サイバーセキュリティ
セミナー‘２４ｉｎ東北

サイバー空間における脅威の情勢

令和６年１２月１１日
宮城県警察本部
サイバー犯罪対策課

サイバー空間の脅威概況
～令和6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～

脅威概況

令和6年上半期においては、サイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数及びランサムウェアの被害報告件数が前年同期から増加した。

また、フィッシングの被害報告件数も前年同期比で約10万件増加したほか、インターネット上には犯罪実行者募集情報が氾濫するなど、極めて深刻な情勢が継続している。

※出典元： 警察庁 “令和6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”

サイバー空間の脅威概況
～令和6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～

高度な技術を悪用したサイバー攻撃の脅威情勢

○　近年、世界各地で重要インフラの機能停止や機密情報の窃取を企図したとみられるサイバー攻撃が相次いで発生

○　警察庁が設置したセンサーにおいて検知した、ぜい弱性探索行為等の不審なアクセス件数は増加

○　令和6年上半期におけるランサムウェアの被害報告件数は、114 件であり、高水準で推移

流出情報は、ダークウェブ上のリークサイトに掲載

※出典元：　警察庁　“令和6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”

サイバー空間の脅威概況
～令和6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～

インターネット空間を悪用した犯罪に係る脅威情勢

○　インターネットバンキングに係る不正送金事案や、SNSを通じて金銭をだまし取るSNS型投資・ロマンス詐欺等が発生

○　令和6年上半期におけるフィッシング報告件数は、63万3,089件、インターネットバンキングに係る不正送金被害総額は約24億4,000万円

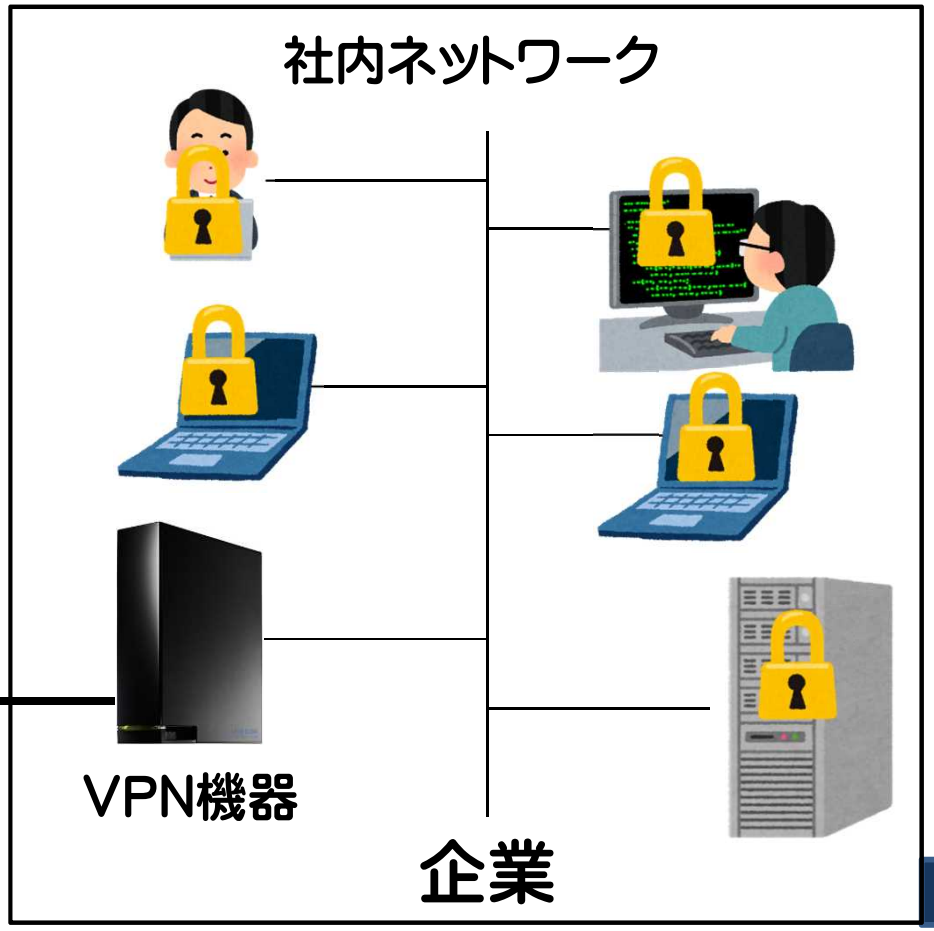
※出典元：　警察庁　“令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について”

ランサムウェアの情勢（ランサムウェアとは）

ランサムウェアとは
　感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム
のこと。

① VPN機器の脆弱性を突いて社内ネットワークに侵入
② 社内ネットワークに接続されているサーバやPCのデータを暗号化
③ データの復号化を対価に金銭を要求

犯罪者

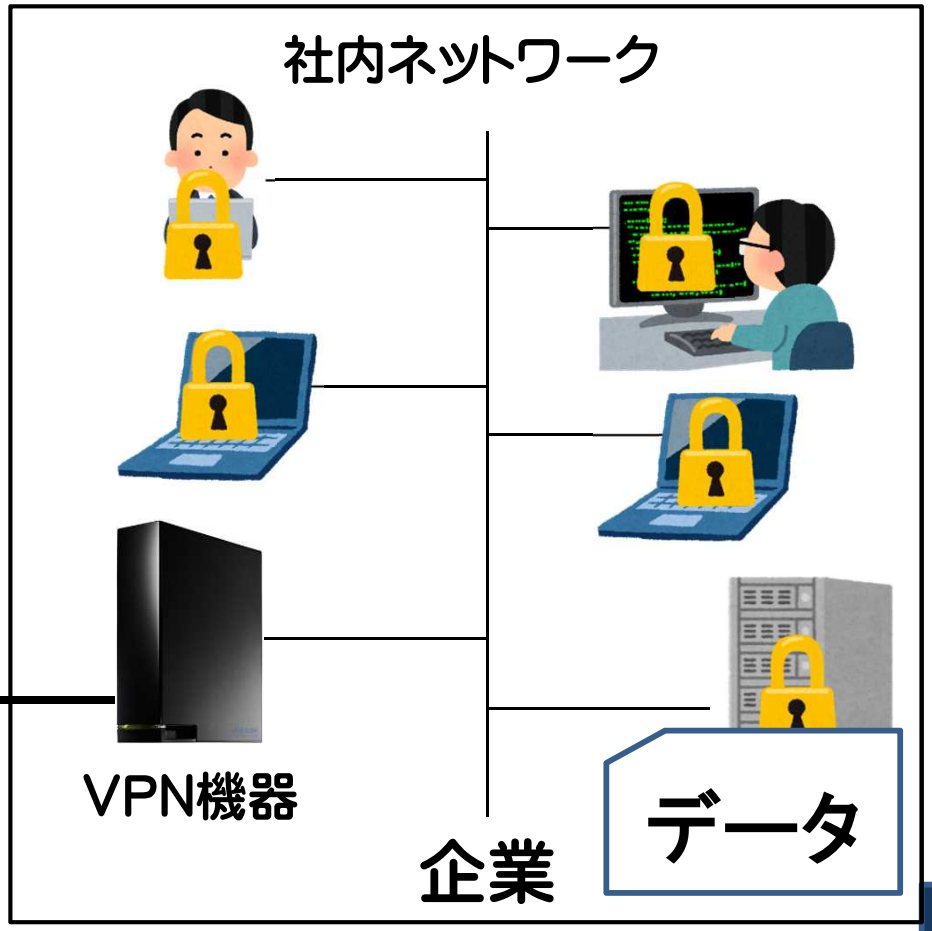


ランサムウェアの情勢（二重恐喝とは）

ランサムウェアの二重恐喝とは
　これまでと同様に暗号化したデータの復号の対価に加え、盗み出したデータを公開しないことを対価に金銭を要求する手口
のこと。

① VPN機器の脆弱性を突いて社内ネットワークに侵入
② 社内ネットワークに接続されているサーバやPCからデータを窃取
③ 社内ネットワークに接続されているサーバやPCのデータを暗号化
④ データの復号化を対価に金銭を要求
　盗み出したデータを公開しないことを対価に金銭を要求

