



2023.12.06

サイバーセキュリティセミナー in Amagasaki

サイバー空間をめぐる 脅威の現状

兵庫県警察サイバーセキュリティ・捜査高度化センター
サイバー企画課 サイバー情報発信室

サイバー空間の現状

過去



現在



地域、年齢性別問わず、全国民が参加する公共空間

脅威の現状

我が国を取り巻く現状

- ◇ サイバー空間の公共空間化が加速
- ◇ 厳しい安全保障環境の中、高い地政学的緊張
- ◇ 先端技術、知的財産等を有する企業等が国内に多数
- ◇ 大阪・関西万博等、関心を集める行事が開催

高水準で推移するランサムウェア被害

クレジットカード不正利用被害の急増

インターネットバンキングに係る不正送金被害の急増

違法情報、有害情報の氾濫

などなど。。。



脅威の現状

サイバー事案への対処能力の強化

諸外国と連携した脅威への対処



令和4年度に警察庁に**サイバー警察局**を、
関東管区警察局に**サイバー特別捜査隊**を新設



兵庫県警察

令和5年3月24日、サイバーセキュリティ・捜査高度化センターに
(略称:サイバーセンター)

サイバー企画課・サイバー捜査課

を新設

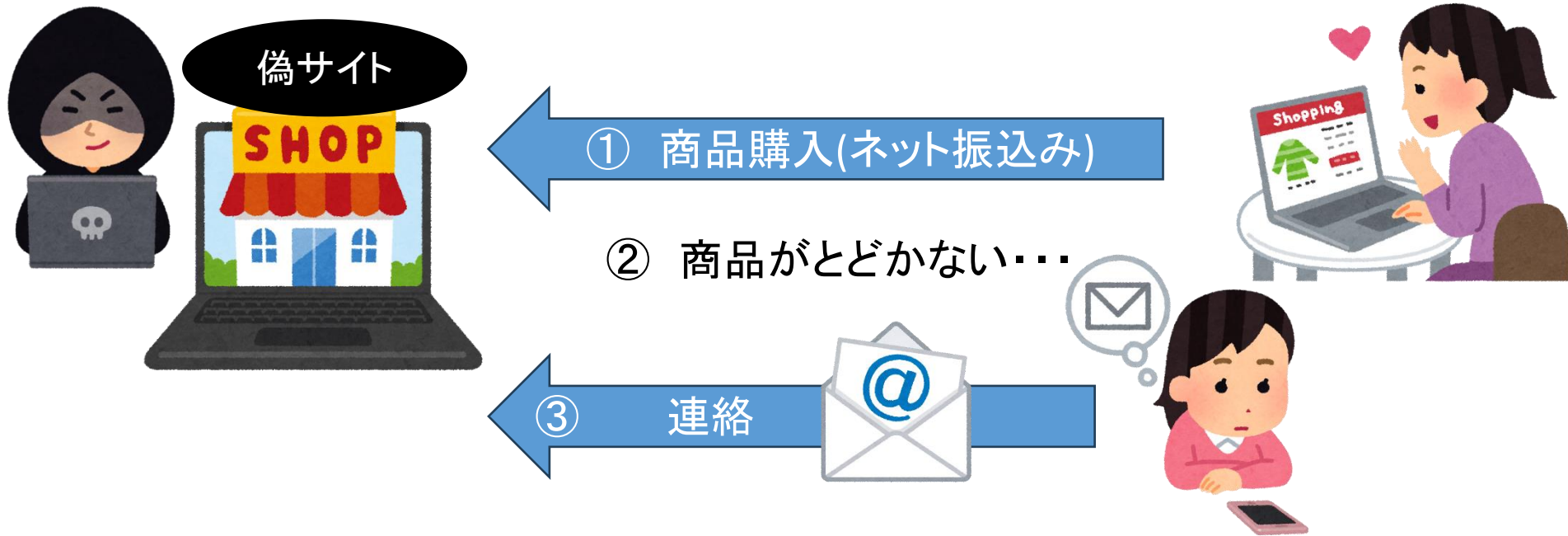


旬な2つのキーワード

返金

NB

新たな詐欺手口



不正送金被害の急増(全国)



警察庁広報資料：「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について(注意喚起)」
https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf

- 被害の多くはフィッシングによるものとみられる。
- 金融機関(銀行)を装ったフィッシングサイト(偽のログインサイト)へ誘導するメールを多数確認
- 上半期だけで、過去最多2,322件、約30億円の被害

サイバーセキュリティ対策について



狙われているのは・・・

大企業だけではない

- サイバー攻撃の標的は政府・自治体や重要インフラだけではない
- 大規模なサイバー攻撃には、数十万台の端末から一斉攻撃をかける手口があり、それに使用される端末は攻撃者に乗っ取られた端末
- 大企業は防御が厳重なため、セキュリティの甘い取引先の中堅・中小企業を狙い、そこから大企業のシステム内部へ侵入するケースも増えている



