広　報　資　料
令和７年３月13日
サイバー企画課

令和６年におけるサイバー空間をめぐる脅威の情勢等について

第１　概要

令和６年におけるサイバー空間をめぐる脅威の情勢と警察の取組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脅威情勢に対する警察の取組

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

令和６年中には、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、年末年始には金融機関等におけるDDoS攻撃とみられる被害が発生。令和６年におけるランサムウェアの被害報告件数も引き続き高水準で推移。

(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のみならず、SNS型投資・ロマンス詐欺等においても、暗号資産によるマネー・ローンダリングが行われるなど、インターネット上のサービスが悪用。

(3)　違法・有害情報に係る情勢

SNS上には、「ホワイト案件」等の文言を用いた犯罪実行者募集情報が氾濫しているほか、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。

２　警察の取組

(1)　検挙に向けた取組

サイバー特別捜査部は、横断的・俯瞰的な分析及び捜査により、検挙を推進。ランサムウェアグループ「Phobos」については、EUROPOL等との国際共同捜査により、運営者が検挙。

(2)　被害の未然防止・拡大防止に向けた取組

- 北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」について、パブリック・アトリビューションを実施。
- インターネット・ホットラインセンター（IHC）において、犯罪実行者募集情報を違法情報に位置付け、取組を強化。

(3)　基盤整備

令和６年度予算において、体制や資機材の整備を推進。

令和６年における
サイバー空間をめぐる脅威の情勢等について

令和７年３月
警察庁サイバー警察局

はじめに

令和６年においては、政府機関、交通機関、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、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年におけるランサムウェアの被害報告件数は、222 件と引き続き高水準で推移しており、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：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、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。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。

このような状況に対し、警察においては、検挙に向けた取組を進めており、匿名性の高い暗号資産「モネロ」に変換して資金洗浄を行っていた、クレジットカード不正利用事案の首謀者を特定・逮捕したほか、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た攻撃グループ「Phobos」について、EUROPOL 等と国際共同捜査を推進した結果、米国司法省により同グループの運営者とみられる男が起訴された。

このほか、警察庁においては、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」について、その手口や対策に関する注意喚起を実施したほか、攻撃者を公表し非難することで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６年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

概要　令和６年における脅威情勢の概要 1
第１部　サイバー空間の脅威情勢 5
１　高度な技術を悪用したサイバー攻撃の脅威情勢 5
(1)　国家の関与が疑われるサイバー攻撃 6
(2)　犯罪組織等によるサイバー攻撃 7
２　インターネット空間を悪用した犯罪に係る脅威情勢 11
(1)　SNS・メッセージングアプリを悪用した犯罪 11
(2)　メール・SMS を悪用した犯罪 12
(3)　ウェブサイトを悪用した犯罪 16
(4)　インターネット空間の資金移動を悪用した犯罪 17
①　インターネットバンキング 17
②　暗号資産 18
３　違法・有害情報に係る情勢 19
(1)　主な違法・有害情報の類型 19
(2)　犯罪実行者募集情報 19
(3)　災害発生時等における偽情報 19
第２部　警察の取組 21
１　検挙に向けた取組 21
(1)　検挙 22
①　サイバー特別捜査部 22
②　都道府県警察サイバー部門 23
(2)　捜査支援 23
(3)　国際連携 25
２　被害の未然防止・拡大防止に向けた取組 28
(1)　情報発信 28
①　国際連携を通じた情報発信 28
②　関係機関との連携を通じた情報発信 30
(2)　犯罪インフラへの対処 30
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 31
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 32
③　違法・有害情報に関するインフラへの対処 34
３　基盤整備 37
(1)　体制の拡充 37
(2)　人材育成 38
(3)　資機材の整備 40
(4)　情報技術解析部門による研究 41

図表目次

図表１：警察庁が検知した不審なアクセス件数（１日・１IP アドレス当たり） ･････ ５
図表２：ランサムウェア攻撃の流れ･････ ８
図表３：ランサムウェア被害報告件数･････ ８
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･････ ９
図表５：SNS 型投資・ロマンス詐欺の認知件数・被害額 ･････ 12
図表６：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･･･ 13
図表７：インターネットバンキングに係る不正送金の流れ･････ 13
図表８：リアルタイム型フィッシングの手口･････ 15
図表９：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･････ 15
図表 10：クレジットカード不正利用の流れ ･････ 16
図表 11：警察庁に対する偽サイト等の情報報告件数 ･････ 16
図表 12：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 ･････ 17
図表 13：令和６年中の特殊詐欺/SNS 型投資・ロマンス詐欺の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･････ 18
図表 14：暗号資産を悪用したマネー・ローンダリングのイメージ ･････ 18
図表 15：犯罪実行者募集のイメージ ･････ 19
図表 16：SNS 上における偽情報投稿のイメージ･････ 20
図表 17：サイバー犯罪の検挙件数 ･････ 21
図表 18：サイバー事案の検挙件数 ･････ 22
図表 19：令和６年のサイバー事案の検挙内訳 ･････ 22
図表 20：クレジットカード不正利用事案の概要 ･････ 23
図表 21：令和６年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 ･････ 24
図表 22：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 ･････ 26
図表 23：ナイジェリアとの国際共同捜査の概要 ･････ 27
図表 24：オペレーション「PowerOFF」の HP･････ 29
図表 25：カウンターランサムウェア・イニシアティブ会合の様子 ･････ 29
図表 26：ウェブスキミングの手口 ･････ 32
図表 27：サイバー防犯ボランティアへの支援 ･････ 33
図表 28：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 ･････ 34
図表 29：インターネット・ホットラインセンター、サイバーパトロールセンターの概要 35
図表 30：令和６年 11 月及び 12 月の犯罪実行者募集情報の最終的な削除率 ･････ 36
図表 31：サイバー警察局及びサイバー特別捜査隊の設置 ･････ 37
図表 32：サイバー特別捜査部への発展的改組 ･････ 38
図表 33：警察におけるサイバー人材 ･････ 39
図表 34：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 ･････ 40
図表 35：生成 AI を用いた不正プログラムの機能推定手法のイメージ ･････ 41

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･････ ９
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･････ 10
コラム：インターネットバンキングに係る不正送金に関する分析･････ 14
コラム：ランサムウェアグループ「Phobos」に対する国際共同捜査･････ 26
コラム：ナイジェリアとの国際共同捜査･････ 27
コラム：TraderTraitor に関するパブリック・アトリビューション ･････ 28
コラム：MirrorFace によるサイバー攻撃に関する注意喚起 ･････ 29
コラム：EC サイトのぜい弱性を狙ったクレジットカード情報等の窃取の実態解明 ･････ 32
コラム：犯罪実行者募集情報の迅速な削除･････ 36
コラム：生成 AI を用いた不正プログラムの機能推定手法･････ 41

概要　令和６年における脅威情勢の概要

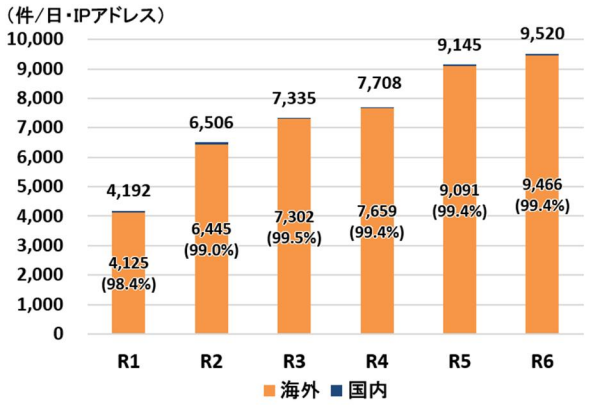
令和６年においては、サイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数及びランサムウェアの被害報告件数が前年から増加した。また、フィッシングの報告件数も前年比で約 52 万件（44%）増加したほか、インターネット上には犯罪実行者募集情報が氾濫するなど、極めて深刻な情勢が継続している。

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

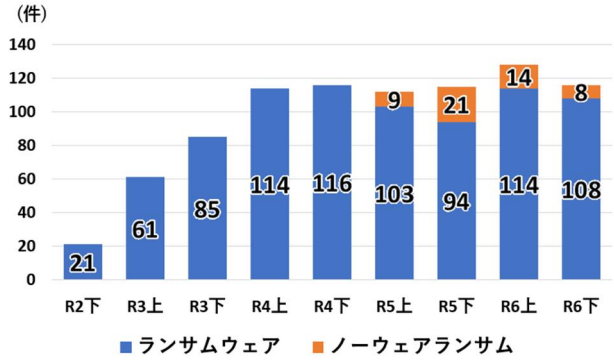
１　高度な技術を悪用したサイバー攻撃の情勢

● 令和６年中、政府機関、交通機関、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。



● 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、その大部分の送信元が海外。

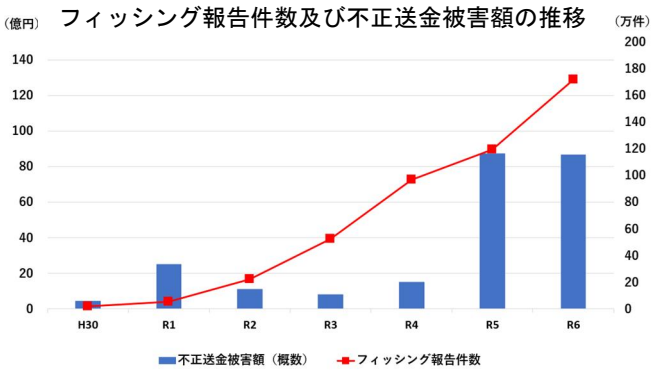
● 令和６年におけるランサムウェアの被害報告件数は 222 件であり、高水準で推移。



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６年におけるフィッシング報告件数は、171 万 8,036 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 86 億 9,000 万円。



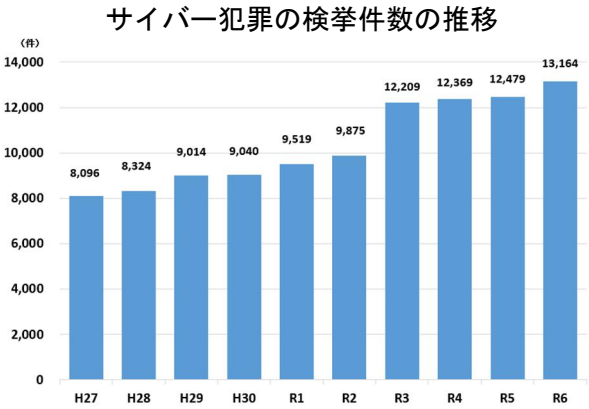
３　違法・有害情報に係る情勢

● インターネット上には、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。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したほか、義援金を募る送金詐欺も確認。

Ⅱ　警察の取組

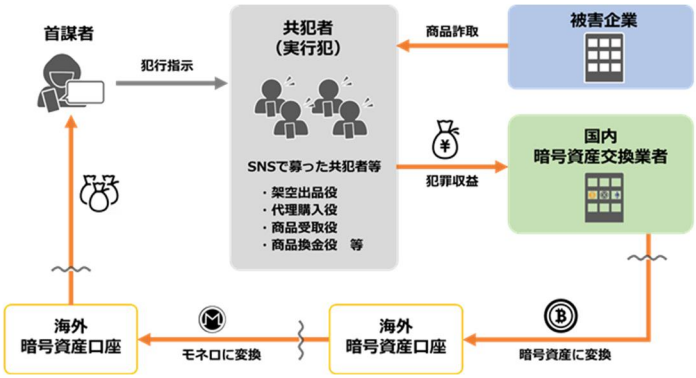
１　検挙に向けた取組

● 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。

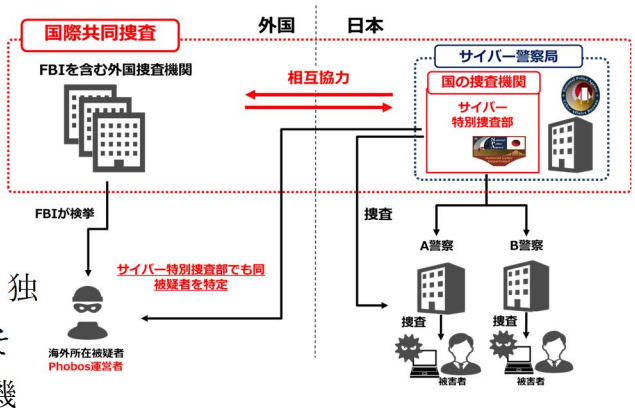


● 令和６年におけるサイバー犯罪の検挙件数は 13,164 件、サイバー事案の検挙件数は 3,611 件。

● オンラインフリーマーケットサービス等を悪用した架空取引・クレジットカード不正利用事件では、実行犯が検挙されても、首謀者は手口や共犯者を変えて犯行を継続するとともに、犯罪収益を匿名性の高い暗号資産「モネロ」に換えて資金洗浄を敢行。サイバー特別捜査部による分析の結果、犯罪収益の流れ及び犯行グループの実態を解明し、首謀者を特定・逮捕。



● 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）」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、米国司法省は、同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。サイバー特別捜査部は、独自の手法により同運営者の特定に成功し、その結果や当該手法について、関係国の捜査機関に提供。



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６年 12 月、警察庁は、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）とともに、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、合同で文書を発出。

　また、関係省庁との連名で TraderTraitor の手口等に関する注意喚起を実施。

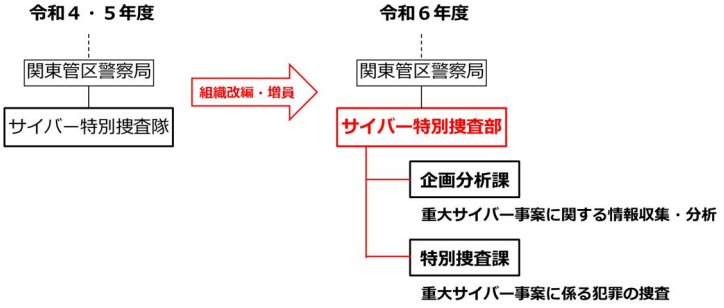
● 令和７年１月、警察庁は、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信や、ソフトウェアのぜい弱性を悪用した標的ネットワーク内への侵入により、情報窃取を目的としたサイバー攻撃を行っていることを確認。さらに、これら攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動であると評価し、同グループの手口や未然防止対策等に関する注意喚起を実施。

● 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、EC サイト構築ソフトのぜい弱性に起因したクレジットカード情報の漏洩を防ぐため、事業者団体に対し、対策の強化を要請したほか、金融庁と連携し、ボイスフィッシングによる不正送金被害の手口や対策に関する注意喚起を実施。

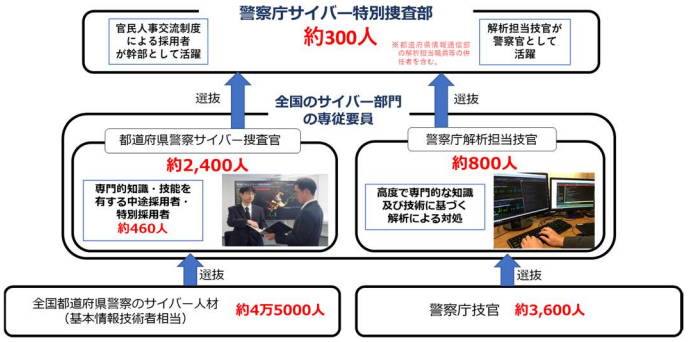
● 警察庁では、インターネット利用者等から違法・有害情報に関する通報を受理し、サイト管理者等への削除依頼等を行うインターネット・ホットラインセンター（IHC）を事業委託。令和７年２月 28 日、IHC の運用ガイドラインを改定し、犯罪実行者募集情報を違法情報に位置付け、取組を強化。

３　基盤整備

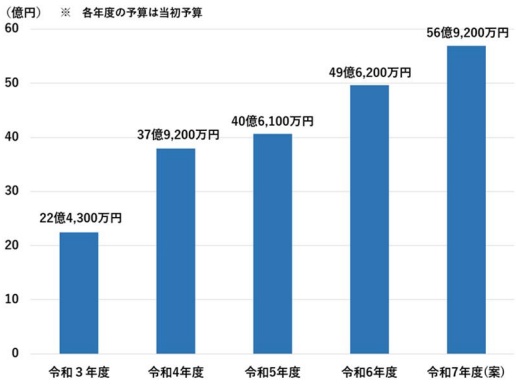
● 令和４年４月、国境を容易に越えて敢行されるサイバー事案に対し、国際共同捜査を通じて被疑者を検挙するため、関東管区警察局に、全国を管轄して直接捜査を実施する「サイバー特別捜査隊」を設置。令和６年４月、同隊を発展的に改組し、「サイバー特別捜査部」を設置することにより、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析等を行う体制を強化。令和７年度予算案には、サイバー特別捜査部の増員に加え、同部に特別対処課を設置することも計上。



● 都道府県警察では、情報通信技術に関する高度な資格の保有等を条件として中途採用・特別採用をした警察官等約 460 人が、サイバー犯罪捜査官等として、捜査の第一線で活躍。警察庁では、情報通信に関する専門的な技術を有する約 800 人の職員が情報技術解析等の第一線で活躍。



● サイバー空間の脅威への対処に係る予算は、令和６年度は 49 億 6,200 万円、令和７年度の予算案では、56 億 9,200 万円を計上。



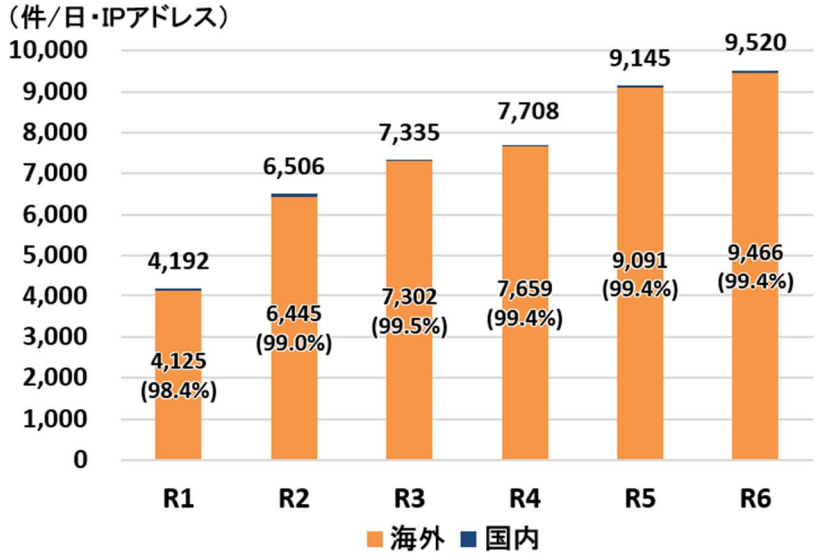
第１部　サイバー空間の脅威情勢

１　高度な技術を悪用したサイバー攻撃の脅威情勢

令和６年においては、政府機関、交通機関、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。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６年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 9,520.2 件と、平成 23 年以降、増加の一途をたどっており（前年比 4.1%増）、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（１日・１IP アドレス当たり）】



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、我が国においても、令和元年頃から、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

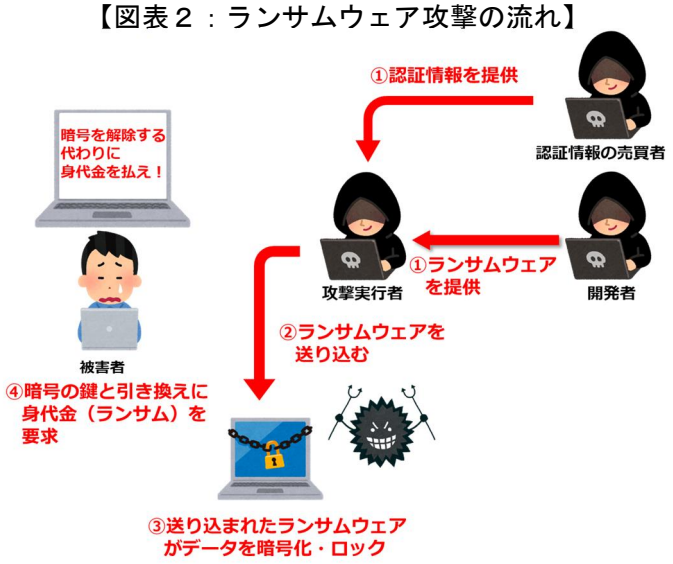
犯罪組織等によるサイバー攻撃としては、まずランサムウェアによる攻撃が挙げられる。ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラムであり（図表２）、近年は、データを窃取したうえ、「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝の被害も多くみられる。また、ランサムウェアによって流出したとみられる事業者の財務情報や個人情報等が、ダークウェブ上のリークサイトに掲載されていたことが確認されている。

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。

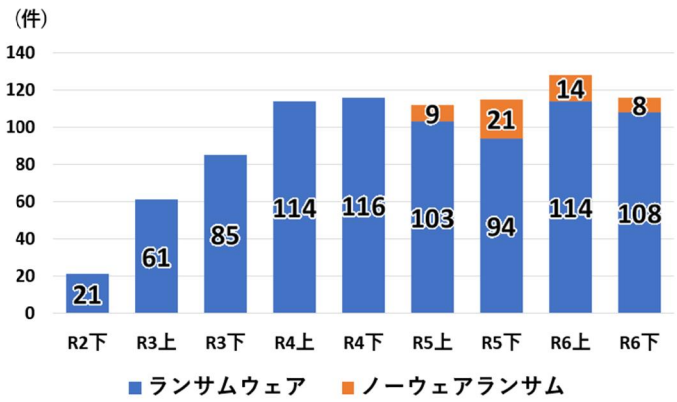
【CASE：出版大手企業に対するランサムウェア攻撃事案】

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 20 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】

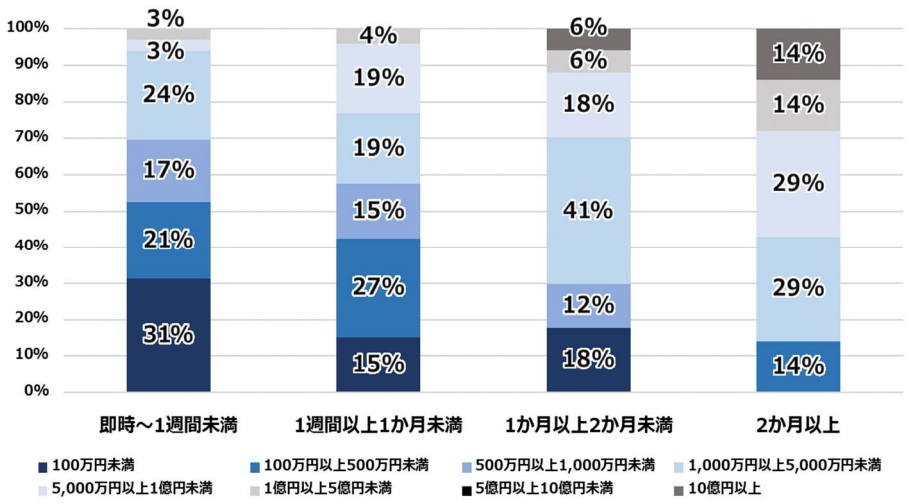


※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

ランサムウェア被害件数を組織規模別に令和５年と比較すると、大企業の被害件数が減少する一方、中小企業の被害件数は 37%増加した。これは、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、調査・復旧に要する期間と費用の関係は図表４のとおりであり、１億円以上の費用を要した組織の割合は、復旧に要した期間が長い方が高いといった傾向が見られた。また、令和５年と比較してランサムウェアの被害による事業影響は長期化・高額化しており、調査・復旧に１か月以上を要した組織（アンケート回答時に「復旧中」だった組織も含む。以下同じ。）は、44%から 49%に増加し、また、1,000 万円以上の費用を要した組織は 37%から 50%に増加した。さらに、調査・復旧に「1,000 万円以上」かつ「１か月以上」を要した組織のうち、サイバー攻撃を想定状況に含む BCP を策定済みである組織は 11.8%にとどまった一方、1 週間未満で復旧した組織の 23.1%が同種の BCP を策定していた。（アンケート結果の詳細は資料編参照。）

【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

上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ところ、その原因としては、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きちんと管理されずに存在していたことなどが挙げられる。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したり、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したり、侵入時に被害企業のログやバックアップを消去したりしている。

