広　報　資　料
令和６年３月14日
サイバー企画課

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

１　概要

令和５年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　行政機関、学術研究機関等において情報窃取を企図したとみられる不正アクセス等が多数発生した。

⑵　令和５年１月から９月までのクレジットカード不正利用被害額は、同期比で過去最多（401.9億円）となった。また、令和５年のインターネットバンキングに係る不正送金被害は、発生件数、被害総額ともに過去最多（5,578件、約87.3億円）となった。

⑶　ランサムウェア被害の件数が197件と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30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）、米国連邦捜査局（ＦＢＩ）等とともに、中国を背景とするサイバー攻撃グループBlackTechによるサイバー攻撃に関する合同の注意喚起（パブリック・アトリビューション）を実施した。

⑵　有識者による「キャッシュレス社会の安全・安心の確保に関する検討会」を開催し、クレジットカード不正利用等の被害に遭わないための環境整備や警察の対処能力向上について検討を進めた。また、金融庁と連携し、金融機関における、暗号資産交換業者への不正送金対策の強化に関し調整を進めた。（本年２月に要請実施）

⑶　サイバー特別捜査隊等がEUROPOL（ユーロポール）等との国際共同捜査を推進した結果、令和６年２月、関係国捜査機関が、世界各国の企業等に対してランサムウェア被害を与えた攻撃グループ「LockBit（ロックビット）」の一員とみられる被疑者２名を逮捕した。

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

令和６年３月14日
警察庁

はじめに

本資料は、令和５年中の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年における脅威情勢の要点」では、令和５年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、「国家を背景とするサイバー攻撃」、「クレジットカード不正利用・インターネットバンキングに係る不正送金」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、被害が深刻であ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、「国際共同捜査によるランサムウェア事案被疑者の検挙」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年における脅威情勢の要点

１　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。

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

○　情報窃取を企図した不正アクセス等

行政機関、学術研究機関、民間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。

○　重要インフラ等の機能に影響を及ぼしたサイバー攻撃

重要インフラ等の機能に障害を発生させ、社会経済活動に影響を及ぼすサイバー攻撃が発生した。

○　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　BlackTechに対するパブリック・アトリビューション】

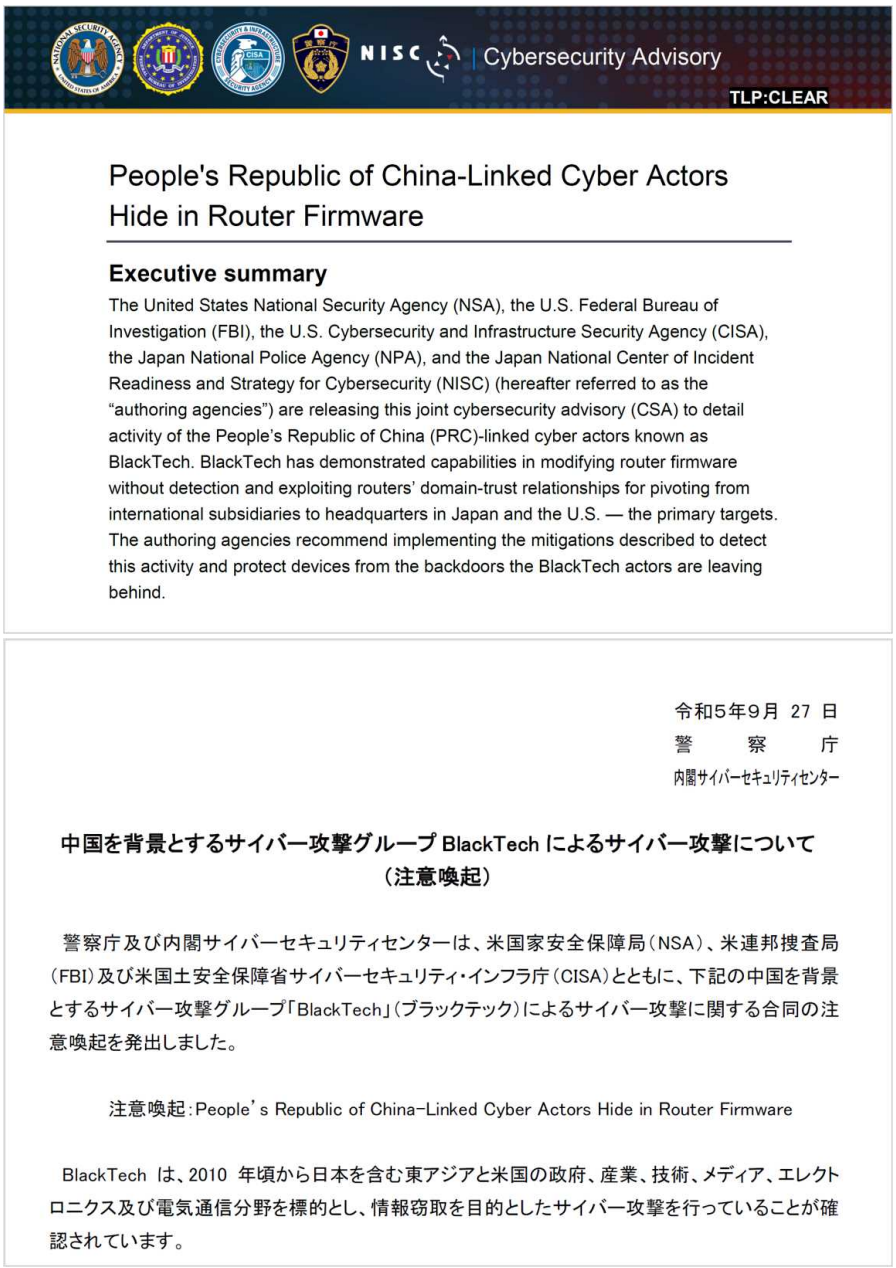
令和５年９月、警察庁は、内閣サイバーセキュリティセンター（ＮＩＳＣ）、米国国家安全保障局（ＮＳＡ）、米国連邦捜査局（ＦＢＩ）及び米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（ＣＩＳＡ）とともに、中国を背景とするサイバー攻撃グループBlackTechによるサイバー攻撃に関する合同の注意喚起を実施した。

【内容】

① BlackTechが、平成22年頃から日本を含む東アジアと米国の政府機関や工業、科学技術、メディア、エレクトロニクス、電気通信分野の事業者を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認された。

② BlackTechによるサイバー攻撃の手口を公表した上で、標的となる可能性のある組織や事業者に、サイバー攻撃の被害拡大を防止するための適切なセキュリティ対策を講じることや、ネットワークの不審な通信を検知した際には所管省庁、警察、セキュリティ関係機関等へ速やかに情報提供することなどを呼び掛けた。

【図表１：BlackTechに関する注意喚起（上：日米合同、下：国内向け）（冒頭抜粋）】



Cybersecurity Advisory

TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the "authoring agencies") are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S. — the primary targets. The authoring agencies recommend implementing the mitigations described to detect this activity and protect devices from the backdoors the BlackTech actors are leaving behind.

令和5年9月 27 日
警　　察　　庁
内閣サイバーセキュリティセンター

中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について
（注意喚起）

警察庁及び内閣サイバーセキュリティセンターは、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、下記の中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出しました。

注意喚起：People's Republic of China-Linked Cyber Actors Hide in Router Firmware

BlackTech は、2010 年頃から日本を含む東アジアと米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認されています。

(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119万6,390件（前年比で23.5%増加）と過去最多であり、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５年１月から９月までのクレジットカード不正利用被害額は401.9億円（前年同期比で30.1%増加）であり、統計を取り始めた平成９年以降、最悪となった。

○　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5,578件（前年比で391.0％増加）であり、過去最多となり、被害総額も約87.3億円（前年比で474.6％増加）であり、過去最多となった。

【トピック２　クレジットカード不正利用、インターネットバンキングに係る不正送金事犯等に関する対策】

１　キャッシュレス社会の安全・安心の確保に関する検討会の開催

我が国における重要な社会基盤であるクレジットカードやインターネットバンキングに関する被害が過去最多となっているなど、キャッシュレス社会の安全・安心の確保は喫緊の課題となっている。

こうした状況を踏まえ、官民の更なる連携によりクレジットカードの不正利用被害等に関する効果的な対策を講じるため、有識者から多様な観点で議論していただくことを目的として、「キャッシュレス社会の安全・安心の確保に関する検討会」を開催し、被害に遭わないための環境整備や警察の対処能力向上について検討している。

２　暗号資産交換業者への不正送金対策の強化に関する金融機関への要請

昨今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よる不正送金事犯や特殊詐欺事犯において、暗号資産交換業者の金融機関口座が送金先となる被害が多発している状況を踏まえ、金融庁と連携し、一般社団法人全国銀行協会等に対して、暗号資産交換業者の金融機関口座に対して送金元口座名義人名と異なる依頼人名で行われる送金の拒否、暗号資産交換業者への不正な送金への監視強化等の、会員等における対策強化を要請するよう調整を進めた。（令和６年２月実施）

(3)　ランサムウェア被害の情勢等

令和５年におけるランサムウェアによる被害件数は197件（前年比で14.3％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。

【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[*1]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9,144.6件（前年比で18.6％増加）と、平成23年以降、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情報が容易に入手できる状況にある。また、犯罪実行者募集情報[*2]が氾濫しており、これらに応募した者等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例も出ているところである。

【トピック３　重要犯罪密接関連情報[*3]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追加した。加えて、令和５年９月、犯罪実行者募集情報を同範囲に追加するなど、爆発物・銃砲等の重要犯罪密接関連情報に関する対策を強化した。

また、ＣＰＣにおける重要犯罪密接関連情報に関す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を導入し、令

---

*1　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。

*2　著しく高額な報酬の支払を示唆して行う犯罪の実行者を直接的かつ明示的に誘引等（募集）する情報（具体的な仕事の内容を明らかにせずに人を募集する投稿であっても、当該投稿や前後の内容、社会的情勢やその他の事情から、社会通念上、重要犯罪に発展する危険性がある犯罪の実行者の募集を誘引等するものと認められる場合を含む。）

*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次の情報
①拳銃等の譲渡等、②爆発物・銃砲等の製造、③殺人等（殺人、強盗、不同意性交等、放火、誘拐、傷害、逮捕・監禁、脅迫）、④臓器売買、⑤人身売買、⑥硫化水素ガスの製造、⑦ストーカー行為等、⑧犯罪実行者募集情報

和５年９月から運用を開始した。

○　重要犯罪密接関連情報の取扱状況

ＩＨＣの運用ガイドラインに基づき、令和５年２月15日から12月31日までの間、重要犯罪密接関連情報と判断し分析した情報は4,876件であり、3,379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、2,411件（71.4％）が削除に至った。このうち、令和５年９月29日から12月31日までの間、犯罪実行者募集情報と判断し分析した情報は4,411件であり、2,979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、2,136件（71.7％）が削除に至った。

【図表２：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	15	10	8
爆発物・銃砲等の製造	16	15	7
殺人・強盗等の勧誘	411	356	252
臓器売買	18	16	5
人身売買	0	0	0
硫化水素ガスの製造	2	1	1
ストーカー行為等	3	2	2
犯罪実行者募集	4,411	2,979	2,136
合計	**4,876**	**3,379**	**2,411**

※　削除完了件数は、令和６年１月末に確認した状況を計上

３　サイバー事案[*4]の検挙状況

(1)　サイバー事案の検挙件数

令和５年中におけるサイバー事案の検挙件数は、3,003件であった。

(2)　不正アクセス禁止法違反[*5]の検挙件数及び特徴

令和５年中における不正アクセス禁止法違反の検挙件数は、521件（前年比で0.2％減少）であり、そのうち475件が識別符号窃用型[*6]で全体の91.2％を占める。

(3)　コンピュータ・電磁的記録対象犯罪[*7]の検挙件数及び特徴

令和５年中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、1,000件（前年比で5.5％増加）であり、そのうち950件が電子計算機使用詐欺で全体の95.0％を占める。

【トピック４　外国捜査機関等と連携したランサムウェア事案被疑者の検挙等】

我が国を含め世界各国の企業等に対してランサムウェア被害を与えている攻撃グループ「LockBit（ロックビット）」について、サイバー特別捜査隊等がEUROPOL（ユーロポール）[*8]等との国際共同捜査を推進した結果、令和６年２月、関係国捜査機関が、同グループの一員とみられる被疑者２名を逮捕するとともに、同グループが使用するサーバ等のテイクダウン（機能停止）を実施し、流出した情報等が掲載されていたリークサイト上に、テイクダウンの実施を告げる「スプラッシュページ」を表示させた。

この事案では、サイバー特別捜査隊が、ランサムウェアLockBitによって暗号化された被害データを復号するツールを独自開発し、令

---

*4　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。

*5　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。）

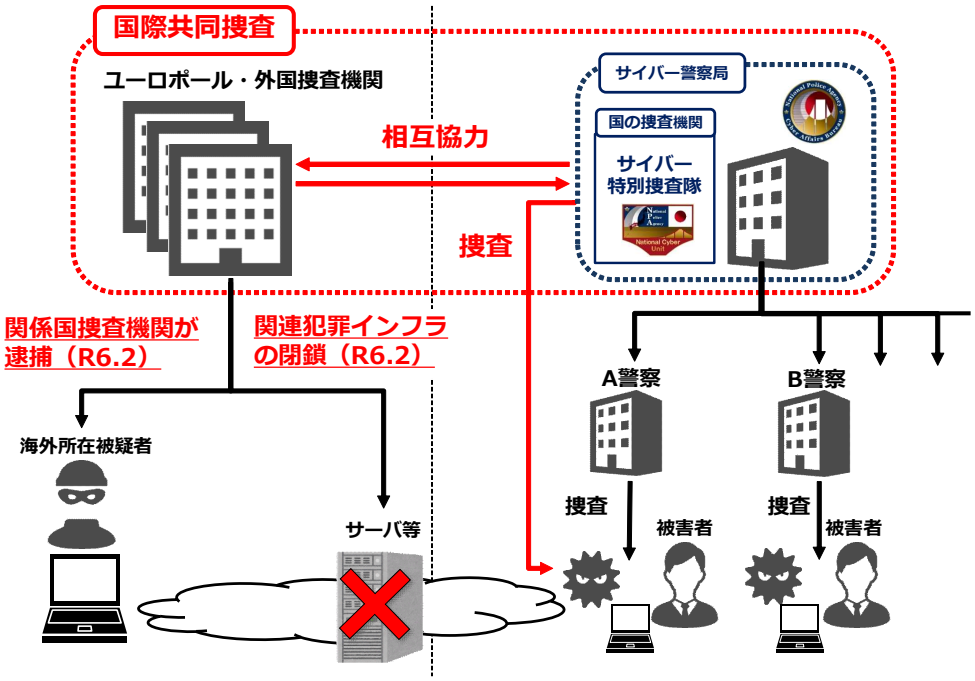
*6　不正アクセス行為は、他人の識別符号を無断で入力する「識別符号窃用型」と、アクセス制御機能による特定利用の制限を免れる情報（識別符号を除く）又は指令を入力する「セキュリティ・ホール攻撃型」に分類することができる。

*7　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

*8　European Union Agency for Law Enforcement Cooperationを指す。欧州連合（EU）の法執行機関であるが、捜査権限はなく、加盟国間の情報交換の促進や収集した情報の分析等が主な任務である。

和５年12月に同ツールをユーロポールに提供しており、令和６年２月、世界中の被害企業等の被害回復が可能となるよう、ユーロポール等と共に警察庁において、日本警察が開発した復号ツールについて情報発信し、その活用を促す旨の発表を行った。

【図表３：事案の概要】



第２部　脅威の情勢

１　サイバー攻撃の情勢等

(1)　情報窃取を企図した不正アクセスの事例

令和５年、情報窃取を企図したとみられる不正アクセス事案が数多く発生した。主な事例は、以下のとおりである。

○　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。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。

○　８月以降、複数の行政機関等は、電子メール関連システムに関係する機器のぜい弱性を悪用したとみられる不正アクセスを受け、メールデータの一部が外部に漏えいした可能性があると発表した。

○　10月、国内の学術研究機関は、職員が使用するコンピュータが標的型メール攻撃によりマルウェアに感染した結果、不正アクセスを受け、同年５月頃に個人情報等が漏えいした可能性があると発表した。

