広　報　資　料
令和６年９月19日
サイバー企画課

令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について

第１　概要

令和６年上半期におけるサイバー空間をめぐる脅威の情勢とサイバー特別捜査部の活動状況等について取りまとめたもの。

第２　サイバー空間の脅威情勢とサイバー特別捜査部の活動状況等

１　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

世界各地でサイバー攻撃が相次いで発生し、我が国でも政府機関等におけるDDoS攻撃とみられる被害が発生。令和６年上半期におけるランサムウェアの被害報告件数は114件となり、流出した情報はダークウェブ上のリークサイトに掲載。また、生成AIを悪用した事案も発生。

(2)　インターネット空間を悪用した犯罪に係る脅威情勢

インターネットバンキングに係る不正送金事案やSNSを通じて金銭をだまし取るSNS型投資・ロマンス詐欺、暗号資産を利用したマネー・ローンダリングの発生など、インターネット上のサービスが悪用。令和６年上半期におけるフィッシング報告件数は63万3,089件、インターネットバンキングに係る不正送金被害額は約24億4,000万円。

(3)　違法・有害情報に係る情勢

インターネット上には、児童ポルノ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、SNS上には、犯罪実行者募集情報が氾濫。

２　サイバー特別捜査部の活動状況等

令和６年４月、サイバー特別捜査隊をサイバー特別捜査部に改組し、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等を行う体制を強化。本年上半期の事案は、以下のとおり。

- 令和６年２月、EUROPOL等との国際共同捜査において、ランサムウェア攻撃グループ「LockBit」の被疑者２名を検挙。また、暗号化されたデータの復号ツールを独自開発して被害回復に活用。
- 令和６年７月、暗号資産の追跡捜査等を実施し、インターネットバンキングに係る不正送金事件の指示役を逮捕。
- 令和６年７月、石川県警察は、サイバー特別捜査部と連携した捜査を実施した結果、能登半島地震に関して虚偽の救助要請を投稿した男を偽計業務妨害罪で逮捕。

令和６年上半期における
サイバー空間をめぐる脅威の情勢等について

令和６年９月
警察庁サイバー警察局

はじめに

近年、世界各地で重要インフラの機能停止や機密情報の窃取を企図したとみられるサイバー攻撃が相次いで発生し、我が国でも政府機関等において DDoS 攻撃とみられる被害が発生しているほか、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、増加の一途をたどり、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 6 年上半期におけるランサムウェアの被害報告件数は、114 件と引き続き高水準で推移しており、流出した情報は、ダークウェブ上のリークサイトに掲載されていることが確認されている。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：Ransomware as a Service）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、児童ポルノ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。令和 6 年 1 月に発生した能登半島地震に際しては、過去の災害時の画像や偽の救助情報が拡散される事態も見られた。

このような状況の中、警察においては、令和 6 年 4 月、全国を管轄して直接捜査を実施するサイバー特別捜査隊を、サイバー特別捜査部に発展的に改組し、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等を行う体制を強化した。サイバー特別捜査部では、EUROPOL 主導の国際共同捜査へ参画し、海外の DDoS 攻撃ウェブサービスを利用した DDoS 攻撃事案の国内被疑者を特定し逮捕したほか、能登半島地震において被災者を装って救助を求める虚偽の内容を投稿した被疑者の逮捕に貢献するなどしている。

そのほか、警察庁においては、中国政府を背景とするサイバー攻撃グループ APT40 による攻撃手法や緩和策が示された国際アドバイザリーの共同署名に参画し、本件アドバイザリーを公表するなど様々な取組を実施している。

本資料は、第 1 部で令和 6 年上半期中のサイバー空間の脅威に関し、情勢及び警察の取組を、第 2 部でサイバー特別捜査部の活動状況を取りまとめたものである。

目次

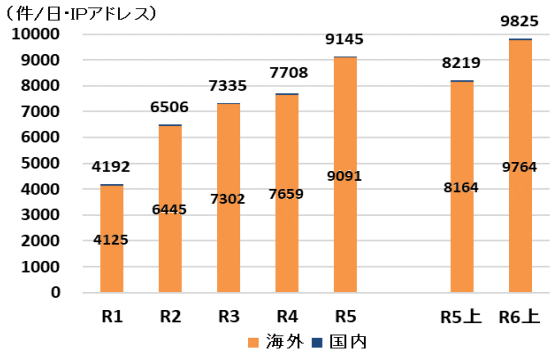
概要　令和６年上半期における脅威情勢の概要

令和６年上半期においては、サイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数及びランサムウェアの被害報告件数が前年同期から増加した。また、フィッシングの被害報告件数も前年同期比で約 10 万件増加したほか、インターネット上には犯罪実行者募集情報が氾濫するなど、極めて深刻な情勢が継続している。そのような中、警察においては、令和６年４月、サイバー特別捜査隊をサイバー特別捜査部に改組し、捜査・分析体制を強化した。

１　高度な技術を悪用したサイバー攻撃の脅威情勢

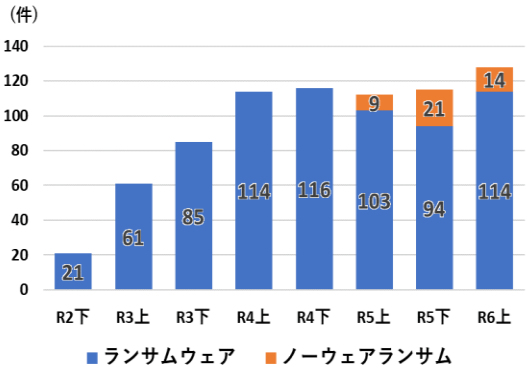
● 近年、世界各地で重要インフラの機能停止や機密情報の窃取を企図したとみられるサイバー攻撃が相次いで発生し、我が国でも、政府機関等において DDoS 攻撃とみられる被害が発生しているほか、生成 AI を悪用した事案も発生。

● 警察庁が設置したセンサーにおいて検知した、ぜい弱性探索行為等の不審なアクセス件数は、増加の一途をたどり、その大部分が海外を送信元とするアクセス。



● 令和６年上半期におけるランサムウェアの被害報告件数は、114 件であり、高水準で推移。流出した情報は、ダークウェブ上のリークサイトに掲載。

※　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。



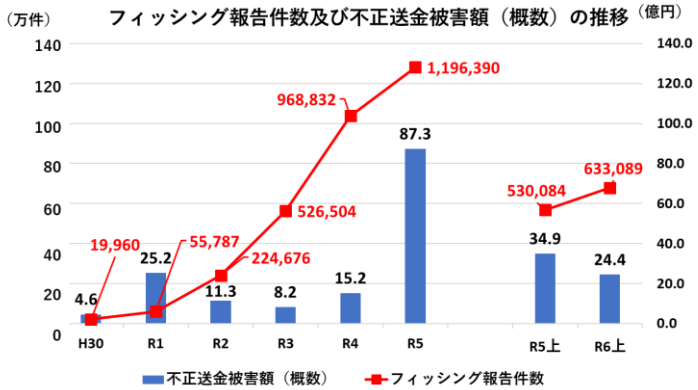
【警察の取組】

● サイバー特別捜査隊（当時）が参画した国際共同捜査において、ランサムウェア事案被疑者が検挙されたほか、警察庁において、中国政府を背景とするサイバー攻撃グループ APT40 による攻撃手法や緩和策が示された国際アドバイザリーの共同署名に参画し、本件アドバイザリーを公表。

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。

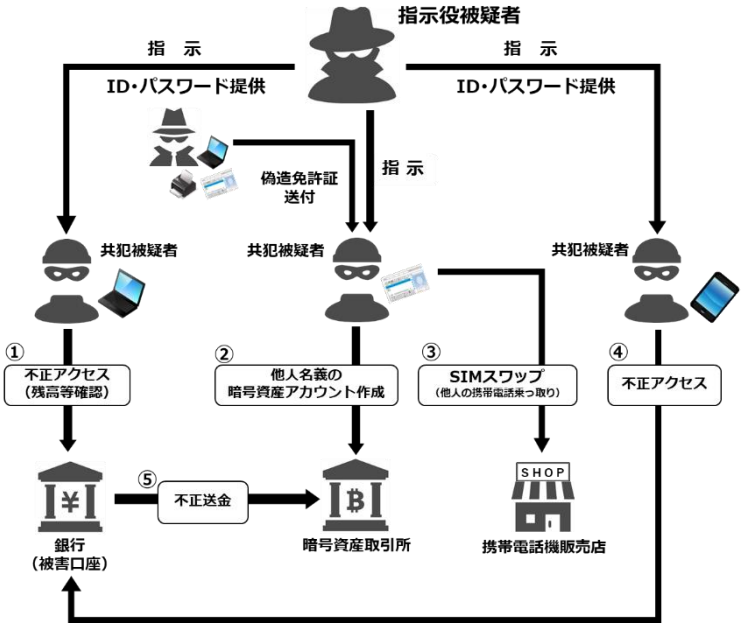
● 令和６年上半期におけるフィッシング報告件数は、63 万 3,089 件、インターネットバンキングに係る不正送金被害総額は約 24 億 4,000 万円。



※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（以下同）

【警察の取組】

● 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。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。令和６年７月、同男を逮捕。



３　違法・有害情報に係る情勢

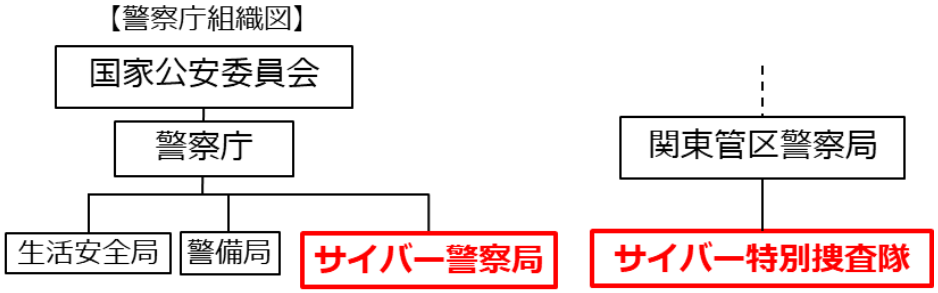
● インターネット上には、児童ポルノ等の違法情報や犯罪を誘発するような有害情報が存在するほか、近年 SNS 上に氾濫する犯罪実行者募集情報は深刻な治安上の脅威。能登半島地震では、過去の災害時の画像や偽の救助情報が拡散。

【警察の取組】

● 石川県警察は、サイバー特別捜査部と連携した捜査を実施した結果、地震当日に被災者を装って SNS 上に救助を求める虚偽の内容を投稿し、本来不要な捜索活動を警察に実施させてその業務を妨害した会社員の男（25 歳）を特定。令和６年７月、同男を偽計業務妨害罪で逮捕。

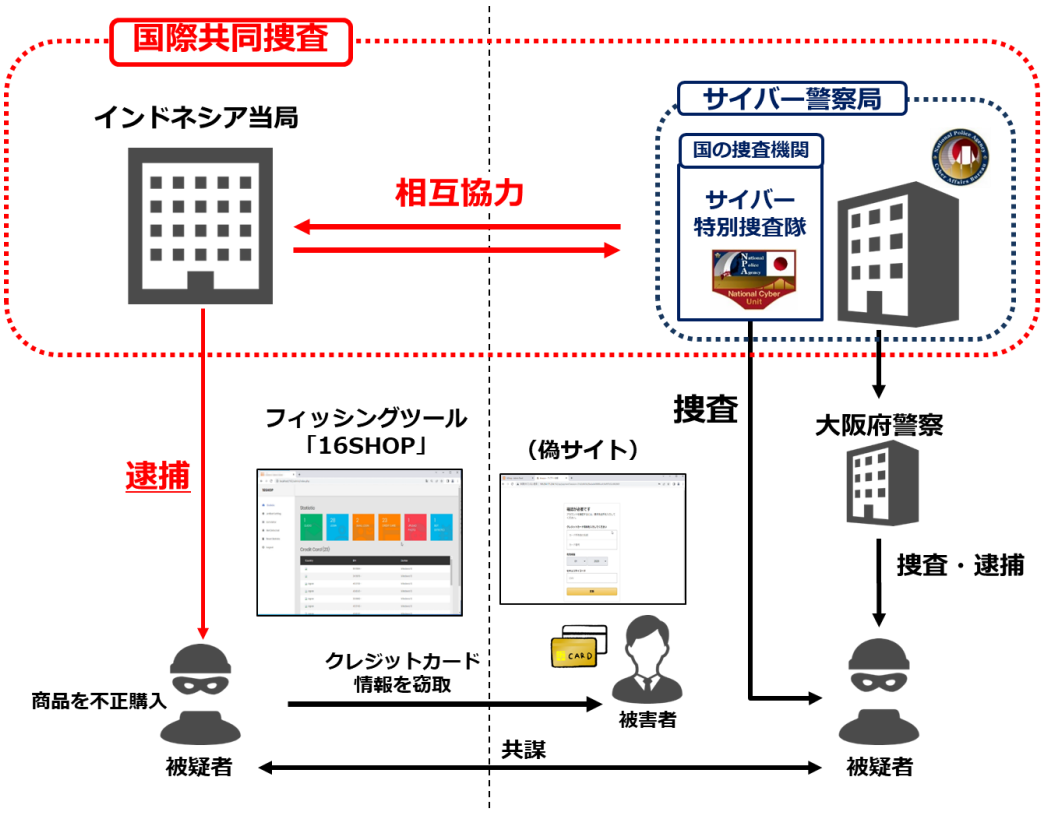
４　サイバー特別捜査部の活動状況

● 令和４年４月、国境を容易に越えて敢行されるサイバー事案に対し、国際共同捜査を通じて被疑者を検挙するため、関東管区警察局に、全国を管轄して直接捜査を実施する「サイバー特別捜査隊」を設置。

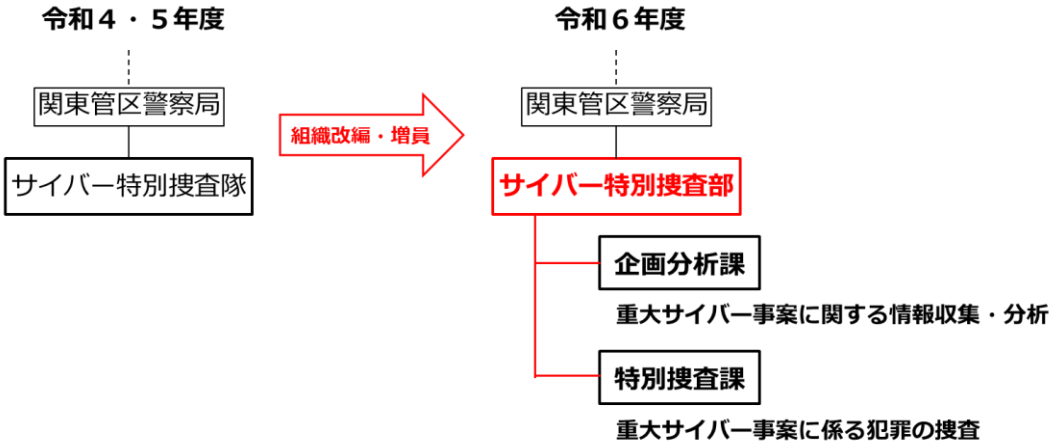


【「16SHOP」を用いたクレジットカード情報不正取得・利用事案】

サイバー特別捜査隊等とインドネシア国家警察との国際共同捜査により、フィッシングツール「16SHOP」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。令和５年７月、インドネシア国家警察が同被疑者を逮捕。本件は、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。

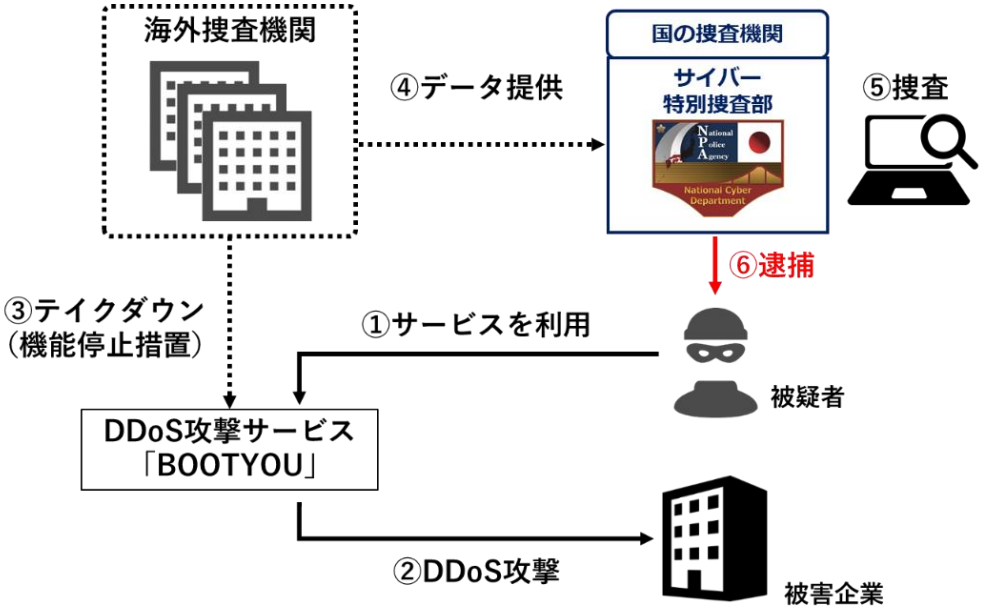


● 令和６年４月、サイバー特別捜査隊を発展的に改組し、「サイバー特別捜査部」を設置することにより、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析等を行う体制を強化。



【DDoS 攻撃ウェブサービスを利用した DDoS 攻撃事案被疑者の検挙】

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、海外の DDoS 攻撃ウェブサービスを利用した DDoS 攻撃事案の国内被疑者を特定・逮捕（令和６年８月）。本件は、EUROPOL 主導の国際共同捜査への参画が国内被疑者の検挙に結びついた初の事例となった。



第１部　サイバー空間の脅威情勢と警察の取組

１　高度な技術を悪用したサイバー攻撃の脅威情勢

(1)　情勢

ア　国家を背景としたサイバー攻撃やDDoS攻撃等の情勢

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

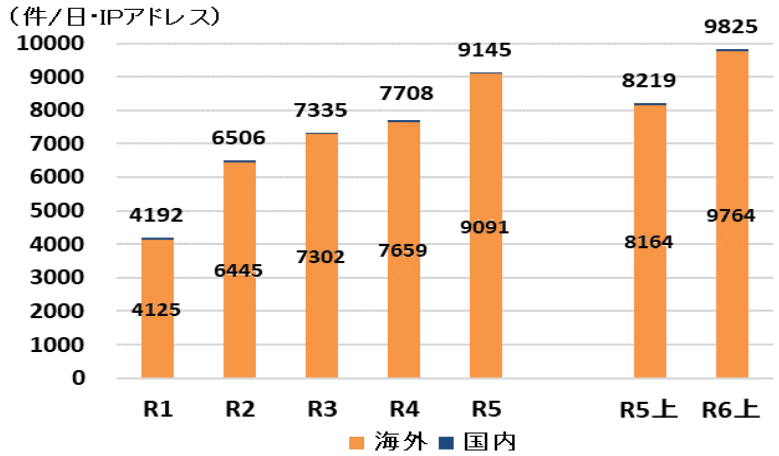
重要インフラの基幹システムに障害を発生させるサイバー攻撃（サイバーテロ）は、インフラ機能の維持やサービスの供給を困難とし、国民の生活や社会経済活動に重大な被害をもたらすおそれがある。また、軍事技術へ転用可能な先端技術や、国の機密情報の窃取を目的とするサイバー攻撃（サイバーエスピオナージ）は、企業の競争力の源泉を失わせるのみならず、我が国の経済安全保障等にも重大な影響を及ぼしかねない。さらに、現実空間におけるテロの準備行為として、重要インフラの警備体制等の機密情報を窃取するためにサイバーエスピオナージが行われるおそれもある。

例えば、我が国においても、令和６年２月には、政府機関や民間企業等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ており、これら事案の中には、障害発生と同じ頃にSNS上でハクティビストのものと思われるアカウントから犯行をほのめかす投稿がなされる事案も確認された。また、過去には中国を背景とするサイバー攻撃グループBlackTech が、日本を含む東アジアと米国の政府機関や事業者を標的とし、情報窃取を目的としたサイバー攻撃を行っていることも確認された。

今後も国や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サイバー攻撃が発生す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６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9,824.7件と、平成23年以降、増加の一途をたどっており（前年同期比19.5%増）、その大部分を海外を送信元とするアクセスが占めている（図表１）。

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



イ　ランサムウェアの被害情勢・「RaaS」を中心とした攻撃者の相互分担状況

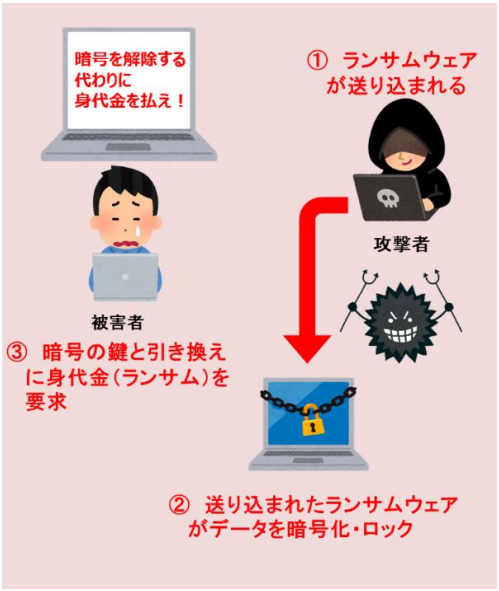
ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラムであり（図表２）、ランサムウェアによって流出したとみられる事業者等の財務情報や個人情報等が、ダークウェブ上のリークサイトに掲載されていたことが確認されている。

