

サイバー空間における脅威動向と 中小企業における対策と各種支援施策

2026年1月19日

独立行政法人情報処理推進機構(IPA)

セキュリティセンター 普及啓発・振興部 普及啓発グループ

篠嶋 秀雄

独立行政法人情報処理推進機構(IPA)について

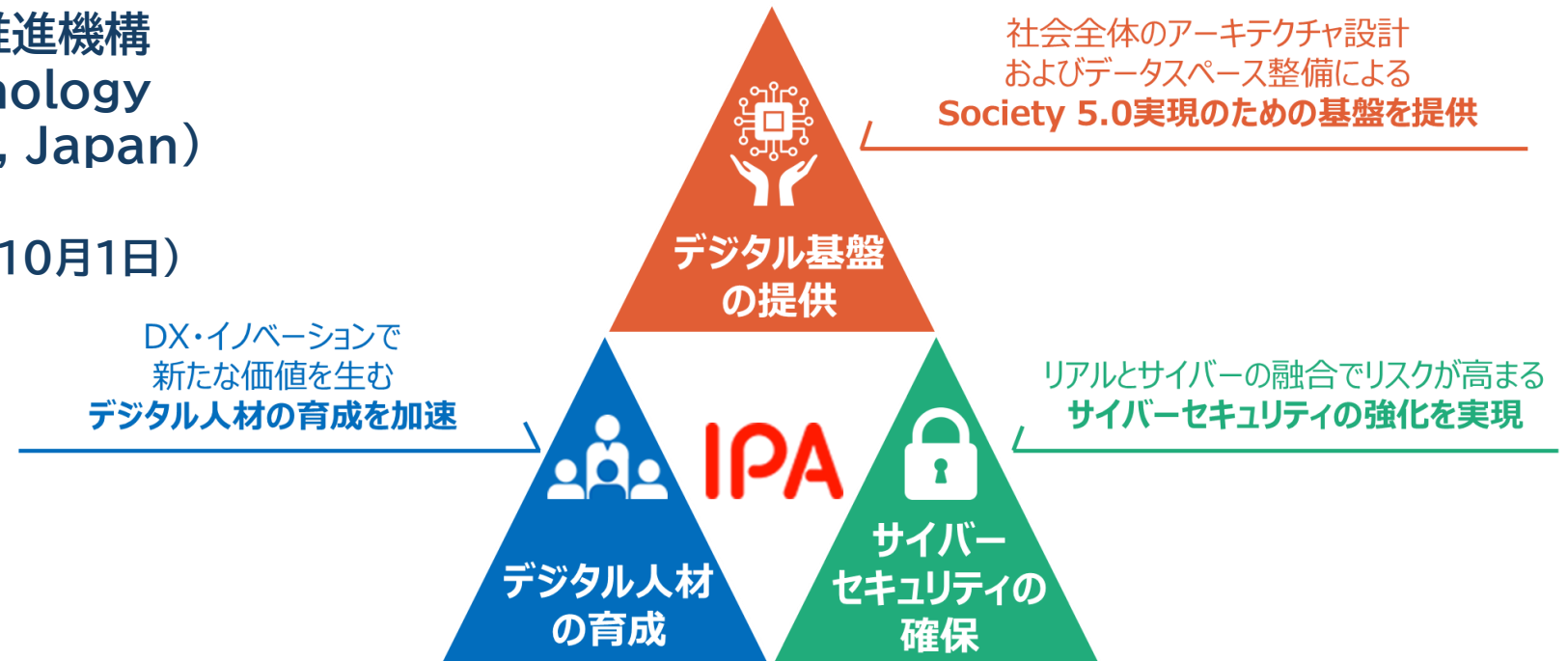
日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「頼れるIT社会」の実現を目指しています。

「人材」、「セキュリティ」、「デジタル基盤」の3つの中核事業

■ 名称: 独立行政法人情報処理推進機構
(Information-technology
Promotion Agency, Japan)

■ 設立: 2004年1月5日
(前身母体の設立は1970年10月1日)

■ 理事長: 齊藤 裕



Agenda

01. サイバー空間における昨今の脅威動向

02. 有事に向けた「仕組み」による対策 “サイバーセキュリティお助け隊サービスのご紹介”

03. 必要となる基本的対策の進め方 –その他支援施策–

01.サイバー空間における昨今の脅威動向

01.サイバー空間における昨今の脅威動向

情報セキュリティ10大脅威 2025 -組織編-

- IPAが情報セキュリティ対策の普及を目的に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、TOP10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

<解説書>



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

- 家庭等でパソコンやスマホを利用する人 「個人」
- 企業や政府機関などの組織 「組織」
- 組織のシステム管理者や社員・職員

「個人」と「組織」の2つの立場で
脅威を解説



01.サイバー空間における昨今の脅威動向

情報セキュリティ10大脅威からみえる脅威動向 -組織編-

順位	「組織」向け脅威	初選出年	選出状況(2016年～)
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

組織編はランキング形式だが…
**順位に囚われずに自組織に
合わせた対策の実施を**

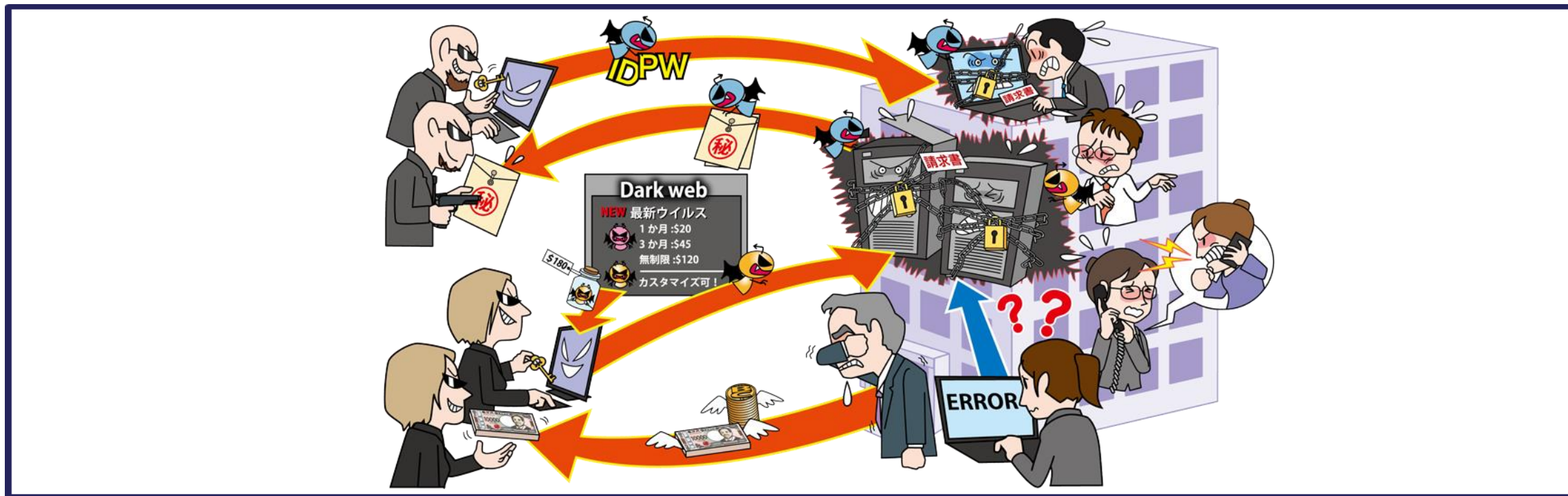
常連の脅威ばかり。
つまり、脅威に対して組織的な対
策ができていない。
**手口を知り、基本的な対策を
行うことが重要**

01.サイバー空間における昨今の脅威動向 (ご参考)情報セキュリティ10大脅威からみえる脅威動向 -個人編-

NO	「個人」向け脅威	初選出年	選出状況(2016年～)
1	インターネット上のサービスからの個人情報の窃取	2016年	6年連続9回目
2	インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
3	クレジットカード情報の不正利用	2016年	10年連続10回目
4	スマホ決済の不正利用	2020年	6年連続6回目
5	偽警告によるインターネット詐欺	2020年	6年連続6回目
6	ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
7	フィッシングによる個人情報等の詐取	2019年	7年連続7回目
8	不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
9	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続7回目
10	ワンクリック請求等の不当請求による金銭被害	2016年	3年連続5回目

個人編でのランキング形式だが
…
**枠に囚われずに啓蒙・啓発
の実施を**

01.サイバー空間における昨今の脅威動向 ランサム攻撃による被害(1位)



- ◆ 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、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

01.サイバー空間における昨今の脅威動向

ランサム攻撃による被害

● 最近のランサム攻撃の傾向

	攻撃内容	身代金を支払わせる際の脅迫内容
従来型	データ暗号化	データを復元したければ・・・
二重脅迫	機密情報の窃取	機密情報を公開されたくなければ・・・
三重脅迫	DDoS攻撃準備	DDoS攻撃をされたくなければ・・・
四重脅迫	取引先情報の窃取	情報漏えいを取引先に知られたくなければ・・・

- ・攻撃者は、**身代金が支払われるまで**何重にも脅迫する。
- ・ランサムウェアを用いずに脅迫をする攻撃 (**No Where Ransom**)が流行っている。

01.サイバー空間における昨今の脅威動向

ランサム攻撃による被害

● 攻撃の手口

- 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

- 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

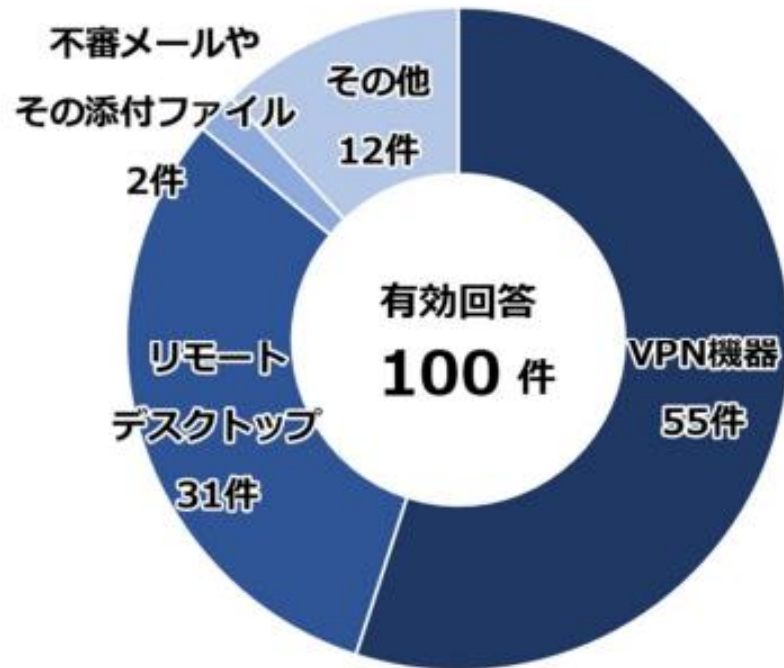
- 不正な添付ファイルを開かせて感染させる

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



01.サイバー空間における昨今の脅威動向 ランサム攻撃による被害

- 狙われ続けるリモートワーク環境
- ・2024年の国内のランサムウェア被害における感染経路は、VPN機器からの侵入が55%、リモートデスクトップからの侵入が31%と8割以上がリモートワーク環境の脆弱性に起因



