広　報　資　料
令和５年９月21日
警　　察　　庁

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

１　概要

令和５年上半期におけるサイバー空間の脅威の情勢を示す指標、事例を示すとともに、サイバー空間における安全・安心の確保に向けた警察の主な施策等を取りまとめたもの。

２　サイバー空間の脅威情勢

サイバー空間をめぐる脅威の情勢については、次に掲げる状況が見受けられるなど、極めて深刻な情勢が続いている。

⑴　DDoS攻撃による被害とみられるウェブサイトの閲覧障害が複数発生し、一部の事案に関しＳＮＳ上でハクティビストや親ロシア派ハッカー集団からの犯行をほのめかす投稿が確認されている。

⑵　令和５年第１四半期のクレジットカード不正利用被害額は、前年同期と比較して増加している。また、令和５年上半期のインターネットバンキングに係る不正送金被害は、年間の数と比較して、被害件数が過去最多、被害総額も過去最多に迫る状況である。

⑶　ランサムウェア被害の件数が高水準で推移するとともに、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（「ノーウェアランサム」）による被害が、新たに６件確認された。

３　警察における主な取組

⑴　内閣サイバーセキュリティセンター（ＮＩＳＣ）と連名で、重要インフラ事業者等のウェブサイトへのDDoS攻撃に関する注意喚起を行った。

⑵　総務省と連携し、携帯電話事業者に対してＳＩＭスワップの対策強化（携帯電話機販売店における本人確認の強化等）を要請した結果、令和５年上半期におけるＳＩＭスワップによる不正送金被害が激減した。

⑶　サイバー特別捜査隊及び大阪府警察において、インドネシア国家警察と連携し、フィッシングツール「16SHOP」を用いて不正に入手したクレジットカード番号等を使用して通販サイトの商品を窃取するなどしたインドネシア在住の同国人被疑者を特定し、令和５年７月に同国国家警察が同被疑者を逮捕した。

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

令和５年９月21日
警察庁

はじめに

本資料は、令和５年上半期におけるサイバー空間の脅威の情勢を示す指標、事例を示すとともに、サイバー空間における安全・安心の確保に向けた警察の主な施策等を取りまとめたものである。また、資料の取りまとめに当たっては、以下の３部構成で内容を整理している。

第１部「令和５年上半期における脅威情勢の要点」では、令和５年上半期におけるサイバー空間の脅威の情勢やサイバー事案の検挙状況等の要点をまとめている。また、「DDoS攻撃による被害とみられるウェブサイトの閲覧障害」、「クレジットカード不正利用被害額及びインターネットバンキングに係る不正送金被害の増加」、「「ノーウェアランサム」による被害」及び「インターネット上の重要犯罪密接関連情報」については、被害が増加するなど特に注視すべき脅威として捉え、それらの対処等をトピックとして取り上げるとともに、「外国捜査機関と連携したフィッシング事犯の検挙」についても、社会的反響が大きい事件検挙として紹介している。

第２部「脅威の情勢」では、「サイバー攻撃の情勢等」、「フィッシング等に伴う被害の情勢等」、「ランサムウェア被害の情勢等」、「サイバー空間におけるぜい弱性探索行為等の観測状況」及び「インターネット上の違法・有害情報の実態等」といった被害等類型ごとに、その指標や特徴、警察における対処状況等を取りまとめている。

第３部「サイバー事案の検挙状況等」では、サイバー特別捜査隊の活動状況やサイバー事案の検挙状況について、その指標や事例等を取りまとめている。

第１部　令和５年上半期における脅威情勢の要点

１　脅威概況

令和５年上半期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、フィッシング被害等に伴うクレジットカード不正利用被害やインターネットバンキングに係る不正送金被害も急増しているほか、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や、自殺サイトや爆発物・銃砲等の製造方法、殺人や強盗の請負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。

２　主な被害等の類型ごとの情勢及び対策

(1)　サイバー攻撃の情勢等

○　企業・団体等を対象とした不正アクセス等

大手システム事業者、電子部品関連企業等に対する不正アクセスが確認されたほか、特定の事業者等に対する標的型メール攻撃が確認された。

○　DDoS攻撃による被害とみられるウェブサイトの閲覧障害

DDoS攻撃による被害とみられるウェブサイトの閲覧障害が複数発生し、一部の事案については、障害発生と同じ頃、ＳＮＳ上でハクティビストや親ロシア派ハッカー集団からの犯行をほのめかす投稿が確認された。

【トピック１　DDoS攻撃に関する注意喚起】

警察庁では、令和５年５月、内閣サイバーセキュリティセンター（以下「ＮＩＳＣ」という。）と連名で、重要インフラ事業者等のウェブサイトへのDDoS攻撃に関する注意喚起を行った。

【内容】

① 令和４年９月に発生した国内の政府関連や重要インフラ事業者などのウェブサイトに対する一連のDDoS攻撃に関する分析結果を示し、同事案で確認されたDDoS攻撃の主な手口のほか、攻撃元のＩＰアドレスについて99％が海外に割り当てられたものであることなどを特徴として挙げた。

② DDoS攻撃への対策として、海外に割り当てられたＩＰアドレスからの通信の遮断、同一ＩＰアドレスからのアクセス回数の制限等のサーバ設定の見直しのほか、システムの重要度に基づく選別・分離、通報先・連絡先一覧作成等の事案発生時の対策マニュアルの策定など、リスク低減に向けたセキュリティ対策の実施を呼び掛けた。

(2)　フィッシング等に伴う被害の情勢等

○　フィッシングの報告件数の増加

令和５年上半期におけるフィッシングの報告件数は、フィッシング対策協議会によれば右肩上がりで増加しており(前年同期比で17.9%増加)、クレジットカード事業者等を装ったものが多くを占めた。

○　クレジットカード不正利用被害額の増加

一般社団法人日本クレジット協会によれば、令和４年のクレジットカード不正利用被害額は436.7億円であり、統計を取り始めた平成９年以降、過去最悪となった。また、令和５年第１四半期におけるクレジットカード不正利用被害額は、121.4億円で前年同期と比較して増加している（21.3%増加)。

○　インターネットバンキングに係る不正送金事犯による被害の急増

令和５年上半期におけるインターネットバンキングに係る不正送金事犯による被害は、発生件数が2,322件（令和４年の年間発生件数と比較して104.4%増加）であり、年間の被害件数と比較しても過去最多となり、被害総額も約29億9,600万円（令和４年の年間被害総額と比較して97.2%増加）であり、年間の被害額と比較しても過去最多に迫る状況にある。

【トピック２　フィッシング等に関する対策】

１　クレジットカード番号の漏えい等事態の対処に資する連携

令和５年３月、クレジットカード番号を含む保有個人情報の漏えい等事態の未然防止、被害の拡大防止及び類似事態の発生防止等のリスク低減並びに同事態への適切かつ迅速な対応を図るため、個人情報保護委員会と覚書を締結した。

また、令和５年６月、サイバー事案に起因する又はそのおそれのあるクレジットカード番号等の漏えい事案への対策の推進に関し、経済産業省と覚書を締結した。

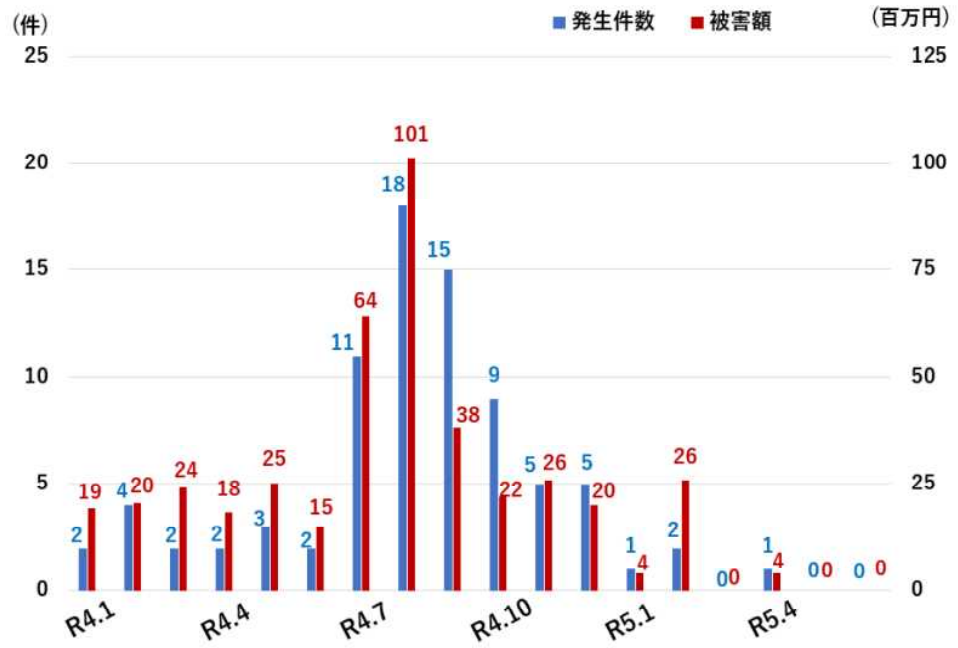
２　ＳＩＭスワップ[*1] 対策

ＳＩＭスワップによるインターネットバンキングに係る不正送金事犯が増加している状況を踏まえ、令和４年９月、総務省と連携し、携帯電話事業者に対して携帯電話機販売店における本人確認の強化を要請し、令和５年２月までに、大手携帯電話事業者において同要請への対応を完了した。その結果、令和５年上半期におけるＳＩＭスワップによる不正送金の被害が激減した。

---

*1　携帯電話機販売店において、偽造した本人確認書類を使い、他人になりすましてＭＮＰ（携帯電話番号ポータビリティ）やＳＩＭカードの再発行の手続を行い、携帯電話番号を乗っ取る手口をいう。

【図表１：SIMスワップに係る不正送金発生状況】



(3)　ランサムウェア被害の情勢等

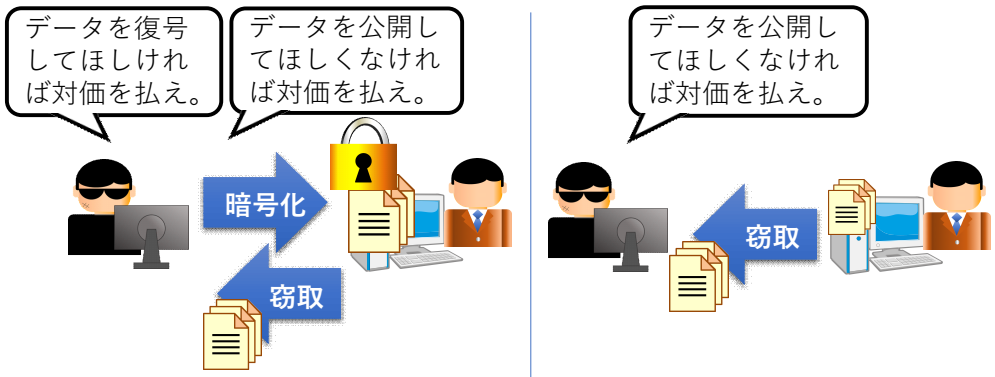
令和５年上半期におけるランサムウェアによる被害件数は103件（前年同期比で9.6%減少）であり、引き続き高い水準で推移している。

手口としては、データの暗号化のみならず、データを窃取した上、企業・団体等に対し「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝（ダブルエクストーション）が多くを占める。

【トピック３　「ノーウェアランサム」】

ランサムウェアによる被害のほか、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（「ノーウェアランサム」）による被害が、新たに６件確認された。

【図表２：攻撃の流れ（左：ランサムウェア攻撃、右：ノーウェアランサム攻撃）】



【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】

【サイバー事案の被害の潜在化防止】

サイバー事案の被害については、社会的評価の悪化の懸念等から警察への通報・相談がためらわれる傾向にあり、いわゆる「被害の潜在化」が課題となっているところ、各界の有識者からなる「サイバー事案の被害の潜在化防止に向けた検討会」を開催し、被害の潜在化防止に関する今後の方策等について報告書を取りまとめ、令和５年４月に公表した。

【医療機関等との連携強化】

医療機関におけるランサムウェア等のサイバー事案に係る被害の未然防止、事案発生時における警察への迅速な通報・相談を促進するため、令和５年４月、公益社団法人日本医師会と覚書を締結した。また、令和５年５月、四病院団体協議会[*2]及び各国公私立大学病院に対してサイバー事案に係る連携強化に関する依頼を行った。

(4) サイバー空間におけるぜい弱性探索行為等の観測状況

警察庁が検知したサイバー空間におけるぜい弱性探索行為等とみられるアクセス件数は、１日・１ＩＰアドレス当たり8,219.0件（前年同期比で5.4%増加）と、増加の一途をたどっており、海外を送信元とするアクセスが大部分を占めている。

(5) インターネット上の違法・有害情報の実態等

インターネット上において、違法情報や、爆発物・銃砲等の製造方法等の重要犯罪密接関連情報[*3]が容易に入手できる状況にある。

【トピック４　重要犯罪密接関連情報に関する対策の強化】

令和５年２月、警察庁で事業委託しているインターネット・ホットラインセンター（以下「ＩＨＣ」という。）及びサイバーパトロールセンター（以下「ＣＰＣ」という。）における取扱情報の範囲に、爆発物・銃砲等の製造に関する情報等をはじめとした重要犯罪密接関連情報を追加した。

また、ＩＨＣ及びＣＰＣの取扱情報の範囲に犯罪実行者募集情報[*4]

---

*2　全国組織の病院団体の連合体であり、一般社団法人日本病院会、公益社団法人日本精神科病院協会、一般社団法人日本医療法人協会及び公益社団法人全日本病院協会で構成されている。

*3　インターネット上に流通することによって、個人の生命・身体に危害を加えるおそれが高い重要犯罪（殺人、強盗、不同意性交等、不同意わいせつ、放火、略取誘拐及び人身売買をいう。）又は重要犯罪に発展する危険性がある犯罪と密接に関連しているものをいう。

*4　著しく高額な報酬の支払いを示唆して行う犯罪の実行者の募集を直接的かつ明示的に誘引等する情報

を追加するための取組を推進するとともに、ＣＰＣにおける情報収集の高度化を図るため、ＡＩを活用した情報収集システムの導入を推進している。

○　重要犯罪密接関連情報の取扱状況

令和５年２月15日から６月30日までの間、ＩＨＣの運用ガイドラインに基づき、重要犯罪密接関連情報と判断し分析した情報は172件であり、148件（削除依頼を行う前に削除されたものを除く。）についてサイト管理者等に削除依頼を行った結果、77件（52.0％）が削除に至った。

【図表３：重要犯罪密接関連情報の削除依頼件数等】

類型	分析件数	削除依頼件数	削除完了件数
拳銃等の譲渡等	3	3	2
爆発物・銃砲等の製造	6	5	5
殺人・強盗等の勧誘	157	136	68
臓器売買	5	4	2
人身売買	0	0	0
硫化水素ガスの製造	1	0	0
ストーカー行為等	0	0	0
合計	**172**	**148**	**77**

※　削除完了件数は、令和５年７月末に確認した状況を計上

３　サイバー事案[*5]の検挙状況

(1)　サイバー事案の検挙件数

令和５年上半期におけるサイバー事案の検挙件数は、1,181件であった。

(2)　不正アクセス禁止法違反[*6]の検挙件数及び特徴

令和５年上半期における不正アクセス禁止法違反の検挙件数は、188件（前

---

*5　サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。

*6　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）違反（「不正アクセス行為・他人の識別符号を不正に取得する行為・不正アクセス行為を助長する行為・他人の識別符号を不正に保管する行為・識別符号の入力を不正に要求する行為」の５つの違反行為が定められている。）

年同期比で19.3%減少）であり、そのうち157件が識別符号窃用型[*7]で全体の83.5%を占める。

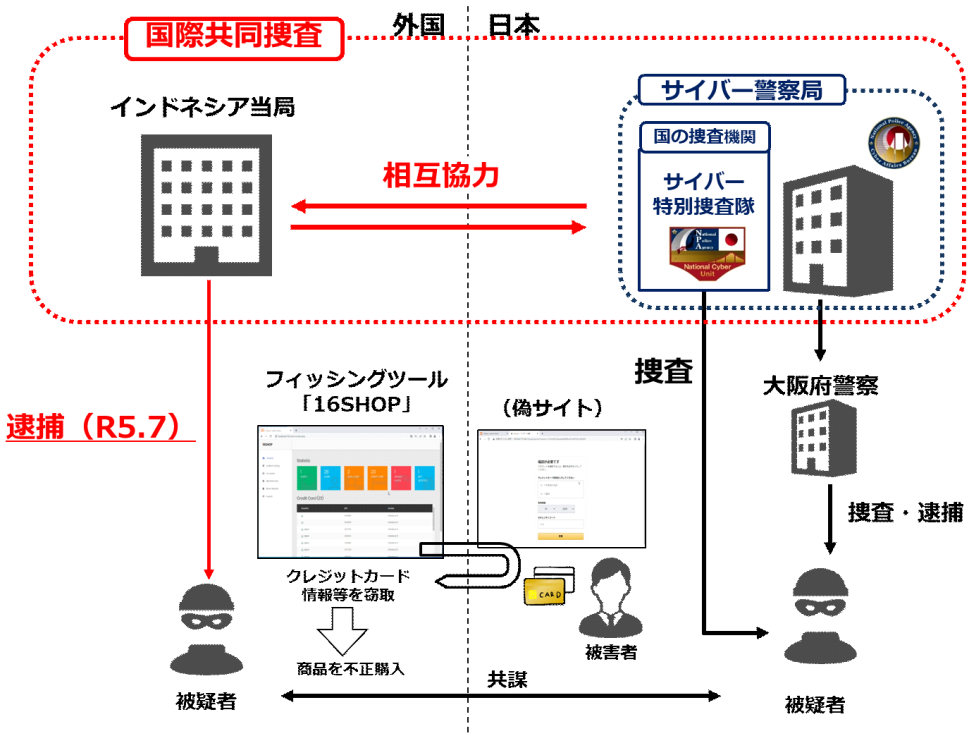
(3)　コンピュータ・電磁的記録対象犯罪[*8]の検挙件数及び特徴

令和５年上半期におけるコンピュータ・電磁的記録対象犯罪の検挙件数は、403件（前年同期比で15.8%増加）であり、そのうち380件が電子計算機使用詐欺で全体の94.3%を占める。

【トピック５　外国捜査機関と連携したフィッシング事犯の検挙】

サイバー特別捜査隊及び大阪府警察は、インドネシア国家警察と連携し、フィッシングツール「16SHOP」を用いて不正に入手したクレジットカード番号等を使用して通販サイトの商品を窃取するなどしたインドネシア在住の同国人被疑者を特定し、令和５年７月９日に同国国家警察が同被疑者を逮捕した。本件は、日本警察の捜査がフィッシング事犯に関する国外被疑者の検挙に結びついた初めての事案となった。

【図表４：事案の概要】



---

*7　不正アクセス行為は、他人の識別符号を無断で入力する「識別符号窃用型」と、アクセス制御機能による特定利用の制限を免れる情報（識別符号を除く）又は指令を入力する「セキュリティ・ホール攻撃型」に分類することができる。