サイバー特別捜査部による事案捜査及び実態解明により、ランサムウェアの開発・運営を行う者（Operator）が、攻撃の実行者（Affiliate）にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る態様（RaaS：Ransomware as a Service）も確認された。さらに、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（IAB: Initial Access Broker）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（図表４）。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、RaaS を中心とした攻撃者の裾野の広がりがランサムウェアの被害を拡大させている背景の一つとして指摘されている。

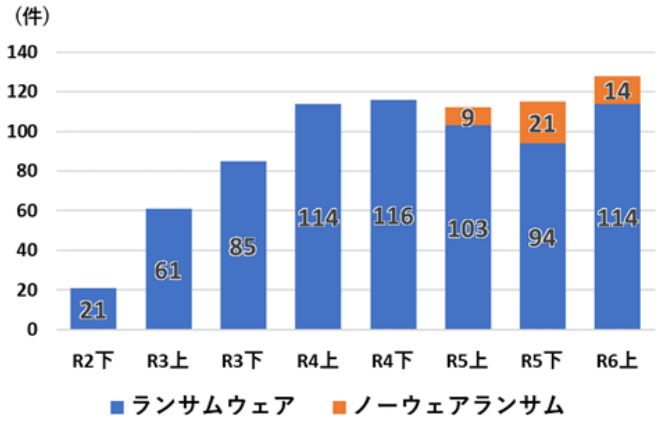
また、ランサムウェアの手口としては、データの暗号化のみならず、データを窃取した上、「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝が多くを占めている。

令和６年６月、出版大手企業は、同社のサーバがランサムウェアを含む大規模な攻撃を受けたと発表した。この攻撃により、同社が提供するウェブサービスが広く停止したほか、書籍の流通等の事業に影響が発生した。同年８月、同社は、この攻撃により 25 万人分を超える個人情報や企業情報が漏えいしたことが確認されたこと及び同年度決算において、調査・復旧費用等として 30 億円を超える損失を計上する見込みであることを発表した。

【図表２：ランサムウェアの攻撃の流れ】

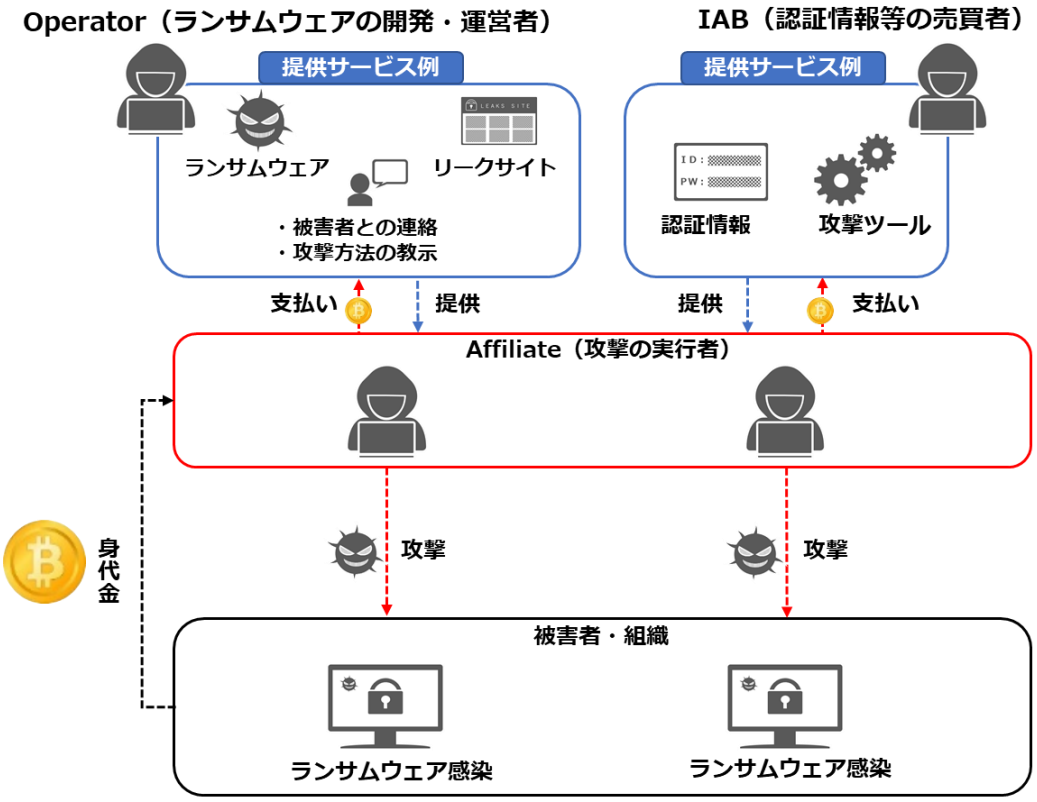


【図表３：ランサムウェア被害報告件数の推移】



※　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。

【図表４：ランサムウェア等を提供する者と攻撃を実行する者】



ウ　AI をめぐる情勢

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で、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、警察庁情報技術解析部門の分析により、一般的な生成 AI サービスでも、悪意あるプログラムを作成できることが判明したほか、生成 AI を利用して不正プログラムを作成した容疑で、逮捕事案も発生している。

(2) 警察の取組

ア 豪州主導の APT40 に関する国際アドバイザリーへの共同署名

中国政府を背景とするサイバー攻撃グループといわれている APT40 は、北米、欧州、豪州等を標的としており、我が国の企業も攻撃の標的になっていたことが確認されている。

令和６年７月、警察庁及び内閣サイバーセキュリティセンター（NISC）は、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 による過去の攻撃事例に基づく攻撃手法、攻撃の検知や緩和策が示された国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action」の共同署名に加わり、本件アドバイザリーを公表した。

【図表５：豪州主導の APT40 に関する国際アドバイザリー（抜粋）】

イ サイバー特別捜査部による国際共同捜査

警察庁サイバー警察局は、令和４年６月から EUROPOL に常駐しているサイバー事案対策専従の連絡担当官による同機関での継続的な情報共有・分析や、国際機関が主催する捜査会議への積極的な参画等を通じ、外国捜査機関等との一層の連携強化に取り組んでいる。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、国際共同捜査への参画を通じて、サイバー事案に係る被疑者を検挙している（第２部参照）。

ウ　生成 AI を悪用した不正プログラム作成事件被疑者の検挙

無職の男（25 歳）は、令和５年３月、生成 AI を利用し、人が電子計算機で実行した際、ファイルのデータを上書きして破壊する機能を有する不正プログラムを作成した。令和６年５月、同男を不正指令電磁的記録作成罪で逮捕した。（警視庁）

エ　警察におけるその他の取組

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、重大なサイバー攻撃を未然に防ぐ「能動的サイバー防御」を導入する方針が掲げられ、内閣官房を中心に検討されているところ、警察もその議論に参画している。

また、令和６年５月、警察庁は、NISC、カナダ、エストニア、フィンランド及び英国の関係機関とともに、米国サイバーセキュリティ・インフラストラクチャー安全保障庁（CISA）が作成した、国家を背景とするサイバー攻撃の被害に遭う危険性が高い人権保護や民主主義の推進に関与する組織・個人向けのリスク緩和策に関する合同ガイダンスの署名に加わった。

【図表６：サイバー脅威を緩和するための合同ガイダンス（表紙抜粋）】

さらに、警察では、各都道府県警察及び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ており、令和６年上半期には、重要インフラ事業者等とのサイバー攻撃事案の発生を想定した共同対処訓練等を約 380 回実施するなど官民連携による取組を実施しているほか、警察庁のウェブサイトに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て、通報・相談に係る負担軽減を図っている。また、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を実施している。

加えて、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ほか、情報セキュリティ大学院大学へ職員を派遣し、現在は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進めている。

２　インターネット空間を悪用した犯罪に係る脅威情勢

(1)　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、また深刻化させている。

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、インターネット上での自由な活動とプライバシー保護等の目的で利用される匿名化技術が活用されたダークウェブには、ランサムウェアにより窃取された情報や児童ポルノ画像、専門的な知識を持たなくともサイバー攻撃を可能にするためのツールキット等が掲載されるなどしており、サイバー特別捜査隊（当時）による実態解明の結果、中国人グループがフィッシングで窃取した情報をダークウェブ上で売買していたとみられる事案が明らかとなっている。

実際、令和６年７月にサイバー特別捜査部等からなる合同捜査本部が検挙した、インターネットバンキングに係る不正送金事案（第２部２(2)参照）においても、その犯行グループの指示役は、ダークウェブ上に存在するマーケットで流通していた、インターネットバンキングの識別符号（ID やパスワード）を入手した可能性がある。

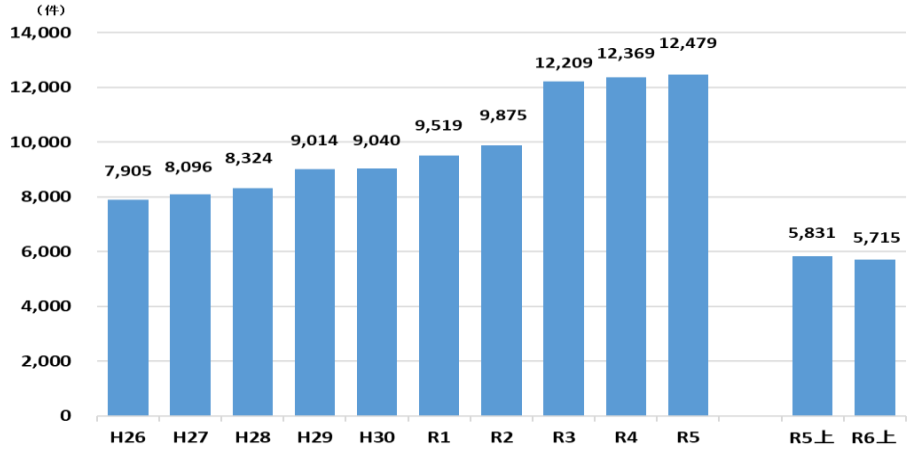
また、多くの国民が利用する SNS についても犯罪インフラとして悪用される例が見られる。例えば、各種犯罪により得た収益を吸い上げる中核部分が匿名化されている、SNS を通じるなどしてメンバー同士が緩やかに結びついているといった特徴を有する「匿名・流動型犯罪グループ」が、SNS で高額な報酬を示唆して犯罪の実行犯を募集して、特殊詐欺等を敢行している実態が見られるほか、SNS を使用した非対面型の投資詐欺やロマンス詐欺、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害においても、同グループの関与がうかがわれている。

さらに、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おり、令和６年上半期に検挙されたインターネット上での名誉毀損罪及び侮辱罪は合計で 217 件となっており、増加傾向にある。

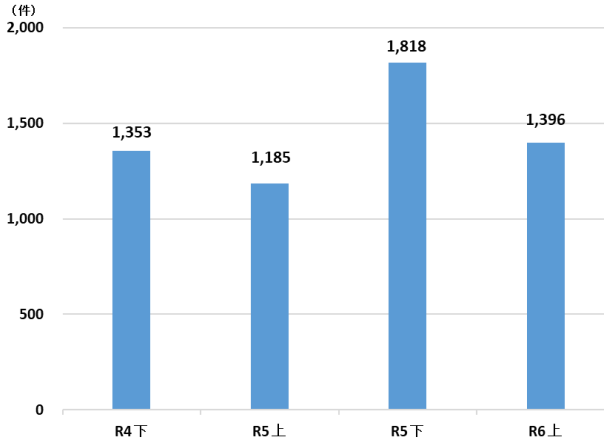
このように現代においては、ありとあらゆる犯罪がインターネット空間を悪用しているともいえる状況であり、その結果、令和６年上半期におけるサイバ

ー犯罪[1]の検挙件数は 5,715 件に、サイバー事案[2]の検挙件数は 1,396 件に達している。

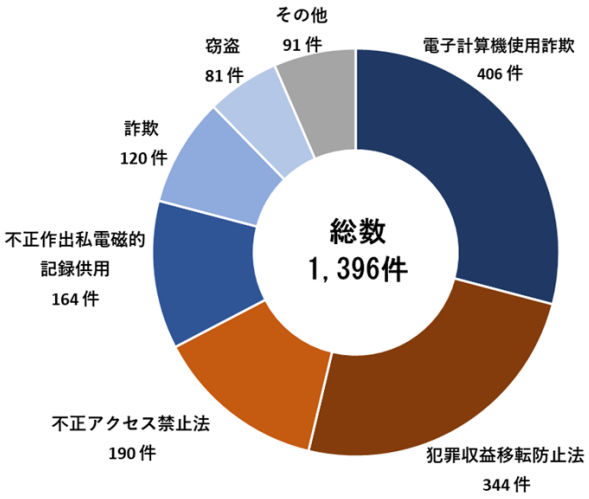
【図表７：サイバー犯罪の検挙件数の推移】



【図表８：サイバー事案の検挙件数の推移】



【図表９：令和６年上半期のサイバー事案の検挙状況】



また、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見られる。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、移転記録が公開されず、追跡が困難で、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。

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

[2] 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

【図表 10：暗号資産を悪用したマネー・ローンダリングのイメージ】

警察においては、警察庁サイバー警察局がサイバー政策の推進における中心的な役割を、サイバー特別捜査部が重大サイバー事案[3]への対処を担い、都道府県警察において被害相談の受付・捜査・対策等を推進する役割を担っている。また、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さないものについては、各事件主管部門において主体的に捜査を行うほか、サイバー部門が各事件主管部門を適切に支援することとされている。

ここからは、インターネット空間を悪用した犯罪に係る情勢について、主な事象ごとに詳細を記述する。

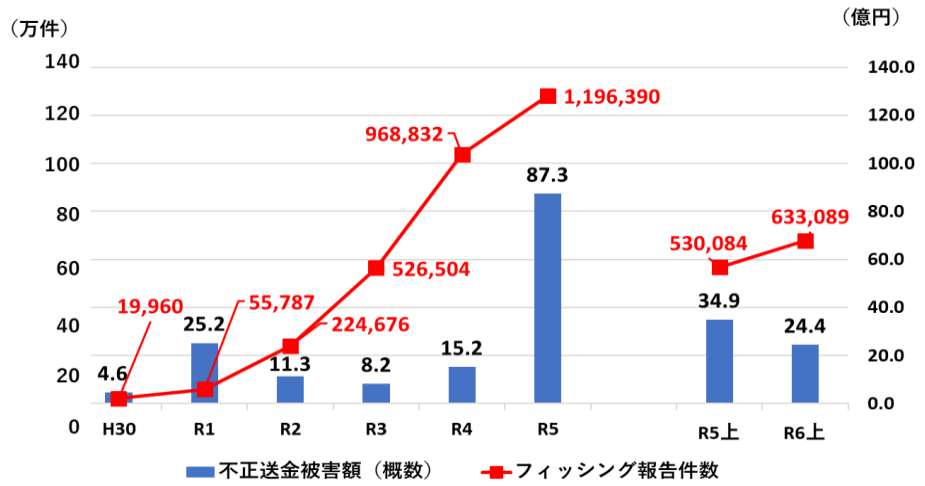
ア　フィッシング

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、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６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、63 万 3,089 件であり、右肩上がりで増加となった。また、令和６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 1,728 件、被害総額は約 24 億４,000 万円となっている。

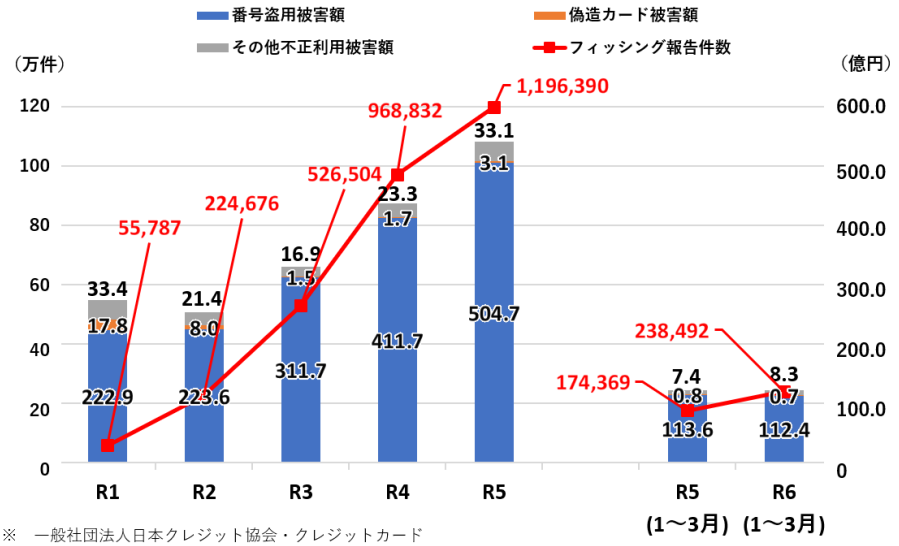
[3] サイバー事案のうち、国若しくは地方公共団体の重要なシステムの運用や重要インフラ事業者の事業の実施に重大な支障が生じ、若しくは生ずるおそれのある事案、高度な技術的手法が用いられるなどの事案（マルウェア事案等）、又は国外に所在するサイバー攻撃者による事案

【図表 11：フィッシング報告件数及び不正送金被害額（概数）の推移】



また、令和６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 121 億円と、依然として厳しい情勢にある。

【図表 12：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（概数）の推移】



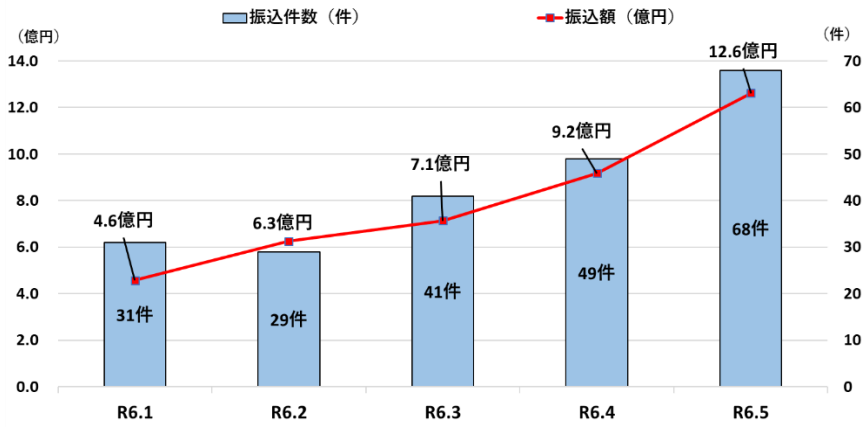
※　一般社団法人日本クレジット協会・クレジットカード不正利用被害の発生状況から作成

イ　特殊詐欺

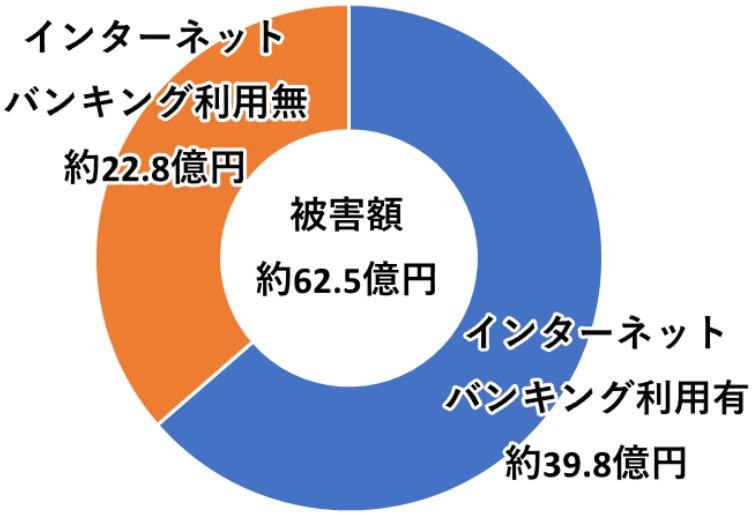
令和５年中の特殊詐欺の被害額は約 453 億円と２年連続増加傾向にあり、令和６年上半期の被害額も約 227 億 8,000 万円と、依然として深刻な情勢にある。近年は、匿名・流動型犯罪グループによるものとみられる特殊詐欺が広域的に行われており、同グループは SNS で高額な報酬を示唆して「受け子」等を募集し、犯行に加担させている。また、首謀者、指示役、実行役の間の連絡手段には、匿名性が高く、メッセージが自動的に消去される仕組みを備えた通信手段を使用するなど、犯罪の証拠を隠滅しようとする手口が多く見られる。

さらに、令和６年１月から５月までの被害額 500 万円以上の振込型被害（認知件数 374 件、被害額約 62 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･被害額は増加傾向にあり、全体の約６割を占めている。このように、特殊詐欺を敢行するに当たっても、サイバー空間や新たな技術が悪用されている。