特にログについては、侵入の実態調査や復旧対応を行う際に必要となり、これ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、再被害に遭う可能性があるため、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。

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。

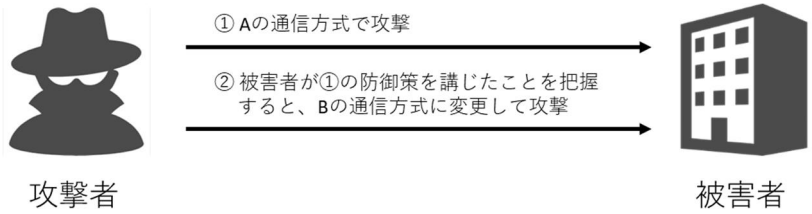
令和６年２月、７月及び 10 月、政府機関や自治体、民間事業者等が運営する複数のウェブサイトにおいて、DDoS 攻撃による被害とみられる閲覧障害が複数発生した。同じ頃、SNS 上に、NoName057(16)を名乗るハクティビストのものと思われる複数のアカウントから、それらの犯行をほのめかす投稿が確認された。

また、令和６年から令和７年の年末年始には、交通機関や金融機関等の重要インフラ事業者等における DDoS 攻撃が発生した。

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、複数種類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。



このほか、EC サイト構築ソフトウェアのぜい弱性を悪用し、クレジットカード番号等の情報を窃取する事例も多数確認されている（詳細は第２部２(2)①参照）。

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は特殊詐欺等における振込に、暗号資産はマネー・ローンダリングに悪用されている。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。

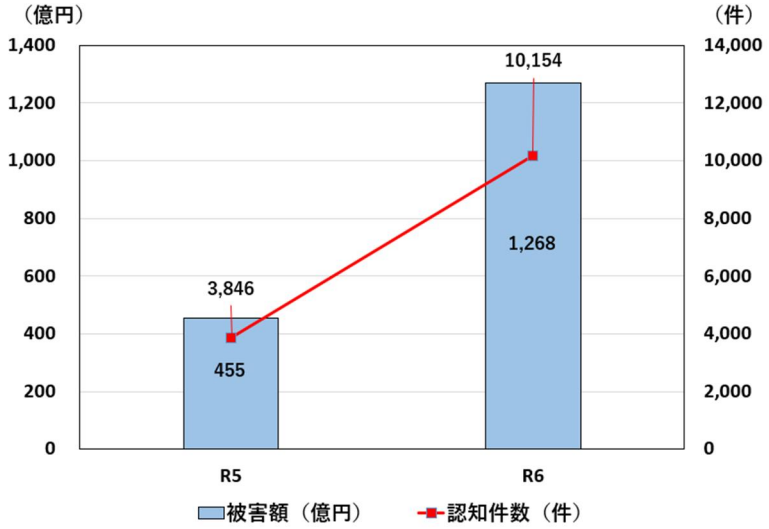
(1)　SNS・メッセージングアプリを悪用した犯罪

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付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「ホワイト案件」等の表現を用いたり、仕事の内容を明らかにせずに著しく高額な報酬の支払を示唆したりするなどして、犯罪の実行犯を募集し、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、実行役の間の連絡手段には、通信が暗号化されており、送信者と受信者以外はメッセージを確認できない、設定した時間でメッセージを自動的に消去できる機能を備えているといった、匿名性の高いメッセージングアプリが使用されるなど、犯罪の証拠を隠滅するため、当該アプリが悪用されている実態が見られる。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、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６年中、特殊詐欺と SNS 型投資・ロマンス詐欺の被害額は、合計で約 2,000 億円に上った。具体的には、特殊詐欺の被害額は約 721 億 5,000 万円

（前年比 59.4%増）と、３年連続増加傾向にあり、SNS 型投資・ロマンス詐欺の被害額は約 1,268 億円（前年比 178.6%増）と急増している。

【図表５：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、オンラインゲーム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、児童買春等の違法行為の「場」となっている状況もうかがえる。実際、SNS に起因して犯罪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。

さらに、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（リベンジポルノ等）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。

(2)　メール・SMS を悪用した犯罪

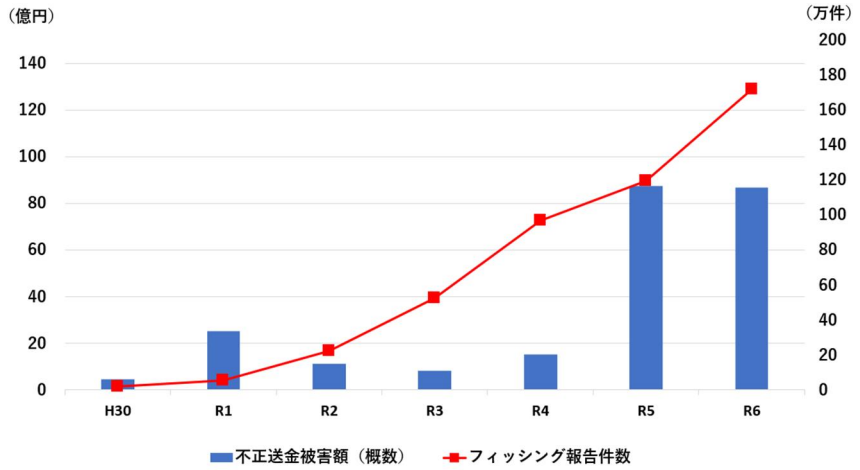
メールや SMS は、フィッシングに悪用される実態がみられる。フィッシングとは、実在する組織を装ってメールや SMS のリンクから偽のウェブサイト（フィッシングサイト）へ誘導し、同サイトでアカウント情報やクレジットカード番号等を不正に入手する手口であり、これによって得られた情報はインターネットバンキングに係る不正送金やクレジットカードの不正利用に使われている。

令和６年におけるフィッシング報告件数は、フィッシング対策協議会によれ

ば、171 万 8,036 件であり、右肩上がりの増加が続いている。

また、令和 6 年におけるインターネットバンキングに係る不正送金事犯の発生件数は 4,369 件、被害総額は約 86 億 9,000 万円となっており、フィッシングがその手口の 9 割を占める。

【図表６：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】

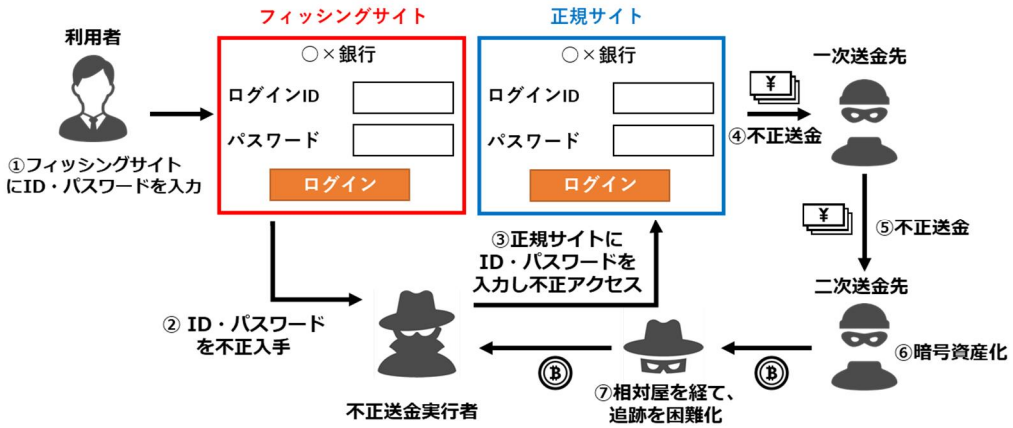


※　フィッシング報告件数：フィッシング対策協議会資料による（以下同）

さらに、令和 6 年秋には、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騙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した。

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[1]によって本人確認を突破する手口も引き続きみられた。

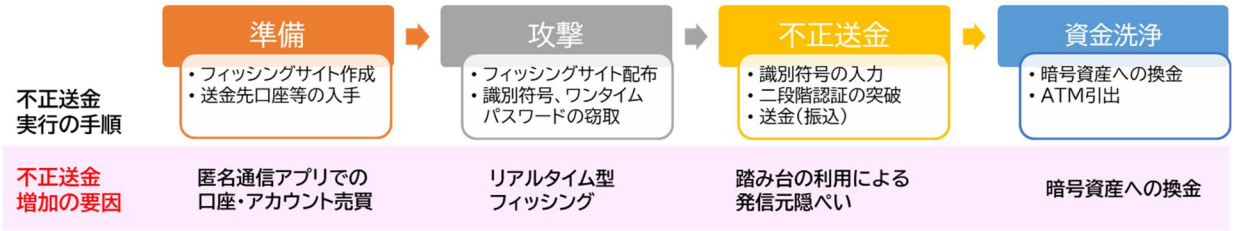
【図表７：インターネットバンキングに係る不正送金の流れ】



[1] 携帯電話機販売店において、偽造した本人確認書類を使い、他人に成りすまして 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

コラム：インターネットバンキングに係る不正送金に関する分析

インターネットバンキングに係る不正送金は、大きく分けて、①準備、②攻撃、③不正送金、④資金洗浄の４つの段階を踏んで行われる。サイバー特別捜査部の分析によると、近年、各段階において手口の変化が見られ、被害件数増加の要因となっていると考えられている。



① の準備段階では、不正送金の受け皿となる銀行口座や、暗号資産に換金するための暗号資産取引所のアカウントが、匿名性の高いメッセージングアプリ等を介して不正に売買されており、入手が容易になっている。

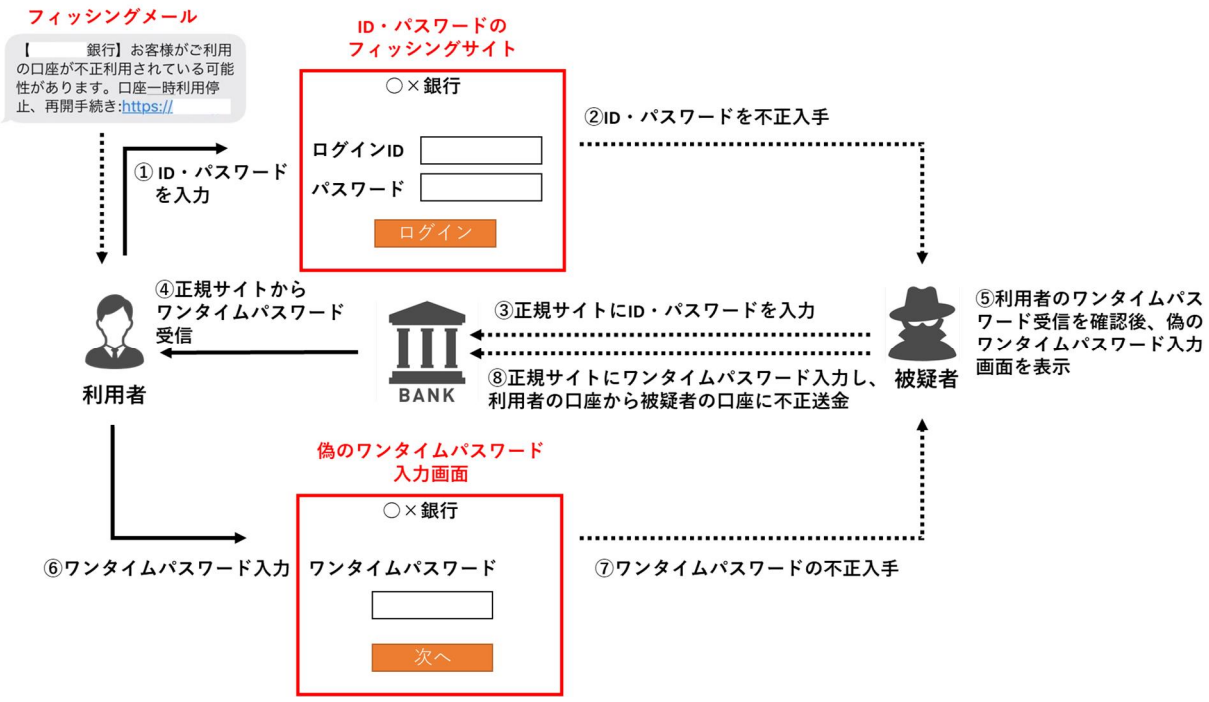
② の攻撃段階では、令和元年頃からリアルタイム型フィッシングにより二段階認証を突破する手口が横行している。

※　リアルタイム型フィッシング：利用者がフィッシングサイトに入力した情報を犯人が正規サイトに即座に入力し、その際利用者に送付される二段階認証のためのワンタイムパスワードもフィッシングサイトに入力させて、不正ログインを試みる手口（図表８）

③ の不正送金段階では、一般家庭のインターネット回線や、第三者のモバイル通信を踏み台として悪用することで、通信元の隠蔽（匿名化）に加え、利用者による一般家庭からの正規のログインを偽っている事案が多数確認されている。例えば、海外で放送されている TV 番組やインターネット配信の動画を視聴するための IoT 機器がマルウェアに感染しており、踏み台として使われるケースも確認している。

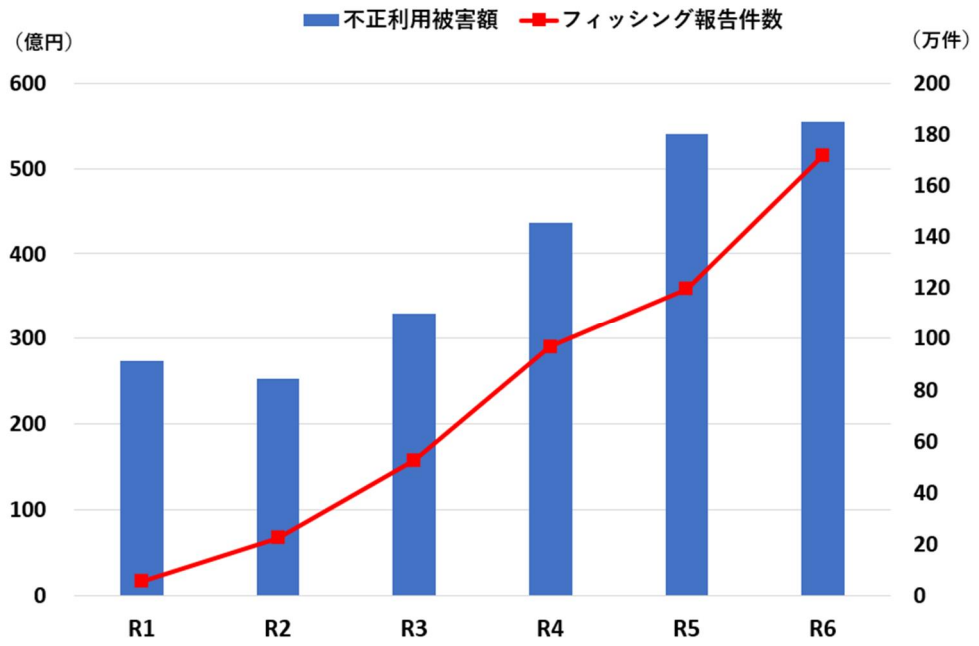
④ の資金洗浄・現金化段階では、いわゆる「出し子」が ATM から現金を引き出すという従来の手口に代わり、暗号資産への換金による資金洗浄が主流となっている。

【図表８：リアルタイム型フィッシングの手口】



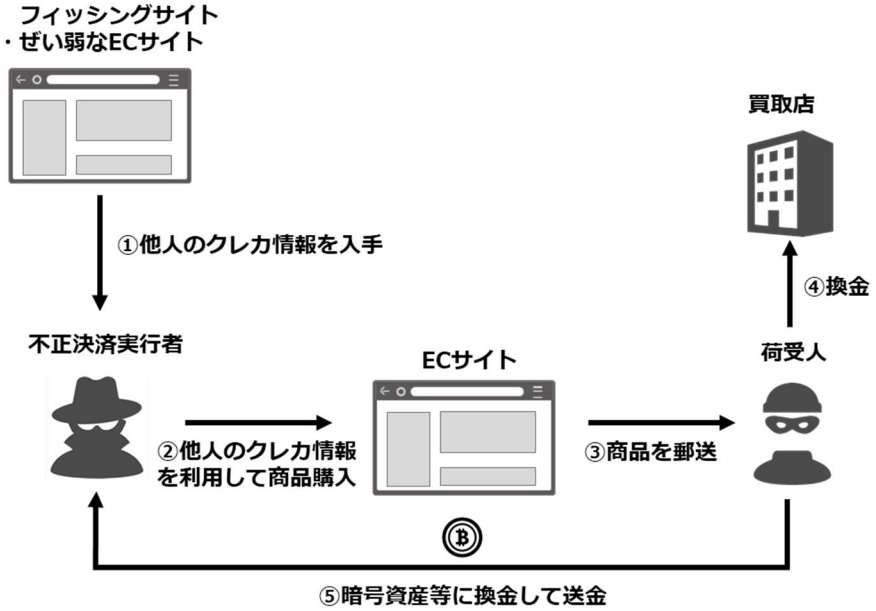
さらに、一般社団法人日本クレジット協会によれば、令和６年におけるクレジットカードの不正利用被害額は約 555 億円（前年比 2.6%増）であり、過去最多となった。

【図表９：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）

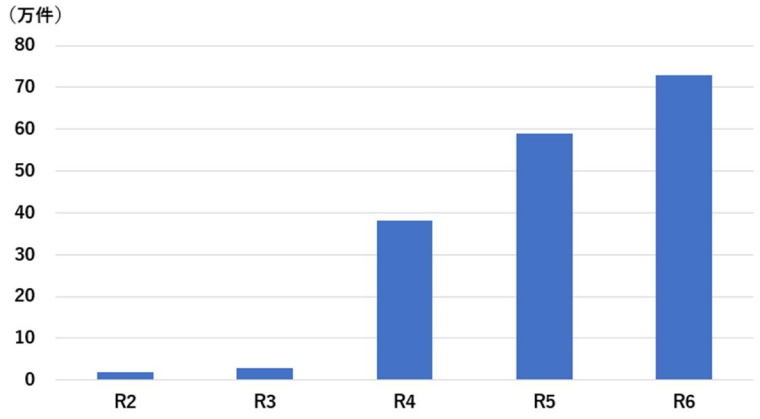
【図表 10：クレジットカード不正利用の流れ】



(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 11】。

【図表 11：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６年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 1,506 件、被害額は 11 億 9,000 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

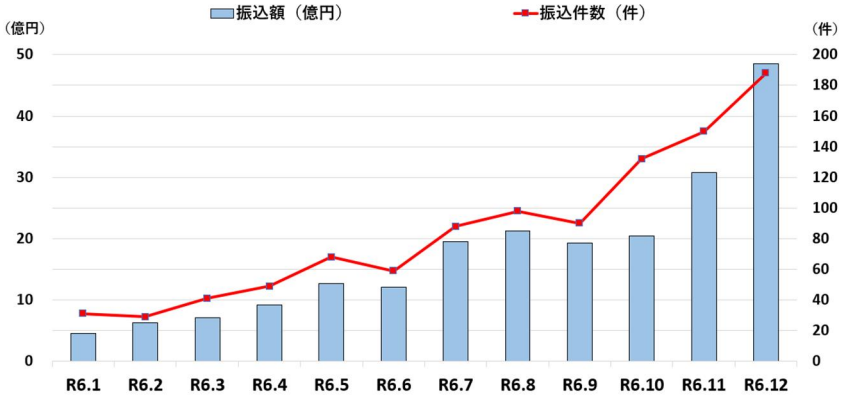
インターネット空間における資金移動は利便性が高い一方、インターネットバンキングでは、振込の１日の上限額を容易に引き上げられる、送金時に第三者の目が届きにくいとった特徴から、犯罪に悪用される実態があり、また、暗号資産についても、匿名性の高さなどから、マネー・ローンダリングに利用される実態が見られる。

①　インターネットバンキング

インターネットバンキングに係る不正送金の情勢については、(2)記載のとおりであるほか、(1)記載の特殊詐欺の被害のうち、被害額 500 万円以上の振込型の事案の被害（認知件数 1,688 件、被害額約 314 億 4,000 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、認知件数は全体の約６割、被害額は全体の約７割を占めている。

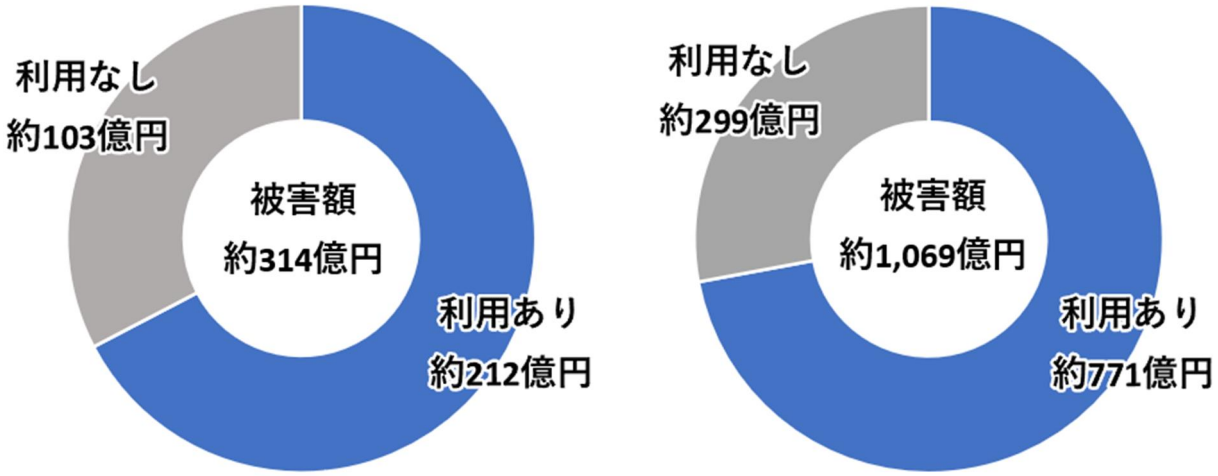
さらに、SNS 型投資・ロマンス詐欺の被害のうち、振込が主な交付形態となっている事案の被害（認知件数 8,287 件、被害額約 1,069 億 4,000 万円）を分析すると、インターネットバンキングを利用したものの認知件数は全体の約６割、被害額は全体の約７割を占めている。

【図表 12：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】



※　特殊詐欺における被害額が 500 万円以上の振込型について調査

【図表 13：令和６年中の特殊詐欺（左）／SNS 型投資・ロマンス詐欺（右）の
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】



※　特殊詐欺（被害額 500 万円以上の振込型の事案の被害）及び SNS 型投資・ロマンス詐欺（振込が主な交付形態となっている事案の被害）に限る。

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、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。実際、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が、暗号資産に変換されている場合もあり、その後、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る場合、追跡が困難となっている。

【図表 14：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」、「覚醒剤等の規制薬物の販売」、「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

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。

特に、強盗・窃盗等について、SNS や求人サイト等で「高額バイト」、「ホワイト案件」、「即日即金」等の文言を用いて実行犯が募集された上で敢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敢行された強盗・窃盗等事件の中には、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。

【図表 15：犯罪実行者募集のイメージ】

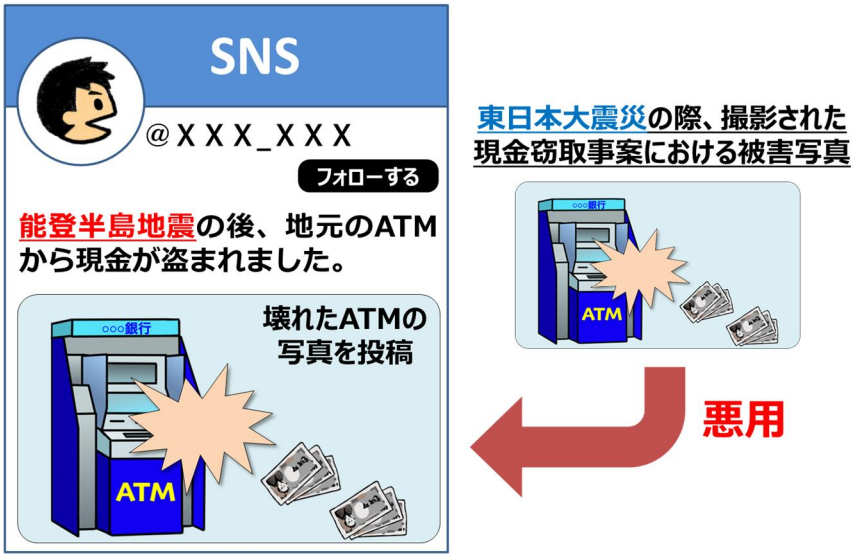
(3)　災害発生時等における偽情報

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、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。