企業におけるサイバーセキュリティ対策の必要性

○ 自社の損失だけにとどまらない！？

被害を受けると金銭の損失だけでなく、サプライチェーン企業が影響を受け、取引が停止するなど、経営に直結する重大なリスクが発生する

○ 実はもう侵入されている！？

ランサムウェアのように、被害が表面化する前からシステムに侵入されているかも

○ あなたが攻撃者にされてしまうかも！？

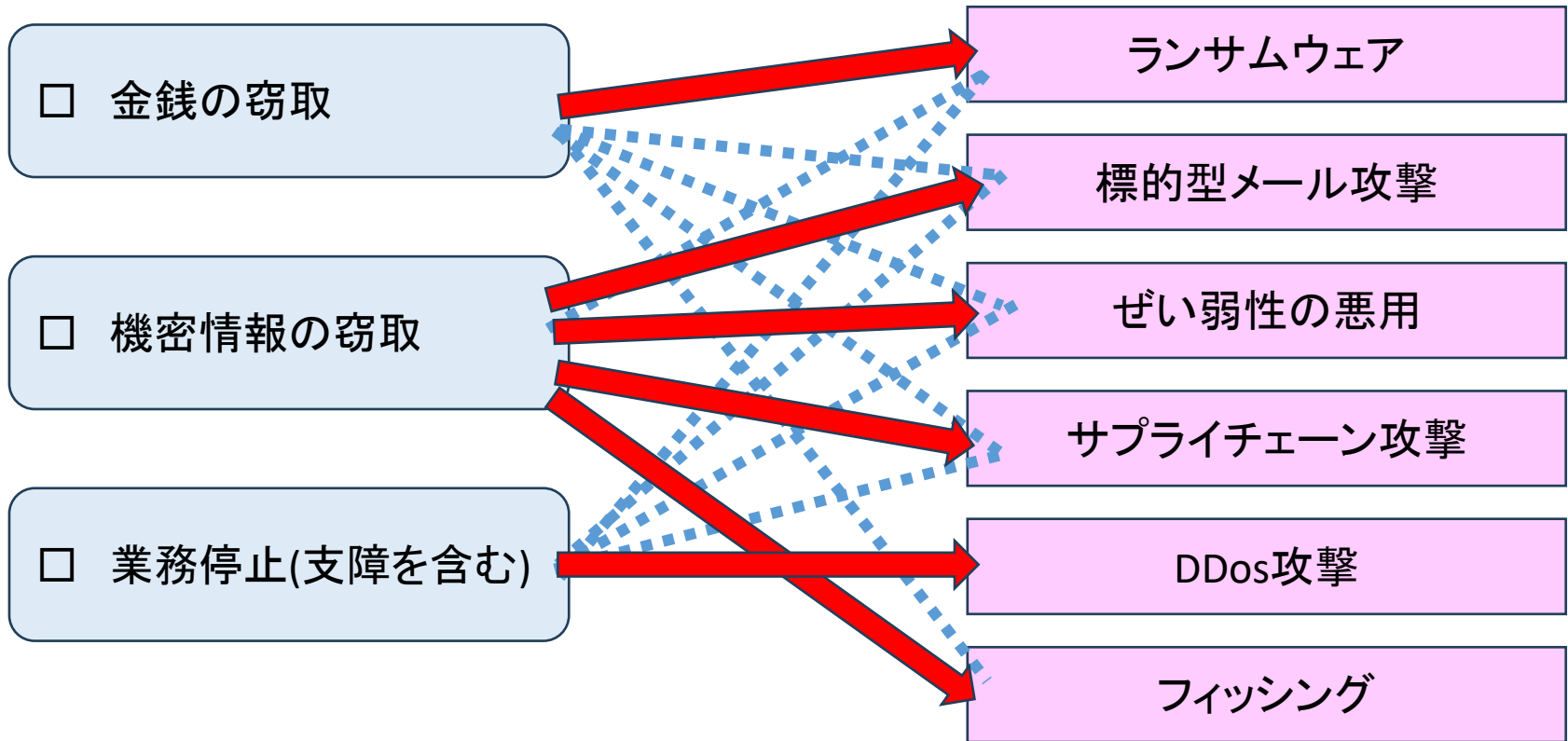
被害を受けるだけでなく、自社の機器が踏み台にされて、他の会社等に攻撃をしかけるなど、意図せずに攻撃側になってしまうことも

「攻撃を受けるような情報を持っていない」、「攻撃を受けるような会社ではない」は、セキュリティ対策を実施しない理由とはなりません。

サイバー事案による組織への影響

主な影響(攻撃目的)

攻撃の手口の例



攻撃の目的及び手口は1つに限られず、
様々な影響を受ける可能性

企業を狙う脅威の現状

～ランサムウェア～



IPA情報セキュリティ10大脅威

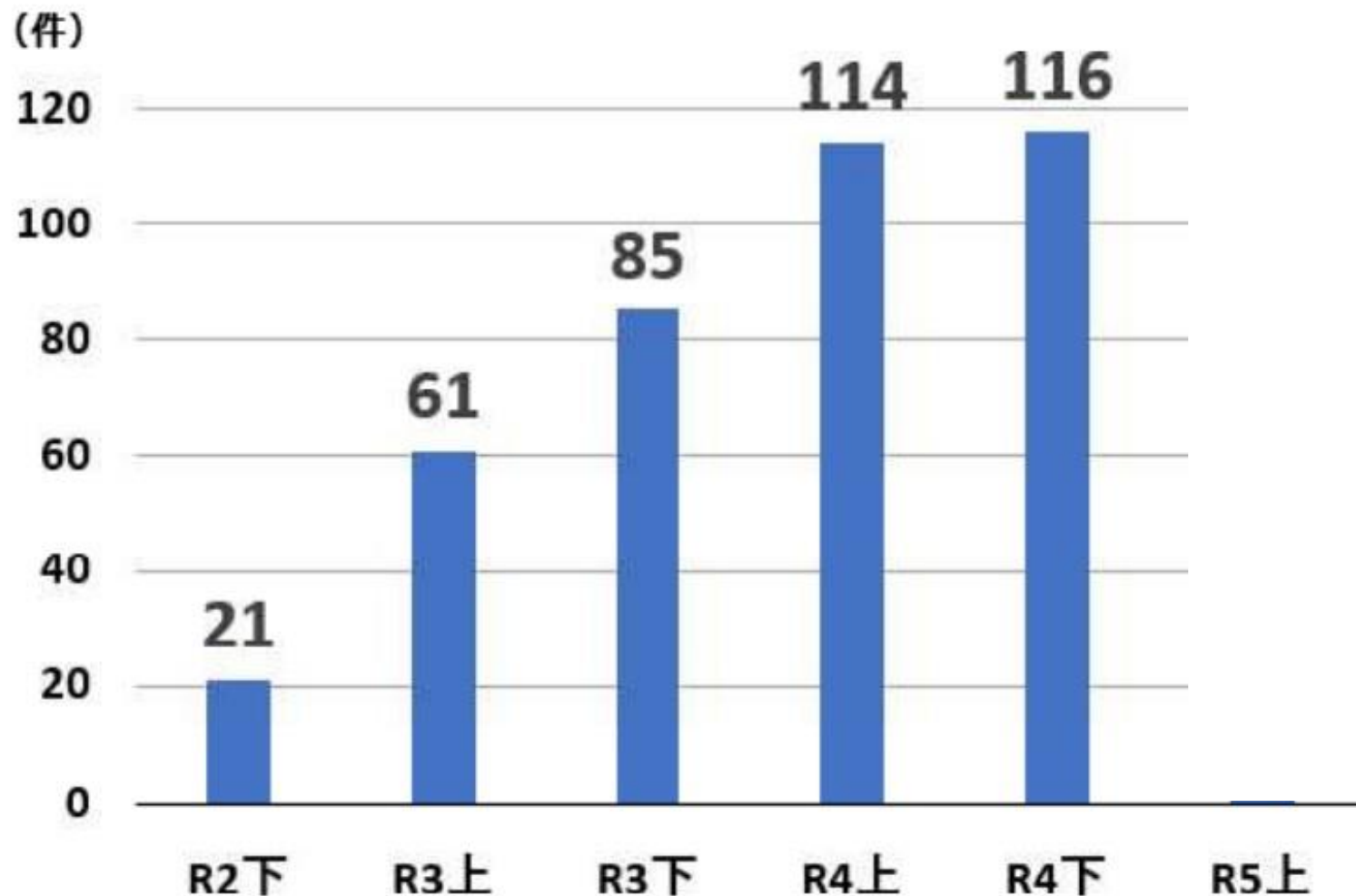


前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐欺	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭被害	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不正請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