*8　刑法（明治40年法律第45号）に規定されているコンピュータ又は電磁的記録を対象とした犯罪

第２部　脅威の情勢

１　サイバー攻撃の情勢等

(1)　サイバー攻撃による被害の事例

○　大手システム事業者に対する不正アクセス

令和４年12月、大手システム事業者は、同社が提供するインターネットサービスを構成する一部のネットワーク機器に関して、外部に不正な通信が行われていたことを確認したと発表した。また、令和５年２月、同社は本件調査結果を公表し、不正通信が行われた時間帯に当該ネットワーク機器を通過していた通信情報が、技術的に外部から窃取可能な状態になっていたことが判明したと発表した。

○　電子部品関連企業に対する不正アクセス

令和５年４月、電子部品関連企業は、同社ネットワークが不正アクセスを受け、ファイルサーバのデータの一部が不正に読み出された可能性があると発表した。令和５年６月、同社は、本件が海外子会社を経由して複数のファイルサーバに不正アクセスされたものであることを発表した。

(2)　標的型メール攻撃の傾向・事例

ア　傾向

令和５年上半期において、警察で把握した標的型メール攻撃の事例では、様々な手口が確認された。具体的には、メールの添付ファイルからフィッシングサイトへ誘導しようとするものや、実在する人物を装ってメールを送り、複数回メールのやり取りを行い相手を信用させた後、相手の興味・関心を惹くファイル名を付けた不正プログラム（マルウェア）のファイルを送り、実行させるものなどが確認されている。

イ　事例

サイバーインテリジェンス情報共有ネットワーク（第２部１(4)参照）等を通じて事業者等から情報提供を受けた標的型メール攻撃の事例は以下のとおりである。

○　部品加工メーカーに対する攻撃

メール本文のリンクからファイルをダウンロードさせ、同ファイルを開くことで不正プログラムに感染させる標的型メールが部品加工メーカーに送信された。

○　実在の組織になりすました攻撃

実在の組織になりすましてメールを送信し、添付ファイルを開くことで、実在するウェブサイトのログイン画面を装いＩＤ・パスワードの入力を求めるフィッシングサイトに誘導する標的型メールが確認された。

○　実在する人物になりすました攻撃

知人になりすまして「論考を作成したので興味があれば送る」旨のメールを送りつけ、何度かやり取りした後、不正プログラムが仕掛けられた添付ファイルを送信する標的型メールが確認された。

(3)　DDoS攻撃による被害とみられるウェブサイトの閲覧障害の事例

令和５年上半期において、DDoS攻撃による被害とみられるウェブサイトの閲覧障害が複数発生した。主な事例は、以下のとおりである。

○　２月から３月にかけて、政府機関や重要インフラ事業者等を含む複数の組織・団体等のウェブサイトにおいて閲覧障害が断続的に発生。同じ頃、ＳＮＳ上に親ロシア派ハッカー集団からの犯行をほのめかす投稿が確認された。

○　３月から６月にかけて、ＤＮＳ権威サーバを狙ったランダムサブドメイン攻撃[*9]によるとみられるウェブサイトの閲覧障害が断続的に発生。ＤＮＳ権威サーバがサービス停止となることで、当該ＤＮＳ権威サーバに登録されているドメイン名のウェブサイトが閲覧不能となるところ、ＤＮＳ権威サーバによっては多数のドメイン名が登録されているため、多数のウェブサイトに閲覧障害が発生したものも確認された。

○　５月、政府機関が運営するウェブサイトに閲覧障害が発生し、同じ頃、ＳＮＳ上にハクティビストと思料されるアカウントからの犯行をほのめかす投稿が確認された。

(4)　対処状況

○　家庭用ルーターの不正利用に関する注意喚起

捜査の過程で、家庭用ルーターがサイバー攻撃に悪用されており、従来の対策のみでは対応できないことが判明したことから、令和５年３月、警察庁及び警視庁において、複数の関係メーカーと協力し、注意喚起を行った。

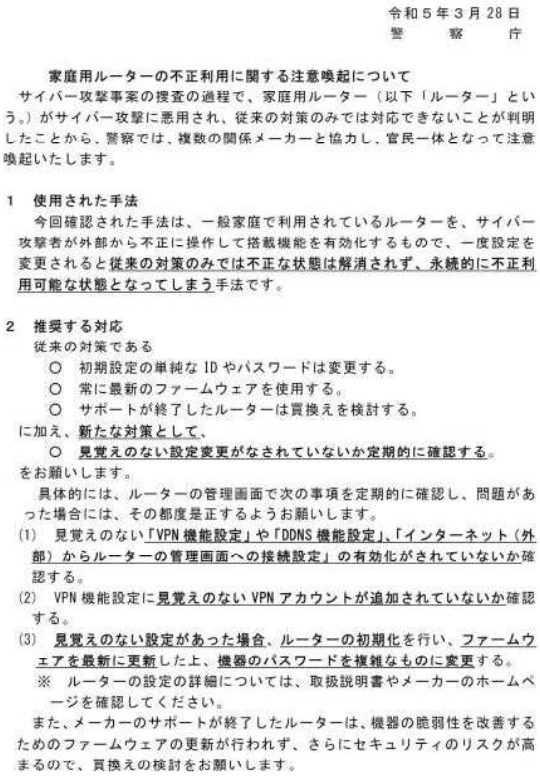
同注意喚起では、各家庭で所有するルーターについて、初期設定のＩＤ・パスワードの変更や最新のソフトウェアへのアップデートなどのほか、見覚えのない設定変更がなされていないか確認するよう呼び掛けた。

---

*9　攻撃対象となる組織のドメインを管理するＤＮＳサーバに対して、ランダムに生成したサブドメイン（※）の問合せを大量に行い、ＤＮＳサーバの機能停止を狙う攻撃手法。

※　サブドメインとは、ドメインを分割して管理・運用するため、ドメイン名の先頭に文字列及び区切り文字（ピリオド）を付加したもの。（「abc.example.co.jp」など）

【図表５：注意喚起】



令和５年３月28日
警　　察　　庁

家庭用ルーターの不正利用に関する注意喚起について

サイバー攻撃事案の捜査の過程で、家庭用ルーター（以下「ルーター」という。）がサイバー攻撃に悪用され、従来の対策のみでは対応できないことが判明したことから、警察では、複数の関係メーカーと協力し、官民一体となって注意喚起いたします。

1　使用された手法

今回確認された手法は、一般家庭で利用されているルーターを、サイバー攻撃者が外部から不正に操作して搭載機能を有効化するもので、一度設定を変更されると従来の対策のみでは不正な状態は解消されず、永続的に不正利用可能な状態となってしまう手法です。

2　推奨する対応

従来の対策である
○　初期設定の単純なIDやパスワードは変更する。
○　常に最新のファームウェアを使用する。
○　サポートが終了したルーターは買換えを検討する。
に加え、新たな対策として、
○　見覚えのない設定変更がなされていないか定期的に確認する。
をお願いします。

具体的には、ルーターの管理画面で次の事項を定期的に確認し、問題があった場合には、その都度是正するようお願いします。

(1)　見覚えのない「VPN機能設定」や「DDNS機能設定」、「インターネット（外部）からルーターの管理画面への接続設定」の有効化がされていないか確認する。
(2)　VPN機能設定に見覚えのないVPNアカウントが追加されていないか確認する。
(3)　見覚えのない設定があった場合、ルーターの初期化を行い、ファームウェアを最新に更新した上、機器のパスワードを複雑なものに変更する。
※　ルーターの設定の詳細については、取扱説明書やメーカーのホームページを確認してください。

また、メーカーのサポートが終了したルーターは、機器の脆弱性を改善するためのファームウェアの更新が行われず、さらにセキュリティのリスクが高まるので、買換えの検討をお願いします。

○　重要インフラ事業者等に対する注意喚起

重要インフラ事業者等に対してサイバー攻撃に関する注意喚起を継続的に実施している。令和５年上半期には特定の情報通信機器のぜい弱性に関して全国に注意喚起を実施したほか、海外の関係機関・団体等からサイバー攻撃等に関する情報を入手した場合は個別に注意喚起を行うなど、サイバー攻撃による重要インフラ事業者等の被害の未然防止・拡大防止を図った。

○　Ｃ２サーバのテイクダウン

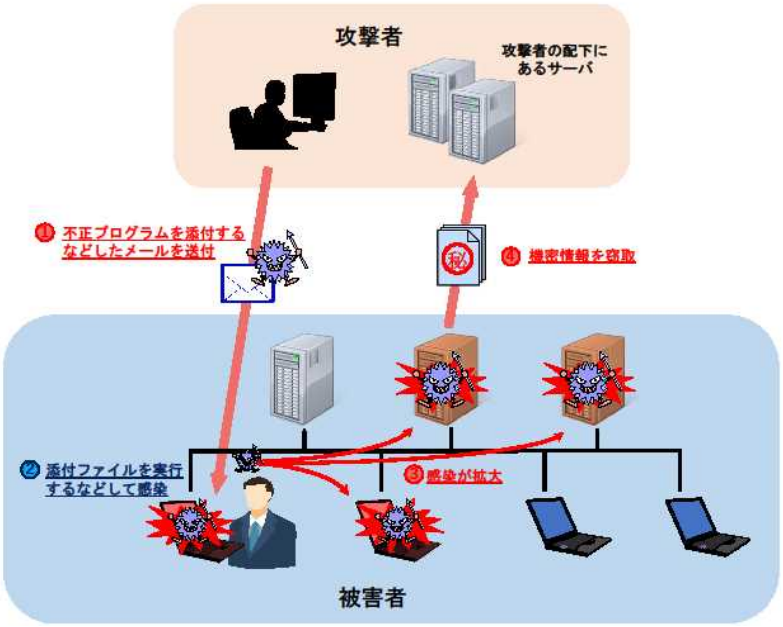
サイバー攻撃事案で使用された不正プログラムの解析等を通じてＣ２サーバとして機能している国内のサーバを把握し、Ｃ２サーバとしての不正な機能を停止（テイクダウン）するよう、サーバを管理する事業者等に依頼するなどの対策を継続的に実施した。

○　サイバーインテリジェンス情報共有ネットワーク

警察及び先端技術を有するなど情報窃取の標的となるおそれのある全国約8,600の事業者等（令和５年６月末現在）から構成されるサイバーインテリジェンス情報共有ネットワーク（ＣＣＩネットワーク）の枠組みを通じて、事業者等から提供される標的型メール攻撃をはじめとする情報窃取を企図したとみられるサイバー攻撃に関する各種情報を集約する

とともに、これらの情報を総合的に分析して、事業者等に対し、分析結果に基づく注意喚起を行っている。

【図表６：標的型メール攻撃による情報窃取の例】



○　共同対処訓練の実施

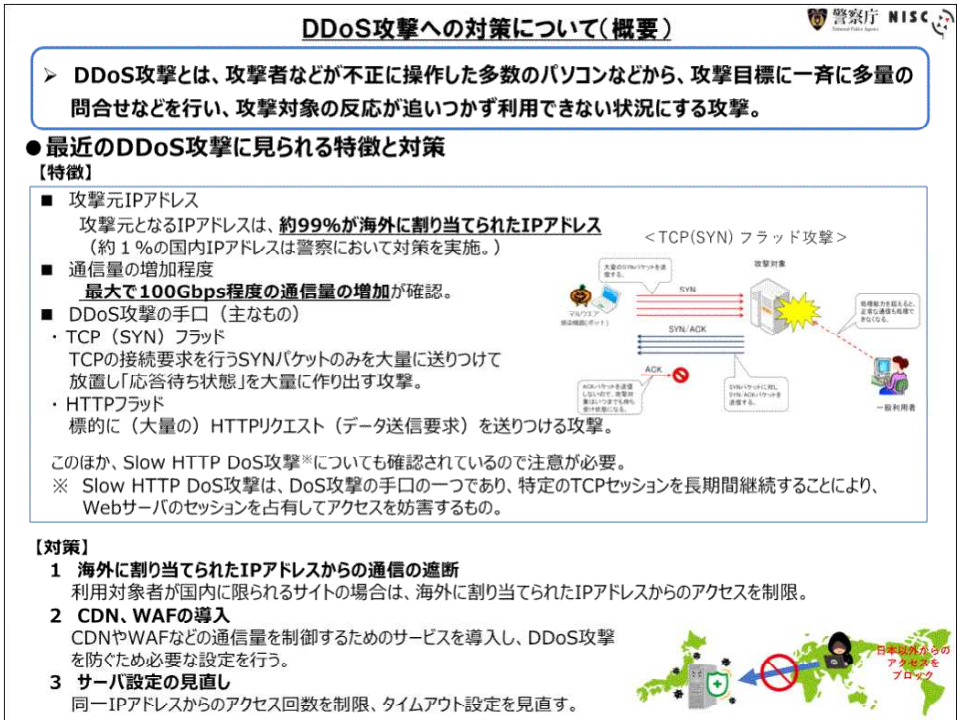
サイバー攻撃事案の発生を想定した重要インフラ事業者等との共同対処訓練を継続的に実施している。令和５年上半期においても、自治体、電力事業者、金融機関等の幅広い分野の事業者等を対象に、標的型メールを題材とした訓練や警察との連携を確認するための現場臨場訓練等の実践的な共同対処訓練を295回実施し、警察との連携強化や各事業者等のサイバー攻撃に対する対処能力の向上を図った。

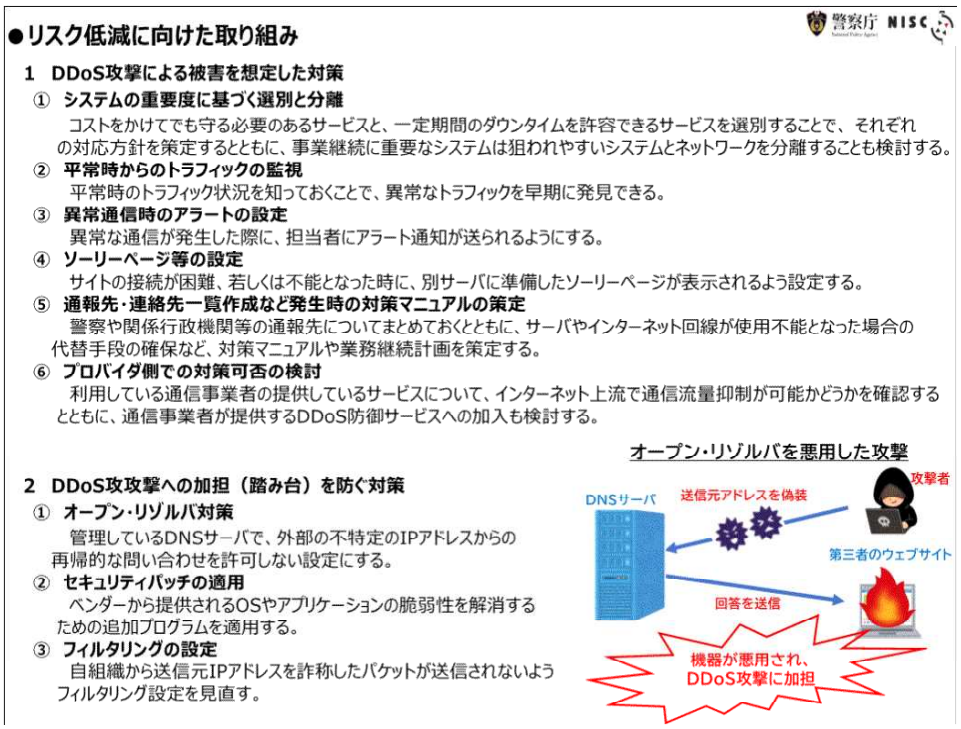
○　DDoS攻撃に関する注意喚起

令和５年５月、ＮＩＳＣと連名で、重要インフラ事業者等のウェブサイトへのDDoS攻撃に関する注意喚起を行った。

同注意喚起では、令和４年９月に発生した国内の政府関連や重要インフラ事業者などのウェブサイトに対する一連のDDoS攻撃に関する分析結果を示しており、同事案で確認されたDDoS攻撃の主な手口のほか、攻撃元のＩＰアドレスについて99%が海外に割り当てられたものであることなどを特徴として挙げている。また、こうした分析結果も踏まえ、DDoS攻撃への対策として、海外に割り当てられたＩＰアドレスからの通信の遮断、同一ＩＰアドレスからのアクセス回数の制限等のサーバ設定の見直しのほか、システムの重要度に基づく選別・分離、通報先・連絡先一覧作成等の事案発生時の対策マニュアルの策定など、リスク低減に向けたセキュリティ対策の実施を呼び掛けた。

【図表７：注意喚起（概要）】





(5)　Ｇ７広島サミット等におけるサイバー攻撃対策

Ｇ７広島サミット及びその関係行事の妨害や情報窃取等を目的としたサイバー攻撃の発生が懸念されていたところ、サイバー攻撃が世界規模で頻発する厳しい情勢を踏まえ、警察庁及び各都道府県警察では、Ｇ７広島サミット等開催に伴うサイバー攻撃対策に万全を期すため、開催地を管轄す

る広島県警察を中心に、推進態勢の確立、情報収集・分析の強化、管理者対策の徹底、事案対処態勢の充実等の各種取組を推進した。

具体的な取組としては、Ｇ７広島サミット等の主催府省庁、関係施設の管理者、電力、空港等の重要インフラ事業者等に対するサイバーセキュリティ対策状況の確認及び助言、関係施設の事業者、重要インフラ事業者等とのサイバー攻撃の発生を想定した共同対処訓練、関係事業者が管理するサーバやネットワーク機器等に対するぜい弱性試験、関連ウェブサイトの改ざんや閲覧障害を早期に検知するための観測強化等のサイバー攻撃対策を実施した。

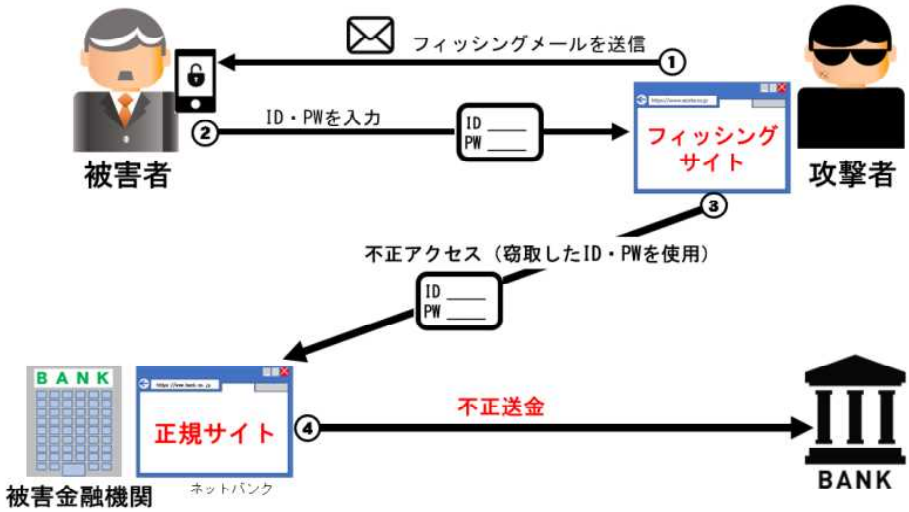
こうした取組の結果、Ｇ７広島サミット期間中、広島市ウェブサイトにおいてDDoS攻撃によるものとみられる閲覧障害が発生するなど、Ｇ７広島サミット等開催の機会を狙ったサイバー攻撃事案が発生したが、Ｇ７広島サミット等の進行に影響を及ぼすようなサイバー攻撃の発生はなかった。