また、同地震に際しては、東日本大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との印象を与えるような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 16：SNS 上における偽情報投稿のイメージ】



第２部　警察の取組

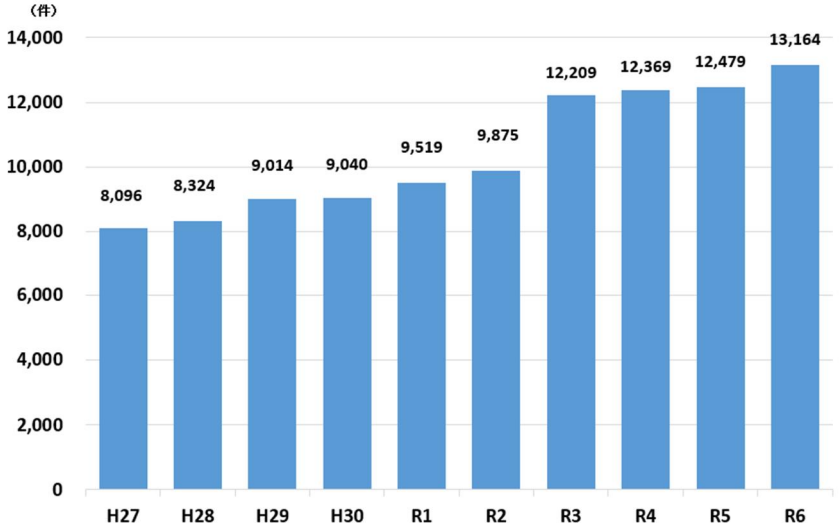
１　検挙に向けた取組

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[2]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[3]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[4]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６年におけるサイバー犯罪の検挙件数は 13,164 件に、サイバー事案の検挙件数は 3,611 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 2,285 件で、そのうち 895 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倍増している。

【図表 17：サイバー犯罪の検挙件数】

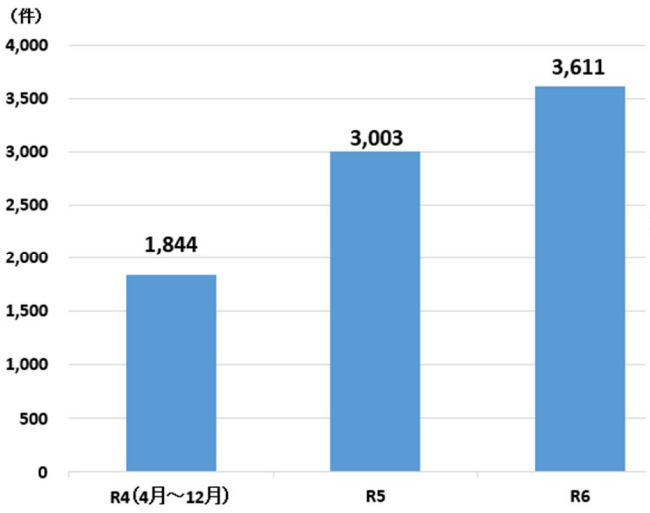


[2] サイバー事案のうち、国若しくは地方公共団体の重要なシステムの運用や重要インフラ事業者の事業の実施に重大な支障が生じ、若しくは生ずるおそれのある事案、高度な技術的手法が用いられるなどの事案（マルウェア事案等）、又は国外に所在するサイバー攻撃者による事案

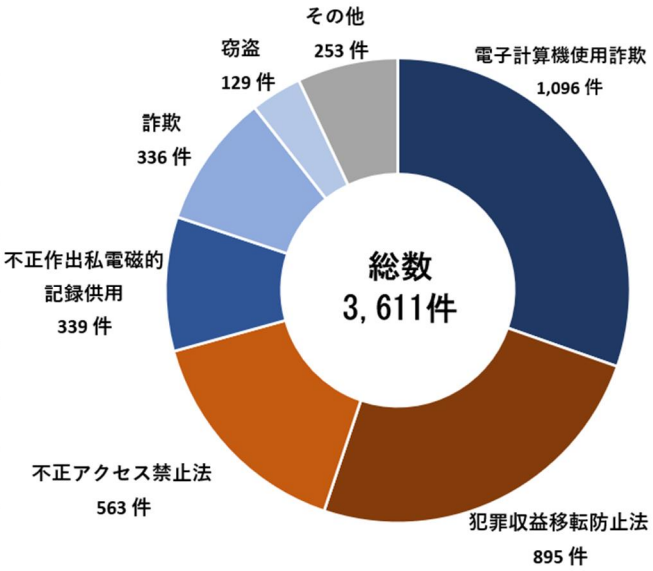
[3] サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案。警察庁サイバー警察局は、「サイバー事案に関する警察に関する」事務を司ることが、その所掌事務の一つとなっている（警察法第 25 条第１号）。

[4] 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

【図表 18：サイバー事案の検挙件数】



【図表 19：令和６年のサイバー事案の検挙内訳】



(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：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。

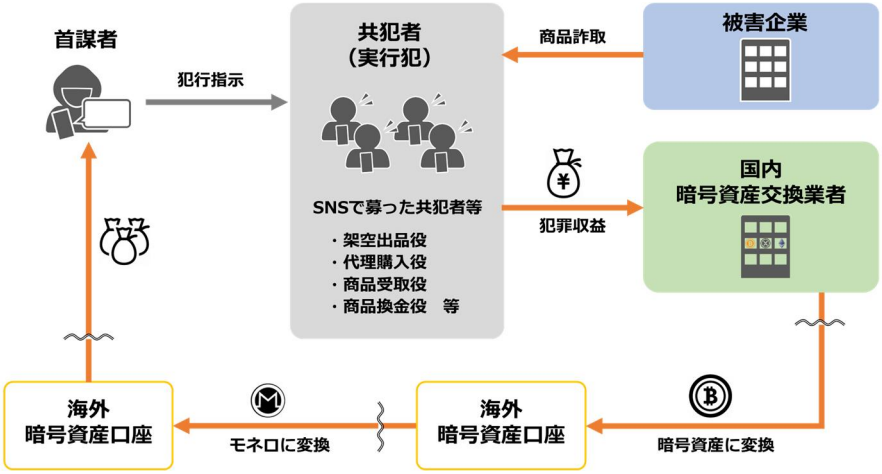
サイバー特別捜査部では、関係都道府県警察での実行犯検挙等の捜査を通じて得られた情報の分析や、モネロに変換された後の犯罪収益の流れの解明により、犯行グループの実態を解明するとともに、首謀者を特定した。

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。

【図表 20：クレジットカード不正利用事案の概要】



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。

【CASE：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）

【CASE：SNS 型ロマンス詐欺事件被疑者の検挙】

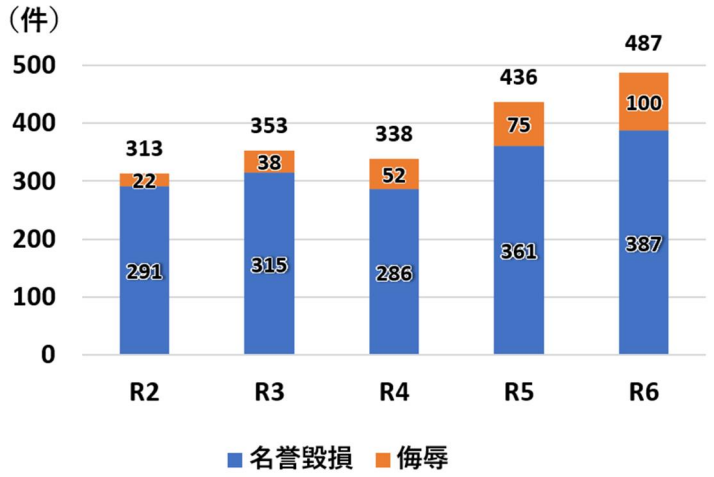
ベトナム国籍の男（24 歳）等は、令和 5 年 3 月、マッチングアプリで知り合った被害者に好意を抱かせ、将来の生活のための投資等の名目で総額約 3000 万円を振込入金させて詐取し、暗号資産に交換して資金洗浄した。令和 6 年 9 月、同男等を詐欺罪で逮捕した。（香川）

(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。

例えば、令和６年中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 487 件となっており、増加傾向にあるところ（図表 21）、これら事案は刑事部門が主管となって捜査をし、サイバー部門が適切に支援している。

【図表 21：令和６年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】



【CASE：SNS 上の名誉毀損事案】

派遣社員の女（28 歳）は、令和５年９月、大阪府内の中学校に在籍する男性教諭を騙り、同校に在校する女子生徒の個人情報等を SNS に投稿し、男性教諭の名誉を毀損するとともに同校の業務を妨害した。令和５年 11 月、大阪府警察捜査第一課が同女を名誉毀損・偽計業務妨害事件で逮捕した。

この事案では、同府警察のサイバー部門が、投稿に関するサイバー空間上の痕跡に関する捜査や被疑者のスマートウォッチ等の電子機器の解析・データ精査等を支援し、男性教諭の犯行を装っていた同女の犯行を裏付けた。（大阪）

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：水没した車両からのデータ抽出】

令和６年 12 月、漁港に沈んでいた車両から遺体が発見された事案について、高度情報技術解析センターは、車両が長期間水没したことにより正常に動作しなくなった車載機器の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、事案の調査に貢献した。

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、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、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、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。

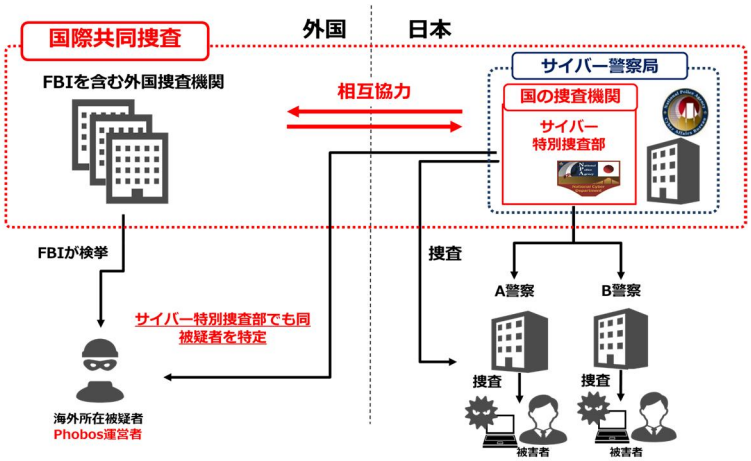
また、ICPO 加盟国の法執行機関に加えて、国外の民間企業や学術機関が参加する ICPO デジタル・フォレンジック専門家会合に参加し、情報技術解析に関する知識・経験等の共有を図っているほか、情報セキュリティ事案に対処する組織の国際的な枠組みである FIRST（Forum of Incident Response and Security Teams）に加盟し、組織間の情報共有を通じ、適切な事案対処に資する技術情報の収集を行っている。

コラム：ランサムウェアグループ「Phobos」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）」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おり、令和６年（2024 年）11 月、米国司法省は、同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。

この事案において、サイバー特別捜査部は、独自の手法により同運営者の特定に成功し、その結果や当該手法について、米国をはじめとする関係国の捜査機関に提供した。

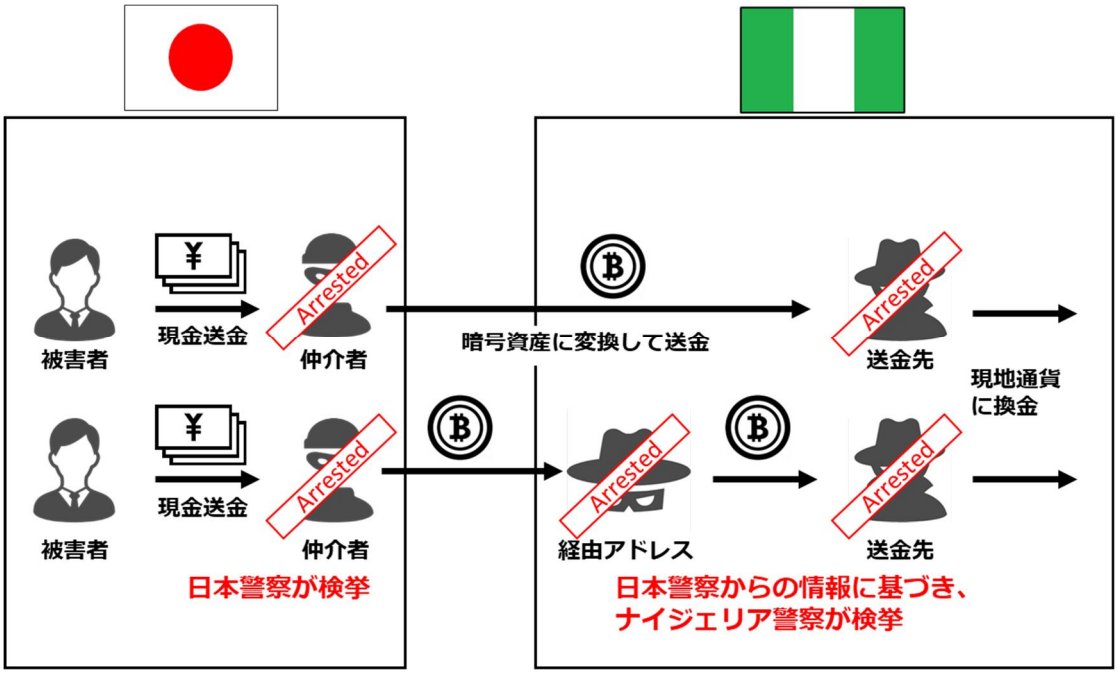
【図表 22：ランサムウェアグループ「Phobos」に対する国際共同捜査の概要】



コラム：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、インターポールが主導するオペレーション「ジャッカル」において国際共同捜査が進められており、日本警察も令和６年４月から同オペレーションに参画していた。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。

【図表 23：ナイジェリアとの国際共同捜査の概要】



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 回国会に提出した。

(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。さらに、これら情報等を活用し、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。

コラム：　TraderTraitor に関するパブリック・アトリビューション

令和６年 12 月、警察庁は、サイバー特別捜査部及び警視庁による捜査及び分析の結果を総合的に評価し、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）とともに、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、合同で文書を発出した。本件において、TraderTraitor は、リクルーターになりすまして接触するソーシャルエンジニアリングの手口で必要な情報を窃取した。

警察庁は、内閣サイバーセキュリティセンター（NISC）及び金融庁との連名で注意喚起を行い、標的となり得る事業者に対し、TraderTraitor の手口を説明したほか、サイバー空間の脅威を認識するとともに、適切なセキュリティ対策を講じるよう呼び掛けた。

コラム： 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、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た。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。

また、日米等の関係各国では、DDoS 攻撃ウェブサービスのインフラ管理者や利用者に対する国際共同捜査を推進しており、我が国も EUROPOL 主導のオペレーション「PowerOFF」に参画してきたところ、令和６年 12 月に DDoS 攻撃ウェブサービスの利用者対策として実施された関係国法執行機関による広報啓発キャンペーンにも参画し、警察庁ウェブサイトにおいて、DDoS 攻撃に関する注意喚起メッセージを掲載した。

【図表 24：オペレーション「PowerOFF」の HP】

さらに、警察庁は、関係省庁等とともに、令和６年９月から 10 月に米国で開催された「カウンターランサムウェア・イニシアティブ会合（CRI 会合）」に参加し、ランサムウェアの脅威への対処に関する国際連携について議論を行った。同会合では共同声明が出されたほか、ランサムウェア攻撃を受けた組織を支援するためのガイダンスが発出された。

【図表 25：CRI 会合の様子】

② 関係機関との連携を通じた情報発信

産学官連携の枠組みである一般財団法人日本サイバー犯罪対策センター（JC3）においては、産学官の情報や知見の集約・分析をし、その結果を還元しているところ、警察からは捜査関連情報等を共有し、産学におけるサイバーセキュリティに関する取組に貢献するとともに、JC3 において共有された情報を警察活動に迅速・的確に活用している。

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、令和 6 年 12 月、警察庁はランサムウェア等のサイバー事案による被害拡大防止のため、関係省庁に対して、サイバー攻撃を想定した事業継続計画（BCP）を策定し、初動対応における警察との連携について記載すること、被害発生時に速やかに通報・相談すること、初動対応としてログの保全に努めること等について、業界団体及び事業者等へ周知するよう要請した。

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。

(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。

また、サイバー特別捜査部における分析（以下コラム参照。）により、令和 2 年頃から確認されている OSS[5]（EC サイト構築ソフト）のぜい弱性に起因するクレジットカード情報の漏えい被害について、現在でも発生している状況が明らかになったことから、令和 6 年 11 月、経済産業省と事業者団体に対し、手口情報等の提供を行うとともに、具体的なぜい弱性対策を講じるよう対策の強化を求めた。

[5] Open-Source Software

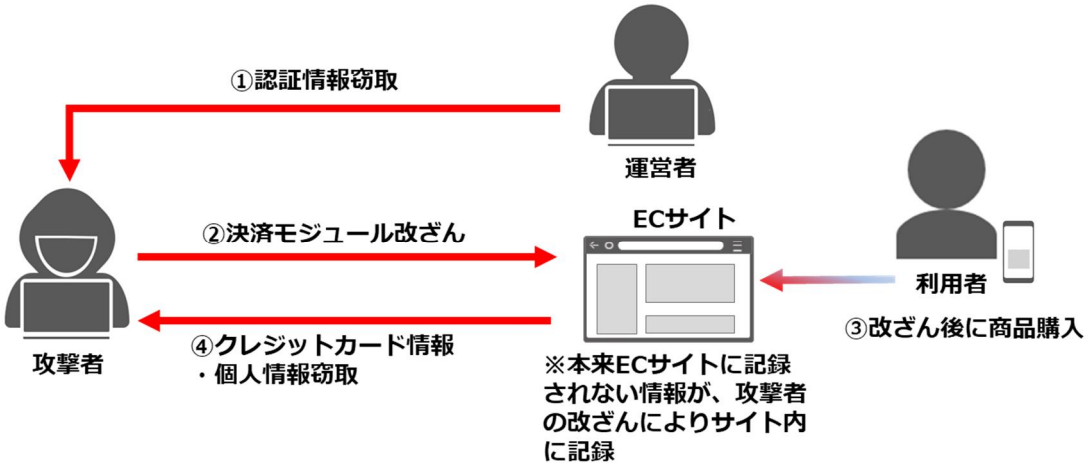
コラム：EC サイトのぜい弱性を狙ったクレジットカード情報等の窃取の実態解明

サイバー特別捜査部においては、インターネットショッピングサイト（EC サイト）を通じてクレジットカード情報や個人情報を盗む「ウェブスキミング」の手口の実態解明を進めている。

ウェブスキミングとは、EC サイトを改ざんし、利用者が商品購入の際に入力したクレジットカード情報等を窃取する手口であり、令和 6 年中、サイバー特別捜査部では、ウェブスキミングと疑われる EC サイトの改ざんを 40 件以上確認した。

これらの改ざんされた EC サイトの大多数は、EC サイト構築ソフトウェアのぜい弱性を狙った攻撃により、EC サイトの運営者用の認証情報が窃取されていた。その後、当該認証情報で不正アクセスされ、攻撃者の侵入を容易にするためのバックドアが設置されるとともに、決済システムの一部が改ざんされ、本来 EC サイト上には残らないはずのクレジットカード情報等が不正に記録されていた。攻撃者は、バックドアを経由してサイト内に記録されたクレジットカード情報や個人情報を継続的に窃取していた。

【図表 26：ウェブスキミングの手口】



改ざんされた EC サイトは、従前と変わらず商品が購入できるなど基本的な機能が変わらないため、運営者側と利用者側の双方とも情報窃取の被害に気付きにくいものがある（特に被害が潜在化・長期化しやすい事例については、資料編参照。）。

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、令和6年9月より、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・提供する取組を新たに開始した。

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[6]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。

【図表 27：サイバー防犯ボランティアへの支援】

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、令和6年2月及び7月に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」を実施した。

○　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年秋にボイスフィッシングによる不正送金被害が急増したことを受け、金融庁等と連携し、その手口や対策に関する注意喚起を実施した。

---

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

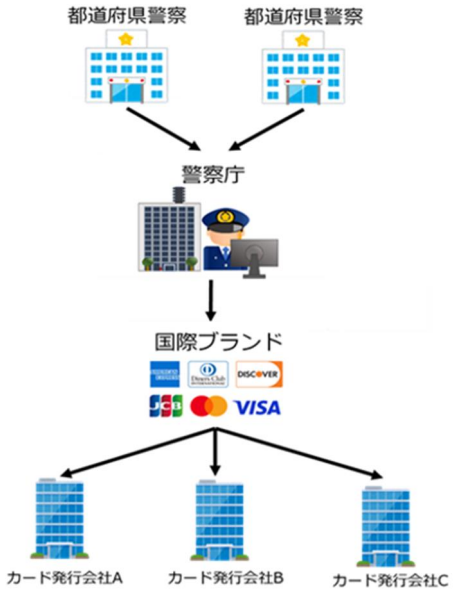
また、警察庁は、暗号資産交換業者等と連携して、犯罪に利用された取引口座の凍結を実施しているほか、令和６年２月、金融庁と連携し、一般社団法人全国銀行協会等に対して、暗号資産交換業者の金融機関口座に対して送金元口座名義人名と異なる依頼人名で行われる送金の拒否、暗号資産交換業者への不正な送金への監視強化等の、会員等における対策強化を要請した。

さらに、SIM スワップによる不正送金対策として、令和４年９月に引き続き、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。

○　クレジットカード不正利用対策

令和６年 12 月、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、一括して提供する仕組みを構築した。これにより、国際ブランド各社から連絡を受けたカード発行会社においては、警察庁から提供されたクレジットカード番号の利用停止等の措置をより迅速に講ずることが可能となった。

【図表 28：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】



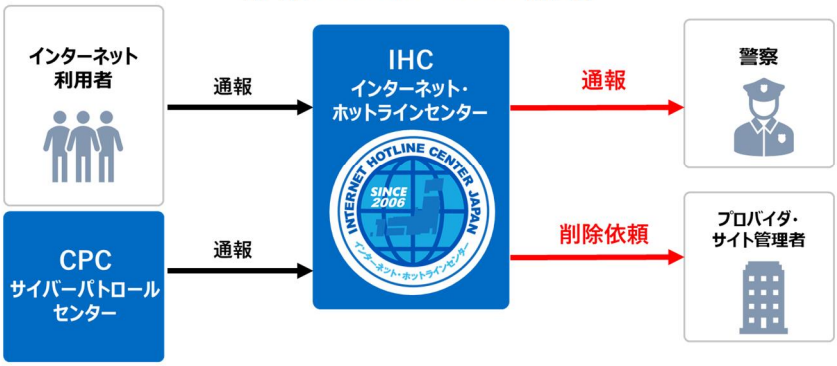
③　違法・有害情報に関するインフラへの対処

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。

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。

[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

【図表 29：IHC・CPC の概要】



令和 6 年における IHC の受理件数のうち、運用ガイドラインに基づいて 546,941 件を分析した結果、違法情報を 66,834 件、重要犯罪密接関連情報を 14,149 件、自殺誘引等情報を 6,582 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。

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等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、令和 7 年 2 月 28 日、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）に位置付けるなど、IHC の取組強化を図った。

