

**令和8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8年9月
警察庁サイバー警察局**

はじめに

令和 8 年上半期においては、政府機関や大手製造業者に対する情報窃取を目的としたとみられるサイバー攻撃のほか、研究機関等に対する不正アクセスが相次ぎ発生した。このようなサイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数は前年同期比で大幅に増加しており、その大部分が海外を送信元とするアクセスが占めている。また、令和 8 年上半期におけるランサムウェアの被害報告件数は 123 件と、統計を取り始めた令和 2 年下半期以降、半期の件数としては過去最多となった。

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、令和 8 年上半期における特殊詐欺（SNS 型投資詐欺及び SNS 型ロマンス詐欺を含む。）の被害額は約 1,816 億 2,000 万円となるなど、過去最悪となった令和 7 年の被害額を上回るペースで推移している。加えて、インターネットバンキングに係る不正送金、ニセ社長詐欺、暗号資産を利用したマネー・ローンダリング等、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ほか、昨今、高性能 AI が出現し、攻撃者に悪用されることでサイバー攻撃がより高速かつ大規模に行われるリスクが懸念されるなど、AI をめぐる情勢は日々刻々と変化している。

さらに、犯罪実行者募集情報等、インターネット上における流通そのものが法令に違反する違法情報のほか、有害情報や偽・誤情報が氾濫しており、サイバー空間における治安上の脅威となっている。

このような情勢等を踏まえ、警察庁は、令和 8 年 4 月、4 年ぶりに「警察におけるサイバー戦略」を改定し、警察において推進すべき取組を明らかにした。全国警察は、同戦略に基づき各種取組を推進している。

例えば、オンラインカジノに誘因する^{あいたいや}相対屋の運営者等を検挙したほか、ユーロポールを中心とした国際共同捜査に参画してミキシングサービスグループの検挙・実態解明を行うなど、検挙に向けた取組を推進している。また、北朝鮮の IT 労働者に関する注意喚起やランサムウェアによって暗号化されたデータの復号、国際共同捜査によるマルウェアと結びついたサーバ等のテイクダウンを行うなど、被害の未然防止・拡大防止に向けた取組を推進しているほか、高度サイバー人材の確保や最先端の情報通信技術に係る研究・開発を進めるなど、基盤整備に向けた取組も推進している。さらに、令和 8 年 10 月 1 日に施行予定のアクセス・無害化措置を着実に実施し、サイバー攻撃による被害の防止を図るべく、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となって中核的な機能を担う体制整備を行っている。

本レポートは、第 1 部で令和 8 年上半期中のサイバー空間の脅威情勢を、第 2 部で警察の取組を取りまとめたものである。本レポートにより、サイバー空間の脅威情勢と警察の取組について、更に理解が深まれば幸いである。

本文 目次

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.....	5
(1) 国家の関与が疑われる高度なサイバー攻撃.....	7
① 中国.....	7
② 北朝鮮.....	8
③ ロシア.....	8
④ その他.....	8
(2) 犯罪組織等による高度なサイバー攻撃.....	9
① ランサムウェア攻撃.....	9
② DDoS攻撃.....	12
2 インターネット空間を悪用した犯罪.....	13
(1) インターネット空間で提供されるサービスの悪用.....	15
① SNS・メッセージングアプリの悪用.....	15
② メール・SMSの悪用.....	17
③ ウェブサイトの悪用.....	22
(2) インターネット空間における資金移動の悪用.....	23
① インターネットバンキング.....	23
② 暗号資産.....	24
(3) IoT機器の悪用.....	25
(4) AIの悪用.....	27
3 違法・有害情報.....	31
(1) 違法情報.....	32
(2) 有害情報.....	32
(3) 偽・誤情報.....	33

本文 目次

第2部 警察の取組	35
1 検挙に向けた取組	35
(1) 事案認知に向けた取組	35
(2) 検挙に向けた捜査	37
① サイバー特別捜査部	38
② 都道府県警察サイバー部門	39
(3) 捜査支援	41
(4) 国際連携	45
① 国際会議への出席	45
② 研修・演習への参加	45
③ 能力構築支援	45
(5) サイバー警察活動における適正性の確保	46
2 被害の未然防止・拡大防止に向けた取組	47
(1) 検挙による抑止	47
(2) 情報発信	48
① 国際連携を通じた情報発信	50
② 関係機関との連携を通じた情報発信	52
③ サイバー防犯ボランティアとの連携を通じた情報発信	55
(3) 犯罪インフラへの対処	57
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	57
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	58
③ 違法・有害情報に関するインフラへの対処	65
(4) アクセス・無害化措置	69
3 基盤整備に向けた取組	71
(1) 体制の整備	71
(2) 人材の確保・育成	73
(3) 資機材の整備	79
(4) 研究・開発	81

図表 目次

図表 1 : 警察庁が検知した国内外からの不審なアクセス件数	5
図表 2 : 警察庁が検知した国別の不審なアクセス件数	6
図表 3 : Mirai ボットの特徴を有するアクセス件数	6
図表 4 : ランサムウェア被害報告件数	9
図表 5 : ランサムウェア攻撃の流れのイメージ	10
図表 6 : ランサムウェア被害企業・団体等の規模別・業種別件数	11
図表 7 : ランサムウェア被害からの復旧期間・費用	11
図表 8 : インターネットを利用した犯罪の認知件数・被害額	13
図表 9 : インターネットを利用した詐欺の認知件数・被害額	13
図表 10 : 特殊詐欺の認知件数・被害額	15
図表 11 : SNS に起因する事犯の学識別被害児童数	16
図表 12 : フィッシングの報告件数	17
図表 13 : フィッシングメールの送信元サーバ所在国の割合	18
図表 14 : 同一送信元 IP アドレスからフィッシングメールを受信した日数・件数	18
図表 15 : インターネットバンキング不正送金被害額	19
図表 16 : クレジットカード不正利用被害額	20
図表 17 : クレジットカード不正利用の流れ	20
図表 18 : 偽サイト等の情報報告件数	22
図表 19 : 特殊詐欺におけるインターネットバンキングの利用状況	23
図表 20 : 犯罪収益移転防止法違反の検挙件数	23
図表 21 : 暗号資産を悪用したマネー・ローンダリングのイメージ	24
図表 22 : IoT 機器が踏み台となる攻撃のイメージ	25
図表 23 : 不正送金被害におけるレジデンシャルプロキシの悪用件数	26
図表 24 : AI をめぐる脅威情勢	27
図表 25 : 生成 AI により児童の画像を性的加工した事案	30
図表 26 : 違法・有害情報の判断件数	31
図表 27 : 犯罪実行者募集のイメージ	32
図表 28 : SNS 上における偽・誤情報投稿のイメージ	33

図表 目次

図表 29：全国統一のオンライン通報・相談受付窓口のイメージ	35
図表 30：サイバー犯罪の検挙件数	37
図表 31：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	41
図表 32：暗号資産追跡依頼件数	44
図表 33：ランサムウェア種別が判明した攻撃件数	47
図表 34：サポート詐欺に係る報告件数	48
図表 35：サイバー分野における他国との協議	50
図表 36：日本サイバー犯罪対策センター（JC3）	52
図表 37：サイバー防犯ボランティアの構成員数・団体数	55
図表 38：「 ^{あいたいや} 相対屋」の検挙	58
図表 39：「道具屋」の検挙	58
図表 40：ウェブサイト対策のイメージ	59
図表 41：不正アプリ対策のイメージ	60
図表 42：インターネット・ホットラインセンターの仕組み	65
図表 43：インターネット・ホットラインセンターの削除依頼対象	65
図表 44：犯罪実行者募集情報に対する個別警告（リプライ）件数	67
図表 45：改正警察官職務執行法	69
図表 46：政府における三位一体によるシームレスな対処	70
図表 47：サイバー警察局・サイバー特別捜査部の組織図	71
図表 48：警察におけるサイバー人材数	73
図表 49：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	80

コラム 目次

コラム：急増するアクセス件数の国別比較	6
コラム：DDoS攻撃のビジネスモデル化	12
コラム：米国におけるサイバー犯罪の情勢	14
コラム：フィッシングメールの送信元分析	18
コラム：ボイスフィッシングによる不正送金被害	19
コラム：メールを悪用した新たな詐欺手口～ニセ社長詐欺～	21
コラム：セキュリティ対策が十分でないIoT機器	26
コラム：生成AIによる児童の性的加工画像	30
コラム：令和8年熊本地震に関連する偽・誤情報	34
コラム：脅威ハンティングに関する警察の取組	36
コラム：ミキシングサービスグループの検挙	38
コラム：オンラインカジノ利用に係る青少年らの検挙	40
コラム：警察捜査を支える解析の高度化	43
コラム：オンライン上の児童の性的搾取に対する国際共同捜査	46
コラム：少年をサイバー犯罪の被害者にも加害者にもさせないための対策	49
コラム：北朝鮮IT労働者に関する注意喚起	51
コラム：サイバー特別捜査部によるデータの復号	54
コラム：「サイバーテスト」を活用した若者向けの教育活動	56
コラム：国際共同捜査によるサーバのテイクダウン	57
コラム：ECサイトにおける不正取引対策	61
コラム：家庭用IoT機器を悪用したサイバー攻撃への官民一体となった対策	62
コラム：AIをめぐる警察の取組	63
コラム：データ通信専用SIM契約時の本人確認の義務化	64
コラム：なりすまし型偽投資広告及び送金犯罪に係る取組	66
コラム：AIを活用した犯罪実行者募集情報の収集	68
コラム：都道府県警察におけるサイバー警察部の設置	72
コラム：サイバー人材の新たな確保方策	74
コラム：高度なサイバーセキュリティ技術を有する民間人の登用	75
コラム：サイバー防犯ボランティア等に向けたサイバー犯罪捜査官の魅力発信	76
コラム：サイバーレンジによる訓練	78
コラム：一体的運用による研究・開発の高度化	82

CASE 目次

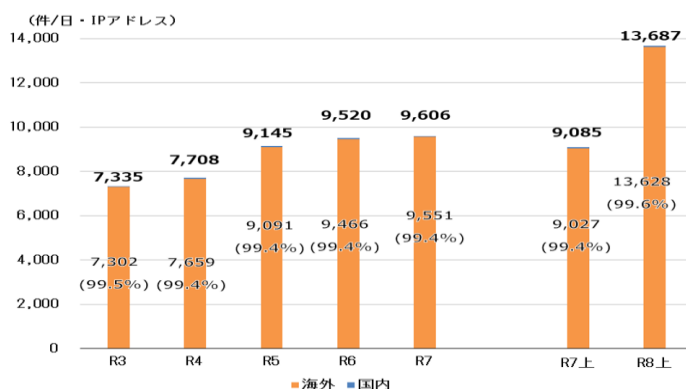
CASE : リアルマネートレードサイトにおける不正課金事案の検挙	16
CASE : A I を悪用してランサムウェアを作成した被疑者の検挙	28
CASE : 少年による動画配信サービス運営会社に対する偽計業務妨害事件の検挙	28
CASE : A I を悪用して警察官になりすました特殊詐欺被疑者の検挙	29
CASE : A I を悪用してわいせつ画像を作成した被疑者の検挙	29
CASE : 中国人グループによる電子決済アプリ利用の不正アクセス等事案の検挙	39
CASE : 盗撮目的の建造物侵入事案における分析支援	41
CASE : 損壊したスマートフォンからのデータ抽出	42
CASE : 生成 A I を悪用するマルウェアの解析	81

概要 令和8年上半期における脅威情勢の概要

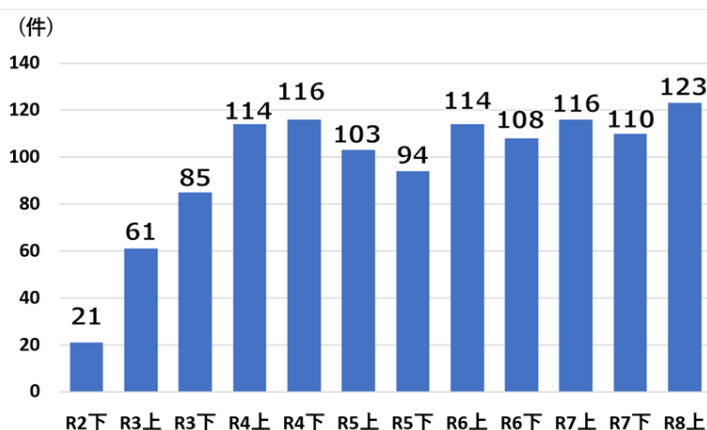
I サイバー空間の脅威情勢

1 高度な技術を悪用したサイバー攻撃

- 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、大幅に増加（前年同期比51%増）。その大部分の送信元が海外。【本文5頁】



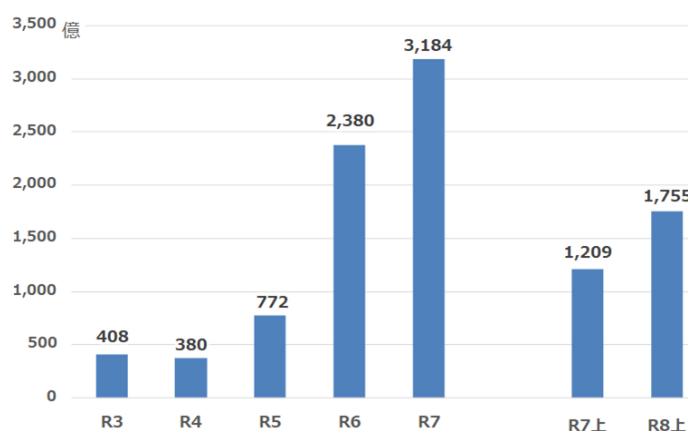
- 令和8年上半期におけるランサムウェアの被害報告件数は123件。半期の件数として統計を取り始めた令和2年下半期以降最多。【本文9頁】



2 インターネット空間を悪用した犯罪

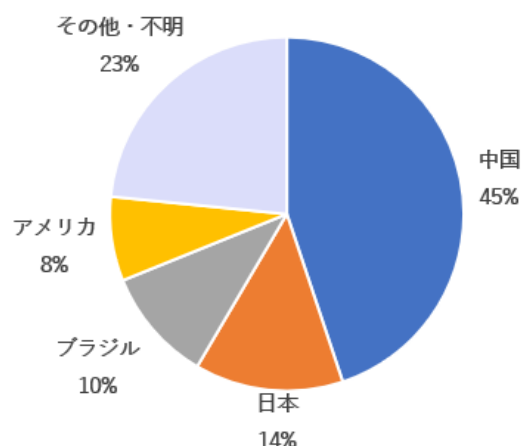
- インターネットを利用した犯罪は右肩上がりで増加しており、その約9割が詐欺。インターネットを利用した詐欺の被害額は増加傾向であり、令和8年上半期は1,755億円（前年同期比45%増）。【本文13頁】

インターネットを利用した詐欺の被害額



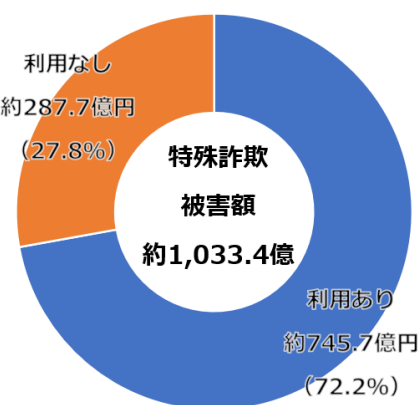
- サイバー特別捜査部が、フィッシングメールと評価されるメールを対象に分析を行ったところ、送信元IPアドレスから推定される送信元サーバの所在国として最も多いのは中国の45%、次いで日本、ブラジルの順。【本文 18 頁】

フィッシングメールの送信元サーバ所在国の割合



- 令和8年上半期における振込型の特殊詐欺被害（被害額約1,033億4,000万円）のうち、全体の約7割でインターネットバンキングを悪用。【本文 26 頁】

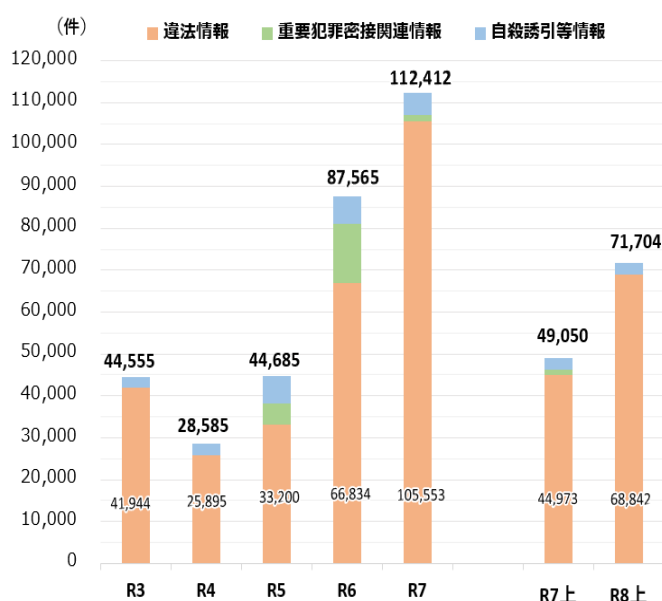
特殊詐欺におけるインターネットバンキング利用状況



3 違法・有害情報

- インターネット上には、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等が存在。令和8年上半期のインターネット・ホットラインセンター（IHC）における違法・有害情報の判断件数は7万1,704件（前年同期比46%増）。【本文 31 頁】

違法・有害情報の判断件数

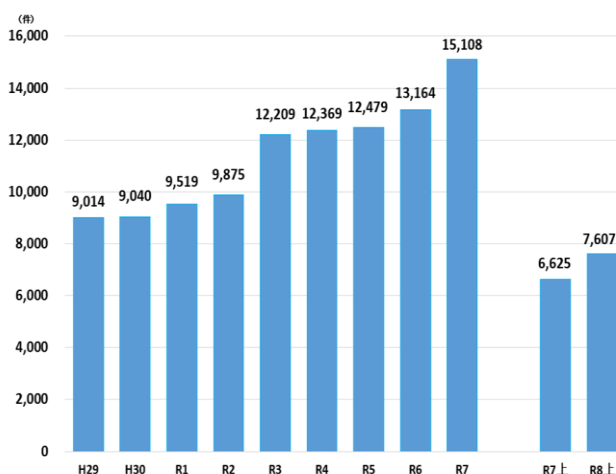


II 警察の取組

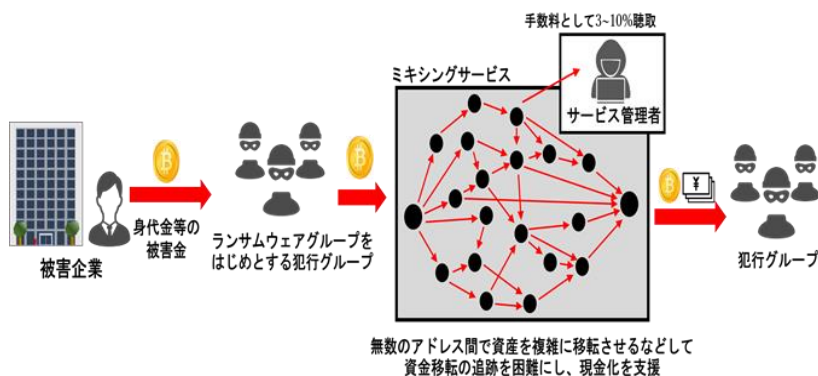
1 検挙に向けた取組

- サイバー犯罪の検挙件数は平成 29 年以降増加を続けており、令和 8 年上半期における検挙件数は 7,607 件（前年同期比 15% 増）。検挙件数のうち、犯罪収益移転防止法及び組織的犯罪処罰法違反等のマネー・ローンダリング関連の犯罪の検挙件数は 1,945 件（前年同期比 37% 増）で、サイバー犯罪のうち 25%。【本文 37 頁】

サイバー犯罪の検挙件数

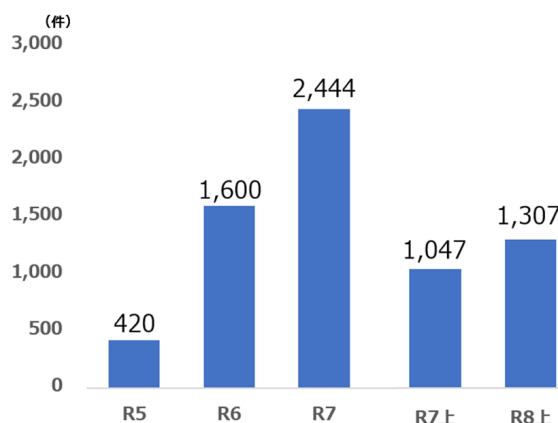


- ユーロポールを中心に組成された国際共同捜査において、暗号資産のミキシングサービス「AudiA6」の管理者とみられる被疑者 2 名を逮捕。被疑者グループが運営・管理するウェブサイトのテイクダウン等を実施。サイバー特別捜査部は、犯行実態を明らかにするデータの復元に成功し、「AudiA6」の実態解明に貢献。【本文 38 頁】



- サイバー部門では、他部門が主管するサイバー事案の捜査に対しても積極的かつ主体的な支援を行い、被疑者の特定や実態解明に貢献。サイバー特別捜査部では、高度に専門的な知識・技術に基づき、都道府県警察からの暗号資産追跡依頼に対応しており、令和 8 年上半期における暗号資産追跡依頼件数は 1,307 件（前年同期比 25% 増）。【本文 44 頁】

暗号資産追跡依頼件数



2 被害の未然防止・拡大防止に向けた取組

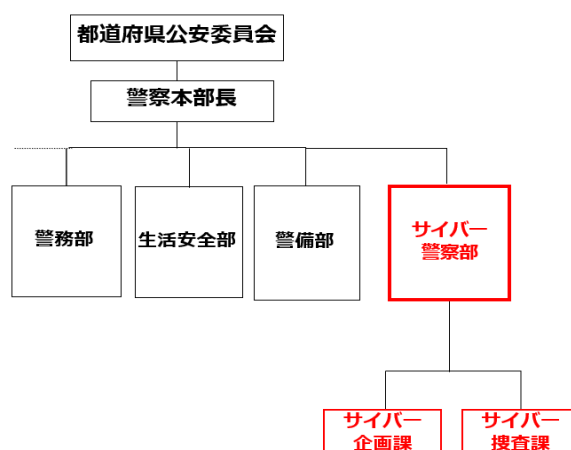
- 令和8年7月、警察庁及び国家サイバー統括室（NCO）等は、米国及び韓国等と共に、「北朝鮮 IT 労働者に関する各国・企業等に対する注意喚起」を公表。北朝鮮が IT 労働者を外国に派遣していること、同労働者は身分を偽って仕事を受注し収入を得ていること、その収入が核・ミサイル開発の資金源になっていることを指摘。【本文 51 頁】



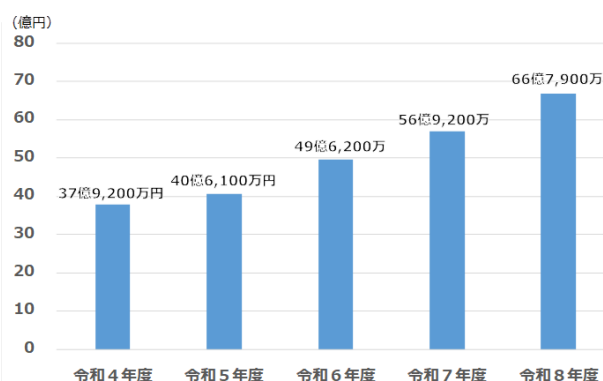
3 基盤整備に向けた取組

- 令和8年5月、都道府県警察本部の内部組織を条例で定めるに当たっての基準を定める警察法施行令を改正。都道府県警察においては、サイバー警察部等においてサイバー警察事務を一元的に所掌することとし、サイバー部門の一元化組織設置に向けた準備を推進。【本文 72 頁】

今後の都道府県警察サイバー部門のイメージ



- 令和8年度当初予算におけるサイバー空間の脅威への対処に係る予算は66億7,900万円（前年度比17%増）と令和4年度以降一貫して増加。【本文 79 頁】



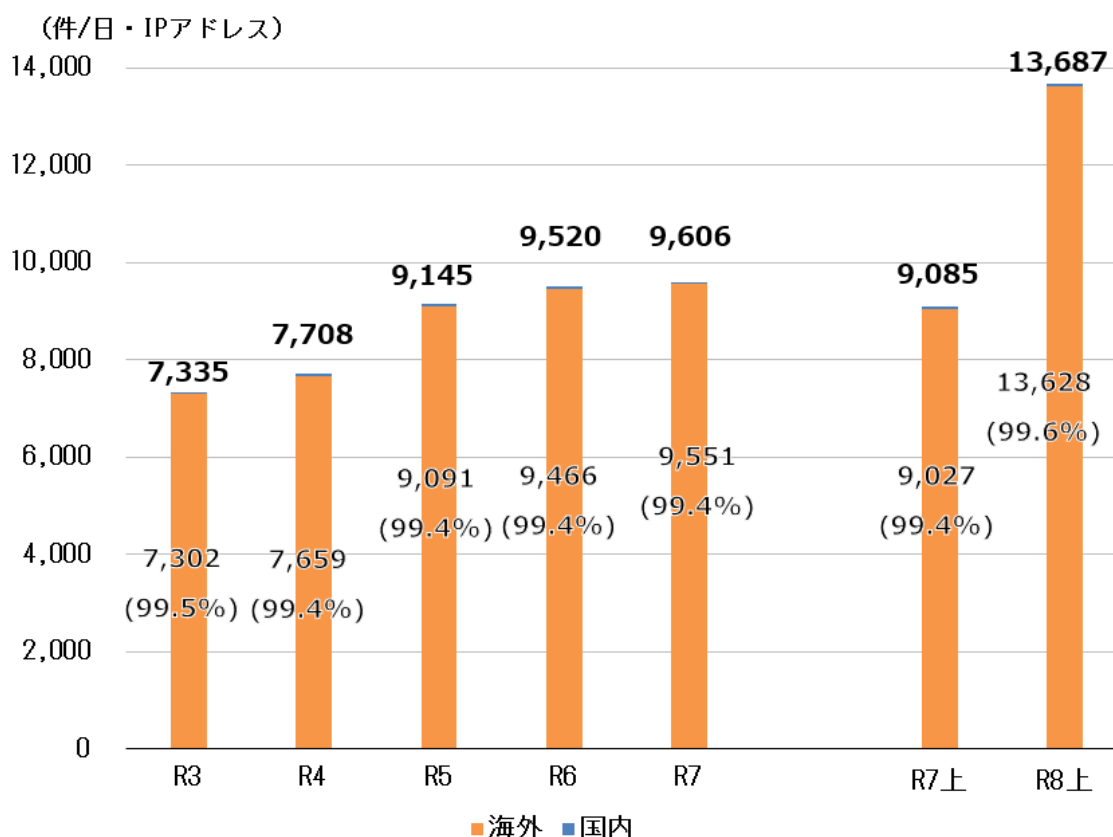
第 1 部 サイバー空間の脅威情勢

1 高度な技術を悪用したサイバー攻撃

令和 8 年上半期においては、政府機関や大手製造業者に対する情報窃取を目的としたとみられるサイバー攻撃事案のほか、研究機関等に対する不正アクセス事案が相次ぎ発生した。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（資料編 97 頁参照）。

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。令和 8 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・1 IP アドレス¹当たり 1 万 3,687 件（前年比 50.7%増）と急増しており、その大部分が海外を送信元とするアクセスで占められている。

【図表 1：警察庁が検知した国内外からの不審なアクセス件数】



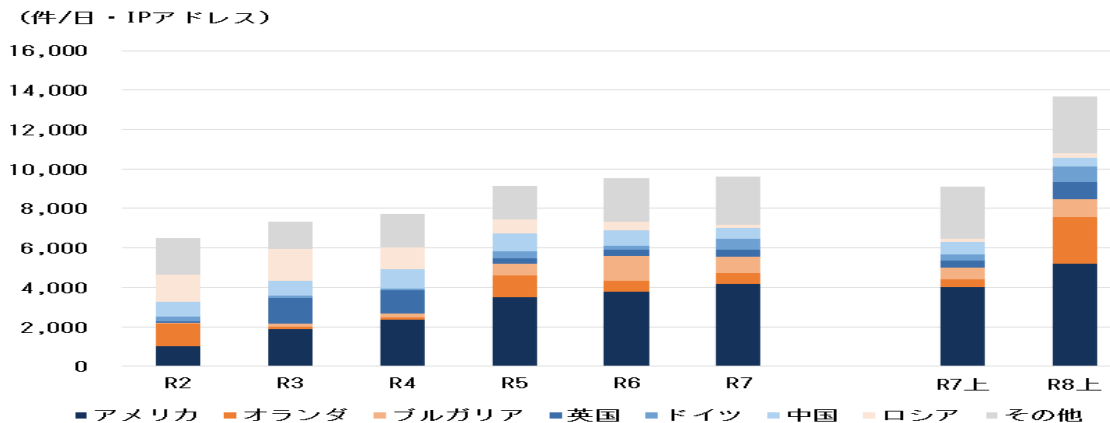
¹ 「IPアドレス」とは、インターネット上の「住所」のようなものであり、ネットワーク機器が通信を行う際、データの送信元や送信先を特定するために割り当てられる固有の識別番号である。

コラム：急増するアクセス件数の国別比較

警察庁が検知した不審なアクセス件数の送信元について分析すると、令和8年上半期はアメリカ、オランダ、ブルガリア、英国、ドイツの順で、それぞれアクセス件数が多くなっている（令和7年上半期はアメリカ、中国、ブルガリア、オランダ、ドイツの順）。

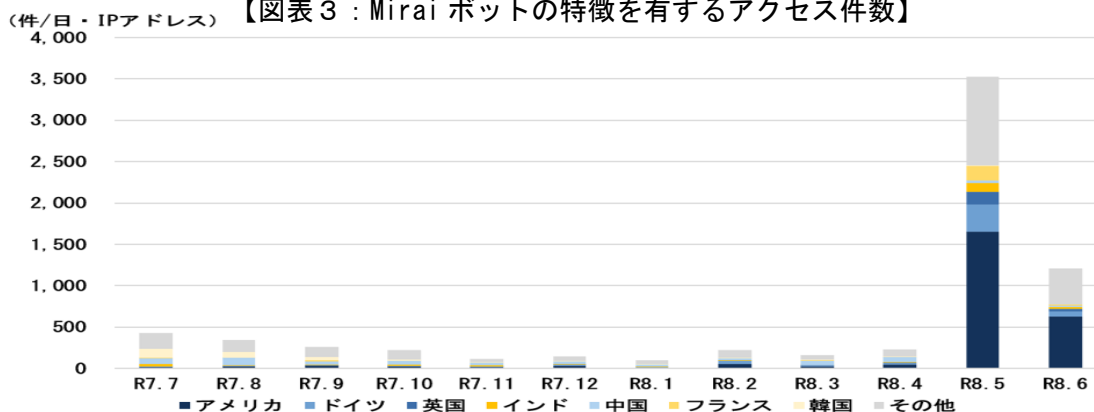
令和7年上半期と令和8年上半期を比較すると、全体的に大幅な増加を示しており、特にオランダを送信元とするアクセス数は1日・1IPアドレス当たり2,377.1件（前年比501.3%増）と大幅に増加している。これは、オランダの特定の組織に割り当てられたIPアドレスから、広範な宛先ポートに対して大量のアクセスが観測されたためであり、ぜい弱性の有無を調査するなどの目的があったと推測される。

【図表2：警察庁が検知した国別の不審なアクセス件数】



また、令和8年5月から、Mirai²ボット³の特徴を有するアクセスの急増が観測された。Mirai ボットとは、Mirai と呼ばれるマルウェアが感染した家庭用無線ルータやIoT機器のことで、所有者が認知しないところで、DDoS攻撃等の不正行為に悪用される可能性がある。

【図表3：Mirai ボットの特徴を有するアクセス件数】



² 無線ルータやIoT機器に感染しDoS攻撃等のサイバー攻撃を行う不正プログラムの一種。「Mirai」という名前の由来は、同マルウェアの開発者が、日本のあるアニメ作品のファンであり、同アニメ作品のタイトルにちなんで命名したとされる。

³ 攻撃者の命令に基づき動作する不正プログラム。「ボット」という言葉は、「ロボット」に由来しており、インターネット上で自動処理を行うプログラムを指す語として普及したものとされる。

(1) 国家の関与が疑われる高度なサイバー攻撃

国家の関与が疑われるサイバー攻撃としては、重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロや、情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバーエスピオナージが挙げられる。

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。

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目的で行われている懸念もある。また、暗号資産等の窃取による外貨獲得を目的とした国家の関与が疑われるサイバー攻撃も発生している。

これまで、警察が確認したサイバー攻撃には、国家を背景とするサイバー攻撃グループの関与が疑われるものが複数存在していた。これらの攻撃グループは、情報通信、先端技術・製造、学術研究等の分野を主な標的としており、情報窃取を目的としているとみられるサイバー攻撃が特に確認されている。

① 中国

中国の攻撃グループは、Salt Typhoon⁴のように、主に情報窃取を目的としたサイバー攻撃を行っているとみられており、これまで、ネットワーク機器等の既知のぜい弱性や機器の設定不備を悪用したネットワーク内部への侵入が確認されているほか、攻撃インフラの構築を目的としているとみられる活動も確認されている。



令和7年（2025年）10月、オランダの情報機関である総合情報保安局（AIVD）は、中国渡航時のマルウェア⁵感染リスクに関する警告を発出した。AIVDによると、中国が高い関心を有する分野を扱う複数の出張者が携行していたラップトップ型パーソナルコンピュータから、情報窃取を目的とするマルウェアが検出され、分析の結果、マルウェアはUSBメモリ等を用いて感染対象に物理的にアクセスし、蔵置されたことが確認されている。

⁴ 「Salt Typhoon」という名称は、米国民間企業の脅威分析チームが命名したコードネームである。後半の「Typhoon」は中国に拠点を置く、又は中国政府の関与が疑われるグループであること意味し、前半の「Salt」は各攻撃グループを識別するための固有の名詞である。同種のサイバー攻撃グループとして、「Volt Typhoon」等がある。

⁵ 「マルウェア（malware）」とは、英語の malicious（マリシャス：悪意のある）と software（ソフトウェア）の2つの単語が組み合わさった造語であり、デバイスに不利益をもたらす悪意のあるプログラムやソフトウェアを総称する言葉である。

② 北朝鮮

北朝鮮の攻撃グループは、主に機密情報の窃取や外貨獲得を目的としたサイバー攻撃を行っているといわれている。これまで、個人を対象とした標的型メールによる情報窃取や窃取した情報を悪用することによる、実在又は架空の人物になりすますための攻撃インフラの構築・拡大が確認されている。



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「TraderTraitor⁶」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た。北朝鮮の外貨収入の大半は暗号資産窃取とロシアへの武器販売が占めていると指摘されている。

③ ロシア

令和 7 年 12 月、米国司法省は、親ロシア系ハクティビストグループ「NoName057(16)⁷」が、ロシア政府の支援を受けている団体が関係する非公然の国家支援プロジェクトにより創設されたことを公表した。また、令和 8 年 7 月、英国外務・英連邦・開発省は、ロシアがマルウェア「Lumma Stealer⁸」により窃取した認証情報を使用して、世界中の標的にサイバーエスピオナージを行っているとして発表した。英国内では、同マルウェアによる被害者が過去 6 か月間で少なくとも 2,100 人以上に上るとされる。



④ その他

令和 8 年（2026 年）4 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）などの米政府機関は、イランの攻撃グループが米国の重要インフラ分野で使用される産業用制御装置を標的に攻撃を行い、その機能を妨害しているとして、重要インフラ事業者に対し緊急警告を発した。

⁶ 「TraderTraitor」は F B I 等の米国政府機関が名付けた名称である。Trader（取引者）と Traitor（裏切り者）を掛け合わせた言葉遊びが語源となっているとされ、攻撃手口と標的の特徴から名付けられたとされる。

⁷ 「NoName057(16)」は同グループ自らが名付けた名称とされる。自らの匿名性を強調するため「No Name」（名無し）と自称しているとされる。

⁸ 「Lumma Stealer」はマルウェア開発者の「Lumma」が自ら名付けた名称であるとされる。開発者のコードネームである「Lumma」とパスワード等を「盗み出す（Steal）」というマルウェアの種別由来しているとされる。

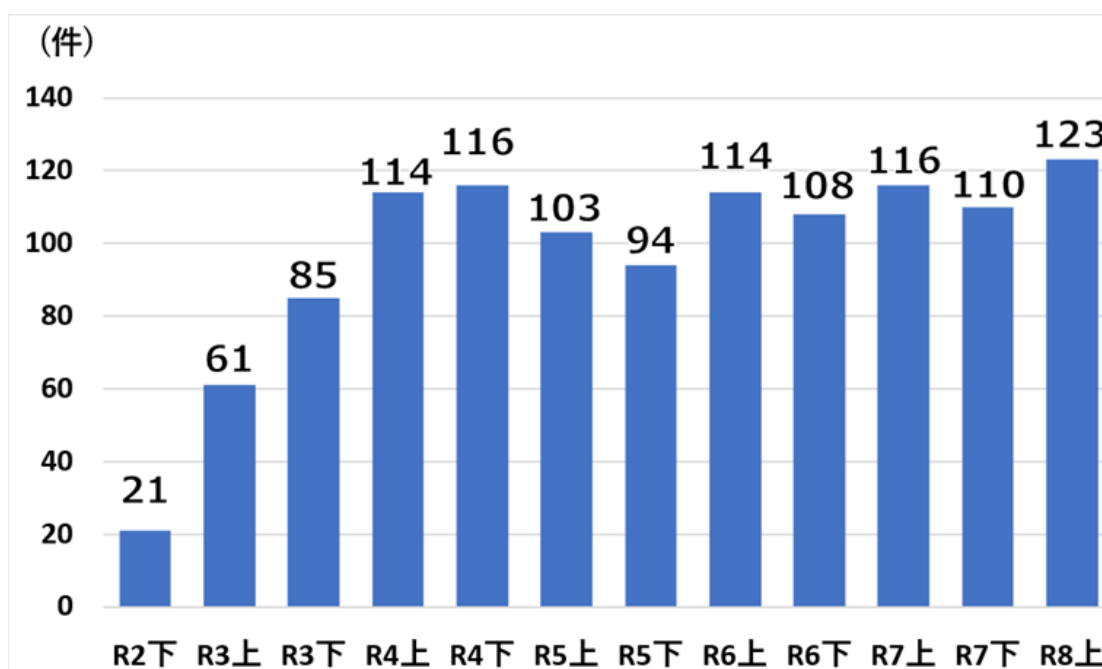
(2) 犯罪組織等による高度なサイバー攻撃

① ランサムウェア攻撃

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⁹による攻撃が挙げられる。ランサムウェアとは、端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラムである。近年は、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被害の多くを占め、実際に事業者の財務情報や個人情報等が、ダークウェブ¹⁰上のリークサイト¹¹に掲載される事例が多数確認されている。また、ランサムウェアで暗号化することなく、データを窃取した上で機密情報等の公開を予告して対価を要求する手口も発生している。

令和8年上半期におけるランサムウェアの被害報告件数は123件であり、半期の件数としては、統計を取り始めた令和2年下半期以降、最多となっている。また、長期にわたり企業活動が阻害され、国民生活に影響を及ぼした被害が依然として発生している。

【図表4：ランサムウェア被害報告件数】



⁹ 「ランサムウェア」とは、英語の ransom（ランサム：身代金）と software（ソフトウェア）の2つの単語が組み合わさった造語である。

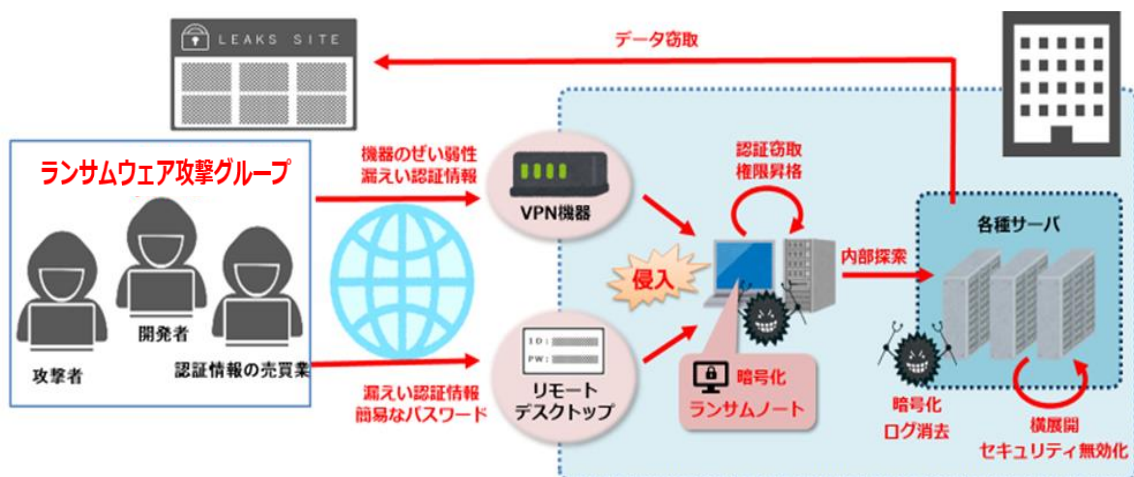
¹⁰ 「ダークウェブ」とは、一般的な検索エンジンでは見つけることができず、特殊なソフトウェアを用いてのみアクセスできるインターネット深層の匿名サイト群をいう。

¹¹ 「リークサイト」とは、サイバー攻撃グループが窃取した機密情報等を流出させるためのウェブサイト。ランサムウェア攻撃の被害企業等と身代金の支払交渉を有利に進めるために利用されることもある。

ランサムウェア攻撃の手口としては、ランサムウェアの開発・運営を行うグループが、攻撃の実行者にランサムウェアやリークサイト等の攻撃に必要な環境を提供し、その見返りとして身代金の一部を受け取る RaaS (Ransomware as a Service) が確認されている。その結果、高度な技術的専門知識を有していない者であっても、ランサムウェア攻撃の実行が可能になるなど、攻撃者の裾野の広がりが見られている。

RaaS を用いた攻撃の実行はアフィリエイト (Affiliate)¹²と呼ばれる多数の実行者によって敢行されているため、同じランサムウェアを用いた攻撃であってもその具体的な手口は様々であるが、ランサムウェア攻撃の代表的な流れは以下のとおりである。近年は、インターネットに露出した箇所から攻撃者が遠隔操作でネットワーク内部に侵入する手口が多くを占め、標的型攻撃メール等の添付ファイルによる感染は少なくなっている。被害組織へのアンケート結果によると、侵入経路は VPN¹³機器が約 5 割を占める状況である。攻撃者は、未修正のぜい弱性や漏えいした認証情報等を悪用して組織のネットワークへ侵入する。そして、より広い領域にアクセスするために管理者権限の奪取やセキュリティ無効化を試みながら、内部探索により重要データやバックアップを物色する。一通り内部探索を終えると、データをクラウド等へアップロードして窃取した後、ランサムウェアを起動して暗号化を実行する。最後に、「ランサムノート」(脅迫状)をデスクトップ等に保管して攻撃者側への連絡と身代金の支払を要求し、ログや使用したツール等の痕跡を消去して攻撃を終了する。

【図表 5：ランサムウェア攻撃の流れのイメージ】

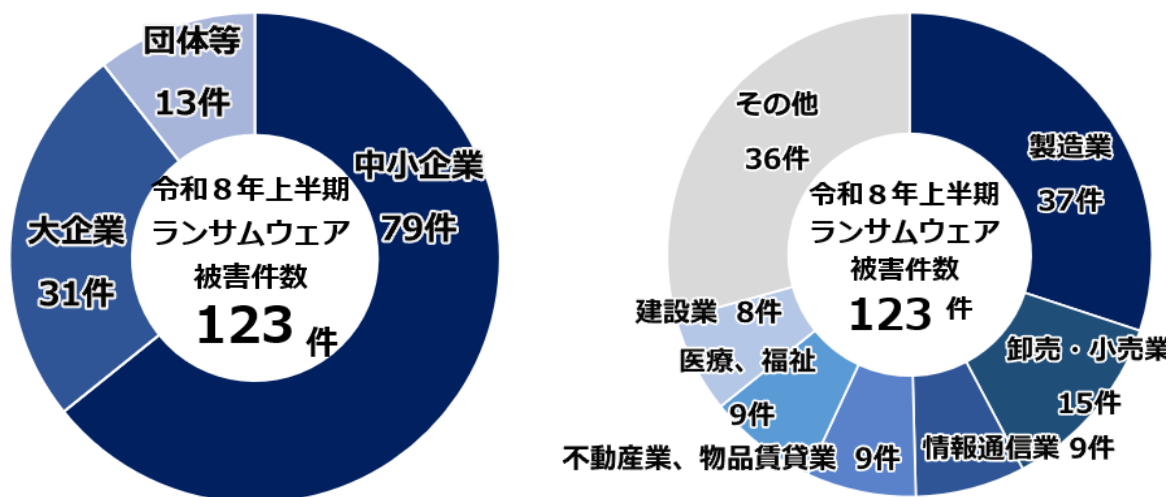


¹² ランサムウェアの開発・運営を行うグループから、攻撃に必要な環境の提供を受け、攻撃を実行する。アフィリエイトの攻撃により身代金が支払われた場合には、その収益の一部が成果報酬として開発・運営側に支払われる。

¹³ Virtual Private Network (仮想専用回線) の略。インターネット上に仮想の専用トンネルを作り、通信内容を暗号化して安全にやり取りする仕組み。管理不備やぜい弱性を突かれると、暗号化を突破され、ランサムウェアの侵入経路となり得る。

ランサムウェア攻撃の被害企業について、組織の規模別で見ると、前年と同様に中小企業が約6割を占めている。業種別では、製造業が約3割を占め、続いて卸売・小売業、情報通信業、不動産、物品賃貸業が上位となっているが、これら以外にも様々な業種で被害が確認されている。

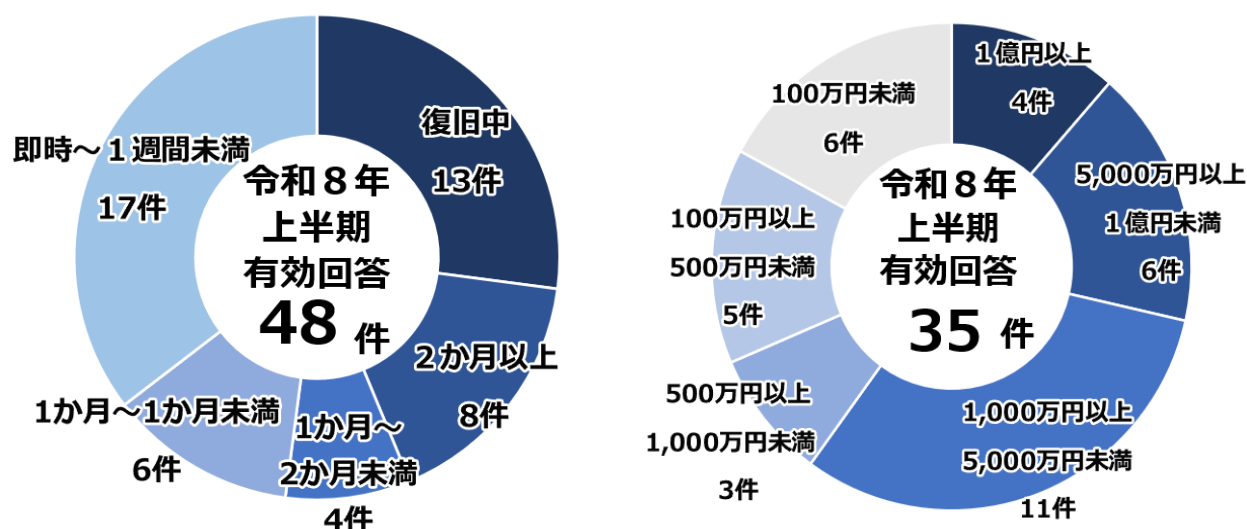
【図表6：ランサムウェア被害企業・団体等の規模別・業種別件数】



令和8年上半期にランサムウェア被害に遭った企業・団体等に対して実施したアンケートの結果によると、ランサムウェア被害に関する調査費用、復旧費用が高額化しており、復旧に総額1,000万円以上を要した組織の割合は全体の6割を占める。また、復旧に要した期間については、1か月未満で復旧した組織の割合は全体の5割弱に留まるなど、被害が長期化する傾向にある。

(ランサムウェア被害に関する各種統計については統計編139～157頁参照)

【図表7：ランサムウェア被害からの復旧期間・費用】



② DDoS攻撃

DDoS攻撃（Distributed Denial of Service「分散型サービス拒否攻撃」）とは、特定のコンピュータに対し、複数のコンピュータから大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃をいう。

例えば、令和8年2月、親ロシア系ハクティビスト¹⁴グループとみられるグループが、政府機関や交通機関、金融機関等、複数の重要インフラ事業者等を狙ったDDoS攻撃を行い、ウェブサイトの閲覧障害等が相次いで発生した。

コラム：DDoS攻撃のビジネスモデル化

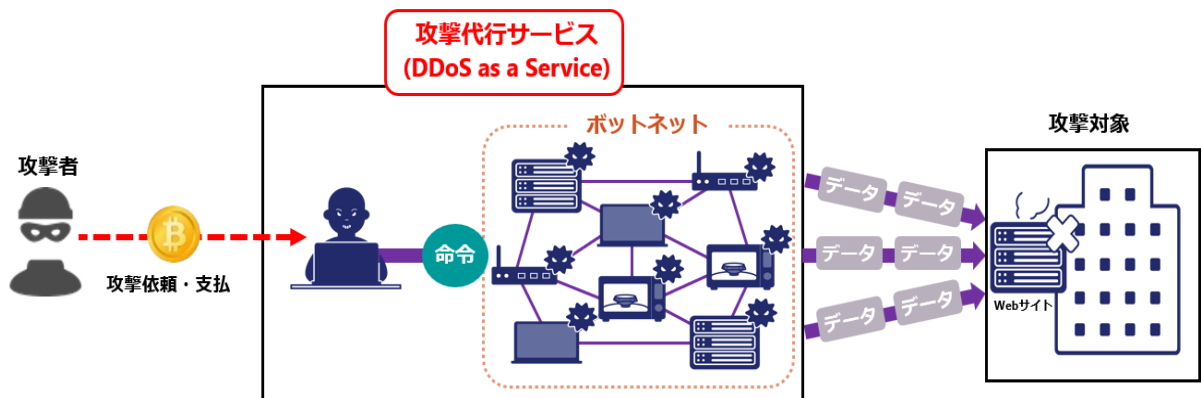
DDoS攻撃についても、ランサムウェア同様に、攻撃インフラを運営するグループが、代金と引き換えに依頼者から攻撃を請け負うDDoS as a Serviceと呼ばれる攻撃代行サービスが確認されており、犯罪のビジネスモデル化の実態が見られる。

DDoS攻撃は、一般に、ボットネット¹⁵群を構成するなど攻撃の実行に情報通信に関する高度な知識・技術が必要であるが、これらサービスの登場により、専門的知識を有しない者であっても容易にDDoS攻撃に関与し得る環境が形成されている。

利用者は少額の料金を支払うのみで、匿名性を確保したまま、広範なウェブサイトに対して攻撃を実行し、サービス停止に至らしめることが可能となり、その裾野の広がりが見られる。

日本国内においても、これら攻撃代行サービスによるDDoS攻撃と見られる事案が確認されており、サイバー特別捜査部と関係都道府県警察が連携して当該サービスの利用者を検挙するなど各種取組を推進している。

【DDoS as a Serviceによる攻撃イメージ】



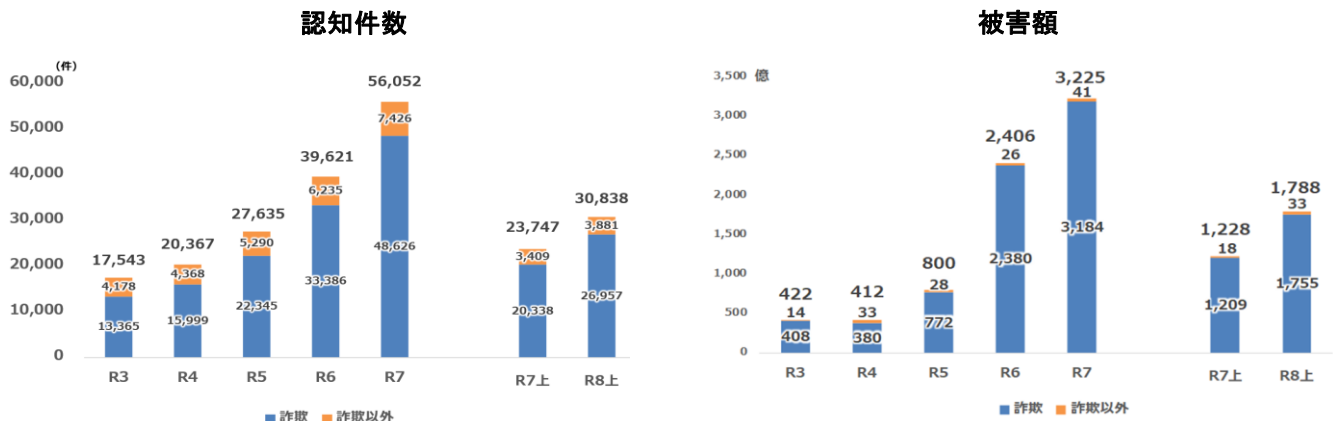
¹⁴ ハクティビスト (Hacktivist) とは、英語の hack (ハック：システムへの侵入) と activist (アクティビスト：活動家) の2つの言葉が組み合わさった造語である。政治的・社会的な主張や目的を果たすために、ハッキングやサイバー攻撃を行う個人・集団を指す。

¹⁵ マルウェアに感染した（攻撃者に乗っ取られた）多数の端末で構成されるネットワークのことで、攻撃者の命令により遠隔操作で一斉に攻撃対象に攻撃を行う。

2 インターネット空間を悪用した犯罪

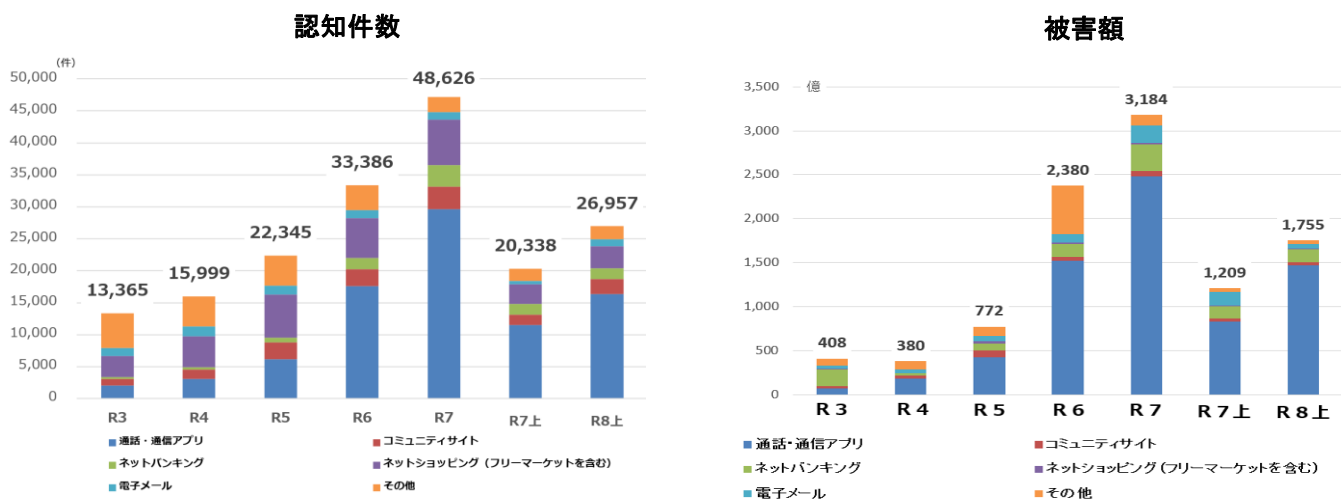
情報通信技術の著しい発展や、日常生活や経済活動へのサイバー空間の浸透は社会に様々な便益をもたらす反面、サイバー空間を舞台とした犯罪をはじめ、新たな治安課題を生み、また深刻化させており、このような情勢は、令和3年以降、インターネットを利用した犯罪の認知件数が増加の一途をたどっていることから見てとれる。令和8年上半期のインターネットを利用した犯罪の認知件数は3万838件（前年同期比30%増）となっており、そのうち、詐欺¹⁶が約9割を占める。

【図表8：インターネットを利用した犯罪の認知件数¹⁷・被害額¹⁸】



インターネットを利用した詐欺は認知件数・被害額ともに増加傾向にあり、令和8年上半期においては、通話・通信アプリを使用した詐欺が約6割を占める。（統計編159頁及び160頁参照）

【図表9：インターネットを利用した詐欺の認知件数・被害額】



¹⁶ 詐欺には、電子計算機使用詐欺を含む。

¹⁷ 令和8年上半期のインターネットを利用した犯罪の認知件数のうち、詐欺以外は、脅迫（876件）、名誉毀損（677件）、恐喝（309件）、信用毀損・威力業務妨害（216件）、横領（107件）等である。

¹⁸ 令和8年上半期のインターネットを利用した犯罪の被害額のうち、詐欺以外は、横領が約29億円と約9割を占める。

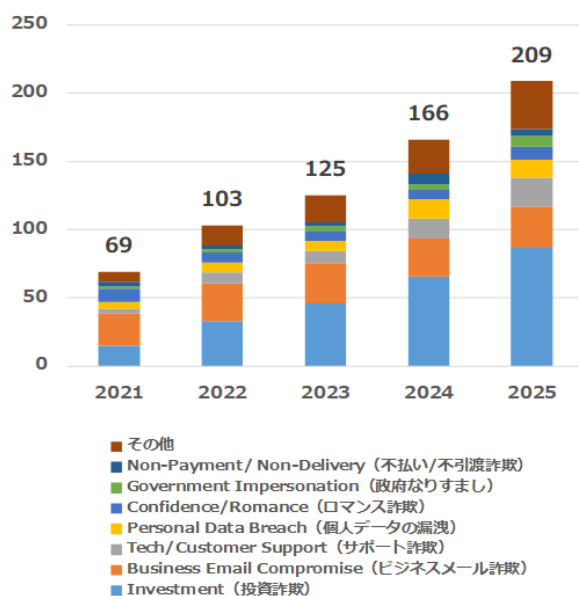
コラム：米国におけるサイバー犯罪の情勢

詐欺被害の急増は我が国のみならず他国でも見られる。米国連邦捜査局（FBI）のインターネット犯罪通報センター（IC3）が発表した 2025 年インターネット犯罪レポート¹⁹によると、2025 年に IC3 が受理したインターネット利用詐欺に関する相談件数は約 100 万件、被害総額は約 209 億ドル（前年比+26%、日本円で約 3.3 兆円（1 ドル=160 円換算））に達するなど、米国においても過去最悪の被害となっている。

日米両国における被害の共通点として、投資詐欺の深刻な被害が挙げられる。日本では、令和 7 年 7 月以降、著名人の画像や動画を無断で使用したバナー等広告による SNS 型投資詐欺の増加が顕著であるほか、令和 7 年中に発生した SNS 型投資詐欺 1 件あたりの被害額が平均 1,358.2 万円に上るなど、非常に大きな脅威となっている。また、米国においても、投資詐欺の被害総額が約 86 億ドル（前年比+31.6%、日本円で約 1.38 兆円（1 ドル=160 円換算））になるなど、全インターネット犯罪中で最大の被害となっている。

また、公的機関職員へのなりすましによる詐欺被害も日米共通の課題である。日本では、令和 7 年中の警察官等をかたる「ニセ警察詐欺」による被害総額が約 1,005 億円を記録し、特殊詐欺全体の被害総額の 70.6%を占めるに至った。米国においても、政府機関なりすまし（Government Impersonation）による詐欺の被害額が約 8.0 億ドル（前年比+97%、日本円で約 1,280 億円）に上るなど、被害の急増が見られており、FBI の公式 YouTube チャンネル²⁰においても、FBI 捜査官等へのなりすましについて注意喚起がなされている。そのほか、同チャンネルでは、東南アジア諸国における詐欺拠点や国際的な詐欺対策に関連する動画が公開されている。

【米国におけるインターネット利用詐欺被害の内訳】
(億ドル)



出典：https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf
https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf

¹⁹ https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

²⁰ <https://www.youtube.com/@fbi>

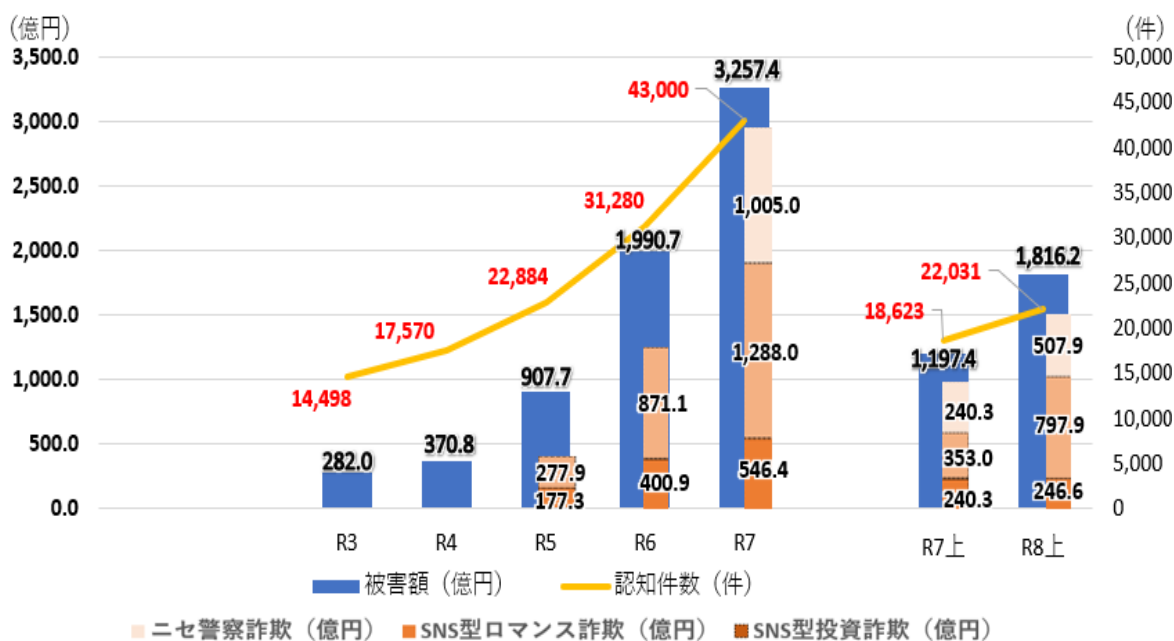
(1) インターネット空間で提供されるサービスの悪用

① SNS・メッセージングアプリの悪用

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

令和8年上半期の特殊詐欺の被害額は約1,816億2,000万円（前年同期比51.7%増）と、過去最悪となった令和7年の被害額を上回るペースで推移している。

【図表10：特殊詐欺の認知件数・被害額】



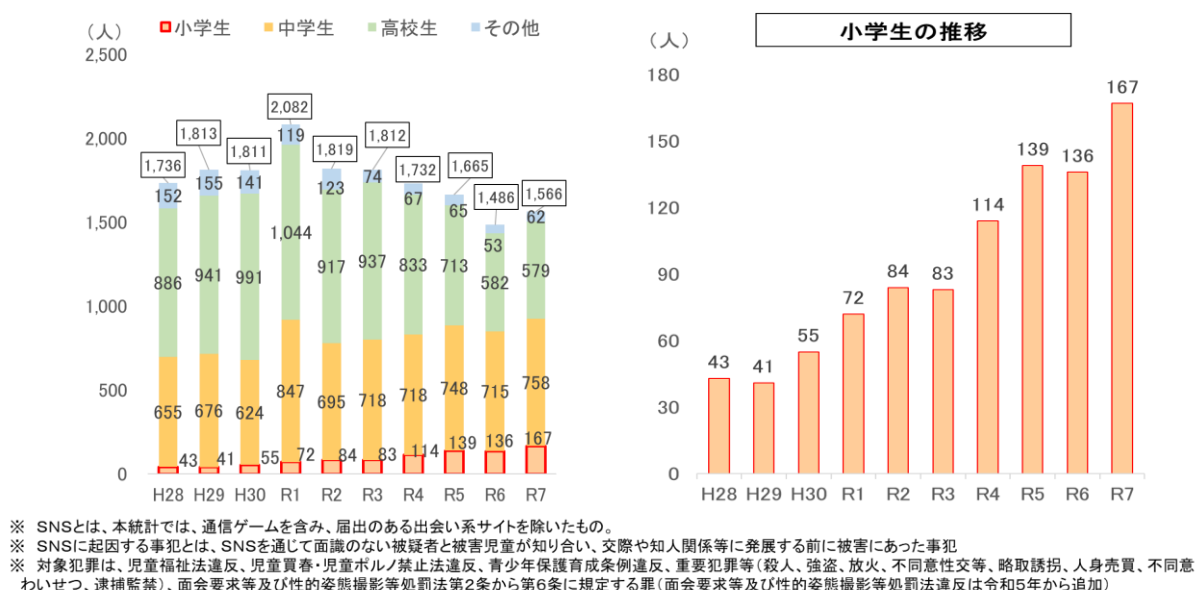
※SNS型投資詐欺・SNS型ロマンス詐欺については、令和5年から計上。

※ニセ警察詐欺については、令和7年から計上。

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

また、近年は、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SNSの特性から、児童買春等の悪質な事犯のコミュニティとなっている状況もうかがえる。実際、SNSに起因して性犯罪等の被害に遭った小学生の被害児童数は、令和7年に167人を記録するなど、近年増加傾向にあり、被害児童の低年齢化の傾向が見られる。

【図表 11：SNS に起因する事犯の学職別被害児童数】



さらに、オンラインゲームに関連する事案も発生しており、例えば、オンラインゲーム内のアイテムやゲーム内通貨等と現実空間の通貨（電子マネー等を含む。）を交換するリアルマネートレードに起因する犯罪が発生している。

【CASE：リアルマネートレードサイトにおける不正課金事案の検挙】

仲間と共謀してゲーム会社のサーバに虚偽の情報を与え、不正にゲーム内通貨を取得したとして、令和6年6月、会社員の男（32歳）を電子計算機使用詐欺で逮捕した。同男は、リアルマネートレードサイトで集客し、複数の課金代行依頼者のゲームアカウントへ不正に取得したゲーム内通貨を付与し、その代金を受け取っていた。（警視庁）

【リアルマネートレードのイメージ】



② メール・SMSの悪用

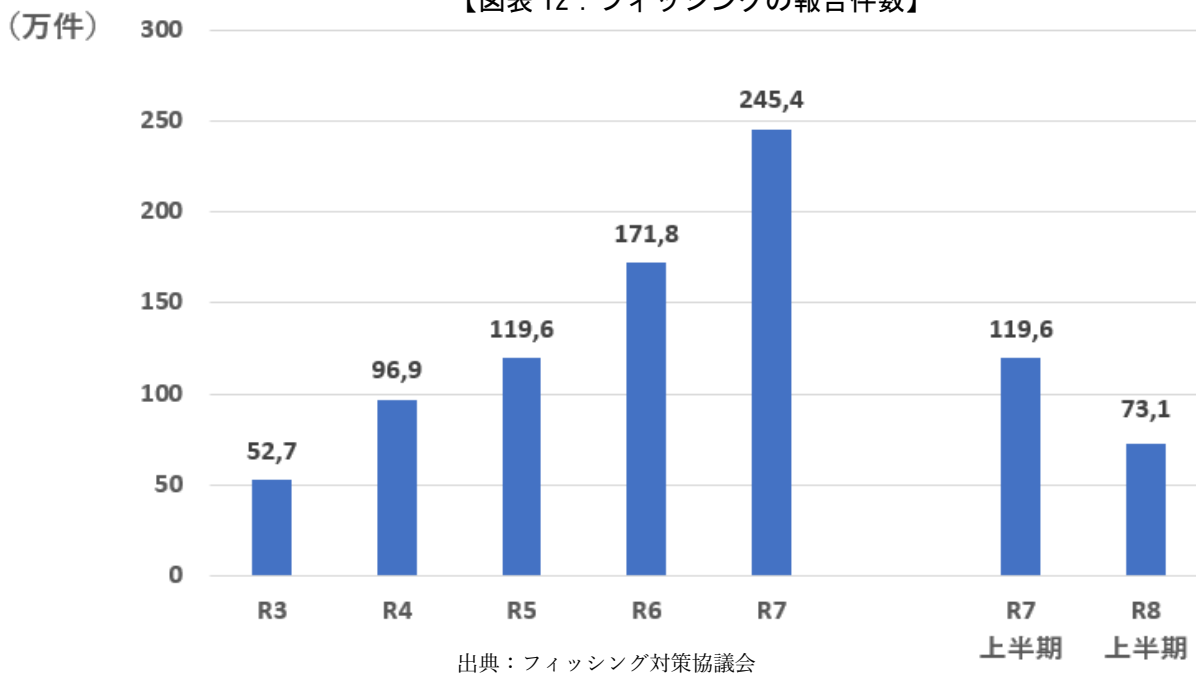
メールやSMS（Short Message Service：電話番号を宛先にしてメッセージをやり取りするサービス）は、フィッシング²¹に悪用される実態がみられる。フィッシングとは、実在する組織を装ってメールやSMSのリンクから偽のウェブサイト（フィッシングサイト）へ誘導し、同サイトでアカウント情報やクレジットカード番号等を不正に入手する手口であり、これによって得られた情報はインターネットバンキングに係る不正送金やクレジットカードの不正利用に使われている（統計編 161 頁及び 162 頁参照）。

