令和７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７年９月
警察庁サイバー警察局

はじめに

令和７年上半期においては、政府機関、金融機関等の重要インフラ事業者等における DDoS 攻撃とみられる被害や情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生したほか、生成 AI を悪用した事案等の高度な技術を悪用した事案も発生している。このようなサイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数は前年に引き続き高水準で推移しており、その大部分が海外を送信元とするアクセスが占めている。また、令和７年上半期におけるランサムウェアの被害報告件数は 116 件と、令和４年下半期と並び最多となっており、このようなランサムウェアの被害拡大の背景には、ランサムウェアの開発・運営を行う者が、攻撃の実行者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）を中心とした攻撃者の裾野の広がりがあると指摘されている。

また、情報通信技術の発展が社会に便益をもたらす反面、インターネット空間を悪用した犯罪も脅威となっている。例えば、インターネットバンキングに係る不正送金、証券口座への不正アクセス・不正取引、SNS を通じて金銭をだまし取る詐欺、暗号資産を利用したマネー・ローンダリングが発生するなど、インターネット上の技術・サービスが犯罪インフラとして悪用されている実態が見られる。

さらに、インターネット上には、規制薬物の広告等の違法情報や犯罪を誘発するような有害情報が存在するほか、近年 SNS 上に氾濫する犯罪実行者募集情報は深刻な治安上の脅威となっている。

このような状況に対し、警察では検挙に向けた取組を進めており、例えば、全国のクレジットカード情報不正利用関連犯罪を分析し、不正に取得・売買されたクレジットカード情報の支払いに用いられたと認められる暗号資産の流れを捜査した結果、令和６年９月から令和７年３月までの間に、サイバー特別捜査部及び関係都道府県警察において、男女 20 名の被疑者を検挙した。

このほか、警察庁では、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に加わり、パブリック・アトリビューションとしてアドバイザリーを公表するとともに、ランサムウェア「Phobos/8Base」により暗号化されたデータを復号するツールを開発し広く周知するなど、被害の未然防止・拡大防止に向けた様々な取組を実施している。

本資料は、第１部で令和７年上半期中のサイバー空間の脅威情勢を、第２部で警察の取組を取りまとめたものである。

本文目次

図表・コラム目次

【図表】

図表・コラム目次

【コラム】

概要　令和７年上半期における脅威情勢の概要

令和７年上半期においては、サイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数及びランサムウェアの被害報告件数が依然として高水準で推移した。また、フィッシングの報告件数も前年上半期比で約 56 万件（約 89%）増加したほか、インターネット上には犯罪実行者募集情報が氾濫するなど、極めて深刻な情勢が継続している。

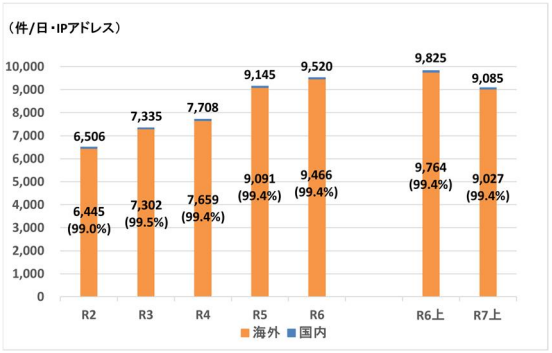
そのような中、警察においては、サイバー特別捜査部を中心に検挙に向けた取組を実施するほか、関係機関との連携を通じた被害の未然防止・拡大防止に向けた取組を実施している。

Ⅰ　サイバー空間の脅威情勢

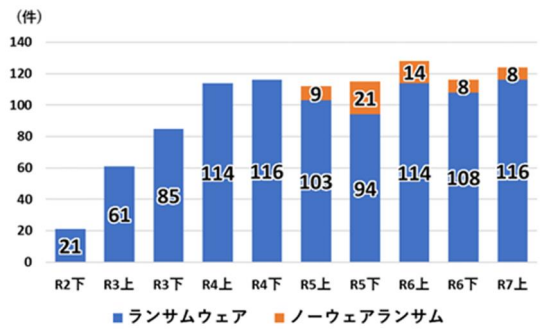
１　高度な技術を悪用したサイバー攻撃の情勢

● 令和７年上半期においては、政府機関や金融機関等の重要インフラ事業者等における DDoS 攻撃とみられる被害や情報窃取を目的としたサイバー攻撃等が相次ぎ発生。

● 警察庁が設置したセンサーにおいて検知した、ぜい弱性探索行為等の不審なアクセス件数は高水準で推移しており、その大部分の送信元が海外。



● 令和７年上半期におけるランサムウェアの被害報告件数は 116 件であり、半期の件数として令和４年下半期と並び最多。

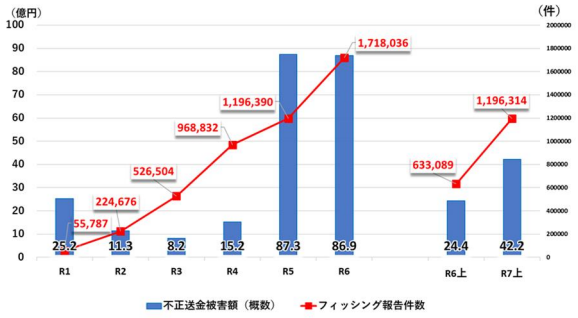


２　インターネット空間を悪用した犯罪に係る情勢

● 情報通信技術の発展が社会に便益をもたらす反面、インターネットバンキングに係る不正送金事案や、SNS を通じて金銭をだまし取る SNS 型投資・ロマンス詐欺、暗号資産を利用したマネー・ローンダリングが発生するなど、インターネット上の技術・サービスが犯罪インフラとして悪用。

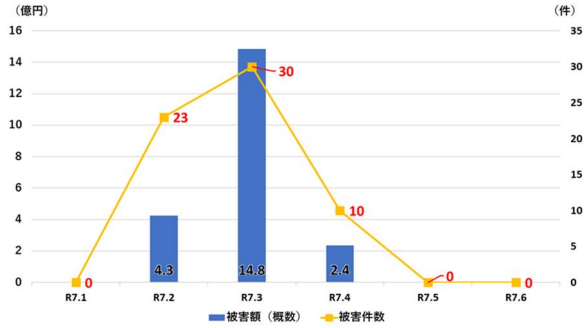
● 令和７年上半期におけるフィッシング報告件数は 119 万 6,314 件、インターネットバンキングに係る不正送金事犯の被害総額は約 42 億 2,400 万円。

フィッシング報告件数及び不正送金被害額の推移



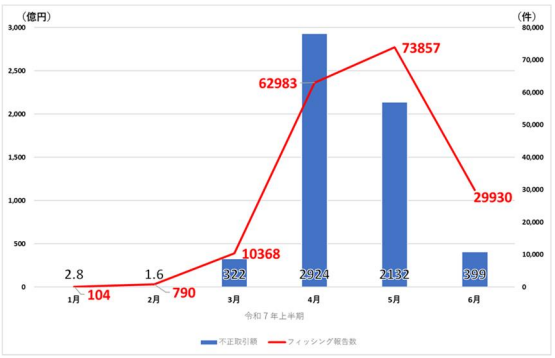
● 令和６年秋以降、犯罪グループが企業に架電し、ネットバンキングの更新手続等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシングという手口による法人口座の不正送金被害が急増。

ボイスフィッシングによる法人口座の不正送金被害件数・被害額



● 令和７年３月から５月にかけて、証券会社をかたるフィッシングメールの送付や証券口座への不正アクセス・不正取引が急増。金融庁及びフィッシング対策協議会によれば、不正売買金額は約 5,780 億円、証券会社をかたるフィッシングメール報告件数は 17 万 8,032 件。

証券口座不正取引額とフィッシング報告件数



３　違法・有害情報に係る情勢

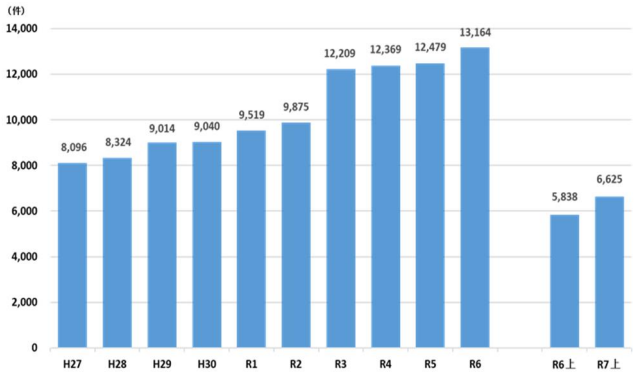
● インターネット上には、規制薬物の広告等の違法情報や犯罪を誘発するような有害情報が存在するほか、近年 SNS 上に氾濫する犯罪実行者募集情報は深刻な治安上の脅威。令和７年上半期中のインターネット・ホットラインセンター（IHC）の受理件数のうち、運用ガイドラインに基づいて 282,787 件を分析した結果、違法情報を 44,973 件と判断。また、犯罪実行者募集情報を 6,346 件と判断。

Ⅱ　警察の取組

１　検挙に向けた取組

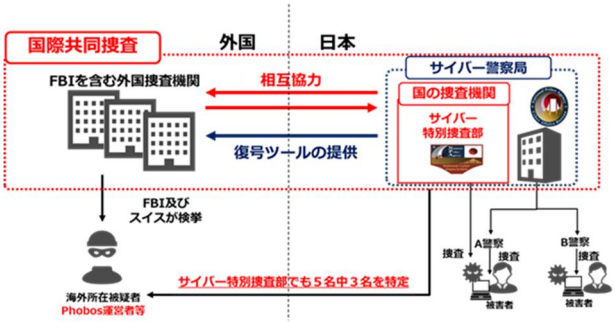
●　サイバー特別捜査部では、重大サイバー事案に、都道府県警察サイバー部門では、高度な専門的知識及び技術を要するサイバー事案に対処。

サイバー犯罪の検挙件数の推移



●　令和７年上半期におけるサイバー犯罪の検挙件数は 6,625 件。

●　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「Phobos（フォボス）」やその関連組織「8Base（エイトベース）」について、サイバー特別捜査部と関係警察は、EUROPOL や FBI 等との国際共同捜査を推進。令和６年 11 月、米国は、「Phobos」の運営者とみられるロシア人の男（42）を起訴。令和７年２月、米国及びスイスは、「８Base」グループ運営者等とみられる男ら４名を検挙。これら５名の被疑者のうち、３名をサイバー特別捜査部の捜査により特定。同結果や当該手法について、関係国の捜査機関に提供。FBI の協力を得つつ、暗号化されたデータを復号するツールを開発し、同年７月、その内容を広く周知。



２　被害の未然防止・拡大防止に向けた取組

●　警察では、捜査や分析で得られた情報に基づき、被害の未然防止に向けた犯行手口の周知等の注意喚起やサイバー攻撃者の公表、広報・啓発を実施。

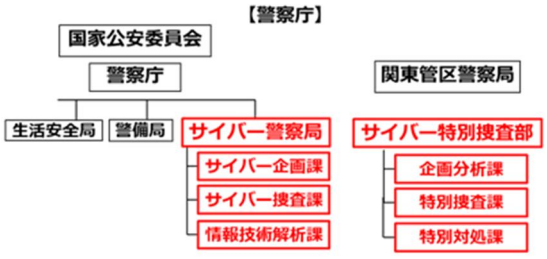
●　令和７年８月、警察庁及び国家サイバー統括室（NCO）は、米国、オーストラリア、ニュージーランド等 13 か国の関係機関により、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名を行い、パブリック・アトリビューションとして、本件アドバイザリーを公表。

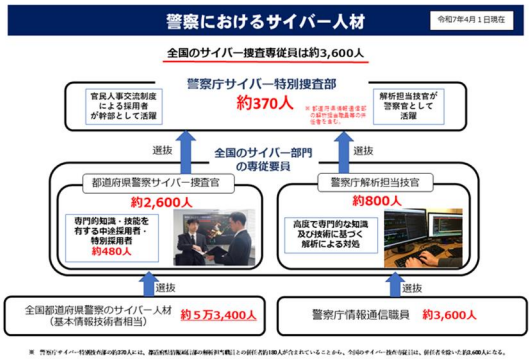
● サイバー事案による被害防止のため、警察では関係機関や民間事業者と連携し、犯罪インフラへの対処を実施。例えば、金融庁、全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（JC3）と連名で、広報啓発資料「サイバー警察局便り」を作成して、警察庁ウェブサイト等にて公開し、ボイスフィッシングによる不正送金被害の手口の詳細や対策に関する注意喚起を実施。

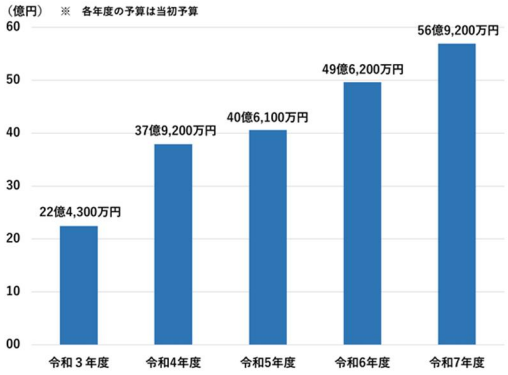
● 警察庁では、インターネット利用者等から違法・有害情報に関する通報を受理し、サイト管理者等への削除依頼等を行うインターネット・ホットラインセンター（IHC）を事業委託。令和７年２月、IHC の運用ガイドラインを改定し、犯罪実行者募集情報を違法情報に位置付け、取組を強化。本年９月の改正ギャンブル等依存症対策基本法の施行に合わせ、インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為等を違法情報に追加すべく、IHC の運用ガイドラインを改定予定。

３　基盤整備

● 令和４年４月、関東管区警察局に、「サイバー特別捜査隊」を設置。令和６年４月、同隊を「サイバー特別捜査部」に発展的に改組。令和７年４月には、サイバー特別捜査部に特別対処課を設置。







● サイバー空間の脅威への対処に係る予算について、令和７年度は 56 億 9,200 万円を計上。

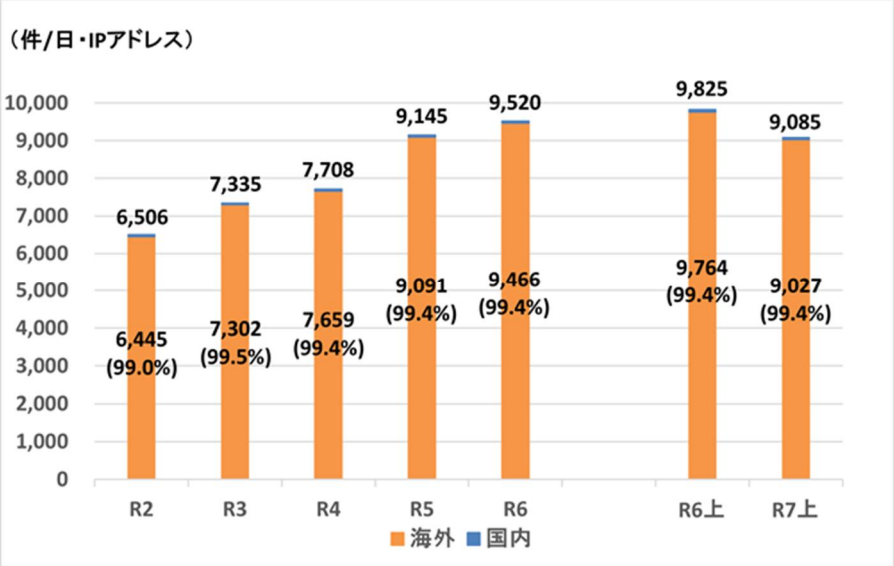
第１部　サイバー空間の脅威情勢

１　高度な技術を悪用したサイバー攻撃の脅威情勢

令和７年上半期においては、政府機関や金融機関等の重要インフラ事業者等における DDoS 攻撃とみられる被害や情報窃取を目的としたサイバー攻撃等が相次ぎ発生した。国や重要インフラ等に対するサイバー攻撃は、安全保障上の懸念を生じさせるおそれがあるなど、サイバー空間における治安の維持は、我が国の安全保障の取組とも密接に絡み合っている。

このようなサイバー攻撃の準備として、攻撃者は攻撃対象を事前に探索する場合があるところ、令和７年上半期に警察庁が設置したセンサーにおいて検知した、ぜい弱性探索行為等の不審なアクセス件数は、１日・１IP アドレス当たり 9,085.4 件（前年比 7.5%減）と、引き続き高水準で推移しており、その大部分が海外を送信元とするアクセスで占められている（図表１）。

【図表１：警察庁が検知した不審なアクセス件数】



また、現在急速に一般社会で利用が広がっている AI についても、様々な便益をもたらすことが期待される一方、不正プログラム、フィッシングメール、偽情報作成への悪用、兵器転用、機密情報の漏えいといった、AI を悪用した犯罪のリスクや安全保障への影響が懸念されている。さらに、AI を悪用することで専門知識のない者でもサイバー攻撃に悪用し得る情報へのアクセスが容易になると考えられている。実際に、生成 AI を利用して不正プログラムを作成した容疑での逮捕事案のほか、生成 AI を悪用した本人確認書類やわいせつ画像の作成といった事例も確認されている。

(1) 国家の関与が疑われるサイバー攻撃

国家の関与が疑われるサイバー攻撃としては、まず、軍事技術へ転用可能な先端技術や、国の機密情報の窃取を目的とするサイバー攻撃（サイバーエスピオナージ）が挙げられる。これは、企業の競争力の源泉を失わせるのみならず、我が国の経済安全保障等にも重大な影響を及ぼしかねず、また、現実空間におけるテロの準備行為として、重要インフラの警備体制等の機密情報を窃取するためにサイバーエスピオナージが行われている懸念もある。例えば、令和元年（2019 年）頃から、日本国内のシンクタンク、政府、政治家、マスコミに関係する個人及び組織に対し、MirrorFace と呼ばれるサイバー攻撃グループが、情報窃取を目的としたサイバー攻撃を行っており、これらサイバー攻撃は、中国の関与が疑われる組織的なサイバー攻撃活動であると評価されている。

また、暗号資産等の窃取による外貨獲得を目的とする国家の関与が疑われるサイバー攻撃も発生している。例えば、令和 6 年（2024 年）3 月、国連安全保障理事会北朝鮮制裁委員会の専門家パネルは、平成 29 年（2017 年）から令和 5 年（2023 年）にかけて世界各国で発生した北朝鮮の関与が疑われる暗号資産関連事業者に対するサイバー攻撃事案 58 件（被害額約 30 億米ドル相当）を調査した結果、北朝鮮における外貨収入の約半数がサイバー攻撃により獲得され、大量破壊兵器計画に使用されていると公表した。我が国においても、令和 6 年（2024 年）5 月、北朝鮮を背景とするサイバー攻撃グループ TraderTraitor が、国内の暗号資産関連事業者から約 482 億円相当の暗号資産を窃取した事案が発生している。

さらに、重要インフラの機能停止等を企図したとみられる国家の関与が疑われるサイバー攻撃も発生している。例えば、令和 4 年（2022 年）5 月には、ロシアによるウクライナ侵略の際の約 1 時間前に、ロシア政府が国際衛星通信へのサイバー攻撃を行い、欧州全域に影響を及ぼした事案が発生したとして、EU やウクライナ等が非難声明を発表している。令和 6 年（2024 年）2 月には、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）等が複数国の関係機関と合同で、中国を背景とするサイバー攻撃グループ Volt Typhoon によるサイバー攻撃に関する注意喚起を実施しており、米国の重要インフラ事業者への侵害が確認されているほか、有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークへのアクセス権限を確保している旨が指摘されている。また、同グループによるサイバー攻撃の特徴として、Living Off The Land 戦術等による高

度な検知回避能力が挙げられているところ、同攻撃手口に関しては、ネットワーク機器のぜい弱性の悪用等により侵入を行った後、従来から行われているマルウェアを用いたサイバー攻撃とは異なり、システム内に組み込まれている正規の管理ツール、コマンド、機能等を用いることから検知が容易ではないとして、令和６年６月、内閣サイバーセキュリティセンター（NISC）等が注意喚起を実施している。

(2) 犯罪組織等によるサイバー攻撃

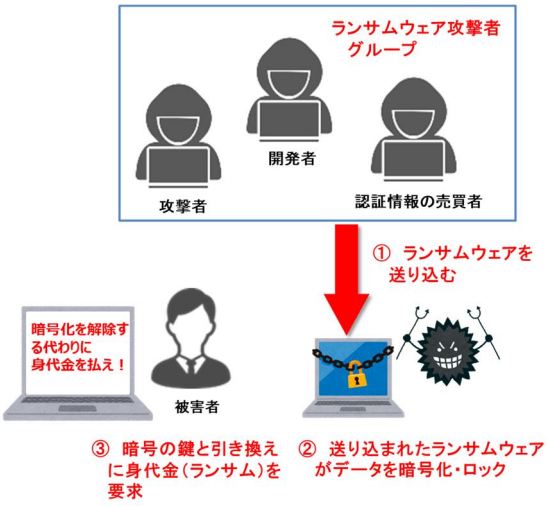
犯罪組織等によるサイバー攻撃としては、まずランサムウェアによる攻撃が挙げられる。ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラムであり（図表２）、近年は、データを窃取したうえ、「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝の被害も多くみられる。また、ランサムウェアによって流出したとみられる事業者の財務情報や個人情報等が、ダークウェブ上のリークサイトに掲載されていたことが確認されている。

攻撃の態様としては、ランサムウェアの開発・運営を行う者が、攻撃の実行者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もの（RaaS：Ransomware as a Service）も確認されている。また、EC サイトのぜい弱性を悪用するなどにより窃取した、標的企業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も存在するように、複数の関与者が役割を分担してサイバー攻撃を成り立たせている。その結果、攻撃の実行者が技術的な専門知識を有する必要もなくなるなど、攻撃者の裾野の広がりがみられている。

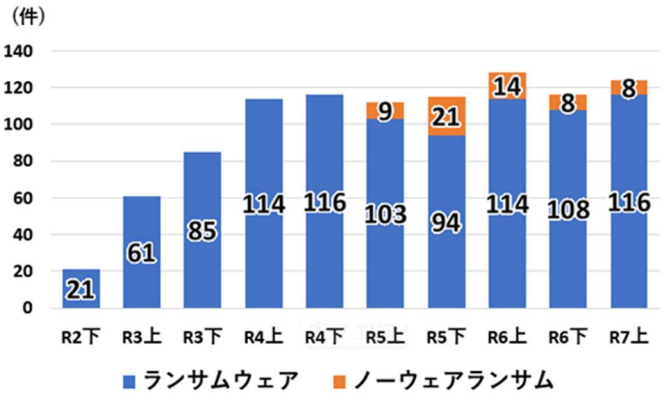
【CASE：保険大手企業に対するランサムウェア攻撃事案】

令和７年２月、保険代理店関連事業等を運営する保険大手企業は、同社のサーバがランサムウェア攻撃を受けたことを発表した。その後の調査により、データサーバの一部で保管しているファイルが暗号化されていることが判明したほか、約 510 万件を超える個人情報が漏えいしたおそれがあることなどを発表した。

【図表２：ランサムウェア攻撃の流れ】



【図表３：ランサムウェア被害報告件数】

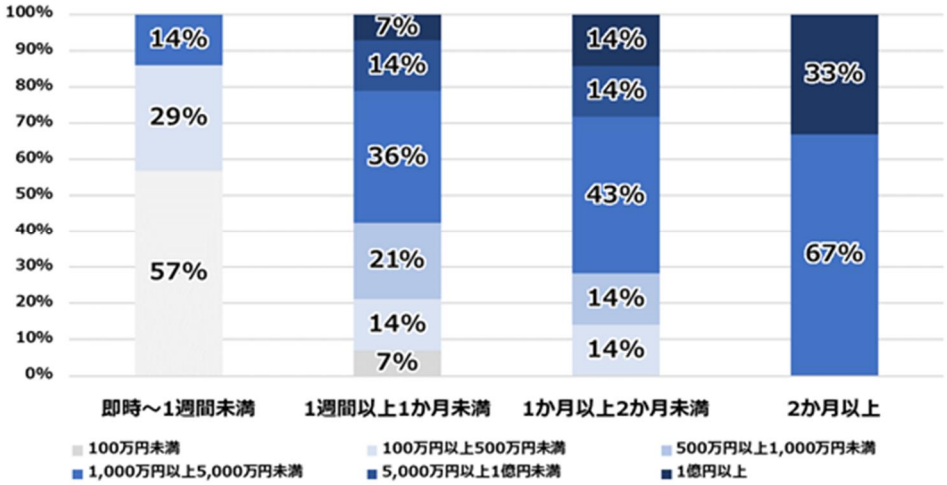


※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

令和７年上半期におけるランサムウェアの被害報告件数は 116 件であり、半期の件数として令和４年下半期と並び最多となった。組織規模別のランサムウェア被害件数は、前年と同様に中小企業が狙われる状況が継続しており、77 件で約３分の２を占めて件数・割合ともに過去最多となった。RaaS による攻撃実行者の裾野の広がりが、対策が比較的手薄な中小企業の被害増加につながっていると考えられる。

ランサムウェアによる被害に遭った企業・団体等に実施したアンケートの結果によると、令和６年と比較して、ランサムウェアの被害による調査・復旧費用が高額化しており、1,000 万円以上を要した組織の割合は、50%から 59%に増加した。中小企業の被害が増える中で費用負担が増加しており、被害組織の経営に与える影響は決して小さくないと考えられる。

【図表４：ランサムウェア被害からの復旧期間と費用の関係性】



※　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。

コラム：ランサムウェアに関するサイバー特別捜査部による分析

前述のアンケート結果によると、VPN やリモートデスクトップ用の機器からの侵入が、全体の感染経路の８割以上を占める状況である。その原因としては、当該機器の ID・パスワード等が非常に安易であったことや、不必要なアカウントが適切に管理されずに存在していたことなどが挙げられる。(P59 参照)

実際、海外支社等の機器を管理できていなかったためにそこから侵入され、国内の本社が被害に遭う事例や、試験的に作成したアカウントの安易な認証情報を利用されて侵入された事例を把握している。

また、ランサムウェアグループは身代金を得るために日々策を講じており、例えば、

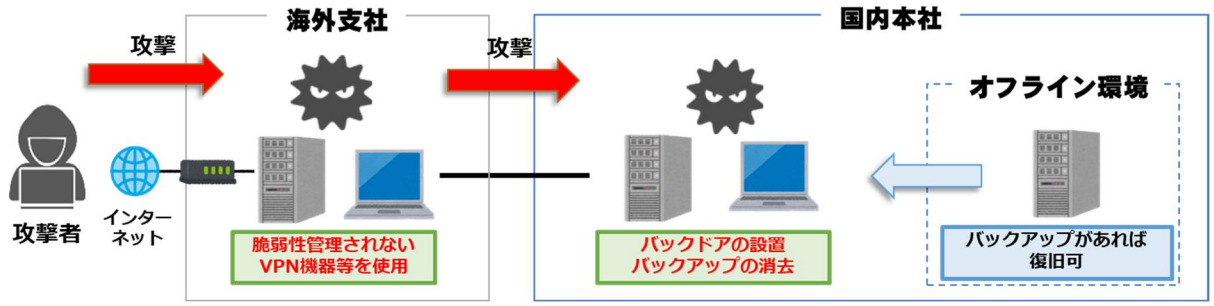
- 土日が休業日の企業を狙う場合に、金曜日の営業終了後にシステムに侵入して月曜日の朝までに暗号化を実行する
- 被害企業に侵入口を閉じられた場合でも再侵入できるように、遠隔操作可能なソフトウェアをバックドアとして設置する
- 侵入時の痕跡を消したり、復旧作業をさせないために、被害企業のログやバックアップを消去する

などしている。

なお、ログは、被害企業が侵入の実態調査やバックアップからの復旧対応を行う際に必要であり、ログが保存されていない場合、適切な対策を講じることができずに脆弱性が放置され、再被害のおそれがあるほか、バックアップからの復旧対応に支障を及ぼすおそれがある。

このため、日頃からのログの取得・保管やバックアップのオフライン環境での保管といった対策が求められる。

【サイバー特捜部による分析結果概要】



次に、犯罪組織等によるサイバー攻撃として、DDoS 攻撃が挙げられる。重要インフラの基幹システムに障害を発生させるサイバー攻撃（サイバーテロ）は、インフラ機能の維持やサービスの供給を困難とし、国民の生活や社会経済活動に重大な被害をもたらすおそれがある。

例えば、令和 6 年 12 月下旬から令和 7 年 1 月上旬にかけ、交通機関や金融機関等の重要インフラ事業者等において、DDoS 攻撃によるとみられる被害が相次いで発生し、空港において手荷物の自動チェックイン機が使えない障害や、インターネットバンキングにログインしづらい状況が発生するなど、実際に国民の生活に被害がもたらされた。（P11 参照）

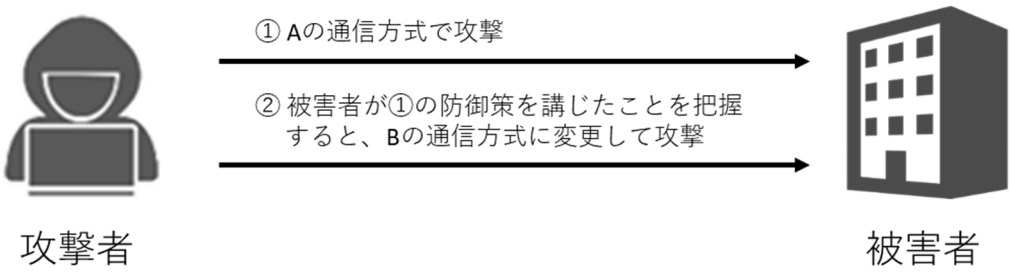
また、令和 7 年 6 月、政府機関、自治体、民間事業者等が運営する複数のウェブサイトにおいて DDoS 攻撃による被害とみられる閲覧障害が複数発生した。同じ頃、SNS 上に、ハクティビストのものと思われるアカウントから、それらの犯行をほのめかす投稿が確認された。

コラム：年末年始にかけての重要インフラ事業者等に対する DDoS 攻撃

令和６年から令和７年の年末年始にかけ、交通機関や金融機関等の重要インフラ事業者等において、DDoS 攻撃によるとみられる被害が相次いで発生し、空港において手荷物の自動チェックイン機が使えない障害や、インターネットバンキングにログインしづらい状況が発生するなど、実際に国民の生活に被害がもたらされた。

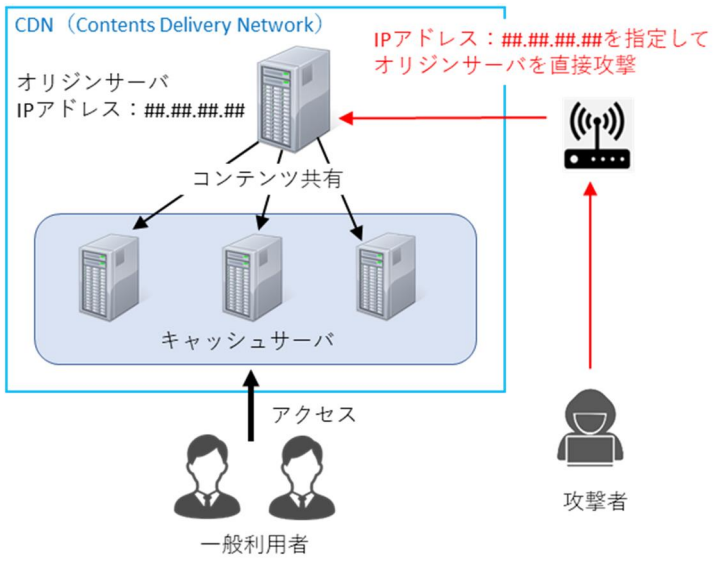
警察においては、当該 DDoS 攻撃について、複数の手口を確認しており、また、攻撃に対し事業者が遮断措置を講じた場合でも、状況に応じて手口を変化させ、攻撃を継続する事例を確認している。

【年末年始にかけての重要インフラ事業者等に対する DDoS 攻撃の手口】



また、IP アドレスを指定し、ウェブコンテンツのオリジナルデータが保存されているオリジンサーバを直接標的にすることで、アクセスの分散によって負荷軽減を実現している CDN（Contents Delivery Network）を回避する攻撃が複数の事案で確認された。

【DDoS 攻撃によるオリジンサーバへの攻撃（イメージ）】



DDoS 攻撃による被害を抑えるための対策として、オリジンサーバに対する CDN を経由しないアクセスの遮断、組織外にオリジンサーバの IP アドレスが露見しないような DNS 設定の見直し、海外に割り当てられた IP アドレスからの通信の遮断、アクセスを監視し攻撃を検知・遮断する機能を持つような対策装置やサービスの導入、サーバ装置、端末、通信回線装置及び通信回線の冗長化等が求められる。

２　インターネット空間を悪用した犯罪に係る脅威情勢

情報通信技術の著しい発展や、日常生活や経済活動へのサイバー空間の浸透は社会に様々な便益をもたらす反面、サイバー空間を舞台とした犯罪をはじめ、新たな治安課題を生み、また深刻化させており、このような情勢は、令和６年中の警察に対する相談のうち、サイバー関係の相談数が約 18 万 6,000 件を占めるなど、高水準で推移していることからも見てとれる。

インターネット上で提供される技術・サービスの中には、犯罪インフラとして悪用され、犯罪の実行を容易にし、あるいは助長するものも存在している。例えば、SNS や匿名性の高いメッセージングアプリは犯罪実行者の募集や、犯罪グループ間の連絡手段として使われ、SMS やメールはフィッシングに悪用されている。また、インターネットバンキングや暗号資産は、特殊詐欺等における被害金の送金先やマネー・ローンダリングなどに悪用されている。さらに、ペイメントサービスのアカウント作成等に利用される SMS 機能付きデータ通信専用 SIM は、契約時の本人確認の義務付けがないことから、犯罪インフラとして悪用されている。

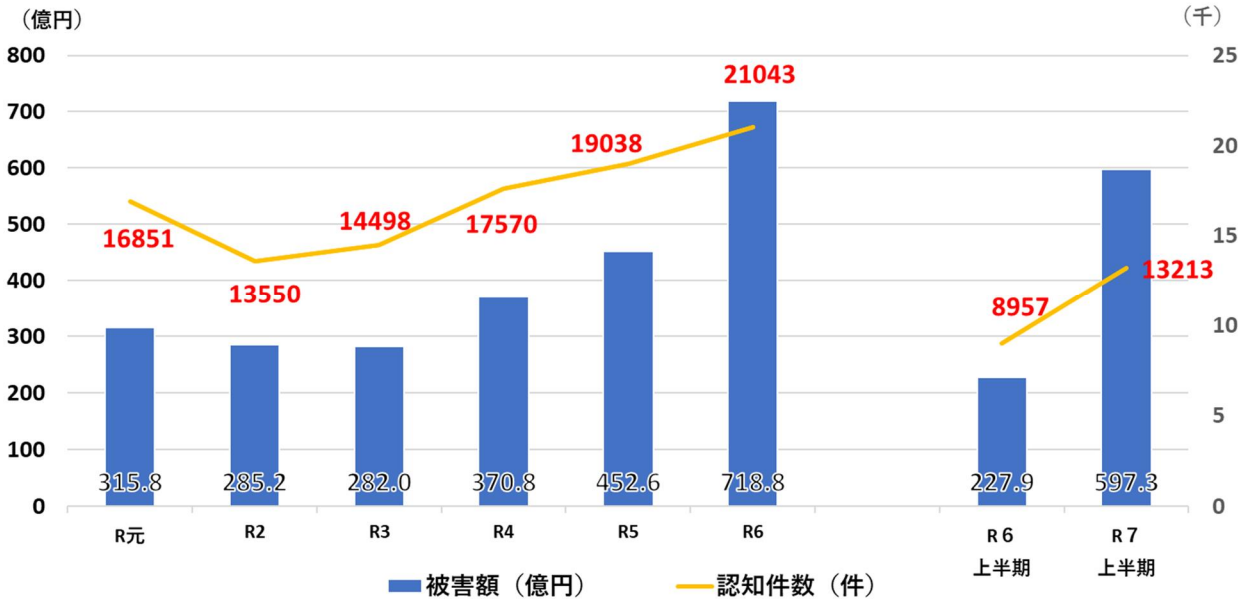
以下、犯罪インフラとして悪用されている技術・サービス別に詳細を記述する。

(1)　SNS・メッセージングアプリ等を悪用した犯罪

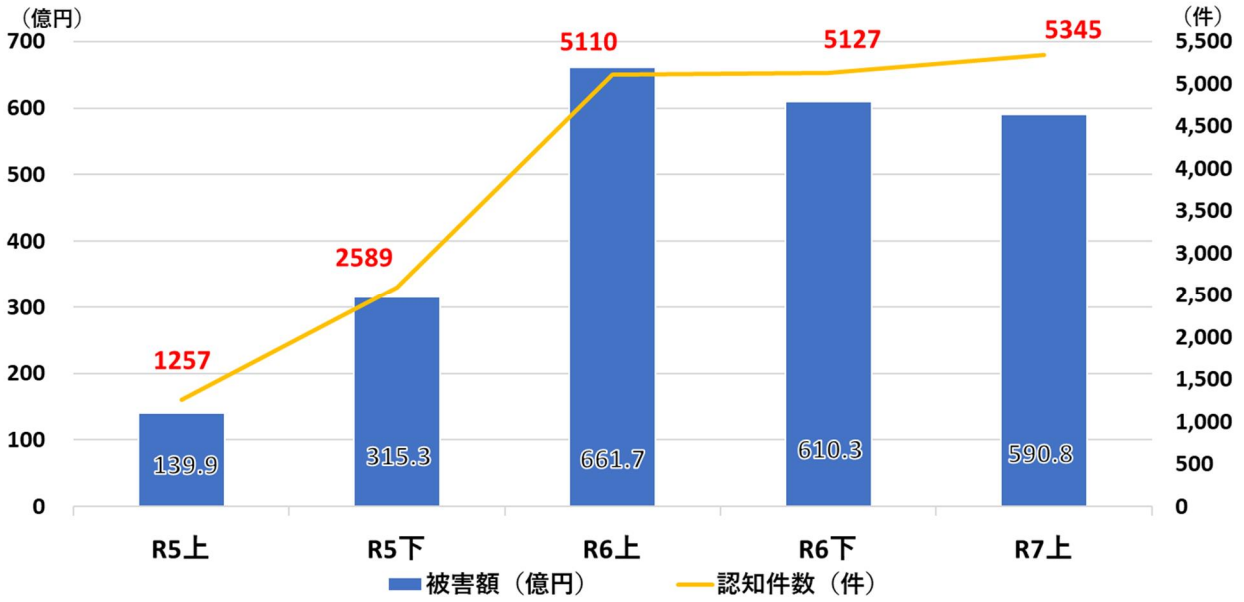
多くの国民が利用する SNS は、犯罪インフラとして悪用されている実態がみられる。例えば、各種犯罪により得た収益を吸い上げる中核部分が匿名化され、SNS を通じるなどしてメンバー同士が緩やかに結び付くなどの特徴を有する「匿名・流動型犯罪グループ」が、SNS で仕事の内容を明らかにせず、「高額」「即日即金」「ホワイト案件」等、「楽で、簡単、高収入」を強調する表現を用いるなどして、犯罪実行者を募集し、特殊詐欺等を敢行している実態がみられる。その際、首謀者、指示役、犯罪実行者の間の連絡手段には、匿名性が高くメッセージが自動的に消去される仕組みを備えた通信手段が悪用されている実態がみられる。このほか、同グループの関与が認められるものとして、SNS を通じて対面することなく、やり取りを重ねるなどして関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭をだまし取る又は恋愛感情や親近感を抱かせて金銭をだまし取る SNS 型投資・ロマンス詐欺があり、まさに SNS が犯罪インフラとして悪用されている。

