企業に求められるサイバー対策セミナー

誰もがサイバー攻撃の標的に！
攻撃の手口・対策・事前対応について

2026年3月9日

MS&ADインターリスク総研株式会社
MS&AD INSURANCE GROUP

目次

１．はじめに ～サイバーセキュリティ対策の重要性～

深刻な被害をもたらすサイバー攻撃

グローバルのみならず、日本国内においてもサイバー攻撃が多発しており、大きな被害が発生しています。

英ジャガー、緊急融資4000億円を銀行に要請－サイバー攻撃で生産停止

Phoebe Sedgman
2025年9月29日 13:32 JST

→ スタンダードチャータードやシティ、MUFGが緊急融資枠提供へ－ET
→ 別枠の融資15億ポンドには英政府の保証付き、今後5年かけて返済へ

インドのタタ・モーターズ傘下の英自動車メーカー、ジャガー・ラ（JLR）は、サイバー攻撃による生産停止で資金繰りが悪化する中、20億ポンド（約4000億円）の緊急融資を要請した。インド紙エコノミック・タイムズ（ET）が報じた。

同紙によると、英銀スタンダードチャータード、米シティグループ、MUFGが緊急融資枠を提供することに。後、貸付債権を売却またはシンジケート化してより多くの金融機関に。期間1年半の融資枠には確約されたバックストップ措置が設定。が収益損失を乗り越えるための流動性を確保していることを示す狙う。

アサヒGHDにランサム攻撃　DX下の「全停止」説明責任

編集委員　須藤龍也

Nikkei Views　＋フォローする
2025年10月6日 17:43 [会員限定記事]

保存

アサヒグループホールディングス（GHD）に対するランサムウエア（ウイルス）によるサイバー攻撃の被害は、公表から1週間が過ぎても復立っていない。デジタルトランスフォーメーション（DX）の進展は被を難しくし、システムの「全停止」につながるリスクをはらむ。専門害に見舞われた状況に似ている」と指摘するが、取引先やステークホめな情報発信は不可...

ニュース

アスクルがサイバー攻撃で取引先企業の顧客情報漏洩の可能性、注意を喚起

玄 忠雄　日経クロステック／日経コンピュータ
2025.11.14

IT

シンプル表示　印刷　保存

アスクルは2025年11月14日、グループ会社のASKUL LOGISTが提供する物流支援サービス「3PL（サードパーティ・ロジスティクス）」を利用する取引先企業の顧客情報が外部に流出した可能性があると公表した。同年10月19日に発生したランサムウエア攻撃による一連のシステム障害に関する調査結果の1つとして明かした。

流出の可能性がある情報は、取引先から委託された物流業務に関する出荷・配送データの一部で、利用者の配送先住所、氏名、電話番号、注文商品情報が含まれる。メールアドレス及びクレジットカード情報は含まれていない。

出典：「英ジャガー、緊急融資4000億円を銀行に要請－サイバー攻撃で生産停止」2025年9月29日公開（Bloomberg）
https://www.bloomberg.co.jp/news/articles/2025-09-29/T3BTG8GOYMTE00
出典：「アサヒGHDにランサム攻撃　DX下の「全停止」リスクと説明責任」2025年10月6日公開（日経新聞）
https://www.nikkei.com/article/DGXZQOCD0600L0W5A001C2000000/
出典：「アスクルがサイバー攻撃で取引先企業の顧客情報漏洩の可能性、注意を喚起」2025年11月14日公開（日経クロステック）
https://xtech.nikkei.com/atcl/nxt/news/24/02975/

クイズ

2025年度上半期、ランサムウェア攻撃にあった中小企業の割合はどれぐらいでしょうか？

※警察庁統計

A　3%

B　30%

C　66%

D　70%

クイズ

2025年度上半期、ランサムウェア攻撃にあった中小企業の割合はどれぐらいでしょうか？

※警察庁統計

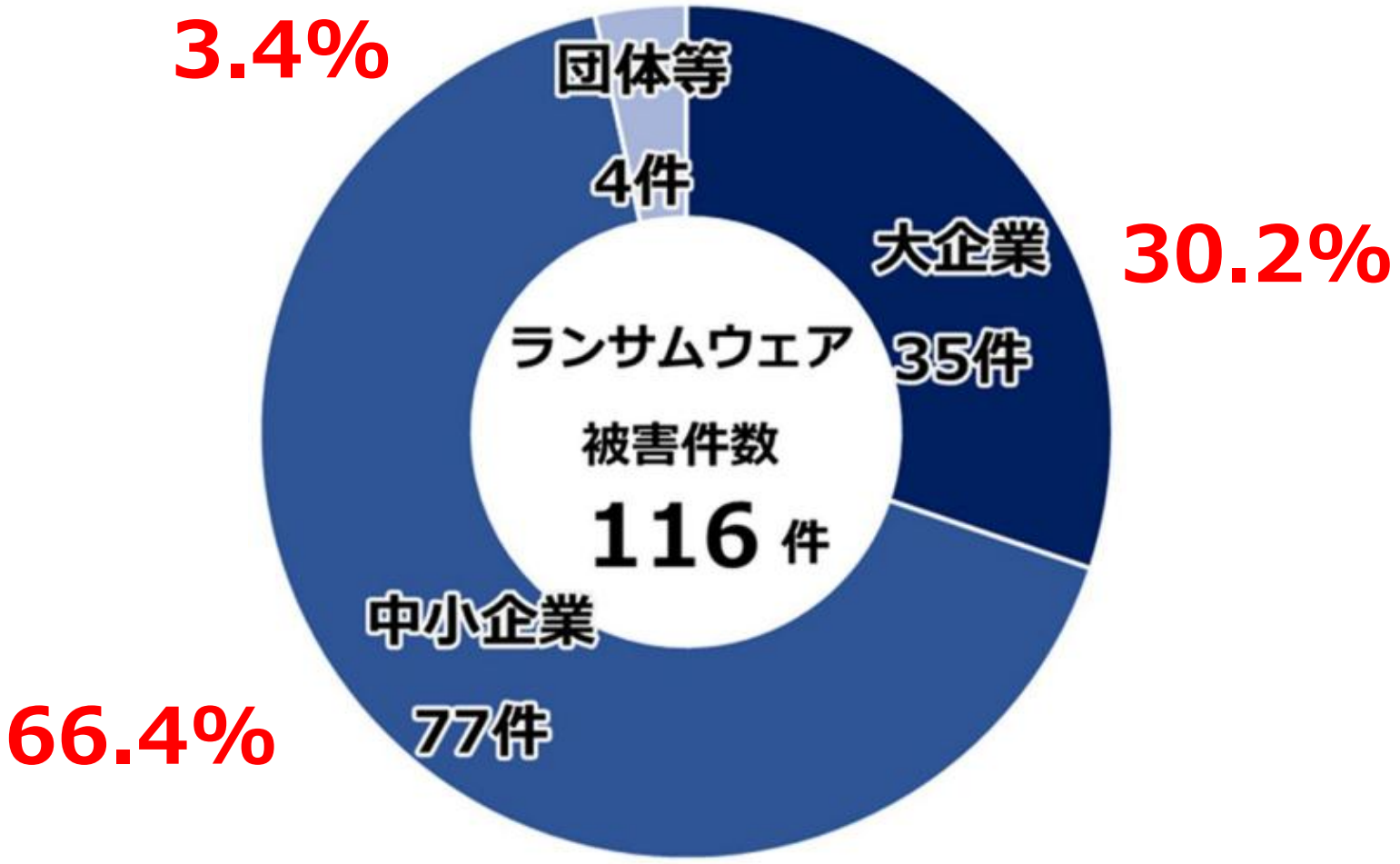
A　3%

B　30%

C　66%

D　70%

ランサムウェアの被害に関する警察庁の統計



出典：「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」2025年9月公開（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

サイバー攻撃は対岸の火事ではない

最近発生したサイバー攻撃被害事例（報告された事例の一部を掲載）

報告年月	被害組織	サイバー攻撃を受けて発生した被害
2026年1月	鉄道	グループ会社のネットワーク環境が第三者による不正アクセスを受け、グループ会社各社（58社）の従業員情報が漏えい
2025年12月	自動車	業務委託先のシステムが不正アクセスを受け、顧客情報約2万1000人の個人情報が流出した可能性があると報告
2025年11月	製造業	連結子会社の社内サーバーが不正アクセスを受け、ランサムウェアに感染しシステム障害が発生した
2025年11月	行政サービス	開発を委託していた企業の再委託先において不正アクセスが行われ、一部利用者の情報が漏えいした可能性があると報告
2025年10月	製造業	ランサムウェアに感染し、一部業務の停止および情報漏えいが発生、対応に数千万円の費用が発生した
2025年9月	行政サービス	業務を委託していた企業がサポート詐欺による不正アクセスを受け、利用者約800人の個人情報が漏えいしたと報告
2025年7月	製造業	ランサムウェア攻撃を受け、クラウド上の基幹システムが暗号化され被害が発生、個人情報の漏洩の可能性もあると報告
2025年6月	通信業	業務委託先で不正アクセスがあり、顧客情報13万7156件が外部に漏えいしている可能性があると報告
2025年5月	製造業	サーバーが外部からの攻撃を受けランサムウェアに感染、影響を最小限にするためネットワークの遮断等の措置を行ったため業務停止等の影響が発生
2025年4月	製造業	海外グループ会社がランサムウェア攻撃を受け、同グループ会社の顧客情報が外部へ流出した可能性があると報告
2025年4月	エネルギー	ランサムウェア攻撃を受け、クラウド上に保存していた業務データの一部が消失していることが発覚、身代金を要求される
2025年3月	エネルギー	顧客情報の管理を委託している子会社が不正アクセスを受け、約11万件の契約者の個人情報が流出した可能性があると報告
2025年3月	製造業	セキュリティ製品の設定に不備があり、ランサムウェア感染、メールサーバー、ドメインコントローラー、財務システムが使用不能となり、社内の機密情報が漏えいした可能性
2025年2月	製造業	ランサムウェア攻撃を受け、機密情報や最大約200万件の個人情報が外部へ流出した可能性があると報告
2025年1月	建設業	業務を委託している事業者が電子メールを誤送信し、同社の従業員の個人情報1082件が漏えいしたと報告
2025年1月	製造業	ランサムウェア攻撃を受け、15万7203件の個人情報が流出した可能性があると報告