2022年に発生した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、決定したものです。

提供：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>

ランサムウェアの認知状況（全国）

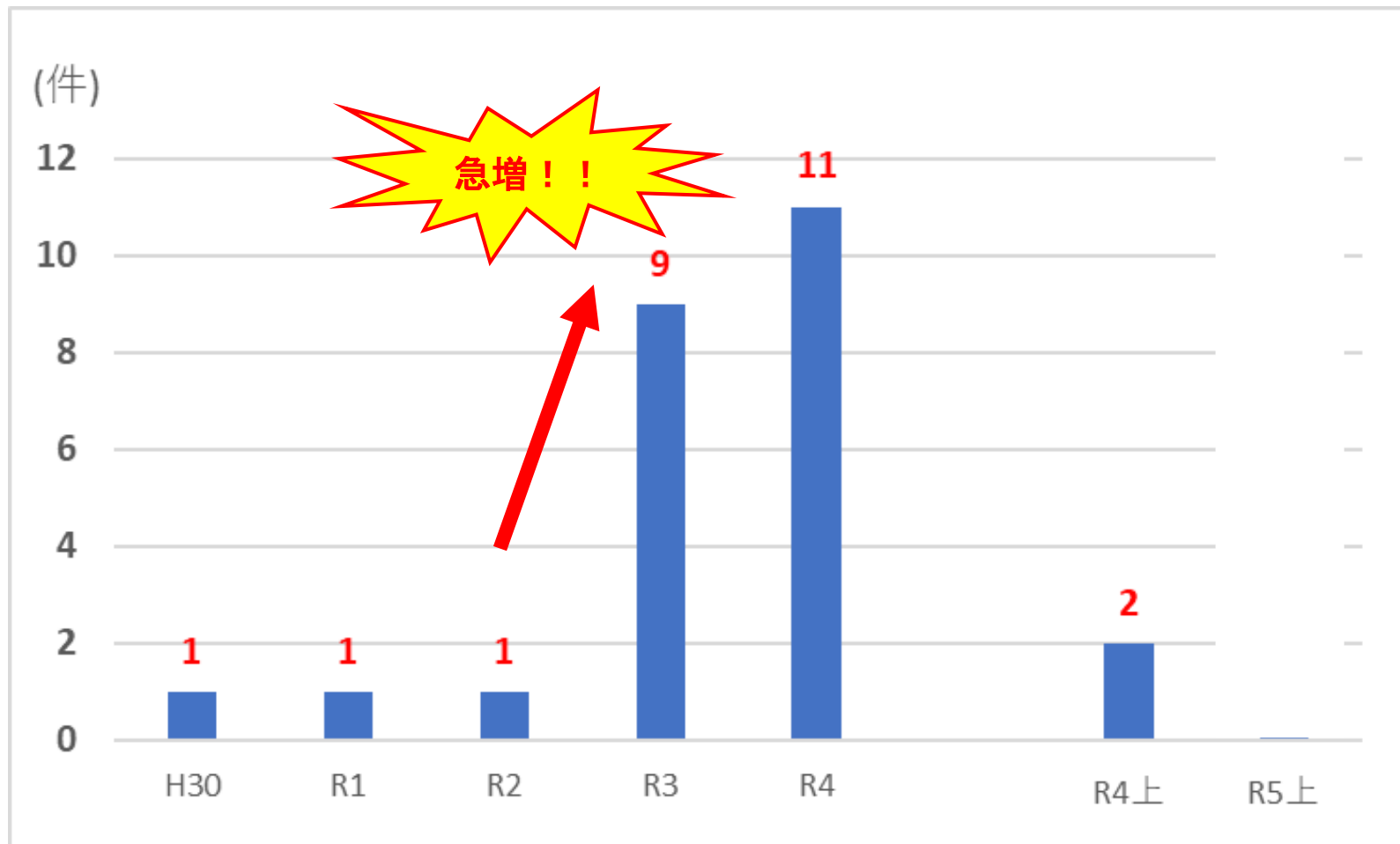


（警察庁広報資料：令和5年上半期中におけるサイバー空間をめぐる脅威の情勢等について）

【令和5年上半期の被害報告件数】

全国： 件(前年同期比 件)

ランサムウェアの認知状況（兵庫県）



令和3年から急増！

令和5年上半期は 件発生！（前年同期比 件）

令和4年下半期は？

ランサムウェアの手口 (二重の脅迫：ダブルエクストーション)

従来のランサムウェア攻撃

不特定多数に攻撃

攻撃者



ばらまき型メール

悪意あるウェブページ

データの復旧と引き換えに身代金を要求

ワーム機能

新たなランサムウェア攻撃

企業・組織を標的に攻撃

攻撃者



企業・組織のネットワークへ
ひそかに侵入

企業・組織の
ネットワーク

ネットワーク内で
侵害範囲拡大

ドメインコントローラ
等の管理サーバ

データの窃取、暗号化

ネットワーク内の端末や
サーバを一斉に攻撃

データ・システムの復旧と引き
換えに身代金を要求

＋
窃取したデータを公開しないこ
とと引き換えに身代金を要求

新たに確認されたサイバー攻撃の手口 ノーウェアランサム(Noware Ransom)

データを暗号化する(ランサムウェアを用いる)ことなくデータを
窃取し対価を要求する手口

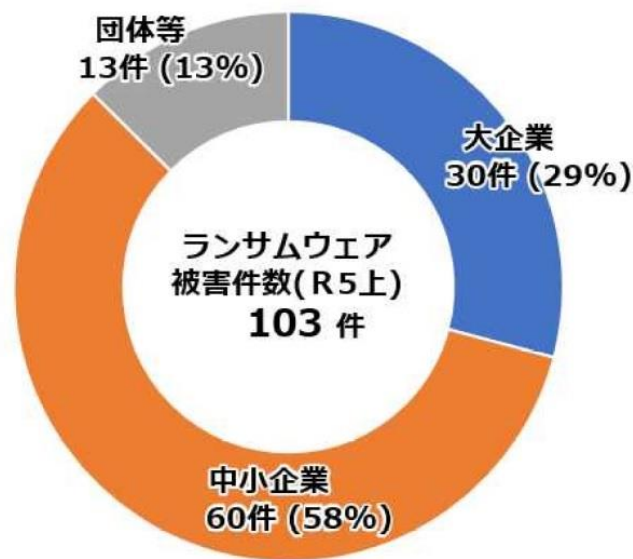


(警察庁広報資料: 令和5年上半期中におけるサイバー空間をめぐる脅威の情勢等について)