【図表 13：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の推移】



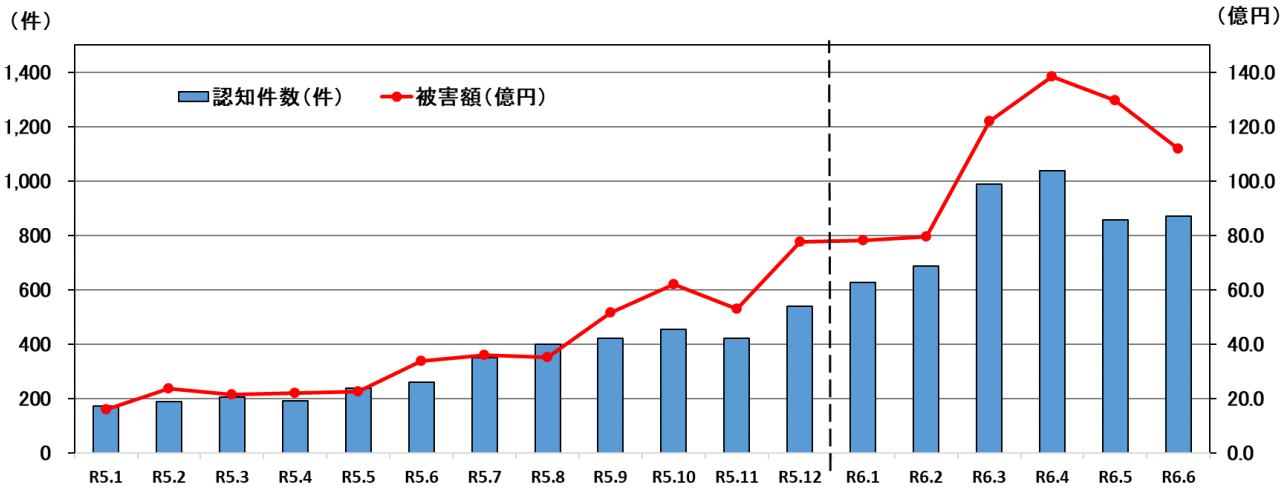
【図表 14：令和６年１月～５月における特殊詐欺の振込形態別被害額】



ウ　SNS 型投資・ロマンス詐欺

SNS を通じて対面することなく、交信を重ねるなどして関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭をだまし取る又は恋愛感情や親近感を抱かせて金銭をだまし取る SNS 型投資・ロマンス詐欺は、認知件数、被害額ともに増加傾向にあり、その犯行に当たって多くの国民が利用する SNS が犯行ツールとして悪用されている。

【図表 15：SNS 型投資・ロマンス詐欺の認知件数・被害額の推移
（令和５年１月～令和６年６月（月別））】



(2) 警察の取組

ア 匿名・流動型犯罪グループの捜査等

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、インターネットバンキングに係る不正送金事犯と特殊詐欺事案に関して同一被疑者の関与が判明するなど、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り、今後も更なる捜査の進展が期待される。

また、暗号資産をめぐっては、ミキシングに代表される、移転状況の追跡を困難にし得る技術や手法に対抗するため、警察庁サイバー警察局では、追跡技術の研究を推進するとともに、国際連携を通じた追跡能力の強化に取り組んでいる。令和６年上半期には、優れた知見・実績で知られるノルウェー王国の捜査機関「オコクリム」の専門家を我が国に招へいし、両国における最新の捜査手法等について情報交換した。

イ 警察におけるその他の取組

警察庁は、暗号資産交換業者等と連携して、犯罪に利用された取引口座の凍結を実施しているほか、令和６年２月、金融庁と連携し、一般社団法人全国銀行協会等に対して、暗号資産交換業者の金融機関口座に対して送金元口座名義人名と異なる依頼人名で行われる送金の拒否、暗号資産交換業者への不正な送金への監視強化等の、会員等における対策強化を要請した。

また、SIM スワップ[4]による不正送金対策として、令和６年５月、総務省と連携し、携帯電話事業者に対して本人確認の強化を要請した（令和４年９月以降２度目）。

さらに、フィッシングサイトの閲覧防止対策として、各都道府県警察では、サイバー防犯ボランティアの拡大・活性化を図るとともに、フィッシングサイトのテイクダウンがより効果的に行われるよう各団体へ助言・指導している。加えて、一般財団法人日本サイバー犯罪対策センター（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、令和６年２月から３月にかけてサイバー

[4] 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

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」を実施しており、警察庁はこれを後援している。

【図表 16：サイバー防犯ボランティアへの支援】

また、令和６年７月には、国際的な詐欺の拠点となっているナイジェリアで、国際刑事警察機構（ICPO）と国際協力機構（JICA）が開催した、ロマンス詐欺等の捜査力向上を目的とした研修会において、警察庁担当者が資金回収等に使われる暗号資産に関する捜査手法を説明するなどした。

このほか、「国民を詐欺から守るための総合対策」（令和６年６月 18 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（「資料編」参照）。

３　違法・有害情報に係る情勢

(1)　情勢

インターネット上には、児童ポルノ、規制薬物の広告等の違法情報のほか、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。

近年 SNS 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直接的かつ明示的に誘引等（募集）する情報（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。

実際、令和６年４月から５月までの間における匿名・流動型犯罪グループによるものとみられる資金獲得犯罪[5]のうち、主な資金獲得犯罪[6]の検挙人員 508 人中、SNS での犯罪実行者募集情報に応募する形で犯行に関与した者は 155 人と、全体の 30.5%を占めている。

また、令和６年１月１日に発生した能登半島地震においては、インターネット上において、過去の別場面に酷似した画像を添付しての投稿や、存在しない住所を記載し不確かな救助を呼び掛ける投稿等が多数拡散されたほか、SNS 上において、QR コードを利用した義援金を募る送金詐欺も確認された。

(2)　警察の取組

ア　犯罪実行者募集情報対策を含む IHC 及び CPC による削除依頼等

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。また、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、重要犯罪密接関連情報[7]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。

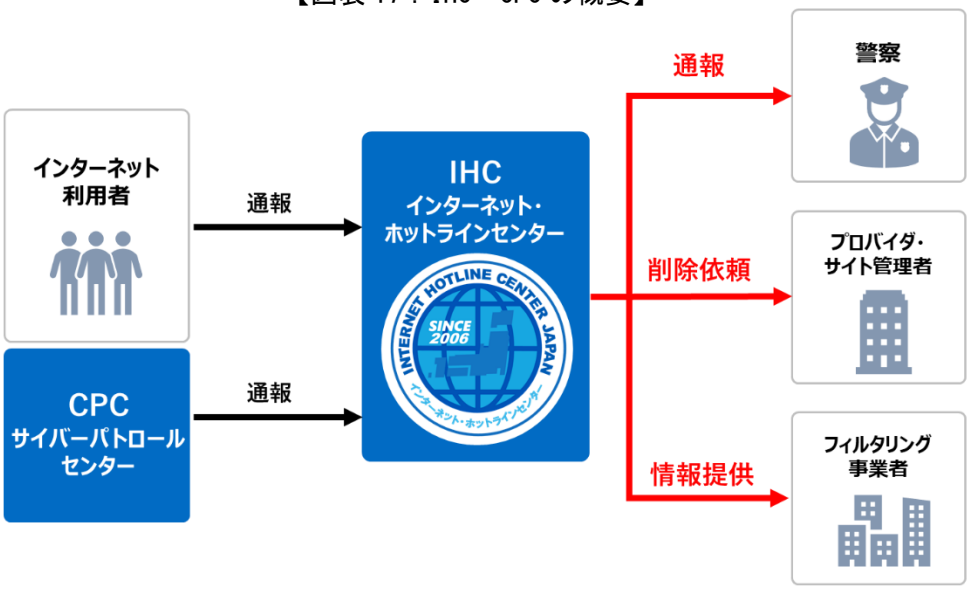
---

[5] 匿名・流動型犯罪グループによる資金獲得犯罪とは、匿名・流動型犯罪グループの活動資金の調達につながる可能性のある犯罪をいい、特殊詐欺や強盗、覚醒剤の密売、繁華街における飲食店等からのみかじめ料の徴収、企業や行政機関を対象とした恐喝又は強要、窃盗、各種公的給付金制度を悪用した詐欺等のほか、一般の経済取引を装った違法な貸金業や風俗店経営、ＡＶへのスカウト等の労働者供給事業等をいう。

[6] 詐欺、強盗、窃盗、薬物事犯及び風営適正化法違反

[7] インターネット上に流通することによって、個人の生命・身体に危害を加えるおそれが高い重要犯罪又は重要犯罪に発展する危険性がある犯罪と密接に関連している次の情報　①拳銃等の譲渡等、②爆発物・銃砲等の製造、③殺人等（殺人、強盗、不同意性交等、放火、誘拐、傷害、逮捕・監禁、脅迫）、④臓器売買、⑤人身売買、⑥硫化水素ガスの製造、⑦ストーカー行為等、⑧犯罪実行者募集情報

【図表 17：IHC・CPC の概要】



令和 5 年 9 月、IHC 及び CPC の取扱情報の範囲に犯罪実行者募集情報を追加するとともに、同月、CPC において 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た。

令和 6 年上半期における IHC の受理件数のうち、運用ガイドラインに基づいて 23 万 9,368 件を分析した結果、違法情報を 3 万 4,045 件、重要犯罪密接関連情報を 8,333 件、自殺誘引等情報を 2,994 件と判断した。

これら違法・有害情報の削除の実効性を確保するため、令和 6 年 7 月、警察庁は総務省と連携し、国内のプロバイダ等事業者に対して、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。

イ　能登半島地震の偽情報投稿事案被疑者の検挙

令和 6 年 1 月 1 日に発生した能登半島地震においては、被災地の警察が捜索活動等に全力を挙げる中、SNS 上において虚偽の救助要請が拡散し、捜索活動等が妨害される事態が生じていた。そうした状況の中、サイバー特別捜査隊（当時）は、各種情報収集を通じて SNS 上で偽の救助要請が行われている疑いを把握し、被災地の警察と連携しながら、関連アカウントに関する所要の捜査を実施した。

石川県警察は、サイバー特別捜査隊の捜査結果を踏まえて更なる捜査を実施した結果、地震当日に被災者を装って SNS 上に救助を求める虚偽の内容を投稿し、本来不要な捜索活動等を警察に実施させてその業務を妨害した会社員の男（25 歳）を特定して、偽計業務妨害罪で逮捕した（令和 6 年 7 月）。

第２部　サイバー特別捜査部の活動状況

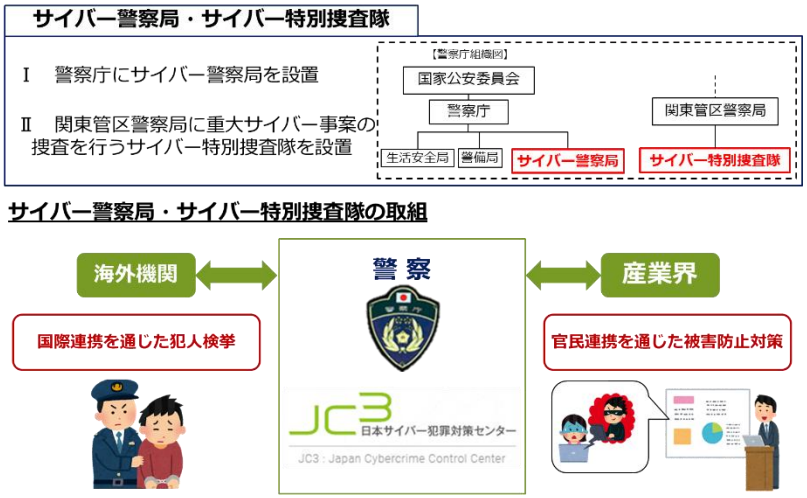
１　サイバー特別捜査隊設置以来の活動状況と発展的改組

(1)　サイバー特別捜査隊の設置と活動状況

サイバー事案の多くは国境を越えて敢行されるため、こうした事案への対処については、一つの国が単独で行うことには自ずと限界がある。そのため、外国捜査機関等との連携が不可欠となるところ、特に、国家を背景とするものを含めた組織的で高度なサイバー事案への対処に当たっては、各国が捜査等により得た情報や証拠を持ち寄り、それらに基づく被疑者の特定や犯行組織の実態解明等を共同して推進する国際共同捜査が有効である。そして、こうした国際共同捜査に参画するためには、高い捜査力・技術力はもちろん、その実績等に裏打ちされた外国捜査機関等との強固な信頼関係が求められる。

そこで、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。

【図表 18：サイバー警察局及びサイバー特別捜査隊の設置】

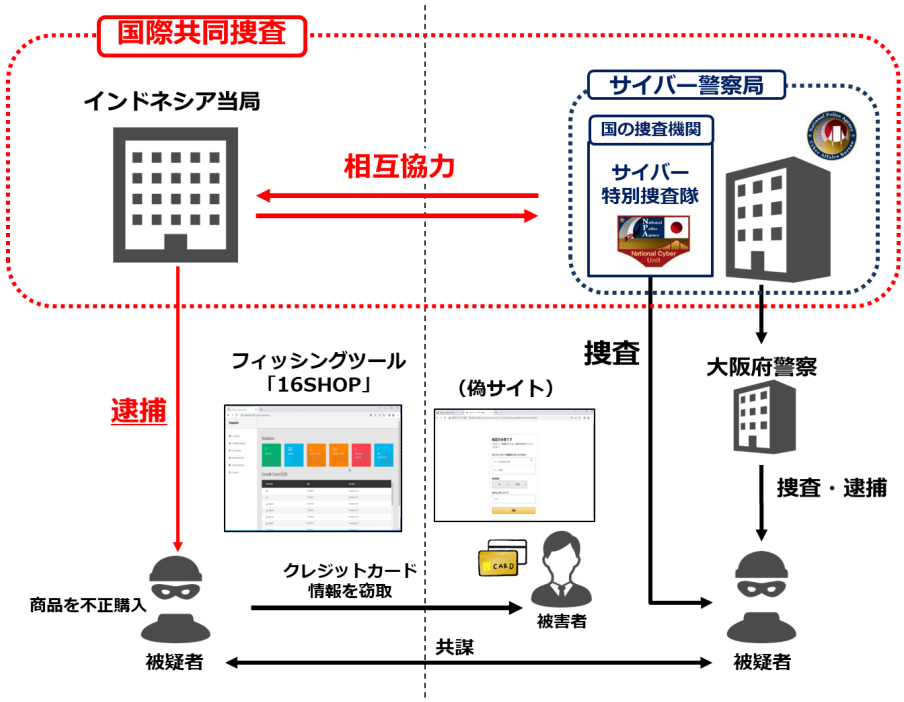


同隊は、従来、外国捜査機関等と都道府県警察との間で調整機能を果たすに過ぎなかった警察庁が、全国を管轄して直接捜査を実施し、国の捜査機関として国際共同捜査を通じて被疑者を検挙することを目的として設置された組織であり、全国警察からサイバー分野の知識や経験を豊富に持つ有為な人材を登用し、高度な資機材を整備した。高い捜査力・技術力を備えた結果、それまで対応が困難であった事案の被疑者の特定・犯罪グループの全体像の解明が可能となるとともに、外国捜査機関等と情報交換を継続的かつ緊密に行うことで、強固な信頼関係の構築を実現している。そして、国際共同捜査の機会を通じ、その実力をいかんなく発揮し、国際社会におけるプレゼンスを確固たるものとしつつある。過去の国際共同捜査の事例としては以下が挙げられる。

ア　「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等とインドネシア国家警察との国際共同捜査により、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。

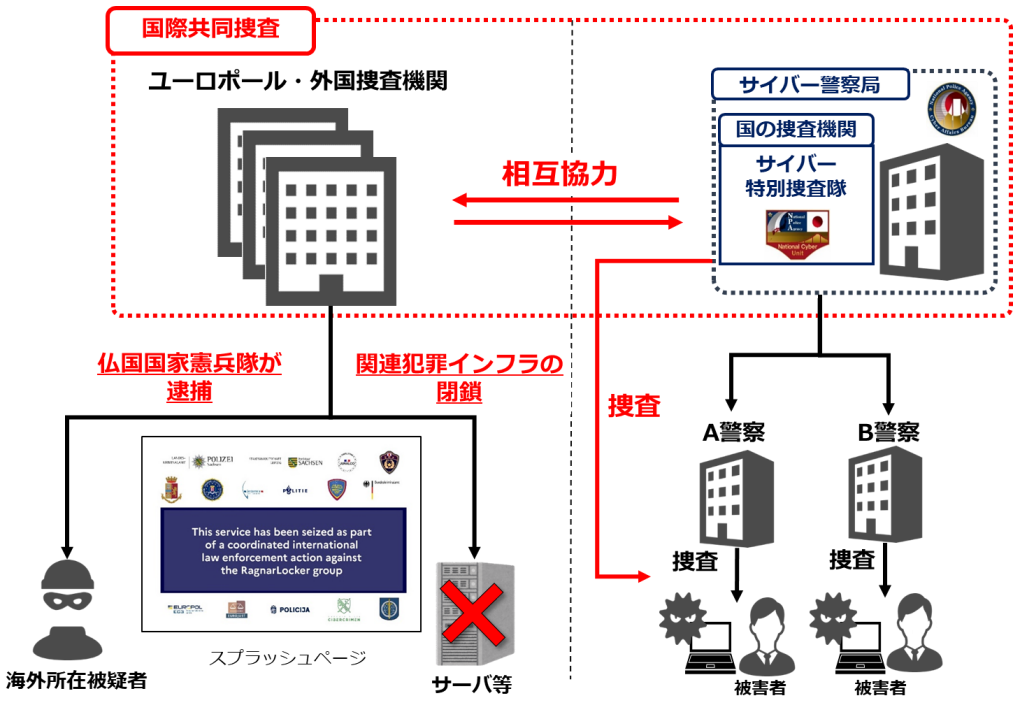
【図表 19：事案概要】



イ　「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においては、サイバー特別捜査隊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 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。

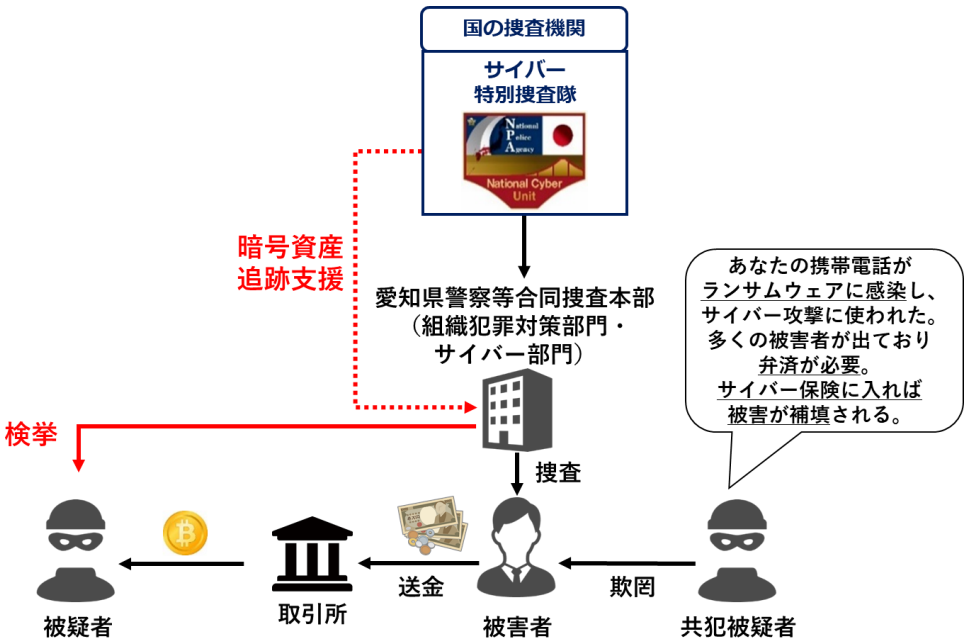
【図表 20：事案概要】



ウ　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り、関係警察による関連被疑者の逮捕に貢献した。

【図表 21：事案概要】

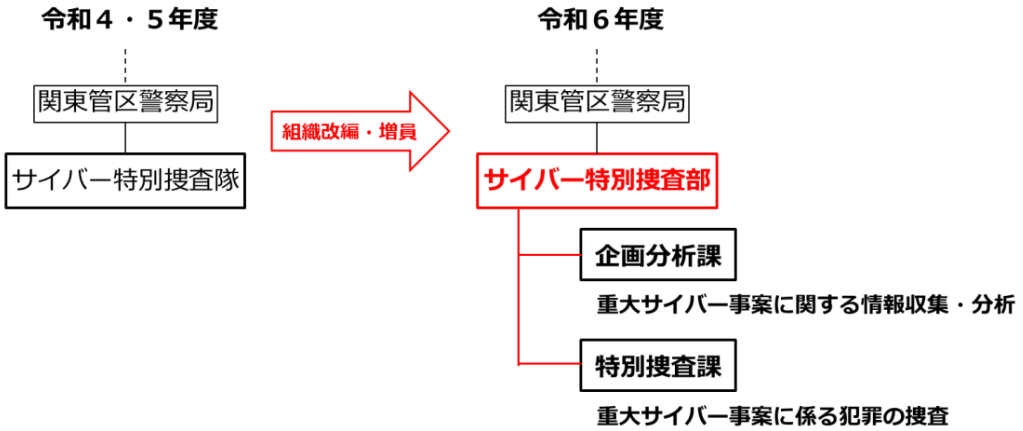


(2)　サイバー特別捜査部への発展的改組と今後の展望

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た。その結果、サイバー特別捜査部は、定員 129 名、情報技術解析部門の解析担当職員等の併任者を併せて総勢約 300 人強の体制となり、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等を行う体制が強化された（図表 22）。

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あわせて高度な分析・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。

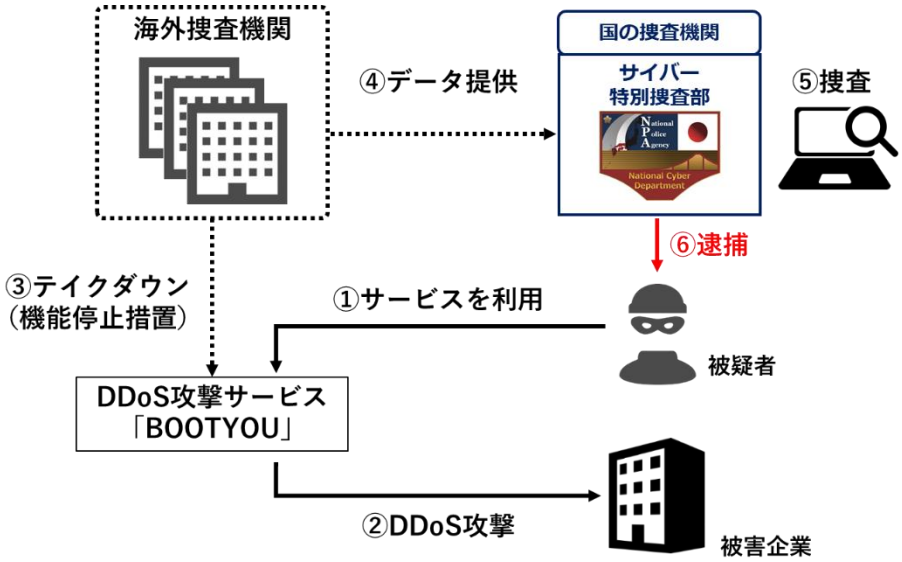
【図表 22：サイバー特別捜査部への発展的改組】



例えば、令和４年から５年にかけて全国で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係る捜査においては、関係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・分析するなどした結果、事案の全体像の解明や犯行グループの指示役とみられる人物の特定・逮捕に至った。本件は、サイバー特別捜査部が逮捕状の発付を得て被疑者を逮捕した初めての事件であるとともに、サイバー特別捜査部の高度な情報集約・分析機能が発揮された事例である（第２部２(2)参照）。