…など他多数

サイバー攻撃は対岸の火事ではない

最近発生したサイバー攻撃被害事例（報告された事例の一部を掲載）

報告年月	被害組織	サイバー攻撃を受けて発生した被害
2026年1月	鉄道	グループ会社のネットワーク環境が第三者による不正アクセスを受け、グループ会社各社（58社）の従業員情報が漏えい
2025年12月	自動車	業務委託先のシステムが不正アクセスを受け、顧客情報約2万1000人の個人情報が流出した可能性があると報告
2025年11月	製造業	連結子会社の社内サーバーが不正アクセスを受け、ランサムウェアに感染しシステム障害が発生した
2025年11月	行政サービス	開発を委託していた企業の再委託先において不正アクセスが行われ、一部利用者の情報が漏えいした可能性があると報告
2025年10月	製造業	ランサムウェアに感染し、一部業務の停止および情報漏えいが発生、対応に数千万円の費用が発生した
2025年9月	行政サービス	業務を委託していた企業がサポート詐欺による不正アクセスを受け、利用者約800人の個人情報が漏えいしたと報告
2025年7月	製造業	ランサムウェア攻撃を受け、クラウド上の基幹システムが暗号化され被害が発生、個人情報の漏洩の可能性もあると報告
2025年6月	通信業	業務委託先で不正アクセスがあり、顧客情報13万7156件が外部に漏えいしている可能性があると報告
2025年5月	製造業	サーバーが外部からの攻撃を受けランサムウェアに感染、影響を最小限にするためネットワークの遮断等の措置を行ったため業務停止等の影響が発生
2025年4月	製造業	海外グループ会社がランサムウェア攻撃を受け、同グループ会社の顧客情報が外部へ流出した可能性があると報告
2025年4月	エネルギー	ランサムウェア攻撃を受け、クラウド上に保存していた業務データの一部が消失していることが発覚、身代金を要求される
2025年3月	エネルギー	顧客情報の管理を委託している子会社が不正アクセスを受け、約11万件の契約者の個人情報が流出した可能性があると報告
2025年3月	製造業	セキュリティ製品の設定に不備があり、ランサムウェア感染、メールサーバー、ドメインコントローラー、財務システムが使用不能となり、社内の機密情報が漏えいした可能性
2025年2月	製造業	ランサムウェア攻撃を受け、機密情報や最大約200万件の個人情報が外部へ流出した可能性があると報告
2025年1月	建設業	業務を委託している事業者が電子メールを誤送信し、同社の従業員の個人情報1082件が漏えいしたと報告
2025年1月	製造業	ランサムウェア攻撃を受け、15万7203件の個人情報が流出した可能性があると報告

…など他多数

サイバー攻撃は対岸の火事ではない

最近発生したサイバー攻撃被害事例（報告された事例の一部を掲載）

報告年月	被害組織	サイバー攻撃を受けて発生した被害
2026年1月	鉄道	グループ会社のネットワーク環境が第三者による不正アクセスを受け、グループ会社各社（58社）の従業員情報が漏えい
2025年12月	自動車	顧客情報が漏えいした可能性があると報告
2025年11月	製造業	連結子会社の社内サーバーが不正アクセスを受け、ランサムウェアに感染しシステム障害が発生した
2025年11月	行政サービス	開発を委託している事業者が電子メールを誤送信し、利用者の情報が漏えいした可能性があると報告
2025年10月	製造業	ランサムウェアに感染し、一部業務の停止および情報漏えいが発生、対応に数千万円の費用が発生した
2025年9月	行政サービス	利用者の情報が漏えいしたと報告
2025年7月	製造業	ランサムウェア攻撃を受け、クラウド上の基幹システムが暗号化され被害が発生、個人情報の漏洩の可能性もあると報告
2025年6月	通信業	業務委託先で不正アクセスがあり、顧客情報13万7156件が外部に漏えいしている可能性があると報告
2025年5月	製造業	サーバーが外部からの攻撃を受けランサムウェアに感染、影響を最小限にするためネットワークの遮断等の措置を行ったため業務停止等の影響が発生
2025年4月	製造業	顧客情報が流出した可能性があると報告
2025年4月	エネルギー	ランサムウェア攻撃を受け、クラウド上に保存していた業務データの一部が消失していることが発覚、身代金を要求される
2025年3月	エネルギー	顧客情報が流出した可能性があると報告
2025年3月	製造業	セキュリティ製品の設定に不備があり、ランサムウェア感染、メールサーバー、ドメインコントローラー、財務システムが使用不能となり、社内の機密情報が漏えいした可能性
2025年2月	製造業	顧客情報が流出した可能性があると報告
2025年1月	建設業	業務を委託している事業者が電子メールを誤送信し、同社の従業員の個人情報1082件が漏えいしたと報告
2025年1月	製造業	ランサムウェア攻撃を受け、15万7203件の個人情報が流出した可能性があると報告

昨今は中小企業のような委託先がサイバー攻撃に遭い、委託元まで影響が及ぶケースが多い

大企業に限らず、中小企業含むすべての組織がサイバー攻撃を受ける可能性がある

…など他多数

２．サイバー攻撃の実態と特徴（トレンド）

IPA情報セキュリティ10大脅威　過去5年の推移

社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものをIPAが毎年公表している。

	2022	2023	2024	2025	2026
1位	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	ランサムウェアによる被害	ランサム攻撃による被害
2位	標的型攻撃による機密情報の窃取	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	サプライチェーンや委託先を狙った攻撃	サプライチェーンや委託先を狙った攻撃
3位	サプライチェーンの弱点を悪用した攻撃	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	システムの脆弱性を突いた攻撃	AIの利用をめぐるサイバーリスク
4位	テレワーク等ニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	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	システムの脆弱性を悪用した攻撃
5位	内部不正による情報漏えい	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)	機密情報等を狙った標的型攻撃	機密情報を狙った標的型攻撃
6位	脆弱性対策情報の公開に伴う悪用増加	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	リモートワーク等の環境や仕組みを狙った攻撃	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	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	内部不正による情報漏えい等
8位	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	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）	リモートワーク等の環境や仕組みを狙った攻撃
9位	予期せぬIT基盤の障害に伴う業務停止	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	DDoS攻撃（分散型サービス妨害攻撃）
10位	不注意による情報漏えい等の被害	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	ビジネスメール詐欺

出典：「情報セキュリティ10大脅威 2026」2026年1月29日公開（独立行政法人情報処理推進機構）よりMS&ADインターリスク総研が作成
https://www.ipa.go.jp/security/10threats/10threats2026.html

IPA情報セキュリティ10大脅威　過去5年の推移

社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものをIPAが毎年公表している。

	2022	2023	2024	2025	2026
1位	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	ランサムウェアによる被害	ランサム攻撃による被害
2位					
3位	サプライチェーンの弱点を悪用した攻撃	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	システムの脆弱性を突いた攻撃	AIの利用をめぐるサイバーリスク
4位	テレワーク等ニューノーマルな働き方を狙った攻撃			による情報漏えい等	システムの脆弱性を悪用した攻撃
5位	内部不正による情報漏えい	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)	機密情報等を狙った標的型攻撃	機密情報を狙った標的型攻撃
6位	脆弱性対策情報の公開に伴う悪用増加		による情報漏えい	境や仕組	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	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	内部不正による情報漏えい等
8位	ビジネスメール詐欺による金銭被害		ビジネスメール詐欺による	ス妨害攻撃	リモートワーク等の環境や仕組みを狙った攻撃
9位	予期せぬIT基盤の障害に伴う業務停止	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	DDoS攻撃（分散型サービス妨害攻撃）
10位	不注意による情報漏えい等の被害	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	ビジネスメール詐欺

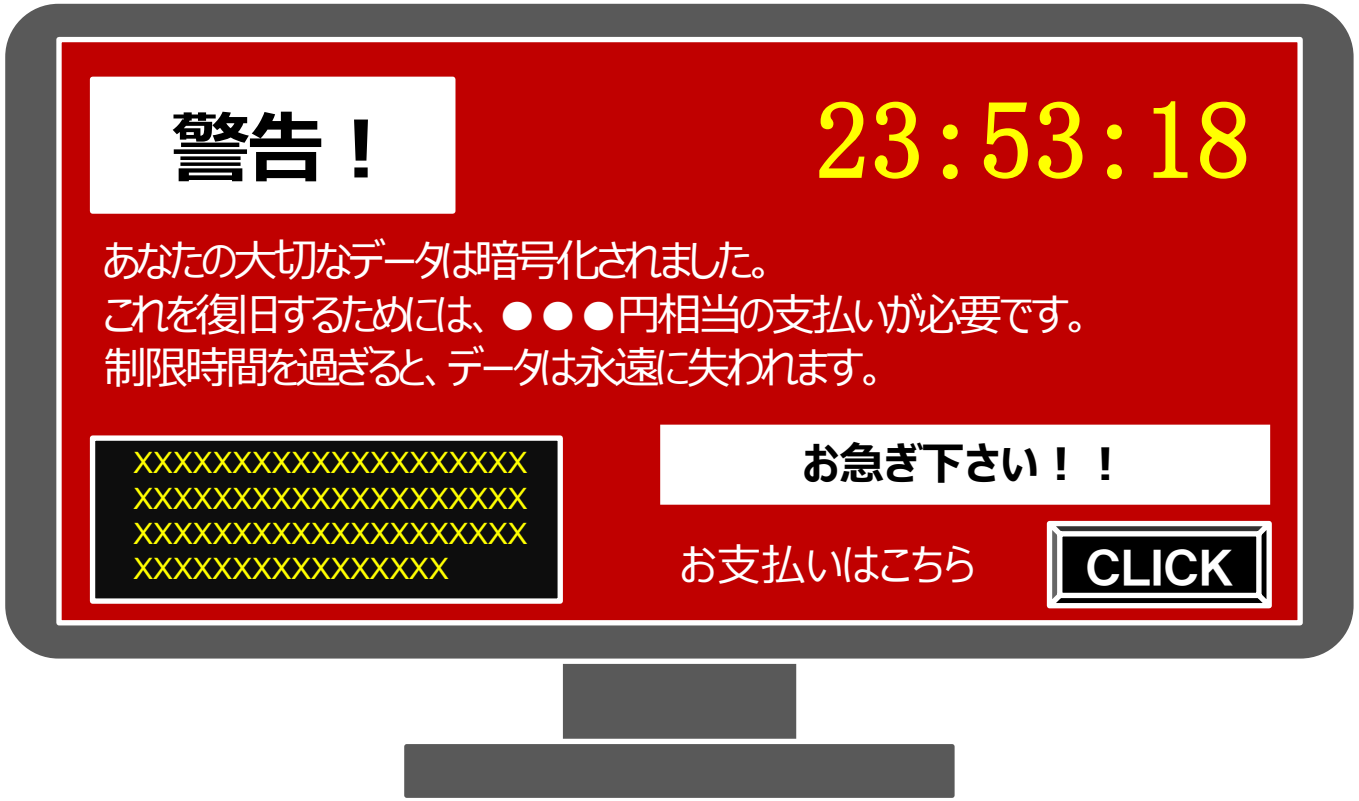
本章では以下の攻撃手法について解説します

- **ランサムウェア攻撃**
- **サプライチェーン攻撃**
- **ビジネスメール詐欺**

出典：「情報セキュリティ10大脅威 2026」2026年1月29日公開（独立行政法人情報処理推進機構）よりMS&ADインターリスク総研が作成
https://www.ipa.go.jp/security/10threats/10threats2026.html