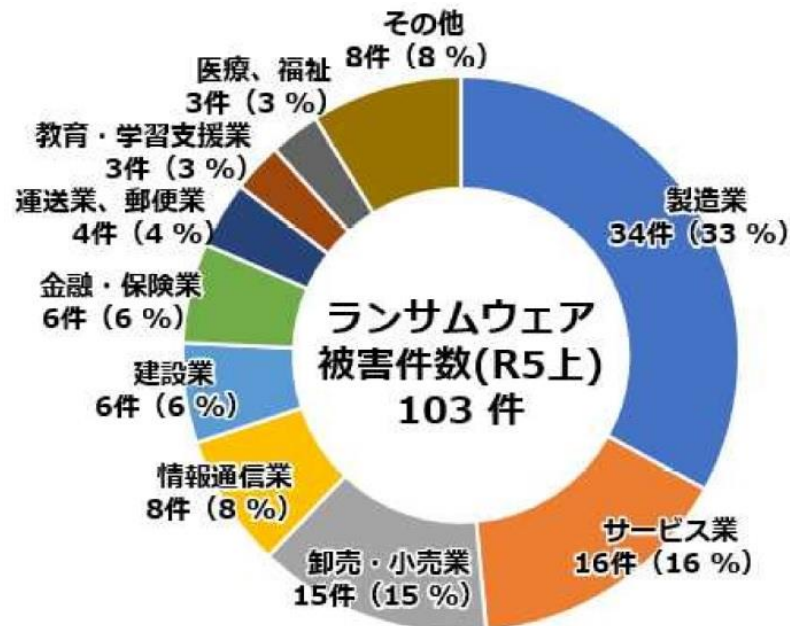
令和5年上半期に全国で 件発生！

ランサムウェアの情勢（被害企業・団体等）

【ランサムウェア被害企業・団体等の規模別報告件数】



【ランサムウェア被害企業・団体等の業種別報告件数】

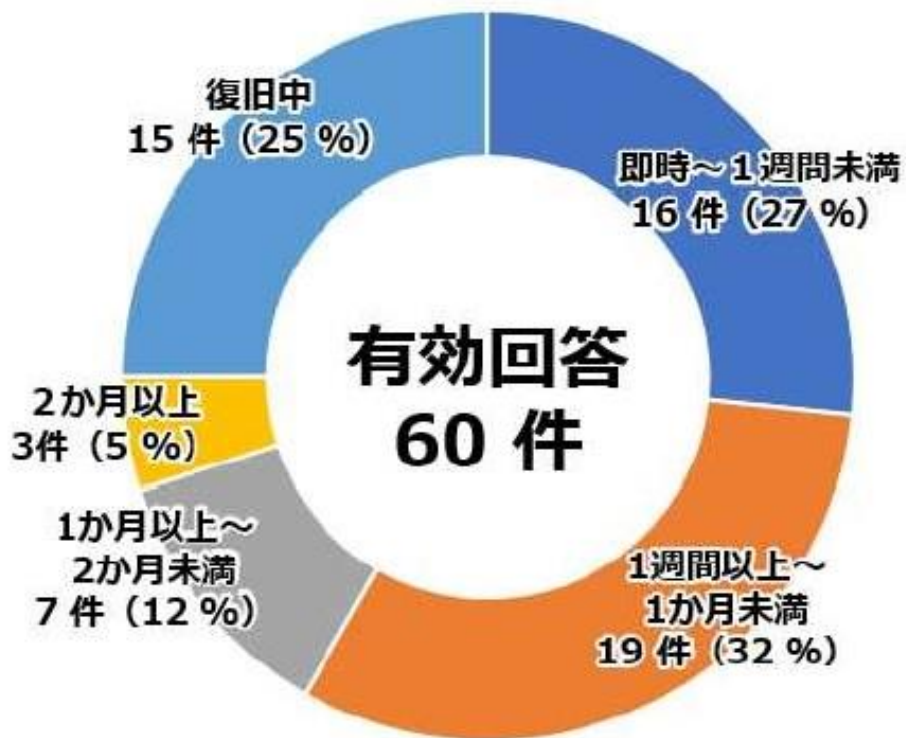


（警察庁広報資料：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について）

ランサムウェアの情勢（被害実態）

警察庁広報資料：令和5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

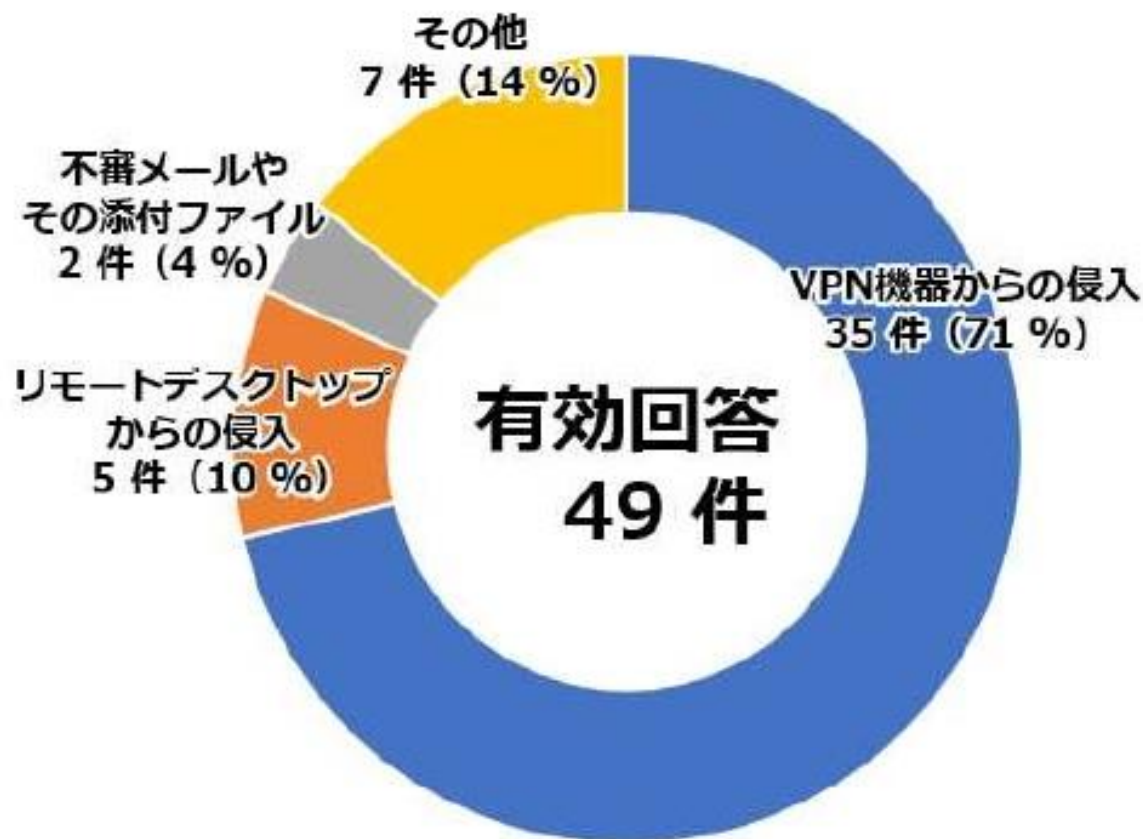
【復旧に要した期間】



【調査・復旧費用の総額】



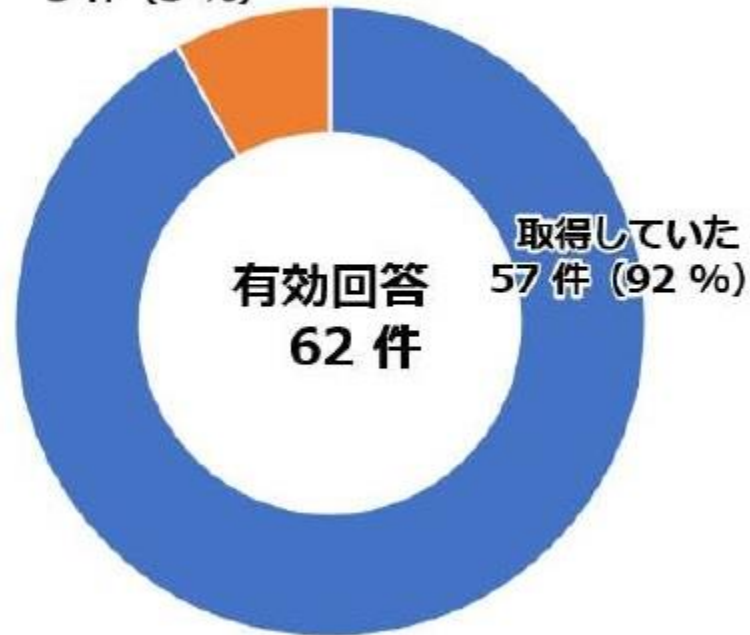
ランサムウェアの情勢（感染経路）



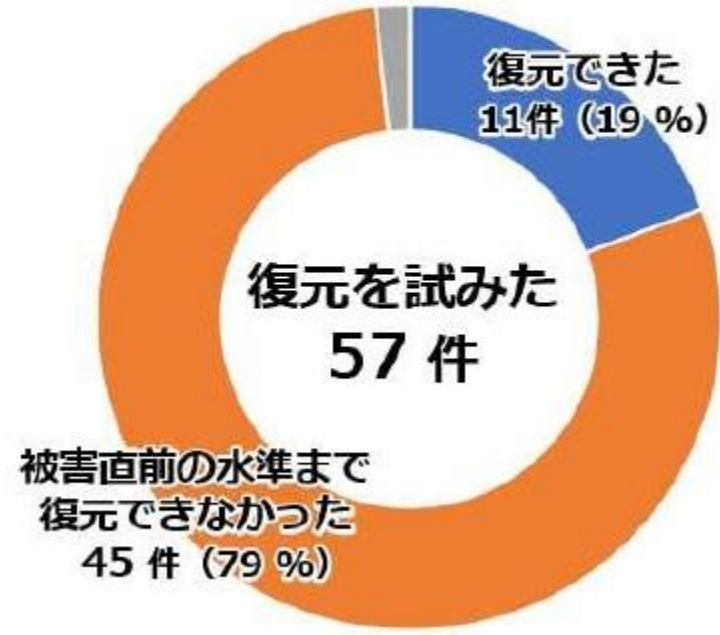
警察庁広報資料：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について

