情報セキュリティ10大脅威　2025

[組織編]

IPA Better Life with IT

「情報セキュリティ10大脅威」とは？

- IPA が2006年から毎年発行している資料
- 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 2025

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	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

情報セキュリティ10大脅威 2025

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	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃		年連続8回目
4	内部不正による情報漏えい等		回目
5	機密情報等を狙った標的		
6	リモートワーク等の環境や		
7	地政学的リスクに起因する		
8	分散型サービス妨害攻撃（DDoS		6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

自組織により強く関係する脅威から対策する
ことが重要

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
- 下記の**「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
マルウェアに感染	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	誤った設定を攻撃に利用されないようにする
誘導(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

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋α の対策を行い、備える必要がある

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

- ここからは脅威毎に解説します
- 組織により強く関係する脅威から確認しましょう
- **各脅威の対策の紹介では前項の「情報セキュリティ対策の基本」は実施していることを前提とし、記載には含めていません**

【1位】ランサム攻撃による被害

- ランサムウェアに感染させ、端末ロックや PC やサーバーのデータ窃取、暗号化を行い、業務継続困難な状態にする
- 攻撃者は複数の脅迫を組み合わせて、被害組織が金銭の支払いを検討せざるを得ない状況を作り出そうとする
- RaaS（Ransomware as a Service）という、サービスとして開発・提供されたランサムウェアによる攻撃もある
- ランサムウェアを用いない金銭要求を行う攻撃として、「ノーウェアランサム」による攻撃や、DDoS 攻撃を仕掛けると脅迫するランサムDDoS 攻撃も確認されている

【出典】 令和６年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/R6/R06_cyber_jousei.pdf

【1位】ランサム攻撃による被害

- **攻撃手口**

・ランサムウェアに感染させて金銭を要求

- **脆弱性を悪用しネットワークから感染させる**
  - ソフトウェアの脆弱性を悪用し
    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**
  - 意図せず公開されているポート(リモートデスクトップ等)を
    利用した不正アクセスからマル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

・ランサムウェアに感染させて金銭を要求

- **Web サイトやメールから感染させる**
  - ランサムウェアをダウンロードさせるように Web サイトの脆弱性を悪用して改ざんし、閲覧した際に感染させる
  - 不正な添付ファイルを開かせて感染させる
  - 悪意のあるリンクをメール本文中に仕込み開くよう誘導し、感染させる

【1位】ランサム攻撃による被害

- **2024年の事例/傾向①**
  - **ランサムウェア感染による被害と二次被害**
    - 2024年6月、KADOKAWA が ランサムウェア攻撃を含む大規模なサイバー攻撃にあった
    - フィッシング攻撃等により従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことが原因と推測
    - 複数のサービスが停止したほか、約25万4,000人分の個人情報や企業情報の漏えいが判明した
    - 攻撃組織が公開したとされる情報が、SNS 等を通じて拡散された

【出典】 ランサムウェア攻撃による情報漏洩に関するお知らせ（株式会社KADOKAWA）
https://group.kadokawa.co.jp/information/media-download/1356/d3f77b589c58d083/
漏洩情報の拡散行為に対する措置ならびに刑事告訴等について（株式会社KADOKAWA）
https://www.kadokawa.co.jp/topics/12010/

【1位】ランサム攻撃による被害

- **2024年の事例/傾向②**
  - **ノーウェアランサムによる攻撃事例**
    - 2024年10月、国立遺伝学研究所の生命情報・DDBJセンターがデータ窃取の脅迫を受けたと情報・システム研究機構が公表した
    - 国際ハッカー集団「CyberVolk」の犯行声明では、DDBJのデータ 5%を公開し、1万ドルを支払わなければ残り95%も公開するとSNS上で脅迫した。
    - 調査によってシステムへの不正侵入やデータ消失等は確認されず、窃取したとされるデータも公開データであった。

【出典】 国際塩基配列データベース「DDBJ」に対するサイバー脅迫に関するご報告（生命情報・DDBJセンター）
https://www.ddbj.nig.ac.jp/news/ja/2024-10-22

【1位】ランサム攻撃による被害

- **2024年の事例/傾向③**
  - **RaaS が利用された国内事例**
    - 2024年6月、ヒロケイが RaaS の一種である「Phobos」を用いた攻撃を受けていたことを公表
    - 原因は、サーバーの脆弱性および VPN ルーターの設定不備で、攻撃者がこれを悪用し社内ネットワークに侵入後、複数のサーバーに対してデータの暗号化を行った
    - この攻撃で、情報の漏えいや二次被害は確認されていない

【出典】 弊社内ネットワークへの外部からの不正アクセス被害の発生について（第一報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/646/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第二報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/649/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第三報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/668/

【1位】ランサム攻撃による被害

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - 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きるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【1位】ランサム攻撃による被害

- **対策**
  - **組織(システム管理者、従業員)**

【被害の予防／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
- 添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない
- 多要素認証の設定を有効にする
- 提供元が不明のソフトウェアを実行しない
- サーバーや PC、ネットワークに適切なセキュリティ対策を行う
- 共有サーバー等へのアクセス権の最小化と管理の強化
- 公開サーバーへの不正アクセス対策
- 適切なバックアップ運用(取得、保管、復旧訓練)を行う
  - バックアップ自体の暗号化対策として、WORM（Write Once Read Many）機能等も有効である。

【1位】ランサム攻撃による被害

- **対策**
  - **組織(システム管理者、従業員)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する
- 適切なバックアップ運用(復旧作業)を行う
- 復号ツール※1の活用

【出典】 ※1 The No More Ransom Project(No More Ransomプロジェクト)
https://www.nomoreransom.org/

【1位】ランサム攻撃による被害

- **身代金の支払いと復旧業者の選定について**
  - 原則、身代金を支払わずに復旧を行う
  - 支払いに応じてもデータの復元や情報の流出を防げるとは限らない
  - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
  - 対応を依頼する業者の選定※1にも注意が必要
  - データの復旧に関しては、復号ツールの活用についても検討すると良い

【出典】 ※1 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://digitalforensic.jp/home/act/products/higai-checksheet/

【2位】サプライチェーンや委託先を狙った攻撃

- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足掛かりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりである「ソフトウェアサプライチェーン」を悪用して攻撃される
- 取引先や業務を委託している外部組織から情報漏えいする

【2位】サプライチェーンや委託先を狙った攻撃

- **攻撃手口**

・取引先や委託先が保有する機密情報を狙う

- セキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、標的組織の機密情報を狙う

・ソフトウェア開発元や MSP※1 等を攻撃し、標的組織を攻撃するための足掛かりとする

- ソフトウェアやサービスを改ざんしてマルウェアを仕込み、インストールやサービス利用の際に顧客にマルウェアを感染させる等

※1 MSP（マネージドサービスプロバイダー／企業システムの運用・監視等を請け負う事業者）

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向①**
  - **業務委託先業者からの顧客情報漏えい**
    - 2024年5月、イセトーは VPN 経由の不正アクセスを受け、端末やサーバー等がランサムウェア攻撃を受けたと公表した
    - 2024年6月、攻撃者が窃取したとされる情報のダウンロード用 URL が攻撃者グループのリークサイトに掲載された
    - 自治体だけでも約 50 万件以上の個人情報が漏えいした
    - 業務委託元より損害賠償請求の予定も報告された