ランサムウェア

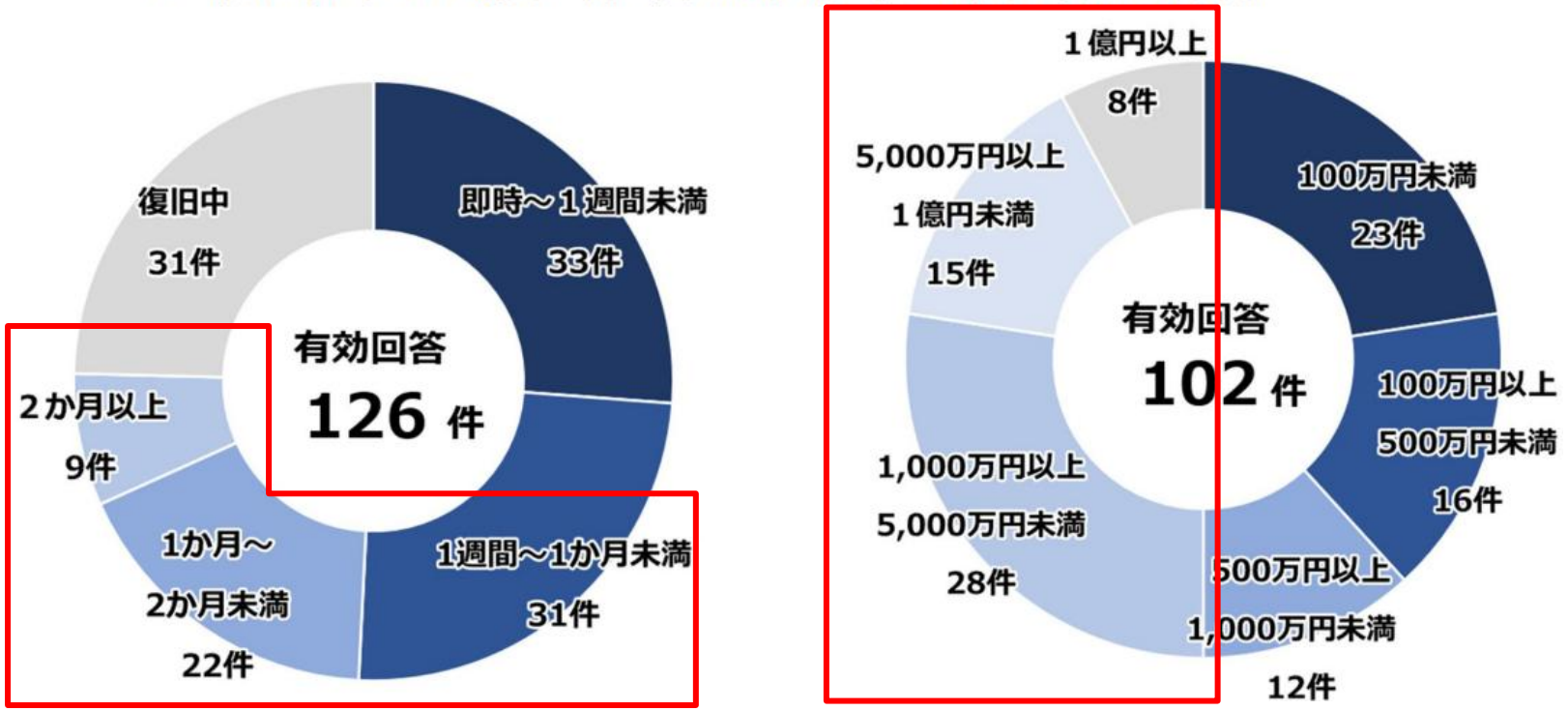
ランサムウェア攻撃とは、VPN機器や電子メールなどを通じて侵入して、PCをロックして使用不能にしたり、PC内のファイルを暗号化することにより参照・使用不能にした後で、元に戻すことと引き換えに「身代金（Ransom）」を要求する不正プログラムを指す。



ランサムウェア感染による業務停止と復旧費用（警察庁）

ランサムウェア感染後、**復旧まで1週間以上**時間を要した事案、および**調査・復旧費用**においても**1000万円以上**を要した事案が全体で50%近くあります。

● 復旧等に要した期間／調査費用の総額／復旧期間と費用の関係性



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」2025年3月13日公開（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

情報セキュリティ事故発生時に想定される損害の相場

損害の種類（例）※抜粋		中小企業における損害額のイメージ
費用損害	法律相談費用	**30～100万円**
	コールセンター費用	3 ヶ月の対応で **700～1,000万円**
	見舞金・見舞品購入費用	1 万人へのプリペイドカード送付で **650万円**
	ダークウェブ調査費用	調査内容によって大きく異なるが**数百万円以上**の額となるケースも
	事故原因・被害範囲調査費用	**300～400万円**、複数台の調査が必要になった場合、**数千万円**のケースも
	システム復旧費用	対応規模等によって大きく異なるが、**数百～数千万円**のケースも
	再発防止費用	対応規模等によって大きく異なるが、**数百～数千万円**のケースも
	超過人件費	対応規模等によって大きく異なるが、多くの従業員等が対応に追われるケースも
賠償損害	損害賠償金	委託先から預かった情報漏えい事案の場合、上記費用損害の合計額が委託先から求償されることも。EC サイトのクレジットカード情報漏えい事案の場合、不正利用の規模によるが**数千万円以上**の額の求償がなされるケースも
	弁護士費用等	損害賠償金に比例して高額に 事案に拠るが着手金、成功報酬、訴訟費用など**300万円以上**になることも
利益損害		数ヶ月の売上高の減少（利益喪失に加え、回避できない固定費の支払い） 事業が完全に停止すれば**数千万円～数億円**規模

出典：「「2024年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」2025年5月27日公開（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

情報セキュリティ事故発生時に想定される損害の相場

損害の種類（例）※抜粋		中小企業における損害額のイメージ
費用損害	法律相談費用	**30～100万円**
	コールセンター費用	3 ヶ月の対応で **700～1,000万円**
	見舞金・見舞品購入費用	1 万人へのプリペイドカード送付で **650万円**
	ダークウェブ調査費用	調査内容によって大きく異なるが**数百万円以上**の額となるケースも
	事故原因・被害範囲調査費用	**300～400万円**、複数分の調査が必要になった場合、**数千万円**のケースも
	システム復旧費用	対応規模等によって大きく異なるが、**数千万円**のケースも
	再発防止費用	対応規模等によって大きく異なるが、**数千万円**のケースも
	超過人件費	対応規模等によって大きく異なるが、多くの従業員等が対応に追われるケースも
賠償損害	損害賠償金	委託先から預かった情報漏えい事案の場合、上記費用損害の合計額が委託先から求償されることも。EC サイトのクレジットカード情報漏えい事案の場合、不正利用の規模によるが**数千万円以上**の額の求償がなされるケースも
	弁護士費用等	損害賠償金に比例して高額に 事案に拠るが着手金、成功報酬、訴訟費用など**300万円以上**になることも
利益損害		数ヶ月の売上高の減少（利益喪失に加え、回避できない固定費の支払い） 事業が完全に停止すれば**数千万円～数億円**規模。

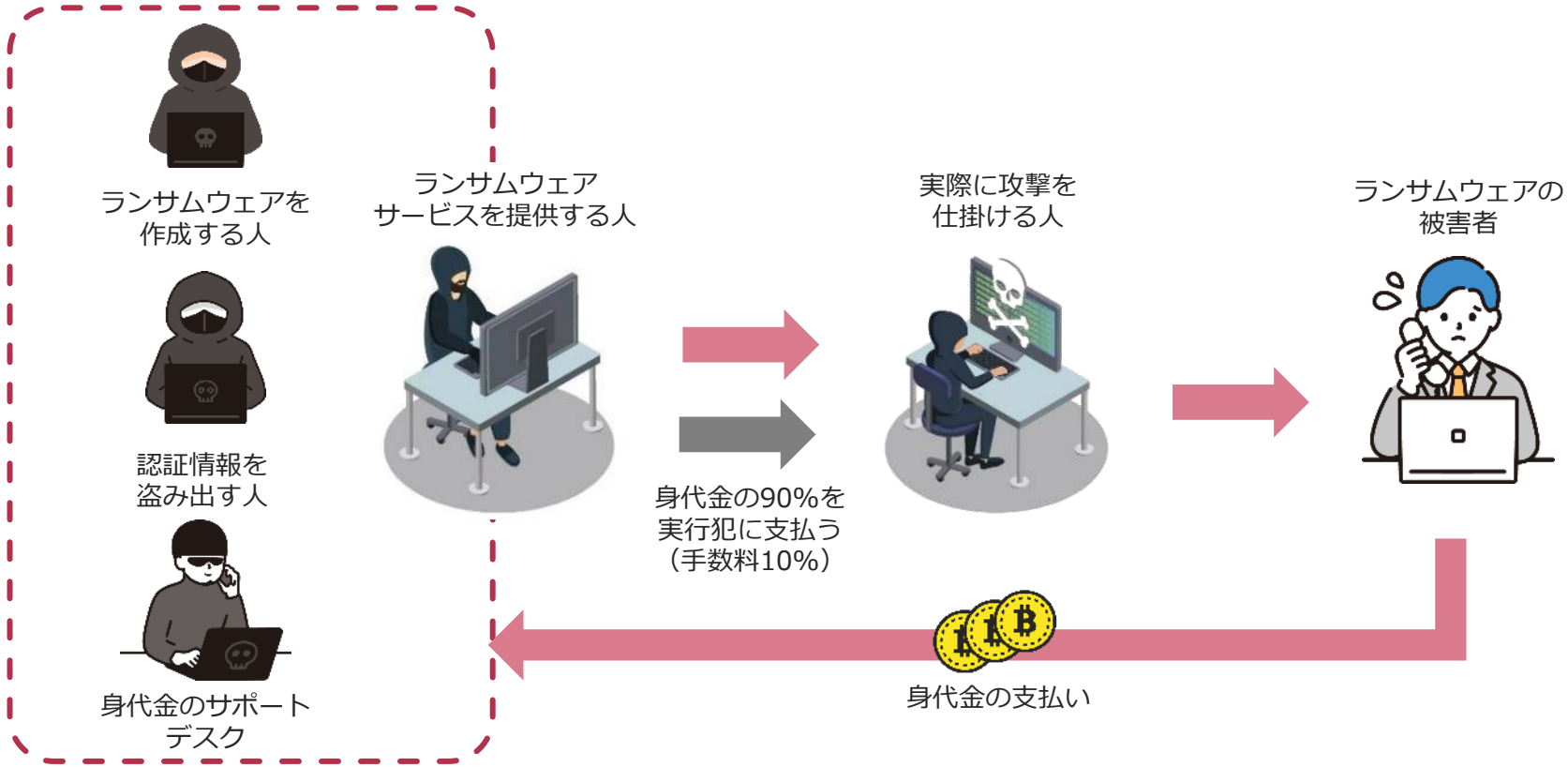
調査・復旧・再発防止策で
数百～数千万かかるケースが多い
※サイバー保険事故事例参照

出典：「「2024年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」2025年5月27日公開（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

なぜ、ランサムウェアの被害が多いのか？

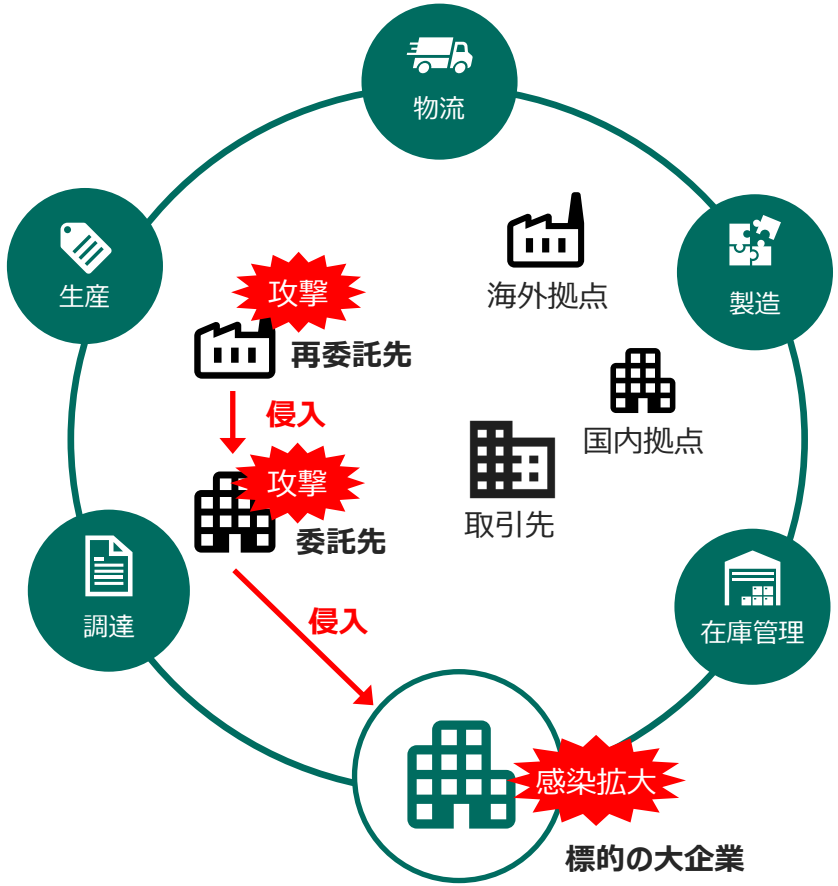
ランサムウェアのビジネス化 （RaaS：Ransomware As A Service）

