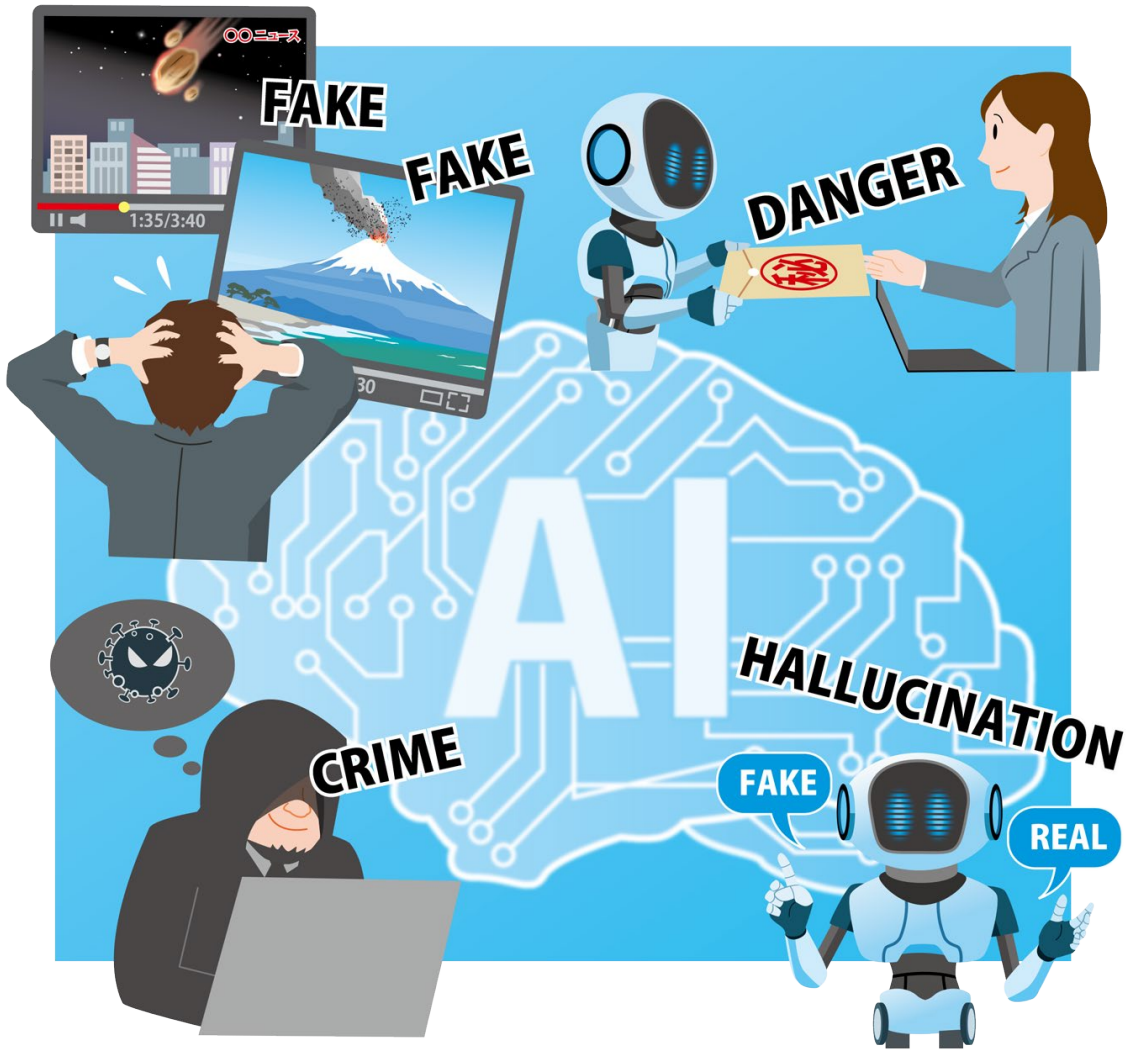
情報セキュリティ
10 大脅威 2026
解説書［組織編］

～当たり前を確実に、基本の徹底と継続的な見直しで被害の最小化を～



独立行政法人**情報処理推進機構**
セキュリティセンター

2026 年 3 月

本書は、以下からダウンロードできます。

「情報セキュリティ 10 大脅威 2026」解説書［組織編］
https://www.ipa.go.jp/security/10threats/10threats2026.html

目次

はじめに

「情報セキュリティ 10 大脅威」は、情報セキュリティの専門家を中心に構成する「10 大脅威選考会」の協力により、主に前年に発生した社会的影響が大きかったセキュリティの事故や攻撃の状況等から脅威候補を選出し、投票により「個人」と「組織」という異なる立場での脅威を決定したものである。

「10 大脅威 2026」解説書[組織編]では、組織向けの各脅威の手口や影響についての説明と、立場ごとに求められる対策、事例を簡潔に記載し、共通の対策については別ページに集約している。

各脅威が自分自身や自組織にどう影響するかを確認しながら本書を読み進めることで、様々な脅威と対策を網羅的に把握できる。

本書が、読者自身のセキュリティ対策への取り組みと、各組織の研修やセキュリティ教育等に活用され、セキュリティ対策の普及の一助となることを期待する。

【本書の概要】

- 情報セキュリティ 10 大脅威 2026

組織の 10 大脅威は、「ランサム攻撃による被害」と「サプライチェーンや委託先を狙った攻撃」が 4 年連続で 1 位と 2 位に選ばれた。また、「AI の利用をめぐるサイバーリスク」が初選出された。業務利用においても、個人利用においても、AI は有用なツールであるが、AI についての理解が不十分なまま利用すると、権利侵害や情報漏えいに繋がることもあり、注意が必要である。

組織の脅威はランキング形式で紹介しているが、順位が危険度を表しているわけではない。昨年の被害事例等の状況から、「10 大脅威選考会」の参加者がそれぞれの観点で、社会的に影響が大きかったと判断した脅威の順である。また、個人の脅威とは異なり、攻撃手口を知っているだけでは対策にならず、セキュリティ対策情報を継続的に収集し、使用している機器やサービスのセキュリティ対策の実施をはじめとした、状況に合わせた迅速な対応が求められている。各脅威の解説を読み、自組織の事業や体制にはどのようなリスクがあるのか洗い出すことが重要である。

本書では、主に 2025 年の脅威の動向を「10 大脅威 2026」として解説する。

1. 情報セキュリティ10 大脅威 2026

情報セキュリティ 10 大脅威 2026

■「情報セキュリティ 10 大脅威 2026」

2025 年において社会的に影響が大きかったセキュリティ上の脅威等について「10 大脅威選考会」の投票結果に基づき、「情報セキュリティ 10 大脅威 2026[1]」を選出した。表 1.1 は、「組織」向け脅威である。

表 1.1 情報セキュリティ 10 大脅威 2026「組織」向けの脅威の順位

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサム攻撃による被害	2016 年	11 年連続 11 回目
2	サプライチェーンや委託先を狙った攻撃	2019 年	8 年連続 8 回目
3	AI の利用をめぐるサイバーリスク	2026 年	初選出
4	システムの脆弱性を悪用した攻撃	2016 年	6 年連続 9 回目
5	機密情報を狙った標的型攻撃	2016 年	11 年連続 11 回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025 年	2 年連続 2 回目
7	内部不正による情報漏えい等	2016 年	11 年連続 11 回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021 年	6 年連続 6 回目
9	DDoS 攻撃（分散型サービス妨害攻撃）	2016 年	2 年連続 7 回目
10	ビジネスメール詐欺	2018 年	9 年連続 9 回目

[1] 情報セキュリティ10大脅威2026
https://www.ipa.go.jp/security/10threats/10threats2026.html

「情報セキュリティ 10 大脅威 2026」をお読みいただくうえでの留意事項

1. 順位の高低ではなく、自組織の立場や環境を考慮して対策を検討する

組織向けの「10 大脅威」は順位付けされているが、対策すべき優先順位ではない。例えば、自組織で利用している製品の脆弱性対策情報が開発会社から公開された場合、「システムの脆弱性を悪用した攻撃」のリスクが高くなるため、優先的な対策が求められる。

順位の高低によらず、組織の環境に照らし合わせて、優先すべき脅威を整理し、優先順位に沿って対策を実施する必要がある。

2. ランクインした脅威が全てではない

「10 大脅威」で解説している脅威は 10 種であるが、これが全てではない。ランク外の脅威にも注意が必要である。例えば、2023 年以降圏外ではあるが「予期せぬ IT 基盤の障害に伴う業務停止」のように、システム障害や自然災害によって社会インフラが停止した場合、企業活動や市民生活への影響は大きい。今回ランクインしなかった脅威についても、過去の「10 大脅威」の解説書 [2]に目を通して内容を把握しておくことが望ましい。

今回ランクインしなかった脅威でも、被害が発生するリスクはある。
現在実施中の対策を見直し、必要な調整をした上で、対策を継続することが重要である。

3. 「情報セキュリティ対策の基本」が重要

情報セキュリティの脅威は多数あり、各脅威で使われる「攻撃の糸口」は似通っている。脆弱性の悪用、マルウェアの利用、ソーシャルエンジニアリング等、古くから知られている手口にこれら糸口が使われている。

表 1.2 に示すように「攻撃の糸口」を 6 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待でき、これを意識して継続的に対策を行うことで、被害の低減が可能である。

---

[2] 情報セキュリティ10大脅威（IPA）
https://www.ipa.go.jp/security/10threats/index.html

表 1.2 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアの利用	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「認証を適切に運用する」で詳細を解説	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定が悪用され、攻撃を受けないようにする
データの暗号化	バックアップの取得	PC やサーバーのデータ削除や暗号化に備える
ソーシャルエンジニアリング（罠にはめる）	脅威・手口を知る	手口から重視すべき対策を理解する

また、昨今はクラウドファーストがすっかり浸透している。クラウドサービスを利用する場合は、表 1.3 の対策を「情報セキュリティ対策の基本」+α として行うことで、被害の低減が可能である。

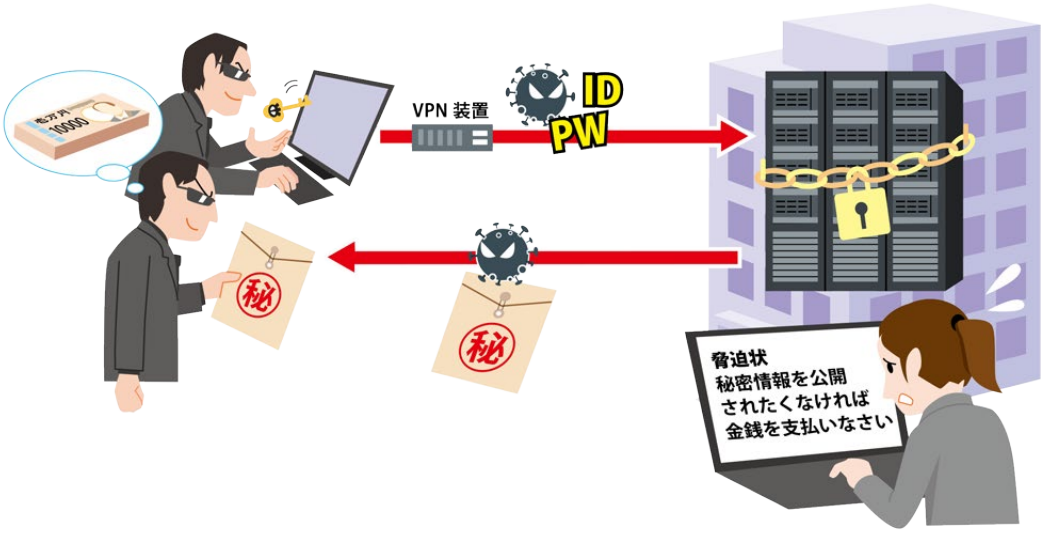
表 1.3 情報セキュリティ対策の基本+α

備える対象	情報セキュリティ対策の基本＋α	目的
クラウドの選定	選定前の事前調査	クラウドサービスのガイドラインに沿った運営をしている業者やそのサービスを選定する [3]
インシデント全般	責任範囲の明確化（理解）	クラウドサービスを契約する際は、インシデント発生時に誰（どの組織）がどこまでインシデント対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報は常に確認し、仕様変更により意図せず変更された設定は適切な設定に修正する（設定不備により発生する情報漏えいや攻撃を防止する）

[3] 中小企業のためのクラウドサービス安全利用の手引き（IPA）
https://www.ipa.go.jp/security/sme/f55m8k0000001wpl-att/outline_guidance_cloud.pdf

2. 情報セキュリティ 10 大脅威（組織）

1位 ランサム攻撃による被害



PC やサーバー内のデータ窃取や暗号化、窃取した情報の暴露予告を行い、これらを取引材料とした様々な脅迫により金銭を要求する攻撃をランサム攻撃という。主にランサムウェアと呼ばれるデータを暗号化するマルウェアを用いるが、ランサムウェアを用いない「ノーウェアランサム [4]」という攻撃もある。また、昨今は業務効率等のために企業が構築したデータ連携基盤が標的にされており、被害は取引先も含め広範になり、調査や復旧に多くの時間と費用を要す。業務やサービス提供の停止による損失が発生し、市場への影響も大きい。

＜脅威と影響＞

① 攻撃者は PC やサーバーをランサムウェアに感染させ、金銭要求を伴う以下のような脅迫を行う。また、下記を組み合わせた「二重脅迫」や「三重、四重脅迫」も確認されている。サーバー等のデータを暗号化し、業務の継続を困難にさせ、データの復元と引き換えに金銭を要求する。

② 重要情報を窃取し、リークサイト等で公開すると脅す。重要情報の窃取時にランサムウェアを利用せず（データを暗号化せず）に同様の脅迫を行う、「ノーウェアランサム」と呼ばれる攻撃を行うこともある。

③ DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）やシステム破壊等を仕掛けると脅す。

④ ランサムウェアに感染したことを被害者の利害関係者等に暴露すると脅す。

＜攻撃手口＞

◆機器の脆弱性を悪用してネットワークから感染させる

インターネットに接続されている機器の脆弱性を悪用し、PC やサーバーをランサムウェアに感染させる。

◆不正アクセスによりネットワークから感染させる

窃取した認証情報（ID、パスワード等）を用いた不正アクセスや、意図せず外部に公開されているポート（リモートデスクトップ等）を悪用した不正アクセスによりネットワークに侵入し、PC やサーバーをランサムウェアに感染させる。

---

[4] 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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

◆Web サイトやメールから感染させる

攻撃者は Web サイトを改ざんし、ランサムウェアを仕込んでおく。その Web サイトで偽の認証画像やエラー画面などを表示し、利用者がその画面に記載されている指示通りの操作をすることで、ランサムウェアがダウンロードされ、PC が感染する。また、そのほかの手口として添付ファイルにマルウェアを仕込み、受信者に開封させたり、メール文中にランサムウェアを仕込んだ Web サイトへのリンクを記載し、クリックさせたりすることで PC にランサムウェアを感染させる。

◆ダークウェブを利用する

匿名性が非常に高いネットワークであるダークウェブ等のマーケットでは、ランサムウェア提供サービス（RaaS：Ransomeware as a Service[5]）によるランサムウェアの売買や攻撃代行、各種認証情報やアクセス情報等の提供が行われており、それらを利用して標的となる組織を攻撃する。

＜事例または傾向＞

◆グループ会社を経由したサイバー攻撃

アサヒグループホールディングスは、2025 年 9 月に国内で管理するシステムがランサムウェアの被害に遭い、個人情報等約 191 万件が流出した可能性があると同年 11 月に公表した。攻撃者は、拠点のネットワーク機器経由でデータセンターに侵入し、一斉にランサムウェア攻撃を実行した。これより、国内グループ各社の受注・出荷業務、お客様相談室等の業務が停止した。同社は封じ込め対応、システムの復元作業および再発防止等のセキュリティ強化を実施し、感染の約 2 ヶ月後に EOS（電子受発注システム）による受注を再開した[6,7,8]。

◆窃取した認証情報により社内ネットワークに不正アクセス

2025 年 10 月 19 日、通販企業のアスクルは、ランサムウェア被害に遭い、業務が停止した。これにより、約 72 万件の顧客情報を含む業務情報が流出し、物流を委託していたグループ会社の業務も一部停止した。同年 12 月 12 日、同社は、多要素認証（MFA:Multi-Factor Authentication）を適用していなかった認証情報が窃取され、不正に社内ネットワークに侵入されたという調査結果を第 13 報として公表した。また、2026 年 1 月 21 日には、業務停止前に提供していた全ての商品購入が可能となったと復旧状況を第 17 報として公表した[9,10]。

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・セキュリティ対策のための予算確保
  - ・身代金要求に対する姿勢を決めておく

---

5 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 P50 コラム：不正プログラム（ランサムウェア）解析の一例（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

6 サイバー攻撃によるシステム障害発生について（アサヒグループホールディングス）
https://www.asahigroup-holdings.com/newsroom/detail/20250929-0102.html

7 サイバー攻撃による情報漏えいに関する調査結果と今後の対応について（アサヒグループホールディングス）
https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html

8 アサヒビール商品出荷状況について（アサヒビール）
https://www.asahibeer.co.jp/info/20251006.html

9 ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告 （ランサムウェア攻撃によるシステム障害関連・第 13 報）（アスクル株式会社）
https://pdf.irpocket.com/C0032/PDLX/O3bg/N4O3.pdf

10 サービスの復旧状況について（ランサムウェア攻撃によるシステム障害関連・第 17 報）（アスクル株式会社）
https://pdf.irpocket.com/C0032/KfQV/YWf9/fDRm.pdf

システム管理者、従業員、職員

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制を整備し対応する
  - ・表 1.2「情報セキュリティ対策の基本」を実施
  - ・安易に添付ファイルの開封やリンク・URL のクリックをしない
  - ・多要素認証（MFA）や FIDO／FIDO2（パスキー[11]など）を利用する
  - ・提供元が不明なソフトウェアを実行しない
  - ・PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う
  - ・ディレクトリーサービスや共有サーバー等へのアクセス権の最小化と管理の強化
  - ・不要なポートは閉じ、必要なサービスのみに絞る
  - ・公開サーバーへの不正アクセス対策
  - ・適切な取得日時、頻度を検討し、バックアップ運用を行う
    WORM（Write Once Read Many）機能等バックアップ自体の改ざん耐性強化策やバックアップからの復旧訓練の実施も有効。
  - ・暗号化された場合を想定したクリーンビルドの手順確立
  - ・定期的な復旧訓練の実施
  - ・例外措置の定期的な見直し、例外適用範囲の最小化
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う
  - ・適切に運用されているバックアップデータからのリカバリーを行う
  - ・整備した対応体制に基づき対応する

＜身代金の支払いと復旧業者の選定について＞

原則として身代金は支払わずに復旧を行うこと。身代金を支払っても、データ復元や流出防止の保証はない。もし、身代金を支払って復旧させた場合、「金銭の支払いに応じた企業」として攻撃者間で情報共有され、異なる攻撃者から再び狙われるおそれがある。また、復旧業者の選定[12]にも注意すること。業者が攻撃者と裏取引を行い、被害組織が知らないところで、業者が攻撃者に身代金を支払うことで復旧させたとしても、実質的には被害組織が業者経由で攻撃者に資金提供をした、とみなされるおそれがある。また、海外ではランサム攻撃の身代金を支払った場合の報告義務や身代金の支払いに応じることを禁じる国もある[13,14]。

