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
警察庁サイバー警察局

はじめに

サイバー空間の匿名性を悪用したサイバー攻撃は、相対的に露見するリスクが低く、攻撃者側が優位にあることから、その脅威は急速に高まっている。また、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リスクをはらんでいる。具体的には、サイバー攻撃による機微情報の窃取、他国の選挙への干渉等は、国家を背景とした形でも平素から行われているとされ、さらに、武力攻撃の前から重要インフラの機能停止や破壊のほか、偽情報の拡散等を通じた情報戦が展開されるなどのハイブリッド戦が、今後更に洗練された形で実施される可能性が高いとされている。

加えて、社会全体のデジタル化の進展により、サイバー空間が重要な社会経済活動が営まれる公共空間へと変貌を遂げたことに伴い、匿名・流動型犯罪グループによる特殊詐欺やSNS型投資・ロマンス詐欺、暗号資産を悪用したマネー・ローンダリング等、その匿名性が悪用されているほか、生成AI等の高度な技術を悪用した事案や事業活動に支障をきたすランサムウェア事案も多発している 。

これらは、いずれも我が国の公共の安全と秩序に対する挑戦であり、我が国の国民生活・経済活動、ひいては国家安全保障や危機管理に深刻な影響を及ぼすおそれがあることに鑑みれば、これらの観点も踏まえつつ対処することが必要である。

他方で、サイバー空間の匿名性を悪用した事案を認知した段階においては、当該事案が、国家を背景とする事案か、犯罪組織による金銭目的の事案かなどを認定することは困難で、また、有事の準備行為として国家を背景とするサイバー攻撃が行われたとしても、その段階でその旨を直ちに覚知することも困難である。さらに、有事においても、警察は、国家安全保障や危機管理の観点を踏まえつつ、平時と同様の対処を求められることからすれば、警察は、全国隅々にまで張り巡らされた対処体制による、事案認知、捜査・実態解明、部門を越えた横断的・俯瞰的分析、検挙、パブリック・アトリビューション、さらにはアクセス・無害化措置まで、官民連携・国際連携を推進しつつ、シームレスに対処することが可能な組織であり、かつ、期待されている。

以上の情勢認識を踏まえ、本レポートにおいては、昨今、急速に社会へ浸透しているAIについて特集Ⅰとして、また、深刻な社会問題となっているランサムウェアについて特集Ⅱとして、それぞれ巻頭にまとめた上で、警察における取組を記載する第２部において、トピックスとして「国家安全保障におけるサイバー警察の果たす役割」と「サイバー空間における匿名性の打破に向けた警察の取組」を記載することとした。

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、さらに理解が深まれば幸いである。

本文目次
【特集・トピックス】

本文目次
【年次報告】

図表目次

【図表】

図表目次

コラム目次

【コラム】

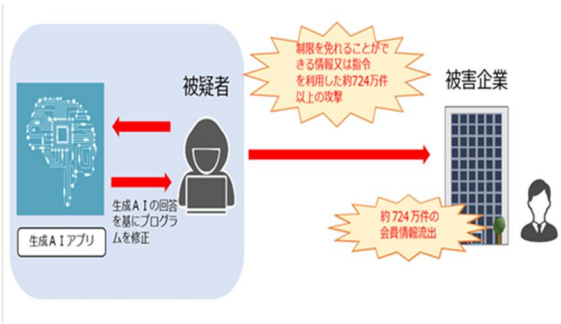
CASE 目次

【CASE】

概要　令和７年における脅威情勢　特集及びトピックス

特集Ⅰ　AI をめぐる脅威の情勢と警察の取組

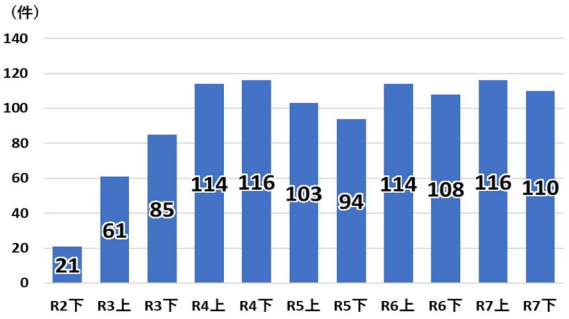
● 高校生の少年（17 歳）が、生成 AI を悪用して、複合カフェのアプリのサーバに不正な指令を送信して会員情報を漏洩させるとともに、アプリ機能の一部を停止させ、カフェ運営会社の業務を妨害。令和７年 12 月、同少年を不正アクセス禁止法違反及び偽計業務妨害罪で逮捕。（警視庁）



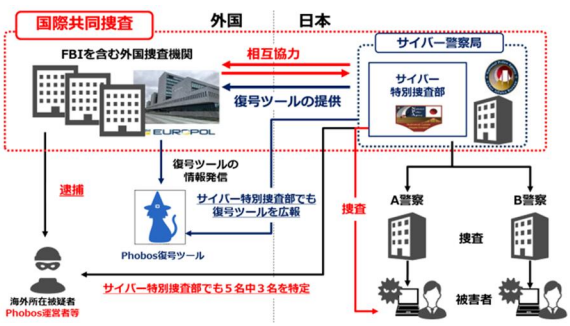
● ICPO・JC３と共催で「AI とデジタル・フォレンジック」をテーマに国際会議を開催し、世界各国から実務家・専門家が参加。 AI を悪用したサイバー攻撃やディープフェイク検知技術等について情報共有。

特集Ⅱ　ランサムウェアをめぐる脅威の情勢と警察の取組

● 令和７年におけるランサムウェアの被害報告件数は 226 件であり、依然として高水準で推移。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も複数発生。

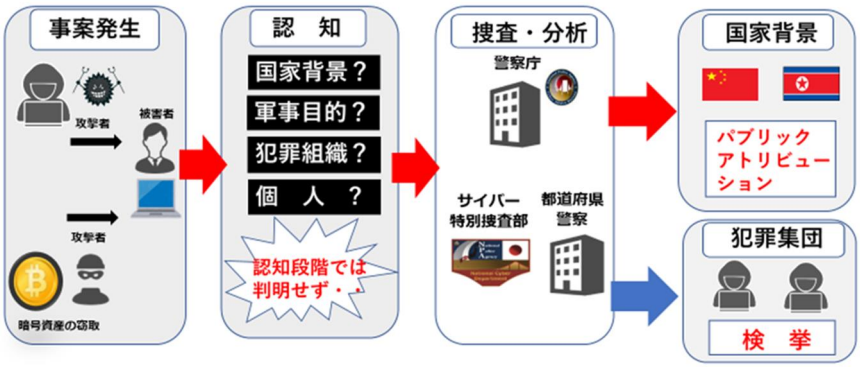


● ランサムウェアグループ「Phobos（フォボス）」「8Base（エイトベース）」について EUROPOL や FBI 等との国際共同捜査を推進。サイバー特別捜査部は、被疑者３名を特定したほか、暗号化されたデータを復号するツールを開発。



トピックスⅠ　国家安全保障におけるサイバー警察の果たす役割

● 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いため、全てのサイバー事案が安全保障に直結する事案である可能性も見据えながら、捜査権を有する警察が事案の捜査を行うとともに、実態解明を進めており、国家を背景としたサイバー攻撃への対応等、サイバー空間をめぐる国家安全保障の文脈においても、サイバー警察は重要な役割を果たしている。

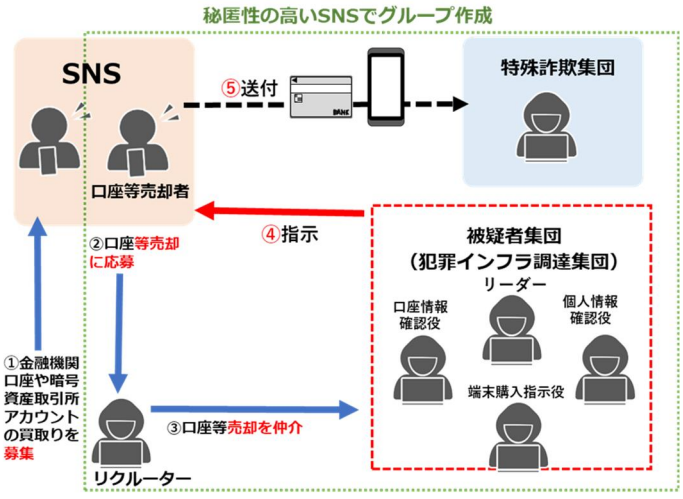


● 令和７年５月、第 217 回国会において、いわゆる能動的サイバー防御法（ACD 法）が成立し、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新設（令和８年 10 月１日に施行予定）。

トピックスⅡ　サイバー空間の匿名性の打破に向けた取組

● 匿名・流動型犯罪グループにおいては、犯罪収益を暗号資産に変換し、海外の暗号資産交換業者の口座に移転することで資金の流れを仮装・隠匿するなど、警察による検挙を免れるため、サイバー空間の匿名性を悪用している。

● 金融機関口座等の売却者等を募り、匿名性の高い SNS を利用して金融機関口座や暗号資産アカウントを不正に調達した上で、複数の特殊詐欺集団らに対して販売していた「道具屋」集団について、情報の集約や分析、隠匿された暗号資産の追跡により、当該犯罪集団の首魁らを特定し、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で逮捕。（愛知、サイバー特別捜査部等）

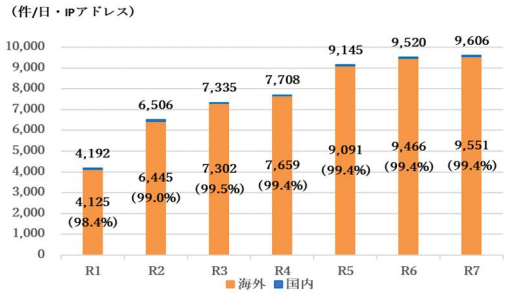


概要　令和７年における脅威情勢の概要

Ⅰ　サイバー空間の脅威情勢

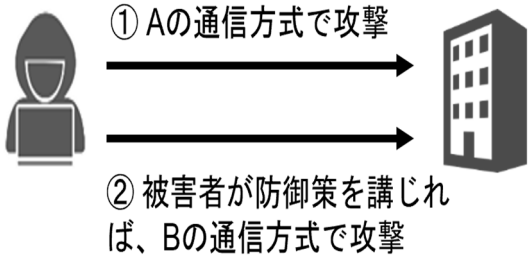
１　高度な技術を悪用したサイバー攻撃の脅威情勢

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



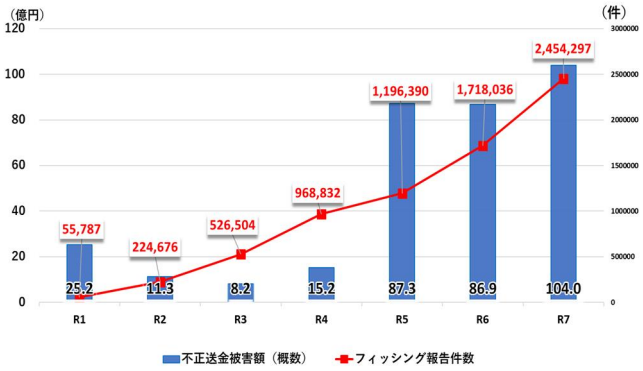
● 令和７年において、国家を背景とするサイバー攻撃グループ（APT 攻撃グループ）の関与が疑われるものが複数存在。特に情報窃取を目的としているとみられるサイバー攻撃が確認。

● 令和６年の年末から令和７年の年始にかけ、重要インフラ事業者等において、DDoS 攻撃によるとみられる被害が相次いで発生し、国民の生活に実際の被害。攻撃に対し事業者が遮断措置を講じた場合でも、状況に応じて手口を変化させ、攻撃を継続する事例を確認。



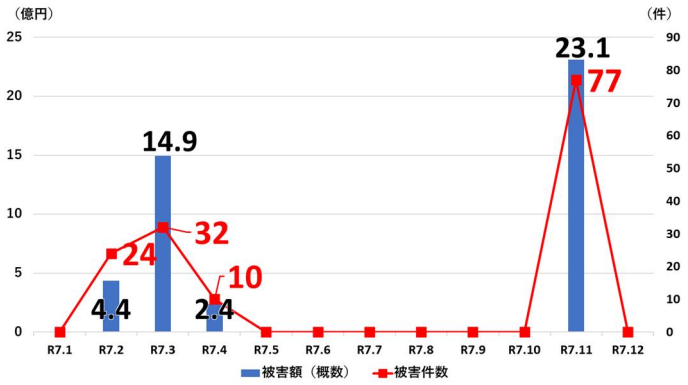
２　インターネット空間を悪用した犯罪に係る情勢

● 令和７年におけるフィッシング報告件数は、245 万 4,297 件であり、右肩上がりの増加が継続。インターネットバンキングに係る不正送金事犯の発生件数は 4,747 件、被害総額は約 103 億 9,700 万円となっており、フィッシングがその手口の約９割。



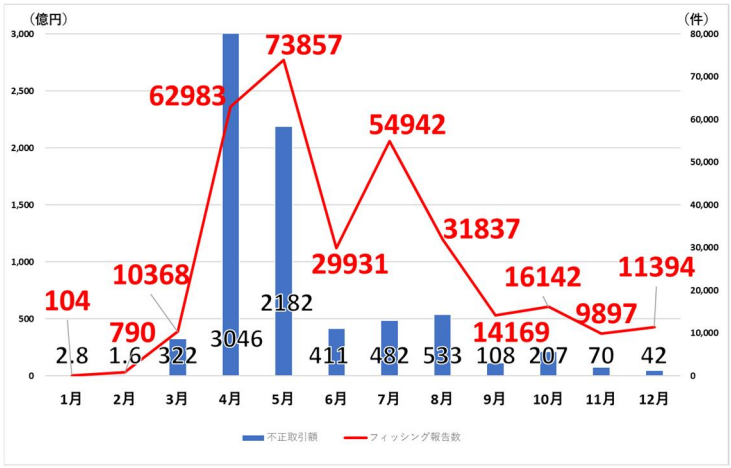
● ボイスフィッシングによる法人口座の不正送金被害が令和６年秋から令和７年４月にかけて急増。その後、同年 10 月まで発生が見られなかったが、11 月には被害が再び急増し、被害法人１社で４億円を超える被害も。

ボイスフィッシングによる不正送金被害件数・被害額



● 証券会社をかたるフィッシングメールの送付や証券口座への不正アクセス・不正取引が発生。令和７年の不正売買金額は約 7,408 億円、証券会社をかたるフィッシングメール報告件数は 31 万 6,414 件となるなど深刻な被害。

証券口座不正取引額とフィッシング報告件数の推移



３　違法・有害情報に係る情勢

● インターネット上には、犯罪や事件を誘発するような有害情報や、犯罪実行者募集情報や薬物関連情報等の違法情報が氾濫しており、深刻な治安上の脅威。令和７年のインターネット・ホットラインセンター（IHC）の受理件数のうち、運用ガイドラインに基づいて 63 万 3,036 件を分析した結果、違法情報を 10 万 5,553 件と判断。また、犯罪実行者募集情報を１万 4,241 件と判断。

犯罪実行者募集のイメージ

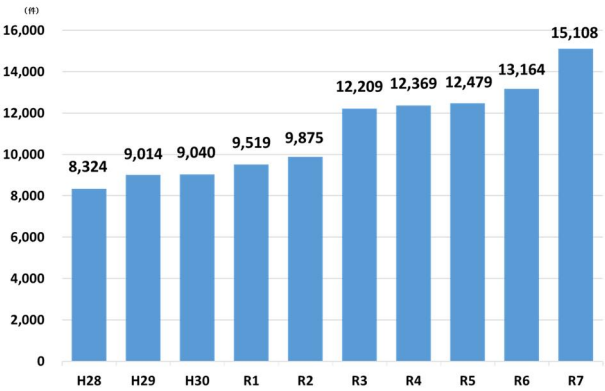
Ⅱ　警察の取組

１　検挙に向けた取組

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

●　令和７年におけるサイバー犯罪の検挙件数は１万 5,108 件に達し過去最高。

サイバー犯罪の検挙件数の推移



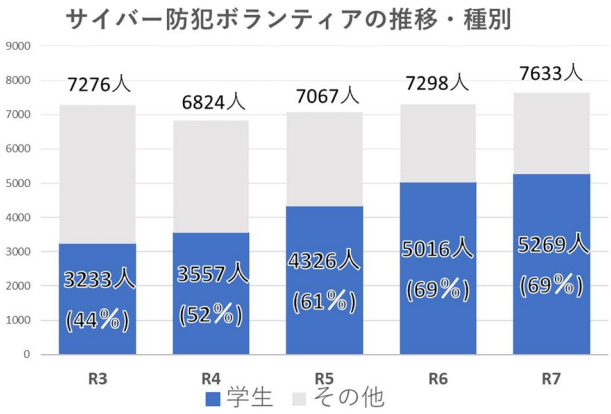
●　インド共和国・中央捜査局（CBI）とともに、日本人を標的としたサポート詐欺事件の国際共同捜査を行った結果、令和７年５月、CBI がインド共和国内に所在するインド人被疑者６人を逮捕。令和８年１月、警察庁サイバー捜査課長が CBI を訪問し、捜査協力への感謝状を手交。