「闇バイト」のように分業・役割を分担して、攻撃を仕掛けています。
専門知識がない攻撃者も**気軽に攻撃を実行できる環境が整っており**、サイバー攻撃の敷居が下がっています。



サプライチェーン攻撃とは

サプライチェーン攻撃とは、サプライチェーン上でセキュリティ対策が進んでいない企業をターゲットに攻撃し、その結果またはそれを契機に大企業や本社に直接的・間接的に被害を与える攻撃を指す。



サプライチェーン攻撃の種類

攻撃者

ビジネス（業務委託先）

- 開発・運用の業務委託先
- 再委託先、再々委託先なども対象
- 委託先の業務停止
- 運用不備等による情報漏えい

サービスプロバイダ

- SaaS、クラウド、レンタルサーバーなど
- DDoS攻撃などによるサービス停止
- サービス基盤攻撃による情報漏えい
- SaaSが提携している企業への攻撃

ソフトウェア

- アプリケーション、ソフトウェア、ライブラリ、開発環境（フレームワーク）など
- アップデートの経路が侵害され、ソフトウェアの利用ユーザーに悪意あるコードが含まれたソフトウェアを配布する

サプライチェーン攻撃 ～「被害者」にも「加害者」にもなり得る可能性がある～

【事例】

委託先がランサムウェア攻撃を受けた結果、多数の委託元企業まで
被害が発生してしまった事例。

発生したインシデント

概要

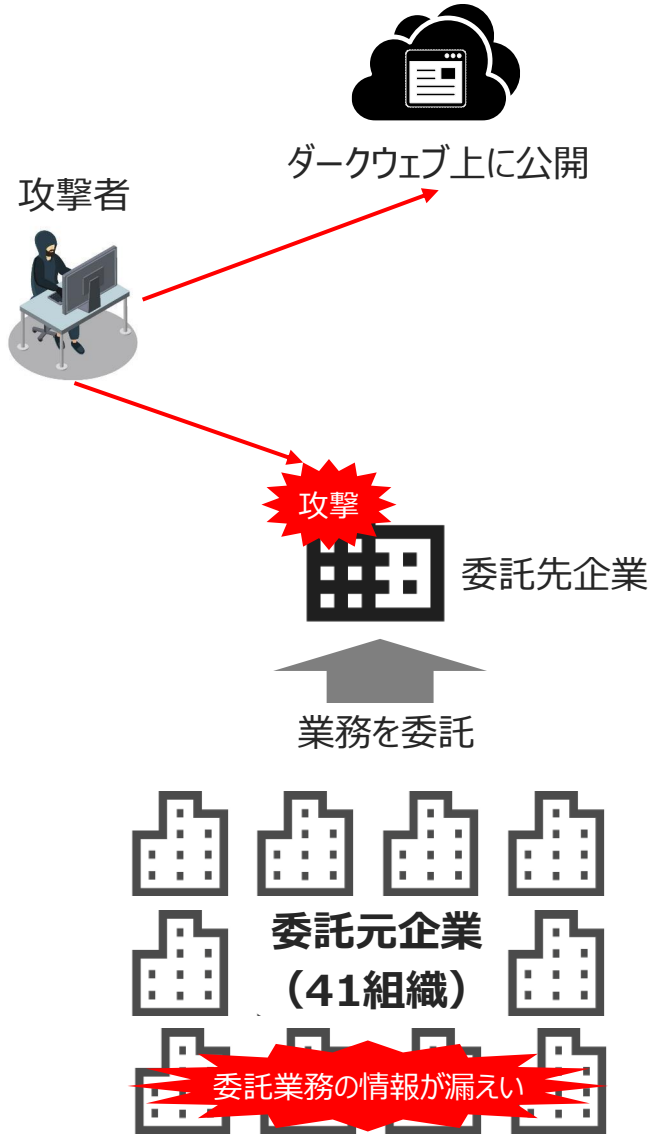
- 2024年5月、情報処理サービスを手掛ける企業が**ランサムウェアに感染**
- 攻撃を行ったランサムウェアグループにより一部の取引先の**情報が公開**される
- 委託していた**民間企業、行政団体等41団体**の情報が漏えい

発生原因

- 攻撃者は**VPN機器を経由**して基幹系ネットワークに侵入したことが判明
- ただし、**ログの取得が十分**でなかったことから侵入の詳細手口は未確認
- VPN機器については令和3年4月以降、**アップデートが行われていなかった**
- データの取り扱い不備により、**本来は基幹系ネットワークに存在しないはずの個人データ**がランサムウェアにより暗号化、窃取される

被害結果

- **合計300万人分の個人情報が漏えい**した可能性がある
- 個人情報保護委員会は本件について**行政指導を公表**



【参考】取引先に対してのサイバー対応を求める傾向にある

大手企業が取引先に対してサイバーセキュリティ対策を求める傾向にあり、中長期的に改善が見込めない場合は他の調達先を検討するなど、厳しい姿勢で取り組みつつある。

サイバー対策で取引先選別　事業停止リスク回避

キオクシア、3000社点検/TOPPAN、除外も検討

2025年8月6日 2:00 [会員限定記事]

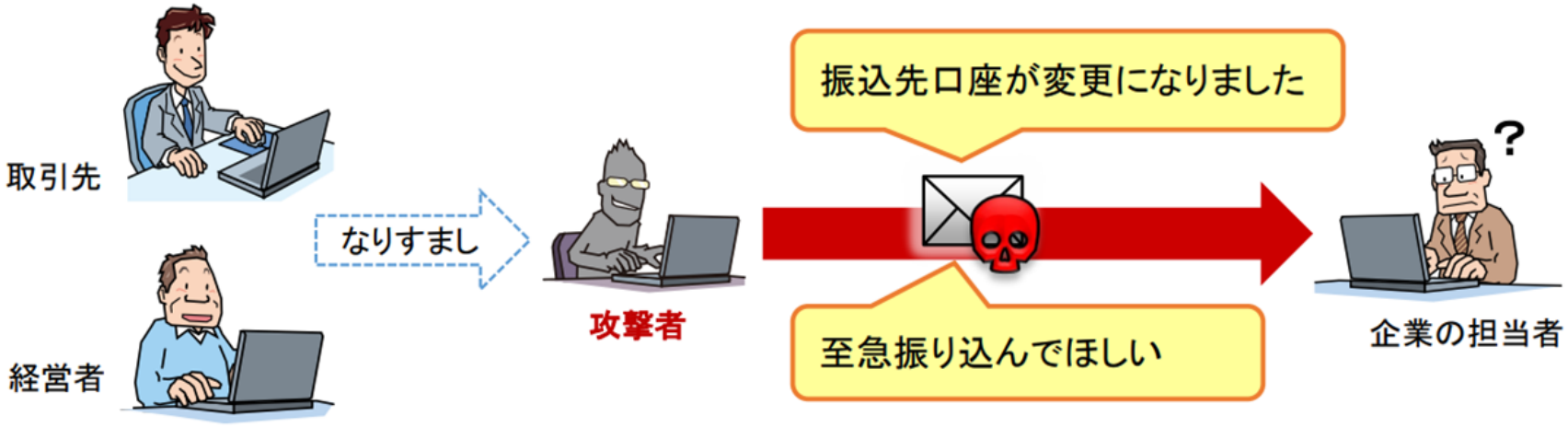
保存

大手企業がサプライチェーン（供給網）全体のサイバーセキュリティー対策を点検し、脆弱な企業との取引を見直している。巨大な調達網の中でわずか1社のサイバー被害によって生産活動が停止し、顧客先も含めて影響が広がる恐れがあるためだ。経済安全保障の観点から半導体産業などでサイバー防衛力を高める動きが広がってきた。

出典：「サイバー対策で取引先選別　事業停止リスク回避」2025年8月6日公開（日本経済新聞）
https://dailydarkweb.net/a-threat-actor-allegedly-offers-unauthorized-vpn-access-to-major-japanese-automotive-corporation/

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

攻撃者が取引先や経営者等へなりすまして、偽のメールを企業の担当者へ送り付け、金銭を騙し取るサイバー攻撃です。



金銭に関する意思決定者である**経営層**や、取引先と送金に関するやり取りを行う、**経理・財務部門の社員**などが狙われる傾向にある。

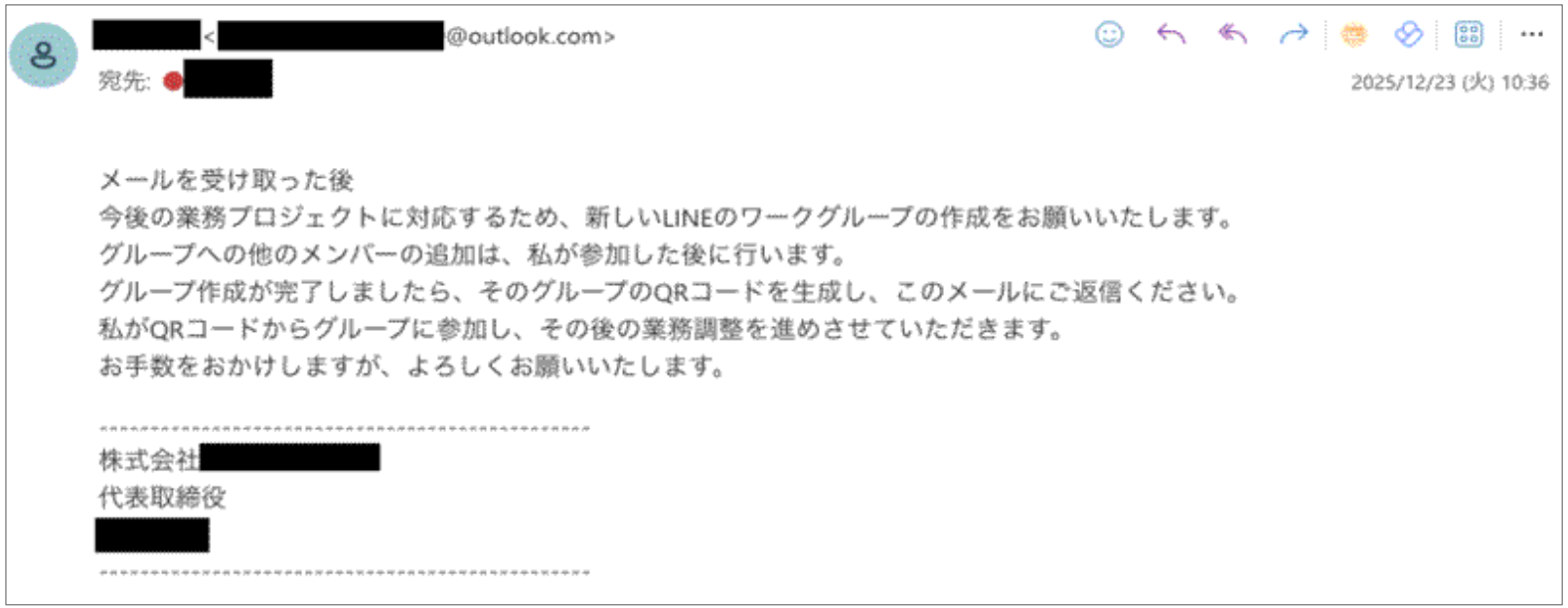
FBIインターネット犯罪（IC3）レポートによると、BECによる損失額は**年間27億ドル**。これに対し、ランサムウェアの被害額は3,400万ドルである。BECの被害額はランサムウェアの約79倍になる。