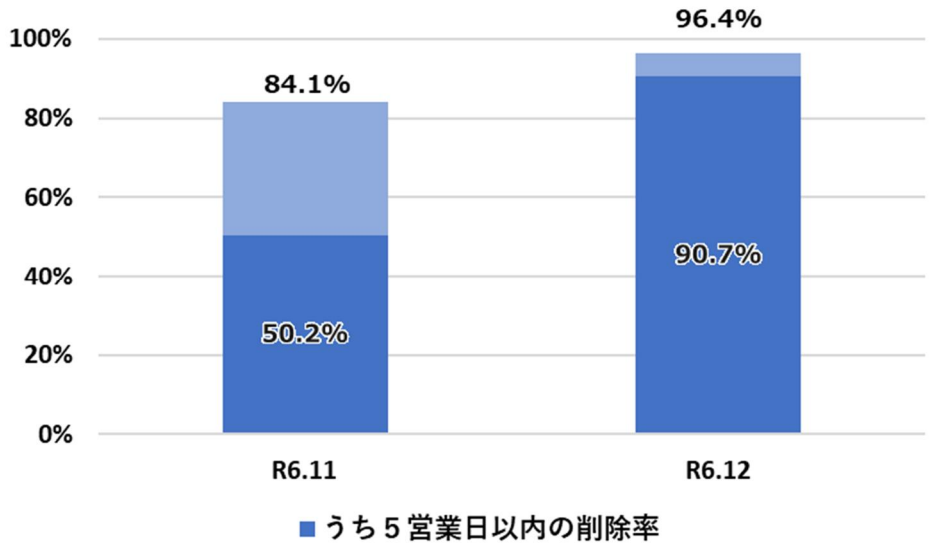
さらに、海外大手 SNS 事業者と連携し、当該 SNS において、「ホワイト案件」等のほか、「バイト」、「仕事」等、求人に関する一般的なキーワード検索を行った際に、「闇バイト」の危険性を注意喚起するポップアップ機能の実装に至った。

このほか、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 6 年中には、4,807 件の個別警告を実施している。

コラム：犯罪実行者募集情報の迅速な削除

警察及び IHC は、関係事業者に対し、違法・有害情報の削除を依頼しているところ、当該投稿を目にする人を減らすためには、投稿の迅速な削除が重要である。令和 6 年 11 月、総務省が犯罪実行者の募集を職業安定法違反と位置付けた違法情報ガイドライン案を公表したことなどを踏まえ、警察庁は、ある事業者と協議し、同事業者は、同月から IHC からの犯罪実行者募集情報の通報方法を違法情報と同様の運用に変更した。その結果、削除依頼に対する 5 営業日以内の削除率が、12 月には 90%を超えるなど、犯罪実行者募集情報の迅速な削除が行われるようになった。

【図表 30：令和６年 11 月及び 12 月の犯罪実行者募集情報の最終的な削除率】



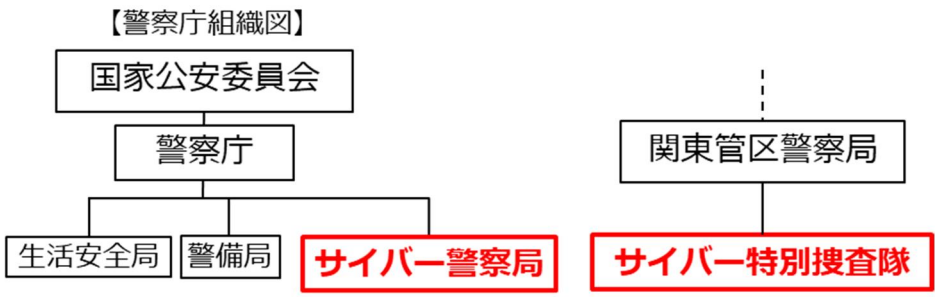
加えて、「いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策」（令和 6 年 12 月 17 日犯罪対策閣僚会議決定）に基づき、関係機関・団体・民間事業者等の協力を得ながら、各種施策を強力に推進している（「資料編」参照）。

３　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。

【図表 31：サイバー警察局及びサイバー特別捜査隊の設置】

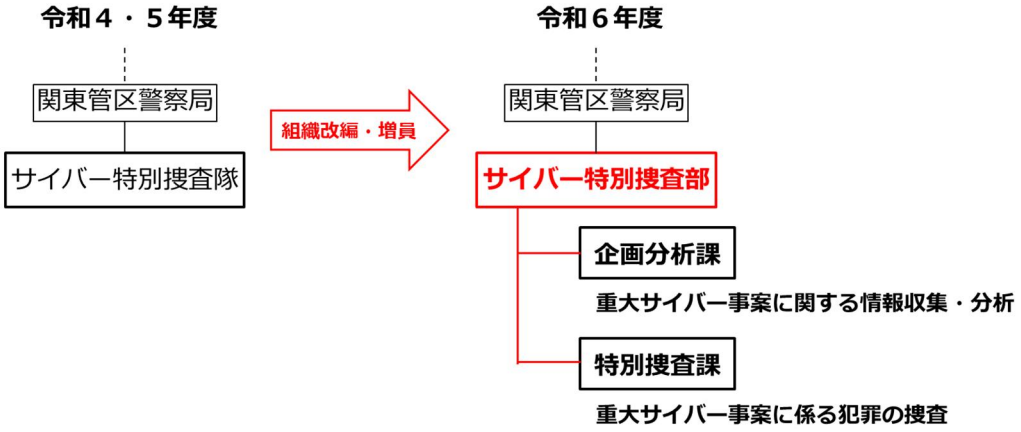


同隊は、従来、外国捜査機関等と都道府県警察との間で調整機能を果たすに過ぎなかった警察庁が、全国を管轄して直接捜査を実施し、国の捜査機関として国際共同捜査を通じて被疑者を検挙することを目的として設置された組織であり、全国警察からサイバー分野の知識や経験を豊富に持つ有為な人材を登用し、高度な資機材を整備した。高い捜査力・技術力を備えた結果、それまで対応が困難であった事案の被疑者の特定・犯罪グループの全体像の解明が可能となるとともに、外国捜査機関等と情報交換を継続的かつ緊密に行うことで、強固な信頼関係の構築を実現している。

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、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 37）。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。

さらに、令和７年度予算案には、サイバー特別捜査部の更なる増員に加え、同部に特別対処課を設置することも盛り込んでいる。

【図表 32：サイバー特別捜査部への発展的改組】



また、都道府県警察においても、京都府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。

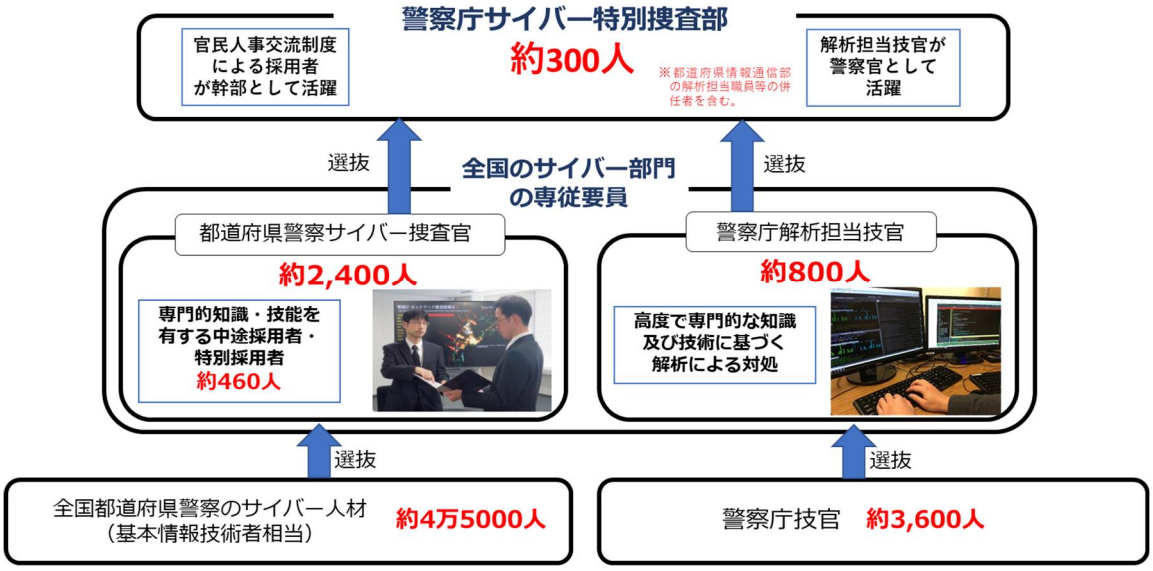
(2) 人材育成

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 460 人が、サイバー事案への対処について高度な知見を有するサイバー犯罪捜査官等の専門捜査員として、捜査の第一線で活躍している。

また、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。

こうした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、警察では、職員の採用・登用、教育・研修、キャリアパスの管理等を部門横断的かつ体系的に実施している。

【図表 33：警察におけるサイバー人材】



また、警察大学校サイバーセキュリティ対策研究・研修センター捜査研修室では、都道府県警察の捜査員等を対象とした高度な実践的研修を実施しており、例えば、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。

加えて、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。

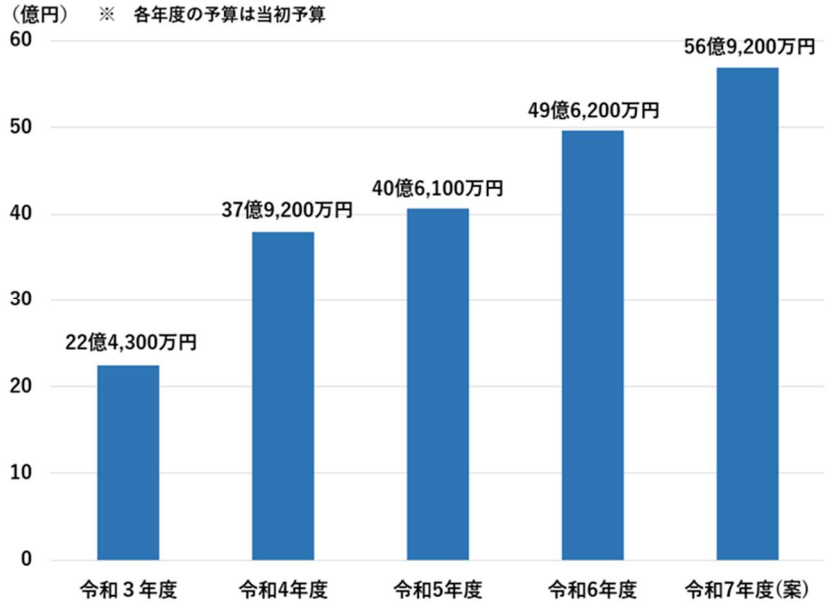
このほか、サイバー関係の知識が、全ての捜査分野において不可欠となっている状況を踏まえ、令和７年４月、警察大学校にサイバー部門に係る研修・訓練に特化したサイバー警察教養部を新設する予定であり、都道府県警察のサイバー部門においてサイバー事案の対処に当たる捜査員を対象とした実践的な研修や、都道府県警察の各部門の捜査幹部に対するサイバーリテラシーに係る研修等を体系的、効果的かつ一元的に実施する予定である。

(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。

実際、令和６年度の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７年度の予算案では、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 34：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

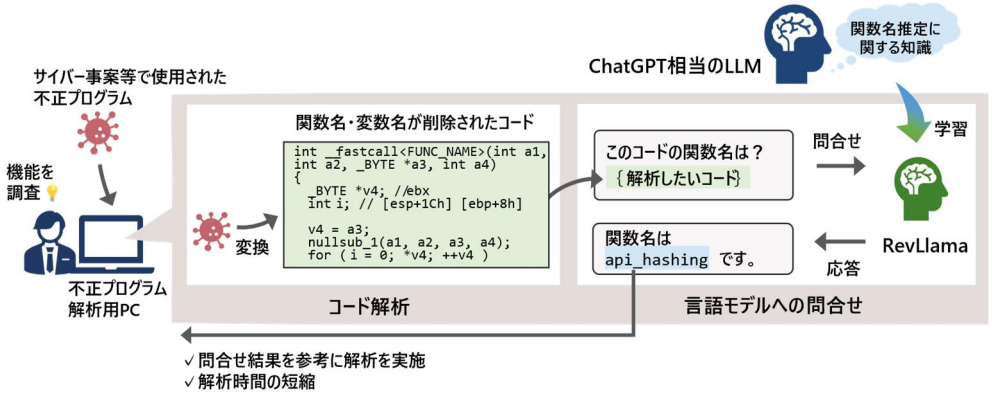
警察庁の情報技術解析部門においては、犯罪捜査、被害拡大の防止等を目的に各種不正プログラムの解析を実施しているほか、情報セキュリティ大学院大学へ職員を派遣し、現在は不正プログラム解析の効率化を目的とした機械学習に関して研究を進めている。

コラム：生成 AI を用いた不正プログラムの機能推定手法

サイバー事案の実態を解明するためには、攻撃で使用された不正プログラムを詳細に解析し、その機能や動作を把握する必要がある。しかし、不正プログラムの開発時に使用された機能の名称が判明せず、解析に時間を要することが多い。

そこで本研究では、機能名を高精度で推定する生成 AI「リブラマ（RevLlama）」を開発した。実際の不正プログラムを用いて RevLlama を検証した結果、適切な機能名を推定できる傾向を確認したことから、この RevLlama を不正プログラムにおける機能の解析に活用することで、実務における解析時間の短縮が期待される。

【図 35：生成 AI を用いた不正プログラムの機能推定手法のイメージ】



資料編[1]

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年における主なサイバー攻撃事例 ･･････････････････････････････････ 42
・令和６年に公表されたぜい弱性の危険性と対策 ･･････････････････････････ 44
・ランサムウェアの被害に関する統計 ･･････････････････････････････････････ 45
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
・警察に対する相談に係る統計 ･･ 52
・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 ･･････････････ 53
・クレジットカード不正利用被害に関する統計 ･･････････････････････････････ 56
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 ･･････････････････････････････ 57
・過去の国際共同捜査の主な事案一覧 ･･････････････････････････････････････ 64
・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 ･･････ 67
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） ･･････････････････････ 68
・サイバー対処能力強化法案及び同整備法案の概要 ･･････････････････････ 69
・パブリック・アトリビューションの事例一覧 ･･････････････････････････････ 70
・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 ･･････････････ 72
・EC サイトのぜい弱性を狙ったクレジットカード情報・個人情報窃取の実態解明
等（改ざんされた EC サイトにおける被害が潜在化・長期化しやすい事例） ･･･ 74
・被害防止に関する警察の取組 ･･ 75
・いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策･ 76
・違法・有害情報の分析に関する統計 ･･････････････････････････････････････ 78
・IHC 運用ガイドラインの改定･･ 81
・違法・有害情報に関する関係機関との連携 ･･････････････････････････････ 82

[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年における主なサイバー攻撃事例

● **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。

● **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６年２月、同年７月及び同年 10 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。

● **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。

● **半導体関連機器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。

● **大手鉄道事業者に対する妨害目的とみられるサイバー攻撃**

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。

---

[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年における主なサイバー攻撃事例②

● **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。

● **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 20 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。

● **国内の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６年７月、国内の宇宙航空分野の研究開発機関は、VPN 装置のぜい弱性を起点とする不正アクセスにより、侵害を受けた端末、サーバ及びクラウド上で管理していた情報の一部が漏洩したことを発表した。

● **エネルギー関連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６年７月、エネルギー関連事業者は、外部からの不正アクセスにより、業務委託元から提供を受けている個人情報等が流出した可能性があることが判明したと発表した。

● **金融機関等に対する 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。

（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）

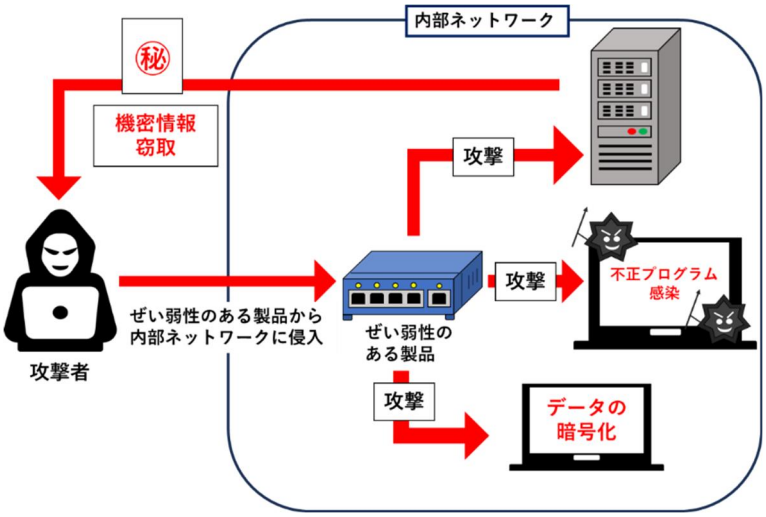
令和６年に公表されたぜい弱性の危険性と対策

令和６年は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おいて、悪用されると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複数公表された。また、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[3]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】