令和７年上半期中の、特殊詐欺の被害額は約 597 億 3,000 万円（前年同期比 162.1%増）と、過去最悪となった令和６年の被害額を上回るペースで推移しており、SNS 型投資・ロマンス詐欺の被害額についても約 590 億 8,000 万円（前年同期比 10.7%減）と昨年に引き続き高止まりしている状況となっている。

【図表５：特殊詐欺の認知件数・被害額】



【図表６：SNS 型投資・ロマンス詐欺の認知件数・被害額】



このような事案に関しては、インターネットを通じて知り合った人物から誘われ、海外渡航した結果、特殊詐欺に加担させられる事案も発生している。

また、近年は、SNS 上での特定の個人に対する誹謗中傷も社会問題化しているほか、SNS の匿名で不特定多数の者に瞬時に連絡を取ることができる特性から、児童買春等の悪質な事犯の「場」となっている状況もうかがえる。実際、

SNS に起因して性犯罪等の被害に遭った児童の数は、依然として高い水準で推移している。特に、小学生の被害児童数が近年増加傾向にあり、被害児童の低年齢化が懸念される状況にある。

加えて、インターネットやスマートフォンの普及に伴い、画像情報等の不特定多数の者への拡散が容易になったことから、交際中に撮影した元交際相手の性的画像等を撮影対象者の同意なくインターネット等を通じて公表する行為により、被害者が長期にわたり精神的苦痛を受ける事案も発生している。

さらに、オンラインゲームに関連する事案も発生しており、例えば、オンラインゲーム内のアイテムを現実世界で取引するリアルマネートレードに起因する犯罪が発生している。

一般財団法人日本サイバー犯罪対策センター（JC3 [1]）（P33 参照）では、警察やサイバー防犯ボランティアの協力の下、その利用におけるトラブル実態把握のためのアンケート調査を行った。

アンケート結果からは、オンラインゲームに関するトラブルに巻き込まれたことがあると回答した人の大半はゲーム内チャットなどのコミュニケーションにまつわるトラブルであったが、その内、3 割程度がアカウント乗っ取りや DDoS 攻撃、リアルマネートレードのトラブルに巻き込まれていることが確認された。

(2) メール・SMS を悪用した犯罪

メールや SMS は、フィッシングに悪用される実態がみられる。フィッシングとは、実在する組織を装ってメールや SMS のリンクから偽のウェブサイト（フィッシングサイト）へ誘導し、同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、これによって得られた情報は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。

令和 7 年上半期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 6,314 件であり、右肩上がりの増加が続いている。

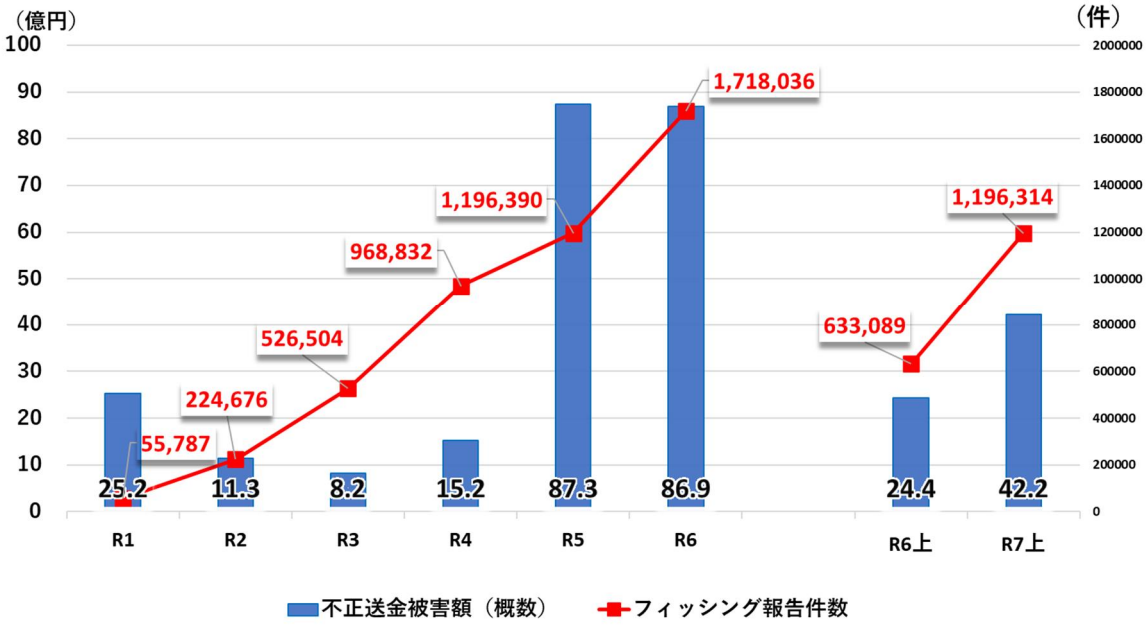
また、令和 7 年上半期におけるインターネットバンキングに係る不正送金事犯の発生件数は 2,593 件、被害総額は約 42 億 2,400 万円となっており、フィッシングがその手口の約 9 割を占める。

なお、令和元年頃からリアルタイム型フィッシングにより二段階認証を突破

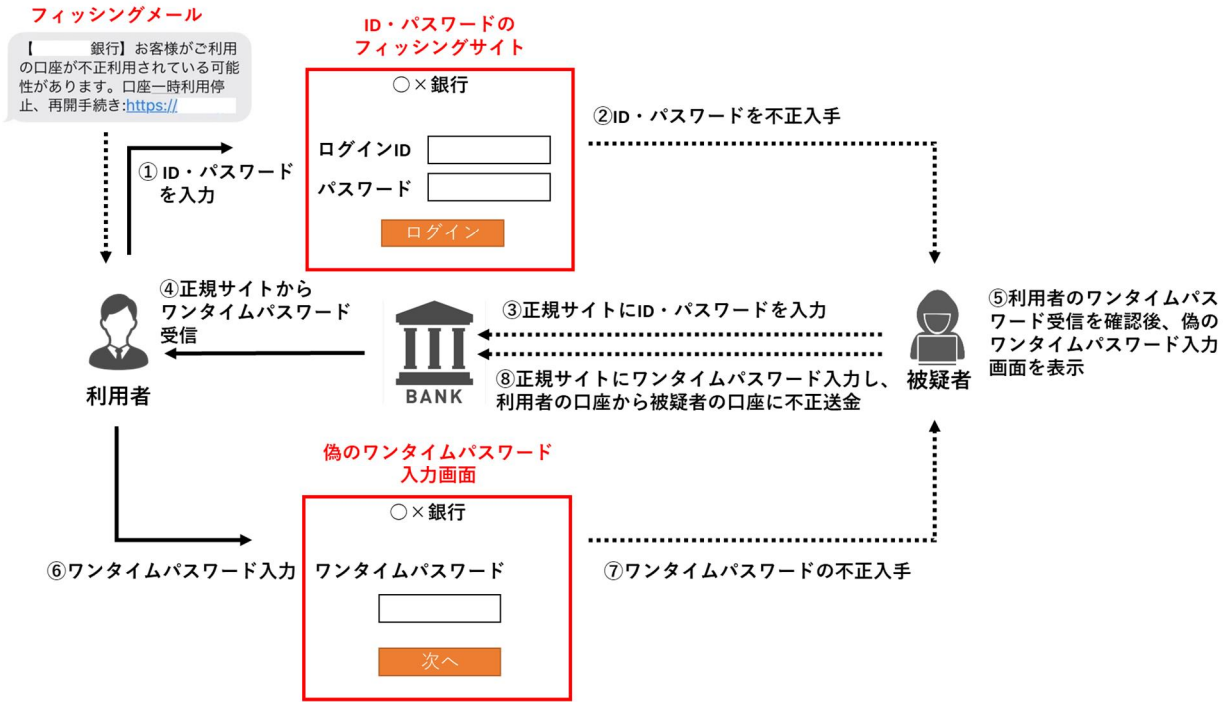
[1] Japan Cybercrime Control Center の略

する手口が横行している。

【図表７：フィッシング報告件数及びインターネットバンキングに係る不正送金被害額】



【図表８：リアルタイム型フィッシングの手口】

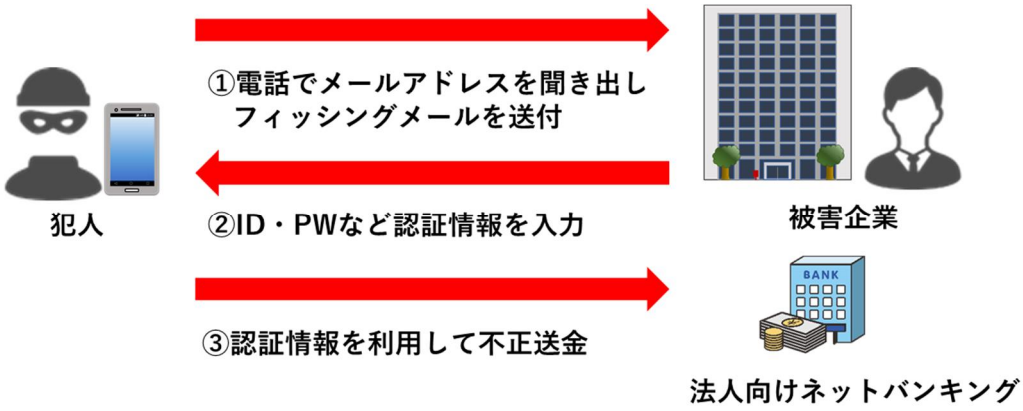


コラム：ボイスフィッシングによる不正送金被害

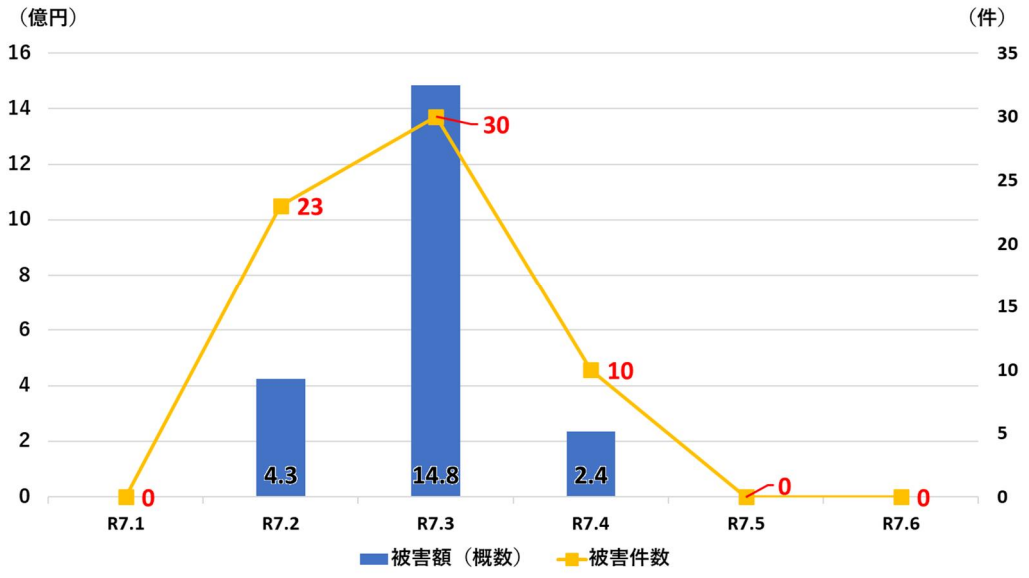
令和６年秋以降、犯罪グループが企業に架電し、ネットバンキングの更新手続等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシング（ビッシング）という手口による法人口座の不正送金被害が急増した。令和７年上半期においては、同年４月にかけて、地方を拠点とした中小規模の金融機関でも多くの被害が出たほか、１回あたりの不正送金額が約４億円となる高額な被害がみられるなど、被害件数及び被害額が急激に増加した。

警察庁及び金融庁では、同種被害を防止するため、注意喚起を始めとした各種対策を講じ、同年４月における被害件数及び被害額は同年３月に比して大きく減少し、同年５月及び６月には被害の発生はみられなかった。

【ボイスフィッシングの流れ】



【図表９：ボイスフィッシングによる法人口座の不正送金被害件数・被害額】



なお、不正送金に関するフィッシング以外の手口については、マルウェア感染を契機とした事例や SIM スワップ[2]によって本人確認を突破する手口も引き続きみられた。

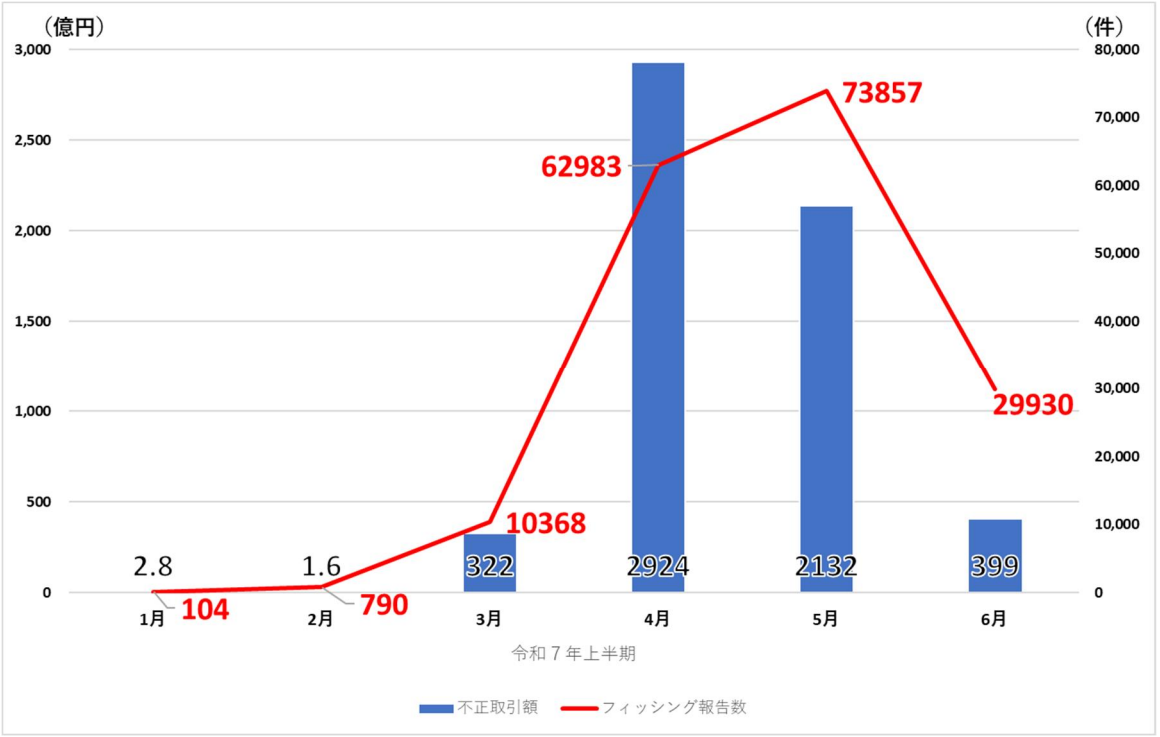
コラム：証券口座への不正アクセス等の急増

令和７年３月から５月にかけて、証券会社をかたるフィッシングメールの送信や証券口座への不正アクセス及び不正取引が急増した。

金融庁及びフィッシング対策協議会によれば、令和７年上半期における証券口座への不正アクセス件数は 13,121 件、不正取引件数は 7,277 件、不正売買金額は約 5,780 億円、証券会社をかたるフィッシングメール報告件数は 17 万 8,032 件となっており、フィッシングメールの増加に伴い、証券口座への不正アクセス及び不正取引も増加したものとみられる。

なお、証券会社におけるインターネット取引認証の強化、警察庁及び金融庁による注意喚起を始めとした各種対策により、同年６月における証券会社をかたるフィッシングメール報告件数及び証券口座不正取引額は同年５月に比して大きく減少した。

【図表 10：証券口座不正取引額と証券口座に関するフィッシング報告件数の推移】

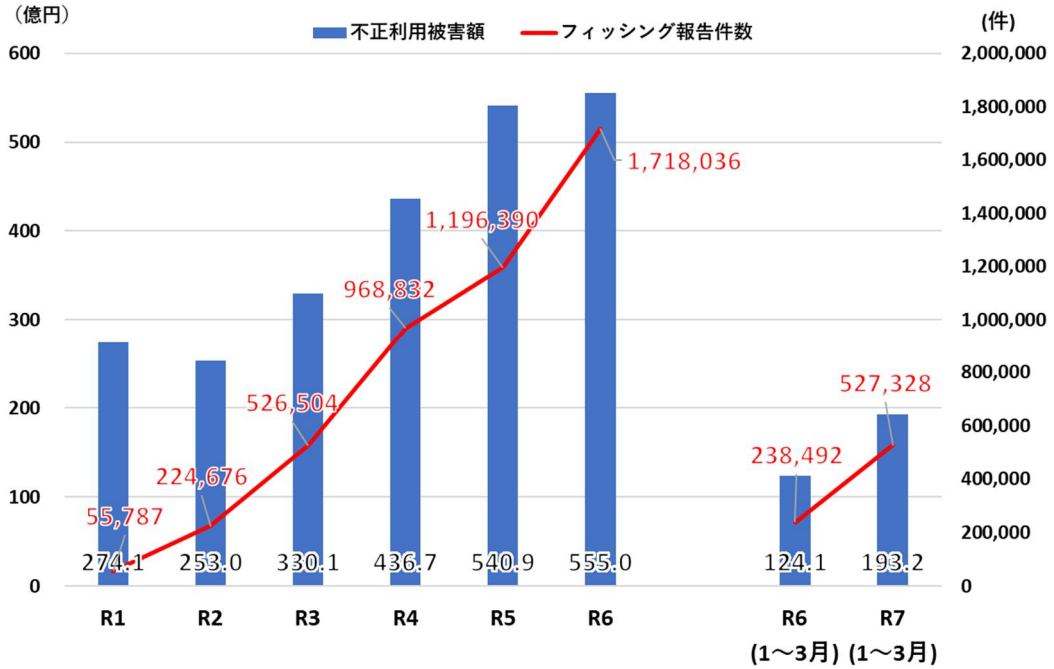


※　不正取引額：金融庁資料による。フィッシング報告件数：フィッシング対策協議会資料による。

[2] 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、他人に成りすまして MNP（携帯電話番号ポータビリティ）や SIM カードの再発行手続きを行い、携帯電話番号を乗っ取る手口をいう

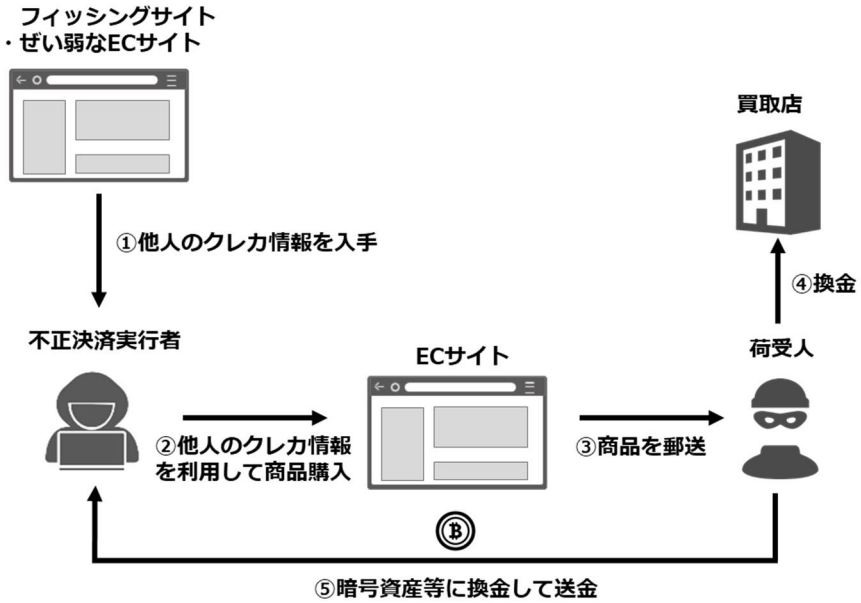
さらに、一般社団法人日本クレジット協会によれば、令和７年１月から３月までのクレジットカードの不正利用被害額は約 193 億円（前年比 55.6%増）と、依然として厳しい情勢にある。

【図表 11：フィッシング報告件数及びクレジットカード不正利用被害額】



※　一般社団法人日本クレジット協会・クレジットカード不正利用被害の発生状況から作成（以下同）

【図表 12：クレジットカード不正利用の流れ】

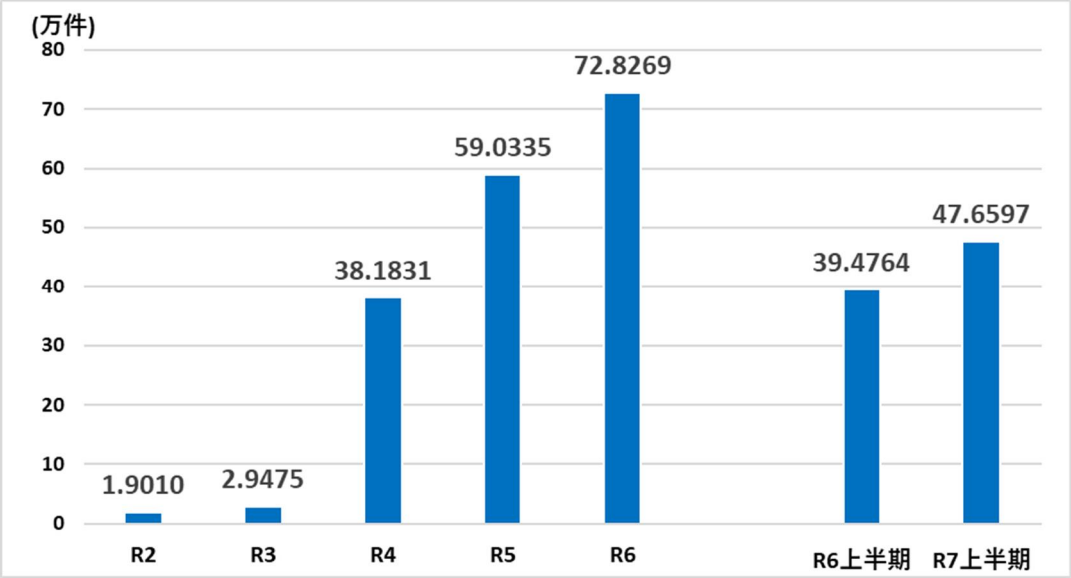


(3)　ウェブサイトを悪用した犯罪

SNS や SMS の利用なく、ウェブサイトそのものが悪用されて犯罪が敢行される実態もみられる。例えば、海外のサーバを通じてインターネット上に掲載

された、実在する企業のサイトを模したフィッシングサイトのほか、インターネットショッピングに係る詐欺や偽ブランド品販売を目的とするサイト等（以下単に「偽サイト等」という。）に係る被害が多発しているところ、警察庁においては、都道府県警察等が相談等を通じて把握した偽サイト等に係る URL 情報を集約しており、その件数は右肩上がりに増加している。

【図表 13：警察庁に対する偽サイト等の情報報告件数】



また、パソコンでインターネットを閲覧中に、突然ウイルスに感染したかのような嘘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だまし取ったり、遠隔操作ソフトをインストールさせたりするサポート詐欺の被害も発生している。令和 7 年上半期における架空料金請求詐欺のうち、パソコンのウイルス除去をサポートするなどの名目で電子マネー等をだまし取る「サポート名目」の認知件数は 679 件、被害額は約 8 億 5,000 万円となっている。

(4)　インターネット空間の資金移動を悪用した犯罪

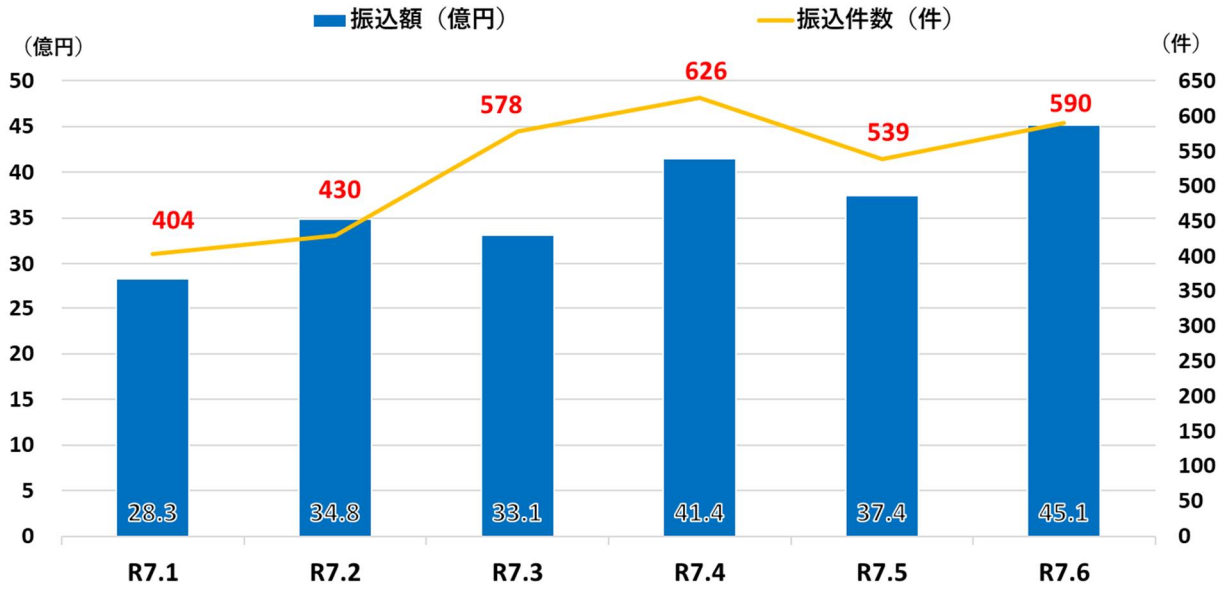
インターネット空間における資金移動は利便性が高い一方、インターネットバンキングでは、振込の 1 日の上限額を容易に引き上げられる、送金時に第三者の目が届きにくいといった特徴から、犯罪に悪用される実態があり、また、暗号資産についても、匿名性の高さなどから、マネー・ローンダリングに利用される実態が見られる。

①　インターネットバンキング

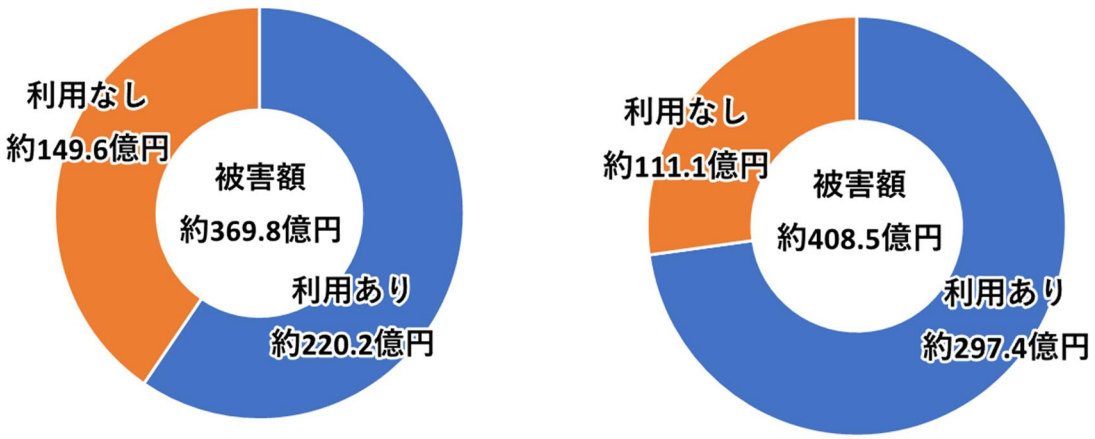
特殊詐欺の被害のうち、振込型による被害（認知件数 8,213 件、被害額約 369 億 8,000 万円）を分析すると、インターネットバンキングを利用したものの認知件数・被害額は増加傾向にあり、認知件数は振込型全体の約 4 割、被害額は振込型全体の約 6 割を占めている。

さらに、SNS 型投資・ロマンス詐欺の被害のうち、振込型による被害（認知件数 3,560 件、被害額約 408 億 5,000 万円）を分析すると、インターネットバンキングを利用したものの認知件数は振込型全体の約 6 割、被害額は振込型全体の約 7 割を占めている。

【図表 14：特殊詐欺におけるインターネットバンキングを利用した振込被害】



【図表 15：令和 7 年上半期の特殊詐欺（左）／SNS 型投資・ロマンス詐欺（右）の振込型に係る被害額に関するインターネットバンキングの利用の有無】



②　暗号資産

暗号資産については、利用者の匿名性が高く、その移転がサイバー空間において瞬時に行われるという性質から、犯罪に悪用されたり、犯罪収益等が暗号資産の形で隠匿されたりするなどの実態がみられる。特に、海外の暗号資産交換業者で取引される暗号資産の中には、取引に関する情報を秘匿化できる暗号資産もあり、マネー・ローンダリングに利用されるおそれが高いものも存在する。また、インターネットバンキングに係る不正送金においても、不正送金された現金を、暗号資産に交換した後、取引の匿名性を高めるサービスや、暗号資産取引所を介さず個人間で暗号資産取引を行う相対屋を経由しながら送金を繰り返すなどして取引を複雑化させ、追跡を困難にしている。

【図表 16：暗号資産を悪用したマネー・ローンダリングのイメージ】

3　違法・有害情報に係る情勢

インターネット上には、規制薬物の広告等、インターネット上の流通そのものが法令に違反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有害情報が存在する。

(1)　主な違法・有害情報の類型

違法情報の主なものとしては、「児童ポルノ公然陳列」、「覚醒剤等の規制薬物の広告」、「犯罪実行者の募集」といった類型が挙げられる。

また、有害情報の主なものとしては、「爆発物の製造」、「殺人の請負」、「自殺の誘引・勧誘」といった類型が挙げられる。

(2)　犯罪実行者募集情報

【図表 17：犯罪実行者募集のイメージ】

近年インターネット上には、匿名・流動型犯罪グループ等による犯罪の実行者を募集する犯罪実行者募集情報が氾濫しており、応募者らにより実際に強盗や特殊詐欺等の犯罪が敢行されるなど、この種情報の氾濫がより深刻な治安上の脅威になっている。

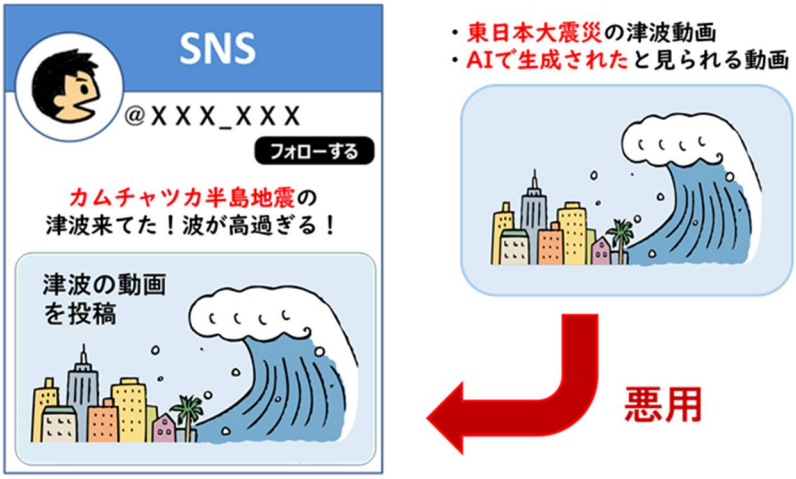
強盗・窃盗等についても、SNS や求人サイト等で「高額」、「即日即金」「ホワイト案件」等の文言を用いて犯罪実行者が募集された上で実行される実態がうかがわれる。このような匿名・流動型犯罪グループによるものとみられる手口により実行された強盗事件等の中には、被害者を拘束した上で暴行を加えるなど、その犯行態様が凶悪なものもみられる。

(3)　災害発生時等における偽情報

大規模災害発生時におけるインターネット上の偽情報・誤情報については、信ぴょう性の確認や判断に時間を要し、被災地等において救助活動への支障や社会的混乱を生じさせるおそれがある。

実際、災害時に、過去の震災の際に撮影された画像を悪用して、同地域における治安が悪化したり、甚大な被害が発生したりしているとの印象を与えるような日本語・外国語の偽情報等が SNS 上で拡散された事例等が確認されている。

【図表 18：SNS 上における偽情報投稿のイメージ】



(4) オンライン上で行われる賭博事犯

警察庁では、令和６年度、オンラインカジノの利用実態やサイトの情報を把握するため、調査研究を行っており、この結果、国内におけるオンラインカジノサイトの利用経験者の推計は約 337 万人であり、国内における年間賭額の推計は約１兆 2,423 億円であった。

スマートフォン等からアクセスして賭博を行う「無店舗型」のオンラインカジノについては、アクセス数の増加及びこれに伴う依存症への問題が強く指摘されているほか、これを通じた我が国資産の海外流出、マネー・ローンダリングへの利用等が懸念されている。

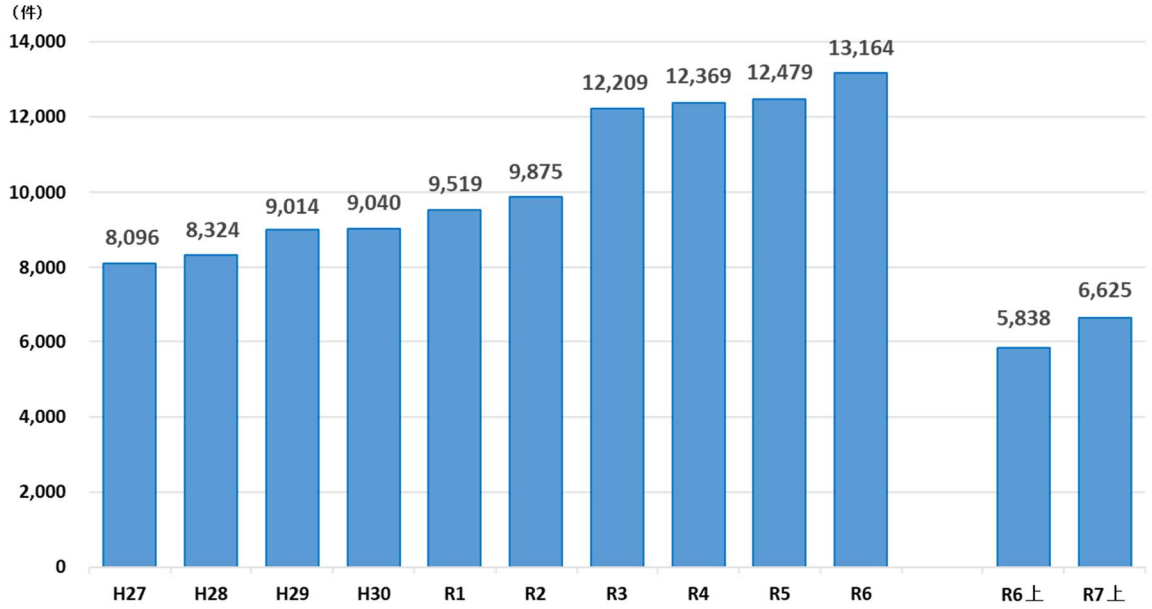
第２部　警察の取組

１　検挙に向けた取組

第１部に記載した脅威情勢に対し、警察では検挙に向けた取組を推進しているところ、サイバー特別捜査部においては重大サイバー事案[3]に、都道府県警察サイバー部門においては、高度な専門的知識及び技術を要するサイバー事案[4]に対処している。また、あらゆる犯罪がインターネット空間を悪用しているともいえる現状を受け、サイバー部門以外の捜査部門においてもサイバー事案やサイバー犯罪[5]に対処できるよう、技術的な支援を行うことができる体制を確保している。

この結果、令和７年上半期におけるサイバー犯罪の検挙件数は 6,625 件に達している。サイバー犯罪の検挙件数のうち、犯罪収益移転防止法の検挙件数は 1,312 件で、そのうち 465 件が匿名性の高い通信方法を用いた犯行としてサイバー事案にも該当し、前年と比較していずれも増加している。

【図表 19：サイバー犯罪の検挙件数】



(1)　検挙

①　サイバー特別捜査部

サイバー特別捜査部は、その高度な情報集約・分析機能により全国警察の

[3] サイバー事案のうち、国若しくは地方公共団体の重要なシステムの運用や重要インフラ事業者の事業の実施に重大な支障が生じ、若しくは生ずるおそれのある事案、高度な技術的手法が用いられるなどの事案（マルウェア事案等）、又は国外に所在するサイバー攻撃者による事案

[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。警察庁サイバー警察局は、「サイバー事案に関する警察に関する」事務をつかさどることが、その所掌業務の一つとなっている（警察法第 25 条第１号）。

[5] 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

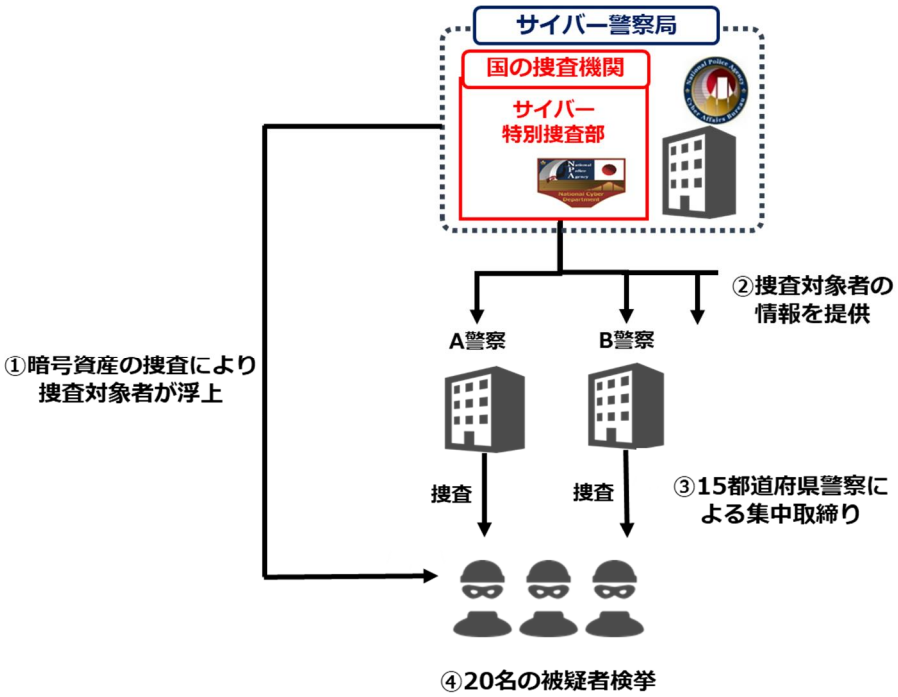
ハブとしての役割を果たすとともに、そうして得られた情報と外国捜査機関等との強固な信頼関係を武器に、国際共同捜査等を通じて、国境を越えて敢行されるサイバー事案に対処する、いわば世界と日本との結節点としての役割を果たしている。