---

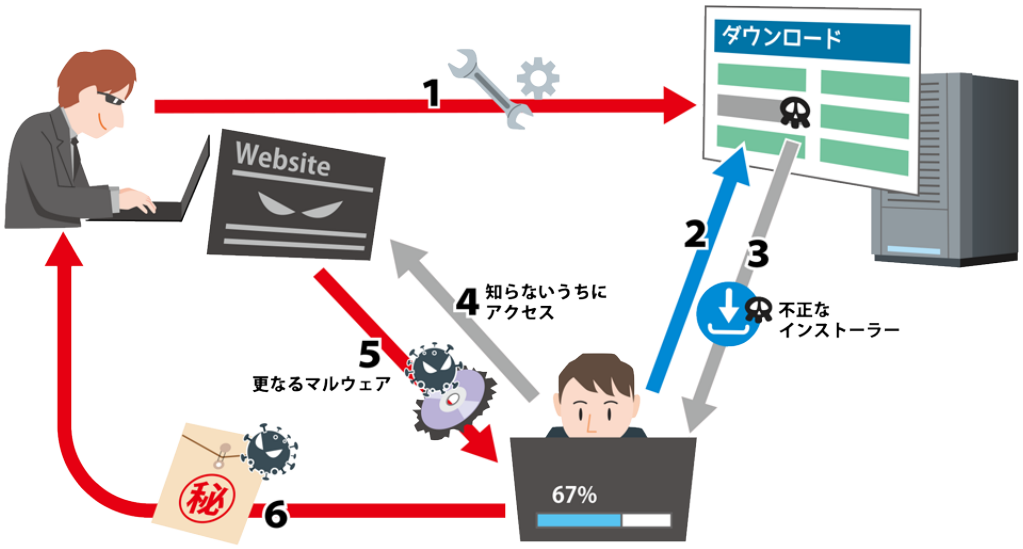
[11] 情報セキュリティ10大脅威 2024「コラム：パスキーを知っていますか？新しい認証方式でパスワードレスの時代に！」（IPA）
https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf

[12] データ被害時のベンダー選定チェックシート Ver.1.0（特定非営利活動法人デジタル・フォレンジック研究会）
https://sakura.digitalforensic.jp/home/act/products/higai-checksheet/

[13] FACTSHEET:Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025(Australia Government Department of Home Affairs オーストラリア内務省)
https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf
豪州政府は 2025 年 5 月 30 日、ランサムウェア攻撃の被害にあい、身代金の支払いに応じてしまった場合、72 時間以内に内務省へ報告を義務付ける法律「Cyber Security (Ransomware Payment Reporting) Rules 2025 」を施行したと発表

[14] UK to lead crackdown on cyber criminals with ransomware measures(英国政府)
https://www.gov.uk/government/news/uk-to-lead-crackdown-on-cyber-criminals-with-ransomware-measures
英国政府は2025年7月22日、ランサムウェア被害から国民を保護するため、公的機関に対し、ランサムウェア攻撃を受けたとしても、身代金の支払いに応じることを禁じることを義務付けることを決定

2位 サプライチェーンや委託先を狙った攻撃



商品の企画から、開発、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびそれらのプロセスに関わる組織および外部サービスも含めサプライチェーンと呼ぶ。このような「ビジネス上の繋がり」を悪用した攻撃に対しては、自組織の対策のみならず、取引先や委託先も含めたセキュリティ対策が必要になる。また、ソフトウェア開発のライフサイクルに関わる要素（ライブラリ、ツール、開発者やインフラ等）や、その要素間の繋がりをソフトウェアサプライチェーンと呼ぶ。このような「ソフトウェアの繋がり」を悪用した攻撃にも対策が求められる。攻撃を受けた組織は、秘密情報の漏えいや信用の失墜等の様々な被害が発生する。また、攻撃の足掛かりにされた組織は取引先に損害を与えることになり、取引停止、損害賠償を求められることもある。

＜脅威と影響＞

組織は、取引先や委託先、ソフトウェアやサービスの提供元や提供先等と様々な形で関わっている。攻撃者は、強固なセキュリティ対策をしている標的組織に対して直接的な攻撃はせず、標的組織が関わるサプライチェーンの中で脆弱な部分を狙って攻撃する。そして、脆弱な部分を経由して、間接的および段階的に標的組織を攻撃する。そのため、強固なセキュリティ対策を行う組織でも、弱点が存在しているサプライチェーン上の関係組織や導入しているソフトウェア等を足掛かりとされ、攻撃を受けるおそれがある。

＜攻撃手口＞

◆標的組織の関連会社や業務委託先を攻撃する

標的組織よりもセキュリティが脆弱な、国内外の関連会社や業務委託先等を攻撃し、攻撃された組織が保有する標的組織の秘密情報等を窃取する。

◆ソフトウェア開発元のソフトウェアにマルウェアを仕込み、利用者の機器をマルウェアに感染させる

多くの組織が利用するソフトウェアを改ざんしてマルウェアを仕込む。組織がそのソフトウェアをインストールやアップデートした際に、PC やサーバーがマルウェアに感染する。また、Web サイトにあるダウンロードリンクを改ざんし、マルウェアを仕込んだソフトウェアをダウンロードさせる手口もある。

◆MSP（マネージドサービスプロバイダー[15]）が利用する資産管理ソフトウェア等にマルウェアを仕込む

MSP が利用する資産管理ソフトウェア等にマルウェアを仕込み、MSP を利用した顧客の PC やサーバーをマルウェアに感染させる。

＜事例または傾向＞

◆業務委託先へのランサム攻撃

2025 年 11 月東海ソフト開発でランサムウェア被害が発生した。これに伴い、同社に業務を委託していた複数の企業が保有する個人情報が漏えいし、その一部と思われる情報がダークウェブ上で公開されていると公表した [16,17]。これを受け、同社に業務を委託する委託元各社においても、ランサムウェア被害に遭ったことを、順次公表した [18,19]。

◆正規の Web サイトを足掛かりにしてマルウェアに感染させる攻撃

Emurasoft 社は、2025 年 12 月と翌 1 月、EmEditor の公式サイトでインストーラーのダウンロードリンクが改ざんされ、偽のインストーラーが配信されるインシデントが発生したことを公表した。ユーザーがインストーラーを実行すると、本来とは異なる Web サイトへアクセスしてマルウェアに感染させられ、パスワード等の情報が窃取されるおそれがあった。同社は、一時的にすべてのサイトを閉鎖した。その後、Web ページ改ざんのリスクがない静的サイトを構築して対処した。偽のインストーラーを実行したユーザーに対しては、PC 等の再構築を推奨すると共に、EmEditor の開発元や JPCERT/CC へのサポートの依頼を推奨している [20]。

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討 [21]
  - ・セキュリティ対策のための予算確保
  - ・脅威インテリジェンスの推進
  - ・被害への補償の検討

システム管理者、従業員、職員

- 被害の予防および被害に備えた対策
  - ・情報管理規則の徹底

    業務委託自体の適切さについて、定期的に確認、検討する。
  - ・セキュリティ評価サービス（SRS[22]）を用いた自組織、委託先等のセキュリティ対策状況の把握

---

15 MSP（Managed Service Provider）：企業のITシステムの運用、保守、監視を行い、システムの可用性を維持するサービス事業者

16 重要なお知らせ ランサムウェア攻撃に関するお知らせとお詫び（第3報）（株式会社東海ソフト開発）
http://www.tokaisoftdev.co.jp/category/important/

17 重要なお知らせ ランサムウェア攻撃に関するご報告と現時点での対応について（第4報）（株式会社東海ソフト開発）
https://www.tokaisoftdev.co.jp/category/important/

18 業務委託先サーバへの不正アクセスに関するお知らせと注意喚起（東海大学）
https://www.u-tokai.ac.jp/news-notice/1358654/

19 業務委託l先サーバーへの不正アクセスに関するお知らせ(第一報)（東海教育産業株式会社）
https://www.tokai-eic.co.jp/news/3089/

20 【重要】EmEditor インストーラのダウンロード導線に関するセキュリティ インシデント（追加情報とまとめ）（Emurasoft, Inc.）
https://jp.emeditor.com/general/【重要】emeditor-インストーラーのダウンロード導線に-3/

21 サイバー保険（日本損害保険協会）
https://www.sonpo.or.jp/sme_insurance/cyber-hoken/

22 セキュリティ評価サービス Security Rating Services：SRS

・信頼できる委託先、取引先、サービスの選定

調達先や業務委託先等、契約時に取引先の規則を確認する。

商流に関わる組織、サービスの信頼性評価（ISMAP 等）、品質基準を検討し、複数の候補から検討する。

・契約内容の確認

組織間の取引や委託契約における情報セキュリティ上の責任範囲を明確化し、合意を得る。また、賠償に関する契約条項を盛り込む。

・委託先組織の管理

委託元組織が委託先組織のセキュリティ対策状況と情報資産の管理の実態を定期的に確認できる契約とすることが重要である。

・納品物の検証

納品物に組み込まれているソフトウェアやハードウェアの把握と脆弱性対策を実施する。ソフトウェアの把握や管理においては SBOM（Software Bill of Materials）の導入を検討する[23]。

・PC やサーバー、ネットワーク機器等の構成管理と変更管理を行い、委託先、取引先の ID やネットワーク接続を把握する

- 被害を受けた後の対応

・整備した対応体制に基づき対応する

・被害への補償

自組織に関わる組織と共に実施

- 被害の予防および被害に備えた対策

・取引先や委託先との連絡プロセスの確立

・取引先や委託先の情報セキュリティ対策の確認、監査を契約形態に応じて実施する

・情報セキュリティの認証取得および維持のため外部レビューを受ける

ISMS、P マーク、SOC2 等の外部認証取得、技術的対策や管理プロセスの維持向上のため、外部レビューをうける。

- 公的機関等が公開している資料の活用[24,25,26]
- 被害を受けた後の対応

・適切な報告／連絡／相談を行う

・整備した対応体制に基づき対応する

＜サイバー保険の検討＞

インシデントが起こると、事故対応費用、損害賠償費用、利益損害・営業継続費用などが発生する可能性がある。これら費用への対策の1つとしてサイバー保険がある。補償内容は保険会社や保険プランにより異なるので、保険会社や代理店に確認する。なお、日本ではランサムウェアの被害によって支払った身代金はサイバー保険の対象にならないので注意が必要である。

---

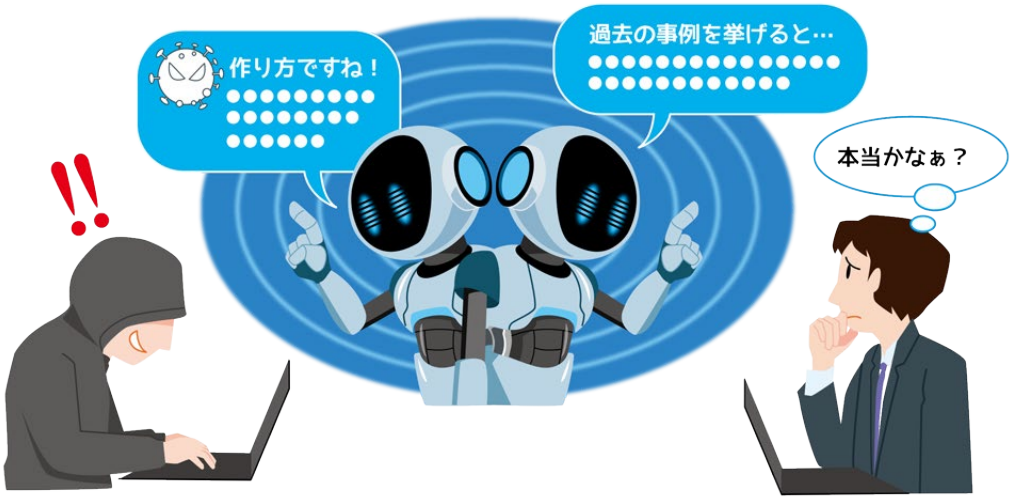
23 サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました（経済産業省）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

24 サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

25 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（国家サイバー統括室）
https://www.cyber.go.jp/pdf/council/cs/taisaku/ciso/dai02/02shiryou0303.pdf

26 自動車産業サイバーセキュリティガイドライン（一般社団法人日本自動車工業会）
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

3位 AI の利用をめぐるサイバーリスク



生成 AI の進化、普及に伴い、様々な問題、懸念が浮上している。例えば、AI に対する不十分な理解による、意図しない問題として他者の権利侵害[27]、情報漏えい、AI が加工・生成した結果を十分に検証せず鵜呑みにすることにより生じる問題、AI の悪用によるサイバー攻撃の容易化[28]、手口の巧妙化などがあげられる。

＜脅威と影響＞

人口減少と急速な高齢化、十分な雇用確保が困難な状況下において、諸外国を追いつつ、AI の積極利用は国内でも進んでいる[29]。一方、AI 活用による懸念も指摘されている。例えば、AI を利用したシステムの様々な脆弱性を狙った、外部からの攻撃リスクや AI 悪用による攻撃の容易化を招く可能性が指摘されている。また、生成 AI の業務利用においては、生成された情報の正確性を確認せず活用した結果、思わぬトラブルが引き起こされるリスクもあるため、利用者が十分に確認する必要性について指摘されている。

＜リスク＞

◆職場に許可なく AI を業務利用し、情報漏えいにつながる可能性

例えば職場で AI サービスの利用が無い場合など、従業員が個人的に利用している AI サービスを業務利用することがある（シャドーAI）[30]。本来組織外への持ち出しが禁止されている業務データや資料等を AI サービスに入力すれば、情報漏えいにつながる。また、職場が従業員の個人アカウントによる AI の業務利用を認識できないこともリスクといえる。

◆実在しない情報を対話型 AI が生成する可能性（ハルシネーション）

対話型 AI は時に、架空の情報をあたかも事実として生成し、利用者に提示することがある。問いに対する答えが容易に得られ、利便性の高さ、手軽さから過剰依存し、誤った生成結果を鵜呑みにしてしまうことも考えられる。利用者は生成結果の精査を行うことが求められる。

---

27 OpenAIと提携したディズニーがGoogleを提訴、AIによる「大規模な著作権侵害」を主張（マイナビニュース）
https://news.mynavi.jp/techplus/article/20251212-3801182/

28 Anthropic、「Claude」が中国政府系攻撃者に悪用されたと報告（アイティメディア株式会社）
https://www.itmedia.co.jp/news/articles/2511/14/news061.html

29 企業における AI 利用の現状（総務省）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/nd112220.html

30 Enterprise AI and SaaS Data Security Report 2025（LayerX Security）
https://go.layerxsecurity.com/hubfs/LayerX_Enterprise_AI_and_SaaS_Data_Security_Report.pdf

◆AI を助力に得たサイバー脅威の増長

AI による翻訳機能・能力の向上により、攻撃者が Web ページの翻訳やフィッシングの文面を標的の母国語で違和感なく表現することを可能にし、言語の壁を実質的に乗り越えた多言語での攻撃を格段に容易にする。また、生成 AI をサイバー攻撃のアシスタントとして利用することで、様々な攻撃が容易に展開できるようになり、対処しなければならないインシデントの頻度・数量が増えたり、平均的な攻撃の技術水準が高まったりしている。

＜事例または傾向＞

◆生成 AI の業務利用による情報漏えい

米国の AI 企業の調査[31]によれば、業務において、生成 AI にデータをコピー＆ペーストしてプロンプト（指示文）として入力している利用者が 77%おり、そのうち 82%が組織に管理されていないアカウントによるものであったという。こうした行為により、組織が把握できない形で情報漏えいが発生するリスクが高まる。

◆生成 AI を使い作成した資料に、実在しない判例が含まれていた事例

2025 年 1 月、米国テキサス州の裁判所で公聴会が開催された。前年に同州の弁護士が提出した意見書に実在しない判例が引用されていることが判明し、生成 AI を用いて作成していたことが明らかになった。当該弁護士は、生成 AI を用いて作成したデータにハルシネーションが起こりうることを知らなかったという[32]。

◆生成 AI を悪用したプログラムの作成

2025 年 2 月、不正に入手した ID とパスワードを機械的に入力して携帯電話の回線契約まで行うプログラムを用いて携帯電話の回線を契約したとして、中高生 3 人が不正アクセス禁止法違反と電子計算機使用詐欺の疑いで逮捕された。生成 AI を補助的に使いプログラムを自作したという[33]。

◆AI の脆弱性

2025 年 6 月、Microsoft 365 Copilot の脆弱性「EchoLeak」の存在が報道された。この脆弱性を悪用する不正プロンプトが外部から注入されると、不適切な AI の動作が誘発され、Microsoft 365 Copilot にアクセスを許可した社内の秘密データ等が流出する可能性があったという[34]（詳細はコラムを参照のこと）。

＜対策と対応＞

※以下では「AI 事業者ガイドライン[35]」に言う AI 利用者における対策を想定している。

経営者層

- シャドーAI 回避のため、AI サービス利用の検討
  - ・未許可・未認可の AI サービス利用（シャドーIT）の禁止
- AI ガバナンスおよびサービス利用規定の整備
  - ・AI 事業者ガイドライン等の参照・準拠
  - ・個人アカウントにおける業務利用の制限
  - ・規程違反時の対応（ペナルティ）の明確化

---

31 NEW Research: AI Is Already the #1 Data Exfiltration Channel in the Enterprise（The Hacker News Media Private Limited）
https://thehackernews.com/2025/10/new-research-ai-is-already-1-data.html

32 生成AIに騙される弁護士がいまだに相次ぐ（JBpress）
https://jbpress.ismedia.jp/articles/-/86872

33 生成AI悪用、楽天回線1000件不正契約か　中高生を逮捕（日本経済新聞）
https://www.nikkei.com/article/DGXZQOUE271BZ0X20C25A2000000/?msockid=31e1fd8ad7c361513e27ea89d6b06018

34 初のゼロクリックAI脆弱性「EchoLeak」,Microsoftの「Copilot」の脆弱性で（修正済み）（ITMedia NEWS）
https://www.itmedia.co.jp/news/articles/2506/12/news074.html

35 AI 事業者ガイドライン（経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

・外部サービス利用時には入力データを学習対象から除外するオプトアウト設定の徹底

- AI サービス契約時の約款の確認
- トラブルの発生に備えた専門家、相談窓口の確保
- 決裁や承認プロセスのガバナンス強化

・業務における決裁・承認プロセスに対し、複数名によるチェックを規程化し、運用を徹底する

（高度化するソーシャルエンジニアリングへの備え）

システム管理者、従業員、職員

- AI 利用におけるセキュリティ強化

・IT 資産管理および構成管理を行い、通信ログ・CASB 等の活用により、AI サービスの利用状況を把握・管理されていない AI サービスの利用を把握

・AI 悪用による不正アクセス、ソーシャルエンジニアリング等抑止のため多要素認証（MFA）の徹底

- セキュリティ対策全般の点検や強化

・攻撃力の高度化・効率化を踏まえ、既存対策全般の点検や強化の検討

- AI 利用における教育の徹底

・AI 利用における講習等プログラムの用意

・社内の秘密情報等を安易に入力しない

・ユーザーの指示等を正確に反映した結果を出力するとは限らないこと、ハルシネーションが存在することを理解する

・AI への過剰な依存に留意する

- 最新の手口・脅威動向の把握
- 被害を受けた後の対応

・適切な報告／連絡／相談を行う

・整備した対応体制に基づき対応する

コラム AI とサイバーセキュリティ～脅威の現在地と見通し～

AI 技術の進化はサイバーセキュリティに新たな課題をもたらしていますが、現状では既存の脅威を増幅させる傾向が強く見られます。このコラムでは、AI がサイバーセキュリティに及ぼす影響、AI を悪用した攻撃事例、そして AI システム自体が抱える脆弱性について、現状と見通しを概説します。