また、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。

【図表 23：事案概要】



今後、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、サイバー空間の匿名性を利用して敢行される様々な犯罪の捜査における全国警察の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すこととしている。

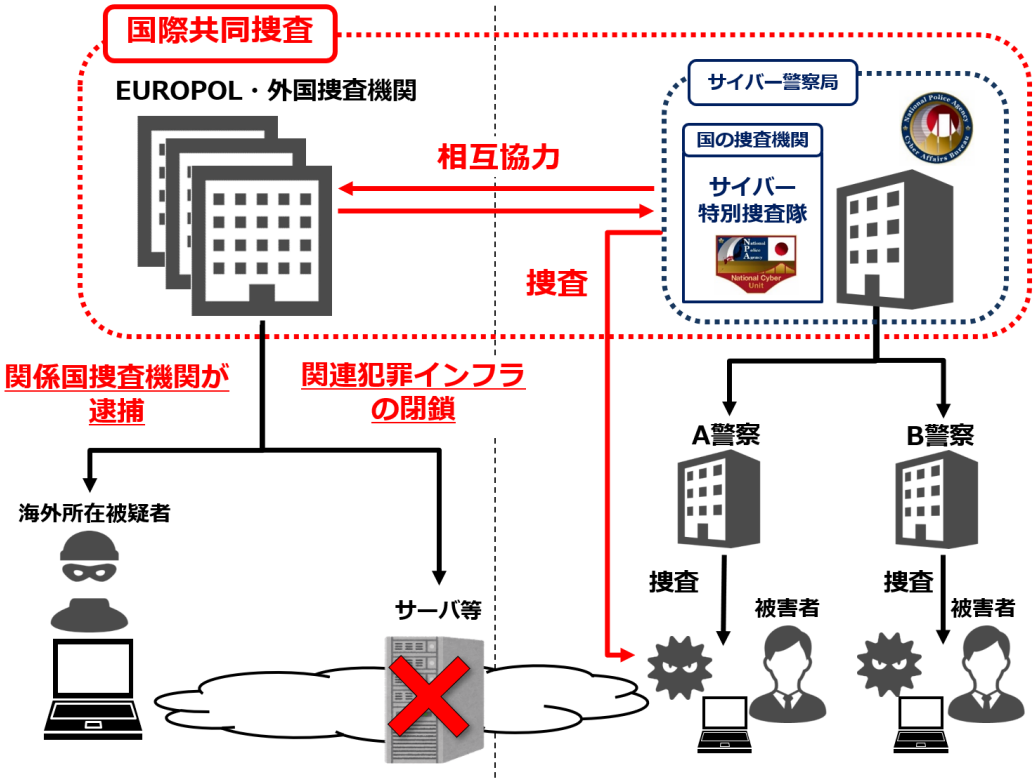
２　令和６年上半期の活動状況

(1)　外国捜査機関等と連携したランサムウェア事案被疑者の検挙・被害回復

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を推進した。その結果、令和６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。

【図表 24：事案概要】



【図表 25：スプラッシュページ】

(2) サイバー特別捜査部等合同捜査本部による不正送金事件の捜査

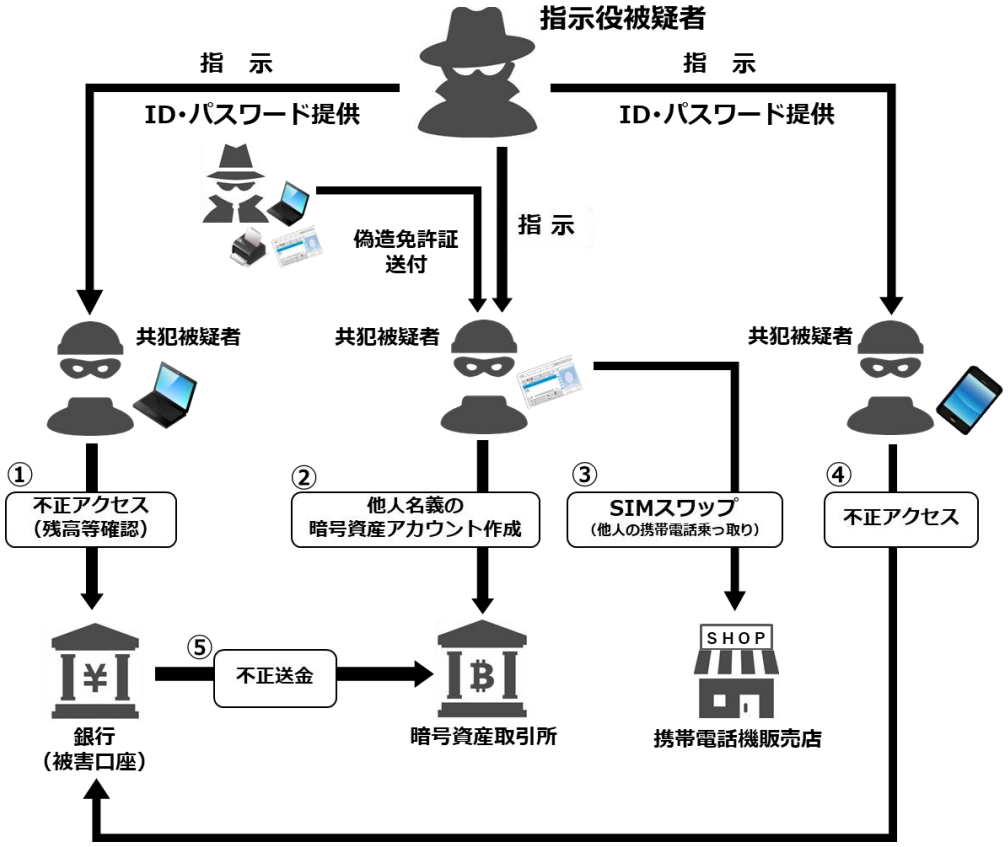
令和４年から５年にかけて発生したインターネットバンキングに係る不正送金事件について、関係都道府県警察による長期にわたる捜査を通じて得られた情報をサイバー特別捜査部が集約・分析するとともに、暗号資産の追跡捜査や関係被疑者の SNS アカウントに係る捜査等を実施した。

その結果、同一の犯行グループが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人物を特定した。

令和６年７月、関東管区警察局及び 16 都道府県警察（警視庁、広島、北海道、宮城、茨城、群馬、千葉、静岡、大阪、兵庫、奈良、岡山、愛媛、福岡、長崎、熊本）の合同捜査本部は、犯行グループの指示役とみられる男（44 歳）を不正アクセス禁止法違反（不正アクセス行為）で逮捕した。

合同捜査本部による捜査により、同グループによる被害件数及び被害額は、少なくとも 20 件・１億 2,000 万円に上ることが明らかになっている。

【図表 26：事案概要】



● 合同捜査本部による本件手口等の実態解明

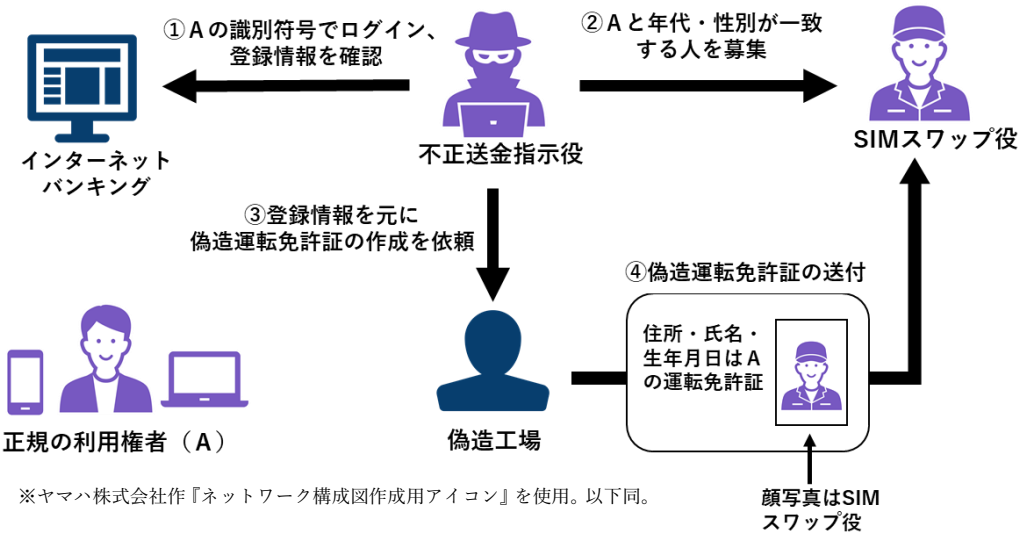
本件においては、インターネットバンキングで送金する際に登録した電話番号宛てに送られてくる SMS 認証による本人確認を回避するため、SIM スワップという手口が利用されていた。

本件における正規の利用権者の多くはフィッシング被害に心当たりがなかったことから、インターネットバンキングの識別符号(ID やパスワード)は情報窃取型の不正プログラムにより窃取された可能性がある。

また、指示役は、ダークウェブ上に存在するマーケット等で流通していたインターネットバンキングの識別符号を入手した上で、これを利用して不正にログインした後、口座の登録情報から正規の利用権者の個人情報を SIM スワップの際に利用するために入手した可能性がある。

さらに、指示役は、SNS 上で、副業を紹介するなどと称して募集を行い、応募者のうち利用権者と年齢等が近い者には SIM スワップの実行役（以下「SIM スワップ役」という。）を担わせ、さらに別の応募者には、利用権者の氏名等が記載され、SIM スワップ役の顔写真が印刷されている偽造運転免許証を準備させていた。

【図表 27：SIM スワップの準備】

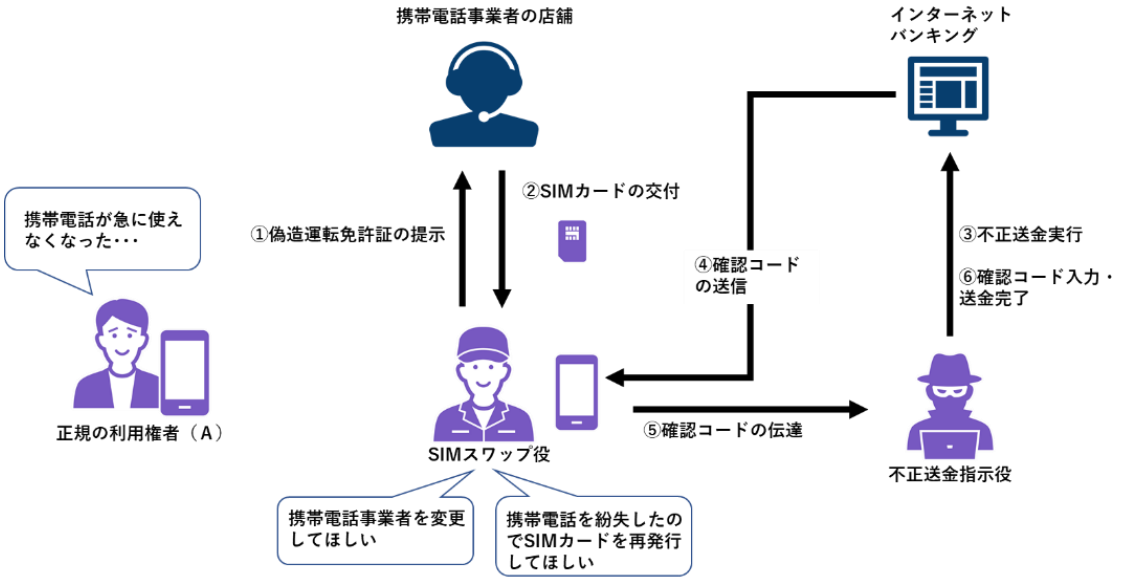


※ヤマハ株式会社作『ネットワーク構成図作成用アイコン』を使用。以下同。

SIM スワップ役は、正規の利用権者が契約する携帯電話事業者の店舗に赴き、偽造運転免許証を提示した上で、「携帯電話事業者を変更したい。」、「携帯電話を紛失したので SIM カードを再発行したい。」などと店員に伝え、正規の利用権者の携帯電話番号を乗っ取っていた。

携帯電話番号の乗っ取り完了後は、送金時の SMS 認証による本人確認のための確認コードは SIM スワップ役の携帯電話に送信されることとなり、SIM スワップ役が指示役等に確認コードを伝達することで、不正送金が実行された。

【図表 28：SIM スワップ及び不正送金】



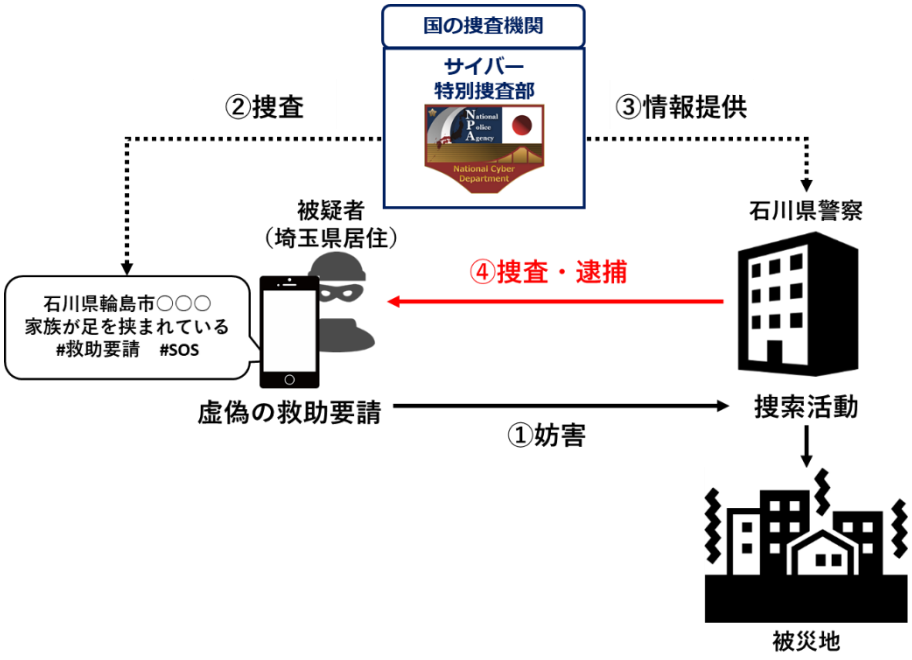
このように、不正送金の巧妙な手口も確認されていることから、合同捜査本部においては、引き続き、不正送金事案の捜査及び実態解明に努めている。

(3) 能登半島地震の偽情報投稿事案被疑者の検挙（再掲）

令和６年１月１日に発生した能登半島地震においては、被災地の警察が捜索活動等に全力を挙げる中、SNS 上において虚偽の救助要請が拡散し、捜索活動等が妨害される事態が生じていた。そうした状況の中、サイバー特別捜査隊（当時）は、各種情報収集を通じて SNS 上で偽の救助要請が行われている疑いを把握し、被災地の警察と連携しながら、関連アカウントに関する所要の捜査を実施した。

石川県警察は、サイバー特別捜査隊の捜査結果を踏まえて更なる捜査を実施した結果、地震当日に被災者を装って SNS 上に救助を求める虚偽の内容を投稿し、本来不要な捜索活動等を警察に実施させてその業務を妨害した会社員の男（25 歳）を特定して、偽計業務妨害罪で逮捕した（令和６年７月）。

【図表 29：事案概要】



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６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６年上半期における主なサイバー攻撃事例

● **情報窃取を企図したとみられる不正アクセス**

令和６年３月、大手システム事業者は、業務上使用する複数のコンピュータが不正プログラムに感染し、個人情報や顧客情報を含むファイルが不正に持ち出せる状況になっていたと発表した。

● **情報窃取を企図したとみられる不正アクセス（その２）**

令和６年３月、半導体関連機器事業者は、同社のサーバ等が第三者による不正アクセスを受けた可能性があると発表した。

● **重要インフラの機能に影響を及ぼしたサイバー攻撃**

令和６年５月、大手鉄道事業者は、インターネット上の乗車券等の予約サービスを提供するウェブサイト、スマートフォンの IC 乗車券サービスを提供するアプリケーション等に接続しづらい状況となっていることを発表した。

● **DDoS 攻撃による被害とみられるウェブサイトの閲覧障害**

令和５年 12 月から翌年４月にかけて、DNS 権威サーバを狙ったランダムサブドメイン攻撃[2]によるとみられるウェブサイトの閲覧障害が断続的に発生した。

● **DDoS 攻撃による被害とみられるウェブサイトの閲覧障害（その２）**

令和６年２月、政府機関、自治体、民間事業者等が運営するウェブサイトにおいて閲覧障害が発生した。同じ頃、SNS 上に、ハクティビストのものと思われる複数のアカウントから、それらの犯行をほのめかす投稿が確認された。

[2] ランダムサブドメイン攻撃：攻撃者がランダムな文字列等を使用して特定のドメインに対する多数のサブドメイン名を生成し、DNS サーバへ名前解決要求を行うことで、攻撃対象とされたドメインの DNS 権威サーバに対して問合せを集中させる攻撃。

（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６年上半期における主なサイバー攻撃事例②

● 出版大手企業に対するランサムウェア攻撃

令和６年６月、出版大手企業は、同社のサーバがランサムウェアを含む大規模な攻撃を受けたと発表した。この攻撃により、同社が提供するウェブサービスが広く停止したほか、書籍の流通等の事業に影響が発生した。同年８月、同社は、この攻撃により 25 万人分を超える個人情報や企業情報が漏えいしたことが確認されたこと及び同年度決算において、調査・復旧費用等として 30 億円を超える損失を計上する見込みであることを発表した。

● 情報処理サービス企業に対するランサムウェア攻撃

令和６年５月、自治体等から印刷業務等を受託する企業は、同社のサーバがランサムウェアに感染し、データが暗号化される被害が発生したと発表した。同年７月、同社は、この攻撃により個人情報が漏えいしたことが確認されたと発表した。

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）

悪用の危険性の高い重大なぜい弱性

１　悪用の危険性の高い重大なぜい弱性の例[3]

● **Ivanti 社：VPN 製品及びネットワークアクセス制御製品**

令和６年１月、Ivanti 社は、同社の VPN 製品である Ivanti Connect Secure 及びネットワークアクセス制御製品である Ivanti Policy Secure ゲートウェイについて、それらのぜい弱性（CVE-2023-46805 及び CVE-2024-21887）[4]に関する情報を公開した。

● **Fortinet 社：次世代ファイアウォール製品及び Web プロキシ製品**

令和６年２月、Fortinet 社は、同社の次世代ファイアウォール製品に搭載されている FortiOS 及び Web プロキシ製品である FortiProxy におけるぜい弱性（CVE-2024-21762）[5]に関する情報を公開した。

● **Palo Alto Networks 社：次世代ファイアウォール製品**

令和６年４月、Palo Alto Networks 社は、同社の次世代ファイアウォール製品に搭載されている PAN-OS ソフトウェアにおけるぜい弱性（CVE-2024-3400）[6]に関する情報を公開した。

● **Check Point Software Technologies 社：次世代ファイアウォール製品**

令和６年５月、Check Point Software Technologies 社は、同社の次世代ファイアウォール製品の VPN 機能におけるぜい弱性（CVE-2024-24919）[7]に関する情報を公開した。

---

[3] 悪用されるとネットワーク機器に侵入されるおそれがある重大なぜい弱性に関する情報が令和６年上半期、複数公表されており、国内又は海外でこれらのぜい弱性を悪用する攻撃が発生したと公表されている。該当製品を使用している場合、サイバー攻撃の被害を防止するために確実な対処が必要である。

[4] https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

[5] https://www.fortiguard.com/psirt/FG-IR-24-015

[6] https://security.paloaltonetworks.com/CVE-2024-3400

[7] https://support.checkpoint.com/results/sk/sk182336

（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）

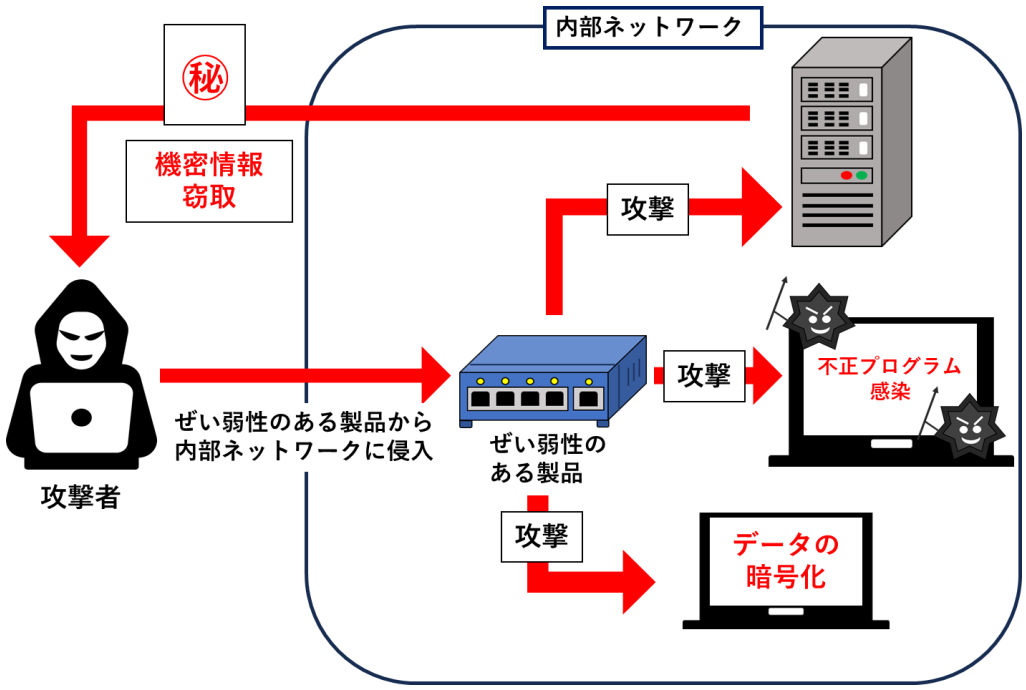
悪用の危険性の高い重大なぜい弱性②

２　危険性と対策

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、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は、その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[8]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ほか、平素からぜい弱性情報やアップデートに関する情報を確認し、対処することが必要である。また、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】