２　フィッシング等に伴う被害の情勢等

(1)　フィッシングの状況

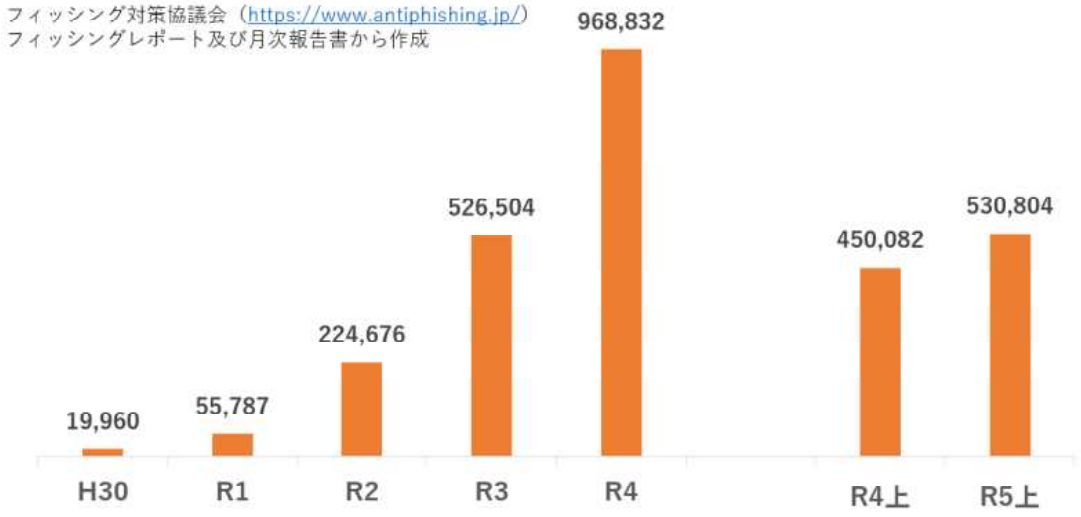
フィッシングとは、実在する企業･団体等や官公庁を装うなどしたメール又はショートメッセージサービス（以下「ＳＭＳ」という。）を送り、その企業等のウェブサイトに見せかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するよう誘導し、当該フィッシングサイトでアカウント情報やクレジットカード番号等を不正に入手する手口であり、インターネットバンキングに係る不正送金やクレジットカードの不正利用に使われている。

【図表８：不正送金の概要】



令和５年上半期のフィッシング報告件数は、フィッシング対策協議会によれば、53万804件（前年同期比で８万722件増加）で、右肩上がりで増加となった。また、フィッシングでかたられた企業等は、クレジットカード事業者、ＥＣ事業者を装ったものが多くを占めた。

【図表９：フィッシング報告件数の推移】



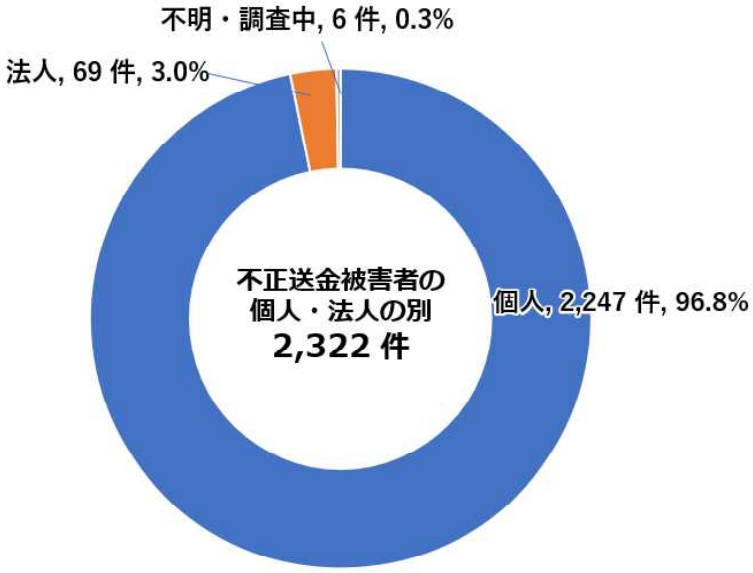
(2)　インターネットバンキングに係る不正送金事犯におけるフィッシングの実態

令和５年上半期におけるインターネットバンキングに係る不正送金事犯による被害は、２月以降被害が多発しており、発生件数は過去最多の2,322件、被害総額は約29億9,600万円である。

【図表10：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及び被害額の推移】

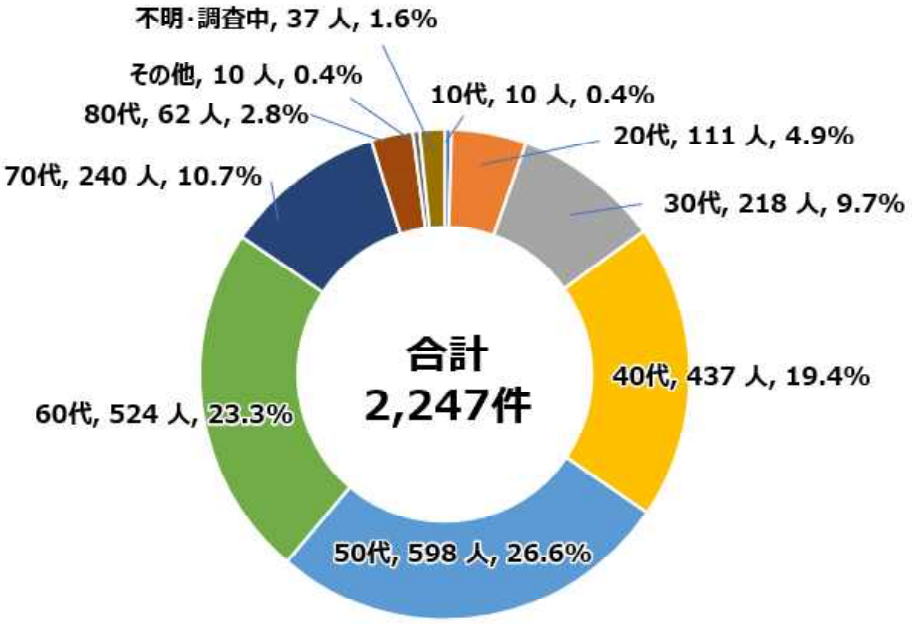
また、被害者の大部分は個人であり（96.8%）、そのうち40代から60代の被害者が約７割を占めている。

【図表11：インターネットバンキングに係る不正送金被害者の個人・法人の別】



注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

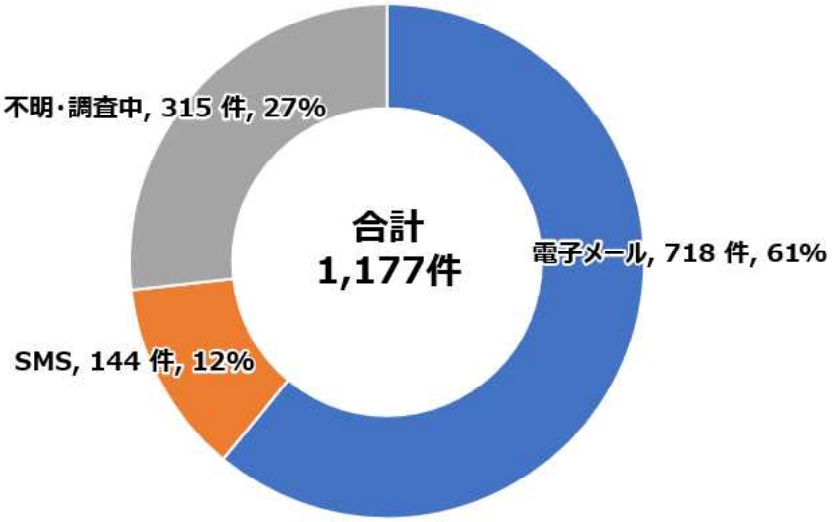
【図表12：個人のインターネットバンキングに係る不正送金被害者の年齢別割合】



注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

さらに、フィッシングの内訳を見ると、電子メールによる誘導が61%、ＳＭＳによる誘導が12%である。

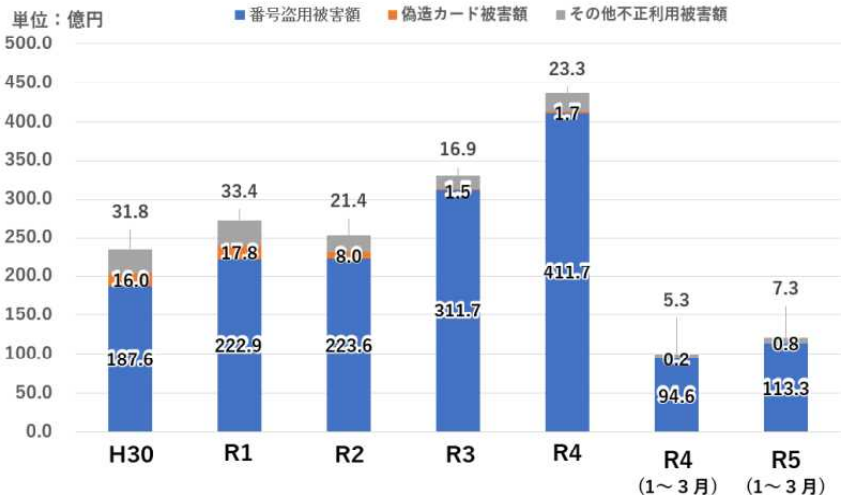
【図表13：フィッシングサイトへ誘導する手口別割合】



(3)　クレジットカード不正利用の情勢

キャッシュレス決済等の普及に伴い、クレジットカード決済市場の規模が増加する一方、クレジットカード不正利用被害も多く発生している。一般社団法人日本クレジット協会（以下「日本クレジット協会」という。）で実施している国内発行クレジットカードの不正利用被害の実態調査によると、クレジットカード不正利用被害額は平成25年以降増加傾向にあり、令和４年の被害額については、436.7億円で統計を取り始めた平成９年以降、過去最悪となった。令和５年第１四半期（令和５年１月～同年３月）の被害額は121.4億円であり、前年同期比（令和４年第１四半期（令和４年１月～同年３月））では21.3%増加しており、厳しい情勢にある。

【図表14：クレジットカード不正利用被害の発生状況】



一般社団法人日本クレジット協会（https://www.j-credit.or.jp）クレジットカード不正利用被害の発生状況から作成

(4)　対処状況

○　金融機関等との連携強化

金融庁及び一般社団法人全国銀行協会等に対して、被害防止対策に活用してもらうため、インターネットバンキングの不正送金に係る被害状況等を提供している。

○　フィッシング対策強化の要請等

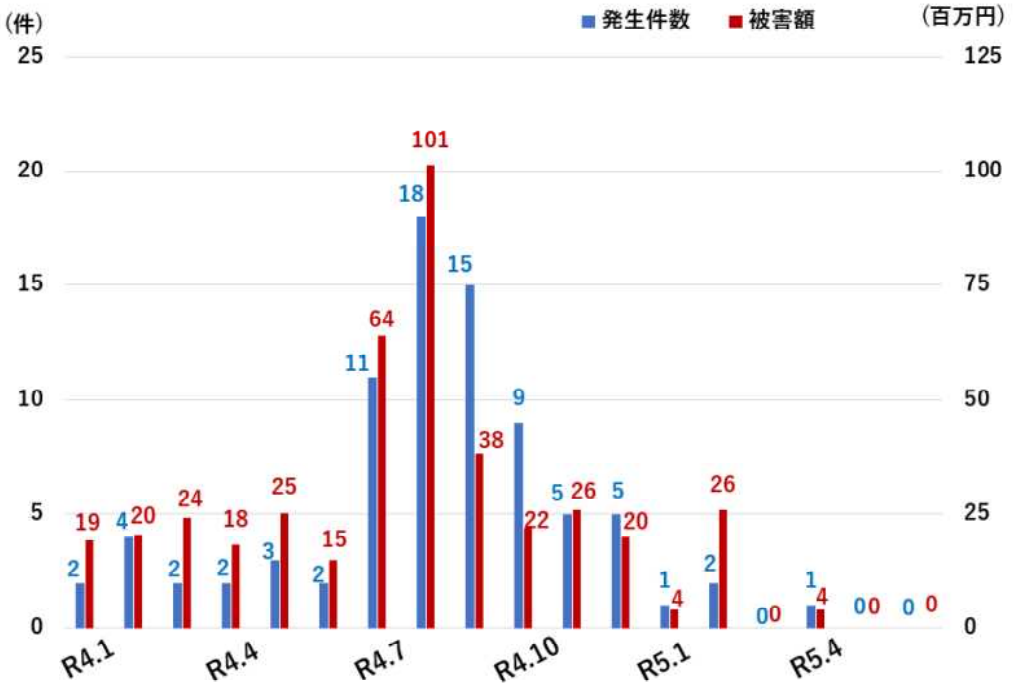
令和５年上半期に、フィッシングによるとみられるインターネットバンキングに係る不正送金被害が急増したことなどを受け、令和５年７月、金融庁と連携し、金融機関に対し、具体的な被害事例を基にしたフィッシング対策を講じるよう要請した。

また、令和５年８月、金融庁、一般社団法人全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（以下「ＪＣ３」という。）と連携し、国民に対し、メールやＳＭＳに記載されたリンクからアクセスしたサイトにＩＤ及びワンタイムパスワード・乱数表等のパスワードを入力しないよう注意喚起を行った。

○　ＳＩＭスワップ対策

ＳＩＭスワップによる不正送金事案が増加していた状況を踏まえ、令和４年９月、総務省と連携し、携帯電話事業者に対して、携帯電話機販売店における本人確認の強化を要請し、令和５年２月までに、大手携帯電話事業者において同要請への対応を完了した。その結果、令和５年上半期におけるＳＩＭスワップによる不正送金の被害が激減した。

【図表15：SIMスワップに係る不正送金発生状況】



○　フィッシングサイトの閲覧防止対策

都道府県警察が把握したフィッシングサイトに係るＵＲＬ情報を集約し、ウイルス対策ソフト事業者等に提供することにより、ウイルス対策ソフトの機能による警告表示等、フィッシングサイトの閲覧を防止する対策を実施している。

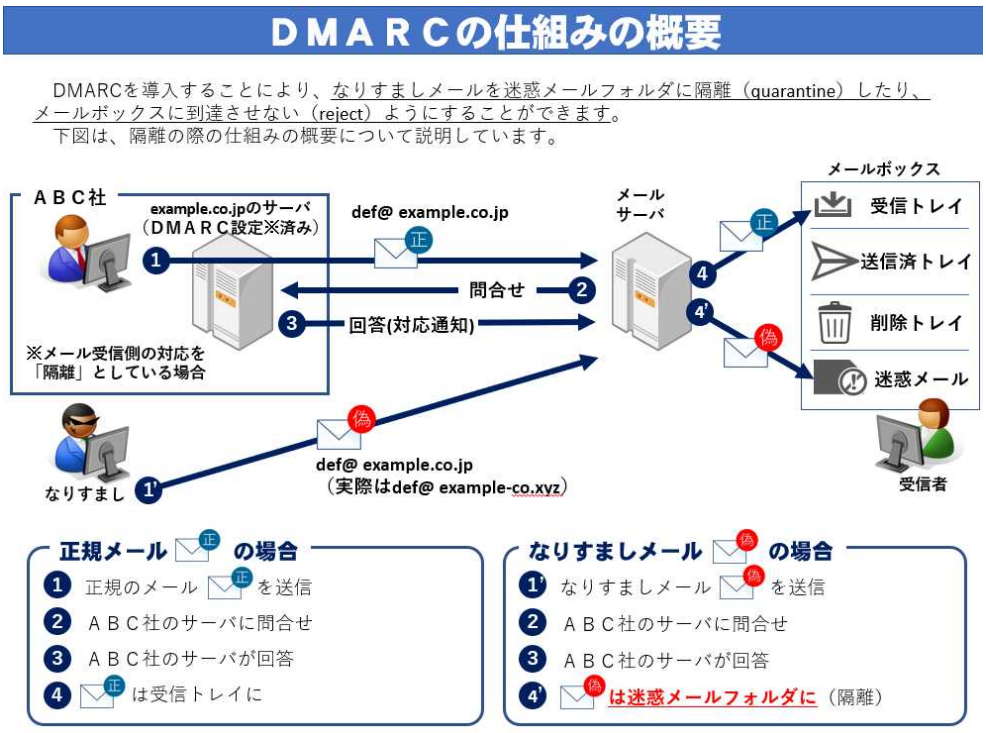
○　フィッシングサイトを含む偽サイト等に係る被害防止対策

福岡県警察においては、画像解析技術を利用したフィッシングサイトを自動的に検出するシステムを開発し、これにより検出したフィッシングサイトに関するＵＲＬ情報等を警察庁に報告し、フィッシングに係る被害防止対策を推進するとともに、ＪＣ３にも本システムに関する技術を提供した。

○　クレジットカード番号等の盗用防止対策

クレジットカード不正利用被害の大部分が、クレジットカードの番号盗用によるものであり、フィッシング等によりクレジットカード番号等を窃取し、利用権者になりすます手口が主要な要因となっている。こうした情勢を踏まえ、クレジットカード番号等の不正利用の原因となるフィッシング被害が増加していることから、警察庁、経済産業省及び総務省は、令和５年２月、日本クレジット協会に対し、送信ドメイン認証技術（DMARC[*10]）の導入をはじめとするフィッシング対策の強化を要請した。

【図表16：DMARCの仕組みの概要】



*10　Domain-based Message Authentication,Reporting,and Conformanceの略称

○　クレジットカード番号の漏えい等事態の対処に資する連携

サイバー攻撃や不正アクセスによる情報流出が相次ぎ発生している状況に鑑み、令和５年３月、不正アクセスによる保有個人情報の漏えい等事態の未然防止、被害の拡大防止及び類似事態の発生防止等のリスク低減並びに同事態への適切かつ迅速な対応を図るため、個人情報保護委員会と覚書を締結したほか、令和５年６月、サイバー事案に起因する又はそのおそれのあるクレジットカード番号等の漏えい事案への対策の推進に関する覚書を経済産業省と締結した。

○　フィッシングによる不正アクセス禁止法違反事件被疑者の検挙

専門学生の男(21)は、令和４年10月から同年11月、正規のＳＮＳになりすましたフィッシングサイトを作成してインターネット上に公開し、複数の利用権者からＩＤ・パスワードを不正に取得した後、取得したＩＤ・パスワードを用いて同ＳＮＳに不正アクセスした。令和５年４月、男を不正アクセス禁止法違反等で検挙した。

○　フィッシングによる詐欺事件被疑者の検挙

専門学生の男（22）らは、令和４年５月から同年７月にかけて、氏名不詳者と共謀のうえ、フィッシングにより入手した電子決済用アプリの識別符号を使用して、他人の決済情報をコンビニ店員に提示して電子タバコを詐取した。令和５年１月、男２名を詐欺罪で検挙した。