【AI がサイバーセキュリティに及ぼす影響の見通し】

英国国家サイバーセキュリティセンター（NCSC）は、2027 年にかけて AI がサイバー攻撃の脅威を質・量ともに増大させると予測しています。AI は侵入作戦の効率を高めるだけでなく、特にゼロデイ脆弱性の発見や攻撃コード開発を加速させることが懸念されています。これにより、修正プログラム公開から攻撃までのタイムラグが短縮されるおそれがあります。偵察やマルウェア改良の自動化が進むことで、攻撃の検知回避能力が向上することも予測されています。一方で、防御側においても、AI 活用の有無によるデジタル格差が拡大し、対応が遅れたシステムのリスクが高まると見られています [36]。

【AI を悪用したサイバー攻撃の実態】

攻撃者が自らの能力を強化するために AI を導入する事例が現れています。Anthropic 社の調査では、中国の国家支援型アクターが AI「Claude Code」を悪用し、高度なサイバー諜報活動を行ったことが確認されました。この事例では、偵察、脆弱性発見、認証情報窃取、データ分析といった一連の攻撃プロセスの 80～90%を AI が自律的に実行しており、標的型攻撃の自動化が進んでいることを示しています。

また、Google Threat Intelligence Group によると、実行中に生成 AI を活用して挙動やコードを変化させるマルウェア（PROMPTFLUX や PROMPTSTEAL など）が出現しています。これらはハードコードされた指令の代わりに、マルウェアの実行時に AI へリクエストを送り、検知回避のための難読化コードや情報窃取コマンドを動的に生成させ、セキュリティソフトによる検出を逃れようとします [37,38]。

【AI システム固有の脆弱性を狙った攻撃】

AI システム、特に大規模言語モデル（LLM）を組み込んだアプリケーションには特有の脆弱性が存在します。Microsoft 365 Copilot では、検索拡張生成（RAG）の仕組みを悪用した攻撃である EchoLeak が発見されました。これはメール等に含まれる不可視のプロンプトを AI に読み込ませることで、ユーザーの操作なしに秘密情報を外部へ送信させるものです。Web ブラウザ統合型 AI（いわゆる AI ブラウザ）に対しては、URL の末尾に悪意ある命令を隠す HashJack という手法が Cato Networks により発見されました。ブラウザ AI が URL 全体を読み取る性質を利用し、フィッシング誘導などを行います。さらに、AI モデル利用時に広く使用されているプロトコルである MCP（Model Context Protocol）を用いた AI 向けサービス（MCP サーバー）においても、営業秘密等を含むデータと Web 検索結果などの信頼できない情報とが混用されることで、外部入力による不正操作のリスクが高まるおそれがあると、Pynt 社の調査で指摘されています。

---

[36] Impact of AI on cyber threat from now to 2027（NCSC）
https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

[37] Disrupting the first reported AI-orchestrated cyber espionage campaign（Anthropic）
https://www.anthropic.com/news/disrupting-AI-espionage

[38] CTIG AI 脅威トラッカー: 脅威アクターによる AI ツール使用の進化（GTIG）
https://cloud.google.com/blog/ja/topics/threat-intelligence/threat-actor-usage-of-ai-tools/

上記で例示した攻撃の多くに共通するのが間接プロンプトインジェクションと呼ばれる手法です。AI には保護措置（セーフガード）が導入されており、サイバー侵入を手助けするようなリクエストは通常であれば拒否されますが、AI に不正プロンプトを入力するプロンプトインジェクション攻撃で、この保護を解除できる場合があります（ジェイルブレイク）。間接プロンプトインジェクションは、AI が動作過程で自ら参照したデータに不正プロンプトが含まれており、それを取り込むことで AI へのプロンプト インジェクションが成立してしまうような攻撃を指しています。AI 側で不正プロンプトを見分けてくれればよいのですが、技術的対策で完璧なものは知られていません。このため、AI が参照するデータが外部由来の危険かもしれないデータで汚染されないようにするといった配慮が必要です [39,40,41]。

【従来型脆弱性と開発プロセスへの攻撃】

AI サービスであっても、その基盤インフラにおける設定ミスや認証不備といった従来型の脆弱性は依然として重要な攻撃経路になりえます。実際、DeepSeek のデータベースや AI コンパニオンアプリのメッセージング基盤（Kafka）が認証なしでインターネットに公開され、機密データが流出した事例が報告されています。これらは AI 技術そのものの欠陥ではなく、基本的なセキュリティ管理の不備に起因します [42]。

ソフトウェア開発の現場でも AI ツールが標的となっています。AI コードエディタ Cursor では、プロジェクト内のファイル（README 等）に悪意ある指示を埋め込むことで、開発者の権限で任意のコードを実行させる間接プロンプトインジェクションの脆弱性が発見されました。また、Koi Security は、AI がコード生成時に存在しないパッケージ名を提案してしまうハルシネーションを悪用したサプライチェーン攻撃の実例を報告しています。攻撃者は AI が提案しそうな名前でマルウェアパッケージを登録し、それを開発者にインストールさせることで、悪意あるコードを実行させます [43,44,45]。AI の生成したプログラムコードには脆弱性が含まれる場合があるという問題の一例とも言えます。

【対策と今後の見通し】

間接プロンプトインジェクションは AI に固有の弱点を狙った新時代の攻撃と言えますが、それ以外の事例の大部分は、従来と変わらないサイバー攻撃が AI によって半自動化・高速化されているといったものに留まります。このため、従来のサイバーセキュリティ対策が有効です。他方で、AI の技術はすさまじい速度で発展しており、数か月の内にも状況が変化する可能性が今のところ常にあります。

サイバーセキュリティの基本をより一層しっかりと押さえつつ、予断を持つことなく最新の状況を注視していく姿勢が求められています。

---

39 Quantifying Risk Exposure Across 281 MCPs（Pynt）
https://www.pynt.io/resources-hub/mcp-security-research-2025

40 ゼロクリックで情報漏えい：Microsoft 365 Copilot の脆弱性「EchoLeak」の調査結果を解説（TrendMicro）
https://www.trendmicro.com/ja_jp/research/25/g/preventing-zero-click-ai-threats-insights-from-echoleak.html

41 HashJack – Novel Indirect Prompt Injection Against AI Browser Assistants（Cato Networks）
https://www.catonetworks.com/blog/cato-ctrl-hashjack-first-known-indirect-prompt-injection/

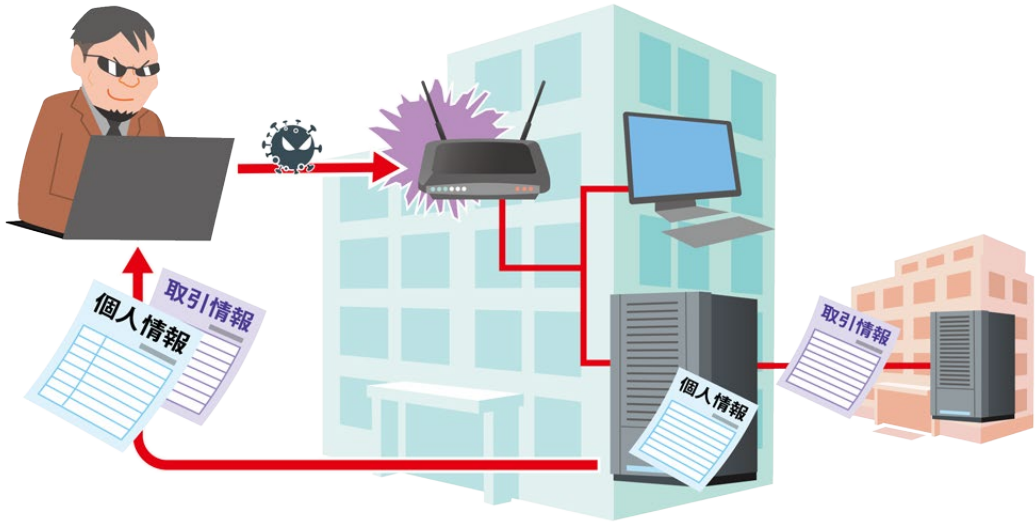
42 AI 彼女アプリからデータ流出、40 万人以上に影響か（TECH+）
https://news.mynavi.jp/techplus/article/20251013-3535170/

43 Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History（WIZ）
https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

44 Cursor AI Code Editor Fixed Flaw Allowing Attackers to Run Commands via Prompt Injection（The Hacker News）
https://thehackernews.com/2025/08/cursor-ai-code-editor-fixed-flaw.html

45 PhantomRaven: NPM Malware Hidden in Invisible Dependencies（Koi Security）
https://www.koi.ai/blog/phantomraven-npm-malware-hidden-in-invisible-dependencies

4位 システムの脆弱性を悪用した攻撃



製品の開発ベンダー等による脆弱性対策情報の公表は、脆弱性の存在や対策の必要性を製品利用者に対して広く呼び掛けることができる。他方、攻撃者はその情報を悪用し、脆弱性対策が講じられていないシステムを狙って攻撃を行うことがある。攻撃者が脆弱性を悪用してシステムに侵入すると様々な攻撃が可能となる。この結果、攻撃の影響が事業やサービスの停止等にまで波及し、甚大な被害に至ることもある。昨今、脆弱性の発見から、それを悪用した攻撃が発生するまでの時間が短くなっているため、脆弱性対策情報が公表された際には、早急な対策が必要である。

＜脅威と影響＞

OS やアプリケーション等のソフトウェアの脆弱性が発見されると、開発ベンダー等が修正プログラム（パッチ）や回避策等を公開し、製品利用者へ対策を促す。他方、攻撃者は、公表された脆弱性対策情報や PoC（Proof of Concept：概念実証）[46]を基に攻撃プログラム等を作成し、パッチ適用等の対策が講じられていないシステムに対して、脆弱性を悪用した攻撃を行う（N デイ攻撃：＜攻撃手口＞を参照のこと）。

脆弱性を悪用した攻撃が行われると、マルウェア感染や情報漏えい、Web ページやファイルの改ざん等の被害が発生し、事業やサービスの停止に追い込まれる場合もある。特に、ネットワーク機器(VPN 機器等)やCMS（プラグインを含む）といったインターネットから直接アクセスできる製品・システムの脆弱性については、攻撃プログラム等が公開された場合に、多くの企業に被害が及ぶおそれがある。

＜攻撃手口＞

◆公表される前の脆弱性を悪用（ゼロデイ攻撃）

開発ベンダー等が脆弱性対策情報を公表する前に、攻撃者が脆弱性を悪用して行う攻撃をゼロデイ攻撃と呼ぶ。悪用の手口は、脆弱性毎に様々だが、例えば、ネットワーク機器の脆弱性を悪用した遠隔での任意のコード実行が挙げられる。

◆製品利用者が対策する前の脆弱性を悪用（N デイ攻撃）

パッチや回避策が公開され、その適用や回避策を講じるまでの期間における脆弱性を N デイ脆弱性と呼ぶ。ソフトウェアの脆弱性管理が不適切な場合、未対策の期間が長くなり、被害に遭うリスクが大きくなる。

---

46 PoC（Proof of Concept）：発見された脆弱性を実証するために公開されたプログラムコード。不正侵入やマルウェア感染を試みる悪意のあるプログラムの一部として悪用されることがある。

◆攻撃ツールや攻撃サービス等を悪用

公表された脆弱性に対しては、短期間で攻撃ツールが作成され、ダークウェブ等で販売されたり、攻撃サービスとして提供されたりすることがある。また、誰でも利用可能なオープンソースのツールでは、攻撃者が脆弱性を利用する機能を実装する、といった悪用をされることもある。

＜事例または傾向＞

◆ゼロデイ攻撃による不正アクセス被害

2025 年 7 月 8 日、日鉄ソリューションズは、同年 3 月 7 日に同社のネットワーク機器に存在した脆弱性を狙ったゼロデイ攻撃による不正アクセス被害があったことを公表した。この攻撃により、サーバー内に保存されていた個人情報等の一部が漏えいしたおそれがあるという。漏えいしたおそれがあるファイルの中には、経済産業省が過去に業務委託した事業に関する情報も含まれていたことから、同省も注意喚起を公表した[47,48]。

◆React Server Components の脆弱性を悪用した攻撃

2025 年 12 月 3 日、React Server Components の脆弱性が公表され、その翌日には、PoC が公開された。この脆弱性は、共通脆弱性評価システム（CVSS：Common Vulnerability Scoring System）の深刻度が緊急（基本値 10.0）と評価されている。世界中で普及している製品であることから、脆弱性を悪用した攻撃が国内外で多数確認され、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）の KEV（Known Exploited Vulnerabilities Catalog）にも掲載された。この脆弱性は発見者の命名から、「React2Shell」とも呼ばれるようになった。IPA や JPCERT/CC においても、早急に対策を実施するよう、注意喚起が行われた[49,50,51,52]。

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・パッチ適用や回避策等、セキュリティ対策のための予算確保
  - ・脅威インテリジェンスを推進する

システム管理者、製品利用者

- 被害の予防および被害に備えた対策
  - ・表 1.2「情報セキュリティ対策の基本」を実施
  - ・利用している資産の把握、管理体制の整備

    情報資産を把握し、その重要度に応じて格付けした上で重要情報の管理者を定める。

---

47 不正アクセスによる情報漏洩の可能性に関するお詫びとお知らせ（日鉄ソリューションズ株式会社）
https://www.nssol.nipponsteel.com/press/2025/20250708_160000.html

48 業務委託先への不正アクセスによる個人情報の漏えいについて（経済産業省）
https://www.meti.go.jp/statistics/toppage/topics/other/other_related_information250711.html

49 Critical Security Vulnerability in React Server Components（React）
https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

50 React Server Componentsにおける脆弱性について（CVE-2025-55182）（IPA）
https://www.ipa.go.jp/security/security-alert/2025/alert20251209.html

51 React Server Componentsの脆弱性（CVE-2025-55182）について（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2025120501.html

52 React Server Componentsの脆弱性CVE-2025-55182（React2Shell）についてまとめてみた。（piyolog）
https://piyolog.hatenadiary.jp/entry/2025/12/08/113316

・セキュリティのサポートが充実しているソフトウェアやバージョンを使う

パッチや回避策の提供が迅速である製品を利用し、サポート対象のソフトウェアを使う。

・脆弱性情報の収集、脆弱性の悪用状況の収集、脆弱性対策の優先度付け、対策状況の管理、パッチマネジメントの実施

・PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う

・ソフトウェアの把握や管理においては SBOM（Software Bill of Materials）の導入を検討する [53]

・ゼロデイ攻撃への対策を行う

修正パッチが無いことを前提とした多層防御、異常を検知する仕組み・体制を構築する。

- 被害の早期検知

・PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う

- 被害を受けた後の対応

・適切な報告／連絡／相談を行う

・整備した対応体制に基づき対応する

・影響調査および原因の追究、対策の強化

開発ベンダー

- 製品セキュリティの管理、対応体制の整備

・製品に組み込まれているソフトウェア、コンポーネントの把握、管理の徹底

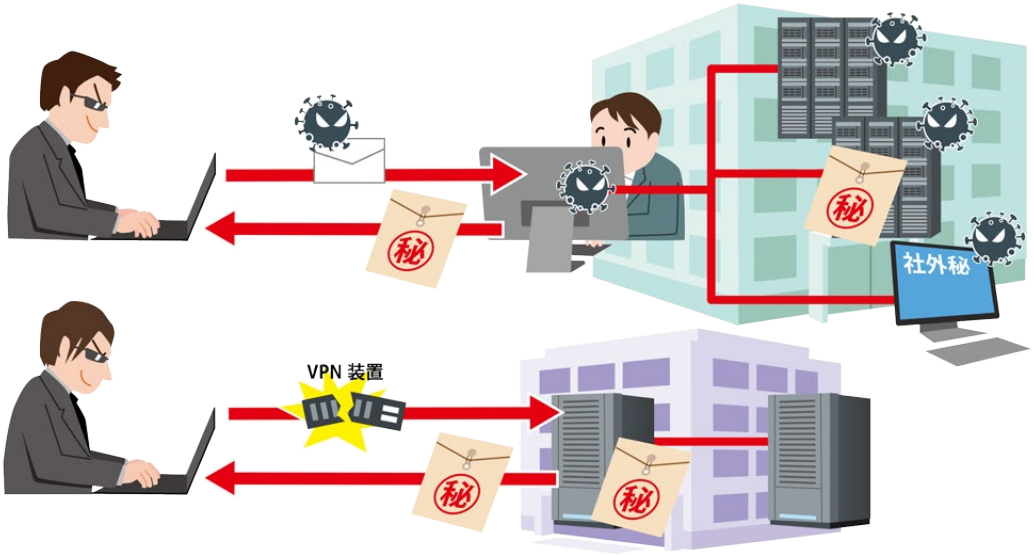
・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う

・脆弱性が発見された時の対応手順の作成

・脆弱性情報を迅速に発信する仕組みの整備

53 サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました（経済産業省）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

5位 機密情報を狙った標的型攻撃



標的型攻撃とは、特定の組織（民間企業、官公庁、団体等）に対して行われるサイバーエスピオナージ（サイバー諜報活動）であり、主に機密情報の窃取を目的としている。攻撃者は社会の動向や慣習の変化に合わせて攻撃手口を変える等、標的とする組織の状況に応じた巧みな攻撃手法で目的を果たそうとする。

＜脅威と影響＞

政府機関や特定のセクターに潜入し、組織内部の機密情報を窃取するサイバー攻撃事例が確認されている。攻撃者はPCやサーバーへのマルウェア感染や不正アクセス等により組織内部に侵入し、マルウェアやOS標準のコマンドを用いて情報の窃取を行う。組織内部に潜伏し、長期にわたり活動を行うケースもある。窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障等に重大な影響を及ぼすおそれがある。

また、データ削除等による企業等の活動の妨害、その企業のサプライチェーンに属する関連組織への攻撃の踏み台としての悪用、暗号資産を窃取して犯罪組織の資金源とする等、組織の規模や業種を問わず狙われるおそれもある。

＜攻撃手口＞

◆不正アクセス

標的組織が利用するクラウドサービスやWebサーバー、VPN装置等のネットワーク機器の脆弱性を悪用するほか、流出・窃取された認証情報や脆弱な認証管理を悪用して不正にアクセスし、組織内部へ侵入する。侵入後は、追加の認証情報の窃取や不正アカウントの作成、バックドアの設置等により永続的なアクセス手段を確保し、活動を継続することがある。また、認証情報等を窃取した上で、正規の経路で組織のシステムへ再侵入することもある。

