実践的なサイバーセキュリティ対策

～なりすまし詐欺等ネット詐欺への対応を含めて～

令和６年７月３日　警視庁サイバーセキュリティ対策本部

1　個人編

(1)　ニセ投資詐欺　　（なりすまし詐欺・SNS型投資詐欺）

(2)　ニセ銀行・宅配等詐欺（フィッシング詐欺）

(3)　ニセ警告詐欺　　（サポート詐欺）

2　企業編

(1)　サイバー空間における脅威の情勢

(2)　メール攻撃

(3)　ランサムウェア攻撃

(4)　社内ネットワークの見える化

1　個人編

(1)　ニセ投資詐欺

【ＳＮＳ型投資詐欺】
ＳＮＳ等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などで金銭等をだまし取る詐欺（ＳＮＳ型ロマンス詐欺に該当するものを除く。）

ＳＮＳ型投資詐欺の特徴

○　犯人らは、ＳＮＳで著名人の名前や写真を悪用し、「投資で儲かる」「投資スクール」等と嘘の投稿をしている

○　犯人らは、被害者の「この著名人であれば、信用できる」「投資で儲けたい」等の心理につけ込み、あたかも利益が出ているように信じさせ、投資金名目やその利益の出金手数料名目などで金銭等をだまし取る

■　認知件数・被害額　全国（都内）

令和６年４月末
　認知件数　2,508件（212件）
　被害金額　334.3億円（48.1億円）

令和５年
　認知件数　2,271件（210件）
　被害金額　277.9億円（38億円）

【手口例】

＜その１（SNS広告型）＞

○　インスタグラムやフェイスブックなどのＳＮＳ上に、投資家や著名人を騙り「投資で稼げる」などの広告を掲載

○　被害者が広告をクリックすると、ＬＩＮＥに誘導し、トークグループに招待する

○　指南役やアシスタント役を装い、投資の取引に必要との名目でアプリをインストールさせ、被疑者側の口座を指定して入金させる

○　アプリ上ではあたかも利益が出ているかのように見せ、さらに追加入金させる

○　被害者が出金しようとすると「手数料」が必要などと理由をつけて追加入金させた後、連絡を絶ち、現金をだまし取る

＜その２（ＤＭ型）＞

○　インスタグラム、フェイスブック、ＴｉｋＴｏｋなどSNSのDM（ダイレクトメッセージ）で接触する

○　ＬＩＮＥに誘導し、メッセージの交換を重ねて親しくなる

○　投資で儲けが出ていると自慢し、信用させるために投資アプリのスクリーンショットを送る

○　必ず儲かるからと参加を求め、入金後、連絡を絶ち現金等をだまし取る

【実践的な対策方法】

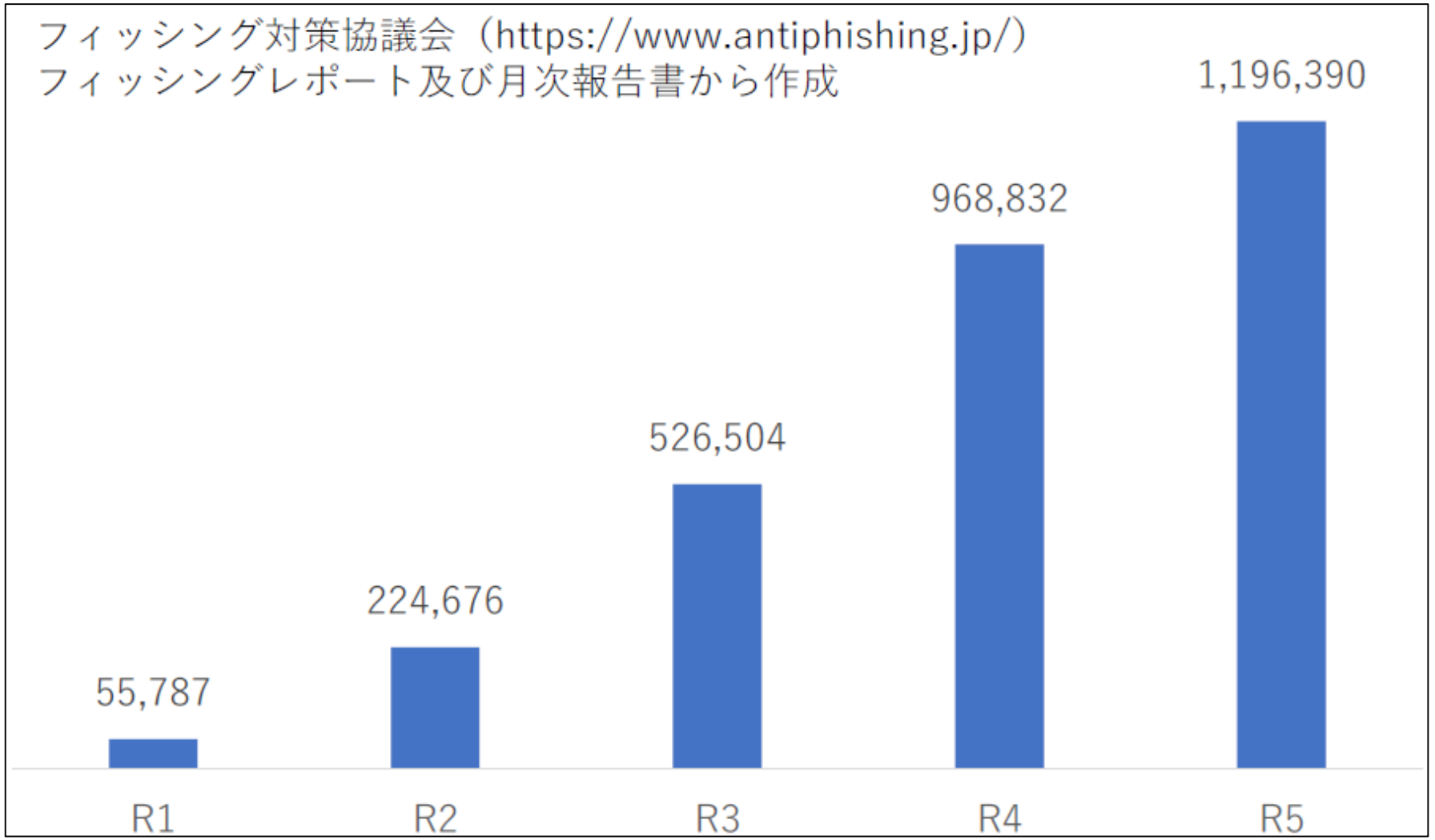
○　有名人の名前や写真が無断で悪用されている広告もあるので注意する
○　勧誘者や業者が金融商品取引業の登録を受けているかを金融庁のＨＰで確認する
○　ＤＭやグループチャットでの儲け話に注意する
○　「個人名の口座」には振り込まない

