することが必要である。詳しくは、営業秘密について不正競争防止法に基づく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を示す営業秘密管理指針を参照されたい。

２．解説

（１）「営業秘密」とは

「営業秘密」とは、一定の要件を満たした場合に不正競争防止法に基づく法的保護が与えられる情報をいう。

どのような情報が「営業秘密」に該当し、また、該当した場合にどのような法的保護が与えられるのかについては、不正競争防止法第 2 条第 6 項が規定する。

「営業秘密」は法律上の用語であるのに対し、これと似た用語である、秘密情報、機密情報や企業秘密（以下、「秘密情報等」という）については、法律上定義されたものではなく、組織内の規程や企業同士における契約において、一定の情報に用いられる呼称にすぎない。

このように、「営業秘密」と秘密情報等とは、法律に基づく保護を受け得るのか、または規程・契約等の合意に基づく保護を受け得るのか、すなわち何かしらの違反行為があった場合に、不法行為責任もしくは刑罰を問えるのか、または債務不履行責任を問えるのか、という点で大きく異なるものといえる。なお、両者は重なる場合もあり、決して択一の関係にあるわけではないが、「営業秘密」に該当しない秘密情報等については、不正競争防止法に基づく法的保護が与えられないことがポイントである。

なお、平成 30 年不正競争防止法改正により新しく創設された「限定提供データ」と営業秘密との異同については、Q20 を参照されたい。

（２）「営業秘密」に該当した場合に受けられる法的保護の内容

大きく分けると民事的措置、刑事的措置及び水際措置である[1]。

民事的措置としては、営業秘密の不正な取得・使用・開示の停止・中止や削除を求める差止請求権（不正競争防止法第 3 条）、及び損害賠償請求権（同法第 4 条）である[2]。

刑事的措置としては、営業秘密侵害罪（同法第 21 条第 1 項各号等）が設けられている[3]ので、被害者は告訴を行うことができる（刑事訴訟法第 230 条）。なお、刑事的措置については、営業秘密の保護強化を図った平成 27 年不正競争防止法改正により、営業秘密侵害罪について告訴がなくても検察官は被疑者を起訴することができるようになり（非親告罪化され）、また、都道府県警本部に営業秘密保護対策官が置かれた[4]。営業秘密を侵害された企業においては、初動対応の一環として早急に警察に相談し、捜査開始後は警察と連携・協力していくことが重要である（「秘密情報保護ハンドブック」第 6 章参照）。

水際措置（水際取締り）[5]とは、税関での輸出又は輸入差止めをいい、営業秘密侵害品（不正競争防止法第 2 条第 1 項第 10 号）についての輸出入差止め（輸出について関税法第 69 条の 2 第 1 項第 4 号等、輸入について同法第 69 条の 11 第 1 項第 10 号等参照）をなし得る。

このように、ある情報が「営業秘密」に該当し、かつ、不正競争防止法が規定する要件を満たす不正な行為が行われた場合には、民事訴訟、刑事告訴または輸出入差止めといった措置を取り得ることができる。なお、「営業秘密」に該当するか否かは、主に裁判所で判断されることとなる。

（３）「営業秘密」として認められるためには

企業が秘密として取り扱いたい情報が裁判において「営業秘密」（不正競争防止法第 2 条第 6 項）として認められるためには、①秘密管理性、②有用性、及び③非公知性の 3 つの要件を満たすことが必要である。

---

1 「不正競争防止法テキスト」（経産省知的財産政策室、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/201909_unfaircompetitiontext.pdf）が、「営業秘密」を含め不正競争防止法について、図表付きでわかりやすく解説しており、参考となる。

2 詳細については逐条不正競争防止法 86 頁以降を参照。

3 詳細については逐条不正競争防止法 245 頁以降を参照

4 警察庁丙生経発第 4 号「不正競争防止法の一部を改正する法律の公布について（通達）」平成 27 年 10 月 2 日警察庁生活安全局長（https://www.npa.go.jp/pdc/notification/seian/seikeitaisakukanrikan/seikei20151002.pdf）。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、秘密保護ハンドブック 176 頁、または右記資料 19 頁参照（経産省知的財産政策室「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）。

5 水際措置については、「水際措置の流れ（輸出入差止申立て及び認定手続きのフロー）」（経産省知的財産政策室、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20161012mizugiwanagare.pdf）を参照されたい。

ア　秘密管理性

（ア）趣旨

「秘密として管理されている」（不正競争防止法第 2 条第 6 項）という要件は、「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や取引相手先（以下、「従業員等」という。）にとって、当該情報が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」ことを踏まえて定められたものである（営業秘密管理指針 4 頁～5 頁）。

（イ）ポイント

秘密管理性が認められるためには、「営業秘密保有企業の秘密管理意思が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る必要がある」とされる（営業秘密管理指針 6 頁～15 頁）。

（ウ）裁判例

刑事事件であるが業務委託先の派遣労働者が被告人となった東京高判平成 29 年 3 月 21 日高刑集 70 巻 1 号 10 頁・判タ 1443 号 80 頁は、秘密管理性について以下のとおり判示した。

◆ 趣旨について

> 不正競争防止法 2 条 6 項が保護されるべき営業秘密に秘密管理性を要件とした趣旨は，営業秘密として保護の対象となる情報とそうでない情報とが明確に区別されていなければ，事業者が保有する情報に接した者にとって，当該情報を使用等することが許されるか否かを予測することが困難となり，その結果，情報の自由な利用を阻害することになるからである。

◆ 解釈・適用について

> 当該情報が秘密として管理されているというためには，当該情報に関して，その保有者が主観的に秘密にしておく意思を有しているだけでなく，当該情報にアクセスした従業員や外部者に，当該情報が秘密であることが十分に認識できるようにされていることが重要であり，そのためには，当該情報にアクセスできる者を制限するなど，保有者が当該情報を合理的な方法で管理していることが必要とされるのである。
>
> この点について，原判決は，②当該情報にアクセスした者につき，それが管理されている秘密情報であると客観的に認識することが可能であることと並んで，①当該情報にアクセスできる者を制限するなど，当該情報の秘密保持のために必要な合理的管理方法がとられていることを秘密管理性の要件とするかのような判示をしている。しかしながら，上記の不正競争防止法の趣旨からすれば，②の客観的認識可能性こそが重要であって，①の点は秘密管理性の有無を判断する上で重要な要素となるものではあるが，②と独立の要件とみるのは相当でな

い。・・・そうすると・・・本件顧客情報へのアクセス制限等の点において不備があり，大企業としてとるべき相当高度な管理方法が採用，実践されたといえなくても，当該情報に接した者が秘密であることが認識できれば，全体として秘密管理性の要件は満たされていたというべきである。

イ　有用性

（ア）趣旨

「生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報」（不正競争防止法第 2 条第 6 項）という要件は、「公序良俗に反する内容の情報（脱税や有害物質の垂れ流し等の反社会的な情報）など、秘密として法律上保護されることに正当な利益が乏しい情報を営業秘密の範囲から除外した上で、広い意味で商業的価値が認められる情報を保護することに主眼がある」とされる（営業秘密管理指針 16 頁～17 頁）。

（イ）ポイント

そこで、「秘密管理性、非公知性要件を満たす情報は、有用性が認められることが通常であり、また、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、また、「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。例えば、過去に失敗した研究データ（当該情報を利用して研究開発費用を節約できる）や、製品の欠陥情報（欠陥製品を検知するための精度の高い AI 技術を利用したソフトウェアの開発には重要な情報）等のいわゆるネガティブ・インフォメーションにも有用性は認められる」とされる。

また、特許制度における「進歩性」概念とは無関係であり、「当業者であれば、公知の情報を組み合わせることによって容易に当該営業秘密を作出することができる場合であっても、有用性が失われることはない」とされる（営業秘密管理指針 16 頁～17 頁）。

（ウ）裁判例

元従業員が技術情報等を持ち出したとして争われた事件（大阪高判平成 30 年 5 月 11 日[6]において、控訴人（元従業員）は「ほとんどが古い情報であり，秘匿の必要性も有用性もない」と主張して争ったが、控訴審は、「情報が古いといっても，同種事業を営もうとする事業者にとっては有用であり，有用性を認めることができる」と判示した。

ウ　非公知性

（ア）趣旨

「公然と知られていない」（不正競争防止法第 2 条第 6 項）とは、「一般的には知られておらず、又は容易に知ることができないこと」（営業秘密管理指針 17 頁～18 頁）を意味する。

（イ）ポイント

非公知性要件は、「発明の新規性の判断における「公然知られた発明」（特許法第 29 条）の解釈と一致するわけではない」ため、混同しないことが肝要である（営業秘密管

[6] http://www.courts.go.jp/app/files/hanrei_jp/912/087912_hanrei.pdf

理指針 17 頁～18 頁)。

また、「ある情報の断片が様々な刊行物に掲載されており、その断片を集めてきた場合、当該営業秘密たる情報に近い情報が再構成され得る」としても「どの情報をどう組み合わせるかといったこと自体に価値がある場合は」「組み合わせの容易性、取得に要する時間や資金等のコスト等を考慮し、保有者の管理下以外で一般的に入手できるかどうかによって」非公知性を判断することになる（同)。

（ウ）裁判例

投資用マンション顧客情報事件（知財高判平成 24 年 7 月 4 日[7]）の控訴審において、一審被告らは、「顧客の氏名や住所，電話番号，勤務先名・所在地が登記事項要約書や NTT の番号案内，名簿業者，インターネットから容易に入手することができる」と主張して非公知性を争ったが、控訴審は、「本件顧客情報は，単なる少数の個人に係る氏名等の情報ではなく，1 審原告ネクストの販売する投資用マンションを購入した約 7000 名の個人に係る氏名等の情報であって，そのような情報を登記事項要約書や NTT の番号案内，名簿業者，インターネットで容易に入手することができないことは明らかである」と判示して、有用性とともに非公知性を認めた。

加えて、同事件において、一審被告らは、氏名や連絡先を記憶し、またはその一部を記憶していた情報に基づいてインターネット等を用いて連絡した顧客が多数であるから、自らが「利用した 51 名というごく一部の顧客に関する情報については有用性及び非公知性について事案に即した判断をしていない」と主張したが、控訴審は、「上記 51 名が上記約 7000 名の顧客に含まれるものであり，当該約 7000 名の顧客情報（本件顧客情報）に有用性及び非公知性が認められる以上，当該 51 名について個別に有用性又は非公知性について論ずる必要はない」とも判示した。

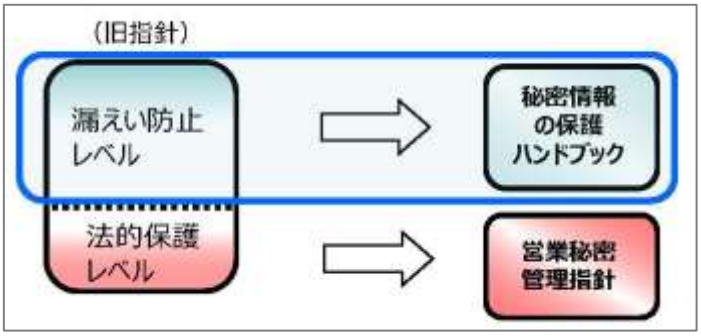
（４）「営業秘密」として認められるための情報管理について

上記（３）に記載の 3 要件を満たす情報管理が、「営業秘密」として認められるための情報管理（営業秘密管理）である。

営業秘密管理の詳細については、不正競争防止法によって差止め（使用・開示の停止・中止の請求または削除の請求など）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を示す営業秘密管理指針を参照されたい。

図 1　不正競争防止法に基づく法的保護を受けるための情報管理のレベルと漏えい防止のための情報管理のレベルとの違い[8]

[7] http://www.courts.go.jp/app/files/hanrei_jp/439/082439_hanrei.pdf
[8] 前掲注 1・不正競争防止法テキスト 67 頁より抜粋。



このような営業秘密管理を行うことで、セキュリティリスクの低減につながる。また、内部不正といった相手方を特定し得るサイバーセキュリティインシデントが生じた場合には、営業秘密侵害罪（同法第 21 条第 1 項各号等）に該当すれば刑事罰も含めた厳正な対処を求めることができる。

もっとも、上記（2）のとおり、不正競争防止法に基づく法的保護は「営業秘密」の漏えい後に受けられるものであることから、営業秘密管理は、サイバーセキュリティインシデント発生後に事後的な措置を取り得ることを目的とした情報管理といえる。さらには、相手方（被疑侵害者）を特定することが困難なサイバー攻撃のような場面ではこれら民事的措置や刑事的措置を取り得ることは極めて難しい。

そこで、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）包括的対策については、平成 28 年 2 月に公表された「秘密情報の保護ハンドブック」が参考となる[9]。秘密情報保護ハンドブックは、場所・状況・環境に潜む「機会」が犯罪を誘発するという犯罪学の考え方なども参考としながら、秘密情報の漏えい要因となる事情を考慮し、下記図 2 に挙げられる 5 つの「対策の目的」を設定した上で、それぞれに係る対策を提示するものである（同書 17 頁～18 頁）[10]。なお、秘密情報保護ハンドブックの概略版である「秘密情報の保護ハンドブックのてびき」も公表されている[11]。

図 2　秘密情報の保護ハンドブックの概要[12]

[9] 前掲注 1・両者の違いについては、不正競争防止法テキスト 21 頁がわかりやすい。
[10] なお、「既に、改訂前の営業秘密管理指針や ISMS などの考え方を参考に、秘密情報の漏えい対策を実施している」場合については、「その全てを一から検討し直す必要はないと考えられますが、対策の更なる水準の向上や、対策の遺漏のチェックなどを行う際に、本書をお役立てください」とされる（秘密情報保護ハンドブック 5 頁）。
[11] 経産省 Web サイト「営業秘密～営業秘密を守り活用する～」（https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html）参照。
[12] 前掲注 1・不正競争防止法テキスト 68 頁より抜粋。

加えて、サイバーセキュリティ対策としては、Q18 も参照されたい。

また、技術等情報の適切な管理に係る認証制度の開始に伴い公示された認証基準（Q54 参照）も、技術等情報の漏えい防止の対策をまとめている。

さらに、「営業秘密」として認められるための情報管理を行う対象の情報に個人情報が含まれる場合については、個情法が個人情報取扱事業者に対して安全管理措置を講ずることを求めている。詳細については Q6～Q12 を参照されたい。

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 6 項
・営業秘密管理指針
・秘密情報保護ハンドブック
・逐条不正競争防止法

４．裁判例

本文中に記載のとおり

Q18 営業秘密管理とサイバーセキュリティ対策との異同

不正競争防止法に基づく営業秘密としての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は、どのような点で異なり、どのような点で共通するか。

タグ：不正競争防止法、営業秘密管理、情報管理、内部統制システム、リスクマネジメント、コンプライアンス

１．概要

不正競争防止法に基づく営業秘密としての法的保護を受けるための情報管理も、サイバーセキュリティ対策としての情報管理も、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。他方で、前者は、企業が秘密として取扱いたい情報が漏えいした後に当該情報について法的保護を受けることを目的とした情報管理であり、後者は、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。

２．解説

（１）不正競争防止法に基づく営業秘密としての法的保護を受けるための情報管理（営業秘密管理）について

ア　概要

営業秘密管理については、Q17 のとおり、企業が秘密として取扱いたい情報へのサイバーセキュリティインシデント発生後に不正競争防止法に基づいて差止め（使用・開示の停止・中止の請求または削除の請求など）等の法的保護、すなわち事後的な措置を取り得ることを目的とした情報管理といえる。

また、当該法的保護の内容は、Q17 のとおり、主に民事的措置（交渉もしくは訴訟提起）または刑事的措置であるから、当該保護を受けるためには、交渉の場合は相手方、訴訟提起の場合は裁判所、捜査の段階においては警察または検察官に、漏えいしたまたは漏えいしそうになっている秘密情報が「営業秘密」であると認めてもらうことに加えて、そもそも被疑侵害者（被告または被疑者）をある程度特定する必要が生じる。

よって、サイバー攻撃のような、被疑侵害者の特定が技術的に困難なサイバーセキュリティインシデントや、交渉・裁判をしようとしても被疑侵害者に応じてもらえないような場合については、不正競争防止法に基づく法的保護を受けることは極めて困難であるといえる。

他方で、サイバーセキュリティインシデントのうち、内部不正（従業員・役員による秘密情報の不正な持ち出し等）のように、被疑侵害者を特定することが可能な場合に、企業のガバナンスとして、被疑侵害者を相手に交渉や訴訟提起をする、または、被疑侵

害者への厳正な処分（刑事的処置）を求めようとするならば、裁判所等において漏えいしたまたは漏えいしそうになっている秘密情報が「営業秘密」であると認めてもらう必要があるため、営業秘密管理が活かされるといえる。

なお、刑事的措置については、営業秘密侵害罪の主観的要件として、故意に加えて、「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」（図利加害目的。不正競争防止法第 21 条第 1 項各号）が必要となる。この目的要件は、処罰範囲を明確に限定するため、違法性を基礎づけるものである[1]。

そこで、刑事的措置においては、被疑侵害者の行為に、故意に加えて、図利加害目的が認められるかという論点が生ずる。

図利加害目的について参考になる裁判例としては、近時、最高裁（最決平成 30 年 12 月 3 日刑集 72 巻 6 号 569 頁）が、営業秘密侵害罪の「不正の利益を得る目的」[2]について以下のとおり判示している。

> 被告人は，勤務先を退職し同業他社へ転職する直前に，勤務先の営業秘密である・・・の各データファイルを私物のハードディスクに複製しているところ，当該複製は勤務先の業務遂行の目的によるものではなく，その他の正当な目的の存在をうかがわせる事情もないなどの本件事実関係によれば，当該複製が被告人自身又は転職先その他の勤務先以外の第三者のために退職後に利用することを目的としたものであったことは合理的に推認できるから，被告人には法 21 条 1 項 3 号にいう「不正の利益を得る目的」があったといえる。

なお、民事的措置の対象となる不正競争についても、一部、図利加害目的を要件とするものがあるが（不正競争防止法第 2 条第 1 項第 7 号～第 10 号）、刑事事件で示された上記最高裁の考えが民事事件においても妥当するか現時点では定かではない。

イ　対策の内容

営業秘密管理の内容については、Q17 のとおり、営業秘密管理指針において紹介されている。

対策のポイントは、以下のとおりである。

- 営業秘密保有企業の秘密管理意思（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（営業秘密管理指針 6 頁）
- 秘密管理措置は、対象情報（営業秘密）の一般情報（営業秘密ではない情報）からの合理的区分と当該対象情報について営業秘密であることを明らかにする措置とで構成される（同 7 頁）。

---

[1] 図利加害目的の趣旨等については、逐条不正競争防止法 256 頁～258 頁も参照されたい。
[2] なお、正確には、平成 27 年改正前の不正競争防止法第 21 条第 1 項第 3 号に規定される「不正の利益を得る目的」についての判示である。

- 従業員に対する「対象情報について営業秘密であることを明らかにする措置」として、一般的には、社内規程または就業規則において、情報の漏えい禁止に関する一般的な義務規定や情報の管理の具体的手法等を定め、また、入社時、異動時、プロジェクト参加時・終了時、退社時等、対象情報の変動や具体化に合わせて、認識可能性を確保するための誓約書等の書面を取得し、適時、教育・研修を行って認識可能性を高めるといった措置が取られている（秘密情報保護ハンドブック参照）。
- 別法人に対する「対象情報について営業秘密であることを明らかにする措置」として、一般的には、対象情報を特定した守秘義務契約または守秘義務規定を含む契約を締結し、開示する文書へのマル秘表示を行うといった措置が取られている（営業秘密管理指針 14 頁～16 頁）。

（２）サイバーセキュリティ対策としての情報管理について

ア　概要

サイバーセキュリティ対策は、「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及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み」て「積極的に対応することを旨として」行われるものである（サイバーセキュリティ基本法第 3 条第 1 項（基本理念）参照）。

すなわち、サイバーセキュリティ対策としての情報管理は、「サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務」（経営ガイドライン I 頁）であることから実施されるものである。

加えて、サイバー攻撃においては「攻撃の踏み台」にされたり「国民の社会生活に重大な影響を及ぼす可能性のある攻撃」を受けたりすることから（経営ガイドライン 1 頁）、サイバーセキュリティ対策の実施は、「経済社会の活力の向上及び持続的発展」（サイバーセキュリティ基本法第 1 条）に資するものであり、ひいては「我が国の安全保障」への寄与（同条）にもつながるものである。

イ　対策の内容

サイバーセキュリティ対策としての情報管理の詳細については、以下のとおり、参考となる資料が提供されている。

- 経営ガイドライン
- 経営ガイドラインの実践に関する国内の実践事例を取りまとめたものとして、IPA「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集」（2019 年 3 月）

また、中小企業自らがセキュリティ対策に取り組むことを宣言する制度（SECURITY

ACTION、IPA）[3]も創設されている。

加えて、子会社を保有しグループ経営を行う企業については、グループ全体の企業価値向上を図るためのガバナンスの在り方として、内部統制システムの一要素として、「サイバーセキュリティについて、グループ全体やサプライチェーンも考慮に入れた対策の在り方が検討されるべきである」とされている（グループガイドライン 92 頁～94 頁[4]。

（３）共通点・相違点について

ア　共通点

（ア）　情報管理であること

営業秘密管理も、サイバーセキュリティ対策としての情報管理も、いずれも情報管理という点で共通する。

このため、ある対策を見たときに、営業秘密管理として行われている側面と、サイバーセキュリティ対策として行われている側面とが見て取れることも多く、また、情報管理における部門間連携や組織横断的な管理体制が望ましいといわれる。

（イ）　管理の対象となる情報の種類

管理の対象となる情報の種類についても、自社が保有する情報、取引先等の他者から提供を受けた情報、協業事業や共同開発等において他者と共同で保有する情報や、社内社外の個人の個人情報まで多種多様であり共通する。

（ウ）　リスクマネジメントであること

いずれも、リスクベースドアプローチに基づいて、限られたリソースの最適配分をどのようにすべきかという観点で行われる、リスクマネジメントである（Q1 参照）。

イ　相違点

（ア）　管理対象となる情報の範囲・秘密管理意思の有無

営業秘密管理においては、営業秘密の要件（秘密管理性、有用性、非公知性）を満たす情報が管理の対象となるのに対し、サイバーセキュリティ対策としての情報管理においては、そのような秘密管理意思の有無に関係なく、サイバーセキュリティリスクが懸念される情報が管理対象となる。

（イ）　漏えい対策か、漏えい・滅失・毀損対策か

不正競争防止法に基づく法的保護が不正取得、不正開示、不正使用を規制していることからわかるように、営業秘密管理は、主に情報の「漏えい」対策に焦点が当てられる。これに対し、サイバーセキュリティ対策としての情報管理においては、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（第 2 条）に「情報の漏えい、滅失

[3] https://www.ipa.go.jp/security/security-action/

[4] グループガイドラインにおいて、グループとは「株式会社、その親会社・子会社から成る企業集団」を指す（会社法施行規則第 100 条第 1 項参照）（グループガイドライン 12 頁）。

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」とあるとおり、情報の「漏えい」「滅失」「毀損」のいずれについても防止しようとするものである[5]。

（ウ） 攻めか守りか

不正競争防止法に基づく法的保護の内容からわかるとおり、営業秘密管理は、不正競争行為に対する事後的な「攻め」を主眼として行う情報管理であるといえる。そのため、営業秘密管理は、法的保護を求めることを念頭に、どのようにすれば立証できるか、どのようにして立証すべきかといった観点を考慮して行われる。

他方で、サイバーセキュリティ対策としての情報管理は、サイバーセキュリティリスクの回避や低減を図るものであり、「守り」のための情報管理であるといえる。

３．参考資料（法令・ガイドラインなど）

・営業秘密管理指針
・秘密情報保護ハンドブック
・経営ガイドライン
・IPA「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集」
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

４．裁判例

特になし

[5] もちろん、営業秘密管理は主に情報の「漏えい」対策に焦点を当てるといっても、秘密情報の滅失または毀損の事実をもって、営業秘密の不正取得・使用・開示の痕跡であるとして、裁判等で争うことは考えられる。

Q19 委託元と営業秘密

従業員や委託先企業が作成や取得に関与した顧客リストや技術情報などの秘密情報について、雇用会社や委託元会社は、営業秘密としての保護を受けることができるのか。

タグ：不正競争防止法、独占禁止法、雇用、委託、営業秘密、従業員、営業秘密保有者

１．概要

従業員や委託先企業が作成や取得に関与した情報であっても、その情報を雇用会社や委託元会社が秘密として管理するに至ったときには、その情報は雇用会社又は委託元会社の営業秘密として不正競争防止法により保護され得る。

２．解説

従業員や委託先企業が自ら作成や取得に関与した情報であっても、雇用契約又は業務委託契約において、労務の提供として又は委託業務の履行として作成又は取得された情報については、雇用会社又は委託元会社が当該情報の保有者となり、当該会社の企業秘密として管理する旨が合意されている場合が多い。

このような合意は、雇用会社又は委託元会社が当該情報を営業秘密として管理する意思を示しているものと解される。

よって、その情報が雇用会社又は委託元会社の業務において用いるために整理されるなど、雇用会社又は委託元会社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、雇用会社又は委託元会社が、営業秘密を保有する事業者として「営業秘密保有者」[1]に該当し得るものと考えられる。

そして、従業員や委託先企業が自ら作成や取得に関与した情報であっても、このように、雇用会社や委託元会社が営業秘密保有者に該当する場合には、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」者に該当するため、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で、営業秘密を使用又は第三者に開示した場合には、当該行為は、不正競争防止法第 2 条第 1 項第 7 号所定の不正競争に該当する。

もっとも、従業員に関しては、あらゆる情報を会社の管理下において一切退職後は使用できないとすることは、転職の自由との関係で問題がある。したがって、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。（なお、従業員に退職後の秘密保持義務を課すための秘密保持契約については Q31 から Q34 までを参照）。

[1] 営業秘密を保有する事業者（不正競争防止法第 2 条第 1 項第 7 号参照）。「営業秘密保有者」という用語は、平成 30 年不正競争防止法改正により導入された。

委託先企業についても、基本的には同様に、秘密として管理すべき情報を具体的に選別して特定した上で秘密保持義務を負わせることが実効性のある秘密保持契約として望ましいと考えられるが、転職の自由を配慮する必要性がない点において従業員の場合とは異なると考えられる。

なお委託元会社（ライセンサー）は、業務委託にともなって委託先企業（ライセンシー）に技術をライセンスする際、秘密保持契約において、委託先企業の事業活動に関して一定の制限を課すことがあるが、当該制限が公正競争阻害性を有する場合には、当該制限は独占禁止法上の不公正な取引方法に該当し得るため、留意が必要である（知的財産の利用に関する独占禁止法上の指針第 4-4 参照）。また、片務的な秘密保持契約についても、場合によっては優越的地位の濫用行為に該当することもあり得るため、留意が必要である（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）。

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
・営業秘密管理指針
・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））
https://www.jftc.go.jp/dk/guideline/unyoukijun/chitekizaisan_files/chitekizaisangl.pdf
・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）
https://www.jftc.go.jp/houdou/pressrelease/2019/jun/190614_files/houkokusyo.pdf

４．裁判例

・札幌地判平成 6 年 7 月 8 日（平 6（モ）725 号）
・東京地判平成 14 年 2 月 5 日判時 1802 号 145 頁・判タ 1114 号 279 頁
・東京高判平成 15 年 3 月 31 日（平 14（ラ）1302 号）
・東京高判平成 16 年 9 月 29 日判タ 1173 号 68 頁
・東京高判平成 18 年 2 月 27 日（平 17（ネ）10007 号）

