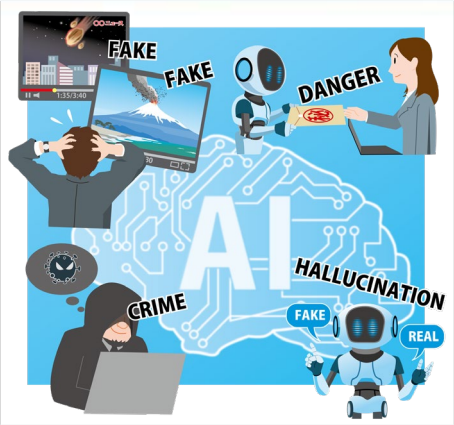
情報セキュリティ10大脅威 2026 [組織編]

～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～



IPA Better Life with IT

20xx年xx月xx日

〇〇部〇〇課

△△ △△

「情報セキュリティ10大脅威」とは？

- IPA が2006年から実施している取り組み
- 前年に発生したセキュリティ事故や攻撃の状況等から
  IPA が脅威候補を選出
- セキュリティ専門家や企業のシステム担当等から
  構成される「10大脅威選考会」が投票
- TOP 10入りした脅威を「10大脅威」として
  脅威の概要、被害事例、対策方法等を解説

「10大脅威」の特徴

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等で PC やスマホを利用する人 「個人」

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員 「組織」

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威 2026

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
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年ぶり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

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 「情報セキュリティ対策の基本」を常に意識することが重要

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	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	手口から重要視するべき対策を理解する

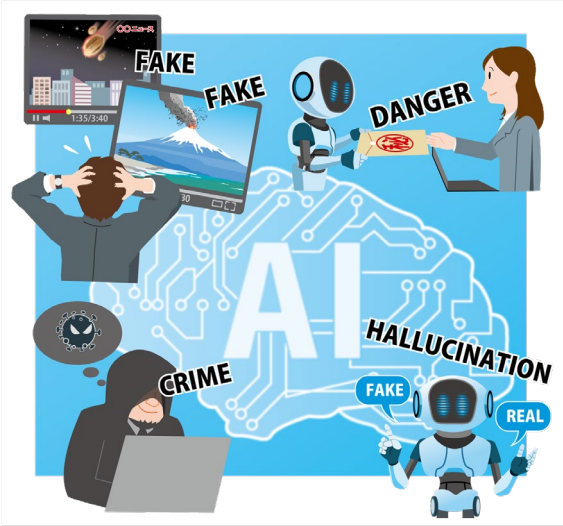
情報セキュリティ対策の基本＋α

- クラウドサービスの利用が浸透している昨今、「情報セキュリティ対策の基本」に加え、クラウドサービス利用を想定した対策も必要である

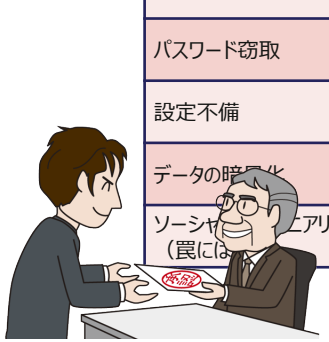
備える対象	情報セキュリティ対策の基本＋α	目　的
クラウドの選定	選定前の事前調査	クラウドサービスのガイドラインに沿った運営をしている業者やそのサービスを選定する
インシデント全般	責任範囲の明確化(理解)	クラウドサービスを契約する際は、インシデント発生時に誰(どの組織)がどこまでインシデント対応する責任があるのかを明確化(理解)する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報は常に確認し、仕様変更により意図せず変更された設定を適切な設定に修正する(設定不備により発生する情報漏えいや攻撃を防止する)

組織向け脅威の解説

- 組織が注目すべき脅威は、順位の高低ではなく、自組織の環境や状況に関係が深いかどうかで考える。
  （順位の高低は対策の優先順位ではない）
- 各脅威は「情報セキュリティ対策の基本」の実施を前提としている。このため、各脅威の「対策」への個別記載はしていない。

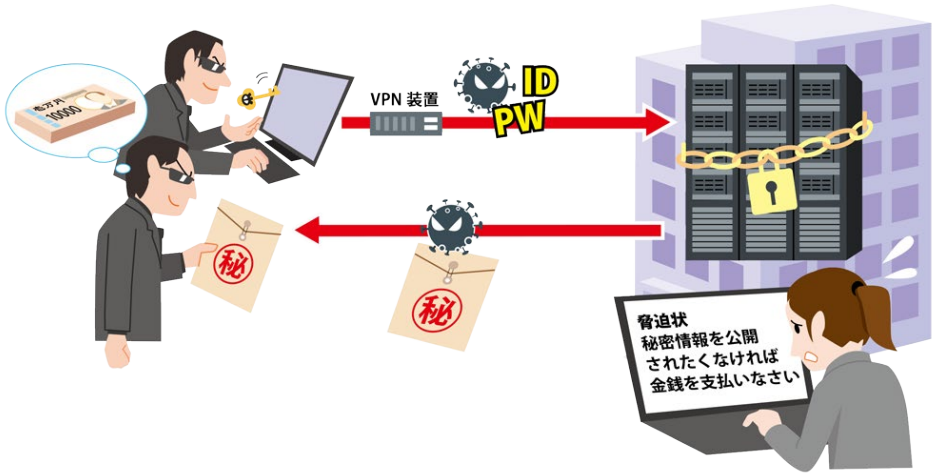


攻撃の糸口	情報セキュリティ対策の基本	目　的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアの利用	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取による情報[illegible]等のリスクを低減する
設定不備	設定の見直し	誤った設定が悪用され攻[illegible]けないようにする
データの暗[illegible]化	バックアップの取得	PCやサーバーのデータ削除[illegible]化に備える
ソーシャ[illegible]エアリング（罠には[illegible]	脅威・手口を知る	手口から重要視するべき対策[illegible]解する