【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

01.サイバー空間における昨今の脅威動向 ランサム攻撃による被害例

● ランサムウェア感染による被害と二次被害

【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/>

KADOKAWAグループ(2024年6月)

- ・ ランサムウェア攻撃を含む大規模なサイバー攻撃
- ・ 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
- ・ 攻撃組織が公開したとされる情報が、SNS 等を通じて拡散

● RaaSが利用された国内事例

【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/>

株式会社ヒロケイ(2024年6月)

- ・ 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
- ・ 攻撃者はサーバーの脆弱性およびVPN ルーターの設定不備を悪用して同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い、同社に対して金銭を要求。
- ・ 個人情報を含む情報漏えいの可能性があったが、同年8月時点では外部への流出や二次被害は確認されていないとのこと。

01.サイバー空間における昨今の脅威動向 ランサム攻撃による被害例（2025年 進行中の事案）

アサヒグループホールディングス

調査結果と今後の対応について(同社ホームページの公表情報より)

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HD

2025.11.27

お知らせ

アサヒグループホールディングス株式会社

アサヒグループホールディングス株式会社(本社 東京、社長 勝木敦志)は9月29日以降、サイバー攻撃によるシステム障害発生について公表しています。

当社は外部の専門家の協力のもと、サイバー攻撃によるシステム障害の経緯、原因の特定、情報漏えいの可能性について調査を進めてきました。現時点で調査が完了した内容や範囲は以下の通りです。調査結果に基づいて、情報漏えいが確認された方および情報漏えいのおそれがある方には、順次お知らせします。11月26日、個人情報保護委員会には確報として報告しています。

1. 事案の概要

- 9月29日午前7時ごろ、当社システムにおいて障害が発生し、調査を進める中で暗号化されたファイルがあることを確認しました
- 同11時ごろ、被害を最小限にとどめるためにネットワークを遮断し、データセンターの隔離措置を講じました
- 調査の結果、攻撃者は当社グループ内の拠点にあるネットワーク機器を経由してデータセンターのネットワークに侵入し、ランサムウェアが一斉に実行され、ネットワークに接続する範囲で起動中の複数のサーバーや一部のパソコン端末のデータが暗号化されたことが判明しました
- 攻撃を受けたシステムを中心に影響する範囲や内容の調査を進めている中で、データセンターを通じて、従業員に貸与している一部のパソコン端末のデータが流出したことが分かりました
- データセンターにあるサーバー内に保管されていた個人情報については、流出の可能性があります、インターネット上に公開された事実
は確認されていません
- 今回の攻撃の影響は、日本で管理しているシステムに限られます

これまでのリリース内容

9月29日 「サイバー攻撃によるシステム障害発生について」

- サイバー攻撃の影響を受け、システム障害が発生。
- 現時点では、個人情報や顧客データなど外部への流出は確認されていない
- 国内グループ各社の受注・出荷業務/お客様相談室などのコールセンター業務が停止

10月3日 「サイバー攻撃によるシステム障害発生について(第2報)」

- お客様および取引先の皆様の個人情報を含む重要データの保護を最優先とし、被害を最小限にとどめるために障害の発生したシステムの遮断措置の実施
- この遮断措置に伴い、国内グループ各社の受注・出荷を含めた各種業務に影響が生じています。関連して、社外の方々からの電子メール受信ができない状況
- 部分的に手作業での受注を進め、順次出荷を開始しています。

10月8日 「サイバー攻撃によるシステム障害発生について(第3報)」

- 今回の攻撃によって当社から流出した疑いのある情報をインターネット上で確認。流出した疑いのある情報の内容や範囲は調査中です。
- アサヒビール全6工場での製造は10月2日から再開しており、「スーパードライ」の出荷を一部再開

10月14日 「サイバー攻撃によるシステム障害発生について(第4報)」

- 今回攻撃を受けたシステムを中心に影響する範囲や内容の調査を進めている中で、個人情報が流出した可能性のあることが判明

<https://www.asahigroupholdings.com/newsroom/detail/20251127-0104.html>

01.サイバー空間における昨今の脅威動向 ランサム攻撃による被害例（2022年度の事案）

大阪急性期・総合医療センター

出典:大阪急性期・総合医療センター情報セキュリティインシデント調査委員会「調査報告書」

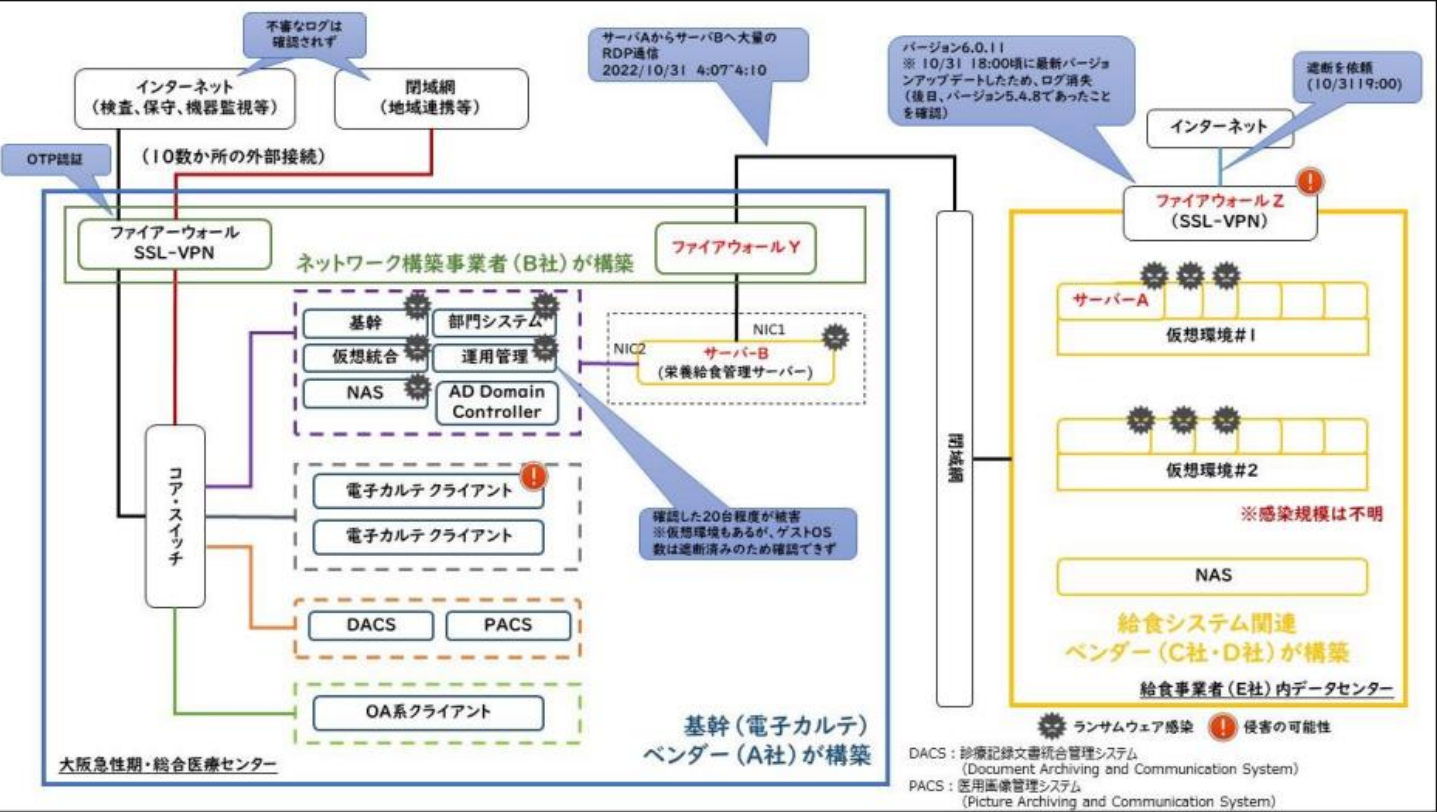


図 1 ネットワーク構成図と感染状況

表 1 侵入経路と攻撃者の手順

No	項目	攻撃者 (X) の手順
1	X が E 社給食センターに侵入	E 社給食センターに、C 社が設置した <u>ファイアウォール Z の脆弱性</u> （または、漏洩され公開されていた ID・パスワード情報）を用いて侵入。
2	E 社探索・情報窃取	E 社給食センターのサーバー A の <u>ID・パスワードが脆弱</u> だったことから、X に容易に不正アクセスされ、その後システム情報（IP アドレスやパスワード情報など）を窃取されたため、給食センター内での攻撃拡大。
3	病院給食サーバー侵入	ファイアウォール Y を通じて、 <u>病院と E 社が常時接続の RDP 通信</u> で結ばれていたことから、E 社給食センターで窃取した病院のサーバー認証情報を用いて、サーバー B に侵入。ウイルス対策ソフトをアンインストールした。
4	病院のシステム情報の窃取	サーバー B を踏み台に、病院の他サーバーの認証情報等を、X がツールを用いて窃取。なお、サーバー B と他サーバーの <u>ID・パスワードが共通</u> だったため、認証情報の窃取は容易であった。
5	他サーバー侵入	窃取した認証情報等を用いて、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示した。

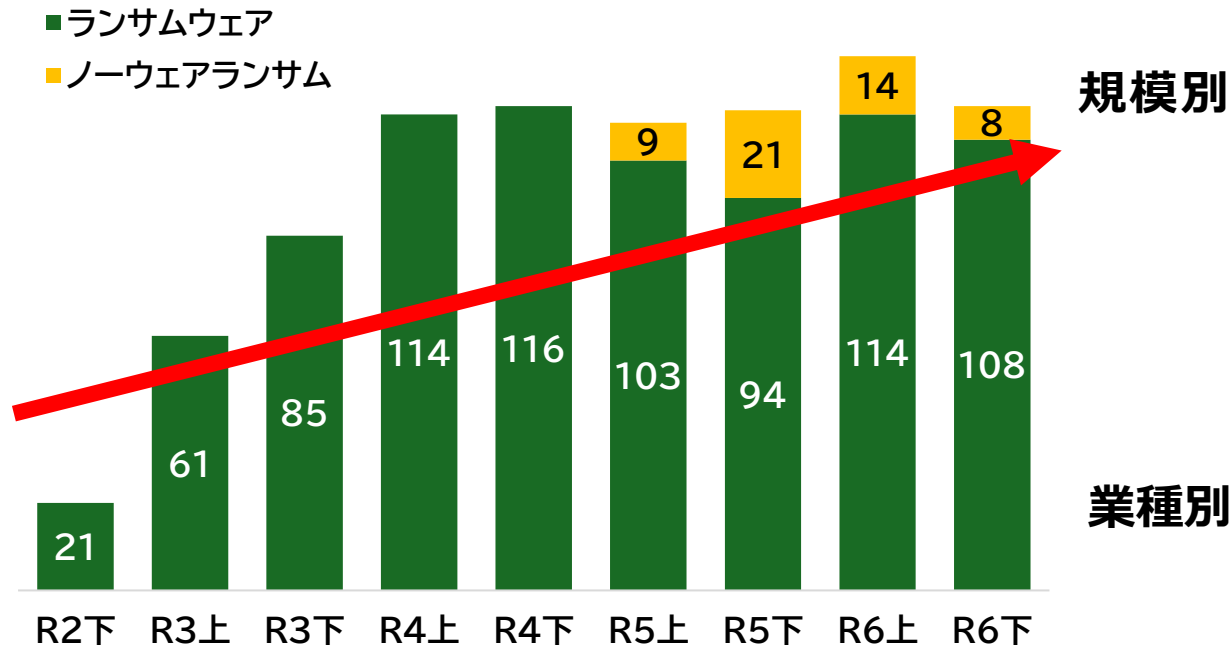
令和7年8月8日
情報セキュリティインシデント発生に伴う和解成立について
民間事業者側が当機構に対して、解決金として連帯して10億円を支払うことで合意