犯罪者

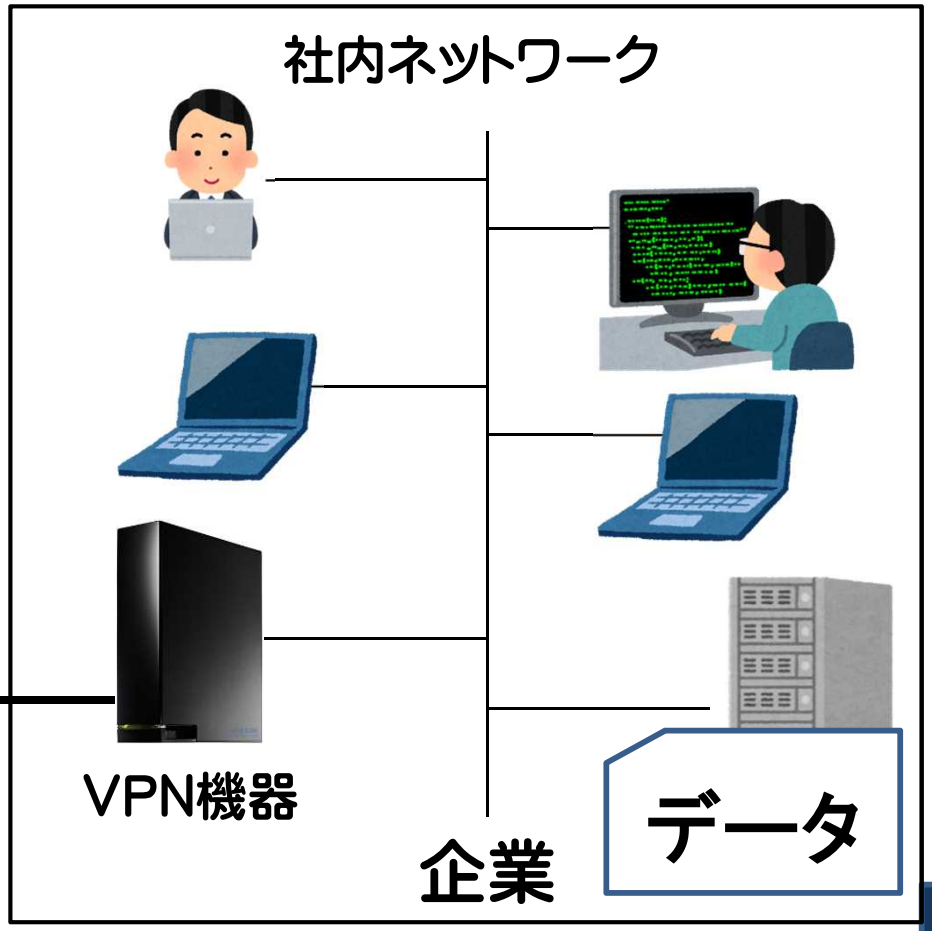


ランサムウェアの情勢（ノーウェアランサムとは）

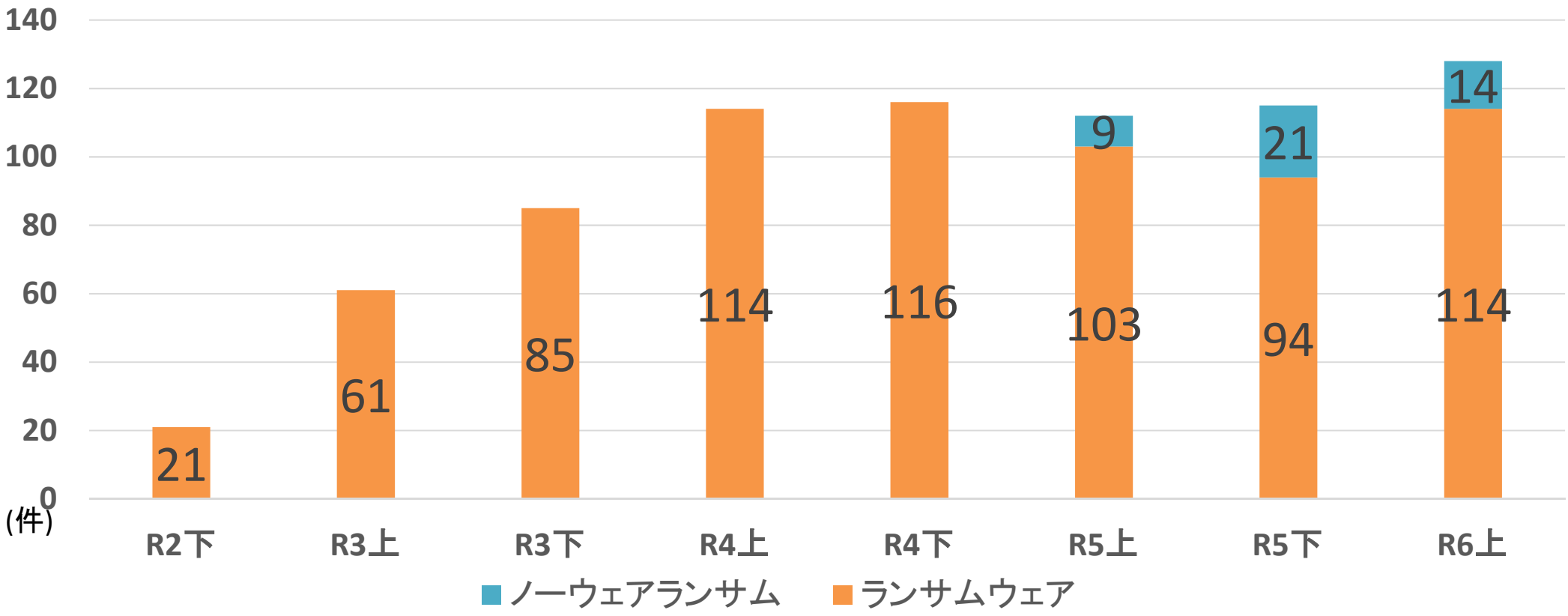
ノーウェアランサムとは
　企業・団体等のネットワークに侵入し、データを暗号化することなく
データを窃取した上で、企業・団体等に対価を要求する手口
のこと。

① VPN機器の脆弱性を突いて社内ネットワークに侵入
② 社内ネットワークに接続されているサーバやPCからデータを窃取
③ 盗み出したデータを公開しないことを対価に金銭を要求


犯罪者



ランサムウェアの情勢（企業・団体等におけるランサムウェア被害）



企業・団体等におけるランサムウェア被害の報告件数の推移（全国）
※　ノーウェアランサムは令和5年上半期から集計

※出典元：　警察庁　“令和6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”