○　11月、国内の宇宙航空分野の研究開発機関は、同年夏頃に組織内のイントラネットの管理用サーバに不正アクセスが行われた可能性があることを明らかにした。

(2)　重要インフラ等の機能に影響を及ぼしたサイバー攻撃の事例

令和５年、重要インフラ等の機能に障害を発生させ、社会経済活動に影響を及ぼすサイバー攻撃が発生した。主な事例は、以下のとおりである。

○　６月、住宅設備関連機器メーカーは、同社が運営するクラウドシステムのサーバが不正アクセスを受け、攻撃者がサーバのデータを破壊し、停止させた結果、クラウドサービスが停止したと発表した。このクラウドシステムを使用する全国約1,000のLPガス会社において、検針業務が行えなくなるなどの影響が生じた。

○　７月、名古屋港運協会は、名古屋港のコンテナターミナルにおけるコンテナの船積み・船卸や搬出入の作業等を一元的に管理するシステムがランサムウェアに感染し、同システムのサーバのデータが暗号化され、システム障害が発生したと発表した。これにより、同ターミナルにおけるコンテナの搬出入等が約３日間停止し、物流に大きな影響が生じた。

(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、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した。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した。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。

○　８月、政府機関、自治体等が運営するウェブサイトにおいて閲覧障害が発生した。同じ頃、ＳＮＳ上に、ハクティビストのものと思われる複数のアカウントから、それらの犯行をほのめかす投稿が確認された。

○　10月以降、事業者等のウェブサイトで閲覧障害が発生したほか、小規模サービス事業者が運営するウェブサイトが書き換えられる事案が発生した。それらの発生と同じ頃、ＳＮＳ上に、反イスラエルを掲げるハクティビストのものと思われるアカウントから、それらの犯行をほのめかす投稿が確認された。

(4)　標的型メール攻撃の傾向・事例

ア　傾向

令和５年、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、実在する人物になりすましてメールを送り、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(5)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。

---

*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）

○　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。

(5)　対処状況

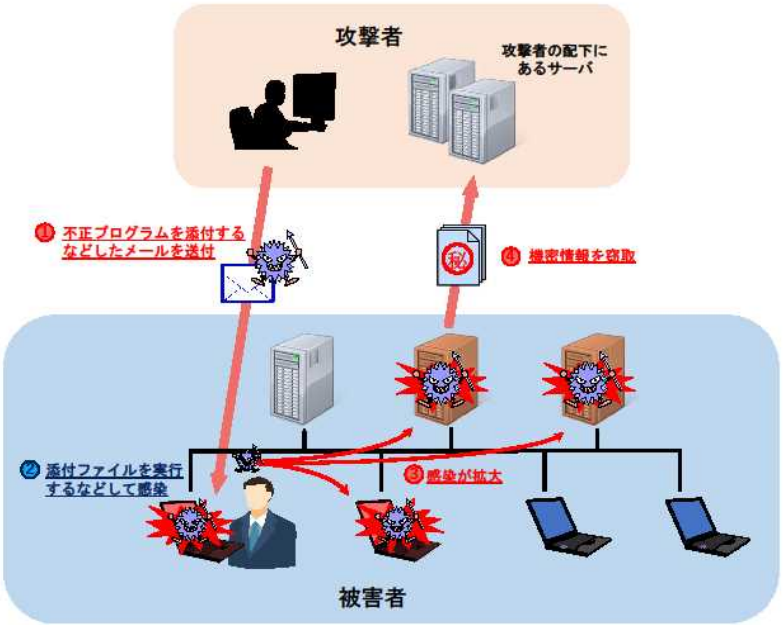
○　共同対処訓練の実施

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約700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。

○　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12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４：標的型メール攻撃による情報窃取の例】



○　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ている。

○　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年には、ネットワーク機器やソフトウェア等の重大なぜい弱性を悪用したサイバー攻撃の手口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。

○　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。

○　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い、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等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すとともに、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。

○　BlackTechに対するパブリック・アトリビューション

中国を背景とするサイバー攻撃グループBlackTechが、平成22年頃から日本を含む東アジアと米国の政府機関や工業、科学技術、メディア、エレクトロニクス、電気通信分野の事業者を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認された。

このことを受け、令和５年９月、警察庁は、ＮＩＳＣ、ＮＳＡ、ＦＢＩ及びＣＩＳＡとともに、BlackTechによるサイバー攻撃に関する合同の注意喚起を実施した。

BlackTechによるサイバー攻撃の手口を公表した上で、標的となる可能性のある組織や事業者にサイバー攻撃の被害拡大を防止するための適切なセキュリティ対策を講じることや、ネットワークの不審な通信を検知した際には所管省庁、警察、セキュリティ関係機関等へ速やかに情報提供することなどを呼び掛けた。

【図表５：BlackTechに関する注意喚起（上：日米合同、下：国内向け）（冒頭抜粋）】

NISC | Cybersecurity Advisory

TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the "authoring agencies") are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S. — the primary targets. The authoring agencies recommend implementing the mitigations described to detect this activity and protect devices from the backdoors the BlackTech actors are leaving behind.

令和５年９月 27 日
警　　察　　庁
内閣サイバーセキュリティセンター

中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について（注意喚起）

警察庁及び内閣サイバーセキュリティセンターは、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、下記の中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出しました。

注意喚起：People's Republic of China-Linked Cyber Actors Hide in Router Firmware

BlackTech は、2010 年頃から日本を含む東アジアと米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認されています。

(6)　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。

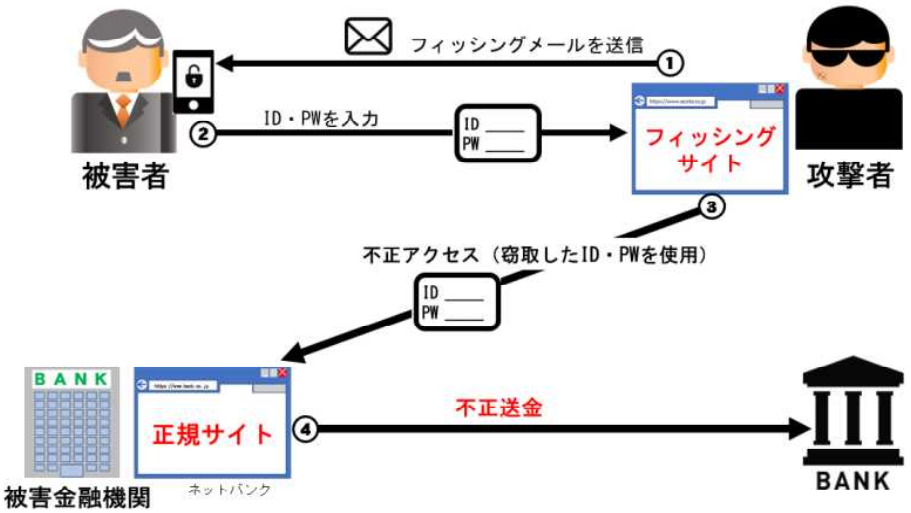
こうした取組の結果、広島市ウェブサイトにおいてDDoS攻撃によるものとみられる閲覧障害が発生するなど、Ｇ７広島サミット等開催期間中におけるサイバー攻撃事案が発生したが、Ｇ７広島サミット等の進行に影響を及ぼすようなサイバー攻撃の発生はなかった。

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。

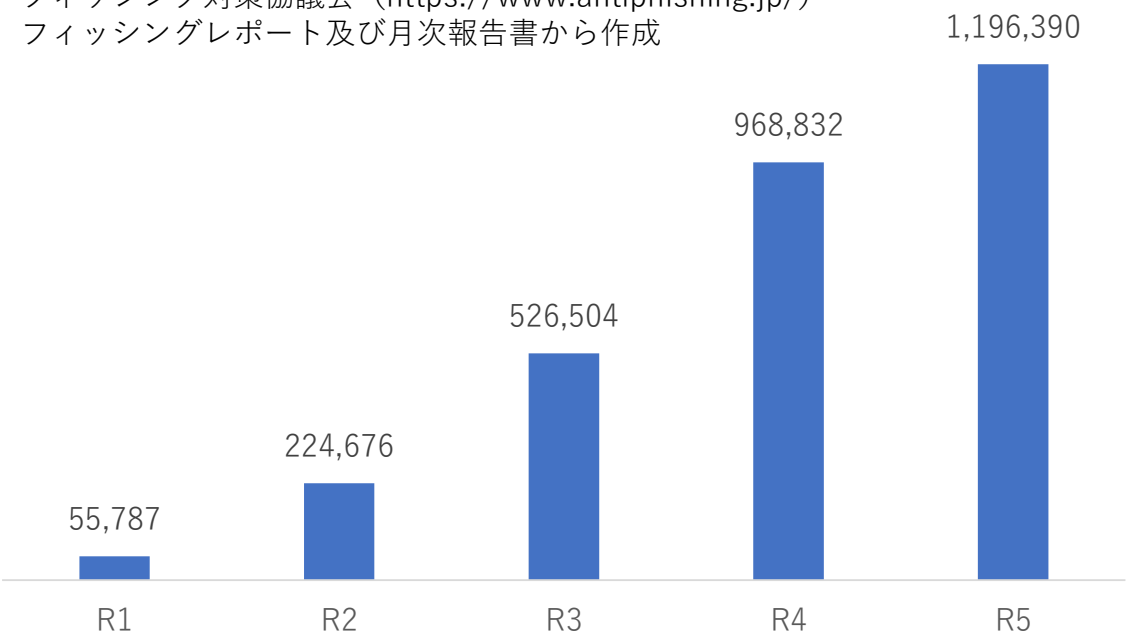
【図表６：不正送金の概要】



令和５年における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、119万6,390件（前年比で22万7,558件増加）であり、過去最多となった。また、フィッシングで多くを占めたのは、クレジットカード事業者、ＥＣ事業者をかたるものであった。

【図表７：フィッシング報告件数の推移】

フィッシング対策協議会（https://www.antiphishing.jp/）
フィッシングレポート及び月次報告書から作成

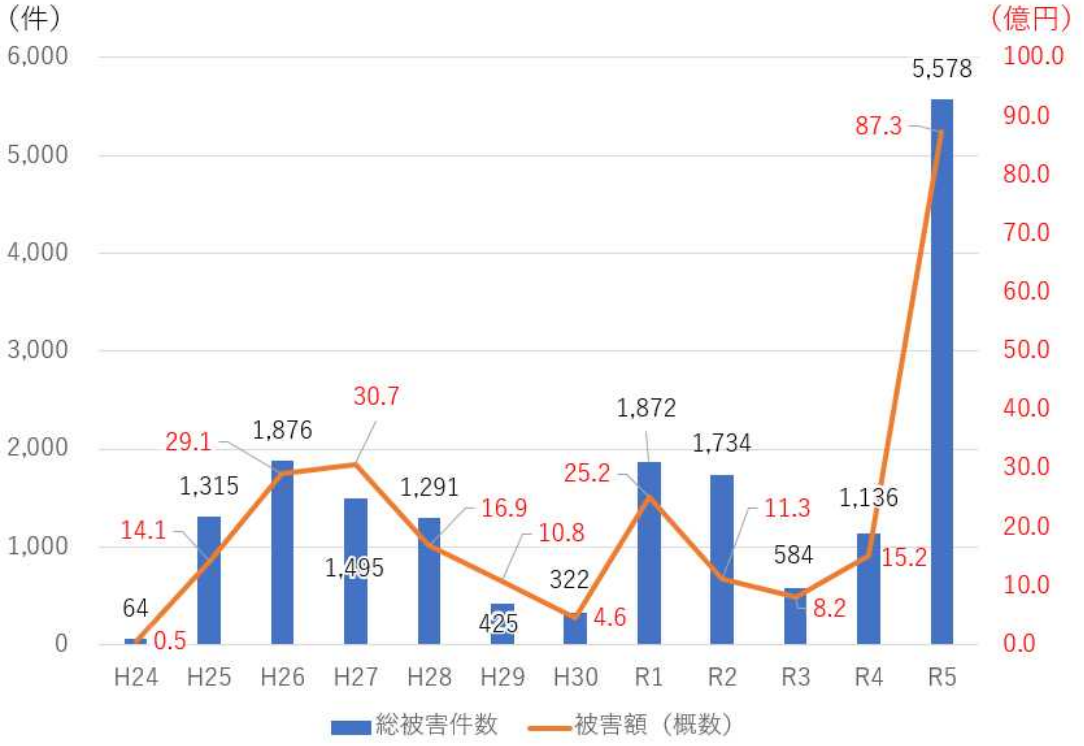


【図表８：実在する金融機関・通信事業者等のログイン画面を模した偽画面の例】

(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

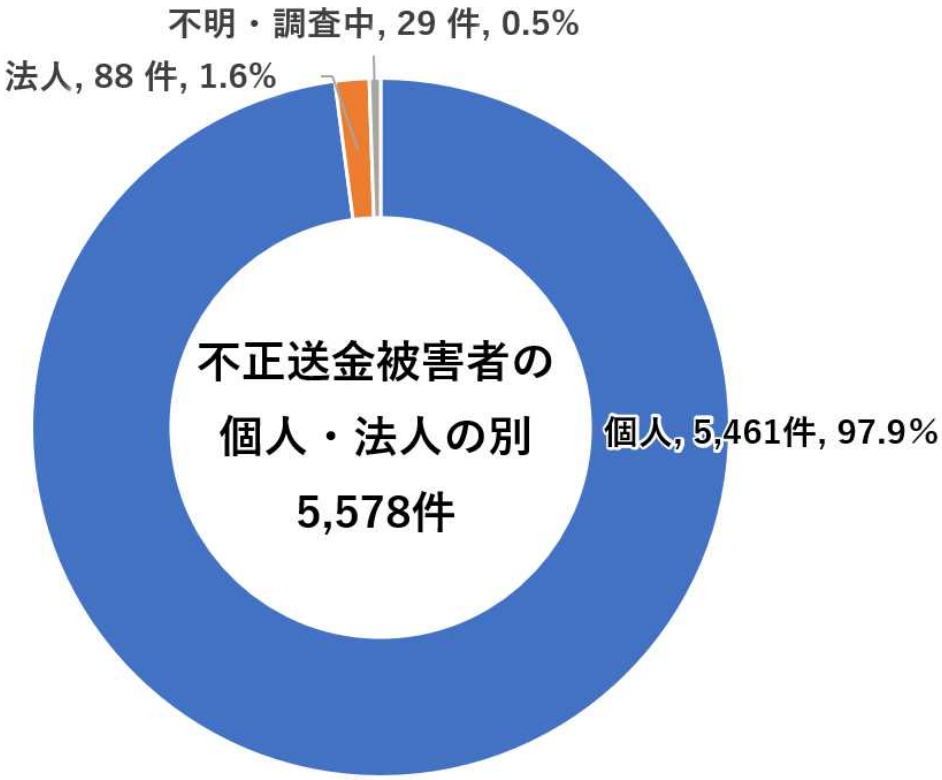
令和５年におけるインターネットバンキングに係る不正送金事犯の発生件数は5,578件、被害総額は約87億3,130万円であり、それぞれ過去最多となっている。