Q20 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、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また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）制度趣旨

「限定提供データ」の制度は、データが企業の競争力の源泉としての価値を増す中で、データの創出、収集、分析、管理等の投資に見合った適正な対価回収が可能な環境を整備すべく、データを安心して提供できるように、限定提供データの不正取得行為等に対して法的措置を取れるようにしたものである（限定提供データ指針 4 頁参照）。平成 30 年改正不正競争防止法により新しく導入され、令和元年 7 月 1 日に施行された。

（２）「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（秘密として管理されているものを除く。）」と定義される（不正競争防止法第 2 条第 7 項）。

すなわち、「技術上又は営業上の情報（秘密として管理されているものを除く。）」が以下の要件を満たせば、「限定提供データ」に該当する。各要件等の詳細な解説については、「限定提供データ指針」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）

[1] 経産省「不正競争防止法等の一部を改正する法律案の概要」（平成 30 年 2 月、https://www.meti.go.jp/press/2017/02/20180227001/20180227001-1.pdf）。なお、中間報告や新旧対照表は、右記 Web 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）。

- 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）

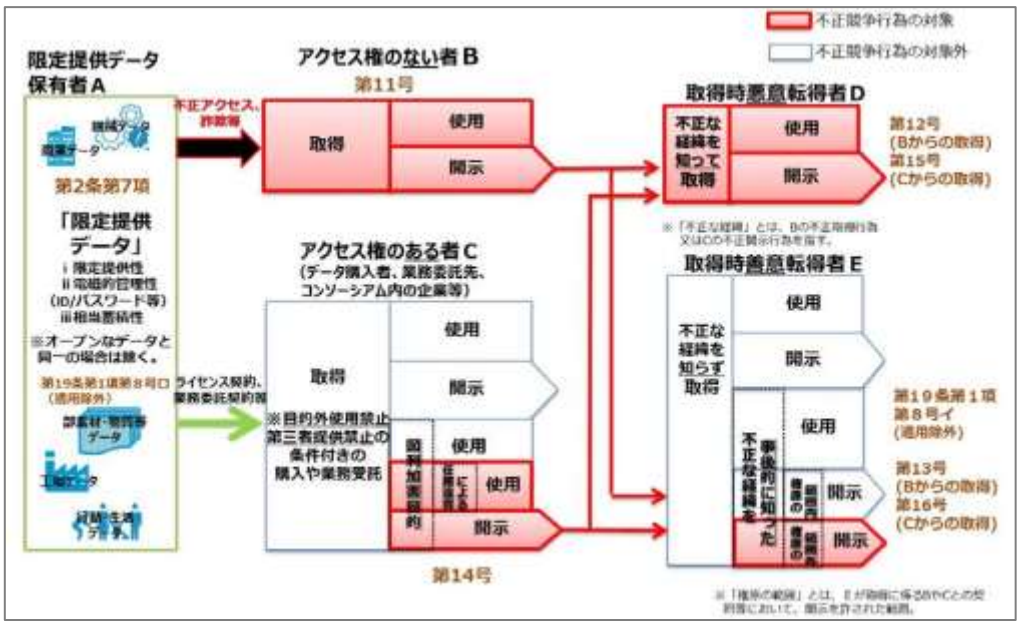
なお、限定提供データが無償で公衆に利用可能となっている情報（オープンなデータ）と同一の情報である場合には、当該情報の不正取得・使用・開示行為については不正競争に該当しない（不正競争防止法第 19 条第 1 項第 8 号ロ[2]）。

（３）法的保護の内容

限定提供データの不正取得・使用・開示行為等の「不正競争」に対しては、差止請求また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）。なお、「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」かねないことから刑事的措置（刑事罰）は設けられていない（限定提供データ指針 4 頁）。

どのような「不正競争」について差止請求または損害賠償請求をなし得るかについて、模式的に整理したものが下記図 1 である。赤く塗られた行為が、対象となり得る「不正競争」である。なお、限定提供データに関する不正競争は、不正競争防止法第 2 条第 1 項第 11 号から第 16 号に規定されているため、下図における「第 11 号」等の数字は、これら条文番号を指す。

図 1　限定提供データに関する不正競争（限定提供データ指針 5 頁）



上記図からもわかるとおり、不正競争の要件として、図利加害目的や不正な経緯を事後的に知ったことといった主観的要件が加重されているので、差止請求または損害賠償請

[2] 不正競争防止法第 19 条第 1 項第 8 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。

求を検討するときには、これら主観的要件も立証できるかといった検討が必要となる。

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）が、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 20 頁）。

（４）「限定提供データ」と「営業秘密」の違いについて

限定提供データは、上記（１）のとおり、データの創出や分析等に投資した者が「データを安心して提供」して、当該「投資に見合った適正な対価回収」をしようとすること、すなわち、他者にデータを提供して利用させることを念頭に置いた制度であるといえる。

他方で、営業秘密は、他者に情報を提供して利用してもらい投資回収をすることを念頭に置いているのではなく、秘密として管理し、利用することに価値がある情報を念頭に置いた制度であるといえる[3]。

そこで、不正競争防止法第 2 条第 7 項は、『このような「営業秘密」と「限定提供データ」の違いに着目し、両者の重複を避けるため、「営業秘密」を特徴づける「秘密として管理されているもの」を「限定提供データ」から除外する』旨を規定する（限定提供データ指針 12 頁～14 頁）。

たとえば、あるデータにアクセスするためには ID・パスワードが必要となるという措置が実施されている場合、限定提供データ指針によれば、

① 当該措置が秘密として管理する意思に基づくものであり、当該意思が客観的に認識できるとき
→「秘密として管理されているもの」に該当する
（⇒有用性及び非公知性を満たせば「営業秘密」に該当する）

② 当該措置が対価を確実に得ること等を目的とするものにとどまり、その目的が満たされる限り誰にデータが知られてもよいという方針の下で施されているとき
→「秘密として管理されているもの」に該当しない

[3] 営業秘密の法的保護の沿革は、TRIPS 協定第 39 条の担保にある（営業秘密管理指針 3 頁～4 頁）。同条は、「合法的に自己の管理する情報」のうち「秘密であることにより商業的価値がある」もの等の一定の要件を満たす情報の不正開示等の防止ができるように保護すべきことを加盟各国に対して求めている。よって、営業秘密の制度は、秘密として管理し、利用することに価値がある情報を念頭に置いたものであるといえる。

なお、TRIPS 協定（知的所有権の貿易関連の側面に関する協定）とは、国際的な自由貿易秩序維持形成のための知的財産権の十分な保護や権利行使手続の整備を加盟各国に義務付けることを目的とした多国間協定である。WTO の規定によって加盟各国は本協定に拘束され、本協定の内容は加盟各国の法律に反映される。（外務省、https://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/trips.pdf）

（⇒他の要件を満たせば「限定提供データ」に該当する）

というように考えられる（限定提供データ指針 13 頁）。

（５）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について

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。たとえば、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 10 頁～11 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 11 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、上記（１）記載のとおり、限定提供データの不正取得等の不正行為が生じた後にまた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また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を利用しての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 8 号ロ
・限定提供データ指針
・営業秘密管理指針

４．裁判例

特になし

Q21 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、も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、また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

著作権法または不正競争防止法に基づく法的責任が生じ得るが、サイバーセキュリティ技術の開発の目的等で技術的手段を回避したり無効化したりする場合には、これら二つの法律に基づく法的責任は生じない。

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）をまとめて、「技術的手段」と呼ぶ[1、2]。

（２）沿革

ア　導入の経緯について

平成 11 年に著作権法と不正競争防止法を改正して、技術的手段の保護に関する制度が創設された。

我が国が著作権に関する世界的所有権機関条約（WIPO 著作権条約、WCT）及び、実演及びレコードに関する世界知的所有権機関条約（WIPO 実演・レコード条約、WPPT）に加入するにあたり、両条約が著作権等を保護するための効果的な技術的手段に対する適当な法的保護を加盟各国に義務づけていたからである。

---

[1] 逐条不正競争防止法 115 頁・脚注 124（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20190701Chikujyou.pdf）。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。

[2] 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。

イ　著作権法と不正競争防止法の二つの法律で対応した経緯について

平成 11 年当時、技術的手段としては、大きく分けると、①著作権等の支分権の対象となる行為を制限する技術（いわゆるコピーコントロール技術：CC）と、②著作権等の支分権の対象外の行為（コンテンツの視聴やプログラムの実行など）を管理する技術（いわゆるアクセスコントロール技術：AC）の二種類が存在した。そこで、CC については著作権法で保護し、AC については不正競争防止法で保護することとされた。

こうして、著作権法は、技術的保護手段を定義し、これを回避する行為等を規制することとなり、不正競争防止法は、技術的制限手段を定義し、これを無効化する装置等の譲渡等の行為を規制することとなった。

ウ　近時の法改正について

著作権法においては、まず平成 24 年改正により、技術的保護手段の対象に、著作物等の利用に用いられる機器が特定の変換を必要とするよう著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、又は送信する方式（暗号方式）が加えられ、また、いわゆる TPP11 協定[3]に対応する改正において、「従前の技術的保護手段に加え，アクセスコントロール機能のみを有する保護技術について，新たに『技術的利用制限手段』を定義した上で，技術的利用制限手段を権原なく回避する行為について，著作権者等の利益を不当に害しない場合を除き，著作権等を侵害する行為とみなして民事上の責任を問いうることとするとともに，技術的利用制限手段の回避を行う装置やプログラムの公衆への譲渡等の行為を刑事罰の対象」とした（平成 30 年 12 月 30 日施行）[4]。

不正競争防止法も、以下の図 1 のとおり技術的制限手段の保護範囲を拡大した（平成 30 年 11 月 29 日施行）[5]。図 1 右端の「最新のプロテクト技術について明確化」とは、技術的制限手段の従前の要件である「影像、音若しくはプログラムとともに」という規定ぶりが、特定の反応をする信号をコンテンツ等の記録・送信と同時に行うことを意味するとも解釈されていたところ、近時急速に普及しているアクティベーション方式等では、前記要件を満たさないのではとの疑義が生じることを踏まえ、アクティベーション方式等も技術的制限手段に含まれることを明確化するために、当該要件を削除

---

[3] TPP11 協定とは、環太平洋パートナーシップに関する包括的及び先進的な協定をいう。当該協定の内容等詳細については、内閣官房 TPP 等政府対策本部 Web サイト（http://www.cas.go.jp/jp/tpp/tpp11/index.html）を参照。

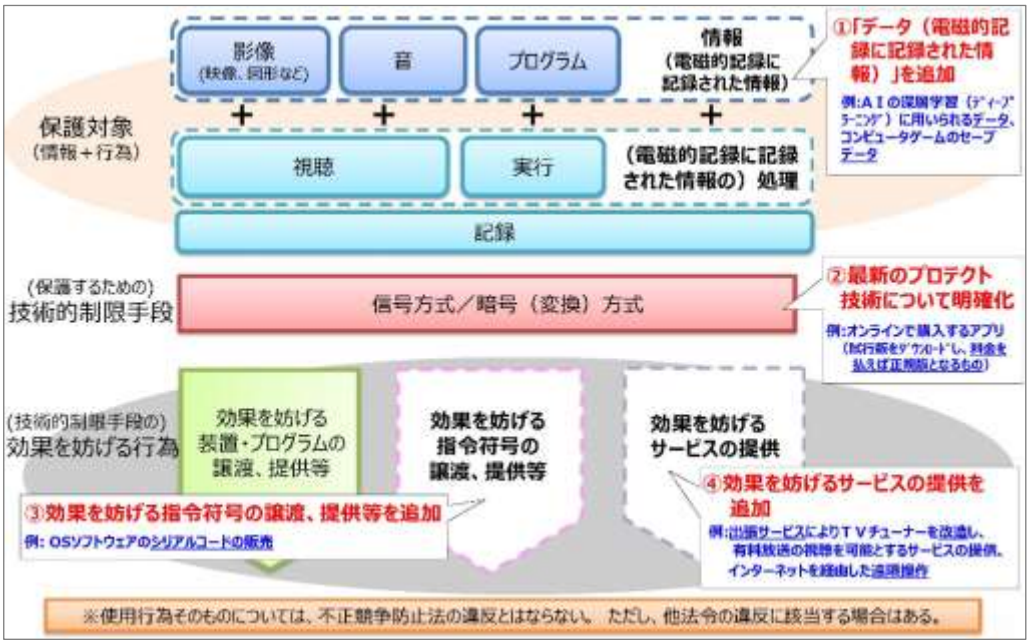
[4] 文化庁「環太平洋パートナーシップ協定の締結に伴う関係法律の整備に関する法律（平成 28 年法律第 108 号）及び環太平洋パートナーシップ協定の締結に伴う関係法律の整備に関する法律の一部を改正する法律（平成 30 年法律第 70 号）について」（http://www.bunka.go.jp/seisaku/chosakuken/hokaisei/kantaiheiyo_hokaisei/）

[5] 技術的制限手段の定義（不正競争防止法第 2 条第 8 項）の構造及び規制対象行為（同条第 1 項第 17 号・第 18 号）の構造については、「不正競争防止法テキスト」38・39 頁（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/201909_unfaircompetitiontext.pdf）がわかりやすい。

したということを意味する。

なお、この不正競争防止法改正を受け、著作権法においても、「技術的保護手段」や「技術的利用制限手段」の定義規定においてアクティベーション方式が含まれることを明確化すること、また、不正な指令符号（シリアルコード等）の提供等を新たに規制対象とすることが適当である旨が「文化審議会著作権分科会報告書」（2019 年 2 月）[6]において取りまとめられており、今後これに基づく法改正が行われる見込みである。

図 1　技術的制限手段の効果を妨げる行為に対する規律の強化[7]



（３）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、主な相違点をまとめると、以下のとおりである。

図 2　技術的手段に関する両法における保護の主な相違点

	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[8]	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

6 文化審議会著作権分科会「文化審議会著作権分科会報告書」（2019 年 2 月）84 頁～95 頁
7 経産省知的財産政策室「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）」13 頁（https://www.meti.go.jp/policy/economy/chizai/chiteki/H30nen_fukyohoshosai.pdf）
8 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。

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
規制対象行為	「指令符号の譲渡、提供等行為」は規制対象ではない[9]	無効化するための「指令符号」の譲渡、提供等も規制対象である
回避行為・無効化行為後の対象物の利用について	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する行為は複製権侵害となる（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、CC 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

（4）技術的手段の回避行為・無効化行為に関する法的責任

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侵害になり得る（第 30 条第 1 項第 2 号）	回避行為がみなし侵害行為（第 113 条第 3 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。
刑事上の責任	－ 以下の行為について、懲役 3 年以下もしくは罰金 300 万円以下または併科 ・ 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		－ 上記行為について、懲役 5 年以下もしくは罰金 500 万円以下または併科（第 21 条第 2 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

[9] 前述のとおり平成 30 年の不正競争防止法改正を受けて、著作権法においても不正な指令符号（シリアルコード等）の提供等を新たに規制対象とすることが適当である旨が「文化審議会著作権分科会報告書」（平成 31 年 2 月）84 頁～95 頁において取りまとめられており、今後これに基づく法改正が行われる見込みである。

	の２第２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）	第１項第３号）

（５）技術・開発目的、試験・研究目的について

著作権法上、技術的利用制限手段の回避行為が「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（第 113 条第３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、または「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限りである（第 120 条の２第１号・第２号）。よって、著作権法上、「公衆」とは、不特定多数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、たとえば、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。

また、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は、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９号）。

よって、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、不正競争防止法上は法的責任を負うことはなく、また、著作権法上も「公衆からの求めに応じて」行うものでない限り、法的責任を負うことはないといえる。

（６）その他法令への抵触の可能性について

以上、技術的手段の回避・無効化に関する行為について不正競争防止法と著作権法の関係を解説したが、その他の法令の関係では、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毀棄罪などにより処罰され得る（詳細は、Q65 参照）。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（詳細は、Q66 参照）、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（詳細は、Q67 参照）、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（詳細は、②と同じく Q67 参照）、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（詳細は、Q70）、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、Q67 及び 68 参照）。

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 11

3 条第 3 項、第 120 条の 2 第 1 号・第 2 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 9 号、第 21 条第 2 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 日最高裁 HP
http://www.courts.go.jp/app/files/hanrei_jp/392/037392_hanrei.pdf
・東京地判平成 25 年 7 月 9 日、知財高裁平成 26 年 6 月 12 日、いずれも最高裁 HP（原審は、http://www.courts.go.jp/app/files/hanrei_jp/447/083447_hanrei.pdf。控訴審は、http://www.courts.go.jp/app/files/hanrei_jp/315/084315_hanrei.pdf。）
・大阪地判平成 28 年 12 月 26 日最高裁 HP
http://www.courts.go.jp/app/files/hanrei_jp/665/086665_hanrei.pdf

Q22 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また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するに過ぎず、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、保護が及ばず、十分とはいえない。

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、データの選択また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、（営業秘密ではない）価値ある重要な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。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）秘密情報の保護

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。また、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。

他方、設計図、模型、写真、製造マニュアル、顧客データベースといった形をとり、著作物性が認められる場合には、これらに著作権や著作者人格権が発生している可能性がある。

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とされることから（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な表現物である必要がある。また、データベースであっても、その情報の選択または体系的な構成によって創作性を有するものは、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、いかに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あいうえお順に並べたものなど、ありふれた構成であった場合には、データベースの著作物としての創作性が認められず、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[1]。

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）LLI/DB 判例秘書登載[2]がある。

秘密情報が著作物として保護される場合、著作者は、公表権を始めとする著作者人格権（同法第 18 条～第 20 条)、複製権を始めとする著作権（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が考えられる。著作権や著作者人格権は、特許権等の、出願して一般に公開しなければならない権利と異なり、その権利取得のために公開が要求されるものではないため、情報を秘匿したまま著作権法で保護することが可能である。

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

[1] 但し、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。

[2] 原審：東京地判平成 26 年 3 月 14 日（平成 21 年（ワ）第 16019 号）LLI/DB 判例秘書登載

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。このため、秘密情報が漏えいし、これが用いられた場合においては、当該秘密情報が著作物として保護される場合であったとしても、著作権は、当該秘密情報に係る表現そのものの公表や複製の差し止め等には有用であるものの、当該秘密情報に含まれるアイデアの活用や、当該秘密情報に基づいた製品やサービスの提供の差し止め等には有用ではないと考えられる。

以上のとおり、著作権法による秘密情報の保護は極めて限定的であるといわざるを得ない。

（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（Q20 参照）。

この点、特許法上、特許権の保護の対象となる発明は、「自然法則を利用した技術的思想の創作のうち高度のものをいう」（特許法第 2 条第 1 項）とされているところ、事業者等が取引等を通じて第三者に提供するデータなど価値ある重要なデータは、データ自体に価値があるとしても、データ自体は「技術的思想」の「創作」には該当しないことが通常であり、特許権の保護の対象となる場合は限定的であると考えられる。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 2 条 4 項）として保護の対象となり得るが、こちらについても、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。

また、前述のとおり、著作権法の保護を受けるためには創作的な表現である必要があるところ、機械稼働データや消費動向データのようにセンサ等の機器により機械的に創出されるデータや、スマートフォン等のユーザの使用履歴等のデータの集合については、そのデータの収集、蓄積及び整理の態様や状況にもよるものの、その情報の選択または体系的な構成による創作性を認めるのが困難な場合もあると考えられる。加えて、前述のとおり、データベースの著作物として保護される場合であったとしても、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公表・複製でない限り、データベースの著作物の公表権侵害や複製権侵害を問えるものではないと考えられる。

このため、価値ある重要なデータは、秘密情報以上に、著作権法等の知的財産権法による保護を図ることは困難であるといわざるを得ない。

（３）契約による保護

このため、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り、これについては別稿（Q41）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 7 項

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
・東京地判平成 12 年 3 月 17 日判時 1714 号 128 頁
・東京地判平成 17 年 11 月 17 日判時 1949 号 95 頁
・大阪地判平成 16 年 11 月 4 日判時 1898 号 117 頁

Q23 セキュリティ上必要となる雇用関係上の措置

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、従業員、就業規則、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あたっては、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。

２．解説

（１）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。

（２）説明

ア　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あ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あたって、特に重要になるのが、就業規則上の規定の整備である。

イ　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前述の労働基準法第 106 条の場合と異なり、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、労働基準法第 106 条による周知の要請が別途存在する以上、企業としては同条所定の方法による周知を心がけるべきである。

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。

第 2 に、判例[1]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あたっては、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（実際に懲戒処分を行うにあたっては、就業規則所定の懲戒処分事由への該当性、懲戒権濫用の成否（労働契約法第 15 条）などが更に問題になる）。

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[2]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順守を求める事項のみを対象とするなど、

[1] 最判平成 15 年 10 月 10 日労判 861 号 5 頁

[2] 情報処理推進機構（IPA）Web 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://www.ipa.go.jp/security/manager/protect/pdca/policy.html

対象範囲が適切となるような検討が必要である。

（イ）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も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。

３．参考資料（法令・ガイドラインなど）

・労働基準法第 89 条、第 90 条、第 106 条
・労働契約法第 7 条、第 10 条、第 12 条

４．裁判例

本文中に記載のとおり

Q24 守秘に関する誓約書の徴収

情報資産の守秘に関する誓約書を従業員から取る意義とは何か、また、取る際にどのようなことを考慮すべきか。

タグ：労働契約法、民法、個情法、不正競争防止法、誓約書、守秘義務

１．概要

誓約書を取る意義としては、在職中、退職後の秘密保持義務を明確化できるということと、サイバーセキュリティに関する法令上の義務の履行ということが挙げられる。

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る。また、誓約書の取得時期のタイミングとしては、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）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、企業秘密遵守の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、契約上の特約また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も明確ではない。そのため、義務の内容を具体化する観点からも、誓約書を取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。

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守秘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っておくことが望ましい。

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 21 条）。

また、例えば情報資産が技術情報であり、当該情報資産につき、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、又は誓約書を取る方法が考えられる。

（２）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[1]。

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[2]。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[3]がある。

イ　誓約書を取得する時期

誓約書を取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ものと考えられる。また、入社時に取った誓約書では、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も、もっとも適切な方法としては、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、Q31 から Q34 を参照。

（３）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

---

[1] 秘密保持誓約書の例として、秘密情報保護ハンドブック 157 頁以下に誓約書例が記載されている。

[2] この点について Q17 も参照。

[3] 奈良地判昭和 45 年 10 月 23 日判時 624 号 78 頁

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にはできない。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。

（４）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。懲戒処分は、「懲戒処分に係る労働者の行為の性質及びその態様その他の事情に照らして、客観的に合理的な理由を欠き、社会通念上相当であると認められない場合には、その権利を濫用したものとして、当該懲戒は、無効」となる（労働契約法第 15 条）からである。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することが必要であり、実際に企業秩序を乱している事情が必要である。

３．参考資料（法令・ガイドラインなど）

・民法第 1 条第 2 項
・労働契約法第 3 条第 4 項、第 15 条
・不正競争防止法 2 条 6 項

４．裁判例

・奈良地判昭和 45 年 10 月 23 日判時 624 号 78 頁
・大阪高判昭和 53 年 10 月 27 日労判 314 号 65 頁
・東京地判平成 15 年 10 月 17 日労経速 1861 号 14 頁
・東京高判平成 29 年 3 月 21 日判タ 1443 号 80 頁

Q25 従業員のモニタリングと個人情報・プライバシー保護

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。

なお、企業が従業員の私用メールや業務用 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

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、あるいは企業が管理する他の情報と容易に組み合わせることで利用者を特定し得るものについては個情法第 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、取得される個人情報の利用目的の特定及びその通知等（同法第 15 条第 1 項、第 18 条）、本人の同意を得ない取得情報の目的外利用の原則禁止（同法第 16 条）、さらに、取得した個人情報が個人データ（同法第 2 条第 4 項）に該当する場合には、本人の同意を得ない取得情報の第三者への提供の原則禁止（第 23 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、個情法との関係では、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 QA の A4-6 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 QA の A4-6 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（労働基準法第 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、就業規則に記載しておくことは望ましいといえる。作成した規程は、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、労働基準法第 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き）

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 23 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（後述「(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」）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、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、おおむ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恐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。

（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。すなわち、このように私的利用が許容されるが故に、法的に許容された私的利用に関する情報が、従業員のプライバシーとして法的保護の対象となり、ひいては企業が行うモニタリング等の措置が、プライバシー侵害の問題を生じさせ得るのである。逆にいえば、仮に、こうした私的利用を禁止することが法的に許容されるとするならば、そのよ

うな措置を徹底し、かつ、電子メール等の利用に関する情報がモニタリングの対象となることを明らかにしておくことで、従業員は電子メール等の利用について、法的に保護されるプライバシーを有しないこととなる。

なお、電子メール等の私的利用の禁止の可否については Q27 を参照。

（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。

３．参考資料（法令・ガイドラインなど）

・個情法 QA
・個情法ガイドライン（通則編）

４．裁判例

本文中に記載のとおり

Q26 私用メール等を禁止・制限する規定と解雇・懲戒処分

企業が従業員の私用メール（企業の電子メールアカウント等を私的なやり取りに利用すること）を禁止し、一定の場合に SNS の利用を禁止または制限する規程を設けることはできるか。また、これに違反したことを理由として、解雇・懲戒を行うことはできるか。

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

１．概要

① 私用メールの禁止について

企業が従業員の私用メールや業務用 PC の私的利用については、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・制限について

企業が一定の場合に SNS の利用を禁止また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 解雇・懲戒を行うことについて

従業員における私用メール等の行為は、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あたっては、あらかじめ私用メール等の規制について定めた規程を作成し、就業規則上で私用メール等規制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）私用メールの禁止について

企業が業務遂行のために従業員に提供する業務用 PC 等の器材・設備及びメールアカウント（以下「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うる。

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。

しかし、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）も極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 PC 等の私的利用を禁止したいという場合には、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・制限について

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）解雇・懲戒を行うことについて

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・懲戒処分の効力を判断すること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 等の私的利用や SNS の利用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 等の私的利用や SNS 利用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うる。

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うる。

以上のとおり、PC 等の私的利用の禁止や SNS の禁止・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また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、規定と実態の乖離を防ぎ、当該規定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 15 条、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
・東京地判平 14 年 2 月 26 日労判 825 号 50 頁
・東京地判平成 15 年 9 月 22 日労判 870 号 83 頁
・札幌地判平 17 年 5 月 26 日労判 929 号 66 頁
・福岡高判平 17 年 9 月 14 日労判 903 号 68 頁
・東京高裁平成 17 年 11 月 30 日労判 919 号 83 頁原判決は、東京地判平成 17 年 4 年 15 日労判 895 号 42 頁）
・東京地判平成 19 年 6 月 22 日労働経済判例速報 1984 号 3 頁
・東京地判平成 19 年 9 月 18 日労働判例 947 号 23 頁

Q27 私物 PC の社内利用、業務用データの社外持ち出し、テレワーク時の注意事項

私物 PC 等の社内持込及び利用禁止を実施する際に、労働法上、どのようなことを考慮すべきか。また、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場合にはどのようなことを考慮すべきか。

タグ：労働基準法、労働契約法、私物 PC、業務用データの社外持ち出し、テレワーク

１．概要

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。

使用者は、就業規則に定めを置くことで、業務用の情報の社外持ち出しを規制することができる。テレワークなど社外における業務を認める場合には、「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン」や「テレワークセキュリティガイドライン（第 4 版）」を参考にすることが望ましい。