【CASE：暗号資産を利用したクレジットカード関連犯罪に関する集中取締り】

サイバー特別捜査部において、フィッシング等により不正に取得されたクレジットカードの情報が、匿名性の高い通信アプリ等を通じて売買され、その支払いに暗号資産が用いられている実態を認知したことから、全国のクレジットカード情報の不正利用関連犯罪の情報を分析し、クレジットカード情報の支払いの対価と認められる暗号資産の流れを捜査した結果、全国各地で捜査対象者を浮上させた。

令和６年９月から令和７年３月までの間に、サイバー特別捜査部及び 15 都道府県警察が緊密に連携して集中取締りを実施し、他人のクレジットカード情報の不正購入や同情報の不正利用について、10 代から 50 代までの男女 20 名の被疑者を検挙した。

【図表 20：暗号資産を利用したクレジットカード関連犯罪に関する集中取締りの概要】



②　都道府県警察サイバー部門

サイバー事案のうち、捜査に当たり高度な専門的知識及び技術を要するものについては、都道府県警察のサイバー部門において捜査等を推進している。

コラム：複数の少年グループによる eSIM 不正取得等事件の検挙

SNS で結びついた中高生の少年３人（14 歳から 16 歳）は、不正に取得した eSIM を販売して利益を得ようと考え、令和６年５月から同年８月までの間に、それぞれ、不正に取得した他人の ID とパスワードを使い、電気通信事業者が管理するサーバコンピュータに不正アクセスした上で、通信契約に係る不実の電磁的記録を作成し、eSIM を不正に取得した。令和７年１月から同年２月にかけて、同少年らを不正アクセス禁止法違反及び電子計算機使用詐欺罪等で逮捕した。（警視庁）

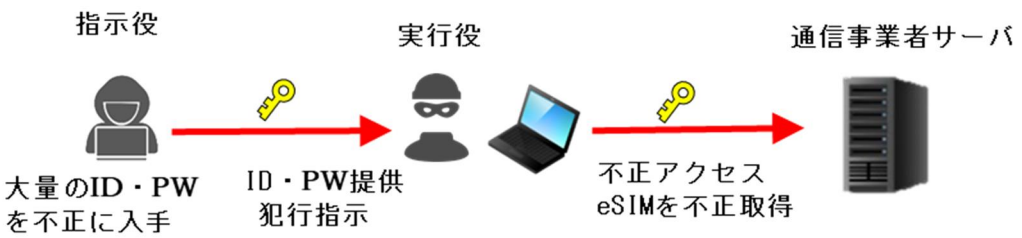
この事件では、同事業者が２回線以降の追加契約をする場合に、ID・パスワードのみの簡易な本人確認を実施していたことが悪用された。なお、生成 AI を悪用した事実も判明している。

また、当該手口を模倣し、不正に取得した eSIM を販売して利益を得ようと考え、無職の少年（16 歳）と高校生の少年（16 歳）が、模倣した手口により eSIM を不正に取得したことを受け、令和７年３月、同少年ら２人を不正アクセス禁止法違反及び電子計算機使用詐欺罪で逮捕した。（警視庁・神奈川）

このように、本年に入り、複数の少年グループにより敢行されたサイバー事案の検挙が散見されるが、例えば、令和７年上半期に不正アクセス禁止法違反で検挙された 119 人の被疑者のうち、49 人（約 41 パーセント）が 14 歳から 19 歳であるなど、サイバー事案を敢行する者の低年齢化が顕著となっている。

このような事案を踏まえ、「国民を詐欺から守るための総合対策 2.0」（P96 参照）において、契約時に本人確認が義務付けられていないデータ通信専用 SIM について、悪用実態を踏まえ、電気通信事業者に対して契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討することとしている。

【eSIM 不正取得事件の検挙の概要】



【CASE：生成 AI を悪用したフィッシングサイト公開事件被疑者の検挙】

職業不詳の男（29 歳）らは、令和６年６月、生成 AI を一部悪用するなどして構築した大手 EC サイトのフィッシングサイトを公開した。令和７年６月、同男らを不正アクセス禁止法違反で逮捕した。（大阪）

(2) 捜査支援

サイバー事案やサイバー犯罪のうち、捜査に当たり高度な専門的知識及び技術を要さないものについては、サイバー部門以外が事件主管となり、当該部門において主体的に捜査を行い、サイバー部門が当該部門を適切に支援している。

【CASE：顧客情報を不正に持ち出した不正競争防止法違反事案】

パート従業員の女（45 歳）は、自身の転職を優位に進める目的で、令和６年２月から３月までの間、当時勤務していた青森県内に所在する介護事業所から営業秘密である同事業所の顧客情報を複製したうえで領得した。令和７年１月、同女を不正競争防止法違反（営業秘密の領得）で逮捕した。

この事案では、同県警察の保安部門から支援要請を受け、サイバー部門が、同女の転職先の介護事業所に設置されたパソコン等の電子機器の解析・データ精査等を支援し、同女の犯行を裏付けた。（青森）

【CASE：オンラインカジノによる組織的な常習賭博事案】

会社役員の男（当時 42 歳）を中心とした犯罪グループは、令和６年４月から５月までの間、海外のオンラインカジノサイトの賭金入金に係る決済システムの管理、システムを利用した資金管理等の業務を継続的に行うなどして、不特定多数の賭客を相手方として、組織的に常習賭博を行っていた。令和７年６月、同人を含む９人を組織犯罪処罰法違反（組織的常習賭博）で逮捕した。

この事案では、神奈川県警察の組織犯罪対策部門から支援要請を受け、サイバー部門が、入金管理システムが蔵置されている国内のレンタルサーバの特定やサーバ検証・解析等を支援し、同人らの犯行を裏付けた。（神奈川）

また、警察庁及び全国の情報通信部に設置された情報技術解析課においては、都道府県警察等に対し、捜索・差押の現場でコンピュータ等を適切に差し押さえるための技術的な指導や、押収したスマートフォン等から証拠となる情報を取り出すための解析の実施についての技術支援を行っている。

さらに、警察庁情報技術解析課に設置された高度情報技術解析センターでは、高度で専門的な知識及び技術を有する職員を配置するとともに、高性能な解析

用資機材を整備し、破損した電磁的記録媒体からの情報の抽出・可視化、不正プログラムの解析等を行っている。

【CASE：焼損したスマートフォンからのデータ抽出】

令和６年 12 月、高度情報技術解析センターは、広島県における死者を伴う火災現場にて発見され焼損により通常の解析手法を用いても解析が行えなかったスマートフォンについて、回路基板に搭載されたメモリチップを取り外して極めて高度かつ卓越した技術によるデータの抽出に成功し、事案の全容解明に貢献した。

加えて、警察では、様々な犯罪に悪用される暗号資産の移転状況を追跡するとともに、サイバー特別捜査部において、追跡結果を横断的・俯瞰的に分析し、その結果を都道府県警察と共有している。こうした取組により、例えば、我が国で発生した SNS 型投資・ロマンス詐欺事案について、関係都道府県警察の捜査情報を横断的に分析し、暗号資産追跡を実施した結果、複数の事案の被害金がナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止め、同情報をナイジェリア警察に提供したところ、同警察において同国内の被疑者が検挙された事例など、従来の捜査では必ずしも明らかにならなかった複数事案同士の関連性や、背景にある組織性が浮き彫りになっているところである。

(3) 国際連携

サイバー事案の多くは国境を越えて敢行されるため、そうした事案への対処には国際連携が重要であるところ、警察においては、サイバー空間における脅威に関する情報の共有、国際捜査共助に関する連携強化、情報技術解析に関する知識・経験等の共有等のため、多国間における情報交換や協力関係の確立等に積極的に取り組んでいる。例えば、警察庁サイバー警察局では、関係省庁と、令和７年６月に仏国で開催されたサイバー犯罪条約の締約国等が参加する「サイバー犯罪条約委員会会合」に参加し、各国におけるサイバー犯罪対策への取組みについて議論や情報共有を行うなど、国際的な連携の更なる強化を推進するとともに、EUROPOL にサイバー事案対策専従の連絡担当官を置いており、同機関での継続的な情報共有・分析、国際機関が主催する捜査会議への積極的な参画等に取り組んでおり、その結果、サイバー特別捜査部をはじめとする日本警察は、国際共同捜査へ参画している。これらの国際共同捜査では、被疑者の検挙、犯罪インフラの停止、暗号資産の押収等によって、ランサムウェアグ

ループの活動を停止又は縮小させるなどの成果を得ている。

また、ICPO 加盟国の法執行機関に加えて、国外の民間企業や学術機関が参加する ICPO デジタル・フォレンジック専門家会合に参加し、情報技術解析に関する知識・経験等の共有を図っているほか、情報セキュリティ事案に対処する組織の国際的な枠組みである FIRST（Forum of Incident Response and Security Teams）に加盟し、組織間の情報共有を通じ、適切な事案対処に資する技術情報の収集を行っている。

【図表 21：サイバー犯罪条約委員会会合の様子】

コラム：ランサムウェアグループ「Phobos/8Base」に対する国際共同捜査

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「Phobos（フォボス）」やその関連組織「8Base（エイトベース）」について、サイバー特別捜査部と関係警察は、EUROPOL や FBI 等との国際共同捜査を推進している。

令和６年 11 月、米国は、「Phobos」グループの運営者とみられるロシア人の男（42）を起訴したことを発表したほか、令和７年２月、米国及びスイスは、「Phobos」の関連組織である「８Base」グループ運営者等とみられる男ら４名を検挙したことを発表した。

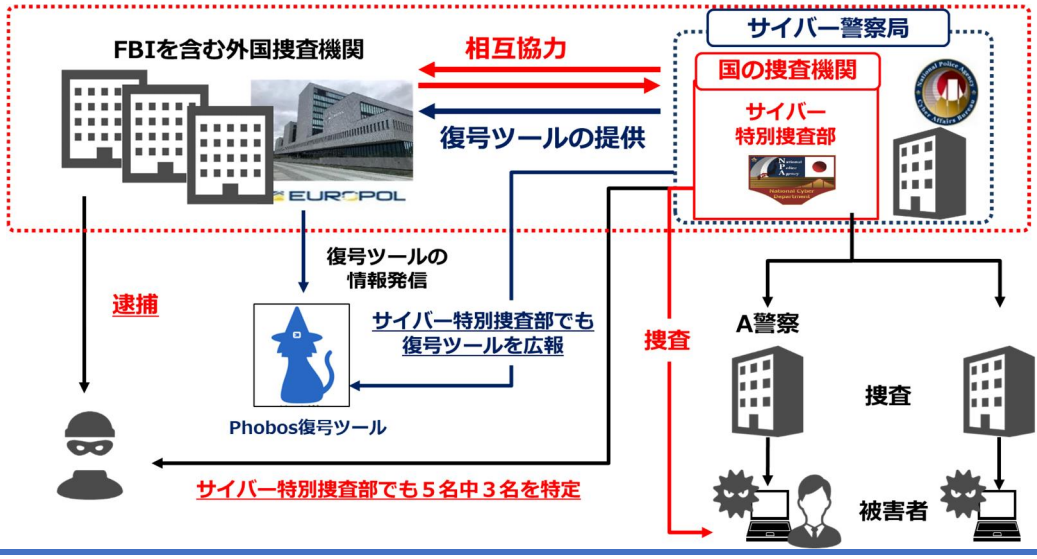
これらの事案において、サイバー特別捜査部は、独自の手法により同運営者等の特定に成功し、その結果や当該手法について、米国やスイスをはじめとする関係国の捜査機関に提供した。本共同捜査を通じて検挙した上記被疑者５名のうち、３名がサイバー特別捜査部の捜査により特定されたものである。

また、サイバー特別捜査部は FBI の協力を得つつ、同年７月、ランサムウェア Phobos/8Base により暗号化されたデータを復号するツールを開発した。

同ツールについては、警察庁ウェブサイトにおいて公開し、国内だけでなく、世界中の被害企業等の被害回復が可能となるよう、その内容を広く周知している。

なお、日本国内において、実際に同ツールを使用し、少なくとも 14 の被害企業が約 87 万件の被害データの復号に成功しており、被害回復した企業からは、「調査会社に依頼しても復号できる保証はなく、費用も掛かるので大変助かった」「実際に復号することができて感謝している」などという声が届いている。

【ランサムウェアグループ「Phobos」に対する国際共同捜査の概要】



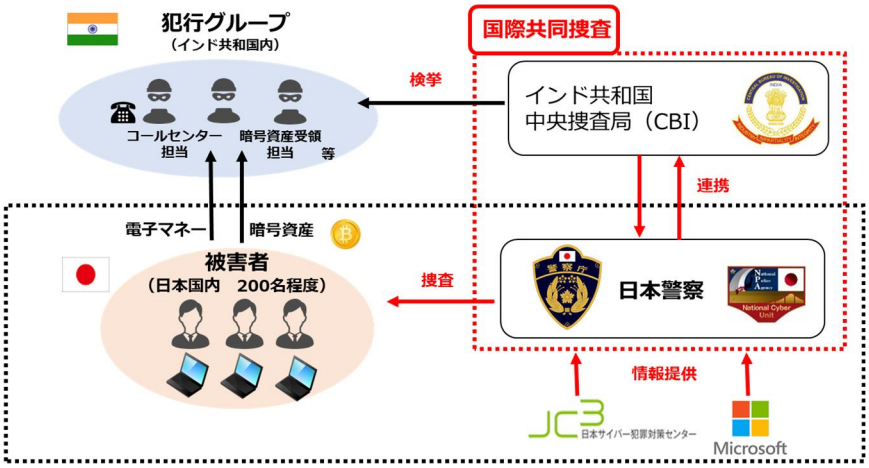
コラム：サポート詐欺の国際共同捜査

日本警察は、インド共和国・中央捜査局（CBI）とともに日本人を標的としたサポート詐欺事件の国際共同捜査を行ってきたところ、令和７年５月、CBI がインド共和国内に所在するインド人被疑者６人を逮捕した。

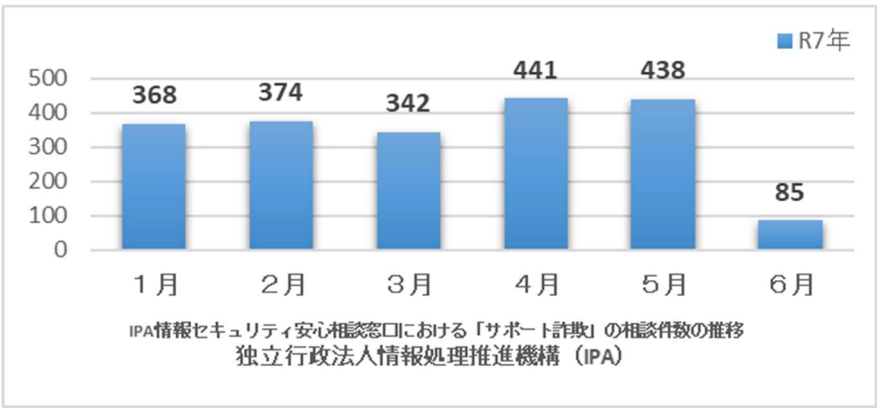
本件は、一般財団法人日本サイバー犯罪対策センター（JC3）と Microsoft 社が行った分析結果を端緒とし、サイバー特別捜査部が暗号資産の追跡により、被害金である暗号資産を受け取ったインド人被疑者を特定したほか、警視庁をはじめとする都道府県警察が把握した捜査情報等を CBI に提供するなどの緊密な連携を行ったことにより、インド国内における被疑者の検挙につながったものである。

なお、本件検挙後の令和７年６月中に IPA（独立行政法人情報処理推進機構）に寄せられた「ウイルス検出の偽警告」に関する相談の件数は 85 件（前年比－139 件）であり、438 件だった同年前月と比べても大幅に減少した。

【インド共和国との国際共同捜査の概要】



【図表 22：「ウイルス検出の偽警告」に関する相談件数】



２　被害の未然防止・拡大防止に向けた取組

サイバー空間の安全・安心を確保するため、警察では、サイバー事案の検挙に向けた取組のみならず、攻撃者・犯行手口等の実態解明、被害の未然防止・拡大防止対策等を推進している。また、政府においては、令和６年 11 月に取りまとめられた有識者会議の提言も踏まえ、令和７年２月、能動的サイバー防御を導入するためのサイバー対処能力強化法案及び同整備法案を第 217 回国会に提出し、令和７年５月、第 217 回国会において、同提言の内容を踏まえたサイバー対処能力強化法[6]及び同整備法[7]が成立した。警察においても同法に基づく、対応を推進している。

(1)　情報発信

警察では、捜査や分析を通じて得られた情報等に基づき、新たな被害を生み出さないために犯行手口の周知等を通じた注意喚起や、新たな犯罪を行わせないための警告等の広報・啓発に取り組んでいる。

①　国際連携を通じた情報発信

国家を背景とするサイバー攻撃等、高度な技術を悪用したサイバー攻撃への対策においては、攻撃者の検挙に向けた捜査を推進するのみならず、サイバー攻撃を受けたコンピュータ等を解析し、その結果や捜査の過程で得た情報等を総合的に分析するなどして、攻撃者及び手口に関する実態解明を進めており、未然防止対策等に関する注意喚起を実施している。例えば、令和７年１月、警察庁は、サイバー特別捜査部及び警視庁ほか道府県警察による捜査の結果を踏まえ、NISC とともに、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から日本国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信や、ソフトウェアのぜい弱性を悪用した標的ネットワーク内への侵入といった方法により、情報窃取を目的としたサイバー攻撃を行っていることを確認し、これらサイバー攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動であると評価した上で、同グループによるサイバー攻撃の手口や未然防止対策等に関する注意喚起を実施した。

このほか、我が国としてサイバー攻撃の攻撃者を公表し、非難することで

---

[6] 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号）

[7] 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第 43 号）

サイバー攻撃を抑止するパブリック・アトリビューションを実施している。例えば、同年８月には中国を背景とするサイバー攻撃グループ「Salt Typhoon」に関するパブリック・アトリビューションを実施した。

コラム：中国を背景とする Salt Typhoon に関するパブリック・アトリビューション

令和７年８月、警察庁及び国家サイバー統括室（NCO）は、米国、オーストラリア、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、及びスペインの関係機関とともに、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリー「Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System」の共同署名に加わり、パブリック・アトリビューションとして、本件アドバイザリーを公表した。

②　関係機関との連携を通じた情報発信

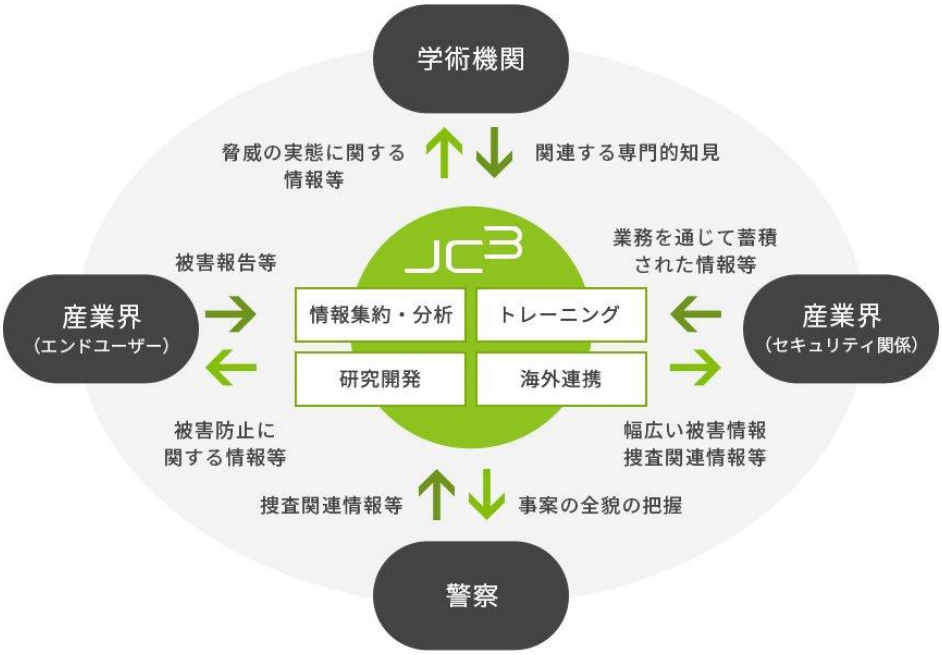
警察では、様々な関係機関と連携した情報発信を行っており、特に一般財団法人日本サイバー犯罪対策センター（JC3）との連携を推進している。

JC3 は、平成 25 年 12 月に閣議決定された「「世界一安全な日本」創造戦略」等において、米国で産学官連携の枠組みとして成果を上げている非営利組織である NCFTA[8] に類似の新たな組織を構築する必要性が指摘されたことを受け、日本版 NCFTA として産学官の情報や知見を集約・分析し、その結果等を還元することにより、国民が安全かつ安心してインターネットを利用できる環境の構築に貢献することを目的として設立され、平成 26 年 11 月に業務を開始した。

警察では、JC3 に対しサイバー犯罪の被害実態、犯行手口等を共有し、セキュリティベンダー、金融機関等の会員企業の対策に反映し、JC3 からは会員企業における被害状況や対策の実施状況の共有を受け、警察における捜査や被害防止活動に活用している。

[8] National Cyber-Forensics & Training Alliance の略。

【図表 23：JC3 の概要】



また、各都道府県警察においては、金融機関、暗号資産交換事業者、医療機関、商工会議所、損害保険会社等と協定を締結し、平時からの情報共有等の連携強化に取り組んでいる。

さらに、警察庁においては、ランサムウェア等のサイバー事案の未然防止及び発生時における被害拡大防止のため、VPN 機器等のぜい弱性対策や認証情報の適切な管理、バックアップやログの適切な取得、サイバー攻撃を想定した業務継続計画（BCP）の策定、被害発生時における速やかな警察への通報・相談等について、特に被害が増加傾向にある中小企業を主な対象としつつ、幅広く周知・啓発に取り組んでいる。そのほか、関係省庁と連携した業界団体及び事業者等への周知、サイバーセキュリティ月間における NISC と連携した中小企業向けセミナー、内閣府政府広報室や損害保険会社との連携による広報啓発記事・動画の制作等を行った。

なお、暗号化されたデータを復号するための対価と称して、ランサムウェア攻撃グループから要求される金銭等を支払うことに関し、警察としては、「犯罪グループ等の活動資金となることが懸念される」「暗号化されたデータの復号が保証されるわけではない」旨を被害者に対して説明しているほか、要求された金銭等の支払いの有無も含む、ランサムウェア被害に係る情報の提供をはじめとした捜査への協力を求めている。

コラム： サイバー攻撃を想定した業務継続計画（BCP）の推進

サイバー攻撃の被害がいつどこでも起こり得る情勢を受け、警察は、企業等におけるサイバー攻撃を想定した体制の構築を推進している。例えばランサムウェア被害により業務停止に陥る例は後を絶たないが、サイバー攻撃を想定した業務継続計画（BCP）を整備済の組織は少ない。ランサムウェア被害のあった企業・団体にアンケート調査を行った結果、BCP を整備済の組織の割合は６％であった。ランサムウェアによるデータ暗号化は地震などの物理的災害とは被害の状況が異なり、調査・復旧作業や広報のあり方も、そのような災害時とは異なる対応が求められるため、サイバー攻撃を想定した BCP を事前に準備しておくことが望ましい。他にも、暗号化対策となるオフラインバックアップ、侵害範囲特定に不可欠なログ取得、訓練、警察との連携等、サイバー攻撃のリスクを考慮した管理体制の構築が被害の抑制に有効である。

令和７年６月には内閣府政府広報室とともにランサムウェア対策を紹介する広報啓発動画を制作するなど、幅広く注意喚起に取り組んでいる。

○政府広報オンライン「中小企業で被害多数　ランサムウェア」
https://www.gov-online.go.jp/useful/202506/video-298784.html

加えて、各都道府県警察や重要インフラ事業者等で構成される「サイバーテロ対策協議会」を全ての都道府県に設置し、サイバー攻撃事案の知見を踏まえた共同対処訓練等を実施しているほか、警察及び全国約 8,700 の事業者等からな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、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、事業者等に対し注意喚起等を実施している。

令和７年１月には、大阪・関西万博開催に備え、大阪府警察及び大阪・関西万博関係事業者と共同で、実際のサイバー攻撃への対処を想定したインシデント対応訓練を実施した（警察庁主催）。訓練では、架空の企業のセキュリティ対応チームの一員として、サイバー攻撃に対する実機を使用した実践訓練に加え、顧客対応や警察への被害報告等が行われた。

このほか、警察庁において大阪・関西万博関係事業者をはじめとした全国の重要インフラ事業者等からの依頼に基づきセキュリティ診断を実施し、診断結果に基づく注意喚起を実施している。

③　サイバー防犯ボランティアとの連携を通じた情報発信

サイバー防犯ボランティアは、全国で 301 団体、7,298 人（令和 6 年 12 月末現在）が、「被害防止のための教育活動」、「広報啓発活動」、「サイバー空間の浄化活動（サイバーパトロール）」を柱とする活動を行っており、警察ではその活動の拡大・活性化に向けた支援を行っている。

警察庁においては、活動状況等の視察や、サイバー事案に関する広報啓発動画のコンテストを開催し、優秀作品を作成した団体への表彰を行うなどの支援を行っている。

各都道府県警察においても、サイバー防犯ボランティアによる、学校における防犯教育や大規模イベント時の広報啓発で活用するクイズの制作等に対して防犯上のアドバイスを行うなどの支援に取り組んでいる。

コラム：　福山大学サイバー防犯ボランティアの取組

サイバー防犯ボランティア「福山大学サイバー防犯ボランティア CyPat FU」は、令和 7 年 5 月に広島県福山市内で開催された「福山ばら祭」において、

○　ブースを出展し、全年齢層を対象としたサイバー犯罪被害防止クイズや、ボランティア活動を紹介するパネル等の展示

○　会場全体にチェックポイントを設置し、子供を対象としたサイバー防犯に関するクイズラリーを実施

するなど、子供やその保護者らの防犯意識向上に向け、工夫を凝らした広報啓発活動を実施している。

同団体には令和 7 年度も新たに 26 名の学生が参加するなど、ボランティアの持続性を意識した活動が展開されていることに加え、同団体の卒業生が広島県警察に採用されるなど、各種活動の輪を通じて、警察活動にも寄与している。

【福山大学サイバー防犯ボランティアの様子】

なお、同団体は、これまでの防犯活動における功績により、令和 6 年 10 月、「安全安心なまちづくり関係功労者表彰」として、内閣総理大臣から表彰を受けた。

(2)　犯罪インフラへの対処

サイバー事案による被害を防止するためには、犯罪インフラへの対処が必要であるところ、この対処に当たっては、警察による取組のみならず、民間事業者、学 術機関、関係省庁等も含めた社会全体における対策が重要である。特に、新たなサービスや技術が、その欠陥を突かれるなどして悪用される例が認められることから、その悪用防止に向けては、産学官の連携による効果的な対策を実施している。

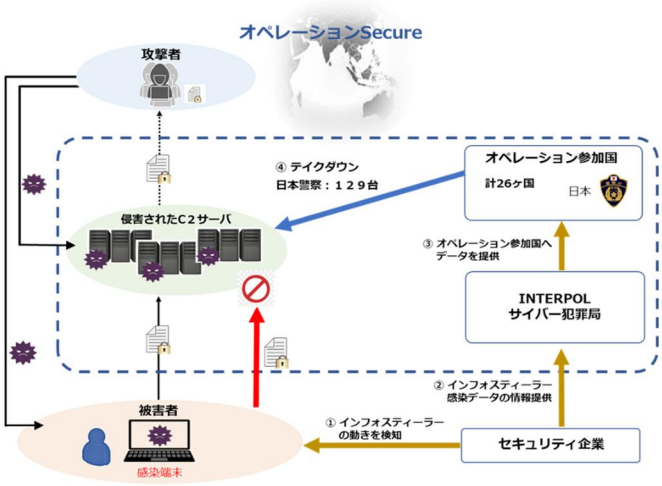
①　高度な技術を悪用したサイバー攻撃に関するインフラへの対処

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、当該C2サーバの不正な機能を停止するよう、サーバを管理する事業者等に依頼するなどして、C2サーバの対策を継続的に実施している。

日本警察は、INTERPOLが主導しているアジア・南太平洋地域における情 報窃取型マルウェアの対策を行うための国際共同捜査「Secure」に参画し、26か国の捜査機関が協力して捜査を行うなどして、関係C2サーバのテイクダウン等を行うことで犯行抑止、被害防止を実施した。(以下コラム参照。)

コラム：情報窃取型マルウェアに対するINTERPOL主導のテイクダウン

令和7年6月、INTERPOLは、アジア・南太平洋地域における情報窃取型マルウェアのInfostealer（インフォスティーラー）対策を行うための国際共同捜査「Secure（セキュア）」において、日本警察を含む26か国の捜査機関が民間事業者とも連携した捜査により、関係サーバの管理者に働きかけるなどしてサーバを停止等させる対策(テイクダウン)を行うことで犯行抑止、被害防止を実施した旨を発表した。日本警察は、INTERPOL から提供を受けた情報に基づき、サイバー特別捜査部及び18都府県警察が緊密に連携し、侵害されたサーバを管理する事業者に順次働きかけを行った結果、当該事業者によって129台のサーバがテイクダウンされた。同サーバは、企業等が通常使用するサーバが何らかの理由で侵害され、管理する企業等が気付かないままに情報窃取行為に悪用されたものであった。



【INTERPOL主導の情報窃取型マルウェアのテイクダウンの概要】

②　インターネット空間を悪用した犯罪に関するインフラへの対処

○　フィッシングサイト対策

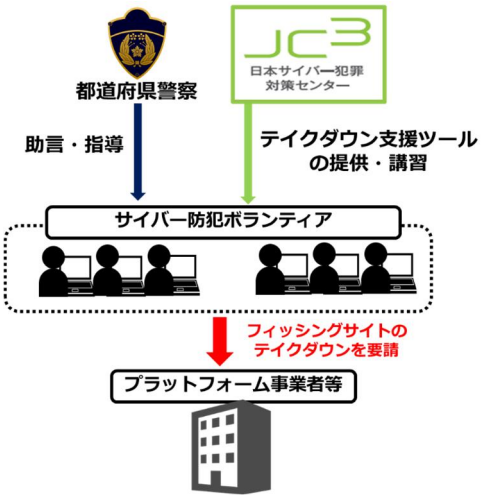
警察庁においては、都道府県警察や一般財団法人日本サイバー犯罪対策センター（JC3）等が相談等を通じて把握した海外の偽サイト等に係るURL 情報を集約し、ウイルス対策ソフト事業者等に提供しており、当該事業者によってウイルス対策ソフトの機能による警告表示等、当該サイトの閲覧を防止する対策がとられている。

また、１つの IP アドレス上に、数百のフィッシングサイトが構築されているといったフィッシングサイトの特性を踏まえた先制的な対策として、警察庁において、同一の IP アドレスに紐づくドメイン情報を独自に収集し、未把握のフィッシングサイトを発見・提供している。

さらに、フィッシングの手口が巧妙化し、被害が急増している情勢に鑑み、利用者保護のため、フィッシングサイトにアクセスさせないための対策として、「なりすましメールを防ぐ技術（DMARC[9]等）への対応促進」を始め、「フィッシングサイトの閉鎖促進」や「パスワードに代わって生体認証等により簡単かつ安全にログインできる認証方法（パスキー）の普及促進」について、所管省庁を通じ、事業者に対する対策の要請を実施した。

フィッシングサイト対策として、JC3 では、専門的な知識を持たない人であってもプラットフォーム事業者等に対してサイトのテイクダウン依頼を行うことができるツールを開発し、サイバー防犯ボランティア等に提供するとともに、警察庁後援のもと、サイバー防犯ボランティア向けの「フィッシングサイト撲滅チャレンジカップ」を実施している。

【図表 24：サイバー防犯ボランティアへの支援】



○　インターネットバンキングに係る不正送金対策

警察庁は、令和６年秋からボイスフィッシングによる法人口座の不正送

[9] Domain-based Message Authentication Reporting, and Conformance

金被害が急増する深刻な事態を受け、金融庁、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）と連名で、広報啓発資料「サイバー警察局便り」を作成した上で、警察庁ウェブサイト等にて公開し、その手口の詳細や対策に関する注意喚起を実施した。

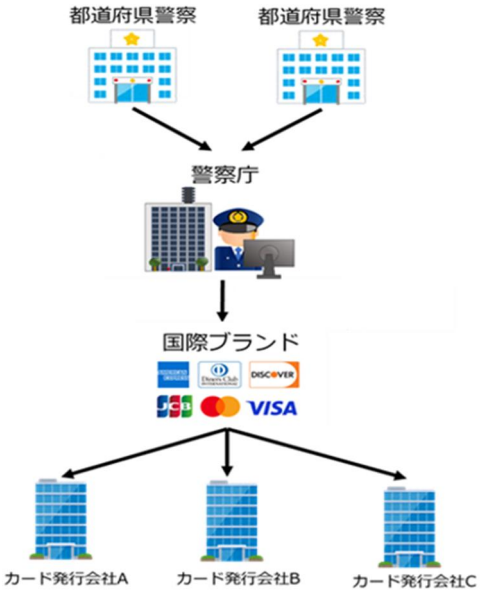
○　証券口座不正取引対策

特に証券口座不正取引の被害情勢を踏まえ、警察庁は、令和７年７月、金融庁と連名で、日本証券業協会を含む金融関係協会に対して、被害を踏まえた具体的なフィッシングの手口やその対策を示した上で、顧客口座・アカウントの不正アクセス・不正取引対策の強化について要請した。(P95参照)

○　クレジットカード不正利用対策

各都道府県警察で把握した、悪用されたクレジットカード番号を警察庁で速やかに集約し、カード発行会社を含む決済システム全体を統括する国際ブランド各社に対し、一括して提供しており、クレジットカード発行会社における不正利用対策に活用されているところ、令和７年上半期は、約 85 万件のクレジットカード番号を国際ブランド各社に提供した。

【図表 25：国際ブランドに対する不正クレジットカード番号情報提供】



③　違法・有害情報に関するインフラへの対処

警察では、サイバーパトロール等による違法・有害情報の把握に努め、これを端緒とした取締り及びサイト管理者等への削除依頼を実施している。

○　IHC 及び CPC における取組

警察庁では、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インターネット・ホットラインセンター（IHC）を事業委託するとともに、違法情

報、重要犯罪密接関連情報[10]及び自殺誘引等情報を収集し、IHC に通報するサイバーパトロールセンター（CPC）を事業委託している。

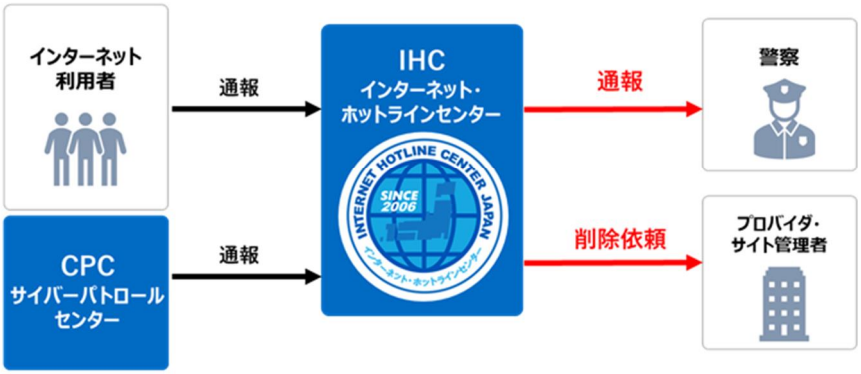
令和 7 年上半期の IHC の受理件数のうち、運用ガイドラインに基づいて 282,787 件を分析した結果、違法情報を 44,973 件、重要犯罪密接関連情報を 1,341 件、自殺誘引等情報を 2,736 件と判断した。

また、厚生労働省は、募集者の氏名又は名称、住所、連絡先、業務内容、就業場所及び賃金について記載がない求人情報が職業安定法に違反することを明確化したほか、その旨が、総務省において検討中の違法情報ガイドライン（案）に盛り込まれたことなどを踏まえ、犯罪実行者募集情報の実効的な削除のため、令和 7 年 2 月、IHC の運用ガイドラインを改定し、重要犯罪密接関連情報の類型であった「犯罪実行者の募集」を違法情報（職業安定法違反等）に位置付けるとともに、同年 3 月、体制を増強した。

本年 6 月 18 日に、ギャンブル等依存症対策基本法の一部を改正する法律が成立し、インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為等が禁止されたことから、本年 9 月の法施行に合わせて IHC の運用ガイドラインを改定し、これら情報を新たに違法情報として取扱範囲に追加し、社会問題となっているこれら情報の流通防止に向けた取組を強化することとしている。

そのほか、CPC では、違法情報等を自動収集してその該当性を判定する AI 検索システムを導入し、サイバーパトロールの高度化を図っている。

【図表 26：IHC・CPC の概要】



[10] 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

○　警察庁における取組

警察庁では、IHC 等の取組について周知を図るとともに、違法・有害情報の削除の実効性を確保するため、令和７年３月、国内のプロバイダ事業者等に対して、違法・有害情報に関する削除への引き続きの協力を依頼した。

また、SNS 型投資・ロマンス詐欺及び特殊詐欺の犯行に利用されたアカウントについて、その利用停止や削除等を促すためにプロバイダ事業者等に対する情報提供や削除請求を行っているところ、令和７年１月から６月までの間に 8,564 件の情報提供を実施したほか、令和７年４月から６月までの間に 814 件の削除請求を実施した。

加えて、令和６年２月、AI を活用して SNS 上の犯罪実行者の募集投稿等を効率的に抽出する仕組みを構築し、同年４月からは、返信（リプライ）機能を活用した投稿者等に対する迅速な個別警告（AI リプライ）等を実施しており、令和７年上半期中には、4,046 件の個別警告を実施している。

そのほか、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）に基づき、関係機関・団体・民間事業者等の協力を得ながら、各種施策を強力に推進している（P96 参照）。

(3)　能動的サイバー防御（ＡＣＤ）について

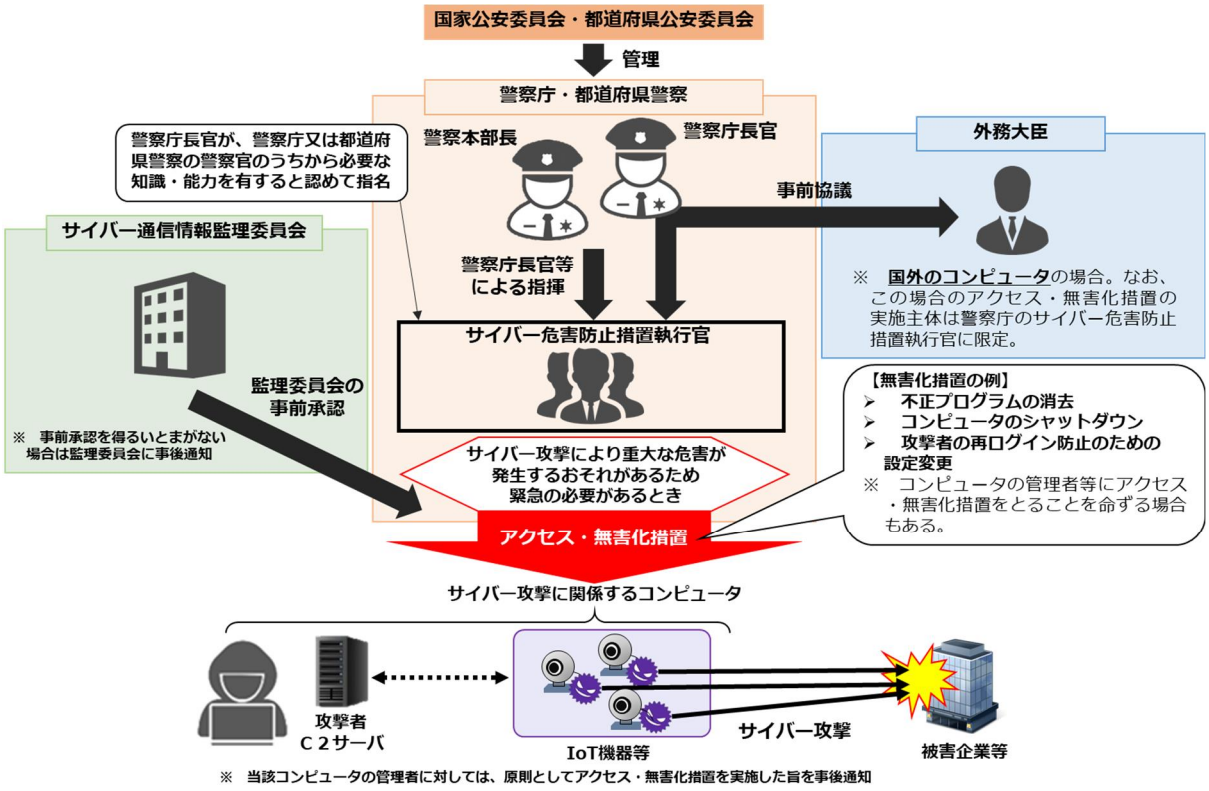
近年、サイバー攻撃による政府や企業の内部システムからの情報窃取等が大きな問題となっているほか、重要インフラ等の機能を停止させることを目的とした高度な侵入・潜伏能力を備えたサイバー攻撃に対する懸念が急速に高まっている。特に、重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家を背景とした形でも日常的に行われるなど、安全保障上の大きな懸念となっている。