出典：「ビジネスメール詐欺対策特設ページ」2023年2月9日公開（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/bec/about.html

CEO詐欺／LINEグループ詐欺（ビジネスメール詐欺）

2025年末から、企業代表者の実名をかたってLINEのグループ作成やMicrosoft Teamsのアカウント情報の提供を求める「CEO詐欺」メールが相次いでいる。

最終的には現金をだまし取る（偽の口座に振り込ませるなど）ことを目的とした攻撃。



出典：「そのメール、本当に社長からですか？企業を狙うメール攻撃「CEO詐欺」とは」2026年1月21日公開（LAC）
https://www.lac.co.jp/lacwatch/alert/20260121_004604.html

CEO詐欺／LINEグループ詐欺（ビジネスメール詐欺）

■ 特徴

- 現在または過去の**代表者や役員の実名**をかたっている
- 送信には**フリーメール**が多く利用されている
- 「【至急】グループ作成依頼」など**緊急性の高い件名**でメールが届く
- 「LINEグループ作成のお願い」「QRコード送付のお願い」などの依頼が多いが、「TeamsアカウントのID/PWの要求」などもある
- 「他の人は入れないで」と**口止めされる**
- LINE上で「残高のスクリーンショット」「取引先への支払い」などを理由に、**口座情報の提出や振込を求められる**

■ 対策

- 必ず、メールとは別の手段で事実確認を行う
- メールへの直接返信や、本文中に記載された連絡先の使用を避ける
- メールに添付されたファイルや、本文中に記載されたリンクをクリックしない
- 社員への周知・対策の徹底

被害事例

報道日など	被害組織	被害額
2025年12月25日	長野県飯田市の企業	2950万円
2025年12月26日	北海道函館市の企業	4980万円
2026年1月5日	北海道札幌市の企業	8000万円
2026年1月9日	山形県酒田市の企業	2300万円
2026年1月14日	三重県いなべ市の企業	1000万円
2026年1月14日	岐阜県多治見市の企業	1億円
2026年1月29日	長崎県佐世保の企業	1130万円
2026年2月2日	千葉県船橋市の企業	5000万円

出典：「LINEグループ作成を要求されるCEO詐欺メールについてまとめてみた」2026年1月16日公開（はてなブログ）
https://piyolog.hatenadiary.jp/entry/2026/01/16/155626

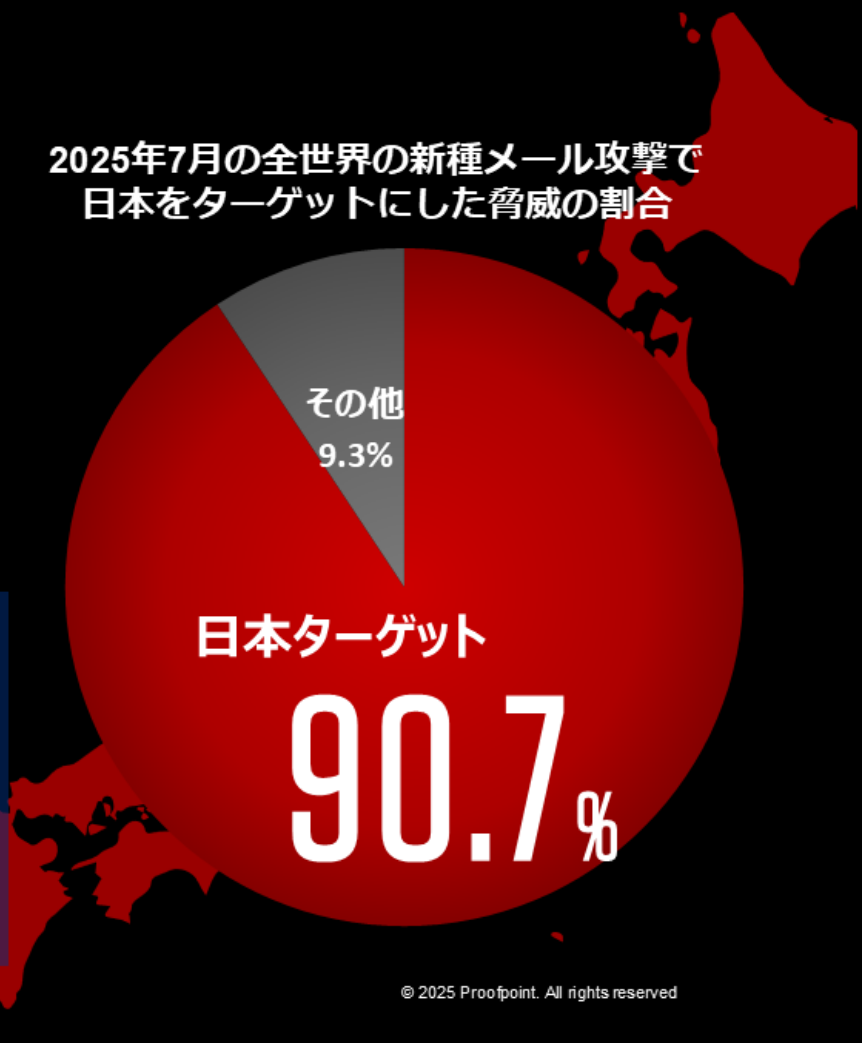
【参考】「今、フィッシング詐欺で世界で一番狙われている国は「日本」。その背景にAI」

2025年７月：全世界のメール攻撃のうち90%が日本をターゲットに

- グローバルで**合計1223の新種のメール攻撃キャンペーン**を観測
- うち105の攻撃キャンペーンが日本をターゲット
  ボリューム数TOP13位までがすべて日本を標的にしたキャンペーン
- 全世界への新種のメール攻撃のうち、
  90.7%が日本をターゲット
- CoGUIフィッシングキットを用いた攻撃が急増
- 多要素認証をすり抜けるAiTMであるEvilginxも使われている

CoGUIフィッシングキットとは：
CoGUI “フィッシング・キットは、プルーフポイントのリサーチャーによって特定された高度な検知回避機能を持つフィッシング・フレームワーク。主に日本のユーザーを標的。他に少数だがオーストラリア、ニュージーランド、カナダ、米国を標的。ジオフェンシング、ヘッダーフェンシング、フィンガープリンティングなどの高度な回避テクニックを使用することにより、セキュリティ対策を回避しながら特定の地理的地域を選択的に標的とすることが可能。標的とされた国のユーザーにとって重大な脅威となっている。
Amazon, 楽天、Apple、ヨドバシなどのショッピングサイト、イオンカード、Orico、VISA、 TS Cubic、セゾンカード、Orico、EPOSカード、Paypay、SMBCなどの決済サービス、SBI証券、大和証券松井証券などの証券会社ほか、NTTドコモ、ヤマト運輸、えきネットなどのサービスになりすまし、ログイン認証権限、個人情報、クレジットカード情報などを窃取する

proofpoint.



出典：「今日本が今、最も狙われている【続編】ープルーフポイントのデータからみる生成AI時代のメール脅威と対策」2025年8月11日公開（Proofpoint）
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/email-threats-and-countermeasures-generative-ai-age

【参考】「今、フィッシング詐欺で世界で一番狙われている国は「日本」。その背景にAI」

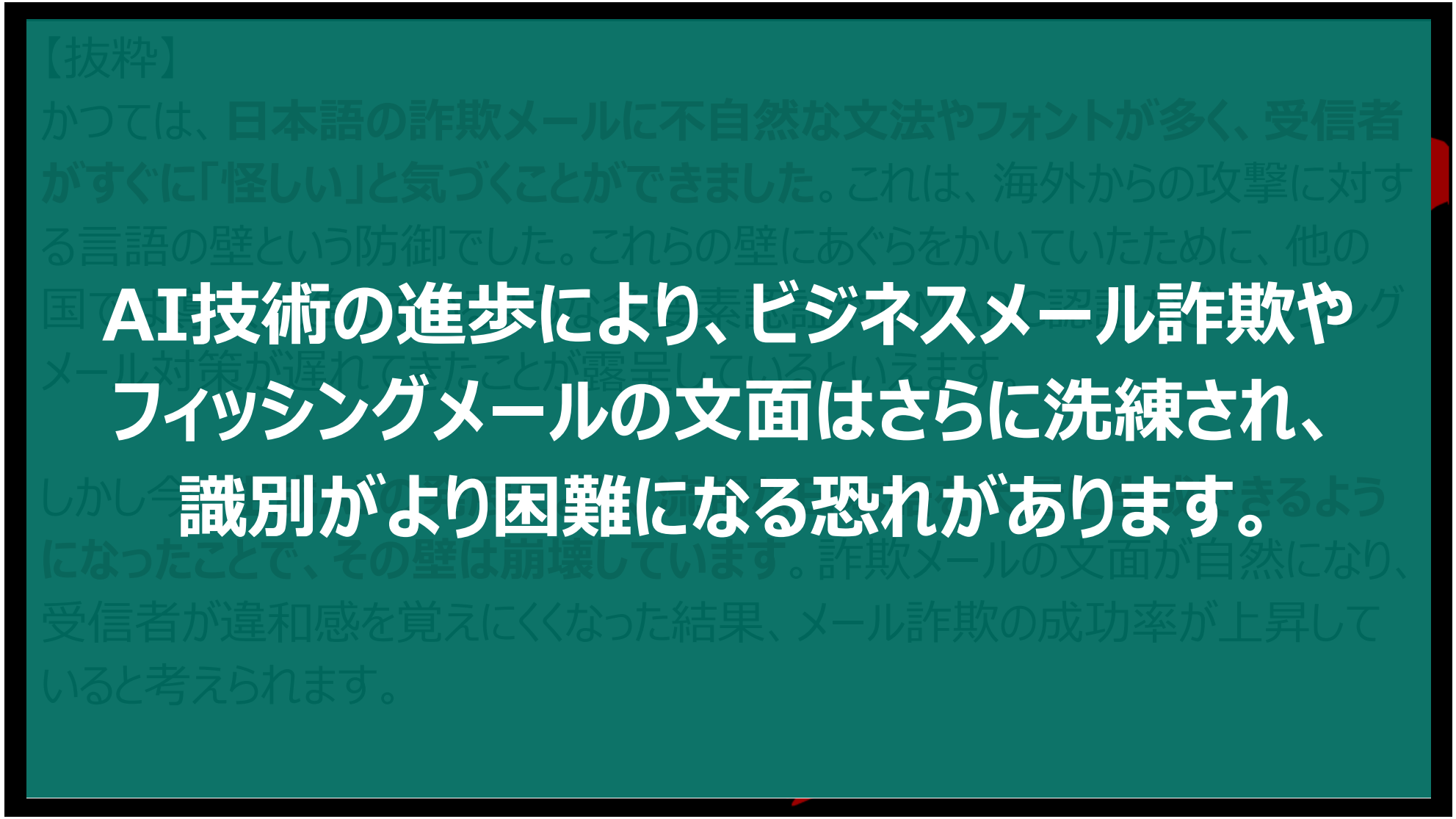
【抜粋】

かつては、**日本語の詐欺メールに不自然な文法やフォントが多く、受信者がすぐに「怪しい」と気づくことができました**。これは、海外からの攻撃に対する言語の壁という防御でした。これらの壁にあぐらをかいていたために、他の国では導入が進んでいるような多要素認証やDMARC認証などフィッシングメール対策が遅れてきたことが露呈しているといえます。