https://www.gh.opho.jp/gh2025/wpcontent/uploads/2025/08/info_20250808.pdf

01.サイバー空間における昨今の脅威動向

企業規模・業種を問わずサイバー攻撃は進化・拡大

企業・団体等におけるランサムウェアの
被害報告件数は右肩上がり



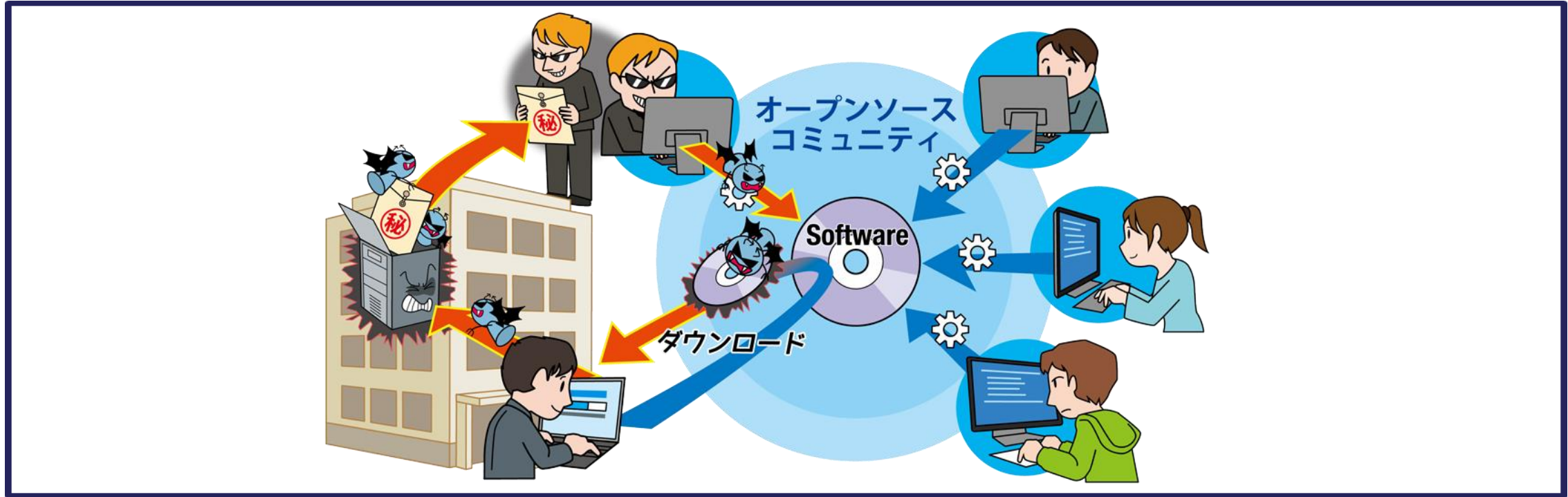
企業・団体のランサムウェア被害報告の
222件:規模・業種は多種多様



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)」をもとにIPAが作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

01.サイバー空間における昨今の脅威動向

サプライチェーンや委託先を狙った攻撃(2位)

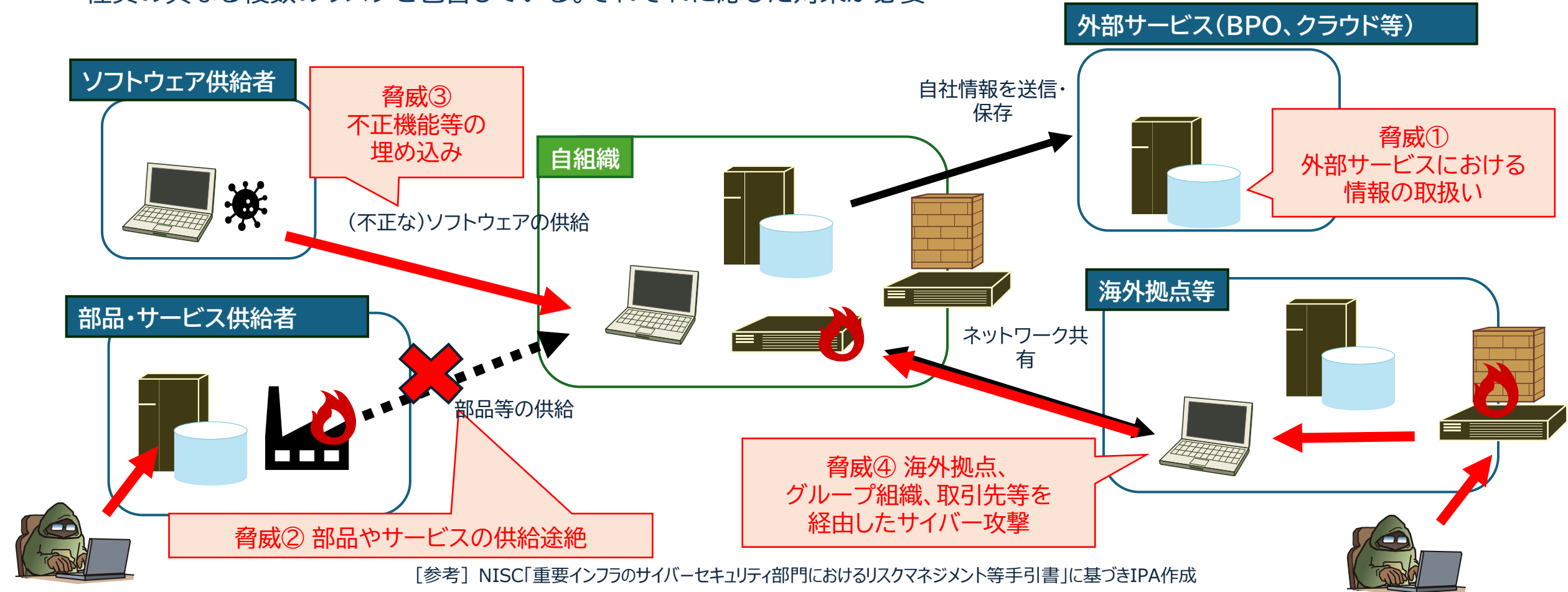


- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足掛かりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりである「ソフトウェアサプライチェーン」を悪用して攻撃される
- 取引先や業務を委託している外部組織から情報漏えいする

01.サイバー空間における昨今の脅威動向

サプライチェーンや委託先を狙った攻撃(2位)

- サプライチェーンに係る脅威は、
「不正機能等の埋め込み」「部品・サービスの提供途絶」「機密情報の漏えい等」「取引先等を踏み台とした不正侵入」等、
性質の異なる複数のリスクを包含している。それぞれに応じた対策が必要



01.サイバー空間における昨今の脅威動向

サプライチェーンや委託先を狙った攻撃被害例

● 業務委託先からの顧客情報の漏えい事例

ダイレクトメール代行会社(2024年5月)

脅威① 外部サービスにおける情報の取扱い

- VPN 経由の不正アクセスを受け、同社の端末やサーバー等がランサムウェア攻撃を受けた事例。同年6月には、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。
- 多数の自治体・民間企業が同社に印刷業務等を委託していた。このため、この攻撃によって業務委託元の組織から情報漏えいに関するお知らせが多数公表され、自治体だけでも約50万件以上の個人情報の漏えいが判明している。

● 委託先への攻撃に起因するサービス停止事例

脅威② 部品やサービスの供給途絶

物流代行・倉庫賃貸会社(2024年9月)

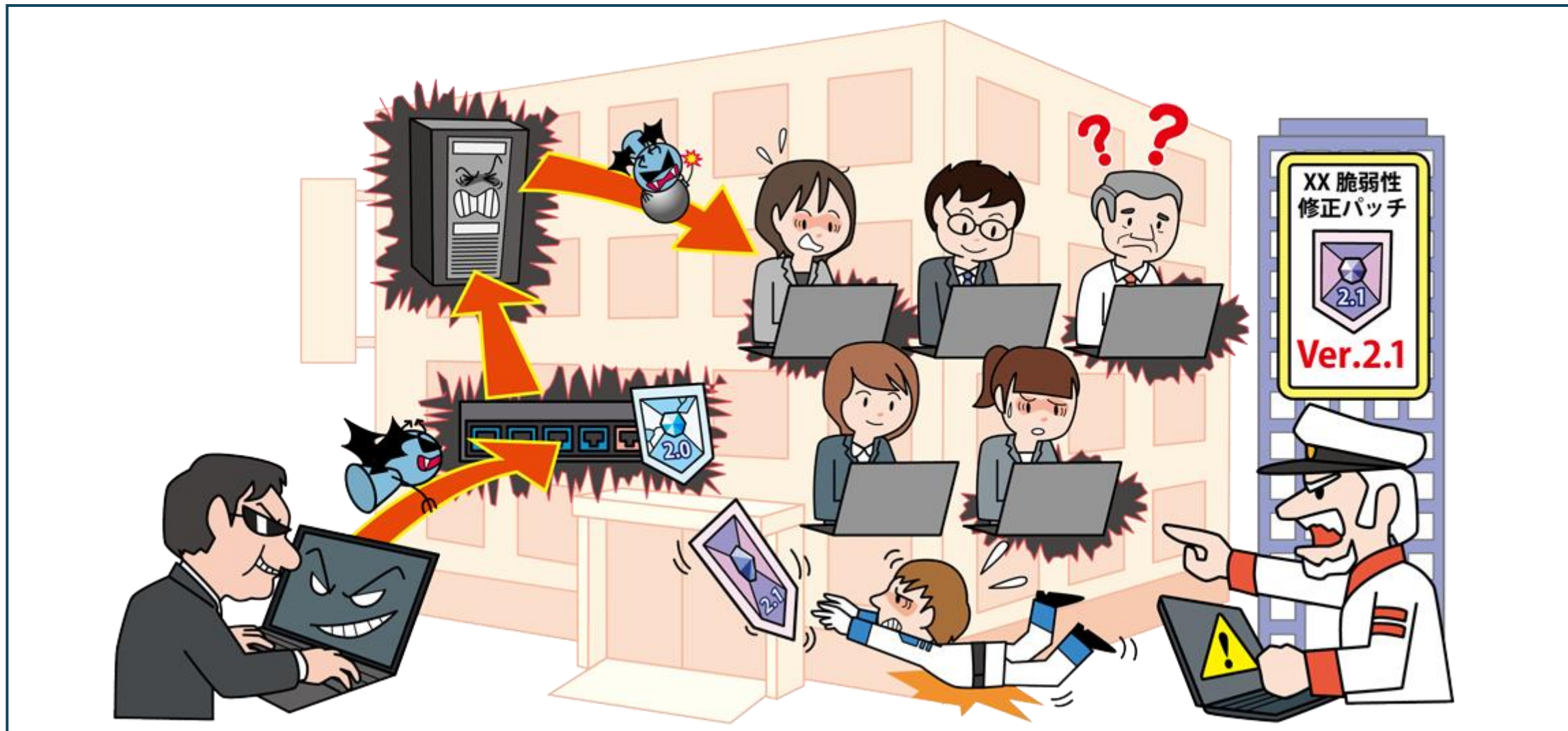
- 悪意ある第三者から不正アクセスを受け、サーバーがランサムウェアに感染した事例。これにより、入出庫関連のシステムが停止し、生産・出荷業務の一部が一時停止となった。また、この攻撃によって影響を受けた業務委託元の多数の組織からも、出荷の遅延や一時停止等が公表された。