(2)　ニセ銀行・宅配等詐欺（フィッシング詐欺）

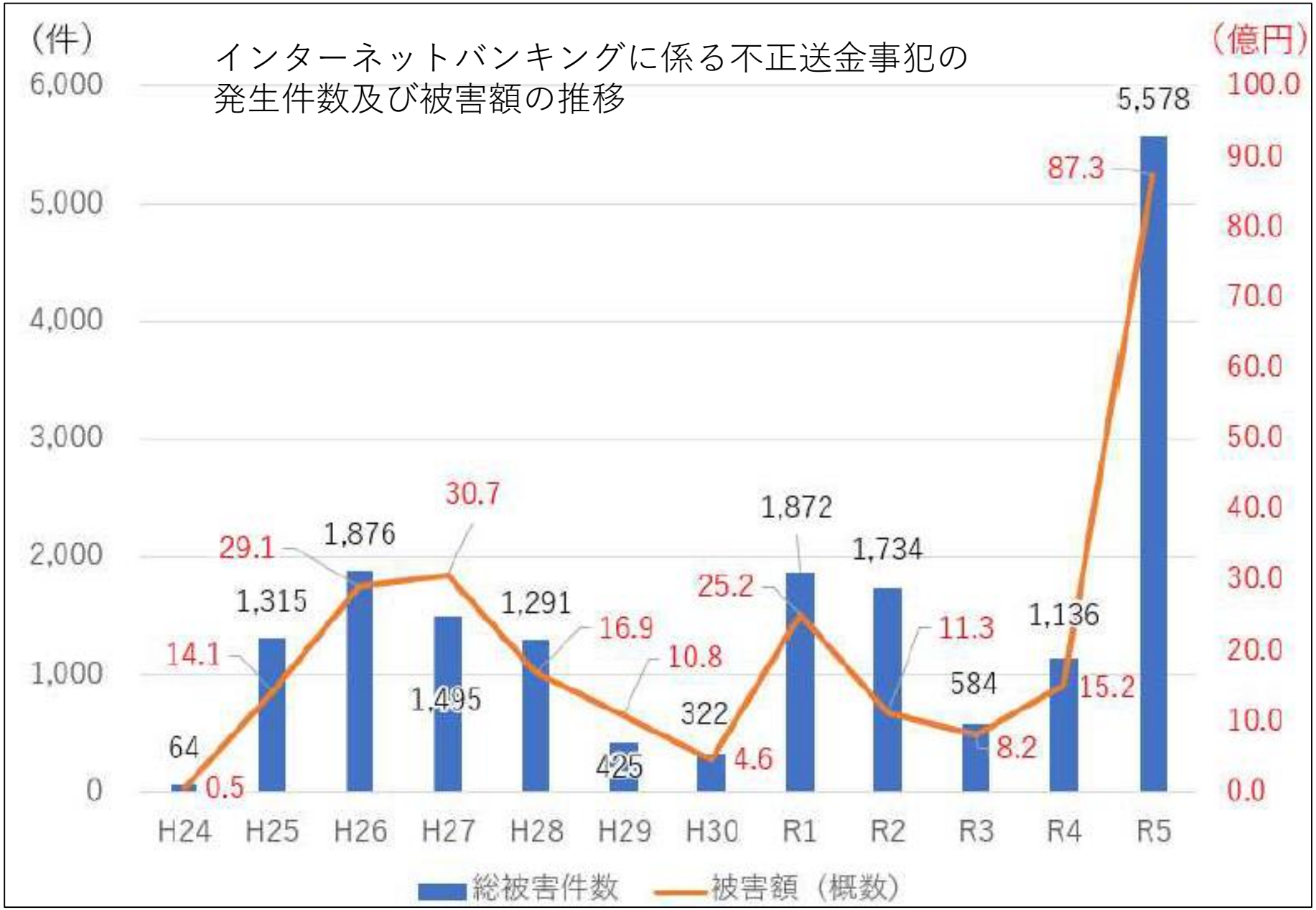
実在のサービスや企業をかたり、偽のメールやＳＭＳ（携帯電話のショートメッセージ）で偽サイトに誘導し、ＩＤやパスワードなどの情報を盗んだり、マルウェアに感染させたりするもの

情報を盗まれると、アカウントを乗っ取られてお金を奪われたり、インターネットの通信販売サイトで勝手に買い物をされる

マルウェアに感染してしまうと、スマートフォンに登録された電話帳の情報が盗まれたり、自分のスマートフォンがフィッシングＳＭＳの発信源になってしまうこともある



出典：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について」



出典：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について」

ＳＭＳによるフィッシング（スミッシング）の事例

偽宅配便業者

佐川急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。http://

お荷物の確認は日本郵便サイトにてご確認ください。http://

やまと運輸よりお荷物を発送しましたが、宛先不明です、下記よりご確認ください。http://

偽通信事業者

auお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。

ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
http

【KDDI】利用料金の未払い金があります。お支払期限を過ぎた利用料金があります。ご確認ください。http

出典：情報処理推進機構「安心相談窓口だより」

税金のお支払い方法に問題があります、更新してください：https://www.td[redacted].net/WbqFUa2494

【国税庁８月12日】未払い税金お支払いのお願い。ご確認ください。https://cutt.ly/[redacted]

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください 1kr[redacted]com?us9ia

【重要なお知らせ】SoftBank未払い料金お支払いのお願い。
http://fhmwt.[redacted].xyz

【利用停止予告】NTTドコモ未払い料金お支払いのお願い。
https://bit.ly/[redacted]

【auからの重要なお知らせ】
ご利用金額が設定した金額を超えました。ご確認が必要です。
https://bit.ly/3[redacted]

出典：フィッシング対策協議会「フィッシング報告状況」月次報告書

A 銀行

本物のサイト

フィッシングサイト

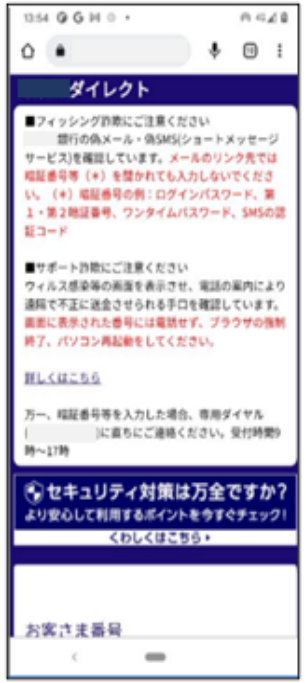
B 銀行

本物のサイト

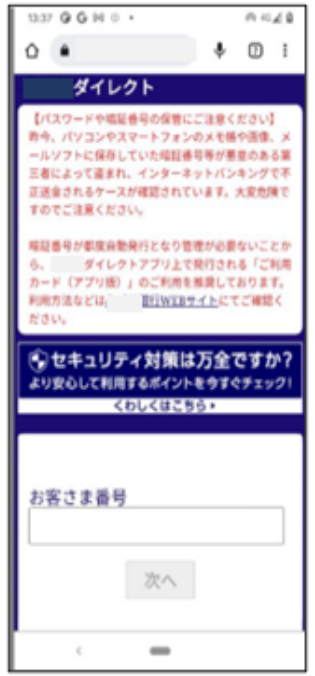
フィッシングサイト

C 銀行

本物のサイト



フィッシングサイト



出典：（一財）日本サイバー犯罪対策センター「JC3コラム-悪質な不正送金の実態」

【実践的な対策方法】

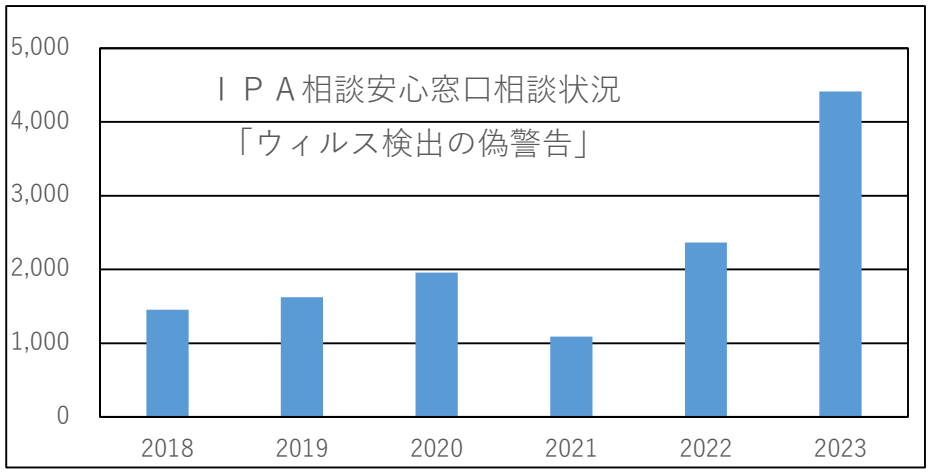
○　メールやＳＭＳ（ショートメッセージサービス）に記載されたＵＲＬにはアクセスしない
○　メールやＳＮＳのリンク先からログインや個人情報を入力しない
○　銀行の公式アプリや公式サイトからアクセスする
○　パスワードの使い回しをしない→※業務用を含めて