しかし今、**生成AIの発展により、流暢な日本語を大量に生成できるようになったことで、その壁は崩壊しています**。詐欺メールの文面が自然になり、受信者が違和感を覚えにくくなった結果、メール詐欺の成功率が上昇していると考えられます。

出典：「今日本が今、最も狙われている【続編】ープルーフポイントのデータからみる生成AI時代のメール脅威と対策」2025年8月11日公開（Proofpoint）
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/email-threats-and-countermeasures-generative-ai-age

【参考】「今、フィッシング詐欺で世界で一番狙われている国は「日本」。その背景にAI」



出典：「今日本が今、最も狙われている【続編】ープルーフポイントのデータからみる生成AI時代のメール脅威と対策」2025年8月11日公開（Proofpoint）
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/email-threats-and-countermeasures-generative-ai-age

３．企業が取り組むべき対策

セキュリティ対策の重要性　サイバーセキュリティ経営ガイドライン

POINT

本ガイドラインは経営者を名宛人に、セキュリティ対策の重要性を説明しており、
サイバーセキュリティ対策は、事業活動を行う上で必要不可欠な要素となっている。

II. 経営者が認識すべき３原則

経営者は、以下の3原則を認識し、対策を進めることが重要である。

(1) 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
（経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の事業継続のためのセキュリティ投資を実施すべきである。）

(2) サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
（自社のサイバーセキュリティ対策にとどまらず、在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全てを含むサプライチェーン全体を意識し、総合的なサイバーセキュリティ対策を実施すべきである。）

(3) 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要
（平時から社外の利害関係者（株主、顧客等）はもとより、社内の関係者（CIO 等セキュリティ担当者、事業担当責任者等）に事業継続に加えてサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。）

（詳細は後述の「２．経営者が認識すべき３原則」を参照）

出典：「サイバーセキュリティ経営ガイドラインVer3.0」2023年3月24日公開（経済産業省・独立行政法人情報処理推進機構）
https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html

サイバーセキュリティ経営ガイドライン（重要10項目）

POINT

経営者は重要10項目について、単なる指示出しだけではなく、経営資源の配分（ヒト・モノ・カネ）や実施状況の確認等を通じてリーダーシップを発揮する必要がある。

■サイバーセキュリティリスクの管理体制構築

指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装

指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築

指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続・復旧体制の整備

■サプライチェーンセキュリティ対策の推進

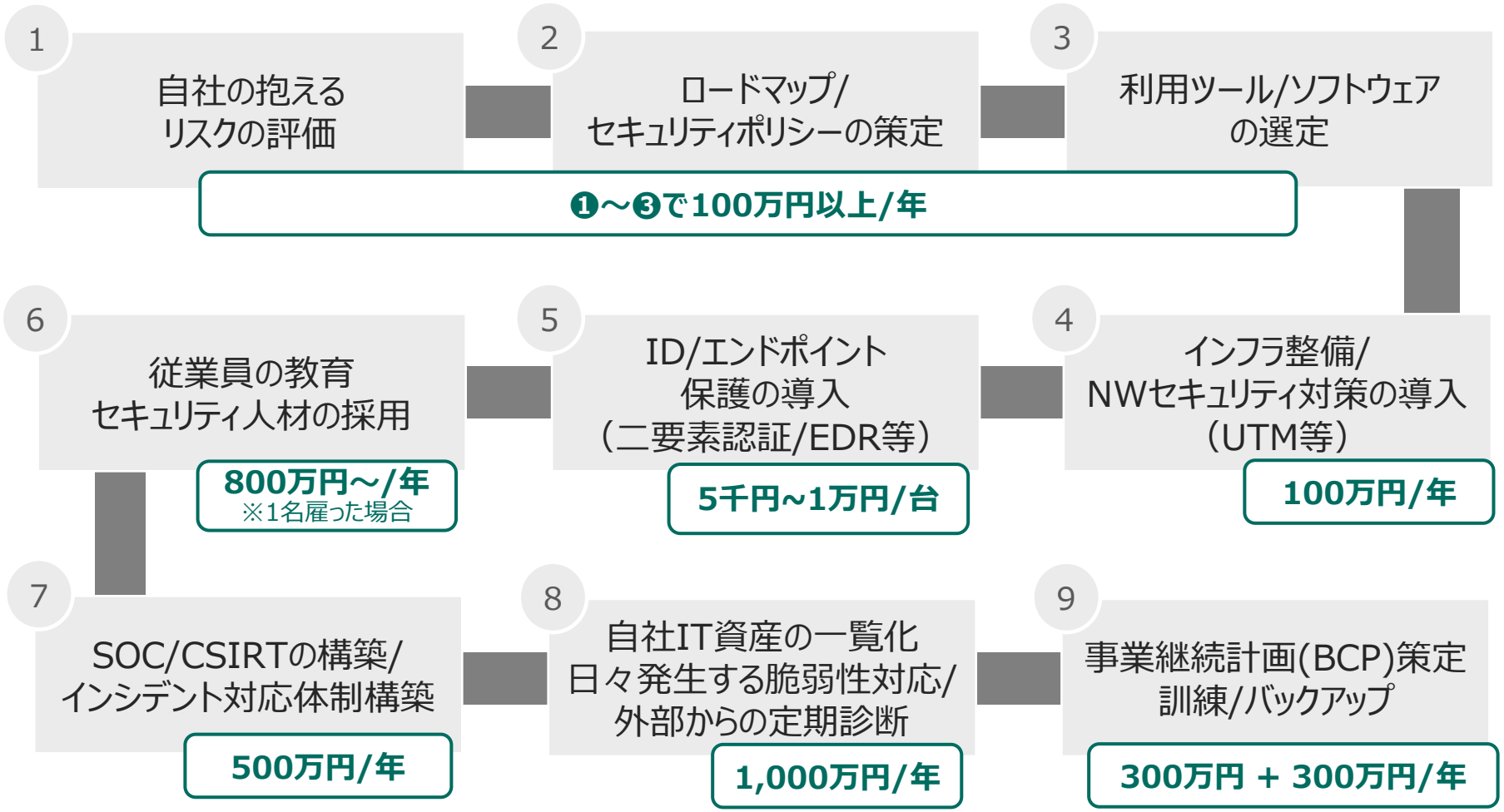
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