こうした中、令和４年 12 月に閣議決定された国家安全保障戦略において、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことを目標に掲げ、重大なサイバー攻撃による被害の未然防止・拡大防止を図るために能動的サイバー防御を導入することとされた。

同戦略に基づき、政府は、令和６年６月、サイバー安全保障分野における新たな取組の実現のために必要となる法制度の整備等について検討を行うため、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」を開催し、同年 11 月、「サイバー安全保障分野での対応能力の向上に向けた提言」が取りまとめられた。

令和７年５月、第 217 回国会において、同提言の内容を踏まえたサイバー対処能力強化法（以下「強化法」という。）及び同整備法（以下「整備法」という。）が成立した。強化法及び整備法は、「官民連携の強化」、「通信情報の利用」及び「攻撃者のサーバ等へのアクセス・無害化措置」の３つを取組の柱としている。このうち警察関係では、整備法により、警察官職務執行法の一部が改正され、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新たに設けられた。同規定は、令和８年 11 月までに施行することとされているところ、警察では、その施行に向け、内閣官房国家サイバー統括室や防衛省・自衛隊、外務省等との連携の強化を図るとともに、サイバー人材の確保・育成や資機材の整備、外国治安機関との関係構築等を通じて、サイバー空間における対処能力の更なる強化を図っている。

【図表 27：改正警察官職務執行法の概要】



３　基盤整備

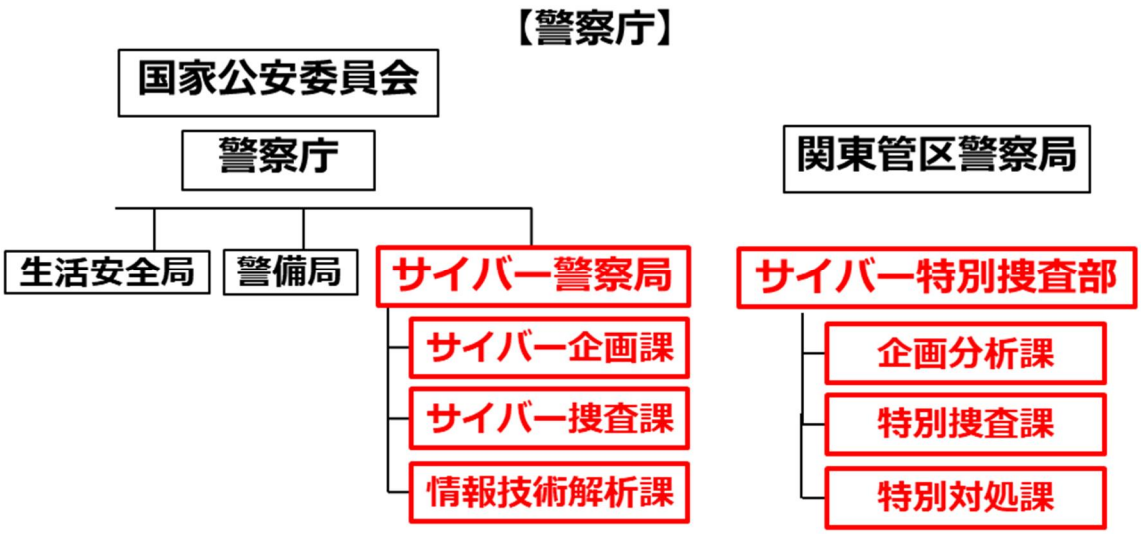
(1)　体制の拡充

令和４年４月、警察法を改正し、重大サイバー事案の対処を担う国の捜査機関として、関東管区警察局にサイバー特別捜査隊を設置した。

同隊は、従来、外国捜査機関等と都道府県警察との間で調整機能を果たすに過ぎなかった警察庁が、全国を管轄して直接捜査を実施し、国の捜査機関として国際共同捜査を通じて被疑者を検挙することを目的として設置された組織であり、全国警察からサイバー分野の知識や経験を豊富に持つ有為な人材を登用し、高度な資機材を整備した。高い捜査力・技術力を備えた結果、それまで対応が困難であった事案の被疑者の特定・犯罪グループの全体像の解明が可能となるとともに、外国捜査機関等と情報交換を継続的かつ緊密に行うことで、強固な信頼関係の構築を実現している。

令和６年４月、サイバー特別捜査隊が発展的に改組され、新たにサイバー特別捜査部が設置されるとともに、その下に企画分析課と特別捜査課が置かれ、さらに令和７年４月には、サイバー特別捜査部に特別対処課が設置された。これらにより、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析、事案発生の予防及び被害の拡大防止等を行う体制が強化された。これは、都道府県警察が捜査により得た膨大な情報をサイバー特別捜査部に集約し、同部が、外国捜査機関等との情報交換や独自の捜査により得た情報と併せて高度な分析・解析を行うことにより、犯罪グループの中枢被疑者の特定や実態解明等を一層推進するためのものである。

【図表 28：サイバー警察局及びサイバー特別捜査部の概要】

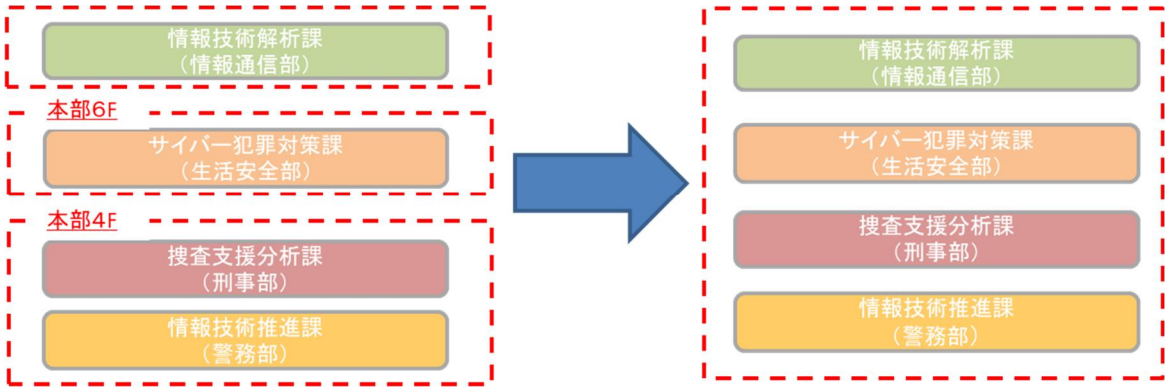


また、都道府県警察においても、静岡県警察におけるサイバー対策本部の設置といった高度な専門的知識及び技術を要するサイバー事案に対処するための体制の拡充や、サイバー部門における捜査部門と支援部門の一体的な運用、サイバー部門所属のフロアの一体化等の取組を推進することにより、サイバー空間における対処能力の強化を図っている。

コラム：山口県警察におけるサイバー部門所属のフロアー体化

山口県警察においては、令和７年４月から、警務部情報技術推進課、生活安全部サイバー犯罪対策課、刑事部捜査支援分析課、中国四国管区警察局山口県情報通信部情報技術解析課のサイバー支援部門４所属を同一フロアに配置するとともに、共同解析室の設置、支援要請窓口のワンストップ化により、支援・解析部門の一体的運用を図っている。

【山口県警察におけるフロアー体化】



(2)　人材確保・育成

○　人材確保

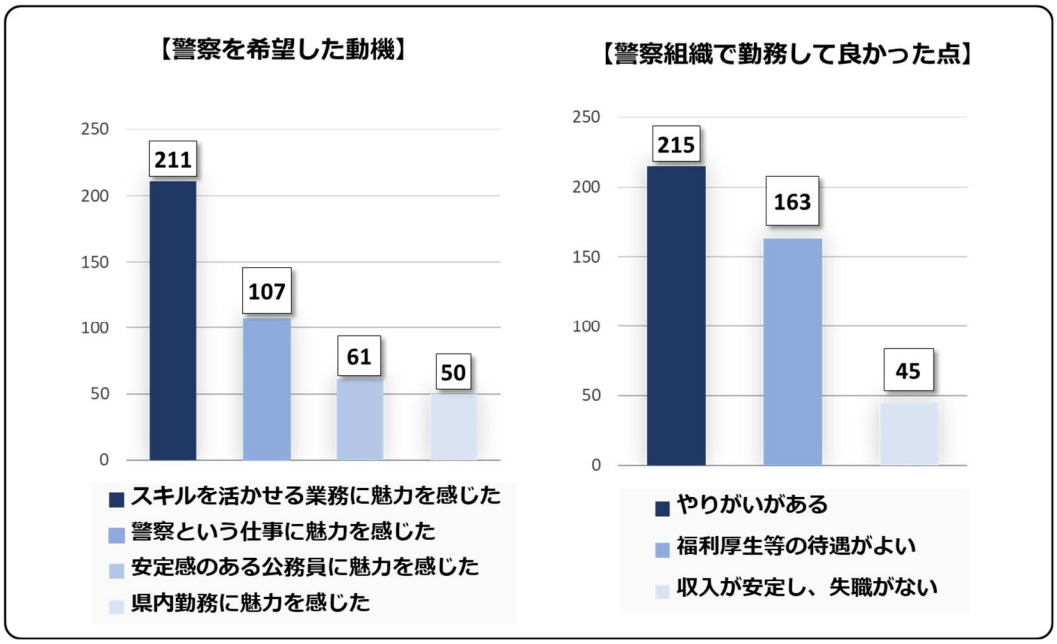
警察では、サイバー空間における脅威への対処のための人的基盤を強化するため、都道府県警察・情報通信部門におけるサイバー人材確保・育成方針に基づき、サイバー人材の確保・育成及びそのキャリアパスの管理並びに全職員の対処能力の向上に係る取組を部門横断的かつ体系的に推進している。

都道府県警察では、民間企業での経験や情報通信技術に関する高度な資格の保有を条件として中途採用・特別採用された警察官等約 480 人が、サイバー事案への対処に係る高度な知見をいかして、サイバー特別捜査官としてサイバー犯罪捜査等の第一線で活躍している。

コラム：中途採用・特別採用制度により採用された職員へのアンケート結果

中途採用・特別採用制度により採用された都道府県警察職員に対するアンケート調査を実施したところ「警察でしかできない事件捜査等仕事にやりがいがある」や「知識・技能を活かせる場であり、現在の業務に満足している」など、多くの採用者が警察での仕事にやりがいを感じていることから、警察における具体的な勤務内容を発信するとともに、同人材が活躍できるキャリアパスの構築を推進し、人材確保に取り組んでいる。

【警察におけるサイバー人材アンケート結果】



コラム：中途採用・官民人事交流制度により採用された幹部警察官

○　サイバー特別捜査官として採用された幹部警察官

丸山篤警視正は、平成 12 年４月にサイバー特別捜査官として千葉県警察に中途採用され、主にサイバー部門で活躍し、千葉県警察本部のサイバー犯罪対策課長、警察署長を経て、令和７年３月、関東管区警察局サイバー特別捜査部特別捜査課長として着任した。

現在、高度な技術的手法が用いられた犯罪等の重大サイバー事案の捜査指揮に従事している。

事件捜査を指揮する
丸山　篤　警視正

○　官民人事交流制度により採用された幹部警察官

濵石佳孝警視正は、官民人事交流制度により平成 31 年４月から３年間、当時の警察庁生活安全局情報技術犯罪対策課に出向していたサイバーセキュリティ関連企業出身者である。

令和５年 10 月、同制度により、改めて警察庁に採用され、民間の最新の知見を活かし、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部においてサイバー事案に関する情報集約・分析の一層の高度化に取り組んでいる。

分析業務に従事する
濵石　佳孝　警視正

警察庁では、情報通信に関する専門的な技術を有する者を技術系職員として採用し、実践的な研修等を通じて育成しており、約 800 人の職員が情報技術解析等の第一線で活躍している。

また、高度なサイバー人材の確保の取組として、官民人事交流制度を拡張した民間人材の登用を進めており、サイバー警察局では、同局設置の令和４年以降、官民人事交流制度により、民間企業から高度な知識・技術を有する８名を採用しているほか、令和８年度からは、サイバー事案の対処等に係る事務に専ら従事する技術系職員の採用を予定している（サイバー採用）。サイバー採用に当たっては、情報処理に関する応用的知識・技能を有する者を対象に、警察庁独自の採用試験（サイバー事案対処に関する能力を判定する筆記試験等）を実施している。なお、サイバー採用により採用された技術系職員は、その専門的知識を生かすべく、主として警察庁サイバー警察局及び関東

管区警察局サイバー特別捜査部において勤務することとなる。

【図表 29：警察におけるサイバー人材の人数】

○　人材育成

令和７年４月、警察大学校に新設されたサイバー警察教養部では、都道府県警察のサイバー部門においてサイバー事案の対処に当たる捜査員等を対象とした高度な実践的研修や都道府県警察の各部門の捜査幹部を対象とした適正な捜査指揮に関する研修を実施している。各研修は、より実践に即した内容となっており、仮想環境下において実際の犯行手口や被害状況を再現することにより、最新の手口により行われるサイバー事案に対する実践的な捜査演習や、大規模なサイバー攻撃の被害事案を想定した訓練等を実施している。

さらに、高度な解析技術を持つ職員の育成を行うため、最新の技術を有する民間企業や研究機関との技術協力を推進している。

また、都道府県警察の捜査員等を対象に、サイバー空間における脅威への対処に関する知識・技能を競うサイバーコンテストを開催している。同コンテストでは、実際の事案を想定したシナリオを使用し、捜査員等の知識・技能の向上を図るとともに、全国の優秀な人材の発掘に取り組んでいる。

このほか、サイバー空間はあらゆる犯罪に悪用され得るところ、サイバー関係の知識が、全ての捜査分野において不可欠となっている状況を踏まえ、各職員に求めるサイバー対処能力を初級、中級及び上級に区分した上で、全職員を対象としたサイバー対処能力検定を実施している。令和７年４月現在、高度な専門的知識及び技術を要するサイバー事案に的確に対処できる能力を有する上級検定の合格者は約 800 人、ネットワーク利用犯罪に的確に対処できる能力を有する中級検定の合格者は約５万 3,400 人となっている。

なお、高度な知識・技能に係る情報処理資格である情報処理安全確保支援士の登録資格取得者及び CISSP[11]の資格取得者は、令和７年４月現在、約 700 人となっている。

このように、極めて深刻な情勢が続いているサイバー空間をめぐる脅威に的確に対処するためには、サイバー人材を確保・育成する取組を部門横断的に推進する必要があるところ、警察庁では、令和８年度組織改正要求及び国家公務員増員要求において、上記取組に係る都道府県警察等の司令塔的存在である「サイバー人材育成指導室（仮称）」の新設及び同室に配置する予定の定員を要求している。

(3) 資機材の整備

警察庁では、技術支援体制の強化に向け、全国の情報技術解析部門の限られた人的・物的資源を効率的かつ最大限に活用するため、全国を結ぶネットワークを通じて、高度な解析を実施するためのソフトウェアの共有・利用や相互支援を可能とする解析基盤装置を、令和５年５月から運用しているほか、最新の資機材の整備を進めるなど、サイバー事案の対処に必要な資機材の整備・高度化を推進している。

具体的には、令和６年度当初予算におけるサイバー空間の脅威への対処に係る予算は 49 億 6,200 万円であり、そのうち捜査用資機材及び情報技術解析用資機材の整備等を含む対処能力の向上に係る予算は 37 億 4,400 万円、人的基盤の強化及び研究の推進に係る予算は６億 7,300 万円、官民連携及び国際連携の推進に係る予算は５億 4,500 万円となっている。また、令和６年度補正予算

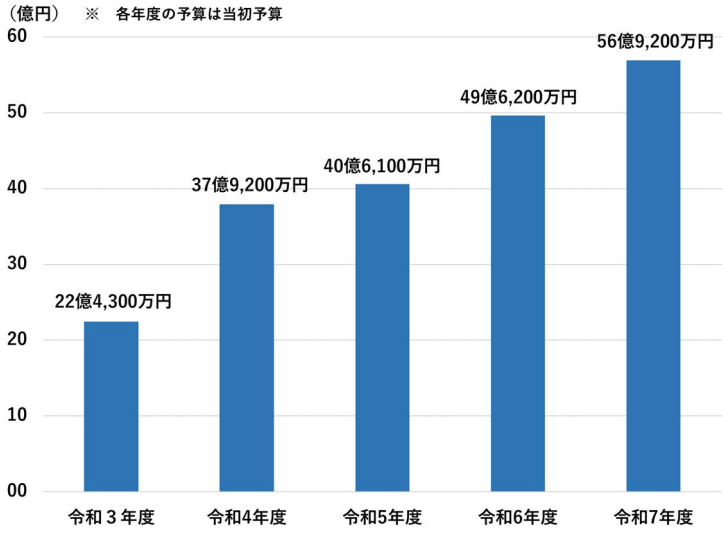
---

[11] CISSP（Certified Information Systems Security Professional）とは、ISC２（International Information Systems Security Certification Consortium）が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認定資格をいう。

におけるサイバーセキュリティ対策の強化に係る予算は 88 億 7,600 万円となっている。

令和 7 年度当初予算におけるサイバー空間の脅威への対処に係る予算は 56 億 9,200 万円であり、そのうち捜査用資機材及び情報技術解析用資機材の整備等を含む対処能力の向上に係る予算は 44 億 5,900 万円、人的基盤の強化及び研究の推進に係る予算は 6 億 7,900 万円、官民連携及び国際連携の推進に係る予算は 5 億 5,300 万円となっている。

【図表 30：警察庁におけるサイバー空間の脅威への対処に係る予算】



(4) 情報技術解析部門による研究

警察庁の情報技術解析部門においては、犯罪捜査、被害拡大の防止等を目的に各種不正プログラムの解析を実施している。また、情報セキュリティ大学院大学へ職員を派遣し、不正プログラム解析の効率化を目的とした機械学習に関して研究を行った。現在は、本研究によって開発した不正プログラムの機能名を高精度で推定する生成ＡＩ「リブラマ（RevLlama）」を実業務に活用するため、推定精度を向上させる取組を行っている。

コラム：不正プログラム（ランサムウェア）解析の一例

令和７年５月、ＳＮＳにおいて、同年３月に登場したランサムウェア「VanHelsing」のソースコードをリークしたとの投稿が確認された。当該投稿を基に警察庁の情報技術解析部門において入手したソースコードには、Windows 用暗号化ツールの開発キット等が含まれていた。ソースコードを解析するための仮想環境を構築し、ランサムウェアで使用されている暗号アルゴリズム、暗号化鍵の生成方法、暗号化ファイルの構造、Ｒａａｓの構成等を解明した。

【解明された「VanHelsing」の構成】

※：攻撃者が攻撃状況や収益を確認するためのサイト

資料編[1]

[1] 資料編中のグラフについて、特段の記載がない場合は令和７年上半期の状況を示している。

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

令和７年上半期における主なサイバー攻撃事例

● **金融機関等に対する DDoS 攻撃被害とみられるウェブサイトの閲覧障害**

令和６年 12 月下旬から令和７年１月上旬にかけ、交通機関や金融機関等において、DDoS 攻撃による被害とみられるウェブサイトの閲覧障害や各種アプリケーションへのアクセス障害が複数発生した。

● **保険大手企業に対するランサムウェア攻撃事案**

令和７年２月、保険代理店関連事業等を運営する保険大手企業は、同社のサーバがランサムウェア攻撃を受けたことを発表した。その後の調査により、データサーバの一部で保管しているファイルが暗号化されていることが判明したほか、約 510 万件を超える個人情報が漏えいしたおそれがあることなどを発表した。

● **研究開発機関に対する情報窃取目的とみられるサイバー攻撃**

令和７年３月、研究開発機関はリモートアクセス機器に対するゼロデイ攻撃による不正アクセスを受け、個人情報が漏えいした可能性があることを発表した。

● **政府要人に対する DDoS 攻撃による被害とみられるウェブサイト閲覧障害**

令和７年３月から４月にかけて、政府要人の個人ウェブサイトにおいて、DDoS 攻撃による被害とみられる閲覧障害が複数発生した。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。

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

令和７年上半期における主なサイバー攻撃事例 ②

● **大手システム事業者に対する情報窃取目的とみられるサイバー攻撃**

令和７年４月、大手システム事業者は、同社のサービスを提供するサーバ等が不正アクセスを受け、個人情報や顧客情報等が漏えいした可能性があると発表した。同月、同社は、個人情報等が漏えいしたことが確認されたほか、その原因が第三者のソフトウェアの脆弱性を悪用されたことによるものであったと発表した。

● **電力事業者に対する情報窃取目的とみられるサイバー攻撃**

令和７年４月、電力事業者は、社内のネットワークへの接続機器の一部が不正アクセスを受け、個人情報等が漏えいした可能性があると発表した。

● **国際総合物流企業に対するランサムウェア攻撃**

令和７年４月、国際総合物流企業は、同社のサーバがランサムウェア攻撃を受け、業務システムにおいて障害が発生し、業務の一部に支障が生じていることなどを発表した。この攻撃により、同社が提供する物流事業に影響が発生した。

● **政府機関等に対する DDoS 攻撃による被害とみられるウェブサイトの閲覧障害**

令和７年６月、政府機関、自治体、民間事業者等が運営する複数のウェブサイトにおいて DDoS 攻撃による被害とみられる閲覧障害が複数発生した。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。

資料編

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

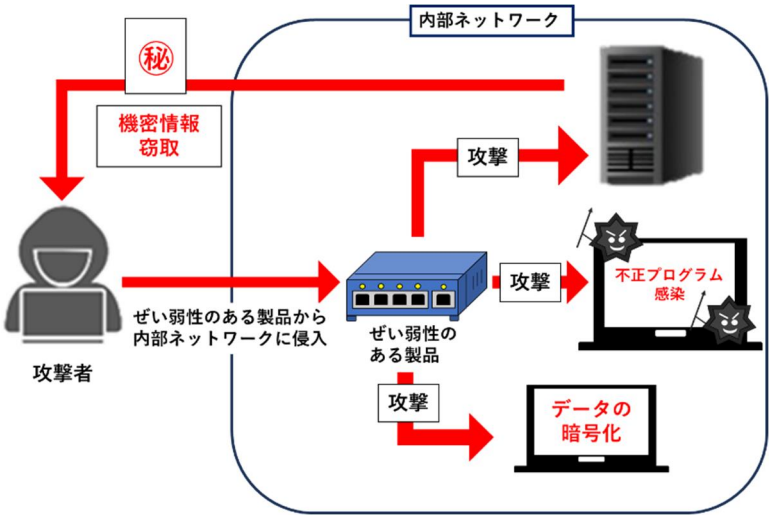
令和７年上半期に公表されたぜい弱性の危険性と対策

令和７年上半期においても前年に引き続き、VPN 製品やファイアウォール製品等のネットワーク機器に関して、悪用されるとこうした機器に侵入されるおそれがある重大なぜい弱性に係る情報が複数公表された。また、国内又は海外で、過去に発表されたものを含め、これらのぜい弱性を悪用する攻撃が発生したことも公表されている。

攻撃者は、ぜい弱性があるネットワーク機器を攻撃の足掛かりとして、事業者の内部ネットワークに侵入し、不正プログラムへの感染や機密情報の窃取、ランサムウェアによるデータの暗号化等の攻撃を行う。その結果、攻撃を受けた事業者は、被害拡大を防止するためにシステムの運用を停止せざるを得なくなる場合や、業務に必要なファイルが暗号化されることによって業務継続に影響が及ぶ場合がある。

そのため、自組織で使用している機器について、平素からぜい弱性やアップデートに関する情報を確認し、ぜい弱性を放置することなく、各製品のベンダーが公表しているアドバイザリー[2]を基にファームウェアのアップデート、侵害の有無の確認等の対策を確実に実施することが必要である。また、自組織内に管理外のネットワーク機器が存在しないか確認することも必要である。システム保守を外部委託している場合は、ぜい弱性の対処が保守契約に含まれているかを確認し、その対処が適切に実施されていることを確認することも重要である。

【ぜい弱性を放置することの危険性】



[2] ぜい弱性の内容や対策方法をまとめた文書

資料編

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

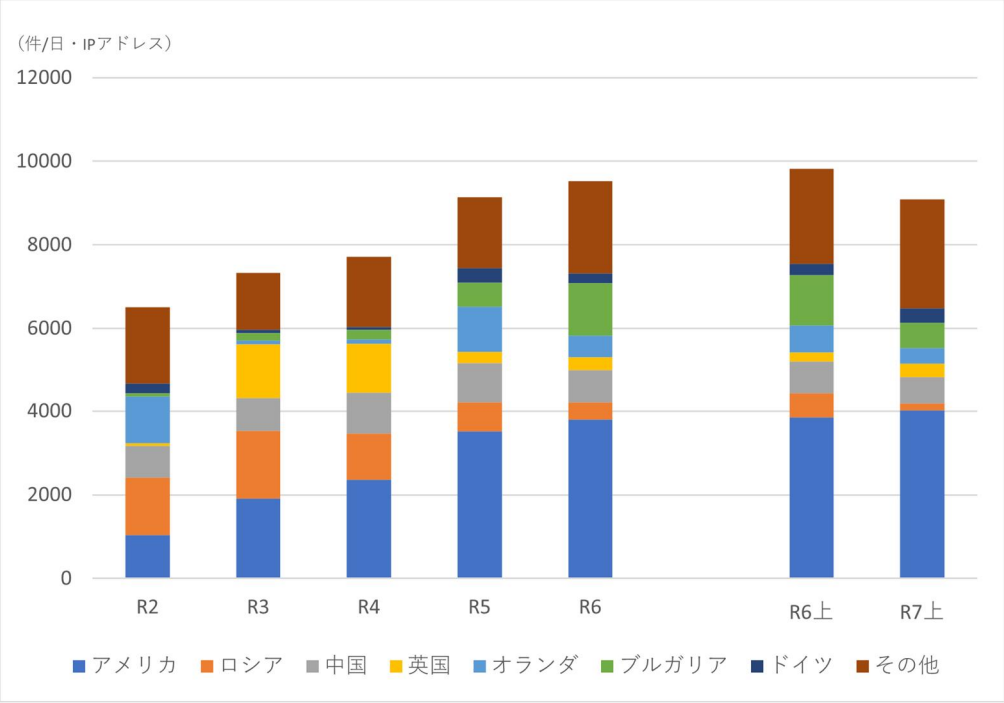
国別の不審なアクセス件数

本文図表１「警察庁が検知した不審なアクセス件数」を送信元国・地域別[3]で色付けしたものが以下の図表である。

令和６年上半期は、アメリカ、ブルガリア、中国、オランダ、ロシアの順で、令和７年上半期は、アメリカ、中国、ブルガリア、オランダ、ドイツの順で、それぞれアクセス件数が多くなっている。

令和６年上半期と令和７年上半期を比較すると、ブルガリアの件数が減り、順位を下げている。これは、令和６年の２月から３月にかけて、ブルガリアの特定のＩＰアドレスから広範な宛先ポートに対してアクセスするといった特徴を含む大量のアクセスが観測されたためで、当該アクセスは、当該期間におけるブルガリアからのアクセスの約78.8%を占めていた。令和７年上半期については、当該アドレスからのアクセスは大幅に減少している。上記の特徴を含むアクセスはインターネット上で稼働する機器やサービスの探索を行う手段として用いられることが多く、今後も継続的に観測をしていく。

図表　不審なアクセス件数の国別の推移（年別、送信元国･地域別）



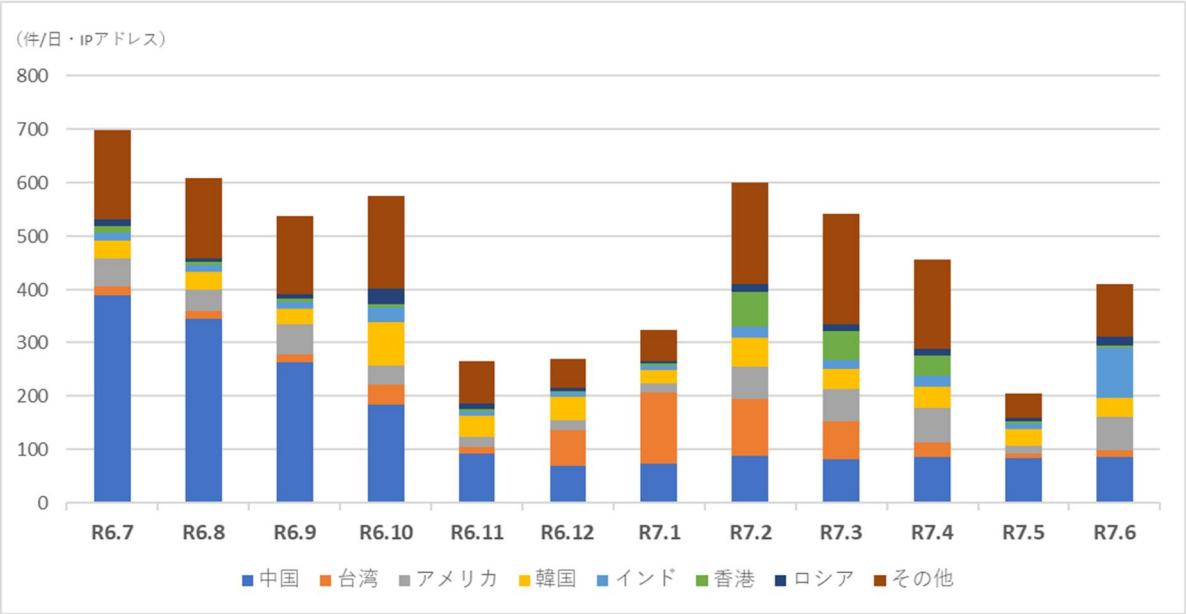
[3] 送信元国・地域については判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなど、送信者の所在と一致しない場合がある

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

Mirai ボットの特徴を有するアクセスの観測

Miraiボットの特徴[4]を有するアクセスの観測状況について、警察庁では継続して観測している（図表）。

図表　Miraiボットの特徴を有するアクセス件数の推移
（月別、送信元国・地域別　R6.7.1～R7.6.30）



Mirai ボットは、Mirai と呼ばれるマルウェアが感染した家庭用無線ルータやＩｏＴ機器のことで、気付かないうちにＤＤｏＳ攻撃等の不正行為に利用される可能性がある。

令和６年下半期に多く観測していた中国からのパケットは減少し、令和６年12月頃から令和７年４月頃にかけて、台湾からのパケットが増加した。令和７年２月頃から令和７年４月頃にかけては、アメリカ及び香港からのパケットが増加した。令和７年６月頃からインドのパケットが増加した。

令和７年上半期は、１月に300件（１日・１ＩＰアドレス当たり）であったものが、２月には600件（１日・１ＩＰアドレス当たり）と倍増している。２月は、クラウドサービスを行っているルータからのアクセスが多く見られた。当該ルータには、認証なしで遠隔からルータの設定を変更するなどの悪用が可能なぜい弱性（CVE-2024-12912）が報告されており、このぜい弱性との関連性が疑われる。Mirai等のマルウェアは、新しく発見されたぜい弱性を突いて感染を広げる亜種が開発されることもあることから、ネットワークに接続された機器については、アップデート等を適切に実施することが必要である。

[4] 宛先の IP アドレスと TCP のシーケンス番号の初期値が一致する特徴

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

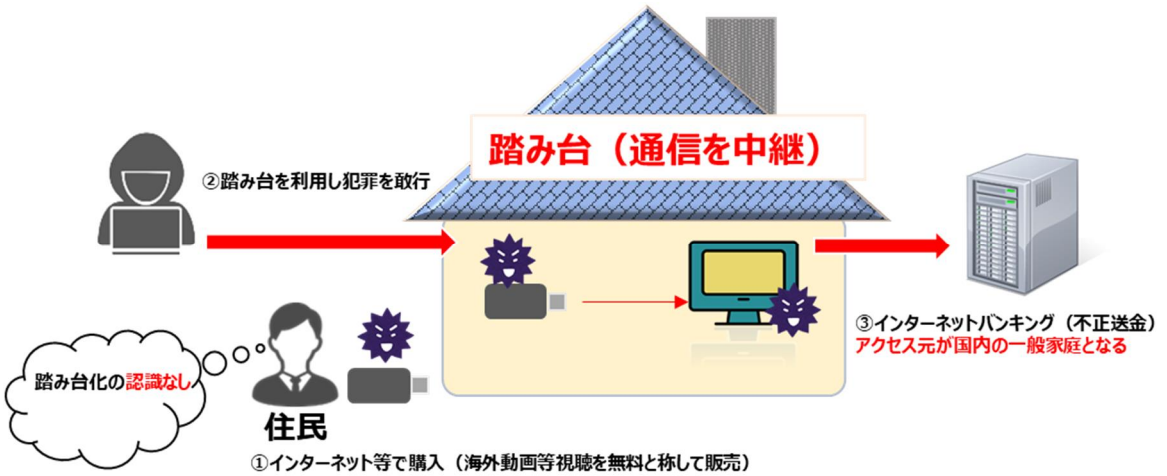
セットトップボックス等を踏み台とする不正アクセス

「テレビに接続して海外動画を無料で視聴できます」などと称して販売されている「セットトップボックス」と呼ばれるＩｏＴ機器が不正アクセス等の踏み台として悪用される事案が発生している。

これらの機器の中には、機器の購入前の段階において、ダウンローダー等の不正なソフトウェアが仕込まれた機器が流通しているものもあり、当該機器をインターネットに接続することにより、使用者の気付かないうちにマルウェアをインストールしてプロキシとして動作するものがある。これらの機器が踏み台となり、攻撃者の通信を中継した場合、通信先のサーバのログには、攻撃者のＩＰアドレスではなく、踏み台となった機器のＩＰアドレスが記録される。海外の攻撃者であっても、国内の機器を踏み台とすることにより、海外からのアクセスを制限したサーバにアクセスすることも可能となるなど、セキュリティ対策上の脅威となっている。

警察庁では、広報啓発資料「サイバー警察局便り」を作成し、警察庁ウェブサイト等において公開して、その手口の詳細や対策に関する注意喚起を実施した。

図表　IoT 機器が踏み台となるイメージ



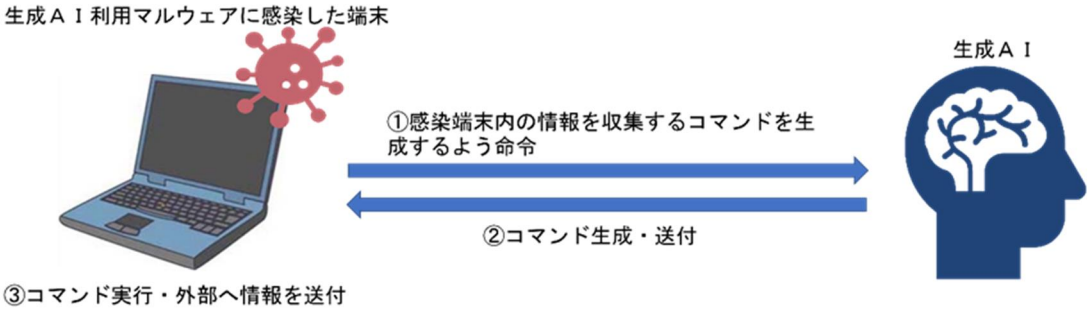
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

生成 AI を利用するマルウェア

令和７年７月、海外において、政府職員を装った者が、生成ＡＩを利用するマルウェアをメールに添付し、政府機関宛てに配布するサイバー攻撃が確認された。

当該マルウェアは、メールに添付されたファイルを開くことによって端末に感染するものであり、警察庁において本件に係る検体を解析したところ、図表に示すような動作が確認された。

図表　生成 AI を利用するマルウェアの動作イメージ



当該マルウェアの本体には攻撃に関する命令が記録されておらず、生成ＡＩによって不正なコマンドが生成されることから、生成される度にコマンドが異なる場合があり、特定のパターンを検出してファイル削除等を行うウイルス対策ソフトによる検知を回避しやすくなると考えられる。また、攻撃の標的となった企業が正規に利用する生成ＡＩサービスが攻撃に利用された場合、当該サービスの攻撃利用に係る通信と正規利用に係る通信との判別が難しく、マルウェアが検知されにくくなることも考えられる。

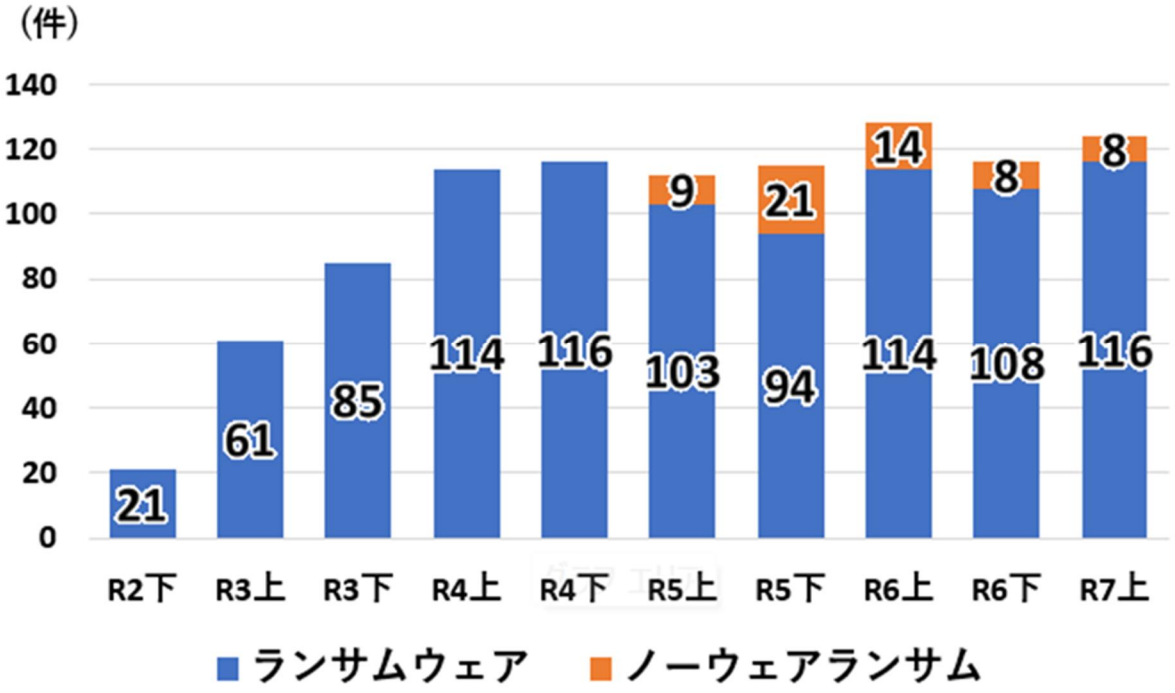
そのため、安易にメールの添付ファイルを開かない、自社の端末に対して生成ＡＩの利用制限を設けるなどの対策が重要になると考えられる。