【出典】 不正アクセスによる個人情報漏えいに関するお詫びとご報告（株式会社イセトー）
https://www.iseto.co.jp/news/news_202410.html
報道発表資料「委託業者のランサムウェア被害に伴う個人情報漏えい事案」に係る市民への対応について（豊田市）
https://www.city.toyota.aichi.jp/pressrelease/1060027/1060257.html
印刷業務委託先のランサムウェア被害について（第3報）（徳島県）
https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7242743/
委託業者におけるコンピューターウイルス感染について（和歌山市）
https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html
委託業者におけるコンピューターウイルス感染について（最終報）（愛媛県）
https://www.pref.ehime.jp/page/85357.html

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向②**
  - **委託先への攻撃に起因するサービス停止**
    - 2024年9月、関通はサイバー攻撃により、サーバーがランサムウェアに感染したことを公表した
    - 入出庫関連のシステムが停止し、生産・出荷業務の一部が一時停止となった
    - 影響を受けた業務委託元の多数の組織からも出荷の遅延や一時停止等も公表された
    - 原因は悪意のある第三者による不正アクセス
    - 個人情報の漏えいは確認されなかった

【出典】 【第1報】当社におけるサイバー攻撃によるシステムの停止事案発生のお知らせ（株式会社関通）
https://www.kantsu.com/news/6573/
【第3報】当社におけるサイバー攻撃によるシステムの停止事案発生のお知らせ（株式会社関通）
https://www.kantsu.com/news/6615/
個人情報漏洩の可能性に関する確報（株式会社関通）
https://www.kantsu.com/news/6628/

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向③**
  - **ソフトウェアサプライチェーンの悪用**
    - 2024年3月、Linux 環境で広く利用されている「XZ Utils」という可逆圧縮ツールに悪意のあるコードが仕込まれたことが確認された
    - この悪意あるコードは共同開発者によって挿入された
    - 特定の条件下でリモートからシステム全体へ不正アクセスできるおそれがあった

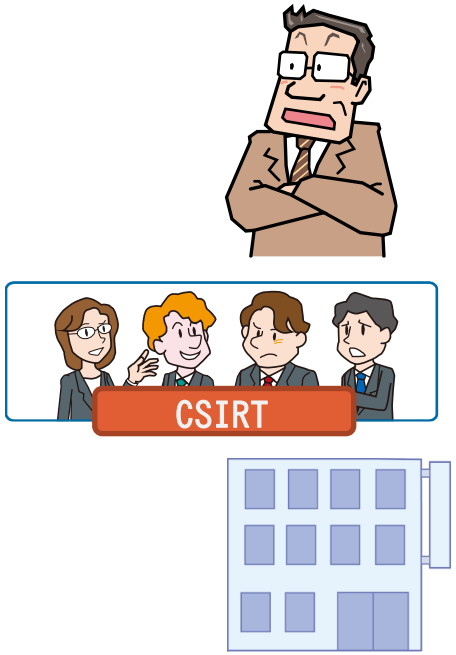
【出典】 XZ Utilsに悪意のあるコードが挿入された問題（CVE-2024-3094）について（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2024040101.html
Urgent security alert for Fedora Linux 40 and Fedora Rawhide users（Red Hat）
https://www.redhat.com/en/blog/urgent-security-alert-fedora-40-and-rawhide-users

【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(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を整備し、対応する
  - 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きるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織で実施)**

【被害の予防／被害に備えた対策】

- 情報管理規則の徹底
- セキュリティ評価サービス(SRS)を用いた自組織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
- 契約内容の確認
- 委託先組織の管理
- 納品物の検証(ソフトウェアの把握や管理※1 、脆弱性対策の実施等)
- サーバーや PC、ネットワークの適切なセキュリティ対策

【出典】 ※1 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

【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織で実施)**

【被害を受けた後の対応】

- インシデント対応体制を整備し、対応する
- 被害への補償請求

【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害の予防／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応の確認、監査
- 情報セキュリティの認証取得および維持
  - ISMS、P マーク、SOC2 等を取得し、
    定期的な見直しと運用維持
- 公的機関等が公開している資料※1の活用

【出典】 ※1 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
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(内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
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

【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

【3位】システムの脆弱性を突いた攻撃

- ソフトウェアの脆弱性が発見されると、開発ベンダー等が脆弱性対策情報（修正プログラムや回避策等）を公開し、製品利用者へ対策を促す
- 攻撃者は、その情報を基に攻撃プログラム等を作成し、対策が行わ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、事業やサービスの停止など、甚大な被害に至ることがある

【3位】システムの脆弱性を突いた攻撃

- 攻撃手口

・公開される前の脆弱性を悪用（ゼロデイ攻撃）

- 脆弱性対策情報を公開する前に、攻撃者が脆弱性を悪用して行う攻撃

・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、パッチの適用や回避策を講じるまでの期間の脆弱性をN デイ脆弱性と呼び、未対策期間に攻撃

・攻撃ツールや攻撃サービス等を悪用

- ダークウェブ等で販売されている攻撃ツールや攻撃サービスを悪用

【3位】システムの脆弱性を突いた攻撃

- **2024年の事例/傾向①**
  - **Palo Alto Networks 製 PAN-OS の機能の脆弱性を悪用したゼロデイ攻撃**
    - 2024年4月、Palo Alto Networks は、PAN-OS の GlobalProtect 機能に関する脆弱性を公表した
    - 深刻度（CVSS v3.0）のベーススコアが、最大の 10.0 と評価され、脆弱性を悪用したゼロデイ攻撃が国内外で確認された
    - IPA、JPCERT コーディネーションセンターからは、侵害調査の推奨等の注意喚起が行われた

【出典】 Palo Alto Networks 製 PAN-OS の脆弱性対策について(CVE-2024-3400)（IPA）
https://www.ipa.go.jp/security/security-alert/2024/alert20240415.html
Palo Alto Networksの「PAN-OS」にゼロデイ脆弱性 - パッチを準備中（SecurityNEXT）
https://www.security-next.com/155956
Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2024/at240009.html

【3位】システムの脆弱性を突いた攻撃

- **2024年の事例/傾向②**
  - **Windows 上の PHP の脆弱性を悪用した攻撃**
    - 2024年6月、Windows 上で動作する CGI モードの PHP に OS コマンドインジェクションの脆弱性が報じられた
    - 既存の脆弱性（CVE-2012-1823）に対する保護を回避できるというもので、この脆弱性が悪用され、webshell を設置される被害や、ランサムウェア「TellYouThePass」の感染活動への悪用が確認された
    - IPA からは、修正プログラムの適用等の注意喚起が行われた

【出典】 PHPの脆弱性（CVE-2024-4577）を狙う攻撃について（IPA）
https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html
Windows環境の「PHP」脆弱性、ランサムの標的に - 他脆弱性にも注意（SecurityNEXT）
https://www.security-next.com/158289

【3位】システムの脆弱性を突いた攻撃

- **2024年の事例/傾向③**
  - **太陽光発電施設の遠隔監視機器に対する攻撃**
    - 2024年5月、コンテック製の太陽光発電施設向け遠隔監視機器がサイバー攻撃を受け、不正送金の踏み台として悪用されたと報じられた
    - この攻撃との関係性は不明だが、コンテック製品に関する脆弱性の一部（CVE-2022-29303 等）については、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の「既知の悪用された脆弱性カタログ」（KEV）に掲載されている
    - コンテックは、複数回の注意喚起（アップデートの推奨等）を行った