宮城県内におけるランサムウェア被害認知状況

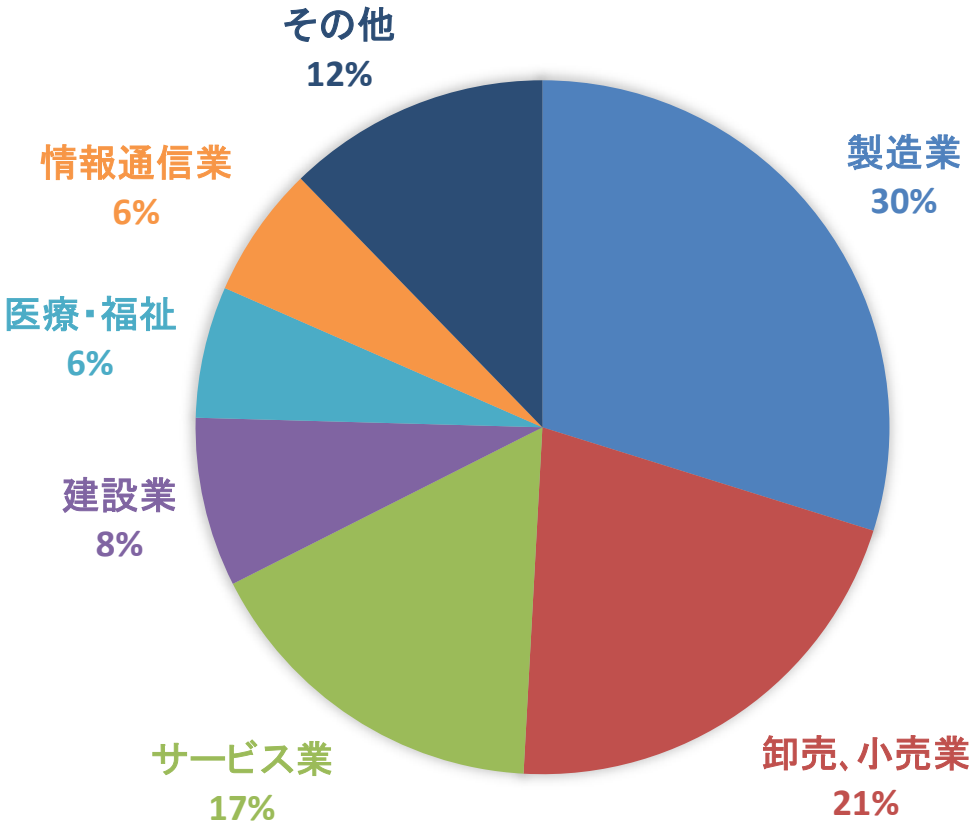
○　ランサムウェア被害認知件数の推移

年	R1	R2	R3	R4	R5	R6.11
件数	2	0	1	2	2	4

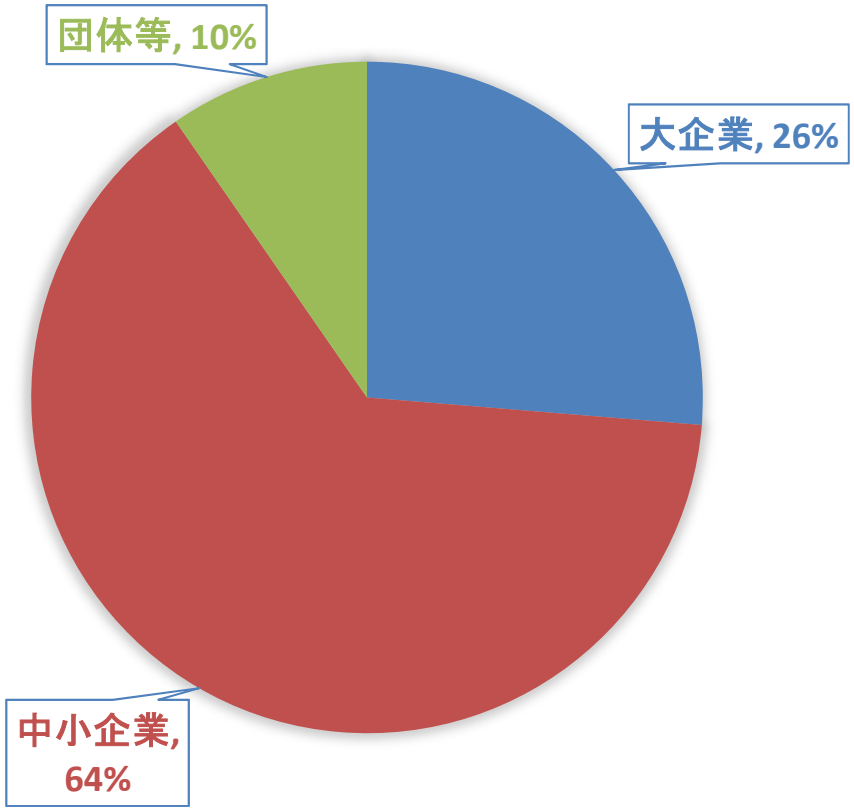
○　令和6年の発生状況

- 令和6年11月末時点で昨年の2倍である4件の被害を認知
- 件数は警察に通報・相談等により認知した件数であり、これ以上の被害が発生している可能性がある

ランサムウェアの情勢（企業・団体等におけるランサムウェア被害の実態）



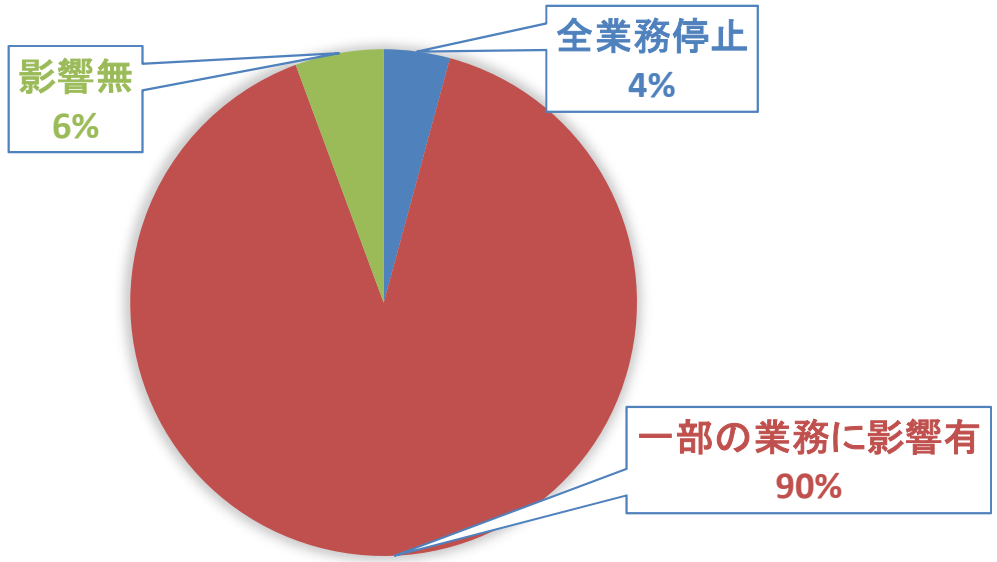
被害企業・団体の業種



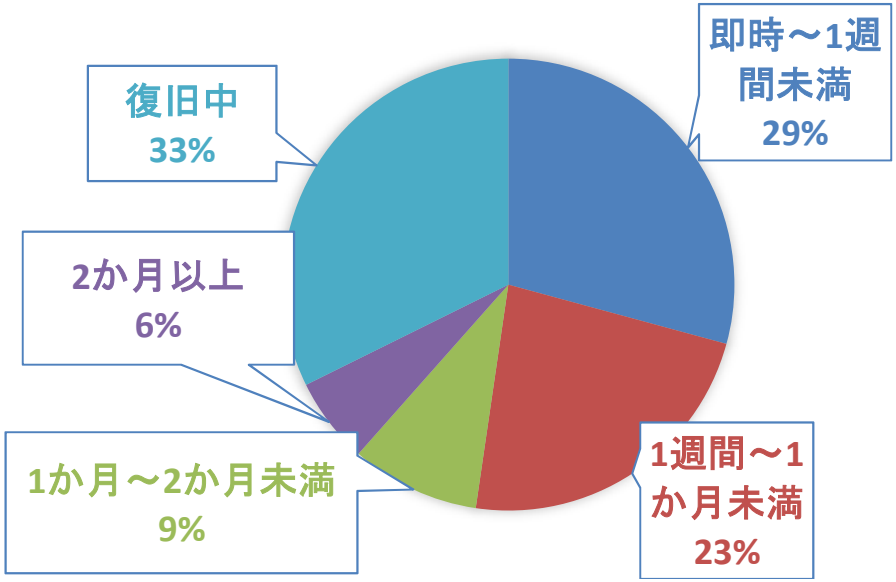
ランサムウェア被害の企業・団体等の規模別報告件数

※出典元： 警察庁 “令和6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”