【1位】ランサム攻撃による被害

- PCやサーバーをランサムウェアに感染させ、データの窃取、暗号化し、事業継続を困難にし、身代金を要求する。
- 窃取した情報を暴露すると脅す「2重脅迫」、DDoS攻撃を仕掛けると脅す「3重脅迫」、ランサムウェアに感染したことを利害関係者等に暴露すると脅す「4重脅迫」が確認されている。
- ランサムウェアを用いた暗号化を行わず、データ・情報を窃取し、暴露すると脅迫する「ノーウェアランサム」という攻撃もある。



【1位】ランサム攻撃による被害

- 攻撃手口 ①

・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。

【1位】ランサム攻撃による被害

- 攻撃手口 ②

・Webサイトやメールから感染させる

- Webサイトを改ざんし、偽の認証画像やエラー画面などを表示させる。
  利用者が画面の指示通りの操作することで感染する。
- メールの添付ファイルにマルウェアを仕込み、受信者に開封させて感染させる。
- メール文中にランサムウェアを仕込んだWebサイトのリンクを記載し、
  クリックさせることで感染させる。

・ダークウェブを利用する

- ダークウェブ等を利用し、RaaS（ランサムウェア提供、攻撃代行）、
  各種認証情報やアクセス情報等を購入して攻撃する。

【1位】ランサム攻撃による被害

- 事例/傾向 ①
  - **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※1、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※2 。
    - 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。
    - 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。
    - 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※3。

※1 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）
※2 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）
※3 アサヒビール商品出荷状況について（アサヒビール）

【1位】ランサム攻撃による被害

- 事例/傾向 ②
  - **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。
    - 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。
    - 同年12月12日、同社は、多要素認証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公表※4。

※4 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）

【1位】ランサム攻撃による被害

- 対策 ①
  - 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

  - 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
- 「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

【1位】ランサム攻撃による被害

- 対策 ②
  - 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】（前ページからの続き）

- 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機能等、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
- 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

【1位】ランサム攻撃による被害

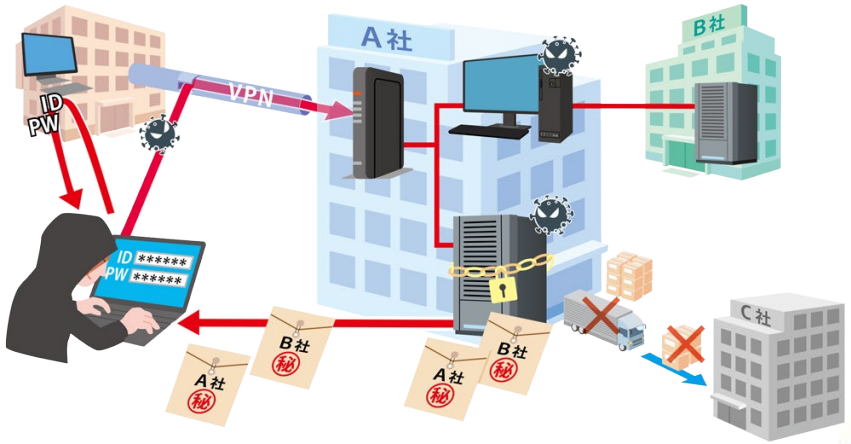
- 対策 ③
  - システム管理者、従業員、職員

【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

【2位】サプライチェーンや委託先を狙った攻撃

- サプライチェーンの概念には以下がある。
  - 商品企画、開発、調達、製造、在庫管理、物流、販売等一連のプロセス、これらに関わる組織、外部サービス
  - ソフトウェア開発のライフサイクルに関わるライブラリ、ツール、開発者、インフラ等の要素、要素間のつながり（ソフトウェアサプライチェーン）
- サプライチェーンの中でセキュリティ対策の脆弱な箇所が狙われ、攻撃の足掛かりにされ、間接的および段階的に標的組織を攻撃する。
- 秘密情報の漏えい等が発生し、信用の失墜、取引停止、損害賠償請求等が生じることがある。



【2位】サプライチェーンや委託先を狙った攻撃

- 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、利用者の機器に感染させる

- 利用者の多いソフトウェアを改ざんし、マルウェアを仕込む。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。
- 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。

・資産管理ソフトウェア等にマルウェアを仕込む

- MSP※5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。

※5 Managed Service Provder: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）

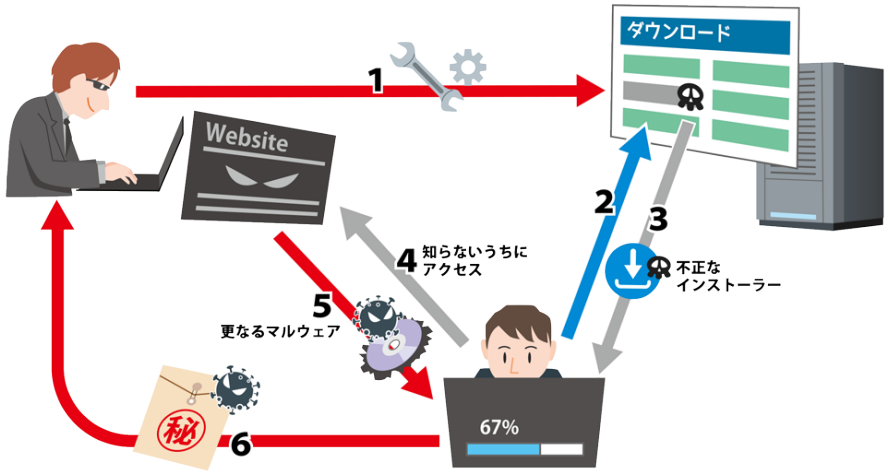
【2位】サプライチェーンや委託先を狙った攻撃

- 事例/傾向 ①
  - **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。
      同社に業務を委託する複数の企業が保有する個人情報が漏えい。
      その一部と思われる情報がダークウェブで公開されていると同社は公表※6 。
    - 同社の業務委託元も、被害に遭ったことを順次公表※7,8 。