【出典】 太陽光発電施設にサイバー攻撃 身元隠し不正送金に悪用（共同通信）
https://nordot.app/1158206853963727018
太陽光発電施設向け当社遠隔監視機器へのサイバー攻撃報道について（株式会社コンテック）
https://www.contec.com/jp/info/2024/2024050700/
太陽光発電 監視機器約800台へのサイバー攻撃について調べてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2024/05/03/015043

【3位】システムの脆弱性を突いた攻撃

- **対策**
  - **組織(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を整備し、対応する
  - 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きるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする
- パッチ適用や回避策を講じるための予算確保

【3位】システムの脆弱性を突いた攻撃

- **対策**
  - **組織(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】

- 利用している資産の把握、対応体制の整備
- 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
- 最新の脆弱性情報の収集、対策状況の管理、パッチマネジメントの実施
- サーバーや PC、ネットワークに適切なセキュリティ対策を行う

【被害の早期検知】

- サーバーや PC、ネットワークに適切なセキュリティ対策を行う

【3位】システムの脆弱性を突いた攻撃

- **対策**
  - **組織(ソフトウェアの利用者、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
- 影響調査、原因の追究、対策の強化
- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

【3位】システムの脆弱性を突いた攻撃

- **対策**
  - **組織(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
- サーバーや PC、ネットワーク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

【4位】内部不正による情報漏えい等

- 組織の従業員や元従業員等による機密情報の漏えい
- 組織関係者による不正行為による、組織の社会的信用の失墜、損害賠償による経済的損失
- 不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある

【4位】内部不正による情報漏えい等

- **攻撃手口**

・内部の従業員は重要情報にアクセスしやすい
・悪意をもって情報を外部に提供してしまう

- **アクセス権限の悪用**
  - 付与されたパスワードを悪用し、組織の重要情報を取得する
  - 必要以上のアクセス権限を付与していると被害が大きくなる
- **在職中に割り当てられたアカウントの悪用**
  - 在職中に使用していたアカウントを使って不正に情報を取得する
- **内部情報の不正な持ち出し**
  - USB メモリー、HDD、メール、クラウドストレージ、スマホカメラ、紙媒体等での不正な持ち出し

【4位】内部不正による情報漏えい等

- **2024年の事例/傾向①**
  - **顧客情報を転職先に持ち出し、営業活動に使用**
    - 2024年4月、プルデンシャル生命保険は元社員が退職時に顧客情報を不正に持ち出し、転職先で使用したと公表した
    - また、2024年8月、東急リバブルも元社員による個人情報の不正持ち出し、転職先でDM（ダイレクトメール）に利用したことを公表した
    - 前者は 979 件を印刷し紙で、後者は 2 万 5,406 件をデータで持ち出していた

【出典】 当社元社員によるお客さまの個人情報の漏えいに関するお詫びとお知らせ（プルデンシャル生命保険株式会社）
https://www.prudential.co.jp/news/pdf/841/20240409.pdf
弊社元従業員による個人情報の不正な持ち出しに関するご報告とお詫び（東急リバブル株式会社）
https://www.livable.co.jp/assets/files/3972

【4位】内部不正による情報漏えい等

- **2024年の事例/傾向②**
  - **委託先企業が仕入先情報を不正ダウンロード**
    - 2024年2月、ダイキン工業は委託先作業者が私用で仕入先情報をダウンロードし、漏えいの可能性があると公表した
    - 不正にダウンロードされた個人情報は、約 2 万 2,000 件であった

【出典】 仕入先様情報の漏洩可能性に関するお詫びとお知らせについて（ダイキン工業株式会社）
https://www.daikin.co.jp/taisetsu/2024/240216

【4位】内部不正による情報漏えい等

- **2024年の事例/傾向③**
  - **退職時の持ち出し**
    - 2024年3月、クラレは欧州グループ会社の元従業員が退職に際し、同社が保有する情報を不正に持ち出したと公表した
    - 持ち出された情報は個人情報も含まれていたが、返却され、外部への流出はないという

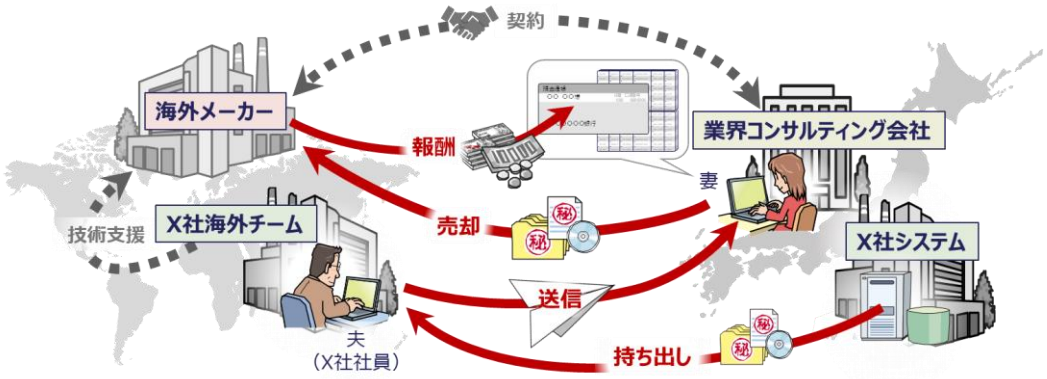
【出典】 当社グループ元従業員による情報の不正な持ち出しに関するお知らせ（株式会社クラレ）
https://www.kuraray.co.jp/news/2024/240325_2

【4位】内部不正による情報漏えい等

【参考情報】
「ヒト」を通じた組織からの長期にわたる情報漏えい

- 自社の機微な情報が、同業他社や他国などに「ヒト」を介在して流出。
  長期間にわたって、流出しているケースも多く存在。

- 2023年、不正競争防止法違反でガラス製造業元社員とその妻を逮捕
- **X社しか製造できないはず**の超軽量ガラス瓶を**海外メーカーが製造**していたことから事後発覚
- X社にて内部調査、男を懲戒解雇処分、兵庫県警による捜査実施。
  - 男は在職時海外担当係長級、妻は関連コンサルティング会社社長
  - **海外メーカー**から妻の会社口座に**5年間で計1億8,960万円**相当振込
  - 夫婦は**もともと外国籍**。事件発覚時は**日本に帰化**。



その他の内部不正事例（発生年）
電子部品の独自の技術情報を元社員が同業他社に渡すため、**国外へ**不正に持ち出し。（2021）
意図して接触してきた某国の外交官に通信会社の社員が技術情報を提供。外交官は**出国**。（2021）
総合商社の同業他社への**転職**に際し、元職場の営業情報を持ち出し。（2022）
大手通信会社の子会社の元派遣社員が**約10年間にわたり**営業秘密を、持ち出し。(2023)

動機
- 金銭取得
- 転職時の利得 等

【4位】内部不正による情報漏えい等

- **対策※1**
  - **組織(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
- 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

【出典】 ※1 組織における内部不正防止ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/insider.html

