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

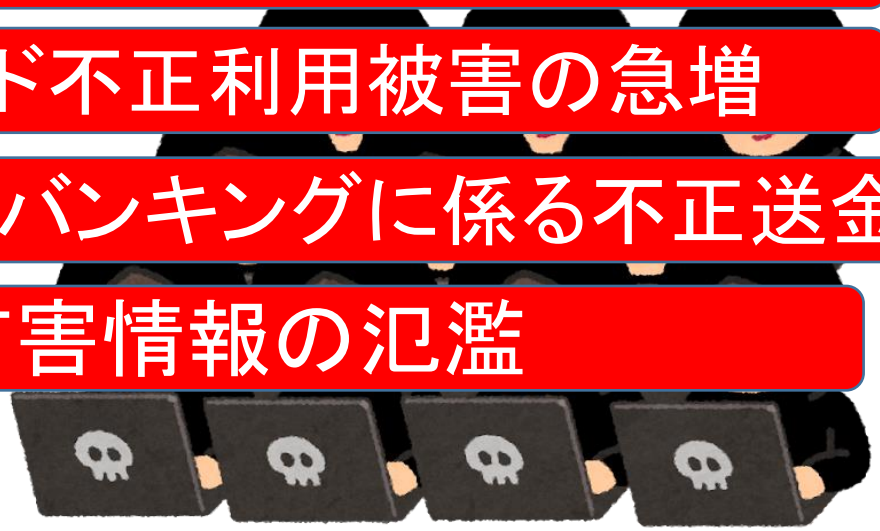
- ◇ サイバー空間の公共空間化が加速
- ◇ 厳しい安全保障環境の中、高い地政学的緊張
- ◇ 先端技術、知的財産等を有する企業等が国内に多数
- ◇ 大阪・関西万博等、関心を集める行事が開催

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

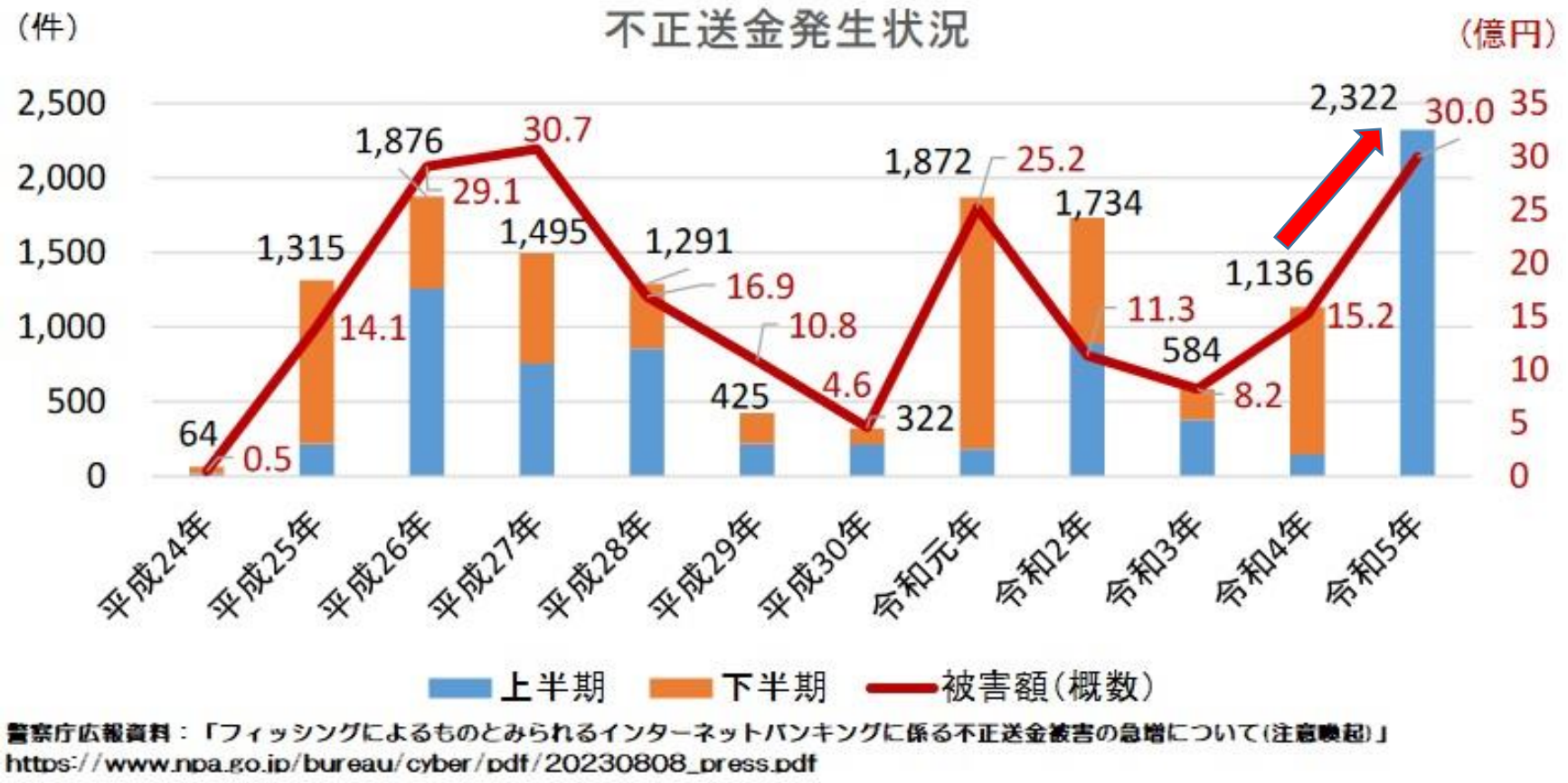
新たな詐欺手口

① 商品購入(ネット振込み)