令和 8 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、約 73 万件である。

フィッシングは、人の信頼や思い込みなどの心理的な隙につけこんだソーシャルエンジニアリングの一形態であるが、近年は、AI 技術の発達により、文章の自然さや偽装の精度が大幅に向上するなど、従来と比較して見抜きにくいフィッシングが増加している。

これらの被害を防ぐためには、メール認証や多要素認証等の技術的な対策だけでは十分ではなく、「メール等に記載のリンクを安易にクリックしない」、「公式サイトや公式アプリからアクセスする」など日常的なサイバーセキュリティ意識の向上を図ることが重要である。

【図表 12：フィッシングの報告件数】



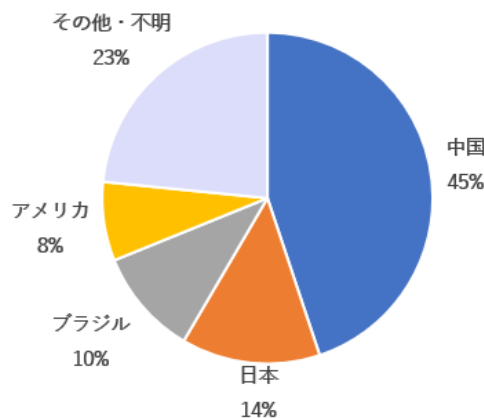
²¹ フィッシング (phishing) とは、英語の fishing (フィッシング：魚釣り) と sophisticated (ソフィスティケイティッド：洗練された) という 2 つの言葉が合わさった造語とされる。エサ (偽のメールやサイト) を使っておびき寄せ、パスワード等の情報を「釣り上げる」手口とその巧妙さに由来するとされる。

コラム：フィッシングメールの送信元分析

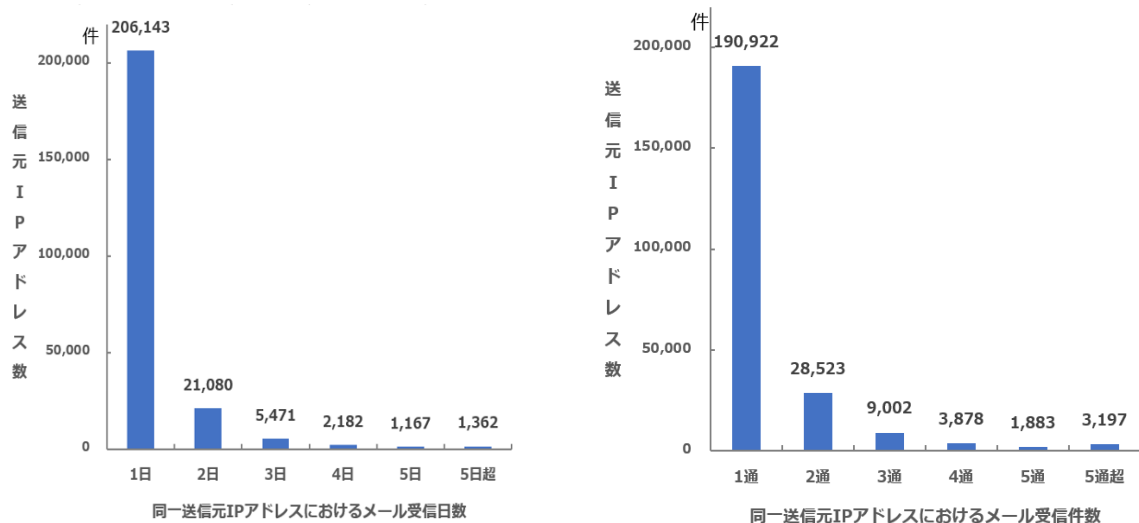
サイバー特別捜査部が入手した過去1年間（令和7年8月1日～令和8年7月31日）のフィッシングメールと評価される約36万件の受信メールを対象に分析を行ったところ、送信元IPアドレスから推定される送信元サーバの所在国として最も多いのは中国、次いで日本、ブラジルの順であった。

また、同一の送信元IPアドレスごとに、何日間にわたってフィッシングメールを受信していたか、何通のフィッシングメールを受信していたか、という点について分析したところ、多くの送信元IPアドレスから1～3日の限られた日数に1～3通のフィッシングメールを受信していた。これは、フィッシンググループがIPアドレスを次々と変えながらフィッシングメールを送っていることを意味している。攻撃者は、ターゲットやキャンペーン²²ごとにメール送信用インフラを短期間で切り替えるなど、メール送信用インフラを継続利用しない傾向が強いと言える。

【図表 13：フィッシングメールの送信元サーバ所在国の割合】



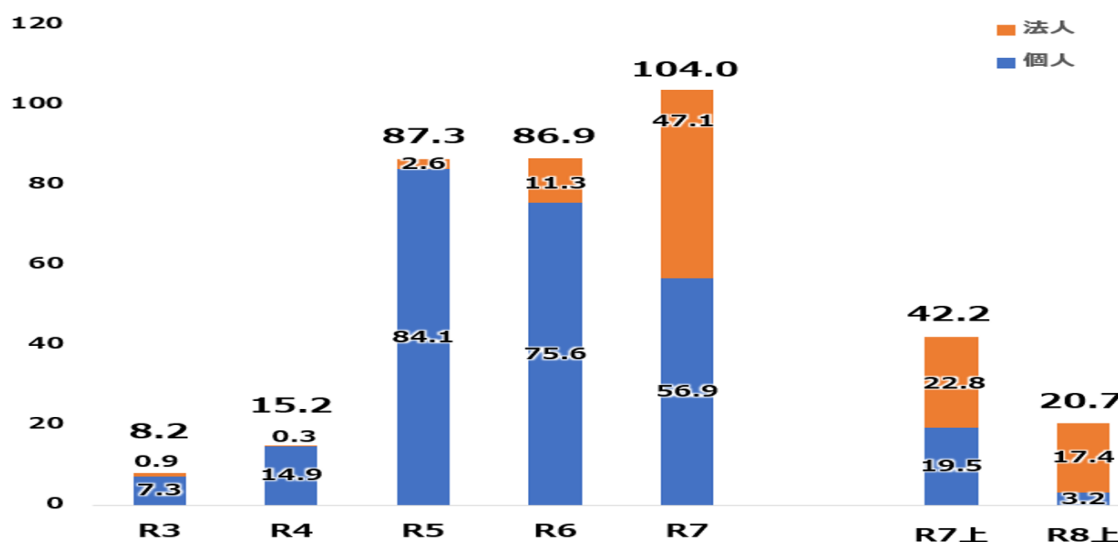
【図表 14：同一送信元IPアドレスからフィッシングメールを受信した日数・件数】



²² 攻撃者が一定の目的やテーマ、対象者を設定して行う一連のサイバー攻撃活動。

また、令和8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253件、被害総額は約20億7,000万円（前年同期比51%減）となっている。

【図表15：インターネットバンキング不正送金被害額】

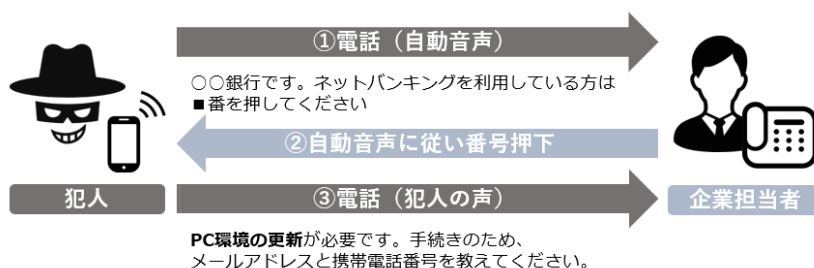


コラム：ボイスフィッシングによる不正送金被害

フィッシングにおいては、令和6年秋から、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き等のかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシング（ビッシング）という手口による法人口座の不正送金被害が急増した。

また、令和8年5月、企業への架電を起点として、外部からの操作を可能とする遠隔操作ソフトをインストールさせ、企業側の端末を遠隔操作すると同時に、偽サイトに誘導してインターネットバンキングのID・パスワードを窃取し、不正送金を実行するという新たな手口による被害が急増するなど、手口の巧妙化が見られる。遠隔操作により、企業が普段使用している端末から送金を実行することで、金融機関による端末認証や不正取引監視を回避しようとする意図があると考えられる。

【ボイスフィッシングの架電イメージ】

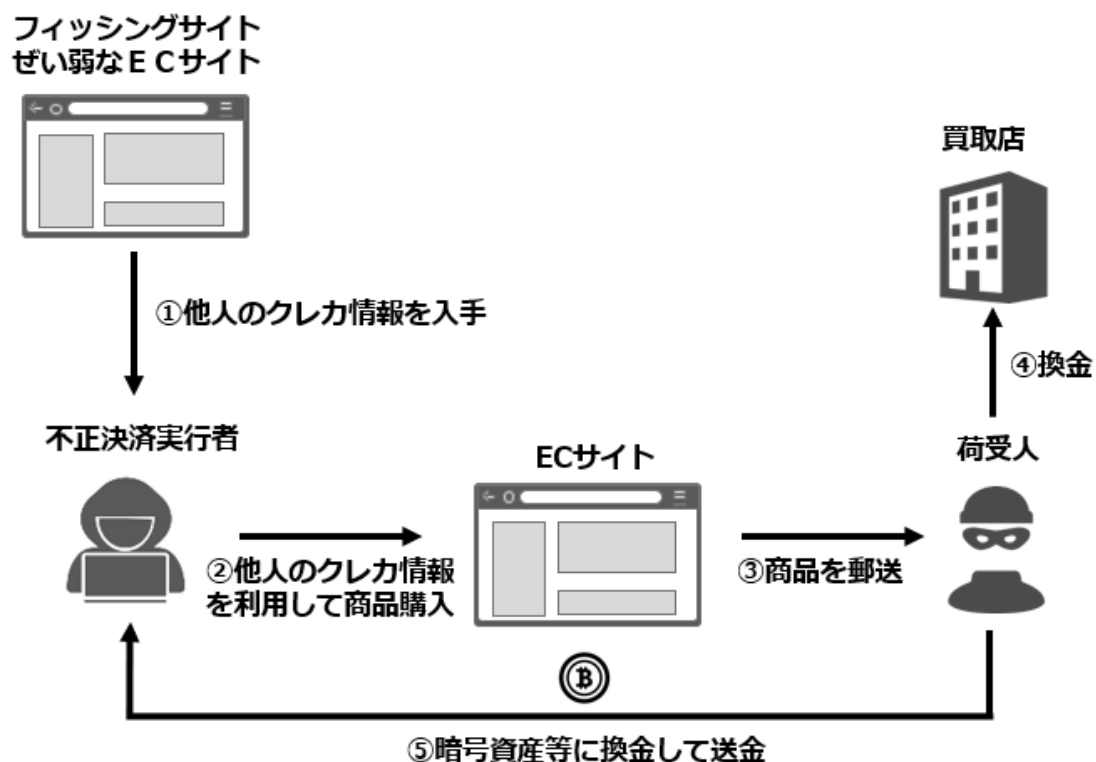


さらに、一般社団法人日本クレジット協会によれば、令和8年上半期のクレジットカードの不正利用被害額は約221億円（前年同期比30%減）となっている。

【図表 16：クレジットカード不正利用被害額】



【図表 17：クレジットカード不正利用の流れ】



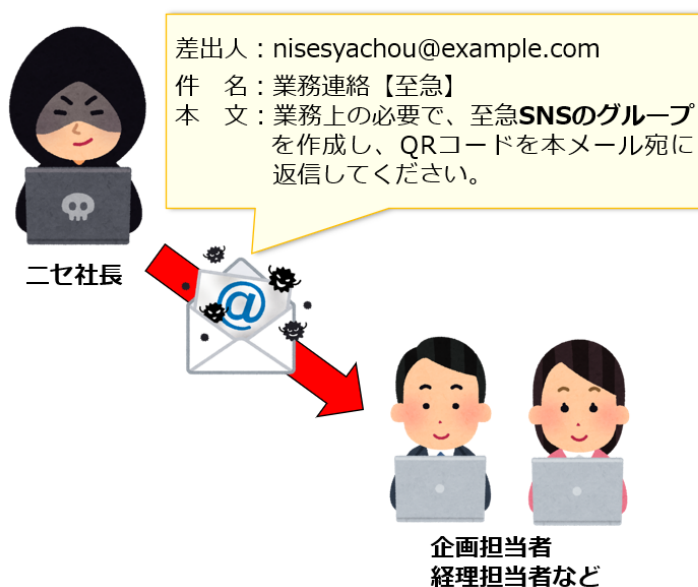
コラム：メールを悪用した新たな詐欺手口～ニセ社長詐欺～

令和8年1月頃から、法人の経営者等になりすまして、インターネット等で公開されている法人等のメールアドレス宛てに電子メールを送信し、業務を装って指定した口座に送金させるなどして金銭をだまし取る詐欺が発生している。

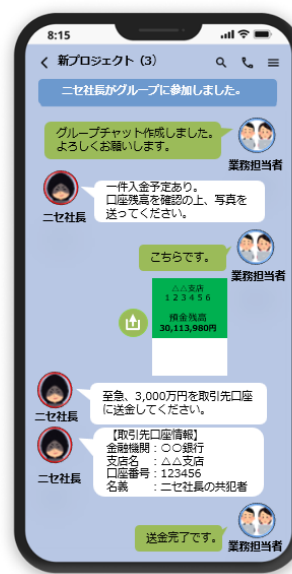
具体的な手口の流れとしては、経営者等になりすましたニセ社長から、インターネット等で公開されている法人のメールアドレスに電子メールが届き、「新しいプロジェクトのため」などと業務を装って、SNSグループの作成が指示され、同グループ内でのやりとりの中で、法人の口座残高を回答させるなどした上で、「事業資金が至急必要」等と指定した口座に送金させるというものである。実在する社長名や会社名が使われているために、気がつきにくいという特徴がある。

令和8年1月から6月までに、認知件数127件、被害額約38億8,000万円が確認されている。法人被害のため被害額が高額になる傾向があり、既遂1件当たりの被害額は約3,100万円であった。

【ニセ社長詐欺の手口イメージ】



【SNSのグループにおける送金指示（イメージ）】



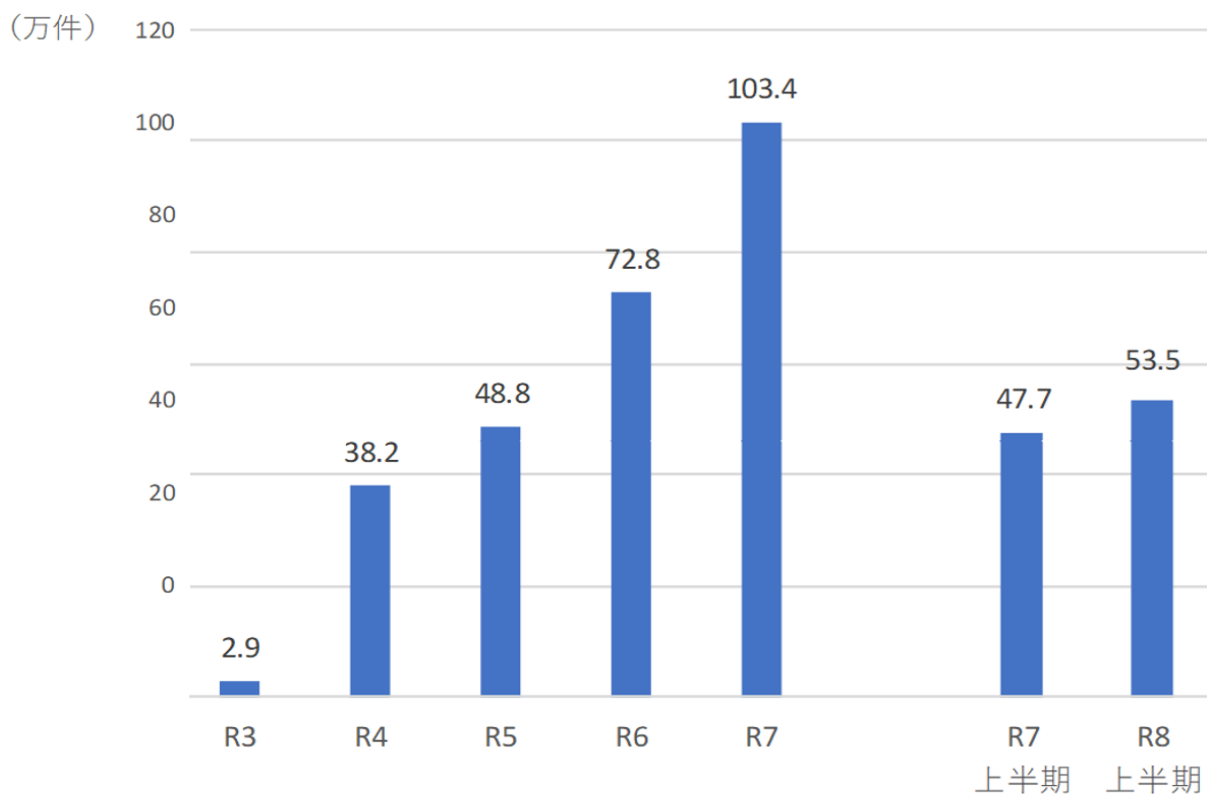
ニセ社長詐欺の被害を防ぐためには、この種事案の発生について社内で情報共有を行うほか、送金に関するルールの再確認や、SNSグループの利用を指示された場合には特に注意するといった対応を社内で徹底する必要がある。仮にSNSグループに誘導されてしまった場合には、SNS内のトーク画面やプロフィール画面等に「通報」²³機能がある場合は通報をした後、速やかにSNSグループから退出することが適切である。

²³ 事業者側に通知する仕組み。事業者側が通報内容を確認し、利用規約に違反していると判断された場合には、アカウントの利用制限等の必要な措置を行うため被害防止対策として有効である。

③ ウェブサイトの悪用

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。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や偽のインターネットショッピングサイト、投資や副業を勧誘するサイト等に係る被害が多発している。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 18：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引き続き発生している。令和8年上半期における架空料金請求詐欺のうち、パソコンのウイルス除去をサポートするなどの名目で電子マネー等をだまし取る「サポート名目」の認知件数は735件（前年同期比10.4%増）、被害額は約8億3,000万円（前年同期比13.3%減）となっている。

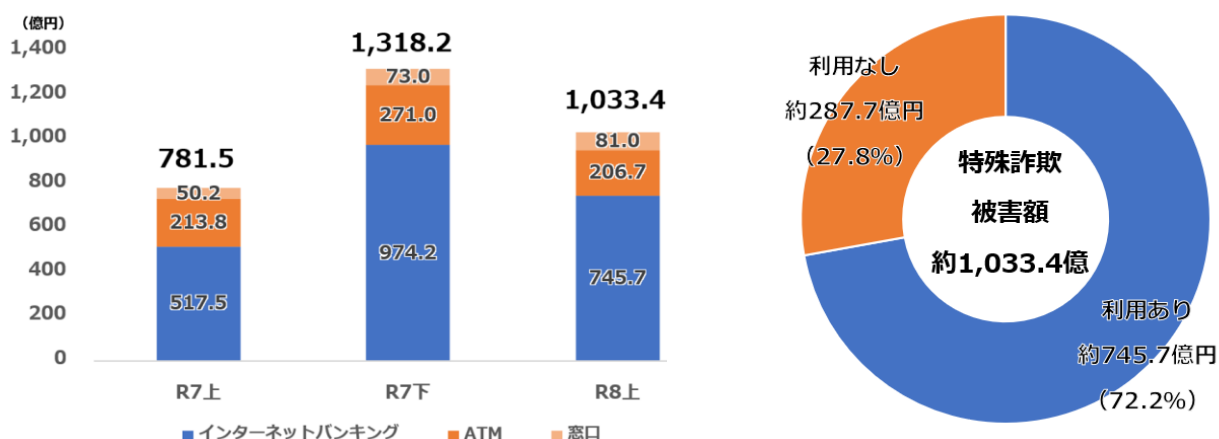
(2) インターネット空間における資金移動の悪用

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

① インターネットバンキング

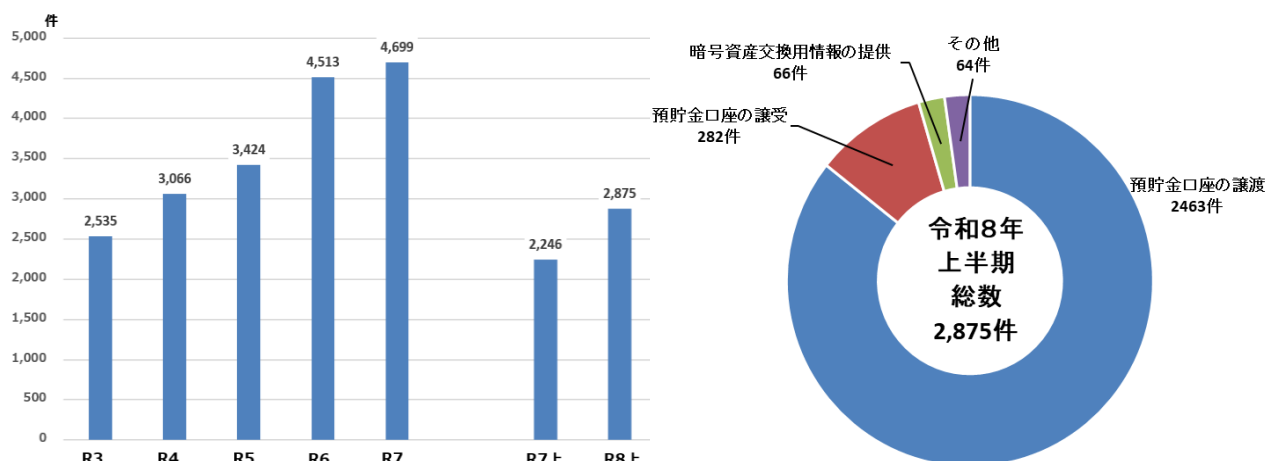
令和8年上半期における振込型の特殊詐欺被害（認知件数1万2,263件、被害額約1,033億4,000万円）のうち、インターネットバンキングを利用したものの被害額は振込型全体の約7割を占めるなど、引き続きインターネット空間における資金移動が犯罪に悪用されている実態が見られる。

【図表19：特殊詐欺におけるインターネットバンキングの利用状況】



また、預貯金口座の譲渡等を規制する犯罪収益移転防止法違反の検挙件数は、年々増加傾向にある。

【図表20：犯罪収益移転防止法違反の検挙件数】



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。また、暗号資産に対する規制は各国において異なることから、暗号資産交換業者が所在する国・地域の中には、本人確認等の措置が義務付けられていないものもあるほか、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、移転の記録が暗号化されるなど、追跡が困難なものもある。さらに、暗号資産取引の匿名性をさらに高めるため、暗号資産交換を個人が無登録で業として行う、いわゆる「^{あいたいや}相対屋」を経由しながら送金を繰り返したり、他の暗号資産と混ぜ合わせ、取引の流れを不透明にすることで送信アドレスと受信アドレスのつながりを隠す「ミキシングサービス」等のサービスを利用したりするなどして、その追跡を困難にし、マネー・ローンダリングに悪用している実態がある。

このほか、国外においては、犯罪収益の洗浄に用いられる「ミキシングサービス」の中には、不正に窃取又は購入された本人確認情報を用いて架空の暗号資産アドレスを開設し、これらの暗号資産アドレスをミキシングに用いるなど、大規模に組織化されている例も確認されている。

【図表 21：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) I o T機器の悪用

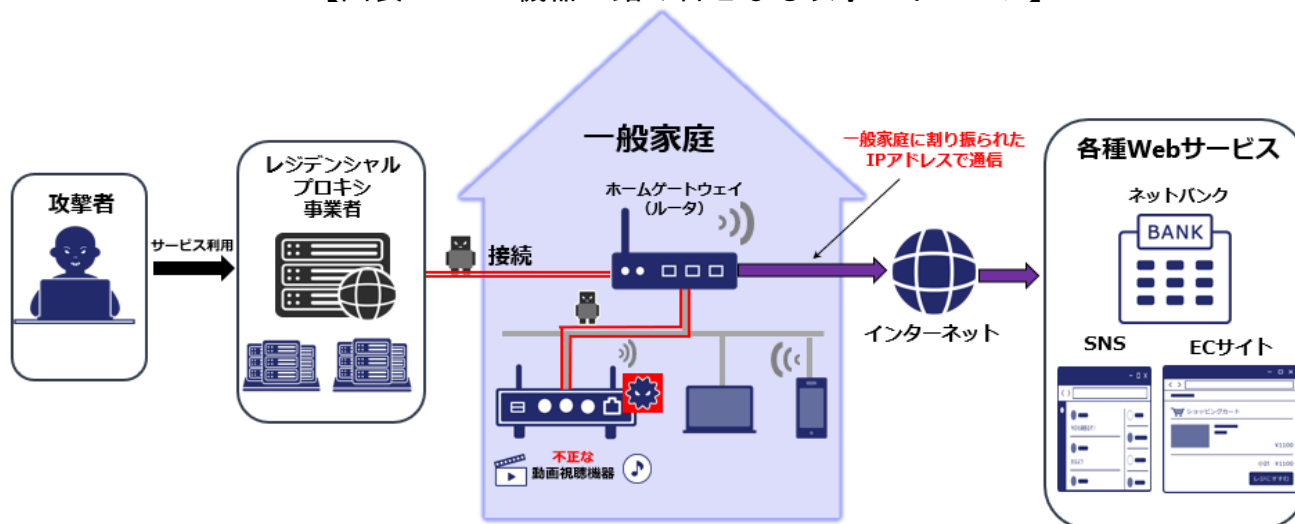
一般家庭で使用されるネットワーク接続機能を有する機器（I o T機器という。I o TとはInternet of Things（モノのインターネット）の略。）について、機器の所有者の認識しないところでいわゆる「レジデンシャルプロキシ」（一般家庭の回線を利用して通信を中継し、接続を行う仕組み。「プロキシ」とは、自分の端末とウェブとの間に入り、通信を代理・仲介する機能をいう。）として動作し、踏み台として悪用される事案が多発している実態が明らかとなっている。

例えば、「テレビに接続して海外動画を無料で視聴できます」などと称して販売されている不正な動画配信用機器が不正アクセス等の踏み台として悪用される事案が発生している。これらの機器の中には、購入前の段階において、ダウンロード等の不正なソフトウェアが仕込まれた機器が流通しているものもあり、当該機器をインターネットに接続することにより、使用者の気付かぬうちにマルウェアをインストールしてプロキシとして動作するものがある。

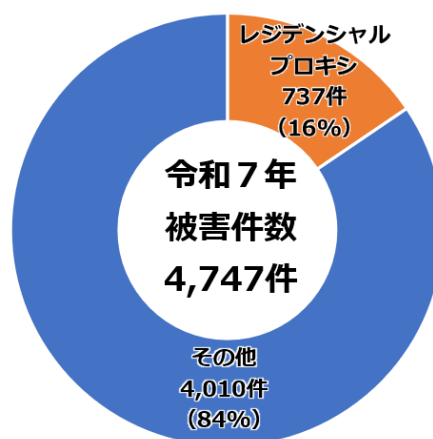
また、無料VPNサービスや無料音楽アプリケーションの中に、プロキシ機能を持たせるためのマルウェアが組み込まれたものが含まれている場合があり、これらを機器にインストールすることで、利用者の端末がレジデンシャルプロキシとなる事例も確認されている。

これらの機器が踏み台となり、攻撃者の通信を中継した場合、通信先のサーバのログには、攻撃者のIPアドレスではなく、踏み台となった機器のIPアドレスが記録される。海外の攻撃者であっても、国内の機器を踏み台とすることにより、海外からのアクセスを制限したサーバにアクセスすることも可能となるなど、セキュリティ対策上の重大な脅威となっているとともに、サイバー犯罪捜査においても深刻な障害となっている。

【図表 22: IoT 機器が踏み台となる攻撃のイメージ】



例えば、令和7年中に発生したインターネットバンキングに係る不正送金事犯（被害件数4,747件、被害額約104億円）において、犯行時にレジデンシャルプロキシが用いられた事案は少なくとも737件、被害額は約13.9億円に及ぶ。令和8年中においても、引き続き犯行時にレジデンシャルプロキシが用いられた事案を多数認知しており、依然としてセキュリティ対策上の脅威となっている。



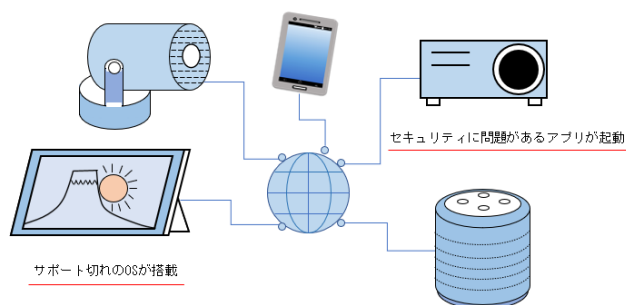
【図表 23：不正送金被害におけるレジデンシャルプロキシの悪用件数】

コラム：セキュリティ対策が十分でないIoT機器

令和8年、警察庁情報技術解析課において、不正アクセスの踏み台となった可能性のあるデジタルフォトフレームやプロジェクタを解析したところ、サポートが終了したOSが搭載されている、OSの管理者権限が簡易な設定で利用できる、セキュリティ上問題のあるアプリがインストールされているなどの状況が判明した。

これらのようにセキュリティ対策が不十分なIoT機器には第三者によって不正プログラムのインストールが行われるなどの危険性が存在するため、JC-STAR²⁴の適合ラベルが付与された製品を選択する、購入前にメーカーのウェブサイト等で仕様やセキュリティ情報を十分に確認する、購入後もセキュリティ対策を継続することなどが重要である。

【セキュリティ対策が十分でないIoT機器の例】



【JC STAR のロゴ】



²⁴ 「JC STAR」とは、Japan Cyber - Security Technical Assessment Requirements の略。IoT製品のセキュリティ評価とラベリング制度により、買い手が安全な製品を安心して選べる環境を作る公的制度であり、経済産業省と情報処理推進機構（IPA）が推進している。

(4) AIの悪用

現在急速に一般社会で利用が広がっているAIについては、国民生活の向上及び国民経済の発展に寄与する一方、多くの国民がAIにより発生するリスクに不安を抱えている。具体的には、AI技術を悪用した不正プログラム・フィッシングサイトの作成、偽・誤情報作成、CBRNE テロ²⁵の実行に必要な情報の収集、機密情報の漏えいといった、犯罪や国家安全保障への影響が懸念されている。実際にも、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が確認されている。

また、近年、高性能AIが出現し、攻撃者に悪用されることでサイバー攻撃がより高速かつ大規模に行われるリスクが懸念されるなど、AIをめぐる情勢は日々刻々と変化している。

【図表 24：AIをめぐる脅威情勢】



(出典：警察庁HP)

(出典：ガバメントAI「源内」で作成)

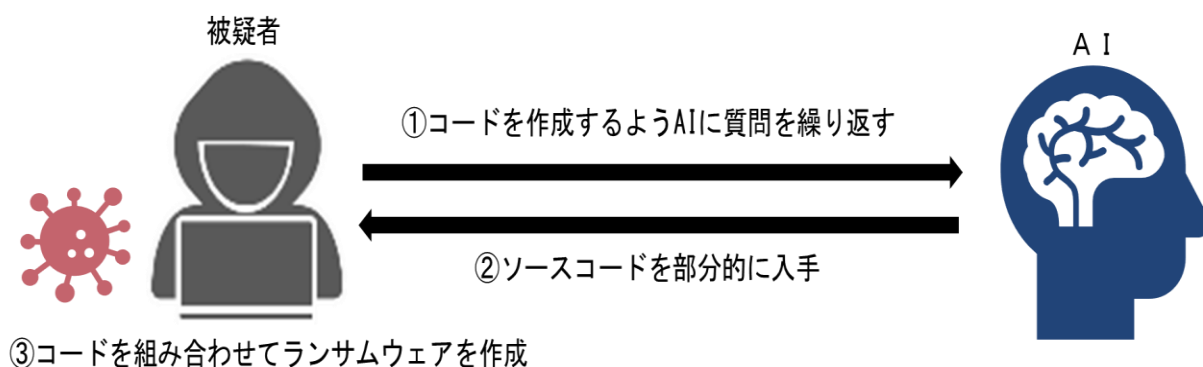
AIが発達することにより、人間が関与せず、AIで自動化したサイバー攻撃が今後増える可能性がある。例えば、国家を背景とするサイバー攻撃グループがAIを利用し、人間の介入なしにサイバー攻撃を実施したとの民間企業の報告がある。生成AIで攻撃のハードルが下がることにより、高度な技術を持ち合わせない者であっても、サイバー攻撃を実行することが容易になると考えられる。

²⁵ C (Chemical：化学) B (Biological：生物) R (Radiological：放射性) N (Nuclear：核) E (Explosive：爆発性) 物質を使用したテロの総称。

【CASE：A I を悪用してランサムウェアを作成した被疑者の検挙】

会社員の男(19 歳)は、飲料メーカーがランサムウェアによる攻撃を受けたという報道を見て、ランサムウェアを作成してお金を稼ごうと思い、令和 8 年 2 月、A I を悪用して作成したソースコード（プログラムの動作を指示する命令文）を組み合わせることでランサムウェアを作成した。令和 8 年 6 月、同男を不正指令電磁的記録作成で逮捕した。（千葉）

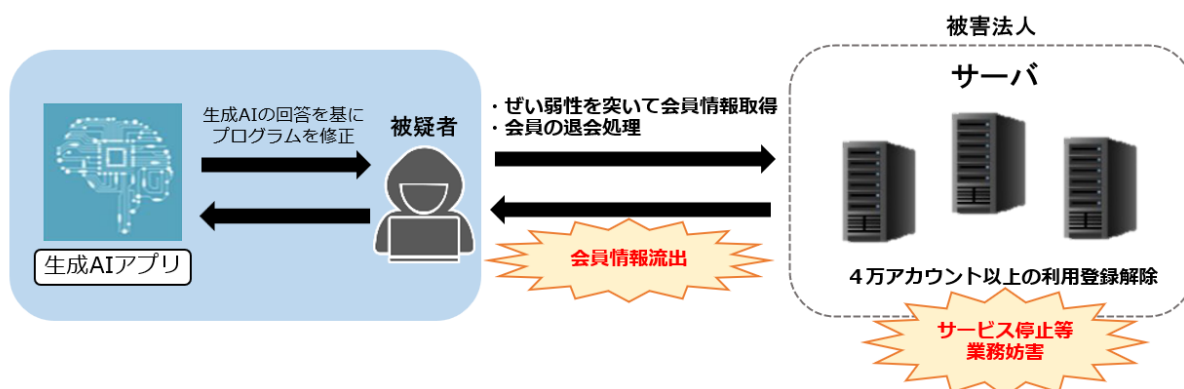
【A I を悪用したランサムウェア作成】



【CASE：少年による動画配信サービス運営会社に対する偽計業務妨害事件の検挙】

高校生の少年（15 歳）は、動画配信サービスのサーバにぜい弱性を発見し、令和 7 年 11 月、生成 A I を用いて修正した自作の攻撃プログラムを使用して同サービス運営会社に対し、同サービス利用会員アカウントの利用登録を解除する旨の虚偽の情報を順次送信して、約 4 万 6,800 アカウントをその利用登録者の意に沿わぬ退会処理をするなどさせて業務を妨害した。令和 8 年 7 月、同少年を偽計業務妨害で逮捕した。（警視庁）

【A I を悪用した偽計業務妨害】



また、A I を悪用することで詐欺や性的ディープフェイクを始めとする各種犯罪が巧妙化している。

【CASE：A I を悪用して警察官になりすました特殊詐欺被疑者の検挙】

令和6年10月頃から令和7年5月頃までの間、被疑者等は、海外の特殊詐欺拠点において、日本国内にいる被害者に対し、電話やSNSの通話機能等を利用して、「マネー・ローンダリング事件に関与している嫌疑があるため、保有する預貯金の流れを確認する必要がある。」などとうそを言い、現金をだまし取っていた。だます過程において、警察官役がSNSのビデオ通話機能を使い、あらかじめ準備していた警察官の制服様のものを着用して、偽の警察手帳を呈示し、さらには警察官役（被疑者）の顔が識別されないよう顔をA I で生成して、被害者をだましていた。警察が提供した情報に基づき海外の当局が犯行拠点を摘発し、令和7年8月、身柄の引き渡しを受け、逮捕した。（愛知、栃木、千葉、静岡、岐阜、三重）

【A I を悪用して警察官になりすました特殊詐欺】



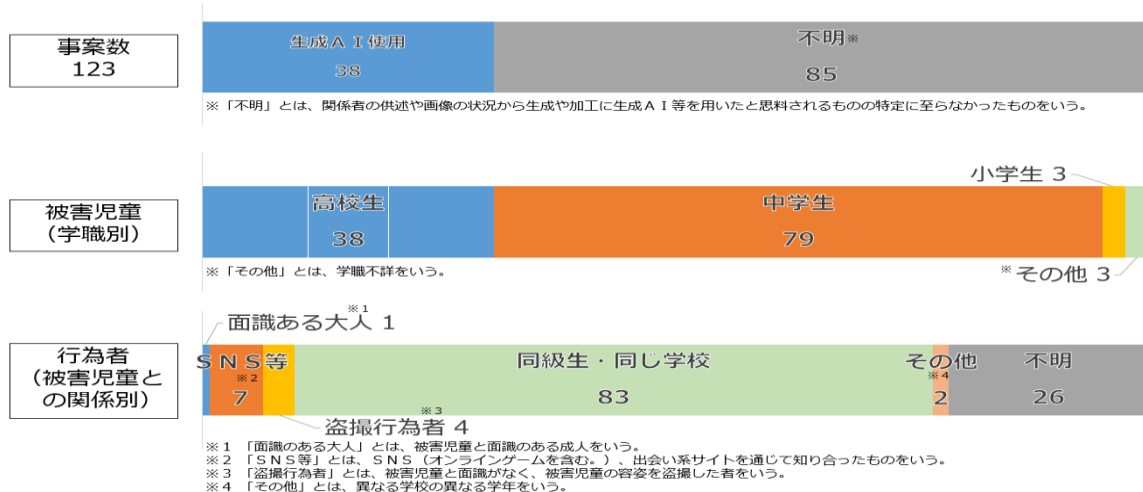
【CASE：A I を悪用してわいせつ画像を作成した被疑者の検挙】

生活費を得る目的から、会員制ウェブサイトを自作し、会員費を徴収した上で、会員に対し、同サイト上で生成A I を利用して作成したわいせつな画像を公開した。令和8年4月、同男をわいせつ電磁的記録記録媒体陳列で逮捕した。（富山）

コラム：生成ＡＩによる児童の性的加工画像

生成ＡＩをはじめとした技術の急速な発展・普及により、専門的な知識を有しない者でも容易に画像を加工・生成できる環境が整うとともに、加工対象となる画像等をインターネットを通じて容易に入手可能な状況になったことで新たな種類の性被害が生じている。

【図表 25：生成ＡＩにより児童の画像を性的加工した事案】



18歳未満の実在する児童の画像に対し、生成ＡＩ等により何らかの加工を加えた性的画像の都道府県警察における取扱事案数は、令和８年上半期（１月～６月）の間において、123件（前年同期比63件（105%）増）であり、上半期のみで令和７年中の取扱事案数（114件）を上回る大幅な増加傾向を示している。

被害児童については、中高生が全体の約９割を占めており、小学生の被害もあるほか、行為者と被害児童との関係は、同級生や同じ学校の者が約７割を占めている一方、教師といった面識のある大人や、盗撮行為によるものも確認されている。

こうした情勢の中、令和７年には、生成ＡＩを悪用した児童の性的加工画像をめぐる事案について、初めて児童ポルノ禁止法を適用して検挙した。（愛知）

同事案は、小学校教諭が児童の画像を第三者に送信の上、生成ＡＩにより裸体の画像に作成するよう依頼し、自己の性的目的で所持していたものであり、これについて名古屋地裁は、令和８年６月、「一般人が見れば当該女子児童の裸の姿態が撮影されたものであると誤信するに足る精巧なもの」などと判示し、同画像を児童ポルノと認定して有罪判決を言い渡した。

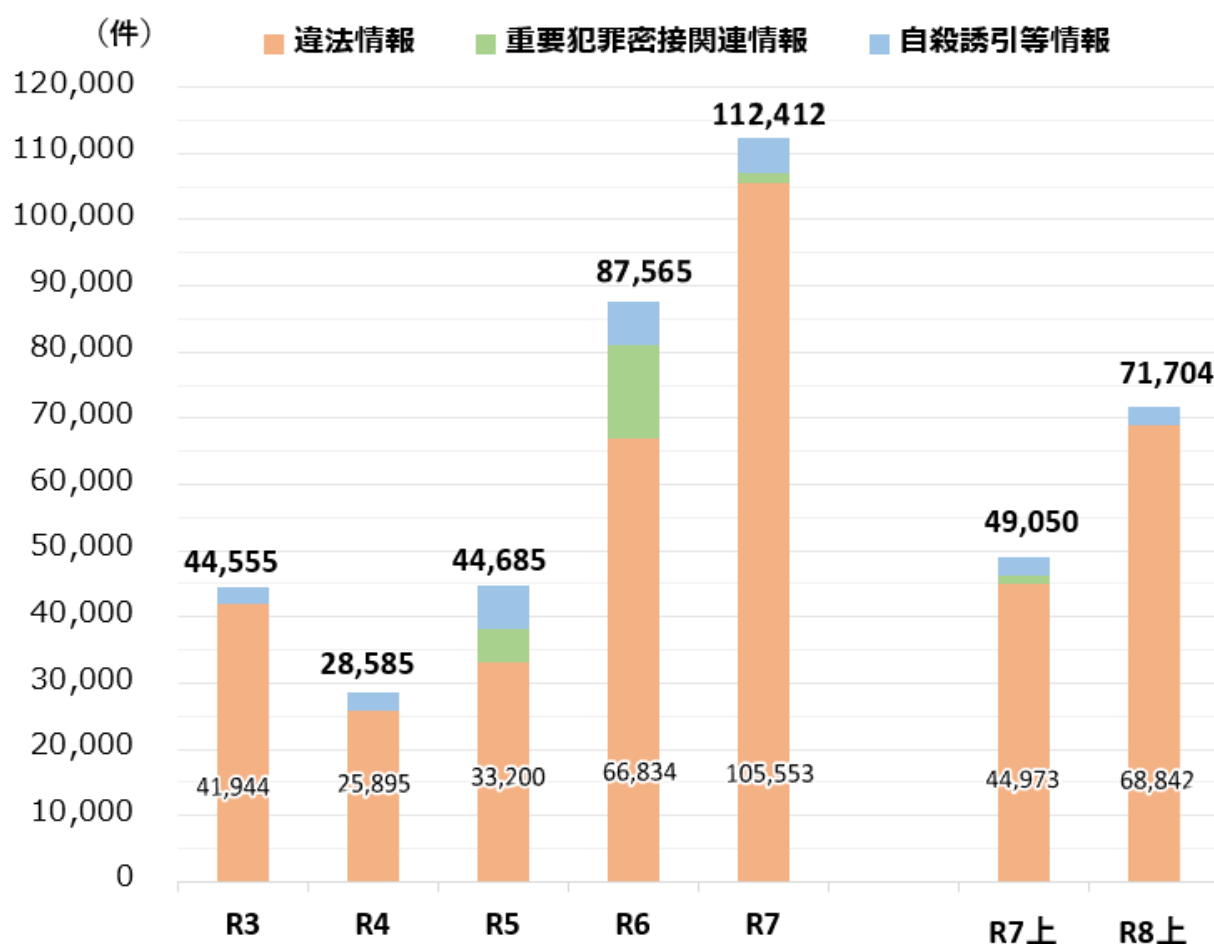
警察では、相談者・被害者の心情に配慮しつつ、事案の内容に応じて刑法や児童ポルノ禁止法等での事件捜査や指導警告等を実施するとともに、学校等の関係機関とも連携し、未然防止のための広報啓発を推進しており、潜在的な事案も含め、今後も注視する必要がある。

3 違法・有害情報

インターネット上には、近年、社会問題となっている「犯罪実行者募集関連情報」、「違法オンラインギャンブル等関連情報」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、社会的混乱を生じさせる偽情報・誤情報が存在しており、サイバー空間における治安上の脅威となっている。

令和8年上半期のIHCにおける判断件数は、違法情報6万8,842件（前年同期比約53%増）、重要犯罪密接関連情報107件（前年同期比約92%減²⁶）、自殺誘引等情報2,755件（前年同期比約0.7%増）であった（統計編171頁参照）。

【図表 26：違法・有害情報の判断件数】



²⁶令和7年2月28日、重要犯罪密接関連情報の類型であった犯罪実行者募集情報を違法情報に位置付けたことにより、令和7年上半期と比較して令和8年上半期における重要犯罪密接関連情報の数が大きく減少した。令和7年2月27日までに犯罪実行者募集情報と判断された重要犯罪密接関連情報の件数は1,158件であった。

(1) 違法情報

近年インターネット上には、匿名・流動型犯罪グループ等による犯罪の実行者を募集する犯罪実行者募集情報が氾濫しており、令和8年上半期のインターネット・ホットラインセンター（IHC）の受理件数のうち、1万2,516件（前年同期比約97%増）が犯罪実行者募集情報と判断された。このような募集情報への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、この種の情報の氾濫により深刻な治安上の脅威になっている。

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

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

令和8年上半期のIHCの受理件数のうち、5,259件が違法オンラインギャンブル等関連情報と判断された²⁷。

【図表 27: 犯罪実行者募集のイメージ】



(2) 有害情報

有害情報としては、「殺人等」、「臓器売買」等の個人の生命・身体に危害を加えるおそれが高い重要犯罪と密接に関連する重要犯罪密接関連情報のほか、「自殺関与」や「自殺の誘引・勧誘」といった自殺誘引等情報が挙げられる。

令和8年上半期の主な重要犯罪密接関連情報のIHC判断件数は、殺人等48件、臓器売買44件であり、自殺誘引等情報の内訳は、自殺関与4件、自殺の誘引・勧誘2,751件であった。

²⁷違法オンラインギャンブル等関連情報は、令和7年9月25日からIHCにおいて違法情報として取扱いを開始し、令和7年中のIHCの受理件数のうち、3,253件が違法オンラインギャンブル等関連情報と判断された。

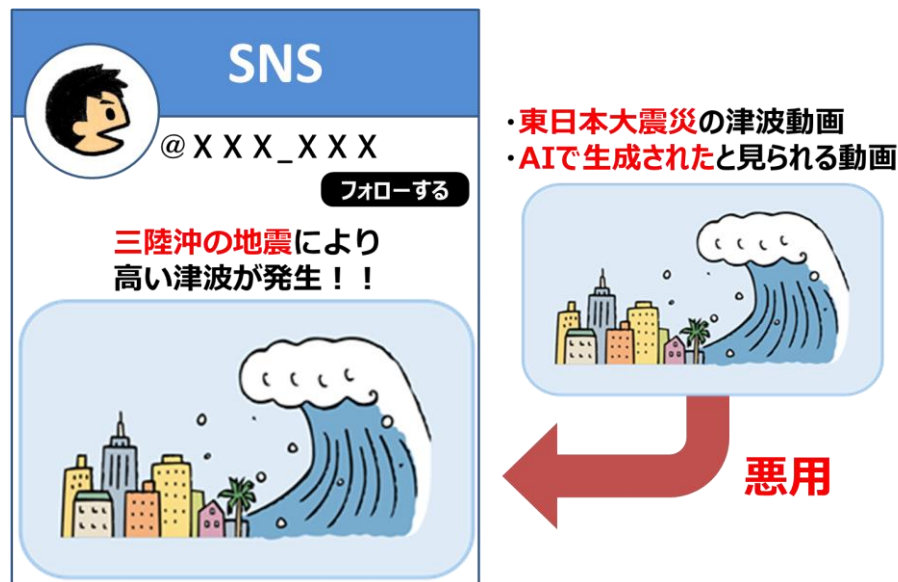
(3) 偽・誤情報

○ 災害発生時における偽・誤情報

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

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

【図表 28：SNS上における偽・誤情報投稿のイメージ】



○ 外国による偽情報

近年、国際社会では、他国の世論や意思決定に影響を及ぼし、自国にとって好ましい情報環境を生み出すため、偽情報の拡散を含む影響工作が様々な形で展開されている。

偽情報等の拡散は、軍事手段に加えて複合的に用いられったり、選挙への不当な介入のために行われたりする状況がみられるが、これは我が国にとっても安全保障上の脅威であり、選挙の公正や自由な報道といった民主主義の根幹を脅かすのみならず、我が国の治安にも悪影響をもたらし得るものであるところ、生成AI技術の進展等に伴い、巧妙な偽情報が大量に生成・拡散されるリスクへの対応が重要な課題となっている。

コラム：令和 8 年熊本地震に関連する偽・誤情報

令和 8 年 7 月 28 日の「令和 8 年熊本地震」が発生した際には、インターネット上において、

- 「令和 8 年熊本地震」とは関係のない建物の倒壊動画や、生成 A I により作成した動画を引用し、甚大な被害が発生していると印象付けるような投稿
 - 「外国人がコンビニで火事場泥棒をしている」旨の事実と異なる投稿
 - 過去の避難所設営状況の画像を転用して虚偽の避難状況を伝える投稿
- といった偽・誤情報が確認された。

【SNSで確認された偽・誤情報投稿のイメージ】



警察庁では、令和 8 年熊本地震が発生した際、災害の発生に乗じて、過去の災害画像を転用して虚偽の被害状況を伝える投稿や、存在しない住所と救助を求める投稿などの偽・誤情報による混乱、寄附金名目の詐欺関連の投稿・メールなどによる被害防止のため、過去の災害時に発生した事例を基にしたサイバー警察局便り「令和 8 年熊本地震に伴うインターネット上の偽・誤情報や災害に乗じた詐欺関連投稿等」に注意！」を警察庁ウェブサイトや警察庁公式 X により迅速に広報・注意喚起を実施した。



サイバー警察局便り

Cyber Police Agency Letter R8 Vol.8

令和 8 年熊本地震に伴うインターネット上の偽・誤情報や災害に乗じた詐欺関連投稿等に注意！

1 被害状況や救助に関する偽・誤情報

- 過去の災害画像を転用して被害状況を伝える投稿
- 存在しない住所と救助を求める投稿

チェックポイント

- ☒ 画像は本物？過去の災害等の無関係のものではない？
- ☒ 災害の専門家が発信している情報？
- ☒ 信頼できる提供元からの情報？（他のメディアでも報じられている等）

！ 不確かな情報を安易に信用し、拡散しないで！
迅速な救助や復旧・復興の妨げになる可能性があります。

2 災害に乗じた詐欺関連の投稿やメール

- 二次元コードを添付して寄附金を求める投稿
- 支援物資や義援金を募る E メールや SMS

チェックポイント

- ☒ 支援を求めるアカウントは、実在する団体等のもの？
- ☒ 文字や文章の一部がおかしかったり送信元メールアドレスが海外ドメインであるといった不審点はない？

！ 安易にコードの読み取りやリンクのクリックをしないで！
詐欺サイト等に誘導されるおそれがあります。

不審な投稿やメール等で不安を感じた場合は警察に通報、相談してください。

最寄りの警察署又は警察相談専用電話 ☎ #9110 (全国共通)

サイバー事案に関する通報等のオンライン受付窓口 (警察庁ウェブサイト)
<https://www.npa.go.jp/bureau/cyber/soudan.html>

避難しています。
今後のための
資金を寄付して
ください。
QR: #pay.●●





警察庁
National Police Agency

第2部 警察の取組

1 検挙に向けた取組

(1) 事案認知に向けた取組

サイバー事案を検挙するためには、まず、サイバー事案を的確に認知することが必要である。そして、国民・事業者等からの通報・相談は、捜査の端緒となるものであることから、いかに警察への通報・相談が積極的になされるか、という点が重要になってくる。他方で、サイバー事案においては、被害者側における風評被害や、早期復旧に支障が及ぶことなどへの懸念、届出すべきなのか分からないなどの理由から、被害者が通報・相談をためらう、いわゆる「被害の潜在化」が起きる傾向がある。

警察では、こうした状況を踏まえ、通報・相談しやすい気運の醸成や環境整備の推進のほか、事業者等との平素からの信頼関係の醸成及び協力関係の構築による官民一体となった通報・相談の促進を行っている。例えば、サイバー事案の標的となるおそれのある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」や、企業等との共同対処協定の枠組みを活用して、サイバー事案の脅威やサイバーセキュリティに関する情報共有を行うことにより、被害に関する警察への通報・相談を促進している。また、サイバー事案等により企業に生じた損害等を補償するサイバー保険を取り扱う損害保険会社との共同対処協定の締結、セミナーの開催等を通じて、被害発生時の警察への通報・相談を促進している。

そのほか、警察庁では、サイバー事案に関する通報、相談及び情報提供の全国統一のオンライン受付窓口を警察庁ホームページに設置し、通報・相談のしやすい環境整備を進めている。

【図表 29：全国統一のオンライン通報・相談受付窓口のイメージ】



また、通報・相談といった受動的な事案認知のみならず、能動的な事案認知も重要である。警察では、サイバーパトロールや能動的解明活動等を通じた積極的な端緒情報の入手に努めている。

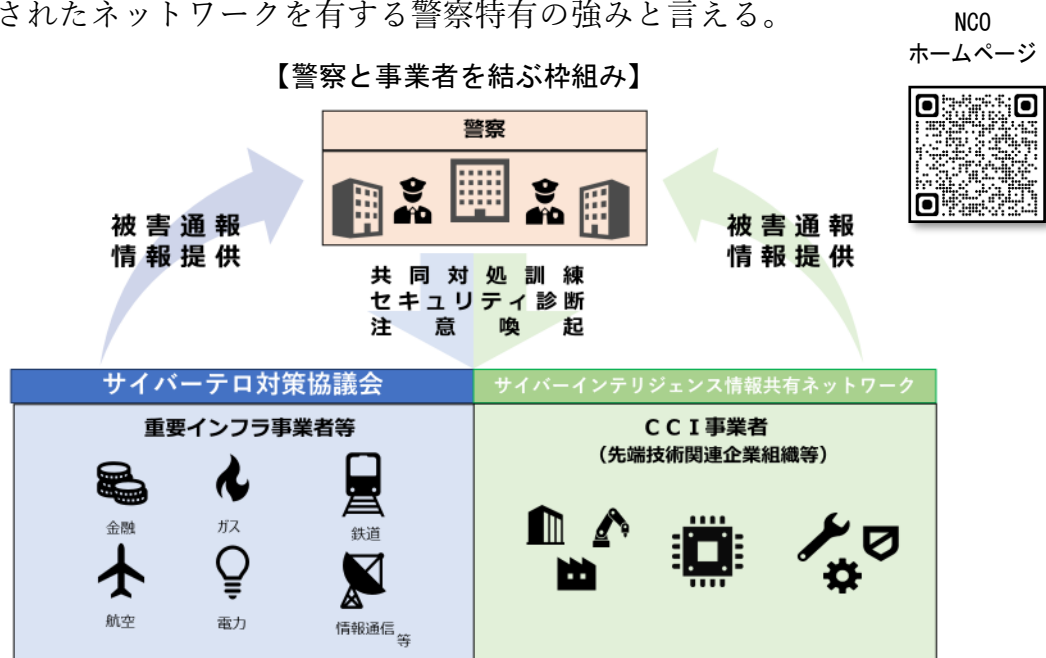
コラム：脅威ハンティングに関する警察の取組

近年、ゼロデイぜい弱性²⁸や LOTL 戦術²⁹を用いた長期間の侵入・潜伏を可能とする、巧妙化・高度化したサイバー攻撃が発生している。こうした状況の中、令和8年7月31日に開催されたサイバーセキュリティ戦略本部において、従来のセキュリティ対策では検知が困難なサイバー脅威を自発的に探索する「脅威ハンティング」の普及促進や実施等に積極的に取り組んでいく基本方針が示された。

警察においては、従来からサイバー攻撃に関する能動的な解明と脅威ハンティングを含む対策の充実に向けた取組を推進しており、サイバー攻撃被害が発生していない場合においても、全国の事業者等からの依頼に基づきセキュリティ診断を実施し、診断結果に基づく注意喚起を実施している。加えて、セキュリティ診断等の結果として得られたぜい弱性情報等を警察庁で集約・分析して、サイバー攻撃の実態解明を行っている。

また、サイバーテロ対策協議会や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、全国警察が収集したサイバー攻撃者に関する各種情報を提供するなど、サイバー攻撃対策に資する注意喚起等を実施している。

これらの枠組みは、警察の平素からの各種警察活動やあらゆる主体と連携した各種取組により構築した地域住民・事業者との良好な関係が土台となっており、全国にはりめぐらされたネットワークを有する警察特有の強みと言える。



²⁸ メーカーが把握しておらず未対処のぜい弱性。メーカーがぜい弱性を知ってから対策を講じるまでの猶予が0日しかない、という状況に由来しているとされる。

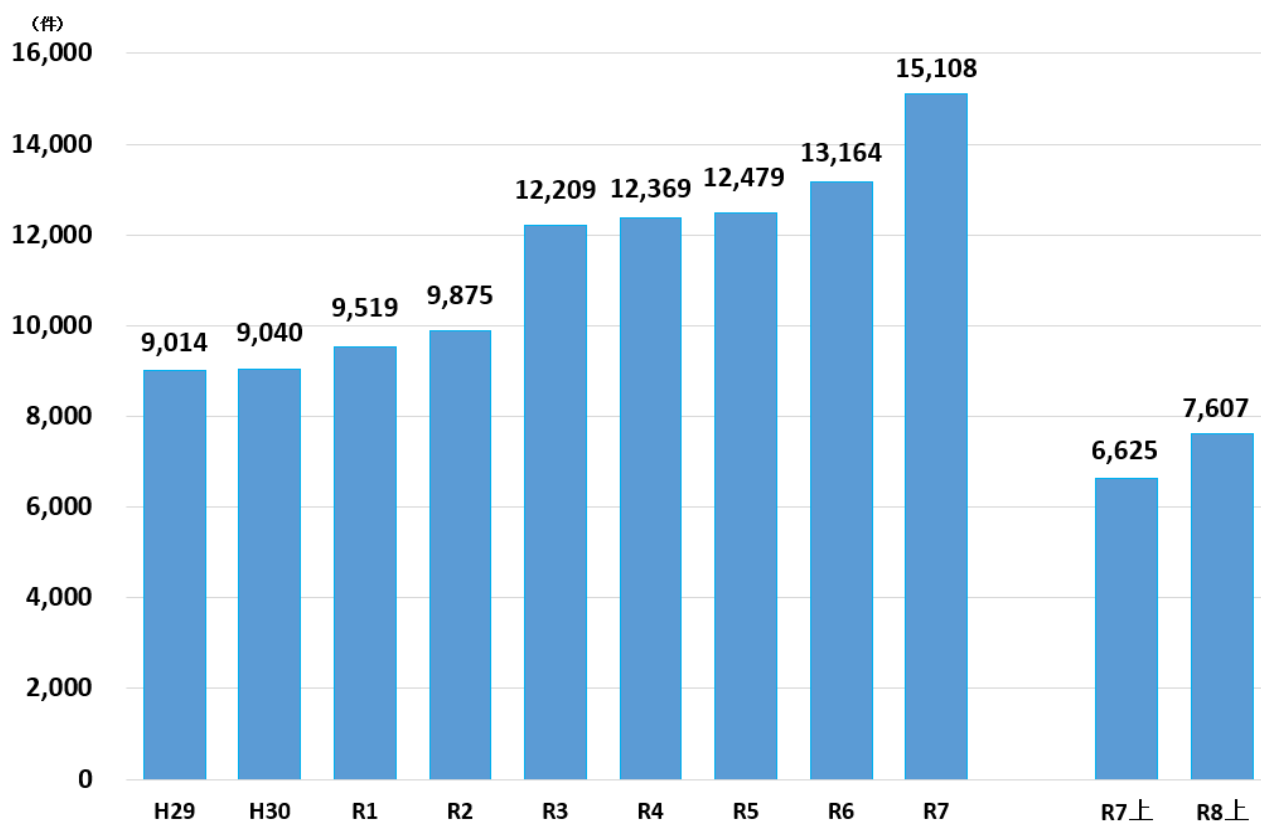
²⁹ Living Off The Land (現地調達) 戦術の略。マルウェアを用いたサイバー攻撃等と異なり、システム内に組み込まれている正規の管理ツール、コマンド、機能等を用いて、認証情報の窃取、システム情報の収集等を行うことから、検知が難しいと言われている。この攻撃手法になぞらえ、「環境寄生型攻撃」とも称される。

(2) 検挙に向けた捜査

警察庁サイバー特別捜査部・都道府県警察サイバー部門においては、重大サイバー事案のほか、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している。また、あらゆる犯罪にインターネット空間が悪用され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に対処できるよう、技術的な支援を行う体制を確保している。

この結果、令和8年上半期におけるサイバー犯罪³⁰の検挙件数は7,607件（前年同期比15%増）に達している。そのうち、犯罪収益移転防止法及び組織的犯罪処罰法違反等の犯罪収益の隠匿等に係るマネー・ローンダリング関連の犯罪の検挙件数は1,945件（前年同期比37%増）で、令和8年上半期におけるサイバー犯罪の検挙件数のうち約25.5%を占める（統計編163頁及び164頁参照）。

【図表 30：サイバー犯罪の検挙件数】



³⁰ 「サイバー犯罪」とは、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪をいう。

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、得られた情報と外国治安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。

コラム：ミキシングサービスグループの検挙

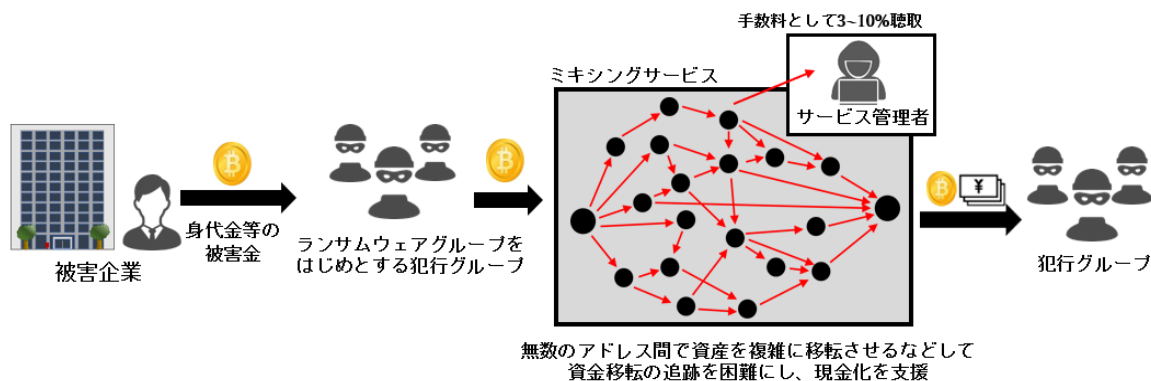
ユーロポール³¹を中心に組成された国際共同捜査であるオペレーション「Throttle（スロットル）」において、関係各国の法執行機関が連携し、ランサムウェアグループをはじめとする犯罪グループが犯罪収益の洗浄のために利用していた暗号資産のミキシングサービス「AudiA6」の管理者とみられるロシア国籍及びウクライナ国籍の被疑者2名を逮捕するとともに、被疑者グループが運営・管理するウェブサイトのテイクダウンや被疑者らの資産凍結等を行った。

このオペレーションにおいて、サイバー特別捜査部は、関係国から被疑者グループが使用していたサーバデータの提供を受け、犯行実態を明らかにするデータの復元に成功し、被疑者らが資金洗浄のために開設した暗号資産アカウントやこれを利用した資金移転状況を判明させ「AudiA6」の実態解明に貢献した。

このほか、ミキシングの際に経由した暗号資産取引所の取引に関する情報を関係各国に展開することで、各国で捜査中のランサムウェアグループの資金移転先の特定に寄与し、捜査の進展に貢献した。

また、同部においては、「AudiA6」によるミキシングの仕組みを解明し、世界で初めてデミキシングに成功している。

【国際共同捜査においてテイクダウンされたミキシングサービス】



³¹ European Union Agency for Law Enforcement Cooperation を指す。欧州連合（EU）の法執行機関であるが、捜査権限はなく、加盟国間の情報交換の促進や収集した情報の分析等が主な任務である。

② 都道府県警察サイバー警察部門

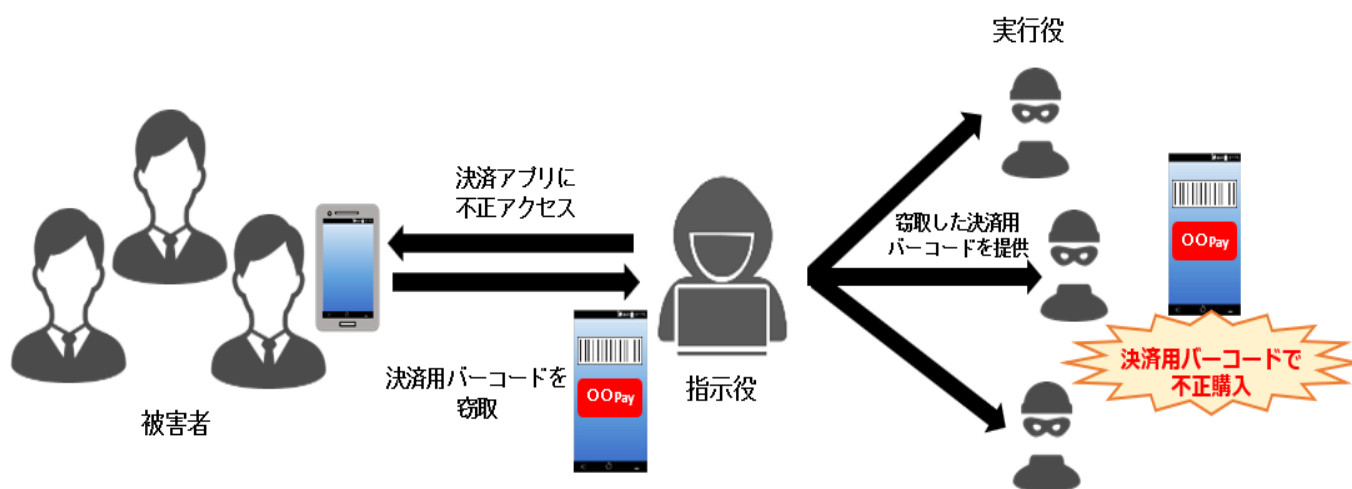
都道府県警察のサイバー部門においては、高度な専門的知識及び技術に基づき、他部門では対処困難なサイバー事案を中心に、捜査を推進している。

【CASE：中国人グループによる電子決済アプリ利用の不正アクセス等事案の検挙】

他人の電子決済サービスに不正アクセスするなどして決済用バーコードを取得し、同サービスの利用権者になりすまして家電量販店等でゲーム機等を不正購入した中国人被疑者8名を不正アクセス禁止法違反、詐欺で逮捕した（福岡・佐賀・大分・岡山・茨城・静岡6県警察合同捜査本部、山形・宮城2県合同捜査本部）。

被疑者らは、出入国を重ねたほか、全国各地において離合集散を繰り返しながら連続的に犯行に及ぶなど、実態は正に匿名・流動型犯罪グループそのものであり、捜査は難航を極めた。しかし、関係県警察が合同捜査本部を設置するなど、全国警察が一体となって捜査を展開した結果、その匿名性を打破することに成功し、被疑者の検挙に至った。また、本件では、押収証拠品の解析結果等から、被疑者側が用意した偽の決済アプリや画面共有アプリを利用した決済状況を明らかにするなど、企業側の被害防止対策を回避する新たな手口の実態を解明した。その上で、被害法人に対して、不正利用防止対策を講じるために必要な情報を提供するなど、検挙を通じた抑止にも積極的に取り組んだ。

