我が国の最新のサイバーセキュリティ政策動向

2026年３月12日

内閣官房 国家サイバー統括室

関口 祐司

最新のサイバー情勢

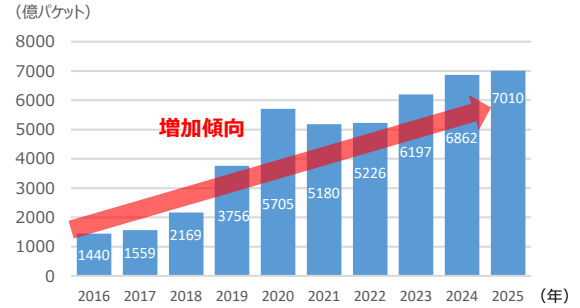
■ **サイバー攻撃関連通信数の増加**や**サイバー攻撃の巧妙化・深刻化**により、**サイバー攻撃は質・量ともに増大**

※令和６年中に観測されたサイバー攻撃関連の通信の99%以上が海外から発信（警察庁資料）

■ **政府機関、重要インフラ事業者、その他の事業者へのサイバー攻撃**が確認され、**社会全体に対してサイバー攻撃の脅威が増大**

サイバー攻撃関連通信や被害の量

① NICTが観測したサイバー攻撃関連通信数（※）の推移



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2025（令和８年２月５日）」を基に作成

※NICTの観測用IPアドレス約28万に届いたパケットの数。

サイバー攻撃の巧妙化・深刻化

② 「公開サーバへの攻撃」から「重要インフラ等への侵入」へ高度化

公開サーバへの攻撃
ウェブサイト等の停止
→ ＩＴ系システムの障害
システム障害・身代金要求
→ 有事を見据えた重要インフラ等への侵入
インフラ機能停止

③ AIツールを活用したサイバー攻撃の自動化

- Anthropic（米）は、2025年９月、**中国政府が支援する攻撃グループが**、同社の**AIエージェントツール（Claude Code）を悪用**して、**約30の組織を標的にサイバー攻撃を実行**していたことを確認。
- **AIエージェントが**人間にサイバー攻撃に関するアドバイスをするのではなく、**サイバー攻撃の大部分（約80～90%）を自ら実行。**

主な国内におけるサイバー攻撃事案

（注）「NISC」と記載されているものは、国家サイバー統括室が改組する2025年6月30日以前の「内閣サイバーセキュリティセンター」のこと。

政府機関等

NISC（当時）	不正アクセス	・ 令和５年６月、**電子メール関連システム**を対象に、**個人情報を含むメールデータの一部が外部に漏えい**した可能性
国交省	不正アクセス	・ 令和７年９月、**近畿地方整備局のネットワーク**への不正アクセスにより、当該ネットワークと繋がっている**内閣府沖縄総合事務局において職員情報が外部に漏えい**した可能性
JAXA	不正アクセス	・ 令和６年７月、**業務用イントラネットの管理用サーバ**を対象に、**外部機関との共同業務に係る情報が外部に漏えい**した可能性

重要インフラ事業者

航空/金融/通信	DDoS	・ 令和６年12月～令和７年１月の年末年始、**JAL、三菱UFJ銀行、NTTドコモ**を対象に、**各社のシステムやサービスに障害**が発生
港湾	ランサムウェア	・ 令和５年７月、**名古屋港のコンテナターミナルシステム**を対象に、約３日間、**コンテナの搬入・搬出作業が停止**
医療	ランサムウェア	・ 令和４年10月、**大阪急性期・総合医療センター**を対象に、**電子カルテシステムに障害**が発生し、数ヶ月間、**通常診療等が一時停止**