(3)　ニセ警告詐欺（サポート詐欺）

　サポート詐欺とは、パソコンでインターネットを閲覧中に、突然、ウイルス感染したかのようなウソの画面を表示させたり、警告音を発生させるなどして、ユーザーの不安を煽り、画面に記載されたサポート窓口に電話をかけさせ、サポート名目で金銭を騙し取ったり、遠隔操作ソフトをインストールさせたりする。

※　コンビニ等で売っている電子マネーカードやネットバンキングによる支払いの被害がある

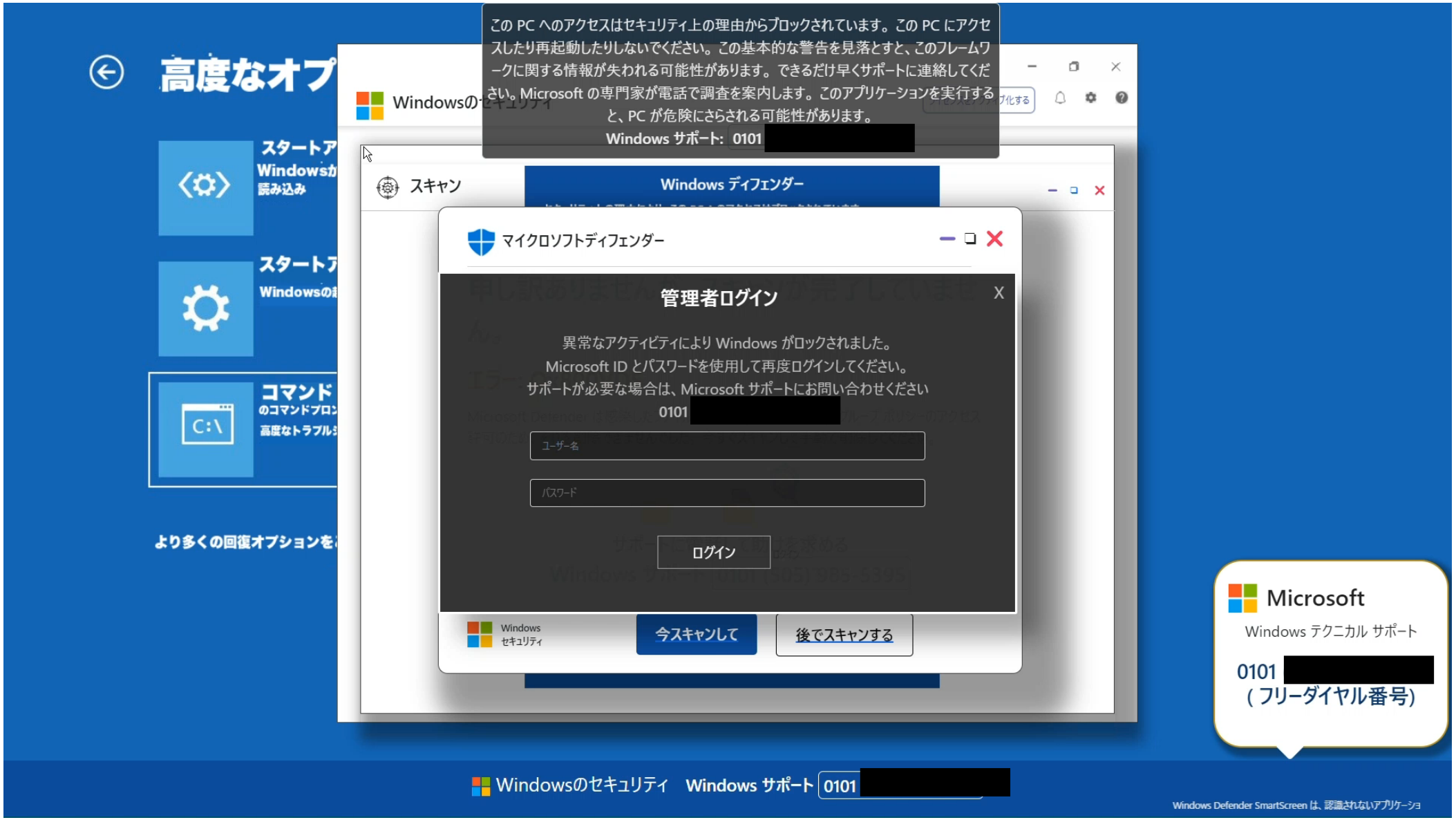
※　遠隔操作ソフトにより、ネットバンキングの送金金額の改ざんやパソコンやネットワーク内の情報が盗まれる（流出）場合がある



■　認知件数・被害額　都内

令和６年５月末
　認知件数　107件
　被害金額　0.4億円

令和５年
　認知件数　233件
　被害金額　1.７億円


この PC へのアクセスはセキュリティ上の理由からブロックされています。この PC にアクセスしたり再起動したりしないでください。この基本的な警告を見落とすと、このフレームワークに関する情報が失われる可能性があります。できるだけ早くサポートに連絡してください。Microsoft の専門家が電話で調査を案内します。このアプリケーションを実行すると、PC が危険にさらされる可能性があります。
Windows サポート: 0101
高度なオプ
スタートア
Windowsか
読み込み
スタートア
Windowsの
コマンド
のコマンドプロン
高度なトラブル
より多くの回復オプションを
Windowsのセキュリティ
スキャン
Windows ディフェンダー
マイクロソフトディフェンダー
管理者ログイン
異常なアクティビティにより Windows がロックされました。
Microsoft ID とパスワードを使用して再度ログインしてください。
サポートが必要な場合は、Microsoft サポートにお問い合わせください
0101
ユーザー名
パスワード
ログイン
Windows セキュリティ
今スキャンして
後でスキャンする
Microsoft
Windows テクニカル サポート
0101
(フリーダイヤル番号)
Windowsのセキュリティ Windows サポート 0101
Windows Defender SmartScreen は、認識されないアプリケーショ

サポート詐欺の被害発生の流れ

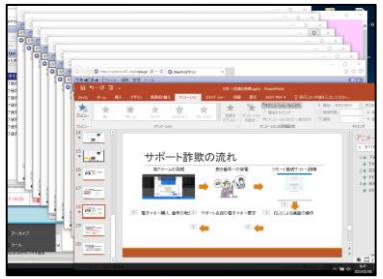
① 偽警告画面の表示

通常の操作では閉じることができない

② 表示番号へ架電

③ 遠隔操作ソフトのインストール

④ 犯人による遠隔操作



ＰＣ内、ネットワークから情報窃取

⑤ サポート料として電子マネーの要求

⑥ 電子マネーの購入コード番号の教示

さらに・・・

ネット銀行で送金を要求する新たな手口も確認されている。

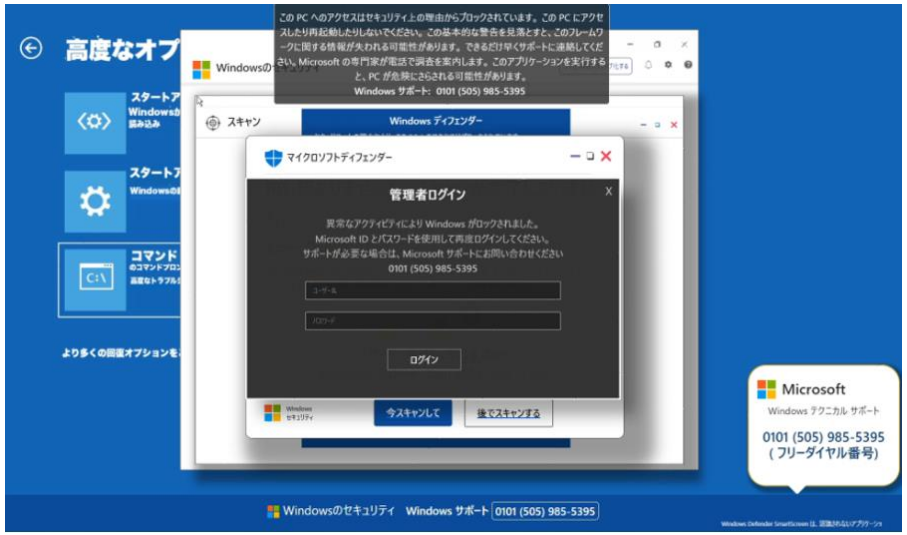
少額の送金を要求されて金額を入力すると、遠隔操作で勝手に送金額の末尾に「０」が追加され、多額の金銭をだまし取られる可能性も！？