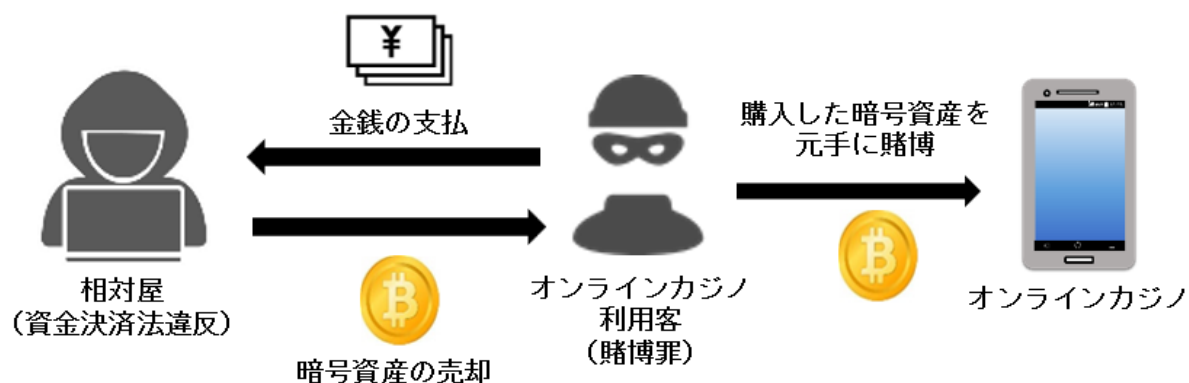
【電子決済アプリ利用の不正アクセス等事案】



コラム：オンラインカジノ利用に係る青少年らの検挙

オンラインカジノでは、暗号資産での賭博が主流であり、その暗号資産は相對屋によってインターネット上で容易に入手可能となっている。こうした状況を踏まえて、オンラインカジノ対策の一環として、SNSに対するサイバーパトロールを端緒として捜査を展開した結果、令和7年6月から令和8年1月にかけて、相對屋の運営者の大学生の男(19歳)ら4人を、オンラインカジノの利用客に対し無登録で電子マネー等を暗号資産に交換するなどしたとして、資金決済法違反で検挙した。(警視庁)

この事案では、オンラインカジノを利用していたとして、中学生の少年(13歳)を常習賭博で児童相談所に通告するなど、合計20人を常習賭博等で検挙又は児童相談所に通告している。



【資金決済法違反・賭博事件】

また、無職の男(31歳)ら2人は、令和4年11月ころから令和7年6月ころまでの間、自ら運営するウェブサイトやSNSを通じて、オンラインカジノの利用客に対して海外オンラインカジノに係る紹介等を行い、カジノサービスの利用を勧誘し、賭客が常習的に賭博をすることを幫助したほか、自らも賭博を行ったとして、令和8年1月、同男ら2人を常習賭博及び常習賭博幫助で逮捕した(千葉)。

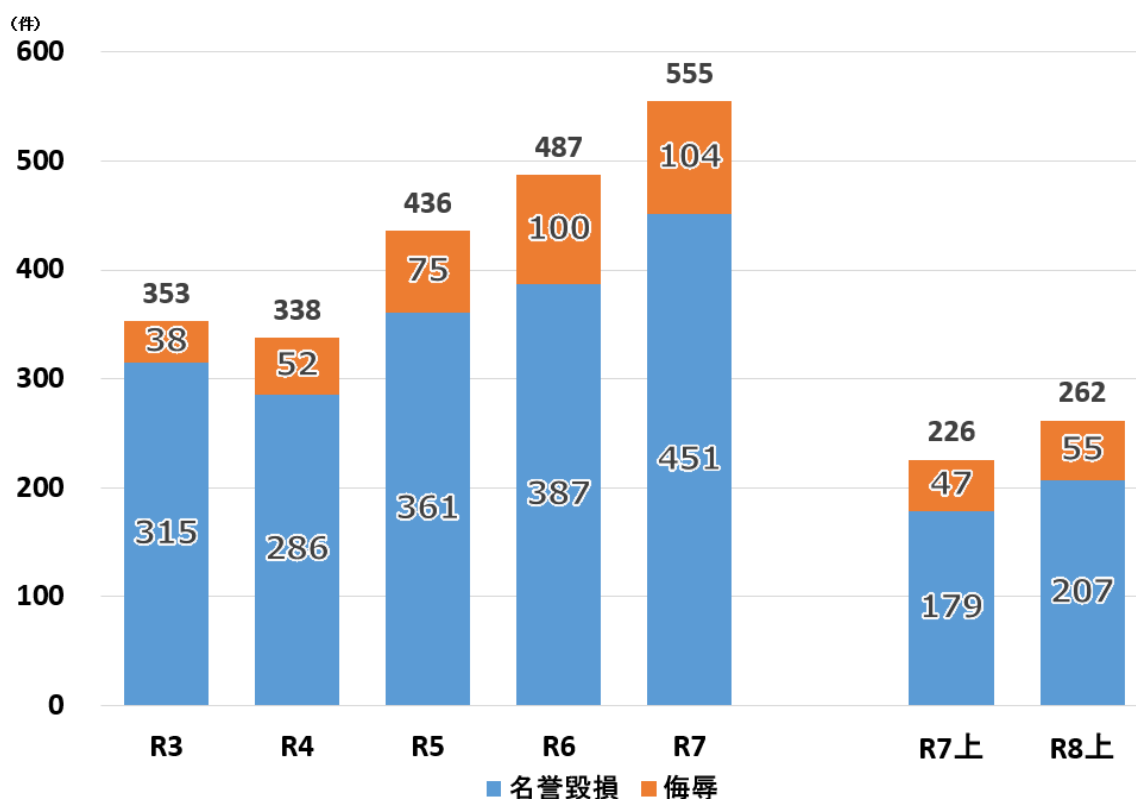
この事案では、サイト運営者の紹介行為により海外オンラインカジノで遊戯をしていた者3人を単純賭博の事実で在宅送致し、同人らの利用状況などから、ギャンブル依存症の様相が認められたことから、再発防止対策として、同人らの情報を保健所に提供した。

(3) 捜査支援

サイバー部門では、他部門が主管するサイバー事案の捜査に対しても積極的かつ主体的な支援を行い、被疑者の特定や実態解明に貢献している。

例えば、インターネット上で敢行された名誉毀損罪及び侮辱罪について、他部門に対し積極的に捜査支援を実施し、被疑者の検挙に貢献している。

【図表 31：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：盗撮目的の建造物侵入事案における分析支援】

職業不詳の男（34歳）は、盗撮等の性的目的で、令和7年11月、小学校校舎内へ侵入したとして、同年12月、同男を建造物侵入で逮捕した。

この事案では、同男がスマートフォンに保存していた、自宅で撮影した動画の撮影時間と犯行時間が重複しており、同男の犯人性の疎明が課題となっていた。そこで、警察署から支援要請を受け、サイバー部門が、スマートフォンの解析結果の精査・データ分析等の支援を行い、動画ファイル等の撮影日時の偽装工作を明らかにし、同男の犯行を裏付けた。（岩手）

また、都道府県警察のサイバー部門と全国の情報通信部に設置された情報技術解析課とのワンフロア化・ワンルーム化を推進し、サイバー部門の一体的運用を確保した上、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、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、不正プログラムの解析等の実施についての技術支援を行っている。

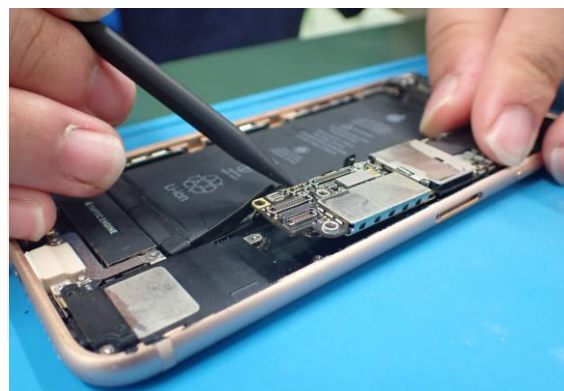
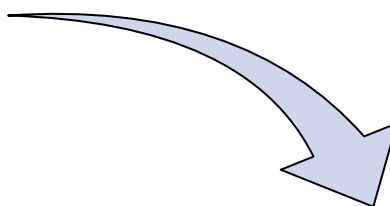
さらに、警察庁情報技術解析課に設置された高度情報技術解析センターでは、高度で専門的な知識及び技術を有する職員を配置するとともに、高度な解析用資機材を整備し、暗号により隠ぺいされたデータ、破損した電子機器等の、全国の情報技術解析課では対応が困難な解析を行っている。

【CASE：損壊したスマートフォンからのデータ抽出】

令和8年3月、警察庁高度情報技術解析センター及び近畿管区警察局兵庫県情報通信部情報技術解析課は、特殊詐欺事件に関し、原形を留めないほど粉碎し、通常の解析が実施できない状態であったスマートフォンについて、極めて高度かつ卓越した技術により当該スマートフォンの機能回復及びデータ抽出を行い、捜査の進展に大きく貢献した。



【押収品の状況】



【機能回復のための作業状況】

(イメージ)

コラム：警察捜査を支える解析の高度化

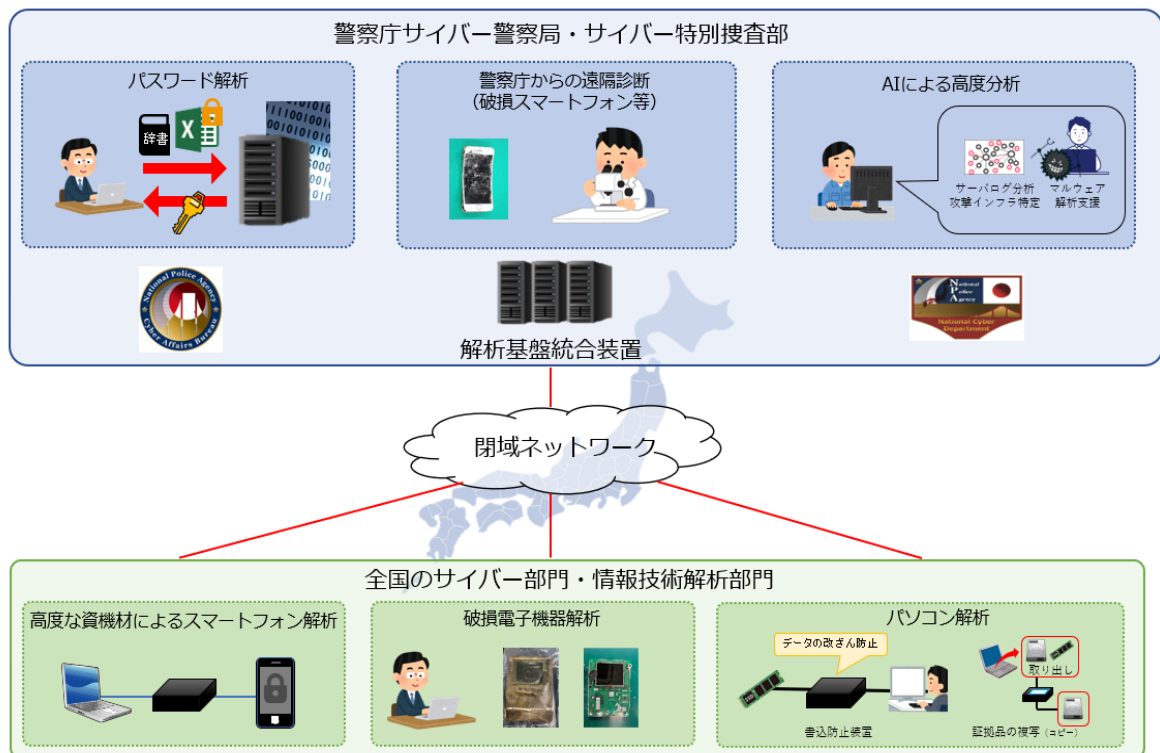
犯人は、犯行に利用していた電磁的記録に暗号化処理を施す、電子機器を破壊するなど、証拠隠滅による捜査妨害を図ることが多い。また、近年、IoT機器等の新たな電子機器やそれに関連するサービスの登場、スマートフォン等のアプリの多様化・複雑化が顕著である。

警察捜査を支えるためには、これら最新の技術に対応した解析能力の向上に取り組む必要がある。

警察庁サイバー警察局においては、解析の高度化・効率化のためのAI利活用も視野に入れた解析用資機材の整備を進めている。

また、捜査により得られた情報等を集約して俯瞰的かつ横断的な分析を行うべく、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において、AIを活用したサイバー事案に関する情報集約・分析の一層の高度化の検討を進めている。

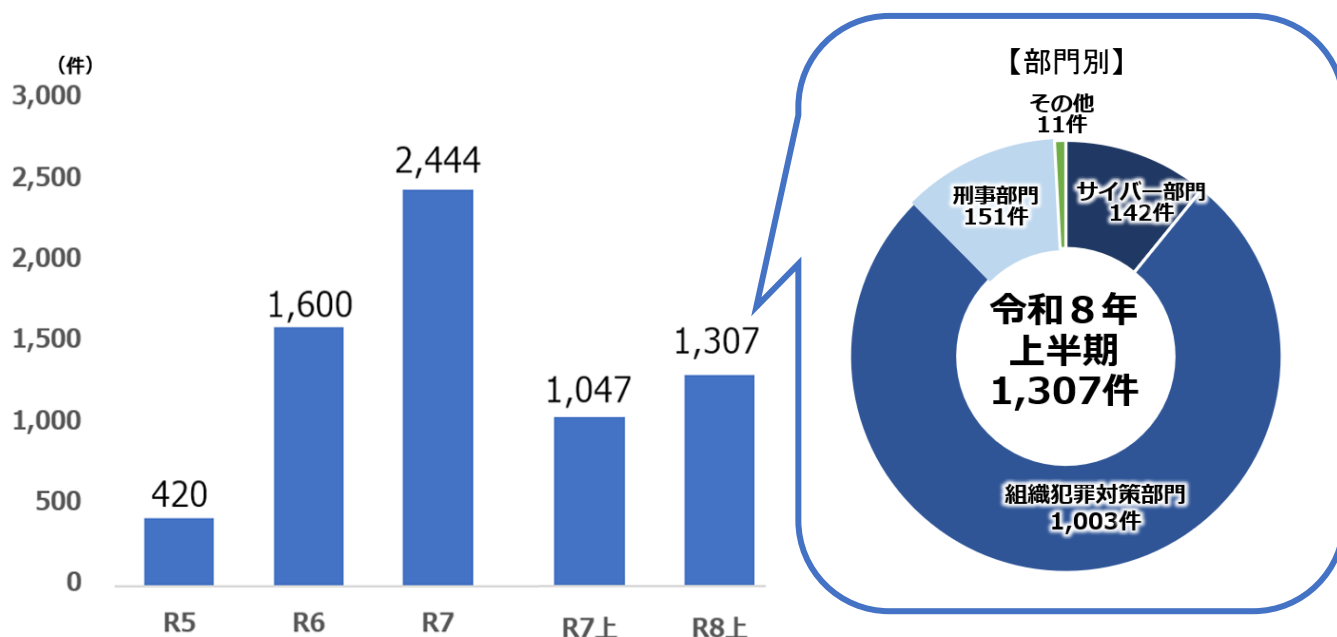
【解析基盤統合装置のイメージ】



加えて、サイバー特別捜査部では、その高度に専門的な知識・技術を駆使し、暗号資産の移転状況を追跡するとともに、追跡結果を横断的・俯瞰的に分析している。

暗号資産は罪名を問わず様々な犯罪に悪用されることから、部門を問わず、都道府県警察からの暗号資産追跡依頼に対応しており、都道府県警察の各種事案の捜査に広く貢献している。令和8年上半期における暗号資産追跡依頼件数は1,307件（前年同期比25%増）であった。

【図表 32：暗号資産追跡依頼件数】



こうした取組により、例えば、我が国で発生したSNS型投資・ロマンス詐欺事案について、関係都道府県警察の捜査情報を横断的に分析し、暗号資産追跡を実施した結果、複数の事案の被害金がナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止め、同情報をナイジェリア警察に提供したところ、令和6年5月から7月までの間に、同警察において同国内の被疑者が検挙された事例など、従来の捜査では必ずしも明らかにならなかった複数事案同士の関連性や、背景にある組織性が浮き彫りになっている（資料編 89 頁参照）。

(4) 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ことから国際連携が重要である。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。

① 国際会議への出席

警察庁サイバー警察局では、令和 8 年 6 月にフランスで開催されたサイバー犯罪条約の締約国が参加する「サイバー犯罪条約委員会会合」に参加し、各国におけるサイバー犯罪対策への取組について議論や情報共有を行うなど、国際的な連携の更なる強化を推進している。

また、情報技術解析に関する知識・経験等の共有を図るため、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平成 28 年から参加しているほか、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) に平成 17 年から加盟しており、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。

② 研修・演習への参加

ICPO 等が提供する各国の法執行機関職員を対象としたサイバー犯罪対策に関する研修に我が国の警察職員を派遣したほか、国際共同捜査に関する捜査情報の交換等を行うなど、国際捜査共助に関する連携強化も推進している。さらに、警察庁は、防衛省や NCO 等の関係省庁及び民間企業等と共に、令和 8 年 4 月、NATO サイバー防衛協力センター (CCDCOE: Cooperative Cyber Defence Centre of Excellence) が主催するサイバー防衛演習「ロックド・シールズ 2026」に参加³²した。

③ 能力構築支援

警察庁では、サイバー空間における脅威への諸外国の対処能力の向上を図るとともに、外国治安機関等との協力関係を強化することを目的として、外務省や独立行政法人国際協力機構 (JICA) と連携して外国治安機関等に対する支援を行っている。平成 26 年度からは、外国治安機関等のサイバー犯罪対策等に従事する職員を招へいし、サイバー空間における脅威への対処に関する知識・技術を習得させることなどを目的とした研修を実施しており、これまで 65 か国から合計 177 名を受け入れている。

³² 警察庁は、令和 4 年から毎年、同演習に参加しており、「ロックド・シールズ 2026」の参加で、5 回目である。

コラム：オンライン上の児童の性的搾取に対する国際共同捜査

令和8年3月から4月までの間、日本、シンガポール、タイ、韓国、香港、ブルネイ、マレーシアの7つの国・地域は、オンライン上の児童ポルノ等の性的搾取事犯に対して集中取締りを行う国際共同捜査「OPERATION CYBER GUARDIAN（オペレーション・サイバー・ガーディアン）」を実施した。期間中に合計445名を検挙し、パソコン116台、携帯電話等340台、タブレット25台、外部記録媒体140個、ルータ16台等を押収した。

日本警察においては、本オペレーション期間を「児童ポルノ撲滅に関する国際協力強化期間」と位置付け、オンライン上の児童の性的搾取等事犯の積極的な取締りを推進した結果、期間中に合計99名を児童ポルノ公然陳列・製造・所持・提供・保管、児童買春、不同意性交等で検挙した。検挙した99名の中には、団体職員や地方公務員のほか、大学生・高校生・中学生など幅広い層が含まれていた。



【被疑者を検挙している様子】

(5) サイバー警察活動における適正性の確保

平成24年に発生した遠隔操作ウイルスを使用した犯行予告事件においては、関係都道府県警察が4名を誤って逮捕した。本件誤認逮捕は、サイバー犯罪捜査に係る知識の不足等が原因であったことから、警察では、当該事件を反省・教訓とし、各種通達、全国会議における幹部指示、警察大学校における教養により、サイバー犯罪捜査における適正性の確保を徹底している。具体的には、多角的な証拠収集による被疑者の特定、供述に基づく裏付け捜査の徹底、電磁的記録の適正な取扱い及び解析・分析の徹底等を指示するなどにより、捜査幹部のみならず、全ての捜査員及び情報技術解析担当職員が適正にサイバー犯罪捜査を行うことができるよう指導・教養を徹底している。

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を推進し、検挙を通じた抑止を図るとともに、国際連携や関係機関との連携を通じた情報発信、各種犯罪インフラへの対処等による被害の未然防止・拡大防止に向けた取組を推進している。

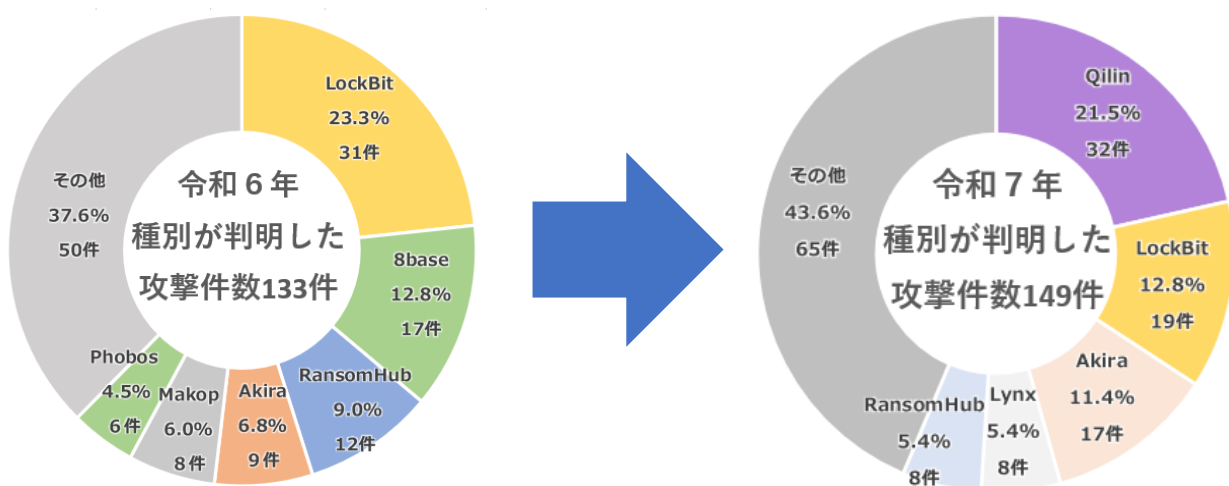
(1) 検挙による抑止

ランサムウェア攻撃等のサイバー事案に対しては、何よりも被疑者の検挙により大本を断つことが最も効果的である。

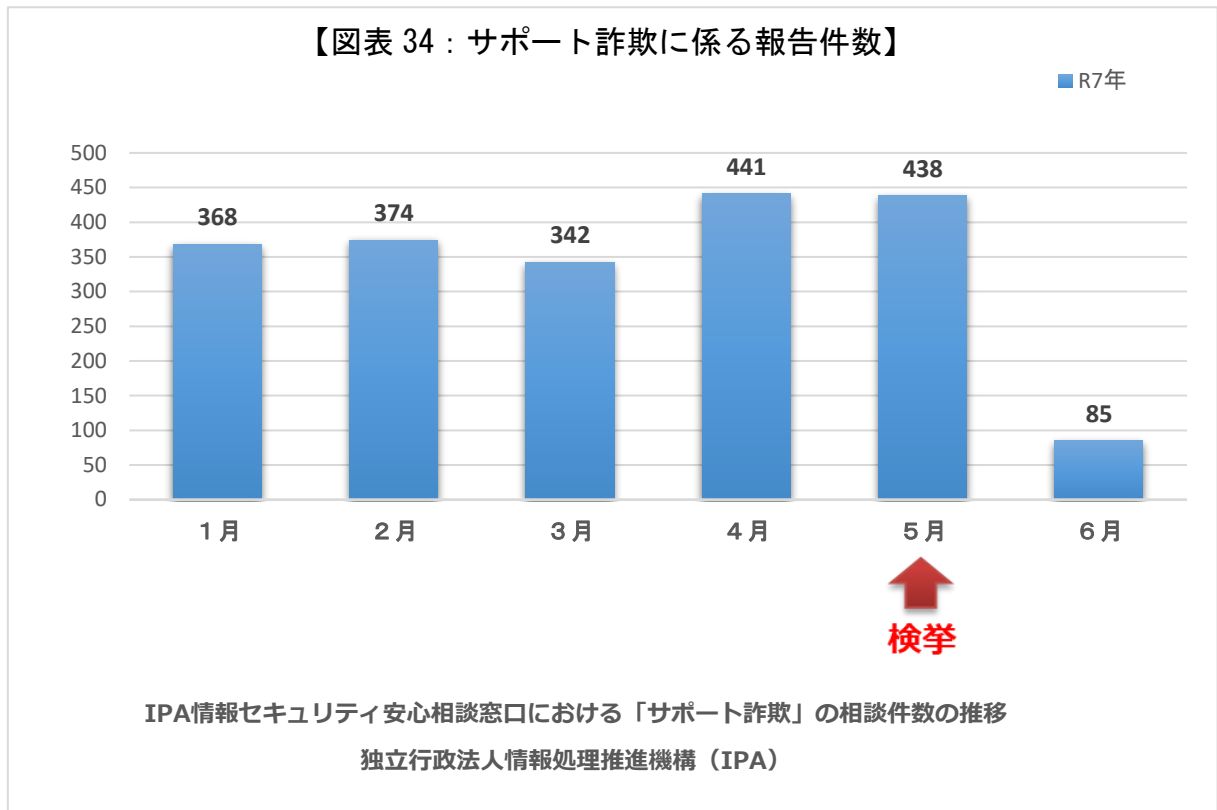
警察では、外国からのサイバー事案についても、国家を背景とした事案を含め、積極的に事件化を図り、検挙を通じた抑止を図っている。

例えば、国際共同捜査によるランサムウェアグループの検挙は、これまで判明している同種ランサムウェア被害の発生を大きく減らすなど、その効果が顕著である。ランサムウェア種別に着目すると、令和6年に多くの被害が報告されたLockBitやPhobos/8Baseは、国際共同捜査の結果、令和7年にはその件数が大きく減少（LockBit31件→19件、Phobos/8Base23件→1件）している。

【図表 33：ランサムウェア種別が判明した攻撃件数】



また、インド共和国・中央捜査局（C B I）と共に行った日本人を標的としたサポート詐欺事件の国際共同捜査では、令和7年5月、C B Iがインド共和国内に所在するインド人被疑者6人を逮捕しているが、本件検挙後の令和7年6月中にI P A（独立行政法人情報処理推進機構）に寄せられた「ウイルス検出の偽警告」に関する相談は85件（前月比80%減）であり、大幅に減少した。



(2) 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、サイバー空間における脅威の情勢を捉えたタイムリーな情報発信として広報啓発資料「サイバー警察局便り」の作成・公表等の広報・啓発に取り組んでいる（資料編 116～128 頁参照）。

コラム：少年をサイバー犯罪の被害者にも加害者にもさせないための対策

令和8年6月、千葉県警察が生成AIを悪用してランサムウェアを作成したとして会社員の男（19歳）を不正指令電磁的記録作成で逮捕した事件（本文28頁参照）において、13歳の少年が情報窃取型のマルウェアを用いて個人情報を抜き取り、「消してほしければ金を払え」などと脅したほか、同マルウェアを保管又は供用したとして、同人を含めた少年ら4名を検挙又は児童相談所に通告するなど少年がサイバー犯罪の加害者になる事案が多く見られる。

令和7年に不正アクセス禁止法違反で検挙された248人の被疑者のうち、14歳から19歳までの者が81人(32.7%)であった。

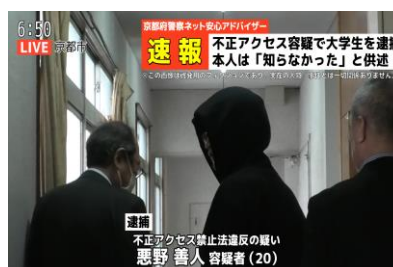
千葉県警察では、本件の被疑少年及び保護者に対して、産学官が連携してサイバーに関する正しい知識やIT知識を活かしたキャリアパスなどを教養し、被疑者の立ち直りを促す取組である「サイバー立ち直り支援」を行い、同支援にはサイバー防犯ボランティアや日本サイバー犯罪対策センター（JC3）等が参加した。

また、警察庁では、サイバー防犯ボランティアの拡大や活動の活性化を目的に、毎年応募テーマを決め、サイバー防犯ボランティア広報啓発コンテストを開催している。令和7年度は初めて「サイバー攻撃者にさせない取組」部門で広報啓発動画を募集し、全国のサイバー防犯ボランティアから多くの応募を受けた。審査の結果、埼玉県警察サイバー防犯ボランティア東京国際大学及び京都府警察ネット安心アドバイザーの作品を優秀作品として表彰を行い、令和8年3月から警察庁公式YouTubeにおいて公開している。

これらに加えて、関係機関・団体と連携した広報啓発活動を推進しているほか、ユーロポールを中心とした、各国法執行機関によるサイバー加害者対策に係る情報共有の枠組みであるInterCOP³³に参加し、他の参加国と積極的に情報共有をするなど、サイバー犯罪の被害者にも加害者にもさせないための対策に取り組んでいる。



【埼玉県警察サイバー学生ボランティア東京国際大学の作品】



【京都府警察ネット安心アドバイザーの作品】



³³ International Cyber Offender Prevention（国際サイバー犯罪者対策）の略

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、攻撃者及び手口に関する実態解明を進め、未然防止対策等に関する注意喚起を実施している。例えば、令和7年1月、警察庁及び NISC³⁴は、MirrorFace³⁵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いたことを確認し、これらサイバー攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動であると評価した上で、同グループによるサイバー攻撃の手口や未然防止対策等に関する注意喚起を実施した。

また、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³⁶を実施している。例えば、令和7年8月、警察庁及び国家サイバー統括室（NCO）は、米国を始めとする12か国の関係機関と共に、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に加わり、パブリック・アトリビューションとして、本件アドバイザリーを公表した。警察では、サイバーテロ対策協議会やサイバーインテリジェンス情報共有ネットワークを活用し、Salt Typhoon の手口や侵害情報、対応策について事業者に周知し、注意喚起を行っている。

そのほか、令和8年上半期、警察庁は、各種二国間・多国間サイバー協議に出席し、同盟国・同志国等との情報・運用面での協力の強化、悪意あるサイバー活動の抑止に向けた国際的な取組への積極的な参画等を推進している。

【図表 35：サイバー分野における他国との協議】

日時	場所	会議名
令和8年1月	ベルギー	第7回日・EUサイバー対話
令和8年2月	東京	第9回日英サイバー対話
令和8年6月	東京	第7回日豪サイバー政策協議
令和8年6月	米国	第5回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会
令和8年7月	米国	第11回日米サイバー対話
令和8年7月	東京	第2回日・リトアニアサイバー協議

³⁴ National center of Incident readiness and Strategy for Cybersecurity（内閣サイバーセキュリティセンター）の略。令和7年7月に、同センターを改組し、内閣官房に「国家サイバー統括室（NCO）」が設置された。

³⁵ 「MirrorFace」という名称は、スロバキアの民間企業が名付けたものである。MirrorFace が攻撃に使用した独自開発のマルウェアを当該民間企業が「MirrorStealer」と名付けたことに由来するとされている。

³⁶ パブリック・アトリビューション（public attribution）とは、政府機関等がサイバー攻撃者の国等の帰属を特定（アトリビューション：attribution）し、公（パブリック：public）にすることを意味する。

コラム：北朝鮮 IT 労働者に関する注意喚起

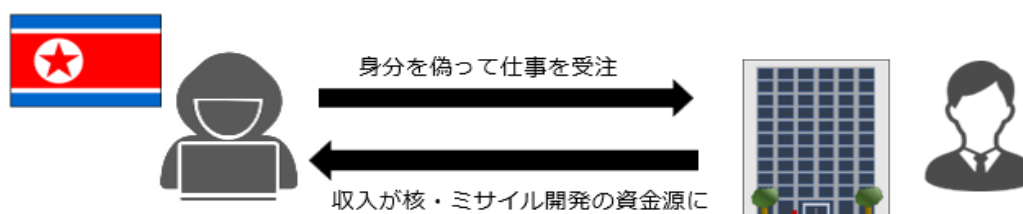
我が国においては、北朝鮮 IT 労働者が日本人になりすまして、日本企業等が提供する業務受発注のためのオンラインプラットフォームを利用して、業務を受注するなどし、収入を得ている事例が確認されている。

こうした北朝鮮 IT 労働者による活動に対しては、これまでも、警察庁等が「北朝鮮 IT 労働者に関する企業等に対する注意喚起」を発出しているほか、日米韓 3 か国でも取組を進めてきた。その一方で、北朝鮮 IT 労働者は手口を一層巧妙化させ、民間企業のシステム侵害も行い、その標的は欧州諸国を含め、世界規模に拡大していることを踏まえ、令和 8 年 7 月、警察庁、国家サイバー統括室、外務省、財務省及び経済産業省は、米国及び韓国を始めとする同盟国・同志国の関係機関とともに、「北朝鮮 IT 労働者に関する各国・企業等に対する注意喚起」を公表した。



本注意喚起において各国の機関は、北朝鮮が IT 労働者を外国に派遣していること、同労働者は身分を偽って仕事を受注することで収入を得ていること、その収入が北朝鮮の核・ミサイル開発の資金源になっていること等を指摘している。

また、各国の企業に対して北朝鮮 IT 労働者の手口に対抗するため、本人確認手続の強化（身分証明書の厳格な審査、対面面接の義務等）や不審なアカウントの探知（異常な情報の登録が通知されるシステムの導入等）といった対策を引き続き強化するように求めるとともに、第三者の代理人を利用して採用面接に参加したり、実際の所在地を隠蔽する目的で、海外の第三者の代理人を利用してラップトップファーム³⁷を運営したりするといった北朝鮮 IT 労働者の手口についても注意喚起している。



³⁷ 支給されたノートパソコン等を海外の第三者宅に設置し、遠隔でアクセスすることによって、実際の所在地を隠蔽すること。北朝鮮 IT 労働者の多くは、中国、ロシア、東南アジア等に在住しているとされているが、VPN やリモートデスクトップ等を用いて外国から作業を行っていることを秘匿している場合がある。

② 関係機関との連携を通じた情報発信

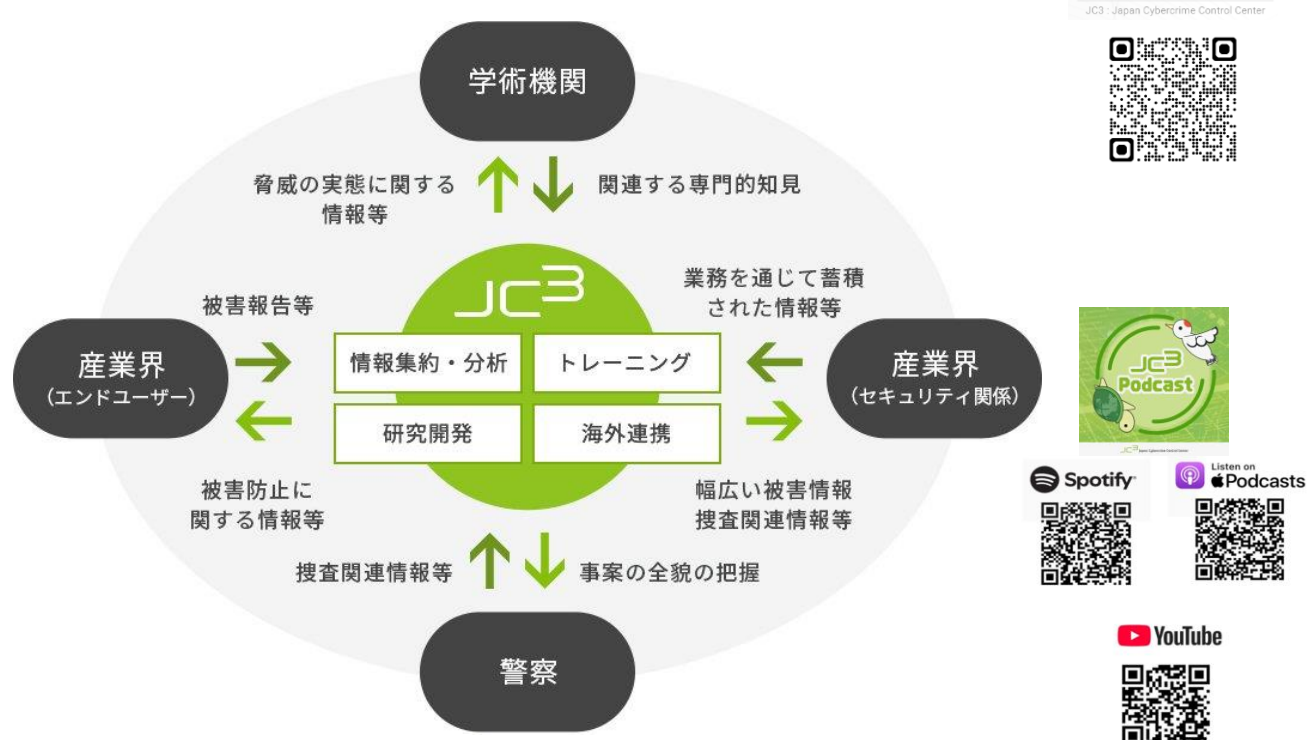
○ J C 3 を軸とした産学官連携

警察では、国民一人一人の自主的な対策を推進し、サイバー犯罪の被害を防止するため様々な関係機関・団体と連携した情報発信を行っており、特に一般財団法人日本サイバー犯罪対策センター（J C 3 : Japan Cybercrime Control Center）との連携を推進している。

J C 3 は、米国で産学官連携の枠組みとして成果を上げている非営利組織である NCFTA(National Cyber-Forensics & Training Alliance)を参考とした新たな組織を構築する必要性が、平成 25 年 12 月に閣議決定された「『世界一安全な日本』創造戦略」等において指摘されたことを踏まえ、日本版 NCFTA として産学官の情報や知見を集約・分析し、その結果等を還元することにより、国民が安全かつ安心してインターネットを利用できる環境の構築に貢献することを目的として設立され、平成 26 年 11 月に業務を開始した組織である。

警察では、J C 3 に対しサイバー犯罪の被害実態、犯行手口等を共有し、セキュリティベンダー、金融機関等の会員企業の対策に反映し、J C 3 からは会員企業における被害状況や対策の実施状況の共有を受け、警察における捜査や被害防止活動に活用している。

【図表 36：日本サイバー犯罪対策センター（J C 3）】



○ 民間団体等との連携

各都道府県警察においては、金融機関、暗号資産交換業者、医療機関、商工会議所、サイバー保険を取り扱う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。

また、警察庁においては、ランサムウェア等のサイバー事案の未然防止及び発生時における被害拡大防止のため、VPN 機器等のぜい弱性対策や認証情報の適切な管理、バックアップやログの適切な取得、サイバー攻撃を想定した業務継続計画（BCP: Business Continuity Plan）の策定、被害発生時における速やかな警察への通報・相談等について、特に被害が増加傾向にある中小企業を主な対象としつつ、幅広く周知・啓発に取り組んでいる。

さらに、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 8,800 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」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 8 年 9 月には第 20 回アジア競技大会、同年 10 月には第 5 回アジアパラ競技大会が開催されることから、主な開催地を管轄する愛知県警察は、大会組織委員会との標的型メール訓練や重要インフラ事業者等とのサイバー攻撃への対処を想定した共同対処訓練を実施するとともに、関係事業者等からの依頼に基づくセキュリティ診断を実施し、診断結果に基づく注意喚起を実施している。

○ 関係省庁との連携

警察庁では、関係省庁と連携した業界団体及び事業者等への周知を行っているほか、内閣府政府広報室と共にランサムウェア対策を紹介する広報啓発動画を制作し、令和 8 年 3 月には広報啓発資料「サイバー警察局便り」を作成した上で、警察庁ウェブサイト等で公開するなど、幅広く注意喚起に取り組んでいる。

コラム：サイバー特別捜査部によるデータの復号

令和8年1月に発生した某県所在の飲料メーカーに係るランサムウェアによるサイバー攻撃では、サーバ上の多数の業務上のデータが暗号化されていた。サイバー特別捜査部が被害データを分析したところ、ランサムウェア LockBit により暗号化されたものと判明した。

そこで、同部が開発したデータ復号ツールを用いてデータの復号を試みたところ、計1テラバイトを超えるファイルの復号に成功した。復号できたデータを、管轄の県警察本部から被害法人に返却したところ、「復旧できなかった場合は、当社業務に計り知れない影響がありました。それだけに復旧できた直後の担当者はとても喜んでいました。ありがとうございました。」との連絡が寄せられた。

【被害企業の声】



調査会社に依頼しても復号できる保証はなく、費用も掛かるので大変助かった



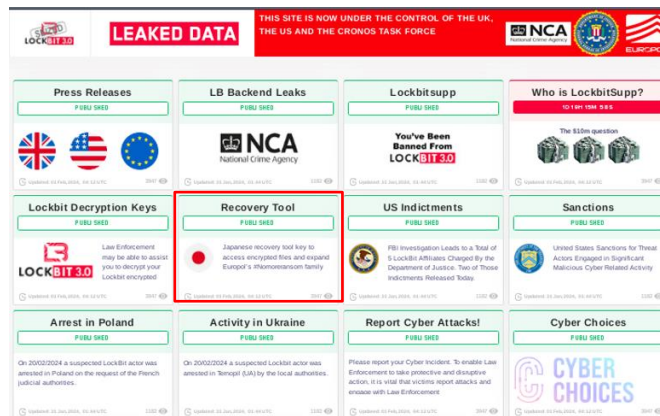
実際に復号することができて感謝している



被害時、すぐに警察に届け出て、サーバ情報等も提供したが、この様な復号ソフトの開発に役立つんだと考えると大切なことだと感じた

このように、警察では、被疑者の検挙に向けた捜査のほか、被害組織の状況に応じて、初動対応に対する助言や復号ツールの提供等の支援を行うことが可能であるので、仮にランサムウェアの被害に遭った際には、早期に警察や関係機関に通報・相談するように呼びかけている。

上記のサイバー特別捜査部では LockBit に対応したものをはじめ複数のデータ復号ツールを開発しており、それらが活用された例として、これまでに日本国内において、41 の被害企業で約 2,011 万件の被害データの復号に成功している。



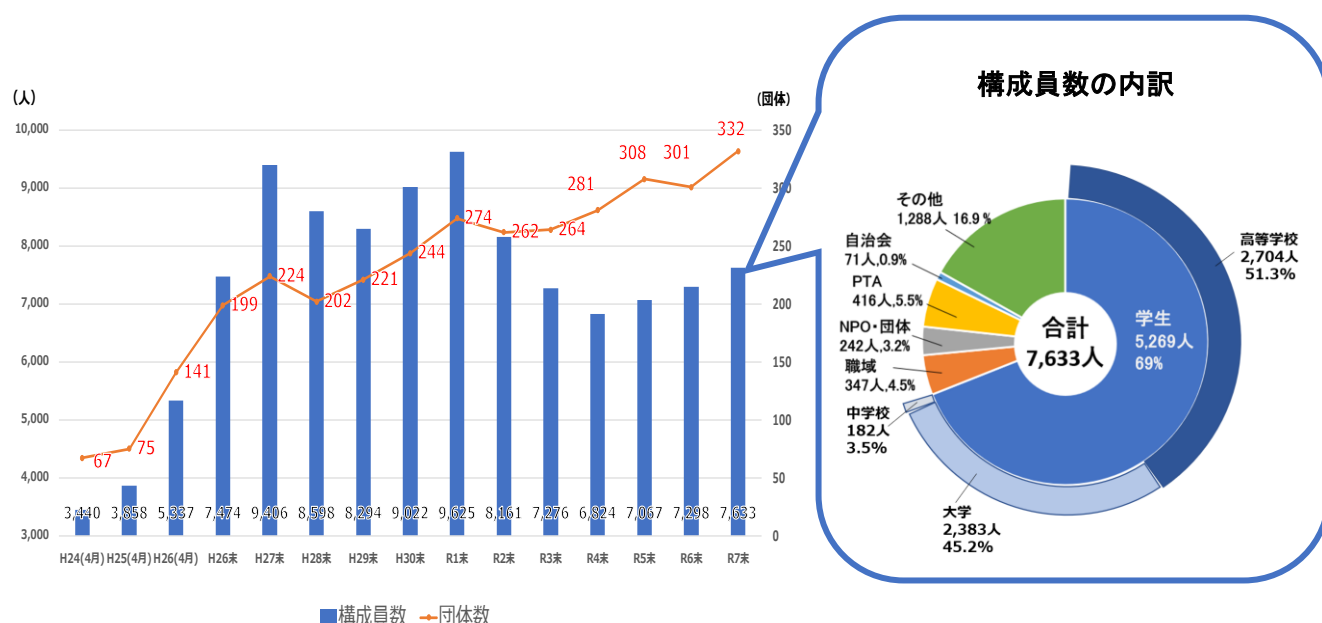
出典：https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

なお、暗号化されたデータを復号するための対価と称して、ランサムウェア攻撃グループから要求される金銭等を支払うことに関し、警察としては、「犯罪グループ等の活動資金となることが懸念される」「暗号化されたデータの復号が保証されるわけではない」旨を被害者に対して説明している。

③ サイバー防犯ボランティアとの連携を通じた情報発信

サイバー防犯ボランティアは、「自分たちの利用するインターネットの安全は自分たちで守る。」というコンセプトの下、安全で安心して利用できるインターネット空間を作るための自主的な防犯活動のことを言う。平成 22 年度総合セキュリティ対策会議の下に設置された「サイバーボランティア育成分科会」では、サイバーボランティアの支援・育成について議論を行い、「サイバー空間の規範意識の低下への対策として、サイバー防犯ボランティアの活動の重要性を国民に訴え、結成を促進し、官民連携により育成する気運を醸成する。」ことの必要性を認識するに至った。これを踏まえ、平成 22 年度総合セキュリティ対策会議においてサイバー防犯ボランティアの活動要領、サイバー防犯ボランティアの育成の在り方、サイバー防犯ボランティアの組織化について提言がなされた。平成 24 年当時は全国で 67 団体、3,440 人で構成されていたサイバー防犯ボランティアは、その後、地域に根ざした主体として着実な発展を遂げ、令和 7 年 12 月末現在、全国で 332 団体、7,633 人が、活動を行っている。サイバー防犯ボランティアの構成員の内訳として、学生の比率が高くなっており、若い世代が中心となった防犯活動が活性化している（統計編 169 頁参照）。

【図表 37：サイバー防犯ボランティアの構成員数・団体数】



サイバー防犯ボランティアは、「被害防止のための教育活動」、「広報啓発活動」、「サイバー空間の浄化活動」(サイバーパトロール)を柱とする活動を行っており、警察ではその活動の拡大・活性化に向けた支援を行っている。例えば、警察庁においては、活動状況等の視察や全国のサイバー防犯ボランティア等を対象とした意見交換の実施、サイバー事案に関する広報啓発動画のコンテストを開催し、優秀作品を作成した団体への表彰を行うなどの支援を行っている。

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

コラム：「サイバーテスト」を活用した若者向けの教育活動

埼玉県警察では、児童や生徒のサイバーセキュリティに関する学習の理解度を測るための確認テスト「サイバーテスト」を作成し、主に学生を対象とした独自のサイバーセキュリティ教育を実施している。

本テストは、JC3や民間企業等と連携し、ネットリテラシー、オンラインゲーム、クレジットカード犯罪等、発達段階に応じた各種テーマを設定して作成している。

また、本テストを活用した若者向けのサイバーセキュリティキャンペーンをサイバー防犯ボランティアと連携して実施するなど、サイバー犯罪の被害者にも加害者にもさせないための取組を推進している。

【サイバーテスト「ネットリテラシー」】

めあて ● インターネットを使うための正しい知識を身につける。

埼玉県警察サイバー局

年 組 番

名前

点

※ネットリテラシーとは・・・インターネットを安全に正しく使うための知識や能力のことです。

1 フェイクニュースに関する問題です。フェイクニュースについて、☐ 内から正しいものを選び、☐ で囲みましょう。(1問10点・30点)

SNSの書き込み

フェイクニュースとは、
【正しい情報・嘘や間違った情報・個人情報】のこと。

フェイクニュースを投稿した人は、
【健康になれる・アプリのポイントが増える・逮捕される】ことがある。

フェイクニュースを投稿すると、
【人の命に関わる・呪われる・携帯のデータが消える】ことがあるので、絶対にしてはいけません。

2 犯罪者に家の場所を知られてしまった経過を順番に並びかえましょう。(1問5点・全問正解30点)

④ 学校に犯罪者が来る
⑤ 家を突き止められる
③ 犯罪者が随でついてくる
⑥ 写真をSNSに投稿

3 インターネットのトラブルに関する問題です。☐ の状況が起こった場合、考えられるトラブルを ☐ から選び、随でつなぎましょう。同じ ☐ を選んでも構いません。(1問5点・20点)

動物をいじめている動画をSNSに投稿した。

みんなと相談して、嫌いな友達をグループチャットで無視をした。

IDとパスワードを他人に知られてしまった。

友達の名前をSNSで投稿した。

不正アクセス

ネットいじめ

ネット炎上

4 次の説明文を読み、正しいものには○、間違っているものには×をつけましょう。(1問5点・20点)

① フェイクニュースを拡散(広めること)した人も、投稿した人を助けたことになるので、犯罪になることがある。()

② 友達から「2人で写っている写真をSNSで投稿していい?」と聞かれたが、自分の顔や学校の制服が写っていたので、断った。()

③ パスワードは、覚えるのも大変で忘れるともっと大変なので、いつも同じパスワードを使っている。()

④ インターネットのトラブルは、自分の問題なので、保護者や先生に知られないようにして、自分で解決しなければならない。()

(3) 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。また、犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働き掛け等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐことが重要である。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

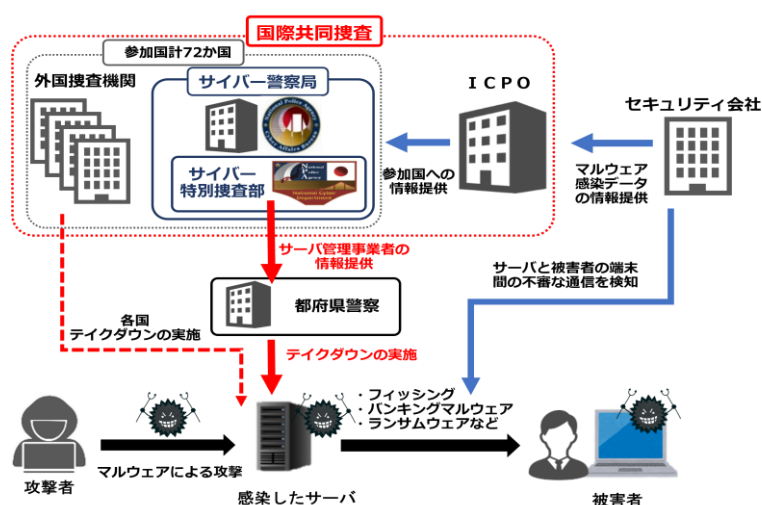
警察では、サイバー攻撃事案で使用された不正プログラムの解析等を通じて、国内における C2 (Command & Control) サーバ³⁸やマルウェアに感染して不正に機能している国内のサーバを把握し、当該サーバの不正な機能を停止するよう、サーバを管理する事業者等に依頼するなどして、犯罪インフラ対策を継続的に実施するなどしている。

コラム：国際共同捜査によるサーバのテイクダウン

令和7年10月から同年12月にかけて、国際刑事警察機構 (ICPO) 主導の下、フィッシング、バンキングマルウェア、ランサムウェアといったマルウェア対策を目的とした大規模な国際共同捜査のオペレーション「Synergia (シナジア) III」が実施された。

この取組には日本警察を含む72か国の捜査機関が参加し、マルウェアと結びついた約45,000台のサーバ等がテイクダウンされた。

サイバー特別捜査部は、ICPO から日本国内に所在するとみられるフィッシングやバンキングマルウェアに関する情報 (IPアドレス等) 45件を一元的に受領し、テイクダウン対象のサーバを管理する事業者を特定するとともに、関係する警視庁、石川県警察、京都府警察、大阪府警察への取組支援を行った。これら4都府県警察は、サーバを管理する事業者に対しマルウェア感染の疑いを伝え、テイクダウン措置を働きかけた結果、対象事業者によって現在までに24台のサーバがテイクダウンされ、さらなる被害拡大の防止に貢献した。



³⁸ 攻撃者が侵害したシステムと通信し、指揮 (Command)・統制 (Control) する目的で用いられるサーバ。

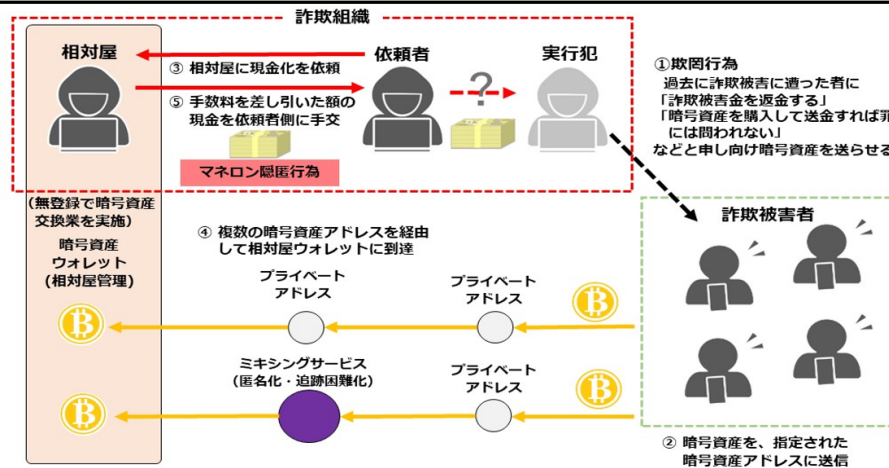
② インターネット空間を悪用した犯罪に関するインフラへの対処

○ 検挙を通じた犯罪インフラの解体

匿名・流動型犯罪グループには、中核的人物の下に構築されたいわゆる「^{あいたいや}相対屋」、「道具屋」といった違法なビジネスによって資金を得ている者がおり、警察では、これら犯罪集団を検挙することで、犯罪インフラを解体している。

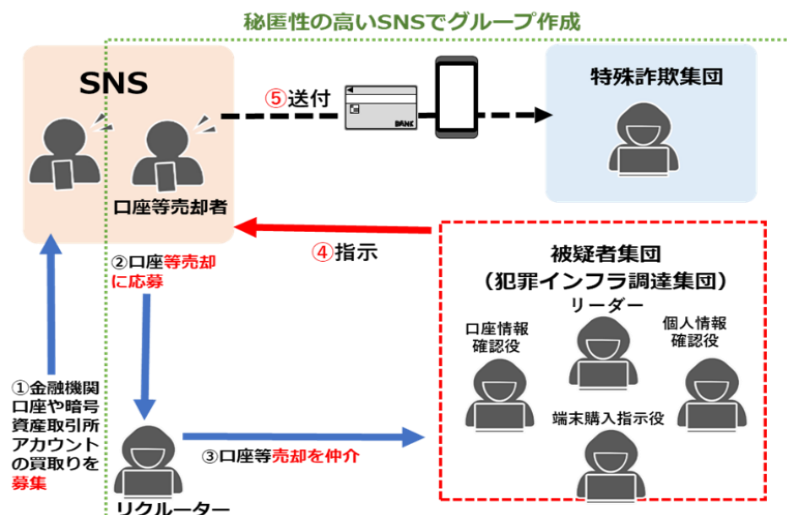
【図表 38 : 「^{あいたいや}相対屋」の検挙】

- 匿名・流動型犯罪グループは、暗号資産を資金洗浄に悪用。無登録で暗号資産を現金化する「相対屋」が暗躍。
- サイバー特捜部において、被害金に係る暗号資産を追跡。犯罪インフラとなっている「相対屋」を検挙。



【図表 39 : 「道具屋」の検挙】

- 匿名・流動型犯罪グループは、他人名義の金融機関口座等を犯罪に悪用。不正に調達し販売する「道具屋」が暗躍。
- サイバー特捜部において、全国警察から集約された情報を分析。犯罪インフラとなっている「道具屋」を検挙。

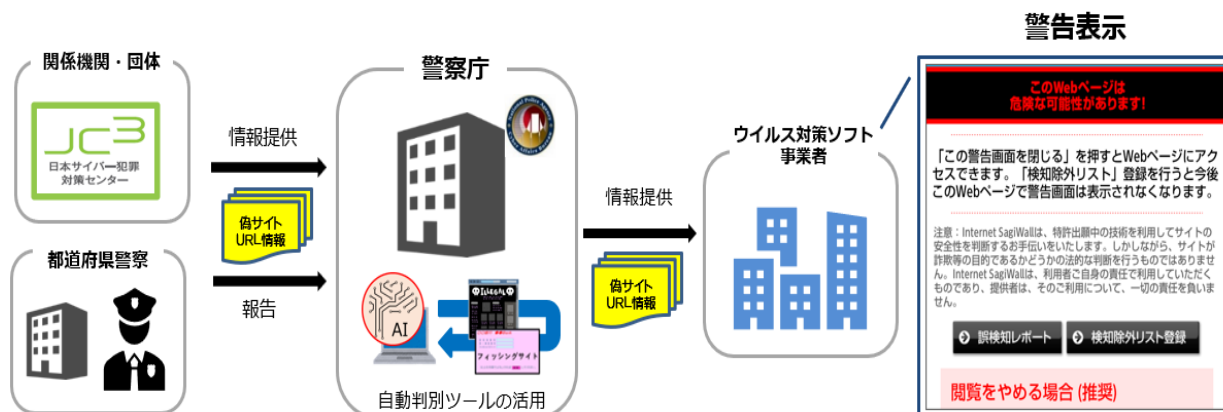


○ 偽サイト・フィッシングサイト対策

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（J C 3）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・判定し、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、令和 8 年 2 月に生成 A I による自動判別ツールを導入し、フィッシングサイト判定の高度化・効率化を図っている。

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

【図表 40：ウェブサイト対策のイメージ】



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（DMARC³⁹）への対応促進」、「フィッシングサイトの閉鎖促進」、「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、あらゆる機会を通じて、事業者等に対する働き掛けを行っている

官民が連携したフィッシングサイト対策として、J C 3 では、専門的な知識を持たない人であってもプラットフォーム事業者等に対してサイトのテイクダウン依頼を行うことができるツールを開発し、サイバー防犯ボランティア等に提供するとともに、警察庁後援のもと、サイバー防犯ボランティア向けの「フィッシングサイト撲滅チャレンジカップ」を実施している。

³⁹ Domain-based Message Authentication Reporting, and Conformance の略。

○ インターネットバンキング不正送金対策

警察庁は、令和 8 年 5 月から遠隔操作ツールを利用するボイスフィッシングによる法人口座の不正送金被害が急増する深刻な事態を受け、金融庁、一般社団法人全国銀行協会等と連名で、広報啓発資料「サイバー警察局便り」を新たに作成して、警察庁ウェブサイトや SNS 等にて公開し、一連の手口の詳細や企業が講じるべき対策に関する注意喚起を実施した。

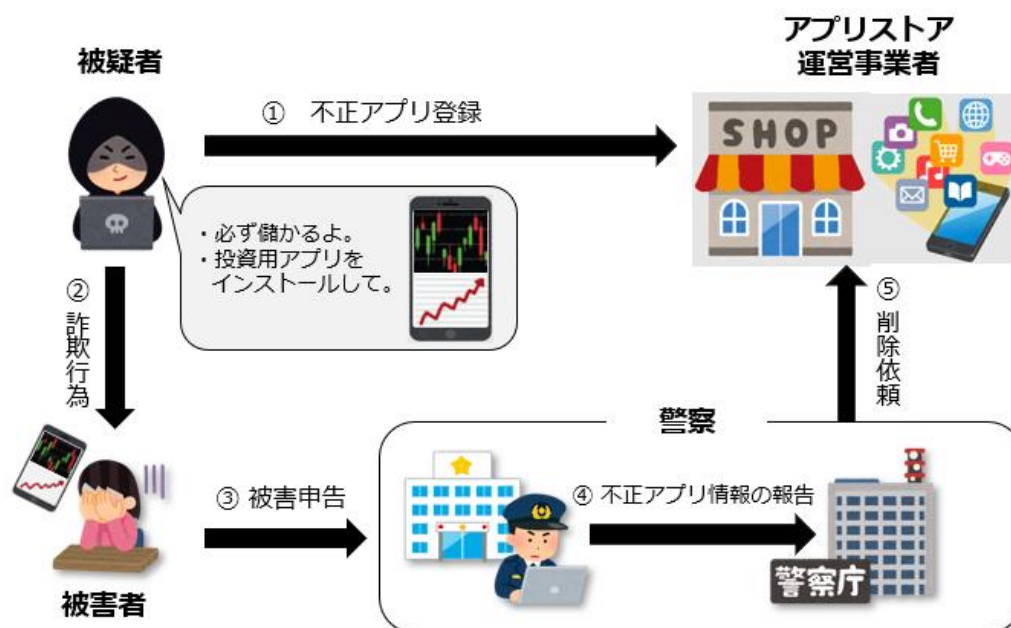
○ クレジットカード不正利用対策

都道府県警察において把握した、悪用されたクレジットカード番号情報を警察庁で集約し、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、一括して提供する枠組みを構築し、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講ずることにより被害防止を推進している。

○ 特殊詐欺に係る SNS アカウント・不正アプリ対策

SNS 事業者等に対し、警察が把握した特殊詐欺の犯行に利用されたアカウントの利用停止や削除等を促すための情報提供を行っており、令和 8 年上半期は、7,500 件を超える情報提供を実施した。また、特殊詐欺においては、SNS で接触をした後に、不正なアプリを用いて被害を拡大させている実態があることから、令和 8 年 3 月、新たにアプリストア運営事業者に対し、犯行に利用された不正なアプリの削除を促すための情報提供を行う仕組みの運用を開始した。

【図表 41：不正アプリ対策のイメージ】



コラム：ECサイトにおける不正取引対策

ECサイト⁴⁰におけるクレジットカードの不正利用等の不正取引が後を絶たないことから、EC加盟店等と警察が連携した被害防止への取組が課題であった。

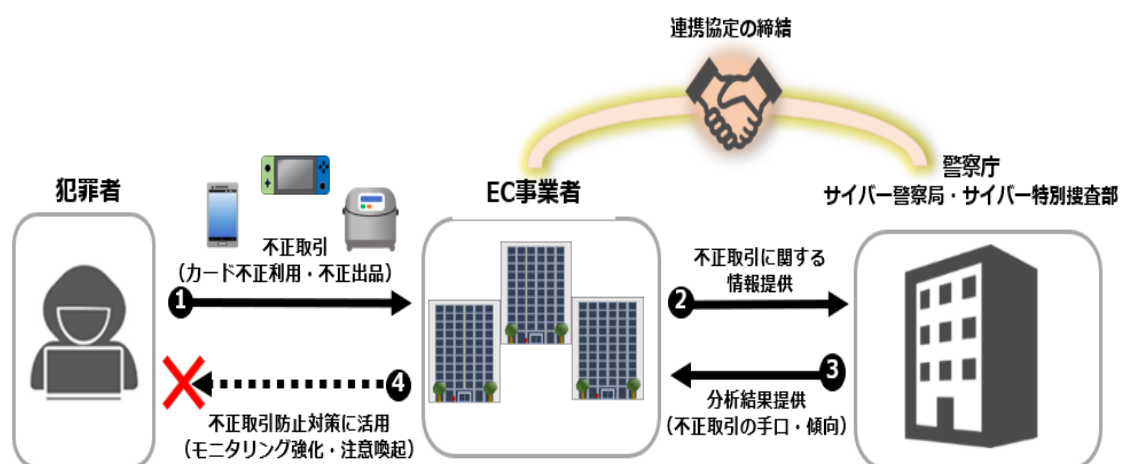
令和6年3月、警察庁の有識者会議が取りまとめた「キャッシュレス社会の安全・安心の確保に関する検討会報告書」において、「EC加盟店等との情報連携の強化」が盛り込まれ、令和7年4月、政府の犯罪対策閣僚会議で決定された「国民を詐欺から守るための総合対策 2.0」においても「EC加盟店等との情報連携」が盛り込まれた。

EC事業者から警察への提供に関して、個人情報保護委員会と調整した結果、令和7年6月、EC事業者が不正取引に関する個人情報を一定の場合に警察に提供することができる旨『『個人情報の保護に関する法律についてのガイドライン』に関するQ&A』に追加された。

これらを踏まえ、令和8年7月、国内大手EC事業者3社と不正取引防止等を目的とした情報連携に関する協定を締結した。

EC事業者から警察庁に提供された複数の不正取引に関する情報をサイバー特別捜査部において横断的・俯瞰的に分析して捜査に活用するとともに、分析により判明した被害防止を講じるために有益な情報をEC事業者に還元することで、EC事業者において効果的な被害防止対策を講じることを可能とするものである。

【EC事業者との情報連携】



⁴⁰ インターネット上で商品やサービスを売買するウェブサイトのこと。「EC」は、Electronic Commerce（エレクトロニック・コマース/電子商取引）の略。

コラム：家庭用 I o T 機器を悪用したサイバー攻撃への官民一体となった対策

警察庁では、総務省、国立研究開発法人情報通信研究機構（NICT）等と連携し、レジデンシャルプロキシに係る不正な I o T 機器のセキュリティ対策を推進するための検討を進め、令和 8 年 7 月 21 日、レジデンシャルプロキシの悪用実態や対策を取りまとめた「家庭用 I o T 機器を悪用するレジデンシャルプロキシの現状」を公開するとともに、社会全体での対策の推進のため、多岐に渡る主体が連携して対応を協議する「レジデンシャルプロキシ対策アライアンス」を設立した。

○ 「家庭用 I o T 機器を悪用するレジデンシャルプロキシの現状」

レジデンシャルプロキシがサイバー事案において悪用されている実態のほか、家庭用 I o T 機器がレジデンシャルプロキシとなる仕組み、悪用されるリスクを軽減するために利用者自身が取り得る対策例等を取りまとめた。

○ 「レジデンシャルプロキシ対策アライアンス」

警察庁及び総務省が事務局となり、家庭用 I o T 機器の利用者に対するレジデンシャルプロキシの実態等の周知広報方策や業界団体、電気通信事業者、セキュリティ事業者等の関係者が連携した対処の方針、必要な環境整備について協議することを目的として、設立した。

令和 8 年 9 月 7 日に第 1 回会合を開催し、レジデンシャルプロキシの実態の整理、関係者の実施事項等について意見交換を行った。

レジデンシャルプロキシ対策アライアンス

【参加機関】

政府関係機関等	警察庁 総務省 国立研究開発法人情報通信研究機構（NICT）
業界団体	一般社団法人 ICT-ISAC 一般財団法人 日本サイバー犯罪対策センター（JC3）
電気通信事業者	NTTドコモビジネス株式会社 KDDI株式会社 JCOM株式会社 ソフトバンク株式会社
セキュリティ製品・サービス	日本サイバーセキュリティ産業振興コミュニティ

警察庁
ホームページ



※今後、メンバーの追加・変更があり得る。

このほか、警察においては、捜査で把握したレジデンシャルプロキシ化させるアプリについて、当該アプリケーションの配信を行っていた事業者に対し、当該アプリケーションが不正アクセス行為に悪用されている実態について情報提供を行い、被害拡大防止のための対応を要請した結果、当該アプリケーションの配信が停止されるなど、捜査情報を活用した対策を行っているほか、広報啓発資料「サイバー警察局便り」による注意喚起を行った。

コラム：A I をめぐる警察の取組

令和7年5月には、A I のイノベーションを促進しつつ、リスクに対応するため、A I 法⁴¹が成立し、同年12月には、A I 基本計画⁴²が閣議決定され、政府が総合的かつ計画的に講ずべき施策が示されるとともに、A I の研究開発・活用の適正性を確保するためのA I 指針⁴³が決定された。A I をめぐる情勢は日々刻々と変化していることを踏まえ、令和8年7月に、改定されたA I 基本計画が閣議決定され、改めて、政府が総合的かつ計画的に講ずべき施策が示された。

警察では、犯罪実行者募集情報の収集にA I を活用しているほか、匿名・流動型犯罪グループやローン・オフエンダーの対策にA I を活用すべく現在取組を推進している。他方、A I を悪用して、不正プログラムを作成した事案等もあることから、A I 基本計画においては、警察活動の高度化のためのA I 利活用やA I を悪用する犯罪等への対処について記載されている。警察では、これらの政府決定文書を踏まえ、各種施策を推進することとしている（資料編109頁及び110頁参照）。

また、A I をめぐる脅威の情勢と警察の取組を紹介し、警鐘を鳴らすために広報啓発活動にも力を入れている。

令和8年5月、「社会安全フォーラム」を主催し、A I をめぐる脅威の情勢を踏まえつつ、A I を悪用した犯罪に対処する警察の取組を紹介した。その上で、A I の利活用についても取り組まなければならない課題であると訴えかけた。

同フォーラムでは、A I を悪用した犯罪の実態を踏まえつつ、安全・安心なA I 社会の実現に向けて、法規制、官民連携及び教育・啓発（A I リテラシー）の観点からどのような対応が必要かについて、有識者が議論した。



出典：警察政策研究センター

⁴¹人工知能関連技術の開発及び活用の推進に関する法律（令和7年法律第53号）

⁴²人工知能基本計画（令和7年12月23日閣議決定）

⁴³人工知能関連技術の研究開発及び活用の適正性確保に関する指針（令和7年12月19日人工知能戦略本部決定）

コラム：データ通信専用SIM契約時の本人確認の義務化

データ通信専用SIM⁴⁴は、携帯電話不正利用防止法上、契約時の本人確認が義務化されておらず、近年、本人確認書類やIDとパスワードを使い、不正契約するなどの悪用事案が数多く発生している。