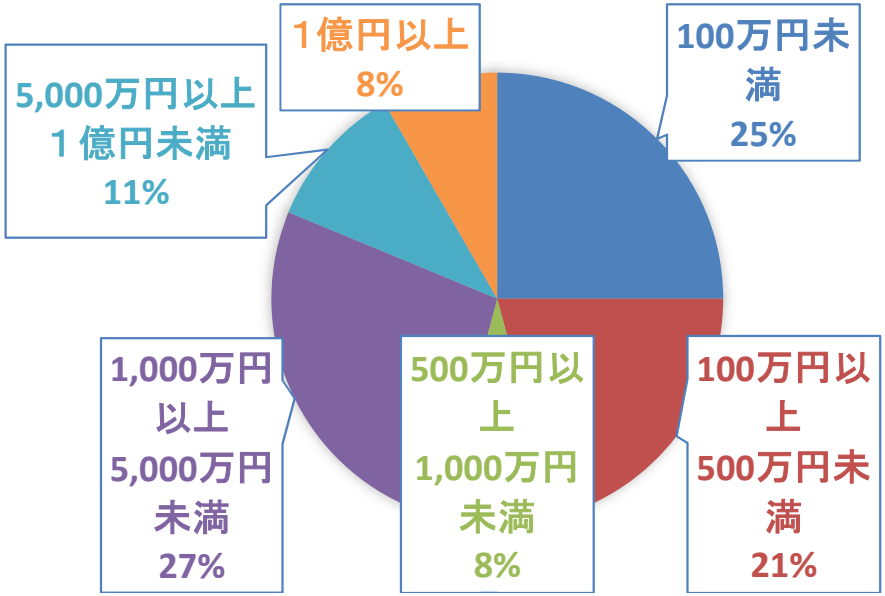
ランサムウェアの情勢（ランサムウェア業務に与えた影響等）



ランサムウェアが業務に与えた影響



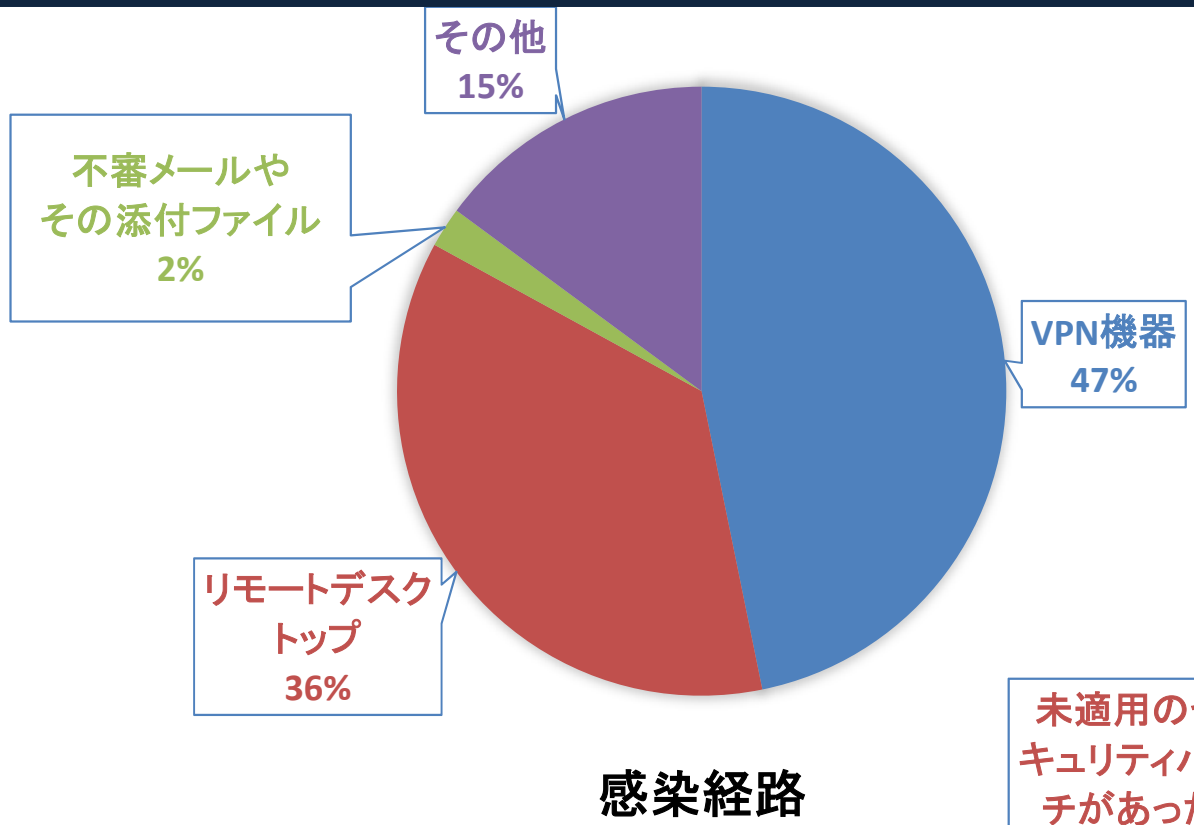
復旧に要した期間



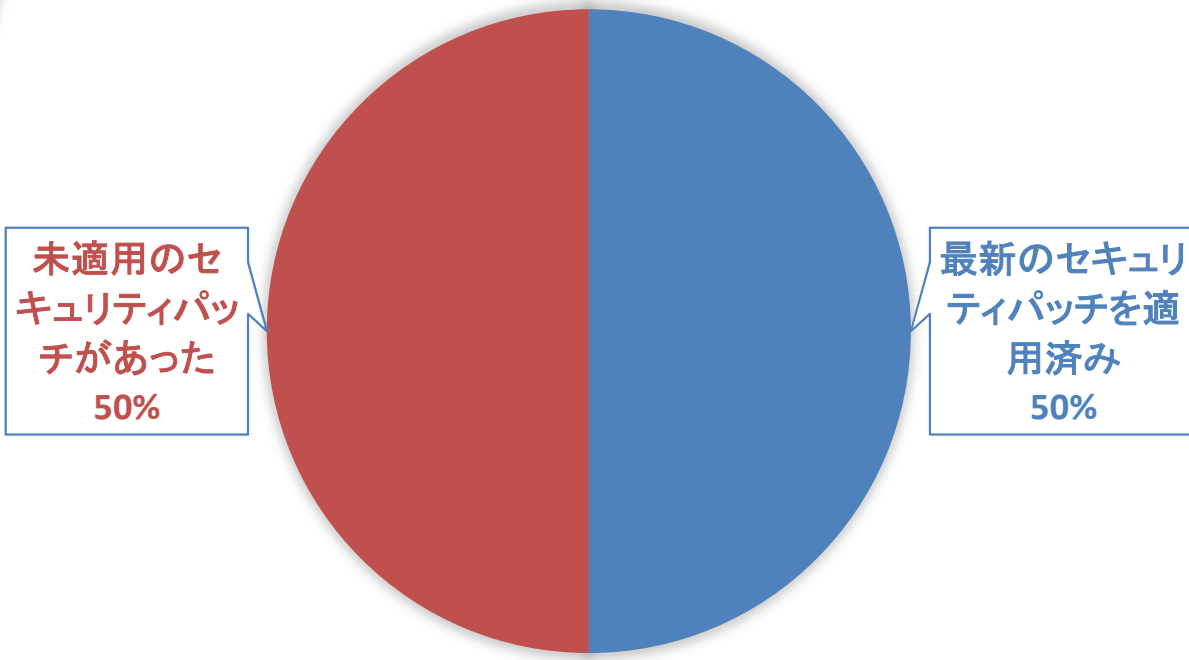
調査・復旧費用の総額

※出典元： 警察庁 “令和6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（ランサムウェアの感染経路等）



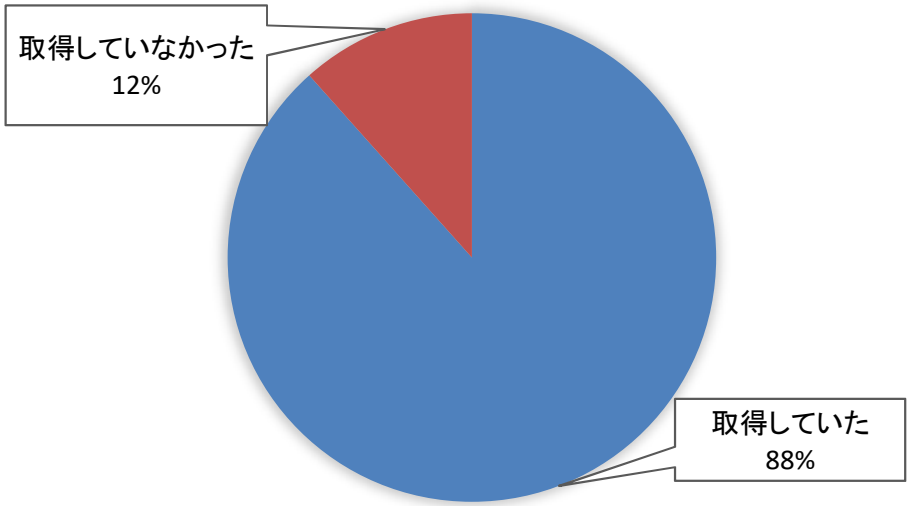
感染経路



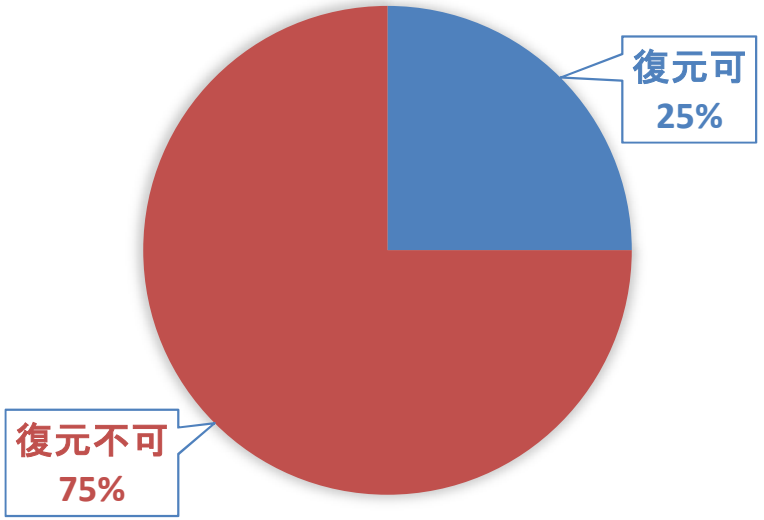
侵入経路とされる機器の
セキュリティパッチの適用状況

※出典元： 警察庁 “令和6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”

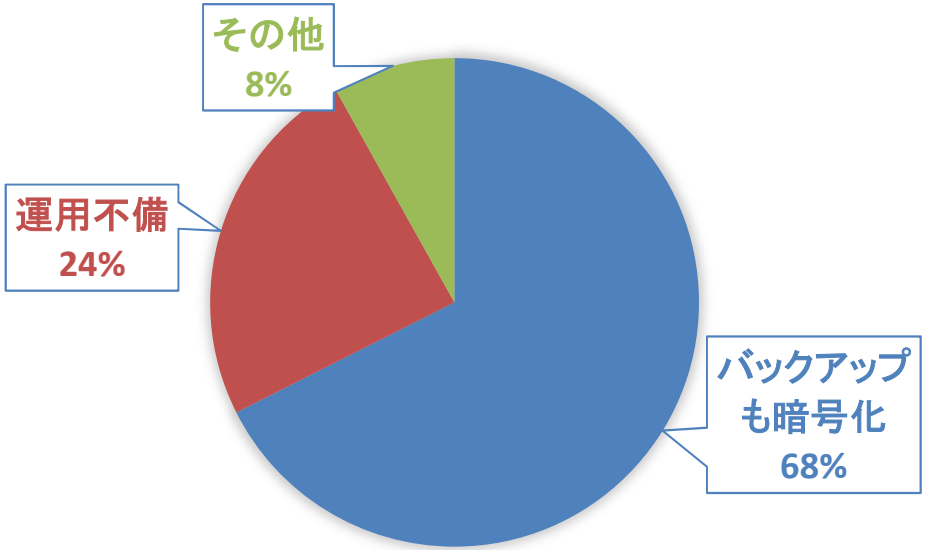
ランサムウェアの情勢（バックアップの取得の有無等）



バックアップの取得の有無



バックアップからの復元結果



バックアップからの復元ができなかった理由

※出典元： 警察庁 “令和6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（被害に遭わないため、被害を減少するため）