○　外国捜査機関と連携したフィッシング事犯の検挙

サイバー特別捜査隊及び大阪府警察は、インドネシア国家警察と連携し、フィッシングツール「16SHOP」を用いて不正に入手したクレジットカード番号等を使用して通販サイトの商品を窃取するなどしたインドネシア在住の同国人被疑者を特定し、令和５年７月９日に同国国家警察が同被疑者を逮捕した。本件は、日本警察の捜査がフィッシング事犯に関する国外被疑者の検挙に結びついた初めての事案となった（第３部１参照)。

３　ランサムウェア被害の情勢等

(1)　概要

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である。

手口としては、データの暗号化のみならず、データを窃取した上、企業・団体等に対し「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝（ダブルエクストーション）が多くを占める。

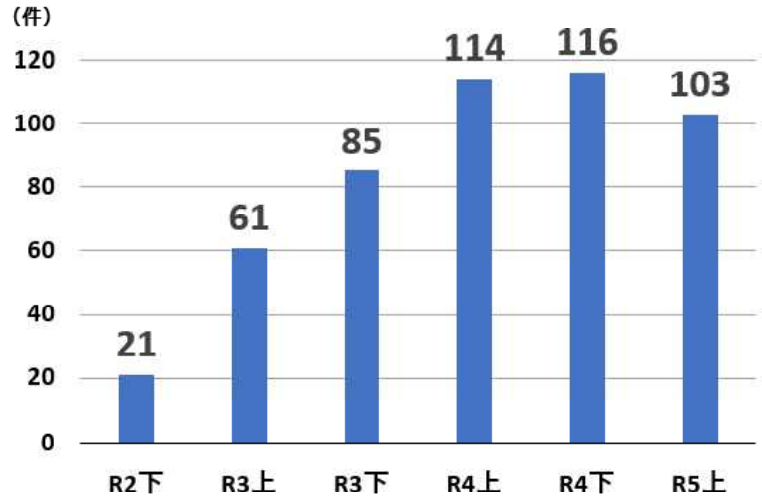
感染経路は、令和４年に引き続き、ぜい弱性を有するＶＰＮ[*11]機器等や強度の弱い認証情報等が設定されたリモートデスクトップサービスが多くを占めた。

(2)　企業・団体等におけるランサムウェア被害

ア　被害件数

企業・団体等におけるランサムウェア被害として、令和５年上半期に都道府県警察から警察庁に報告のあった件数は103件であり、令和４年上半期以降、高い水準で推移している。

【図表17：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】



イ　特徴

○　二重恐喝（ダブルエクストーション）による被害が多くを占める

被害（103件）のうち、手口を確認できたものは83件あり、このうち、二重恐喝の手口によるものは65件で78％を占めた。

○　「ノーウェアランサム」による被害

ランサムウェアによる被害のほか、最近の事例では、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（ランサムウェアを用いる）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（「ノーウェアランサム」）による被害が、新たに６件確認された。

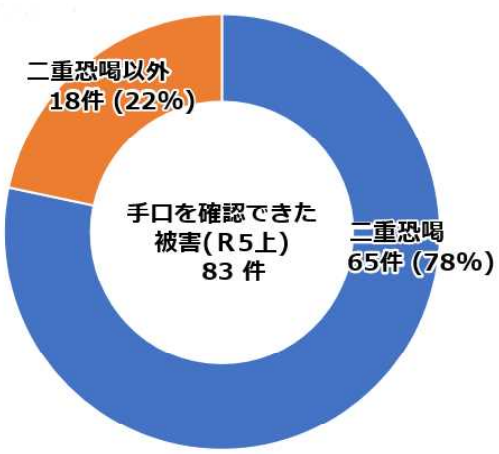
○　暗号資産による対価の要求が多くを占める

被害（103件）のうち、直接的な対価の要求を確認できたものは22件あり、このうち、暗号資産による支払いの要求があったものは21件で95％を占めた。

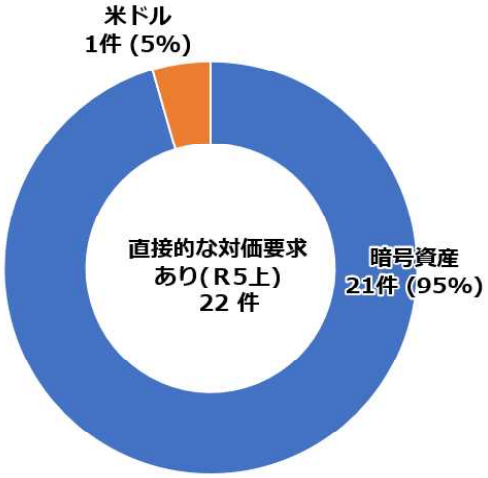
---

*11　Virtual Private Networkの略。公衆回線等を利用して構築する仮想的なプライベートネットワークのこと。

【図表18：ランサムウェア被害の手口別報告件数】



【図表19：要求された対価支払い方法別報告件数】

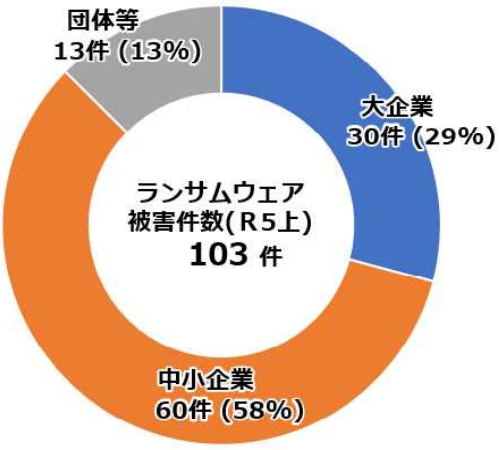


ウ　被害企業・団体等の規模

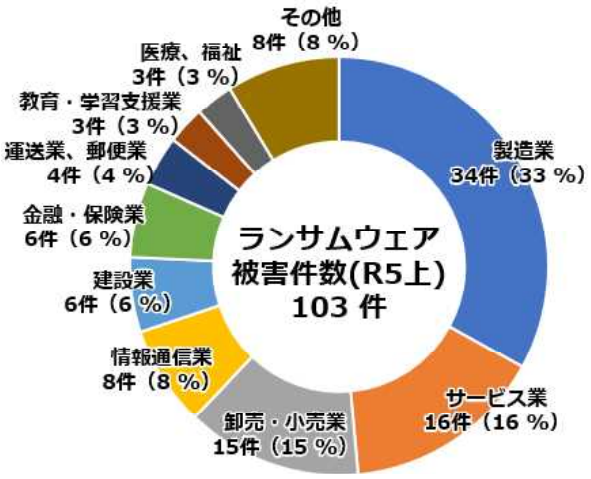
被害（103件）の内訳を企業・団体等の規模別[*12]に見ると、大企業は30件、中小企業は60件であり、その規模を問わず、被害が発生した。

また、業種別[*13]に見ると、製造業は34件、サービス業は16件、卸売・小売業は15件であり、その業種を問わず、被害が発生した。

【図表20：ランサムウェア被害の企業・団体等の規模別報告件数】



【図表21：ランサムウェア被害の企業・団体等の業種別報告件数】



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(3)　企業・団体等におけるランサムウェア被害の実態

企業・団体等におけるランサムウェア被害の実態を把握するため、被害（103件）のあった企業・団体等にアンケート調査を実施し、その回答結果について分析を行った。

---

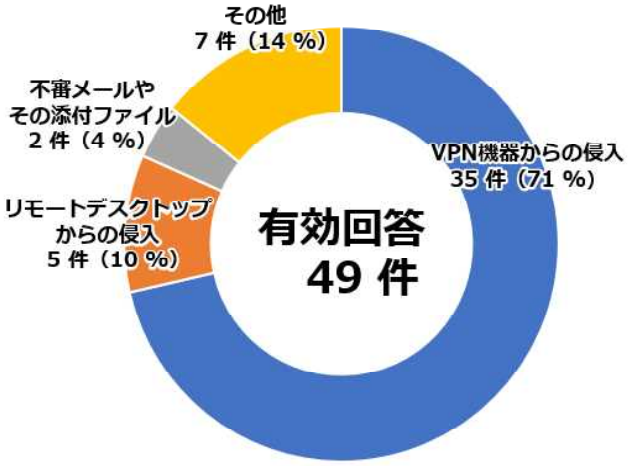
*12　中小企業基本法（昭和38年法律第154号）第２条第１項に基づき分類

*13　日本標準産業分類に基づき分類

ア　感染経路

ランサムウェアの感染経路について質問したところ、49件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が35件で71％、リモートデスクトップからの侵入が５件で10％を占め、テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが82％と大半を占めた。

【図表22：感染経路】



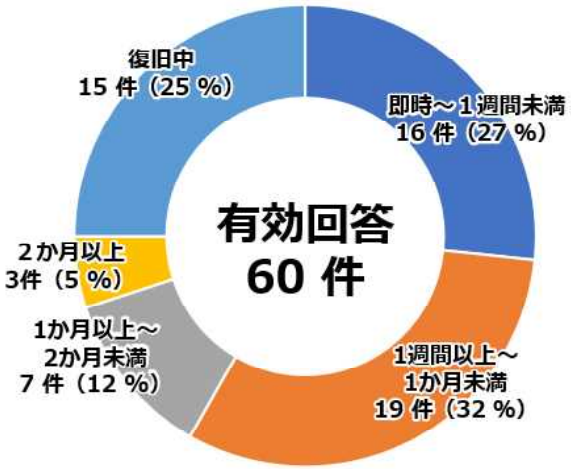
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

イ　復旧等に要した期間・費用

復旧に要した期間について質問したところ、60件の有効な回答があり、このうち、復旧までに１か月以上を要したものが10件あった。

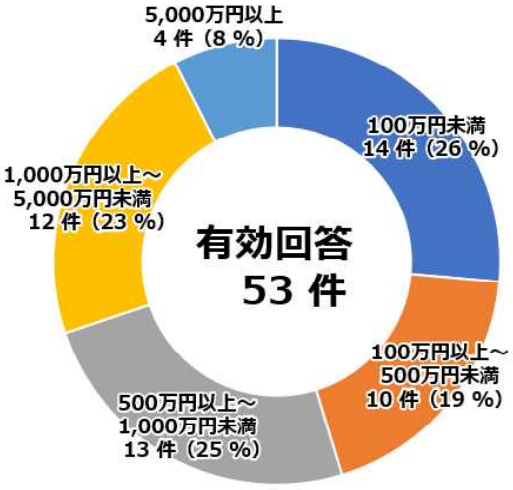
また、ランサムウェア被害に関連して要した調査・復旧費用の総額について質問したところ、53件の有効な回答があり、このうち、1,000万円以上の費用を要したものが16件で30％を占めた。

【図表23：復旧に要した期間】



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

【図表24：調査・復旧費用の総額】

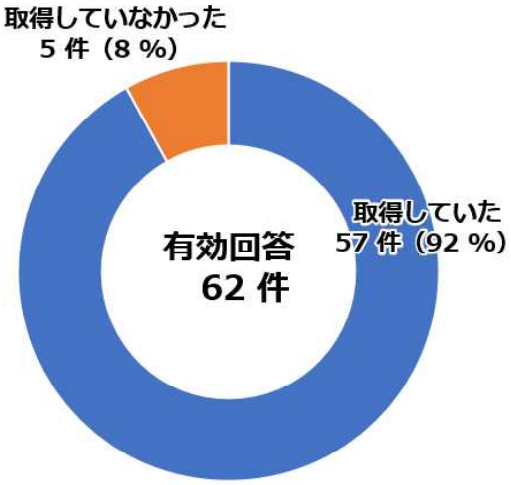


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

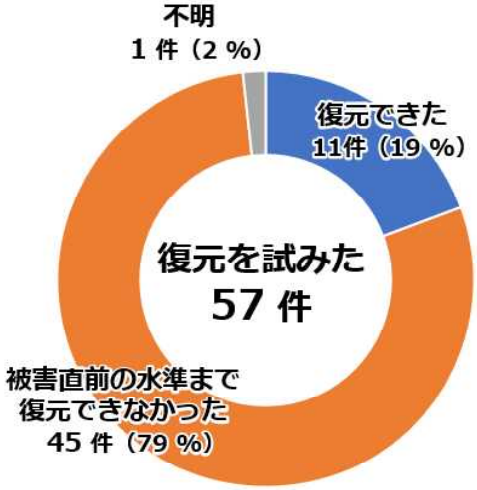
ウ　バックアップの取得・活用状況

被害に遭ったシステム又は機器のバックアップの取得状況について質問したところ、62件の有効な回答があり、このうち、取得していたものが57件で92％を占めた。また、取得していたバックアップから復元を試みた57件の回答のうち、バックアップから被害直前の水準まで復旧できなかったものは45件で79％であった。

【図表25：バックアップ取得の有無】



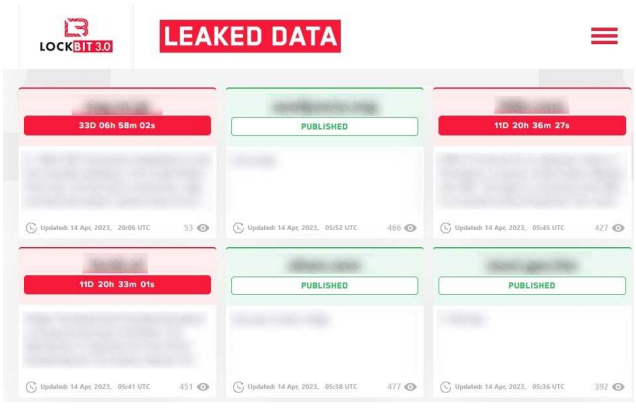
【図表26：バックアップからの復元結果】

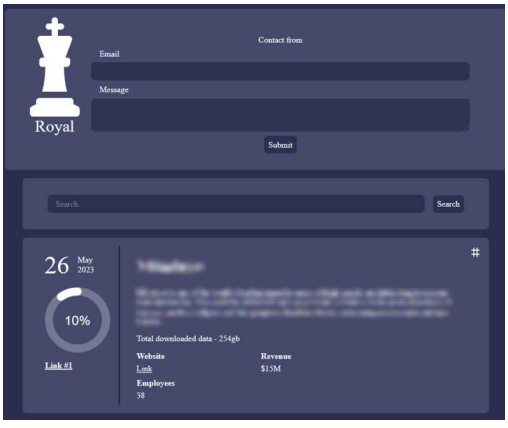


(4)　ランサムウェアと関連するリークサイトの状況

令和５年上半期においても、ランサムウェアによって流出した情報等が掲載されているダークウェブ上のリークサイトに、国内の事業者等の情報が掲載されていたことを確認した。掲載された情報には、製品に関する情報や顧客の個人情報等が含まれていた。

【図表27：ダークウェブ上のリークサイト例】





(5)　対処状況

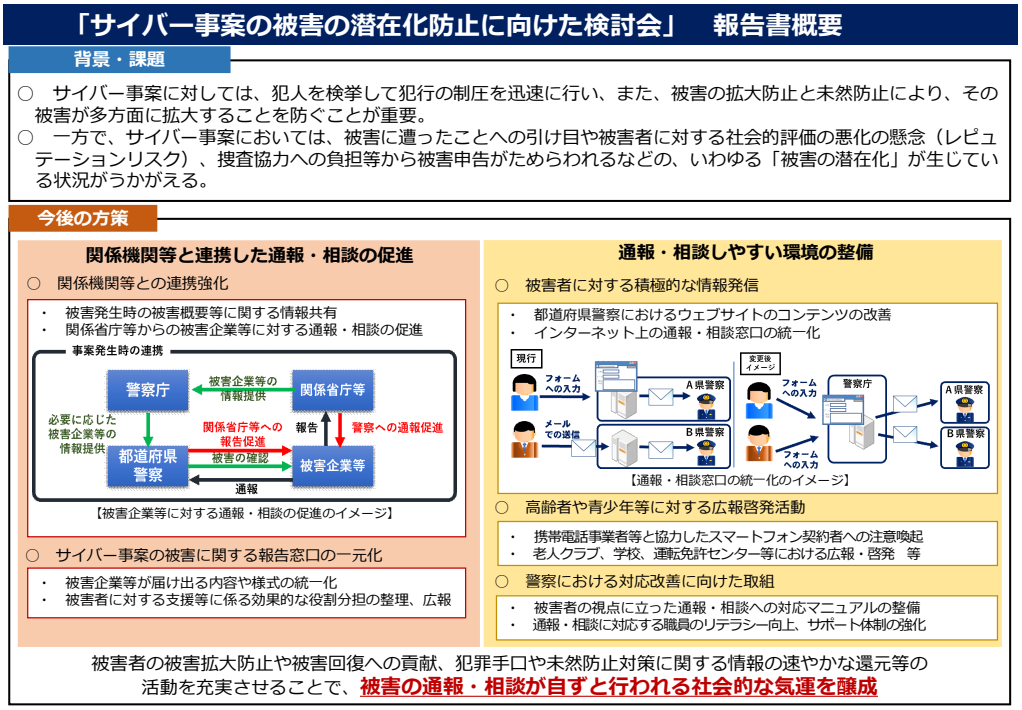
○　サイバー事案の被害の潜在化防止に向けた取組

警察では、サイバー事案を把握した場合には検挙のための捜査のみならず、攻撃者・犯行手口等の実態解明、被害の未然防止・拡大防止対策を推進しており、これらは、国民や事業者等からの通報・相談によって

得られた情報等を端緒として実施していることから、通報・相談は、警察活動において重要な役割を担っている。一方、サイバー事案の被害は、被害者自身に対する社会的評価の悪化の懸念等から警察への通報・相談そのものがためらわれる傾向にあり、いわゆる「被害の潜在化」が課題となっている。

これらの状況から、警察庁では、「サイバー事案の被害の潜在化防止に向けた検討会」を開催し、産業界、セキュリティ関係団体、法曹界、学術界の有識者により被害の潜在化防止に関する今後の方策について議論いただき、報告書を取りまとめ令和５年４月に公表した。

【図表28：「サイバー事案の被害の潜在化防止に向けた検討会」報告書概要】



○　医療機関等との連携強化に向けた取組

医療機関におけるランサムウェアによる被害が発生していることを踏まえ、サイバー事案に係る被害の未然防止等を図る必要があることから、平時から緊密な連携を図り、事案発生時における警察への迅速な通報・相談を促進するため、令和５年４月、公益社団法人日本医師会と覚書を締結するとともに、令和５年５月、四病院団体協議会及び各国公私立大学病院に対して連携強化に関する依頼を行った。

○　ＶＰＮ機器のぜい弱性に関する広報啓発

ランサムウェア被害の主たる要因となるＶＰＮ機器のぜい弱性については、警察庁ウェブサイト、警察庁Twitter等の様々な媒体を活用するとともに、各都道府県警察が関係機関・団体等と構築する協議会等を通じて情報発信を行うなど積極的な広報活動を実施した。