ランサムウェアの情勢（バックアップの取得）

取得していなかった
5件（8%）

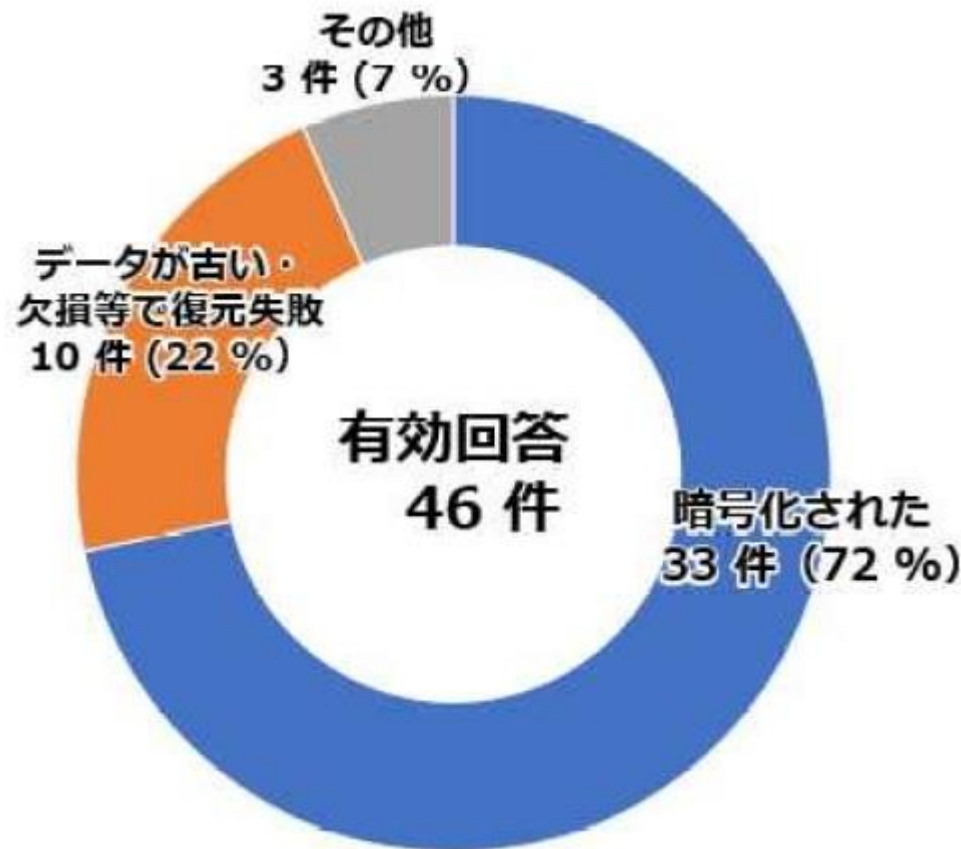


不明
1件（2%）



警察庁広報資料：令和5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

なぜバックアップが使えない???



ネットワーク内にバックアップをとっている

バックアップデータのチェックをしていない

復元のテストをしていない

ランサムウェア対策

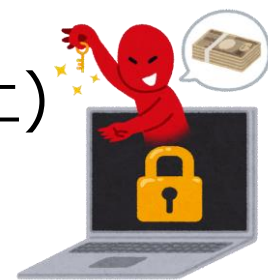
○ 予防措置

- ・ ウイルス対策ソフトの導入、定義ファイルの更新
- ・ 認証情報(ID・パスワード)の見直し及び適切な管理
- ・ 機器の脆弱性対策を迅速に(パッチ適用を迅速に行う)
- ・ OS及びソフトを最新の状態にする
- ・ メールに注意 (添付ファイル、リンク)
- ・ 重要なファイルは定期的にバックアップ
(バックアップはネットワークから切り離す)
- ・ 多要素認証の設定を有効にする
- ・ 共有サーバ等へのアクセス権の最小化