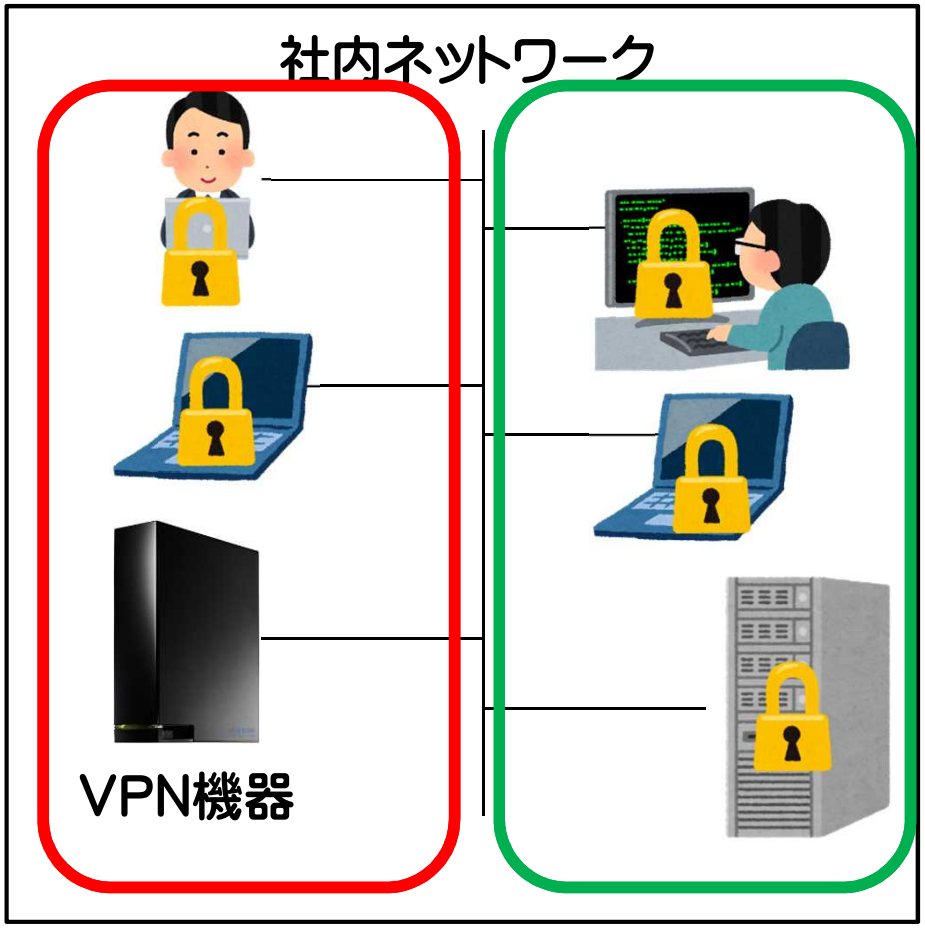
○ ランサムウェア被害に遭わないための対策

- VPN機器等のネットワーク機器のセキュリティアップデートの実施、設定の見直し
- 添付ファイルを安易に開かないよう社員教育
- ネットワークの切り分け

○ ランサムウェア被害を減少するための対策

- こまめなバックアップ
- バックアップ機器のネットワークからの隔離

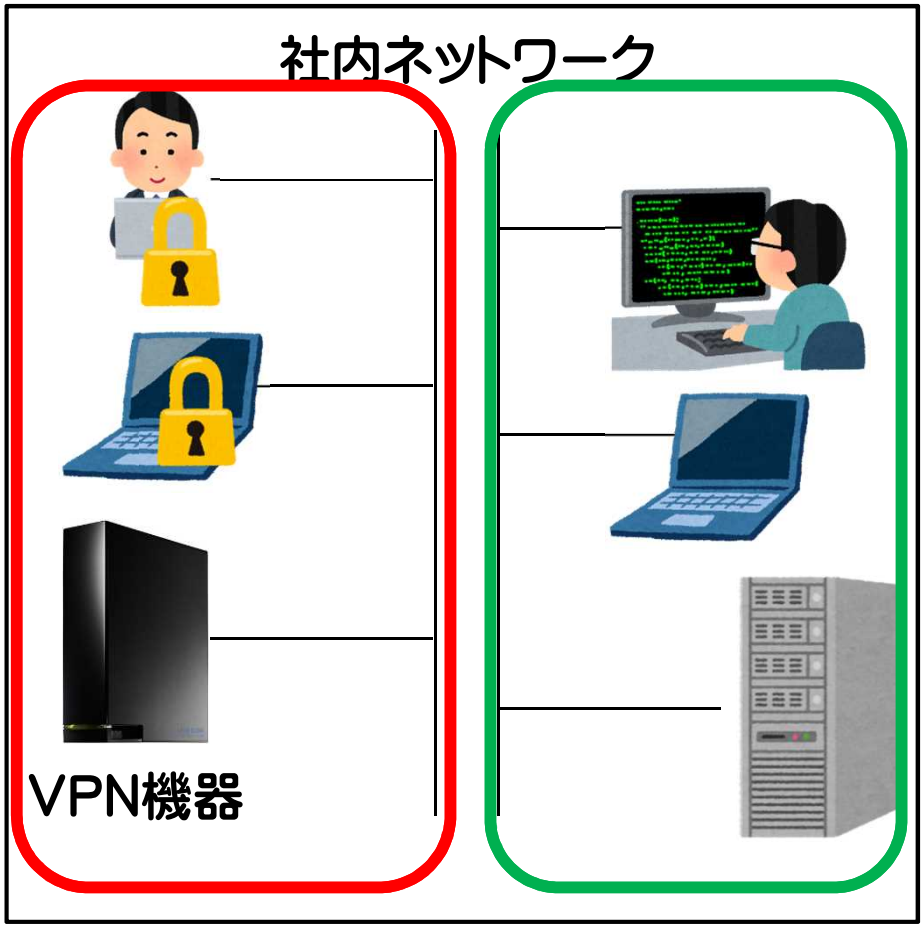
ランサムウェアの情勢（ネットワークの切り分けとは）



インターネット
接続必要

インターネット
接続不要

本来インターネット接続が不要なPC等も被害に！

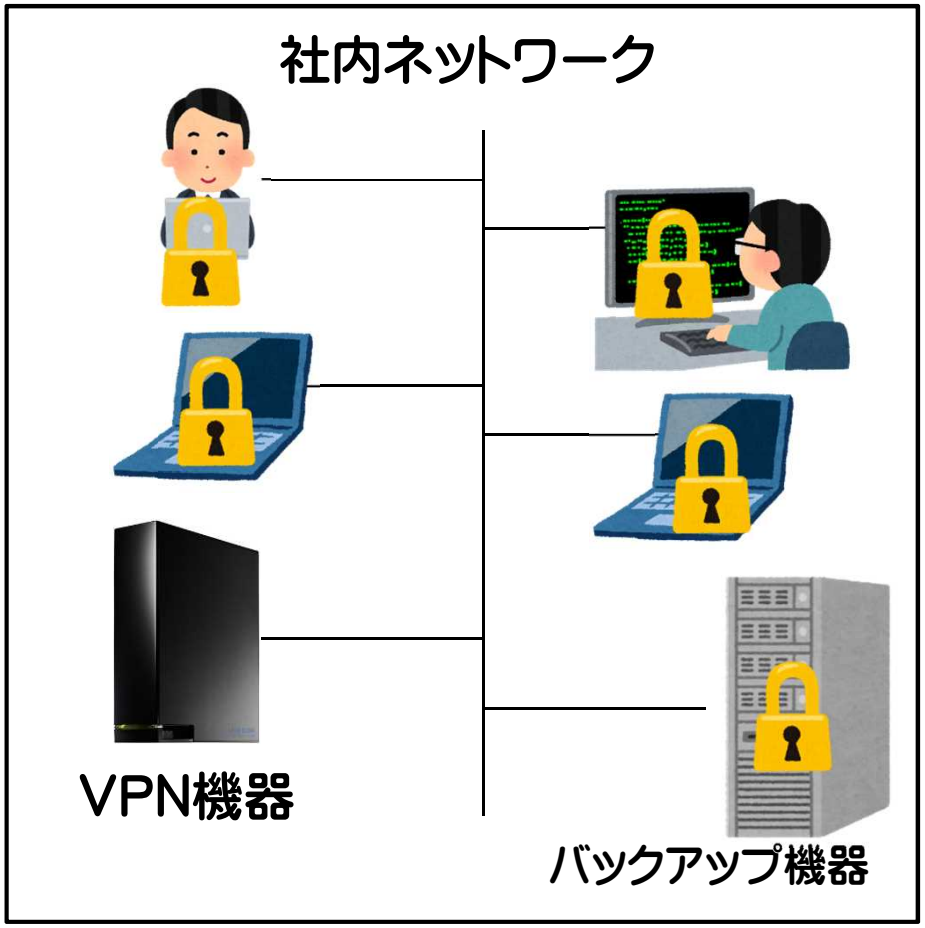


インターネット
接続必要

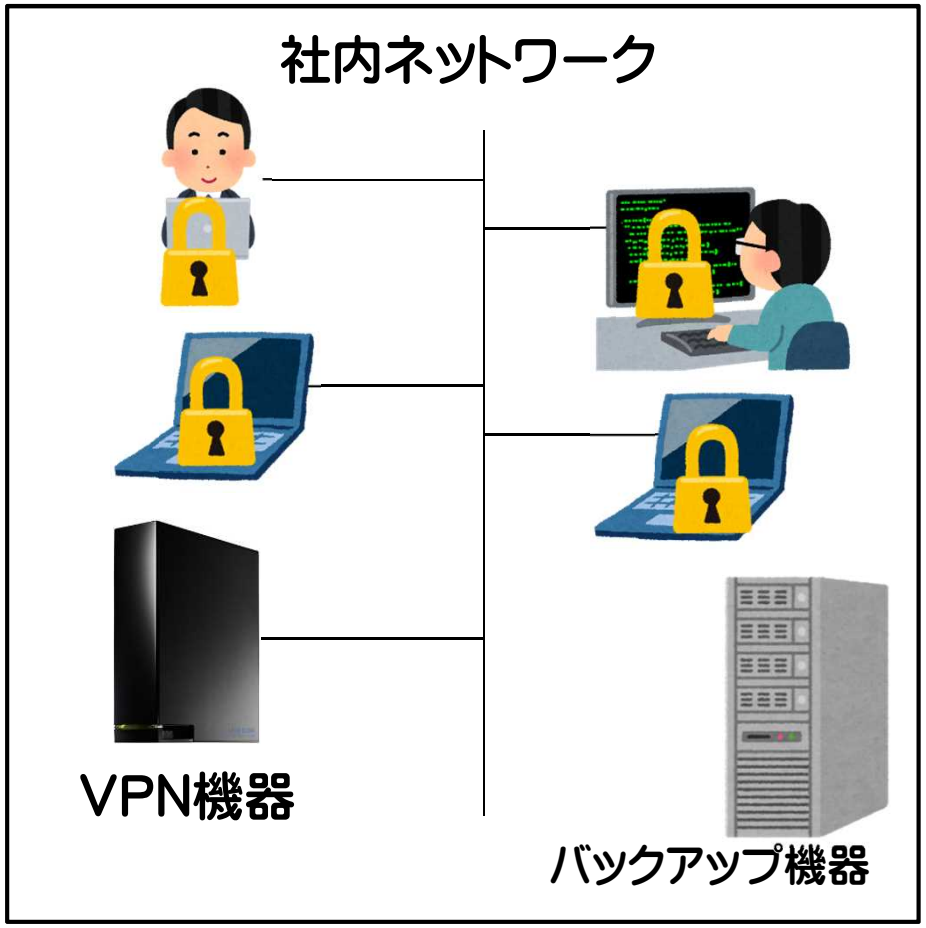
インターネット
接続不要

被害に遭うPC等を限定できる！

ランサムウェアの情勢（バックアップ機器のネットワークからの隔離とは）



バックアップ機器を常時ネットワークに接続しているとバックアップ機器も被害に！



バックアップ機器を必要時以外はネットワークから隔離すると、バックアップデータは被害から免れる！

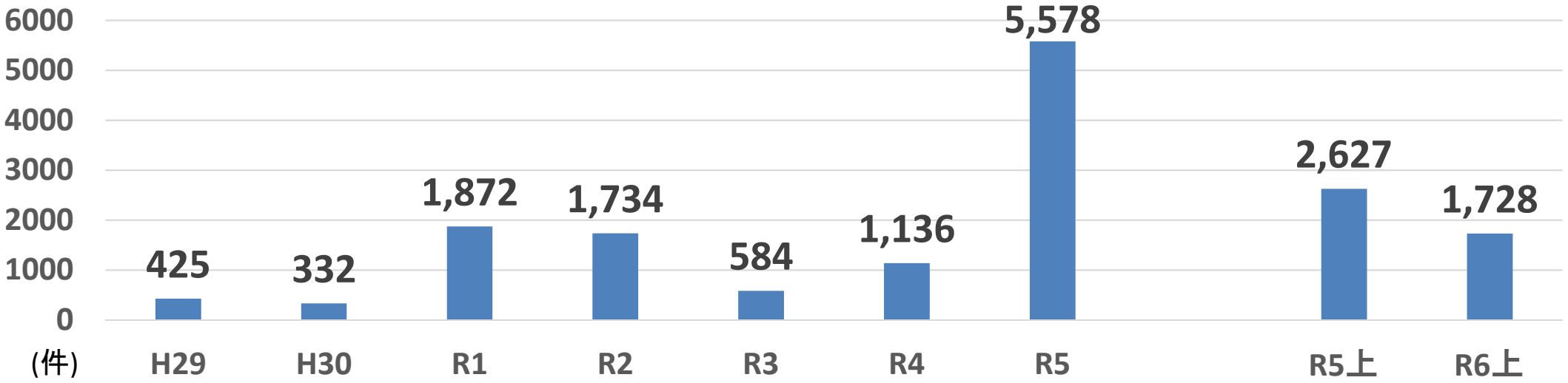
サイバー空間の脅威概況
～令和５年におけるサイバー空間をめぐる脅威の情勢等について～

脅威概況