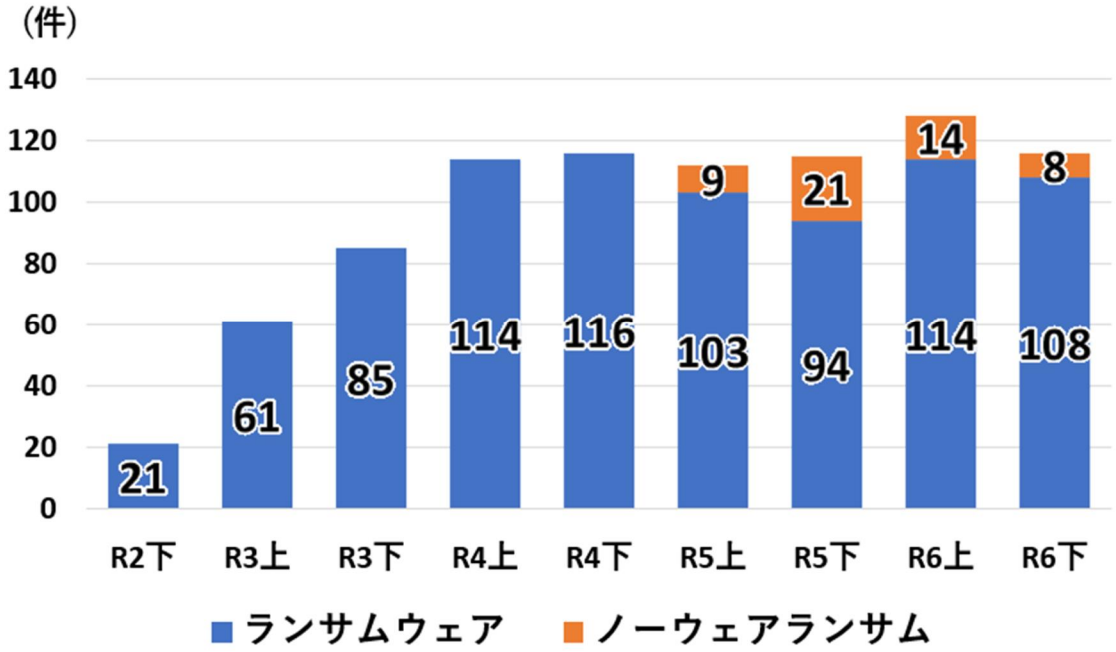
[3] ぜい弱性の内容や対策方法をまとめた文書

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）

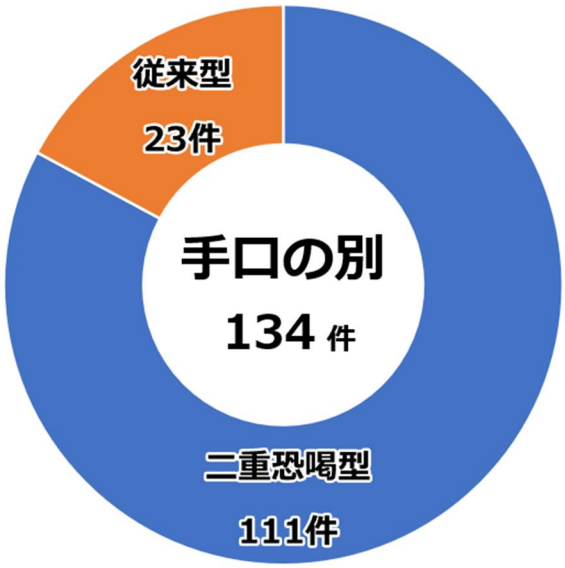
ランサムウェアの被害に関する統計

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。

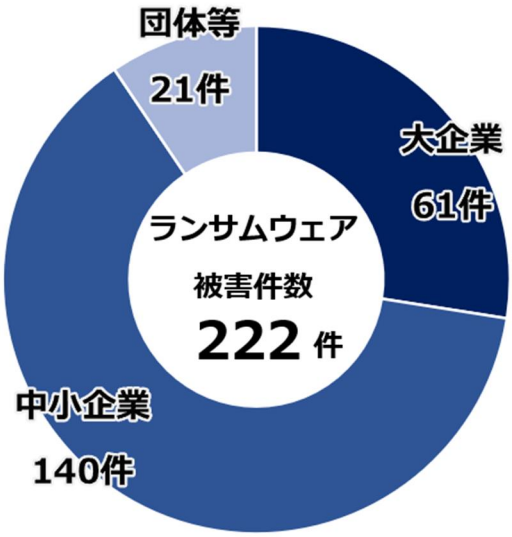
２　手口別報告件数

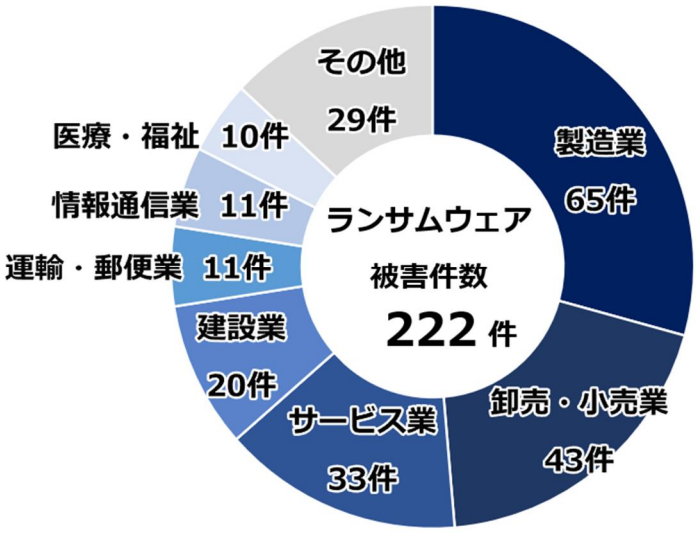


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

ランサムウェアの被害に関する統計②

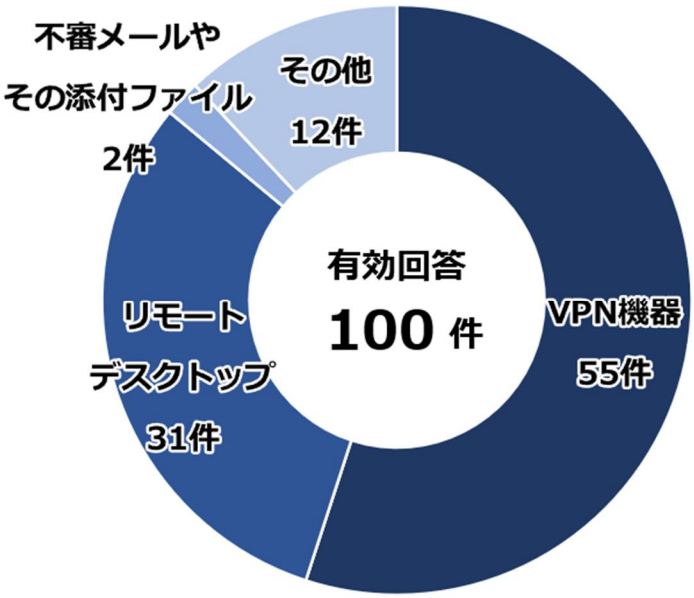
３　被害企業・団体等の規模別／業種別報告件数





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

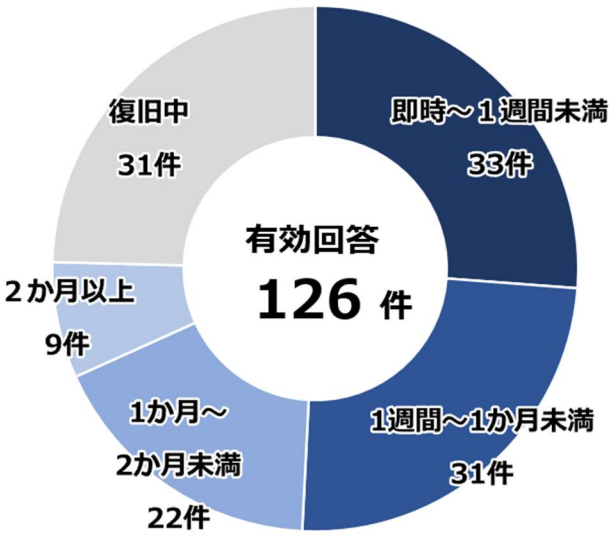
● 感染経路

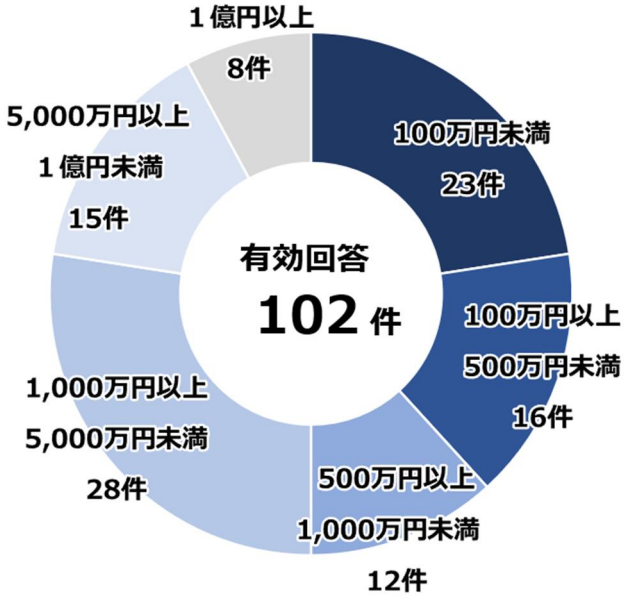


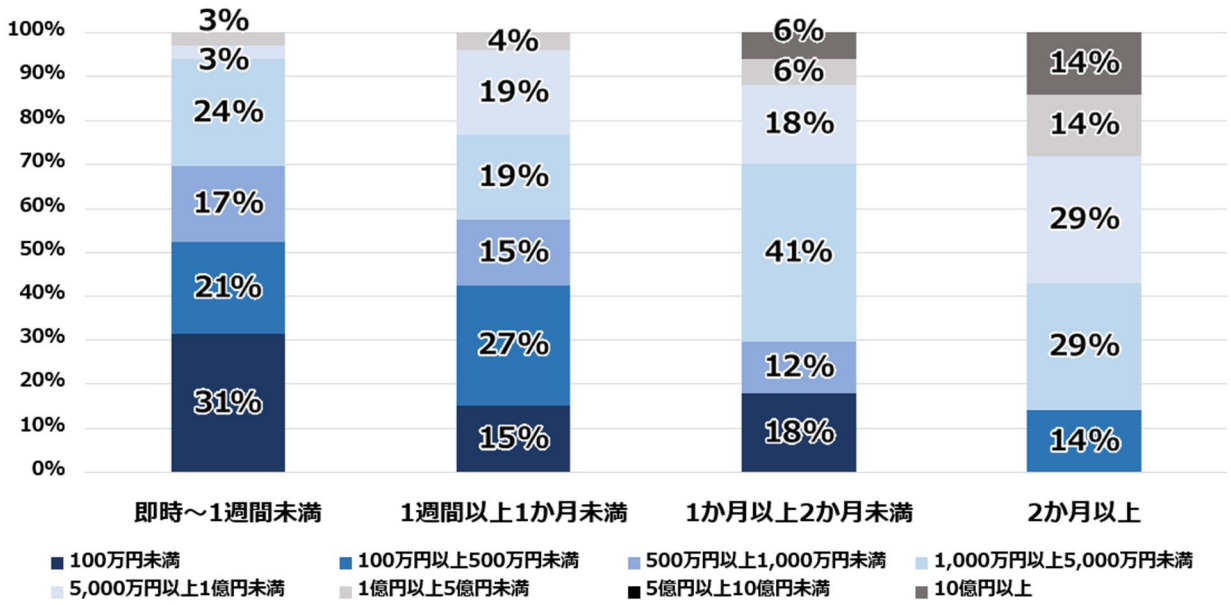
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

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





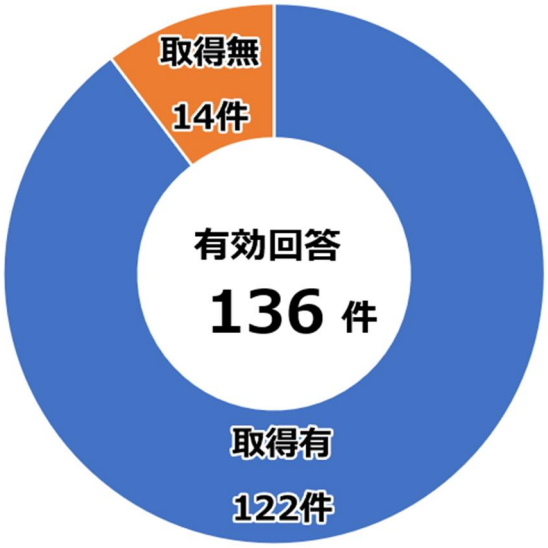


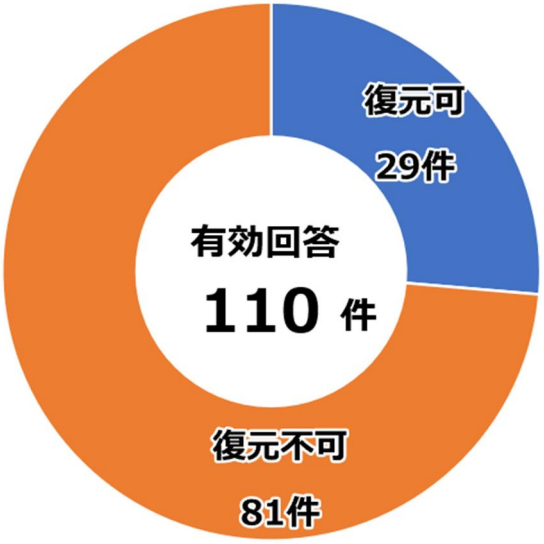
※　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも 100 にならない。

（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）

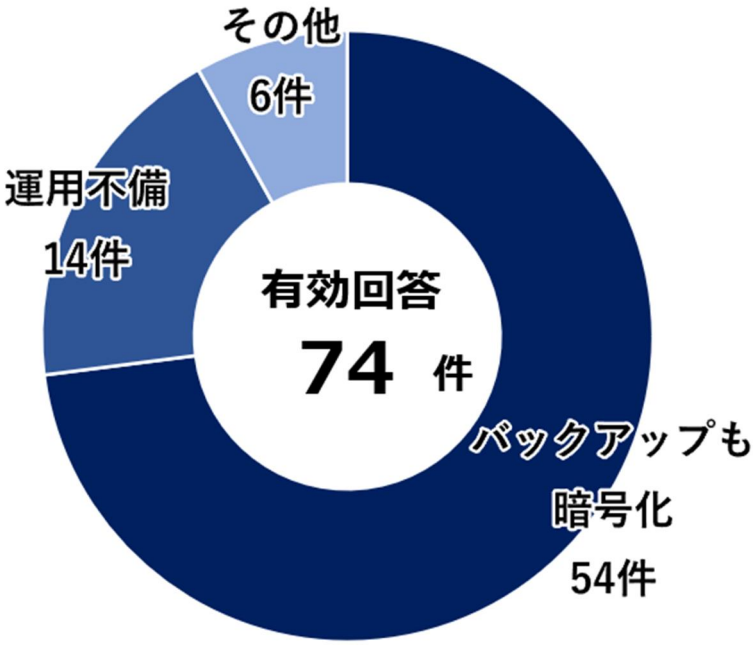
ランサムウェアの被害に関する統計④

● バックアップの取得状況／バックアップからの復元結果





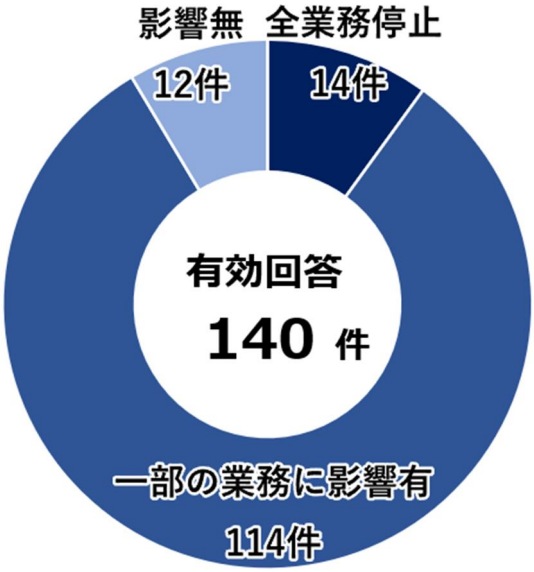
● バックアップから復元できなかった理由

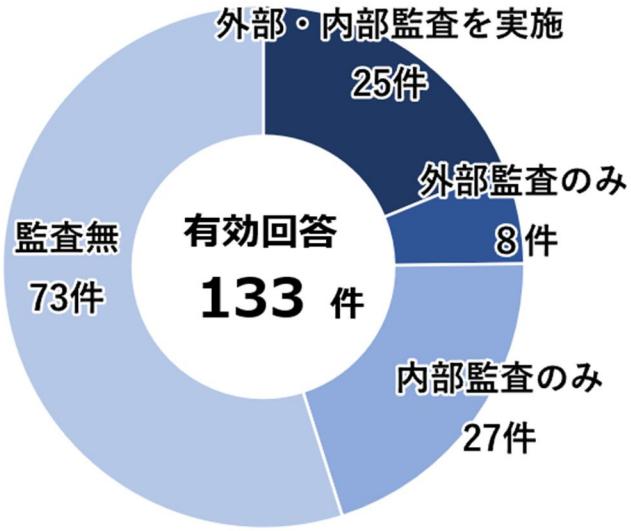


（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

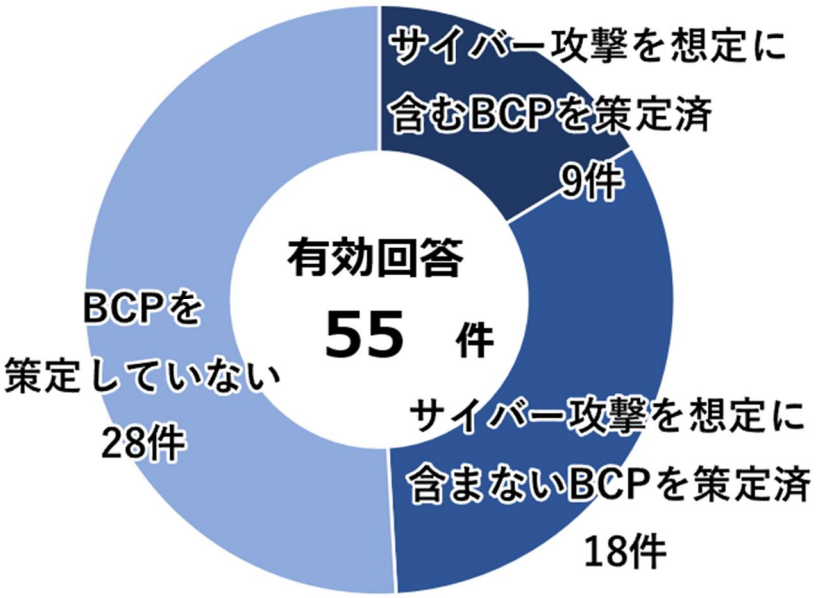
ランサムウェアの被害に関する統計⑤

● 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





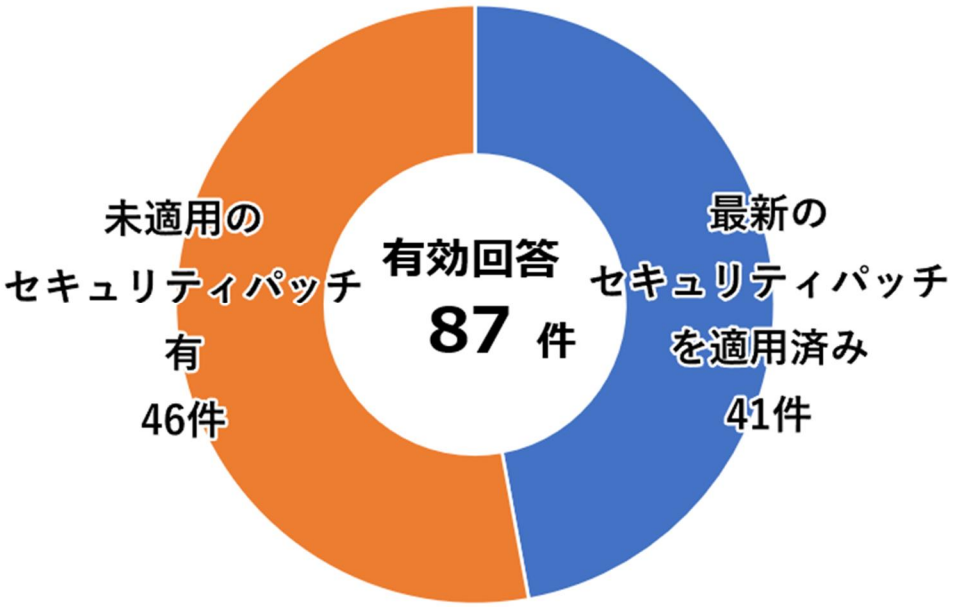
● 被害企業・団体等における事業継続計画（BCP）の策定状況



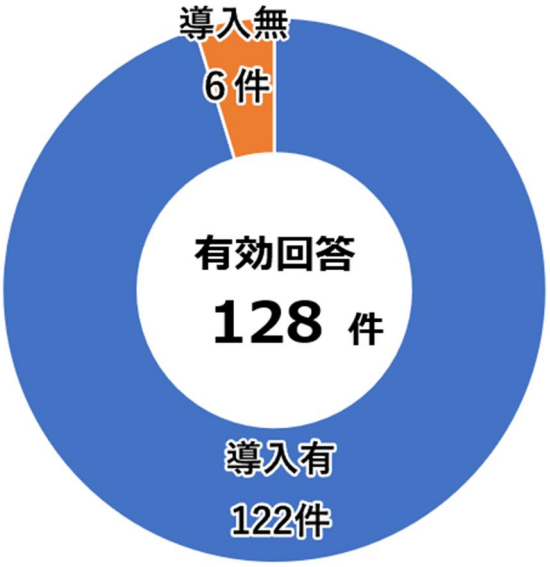
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

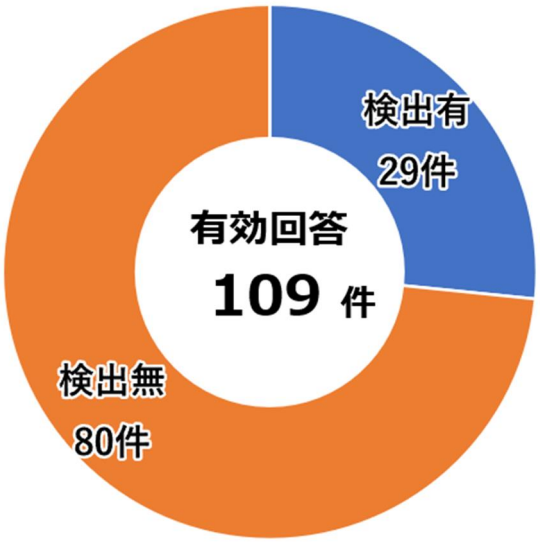
ランサムウェアの被害に関する統計⑥

● 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

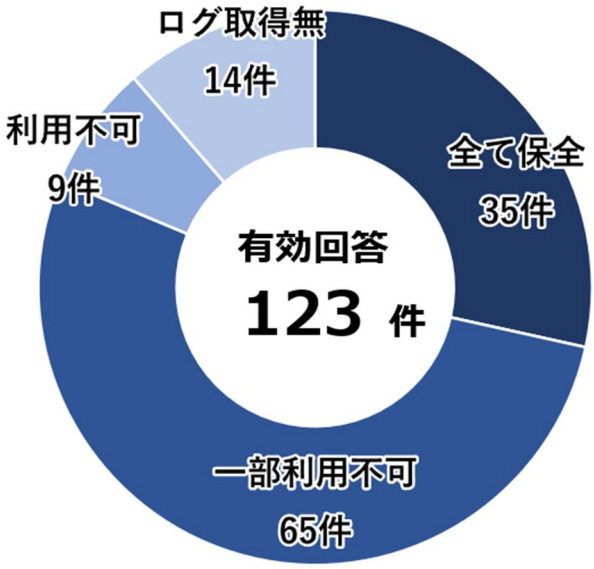




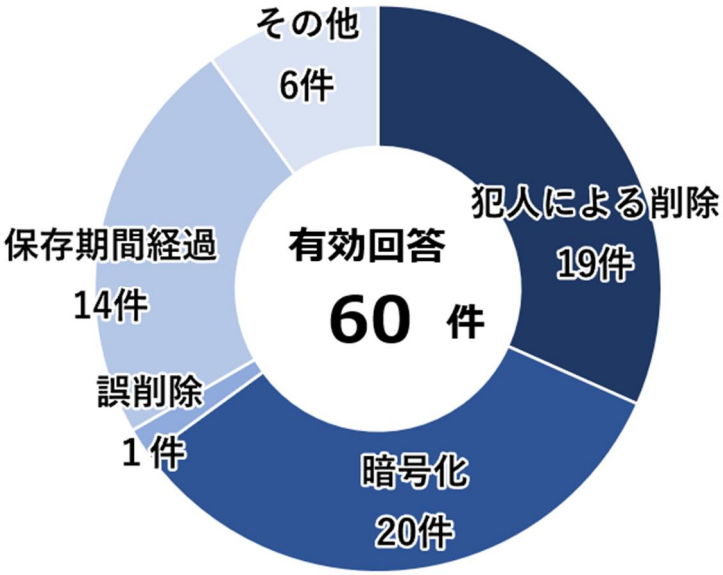
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

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

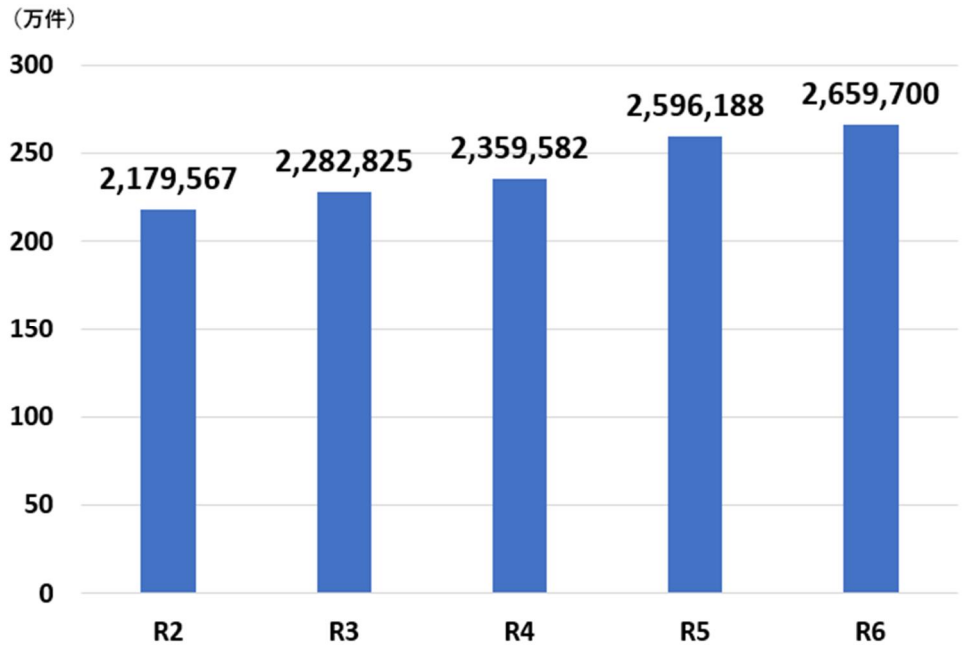


資料編

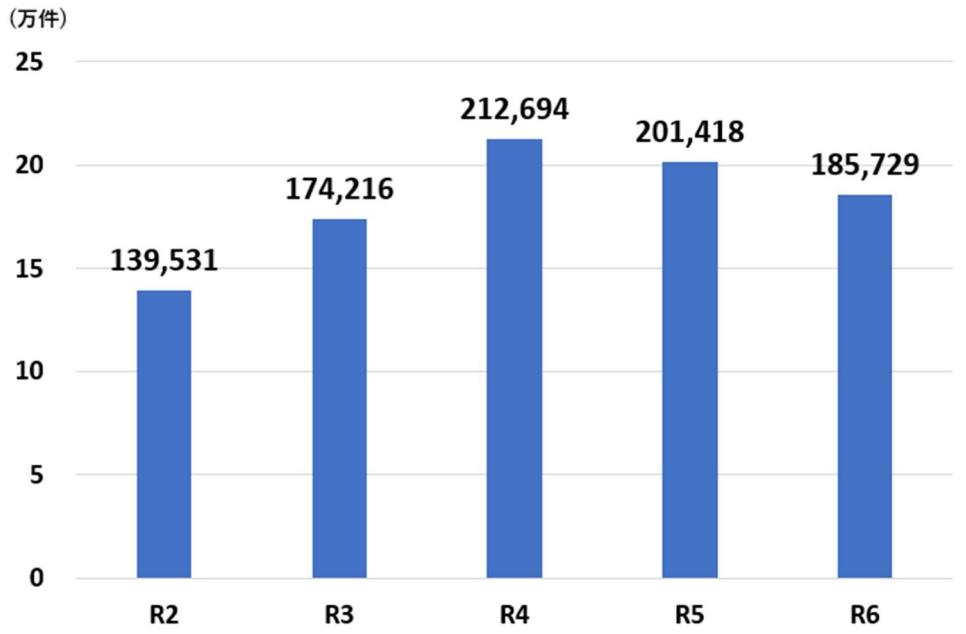
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

警察に対する相談に係る統計

１　警察で取り扱った相談件数の推移



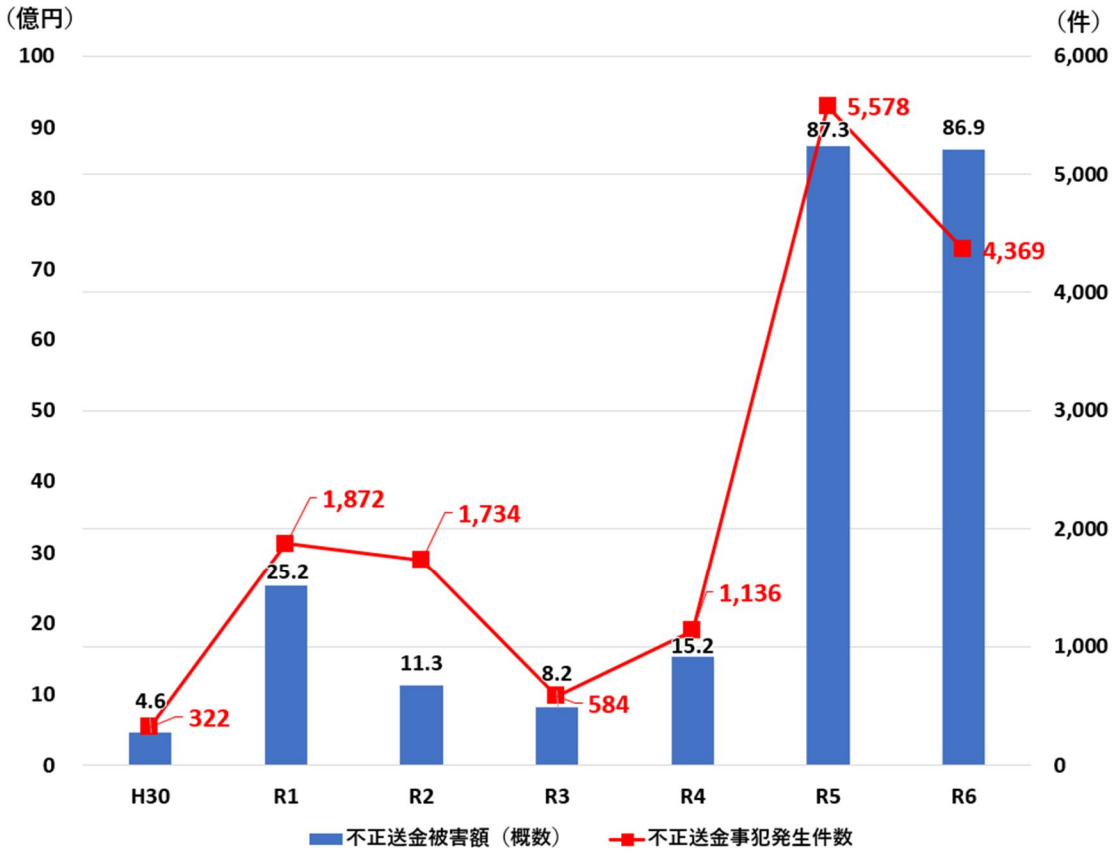
２　警察で取り扱ったサイバー関係の相談件数の推移



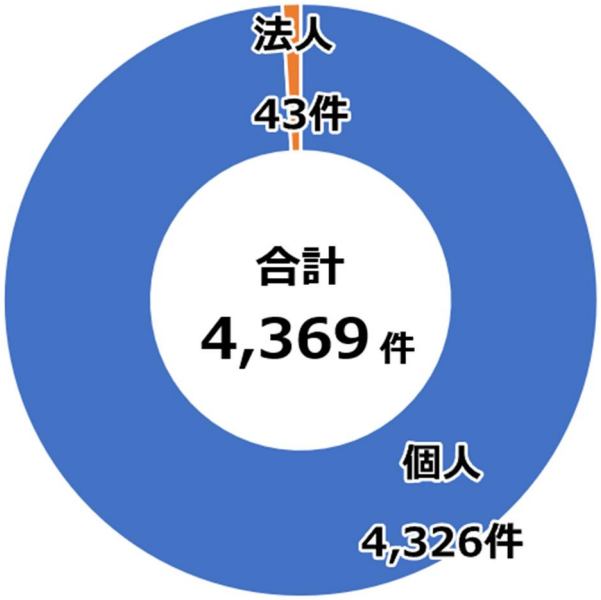
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