【図表９：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】

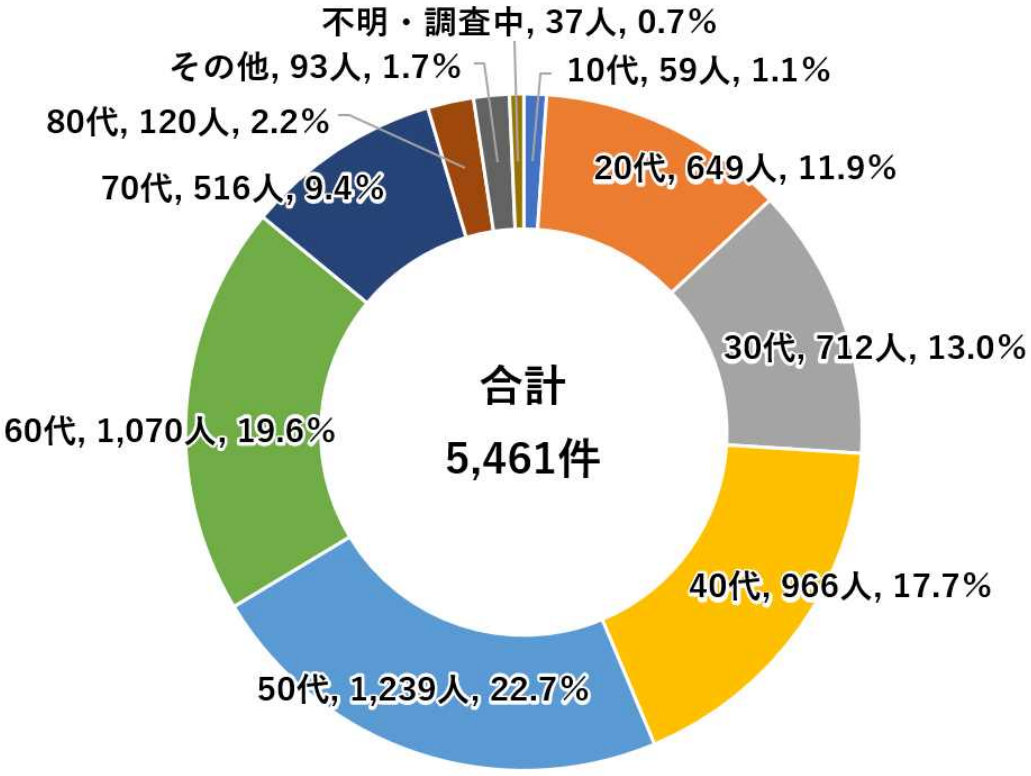


また、被害者の大部分は個人であり（5,461件、97.9%）、そのうち40代から60代の被害者が約６割を占めている。

【図表10：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】

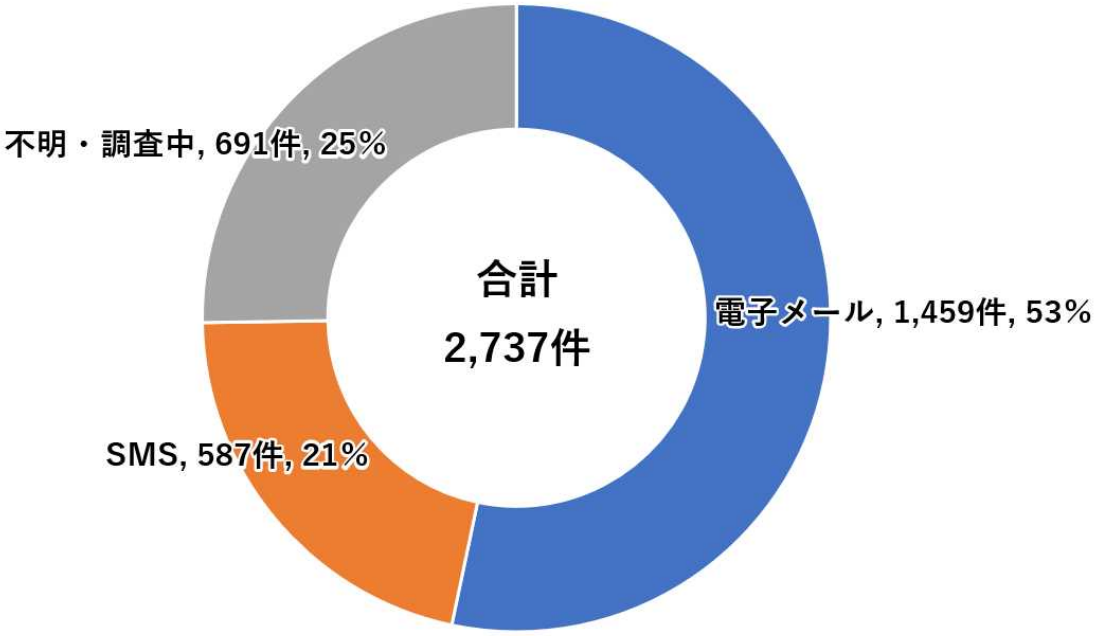


【図表11：個人のインターネットバンキングに係る不正送金被害者の年齢別割合】



さらに、インターネットバンキングに係る不正送金事犯において用いられたフィッシングの手口の内訳を見ると、電子メールによる誘導が53%、ＳＭＳによる誘導が21%である。

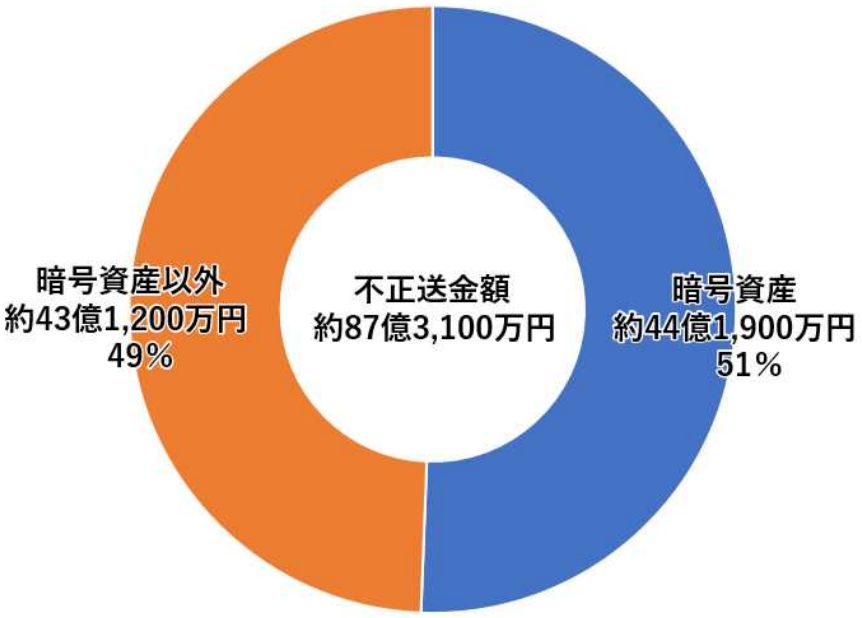
【図表12：フィッシングサイトへ誘導する手口別割合】



注　図中の割合は小数第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。

また、不正送金額の半額以上が暗号資産交換業者の金融機関口座に不正送金されている状況にある。

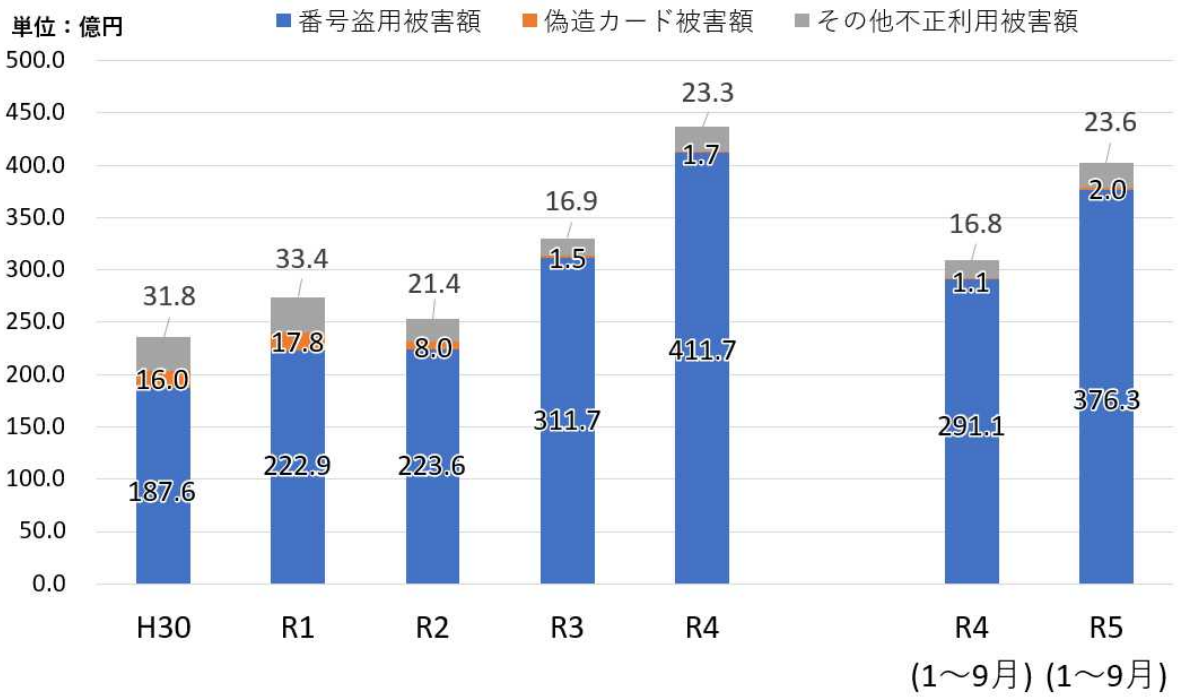
【図表13：暗号資産交換業者の金融機関口座への送金状況】



(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５年１月から９月までの被害額は401.9億円で、統計を取り始めた平成９年以降、最悪となった。前年同期比（令和４年第３四半期（令和４年１月～同年９月））では30.1%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。

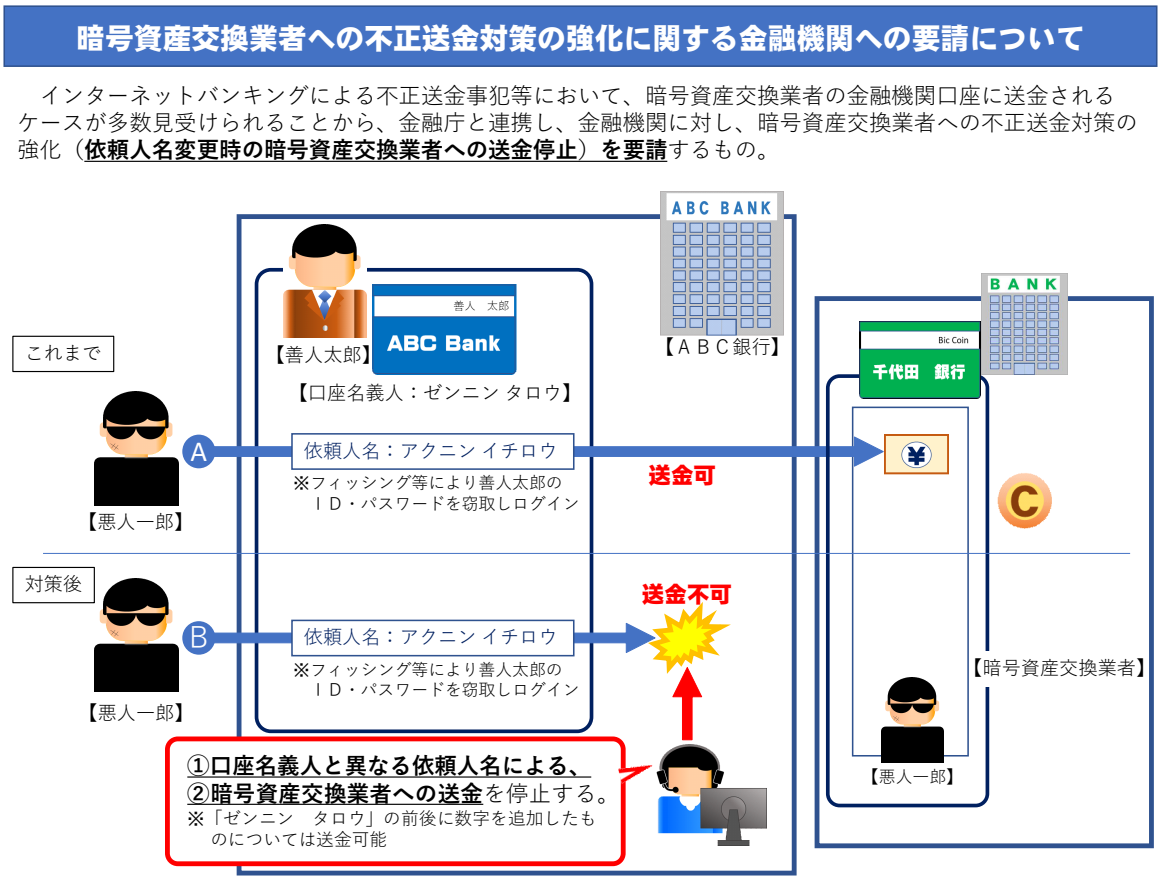
我が国における重要な社会基盤であるクレジットカードやインターネットバンキングに関する被害が過去最多となっているなど、キャッシュレス社会の安全・安心の確保は喫緊の課題となっている。

こうした状況を踏まえ、官民の更なる連携によりクレジットカードの不正利用被害等に関する効果的な対策を講じるため、有識者から多様な観点で議論していただくことを目的として、「キャッシュレス社会の安全

・安心の確保に関する検討会」を開催し、被害に遭わないための環境整備や警察の対処能力向上について検討している。

昨今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よる不正送金事犯や特殊詐欺事犯において、暗号資産交換業者の金融機関口座が送金先となる被害が多発している状況を踏まえ、金融庁と連携し、一般社団法人全国銀行協会等に対して、暗号資産交換業者の金融機関口座に対して送金元口座名義人名と異なる依頼人名で行われる送金の拒否、暗号資産交換業者への不正な送金への監視強化等の、会員等における対策強化を要請するよう調整を進めた。（令和６年２月実施）

【図表15：暗号資産交換業者への不正送金対策の強化に関する金融機関への要請について】



○　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。

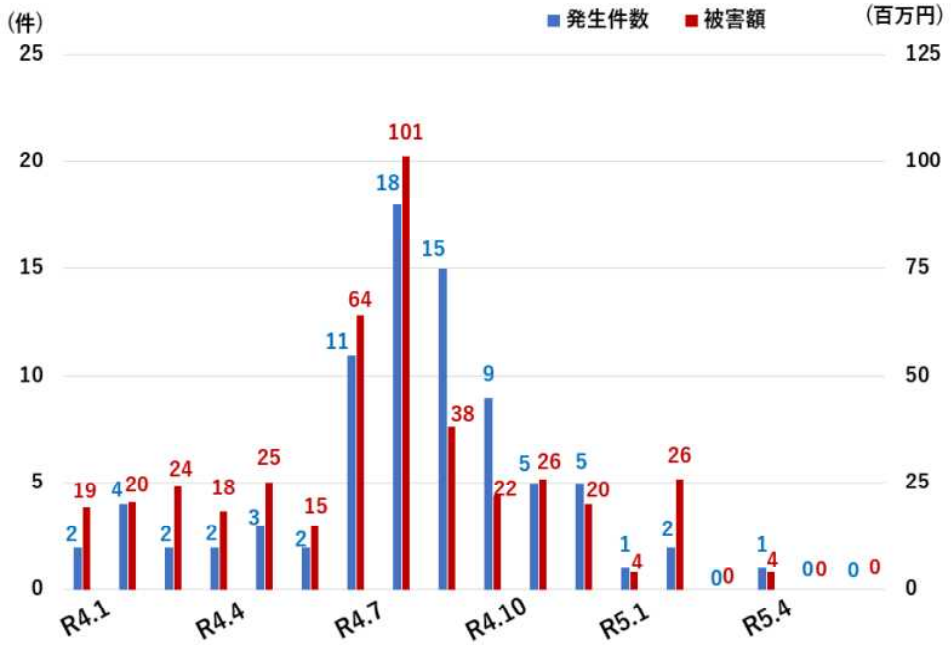
また、令和５年８月、金融庁、一般社団法人全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（ＪＣ３）と連携し、国民に対し、メールやＳＭＳに記載されたリンクからアクセスしたサイトにＩＤ及びワンタイムパスワード・乱数表等のパスワードを入力しないよう注意喚

起を行うほか、「サイバー警察局便り」を警察庁ウェブサイト及び警察庁ＳＮＳアカウントに掲載し、フィッシングの被害防止に関する広報啓発を実施した。

○　ＳＩＭスワップ[*10]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５月以降、ＳＩＭスワップによる不正送金の被害は確認されていない。