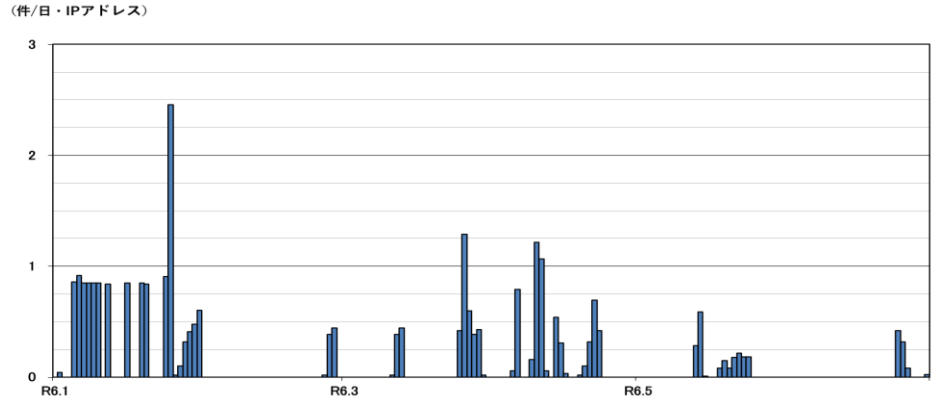


[8] ぜい弱性の内容や対策方法をまとめた文書

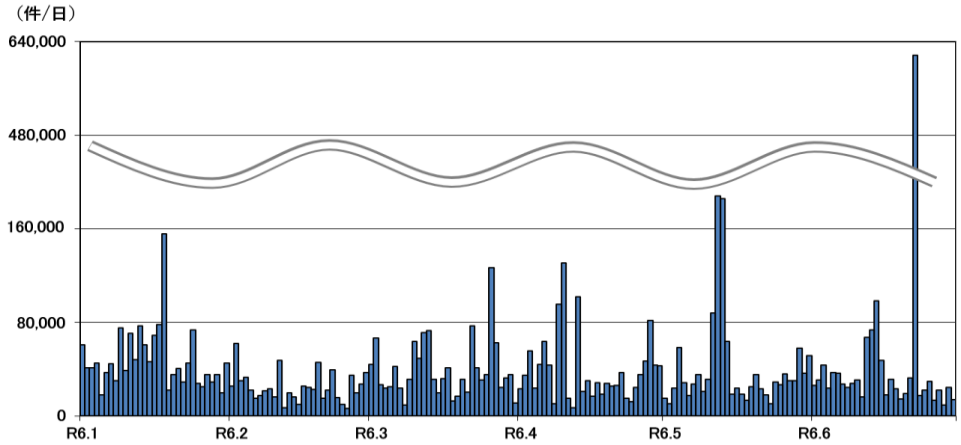
コラム１　令和６年上半期における DNS サーバを標的とした特徴的な観測

DNS サーバのうち、外部の不特定の IP アドレスからの再帰的な問合せ[9]に回答する特性を持つオープンリゾルバは、DDoS 攻撃の踏み台として悪用されることがある。近年、対策が進み、国内のオープンリゾルバは減少傾向にあるものの、対策済みとされる DNS サーバの中には、送信元 IP アドレスを偽装することにより再帰的な問合せが可能となるものが存在し得るところ、そのような DNS サーバを調査する目的と思われるアクセスが観測されている。効果的な対策としては、送信元 IP アドレスを偽装したアクセスをファイアウォールなどでブロックすることが挙げられる。

【偽装した IP アドレスからの問合せに回答する DNS サーバを調査する目的と思われるアクセス件数の推移】



【警察庁の設置する観測システムにおける「.jp」をトップドメインとするドメインに対する再帰的な問合せ件数の推移[10]】



[9] 問合せを受けた DNS サーバが他の DNS サーバに問合せを行い、その結果を回答する問合せ

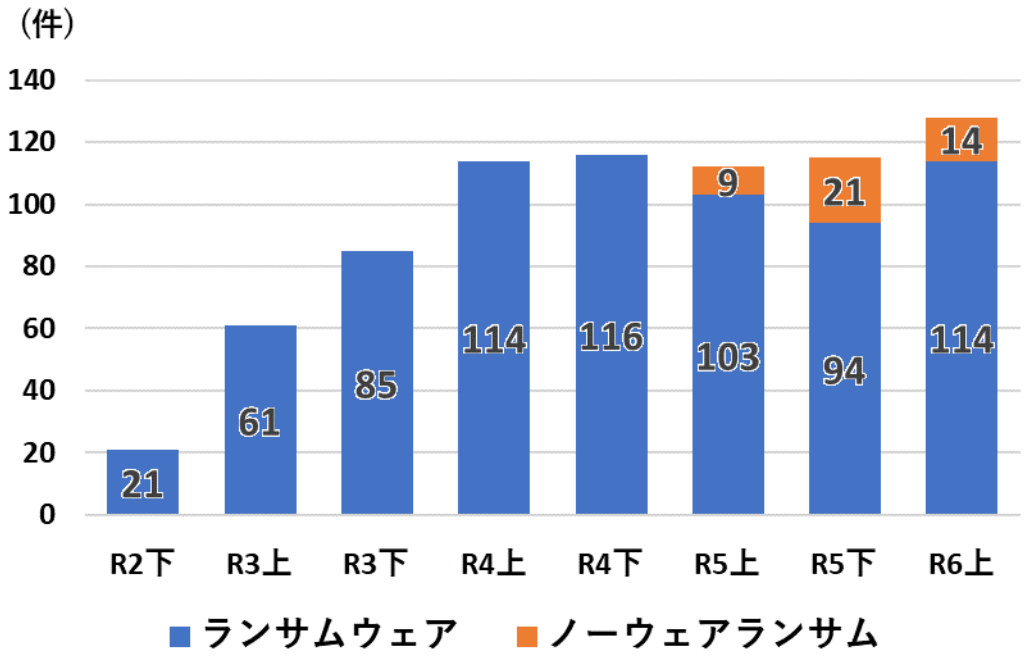
[10] 国の機関、地方自治体、国内企業等のドメインに対するランダムサブドメイン攻撃と思われるアクセスを観測