●　令和７年 11 月、サイバー特別捜査部及び警視庁等の都道府県警察は、証券口座への不正アクセス及び不正取引に関し、中国籍の男(38)らを金融商品取引法違反（相場操縦行為等の禁止）及び不正アクセス禁止法違反で逮捕。

２　被害の未然防止・拡大防止に向けた取組

●　令和７年８月、警察庁及び国家サイバー統括室（NCO）は、米国、オーストラリア、ニュージーランド等と共に、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を行い、パブリック・アトリビューションとして、本件アドバイザリーを公表。

● 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であるサイバー防犯ボランティアは、全国で 322 団体、7,633 人（令和 7 年 12 月末現在）。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。

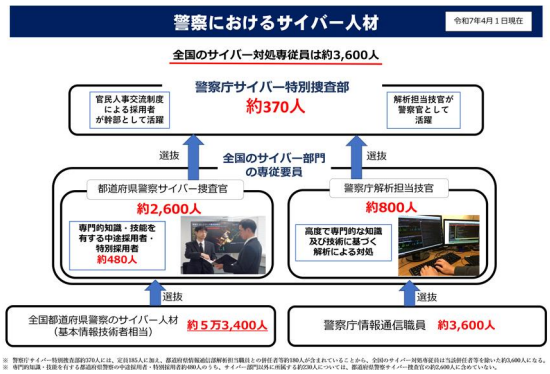


● 令和 7 年中は、IHC の運用ガイドラインを改定し、犯罪実行者募集情報やインターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を違法情報に追加するなど、違法・有害情報に関するインフラへの対処を強化。犯罪実行者募集情報に関しては、6,679 件の削除依頼に対し、6,351 件が削除完了（削除率約 95%）。

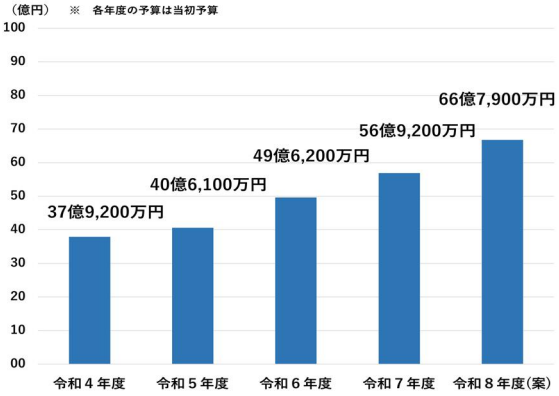
3　基盤整備

● 令和 7 年 4 月、サイバー特別捜査部に特別対処課を設置。捜査はもとより、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。

● 警察庁では、令和 8 年度からサイバー事案対処に専従する技術系職員の採用を予定（サイバー採用）。都道府県警察では、中途採用・特別採用された警察官等約 480 人がサイバー特別捜査官等として第一線で活躍。



● 令和 8 年度当初予算（案）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。



特集Ⅰ　AIをめぐる脅威の情勢と警察の取組

１　AI情勢

現在急速に一般社会で利用が広がっているAIについては、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。このような情勢を踏まえ、令和7年5月には、AIのイノベーションを促進しつつ、リスクに対応するため、AI法[1]が成立した。また、同年12月には、AI基本計画[2]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、AIの研究開発・活用の適正性を確保するためのAI指針[3]が決定された。警察庁では、AIの研究開発及び活用にかかる取組を関係省庁と連携して推進するため、人工知能戦略推進会議等を通じて、AI法に基づく検討に参画している。

令和6年2月に独立行政法人情報処理推進機構（IPA）を事務局として設置されたAIセーフティ・インスティチュート（AISI）についても、警察庁は、AISI関係府省庁等連絡会議等において、AIの安全性評価に関する基準や手法に関する検討に係る議論に参画している。令和7年12月の人工知能戦略本部において総理より、AISIの抜本的強化について指示がされているところ、警察庁も必要な協力を行い、AIセキュリティに万全を期していくこととしている。

２　AI技術の悪用事例

AIについては、不正プログラム、フィッシングサイトの作成、偽・誤情報作成への悪用、兵器転用、機密情報の漏えいといった、犯罪のリスクや安全保障への影響が懸念されている。実際に、生成AIを利用して不正プログラムを作成した容疑での逮捕事案のほか、生成AIを悪用した本人確認書類やわいせつ画像の作成といった事例が確認されている。また、日本警察は、インド共和国・中央捜査局（CBI）とともに日本人を標的としたサポート詐欺事件の国際共同捜査を行った（53頁参照）が、被疑者グループが生成AIを悪用し、標的の特定やポップアップの生成、日本語への翻訳をしていたことが判明している。

---

[1]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）

[2]人工知能基本計画（令和7年12月23日閣議決定）

[3]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）

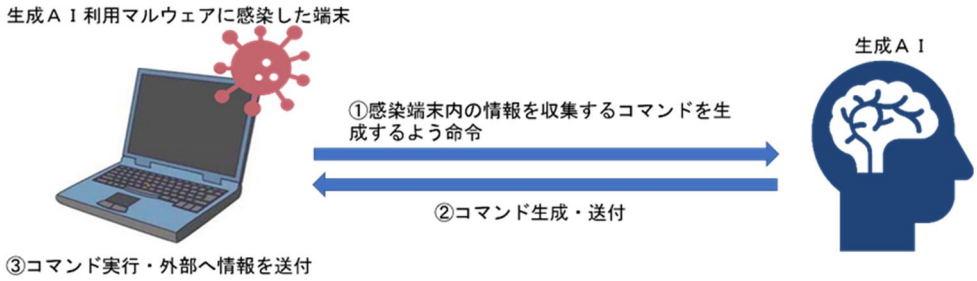
(1)　AI を悪用したサイバー攻撃に係る脅威情勢

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。自律的に作業を実行するシステムを AI エージェントというが、この事例は、AI エージェントによりサイバー攻撃の全工程をほぼ自律的に実行できることを示している。

【CASE：生成 AI を悪用するマルウェアの解析】

令和７年７月、海外において、政府職員を装った者が、生成 AI を悪用するマルウェアをメールに添付し、政府機関宛てに配布するサイバー攻撃が確認された。当該マルウェアはメールに添付されたファイルを開くことによって端末に感染するものであり、警察庁において本件に係るマルウェアの検体を解析したところ、マルウェア本体にはサイバー攻撃に関する命令が記録されておらず、感染先の端末が利用する生成 AI サービスを悪用して不正な命令を生成することが確認された。

【図表１：生成 AI を利用したマルウェアの動作イメージ】



(2) AI を悪用した犯罪に係る脅威情勢

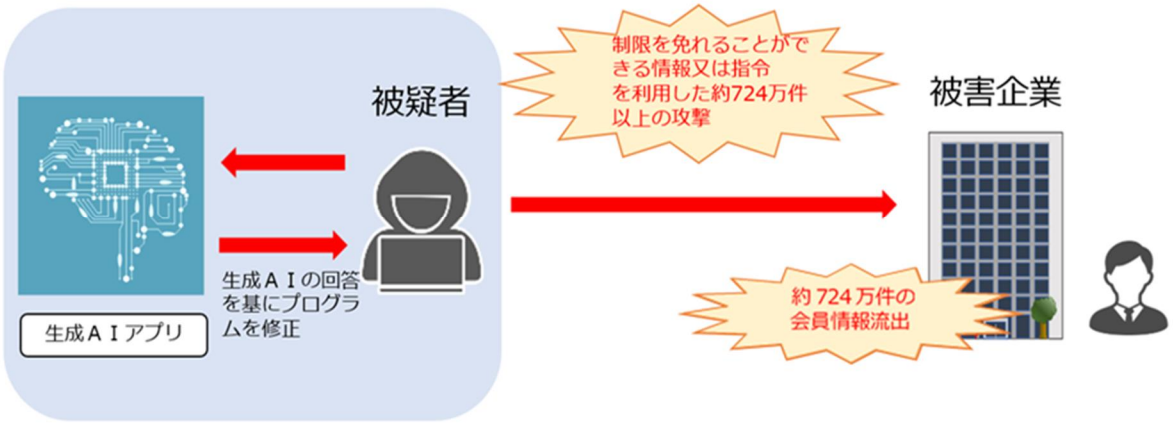
AI を悪用することで専門知識のない者でもサイバー攻撃に利用し得る情報へのアクセスが容易になると考えられる。

【CASE：生成 AI を悪用してフィッシングサイトを作成した被疑者の検挙】

無職の男（36）らは、令和６年６月及び９月、大手 EC サイトを装ったフィッシングサイトを公開するとともに、同年 11 月、不正に取得した他人の識別符号を保管した。本件では、フィッシングサイトを作成する際、生成 AI を悪用して改修を行っていたことが判明している。一般財団法人日本サイバー犯罪対策センター（JC3[4]）（56 頁参照）の捜査協力を得て、令和７年６月、同男らを不正アクセス禁止法違反（識別符号の入力要求及び保管）で逮捕した（大阪）。

【CASE：生成 AI を悪用して不正プログラムを作成した被疑者の検挙】

高校生の少年（17 歳）は、令和７年１月、生成 AI を悪用して、複合カフェのアプリのサーバに約 724 万件の不正な指令を送信して会員情報を漏えいさせるとともに、同アプリ機能の一部を停止し、同カフェ運営会社の業務を妨害した。令和７年 12 月、同学生を不正アクセス禁止法違反及び偽計業務妨害罪で逮捕した。（警視庁）



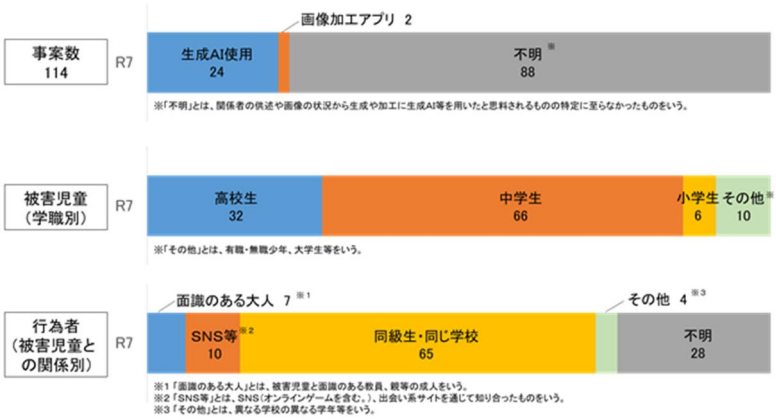
【図表２：生成 AI を悪用した不正プログラム作成の概要】

(3) 児童の性的加工画像

生成 AI サイトや画像加工アプリ等により、実在する児童の画像を性的に加工して悪用する事案について、警察庁では、令和７年における都道府県警察の取

[4] Japan Cybercrime Control Center の略

扱い事案の実態把握[5]を実施した。令和７年中の取扱い事案数は　114 件で、このうち生成 AI が使用されたと認められる事案は、24 件であった。



【図表３：児童の画像を生成 AI 等により性的に加工し悪用した事案】

また、被害児童の学職別では、被害児童が高校生の事案は 32 件、中学生の事案は 66 件、小学生の事案は 6 件であった。

被害児童と行為者の関係については、面識のある大人が７件、SNS 等が 10 件、同級生・同じ学校が 65 件であった。

警察では、相談者・被害者の心情に配意しつつ、事案の内容に応じて刑法（名誉毀損罪、わいせつ物頒布罪等）等での検挙や指導警告等を実施している。

コラム：AI とデジタル・フォレンジックに係る国際会議の開催

令和７年 10 月、ICPO・警察庁・JC3 共催で AI とデジタル・フォレンジックに係る国際会議「Interpol Conference on AI in Digital Forensics」を開催した。同会議には、外国治安機関等、民間企業、学術機関等から 90 人を超える実務者・専門家が参加し、各国で顕在化している AI を悪用した犯罪手口やディープフェイクを検知するための技術等について情報共有や討議が行われた。

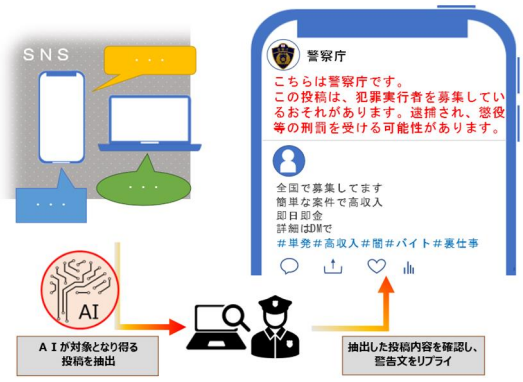
【サイバー警察局長による国際会議での説明の様子】

[5] 警察が把握した生成 AI などを悪用して児童（18 歳未満）の性的画像を作成した事案で、相談・被害申告時に相談・被害者が 20 歳未満であるもの。

３　警察における AI 技術の利活用に向けた取組

(1)　犯罪実行者募集情報への対策

警察庁では、令和６年２月、AI を活用して SNS 上の犯罪実行者の募集投稿等を効率的に抽出する仕組みを構築し、同年４月からは、返信（リプライ）機能を活用した投稿者等に対する迅速な個別警告（AI リプライ）等を実施しており、令和７年中には、6,829 件の個別警告を実施している。



【図表４：AI を活用した個別警告の実施】

(2)　サイバーパトロールの高度化

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）[6]では、SNS 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[7]を自動収集してその該当性を判定する AI 検索システムを導入し、サイバーパトロールの高度化を図っている。

(3)　フィッシングサイト判定の高度化・効率化

警察庁では、フィッシング対策として各都道府県警察等が相談等を通じて把握したフィッシングサイト URL 情報を集約・判定し、フィルタリング事業者等に提供しているところ、令和８年２月に生成 AI 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。

---

[6] 65 頁参照

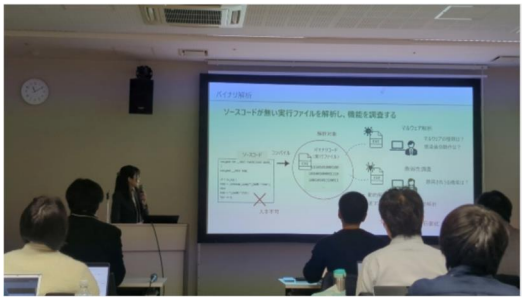
[7] インターネット上に流通することによって、個人の生命・身体に危害を加えるおそれが高い重要犯罪又は重要犯罪に発展する危険性がある犯罪と密接に関連している次の情報　①拳銃等の譲渡等、②爆発物の製造、③殺人等（殺人、強盗、不同意性交等、放火、誘拐、傷害、逮捕・監禁、脅迫）、④臓器売買、⑤人身売買、⑥硫化水素ガスの製造、⑦ストーカー行為等

(4)　生成 AI による不正プログラム解析の効率化

警察庁の情報技術解析部門においては、解析の高度化・効率化を推進しているところ、例えば、情報セキュリティ大学院大学に職員を派遣し、不正プログラム解析の効率化を目的とした機械学習に関する研究を行った。本研究によって開発した不正プログラムの機能を推定する生成 AI「リブラマ（RevLlama）」を実業務に活用するため、過去に実施した不正プログラムの解析結果を学習させたところ、不正プログラムの一部の機能をＡＩで推定できた。

コラム：サイバーセキュリティ対策研究センターにおける取組

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、サイバー事案に悪用される不正プログラム解析のため、生成 AI を活用した解析の高度化に向けた研究を行っている。令和７年度は、学術機関と共同研究を実施し、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。



【研究結果の発表の様子】

４　今後の展望

AI が社会にもたらす影響に鑑みれば、警察においても、これに積極的に対応することが必要不可欠である。警察では、犯罪実行者募集情報の収集に AI を活用しているほか、匿名・流動型犯罪グループやローン・オフェンダーの対策に AI を活用すべく現在取組を推進している。他方、AI を悪用して、不正プログラムを作成した事案等もあるところ、AI 基本計画においては、警察活動の高度化のための AI 利活用や AI を悪用する犯罪等への対処について記載されている。また、サイバーセキュリティ戦略において、AI を活用したサイバーセキュリティ確保に向けた取組や、AI により一層脅威が高まると予想されるサイバー攻撃の被害の防止に向けた取組等を推進する旨が記載されている[8]。警察では、これらの政府決定文書を踏まえ、各種施策を強力に推進し、国民の期待と信頼に応えていく。