● ソフトウェアサプライチェーンの悪用事例

脅威③ 不正機能等の埋め込み

- 2024年3月、Linux 環境で広く利用されている「XZ Utils」という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ており、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。

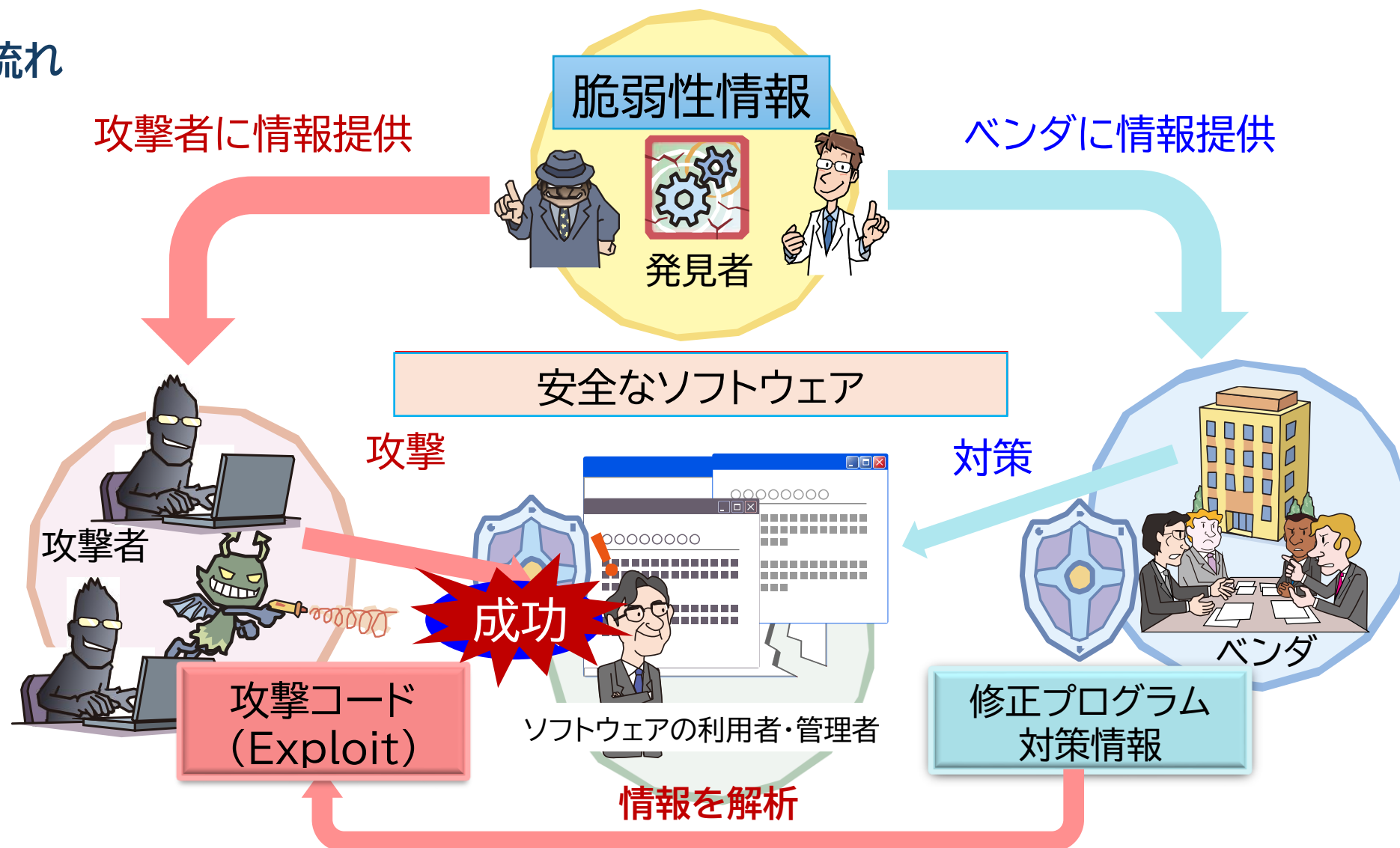
01.サイバー空間における昨今の脅威動向 システムの脆弱性を突いた攻撃



01.サイバー空間における昨今の脅威動向

【概要】システムの脆弱性を突いた攻撃

● 攻撃の流れ



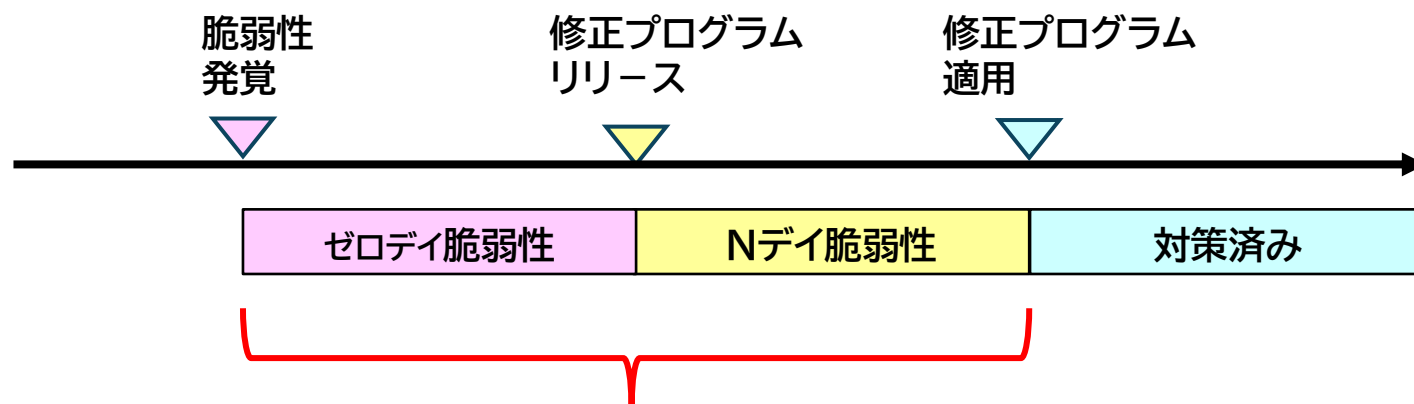
01.サイバー空間における昨今の脅威動向

【手口】システムの脆弱性を突いた攻撃

● 攻撃手口

修正プログラム適用前に脆弱性を悪用する

- ・ 開発ベンダ等が公開した修正プログラムを適用していない
- ・ 開発ベンダ等が脆弱性を認識していないと、その脆弱性に対する修正プログラムは作成されない
→ 無防備な状態の組織を攻撃する



01.サイバー空間における昨今の脅威動向

【事例】システムの脆弱性を突いた攻撃

● ゼロデイ攻撃が行われたケース

- 2024年4月、米国のセキュリティベンダは、自社のファイアウォール製品に脆弱性が見つかったことを公表した
- この脆弱性は、リモートからroot権限で任意のコード実行ができてしまうものであり、**脆弱性を悪用した攻撃が既に行われていた**ことも公表した
- IPAやJPCERT/CCからは、この脆弱性に関する注意喚起が行われ、**暫定的な緩和策等**も併せて公表された
- 脆弱性が発覚してから数日後には、セキュリティベンダから修正プログラムが提供された

【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>

01.サイバー空間における昨今の脅威動向

【事例】システムの脆弱性を突いた攻撃

● Nデイ攻撃が行われたケース

- 2024年7月、多くのシステムで利用されているプログラミング言語PHPに脆弱性があり、それを悪用した攻撃が行われていることが公表された
- この脆弱性は、組織内のネットワークに不正侵入することや、システムへの不正侵入の踏み台になるものであった
- 修正プログラムは既に提供されており、IPAからも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>

01.サイバー空間における昨今の脅威動向 サイバー脅威から組織・情報をどう守る？

“平時からの「人」の対策”と“有事に向けた「仕組み」による対策”
をバランスよく取組むことが重要

自工会/部工会・ サイバーセキュリティガイドライン

JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.3 版

2025 年 9 月 1 日

jama
Japan Automobile Manufacturers Association, Inc.

一般社団法人 日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

JAPIA
Japan Auto Parts Industries Association

一般社団法人 日本自動車部品工業会
総合技術委員会
DX 対応委員会
サイバーセキュリティ部会

よくあるご質問

中小企業において、
「自動車産業サイ
バーセキュリティ
ガイドライン」自己
評価点検で判明し
た課題にどのよう
に取組むか？

IPAからのご提案

平時からの「人」の対策(防御等)

- ・ サイバーセキュリティマネジメント体制の整備
- ・ 情報セキュリティ規程の作成、周知徹底
- ・ 教育等による社員意識醸成、向上



本日のご説明

有事に向けた「仕組み」による対策 (検知、対応、復旧等)

- ・ 目に見えないサイバー攻撃を可視化
- ・ 何か起きた場合の緊急対応・復旧

01.サイバー空間における昨今の脅威動向

IPAが提供する中小企業向け対策実践のためのツール、制度

- ・情報セキュリティの考え方や段階的に実現する為の方策を紹介する「中小企業の情報セキュリティ対策ガイドライン」。
- ・ガイドラインをベースに、セキュリティ対策への意識を持つための自己宣言「SECURITY ACTION」。
- ・常時サイバー環境を監視しつつ、インシデントが発生してしまったが対処方法がわからない、
この様な中小企業の事後対応を支援し、また簡易サイバー保険を付帯した「サイバーセキュリティお助け隊」

1 平時の対策支援(社内体制整備、意識向上)

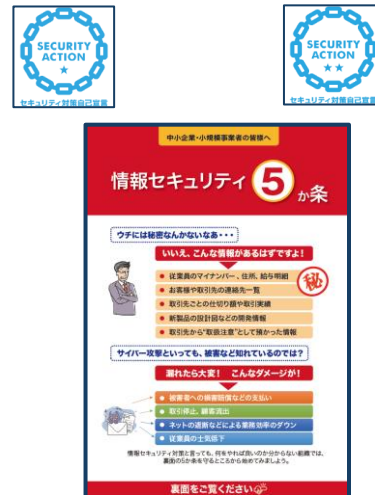
中小企業情報セキュリティ対策ガイドライン

中小企業におけるセキュリティ対策の考え方、具体的方策を紹介。



SECURITY ACTION

セキュリティ対策に取り組むことを事業者が自己宣言する制度。



2 有事の対策支援(検知、対応、復旧等)