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

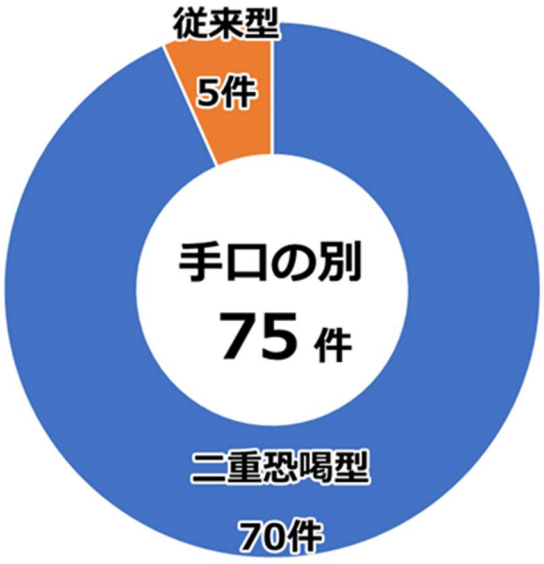
ランサムウェアの被害に関する統計

１　企業・団体等における被害の報告件数の推移

※ノーウェアランサムの被害については、令和５年上半期から集計。



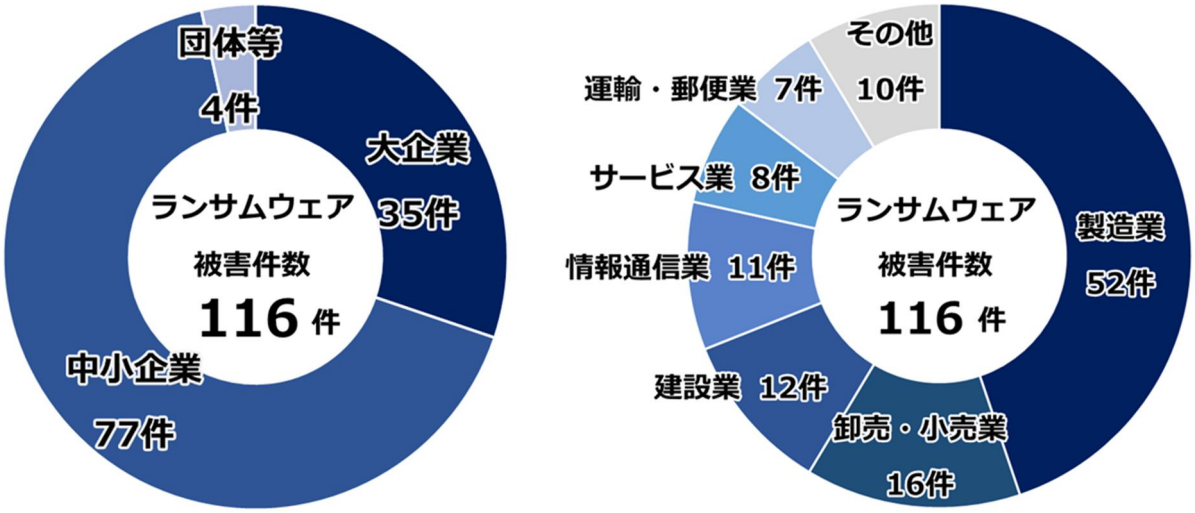
２　手口別報告件数



（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

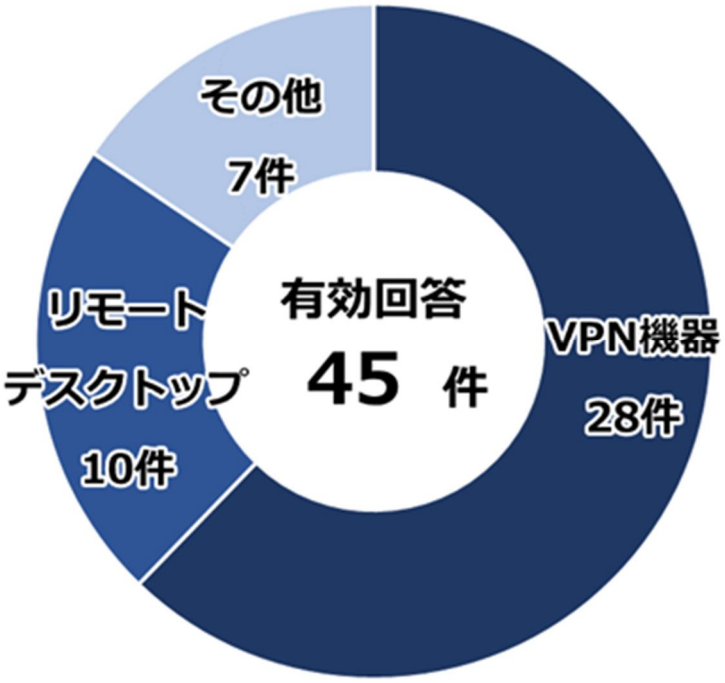
ランサムウェアの被害に関する統計②

３　被害企業・団体等の規模別／業種別報告件数



４　ランサムウェア被害にあった企業・団体等へのアンケート調査の回答結果

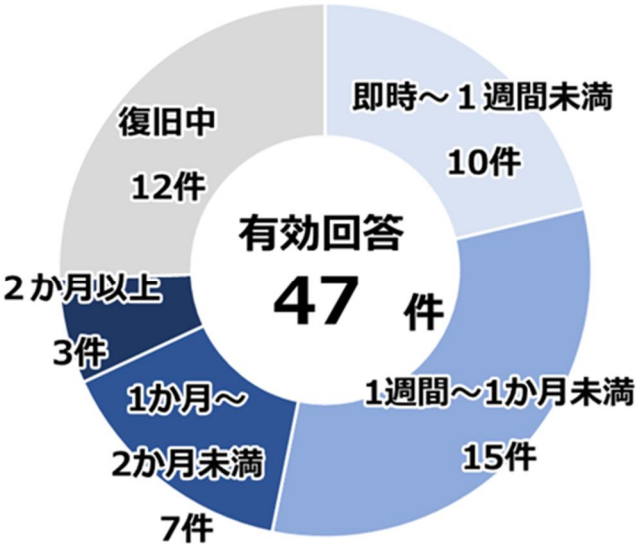
● 感染経路

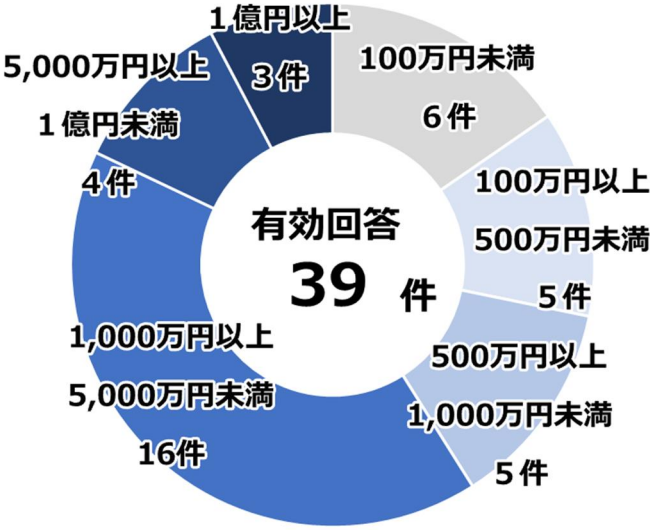


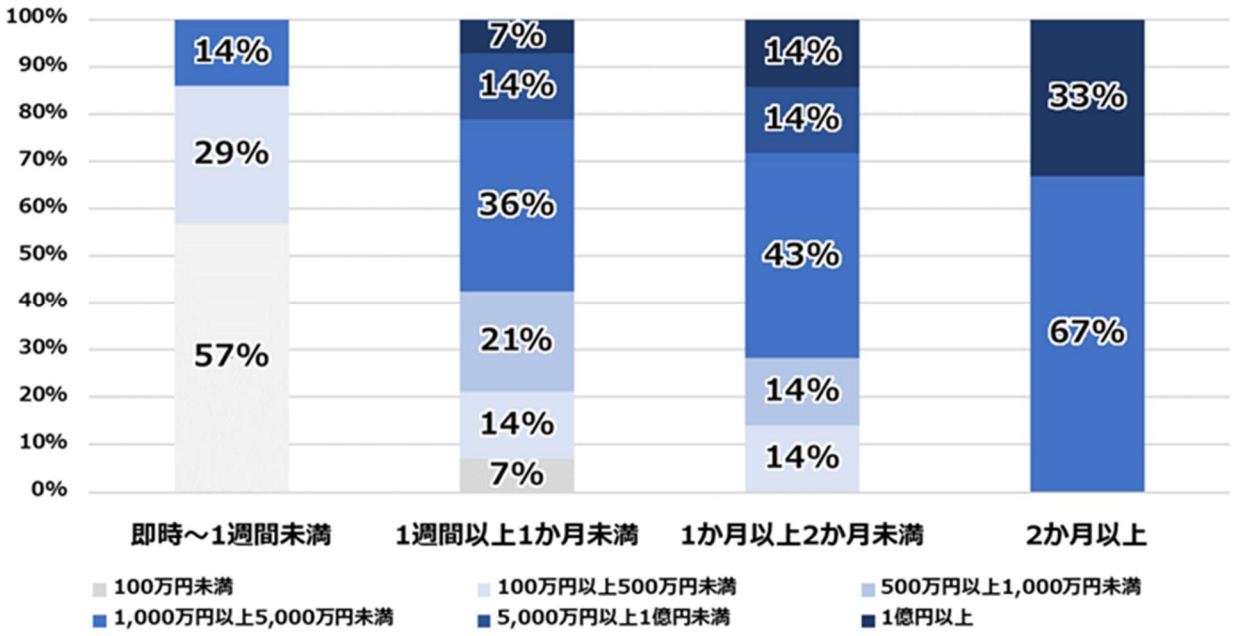
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

ランサムウェアの被害に関する統計③

● 復旧等に要した期間／調査費用の総額／復旧期間と費用の関係性





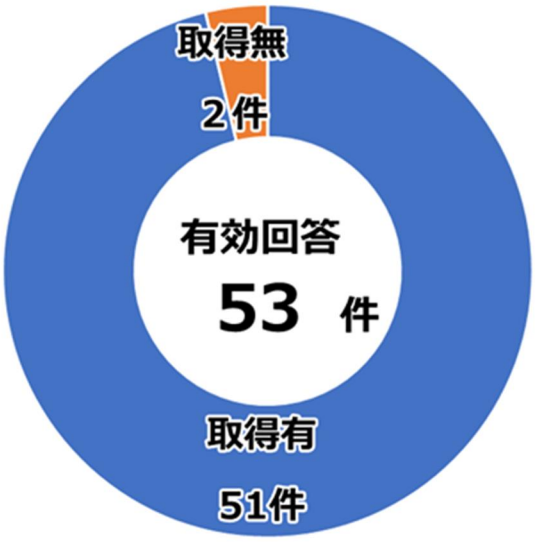


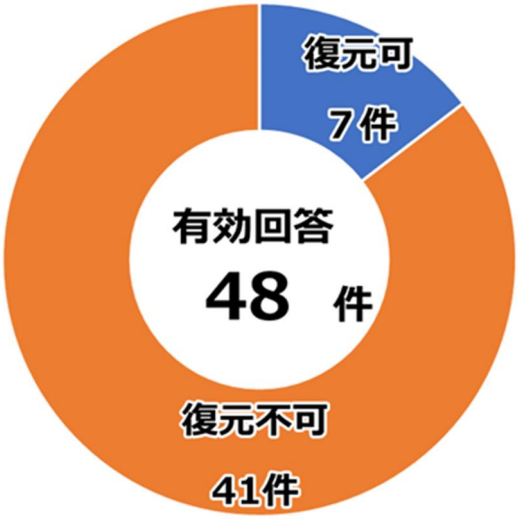
※　図中の割合は小数第１位以下を四捨五入しているため、統計が必ずしも 100 にならない。

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

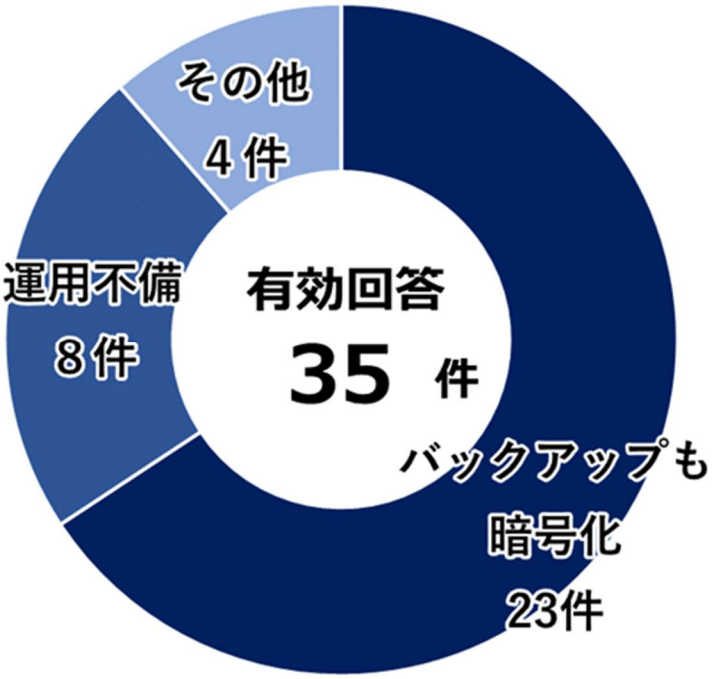
ランサムウェアの被害に関する統計④

● バックアップの取得状況／バックアップからの復元結果





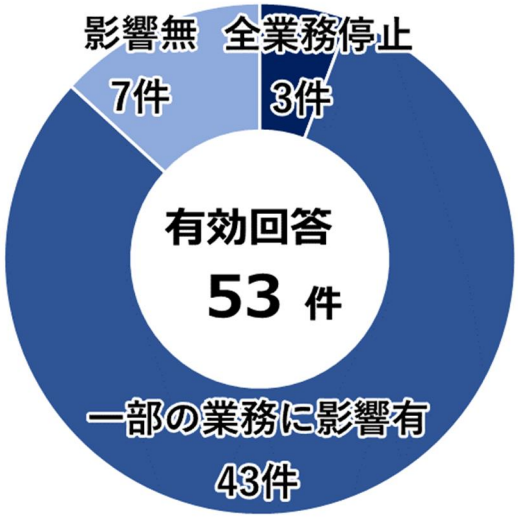
● バックアップから復元できなかった理由

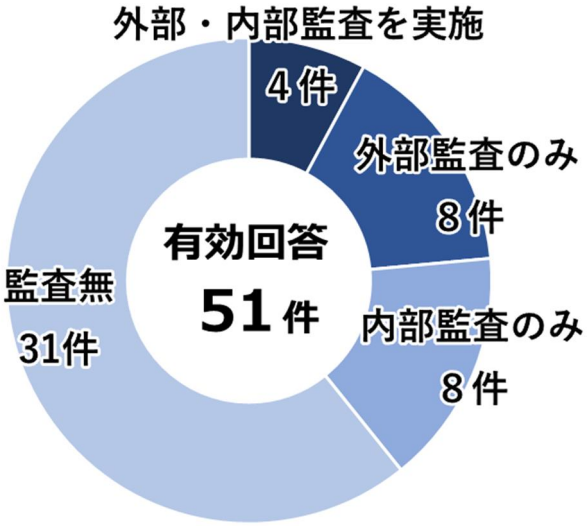


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

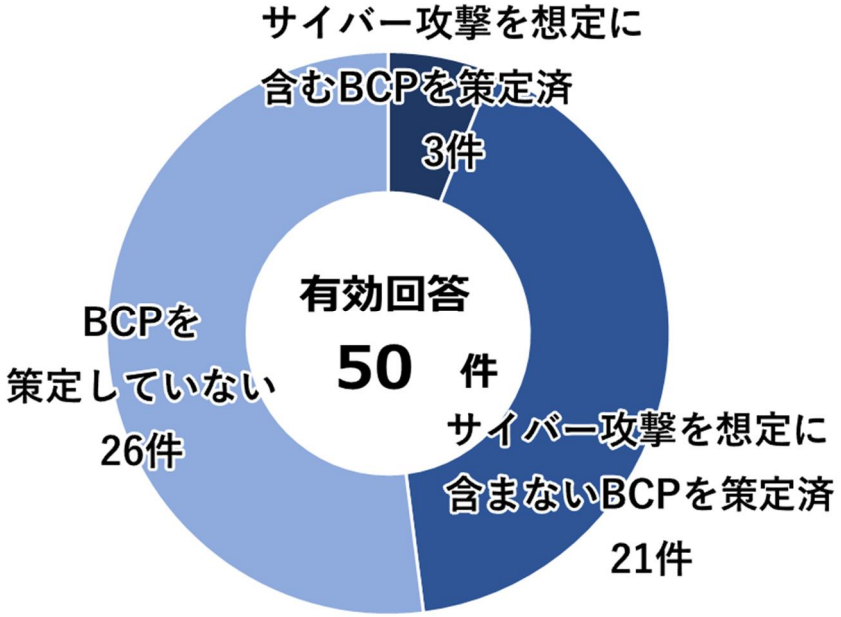
ランサムウェアの被害に関する統計⑤

● ランサムウェア被害が業務に与えた影響の程度
／被害企業・団体等の情報セキュリティ監査の実施状況





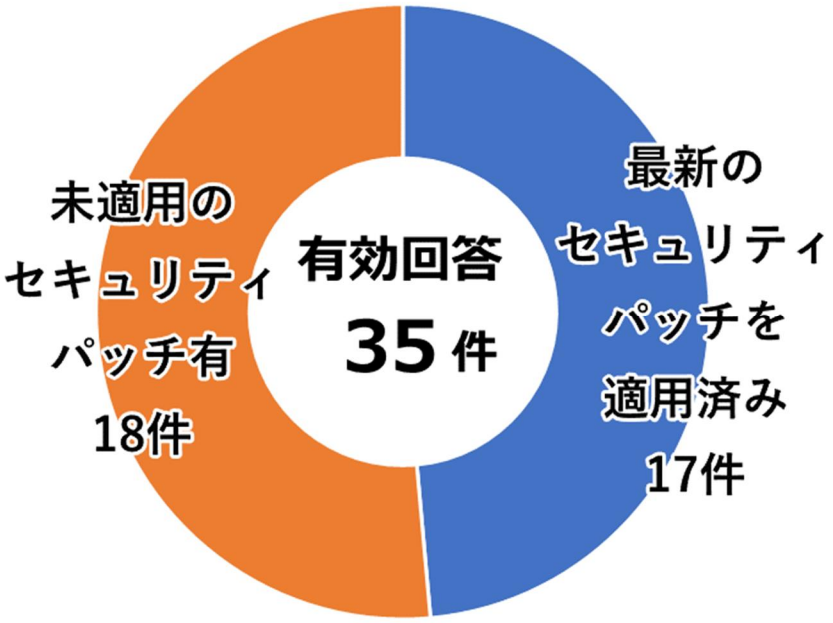
● 被害企業・団体等における業務継続計画（BCP）の策定状況



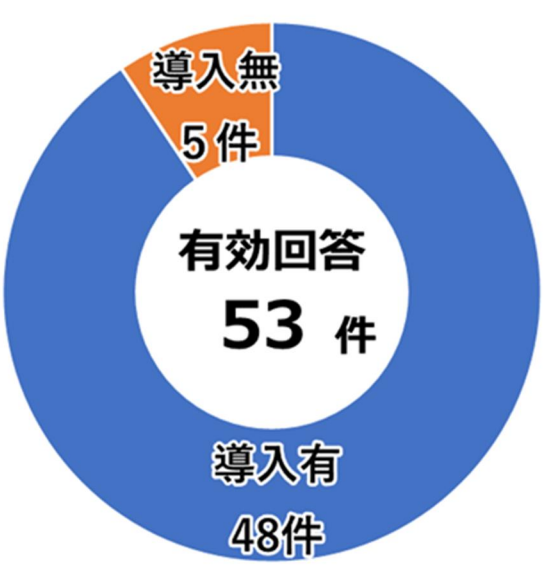
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

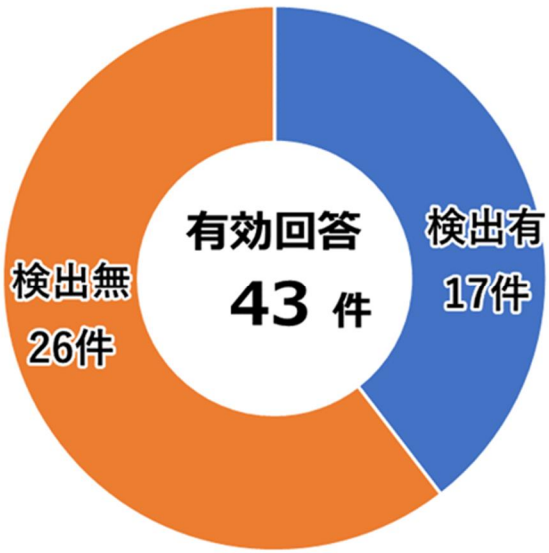
ランサムウェアの被害に関する統計⑥

● 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



● 被害企業・団体等のウイルス対策ソフト等導入／検出状況

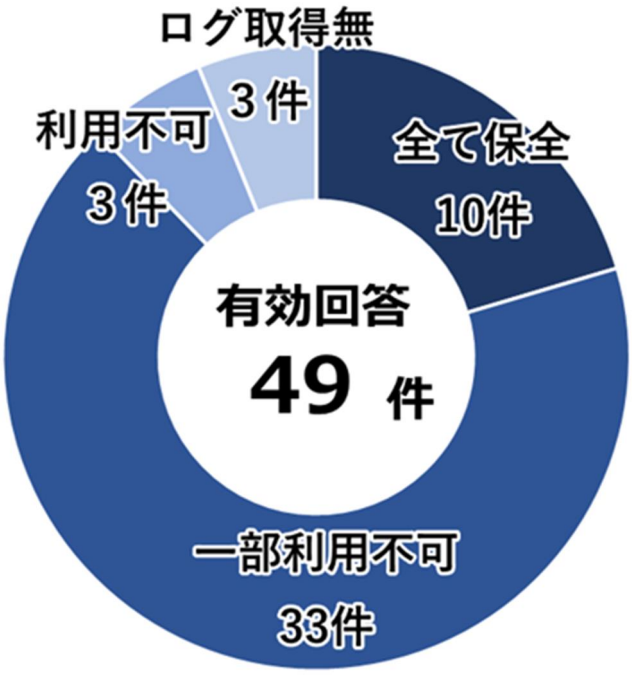




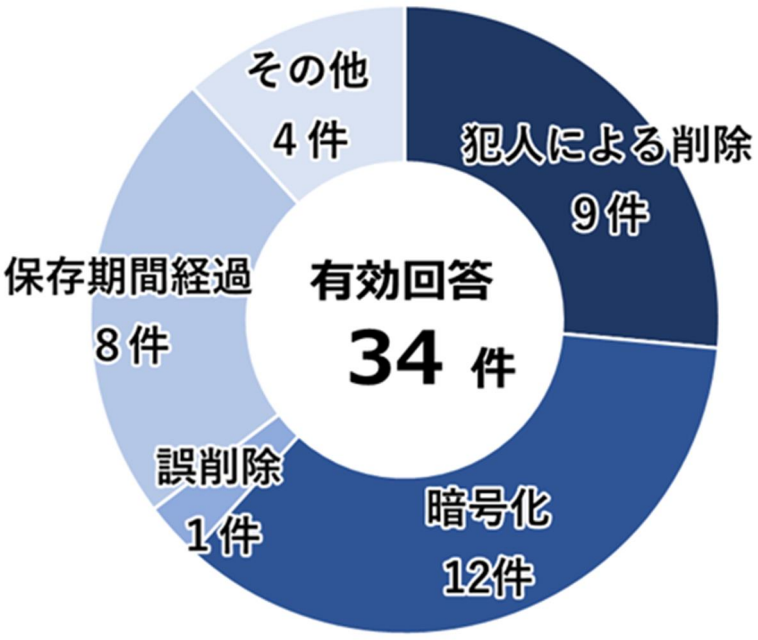
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

ランサムウェアの被害に関する統計⑦

● 被害企業・団体等のログ保全状況



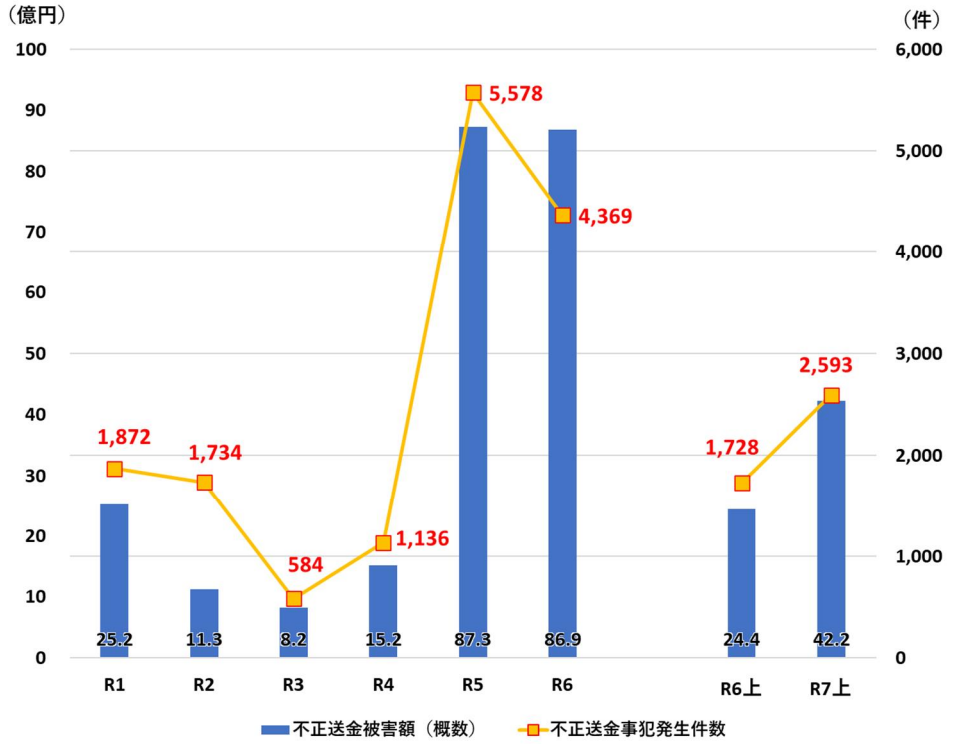
● ログが使用できなくなっていた原因



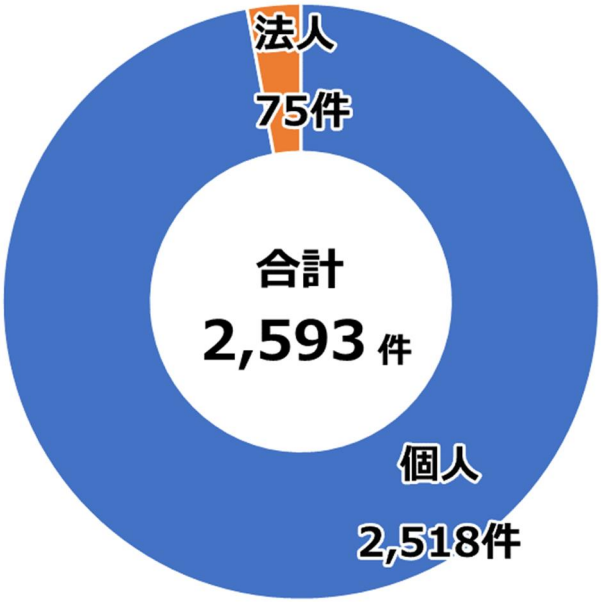
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯に関する統計

１　インターネットバンキングに係る不正送金事犯発生件数及び被害額の推移



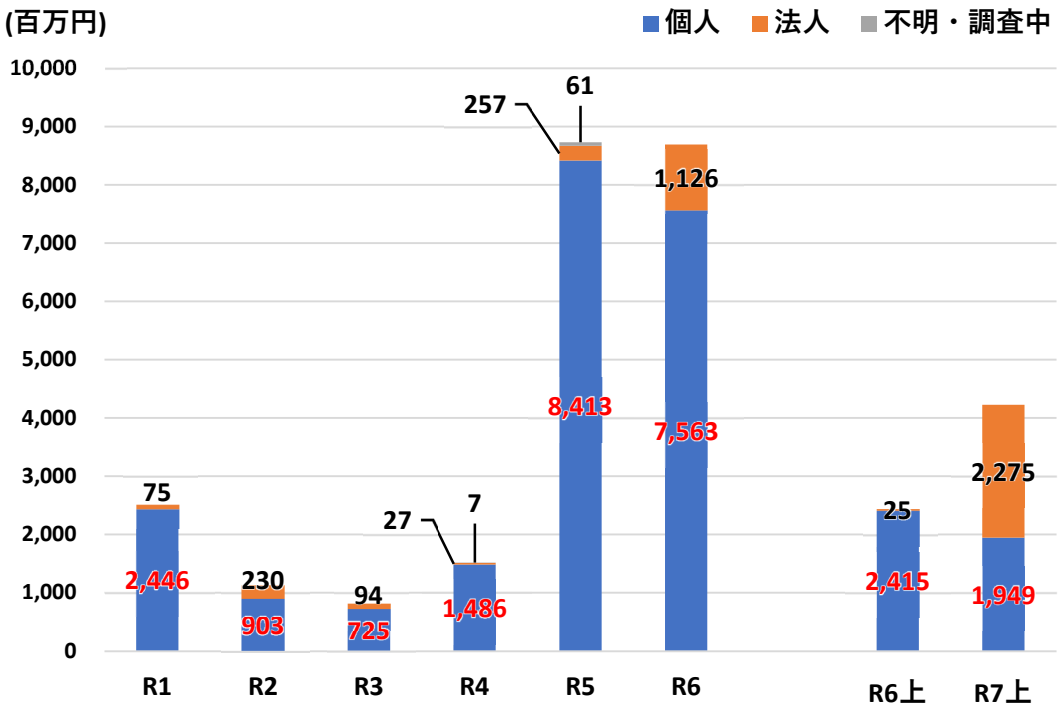
２　インターネットバンキングに係る不正送金発生件数（個人・法人別）



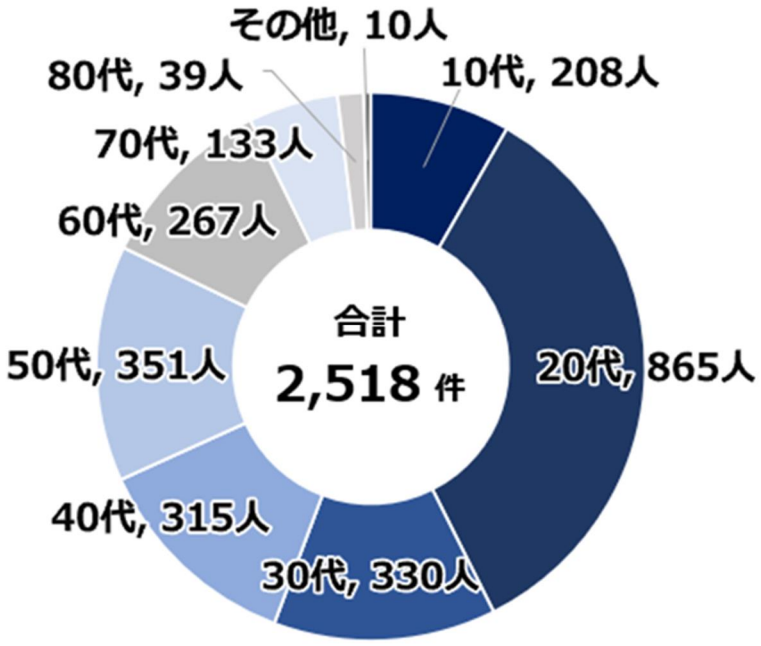
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯に関する統計②

３　インターネットバンキングに係る不正送金被害額の推移（個人・法人別）

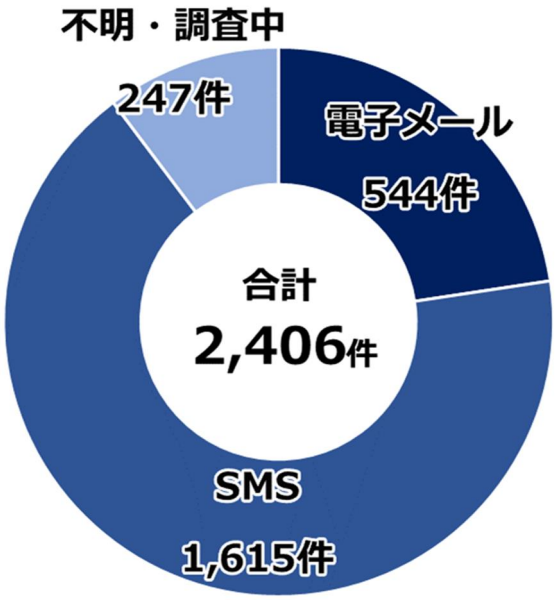


４　個人のインターネットバンキングに係る年齢別の不正送金被害者数

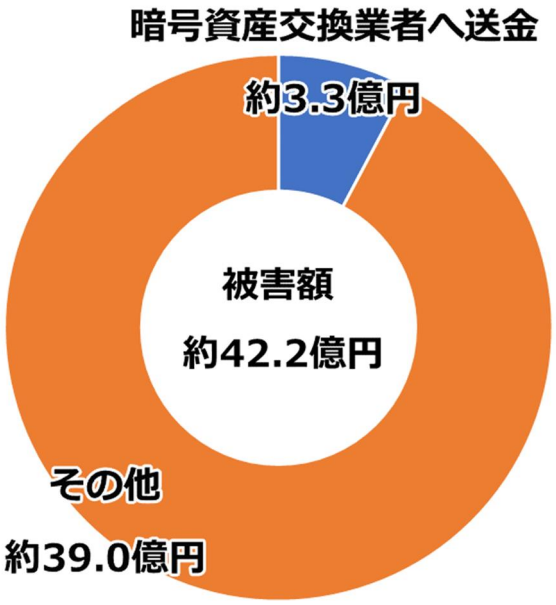


インターネットバンキングに係る不正送金事犯に関する統計③

５　フィッシングサイトへ誘導する手口別の不正送金発生件数



６　不正送金被害額のうち暗号資産交換業者名義の金融機関口座へ送金された額[5]



※　図中の金額は四捨五入しているため、被害額の合計が必ずしも一致しない。

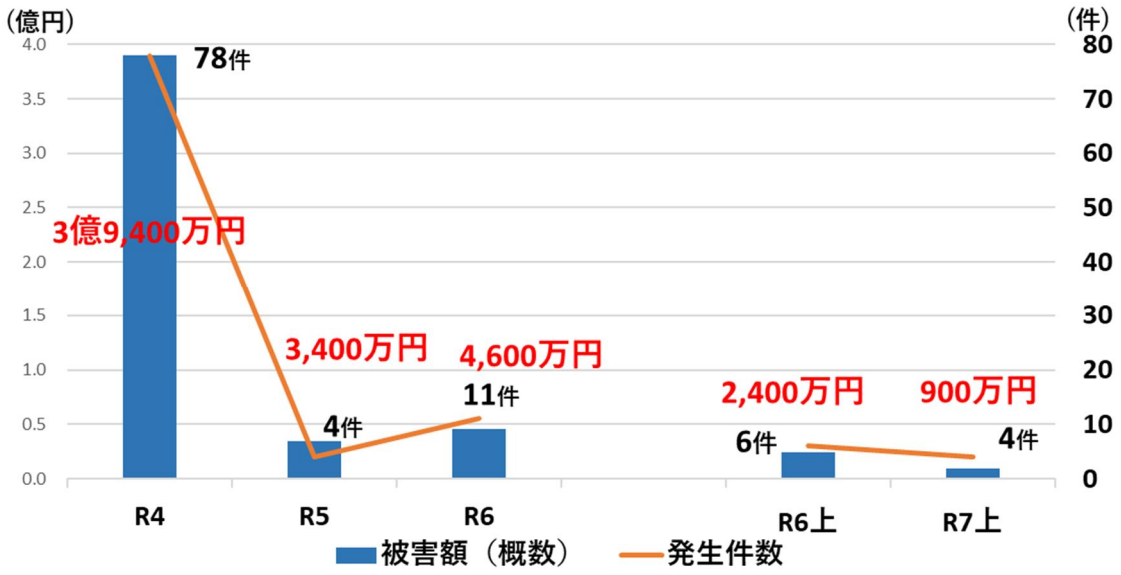
[5] 暗号資産交換業者の金融機関口座へ送金された後は、そのほとんどが暗号資産に変換されているものと考えられる。また、「その他」には、暗号資産交換業者の金融機関口座へ送金される前に被疑者等により使用されたもの、金融機関口座間の資金移動中に口座が凍結されたものを含む。