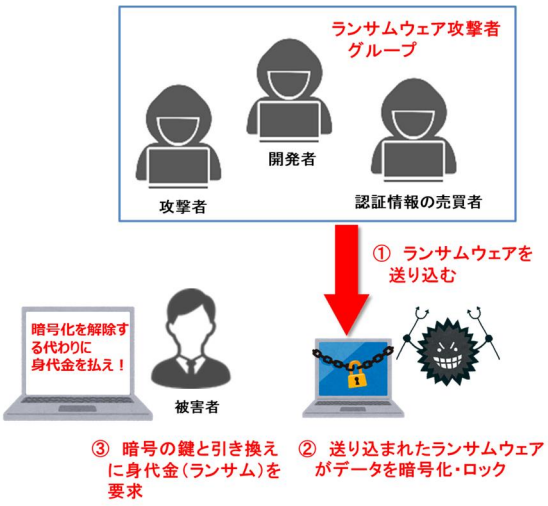
[8] サイバーセキュリティ戦略Ⅱ.3.（３）.①.参照

特集Ⅱ　ランサムウェアをめぐる脅威の情勢と警察の取組

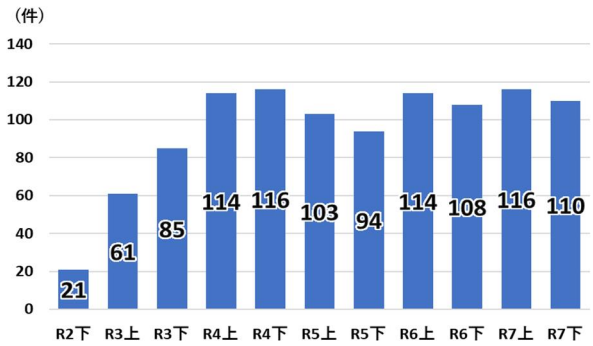
１　ランサムウェアの情勢

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、ダークウェブ上のリークサイト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。

【図表５：ランサムウェア攻撃の概要】



【図表６：ランサムウェア被害報告件数】



令和７年におけるランサムウェアの被害報告件数は 226 件であり、依然として高水準で推移しているところ、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も複数発生した。

【CASE：令和７年下半期に発生した主なランサムウェア攻撃事案】

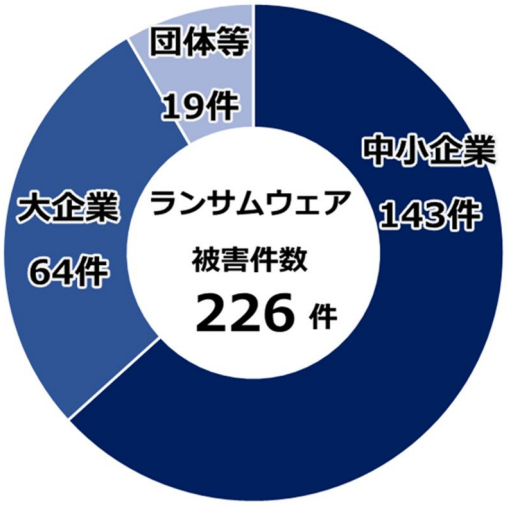
令和７年９月、飲料メーカー大手が自社のサーバがランサムウェアによる攻撃を受けたことを公表した。当該企業の調査によれば、攻撃者は当該企業のグループ内のネットワーク機器を経由することで、データセンターのネットワークに侵入、ランサムウェア攻撃を実行することで複数のサーバのデータを暗号化した。この攻撃により、製品の受注・出荷が停止したほか、顧客や従業員等の個人情報約 191 万件が漏えい又はそのおそれがあるとしている。

また、同年 10 月にも通販大手が、自社のサーバがランサムウェアによる攻撃を受

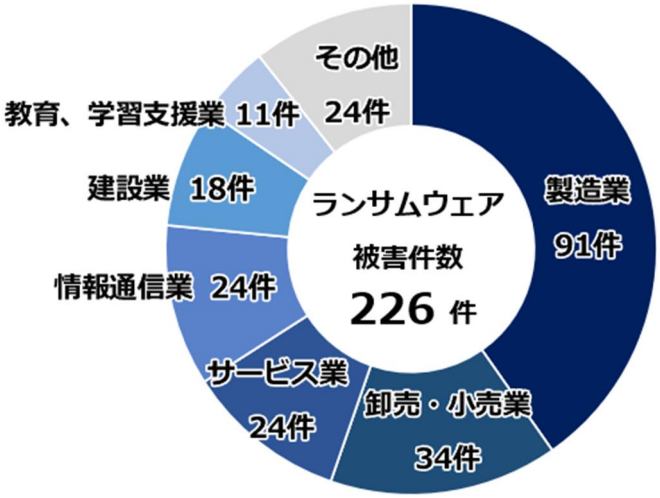
けたことを公表した。当該企業の調査によれば、攻撃者は認証情報を窃取し、不正に使用することで複数のサーバにアクセスし、ランサムウェア攻撃を実行した。この攻撃により、製品の受注・出荷について影響が出ているほか、顧客や従業員等に関する個人情報約 74 万件について漏えいのおそれがあることが判明している。

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４割を占め、続いて卸売・小売業、サービス業、情報通信業が上位となっているが、様々な業種で被害が確認されている。

【図表７：被害企業・団体等の規模別件数】

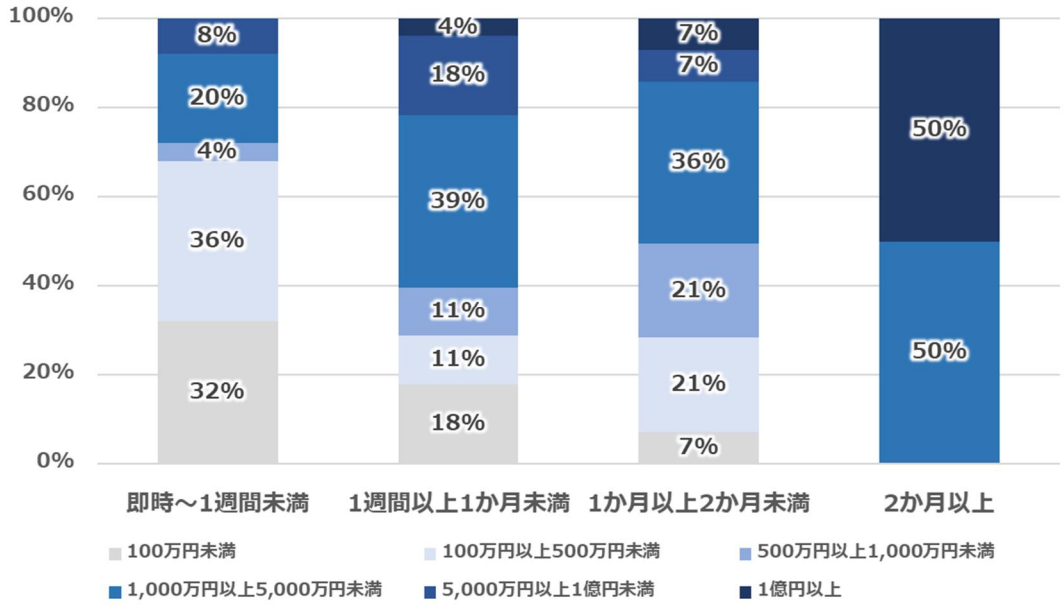


【図表８：業種別件数】



令和７年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、令和６年に引き続き、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５割を超えている。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割強に留まるなど、被害が長期化する傾向にあり、被害組織の経営に与える影響は決して小さくないと考えられるとともに、被害組織の業種によっては国民の生活にも大きく影響を与えることとなる。（統計編 125 頁・126 頁参照）

【図表９：ランサムウェア被害からの復旧期間と費用の関係】



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

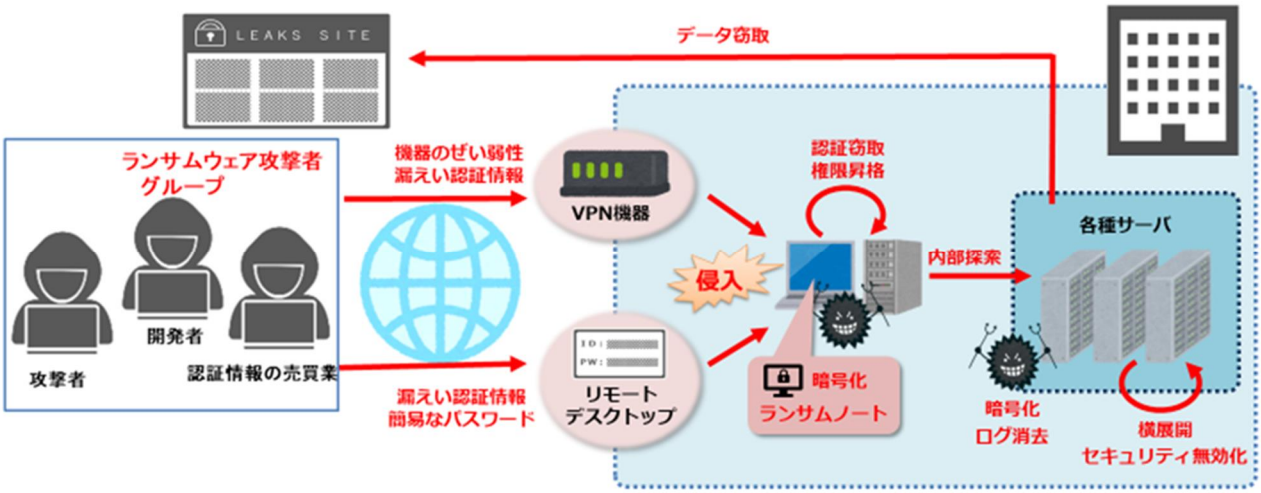
２　ランサムウェア攻撃の手口

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）が確認されており、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、企業等組織に対する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 VPN（Virtual Private Network）機器が６割以上を占める状況である。攻撃者は、未修正のぜい弱性、漏えいした認証情報や簡易なパスワード、設定不備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、ネットワーク内部を探索して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、データをクラウドストレージ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。復旧を妨害するため、バックアップも一緒に暗号化される場合が多い。最後に、「脅迫状（ランサムノート）」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。

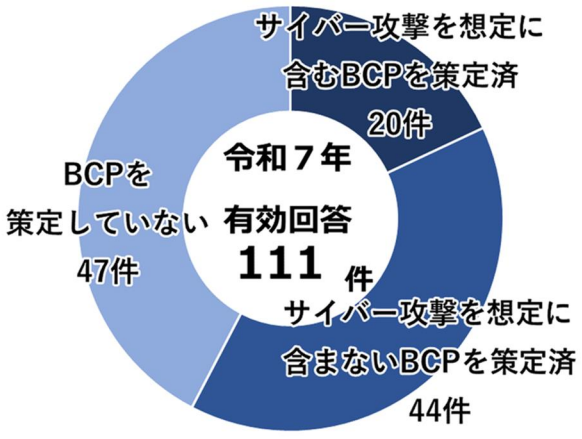
【図表 10：ランサムウェア攻撃の流れのイメージ】



３　ランサムウェア攻撃への備え

ランサムウェア攻撃は基本的に金銭目的であり、攻撃者は侵入する「隙」のある標的を探して攻撃を行う。そこで、ランサムウェア被害を防ぐためには、この「隙」を作らないよう、組織・企業のセキュリティや管理を徹底するとともに、経営者及び従業員が高いリテラシーを持つことが求められる。具体的には、基本的なセキュリティ対策の徹底を継続することが最も重要であり、例えば、ソフトウェア更新、パスワードの適切な管理、アクセス権限等の適切な設定等であり、特に、主要な侵入経路であるＶＰＮ機器等は速やかな対応が必要である。

一方、日々手口が変化、巧妙化するサイバー攻撃を完全に防ぐことは困難であることから、警察は、企業等におけるサイバー攻撃を想定した体制の構築を推進している。ランサムウェア被害により業務停止に陥る例は後を絶たないが、サイバー攻撃を想定した業務継続計画（ＢＣＰ）を策定済の組織は少ない。ランサムウェア被害にあった企業・団体にアンケート調査を行った



【図表 11：被害企業・団体等における業務継続計画（BCP）の策定状況】

結果、ＢＣＰを策定済の組織の割合は約 18%であった。ランサムウェアによるデータの暗号化は地震等の物理的災害とは被害の状況が異なり、調査・復旧作業や広報の在り方も、物理的災害時とは異なる対応が求められるため、サイバー攻撃を想定したＢＣＰを事前に準備しておく必要がある。他にも、暗号化対策となるオフラインバックアップといった情報資産の管理、侵害範囲特定に不可欠なログの取得、ランサムウェア攻撃を受けた際の対応に関する訓練、警察との連携等、サイバー攻撃のリスクを考慮した管理体制の構築が被害の抑制に有効である。令和７年６月には内閣府政府広報室と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するなど、幅広く注意喚起に取り組んでいる。

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

４　ランサムウェア被害後の対応策

もしもランサムウェア被害に遭ってしまった場合は、まず感染端末等をネットワークから隔離し、被害拡大を防ぐのが望ましい。慌てて電源をオフにすると、ログ等の侵入の痕跡が失われてしまい、その後のフォレンジック調査が困難になる可能性があるので注意が必要である。初動では被害拡大防止とログ等のデータ保全を行い、組織の対応態勢を整えた上で、調査・復旧に取り組むべきである。

また、被害が発覚した際は早期に警察や関係機関への通報をすることが求められる。ＢＣＰ等で連絡先を整理して記載しておくと、被害発生時に円滑な連携が可能になる。警察は、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ほか、関係各国と連携しながら被疑者検挙に向けた捜査を推進する。

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

５　ランサムウェア事案の検挙

警察では、サイバー特別捜査部が、我が国を含む世界各国の企業に対してランサムウェア被害を与えているグループについて、国際共同捜査を推進し、被疑者の検挙に貢献している。

【CASE：ランサムウェアグループ「LockBit」に対する国際共同捜査」】

ランサムウェア被害を与えていた攻撃グループ「LockBit」について、日本警察はEUROPOL 等と国際共同捜査を推進した。

この事案において、サイバー特別捜査隊（当時）は、暗号化されたデータを復号する独自ツールを開発するとともに、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った。同国際共同捜査によって、令和 6 年 10 月には、関係被疑者 4 名が逮捕された。（資料編 94 頁参照）

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

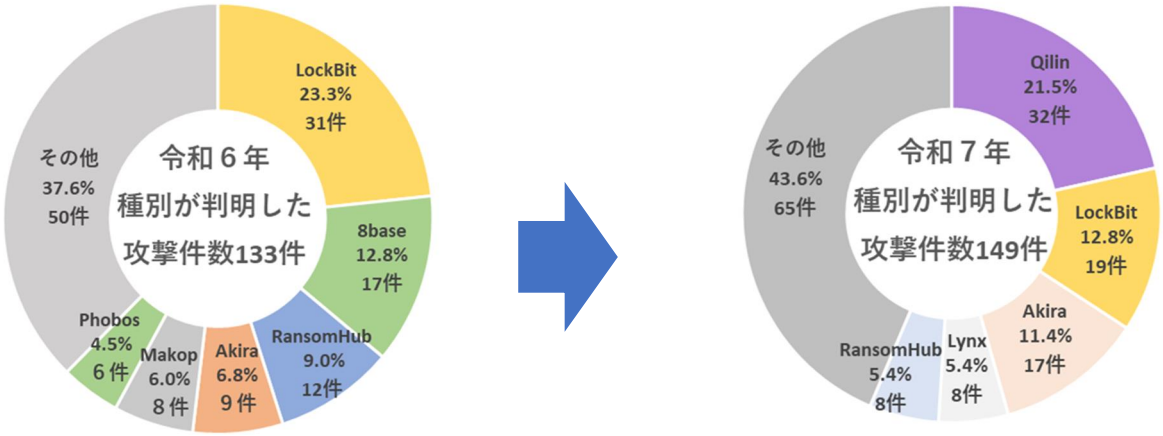
ランサムウェア被害を与えていた攻撃グループ「Phobos（フォボス）」やその関連組織「8Base（エイトベース）」について日本警察は、EUROPOL や FBI 等との国際共同捜査を推進した。

その結果、本共同捜査を通じて被疑者 5 名が逮捕されたが、そのうち 3 名はサイバー特別捜査部の捜査によって特定したほか、令和 7 年 7 月には、FBI の協力を得つつ、サイバー特別捜査部がランサムウェア 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。（資料編 96 頁参照）

このような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。

他方で、令和 7 年は、Qilin というランサムウェア種別の割合が急増するなど、新たなランサムウェアの脅威が確認されていることから、警察では、引き続き、国際共同捜査への積極的な参画等により、ランサムウェアグループの摘発を推進している。