【4位】内部不正による情報漏えい等

- **対策※1**
  - **組織(システム管理者)**

【被害の予防／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」※2を意識する
  - 情報取扱ポリシーの作成や、内部不正者に対する懲戒処分等を規定した就業規則等を整備する※3
  - 役職員への定期的な教育も行う
- 情報リテラシー、モラル醸成、法令順守のための定期的な人材教育
- 資産の把握、管理体制の整備
- 機密情報の管理、保護
- 物理的管理の実施
- 定期的な職務の変更、職場の異動
- 必要に応じ、秘密保持義務を課す誓約書に署名させる

【出典】 ※1 組織における内部不正防止ガイドライン(IPA)
https://www.ipa.go.jp/security/guide/hjuojm00000055l0-att/ps6vr7000000jvcb.pdf
※2 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
※3 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

【4位】内部不正による情報漏えい等

- **対策**
  - **組織(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
  - 機密情報へのアクセス履歴や利用者の操作履歴等のログを監視する
  - 監視していることを従業員に周知する
  - 退職予定者の退職前後の監視を強化する

【4位】内部不正による情報漏えい等

- **対策**
  - **組織(システム管理者)**

【被害に遭った際の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する
- 内部不正者に対する適切な処罰の実施

【5位】機密情報等を狙った標的型攻撃

- 機密情報等の窃取や業務妨害を目的とし、特定の組織（民間企業、官公庁、団体等）を狙う
- 標的とする組織の状況に応じて攻撃手口を変える等巧みな攻撃手法で目的を果たそうとする

【5位】機密情報等を狙った標的型攻撃

- **攻撃手口**

・不正アクセス

- **標的組織が利用するサービスや機器の脆弱性を悪用して不正アクセスをし、組織内部に侵入する**
  - クラウドサービス
  - Web サーバー
  - VPN 装置
- **認証情報等を窃取し、正規の経路で組織のシステムへ再侵入する**

【5位】機密情報等を狙った標的型攻撃

- **攻撃手口**

・メールを用いた攻撃

- **メールからマルウェアに感染させる**
  - マルウェアを仕込んだ添付ファイルを開封させる
  - メール本文に記載したリンク先にマルウェアを仕込み、リンクにアクセスさせる
- **標的組織の従業員や職員になりすます**
  - 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ように偽装する
  - 実在する組織の差出人名が使われる

【5位】機密情報等を狙った標的型攻撃

- 攻撃手口

・Web サイトの改ざん（水飲み場型攻撃）

- 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
- 従業員が**その Web サイトにアクセスし、偽装されたマルウェアをインストールするなどして** PC を**感染**させる

【5位】機密情報等を狙った標的型攻撃

- **2024年の事例/傾向①**
  - **マルウェア感染による情報漏えい**
    - 2024年3月、富士通にて情報漏えいが発生した
    - 原因はマルウェアによるものと見られるが、様々な偽装を行って検知されにくくするなど高度な手法を用いていたため、発見が非常に困難であった
    - 通信ログや操作ログを確認したところ、個人情報を含むファイルが社外に持ち出されたおそれがあった

【出典】 個人情報を含む情報漏えいのおそれについて（富士通）
https://pr.fujitsu.com/jp/news/2024/07/9.html
富士通が3月セキュリティー事故の調査結果発表、個人情報含むファイルに複製コマンド（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/24/01158/
富士通がマルウェア感染による情報漏洩の可能性（デジタルデータ フォレンジック）
https://digitaldata-forensics.com/column/cyber_security/15146/

【5位】機密情報等を狙った標的型攻撃

- **2024年の事例/傾向②**
  - **日本の暗号資産関連事業者へのサイバー攻撃**
    - 2024年5月、DMM Bitcoin から約 482 億円相当の暗号資産が窃取された
    - サイバー攻撃グループ TraderTraitorがリクルーターになりすまし、暗号資産ウォレットソフトウェアを開発するGincoの従業員に接触
    - 採用前試験を装った悪意あるスクリプトを送付し、その従業員のPCの情報を窃取した
    - その後、この従業員になりすまし、システムに不正アクセスした上で、DMM Bitcoin の暗号資産を盗み出した

【出典】【重要】暗号資産の不正流出発生に関するご報告（第一報）（DMM Bitcoin）
https://bitcoin.dmm.com/news/20240531_01
北朝鮮を背景とするサイバー攻撃グループTraderTraitorによる暗号資産関連事業者を標的としたサイバー攻撃について（警察庁）
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html
【重要】口座及び預かり資産のSBI VCトレードへの移管に向けた基本合意について（DMM Bitcoin）
https://bitcoin.dmm.com/news/20241202_01

【5位】機密情報等を狙った標的型攻撃

- **2024年の事例/傾向③**
  - **JAXA に対する不正アクセスの対応状況を公表**
    - 2024年7月、前年6月に発生した JAXA に対する不正アクセスについて、対応状況を公表した
    - 攻撃は、一般業務の情報を扱うネットワークへの攻撃であったため、ロケットや人工衛星に関する情報の漏えいはなかったが、機密保持契約締結を含む情報が漏えいしたとみられる
    - 不正アクセスは2024年1月以降も複数回発生した
    - いずれも VPN 機器の脆弱性を狙った攻撃であることが確認された

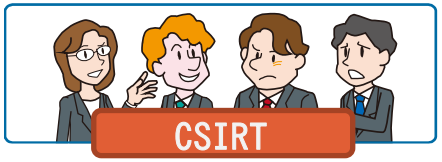
【出典】 JAXAにおいて発生した不正アクセスによる情報漏洩について（宇宙航空研究開発機構）
https://www.jaxa.jp/press/2024/07/20240705-2_j.html
JAXAに複数回サイバー攻撃、23～24年 機密情報流出か（日本経済新聞）
https://www.nikkei.com/article/DGXZQOUE210L20R20C24A6000000/

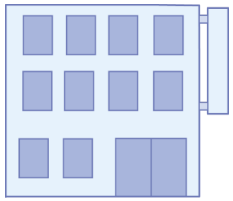
【5位】機密情報等を狙った標的型攻撃

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - 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きるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



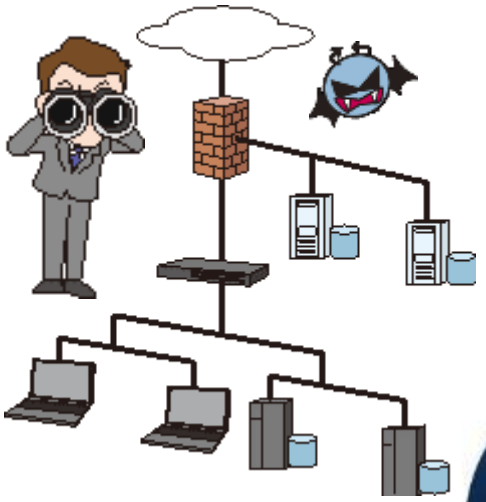


【5位】機密情報等を狙った標的型攻撃

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の予防／被害に備えた対策】

- 情報の管理と運用規則策定
- 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
- サーバーや PC、ネットワーク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
- 海外拠点等も含めたセキュリティ対策の向上