¥5,000 ⇒ ¥5,000,000？！

【実践的な対策方法】

○　警告画面は無視してＥＳＣキーを長押し（３秒以上）後、×ボタンで閉じる
○　警告画面の電話番号に連絡をしない
○　電子マネーカードの購入を要求されても従わない
○　ネットバンキングの接続を行わない

偽の警告画面が表示されたら→



ＥＳＣキー長押しの後×ボタンで閉じる

2　企業編

(1)　サイバー空間における脅威の情勢

(2)　メール攻撃

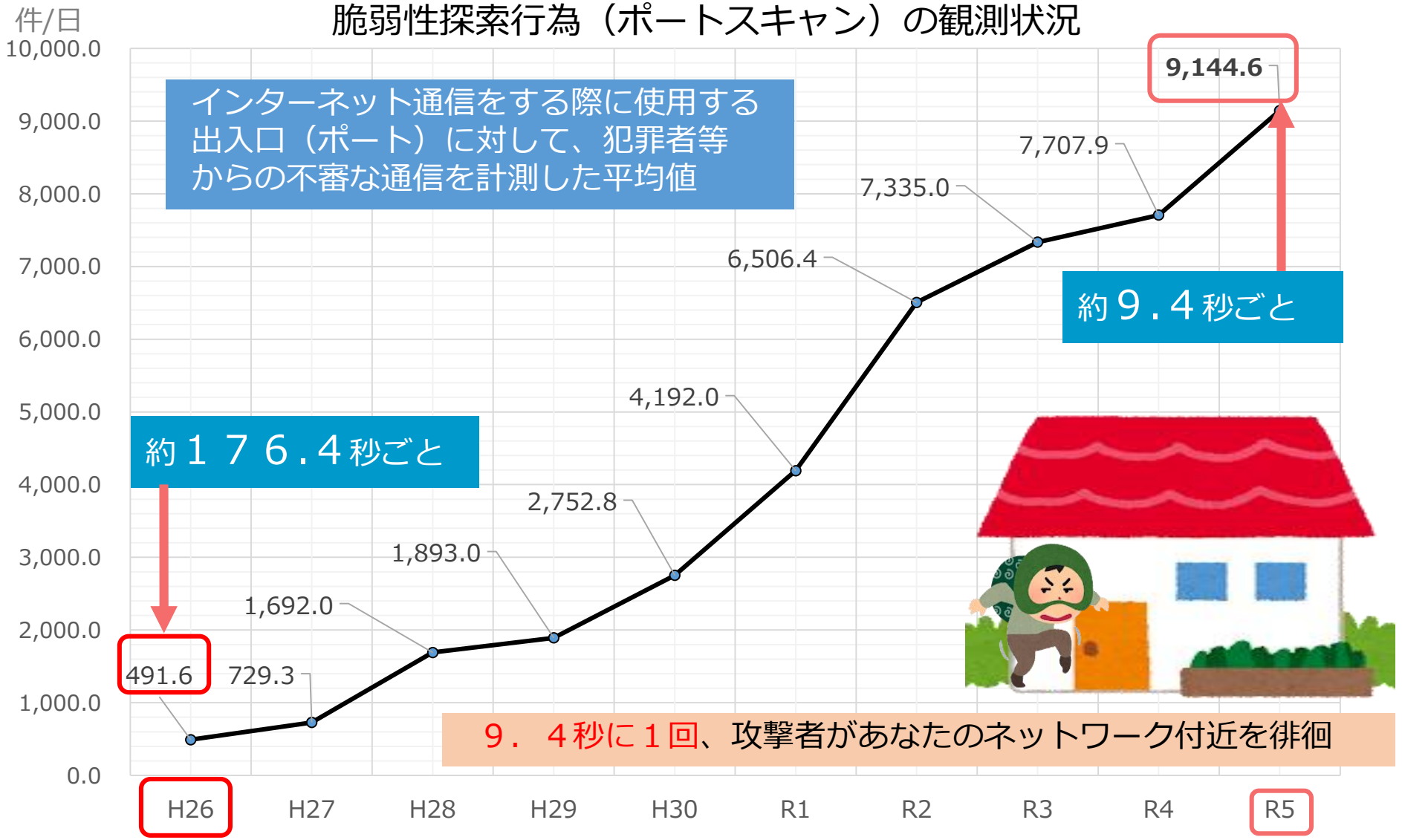
(3)　ランサムウェア攻撃

(4)　社内ネットワークの見える化

2　企業編

(1)　サイバー空間における脅威の情勢

脆弱性探索行為（ポートスキャン）の観測状況

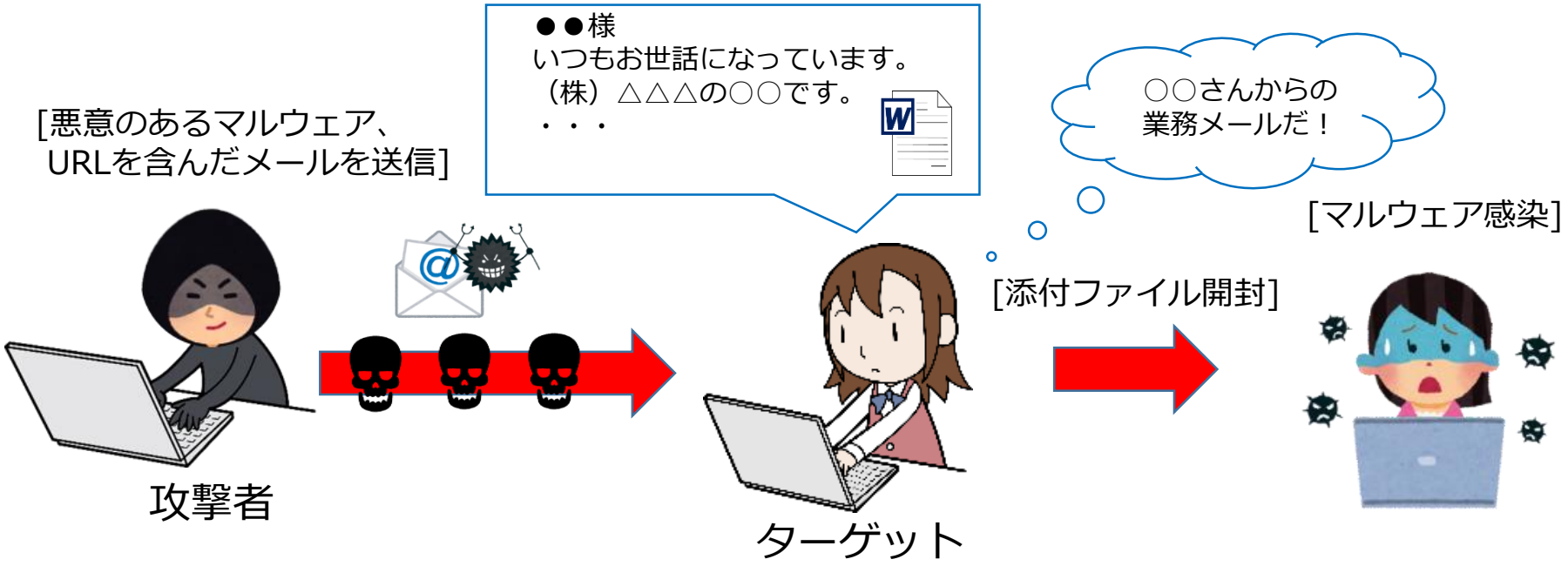


※　警察庁が設置した機器に対するポートスキャン計測回数（1IPアドレスに対して）
出典：警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢について」

（２） メール攻撃

○　特定の企業や個人を狙って、機密情報、知的財産、アカウント情報 (ID・パスワード) などを窃取しようとするメールのこと。(※標的型メール攻撃)