資料編

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

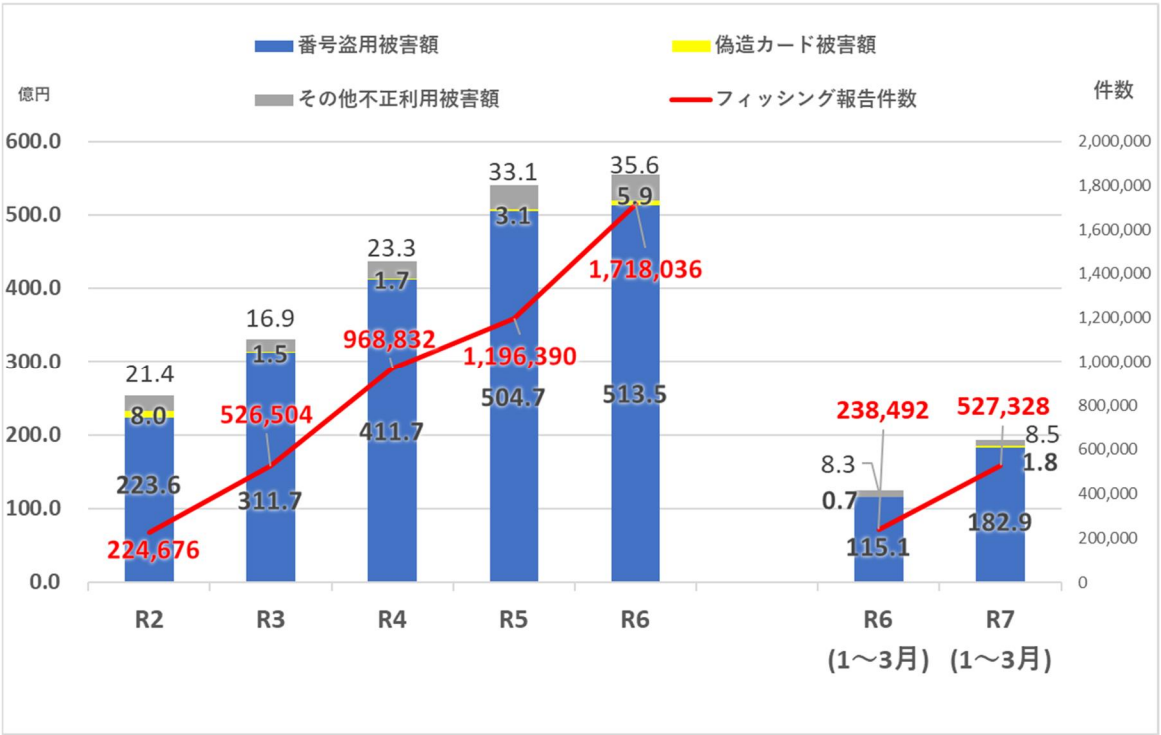
インターネットバンキングに係る不正送金事犯に関する統計④

７　ＳＩＭスワップに係る不正送金発生状況



クレジットカード不正利用被害に関する統計

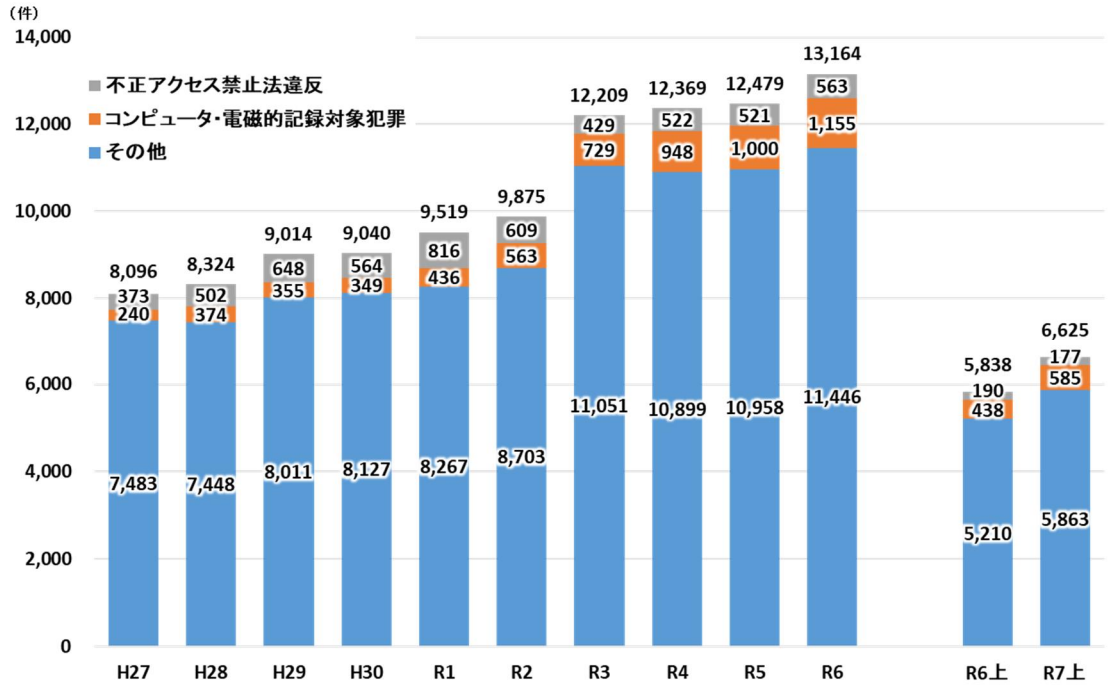
１　フィッシング報告件数及びクレジットカード不正利用被害額の推移



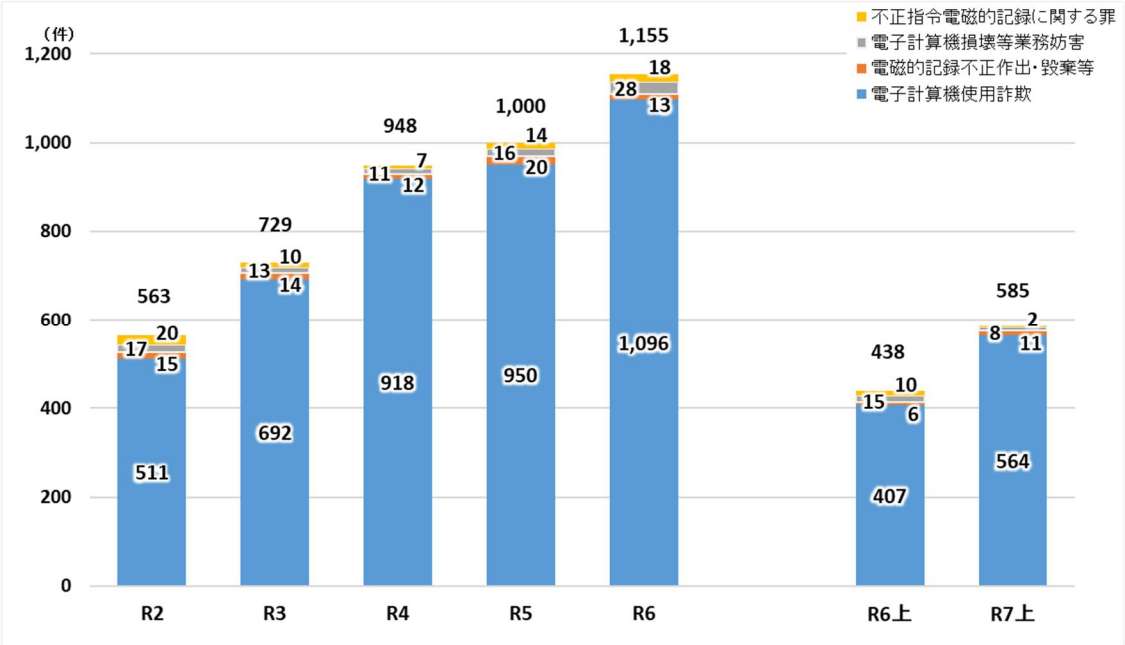
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計

１　サイバー犯罪[6]の検挙件数の推移



２　上記１中、コンピュータ・電磁的記録対象犯罪の検挙件数の推移

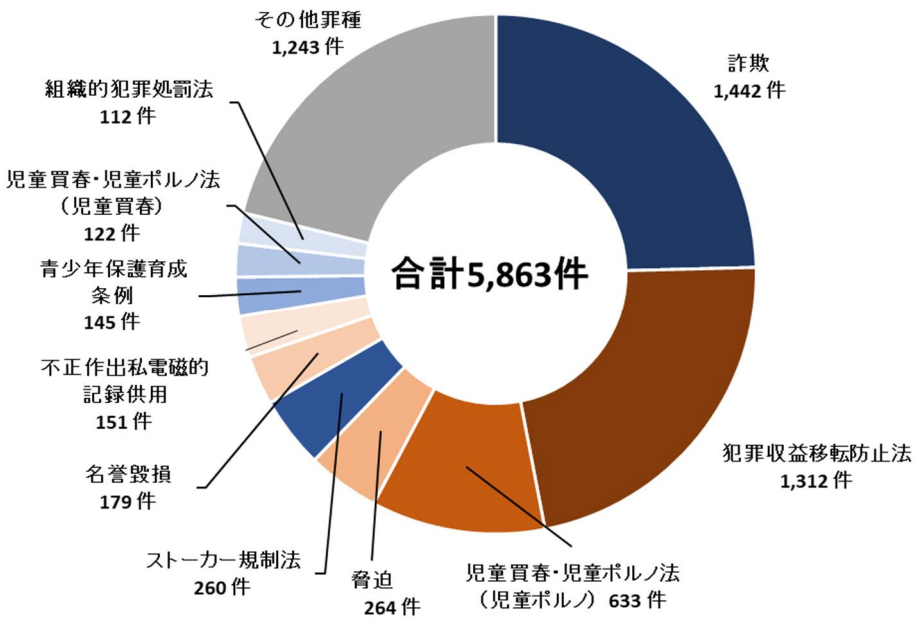


[6] 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

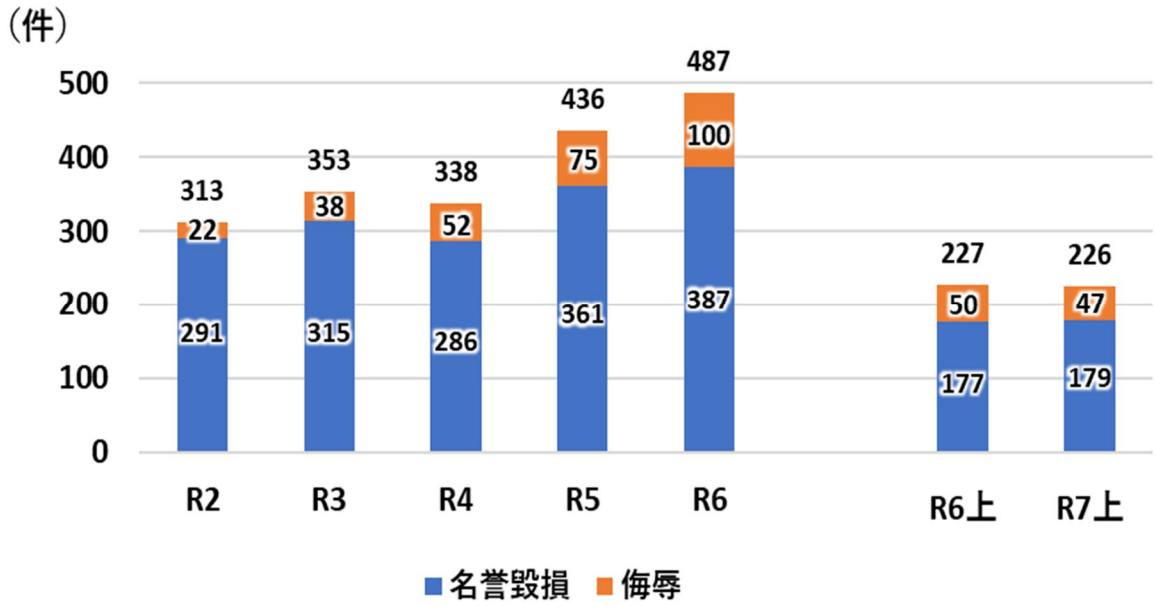
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計②

３　前記１中、「その他」の検挙状況



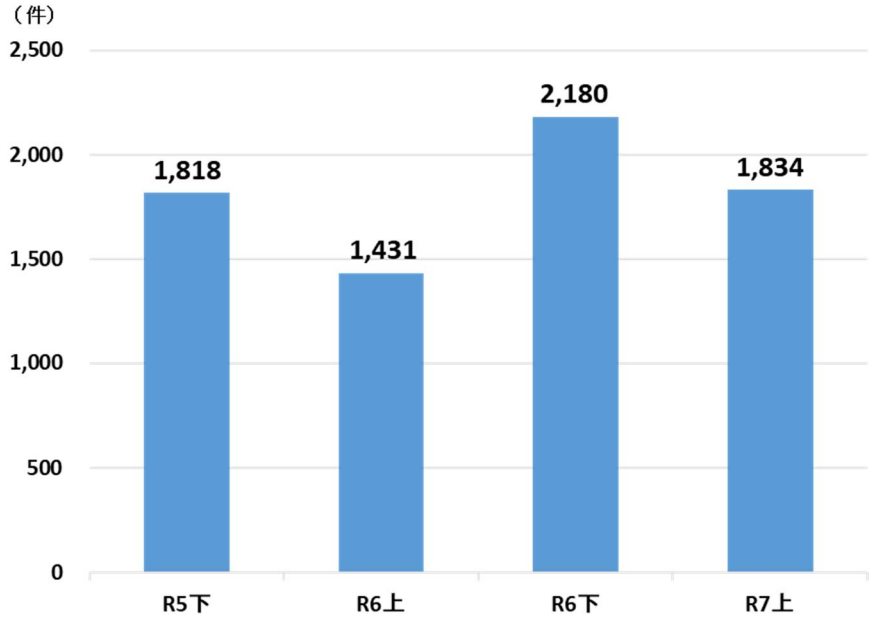
４　令和７年上半期中のインターネット上での名誉毀損罪及び侮辱罪の検挙件数



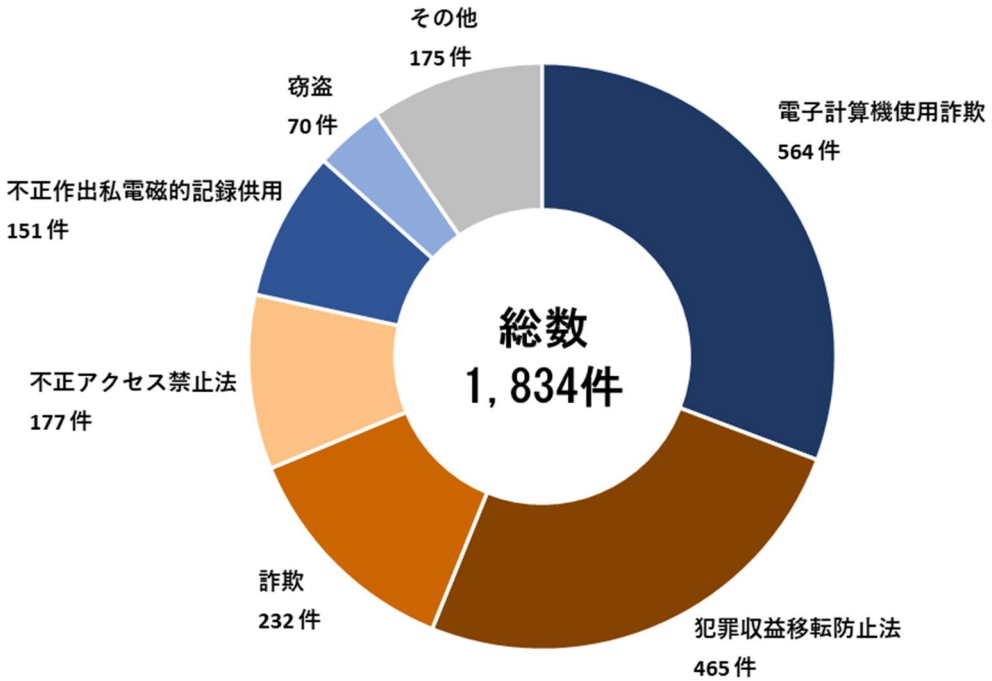
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計③

５　サイバー事案[7]の検挙件数の推移



６　サイバー事案の検挙状況

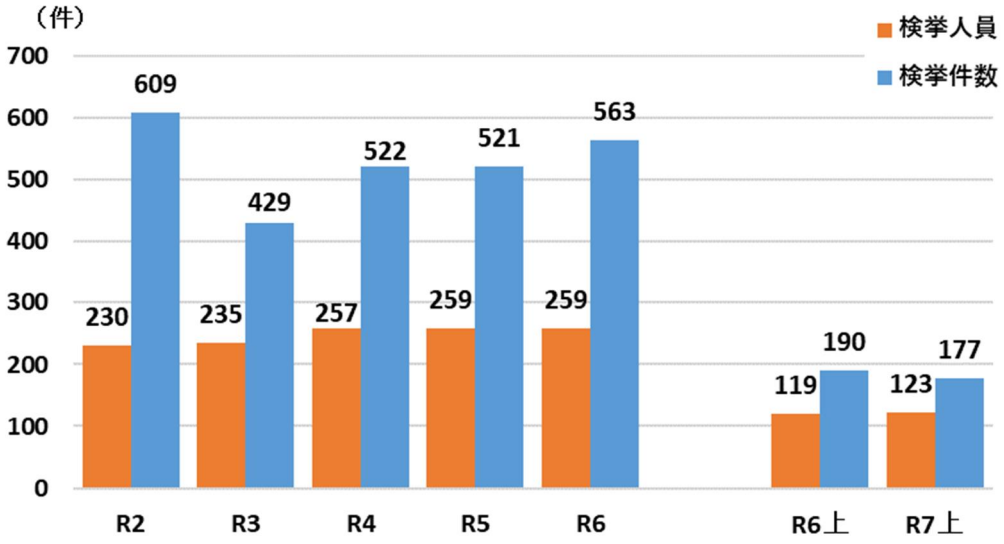


[7] サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。

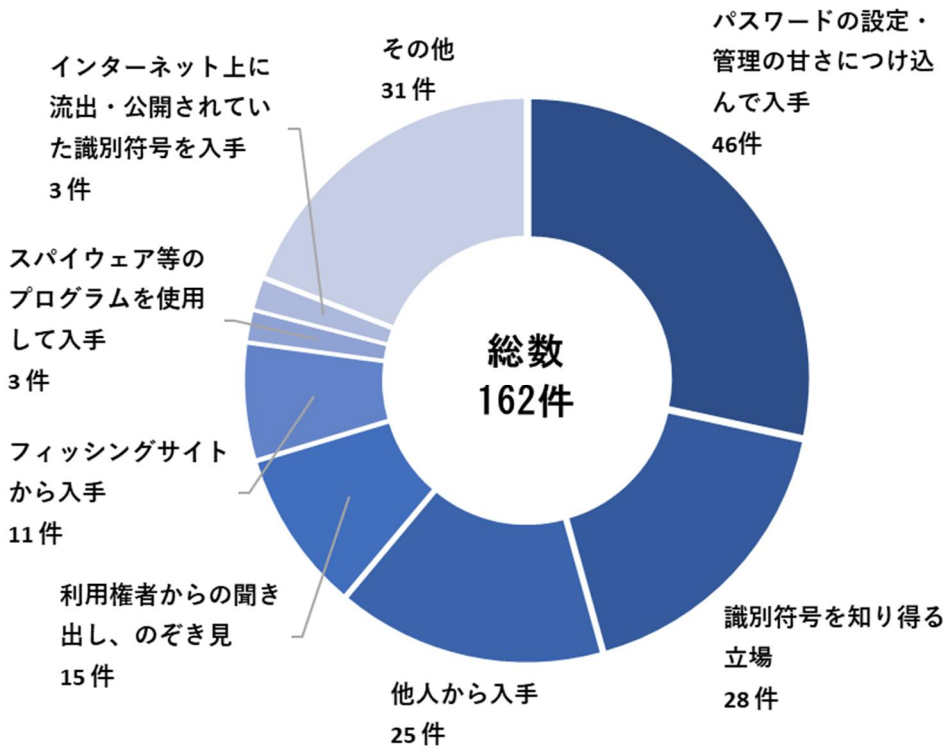
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計④

７　不正アクセス禁止法違反の検挙件数の推移



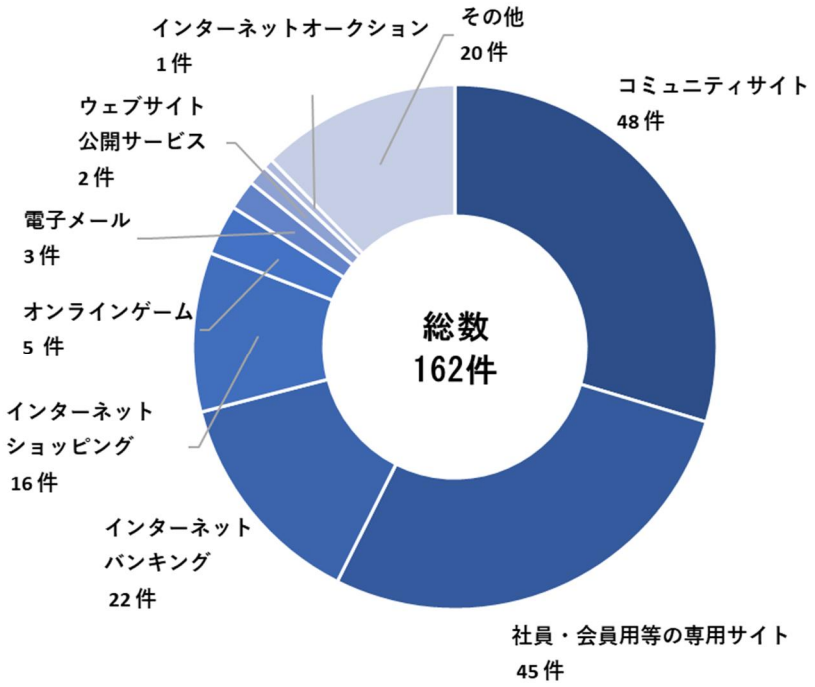
８　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



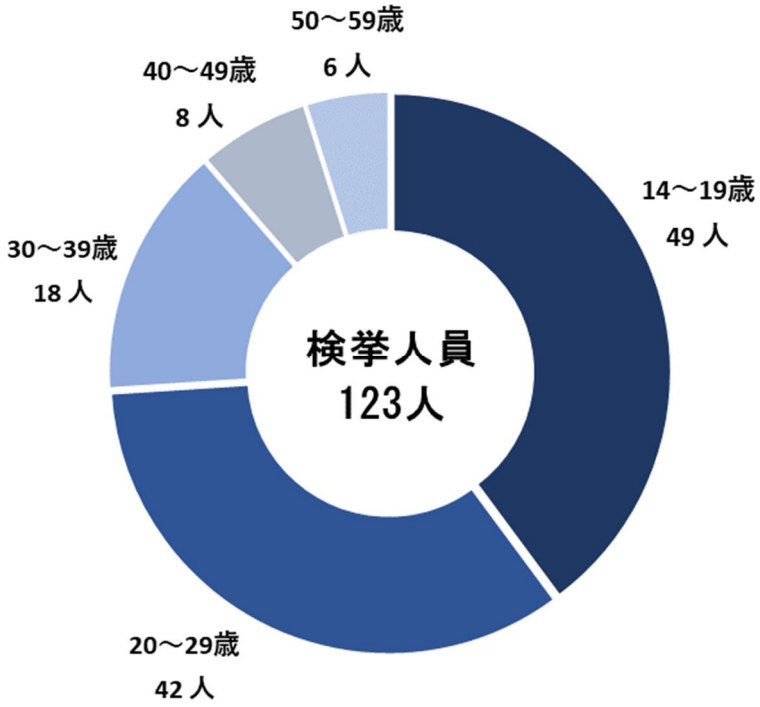
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計⑤

９　不正に利用されたサービス別検挙件数（識別符号窃用型）



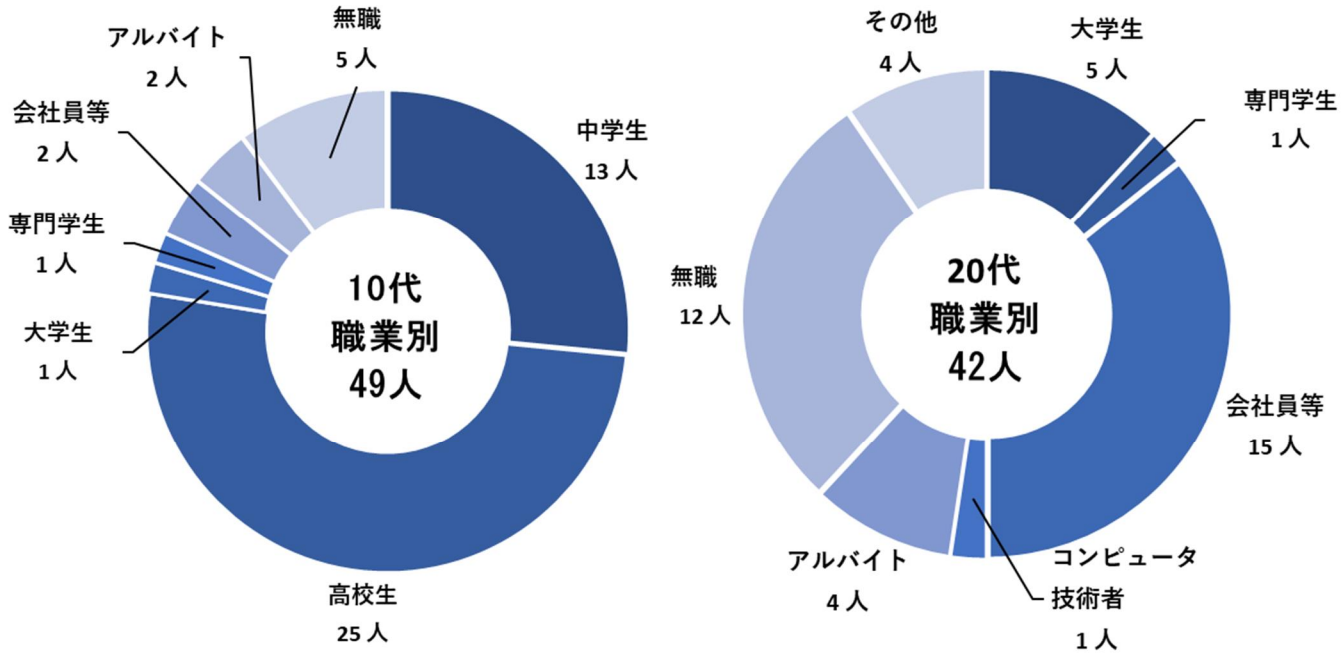
１０　不正アクセス禁止法違反被疑者の年齢構成



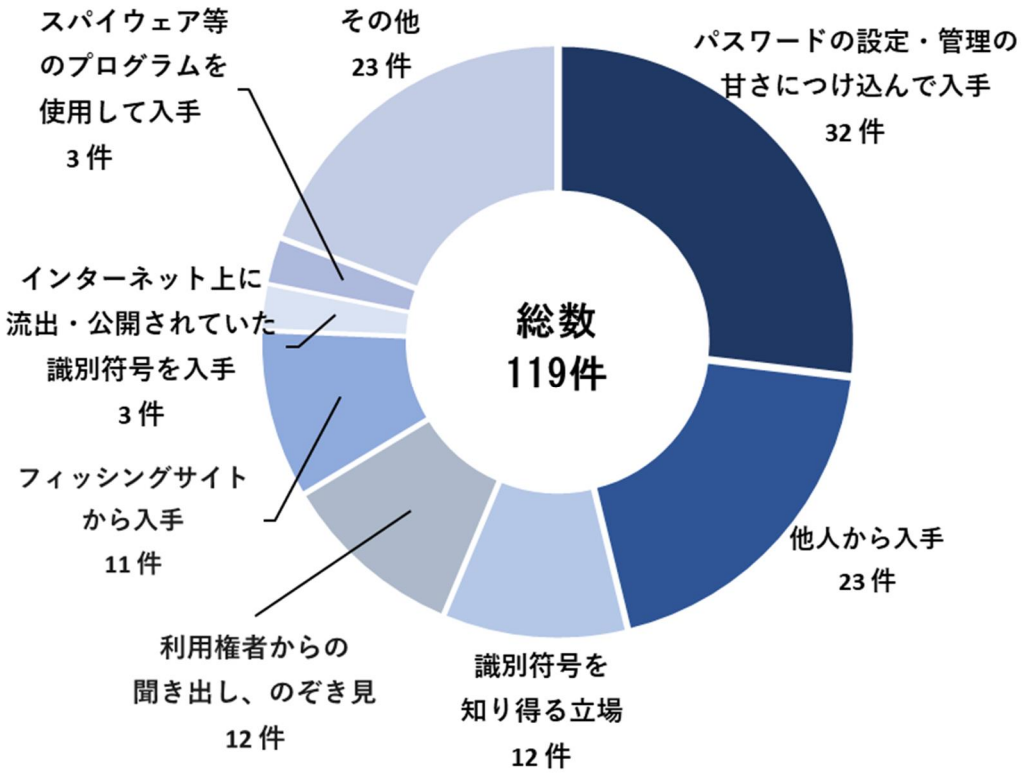
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計⑥

11　不正アクセス禁止法違反被疑者の 10 代～20 代における職業別



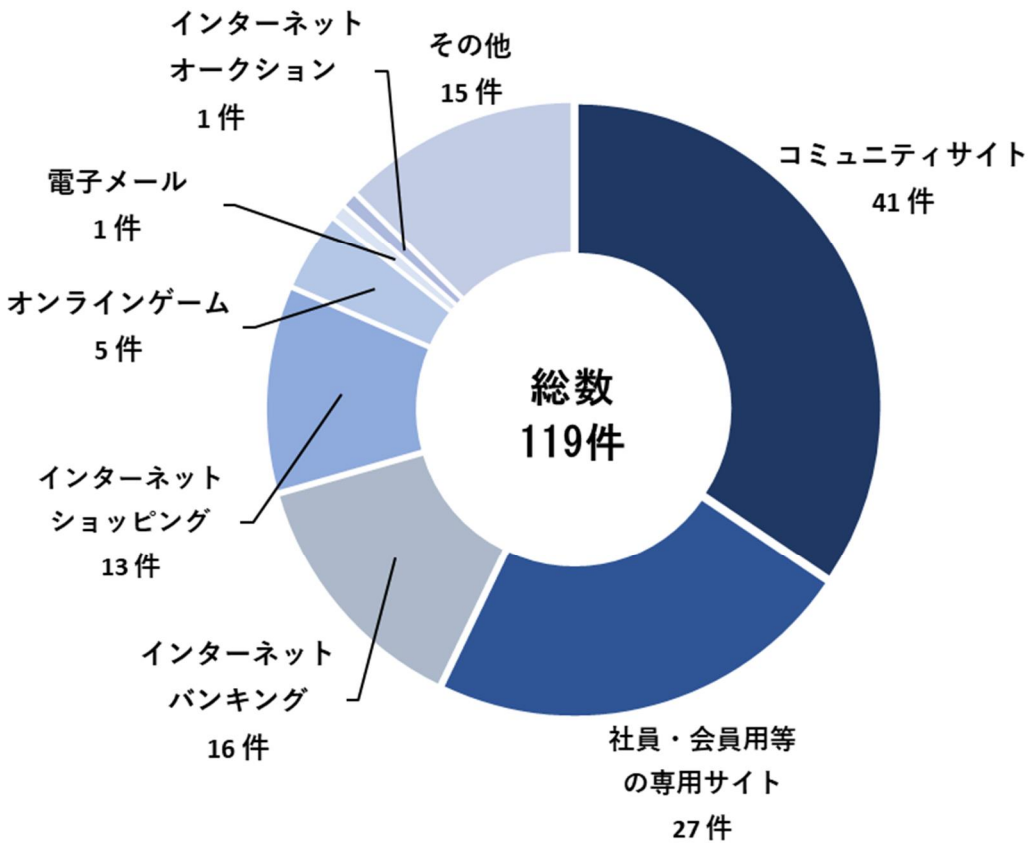
12　10 代～20 代における不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計⑦

13　10 代～20 代における不正に利用されたサービス別検挙件数（識別符号窃用型）の推移

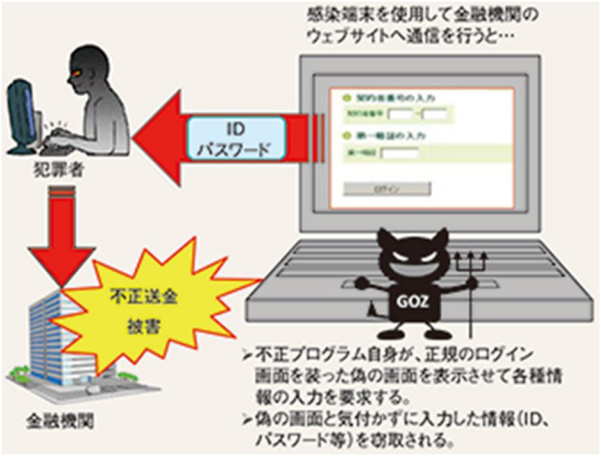


（第２部１「検挙に向けた取組」関連）

サイバー警察局設置前における国際共同捜査の主な事案一覧

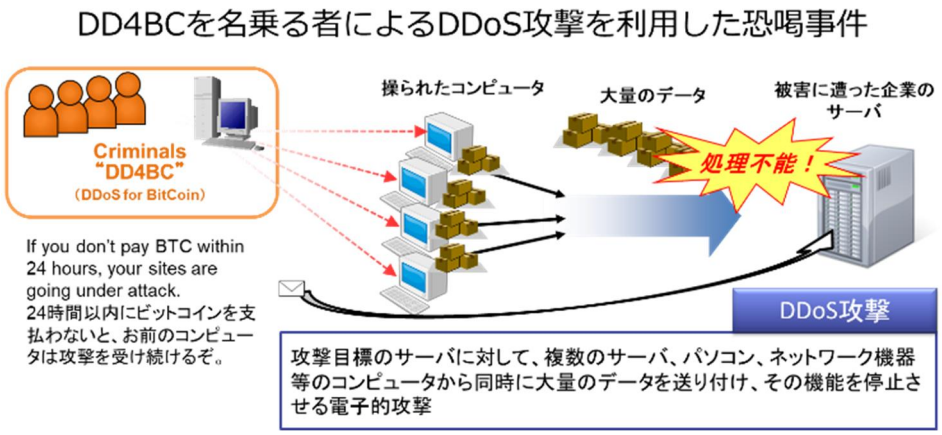
● 国際的なボットネットのテイクダウン

不正送金事犯に使用されているとみられる不正プログラム「Game Over Zeus(ゲームオーバーゼウス)」が世界的にまん延したことから、平成 26 年５月、FBI 及び EUROPOL を中心に、日本を含む協力国の法執行機関が連携して、同プログラムに感染した端末の情報を収集し、当該端末を特定した上で、プロバイダ等を通じて当該端の利用者に対して不正プログラムの駆除を促すことにより、国際的なボットネットのテイクダウンを決行した。



● DD4BC 犯罪者グループに対する国際的な対処

平成 27 年５月以降、DD4BC 等と名乗って金融機関、IT 企業等のサーバに DDoS 攻撃を仕掛け、当該攻撃回避のための支払いをビットコインで要求する恐喝未遂事件が発生した。同種手口事案は海外でも発生していたことから、EUROPOL 及び INTERPOL の調整の下、国際共同捜査が行われ、ボスニア・ヘルツェゴビナ警察等が関連する被疑者２人を検挙した。



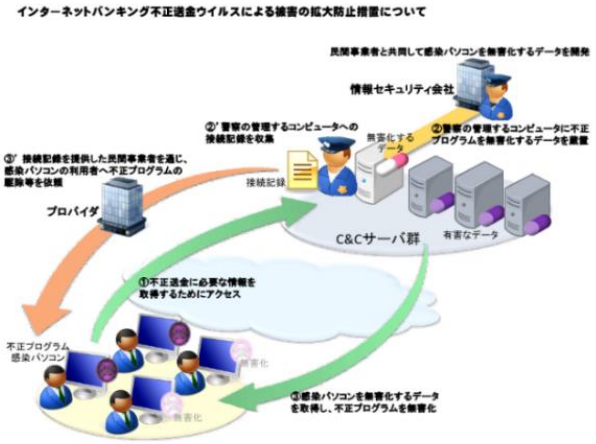
（第２部１「検挙に向けた取組」関連）

サイバー警察局設置前における国際共同捜査の主な事案一覧②

● 不正プログラムの無害化作戦の実施

平成 27 年４月、警視庁は、インターネットバンキングに係る不正送金事犯に利用されるＣ２サーバの動作を観測することにより、国内外において約８万 2,000 台の端末が不正プログラム「VAWTRAK（ボートラック）」に感染していることを把握し、不正プログラムによる被害の拡大防止措置を実施した。警視庁は、プロバイダを通じた国内の感染端末の利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供に加え、被害拡大防止措置として、不正プログラムの無害化措置の実施にも成功した。

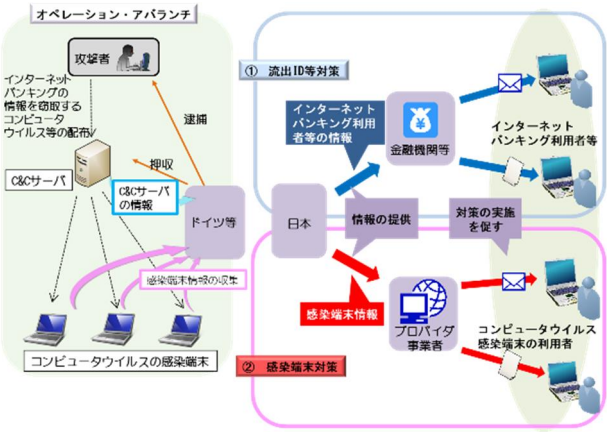
この不正プログラムに感染した端末は、Ｃ２サーバと定期的に通信を行い情報を取得するという性質があったことから、この性質を逆手に取り、無害なデータを取得させることにより、不正プログラムの無害化を行ったものである。



【インターネットバンキング不正送金に関する不正プログラムの無害化措置】

● インターネットバンキングに係る不正送金事犯に関する国際的な取組

平成 29 年３月、インターネットバンキングに係る不正送金事犯に関し、国際的な取組「オペレーション Avalanche（アバランチ）」に係る流出 ID 等対策及び感染端末対策を実施した。日本国内のインターネットバンキング利用者の ID・パスワード等の情報、コンピュータウィルスの感染端末情報等を入手するに至ったことから、関係省庁・団体と連携して、インターネットバンキング利用者、感染端末利用者等に対し、被害拡大防止のための注意喚起を実施した。

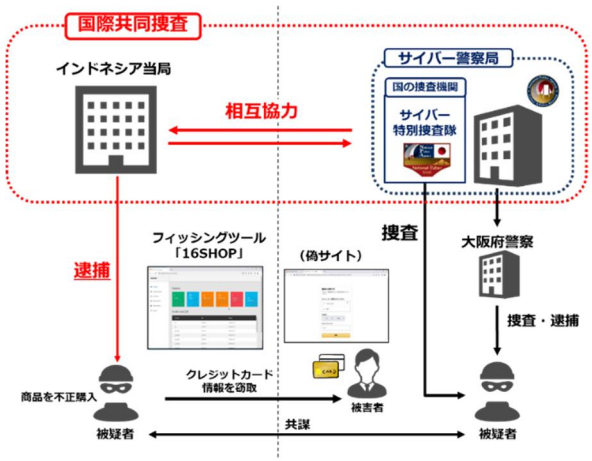


（第２部１「検挙に向けた取組」関連）

サイバー警察局設置後における国際共同捜査の主な事案一覧

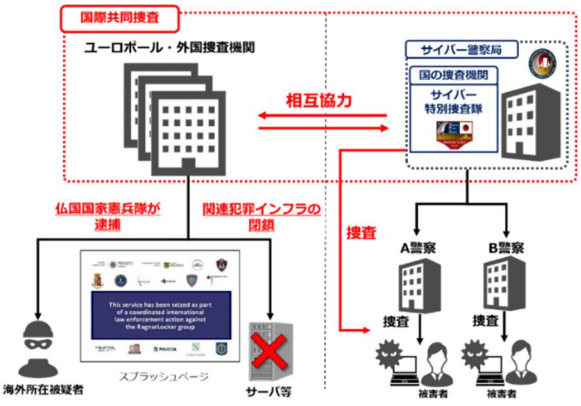
●　「16SHOP」を用いたクレジットカード情報不正取得・利用事案

フィッシングツール「16SHOP」を用いたクレジットカード情報不正取得・利用事案に係る捜査では、サイバー特別捜査隊（当時）等とインドネシア国家警察との国際共同捜査「オペレーション Kingfisher（キングフィッシャー）」により、同ツールを用いて日本国内の被害者等に対しフィッシングを行い、不正に入手したクレジットカード情報等を用いて EC サイトで不正注文を行ったとみられるインドネシア所在の被疑者を特定した。令和５年（2023 年）７月、インドネシア国家警察が同被疑者を逮捕するに至り、フィッシングに関して国外被疑者を検挙した初の事例となった。