【データ通信専用SIMの不正契約に係る主な検挙事例】

- SMS機能付きデータ通信専用SIMを悪用したSMS認証代行⁴⁵の検挙
サイバーパトロールにより把握したインターネット上でSMS認証代行の依頼者を募集する者を捜査し、令和4年3月から6月、SMS認証代行者及び依頼者（7名）を検挙した。（京都府）
- 不正アクセス行為によるeSIMの不正取得の検挙
SNSで結びついた中高生の少年3人が、不正に取得した他人のIDとパスワードを使い、電気通信事業者が管理するサーバコンピュータに不正アクセスした上で、eSIMを不正に取得したとして、令和7年1月から同年2月にかけて、同少年らを不正アクセス禁止法違反及び電子計算機使用詐欺罪等で逮捕した。（警視庁）

このような悪用事例が後を絶たないことから、警察庁から総務省に対して、データ通信専用SIMが詐欺等の犯罪に悪用されている実態について情報提供を行ったほか、「国民を詐欺から守るための総合対策2.0」（令和7年4月22日犯罪対策閣僚会議決定）においても、「データ通信専用SIMの契約時における本人確認の義務付け」を含めた検討が盛り込まれた。

これらを踏まえ、政府においては、本人確認の対象にデータ通信専用SIMを追加し、データ通信専用SIMの契約時における本人確認を義務化する内容を盛り込んだ携帯電話不正利用防止法の改正案を国会に提出し、令和8年5月、同改正法が成立・公布⁴⁶された。

【データ通信専用SIM本人確認の義務化】



⁴⁴Subscriber Identity Module の略。契約者の識別番号や電話番号、メールアドレス等の情報を記録するICカード。

⁴⁵ ポイントの不正取得やフリマサイトにおける不正出品などに利用するアカウントを不正に取得するために、SMS認証を代行する手口。認証代行者は、通信事業者とSMS機能付きデータ通信契約を行い、当該契約に係る電話番号や認証コードを依頼者に提供する。

⁴⁶ 改正法は、一部を除き、公布の日から起算して一年を超えない範囲内において政令で定める日から施行。

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。

○ インターネット・ホットラインセンターにおける取組

警察庁では、インターネット利用者等から違法・有害情報に関する通報を受け、警察への通報、サイト管理者等への削除依頼等を行うインターネット・ホットラインセンター（IHC）を事業委託するとともに、違法情報、重要犯罪密接関連情報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。

【図表 42：インターネット・ホットラインセンターの仕組み】



【図表 43：インターネット・ホットラインセンターの削除依頼対象】

インターネットの安全と安心のために

インターネット・ホットラインセンターは、皆様からインターネット上の違法情報や自殺誘引等情報、重要犯罪密接関連情報の通報を受け、ガイドラインに基づいて警察に情報提供するとともに、サイト管理者等に送信防止措置を依頼します。



今すぐホットラインへ 通報する

通報結果を見る >

なりすまし型偽投資広告

**犯罪実行者の募集
(闇バイト、送金犯罪)**

違法オンラインギャンブル

通帳や携帯電話の売買

薬物・ドラッグ

**無登録貸金業者による
広告（ヤミ金）**

わいせつ

児童ポルノ

出会い系・売春

フィッシング

**鉄砲所持、爆発物製造、
殺人等の請負等**

**自殺関連、その他の
違法情報**

コラム：なりすまし型偽投資広告及び送金犯罪に係る取組

令和7年中のSNS型投資詐欺の認知件数は9,523件、被害総額は約1,288億円と危機的な状況であった。これらSNS型投資詐欺について、被害者が犯人側と接触した手口としてはバナー等広告が最も多く、著名人になりすました偽の投資広告を入口としてSNSでのやりとりに誘導され、被害者がSNSでやりとりを重ねる中で、投資名目で現金等を詐取されているケースが多く見られる。

こうした深刻な被害状況を背景に、「詐欺及びストーカー被害拡大防止のための緊急対策」（令和8年7月28日犯罪対策閣僚会議決定）等において、なりすまし型偽広告の削除を大手プラットフォームに促す取組の加速や、なりすまし型偽広告等への対策の更なる強化が掲げられた。

また、近年、新たなマネー・ローンダリングの手口として、SNS等を通じた他人からの依頼を受けて自身の預貯金口座等を利用した財産の移転等を有償で行う行為（「送金犯罪」⁴⁷）が増加していることを踏まえ、令和8年6月、犯罪収益移転防止法の一部を改正する法律が成立し、「送金犯罪」に関する罰則の創設等が行われた。

同法において、上記依頼行為等が違法とされたことに伴い、「なりすまし型偽投資広告を掲載する行為」と併せて、同年8月7日、IHCの運用ガイドラインの対象範囲とした。

このように、プラットフォーム事業者等にこれら情報の削除を促すため、総務省違法情報ガイドラインの改定に併せてIHCの運用ガイドラインを改定し、社会問題となっている情報を新たに違法情報として取扱範囲に追加することにより、これら情報の流通防止に向けた取組を強化している。

令和8年8月7日からIHCでは
なりすまし型偽投資広告を掲載する行為
及び
「送金犯罪」の依頼又は誘引行為
を「違法情報」として通報を受け付けています。

※ 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

⚠ 次のような情報は、違法情報に該当し得るものとして、IHCへの通報対象となります。

なりすまし型偽投資広告を掲載する行為

● こんにちは、〇〇です。
100万→1億円
利益100倍！！

● 私の無料投資グループで、
急騰銘柄を提供！
★毎月10%以上のリターン

● ここをクリック
〇〇のグループに参加

● 著名人等になりすまして
当該著名人等の名義を無断で使用した

○ 投資実績を表示する広告

○ 投資セミナーに勧誘する広告

等

「送金犯罪」の依頼又は誘引行為

● ★誘引行為の例

● 副業紹介します！

【内容】
送金アプリや銀行口座に振り込まれた
お金を指定の口座に振り込むだけ！

【報酬】
送金する際、送金分の5%を報酬とし
て差し引いてください。

①「依頼行為」
・特定の者に対して、送金の依頼等をする
よう働きかけること

②「誘引行為」
・送金する者を募集する等、自らの意思を
間接的に表示して誘いかけ、相手方となる
者の申込みを待つこと

※「送金犯罪」の詳細については、警察庁ホームページを参照

警察庁
National Police Agency

インターネット・
ホットラインセンター
Internet Hotline Center

<https://www.internethotline.jp>

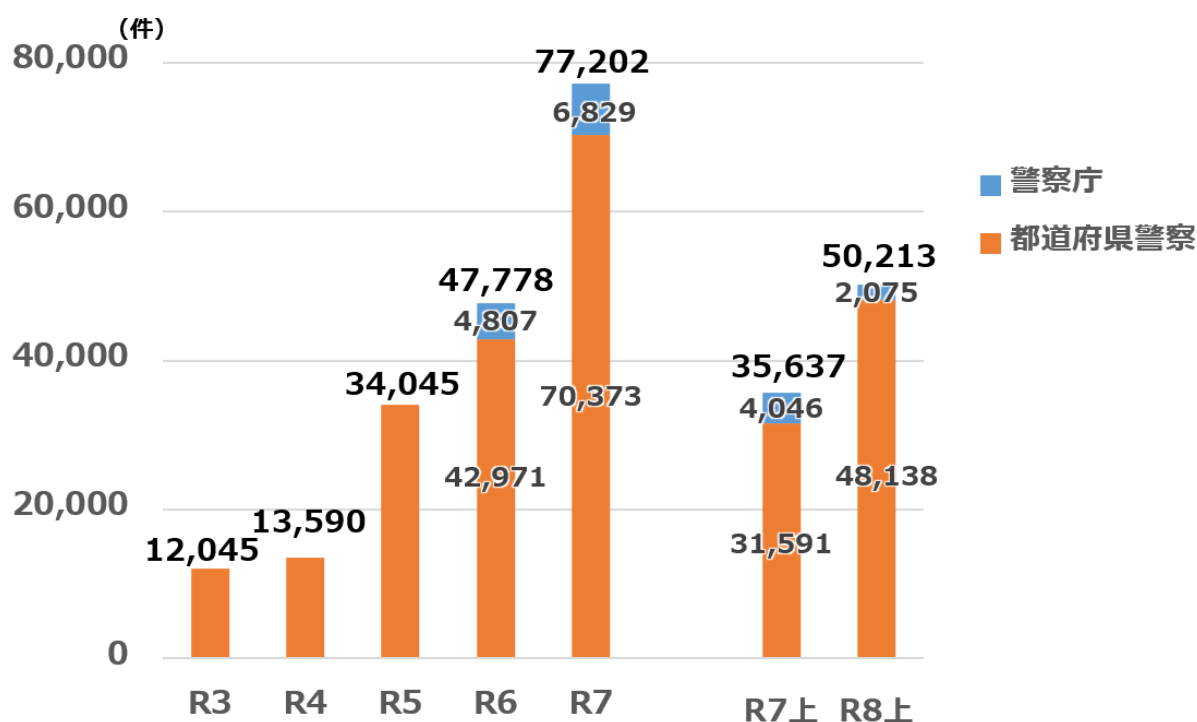
⁴⁷ 「送金犯罪」は、「送金バイト」等と表記されることもある。（「送金バイト」という表現には、犯罪への気軽な参画を容易にするという指摘もあるため、警察ではこのような犯罪を「送金犯罪」と呼称している。）

○ 警察における取組

警察庁では、インターネット・ホットラインセンターの取組について周知を図るとともに、違法・有害情報の削除の実効性を確保するため、プロバイダ事業者等に対して、違法・有害情報に関する削除への協力を依頼している。

また、警察庁ではその所掌事務の、都道府県警察では警察の責務の、それぞれ範囲内において、SNS上の犯罪実行者を募集する投稿に対するリプライ（返信）機能を使った個別警告を実施している。令和8年上半期は5万213件（前年同期比41%増）の個別警告を行った。

【図表 44：犯罪実行者募集情報に対する個別警告（リプライ）件数】



加えて、特定のテロ組織等と関わりのないままに過激化した個人、いわゆるローン・オフエンダーへの対策として、インターネット上の銃砲や爆発物の製造方法等に関する情報の発見に努め、それらの情報についてサイト管理者等への削除依頼等を行っている。

そのほか、「国民を詐欺から守るための総合対策 2.0」（令和7年4月22日犯罪対策閣僚会議決定）に基づき、関係機関・団体・民間事業者等の協力を得ながら、引き続き各種施策を推進している（資料編 111 頁参照）。

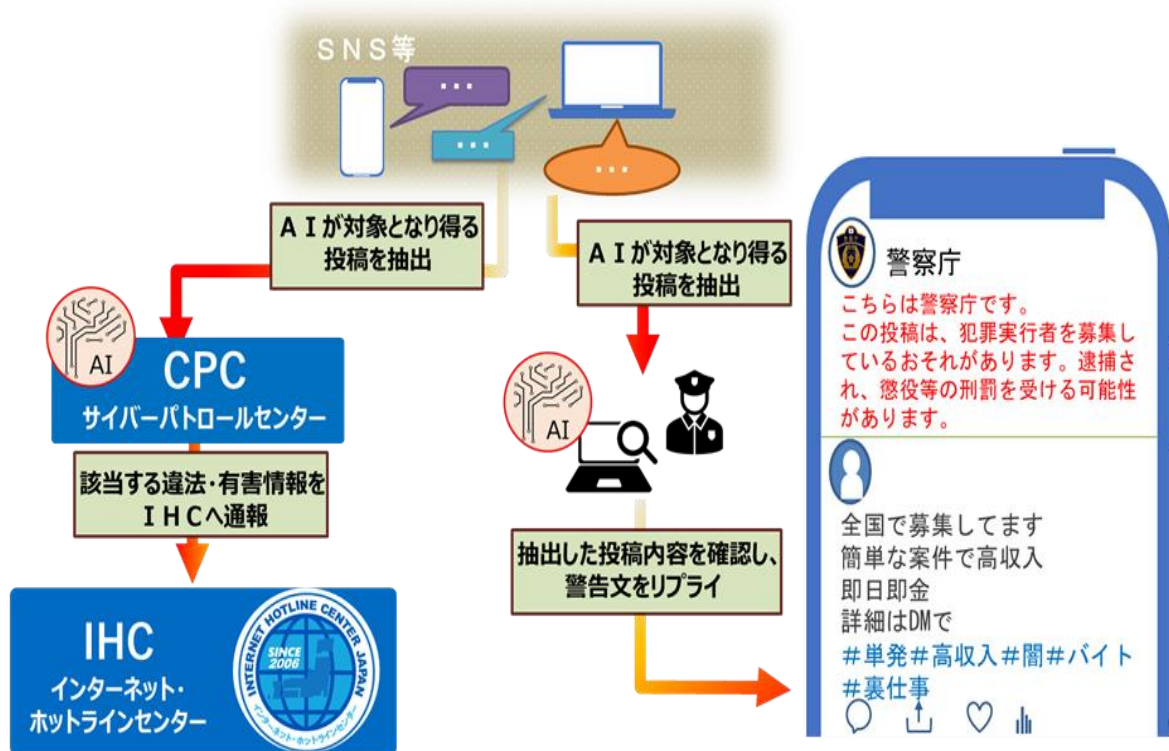
コラム：A I を活用した犯罪実行者募集情報の収集

警察庁では、令和3年度にA Iを活用してS N Sにおける規制薬物に関する情報等の探索・分析を行う実証実験を実施した。具体的には、規制薬物の広告等に関するS N S上の投稿をA Iに学習させることで、S N S上の投稿の中から、規制薬物の広告等に関するものをA Iにより効率的に抽出する仕組みを構築した。

同実証実験の結果、規制薬物の広告等に関するS N S上の投稿を高い精度で抽出できることが確認できたことから、抽出する対象情報の範囲の拡充について検討を行い、令和6年2月、A Iを活用してS N S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た。さらに、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（A Iリプライ）等を実施しており、令和8年上半期中、警察庁は、犯罪実行者の募集情報に対し、2,075件の個別警告を実施した。

また、警察庁が業務委託しているサイバーパトロールセンター（CPC）では、S N S上の情報の探索・分析を効率化するため、違法情報や重要犯罪密接関連情報を自動収集してその該当性を判定するA I検索システムを導入し、サイバーパトロールの高度化を図っている。

【A I を活用した犯罪実行者募集情報の収集のイメージ】



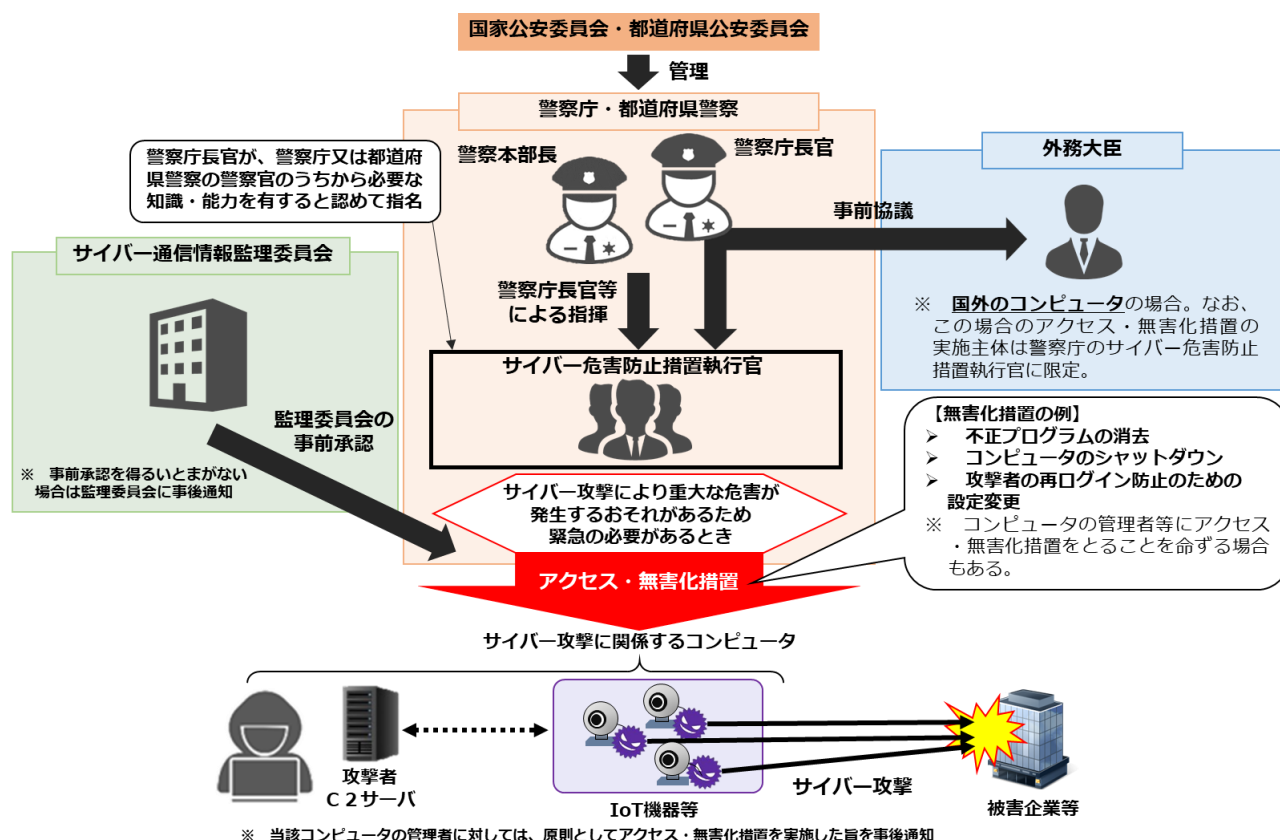
(4) アクセス・無害化措置

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

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

令和7年5月、第217回国会において、サイバー対処能力強化法⁴⁸（及び同整備法⁴⁹）が成立した。強化法及び整備法は、「官民連携の強化」、「通信情報の利用」及び「攻撃者のサーバ等へのアクセス・無害化措置」を取組の柱としている。

【図表 45：改正警察官職務執行法】



⁴⁸ 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和7年法律第42号）

⁴⁹ 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和7年法律第43号）

令和7年12月、サイバー対処能力強化法に基づく各般の施策を適切に機能させ、これらの施策に係る事務の適正な実施を確保するための基本的事項を定めた「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」が閣議決定された。

警察関係では、整備法により、警察官職務執行法の一部が改正され、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新たに設けられた。

同規定は、令和8年10月1日に施行される予定であるが、アクセス・無害化措置は、警察に新たに課せられた重要な任務であり、当該措置の対象となるサイバー攻撃は、公共の安全と秩序の維持を責務とする警察が対処を行うこととなる。他方、こうしたサイバー攻撃の中には国家安全保障に関わる事案が含まれ得るほか、自衛隊が有する特別の技術又は情報が必要不可欠である事案もあり、こうした事案においては警察が自衛隊と共同して対処することとなる。これらを踏まえると、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となってシームレスな対応を行うことにより、サイバー攻撃による被害の防止を図る必要がある。アクセス・無害化措置は、今後サイバー特別捜査部を中心に実施していくこととなるが、それには高い専門性や技術が必要になることから、その確実な実施に向けた更なる態勢の整備が必要になる。

【図表 46：政府における三位一体によるシームレスな対処】



3 基盤整備に向けた取組

(1) 体制の整備

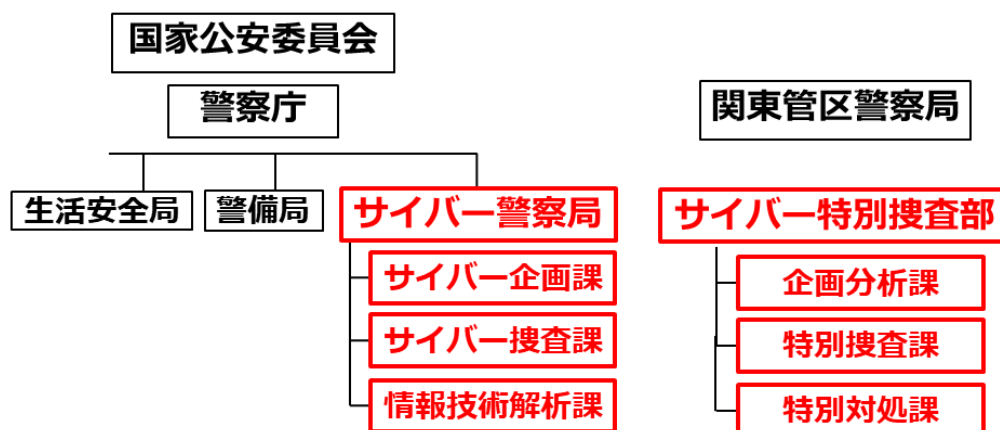
警察庁サイバー警察局は、令和8年度の定員数が265名（前年比＋5名）であり、関東管区サイバー特別捜査部の定員数が227名（前年比＋42名）と年々体制を拡充している。

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

同隊は、従来、外国治安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、外国治安機関等と情報交換を継続的かつ緊密に行うことで、強固な信頼関係の構築を実現している。

令和6年4月、サイバー特別捜査隊が発展的に改組され、新たにサイバー特別捜査部が設置されるとともに、その下に企画分析課と特別捜査課が置かれ、さらに令和7年4月には、サイバー特別捜査部に特別対処課が設置された。これらにより、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析、事案発生の予防及び被害の拡大防止等を行う体制が強化された。これは、都道府県警察が捜査により得た膨大な情報をサイバー特別捜査部に集約し、同部が、外国治安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、犯罪グループの中核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 47：サイバー警察局・サイバー特別捜査部の組織図】

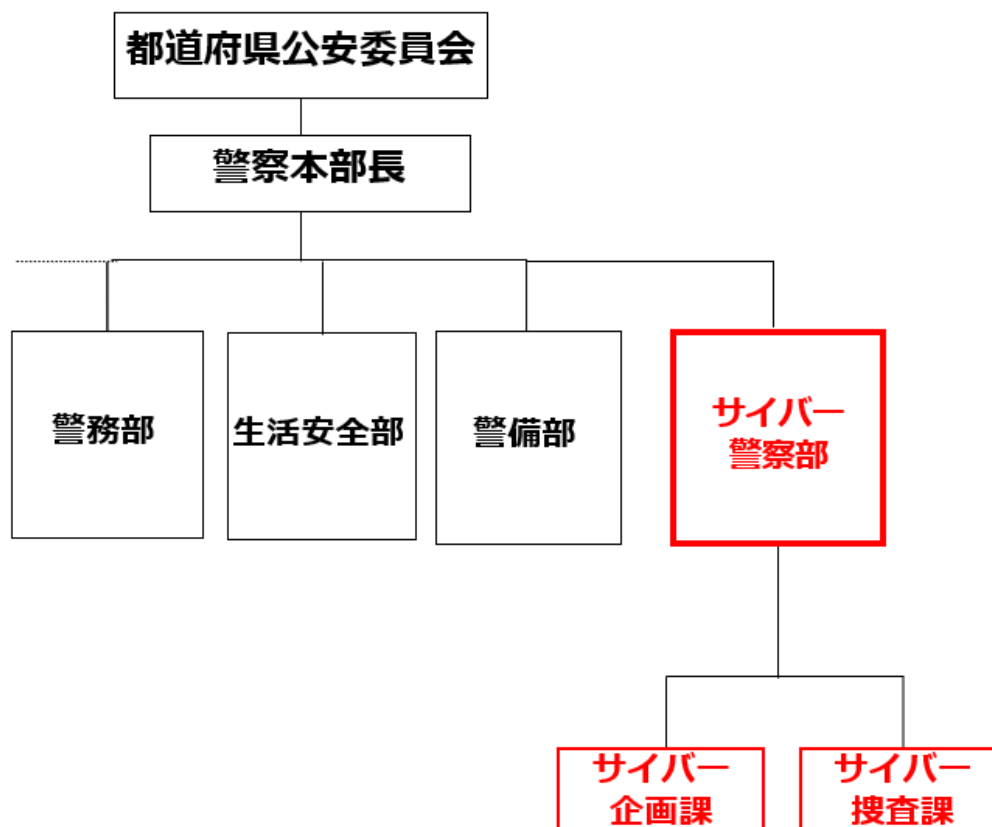


コラム：都道府県警察におけるサイバー警察部の設置

深刻化するサイバー空間をめぐる脅威に的確に対応するためには、警察の限られた人的・物的リソースを効果的かつ効率的に活用する必要がある。そのためには、サイバー警察事務を一元化している警察庁と同様、都道府県警察においても、他部門への支援や人材育成等をはじめ、部門横断的の性質が強いサイバー警察事務について、各部に分散させるのではなく、中立的な組織に集約し、一元的に行うことが効果的・効率的である。こうした観点から、令和8年5月29日、都道府県警察本部の内部組織を条例で定めるに当たっての基準を定める警察法施行令が改正され、サイバー警察部等においてサイバー警察事務を一元的に所掌することとされた。

都道府県警察においては、それぞれの実情を踏まえつつ、改正警察法施行令に基づき、サイバー部門の一元化組織の設置に向けた準備を進めている。これまでもフロア一体化や資機材の集約をはじめとする様々な取組によりサイバー部門の一体的運用を確保してきたが、一元化組織の整備により、サイバー部門の一体的運用が一層確保され、これにより、警察全体のサイバー対処能力の向上が期待される。

【今後の都道府県警察サイバー部門のイメージ】

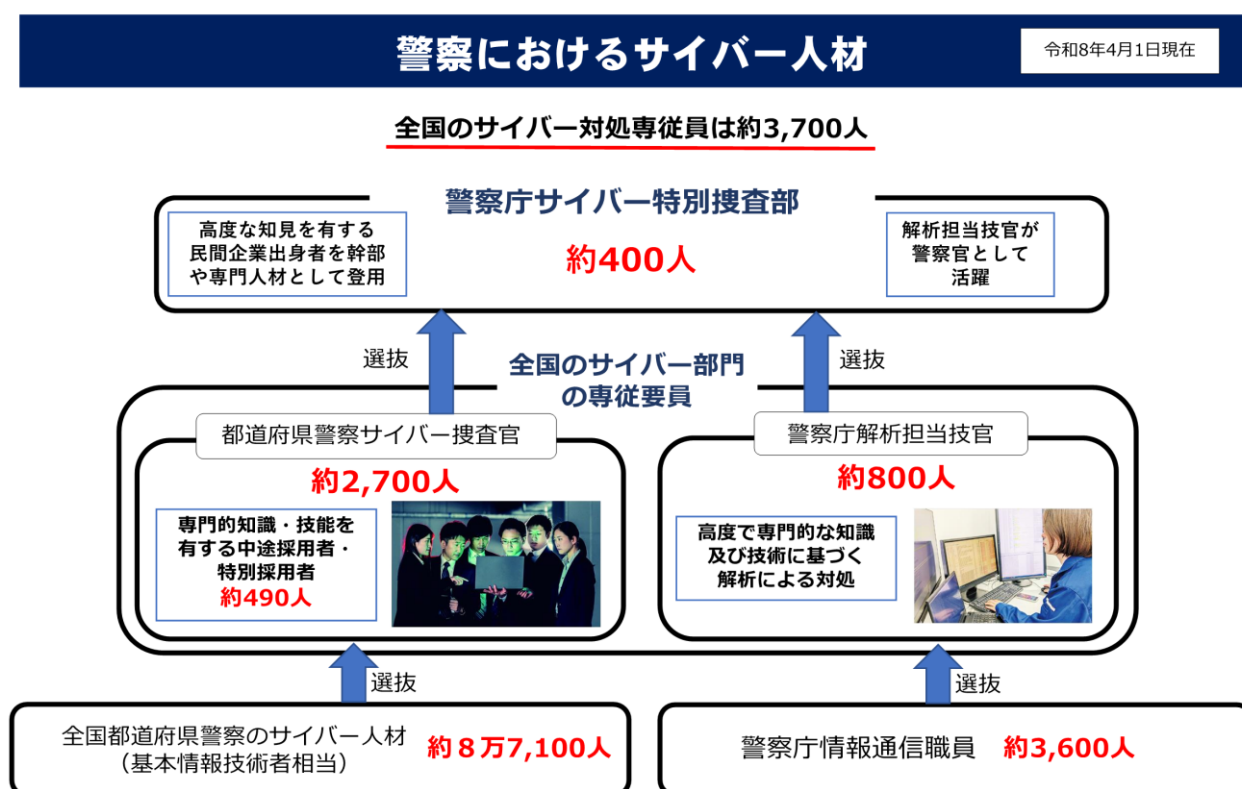


(2) 人材の確保・育成

社会全体においてサイバー分野における高度な専門的知識及び技術を有する人材の重要性が高まっている一方で、少子高齢化・人口減少、地方の過疎化と都市部への人口集中等の急速な進行により、社会構造が変化し、警察職員の採用情勢も厳しさを増している。

警察では、サイバー空間における脅威への対処のための人的基盤を強化するため、令和7年3月、都道府県警察・情報通信部門におけるサイバー人材確保・育成方針に基づき、サイバー人材の確保・育成及びそのキャリアパスの管理並びに全職員の対処能力の向上に係る取組を部門横断的かつ体系的に推進している。

【図表 48：警察におけるサイバー人材数】



※ 警察庁サイバー特別捜査部約400人には、定員227人に加え、都道府県情報通信部解析担当職員との併任者等約180人が含まれていることから、全国のサイバー対処専従員は当該併任者等を除いた約3,700人になる。
 ※ 専門的知識・技能を有する都道府県警察の中途採用者・特別採用者約490人のうち、サイバー部門以外に所属する約270人については、都道府県警察サイバー捜査官の約2,700人に含めていない。

① 人材確保

警察では、サイバー事案について高度な知見を有する人材を確保するため、効果的な採用募集活動や警察部内のサイバー人材の発掘などに取り組んでいる。

○ 高度サイバー人材の確保

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 490 人が、サイバー事案への対処に係る高度な知見を生かして、サイバー犯罪捜査官としてサイバー犯罪捜査等の第一線で活躍している。

警察庁では、従前から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、実践的な研修を実施するなどして育成しており、約 800 人の技術系職員が、情報技術解析等の第一線で活躍している。

また、令和 8 年度に、警察庁では、専らサイバー事案の対処等に係る事務に従事する技術系職員 2 名を採用（サイバー採用）したほか、地方機関では、サイバー事案等への技術的な支援を行う情報技術解析課に配置される技術系職員 14 名を採用（情報処理技術者採用）した。

コラム：サイバー人材の新たな確保方策

警察庁におけるサイバー採用は、情報処理に関する応用的知識・技能を有する者を対象とする採用選考であり、令和 8 年度採用が初めての試みである。

サイバー採用により採用された技術系職員は、採用後、警察学校及び職場における教育訓練を通じて、重大サイバー事案への対処等に必要な知識・能力を早期に習得した上で、その専門性を生かし、主として警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において勤務することとなる。令和 8 年度に引き続き、令和 9 年度の採用募集を実施するとともに、街頭に設置された大型ビジョンや警察庁公式 X 等を通じた画像や動画により、サイバー採用の魅力を効果的に発信している（資料編 127 頁参照）。



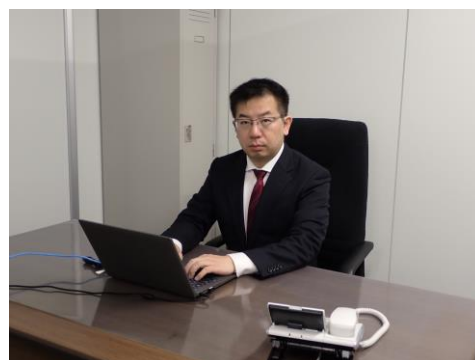
街頭の大型ビジョンで採用募集に係る映像が放映されている様子

さらに、官民人事交流制度による民間人材の登用を進めており、サイバー警察局では、同局設置の令和4年以降、官民人事交流制度により、民間企業から高度な知識・技術を有する9名を採用している（資料編115頁参照）。

コラム：高度なサイバーセキュリティ技術を有する民間人の登用

警察組織の能力強化を目的として、特に高度な技術を有する民間人材を非常勤の国家公務員として採用する取組が開始された。

令和8年6月に重大サイバー事案対策戦略官として採用された小河哲之氏は、民間企業での勤務を継続しながら、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において、重大サイバー事案に関する技術的知見の提供や警察組織における人材育成に関する助言等の幅広い業務に取り組んでいる。



新たに採用された
小河重大サイバー事案対策戦略官

○ サイバーコンテスト

警察庁では、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。

令和8年10月1日に、アクセス・無害化措置について定める改正警察官職務執行法が施行される予定であることを踏まえ、令和7年度に警察庁が実施したサイバーコンテストにおいては、より実践的な技能を確認するため、従来から実施していた「サイバー捜査部門」及び「デジタル・フォレンジック部門」に加え、サーバのぜい弱性を発見するなどの実務能力を確認する「オフENSEンシブセキュリティ部門」を新たに実施した。

また、都道府県警察においては、警察職員を対象としたサイバーコンテストを開催し、サイバー空間における脅威への対処能力の向上や素養のある人材の発掘に取り組んでいるだけでなく、学生等を対象としたサイバーコンテストを開催し、若年層のサイバーセキュリティに関する意識の醸成及びサイバー犯罪捜査官となり得るサイバーセキュリティ人材の裾野拡大に取り組んでいる。

コラム：サイバー防犯ボランティア等に向けたサイバー犯罪捜査官の魅力発信

令和8年2月、埼玉県警察は、サイバー空間における被害防止のための教育活動やサイバー犯罪捜査官の魅力に触れてもらう観点から、高校生、専門学校生、大学生のサイバー防犯ボランティア等を対象とした「サイバーボランティア・学生CTF⁵⁰大会」を開催した。本大会は、10都県警察及び一般財団法人日本サイバー犯罪対策センター（JC3）との合同で行われ、計約60チーム約150人が参加した。参加者からは「解きごたえのある問題が多く、楽しみながら取り組めた。スキルを活かして社会貢献していきたい。」といった感想が聞かれるとともに、本大会を契機として、若年層がサイバー犯罪捜査官を身近に感じるなど、具体的な採用募集活動につながった事例もみられる。



サイバー防犯ボランティア等の学生がCTF大会に参加する様子

② 人材育成

サイバー人材を確保・育成する取組は部門横断的に推進する必要があるが、警察庁では、都道府県警察等の指導体制をリードしていくための司令塔的存在として、指導・人材育成部門の体制強化を図っている。

また、AI技術の急速な進展・普及に伴うサイバー空間の脅威に的確に対応するため、AIを悪用した事案や高度な攻撃能力を有するAIモデルの出現に対処できるサイバー人材の育成を図っている。

○ 能力検定

サイバー空間はあらゆる犯罪に悪用され得るため、サイバー関係の知識は、全ての捜査分野において不可欠となっている。そこで、各職員に求めるサイバー対処能力を初級、中級及び上級に区分した上で、全職員を対象としたサイバー対処能力検定を実施している。令和8年4月現在、高度な専門的知識及び技術を要するサイバー事案に的確に対処できる能力を有する上級検定の合格者は約900人、ネットワーク利用犯罪に的確に対処できる能力を有する中級検定の合格者は約8万7,100人となっている。

また、サイバー事案に関する相談の内容を理解し、適切に受理することができる能力を有する初級検定については、採用時教養の機会に全ての警察官が受検している。

⁵⁰ CTF（Capture The Flag）とは、サイバーセキュリティの分野で専門知識や技術を駆使して隠された答え（Flag）を見つけるクイズ形式の競技をいう。

○ 資格取得

高度な知識・技能に係る情報処理資格である情報処理安全確保支援士の登録資格取得者数及び CISSP⁵¹の資格取得者数は、令和 8 年 4 月現在、それぞれ、情報処理安全確保支援士が約 760 人、CISSP が約 50 人となっている（このうち、約 40 人が両資格を重複して有している。）。

○ 学校教養

警察大学校サイバー警察教養部では、都道府県警察のサイバー部門においてサイバー事案の対処に当たる捜査員等を対象とした高度な実践的研修や都道府県警察の各部門の捜査幹部を対象とした適正な捜査指揮に関する研修を実施している。また、令和 8 年度から新たにオフENSEシブセキュリティに関する高度な人材の育成を行うなど、警察を取り巻く諸情勢の変化を踏まえた教養を実施している。

都道府県警察においては、学校教養及び職場教養を通じて職員のサイバー対処能力を育成するための中核的な組織として、サイバー部門に指導・教養班を整備するとともに、警察学校においては、令和 8 年度から初任科教養でサイバー科目の新設及び授業数が拡充されており、学校教養を通じてサイバー人材を育成する観点から、サイバー事案捜査に関する教養を実施できる教官を配置するなど教養体制の整備を推進している。

○ 職場教養

都道府県警察では、業務を通じた能力向上を図るため、戦略的な人事配置に取り組んでいる。具体的には、各部門の将来を担う優秀な若手警察官をサイバー部門で勤務させ、サイバー空間における犯罪の捜査要領を習得させた後、各部門に再配置するなど、サイバー部門の知見が組織全体に還元される部門横断的な人事配置を行っている。

また、各部門の優秀な若手職員を先進的な取組を進める他の都道府県警察のサイバー部門に継続的かつ計画的に派遣しており、警視庁サイバー犯罪対策課協働捜査班⁵²では、令和 4 年以降、延べ 194 人の派遣を受け入れている。

⁵¹ CISSP（Certified Information Systems Security Professional）とは、ISC 2（International Information Systems Security Certification Consortium）が認定を行っている国際的に認められた認定資格をいう。

⁵² 警視庁では、協働捜査班の前身である「情報追跡班」が設立された翌年の平成 23 年から、他の道府県警察からの派遣捜査員を受け入れている。協働捜査班は、インターネット・ホットラインセンターから通報を受けた違法情報に対する情報追跡、インターネットバンキングに係る不正送金事犯の初期捜査、道府県警察からの捜査共助依頼に対する対応等を任務とし、全国警察の効果的・効率的な捜査の推進に寄与している。

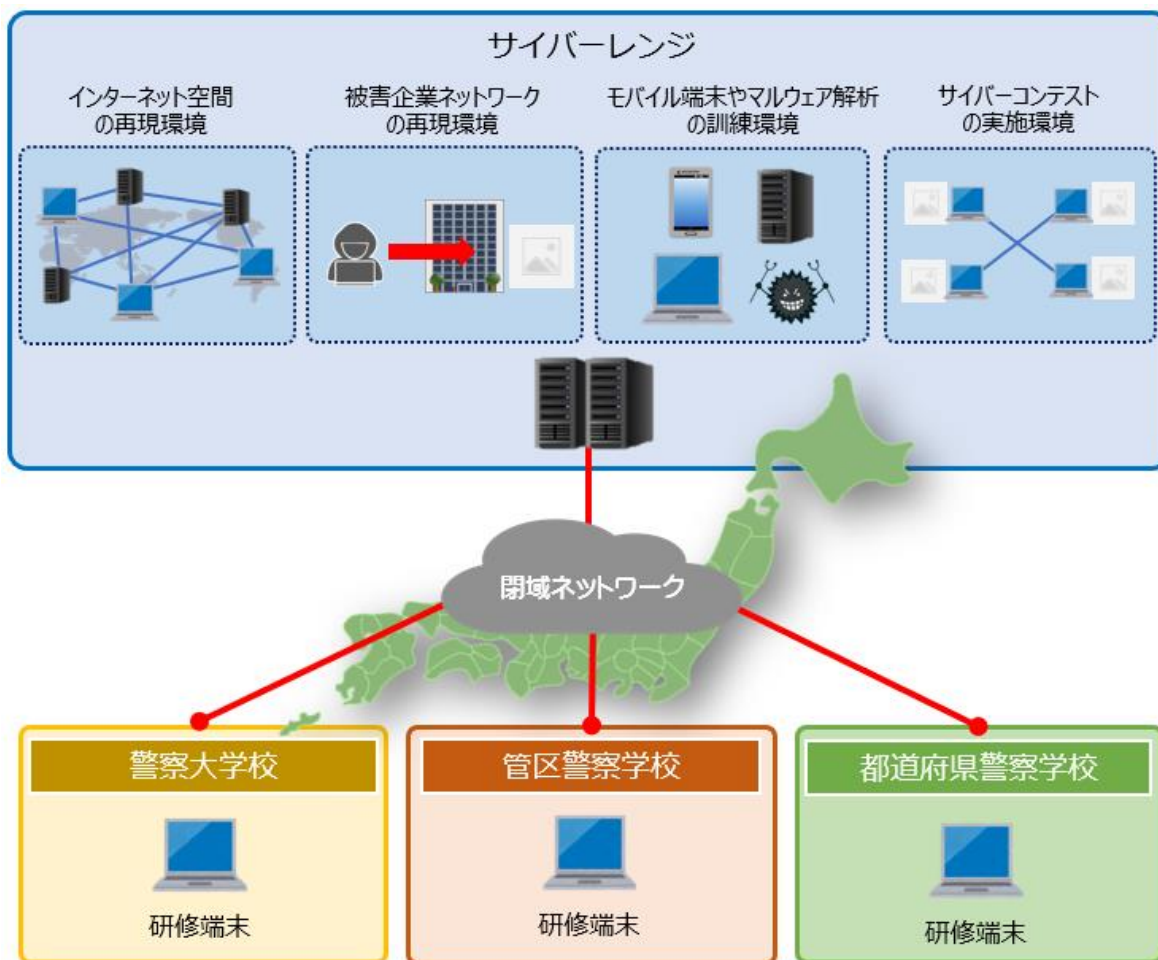
コラム：サイバーレンジによる訓練

平成 30 年度以降、警察大学校にサイバーレンジ（サイバー事案に対する実践的な訓練を行うためのサイバー演習環境をいう。）を導入し、仮想環境下で実際の犯行手口や被害状況を再現することにより、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の実施を可能としている。

日々のサイバー事案に対処する都道府県警察の捜査員に対しても、実践的な研修を行い、全国的なサイバー事案対処能力を向上させるため、警察庁は、都道府県警察からも同サイバーレンジを遠隔利用できるようなネットワークを整備している。

サイバーレンジは、警察のサイバー人材育成に必要不可欠なインフラとして、高度な専門的知識・技術を必要とするサイバー事案への対処能力を習得するために活用されている。サイバー空間の脅威は、急速に変化・高度化し続けていることから、対処能力を陳腐化させないために、サイバーレンジも最新のものを導入し、これを高度化し続ける必要がある。

【サイバーレンジの仕組み】



(3) 資機材の整備

深刻化するサイバー空間の脅威に的確に対処するためには、資機材の整備・高度化が急務であることから、警察庁においては、サイバー特別捜査部を中心とした国の機関への集中的な資機材整備を推進している。例えば、(2)に記載のサイバー人材を育成するためのサイバーレンジのほか、匿名・流動型犯罪グループの検挙や重大なサイバー攻撃による被害の未然防止・拡大防止に寄与する資機材として、暗号資産分析ツール、サイバー捜査分析用資機材、スマートフォン解析用資機材、解析基盤装置、高速演算装置等を整備している。

また、令和8年10月1日にアクセス・無害化措置に係る改正警察官職務執行法が施行される予定であることから、令和7年12月に国家安全保障会議において決定された「アクセス・無害化措置の運用に関する指針」を踏まえつつ、引き続き、AIを活用した資機材の導入等を含め、運用開始に向けた諸準備を継続し、サイバー対処能力の一層の向上を図っていくこととしている。

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

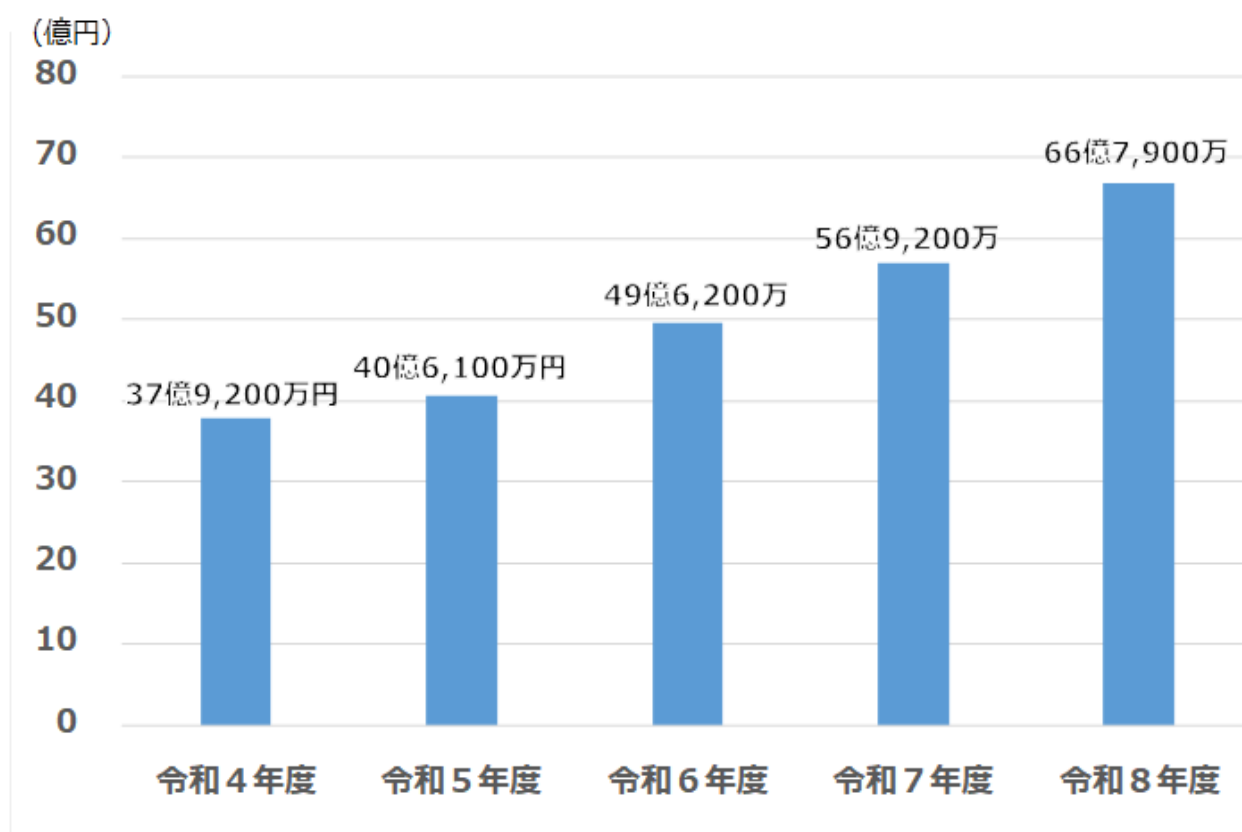
また、令和6年度補正予算・令和7年度補正予算におけるサイバーセキュリティ対策の強化に係る予算は、それぞれ、88億7,600万円・39億6,400万円となっている。

令和8年度当初予算におけるサイバー空間の脅威への対処に係る予算は66億7,900万円（前年度比17%増）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53億8,000万円（前年度比21%増）、人的基盤の強化及び研究の推進に係る予算は7億1,100万円（前年度比5%増）、官民連携及び国際連携の推進に係る予算は5億8,800万円（前年度比6%増）となっている。

なお、サイバー攻撃は、その性質上、事案発生時点では、その攻撃主体や目的等を即座に判断できるものではなく、サイバー警察の全ての対処能力をもって判明させていくものであることから、サイバー空間の脅威への対処に係る予算は、全て、サイバー安全保障関連経費と整理されている。

このように、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はサイバー警察局が設置された令和4年度以降、増加が続いているが、国家安全保障や危機管理の観点も踏まえて行われる能動的サイバー防御の実施等、サイバー空間の脅威に対して的確に対処するためには、更なる資機材の整備・高度化は必要不可欠である。警察庁では、昨今その脅威が増大しているAIを含め、サイバー空間をめぐる脅威の情勢を踏まえながら、引き続き、必要となる予算の持続的な確保を推進していく。

【図表 49：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) 研究・開発

近年、不正プログラムを悪用したサイバー事案が多発する中、その手口の巧妙化・多様化により、不正プログラム解析には極めて高い技術力が求められており、警察捜査を支えるためには、最新の技術に対応した解析能力の向上を図っていく必要がある。このため、警察では、解析手法の開発や犯罪に悪用され得る最先端の情報通信技術の調査・研究を推進している。

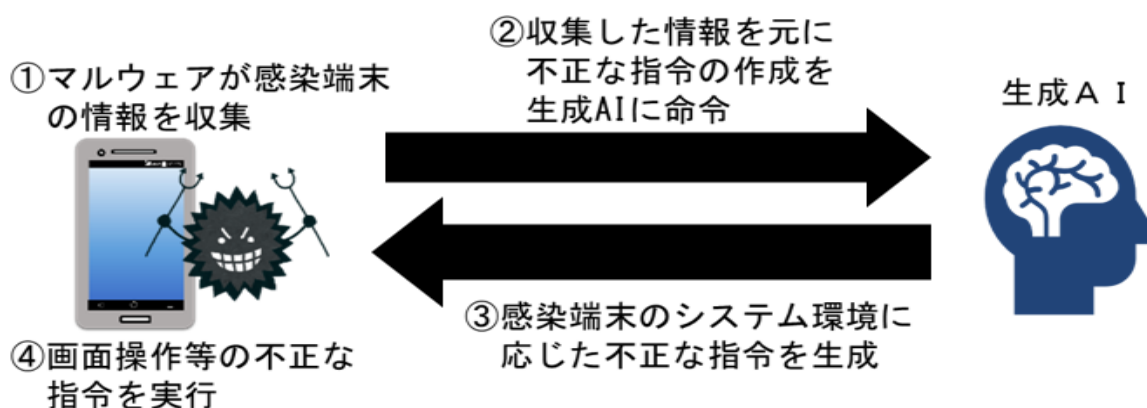
例えば、解析の高度化・効率化の取組として、A I を活用した不正プログラムの機能推定や不正プログラムを仮想環境で自動的に実行して他のコンピュータとの通信、ファイルの作成、プログラムの実行等の挙動を取得するサンドボックス⁵³を使用した簡易解析の仕組みを取り入れている。

また、近年、ランサムウェアの被害が深刻であり、データ復号ツールの重要性・必要性が今後更に大きくなっていくと見込まれることから、A I を駆使した解析機能の高度化等により、データ復号ツールの研究・開発を一層強化していくこととしている（本文 43 頁参照）。

【CASE：生成A I を悪用するマルウェアの解析】

令和8年2月、スマートフォン端末等において、生成A I を悪用する新たなマルウェアの存在が確認された。警察庁において、当該マルウェアを解析したところ、感染した被害端末は、被害端末自身の情報を生成A I に送信することで、生成A I に被害端末のメーカーや機種等に応じた画面操作に関する命令を生成し、ユーザーの操作なしに不正な命令を実行する機能を有することが確認された。

【生成A I を悪用するマルウェアの動作イメージ】



⁵³ プログラムを隔離した仮想環境で安全に動かす仕組み。「サンドボックス (sandbox)」は直訳すると「砂場」という意味で、外部から仕切られた安全な遊び場になぞらえている。

電子機器の解析に関する研究や犯罪に悪用され得る最先端の情報通信技術に関する研究を行う警察大学校サイバーセキュリティ対策研究センターでは、ハードウェア及びソフトウェアに関する知識や技術を駆使して、生成AIを活用した不正プログラム解析の高度化に向けた研究や、自動運転システムを搭載した車両に対するサイバー攻撃を想定した研究などを実施している。

例えば、学術機関と連携し、自律的に不正プログラムの解析を行うシステムを構築・検証したほか、自動運転システムを搭載した車両に対するサイバー攻撃を想定したセキュリティインシデントの解明に関する共同研究を実施した。また、ドローンの機体、操縦器等に記録されているデータの抽出や可視化・可読化手法に関する研究を実施した。



【自動運転技術の研究の様子】



【ドローン研究の様子】

コラム：一体的運用による研究・開発の高度化

警察では最新技術を最大限に活用した対応を行うため、サイバーセキュリティに関する研究・開発を継続的に推進している。

現在、サイバー警察局では情報技術解析課が中心となり、捜査で使う解析ツールの開発など、実務に直結する取り組みを行っている。一方、警察大学校サイバーセキュリティ対策研究センターでは、デバイスやネットワークの新しい解析手法など、より基礎的・学術的な研究を進めている。

これら二つの機関は、従来から相互に連携しつつ研究開発を進めてきたが、サイバー領域の変化が加速度的に進む現在においては、個別の場所・個別の体制で業務を進める従来の枠組みでは、脅威への対応能力を十分に高めることが困難となりつつある。

このため、研究・開発機能を統合し、一体的に運用することで、実務面と基礎研究面を有機的に結び付け、より高度かつ迅速な研究開発を可能とする体制の構築が求められている。

資料編

「はじめに」関連

- ・警察におけるサイバー戦略 83
- ・サイバー警察によるシームレスな対処 83
- ・政府における三位一体の対処 84

「検挙に向けた取組」関連

- ・サイバー警察局設置前における国際共同捜査 85
- ・サイバー警察局設置後における国際共同捜査 87
- ・サイバー特別捜査部の国内における合・共同捜査 92

「未然防止・拡大防止に向けた取組」関連

- ・令和8年上半期における主なサイバー攻撃 97
- ・事案認知に向けた取組 98
- ・サイバー攻撃に対するパブリック・アトリビューション 99
- ・サイバー攻撃に対する主な注意喚起 101
- ・国家を背景とするサイバー攻撃 103
- ・サイバー対処能力強化法及びアクセス・無害化措置の運用の流れ 105

「政府の戦略・文書」関連

- ・サイバーセキュリティ戦略（令和7年12月23日）（抄） 107
- ・AI法・AI基本計画及びバーティカルAI領域別戦略 109
- ・「国民を詐欺から守るための総合対策2.0」の取組状況 111
- ・違法・有害情報に対する通報・相談窓口 112

「基盤整備に向けた取組」関連

- ・サイバー人材の確保・育成 113

「情報発信・広報啓発」

- ・「サイバー警察局便り」を活用した広報啓発 116

「変遷」

- ・サイバー部門の変遷 129
- ・インターネット・ホットラインセンターの変遷 130

「関係法令」

- ・警察法施行令・警察庁組織令 131
- ・警察法 132
- ・警察官職務執行法 133
- ・自衛隊法 135
- ・不正アクセス行為の禁止等に関する法律 137
- ・刑法 138

警察におけるサイバー戦略

情勢認識

- 我が国が戦後最も厳しく複雑な安全保障環境に直面する中、地政学的緊張を反映したサイバー空間を取り巻く情勢は、一層深刻化しており、重大な事態へと急速に発展していく可能性
- また、社会全体のデジタル化の進展に伴い、サイバー空間の匿名性が様々な犯罪で悪用
- サイバー空間の匿名性を悪用した事案については、認知した段階においては、国家を背景とする事案及び犯罪組織による金銭目的の事案のいずれに該当するかなどは判然としないことが多いものの、国民の生命、身体及び財産の保護の任に当たる警察として、国家安全保障や危機管理の観点も踏まえつつ、平時から有事に至るまでシームレスに対処する必要

検挙に向けた取組

- 事案認知の徹底
 - 事業者との協力関係の構築による通報・相談の促進
 - サイバーパトロール、JC3の知見活用等の能動的な事案認知
- 検挙に向けた捜査の推進
 - 他部門では対処困難なサイバー事案への対処・捜査支援
 - 警察庁サイバー警察局・サイバー特別捜査部への情報集約
 - これらを通じた「匿名性の打破」
- 国際連携の強化
 - 被疑者の検挙に向けた国際共同捜査の推進
 - 外国治安機関等との協力関係の強化
- サイバー警察活動における適正性の確保
 - サイバー捜査における基本的留意事項の徹底

未然防止・拡大防止に向けた取組

- 検挙による未然防止の推進
 - 検挙を通じたサイバー事案の抑止
- 情報発信の推進
 - 国際連携によるパブリック・アトリビューションの推進
 - 官民連携による情報発信の推進
- 犯罪インフラへの対処の推進
 - 関係省庁等との連携や事件検挙を通じた犯罪インフラの解体
 - 違法・有害情報への対処の推進
- 効果的なアクセス・無害化措置の実施
 - サイバー特別捜査部によるアクセス・無害化措置の実施

基盤整備に向けた取組

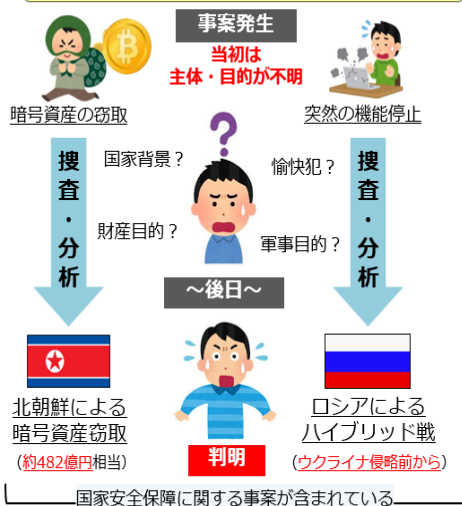
- 人材の確保・育成
 - 人口減少社会を踏まえたサイバー人材の確保・育成の総合的かつ一体的な推進
 - 組織を挙げた全職員の対処能力の向上
- 資機材の整備
 - 真に必要な資機材の計画的な整備・集約
 - AI等の先端技術を活用した分析・解析の高度化・効率化
- 研究・開発の推進
 - ランサムウェアに係る復号ツール等、未然防止・拡大防止に資する研究・開発の推進
 - 政府が推進する各種プログラムの有効活用

警察庁
ホームページ



サイバー警察によるシームレスな対処

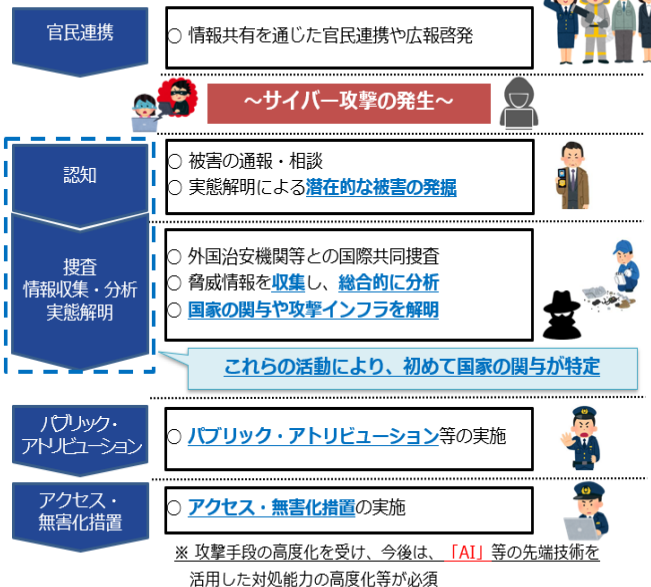
巧妙化・高度化するサイバー攻撃の特徴



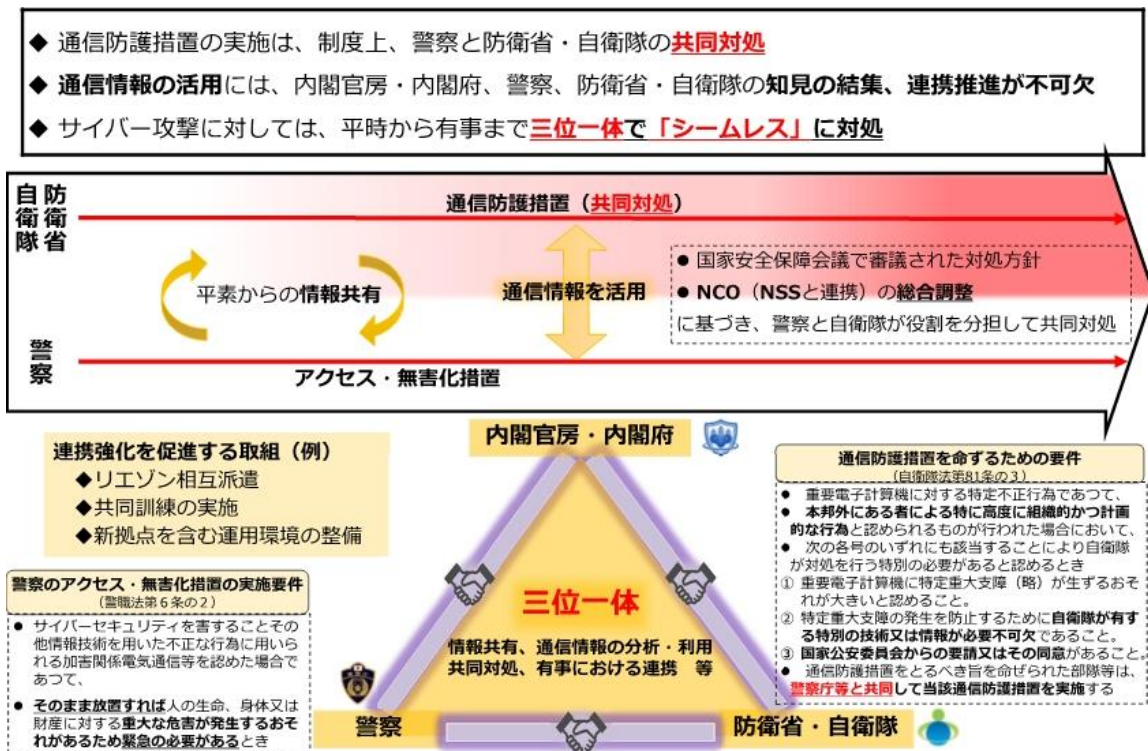
国家安全保障に関する事案を含む
認知した全ての事案に対応する必要

サイバー空間の脅威に平素から有事に至るまで切れ目なく対応するのは警察のみ
警察の諸活動は、「危機管理の観点」・「安全保障の観点」から必要不可欠

警察の取組



政府における三位一体の対処



【内閣官房・内閣府、警察、防衛省・自衛隊の三位一体の対処】

●日本成長戦略 (抄)

17の戦略分野における成長投資を下支えするため、「サイバーセキュリティ戦略」に基づき、サイバー対処能力強化法等の着実な実施^(注)や関連制度の機動的な見直し等により、サイバー脅威への対応を強化する。その際、この対応が成長に必要な投資との認識を共有した上で、官民が協力した持続可能なサイバーセキュリティ確保の在り方を検討する。

(注) サイバー対処能力強化法等の着実な実施のため、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となって中核的な機能を担う体制整備を行う。

内閣官房
ホームページ



●経済財政運営と改革の基本方針 2026 (抄)

サイバー対処能力強化法等を着実に実施するための体制整備^(注)を行うとともに、国家安全保障の観点からサイバー空間での情報収集や対処の在り方を検討する。…国家安全保障戦略の改定に係る議論を踏まえ、所要の措置を検討する。

(注) 内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となって中核的な機能を担う体制整備を行う。

内閣府
ホームページ

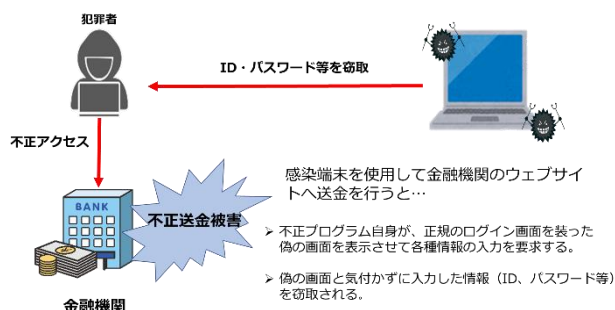


サイバー警察局設置前における国際共同捜査 ①

● 国際的なボットネットを利用した不正送金事案

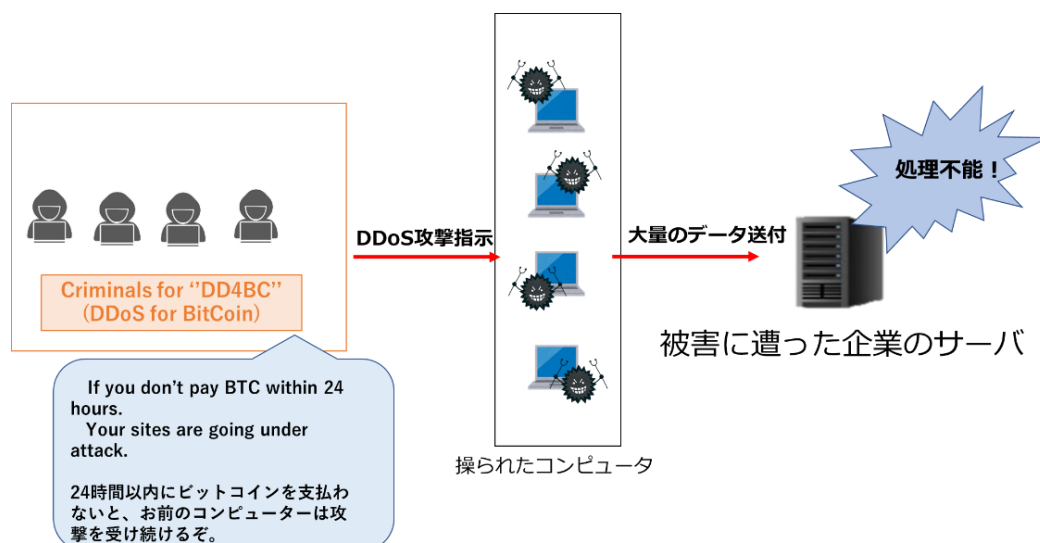
不正送金事犯に使用されているとみられる不正プログラム「Game Over Zeus(ゲームオーバーゼウス)」が世界的にまん延したことから、平成 26 年 5 月、FBI 及び EUROPOL を中心に、日本を含む協力国の

法執行機関が連携して、同プログラムに感染した端末の情報を収集し、当該端末を特定した上で、プロバイダ等を通じて当該端末の利用者に対して不正プログラムの駆除を促すことにより、国際的なボットネットのテイクダウンを決行した。



● DD4BC 犯罪者グループによる金融機関等への DDoS 攻撃事案

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

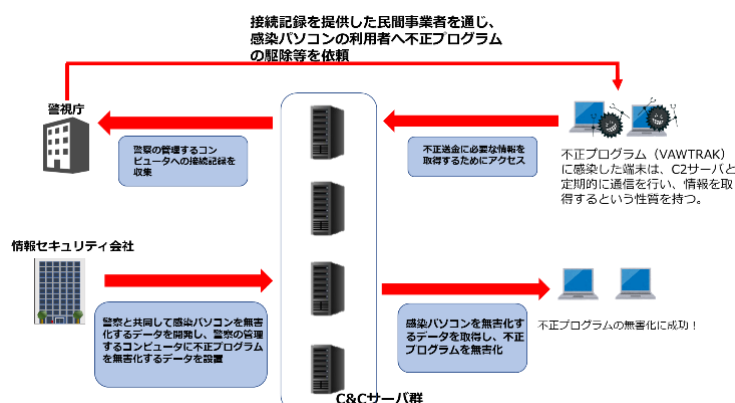


サイバー警察局設置前における国際共同捜査②

● 不正プログラム「VAWTRAK（ボートラック）」を利用した不正送金事案

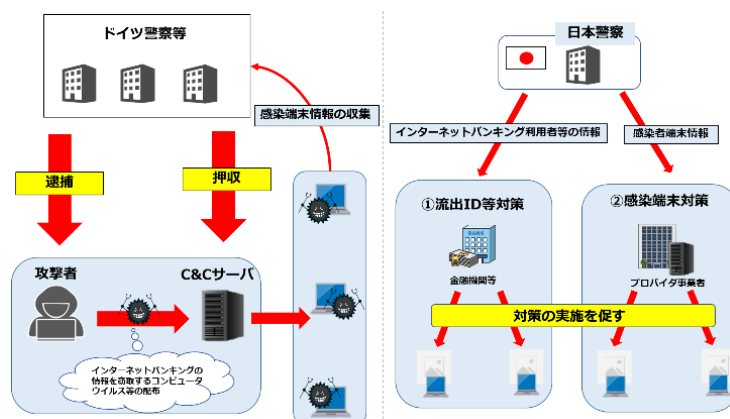
平成 27 年 4 月、警視庁は、インターネットバンキングに係る不正送金事犯に利用される C 2 サーバの動作を観測することにより、国内外において約 8 万 2,000 台の端末が不正プログラム「VAWTRAK（ボートラック）」に感染していることを把握し、不正プログラムによる被害の拡大防止措置を実施した。警視庁は、プロバイダを通じた国内の感染端末の利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供に加え、被害拡大防止措置として、不正プログラムの無害化措置の実施にも成功した。

この不正プログラムに感染した端末は、C 2 サーバと定期的に通信を行い情報を取得するという性質があったことから、この性質を逆手に取り、無害なデータを取得させることにより、不正プログラムの無害化を行ったものである。