２．解説

（１）服務規律の作成

企業は、私物パソコン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あたっては、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。

（２）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

私物パソコン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。

（３）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報にアクセスすることも業務用データの社会持ち出しに該当することに注意する必要がある。

（４）テレワークなど社外における業務を認める場合の考慮事項

テレワーク[1]など社外における業務を認める場合、前提として、業務用データの社外持ち出しを認めることとなる。このため、上記（３）の考慮事項について検討し、就業規則に根拠規定を置いた社内規程等において、実施に関する明確な定めを置く必要がある。

特に、テレワークを実施する場合における社内規程等の内容を検討するにあたっては、次の 2 つのガイドラインを参考にすることが望ましい。

まず、厚生労働省は、平成 30 年 2 月に、「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン」を策定している。同ガイドラインでは、テレワークにおける適切な労務管理の留意点を明らかにするとともに、長時間労働の対策例等を示している。

また、総務省では、平成 30 年 4 月に、「テレワークセキュリティガイドライン（第 4 版）」を策定している。同ガイドラインでは、経営者、システム管理者、テレワーク勤務者という立場に分けて、それぞれが実施すべき対策（情報セキュリティ保全対策の大枠、悪意のソフトウェアに対する対策、端末の紛失・盗難に対する対策、重要情報の盗聴に対する対策、不正侵入・踏み台に対する対策、外部サービスの利用に対する対策）を明示している。セキュリティ上必要となる対策への対応を検討するにあたっては、同ガイドラインを参考にされたい。

---

[1] 厚生労働省「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン」によれば、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うとされており、業務を行う場所に応じた分類として、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等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が挙げられている。

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
・厚労省「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン」（平成 30 年 2 月 22 日）
https://www.mhlw.go.jp/content/000545678.pdf
・総務省「テレワークセキュリティガイドライン（第 4 版）」（平成 30 年 4 月）
https://www.soumu.go.jp/main_content/000545372.pdf

４．裁判例

特になし

Q28 派遣労働者に対する誓約書の要請･教育訓練の実施

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。

タグ：民法、労働者派遣法、派遣労働者、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）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教育訓練を行うことは可能である。

２．解説

（１）労働契約に付随する秘密保持義務等について

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、基本的には派遣元との労働者派遣契約（労働者派遣法第 26 条）において、派遣元・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、派遣元が損害賠償額の支払の責任を負う旨など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について

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）である。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について

派遣先は、派遣労働者の就業に際して、当該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、できるかぎり労働者派遣契約の中に明確化しておいた方がより適切であると思われる。

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
・秘密情報保護ハンドブック

４．裁判例

特になし

Q29 従業員の調査協力、始末書の徴収、教育訓練の実施

情報流出事故を発生させた従業員に対し、調査に協力させたり、始末書を徴収したり、セキュリティ啓発教育を受けさせたりする等の措置をとる際に労働法上考慮すべき事項としてはどのようなものがあるか。

タグ：労働基準法、従業員、情報流出事故、調査協力、始末書、セキュリティ啓発教育

１．概要

（１）従業員の負う調査協力義務

情報流出事故が発生した場合、この事故にかかわる従業員は、調査に協力する義務を負うと考えられる。

（２）始末書の提出

始末書の内容が客観的に状況説明に過ぎないものであれば、業務命令により提出を命ずることができる。これに対して、謝罪の言葉を述べること強制する内容の始末書の提出命令に関しては、懲戒処分となるので、あらかじめこのような始末書提出義務を定める就業規則上の規定が必要である。

（３）教育訓練

業務命令によりセキュリティ啓発教育を受けさせることができる。ただし、その教育内容が、実質的に教育の意味がない見せしめ的なものであるときは、業務命令権の濫用となる。

２．解説

（１）従業員の調査協力

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。

そこで、情報流出事故が発生した場合、この事故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。これに関しても、事故発生の場合に調査があり得る旨をあらかじめ規程において明確にしておく必要がある。

（２）始末書の提出

始末書の内容が状況説明に過ぎないものであれば、業務命令により提出を命ずることができる。これに従わない業務命令違反に対しては、懲戒処分を課すことは可能である。この場合、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、心構え等について、書かせることは、業務命令権の範囲内であるといえ、問題なく行えよう。

これに対して、その内容に「謝罪の言葉を述べること」が含まれる場合には、懲戒の一類型としての始末書の提出となるので、これを義務付ける就業規則上の規定が必要である。

ところで、「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。このような危険を冒して「謝らせよう」とあまりに感情的になるよりも、今後二度と同様の事件が生じないよう冷静・客観的に事態を収拾することのほうが得策であろう。

（３）教育訓練

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いわゆる「いじめ」的制裁を含むような場合などは、権利濫用となる。セキュリティ啓発教育に関しても、この点に特にこの点に問題が生じていない限り、命令することは、可能である。

３．参考資料（法令・ガイドラインなど）

・労働基準法第 89 条第 9 号

４．裁判例

・最判昭和 43 年 8 月 2 日民集 22 巻 8 号 1603 頁
・最判昭和 52 年 12 月 13 日民集 31 巻 7 号 1037 頁
・大阪地堺支判昭和 53 年 1 月 11 日労判 304 号 61 頁
・東京地判昭和 42 年 11 月 15 日労民 18 巻 6 号 1136 頁
・東京地判昭和 62 年 1 月 30 日労判 495 号 65 頁
・大阪地判昭和 50 年 7 月 17 日労経速 892 号 3 頁
・高松高判昭和 46 年 2 月 25 日労民 22 巻 1 号 87 頁
・大阪高判昭和 53 年 10 月 27 日労判 314 号 65 頁
・最判平成 8 年 2 月 23 日労判 690 号 12 頁

Q30 従業員に対する解雇、懲戒処分、損害賠償請求等

営業上の秘密の漏えい等のサイバーセキュリティインシデントを発生させた従業員に対し、企業が解雇、懲戒処分、損害賠償請求等を行うことができるのはどのような場合か。

タグ：労働契約法、従業員、解雇、懲戒処分、損害賠償請求

１．概要

従業員が在職中に営業上の秘密の漏えい等を行うことは、原則的には従業員が労働契約の付随義務として負っている秘密保持義務の違反に該当し、企業はこのような従業員に対し、解雇、懲戒処分、損害賠償請求等の法的手段をとり得る。

ただし、具体的な解雇や懲戒処分の効力は、労働法上の判断枠組みに基づいて判断されることになる。

秘密の漏えい等以外のサイバーセキュリティインシデント（例えば、情報の改ざんなど）についても、具体的行為態様に照らして解雇、懲戒処分、損害賠償請求の対象となる場合がある。

２．解説

（１）秘密の漏えい行為等に対する解雇、懲戒処分、損害賠償請求

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、それぞれの効力を判断する労働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分を行うことが必要であるほか、ここでも、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会社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・情報管理のために会社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 27 日労判 858 号 57 頁）などが存在する。

（２）営業上の秘密の漏えい行為等以外のサイバーセキュリティインシデント

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 17 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。

３．参考資料（法令・ガイドラインなど）

・労働契約法第 15 条、第 16 条など

４．裁判例

本文中に記載のとおり

Q31 退職後の従業員の競業避止義務、秘密保持義務

企業が、従業員が退職後に他社に転職するなどして会社の秘密情報を流出させることを防止しようとする場合、雇用関係上の対策としては、どのようなものを講じることが考えられるか。

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

１．概要

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定めを整備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 退職後の従業員に秘密保持義務を課す定め
② 退職後の従業員に競業避止義務を課す定め
③ 従業員が退職後に競業行為を行った場合に、支給される退職金の額を減らす又は支給しない（既に退職金が支給されている場合、その全部又は一部を返還させる）旨の定め

ただし、これらの定めは、常に有効と判断されるとは限らない。各定めの有効性等は、それぞれ異なる枠組みの下で判断され（①につき Q32、②につき Q33、③につき Q35）、認められ得る効力も異なる。そこで企業としては、それぞれの定めの特質を考慮しつつ、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ことになる。

①②のタイプの定めを設けようとする場合、当該定めは、従業員との間の個別合意という形態をとるべきである（就業規則に規定を置くことも考えられるが、その場合もこれと併せて個別合意を結んでおくべきである）。③のタイプは、退職金制度を定める規程の中に当該定めを置くことになる。

これらの定めを設けていない場合、あるいはこれらの定めに該当しない場合には、従業員が退職後に行う秘密情報の流出行為は、不正競争防止法上の不正競争行為若しくは民法上の不法行為に該当する場合に限って、これらの法律に基づく規制の対象となる。

２．解説

（１）退職後の従業員による秘密情報の流出を防止するための契約上の規制の枠組み

企業が、退職後の従業員による秘密情報の流出を防止しようとする場合、雇用関係上の対応としては、従業員によるこうした行為、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定めを、従業員との間の契約関係の中で定めておく必要がある。従業員は、退職後は自由に職業活動をなし得るのが原則であるため、このような定めがなければ、不正競争防止

法上の不正競争行為[1]や民法上の不法行為に該当し、これらの法律に基づく規制の対象となる場合を除けば、在職中に知り得た元使用者の秘密情報の利用・開示に対する法的な制約は存在しないことになる（退職後の競業避止義務に関する特約の定めなく退職した従業員による退職後の競業行為が不法行為に該当するか否かの判断を行った最高裁判決として、最判平成22年3月25日民集64巻2号562頁。同判決についてはQ33も参照）。

退職後の従業員による秘密情報の流出防止を図るための契約上の定めとしては、次のようなものがある。

第1は、従業員に対して、在職中に知り得た会社の秘密情報を他者に漏らしたり、自ら利用したりしない義務（秘密保持義務）を課すことである。

第2は、従業員に対して、会社の業務と競合する事業を自ら営んだり、このような事業に就職したりしない義務（競業避止義務）を課すことである。このタイプの定めについては、様態として、禁止される行為の内容を、情報漏えいのおそれが類型的に高い行為に限定する形で従業員に義務を課すこと（例えば、従業員に対し、在職中に担当していた顧客への勧誘行為を禁止するなど）も考えられる（このように禁止される行為の範囲が絞り込まれていた方が、当該定めの有効性が認められやすくなる）。

第3は、従業員が第2に挙げた競業行為を行った場合に、支給される退職金の額を減らす、又は支給しない（既に退職金が支給されている場合、その全部又は一部を返還させる）旨を定めることである。

これらのうち、第1と第2の手法をとった場合、企業は、禁止された行為を行った元従業員に対して、当該行為の差止めや、当該行為によって被った損害の賠償の請求をなし得る。

第3の手法をとった場合には、禁止された行為を行った従業員に対しては、退職金の全部又は一部の支払を拒むか、既に支払っていた場合にはその返還を求めることになる。

これら3つの手法を比較すると、まず、第1の手法（秘密保持義務の定め）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、第2の手法（競業避止義務の定め）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、第2の手法は第1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、第1の手法の方が、第2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、第3の手法（退職金の減額等）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。

---

[1] 不正競争防止法では、「秘密管理性」「有用性」「非公知性」の3要件をみたす情報を営業秘密として規律している。詳細は、Q17を参照されたい。

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（各類型の効力等の判断手法の詳細は、第1の手法につき Q32、第2の手法につき Q33、第3の手法につき Q35）。

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。

以下では、こうした諸問題のうち、上記第 1 及び第 2 の定めを設けることの要否及び就業規則において設ける場面で問題になり得る点を取り上げて解説する。

（２）退職後の従業員の競業避止義務、秘密保持義務に関する明示的根拠の要否

従業員（労働者）は、在職中は労働契約の付随義務として、特に明示的な合意がなくとも使用者に対して競業避止義務や秘密保持義務を負っていると解される。

これに対し、こうした労働契約に付随する競業避止義務や秘密保持義務は、従業員の退職後にまで存続するものではなく、したがって、企業が退職後の従業員に対し、契約上の競業避止義務や秘密保持義務を課そうとする場合には、その旨を明示的に定める根拠が原則として必要であるというのが、現在では、裁判例、学説の双方においてほぼ異論のないところである。そこで、企業が退職後の従業員にも契約上の競業避止義務や秘密保持義務を課そうとする場合、その旨を就業規則に定めておく、その旨を定める合意を個々の従業員との間で締結する、等の措置を講じることが望ましい。

（３）就業規則で退職後の従業員の競業避止義務、秘密保持義務を定めることについての問題点

このうち就業規則については、その内容に合理性が認められ、かつ従業員に対して周知されている場合に別段の合意のない限り就業規則の規定が労働契約内容になる（労働契約法第 7 条）ものの、従業員が退職した後についても同様に、退職従業員と企業の間の契約内容を就業規則で定めることができるかは問題となる。裁判例においては、従業員の在職中に退職後の競業避止義務の定めを新設する就業規則の変更が行われた事案において（一般の就業規則変更による労働条件変更の場合と同様に）当該変更の合理性が認められれば退職後の競業避止義務がそれによって定められる旨の判断を示すものが見られ、この点については肯定的に解する傾向にあるといえそうである（大阪地決平成 21 年 10 月 23 日労判 1000 号 50 頁、東京地決平成 7 年 10 月 16 日労判 690 号 75 頁、東京地判平成 15 年 10 月 17 日労経速 1861 号 14 頁など）。

しかし、学説上は就業規則で従業員が退職した後の法律関係を定めることはできないとの見解も有力であること、上記のような裁判例も、裁判実務上の処理基準として確立しているとまでは言いがたいことを考えると、退職後の従業員の競業避止義務、秘密保持義務の定めを就業規則規定のみに依拠して行うことは、少なからぬ法的リスクを伴うというべきであろう。

したがって、このような定めを設ける場合には、（仮に就業規則に規定を設ける場合にもこれとは別に）従業員との間で個別に合意を交わしておくべきである。
このことを前提として、就業規則に（も）規定を設ける場合の留意点としては、次のようなものがある。

まず、就業規則を変更して新たに退職後の秘密保持義務、競業避止義務に関する定めを設ける場合、就業規則変更の合理性（労働契約法第 10 条）が認められるための基準（すなわち、就業規則を変更することで、従業員に退職後の競業避止義務を新たに負わせることが許容されるための基準）は、裁判例上確立しているとは言いがたいものの、退職後の従業員に競業避止義務を負わせる定めの公序良俗違反性（Q33）と概ね同様の判断をする傾向が見られることから、公序良俗違反が否定される場合には、就業規則変更の合理性も肯定される可能性が高いと考えられる（前掲・東京地決平成 7 年 10 月 16 日など）。

次に、就業規則に退職後の従業員の競業避止義務や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）。また、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、裁判例は存在しないが、許容されないと解すべきものと思われる。

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

４．裁判例

本文中に記載したもののほか、

・東京地決平成 7 年 10 月 16 日労判 690 号 75 頁
・東京地判平成 15 年 10 月 17 日労経速 1861 号 14 頁

Q32 退職後の情報漏えい防止のための秘密保持契約

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：不正競争防止法、労働基準法、秘密保持契約、秘密保持義務

１．概要

在職中に、秘密保持義務の対象となる情報を特定し、退職後もその情報について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個別に締結することが望ましい。さらに、従業員のプロジェクトへの参加時など、具体的に秘密情報に接する機会を得る際に、その都度、秘密保持義務の対象となる情報をより具体的に特定し、退職後もその情報について秘密保持義務を継続的に負うことを明示した誓約書をとることが望ましい。

２．解説

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、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（就業規則による退職後の秘密保持義務の有効性については Q31 参照）。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、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営業秘密保持義務は、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[1]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（契約における秘密情報の特定については Q18 参照）。

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

[1] 東京地判平成 17 年 2 月 25 日判時 1897 号 98 頁参照

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[2]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、同条に違反することを否定する方向に向かいつつあると評価する余地があるものの、他法で、違反であるとされる可能性も相当程度存在する状態にあると考えられるため、企業としては、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。

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、第 21 条第 1 項第 3 号・第 5 号
・秘密情報保護ハンドブック

４．裁判例

本文中に記載のとおり

[2] 東京地判平成 14 年 8 月 30 日労判 838 号 32 頁

Q33 退職後の競業避止義務の効力

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。

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

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)によりその全部また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およ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。

２．解説

（１）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、更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また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およ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、秘密情報保護ハンドブック参考資料５に沿って概要を解説する。

（２）裁判例における具体的判断

ア　企業側の守るべき利益

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、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

して判断されることとなる（モップ等のレンタル事業についてこれを肯定した例として、東京地判平成 14 年 8 月 30 日労判 838 号 32 頁など参照）。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

合理的な理由なく従業員すべ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するというよりは、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うえで、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、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、前掲・東京地判平成 14 年 8 月 30 日は、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な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。

（３）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　労働法との関係におけるポイント

◆　就業規則に規定する場合は、個別契約による場合がある旨を規定しておく。

◆　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。

（４）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 頁など参照）も存在する。

３．参考資料（法令・ガイドラインなど）

・民法第 90 条

・秘密情報保護ハンドブック　参考資料５ 競業避止義務契約の有効性について

４．裁判例

本文中に記載のとおり

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、産業競争力強化法、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、懸念国

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）違反もしくは不正競争防止法違反を主張して争う、または営業秘密侵害罪の適用を求めて警察・検察に相談するという措置を取り得る。

もっとも、このようなセキュリティインシデントについては、秘密保持義務契約を反故にされても、技術的また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[1]。そこで、企業では、秘密情報のこのような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・退任または解雇・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。

（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また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、

---

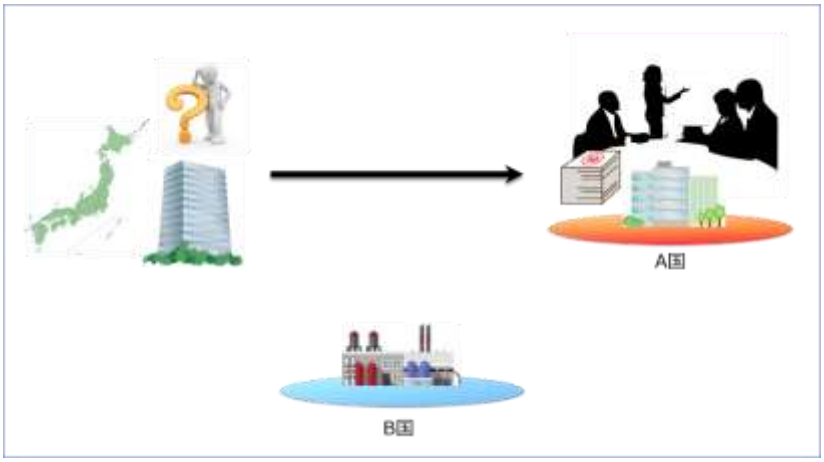
[1] 「平成 24 年度 経済産業省委託調査 人材を通じた技術流出に関する調査研究 報告書」（平成 25 年 4 月。本体は、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/houkokusho130319.pdf。別冊『「営業秘密の管理実態に関するアンケート」調査結果』は、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf。）

[2] なお、誓約書の徴収については Q24 参照。また、退職後の秘密保持義務の効力については Q31 及び Q32 を、退職後の競業避止義務の効力については Q33 を参照されたい。

① 日本で労務提供・職務執行していた場合に、
(i) 日本本社との間で退職・退任前に秘密保持義務契約を締結するとき
(ii) 日本本社との間で退職・退任後に秘密保持義務契約を締結するとき
② 海外（仮にB国とする）の支店において労務提供・職務執行していた場合に、
(i) 日本本社との間で退職・退任前に秘密保持義務契約を締結するとき
(ii) 日本本社との間で退職・退任後に秘密保持義務契約を締結するとき
③ B国にある海外子会社で労務提供・職務執行していた場合に
(i) 海外子会社との間で退職・退任前に秘密保持義務契約を締結するとき
(ii) 海外子会社との間で退職・退任後に秘密保持義務契約を締結するとき

の6つに大きく分類される。

図1 海外における秘密保持義務違反行為の設例の概要



（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、または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]。

---

[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、民事訴訟法および民事保全法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〕」449頁（商事法務、平成26年12月））。
[4] 山田鐐一「国際私法 第3版」2頁（有斐閣、平成16年12月）。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1「国際私法」2頁

我が国における代表的な国際私法としては、法例（明治 31 年法律第 10 号）を全部改定する形で制定された「法の適用に関する通則法」（平成 18 年法律第 78 号。法適用通則法）[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または使用行為を差し止めたり損害賠償を請求しようとする場合、①A 国の裁判所また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、不正開示先または不正使用先（たとえば、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、または 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 国また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・元役員または不正開示先・不正使用先を相手方として、日本の不正競争防止法違反、または 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

---

[6] 法例においては「法律」との文言であったところ、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」66 頁（平成 23 年 12 月、有斐閣））。

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、秘密保持義務違反また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

[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。

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、すで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 条の適用また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・第 8 条）の問題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 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・元役員または不正開示先・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。

---

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「注釈国際私法」275 頁）

9 前掲注 6「注釈国際私法」277 頁

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「逐条解説 法の適用に関する通則法〔増補版〕」108～109 頁）。

11 前掲注 3「逐条解説 法の適用に関する通則法〔増補版〕」232～237 頁）

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）説また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（法例第11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）または（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

---

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。

13 前掲注6「注釈国際私法」450頁

14 前掲注6「注釈国際私法」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「注釈国際私法」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付不競法」（私法判例リマークス59-142）

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Q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。

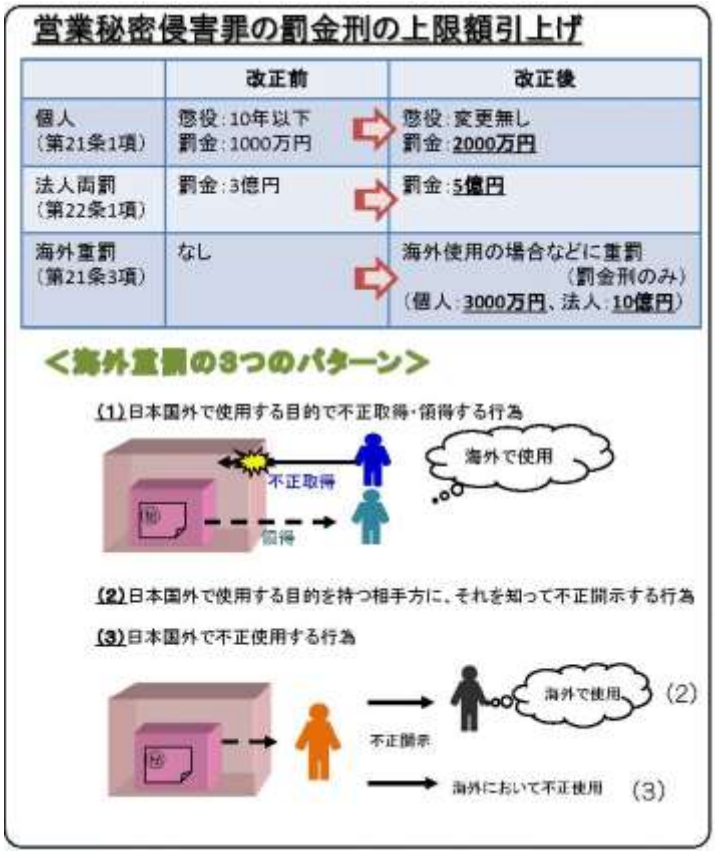
18 なお、上記設例とは逆であるが、日本において技術の不正開示・使用をされたことを理由とする不法行為に基づく損害賠償請求及び当該不正使用行為等の差止請求を認容した米国判決を日本で執行しようとした場合については、最決平成26年4月24日（民集68巻4号329頁）を参照されたい。

19 正しくは、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。

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 6 項）。また、下記図 2 のとおり、海外重罰規定も設けられた（不正競争防止法第 21 条第 3 項。）。

そこで、これら規定の適用を求めて、警察・検察に相談するという手段もある[20]。

図 2　海外重罰規定の内容[21]



（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

---

[20] 都道府県警本部に営業秘密保護対策官が置かれていることについては、Q17 参照。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（経産省知的財産政策室「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）。

[21] 経産省知的財産政策室「平成 27 年不正競争防止法の改正概要（営業秘密の保護強化）」7 頁（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/27kaiseigaiyou.pdf）

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 3 項、第 21 条第 6 項

４．裁判例

本文に記載のとおり

Q35 競業避止義務違反による退職金の減額不支給

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。

タグ：労働基準法、競業避止義務、退職金

１．概要

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。

２．解説

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（したがって、退職金を全額支払わなくても、労働基準法第24条第1項の全額払の原則に違反することにはならない)。

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)。

[1] 菅野和夫『労働法』（弘文堂、第 11 版補正版、平成 29 年）423 頁等参照

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。

３．参考資料（法令・ガイドラインなど）

・労働基準法第 16 条、第 24 条、第 89 条第 3 号の 2

４．裁判例

・最判昭和 52 年 8 月 9 日労経速 958 号 25 頁
・名古屋高判平成 2 年 8 月 31 日労判 569 号 37 頁
・大阪高判平成 10 年 5 月 29 日労判 745 号 42 頁
・名古屋地判平成 6 年 6 月 3 日労判 680 号 92 頁

Q36 電気通信事業者に関する規律の概要

どのような事業を行うと電気通信事業者に該当するか。電気通信事業者はどのような義務を負うか。

タグ：電気通信事業法、電気通信事業参入マニュアル、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、電気通信役務、電気通信設備、重要インフラ、電気通信事業、通信の秘密

１．概要

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。）第 2 条第 4 号に規定する電気通信事業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、又は第 16 条第 1 項の規定による届出を行い、電気通信事業者となる必要がある。

電気通信事業者は、事業法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）電気通信事業者の定義

電気通信事業者とは、電気通信事業を営むことについて、事業法第 9 条の登録を受けた者及び第 16 条第 1 項の規定による届出をした者をいう（事業法第 2 条第 5 号）。

（２）電気通信事業者に該当する場合

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（事業法第 16 条第 1 項）を要する電気通信事業であるため、登録又は届出を行い、電気通信事業者となる必要がある。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「電気通信事業参入マニュアル」［追補版］を参照されたい。

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（事業法第 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。）（事業法第 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（事業法第 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

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（事業法第 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

次の場合には、「適用除外となる電気通信事業」（事業法第 164 条第 1 項）に該当する。

表 1「適用除外となる電気通信事業」

・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。）・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）

なお、適用除外となる電気通信事業である場合でも、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、事業法第 3 条（検閲の禁止）及び第 4 条（秘密の保護）の対象となるので（事業法第 164 条第 3 項）、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、電気通信役務を利用者に反復継続して提供して、電気通信事業自体で利益を上げようとすること、すなわち収益事業を行うことを意味する。

（3）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「ポータルサイト」、「SNS（Social Networking Service）」

など、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・届出の要否を判断することとなる。

（４）電気通信事業者に係る規律

ア　全般的な規律

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。

イ　通信の秘密の大要

特に、サイバー攻撃などとの関係で問題となることがある、通信の秘密の大要を説明する。

日本国憲法第 21 条第 2 項は、「通信の秘密は、これを侵してはならない」と規定しているが、プライバシー権の観念が発展した現在では、通信の秘密はその一局面を取り上げて明文で保証した規定であるとともに、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と解される[1]。同規定を受けて、電気通信事業法第 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、

---

[1] 渡辺康行・宍戸常寿・松本和彦・工藤達朗『憲法Ⅰ　基本権』（日本評論社、平成 28 年）256 頁

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得しようとする行為[2]

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、契約約款等に基づく事前の包括同意のみでは一般的に有効な同意と解されていないので、注意が必要である。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、ISP 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[3]（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[4]。