■ステークホルダーを含めた関係者とのコミュニケーションの推進

指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

セキュリティ対策のモデルケース

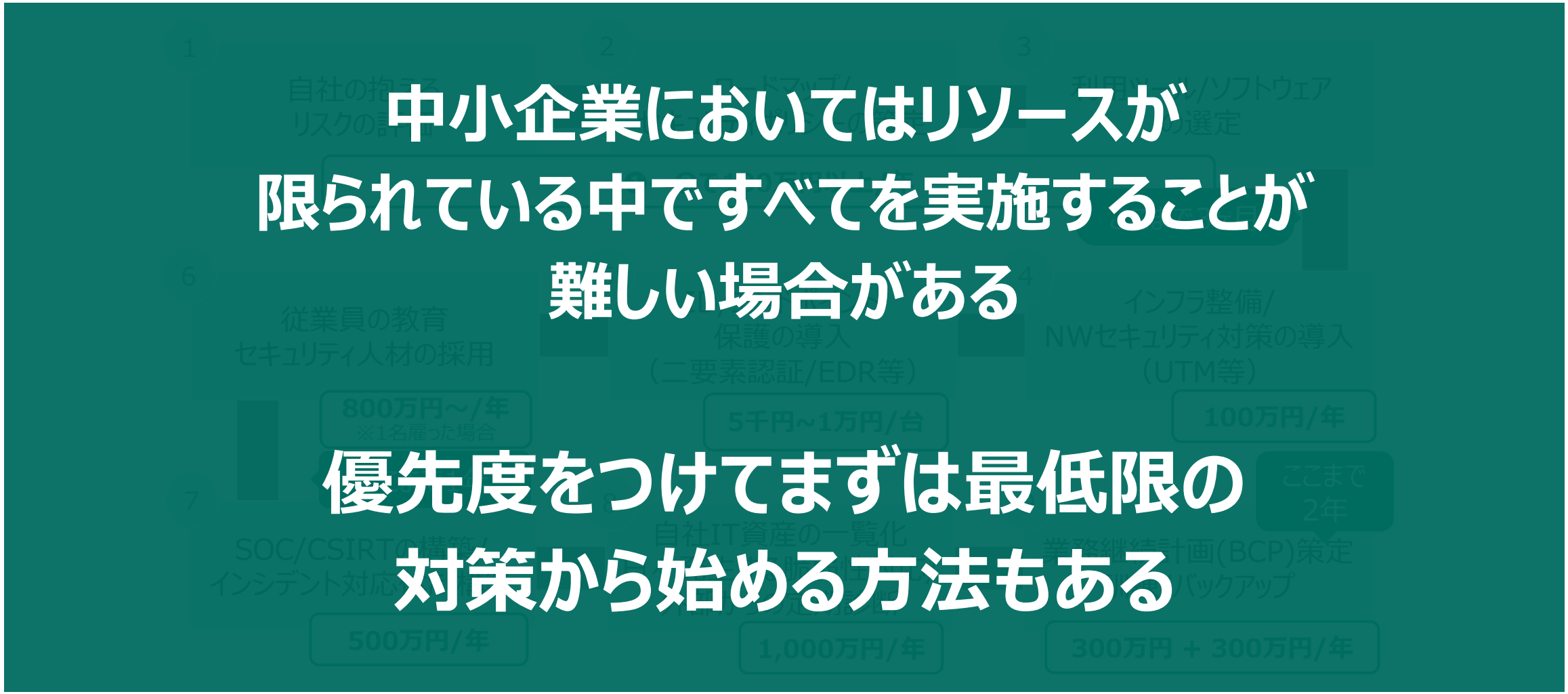
一般的なセキュリティ対策や体制の構築に関するケース



※ 記載している金額は目安であり、PC台数や現在の対策情報によって異なります

セキュリティ対策のモデルケース

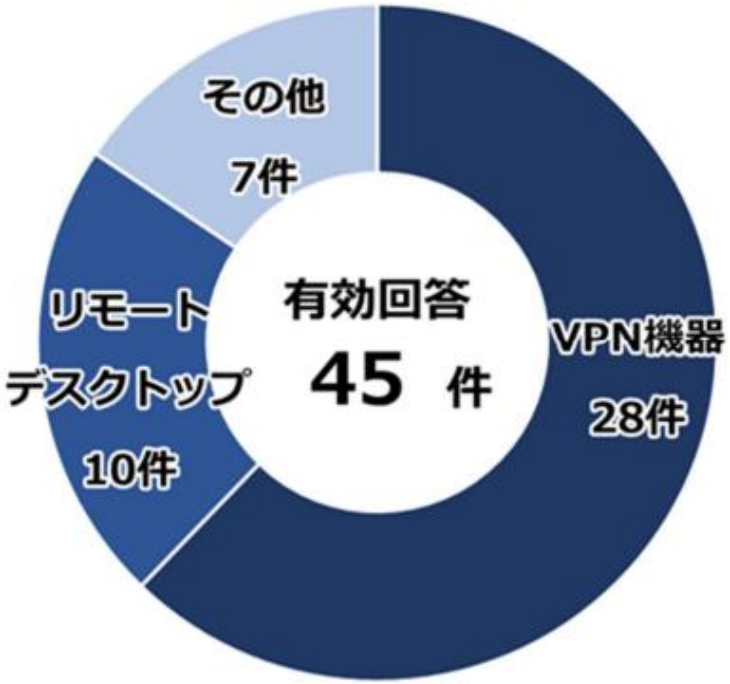
一般的なセキュリティ対策や体制の構築に関するケース



※ 記載している金額は目安であり、PC台数や現在の対策情報によって異なります

ランサムウェアの感染経路

ランサムウェア被害に感染経路は依然としてVPNやリモートデスクトップが8割以上を占める状況です



- 日本国内においては**依然として**VPN機器やリモートデスクトップ経由でランサムウェアに感染している
- その原因として、**ID/パスワードが非常に容易**であったこと、**不要なアカウントが適切に管理されていなかった**ことなどがあげられている
- またVPN機器や管理画面等の**脆弱性を悪用**した被害も報告されている
- **基本的な対応をしていない**組織が被害に遭っている
- 裏を返せば、リモートアクセスツールの**適切な運用・管理、脆弱性のないバージョンの使用**など基本的な対策を継続　するだけでも、多くの被害が防ぐことができる

出典：「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2025年9月公開）警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

ランサムウェアの感染経路

基本的な対策が講じられていないことを
原因とする感染が、いまだに多く発生

基本的な対策を実施するだけでも
多くの被害を防ぐことができる

出典：「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2025年9月公開）警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

優先的に実施すべき基本的なセキュリティ対策

外部資産の把握	外部公開サーバーの把握および脆弱性への是正措置
認証方法の強化	多要素認証（MFA）の有効化とパスワードポリシーの強化
最新バージョンの使用	既知の脆弱性が修正された最新バージョンの継続利用 最新のセキュリティパッチの迅速な適用
バックアップの取得	重要システムの定期的なバックアップの取得 復旧手順の確認・リストアテストの実施
アクセス権限の見直し	不要な管理者権限を付与していないか アカウントの棚卸
アクセス制限の実施	必要最低限のアクセス元のみを許可する
ログの取得	ログの取得と適切な保管
インシデント対応体制の構築	万が一サイバー攻撃を受けた場合の体制を事前に準備しておく

特に優先して実施していただきたい対策

※ 当社見解であり、当然上記以外にも必要な対策はありますが、優先的に対応すべき対策を記載しています
※ アンチウイルス製品の導入は実施済みの想定です

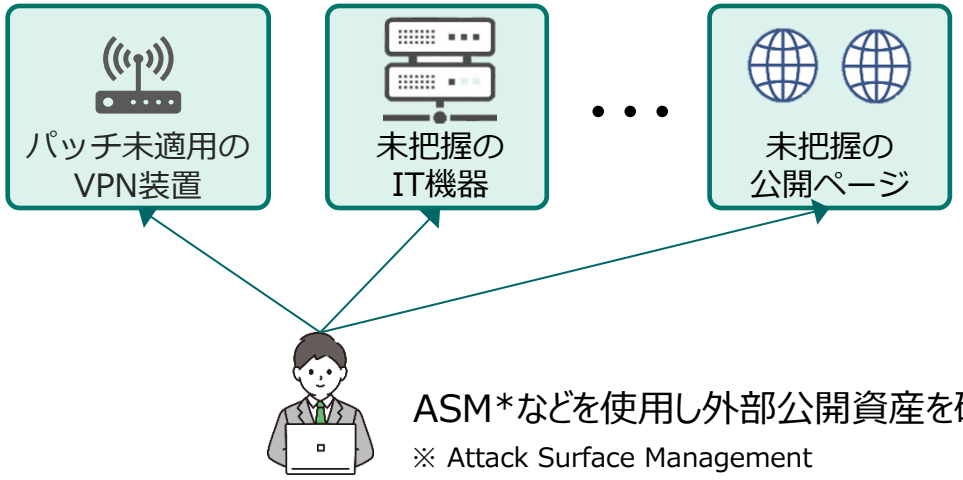
優先的に実施すべき基本的なセキュリティ対策

外部資産の把握

攻撃者がまず最初に狙う箇所は、インターネットに公開しているシステム（サーバー等）です。例えば悪用容易な脆弱性が報告された場合、攻撃者は**インターネット上にあるシステムを無差別にスキャン**し、侵入できるところから攻撃を実施する傾向にあります。

【対策方法】

まずは自社が**外部に公開しているシステムを把握**し、脆弱性などセキュリティ上の課題があれば是正します。また、本当に公開するべき必要があるかについても確認します。



認証方法の強化

他社サイトが攻撃を受け、自社の認証情報が漏えいするケースがあります。また、推測容易なパスワードを設定していたため、リモートアクセスサービス経由で侵入されるケースも多発しています。システム構築時やメンテナンスのために一時的に作成したアカウントなどがよく悪用されています。

【対策方法】

万が一認証情報が漏えいした場合でも、**多要素認証（MFA）**を導入することで侵入を防ぐことができます。また、**すべてのアカウント**に対して強度の強い（文字数が長い）パスワードを設定し、多要素認証が有効になっていることを確認します。

優先的に実施すべき基本的なセキュリティ対策

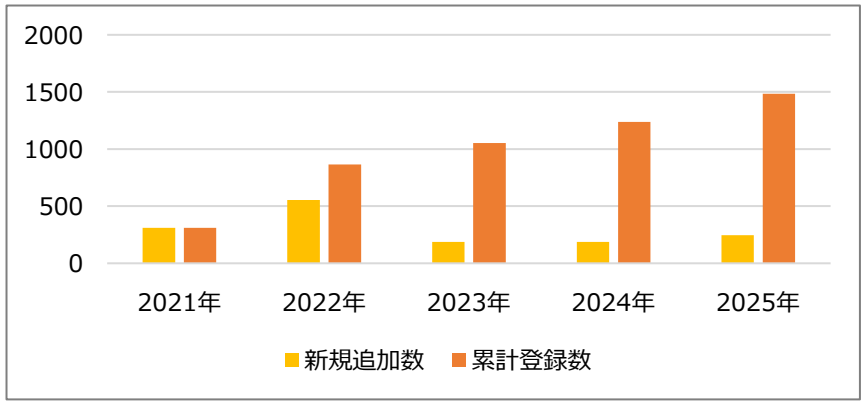
最新バージョンの使用

日々、脆弱性が報告されており、時には非常に危険度の高い脆弱性も報告されます。ゼロデイ攻撃を防ぐことは難しいですが、古い脆弱性を放置していたために侵入されるケースも多数報告されています。

【対策方法】

導入ベンダーなどに対しては、最新の脆弱性情報を収集するよう要件に組込み、脆弱性が報告された場合は迅速にセキュリティパッチの適用やバージョンアップができるような体制にします。また、脆弱性が報告された場合だけに限らず、**継続的に最新のバージョンを使用する**ことも検討します。

【実際に悪用された脆弱性（米CISA 参考）】



バックアップの取得

ランサムウェアに感染した際、バックアップが存在しない、バックアップデータも暗号化された、バックアップデータが破損しているなどで、復旧に多くの時間を要したケースも報告されています。迅速に復旧できない場合は業務の再稼働までに時間がかかり、損失が増大します。

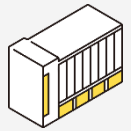
【対策方法】

重要なシステムから優先的にバックアップを取得します。特に基幹システムなど最重要なシステムにおいては、「3-2-1ルール」などを参考に、保管先を別サイトにするなどの方法も有効です。また、必要な時にリストアできないなど発生する可能性もあるため、**リストアテストの実施も重要**です。

3つのバックアップコピーを作成

2つの異なるメディアに保存

1つをオフサイトに保存



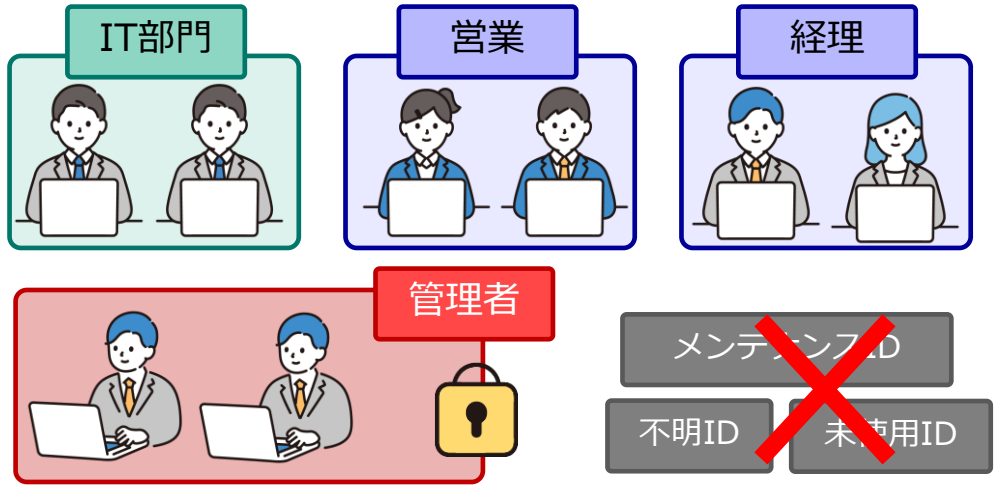
優先的に実施すべき基本的なセキュリティ対策

アクセス権限の見直し

不必要に管理者権限など権限の高いアカウントを付与している場合、マルウェア等に感染した場合に簡単に社内システム全体を掌握されてしまう可能性があります。また、適切に権限が設定されていない場合、被害範囲が拡大する可能性があります。

【対策方法】

アカウントの棚卸を行い、**管理者権限を付与しているアカウントの見直し**や**部署・担当業務ごとに適切な権限を付与**します。特に一時的に使用していたメンテナンス用のアカウントなど残存していないか確認します。