② 商品がとどかない・・・

③ 連絡

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

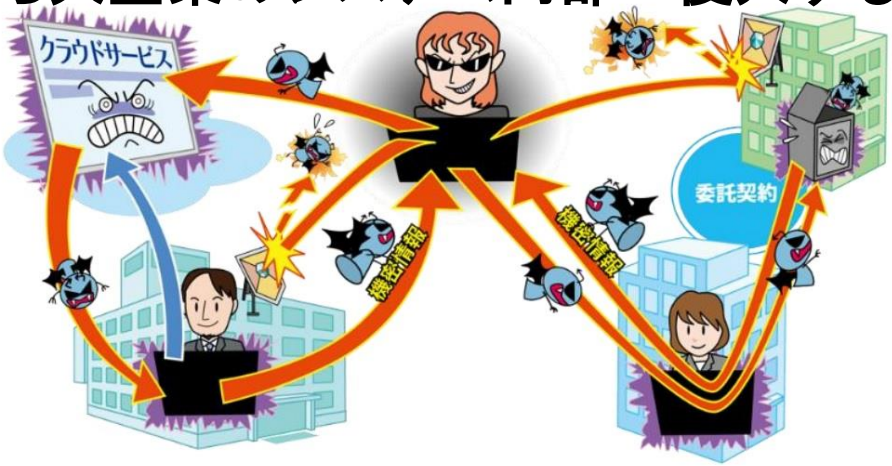
○　被害の多くはフィッシングによるものとみられる。
○　金融機関(銀行)を装ったフィッシングサイト(偽のログインサイト)へ誘導するメールを多数確認
○　上半期だけで、過去最多2,322件、約30億円の被害