その他の事業者

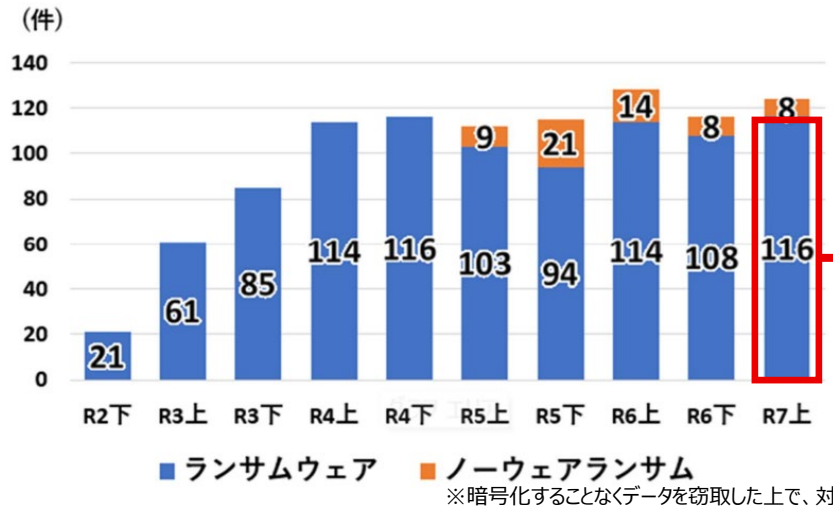
出版/Webサービス	ランサムウェア	・ 令和６年６月、**KADOKAWAグループ**を対象に、**複数のサーバに障害が発生**し、**ニコニコサービス等のサービス停止の他、情報漏えい**が発生。
飲料メーカー	ランサムウェア	・ 令和７年９月、**アサヒグループHD**のシステムに障害が発生し、**酒類・清涼飲料水の受注・出荷業務が一時停止**
通販	ランサムウェア	・ 令和７年10月、**アスクル**のシステムに障害が発生し、**オフィス用品、医療・介護用品の受注・出荷業務が一時停止**

企業が受けるサイバーリスク：ランサムウェア

ランサムウェア

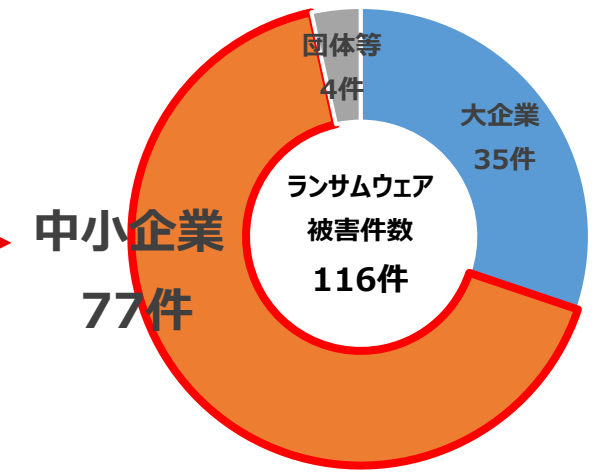
- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。**感染したパソコンのデータを暗号化するなど使用不可にし、その解除と引換えに金銭を要求**する。
- 企業のサービスが停止する、個人情報が漏えいするなどの甚大な被害に繋がることもある。
- 2025年(令和7年)上半期に全国の都道府県警察から警察庁に報告があった件数は**116件**であり、前年と同じく高い水準で推移。
- 被害件数(116件)の内訳は、**大企業が35件（30%）**に対して、**中小企業は77件（66%）と３分の２を占める。**

企業・団体等におけるランサムウェア被害の報告件数の推移



※暗号化することなくデータを窃取した上で、対価を要求する手口

ランサムウェア被害の被害企業・団体等の規模別報告件数（令和7年上半期）



中小企業の
被害が３分の２

警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（2025年９月）」より作成

サイバー対策強化に向けた政策の推進

サイバー対処能力強化法・整備法の成立(2025年5月)

- サイバー対処能力を強化する「能動的サイバー防御」が可能に

政府のサイバーセキュリティの体制強化(2025年７月)

- サイバーセキュリティ戦略本部を全大臣で構成。トップを内閣総理大臣に
- 国家サイバー統括室(NCO)の設置

新たなサイバーセキュリティ戦略の策定(2025年12月)