◆メールを用いた攻撃

メールの添付ファイルや本文に記載されたリンク先にマルウェアを仕込み、そのファイルを開封させたり、リンクにアクセスさせたりすることでPCをマルウェアに感染させる。メール本文や件名、添付ファイル名は業務や取引に関連する内容に偽装され、実在する組織の差出人名が使われる場合もある。

◆Webサイトの改ざん（水飲み場型攻撃）

攻撃者は標的組織が頻繁に利用するWebサイトを調査し、改ざんする。そして、従業員や職員がそのWebサイトにアクセスした際、偽装されたマルウェアのインストールを誘導し、PCをマルウェアに感染させる。

＜事例または傾向＞

◆MirrorFace による標的型攻撃

日本等を標的としている標的型攻撃グループである MirrorFace（別名 Earth Kasha）は、2025 年 3 月頃、新たなサイバー攻撃を行ったとされる。MirrorFace は、同年 1 月に警察庁、国家サイバー統括室（NCO）から注意喚起がなされ [54]、今回は、以前から利用されている ANEL と呼ばれるマルウェアの新型亜種の利用が判明した。手口としては、標的に OneDrive のリンクが埋め込まれたスピアフィッシングメールを送信し、そのリンクをクリックさせることで、最終的に ANEL の展開につなげる。サイバー諜報活動、情報窃取を目的に、標的の対象を日本や台湾の行政組織や公共機関に広げていると推測されている [55]。そのほか MirrorFace については、2024 年 8 月に 2025 年日本国際博覧会（大阪・関西万博）に便乗して欧州の外交機関を標的として攻撃を行っていたことも分かっている [56]。

◆ネットワーク機器等に対するネットワーク貫通型攻撃のおそれ

2025 年 10 月 31 日、IPA は、「VPN 機器等に対する ORB（Operational Relay Box：攻撃の中継拠点）化を伴うネットワーク貫通型攻撃のおそれについて」と題した注意喚起を公表した。これは、ネットワーク境界に設置される VPN 機器等の脆弱性が攻撃に悪用される事例が確認されているためである。その被害は自組織内にとどまらず、機器が攻撃者に乗っ取られることにより、当該機器は ORB として第三者への攻撃の踏み台として利用されるおそれがある。この対策として、迅速なパッチ適用や機器の更新、可視化、監視の強化などを例に挙げ、VPN 機器等の利用者に注意を促している [57]。

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・セキュリティ対策のための予算確保

セキュリティ担当者、システム管理者

- 被害の予防および被害に備えた対策
  - ・情報の管理と運用規則策定
    情報を保存するときに暗号化する等、管理や運用の規則を定めて運用する。
  - ・サイバー攻撃に関する継続的な情報収集
  - ・情報リテラシー、モラルを向上させる
  - ・インシデント対応の定期的な訓練を実施
    関係者やセキュリティ事業者、専門家と迅速に連携する対応方法や連絡方法を整備する。
  - ・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う
  - ・アプリケーション許可リストの整備
  - ・取引先のセキュリティ対策実施状況の確認

---

54 日本や台湾を狙う標的型攻撃：「Earth Kasha」が攻撃手法を更新して新たな攻撃キャンペーンを開始（トレンドマイクロ）
https://www.trendmicro.com/ja_jp/research/25/e/earth-kasha-updates-ttps.html

55 MirrorFace によるサイバー攻撃について（注意喚起）（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf

56 AKAIRYŪ（赤い龍）作戦：MIRRORFACE、EXPO 2025大阪・関西万博に便乗して欧州の外交機関を攻撃（イーセットジャパン）
https://www.eset.com/jp/blog/welivesecurity/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor-jp/

57 VPN機器等に対するORB（Operational Relay Box）化を伴うネットワーク貫通型攻撃のおそれについて（IPA）
https://www.ipa.go.jp/security/security-alert/2025/alert20251031_vpn.html

「2 位 サプライチェーンや委託先を狙った攻撃」の「対策と対応」を参照のこと。

・海外拠点等も含めたセキュリティ対策の向上

- 被害の早期検知・攻撃の監視

・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う

- 被害を受けた後の対応

・整備した対応体制に基づき対応する

従業員、職員

- 被害の予防および被害に備えた対策（通常、組織全体で実施）

・表 1.3「情報セキュリティ対策の基本+α」を実施

・安易に添付ファイルの開封やリンク・URL のクリックをしない

- 被害を受けた後の対応

・整備した対応体制に基づき対応する

6位 地政学的リスクに起因するサイバー攻撃（情報戦を含む）

地政学的リスクとは、地理的な条件との関係により、政治的・軍事的な緊張が引き起こすリスクを指す。政治的に対立する周辺国に対して、社会的な混乱を引き起こすことを目的としたサイバー攻撃を行う国家が存在する。この場合のサイバー攻撃は、外交・安全保障上の対立をきっかけに、嫌がらせや報復、周辺国の機密情報の窃取、外貨獲得等が目的とされる。そのほか、SNS を中心として、他国の評判を貶め自国に優位な状況を作ること等を目的とした偽情報による影響工作も行われている。

＜脅威と影響＞

国家支援型の組織的犯罪グループや国家機関の職員等で構成されるグループ等が、社会的なインパクトが大きい組織や重要インフラ企業等に攻撃を行うことで、社会的な混乱が引き起こされるおそれがある。時には、経済的打撃を与えるためにランサム攻撃を装い、サプライチェーン全体が影響を受けることもある。また、国や組織の機密情報、技術情報等が窃取され、競争優位性が損なわれるおそれがある。加えて、経済制裁を受けている国家がサイバー攻撃を通じて金銭を得ることで経済制裁の実効性が低下することも想定される。

＜攻撃手口＞

◆DDoS 攻撃

標的のシステムに大量のデータを送り付け、システムが提供するサービスを停止させることで、そのサービスを利用する人々を混乱させる（手口の詳細は「9 位 DDoS 攻撃（分散型サービス妨害攻撃）」を参照のこと）。

◆ランサム攻撃を偽装したサイバー攻撃

国家主導もしくは国家支援のもと、標的組織の業務停止や機密情報の窃取を狙い、ランサムウェアに感染させる。外交問題の回避や侵入目的の隠ぺいを狙い、通常のランサム攻撃のように金銭要求をすることで、一般的な犯罪グループを装うことがある。

◆ネットワーク貫通型攻撃

標的組織のネットワークとインターネットの境界に設置されたセキュリティ製品の脆弱性を悪用して攻撃し、標的組織に不正侵入し、有事のシステム破壊、機密情報の窃取、他組織への攻撃の踏み台（中継）とする。

◆スピアフィッシングによる情報窃取

特定の個人を標的に、電話、メール、SNS 等を用いたソーシャルエンジニアリング等で情報を収集し、それを基に標的へメールを送信し、添付ファイルの実行や URL をクリックさせ、認証情報や機密情報を窃取する。

◆偽情報の流布

国家を背景とした機関が自国に優位な状況を作ること等を目的として、サイバー空間上の偽情報やディープフェイクを用いて影響工作等を行う。

＜事例または傾向＞

◆国家を背景とした DDoS 攻撃の状況

2025 年 12 月、米司法省はハクティビスト集団である Noname057（16）および Cyber Army of Russia Reborn（CARR）の活動をほう助した疑いで容疑者を起訴した。起訴状によれば、両集団は外国の政府によって設立、資金支援を受けて世界中の企業・政府機関へサイバー攻撃を行っていたことが指摘された [58]。

Noname057（16）に関しては、同年 12 月と翌年 1 月に英米のサイバーセキュリティ機関が注意喚起を発出しているほか [59,60]、日本では外国への経済制裁に対する報復等を動機とした DDoS 攻撃が観測されている状況であった [61]。

◆国家を背景とした影響工作の状況

近年では国家に紐づくアクターによる、偽アカウントやボットアカウントによる偽情報の拡散や AI で生成された偽の音声、動画等を悪用した情報戦・認知戦、影響工作活動が活発化している。欧州では、2024 年 11 月のルーマニア大統領選挙 [62]や 2025 年 2 月のドイツ総選挙 [63]、同年 6 月のポーランド大統領選挙 [64]、同年 9 月のモルドバ共和国議会選挙 [65]で外国からの影響工作が観測されている。

さらに、こうした選挙干渉だけでなく、国際世論を分断させるような情報操作も行われている。2024 年から 2025 年にかけては、トランプ米政権による米国際開発局（USAID）の閉鎖などに絡め、途上国支援にネガティブな印象を与え、国際世論を分断させるための情報操作が確認された [66]。

また、紛争などの有事の際には、情報戦・認知戦も活発化する。2025 年 12 月には、タイ・カンボジア間で武力衝突が発生したが、情報空間での偽情報流布やナラティブ（物語）の戦いが問題となった。そのため、2025 年 12 月 27 日に停戦延長のために署名した両国共同声明では、「双方は緊張緩和、否定的な世論の緩和、平和的対話に資する環境の醸成を図るため、虚偽の情報や偽ニュースの拡散を控えることに合意する」といった文言が盛り込まれるに至った [67]。

---

58 Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups（Office of Public Affairs）
https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal

59 Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure（Cybersecurity and Infrastructure Security Agency）
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

60 Pro-Russia hacktivist activity continues to target UK organisations（National Cyber Security Centre）
https://www.ncsc.gov.uk/news/pro-russia-hacktivist-activity-continues-to-target-uk-organisations

61 親ロシアのハクティビストNoName057(16)が日本のWebサイトを攻撃（SOMPO CYBER SECURITY）
https://www.sompocybersecurity.com/column/column/pro-russia-hacktivist-attacks-japanese-entities

62 How Romania's Presidential Election Became the Plot of a Cyber-Thriller（European Union）
https://youth.europa.eu/news/how-romanias-presidential-election-became-plot-of-cyber-thriller_en

63 ドイツがロシア非難、航空安全へのサイバー攻撃と選挙での偽情報拡散（AFPBB News）
https://www.afpbb.com/articles/-/3613720

64 Illegal Doppelganger Operation: Targeting the Polish Elections（Alliance4Europe）
https://alliance4europe.eu/doppelganger-poland-elections

65 How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation（BBC）
https://www.bbc.com/news/articles/c4g5kl0n5d2o

66 ロシア「国際協力」で日本に情報操作　途上国支援、SNSで批判あおる（日本経済新聞）
https://www.nikkei.com/article/DGXZQOCD01B120R01C25A0000000/

67 Cambodia-Thailand Border Conflict: Restraint in the Digital Information Battlefield（moderndiplomacy）
https://moderndiplomacy.eu/2026/01/14/cambodia-thailand-border-conflict-restraint-in-the-digital-information-battlefield/

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・地政学的リスクの情報収集体制を整備する
  - ・自社事業に関する地政学的リスクの影響調査
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・セキュリティ対策のための予算確保

システム管理者

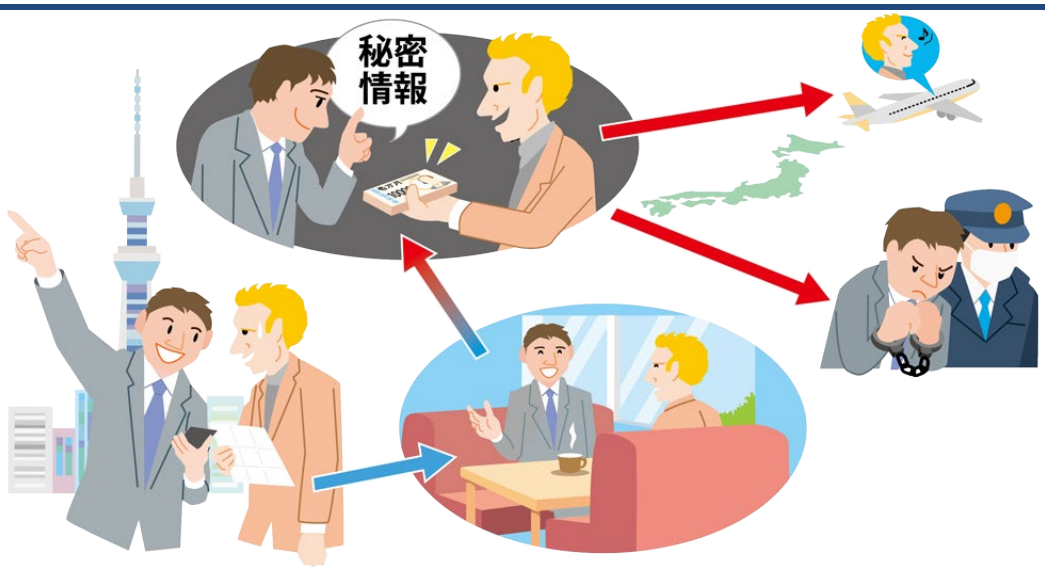
- DDoS 攻撃への対策

  「9 位　DDoS 攻撃（分散型サービス妨害攻撃）」の「対策と対応」を参照のこと。
- 被害の予防および被害に備えた対策
  - ・インシデント対応体制を整備し対応する
  - ・多要素認証（MFA）や FIDO／FIDO2（パスキーなど）を利用する
  - ・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う
  - ・Web サイト停止時のマニュアル作成、代替サーバーの用意、および告知手段の整備（SNS 等）
  - ・適切な取得日時、頻度を検討し、バックアップ運用を行う
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う
  - ・整備した対応体制に基づき対応する
  - ・Web サイトの停止、代替サーバーの稼働と告知
  - ・適切に運用されているバックアップデータからのリカバリーを行う

従業員、職員

- 被害の予防および被害に備えた対策
  - ・パスワードの適切な運用を実施する
  - ・安易に添付ファイルの開封やリンク・URL のクリックをしない
  - ・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う
  - ・組織外で開発されたプログラムは、業務端末以外の仮想環境等で開く
- 被害の早期検知
  - ・不審なログイン履歴の確認
- 被害を受けた後の対応
  - ・適切な報告／連絡／相談を行う
  - ・整備した対応体制に基づき対応する

7位 内部不正による情報漏えい等



内部不正による情報漏えいには、従業員や元従業員等、組織の内部関係者による意図的な秘密情報の持ち出しや社内情報の削除等の不正行為のほか、組織の情報管理規則に背いた情報の持ち出しや不注意で情報を紛失する等の情報漏えいになるケースも含まれる。組織の内部関係者による不正行為は、社会的信用の失墜、損害賠償による経済的損失を招く。また、不正に取得された情報を使用した組織や個人も責任を問われる場合がある。

＜脅威と影響＞

内部不正とは、組織が保有する技術情報や顧客情報といった秘密情報の持ち出し、第三者への提供、不特定多数が閲覧できる場所への公開、情報の改ざんや削除等の不正行為を指す。

職場への私怨に伴う嫌がらせや金銭の授受、転職先で有利な立場を得ることを目的に、組織の内部関係者が行うことがあるほか、在職中に組織の外部者に金銭、思想、脅迫等で勧誘、買収され、情報提供するケースも確認されている。また、多忙等の事情により、自宅等、組織外に情報を持ち出し、置き忘れ、紛失等で漏えいにつながることがある。

漏えいした情報の重要度や被害の規模によっては、組織の社会的信用の失墜、顧客等への損害賠償や損失補填、業務停滞、復旧作業等による経済的損失が発生する。その結果、業績の悪化等、経営の根幹を揺るがすおそれがある。

また、自組織に持ち込まれた情報が不正に取得されたものと知りつつ使用すると、不正競争防止法違反となり、刑事罰の対象になることもある。

＜攻撃手口＞

◆アクセス権限の悪用

付与された正当な権限を悪用し、組織の秘密情報の窃取や不正操作を行う。必要以上に高いアクセス権限が付与されていると、より重要度の高い情報にアクセスでき、より大きな被害が発生するおそれがある。また、複数人で端末やアカウントを共用している場合、誰が不正アクセスしたのか確認できない。

◆在職中に割り当てられたアカウントの悪用

離職者が、在職中に割り当てられたアカウントを用いて、外部から社内システムや業務サーバー等に不正アクセスする。離職者の利用者 ID やアクセス権を削除していないと、情報窃取や不正操作ができてしまう。

◆内部情報の不正な持ち出し

USB メモリーや HDD などの外部記録媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を使い、組織の情報を外部に不正に持ち出す。また証拠を残さないため、口頭で伝達する場合もある。

＜事例または傾向＞

◆元ロシア通商代表部員への営業秘密情報漏えい

工作機械メーカーの元社員は身分を隠した在日ロシア通商代表部の元職員に、道を尋ねられたことを機に飲食などの接待を受けていた。2024 年 11 月と 2025 年 2 月に営業秘密を口頭で伝え、対価に総額 70 万円を受領していたとされ、元社員は不正競争防止法に違反したとして書類送検された。なお、元職員はすでに帰国している[68]。

◆委託先企業の協力会社の元社員による個人情報持ち出しの疑い

2025 年 6 月、ソフトバンクの委託先である UF ジャパンから約 14 万件の顧客情報流出の可能性があると発表された。UF ジャパンの協力会社の元社員が、UF ジャパンの事業所に不正に立ち入り、USB メモリーを情報管理端末に接続している監視カメラの映像が確認されており、顧客情報を持ち出した可能性がある[69,70]。

＜対策と対応[71]＞

「秘密管理性」「有用性」「非公知性」の 3 要件を満たす対策が必要

経営者層

- **積極的な関与と対策の推進**
  - ・情報の適切な管理、法令への対応
  - ・内部不正対策推進の周知徹底
  - ・総括責任者の任命、横断的な管理体制の整備
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・セキュリティ対策のための予算確保
  - ・対策の実施策の承認
  - ・対策意識醸成のための人材教育の推進
  - ・定期的な職務の変更、職場の異動

---

68 ロシア元職員ら書類送検　メーカー機密情報漏洩疑い、スパイ活動か（日本経済新聞）
https://www.nikkei.com/article/DGXZQOUD0948B0Z00C26A1000000/

69 ソフトバンクの業務委託先で個人情報漏えいか、内部不正で約 14 万件（ZDNET Japan）
https://japan.zdnet.com/article/35234140/

70 業務委託先企業による個人情報漏えいの可能性について（ソフトバンク株式会社）
https://www.softbank.jp/corp/news/press/sbkk/2025/20250611_01/

71 組織における内部不正防止ガイドライン第 5 版（IPA）
https://www.ipa.go.jp/security/guide/hjuojm00000055l0-att/ps6vr7000000jvcb.pdf

システム管理者

- 被害の予防および被害に備えた対策

・基本方針の策定

「不正のトライアングル [72]」を意識した基本方針の策定、情報取扱ポリシーの作成、内部不正者に対する懲戒処分等を規定した就業規則等の整備 [73]。

・情報リテラシー、モラル醸成、法令遵守のための定期的な人材教育

・利用している資産の把握、管理体制の整備

情報資産を把握し、その重要度に応じて格付けした上で重要情報の管理者を定める。

・秘密情報の管理、保護

利用者 ID およびアクセス権の登録・変更・削除に関する手順を定め運用する。アクセス権は部門や職位、業務に応じた責任を明確にし、必要最小限を付与する。また、従業員の異動や離職に伴い不要になった利用者 ID 等は直ちに削除し、適切な管理、定期的な監査を行う。さらに、CASB（Cloud Access Security Broker：クラウド利用時のセキュリティソリューション）、DLP（Data Loss Prevention：情報漏えい対策）等のツールの導入、利用者 ID の共用禁止等を検討する。