【図表 12：ランサムウェア種別が判明した攻撃件数】



第１部　サイバー空間の脅威情勢

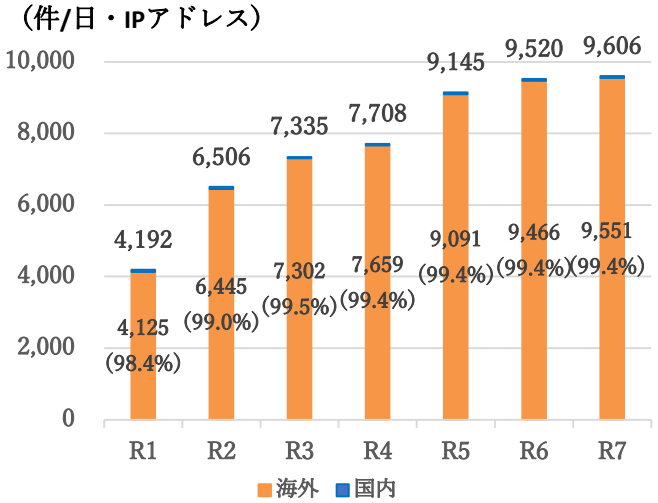
１　高度な技術を悪用したサイバー攻撃の脅威情勢

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

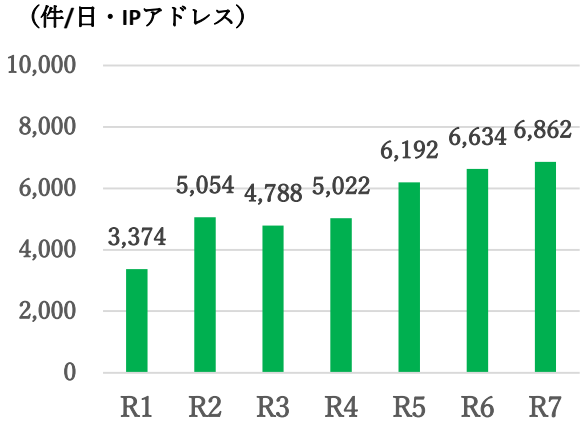
このようなサイバー攻撃の準備として、攻撃者は攻撃対象を事前に探索する場合があるところ、令和７年に警察庁が設置したセンサーにおいて検知した、ぜい弱性探索行為等の不審なアクセス件数は、１日・１IP アドレス当たり 9,605.7 件（前年比 0.9%増）と、引き続き高水準で推移しており、その大部分が海外を送信元とするアクセスで占められている（図表 13）。

また、国立研究開発法人情報通信研究機構（NICT）が運用している大規模サイバー攻撃観測網（NICTER）において観測した不審なアクセス観測件数においても、令和７年における不審なアクセス観測件数は、１日・１IP アドレス当たり 6,862.1 件（前年比 3.4%増）と、観測開始以降で最多となり、増加傾向が引き続き確認された（図表 14）。このうち、NICT が、攻撃関連のアクセスと分類したものは約 45.0%であり、令和６年の約 39.8%を上回った。また、不特定多数の機器を対象としたアクセスが、観測された全アクセス数の半数以上を占めており、個別のぜい弱性や攻撃手法といった特定の脅威に限らず、インターネット上に公開された機器やサービスが、常時第三者に探索される前提で運用されている現状を意味している。

【図表 13：警察庁が検知した不審なアクセス】



【図表 14:NICT が検知した不審なアクセス】



出典：国立研究開発法人情報通信研究機構
NICTER 観測レポート 2025 数値を引用

警察庁及びNICTが観測した不審なアクセス件数を比較すると、一定の差異が認められるものの、両者とも不審なアクセス数が増加傾向であるという同一の結果を示している。

(1) 国家の関与が疑われるサイバー攻撃

国家の関与が疑われるサイバー攻撃としては、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。例えば、令和7年（2025年）5月、米国及び西側諸国当局等は、ロシア軍参謀本部情報総局（GRU）による西側諸国の物流企業やテクノロジー企業を標的とするサイバー攻撃に関し、共同サイバーセキュリティアドバイザリーを発出した。同アドバイザリーによれば、GRUは、ウクライナや隣接するNATO諸国のIPカメラを標的とする大規模な攻撃にも関連している可能性が高いとしている。

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。例えば、令和7年（2025年）8月、警察庁及び国家サイバー統括室（NCO）は、中国を背景とするサイバー攻撃グループ「Salt Typhoon」が通信事業者に対する情報窃取を目的としたサイバー攻撃を行ったとして、米国が作成した国際アドバイザリーの共同署名に加わり、公表した。世界中のネットワークを標的としたSalt Typhoonによる活動は、中国人民解放軍（PLA）及び中国国家安全部（MSS）にサイバー関連の製品・サービスを提供している中国の複数企業と関連付けられており、Salt Typhoonによる活動を通じて取得されたデータは中国の諜報機関による活動を可能としている。

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。令和6年（2024年）3月に発表された国連安全保障理事会の報告書[9]では、北朝鮮における外貨収入の約半数がサイバー攻撃により獲得されたものであり、こうした外貨が大量破壊兵器計画に使用されているという見解等が示された。我が国においても、令和6年（2024年）5月、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が、国内の暗号資産関連事業者から約482億円相当の暗号資産を窃取した事案が発生している。

---

9 https://docs.un.org/en/S/2024/215

コラム：令和７年における国家を背景とするサイバー攻撃の傾向

令和７年において、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（APT 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。ＡＰＴ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、令和７年中には、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た。このような日本を対象としたサイバー攻撃活動は令和８年以降も継続するものと推測されている。

中国の APT 攻撃グループは、Salt Typhoon 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、令和７年においては、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。また、攻撃者の技術向上による情報窃取被害の潜在化も懸念される。

一方、北朝鮮のＡＰＴ攻撃グループは、主に政治目標の達成や TraderTraitor のように外貨獲得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、令和７年においては、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。また、暗号資産事業者の従業員に対する SNS 利用による初期侵害の手口が確認されているところ、過去に国内事業者から多額の暗号資産が窃取されていることからも、外貨獲得を目的としたサイバー攻撃は継続する可能性が高いとみられる。

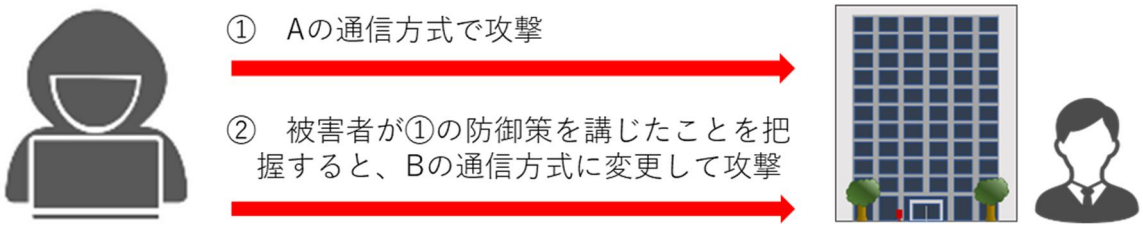
(2)　犯罪組織等によるサイバー攻撃

犯罪組織等によるサイバー攻撃としては、まずランサムウェアによる攻撃が挙げられ、ランサムウェアの情勢や対策に関しては特集Ⅱに記載しているとおりである。

次に、DDoS 攻撃（Distributed Denial of Service「分散型サービス拒否攻撃」）が挙げられる。DDoS 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６年 12 月下旬から令和７年１月上旬にかけ、交通機関や金融機関等の重要インフラ事業者等において、DDoS 攻撃によるとみられる被害が相次いで発生し、空港において手荷物の自動チェックイン機が使えない障害や、インターネットバンキングにログインしづらい状況が発生するなど、実際に国民の生活に被害がもたらされた。警察においては、当該 DDoS 攻撃について、複数の手口を確認しており、また、攻撃に対し事業者が遮断措置を講じた場合でも、状況に応じて手口を変化させ、攻撃を継続する事例を確認している。さらに、IP アドレスを指定し、ウェブコンテンツのオリジナルデータが保存されているオリジンサーバを直接標的にすることで、アクセスの分散によって負荷軽減を実現している CDN（Contents Delivery Network）を回避する攻撃が複数の事案で確認された。

【図表 15：重要インフラ事業者等に対する DDoS 攻撃の手口】

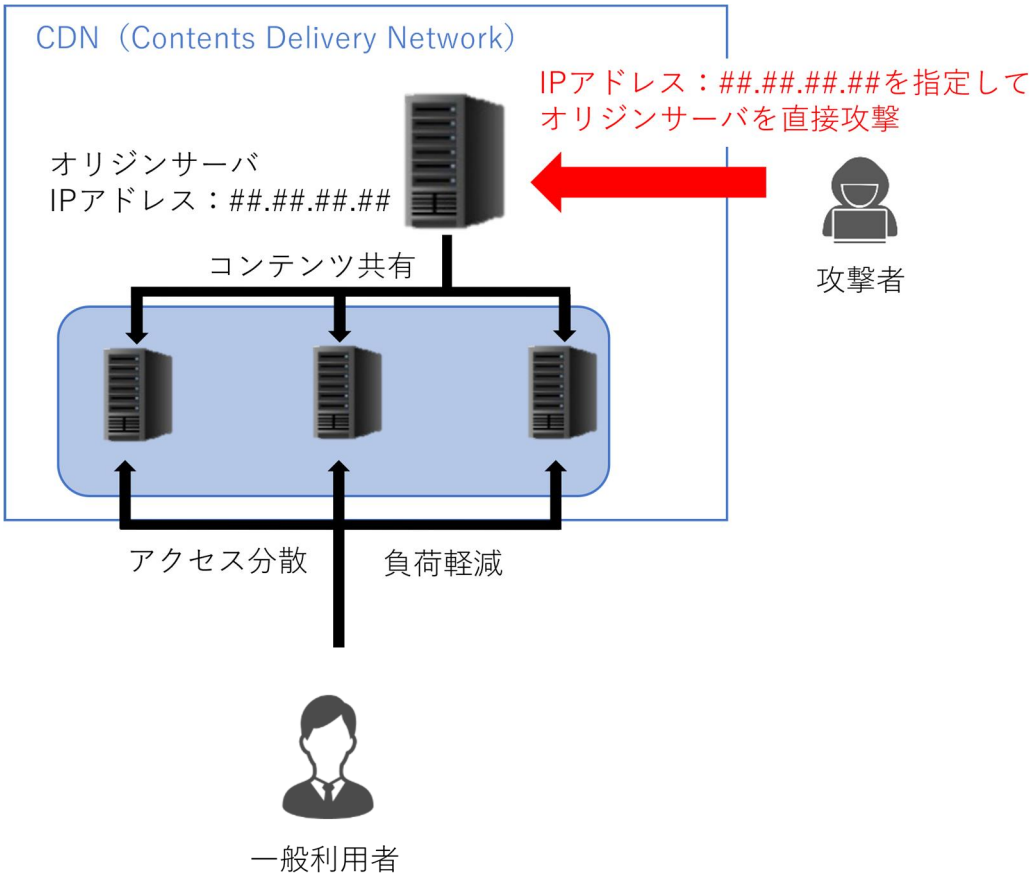


また、令和７年６月、政府機関、自治体、民間事業者等が運営する複数のウェブサイトにおいて DDoS 攻撃による被害とみられる閲覧障害が複数発生した。同じ頃、SNS 上に、ハクティビストのものと思われるアカウントから、それらの犯行をほのめかす投稿が確認された。

DDoS 攻撃による被害を抑えるための対策として、オリジンサーバに対する CDN を経由しないアクセスの遮断、組織外にオリジンサーバの IP アドレスが露見しないような DNS 設定の見直し、海外に割り当てられた IP アドレスから

の通信の遮断、アクセスを監視し攻撃を検知・遮断する機能を持つような対策装置やサービスの導入、サーバ装置、端末、通信回線装置及び通信回線の冗長化等が求められる。

【図表 16：DDoS 攻撃におけるオリジンサーバへの攻撃のイメージ】

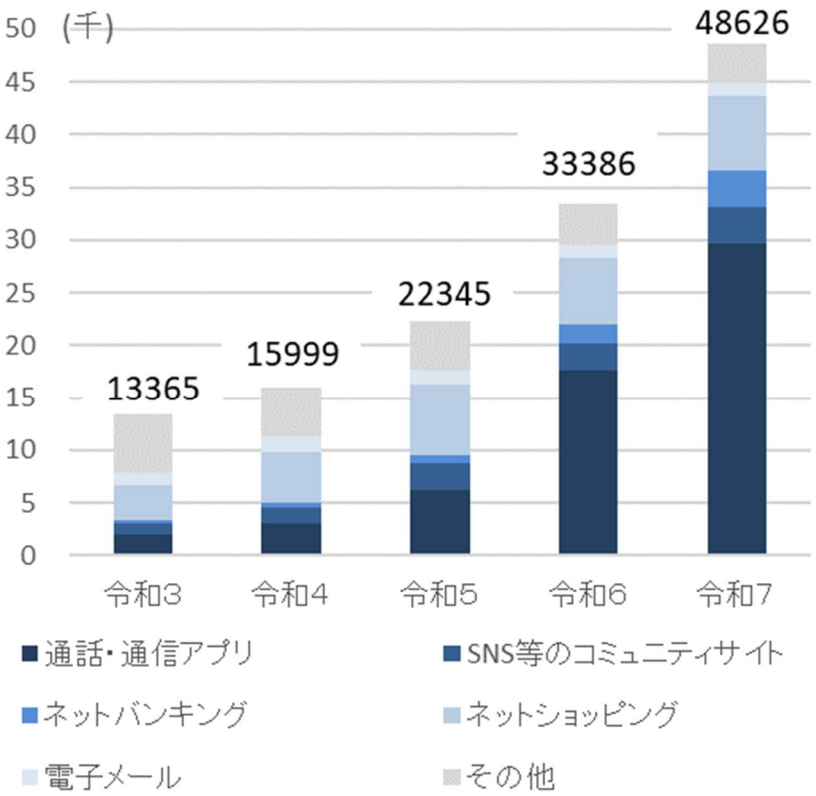


２　インターネット空間を悪用した犯罪に係る脅威情勢

情報通信技術の著しい発展や、日常生活や経済活動へのサイバー空間の浸透は社会に様々な便益をもたらす反面、サイバー空間を舞台とした犯罪をはじめ、新たな治安課題を生み、また深刻化させており、このような情勢は、令和７年中のサイバー関係の警察に対する相談数が約 18 万 5,000 件に達するなどしていることからも見てとれる。

また、インターネットを利用した詐欺事案の発生が右肩上がりで増加しており、令和７年においては、通話・通信アプリを使用した詐欺が約６割を占める。

【図表 17：インターネットを利用した詐欺の認知件数と内訳】



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

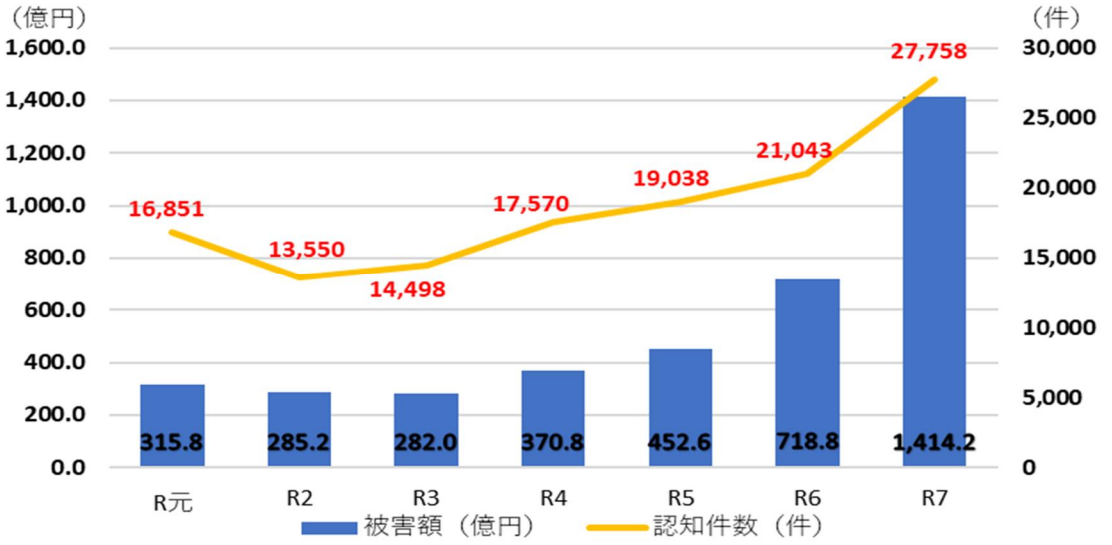
(1) SNS・メッセージングアプリ等を悪用する犯罪

多くの国民が利用する SNS は、犯罪インフラとして悪用されている実態がみられる。例えば、各種犯罪により得た収益を吸い上げる中核部分が匿名化され、SNS を通じるなどしてメンバー同士が緩やかに結び付くなどの特徴を有する「匿名・流動型犯罪グループ」が、SNS で仕事の内容を明らかにせず、「高額」「即日即金」「ホワイト案件」等、「楽で、簡単、高収入」を強調する表現を用いるなどして、犯罪実行者を募集し、特殊詐欺等を敢行している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