● 流出 ID 対策等に繋がったインターネットバンキングに係る不正送金事案

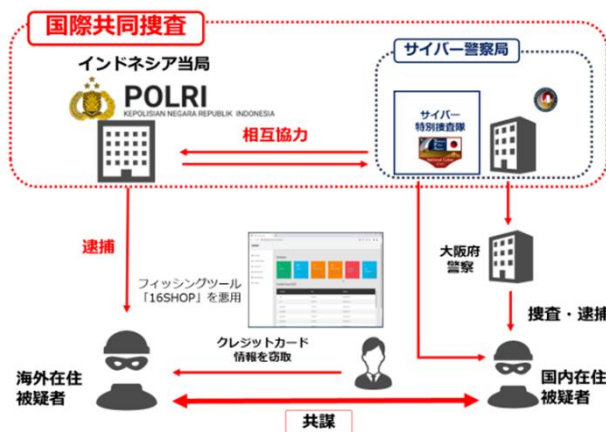
平成 29 年 3 月、インターネットバンキングに係る不正送金事犯に関し、国際的な取組「オペレーション Avalanche（アバランチ）」に係る流出 ID 等対策及び感染端末対策を実施した。日本国内のインターネットバンキング利用者の ID・パスワード等の情報、コンピュータウィルスの感染端末情報等を入手するに至ったことから、関係省庁・団体と連携して、インターネットバンキング利用者、感染端末利用者等に対し、被害拡大防止のための注意喚起を実施した。



サイバー警察局設置後における国際共同捜査①

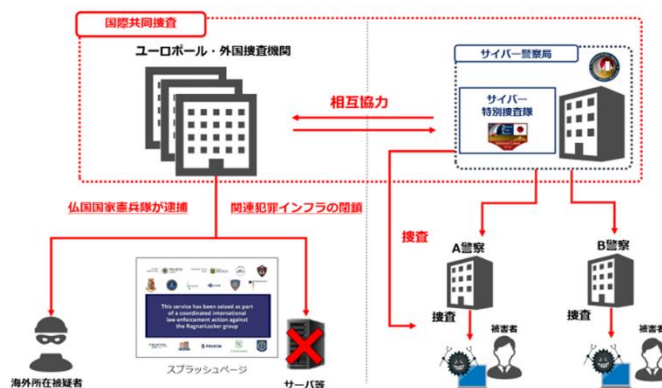
● 「16SHOP」を用いたクレジットカード情報不正取得・利用事案

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



● 「Ragnar Locker」によるランサムウェア攻撃事案

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



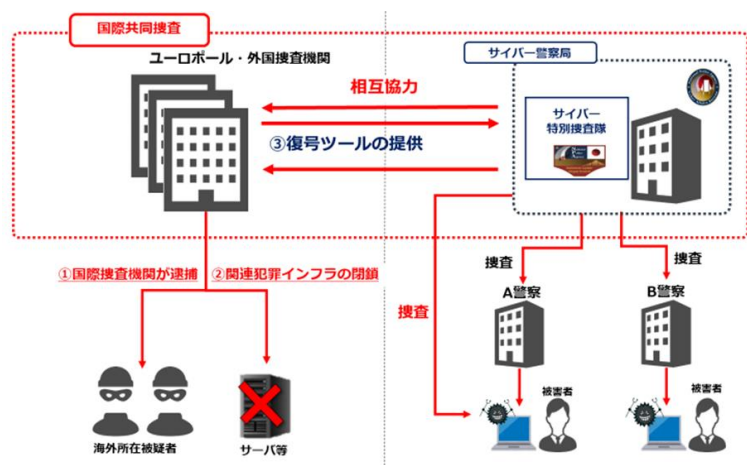
サイバー警察局設置後における国際共同捜査②

● 「LockBit」によるランサムウェア攻撃事案

我が国を含め世界各国の企業等に対してランサムウェア被害を与えている攻撃グループ「LockBit」について、サイバー特別捜査隊（当時）と関係警察は、EUROPOL 等との国際共同捜査「オペレーション Cronos（クロノス）」を推進した。その結果、令和 6 年（2024 年）2 月、関係国の捜査機関が同グループの一員とみられる被疑者 2 名を逮捕したほか、同グループが使用するサーバ等がテイクダウン（機能停止）され、流出した情報等が掲載されていたリークサイト上に、テイクダウンの実施を告げるスプラッシュページが表示された。

この事案では、LockBit により暗号化されたデータを復号するツールを、サイバー特別捜査隊が独自

開発し、国内での被害回復に活用するとともに、令和 5 年 12 月には同ツールを EUROPOL に提供した。また、令和 6 年 2 月、警察庁は EUROPOL 等と連携し、世界中の企業等において被害回復が可能となるよう、同ツールについて情報発信を行い、その活用を促す旨の発表を行った。



【スプラッシュページ】

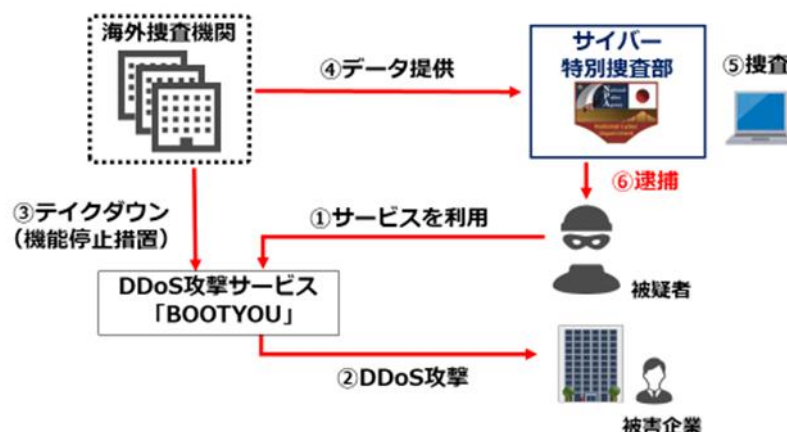
また、これに続く措置として、令和 6 年（2024 年）5 月、ランサムウェアの開発・運営を行っていた被疑者について資産凍結及び起訴が行われ、令和 6 年（2024 年）10 月には関連被疑者 4 名が逮捕された。

サイバー警察局設置後における国際共同捜査③

● 海外の DDoS 攻撃ウェブサービスを利用した日本人被疑者による DDoS 攻撃事案

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

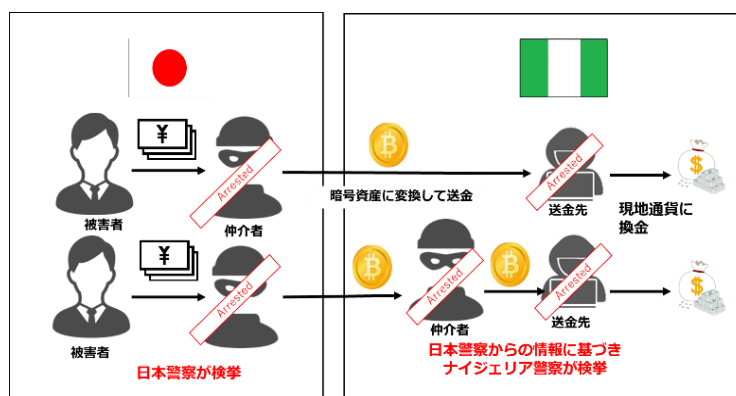
また、令和 6 年 12 月には、本国際共同捜査の一環として実施された広報啓発キャンペーンに参画した。



● ナイジェリア人らによる SNS 型投資・ロマンス詐欺事案

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

サイバー特別捜査部は、我が国で発生した SNS 型投資・ロマンス詐欺事案について、関係都道府県警察の捜査情報を横断的に分析し、また、暗号資産追跡を実施した結果、複数の事案の被害金がナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止めたことから、同情報をナイジェリア警察に提供したところ、令和 6 年 5 月から 7 月までの間に、同警察において同国内の被疑者の検挙が行われた。なお、令和 4 年から令和 6 年までの間に、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。



サイバー警察局設置後における国際共同捜査④

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

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

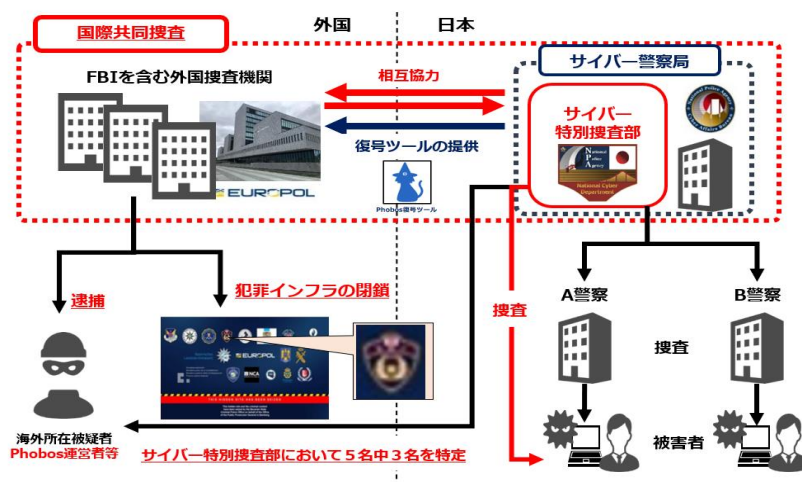
これらの事案において、サイバー特別捜査部は、独自の手法により同運営者等の特定に成功し、その結果や当該手法について、米国やスイスをはじめとする関係国の捜査機関に提供した。本共同捜査を通じて検挙した上記被疑者5名のうち、3名がサイバー特別捜査部の捜査により特定されたものである。

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

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

なお、日本国内において、実際に同ツールを使用し、少なくとも17の被害企業が約717万件の被害データの復号に成功しており、被害回復した企業からは、「調査会社

に依頼しても復号できる保証はなく、費用も掛かるので大変助かった」「実際に復号することができて感謝している」などという声が届いている。

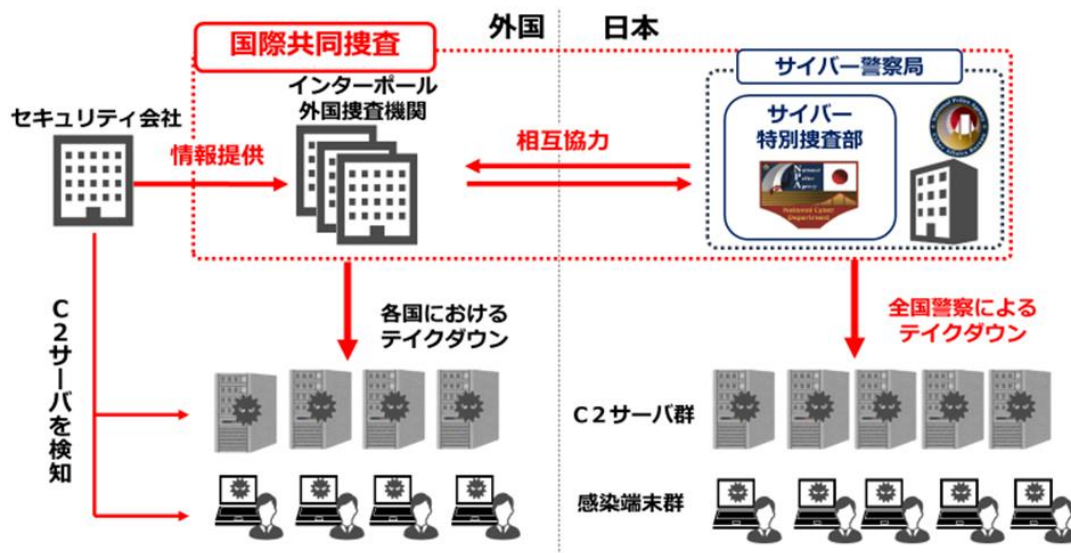


サイバー警察局設置後における国際共同捜査⑤

● 外国捜査機関と連携した C2 サーバテイクダウン

令和7年6月、INTERPOL は、アジア・南太平洋における情報窃取型マルウェアの Infostealer（インフォスティーラー）対策を行うための国際共同捜査「Secure（セキュア）」において、日本警察を含む 26 か国の捜査機関が民間事業者とも連携した捜査により、関係 C2 サーバの管理者に働きかけるなどして当該サーバを停止等させる対策（テイクダウン）を行うことで犯行防止、被害防止を実施した旨を発表した。日本警察は、INTERPOL から提供を受けた情報に基づき、サイバー特別捜査部及び 18 都道府県警察が緊密に連携し、侵害されたサーバを管理する事業者にも順次働きかけを行った結果、当該事業者によって 129 台の C2 サーバがテイクダウンされた。同サーバは、企業等が通常使用するサーバが何らかの理由で侵害され、管理する企業等が気付かないままに情報窃取行為に悪用されたものであった。

【インフォスティーラーに対する INTERPOL との国際共同捜査】



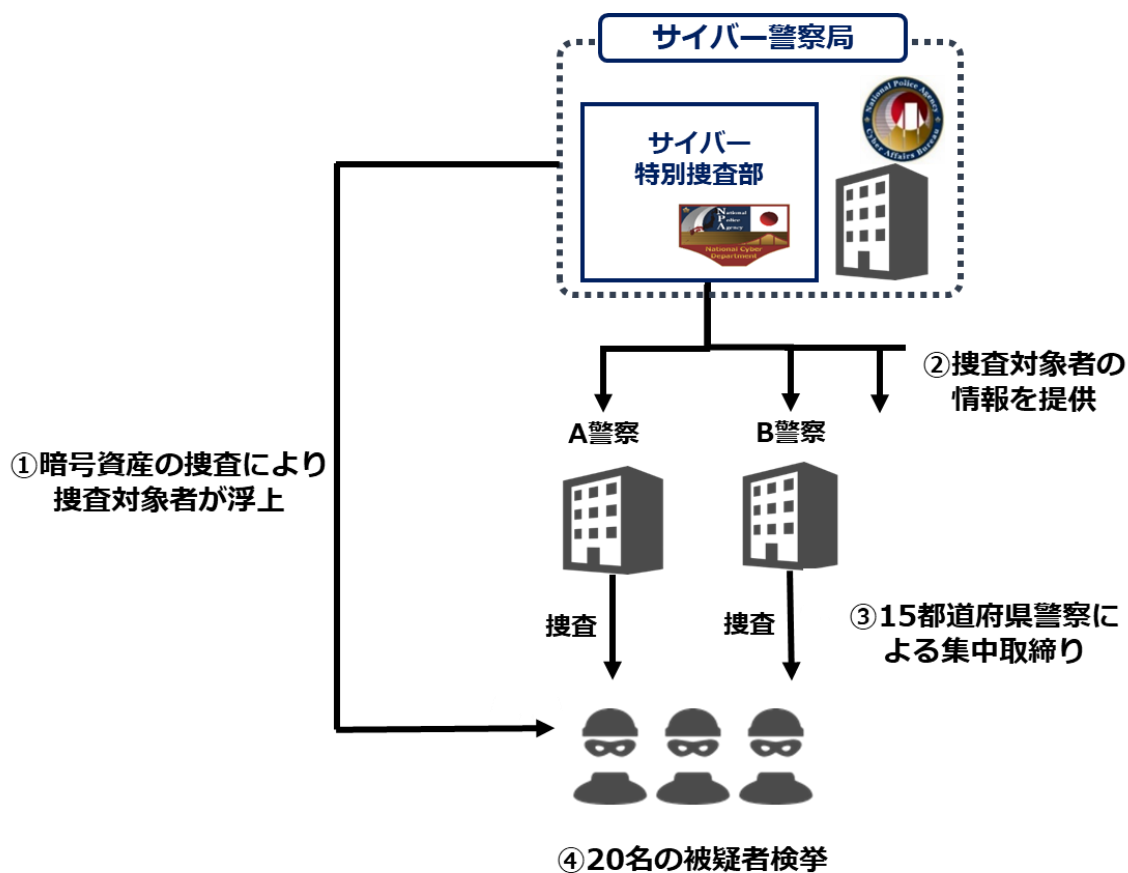
サイバー特別捜査部の国内における合・共同捜査①

● 暗号資産の追跡技術を用いた集中取締り

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

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

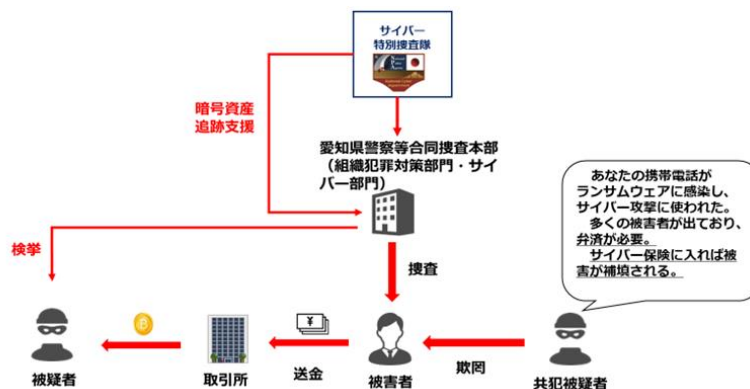
【暗号資産の追跡技術を用いた集中取締りの概要】



サイバー特別捜査部の国内における合・共同捜査②

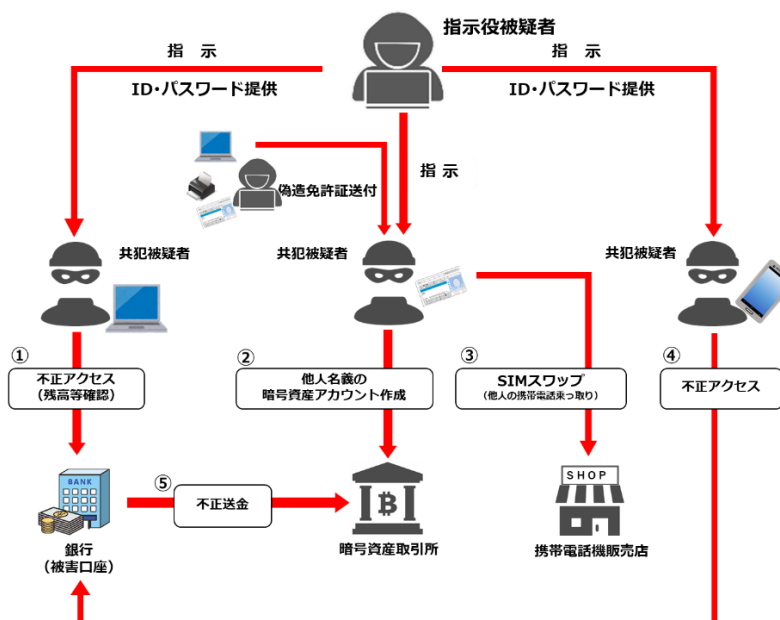
● サイバー保険名目の架空料金請求詐欺事案

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案

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。



サイバー特別捜査部の国内における合・共同捜査③

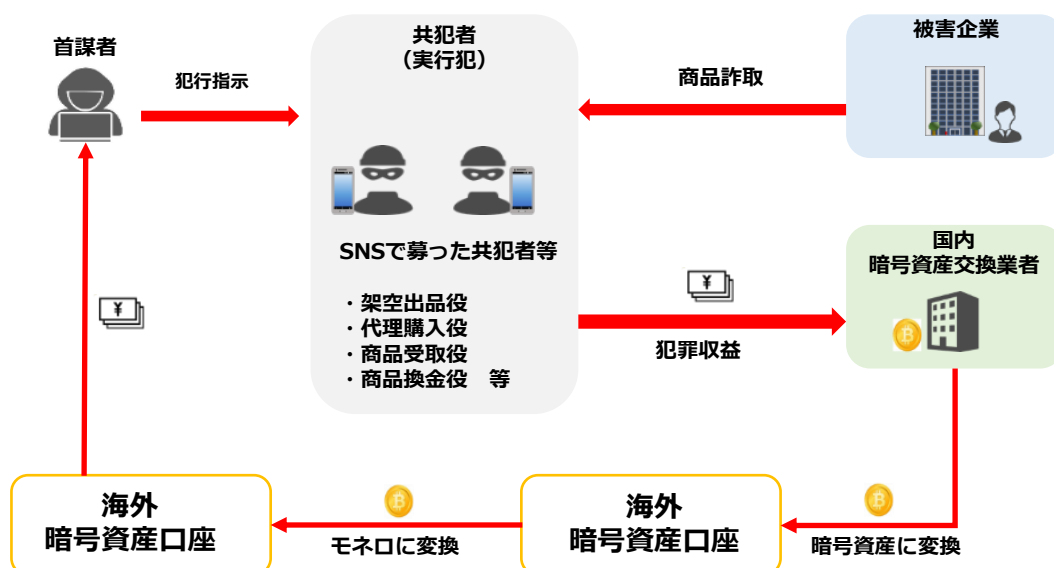
● クレジットカード不正利用事案

令和3年から4年にかけて、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。

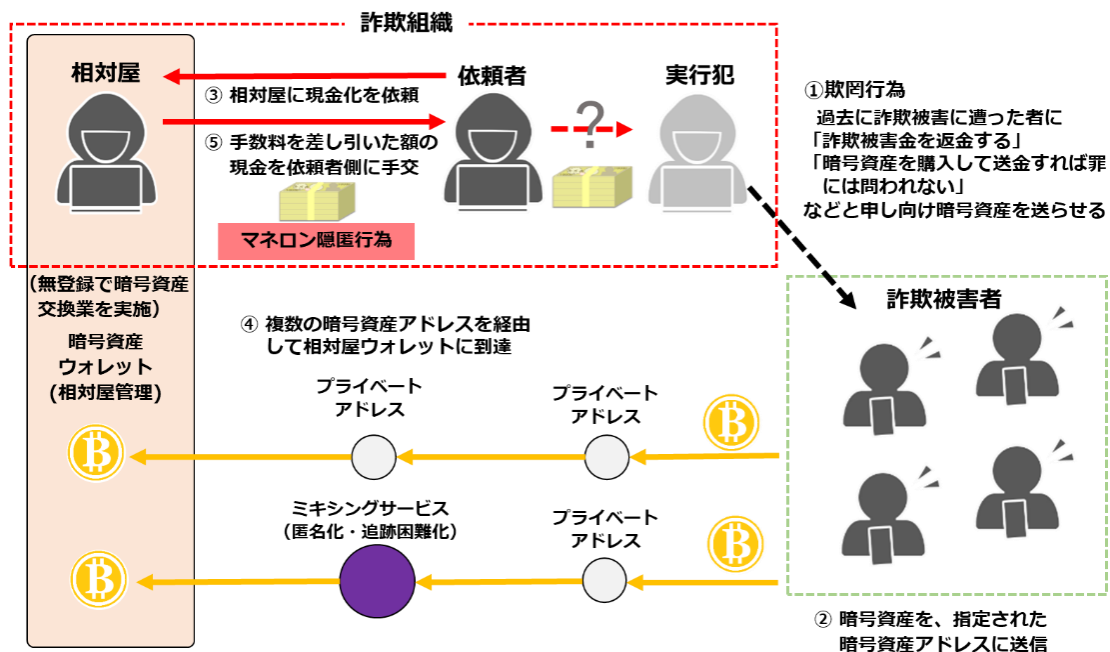


サイバー特別捜査部の国内における合・共同捜査④

犯罪収益に係る暗号資産取引の匿名性を高めるため、暗号資産交換を個人が無登録で業として行う、いわゆる「^{あいたいや}相対屋」を経由するなどして、暗号資産の追跡を困難にし、マネー・ローンダリングに悪用している実態がある。

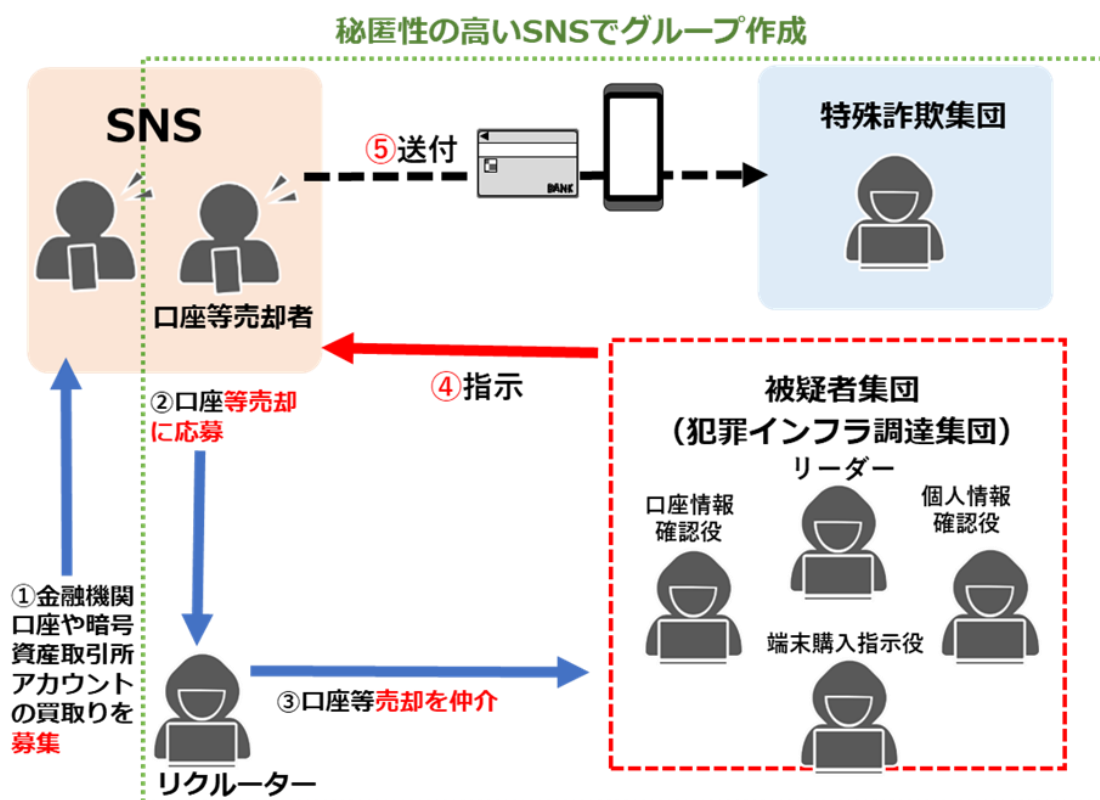
会社役員の男ら2名は、令和4年11月、特殊詐欺事件の被害者から詐取した犯罪収益を含む暗号資産を現金化し、隠匿するほか、うち1名は、令和6年3月から同年10月までの間、本件詐欺の被害金以外の犯罪収益についても暗号資産と現金との交換を継続して実施しており、正規の届出を経ずに業として暗号資産交換業を行う、いわゆる「相対屋」として活動していたことから、令和7年11月、同男ら2名を組織的な犯罪の処罰及び犯罪収益の規制に関する法律違反等、うち1名を資金決済に関する法律違反で逮捕した。（広島、サイバー特別捜査部）

本件においては、特殊詐欺の被害金である暗号資産の移動に、匿名性を高める「ミキシングサービス」が利用されていたところ、サイバー特別捜査部の高度な分析により、被疑者名義のアカウントに被害金が流れていることを解明し、当該アカウントを都道府県警察からサイバー特別捜査部に集約された情報と照合することで、他県での被害との関係性を浮き彫りにするなど、事件構図の解明に貢献した。



サイバー特別捜査部の国内における合・共同捜査⑤

愛知県警によるサイバーパトロールの結果、SNS上に口座買取広告の投稿が確認され、捜査を実施したところ、金融機関口座等の売却者やその仲介者を募り、匿名性の高いSNSを利用して犯罪インフラとなる金融口座や暗号資産アカウントを不正に調達し、複数の特殊詐欺集団らに対して販売していた犯罪集団の関与が確認されたことから、関係道府県警察とサイバー特別捜査部による合同捜査本部が捜査を行った。特に、サイバー特別捜査部においては、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）から提供された情報を集約し、横断的・俯瞰的に分析するとともに、隠匿された暗号資産を高度な専門的知識・技術を用いて追跡したことなどにより、同集団の首魁の男（32）らを特定し、令和7年10月、同男ら7人を詐欺罪及び犯罪収益移転防止法違反（なりませし目的・有償による譲渡し）で逮捕した（愛知、サイバー特別捜査部、北海道、埼玉、神奈川、岐阜、岡山、山口、福岡、長崎及び沖縄）。



令和8年上半期における主なサイバー攻撃

● 医療機関に対するランサムウェア攻撃

令和8年2月、医療機関は、医療情報システムの一部がランサムウェア攻撃を受け、ナースコールシステムに障害が発生したほか、約13万人の患者の個人情報に漏えいしたことを発表した。

● 大手製造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8年3月、大手製造事業者は、外部からの不正アクセスが行われ、社内のデータが不正に取得されたことが判明したと発表した。その後の調査により、約8万8,000件の顧客や従業員の個人情報に不正に取得された、又はそのおそれがあることが判明した。

● 政府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8年4月、政府機関は、官公庁で利用する大容量ファイル転送サービスの専用サーバに対して、不正アクセスがあり、当該サーバに保存されていた個人情報に外部に漏えいした可能性があると発表した。

● 鉄道業界団体に対する不正アクセス

令和8年4月、鉄道業界団体は、ホームページのシステム領域を用いた大容量ファイル転送サービスの脆弱性を突いた外部からの不正アクセスを受け、同サービス利用者の個人情報に漏えいしたと発表した。

● 研究機関に対する不正アクセス

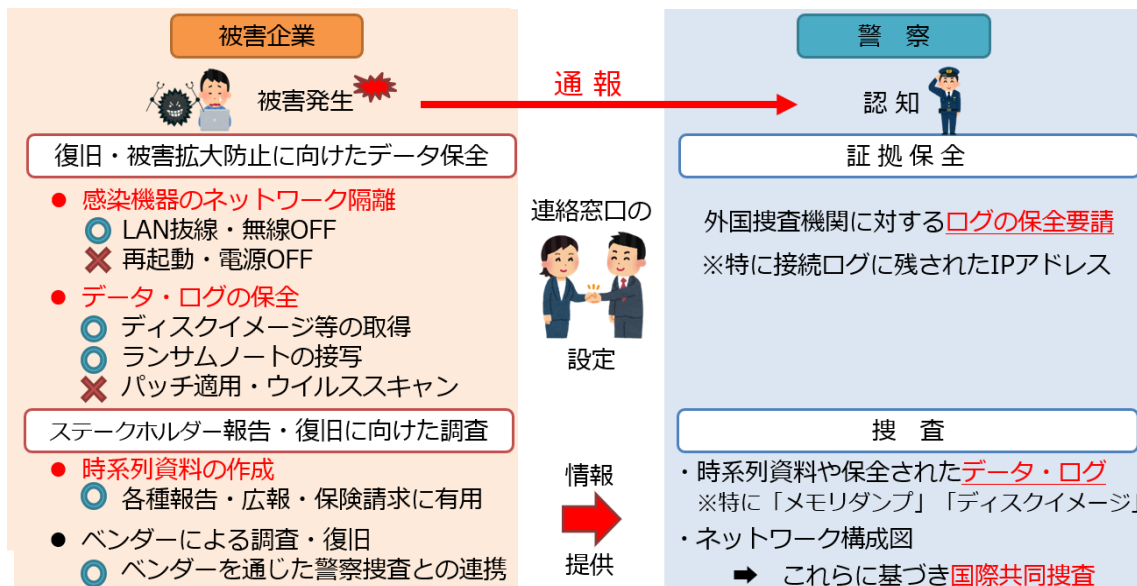
令和8年5月、研究機関は、ウェブサイトの一部コンテンツに関するサーバに外部からの不正アクセスを示す痕跡を確認したと発表した。

● 大手通信事業者に対する不正アクセス

令和8年6月、大手通信事業者は、インターネットサービスプロバイダー（ISP）向けに提供するメールシステムにおいて、各ISPが提供する電子メールサービスで作成されたメールアドレスやパスワードなどの情報が外部に漏えいした可能性があると公表した。その後の調査により、約1,200万人の情報が漏えいしたことが判明した。

事案認知に向けた取組①

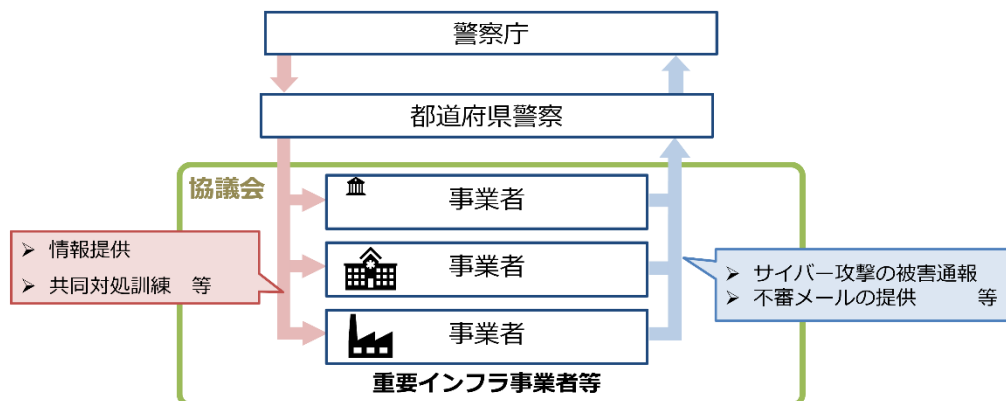
【復旧に向けた調査と警察捜査の関係】



＜コンテナターミナルにおける情報セキュリティ対策等検討委員会取りまとめ（令和6年1月24日）（抄）＞
日頃より情報セキュリティ研修等の場を通じて愛知県警と名古屋港運協会との関係が構築できていたこと。これにより、事案発生時の相談、対応がスムーズになされた。

事案認知に向けた取組②

- 都道府県警察ごとに管内の重要インフラ事業者等をメンバーとする「**サイバーテロ対策協議会**」を設置。
- **サイバー攻撃に関する情報共有や共同対処訓練を実施。**
- 警察と事業者との関係構築により、事案発生時の相談や対応等がスムーズに。



サイバー攻撃に対するパブリック・アトリビューション①

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

サイバー攻撃に対するパブリック・アトリビューション②

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

サイバー攻撃に対する主な注意喚起 ①

事例	年月日	概要
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	R4.11.30 	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に鑑み、NISC と連名で注意喚起を実施。
家庭用ルーターの不正利用に関する注意喚起	R5.3.28 	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。
DDoS 攻撃に関する注意喚起	R5.5.1 	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。
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	R6.10.2 	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」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が行うことを支援する 6 つの原則を示した文書を公表。

サイバー攻撃に対する主な注意喚起 ②

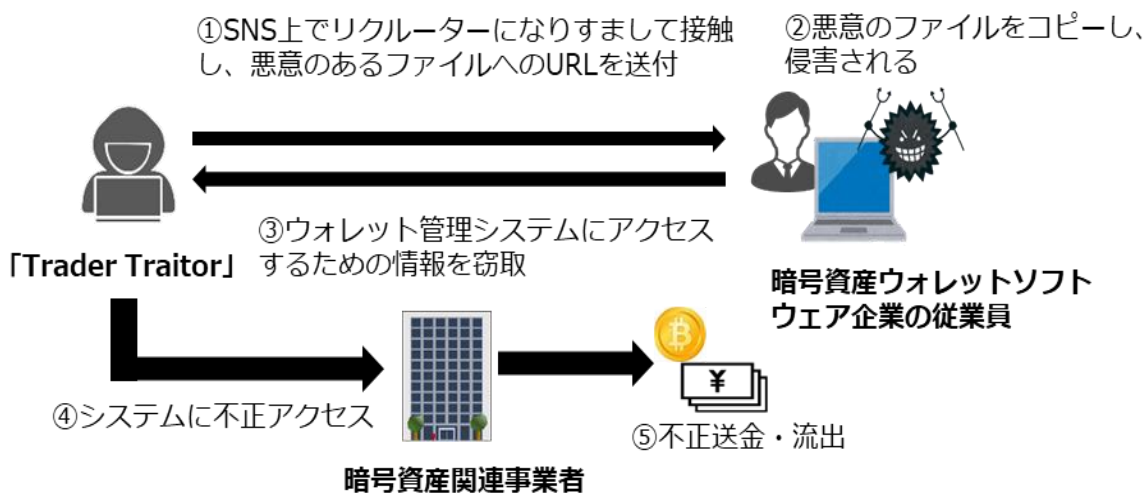
事例	年月日	概要
【北朝鮮】北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について	R6.12.24 	北朝鮮を背景とするサイバー攻撃グループ TraderTraitor が日本国内の暗号資産関連事業者から約 482 億円相当の暗号資産を窃取した。警察庁、NISC 及び金融庁が連名で、同グループの手口例及び緩和策に関する文書を発表。
MirrorFace によるサイバー攻撃に関する注意喚起	R7.1.8 	警察庁は、NISC とともに、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から日本国内の組織、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。
豪州主導国際文書「最新の防御可能なアーキテクチャのための基礎」への共同署名	R7.10.23 	警察庁及び NCO は、豪州、ドイツ、カナダ、ニュージーランド、韓国及びチェコの関係機関と共に、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「最新の防御可能なアーキテクチャのための基礎」の共同署名に加わり、サイバー脅威に対応したシステムの構築、維持、更新、強化のために役に立つアプローチを提供する文書を公表。
北朝鮮 IT 労働者に関する注意喚起	R8.7.31 	警察庁、国家サイバー統括室、外務省、財務省及び経済産業省は、米国及び韓国を始めとする同盟国・同志国の関係機関とともに、「北朝鮮 IT 労働者に関する各国・企業等に対する注意喚起」を公表。

北朝鮮によるサイバー攻撃

- 令和6年5月、北朝鮮を背景とするサイバー攻撃グループ TraderTraitor が日本国内の暗号資産関連事業者から約 482 億円相当の暗号資産を窃取した。当該事案において、TraderTraitor は、①SNS 上でリクルーターになりすまし、暗号資産ウォレット管理システムへのアクセス権を保有する従業員に接触、②悪意あるファイルの URL を送付することで管理システムへのアクセスに必要な情報を窃取、③窃取した情報を利用してシステムに不正にアクセスし、同管理システムを利用していた暗号資産関連事業者の暗号資産を窃取したことが判明している。



- 令和6年12月、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した。



中国の関与が疑われるサイバー攻撃

- 令和元年頃から、MirrorFace と呼ばれるサイバー攻撃グループによる、日本国内の組織、事業者及び個人への情報窃取を目的としたサイバー攻撃が確認された。主な手口として、第三者になりすまし、マルウェアを添付したメールやマルウェアをダウンロードさせるリンクを記載したメールを送信して感染させる標的型メール攻撃、ネットワーク機器（特に VPN 機器等）のぜい弱性を悪用して侵入する攻撃等が確認されている。

- 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、MirrorFace によるサイバー攻撃が、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。



警察庁
ホームページ



■ 攻撃手法

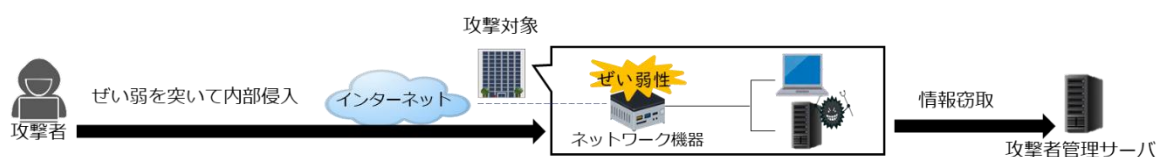
● 標的型メール攻撃

攻撃対象が興味を引く内容のメール、送信者を攻撃対象と親しい者に偽装したメール等（標的型メール）を送付し、マルウェアに感染させて情報を窃取する。



● ネットワーク機器のぜい弱性を悪用した攻撃

攻撃対象が使用しているインターネットと接続している機器（ネットワーク機器）のぜい弱性について内部に侵入し、マルウェアを蔵置して情報を窃取する。



内閣官房
ホームページ



【グローバルな安全保障環境と課題】

サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。

【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。（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。

サイバー対処能力強化法

法の全体像

- 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、④NISC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。
- 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、令和6年6月7日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概要

総則 □ 目的規定、基本方針等 (第1章)

官民連携 (強化法)

- 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 (第2章)
 - ・ インシデント報告
- 情報共有・対策のための協議会の設置 (第9章)
- 脆弱性対応の強化 (第42条)
- [その他、雑則(第11章)、罰則(第12章)]

通信情報の利用 (強化法)

- 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 (第3章)
- (同意によらない)通信情報の取得 (第4章、第6章)
- 自動的な方法による機械的情報の選別の実施 (第22条、第35条)
- 関係行政機関の分析への協力 (第27条)
- 取得した通信情報の取扱制限 (第5章)
- 独立機関による事前審査・継続的検査等 (第10章)

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・日本に所在する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)

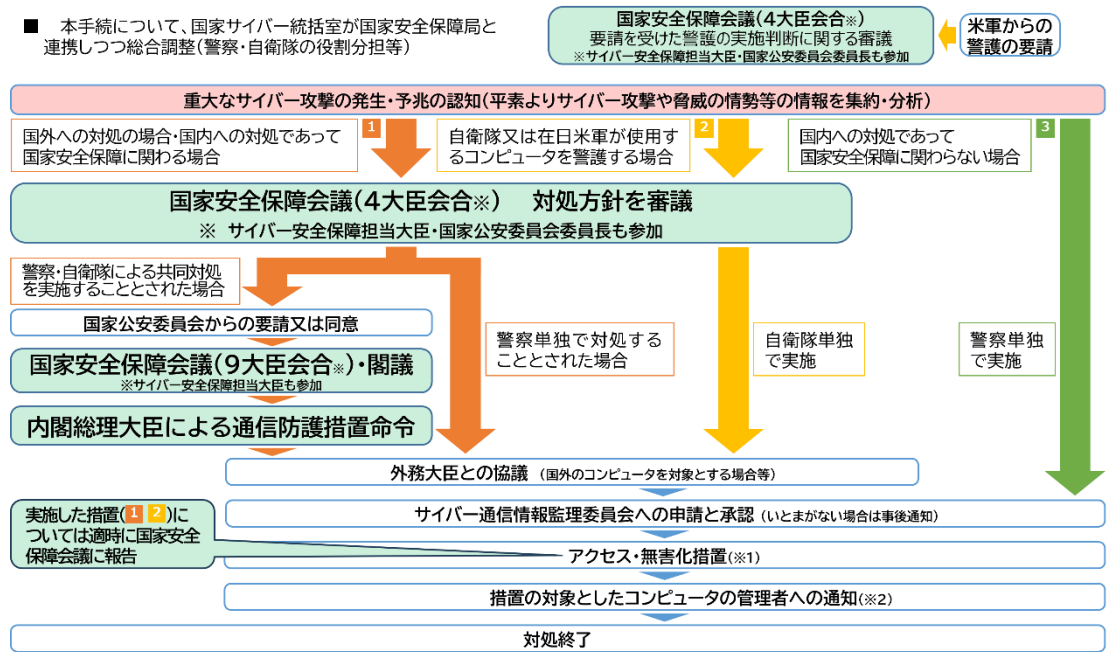
組織・体制整備等 (整備法)

- サイバーセキュリティ戦略本部の改組、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

分析情報・脆弱性情報の提供等 (第8章)

施行期日 公布の日(令和7年5月23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

アクセス・無害化措置の運用の流れ



(※1) 措置の過程で、新たに攻撃に使用されているサーバ等を認めた場合には、必要な手続きを経た上で、当該サーバ等にもアクセス・無害化措置を実施
(※2) 管理者に措置をとることを命じた場合や、当該措置の対象としたコンピュータに開示する危害の防止に支障がある場合及び当該管理者の所在が不明である場合は除く。

出典：内閣官房

内閣官房
ホームページ



NCO
ホームページ



サイバーセキュリティ戦略(令和7年 12 月 23 日) ①

サイバーセキュリティ戦略の全体像

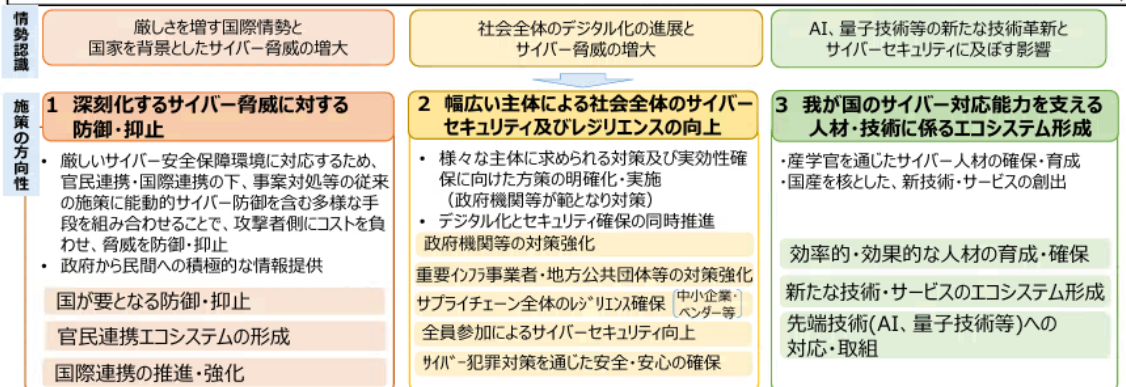
- 「国家安全保障戦略」及びサイバー対処能力強化法等に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、今後5年の期間を念頭に、実施すべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

- サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。
○法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「5つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

(※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」)



官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靭さを持つ国家を目指す。

2

【国が要となる防御・抑止】

アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止国家を背景としたサイバー攻撃キャンペーンを含め、日常的、持続的に行われているサイバー攻撃に対しては、既存の防御の取組と、アクセス・無害化措置を始めとする能動的サイバー防御に係る新たな施策を組み合わせ、多様な手段で粘り強く能動的に対応していく必要がある。そのための体制を早期に確立し、強化を図っていく。具体的には、武力攻撃に至らないものの、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、攻撃者のサーバ等への直接的な働きかけを通じ、攻撃による被害の防止を目的として、国際法上許容される範囲内でアクセス・無害化措置を実施する。この措置は、サイバー攻撃の脅威の抑止にもつながるものであり、我が国の総力を十全に活用する必要があるため、不正プログラムの解析等の高度なフォレンジック能力や、攻撃者やサイバー攻撃の手口等を解明する高度情報分析能力等を有する警察と、武力攻撃事態等における高烈度なサイバー攻撃に対処するための高度なサイバー防衛能力等を有する防衛省・自衛隊が共同して対処する体制を構築する。この措置は国家安全保障の観点から整合性のとれた形で行われ、平素から有事に至るまでシームレスな対応を確保する必要がある。サイバー安全保障担当大臣の下、司令塔組織である国家サイバー統括室が国家安全保障局と連携し

サイバーセキュリティ戦略(令和7年 12 月 23 日) ②

て総合調整機能を発揮し、統一した方針の下で、警察と防衛省・自衛隊が当該措置を適切かつ効率的に実施できる体制を確立する。

【国際連携の推進・強化】

国際共同捜査を引き続き推進し、検挙を通じたサイバー脅威の抑止に向け、インターポール及びユーロポールとの更なる連携強化を含む多国間における捜査機関の協力関係の確立等に積極的に取り組む。

【サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保】

サイバー空間が、あらゆる主体が参画する公共空間へと進化していることを踏まえ、実空間と変わらぬ安全・安心を確保するため、国は、暗号資産、SNS 等のサイバー空間の匿名性を悪用する犯罪者や犯罪者グループ、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

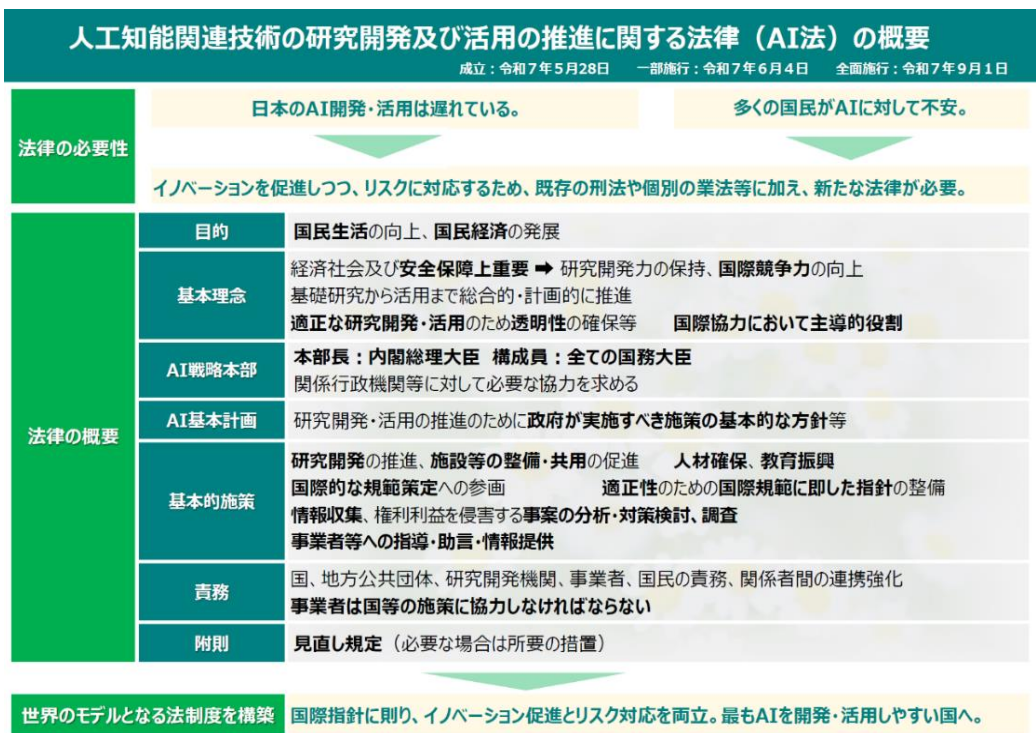
また、重大サイバー事案の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進するとともに、AI 等を悪用した犯罪やランサムウェア等の高度な情報通信技術を用いた犯罪に対処できるよう、捜査能力・技術力の向上に取り組む。

さらに、犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働きかけ等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐほか、情報の共有・分析、被害の防止、人材教育等の観点から、産学官連携の枠組みを活用するなどしたサイバー犯罪対策を推進するとともに、国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯ボランティア等の関係機関・団体と連携し、広報啓発等を推進する。

あわせて、高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化すること等、情報技術の解析に関する態勢を強化する。

こうした取組に加え、国境を越えて敢行されるサイバー事案に適切に対処するため、国は、諸外国における取組状況等を参考にしつつ、関連事業者との協力や外国関係機関との国際連携等必要な取組を推進する。

AI法及びAI基本計画



内閣府
ホームページ

※ 出典：内閣府



● 人工知能基本計画（令和8年7月14日閣議決定）

- 医療・ヘルスケア、介護、金融、教育、警察、・・（略）・・等の各分野において、エージェント型AIの積極導入も含めたバーティカルAIやフィジカルAIを核としたAI開発・実証・導入・社会実装を促進する。
- 国民の安全・安心の確保に向けた警察活動の高度化のためのAI利活用を推進する。
- AI関連のサイバー事案の対処能力の向上など、AIを悪用したサイバー攻撃、詐欺を始めとする各種の犯罪、CBRNEテロを始めとする各種テロ等への対応を図る。
- 高性能AIがもたらす潜在的な機会と深刻なリスクへの対応のため、高性能AIを活用した取組の強化も含めサイバー対処能力を不断に強化する。

バーティカルA I 領域別戦略

バーティカルA I 領域別戦略 中間とりまとめ（概要）

資料 2-1

領域設定の考え方 官民の限られたリソースを戦略的に投資し、効果を最大化することで、社会全体のA Xを実現	
市場性 ：現場力のデータ化・集積と領域特化型基盤モデルの開発・実装により、産業構造改革と国際競争力を強化 公共性 ：官民連携による、A I の徹底活用を通じて、業務の効率化・負担軽減、サービスの質の向上を実現 戦略性 ：計算資源、データプラットフォーム、モデル、アプリ等の自律性確保により、耐遮断性と運用能力を強化	
1. 市場性を有する領域別戦略：産業構造改革、競争力のあるA I システムの創出、海外展開の推進	
● 製造領域：A I ロボティクスや工場等の自動制御A I に貢献するマルチモーダル基盤モデルの開発とデータ連携手法の確立 ● 造船領域：溶接、塗装、曲げ加工等の造船の主要工程を自動化するA I 生産技術システム等の開発・導入 ● 物流・交通領域：物流領域特化モデルの開発と運行管理・遠隔監視・情報管理等に資するデータエコシステムの確立 ● 情報通信領域：通信インフラ等の現場データを連携・活用するバーティカルA I と、A I を支える通信基盤等の整備 ● 金融領域：エージェント型A I やブロックチェーン等を活用した金融ユースケースの創出・横展開の推進 ● 創薬領域：基礎研究から臨床研究、製造工程開発等の創薬の迅速化・高度化に必要なA I 駆動型共用自律ラボ等の整備・運用	
2. 公共性のある領域別戦略：A I で人手不足を解消、我が国の供給力の維持	
● 医療・介護・福祉領域：看護記録等の文書作成や福祉相談業務の支援等の現場の負担軽減のためのA I 開発普及 ● 農林水産領域：農林水産・食品産業の生産性向上のためのA I 開発・実装、データエコシステムの構築・開発基盤整備 ● 建設領域：建設機械等の協調領域のデータセット構築とフィジカルA I への活用による建設施工の自動化・省人化の推進 ● 教育領域：深い学び、多様な児童生徒への対応、教師の働き方改革を実現するためのA I の実装・データ整備 ● 行政領域：ガバナンスA I を通じたA I ネイティブな業務プロセスへの変革とA I 自律性確保、行政データの機械可読性確保 ● エネルギー領域：災害対応や設備監視・点検、系統運用等の協調領域におけるA I 活用に係る業界内連携の推進	
3. 戦略性のある領域別戦略：特定の国や企業への過度な依存を解消	
● 防衛領域：防衛力強化の観点から、データ基盤の強化やA I 実装を進め、迅速かつ的確な意思決定を実現 ● 警察領域：匿名・流動型犯罪グループによる犯罪をはじめ、様々な治安課題への対処等のためのA I 基盤の整備・運用 ● 防災領域：被災者一人一人に寄り添った支援や応急対応、復旧対策等の方針決定・遂行支援へのA I 活用の推進 ● 消防領域：災害現場等の状況を即座に分析し、迅速・的確な判断をA I が支援するための研究開発等の推進 ● サイバー領域：「Project YATA-Shield」の推進、制御系システム等におけるサイバーセキュリティ対策強化 ● 海洋領域：海洋における異常兆候の自動検知やリスク判断を行える領域特化のA I 開発・実装 ● 宇宙領域：地上局を含む宇宙機システム全体の運用を最適化・効率化等、宇宙分野におけるA I 活用の推進 ● 科学研究領域：AI for Scienceの波及や国際・産学連携研究の推進、データ共有強化と研究インフラの一体的構築	
A I 実装能力を共有する観点から、現場記録作成や意思決定支援へのA I 活用、A I ・データ基盤の開発や実装、担い手育成を省庁横断で加速 (令和8年7月10日第5回人工知能戦略本部資料)	

バーティカルA I 領域別戦略中間とりまとめ 警察領域

- **トクリュウ対策の強化**：①特殊詐欺対策アプリについて、A I を活用したリアルタイムでの通話内容の分析等により、自動で詐欺電話を検知・警告・遮断等する機能の新規実装を支援するなど、特殊詐欺対策を強化。②トクリュウに関する膨大な捜査情報について、A I を活用して中核メンバーを含む関連人物等の相関図を自動作成するなどの機能を有する分析システムを整備・高度化。③A I を活用した犯罪関連情報等の自動峻別、不要情報の削除等による解析・分析の更なる高度化。
- **違法・有害情報対策とLO対策の強化**：サイバー空間における大量のオシント情報から違法・有害情報やLO関連投稿等をA I を活用して抽出し、危険度評価等を実施。
- **110番通報・相談対応の高度化**：110番通報やDV・ストーカー関連を含む警察に対する相談について、A I を活用して文字起こし・要約、緊急性評価を含む通報・相談内容の分析等を実施。
- **サイバー対処能力の強化**：A I を活用した資機材や人材育成基盤の導入等によりサイバー対処能力を向上・高度化。
- **大規模災害やテロへの対処能力の強化**：災害現場における要救助者の探索や救出・救助活動、CBRNEテロ現場における情報収集等を支援するA I ロボットを開発・導入。その際、現場の状況把握等のためのバーティカルA I を活用しつつ、将来的なフィジカルA I の開発・活用につなげる。
- **その他の警察業務の高度化・効率化**：被害者や行方不明者等の捜索、雑踏警備、犯罪鑑識、交通取締り、許認可業務、対日有害活動に係る分析、サイバー犯罪捜査でのログ解析、留置管理、擬律判断や指揮命令等、様々な警察活動をバーティカルA I 等を活用して高度化・効率化。
- **警察A I 基盤の整備**：上記施策に係るA I 基盤について、基本的にはクラウド利用環境において整備。また、必要に応じてクラウドサービスも利用しつつ、高度A I 開発のための学習環境も整備。その際、既存システムの有効活用による最適化や関係法令の遵守を前提とした組織横断的なデータ利活用の推進を図るとともに、厳格なセキュリティを確保。研究開発人材や実装人材の育成も推進。

(令和8年7月10日第5回人工知能戦略本部資料)

内閣府
ホームページ



国民を詐欺から守るための総合対策 2.0

「国民を詐欺から守るための総合対策 2.0」の取組状況の概要

内閣官房
ホームページ

1 SNS型投資・ロマンス詐欺対策 / 2 特殊詐欺対策

(1) 犯行準備段階への対策

- 音声通話SIMと異なり、法令により契約時における本人確認が義務付けられていないデータ通信専用SIMについて、本人確認を義務付けること等を内容とする携帯電話不正利用防止法改正案が令和8年5月に成立。
- いわゆる「闇バイト」とは知らずに応募し、自身や家族に危害を加えるなどと脅迫されている者等に対する保護措置を699件講じた（令和6年10月～令和8年5月）。

(2) 着手段階への対策

- 「詐欺対策 by NTTタウンページ」及び「詐欺バスター Lite」の2つの特殊詐欺対策アプリを「警察庁推奨アプリ」に認定し、様々な機関・団体等と連携しながら国民への普及促進に向け、広報啓発を実施するとともに、機能の高度化に向けた取組を協議中。 ※ 両アプリのダウンロード数の累計は、本年5月末時点で1,142,800件
- 事業者に働きかけ、国際電話を休止する国際電話不取扱受付センターの体制強化・処理向上等の取組を実施しているほか、契約変更時に国際電話の要否の確認を実施。 ※ 令和7年中の利用休止手続件数は、約48万件（前年比+約41万件）

(3) 欺罔段階への対策

- SNS型投資詐欺の欺罔手段として、SNSのバナー等広告において著名人のかたが投資を呼びかける手口の増加が顕著であることを踏まえ、当該バナー等広告でかたられている著名人と連携した広報啓発を実施。

(4) 金銭等の交付段階への対策

- 令和7年9月、業界団体等に対し、インターネットバンキングの利用申込時及び利用限度額引き上げ時の確認等を含む対策の強化を要請。同年11月、各金融機関に対し、要請への取組状況に関するフォローアップを実施。
- 預金取扱金融機関における情報共有等の枠組みの創設について、不正利用口座の情報を共有するためのシステム構築費用の補助対象事業者を選定するとともに、令和8年6月、根拠規定の措置等を内容とする犯罪収益移転防止法施行規則等の改正を実施。
- いわゆる「架空名義口座」を利用した新たな措置の創設等を内容とする改正犯罪収益移転防止法が令和8年6月に成立したことを踏まえ、改正法に基づく措置を着実に推進。

(5) 犯行後の捜査段階における対策

- 特殊詐欺事犯の取締りを強力に推進し、令和7年中の検挙件数は7,205件（前年比+367件）、検挙人員は2,735人（前年比+332人）。
- 「仮装身分捜査」を令和7年中に13件実施し、強盗予備、詐欺未遂で4件5名の被疑者を検挙するとともに、これら4件を含む7件の被害防止が図られた。
- 「電気通信事業における個人情報等の保護に関するガイドライン（解説）」を改正し、誹謗中傷をはじめとする違法・有害情報の流通といった社会環境の変化も踏まえ、通信履歴について少なくとも3～6か月程度の保存が望ましいと明記。また、事業者に対応を要請。

3 ID・パスワード等の窃取・不正利用への対策

(1) フィッシングサイトへの対策

- フィッシングサイト判定の高度化・効率化のため、生成AIによる自動判別ツールを導入。

(2) ID・パスワードやクレジットカード情報の不正入手対策

- 日本証券業協会に対する働き掛けを実施し、同協会が定めるインターネット取引における不正アクセス等防止に向けたガイドラインにフィッシングに耐性のある多要素認証（パスキー等）導入等を求める内容を追記。

(3) ID・パスワードやクレジットカード情報の不正利用対策

- 悪用のおそれのあるクレジットカード番号等を集約し、カードの利用停止等の対策に活用するため、国際ブランド各社に一括して提供する枠組みを構築し、令和7年中、約187万件のクレジットカード番号を提供。
- 令和8年7月、E Cサイトにおける不正取引防止等を目的としたE C事業者との情報連携に関する協定を締結。

(4) マネー・ローンダリングや現金化への対策

- 金融機関が、詐欺被害のおそれが高い取引を都道府県警察へ迅速に情報提供する連携体制について、令和8年5月末時点で、47警察本部と938金融機関が、警察庁と全国に顧客を有する都市銀行等30金融機関が情報連携協定を締結。

(5) 犯行後の捜査段階における対策

- サイバー特別捜査部において、暗号資産追跡結果等、都道府県警察から集約した情報について、横断的・俯瞰的に分析。

4 治安基盤の強化等

- 捜査により判明した被疑者に関する情報を東南アジア諸国等の現地当局に提供し、令和7年中、海外拠点に関する特殊詐欺事件の被疑者54人を検挙。
- 令和7年10月、警察庁に匿名・流動型犯罪グループ情報分析室を設置、警視庁には全国警察から捜査員を集めた「匿流ターゲット取締りチーム」（T3）を構築し（令和8年4月に100人を増強）、匿名・流動型犯罪グループの中核的人物の実態解明・取締りを推進。
- サイバー特別捜査部の態勢の増強等を通じて、サイバー空間における取締りを推進。

違法・有害情報に対する通報・相談窓口

インターネット上の書き込みなどに関する相談・通報窓口のご案内

 対面
  電話
  メール
  チャット
  SNS
 左記マーク以外は各機関のWebフォームから相談

インターネット上の誹謗中傷やプライバシー侵害等のトラブルにあった

インターネット上の違法・有害情報を見つけた

解決策について相談したい

悩みや不安について話をしたい

違法薬物の販売情報、
違法なわいせつ画像、
児童ポルノ、
爆発物・銃砲等の製造、
殺人や強盗等の犯罪行為の
請負・仲介・誘引、
自殺の誘引・勧誘などを
通報したい

心のSOS まもろうよこころ (厚生労働省)

www.mhlw.go.jp/mamorouyokokoro

生きるのがつらいほどの悩みや不安を抱えている方に対して、気軽に相談できる窓口を紹介しています。







どうしたらよいか
分からないネット上の
書き込み・画像を
削除したい書き込んだ相手に
損害賠償を
求めたい身の危険を感じている／
脅迫されている・犯人の捜査、
処罰を求めたい弁護士
または

法的トラブル解決のための「総合案内所」 法テラス

0570-078374 www.houterasu.or.jp

問合せ内容に応じて解決に役立つ法制度や相談窓口に関する情報を案内します。経済的に余裕のない方を対象に無料の法律相談や弁護士費用等を立て替える制度があります(要件確認あり)。








サイバー犯罪の情報提供、相談窓口

警察または居住地の
サイバー犯罪相談窓口

www.npa.go.jp/cyber/soudan.html







ネットトラブルの
専門家に
相談したい人権問題の専門機関に
相談したいプロバイダ等に削除を
促してほしい(民間機関)有害情報も
通報したい
(民間機関)

迅速な助言

**違法・有害情報
相談センター
(総務省)**



www.ihaho.jp

相談者自身で行う削除依頼の方法などを迅速にアドバイスします。インターネットに関する技術や制度等の専門知識や経験を有する相談員が、人権侵害に限らず、様々な事案に対して幅広くアドバイスします。



削除要請・助言

**人権相談
(法務省)**



0570-003-110 www.jinken.go.jp

相談者自身で行う削除依頼の方法などの助言に加え、法務局が事案に応じてプロバイダ等に対する削除要請^(注)を行います。

※削除要請は専門的な知見を有する法務局が違法性を判断した上で行うものでありこの判断には時間を要する場合があります。



プロバイダへの連絡

**誹謗中傷
ホットライン**



www.saferinternet.or.jp/bullying/

インターネット上の誹謗中傷について連絡を受け付け、一定の基準に該当すると判断したものについては、国内外のプロバイダに各社の利用規約等に沿った対応を促す連絡を行います。



迅速な削除の要請

セーフライン



www.safe-line.jp

インターネット上の違法情報や有害情報の通報を受け付け、国内外のサイトへの削除の要請や、警察等への通報を行います。リベンジポルノの被害に遭われた方、いじめの動画の通報も受け付けています。



サイトへの削除依頼

**インターネット・
ホットライン
センター(警察庁)**



www.internethotline.jp

インターネット上の違法情報及び重要犯罪密接関連情報、自殺誘引等情報の通報を受け付け、ガイドラインに基づいて該当性の判断を行い、警察への情報提供とサイトへの削除依頼をします。



※上記機関以外に、一般的な情報セキュリティ(主にウイルスや不正アクセス)に関する技術的な相談に対してアドバイスを提供する窓口としてIPA「**情報セキュリティ安心相談窓口**」があります。

※上記のほか、学校や地方公共団体にある相談窓口も活用してください。

サイバー人材の確保・育成 ①

都道府県警察におけるサイバー人材確保・育成方針

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

サイバー人材の確保

- 試験制度の整備・運用**
 - ✓ 一般採用試験の前倒し・複数回実施
 - ✓ 中途・特別・任期付採用制度の整備運用・リボルビングドアの取組
- 効果的な採用募集活動**
 - ✓ 高度人材に対するキャリアパス明示（サイバー特捜部出向等）と活躍実例の広報による魅力発信
 - ✓ IT関連の広報媒体活用や高等専門学校等への学校訪問の推進
 - ✓ 学生対象のサイバーコンテスト開催やサイバー防犯ボランティアの拡大
- 部内のサイバー人材の発掘**
 - ✓ 部内競技会の開催、経歴・資格の把握を通じた内部人材の発掘

サイバー人材の育成

- 必要な能力の明確化と検定による確認**
 - ✓ 全警察官に通報・相談受能力、全捜査員にネットワーク利用犯罪捜査能力、中核サイバー捜査員に高度サイバー事案対処能力を取得させ、検定制により確認
 - ✓ 都道府県警察の昇任試験におけるサイバー関連の出題
- 教養・研修の推進**
 - ✓ 司令塔となる指導・教養班の設置
 - ✓ 専務任用専科等の学校教養におけるサイバー教養の拡充
 - ✓ 警視庁等他都道府県警察への派遣・出向、他部門捜査員のサイバー部門受入れによる職場教養の推進
 - ✓ 民間研修への積極的派遣及び民間委託研修受講・民間資格取得を支援

サイバー人材のキャリアパス管理

- サイバー・警務両部門の緊密な連携**
 - ✓ サイバー・警務両部門を中核に全部門一体となって、中途・特別採用等の高度サイバー人材を含むサイバー人材のキャリアパスを管理
- キャリアパス管理に基づく職員の配置等**
 - ✓ 中途・特別採用のサイバー人材は本部への卒業配置に配慮。昇任配置も希望に応じて配置ポストを検討
 - ✓ 署配置を行う場合は、能力と適性を活かすことができるポストを検討
 - ✓ 高度人材を処遇するためサイバー部門に所要の幹部ポストを整備
 - ✓ 高度サイバー人材を、情報通信部や警察庁サイバー特捜部・サイバー警察局に積極的に出向・派遣

上記方針に基づき本部長の指揮の下すべての都道府県警察が施策を推進

警察庁
ホームページ



情報通信部門におけるサイバー人材確保・育成方針

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

サイバー人材の確保

- 効果的な採用活動の推進**
 - ✓ 中途採用・官民人事交流による高度人材の確保。リボルビングドアの推進
 - ✓ IT求人情報サイト等への募集広告、学校訪問・業務説明会の一層の推進
 - ✓ サイバー人材のキャリアパスを「見える化」し外部にアウトリーチ
 - ✓ 都道府県警察が行うサイバーコンテスト等に積極的に参画
- 部内におけるサイバー人材の発掘**
 - ✓ 警察庁と全国の情報通信部門が一体となって、部内で勤務する職員の経歴・資格について確実に確認
 - ✓ 解析に関する部内競技会の開催その他の取組を通じて、サイバー人材となり得る警察職員を発掘

サイバー人材の育成

- 必要な能力の明確化と確認**
 - ✓ 必要な能力を明確化しつつ、既存の認定制度の根拠を整備
 - ✓ 警察庁サイバー特別捜査部・都道府県警察への異動・出向を念頭に警察官の検定制を活用
 - ✓ 昇任候補者選考においてサイバー関連分野に関する知識を含めて審査
- 教養・研修の推進**
 - ✓ 警察情報通信学校で全ての技官に対する底上げ教養を実施
 - ✓ 都道府県警察や警察庁への出向・異動を通じ職場教養を推進
 - ✓ 留学・民間研修でトップ人材育成
 - ✓ 資格取得に対する支援

サイバー人材のキャリアパス管理

- 警察庁サイバー警察局と長官官房人事課の緊密な連携**
 - ✓ サイバー警察局・長官官房を中核に全情報通信部門一体となって、サイバー人材のキャリアパスを管理
- キャリアパス管理に基づく職員の配置等**
 - ✓ 高度サイバー人材については能力をいかにポストへの配置に配慮
 - ✓ ハイブリッド人材育成の観点から都道府県警察サイバー部門に積極的に出向、情管への出向も検討
 - ✓ 警察庁サイバー警察局・サイバー特別捜査部に長期勤務も念頭に配置、特に優秀な者については幹部ポストに登用

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

警察庁
ホームページ



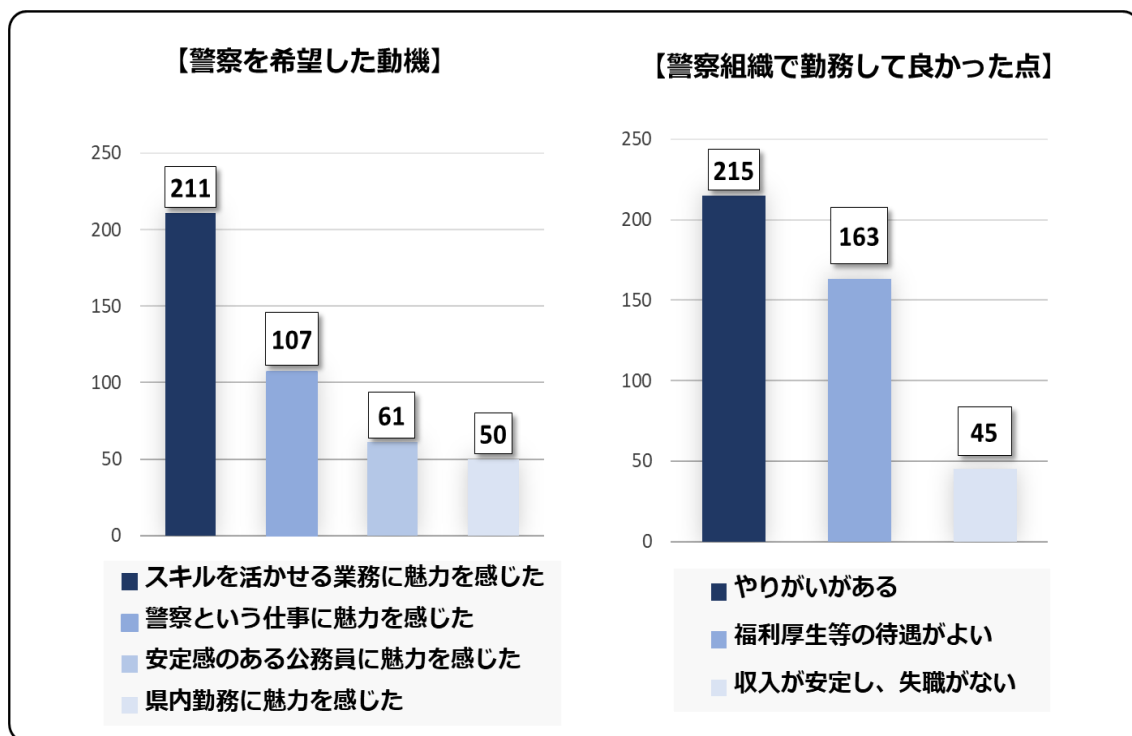
サイバー人材の確保・育成 ②

令和6年9月から10月において、中途採用・特別採用制度により採用された都道府県警察職員に対して、「中途・特別採用に対するキャリアパスに関するアンケート」の調査を実施した。

同アンケートの調査結果では、警察官を希望した動機として、「スキルを活かせる業務に魅力を感じた」と回答する者が多く、実際に勤務を行った後に感じた警察組織で勤務して良かった点として、「警察でしかできない事件捜査等、仕事にやりがいがある」や「知識・技能を活かせる場であり、現在の業務に満足している」など、多くの採用者が警察での仕事にやりがいを感じていた。

都道府県警察においても、警察における具体的な勤務内容を発信するとともに、同人材が活躍できるキャリアパスの構築を推進し、人材確保に取り組んでいる。

【警察におけるサイバー人材アンケート結果】



サイバー人材の確保・育成 ③ ～中途採用・官民人事交流制度により採用された幹部警察官

○ サイバー特別捜査官として採用された幹部警察官

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

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



事件捜査を指揮する
丸山 篤 警視正

○ 官民人事交流制度により採用された幹部警察官

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

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



分析業務に従事する
濱石 佳孝 警視正

「サイバー警察局便り」を活用した情報発信・広報啓発

警察庁では、サイバーセキュリティの向上に資することを目的に、令和4年のサイバー警察局発足後から令和8年6月末までに、計74件の広報啓発資料「サイバー警察局便り」を公表し、広報啓発を行っている。



サイバー警察局便り

Cyber Police Agency Letter

◆ 警察白書にサイバー警察の取組が特集されました	117
◆ 警察への通報・相談を躊躇しないで	118
◆ SNS やメールの乗っ取り・なりすましに注意！！	119
◆ 家庭にある機器が悪用されています	120
◆ あなたの会社のメール、「誰でも名乗れる状態」になっていませんか	121
◆ パスワードだけの認証はもう限界です	122
◆ ランサムウェア被害多発中	123
◆ あなたに役立つ動画があります！	124
◆ SNSなどを運営する大規模プラットフォーム事業者の削除申出窓口があります！	125
◆ 高性能 AI を踏まえたサイバー攻撃対策を！	126
◆ サイバー犯罪捜査官募集中！	127
◆ DDoS 攻撃対策のお願い	128



警察庁サイバー警察局ウェブサイト「サイバー警察局便り」
<https://www.npa.go.jp/bureau/cyber/koho/letter.html>



「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.14 (R8.9)

サイバー警察の取組が特集されました



『令和8年版警察白書』を

警察庁ウェブサイトにおいて公表しました

<https://www.npa.go.jp/publications/whitepaper/r08/index.html>



サイバー攻撃の国際共同捜査に数多く取り組んでいます



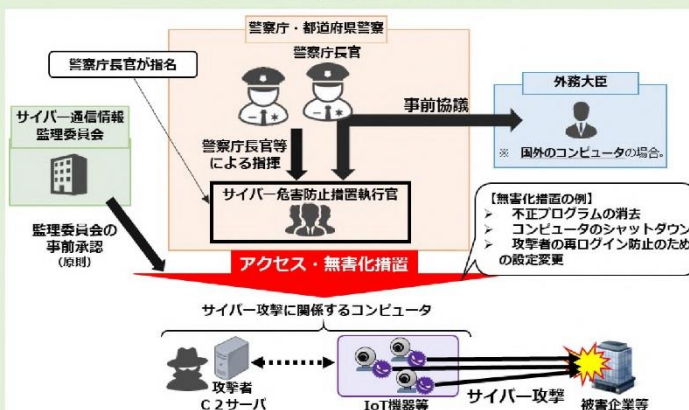
ユーロポール E C 3 オペレーション部長
※令和8年版警察白書8頁から引用

- ・ 国境を越える詐欺やランサムウェア攻撃が多発
- ・ 日本警察は、国際共同捜査を通じた被疑者の検挙や暗号化されたデータの復号に貢献
- ・ 他国の捜査員による日本警察の存在感や特徴についての寄稿も掲載

能動的サイバー防御に三位一体で取り組みます

- ・ アクセス・無害化措置に係る能動的サイバー防御関連法は、**本年10月1日に施行予定**
- ・ アクセス・無害化措置の着実な実施のため、内閣官房・内閣府、警察、防衛省・自衛隊が**三位一体**となった中核的な機能を担う体制を整備

【アクセス・無害化措置の概要】



警察庁
National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.10 (R8.8)

警察への通報・相談を躊躇しないで



会社のパソコンがランサムウェアに感染したようだ。
どのように対応したらいいのか。



取引先名のメールが届き、記載されたリンクにアクセスして
認証情報を入力したが、先方に確認したら「そのような
メールは送っていない」と言われた。



突然パソコンに警告画面が表示され、表示されたサポート
センターに電話したら電子マネーを支払うように言われた。

警察では発生した事件を捜査するだけでなく、
① 被害拡大防止に必要な情報の提供・助言
② 官民連携を通じたサイバーセキュリティ教育
③ サイバー攻撃を想定した合同訓練
等を行っています。

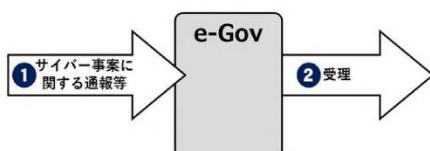


速やかな通報・相談にご協力を

警察では、サイバー事案に関する全国統一のオンライン窓口を
設置しています。



利用者



e-Gov : デジタル庁が運営するポータルサイト



都道府県警察

よくある相談事例も
掲載しています。



※緊急を要するものは、110番に通報してください。

サイバー事案に関する相談窓口

<https://www.npa.go.jp/bureau/cyber/soudan.html>



警察庁

National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.13 (R8.9)

SNSやメールの乗っ取り・なりすましに注意!!