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）

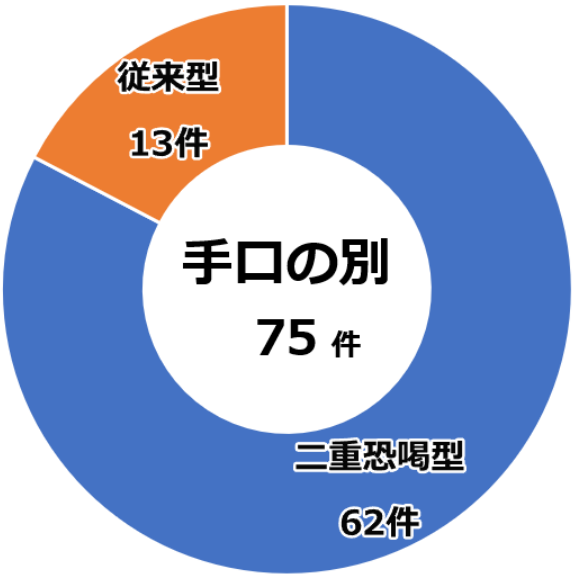
ランサムウェアの被害に係る統計

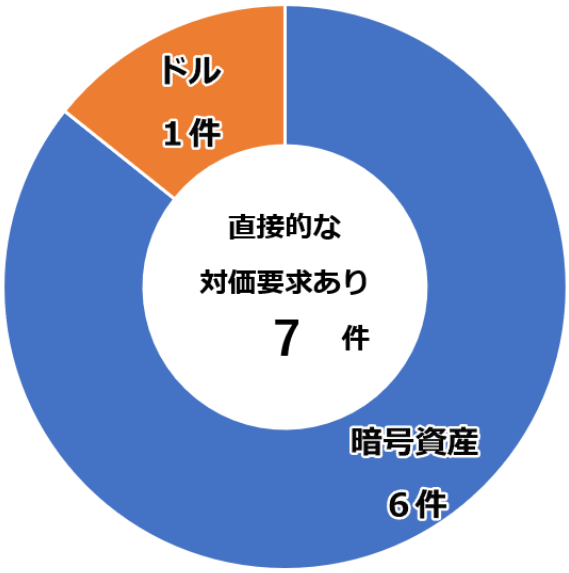
１　企業・団体等における被害の報告件数の推移



※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／要求された対価支払方法別報告件数

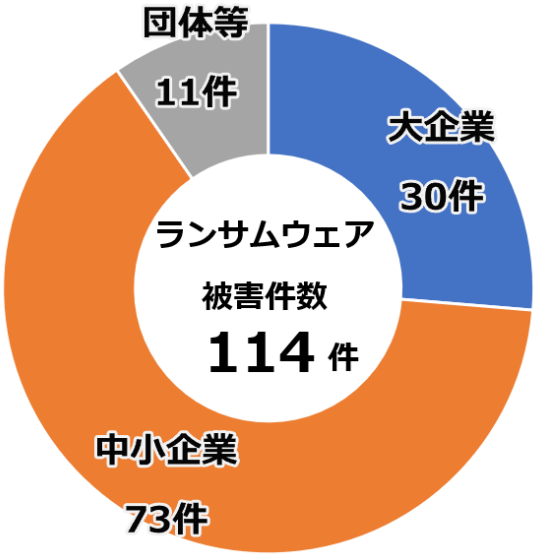


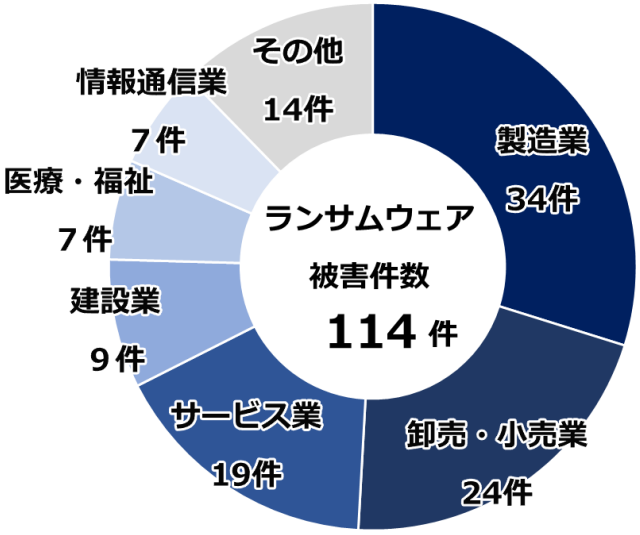


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

ランサムウェアの被害に係る統計②

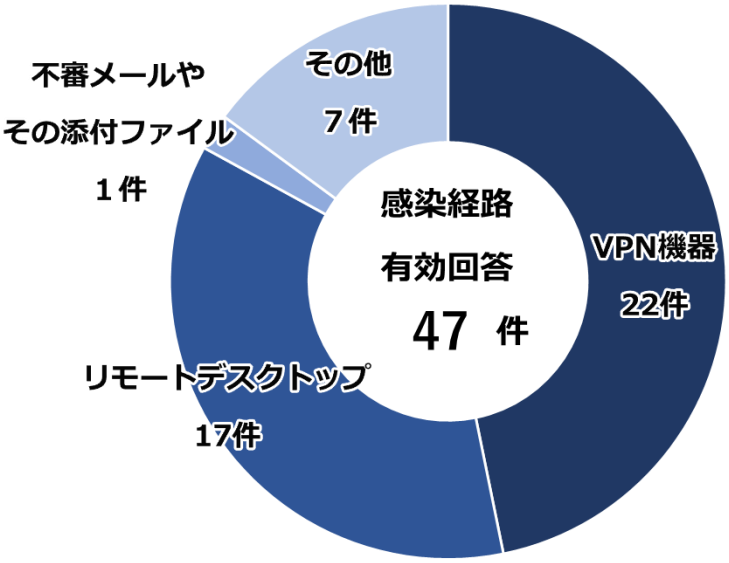
３　被害企業・団体等の規模別／業種別報告件数





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

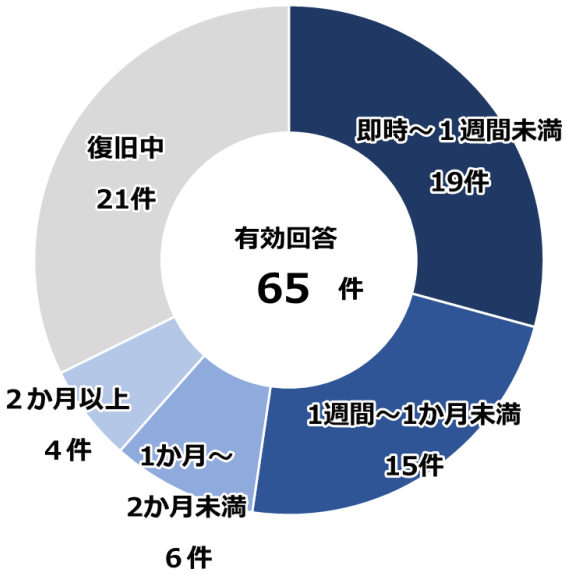
● 感染経路

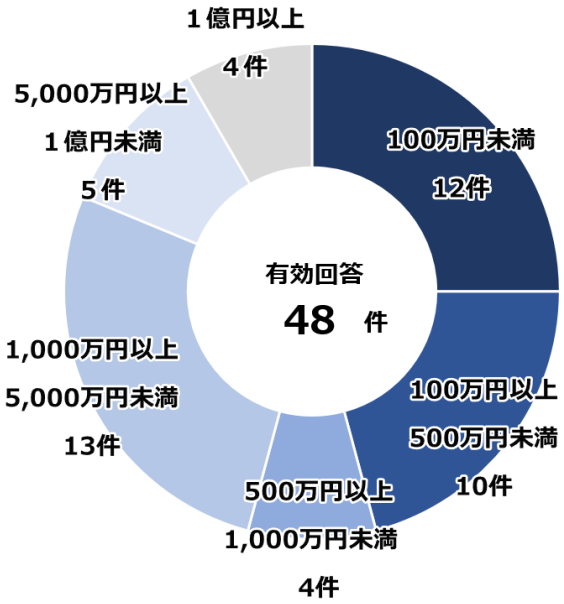


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

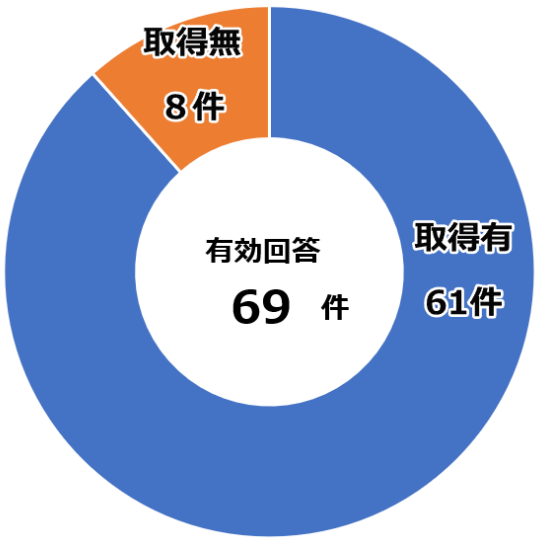
ランサムウェアの被害に係る統計③

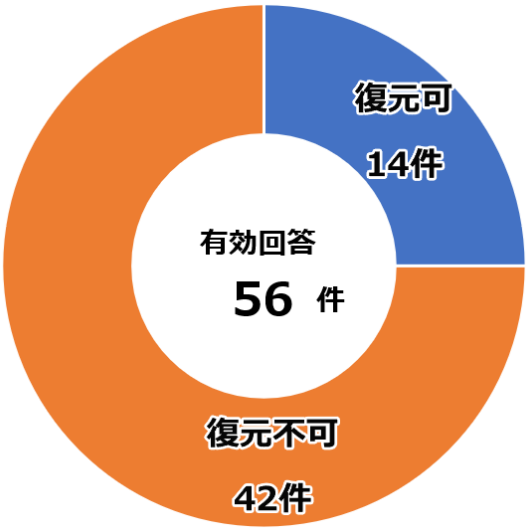
● 復旧等に要した期間／調査費用の総額





● バックアップの取得状況／バックアップからの復元結果

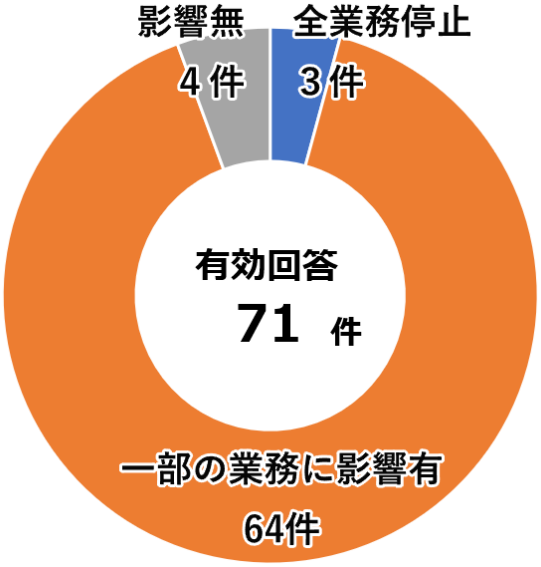


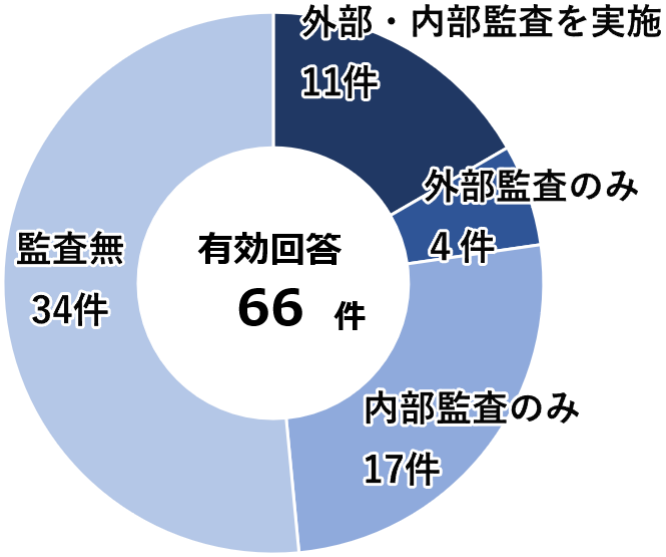


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

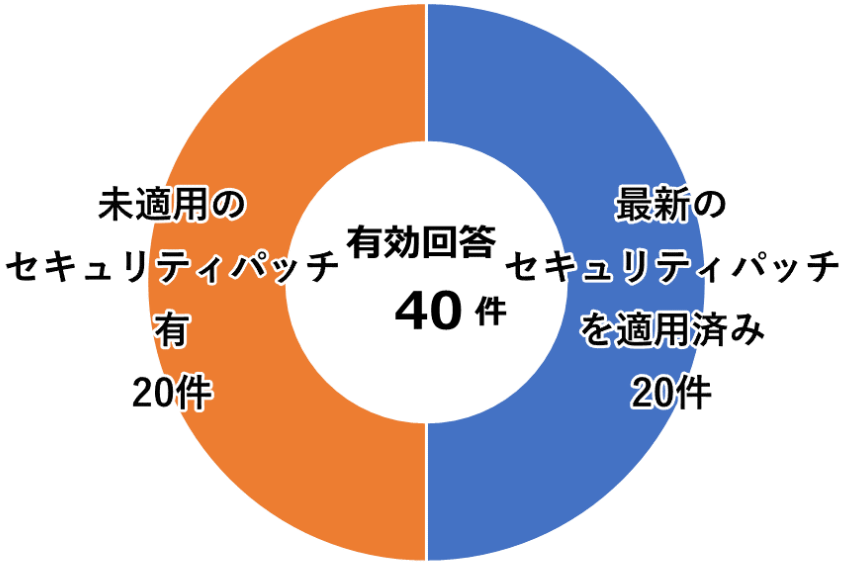
ランサムウェアの被害に係る統計④

● 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・団体の情報セキュリティ監査の実施状況





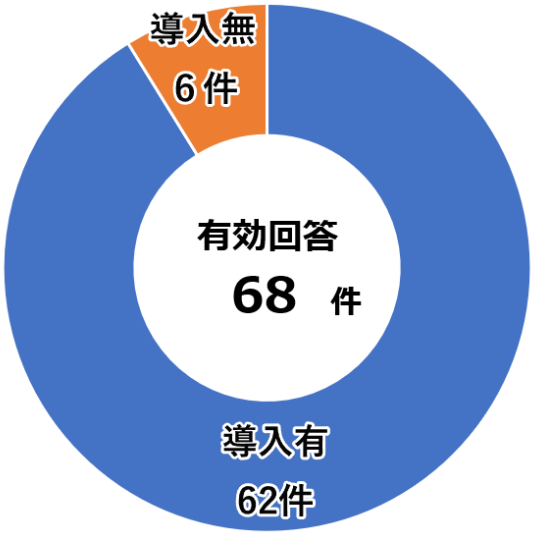
● 侵入経路とされる機器のセキュリティパッチの適用状況

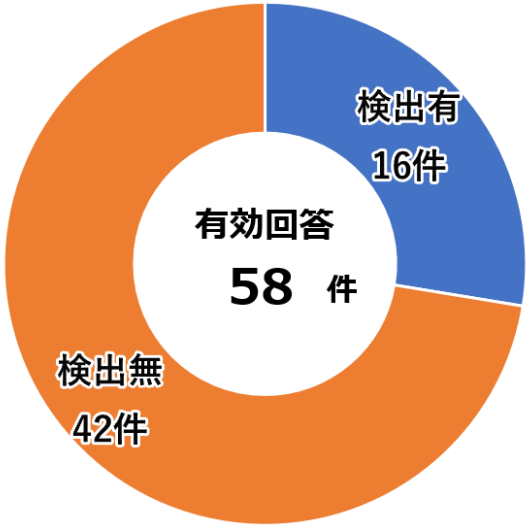


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

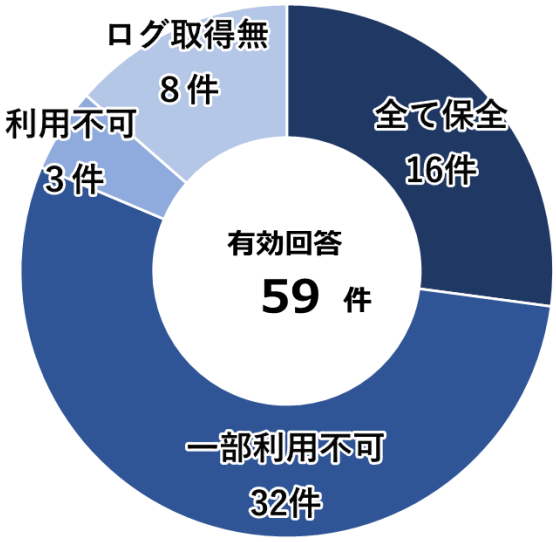
ランサムウェアの被害に係る統計⑤

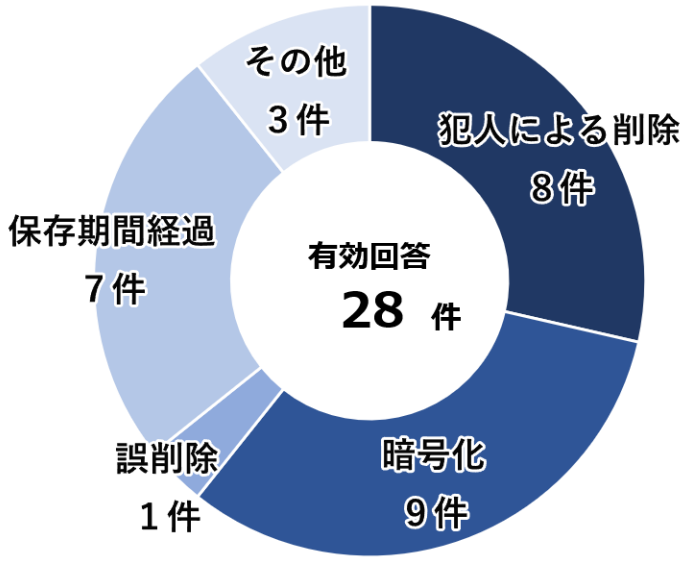
● 被害企業・団体等のウイルス対策ソフト等導入／活用状況





● ランサムウェア被害における被害企業・団体等のログの保全状況
／ログが使用できなくなっていた原因

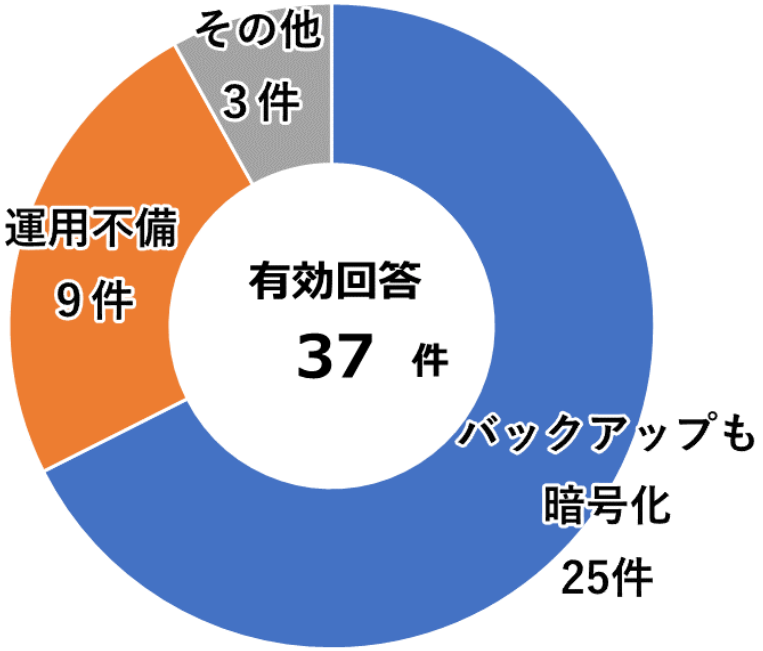




（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

ランサムウェアの被害に係る統計⑥

● 被害企業・団体のバックアップから復元できなかった理由



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）

高度な技術を悪用したサイバー攻撃に対する警察の取組

１　サイバー攻撃関連

●　共同対処訓練の継続的な実施

令和６年上半期には、自治体、電力事業者、金融機関等の幅広い分野の事業者等を対象に、標的型メールを題材とした訓練や警察との連携を確認するための現場臨場訓練等の実践的な共同対処訓練を約 380 回実施した。

●　サイバーインテリジェンス情報共有ネットワーク（CCI ネットワーク）

警察及び全国約 8,700 の事業者等から構成されるサイバーインテリジェンス情報共有ネットワークの枠組みを通じて、情報窃取を企図したとみられるサイバー攻撃に関する各種情報を集約するとともに、これらの情報を総合的に分析して、事業者等に対し注意喚起を実施している。

●　C2 サーバのテイクダウン

サイバー攻撃事案で使用された不正プログラムの解析等を通じて C2 サーバとして機能している国内のサーバを把握し、C2 サーバがテイクダウン（機能停止）されるよう、サーバ管理事業者等に依頼している。

●　重要インフラ事業者等に対する継続的な注意喚起

令和６年上半期には、ネットワーク機器やソフトウェアの重大なぜい弱性を悪用したサイバー攻撃の手口に関して全国の重要インフラ事業者等に注意喚起を実施したほか、海外の関係機関・団体から入手したサイバー攻撃等に関する情報を踏まえて個別に注意喚起を実施した。

（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）

高度な技術を悪用したサイバー攻撃に対する警察の取組②

●　サイバー脅威を緩和するための合同ガイダンス

令和６年５月、警察庁及び内閣サイバーセキュリティセンター（NISC）は、カナダ、エストニア、フィンランド及び英国の関係機関とともに、米国サイバーセキュリティ・インフラストラクチャー安全保障庁（CISA）が作成・公表した、サイバー攻撃の被害に遭う危険性が高い組織・個人向けのリスク緩和策に関する合同ガイダンスの共同署名に加わった。

【合同ガイダンスの内容】

①　学術界、シンクタンク、ジャーナリスト、NGO 等の人権保護や民主主義の推進に関与する組織・個人は、民主主義の価値や利益を損なおうとする「国家」を背景とするサイバー攻撃集団の攻撃対象となる危険性が高いと考えられている旨を言及。

②　産業界からの報告を引用して、「国家」を背景とするサイバー攻撃は主にロシア、中国、イラン及び北朝鮮の「政府」からのものである旨を指摘。

③　攻撃対象となる危険性の高い組織・個人に対して、サイバー攻撃の脅威を緩和するためのリスク緩和策を提言するとともに、ソフトウェア作成業者に対して、顧客のセキュリティに対する態勢改善を提言。

２　ランサムウェア関連

●　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。

●　リークサイト上において売買されるアクセス権の把握等

ダークウェブ上のリークサイトにおけるアクセス権の売買等を監視し、国内の事業者等のユーザ ID・パスワード等が掲載されていることを把握した場合は、都道府県警察を通じ、その旨を連絡し、必要な対策を講じるよう求めている。

（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）

高度な技術を悪用したサイバー攻撃に対する警察の取組③

３　AI を悪用したサイバー事案関連

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。

４　情報技術解析部門における不正プログラムの解析・研究状況

●　不正プログラムの解析結果及び危険性

犯罪捜査や被害拡大の防止等を目的に、警察庁において「XLoader」や「MoqHao」と呼ばれる Android スマートフォンを対象に感染する不正プログラムを解析したところ、「指定した電話番号宛やスマートフォンの連絡先に登録されている全ての電話番号宛に指定した内容の SMS を送信する機能」や「フィッシングページを表示する機能」等を持つことが判明した。

これらの不正プログラムは、スマートフォン使用者が気付くことなく勝手に SMS を送信できることから、SMS を利用したフィッシングへの悪用が懸念される。

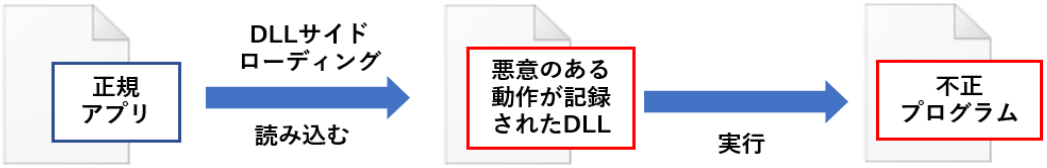
●　不正プログラムの感染経路及び感染対策

Android スマートフォンで SMS 等に記載されている URL にアクセスし、アプリのダウンロード及びインストールを行うことで、これらの不正プログラムに感染することとなる。

感染を防ぐには、SMS 等のリンクを無闇にクリックしない、公式サイト以外のアプリをインストールしないといった注意をする必要がある。また、感染していた場合、SMS の利用頻度に比して、通信料金が高額になっていることが想定され、通信料金の確認によって感染に気付くことが考えられる。

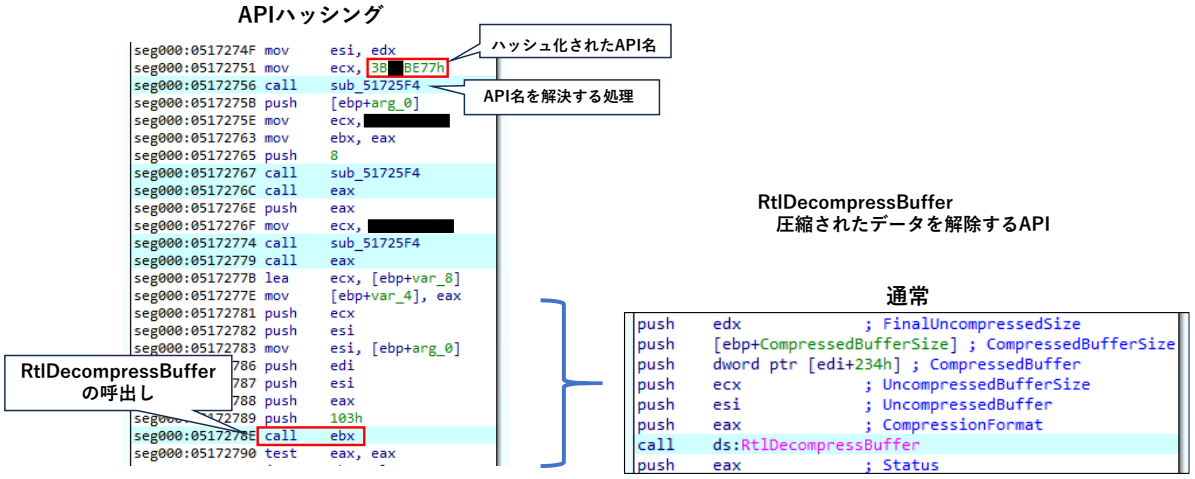
コラム２　不正プログラムの検出回避手法（DLL サイドローディング）

Windows で実行されるアプリ等のプログラムは、プログラムの実行に必要な情報が記録されている DLL というファイルを使用している。DLL サイドローディングとは、悪意のある動作が記録された DLL を正規のアプリから読み込ませ、不正プログラムを実行する手法である。ウイルス対策ソフトからは、正規のアプリが動作を実行しているように見えるため、検出が困難となる。



コラム３　不正プログラムの解析妨害手法（API ハッシング）

サイバー攻撃者は、Windows 等 OS の機能を利用するための仕組みである API の名前を難読化（ハッシュ化）し、解析者がプログラムコードを確認しただけでは、プログラムの機能を理解しにくいようにしている。



（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）

高度な技術を悪用したサイバー攻撃に対する警察の取組④

５　サイバーセキュリティに係る研究の推進

● 「関数のコールグラフに基づく解釈可能なマルウェアの分類手法」

機械学習を利用した不正プログラムの分類に関する研究であり、信頼性の高い分類を行う手法「FCGAT」（Function Call Graph and Attention Mechanism）を構築した。本手法により分類の根拠となるプログラム内の処理が示されるなど、解析に必要な時間の短縮が期待される。

● 「大規模言語モデル（LLM）を用いたバイナリコードの機能推定手法」

不正プログラムのバイナリコードを解析する際は、プログラムの作成時に使用されていた関数名及び変数名は判明しないことが多く、動作や機能の理解に時間を要する。本研究により、関数名推定の正確性を向上させたローカルLLM[11]である「RevLlama」（リブラマ、Reverse engineering Llamaの略）を構築した。本手法は、ローカルのサーバで動作可能であるため、ChatGPT等とは異なり、機密性の高い解析業務に活用可能である。推定された関数名により解析に必要な時間の短縮が期待される。

[11] LLM：人工知能の一種で、大量のテキストデータをもとに人間と同じように文章を理解し、自然に文字を生成できる。

（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）

国家安全保障戦略（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。

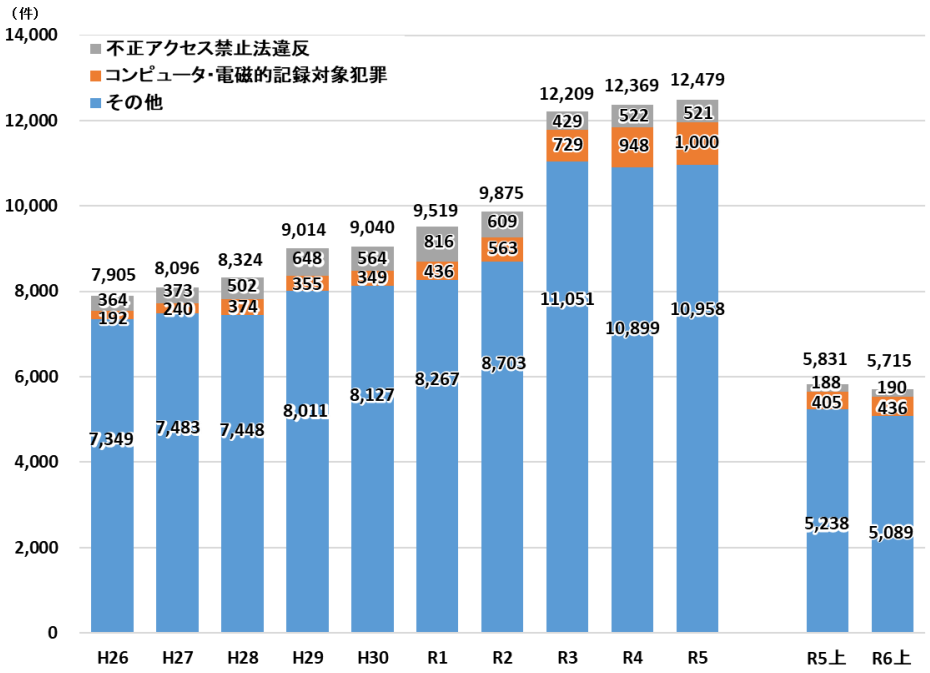
（ウ） 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

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。

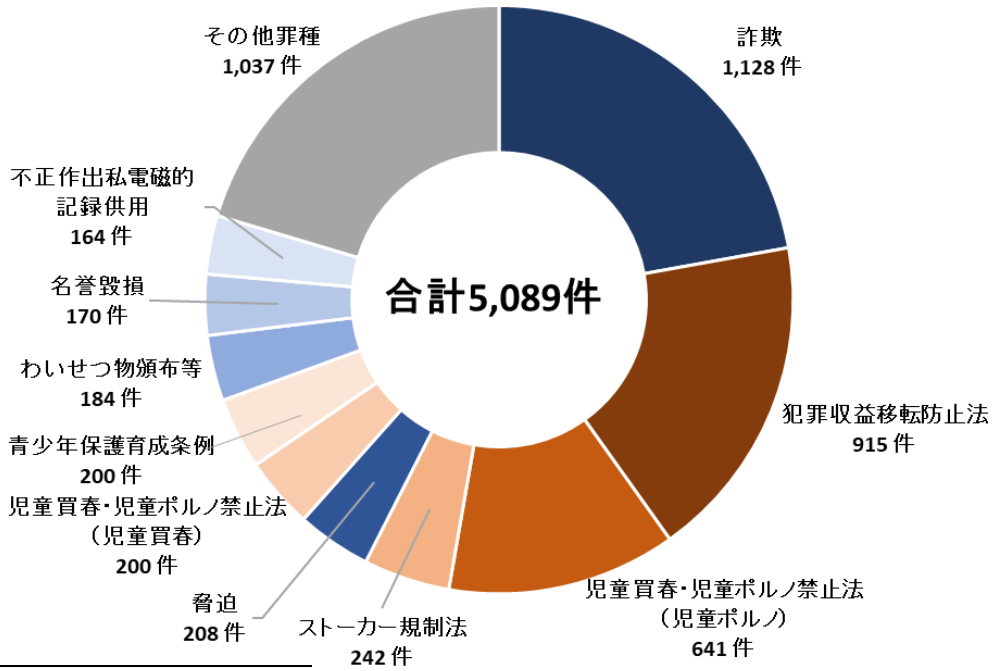
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計

１　サイバー犯罪[12]の検挙件数の推移



２　上記１中、「その他」の検挙状況

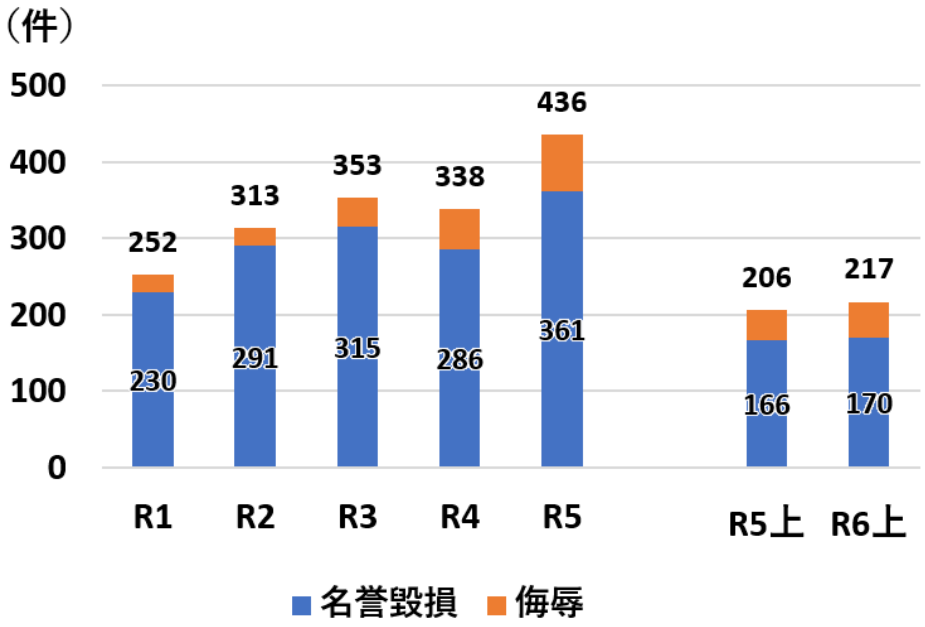


[12] 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

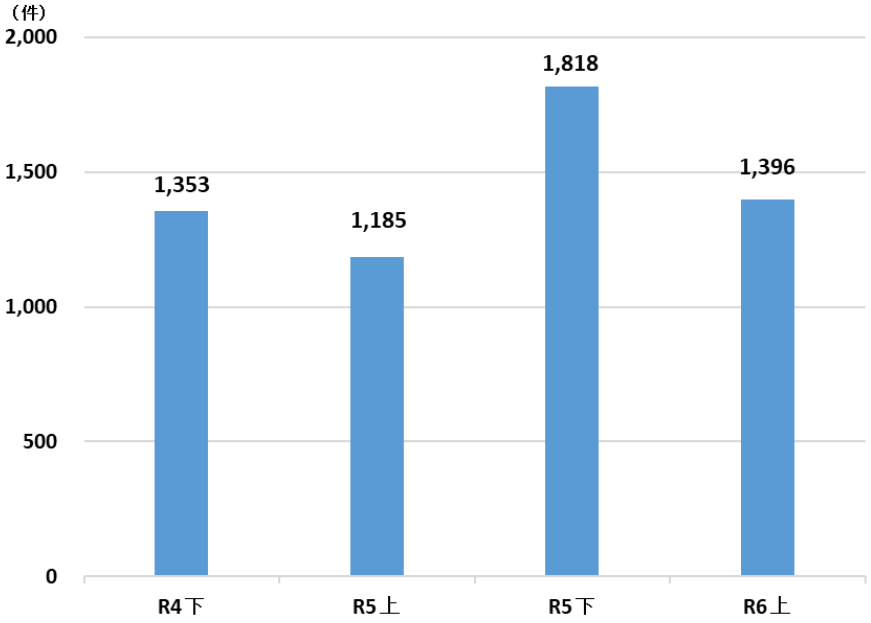
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計②