- 官民連携・国際連携の下、様々なサイバー施策を一体的に推進

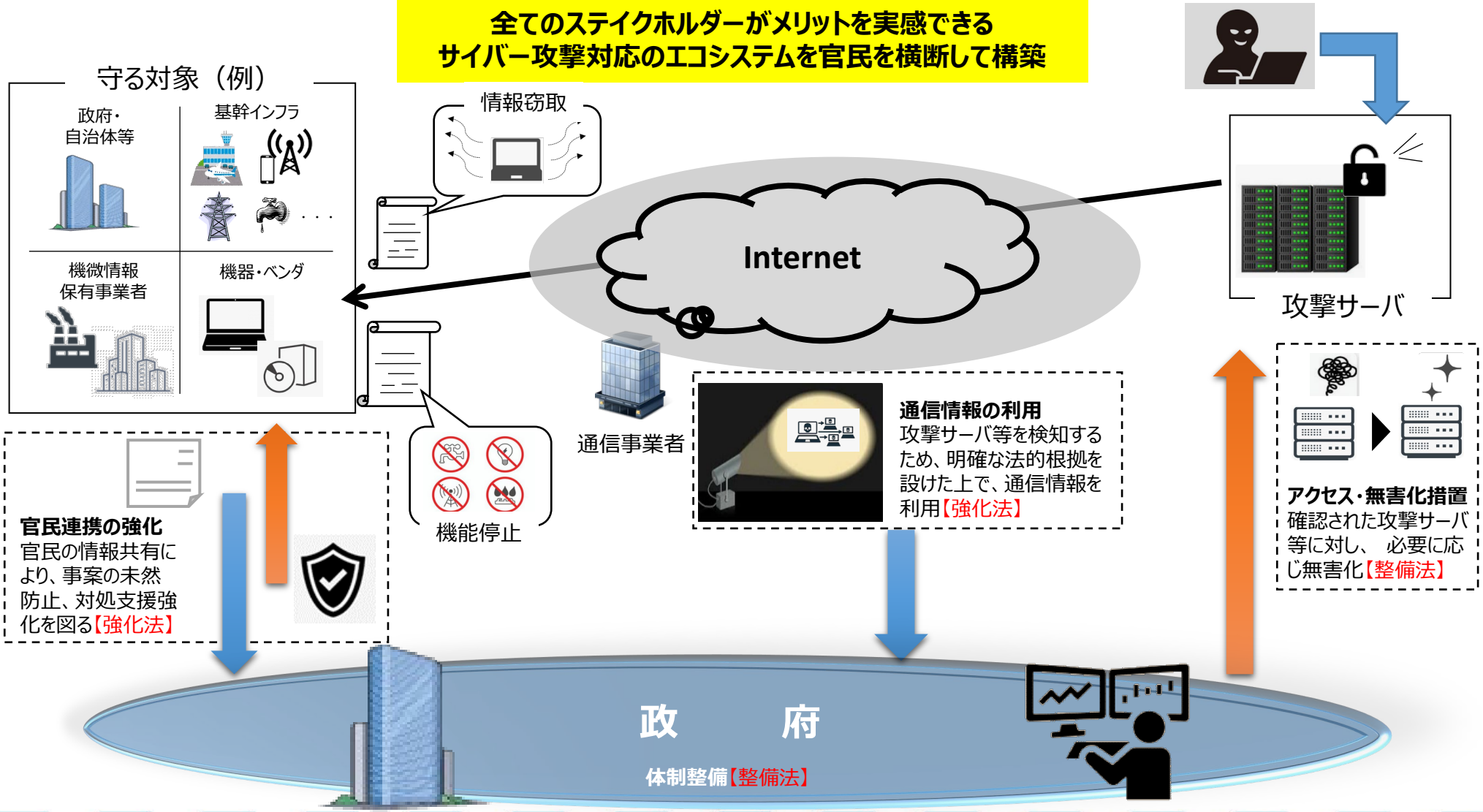
サイバー対処能力強化法・整備法の施行による環境整備(2026年以降)

- サイバー通信情報監理委員会設置（2026年４月１日）
- 新たな官民協議会の立ち上げ、「官民連携」、「アクセス・無害化措置」に係る制度施行（2026年10月１日想定）
- 「通信情報の利用」に係る制度施行（2027年11月までに）

サイバー対処能力強化法・同整備法　全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築



サイバー対処能力強化法(※1)・同整備法(※2)の全体像

※１ 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）※２ 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

- 国家安全保障戦略（令和4年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則
- 目的規定、基本方針等（第１章）

官 民 連 携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）

アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日

公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

サイバーセキュリティ戦略（2025年12月23日閣議決定）の全体像

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、**サイバー空間上の脅威に対応するための取組**を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**実施すべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

- 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大
- 社会全体のデジタル化の進展とサイバー脅威の増大
- AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1　深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2　幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3　我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

サイバーセキュリティ戦略における「中小企業」に関する記述（ポイント）

２．幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上
（３）ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保
③ 中小企業を始めとした個々の民間企業等における対策の強化