・物理的管理の実施

秘密情報の格納場所や扱う執務室への入退室を管理する。USB メモリー、スマートフォン、プリンター等の利用制限、利用履歴を管理する。記録媒体の廃棄は、物理的な破壊も含め、復元不可能な方法でデータ消去する。また、リース品は初期化してから返却する。

・必要に応じ、秘密保持義務を課す誓約書に署名させる

- 被害の早期発見

・システム操作履歴の監視

秘密情報へのアクセス履歴や利用者の操作履歴等のログ、証跡の記録、監視による早期検知に努める。また、監視していることを従業員に周知することで不正を抑止する。

・特定時期の監視の強化

退職予定者の退職前後の監視を強化する。

- 被害を受けた後の対応

・適切な報告／連絡／相談を行う

・整備した対応体制に基づき対応する

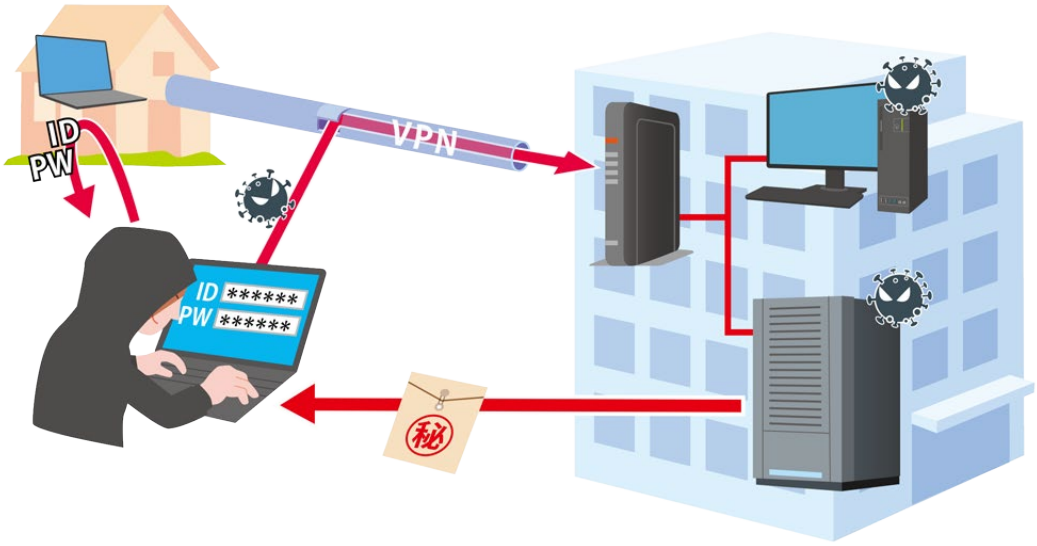
・内部不正者に対する適切な処罰の実施

---

72 IPA NEWS Vol.64(2023 年 12 月号) セキュリティのすゝめ（IPA）
https://www.ipa.go.jp/about/ipanews/ipanews202312.html

73 営業秘密管理指針（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

8位 リモートワーク等の環境や仕組みを狙った攻撃



リモートワークによる働き方が多くの組織に定着し、必要な環境や仕組みを導入した組織が増えた。これは攻撃者にとって外部からの攻撃対象領域（アタックサーフェス）が増えたことを意味する。その結果、それらを狙ったサイバー攻撃が多発している。

＜脅威と影響＞

ICT を活用した柔軟な働き方の普及により、リモートワークが定着している。そうした組織では、自宅やシェアオフィス等の外部ネットワークからVPN経由で社内システムや社内リソースへのアクセスを許可し、業務を行っている。組織はこのような業務環境を従業員へ提供している一方、攻撃者はその業務環境に攻撃を仕掛けてくる。リモートワーク用の端末や VPN 機器等が標的になりやすい。攻撃を受けると社内システムへの不正アクセスやマルウェア感染等、様々な被害が起きるおそれがある。また、業務の停止や遅延が生じ、業務の再開までの間、大きな影響を及ぼすことがある。

＜攻撃手口＞

◆リモートワーク用製品の脆弱性等の悪用

リモートワーク用に導入されている VPN 機器等に存在する脆弱性や設定ミス等を悪用し、組織内システムへ侵入し不正アクセスを行う。

◆アカウント情報の不正利用

ブルートフォース攻撃（総当たり攻撃）や何らかの方法で窃取したアカウント情報を悪用し、VPN 機器やリモートデスクトップを介して社内システムへ侵入し、不正アクセスを行う。

◆リモートワーク用端末への攻撃

私物端末（BYOD）や組織支給の端末を標的とし、マルウェア感染を目的としたメール等を送りつけ、端末をマルウェア感染させることで端末内の業務情報や認証情報等を窃取する。攻撃者はそれらの情報を悪用し、VPN 経由等で社内システムへ不正アクセスを行い、マルウェア感染や業務情報の窃取等を行う。

＜事例または傾向＞

◆リモートワーク環境を狙った攻撃の状況

ランサムウェア被害の感染経路を分類した警察庁の過去数年の統計資料[74]を見てみると、VPN 機器を経由したものが過半数を占めている。また、リモートデスクトップを経由した感染との合計値では 8 割を超えている。具体的には 2022 年 80.4%、2023 年 81.7%、2024 年 86.0%、2025 年 87.0%、と右肩上がりである。

表：ランサムウェアの感染経路の割合

感染経路	2022年	2023年	2024年	2025年
① VPN機器	61.8%	63.5%	55.0%	66.3%
② リモートデスクトップ	18.6%	18.3%	31.0%	20.7%
③ メール・添付ファイル	8.8%	5.2%	2.0%	2.2%
④ その他	10.8%	13.0%	12.0%	10.9%
合計	100.0%	100.0%	100.0%	100.0%
①＋②	**80.4%**	**81.8%**	**86.0%**	**87.0%**

出典：サイバー空間をめぐる脅威の情勢等（出典：警察庁）

＜対策と対応＞

経営者層

- 被害の予防および被害に備えた対策
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討

  リモートワーク環境ならではの状況や環境に応じた連絡方法、対応手順を策定し、社員に周知しておく必要がある。
  - ・リモートワークのセキュリティポリシーの策定
  - ・セキュリティ対策のための予算確保

セキュリティ担当者、システム管理者

- 被害の予防および被害に備えた対策
  - ・シンクライアント、VDI（Virual Desktop Infrastructure）、ZTNA（Zero Trust Network Access）/SDP（Software Deffined Perimeter）等のセキュリティに強いリモートワーク環境の採用
  - ・リモートワークの規程や運用規則の整備

    組織支給端末と私有端末の違いを考慮する。また、リモートワーク導入時の暫定的なセキュリティ対策や例外措置を見直す。
  - ・情報リテラシー、モラルを向上させる
  - ・PC やサーバー、ネットワーク機器、Web サイトに適切なセキュリティ対策を行う
  - ・サポート切れやメンテナンスが行えない機器の使用を避ける
  - ・RDP（Remote Desktop Protocol）利用時はネットワークレベル認証（NLA）を行う

74 サイバー空間をめぐる脅威の情勢等（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

・多要素認証（MFA）や FIDO／FIDO2（パスキーなど）を利用する

- 被害を受けた後の対応

・整備した対応体制に基づき対応する

従業員、職員

- 被害の予防および被害に備えた対策

・表 1.2「情報セキュリティ対策の基本」、表 1.3「情報セキュリティ対策の基本＋α」を実施

・組織のリモートワークの規則を遵守（使用する端末、ネットワーク環境、作業場所等）

・自宅のネットワーク環境はルーターを使用する

・家庭環境のネットワーク機器の設定の見直しやファームウェアの更新を行う

- 被害を受けた後の対応

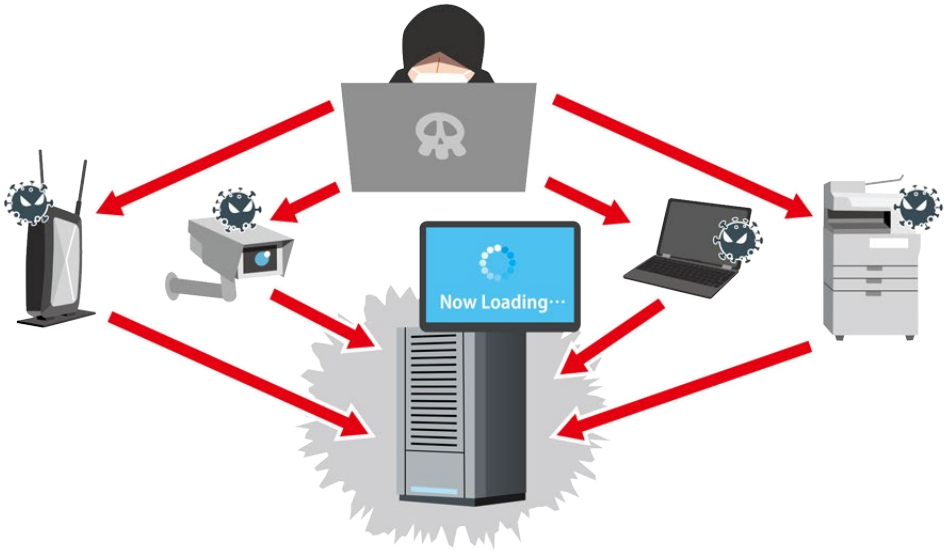
・適切な報告／連絡／相談を行う

＜リモートワーク関連サイトの紹介＞

IPA では「テレワークを行う際のセキュリティ上の注意事項」のページを公開している。このページでは、リモートワークを行う際のセキュリティ上の注意事項に加え、リモートワークから職場に戻る際のセキュリティ上の注意事項も解説している。また、IPA や他機関のリモートワーク関連セキュリティ情報へのリンクも紹介しているので、参考にしていただきたい[75]。

[75] テレワークを行う際のセキュリティ上の注意事項 （IPA）
https://www.ipa.go.jp/security/anshin/measures/telework.html

9位 DDoS 攻撃（分散型サービス妨害攻撃）



攻撃者に乗っ取られた複数の機器から構成されるネットワーク（ボットネット）から、企業や組織が提供しているインターネット上のサービスに対して大量のアクセスを一斉に仕掛けて高負荷状態にさせる、もしくは回線帯域を占有してサービスを利用不能にする等の DDoS 攻撃（分散型サービス妨害攻撃）が行われている。標的にされた組織・サービスは攻撃されると、Web サイト等の応答遅延や機能停止が発生し、サービス提供に支障が出るおそれがある。

＜脅威と影響＞

多くの組織がインターネット上の Web サイトを運営し、情報発信やサービス提供を行っている。攻撃者が処理能力を超える負荷をサーバーにかけることで、Web サイトの閲覧ができなくなる、応答が著しく遅延する等、サービス提供が正常に行えなくなる。DDoS 攻撃は組織の事業に大きな影響を及ぼすだけではなく、人々の日常生活にも支障をきたすおそれもある。攻撃者は、こうした Web サイト等に DDoS 攻撃を仕掛け、アクセスを困難にすることで主義主張の誇示や、攻撃の停止と引き換えに金銭を要求することがある。

＜攻撃手口＞

◆ボットネットを利用した DDoS 攻撃

IoT 機器等により構成されたボットネットに攻撃命令を出し、標的組織の Web サイトや利用している DNS（Domain Name System）サーバー等へ大量のアクセスを行い、高負荷をかける。

◆フラッド攻撃

通信のパケットをサーバー等へ大量に送りつけて高負荷をかける。通信に使用される TCP プロトコル・UDP プロトコルいずれにおいても攻撃手段があり、攻撃に使用するパケットの種類により、SYN フラッド攻撃、ACK フラッド攻撃、FIN フラッド攻撃等が存在する。

◆リフレクション攻撃

送信元の IP アドレスを標的組織のサーバーの IP アドレスに偽装して、多数のサーバー等に問い合わせを送り、その応答を標的組織のサーバーに集中させることで高負荷をかける。DNS サーバーを利用した DNS リフレクション攻撃や、NTP（Network Time Protocol）サーバーを利用した NTP リフレクション攻撃が存在する。

◆ランダムサブドメイン攻撃（DNS 水責め攻撃）

標的組織のドメインにランダムなサブドメインを付加して DNS へ問い合わせすることで、標的組織の DNS サーバーに高負荷をかける。DNS サーバーは悪意のある問い合わせか、通常の問い合わせかの区別が付かないため、根本対策が難しい。

◆DDoS 代行サービスの利用

専用サイト、SNS、ダークウェブ等で提供している DDoS 代行サービスを利用して攻撃する。この攻撃は専門的な技術や設備がなくても行える。

＜事例または傾向＞

◆断続的に行われた DDoS 攻撃

2025 年 6 月 26 日、ナード研究所でネットワークの不具合が発生し、メールの受信、ホームページへのアクセスができない障害が発生した。同月 30 日には問題解消のうえ復旧したことを公表した [76]が、翌月の 7 月 9 日に再度メールの送受信、ホームページへのアクセスがしづらい状況が一時的に発生した [77]。その後、障害の原因が DDoS 攻撃によるものであったこと、現時点で情報漏えいは確認されていないこと等、継続的に状況を更新し [78]、7 月 31 日にはネットワークの復旧が完了した [79]。

◆DDoS 攻撃後、早期に復旧した事例

2025 年 7 月 30 日、カゴヤ・ジャパン社は DDoS 攻撃を受けて、同社のビジネス Web メールである Active! mail とコントロールパネルにアクセスできない、またはアクセスしづらい状況が発生したことを公表した [80]。原因は、同日 16 時 30 分頃から Active! mail に対し複数の IP アドレスから大量のログイン試行が発生し、サーバーへのアクセスが集中したためとしており、これにより Active! mail のログインにも影響が生じたという。同日 17 時 45 分頃には、攻撃元の一部地域の IP アドレスからのアクセスを遮断しており、アクセスが落ち着いた後に、正常にログイン、利用できることを確認した。

＜対策と対応＞

Web サイトの運営者

- 被害の予防
  - ・インシデント対応体制の整備
  - ・サイバー保険の検討
  - ・セキュリティ対策のための予算確保
  - ・DDoS 攻撃の影響を緩和する CDN（Content Delivery Network）を利用
  - ・WAF（Web Application Firewall）、IDS（Intrusion Detection System:不正侵入検知システム）/IPS（Intrusion Prevention System:不正侵入防止システム）、DDoS 対策サービスの導入
  - ・システムの冗長化等の軽減策

---

76 ネットワーク不具合によるメール受信遅延のお詫び（ナード研究所）
https://www.nard.co.jp/info/detail.php?id=166

77 ネットワーク不具合による影響についてのお詫び（ナード研究所）
https://www.nard.co.jp/info/detail.php?id=167

78 ネットワーク不具合に関するお詫び（続報）（ナード研究所）
https://www.nard.co.jp/info/detail.php?id=171

79 ネットワーク復旧のお知らせ（ナード研究所）
https://www.nard.co.jp/info/detail.php?id=172

80 【レンタルサーバー：290322】Webメール(Active!mail) 、コントロールパネル接続障害復旧のお知らせ (7月30日18時18分更新)（カゴヤ・ジャパン）
https://www.kagoya.jp/news/2025073033092/

・ネットワークの冗長化

DDoS 攻撃の影響を受けない非常時用ネットワークを事前に準備する。

・Web サイト停止時のマニュアル作成、代替サーバーの用意、および告知手段の整備（SNS 等）

● 被害を受けた後の対応

・CSIRT への連絡

・WAF、IDS/IPS、DDoS 対策サービスの導入

・通信制御（攻撃元 IP アドレスからの通信をブロック等）

・利用者への状況の告知

・影響調査および原因の追究

サービス事業者

● 被害の予防

・インシデント対応体制の整備

・セキュリティ対策のための予算確保

・公開サーバーの設定の見直し（DNS サーバーや NTP サーバー等）

・IoT 機器の脆弱性対策

IoT 機器への不正アクセスやマルウェア感染でシステムを乗っ取られ、ボットネットとして悪用される。攻撃の踏み台にされないためにサポートの切れた IoT 機器を使わない。また、IoT 機器のセキュリティ対策を強化する[81,82,83]。

・把握されていない IT 資産の顕在化と対策

組織が把握しきれていない IT 資産へ攻撃が行われることも想定し、ASM 等で IT 資産を顕在化し、潜在リスクを把握して対策する。

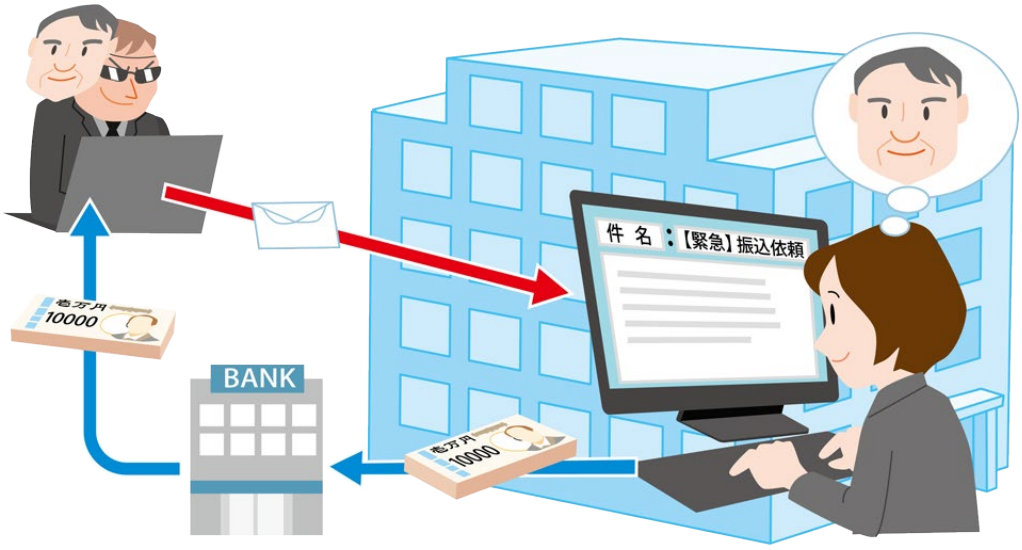
※WAF、IDS/IPS、ASM については、「PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う」を参照のこと。

81 「IoT開発におけるセキュリティ設計の手引き」を公開（IPA）
https://www.ipa.go.jp/security/iot/iotguide.html

82 経済産業省：「IoT 機器を開発する中小企業向け 製品セキュリティ対策ガイド」（経済産業省）
https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide_r6.pdf

83 DDoS 攻撃への対策について（注意喚起）（国家サイバー統括室）
https://www.cyber.go.jp/pdf/news/press/20250204_ddos.pdf

10位 ビジネスメール詐欺



悪意ある第三者が標的組織やその取引先の従業員等になりすまして虚偽のメールを送り、偽の銀行口座に金銭を振り込ませるサイバー攻撃を指す。この攻撃はビジネスメール詐欺（Business E-mail Compromise：BEC）と呼ばれる。そして、最近では生成 AI を悪用した手口が多様化しており、CEO 詐欺と呼ばれる手口等も発生しており、より一層の対策が必要である。