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



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

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！？

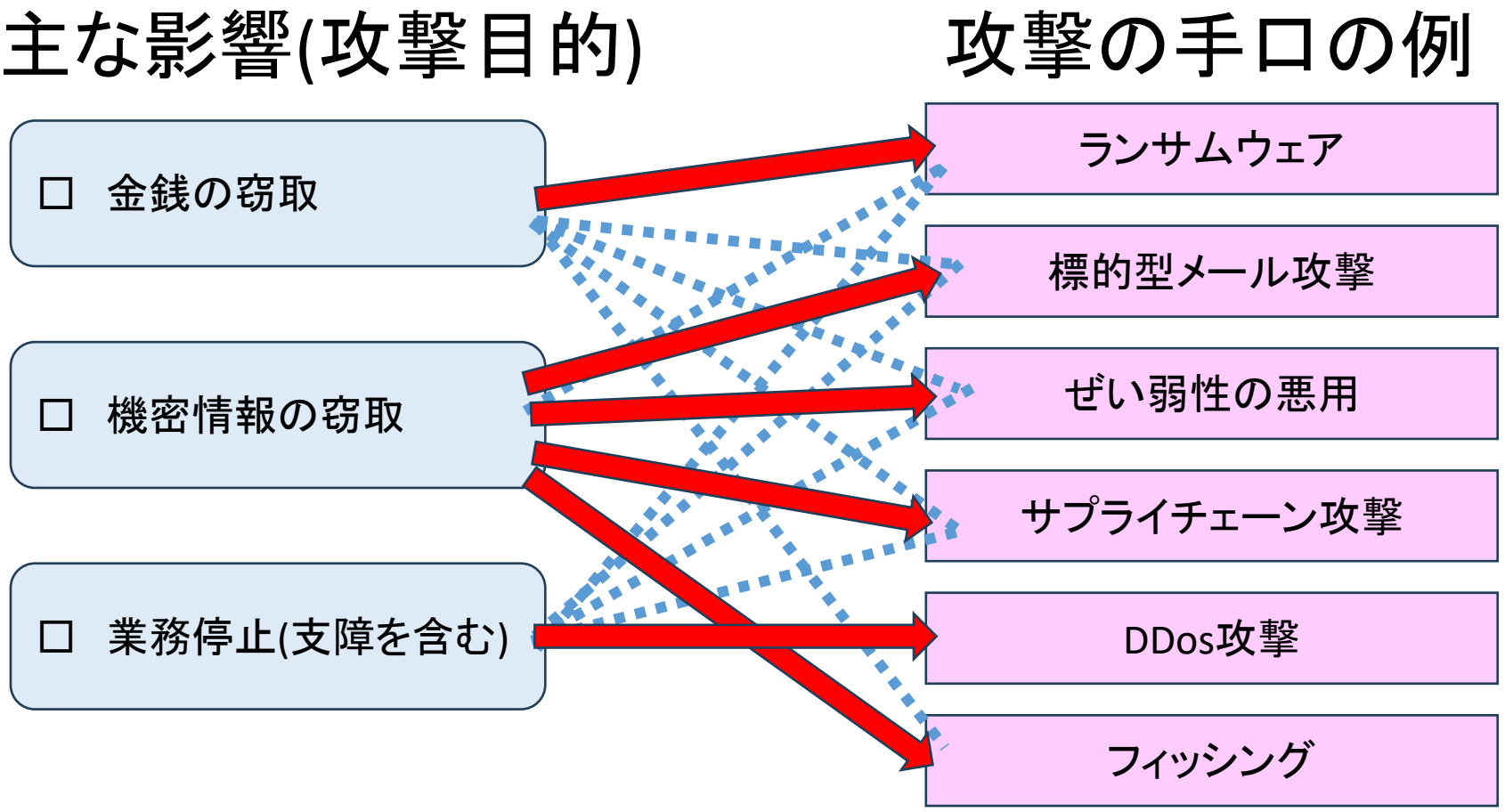
ランサムウェアのように、被害が表面化する前からシステムに侵入されているかも

○　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



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～