３　名誉毀損罪・侮辱罪の検挙件数の推移



４　サイバー事案[13]の検挙件数の推移



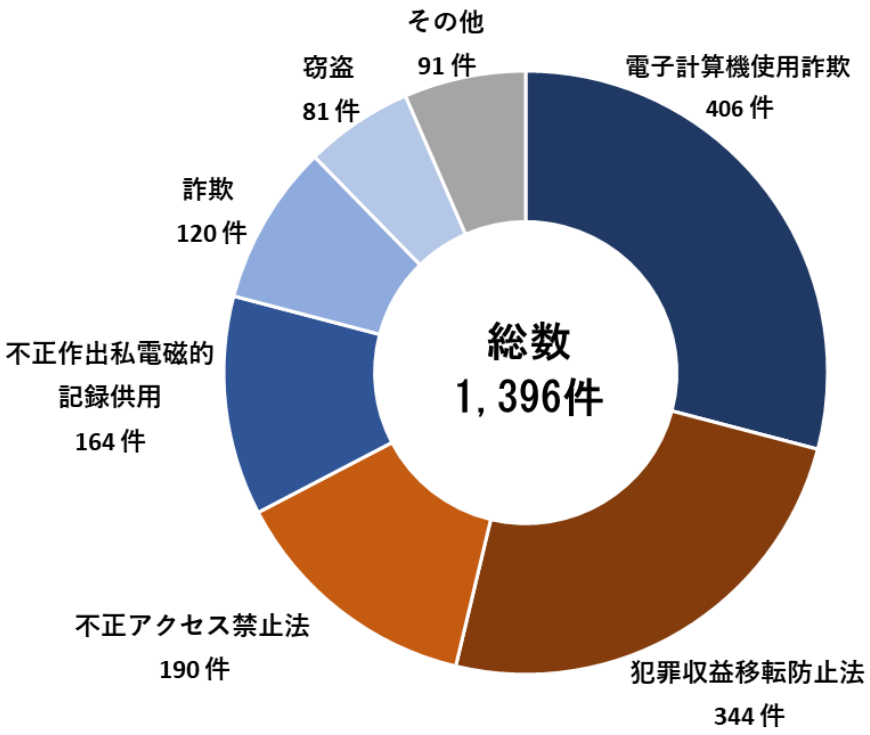
[13] サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。

資料編

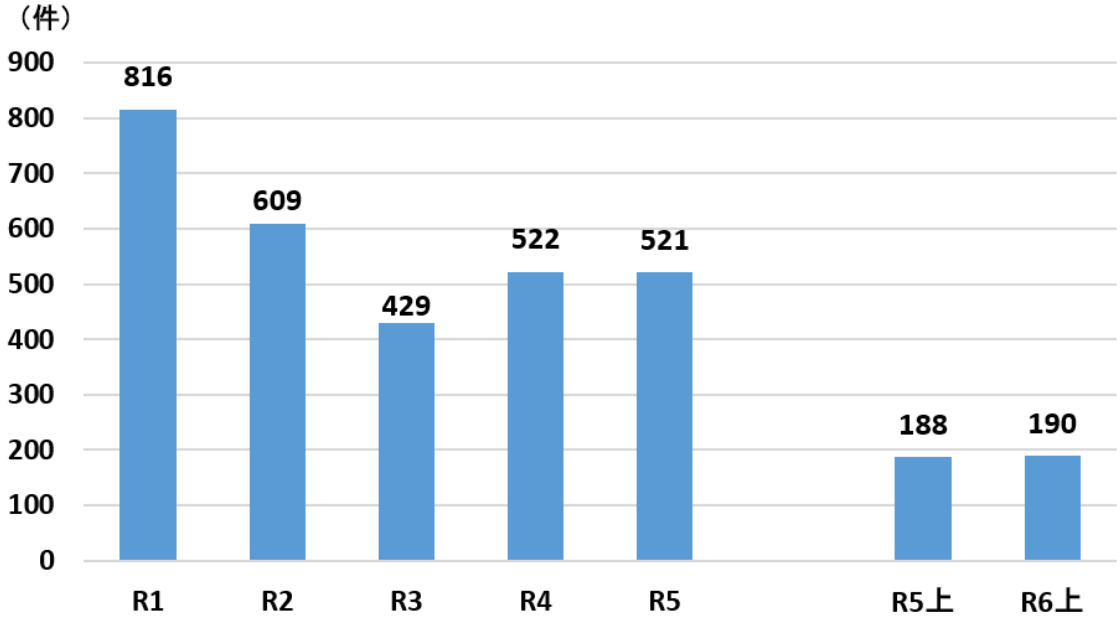
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計③

５　サイバー事案の検挙状況



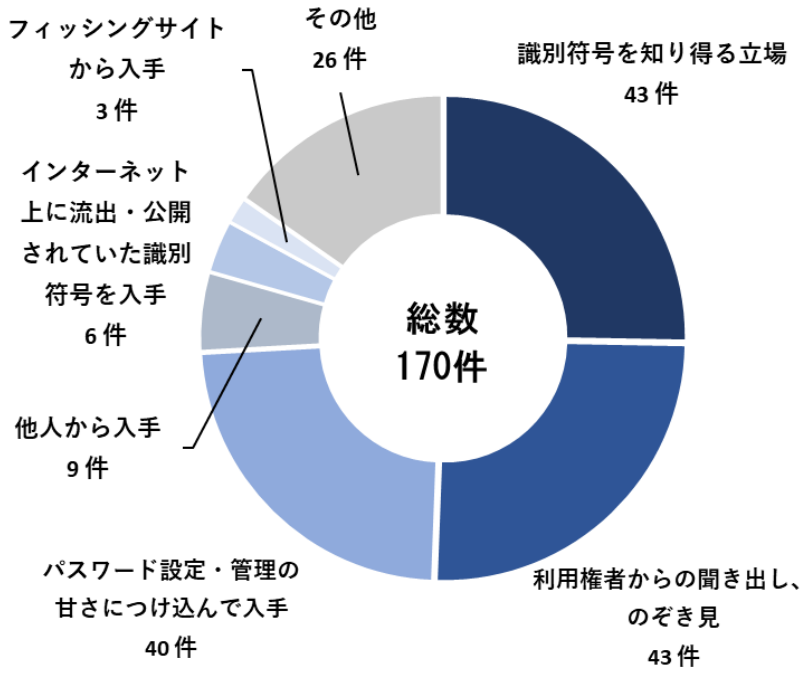
６　不正アクセス禁止法違反の検挙件数の推移



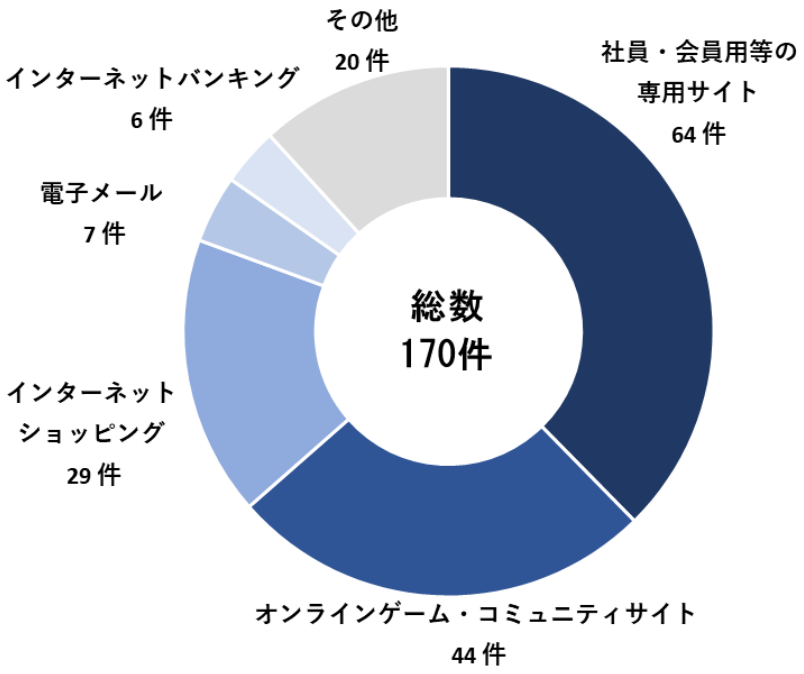
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計④

７　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



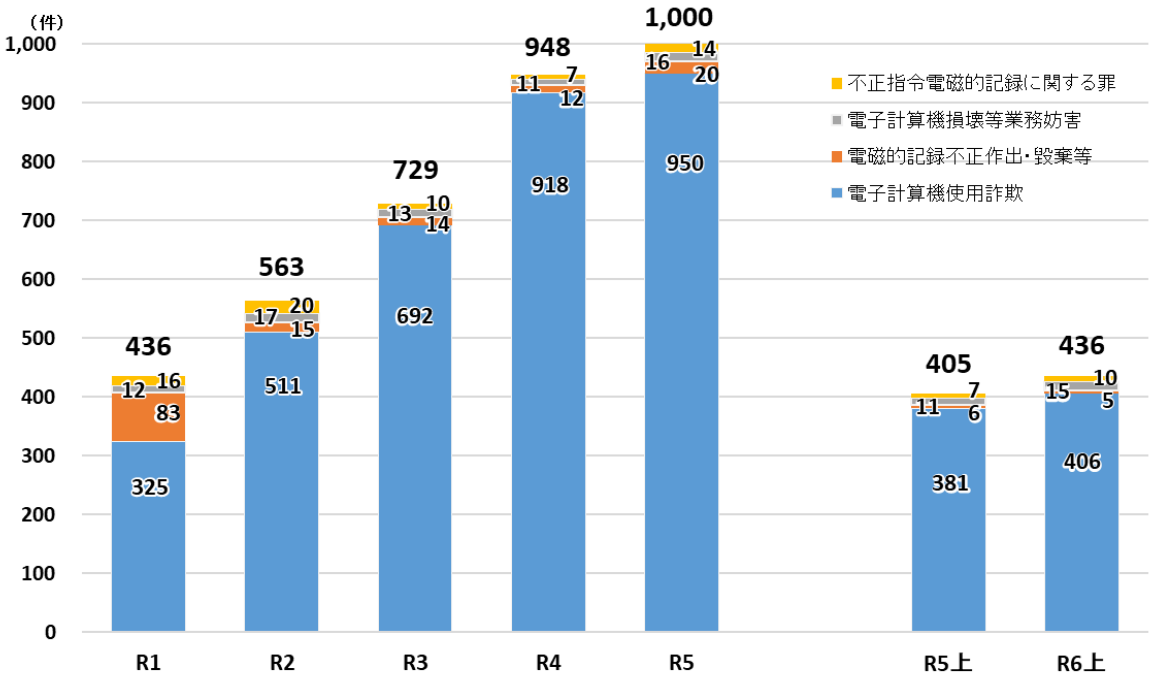
８　不正に利用されたサービス別検挙件数（識別符号窃用型）



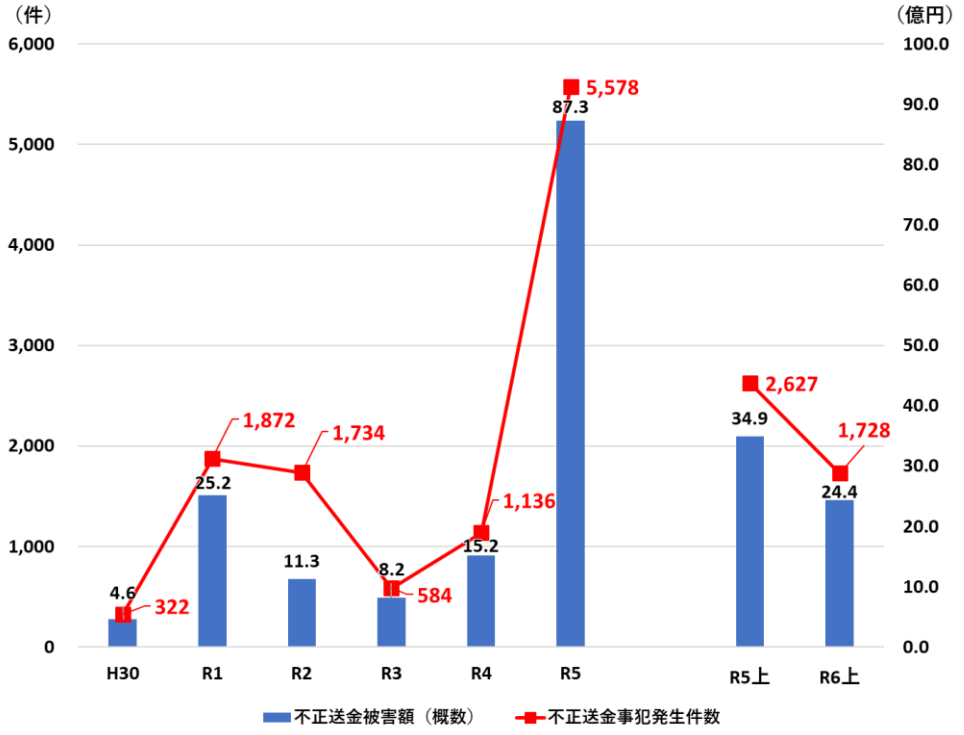
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計⑤

９　コンピュータ・電磁的記録対象犯罪の検挙件数の推移



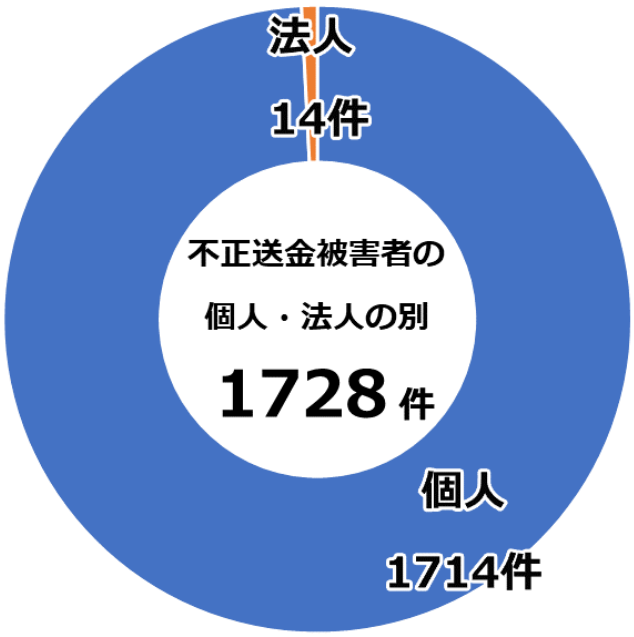
10　インターネットバンキングに係る不正送金事犯発生件数及び被害額の推移



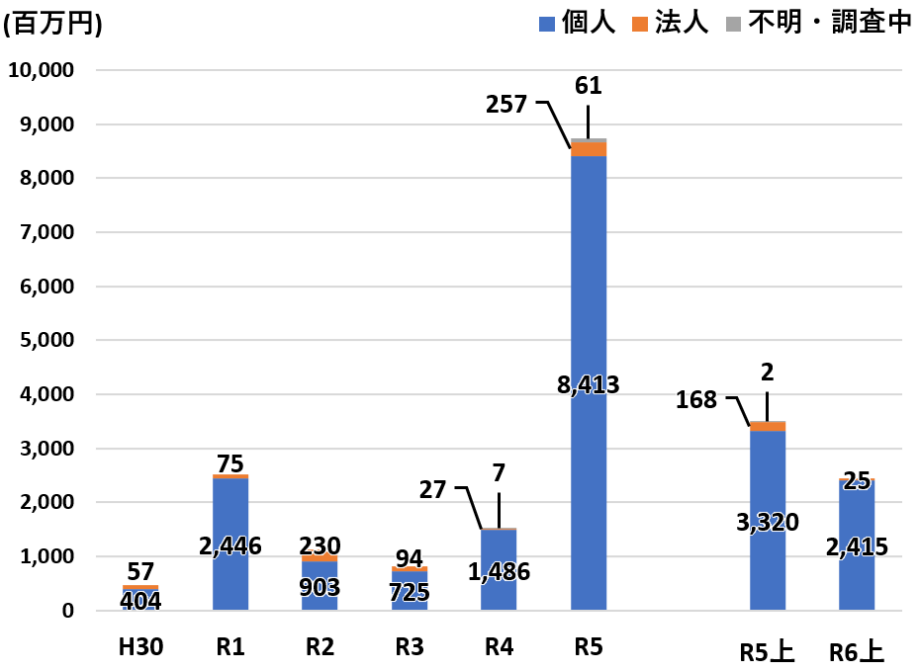
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計⑥

11　インターネットバンキングに係る不正送金被害件数（個人・法人別）



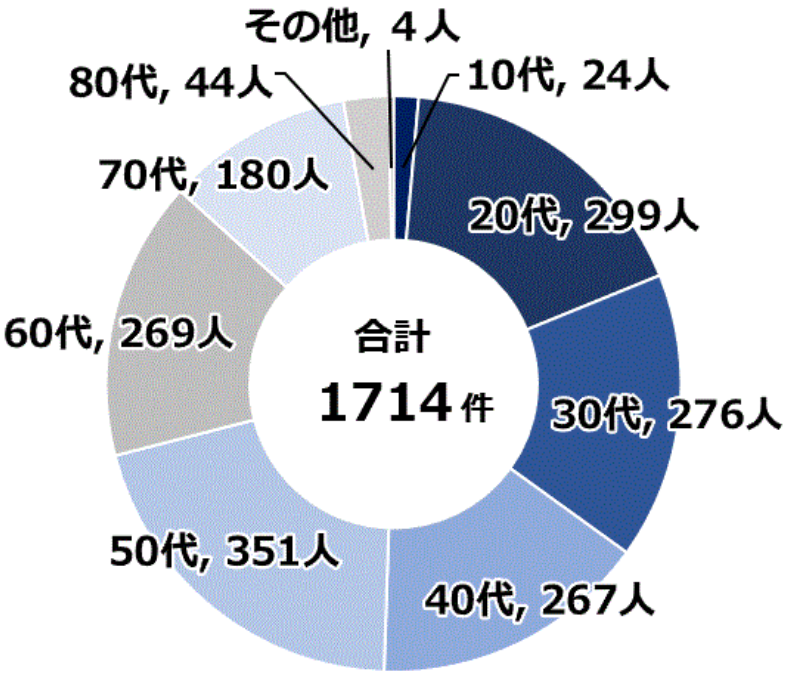
12　インターネットバンキングに係る不正送金被害額の推移（個人・法人別）



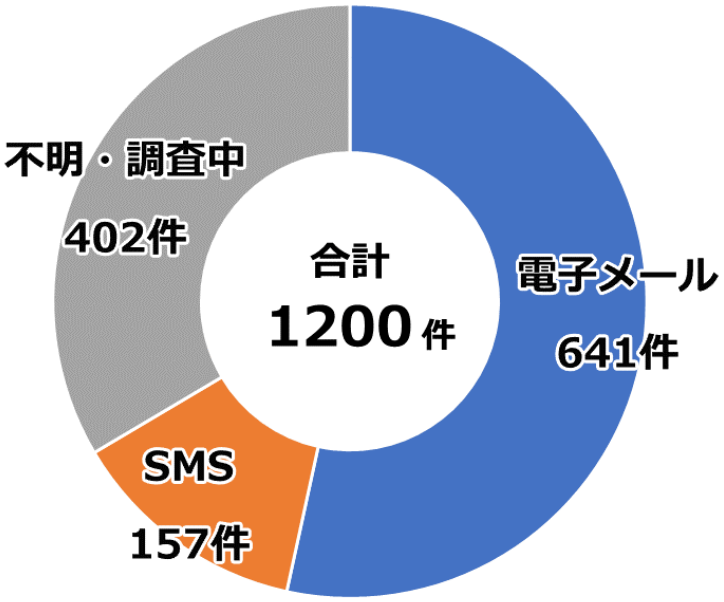
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計⑦