【図表16：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。

○　クレジットカード番号等の盗用防止対策

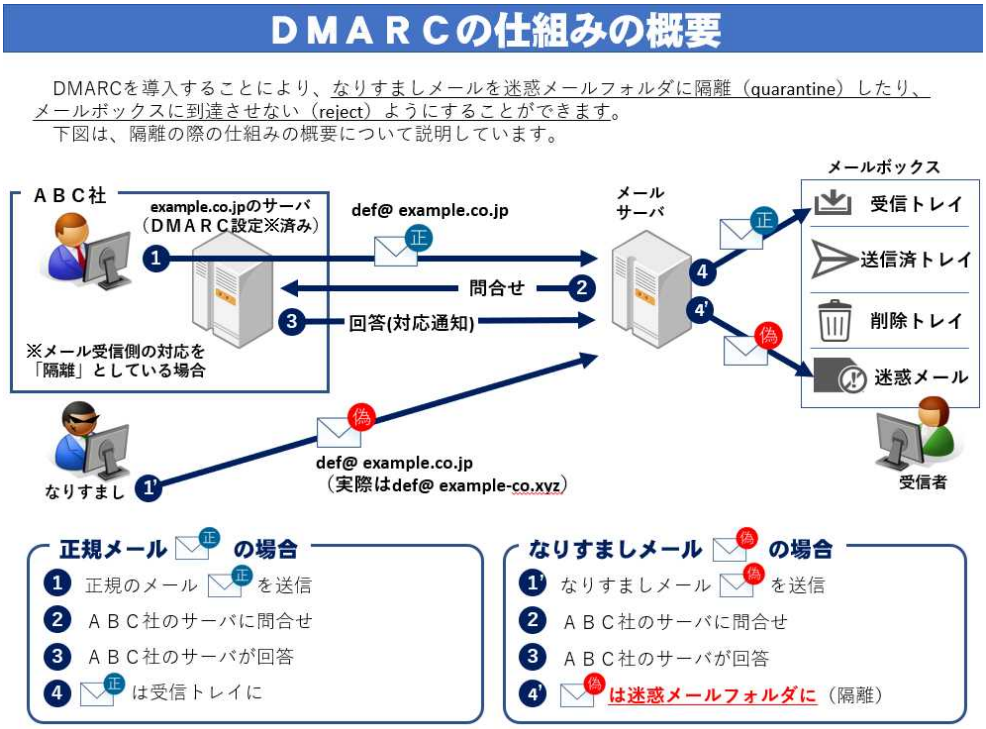
クレジットカード不正利用被害の大部分が、クレジットカードの番号盗用によるものであり、フィッシング等によりクレジットカード番号等を窃取し、利用権者になりすます手口が主となっている。こうした情勢を踏まえ、クレジットカード番号等の不正利用の原因となるフィッシン

---

*10　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。

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[*11]）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17：DMARCの仕組みの概要】



○　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月までの間、正規のＳＮＳを偽装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、同ＩＤ・パスワードを使用して同ＳＮＳへ不正アクセスした。令和５年４月、同男を不正アクセス禁止法違反（不正アクセス行為）及び私電磁的記録不正作出・同供用罪で逮捕した。

---

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

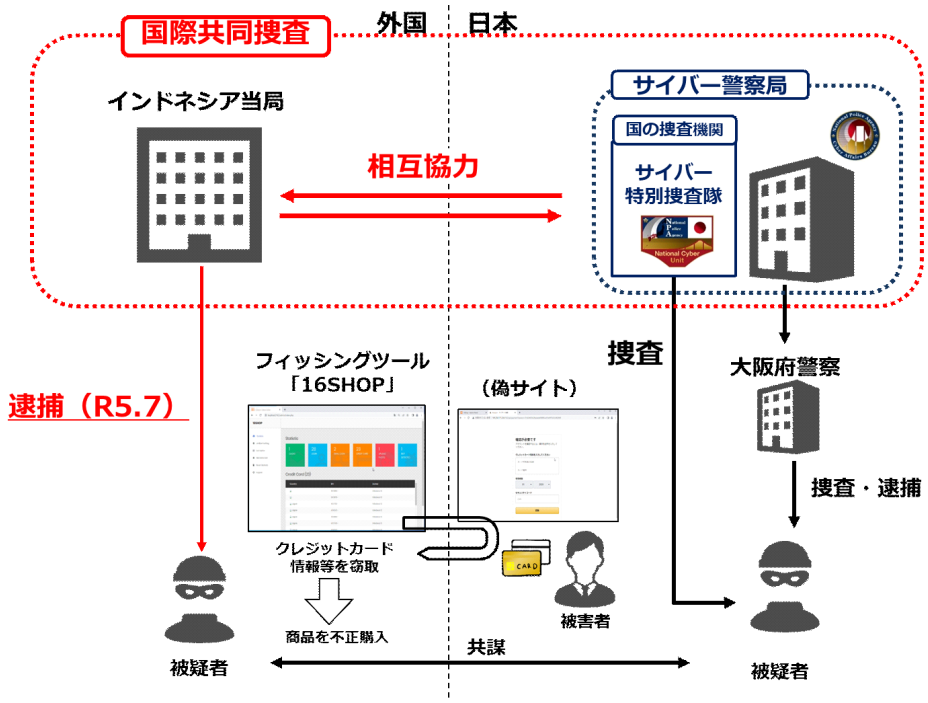
○　フィッシングによる詐欺事件被疑者の検挙

中国人の男（22）らは、令和４年７月、氏名不詳者と共謀の上、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だまし取った。令和５年１月、同男２名を詐欺罪で逮捕した。

○　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購入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、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18：事案の概要】



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[*12]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。

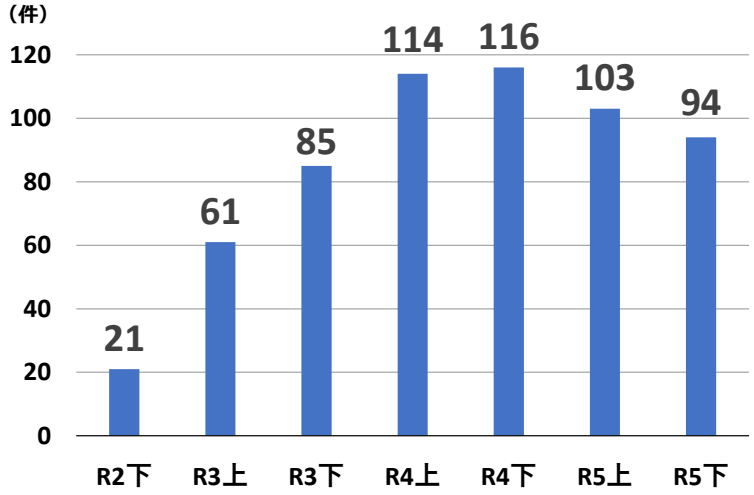
(2)　企業・団体等におけるランサムウェア被害

ア　被害件数

○　ランサムウェアによる被害

企業・団体等におけるランサムウェア被害として、令和５年に都道府県警察から警察庁に報告のあった件数は197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19：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】



○　「ノーウェアランサム」による被害

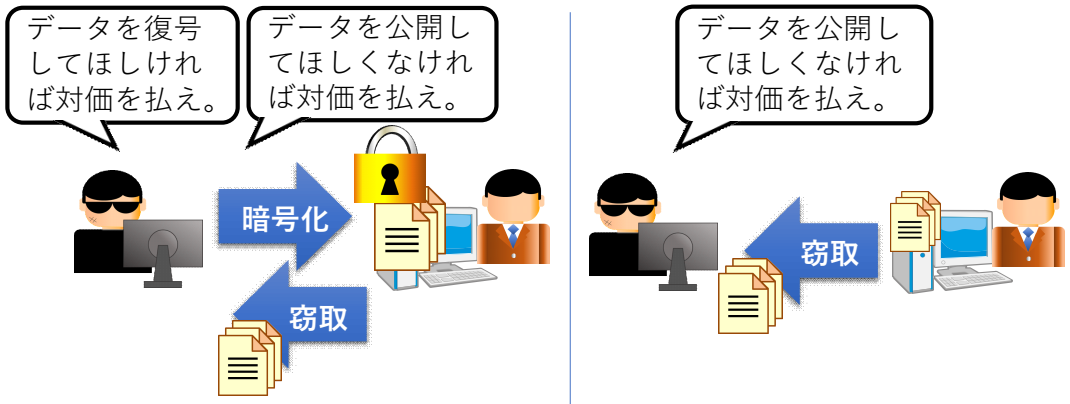
ランサムウェアによる被害のほか、最近の事例では、企業・団体等のネットワークに侵入し、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取した上で、企業・団体等に対価を要求する手口（「ノーウェアランサム」）による被害が、新たに30件確認された。

なお、「ノーウェアランサム」による被害件数は、令和５年におけるランサムウェア被害の報告件数（197件）には含まれない。

---

*12　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20：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）】



イ　特徴

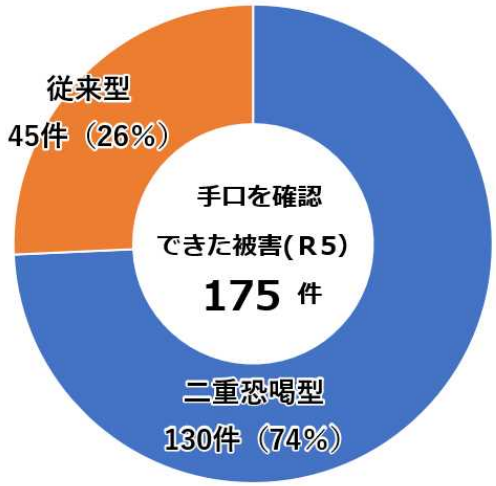
○　二重恐喝（ダブルエクストーション）による被害が多くを占める

ランサムウェアによる被害（197件）のうち、手口を確認できたものは175件あり、このうち、二重恐喝の手口によるものは130件で74％を占めた。

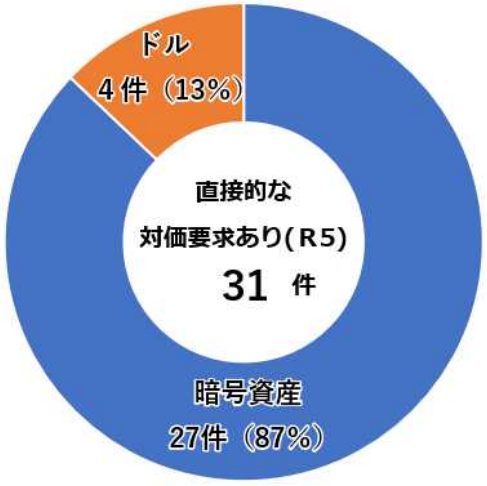
○　暗号資産による対価の要求が多くを占める

ランサムウェアによる被害（197件）のうち、直接的な対価の要求を確認できたものは31件あり、このうち、暗号資産による支払の要求があったものは27件で87％を占めた。

【図表21：ランサムウェア被害の手口別報告件数】



【図表22：要求された対価支払方法別報告件数】

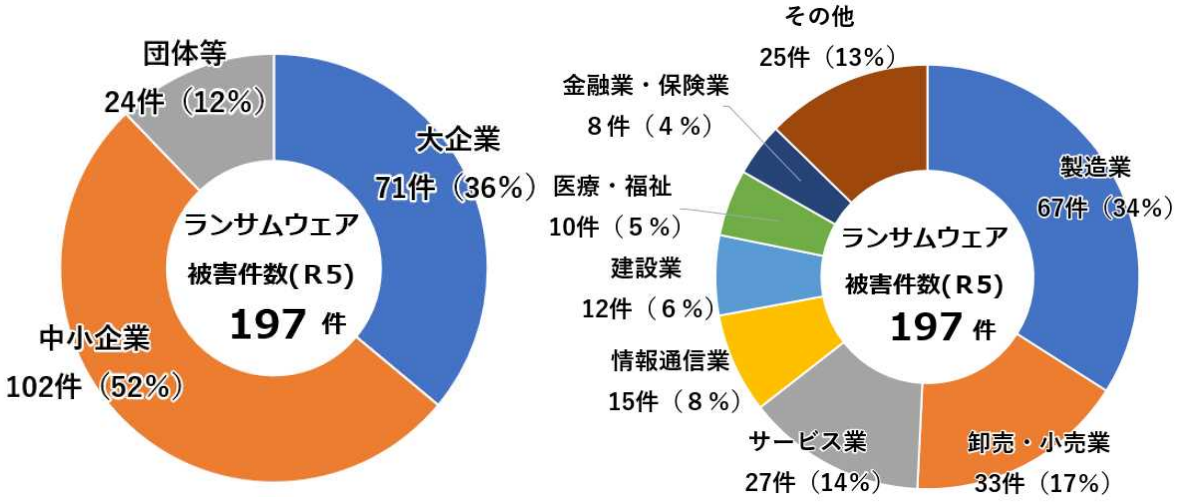


ウ　被害企業・団体等の規模

ランサムウェアによる被害（197件）の内訳を企業・団体等の規模別[*13]に見ると、大企業は71件、中小企業は102件であり、その規模を問わず、被害が発生した。

また、業種別[*14]に見ると、製造業は67件、卸売・小売業は33件、サービス業は27件であり、その業種を問わず、被害が発生した。

【図表23：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24：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、ランサムウェアによる被害（197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。

ア　感染経路

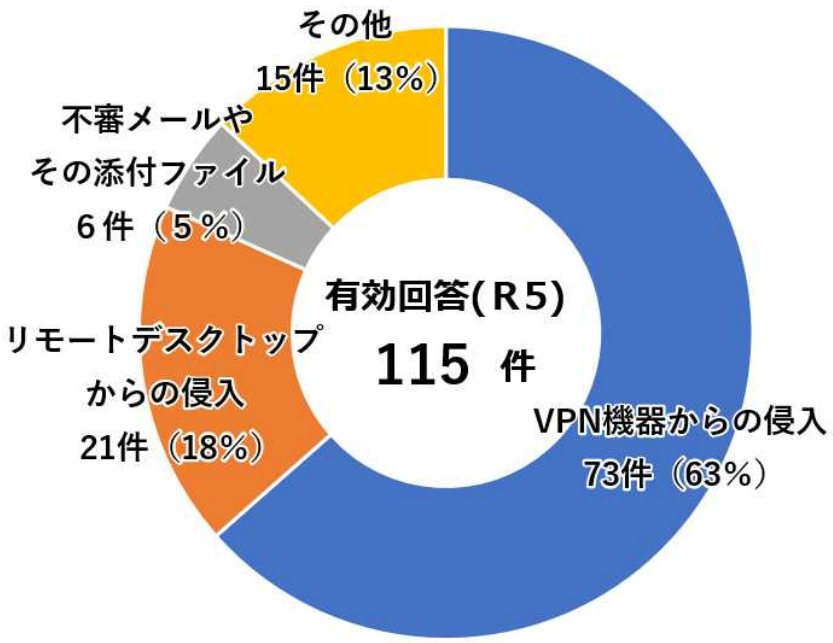
ランサムウェアの感染経路について質問したところ、115件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が73件で63%、リモートデスクトップからの侵入が21件で18%を占め、テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが約82%と大半を占めた。

---

*13　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

*14　日本標準産業分類に基づき分類

【図表25：感染経路】



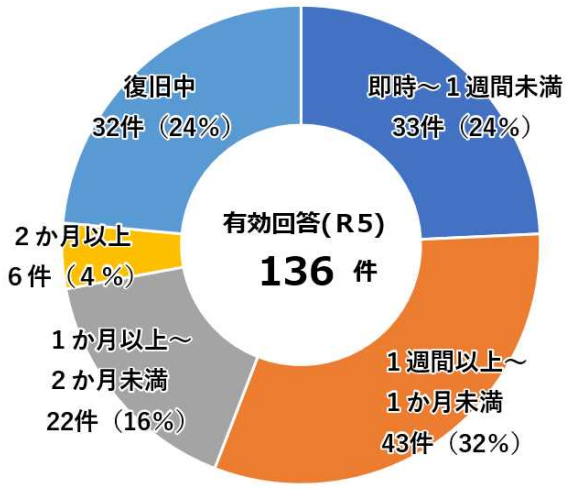
注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

イ　復旧等に要した期間・費用

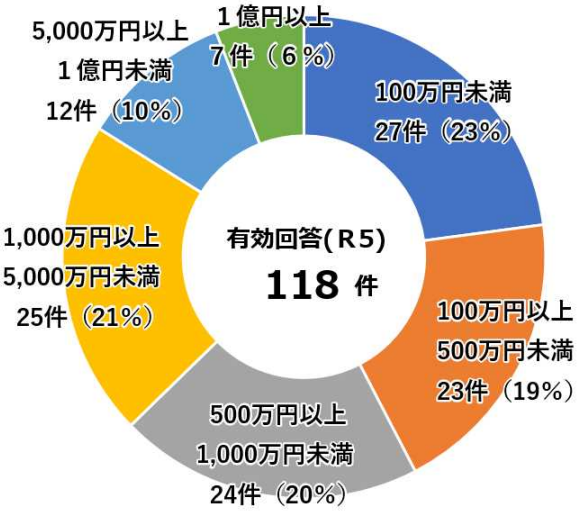
復旧に要した期間について質問したところ、136件の有効な回答があり、このうち、復旧までに１か月以上を要したものが28件あった。

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、118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44件で37%を占めた。