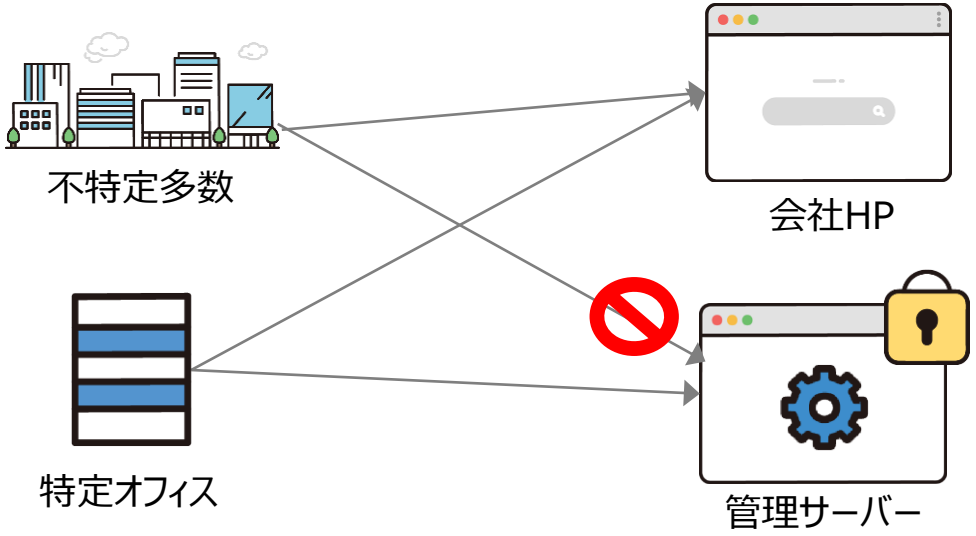


アクセス制限の実施

本来インターネットに公開不要な管理画面や管理用のサービスに脆弱性が存在し、侵入されるケースが報告されています。また、パスワード攻撃により不正ログインされる可能性もあります。

【対策方法】

外部に公開している管理画面や管理用サービスがあるか確認し、**必要なアクセス元のみアクセスを許可**します。また、社内のサービスにおいても本当に必要なサービスがあるか、不要な共有設定がされていないか確認します。



優先的に実施すべき基本的なセキュリティ対策

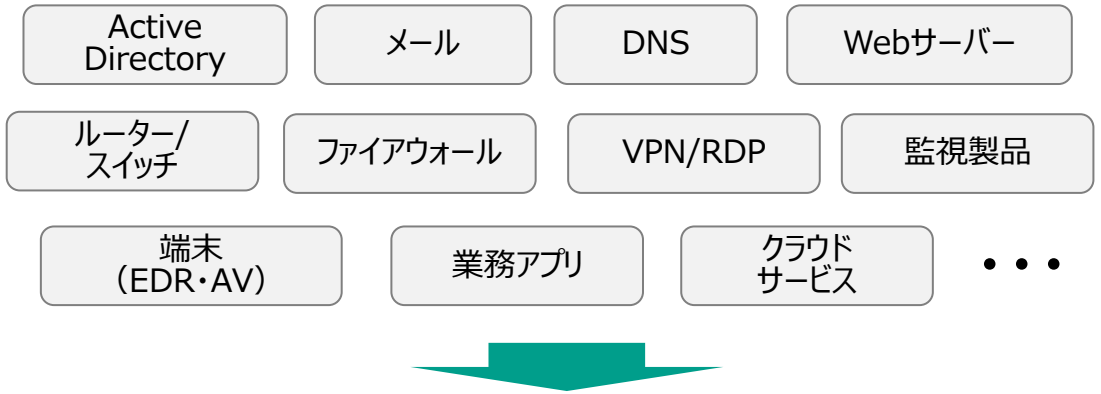
ログの取得

サイバー攻撃を受けた際に、ログが残っておらず、被害状況や影響範囲、原因を特定できないケースがあります。その結果、顧客・取引先などに状況を報告できず、**説明責任を果たせない可能性があります**。

【対策方法】

ログを取得し、**適切な期間保存**しておきます。また、不正侵入後に攻撃者がログを削除するケースもあるため、ログサーバー（SIEMなど）に保存する方法が推奨となります。

※ 端末・サーバーにEDRの導入も要検討

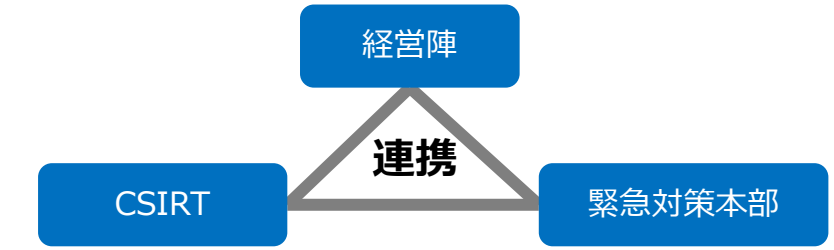


インシデント対応体制の構築

影響範囲や損害の特定、被害拡大防止のため初動対応は重要ですが、事前に準備していないためにサイバー攻撃を受けた際に何をしてよいかわからず、被害が拡大してしまう恐れがあります。

【対策方法】

インシデントが発生した場合に**誰が何をどのような対応をするのか**、インシデントの種類ごとに対応手順を準備し、信頼できる外部の専門ベンダーに依頼できるように事前に準備しておきます（CSIRT*の構築）。また、**経営層を巻き込んだインシデント対応訓練**なども実施します。



システム面の対応
- CISO
- セキュリティ部門
- システム部門 など

緊急時対応（統括）
- 経営企画
- 総務、広報
- 各業務部門 など

※ Computer Security Incident Response Team

その他のセキュリティ対策

その他にも検討すべきセキュリティ対策は多数あります。自社のリスクを把握し、優先順位を定めて段階的に強化します。

セキュリティポリシー・既定の見直し	昨今の最新のテクノロジを反映したポリシーや規定になっていないか見直す
セキュリティアセスメント	攻撃に遭う可能性が高い、システム（外部公開サーバ・Webアプリなど）に対して、脆弱性診断やペネトレーションテストなどを実施する
サプライチェーン・リスク管理	委託先のセキュリティ監査、クラウドサービス、使用ソフトウェアなどのリスク評価
ネットワークの細分化	ネットワークを最小単位で分割しサイバー攻撃の影響拡大を防止する（マイクロセグメンテーション）
セキュリティ監視	端末・サーバーにEDR*やSIEM*を導入し、侵入後の不審な挙動を　早期に検知・封じ込める
事業継続計画(BCP)策定	災害、サイバー攻撃等の緊急事態に中核業務を継続し、早期復旧を実現するための具体的な行動計画を策定、訓練を実施
従業員に対する教育・訓練	組織全体でセキュリティ意識を高めるための教育や訓練（メール訓練など）を実施する

※EDR：Endpoint Detection and Response
※SIEM：Security Information and Event Management

など…

【参考】「2024年度 中小企業における情報セキュリティ対策に関する実態調査」

情報セキュリティ対策を行ったことが取引につながった大きな要因と考える企業は4割強存在しています。
今後、さらにこのような傾向が強まる可能性があります。

※今後、セキュリティ対策が企業間の取引に重要な要因となる

Q49.（Q46.で「はい」と回答された方について）貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）

要請に基づき、情報セキュリティ対策を行ったことが取引に繋がった大きな要因だと考える企業は全体の 4 割強に上る。

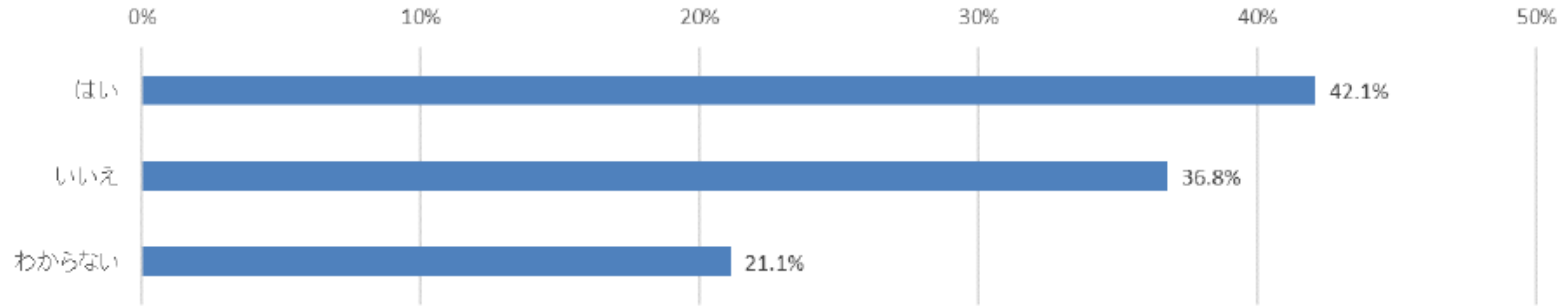


図 3-62 販売先（発注元企業）の要請に応じたことが取引につながった大きな要因か(n=511)

出典：「「2024年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」2025年5月27日公開（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

【参考】サプライチェーン対策評価制度

サプライチェーン企業の対策を評価・可視化して信頼性向上を図る制度で、2026年度中の制度開始を予定している

	★3	★4	★5（※）
想定される脅威	• 広く認知された脆弱性等を悪用する**一般的なサイバー攻撃**	• **供給停止**等によりサプライチェーンに**大きな影響**をもたらす企業への攻撃 • 機密情報等、**情報漏えい**により**大きな影響**をもたらす資産への攻撃	• **未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	• 全てのサプライチェーン企業が**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に実施	• サプライチェーン企業等が**標準的に目指すべきセキュリティ対策**として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策**を実施	• サプライチェーン企業等が**到達点として目指すべき対策**として、**国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した**上で、**システムに対しては現時点でのベストプラクティスに基づく対策**を実施
脅威に対する達成水準（イメージ）	• **組織内の役割と責任が定義**されている。 • 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• セキュリティ対策が**組織的な仕組みに基づいて実施され、継続的に改善**している。 • **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。	• 組織において**国際規格等に基づくマネジメントシステム**が確立されている。 • **リスクを適宜適切に把握**した上で、インシデントに対して迅速に検知・対応するなど、**ベストプラクティスに基づくサイバーレジリエンス確保策**が講じられている。 • 取引先等への指導や共同での訓練の実施など、**自社サプライチェーン全体のセキュリティ水準向上に資する対策**が講じられている。
評価スキーム	**自己評価** （※）社内等の専門家による評価を想定	**第三者評価** ※第三者評価を原則とするが、評価コストの負担を抑える観点から詳細は今後検討	**第三者評価**
ベンチマーク （対象企業やリスクが同様であり、対策項目を検討する上で参考）	• 自工会・部工会ガイドLv1 • Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出	• 自工会・部工会ガイドLv2～3 • 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出	• ISO/IEC27001 • 自工会・部工会ガイドLv3 等 （※）ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

出典：「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）」（2025年4月14日公開）経済産業省
https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf

企業が取り組むべき対策

どの組織においても100点満点のセキュリティ対策を
実施することは現実的には不可能

特にリソースが限られている中小企業においては、
できるところから対応するのも一つの方法

※ 目指すべき姿を定義し、ロードマップを作成しながら
進めると、今後も見据えた対策ができる

４．まとめ

まとめ

■どんな組織でもサイバー攻撃を受ける可能性がある

- 攻撃者のビジネス化、生成AIの性能向上により攻撃の敷居が低くなっている
- リソース（人・モノ・金）が十分にない、対策が遅れている中小企業の被害が増加している

■サイバー攻撃を受けた場合、被害・影響が広範囲に及ぶ

- 業務復旧までに長期間かかるケースもあり、大幅な売上減の可能性がある
- サプライチェーン上の組織が被害に遭い、間接的に影響が及ぶ可能性もある

■情報リスクを認識し、平常時から対策を講じておく

- 自社のリスクを把握し、優先度をつけて対策を行う
- 平時においても関係者との積極的なコミュニケーションをとる
- サイバーセキュリティ経営ガイドラインを参考に管理体制／緊急対応体制を構築する

ご清聴ありがとうございました。

MS&AD

MS&ADインターリスク総研