※6 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）
※7 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）
※8 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）

【2位】サプライチェーンや委託先を狙った攻撃

- 事例/傾向 ②
  - **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※9 。
    - 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、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。



※9 【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.）

【2位】サプライチェーンや委託先を狙った攻撃

- 対策 ①
  - 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
  - CISOを配置する
  - CSIRTを構築する
  - 報告フォーマットは決めておく
  - 有事の際の対応フローを確立、社員へ通知する
  - 対応フロー通りに実施でいるか訓練する
  - 外部オン協力依頼先を用意する
  - 社内規則の整備や予算を確保する
- サイバー保険の検討
- 脅威インテリジェンスの推進
- 被害への補償の検討

【2位】サプライチェーンや委託先を狙った攻撃

- 対策 ②
  - 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を定期的に確認・検討
- セキュリティ評価サービス(SRS)※10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
- 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

  複数の候補から、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
- 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の明確化、合意形成、契約書に賠償に関する条項の盛り込み

※10 Security Rating Services

【2位】サプライチェーンや委託先を狙った攻撃

- 対策 ③
  - 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】（前ページからの続き）

- 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

- 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

【2位】サプライチェーンや委託先を狙った攻撃

- 対策 ④
  - 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、契約形態に応じた監査の実施
- 情報セキュリティの認証取得、維持のため外部レビューの実施

  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】

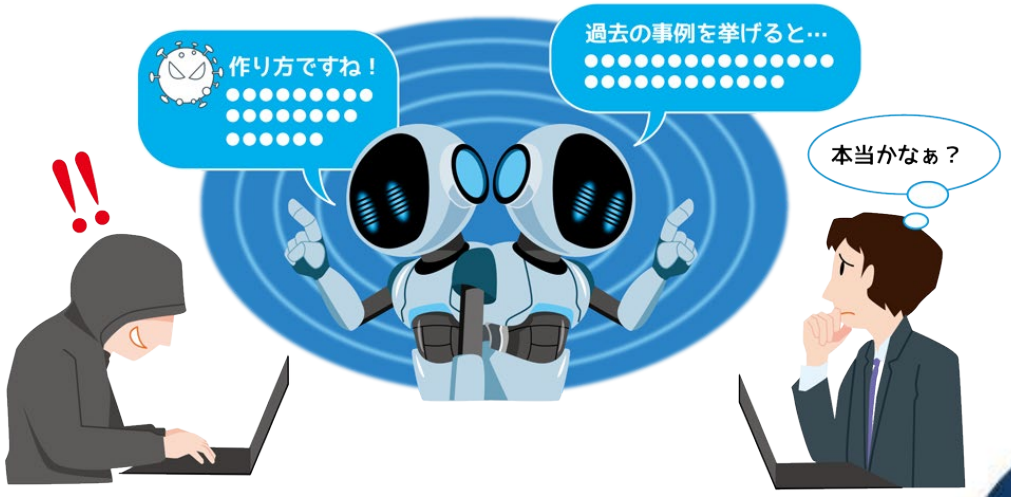
【被害を受けた後の対応】

- 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

【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

- AIに対する不十分な理解による、意図しない問題
  （他者の権利侵害、情報漏えい）
- AIが加工・生成した結果を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、手口の巧妙化



【3位】AIの利用をめぐるサイバーリスク

- リスク ①

・職場に許可なくAIを業務利用し、情報漏洩につながる可能性

- 従業員が個人的に利用しているAIサービスを業務利用し、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サービスに入力することで、情報漏洩につながる。
- 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。

・実在しない情報を対話型AIが生成する可能性

- 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（ハルシネーション）。
- 事実や正確性の確認等、生成結果の精査が必要。

【3位】AIの利用をめぐるサイバーリスク

- リスク ②

・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、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が可能。
- 言語の壁を実質的に乗り越え、多言語での攻撃が格段に容易。
- 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。
- 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る。

【3位】AIの利用をめぐるサイバーリスク

- 事例/傾向 ①
  - **生成AIの業務利用による情報漏洩**
    - 米国のAI企業の調査※11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%。
    - そのうち82%が組織に管理されていないアカウント。
  - **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**
    - 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。生成AIを用いて作成していたことが明らかになった※12 。
    - 生成AIが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。

※11 NEW Research: AI Is Already the #1 Data Exfiltration Channel in the Enterprise（The Hacker News Media Private Limited）
※12 生成AIに騙される弁護士がいまだに相次ぐ（JBpress）

【3位】AIの利用をめぐるサイバーリスク

- 事例/傾向 ②
  - **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。
    - 生成AIを補助的に使いプログラムを自作。
    - 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の疑いで逮捕※13 。
  - **AIの脆弱性**
    - 2025年6月、Microsoft 365 Copilot の脆弱性「EchoLeak」が報道された。
    - 脆弱性を悪用する不正プロンプトが注入されると、不適切なAIの動作が誘発され、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※14 。