サイバーセキュリティお助け隊

中小企業等がサイバー攻撃等で困った時の相談窓口、駆けつけ支援体制を構築。



相談窓口
異常監視

緊急時対応

簡易サイバー保険

中小企業等

相談

駆けつけ等の
対応支援

02. 有事に向けた「仕組み」による対策 “サイバーセキュリティお助け隊サービスのご紹介”

02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービスのご紹介



サイバーセキュリティお助け隊サービス

手遅れになるまえに、
手を打つ。

サイバーセキュリティ問題、起こる前に考えよう！

ワンパッケージで安価に！

見守り

(異常の監視)

24時間365日監視
挙動や問題のある攻撃を
検知しあなたのPCと
ネットワークを守ります。

駆け付け

問題が発生したときに、
地域のIT事業者等が
駆け付け対応します。
(リモート支援の場合あり)

保険

簡易サイバー保険で、
駆け付け支援等インシデント
対応時に突発的に発生する
各種コストが補償されます。



<https://www.ipa.go.jp/security/otasuketai-pr/>

02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービス制度

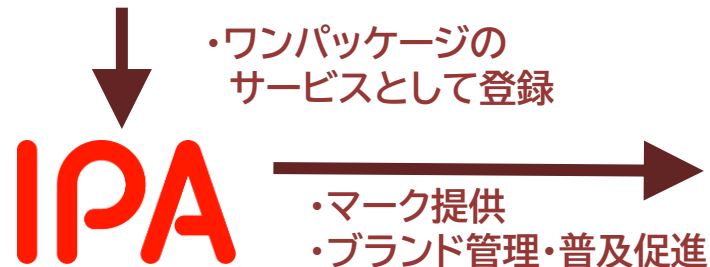
中小企業に対するサイバー攻撃への対処として不可欠なサービス要件を、ワンパッケージとしてサービス基準にまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが「サイバーセキュリティお助け隊サービス」として登録・公表する制度

◇「サイバーセキュリティお助け隊サービス基準」の主な内容

主な要件	概要
相談窓口	ユーザーからの相談を受け付ける窓口を設置／案内
異常の監視の仕組み	ネットワーク又は端末を24時間見守る仕組みを提供
緊急時の対応支援	インシデント発生などの緊急時には駆け付け支援
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：月額1万円以下(税抜き) ・端末監視型：月額2,000円以下／台(税抜き)
簡易サイバー保険	インシデント対応時に突発的に発生する駆け付け費用等を補償するサイバー保険を付帯

相談窓口、緊急時の対応支援、
簡易サイバー保険などを
ワンパッケージで提供

本サービスを採用することを通じて、
取引先企業に対する
自社の信頼性をアピール



マーク付きの
民間サービス

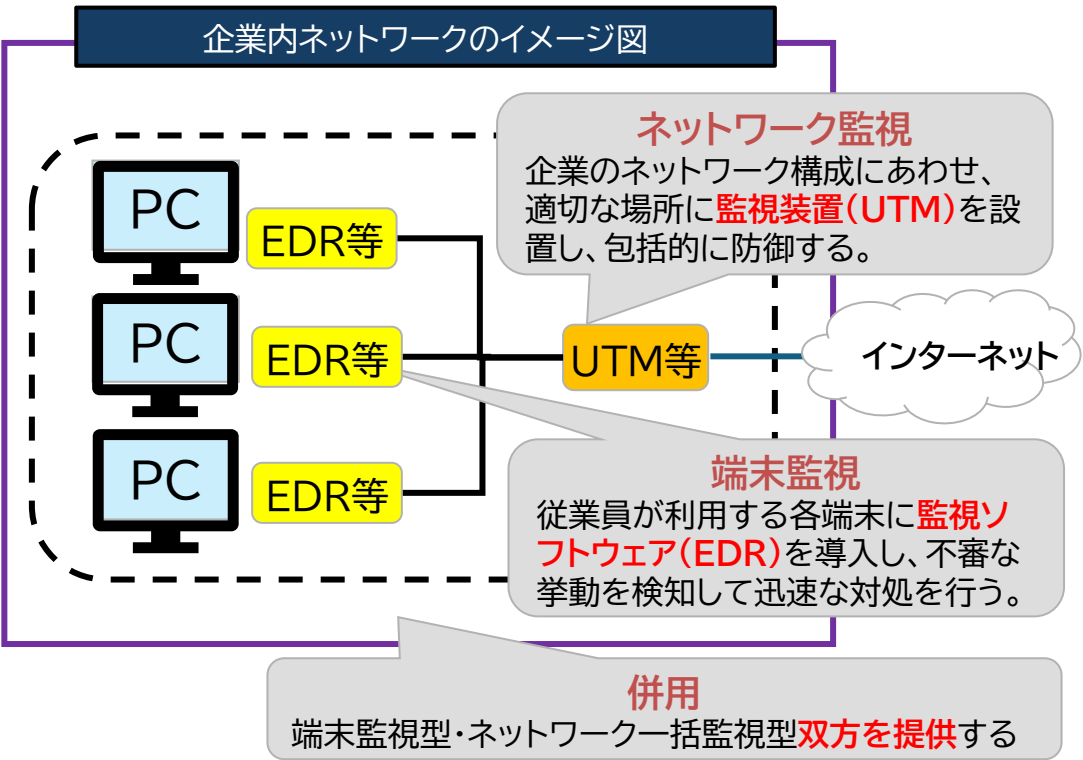


02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービス ー異常監視の仕組みー

目に見えないサイバー攻撃を可視化し、**侵入等の異常に素早く気付くことが大切。**
サイバーセキュリティお助け隊サービスでは、**ネットワーク監視、端末監視、**
または**その両方(併用)**による異常監視の仕組みを提供



◇サイバーセキュリティお助け隊サービスの監視タイプ



タイプ	特長(メリット)	導入の注意点
ネットワーク監視	<ul style="list-style-type: none"> 機器1台で監視が可能のため、設定やバージョンアップ等の更新作業などの運用コスト、業務負担が軽い。(セキュリティ管理者のみの対応) 	<ul style="list-style-type: none"> 内外の通信を監視するため、機器導入によりメールの送受信に時間がかかったり、ネットワーク接続に遅延が生じたりする可能性があるため確認が必要。
端末監視	<ul style="list-style-type: none"> 社外での打ち合わせであったり、テレワーク勤務など、社内ネットワーク外に持ち出されたPCであっても監視が可能。 	<ul style="list-style-type: none"> 導入するPC台数に応じてコストが高くなるため、社内ネットワークに接続しているPC台数の確認と、セキュリティソフトによってはインストールできないPCもあり、確認が必要。
併用	<ul style="list-style-type: none"> ネットワーク一括監視型と端末監視型の両方を設置し、多層的に防御を行う形態のため、より強固なセキュリティ監視が可能。 	<ul style="list-style-type: none"> ネットワーク一括監視型、端末監視型のそれぞれを導入することの運用の手間・コストが発生(セキュリティ管理者、従業員それぞれの対応が必要)。

※UTM(Unified Threat Management):ネットワークセキュリティ監視装置
 ※EDR(Endpoint Detection and Response):エンドポイントセキュリティソフトウェア

02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービス ー2類についてー

- お助け隊サービス1類のサービス内容では対応することが難しい中規模以上の中小企業へ向け、**お助け隊サービス2類が開始。**
- お助け隊サービス2類は提供中のお助け隊サービス1類をベースに監視製品を上位モデルに変更、**セキュリティに関する機能やサービスの追加等の拡充を行ったお助け隊サービス。**
- サービス内容の拡充に伴い、1類サービスで定めている価格要件は緩和される。



02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービス サービスを探すー

<https://www.ipa.go.jp/security/otasuketai-pr/>



サイバーセキュリティお助け隊 サービス IPA Better Life with IT

ワンパッケージで安価に！

手遅れになるまえに、
手を打つ。
サイバーセキュリティ問題、起こる前に考えよう！

見守り
(異常の監視)
24時間365日監視
事象や問題のある攻撃を
検知し必要なPCと
ネットワークを守ります。

駆付け
問題が発生したときに、
地域のIT事業者等が
駆付け対応します。
(リモート支援の場合あり)

保険
最新サイバー被害で、
駆付け支援等インシデント
対応時に実発的に発生する
各種コストが補償されます。

サイバーセキュリティ
お助け隊

サービスを探す

サービス提供事業者一覧
(対象地域から探す)

監視種別サービス一覧
(サービスを比較する)

中小企業は
サイバー攻撃の脅威にさらされている！

企業規模の小さい会社は狙われない？

いいえ、企業規模に関わらずサイバー攻撃や不正なアクセスなどの脅威に晒されています！目に見えないサイバー攻撃は気づきにくいのです。

サイバー被害を受けたらどうなるの？

対応を怠った場合の想定被害金額が5,000万円を超える事案も！

出典：令和2年度版中小企業サイバーセキュリティ対策支援体制構築事業 成果報告書

現在のサイバーセキュリティ対策では、目に見えないサイバー攻撃を可視化し、侵入等の異常に素早く気づき対応することが大切です。そこで…

02. 有事に向けた「仕組み」による対策

サイバーセキュリティお助け隊サービス サービス提供事業者を探すー

サービス提供事業者		北海道	東北	関東	中部	近畿	中国	四国	九州	沖縄
ア行	株式会社アクシス	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社アクト(東京都)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社ウェバートン			✓	✓	✓	✓		✓	✓
	大阪商工会議所	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社大塚商会	✓	✓	✓	✓	✓	✓		✓	
カ行	京セラドキュメントソリューションズジャパン株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社グローバル・リンク・コミュニケーション	✓	✓	✓	✓	✓	✓	✓	✓	✓
	コアネットインタナショナル株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	コスモテレコム株式会社		✓							
	株式会社コハマ				✓					
サ行	サンライズソフト株式会社					✓				
	株式会社清芳屋				✓					
	セキュアエッジ株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	セントラル警備保障株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社ソフトクリエイト			✓	✓	✓	✓	✓		
タ行	タクテックス株式会社				✓					
	田中工業株式会社								✓	
	中部エレコム株式会社 (旧名称:FIRAセキュリティ株式会社)				✓	✓				
	中部電力ミライズ株式会社				✓	✓				
ナ行	株式会社奈良事務機					✓				
	日本通信機器株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	日本ビジネスシステムズ株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓

02. 有事に向けた「仕組み」による対策 サイバーセキュリティお助け隊サービス サービス提供事業者を探すー

サービス提供事業者		北海道	東北	関東	中部	近畿	中国	四国	九州	沖縄
ハ行	株式会社ハイテックシステム		✓							
	バリオセキュア株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社ビープラス	✓	✓	✓	✓	✓	✓	✓	✓	✓
	富士ソフト株式会社		✓							
	富士フイルムビジネスイノベーションジャパン株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
マ行	株式会社ブライトス				✓					
	株式会社ブロードバンドセキュリティ	✓	✓	✓	✓	✓	✓	✓	✓	✓
ヤ行	三井物産セキュアディレクション株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
ラ行	株式会社四日市事務機センター					✓				
	ラディックス株式会社	✓	✓	✓	✓	✓	✓		✓	✓
ワ行	株式会社リ्यूズ			✓						
	株式会社ワールドスカイ			✓						
A～Z	株式会社BCC	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社BIZTECH								✓	
	株式会社ITガード	✓	✓	✓	✓	✓	✓	✓	✓	✓
	MS&ADインターリスク総研株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	NTTアドバンステクノロジー株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	NTT西日本株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	NTT東日本株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社PFU	✓	✓	✓	✓	✓	✓	✓	✓	✓
	株式会社Sエナジーユニオン					✓				
	SOMPOリスクマネジメント株式会社	✓	✓	✓	✓	✓	✓	✓	✓	✓

サイバーセキュリティお助け隊サービス 事例紹介① 株式会社 クロスエフェクト様

株式会社クロスエフェクト

Hatanaka Katsunori

畑中克宣



畑中克宣（はたなか・かつのり）

株式会社クロスエフェクト 専務取締役

大学卒業後、特殊車両製造メーカーで3DCAD設計に従事。2001年にクロスエフェクト、2011年に医療系臓器シミュレーター開発のクロスメディカル、2022年にデジタルに特化したクロスデザインを設立し、各社の専務取締役に就任。2013年第5回ものづくり日本大賞内閣総理大臣賞を受賞。

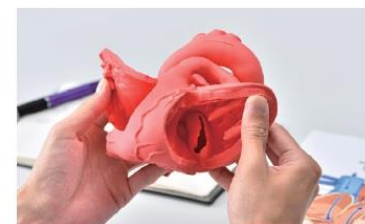
● 企業プロフィール

- ・ 所在地:京都市伏見区
- ・ 資本金:1,000万円
- ・ 従業員数:44名(グループ合計)
- ・ 2000年創業、2001年設立
- ・ 業種:樹脂成型品製造業
(プロダクトデザインおよび樹脂筐体設計、3Dスキャニング、3D開発試作モデル、真空注型品製作やその他新製品開発に係わるトータルサービス)
- ・ 特徴:さまざまな業種とメーカー等からの依頼により、試作品の提案から製造までを短納期で手がける
→機密性の高い情報を取り扱う

世界トップクラスのクオリティで心臓を3Dモデル化。 Creating 3D heart models of world class quality.



CT スキャンデータを元にリアルな臓器モデルを作成



軟質樹脂による内部構造まで再現した臓器モデル



様々な部位をリアルに再現

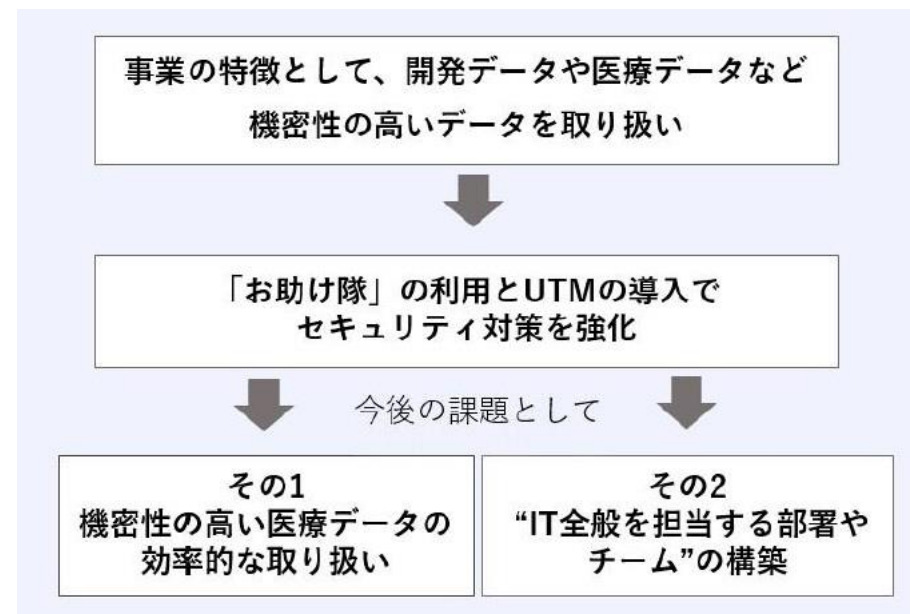
サイバーセキュリティお助け隊サービス 事例紹介① 株式会社 クロスエフェクト様

製品の極秘情報を取扱う中、お助け隊サービス(ネットワーク監視型)の導入で、セキュリティ対応の状況が手元で見えるようになり、経営陣の安心感が格段に向上！

- 開発段階の図面は、まだ上市されていない製品の極秘情報なので、絶対に外部に漏らすわけにはいかない。
また、患者さんデータ等の医療データはさらに機密性が高く、万が一、データの漏えいが発生すると、当社の信頼が失われ、すべての事業にわたって影響を及ぼしてしまう怖さがある。
- サイバーセキュリティお助け隊サービス(ネットワーク監視型/UTM)の導入により、ウイルス付きメールの防御や、不審動作の警報、メール操作状況の確認等、セキュリティ対応の状況が手元で見えるようになり、非常に安心感を与えてもらっている。
- 更には、流行りの脅威など、サイバーセキュリティお助け隊サービスから配信されるリアルタイムな「セキュリティ情報」を、そのまま従業員に転送できるので、活発なセキュリティ啓発活動が実現できている。

クロスエフェクトの取り組みのポイント

- 「お助け隊サービス(UTM)」の導入でセキュリティ対策を強化
- 今後の大きな課題は、機密性がより高い医療データの効率的な取り扱いとIT担当チームの構築
- セキュリティ意識が「自分事」となるよう、身近なトラブルや被害の実例を地道に社内発信することが重要



サイバーセキュリティお助け隊サービス 事例紹介② 創ネット 株式会社様

創ネット株式会社

Oguchi Koji

小口幸士



小口幸士(おぐち・こうじ)

創ネット株式会社 代表取締役社長

福岡市内に本社を置く、創業70年の地域密着型専門商社の3代目社長。卒業後、大手電機メーカーへ就職、企画やビジネスのノウハウを学び、2002年に創ネット株式会社へ入社。マーケティングオートメーションなど営業DXを積極的に展開中。

● 企業プロフィール

- ・ 所在地:福岡市博多区
- ・ 資本金:2,000万円
- ・ 従業員数:26名(役員・パート含む)
- ・ 1950年創業
- ・ 業種:電気設備資材卸売業
(工場で使用する生産機械(ロボット、電機・制御・電子・電材・機構部品等)、ユーティリティ設備(電気、照明、エア、蒸気、空調、省エネ機器等)の販売)
- ・ 特徴:工場のオートメーションを推進する部品の卸売り、およびエンジニアリングを行う地域密着型の企業
→中国のロボットメーカーとも取引を行う



サイバーセキュリティお助け隊サービス 事例紹介② 創ネット 株式会社様

「サイバー被害にあった」ことがセキュリティ対策のきっかけに！お助け隊サービス(端末監視型)の導入は社用車のドライブレコーダーと同じ安全策と捉えている。

- 以前に、リモートワーク中の営業社員がEmotet(エモテット※)に感染し、メールアドレスが乗っ取られ、お客様数社にも不正なメールが送信されてしまった。幸いお客様の端末感染の連絡は無く、社内端末の感染も無かったが、もし感染が広がってれば、お客様の信用失墜、営業停止まで至った可能性がある。
- サイバーセキュリティお助け隊サービス(端末監視型／EDR)の導入により、端末から不正サイトへのアクセスをブロック、ウイルスに感染した時は自動でネットワーク隔離対応を行えるようになり、自宅でのテレワークでも社員が安心して業務ができるようになった。
- 端末ごとに不正アクセスのブロック数のレポートをもらえるので、当社ではこのレポートをグループウェアにあげて、全員で見れるようにしている。これは、社用車に搭載しているドライブレコーダーと同様に、ネットワークへのアクセス状況の見える化として社員のセキュリティ意識を高めると同時に、万が一インシデントが発生した際の原因究明に役立つものと考えている。

創ネットの取り組みのポイント

- サイバーセキュリティの専門部署が無い中、もし、社内のパソコンがウイルスに感染し、大切な取引先に迷惑をかけたらどうするかを考えて対策を行う。
- 社員が出先や自宅からでも、安心して社内ネットワークにリモート接続できる環境整備が重要。
- 導入した「お助け隊サービス(EDR)」は、いわばパソコンのドライブレコーダーと考えている。



※ Emotet(エモテット): ウイルスの一種。ユーザアカウントやアドレス帳、過去のメール履歴などを窃取し、その情報を元になりすましメールを送信し、感染を拡大させる。

サイバーセキュリティお助け隊サービス

【参考】業界・業種における推奨例

- 「自工会/部工会 サイバーセキュリティガイドライン V2.3 解説書」において、サイバー攻撃や予兆を監視・分析をする体制、およびマルウェア感染後の行動追跡システムとして、サイバーセキュリティお助け隊サービスを紹介。

ラベル	目的	要求事項	No.	レベル	達成条件	解説
4 体制(平時)	情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	17	Lv2	サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有しているサイバー攻撃や予兆を監視・分析をする体制を整備している	“サイバー攻撃や予兆を監視・分析をする 体制”は、サイバー攻撃の検出や特定を行うSOC(Security Operation Center)や、インシデント対応を担うCSIRT(Computer Security Incident Response Team)と呼ばれるセキュリティ組織を指す。これらの組織は、自社で体制を整備する方法と、外部委託を活用する方法の2つがある。
22 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	138	Lv3	エンドポイントでの詳細な履歴取得およびマルウェア感染後の遠隔対応が可能な行動追跡システムを導入している	“詳細な履歴取得およびマルウェア感染後の遠隔対応が可能な行動追跡システム”としては、各種ログ取得や端末の遠隔操作ができるツール(EDR :Endpoint Detection and Response等)を導入すればよい。遠隔からの端末調査やネットワーク切断ができることがマルウェア感染後の対応として重要なポイントであるため、ログ取得を行うだけのツールでは基準に満たないことに注意すること。