偽

コンビニで電子マネー1万円分買って
その番号教えて

私のSNSアカウントが乗っ取られて
友人宛てにメッセージが送られた!

偽

090●●●●●●●●

【■■■庁】至急のお手続きが必要です。
内容をご確認ください。
<https://example...>

私の携帯電話番号から勝手に
メッセージが送られた!

From: (株) ■■■
件名: 資料のご送付

いつもお世話になっております。
添付の資料を送付いたします。
ご査収いただきますよう、よろしく
お願いいたします。
[資料.zip](#)

(株) ■■■ 担当 ●●

偽

私の会社の従業員になりました
メールが取引先企業に届いた!

■ 乗っ取り防止・早期発見のために

- パスワードを使用する場合は、複雑で推測しにくいものに設定する
- 使用するパスワードは、他のアカウントで使い回さない
- 多要素認証やログイン通知、セキュリティサービスを利用する

■ 乗っ取り被害に遭った時は

- ログインできる場合は、新しいパスワードに変更する
- 自分以外の見覚えのない端末は、全てログアウトする
- アカウントの登録情報や認証方法が変更されていないか確認する

■ 乗っ取り・なりすまし被害に遭った時は

- 交流相手に注意喚起する
- サービス提供会社に相談する

○ 警察に通報・相談する

▶ 最寄りの警察署又はサイバー犯罪相談窓口
<https://www.npa.go.jp/bureau/cyber/soudan.html>



警察庁
National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.9 (R8.8)

家庭にある機器が悪用されています

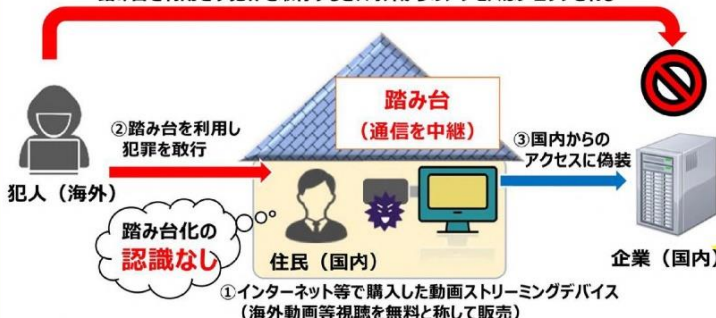
一般家庭で使用されている動画視聴用の端末（「ストリーミングデバイス」）やデジタルフォトフレームなどがサイバー攻撃の踏み台として悪用されています。

このような踏み台となる機器は「**レジデンシャルプロキシ**※」と呼ばれます。

※ 一般家庭向けのネット回線に接続された機器が第三者の通信を中継すること。

「インターネットバンキング不正送金事犯に悪用されたイメージ」

踏み台を利用せず犯罪を敢行すると、海外からのアクセスはブロックされる



「不正送金の手口内訳」



海外からのサイバー攻撃が、国内の個人宅からのアクセスに**偽装される**ため、住民の方に捜査へ御協力いただく場合があります。

あなたの家庭ではいくつ当てはまりますか？

- ☐ 提供元不明のソフトウェア、アプリ、無料VPNを利用している
- ☐ 「収益が得られます」と宣伝するサービスやアプリを利用している
- ☐ 無料で動画が見られるストリーミングデバイスを使用している
- ☐ 購入してから一度も更新を行っていない古いIoT機器※を使用している

※ インターネットに繋がる機器のこと。

みんなで悪用を防ぐために必ずチェック

警察庁、総務省、NICTではウェブサイトにおいて、「家庭用IoT機器を悪用するレジデンシャルプロキシの現状」を公開しました。

「家庭用IoT機器を悪用したサイバー攻撃への官民一体となった対策の推進について」
<https://www.npa.go.jp/bureau/cyber/koho/news/residentialproxy.html>

警察庁
National Police Agency総務省
Ministry of Internal Affairs and CommunicationsNICT
国立研究開発法人
情報通信研究機構日本サイバー犯罪
対策センター

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.11 (R8.9)

あなたの会社のメール、
「誰でも名乗れる状態」になっていませんか？
DMARCは、自社ドメインを悪用したなりすましメールから
顧客・取引先・自社ブランドを守る仕組みです。

郵便局にたとえるDMARCの仕組み

① 住所・封蝋確認 (SPF・DKIM認証)



郵便局員が、送り主の住所に紐
付く氏名と封蝋（印）を確認。
(送信元IP・電子署名の検証)

② 名義の照合 (アライメント確認)



送り主の氏名と、郵便局が持つ
送り主リストを照合。
(送信元ドメインの検証)

③ 怪しい手紙に対応 (ポリシー処理)



異常発見時は、定めたマニユア
ルに沿って厳正に対応。

③の対応（ポリシー設定）

① None（記録のみ）



記録し、宛先に送付
(=顧客が受信)

② Quarantine（隔離）



不審物として保管
(=顧客の迷惑フォルダへ)

③ Reject（拒否）



配達しない
(=顧客に届かない)

DMARC導入の 主なメリット

顧客・取引先の保護



なりすましによる詐欺や
情報漏えいを防止

ブランド・信頼の維持



自社ドメインの悪用を防ぎ、
企業イメージを守る

メール到達性の向上



迷惑メール判定を減らし、
自社メールを届きやすく

今すぐ
チェック！

設定が「None（記録のみ）」のまま放置されていませんか？

- ☐ DMARCポリシーの設定（Noneのままか？）を確認する。
- ☐ レポートを確認し、自社ドメインを名乗るメールを把握する。
- ☐ 把握できたら、Quarantine又はRejectへの移行を検討する。



警察庁
National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.12 (R8.9)

パスワードだけの認証はもう限界です。

自社サービスにパスキーを導入し、
安全で快適なログインを実現しましょう！



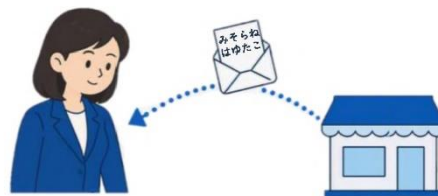
手紙のやり取りにたとえるパスキーの仕組み

① 印鑑作成 (鍵ペア作成)



利用者が印鑑を作成し、金庫に保管。
印影をサービス事業者へ提出。
(印鑑=秘密鍵、印影=公開鍵、金庫=スマホ)

② 手紙の送付 (認証要求)



サービス事業者がランダムな文字列の手紙を送付。
(チャレンジ送信)

③ 手紙に押印 (本人確認・電子署名)



利用者が顔認証や指紋認証を行い、
金庫から印鑑を取り出して押印。

④ 印鑑の照合 (署名検証)



サービス事業者が
・ 登録済の印影と一致するか
・ 手紙の内容が②と一致するかを確認。

パスキー導入の 主なメリット

漏えいリスク低減



秘密鍵は端末の安全な領域に保存
されるため、漏えい被害を抑制

ブランド・信頼の維持



偽サイトでは認証できないため、
自社ブランドの悪用を防ぎ、
企業イメージを守る

利用者満足度の向上



パスワード入力不要。
顔認証・指紋認証ですぐログイン



パスワードから、パスキーへ。

パスワード漏えいやフィッシングのリスクから利用者を守るために。
より安全な認証方式として、パスキーの導入を御検討ください。



警察庁

National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.15 (R8.3)

⚠️ ランサムウェア被害 多発中 ⚠️

👉 令和7年は国内で**226件**の被害を認知

👉 大規模被害も発生し、市民生活に影響



政府広報

で対策情報公開中

✅ 政府広報オンライン記事

「ランサムウェア、あなたの会社も標的に？
被害を防ぐためにやるべきこと」

<https://www.gov-online.go.jp/article/202210/entry-10263.html>



✅ 政府広報オンライン動画

「中小企業で被害多数 ランサムウェア」

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



✅ 政府広報オンライン動画

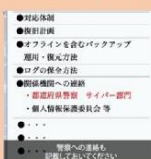
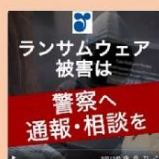
「ランサムウェア対策の基本」

<https://www.gov-online.go.jp/vertical/online/video-478.html>



✅ 政府広報公式SNSでも関連動画を公開中

X



https://x.com/gov_online/status/1980906976910467369

Instagram



<https://www.instagram.com/reel/DKiqpIGTUCM/>

サイバー攻撃発生時の調査に関する資料が公開されました

✅ 「不正アクセス発生時のフォレンジック調査の有効活用
に向けた着眼点」 (個人情報保護法サイバーセキュリティ連絡会)

https://www.ppc.go.jp/files/pdf/260116_forensics_keypoints.pdf



警察庁
National Police Agency



2月1日から3月18日は
「サイバーセキュリティ月間」
<https://security-portal.cyber.go.jp/cybersecuritymonth/2026/>

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.16 (R8.3)

あなたに役立つ動画があります！

PCやスマホに警告画面が出て慌てないで！
「サポート詐欺」にご注意



<https://www.gov-online.go.jp/prg/prg27221.html>

詳しくは、
政府広報オンライン
をご覧ください！



政府広報

『闇バイト』の真実
高額報酬をうたう犯罪実行役の募集
#SNS#実行犯



<https://www.gov-online.go.jp/prg/prg27114.html>



<https://www.gov-online.go.jp/article/202507/tv-6049.html>

スマートフォンのセキュリティ対策できていますか？

4つのポイント



<https://www.gov-online.go.jp/prg/prg25924.html>

サイバー防御



<https://www.gov-online.go.jp/article/202507/tv-6037.html>



警察庁
National Police Agency

2月1日から3月18日は
「サイバーセキュリティ月間」

<https://security-porta.cyber.go.jp/cybersecuritymonth/2026/>



「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.14 (R8.2) ※R8.5更新

SNSなどを運営する大規模プラットフォーム事業者の 削除申出窓口があります！

SNSに、誹謗中傷の
投稿をされた。



掲示板サイトに、個人
情報を書き込まれた。

このような情報を削除してもらいたい

「**情報流通プラットフォーム対処法***」で、大規模プラットフォーム事業者に対して、インターネット上の誹謗中傷等に関する**削除申出窓口の公表**等が義務付けられました。

大規模プラットフォーム事業者の主な義務

- **削除申出窓口の整備・公表**
権利侵害情報の削除申出窓口を定めて、公表する義務
- **侵害情報に関する調査の実施**
権利侵害に当たるか、遅滞なく必要な調査を行う義務
- **申出者に対する通知**
申出に対して、原則7日間以内に措置の有無等を通知する義務

削除申出の流れ



大規模プラットフォーム事業者の削除申出窓口及び削除基準は**こちら**

(X Corp. (X)、Meta Platforms, Inc. (Facebook、Instagram、Threads) 等)

(総務省ウェブサイト)



具体的な削除依頼の手順については**こちら**も御参照ください
(法務省ウェブサイト)

※ 特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（平成13年法律第137号）



警察庁
National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 号外 (R8.6)

事業者向け資料

高性能AIを踏まえたサイバー攻撃対策を！

AIの性能が急速に向上

セキュリティ対策に活用
⇒ 脆弱性の発見や
修正の高速化



攻撃者による悪用
⇒ 高速・大規模な
サイバー攻撃



変化に備えた対策強化が必要



政府において

「Project YATA-Shield※」

を策定



「Project YATA-Shield」概要資料
(国家サイバー統括室ウェブサイト)
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf



「重要インフラ事業者等に対する注意喚起」
(国家サイバー統括室ウェブサイト)
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Critical_Infrastructure.pdf

YATA: Yielding Advanced Threat Awareness with AI (脅威の可視化) の頭文字。
「正確に写す」という八咫鏡(やたのかがみ)もあるように「AI性能の高度化に伴うサイバー脅威を正しく認識し、防御する/対応する」という趣旨

重要インフラ事業者等に対し、次のような注意喚起※を実施中



「サイバーセキュリティ経営ガイドライン」
(経済産業省ウェブサイト)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経営層のリーダーシップ※の下、対策を実施

組織のリスクマネジメントとして、必要な投資と捉え、対策を実施

基本的な対策の確実な実施

策定予定の重要インフラ統一基準※を踏まえ

資産管理、脆弱性対策、インシデント対応・復旧などを実施

高速化する脆弱性の発見・修正に速やかに対応

脆弱性のリスク評価、パッチ適用、リスク緩和措置の速やかな実施



「重要インフラ統一基準(案)」
(国家サイバー統括室ウェブサイト)
https://www.cyber.go.jp/policy/group/infra/pubcom_jyuhurakijun2026.html



被害に遭ったら、警察に通報・相談を！



警察庁
National Police Agency



国家サイバー統括室
National Cybersecurity Office

「サイバー警察局便り」を活用した情報発信・広報啓発



サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.1 (R8.4) ※R8.9更新

サイバー犯罪捜査官 募集中！

全国の約3,700人がサイバー空間の脅威への対処に専従
全国で『サイバー犯罪捜査官』が活躍中

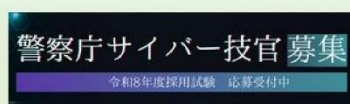


即戦力として

中途・特別採用された都道府県の
警察官・警察職員は 計約490人



採用募集
リンク



警察庁ではサイバー事案の対処に
専門的に従事する
『サイバー技官』を採用

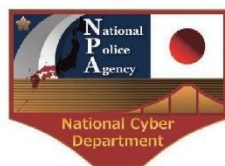


採用募集リンク



紹介動画リンク

全国のトップ人材が
『サイバー特別捜査部』
で活躍



サイバー警察の取組
令和8年上半年における
サイバー空間をめぐる
脅威の情勢等について

※人数は令和8年4月1日現在

全国のサイバー犯罪捜査官による活躍事例



サイバー犯罪捜査官は
各種メディアで
取り上げられています！



YouTubeリンク



Googleニュースリンク

※リンク先は令和8年8月31日以前の検索結果



警察庁
National Police Agency

「サイバー警察局便り」を活用した情報発信・広報啓発

DDoS攻撃対策のお願い



- 令和6年から7年の年末年始にかけ、交通・金融機関などの重要インフラ事業者において、**DDoS攻撃が相次いで発生**しました。
- これらの攻撃の特徴を基に、**対策をまとめましたので確認をお願いします。**

攻撃の特徴

- ✓ **長時間**にわたる攻撃&**サービス提供に影響する部分**を集中的に狙う
 - ✓ **オリジンサーバのIPアドレスを直接標的に**することで、CDNを回避
 - ✓ 対策の状況を観測し、**攻撃手法を変化**
 - ✓ 最大で**220Gbps**の大規模なDDoS攻撃
 - ✓ ぜい弱性を放置&サポート切れの**無線ルータやIPカメラなどを踏み台**に利用
- ➡ **攻撃リスク低減&攻撃を想定した対策が必要！！**

対策

※セキュリティ担当者の方向けの内容となります。

🔑 **アクセスを監視し攻撃を検知・遮断する機能を持つ対策装置やサービスの導入**

🔑 **各種機器のDDoS攻撃対策の設定の再確認**

- ・オリジンサーバに対するCDNを経由しないアクセスの遮断
- ・組織外にオリジンサーバのIPアドレスが露見しないDNS設定の見直し
- ・複数の対策による攻撃への耐性確認

🔑 **サーバ装置、端末、通信回線装置及び通信回線の冗長化**

🔑 **本社・支社使用のIoT機器の再確認**（踏み台としての悪用防止）

- ・ぜい弱性の解消のためのファームウェアの更新
- ・ぜい弱性の解消のためのパッチの適用
- ・サポート切れになっていないか等の再確認

DDoS攻撃が発生した場合に警察への相談・通報ができるよう、あらかじめ攻撃発生時の対応要領やBCPの確認をお願いします。

参考資料

サイバー警察局便り（R5 Vol.20）IoT機器への注意喚起【警察庁】
<https://www.npa.go.jp/bureau/cyber/pdf/Vol.20cpal.pdf>



サイバー部門の変遷

H8.4	警察庁長官官房にネットワークセキュリティ対策室を設置。
H10.6	「ハイテク犯罪対策重点プログラム」を策定。
H11.4	警察庁情報通信局に技術対策課を設置。
H11.8	不正アクセス行為の禁止等に関する法律の成立・公布。
H12.2	「警察庁情報セキュリティ政策大系」を策定。
H16.4	警察庁生活安全局に情報技術犯罪対策課を設置し、警察庁情報通信局の技術対策課を情報技術解析課に改組。
H23.6	刑法の一部が改正。不正指令電磁的記録に関する罪が新設。
H23.10	「サイバー空間の脅威に対する総合対策推進要綱」を策定。
H24.7	警察庁長官官房審議官（サイバーセキュリティ戦略担当）を設置。
H25.1	「サイバー犯罪対処能力の強化等に向けた緊急プログラム」を策定。
H25.5	警察庁警備局警備企画課にサイバー攻撃対策官を設置。
H26.4	警察庁長官官房審議官（サイバーセキュリティ戦略担当）の担務を「サイバーセキュリティ」に変更するとともに、長官官房参事官（サイバーセキュリティ担当）を設置。 警察大学校にサイバーセキュリティ研究・研修センターを設置。
H27.9	「警察におけるサイバーセキュリティ戦略」を策定。
R4.4	警察庁サイバー警察局を設置。 警察庁関東管区警察局にサイバー特別捜査隊を設置。
R6.4	サイバー特別捜査隊をサイバー特別捜査部に発展的改組。
R7.4	サイバー特別捜査部に特別対処課を設置。 警察大学校にサイバー警察教養部を設置。
R8.4	「警察におけるサイバー戦略」を改定。
R8.5	警察法施行令の一部を改正。都道府県警察本部の内部組織の基準にサイバー警察部に関する規定等を整備

インターネット・ホットラインセンターの変遷

H18.3	総合セキュリティ対策会議において、インターネット上の違法・有害情報への対応を効果的かつ効率的に推進していくためにはホットラインの導入が必要である旨の提言。
H18.6	インターネット・ホットラインセンター運用開始。 【違法情報】：「わいせつ情報」、「薬物関連情報」、「振り込め詐欺等関連情報」 【有害情報】：「情報自体から、違法行為を直接的かつ明示的に請負・仲介・誘因等する情報」、「違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報」、「人を自殺に勧誘・誘引する情報」
H24.7	不正アクセス禁止法改正に伴い、「不正アクセス関連情報」を違法情報に追加。
H28.3	平成 24 年度行政事業レビューにおける事業仕分け等により、平成 28 年度からは、有害情報は民間の自主的対応によることとされたことを踏まえ、有害情報に係る事業を終了。
H30.1	平成 29 年 10 月に発覚した神奈川県座間市における殺人事件を受け、有害情報に係る事業を再開。「自殺誘引等情報」を有害情報に追加。
R5.2	令和 4 年 7 月に発生した元内閣総理大臣殺害事件を受け、「重要犯罪密接関連情報」を有害情報に追加。
R5.9	「闇バイト」に応募した者らによる凶悪事件発生を受け、「犯罪実行者募集情報」を有害情報たる重要犯罪密接関連情報の一類型として追加。
R7.2	・無登録貸金業者の広告排除に向けた対策の強化が求められたことを踏まえ、「無登録貸金業関連情報」を違法情報に追加。 ・銃刀法改正に伴い、「銃砲等所持関連情報」を違法情報に追加。 ・令和 6 年 12 月の犯罪対策閣僚会議において決定した緊急対策に基づき、「犯罪実行者募集情報」を有害情報から違法情報に変更。
R7.9	ギャンブル等依存症対策基本法改正に伴い、「違法オンラインギャンブル等関連情報」を違法情報に追加。
R8.8	・「詐欺及びスティーカー被害拡大防止のための緊急対策」を踏まえ、「なりすまし型偽投資広告を掲載する行為」を違法情報に追加。

警察法施行令・警察庁組織令

【警察法施行令（昭和二十九年政令第百五十一号）】

（警視庁及び道府県警察本部並びに方面本部の内部組織の基準）

第四条 法第四十七条第四項に規定する警視庁及び道府県警察本部の内部組織の基準は、別表第一のとおりとする。

2 （略）

3 警視庁及び道府県警察本部並びに方面本部の内部組織を定めるに当たつては、前二項の基準に従うほか、当該都道府県の知事の直近下位の内部組織又は直近下位以外の内部組織との権衡を考慮するものとする

別表第一（第四条関係）

警視庁及び道府県警察本部の内部組織の基準

第一 部の名称及び所掌事務

一 警務部

イ タ （略）

レ 警察教養に関すること。

ソ ム （略）

ウ サイバー事案（法第五条第四項第六号ハに規定するサイバー事案をいう。以下この表において同じ。）に関する警察に関すること。

二 生活安全部

イ 犯罪、事故その他の事案に係る市民生活の安全と平穩に関すること。

ロ ハ （略）

ニ 犯罪の予防に関すること。

ホ （略）

ヘ 保安警察に関すること。

三・四 （略）

五 警備部

イ 警備警察に関すること。

ロ ト （略）

第二 （略）

第三 人口、犯罪発生状況その他の事情により必要があるときは、第一の基準にかかわらず、第一各号に掲げる部のほか、警務部の所掌事務（サイバー事案に関する警察に関することを除く。）の一部を所掌する総務部、サイバー事案に関する警察に関することを所掌するサイバー警察部、地域警察その他の警らに関することを所掌する地域部、警備警察に関することを所掌する公安部その他第一各号の部の所掌事務の一部を所掌する部を置き、又は部の名称若しくは所掌事務を変更することができる。

第四 （略）

【警察庁組織令（昭和二十九年政令第百八十号）】

（サイバー警察局の分課）

第四十四条 サイバー警察局に、次の三課を置く。

サイバー企画課

サイバー捜査課

情報技術解析課

（サイバー企画課）

第四十五条 サイバー企画課においては、次の事務をつかさどる。

一 一局の所掌に係る警察（以下この条において「サイバー警察」という。）に関する制度及びサイバー警察の運営に関する企画及び立案に関すること。

二 サイバー事案の防止対策一般に関すること。

三 局の事務の総合調整に関すること。

四 サイバー警察に関する法令の調査及び研究に関すること。

五 サイバー警察に関する資料及び情報の収集、整理及び分析に関すること。

六 サイバー警察に関する国際会議その他の国際的な枠組み及び外国の行政機関その他の関係機関との連絡調整に関すること（サイバー捜査課の所掌に属するものを除く。）。

七 前各号に掲げるもののほか、局内の他の所掌に属しないこと。

（サイバー捜査課）

第四十六条 サイバー捜査課においては、次の事務をつかさどる。

一 サイバー事案に係る犯罪の捜査に関すること。

二 サイバー事案に係る犯罪の取締りに関する外国の警察行政機関との連絡に関すること。

（情報技術解析課）

第四十七条 情報技術解析課においては、次の事務をつかさどる。

一 犯罪の取締りのための情報技術の解析に関すること。

二 サイバー事案の防止対策に関する事務のうち技術に関すること

（管区警察局の内部組織）

第四十八条 管区警察局には、関東管区警察局及び近畿管区警察局を除き、総務監察・広域調整部及び情報通信部を置く。

2 関東管区警察局には、総務監察部、広域調整部、サイバー特別捜査部及び情報通信部を置く。

3 5 （略）

警察法

【警察法（昭和二十九年法律第六十二号）】

（任務及び所掌事務）

第五条 国家公安委員会は、国の公安に係る警察運営をつかさどり、警察教養、警察通信、情報技術の解析、犯罪鑑識、犯罪統計及び警察装備に関する事項を統轄し、並びに警察行政に関する調整を行うことにより、個人の権利と自由を保護し、公共の安全と秩序を維持することを任務とする。

2・3 （略）

4 国家公安委員会は、第一項の任務を達成するため、次に掲げる事務について、警察庁を管理する。

一〇五 （略）

六 次のいずれかに該当する広域組織犯罪その他の事案（以下「広域組織犯罪等」という。）に対処するための警察の態勢に関すること。

イ・ロ （略）

ハ サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第四号）第二条に規定するサイバーセキュリティをいう。）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（以下この号及び第二十五条第一号において「サイバー事案」という。）のうち次のいずれかに該当するもの（第十六号及び第六十一条の三において「重大サイバー事案」という。）

(1) 次に掲げる事務又は事業の実施に重大な支障が生じ、又は生ずるおそれのある事案

i 国又は地方公共団体の重要な情報の管理又は重要な情報システムの運用に関する事務

ii 国民生活及び経済活動の基盤であつて、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業

(2) 高度な技術的手法が用いられる事案その他のその対処に高度な技術を要する事案

(3) 国外に所在する者であつてサイバー事案を生じさせる不正な活動を行うものが関与する事案

七〇十五 （略）

十六 重大サイバー事案に係る犯罪の捜査その他の重大サイバー事案に対処するための警察の活動に関すること。

十七〇十九 （略）

二十 犯罪の取締りのための電子情報処理組織及び電磁的記録（電子的方式、磁気的方式その他の人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。）の解析その他情報技術の解析に関すること。

二十一〇二十七 （略）

五〇七 （略）

（サイバー警察局の所掌事務）

第二十五条 サイバー警察局においては、警察庁の所掌事務に関し、次に掲げる事務をつかさどる。

一 サイバー事案に関する警察に関すること。

二 犯罪の取締りのための情報技術の解析に関すること。

（関東管区警察局の所掌事務の特例）

第三十条の二 前条の規定にかかわらず、関東管区警察局は、全国を管轄区域として、警察庁の所掌事務のうち第五条第四項第十六号に掲げるものに係るものを分掌する。

（警視庁及び道府県警察本部）

第四十七条 都警察の本部として警視庁を、道府県警察の本部として道府県警察本部を置く。

2〇三 （略）

4 警視庁及び道府県警察本部の内部組織は、政令で定める基準に従い、条例で定める。

（広域組織犯罪等に対処するための措置）

第六十一条の三 （略）

2 （略）

3 長官は、重大サイバー事案について警察庁と都道府県警察が共同して処理を行う必要があると認めるときは、当該重大サイバー事案の処理に関する方針を定め、警察庁又は関係都道府県警察の一の警察官（第六十条第一項の規定による援助の要求又は第一項の規定による指示により派遣された者を含む。）に、当該重大サイバー事案の処理に関し、当該方針の範囲内で、警察庁及び関係都道府県警察の警察職員に対して必要な指揮を行わせることができる。

4 第一項の規定による指示により重大サイバー事案の処理に関して警察庁に派遣された都道府県警察の警察官は、国家公安委員会の管理の下に、当該重大サイバー事案の処理に必要な限度で、全国において、職権を行うことができる。

警察官職務執行法

- 害関係電子計算機から重要電子計算機（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第四十二号）第二条第二項に規定する重要電子計算機をいう。）に対してその機能に重大な障害を生じさせ、又は生じさせるおそれのある加害関係電気通信が現に送信されている場合その他の当該危害防止のためにはサイバー通信情報監理委員会の承認を得るいとまがないと認める特段の事由がある場合は、この限りでない。
- 5 第三項に規定する場合における前項の承認の求めは、第三項の規定による協議の結果を添えて行わなければならない。
- 6 サイバー通信情報監理委員会は、第四項の承認の求めがあつた場合において、当該求めが第二項及び第三項の規定に照らして適切であると認めるときは、当該承認をするものとする。
- 7 サイバー危害防止措置執行官は、第二項の規定による処置をとるに際しては、みだりに関係者の正当な業務を妨害してはならない。
- 8 サイバー危害防止措置執行官は、第二項の規定による処置をとつたときは、当該加害関係電子計算機の管理者に同項に規定する措置をとることを命じた場合を除き、国家公安委員会規則で定めるところにより、遅滞なく、その旨を当該管理者に通知するものとする。ただし、当該加害関係電子計算機に関係する危害の防止に支障がある場合及び当該管理者の所在が不明である場合は、この限りでない。
- 9 サイバー危害防止措置執行官は、第四項ただし書の規定によりサイバー通信情報監理委員会の承認を得ないで第二項の規定による処置をとつたときは、速やかに、当該処置についてサイバー通信情報監理委員会に通知しなければならない。
- 10 前項の規定による通知を受けたサイバー通信情報監理委員会は、当該通知に係る処置が第二項、第三項及び第四項ただし書の規定に照らして適切に行われたかどうかを確認し、第二項の規定による処置に係る事務の適正な実施を確保するため必要があると認めるときは、当該承認の結果に基づき、当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）に対し、必要な措置をとるべきことを勧告するものとする。
- 11 サイバー危害防止措置執行官は、この条の規定による措置の実施について、警察庁長官等（第三項に規定する場合にあつては、警察庁長官）の指揮を受けなければならない。

警察官職務執行法

【警察官職務執行法（昭和二十三年法律第百三十六号）】

（サイバー危害防止措置執行官による措置）

第六条の二 警察庁長官は、警察庁又は都道府県警察の警察官のうちから、次項の規定による処置を適正にとるために必要な知識及び能力を有すると認められる警察官をサイバー危害防止措置執行官として指名するものとする。

2 サイバー危害防止措置執行官は、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為（以下この項において「情報技術利用不正行為」という。）に用いられる電気通信若しくはその疑いがある電気通信（以下この項及び第四項ただし書において「加害関係電気通信」という。）又は情報技術利用不正行為に用いられる電磁的記録（電子的方式、磁気的方式その他の人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。以下この項において同じ。）若しくはその疑いがある電磁的記録（以下この項において「加害関係電磁的記録」という。）を認めた場合であつて、そのまま放置すれば人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、加害関係電気通信の送信元若しくは送信先であ

る電子計算機又は加害関係電磁的記録が記録された電子計算機（以下この条において「加害関係電子計算機」と総称する。）の管理者その他関係者に対し、加害関係電子計算機に記録されている加害関係電磁的記録の消去その他の危害防止のため通常必要と認められる措置であつて電気通信回線を介して行う加害関係電子計算機の動作に係るもの（適切に危害防止を図るために通常必要と認められる限度において、電気通信回線を介して当該加害関係電子計算機に接続して当該加害関係電子計算機に記録されたその動作に係る電磁的記録を確認することを含む。）をとることを命じ、又は自らその措置をとることができる。

3 加害関係電子計算機が国内に設置されていると認める相当な理由がない場合における当該加害関係電子計算機の動作に係る前項の規定による処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該サイバー危害防止措置執行官は、あらかじめ、警察庁長官を通じて、外務大臣に協議しなければならない。

4 サイバー危害防止措置執行官は、第二項の規定による処置をとる場合には、あらかじめ、サイバー通信情報監視委員会の承認を得なければならない。ただし、当該加

自衛隊法

じ。）」と、「情報技術利用不正行為に」とあるのは「当該特定不正行為に」と、同条第三項中「処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該」とあるのは「処置をとる」と、「警察庁長官」とあるのは「防衛大臣」と、同条第四項中「あらかじめ」とあるのは「あらかじめ、防衛大臣を通じて」と、同項ただし書中「重要電子計算機（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第四十二号）第二条第二項に規定する重要電子計算機をいう。）」とあるのは「重要電子計算機」と、同条第八項中「国家公安委員会規則」とあるのは「防衛省令」と、「その旨を」とあるのは「その旨を部隊等の長を通じて」と、同条第九項中「サイバー通信情報監理委員会に」とあるのは「防衛大臣を通じてサイバー通信情報監理委員会に」と、同条第十項中「当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）」とあり、及び同条第十一項中「警察庁長官等（第三項に規定する場合にあつては、警察庁長官）」とあるのは「防衛大臣」と読み替えるものとする。

（自衛隊等が使用する特定電子計算機の警護のための権限）
第九十五条の四 警察官職務執行法第六条の二第二項から第十項までの規定は、次に掲げる特定電子計算機（不正アクセス行為の禁止等に関する法律（平成十一年法律第二百二十八号）第二条第一項に規定する特定電子計算機をいう。）をサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第四百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為から職務上警護する自衛官の職務の執行について準用する。この場合において、警察官職務執行法第六条の二第二項中「サイバーセキュリティ」とあるのは、「自衛隊法（昭和二十九年法律第百

六十五号）第九十五条の四第一項各号に掲げる特定電子計算機（第四項ただし書において「特定電子計算機」という。）に対するサイバーセキュリティ」と、「情報技術利用不正行為に」とあるのは「当該情報技術利用不正行為に」と、同条第三項中「処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該」とあるのは「処置をとる」と、「警察庁長官」とあるのは「防衛大臣」と、同条第四項中「あらかじめ」とあるのは「あらかじめ、防衛大臣を通じて」と、同項ただし書中「に対し」とあるのは「である特定電子計算機に対し」と、同条第八項中「国家公安委員会規則」とあるのは「防衛省令」と、「その旨を」とあるのは「その旨を部隊等の長を通じて」と、同条第九項中「サイバー通信情報監理委員会に」とあるのは「防衛大臣を通じてサイバー通信情報監理委員会に」と、同条第十項中「当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）」とあり、及び同条第十一項中「警察庁長官等（第三項に規定する場合にあつては、警察庁長官）」とあるのは「防衛大臣」と読み替えるものとする。

一 自衛隊が使用する特定電子計算機

二 日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の軍隊が使用する特定電子計算機

2 前項第二号に掲げる特定電子計算機に対する同項の警護は、アメリカ合衆国の軍隊から要請があつた場合であつて、防衛大臣が必要と認めるときに限り、自衛官が行うものとする。

自衛隊法

【自衛隊法（昭和二十九年法律第百六十五号）】

（自衛隊の任務）

第三条 自衛隊は、我が国の平和と独立を守り、国の安全を保つため、我が国を防衛することを主たる任務とし、必要に応じ、公共の秩序の維持に当たるものとする。

2・3 （略）

（重要電子計算機に対する通信防護措置）

第八十一条の三 内閣総理大臣は、重要電子計算機に対する特定不正行為（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第四十二号）第二条第四項に規定する特定不正行為をいい、電気通信回線を介して行われるものに限る。以下この項及び第四項第一号において同じ。）であつて、本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、次の各号のいずれにも該当することにより自衛隊が対処を行う特別の必要があると認めるときは、部隊等に当該特定不正行為（当該特定不正行為を行つた者による同種の特定不正行為を含む。第一号において同じ。）による当該重要電子計算機への被害を防止するために必要な電子計算機の動作に係る措置であつて電気通信回線を介して行うもの（以下この条及び第九十一条の三において「通信防護措置」という。）をとるべき旨を命ずることができる。

- 一 当該特定不正行為により重要電子計算機に特定重大支障（重要電子計算機の機能の停止又は低下であつて、当該機能の停止又は低下が生じた場合に、当該重要電子計算機に係る事務又は事業の安定的な遂行に容易に回復することができない支障が生じ、これによつて国家及び国民の安全を著しく損なう事態が生ずるものという。次号において同じ。）が生ずるおそれ大きいと認めること。
- 二 特定重大支障の発生を防止するために自衛隊が有する特別の技術又は情報が必要不可欠であること。

3 国家公安委員会からの要請又はその同意があること。

2 （略）

3 第一項の規定により通信防護措置をとるべき旨を命ぜられた部隊等は、警察庁又は都道府県警察（次項第四号において「警察庁等」という。）と共同して当該通信防護措置を実施するものとする。

4 内閣総理大臣は、第一項の規定により部隊等に通信防護措置をとるべき旨を命ずる場合には、あらかじめ、防衛大臣と国家公安委員会との間で協議をさせた上で、次に掲げる事項を指定しなければならない。

- 一 通信防護措置により対処を行う特定不正行為及び防護の対象となる第二項に規定する重要電子計算機
- 二 通信防護措置として実施すべき措置に関する事項
- 三 通信防護措置の期間
- 四 警察庁等と共同して通信防護措置を実施する要領その他の警察庁等との連携に関する事項
- 五 その他必要な事項

5 （略）

（重要電子計算機に対する通信防護措置の際の権限）

第九十一条の三 警察官職務執行法第六条の二第二項から第十項までの規定は、第八十一条の三第一項の規定により通信防護措置をとるべき旨を命ぜられた部隊等の自衛官の職務の執行について準用する。この場合において、同法第六条の二第二項中「サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為（以下この項において「情報技術利用不正行為」という。）」とあるのは「重要電子計算機（自衛隊法（昭和二十九年法律第百六十五号）第八十一条の三第二項に規定する重要電子計算機をいう。第四項において同じ。）に対する特定不正行為（同条第一項に規定する特定不正行為をいう。以下この項において同

刑法

【刑法（明治四十年法律第四十五号）】

（不正指令電磁的記録作成等）

第百六十八條の二 正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の拘禁刑又は五十万円以下の罰金に処する。

一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

2 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

3 前項の罪の未遂は、罰する。

（不正指令電磁的記録取得等）

第百六十八條の三 正当な理由がないのに、前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の拘禁刑又は三十万円以下の罰金に処する。

（電子計算機損壊等業務妨害）

第百三十四條の二 人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の拘禁刑又は百万円以下の罰金に処する。

2 前項の罪の未遂は、罰する。

（電子計算機損壊等公務執行妨害）

第九十五條の二 公務員が職務を執行するに当たり、その職務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくはその職務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、その電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせた者は、三年以下の拘禁刑又は五十万円以下の罰金に処する。

（電磁的記録不正作出及び供用）

第百六十一條の二 人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作つた者は、五年以下の拘禁刑又は五十万円以下の罰金に処する。

2 前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、十年以下の拘禁刑又は百万円以下の罰金に処する。

3 不正に作られた権利、義務又は事実証明に関する電磁的記録を、第一項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作つた者と同じの刑に処する。

4 前項の罪の未遂は、罰する。

（公用文書等毀棄）

第百五十八條 公務所の用に供する文書又は電磁的記録を毀棄した者は、三年以上七年以下の拘禁刑に処する。

（私用文書等毀棄）

第百五十九條 権利又は義務に関する他人の文書又は電磁的記録を毀棄した者は、五年以下の拘禁刑に処する。

（電子計算機使用詐欺）

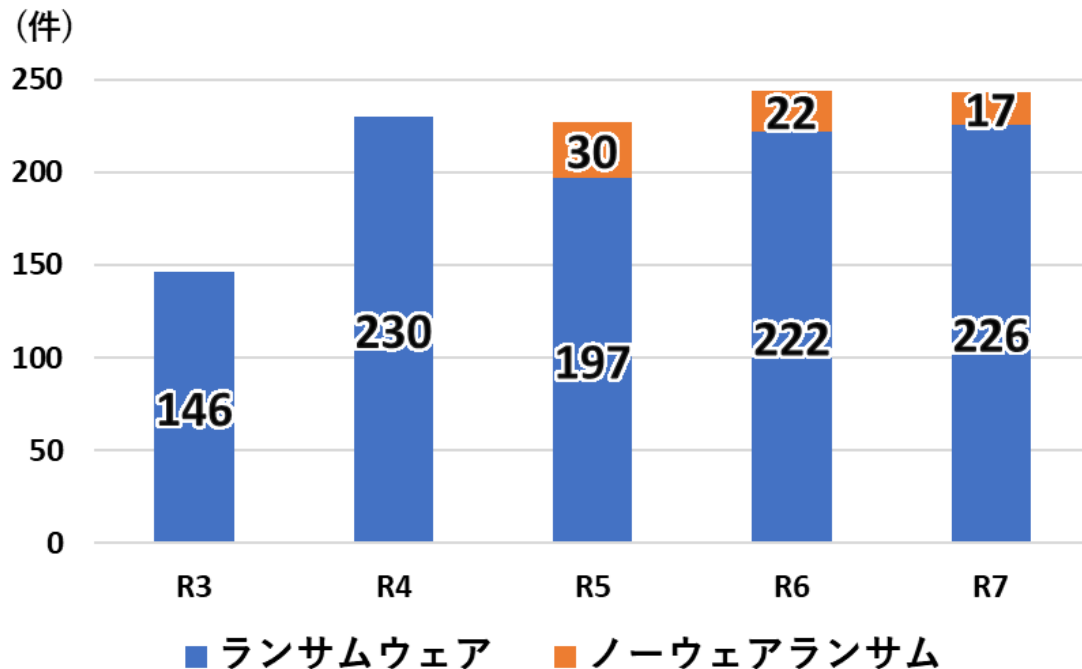
第二百四十六條の二 前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の拘禁刑に処する。

統計編

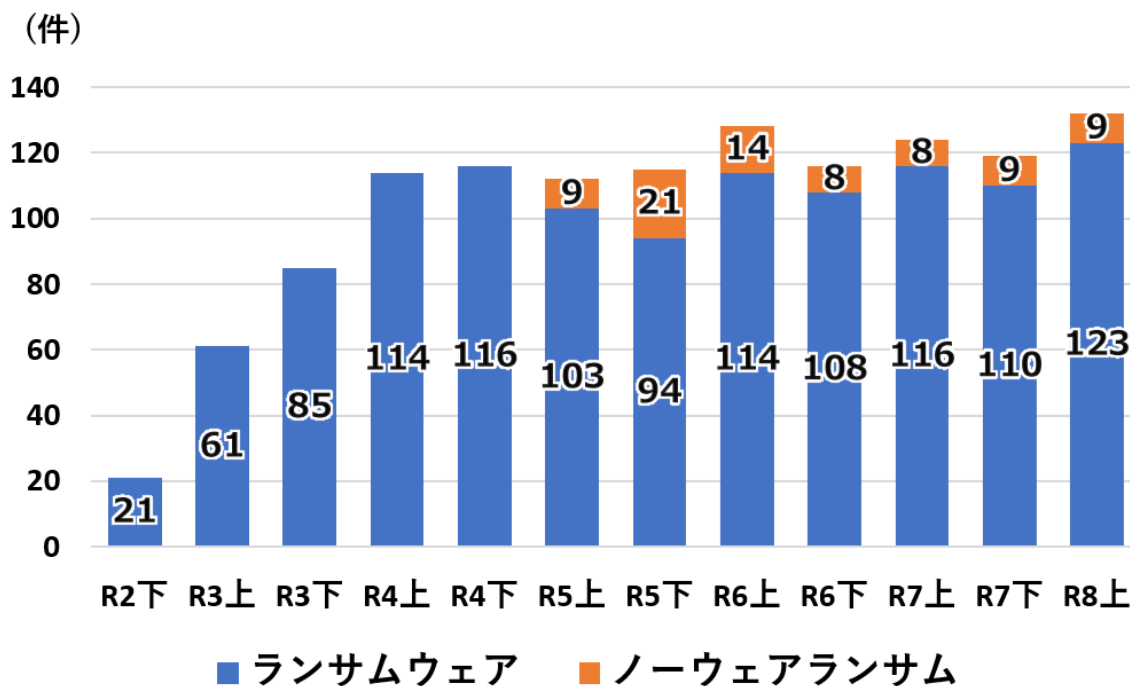
1 脅威情勢「ランサムウェア攻撃」関連	
・被害報告件数等	139
・被害企業・団体等の種別	141
・感染経路	143
・復旧期間・費用	144
・バックアップ	147
・業務に与えた影響	150
・情報セキュリティ監査・業務継続計画（BCP）	151
・セキュリティパッチ・ウイルス対策ソフトの適用	153
・ログの保全	156
2 脅威情勢「インターネット空間の悪用」関連	
・警察に対する相談	158
・インターネットを利用した詐欺	159
・インターネットバンキング不正送金	161
・クレジットカード不正利用	162
3 「検挙に向けた取組」関連	
・サイバー犯罪	163
・サイバー事案	165
・不正アクセス禁止法違反	166
4 「被害の未然防止・拡大防止に向けた取組」関連	
・サイバー保険契約に関する日本損害保険協会による調査結果	168
・サイバー防犯ボランティア団体数及び構成員数	169
・違法・有害情報に関する統計	170
その他	
・これまでの「サイバー空間をめぐる脅威の情勢等について」へのアクセス数	174

被害報告件数等 ①

企業・団体等における被害の報告件数

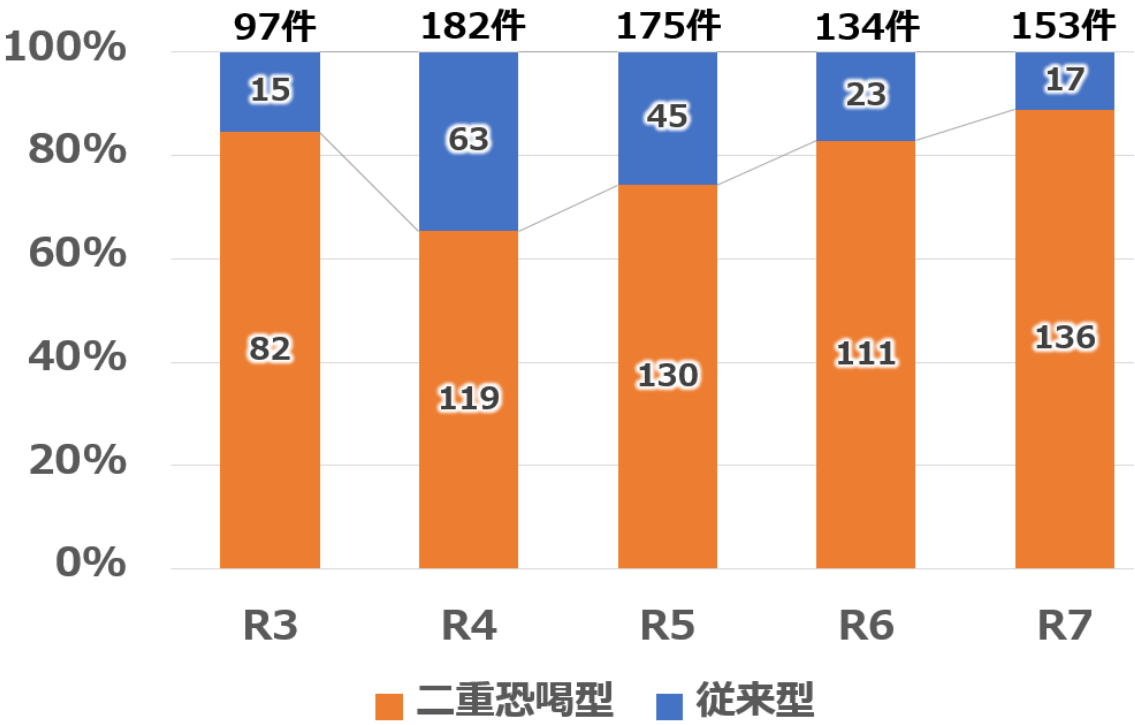
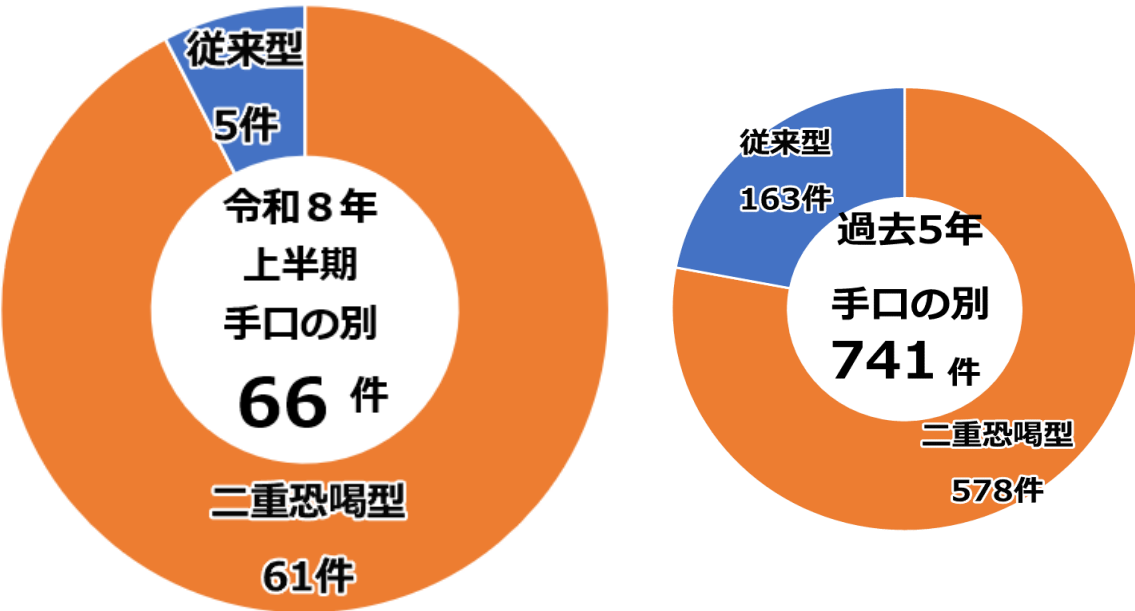


※ノーウェアランサムの被害については、令和5年上半期から集計。



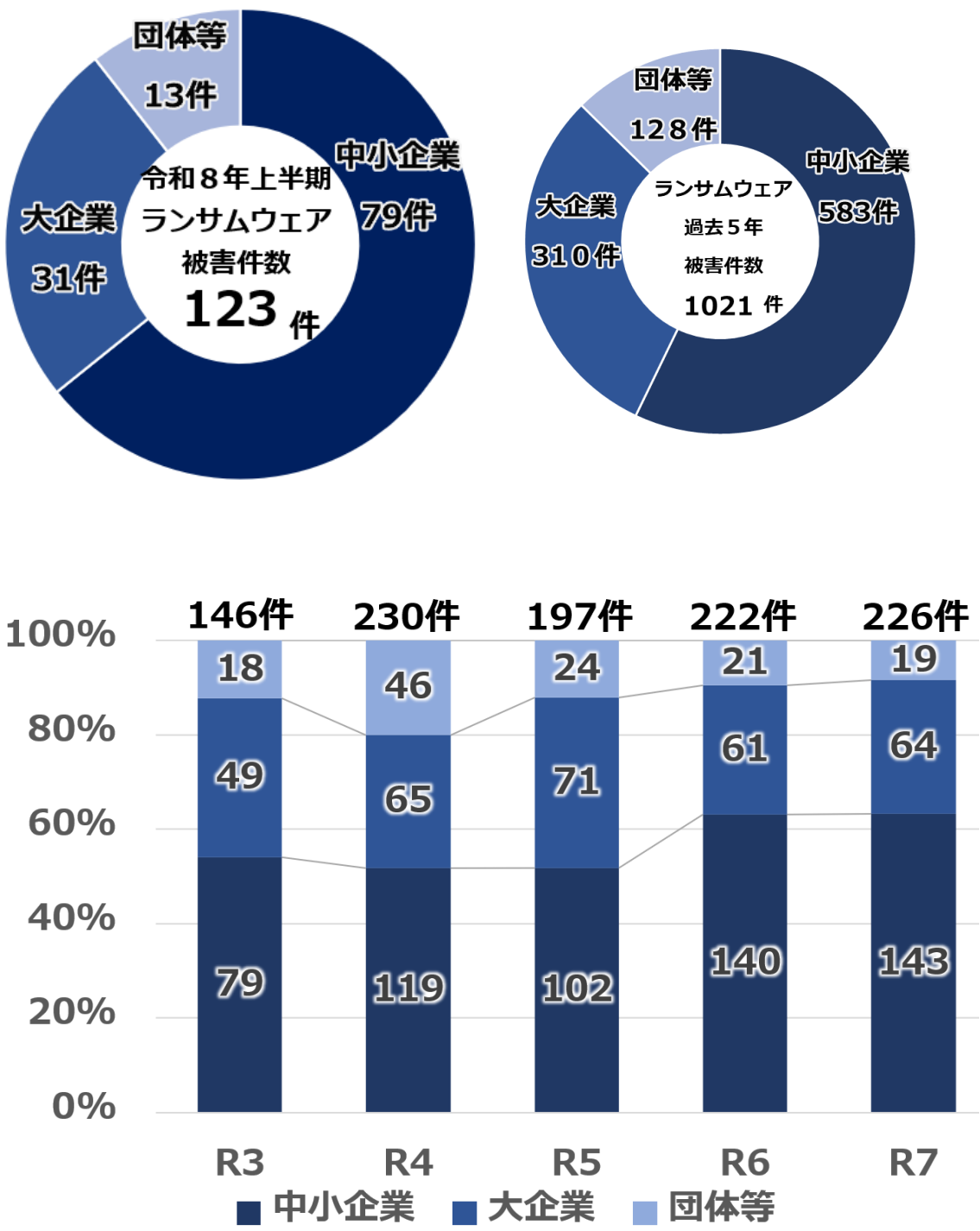
被害報告件数等 ②

手口別報告件数



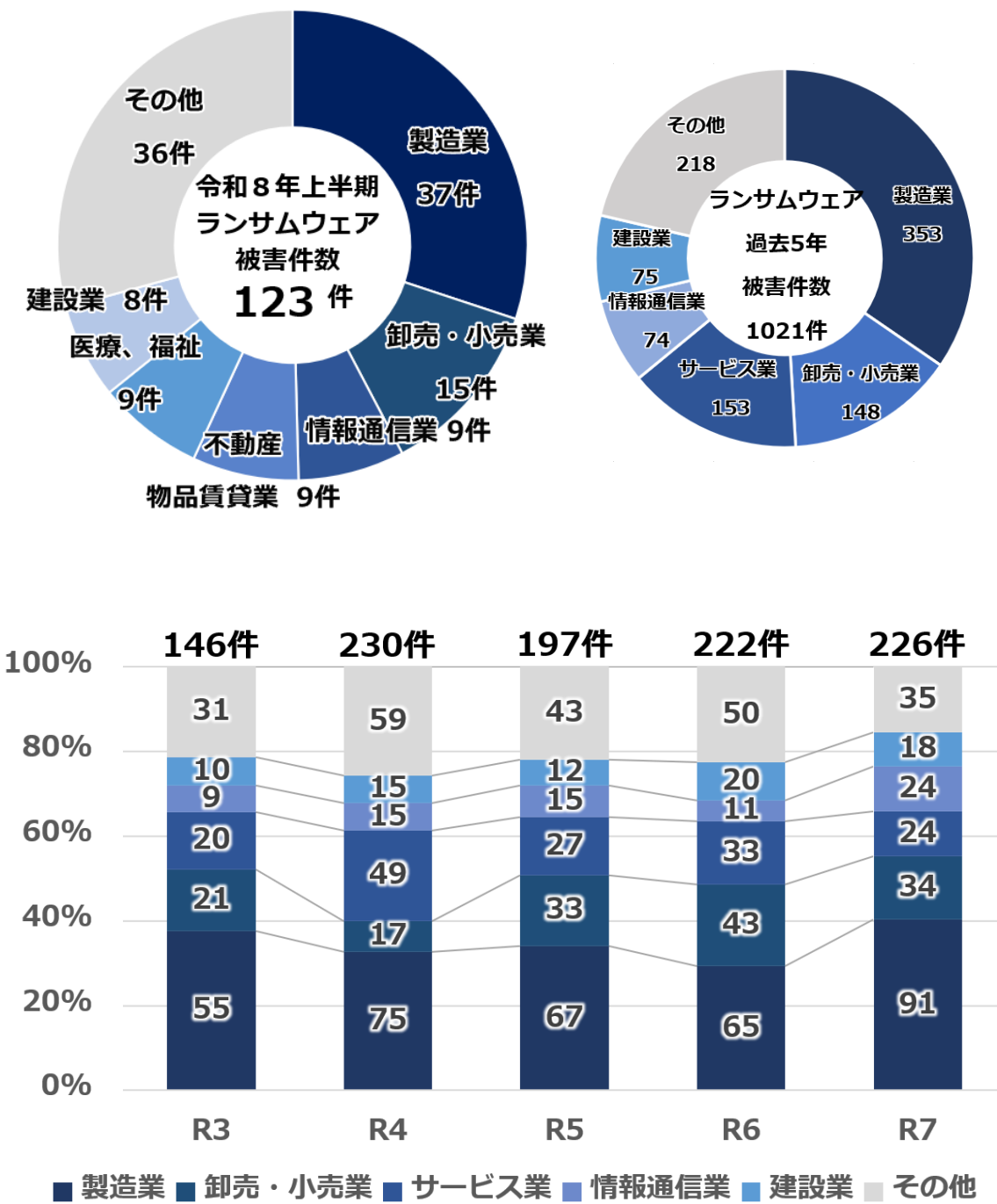
被害企業・団体等の種別 ①

規模別報告件数

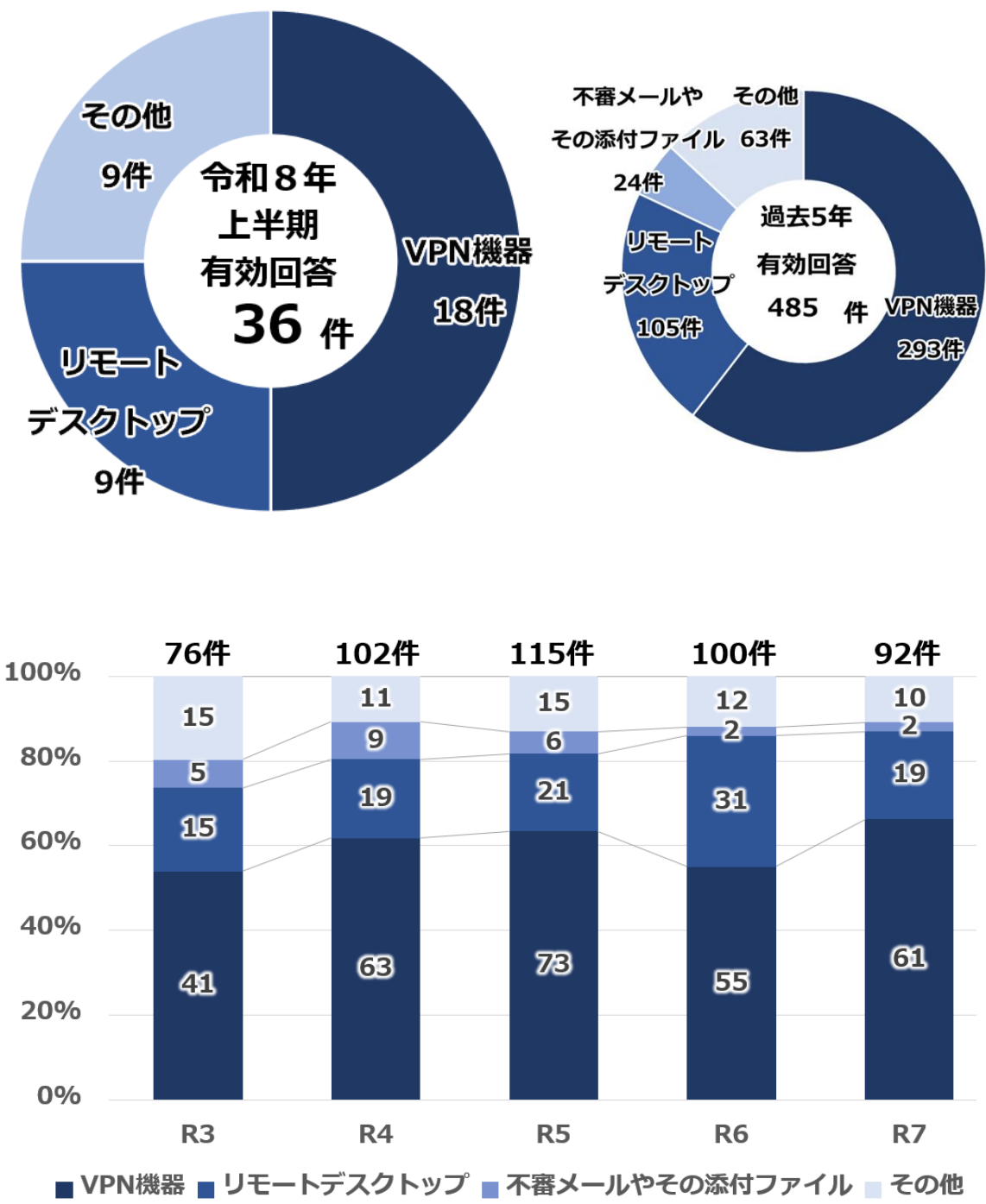


被害企業・団体等の種別 ②

業種別報告件数

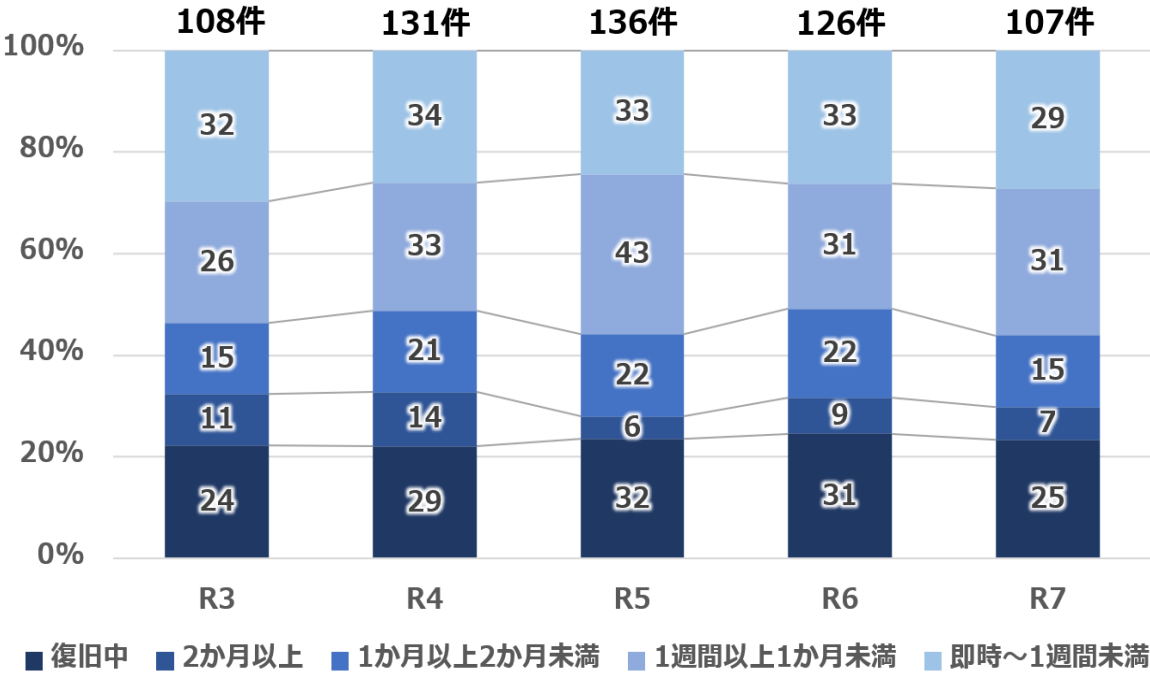
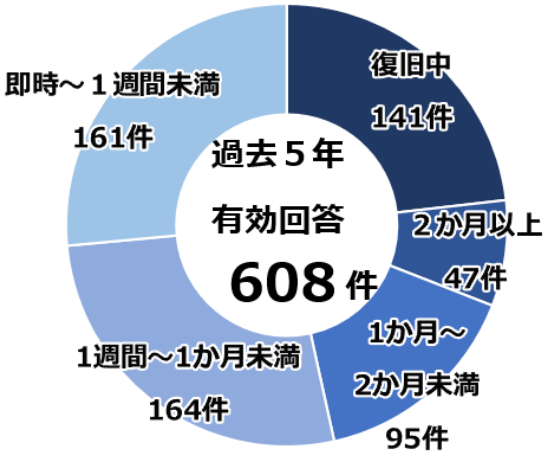
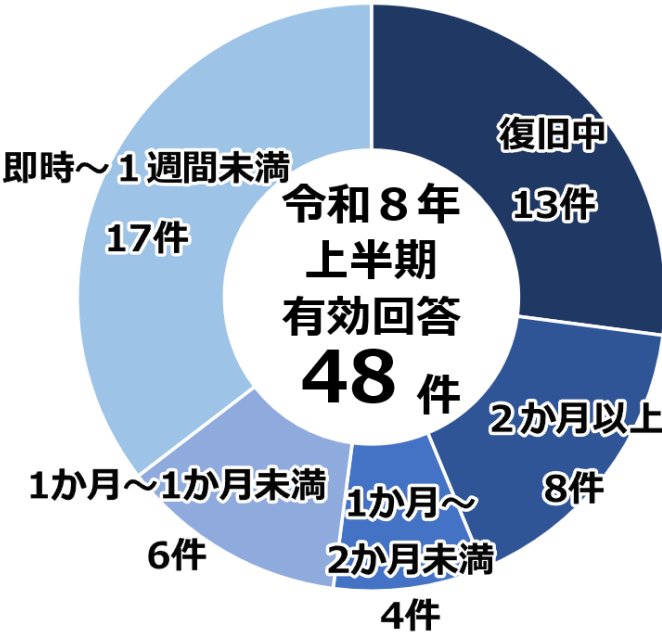