※13 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）
※14 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）

【3位】AIの利用をめぐるサイバーリスク

- 対策 ①
  「AI事業者ガイドライン※15」における「AI利用者」を想定した対策
  - 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
      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

※15 AI事業者ガイドライン（経済産業省）

【3位】AIの利用をめぐるサイバーリスク

- 対策 ②
  - 経営者層
    - 決裁や承認プロセスのガバナンス強化

      高度化するソーシャルエンジニアリングへの備えとして、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

【3位】AIの利用をめぐるサイバーリスク

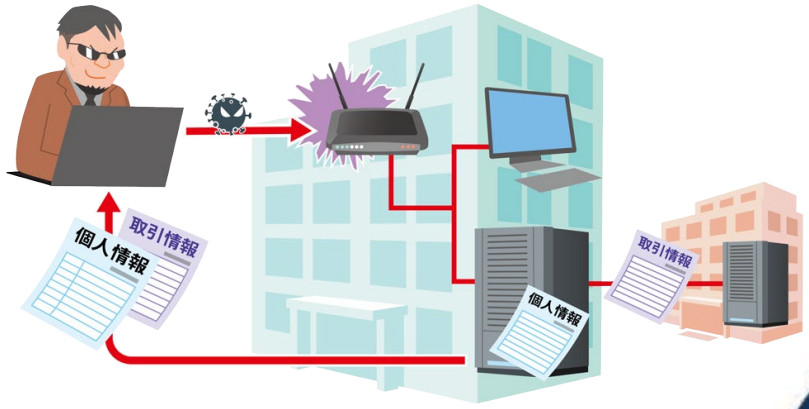
- 対策 ③
  - システム管理者、従業員、職員
    - AI利用におけるセキュリティ強化

      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
    - 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

【4位】システムの脆弱性を悪用した攻撃

- 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。
- 攻撃者は、公表された脆弱性対策情報やPoC（概念実証）を基に攻撃プログラム等を作成し、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
- 脆弱性を悪用した攻撃が行われると、様々な被害が発生し、事業やサービスの停止に追い込まれる場合もある。



【4位】システムの脆弱性を悪用した攻撃

- 攻撃手口 ①

・公表される前の脆弱性を悪用

- 脆弱性対策情報の公表前の脆弱性をゼロデイ脆弱性という。
- 公表前の脆弱性（ゼロデイ脆弱性）を悪用して攻撃する（ゼロデイ攻撃）。

・製品利用者が対策する前の脆弱性を悪用

- パッチや回避策が公開され、その対策を講じるまでの期間の脆弱性をNデイ脆弱性という。
- 製品利用者が対策を講じる前の脆弱性（ Nデイ脆弱性）を悪用して攻撃する（Nデイ攻撃）。
- 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。

【4位】システムの脆弱性を悪用した攻撃

- 攻撃手口 ②

・攻撃ツールや攻撃サービス等を悪用

- 公表された脆弱性は、短期間で攻撃ツールが作成される。
- ダークウェブ等で販売、提供された攻撃ツールを悪用する。
- オープンソースのツールに脆弱性を悪用した機能を実装する。

【4位】システムの脆弱性を悪用した攻撃

- 事例/傾向 ①
  - **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の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※16。
    - 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。
    - 漏えいの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おり、同省も注意喚起を公表※17。

※16 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）
※17 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）

【4位】システムの脆弱性を悪用した攻撃

- 事例/傾向 ②
  - **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※18 、その翌日には、PoCが公開※19
    - 共通脆弱性評価システム（CVSS）の深刻度は緊急（基本値 10.0）※20
    - 世界中で普及している製品であり、攻撃が国内外で多数確認され、IPAやJPCERT/CCから、早急に対策を促す、注意喚起が発出※21

※18 Critical Security Vulnerability in React Server Components（React）
※19 React Server Componentsの脆弱性（CVE-2025-55182）について（JPCERT/CC）
※20 React Server Componentsの脆弱性CVE-2025-55182（React2Shell）についてまとめてみた。（piyolog）
※21 React Server Componentsにおける脆弱性について（CVE-2025-55182）（IPA）

【4位】システムの脆弱性を悪用した攻撃

- 対策 ①
  - 経営者層

【被害の予防/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/被害に備えた対策】

    - 「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
    - 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

【4位】システムの脆弱性を悪用した攻撃

- 対策 ②
  - システム管理者、製品利用者

【被害の予防/被害に備えた対策】（前ページからの続き）

- 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の導入を検討する
- 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