●サプライチェーン全体のセキュリティ・レジリエンス確保には、中小企業等における対策が不可欠
●一方、中小企業等には、対策の必要性に対する認識不足、人材・予算等の十分なリソース確保が困難といった課題
→政府・業界団体・支援組織等が連携して行ってきた「自助」、「共助」、「公助」を組み合わせた施策を一層強化する必要

中小企業等の「自助」を促す取組
・サプライチェーンにおけるリスクに応じて各企業が取るべき対策水準を可視化・確認する制度の活用促進
・中小企業が身近に感じられる事例や防止策の発信　等

主体同士の「共助」を促す取組
・地域金融機関、士業といった地域に根付いた主体との連携等の促進
・産業界主導のコンソーシアムを通じた普及展開活動の強化、サイバー関連情報の発信・共有　等

十分な対応が難しい中小企業等に対する「公助」の推進
・サイバーセキュリティお助け隊サービスの利用改善に向けた見直し
・セキュリティの外部専門家による支援を容易に探索・依頼できるような仕組みの整備・活用促進
・基幹インフラ事業者等のサプライチェーンに属する中小企業等からテレメトリ情報(※)を収集・統合・分析し、
サイバー攻撃検知情報等、対策強化に資する有用な情報を還元する「集団的防御」の枠組みの導入　等

※テレメトリ情報とは、システムの稼働状況やイベント（不正アクセス等）のログ等の形で収集されたデータであって、監視・分析等のために遠隔地に送信されたもの。

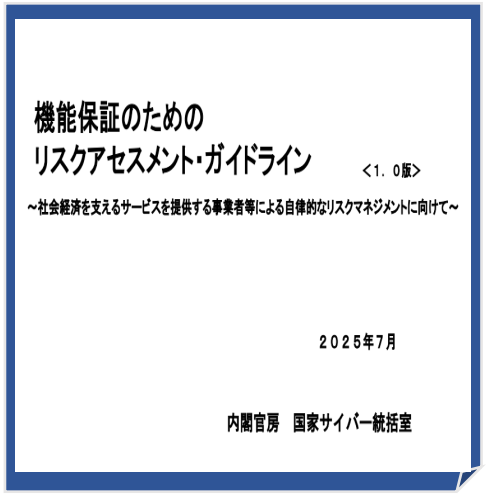
サイバー攻撃から企業を守るために。リスクアセスメントの実施に向けて

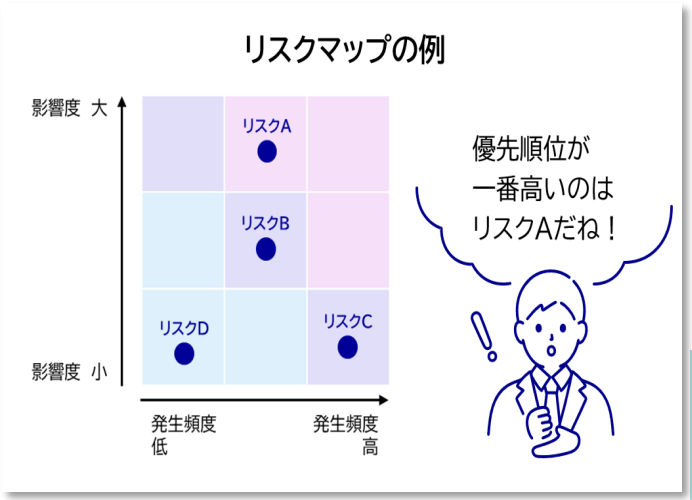
- 自組織のどこにリスクが存在しているか把握するために行う**リスクアセスメント(*1)はサイバーセキュリティに係わる第１歩**の取組です。リスクアセスメントを行うことで、効果・効率的なサイバーセキュリティ対策の実施が可能となります。
- リスクアセスメントの重要性を認識しながらも、具体的にどのように進めたらよいかが分からないなどの理由により、実施できていない事業者等も多く存在しており、リスクアセスメントの考え方や実施方法が定着しているとは言い難い状況です。
- 国家サイバー統括室（NCO)では、こうした状況を踏まえ、情報セキュリティに係るリスクアセスメントの実施方法についての**具体的な手順を含む基礎的なフレームワーク**(*2)を提供しています。また先日、自己学習や社内研修において学習教材としてご活用いただくことを想定して作成した**「リスクアセスメント実践ラーニングキット」(*3)を新たに公開**しました。
- サイバー攻撃から企業を守るために、**経営層主導のリスクアセスメントの実施**に向けて、是非ご活用ください。