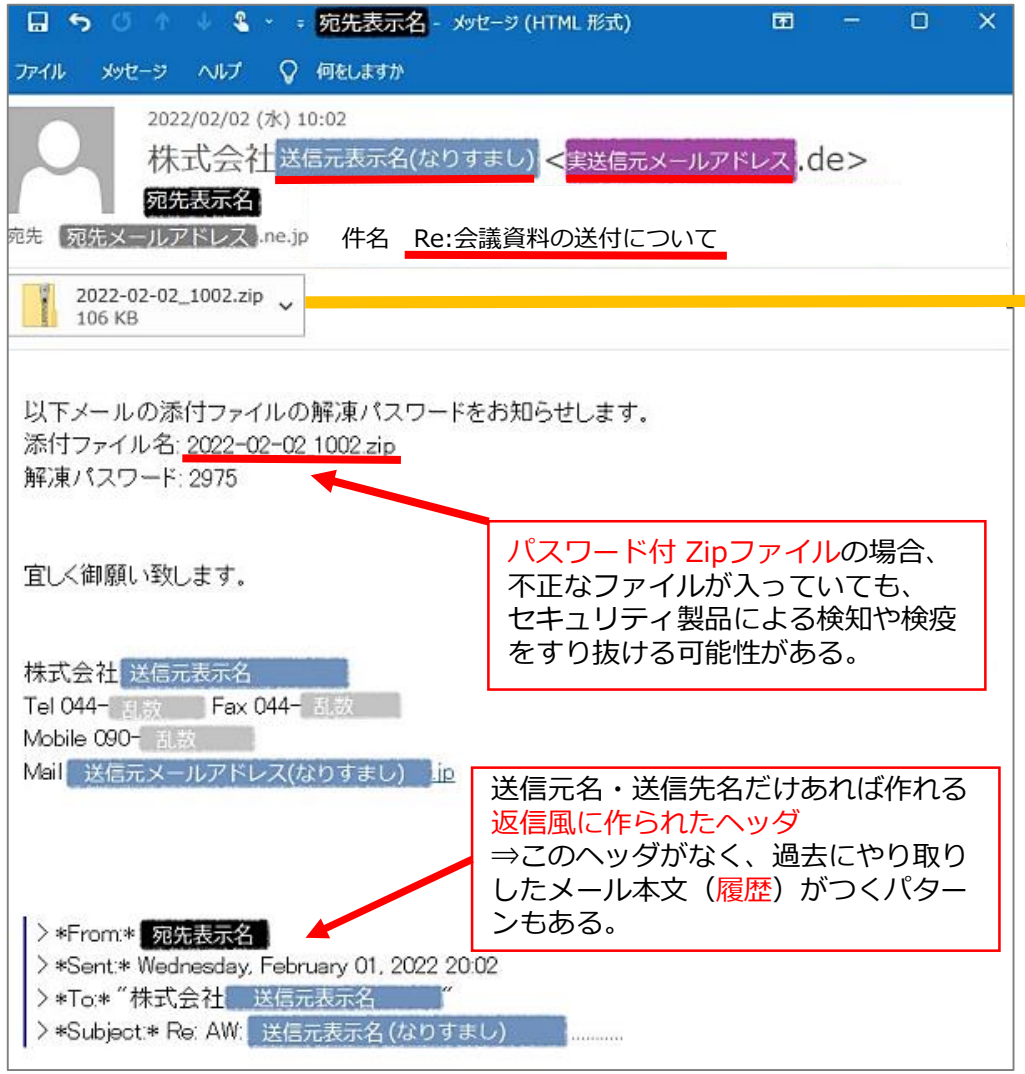
○　受信者が不審を抱かないよう、取引先からの業務連絡、マスコミからの取材申し込み、官庁からの資料配信など、あたかも関連機関を装ってメールを送信してくる。

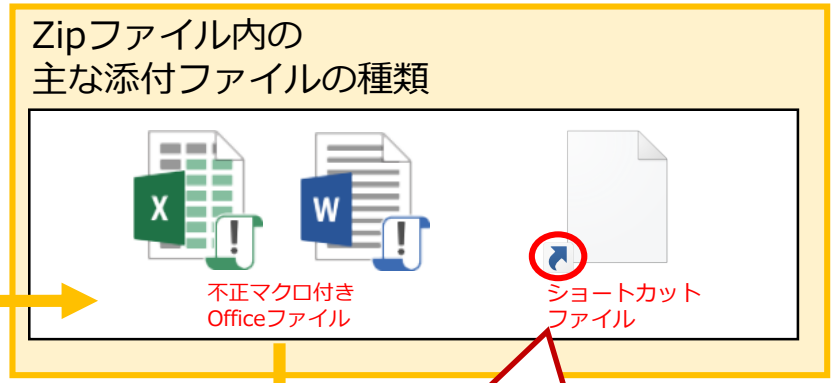


メール攻撃は、受信者が悪意ある添付ファイルを開くことで
マルウェアに感染する手口が多い。

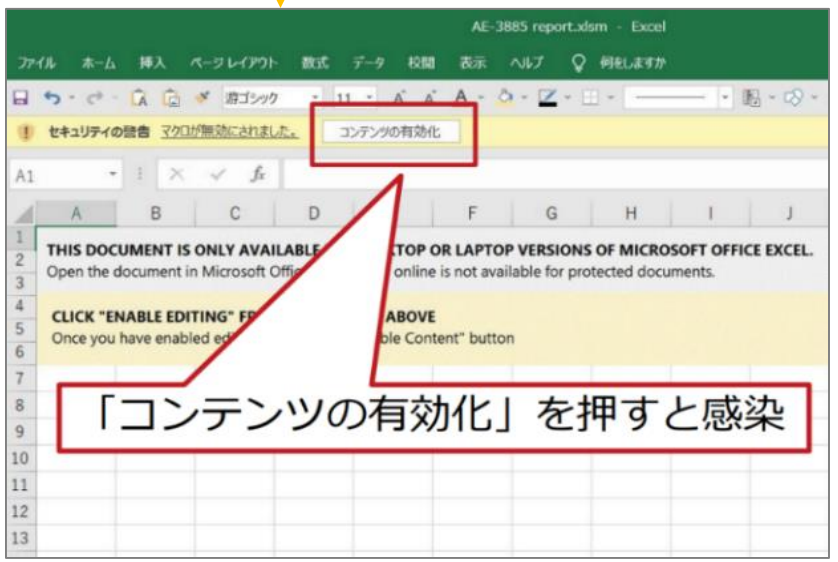
マルウェア感染を狙うメール攻撃の例

特徴① 差出人名に存在する関係者の氏名が使われ、取引先や知人になります。
特徴② 過去のメール本文の内容を引用したり、件名にRE:・FW:を使い返信・転送を装う。
特徴③ マルウェア感染を狙うファイルが添付されていたり、URLが記載されている。