【図表29：Fortinet社製品に関する警察庁からの注意喚起】

○　リークサイト上において売買されるアクセス権の把握等

ダークウェブ上のリークサイトにおいて売買されるアクセス権等を監視し、国内の事業者等のユーザＩＤ・パスワード等が掲載されていることを把握した場合は、都道府県警察を通じて、当該事業者等に対してユーザＩＤ・パスワード等が漏えいしていることを教示した上で、必要な対策を講じるよう求めている。

○　国際連携の強化

令和４年６月から、欧州各国の捜査機関との緊密な連携を図るため、サイバー事案に専従する連絡担当官として警察職員をＥＵＲＯＰＯＬ（European Union Agency for Law Enforcement Cooperation）に初めて常駐させ、信頼関係の構築を進めている。さらに、令和５年２月から、連絡担当官を増員し、国際共同捜査への参画に向けて各国捜査機関とのさらなる連携強化を推進している。

(6)　サイバー特別捜査隊によるランサムウェア事案の実態解明等

サイバー特別捜査隊では、ランサムウェアが用いられた事案の捜査及び実態解明を推進している。ランサムウェアには様々な種類があるが、ランサムウェアの開発・運営を行う者（Operator）が、攻撃の実行者（Affiliate）にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る態様（RaaS：Ransomware as a Service）のものが確認された。また、ラン

サムウェアの標的となる企業等のネットワークに侵入するための認証情報等を売買する者（IAB：Initial Access Broker）も存在する。このため、攻撃の実行者が必ずしも技術的な専門知識を有している必要はなく、同種のランサムウェアが用いられた事案であっても攻撃の実行者が異なる場合や、異なる種類のランサムウェアが用いられた事案であっても攻撃の実行者が同じである場合がある。

さらに、サイバー特別捜査隊の捜査により、ランサムウェアが用いられた複数の事案において、①侵入時、②侵入後、③攻撃実行時の各段階で共通してみられる攻撃者の手口についても明らかとなってきた。①～③のいずれかの段階で攻撃者の行動を止めることができれば被害は発生しないため、各段階において適切なセキュリティ対策を講じることで、ランサムウェアによる被害を未然に防止・軽減することができる（第３部１参照）。

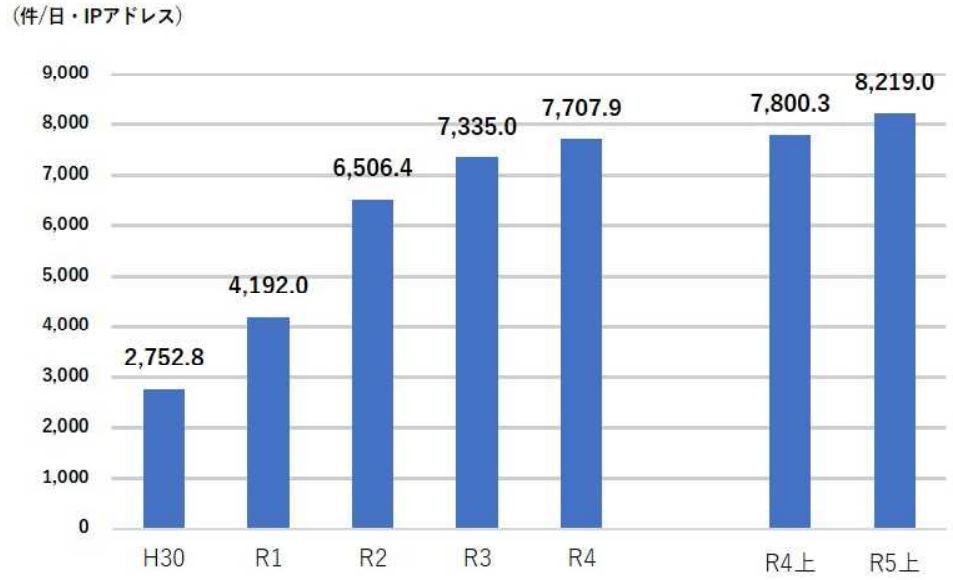
４　サイバー空間におけるぜい弱性探索行為等の観測状況

(1)　センサーにおいて検知したアクセスの概況

警察庁では、インターネット上にセンサーを設置し、当該センサーに対して送られてくる通信パケットを収集している。このセンサーは、外部に対して何らサービスを提供していないので、本来であれば外部から通信パケットが送られてくることはない。送られてくるのは不特定多数のＩＰアドレスに対して無差別に送信される通信パケットであり、これらの通信パケットを分析することで、インターネットに接続された各種機器のぜい弱性の探索行為等を観測し、ぜい弱性を悪用した攻撃、不正プログラムに感染したコンピュータの動向等、インターネット上で発生している各種事象を把握することができる。

令和５年上半期にセンサーにおいて検知したアクセス件数は、１日・１ＩＰアドレス当たり8,219.0件であり、増加の一途をたどっている（前年同期比で5.4%増加）。アクセス件数が増加しているのは、ＩｏＴ機器の普及により攻撃対象が増加していること、技術の進歩により攻撃手法が高度化していることなどが背景にあるものとみられる。

【図表30：センサーにおいて検知したアクセス件数の推移】



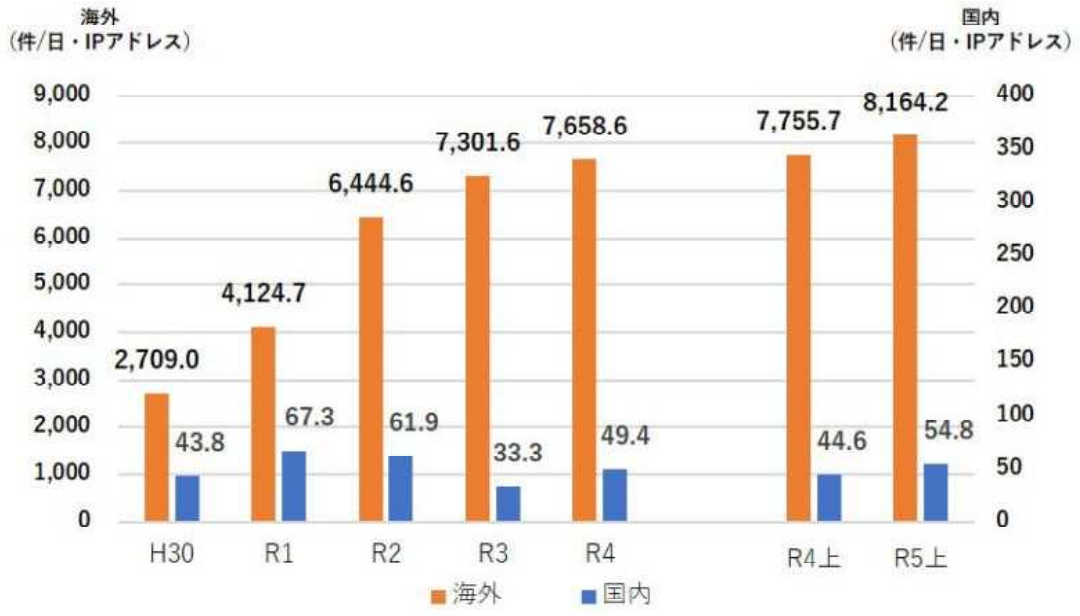
(2)　特徴的な観測

○　海外を送信元とするアクセスが高水準で推移

検知したアクセスの送信元の国・地域に着目すると、海外の送信元が高い割合を占めている。

令和５年上半期においても、国内を送信元とするアクセスが１日・１ＩＰアドレス当たり54.8件であるのに対して、海外を送信元とするアクセスが8,164.2件と、検知したアクセスの大部分を占めており、海外からの脅威への対処が引き続き重要となっている。

【図表31：検知したアクセスの送信元で比較した１日・１ＩＰアドレス当たりの件数の推移】

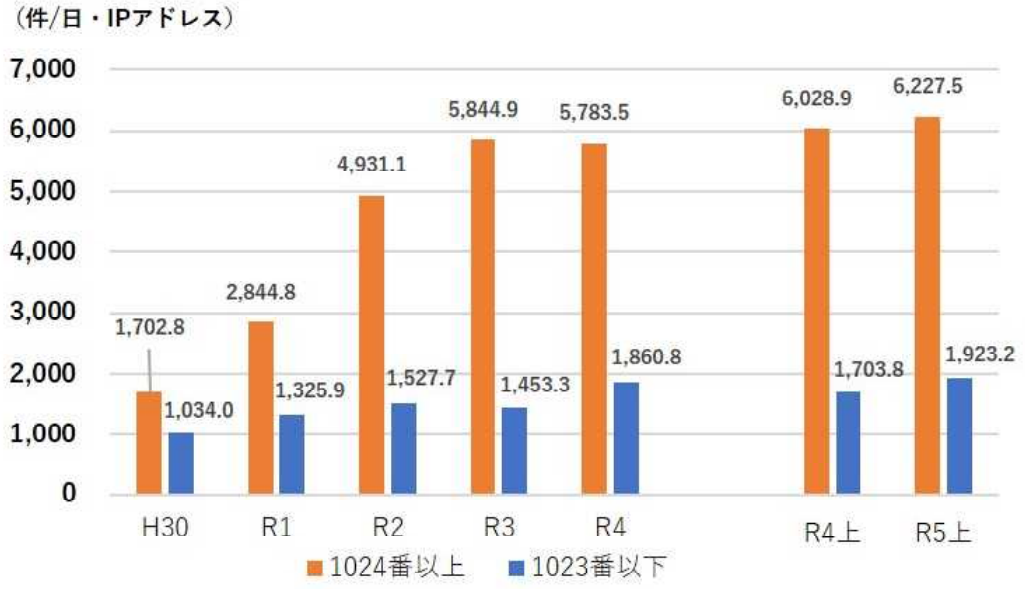


○　ＩｏＴ機器を対象としたぜい弱性探索行為等

検知したアクセスの宛先ポートに着目すると、ポート番号1024以上のポートへのアクセスが多数を占めており、全体のアクセス件数が増加する要因となっている。

ＩｏＴ機器では標準設定として1024番以上のポート番号を使用しているものが多いことから、ポート番号1024以上のポートへのアクセスの多くが、ぜい弱性を有するＩｏＴ機器の探索やＩｏＴ機器に対するサイバー攻撃を目的とするためのものであるとみられる。

【図表32：検知したアクセスの宛先ポートで比較した１日・１ＩＰアドレス当たりの件数の推移】



○　ＩｏＴ機器に対する不正プログラムの感染拡大を狙ったと思われるアクセスの観測

令和５年上半期において、国内を送信元とするＭｉｒａｉ[*14]ボットの特徴を有するアクセスを宛先ポート別に見ると、５月中旬頃から宛先ポート52869/ＴＣＰに対するアクセスが増加していた。

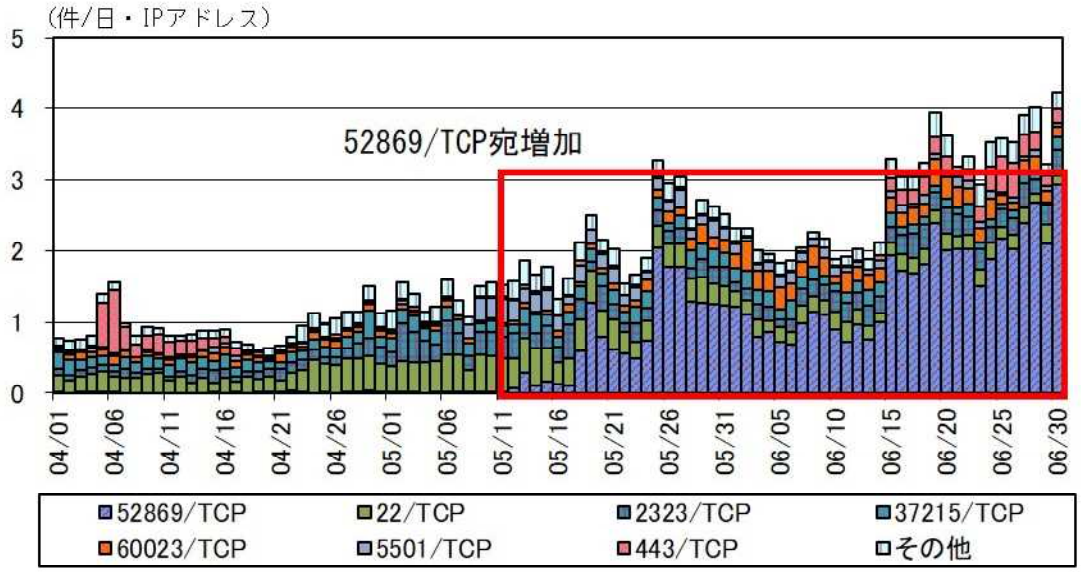
このポートは、過去にＭｉｒａｉの亜種が、家庭用ルーターやＩＰカメラ等のＩｏＴ機器に存在するぜい弱性を悪用して感染拡大を行う際に狙われたポートであることから、今回増加が観測されたアクセスについても、ＩｏＴ機器に対して、Ｍｉｒａｉ等の不正プログラムの感染拡大を狙ったものであると考えられる。

ＩｏＴ機器を利用する際は、適切なアクセス制御、初期設定のユーザ名及びパスワードの変更、セキュリティパッチの適用、サポートが終了した機器の更新等の対策を継続的に実施する必要がある。

---

*14　IoT機器等に感染しDoS攻撃等を行う不正プログラムの一種

【図表33：国内を送信元とするMiraiボットの特徴を有するアクセス件数の推移(23/TCPを除く宛先ポート別)】



○　ＶＰＮ機器等のぜい弱性を狙ったと思われるアクセスの観測

令和５年上半期において、ぜい弱性を有するＶＰＮ機器等を探索する目的と思われる複数種類のアクセスが断続的に観測された。

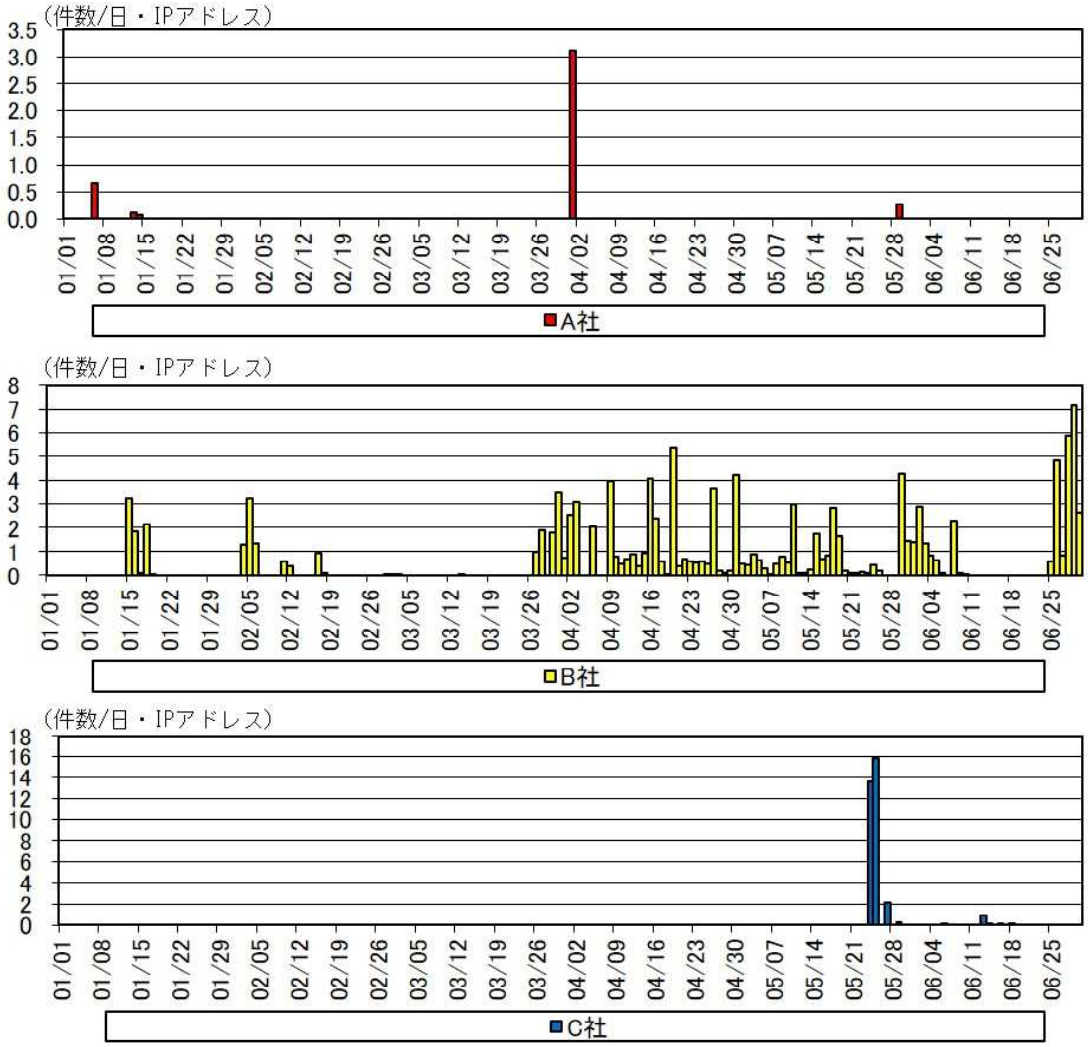
ＶＰＮ機器等のぜい弱性を悪用されてネットワークに侵入された場合は、情報を窃取される、ランサムウェアの感染によりデータを暗号化されるなどの被害に遭う可能性がある。

観測されたアクセスは、ぜい弱性公開後からごく短時間のみ観測されたものがある一方で、継続的に観測されたものもあった。

ＶＰＮ機器等については、適切なアクセス制御やセキュリティパッチの適用等の対策を継続的に実施する必要がある。

また、セキュリティパッチ適用前にぜい弱性が悪用されてＩＤやパスワードが漏えいしている可能性も考慮し、パスワードの変更等を検討することも重要である。

【図表34：ＶＰＮ機器等のぜい弱性を狙ったと思われるアクセス件数の推移】



５　インターネット上の違法・有害情報の実態等

(1)　インターネット・ホットラインセンター（ＩＨＣ）の概要

○　違法・有害情報の概要

インターネット上には、児童ポルノ、規制薬物の広告等に関する違法情報や、違法情報には該当しないものの、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない人を自殺に誘引する情報や爆発物・銃砲等の製造方法、殺人、強盗等の請負等の有害情報が多数存在している。

○　違法・有害情報の現状

近年では、インターネット上において、違法・有害情報を容易に入手できる状況にあるほか、仕事の内容を明らかにせずに著しく高額な報酬の支払いを示唆したりして実行者を募集するＳＮＳ上の投稿や当該投稿に関する情報（以下「犯罪実行者募集情報」という。）が氾濫しており、これに応募した者らにより実際に犯罪が敢行され、中には凶悪事件に発