※本項目達成の一助になるサービスとしてIPAのサイバーセキュリティお助け隊サービスなどがある。

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

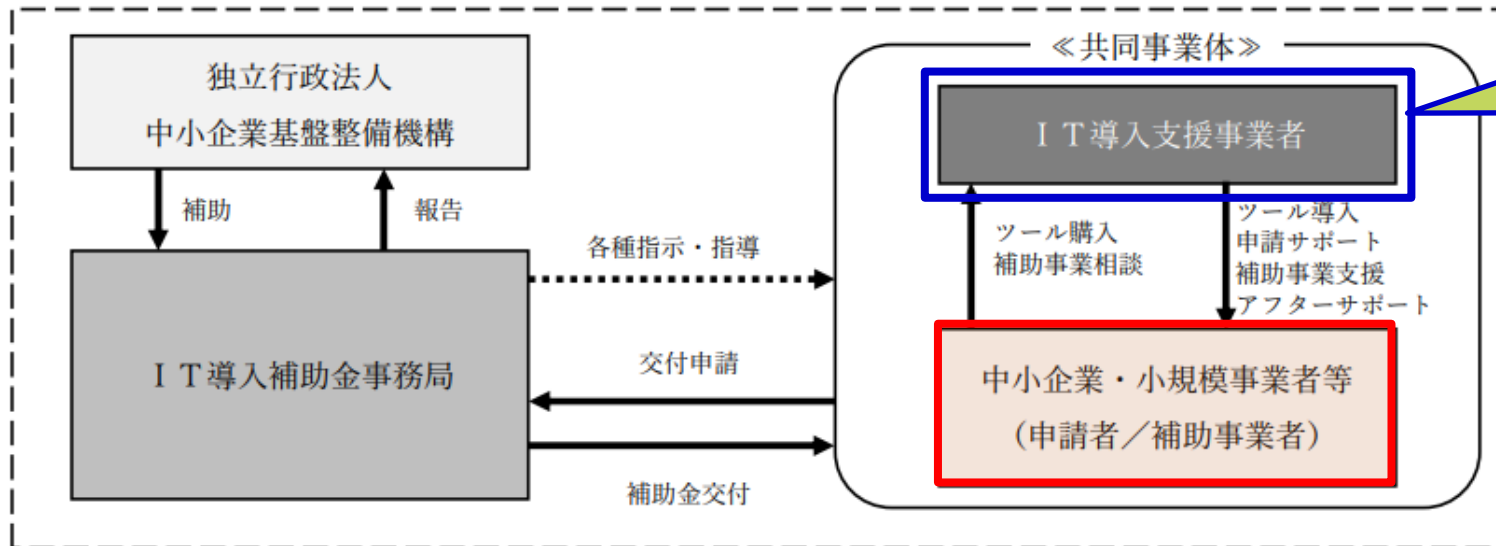
【ご参考】IT導入補助金2025 セキュリティ対策推進枠

<https://it-shien.smrj.go.jp/applicant/subsidy/security/>

中小企業・小規模事業者等が、ITツール(「サイバーセキュリティお助け隊サービス」)を導入する際の経費の一部を補助し、サイバーセキュリティ対策の強化を図る

- サイバーインシデントが原因で事業継続が困難となる事態の回避
- サイバー攻撃被害が供給制約・価格高騰を潜在的に引き起こすリスク、中小企業・小規模事業者等の生産性向上を阻害するリスクの低減

種類	セキュリティ対策推進枠
補助額	5万円～150万円
補助率	中小企業:1/2以内 小規模事業者:2/3以内
機能要件	独立行政法人情報処理推進機構が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているいずれかのサービス
補助対象	導入費用・サービス利用料(最大2年分)



お助け隊サービス提供事業者 (または再販協力事業者)
 ※ IT導入補助金事務局にIT導入支援事業者として別途登録した事業者

詳細は「IT導入補助金2025」
<https://it-shien.smrj.go.jp/>

※ IT導入補助金2023 公募要領セキュリティ対策推進枠から転載、引用 https://www.it-hojo.jp/r04/doc/pdf/r4_application_guidelines_security.pdf

03. 必要となる基本的対策の進め方 —その他支援施策—

03. 必要となる基本的対策の進め方 -その他支援施策- IPAが提供する中小企業向け対策実践のためのツール、制度

- ・情報セキュリティの考え方や段階的に実現する為の方策を紹介する「中小企業の情報セキュリティ対策ガイドライン」。
- ・ガイドラインをベースに、セキュリティ対策への意識を持つための自己宣言「**SECURITY ACTION**」。
- ・常時サイバー環境を監視しつつ、インシデントが発生してしまったが対処方法がわからない、
この様な中小企業の事後対応を支援し、また簡易サイバー保険を付帯した「サイバーセキュリティお助け隊」

1 平時の対策支援(社内体制整備、意識向上)

中小企業情報セキュリティ対策ガイドライン

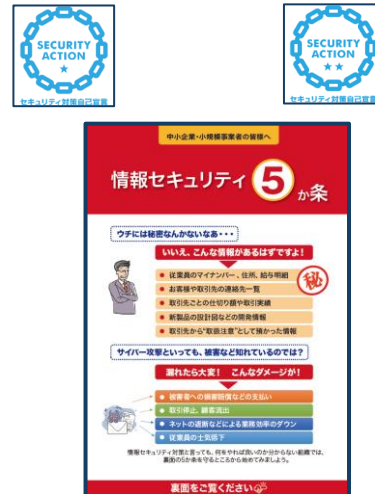
中小企業におけるセキュリティ対策の考え方、具体的方策を紹介。



2

SECURITY ACTION

セキュリティ対策に取り組むことを事業者が自己宣言する制度。



有事の対策支援(検知、対応、復旧等)

サイバーセキュリティお助け隊

中小企業等がサイバー攻撃等で困った時の相談窓口、駆けつけ支援体制を構築。



お助け隊サービス

相談窓口
異常監視

緊急時対応

簡易サイバー保険

中小企業等

相談

駆けつけ等の
対応支援

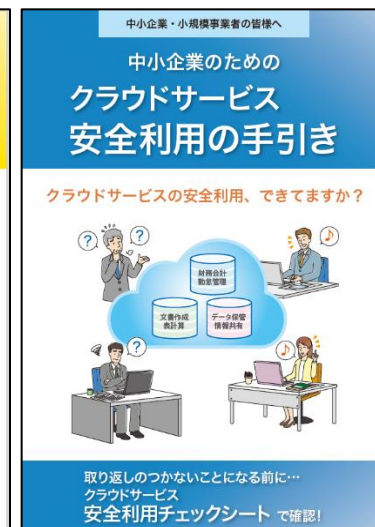
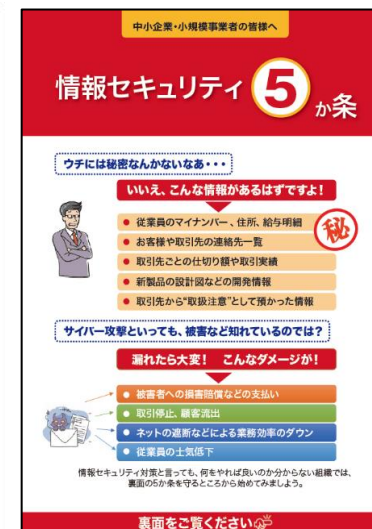
03. 必要となる基本的対策の進め方 -その他支援施策- 中小企業の情報セキュリティ対策ガイドライン 第3.1版

- 中小企業の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し、**情報を安全に管理**するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
 - 経営者が認識すべき**「3原則」**、経営者がやらなければならない**「重要7項目の取組」**を記載
 - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
 - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等の**ひな形**を付録
 - **「中小企業のためのセキュリティインシデント対応の手引き」**を追加



03. 必要となる基本的対策の進め方 -その他支援施策- 中小企業の情報セキュリティ対策ガイドライン 第3.1版

構 成		概 要
本 編	第1部 経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
	第2部 実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付 録	付録1 情報セキュリティ5か条	組織の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明しています。
	付録2 情報セキュリティ基本方針(サンプル)	組織としての情報セキュリティに対する基本方針書のサンプルです。
	付録3 5分でできる！ 情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
	付録4 情報セキュリティハンドブック(ひな形)	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
	付録5 情報セキュリティ関連規程(サンプル)	情報セキュリティに関する社内規則を文書化したもののサンプルです。
	付録6 中小企業のための クラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
	付録7 リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性(リスク)の見当をつけることができます。
	付録8 中小企業のためのセキュリティ インシデント対応の手引き	情報漏えいやシステム停止などのインシデント対応のための手引きです。



03. 必要となる基本的対策の進め方 -その他支援施策- 中小企業の情報セキュリティ対策ガイドライン 活用方法

・できるところから始めて段階的にステップアップ



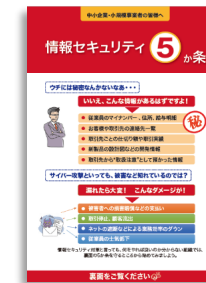
03. 必要となる基本的対策の進め方 -その他支援施策- SECURITY ACTION制度

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度（2025年5月時点で、40万件に到達）
- 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取り組み目標を用意



1段階目(一つ星)

「情報セキュリティ5か条」に取り組むことを宣言



- 情報セキュリティ5か条に取り組む

【情報セキュリティ5か条】

- OSやソフトウェアは常に最新の状態にしよう！
- ウィルス対策ソフトを導入しよう！
- パスワードを強化しよう！
- 共有設定を見直そう！
- 脅威や攻撃の手口を知ろう！



2段階目(二つ星)

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言



- 情報セキュリティ自社診断を実施
- 基本方針を策定

【基本方針の記載項目例】

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善 など

【ご参考】SECURITY ACTION 申請・加点要件としている補助金・助成金

- デジタル化やサイバーセキュリティ対策などを支援するIT導入の補助金申請の要件にするなど、各種補助金・助成金制度においてSECURITY ACTION制度を活用
- 引き続き各地方自治体や団体組織等とも連携の上、取組みを拡大予定

【自治体等におけるSA制度の活用事例】

- IT導入補助金(通常枠・セキュリティ対策推進枠・デジタル化基盤導入枠):中小企業庁
- 事業承継・引継ぎ補助金(経営革新):中小企業庁
- 地域医療介護総合確保基金を利用したICT導入支援事業:厚生労働省 ※実施主体は各都道府県
- 事業再構築補助金(サプライチェーン強靱化枠):中小企業庁 (2023/3)
- -----
- サイバーセキュリティ対策促進助成金:東京都中小企業振興公社
- 鹿児島県 かごしま中小企業DX推進事業費補助金(令和6年度): 鹿児島県
- 堺市中小企業デジタル化促進補助金:大阪府堺市
- デジタル化トライアル事業費補助金(2023年度):秋田県
- 「情報セキュリティ基本方針 策定支援専門家派遣」事業(2019年度):東京都中小企業振興公社
- 中小企業等スマートワーク促進補助金(情報セキュリティ事業)(2022年度):岐阜県
- デジタル技術導入補助金(2023年度):愛知県 (2023/5) ※採択審査の加点対象
- デジタル化促進補助金(2023年度):北海道札幌市 (2023/5) ※採択審査の加点対象、採択後の自己宣言
- 産業デジタル実装支援事業費補助金(2023年度):宮崎県 (2023/9)
- DX(デジタル化)設備導入補助金(2023年度):石川県 (2023/12)
- -----
- DX認定制度:IPA ※サイバーセキュリティ対策の推進においてセキュリティ監査の実施概要をまとめることが要件であるが、中小企業、個人事業主の場合は二つ星で代替可

03. 必要となる基本的対策の進め方 -その他支援施策- SECURITY ACTION制度 -申し込み方法-

SECURITY ACTION

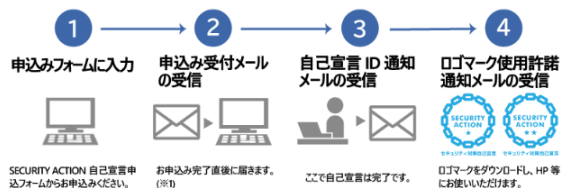
セキュリティ対策自己宣言

お問い合わせ

IPA

Home SECURITY ACTIONとは? 「一つ星」を宣言する 「二つ星」を宣言する 自己宣言の申込方法 宣言事業者一覧

セキュリティアクション SECURITY ACTION 自己宣言の申込方法



お申込日 お申込日から1週間後 (※1) お申込日から2～3週間後

(※1) 申込み受付メールが届かない場合は、メールアドレス登録誤り、あるいは迷惑メールフォルダ等に振り分けされている可能性があります。受け取れない場合は再度お申込みいただきますよう、お願いいたします。

(※2) 当機構の営業日対応で、通常は申込日から3日後の届でお知らせをしていますが、お申し込み状況によっては1週間となるケースも考えられます。余裕を持ってお申し込みいただくよう、お願いします。

Caution!