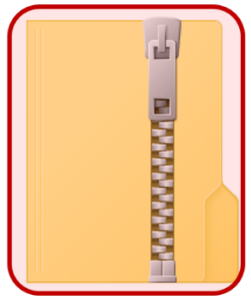
ショートカットファイルは
ダブルクリックだけで感染

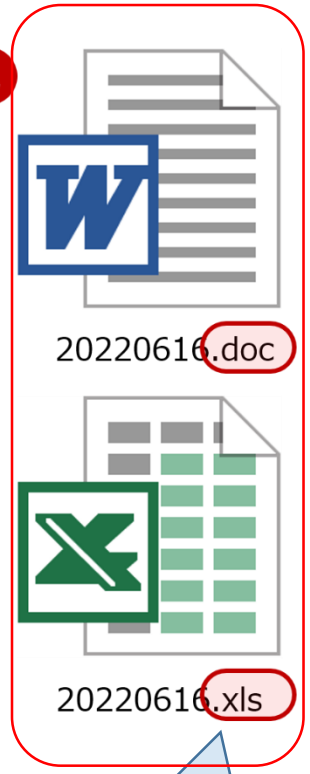


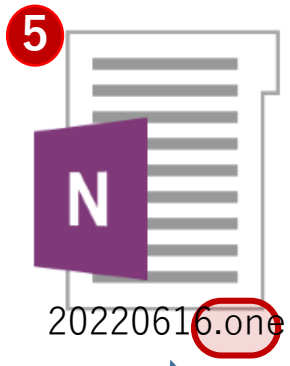
出典：JPCERT/CC「日本中で感染が広がるマルウェアEmotet 」

攻撃メールに添付されているファイルの主なアイコン・拡張子

攻撃者は、ウイルス対策ソフトによる検知を逃れるために、パスワード付きZIPファイルに悪意あるファイルを入れて送信する。







MicrosoftのOneNote形式のファイルで拡張子は「.one」。マクロを使わない手口が新しく発生している。

添付ファイルを開いた時点でEmotetに感染させる手口として、注意が必要な添付ファイル

約２０年前（1997年-2003年）まで使われていた古いファイル形式。ここまで古いと、現在このバージョンを使うのは不自然です。

現行のバージョンでは、マクロが仕込まれているファイル拡張子の末尾に「**m**（マクロのm）」と、アイコンに「**!**」が付いていて、分かりやすい。

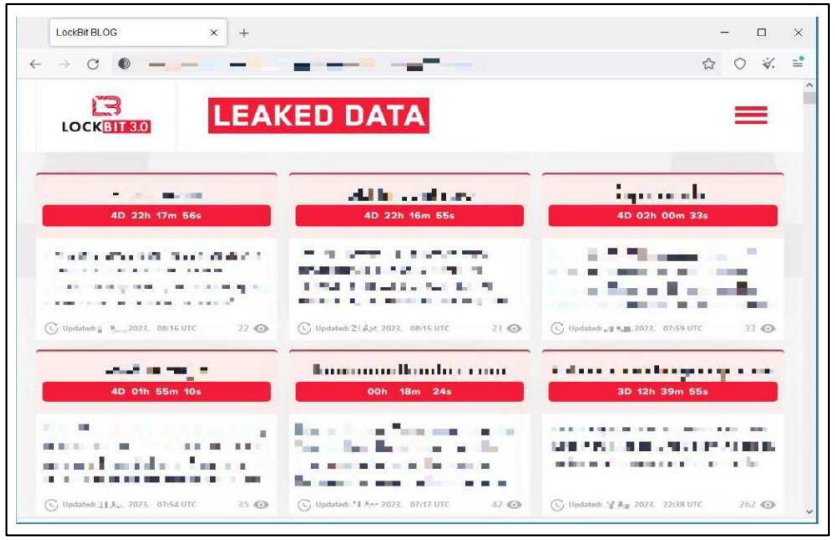
(3)　ランサムウェア攻撃

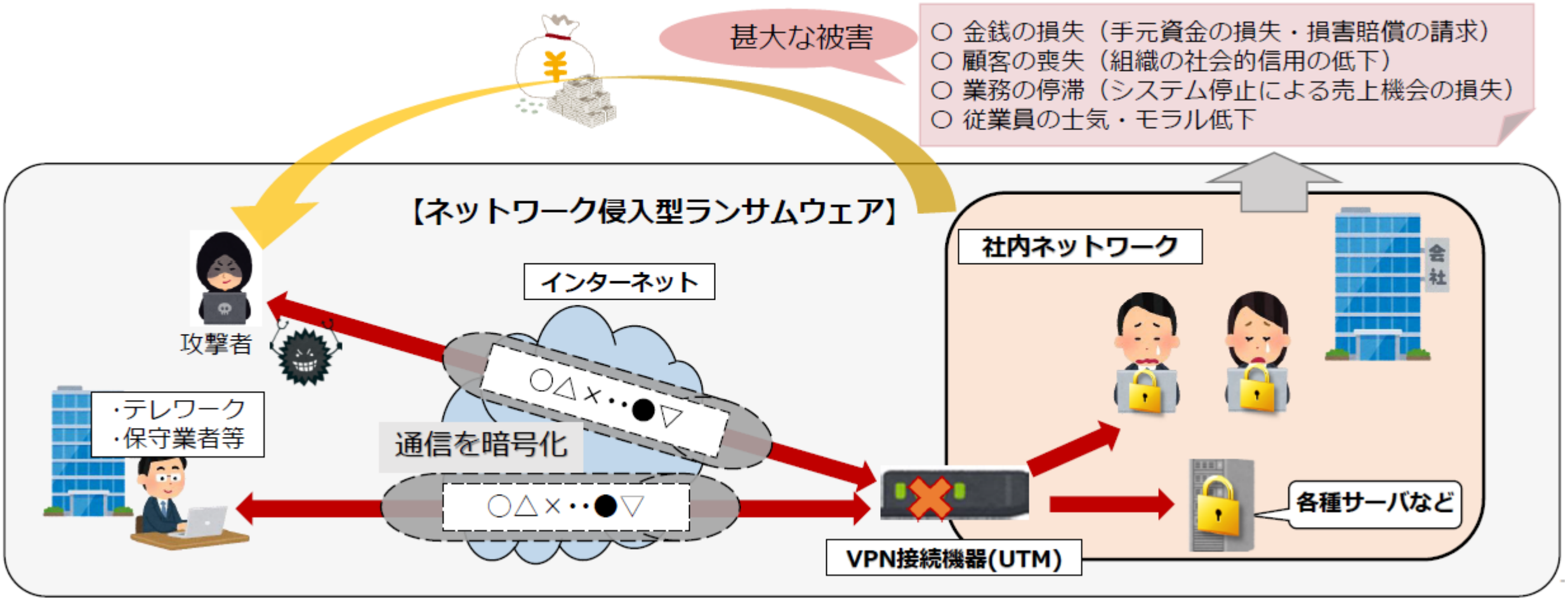
○「ransom」(身代金)と「software」(ソフトウェア)を組み合わせた造語で不正プログラム

○ データやシステムなどを暗号化で使用不能にし、復旧に必要な鍵と引き換えに金銭を要求

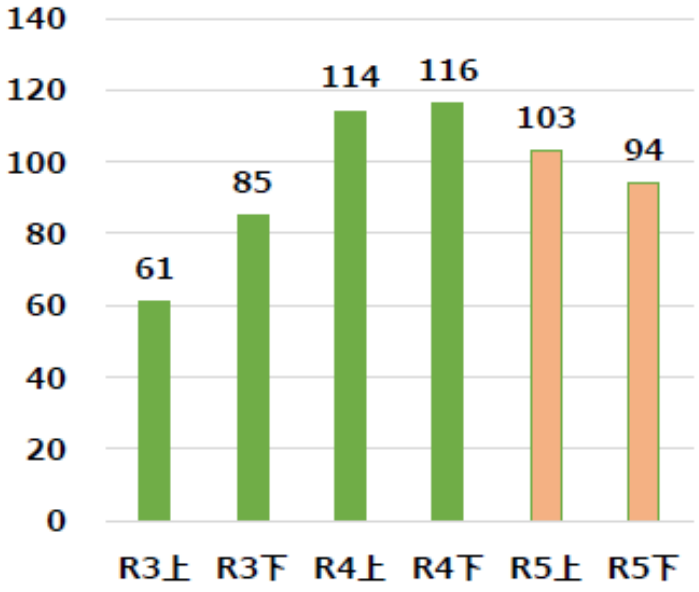
○ 二重恐喝型が主流。さらに、より多くの身代金を要求するため、組織ネットワークの深部まで侵入し、広範囲の暗号化により**事業継続を困難にする攻撃**が多い（**ネットワーク侵入型**）