展する事案も発生している状況が見受けられることから、こうした情報への対策が重要かつ喫緊の課題となっている。

○　警察における取組状況

警察では、サイバーパトロール等により、違法・有害情報の把握に努め、これを端緒とした取締りを推進するとともに、サイト管理者等への削除依頼を行っている。

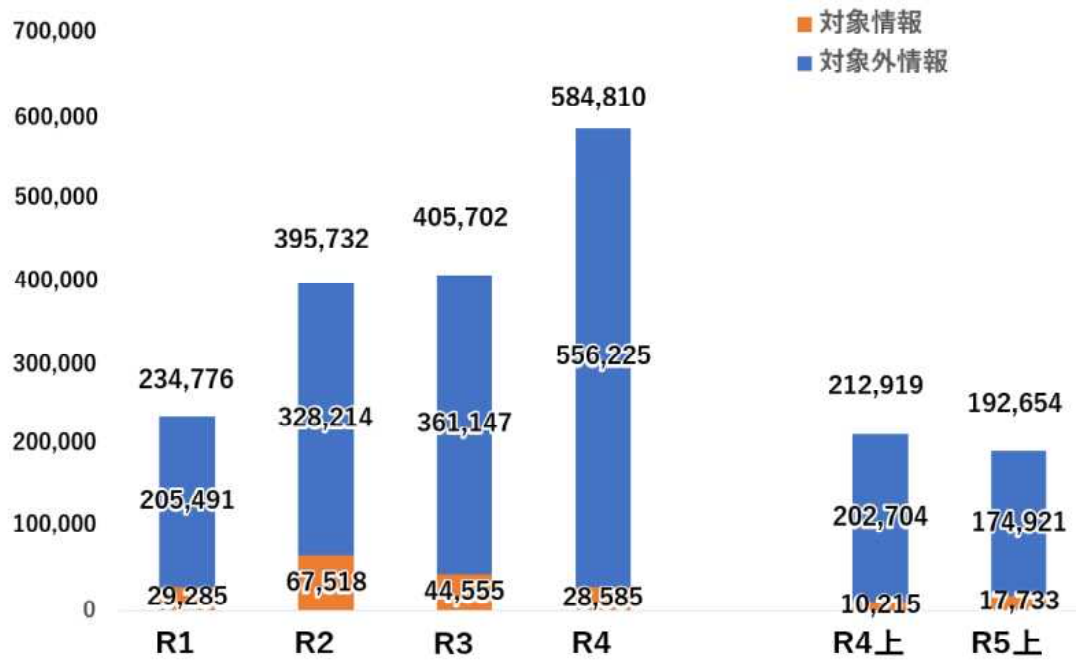
また、警察庁においては、インターネット利用者等から違法・有害情報に関する通報を受理し、警察への通報、サイト管理者等への削除依頼等を行うＩＨＣを事業委託するとともに、サイバーパトロールにより重要犯罪密接関連情報及び自殺誘引等情報[*15]を収集し、ＩＨＣに通報するＣＰＣを事業委託している。

(2)　違法・有害情報の実態、対処状況

○　令和５年上半期における違法情報の対処状況

令和５年上半期におけるＩＨＣの通報受理件数は192,591件であり、運用ガイドラインに基づいて192,654件を分析した結果、違法情報を13,875件、重要犯罪密接関連情報を172件、自殺誘引等情報を3,686件と判断した。違法情報と判断した通報のうち、通報前に削除された82件を除く1,584件を警察に通報し、削除依頼を行う前に削除されたもの等を除く1,106件についてサイト管理者等に対して削除依頼を行い、そのうち924件（83.5％）が削除された。

【図表35：違法情報等の分析件数の推移】



*15　他人を自殺に誘引・勧誘する情報等

○　ＩＨＣ及びＣＰＣにおける取組の強化

インターネットを通じて銃砲等の設計図、製造方法等に関する情報を容易に入手できる現代社会の特性を踏まえ、令和５年２月、運用ガイドラインを改定し、ＩＨＣ及びＣＰＣにおける取扱情報の範囲に、重要犯罪密接関連情報を追加し、ＩＨＣ及びＣＰＣの運用体制の強化を図った。

【図表36：重要犯罪密接関連情報に関する広報用ポスター】

○　重要犯罪密接関連情報の対処状況

令和５年２月15日から６月30日までの間、ＩＨＣの運用ガイドラインに基づき、重要犯罪密接関連情報と判断し分析した情報は172件であり、148件（削除依頼を行う前に削除されたものを除く。）についてサイト管理者等に削除依頼を行った結果、77件（52.0％）が削除に至った。

【図表37：重要犯罪密接関連情報の削除依頼件数等】

類型	分析件数	削除依頼件数	削除完了件数
拳銃等の譲渡等	3	3	2
爆発物・銃砲等の製造	6	5	5
殺人・強盗等の勧誘	157	136	68
臓器売買	5	4	2
人身売買	0	0	0
硫化水素ガスの製造	1	0	0
ストーカー行為等	0	0	0
合計	**172**	**148**	**77**

※　削除完了件数は、令和５年７月末に確認した状況を計上

○　犯罪実行者募集情報対策の推進

近年、インターネット上において、犯罪実行者募集情報が氾濫している状況を踏まえ、警察庁では、令和５年２月、都道府県警察に対し、これらの投稿に関する情報収集を強化し、取締りや削除依頼、警告につなげるよう指示した。

また、令和５年３月、犯罪対策閣僚会議において、「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」が決定し、ＩＨＣ及びＣＰＣの効果的な運用により、犯罪実行者募集情報の排除に向けた更なる取組の推進等が示された。これを踏まえ、令和５年９月、ＩＨＣ及びＣＰＣの取扱情報の範囲に犯罪実行者募集情報を追加するとともに、同月、情報収集の体制強化・高度化を図るため、ＣＰＣにおいてＡＩシステムを導入し、犯罪実行者募集情報を含む重要犯罪密接関連情報や自殺誘引等情報に関するサイバーパトロールの高度化を図る予定である。

第３部　サイバー事案の検挙状況等

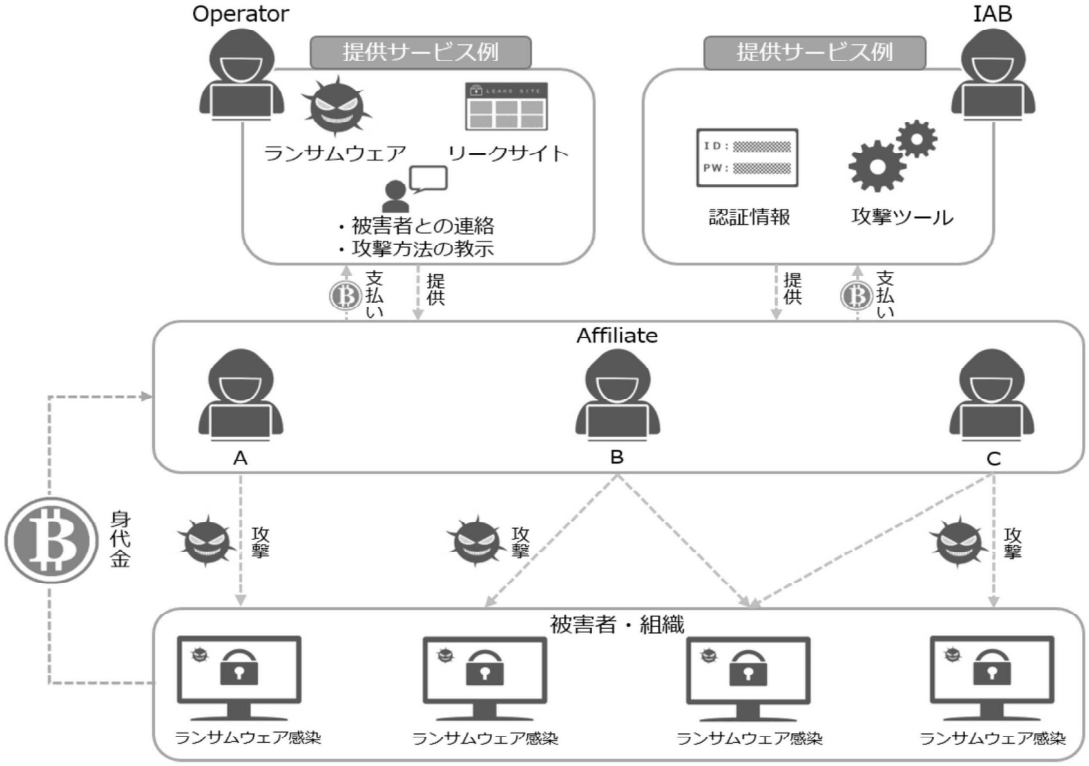
１　サイバー特別捜査隊の活動状況

サイバー空間における極めて深刻な脅威の情勢を踏まえ、令和４年４月、重大サイバー事案への対処を担う国の捜査機関としてサイバー特別捜査隊が設置された。重大サイバー事案について、サイバー特別捜査隊が都道府県警察と共同で捜査を進める中、サイバー特別捜査隊による情報の集約・分析や、その結果に基づく外国捜査機関との情報交換等を通じ、各種事案の実態解明のほか、外国に被疑者が存在するなど検挙が困難とみられるような事案についても、捜査が着実に進められている。以下に、主な取組を記載する。

○　サイバー特別捜査隊によるランサムウェア事案の実態解明等

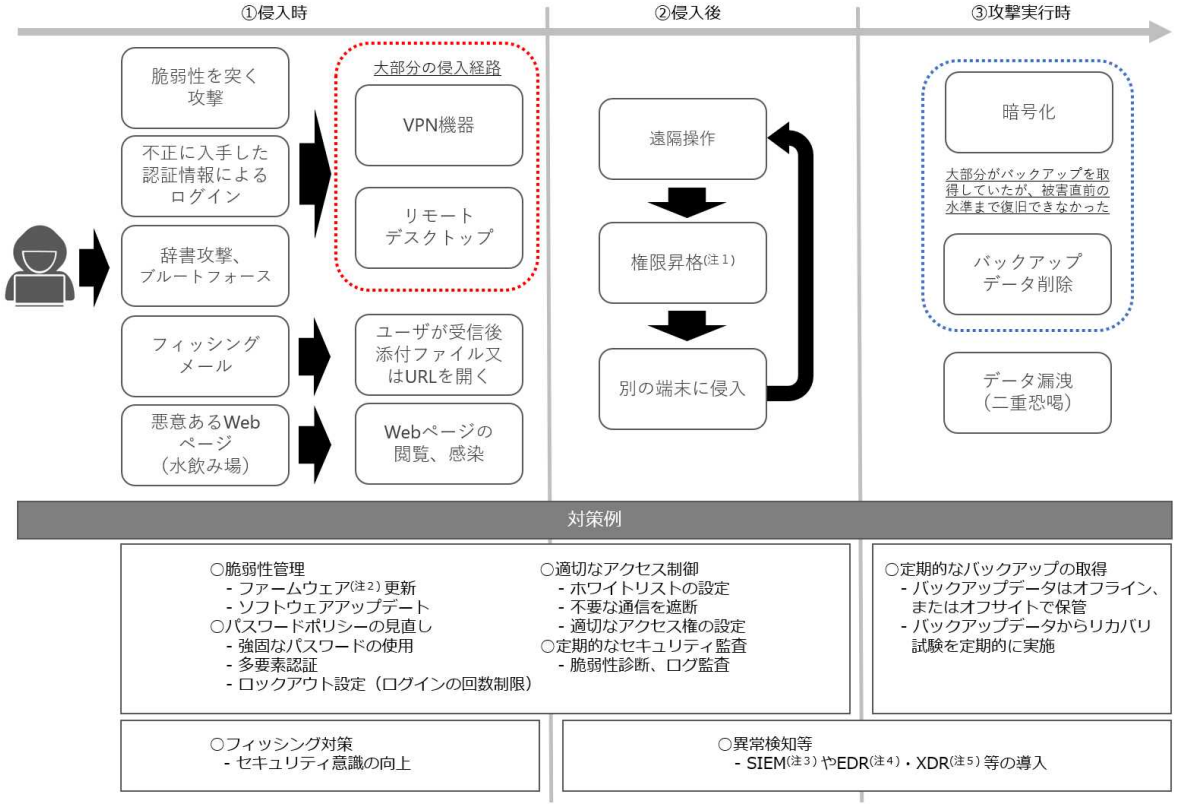
サイバー特別捜査隊では、ランサムウェアが用いられた事案の捜査及び実態解明を推進している。ランサムウェアには様々な種類があるが、ランサムウェアの開発・運営を行う者（Operator）が、攻撃の実行者（Affiliate）にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る態様（RaaS：Ransomware as a Service）のものが確認された。また、ランサムウェアの標的となる企業等のネットワークに侵入するための認証情報等を売買する者（IAB：Initial Access Broker）も存在する。このため、攻撃の実行者が必ずしも技術的な専門知識を有している必要はなく、同種のランサムウェアが用いられた事案であっても攻撃の実行者が異なる場合や、異なる種類のランサムウェアが用いられた事案であっても攻撃の実行者が同じである場合がある。

【図表38：ランサムウェア等を提供する者と攻撃を実行する者】



さらに、サイバー特別捜査隊の捜査により、ランサムウェアが用いられた複数の事案において、①侵入時、②侵入後、③攻撃実行時の各段階で共通してみられる攻撃者の手口についても明らかとなってきた。①～③のいずれかの段階で攻撃者の行動を止めることができれば被害は発生しないため、各段階において適切なセキュリティ対策を講じることで、ランサムウェアによる被害を未然に防止・軽減することができる。

【図表39：一般的なランサムウェア攻撃の流れと被害防止対策】



（注１）　パスワードの窃取や設定ミス、ぜい弱性等を利用してシステムの管理者権限を取得すること。

（注２）　電子機器に組み込まれたハードウェアを制御するソフトウェアのこと。

（注３）　Security Information and Event Managementの略。IT機器のログを一元管理し、セキュリティの脅威を検知・監視する仕組みのこと。

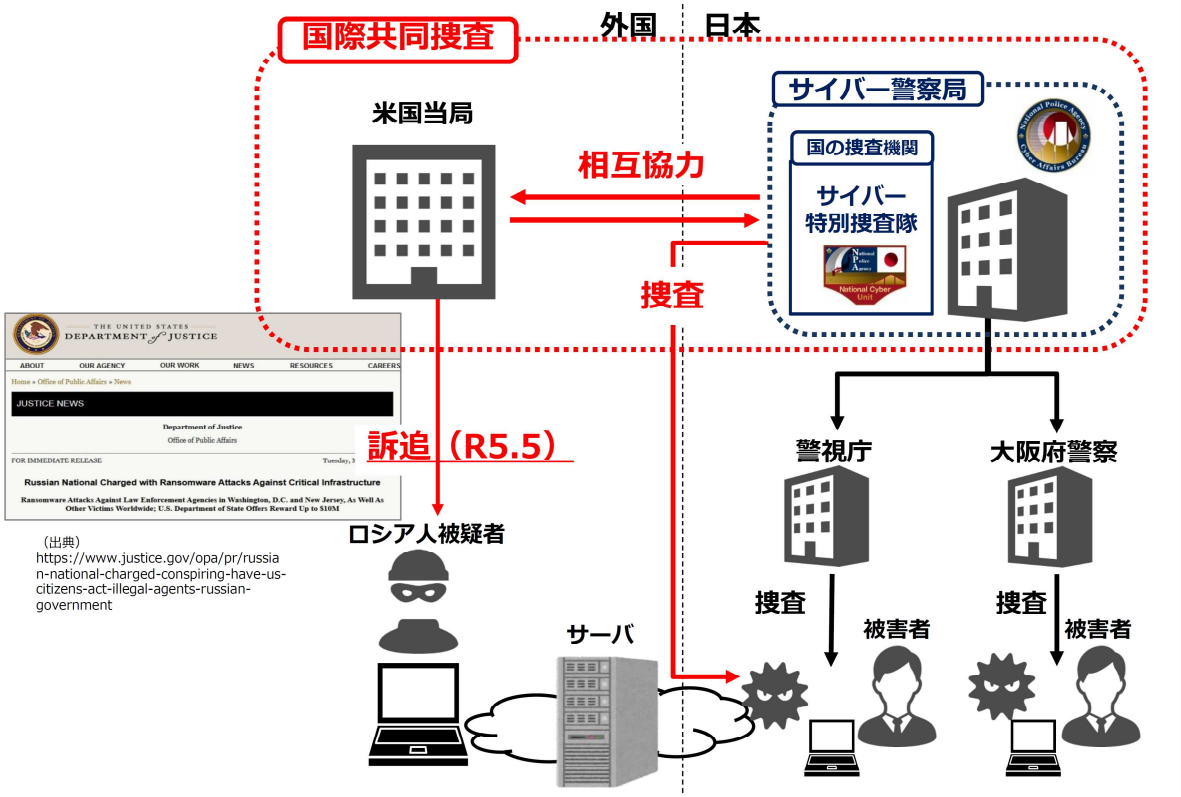
（注４）　Endpoint Detection and Responseの略。エンドポイント（クライアントPC等）で、不審な挙動を検知・対応する仕組みのこと。

（注５）　Extended Detection and Responseの略。エンドポイント・メール・サーバ・ネットワークなど複数のITリソースを総合的に監視し、不審な挙動を検知・対応する仕組みのこと。

○　外国捜査機関との連携

米国でのランサムウェア事案について、サイバー特別捜査隊等の捜査において得られた情報をＦＢＩに提供するなどの協力を行ったところ、令和５年５月、米国司法省から被疑者の一人を起訴した旨の発表があり、捜査に当たって日本警察の支援が有益であったとの言及があった。

【図表40：事案の概要】



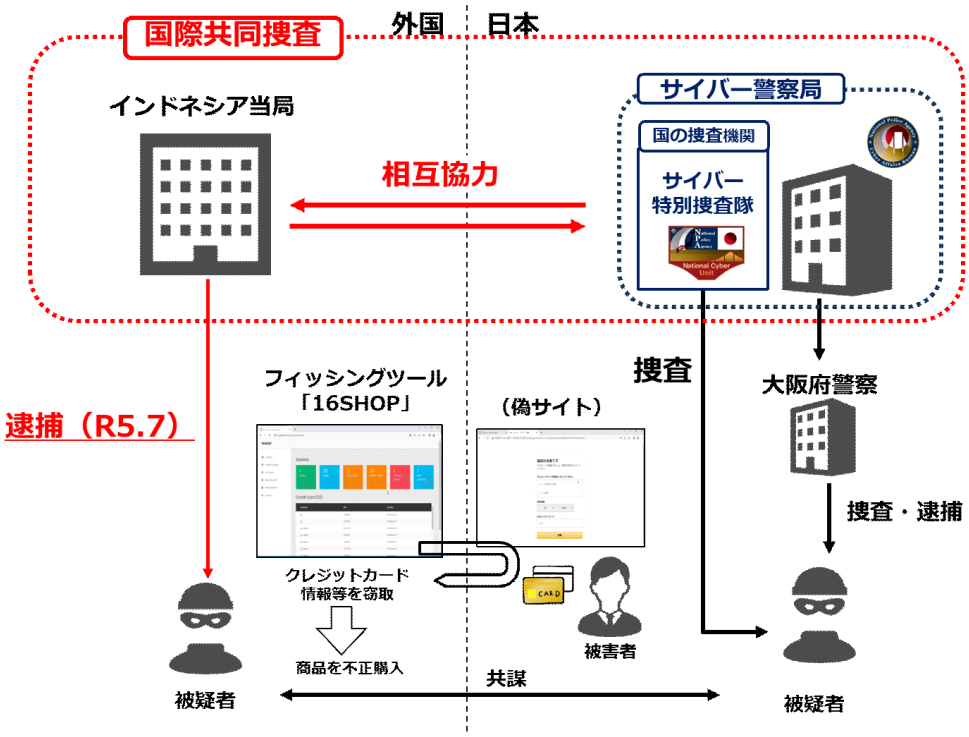
○　外国捜査機関と連携したフィッシング事犯の検挙

警察庁では外国捜査機関等との連携を推進しており、クレジットカード情報等を窃取するフィッシングサイトの作成ツールである「16SHOP」を利用した犯罪の被害拡大に対処するため、サイバー特別捜査隊及び大阪府警察が「キングフィッシャー作戦」と呼称される作戦にインドネシア国家警察等と連携して従事してきた。