感染経路



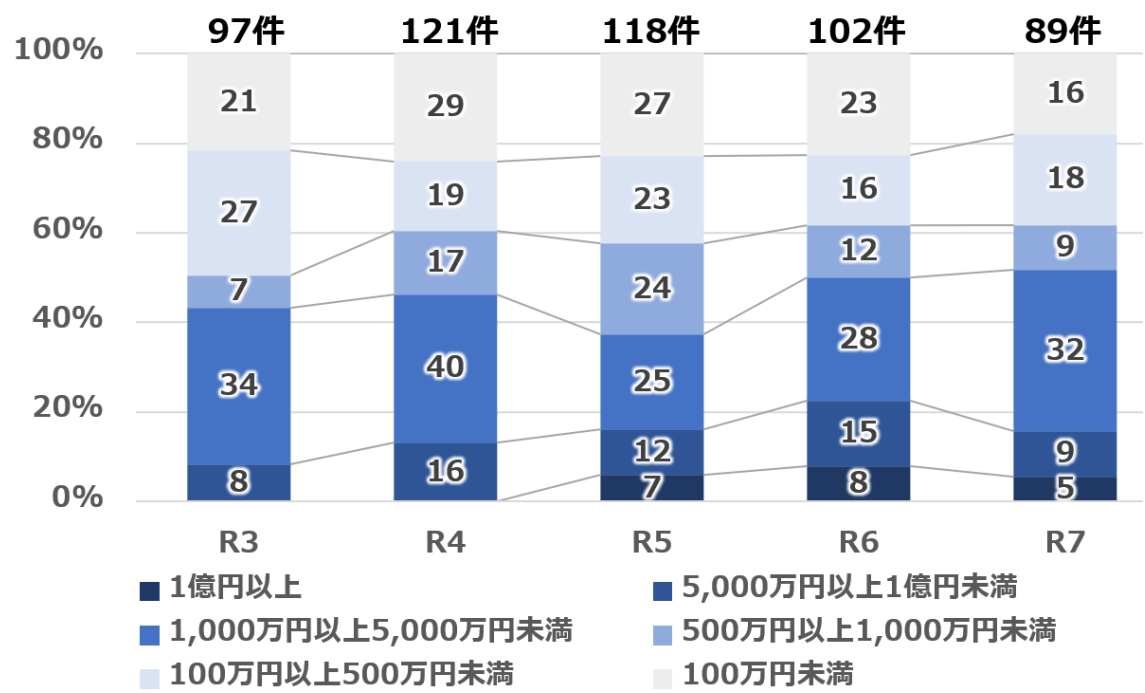
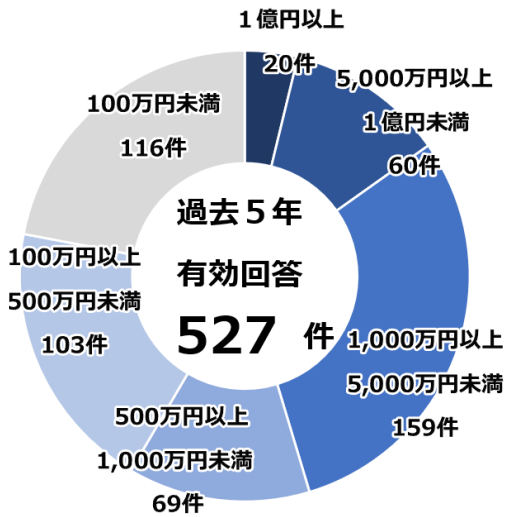
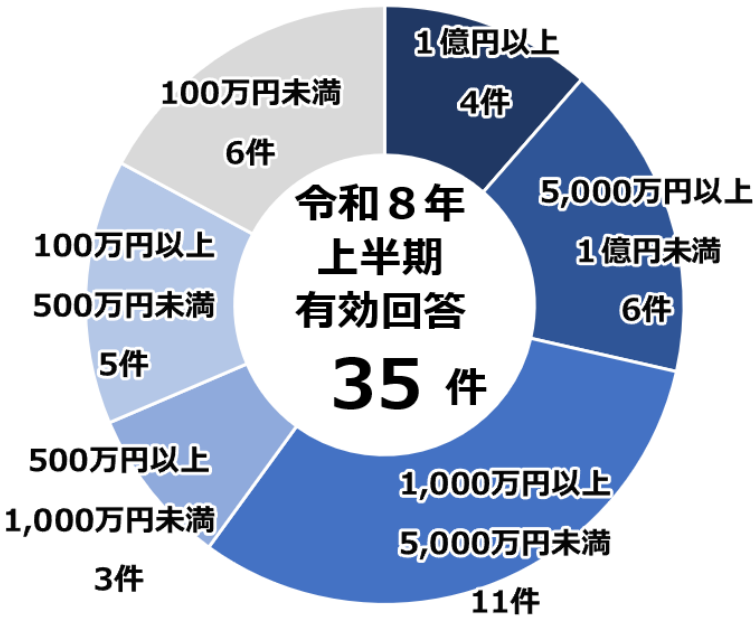
復旧期間・費用 ①

復旧等に要した期間



復旧期間・費用 ②

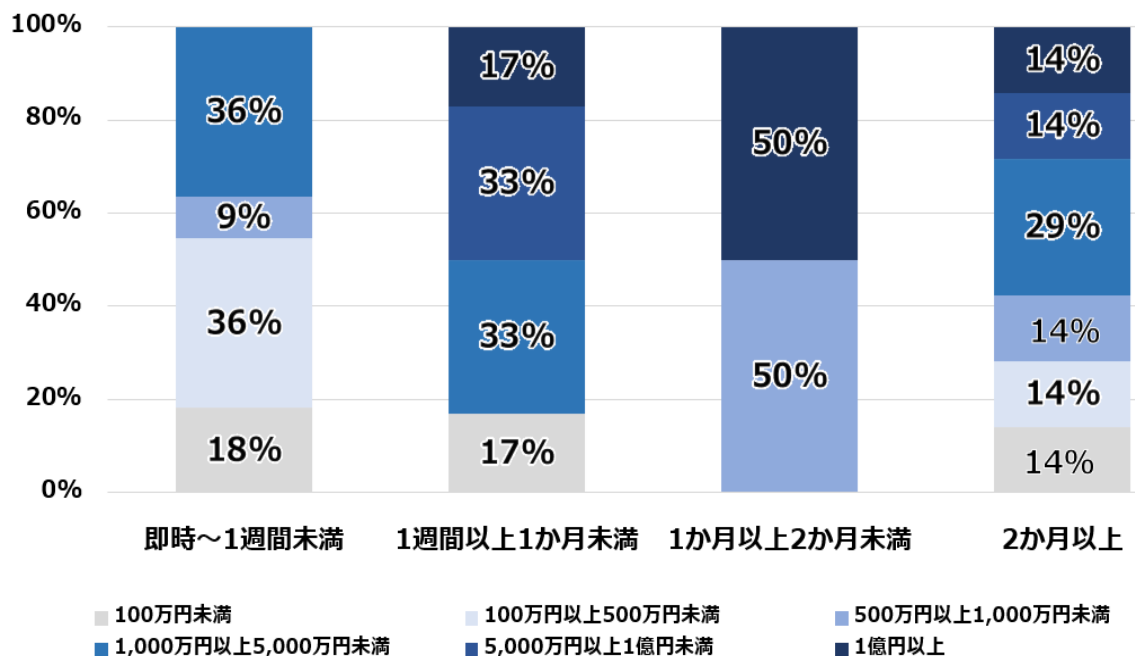
調査・復旧費用の総額



復旧期間・費用 ③

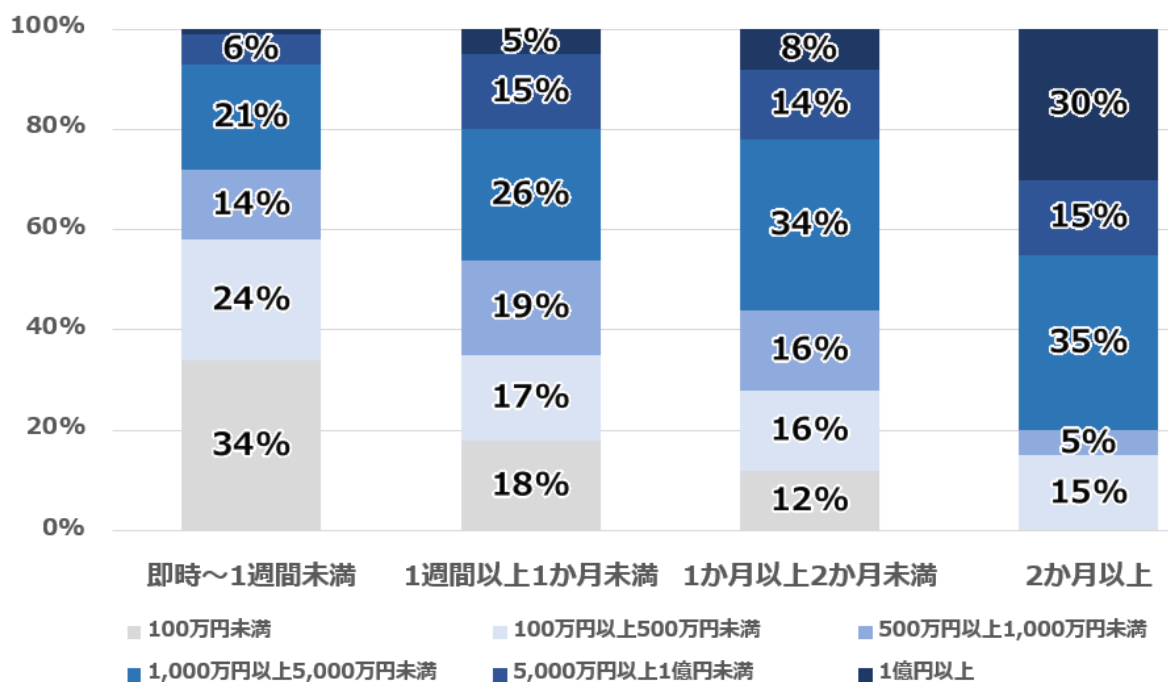
復旧期間と費用の関係性

【令和8年上半期 アンケート調査結果】



※ 被害企業の一部においては、業務継続に必要な不可欠なシステムの感染ではなかったことから、通常業務を遂行しつつ、時間をかけて復旧作業を行った。その結果、復旧期間が長期にわたったものの、費用が小さくなった。

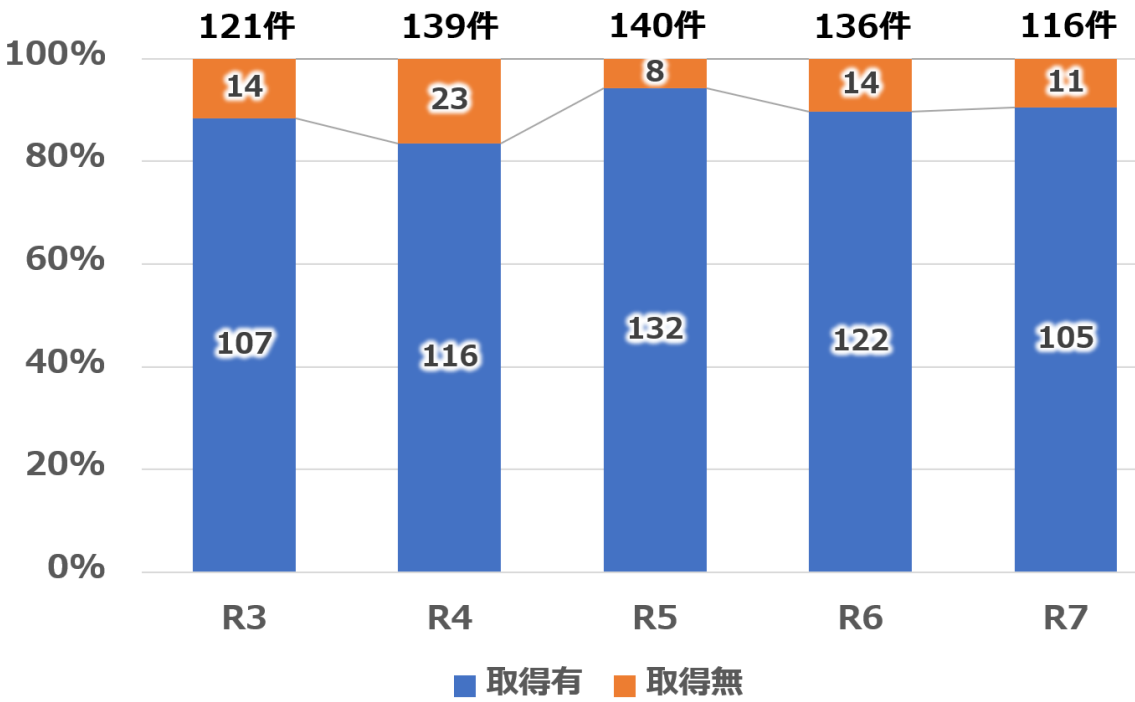
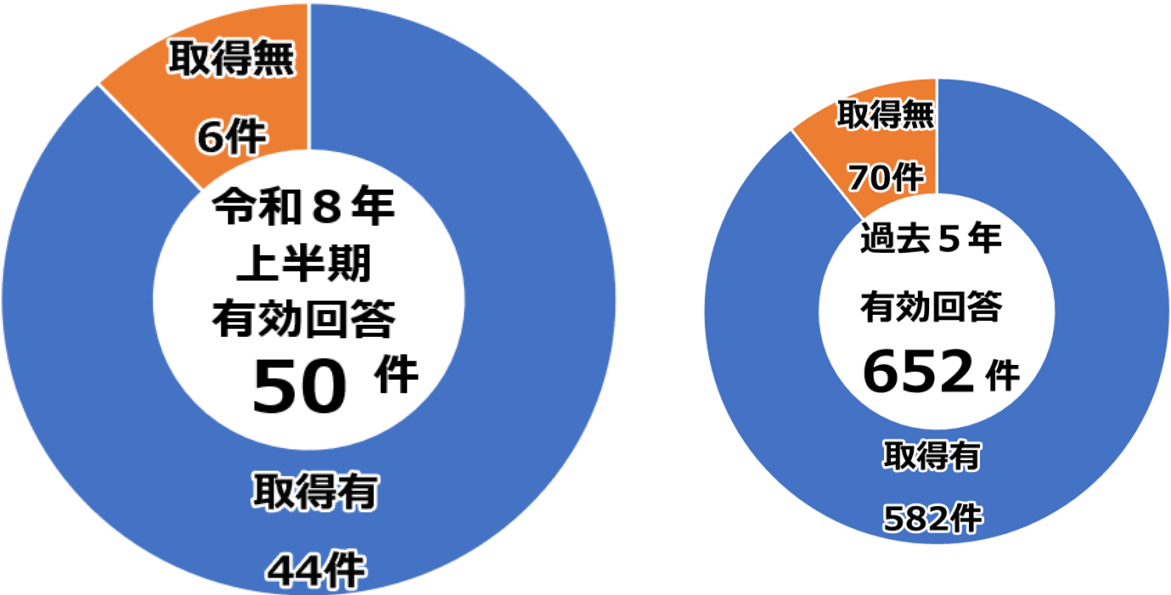
【過去3年 アンケート調査結果】



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

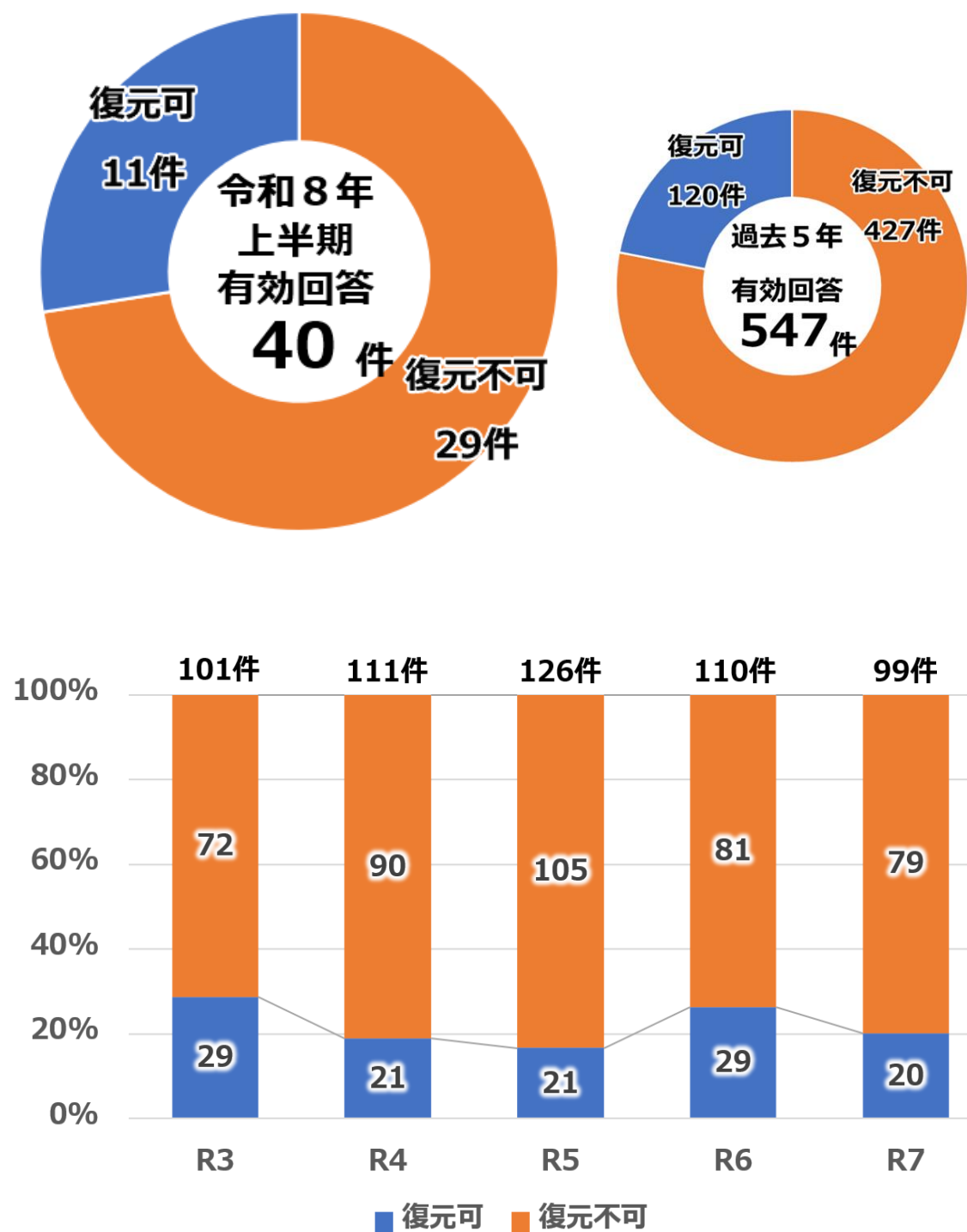
バックアップ ①

バックアップの取得状況



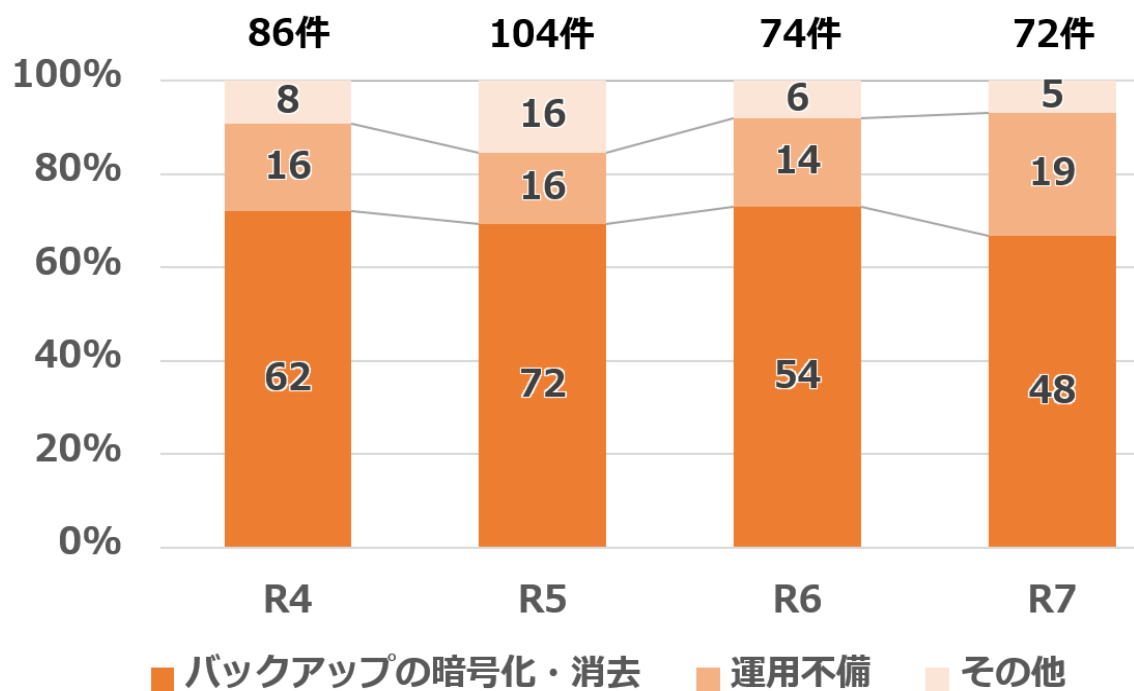
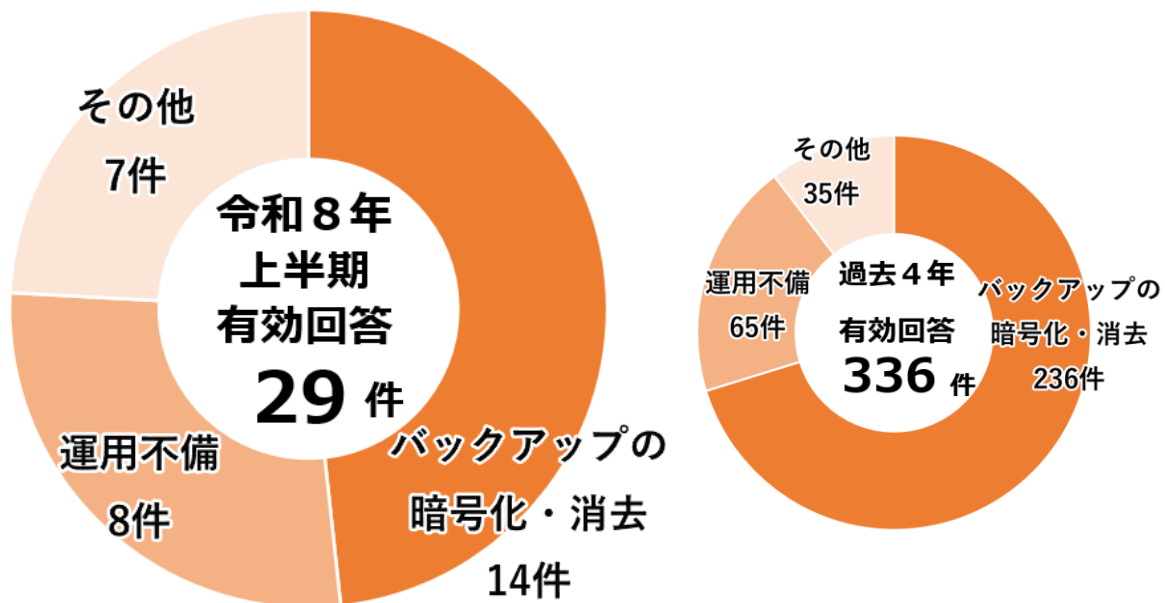
バックアップ ②

バックアップからの復元結果



バックアップ ③

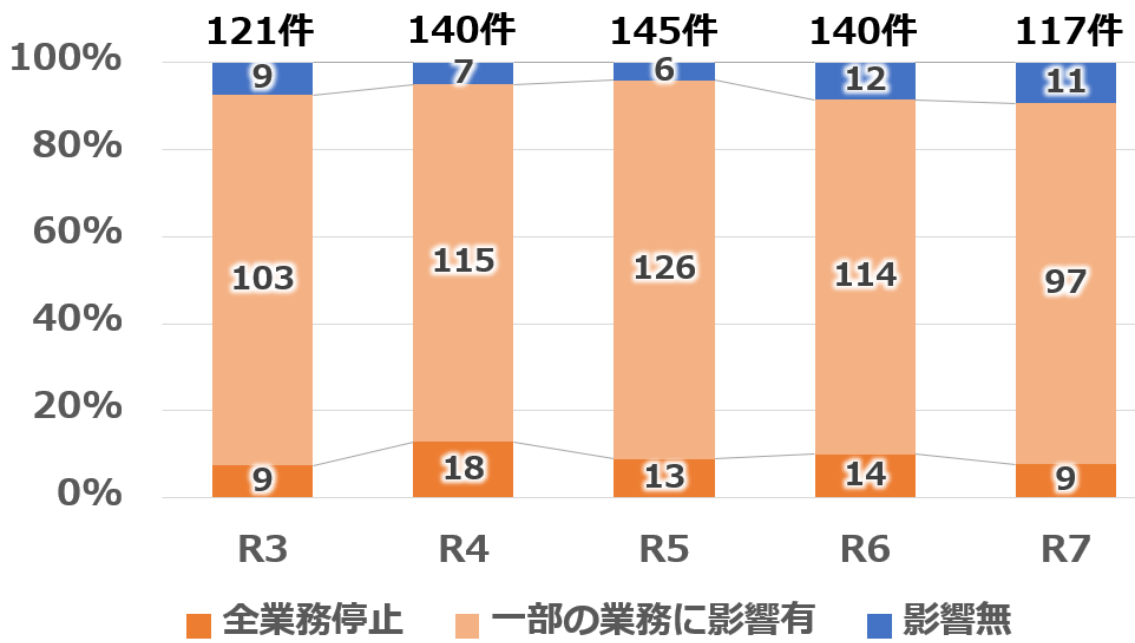
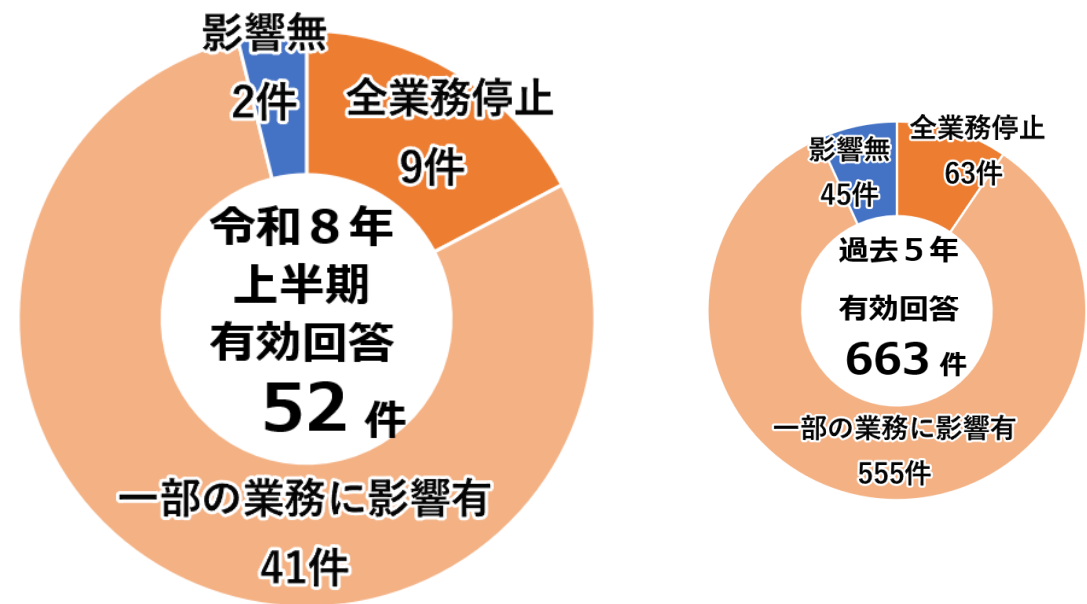
バックアップから復元できなかった理由



※ 令和4年から集計。

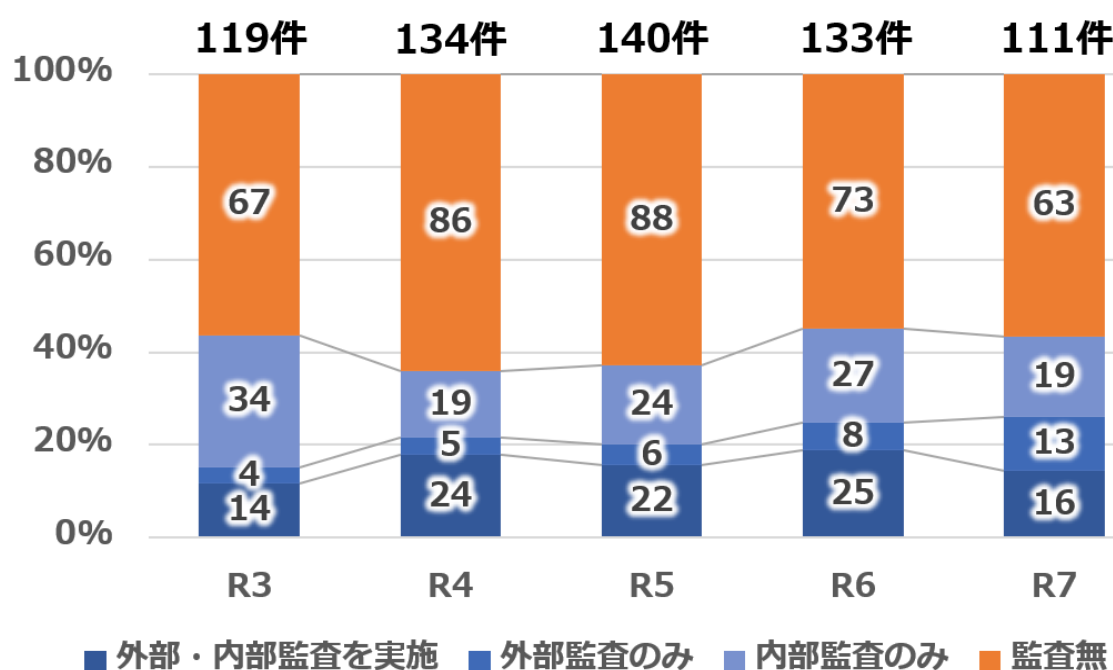
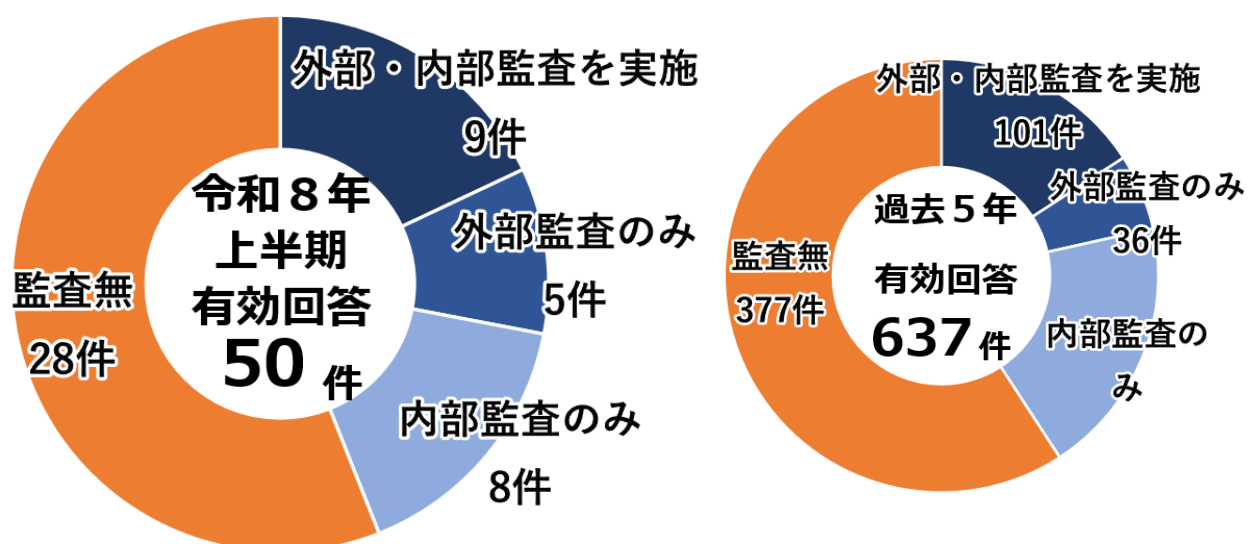
業務に与えた影響

業務に与えた影響の程度



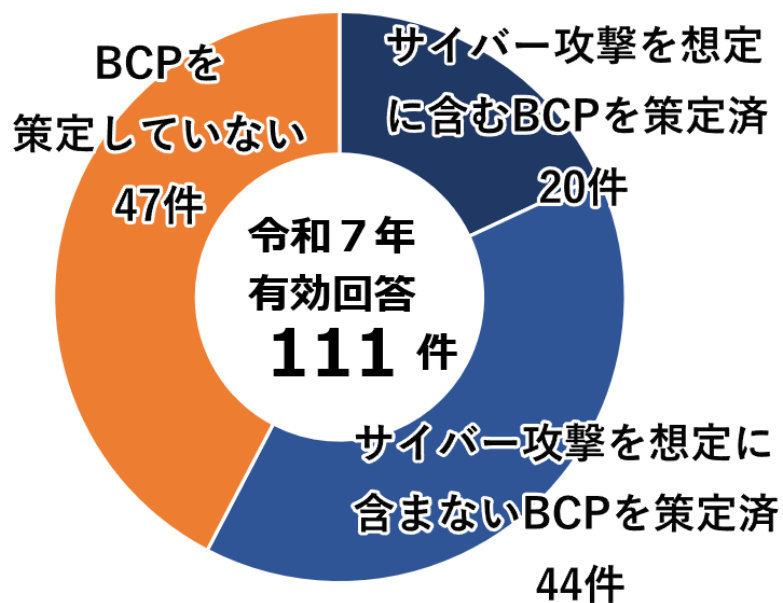
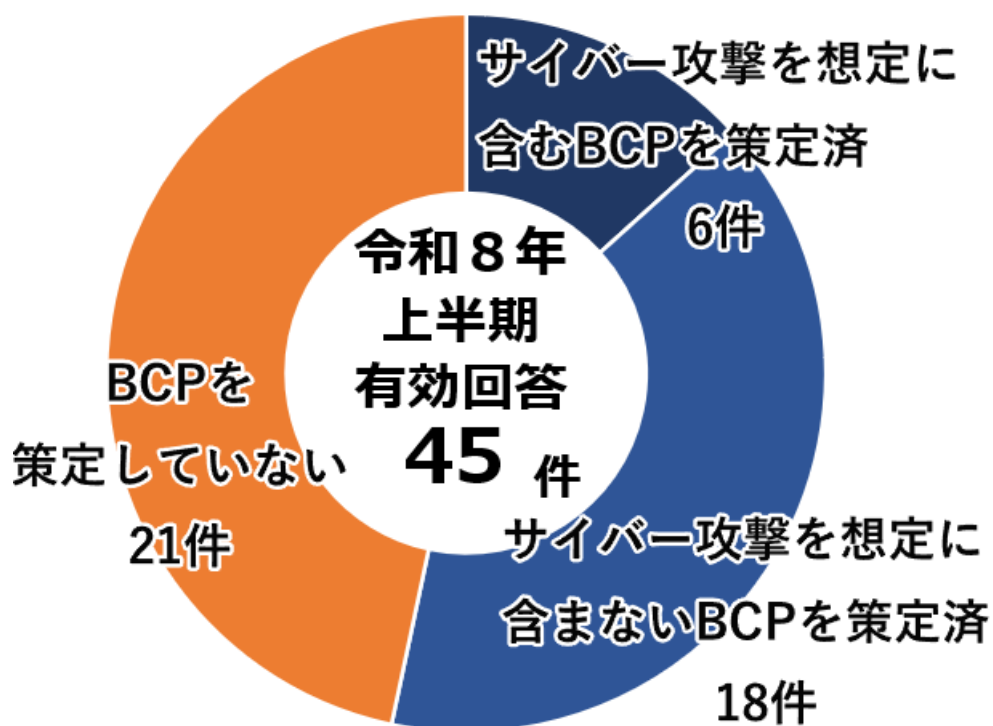
情報セキュリティ監査

情報セキュリティ監査の実施状況



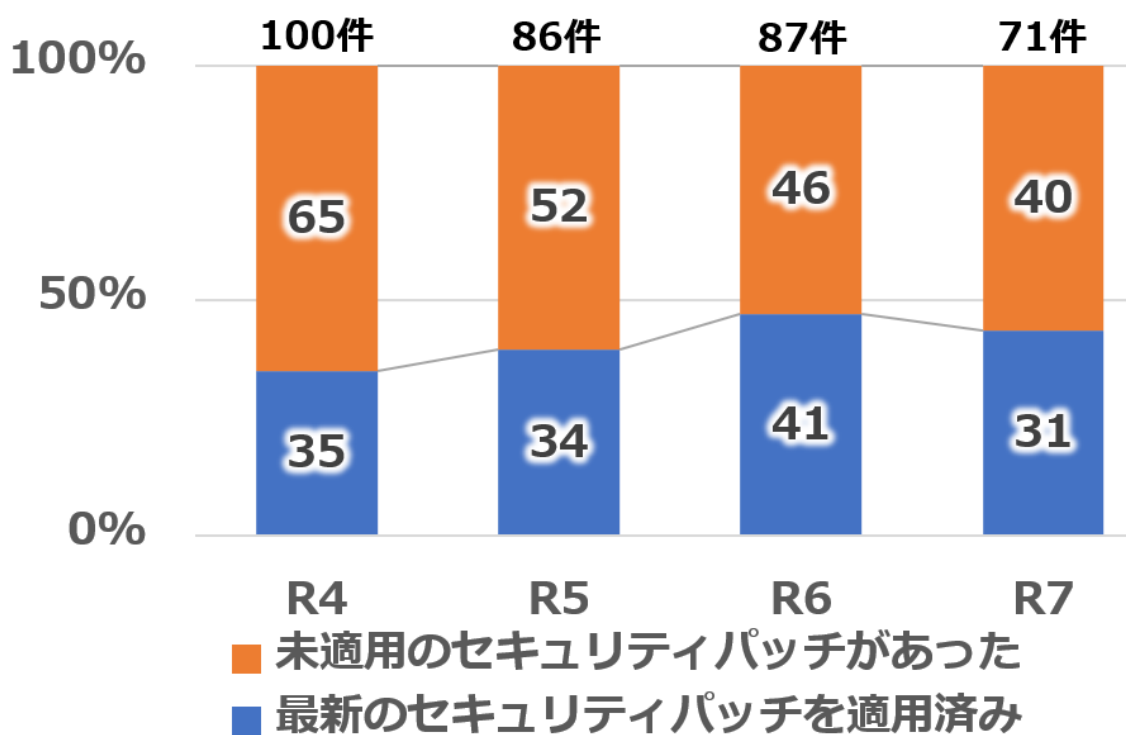
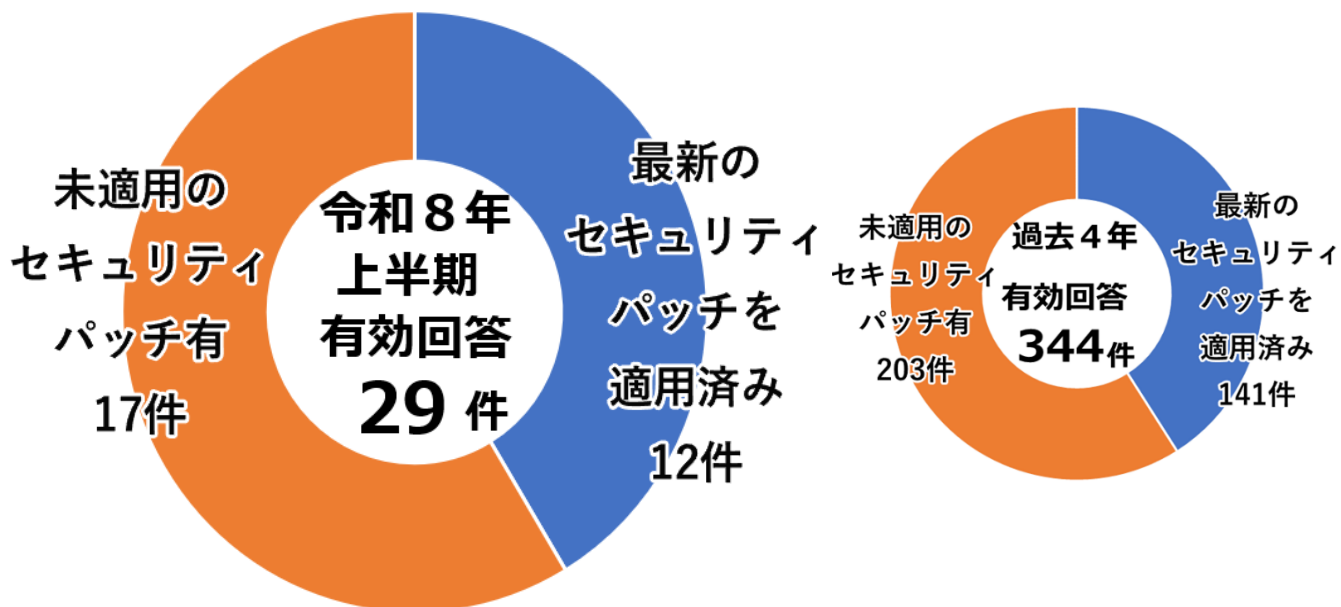
業務継続計画（BCP）

業務継続計画（BCP）の策定状況



セキュリティパッチ・ウイルス対策ソフトの適用 ①

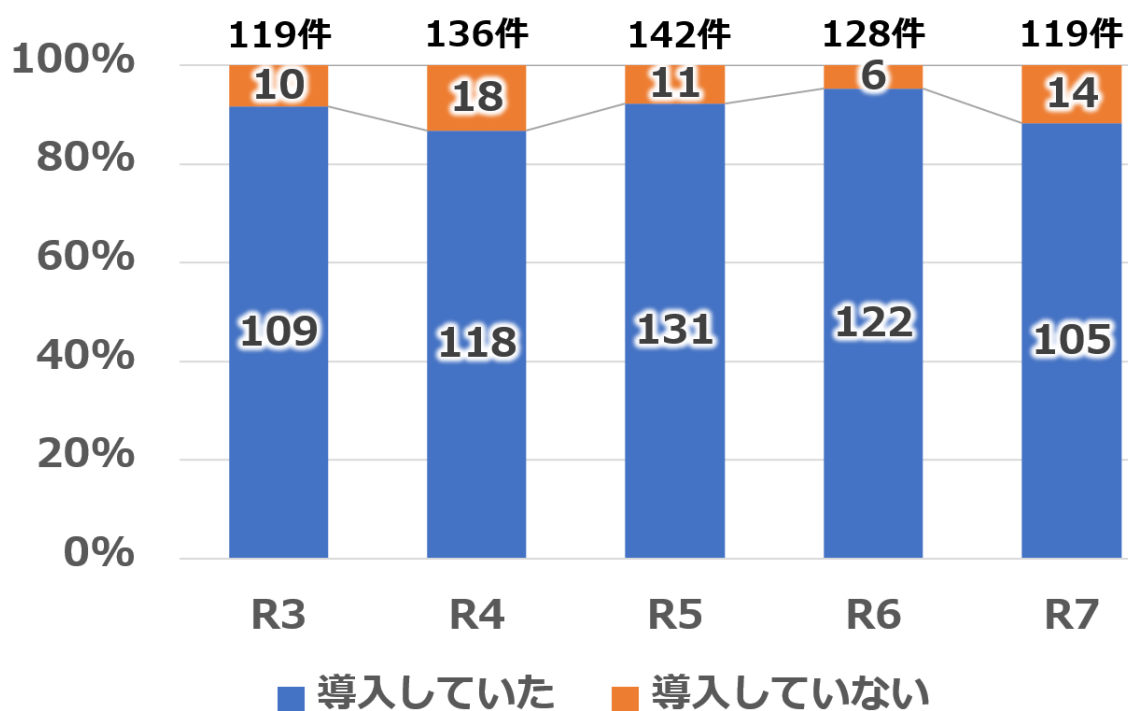
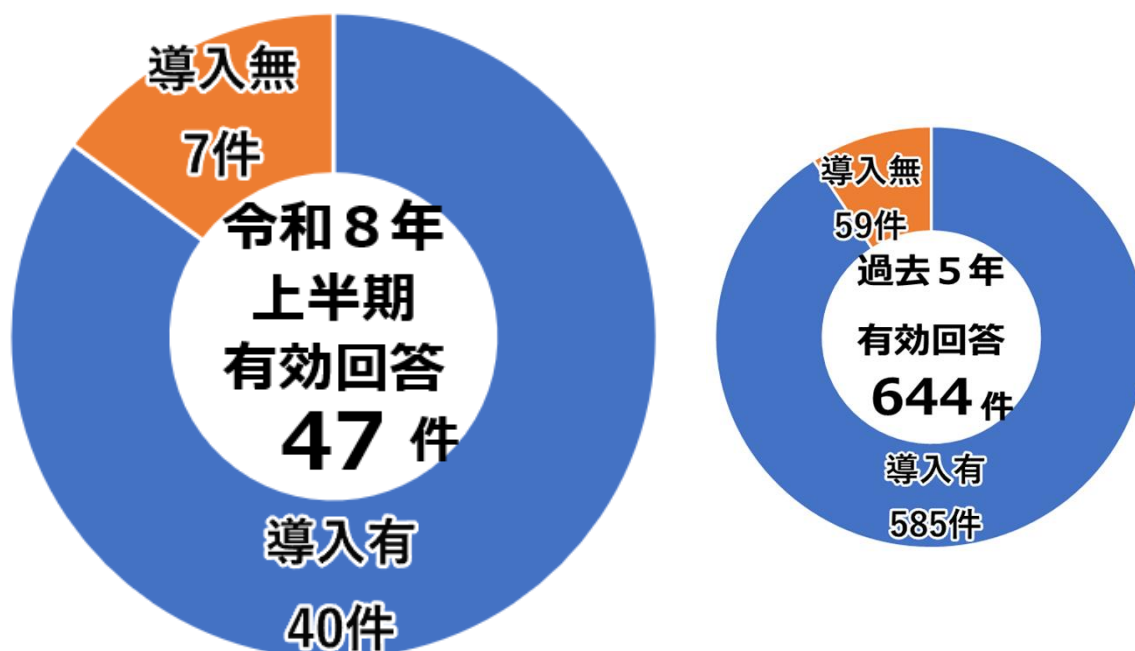
セキュリティパッチの適用状況



※ 令和4年から集計。

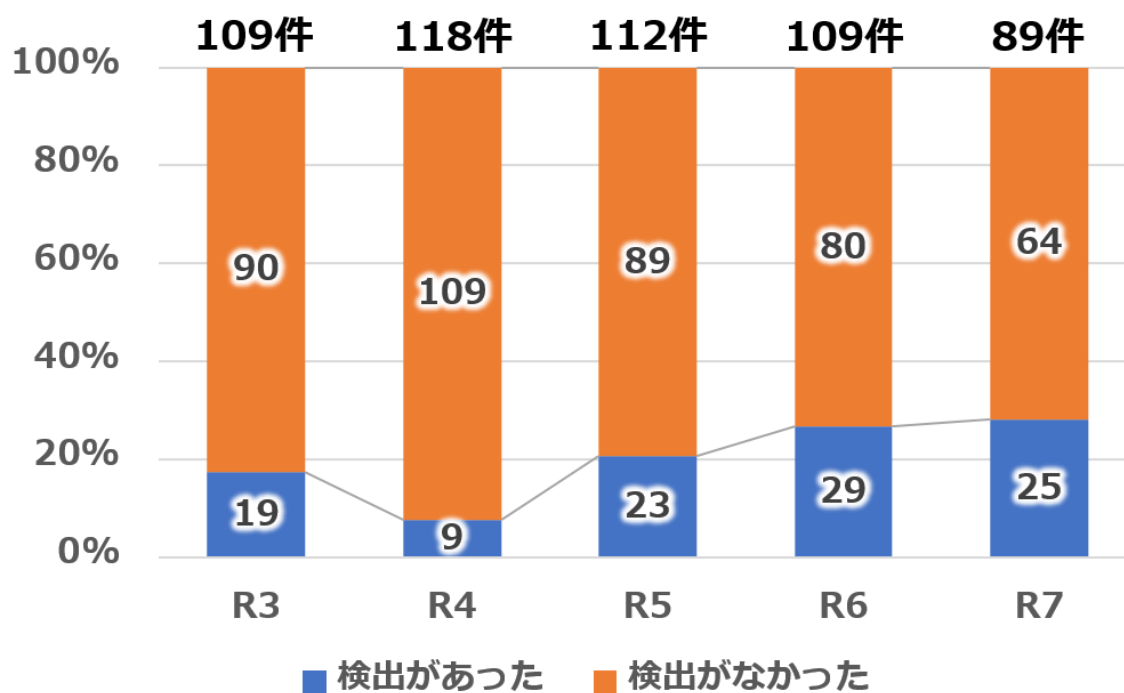
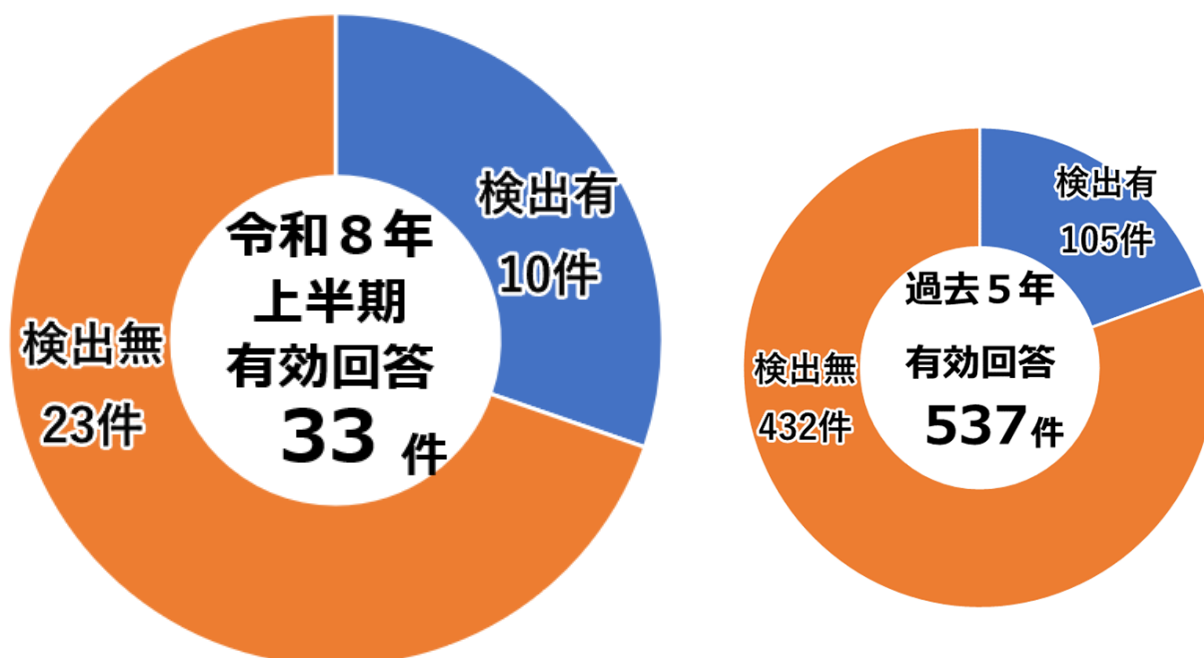
セキュリティパッチ・ウイルス対策ソフトの適用 ②

ウイルス対策ソフト導入状況



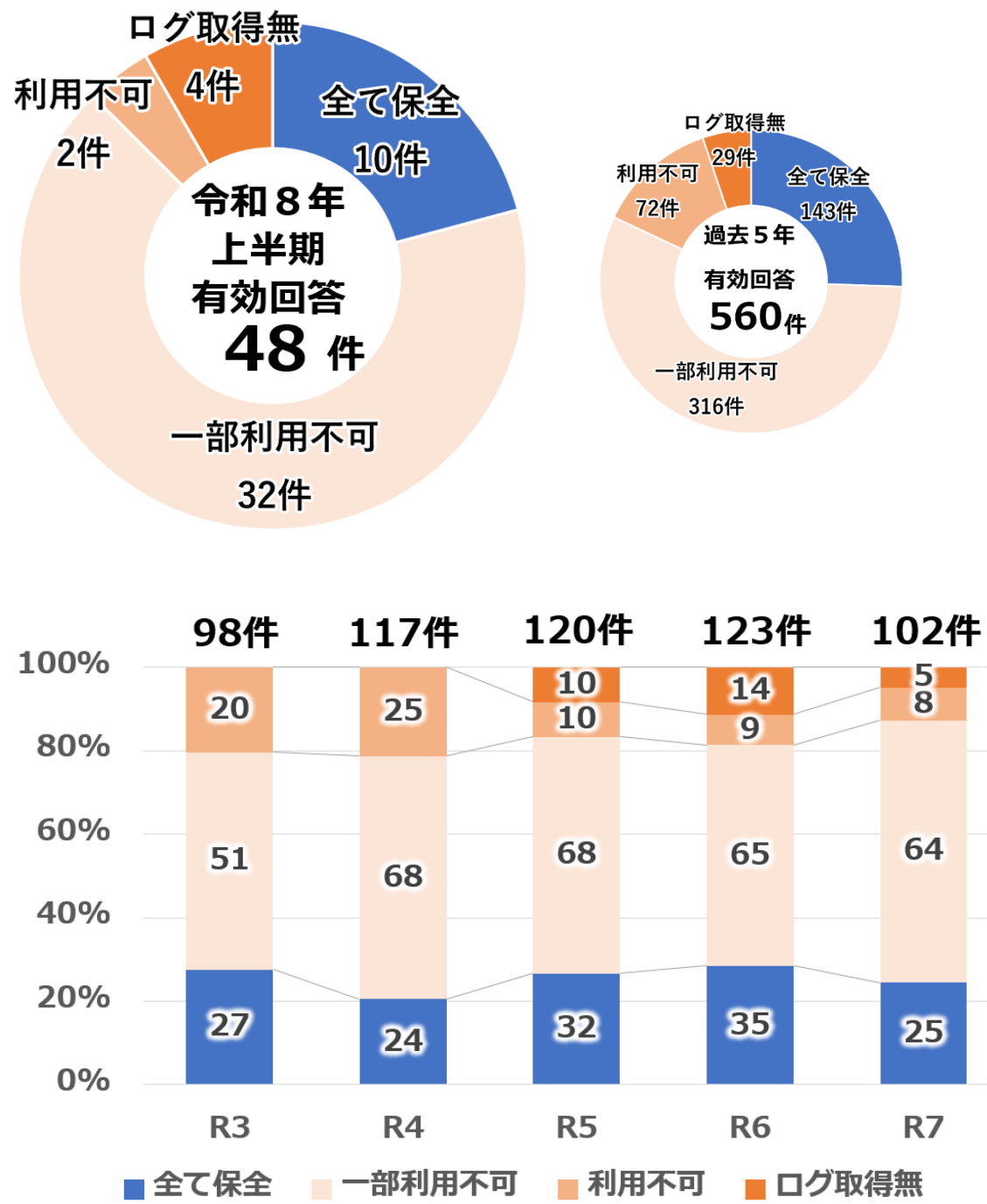
セキュリティパッチ・ウイルス対策ソフトの適用 ③

ウイルス対策ソフト検出状況



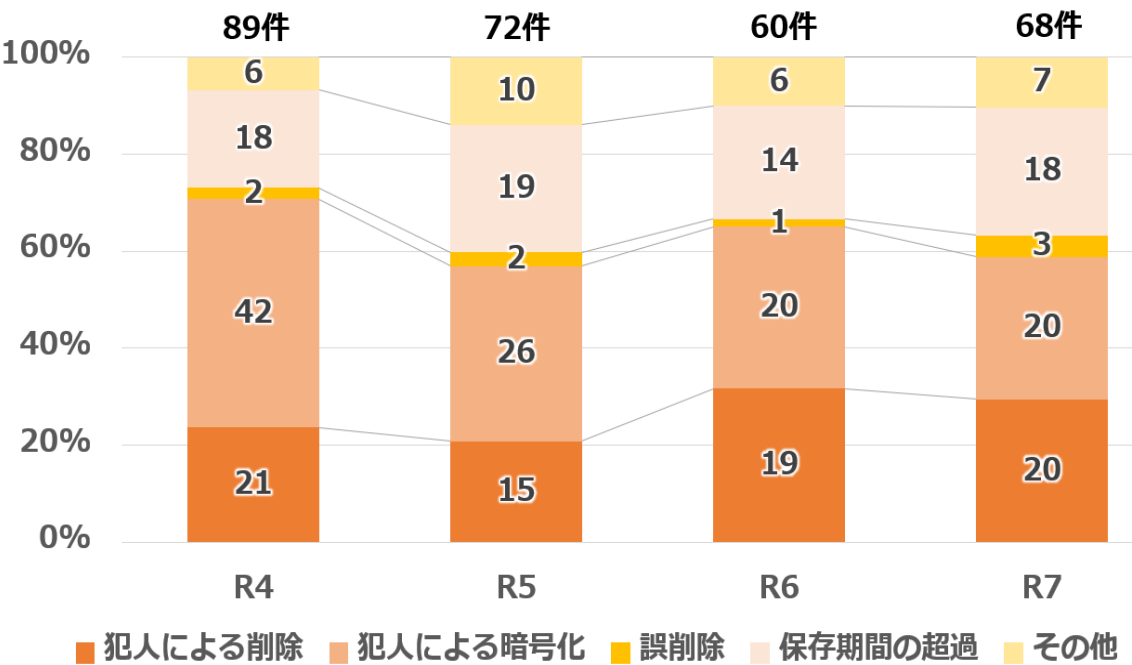
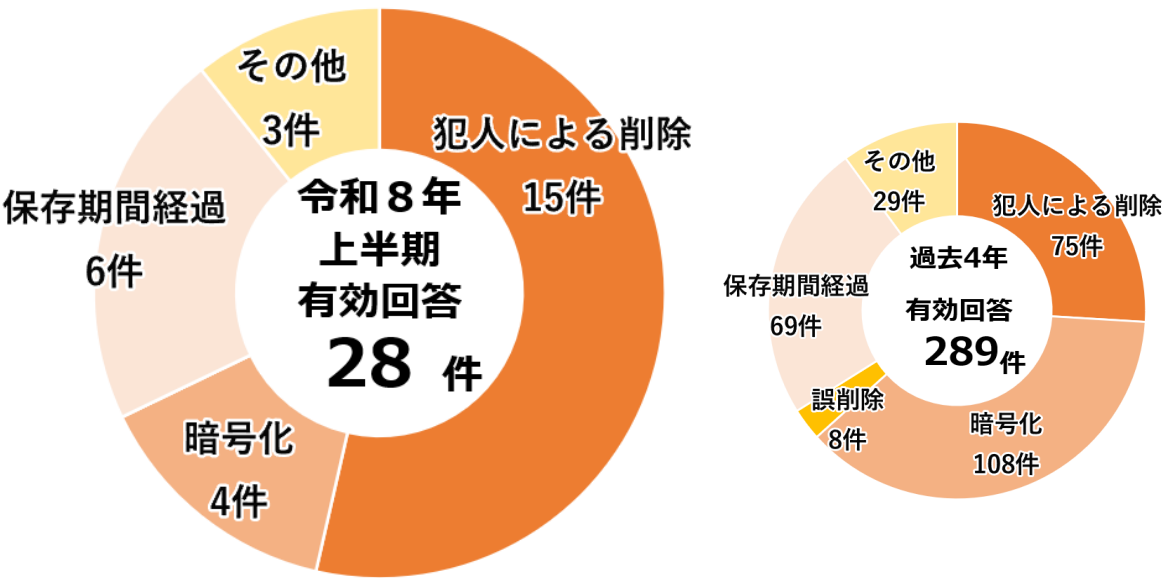
ログの保全 ①

被害企業・団体等のログ保全状況



ログの保全 ②

ログが使用できなくなっていた原因

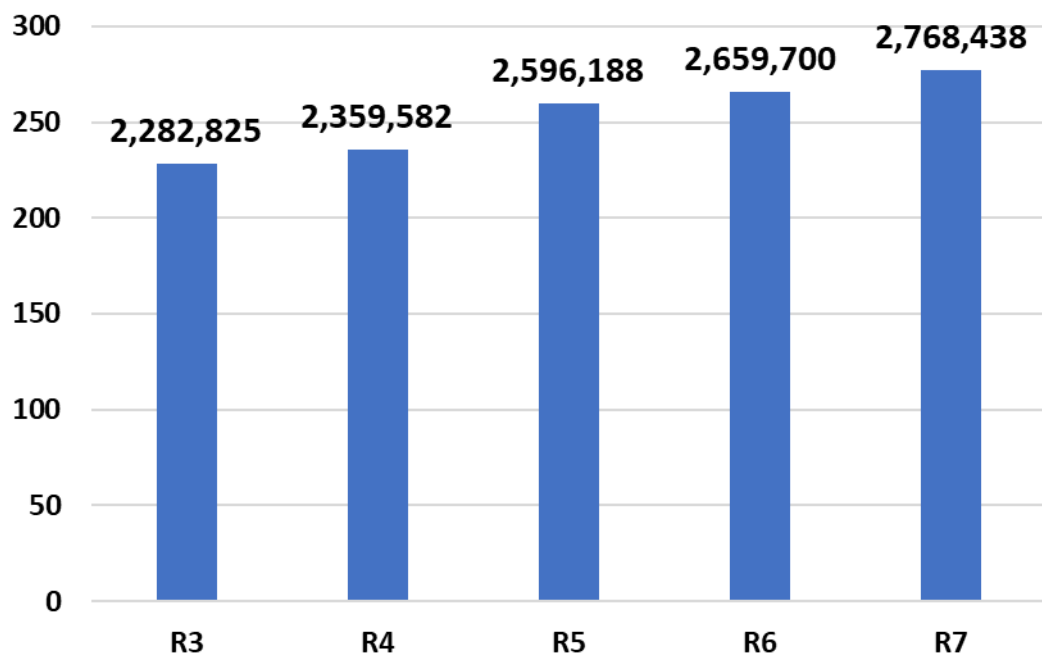


※ 令和4年から集計。

警察に対する相談

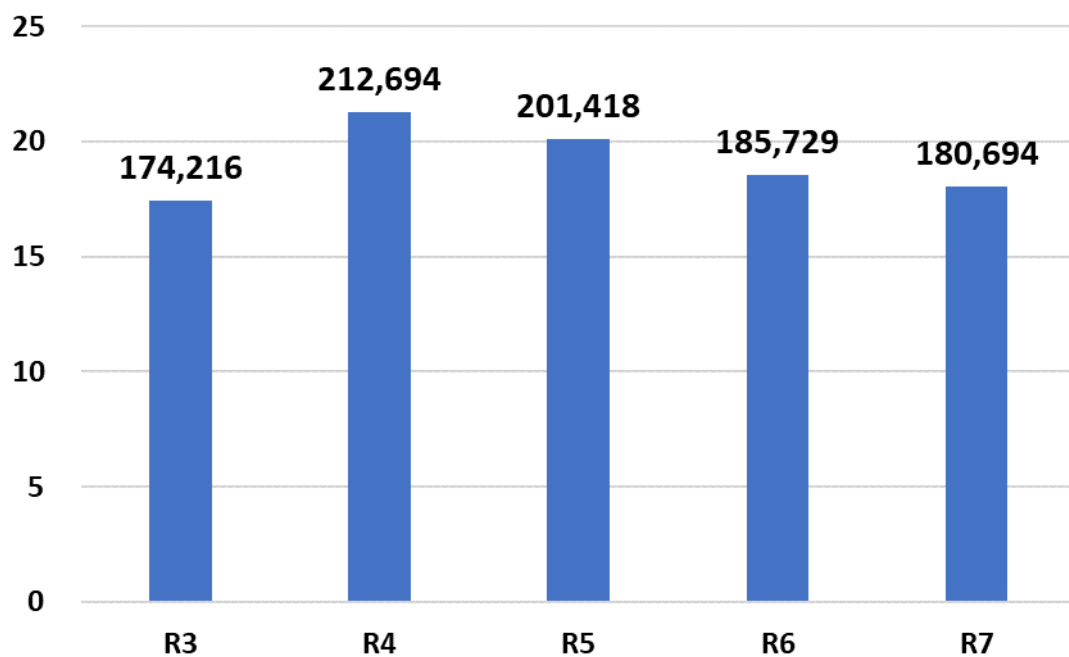
警察で取り扱った相談件数

(万件)