○ 暗号化せずにデータを盗み脅迫する手口「**ノーウェアランサム**」が増加

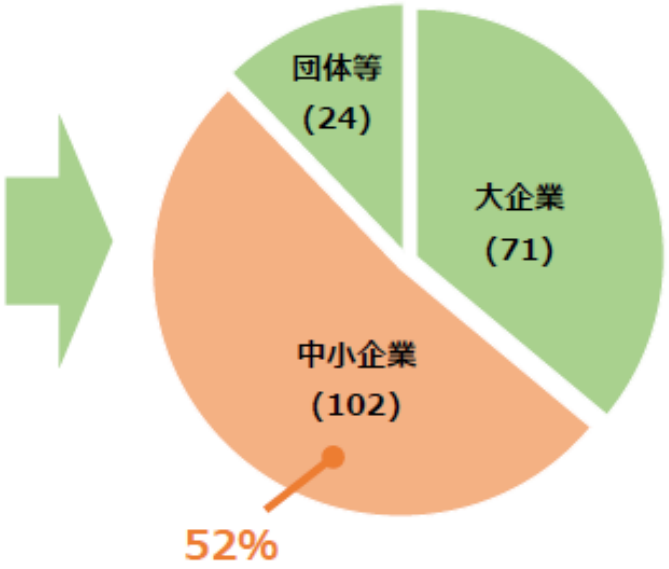



甚大な被害
○ 金銭の損失（手元資金の損失・損害賠償の請求）
○ 顧客の喪失（組織の社会的信用の低下）
○ 業務の停滞（システム停止による売上機会の損失）
○ 従業員の士気・モラル低下
【ネットワーク侵入型ランサムウェア】
攻撃者
インターネット
社内ネットワーク
会社
・テレワーク
・保守業者等
通信を暗号化
○△×・・●▽
○△×・・●▽
VPN接続機器(UTM)
各種サーバなど

警察庁への報告件数

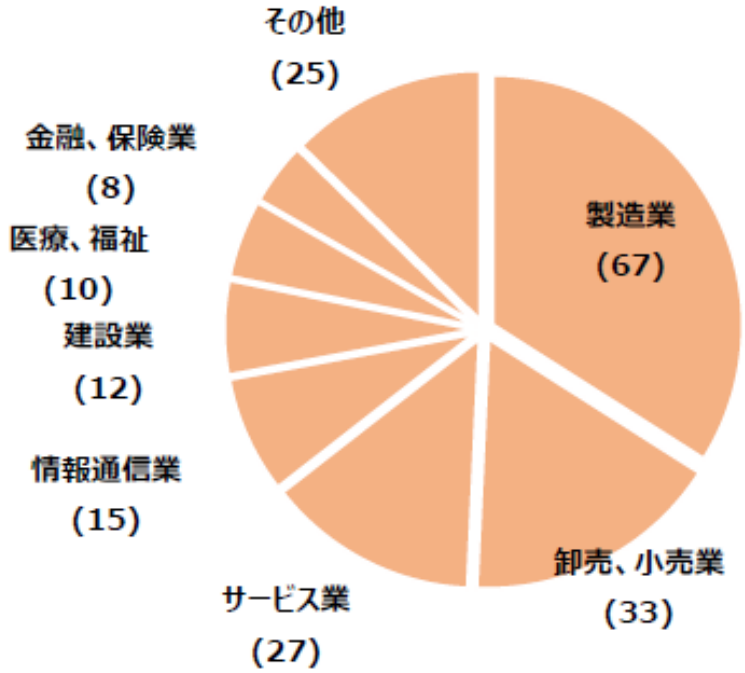


報告内訳（規模別）



<有効回答 197件>

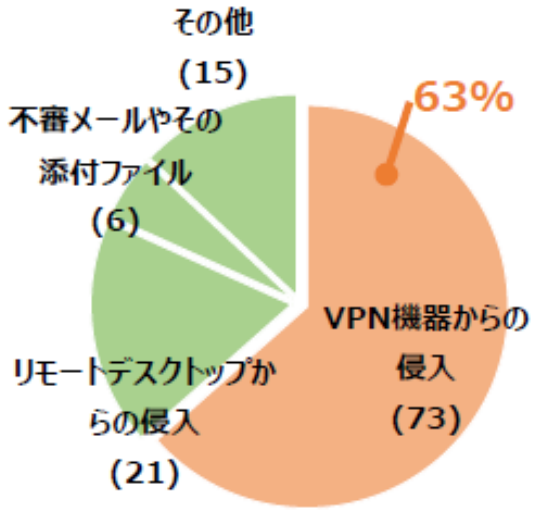
報告内訳（業種別）



<有効回答 197件>

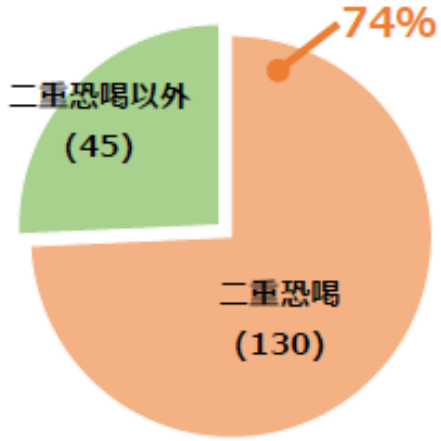
【出典】警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」
（https://www.npa.go.jp/publications/statistics/cybersecurity/index.html）