【4位】システムの脆弱性を悪用した攻撃

- 対策 ③
  - システム管理者、製品利用者

【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

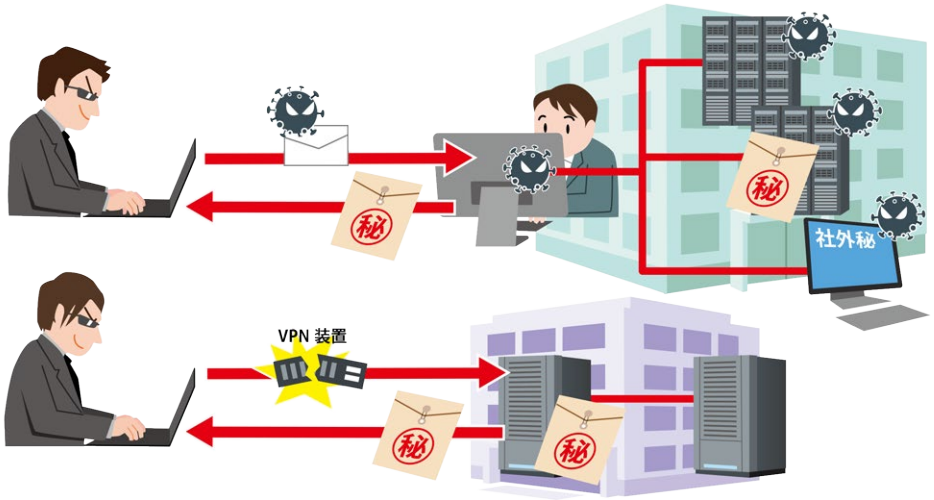
  - 開発ベンダー

【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

【5位】機密情報を狙った標的型攻撃

- 標的型攻撃は、特定の組織（民間企業、官公庁、団体等）に対するサイバーエスピオナージ（サイバー諜報活動）
- 機密情報等の窃取が目的
- 社会の動向や慣習の変化に合わせて攻撃手口を変える



【5位】機密情報を狙った標的型攻撃

- 攻撃手口 ①

・不正アクセス

- 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
- 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
- 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

【5位】機密情報を狙った標的型攻撃

- 攻撃手口 ②

・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。
- 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。

【5位】機密情報を狙った標的型攻撃

- 事例/傾向 ①
  - **MirrorFaceによる標的型攻撃**
    - 2025年3月頃、日本等を標的としている標的型攻撃グループのMirrorFace（別名Earth Kasha）が、新たなサイバー攻撃を行ったとされた。
    - 2025年1月に警察庁、国家サイバー統括室（NCO）がMirrorFaceについて、注意喚起※22 。
    - 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た※23 。
    - 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※24。

※22 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）
※23 MirrorFace によるサイバー攻撃について （注意喚起）（警察庁）
※24 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）

【5位】機密情報を狙った標的型攻撃

- 事例/傾向 ②
  - **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、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たため、「VPN機器等に対するORB（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※25。
    - 被害に遭うと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、ORBとして第三者への攻撃の踏み台として悪用されるおそれがある。

※25 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）

【5位】機密情報を狙った標的型攻撃

- 対策 ①
  - 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

【5位】機密情報を狙った標的型攻撃

- 対策 ②
  - 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】（前ページからの続き）

- 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。
- 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
  「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

【5位】機密情報を狙った標的型攻撃

- 対策 ③
  - 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）】

- 「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）

- **発生要因**
  - 地理的条件、政治的、外交・安全保障上の対立や軍事緊張が契機。
- **手段と目的**
  - 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、周辺国の機密情報の窃取、外貨獲得、嫌がらせや報復などを目的として実行。
  - SNSを中心とした偽情報により、他国の評判を貶め自国に優位な状況を作る等の影響工作を実施。
- **影響**
  - ランサム攻撃等により、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へ経済的打撃を与える。サプライチェーン全体へも影響を与えることがある。
  - 経済制裁を受けている国家がサイバー攻撃を通じた金銭獲得による、経済制裁の実効性低下

【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）

- 攻撃手口 ①

・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。
  （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秘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。

【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）

- 攻撃手口 ②

・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、秘密情報の窃取、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。

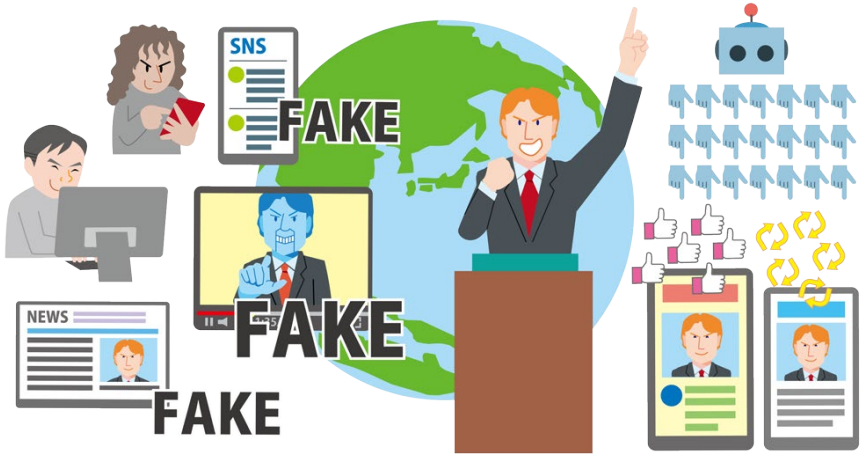
【6位】地政学的リスクに起因するサイバー攻撃（情報戦を含む）

- 事例/傾向 ①
  - **国家を背景としたDDoS攻撃**
    - 2025年12月、米司法省はハクティビスト集団であるNoname057（16）とCyber Army of Russia Reborn（CARR）の活動をほう助した疑いで容疑者を起訴。
    - 両集団は外国の政府によって設立、資金援助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※26。
    - 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Noname057（16）に関し、注意喚起を発出 ※27,28 。
    - 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※29

※26 Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups（Office of Public Affairs）
※27 Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure（Cybersecurity and Infrastructure Security Agency）
※28 Pro-Russia hacktivist activity continues to target UK organisations（National Cyber Security Centre）
※29 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）

【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）

- 事例/傾向 ②
  - **国家を背景とした影響工作**
    - 欧州では、2025年2月のドイツ総選挙※30 、同年6月のポーランド大統領選挙※31 、同年9月のモルドバ共和国議会選挙※32で外国からの影響工作が観測。
    - 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、2024年から2025年にかけ、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を確認※33 。



※30 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）
※31 Illegal Doppelganger Operation: Targeting the Polish Elections（Alliance4Europe）
※32 How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation（BBC）
※33 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）