＜脅威と影響＞

企業の経営者や弁護士、または取引先の関係者等になりすました攻撃者が、標的組織の従業員等に虚偽のメールを送信する。メールの受信者は、送信者の立場や業務指示等の内容から虚偽と見抜けず、指示に従ってしまう。また、文面が業界の慣例や日常のやりとり等、違和感がなく巧妙で、なりすましだと見抜けないことがある。その結果、攻撃者があらかじめ用意した口座への送金指示に従い、金銭的な被害が発生する。

＜攻撃手口＞

◆BEC の準備としての情報窃取

攻撃者は BEC の準備として、標的組織の経営者や経営幹部、または人事担当者等の特定職務を担う従業員になりすまし、標的組織の従業員の個人情報を窃取する。また、マルウェア感染やフィッシング、不正ログインなどにより、個人情報を窃取することもある。窃取された個人情報の中には、従業員の氏名やメールアドレス等が含まれている。

さらに、攻撃者は取引に関わるメールのやり取りを事前に盗聴し、取引や請求に関する情報やそれらの業務に関与している関係者の情報も入手する。

◆取引先へのなりすまし

攻撃者は正規の請求書に記載された口座情報を、攻撃者が用意した虚偽の口座情報に差し替える。そして、攻撃者は取引先になりすまし、偽の請求書を標的組織の従業員にメールで送り、振り込みを促す。

◆経営者等へのなりすまし

組織の経営者等になりすまし、同組織の従業員に業務指示の体裁のメールを送る。従業員にそのメールが本物であると信じ込ませ、金銭の振り込みを促す。

◆社外の権威ある第三者へのなりすまし

弁護士等の社外の権威ある第三者になりすまし、標的組織の財務担当者等に虚偽のメールを送る（時に生成 AI 等による偽電話もある）。そのメールが本物であると従業員に信じ込ませ、振り込みを促す。

なりすましに AI によるディープフェイク等の利用も確認されている。また「緊急」や「他の従業員には秘密」と申し添えるケースがある。さらに、昨今では、簡潔なメールで LINE グループの作成と QR コードの返信を命じたり、ビジネスチャットのアカウント情報の返信を指示したりするメールの発出も確認されている。

＜事例または傾向＞

◆取引先担当者のアカウントが乗っ取られ、虚偽の支払い依頼を見抜けず、約 1,400 万円の損失

2025 年 1 月、米国を拠点とする製造委託先 A 社からの虚偽の支払依頼に子会社が応じてしまったと、モダリス社が公表した。最終的な被害額は日本円で約 1,400 万円という。虚偽のメールは A 社担当者の正規のメールアドレスから送信されていた。メールの内容、送信のタイミングも的確で、A 社担当者のアカウントを乗っ取り、一定期間 A 社担当者のメールを盗聴していたことが推測された [84]。

◆社長･役員を装う「LINE グループ作成依頼」メールによる詐欺

2025 年 12 月以降、社長や役員等になりすましたメールを従業員へ送り、LINE グループ作成を依頼する簡潔な文面のメール着信が相次いでいる。LINE ヤフーは金銭を詐取する手口であると 2026 年 1 月に注意を呼びかけた [85]。また、同様の事案が急増し、被害も発生していることから、警視庁も 2026 年 1 月に注意喚起を行い、少しでも不審に感じた場合は、周囲や警察へ相談するよう促している [86]。

＜対策と対応＞

● 被害の予防および被害に備えた対策

・インシデント対応体制の整備

・サイバー保険の検討

・セキュリティ対策のための予算確保

・表 1.2「情報セキュリティ対策の基本」を実施

・インシデント対応体制を整備し対応する

・BEC の認識・理解を深めるための教育の実施

・ガバナンスが機能する業務フローの構築

金銭支払いの業務は、複数人での審査、承認フローを構築し、単独で判断を完結させない。

・ダブルチェック

振込依頼・口座変更の依頼があった場合、普段の連絡手段以外に事前に取り決めた別ルートで確認し、絶対、電話・メール単体では受け付けない。

・社内メールに電子署名を活用した方式（S/MIME や PGP）の導入

・送信ドメイン認証の導入

自社ドメインを騙ったなりすましメールを受信できないようにする（DMARC ポリシー、SPF・DKIM 等）。

---

84 当社子会社における資金流出被害の発生と特損計上に関するお知らせ（株式会社モダリス）
http://ke.kabupro.jp/tsp/20250106/140120241227545975.pdf

85 【重要】社長・役員を装う「LINE グループ作成依頼」メールによる詐欺にご注意ください（2024 年 2 月 5 日）（LINE ヤフー株式会社）
https://help.line.me/line/smartphone?contentId=200002034&lang=ja

86 社長・上司を装ったメールが急増中（警視庁）
https://action.digipolice.jp/view/notice/301

・私有メールアドレスを業務に使用しない

・認証を適切に運用する

詐欺の準備行為への対策としてメールアカウントの認証等の設定を適切に運用する。その際、AiTM（Adversary-in-the-Middle）攻撃への対策として、FIDO／FIDO2（パスキーなど）やデバイス認証などの強固な MFA の採用も検討する。

＜メールの真正性の確認＞

・メールだけでなく複数の手段での事実確認

振込先口座の変更依頼等を受けた場合は、メール以外に電話等の方法で直接取引先に確認をする。また、金融機関にその口座の名義等を確認する。

・普段とは異なるメールに注意する

普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意する。

・判断を急がせるメールに注意

至急の対応を要求する等、担当者に真偽を判断する時間を与えないようにする手口もあり得るため、真偽を確認するフローを予め策定しておく。

● 被害を受けた後の対応

・適切な報告／連絡／相談を行う

・整備した対応体制に基づき対応する

・メールアカウントの設定を確認する

攻撃者による不正な転送設定やメール振り分けの設定等がされていないか確認する。

3.「共通対策」

脅威の種類は多岐にわたるが、対策には共通しているものもある。複数の脅威に対して有効な共通の対策があれば、効率的に対策を進めることができる。そこで、本項では表 1.4 の 7 つの対策について、「複数の脅威に有効な対策」として、注意事項、検討事項等も含めて具体的に解説する。

読者には本項を自身や自組織のセキュリティ対策を進める上での参考としてほしい。なお、共通対策を実施すれば完璧ということではない。そのため、各脅威の解説も参照し、対策を実施することが重要である。

表 1.4 複数の脅威に有効な対策

対策	対象	
	個人	組織
インシデント対応体制を整備し対応する	－	○
PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う	○	○
適切な取得日時、頻度を検討し、バックアップ運用を行う	○	○
適切な報告／連絡／相談を行う	○	○
情報リテラシー、モラルを向上させる	○	○
認証を適切に運用する	○	○
安易に添付ファイルの開封やリンク・URL のクリックをしない	○	○

インシデント対応体制を整備し対応する

セキュリティインシデントが発生した場合に備え、誰が何をどのようにすれば良いのか、あらかじめ対応する仕組みを整えておく必要がある。インシデントが起きたとしても、事前準備の有無で受ける被害の影響の大きさは全く異なる。特に、サイバー攻撃を受けた場合はより迅速な対応が必要である。そこで、本項ではセキュリティインシデント発生時の対応やそれを行うために必要なことについて解説する。自組織における対応計画作成の参考として欲しい。

- インシデント対応の事前準備

・CISO（Chief Information Security Officer）等、専門知識をもつ責任者を配置する

・CSIRT（Computer Security Incident Response Team）を構築する

一般社員がインシデント対応を兼務するのは難しい。そのため組織内の情報セキュリティ問題を専門に扱う CSIRT の構築が望ましい。ただし、CSIRT の構築が難しい場合はインシデント対応を統制する責任者と担当者を決めておき、インシデント発生時は優先して事案に対応させる。

・CSIRT を中心に有事の対応フローを確立する。

・連絡先を明記した運用手順および報告フォーマットを作成し、運用手順を社員へ周知する

・実際に運用できるか訓練し、確認する

作成した運用手順は、定期的に訓練を行い、実運用性を点検し、その結果を元に手順を見直すことも必要である。

・自組織で解決できない場合を想定して外部の協力依頼先を手配する

・これら全てを継続的に行える体制と社内の規則やポリシーの整備、予算の確保を経営者層が主体となって行う

- 組織の職員や、企業の経営者や従業員等が行うべきインシデント対応

・インシデント発生時は、表 1.5 の「報告／連絡／相談する相手」に報告等を行う。

- CSIRT が行うべきインシデント対応

① 検知／連絡受付

セキュリティ機器での検知や組織内外からの通報によりインシデントの発生を認知する。

② トリアージ

認知したインシデントについて通報者やインシデントに関係する可能性がある者とやり取りし、情報を収集することで事実確認をする。確認結果から CSIRT で対応すべきか否かを判断する。そして、判断結果を通報者や関係者に共有する。その際、インシデントが発生している対象への初動対応に合わせて、組織内への注意喚起や社内外への情報発信を速やかに行う。なお、システム対応が不必要な場合でも、注意喚起や情報発信は必要となる場合がある。

③ インシデントレスポンス

対応すべきと判断したインシデントを分析し、対応計画を策定する。組織内の関連部門だけでは対応しきれない場合は技術支援の外注も視野に入れて、経営者等の責任者と連携して計画を立てることも必要である。技術的なこと以外でも外部の専門機関や関係する組織への支援依頼や、情報提供の依頼をする。その後、策定した計画に従って対応し、問題が解決しているかを確認する。

④ 報告／情報公開

対応計画の策定や実施と並行してインシデントの通報者や関係者、監督省庁への報告を行うとともに、メディアや社会には、プレスリリース等で経緯・調査結果等を報告する。

CSIRT の構築が難しい組織であっても最低限インシデント対応を取り纏める者を定めておく必要がある。自組織では対応の準備ができているか事前に確認しておくことを推奨する[87,88,89,90,91]。

[87] サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
[88] インシデント発生時に組織内で整理しておくべき事項（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C_for_3.0.xlsx
[89] CSIRT マテリアル 運用フェーズ（JPCERT/CC）
https://www.jpcert.or.jp/csirt_material/operation_phase.html
[90] サイバーインシデント緊急対応企業一覧（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）
https://www.jnsa.org/emergency_response/
[91] デジタル・フォレンジック調査・解析対応企業紹介（デジタル・フォレンジック研究会）
https://digitalforensic.jp/df-investigator-list/

PC やサーバー、ネットワーク機器、Web サイト等に適切なセキュリティ対策を行う

組織に対する脅威は PC やサーバー、ネットワーク機器等に関連したものが多い。これらの機器には重要な情報が保存されており、企業活動における生命線である。つまり、常に攻撃者から狙われるということである。個人の PC やスマートフォンとは異なり、組織のサーバーは例えば、「更新プログラムの適用」を1つ取ってみても組織としてのポリシーの制定や要員確保、事前検証、手順の確立、さらにそれを維持し続ける予算の確保と仕組みが必要である。そして、検討事項は多く、頭を抱える組織も多いと考えられる。本項では、今後の運用の参考に、サーバーやネットワークに対するセキュリティ対策の検討事項をまとめる。

● ネットワーク管理を適切に行う

・ネットワークの分割と個別遮断を行う

ネットワークを事業所や部署、機器の用途などの単位で論理的、もしくは物理的に分割する。インシデントが発生した際は分割されたネットワークを隔離することでマルウェアに感染時の被害を局所化する。

・ファイアウォールを設置し、アクセス制御する

どこから、どのサーバーの、どのサービスにアクセスさせるかを検討し、必要最小限のアクセスだけを許可するように制御する。

・DNS フィルタリングを行う

新しく登録された未検証のドメインや不審なドメイン、悪性の類似ドメインへのアクセスを名前解決の段階で防止する。これにより悪意ある Web ページでのマルウェア感染、フィッシングサイトへの誘導、業務に関係ない Web ページへのアクセスを防げる。

・プロキシーサーバーを導入する

プロキシーサーバーは、利用者認証を受けない外部への通信をブロックすることや、各クライアントから外部への通信を上位レイヤーで詳細に記録することができる。

・ASM（Attack Surface Management）を行う

ASM とは組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのことである。組織管理者が把握していない機器や意図しない設定ミスを攻撃者視点で発見でき、脆弱性管理活動において、リスク低減の効果が期待できる[92]。

・不要なポートへの通信や不要なプロトコルの通信は遮断する

● 脆弱性対策を適切に行う

・サポート切れのソフトウェアやハードウェアを使用しない

自組織で使用している製品のサポート期限を把握しておき、サポート切れになる前に移行計画を立てて運用を検討する。

・提供元が不明のソフトウェアを利用しない

・迅速に更新プログラムを適用する

漏れなく適用するために資産管理や脆弱性情報の収集、更新プログラムの適用状況を管理する手順や体制を整備しておく。利用しているソフトウェアの管理においては SBOM(Software Bill of Materials)の導入

92 「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました（経済産業省）
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

を検討する[93]。

また、誰がどのように動作検証を行うか、構築時や保守契約時に決めておく。

・サーバーに更新プログラムを適用するには事前検証や再起動が伴う。もし、迅速に更新プログラムを適用できない場合、ネットワークレベルで攻撃の通信を遮断することで一時的に問題を解決する手法もある（この対応を仮想パッチと呼ぶ）。ただし根本的な解決方法ではなく、あくまで暫定対策であることに注意が必要である。

・不要なサービスを停止または無効化する

サーバー再起動により、停止したサービスが自動起動されないよう、自動起動が無効の設定になっていることを確認する。

● セキュリティ製品を導入する

・セキュリティソフト

セキュリティソフトとは様々なセキュリティ機能が統合されたソフトウェアである。アンチウイルスや迷惑メールのフィルタリング、Web アクセスのフィルタリングをはじめ、製品によって様々な機能を搭載している。特にアンチウイルスに関しては、最初に導入するだけでなく、定期的なスキャンやパターンファイルの更新を行うように設定し、結果を確認することが重要である。

・EDR（Endpoint Detection and Response）

サーバーおよび PC 内の処理や外部との通信等の不審な振る舞いを検知することで迅速な対応を可能にする。

・NDR（Network Detection and Response）

ネットワーク上の通信を監視、分析することで不審な通信を検知し、迅速な対応を可能にする。

・DLP（Data Loss Prevention）

特定のデータのコピー等持ち出しを検知し、ブロックする。例えば、管理対象のデータがメールに添付されている場合にアラートを出したり、ブロックしたりする。意図的な持ち出し、誤送信等、作業ミスによる漏えいの防止等も可能である。

・CSPM（Cloud Security Posture Management）

クラウドの設定ミスによる情報漏えいを防ぐ。あらかじめ自社のポリシーを元にチェックのルールを設定しておき、そのルールに抵触する設定がなされた場合にアラートを出すことで設定ミスに気が付けるようにする。なお、CSPM が IaaS, PaaS の設定の監査を行うのに対して、SaaS については、SSPM（SaaS Security Posture Management）により監査が可能である。

・SSPM（SaaS Security Posture Management）

SaaS のセキュリティ設定のミス、アカウント管理の不備、不審なアクセスの有無等を監視し、これらを検知すると管理者へアラートを通知する。

・DSPM（Data Security Posture Management）

オンプレミス環境とクラウド環境を含む組織全体に存在するデータを保護するための、データ検出、データ分類、リスク評価、リスク対策を行う。

・IDS（Intrusion Detection System）

不正侵入検知システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった際に担当者へ通知を

[93] サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました（経済産業省）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

行う。自動でブロックする機能はないが、通知を受けることで、担当者が内容を確認し対応に着手する契機となる。

・IPS（Intrusion Prevention System）

不正侵入防止システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった場合は担当者への通知だけでなく自動でブロックも行う。IDS よりリスクの低減はできるが正規の通信をブロックしてしまうおそれもあり、組織の方針を踏まえた上での選定が必要である。

・DNS フィルタリング

新しく登録された未検証のドメインや不審なドメイン、悪性の類似ドメインへのアクセスを名前解決の段階で防止する。

・WAF（Web Application Firewall）

Web サーバーの前段または Web サーバー内に設置することで通信を監視し、Web サイトを保護する。IDS、IPS がネットワークレベルでの監視を行うのに対して WAF はアプリケーションレベルで監視する。組み合わせて適用することでより強固な防御が可能になる。

・UTM（Unified Threat Management）

統合脅威管理と呼び、IDS や IPS の機能やファイアウォール、アンチウイルス等、他の機能も備えた製品である。1 つに統合されていることで運用コストや手間の低減が期待できる。

・SIEM（Security Information and Event Management）

アンチウイルスや EDR 等から出力されるログやイベント情報を一か所に集約し、相関関係を踏まえた分析を可能にする。情報を統合的に可視化することで、インシデントの調査を効率化でき、運用コストや手間の低減が期待できる。

● アクセス権限管理を適切に行う

・アクセス権限を最小化する

むやみにアカウントを作成せず、作成したアカウントに過剰な管理者権限や更新権限を与えない。

・管理者権限の運用体制を整える

内部不正防止のため、運用作業手順や作業記録方法等を整理する。システムによる制御だけでなく、ルールの策定などによる運用面での仕組みづくりも重要である。例えば、担当者の任命、作業理由の記載、クロスチェック等を遵守事項として定めることは、不正リスクへの対策として有効である。

・定期的にアカウントの棚卸を行う

従業員や職員の離任時に対象者のアカウントを削除し、その上で定期的に棚卸を行うことで、権限付与の妥当性や、不要なアカウントの存在を確認等も行う。

・同一のアカウントを複数人で共用しない

・アクセスログを収集し監視する

インシデント発生時には過去に遡って調査できるよう、保存期間やログファイルの運用方法も組織の方針に併せて検討する必要がある。

・認証を適切に運用する（詳細は「認証を適切に運用する」を参照のこと。）

・多要素認証（MFA）の設定を有効にする

利用している機器が多要素認証（MFA）に対応している場合は設定を有効にしておく。

● その他

・セキュリティのサポートが充実している製品を使う

製品パッチや回避策の提供が迅速な製品・サービスを導入・使用する。

・統合運用管理ツールを導入する

統合運用管理ツールとは社内ネットワーク機器やサーバー等の IT 機器を一元管理するツールである。様々な管理項目があり、セキュリティ管理機能ではシステムへのアクセス権限の管理やファイアウォールの設定、暗号化が可能である。他にも様々な機能があるため、導入により、セキュリティ対策以外にも、大きなメリットを期待できる。

・重要データやファイルを暗号化する

・外部記憶媒体の接続を制限する

・脆弱性診断を行う

セキュリティベンダーから提供されている診断サービスはサーバーやネットワーク全体を診断でき、適切な助言を受けられるため実施を検討する。

・ペネトレーションテストを行う

実際の攻撃シミュレーションを通じてセキュリティ体制の実効性を評価する。

・ログを取得し、監視や解析をする

システムログ、アプリケーションログ、サーバーへのアクセスログ、認証ログ、データベース操作ログ、通信ログ等の各種ログを取得し、監視や解析をすることで不審な振る舞いの迅速な検知だけでなく被害に遭った際の原因特定が可能になる。

また、ログの取得は、ログレベルや保管期間について事前に検討が必要である。特に、運用を外注するのであればログの取得や監視、解析に関する仕様や運用の確認を行う。

IPA では Web サーバーや SSH、FTP サーバーのログを解析することで攻撃と思われる痕跡を検出するためのツール（iLogScanner[94]）を無料で提供しているので利用を検討する。