【図表26：復旧に要した期間】



【図表27：調査・復旧費用の総額】

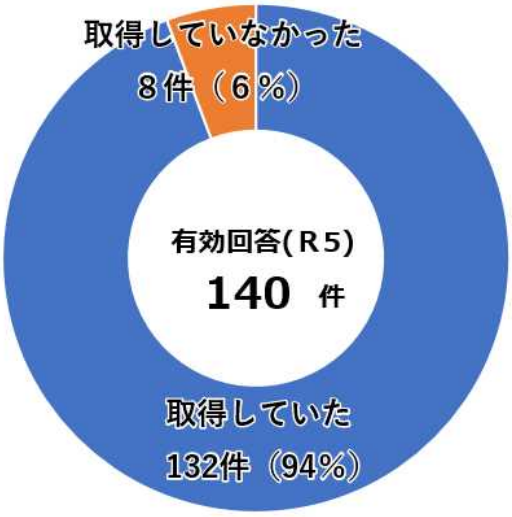


注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

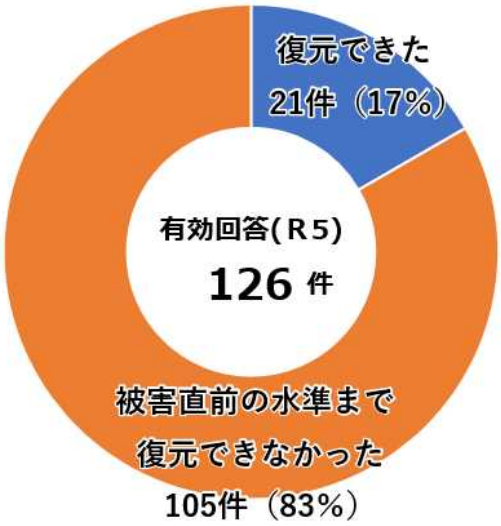
ウ　バックアップの取得・活用状況

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、140件の有効な回答があり、このうち、取得していたものが132件で94％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126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元できなかったものは105件で83％であった。

【図表28：バックアップ取得の有無】



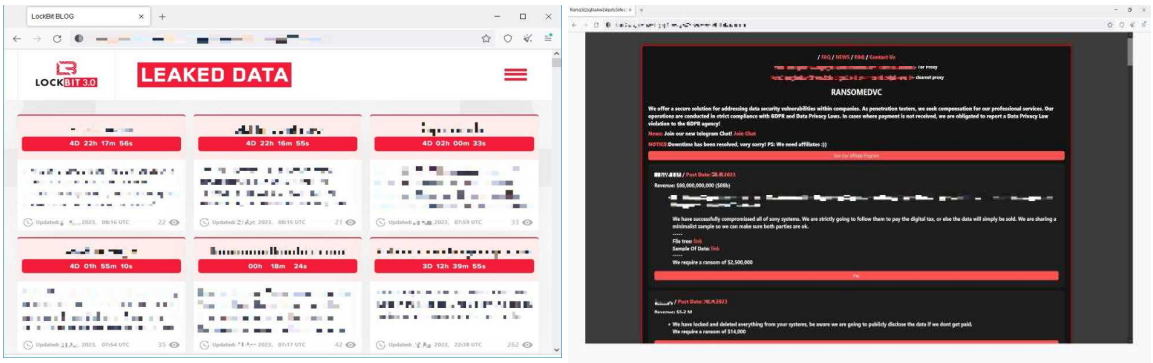
【図表29：バックアップからの復元結果】



(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、製品開発に関する情報や会計情報等が含まれていた。

【図表30：ダークウェブ上のリークサイト例】



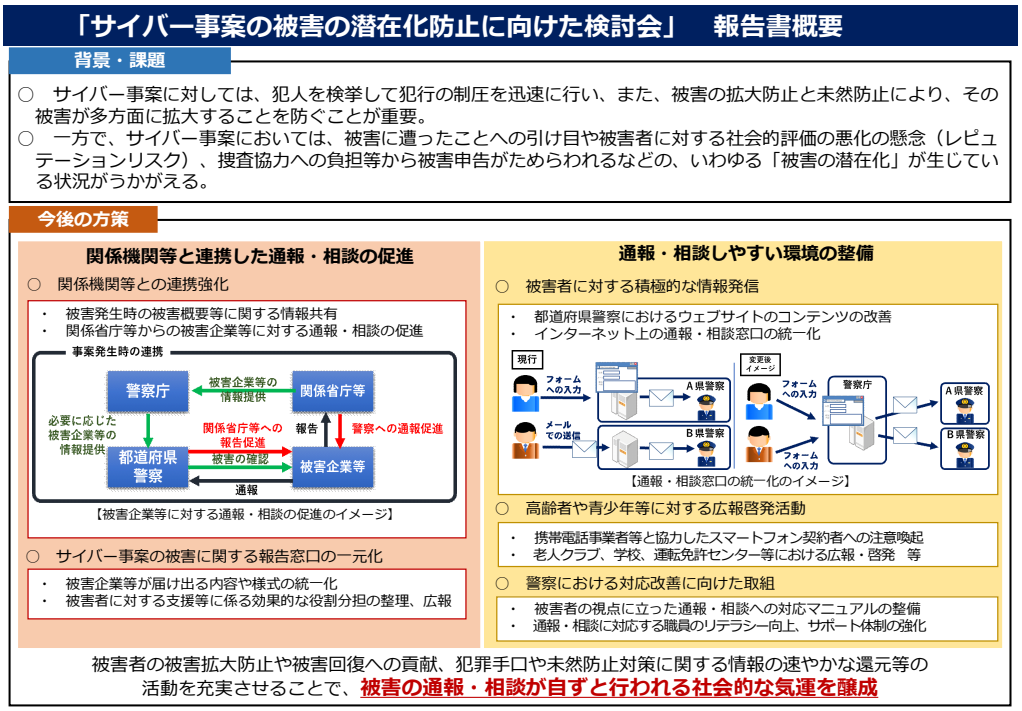
(5)　対処状況

○　サイバー事案の被害の潜在化防止に向けた取組

サイバー事案対処における通報・相談の重要性やサイバー事案の被害の潜在化改善の必要性を踏まえ、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る議論の結果について、令和５年４月、報告書を取りまとめた。

【図表31：「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。

○　通報・相談しやすい環境の整備

通報・相談を行う企業等の負担軽減等の観点から、インターネットから警察に対し通報・相談できる窓口を警察庁のウェブサイトにおいて、令和６年３月から運用するべく準備を進めた。

○　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Ｘ（旧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32：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けるアクセス権の売買等を監視し、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連絡した上で、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（ユーロポール）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更なる連携強化を推進している。

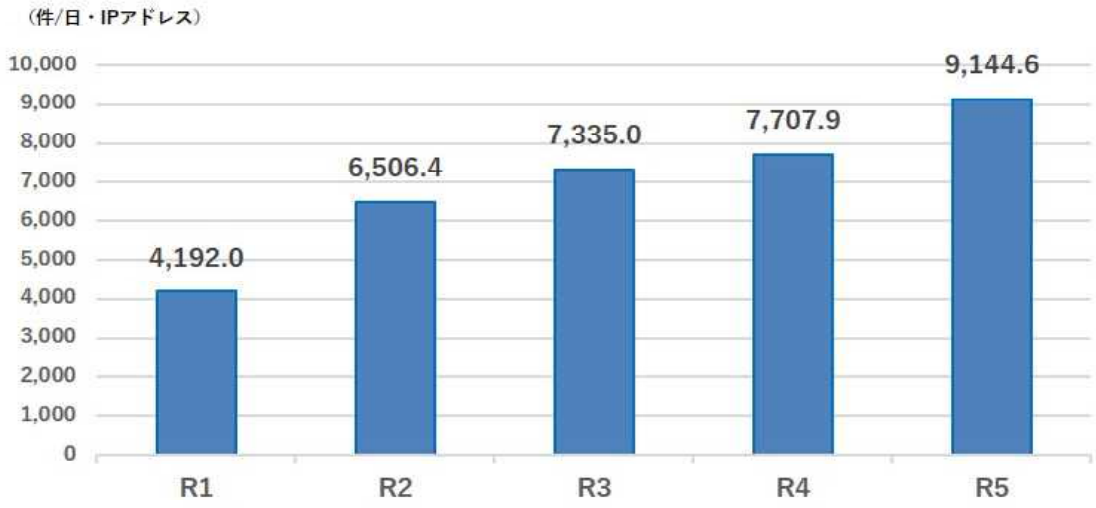
４　サイバー空間におけるぜい弱性探索行為等の観測状況

(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9,144.6件であり、平成23年以降、増加の一途をたどっている（前年比で18.6%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、調査目的と公表している特定のＩＰアドレスからのアクセスが増加していることなどが背景にあるものとみられる。

【図表33：センサーにおいて検知したアクセス件数の推移】



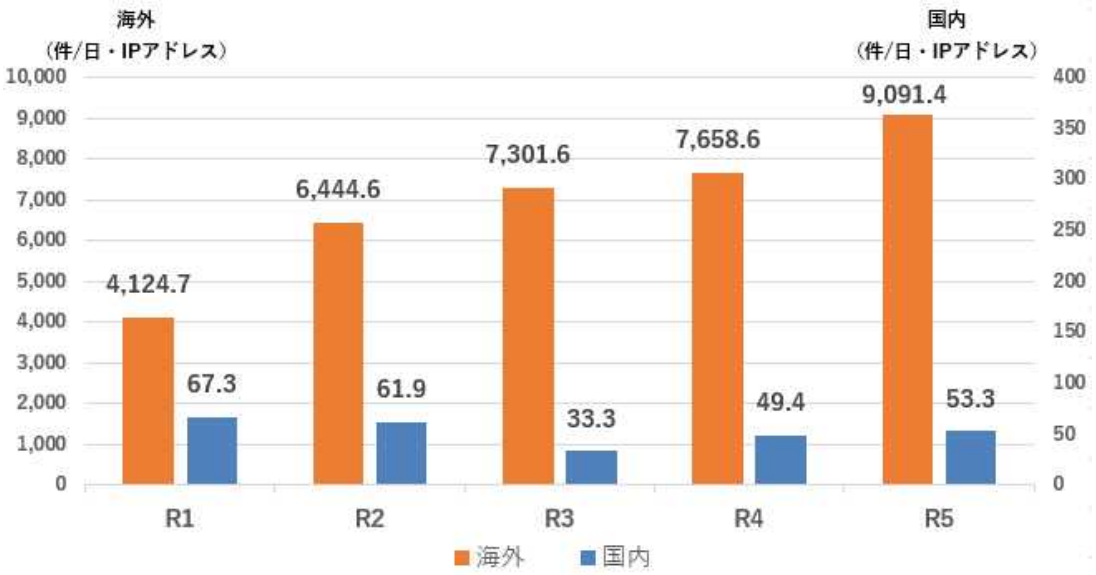
(2)　特徴的な観測

○　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53.3件であるのに対して、海外を送信元とするアクセスが9,091.4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34：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】

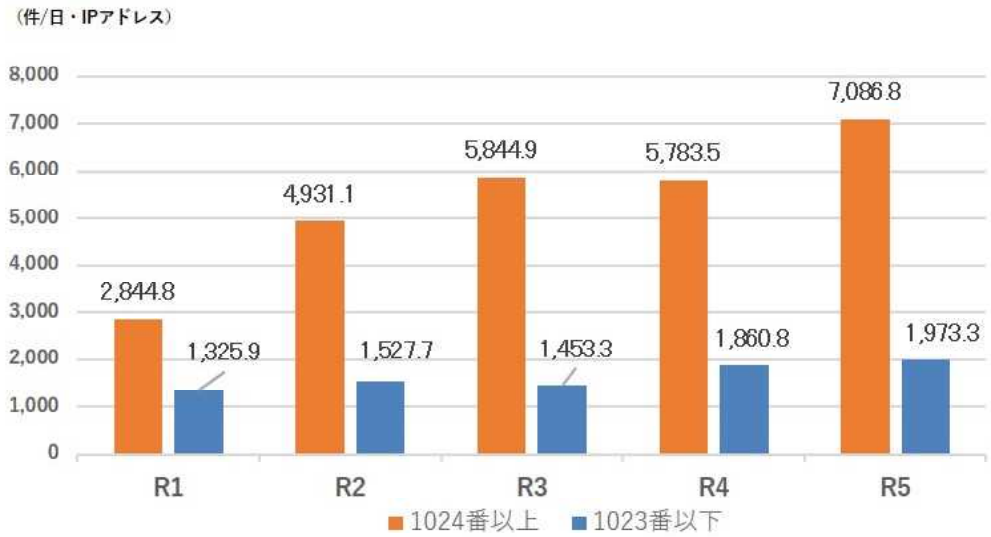


○　ＩｏＴ機器を対象としたぜい弱性探索行為等

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ものであるとみられる。

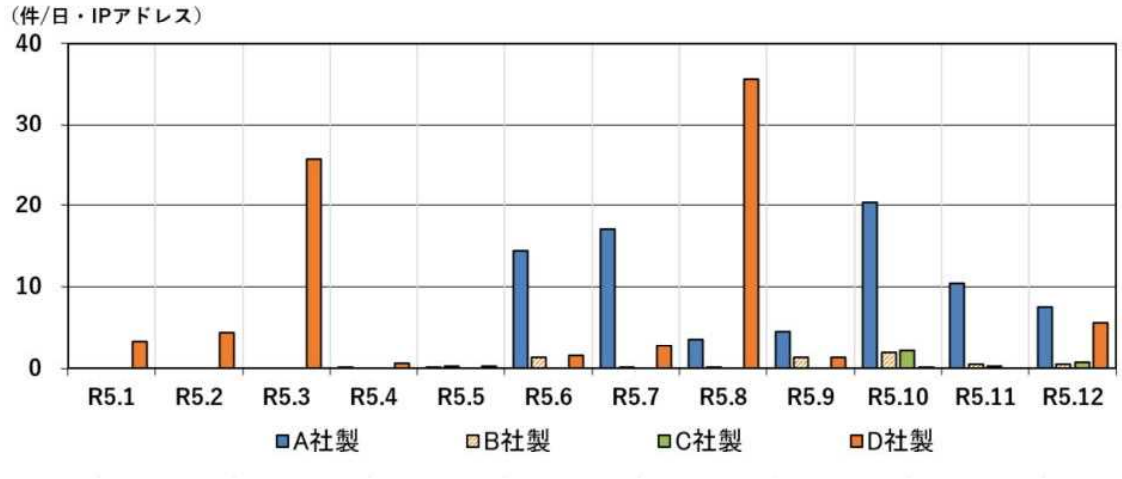
【図表35：検知したアクセスの宛先ポートで比較した１日・１ＩＰアドレス当たりの件数の推移】



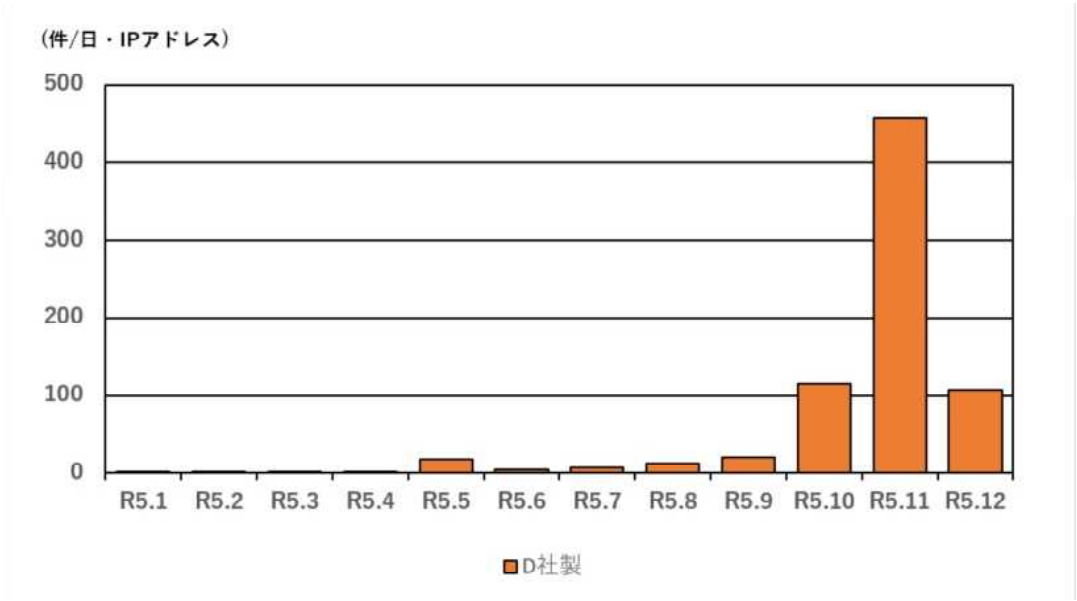
○　Wi-Fiルーターを対象とした不審なアクセスの観測

令和５年において、複数のWi-Fiルーターを対象とした不審なアクセスが観測された。観測されたアクセスは、それぞれのWi-Fiルーターのぜい弱性を狙ったもののほか、管理用のポートに対してユーザ名・パスワードを送信してログインを試行したと思われるものであった。