【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）

- 対策 ①
  - 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

【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）

- 対策 ②
  - システム管理者

【被害の予防および被害に備えた対策】（前ページからの続き）

- 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

【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）

- 対策 ③
  - 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

- **要因**
  - 職場への私怨に伴う嫌がらせ、転職先で有利な立場を得るため、金銭目的、外部者からの勧誘、買収、多忙等地理的条件
- **手段**
  - 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、改ざん、削除等の不正行為
  - 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も含む
- **影響**
  - 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。

    →経営の根幹を揺るがす業績の悪化
  - 自組織に持ち込まれた情報が不正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。

【7位】内部不正による情報漏えい等

- 攻撃手口 ①

・アクセス権限の悪用

- 付与された正当な権限を悪用し、不正操作などにより組織の秘密情報を窃取する
- 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。
- 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

- 離職者の利用者IDやアクセス権を削除していないと、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し、情報窃取や不正操作ができてしまう。

【7位】内部不正による情報漏えい等

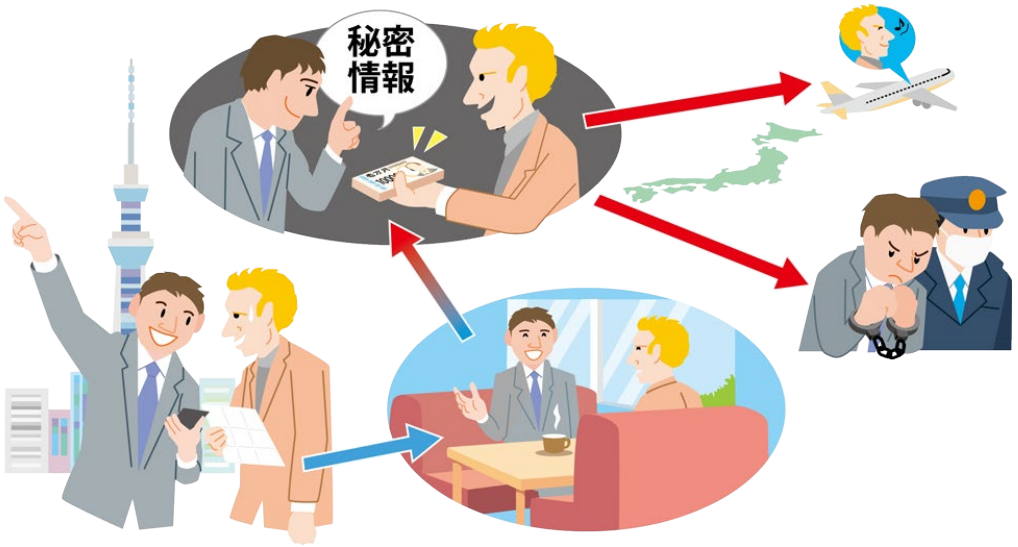
- 攻撃手口 ②

・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、スマートフォンのカメラ、紙媒体等を使い、組織の情報を外部に不正に持ち出す。
- 証拠を残さないため、口頭で伝える場合もある。

【7位】内部不正による情報漏えい等

- 事例/傾向 ①
  - **元ロシア通商代表部員への営業秘密情報漏えい※34**
    - 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。
    - 元社員は、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、不正競争防止法に違反したとして書類送検。
    - 元職員はすでに帰国。



※34 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）

【7位】内部不正による情報漏えい等

- 事例/傾向 ②
  - **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※35。
    - 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、顧客情報を持ち出した可能性※36 。

※35 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）
※36 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）

【7位】内部不正による情報漏えい等

- 対策 ①

「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

【7位】内部不正による情報漏えい等

- 対策 ②
  - 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」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。
- 情報リテラシー、モラルの醸成、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。

【7位】内部不正による情報漏えい等

- 対策 ③
  - システム管理者

【被害の予防および被害に備えた対策】（前ページからの続き）

- 秘密情報の管理、保護　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。
- CASB（クラウド利用時のセキュリ）、DLP（情報漏えい対策）等のツール導入、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。
  - ・記録媒体は、物理的破壊も含め、復元不可能な方法でデータ消去して廃棄。
  - ・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

【7位】内部不正による情報漏えい等

- 対策 ④
  - システム管理者

【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。

  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

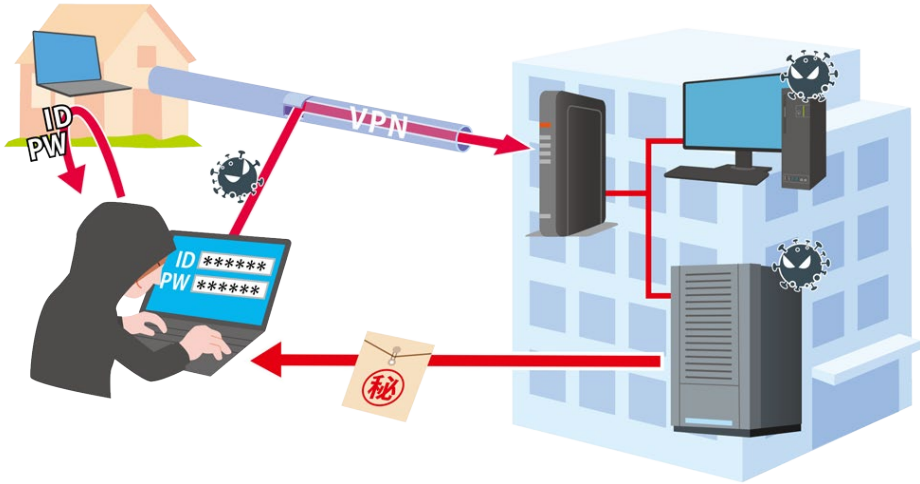
退職予定者の退職前後の監視を強化する。

【被害のを受けた後の対応】

- 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

【8位】リモートワーク等の環境や仕組を狙った攻撃

- リモートワークに必要な環境や仕組みである、VPN機器等に対して攻撃を仕掛け、組織内部への侵入を図る
- VPN機器等に残存した脆弱性や、別途入手したアカウント情報を悪用し、侵入を図る。
- 侵入を許すと、社内システムへの不正アクセスやマルウェア感染などにより、業務の停止や遅延が発生するおそれがある