・サイバーセキュリティお助け隊サービス

中小企業に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージにまとめた、民間の事業者から提供されるサービスである。これを活用し安価にセキュリティ対策を行う[95]。

94 ウェブサイトの攻撃兆候検出ツール iLogScanner（IPA）
https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

95 サイバーセキュリティお助け隊サービス（IPA）
https://www.ipa.go.jp/security/otasuketai-pr/index.html

適切な取得日時、頻度を検討し、バックアップ運用を行う

データの破損の原因は記憶装置の故障やランサムウェア等のサイバー攻撃だけではなく、運用時の操作ミスによる消去や誤った更新と多岐に渡る。失ったデータの復旧は困難であり、復旧には人手と時間を要する。しかし、バックアップを取得しておくことでこの被害を軽減することが可能である。迅速にデータを復旧し業務継続できなければ、組織の信頼も失墜し、組織存続の問題に繋がりかねない大きなリスクとなる。そこで本項では適切なバックアップ運用について解説するので今後の運用の参考にしてほしい。

● リストアまでを含めたバックアップ設計を行う

・システムおけるリストアをシステム間の矛盾なく行えるように設計する

バックアップは取得するだけで終わりではなく、それを利用していかに早く復旧させるかが重要である。そのために想定される障害とその被害をあらかじめ考え、それぞれに対して復旧する時点やリストア手順を確立する。

● バックアップを取得する

・サーバーの要件に合わせた手法を選定する

サーバーの稼働要件や復旧要件に合わせ、次のような手法から適切な手法や組み合わせを検討する。

オフラインバックアップ：サーバーを停止してフルバックアップを取得する

オンラインバックアップ：サーバーを起動した状態でデータベース等のデータをコピーする

・対象の選定

業務データだけでなく、システムの稼働に必要な設定ファイルやプログラムも含め、バックアップ対象を選定する。

・頻度の検討

対象のデータ毎に適切な取得日時、頻度を検討する。例えば、業務データは週に1回フルバックアップし、その他の日に差分バックアップをする。プログラムファイルはシステム改修が無い限り変更はないので、リリース時にのみバックアップをする。設定ファイルは随時変更があるため、週に1回取得する等のようにタイミング、頻度を検討する。

● バックアップを保管する

・保管場所を検討する

ランサム攻撃に備えて、ネットワークから隔離した場所へ保管する。外部記憶装置に保管し、バックアップ取得時やリストア時を除いてネットワークから切り離しておく。さらに、地政学的リスクや災害対策も含める場合、地理的に離れた異なる場所での保管や、分散して保管することを強く推奨する。

・3-2-1 ルール [96]

データはコピーして 2 つ持ち（稼働システムと合わせて計 3 つのデータを保持）、それらのコピーは 2 種類のメディアでバックアップを保管し、そのうち 1 つは稼働システムとは異なる、別拠点等で保存する。

また、3-2-1 ルールを拡張した 3-2-1-1-0 ルールもある。これは、3-2-1 ルールに加えて、不変（immutable）またはオフラインコピーを1つ追加し、定期的な検証でエラーゼロを維持するものである。

・WORM（Write Once Read Many）機能の利用

96 Data Backup Options（サイバーセキュリティ・インフラストラクチャセキュリティ庁）
https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf

WORM は、一度書き込んだデータの変更や削除をできなくし、読み取りは何でもできるという機能である。WORM 機能が搭載されたストレージを利用することにより、データ改ざんやデータ消失を防げる。

・世代管理を行う

最新のバックアップだけでなく、過去のバックアップも保管し、いつ時点のどのデータが含まれているのか、ファイルの名称や保管している外部記憶装置を判別できるようにしておき、複数時点に復旧できるようにしておくことが望ましい。データの破損からそれを認知するまでに時間がかかると最新のバックアップもすでに破損しているおそれがあるためである。

また、ランサム攻撃を受けた際、破損したデータで上書きしないよう、バックアップ取得や削除処理を止める必要がある。誤って上書きしたり、消去したりしてしまわぬよう、それらを扱う際の運用手順を定めておく。

・保管期間を決める

バックアップの保管方法や世代管理と合わせて組織の方針を満たせる保管期間を決定する。

● バックアップからリストアする

・正しく復旧できることを確認する

初回のバックアップ時に正常に復旧ができることを確認し、さらに、計画に基づいて正しく復旧できるか定期的に確認し、必要に応じた手順の見直しを行う。また、システム導入時ならびに大規模な更改時は、リストア実施のテストを実施することが望ましい。

適切な報告／連絡／相談を行う

組織において上司や責任者、経営者層に適時・適切に報告をしないと被害拡大につながるだけでなく、外部から隠蔽を疑われ、さらなる信頼の失墜につながるおそれもある。そうならないためにあらかじめ対応マニュアルを作成し、エスカレーション先を定め、インシデント発生時にはマニュアルに従い報告等を行う。また、場合によっては組織外への情報発信も必要である[97]。これら一連のエスカレーションを迅速に行うため、組織に所属する全員がインシデント発生時の対応を十分に理解し、訓練しておく必要がある。また、経営者や上司、責任者は部下や担当者が包み隠さず、躊躇なくエスカレーションできる環境や良好な関係の構築も重要である。

対応マニュアルの作成においては、連絡先の例を以下に列挙するので参考にして欲しい。

表 1.5 報告／連絡／相談先の例

組織内の立場	報告／連絡／相談する相手
従業員、職員	些細なことから重大インシデントを発見できる可能性がある。また、自身がインシデントを起こしてしまった場合、適時・適切にエスカレーションをしないと隠蔽を疑われ、責任を問われるおそれがある。 そのため、躊躇せずにエスカレーションすることが重要である。 ①上司や責任者、セキュリティの管理者にエスカレーションする ※自身がインシデントを起こした、発見した場合 ②システム管理者にエスカレーションする ※自身が利用している PC やスマートフォン、システムに関するインシデントの場合 ③CSIRT にエスカレーションする ※組織内で CSIRT が構築されている場合
上司や責任者	報告を受け、対応を判断する必要もある。日頃から関係者を把握しておくことや対応手順を理解し、組織内の関連部署へ横展開する。
経営者層や組織として	組織として、自組織や関係者の被害拡大防止、社会的責任を果たすために、外部へ報告、相談、公表する必要がある。場合によって、被害拡大防止や原因と対応の報告等を 1 次、2 次と報告を段階に分けて適切に行うことが重要である。 ①セキュリティの専門会社に技術支援依頼をする（契約がなくても、スポットで緊急対応してくれるサービスもある） ※自組織だけでは調査や解決できない場合 サイバーインシデント緊急対応企業一覧（JNSA） （https://www.jnsa.org/emergency_response/） ②顧客、取引先、委託先、委託元、関連組織に報告する ※場合によってはメディアへの公表を検討する ③金融機関、クレジットカード会社へ連絡する ※情報漏えい等によるさらなる被害拡大防止 ④監督省庁、IPA、JPCERT/CC に報告する ※発生したインシデントに併せて公的機関等に報告する 企業組織向けサイバーセキュリティ相談窓口 （https://www.ipa.go.jp/security/support/soudan.html） コンピュータウイルス・不正アクセスに関する届出 （https://www.ipa.go.jp/security/todokede/crack-virus/about.html） JPCERT/CC インシデント対応依頼 （https://www.jpcert.or.jp/form/）

97 JPCERT/CCがとりまとめた「サイバー攻撃被害情報の共有と公表のあり方」に係る調査報告書の公表（JPCERT/CC）
https://www.jpcert.or.jp/tips/2021/wr213201.html

	⑤個人情報保護委員会に報告する 個人データの漏えい等が発生し、個人の権利、利益を害するおそれがある場合は、個人情報保護委員会への報告が法律上の義務である（個人情報保護法第 26 条）。速報は事態の発覚後おおむね 3～5 日以内、確報は 30 日以内（不正アクセス等の場合は 60 日以内）に行う必要がある。 ⑥警察に相談する ⑦弁護士に相談する また、組織内で報告を躊躇するような一律的で過剰な懲罰等を設定せず、積極的に報告が上がる環境、施策づくりが求められる。

情報リテラシー、モラルを向上させる

意図せず情報モラル [98]に反する行為をする人や、故意に不正行為をする人がいる。組織においては業務多忙や、緊急対応等、時間的制約の中、精神的に追い込まれ、規則に反してしまうこともあると考えられる。悪意の有無に関わらず規則に反する行為には責任が伴う。特に、組織においては例え従業員の身勝手な行動であったとしても組織への影響や責任が問われることは少なくない。本項を読み、個人として、また組織としてどのように対処すべきか参考にしてほしい。

● 家族や組織（経営者や従業員、職員）を教育する

情報リテラシーの向上が必要な人は気を付けるべきことに自身で気付けないことが多い。個人であれば、これから PC やスマートフォンを使う子 [99]、使い慣れていない親に対し、組織であれば従業員への教育を行う。教育内容は教育対象により異なるため、以下に例を記載する。

【個人、組織共通】

① SNS の利用

・掲載されている情報が正しいとは限らない

悪意の有無に関わらず、誤った情報が掲載されているおそれもあり、情報を鵜呑みにしない。

・安易に情報を拡散しない

情報を安易に拡散してしまうと名誉毀損で訴追されることや損害賠償を請求されることがある。特に SNS では簡単に情報を見つけ、拡散できるが、意図せずデマの拡散や誹謗・中傷に加担してしまうおそれもある。情報を拡散する場合は一次情報にあたり、発信者や発信内容のファクトチェック等も行う必要がある [100]。

・情報発信は慎重に行う

真偽を判断できない情報や他人を攻撃するような発言・発信は控える。情報拡散と同様に情報が正しいか、確認した上で発信する。

一度インターネット上に発信した内容は完全に消去することは難しい。（デジタルタトゥーと呼ばれている）そのため、感情のままに発信せず、一旦時間をおいて落ち着いてから発信する。

② インターネットの利用

次のような Web サイトが存在することを認識し、表示されている内容をうのみにせず、安易な入力を避ける。

・正規の企業やサービスを騙った偽の Web サイトがある

・偽セキュリティ警告画面を出した上で、偽のサポート（サポート詐欺）に誘導する Web サイトがある

・個人情報を盗もうとする Web サイトがある

特に個人情報や金銭に関する情報の入力を求められたときには注意が必要である。

③ 生成 AI の利用

・学習機能の有無を確認する

利用時に学習機能の有無を確認し、個人情報等の機微情報の入力は避ける

・生成・掲載されている情報が正しいとは限らない

悪意の有無に関わらず、誤った情報が生成・掲載されているおそれもあり、情報を鵜呑みにしない。

---

98 第5章 情報モラル教育（文部科学省）
https://www.mext.go.jp/b_menu/shingi/chousa/shotou/056/shiryo/attach/1249674.htm

99 情報セキュリティ関連サイト（IPA）
https://www.ipa.go.jp/security/guide/keihatsu.html

100 ファクトチェックとは（認定NPO法人 ファクトチェック・イニシアティブ）
https://fij.info/introduction

【組織での対応】

① 情報セキュリティ・情報モラル

・定期的な教育を継続し、底上げを図る

② コンプライアンス

・内部不正に対する懲戒処分やそれを規定した就業規則に関する周知を行う

教育のコンテンツに何を取り入れるかは業務により異なるが、IPA から発信しているコンテンツを紹介するので参考にすることを推奨する[101,102]。

● 教育プログラムへの意識付け

・他人事と考えず、受講する

・就業規則、社内運用規則を理解する

・緊急時の報告先、報告方法を把握すること

● 継続的に取り組む

・定期的かつ、適時な教育プログラムの実施

組織における教育では、人の入れ替わり（新入社員、中途社員、派遣、出向等）やイベント（長期休暇、社会情勢等）を考慮し、教育プログラムを実施することも有効である。そのうえで、毎回同じ教育コンテンツではなく、定期的に従業員の行動やポリシーを評価し、コンテンツを見直す。

101 サイバーセキュリティのひみつ（IPA）
https://www.ipa.go.jp/security/security-himitsu/index.html
102 対策のしおり（IPA）
https://www.ipa.go.jp/security/guide/shiori.html

認証を適切に運用する

ネットショッピングや SNS の利用等、様々な場面でパスワードの設定が求められる。推測可能なパスワードの設定やパスワードの使い回し等の不適切な管理をすると、攻撃者に不正ログインをされるおそれがある。そうならないために本項を読み、適切な対策を実施し、リスク低減に努めてほしい。また、最近ではパスワード認証以外の認証方式の利用も推奨されてきているので、それらについても紹介する。

● 適切な設定をする [103]

・初期設定のままにしない

ネットワークカメラ等の IoT 機器は出荷の際に共通したパスワードが初期設定されており、それが周知されている場合もある。その場合、初期設定が悪用される危険性が高くなるため、必ず変更する。

・推測されにくいパスワードを設定する [104]

パスワードを推測されにくくするためには、文字数を多くすることが有効である。国家サイバー統括室（NCO）が発行している「インターネットの安全・安心ハンドブック」[105]でも、「最近では、桁数をできるだけ長くする方が安全である」としている。パスワード作成時は特に以下に留意する必要がある。

① ID とパスワードを同じ文字列にしない
② 数字、アルファベット、記号等の複数の文字種を組み合わせる
③ 生年月日や名前を使わない
④ 連続した数字やアルファベットにしない
⑤ 単純な単語一語だけにしない

表 1.6 悪いパスワードの例

パスワード	悪い点
123456	連続した数字
Password p@ssw0rd	単純な単語やその類似系
taro1202	名前や誕生日
1qaz2wsx	キーボードの縦配列
Qwerty	キーボードの横配列

・パスワードを使い回さない

個人情報や金銭情報を登録しているサービスや、登録したメールアドレスを ID として利用するサービスでは、特にパスワードの使い回しを避けるべきである。複数のサービスで同じパスワードを利用していると、いずれかのサービスでパスワードの漏えいが起きた時に、使いまわしている全てのサービスが不正ログインされるおそれがある。また、IPA では使い回しを避けるためのパスワード作成方法を紹介しているので参考にしてほしい [106]。

● 適切な保管、運用を行う

・パスワードは他人に教えない

・PC やスマートフォンにパスワードを書いた付箋等のメモを貼らない

---

103 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/account_security.html
104 チョコっとプラスパスワード（IPA）
https://www.ipa.go.jp/security/chocotto/index.html
105 インターネットの安全・安心ハンドブック（国家サイバー統括室：NCO）
https://security-portal.cyber.go.jp/guidance/handbook.html
106 安心相談窓口だより「不正ログイン被害の原因となるパスワードの使い回しはNG」（IPA）
https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

目を離した隙に不正ログインされてしまうリスクがある。また、PC やスマートフォンを紛失した際に簡単に不正ログインされてしまう。覚えきれない場合は自宅で保管するノート等、オフラインの媒体への記録や、OS やブラウザのパスワード管理機能の利用、パスワードマネージャー（パスワード管理ソフト）の利用を推奨する。

・PC やスマートフォン内のファイルにパスワードを記載しない

・複数人で使用する PC ではブラウザにパスワードを記憶させない

便利な機能だが複数人で利用している PC では、本人以外の人が本人になりすましてログインできてしまうので注意が必要である。

・メールによるログイン通知の設定をする

・漏えい・侵害が確認された場合は、速やかにパスワードを変更する

・パスワードの漏えいをチェックするサイト[107]等で自身のパスワードが漏えいしていないかを確認する

● 不正ログインされてしまったときの対応

・パスワードを変更する

以後の不正ログインを防ぐために、早急にパスワードを変更する。

・パスワードを使い回していないか確認する

他のサービスでパスワードを使い回している場合、合わせてパスワードを変更する。

・「適切な報告／連絡／相談を行う」に書かれた連絡先に連絡をする

● パスワード認証以外の認証方式の利用

・多要素認証（MFA）を利用する

多要素認証（MFA）とは、認証の 3 要素である「知識情報」、「所持情報」、「生体情報」のうち、2 つ以上を組み合わせて認証することを指す。可能な場合は「知識情報」であるパスワードだけではなく、スマートフォンに届いた SMS を介した番号入力などの「所持情報」や指紋認証などの「生体情報」等も加えた多要素認証（MFA）を利用することを推奨する。例えば、Web サイトにログインする際にパスワード認証を行い、その後、スマホの認証アプリを使いワンタイムパスワードを入力する等の多要素認証（MFA）を行う。

・FIDO／FIDO2（パスキーなど）を利用する

生体情報のみで認証を行うことや PIN コードのみで認証を行う等、パスワードを利用しない認証方式であるパスキーが提供されていれば利用することを推奨する。パスキーを使用するデバイスは生体情報や PIN コードのみで起動ができるため、パスワードレスでのシステム利用が可能となる。

[107] Have I Been Pwned?（HaveIBeenPwned.com）
https://haveibeenpwned.com/

安易に添付ファイルの開封やリンク・URL のクリックをしない

様々なサービスからメールや SMS でお知らせが届くが、正当な機関や取引先を装って虚偽のメールが送られてくるおそれがある。虚偽の場合、不用意に返信するとそれを起点に個人情報が詐取されたり、金銭被害に繋がったりするおそれがあるので、不審な点が少しでもあれば注意して取り扱う。また、ランサム攻撃や標的型攻撃等において、一連の攻撃の端緒としてマルウェアの添付や不正なリンク先が記載されたメールが送りつけられることがある。手口が高妙化しており、真偽の見極めが困難になっている。

● 被害に遭うタイミング

悪意があるメール、SMS を受信して、内容を閲覧した時点ではまだ情報を盗まれたり、PC やスマートフォンがマルウェアに感染したりする可能性は低い。そのメール・SMS から誘導された Web サイトで情報を入力するとその情報が攻撃側に渡る。また、添付ファイルを開くことでマルウェアに感染してしまうことがある。

PC やスマートフォンは、マルウェアに感染すると正常に動作しなくなったり、保存しているデータが攻撃者に送付されてしまったりする。

さらにクレジットカードや銀行口座の情報が盗まれると、悪用され金銭被害につながる。

● メール・SMS、SNS に関する注意事項

・安易にリンクや QR コードを開かない

メールの添付ファイルの開封や、メール・SMS のリンク、SNS のチャットの URL を安易にクリック、タップしない。もしアクセス先が少しでも不審だと感じた場合、直ちに利用を停止し、個人情報やクレジットカード情報を安易に入力しないようにする。メール本文に記載されている URL もブラウザに安易に入力して開かない。

・もし、クリック・開封してしまった場合は適切な方法で報告する（「共通対策：適切な報告／連絡／相談を行う」を参照のこと。）

・記載された電話番号に電話をかけない

悪意あるメール・SMS に記載された電話番号は偽のサポート窓口等につながるおそれがあり、虚偽の案内をされ、個人情報等を聞き出されてしまうおそれがある。

・リンクを開いてしまった場合は、表 1.5 の「報告／連絡／相談する相手」に報告する。

● メールや SMS 固有の注意事項

メールや SMS に記載されたショッピングサイトやサービス等をそもそも、自分が利用しているかを確認する

・HTML 形式ではなくテキスト形式で表示する設定にする

（同様にテキスト形式で送信することで受信者に安心を与えられるという側面もある）

・画像のクリックやタップをしない

一見ただの画像であってもリンクが設定されており、偽の Web サイトが開くおそれがあるので、安易にクリックやタップをしない。

・添付ファイルを開かない

添付ファイルを開くと悪意あるプログラムが起動し、マルウェアに感染するおそれがある。Microsoft Word や Excel を開いてしまった際に「マクロを有効にする」、「コンテンツの有効化」というボタンが表示されることがある。このボタンをクリックすると悪意あるプログラムが起動することがある。さらに、「信頼できる場所」に指定された特定のフォルダでファイルを開くと、上記のボタンは表示されず、マクロを実行してしまう問題もあ

