



2023年～2025年  
情報セキュリティ10大脅威  
[組織編]から見る  
セキュリティトレンド

2026年1月14日  
インフォテック株式会社

本資料は、2025年4月時点での情報をもとに作成をしております。

# 「情報セキュリティ10大脅威[組織編]」とは

- 「情報セキュリティ10大脅威 (※1)」は、前年に発生したセキュリティ事案を元に、独立行政法人 情報処理推進機構(以下、IPAと記載する)が、候補を選定、専門家による審議投票を経て決定されるものです
- 組織に対する脅威と個人に対する脅威、2つの観点でまとめられておりますが、本資料では組織に対する脅威に焦点を当てて、セキュリティトレンドを分析しています



※1 独立行政法人情報処理推進機構(IPA) 情報セキュリティ10大脅威 <https://www.ipa.go.jp/security/10threats/index.html>

# 過去3年間の「情報セキュリティ10大脅威[組織編]」動向

ランサムウェアによる被害は3年連続1位、サプライチェーンの弱点を悪用した攻撃は3年連続2位、内部不正による情報漏えい等の被害、標的型攻撃による機密情報の窃取も継続的に上位に位置しています

順位	2023年 (※2)	2024年 (※3)	2025年 (※4)
1	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等の被害	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい等の被害	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等の被害
5	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	標的型攻撃による機密情報の窃取
6	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃
7	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加	地政学的リスクに起因するサイバー攻撃
8	脆弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃(DDoS攻撃)
9	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺による金銭被害
10	犯罪のビジネス化(アンダーグラウンドサービス)	犯罪のビジネス化(アンダーグラウンドサービス)	不注意による情報漏えい等の被害

(※2) 独立行政法人情報処理推進機構(IPA)情報セキュリティ10大脅威2023 <https://www.ipa.go.jp/security/10threats/10threats2023.html>

(※3) 独立行政法人情報処理推進機構(IPA)情報セキュリティ10大脅威2024 <https://www.ipa.go.jp/security/10threats/10threats2024.html>

(※4) 独立行政法人情報処理推進機構(IPA)情報セキュリティ10大脅威2025 <https://www.ipa.go.jp/security/10threats/10threats2025.html>

# 上位の脅威と求められる対策

過去3年のランキングで上位を占める4つの脅威について、概要、脅威による被害、攻撃の手法、求められる対策の4つの観点から説明します

- ランサムウェアによる被害
- サプライチェーンの弱点を悪用した攻撃
- 内部不正による情報漏えい等の被害
- 標的型攻撃による機密情報の窃取



# ランサムウェアによる被害



## 脅威の概要

企業のシステム停止およびデータの暗号化と窃取を行い、復旧のための身代金の要求や窃取した機密データの公開による脅迫を行う攻撃

## 脅威による被害

身代金の支払いによる金銭被害だけでなく、業務停止による売り上げの減少、機密情報の漏洩、社会的信用の失墜といった被害をもたらす

## 攻撃の手法

- VPNルータなどのネットワーク機器の脆弱性の悪用
- クラウドサービスやリモートデスクトップの設定不備をついた侵入
- 悪意のあるメールの添付ファイルやリンク

## 求められる対策

複数の手法を組み合わせるため、単一の対策ではなく複数の技術を組み合わせた多層防御や、社員教育などの対策が必要

# サプライチェーンの弱点を悪用した攻撃



## 脅威の概要

企業活動を行う上で必要な繋がり(業務の委託、IT機器やソフトウェアの利用など)を悪用し、つながりの中で脆弱な個所を足掛かりに、被害・影響を及ぼす攻撃

## 脅威による被害

業務の停止による売り上げの減少や、機密情報の漏洩、社会的信用の失墜といった被害をもたらす

## 攻撃の手法

- 攻撃の標的とする組織の子会社や委託先の会社を攻撃し、それを足掛かりにした標的への侵入
- IT/IoT機器やサービス・ソフトウェアを改ざんしマルウェアを仕込む