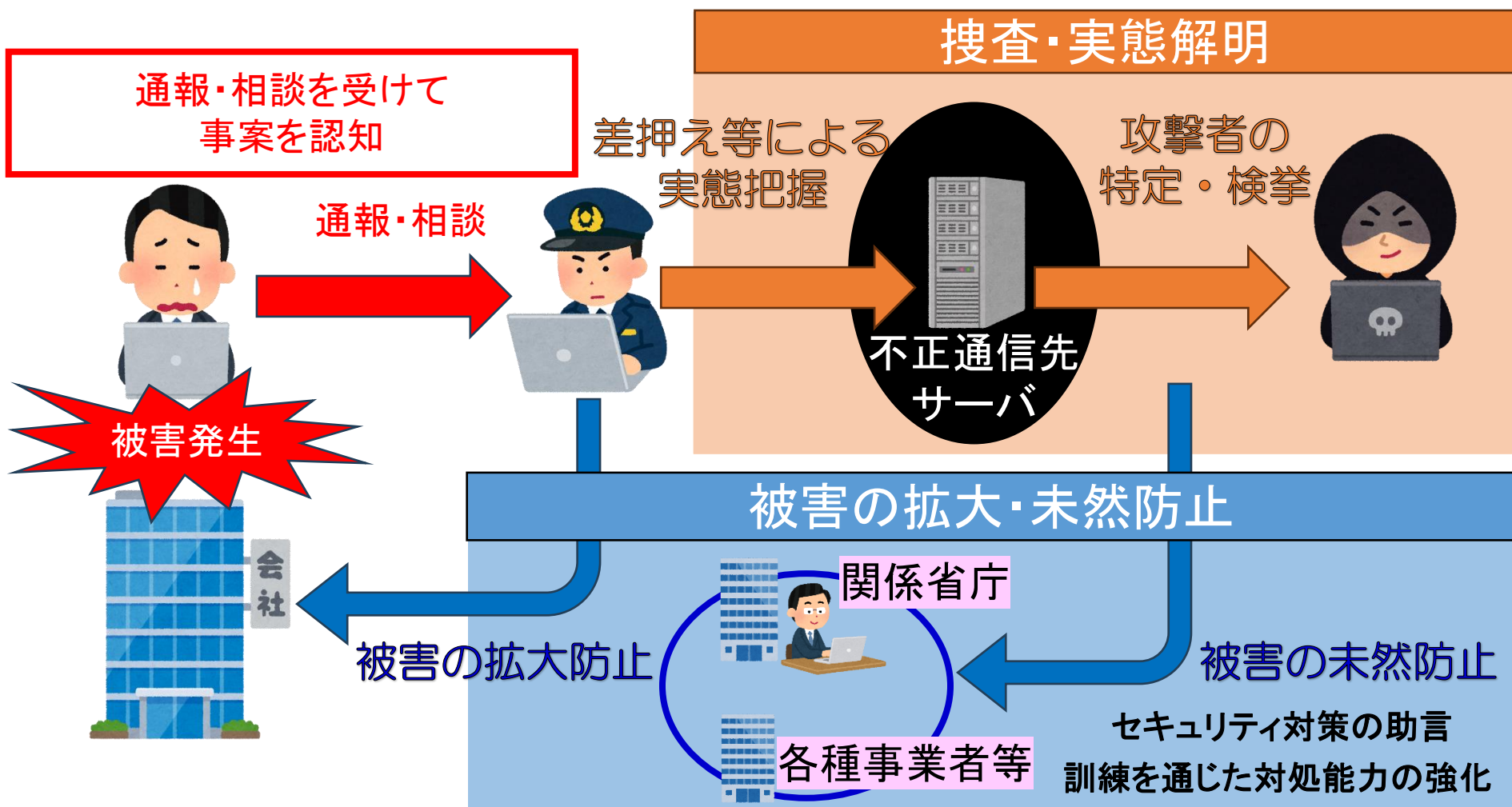


○ もし感染したら…

- ・ ネットワークから端末を切り離す(感染拡大防止)
- ・ 端末の電源は切らない(メモリの情報を保全)
- ・ 復号ツールの利用 (システム会社、セキュリティベンダーと相談)
- ・ 警察への通報・相談



サイバー事案発生時における通報・相談の重要性



サイバー事案の捜査・実態解明、被害防止対策には、被害企業等から警察への通報・相談が必要不可欠

サイバー事案発生時における通報・相談

被害者・被害企業等におけるメリット

- 個別の企業等における被害拡大防止
- 被害回復への貢献
- 顧客等に対する社会的責任の説明
- 犯罪の被害者であることの疎明 等

警察における被害の潜在化防止対策

- ウェブからの通報窓口の一元化、報告様式の統一化
- 関係機関等と連携した広報・啓発
- 警察における対応改善に向けた取組 等



不審なメールへの対策

- システムやセキュリティソフトでの対策が回避されてしまう場合もあるため、**一人ひとり**が注意する。**(パスワード付きZIPファイルに注意!)**
- 身に覚えのないメールの**添付ファイル**を開かない。
- メール本文中の**URLリンク**を安易に開かない。
- 不審なメールが届いた場合は、**システム管理部門へ連絡**、情報共有し、組織的に対応。
- **Wordマクロの自動実行を無効化**にし、Word文書ファイルやExcelファイルが信頼できるものと判断できない限り、**「コンテンツの有効化」**ボタンや**「マクロを有効にする」**ボタンをクリックしない。
- OSに定期的に**修正プログラム**を適用
- メール監査**ログ**の有効化
- メールセキュリティ製品導入によるマルウェア付きメールの**検知**
- 定期的な**バックアップ**

資料紹介

- サイバーセキュリティ経営ガイドライン
- 中小企業の情報セキュリティガイドライン
- サイバーセキュリティお助け隊
- ランサムウェアに関するウェブサイト
- インシデント損害額調査レポート



「サイバーセキュリティ経営ガイドライン」Ver3.0 (経済産業省・IPA)

なぜ改訂？？？

(2017年(平成29年)のVer2.0以来)



企業のサイバーセキュリティ対策を取り巻く環境の変化

働き方の
多様化

リスクの
顕在化

対象の
変化・拡大

影響が
拡大

サプライチェーン
全体の対策

ESG投資
の拡大

経営リスク

サイバーセキュリティ対策はコストがかかる・・・

将来の事業活動・成長のため、**企業活動のコストや損失を減らすため**

投資

企業として果たすべき
「社会的責任」

経営者としての
「責務」

IPA「中小企業の情報セキュリティ対策ガイドライン」

2019年3月以降4年ぶりの改訂

新付録



全72ページ



全8ページ

ステップ1
検知・初動対応

ステップ2
報告・公表

ステップ3
復旧・再発防止

○ウイルス感染場合
○情報漏えいの場合
○システム停止の場合

○ 経営者編、実践編の2部構成

第1部：経営者が認識し、自らの責任で考えなければならない事項等について

第2部：責任者・担当者を対象に実務的な進め方等について



こんな時には・・・

なにから始めたらいいのか。。。 セキュリティ始めたいけどお金がかかるし。。。

サイバーセキュリティお助け隊(IPA)

「見守り」・「駆けつけ」・「保険」をワンパッケージで安価に提供



中小企業のみなさん サイバーセキュリティしていますか？

最近よく、サイバーセキュリティ、サイバー攻撃という言葉を聞くけど、インターネットを使っても中小企業には関係ない、他人事だと思いませんか？
中小企業は人材や予算の制約からセキュリティ対策が手薄なことも多く、サプライチェーンを構成する中小企業がサイバー攻撃の足掛かりになることで、被害が取引先へ波及する例も。

中小企業はサイバー攻撃の脅威に晒されている！

FACT 1	FACT 2	FACT 3
中小企業約 1,100 社に対し、社内アクセスへの侵入等を試みる不審なアクセス検知数	ランサムウェアやトロイの木馬などのウイルスを検知し、無害化した件数	対応を怠った場合の想定被害額が 5,000 万円を超える案件も確認
181,536 件	1,345 件	