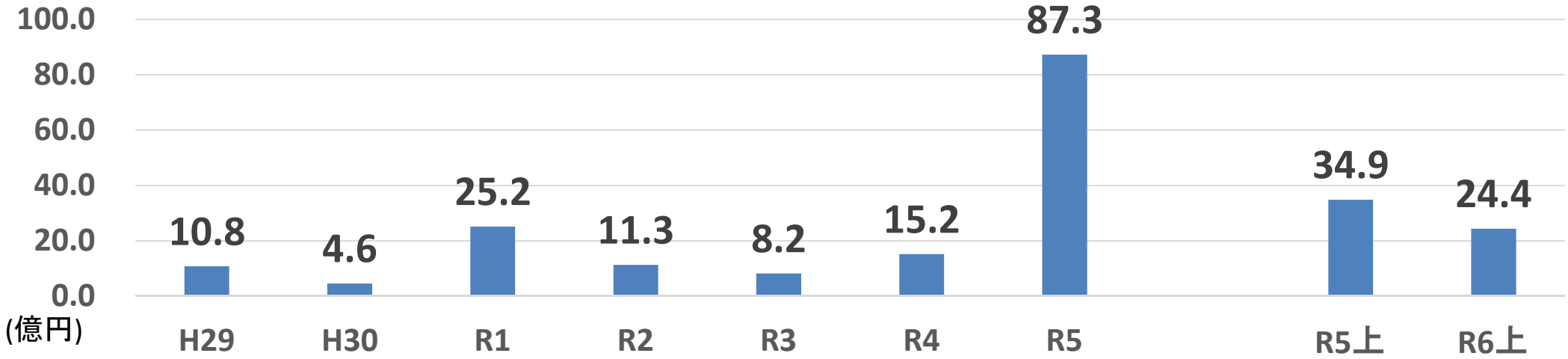
令和５年におけるサイバー空間をめぐる脅威については、ランサムウェア被害が依然として高水準で推移するとともに、クレジットカード不正利用被害が急増し、インターネットバンキングに係る不正送金被害が過去最多となり、インターネット上では児童ポルノや規制薬物の広告等の違法情報のほか、自殺サイトやいわゆる「闇バイト」の募集等の有害情報が氾濫するなど、極めて深刻な情勢が続いている。

※出典元：　警察庁　“令和５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”

インターネットバンキングに係る不正送金事犯の件数と金額（全国）



インターネットバンキングに係る不正送金事犯の発生件数の推移



インターネットバンキングに係る不正送金事犯の被害額の推移

※出典元： 警察庁 “令和6年下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”

インターネットバンキング不正送金（識別符号が流出する仕組み）

フィッシングとは
　実在する企業・団体等や官公庁を装うなどしたメール又はショートメッセージサービスを送り、その企業等のウェブサイトに見せかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するよう誘導し、当該フィッシングサイトでアカウント情報やクレジットカード番号等を不正に入手する手口
のこと。