## 求められる対策

サプライチェーンの可視化を行ったうえで、子会社・委託先やIT/IoT機器・サービスの評価・管理体制を強化することが求められる

# 内部不正による情報漏えい等の被害



## 脅威の概要

従業員や元従業員などの関係者による、意図的な機密情報の持ち出し、漏洩、削除といった不正行為

## 脅威による被害

漏洩した情報の重要度や規模によっては、社会的信用の失墜、顧客への損害賠償や損失の補填といった金銭的損失が生じる可能性がある

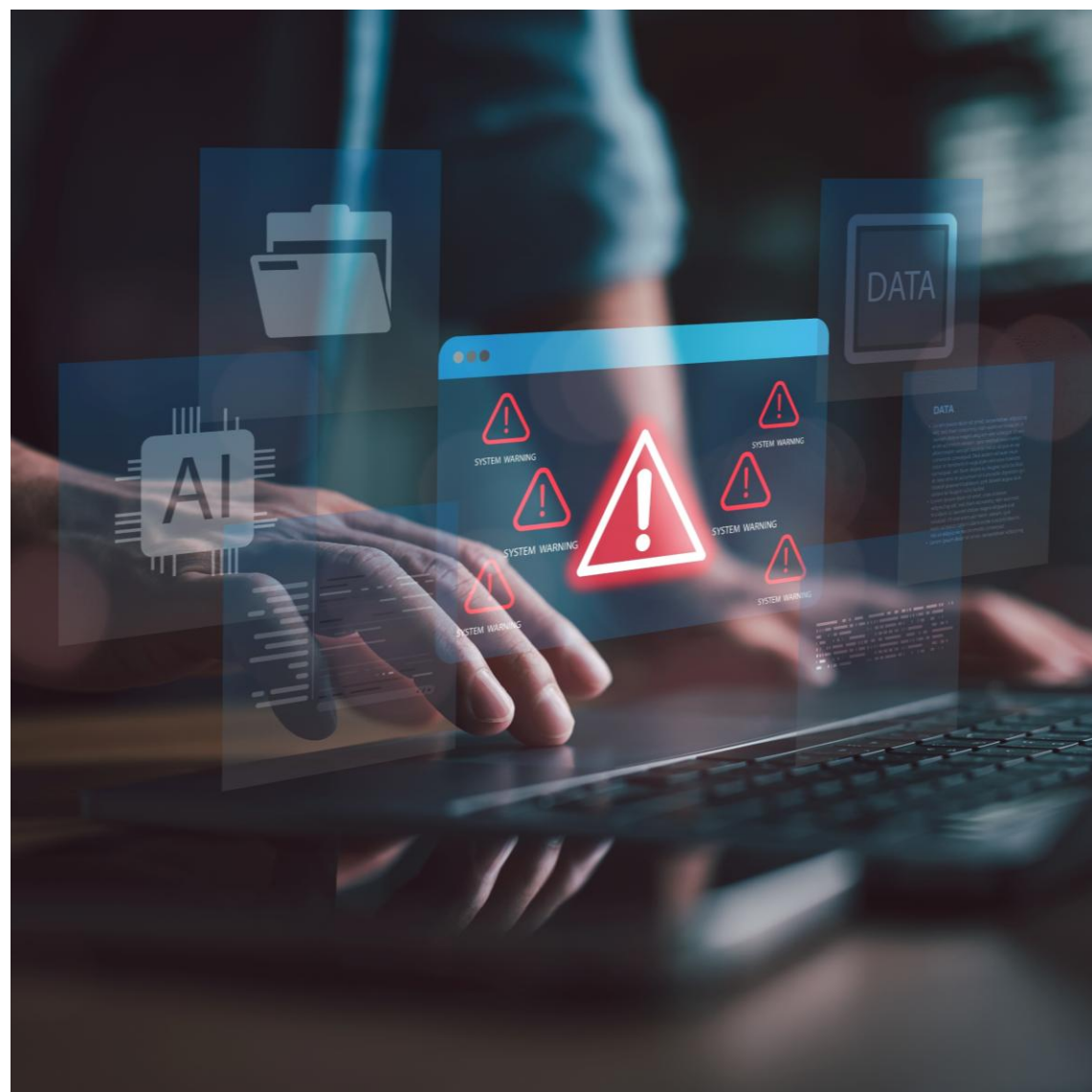
## 攻撃の手法

- 必要以上のアクセス権限の悪用
- 離職後も有効なままのアカウントの悪用
- 管理外のUSBメモリ等の外部記憶媒体による持ち出し

## 求められる対策

企業にて利用する製品・サービスについて、アカウントへの適切な権限付与やログの監視、外部記憶媒体接続の防止などの対策が求められる

# 標的型攻撃による機密情報の窃取



## 脅威の概要

特定の組織(民間企業、官公庁、団体等)を狙う攻撃のことであり、機密情報等の窃取や業務妨害を目的としている

## 脅威による被害

被害を受けた場合は組織の事業継続への影響だけでなく、国家の安全保障に影響を及ぼす可能性がある

## 攻撃の手法

- クラウドサービスやリモートデスクトップの設定不備をついた侵入
- 悪意のあるメールの添付ファイルやリンク
- 標的組織が頻繁に利用するWebサイトの改ざん(水飲み場攻撃)

## 求められる対策

複数の手法を組み合わせるため、単一の対策ではなく複数の技術を組み合わせた多層防御や、社員教育などの対策が必要

## まとめ

ランキング上位にある脅威について、攻撃の手法は1つでなく、様々な手法が使われていることがわかります。

対策を講じるにあたって、まずは「自社の資産や利用している製品・サービスの整理」「セキュリティに関する情報収集」から始めてみてはいかがでしょうか。

些細なことでもよいので、できることから始めて、脅威に備えることが大切です。



# セキュリティは後付けでは守れない

セキュリティ対策は、システム開発の設計段階から対策することが重要です。  