なお、総務省で「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」が開催され、取りまとめが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されたい。

ウ　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、サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」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[5]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大規模かつ有料の電気通信役務を提供する電気

---

[2] 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。

[3] 「正当業務行為」とは、電気通信役務を提供する観点から、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をいう（総務省「電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号）の解説」平成 29 年 9 月（平成 31 年 1 月更新）参照）。電気通信役務の提供に「不可欠な場合」には原則として正当業務行為として許容される。同役務の「安定的な提供」のために利用する場合については「目的の正当性や行為の必要性、手段の相当性から相当と認められる」場合にのみ正当業務行為として許容される。

[4] 「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）

[5] 重要インフラに係る取組について Q2 参照。

通信事業者に対し、その電気通信事業の用に供する電気通信設備（以下「事業用電気通信設備」という。）について、その損壊又は故障により電気通信役務の提供に著しい支障を及ぼさないようにするため、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（昭和 60 年郵政省令第 30 号）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。

また、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[6]。

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。

エ　そのほか、参入などの各場面に関する規律

そのほか、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 月の最終改定版を参照されたい。

表 2「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	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

[6] 施行規則第 29 条及び平成 27 年総務省告示第 67 号

の変更や事業の休廃止等に関する規律	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)、媒介等業務受託者に対する指導（事業法第 27 条の 3)
報告等に関する規律	業務の一部停止、通信の秘密の漏えいその他の重大な事故の報告（事業法第 28 条)、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）

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［追補版］」（平成 17 年 8 月 18 日策定（令和元年 10 月 1 日 最終改定))
https://www.soumu.go.jp/main_content/000477428.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 29 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

・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（2016 年）3 月（令和元年（2019 年）9 月最終改定）
https://www.soumu.go.jp/main_content/000406001.pdf

・総務省「電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号）の解説」平成 29 年 9 月（平成 31 年 1 月更新)
https://www.soumu.go.jp/main_content/000603940.pdf

４．裁判例

・東京地判平成 14 年 4 月 30 日平 11（刑わ）3255 号

Q37 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。電気通信事業法の技術基準関係では令和 2 年 4 月から、IoT 機器の技術基準にセキュリティ対策を追加することとされている。

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・IoT サービス全体へその影響が波及する可能性が高い。

②IoT 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つづける可能性がある。

③IoT 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。

④IoT 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

IoT 機器側とネットワーク側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。

⑤IoT 機器の機能・性能が限られていること

---

[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 ver 1.0」平成 28 年 7 月

センサ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影響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 30 年 5 月、IoT 機器に対する脆弱性対策を実施する体制整備を含んだ「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が成立し、公布された。同改正法に基づき、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（NICT 法）附則第 8 条に基づき、「平成三十六年三月三十一日までの間」（同条第 2 項柱書）、つまり、令和 6 年（2024 年）３月までの時限的な業務として行われるものであり、すで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[3]。

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[4]を入力し、特定アクセス行為[5]を行うことができるかを確認することなどにより、サイバー攻撃[6]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

[3] NOTICE Web サイト参照。 https://notice.go.jp/

[4] NICT 法附則第 8 条第 4 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、国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令（平成 30 年総務省令第 61 号）第 1 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。

[5] NICT 法附則第 8 条第 4 項第 1 号に定義されている。なお、同法附則に基づく 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（同法附則第 8 条第 7 項）。

[6] NICT 法附則においては、「送信型対電気通信設備サイバー攻撃」（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

ットプロバイダに通知する（NICT 法附則第 8 条第 2 項）。

②注意喚起：インターネットプロバイダは、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する。

（３）電気通信事業法の技術基準関係

利用者[7]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、電気通信事業者の接続の検査を受け、当該端末機器が電気通信事業法に基づく技術基準に適合していることを確認する必要がある（電気通信事業法第 52 条第 1 項）。

そして、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（電気通信事業法第 52 条第 2 項各号）の各事項が確保されるものとして、端末設備等規則（昭和 60 年郵政省令第 31 号）において定められている[8]。

総務省は、平成 31 年 3 月、IoT 機器の技術基準にセキュリティ対策を追加することなどを目的として、「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）」を公布し、端末設備等規則の一部改正を実施した。なお、同改正省令は、IoT 機器メーカや登録認定機関等の対応を考慮し、令和 2 年 4 月から施行される。

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、最低限のセキュリティ対策として、①アクセス制御機能（端末への電力供給が停止した場合でも機能の維持が可能）、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

る電気通信の送信を含む。…）により行われるもの）とされている（NICT 法附則第 8 条第 4 項第 3 号、電気通信事業法 116 条の 2 第 1 項第 1 号）。具体的には、DDoS 攻撃等を想定したものである。

[7] 「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。エンドユーザーのほか、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、改訂版、令和元年）318 頁参照）。

[8] 以上①から③について、総務省 Web 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

ェアの更新機能（端末への電力供給が停止した場合でも更新されたファームウェアの維持が可能）、又は①～③と同等以上の機能を具備することである。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対策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も認定等を要しない。

総務省は、平成 31 年 4 月、当該改正後の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 1 版）」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。

（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が 2018 年 9 月に成立し、2020 年 1 月から施行されている。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、同法の対象となりえるので、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（昭和 59 年法律第 86 号）
・端末設備等規則（昭和 60 年郵政省令第 31 号）
・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（平成 11 年法律第 162 号）
・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
・総務省サイバーセキュリティタスクフォース
「IoT セキュリティ総合対策」（平成 29 年 10 月）
https://www.soumu.go.jp/main_content/000648314.pdf
・総務省サイバーセキュリティタスクフォース
「IoT セキュリティ総合対策プログレスレポート 2019」（令和元年 5 月）
https://www.soumu.go.jp/main_content/000648300.pdf
・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 1 版)」（平

成 31 年 4 月 22 日）
https://www.soumu.go.jp/main_content/000615696.pdf

・米国カリフォルニア州 IoT セキュリティ法
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.91.05.&lawCode=CIV

４．裁判例

特になし

Q38 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

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を負う可能性がある。この場合、データ漏えいの被害者は、製造物責任を追及することができる。

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、原因が解明しづらくなることから、データが漏えいした場合には、訴訟において多数の者が被告となりう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、データ漏洩時における損害額については、Q52 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、製造物責任法第 3 条では、

「製造業者等[1]は、その製造（中略）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、製造者（同法上では、製造業者等）に欠陥があることを証明すれば、故意また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 機器に欠陥があった場合には、製造物責任法が適用されることとなる。

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。

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ー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、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。

ウ　利用者に原因があった場合

利用者が製品出荷時のパスワードを変更するべきであったのに、そのまま利用していた場合など、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、IoT 機器の製造者は法的な責任は負わない。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、特別な事由がある場合には、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。

---

[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

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洩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ことを目的として、製造メーカー等が 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、13 項目のベストプラクティスを公表している[2]。具体的な項目は次のとおりであるが、参考にあ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。② 脆弱性の情報公開ポリシーを策定する。③ ソフトウェアを定期的に更新する。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。⑤ 安全に通信する。⑥ 攻撃対象になる場所を最小限に抑える。⑦ ソフトウェアの整合性を確認する。⑧ 個人データの保護を徹底する。⑨ 機能停止時の復旧性を確保する。⑩ システムの遠隔データを監視する。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。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。⑬ 入力データを検証する。

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
・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/pdf/001_04_00.pdf

４．裁判例

特になし

[2] Department for Digital, Culture,Media & Sport，Guidance Code of Practice for consumer IoT security，2018 https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

Q39 電子契約実務と電子署名法

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

電子的な契約も可能だが、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、電子帳簿保存法[1]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。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。ネットショッピングの場合も、買い物かごに入れて注文する形式が多く、契約書等は交わさない場合が多い。

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。

[1] 令和 2 年度税制改正の大綱（令和元年 12 月 20 日閣議決定）において、電子帳簿等保存制度の見直し（令和 2 年 10 月 1 日から施行）が盛りこまれているため、その点留意が必要である。https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2020/02taikou_06.htm#06_04

（２）文書証拠の形式的証拠力

書証については、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。これを形式的証拠力と言い、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、その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、その私文書に文書作成者の印章により顕出された印影があれば、その印影は、その私文書の作成者の意思に基づくものであり、その私文書の作成者がその意思に基づいて押印したものと事実上推定される。

（３）電子データの場合

電子データの場合も、その意味内容を証拠資料としたいのであれば、その成立の真正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のほか、契約に限らずあらゆる電子データについても同様である。電子データについて電子署名が行われた場合には、その電子データは真正に成立したものと推定される。つまり、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こととなる。

ただし、その電子署名は、電子署名法第 3 条に規定する電子署名に限られ、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該当しない。

もっとも、電子署名法第 3 条の要件を満たさない場合であっても、自ら、その電子契約が本人の意思に基づき作成されたことを立証できれば良い。

（４）電子契約の有効性と電子署名法

ア　電子署名の定義

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。

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（本人性）

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（非改ざん性）

イ　電子署名法第 3 条の要件を満たす電子署名と電子契約

また、電子署名法第 3 条は、さらに、当該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（これ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限る。）が行われているときは、真正に成立したものと推定すると定めている。

このことから分かるように、電子契約においては、「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」との要件を満たす「本人による電子署名」が付された場合にのみ、電子契約における当該電磁的記録の成立の真正が推定される。

この「本人だけが行うことができること」との要件を満たすために必要な措置については、

条文上必ずしも明確ではないが、現時点においては、一般的に、公開鍵暗号方式による電子署名のうち特定認証業務を行う事業者による電子証明書が付されたもの等についてはこの要件を満たすと考えられる。

なお、電子署名法の体系では、認証業務を3段階に定義している。電子署名が行われた情報を受け取った者は、当該情報が本当に本人から送られてきたものであるのかを確認する必要があるが、認証業務とは、その確認のために用いる事項が本人に係るものであることを証明する業務のことである（電子署名法第2条第2項）。そして、この中から、電子署名法のうち、その方式に応じて本人だけが行うことができるものとして主務省令で規定された基準[2]に適合するものについて行われる認証業務を「特定認証業務」（電子署名法第2条第3項）と称し、さらに、設備や業務の実施方法が電子署名法第6条第1項に規定する基準を満たし、電子署名法第4条に規定する認定を受けた認証業務を「認定認証業務」（電子署名法施行規則第6条第2号）と称している。

もっとも、電子署名法第3条の「本人だけが行うことができること」との要件を満たす電子署名は、必ずしも特定認証業務や認定認証業務による電子署名に限られるものではないと考えられ[3]、現時点で確定的な見解はない。

ウ　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

他方、仮に、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としても、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有効性が全て否定されるものではない。電子署名法第3条の要件を満たさない電子署名が行われている電子契約であっても、当該電子契約が、電子データの作成者として主張される特定人の意思に基づいて作成されたものであることを立証するのに必要な証跡が記録される仕組みを備えたものであれば、その電子契約の真正な成立を立証可能であるため、その法的効力においては、書面での契約と有意な違いは生じない。ただし、電子署名法第3条の要件を満たす電子署名が行われた電子契約とは異なり、電子契約の真正な成立を自ら立証する必要があることには留意が必要である。

---

[2] 電子署名法施行規則第2条は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。
一　ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因数分解
二　大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算
三　楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算
四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの
なお、令和2年2月18日現在、電子署名法施行規則第2条は改正される方針である（改正案について令和元年2月26日までパブリックコメントが実施された）。
https://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=145209452&Mode=0

[3] 「電子署名及び認証業務に関する法律の施行状況に係る検討会報告書」（平成20年3月、https://www.meti.go.jp/policy/netsecurity/docs/esig/080530_esignreport.pdf）の20頁においても、「もとより、電子署名法第3条の推定効が適用される電子署名は、第2条第3項の特定認証業務の対象となる電子署名と必ずしも一致するものではない」旨記載されている。

（５）電子保存と電子帳簿保存法

契約締結業務を電子化する場合、締結後の契約を電子保存することも検討されることが多い。その場合には、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」（電子帳簿保存法第２条第１項第６号）[4]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、別途、電子取引データを印刷した書面等を保存する場合を除き、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（電子帳簿保存法第 10 条）。

そして、「財務省令」とは電子帳簿保存法施行規則を指すが、同施行規則第８条第１項が、電磁的記録を保存するにあ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[5]。

① 以下のいずれかの要件を充足する。

(ア) タイムスタンプ[6]を付すとともに、当該取引データの保存を行う者又はその者を直接監督する者に関する情報を確認することができるようにしておくこと（電子帳簿保存法施行規則第８条第１項第１号）。

(イ) 当該電磁的記録の記録事項について正当な理由がない訂正及び削除の防止に関する事務処理の規程を定め、当該規程に沿った運用を行うこと（電子帳簿保存法施行規則第８条第１項第２号）。

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付を行う。

③ 当該電磁的記録の備付け及び保存の場所に、パソコン、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] 「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。」（電子帳簿保存法第２条第１項第６号）とされる。

[5] 令和２年度税制改正の大綱（令和元年 12 月 20 日閣議決定）において、電子帳簿等保存制度の見直しとして、国税関係帳簿書類の保存義務者が電子取引（取引情報の授受を電磁的方式により行う取引をいう。）を行った場合の電磁的記録の保存方法の範囲に、次の方法を加えることとされている（令和２年 10 月１日から施行）。

（1）発行者のタイムスタンプが付された電磁的記録を受領した場合において、その電磁的記録を保存する方法

（2）電磁的記録について訂正又は削除を行った事実及び内容を確認することができるシステム（訂正又は削除を行うことができないシステムを含む。）において、その電磁的記録の授受及び保存を行う方法

[6] 「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、総務省「タイムビジネスに係る指針 ～ネットワークの安心な利用と電子データの安全な長期保存のために～」(平成 16 年)にいう時刻認証業務において付与される、「電子データがある時刻に存在していたこと及びその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報。」を指す。本指針を踏まえ、一般財団法人日本データ通信協会は、「タイムビジネス信頼・安心認定制度」を創設・運営している。

④　当該電磁的記録について、施行規則所定の検索機能を確保する。

上記①に関し、利用する電子契約サービスが、時刻認証業務認定事業者のタイムスタンプを付すものではない場合、（イ）記載の「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が、当該規程の例は、国税庁「電子帳簿保存法一問一答【電子計算機を使用して作成する帳簿書類及び電子取引関係】」問 61 に掲載されているため参照されたい。

３．参考資料（法令・ガイドラインなど）

・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
・国税庁「電子帳簿保存法一問一答【電子計算機を使用して作成する帳簿書類及び電子取引関係】」問 61
・令和 2 年度税制改正の大綱（令和元年 12 月 20 日閣議決定）六 納税環境整備　4 電子帳簿等保存制度の見直し
https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2020/02taikou_06.htm#06_04

４．裁判例

特になし

Q40 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、どのようなサイバーセキュリティ関連法令上の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、個情法、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守秘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）[2]の活用が指摘されるようになった。たとえば、世界では、「パーソナルデータは、インターネットにおける新しい石油であり、デジタル世界における新たな通貨である」といわれ始め[3]、我が国では、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”」という考え方を示されるようになり[4、5]、平成 28 年には、官民データ活

[1] 総務省「平成 30 年版情報通信白書」1-1-1-1（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd111200.html）によれば、世界の IoT デバイス数は、平成 26 年に 170.8 億であったが、令和 2 年には 403 億に伸びるという予測があるとのことである。なお、ここで IoT デバイスとは、固有の IP アドレスを持ちインターネットに接続が可能な機器及びセンサーネットワークの末端として使われる端末等をいうとのことである。

[2] 総務省「平成 24 年版情報通信白書」1-2-1-4-(1)及び(2)（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc121410.html）

[3] World Economic Forum ウェブページ「パーソナルデータ：新たな資産カテゴリーの出現」（”Personal Data: The Emergence of a New Asset Class”、https://www.weforum.org/reports/personal-data-emergence-new-asset-class）。なお、同レポートによれば、新しい石油・新たな通貨という発言は、欧州委員会消費者保護担当委員のメグレナ・クネワ氏が平成 21 年 3 月に行ったものとのことである。

[4] 経産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）

[5] 「データ主導社会」という場合もある（総務省「プラットフォームサービスに関する研究会中間報告書」4 頁（平成 31 年 4 月、https://www.soumu.go.jp/main_content/000613197.pdf）参照）

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、第三次人工知能ブームを牽引する、知識を定義する要素（特徴量）を人工知能（AI）が自ら習得するディープラーニング[6]も、日常生活に浸透し始めている[7]。

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守秘義務の合意（契約）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[8]。

たとえば、平成 30 年 6 月には、経産省が、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、「契約ガイドライン」という）を策定し[9]、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[10]。

（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また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。たとえば、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、近時増えつつある、AI 技術を利用したソフトウェアの開発の委託や学習用データのアノテーションの外部委託なども、データ取引といえる。

（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[11]は、有体物ではないため、我が国法制度上、

---

6 深層学習や特徴表現学習とも呼ばれる（総務省「平成 28 年版情報通信白書」1-4-2-1-(2)（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc142120.html））。

7 前掲注 6・中間報告書 1-4-2-1-(1)（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc142110.html）

8 たとえば、経産省及び 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（経産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://www.meti.go.jp/press/2017/05/20170530003/20170530003.html））

9 経産省ニュースリリース平成 30 年 6 月 15 日『「AI・データの利用に関する契約ガイドライン」を策定しました」』（https://www.meti.go.jp/press/2018/06/20180615001/20180615001.html）

10 経産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://www.meti.go.jp/press/2019/12/20191209001/20191209001.html）

11 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（略））に記

所有権の対象とはならない。つまり、データの使用・収益・処分をする権利の全面的な支配について、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 Q20 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 Q48 参照）などの制約（以下、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（Q22 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)）[12]。

（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あたって）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、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・合意にあ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）

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 たとえば、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。

録された情報（後略）」と定義されている（同法第 2 条第 1 項）。

[12] なお、実務上、企業は内規などで有体物に関する職務権限を定めていることが一般的であるが、データについては、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となっておらず、そのためにデータ契約の交渉、合意や実行に至らないとの指摘もある。そこで、データ取引を始めたり、データ契約を交渉・締結するにあたっては、企業内でデータに関する職務権限を明らかにするような社内体制の検討・整備も必要であるといえる。

イ　守秘義務・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、典型的な守秘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。

③ 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（Q17 及び 18 参照）であると主張して秘密管理性を争う予定があるか、または限定提供データ（Q20 参照）であると主張して電磁的管理性を争う予定があるか、さらに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。

ウ　セキュリティのレベルまたはデータの管理体制に関する合意について

① 上記イと同じく、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（Q17 及び 18 参照）または限定提供データ（Q20 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また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（ウィルスに感染していないこと）または完全性について、保証また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。たとえば、データに基づいて生じた成果物の安全性または完全性についても保証または免責の対象とするかを検討するにあたっては、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という（契約ガイドライン AI 編第 3-4 及び第 4-3-(4)）ように、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、どのような違反時の効果（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）を設けるか。

② そもそも、遵守できているのか、また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、どのような基準でもって義務違反と判断すべきか。

なお、契約ガイドラインが、サイバーセキュリティに限らず、データ取引の事例の紹介や検討を展開しており、またモデル契約の紹介・解説も掲載しているので、参考となる。

３． 参考資料（法令・ガイドラインなど）

・経産省「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/press/2019/12/20191209001/20191209001.html

４． 裁判例

特になし

Q41 情報流出に関するシステム開発ベンダの責任

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

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、個人データ等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記述されていない場合でも、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くとも当然に実施すべきものではない。

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あたり、平成 18

[1] なお、情報漏えいが発生していない段階でも、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 715 条）が問われ、損害賠償責任が認容された事案もある（東京地判平成 30 年 10 月 26 日判例集未登載）。

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」旨を述べ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（前掲東京地判平成 26 年 1 月 23 日）

（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しないとし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に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よって、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。

（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、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。

システム開発契約において合意していたベンダが賠償すべき損害額の上限に関する規定

---

[2] 経産省「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://www.ipa.go.jp/security/products/products2006.html

などの免責条項の有効性に関して、前掲東京地判平成 26 年 1 月 23 日は、一律に責任を免除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 Q53 参照）。

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

４．裁判例

・東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁
・東京地判平成 30 年 10 月 26 日判例集未登載

Q42 クラウドサービスの利用にあたっての留意点

クラウドサービスを利用するにあたって、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あたっても、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みられるようになってきている。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

[1] 本項の議論につき、経産省「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「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。

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あたっては、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、このように自社ですべ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、外部リソースを利用しているのではなく、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、クラウドサービスが多様化するにつれて、クラウドサービスの提供側にも分化や統合が見られるようになっている。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ー（IaaS、PaaS、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ー（SaaS）への分化がみられる。一方で、多様なクラウドサービスをできるだけ一元化して利用したいというユーザ側のニーズを背景に、①複数の SaaS が連携してサービスを提供する（アグリゲーションサービス）、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）などの形態が表れてきている。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あ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あたっては、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。

[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２版）」（以下「クラウドサービス提供ガイドライン」という。）188 頁以下

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あたり、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うる。

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、個人データについて、安全管理措置を行い（個情法第 20 条）、また、委託先の必要かつ適切な監督を行わなければならない（同法第 22 条）とされている。クラウドサービスにおいてユーザが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委託、第三者提供、又はユーザ自らの保有のいずれと考えるのかを検討し、対応しなければならない（Q9 参照）。

また、個人データを第三者提供する場合には、原則として本人の同意が必要となる（個情法第 23 条第 1 項）。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、ID 連携を行い、情報の交換を行っていることがあるが、提供又は受領している情報の中に個人データが含まれていることがあり、本人の同意の取得等を要することがある。

（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[4]。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、契約の締結にあたって解釈を確認することが必要である。

[4] 営業秘密管理指針 11 頁

（エ）リージョン

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[5]。

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 24 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、越境移転と考えるのか、越境と考える場合、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）（Q9 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（Q48 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に加えて、法的には以下のような点があげられる[6]。

（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あたっては、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、サービス自体の権利者と保守、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、適切な権利者を選択し、適切な契

---

[5] 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）である。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、国家がかかわる公法の適用は、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）。

[6] 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。

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、提供される役務が不定形なサービス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、所期の目的を達成したために解約したい、サービス提供者が倒産した等、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側の複雑化により、窓口になっているクラウドサービス提供事業者が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。

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がある監査をなしえないことが多く、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」[7]などがある[8]。

エ　（参考）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

サイバーセキュリティ戦略本部は、令和 2 年 1 月 30 日に「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」を決定した。

これは、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に関する基本的な枠組みを示すもので、当該制度においては、まず、政府機関等がクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準を策定し、定められた評価プロセスに基づき、要求される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確認されたクラウドサービスについて、公表されるクラウドサービスリストに登録するというものである。各政府機関等は、クラウドサービスを調達する際は、当該制度において登録されたサービスから調達することを原則にすることとされている。

当該制度は、飽くまで政府機関等が利用するクラウドサービスについて登録簿を作成するものであるが、情報システムの調達者・ユーザがセキュリティ確保についての最終的な責任を負わなければならない点に留意しつつも、公開される情報等について、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。

なお、当該制度の所管は、内閣官房（NISC、情報通信技術（IT）総合戦略室）、総務省、経産省とされている。加えて IPA は、制度運用に係る実務及び評価に係る技術的な支援を行うものとされており、情報処理の促進に関する法律の一部を改正する法律（令和元年法律第 67 号）[9]による改正後の情促法第 51 条第 1 項第 5 号（現第 43 条第 1 項第 5 号）において、IPA の所掌事務に当該制度に関することが追加されている。

（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ー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

---

[7] 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）

[8] 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）（Q13 参照）等がある。

[9] 公布の日（令和元年 12 月 6 日）から 6 月を超えない範囲内において政令で定める日から施行予定

あり、修正が可能であるのか、それとも定型約款[10]となるのかについて検討することが必要である。

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、改正民法が施行される令和2年4月1日以降、原則として同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まで）の適用を受けることになる[11]。

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あ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、また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[12]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あたって、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、当該契約が改正民法第548条の2にいう定型約款に該当すれば、不当条項規制（改正民法第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（Q53参照）。

---

10 債権法を大きく改正した民法の一部を改正する法律（平成29年法律第44号、一部を除き令和2年4月1日施行）による改正後の民法（以下本項において「改正民法」という。）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。

11 民法の一部を改正する法律（平成29年法律第44号）附則第33条第1項（定型約款に関する経過措置）。ただし、令和2年4月1日までに、契約の当事者の一方から反対の意思の表示が示された場合はこの限りではない（同条第2項、第3項）。

12 電子商取引準則255頁～「Ⅲ-6 SaaS・ASPのためのSLA（Service Level Agreement）も参照。

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「政府機関等の情報セキュリティ対策のための統一基準」
https://www.nisc.go.jp/active/general/kijun30.html
・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.nisc.go.jp/active/general/pdf/wakugumi2020.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 2 版）」（2018 年 7 月）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html
・経産省「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 ver4.0）
・電子商取引準則

４．裁判例

特になし

Q43 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、下請代金支払遅延等防止法（下請法）、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

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下請法に留意すべき場合もある。

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 におけるサプライチェーンでは、製品の設計段階や、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がある。

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恐れがあるというリスクを主に想定していたが、IT におけるサプライチェーン・リスクとしては、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[1]。

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、たとえば、①委託元が用いるハードウェア製品を意図的に不正改造したり、情報システムやソフトウェアに不正なプログラムを埋め込んだりされるおそれや、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 2 次被

[1] サイバーセキュリティ 2019・364 頁参照

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[2]。

（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、「国内外に関わらずサプライチェーンのセキュリティ対策の必要性も高まっており、業務を請け負う企業にあっては、国際的なビジネスに影響をもたらす可能性が出てきている」[3]とされる。

実務においても、一例として、システム管理等を委託する場合に、委託先を選定するときには、与信、業務体制や契約条件の各審査に加えて、セキュリティ対策状況も審査する、審査方法としては、取引（予定）先にチェックリスト形式で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対策例や、委託先と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対策例が考えられる。

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、「自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要」（同 5 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 15 頁）。

① 監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について、系列企業、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の運用委託先等を含めた運用をさせる。

② システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

ウ　再委託先について

再委託を行うにあたっては、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。

---

[2] 経営ガイドライン 5 頁、15 頁参照

[3] 前掲注 2・1 頁。

エ　認証・保証報告書の取得について

取引先から取引条件として求められることから、または、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に関する認証を取得する企業もいる（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 Q45 参照）。

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（独占禁止法第 2 条第 9 項、第 19 条）のうち、①その他の取引拒絶（一般指定[4]2 項）、②拘束条件付取引（一般指定 12 項）、③優越的地位の濫用（独占禁止法第 2 条第 9 項第 5 号）、または④下請法に抵触しないかが問題となる。

ア　その他の取引拒絶（一般指定 2 項）

（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」[5]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

---

[4] 独占禁止法第 2 条第 9 項第 6 号イからへのいずれかに該当する行為であって、公正な競争を阻害するおそれがあるもののうち、公取委が指定するものであって、全ての業種について適用されるものを「一般指定」といい、昭和 57 年 6 月 18 日公取委告示第 15 号（改正平成 21 年 10 月 28 日公取委告示第 18 号）により指定されている。

[5] 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）

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

よって、真にサプライチェーン・リスク対策を目的として、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ことは、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しているとはいえず、また、「競争者を市場から排除する」といった目的を達成するためとはいえないことから、基本的には独占禁止法上問題となる場合は想定し難いといえる。