【8位】リモートワーク等の環境や仕組を狙った攻撃

- 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機器等の脆弱性や設定ミス等を悪用し、組織内システムへ侵入する。

・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する。

・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、端末内の業務情報や認証情報等を窃取する。
- 窃取した情報を悪用し、VPN経由等で社内システムへ侵入する。

【8位】リモートワーク等の環境や仕組を狙った攻撃

- 事例/傾向
  - **リモートワーク環境を狙った攻撃の状況**
    - 警察庁の過去数年の統計資料※37 ではランサムウェア被害の感染経路はVPN機器を経由したものが過半数。
    - VPN機器経由とリモートデスクトップ経由の合計は毎年8割を超過。
    - これら感染経路の割合の合計は上昇傾向にあり、2025年は87%

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%**

※37 サイバー空間をめぐる脅威の情勢等（警察庁）

【8位】リモートワーク等の環境や仕組を狙った攻撃

- 対策 ①
  - 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
- リモートワークならでは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
- 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

【8位】リモートワーク等の環境や仕組を狙った攻撃

- 対策 ②
  - 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、ZTNA/SDP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利用時はネットワークレベル認証（NLA）を行う
- 多要素認証（MFA）やFIDO／FIDO2（パスキーなど）を利用する

【8位】リモートワーク等の環境や仕組を狙った攻撃

- 対策 ③
  - セキュリティ担当者、システム管理者

【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】

- 「情報セキュリティ対策の基本」、「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で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

【8位】リモートワーク等の環境や仕組を狙った攻撃

- 対策 ④
  - 従業員、職員

【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※38＞

「テレワークを行う際のセキュリティ上の注意事項」（IPA）

・リモートワークを行う際のセキュリティ上の注意事項

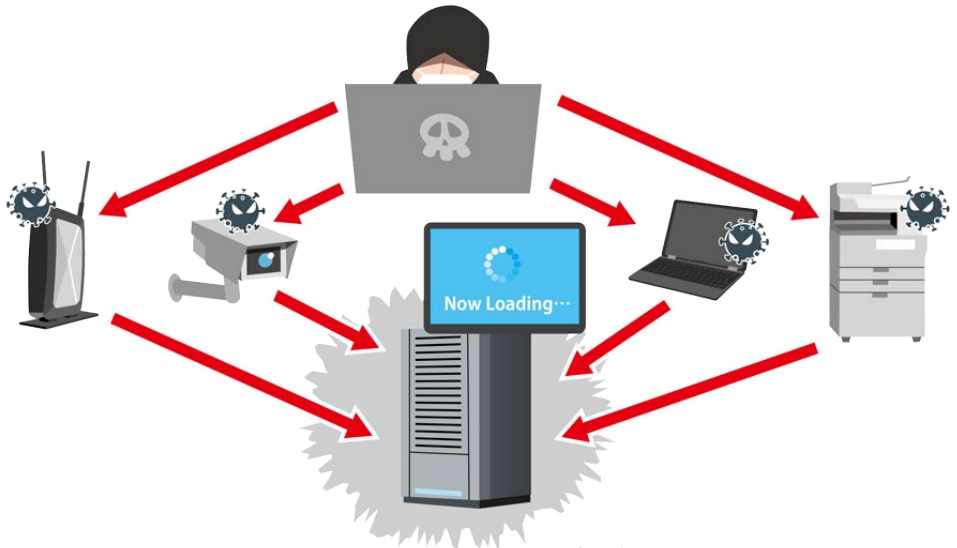
・リモートワークから職場に戻る際のセキュリティ上の注意事項

・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

※38 テレワークを行う際のセキュリティ上の注意事項（IPA）

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 乗っ取った複数の機器で構成したネットワーク（ボットネット）から大量のアクセスを一斉にしかけ、高負荷な状態にさせ、Webサイトや Webサービスを利用不能にする。
- これによりサービス提供、事業継続に大きな影響を及ぼし、人々の日常生活にも支障をきたすことがある。
- 主義主張の誇示やDDoS攻撃の停止と引き換えに金銭を要求することもある。



【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 攻撃手口 ①

・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

- 通信に使用されるTCPプロトコル・UDPプロトコルを悪用し、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。
- 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。

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 攻撃手口 ②

・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。

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 攻撃手口 ③

・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されている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。

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 事例/傾向 ①
  - **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。
    - 同月30日には問題解消のうえ復旧したことを公表※39。
    - 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※40 。
    - 障害の原因がDDoS攻撃によるものであること、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※41 、7月31日にはネットワークの復旧を完了※42 。

※39 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）
※40 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）
※41 ネットワーク不具合に関するお詫び（続報）（ナード研究所）
※42 ネットワーク復旧のお知らせ（ナード研究所）

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 事例/傾向 ②
  - **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、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※43。
    - 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発生。
    - 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、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。