 インフォテックが提供するセキュリティソリューションは  
**Security By Design x DevSecOps**をベースに構築、確かな安心をお届けします。

## Security By Design

システム設計段階からセキュリティを組み込んで開発を行います  
 CIS Benchmarks® (\*1)やCIS Controls® (\*2)を活用し、設計・開発・保守におけるセキュリティの標準化と継続的な評価改善を可能とします

## DevSecOps

保守フェーズではDevSecOpsに基づき、PDCAサイクルにWebアプリケーション脆弱性診断(\*3)やクラウド/SaaSのセキュリティ態勢管理(CSPM(\*4)・SSPM(\*5))を組み込むことで、運用の継続的な改善をご支援します

### お問い合わせ・資料請求はこちらから

インフォテック株式会社HP お問い合わせ窓口

<https://www.iftc.co.jp/contact/form/?kind=2>

お電話でのお問い合わせ

03-3348-0360 ※【受付時間】土日祝日を除く平日の9:00~17:30

- (\*1) OSやクラウドなどのITシステムに対する安全な設定方法をまとめたガイドラインで、セキュリティ強化や監査対応に活用
- (\*2) サイバー攻撃から組織を守るための18の優先度付きセキュリティ対策で、実践的かつ段階的な導入が可能なベストプラクティス集
- (\*3) スリーシェイク社の「Securify」を用いた自動診断
- (\*4) クラウド環境の設定ミスや脆弱性を検出・修正し、セキュリティとコンプライアンスを維持する管理ツール
- (\*5) SaaSアプリのセキュリティ設定を監視・管理し、データ漏洩や権限の過剰付与などのリスクを防ぐための管理ツール

「CIS®」、「CIS Benchmarks®」、「CIS Controls®」、「CIS SecureSuite®」、「CIS-CAT®」は、Center for Internet Security, Inc.(CIS)の米国およびその他の国における登録商標です。本記事は、CISの商標またはサービスに関する公式な提携、認定、スポンサーシップを示すものではありません。