フィッシングとは

攻撃者

① 攻撃者がフィッシングサイトを開設

フィッシング
サイト

④ クレジットカード情報が流出

② インターネット利用者に
フィッシングサイトへ誘導する
メールを送信

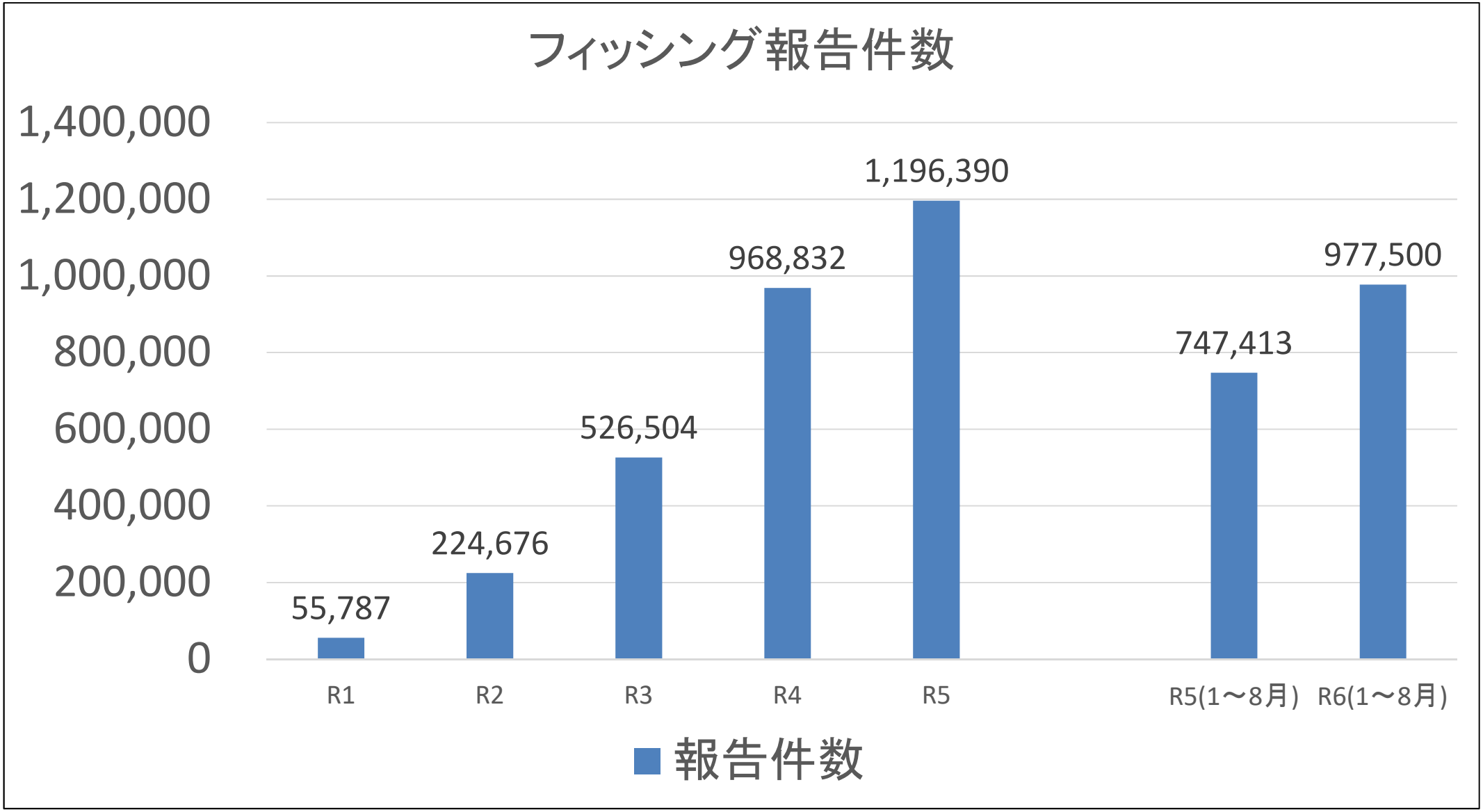
インターネット
利用者

③ インターネット利用者
がフィッシングサイトに
クレジットカード情報を
入力

○ メールは「このままだと利用停止になる」などの
慌てさせる内容

○ フィッシングサイトの表示内容は本物と全く同じ

フィッシングの現状
～過去5年間のフィッシング報告件数～



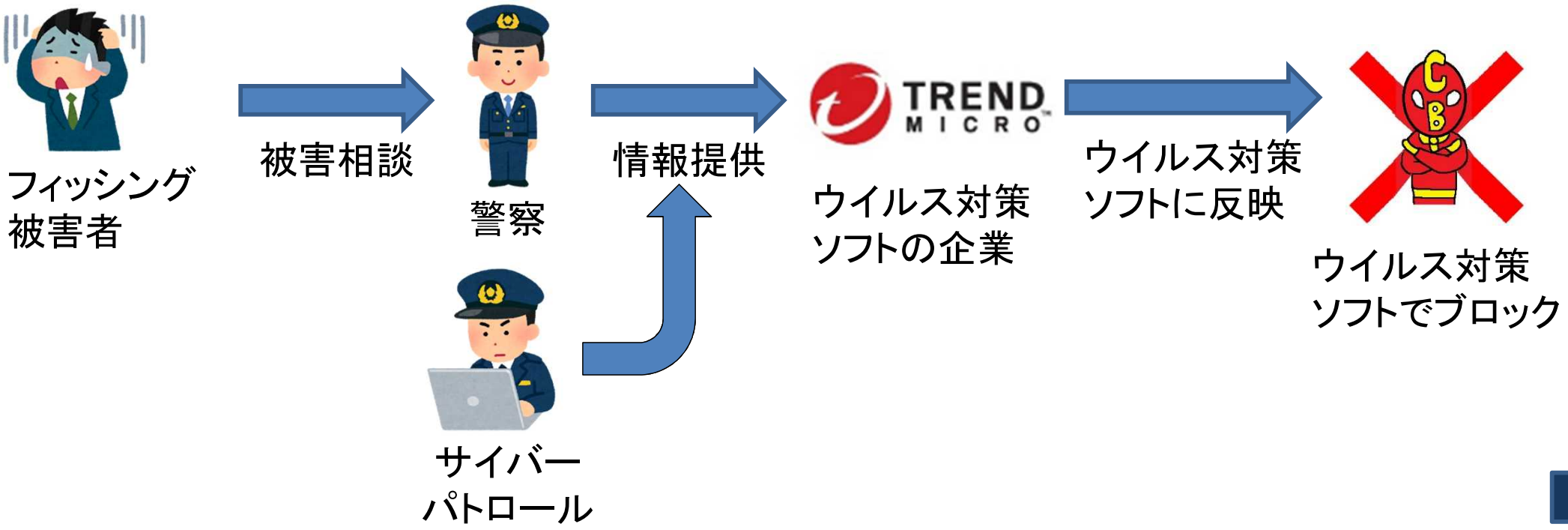
※出典元：フィッシング対策協議会“月次報告”を集計

インターネットバンキング不正送金（実際のフィッシングメール）

フィッシング対策
～警察におけるフィッシング対策～

○　フィッシングサイトのブロッキング措置

　警察では相談等で認知したフィッシングサイトのURLをウイルス対策ソフト企業に提供することで被害を抑止



フィッシング対策
～今からできるフィッシング対策～

○　メールやショートメールに書かれているURLからは接続しない

○　銀行やクレジットカード会社が提供しているアプリを活用する

○　ブラウザからログインする場合は、登録したブックマークから接続する

○　ウイルス対策ソフトを導入する

企業が被害に遭う事例（HP改ざん）

攻撃者

① 攻撃者がクレジットカード情報を収集するようにウェブサイトを改ざん

③ クレジットカード情報が流出

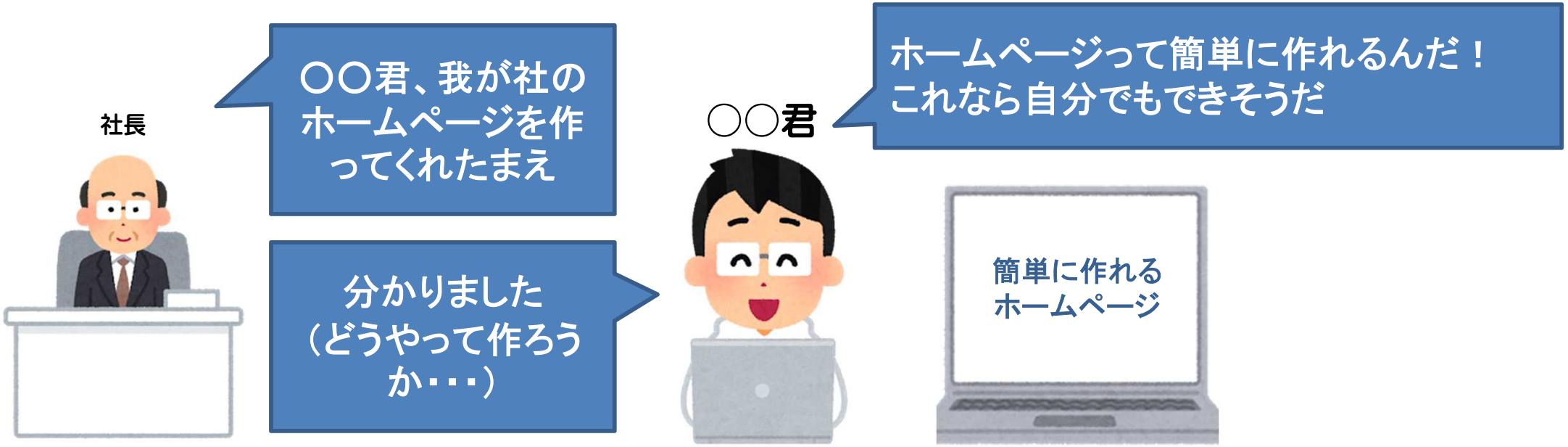
ウェブサイト

② 利用者がクレジットカード情報を入力

ウェブサイト利用者

○ クレジットカード情報の入手が目的
○ 見た目の変化がないので改ざんに気付きにくい

企業が被害に遭う事例（改ざんされやすいHP）



書かれているのは「ホームページの作り方のみ」であり、定期的にバージョンアップするなどのセキュリティに関する記載がない

見た目は奇麗だが改ざんしやすいホームページができあがる

企業が被害に遭う事例（無料のシステム）

○　無料システムの存在

- インターネット上には、無料の「ホームページ構築システム」、「ECサイト作成システム」、「メールマガジン配信システム」が存在
- 使用方法を紹介するサイトも存在し、簡単にシステムを構築できる

○　攻撃者から見た無料のシステム

「利用者が多い」、「ぜい弱性が放置されているケースが多い」ため、攻撃するメリットが高い

攻撃者

ぜい弱性が放置されてるじゃん！
攻撃し放題だ！

ウェブサイト

企業が被害に遭う事例（システムの悪用）

○ ホームページ改ざん

- 個人情報の流出
- クレジットカード情報の流出
- 不正プログラム感染の踏み台

○ メールシステムへの不正アクセス

- 個人情報の流出
- 脅迫メール送信の踏み台

最新版にしておくことが重要！

お宅の会社からクレジットカード情報が漏れたんだけど！
補償してくれるんでしょ！

企業が被害に遭う事例（標的型メール攻撃）

- ○　会計担当者への請求書データが添付されたメール
- ○　人事担当者への履歴書データが添付されたメール
- ○　修理担当者への故障部位の写真が添付されたメール