●　「Ragnar Locker」によるランサムウェア攻撃事案

ランサムウェア攻撃グループ「Ragnar Locker」に係る国際共同捜査「オペレーション Talpa（タルパ）」においては、サイバー特別捜査隊（当時）等による国内捜査により得られた情報を関係国捜査機関等に提供するなどした結果、令和５年（2023 年）10 月、関係国捜査機関により「Ragnar Locker」の開発者であると考えられている被疑者が逮捕されたほか、同グループが使用するサーバ等の犯罪インフラがテイクダウン（機能停止）された。テイクダウンに当たっては、同グループが使用し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が表示された。同ページには、我が国を含む関係国捜査機関の記章が掲げられており、多国間の国際共同捜査への我が国の参画を強く示すものとなった。



（第２部１「検挙に向けた取組」関連）

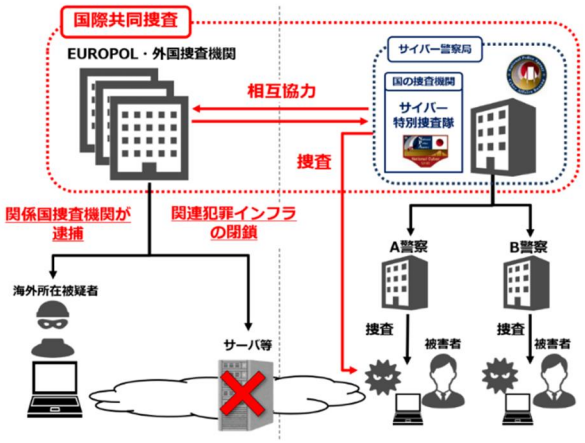
サイバー警察局設置後における国際共同捜査の主な事案一覧②

●　「LockBit」によるランサムウェア攻撃事案

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」について、サイバー特別捜査隊（当時）と関係警察は、EUROPOL 等との国際共同捜査「オペレーション Cronos（クロノス）」を推進した。その結果、令和６年（2024 年）２月、関係国の捜査機関が同グループの一員とみられる被疑者２名を逮捕したほか、同グループが使用するサーバ等がテイクダウン（機能停止）され、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が表示された。

この事案では、LockBit により暗号化されたデータを復号するツールを、サイバー特別捜査隊が独自開発し、国内での被害回復に活用するとともに、令和５年 12 月には同ツールを EUROPOL に提供した。また、令和６年２月、警察庁は EUROPOL 等と連携し、世界中の企業等において被害回復が可能となるよう、同ツールについて情報発信を行い、その活用を促す旨の発表を行った。

また、これに続く措置として、令和６年（2024 年）５月、ランサムウェアの開発・運営を行っていた被疑者について資産凍結及び起訴が行われ、令和６年（2024 年）10 月には関連被疑者４名が逮捕された。



【スプラッシュページ】

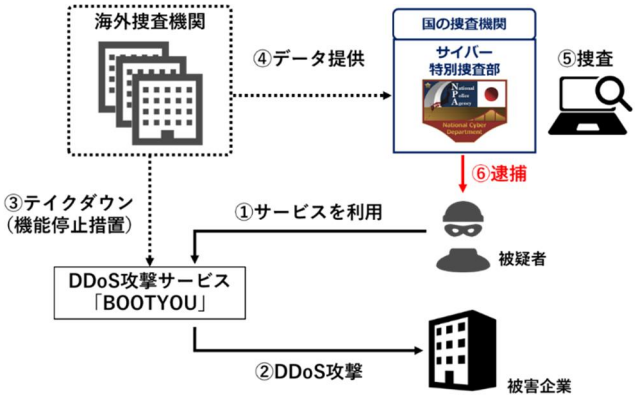
（第２部１「検挙に向けた取組」関連）

サイバー警察局設置後における国際共同捜査の主な事案一覧③

● 海外の DDoS 攻撃ウェブサービスを利用した国内の DDoS 攻撃事案

海外の DDoS 攻撃ウェブサービスを利用した国内の DDoS 攻撃事案について、サイバー特別捜査部が外国捜査機関から提供を受けた情報を精査した結果、被疑者を特定・逮捕した（令和６年８月）。本件は、EUROPOL 主導の国際共同捜査「オペレーション Power OFF（パワーオフ）」への参画が国内被疑者の検挙に結びついた初の事例である。

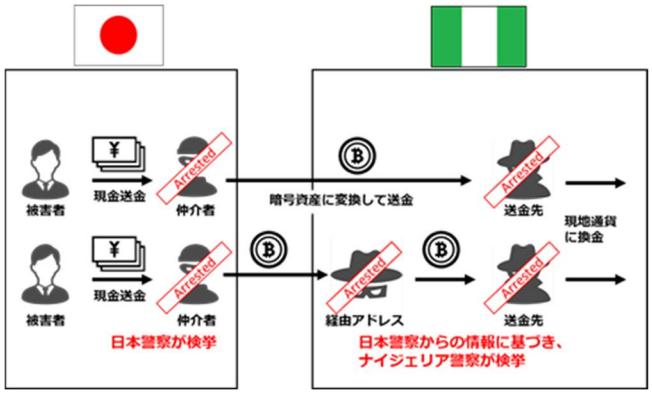
また、令和６年 12 月には、本国際共同捜査の一環として実施された広報啓発キャンペーンに参画した。



● ナイジェリアとの国際共同捜査

西アフリカにおける組織的な金融犯罪に対し、INTERPOL が主導する国際共同捜査「オペレーション Jackal（ジャッカル）」が進められており、日本警察も令和６年４月から同共同捜査に参画していた。

サイバー特別捜査部は、我が国で発生した SNS 型投資・ロマンス詐欺事案について、関係都道府県警察の捜査情報を横断的に分析し、また、暗号資産追跡を実施した結果、複数の事案の被害金がナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止めたことから、同情報をナイジェリア警察に提供したところ、同警察において同国内の被疑者の検挙が行われた。また、関係都道府県警察において、日本国内の仲介者も検挙している。

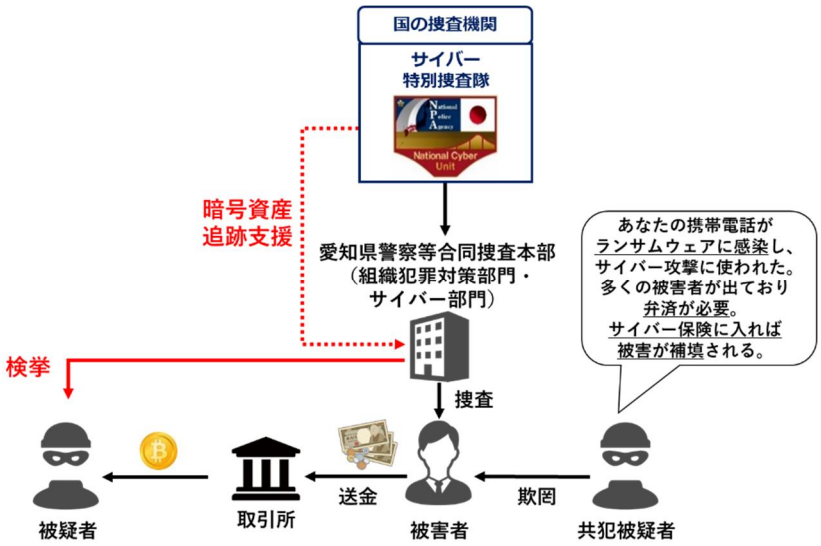


（第２部１「検挙に向けた取組」関連）

サイバー特別捜査部等合同捜査本部による国内における主な捜査事例

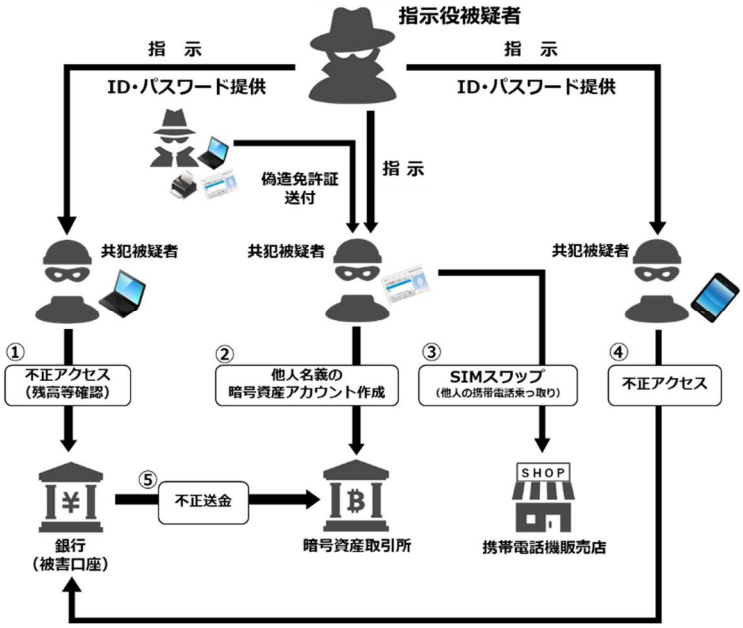
● サイバー保険名目の架空料金請求詐欺事件

国内におけるサイバー保険を名目とした架空料金請求詐欺事件に係る捜査においては、サイバー特別捜査隊（当時）による暗号資産追跡と、その結果の事案横断的な分析により、従来明らかになっていなかった事案相互の関連性が明らかになった。令和５年５月、愛知県警察が被疑者を逮捕した。



● インターネットバンキングに係る不正送金事件

令和４年から５年にかけて発生したインターネットバンキングに係る不正送金事件について、関係都道府県警察による捜査を通じて得られた情報をサイバー特別捜査部が集約・分析するとともに、暗号資産の追跡捜査や関係被疑者の SNS アカウントに係る捜査を実施した。その結果、サイバー特別捜査部等の合同捜査本部は、同一の犯行グループが、SIM スワップという手口を駆使しながら組織的に不正送金を敢行している実態を解明するとともに、犯行グループの指示役とみられる男を特定し、令和６年７月、同男を逮捕した。



（第２部１「検挙に向けた取組」関連）

サイバー特別捜査部等合同捜査本部による国内における主な捜査事例②

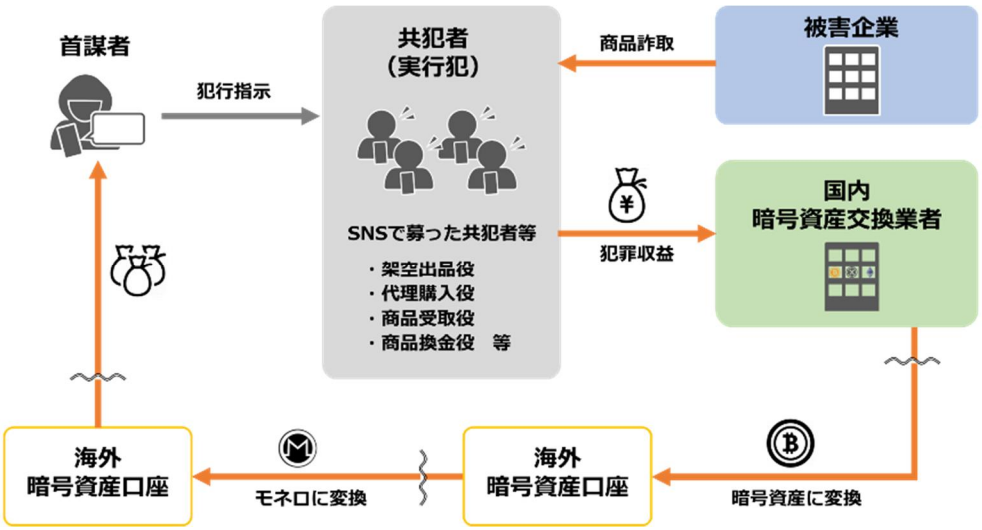
● クレジットカード不正利用事案の首謀者検挙

令和３年から４年にかけ、オンラインのフリーマーケットサービス等で、「他人のクレジットカード情報で商品を購入して商品を転売する」などの手口によるクレジットカード不正利用事件が発生した。同事件において、首謀者はSNS上で募集した実行者を使用して犯罪を敢行し、実行犯の検挙後も、手口や共犯者を変えて犯行を継続していた。さらに、犯罪収益を、取引履歴の追跡が極めて困難となるように設計された、匿名性の高い暗号資産「モネロ」に換えて資金洗浄を行っていた。

サイバー特別捜査部では、関係都道府県警察での実行犯検挙等の捜査を通じて得られた情報の分析や、モネロに変換された後の犯罪収益の流れの解明により、犯行グループの実態を解明するとともに、首謀者を特定した。

令和６年 10 月、サイバー特別捜査部及び９府県警察（埼玉、青森、宮城、滋賀、京都、福岡、佐賀、長崎、熊本）の合同捜査本部は、犯行グループの首謀者とみられる男（26 歳）を電子計算機使用詐欺罪で逮捕した。

本件は、匿名性が高く追跡が困難とされていたモネロの分析に成功し被疑者を検挙した初めての事案となった。



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

国家安全保障戦略（令和４年 12 月 16 日）（抄）

【サイバー安全保障分野での対応能力の向上】

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。(略)

その上で、武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

（ア） 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

（イ） 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

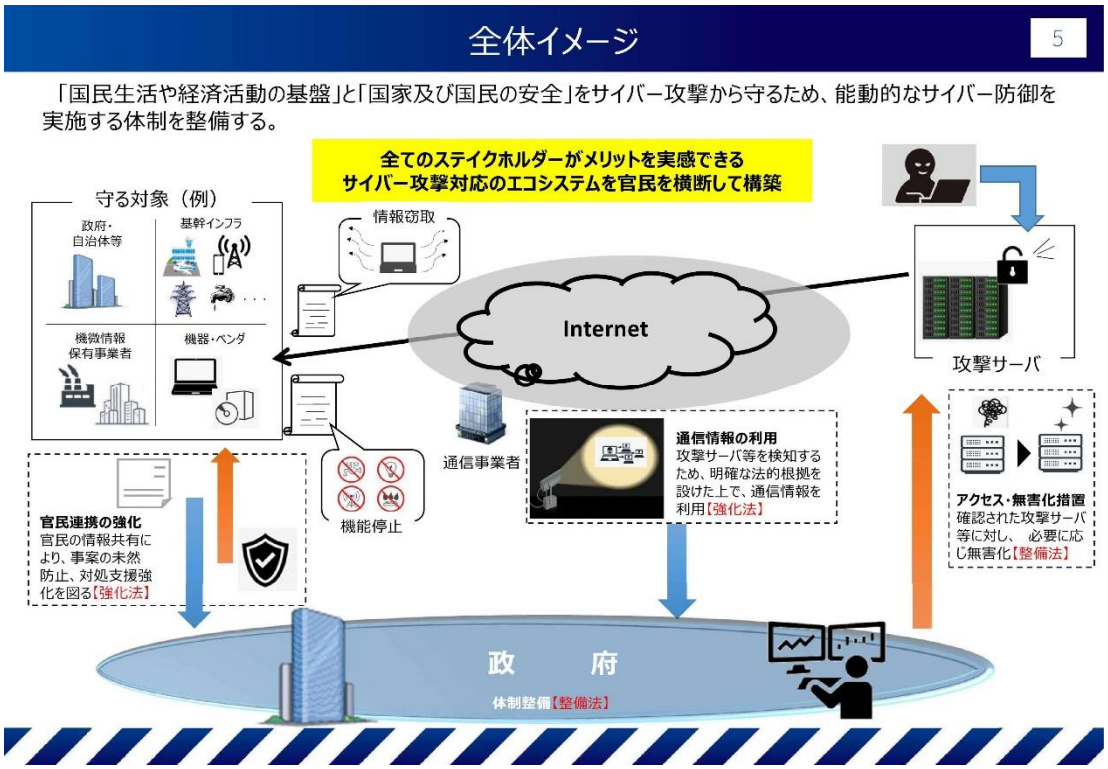
（ウ） 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

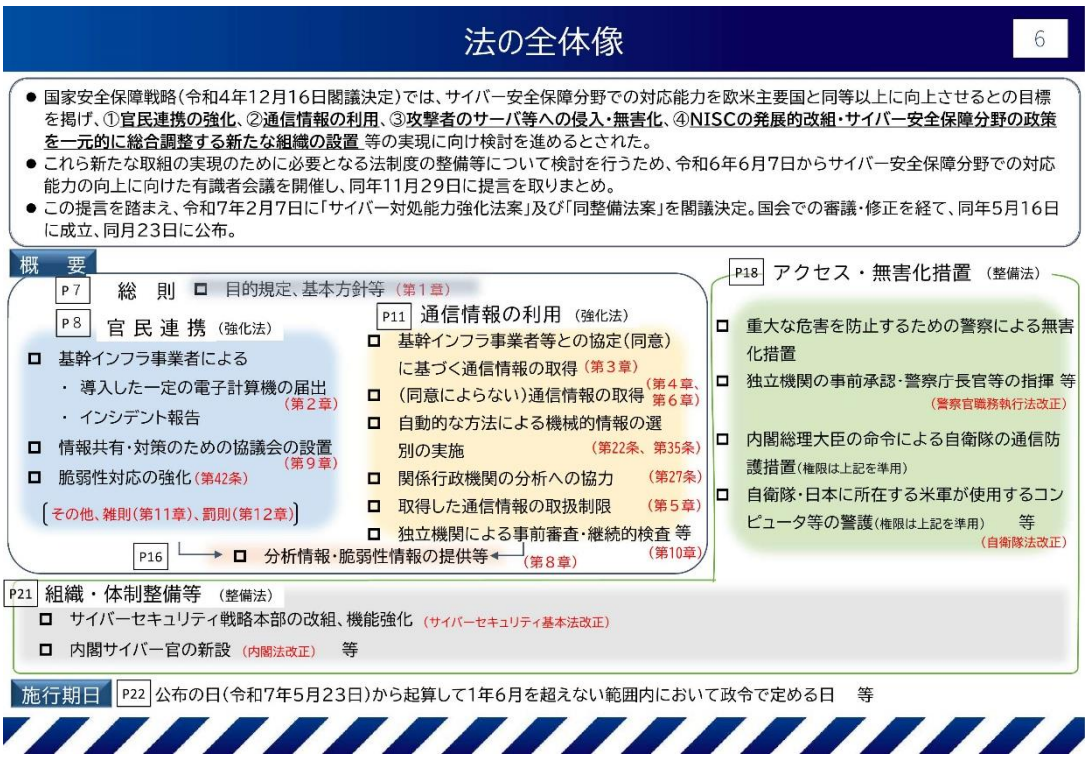
能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。

資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー対処能力強化法及び同整備法





※　出典：内閣官房

資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

パブリック・アトリビューションの事例一覧

事例	年月日	概要
【北朝鮮】米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）	H29.12.20	米国の声明を受け、日本においても、マルウェア「ワナクライ」を用いたサイバー攻撃の背後に北朝鮮の関与があったとして非難。
【中国】中国を拠点とする APT10 といわれるグループによるサイバー攻撃について（外務報道官談話）	H30.12.21	英国及び米国等の声明を受け、日本においても、中国を拠点とする APT10 といわれるサイバー攻撃グループによる国内の民間企業や学術機関等を対象としたサイバー攻撃が確認されているとして非難。
【中国】人民解放軍を背景に持つ Tick と呼ばれる攻撃グループによるサイバー攻撃について（国家公安委員会委員長記者会見）	R3.4.22	JAXA 等に対する一連のサイバー攻撃が Tick と呼ばれるサイバー攻撃グループによって実行され、また、Tick の背景に中国人民解放軍第 61419 部隊が関与している可能性が高いと結論付け、公表。
【中国】中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃について（外務報道官談話）	R3.7.19	英国及び米国等の声明等を受け、日本においても、APT40 といわれるサイバー攻撃グループが中国政府を背景に持つ可能性が高いと評価するとともに、国内企業が同グループからの攻撃の標的となっているとして非難。
【北朝鮮】北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）	R4.10.14	日本国内の暗号資産関連事業者等が北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況を踏まえ、警察庁、金融庁及び NISC が連名で注意喚起を実施。主に、虚偽の SNS アカウントを用いて標的企業の社員に接近するなどのソーシャルエンジニアリングの手口を確認。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

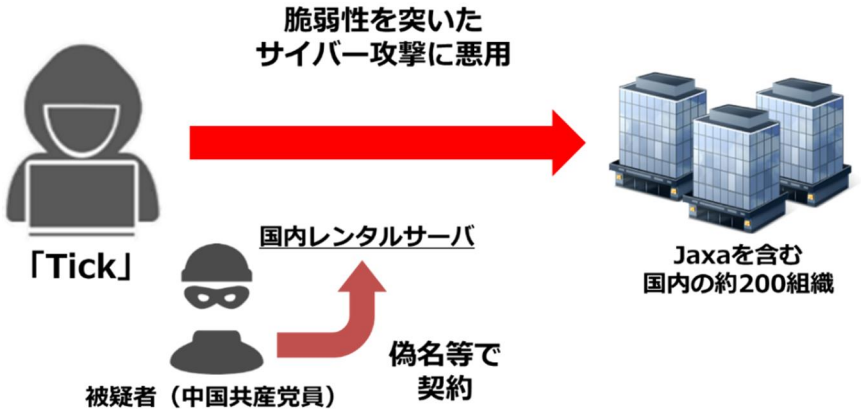
パブリック・アトリビューションの事例一覧②

【中国】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）	R5.9.27	中国を背景とするサイバー攻撃グループ「BlackTech」が、平成 22 年（2010 年）頃から日本を含む東アジアと米国の政府機関等を標的とする情報窃取を目的としたサイバー攻撃がを行っているとして、警察庁、NISC 及び米国関係機関が連名で注意喚起を実施。主に、ネットワークの脆弱性や設定の不備を突いて侵入する手口や、海外子会社を足がかりに同企業内のルーター等を通じて、親会社に侵入するなどの手口を確認。
【中国】豪州主導の APT40 グループに関する国際アドバイザリーへの共同署名について	R6.7.9	警察庁及び NISC が、米国、英国、カナダ、ニュージーランド、ドイツ及び韓国の関係機関とともに、豪州通信電子局豪州サイバーセキュリティセンターが作成した APT40 に関する国際アドバイザリーの共同署名に参加。
【北朝鮮】北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について	R6.12.24	警察庁及び FBI 等が、令和６年５月に北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が日本国内の暗号資産関連事業者から暗号資産を窃取したと評価し、合同で文書を公表。併せて、警察庁、NISC 及び金融庁が連名で注意喚起を実施。
【中国】中国を背景とするサイバー攻撃グループ Salt Typhoon に関する国際アドバイザリーへの共同署名について	R7.8.27	警察庁及び NCO が、米国、オーストラリア、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、及びスペインの関係機関とともに、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に参加。

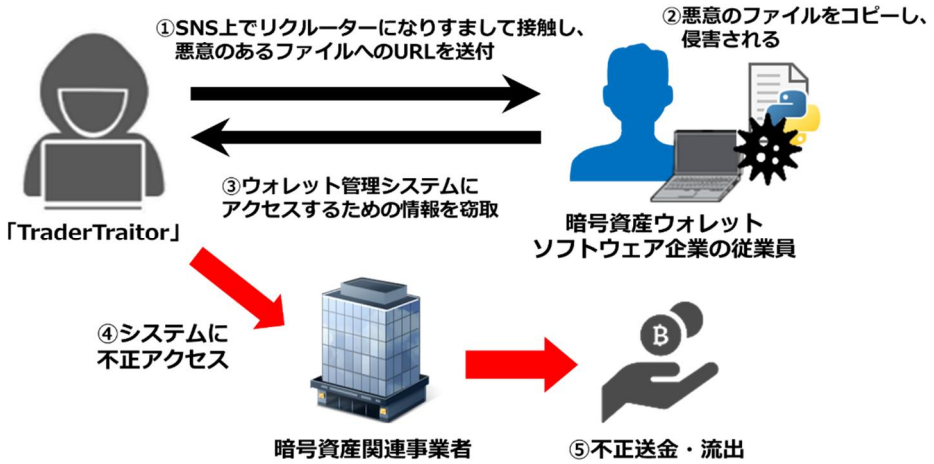
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

パブリック・アトリビューションの事例【主な手口】

● 令和３年４月、Jaxa 等に対する一連のサイバー攻撃が Tick と呼ばれるサイバー攻撃グループによって実行され、Tick の背景に中国人民解放軍第 61419 部隊が関与している可能性が高いと結論付け、公表した。平成 28 年頃から、Tick と呼ばれる攻撃グループが、Jaxa を含む約 200 の国内企業等に対し、脆弱性を突いたサイバー攻撃を実行しており、一連のサイバー攻撃の中には、中国共産党員の男が氏名等を偽って契約した日本のレンタルサーバが利用されていたことが判明している。



● 令和６年５月、北朝鮮を背景とするサイバー攻撃グループ TraderTraitor が日本国内の暗号資産関連事業者から約 482 億円相当の暗号資産を窃取した。当該事案において、TraderTraitor は、SNS 上でリクルーターになりすまし、暗号資産ウォレット管理システムへのアクセス権を保有する従業員に接触し、悪意あるファイルの URL を送付することで管理システムへのアクセスに必要な情報を窃取した後、従業員になりすまして、当該システムに不正にアクセスし、同管理システムを利用していた暗号資産交換業者の暗号資産を窃取したことが判明している。



サイバー警察局設置後のサイバー攻撃に対する主な注意喚起

●　学術関係者・シンクタンク研究員等を標的としたサイバー攻撃に関する注意喚起

令和４年 11 月、警察庁は、日本国内の学術関係者、シンクタンク研究員等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラムを実行させ、当該人物のメールやコンピュータ内のファイルの内容を盗み見るサイバー攻撃を多数確認したところ、情報窃取被害の発生が深く懸念されることを鑑み、NISC と連名で注意喚起を実施した。

●　家庭用ルーターの不正利用に関する注意喚起

令和５年３月、警察庁及び警視庁は、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、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を実施した。

●　DDoS 攻撃に関する注意喚起

令和５年５月、警察庁は、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。

●　サイバー特別捜査隊をかたる不審メールに関する注意喚起

令和５年６月、警察庁は、関東管区警察局サイバー特別捜査隊をかたる不審メールを確認したことから、その内容やメールが届いた場合の対処要領等について注意喚起を実施した。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー警察局設置後のサイバー攻撃に対する主な注意喚起②

● 豪州主導国際文書「OT サイバーセキュリティの原則」への共同署名

令和６年 10 月、警察庁は、NISC のほか、米国、英国、カナダ、ニュージーランド、ドイツ、オランダ及び韓国の関係機関と共に、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）が策定した文書「OT サイバーセキュリティの原則」（Principles of operational technology cyber security ）の共同署名に加わり、重要インフラ事業者がオペレーショナル・テクノロジー（OT）環境の設計、実装及び管理に係る意思決定を行うことを支援する６つの原則を示した文書を公表した。

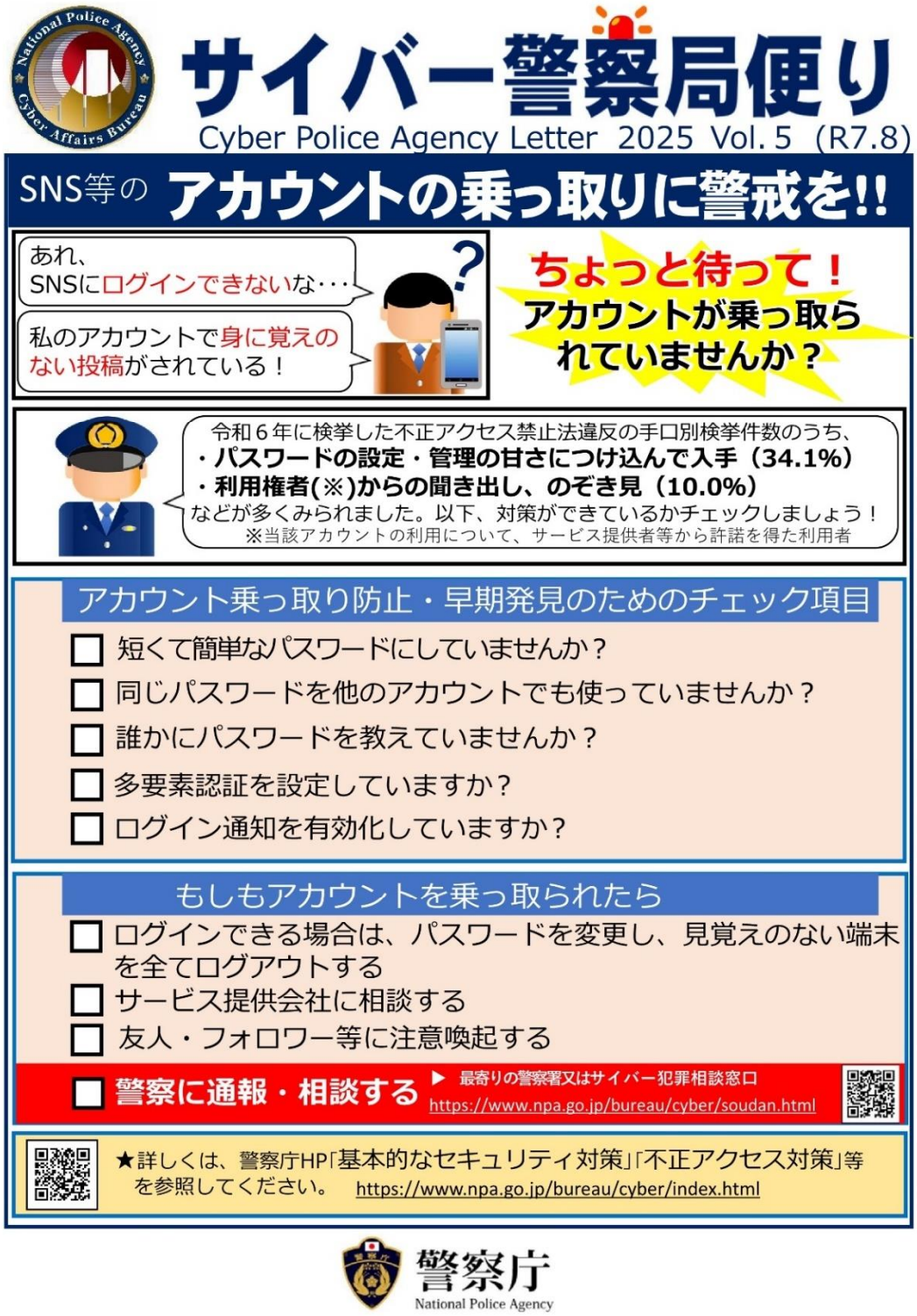
● MirrorFace によるサイバー攻撃に関する注意喚起

令和７年１月、警察庁は、関東管区警察局サイバー特別捜査部及び警視庁ほか道府県警察による捜査等の結果を踏まえ、NISC とともに、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から日本国内の組織、事業者及び個人に対して、情報窃取を目的としたサイバー攻撃を行っており、さらに、これらサイバー攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動であると評価し、同グループの背景や手口、未然防止対策等に関する注意喚起を実施した。なお、主な手口として、第三者になりすまし、マルウェアを添付したメールやマルウェアをダウンロードさせるリンクを記載したメールを送信して感染させる標的型メール攻撃、ネットワーク機器（特に VPN 機器等）の脆弱性を悪用して侵入する攻撃等が確認されている。

資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

SNS 等のアカウントの乗っ取り被害防止及び被害時の措置



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー攻撃のリスクを考慮した管理体制の構築

サイバー警察局便り

Cyber Police Agency Letter　2025 Vol.4 (R7.7)

中小企業で被害多数 ランサムウェア

サイバー攻撃のリスクを考慮した管理体制の構築を！

- 中小企業のランサムウェア被害は前年比で約4割の増加

- 被害未然防止の要は基本的対策の継続
  - ＶＰＮ機器等のソフトウェア更新
  - パスワードの強度確保　等

- 被害拡大防止のために必要な備え
  - サイバー攻撃を想定したＢＣＰの策定
  - オフラインを含むバックアップの取得
  - 被害調査に必要不可欠なログの取得

- 被害発生時は警察へ通報・相談を

※政府広報オンライン「中小企業で被害多数 ランサムウェア」より

詳しくは、政府広報オンライン動画「中小企業で被害多数 ランサムウェア」

警察庁制作協力

https://www.gov-online.go.jp/useful/202506/video-298784.html

動画「ランサムウェア対策の基本」
https://www.gov-online.go.jp/vertical/online/video-478.html

記事「ランサムウェア、あなたの会社も標的に?被害を防ぐためにやるべきこと」
https://www.gov-online.go.jp/useful/article/202210/2.html

政府広報 SNSでも関連動画を公開中

X

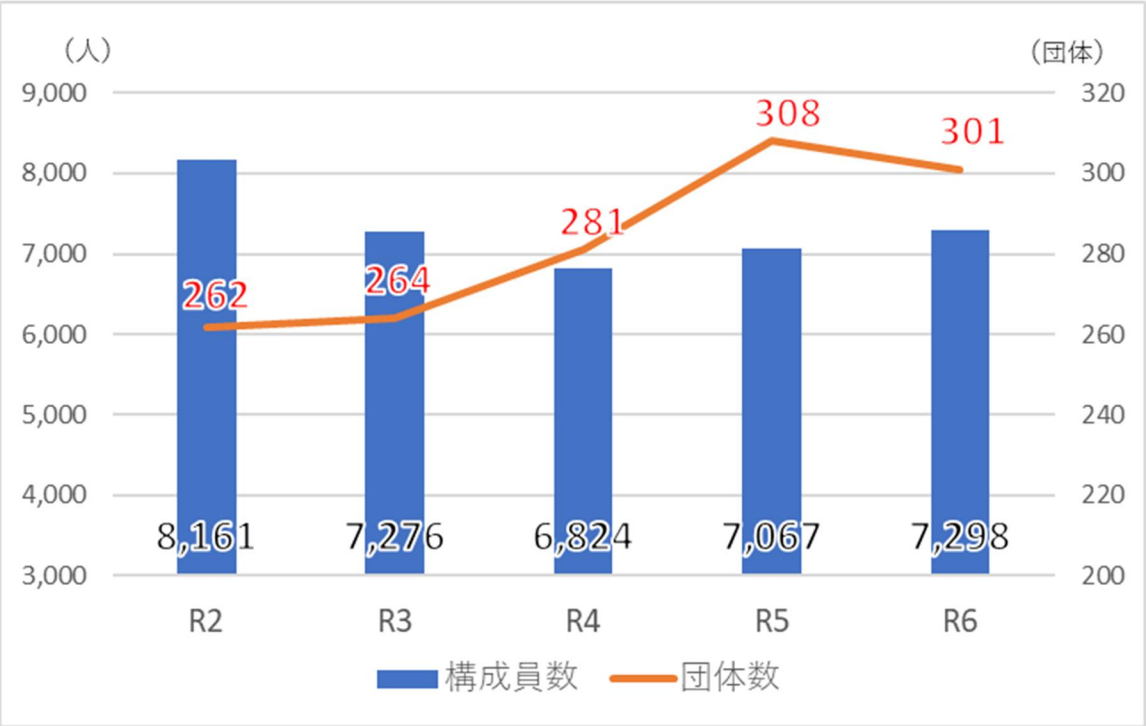
Instagram

警察庁
National Police Agency

資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー防犯ボランティア団体数及び構成員数の推移



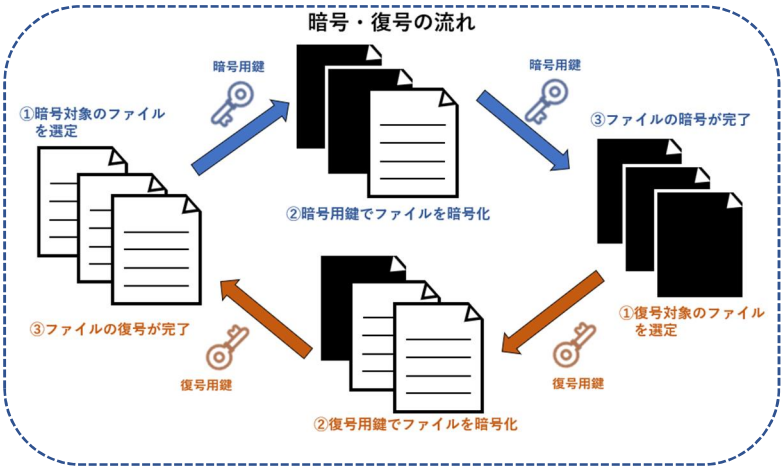
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

ランサムウェアの暗号化の仕組み及び復号ツールの作成

● 暗号・復号の仕組み

暗号時は、暗号対象のファイルを選定した上で、「暗号用鍵」を使って対象ファイルを暗号化し、元のファイルは削除又は上書き。

復号時は、「復号用鍵」を使って対象ファイルを復号する。

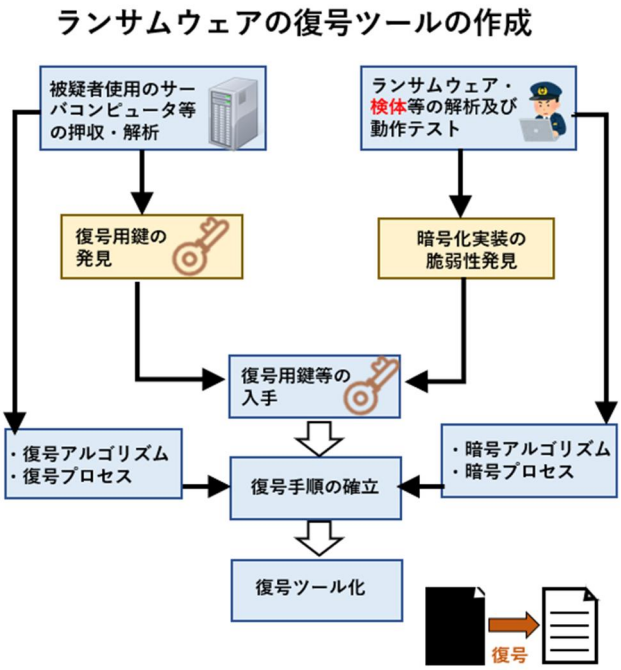


● 復号ツールの作成

ランサムウェア検体の解析等により、暗号に使用されたアルゴリズム（手順等）、暗号プロセス等を把握。

暗号に使用されたアルゴリズム又は暗号プロセスに脆弱性があれば、それらを利用して復号用鍵を生成。また、被疑者使用のサーバコンピュータ等の解析により、復号に使用されたアルゴリズム、復号プロセス等を把握するとともに、復号用鍵を発見。

これらの暗号・復号の把握事項と、復号用鍵を利用して復号ツールを作成。



資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

被害防止に関する警察の取組

● 政府における AI 戦略に係る検討への参画

人工知能関連技術の研究開発及び活用の推進に向けて、政府においては令和６年１月に決定・公表された有識者会議の中間とりまとめを踏まえ、令和７年５月、人工知能関連技術の研究開発及び活用の推進に関する法律（AI 法）が成立した。警察庁としては、総合的な施策を検討・推進するため開催している AI 戦略推進関係省庁会議等を通じて、AI 法に基づく検討に参画している。

● AI セーフティ・インスティテュートへの参画

令和６年２月に設置された AI セーフティ・インスティテュート（AISI）について、警察庁は、AISI 関係府省庁等連絡会議等において、AI の安全性評価に関する基準や手法の検討に係る議論に参画している。

● 通報・相談しやすい環境の整備

通報・相談に係る負担軽減の観点から、警察庁のウェブサイトにおいて、都道府県警察に対するサイバー事案に関する通報・相談・情報提供の統一窓口を設置し、令和６年３月から運用を開始した。また、同年５月、一般社団法人日本損害保険協会長とサイバー警察局長が対談し、同協会の会員企業等に対してランサムウェア被害に遭った場合の警察への通報・相談の重要性を訴求するよう依頼した。