(*1)事業経営・事業活動における目的、その目的に照らした製品・サービスの経営上の位置付け、利害関係者からの期待、社会的責任(CSR)、法制面の要求(コンプライアンス)等を分析した上、保有する経営資源の重要性の尺度に基づくリスクの特定・分析・評価を行うこと。

(*2) https://www.cyber.go.jp/policy/group/cyber/policy.html よりダウンロード可能。実施手順を解説したガイドラインのほか、記入様式、参考資料等、リスクアセスメントを実施するための資料一式をフレームワークとして提供。

(*3) https://security-portal.cyber.go.jp/guidance/nco risk.html よりダウンロード可能。





「みんなで使おう サイバーセキュリティ・ポータルサイト」
TOP ＞ お役立ちコンテンツ ＞ 学習用コンテンツ
からアクセスしてください！

リスクアセスメントの実施方法や手順等、疑問・ご不明な点がございましたら、下記までお気軽にお問合せください。

<担当>
内閣官房 国家サイバー統括室　対処調整･官民連携等ユニット
メール：riskassess2020-ot4yi@cyber.go.jp

リスクアセスメント実践ラーニングキット　～自己学習、研修教材～

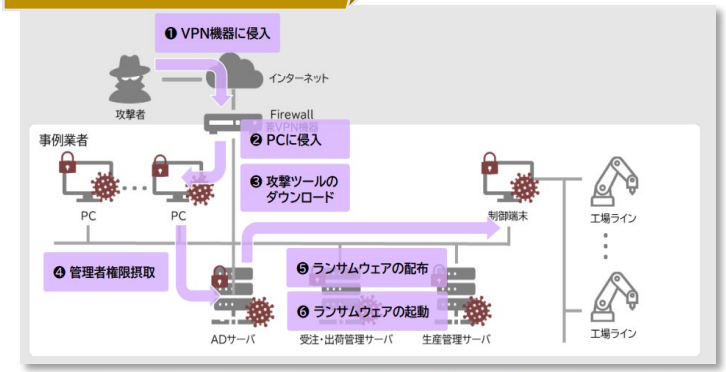
00	はじめに	5分
01	事前準備	10分
02	リスクアセスメントの対象の特定	10分
03	リスク評価方針の策定	10分
04	リスクアセスメント	40分
05	リスクアセスメントの妥当性確認・評価	5分
06	リスクアセスメントの継続的な見直し	5分
99	おわりに	5分

-- Question --

重要サービスの選定にあたって必要となる観点を選びましょう

- A 事業経営上の観点
- B 社会的責任の観点
- C 財務的損失の観点
- D 法令遵守の観点

-- Case Study --



ご利用イメージ

想定利用事業者

企業規模問わず、
幅広い事業者にて
ご利用いただけるよう
作成しています。

想定利用部署

リスクマネジメントに関わる方々での
ご利用を想定しています。

情報セキュリティ部署

リスク管理部署

想定利用場面

自己学習

自己学習や社内研修において
学習教材としてご活用いただくことを
想定して作成しています。

社内研修

2026年「サイバーセキュリティ月間」

■ 毎年**2月1日から3月18日**を「**サイバーセキュリティ月間**」と位置づけ、 産官学民を巻き込み、関係機関・団体と連携し、サイバーセキュリティ（CS）に関する**普及啓発活動を集中的に実施**しています。
※ 前身の「情報セキュリティ月間」（2011～2014年）を含め、2026年で16回目。

テーマ

●今年のテーマは**「サイバーはひとごとじゃない」**。
●一人一人が、サイバー攻撃による被害をひとごとではなく、自分ごとだと考えて、対策していただけるようなコンテンツの発信、普及啓発を実施。

普及啓発協力キャラクター

総理（CS戦略本部長）からのメッセージ

CS月間特設サイト

関連行事（約190件）やコラムを掲載。

サイバーセキュリティ月間2026特設サイトはこちら

基本的なサイバーセキュリティ対策の徹底

国家サイバー統括室（NCO）と独立行政法人情報処理推進機構（IPA）では、みなさん一人一人に実施していただきたい基本的な対策を**「サイバーセキュリティ対策９か条」**として示しています。