※43 【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）

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 対策 ①
  - 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を利用
- WAF、IDS/ IPS、DDoS対策サービスの導入
- システムの冗長化等の軽減策
- 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SNS等の告知手段の整備

【9位】DDoS攻撃（分散型サービス妨害攻撃）

- 対策 ②
  - Webサイトの運営者

【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）

【9位】DDoS攻撃（分散型サービス妨害攻撃）

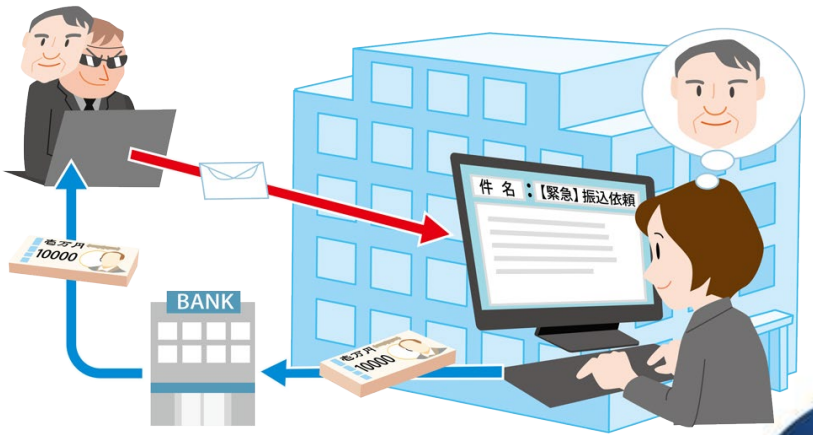
- 対策 ③
  - サービス事業者

【被害の予防】（前ページからの続き）

- IoT機器の脆弱性対策
  - ・サポートの切れたIoT機器を使わない。
  - ・IoT 機器のセキュリティ対策を強化する。
- 把握されていないIT資産の顕在化と対策
  - ・ASM等でIT資産を顕在化する。

【10位】ビジネスメール詐欺

- 経営者や弁護士等、権威ある第三者や取引先になりすまし、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。
- 生成AIを悪用し、経営者等の声や画像（動画）を生成し、相手をだます手口も確認されている。
- メール受信者は、送信者の立場や業務指示に対し、従わなければという社会適合性や、違和感のない巧妙な文面から、虚偽と見抜けず、指示に従ってしまう。
- 最近ではSNSも悪用されている。



【10位】ビジネスメール詐欺

- 手口 ①

・ビジネスメール詐欺の準備としての情報窃取

- 標的組織の経営者や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。
- 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（従業員の氏名やメールアドレス等）を窃取する。
- 取引に関わるメールのやり取りを盗聴し、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。

【10位】ビジネスメール詐欺

- 手口 ②

・取引先へのなりすまし

- 請求書の口座情報を、攻撃者が用意した虚偽の口座情報に差し替える。
- 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、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。

【10位】ビジネスメール詐欺

- 手口 ③

・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ったり、生成AIによる偽電話を掛け、本物であると従業員に信じ込ませ、振り込みを促す。

【その他の特徴】

- AIによるディープフェイク等を悪用したなりすまし。
- 「緊急」や「他の従業員には秘密」と申し添える。
- 簡潔なメールで、LINEグループの作成とQRコードの返信や、ビジネスチャットのアカウント情報の返信を指示。

【10位】ビジネスメール詐欺

- 事例/傾向 ①
  - **取引先担当者のアカウントが乗っ取られ、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。
    - 最終的な被害額は日本円で約1,400万円。
    - 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。
    - 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※44。

※44 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）

【10位】ビジネスメール詐欺

- 事例/傾向 ②
  - **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グループの作成を依頼する簡潔な文面のメール着信が相次いだ。
    - LINEヤフーは金銭を詐取する手口であると2026年1月に注意喚起※45。
    - 同様の事案の急増、被害の発生うけ、警視庁も2026年1月に注意喚起、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た※46。

※45 【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）
※46 社長・上司を装ったメールが急増中（警視庁）

【10位】ビジネスメール詐欺

- 対策 ①

【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
- 「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。

【10位】ビジネスメール詐欺

- 対策 ②

【被害の予防および被害に備えた対策】（前ページからの続き）

- 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）。
- 私有メールアドレスを業務に使用しない

【10位】ビジネスメール詐欺

- 対策 ③

【被害の予防および被害に備えた対策】（前ページからの続き）

- 認証を適切に運用する

  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。
  AiTM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。

＜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、メール以外に電話等の方法で直接取引先に確認をする。
  金融機関にその口座の名義等を確認する。

【10位】ビジネスメール詐欺

- 対策 ④

＜メールの真正性の確認＞ （前ページからの続き）

- 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、表現の誤り、送信元のメールドメインに注意。

- 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る。

  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

まとめ

「情報セキュリティ対策の基本」を実践

・「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は変わらない

各脅威の手口の把握および対策の実践

・脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要

・「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない

組織ごとの状況を考慮して対策の優先度を決定する

まとめ

「共通対策」を実践

- 対策を種類別で見ると、複数の脅威に有効な対策がある
- 以下の「共通対策」を「情報セキュリティ対策の基本」と共に実施することで、より効率的で広範囲に対策を実践することが可能

※「情報セキュリティ10大脅威 2026」解説書［組織編］で共通対策の詳細な解説資料を公開中

共通対策
インシデント体制の整備し対応する
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 をクリックしない

資料のダウンロード

- 情報セキュリティ10大脅威　2026
  - 情報セキュリティ10大脅威に関する各種資料は以下のWebページをご覧ください。

https://www.ipa.go.jp/security/10threats/10threats2026.html