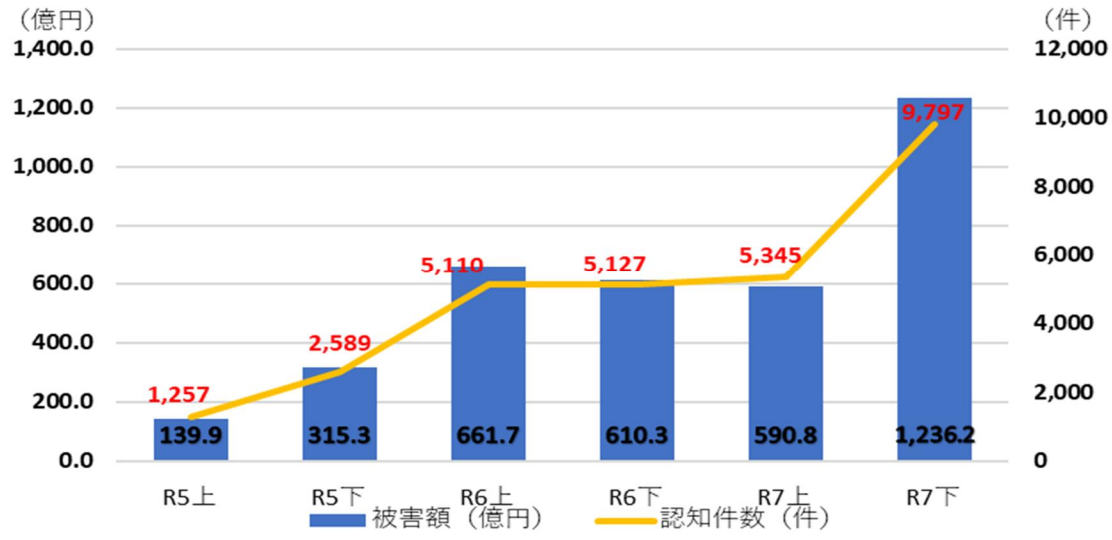
高くメッセージが自動的に消去される仕組みを備えた通信手段が悪用されている実態がみられる。このほか、匿名・流動型犯罪グループの関与が認められるものとして、SNS を通じて対面することなく、やり取りを重ねるなどして関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭をだまし取る又は恋愛感情や親近感を抱かせて金銭をだまし取る SNS 型投資・ロマンス詐欺があり、まさに SNS が犯罪インフラとして悪用されている。

令和 7 年の特殊詐欺の被害額は約 1,414 億 2,000 万円（前年同期比 96.7%増と、過去最悪となった令和 6 年の被害額を上回り、SNS 型投資・ロマンス詐欺の被害額についても約 1,827 億円（前年同期比 43.6%増）と昨年を上回った。

【図表 18：特殊詐欺の認知件数・被害額】



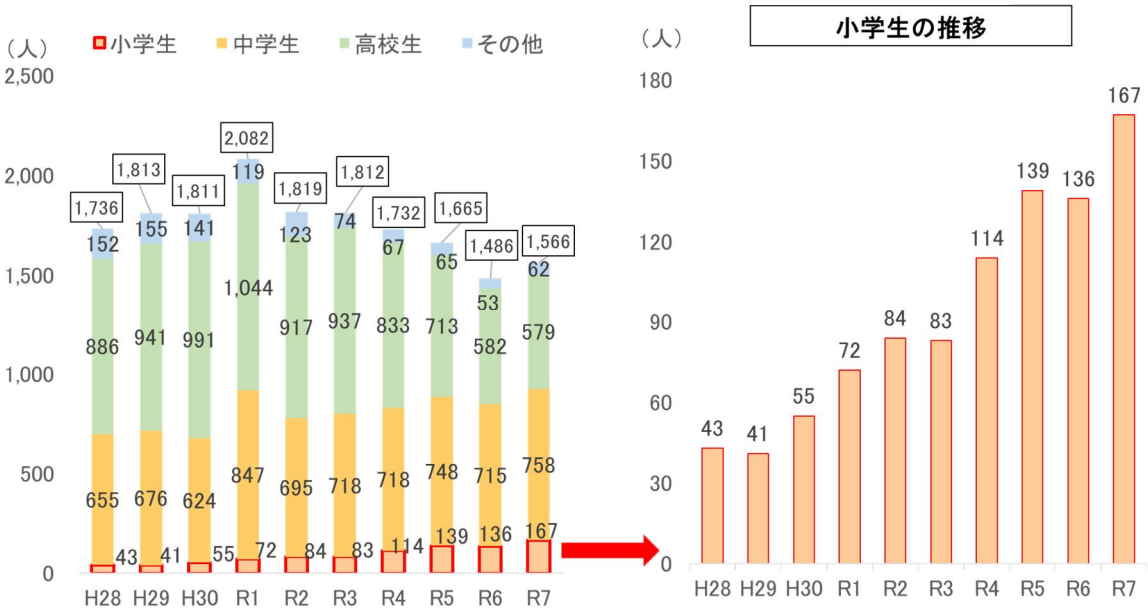
【図表 19：SNS 型投資・ロマンス詐欺の認知件数・被害額】



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

また、近年は、SNS 上での特定の個人に対する誹謗中傷も社会問題化しているほか、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「場」となっている状況もうかがえる。実際、SNS に起因して性犯罪等の被害に遭った児童の数は、依然として高い水準で推移している。特に、小学生の被害児童数が近年増加傾向にあり、被害児童の低年齢化の傾向が見られる。

【図表 20：SNS に起因する事犯の学職別被害児童数の推移】



※ SNSとは、本統計では、通信ゲームを含み、届出のある出会い系サイトを除いたもの。
※ SNSに起因する事犯とは、SNSを通じて面識のない被疑者と被害児童が知り合い、交際や知人関係等に発展する前に被害にあった事犯
※ 対象犯罪は、児童福祉法違反、児童買春・児童ポルノ禁止法違反、青少年保護育成条例違反、重要犯罪等（殺人、強盗、放火、不同意性交等、略取誘拐、人身売買、不同意わいせつ、逮捕監禁）、面会要求等及び性的姿態撮影等処罰法第2条から第6条に規定する罪（面会要求等及び性的姿態撮影等処罰法違反は令和5年から追加）

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

さらに、オンラインゲームに関連する事案も発生しており、例えば、オンラインゲーム内のアイテム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。

一般財団法人日本サイバー犯罪対策センター（JC3）（56 頁参照）では、警察やサイバー防犯ボランティアの協力の下、オンラインゲームの利用におけるトラブル実態把握のためのアンケート調査を行い、令和 7 年 12 月に JC 3 のホー

ムページ上で公開している。

アンケート結果からは、オンラインゲームに関するトラブルに巻き込まれたことがあると回答した人の大半はゲーム内チャットなどのコミュニケーションにまつわるトラブルであったが、その内、3割程度がアカウント乗っ取りやDDoS攻撃、リアルマネートレードのトラブルに巻き込まれていることが確認され、トラブルの内容としては、チャット機能等の交流機能を通じて暴言を吐かれる等の被害に遭うケースが多く見られる一方で、フィッシングやアカウント乗っ取り等の被害に遭うケースも複数発生していることが確認できた。

また、トラブルに遭った際の対応を分析したところ、アンケート規模の問題により確度は低いが、相談・連絡等の手段を取った場合には、何もアクションを取らなかった場合に対して有意にトラブルが解決しやすいことが見て取れた。

(2) メール・SMSを悪用する犯罪

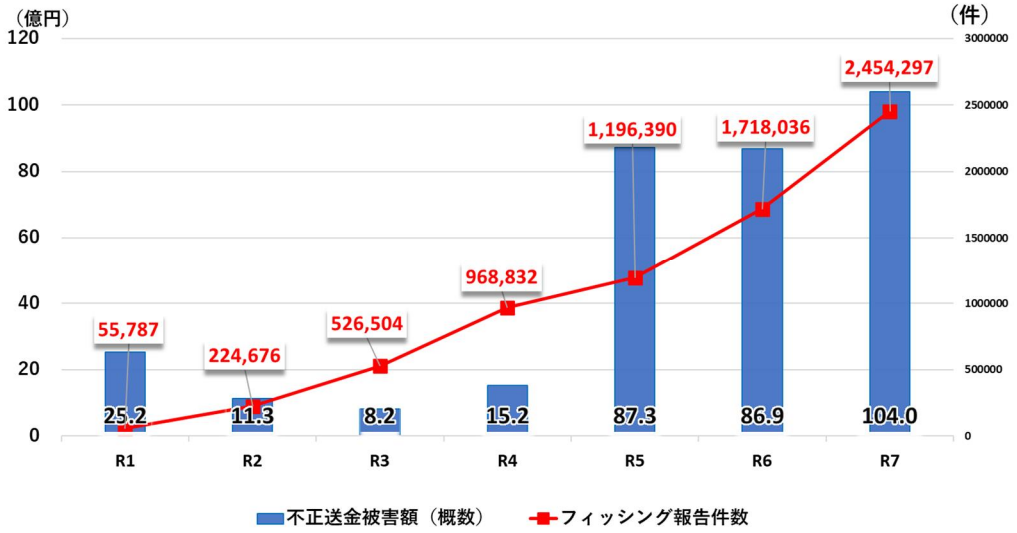
メールやSMSは、フィッシングに悪用される実態がみられる。フィッシングとは、実在する組織を装ってメールやSMSのリンクから偽のウェブサイト（フィッシングサイト）へ誘導し、同サイトでアカウント情報やクレジットカード番号等を不正に入手する手口であり、これによって得られた情報はインターネットバンキングに係る不正送金やクレジットカードの不正利用に使われている（統計編143頁参照）。

令和7年におけるフィッシング報告件数は、フィッシング対策協議会によれば、245万4,297件であり、右肩上がりの増加が続いている。

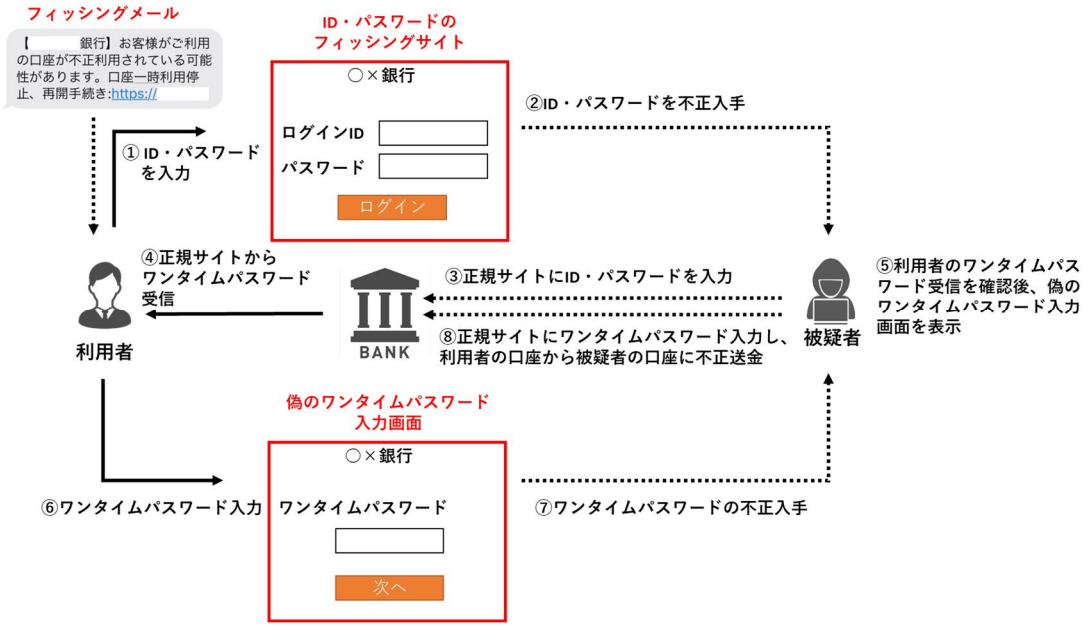
また、令和7年におけるインターネットバンキングに係る不正送金事犯の発生件数は4,747件、被害総額は約103億9,700万円となっており、フィッシングがその手口の約9割を占める。

フィッシングにおいては、令和元年頃からリアルタイム型フィッシングにより二段階認証を突破する手口が横行するなど、手口の巧妙化が見られる。

【図表 21：インターネットバンキングに係る不正送金被害額及びフィッシング報告件数】



【図表 22：リアルタイム型フィッシングの手口】



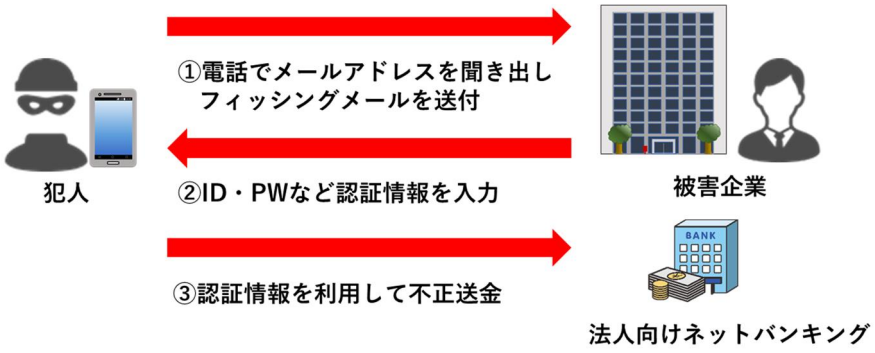
コラム：ボイスフィッシングによる不正送金被害

令和６年秋から令和７年４月にかけて、犯罪グループが企業に架電し、ネットバンキングの更新手続等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシング（ビッシング）という手口による法人口座の不正送金被害が急増した。同年５月から 10 月にかけては被害の発生がみられなかったものの、11 月には不正送金被害が再び急増し、地方を拠点とした中小規模の金融機関でも多くの被害が出た。

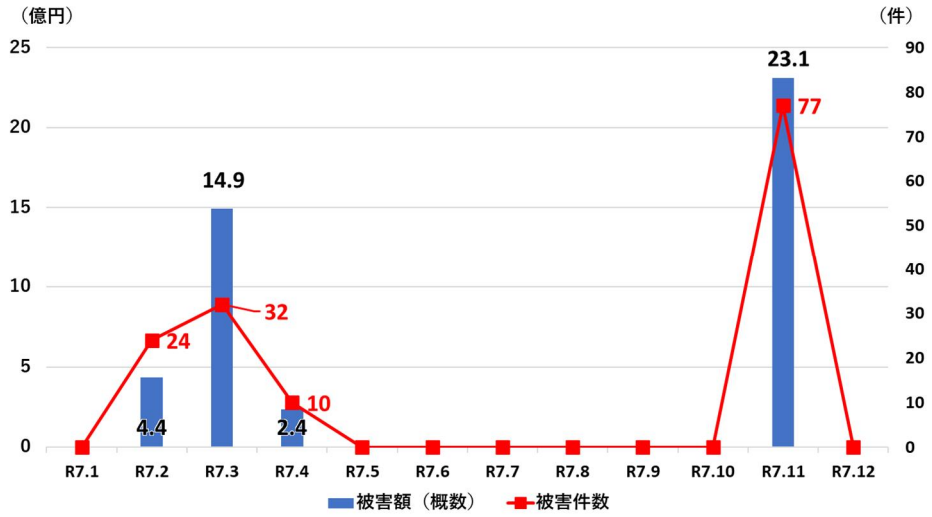
こうしたボイスフィッシングには、発信元番号が国際番号である、自動音声ガイダンスが流れた後に人間の声に切り替わる、通話中にメールアドレスを聴取されリンク付きメールが送られる、といった特徴が見られる。

そこで、ボイスフィッシングの被害を防ぐためには、銀行から電話があった場合に、営業店・代表電話に折り返して本物かどうか確認するといった対応や、インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスするといった対応を社内で徹底する必要がある。