1. **OSやソフトウェアは常に最新の状態に**しておこう
2. **パスワードは長く複雑**にして、**他と使い回さない**ようにしよう
3. **多要素認証**を**利用**しよう
4. **偽メール**や**偽サイト**に騙されないように**用心**しよう
5. メールの**添付ファイル**や**本文中のリンク**に**注意**しよう
6. スマホやPCの**画面ロックを利用**しよう
7. 大切な情報は失う前に**バックアップ（複製）**しよう
8. **外出先**では**紛失・盗難・覗き見に注意**しよう
9. **困った時は**ひとりで悩まず、**まず相談**しよう

一人一人が基本的な対策をしていただくことが重要です。

サイバーセキュリティ対策9か条

「サイバーセキュリティ対策９か条」では、「パスワードは長く複雑に」「OSやソフトウェアは常に最新の状態にしておく」など、重要な対策をコンパクトにまとめています。若年層向けやシニア向けにコミカルで分かりやすいリーフレットや動画を制作し、「みんなで使おう サイバーセキュリティ・ポータルサイト」において発信しています。ぜひご覧ください。

若年層向け「サイバーセキュリティ過剰な九条くん」

シニア向け「サイバーセキュリティ川柳」

「みんなで使おう サイバーセキュリティ・ポータルサイト」
TOP ＞ お役立ちコンテンツ ＞ サイバーセキュリティ対策9か条
からアクセスしてください！

サイバーセキュリティ対策９か条　コンテンツページはこちら→
https://security-portal.cyber.go.jp/guidance/cybersecurity9principles.html

国家サイバー統括室（NCO）が発信する様々なコンテンツ

NCOが運営する「みんなで使おう サイバーセキュリティ・ポータルサイト」では、セキュリティを学べる様々なコンテンツを発信しています。すべて無料でダウンロード、活用いただけます。自主学習や社内教育にお役立てください。

インターネットの安全・安心ハンドブック

豊富なイラストと分かりやすい文章で、サイバー攻撃の手口と基本的なセキュリティ対策を解説します。NCOのサイトからダウンロードでき、印刷して従業員への配布も可能です。

「みんなで使おう サイバーセキュリティ・ポータルサイト」
TOP ＞ お役立ちコンテンツ
＞インターネットの安全・安心ハンドブック
からアクセスしてください！

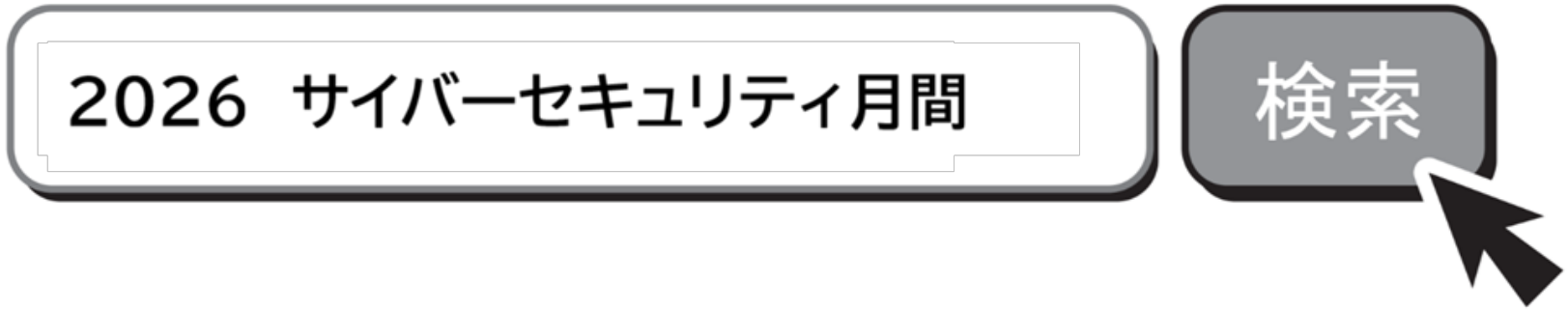
ダウンロードはこちら→
https://security-portal.cyber.go.jp/guidance/handbook.html

企業で講習などに役立てるため、ハンドブックの内容を分かりやすく解説した動画も公開中です。ぜひご覧ください。

YouTubeチャンネル
「NCOサイバーセキュリティ普及啓発動画ポータル」
→「インターネットの安全・安心ハンドブックを活用したコンテンツ」からアクセスしてください！

企業・従業員層向け講習用動画はこちら→
https://www.youtube.com/watch?v=7mkclKwDHEw

ご清聴ありがとうございました。



国家サイバー統括室
National Cybersecurity Office