イ　拘束条件付取引（一般指定 12 項）

（ア）基準

拘束条件付取引とは、独占禁止「法第 2 条第 9 項第 4 号又は前項に該当する行為のほか、相手方とその取引の相手方との取引その他相手方の事業活動を不当に拘束する条件をつけて、当該相手方と取引すること」とされている。

考え方としては、前掲「流通・取引慣行ガイドライン」が「垂直的制限行為に係る適法・違法性判断基準」を示している。「垂直的制限行為」とは、事業者が取引先事業者の販売価格、取扱商品、販売地域、取引先等の制限を行う行為をいい、①再販売価格維持行為と、②取引先事業者の取扱商品、販売地域、取引先等の制限を行う行為（「非価格制限行為」という）とに分類される。

上記基準に照らすと、まず、通常、取引先にサイバーセキュリティ対策を求めることが再販価格維持（上記①）につながることは考えられない。

次に、「非価格制限行為」（上記②）の考え方を見ると、『非価格制限行為は、一般的に、その行為類型及び個別具体的なケースごとに市場の競争に与える影響が異なる。すなわち、非価格制限行為の中には、[1]行為類型のみから違法と判断されるのではなく、個々のケースに応じて、当該行為を行う事業者の市場における地位等から、「市場閉鎖効果が生じる場合」や、「価格維持効果が生じる場合」といった公正な競争を阻害するおそれがある場合に当たるか否かが判断されるもの及び[2]通常、価格競争を阻害するおそれがあり、当該行為を行う事業者の市場における地位を問わず、原則として公正な競争を阻害するおそれがあると判断されるものがある』（同 5 頁）とのことである。また、「市場閉鎖効果が生じる場合」とは、「非価格制限行為により、新規参入者や既存の競争者にとって、代替的な取引先を容易に確保することができなくなり、事業活動に要する費用が引き上げられる、新規参入や新商品開発等の意欲が損なわれるといった、新規参入者や既存の競争者が排除される又はこれらの取引機会が減少するような状態をもたらすおそれが生じる場合をいう」（同 5 頁）とのことである。

（イ）検討

上記考え方に照らすと、取引先に一定のサイバーセキュリティ対策を求める場合、自社が当該対策を実施し得る代替的な取引先を容易に確保することができなくなる可能性はあっても、新規参入者や既存の競争者において代替的な取引先を容易に確保する

ことができなくなることは想定し難いといえる。

よって、取引先に一定のサイバーセキュリティ対策を求めることが不公正な取引方法に該当し、独占禁止法上問題となる場合は想定し難いといえる。

ウ　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」、または（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」[6]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。

なお、現行の「優越的地位濫用ガイドライン」においては、想定例としてサプライチェーン・リスク対策は示されてはいないが、「ここに示されていないものを含め、具体的な行為が優越的地位の濫用として問題となるかどうかは、独占禁止法の規定に照らして個別の事案ごとに判断されるものであることはいうまでもない」とされる。

（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

[6] 公取委「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）

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。

エ　下請法（下請代金支払遅延等防止法（昭和 31 年法律第 120 号））

（ア）基準

下請法は、事業者の資本金規模と取引の内容により規制対象を画するものである[7]。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役務提供委託の 4 種類が対象となる。

そして、資本金規模と取引の内容が下請法の定める要件に該当する場合には、下請法上の親事業者又は下請事業者に該当し、親事業者に対して、書面の交付義務等が課せられ、加えて、下請法第 4 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。

親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、割引困難な手形の交付、不当な経済上の利益の提供要請、および、不当な給付内容の変更及び不当なやり直しの 11 種類がある。

このうち、「購入・利用強制」とは、「下請代金支払遅延等防止法に関する運用基準」[8]によれば、「下請事業者の給付の内容を均質にし、又はその改善を図るため必要がある場合その他正当な理由がある場合を除き、自己の指定する物を強制して購入させ、又は役務を強制して利用させること」により、下請事業者にその対価を負担させることをいう。

（イ）検討

よって、親事業者は、下請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または役務の利用を強制する場合には、「下請事業者の給付の内容を均質にし、又はその改善を図るため」の必要があるか、またはその他正当な理由がないと、「購入・利用強制の禁止」（下請法第 4 条第 1 項第 6 号）に抵触し得るため、留意する必要があるといえる。

３．参考資料（法令・ガイドラインなど）

・独占禁止法第 2 条第 9 項第 5 号イ～ハ、第 2 条第 9 項第 6 号、第 19 条、一般指定 2 項、一般指定 12 項
・下請法第 4 条第 1 項各号・第 2 項各号
・経営ガイドライン
・「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
・「優越的地位の濫用に関する独占禁止法上の考え方」

[7] 公取委 Web サイト「下請法の概要」（https://www.jftc.go.jp/shitauke/shitaukegaiyo/gaiyo.html）
[8] https://www.jftc.go.jp/shitauke/legislation/unyou.html

https://www.jftc.go.jp/hourei_files/yuuetsutekichii.pdf

・「下請代金支払遅延等防止法に関する運用基準」
https://www.jftc.go.jp/shitauke/legislation/unyou.html

４．裁判例

特になし

Q44 情報処理安全確保支援士

「情報処理安全確保支援士」とはどのような者か。

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 2 年 2 月現在約 2 万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「登録セキスペ」という。）[1]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。

令和元年 10 月現在、19,417 名が登録されている。

なお、情報処理の促進に関する法律の一部を改正する法律[2]（令和元年法律第 67 号）により新設された改正後の情促法第 15 条第 2 項により、登録セキスペの登録は、3 年ごとに更

[1] 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。

[2] 公布の日（令和元年 12 月 6 日）から 6 月を超えない範囲内において政令で定める日から施行される。

新を受けなければ効力を失うこととされているため、留意が必要である。

（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 24 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 25 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 26 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 19 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 51 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 27 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 53 条第 2 号）。

（４）登録セキスペとなることのメリット

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、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[3]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。

[3] 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」

（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、登録セキスペが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及びセキュリティ監視・運用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産省が策定した「情報セキュリティサービス基準」（平成 30 年 2 月 28 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及びセキュリティ監視・運用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　ユーザー企業の場合

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 6 条から第 28 条
・経産省「情報セキュリティサービス基準」（平成 30 年 2 月 28 日）

４．裁判例

特になし

Q45 技術等情報の適切な管理に係る認証制度について

平成 30 年 9 月 25 日からスタートした「技術等情報の適切な管理に係る認証制度」は、どのような制度か。

タグ：産業競争力強化法、技術等情報の適切な管理に係る認証制度、技術等情報漏えい防止措置、重要技術マネジメント、自己適合宣言確認型認証、現地審査を含む認証

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、国外への技術流出防止等、事業者の適切な管理を担保するため、改正産業競争力強化法（平成 30 年 5 月成立）により新たに創設された、技術等情報を適切に管理している事業者を認証する制度（以下「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[3]、情報管理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、情報管理を実施す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、情報管理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] 経産省製造産業局「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://www.meti.go.jp/policy/mono_info_service/mono/technology_management/guideline0.pdf)

[2] 経産省「法律概要（参考資料：生産性向上特別措置法、産業競争力強化法等の一部を改正する法律）」（平成 30 年 7 月）
https://www.meti.go.jp/policy/jigyou_saisei/seisanseisochihoukyoukahou/pdf/gaiyou-2.pdf
なお、法律概要、法律・理由及び新旧対照条文は、経産省の右記 Web サイト参照（「生産性向上特別措置法及び産業競争力強化法等の一部を改正する法律」
（https://www.meti.go.jp/policy/jigyou_saisei/seisanseisochihoukyoukahou/index.html））。

[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
https://www.meti.go.jp/meti_lib/report/H30FY/000010.pdf

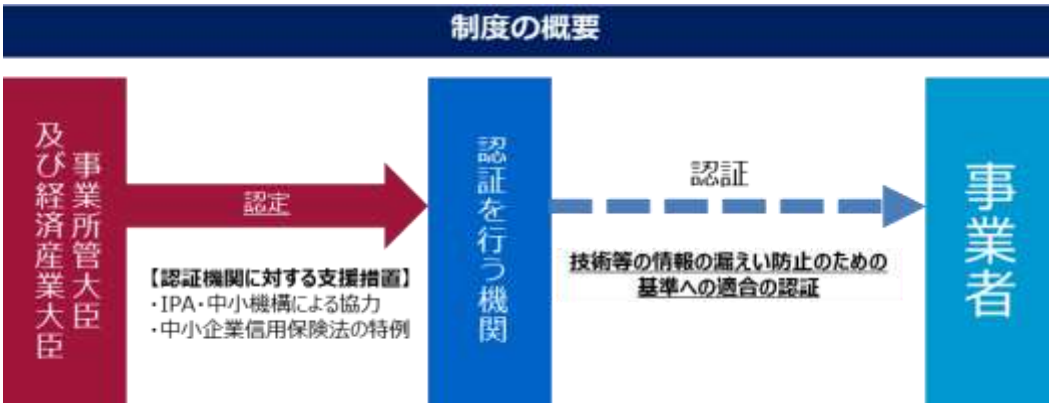
（２）要旨

本認証制度は、上記背景を踏まえ、技術等情報について、国外への技術流出防止等、事業者の適切な管理を担保するため、事業者の情報管理が国で示した「守り方」に即していれば、国が認定した「認定技術等情報漏えい防止措置認証機関（以下「認証機関」という）」から認証を受けられる制度である。

下記図のとおり、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２年１月末現在、２機関が認証機関として認定されている。

本認証制度を活用することにより、自社が適切な情報管理対策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、実際の確認（監査）を行うことなく取引先の情報管理レベルを把握してもらうことができるため、一定の信頼性を確保することができる。

図　本認証制度の概要[4]



また、「守り方」については、中小企業等における情報の管理の状況についての確認・評価手法に係る調査（認証トライアル調査）を踏まえた検討会で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]。

（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、自社のレベルに合わせて情報管理対策を選択できるものであり、まずは内部監査による自己宣言に対する認証（シルバー認証）、次に認証機関による現地審査での認証（ゴールド認証）と段階的な認証制度になっているため、ISMS 認証へのステップ

[4] 経産省「重要技術マネジメント」Web サイト（https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html）

として活用することができる[5]。

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 18 項、第 67 条
・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、関係省庁共同告示第 3 号）[6]
・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、関係省庁共同告示第 5 号）[7]
・「技術等情報の適切な管理に向けて」Web サイト[8]

４．裁判例

特になし

[6] 経産省「わが社の技術の管理はたぶん大丈夫！だなんて企業の一大事を後回しにしていませんか？ 技術等情報管理認証制度」
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/pam.pdf
[7] 内閣府、総務省、財務省、文科省、厚労省、農水省、経産省、国土交通省、環境省告示第三号
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf
[8] 内閣府、総務省、財務省、文科省、厚労省、農水省、経産省、国土交通省、環境省告示第五号
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/02.pdf
[9] 前掲注 4 と同じ。

Q46 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、このような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[2]については、平成 30 年の著作権法改正以前は、一部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は否定できなかった。

しかし、平成 30 年に著作権法が改正され、サイバーセキュリティ対策の目的やプログラムの調査解析の目的で行われる当該プログラムの複製や改変等、いわゆるリバースエンジニアリングについては、同法第 30 条の 4 に規定される権利制限の対象として、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「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）[3]に該当するものは多いと考えられる。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

[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 2019・367 頁）。
[2] Reverse engineering。ソフトウェアやハードウェアなどを解析・分解し、その仕組みや仕様、目的、要素技術などを明らかにすること（サイバーセキュリティ 2019・368 頁）。
[3] 知財高判平成 18 年 12 月 26 日平成 18 年（ネ）第 10003 号は、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。

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（以下まとめて「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[4]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」[5]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「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[6]とい

---

[4] 「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。

[5] 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）」6 頁参照。

[6] 前掲注 4・7 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。

う観点から判断」される[7]。

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[8]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[9]」としている。

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[10]

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、このような目的での利用は、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。

その他具体的な利用方法として、以下のような行為が、非享受目的に該当すると考えられている[11]。

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

---

[7] 詳細は、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）」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。

[8] 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。

[9] 前掲注 7・37～42 頁参照。

[10] 前掲注 7・11 頁及び 37～42 頁参照。

[11] 前掲注 7・11 頁参照。

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」[12]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[13]

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、独占禁止法上違法となる効力が私法上の効力にも及ぶ可能性がある。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[14]。

---

[12] 前掲注 7・11 頁参照。

[13] 電子商取引準則 240 頁参照。

[14] 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）（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

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[15]。

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）」
http://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_17.pdf
・電子商取引準則 240 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）
http://warp.ndl.go.jp/info:ndljp/pid/247419/www.jftc.go.jp/pressrelease/02.march/020320.pdf

４．裁判例

本文中に記載のとおり

されている。（※）現行一般指定 12 項。
[15] 前掲注 16・241 頁参照。

Q47 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、行個法、独個法、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（個情法等）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、著作権法等）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）。

暗号を利用するにあたっては、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、復号にあたっては、鍵が必要である。情報を暗号化したとしても、鍵が流出してしまうと、その流出した鍵を利用して第三者が復号することが可能になるなど、情報を暗号化した意味がなくなってしまう。そこで、鍵の適切な管理も重要である。鍵の適切な管理のために

[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/security/enc/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。

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生まれた時点ではセキュリティ上、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、暗号の実装にあたっては、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がある。

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うえで、利用する暗号アルゴリズムを更新すること、復号のための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に利用される、②一定の情報については、セキュリティを確保している場合に法的保護を受けることができるところ、そのセキュリティ確保のために利用される。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利用されるといった関係にある。

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20条）を行わなければならないが、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

---

[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。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。

[5] 暗号の評価、導入、管理について、NISC「政府機関等の対策基準策定のためのガイドライン（平成30年度版）」192頁「6.1.5 暗号・電子署名」が参考になる。

例示の一つとして挙げられている。同様に、行政機関の長や独立行政法人等は、保有個人情報について安全確保措置を取らなければならず（行個法第 6 条第 1 項、独個法第 7 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実行のために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[6]。もっとも、個人データについて、高度な暗号化により秘匿化がされている場合には、仮に漏えい事故が起こった場合であっても、実質的に漏えいがなかったといえ、本人の権利利益が侵害されておらず、二次被害の防止の観点からも必要はないと認められる場合等には、本人への連絡等や公表を省略することも考えられる[7]。

ここにいう高度な暗号化により秘匿化されている場合とは、漏えい事故が起こった時点での技術水準に照らし、暗号化された情報が第三者に見読される状態にすることが困難となるような水準の暗号技術により暗号化されており、また、暗号化された情報の復号鍵が適切に管理されている場合である。そして、見読される状態にすることが困難となるような水準の暗号技術とは、電子政府推奨暗号リストや ISO/IEC18033 等に掲載されている暗号をいい、また、復号鍵が適切に管理されていることとは、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ることのいずれかを満たすことが必要である[8]。

このように一定の情報に対してサイバーセキュリティに関する義務が課されている法律は、金融分野、医療分野、労働分野などに多岐にわたっている。

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うることがあるが、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（不正競争防止法第 2 条第 7 項）に該当する場合、民事上、刑事上の保護を受けうる[9]。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、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によって、これらの要件を満たすことが可能である[10]。

また、技術的制限手段（不正競争防止法第 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（不正

---

6 個情法ガイドライン（通則編）5 頁
7 個情法 QA 12-5
8 個情法 QA 12-10
9 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。
10 Q17、Q20 も参照。

競争防止法第 2 条第 1 項第 17 号、第 18 号)、民事上、刑事上の保護を受けることができる。

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（著作権法第 2 条第 1 項第 20 号）として暗号が利用されている。技術的利用制限手段を回避する行為は、当該技術的利用制限手段にかかる著作物に係る著作権、出版権又は著作隣接権を侵害する行為とみなされる（著作権法第 113 条第 3 項)。また、著作物の利用については、私的使用のための複製（著作権法第 30 条第 1 項本文）について著作権の制限であるとされているが、その場合であっても、技術的利用制限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、制限の例外とされている（著作権法第 30 条第 1 項第 2 号）[11]。

最後に、無線通信の傍受自体は、通信の秘密の対象とはなっていないが（電波法第 109 条)、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っている(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（電子署名法第 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（電子署名法施行規則第 2 条各号）[12]。

３．参考資料（法令・ガイドラインなど）

・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)
・個情法第 20 条
・行個法第 6 条第 1 項
・独個法第 7 条第 1 項
・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 7 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

[11] Q21 も参照。
[12] Q39 も参照。

４．裁判例

特になし

Q48 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、サイバー攻撃に転用されるおそれがあるものについて、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うるが、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

安全保障上リスクのある貨物や技術が、我が国及び国際的な平和及び安全の維持を脅かす国家やテロリスト等に渡り、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）により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（以下「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）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）について経済産業大臣の事前の許可が必要である。

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兵器の開発等に関する懸念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

①　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、例えば、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など、かなり広範な行為が外為法上の「輸出」に該当する。

②　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」、「使用」に必要な技術やプログラムが規制対象となる。

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「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。

ここにいう「提供」については、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」（以下「役務通達」という。）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、いわゆるクラウドサービスの利用についても規制対象となりうる。

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」[1]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[2]外為法第 25 条第 1 項に規定する役務取引に該当しない

[1] クラウドサービスに関しては、役務通達別紙１－２のほか、経産省安全保障貿易管理の Web サイト「技術関係」の Q&A において、Q55 から Q63 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」（Q55）とされているため、その点留意が必要である。

[2] 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

とされている。

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 項に定める役務取引に該当する[3]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。

サイバーセキュリティに関して何を規制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[4]で議論されており、平成 25 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うるが、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（詳細は後述する）。

（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」によれば、監視ツールによる検出を回避、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データ又は情報の抽出を行う、又はシステムや利用者のデータを変更するもの、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一の八の項において、「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

る。

[3] 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。

[4] Wassenaar Arrangement（http://www.wassenaar.org）

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（以下「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」が挙げられている。

典型的にはいわゆる C&C サーバ[5]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

外国為替令別表の八の項において、「(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。）が挙げられている。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 条各号に該当する貨物を設計し、又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 5 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 上記アの規制対象貨物等の設計又は製造に必要な技術（貨物等省令第 20 条第 1 項第 2 号）若しくは使用に必要な技術（同項第 6 号）

b 上記①a 又は b のプログラムの設計、製造又は使用に必要な技術（同項第 5 号、同条第 2 項第 6 号）

c 侵入プログラムの設計に必要な技術（同項第 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は、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

[5] 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。

又はこれらの個人若しくは組織と分析するもの」をいい、脆弱性関連情報の取扱いプロセス（Q56 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（ママ）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 Web 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
・貨物等省令
・役務通達
・経済産業省安全保障貿易管理WebサイトQ&A「技術関係」
https://www.meti.go.jp/policy/anpo/qanda25.html

４．裁判例

特になし

Q49 サイバーセキュリティと情報共有

サイバーセキュリティに関する情報共有体制へ参画し、情報共有を行おうとする場合に、法令上どのような点に留意すべきか。

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あたっては、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、刑法といった法令に注意が必要である。

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「情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供」が挙げられている。

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、NISC 及び政令指定法人 JPCERT/CC[1]が事務局を務めている。情報共有を行う

[1] 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

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）。

イ　早期警戒情報の提供システム「CISTA[2]」

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、セキュリティに関する脅威情報やそれらの分析・対策情報を早期警戒情報として提供している[3]。

ウ　第 4 次行動計画に基づく情報共有体制

サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」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、NISC 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。

エ　サイバー情報共有イニシアティブ「J-CSIP[4]」（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。

オ　日本サイバー犯罪対策センター（JC3[5]）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。

カ　サイバーセキュリティ対処調整センター

NISC は、サイバーセキュリティ戦略を踏まえ、2020 年東京オリンピック・パラリンピック競技大会（以下本項において「大会」という。）におけるサイバーセキュリティの確保に向け、脅威・事案情報の共有等を担う中核組織としてサイバーセキュリティ対処調整性センターを構築し、情報共有システム（JISP[6]）を構築、運用している。サイバーセキュリティ対処調整センターは大会後も日本のサイバーセキュリティの確保に活用して

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（基本法第 26 条第 1 項第 4 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（同法第 31 条第 1 項第 2 号）とされているところ、当該政令で委託する法人として、JPCERT/CC が指定されている（サイバーセキュリティ基本法施行令第 5 条）。

[2] Collective Intelligence Station for Trusted Advocates の略

[3] https://www.jpcert.or.jp/wwinfo/

[4] Initiative for Cyber Security Information sharing Partnership of Japan の略

[5] Japan Cybercrime Control Center の略

[6] Japan cyber security Information Sharing Platform の略

いく。

キ　セプター及びセプターカウンシル

NISC 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）[7]」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」の運営および活動を支援している。

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[8]」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）などがある。

（２）情報共有において留意すべき法令

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うるが、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 2 条第 6 項）[9]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 23 条第 1 項）。

ただし、以下に挙げる同法第 23 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。

① 法令に基づく場合

② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

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」（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「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、または限定提供データ

---

[7] Capability for Engineering of Protection Technical Operation, Analysis and Response の略、令和 2 年 2 月現在、14 分野 19 セプターが存在している。

[8] Information Sharing and Analysis Center の略。

[9] 個人情報データベース等を構成する個人情報（詳細は Q7 参照）。

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、個人については 5 年以下の懲役又は 500 万円以下の罰金（同法第 197 条の 2 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あたっては、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すべて「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）[10]。

---

[10] 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、また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し、または当該売買等を推奨してはならない（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 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あたっての情報伝達・取引推奨行為は、「他人に利益を得させ、また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。

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。

エ　刑法（不正指令電磁的記録に関する罪）[11]

サイバーセキュリティに関する情報共有を行うにあたっては、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。

（3）サイバーセキュリティ協議会について

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、平成 31 年 4 月、上記留意すべき法令に対応した法定の情報共有体制として、サイバーセキュリティ協議会が組織され、官民又は業界を超えた、全 155 者の多様な主体が参加（令和 2 年 2 月末時点）している。本協議会では、他の情報共有体制では拾えていなかった情報など、真に有益で、他では得られない情報にしぼりこんで共有を行っており、既に一定の成果が出始めている。

本協議会では、情報共有を行う上での阻害要因を除去するため、協議会構成員に対する情報提供義務及び守秘義務を法定化しており、以下概説する。

ア　情報提供等協力の求めと応答義務

協議会は、構成員に対して必要に応じて情報の提供等の協力を求めることができ、当該求めを受けた構成員は、正当な理由がない限り、これに応じなければならない（サイバーセキュリティ基本法第 17 条第 3 項）。

これは、協議会の判断で必要な協力の求めを行い、それに対応して情報の提供等の協力を行うことに法的な裏付けを付与することを趣旨の一つとしており、例えば、本項に基づく情報提供の求めに応じて情報を提供する場合に、そこに個人データに当たるものが含まれているとしても、「法令に基づく場合」（個情法第 23 条第 1 項第 1 号）の提供として許容されうる[12]。ただし、個人のプライバシーに配慮し、サイバーセキュリティの確保のために必要のない余分な情報を提供しないよう留意が必要である。

---

[11] 構成要件などの詳細については Q65 参照

[12] 本号に該当すると言えるためには、法令上明文の根拠が存在し、かつその根拠法令に基づいて適正な運用がなされていることが前提となる。

なお、情報提供の求めが濫用されないよう、サイバーセキュリティ協議会規約においては、本項に基づき、以下の 2 つの場合に限って一般の構成員に対する情報提供等の協力の求めを行うこととしている。

① 大規模なサイバー攻撃が発生するなど、情報提供等の協力を求める特別の必要性が認められる場合又はこれに準ずる状況であると認められる場合

② 構成員が協議会による協力の求めを受けることについて同意している場合

イ 守秘義務

協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事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（サイバーセキュリティ基本法第 17 条第 4 項）。

ここで禁止されている行為は、秘密を「漏ら」すという第三者への提供行為のみならず、「盗用」、つまり、受領した情報を自らが不正に利用することも含まれているため、サイバーセキュリティ協議会において情報共有を行う者は、情報を受領する者に守秘義務がかかっており、提供した情報が不正に利用・提供されないことを前提として、安心して情報を提供できる仕組みとなっている。

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」（令和元年 9 月 6 日一部改正）
・経営ガイドライン

４．裁判例

特になし

Q50 企業が保有する情報が漏えいした場合の対応

企業が保有する情報が流出した場合、企業はどのような対応をとるべきか。

タグ：個情法、不正競争防止法、刑事訴訟法、金融商品取引法、個人データ、営業秘密、限定提供データ

１．概要

企業が保有する情報が漏えいした場合は、一般的に、被害の拡大防止、事実関係及び原因の調査、被害や影響の範囲の特定、再発防止策の検討・実施、外部への公表や関係機関への報告といった対応を取るべきである。

また、上記の共通の対応に加えて、漏えいした情報が個人データであれば、個情委等への報告を、営業秘密や限定提供データであれば、警察への被害届や刑事告訴、差止請求や損害賠償請求を検討するべきである。

２．解説

（１）情報一般

企業が保有する情報が漏えいした場合は、被害の拡大防止措置（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）を講ずる必要がある。

そのうえで、漏えいの事実関係の調査、原因の究明や、漏洩による影響の範囲を具体的に特定した上で、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べきである。

また、事案の内容に応じて、二次被害の防止、類似事案の発生防止等の観点から、影響を受ける可能性のある本人への連絡や外部への報告・公表を検討することが望ましい。

（２）個人データの漏えい

漏えいした情報が個人データであった場合は、個情委「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」によれば、以下の措置を講じることが望ましいとされている[1]。

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

[1] その他詳細については個情法 QA12 も参照。

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。

⑤影響を受ける可能性のある本人への連絡等

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、事実関係等について、速やかに本人へ連絡し、又は本人が容易に知り得る状態に置く。

⑥事実関係及び再発防止策等の公表

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。

また、事実関係及び再発防止策等については、原則として個情委に対し、速やかに報告するよう努めるものとされている。但し、実質的には個人データが外部に漏えいしていないと判断される場合（個人データが高度な暗号化等の秘匿化がされている場合、第三者に閲覧されないうちに全てを回収した場合など）や、FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合については、個情委等への報告を要しないとされているため、個人データの漏えいの事実関係を精査した上で、個情委等へ報告するかどうかを検討すべきである。

なお、報告先については、個情委（個情委の Web サイトに設置している漏えい等事案の報告フォーム）が原則であるが、それ以外にも、認定個人情報保護団体や個情委から権限が委任されている事業所管大臣（個情法第 44 条第 1 項、同法第 40 条第 1 項）となる場合がある。

また、上記の報告先以外にも、別途業法等で監督当局への報告が義務付けられている場合もあることに留意が必要である。

（３）営業秘密の漏えい

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には、漏えいした情報が営業秘密でもあり個人データでもあることが考えられる）、上記（１）の対応に加え、営業秘密を取得した者等の行為が、不競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。

そのため、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、上記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、営業秘密の取得者等に対して差止（不正競争防止法第 3 条）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）を行うことを検討すべきである。
さらに、企業に在籍している従業員により営業秘密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）を行うことを検討すべきである。

（４）限定提供データの漏えい

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 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を検討すべきである。
また、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が、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、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や告訴を検討すべきである。

（５）情報漏えい等があったという事実とインサイダー取引

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、漏えいした情報の内容とは別に、情報漏えいがあったという情報そのものが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「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 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うえで、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恐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。

３．参考資料（法令・ガイドラインなど）

・個情法
・個情法 QA
・個情委「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」
・不正競争防止法
・営業秘密管理指針

４．裁判例

特になし

Q51 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

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「電子メール守秘義務条項」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[1]。