【図表36：Wi-Fiルーターのぜい弱性を狙ったアクセス件数の推移】[*15]



【図表37：Wi-Fiルーターの管理用のポートに対するログイン試行件数の推移】



Wi-Fiルーターのぜい弱性を悪用された場合又は不正なログインに成功された場合、ネットワークに侵入され情報を窃取される、不正プログラムを送り込まれるなどして他の被害者への攻撃の踏み台として悪用され

---

*15　Ａ社製、Ｂ社製及びＣ社製のWi-Fiルーターへのアクセスにおいて狙われたぜい弱性は、令和５年に公開されたものであり、Ｄ社製のWi-Fiルーターへのアクセスにおいて狙われたぜい弱性は、令和４年以前に公開されたものである。

るなどの被害に遭う可能性がある。

Wi-Fiルーターを利用する際は、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、最新のファームウェアへの更新、サポートが終了した製品の買い替え等の対策が必要である。

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のほか、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のできない、爆発物・銃砲等の製造方法等の情報や人を自殺に誘引する情報が存在している。中でも、犯罪実行者募集情報が氾濫しており、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[*16]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

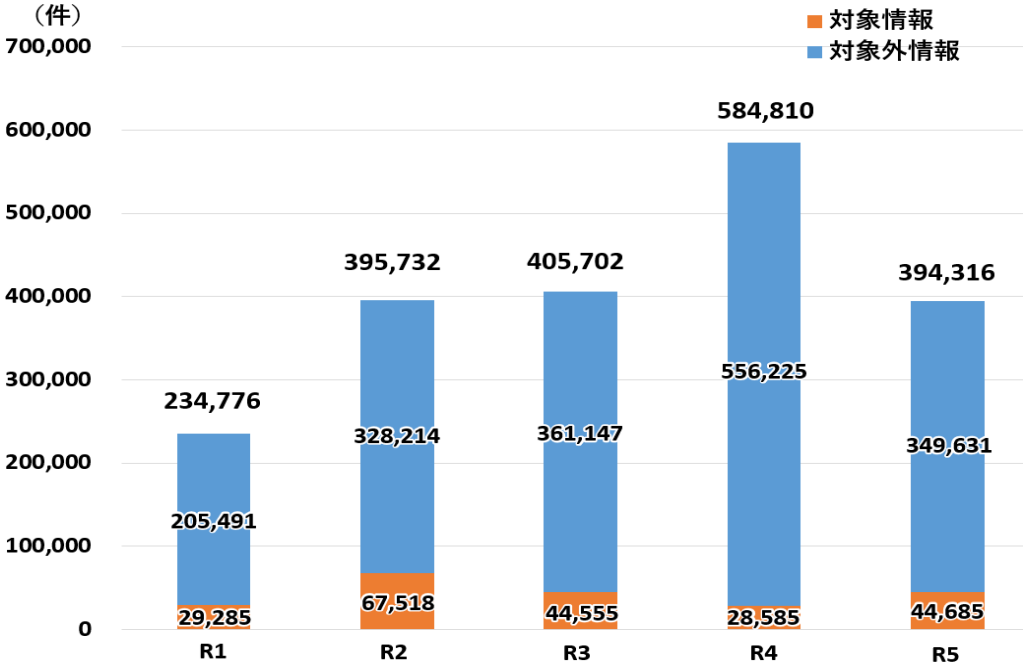
○　令和５年における違法情報の対処状況

令和５年におけるＩＨＣの通報受理件数は393,942件であり、運用ガイドラインに基づいて394,316件を分析した結果、違法情報を33,200件、重要犯罪密接関連情報を4,876件、自殺誘引等情報を6,609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140件を除く2,818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1,913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1,645件（86.0％）が削除された。

---

*16　他人を自殺に誘引・勧誘する情報等

【図表38：違法情報等の分析件数の推移】



○　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39：重要犯罪密接関連情報に関する広報用ポスター】

○　犯罪実行者募集情報対策の推進

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った。

【図表40：犯罪実行者募集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

ＩＨＣの運用ガイドラインに基づき、令和５年２月15日から12月31日までの間､重要犯罪密接関連情報と判断し分析した情報は4,876件であり、3,379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、2,411件（71.4％）が削除に至った。このうち、令和５年９月29日から12月31日までの間、犯罪実行者募集情報と判断し分析した情報は4,411件であり、2,979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、2,136件（71.7％）が削除に至った。

【図表41：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	15	10	8
爆発物・銃砲等の製造	16	15	7
殺人・強盗等の勧誘	411	356	252
臓器売買	18	16	5
人身売買	0	0	0
硫化水素ガスの製造	2	1	1
ストーカー行為等	3	2	2
犯罪実行者募集	4,411	2,979	2,136
合計	**4,876**	**3,379**	**2,411**

※　削除完了件数は、令和６年１月末に確認した状況を計上

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。

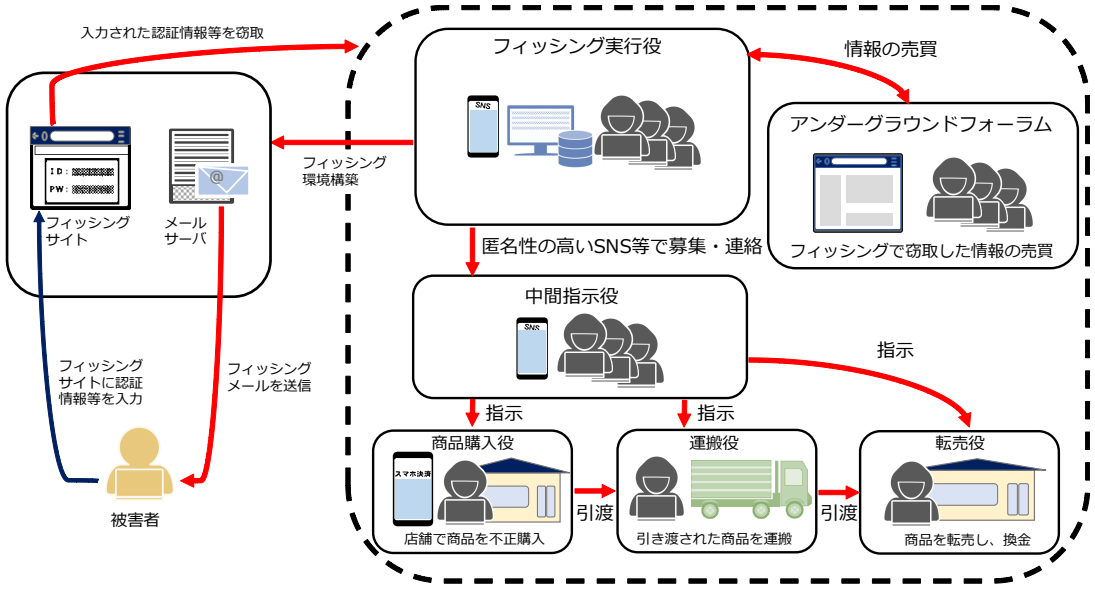
○　中国人フィッシンググループの実態解明等

フィッシングは、世界中で被害が発生し、日本国内でも多数の事例が確認されており、中には、被疑者が数百万件の認証情報と数万件のクレジットカード情報を自身の端末に保管していた例も確認されている。また、日本国内におけるフィッシング事犯及びフィッシング等により流出した情報の不正利用事案等の捜査を推進した結果、日本人だけでなく、外国人が犯行に関与している実態が判明し、中には、外国人が組織的に関与していることがうかがわれる例も確認されている。

サイバー特別捜査隊では、このようなフィッシング事犯等の捜査及び実態解明を推進しているところ、その過程において、フィッシングを組織的に行う中国人グループ（以下「中国人フィッシンググループ」という。）の存在を認知した。このグループでは、フィッシングを容易にするようなエコシステムが構築されていることが判明している。具体的には、匿名性の高いＳＮＳ等を通じて中間的役割を担う指示役（以下「中間指示役」という。）や商品購入役等の募集・連絡を行っており、フィッシング実行役がフィッシングで認証情報等を窃取した後、中間指示役を通じて、スマートフォン決済サービスやクレジットカード情報を悪用した商品の不正購入、購入した商品の運搬、転売による換金を分担して行わせ、不正な利益を獲得している態様のものが確認された。また、フィッシング実行役は、匿名性の高いＳＮＳ等を通じ、フィッシングで窃取した情報の売買やフィッシングの指南等も行っているとみられる。

このようなエコシステムは、他のフィッシング事犯等においても構築されているとみられており、サイバー特別捜査隊においては、引き続き、フィッシング事犯等の捜査及び実態解明に努めている。

【図表42：中国人フィッシンググループによるフィッシングに係るエコシステム】



この中国人フィッシンググループが標的とした対象には、日本国内の企業・団体のみならず、外国の企業・団体も含まれていることから、サイバー特別捜査隊においては、外国捜査機関に対して、必要な情報提供を行った。

フィッシングに対処するためには、社会全体で被害防止に向けた取組を推進する必要があり、以下は、求められる被害防止対策の例である。

【フィッシングに使われるおそれのある企業における対策】

・自社サイトを模したフィッシングサイトを発見した際のインターネットプロバイダ等への連絡
・サーバへの電子証明書の導入

【クレジットカード会社における対策】

・不正利用検知システムの導入
・DMARCによるなりすましメールの抑止

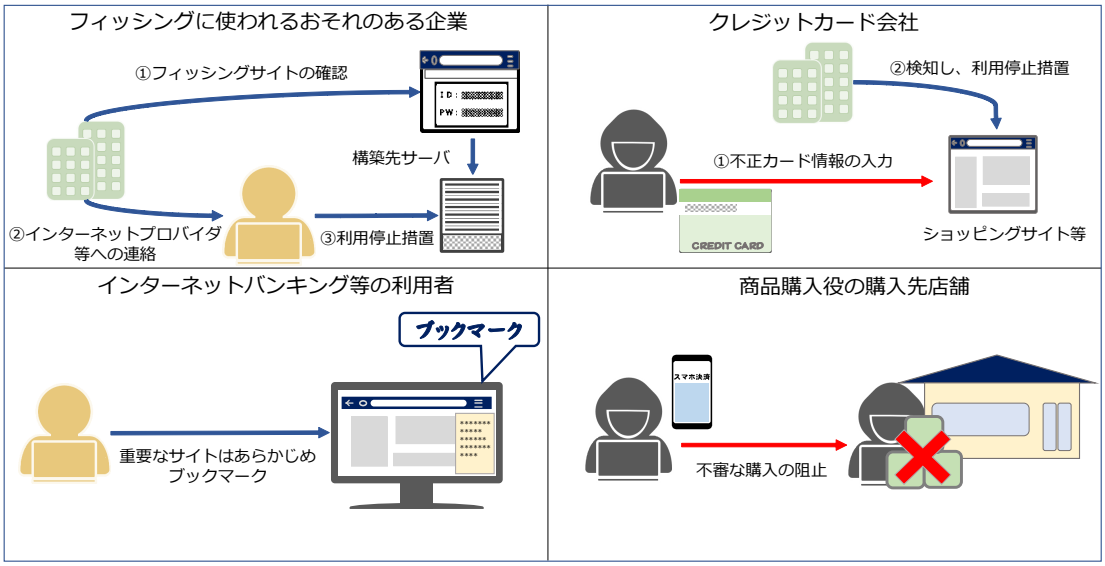
【インターネットバンキング等の利用者における対策】

・重要なサイトはあらかじめブックマークする
・多要素認証の活用

【商品購入役の購入先店舗における対策】

・電子決済によるタバコ、電子ギフト券等の大量購入等不審な来客時の警察への通報

【図表43：求められる被害防止対策】



犯行グループによるフィッシングサイトやフィッシングメールは、極めて精巧に作成されており、真偽を判断することが極めて困難となっていることから、ウェブサービスの利用者においては、重要なサイトやよく使用するサイトはあらかじめブックマークしたＵＲＬからアクセスするなど、より慎重な対応が求められる。

また、同一のＩＤ・パスワードを複数のウェブサービスにおいて使用している場合は、一度フィッシングにより情報を盗まれると、被害が急速に拡大するおそれがあるため、インターネットバンキング等の利用者はＩＤ・パスワード等の認証情報の使い回しを避けることで被害の拡大を防止することができる。

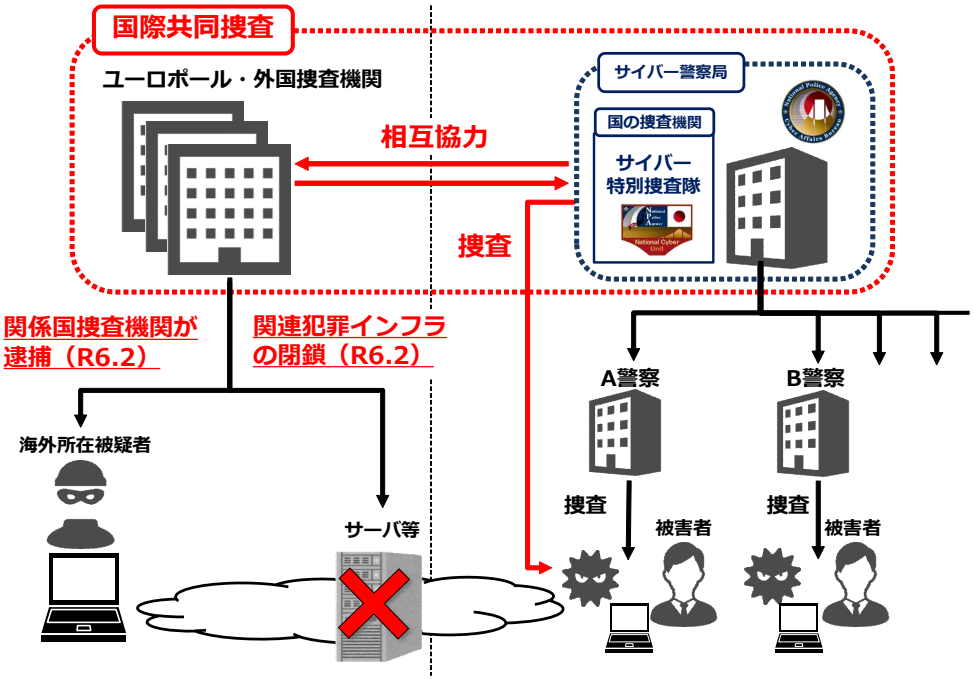
○　外国捜査機関等と連携したランサムウェア事案被疑者の検挙等

警察庁では、外国捜査機関等との連携を推進しており、世界各国の企業等に対してランサムウェア被害を与えている攻撃グループ「LockBit（ロックビット）」に対処するため、サイバー特別捜査隊等がEUROPOL（ユーロポール）が主導する「クロノス作戦（Operation Cronos）」に参画し、外国捜査機関等と連携して捜査を推進してきた。

その結果、令和６年２月、関係国捜査機関が、同グループの一員とみられる海外所在の被疑者２名を逮捕するとともに、同グループが使用するサーバ等のテイクダウン（機能停止）を実施し、流出した情報等が掲載されていたリークサイト上に、テイクダウンの実施を告げる「スプラッシュページ」を表示させた。

この事案では、サイバー特別捜査隊が、LockBitによって暗号化された被害データを復号するツールを独自開発し、令和５年12月、警察庁サイバー警察局からユーロポールに同ツールを提供しており、同ツールの有効性が認められている。また、令和６年２月、世界中の被害企業等の被害回復が可能となるよう、ユーロポール等と共に警察庁において、日本警察が開発した復号ツールについて情報発信し、その活用を促す旨の発表を行った。