○　不用意に添付ファイルを開くと、情報を盗み取る等の不正プログラムに感染する

○　「うちの会社は大した技術はないから」などと過小評価しない

企業が被害に遭う事例（BEC）

「BEC」とは「ビジネスメール詐欺」のこと

A社の○○です。
代金はABC銀行に振り込んでください。

A社の○○です。
代金はABC銀行ではなくXYZ銀行に振り込んでください。

A社の○○です。
ABC銀行への振り込みはまだですか？

ABC銀行に振り込めばいいのね

そうなんだ。じゃあXYZ銀行に振り込めばいいのね

え？
XYZ銀行じゃないの？

振込先は犯罪者の口座

企業が被害に遭う事例（BEC）

社長だが、至急XYZ銀行に1，000万円を振り込んでくれ。

なに！？
私はそんな指示なんかしていないぞ！

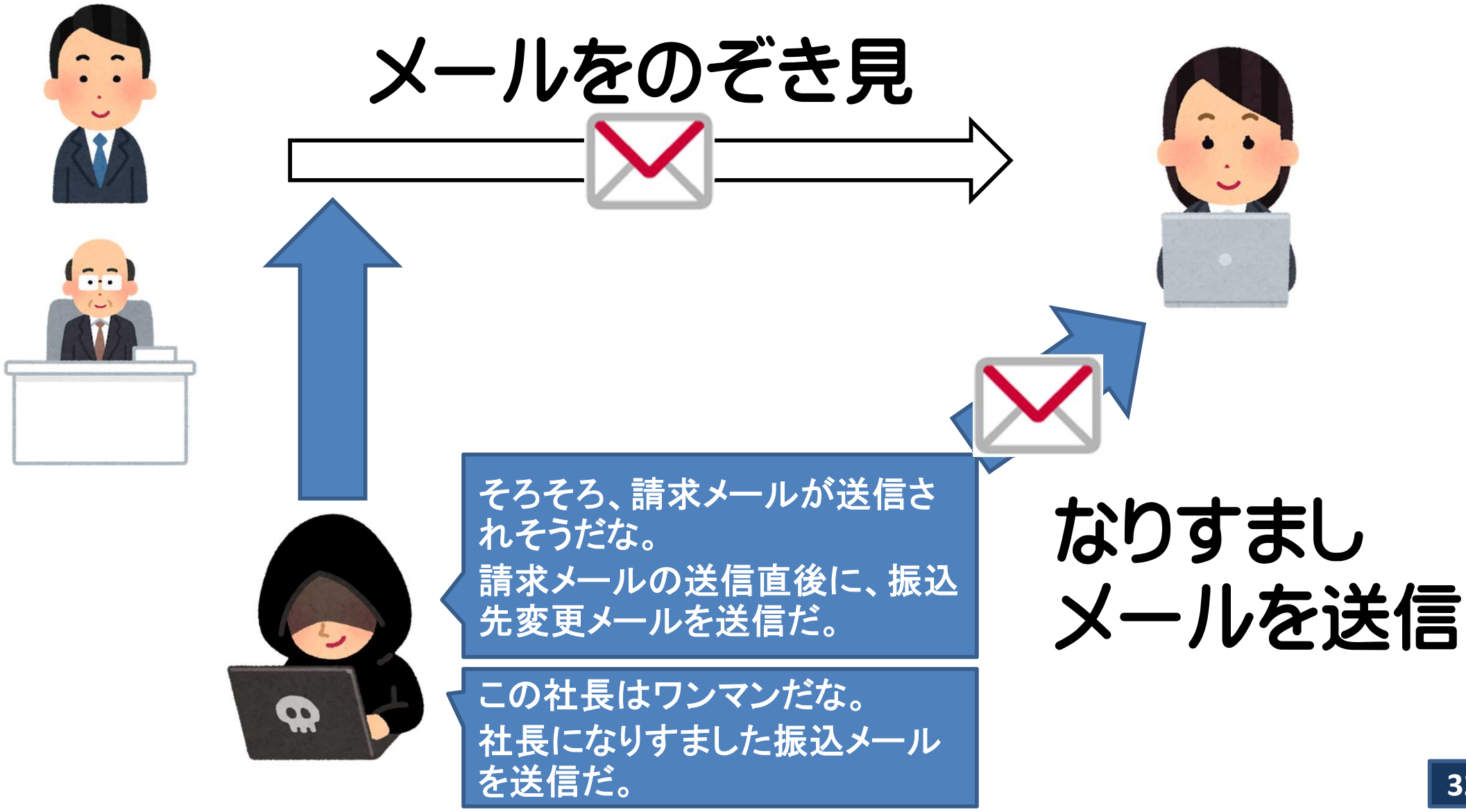
大金だけど、社長の指示だから従うしかねないわね。

社長。指示どおりXYZ銀行に1,000万円を振り込みました。

でも、社長のメールアドレスから来てましたよ？

振込先は犯罪者の口座

企業が被害に遭う事例（BEC）



被害に遭わないために

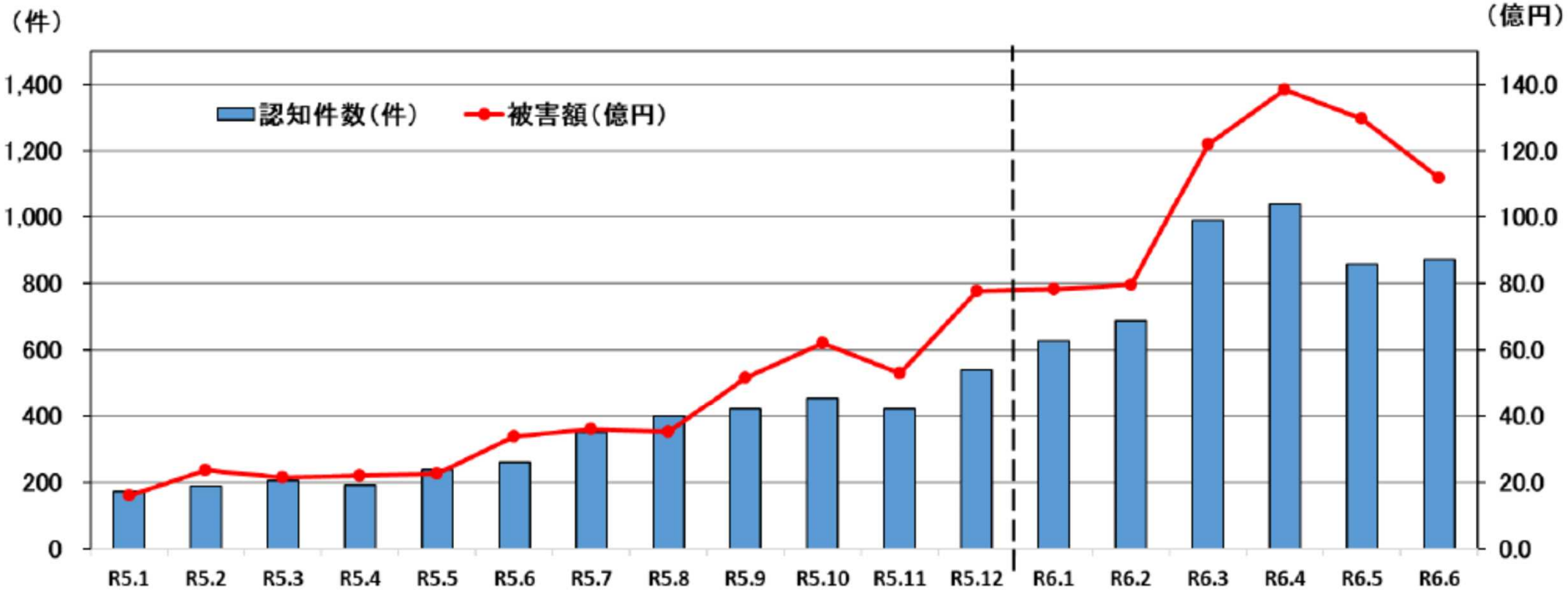
○　セキュリティ専従担当者を配置する又は信頼できる会社へ委託する
○　経営層はセキュリティ費用は必要経費という認識を持つ
○　常に「狙われている」という認識を持つ
○　適切な社員教育を行う

それでも被害に遭ってしまったら

○　速やかに警察に通報・相談する

SNS型投資詐欺・ロマンス詐欺

SNS型投資・ロマンス詐欺とは
　SNSを通じて対面することなく、交信を重ねるなどして関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭をだまし取る又は恋愛感情や親近感を抱かせて金銭をだまし取る犯罪
のこと。



※出典元：　警察庁　“令和6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”

SNS型投資・ロマンス詐欺の特徴

○　昨年下半期の増加が顕著
○　被害者の性別は男性が約52.4%、女性が約47.6%
○　被害者は40代以上で約9割を占める
○　当初の接触の約6割がLINE、フェイスブック、インスタグラム
○　その後、9割以上がLINEに移行してだまされる
○　LINEでは著名人や投資家になりすました者が現れ、投資を勧める
○　アプリ上では運用利益が上昇しているように見えるため、投資額が増加する（利益と称して少額が振り込まれるため信用してしまう）
○　出金できないため詐欺であることが判明する
○　ロマンス詐欺でも投資に引き込まれる

現役世代が狙われる！

※出典元：　警察庁　“特殊詐欺対策ページ”

SNS型投資・ロマンス詐欺の防止対策

○ 「投資先が実在しているか」、「国の登録業者かどうか」を確認する
○ 「確実に利益が出る」、「絶対に儲かる」、「あなたにだけ教えます」などの文言に注意する
○ 「著名人」がなりすましでないか公式アカウントで確認する
○ 振込先口座が「個人名義」や「毎回変わる」等の不審点がないか確認する
○ 実際に会ったことのない相手の言葉は鵜呑みにしない
（生成AIの進歩によりフェイク動画が簡単に作られるようになり、動画だけでは実在するかどうか判断できない）
○ 友人・同僚からの紹介でも安易に信用しない

家族・友人・職員を守ろう！

御清聴ありがとうございました