感染経路



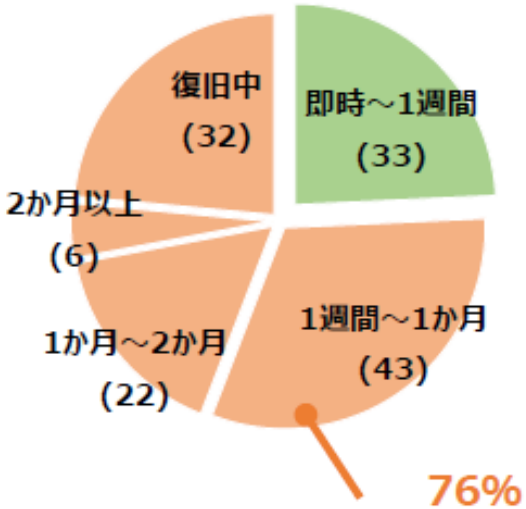
<有効回答 115件>

被害手口



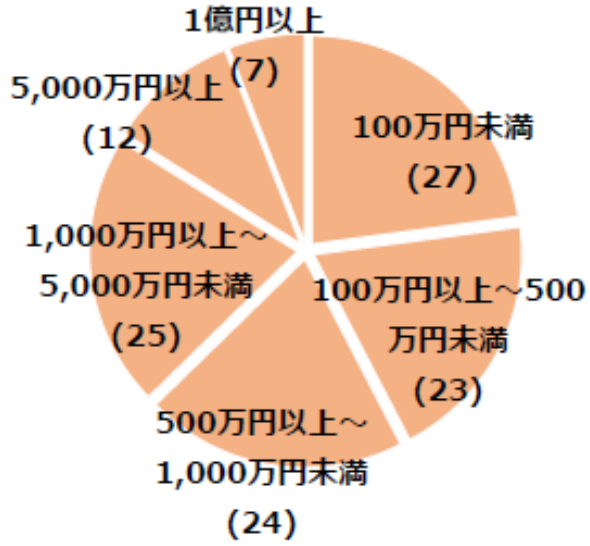
<有効回答 175件>

復旧に要した時間



<有効回答 136件>

調査・復旧費用の総額

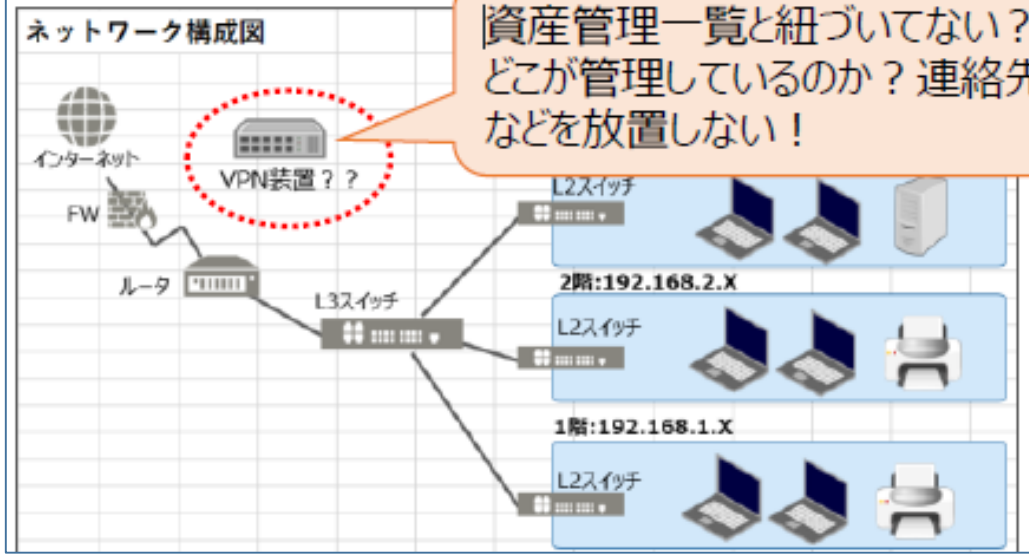


<有効回答 118件>

（4） ネットワークの見える化

資産管理一覧

No	マシン名	機器区分	管理部署名	管理者	設置場所	OS	IP	備考	更新日
1	PC-001	ノートPC	総務部	XXXXXX	2階A	Windows10	192.168.1.1	Office2019、Google Crome	2023/10/20
2	PC-002	ノートPC	総務部	XXXXXX	2階A	Windows10	192.168.1.2	Office2019、Google Crome	2023/10/20
3	PC-003	デスクトップPC	情報システム部	XXXXXX	3階	Windows10	192.168.2.1	Office2019、Google Crome、WinSC	2023/10/20
4	PC-004	ノートPC	営業部	XXXXXX	1階B	Windows10	192.168.3.1	Office2019、Google Crome	2023/10/20
5	SVR-001	サーバ	情報システム部	XXXXXX	サーバルーム	WindowsServer2019	192.168.100.1	IIS、FTP、保守ベンダ連絡先	2023/10/20
6	RT-01	ルータ	情報システム部	XXXXXX	サーバルーム	—	192.168.200.254	XXX社の製品、保守ベンダ連絡先	2023/10/20
7	PT-01	プリンタ	総務部	XXXXXX	2階A	—	192.168.1.200	XXX社の製品、保守ベンダ連絡先	2023/10/20



資産管理一覧と紐づいてない？
どこが管理しているのか？連絡先は？
などを放置しない！

資産の一覧化、ネットワーク構成図をまとめます。また**定期的に目視による現物確認**を推奨します。

資産を管理することで、管理漏れ、脆弱性の軽減、インシデント発生時の対応の効率化を図ることができます。

見える化チェックリスト

□　現物を見ながらネットワーク構成図の作成・確認
□　外部との接続点は物理的に何か所か（ネット回線数）
□　見知らぬ機器が接続されていないか
□　機器の保守業者が設置した機器（保守用VPN等）はないか
□　各機器等はメーカーのサポート期間内か
□　各機器（ファームウェア）等のバージョンは最新か
□　各機器等のメンテナンス（アップデート）は誰が行うのか
□　メンテナンスをベンダーに委託している場合、契約内容に
　にアップデートが入っているか
□　他社のネットワークに接続しているか

WebでPHPをお使い方

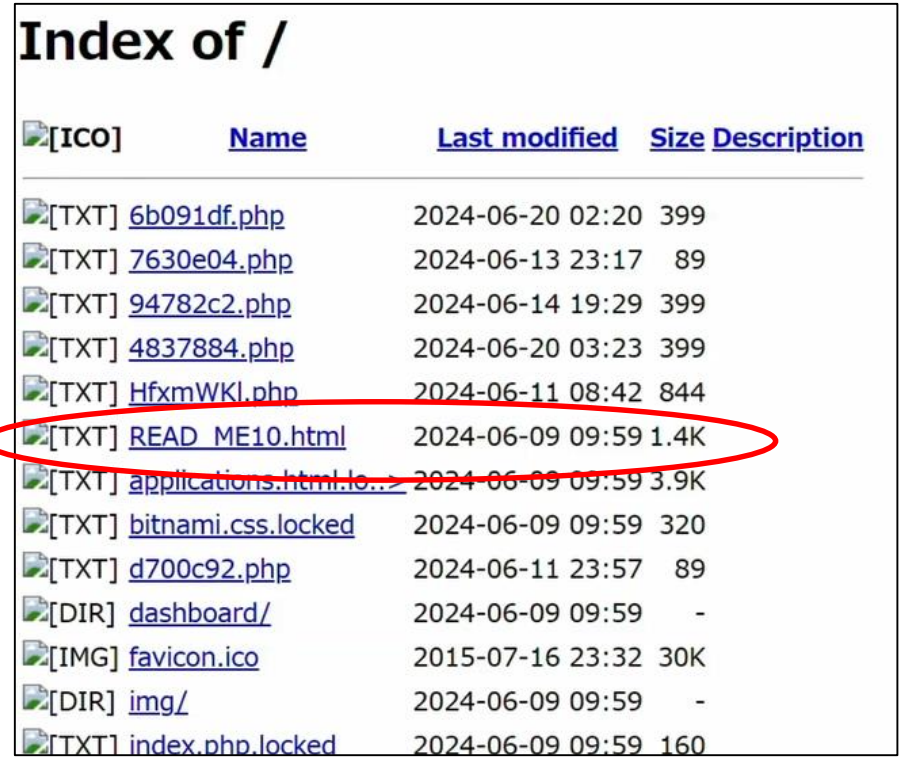
ランサムウェア被害に繋がる緊急性の高い脆弱性（PHP、CVSSv3 9.8 Critical） に関する情報について

CVE-2024-4577（CVSS v 3　9.8Critical）

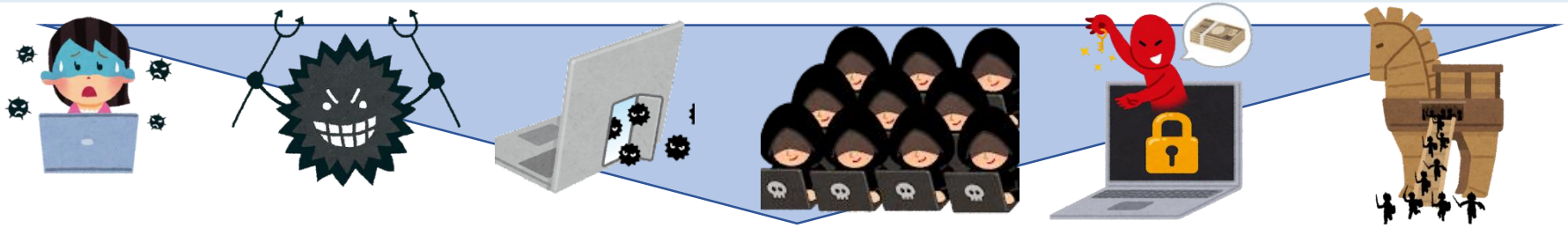
PHP バージョン5.0.0~8.1.29未満
PHP バージョン 8.2.0~8.2.20未満
PHP バージョン 8.3.0~8.3.8未満

6月11日にPHPの脆弱性情報が公開されました。
JVNによりますと、The PHP GroupのPHPにおけるOSコマンドインジェクションの脆弱性が存在します。
既に同脆弱性が悪用された、ランサムウェア （TellYouthePass）被害を複数確認しています。
　JVNのホームページ（JVNDB-2024-003292）を参照し、最新の情報を確認の後、システム機器等のベンダー等とも連携して、速やかにPHPを最新バージョンへの変更の検討をお願いします。
　なお、PHPをアップグレードできない等の場合は、暫定的な回避策の検討をお願いします。

暗号化され、改ざんされたHP



企業の皆様へ　サイバー事案に関する通報・相談・情報提供を！



まずは管轄警察署へ通報相談！

【管轄警察署】

○○警察署

電話による相談はこちらまで！！

【警視庁　サイバー犯罪対策課相談窓口】

電話：03-5805-1731

時間：午前８時３０分から午後５時１５分まで
（平日のみ）

インターネットによる相談はこちらまで！！

令和６年３月２９日より警察庁において、
【サイバー事案に関する通報等のオンライン受付窓口】
を開設し、サイバー事案に関する通報、相談及び情報提供の全国統一窓口を整備・運用中！

企業の皆様からの通報･相談･情報提供がサイバー空間の安全につながります！！