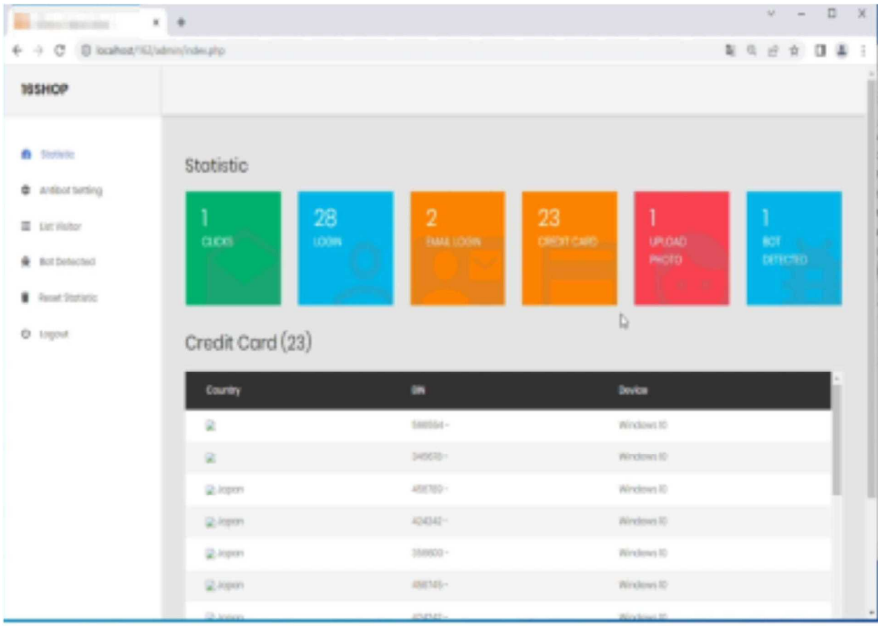
インドネシア国家警察に対して必要な協力を行ってきたところ、国内居住共犯者と共謀の上、上記フィッシングツールを用いて不正に入手したクレジットカード番号等を使用して通販サイトの商品を窃取するなどしたインドネシア在住同国人被疑者を、令和５年７月９日に同国国家警察が逮捕した。

本件は、サイバー特別捜査隊と都道府県警察が初めて警察庁長官の態勢の指示に基づく合同捜査を行った事例であり、また、日本警察の捜査がフィッシング事犯に関する国外被疑者の検挙に結びついた初めての事案である。

【図表41：事案の概要】

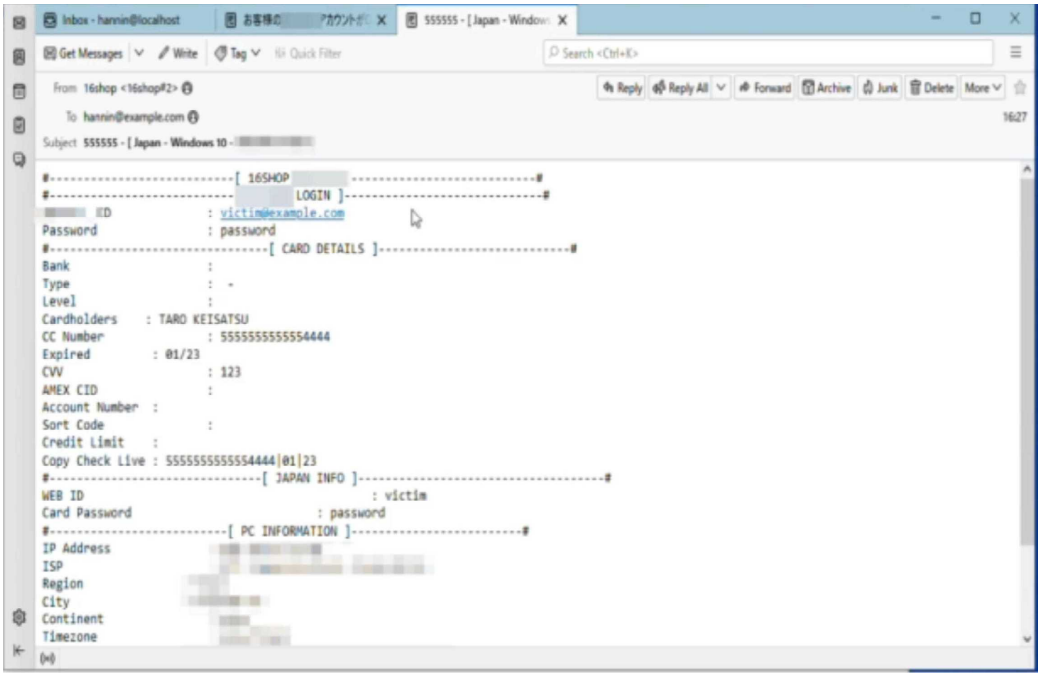


【図表42：フィッシングツール「16SHOP」の管理者画面】



【図表43：フィッシングツール「16SHOP」のクレジット番号の入力画面】

【図表44：窃取されたのクレジット番号の確認状況】



○　都道府県警察との連携

サイバー保険を名目とした架空料金請求詐欺事件について、サイバー特別捜査隊において暗号資産追跡の支援を行い、令和５年５月、愛知県警察などの合同捜査本部が被疑者２名を逮捕した。

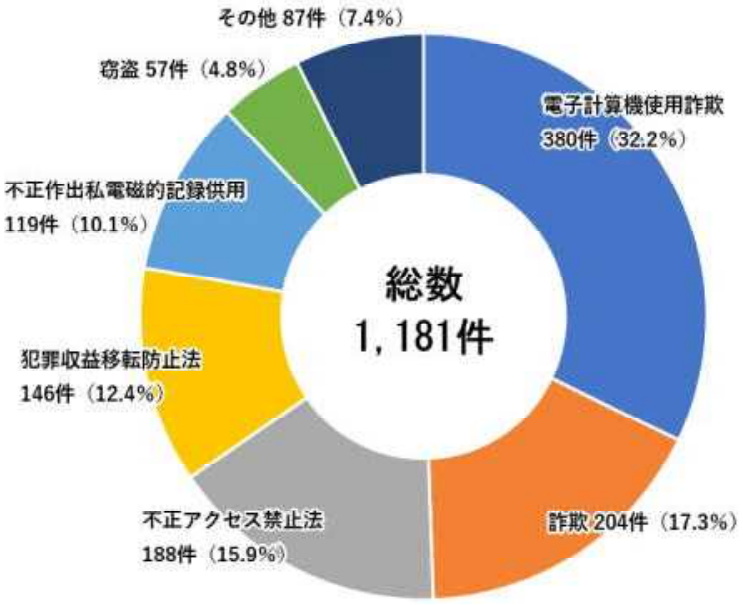
【図表45：事案の概要】

２　サイバー事案の検挙状況

(1)　サイバー事案の検挙状況

令和５年上半期のサイバー事案の検挙件数は、1,181件であった。

【図表46：サイバー事案の検挙状況】



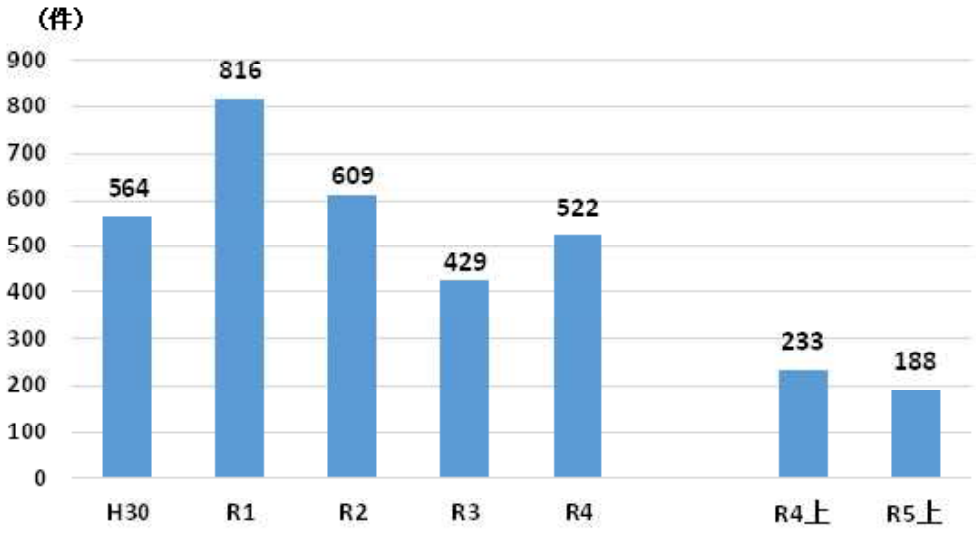
注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

(2)　不正アクセス禁止法違反の検挙件数、特徴

ア　検挙件数

令和５年上半期における不正アクセス禁止法違反の検挙件数は、188件と前年同期と比べて45件減少した。

【図表47：不正アクセス禁止法違反の検挙件数の推移】



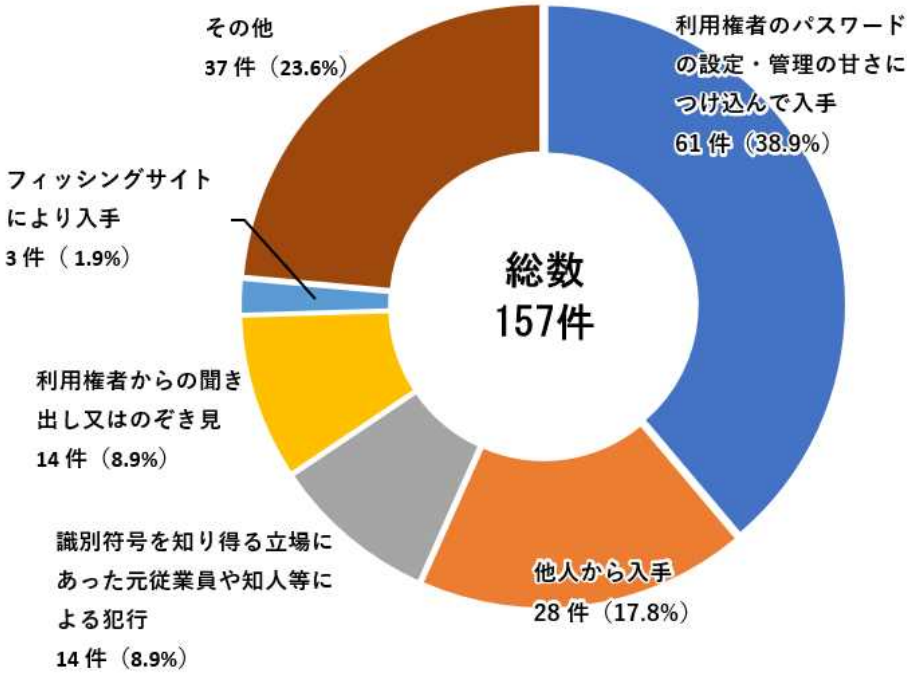
イ　特徴

検挙件数のうち、157件が識別符号窃用型で全体の83.5%を占めた。

○　「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が最多

識別符号窃用型の不正アクセス行為に係る手口では、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が61件と最も多く、全体の38.9%を占めており、次いで「他人から入手」が28件で全体の17.8%を占めた。

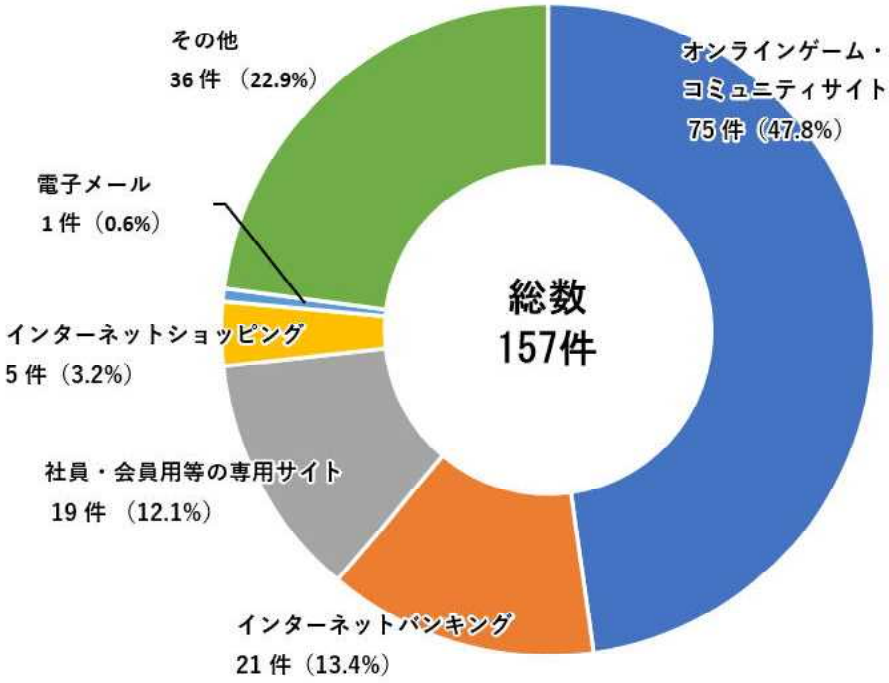
【図表48：不正アクセス行為（識別符号窃用型）に係る手口別検挙件数】



○　被疑者が不正に利用したサービスは「オンラインゲーム・コミュニティサイト」が最多

識別符号窃用型の不正アクセス行為に係る被疑者が不正に利用したサービスは、「オンラインゲーム・コミュニティサイト」が75件と最も多く、全体の47.8％を占めており、次いで「インターネットバンキング」が21件で全体の13.4％を占めた。

【図表49：不正に利用されたサービス別検挙件数（識別符号窃用型）】



ウ　検挙事例

○　会社員の男（33）は、令和４年６月、元勤務先Ａ社の社員に割り当てられた識別符号を使用して、Ａ社が管理するサーバに不正アクセスした上、サーバ内のデータを削除してＡ社の業務を妨害した。令和５年１月、男を不正アクセス禁止法違反、電子計算機損壊等業務妨害罪で検挙した。

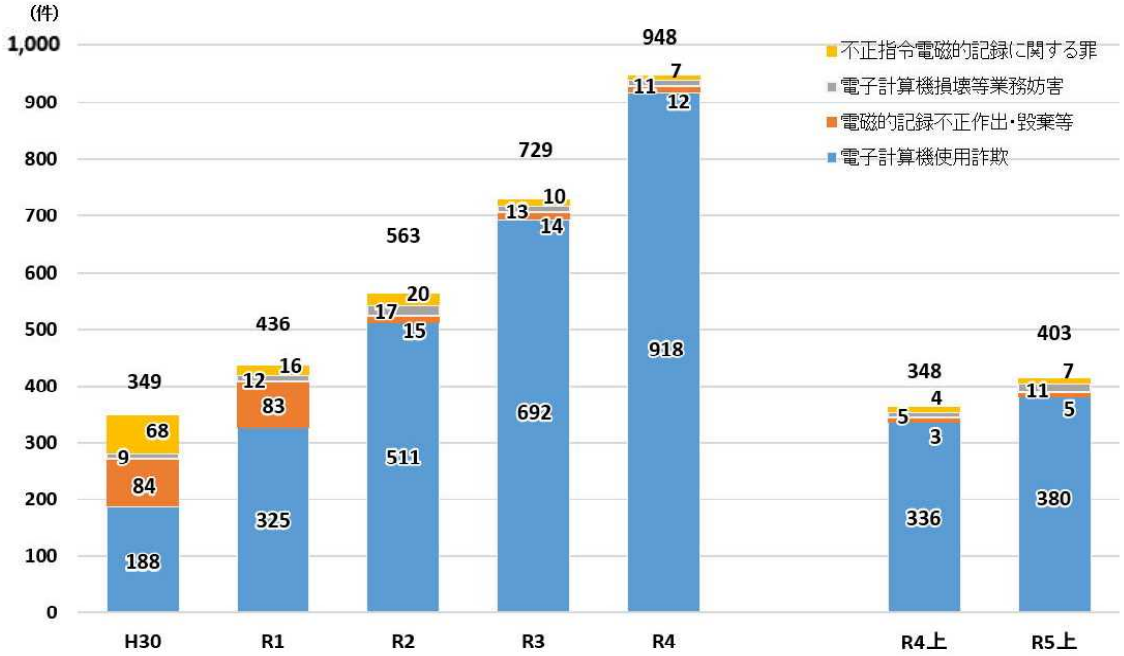
○　会社員の男（30）は、令和２年10月、他人のインターネットバンキング口座から不正に送金する目的で、ＳＮＳで口座名義人に融資話を持ちかけてログイン情報をだまし取り、当該口座から約20万円を他人名義の口座に送金した。令和５年１月、男を不正アクセス禁止法違反、電子計算機使用詐欺罪で検挙した。

(3)　コンピュータ・電磁的記録対象犯罪の検挙件数、特徴

ア　検挙件数

令和５年上半期におけるコンピュータ・電磁的記録対象犯罪の検挙件数は403件で、前年同期と比べて55件増加した。

【図表50：コンピュータ・電磁的記録対象犯罪の検挙件数の推移】



イ　特徴

検挙件数のうち、電子計算機使用詐欺が380件と最も多く、全体の94.3％を占めた。

ウ　検挙事例

○　地方公務員（逮捕時：無職）の女（30）は、令和４年12月、他人の個人番号カードを不正に使用して、同名義人になりすまし、マイナポイントの事務処理に使用するサーバに対し、自身が利用するキャッシュレス決済サービスにマイナポイントを付与させる旨の虚偽の申し込みを行った。令和５年４月、女を公電磁的記録不正作出・同供用罪等で検挙した。