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）電子メール守秘義務条項

電子メール守秘義務条項とは、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、また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義務条項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、削除等の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

[1] 電子メールの誤送信により企業が保有した情報が漏えいした場合の対応については Q50 を参照。

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。

（２）営業秘密侵害

営業秘密を保有する事業者（以下「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」にあ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

[2] 逐条不正競争防止法 94 頁以下参照。
[3] 逐条不正競争防止法 94 頁以下参照。

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。

（３）情報記録媒体物の返還請求

誤配送された書類など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している。

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 94 頁以下

４．裁判例

特になし

Q52 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、個情法

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等の主体たる企業から、営業秘密等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」、「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あたっては、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（慰謝料および弁護士費用）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、および電話番号（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（慰謝料および弁護士費用）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

（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等の 2 次被害が発生した。原告らは 1 人当たり慰謝料 100 万円および弁護士費用 15 万円なら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すでに 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。

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、通常第三者に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。犯罪歴や病歴など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など、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などの 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うえ、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「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）」は、2018 年データに基づく個人情報漏えい時における 1 人当たりの平均想定損害賠償額につき 2 万 9,768 円、同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、あくまで同 JNSA の「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あ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等の主体たる企業から、営業秘密等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あたっては、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およ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およ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]）

侵害者が営業秘密侵害行為に係る物を譲渡したときは、その譲渡した物の数量（以下「譲渡数量」という。）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の単位数量当たりの利益の額を乗じて得た額を、被侵害者が受けた損害の額とすることができる（ただし、被侵害者の当該物に係る販売その他の行為を行う能力に応じた額を超えない限度）。

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]）

---

[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。

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。

（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）対して支払った損害賠償額
② 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。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、当該個人情報の漏洩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、情報漏えいと④委託元企業自体の信用棄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」（2017 年 5 月 17 日）

４．裁判例

本文中に記載のとおり

Q53 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

データを受託して管理している事業者は、データの保管を受託された場合、依頼者に対し、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、係る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は区別することはなく、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。当該データの保管サービス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となる可能性がある。

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り、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（昭和 59 年法律第 86 号。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（事業法第 179 条第 2 項、第 190 条第 1 項第 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。他方、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責任の一部免除を定める条項は、基本的には有効であり、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 12(ワ)18753 号・平 12(ワ)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義務を負っている。

一方、データ受託事業者（クラウドサービス提供事業者）とユーザ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。他方、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（平成 20 年（ワ）24300 号））。

（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（Q41 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、データ受託事業者に故意又は重過失がある場合には一律に責任を免除する旨の免責規定が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、裁判例[1]を踏まえると、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うえで判断することとなると考えられる[2]。

なお、SLA（サービスレベル契約）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）[3]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は、ユーザにも一定の過失が認められる。

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、又は損害の発生を極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」(東京地判平成 13 年 9 月 28 日（平 12(ワ)18753 号・平 12(ワ)18468 号)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

---

[1] その他、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）19457 号)）などがある。

[2] 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、令和 2 年 4 月 1 日に施行される改正民法における定型約款の規定の適用について留意する必要がある（Q42 参照)。

[3] 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場合は、公的認証取得や脆弱性対応などが挙げられる。

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、当該データは電気通信事業法第 4 条第 1 項に規定する通信の秘密の保護対象であり、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等の過失が認められる場合には、事業法第 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事業法第 186 条第 1 項第 3 号の規定に基づき、200 万円以下の罰金に処せられる。

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 年以下の懲役又は 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。なお、故意による漏えいは、未遂も処罰の対象である（事業法第 179 条第 3 項）。

3．参考資料（法令・ガイドラインなど）

・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
・経産省「SaaS 向け SLA ガイドライン」平成 20 年
・電子商取引準則 317 頁以下
・事業法 4 条第 1 項、29 条第 1 項、179 条第 2 項、186 条第 1 項、190 条第 1 項

4．裁判例

本文中に記載のとおり

Q54 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と解され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

情報媒体が滅失・損傷した場合において、その損害について債務不履行・不法行為等の責任が成立するときには、「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（中略）、当事者がその事情を予見し、又は予見することができた」ものについて、損害賠償責任を負担することになる（民法第 416 条）[1]。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うること(Q41、Q53 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について過失相殺の判断がなされうること（Q53 参照）について留意が必要である。

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、それは「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、

[1] 令和 2 年 4 月 1 日に改正民法が施行された後は、この一文は次の記載となる。
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も、当事者がその事情を予見すべきであった」もの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）

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）

・民法第 415 条、第 416 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
・広島地判平成 11 年 2 月 24 日判タ 1023 号 212 頁
・東京地判平成 13 年 9 月 28 日（平成 12(ワ)18753 号、平成 12(ワ)18468 号）
・岡山地判平成 14 年 11 月 12 日（平成 13 年（ワ）第 967 号）
・東京地判平成 21 年 5 月 20 日判タ 1308 号 260 頁
・東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁

Q55 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

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 2019・365 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）等への対応等を言う。）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「平成 30 年警察白書」112 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かれている定義になっている。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　端末の収集または特定

収集又は特定は、被害端末又は攻撃端末を特定することである。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った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ことである。

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すべてコピーすること（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ついて、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。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。

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する作業である。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

[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 8 版」（令和元年）等を参照。

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。

このような解析には、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扱われ、第三者によって内容が改変等されることはないという同一性が保たれていたことを担保することである。ハッシュ値によって同一性が担保されるが、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、ハッシュ値だけでは同一性を担保できないため、厳格な管理下であることによって同一性が保たれていたといえることになる。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、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統一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 1 800 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

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と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。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。

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、第三者委員会などがある。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。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 Twitter、Facebook、WeChat、Slack や Teams 等があり、やり取りされた過去の履歴等がパソコン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、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検討されている。

（５）デジタル・フォレンジックを行う際の法的課題

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(Q46 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おいて OS やプログラム等を複製したとしても著作権侵害には該当しない（同法第 42 条第 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。

また、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 Q25 も参照)。

さらに、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に問題となる。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、他人のパソコン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。

他にも、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も留意すべきである（金融商品取引法第 166 条第 1 項第 4 号、第 5 号等）。

（６）情報セキュリティサービス基準

経産省は、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[2]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。

---

[2] https://www.ipa.go.jp/security/it-service/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 Web サイトも参照
https://sss-erc.org/digital

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 8 版」
https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/
・経産省「情報セキュリティサービス基準」

４．裁判例

本文中に記載のとおり

Q56 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といった対応が推奨される。

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

ソフトウェア製品また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う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」（平成 29 年経済産業省告示第 19 号。以下「本規程」という。）が、ソフトウェア製品（ソフトウェアまた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）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。

---

[1] Japan Vulnerability Notes の略。
[2] 本規程第１の３(3)

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また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また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（Q41 参照）。

（２）本規程の制定経緯

平成 28 年に情促法が改正され、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 43 条第 1 項第 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 42 条、第 43 条）。

そして、情促法施行規則第 43 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、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）。

（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 脆弱性情報を発見または取得した発見者（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「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[3]、脆弱性関連情報は必ずその対策情報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」[4]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 43 条第 3 項、第 4 項
・情促法施行規則第 42 条、第 43 条
・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）
・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」（令和元年 5 月）

４．裁判例

特になし

[3] https://www.jpcert.or.jp/vh/index.html
[4] https://jvn.jp/index.html

Q57 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、信用回復措置実施請求が可能である。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また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。

（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 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。

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[1]。

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[2]。なお、JP-DRP の内容も非常に類似している[3]。

ア　UDRP 手続の特徴

UDRP 手続の特徴としては、簡易・迅速・低費用・非拘束という点があげられる。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

---

[1] 沿革としては、当初、ICANN や JPDRP 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 137・138 頁参照）。

[2] 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））。

[3] 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。

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[4]、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また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また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。

① 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

② 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

③ 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

④ 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・提出にあたっては、事案に応じた各論点の要件立証のための要素を検討する上で、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 HP 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

[4] レジストラとは、ドメイン名登録機関のことである。

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名または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 手続の利用にあたっては、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。これにあたっては、WHOIS検索の活用、ならびにWIPOにおける申立書雛形[5]及び過去の裁定例検索[6]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

[5] WIPO申立書雛形（http://www.wipo.int/amc/en/domains/complainant/）
[6] Search WIPO Cases and WIPO Panel Decisions（https://www.wipo.int/amc/en/domains/search/）

た手続であり[7]、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 Web 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 Web 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（全米仲裁協議会）と ADNDRC（アジアドメイン名仲裁センター）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
・JP ドメイン名紛争処理方針
・Uniform Rapid Suspension

４．裁判例

・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成 13 年 9 月 10 日最高裁 HP
・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 日最高裁 HP
・東京高判平成 14 年 10 月 17 日最高裁 HP
・知財高判平成 29 年 9 月 27 日最高裁 HP
・知財高裁中間判決令和元年 5 月 30 日最高裁 HP

[7] http://newgtlds.icann.org/en/applicants/urs/

Q58 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：プロバイダ責任制限法、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「発信者」という。）に対して、不正競争防止法に基づき差止を請求し得る。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「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保有者の情報が秘密管理性、有用性、非公知性の要件（Q17 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、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、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「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」に該当するときは、その情報を流通させた電気通信の提供者に対して、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をいう。）の開示を請求することができる（プロバイダ責任制限法第4条第1項）。なお、プロバイダ責任制限法における「権利の侵害」とは、不特定の権利侵害を対象とするものではなく、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[1]、裁判例は存在しないが、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、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[2]。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、プロバイダ責任制限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）に考慮した「相当性」の判断をも含むものである[3]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。

（３）削除請求

さらに、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

---

[1] 総務省総合通信基盤局消費者行政第二課『プロバイダ責任制限法』（第一法規、改訂増補第 2 版、平成 30 年）17 頁
[2] 同 79 頁
[3] 同 81 頁

対して、当該情報の送信を防止するための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、一次的に送信防止措置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、送信防止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。プロバイダ責任制限法第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、プロバイダ責任制限法第3条第2項は、プロバイダ等が送信防止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送信防止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、プロバイダ等は損害賠償責任を免責される旨を規定している。

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
・プロバイダ責任制限法第4条第1項

４．裁判例

特になし

Q59 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、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もと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。

１．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だという特性があり、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、上記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（Q39 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。

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

４．裁判例

デジタルデータ又はそれにより作成された紙媒体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

・最判平成 19 年 8 月 23 日判時 1985 号 63 頁

[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、Q55 を参照

Q60 営業秘密の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、原告は、被疑侵害者が営業秘密を使用した事実をどのように立証すればよいのか。特に、技術上の情報の場合はどうか。

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

１．概要

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。

２．解説

（１）営業秘密侵害訴訟とは

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、また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）、または不正取得・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。本案訴訟のみならず、本案に先んじて、または本案の訴訟提起と同時に、当該差止めについての仮処分命令を得るべく、または当該損害賠償請求権を保全すべく、民事保全手続を選択する場合もある（民事保全法第二章第二節第三款「仮処分命令」）。

（２）不正競争の立証について

営業秘密侵害訴訟においては、他の民事訴訟同様、原告となる営業秘密保有者において、被告を特定し、訴訟を提起して、不正競争の各要件に該当する事実を主張・立証する必要がある。

たとえば、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、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、たとえば、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して解析する等して、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、Q55参照。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、Q25参照。）。

また、営業秘密侵害訴訟において証拠を提出するときの留意点については、Q63及びQ59を参照されたい。

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。

（3）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）が新しく設けられた。

ア　趣旨

本推定規定は、上記（2）のとおり、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つすべて）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て、立証責任が被告に転換され、被告が当該営業秘密を使用していないことを立証しなければならなくなる。

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 被疑侵害者（被告）による第2条第1項第4号、第5号または第8号に該当する不正取得行為があったこと

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

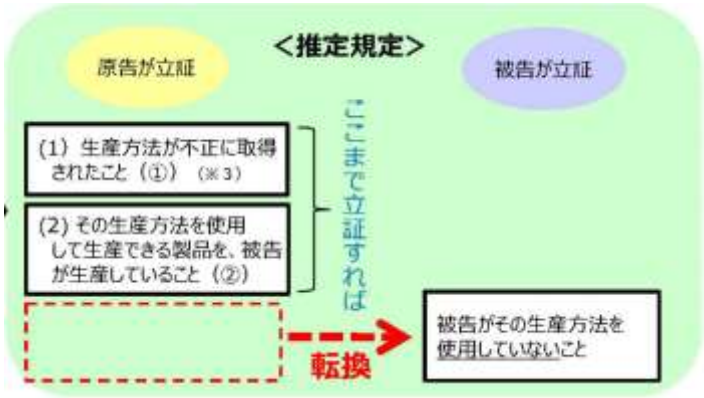
これを模式図で表すと、下記図1のとおりである。

---

[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」173・174頁

図 1 推定規定の構造[3]



ウ　対象となる営業秘密及び使用行為の内容について

不正競争防止法第 5 条の 2 は、「生産方法」について上記①～③を立証すると「生産」行為が推定される旨を規定する。加えて、同条は、「その他政令で定める情報」については「その他技術上の秘密を使用したことが明らかな行為として政令で定める行為」が推定されると規定し、政令にゆだねている。

当該政令（不正競争防止法施行令）は、「情報の評価又は分析の方法（生産方法に該当するものを除く。）」について上記①～③を立証すると、「技術上の秘密（情報の評価又は分析の方法（生産方法に該当するものを含む。）に係るものに限る。）を使用して評価し、又は分析する役務の提供」行為が推定されると規定する（同施行令第 1 条及び第 2 条[4]）。

エ　注意点

本推定規定は、すべての営業秘密に関する不正競争の立証に用いることができるものではなく、上記のとおり、不正使用類型のうちの第 4 号、第 5 号及び第 8 号の 3 類型に限られている。

また、「技術上の秘密」であるため、顧客名簿といった営業上の情報については、本推定規定を用いることはできず、技術上の秘密であってもすべてが対象とされているものではなく、上記ウのとおり一定の情報に限られる。

（４）具体的態様の明示義務について

ア　内容

不正競争防止法第 6 条は、被疑侵害者に対して、営業秘密保有者が「侵害の行為を組成

[3] 経産省知的財産政策室「不正競争防止法テキスト」58 頁（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/201909_unfaircompetitiontext.pdf）

[4] 上記施行令は、平成 30 年 11 月 1 日から施行された（平成 30 年 9 月 4 日付経産省ニュースリリース「「不正競争防止法第十八条第二項第三号の外国公務員等で政令で定める者を定める政令の一部を改正する政令」が閣議決定されました」（https://www.meti.go.jp/press/2018/09/20180904001/20180904001.html））。

したものとして主張する物又は方法の具体的態様を否認するとき」は、「自己の行為の具体的態様を明らかにしなければならない」という具体的態様の明示義務を課す。

具体的態様の明示義務は、上記（３）の推定規定が設けられるよりも前の平成 15 年改正で導入されたものである。

イ　趣旨

第 6 条の趣旨は、不正競争防止法においても、特許法第 104 条の 2 と同様の規定を設けることにより、営業秘密保有者（原告）のみならず、被疑侵害者（被告）にも侵害行為の特定に積極的に関与させ、訴訟審理の促進・争点の明確化を図るためである[5]。

ウ　具体的態様の明示を拒否できる場合

被疑侵害者（被告）としては、侵害行為に関する物または方法の具体的態様を「明らかにすることができない相当の理由がある」ときは、具体的態様の明示を拒むことができる（第 6 条但書)。「相当の理由」としては、たとえば、自己の具体的態様の内容に営業秘密が含まれている場合が考えらえる[6]。

（５）その他

訴訟記録の閲覧等制限の申立て（民事訴訟法第 92 条)、文書提出命令制度（不正競争防止法第 7 条第 1 項)、文書提出命令制度におけるインカメラ手続（民事訴訟法第 223 条第 6 項、不正競争防止法第 7 条第 2 項・第 3 項)、秘密保持命令（不正競争防止法第 10 条)、尋問の公開停止（不正競争防止法第 13 条）等を活用した立証活動をすることが考えられる。

たとえば、文書提出命令制度については、営業秘密侵害訴訟に基づく文書提出命令申立事件（東京地裁平成 27 年 7 月 27 日決定・判タ 1419 号 367 頁）において、東京地裁が以下のとおり判示し、原告が提出を求めた文書について裁判所に提出すべき旨の命令を決定した事例が参考になる。

> 不正競争防止法 7 条 1 項は，不正競争による営業上の利益の侵害に係る訴訟において，裁判所が，当事者の申立てにより，当事者に対し，侵害行為について立証するため必要な書類の提出を命ずることができる旨規定するところ，当事者間の衡平の観点から模索的な文書提出命令の申立ては許されるべきではないことや，当事者が文書提出命令に従わない場合の制裁の存在（民事訴訟法 224 条）等を考慮すると，そこにおける証拠調べの必要性があるというためには，その前提として，侵害行為があったことについての合理的疑いが一応認められることが必要であると解すべきである。

[5] 「逐条不正競争防止法」185 頁
[6] 「逐条不正競争防止法」185・186 頁

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 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
・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

４．裁判例

本文中に記載のとおり

Q61 営業秘密等の漏えい事実の立証と情報管理体制

情報漏えいが営業秘密侵害や限定提供データ侵害に該当すると裁判で認められるためには、営業秘密や限定提供データを不正に取得されたことや、情報の取得者が当該情報を使用したこと、第三者へ開示したことなどを立証する必要がある。しかし、取得対象が情報という無体物であるがゆえに、その証拠を確保することは容易ではない。そこで、情報漏えいが発生した場合に、事後的に、営業秘密や限定提供データの漏えいの事実を立証することを容易にするために、どのような方法により情報を管理しておくべきか。

タグ：不正競争防止法、営業秘密、限定提供データ

１．概要

まず、情報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必要である。

また、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、予め、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必要である。

２．解説

（１）総論

営業秘密や限定提供データ（以下「営業秘密等」という。）の情報漏えいに関する証拠を保全することは、情報を漏えいさせた者や漏えいした営業秘密等を使用した第三者に対して民事上の請求をするために必要となる。

（２）情報漏えいの事実立証のための管理体制

まず、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（３）の営業秘密の秘密管理性（詳細は Q17）の要件、また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洩時に推奨される（高度なものも含めた）包括的対策を示した経産省の秘密情報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（秘密情報保護ハンドブックの概要については、Q17 も参照）。

例えば、秘密情報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、予め、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うえ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、Q25 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、秘密情報保護ハンドブックにおいては、①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、②印刷者の氏名等の「透かし」が印字される設定の導入、③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、④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）、⑤PC 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、⑥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。

（３）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

あわせて、情報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（たとえば、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。

① 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）
② 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
③ 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
④ 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）
⑤ 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）

（４）事後的な立証方法

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、Q55

参照)。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。

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 6 項、第 2 条第 7 項、第 21 条第 1 項
・秘密情報保護ハンドブック
・限定提供データ指針

４．裁判例

特になし

Q62 民事訴訟等における情報提供

民事訴訟等において、訴訟の当事者から、自社が保有する情報の提供を求められることはあるか。

タグ：民事訴訟法、特許法、著作権法、不正競争防止法、会社法、弁護士法、弁護士会照会、証拠保全

１．概要

民事訴訟の当事者が相手方や第三者の保有する情報の提供を求める手段としては、文書提出命令、検証物提示命令、証人尋問・本人尋問、訴訟前または訴訟中の当事者照会、証拠保全、訴えの提起前の証拠収集処分、その他裁判外で弁護士会照会がある。特別法上の提出義務としては、会社法において計算書類等の提出義務が定められ、また特許法や著作権法など知的財産関係法にも書類の提出義務が規定されている。

以上のほか、裁判所を通じて釈明を求める、または、文書送付嘱託や調査嘱託を求めることも、相手方や第三者が保有する情報の提供を求める手段の一つと位置付けられる。

２．解説

（１）裁判所の命令等による証拠の提出

民事訴訟において、相手方が保有する文書その他の情報媒体は、それを訴訟に提出するかどうかの選択を保有者が持っている。しかし文書提出命令によりその文書等の提出を命じられた場合には、当該文書を提出しなければならない。文書提出義務は、平成 8 年の民事訴訟法改正により一般義務化された。この結果、裁判所は、文書提出命令の申立て（民事訴訟法第 221 条）がされた場合、証拠とすべき必要性が認められ、同法第 220 条第 4 号が掲げる提出義務除外事由に該当しない限り、文書提出命令を発し、当該文書の所持者はその提出義務を負うことになる。文書提出命令の対象には、紙媒体そのもののみならず、録音テープやビデオテープ、デジタルデータの記録された記録媒体なども含まれる。

こうした文書提出義務と類似の規定は、他の法令にもみられる。例えば、知的財産権の侵害訴訟においては、侵害行為を立証するため、又は侵害行為による損害の計算をするため、必要な書類の提出命令が規定されている（特許法第 105 条、著作権法第 114 条の 3、不正競争防止法第 7 条等[1]）[2]。また、会社法においては、計算書類等（同法第 443 条、第 619 条）、会計帳簿（同法第 434 条、第 616 条）、貸借対照表等（同法第 498 条）、財産目録等（会社法第 493 条、第 659 条）の提出命令が規定されている。当事者が文書提出命令に従

[1] Q63 も参照。
[2] なお、平成 31 年特許法改正により導入される予定の査証制度（裁判所が指定する中立的な技術専門家（査証人）が、被侵害者の工場等に立ち入り、特許権の侵害立証に必要な調査を行い、裁判所に報告書を提出することができる制度）については、Q63 を参照。

わない場合、裁判所は、相手方の当該文書の記載に関する主張を真実と認めることができ、また、相手方が、当該文書の記載に関して具体的な主張をすること及び当該文書により証明すべき事実を他の証拠により証明することが著しく困難な場合には、その文書によって証明しようとした事実に関する主張を真実と認めることができる（民事訴訟法第 224 条）。また、訴訟の当事者ではない第三者が文書提出命令に従わない場合には、過料の制裁を課されることがある。文書の内容ではなく物の形状や性質などを証拠資料とする検証についても、文書と同様に検証物提示命令の規定（民事訴訟法第 232 条による第 223 条の準用）がある。なお文書であっても、その形状や改ざんの有無などを明らかにするための証拠調べは検証によることになる。

裁判所は、原則として誰でも証人として尋問することができ、また、当事者本人を尋問することができる。当事者は、自己に協力的な証人や自分自身の尋問を申し出ることも、いわゆる敵性証人の尋問を求める、あるいは、相手方当事者の尋問を申し出ることも可能である。証人が正当な理由なく出頭せず、又は証言拒絶権や宣誓拒絶事由がないにもかかわらず証言や宣誓を拒んだ場合には、過料や罰金の制裁が課されることがある。また、宣誓の上で虚偽の事実を述べれば、偽証罪の制裁が課されることがある。当事者尋問の場合、偽証罪の適用はないが、正当な理由のない不出頭や陳述拒絶、宣誓拒絶があった場合には、裁判所は、尋問事項に関する相手方当事者の主張を真実と認めることができ、また虚偽の陳述があった場合には過料の制裁を課すことがある。

（２）その他の場合

上記（１）と異なり、制裁を伴わない制度としては、当事者照会（民事訴訟法第 163 条）があり、照会を受けた相手方は照会に対して回答する義務があると解されているが、制裁規定を欠くため、ほとんど利用はされていないとの指摘がある。また、裁判長は、訴訟関係を明瞭にするため、事実上及び法律上の事項に関し、当事者に対して問いを発し、又は立証を促すことができ（釈明権）、実務上活用されている。当事者が相手方に対して主張や立証を求める場合、裁判長に発問を求めるという形がとられる。これを実務上は求釈明という。このほか、裁判所は、必要な調査を官庁等の団体に対して嘱託することができ（民事訴訟法第 186 条）、また、当事者は、文書の所持者にその文書の送付を嘱託することを裁判所に申し立てることができ（民事訴訟法第 226 条）、これらも実務上活用されている。

（３）訴えの提起前における証拠収集

訴えの提起の前後にかかわらず、証拠調べの対象となる物が滅失するおそれがあるなど、あらかじめ証拠調べをしておかなければその証拠を使用することが困難となる事情があると認められる場合、裁判所は証拠調べをすることができ（証拠保全　民事訴訟法第 234 条以下）、医療事故紛争における患者側が医療側の保有する医療記録について改ざんのおそれを理由として証拠保全を申し立てることは実務上よくある。また、訴えを提起しようとする

者が訴えの被告となるべき者に対し訴えの提起を予告する通知を書面ですることなどを要件として、訴えの提起前における当事者照会及び証拠収集処分（文書送付嘱託等）がある（民事訴訟法第 132 条の 2）。

（４）弁護士会照会

民事訴訟法上の制度とは別に、民事には限られないが、弁護士会照会（弁護士法第 23 条の 2）が行われている。弁護士会照会により、弁護士は、受任している事件について、所属弁護士会に対し、公務所又は公私の団体に照会して必要な事項の報告を求めることを申し出ることができ、弁護士会は、その申出に基づき、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

３．参考資料（法令・ガイドラインなど）

・民事訴訟法第 132 条の 2～第 132 条の 4、第 149 条、第 163 条、第 186 条、第 190 条、第 211 条、第 220 条、第 223 条～第 226 条、第 232 条、第 234 条
・弁護士法第 23 条の 2、第 30 条の 21
・外国弁護士による法律事務の取扱いに関する特別措置法第 50 条
・沖縄の弁護士資格等に対する本邦の弁護士資格等の付与に関する特別措置法第 7 条
・沖縄弁護士に関する政令第 10 条
・会社法第 443 条、第 493 条、第 498 条、第 616 条、第 619 条、第 659 条
・特許法第 105 条
・著作権法第 114 条の 3
・不正競争防止法 7 条

４．裁判例

文書提出命令に対する提出拒絶が問題となった事例につき、Q63 参照。

Q63 民事訴訟における営業秘密やプライバシーに関する情報の非公開の可否

民事訴訟において、営業秘密やプライバシーに関する情報を公開しないことができるか。

タグ：民事訴訟法、特許法、不正競争防止法、著作権法、証言拒絶、文書提出命令、インカメラ手続、閲覧等制限、査証制度

１．概要

証人尋問・当事者尋問には不出頭や証言拒否等に一定の制裁が設けられており、また、文書の所持者は、文書提出命令が発せられた場合には、文書提出義務を負う。そして、民事訴訟手続は公開が原則であり、何人も訴訟記録の閲覧を請求することができる。

しかし、秘密として保護されるべき情報等は、証言義務や文書提出義務等を免れることができる場合がある。また、訴訟記録中の営業秘密等が記載された部分は閲覧等制限の対象となることがある。加えて、営業秘密の侵害訴訟などにおいては、秘密保持命令制度と当事者尋問等の公開停止の措置が導入されており、裁判の公開と秘密保護との両立が図られている。

なお、令和元年の特許法改正により、新たに創設された証拠収集手続である査証制度においても、秘密保護の仕組みが導入されている。

２．解説

（１）証言や文書提出の拒絶事由等

民事訴訟において、営業秘密もしくはプライバシーに関する情報について証言を求められた場合、またはそのような情報を含む文書の提出を求められた場合、①証言については、民事訴訟法第 197 条第 1 項第 3 号の技術又は職業の秘密に関する事項についての証言拒絶権の要件に該当すれば、証言を拒むことができ、②文書の提出については、同号の職業の秘密に関する民事訴訟法第 220 条第 4 号ハの文書提出義務の除外事由[1]または同号ニの自己使用文書の提出義務除外事由[2]に該当すれば、提出を拒むことができる。