【5位】機密情報等を狙った標的型攻撃

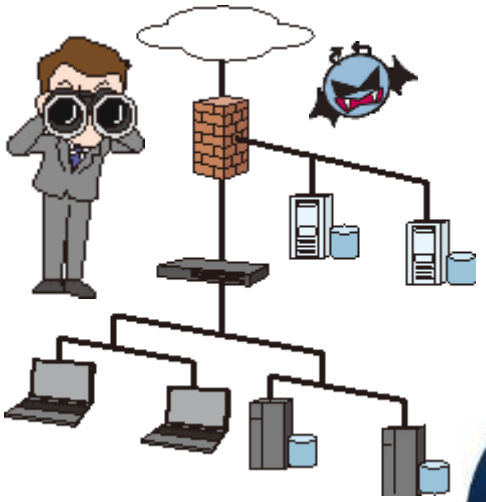
- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の早期検知】

- サーバーや PC、ネットワーク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】

- インシデント対応体制を整備し、対応する



【5位】機密情報等を狙った標的型攻撃

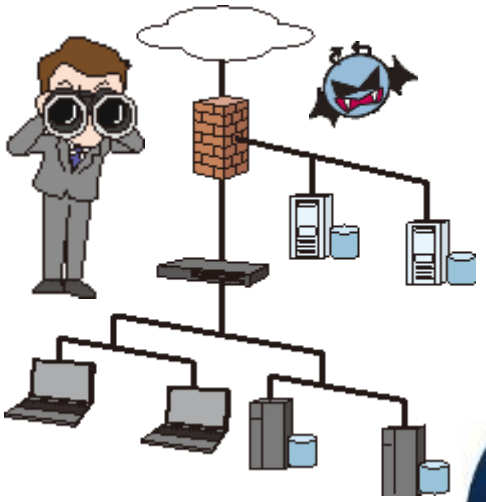
- **対策**
  - **組織(従業員、職員)**

【被害の予防／被害に備えた対策(通常、組織全体で実施)】

- メールの添付ファイル開封や、リンク、URL のクリックを安易にしない

【被害を受けた後の対応】

- インシデント対応体制を整備し、対応する



【6位】リモートワーク等の環境や仕組みを狙った攻撃

- リモートワークの実現に必要な環境や仕組みを狙ったサイバー攻撃が多発している
- 攻撃を受けると、マルウェア感染や情報漏えい等により、組織の事業が停止するおそれがある

【6位】リモートワーク等の環境や仕組みを狙った攻撃

♦ 攻撃手口/発生要因

・リモートワーク環境や管理体制の不備

- **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 等の製品やデバイスに存在する脆弱性や設定ミス等を悪用する
    - 端末や社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）や過去に漏えいしたアカウント情報を悪用する
    - VPN 機器やリモートデスクトップを介し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)や組織支給端末を標的にメール等を送りつけてマルウェアに感染させ、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て社内システムへ侵入、不正アクセスを行う

【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **2024年の事例/傾向①**
  - **VPN 機器を介した個人情報の流失**
    - 2024年7月、東京ガス、およびグループ子会社 TGES は、不正アクセスにより個人情報、約 416 万人分が流出した可能性があると公表した
    - 攻撃者は、TGES の VPN 機器から社内ネットワークに侵入しているが、VPN 機器の脆弱性有無などについては「セキュリティの関係で回答を控える」としている
    - ファイル暗号化や身代金要求といったランサムウェアの被害は確認されていない

【出典】 東京ガスエンジニアリングソリューションズへの不正アクセスについてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2024/07/23/023045
東京ガス子会社への不正アクセスは「VPN装置経由」、個人情報約416万人分漏洩か（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/24/01202/

【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **2024年の事例/傾向②**
  - **SIM 搭載ノート PC への侵入**
    - 2024年11月に石光商事は、同年9月に発生したランサムウェア被害の調査が完了したと、調査結果や対応状況を公表した
    - グループ会社の SIM カード搭載のノート PC に対して、リモートデスクトップ接続を介した不正アクセスが行われ、社内ネットワークに侵入された
    - 同社、国内グループ会社の一部サーバーに保存されていたデータが暗号化され、データが外部へ転送された痕跡を確認した
    - 流出データの範囲を特定し、個人情報等は含まれていなかったと報告している

【出典】 （開示事項の経過）ランサムウェア被害への対応状況に関するお知らせ（石光商事）
https://contents.xj-storage.jp/xcontents/AS90749/c1283b79/e663/48c3/9970/671ac391c2bc/140120241031508178.pdf

【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **2024年の事例/傾向③**
  - **狙われ続けるリモートワーク環境**
    - 警察庁によると、2024年のランサムウェア被害（100件）の感染経路の上位は以下のとおり
      - VPN 機器　　：55 件、全体の 55.0 %
      - リモートデスクトップ経由：31 件、全体の 31.0 %
    - これら２つの感染経路で全体の86.0%を占めている。
    - この割合を過去２年の通年で見ると、2022年は約80.4%、2023年は約81.7%を占めており、リモートワーク環境が依然として狙われている

【出典】 令和６年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/R6/R06_cyber_jousei.pdf
令和５年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/R5/R05_cyber_jousei.pdf
令和４年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/R04_cyber_jousei.pdf

【6位】リモートワーク等の環境や仕組みを狙った攻撃

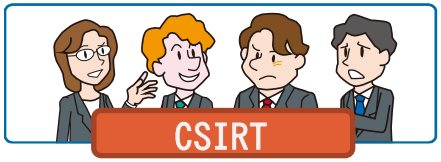
- **対策**
  - **個人(従業員)**

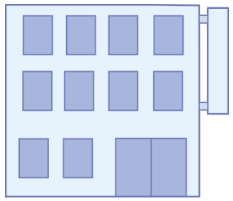
【被害の予防／被害に備えた対策】

- 組織のリモートワークの規則を遵守する
  (使用する端末、ネットワーク環境、作業場所等)
- 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
  - 上司、CSIRT、関係組織、公的機関等

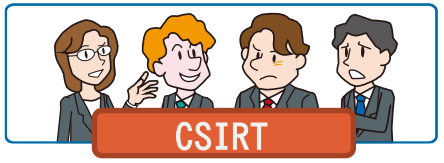


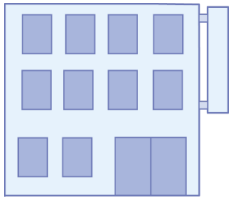


【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】





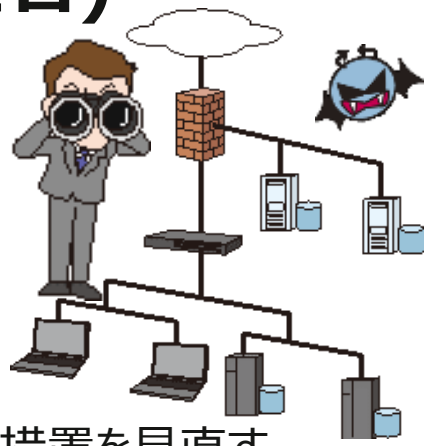
- インシデント対応体制を整備し、対応する
  - CISO を配置する
  - CSIRT を構築する
  - 報告フォーマットは決めておく
  - 有事の際の対応フローを確立、社員へ通知する
  - 対応フロー通りに実施できるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする
  - リモートワーク環境ならではの連絡方法や対応手順の作成と周知
- リモートワークのセキュリティポリシーを策定する