【ボイスフィッシングの流れ】



【図表 23：ボイスフィッシングによる法人口座の不正送金被害件数・被害額】



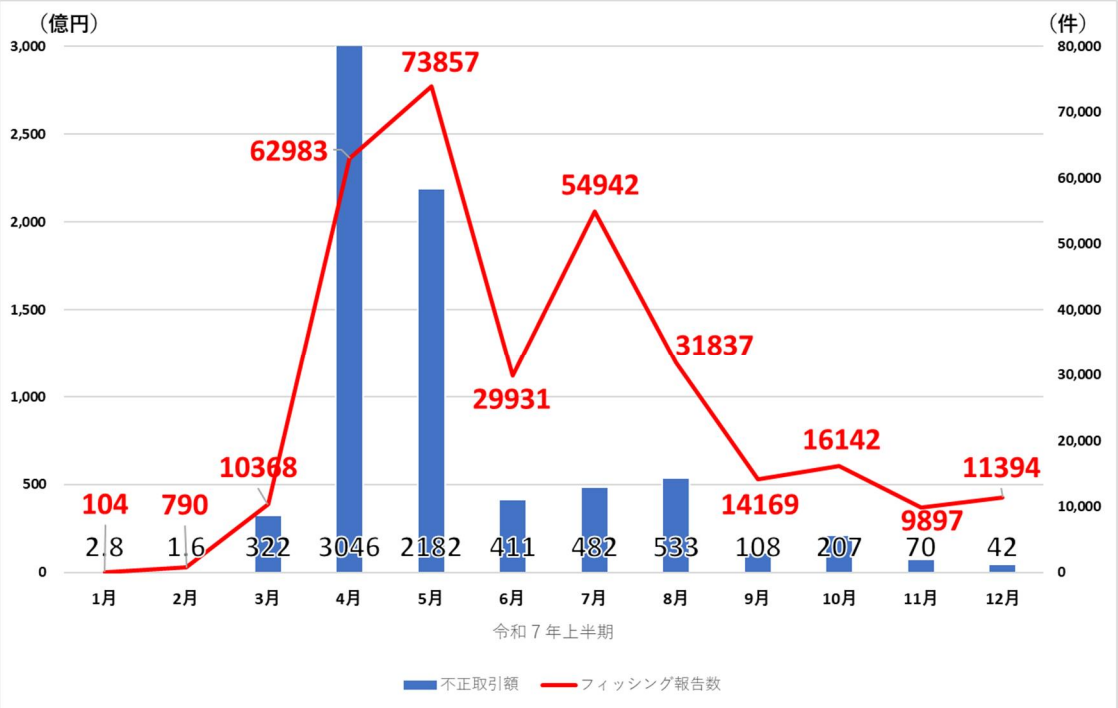
コラム：証券口座への不正アクセス等の急増及び検挙

令和７年３月から５月にかけて、証券会社をかたるフィッシングメールの送信や証券口座への不正アクセス及び不正取引が急増し、金融庁及びフィッシング対策協議会によれば、令和７年における証券口座への不正アクセス件数は１万 7,668 件、不正取引件数は 9,824 件、不正売買金額は約 7,408 億円、証券会社をかたるフィッシングメール報告件数は 31 万 6,414 件となるなど、深刻な被害が生じた。

令和７年 11 月、サイバー特別捜査部及び警視庁等の都道府県警察は、関係機関の協力を得て、捜査を推進した結果、中国籍の男(38)らを金融商品取引法違反（相場操縦行為等の禁止）及び不正アクセス禁止法違反（不正アクセス行為の禁止）で逮捕した。同男らは、自身が管理する証券口座を用いて相場操縦の対象となる株（以下「対象株」という。）を事前に大量に買い付けた上で、氏名不詳者と共謀の上、他人の証券口座に不正アクセスし、被害口座において保有していた株を売却するなどして資金を確保し、対象株を大量に買い付けることで株価を上昇させた。その後、同男が保有していた対象株を高値で売却の発注をするとともに、被害口座において対象株を買い付けることで取引を成立させ、購入額と売却額の差額を利益として得ていた。

本件を含め、多発した証券口座への不正アクセスや不正取引に対し、サイバー特別捜査部は、証券会社をかたるフィッシングメールやフィッシングサイトに関するデータの解析、暗号資産の送信先アドレスの分析、全国で発生した同事案の情報集約等により、関係都道府県警察による捜査に貢献している。

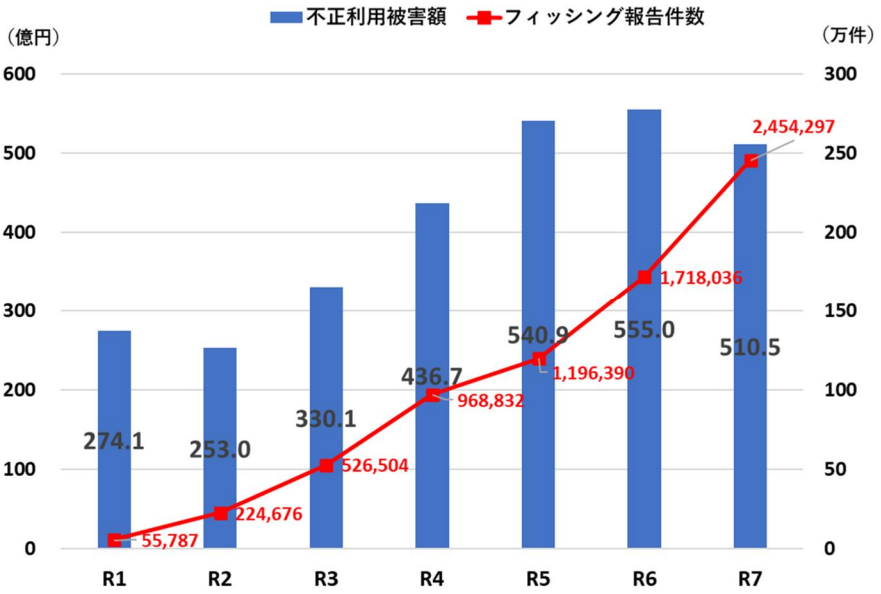
【図表 24：証券口座不正取引額と証券口座に関するフィッシング報告件数】



また、不正送金に関するフィッシング以外の手口については、マルウェア感染を契機とした事例や SIM スワップ[10]によって本人確認を突破する手口も引き続きみられた。

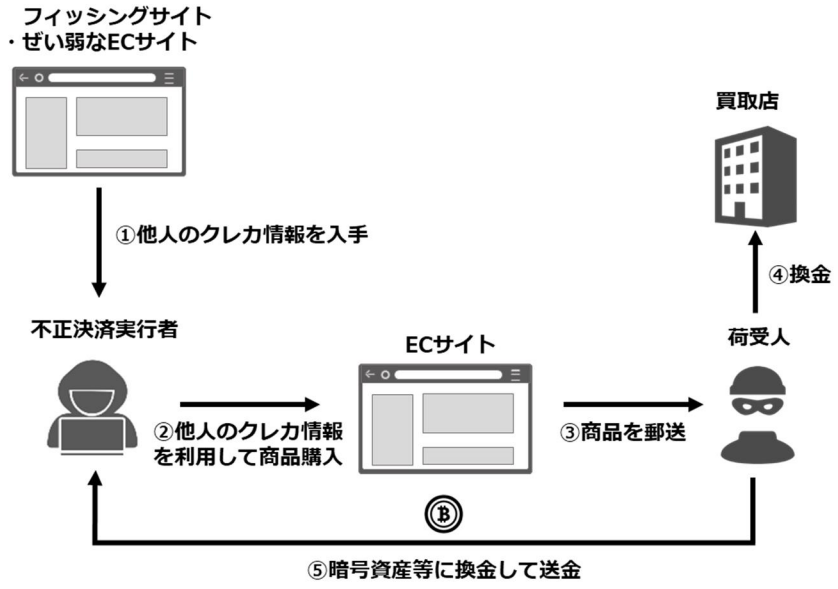
さらに、一般社団法人日本クレジット協会によれば、令和７年中のクレジットカードの不正利用被害額は約 510 億円（前年比約９％減）と、依然として厳しい情勢にある。

【図表 25：クレジットカード不正利用被害額及びフィッシング報告件数】



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

【図表 26：クレジットカード不正利用の流れ】

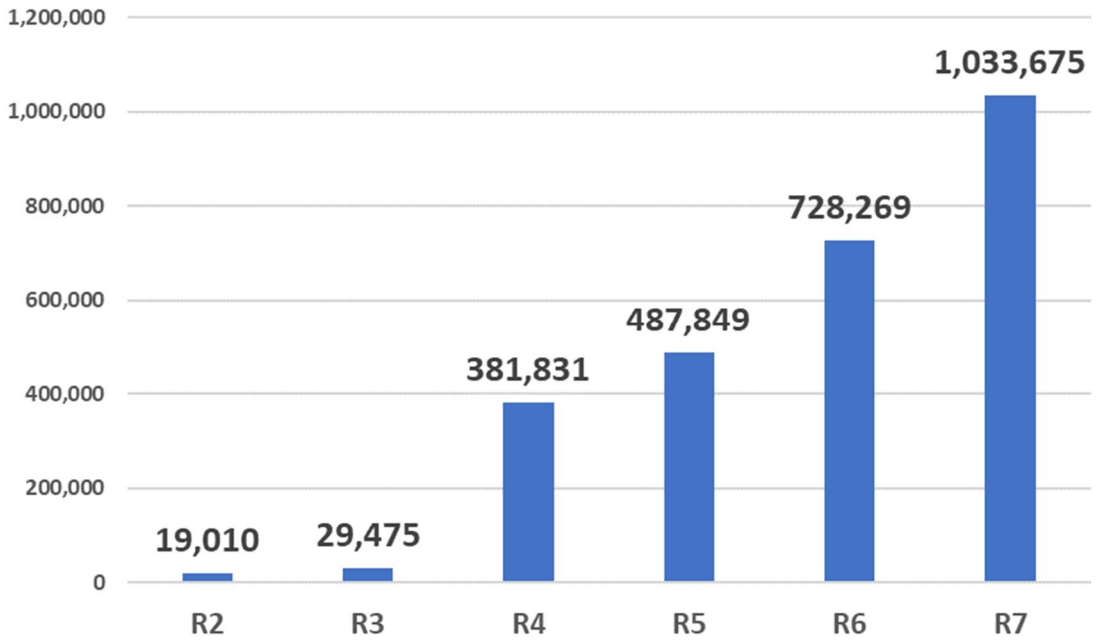


[10] 携帯電話機販売店において、偽造した本人確認書類を使い、他人に成りすまして MNP（携帯電話番号ポータビリティ）や SIM カードの再発行手続きを行い、携帯電話番号を乗っ取る手口をいう

(3) ウェブサイトを悪用する犯罪

SNS や SMS の利用なく、ウェブサイトそのものが悪用されて犯罪が敢行される実態もみられる。例えば、海外のサーバを通じてインターネット上に掲載された、実在する企業のサイトを模したフィッシングサイトのほか、インターネットショッピングに係る詐欺や偽ブランド品販売を目的とするサイト等（以下単に「偽サイト等」という。）に係る被害が多発しているところ、警察庁においては、都道府県警察等が相談等を通じて把握した偽サイト等に係る URL 情報を集約しており、その件数は右肩上がりに増加している。

【図表 27：警察庁に対する偽サイト等の情報報告件数】



また、パソコンでインターネットを閲覧中に、突然ウイルスに感染したかのような嘘の画面を表示させたり、警告音を発生させるなどして、ユーザーの不安を煽り、画面に記載されたサポート窓口に電話をかけさせ、サポート名目で金銭をだまし取ったり、遠隔操作ソフトをインストールさせたりするサポート詐欺の被害も引き続き発生している。令和 7 年における架空料金請求詐欺のうち、パソコンのウイルス除去をサポートするなどの名目で電子マネー等をだまし取る「サポート名目」の認知件数は 1,066 件（前年同期比 30.1%減）、被害額は約 14 億円（前年同期比 39.6%増）となっている。

(4)　インターネット空間の資金移動を悪用する犯罪

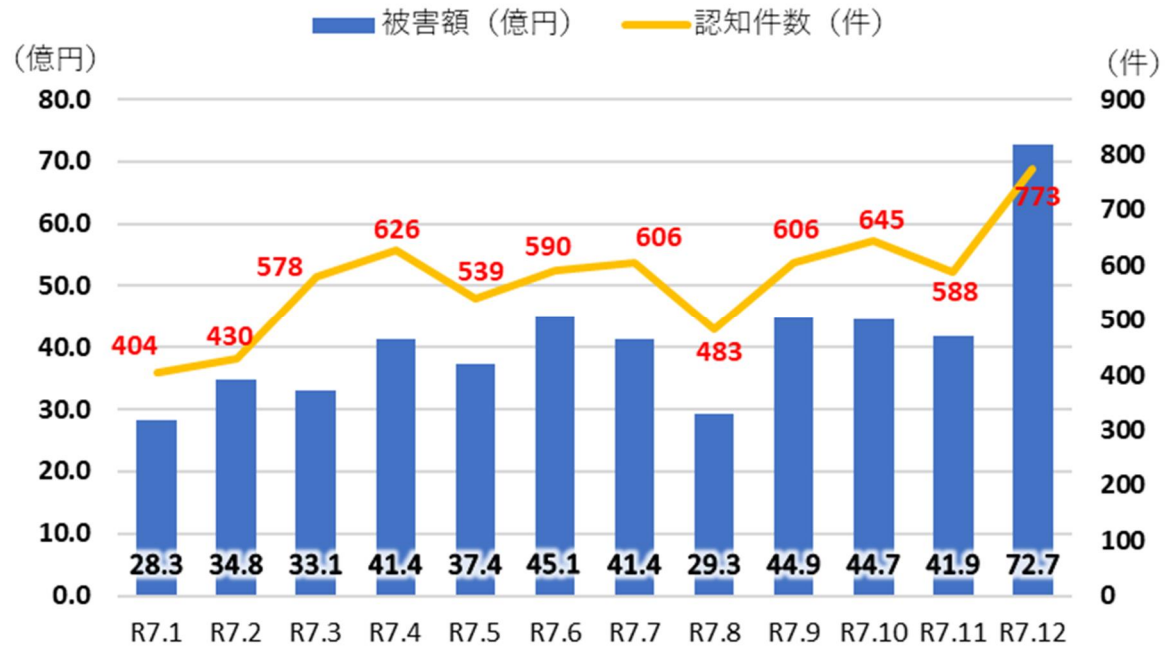
インターネット空間における資金移動は利便性が高い一方、インターネットバンキングでは、振込の１日の上限額を容易に引き上げられる、送金時に第三者の目が届きにくいといった特徴から、犯罪に悪用される実態があり、また、暗号資産についても、匿名性の高さなどから、マネー・ローンダリングに利用される実態が見られる。

①　インターネットバンキング

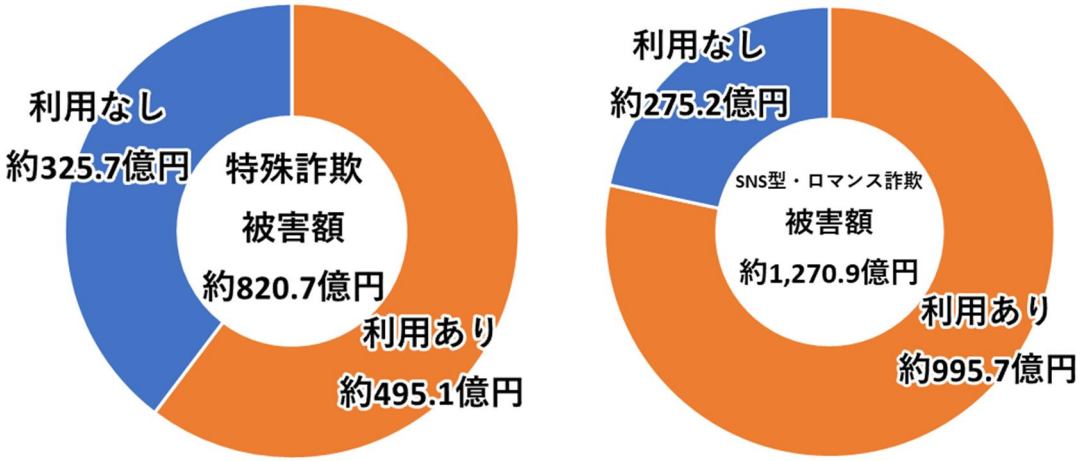
特殊詐欺の被害のうち、振込型による被害（認知件数１万 6,862 件、被害額約 820 億 7,000 万円）を分析すると、インターネットバンキングを利用したものの認知件数・被害額は増加傾向にあり、認知件数は振込型全体の約４割、被害額は振込型全体の約６割を占めている。

さらに、SNS 型投資・ロマンス詐欺の被害のうち、振込型による被害（認知件数１万 168 件、被害額約 1,270 億 9,000 万円）を分析すると、インターネットバンキングを利用したものの認知件数は振込型全体の約７割、被害額は振込型全体の約８割を占めている。

【図表 28：特殊詐欺におけるインターネットバンキングを利用した振込被害】



【図表 29：特殊詐欺及び SNS 型投資・ロマンス詐欺におけるインターネットバンキングの利用の有無】



② 暗号資産

暗号資産については、利用者の匿名性が高く、その移転がサイバー空間において瞬時に行われるという性質から、犯罪に悪用されたり、犯罪収益等が暗号資産の形で隠匿されたりするなどの実態がみられる。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づ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「相対屋（あいたいや）」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。