上記①に関し、営業秘密やプライバシーに関する情報を「職業の秘密」として保有する場

[1] 民事訴訟法第 220 条第 4 号は文書提出義務を一般義務化し、提出義務が認められるか否かは、同号イ～ホに規定される除外事由の有無によって決せられる。
同号ハは、「第百九十七条第一項第二号に規定する事実又は同項第三号に規定する事項で、黙秘の義務が免除されていないものが記載されている文書」と規定する。なお、同法第 197 条第 1 項第 2 号は、「医師、歯科医師（中略）の職にある者又はこれらの職にあった者が職務上知り得た事実で黙秘すべきものについて尋問を受ける場合」と規定し、同項第 3 号は、「技術又は職業の秘密に関する事項について尋問を受ける場合」と規定する。

[2] 民事訴訟法第 220 条第 4 号ニは、「専ら文書の所持者の利用に供するための文書（国又は地方公共団体が所持する文書にあっては、公務員が組織的に用いるものを除く。）」と規定する。

合、職業の秘密に関する証言拒絶については、判例によれば、その事項が公開されると当該職業に深刻な影響を与え、その遂行が困難になるもののうち、保護に値する秘密についてのみ証言拒絶が認められ、保護に値する秘密かどうかは、秘密の公表によって生ずる不利益と証言の拒絶によって犠牲になる真実発見及び裁判の公正との比較衡量により決せられるとされている。

上記②に関し、自己使用文書として文書提出義務の除外事由に該当する（民事訴訟法第220条第4号二の提出義務除外事由に該当する）ためには、判例によれば、ある文書の作成目的・記載内容・現在の所持者が所持するに至るまでの経緯・その他の事情から判断して、専ら内部の利用に供する目的で作成され、外部に開示されることが予定されておらず、開示によって所持者に看過し難い不利益が生ずるおそれがあり、自己使用文書に該当することを否定すべき特段の事情がないことを要するとされている。

また、営業秘密の不正取得等によって営業上の利益を侵害されたことを訴える訴訟や特許権侵害訴訟や専用実施権侵害訴訟（以下、まとめて「営業秘密侵害訴訟等」という）などにおいては、侵害行為の立証又は侵害行為による損害額の立証に必要な文書の提出を求めることができるものの、文書の所持者には「正当な理由」による提出拒絶が認められている（不正競争防止法第7条第1項、特許法第105条第1項、著作権法114条の3第1項など）。

（2）インカメラ審理

訴訟当事者に対する営業秘密やプライバシーに関する情報を含む文書について文書提出命令の申立てがなされ、当該訴訟当事者が当該文書の提出を拒む場合は、同報第220条第4号（ただし、同号ホは除く。）に該当するか否かを判断するため、裁判官だけが文書を見るいわゆるインカメラ審理がなされ得る（民事訴訟法第223条第6項）。

これは、民事訴訟法第220条第4号が除外事由を認めて、文書所持者の秘密等を保護しようとするものであることから、秘密等が漏えいすることを防止しつつ、文書の記載内容を裁判所が確認して除外事由の判断を迅速かつ適正に行うことができるようにする手続である[3]。インカメラ審理においては、裁判所に対象となる文書を提示し裁判所だけに閲読してもらい、当該文書に対する文書提出命令申立ての適否を判断してもらうこととなる。

また、営業秘密侵害訴訟等においては、侵害訴訟におけるインカメラ手続の拡充が図られている（不正競争防止法第7条第2項～第4項、特許法第105条第2項～第4項、著作権法第114条の3第2項～第4項など[4]）

[3] 菊井維大＝村松俊夫原著「コンメンタール民事訴訟法４［第２版］」493・494頁（日本評論社）

[4] 従来は、いずれの法律においても、書類の提出を拒むための「正当な理由」の判断のためにのみインカメラ審理が認められていたが、平成30年の不正競争防止法及び特許法の改正により、これらの法律については、そもそも「必要な書類」といえるかどうかについてもインカメラ審理が認められることとなった。なお、著作権法においては、「正当な理由」の有無について

（３）閲覧等制限

閲覧等制限は、訴訟記録中に当事者の私生活上の重大な秘密、当事者が保有する営業秘密等が記載又は記録されている場合に、当該部分の閲覧若しくは謄写、その正本、謄本若しくは抄本の交付又はその複製の請求をすることができる者を、訴訟の当事者だけに限ることを認める裁判所の決定をいう（民事訴訟法第 92 条第 1 項）。

閲覧等制限の効果は、これを認める裁判所の決定があった場合のほか、閲覧等制限の申立てがあってからその裁判が確定するまでの間においても暫定的に発生する（同条第 2 項）。

（４）秘密保持命令

営業秘密侵害訴訟等では、秘密保持命令が導入されている（不正競争防止法第 10 条、特許法第 105 条の 4）。営業秘密侵害訴訟等では、営業秘密に属する事項を主張立証の中で開示せざるを得ないことが多いため、公開を恐れて十分な訴訟活動ができないことのないよう、適正な裁判のために訴訟における営業秘密の保護を図るものである。

具体的には、当事者の申立てにより、訴訟において提出された準備書面や証拠書類に営業秘密が含まれている等の事由について疎明があった場合には、裁判所が、当該準備書面等を訴訟追行以外の目的で使用することや、秘密保持命令を受けた者以外に開示することを禁止する内容の秘密保持命令を発することができ、同命令に違反した場合は刑事罰が科される。

なお、上記（２）のとおり、営業秘密侵害訴訟等では、通常の民事訴訟と異なり、文書提出命令申立手続において行われるインカメラ審理を拡充し、申立人やその代理人の立会いを認めているため（不正競争防止法第 7 条第 3 項、特許法第 105 条第 3 項）、立ち会った申立人等も秘密保持命令の対象となる[5]。

（５）当事者尋問等の公開停止

営業秘密侵害訴訟等では、当事者尋問等の公開停止があり得る（不正競争防止法第 13 条など[6]）。そもそも裁判の公開は憲法上の要請であり、従来は少なくとも訴訟事件について非公開審理を認めることに極めて慎重であった。しかし、秘密保護やプライバシー保護の要請が強くなり、訴訟記録の閲覧制限だけでは秘密保護が不十分であり、他方で、審理の充実も必要であり、秘密保護のための証言拒絶、文書提出拒絶を一方的に拡張することは適当では

のみインカメラ審理が認められている（著作権法 114 条の 3 第 2 項）が、この点については、文化審議会著作権分科会「文化審議会著作権分科会報告書」（平成 31 年 2 月）98 頁・99 頁において、特許法等と同様の改正を行うことが適当である旨の報告がなされており、今後特許法等と同様の法改正が行われる見込みである。

[5] なお、秘密保持命令は、不正競争防止法及び特許法のほか、著作権法、商標法、意匠法、実用新案法及び種苗法においても規定されている。

[6] なお、当事者尋問等の公開停止は、不正競争防止法のほか、特許法、実用新案法及び種苗法においても規定されている。

ないため、平成 16 年の改正により、例外的に非公開審理の可能性を認め、裁判の公開と秘密保護とを両立させたものである。

具体的には、営業秘密侵害訴訟等で当事者本人、法定代理人、証人が当事者の保有する営業秘密について尋問を受ける場合に、公開の法廷で陳述することにより当事者の事業活動に著しい支障を生ずることが明らかな営業秘密が含まれているために営業上の利益の侵害の有無についての判断の基礎となる事項について十分な陳述ができず、かつ他の証拠のみによっては当該侵害の有無について適正な裁判ができないと認められるときに、裁判官全員一致の決定によって、尋問が非公開となる。

（６）査証制度

令和元年の特許法改正により、特許権の侵害に係る訴訟における当事者の証拠収集手続を強化するため、新たに第 105 条の 2 等が新設され、特許権の侵害の可能性がある場合、裁判所が指定する中立的な技術専門家（査証人）が、被疑侵害者の工場等に立ち入り、特許権の侵害立証に必要な調査を行い、裁判所に報告書を提出することができる制度（査証制度）が設けられた[7]。査証命令の発令要件は、侵害行為の立証への必要性、特許権侵害の蓋然性、他の手段では証拠が十分に集まらないという補充性、及び相手方の負担が不相当なものにならないという相当性である。このような新たな証拠収集制度においては、査証人の選定に係る忌避申立て、報告書中の秘密情報の黒塗り、及び査証人の秘密漏えいに対する刑事罰を設けることによって秘密保護の仕組みが導入されている。

（７）訴訟当事者ではない場合

訴訟の当事者ではない第三者に対しても、文書提出命令の発令がなされることがある。この場合、手続保障のため、裁判所が口頭または書面による審尋を行うため（民事訴訟法第 223 条第 2 項）、当該第三者（被申立人）としては、申立ての対象となった文書に秘密情報やプライバシーに関する情報が記載されている旨を主張することができる。

また、文書送付嘱託の決定（民事訴訟法第 226 条）により、所持する文書の送付を嘱託されることがあるが、文書を所持する企業は正当な理由がある場合は、嘱託を拒絶することを妨げないため、当該文書に秘密情報やプライシーに関する情報が記載されているときは、提出しないことができる。

３．参考資料（法令・ガイドラインなど）

・民事訴訟法第 92 条、第 197 条、第 220 条、第 223 条第 1 項・第 6 項、第 226 条など
・不正競争防止法第 7 条、特に同条第 3 項、第 10 条～第 13 条

[7] 特許法等の一部を改正する法律（令和元年法律第 3 号）参照。査証制度は、公布の日（令和元年 5 月 17 日）から 1 年 6 月を超えない範囲内において政令で定める日から施行される（同法附則第 1 条第 3 号）。

・特許法第 105 条、特に同条第 3 項、第 105 条の 2～第 105 条の 2 の 10、第 105 条の 4～第 105 条の 7、第 200 条の 2（ただし、査証制度施行後の条文番号）
・著作権法第 114 条の 3

４．裁判例

・最決平成 11 年 11 月 12 日民集 53 巻 8 号 1787 頁
・最決平成 12 年 3 月 10 日民集 54 巻 3 号 1073 頁
・最決平成 13 年 12 月 7 日民集 55 巻 7 号 1411 頁
・最決平成 16 年 11 月 26 日民集 58 巻 8 号 2393 頁
・最決平成 18 年 2 月 17 日民集 60 巻 2 号 496 頁
・最決平成 18 年 10 月 3 日民集 60 巻 8 号 2647 頁
・最決平成 19 年 8 月 23 日判時 1985 号 63 頁・判タ 1252 号 163 頁
・最決平成 19 年 11 月 30 日民集 61 巻 8 号 3186 頁
・最決平成 19 年 12 月 11 日民集 61 巻 9 号 3364 頁
・最決平成 21 年 1 月 27 日民集 63 巻 1 号 271 頁

Q64 自社に不利な証拠となり得る社内文書の破棄について

自社に不利な証拠となり得る情報が記載された社内文書を破棄した場合、破棄したことで訴訟上の不都合を招くことはあるか。

タグ：民事訴訟法、文書提出命令、証明妨害、e-Discovery

１．概要

文書提出命令の対象となる文書を破棄すれば、裁判所がその文書の記載に関する相手方の主張を真実と認めることができるという規定があり、提出義務がないとしても、不利な内容の文書が破棄された事実が明るみに出れば、裁判所が不利益に考慮する可能性がある。

２．解説

（１）証明妨害

文書提出命令に従わない場合について、民事訴訟法第 224 条第 1 項は「裁判所は、当該文書の記載に関する相手方の主張を真実と認めることができる」と定め、文書提出義務を負う文書について、同条第 2 項は「当事者が相手方の使用を妨げる目的で提出の義務がある文書を滅失させ、その他これを使用することができないようにしたときも、前項と同様とする」と定め、同条第 3 項ではさらに「相手方が、当該文書の記載に関して具体的な主張をすること及び当該文書により証明すべき事実を他の証拠により証明することが著しく困難であるときは、裁判所は、その事実に関する相手方の主張を真実と認めることができる」と定めている。

これは講学上「証明妨害」と呼ばれる。民事訴訟法第 224 条第 2 項にいう「提出の義務がある文書」とは、同法第 220 条の提出義務があると定められている文書であって、実際の文書提出命令の有無とは関係がなく、文書の破棄等の行為は、裁判所が提出命令を発する以前に行われても同法 224 条第 3 項に当たると解される。

（２）実務上の取扱い

例えばカルテの改ざんのケースのように、証拠となることが当然予想できる文書や、法令上作成・保管が要求されている文書、事業の性質上、通常あるはずの文書について滅失、毀損、または改ざんを施せば、裁判所が不利益に考慮する可能性があるため、証明妨害とならないように不用意に文書を破棄することは避けるべきである。

裁判例に現れた例では、当事者が文書を破棄したことを理由に当該文書の記載に係る相手方の主張や当事者尋問における供述を真実と認めた事例として、本庄簡判平成 19 年 6 月 14 日判タ 1254 号 199 頁及び東京地判平成 6 年 3 月 30 日タ 878 号 253 頁がある。また、破棄の事例に限らなければ、裁判所の文書提出命令に従わなかったとして当該文書の記載

に係る相手方の主張を真実と認めた事例は複数あり、特許権侵害訴訟において民事訴訟法第 224 条第 3 項を適用して、被告による侵害物件の販売台数に係る原告の主張を真実と認めた知財高判平成 21 年 1 月 28 日判タ 1300 号 287 頁がある。

（３）アメリカの e-Discovery 対策

なお、この関連でアメリカ連邦民訴規則における e-Discovery のための証拠保存義務も、渉外取引を行う企業にとっては極めて重要である。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。

（４）その他

デジタル・フォレンジックによる削除されたメールやファイル等のデータの抽出又は復元については、Q55 を参照されたい。

３．参考資料（法令・ガイドラインなど）

・民事訴訟法第224条

４．裁判例

本文中に記載したもののほか、

・東京地判平成27年8月13日平25（ワ）8002号
・東京高判平成24年6月4日判タ1386号212頁
・東京地判平成22年2月24日平21（ワ）12668号

Q65 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について、刑法上どのような罰則があるか。

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

不正プログラムによって企業活動を阻害した場合は、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毀棄罪などにより処罰され得る。

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[1]を含む不正指令電磁的記録を作成した場合や、阻害した場合は、不正指令電磁的記録に関する罪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は、電子計算機損壊等業務妨害罪や電磁的記録毀棄罪など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、国民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、不正な指令を有するプログラムが実行されれば、社会生活に深刻な被害をもたらす可能性がある。

しかし、このような不正プログラムに対して、コンピュータの社会的機能を保護する必要性があるにもかかわらず、平成 23 年改正以前の刑法では、不正のプログラムを用いて一定の結果を生じさせた場合に、電子計算機損壊等業務妨害罪（刑法第 234 条の 2）や公電磁的記録毀棄罪（同法第 258 条）等が成立するにとどまっていた。

---

[1] 「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。

そこで、これらの不正指令電磁的記録を作成、提供、供用、取得及び保管する行為を処罰できるように、平成23年に刑法が改正され、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）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19章の2）は、コンピュータに不正な指令を与える電磁的記録である、いわゆるコンピュータ・ウイルスに関して、刑法第168条の2第1項第1号及び第2号の定義を満たす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。）の作成、供用等を処罰対象としている。

いわゆるコンピュータ・ウイルスは、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[2]、ワーム[3]、スパイウェア[4]等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同条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

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。同項第2号は、プログラムのソースコードを記録した電磁的記録や紙に印刷したもの等も含まれることを意味する。

「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）ものかどうかの「意図」は、「個別具体的な使用者の実際の認識を基準として判断するのではなく、当該プログラムの機能の内容や、機能に関する説明内容、想定される利用方法等を総合的に考慮して、その機能につき一般に認識すべきと考えられるところを基準として判断する」[5]。

「例えば、ハードディスク内のファイルを全て消去するプログラムがその機能を適切に

---

[2] 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。

[3] 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。

[4] 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。

[5] 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)

説明した上で公開されるなどしており、ハードディスク内のファイルを全て消去するという動作が使用者の『意図に反する』ものでない場合は、処罰対象とはならない」[6]が、他方で、当該プログラムを当局からの通知文書であるかのように装い、「事情を知らない第三者に電子メールで送り付け、その旨を誤信させて実行させ、ハードディスク内のファイルを全て消去させたというような場合には、そのプログラムの動作は、使用者の『意図に反する』『不正な』もの」[7]に当たり、不正プログラムとして処罰対象となり得ると考えられる。

次に、不正プログラムの対象は「不正な」指令（不正性）とされているところ、当該要件については、プログラムが有する機能を踏まえ、社会的に許容し得るものであるか否かという観点から判断されることとなる[8]。

なお、バグ（プログラムを作成する過程で作成者も気付かないうちに発生するプログラムの誤りや不具合）は、重大なものも含め、コンピュータの使用者には「バグは不可避的なものとして許容されていると考えられることから、その限りにおいては、『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』との要件も『不正な』との要件も欠くこととなり、」[9]不正プログラムには該当しない。

刑法では、不正指令電磁的記録に関する罪として、作成、提供、供用、取得及び保管の5つの行為に対して処罰が規定されているところ、本問に関係する同作成罪及び同供用罪について解説する。

ア　不正指令電磁的記録作成罪（刑法第168条の2第1項）

不正指令電磁的記録作成罪が成立するには、「正当な理由がないのに」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することが必要である。「実行の用に供する目的」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る状態に置く目的のことをいう。不正プログラムを作成した時点でこの目的がなければ成立しない。

また、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研究やウイルス対策ソフトの開発を行う場合には、不正プログラムを作成することがあり得るところ、このような場合には人のコンピュータで「実行の用に供する目的」が欠けることなり、更に「正当な理由がある」場合にも該当す

[6] 前掲5参照。
[7] 前掲5参照。
[8] 前掲5参照
[9] 前掲5参照。

るといえる。これらのような場合に不正指令電磁的記録作成罪等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ている。

不正指令電磁的記録作成罪及び同提供罪を犯した者は、3 年以下の懲役又は 50 万円以下の罰金に処せられる。

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には、「正当な理由がないのに」不正プログラムを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、事情を知らない使用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」等がこれに当たり得る[10]。企業活動を阻害しようとして、不正プログラムを電子メールに添付して送付し、事情を知らない企業の従業員等が電子メールを受信して、不正プログラム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であれば、本罪が成立する可能性がある。

当該不正プログラムが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ものであることは不要である。

不正指令電磁的記録供用罪を犯した者は、3 年以下の懲役又は 50 万円以下の罰金に処せられる。また、同供用罪は、未遂犯も処罰される（同条第 3 項）。

（4）その他

不正プログラム等に関する罪以外にも、何らかの方法でコンピュータに侵入し又は操作ができる状態にし、コンピュータ内に保存してあるデータ等を権限なく不正に追加、修正、変更、削除等を行った場合には、以下の罪により処罰され得る。

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 年以下の懲役又は 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 年以下の懲役又は 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）、同未遂罪（刑条第 4 項）	対象となる電磁的記録が私電磁的記録の場合には 5 年以下の懲役又は 50 万円以下の罰金に、公電磁的記録の場合には 10 年以下の懲役又は 100 万円以下の罰金

[10] 前掲 5 参照。

電子計算機損壊等業務妨害罪（刑法第 234 条の 2）	5 年以下の懲役又は 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 年以下の懲役
私電磁的記録毀棄罪（刑法第 259 条）	5 年以下の懲役
公電磁的記録毀棄罪（刑法第 258 条）	3 月以上 7 年以下の懲役

３．参考資料（法令・ガイドラインなど）

・刑法第 157 条、第 158 条、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「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）

４．裁判例

・千葉地判平成 25 年 11 月 8 日（平成 25 年（わ）第 1111 号、1204 号）

・京都地判平成 27 年 7 月 3 日（平成 24 年（わ）第 133 号、232 号）

・広島地判平成 27 年 12 月 7 日（平成 27 年（わ）第 147 号、202 号、341 号、431 号）

Q66 電磁的記録不正作出罪

Web 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

Web サイトに登録されたユーザデータ、すなわち、電磁的記録を変更するなど不正にデータを改ざんする行為は、電磁的記録不正作出罪（刑法第 161 条の 2）に該当し得る。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、他人の財産上、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、義務又は事実証明の用に関する」とは、権利、義務の発生、存続、変更、消滅の効果等を生じさせることを目的とするもの、または実社会生活に交渉を有する事項を証明するに足りるもの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。

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 年以下の懲役又は 50 万円以下の罰金に処する。

電磁的記録不正作出罪は、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ところ、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。人の事務処理とは、他人の財産上、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、消滅の効果等を生じさせるものをいい、オンライン化された銀行元帳ファイル記録、乗車券の磁気ストライプ部分等が当たり得る。

「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ものをいい、裁判例では、パソコン通信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日判例時報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（後述する大阪高判平成19年3月27日判タ1252号174頁）がこれに当たるとしたものがある。

本罪は、「関する」という単語が使われており、電子計算機使用詐欺罪(刑法第246条の2)の「係る」とは異なるところ、電子計算機使用詐欺罪においては、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。

「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[1]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年以下の懲役又は100万円以下の罰金に処する。

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。

なお、私電磁的記録、公電磁的記録のいずれの電磁的記録も、文書と異なり、作出に当たって印章や署名が用いられることは規定されていない。

（３）裁判例

ア　大阪高判平成19年3月27日判タ1252号174頁

大阪高裁は、以下のように、Y社が運営するオークションを利用するY社会員のパスワ

[1] 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。

ードは、事実証明に関する電磁的記録であり、出品された商品に対する入札情報は、権利、義務に関する電磁的記録であると判示した。

被告人は、「Y 社の事務処理を誤らせる目的で、…Y 社が設置管理する電子計算機(サーバコンピュータ)に対し、Y 社会員 2 名がパスワードを変更した事実がないのに、同会員らがパスワードを変更する手続を取った旨の虚偽の情報を送信し、上記サーバコンピュータに接続された記憶装置に同情報を記憶蔵置させ、事実証明に関する電磁的記録を不正に作出し」たと判示し、Y 社会員のパスワードは事実証明に関する電磁的記録に該当すると判断した。

また、被告人は、「Y 社及び同会員らの事務処理を誤らせる目的で、ほしいままに、…多数回にわたり、…サーバコンピュータに対し、実際は、同会員が、オークションにおいて…出品された商品に対して入札を行った事実がないのに、同会員が同商品に対して入札を行った旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、…権利、義務に関する電磁的記録を不正に作出し」たと判示し、オークションにおける入札情報が権利、義務に関する電磁的記録に該当すると判断した。

なお、罪数に関しては、これらの電磁的記録不正作出罪、当該電磁的記録を Y 社の事務処理の用に供した不正電磁的記録供用罪及び Y 社会員らのアカウントに不正アクセスを行った不正アクセス禁止法違反について、前者 2 つの罪は牽連犯であるが、これらと不正アクセス禁止法違反とは併合罪の関係にあると判示している。

イ　大阪高判平成 26 年 5 月 22 日（平成 26 年（う）第 121 号）

大阪高裁は、以下のように、A 社が開発した衛星放送を視聴するための A カードは権利、義務に関する電磁的記録であり、A カードを用いた事務処理も観念でき、A カードの電磁的記録を改変する行為は、私電磁的記録不正作出罪の構成要件を客観的に充足すると判示した。

原判決は、A 社等が開発した A カードにより、「『暗号化した番組の映像・音声等の信号を用い、限定された者が受信機で暗号を復号し、映像・音声等を受信して視聴すること』が可能となる」ものであり、「A カードの所有権は A 社に帰属し、…利用者は…貸与契約に基づき A カードを利用するに」過ぎないこと等から、「A カードは、衛星放送事業者と視聴申込者との間で交わされた、当該衛星放送を視聴する旨の契約に係る権利・義務の発生、存続、変更、消滅に関する電磁的記録であること、衛星放送事業者は、A カードを用いて、当該衛星放送の視聴の可否を管理する」等して、「財産上、身分上その他人の社会生活に影響を及ぼし得ると認められる事柄を処理している」と判断した。大阪高裁は、これに付言して、A カードの受信方式や視聴可能となる方式の説明を加えた上で、「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、…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…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」と認定した。

その上で、大阪高裁は、「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、…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」と判断した。

３．参考資料（法令・ガイドラインなど）

・刑法第 7 条の 2、161 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

４．裁判例

本文中に記載のとおり

Q67 電算機使用詐欺

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成りすましてログイン[1]し、別の銀行口座に送金するような場合、電子計算機使用詐欺罪により処罰され得る。同罪は、「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」る行為、及び「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」する行為を処罰の対象としている。

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年以下の懲役に処する。

（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されるものについて、その処罰を可能にするために創設された規定である。

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

[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うる。詳細については Q70 を参照。

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、電子計算機で使用する当該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 日高裁判例集 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の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」に当たるとした判例がある（最決平成 18 年２月 14 日最高裁判所判例解説刑事篇（平成 18 年度）56 頁）。クレジットカードの名義人でない者が名義人に成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のは、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）、部外者が点検員等を装って農協のオンラインシステムの端末機を不正に操作して自己の仮名口座に振込入金を行った事例（高松地判平成元年４月 26 日公刊物未登載）などがある。

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 Q66 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。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 日判例時報 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。

「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。前記最高裁決定は、「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。

（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、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。

３．参考資料（法令・ガイドラインなど）

・刑法第 246 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）

４．裁判例

本文中に記載のとおり

Q68 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。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、Q71 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、加盟店にクレジット決済端末の IC 化の対応を求めている（詳細については Q13 を参

照）[1、2]。

また、平成 12 年からデビットカード[3]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。

（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（同法第 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、支払用カードを構成する電磁的記録に関する規定が整備された。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（刑法第 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 年以下の懲役又は 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（刑法第 163 条の 3）は、5 年以下の懲役又は 50 万円以下の罰金に、刑法第 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（刑法第 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 年以下の懲役又は 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、刑法第 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（刑法第 163 条の 5）。

なお、電磁的記録不正作出罪の詳細については Q66 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 Q67 を参照されたい。

（３）クレジット決済端末の 100%の 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。現在、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移行が進められている。IC

---

[1] 割賦販売法令関係資料（https://www.meti.go.jp/policy/economy/consumer/credit/112kappuhanbaihoukankeishiryou.html）

[2] 「「割賦販売法の一部を改正する法律案」が閣議決定されました」（https://www.meti.go.jp/press/2016/10/20161018001/20161018001.html）

[3] デビットカードとは、金融機関発行のキャッシュカードを加盟店店頭での支払い時に利用できるサービスのことである。

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、極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）

・刑法第 163 条の 2（支払用カード電磁的記録不正作出等）、第 163 条の 3（不正電磁的記録カード所持）、第 163 条の 4（支払用カード電磁的記録不正作出準備）、第 163 条の 5（未遂罪）
・割賦販売法

４．裁判例

特になし

Q69 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、個情法、行個法、独個法、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、情報の不正入手、漏えい、ダークウェブ

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、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。

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。

（２）個人情報データベース等提供罪等

個人情報取扱事業者も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し、又は盗用した場合には罰則が科される（個情法第 83 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 87 条）。

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 17 条）等が義務づけられており、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 84 条）となる。

その他個情法以外の個人情報保護に関する主な法令においては、例えば、行個法第 54 条、独個法第 51 条、及び番号利用法第 49 条、第 57 条にも個情法第 83 条と類似の罰則が設けられており、個人情報保護条例においても、漏えい者に対する罰則が規定されている例が多い[1]。

その他、行個法、独個法及び番号利用法においては、個情法第 83 条と類似の罰則以外にもいくつか罰則が設けられており、例えば、行個法第 57 条、独個法第 54 条、及び番号利用法第 51 条においては、保有個人情報等を不正の手段で開示させた場合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 年以下の懲役又は 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）、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 参照）。