【図表44：事案の概要】

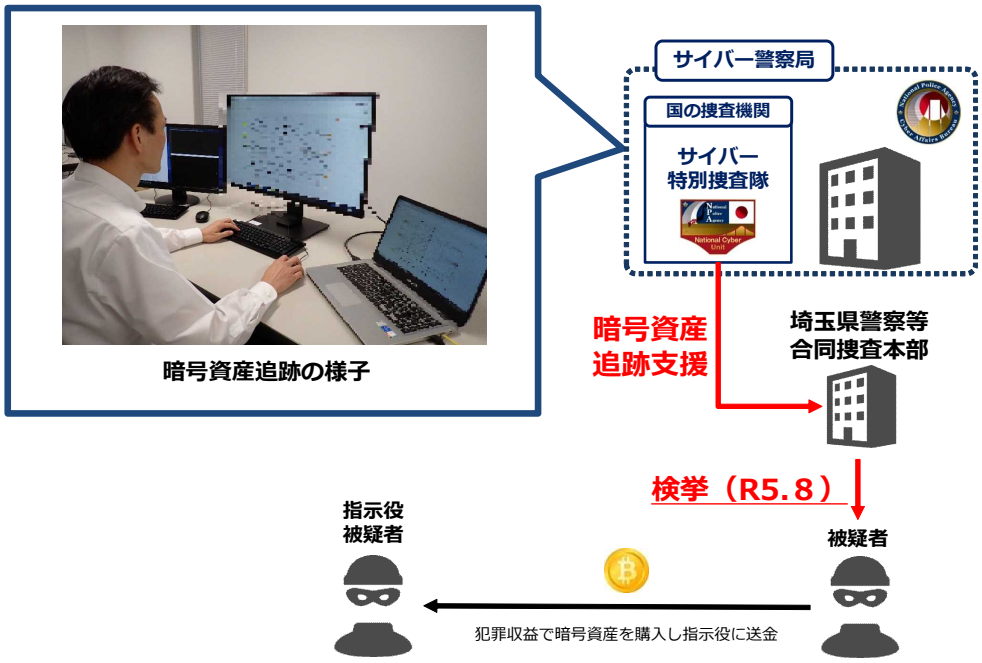


【図表45：スプラッシュページ】

○　都道府県警察との連携

他人のクレジットカード情報を不正利用して得た犯罪収益等を暗号資産に換え、海外口座に送金した組織的犯罪処罰法違反（犯罪収益等隠匿）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８月、埼玉県警察等の合同捜査本部が被疑者５名を逮捕した。

【図表46：事案の概要】

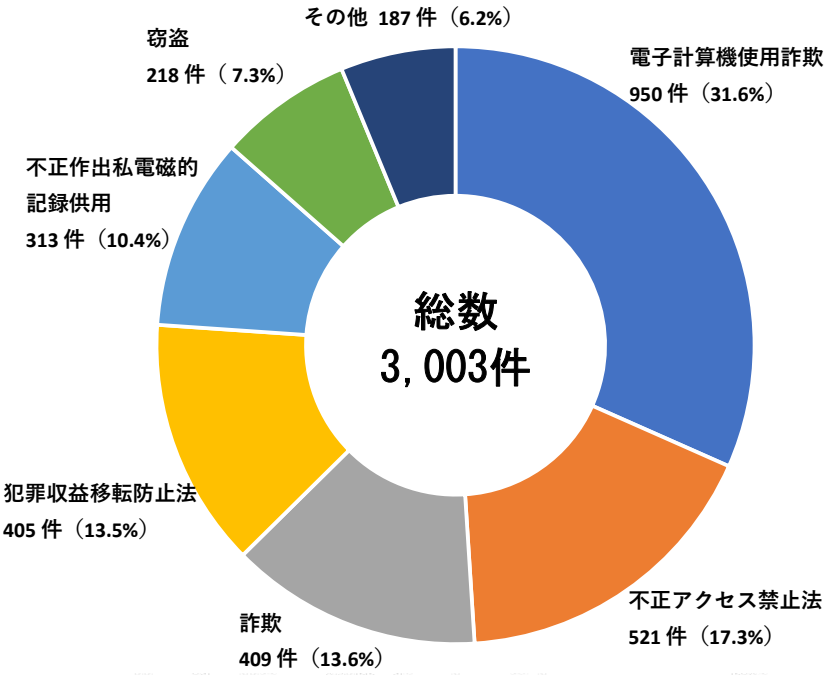


2　サイバー事案の検挙状況

(1)　サイバー事案の検挙状況

令和５年中におけるサイバー事案の検挙件数は、3,003件であった。

【図表47：サイバー事案の検挙状況】



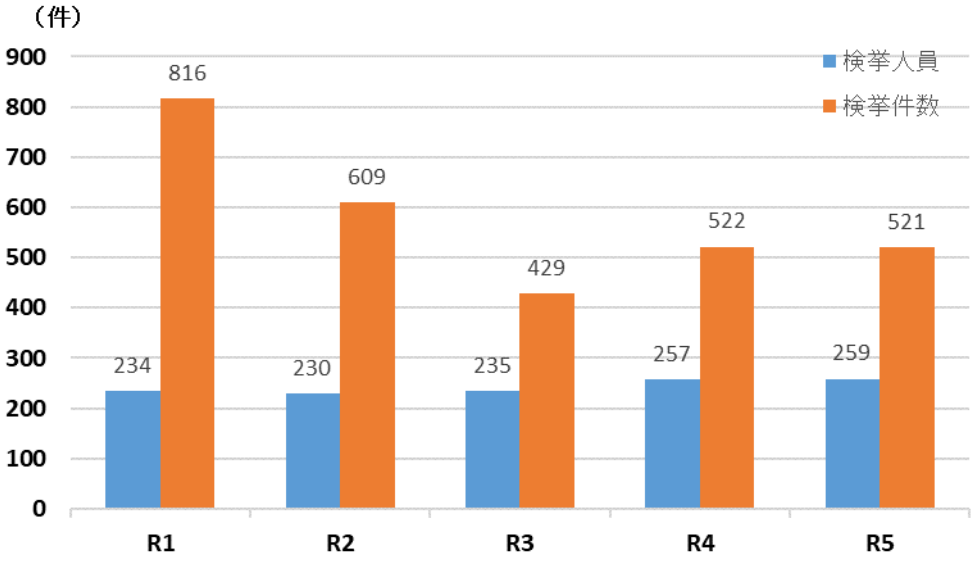
注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

(2)　不正アクセス禁止法違反の検挙件数及び特徴

ア　検挙件数

令和５年中における不正アクセス禁止法違反の検挙件数は521件で、前年と比べて１件減少した。

【図表48：不正アクセス禁止法違反の検挙件数の推移】



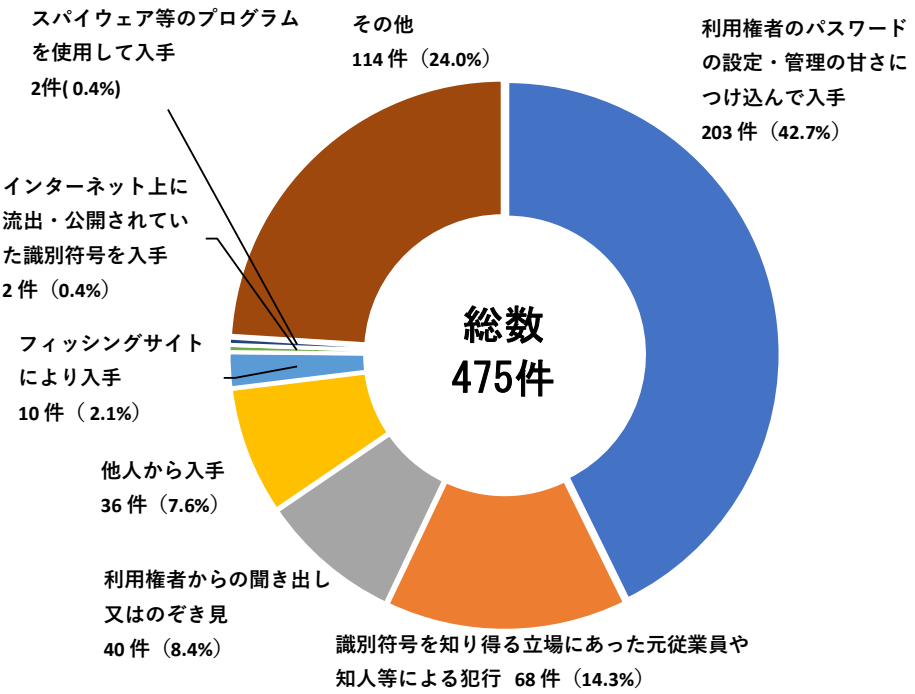
イ　特徴

検挙件数のうち、475件が識別符号窃用型で全体の91.2%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203件と最も多く、全体の42.7%を占めており、次いで「識別符号を知り得る立場にあった元従業員や知人等による犯行」が68件で全体の14.3%を占めた。

【図表49：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】

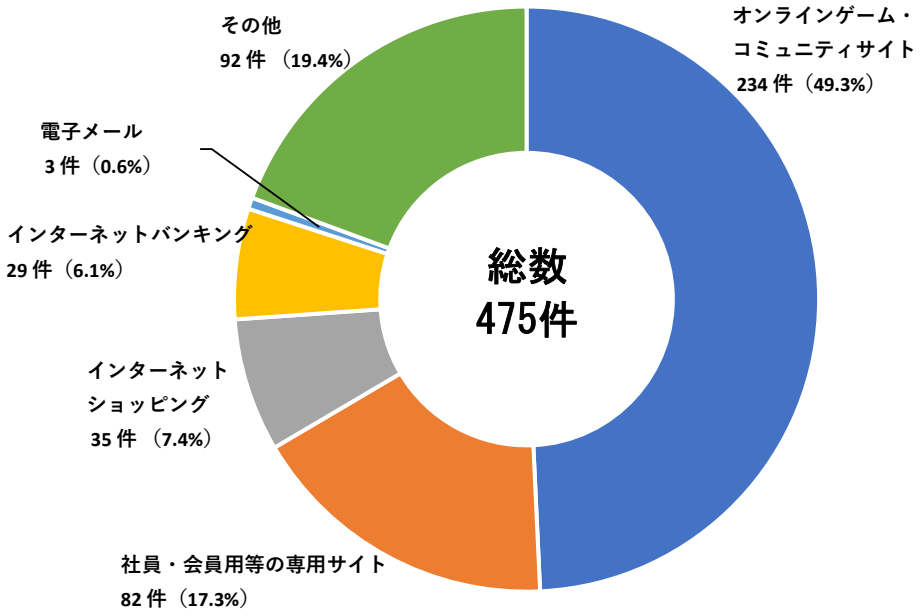


注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

○　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234件と最も多く、全体の49.3%を占めており、次いで「社員・会員用等の専用サイト」が82件で全体の17.3%を占めた。

【図表50：不正に利用されたサービス別検挙件数（識別符号窃用型）】



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。

ウ　検挙事例

○　会社員の男（43）は、令和３年６月から令和４年９月までの間、元勤務先会社の名刺管理システムに係るＩＤ・パスワードを転職先の同僚に提供した上、自身も同ＩＤ・パスワードを無断で使用して同システムへ不正アクセスした。令和５年９月、同男を個人情報保護法違反及び不正アクセス禁止法違反（不正アクセス行為）で逮捕した。

○　専門学生の男（18）は、令和５年２月から同年３月までの間、ゲームアカウント売買サイトの利用者にゲームアカウントの購入を持ちかけ、購入希望者の本人確認のためと偽って、同人の同サイトに係るＩＤ・パスワードを不正に取得し、同サイトへ不正アクセスした上、同サイトの使用するサーバに虚偽の情報を与え、同サイトの運営会社が管理するポイント合計約２万円相当を移転させ、財産上不法の利益を得た。令和５年８月までに、同男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺罪で検挙した。

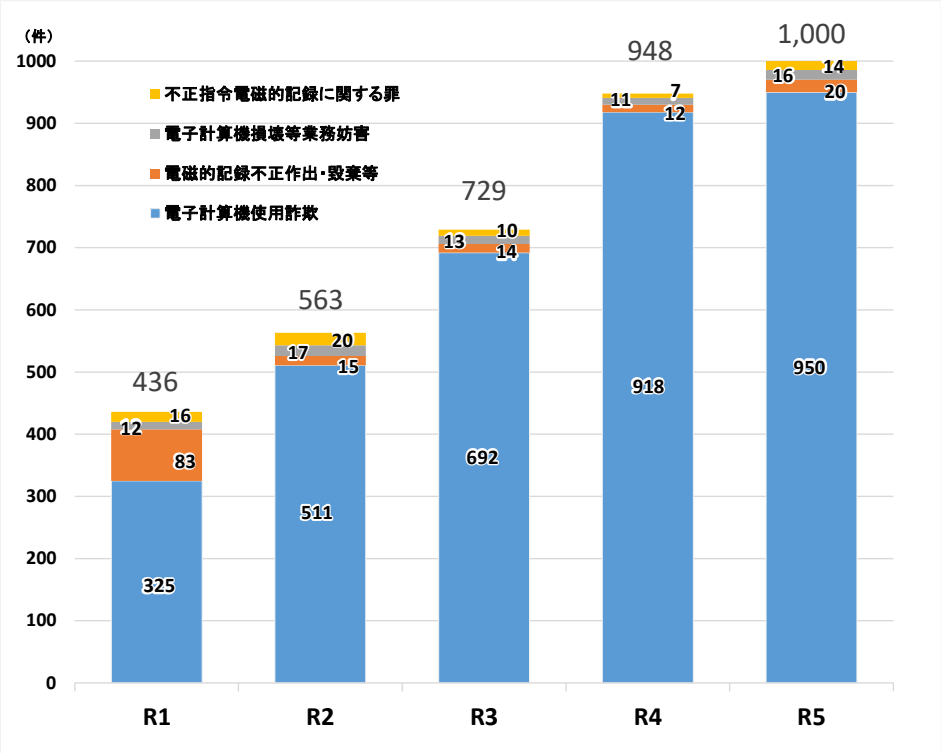
○　無職の男（22）は、令和５年５月、氏名不詳者と共謀の上、ＳＮＳで影響力のあるインフルエンサーに対し、実在する企業を装ってＳＮＳに消費者金融会社に登録すれば現金が得られる旨の虚偽の広告を掲載するよう依頼した上、同広告を見て連絡してきた利用者に対し、同会社が提供する借入システムに係るアカウントを同男が指定するＩＤ・パスワードで登録させ、同アカウントへ不正アクセスし、コンビニエンスストアのＡＴＭから現金を引き出した。令和５年10月、同男を不正アクセス禁止法違反（不正アクセス行為）及び窃盗罪で逮捕した。

(3)　コンピュータ・電磁的記録対象犯罪の検挙件数及び特徴

ア　検挙件数

令和５年中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1,000件で、前年と比べて52件増加した。

【図表51：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950件と最も多く、全体の95.0％を占めた。

ウ　検挙事例

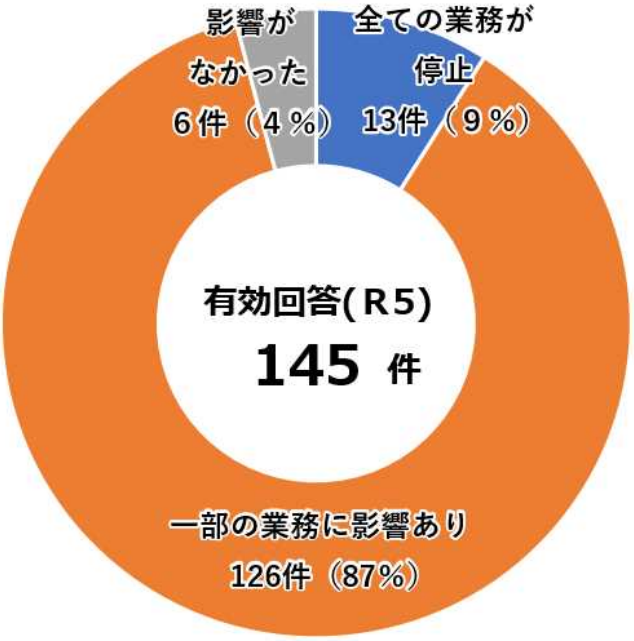
○　無職の男（26）は、令和４年10月から同年11月までの間、ＥＣサイトの管理者に無断で、同サイトに入力されたクレジットカード情報を取得するプログラムを仕掛け、同サイトの利用者らが入力した同情報を不正に取得した。令和５年11月、同男を不正指令電磁的記録供用罪及び割賦販売法違反で逮捕した。

○　高校生の男（17）は、令和５年３月から同年４月までの間、人の電子計算機における実行の用に供する目的で、ウェブブラウザに記録されたＩＤ・パスワード等の情報を特定のサーバに送信するプログラムを作成した上、同プログラムをゲームのチートツールと偽って、情を知らない他人にダウンロードさせ、同人の端末に保存されている情報を不正に取得した。令和５年11月、同男を不正指令電磁的記録作成・同供用罪で検挙した。