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



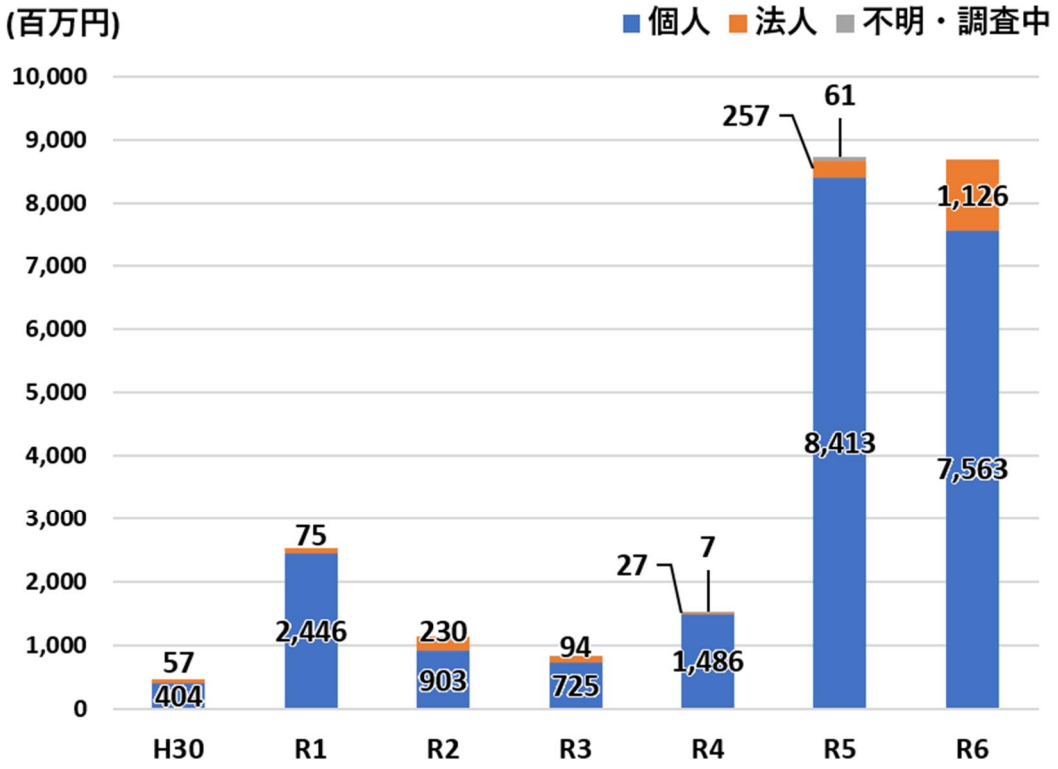
２　インターネットバンキングに係る不正送金発生件数（個人・法人別）



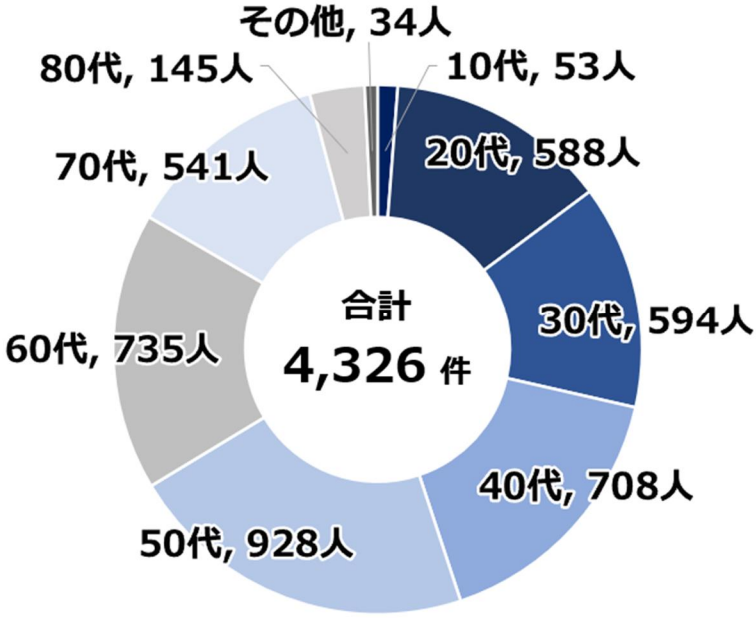
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

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）



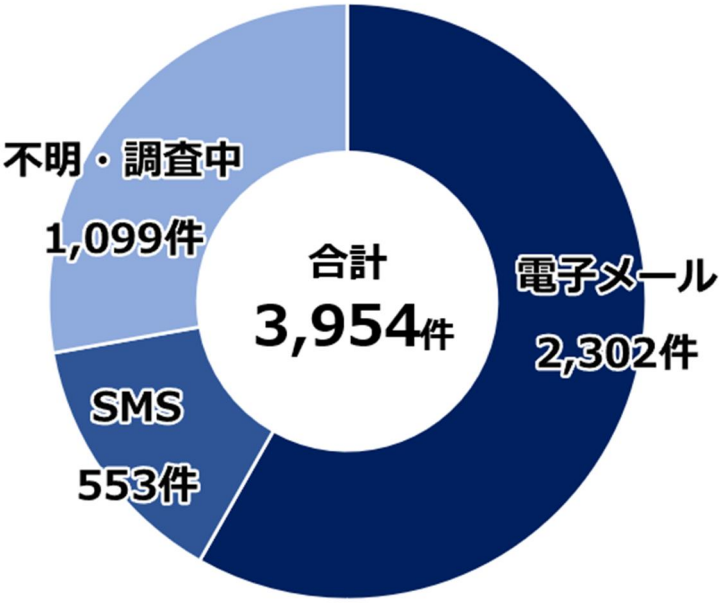
４　個人のインターネットバンキングに係る年齢別の不正送金被害者数



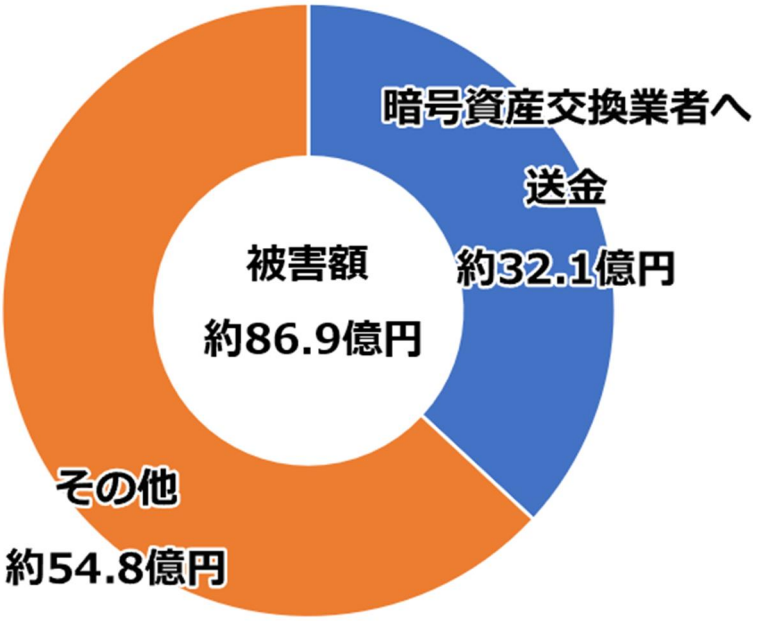
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

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[4]

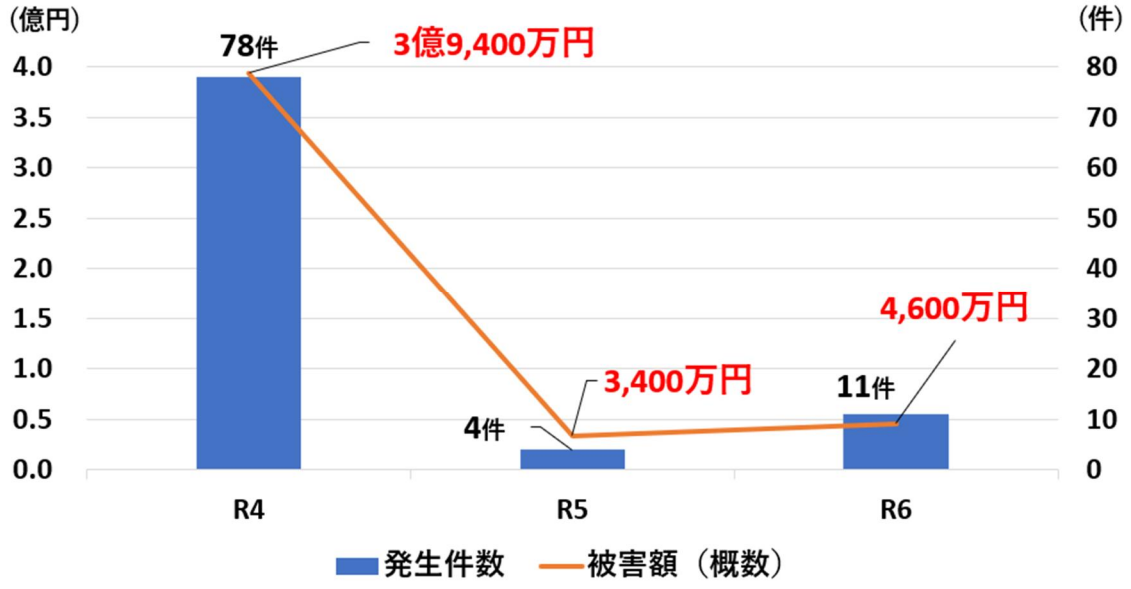


[4] 暗号資産交換業者の金融機関口座へ送金された後は、そのほとんどが暗号資産に変換されているものと考えられる。また、「その他」には、暗号資産交換業者の金融機関口座へ送金される前に被疑者等により使用されたもの、金融機関口座間の資金移動中に口座が凍結されたものを含む。

（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）

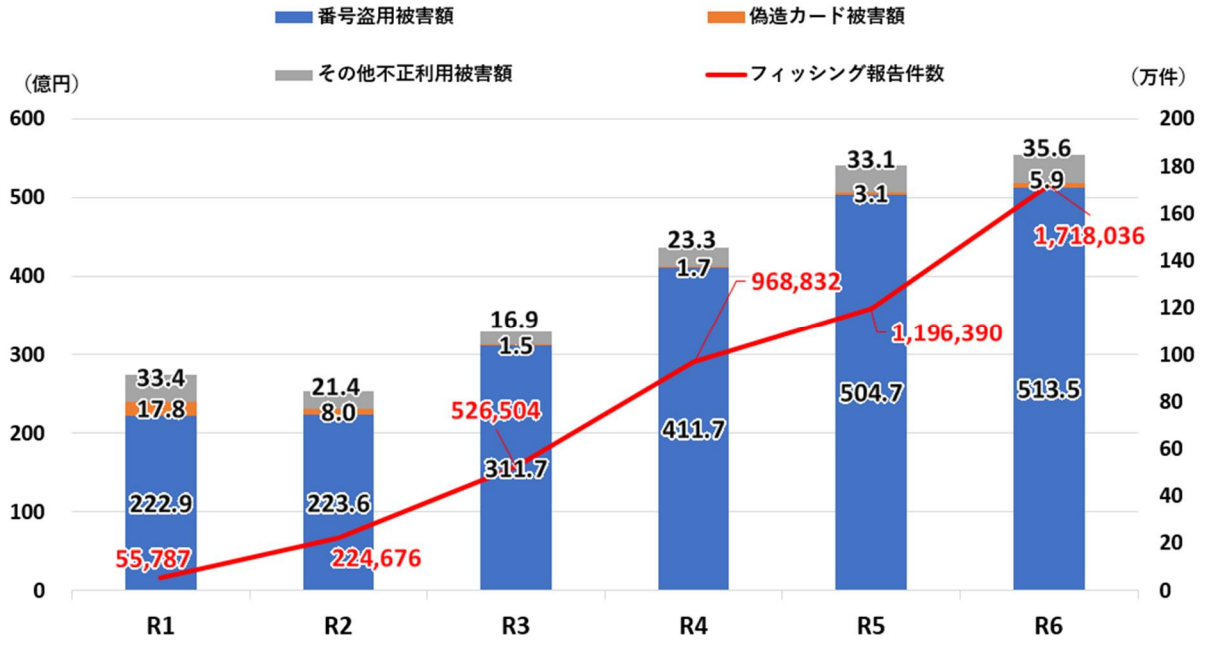
インターネットバンキングに係る不正送金事犯に関する統計④

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

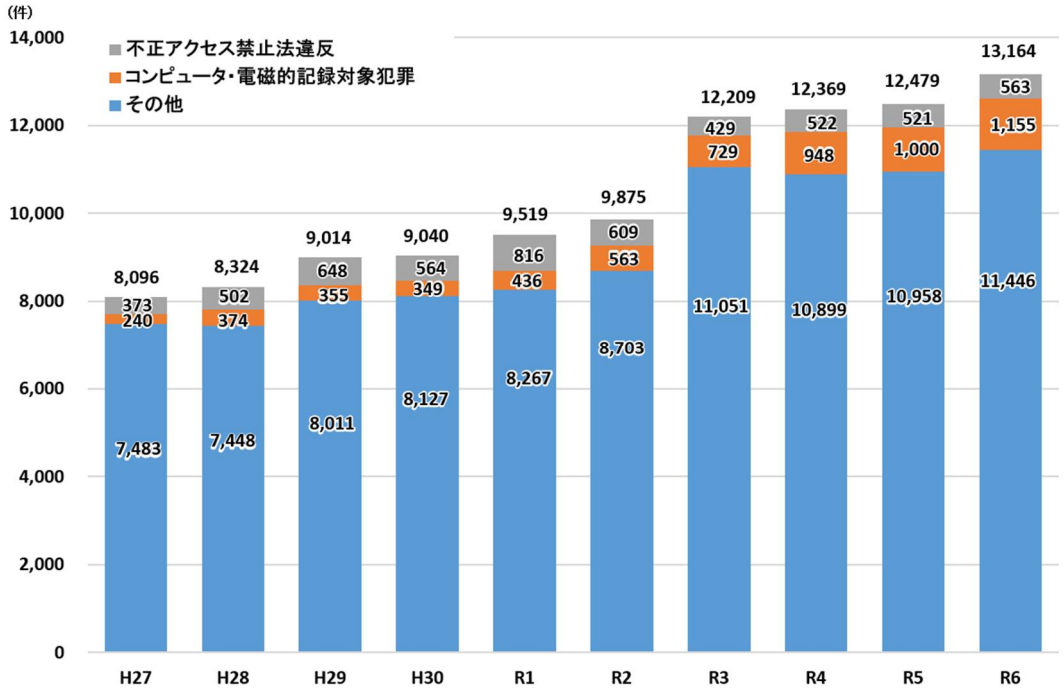


資料編

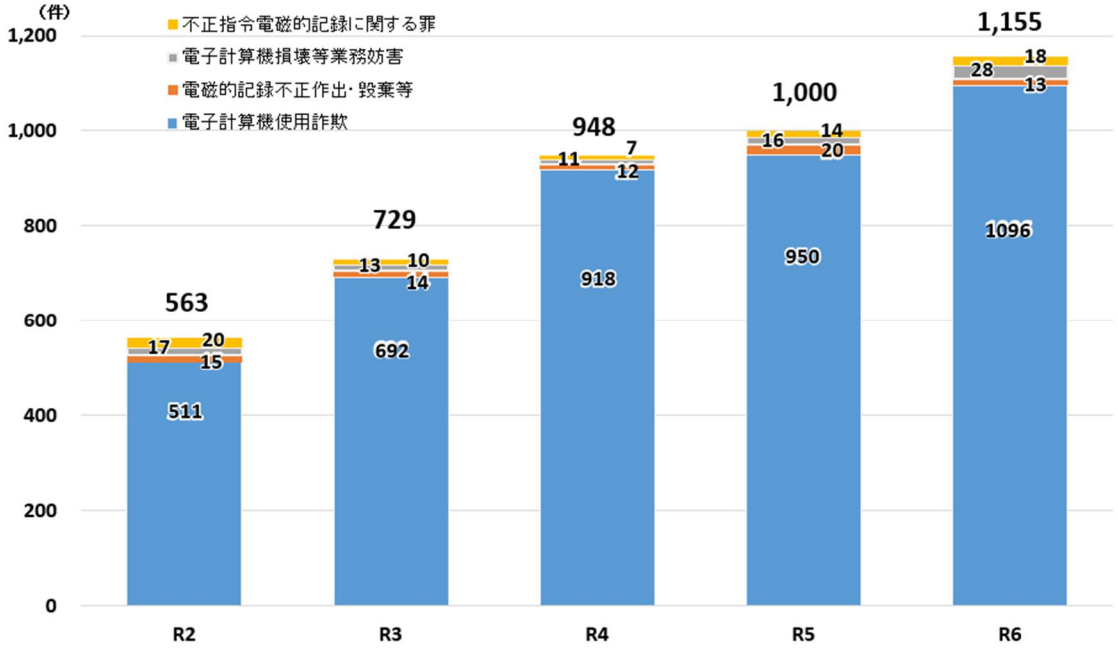
（第２部１「検挙に向けた取組」関連）

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[5]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

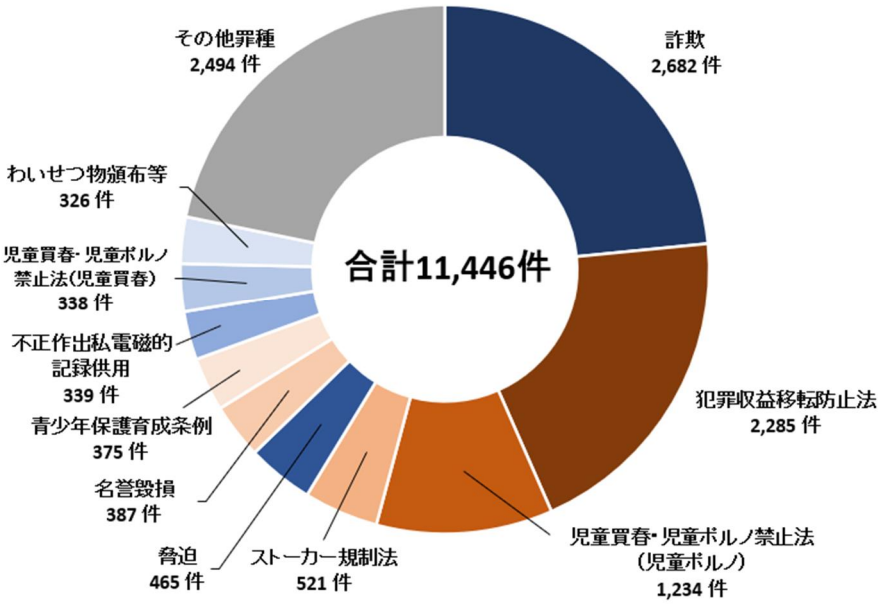


[5] 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

（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

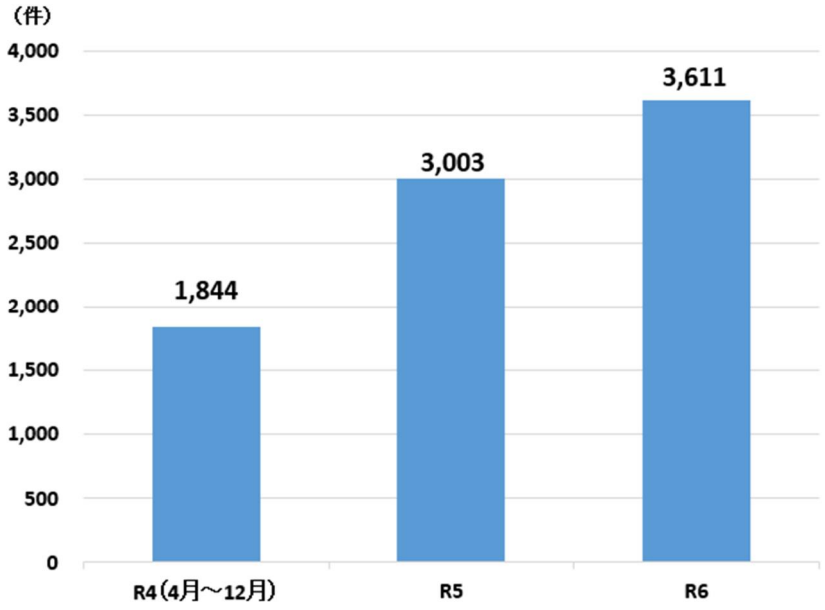
３　前記１中、「その他」の検挙状況



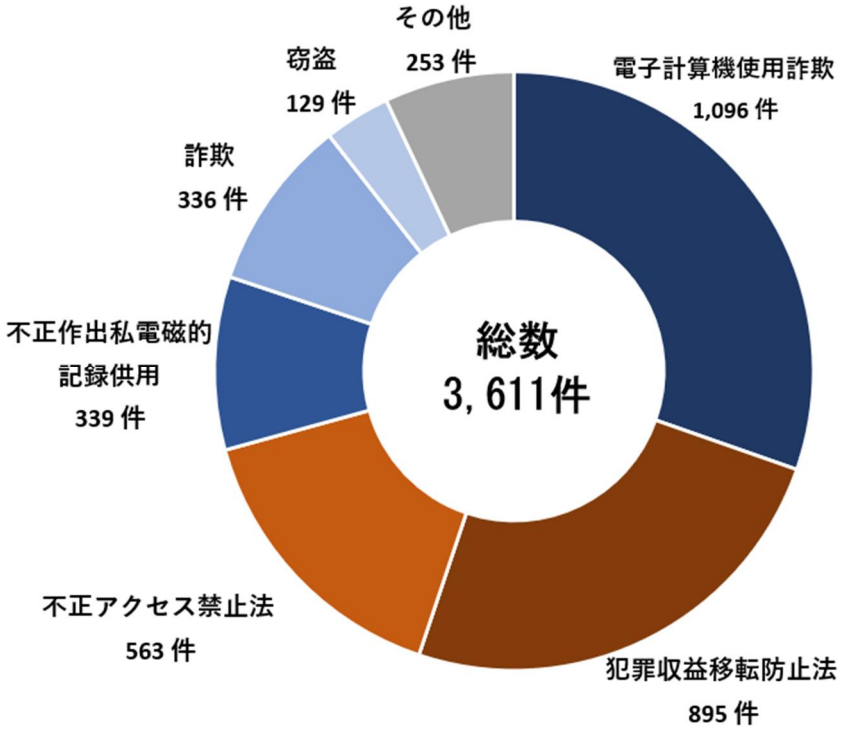
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計③