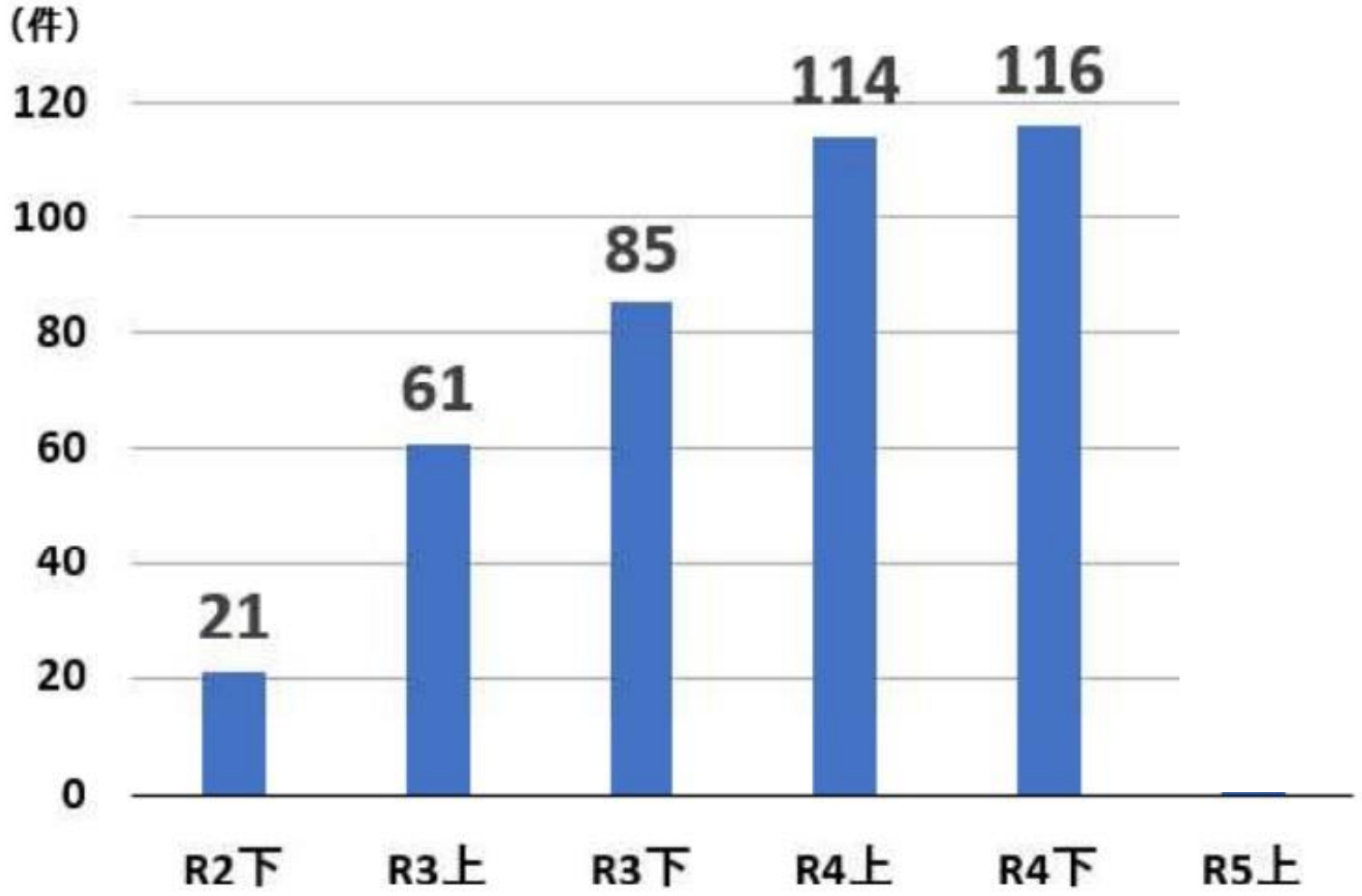
IPA情報セキュリティ１０大脅威

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）

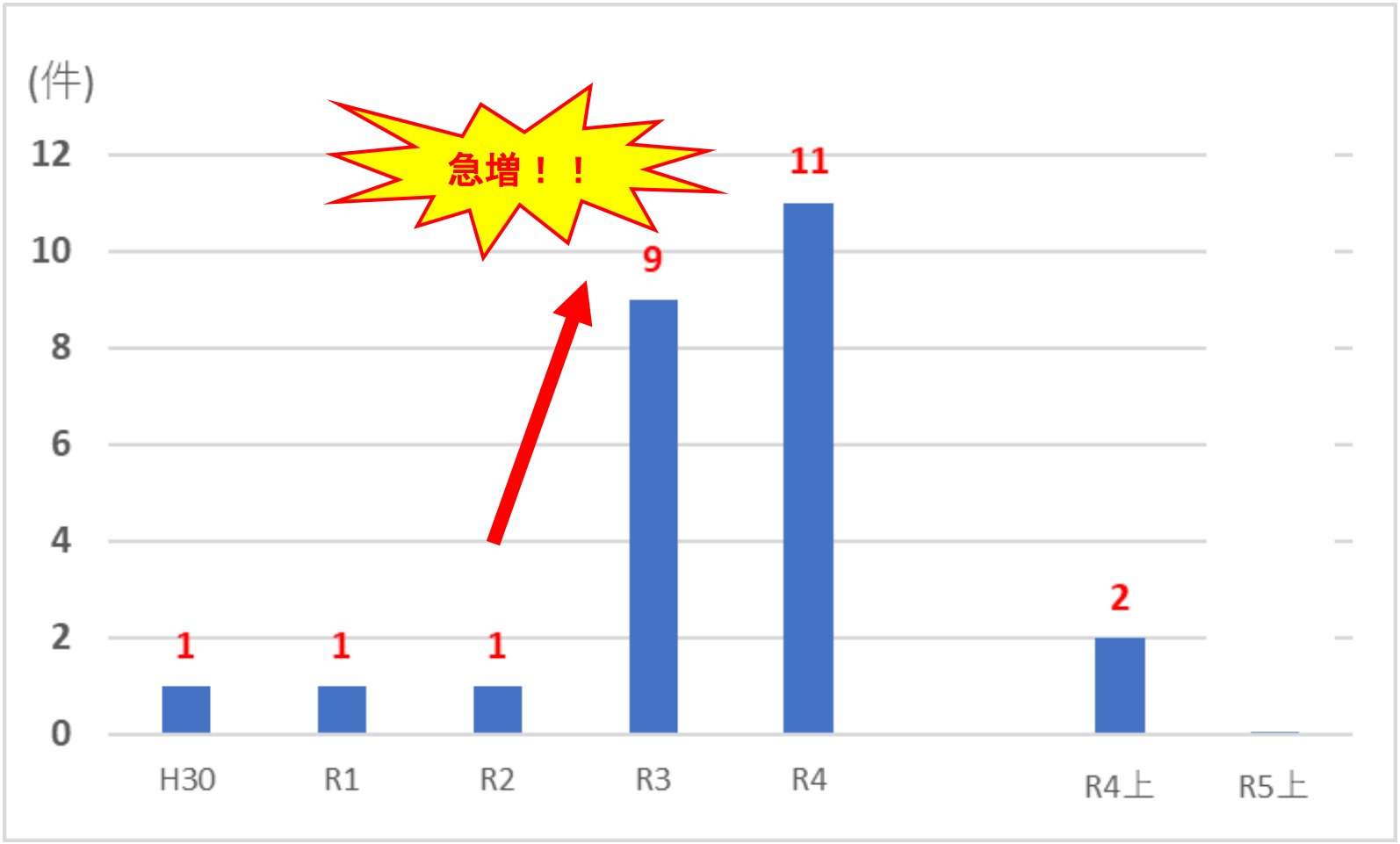


（警察庁広報資料：令和5年上半期中におけるサイバー空間をめぐる脅威の情勢等について）

【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）

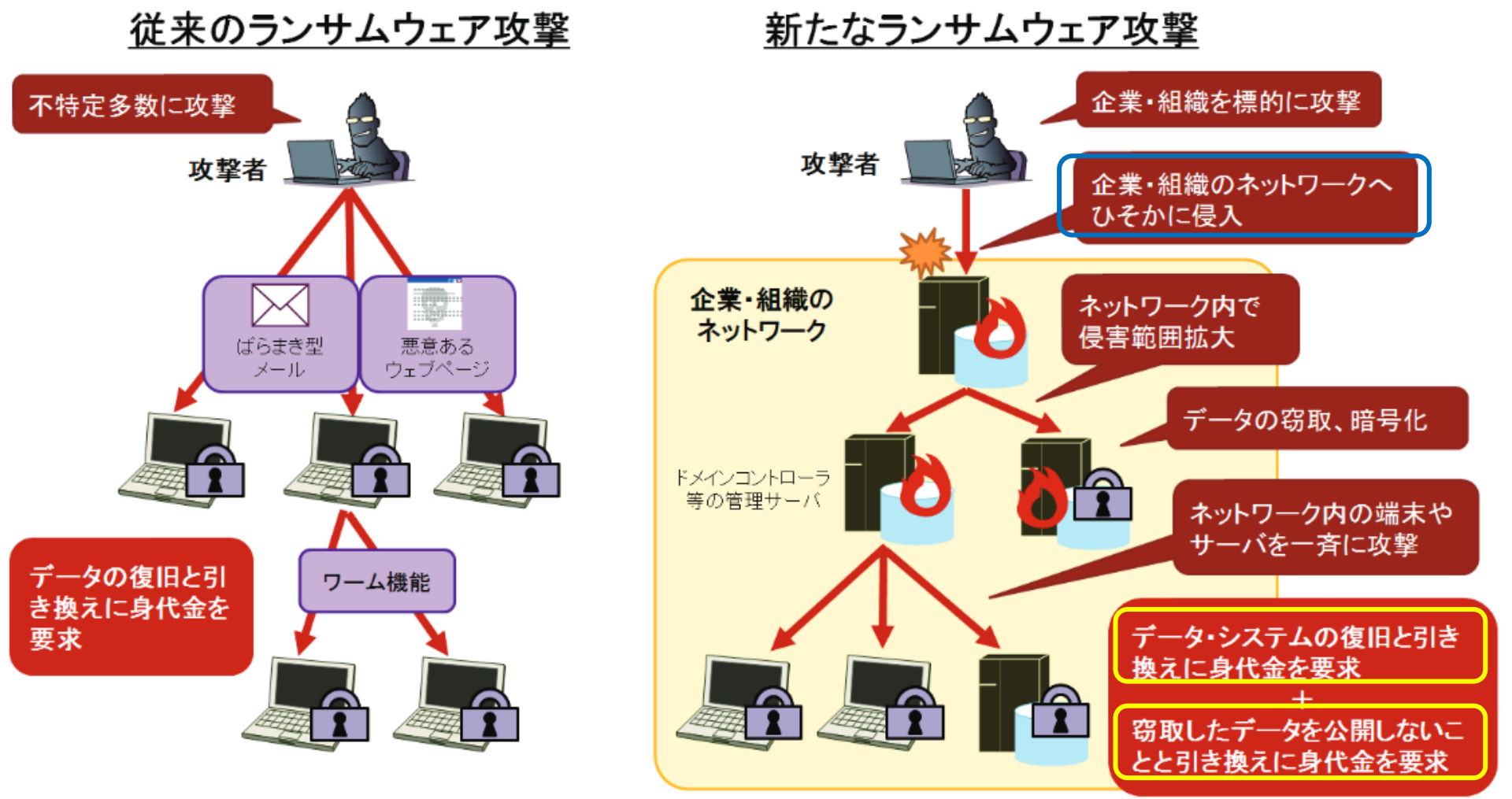


令和３年から急増！

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？