(5) ＩｏＴ機器を踏み台として悪用する犯罪

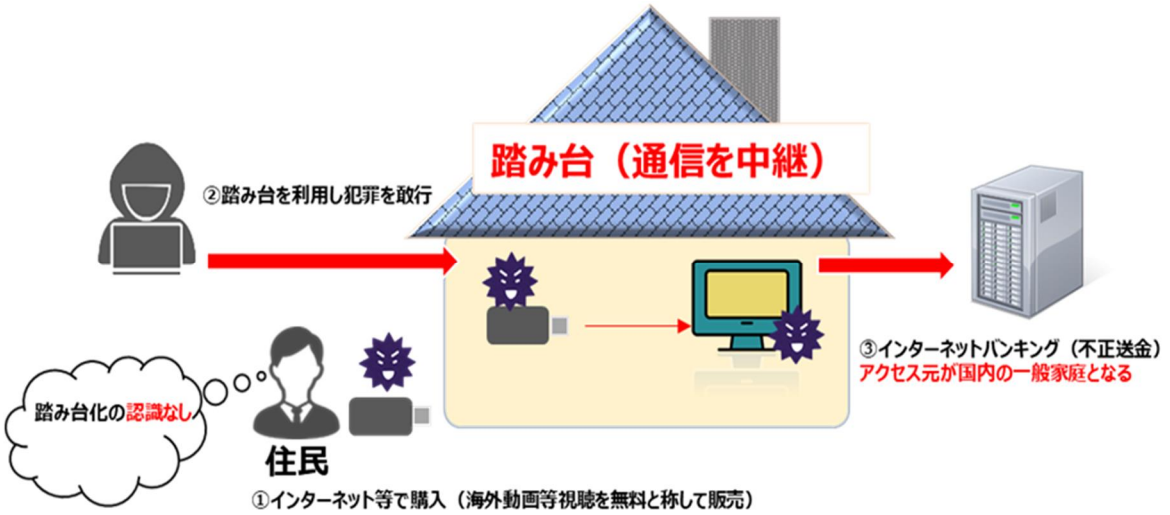
一般家庭で使用されるネットワーク接続機能を有する機器（ＩｏＴ機器）について、機器の所有者の認識しないところでいわゆる「レジデンシャルプロキシ」（一般家庭の回線を利用するプロキシ）として動作し、踏み台として悪用される事案が多発している実態が明らかとなっている。

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ストリーミング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。

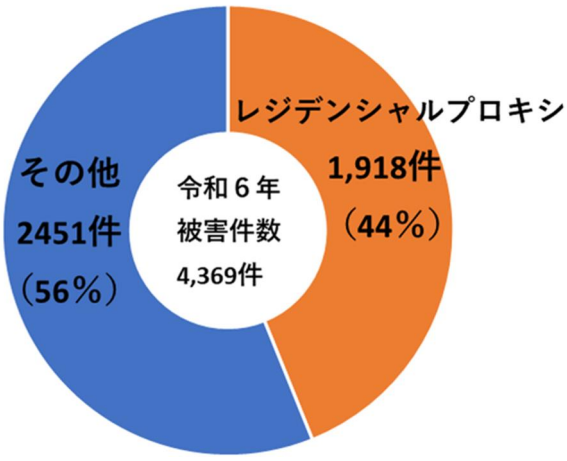
これらの機器の中には、機器の購入前の段階において、ダウンローダー等の

不正なソフトウェアが仕込まれた機器が流通しているものもあり、当該機器をインターネットに接続することにより、使用者の気付かないうちにマルウェアをインストールしてプロキシとして動作するものがある。これらの機器が踏み台となり、攻撃者の通信を中継した場合、通信先のサーバのログには、攻撃者の IP アドレスではなく、踏み台となった機器のＩＰアドレスが記録される。海外の攻撃者であっても、国内の機器を踏み台とすることにより、海外からのアクセスを制限したサーバにアクセスすることも可能となるなど、セキュリティ対策上の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 30：IoT 機器が踏み台となる攻撃のイメージ】



例えば、令和６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 4,369 件、被害額約 86.9 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のは少なくとも 1,918 件、被害額は約 28.9 億円に及び、被害件数全体の約 44%、被害額では約 33%を占める。また、令和７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 31：インターネットバンキング不正送金被害件数の内訳】

３　違法・有害情報に係る情勢

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。

(1)　主な違法・有害情報の類型

違法情報の主な類型としては、「児童ポルノ公然陳列」や「売春目的等の誘引」等のわいせつ関連情報、「規制薬物の広告」や「危険ドラッグに係る未承認医薬品の広告」等の薬物関連情報のほか、銃砲等所持関連情報や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といった類型が挙げられる。

また、有害情報としては、「爆発物の製造」、「殺人の請負」、「人身売買」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。

(2)　犯罪実行者募集情報

【図表 32：犯罪実行者募集のイメージ】

近年インターネット上には、匿名・流動型犯罪グループ等による犯罪の実行者を募集する犯罪実行者募集情報が氾濫しており、令和７年中のインターネット・ホットラインセンター（IHC）の受理件数のうち、１万 4,241 件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がより深刻な治安上の脅威になっている。

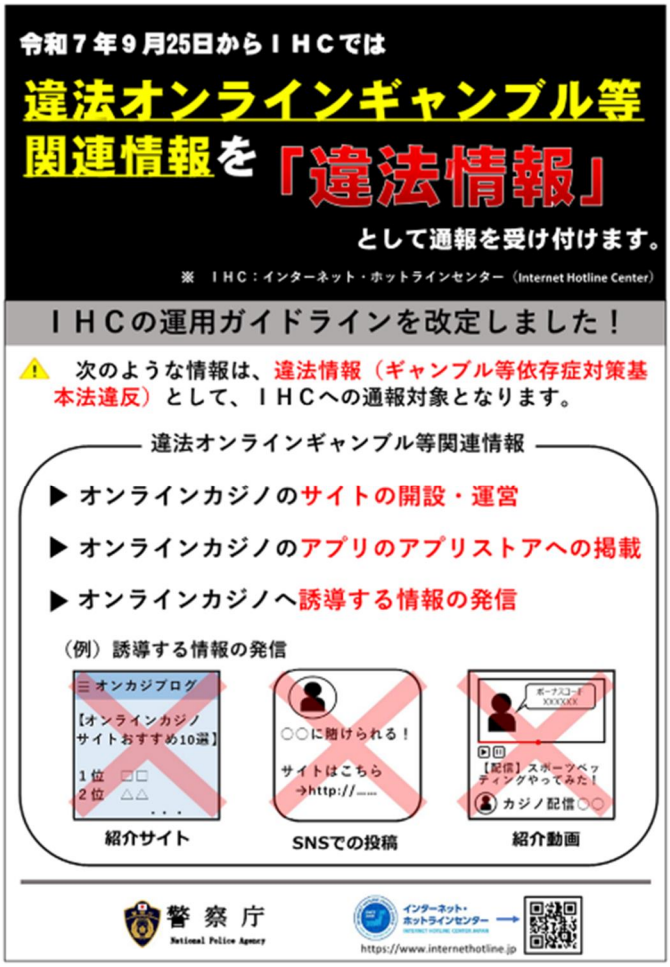
強盗・窃盗等についても、SNS や求人サイト等で「高額」、「即日即金」、「ホワイト案件」等の文言を用いて犯罪実行者が募集された上で実行される実態がうかがわれる。このような匿名・流動型犯罪グループによるものとみられる手口により実行された強盗事件等の中には、被害者を拘束した上で暴行を加えるなど、その犯行態様が凶悪なものもみられる。

コラム：違法オンラインギャンブル等関連情報に対する取組

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

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

令和７年６月 18 日、ギャンブル等依存症対策基本法の一部を改正する法律が成立し、インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為等が禁止されたことから、同年９月 25 日の施行に合わせて、総務省により「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第 26 条に関するガイドライン」が改定されるとともに、業界４団体で構成される違法情報等対応連絡会が作成する「インターネット上の違法な情報への対応に関するガイドライン」が改定された。



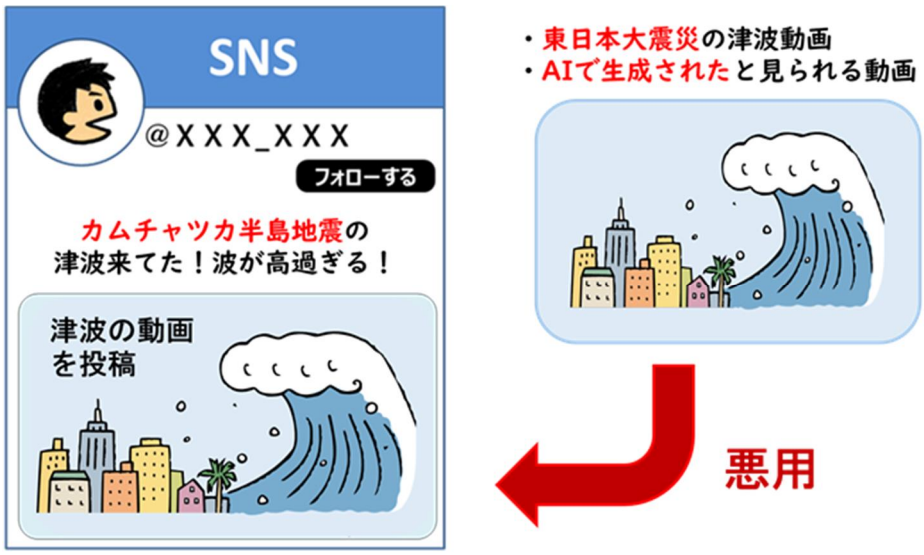
インターネット・ホットラインセンター（IHC）においても、同日、運用ガイドラインを改定し、違法オンラインギャンブル等関連情報を新たに違法情報と位置付け、インターネット利用者からの通報を受け付けるとともに、警察への通報やサイト管理者等への削除依頼を行うなど、社会問題となっているこれら情報の流通防止に向けた取組を強化している。

(3)　災害発生時における偽情報

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

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

【図表 33：SNS 上における偽情報投稿のイメージ】



(4)　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。

第２部　警察の取組

トピックスⅠ　国家安全保障におけるサイバー警察の果たす役割

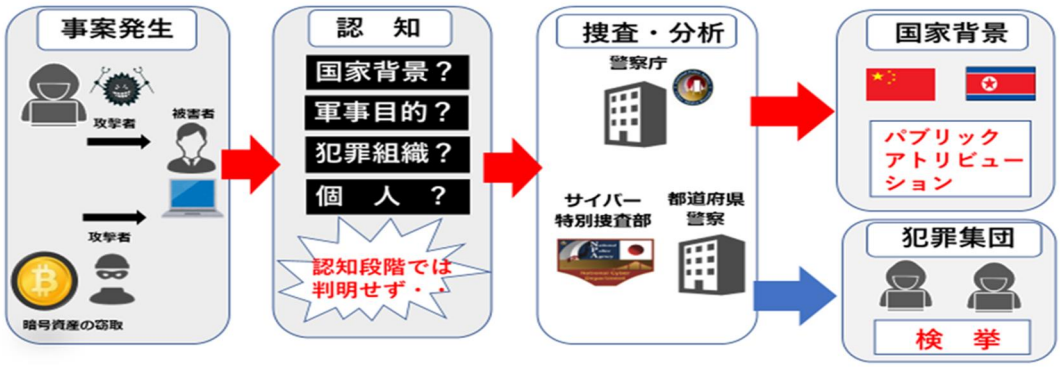
１　国家安全保障上の脅威である可能性を念頭に置いた警察の捜査及び実態解明

政府機関や重要インフラ事業者等をターゲットとするサイバー攻撃は、我が国にとっても現に直面する安全保障上の脅威となっている。しかしながら、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い。したがって、国家を背景とするものや、軍事目的遂行のためのものなど、国家安全保障に関わる事案が含まれているおそれがあることを念頭に、全てのサイバー事案について警察が対応する必要がある。

具体的には、まずは、地域に密着する警察が、110 番通報や警察相談、外国治安機関等からの情報提供等、様々な警察活動を通じてサイバー事案による被害やその疑いを把握することになる。その上で、これらサイバー事案が安全保障に直結する事案である可能性も見据えながら、捜査権を有する警察が事案の捜査を行うとともに、サイバー攻撃に係る脅威情報の収集・把握や総合的な分析等を行うなどの実態解明を進めることとなる。警察による捜査等の結果、攻撃手口や攻撃の背景に国家が関与している可能性が判明した場合には、判明した攻撃手口や攻撃インフラ等に関する注意喚起を行うことで、更なる被害の未然防止につなげており、より詳細に国家の関与を特定できた場合には、関係機関等とも連携しつつ、その旨を公表し、非難することでサイバー攻撃を抑止する、いわゆるパブリック・アトリビューションを行っている。仮に、捜査等の結果、そのサイバー事案が一般人や犯罪組織による金融犯罪等であることが判明した場合には、被疑者の逮捕・検挙はもとより、国際共同捜査等による事案の解決を進めることとなる。

このように、国家を背景としたサイバー攻撃への対応等、サイバー空間をめぐる国家安全保障の文脈においても、サイバー警察は重要な役割を果たしている。

【図表 34：サイバー攻撃に対する警察の対処の流れのイメージ】



コラム：ウクライナへの大規模な DoS 攻撃の観測

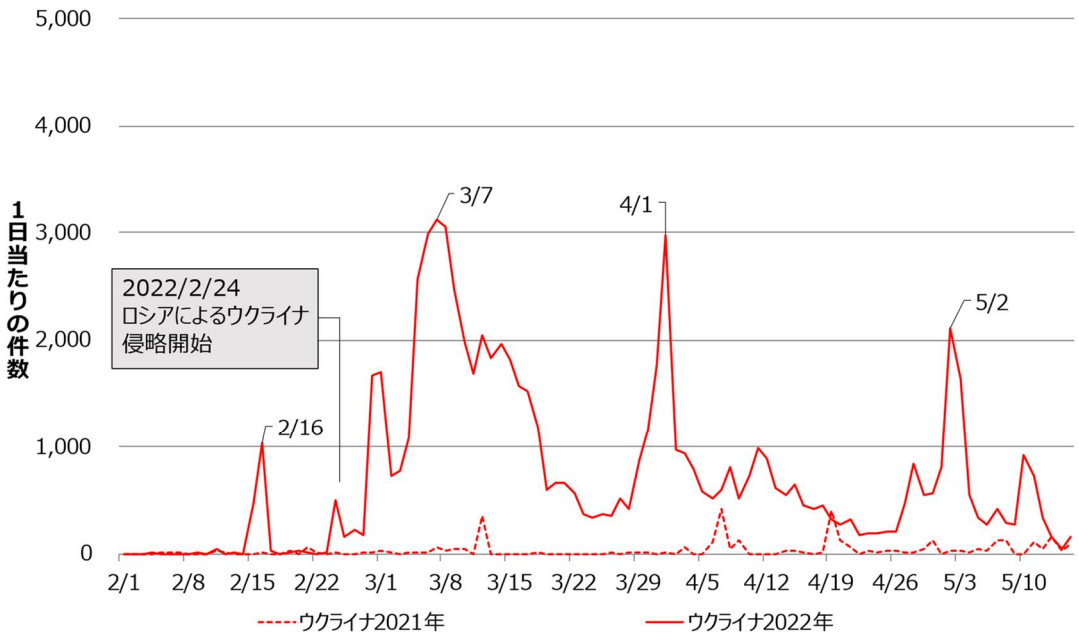
以下のグラフは、令和３年（2021年）及び令和４年（2022年）のそれぞれ２月から５月の間において警察庁の設置したセンサーが観測したウクライナに対するDoS攻撃の状況である。

令和３年（2021年）は非常に少ない一方、令和４年（2022年）にあっては、ロシア軍によるウクライナへの侵略が開始される直前の２月16日や侵略を開始した２月24日以降、ウクライナへの大規模なDoS攻撃が観測されるなど、ウクライナ侵略とサイバー攻撃の発生に時間的・地理的な相関が見られる。

実際に、令和４年（2022年）５月、EUやウクライナ等は、ウクライナ侵略の際の約１時間前に、ロシア政府が国際衛星通信へのサイバー攻撃を行い、欧州全域に影響を及ぼした事案が発生したとして、非難声明を発表している。

我が国に対する武力攻撃の前段階において政府機関や重要インフラ事業者等に対するサイバー攻撃が行われ、武力攻撃が生起した後も軍事的・物理的な手段と組み合わせたハイブリッド戦としてサイバー攻撃が継続されることも想定されるところ、警察におけるこのようなサイバー攻撃情勢の把握は国家安全保障上も非常に重要である。

【図表 35：ウクライナに対する DoS 攻撃の観測】



２　能動的サイバー防御（ＡＣＤ）

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。

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

令和７年５月、第 217 回国会において、同提言の内容を踏まえたサイバー対処能力強化法[11]（以下「強化法」という。）及び同整備法[12]（以下「整備法」という。）が成立した。強化法及び整備法は、「官民連携の強化」、「通信情報の利用」及び「攻撃者のサーバ等へのアクセス・無害化措置」の３つを取組の柱としている。