４　サイバー事案[6]の検挙件数の推移



５　サイバー事案の検挙状況

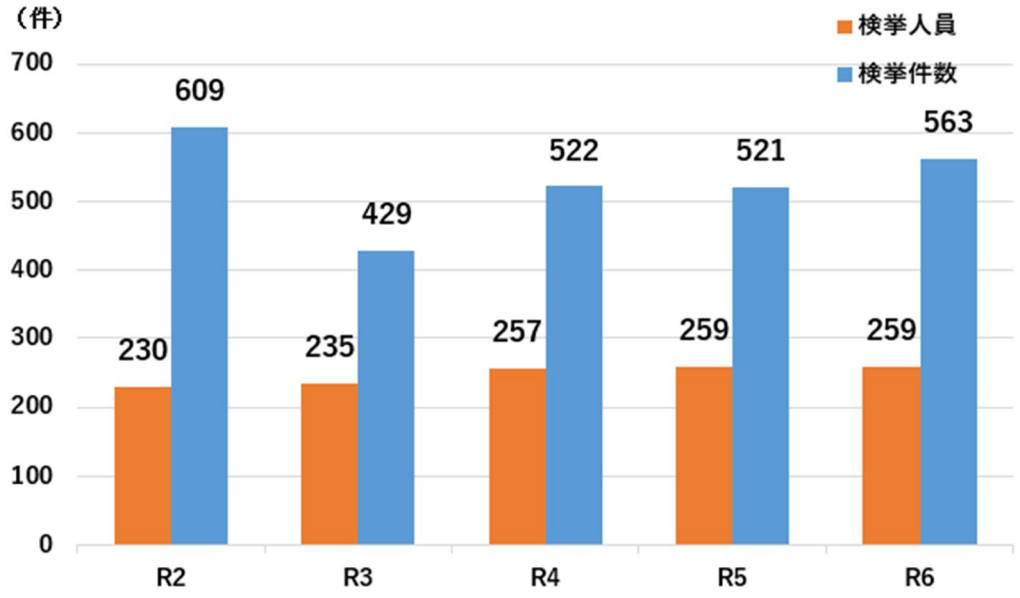


[6] サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。

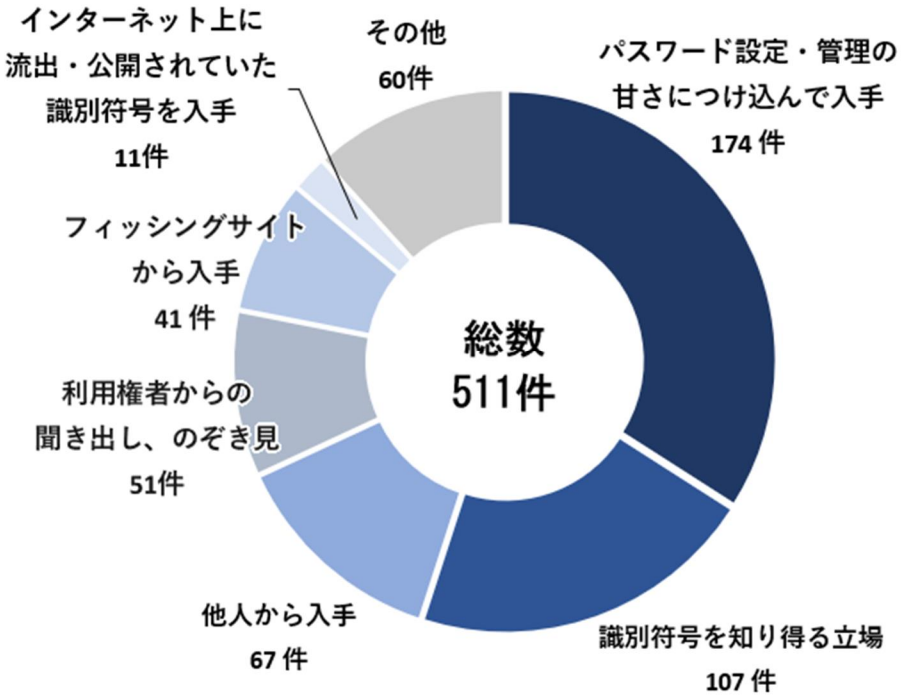
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計④

６　不正アクセス禁止法違反の検挙件数の推移



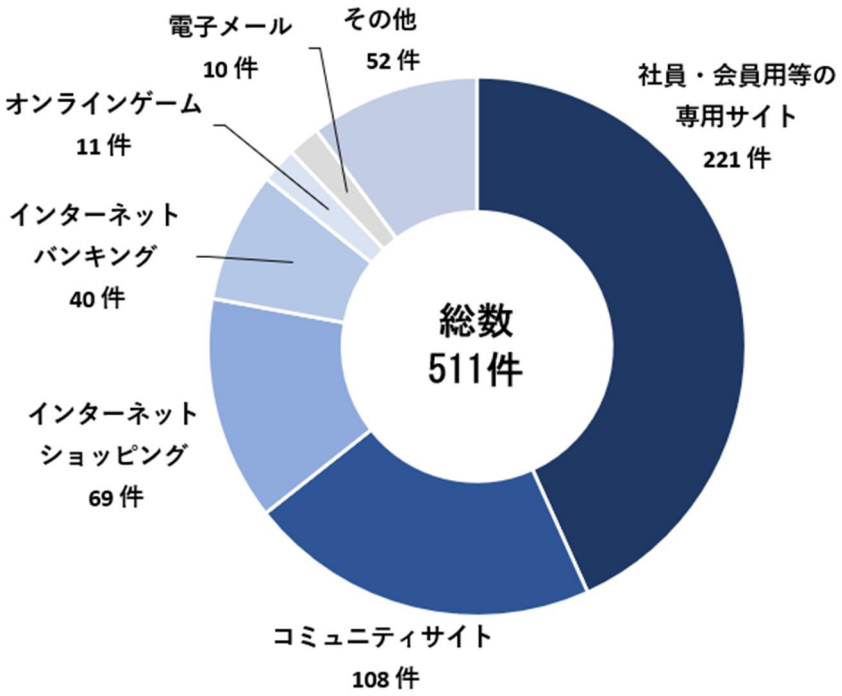
７　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



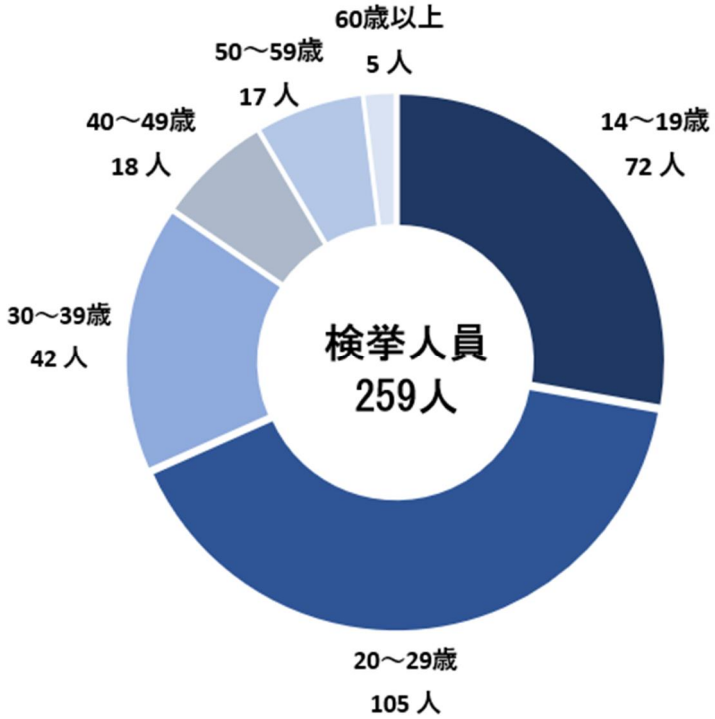
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案に関する統計⑤

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）



９　不正アクセス禁止法違反被疑者の年齢構成

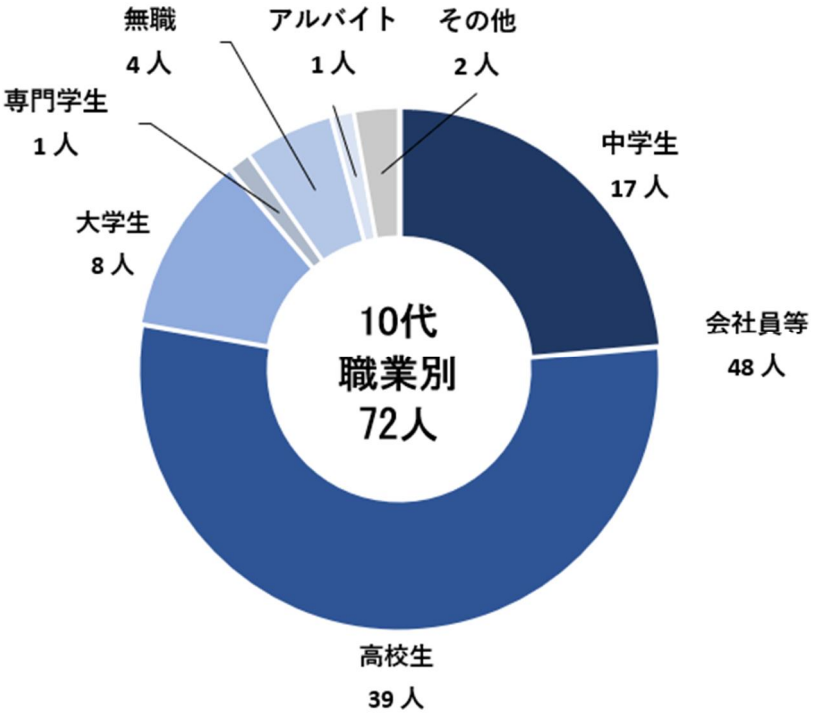


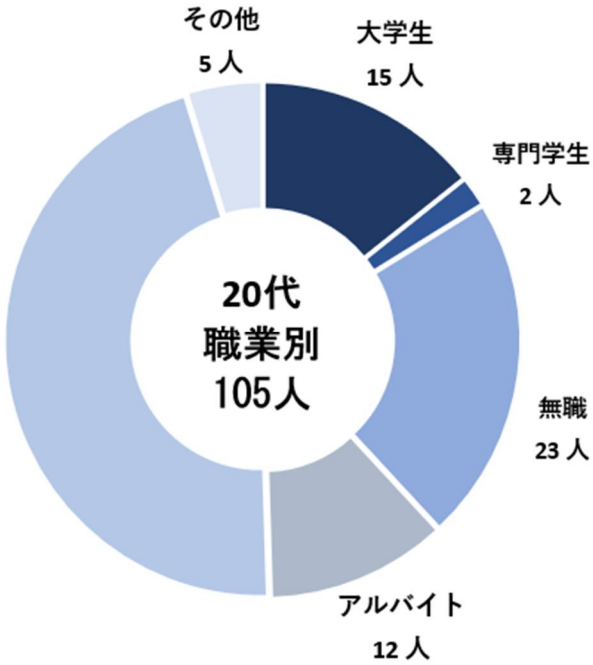
資料編

（第２部１「検挙に向けた取組」関連）

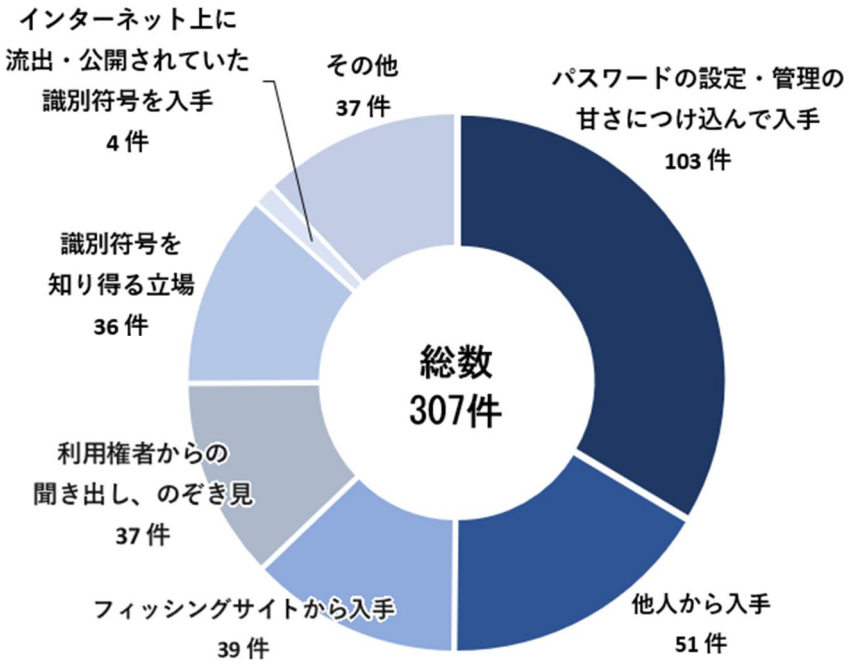
サイバー犯罪・サイバー事案に関する統計⑥

10　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





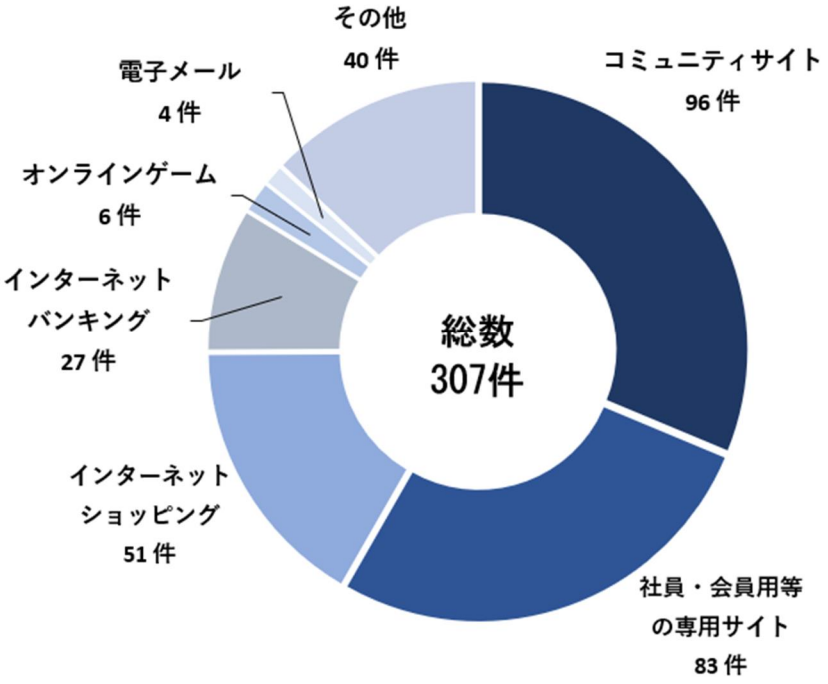
11　10 代～20 代における不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



（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

12　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

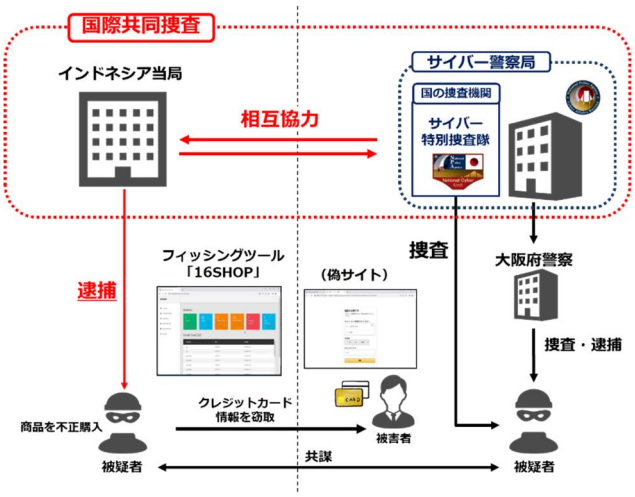


（第２部１「検挙に向けた取組」関連）

過去の国際共同捜査の主な事案一覧

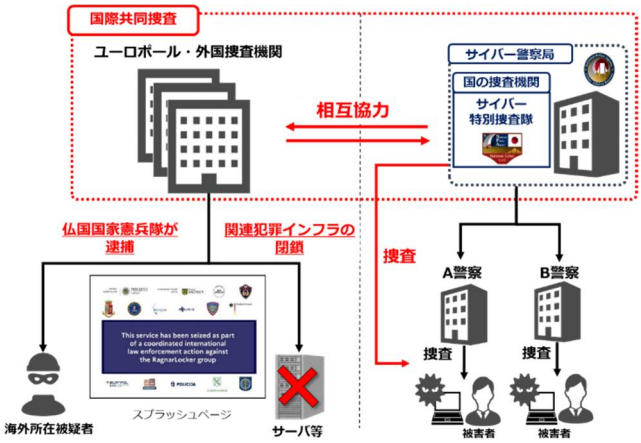
● 「16SHOP」を用いたクレジットカード情報不正取得・利用事案

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。



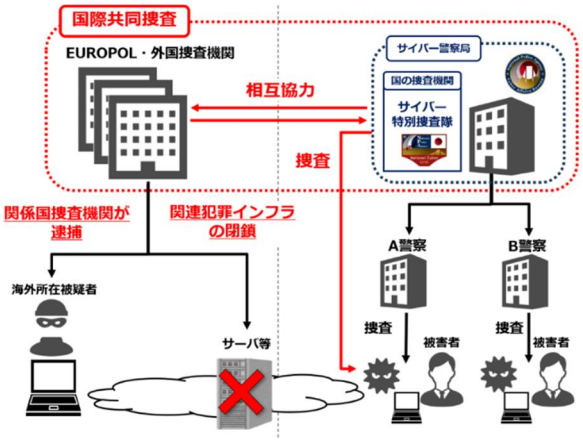
（第２部１「検挙に向けた取組」関連）

過去の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。



【スプラッシュページ】

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。

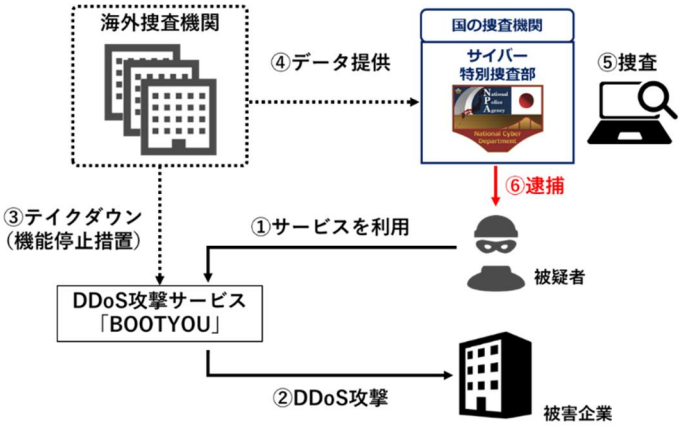
（第２部１「検挙に向けた取組」関連）

過去の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。

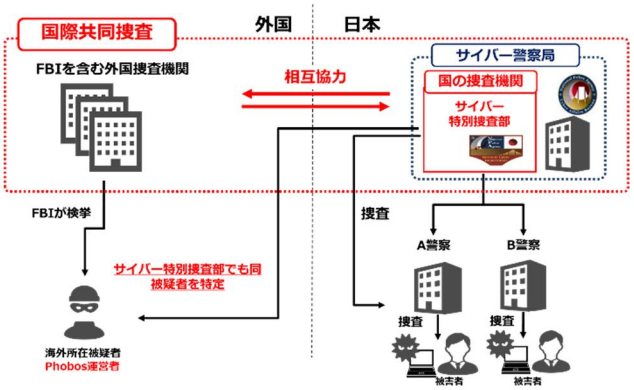
また、令和６年 12 月には、本国際共同捜査の一環として実施された広報啓発キャンペーンに参画した（本編 P29 参照）。



● 「Phobos」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「Phobos（フォボス）」について、サイバー特別捜査部と関係警察は、EUROPOL等との国際共同捜査を推進している。令和６年（2024年）11月、米国司法省は、同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。

この事案において、サイバー特別捜査部は、独自の手法により同運営者の特定に成功し、その結果や当該手法について、米国をはじめとする関係国の捜査機関に提供した。

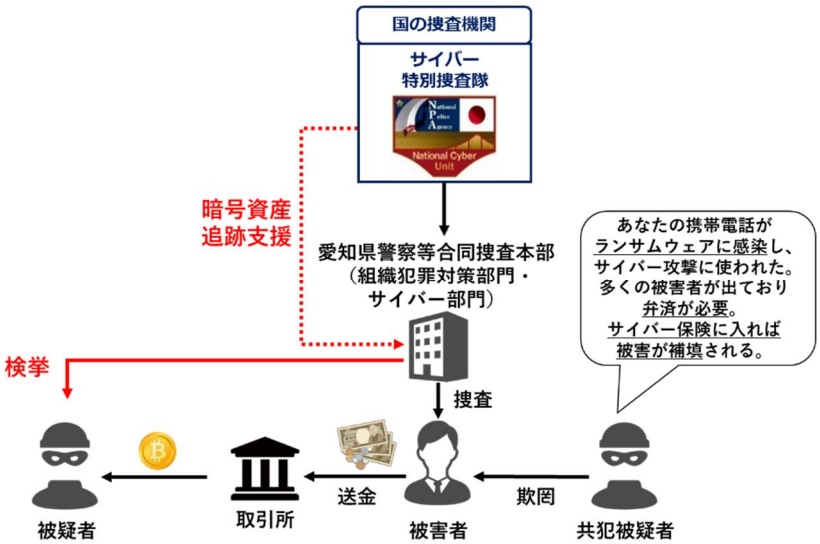


（第２部１「検挙に向けた取組」関連）

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

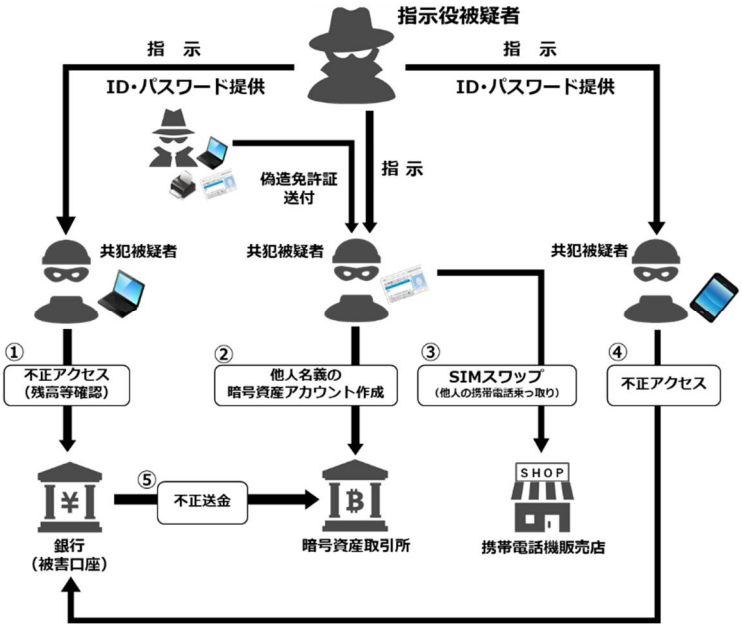
● サイバー保険名目の架空料金請求詐欺事件

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。

（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案及び同整備法案の概要

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案 及び 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案　概要

内閣官房サイバー安全保障体制整備準備室

趣　旨

○　国家安全保障戦略（令和４年12月16日閣議決定）では、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との目標を掲げ、①官民連携の強化、②通信情報の利用、③攻撃者のサーバ等への侵入・無害化、④内閣サイバーセキュリティセンター（ＮＩＳＣ）の発展的改組・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の設置等の実現に向け検討を進めるとされた。

○　国家安全保障戦略に掲げられたこれら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（令和６年６月７日～11月29日）、「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」を取りまとめ。

→　これらを踏まえ、「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案」（新法）及び「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案」（整備法）として必要な法制度を整備。