13　個人のインターネットバンキングに係る不正送金被害者の年齢別割合



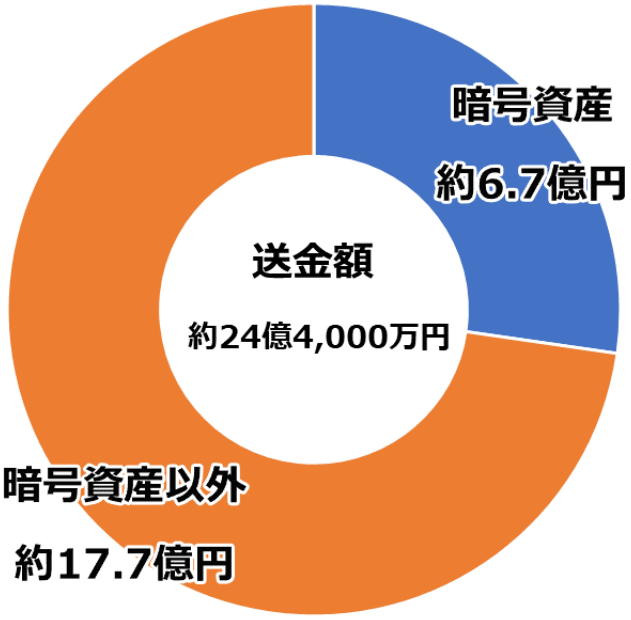
14　フィッシングサイトへ誘導する手口別割合



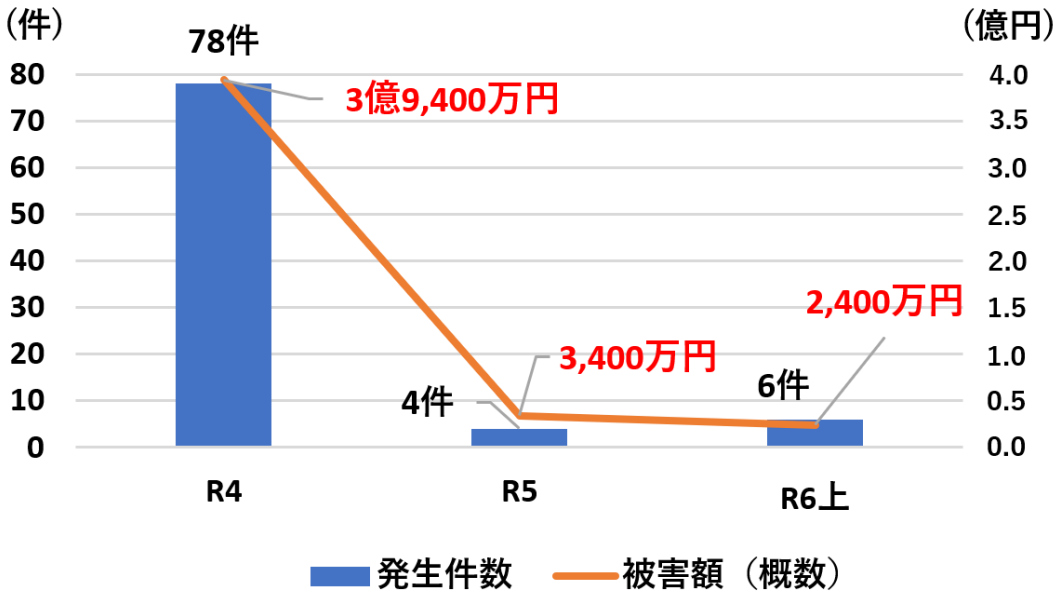
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネット空間を悪用した犯罪に係る脅威情勢に関する統計⑧

15　暗号資産交換業者の金融機関口座への不正送金状況



16　ＳＩＭスワップに係る不正送金発生状況



（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）

インターネット空間を悪用した犯罪に係る脅威情勢に対する警察の取組

●　「キャッシュレス社会の安全・安心の確保に関する検討会」を踏まえた対応

警察庁では、「キャッシュレス社会の安全・安心の確保に関する検討会」を開催し、金融業界、EC 業界、法曹界、学術界及びセキュリティ関係団体の有識者による議論の結果について、令和６年３月、報告書を取りまとめた。

●　次世代認証技術の普及促進

次世代認証技術の１つであるパスキー[14]について、採用済みの事業者等における効果等を踏まえ、金融機関や EC 加盟店等のサービスにおける採用や、当該サービスの利用者に働き掛けるなど、普及を促進する取組を実施している。

●　SIM スワップ 対策

令和５年５月以降確認されていなかった SIM スワップによる不正送金事案が、令和６年に入り再び確認されたことなどから、同年５月、総務省と連携し、携帯電話事業者に対して本人確認の強化を要請した（令和４年９月以降２度目）。

●　「国民を詐欺から守るための総合対策」に基づいた各種施策の推進

「国民を詐欺から守るための総合対策」（令和６年６月 18 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（概要は次ページ。）。

[14] パスワードが不要で生体認証等を利用する認証技術。フィッシングサイト等の正規サイト以外のウェブサイトにおいては認証が機能しないといった観点から認証情報の漏えいリスクを低減できる効果があるとされている。

「国民を詐欺から守るための総合対策」における主な施策
（項目抜粋）

1.「被害に遭わせない」ための対策

ＳＮＳ型投資・ロマンス詐欺対策

- **被害発生状況等に応じた効果的な広報・啓発等**
- ＳＮＳ事業者等による実効的な広告審査等の推進
- **なりすまし型偽広告の削除等の適正な対応の推進**
- **大規模プラットフォーム事業者に対する削除対応の迅速化や運用状況の透明化に係る措置の義務付け等**
- 知らない者のアカウントの友だち追加時の実効的な警告表示・同意取得の実施等
- **ＳＮＳの公式アカウント・マッチングアプリアカウント開設時の本人確認強化**
- 新たに開始された金融教育における被害防止に向けた啓発

フィッシング対策

- **送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
- **フィッシングサイトの閉鎖促進**
- **フィッシングサイトの特性を踏まえた先制的な対策**

特殊詐欺等対策

- 国際電話の利用休止申請の受付体制の拡充
- **ＳＭＳの不適正利用対策の推進**
- 携帯電話を使用しながらＡＴＭを利用する者への注意喚起の推進

2.「犯行に加担させない」ための対策

- **「闇バイト」等情報に関する情報収集、削除、取締り等の推進**
- 青少年をアルバイト感覚で犯罪に加担させない教育・啓発

3.「犯罪者のツールを奪う」ための対策

- 本人確認の実効性の確保に向けた取組
- 金融機関と連携した検挙対策の推進
- 電子マネーの犯行利用防止対策
- 預貯金口座の不正利用防止対策の強化等
- 暗号資産の没収・保全の推進

4.「犯罪者を逃さない」ための対策

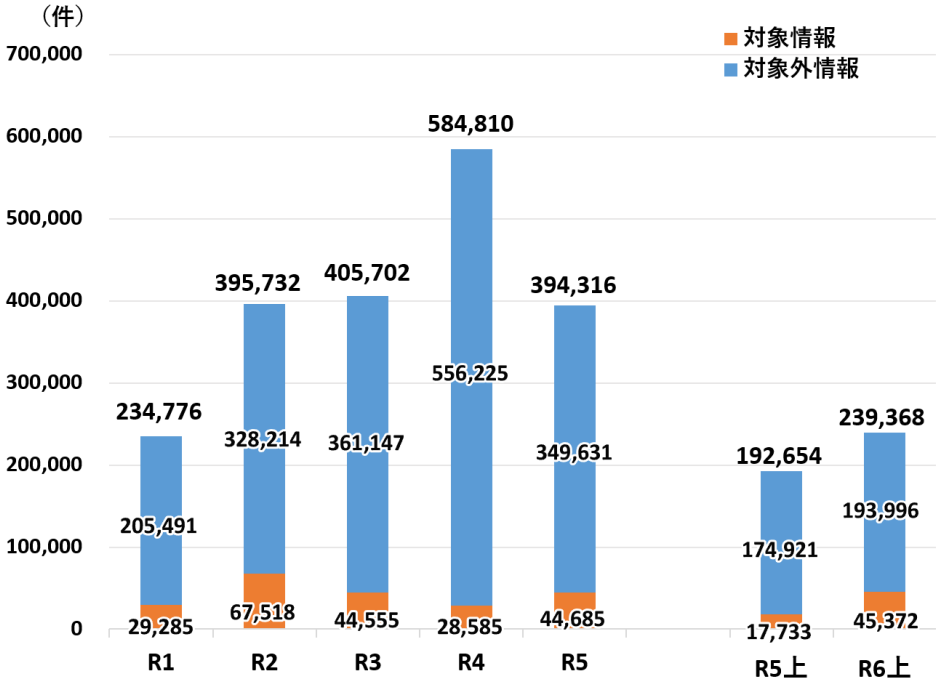
- **匿名・流動型犯罪グループに対する取締り及び実態解明体制の強化**
- ＳＮＳ事業者における照会対応の強化
- 海外拠点の摘発の推進等
- 法人がマネー・ローンダリングに悪用されることを防ぐ取組の推進
- 財産的被害の回復の推進

資料編

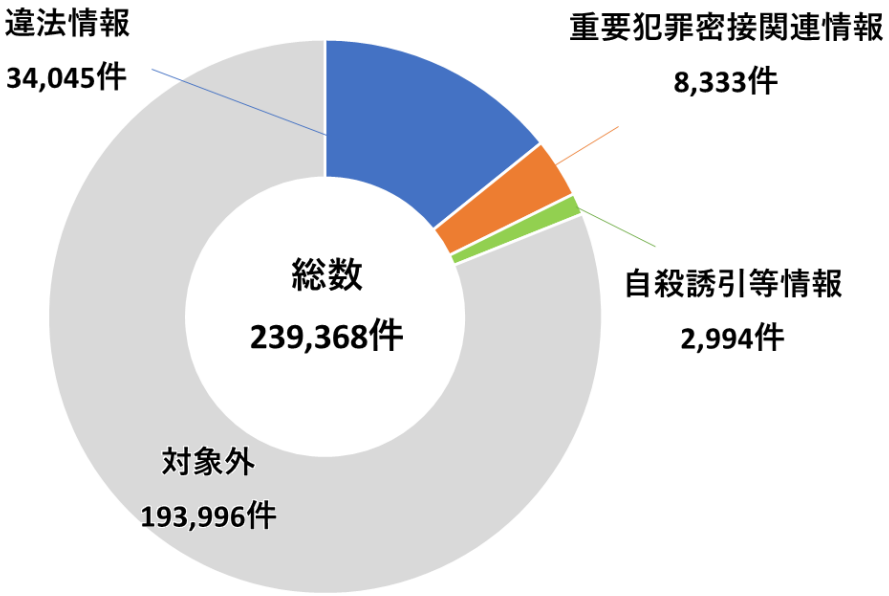
（第１部３「違法・有害情報に係る情勢」関連）

違法・有害情報の分析に係る統計

１　違法情報等の分析件数の推移



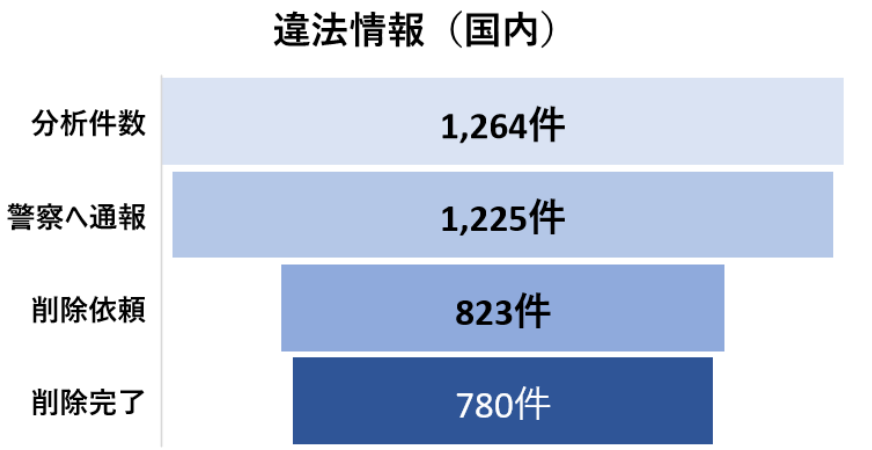
２　分析結果の内訳

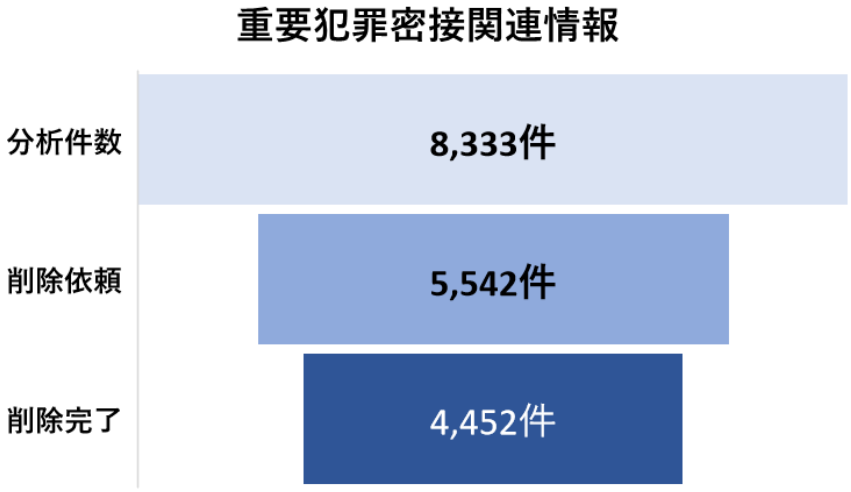


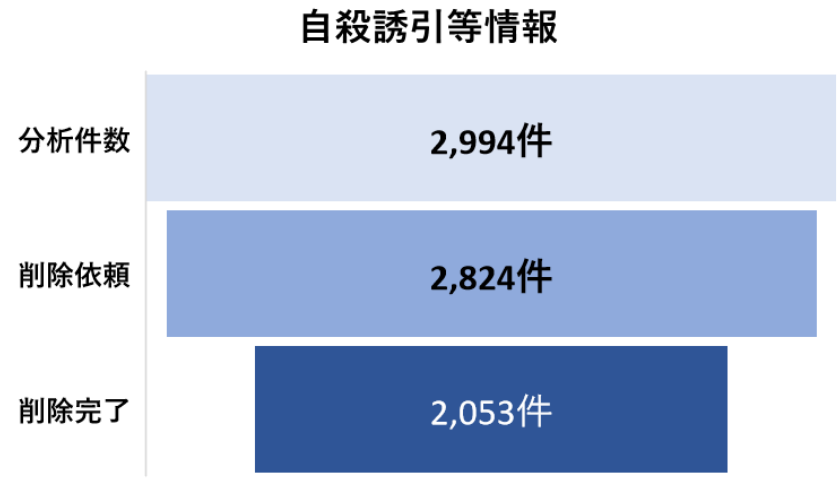
（第１部３「違法・有害情報に係る情勢」関連）

違法・有害情報の分析に係る統計②

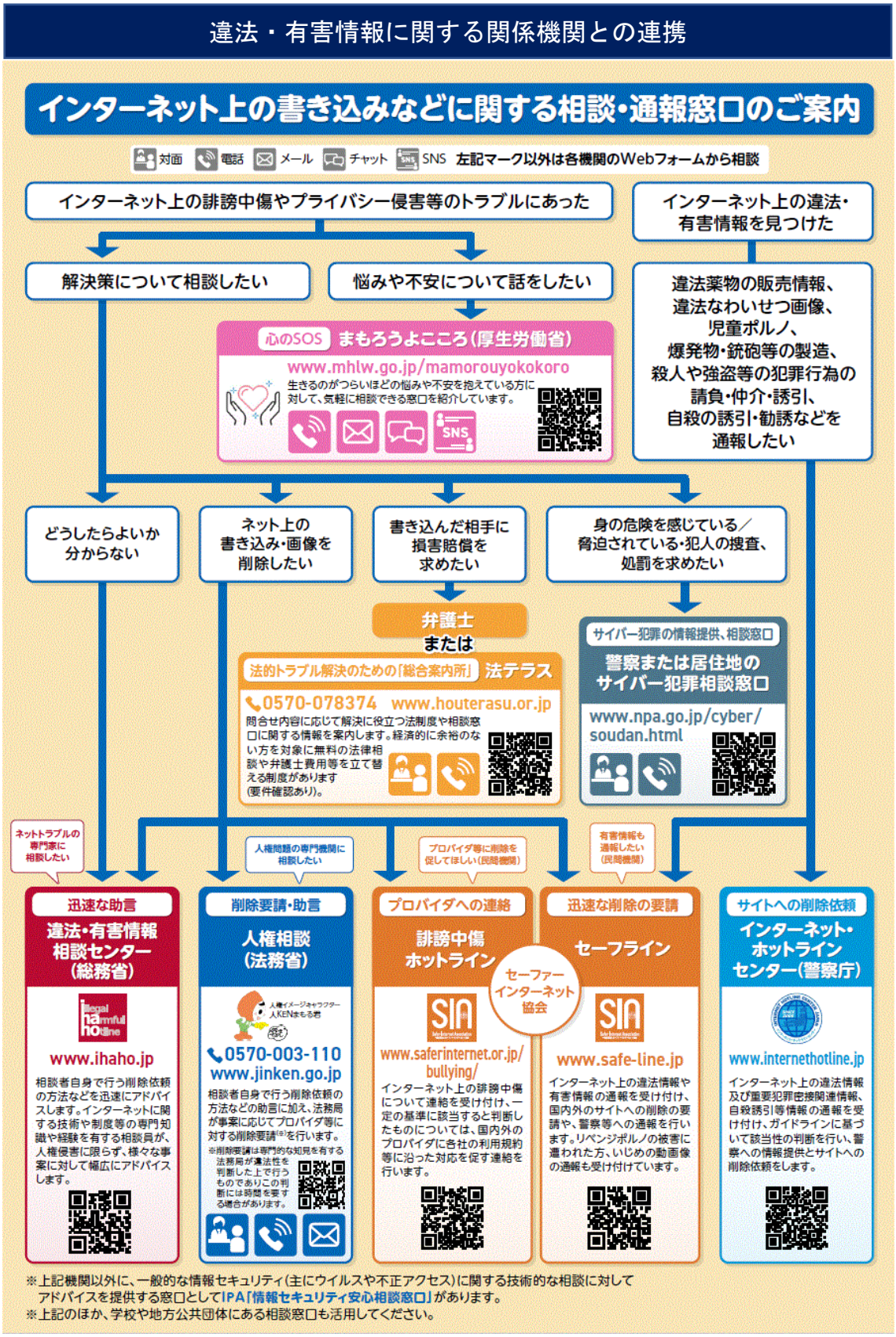
３　分析件数と処理結果







（第１部３「違法・有害情報に係る情勢」関連）



（検挙事例関連）

主な検挙事例一覧

● **フィッシングを手口とする電子計算機使用詐欺等事件被疑者の検挙**

無職の少年（17 歳）は、令和５年 12 月、ゲームアカウント売買サイトの入力画面を模したフィッシング画面を用い、他人の識別符号を不正取得した後、同識別符号を用いて不正アクセスした上、自身との虚偽の取引を成立させることで財産上不法の利益を得た。令和６年６月、同少年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）

● **クレジットカード情報等の不正提供事件被疑者の検挙**

無職の男（20 歳）は、令和５年８月、不正入手した他人名義のクレジットカード情報や EC サイトの識別符号を、匿名性の高いアプリケーションソフトを利用して有償で他人に提供した。令和６年３月までに、同男を割賦販売法違反及び不正アクセス禁止法違反で逮捕した。（北海道）

● **生成 AI を悪用した不正プログラム作成事件被疑者の検挙**

無職の男（25 歳）は、令和５年３月、生成 AI を利用し、人が電子計算機で実行した際、ファイルのデータを上書きして破壊する機能を有する不正プログラムを作成した。令和６年５月、同男を不正指令電磁的記録作成罪で逮捕した。（警視庁）

● **暗号資産窃取を目的とする不正プログラム供用事件被疑者の検挙**

会社員の男（30 歳）は、令和４年４月から５月にかけ、氏名不詳者と共謀し、他人の暗号資産を不正に入手する目的で、実行者の意図に基づかず暗号資産の取引に必要な認証情報等を取得する機能を有する不正プログラムを、暗号資産の自動取引ツールであると偽って他人にダウンロードさせた上、同プログラムを実行の用に供した。令和６年１月、同男を不正指令電磁的記録供用罪で逮捕した。（千葉）

● **暗号資産交換業の無登録営業事件被疑者の検挙**

高校生の少年（18 歳）は、SNS 上で暗号資産の売買を広告し、令和５年７月から同年９月にかけ、内閣総理大臣の登録を受けることなく、業として暗号資産と現金等の売買を行った。令和６年３月、同少年を資金決済法違反で検挙した。（警視庁）

（情報技術解析関連）

主な情報技術解析の実施状況一覧

１　情報技術解析に関する警察の取組

●　警察庁及び情報技術解析課の取組

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、都道府県警察に対し、捜索・差押え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。

また、警察庁の高度情報技術解析センターは、高度で専門的な知識及び技術を有する職員を配置し、高性能な解析用資機材を整備して、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。令和６年上半期中には、都道府県情報通信部の情報技術解析課において、スマートフォン等合計 5,426 台の解析を実施した。

●　各都道府県警察のサイバー部門の取組

各都道府県警察のサイバー部門は、高度な専門的知識及び技術を要するサイバー事案（重大サイバー事案を含む。）に対処するための体制を拡充している。また、サイバー部門以外の事件主管課の捜査力のみでは対処が困難な捜査事項について、高度な専門的知識及び技術に基づいた支援を行うことができる体制を構築している。さらに、各都道府県情報通信部の情報技術解析課に対してなされる解析要請を含め、支援要請窓口を支援部門に一本化し、ワンストップ化するなど、情報技術解析部門も含めた支援の一体的運用を図っている。令和６年上半期中には、都道府県警察の支援部門において、スマートフォン等合計 24,829 台の解析を実施した。

（情報技術解析関連）

主な情報技術解析の実施状況一覧②

２　近年の開発及び解析事例

● **ショート箇所特定装置の独自開発**

通常、ショートが原因で破損したスマートフォンの機能回復を行う場合はショート箇所の特定が困難なものが多く、機能回復までに長期間を要するところ、高度情報技術解析センターにおいてショート箇所を早期に特定する装置を独自に開発し、同装置を用いて破損したスマートフォン８台の機能回復に成功したことにより、架空料金請求詐欺事件の検挙に貢献した。

● **被疑者動向の自動確認プログラムの開発**

Web サービス上における被疑者の動向を自動で確認し、捜査員へ通知するプログラムを開発したことで、オンラインサイトにおける賭博事件の検挙に貢献した。

● **腐食した USB メモリの機能回復**

腐食等により正常に動作しなくなった USB メモリについて、微細な破損箇所を特定するとともに、修復作業を行うことで機能回復及びデータの抽出に成功し、盗撮事件の検挙に貢献した。

● **破損したドライブレコーダー映像の復元**

交通事故発生時のドライブレコーダの映像について、機器の不具合により破損した動画データの構造を解析して、事故発生当時の映像を復元し、自動車と歩行者の交通死亡事故の真相解明に貢献した。