【参考】 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

【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の予防／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を採用する
- リモートワークの規程や運用規則を整備する
  - 組織支給端末と私有端末の違いも考慮する
  - リモートワーク開始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
- サーバーや PC、ネットワーク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スが行えない機器の使用を避ける
- ネットワークレベル認証(NLA)を行う
- 多要素認証(MFA)の設定を有効にする

【参考】 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

【6位】リモートワーク等の環境や仕組みを狙った攻撃

- **対策**
  - **組織(セキュリティ担当者、システム管理者)**

【被害の早期検知】

- サーバーや PC、ネットワーク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】

- インシデント対応体制を整備し、対応する

＜リモートワーク関連サイトの紹介＞

- IPA 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「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
- 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

【参考】 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

【7位】地政学的リスクに起因するサイバー攻撃

- 政治的に対立する周辺国に対し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
- 外交・安全保障上の対立をきっかけとして、嫌がらせや報復のためのサイバー攻撃を行うことがある
- 自国の産業の競争優位性を確保するために周辺国の機密情報等の窃取を目的とした攻撃や、自国の政治体制維持のために外貨獲得を目的とした攻撃もある

【7位】地政学的リスクに起因するサイバー攻撃

- 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、そのサービスを利用する人々を混乱させる

・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、標的組織に不正侵入をする

【7位】地政学的リスクに起因するサイバー攻撃

- 攻撃手口

・スピアフィッシング

- 特定の個人を標的にして、ソーシャルエンジアリング等を用いて情報収集を行い、収集した情報を基に標的へメールを送信する。添付ファイルを実行させたり、本文に記載したURLをクリックさせたりすることで、認証情報や機密データを窃取する。

【7位】地政学的リスクに起因するサイバー攻撃

- 攻撃手口

・ソーシャルエンジニアリング

- 標的組織の人間に対して、SNSを利用した接触等をして、標的組織から機密情報を詐取する

・偽情報の流布

- 国家を背景とした機関が、サイバー空間上の偽情報やフェイクによる影響工作等を行う

【7位】地政学的リスクに起因するサイバー攻撃

- **2024年の事例/傾向①**
  - **日本の自治体サービスへのサイバー攻撃**
    - 2024年10月、ロシアを支持するハッカー集団は日米軍事演習に対する抗議のため、日本の自治体や交通機関等のウェブサイトに対してサイバー攻撃を行ったことを SNS に投稿した
    - 山梨県の Web サイトは海外からアクセスが集中し、４ 時間ほど閲覧しにくい状態が続いた
    - 名古屋市、福岡空港、北海道のフェリー会社等のサイトも、一時的に閲覧しにくい状態になった

【出典】 ロシア系ハッカー集団 日本の自治体サイトなどサイバー攻撃か（NHK）
https://www3.nhk.or.jp/news/html/20241018/k10014613281000.html

【7位】地政学的リスクに起因するサイバー攻撃

- **2024年の事例/傾向②**
  - **LotL 戦術による標的型攻撃に注意**
    - 2024年6月、Living Off The Land 戦術（LotL)というサイバー攻撃が国際的に確認され注意喚起が行われた
      攻撃組織としてはVolt TyphoonやSalt Typhoon等がある
    - マルウェアを用いず標的の環境にある機能を悪用して攻撃する
    - 攻撃者は長期間潜伏し、活動を継続することもある
    - 企業や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る機器の脆弱性が狙われる

【出典】 Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/pdf/news/press/240625NISC_press.pdf
Operation Blotless攻撃キャンペーンに関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2024/at240013.html
”Typhoon” の真っ只中の嵐を乗り越える
https://gblogs.cisco.com/jp/2025/02/salt-typhoon-analysis/
Strengthening America’s Resilience Against the PRC Cyber Threats
https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

【7位】地政学的リスクに起因するサイバー攻撃

- **2024年の事例/傾向③**
  - **日本の個人や組織に対する標的型攻撃**
    - 2024年6月頃から日本の学術機関、シンクタンク、政治家、マスコミに関係する個人や組織に対するサイバー攻撃を、中国の関与が疑われるサイバー攻撃グループ MirrorFace が行っていたことを、2025年1月に警察庁および内閣サイバーセキュリティセンターが確認した
    - この攻撃では、ANEL と呼ばれるマルウェアをダウンロードするリンクを記載したメールが送信された
    - MirrorFace による組織的なサイバー攻撃活動は、主に日本の安全保障や先端技術に係る情報窃取を目的とした攻撃とし、注意喚起が行われた

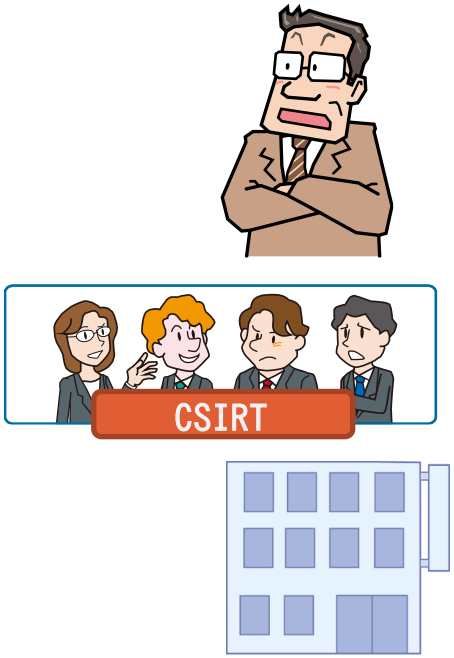
【出典】 MirrorFace によるサイバー攻撃について （注意喚起） （内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/pdf/news/press/20250108_MirrorFace.pdf

【7位】地政学的リスクに起因するサイバー攻撃

- **対策**
  - **組織(経営者層)**

【組織としての体制の確立】

- 地政学的リスクにおける情報収集をする
- 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を整備し、対応する
  - 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きるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【7位】地政学的リスクに起因するサイバー攻撃

- **対策**
  - **組織(システム管理者)**

【被害の予防】

- DDoS への対策
- 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する
  - 多要素認証等の強い認証方式を利用する
  - サーバーや PC、ネットワーク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
  - 適切なバックアップを行う

【7位】地政学的リスクに起因するサイバー攻撃

- **対策**
  - **組織(システム管理者)**

【被害に遭った後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応を行う
- Web サイトの停止および代替サーバーの稼働と告知を行う
- バックアップからのリストアを行う

【7位】地政学的リスクに起因するサイバー攻撃

- **対策**
  - **組織(従業員)**

【被害の予防／被害に備えた対策】

- パスワードの適切な運用を実施する
- 添付ファイルの開封やリンク・URL のクリックを安易にしない
- サーバーや PC、ネットワーク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、業務端末ではない仮想環境等で開く

【被害の早期検知】

- 不審なログイン履歴の確認を行う

【7位】地政学的リスクに起因するサイバー攻撃

- **対策**
  - **組織(従業員)**

【被害に遭った後の対策】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応をする

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- インターネット上のサービスに大量のアクセスを一斉に仕掛けて高負荷状態にさせる
- 回線帯域を占有し、サービスを利用不能にする
- 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

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **攻撃手口**

・高負荷をかける様々な攻撃

- **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 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**
  - TCP で使用する制御パケット（SYN、FIN、ACK 等）や UDP で使用するパケット等をサーバー等へ大量に送りつけて高負荷をかける