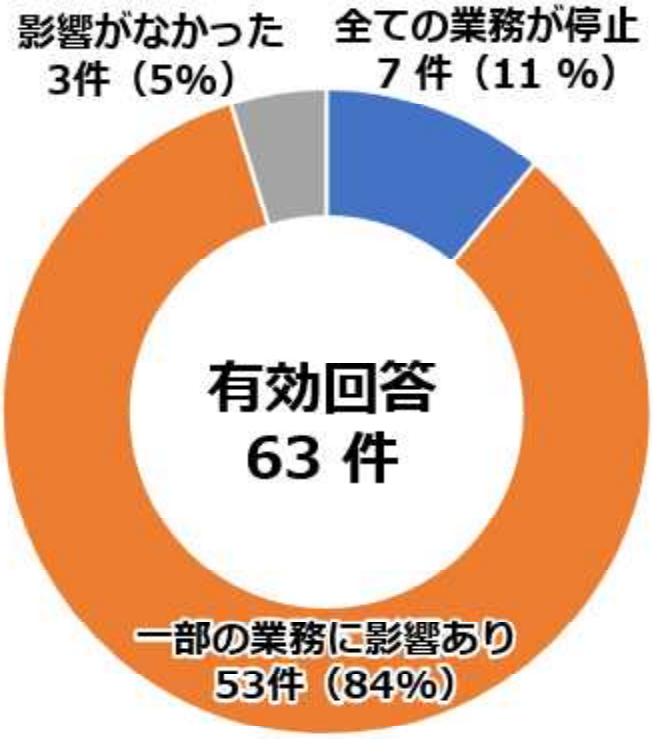
○　会社役員の男（27）ほか３名は、令和３年12月、フリーマーケットサイトのアカウント作成に必要な本人確認を行うに当たり、同サイト運営会社のサーバに対し、本来の利用者とは異なる携帯電話番号及び認証コードを記録させ、その事務処理を誤らせた。令和５年３月、同４名を私電磁的記録不正作出・同供用罪で検挙した。

○　建設作業員の男（37）は、令和４年６月、氏名不詳者と共謀のうえ、他人のインターネットバンキング口座から不正に送金する目的で、電話工事業者を装って口座名義人方に上がり込み、固定電話を使用して、送金を可能とするためのワンタイムパスワード有効化手続等をすることで、約500万円を他人名義の口座に送金した。令和５年４月、男を住居侵入罪、電子計算機使用詐欺罪で検挙した。

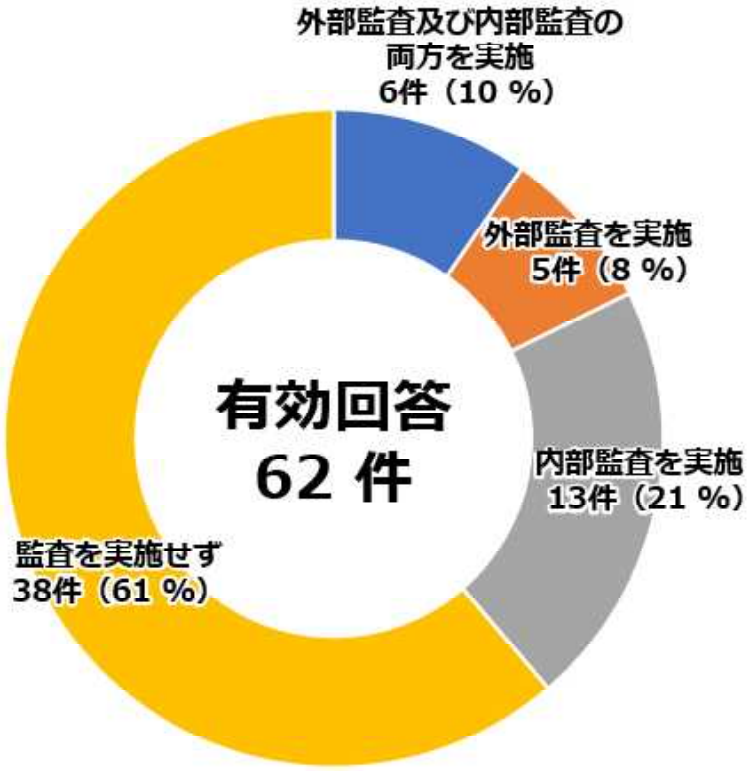
参考

1　企業・団体等におけるランサムウェア被害及びその実態

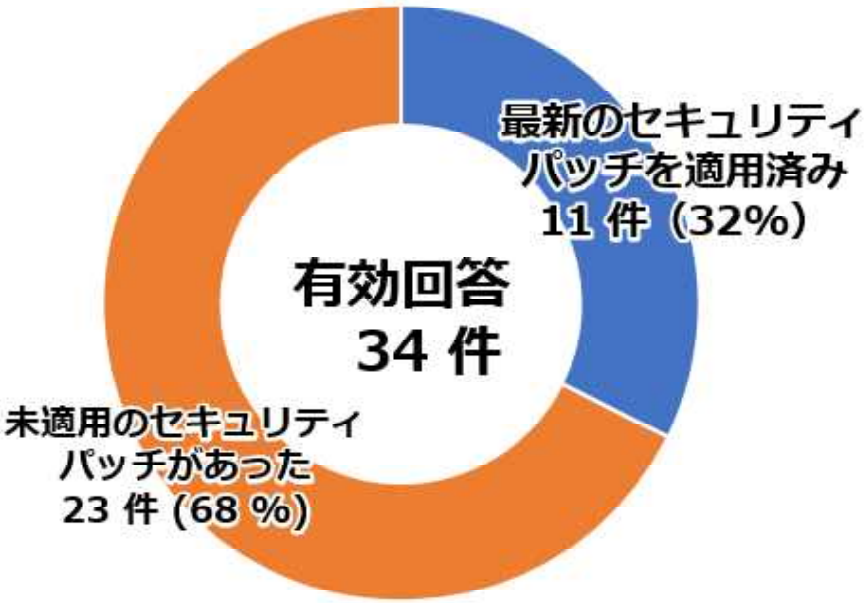
(1)　ランサムウェア被害が業務に与えた影響



(2)　被害企業・団体の情報セキュリティ監査の実施状況

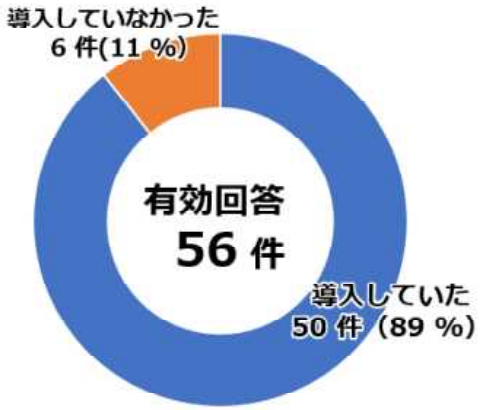


(3)　侵入経路とされる機器のセキュリティパッチの適用状況

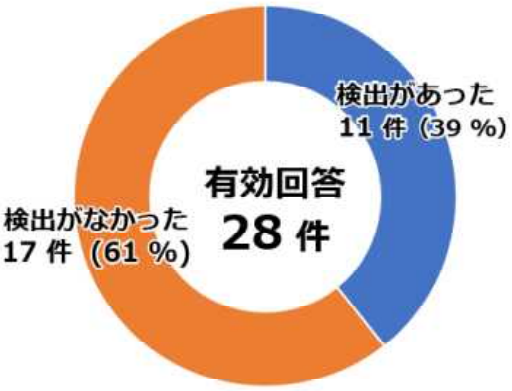


(4)　被害企業・団体等のウイルス対策ソフト等導入・活用状況

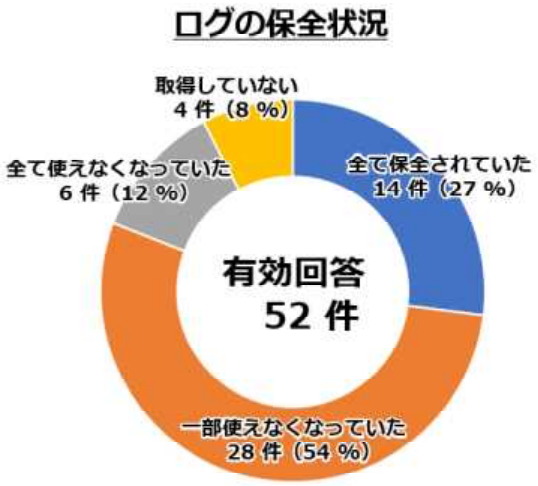
導入状況



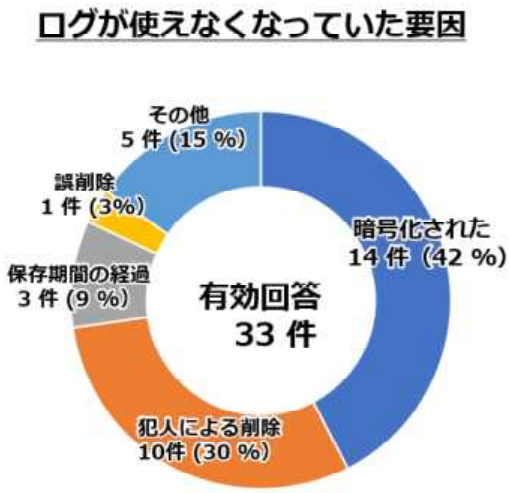
検出の有無



(5)　ランサムウェア被害における被害企業・団体等のログの保全状況

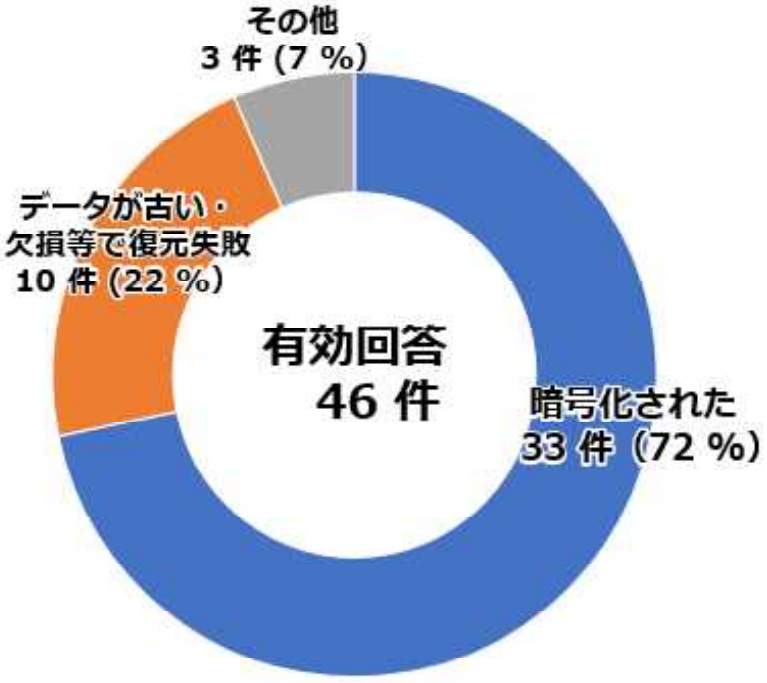


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

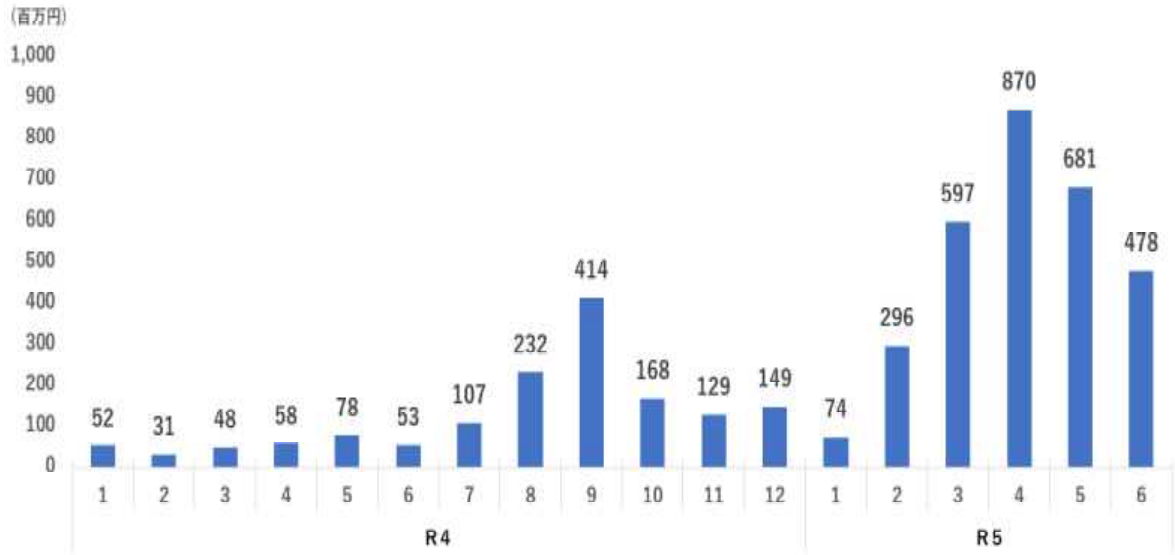
(6)　被害企業・団体のバックアップから復元できなかった理由



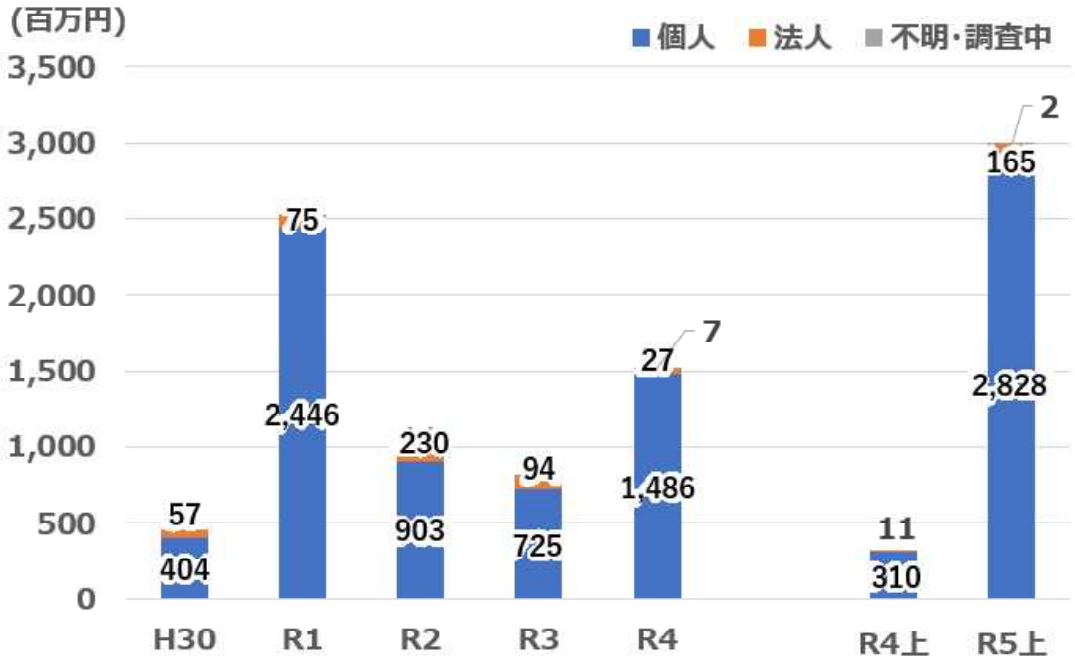
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

2　インターネットバンキングに係る不正送金事犯の発生状況

(1)　被害額の推移

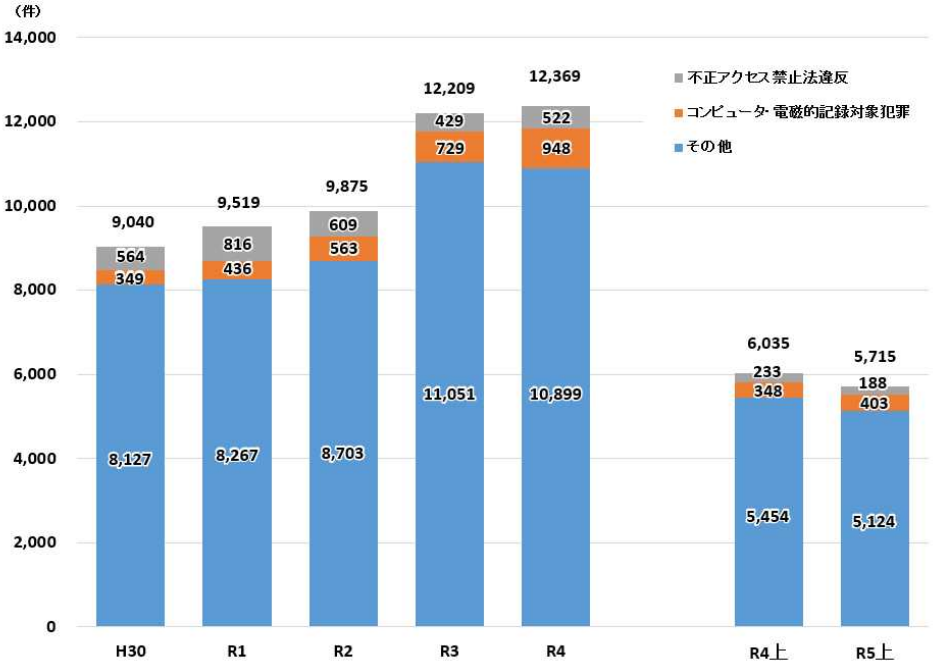


(2)　口座開設者別の被害状況

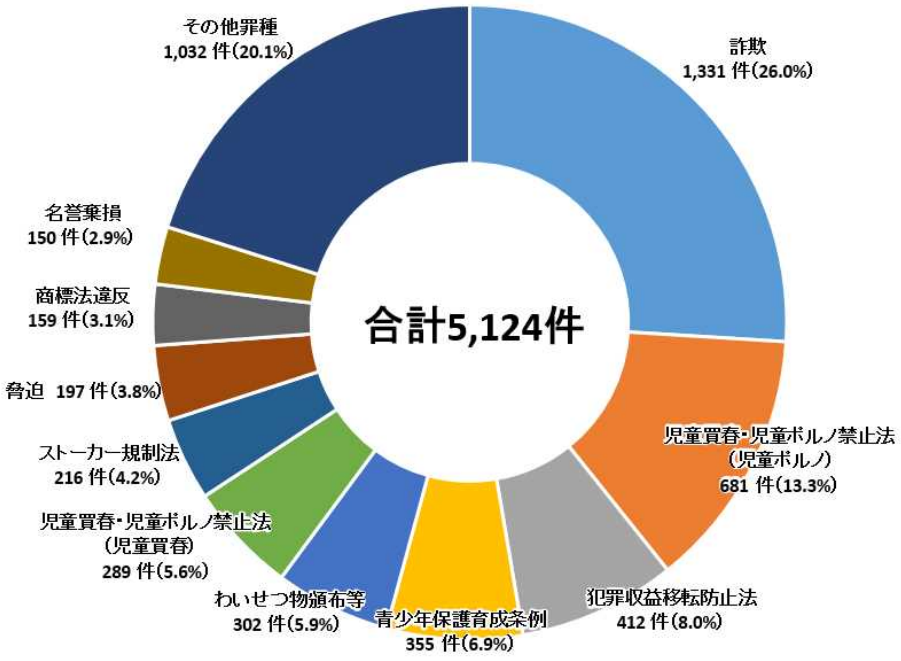


3　サイバー犯罪[*1]の検挙状況

(1)　サイバー犯罪の検挙件数の推移



(2)　その他の検挙状況[*2]



注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

---

*1　サイバー犯罪とは、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪。

*2　その他の検挙状況は、サイバー犯罪の検挙状況から不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪の検挙を除いたもの。