【注意】
自己宣言を過去に行っているかどうか、ご不明の場合は以下でご確認ください。
お申し込みされるより早く、宣言有無や自己宣言IDを確認できる場合もあります。

方法1: 宣言事業者一覧から検索
方法2: お問い合わせフォームで「自己宣言をしているか忘れた、自己宣言IDを忘れた」を選択し、必要事項を入力してお問い合わせ (お問い合わせフォームは外部サービス (WEBCAS) を利用しています。)

※自己宣言ID・登録状況の照会には自己宣言事業者 (ご担当者様) ご本人より行ってください。

SECURITY ACTION自己宣言のお申し込み手順

1: 申込みフォームに入力

- (1) 個人情報の取扱いについての同意
- (2) 「SECURITY ACTIONロゴマーク使用規約」の同意
「SECURITY ACTIONロゴマーク使用規約」のダウンロード(PDF:200KB)
- (3) 自己宣言の取組内容 (一つ星or二つ星) の選択
※「一つ星」「二つ星」同時に使用することはできません。
情報セキュリティ対策への取組段階に応じて、使用いただけるロゴマークは異なります。
- (4) 自己宣言の目的、担当者等の入力
- (5) 事業者情報の入力
宣言事業者として、IPAホームページで公開される情報は以下となります。
【法人】 事業者名、都道府県、市区町村・町名、業種、取組段階 (一つ星or二つ星)
【個人事業主】 代表者名、屋号、都道府県、市区町村・町名、業種、取組段階 (一つ星or二つ星)
- (6) お申込み完了

2: 申込み受付メールの受信

「1: 申込みフォームに入力(6)」の直後に届きます。
From: application@ipa.go.jp
Subject: 【SECURITY ACTION】 ○つ星: 自己宣言受け付け確認のお知らせ
※○は一つ星 or 二つ星

【注意】 メールアドレスの入力誤りにご注意ください
メールアドレスを誤って入力されると、自己宣言のお申込み受付はできません。お申込み直後に発信している受付メールが届かない場合は、迷惑メールに入っている、もしくは入力したアドレスが間違っている可能性がありますので、再度お申込みいただきますよう、お願いいたします。

3: 自己宣言ID通知メールの受信

1週間程度で自己宣言IDをお知らせするメールが届きます。
From: security-action-info@ipa.go.jp
Subject: 【SECURITY ACTION】 自己宣言IDのお知らせ

SECURITY ACTION自己宣言のお申し込みはこちら

自己宣言申込みフォーム

お申込みフォームは外部サービス (WEBCAS) を利用しています。



<https://www.ipa.go.jp/security-action/entry/>

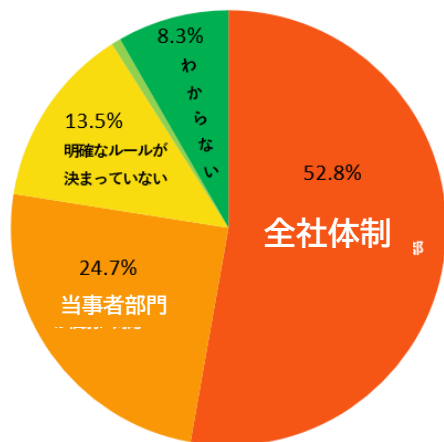
03. 必要となる基本的対策の進め方 -その他支援施策-

内部不正対策

海外子会社、グループ子会社、委託先事業者も含め、
守るべき情報資産の所在を把握し、それを適切にカバー
できるよう全社的な内部不正対策が重要

内部不正対策を全社体制で行っているのは全体の5割のみ

重要情報が漏えいした時に対応する部門



企業の内部不正防止体制に関する実態調査(2023年4月)Q10を基に再構成

👉 各部門が連携した全社的な対応が重要

経営者、コンプライアンス部門

- 基本方針の策定
 - 資産の把握、対応体制の整備
 - 人的管理およびコンプライアンス教育の徹底
- 情報システム／セキュリティ管理部門
- 重要情報の利用者ID、アクセス権の管理
 - システム操作履歴の監視

「組織における内部不正防止ガイドライン」
第5版(IPA)



「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の33項目の具体的な対策を提示

<https://www.ipa.go.jp/security/guide/insider.html>

「秘密情報の保護ハンドブック」令和6年2月改訂版(経産省)



秘密情報の漏えいを防止する、様々な対策例を紹介

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

「営業秘密支援窓口」(INPIT)



中小企業等を対象に、秘密情報の抽出や管理ルールの整備、社内セミナーの実施等の支援サービスを提供





<https://www.inpit.go.jp/katsuyo/tradecret/madoguchi.html>

03. 必要となる基本的対策の進め方 –その他支援施策– 映像で知る情報セキュリティ

- ・ 情報セキュリティに関する様々な脅威と対策を10分程度のドラマなどで分かりやすく解説した映像コンテンツ掲載。
YouTube「IPAチャンネル」では全タイトルをいつでも視聴可能
- ・ 社内研修等営利を目的としない用途に限り、主な映像の動画ファイルを無償で提供(ダウンロード)



主な映像コンテンツ

	<p>今、そこにある脅威～内部不正による情報流出のリスク～ 社員による内部不正で機密情報が外部に流出する危機が発覚。機密情報の流出は防げたが、なぜこのような事態が発生したのか、背景を探りつつ内部不正による被害事例や手口、不正を起こさせないポイントの他、自社における経営者や管理部門だけでなく、関連会社や国内外の委託先なども含め、組織全体で実施すべき内部不正対策について解説しています。</p>	約18分
	<p>今、そこにある脅威～組織を狙うランサムウェア攻撃～ 身代金として金銭を得ることを目的に企業・組織内のネットワークへ侵入し、データを一斉に暗号化して使用できなくしたりする”ランサムウェア攻撃”。本作ではその攻撃の手口、経営者・管理者・システム担当者、従業員が行うべき対策などを解説しています。</p>	約15分
	<p>華麗なる情報セキュリティ対策 「華麗なる情報セキュリティ対策」シリーズは、組織の従業員が日常行うべき8つの対策をご紹介します。</p>	8話構成 各話2分
	<p>妻からのメッセージ ～テレワークのセキュリティ～ テレワークでは職場の情報セキュリティ対策と同様に「情報漏えい」や「不正アクセス」などの被害に遭わないよう対策を講じる必要があります。本映像の主人公と一緒にテレワークのセキュリティ対策を学んでいきましょう。</p>	約10分

03. 必要となる基本的対策の進め方 -その他支援施策- 企業向けの総合的な相談窓口の設置

- ・IPAでは、企業・組織向けに、コンピュータウイルス感染や不正アクセス等のセキュリティインシデントに関する相談や届出、情報提供を受け付ける窓口を設置！
- ・セキュリティインシデント等が発生し、お困りの際は、下記ポータルページの活用を！

提供中




詳細はこちらのページにて

■ URL
<https://www.ipa.go.jp/security/todokede/incidentportal.html>



複数の窓口を整理統合

2025年4月企業向けの総合的な相談窓口を新たに開設

■ 「企業/組織向けサイバーセキュリティ相談窓口」

- ・ 各種インシデント発生時の初動対応に関する相談
- ・ 標的型サイバー攻撃に関するインシデント相談
- ・ その他の情報セキュリティに関する一般的な相談
 - ・ 脅威情報に関する情報提供受付

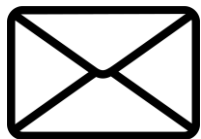
	相談・届出の例
インシデント発生時の初動対応	<ul style="list-style-type: none"> ・ ランサムウェアに感染した。対処方法を相談したい ・ 自組織のウェブサイトが改ざんされた。対処方法と再発防止策を相談したい など
標的型サイバー攻撃に関するインシデント相談	<ul style="list-style-type: none"> ・ 標的型サイバー攻撃が疑われる事案が発生したため、相談や情報提供を行いたい
脅威情報に関する情報提供受付	<ul style="list-style-type: none"> ・ ランサムウェア感染したためインシデント内容を公的機関へ届出(情報提供)したい ・ サイバー攻撃被害の保険適用を受けるため公的機関への届出を行いたい ・ 日本国内利用のOS、ブラウザ、メール等の脆弱性を届出たい ・ 日本国内からのアクセスが想定されているインターネット上のウェブサイト等で稼動するシステムの脆弱性など

03. 必要となる基本的対策の進め方 -その他支援施策- 中小企業向けサイバーセキュリティ対策支援者リスト

- 国家資格「**情報処理安全確保支援士(登録セキスペ)※**」の資格者のうち、**中小企業向けのサイバーセキュリティ対策支援が実施できる専門家の得意分野・専門領域を可視化**したリスト(支援対象地域別)
- 現段階の情報を試行公開(PDF)。今後、整備・拡充する予定
※サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、セキュリティの確保を支援する。国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務を有する。<https://www.ipa.go.jp/jinzai/riss/index.html>
- 掲載専門家の**支援対象地域別**にリスト化。
 - 支援対象地域:北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄
- 掲載専門家が**支援可能な指導テーマ、支援実績、得意とする業界、支援可能形態、支援料金、保有資格、保有スキル等**を記載。
- 専門家による中小企業指導の支援ツール(5テーマの実施要領)を整備・公表
 - テーマ(1) 情報セキュリティ規程の整備
 - テーマ(2) 情報資産の洗い出しとリスク分析
 - テーマ(3) クラウドサービスの安全利用
 - テーマ(4) セキュリティインシデント対応
 - テーマ(5) 従業員向け情報セキュリティ教育



IPAメールニュース & 公式アカウント



セキュリティ関連情報、イベント・セミナーの開催情報や情報処理技術者試験に関する情報をメール配信しています。

メールニュースご登録 <https://www.ipa.go.jp/mailnews.html>



IPAの各種情報を配信する公式アカウントです。このほか、各専門分野の最新情報を発信するアカウントもございます。

X公式アカウント <https://x.com/IPAjp/>



IPAのイベント情報や情報セキュリティ関連などの最新情報を配信するIPA公式アカウントです。

Facebook公式アカウント <https://www.facebook.com/ipaprip/>



情報セキュリティやソフトウェア開発関連など、研修や個人学習に最適な映像コンテンツを見ることができます。

YouTube「IPA Channel」 <https://www.youtube.com/user/ipajp/>



IPA