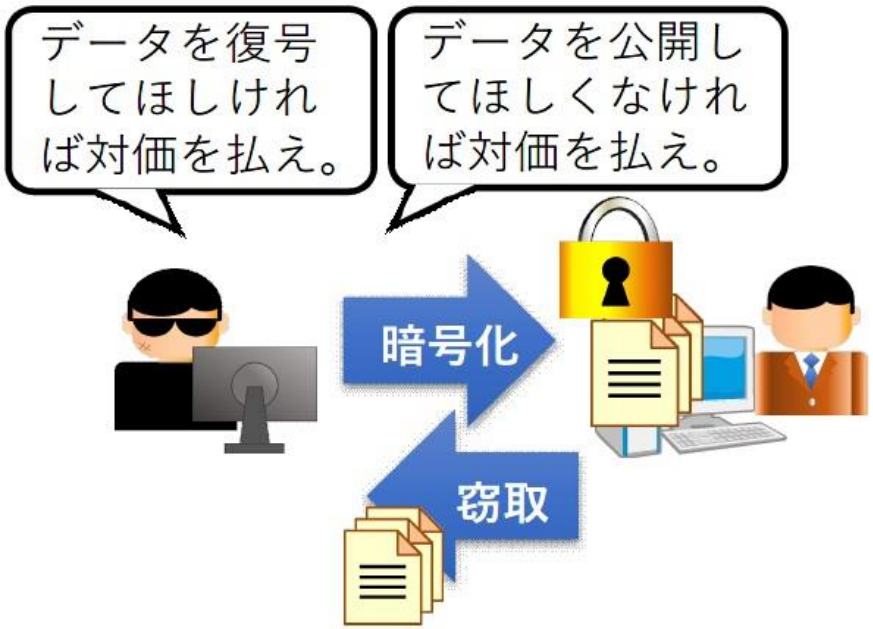
ランサムウェアの手口
（二重の脅迫：ダブルエクストーション）



出典：独立行政法人情報処理推進機構（IPA）「事業継続を脅かす新たなランサムウエア攻撃について」
https://www.ipa.go.jp/archive/security/security-alert/2020/ransom.html

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



【ランサムウェア攻撃】
(ダブルエクストーション)

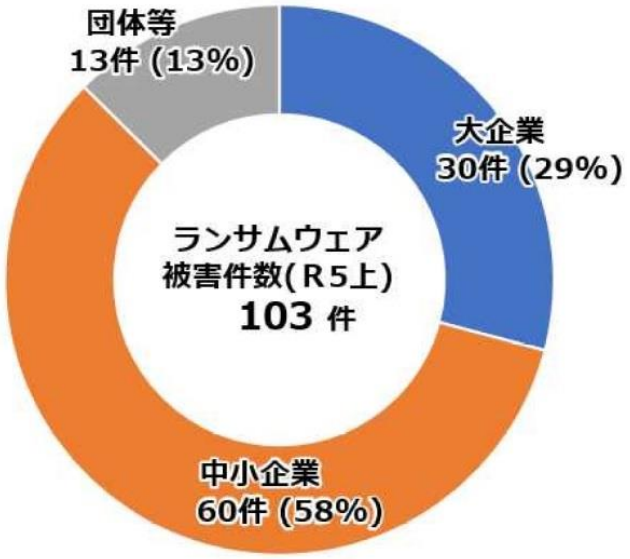
【ノーウェアランサム攻撃】

(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)