概　要

官民連携（新法）

○基幹インフラ事業者による
・導入した一定の電子計算機の届出
・インシデント報告

○情報共有・対策のための協議会の設置

○脆弱性対応の強化

等

通信情報の利用（新法）

○基幹インフラ事業者等との協定（同意）に基づく通信情報の取得

○（同意によらない）通信情報の取得

○自動的な方法による機械的情報の選別の実施

○関係行政機関の分析への協力

○取得した通信情報の厳格な取扱い

○独立機関による事前審査・継続的検査

等

↳ 分析情報・脆弱性情報の提供等 ↲

アクセス・無害化措置（整備法）

○重大な危害を防止するための警察による無害化措置

○独立機関の事前承認・警察庁長官等の指揮

等

（警察官職務執行法改正）

○内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）

○自衛隊・在日米軍が使用するコンピュータ等の警護（権限は上記を準用）　等

（自衛隊法改正）

組織・体制整備等（整備法）

○サイバーセキュリティ戦略本部の改組　（サイバーセキュリティ基本法改正）
○サイバーセキュリティ戦略本部の機能強化　（サイバーセキュリティ基本法改正）
○内閣サイバー官の新設　（内閣法改正）　等

施行期日　公布の日から起算して１年６月を超えない範囲内において政令で定める日　等

※　出典：内閣官房

（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。

（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。
【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。

（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

● 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。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

EC サイトのぜい弱性を狙ったクレジットカード情報･個人情報窃取の実態解明等（改ざんされた EC サイトにおける被害が潜在化・長期化しやすい事例）

【事例①】

Web サイト製作会社に EC サイトの作成を依頼したところ、すでに公開されている他社（図中のＡ社）の EC サイトのソースコードを流用し、その改ざんされたソースコードやバックドアをそのままコピーしてしまったためにぜい弱性等を持つ EC サイトが作成され、被害が発生した事例。

【事例②】

EC サイトが改ざんされていることに運営者が気付き、サイトを修正したが、その際にバックドアが設置されていることに気付かなかったため、修正後もバックドアが存在しており、再び侵入被害に遭った事例。

【事例③】

EC サイトが改ざんされていることとバックドアの存在に気付き、サイトを修正してバックドアの削除を試みたが、複数種類のバックドアが多数仕掛けられていたため、全てのバックドアの削除ができず、再び侵入被害に遭った事例。

【事例④】

EC サイトから窃取したクレジットカード情報を、別の侵害済みウェブサイトに転送して窃取していた事例。この場合、図中Ｅ社のサイト内にカード情報が蓄積されない場合があることや、窃取自体はＥ社と無関係な転送先Ｆ社のサイトから行われていることから、被害の発覚が遅れる可能性がある。

（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２月AI法案を閣議決定し、第217回国会に提出した。警察庁としても、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、同法案に関する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。

● 「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。

● 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）

いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策

いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策

（「国民を詐欺から守るための総合対策」のフォローアップを含む。）

緊急対策

1「被害に遭わせない」ための対策

○　ＳＮＳ等を利用した犯罪の捜査上の課題に対応するための**ＳＮＳアカウントの開設時の本人確認の強化を含む措置について検討を行うほか、事業者に対して本人確認の厳格化を要請する**。

○　犯罪の発生実態等を踏まえ、**防犯カメラの増設が必要な場所を整理するほか、地域社会の多様な関係者に保存期間の十分な防犯カメラの増設**を働き掛けていく。

○　**新しい地方経済・生活環境創生交付金については地域防犯力の強化を推奨すべき事業として明示**し、**地方創生臨時交付金については地域防犯力の強化を推奨事業メニューとして特別に明示**し、これを自治体に周知徹底することにより**確実に防犯カメラの整備が行われるように支援**する。

2「犯行に加担させない」ための対策

○　「闇バイト」の募集情報の実効的な削除に資するよう、労働者の募集を行う者が広告等により募集情報を提供するときは、**職業安定法に基づき、求人者の氏名又は名称・住所・連絡先、業務内容、就業場所及び賃金の表示が求められ、これらの表示がないものについては違法である旨を通知により明確化し、広く周知徹底**する。**フリーランスに対する業務委託の募集についても、同様の対策を講じる**。

○　検討中の違法情報ガイドラインにおいて、**「闇バイト」を募集することや、募集者の氏名等が含まれていない募集広告が職業安定法等に違反する旨の記載を盛り込む方向で検討を進める**。あわせて、**プラットフォーム事業者に対し、同ガイドラインにおける記載内容を各者の削除等に関する基準に盛り込むよう求める**。

○　**雇用仲介事業者に対し、「闇バイト」に関する求人情報の掲載防止のための取組内容を確認し、必要に応じ、事前審査の厳格化を始めとした防止措置の強化など指導等を行う**とともに、業界団体においても「闇バイト」に関する求人情報の掲載防止のための取組を推進する。

○　**若者に訴求力の高い著名人にＳＮＳ上に「闇バイト」等の危険性等について投稿を要請**するほか、**ターゲティング広告やアドトラックの活用等、その他の媒体や方法の拡充を図る**。

○　インターネット上の違法情報の削除要請を行う**インターネットホットラインセンターの体制の更なる増強**に取り組む。

3「犯罪者のツールを奪う」ための対策

○　個人情報を悪用する事業者等に対して、個人が個人情報を提供する事例も見受けられることから、警察からの情報提供を踏まえ、**個人情報に係る規律を周知するなど、国民が自らの個人情報を適切に取り扱うための広報啓発を更に推進**する。

○　「闇バイト」等による強盗事件等の捜査においては、**被害金の追跡を行うに当たって、金融機関に照会を行う必要があるところ、金融機関への照会・回答の迅速化**を図る。

4「犯罪者を逃がさない」ための対策

○　**現行法の範囲内で実施可能な仮装身分捜査の在り方を検討し、ガイドライン等で明確化した上で、早期に仮装身分捜査を実施**する。

○　**警察におけるサイバー犯罪対策部門の更なる体制強化、各種装備資機材の充実強化、幹部警察官や技術系職員を含む警察職員に対するサイバー教育の更なる充実強化**に取り組むほか、**更なる情報技術解析の高度化に向け、外国機関との連携等**を行う。

○　諸外国の例を参考にした**インターネットサービスの悪用の実効的排除に資する法制度の調査・検討**を行う。

○　**海外事業者の日本法人窓口の設置の働きかけなど情報提供の迅速化のための環境整備を行う。**

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策②

いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策

（「国民を詐欺から守るための総合対策」のフォローアップを含む。）

フォローアップ

1「被害に遭わせない」ための対策

○　多様な媒体を活用した被害防止に資する情報発信

⇨　**X、YouTube、Yahoo!、Smart Newsにおいて、特殊詐欺や犯罪実行者募集に係るターゲティング広告**を実施。

2「犯行に加担させない」ための対策

○　犯罪実行者募集投稿に対する

・　返信（リプライ）機能を活用した投稿者への迅速な個別警告

⇨　**3,922件の個別警告**（令和６年４月～11月）

・　**インターネット・ホットラインセンターによる**SNS事業者への削除依頼

⇨　**3,467件が削除**（令和６年４月～11月）

を実施

○　サイバー空間からの違法・有害な労働者募集の排除

⇨　雇用仲介事業者に対し、**違法・有害な募集情報の掲載防止のための措置、掲載されていることを発見した場合における迅速な削除等を要請**するとともに、事業者が違法・有害な募集情報を放置した場合には労働局による指導・監督の対象となり得ることを周知。

出典：警視庁SNS（X、YouTube等）

○　青少年をアルバイト感覚で犯罪に加担させないための教育・啓発

⇨　**全ての大学等に闇バイト等で学生が犯罪に加担することがないよう、学生向けの周知啓発の取組を求める通知の発出を行う**とともに、**児童生徒に対しても、非行防止教室や防犯指導**を実施。

⇨　犯罪実行者に応募した者が犯行実行前に踏みとどまれるよう、**警察による保護と実行前の相談を呼びかける動画を発信し、11月末時点で125件で保護**。

3「犯罪者のツールを奪う」ための対策

○　闇名簿対策

⇨　名簿屋等の事業者における個人データの取扱いについて、**大量の個人データが不正に持ち出され、名簿業者に売却された事案については、立入検査を実施し、個人情報保護法違反が認められたため、売却先に指導等**を行うとともに、**虚偽報告を行った業者に対して刑事告発**を実施。

⇨　令和６年６月～11月に**立入検査２件、指導等２件（うち１件は刑事告発）を実施。**

○　携帯電話契約時の本人確認の実効性確保に向けた取組

⇨　携帯電話契約時の本人確認方法等について、**偽変造された本人確認書類による不正契約等を防ぐ観点から、**本人確認書類の写しを用いた非対面の方法を廃止する等、**見直しの方向性に係る意見募集を実施したところ。その結果等を踏まえ、制度改正を予定。**

4「犯罪者を逃がさない」ための対策

○　SNS事業者における照会対応の強化

⇨　**ＳＮＳ事業者に対し、捜査の迅速化の観点から、照会対応体制の拡充等を要請した結果、被害者との連絡ツールとして利用されていたＳＮＳを運用するＳＮＳ事業者との間で、より迅速・合理的な照会方法について合意し、運用を開始**。

○　「闇バイト」関連の強盗等事件の取締り

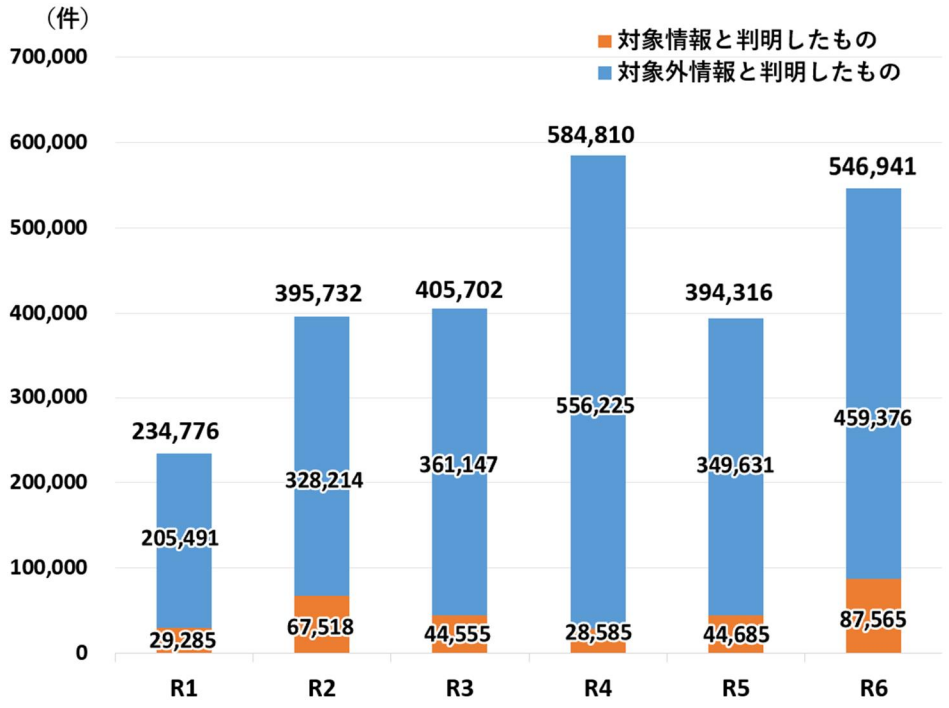
⇨　令和６年８月～11月までに１都３県において発生した**「闇バイト」との関連が疑われる一連の強盗等事件19事件について、17事件・46人を検挙**（12月5日時点）。

資料編

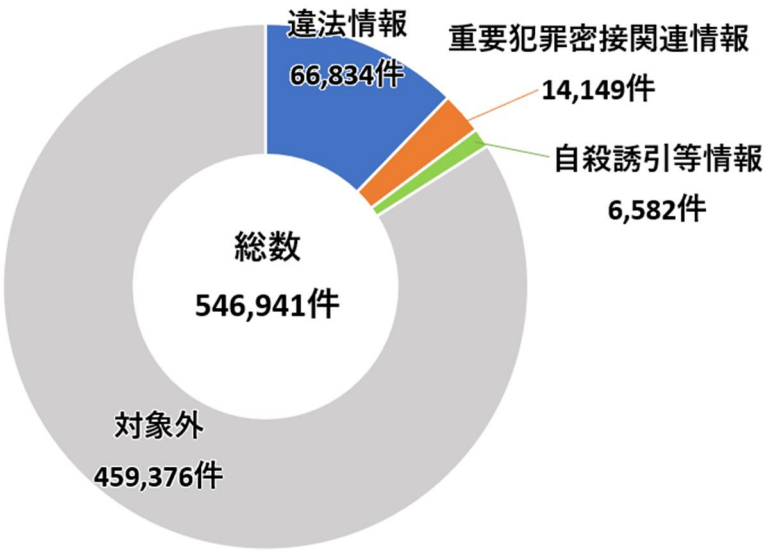
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

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[7]の推移



２　分析結果の内訳

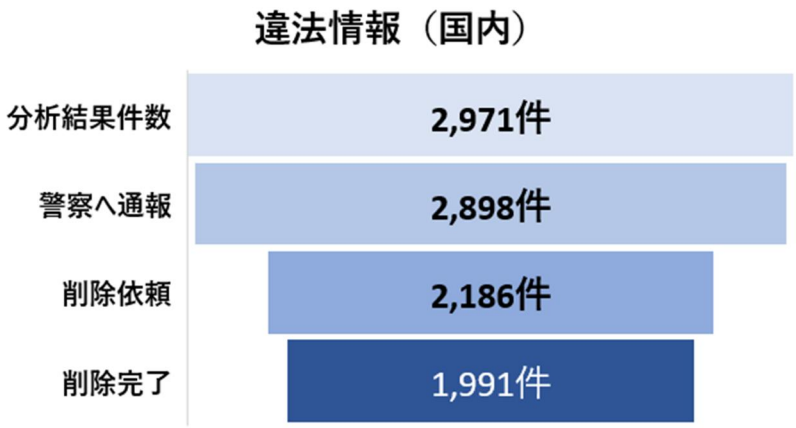


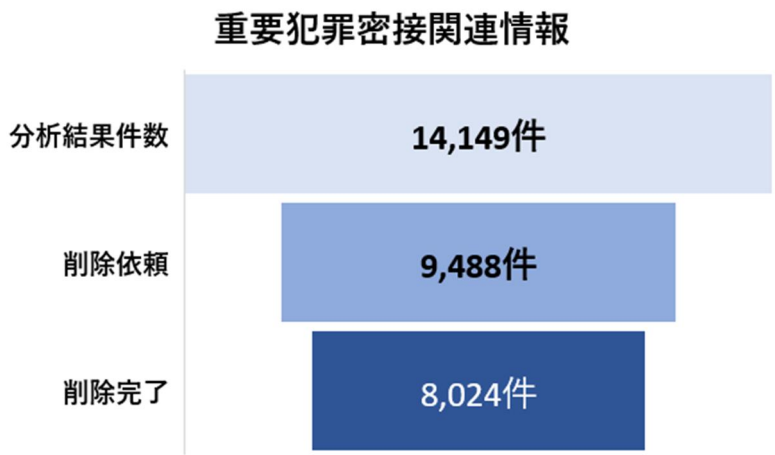
[7] インターネット・ホットラインセンター（IHC）への通報について、運用ガイドラインに基づいて分析対象とされた件数。１件の通報に複数の類型が含まれる場合、重複してカウントされるため、通報件数よりも多くなる。

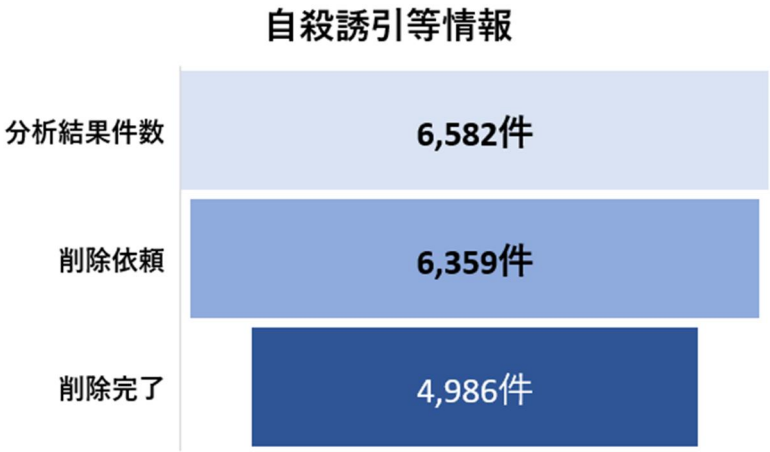
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

違法・有害情報の分析に関する統計②

３　分析結果件数[8]と処理結果



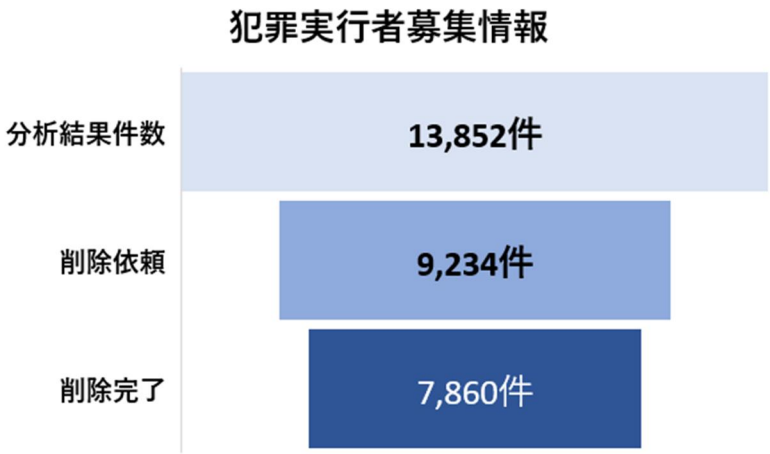




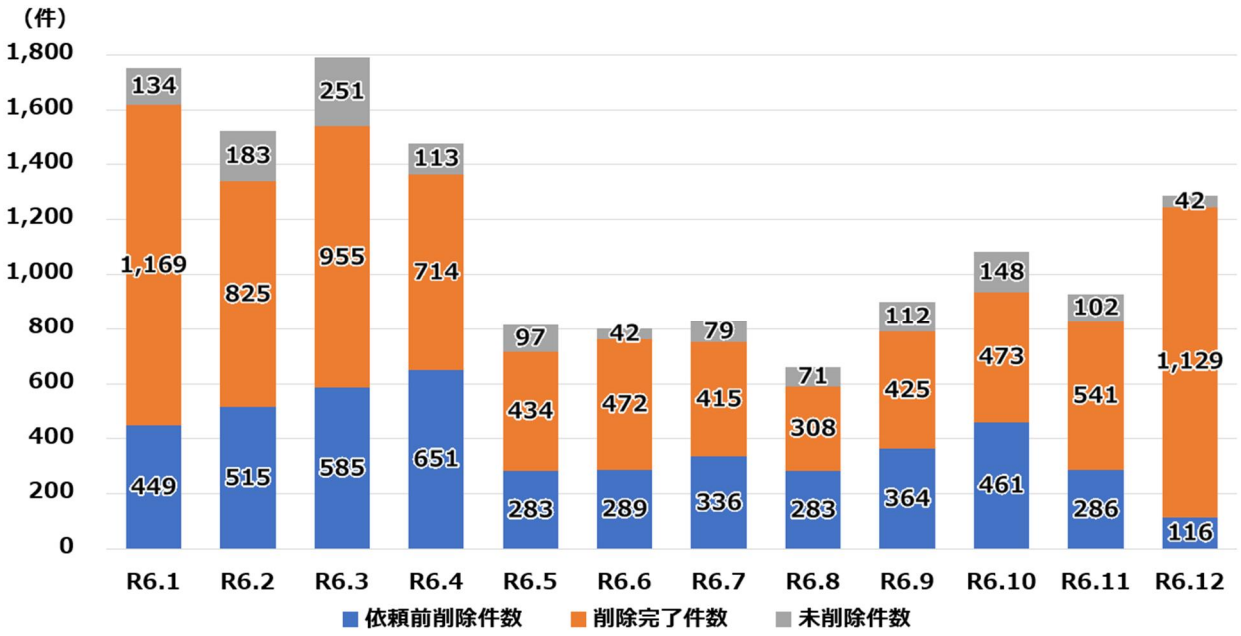
[8] IHC への通報について、運用ガイドラインに基づいて分析した結果、違法情報、重要犯罪密接関連情報、自殺誘引等情報、犯罪実行者募集情報として分類された件数。

（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



４　令和６年中の IHC における犯罪実行者募集情報の削除依頼対象件数



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

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

ホワイト案件
即日即金
運びの仕事
詳細はテレグラムで

▶ 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

高収入バイト
全国で募集
低リスク
詳しくはDMで

⚠ 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。

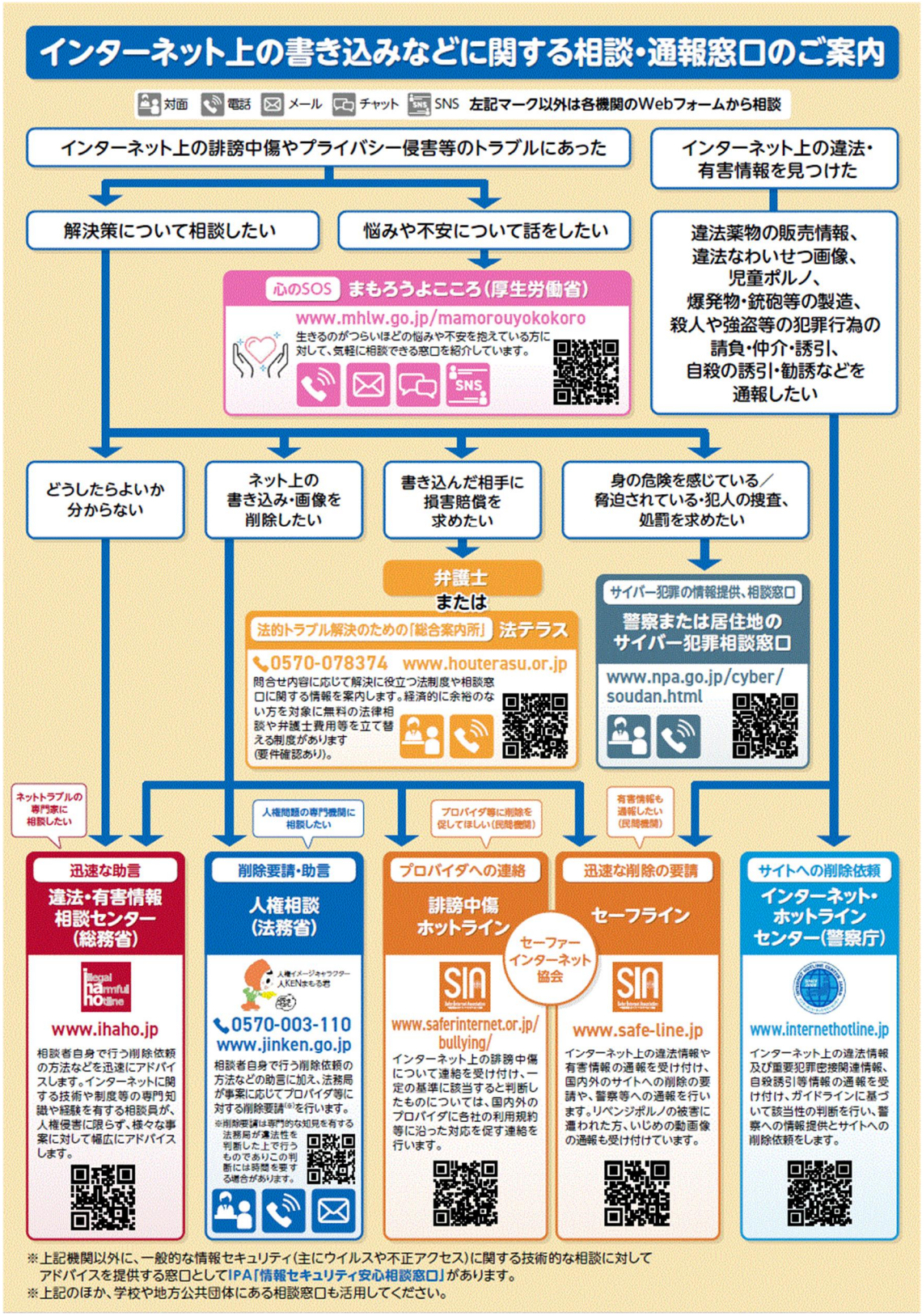
○　無登録貸金業者による広告（いわゆる「ヤミ金」の広告）

○　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