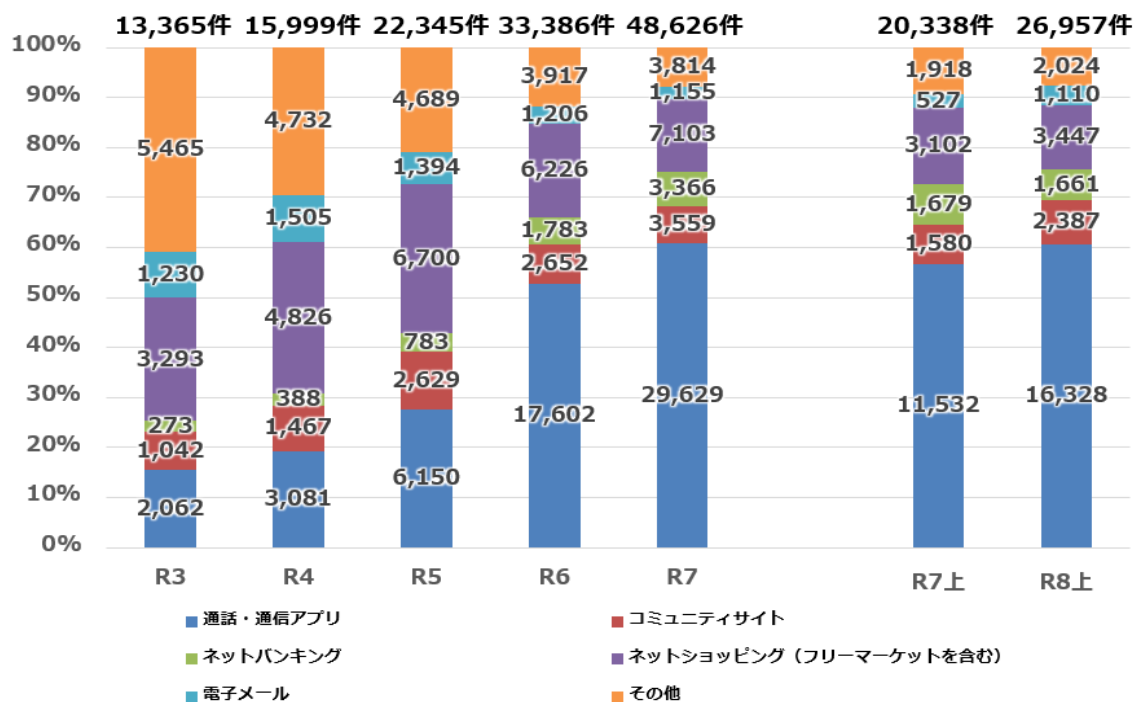
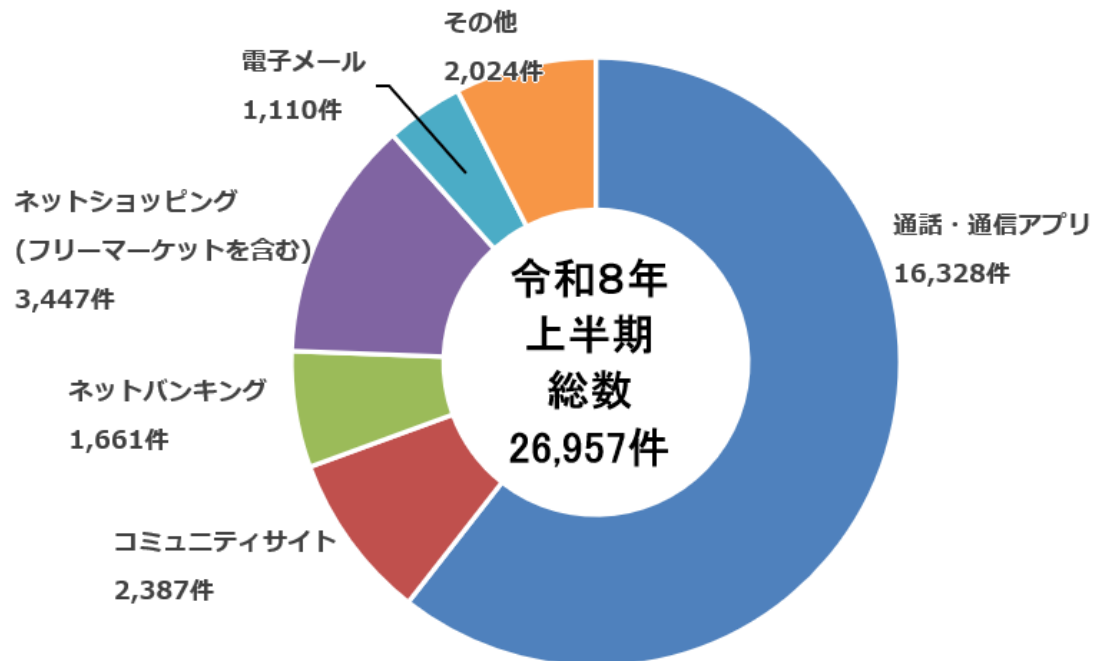
警察で取り扱ったサイバー関係の相談件数

(万件)



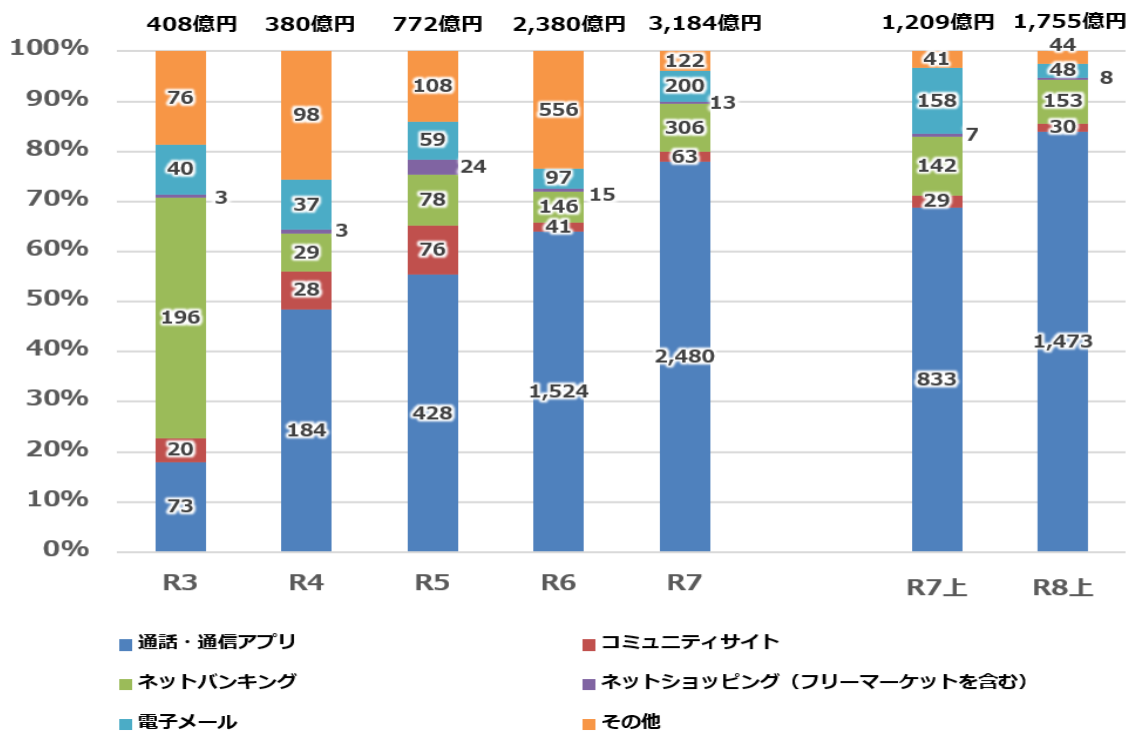
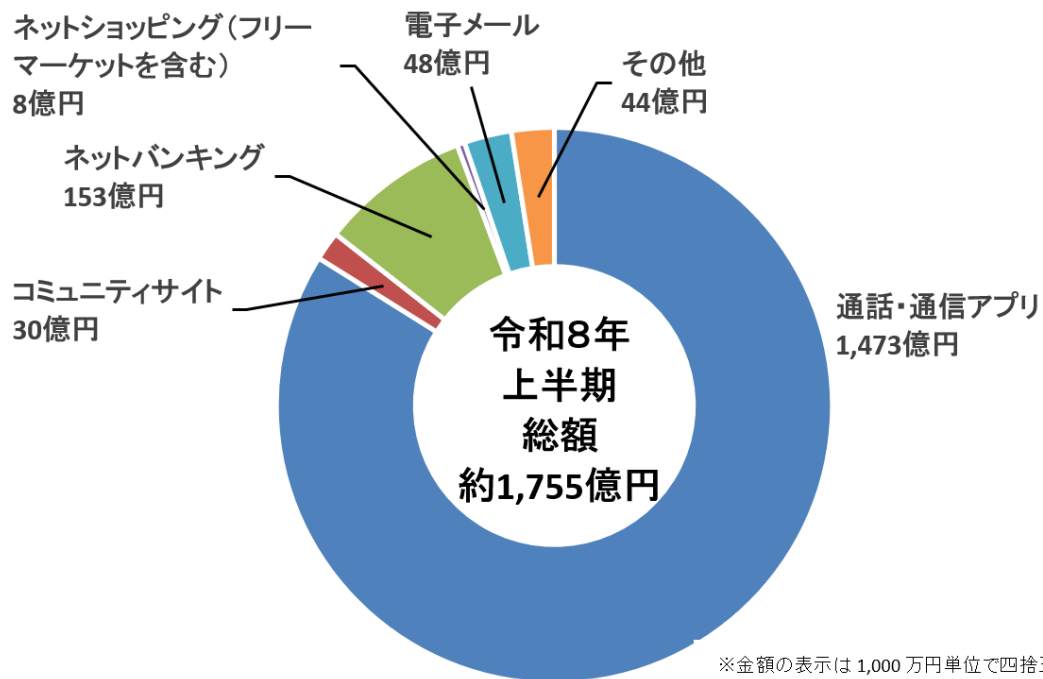
インターネットを利用した詐欺 ①

認知件数



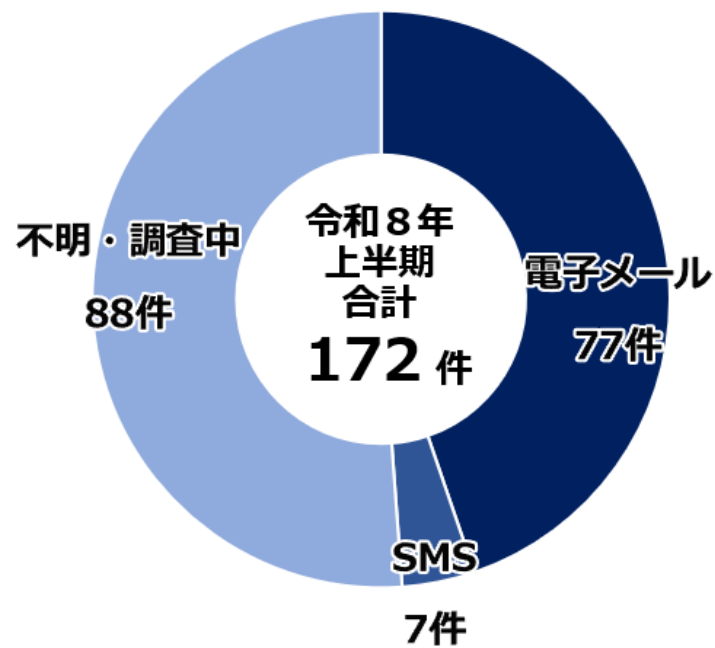
インターネットを利用した詐欺②

被害額

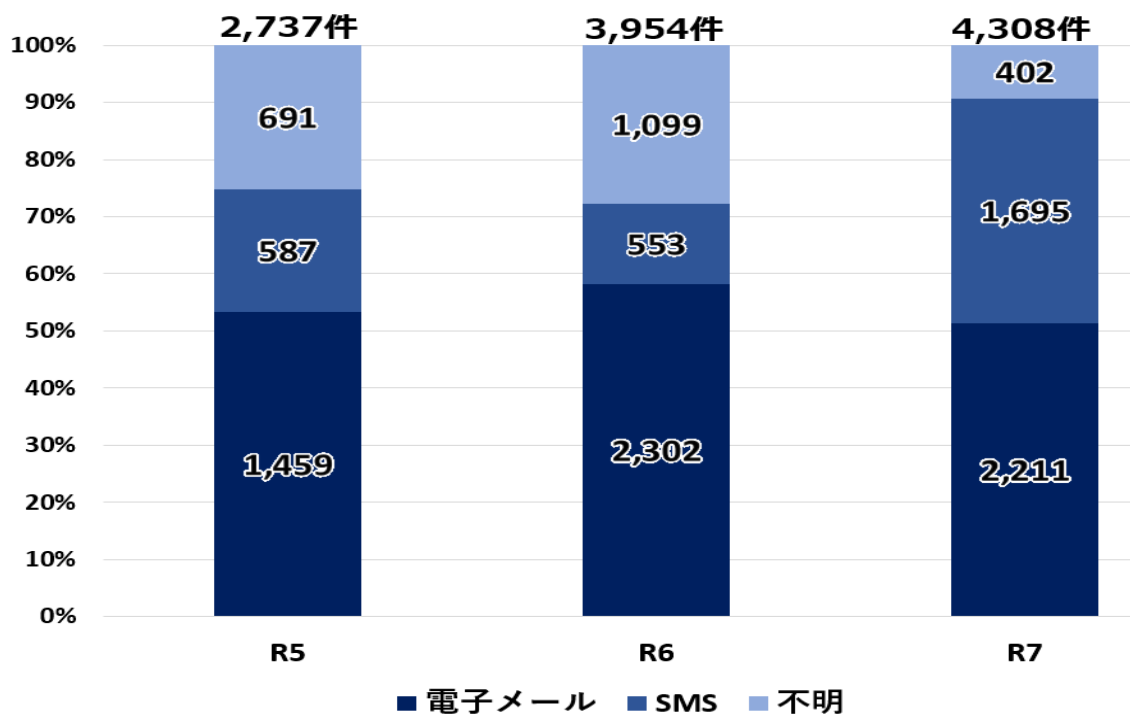


インターネットバンキング不正送金

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



過去3年の経年比較

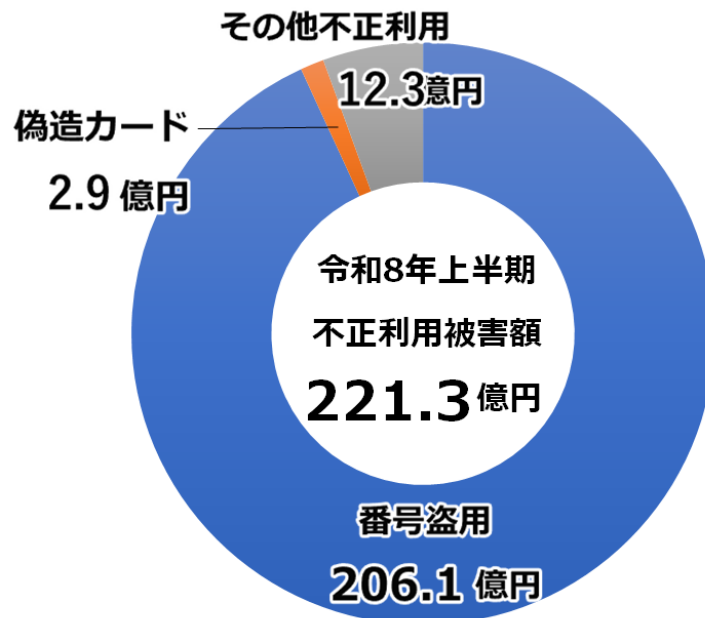


※ 令和5年から集計。

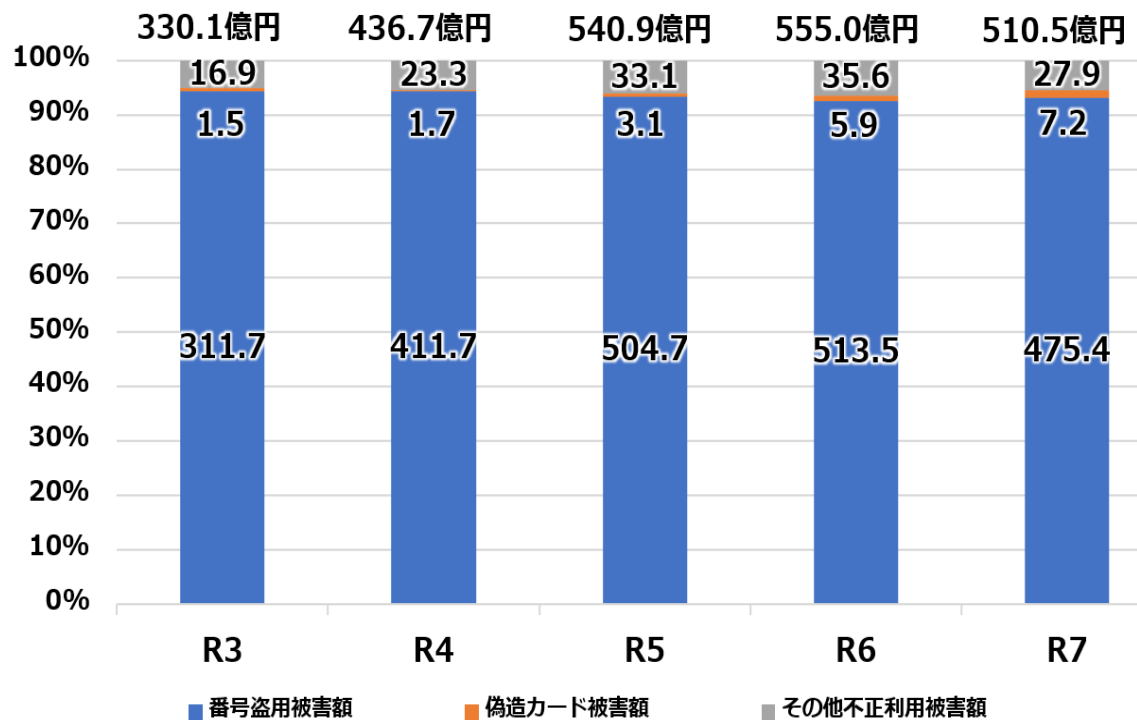
※ 令和7年中にSMSが増加した要因として、モバイルマルウェアに感染した端末を悪用して、フィッシングサイトへ誘導する悪質なSMSを大量配信されていることが考えられる。

クレジットカード不正利用

クレジットカード不正利用被害額



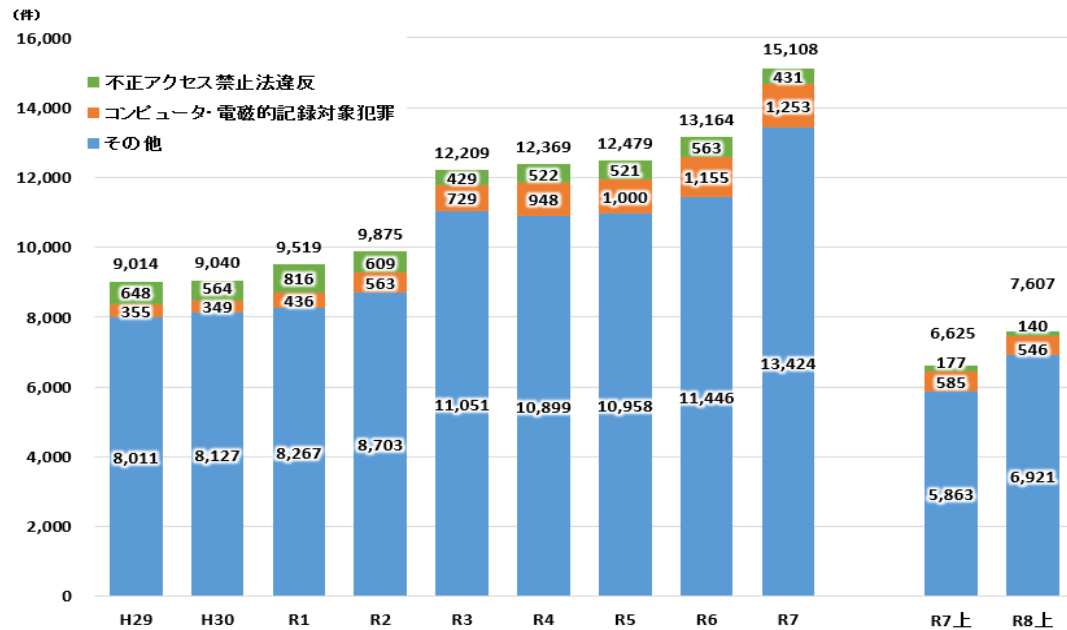
クレジットカード不正利用被害額



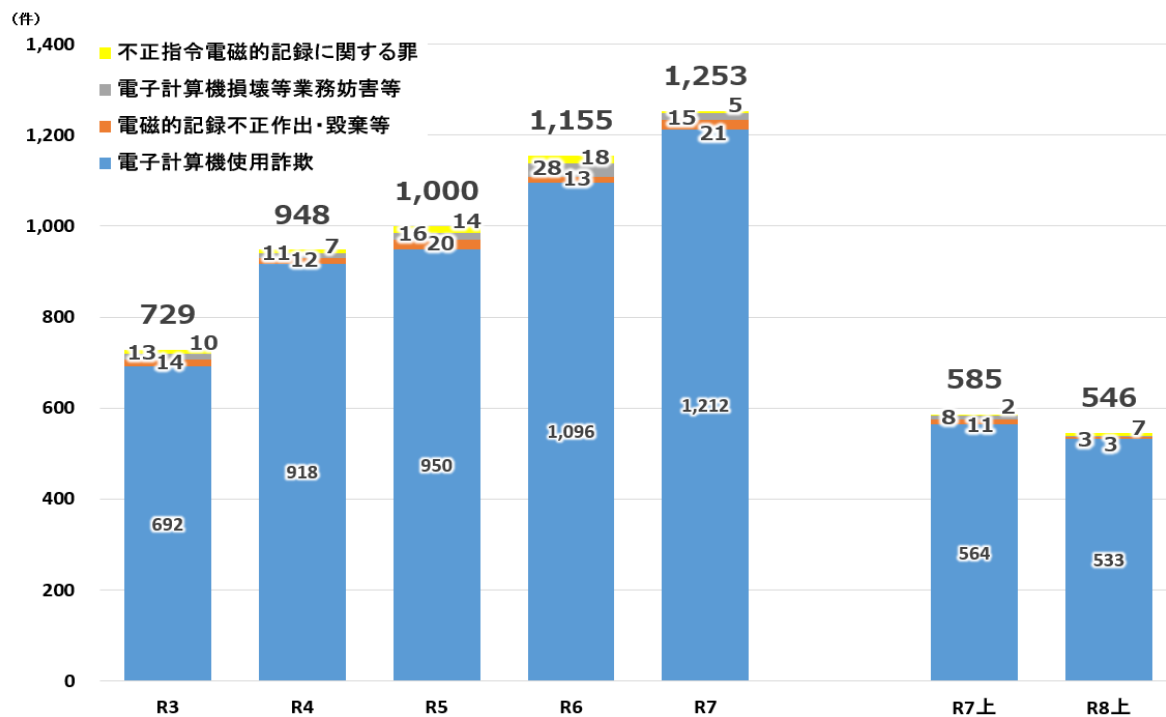
※ 「その他不正利用」とは、紛失・盗難カードによる不正利用などを指す。

サイバー犯罪①

サイバー犯罪¹の検挙件数



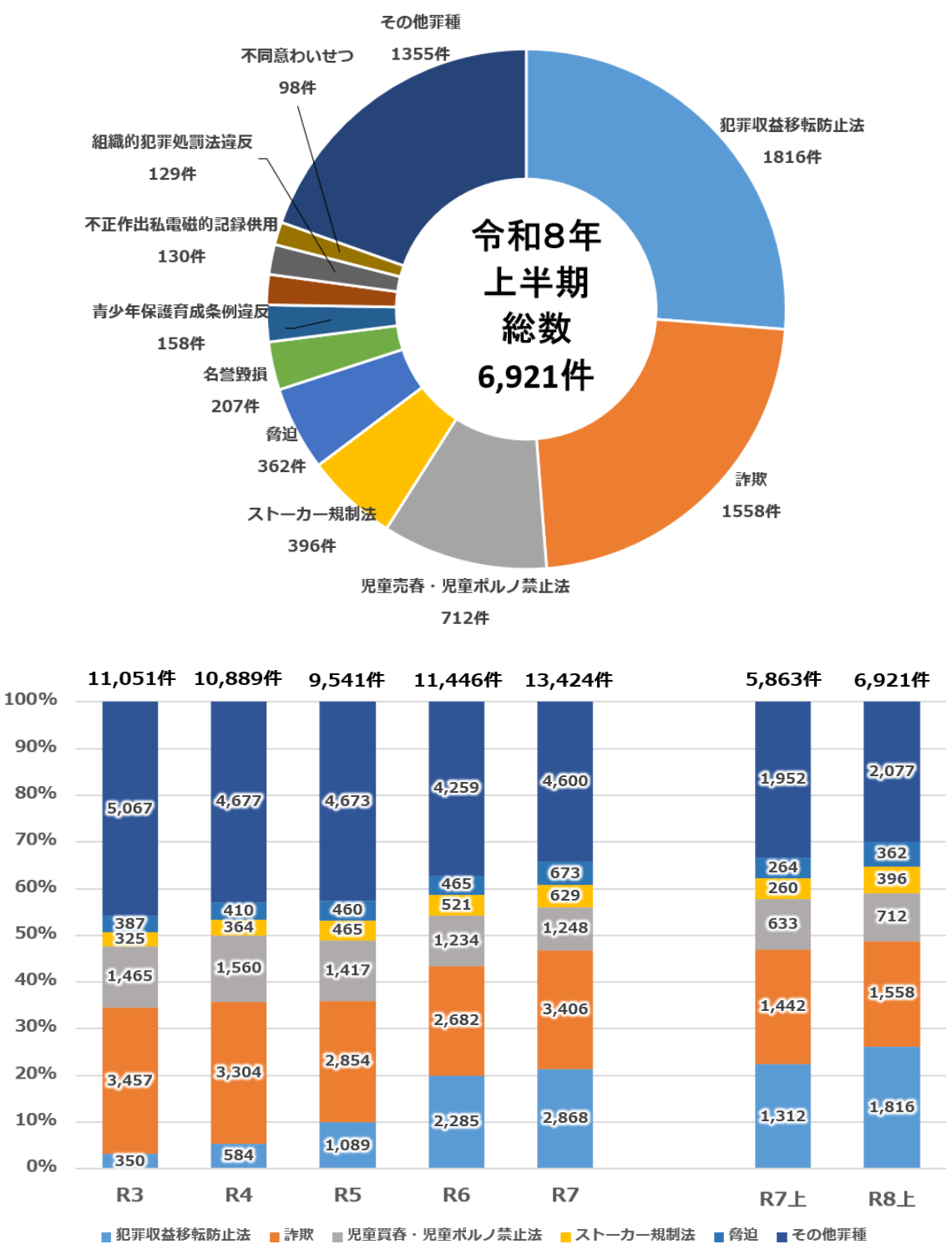
「コンピュータ・電磁的記録対象犯罪」の検挙件数



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

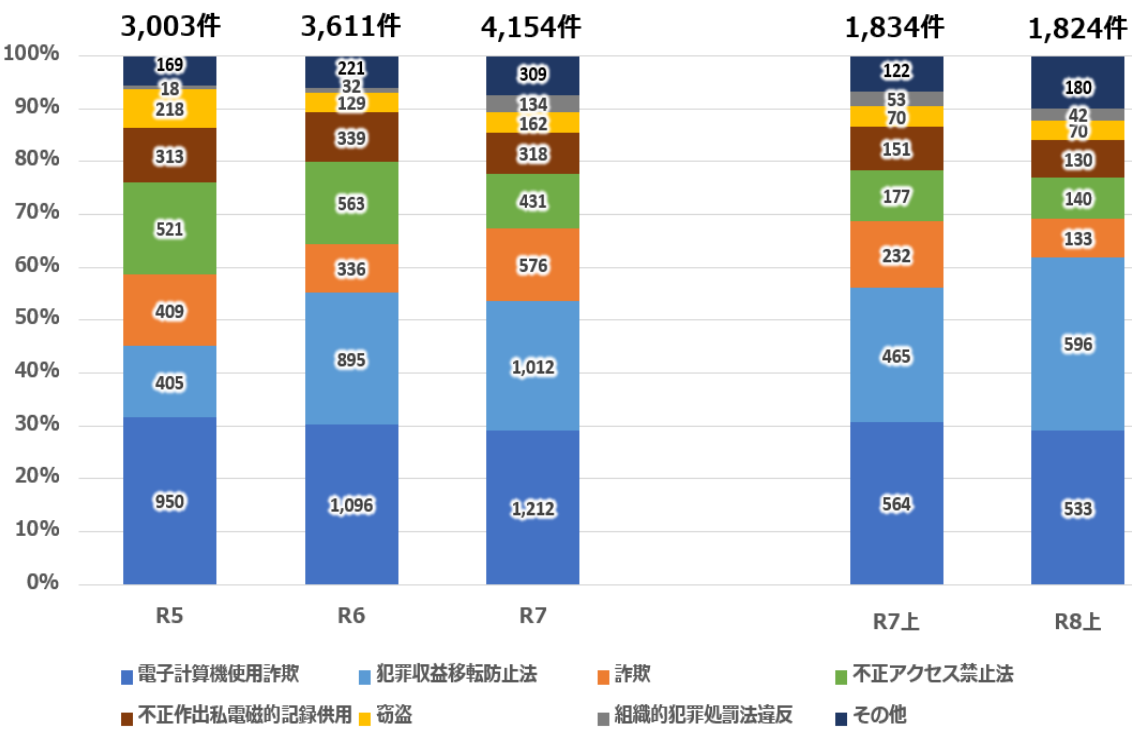
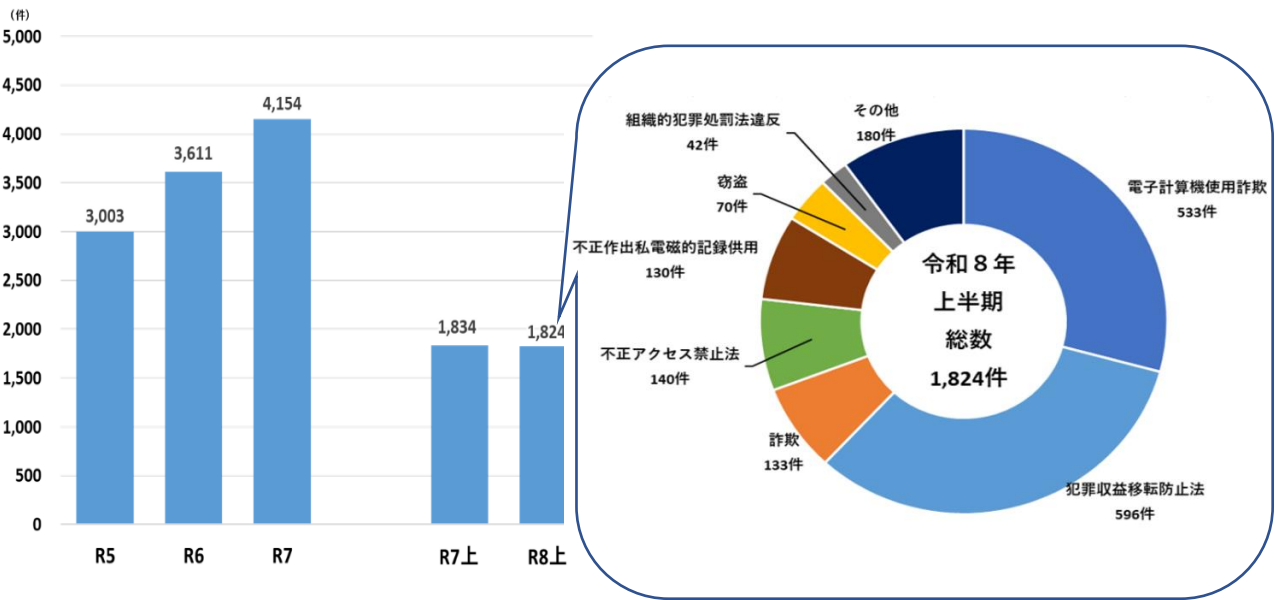
サイバー犯罪 ②

「その他」の検挙状況



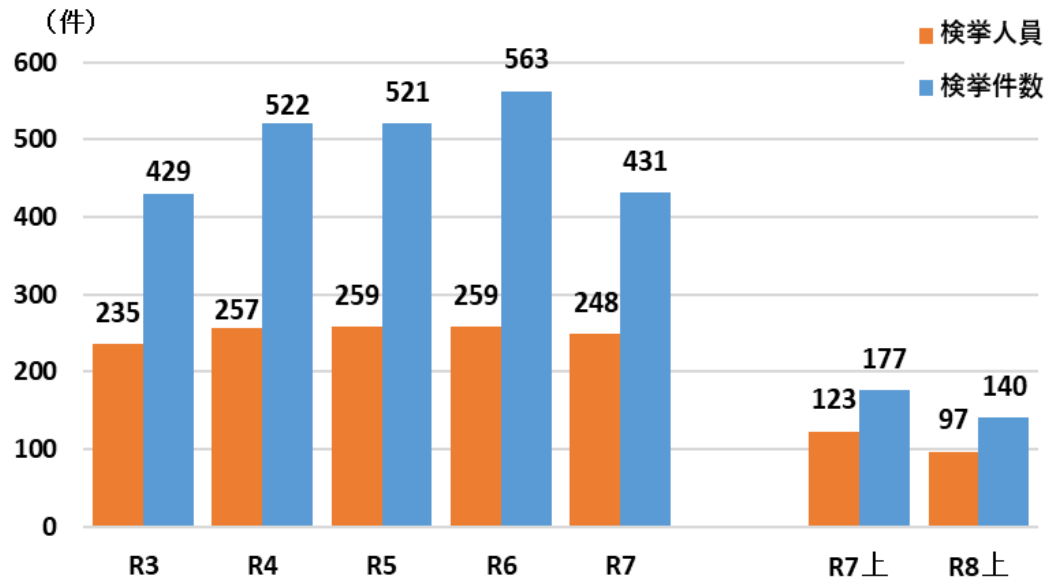
サイバー事案

サイバー事案の検挙件数



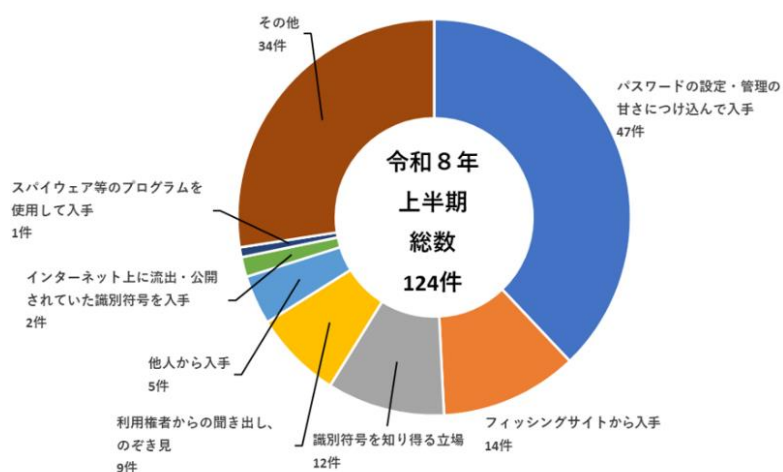
不正アクセス禁止法違反 ①

不正アクセス禁止法違反の検挙件数

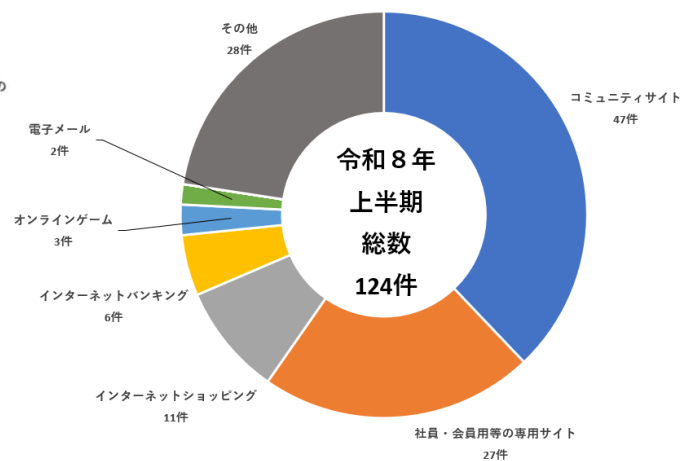


不正アクセス行為に係る手口別・サービス別検挙件数（識別符号窃用型）

【手口別】

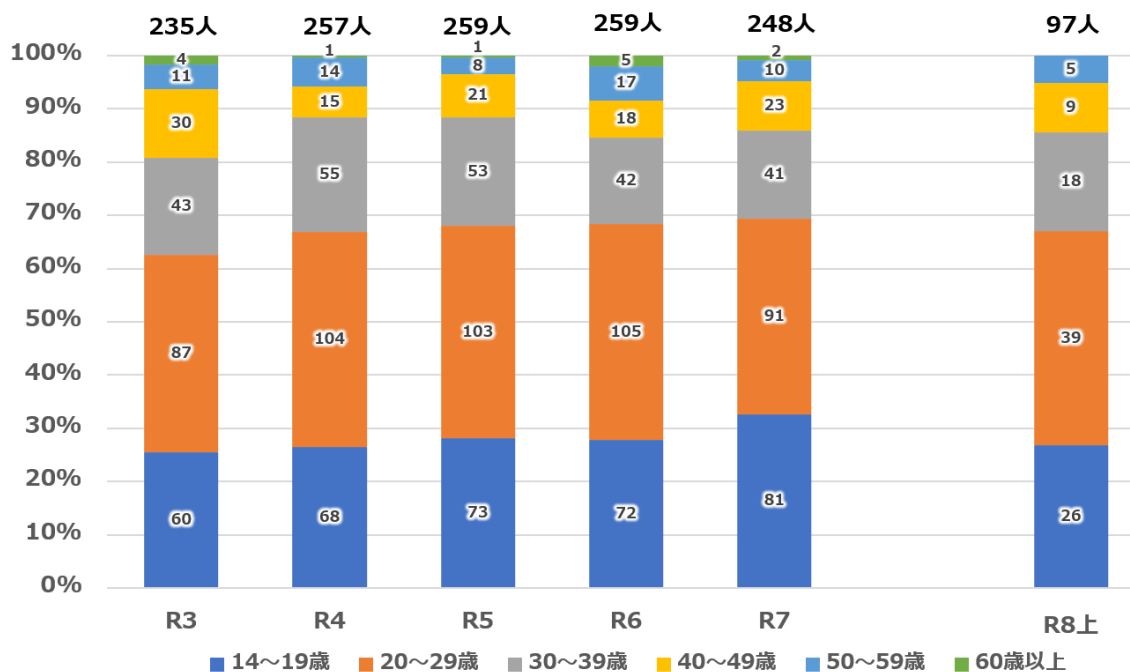
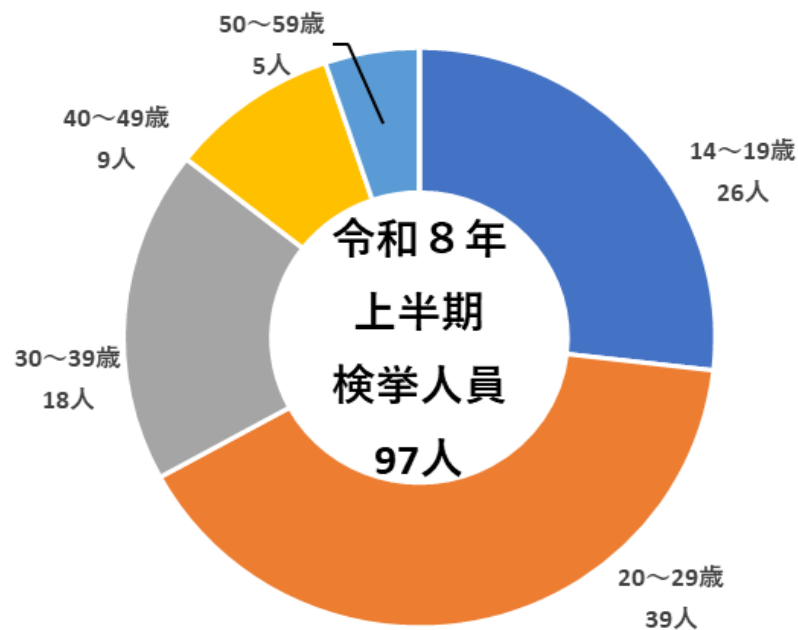


【サービス別】



不正アクセス禁止法違反②

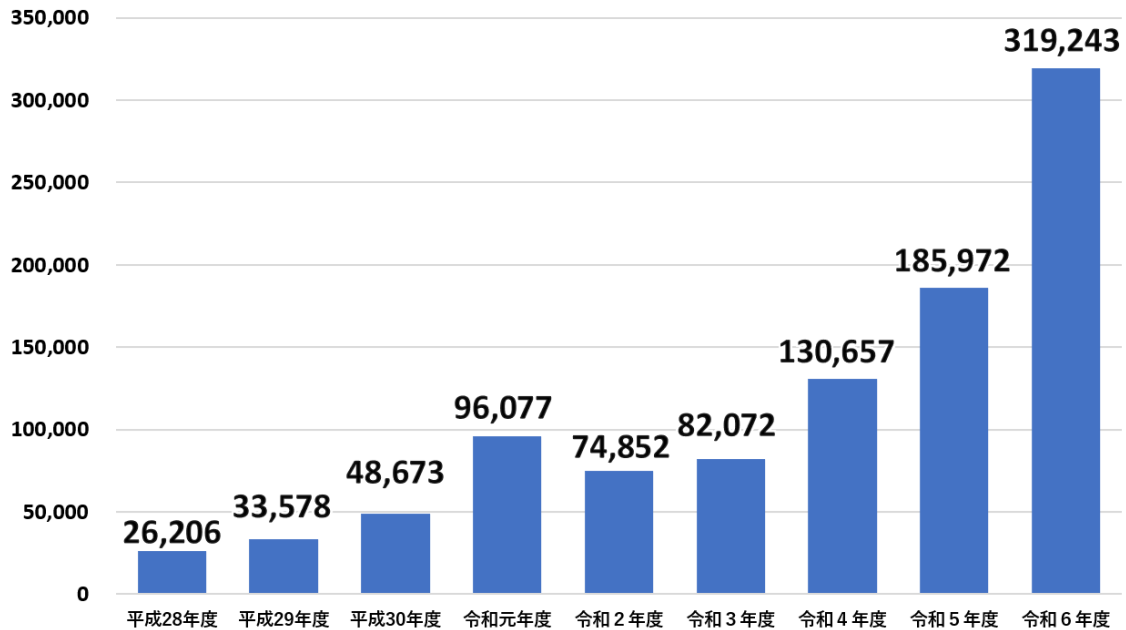
不正アクセス禁止法違反被疑者の年齢構成



サイバー保険契約に関する日本損害保険協会による調査結果

サイバー保険の契約件数

(件)

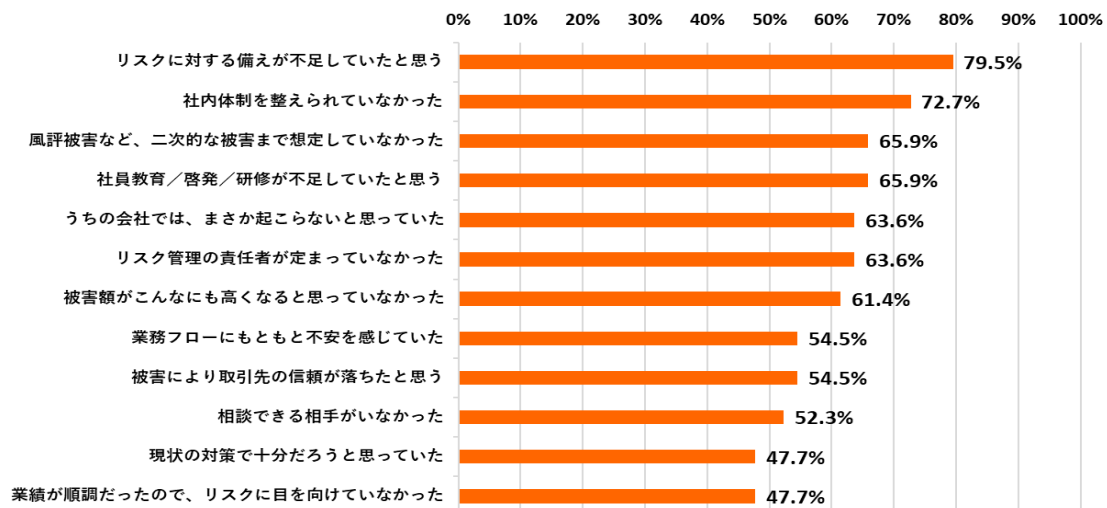


※一般社団法人日本損害保険協会の調査による。

サイバーリスクによる被害にあった企業の認識

全体(n=44)

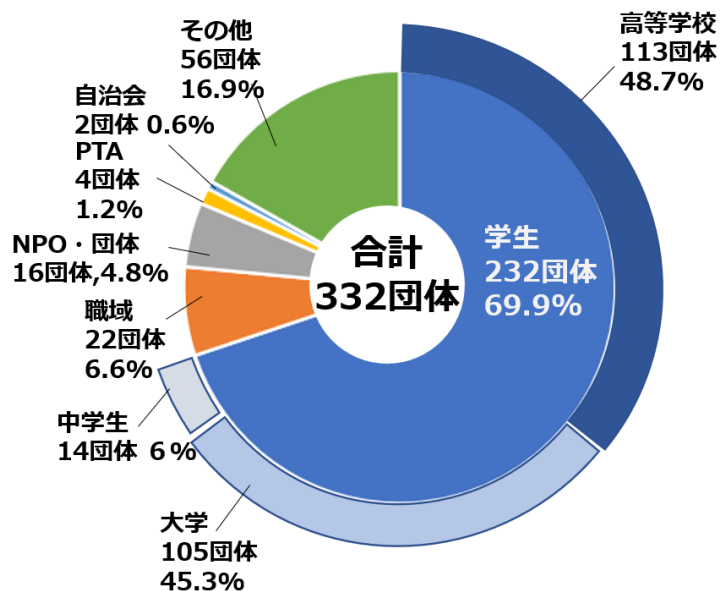
※サイバーリスクによる被害を被ったことがある企業の回答数



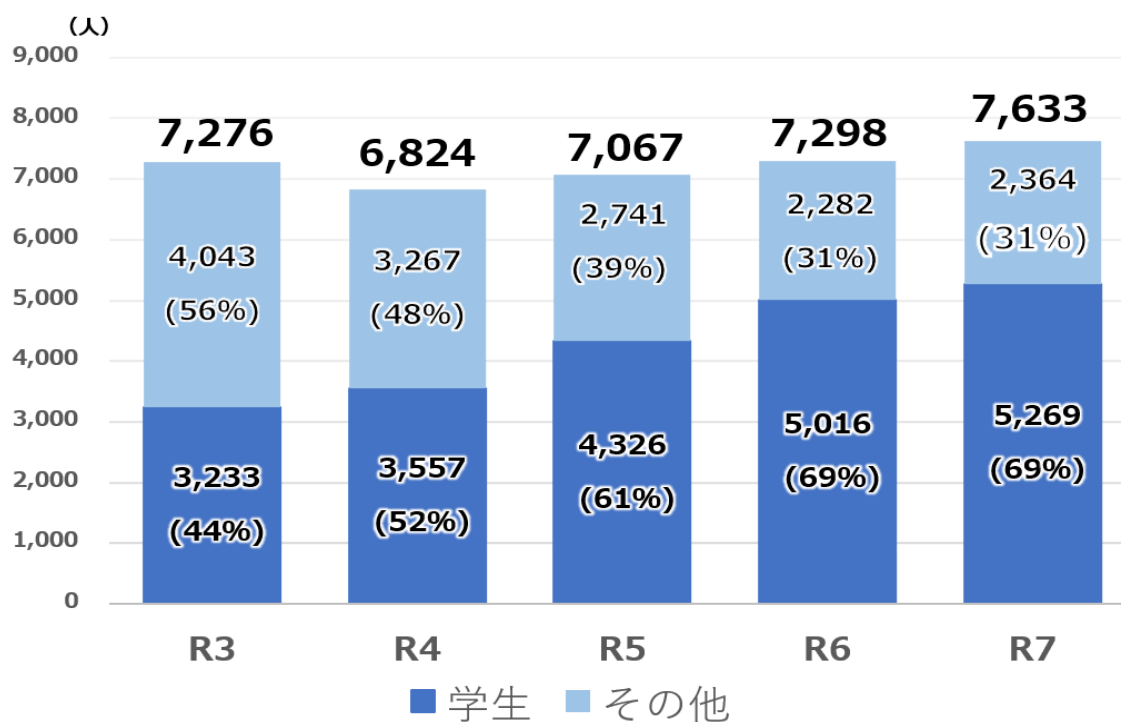
※一般社団法人日本損害保険協会の調査による。

サイバー防犯ボランティア団体数及び構成員数

サイバー防犯ボランティア団体構成



サイバー防犯ボランティア数（学生割合）



違法・有害情報に関する統計 ①

インターネット・ホットラインセンターの削除依頼対象

令和8年9月現在

インターネット・ホットラインセンターの削除依頼対象は、
① 民間団体である同センターにおいて、掲載情報のみから適切かつ円滑に該当性を判断することができるもの
② 総務省違法情報ガイドラインで定める情報等、事業者等による約款等に基づく削除対象となり得るもののいずれにも該当するものについて、法学者等の有識者で構成されるホットライン運用ガイドライン検討協議会で決定。

【違法情報】

【わいせつ関連情報】

- わいせつ電磁的記録記録媒体陳列
- 児童ポルノ公然陳列
- 売春目的等の誘引
- 出会い系サイト規制法違反の禁止誘引行為

【薬物関連情報】

- 薬物犯罪等の実行又は規制薬物の濫用を、公然、あおり、又は唆す行為
- 規制薬物の広告
- 指定薬物の広告
- 指定薬物等である疑いがある物品の広告
- 危険ドラッグに係る未承認医薬品の広告

【特殊詐欺等関連情報】

- 預貯金通帳等の譲渡等の勧誘・誘引
- 携帯電話等の無断有償譲渡等の勧誘・誘引
- なりすまし型偽投資広告を掲載する行為

【不正アクセス関連情報】

- 識別符号の入力を不正に要求する行為
- 不正アクセス行為を助長する行為

【無登録貸金業関連情報】

- 無登録貸金業者による広告

【銃砲等所持関連情報】

- 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

【犯罪実行者募集等関連情報】

- 犯罪実行者の募集
- 「送金犯罪」の依頼又は誘引行為

【違法オンラインギャンブル等関連情報】

- 国内にある不特定の者に対し違法オンラインギャンブル等ウェブサイト又は違法オンラインギャンブル等プログラムを提示する行為
- インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為

【有害情報】

【自殺誘引等情報】

自殺へ積極的に加担したり、自殺願望を持つ人の生命に危害を加えることとなる次に掲げる情報

- 自殺関与
- 自殺の誘引・勧誘

【重要犯罪密接関連情報】

個人の生命・身体に危害を加えるおそれが高い重要犯罪等と密接に関連する違法行為を直接的かつ明示的に請負・仲介・誘引等する次に掲げる情報

- 拳銃等の譲渡等
- 爆発物の製造
- 殺人・強盗・放火・誘拐等
- 麻薬売買
- 人身売買
- 硫化水素ガスの製造
- ストーカー行為等

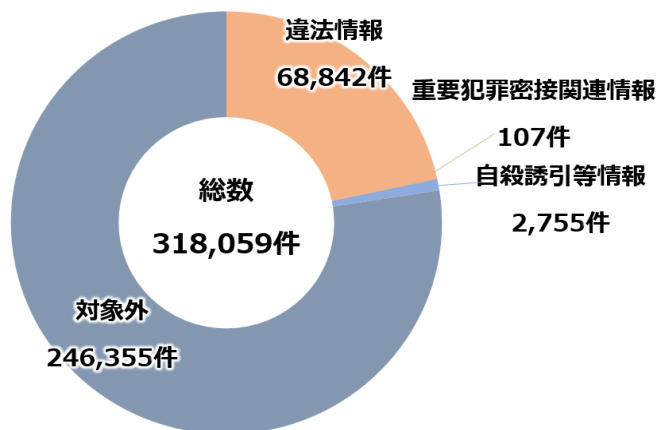
【類型別削除依頼件数等²³⁴（令和8年上半期）】

類型		判断件数			削除依頼			削除完了			削除率		
		国外	国内	計	国外	国内	計	国外	国内	計	国外	国内	計
違法情報	わいせつ	13,211	784	13,995	11,995	722	12,717	2,302	690	2,992	19.2%	95.6%	23.5%
	薬物	441	209	650	240	47	287	180	38	218	75.0%	80.9%	76.0%
	振り込め詐欺	3,838	1	3,839	2,345	1	2,346	988	1	989	42.1%	100.0%	42.2%
	不正アクセス	627	2	629	238	0	238	130	0	130	54.6%	—	54.6%
	無登録貸金業	31,864	89	31,953	20,984	77	21,061	16,249	27	16,276	77.4%	35.1%	77.3%
	銃砲等所持	0	1	1	0	1	1	0	1	1	—	100.0%	100.0%
	犯罪実行者募集	12,459	57	12,516	7,538	45	7,583	7,432	40	7,472	98.6%	88.9%	98.5%
	違法ギャンブル	4,981	278	5,259	4,715	273	4,988	751	149	900	15.9%	54.6%	18.0%
	小計	67,421	1,421	68,842	48,055	1,166	49,221	28,032	946	28,978	58.3%	81.1%	58.9%
有害情報	自殺誘引	2,676	79	2,755	2,625	79	2,704	2,409	65	2,474	91.8%	82.3%	91.5%
	重要犯罪密接	102	5	107	89	5	94	52	4	56	58.4%	80.0%	59.6%
	小計	2,778	84	2,862	2,714	84	2,798	2,461	69	2,530	90.7%	82.1%	90.4%
合計		70,199	1,505	71,704	50,769	1,250	52,019	30,493	1,015	31,508	60.1%	81.2%	60.6%

² 削除完了の件数については、削除依頼から5営業日後に確認した際の件数。
³ 警察が行うリプライ警告等により、削除依頼前に削除されるものもあるため、削除依頼に至らないものがある。
⁴ 「国外」とはプロバイダ等の所在地が不明又は国外に所在し、かつ、国外に所在するサーバに蔵置されている場合をいい、「国内」とは情報が日本国内のプロバイダ及びウェブサイト等に係るものである場合をいう。

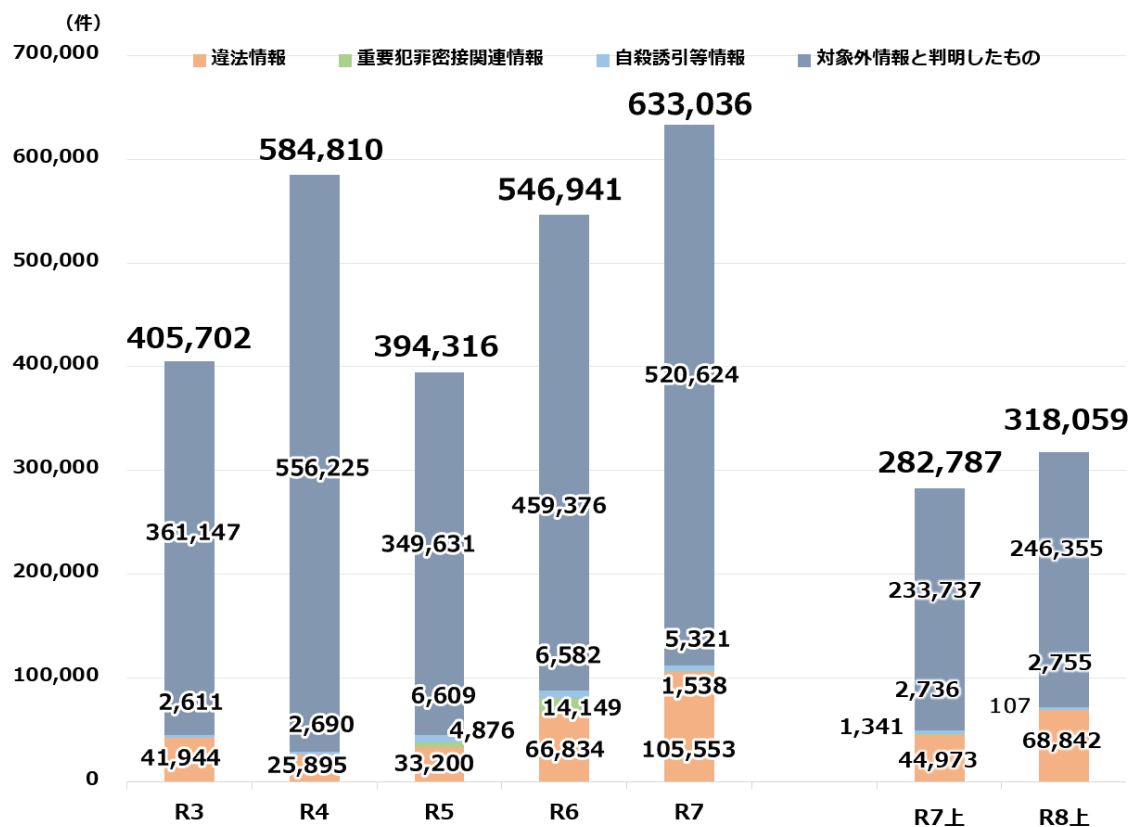
違法・有害情報に関する統計 ②

判断結果の内訳



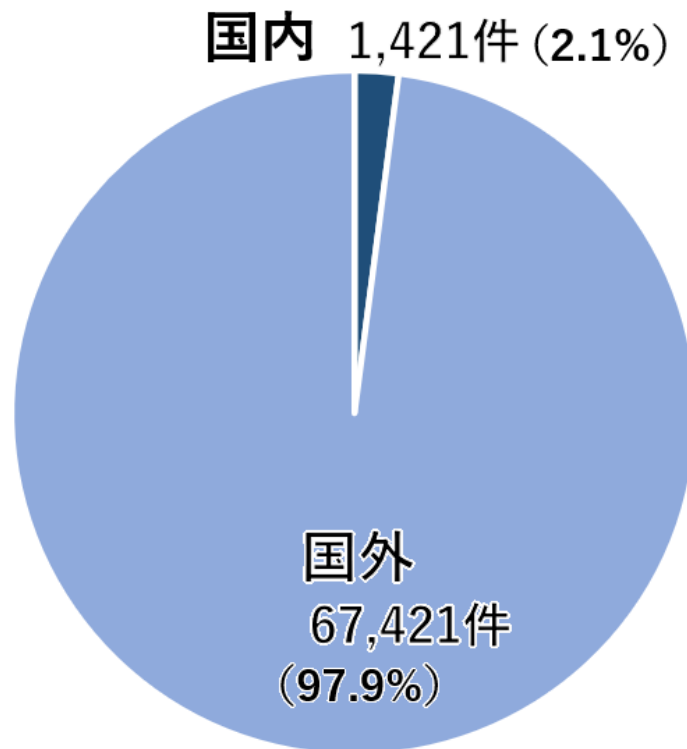
「違法情報」とは「インターネット上の流通が法令に違反する情報」を、「有害情報」とは違法情報に該当しないものの「犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない情報」を、それぞれいう。IHCでは、運用ガイドラインに基づき、「有害情報」のうち、個人の生命・身体等に危害を加えるおそれが高い重要犯罪等と密接に関連する「重要犯罪密接関連情報」と「自殺誘引等情報」を削除依頼の対象としている。

IHCにおける違法・有害情報の判断件数

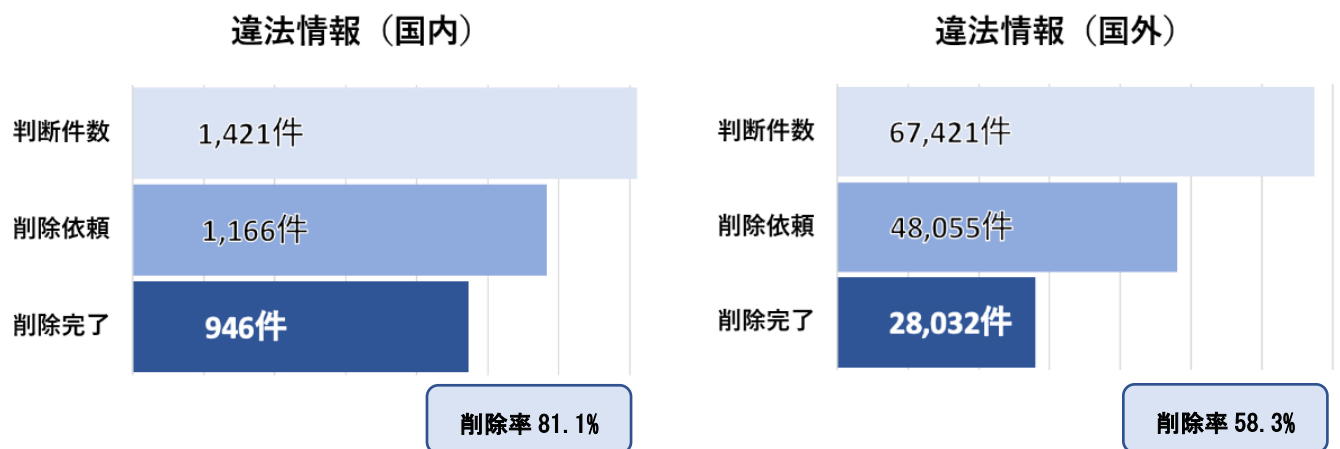


違法・有害情報に関する統計 ③

違法情報分析結果件数



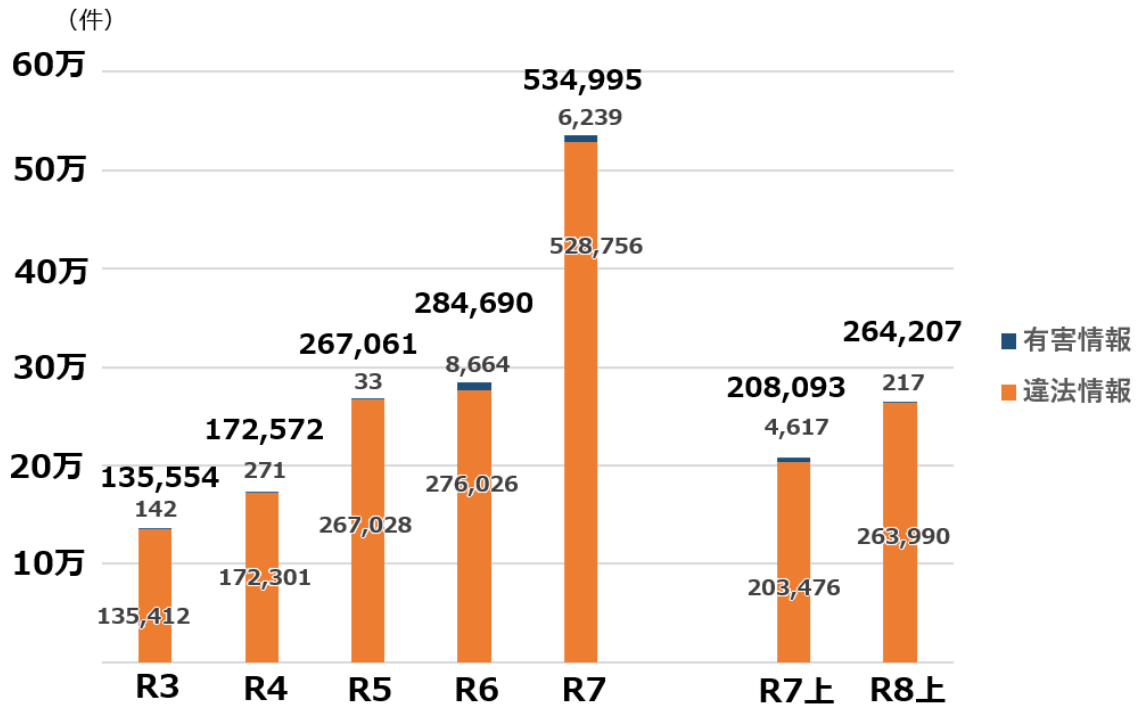
処理結果



統計編

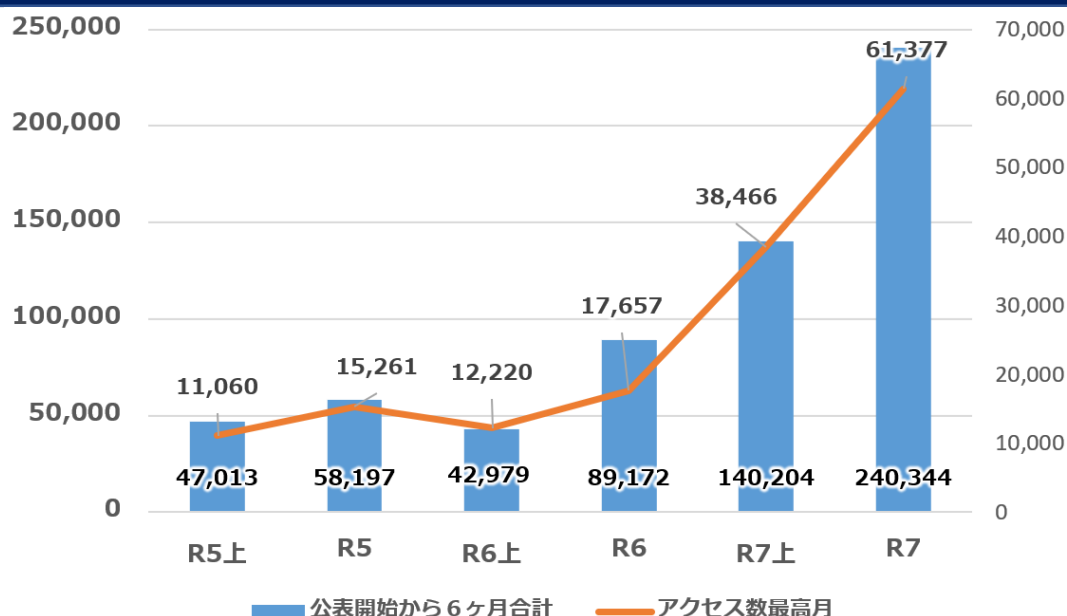
違法・有害情報に関する統計 ④

都道府県警察による違法・有害情報の削除依頼件数



類型		R3	R4	R5	R6	R7	R7上半期	R8上半期
違法情報	わいせつ	4,782	4,441	8,032	4,440	8,341	2,601	1,248
	事物	11,537	19,776	15,862	21,946	65,707	19,273	38,168
	振り込め詐欺	16,166	39,691	36,990	61,104	54,403	24,939	13,562
	不正アクセス	0	0	0	0	1	0	829
	無登録貸金業	70,835	65,966	161,970	167,193	365,519	143,075	188,395
	銃砲等所持	—	—	—	—	0	—	0
	犯罪実行者募集	—	—	—	—	10,514	—	20,432
	違法ギャンブル	—	—	—	—	70	—	122
	その他の違法情報	32,092	42,427	44,174	21,343	24,201	13,588	1,234
	小計	135,412	172,301	267,028	276,026	528,756	203,476	263,990
有害情報	自殺誘引	15	0	1	76	24	9	27
	重要犯罪密接	127	269	26	8,580	6,201	4,606	173
	その他の有害情報	0	2	6	8	14	2	17
	小計	142	271	33	8,664	6,239	4,617	217
合計		135,554	172,572	267,061	284,690	534,995	208,093	264,207

これまでの「サイバー空間をめぐる脅威の情勢等について」へのアクセス数



※上記グラフはそれぞれ以下の公表資料をさしている。

- R5上：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和5年9月公表）
- R5：令和5年におけるサイバー空間をめぐる脅威の情勢等について（令和6年3月公表）
- R6上：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月公表）
- R6：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月公表）
- R7上：令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和7年9月公表）
- R7：令和7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8年3月公表）

このグラフは、警察庁サイバー警察局が警察庁のホームページにおいて年2回公表している「サイバー空間をめぐる脅威の情勢等について」に関し、それぞれの公表後6か月間のアクセス数の合計及び公表後6か月間でアクセス数が最も多かった月のアクセス数を表したものである。

近年、合計アクセス数は右肩上がりであり、「サイバー空間をめぐる脅威の情勢等について」に対する国民からの関心・期待が年々大きくなっていることがうかがえる。

特に、令和8年3月に公表した「令和7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」にあっては、令和8年5月に月間アクセス数が6万1,377件を記録するなど、多くのアクセスが確認された。これは、同年4月以降、高性能AIの脅威についてニュース等で大きく取り上げられたことに伴い、AIを特集として扱った同レポートの閲読が増加したほか、AIを含むサイバー空間の脅威に対する社会的関心が一層高まったことが背景にあると考えられる。