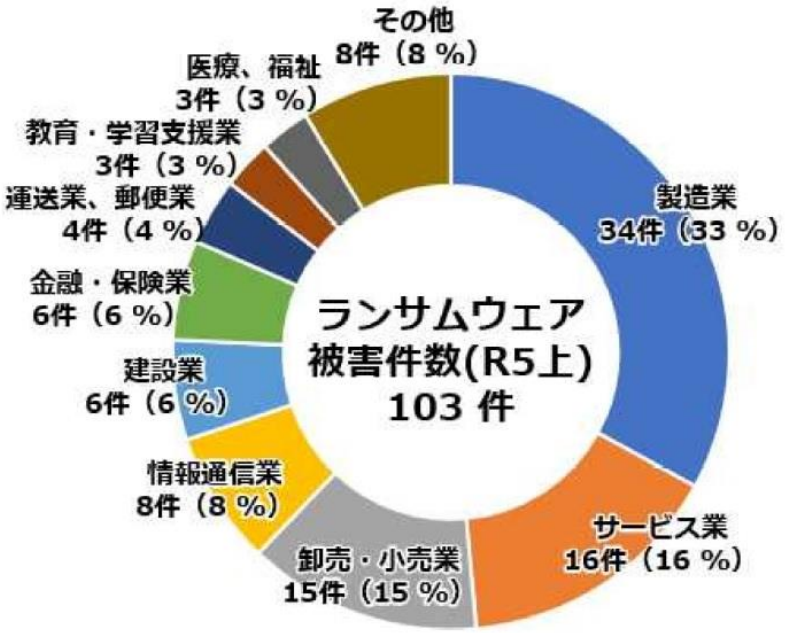
令和5年上半期に全国で　　件発生！

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】

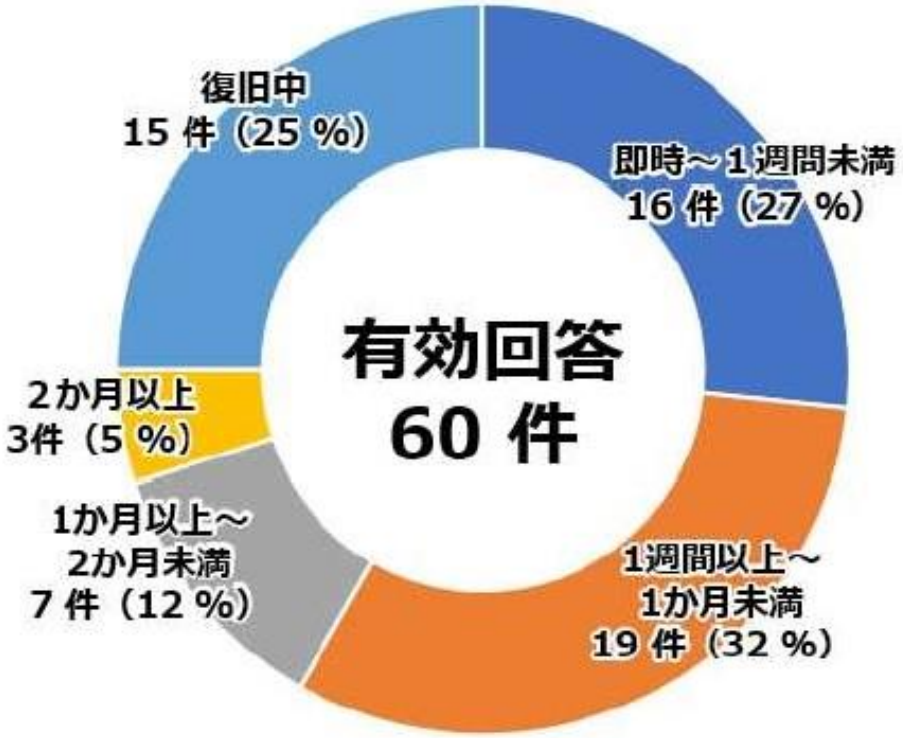


（警察庁広報資料：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について）

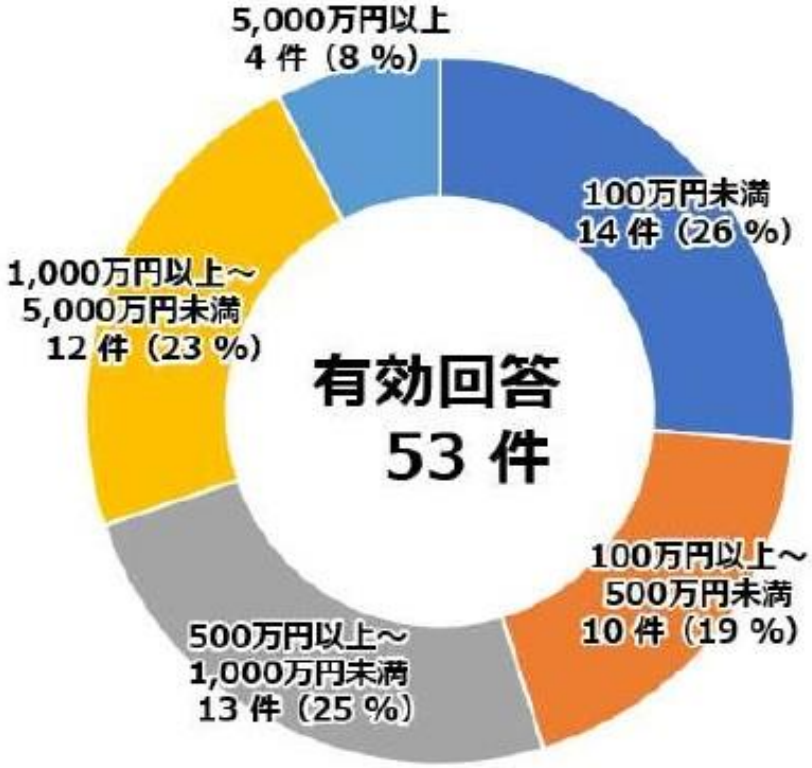
ランサムウェアの情勢（被害実態）

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

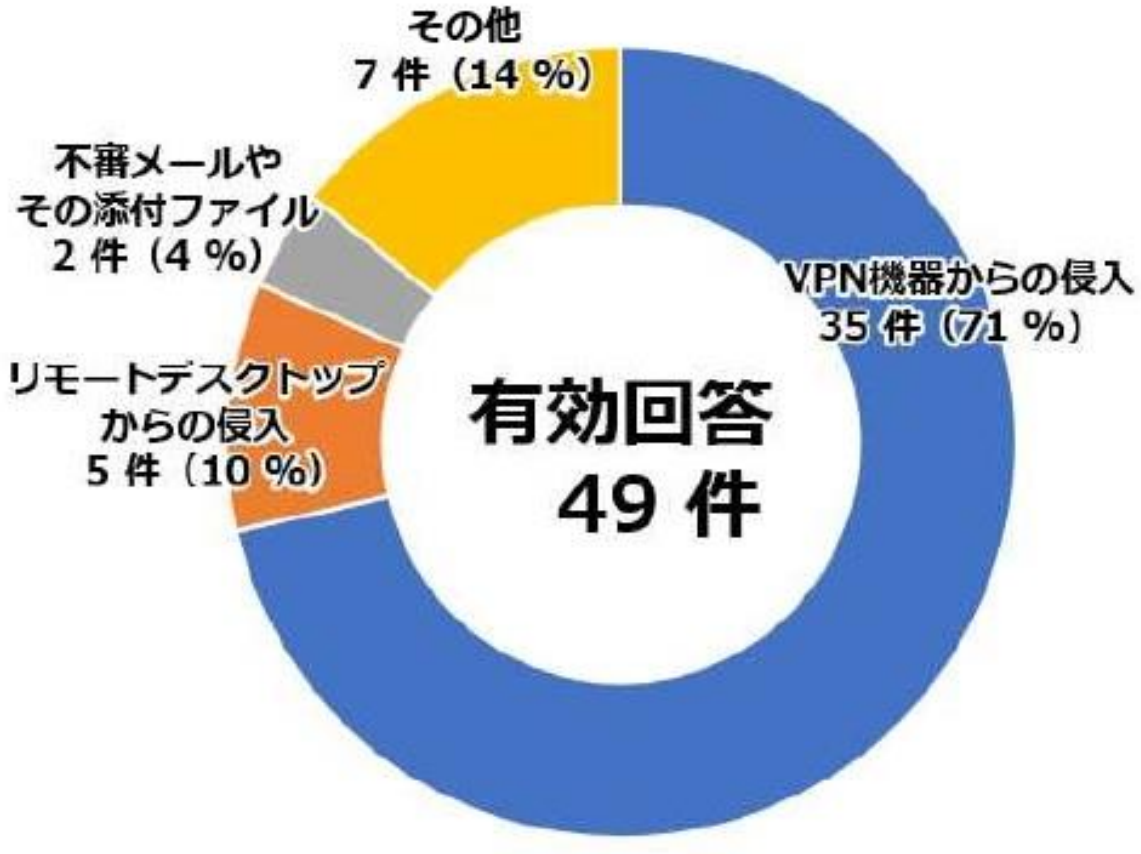
【復旧に要した期間】



【調査・復旧費用の総額】

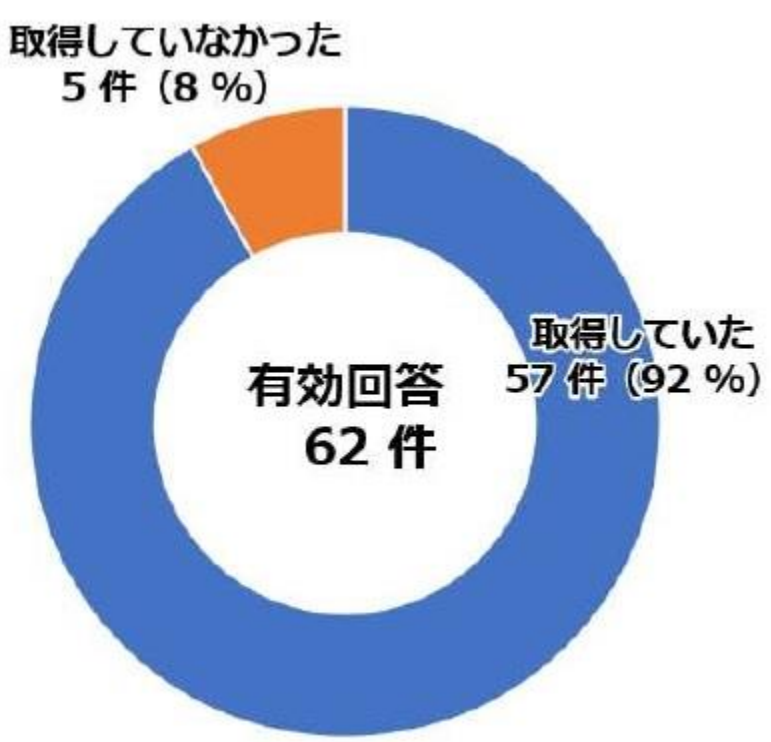


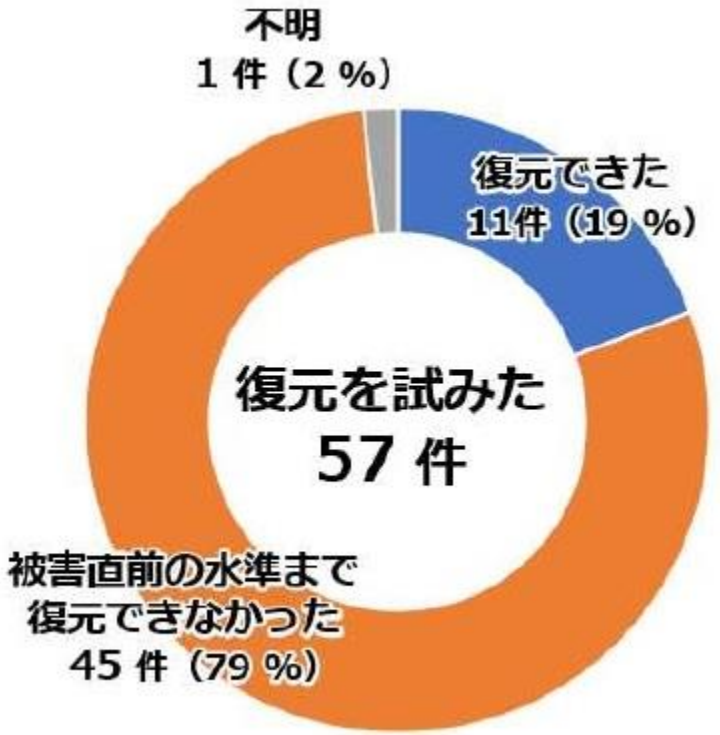
ランサムウェアの情勢（感染経路）



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

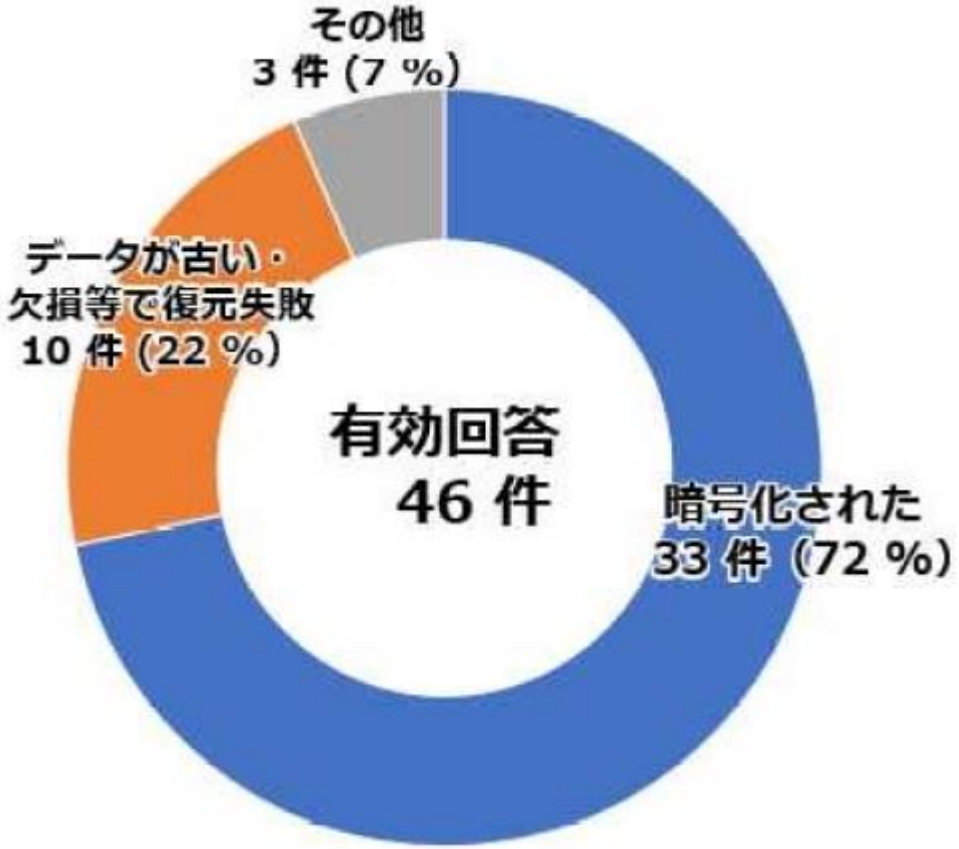
ランサムウェアの情勢（バックアップの取得）