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **攻撃手口**

・高負荷をかける様々な攻撃

- **リフレクション（リフレクター）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 リフレクション攻撃、NTP リフレクション攻撃
- **DNS ランダムサブドメイン攻撃**
  - 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
- **DDoS 代行サービスの利用**
  - 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

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **2024年の事例/傾向①**
  - **日本航空や金融機関などへの DDoS 攻撃**
    - 2024年12月、日本航空は大規模な DDoS 攻撃を受けて一部のシステムに障害が発生した
    - この障害により当日の国内線、国際線のチケット販売が一時停止する等の影響が出た
    - 攻撃は社内外を繋ぐネットワーク機器に対して行われ、航空便を利用する日本郵便の郵便物や宅配便「ゆうパック」などの配達にも影響
    - 2024年年末にかけて、DDoS 攻撃により金融機関のインターネットバンキングが利用できない事態が発生し、2025年1月に入っても同様の攻撃は様々な企業に対して続けられていた

【出典】 日本航空で発生した大量データ送付起因のネットワーク障害についてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2024/12/30/154109
アカマイ、国内事業者向けでは過去最大規模のDDoS攻撃について解説（ZDNET Japan）
https://japan.zdnet.com/article/35228883/
2024年末からのDDoS攻撃被害と関連性が疑われるIoTボットネットの大規模な活動を観測（トレンドマイクロ）
https://www.trendmicro.com/ja_jp/research/24/l/iot-botnet-activity-ddos-attacks.html

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **2024年の事例/傾向②**
  - **サイバー攻撃の代行サービスを使った攻撃**
    - 2024年12月、警察庁は攻撃の代行をする海外サイトに攻撃の依頼をしたとして、中学生 2人を摘発していたことを明らかにした
    - 1人は、サイバー攻撃を代行する「IP ストレッサー」という海外サービスを使い、国内の企業や自身が通っている学校に関係するWeb サイトにサイバー攻撃を仕掛けた
    - もう 1人も同様に「IP ストレッサー」を使い、国内企業や外国の政府機関の Web サイトに DDoS 攻撃を仕掛けた

【出典】 「DDoS攻撃」を代行サイトに依頼疑い 中学生計2人を摘発 警察庁、Xなどで啓発強化」(ITmedia NEWS)
https://www.itmedia.co.jp/news/articles/2412/11/news172.html
サイバー攻撃の代行サービス使い企業攻撃か 中学生が書類送検 (NHK)
https://www3.nhk.or.jp/news/html/20241212/k10014665381000.html

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **対策**
  - **組織(Web サイトの運営者)**

【被害の予防】

- DDoS 攻撃の影響を緩和する CDN を利用する
- WAF、IDS/IPS、DDoS 対策サービスの導入する
- システムの冗長化等の軽減策を実施する
- ネットワークの冗長化として DDoS 攻撃の影響を受けない非常時用ネットワークを準備する
- Web サイト停止時の代替サーバーの用意と告知手段の整備をする

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **対策**
  - **組織(Web サイトの運営者)**

【被害を受けた後の対応】

- CSIRT へ連絡する
- WAF、IDS/IPS、DDoS 対策サービスの導入する
- 通信制御（攻撃元 IP アドレスからの通信をブロック等）をする
- 利用者への状況の告知をする
- 影響調査および原因の追究をする

【8位】分散型サービス妨害攻撃（DDoS攻撃）

- **対策**
  - **組織(サービス事業者)**

【被害の予防】

- 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）をする
- IoT 機器の脆弱性対策を行う
  - 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
  - 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を行う
  - 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 資産の顕在化、潜在リスクを把握し対策する

【9位】ビジネスメール詐欺

- 取引先や経営者とやりとりするようなビジネスメールを装う
- メールを巧妙に細工し、企業の金銭を取り扱う担当者を騙す
- 攻撃者が用意した口座へ送金させる
- 生成 AI を利用したビジネスメール詐欺が増加している

【9位】ビジネスメール詐欺

- 攻撃手口

・BEC の準備としての情報窃取

- 標的組織の個人情報を窃取する
- 標的組織の経営者等になりすまし、組織内の他の従業員の個人情報等を窃取する
- マルウェア感染や不正ログインなどにより、個人情報を窃取する
- 取引に関わるメールのやり取りを盗聴し、取引や請求に関わる情報や関係者の情報を入手する

BEC：ビジネスメール詐欺／Business E-mail Compromise

【9位】ビジネスメール詐欺

- 攻撃手口

・偽装、なりすまし、悪用、窃取

- 取引先へなりすまし、振込口座を差し替えた請求書に金銭を振り込ませる
- 経営者等へなりすまして、金銭を振り込ませる
- 社外の権威ある第三者へなりすまして、金銭を振り込ませる

【9位】ビジネスメール詐欺

- **2024年の事例/傾向①**
  - **ディープフェイクによる映像や音声のなりすまし**
    - 2024年1月、多国籍企業にて約 37.5 億円が詐取される事件が発生
    - 英国本社 CFO（最高財務責任者）になりすまし、香港支社の従業員へ秘密の取引に関するメールとビデオ会議の URL 付きメールを送信した
    - 香港支社の従業員は、URLよりビデオ会議に参加し、ディープフェイクにより生成された CFO の映像や声、同僚の映像を信じてしまった
    - ビデオ会議で、香港支社の資金を振込むように指示を受けたこの従業員は、不審に思い質問したが、CFO に叱責されたため、最終的に送金してしまった
    - その後、詐欺だと気づき警察に通報したが、既に資金は海外に送付され、回収できなかった

【出典】 ビデオ会議の相手は知らない他人だった。香港で37億円のディープフェイク詐欺事件、被害を防止する3ヶ条（レバテックラボ）
https://levtech.jp/media/article/column/oversea/detail_521/
会計担当が38億円を詐欺グループに送金、ビデオ会議のCFOは偽物 香港（2024年2月5日）（CNN.co.jp）
https://www.cnn.co.jp/world/35214839.html

【9位】ビジネスメール詐欺

- **2024年の事例/傾向②**
  - **生成 AI を利用した BEC の増加**
    - 2024年8月、Vipre Security Group は、過去 1 年間で BEC が急増したと報告した
    - 同社はこの 1 年に世界中で電子メール 18 億通を処理し、2 億 2,600 万件のスパムメッセージを検出した
    - ブロックされたスパムメールの 49 %が BEC であり、標的は CEO、次いで人事部門と IT 部門が多かった
    - BEC の 40 %は AI によって生成されていた

【出典】 BEC Attacks Surge 20% Annually Thanks to AI Tooling（Infosecurity Magazine）
https://www.infosecurity-magazine.com/news/bec-attacks-surge-20-annually-ai/