出典：令和 2 年度中小企業サイバーセキュリティ対策支援はねだり調査（「サイバーセキュリティお助け隊」成果報告書（5/20版））

- 業種や事業規模を問わずにサイバー攻撃や不審なアクセスなどの脅威に晒されている
- 中には攻撃者が狙った企業に対して集中的に攻撃を仕掛けていたといったケースも
- ウイルス対策ソフトの導入といった既存対策だけでは攻撃を防ぎきれない実態も明らかに……。



サイバーセキュリティといっても、 人材や予算が限られる中小企業でできる対策は？

裏面を CHECK→

サイバーセキュリティお助け隊サービスの活用を！

手遅れになるまえに、 手を打つ。



「見守り」「駆けつけ」「保険」など中小企業のセキュリティ対策に 不可欠なサービスをワンパッケージで安価に提供

「サイバーセキュリティお助け隊サービス」制度とは、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ワンパッケージのサービスを要件としてまとめ、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 が登録・公表する制度です。

見守り (異常の監視) 24 時間 365 日監視 挙動や危険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。	駆けつけ 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 最もサイバー保険で、 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。
--	--	---

ワンパッケージで安価に！



サイバーセキュリティ 対策かるた

日常の業務に潜む
リスクをかるたで紹介
対策のポイントにも
役立ちます
詳細はこちら→



サイバーセキュリティ お助け隊 THE MOVIE

サイバーセキュリティお助け隊について
ラップ調の MOVIE でご紹介
詳細はこちら→

サイバーセキュリティお助け隊サービス WEB サイトはこちら

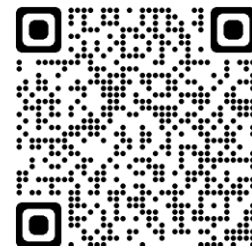
各サービスの詳細な情報や中小企業向けの情報セキュリティ関連情報へのリンクなどを掲載
大事な事が一目でわかります





独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
E-mail : isec-otasuketai@ipa.go.jp
URL : <https://www.ipa.go.jp/security/>



ランサムウェアに関するウェブサイト

○ 内閣サイバーセキュリティセンター (NISC)

【ランサムウェア特設ページ「ストップ！ランサムウェア」】

<https://www.nisc.go.jp/tokusetsu/stopransomeware.html>

※ランサムウェアに関するポータルサイト



○ 一般財団法人日本サイバー犯罪対策センター (JC3)

【ランサムウェア対策について】

<https://www.jc3.or.jp/threats/topics/article-375.html>

※ランサムウェアをめぐる状況や復号ツール、ランサムウェアの種類を特定する方法等を掲載



○ 独立行政法人情報処理推進機構 (IPA)

【ランサムウェア対策特設ページ】

https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

※ランサムウェアの感染防止や被害低減のための情報を掲載



○ JPCERTコーディネーションセンター (JPCERT/CC)

【ランサムウェア対策特設サイト】

<https://www.jpccert.or.jp/magazine/security/nomore-ransom.html>

※ランサムウェアの対策・対処法や「No More Ransom」プロジェクトを紹介

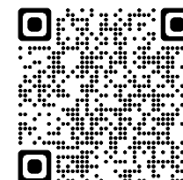


○ 警察庁サイバー警察局

【ランサムウェア被害防止対策】

<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>

※ランサムウェアの被害防止対策、感染に備えた被害軽減対策等を掲載



是非見ていただきたい資料【必見！！】

インシデント損害額調査レポート 2021年版 特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)



インシデント発生時の対応の流れや、インシデント発生時の対応及びコスト、モデルケースが記載

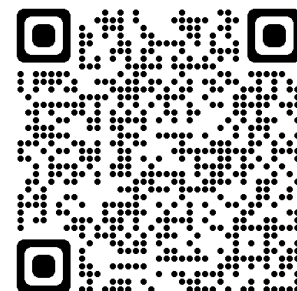


「インシデント損害額調査レポート」 2021年版 掲載場所

<https://www.jnsa.org/result/incidentdamage/2021.html>

ダウンロード先 ≪3.2MB≫

https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20210910.pdf



サイバー攻撃被害組織のアンケート調査(速報版)

令和5年10月24日発表

特定非営利活動法人日本ネットワークセキュリティ協会 (JNSA)

インシデント損害額調査レポート
2023年版が年内に発表

- ランサムウェア感染組織の被害金額
- エモテット感染組織の被害金額
- ウェブサイトからの情報漏えい被害組織の被害金額

インシデント損害額
調査レポート
第2版

JNSA
インシデント被害調査WG

Version 1.0

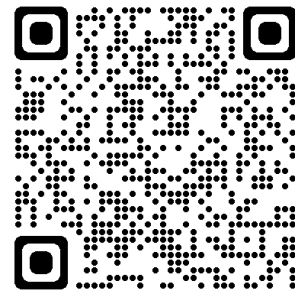
【 総 括 】
今回の調査から中小企業であっても
被害額が数千万円～
に及ぶケースを考慮すべきといえる

「サイバー攻撃被害組織のアンケート調査(速報版)」 掲載場所

<https://www.jnsa.org/result/incidentdamage/2023.html>

ダウンロード先 ≪2.4MB≫

https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20231024.pdf



取組紹介

- サイバーセキュリティセミナー
- 中小企業サイバーセキュリティ対策PR動画



サイバーセキュリティセミナー

サイバーセンターでは、平成26年から県下の商工会議所と連携して企業を対象としたサイバーセキュリティセミナーを毎年開催(10年目)。

サイバー防犯通信
<https://www.police.pref.hyogo.lg.jp/cyber/index.htm>

令和5年22号
兵庫県警察サイバーセンター
サイバー情報発信室

企業の皆様、今年もやります！10年目
～「サイバーセキュリティセミナー」の開催が決定！～

① 姫路会場

日時: 令和5年10月25日(水) 午後3時00分～午後5時00分
場所: 姫路商工会議所6階605会議室(姫路市下寺町43)
共催: 姫路商工会議所

② 龍野会場

日時: 令和5年11月6日(月) 午後2時00分～午後4時00分
場所: 龍野経済交流センター2階セミナー室(たつの市龍野町富永702-1)
共催: 龍野商工会議所

③ 三木会場

日時: 令和5年11月30日(木) 午後2時00分～午後4時00分
場所: 三木商工会館4階大会議室(三木市本町2丁目1-18)
共催: 三木商工会議所

④ 加古川会場

日時: 令和5年12月4日(月) 午後3時00分～午後5時00分
場所: 加古川商工会議所1階展示ホール(加古川市加古川町溝之口800)
共催: 加古川商工会議所