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。

（４）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、国家公務員法や地方公務員法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

[1] 個人情報保護関係法令全般については Q10 を参照。

おいて守秘義務違反の罪が規定されている。

（５）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 2 条第 1 項）、「有線電気通信」（有線電気通信法第 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。

通信の秘密を侵害する行為は、知得（積極的に通信の秘密を知ろうとする意思のもとでこれを取得すること）、窃用（通信当事者の意思に反して利用すること）、漏えい（他人が知り得る状態に置くこと）であるが、無線通信については、誰でも無線通信を受信することが可能であるという特質があるため、知得については、処罰の対象となっていない。もっとも、窃用又は漏えいの目的で暗号通信を復元した場合に通信の秘密侵害罪が成立する（電波法第 109 条の 2）。

（６）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（Q70 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、窃盗罪や横領罪が成立し得る。

（７）ダークウェブからの情報取得

今日においては、ダークウェブにおいて取得した情報をもとに顧客に対してサイバーセキュリティ上の脅威となる情報の提供などを行う、いわゆる脅威インテリジェンスサービスを提供する企業が増加しつつある。

ダークウェブとは、インターネットを使用するものであるが、一般的なウェブブラウザでは閲覧することができず、また、一般的な検索エンジンでも探すことができず、アクセスするためには特定のソフトウェアや設定、認証が必要なもの、と一般的にいうことができるが、確立した定義が存在するものではない。

ダークウェブは、匿名性の高いアクセスを可能としているものが多く、その一部については、漏えいしたクレジットカード情報や、児童ポルノの販売など、違法なコンテンツを提供

しているものもある。

このようなダークウェブから、例えばサイバー攻撃により不正に入手された個人データを取得するような場合、それが不正な手段によらない個人情報の取得といえるか（個情法第17条第1項）など、情報の取得が適法かどうか、さらに、そのように取得された情報をもとに脅威情報の提供などを受けることに問題はないか等を個別の事例に即して慎重に検討する必要があると考えられる。

３．参考資料（法令・ガイドラインなど）

・個情法第17条、第83条、第87条
・行個法第54条、第57条
・独個法第51条、第54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
・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

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
・最判平成30年12月3日判時2407号106頁

Q70 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「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、上述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（本項２(5)参照）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）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

Web 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。

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。

---

[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・45 頁参照。

（４）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 年以下の懲役または 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。

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。

（５）その他不正アクセス行為の予備的行為について[3]

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 業務その他の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 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）

（６）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（後掲）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[4]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。

---

[3] 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 Q71 を参照。
[4] ネットワーク上で通信するための手順や規約。

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。

なお、本判決に対しては控訴がなされておらず、すでに確定しているため、この問題に関する上級審の判断はまだ出されていない。

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、刑(わ)第 2373 号　等

Q71 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、これらのホームページ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述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 Web 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、不正アクセス禁止法第 7 条各号で禁止する行為ではなく割賦販売法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。

２．解説

（１）不正アクセス禁止法第 7 条各号で禁止する行為

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

[1] サイバーセキュリティ 2019・367 頁

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（不正アクセス禁止法第 2 条第 1 項）が公開した Web 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 Q70 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 Web 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、Web 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[2]）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 Web 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 Web 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

[2] 「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」https://www.j-credit.or.jp/security/pdf/plan_2019.pdf）。

49 条の 2 第 2 項本文)。

割賦販売法 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 年以下の懲役又は 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）フィッシング行為への処罰

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。

しかし、クレジットカード番号等の情報を入力させる目的で Web サイトを公開した場合や、クレジットカード番号等の情報や ID・パスワード等の識別符号を入力させる Web サイトへ誘導するための電子メールを送信した場合、それらの行為のみをもっては、いずれも不正アクセス禁止法違反でも割賦販売法違反でも処罰されないことになる。

（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[3]。

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

[3] 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 2019」（令和元年 5 月）

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」としてとりまとめており、Web 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 7 つの項目を挙げ、合計 40 の要件を設けている。

① 利用者が正規メールとフィッシングメールを判別可能とする対策
② 利用者が正規サイトを判別可能とする対策
③ フィッシング詐欺被害を拡大させないための対策
④ ドメイン名に関する配慮事項
⑤ 組織的な対応体制の整備
⑥ 利用者への啓発活動
⑦ フィッシング詐欺被害の発生を迅速に検知するための対策

このうち⑤の組織的な対応体制の整備としては、フィッシング詐欺発生時の行動計画の策定、フィッシングサイト閉鎖体制の整備が重要である。

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においては、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。

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 7 条各号、第 12 条第 4 号
・割賦販売法第 49 条の 2
・警察庁サイバー犯罪対策プロジェクト「不正アクセス禁止法改正 Q&A」（平成 24 年）11 頁以下
https://www.npa.go.jp/cyber/legislation/pdf/6_QA.pdf
・サイバーセキュリティ 2019・367 頁
・フィッシング対策協議会「フィッシング対策ガイドライン 2019 年度版」
https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

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)

Q72 欧州一般データ保護規則

欧州一般データ保護規則（GDPR）について、日本企業が留意すべき個人データの安全管理に関するポイントは何か。

タグ：個情法、欧州一般データ保護規則、GDPR、域外適用、安全管理、データ侵害通知、データ保護オフィサー（DPO）、データ保護影響評価（DPIA）

１．概要

日本企業であっても、個人データの取扱い実態によっては、欧州一般データ保護規則の適用を受け得る。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。

２．解説

（１）はじめに

欧州一般データ保護規則（General Data Protection Regulation。以下「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）。個情法、行個法、独個法、地方公共団体が定める個人情報の保護に係る条例等、わが国の個人情報保護法制に相当するものということができる。

以下の通り、日本企業であっても 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 を課題とする企業は少なくないと考えらえる。そこで、本項においては、GDPR 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。

（２）適用範囲

GDPR は、その取扱いが EU[1]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[2]ついて適用される（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

[1] 欧州連合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、欧州連合（European Union）

[2] 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）。

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 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 22 項。「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）、データ主体に対する個人データ侵害の連絡（同第 34 条）がある。その他、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。

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[3]）が公表する「THE CNIL'S GUIDES-2018 EDITION SECURITY OF PERSONAL DATA」や、欧州ネットワーク・

[3] Commission nationale de l'informatique et des libertes の略。

情報セキュリティ機関（ENISA[4]）が公表する「Handbook on Security of Personal Data Processing」が参考となる。

イ　個人データ侵害への対応

「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、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。」とされている（GDPR 第 33 条）。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。

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[5]）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[6]。

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」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。

---

[4] Europian Union Agency for Network and Information Security の略。
[5] Data Protection Officer の略。
[6] 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）。

（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 1 項）。この評価をデータ保護影響評価（DPIA[7]）という。

高いリスクを発生させる恐れがあり（「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」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 1 項）。

（４）事例

2019 年に入って、安全管理措置を問題とした事例であって、巨額の制裁金を課すことを検討するケースが見られるようになった。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[8]）に関して、以下の 2 件が事例として挙げられる。

①　ICO がブリティッシュ・エアウェイズに対して 1 億 8,300 万ポンドの制裁金を課すことを検討している事例

顧客 50 万人の個人データが漏洩した事例（クレジットカード情報含む）であり、セキュリティ対策の不備が指摘された。

[7] Data Protection Impact Assesment の略
[8] Information Commissioner's Office の略。

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

② ICO がマリオット・インターナショナルに対して 9,920 万ポンドの制裁金を課すことを検討している事例

顧客に関する 3 億 3900 万件の個人データが漏えいした事例（EEA 域内の人間のものはその一部）であり、セキュリティ対策の不備が指摘された。

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

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/en/new-guide-regarding-security-personal-data

４．裁判例

特になし

Q73 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、中国サイバーセキュリティ法、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

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。中国サイバーセキュリティ法、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。例えば中国サイバーセキュリティ法においては、重要情報インフラ運営者に該当する場合には、中国国内において収集・生成する個人情報および重要データについては、中国国内において保管しなければならないとされ、業務上の必要から、確かに中国国外へと越境移転する必要がある場合には、一定の要件に従った安全評価を行わなければならないとされる。このため、国内へのデータセンター設置や、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、いま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。

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路安全法（中華人民共和国サイバーセキュリティ法、以下「中国サイバーセキュリティ法」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

[1] 法律の下位規則にあたる行政法規等を意味する。

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「GDPR」という）などにおいては、個人データの国外移転にあ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、中国サイバーセキュリティ法の内容を中心に、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）中国サイバーセキュリティ法とデータローカライゼーション規制

ア　適用範囲

中国サイバーセキュリティ法においては、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は、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、中国国内で保存しなければならず、また業務の必要により国外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安全評価を行わなければならないとされる（第 37 条）。

ここで、「重要情報インフラ」とは、「公共通信・情報サービス、エネルギー、交通、金融等の重要な産業及び分野、並びに、その機能が破壊、喪失またはそのデータが漏えいすれば、国の安全、国の経済、人民の生活、公共の利益に重大な危害を与え得るその他の重要情報インフラ」とされ（第 31 条）[2]、中国サイバーセキュリティ法の条文上は、この「重要情報インフラ」の運営者にのみ、データローカライゼーション規制の適用があるとされている。

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 5 項）とされ、また、「重要データ」とは、国の安全、経済成長及び公共の利益と密接にかかわるデータをいうとされる（「情報安全技術データ越境セキュリティ評価ガイドライン」（2017 年 8 月 25 日付意見募集稿）3.5 条及び同ガイドライン付属文書 A「重要データ識別ガイドライン」参照）。

なお、上記のとおり、中国サイバーセキュリティ法の条文上は、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、「個人情報と重要データ越境セキュリティ評価弁法」（2017 年 4 月 11 日付意見募集稿）及び「個人情報越境セキュリティ評価弁法」（2019 年 6 月 13 日付意見募集稿）において、かかる義務主体が、重要情

[2] 重要情報インフラの具体的な範囲は国務院が制定するとされている（第 31 条）。

報インフラの運営者だけではなく、一般の「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、管理者およびネットワークサービス提供者をいうとされる。第 76 条第 3 項。）に拡大される可能性もある[3]。令和 2 年 2 月 1 日現在、いまだ、当該各弁法は意見募集稿段階であり、確定していないため、今後の弁法やガイドラインの制定動向に留意が必要である。

イ　規制内容

中国サイバーセキュリティ法の条文上の規制内容は、前述のとおり、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、業務の必要により国外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安全評価を行うことであるが、特に、後半の安全評価につき、条文からはその具体的内容は明らかではない。この点、前述「情報安全技術データ越境セキュリティ評価ガイドライン」（2017 年 8 月 25 日付意見募集稿）の現状の内容によれば、越境移転制限の適用対象となる企業であって、例えば、日本と中国において個人情報及び重要データを共有している場合等においては、概要、以下のプロセスを実施する必要があるとされる。

① データの越境移転に関するセキュリティ自己評価グループを設立する。
② データの越境移転計画を制定する。
③ データの越境移転に関するセキュリティ自己評価を実施し、セキュリティ自己評価報告書を作成する。
④ セキュリティ自己評価報告書及びその関連証明資料を提出し、国家インターネット情報部門及び産業主管部門に対して申告する（必要な場合にはその同意を得る。なお、評価の結果、越境移転が禁止された場合には、データの越境移転計画を修正し、セキュリティ自己評価を再実施しなければならない。）。
⑤ 毎年セキュリティ自己評価を実施する。

令和 2 年 2 月 1 日現在、いまだ、当該ガイドラインは意見募集稿段階であり、確定していないため、今後のガイドラインの制定動向に留意が必要である。

また、重要情報インフラの運営者が第 37 条の規定に違反して、国外でネットワークデータを保存する、又は国外にネットワークデータを提供した場合は、関連の主管部門が是正を

[3] 「個人情報と重要データ越境セキュリティ評価弁法」（2017 年 4 月 11 日付意見募集稿）第 2 条は、「ネットワーク運営者は、中華人民共和国国内の運営において収集、発生した個人情報と重要データについて、国内に保存しなければならない。業務上の必要により、著しく国外に提供する必要がある場合、この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。」と規定し、「個人情報越境セキュリティ評価弁法」（2019 年 6 月 13 日付意見募集稿）第 2 条は、「ネットワーク運営者は、中華人民共和国内での運営において収集した個人情報を国外に提供する（以下「個人情報の越境」という）場合には、本弁法に従い、セキュリティ評価を行わなければならない。セキュリティ評価により、個人情報の越境が国のセキュリティに影響を及ぼし、公共の利益を損ねる可能性があり、又は個人情報のセキュリティを有効に保障することが困難であると認定された場合には、越境させてはならない。国の個人情報の越境に関する別段の規定がある場合には、当該規定に従う。」と規定する。

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（令和 2 年 2 月 1 日現在において、約 75 万円以上 750 万円以下）の罰金が課されるにとどまらず、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とされる（第 66 条）。この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ない重い法的負担となり得る。

（４）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。

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、正統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。

３．参考資料（法令・ガイドラインなど）

・中国サイバーセキュリティ法
・個人情報と重要データ越境セキュリティ評価弁法（2017 年 4 月 11 日付意見募集稿）
・個人情報越境セキュリティ評価弁法（2019 年 6 月 13 日付意見募集稿）
・情報安全技術データ越境セキュリティ評価ガイドライン（2017 年 8 月 25 日付意見募集稿）

４．裁判例

特になし

付録１　サイバーセキュリティ関係法令・ガイドライン調査結果

本調査結果は、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のオブザーバー（警察庁・個人情報保護委員会事務局・総務省・厚労省・法務省・経済産業省）及び NISC に対し、サイバーセキュリティに関する法令・ガイドラインに関する調査を行い、その結果をとりまとめつつ追加を行ったものである。

本書において引用する全てのガイドライン等を網羅的に記載したものではなく、本書に付録として付加する参考資料であるため、その点留意されたい。

No	名称	種別	URL
1	サイバーセキュリティ基本法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104
2	サイバーセキュリティ戦略（平成 30 年）	閣議決定文書	https://www.nisc.go.jp/materials/index.html
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）	ガイドライン	https://www.nisc.go.jp/active/general/kijun30.html
4	重要インフラの情報セキュリティ対策に係る第４次行動計画（令和２年１月改定）	ガイドライン	https://www.nisc.go.jp/active/infra/outline.html
5	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）令和元年改訂版	ガイドライン	https://www.nisc.go.jp/active/infra/shisaku1.html
6	不正アクセス行為の禁止等に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=411AC0000000128
7	不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則	規則	https://www.npa.go.jp/cyber/legislation/pdf/3_kisoku.pdf
8	不正アクセス禁止法改正Ｑ＆Ａ	Ｑ＆Ａ	https://www.npa.go.jp/cyber/legislation/pdf/6_QA.pdf
9	不正アクセス行為の禁止等に関する法律の解説	解説	https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf
10	個人情報の保護に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000057
11	個人情報の保護に関する基本方針	閣議決定文書	https://www.ppc.go.jp/files/pdf/300612_personal_basicpolicy.pdf
12	個人情報の保護に関する法律施行規則	施行規則	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428M60000000003
13	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）	告示	https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf
14	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）	告示	https://www.ppc.go.jp/files/pdf/190123_guidelines02.pdf
15	個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）	告示	https://www.ppc.go.jp/files/pdf/guidelines04.pdf

16	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	告示	https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf
17	認定個人情報保護団体の認定等に関する指針	告示	https://www.ppc.go.jp/files/pdf/nintei_sisin.pdf
18	個人情報の保護に関する法律に係るＥＵ域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール	告示	https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf
19	「個人情報の保護に関する法律についてのガイドライン」及び「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」に関するＱ＆Ａ	Ｑ＆Ａ	https://www.ppc.go.jp/files/pdf/1906_APPI_QA.pdf
20	行政機関の保有する個人情報の保護に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000058
21	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	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000059
22	行政機関の保有す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（行政機関非識別加工情報編）	告示	https://www.ppc.go.jp/files/pdf/guidelines05.pdf
23	行政機関の保有する個人情報の保護に関する法律第四章の二の規定による行政機関非識別加工情報の提供に関する規則	施行規則	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429M60020000001
24	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についてのガイドライン（独立行政法人等非識別加工情報編）	告示	https://www.ppc.go.jp/files/pdf/guidelines06.pdf
25	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第四章の二の規定による独立行政法人等非識別加工情報の提供に関する規則	施行規則	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429M60020000002
26	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	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=425AC0000000027
27	特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則	規則	https://www.ppc.go.jp/files/pdf/rouei_kisoku.pdf
28	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）	告示	https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha_laws.pdf
29	「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	Q&A	https://www.ppc.go.jp/legal/policy/faq/
30	事業者における特定個人情報の漏えい事案等が発生した場合の対応について	告示	https://www.ppc.go.jp/files/pdf/roueitaiou_jigyosha.pdf
31	電子署名及び認証業務に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000102
32	国立研究開発法人情報通信研究機構法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=411AC0000000162
33	国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=430M60000008061

34	IoT セキュリティガイドライン ver 1.0	ガイドライン	https://www.soumu.go.jp/main_content/000428393.pdf https://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf
35	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 2 版）	ガイドライン	https://www.soumu.go.jp/main_content/000566969.pdf
36	IoT クラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）	ガイドライン	https://www.soumu.go.jp/main_content/000581002.pdf
37	IoT クラウドサービスの安全・信頼性に係る情報開示指針（IaaS・PaaS 編）	ガイドライン	https://www.soumu.go.jp/main_content/000581003.pdf
38	クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン	ガイドライン	https://www.soumu.go.jp/main_content/000567229.pdf
39	テレワークセキュリティガイドライン 第４版	ガイドライン	https://www.soumu.go.jp/main_content/000545372.pdf
40	放送受信者等の個人情報保護に関するガイドライン	告示	https://www.soumu.go.jp/main_content/000483164.pdf
41	放送法施行規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=325M50080000010
42	郵便事業分野における個人情報保護に関するガイドライン	告示	https://www.soumu.go.jp/main_content/000485290.pdf
43	信書便事業分野における個人情報保護に関するガイドライン	告示	https://www.soumu.go.jp/main_content/000485167.pdf
44	電気通信事業法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=359AC0000000086
45	端末設備等規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=360M50001000031
46	事業用電気通信設備規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=360M50001000030
47	情報通信ネットワーク安全・信頼性基準	告示	https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/anshin/index.html
48	電気通信事業における個人情報保護に関するガイドライン	ガイドライン	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html
49	電気通信事業における個人情報保護に関するガイドラインの解説	ガイドライン	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html
50	管理規程記載マニュアル	ガイドライン	https://www.soumu.go.jp/main_content/000345435.pdf
51	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	ガイドライン	https://www.soumu.go.jp/main_content/000615696.pdf
52	特定電子メールの送信の適正化等に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=414AC1000000026
53	電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第５版）	ガイドライン	https://www.jaipa.or.jp/topics/2018/11/post-16.php

54	郵便事業分野における個人情報保護に関するガイドライン（平成 29 年総務省告示 167 号）の解説	ガイドラインの解説を示す資料	https://www.soumu.go.jp/main_content/000485291.pdf
55	信書便事業分野における個人情報保護に関するガイドライン（平成 29 年総務省告示第 168 号）の解説	ガイドラインの解説を示す資料	https://www.soumu.go.jp/main_content/000595986.pdf
56	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	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=413AC0000000137
57	インターネット上の違法・有害情報に対する対応（プロバイダ責任制限法）	法律の概説	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html
58	サイバーセキュリティ対策情報開示の手引き	ガイドライン	https://www.soumu.go.jp/main_content/000630516.pdf
59	電気通信事業参入マニュアル	ガイドライン	https://www.soumu.go.jp/main_content/000426542.pdf
60	電気通信事業参入マニュアル（追補版）	ガイドライン	https://www.soumu.go.jp/main_content/000477428.pdf
61	労働基準法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=322AC0000000049
62	労働契約法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000128
63	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	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=360AC0000000088
64	労働安全衛生法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=347AC0000000057
65	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）	指針	https://www.mhlw.go.jp/stf/newpage_01170.html
66	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 月公表）	手引き	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/anzen/anzeneisei02.html
67	テレワークモデル就業規則	ガイドライン	https://www.tw-sodan.jp/dl_pdf/16.pdf
68	会社法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=417AC0000000086
69	会社法施行規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=359AC0000000086
70	刑法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=140AC0000000045

71	いわゆるコンピュータ・ウイルスに関する罪について	ガイドライン	http://www.moj.go.jp/content/000076666.pdf
72	不正競争防止法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=405AC0000000047
73	逐条解説 不正競争防止法（令和元年７月１日施行版）	逐条	https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20190701Chikujyou.pdf
74	営業秘密管理指針	ガイドライン	https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf
75	秘密情報の保護ハンドブック ～企業価値向上に向けて～	ガイドライン	https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html
76	限定提供データに関する指針	ガイドライン	https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf
77	産業競争力強化法	法律	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
78	産業競争力強化法に基づく認定技術等情報漏えい防止措置認証機関に関する命令	省令	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
79	技術等情報漏えい防止措置認証業務の実施の方法	告示	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
80	技術等情報漏えい防止措置の実施の促進に関する指針	告示	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
81	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	告示	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
82	電気事業法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=339AC0000000170
83	電気設備に関する技術基準を定める省令	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=409M50000400052
84	電気設備の技術基準の解釈	内規	https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/files/dengikaishaku.pdf
85	電気事業法施行規則第 50 条第 2 項の解釈適用に当たっての考え方	内規	https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2016/09/280923-1-3.pdf
86	電力制御システムセキュリティガイドライン	民間規格	（抜粋版） https://www.denki.or.jp/wp-content/uploads/2016/07/d20160707.pdf
87	スマートメーターシステムセキュリティガイドライン	民間規格	（抜粋版） https://www.denki.or.jp/wp-content/uploads/2016/07/s20160609.pdf
88	ガス事業法	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=329AC0000000051
89	ガス事業法施行規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=345M50000400097

90	IoT セキュリティ対応マニュアル 産業保安版	ガイドライン	https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2019/4/20190425.html
91	サイバーセキュリティ経営ガイドライン Ver2.0	ガイドライン	https://www.meti.go.jp/policy/netsecurity/mng_guide.html
92	AI・データの利用に関する契約ガイドライン 1.1 版	ガイドライン	https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html
93	電子商取引及び情報財取引等に関する準則（令和元年 12 月）	ガイドライン	https://www.meti.go.jp/press/2019/12/20191219003/20191219003-2.pdf
94	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）	ガイドライン	https://www.meti.go.jp/policy/economy/keiei_innovation/keizaihousei/corporategovernance.html
95	情報処理の促進に関する法律	法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=345AC0000000090
96	情報処理の促進に関する法律施行規則	省令	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428M60000400102
97	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	告示	https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf
98	平成三十一年経済産業省告示第十九号（調整機関等を定める告示）	告示	https://www.meti.go.jp/policy/netsecurity/vul_institutions.pdf

付録２　「重要インフラの情報セキュリティ対策に係る第４次行動計画」別紙２部分抜粋

重要インフラ分野	重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
情報通信	・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること（電気通信事業法第２条）	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障	・電気通信事業法（業務停止等の報告）第28条 ・電気通信事業法施行規則（報告を要する重大な事故）第58条 【サービス維持レベル】 ・電気通信設備の故障により、役務提供の停止・品質の低下が、３万以上の利用者に対し２時間以上継続する事故が生じないこと
	・放送	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第113条、第122条 ・放送法施行規則（報告を要する重大な事故）第125条 【サービス維持レベル】 ・基幹放送設備の故障により、放送の停止が15分以上継続する事故が生じないこと ・特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が15分以上（中継局の無線設備にあっては、２時間以上）継続する事故が生じないこと
	・ケーブルテレビ	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第137条 ・放送法施行規則（報告を要する重大な事故）第157条 【サービス維持レベル】 ・有線一般放送の業務に用いられる電気通信設備の故障により、放送の停止を受けた利用者の数が３万以上、かつ、停止時間が２時間以上の事故が生じないこと

重要インフラ分野		重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
		呼称	サービス（手続を含む）の説明（関連する法令）		
金融	銀行等	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ（銀行法第10条第１項第１号） ・資金の貸付け又は手形の割引（銀行法第10条第１項第２号） ・為替取引（銀行法第10条第１項第３号）	・預金の払戻しの遅延・停止 ・融資業務の遅延・停止 ・振込等資金移動の遅延・停止	・主要行等向けの総合的な監督指針 ・中小・地域金融機関向けの総合的な監督指針 ・系統金融機関向けの総合的な監督指針
		・資金清算	・資金清算（資金決済に関する法律第２条第10項）	・資金清算の遅延・停止	・清算・振替機関等向けの総合的な監督指針
		・電子記録等	・電子記録（電子記録債権法第56条） ・資金決済に関する情報提供（電子記録債権法第62条及び第63条）	・電子記録、資金決済に関する情報提供の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（12 電子債権記録機関関係）
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付 ・保険金等の支払審査 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針
	損害保険	・保険金等の支払い	・事故受付 ・損害調査等 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針
	証券	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引（金融商品取引法第２条第８項第１号） ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理（金融商品取引法第２条第８項第２号） ・有価証券等清算取次ぎ（金融商品取引法第２条第８項第５号）	・有価証券売買の遅延・停止	・金融商品取引業者等向けの総合的な監督指針
		・金融商品市場の開設	・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務（金融商品取引法第２条第14項及び第16項、第80条並びに第84条）	・有価証券の売買、市場デリバティブ取引等の遅延・停止	・金融商品取引所等に関する内閣府令第112条

重要インフラ分野	重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
	・振替業	・社債等の振替に関する業務（社債、株式等の振替に関する法律第８条）	・社債・株式等の振替等の遅延・停止	・社債、株式等の振替に関する法律（事故の報告）第19条 ・一般振替機関の監督に関する命令（事故）第17条 ・清算・振替機関等向けの総合的な監督指針
	・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
航空	・旅客、貨物の航空輸送サービス	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条）	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空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
	・予約、発券、搭乗・搭載手続	・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・搭乗、航空貨物の搭載		
	・運航整備	・航空機の点検・整備		
	・飛行計画作成	・飛行計画の作成、航空局への提出		
空港	・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港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

重要インフラ分野	重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
鉄道	・旅客輸送サービス ・発券、入出場手続	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業（鉄道事業法第２条） ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告） 第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第５条 ・鉄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
電力	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条第１項第８号） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条第１項第14号）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第３条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス	・一般ガス導管事業 ・ガス製造事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項） ・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第２条第９項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・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
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）(注1)		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
	呼称	サービス（手続を含む）の説明（関連する法令）		
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン
物流	・貨物自動車運送事業 ・船舶運航事業 ・港湾運送事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・他人の需要に応じ、港湾においてする船舶への貨物の積込又は船舶からの貨物の取卸の行為等を行う事業（港湾運送事業法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流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
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期に渡る製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	・クレジットカード決済	・クレジットカード決済サービス（割賦販売法第２条第３項第１号及び第２号並びに第35条の16第１項第２号及び第２項）	・クレジットカード決済サービスの遅延・停止、カード情報の大規模漏えい	・割賦販売法（後払分野）に基づく監督の基本方針 ・クレジットCEPTOARにおける情報セキュリティガイドライン
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油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

注１　ＩＴを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。
注３　別紙２に記載された内容は令和元年12月現在のものである。法令等の最新の状況については、必要に応じて、所管省庁等へ確認すること。

関係者一覧

（全て敬称略）

◇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[1]　　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

[1] 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