【9位】ビジネスメール詐欺

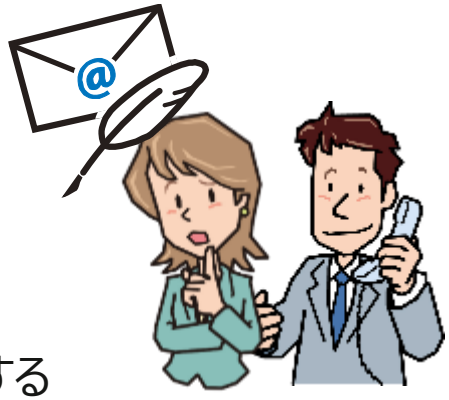
- **対策**

【被害の予防／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
- BEC への認識と理解を深める
- ガバナンスが機能する業務フローを構築する
- 振込依頼がメールであった場合、電話等の複数の手段での確認を行う
- メールの電子署名を付与(S/MIMEやPGP)する
- 送信ドメイン認証を導入する
- 認証を適切に運用する

＜メールの真正性を確認＞

- メールだけでなく複数の手段での事実確認を行う
- 普段とは異なるメールや判断を急がせるメールに注意する



【9位】ビジネスメール詐欺

- **対策**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応をする
- 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

【10位】不注意による情報漏えい等

- 従業員の不注意等によって意図せず機密情報を漏えい
- 情報漏えいすることによる社会的信用の失墜、経済的損失、漏えいした情報の悪用による二次被害

【10位】不注意による情報漏えい等

- **要因**

・情報取扱者本人の問題

- **情報取扱者の情報リテラシー・モラルの低さ**
  - 情報の機密性や重要性等への理解やモラルが不十分なため、不用意に外部へ情報漏えいしてしまう
    - 重要情報が記載されたメールの宛先を間違う、メール添付ファイルを取り違える
    - 重要情報が入った情報端末・記録媒体・紙を紛失する
    - 重要情報を私的に利用して外部の Web サイト等に公開する
- **情報取扱い時の本人の状況**
  - 体調不良や多忙等により、注意力が散漫になり、メールの誤送信等による情報漏えいを起こしてしまう

【10位】不注意による情報漏えい等

- 要因

・組織の規程および情報の取扱い手順の不備

- 外部に持ち出す情報や記録媒体の暗号化確認、持ち出す際の申請・承認手順に不備があると漏えいが起きやすい

・誤送信を当て込んだ偽ドメインの存在

- 組織が利用しているドメインと似たドメインのメールアドレス(ドッペルゲンガードメイン)を、第三者が悪意をもってあらかじめ準備している
  - 従業員がそのメールアドレスに誤送信したタイミングで情報が漏えいする

【10位】不注意による情報漏えい等

- **不注意による情報漏えいの例**
  - メールの誤送信(宛先誤り、To/Cc/Bcc の設定間違い、添付ファイル取り違え等)
  - Web サイトの設定不備(機密情報のマスキングの不備、公開ファイルや参照権限の誤り、クラウドの設定誤り等)
  - 外部サイトへの安易な機密情報の入力
  - 機密情報を保存した情報端末(PC やスマートフォン等)、記録媒体(USB メモリー等)の紛失
  - 重要書類(紙媒体)の紛失

【10位】不注意による情報漏えい等

- **2024年の事例/傾向①**
  - **委託先が業務に使用した私物 HDD のデータを削除せず廃棄**
    - 2024年6月、BANDAI SPIRITS が会員の個人情報漏えいの可能性について発表した
    - 委託先従業員が、2019年11月に私物の外付け HDD を業務に使用し、顧客情報が含まれるデータを消去せず2023年12月にこの HDD を 廃棄した
    - 2024年4月この HDD を入手した第三者がデータの残存を指摘した

【出典】 委託先が私物HDD使用、データ削除せず廃棄「プレミアムバンダイ」顧客情報漏えいの可能性（ITmedia）
https://www.itmedia.co.jp/news/articles/2406/14/news130.html

【10位】不注意による情報漏えい等

- **2024年の事例/傾向②**
  - **社内利用が前提のツールを顧客に送付し、人事情報が流出**
    - 2024年7月、帝国データバンクは「個人情報流出に関するお詫びとご報告」を公表した
    - 複数の社員が社内ルールに反し、見積書作成に使用したツールを見積書と一緒にメールで送付していた
    - ツールには人事情報（退職者や委託先スタッフ等の個人情報）が組み込まれており、容易に再表示できる状態であった
    - 二次被害のおそれが高い情報は含まれていなかった

【出典】 過去に当社と雇用関係にあった従業員、企業調査スタッフ、派遣スタッフの皆さまへ（株式会社帝国データバンク）
https://www.tdb.co.jp/newsroom/news/5qv35g4a1w/

【10位】不注意による情報漏えい等

- **2024年の事例/傾向③**
  - **教育機関における意図しない個人情報漏えい**
    - 2024年5月に東京都教育委員会は、都立高校の教諭が公開範囲を制限せず、Teams に電子データをアップロードしたため、個人情報が漏えいしていたことを発表した
    - また2024年7月に目黒区は、小学校（1 校）の体力テスト結果記録アプリのログイン情報一覧等が誰でも閲覧可能な状態になっていたことが判明し、個人情報漏えい事案として公表した

【出典】 都立高等学校における個人情報の漏えいについて（東京都教育委員会）
https://www.kyoiku.metro.tokyo.lg.jp/information/press/2024/05/2024053105
区立小学校における個人情報の漏えいについて（目黒区）
https://www.city.meguro.tokyo.jp/kyouikushidou/kosodatekyouiku/gakkoukyouiku/ed20240729.html

【10位】不注意による情報漏えい等

- **対策**
  - **組織(当事者)**

【被害の予防／被害に備えた対策】

- 自動化やシステム化により、作業負荷やヒューマンエラーの回避に努める
- 業務委託先に対するセキュリティ基準、選定基準を定め、委託先の情報管理を徹底させる
- 情報リテラシー、モラルを向上させる
- 確認プロセスの策定とこれに基づく運用を行う
- 特定の担当者に業務を集中させない体制整備
- 取扱い情報の格付けとそれに応じた運用を行う
- 情報の保護(暗号化、認証)、機密情報の格納場所の把握、可視化
- DLP(情報漏えい対策)製品を導入する
- 情報を持ち出す際の運用を検討する　・メールの誤送信対策等の実施する
- 業務用携帯端末の紛失に備えた探索機能の有効化を行う
- HDD の廃棄の際、復旧できない方法での消去を周知し、徹底する

【10位】不注意による情報漏えい等

- **対策**
  - **組織(当事者)**

【被害の早期検知】

- 問題発生時の内部報告体制の整備
- 外部からの連絡受付窓口の設置

【被害に遭った際の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する

【10位】不注意による情報漏えい等

- **対策**
  - **組織(被害者)**

【被害に遭った際の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

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を実践

・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

そのため、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

- 対策の種類単位で見ると、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、より効率的に広範囲な対策を進めることが可能

※情報セキュリティ10大脅威 2025 のページで共通対策の詳細な解説資料を公開中

共通対策
認証を適切に運用する
情報リテラシー、モラルを向上させる
添付ファイル開封や、リンク、URL のクリックを安易にしない
適切な報告/連絡/相談を行う
インシデント体制の整備し対応を行う
サーバーや PC、ネットワークに適切なセキュリティ対策を行う
適切なバックアップ運用を行う

詳細な資料のダウンロード

- 情報セキュリティ10大脅威　2025

  本資料に関する詳細な内容はWebサイトをご覧ください

https://www.ipa.go.jp/security/10threats/10threats2025.html

※こちらの QR コードをスマートフォンの
QR コードリーダーアプリで読み込む
ことでもアクセスできます