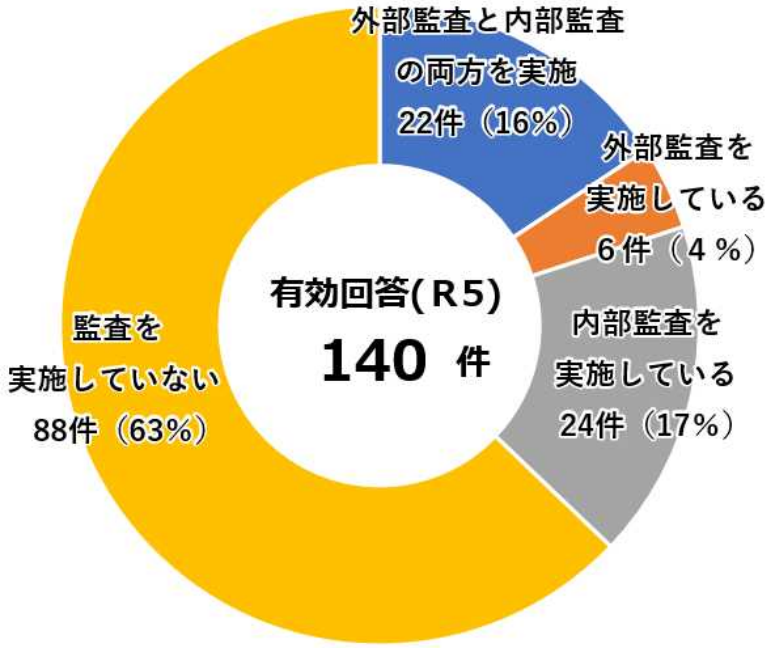
参考

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

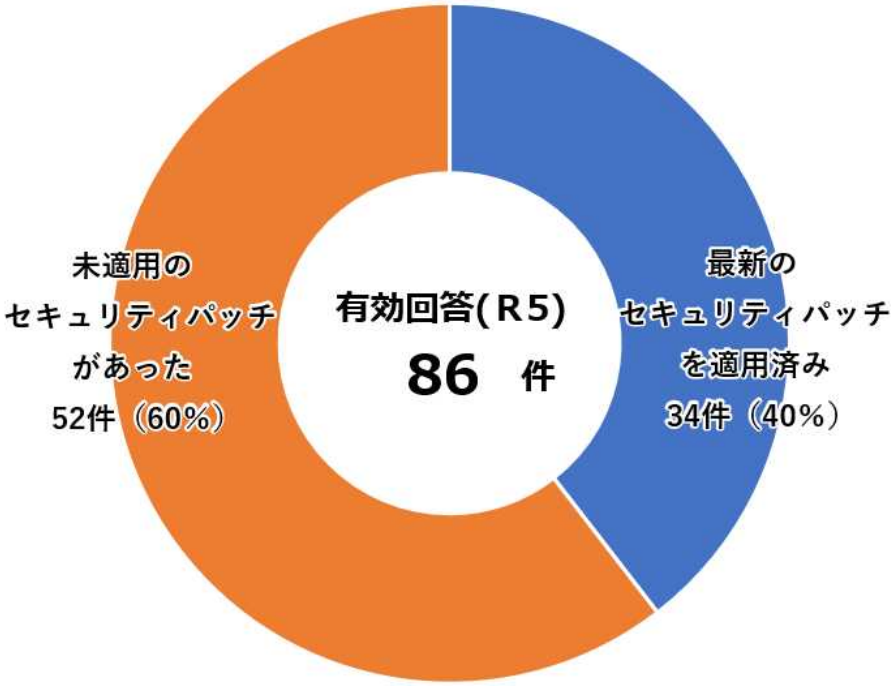
(1)　ランサムウェア被害が業務に与えた影響



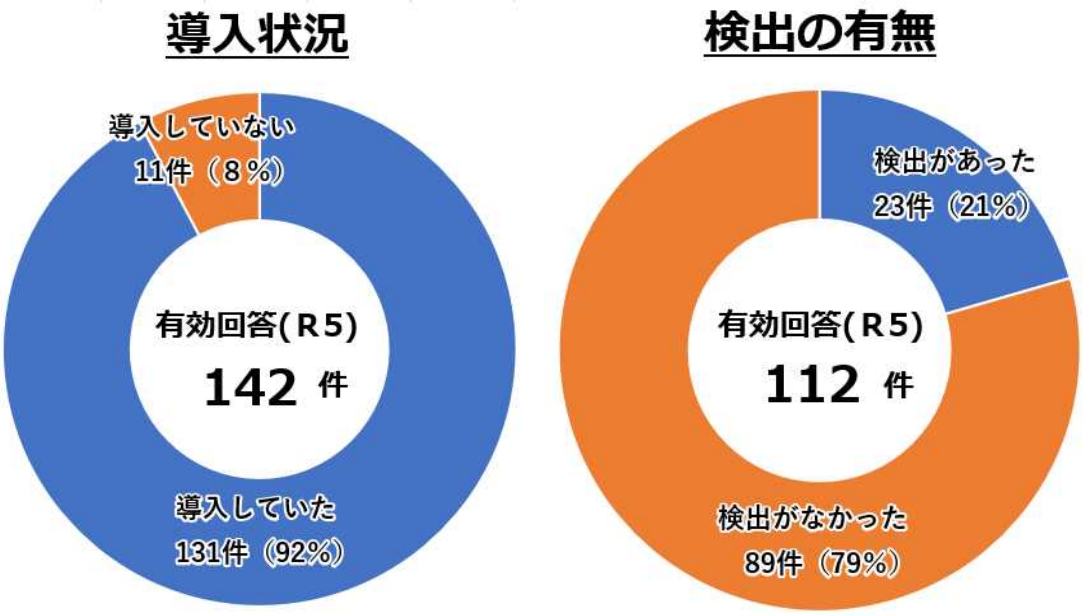
(2)　被害企業・団体の情報セキュリティ監査の実施状況



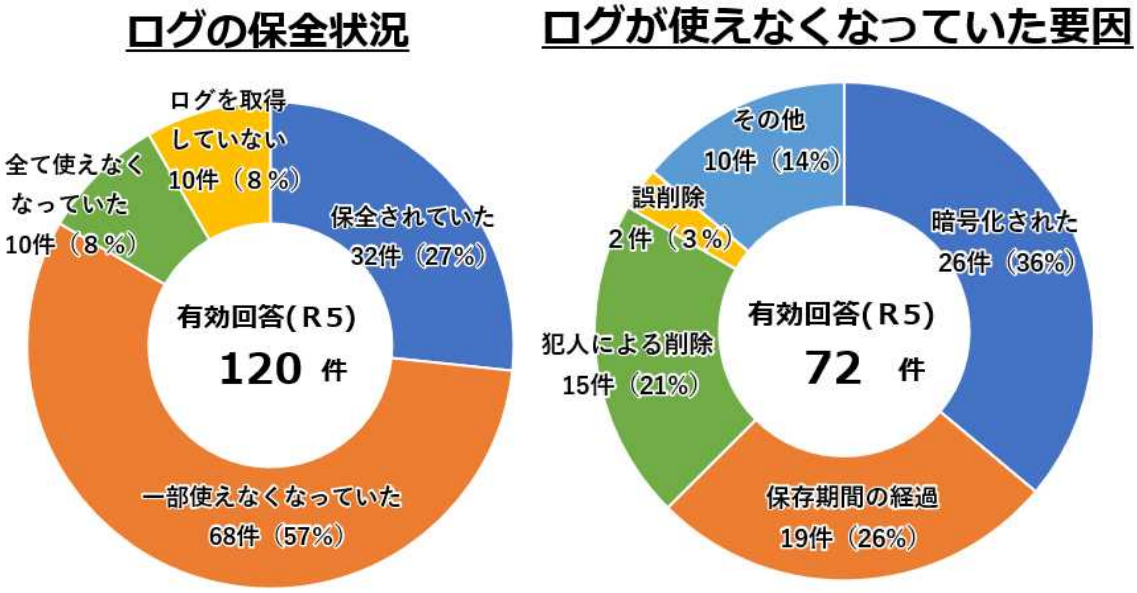
(3)　侵入経路とされる機器のセキュリティパッチの適用状況



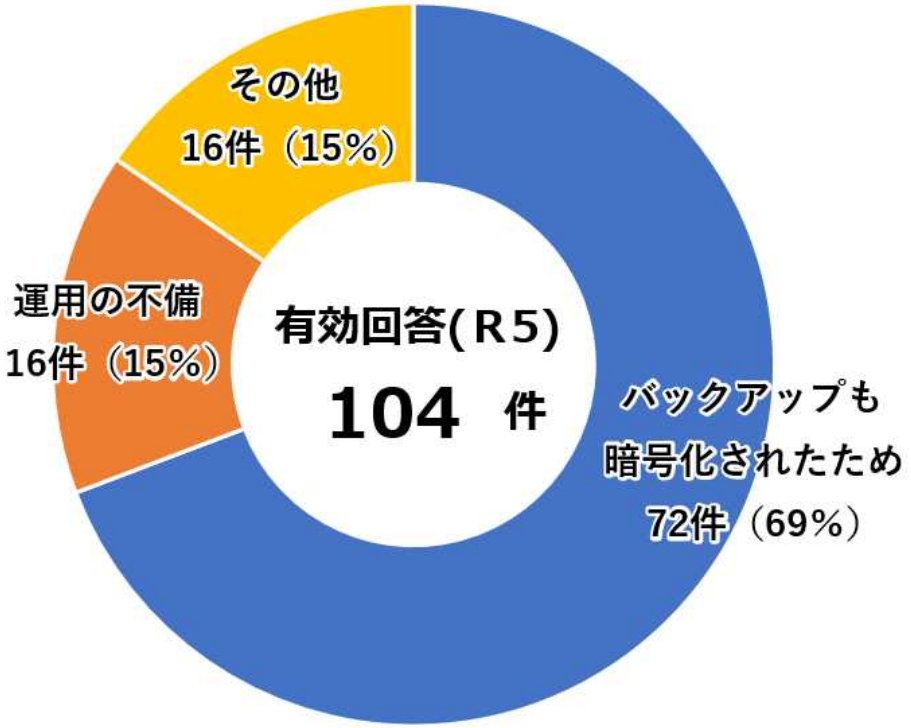
(4)　被害企業・団体等のウイルス対策ソフト等導入・活用状況



(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



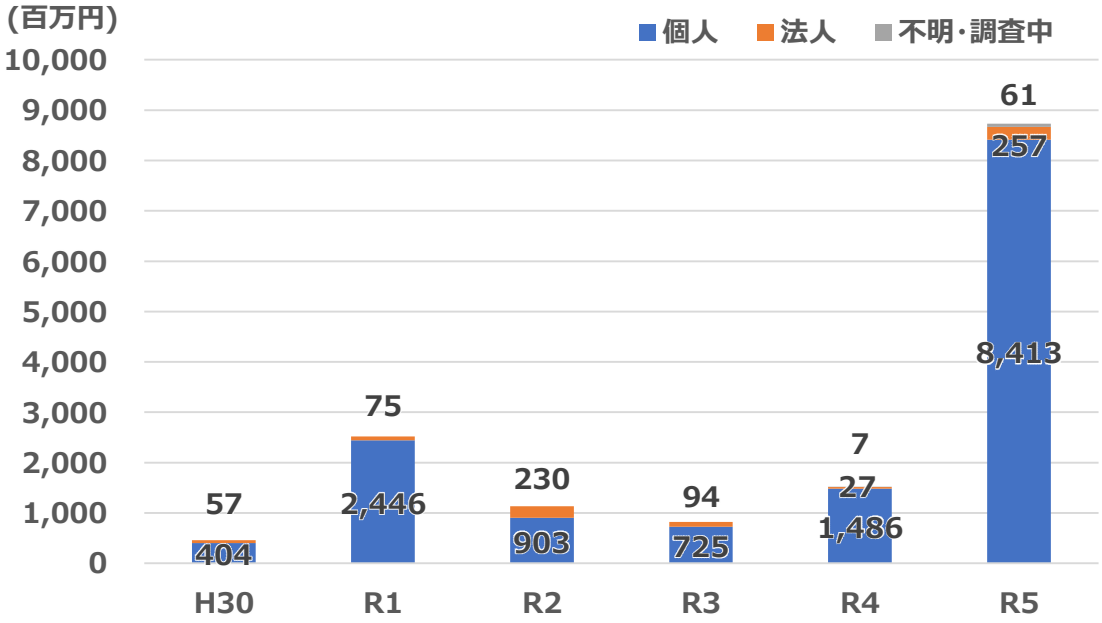
(6)　被害企業・団体のバックアップから復元できなかった理由



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。

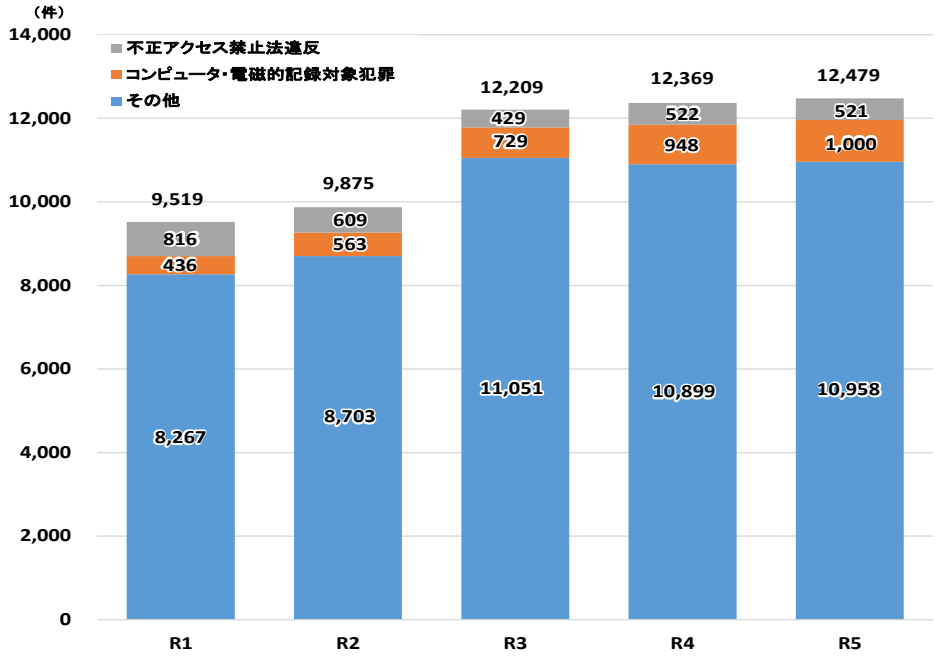
2　インターネットバンキングに係る不正送金事犯の発生状況

(1)　口座開設者別の被害状況

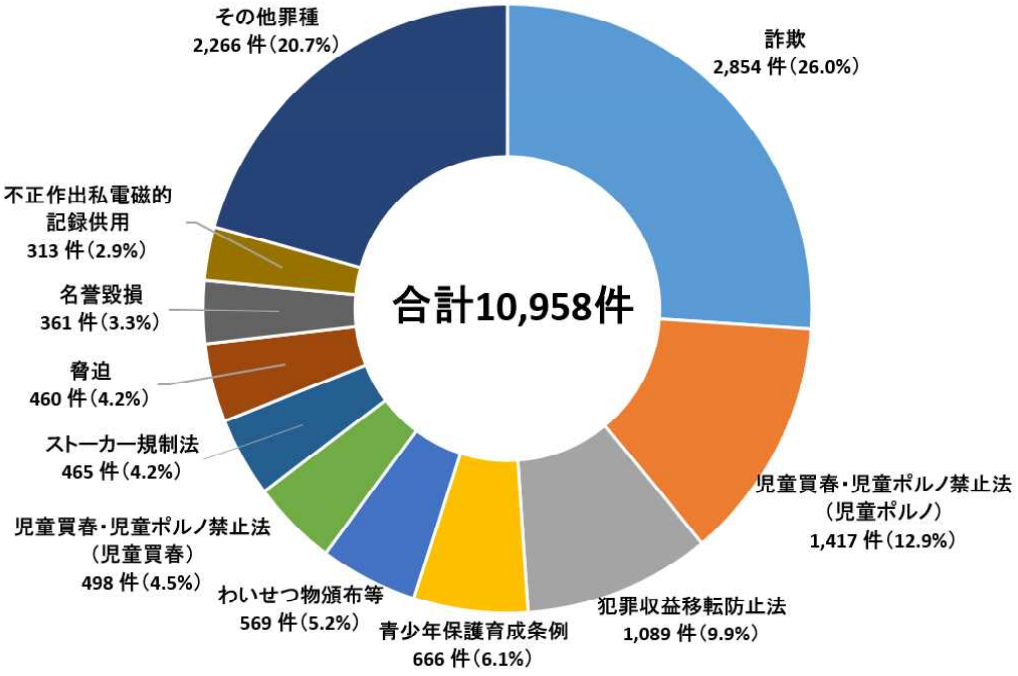


3　サイバー犯罪[*1]の検挙状況

(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。