⑤ 尼崎会場

日時: 令和5年12月6日(水) 午後3時00分～午後5時00分
場所: 尼崎商工会議所7階701会議室(尼崎市昭和通3-96)
共催: 尼崎商工会議所

⑥ 豊岡会場

日時: 令和5年12月7日(木) 午後3時00分～午後5時00分
場所: 豊岡商工会議所会議室(豊岡市大磯町1-79)
共催: 豊岡商工会議所

⑦ 伊丹会場

日時: 令和6年1月15日(月) 午後2時30分～午後4時30分
場所: 伊丹工プラザ4階会議・研修室A(伊丹市宮ノ前2-2-2)
共催: 伊丹商工会議所

⑧ 加西会場

日時: 令和6年1月24日(水) 午後2時00分～午後4時00分
場所: アステアがさい3階多目的ホール(加西市北条町北条28番1号)
共催: 加西商工会議所

⑨ 洲本会場

日時: 令和6年2月7日(水) 午後3時00分～午後5時00分
場所: 洲本商工会議所2階多目的ホール(洲本市本町3-3-25)
共催: 洲本商工会議所

⑩ 神戸会場

令和6年2月21日 みなと銀行セミナーホール

サイバー情報発信室ホームページ(イベント情報等)に掲載
申込み方法等の詳細はホームページに掲載しています。(各商工会議所案内チラシを掲載)
<https://www.police.pref.hyogo.lg.jp/cyber/event/index.htm> ※随時更新

サイバーセンター公式「X」(旧Twitter)
兵庫県警察サイバーセンターではX(旧Twitter)で、サイバー犯罪やサイバーセキュリティの情報をいち早くお届けしています。
https://twitter.com/HPP_c3division

- 令和5年度は、県下9会場(姫路、龍野、三木、加古川、尼崎、豊岡、伊丹、加西、洲本)において開催
- 令和6年2月21日(水)に神戸でも開催予定

※神戸会場は内容を変更する場合がございます。



神戸会場の状況(ハイブリッド形式)

中小企業サイバーセキュリティ対策PR動画

**サイバー攻撃被害 次の標的は、
ウチは関係ない
という御社です。**

対策をしていないと、企業の危機を招くことも！
中小企業を狙ったサイバー攻撃被害、急増中！

サイバーセキュリティ対策がよくわかる！
解説ムービー公開中！

サイバー攻撃による
想定被害額
5,000万円超

不審なアクセス
検知数
中小企業約1300社に対して
181,536件

ウイルスを検知し
無害化された件数
1,345件

本当に、被害にあわない
と言いきれる？ **兵庫県内の中小企業で起こったサイバー攻撃事例**

権威型攻撃(マルウェア攻撃など)被害事例
2021年12月
権威型攻撃により、
一部個人情報や企業情報が外部に流出。
加古川市に本社を構える企業の従業員やその家族、取引先などの
情報約100名が、サイバー攻撃により流出。また、攻撃の影響により
サーバー内の一部データが破壊。攻撃発生後は外部との通信を遮断し、
サーバーの復旧には2日がかかった。

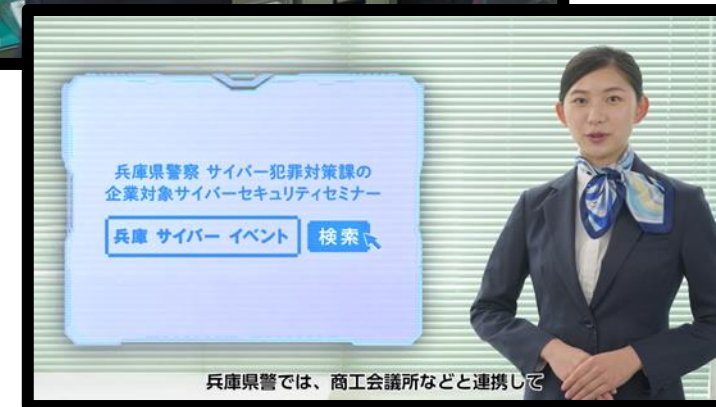
サプライチェーンを狙った攻撃被害事例
2022年8月
サプライチェーン攻撃により、
身代金要求型「ランサムウェア」に感染。
姫路市の製造会社において、米軍の予備隊が外部から不正アクセスを
実行。同社のサーバーが身代金要求型コンピュータウイルス「ランサム
ウェア」の感染を確認。その後、速やかに同予備隊のネットワークを遮断、
生産管理システムも停止し、手作業で生産・出荷に当たった。

ウチの会社に
狙われる情報は？ **サイバー犯罪者が悪用する主な情報**

- 従業員のマイナンバー・住所・給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から「取扱い注意」として預かった情報 など
- 事業の停止
- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遮断などによる業務効率のダウン
- 従業員の士気低下

もし、
サイバー攻撃の
被害に
あつたら

兵庫県 裏面にサイバーセキュリティ「5つの基本対策」を解説！ぜひ、ご確認ください。▶



兵庫県警では、商工会議所などと連携して

《中小企業サイバーセキュリティ対策啓発チラシ》

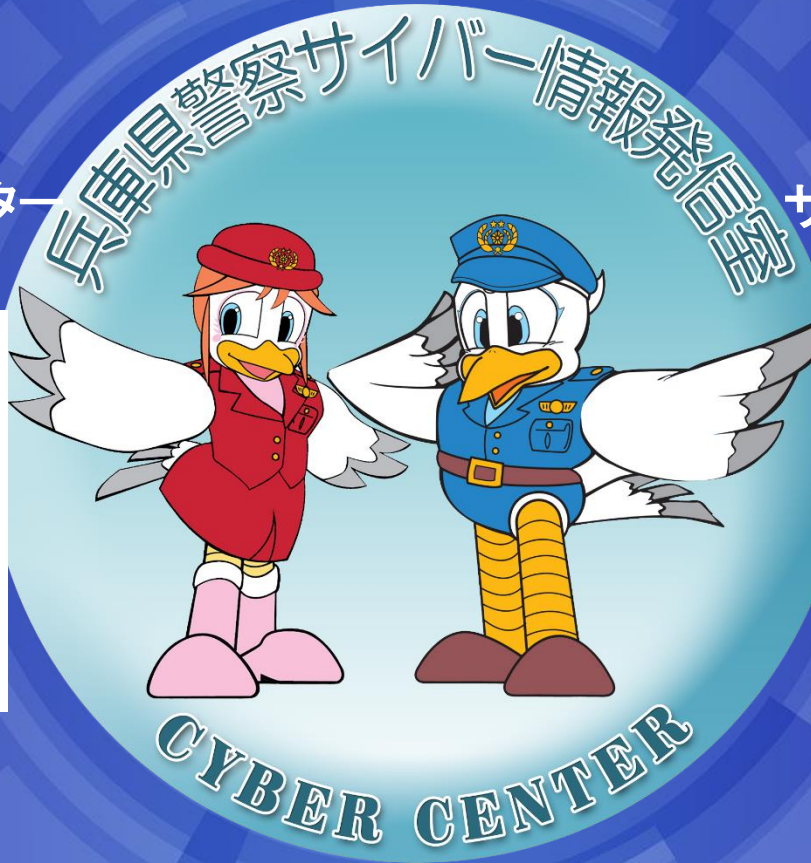
《中小企業サイバーセキュリティ対策PR動画》

<https://web.pref.hyogo.lg.jp/cybertaisaku/>

制作:兵庫県産業労働部地域経済課 協力:兵庫県警察本部・情報処理推進機構(IPA)

ご清聴ありがとうございました

兵庫県警察サイバーセンター
「X」(旧Twitter)



サイバー情報発信室
ウェブページ