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

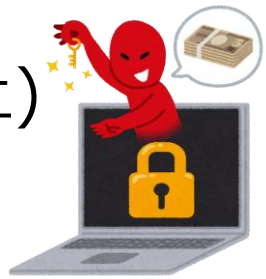
ランサムウェア対策

○　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

通報・相談を受けて
事案を認知

通報・相談

被害発生

会社

捜査・実態解明

差押え等による
実態把握

不正通信先
サーバ

攻撃者の
特定・検挙

被害の拡大・未然防止

被害の拡大防止

関係省庁

各種事業者等

被害の未然防止

セキュリティ対策の助言
訓練を通じた対処能力の強化

**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
- メールの監査ログの有効化
- 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」**

経済産業省・IPA「サイバーセキュリティ経営ガイドラインVer3.0」より

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

全72ページ

新付録

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

〇ウイルス感染場合
〇情報漏えいの場合
〇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

出典：情報処理推進機構(IPA)「中小企業の情報セキュリティ対策ガイドライン」 https://www.ipa.go.jp/security/guide/sme/about.html

こんな時には・・・

なにから始めたらよいのか。。。　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

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

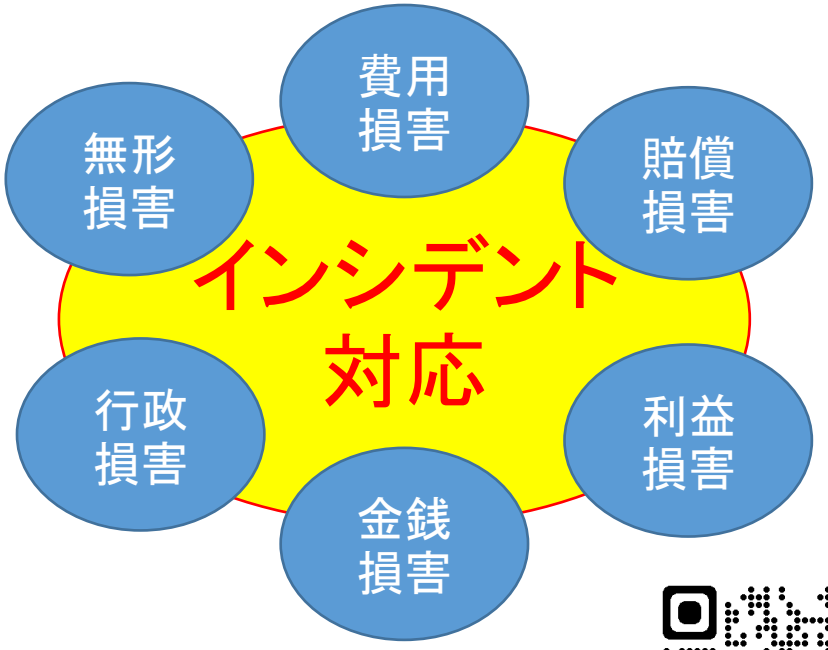
○ **JPCERTコーディネーションセンター（JPCERT／CC）**
【ランサムウェア対策特設サイト】
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html
※ランサムウェアの対策・対処法や「No More Ransom」プロジェクトを紹介

○ **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

【　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)。

○ 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

≪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