る [108]。そのため、業務でマクロ機能を使用しない場合は、マクロを無効化しておくべきである。他にも、ファイルを開くと「編集を有効にする」というボタンが表示されることがある。ファイルの安全性が確認できない場合、安易にボタンをクリックやタップしないようにする。

● リンクや URL をクリックせずに確認する方法

不審なメール・SMS の案内は以下のような、リンクや URL をクリックさせる文面が多い。

「〇〇については下記よりご確認ください。」

「詳細はコチラ」

クリックやタップをしてはいけないとはいえ内容が気になり、確認したいと思うことがある。その場合はメール内のリンクは使用せず、次のようにして正規の情報を確認することを推奨する。

① メールの送信元の情報や電話番号を Web 検索し、フィッシング等悪用の有無を確認する
② よく利用する Web サイトは事前にブックマーク（お気に入り）に登録し、ブックマークからアクセスする
③ よく利用するサービスはあらかじめ正規のアプリをインストールし、そのアプリを利用する
④ ②、③の対処ができない普段利用しないサービスは、対象の Web サイトを検索して開いて確認する
この場合、検索結果の上部にある広告は偽のサイトの場合があるので、それらをクリックしないように注意する。不在通知や購入履歴を示す内容であれば、正規の Web サイトやアプリから確認する。

IPA の Web ページでは攻撃手口を紹介しているので、これを確認し、不審なメール・SMS に備えることを推奨する [109]。

108 Emotet（エモテット）攻撃の手口（IPA）
https://www.ipa.go.jp/security/emotet/attack.html
109 安心相談窓口だより「URLリンクへのアクセスに注意」（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

4. 10 大脅威選考会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	田口 裕介	NTT ドコモビジネス(株)
神山 太朗	あいおいニッセイ同和損害保険(株)	戸畑 洋介	NTT ドコモビジネス(株)
橋田 幸浩	あいおいニッセイ同和損害保険(株)	皆川 諒	NTT ドコモビジネス(株)
宮﨑 清隆	ICMS(株)	杉野 明宏	NTT 社会情報研究所
上前田 浩章	(株)アクセルスペースホールディングス	大石 眞央	(株)NTT データグループ
中嶋 美貴	アクセンチュア(株)	大嶋 真一	(株)NTT データグループ
大泉 久	AKKODiS コンサルティング(株)	植草 祐則	(株)NTT データ先端技術
石井 彰	旭化成(株)	佐藤 功視	(株)NTT データ先端技術
高橋 広	旭有機材(株)	藤原 稔也	(株)NTT データ先端技術
真藤 直観	(株)アシュアード	齊藤 純一郎	NTT 東日本(株)
鈴木 康弘	(株)アシュアード	杉井 俊也	NTT 東日本(株)
早崎 敏寛	(株)アシュアード	平本 陽介	NTT 東日本(株)
中山 貴禎	(株)アズジェント	井上 茂	NTT ビジネスソリューションズ(株)
岡田 良太郎	(株)アスタリスク・リサーチ	中西 克彦	(株)FFRI セキュリティ
篠﨑 雄一郎	伊藤忠テクノソリューションズ(株)	前田 典彦	(株)FFRI セキュリティ
筒井 秀徳	伊藤忠テクノソリューションズ(株)	梶浦 勉	MS&AD インターリスク総研(株)
森田 拓哉	伊藤忠テクノソリューションズ(株)	田中 響	MS&AD インターリスク総研(株)
瀧川 裕史	(株)イルグルム	松森 純	MS&AD インターリスク総研(株)
岡田 琢央	Infoblox(株)	西城 秀行	MS&AD システムズ(株)
才藤 丈己	ウイングアーク1st(株)	福地 有紀	MS&AD システムズ(株)
橋本 賢一郎	ULTRA RED, Ltd.	田野 真也	エムオーテックス(株)
大桶 夏津	(株)エーアイセキュリティラボ	前田 征大	エムオーテックス(株)
関根 鉄平	(株)エーアイセキュリティラボ	松井 将吾	エムオーテックス(株)
岸上 健吾	(株)エーピーコミュニケーションズ	池田 耕作	(株)オージス総研
柳田 大心	(株)エーピーコミュニケーションズ	姫野 猛	(株)オージス総研
山根 康裕	(株)エーピーコミュニケーションズ	藪下 孝一	(株)オージス総研
斎藤 泰輔	au フィナンシャルホールディングス(株)	岡村 耕二	九州大学
溝口 英利	(株)AIT	加藤 浩治	京セラ(株)
鈴木 祥一	SAK University	手島 康太	京セラ(株)
	東京イノベーションキャンパス	福山 諒	京セラ(株)
野口 敏宏	SMBC コンシューマーファイナンス(株)	金井 智哉	京セラコミュニケーションシステム(株)
佐藤 直之	SCSK セキュリティ(株)	北 章希	京セラコミュニケーションシステム(株)
鈴木 寛明	SCSK セキュリティ(株)	西山 健太	京セラコミュニケーションシステム(株)
中井 俊晃	SCSK セキュリティ(株)	大脇 旭洋	キンドリルジャパン(株)
辻 伸弘	SB テクノロジー(株) （2026 年 3 月時点）	小林 勝	キンドリルジャパン(株)
笠井 靖記	NEC ネクサソリューションズ(株)	宮内 雄太	(一社)金融 ISAC
生方 秀則	(株)エヌ・ティ・ティ エムイー	古澤 一憲	グーグル・クラウド・ジャパン(同)
鈴木 雅斗	(株)エヌ・ティ・ティ エムイー	清水 将人	(一財)草の根サイバーセキュリティ推進協議会(Grafsec)
髙橋 昌士	(株)エヌ・ティ・ティ エムイー	山田 宜史	(株)クリーチャーズ
大島 悠司	NRI セキュアテクノロジーズ(株)	笹倉 真喜子	グローバルセキュリティエキスパート(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	鈴木 貴志	グローバルセキュリティエキスパート(株)
奥村 哲平	NRI セキュアテクノロジーズ(株)	田中 悠	グローバルセキュリティエキスパート(株)
北河 拓士	NTT セキュリティ・ジャパン(株)	斎数 真人	(株)クロスポイントソリューション
斯波 彰	NTT セキュリティ・ジャパン(株)	小熊 慶一郎	KBIZ /ISC2
杉山 毅	NTT セキュリティ・ジャパン(株)	保村 啓太	KPMG コンサルティング(株)

氏名	所属	氏名	所属
遠藤 誠	(株)ケイテック	松本 隆	(株)ディー・エヌ・エー
根古谷 聡一	(株)京葉銀行	吉村 修	デロイト トーマツ サイバー(同)
坂 明	(公財)公共政策調査会	駒澤 悠二	(株)電算
北田 高之	(株)神戸デジタル・ラボ	河合 翔平	東京海上日動あんしん生命保険(株)
松田 康司	(株)神戸デジタル・ラボ	花田 隆仁	東京海上日動火災保険(株)
持田 啓司	サイバーセキュリティイニシアティブジャパン	猪狩 大祐	東京海上日動システムズ(株)
松本 純	サイボウズ(株)	石山 圭佑	東京海上日動システムズ(株)
宮内 伸崇	(株)サイント	中西 祐介	東京海上日動システムズ(株)
熊坂 駿吾	GMO サイバーセキュリティ by イエラエ(株)	石川 朝久	東京海上ホールディングス(株)
飯山 志保	(株)JR東日本情報システム	嶋谷 巧	東京海上ホールディングス(株)
大賀 麻衣子	(株)JR東日本情報システム	富山 寛之	東京海上ホールディングス(株)
佐藤 勤子	(株)JR東日本情報システム	佐々木 良一	東京電機大学
椎野 紘平	(株)JTB	小島 健司	(株)東芝
利光 剛	(株)JTB	大浪 大介	東芝インフォメーションシステムズ(株)
桑原 俊	(一社)JPCERT コーディネーションセンター	山田 幸奈	トランスコスモス(株)
齋藤 美香	(一社)JPCERT コーディネーションセンター	綿口 吉郎	トランスコスモス(株)
矢野 雄紀	(一社)JPCERT コーディネーションセンター	山室 太平	Trellix
唐沢 勇輔	Japan Digital Design(株)	岡本 勝之	トレンドマイクロ(株)
加藤 雅彦	順天堂大学	林 憲明	トレンドマイクロ(株)
大久保 隆夫	情報セキュリティ大学院大学	今成 勇人	(株)ナレッジワーク
伊東 寛	(国研)情報通信研究機構（NICT)	須川 賢洋	新潟大学
内山 巧	信州大学	北條 孝佳	西村あさひ法律事務所・外国法共同事業
竹林 和賢	スターネット(株)	堀江 昌宏	ニッセイ・ウェルス生命保険(株)
山本 幸稔	スターネット(株)	菅 賢太郎	日本アイ・ビー・エム(株)
正木 義和	スワットブレインズ(株)	窪田 豪史	日本アイ・ビー・エム(株)
東 恵寿	NPO セカンドワーク協会	柳 優	日本アイ・ビー・エム(株)
金城 夏樹	(株)セキュアイノベーション	髙﨑 庸一	(一社)日本サイバーセキュリティ人材キャリア支援協会
鉢嶺 光	(株)セキュアイノベーション	青木 聡	日本電気(株)
服部 祐一	(株)セキュアサイクル	谷川 哲司	日本電気(株)
阿部 実洋	(株)セキュアベース	斉藤 健一	(一社)日本ハッカー協会
上村 理	ゼットスケーラー(株)	宮本 久仁男	(一社)日本ハッカー協会
古澤 大樹	(株)セブン&アイ・ホールディングス	中西 基裕	日本プルーフポイント(株)
勝海 直人	(株)ソニー・インタラクティブエンタテインメント	松山 保	(株)ヌーラボ
佐久間 義明	ソニーフィナンシャルグループ(株)	小島 博行	(国研)農業・食品産業技術総合研究機構(農研機構)
直井 信次郎	ソフトバンク(株)	小林 克巳	(株)野村総合研究所
上田 将史	第一生命保険(株)	山崎 英人	パーソルキャリア(株)
櫻庭 信之	第一東京弁護士会	伊藤 秀明	パーソルクロステクノロジー(株)
岩脇 正浩	ダイキン工業(株)	南 和哉	パナソニック(株)
小島 陽平	ダイキン工業(株)	勝見 松則	パナソニックコネクト(株)
永野 英世	(一社)地域セキュリティ協議会	高橋 洋一	パナソニックコネクト(株)
鈴木 一弘	地方公共団体情報システム機構（J-LIS）	常川 直樹	パナソニックコネクト(株)
百瀬 昌幸	地方公共団体情報システム機構（J-LIS）	安岡 祥吾	パロアルトネットワークス(株)
大島 和紘	中外製薬(株)	折田 彰	(株)日立システムズ
戸田 貴裕	中外製薬(株)	沼田 亜希子	(株)日立製作所
藤木 晃史	中外製薬(株)	森田 光	(株)日立製作所
田中 卓朗	TIS(株)	田中 秀和	(株)日立ソリューションズ
三木 基司	TIS(株)	古賀 洋一郎	ビッグローブ(株)
遠藤 宗	DXC テクノロジー・ジャパン(株)	菅野 裕之	富士通(株)

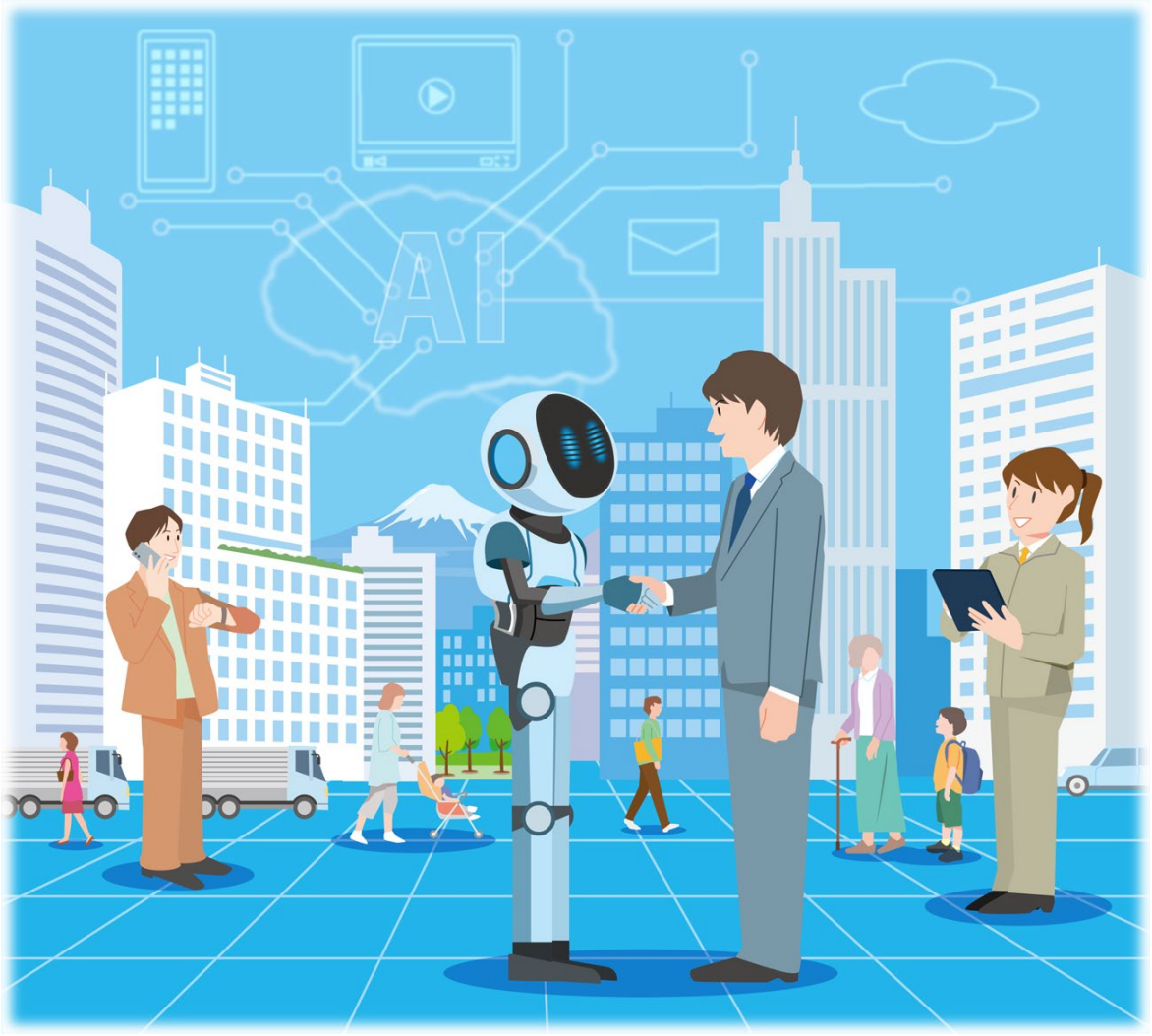
氏名	所属	氏名	所属
田中 昌弘	富士通(株)	石山 倫大朗	(株)ユービーセキュア
濱田 達也	富士通(株)	勝田 嵐士	(株)ユービーセキュア
菅原 尚志	フューチャー(株)	西大條 春仁	(株)ユービーセキュア
海老原 俊一	(株)Bridge	江面 祥行	(株)ユビテック
柳川 俊一	(株)Bridge	島田 理枝	(株)ユビテック
吉井 史和	(株)Bridge	久世 拓海	(株)横浜銀行
鴫原 祐輔	(株)Blue Planet-works	吉岡 克成	横浜国立大学
原 和宏	(株)ベイシア	佐久間 矩仁	横浜市役所
小野 洲平	PayPay(株)	牧野 尚彦	横浜市役所
川口 元輝	PayPay(株)	三国 貴正	(株)YONA
角 亮一郎	PayPay(株)	橘 喜胤	楽天カード(株)
有田 将也	(株)ベリサーブ	石原 亨	楽天銀行(株)
島津 祐希	(株)ベリサーブ	西村 茉優	楽天グループ(株)
橋本 葉介	(株)ベリサーブ	鳥越 真理子	楽天ペイメント(株)
太田 良典	弁護士ドットコム(株)	原子 拓	楽天ペイメント(株)
吉岡 宏樹	(株)Hokan グループ	石黒 友香子	楽天モバイル(株)
結城 亮史	(株)Box Japan	間下 義暁	楽天モバイル(株)
垣内 由梨香	マイクロソフトコーポレーション	山崎 圭吾	(株)ラック
髙倉 万記子	万記子コミュニケーションズ(同)	若居 和直	(株)ラック
鈴木 駿人	(株)マクニカ	猪野 裕司	(株)リクルート
瀬治山 豊	(株)マクニカ	六宮 智悟	(株)リクルート
政本 憲蔵	(株)マクニカ	上原 哲太郎	立命館大学
小野 晋司	(株)ミズ	有森 貞和	(株)両備システムズ
大山 水帆	MIZUHO デジタルサポート(同)	鈴木 堅太	(株)両備システムズ
佐々木 裕斗	三井住友カード(株)	矢儀 真也	(株)両備システムズ
鈴木 智也	三井住友カード(株)	板倉 英史	(株)Works Human Intelligence
高橋 洋樹	三井住友カード(株)	長谷川 淳一	(株)Works Human Intelligence
中村 直樹	三井住友海上火災保険(株)	羽場 満	YKK AP(株)
阿部 巧	(株)三井住友銀行	一條 敦	-
武笠 雄介	(株)三井住友銀行	今 佑輔	-
中村 智史	(株)三井住友銀行	清水 秀一郎	-
東内 裕二	三井物産セキュアディレクション(株)	piyokango	-
平田 真由美	みゅーらぼ		

編集責任	土屋 正				
イラスト製作	株式会社 創樹				
執筆協力者	10 大脅威選考会				
10 大脅威執筆者	井上 佳春	大久保 直人	篠塚 耕一	白石 歩	銭谷 謙吾
	土屋 正				
IPA 執筆協力者	高柳 大輔	大澤 淳	沖田 孝裕	金木 陽一	釜谷 誠
	岸野 照明	小山 明美	奥村 元	瀬川 雄涼	長迫 智子
	菊池 秀一	松本 穂乃花			

「情報セキュリティ 10 大脅威 2026」解説書［組織編］

2026 年 3 月 12 日 初 版
2026 年 3 月 23 日 二 版
2026 年 3 月 27 日 三 版
2026 年 4 月 11 日 四 版

［発行］ 独立行政法人情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
https://www.ipa.go.jp/



IPA 独立行政法人**情報処理推進機構**
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス

https://www.ipa.go.jp/security/