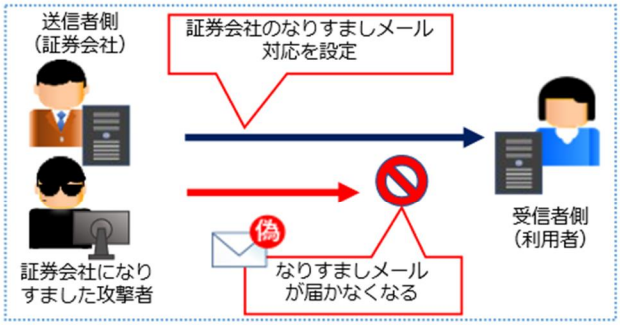
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

日本証券業協会等に対する要請

証券会社をかたるフィッシングメールや、証券口座への不正アクセス・不正取引が急増していることから、令和７年７月、金融庁と警察庁は局長等連名で日本証券業協会を含む金融関係協会に対して①送信ドメイン認証技術（DMARC）の普及促進、②フィッシングサイトの閉鎖活動、③パスキーの導入促進について要請を実施した。

① 送信ドメイン認証技術(DMARC※)の普及促進

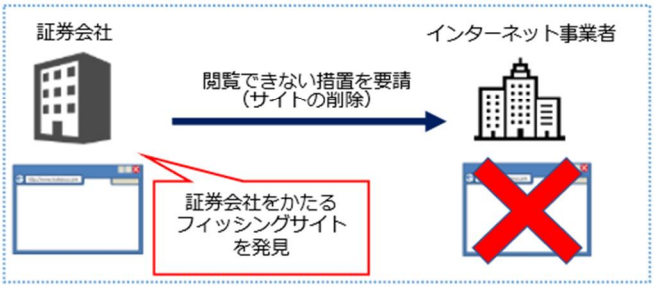
※ Domain-based Message Authentication Reporting and Conformance



・利用者に送信されたメールが、正規の送信元（証券会社）からのメールであるかどうかを検証する仕組み

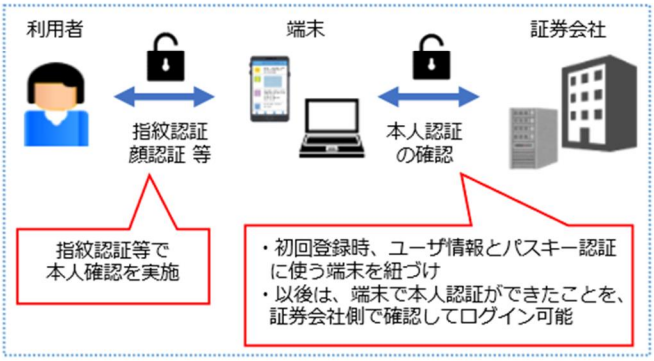
・証券会社のメールアドレスを騙ったメールが利用者に届かないよう、証券会社において、利用者に受信させない／迷惑メールフォルダに入れる、といった設定を行うことが可能

② フィッシングサイトの閉鎖活動



・証券会社のフィッシングサイトを、利用者が閲覧できないようにするため、インターネット事業者に対して、フィッシングサイトの閉鎖（削除）を要請するもの

③ パスキーの導入促進



・証券会社のアプリ等において、簡単で安全な認証方式である「パスキー」を利用できるようにするもの

・端末(スマホ)そのものが認証に必要な鍵となり、端末のロック解除と同様の本人認証により、アプリへのログインを可能とする

・ネット上に、パスワードを送信しないため、パスワードが窃取されない

資料編

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

国民を詐欺から守るための総合対策 2.0

「国民を詐欺から守るための総合対策2.0」における主な施策

1 SNS型投資・ロマンス詐欺対策 ／ 2 特殊詐欺対策

（1） 犯行準備段階への対策

○ 携帯電話不正利用防止法上、契約時における本人確認が義務付けられていないデータ通信専用SIMについて、悪用実態を踏まえ、電気通信事業者に対して契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討。

○ 犯罪実行者募集情報の削除等の取組を促進するほか、犯罪グループの人的基盤となり得る非行集団等からの少年の離脱に向けた取組等犯罪への加担を防止するための取組を推進。

（2） 着手段階への対策

○ 詐欺に誘引するダイレクトメッセージ等が被害者等の端末に届く前にフィルターする取組や利用者が詐欺に誘因するダイレクトメッセージ等を受信した際に警告表示を行う取組を推進。

○ 契約変更等の機会も活用しながら、国際電話サービスを利用しない設定があることを一層強く国民に周知。また、将来的には、国際電話サービスを利用しない者に対する優遇措置等、国際電話を必要としない人への利用休止を促すような効果的な対策の導入を検討。

○ 迷惑電話、迷惑SMS等の受信を防止又は受信した際の警告を行う有料のサービスについて、事業者に対し、無償化を含めた効果的な措置を要請するとともに、被害防止機能向上のためより効果的な方策を検討し、その普及や有効性の向上を図る。

○ 発信者番号の表示が官公庁等の電話番号に偽装されている手口について、国民に注意喚起を実施するとともに、関係事業者と連携して効果的な対策を検討し、速やかに実施。

（3） 欺罔段階への対策

○ 変化する欺罔の手口について、迅速・的確にその特徴や被害者層、具体的に講じるべき対策等を明らかにした上で、訴求対象・訴求内容と合致する広報啓発の手段を選定するなど、効果的な広報啓発を実施。

（4） 金銭等の交付段階への対策

○ インターネットバンキングの初期利用限度額の適切な設定、インターネットバンキングの申込みがあった際や利用限度額引上げ時の利用者への確認や注意喚起等の取組を推進。

○ 預金取扱金融機関や暗号資産交換業者によるモニタリングの強化や、暗号資産交換業者への不正送金防止に係る取組を推進。

○ 預金取扱金融機関間において不正利用口座に係る情報を共有しつつ、速やかに口座凍結を行うことが可能となる枠組みの創設について検討。預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組を推進。

○ 犯罪者グループの上位被疑者の検挙、犯罪収益の剥奪等を図るとともに、口座の悪用を牽制するため、捜査機関等が管理する架空名義口座を利用した新たな捜査手法や関係法令の改正を早急に検討。

（5） 犯行後の捜査段階における対策

○ 匿名性の高い通信アプリをはじめとする犯罪に悪用される通信アプリ等について、被疑者間の通信内容や登録者情報等を迅速に把握するために効果的と考えられる手法について、諸外国における取組を参考にしつつ、技術的アプローチや新たな法制度導入の可能性も含めて検討。

○ 通信履歴の保存の在り方について、電気通信事業における個人情報等保護に関するガイドライン改正や保存義務付けを含め検討。

○ 仮装身分捜査を、令和７年１月に制定した実施要領に基づき適正に実施し、詐欺や強盗等の犯人の検挙、被害の抑止を推進。

3 ID・パスワード等の窃取・不正利用対策

（1） フィッシングサイトへの対策

○ フィッシングサイト判定の高度化・効率化のために生成AIを活用し、閲覧防止措置や警告表示による対策の効率化を図るなど、フィッシングサイトへの対策を推進。

（2）・(3) ID・パスワードやクレジットカード情報の不正入手・利用対策

○ 悪用のおそれのあるクレジットカード情報を国際ブランド各社に提供する枠組みを活用するほか、ECサイトの脆弱性を悪用したクレジットカード情報窃取対策の実施について、カード会社がEC事業者に対して適切に指導を行うよう監督。

○ なりすましメールの対象となる事業者に対し、関係省庁が連携し、メールのなりすまし防止技術（DMARC）の導入推進のため、必要に応じたフォローアップや受信拒否を要求するポリシーでの運用の働き掛けを実施。

（4） マネー・ローンダリングや現金化への対策 預金取扱金融機関等によるモニタリングの強化、EC加盟店等との情報連携等(1･2(4)等再掲)

（5） 犯行後の捜査段階における対策

○ インターネットバンキングに係る不正送金等の実行時に、一般家庭からのアクセスに偽装するための踏み台として家庭用インターネット通信機器が悪用されていることから、その実態を調査・分析し、悪用実態を踏まえた対策を実施。

4 治安基盤の強化等

○ 犯罪グループの首謀者等の検挙、警察・検察におけるサイバー人材の育成の更なる推進、警察庁・都道府県警察間の連携強化等のため、態勢の充実強化を推進。

○ スマートフォン端末等の解析能力の強化、捜査に必要な情報収集の効率化のため、警察・検察の装備資機材の充実強化を推進。

○ 外国機関と連携し、詐欺等対策や邦人保護の取組のほか、情報技術解析の高度化を推進。

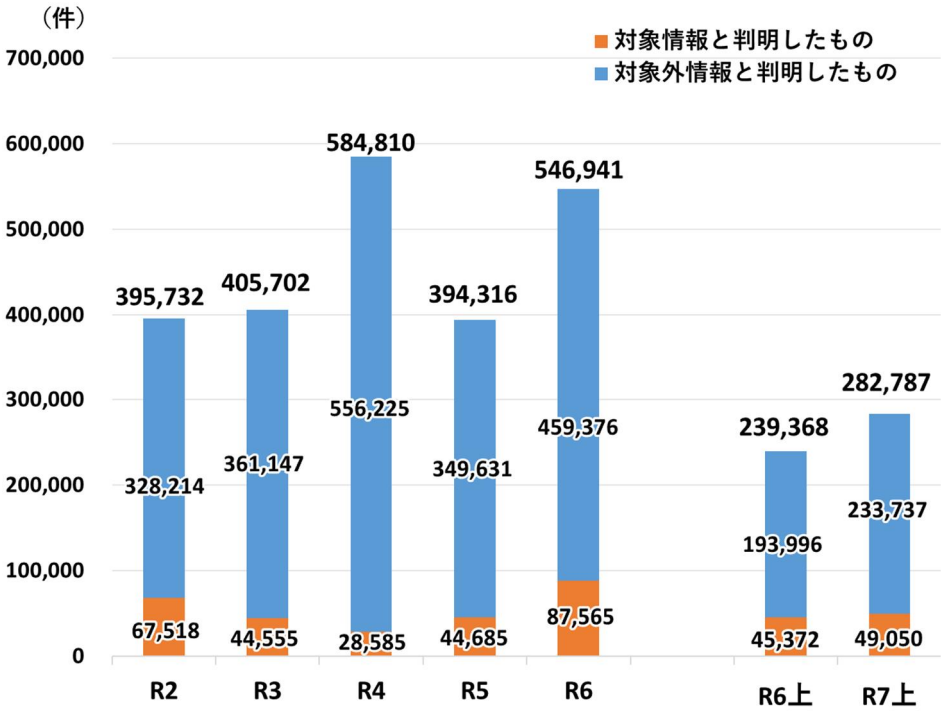
○ 地方創生の交付金を活用した防犯カメラの設置等地域防犯力の強化に資する取組への支援を行うなど、防犯対策の強化を推進。

○ 詐欺等のほか、組織的な窃盗や強盗、違法・悪質なホストクラブ営業やスカウト行為、薬物密売、オンラインカジノ等多岐にわたる資金獲得活動に着目した取締り等を推進し、匿名・流動型犯罪グループの資金源への対策を推進。

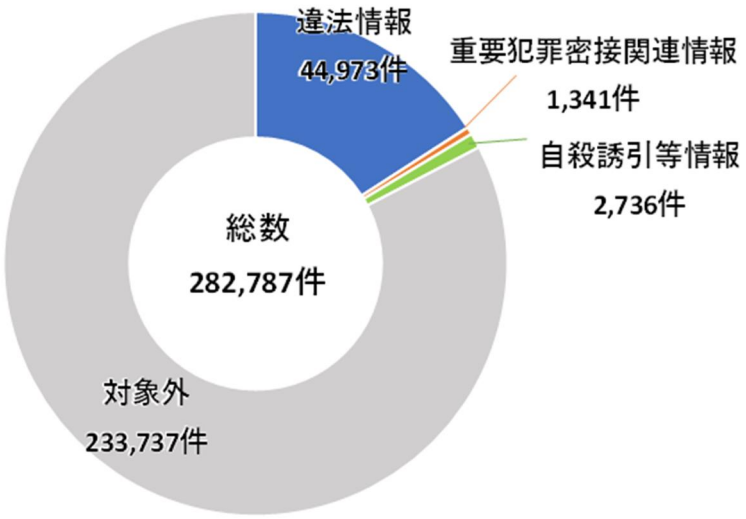
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報の分析に関する統計

１　違法情報等の分析件数[8]の推移



２　分析結果の内訳



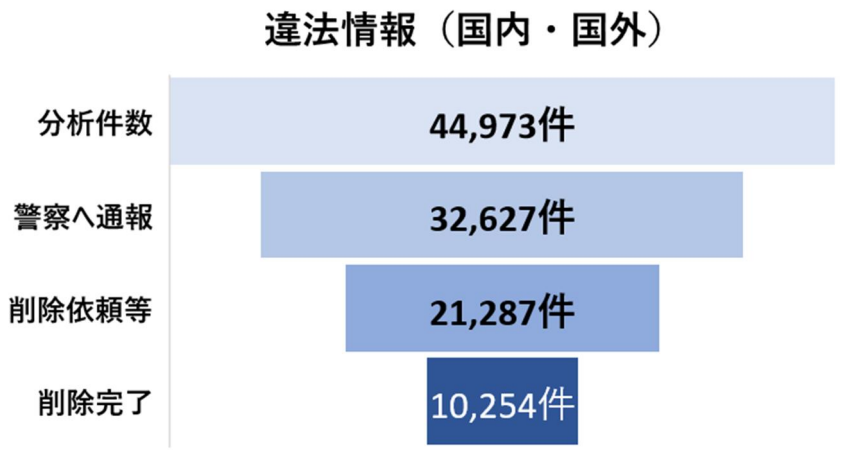
・違法情報
インターネット上の流通自体が法令に違反する情報（「わいせつ電磁的記録記録媒体陳列」など）
・重要犯罪密接関連情報
個人の生命・身体に危害を加えるおそれが高い重要犯罪と密接に関連する殺人、強盗などを直接的かつ明示的に誘引等する情報など

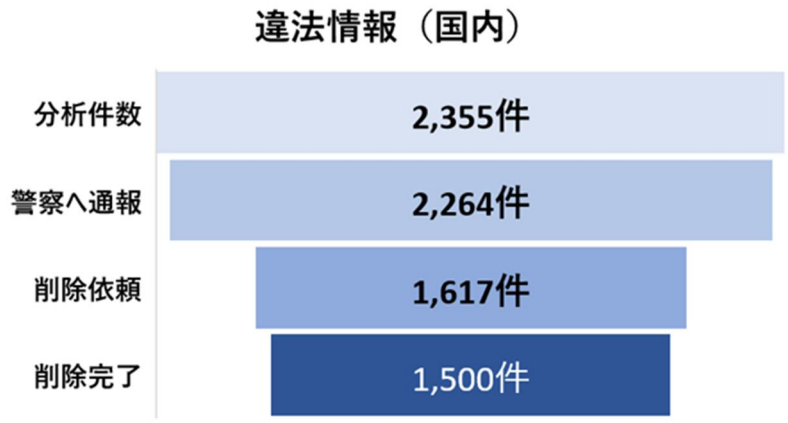
[8] インターネット・ホットラインセンター（IHC）への通報について、運用ガイドラインに基づいて分析対象とされた件数。１件の通報に複数の類型が含まれる場合、重複してカウントされるため、通報件数よりも多くなる。

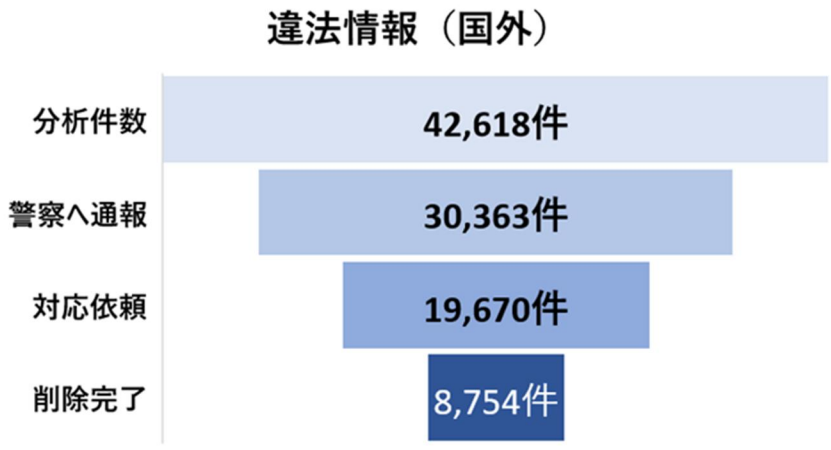
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報の分析に関する統計②

３　分析結果件数[9]と処理結果



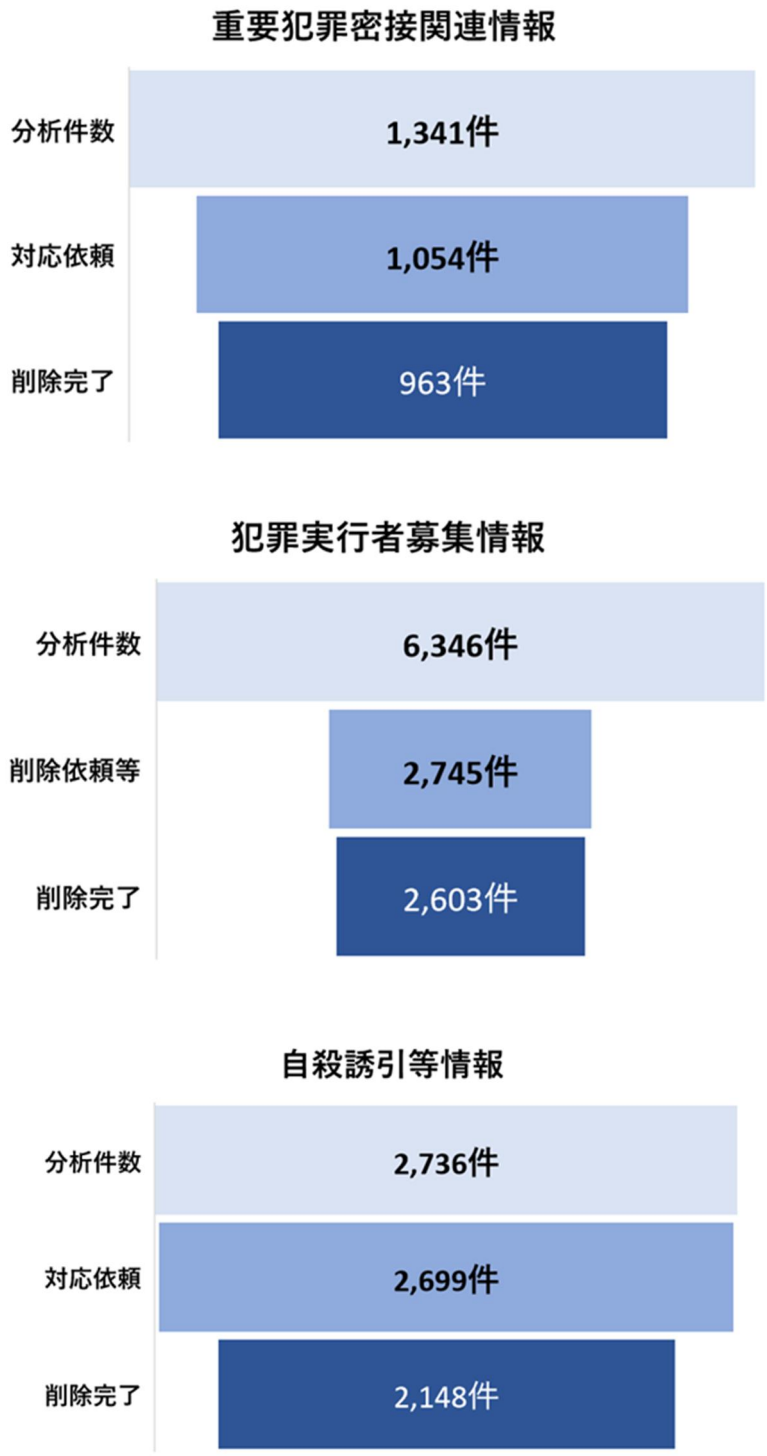




[9] IHC への通報について、運用ガイドラインに基づいて分析した結果、違法情報、重要犯罪密接関連情報、自殺誘引等情報、犯罪実行者募集情報として分類された件数。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報の分析に関する統計③



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

ＩＨＣ運用ガイドラインの改定

令和７年３月１日からＩＨＣでは

犯罪実行者募集情報を

いわゆる闇バイト投稿「違法情報」として通報を受け付けます。

※　ＩＨＣ：インターネット・ホットラインセンター（Internet Hotline Center）

ＩＨＣの運用ガイドラインを改定しました！

⚠ 次のような投稿は、違法情報（職業安定法違反等）として、ＩＨＣへの通報対象となります。

犯罪実行者募集情報

▶ 公衆衛生又は公衆道徳上有害な業務に就かせる目的での労働者の募集

「闇バイト」「ホワイト案件」「叩き」「受け子」「出し子」「運びの仕事」等の犯罪の実行者の募集を示唆する表現が記載された投稿

▶ 虚偽に当たる又は誤解を生じさせるような労働者募集の表示

募集者の氏名（名称）、住所、連絡先、業務内容、就業場所、賃金について記載のない求人の投稿

⚠ 今回の改定では、次の情報も違法情報として新たに通報対象に追加されました。

○ 無登録貸金業者による広告（いわゆる「ヤミ金」の広告）

○ 拳銃等又は人の生命、身体若しくは財産を害する目的での拳銃等以外の銃砲等の所持を、公然、あおり、又は唆す行為

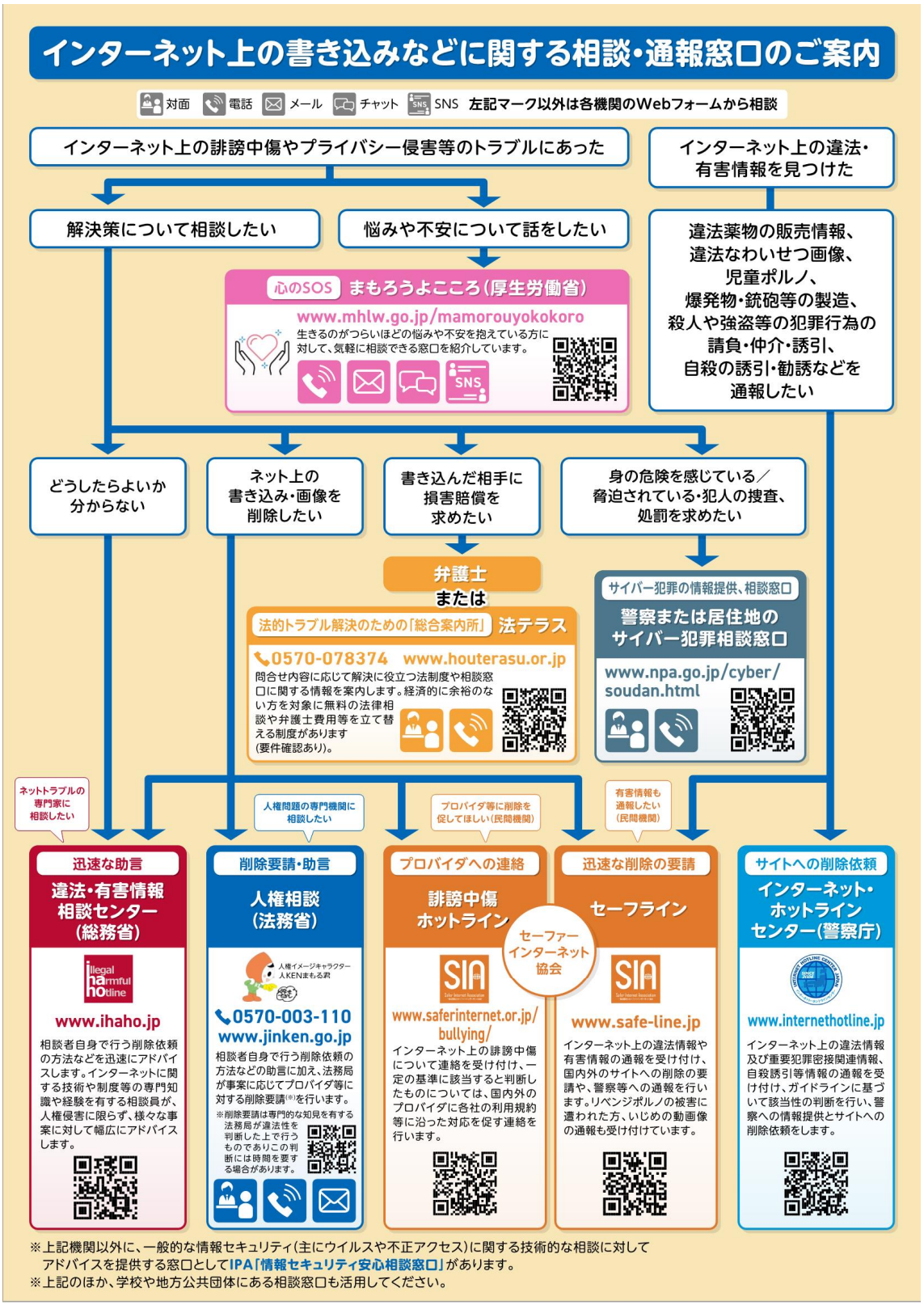
インターネット・ホットラインセンター INTERNET HOTLINE CENTER JAPAN
https://www.internethotline.jp

警察庁 National Police Agency

ひと、くらし、みらいのために 厚生労働省 Ministry of Health, Labour and Welfare

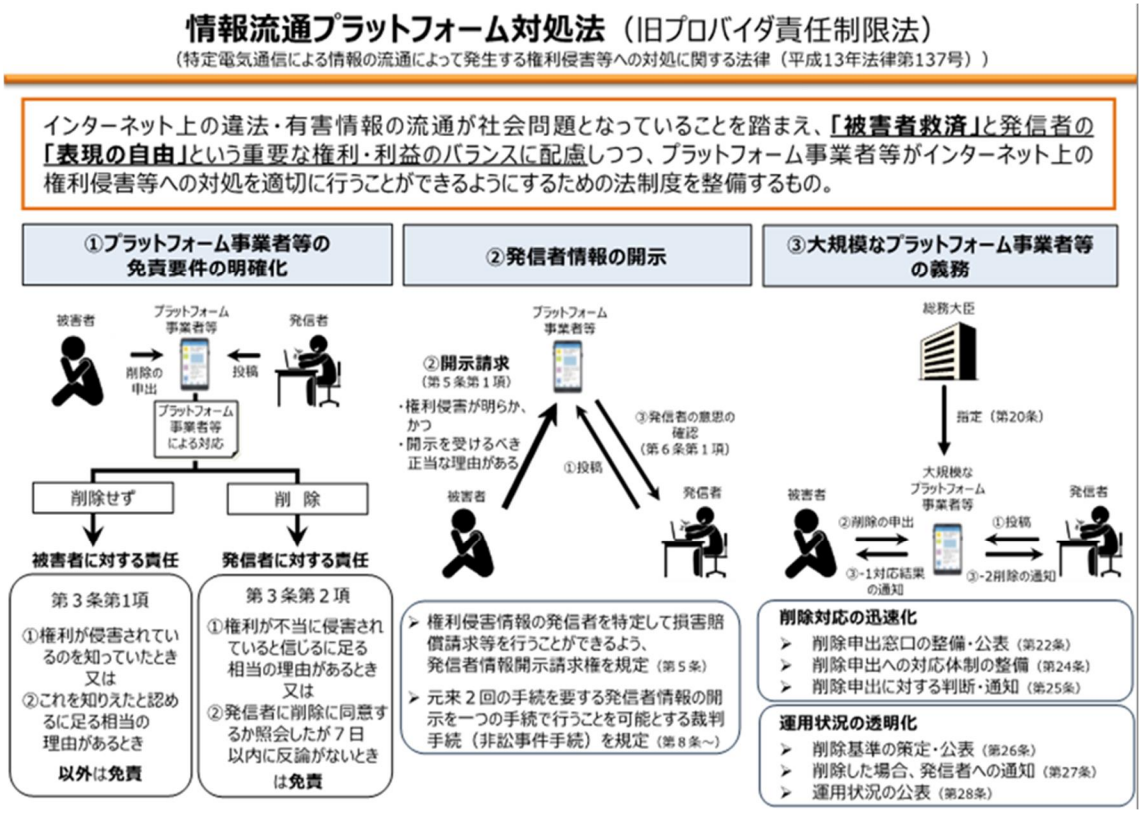
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報に関する関係機関との連携



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報に関する関係機関との連携②

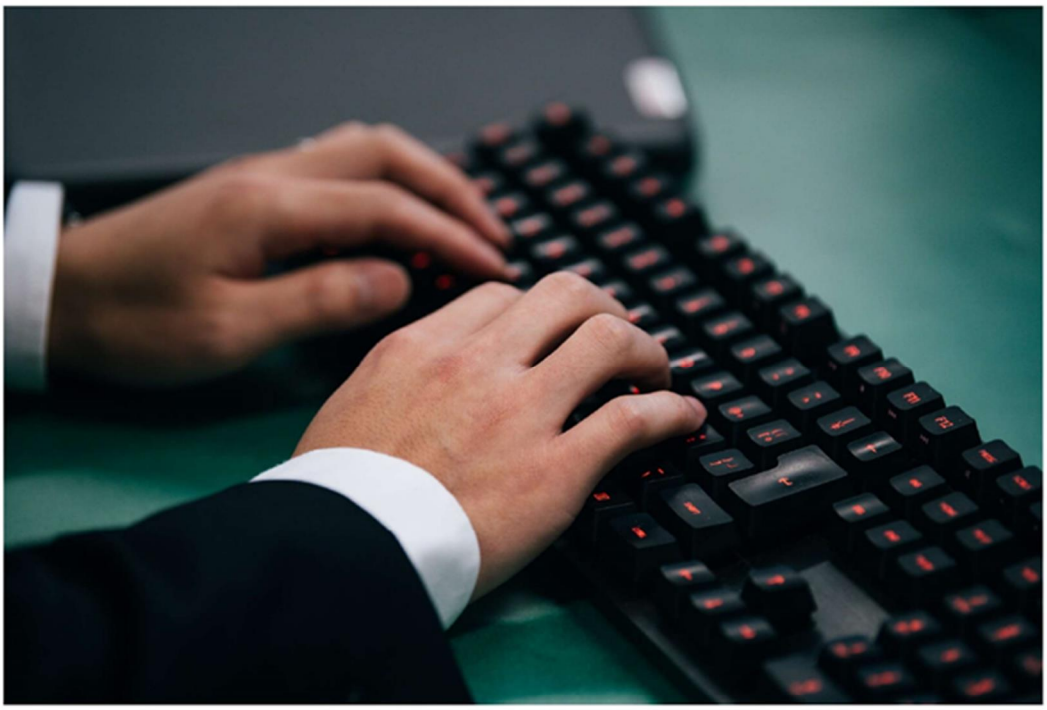


※　出典：総務省

（第２部３「基盤整備」関連）

サイバー人材確保・育成方針①

サイバー犯罪捜査官(都道府県警察)・技術職員(警察庁)募集



ランサムウェアによる被害が広範に及んでいるほか、国家を背景に持つサイバー攻撃集団によるサイバー攻撃も確認されているなど、サイバー空間をめぐる脅威は、極めて深刻な状況にあります。

警察では、サイバー空間の脅威に係る様々な課題に対応するため、サイバー事案について高度な知見を有する人材の確保・育成等に取り組んできたところですが、複雑化する治安課題に対処し続けるためには、このような取組を継続・強化していく必要があります。

そこで、警察では、

- 情報通信技術に関する民間企業での経験
- 情報通信技術に関する高度な知識や資格

サイバー警察局サイト

を有する方を、**サイバー犯罪捜査官(都道府県警察)・技術職員(警察庁)**として募集しています。

最前線で活躍する捜査官・技術職員として、最新の知識と技術を駆使し、社会の安全・安心を守る一員になりませんか？

（第２部３「基盤整備」関連）

サイバー人材確保・育成方針②

都道府県警察におけるサイバー人材確保・育成方針

- 現在の人口減少社会において、極めて深刻なサイバー空間情勢に対処するためのサイバー人材を確保・育成するためには、**警察内部の所属・部門間の縦割り等を排し、**サイバー部門と警務部門の緊密な連携を中核としつつ、**全ての部門が一体**となって、その**確保・育成**と**キャリアパス管理**を推進することが不可欠。
- 以上の基本的考え方を踏まえ、①全ての警察官に対するサイバーに関する教養を推進するなどの**全体の底上げ**と、②警察におけるサイバー人材のキャリアパスを明示しつつ外部にアウトリーチするなどの**高度人材の確保**という双方の観点から、都道府県警察が取り組むべき取組を指示。

サイバー人材の確保

1　試験制度の整備・運用
- ✓ 一般採用試験の前倒し・複数回実施
- ✓ 中途・特別・任期付採用制度の整備運用・リボルビングドアの取組

2　効果的な採用募集活動
- ✓ 高度人材に対するキャリアパス明示（サイバー特捜部出向等）と活躍実例の広報による魅力発信
- ✓ IT関連の広報媒体活用や高等専門学校等への学校訪問の推進
- ✓ 学生対象のサイバーコンテスト開催やサイバー防犯ボランティアの拡大

3　部内のサイバー人材の発掘
- ✓ 部内競技会の開催、経歴・資格の把握を通じた内部人材の発掘

サイバー人材の育成

1　必要な能力の明確化と検定による確認
- ✓ 全警察官に通報・相談受理能力、全捜査員にネットワーク利用犯罪捜査能力、中核サイバー捜査員に高度サイバー事案対処能力を取得させ、検定制度により確認
- ✓ 都道府県警察の昇任試験におけるサイバー関連の出題

2　教養・研修の推進
- ✓ 司令塔となる指導・教養班の設置
- ✓ 専務任用専科等の学校教養におけるサイバー教養の拡充
- ✓ 警視庁等他都道府県警察への派遣・出向、他部門捜査員のサイバー部門受入れによる職場教養の推進
- ✓ 民間研修への積極的派遣及び民間委託研修受講・民間資格取得を支援

サイバー人材のキャリアパス管理

1　サイバー・警務両部門の緊密な連携
- ✓ サイバー・警務両部門を中核に全部門一体となって、中途・特別採用等の高度サイバー人材を含むサイバー人材のキャリアパスを管理

2　キャリアパス管理に基づく職員の配置等
- ✓ 中途・特別採用のサイバー人材は本部への卒業配置に配慮。昇任配置も希望に応じて配置ポストを検討
- ✓ 署配置を行う場合は、能力と適性を活かすことができるポストを検討
- ✓ 高度人材を処遇するためサイバー部門に所要の幹部ポストを整備
- ✓ 高度サイバー人材を、情報通信部や警察庁サイバー特捜部・サイバー警察局に積極的に出向・派遣

上記方針に基づき本部長の指揮の下すべての都道府県警察が施策を推進

情報通信部門におけるサイバー人材確保・育成方針

- 現在の人口減少社会において、極めて深刻なサイバー空間情勢に対処するためのサイバー人材を確保・育成するためには、縦割り等を排し、**警察庁サイバー警察局と長官官房が緊密に連携しつつ、全国の情報通信部門が一体**となって、その**確保・育成**と**キャリアパス管理**を推進することが不可欠。
- 以上の基本的考え方を踏まえ、①全ての情報通信部門の職員に対する情報技術解析に関する教養を推進するとともに、②解析と捜査のいずれをも実施可能な**ハイブリッド人材**と**技術特化型トップレベルの人材**のそれぞれの育成とキャリアパス管理を推進。

サイバー人材の確保

1　効果的な採用活動の推進
- ✓ 中途採用・官民人事交流による高度人材の確保。リボルビングドアの推進
- ✓ ＩＴ求人情報サイト等への募集広告、学校訪問・業務説明会の一層の推進
- ✓ サイバー人材のキャリアパスを「見える化」し外部にアウトリーチ
- ✓ 都道府県警察が行うサイバーコンテスト等に積極的に参画

2　部内におけるサイバー人材の発掘
- ✓ 警察庁と全国の情報通信部門が一体となって、部内で勤務する職員の経歴・資格について確実に確認
- ✓ 解析に関する部内競技会の開催その他の取組を通じて、サイバー人材となり得る警察職員を発掘

サイバー人材の育成

1　必要な能力の明確化と確認
- ✓ 必要な能力を明確化しつつ、既存の認定制度の根拠を整備
- ✓ 警察庁サイバー特別捜査部・都道府県警察への異動・出向を念頭に警察官の検定制度を活用
- ✓ 昇任候補者選考においてサイバー関連分野に関する知識を含めて審査

2　教養・研修の推進
- ✓ 警察情報通信学校で全ての技官に対する底上げ教養を実施
- ✓ 都道府県警察や警察庁への出向・異動を通じ職場教養を推進
- ✓ 留学・民間研修でトップ人材育成
- ✓ 資格取得に対する支援

サイバー人材のキャリアパス管理

1　警察庁サイバー警察局と長官官房人事課の緊密な連携
- ✓ サイバー警察局・長官官房を中核に全情報通信部門一体となって、サイバー人材のキャリアパスを管理

2　キャリアパス管理に基づく職員の配置等
- ✓ 高度サイバー人材については能力をいかせるポストへの配置に配意
- ✓ ハイブリッド人材育成の観点から都道府県警察サイバー部門に積極的に出向、情管への出向も検討
- ✓ 警察庁サイバー警察局・サイバー特別捜査部に長期勤務も念頭に配置、特に優秀な者については幹部ポストに登用

上記方針に基づき、警察庁サイバー警察局と長官官房の緊密な連携の下、全国の情報通信部門が一体となって必要な施策を推進

資料編

（第２部３「基盤整備」関連）

サイバー部門の変遷

年　月	概　要
H8.4	警察庁長官官房にネットワークセキュリティ対策室を設置。
H10.6	「ハイテク犯罪対策重点プログラム」を策定。
H11.4	警察庁情報通信局に技術対策課を設置。
H11.8	不正アクセス行為の禁止等に関する法律の成立・公布。
H12.2	「警察庁情報セキュリティ政策大系」を策定。
H16.4	警察庁生活安全局に情報技術犯罪対策課を設置し、警察庁情報通信局の技術対策課を情報技術解析課に改組。
H23.6	刑法の一部が改正。不正指令電磁的記録に関する罪が新設。
H23.10	「サイバー空間の脅威に対する総合対策推進要綱」を策定。
H24.7	警察庁長官官房審議官（サイバーセキュリティ戦略担当）を設置。
H25.1	「サイバー犯罪対処能力の強化等に向けた緊急プログラム」を策定。
H25.5	警察庁警備局警備企画課にサイバー攻撃対策官を設置。
H26.4	警察庁長官官房審議官（サイバーセキュリティ戦略担当）の担務を「サイバーセキュリティ」に変更するとともに、長官官房参事官（サイバーセキュリティ担当）を設置。 警察大学校にサイバーセキュリティ研究・研修センターを設置。
H27.9	「警察におけるサイバーセキュリティ戦略」を策定。
R4.4	警察庁サイバー警察局を設置。 警察庁関東管区警察局にサイバー特別捜査隊を設置。
R6.4	サイバー特別捜査隊をサイバー特別捜査部に発展的改組。
R7.4	サイバー特別捜査部に特別対処課を設置。 警察大学校にサイバー警察教養部を設置。