令和７年 12 月、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。

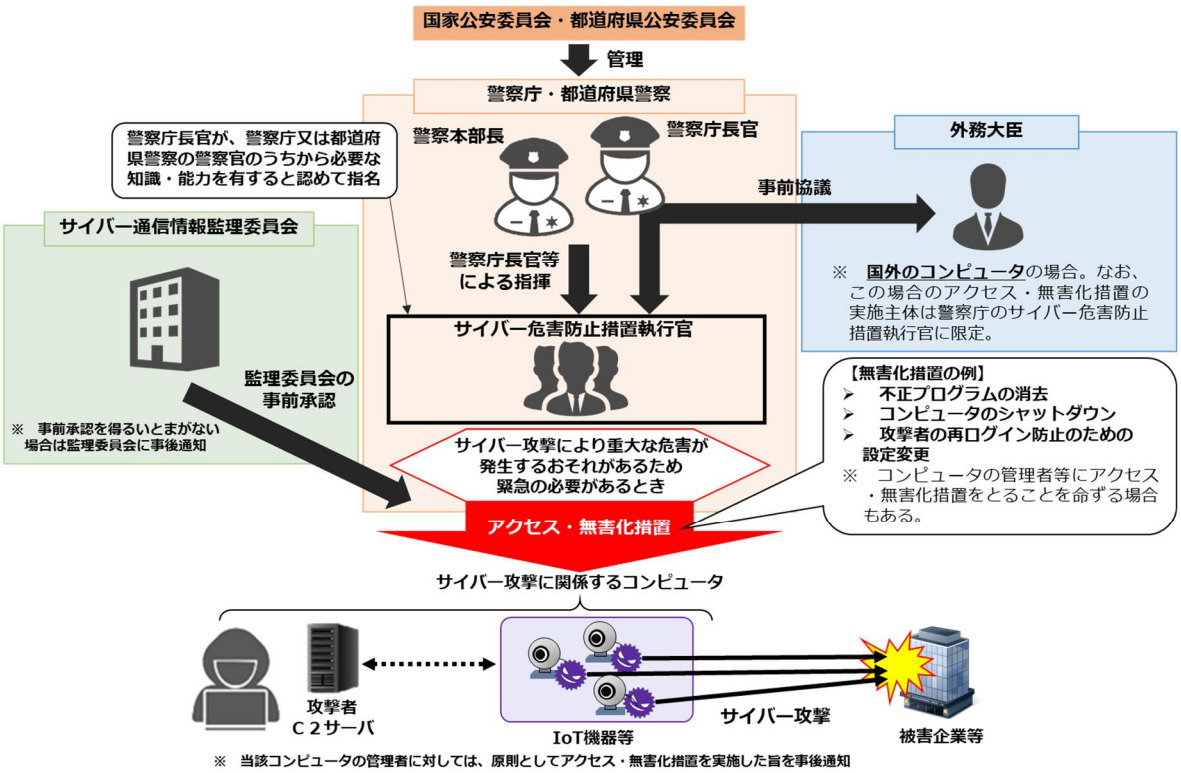
警察関係では、整備法により、警察官職務執行法の一部が改正され、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新たに設けられた。同規定は、令和８年 10 月１日に施行される予定であることから、警察では、令和７年 12 月に国家安全保障会議において決定された「アクセス・無害化措置の運用に関する指針」も踏まえつつ、その施行に向け、内閣官房国家サイバー統括室(NCO)や防衛省・自衛隊、外務省等との連携の強化を図っている。アクセス・無害化措置は、今後サイバー特別捜査部を中心に実施していくこととなるが、それには高い専門性や技術が必要になることから、その技術的支援に向けた更なる態勢の整備が必要になるものと考えられる。

---

[11] 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）

[12] 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）

【図表 36：改正警察官職務執行法の概要】



【図表 37：アクセス・無害化措置の運用に係る考え方】

■　アクセス・無害化措置の運用に関する指針は、アクセス・無害化措置が国家安全保障の観点から整合ある形で行われるよう、国家安全保障会議の関与の在り方を始めとする運用の指針を定めるもの。具体的には、1・2 の場合に国家安全保障会議で対処方針を審議

1
○　国外のコンピュータを対象とする場合
○　国内のコンピュータを対象とし、かつ、国家安全保障に関わると判断する場合
→ 警察・自衛隊による共同対処 又は 警察単独で実施(※)

2
自衛隊又は日本に所在する米軍が使用するコンピュータを警護する場合
→ 自衛隊単独で実施

3
国内のコンピュータを対象とし、かつ、国家安全保障に関わらないと判断する場合
→ 警察単独で実施

【出典：内閣官房】

（※）国家安全保障会議で自衛隊が対処を行う必要がないと判断される場合又は自衛隊法上の共同対処の要件を満たさない場合

トピックスⅡ　サイバー空間の匿名性の打破に向けた取組

１　サイバー空間の匿名性を悪用する匿名・流動型犯罪グループによる犯罪

情報通信技術の発達や社会のデジタル化の進展により、サイバー空間は、重要な社会経済活動が営まれる公共空間へと進化している。様々な社会経済活動が、サイバー空間を通じて非対面・非接触で行われるものへと大きく移行する中、サイバー空間が組織的詐欺等の犯行に悪用されることで、甚大な被害が生じている。例えば、多くの国民が利用するＳＮＳ上では、匿名・流動型犯罪グループによって、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ている実態が認められ、また、こうした募集への応募者が、リクルーターや指示役から、連絡に秘匿性の高い通信アプリケーションを用いるように誘導されている実態がある。このように、首謀者、指示役、犯罪実行役の間の連絡手段には、匿名性が高くメッセージが自動的に消去される仕組みを備えた通信手段が悪用されている。さらに、サイバー空間における資金移動は利便性が高い一方で、匿名・流動型犯罪グループにおいては、犯罪収益を暗号資産に変換し、海外の暗号資産交換業者の口座に移転することで資金の流れを仮装・隠匿するなど、警察による検挙を免れるため、サイバー空間の匿名性を悪用している実態がある。

２　匿名・流動型犯罪グループの検挙

サイバー特別捜査部では、犯罪に悪用される暗号資産の移転状況を追跡するとともに、追跡結果の横断的・俯瞰的な分析を行い、その結果を都道府県警察と共有している。このような分析により、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及び上位被疑者が浮き彫りになっている。

また、匿名・流動型犯罪グループの更なる検挙のため、令和７年 10 月、サイバー特別捜査部の態勢を強化した上で、同部の一部の職員について、警察庁匿名・流動型犯罪グループ情報分析室における分析要員としても勤務することとした。このような職員が、同室の有する他の情報も含めた多角的な分析を行うなど、サイバー空間の匿名性の打破と中核的人物の検挙につながるよう、取組を一層強化している。

コラム：サイバー空間の匿名性を悪用した「道具屋」、「相対屋」の検挙

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「道具屋」、「相対屋（あいたいや）」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。

例えば、「道具屋」については、サイバーパトロールの結果、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機関口座や暗号資産アカウントを不正に調達した上で、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、愛知県警察等の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。サイバー特別捜査部においては、都道府県警察や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結果、当該犯罪集団の首魁の男（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で逮捕した。

また、「相対屋」にあっては、広島県警察及びサイバー特別捜査部による合同捜査の結果、２名の男が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、隠匿していたほか、うち１名は、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いたことが判明したことから、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で逮捕した。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が特定され、事件構図の全容解明につながった。このように、相対屋を経由することで、暗号資産の追跡を困難にするなど、サイバー空間の匿名性をマネー・ローンダリングに悪用している実態が認められる。

【暗号資産を悪用したマネー・ローンダリングのイメージ】

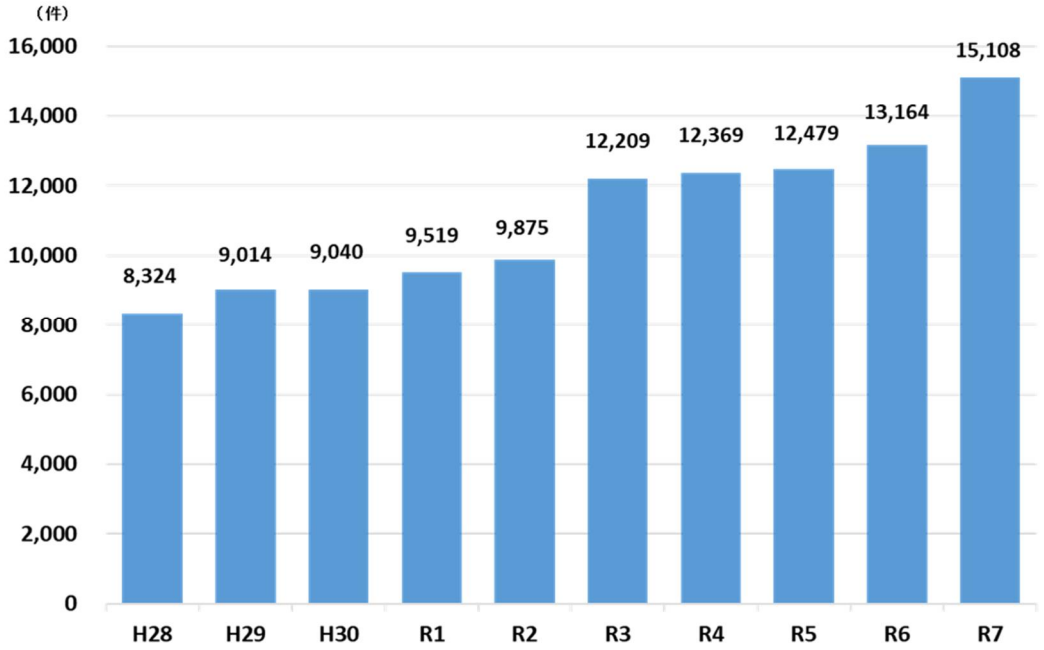
第２部　警察の取組

１　検挙に向けた取組

第１部に記載した脅威情勢に対し、警察では検挙に向けた取組を推進しているところ、サイバー特別捜査部においては重大サイバー事案[13]に、都道府県警察サイバー部門においては、高度な専門的知識及び技術を要するサイバー事案[14]に対処している。また、あらゆる犯罪がインターネット空間を悪用しているともいえる現状を受け、サイバー部門以外の捜査部門においてもサイバー事案やサイバー犯罪[15]に対処できるよう、技術的な支援を行うことができる体制を確保している。

この結果、令和７年におけるサイバー犯罪の検挙件数は１万 5,108 件に達している。サイバー犯罪の検挙件数のうち、犯罪収益移転防止法の検挙件数は 2,868 件で、そのうち 1,012 件が匿名性の高い通信方法を用いた犯行としてサイバー事案にも該当し、前年と比較していずれも増加している。

【図表 38：サイバー犯罪の検挙件数】



(1)　検挙

①　サイバー特別捜査部

サイバー特別捜査部は、その高度な情報集約・分析機能により全国警察の

---

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

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

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

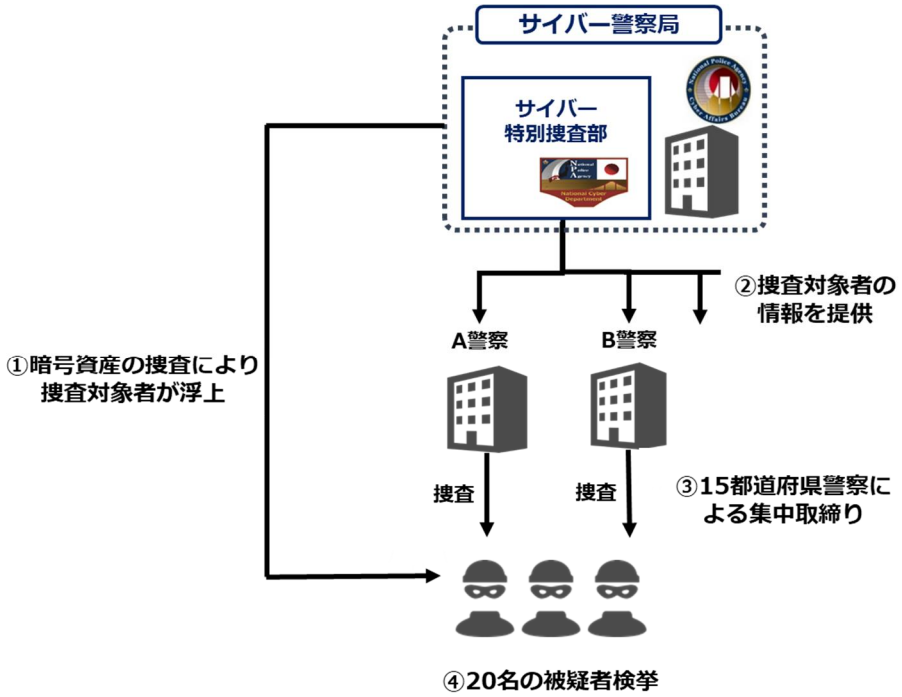
ハブとしての役割を果たすとともに、そうして得られた情報と外国治安機関等との強固な信頼関係を武器に、国際共同捜査等を通じて、国境を越えて敢行されるサイバー事案に対処する、いわば世界と日本との結節点としての役割を果たしている。

【CASE：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。

【図表 39：暗号資産の追跡技術を用いた集中取締りの概要】



②　都道府県警察サイバー部門

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

コラム：少年グループによる eSIM 不正取得等事件の検挙

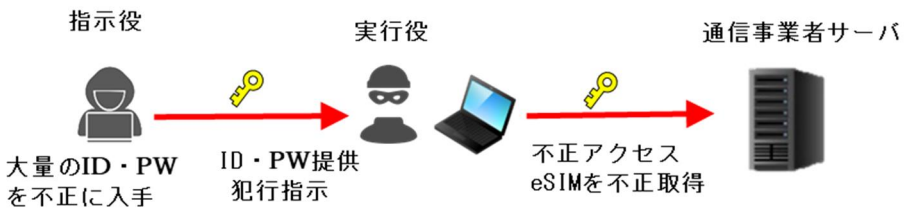
SNS で結びついた中高生の少年３人(14 歳から 16 歳)は、不正に取得した eSIM を販売して利益を得ようと考え、令和６年５月から同年８月までの間に、それぞれ、不正に取得した他人の ID とパスワードを使い、電気通信事業者が管理するサーバコンピュータに不正アクセスした上で、通信契約に係る不実の電磁的記録を作成し、eSIM を不正に取得した。令和７年１月から同年２月にかけて、同少年らを不正アクセス禁止法違反及び電子計算機使用詐欺罪等で逮捕した。(警視庁)

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

また、当該手口を模倣し、不正に取得した eSIM を販売して利益を得ようと考え、無職の少年(16 歳)と高校生の少年(16 歳)２名が、模倣した手口により eSIM を不正に取得したことを受け、令和７年３月及び８月、同少年ら２人を不正アクセス禁止法違反及び電子計算機使用詐欺罪で逮捕した。(警視庁・神奈川)

eSIM を含むデータ通信専用 SIM 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、このような悪用事例が後を絶たないため、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ているほか、政府全体としても「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、各種サービスやインフラの不正利用を防止するための取組として、「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」を盛り込んだところである。これらを踏まえ、政府では、データ通信専用 SIM の契約時において本人確認を厳格化することなどを内容とする携帯電話不正利用防止法の改正に向けた検討を行っている。

【eSIM 不正取得事件の検挙の概要】



【CASE:少年らによるオンラインカジノ利用に係る資金決済法違反事案】

オンラインカジノについてサイバーパトロールを端緒とした取締りを行った結果、令和６年５月から令和７年５月にかけて、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変換したとして、令和７年 10 月、大学生の男(19)を常習賭博罪、資金決済法違反等で逮捕した（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)を常習賭博罪で児童相談所に通告するなど、合計 19 人を常習賭博罪等で検挙又は児童相談所に通告した。

(2) 捜査支援

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

【CASE：顧客情報を不正に持ち出した不正競争防止法違反事案】

パート従業員の女（45 歳）は、自身の転職を優位に進める目的で、令和 6 年 2 月から 3 月までの間、当時勤務していた青森県内に所在する介護事業所から営業秘密である同事業所の顧客情報を複製したうえで領得した。令和７年１月、同女を不正競争防止法違反（営業秘密の領得）で逮捕した。この事案では、同県警察の保安部門から支援要請を受け、サイバー部門が、同女の転職先の介護事業所に設置されたパソコン等の電子機器の解析・データ精査等を支援し、同女の犯行を裏付けた。（青森）

【CASE：オンラインカジノによる組織的な常習賭博事案】

会社役員の男（42 歳）を中心とした犯罪グループは、令和６年４月から５月までの間、海外のオンラインカジノサイトの賭金入金に係る決済システムの管理、システムを利用した資金管理等の業務を継続的に行うなどして、不特定多数の賭客を相手方として、組織的に常習賭博を行っていた。令和７年６月、同人を含む９人を組織犯罪処罰法違反（組織的常習賭博）で逮捕した。この事案では、神奈川県警察の組織犯罪対策部門から支援要請を受け、サイバー部門が、入金管理システムが蔵置されている国内のレンタルサーバの特定やサーバ検証・解析等を支援し、同人らの犯行を裏付けた。（神奈川）

【CASE：特殊詐欺等の被害金を隠匿した組織犯罪処罰法違反事案】

会社役員の男（52 歳）らは、令和５年 10 月、特殊詐欺グループから依頼を受け、当該グループが特殊詐欺等によって得た犯罪収益について、複数の銀行口座を経由して国内暗号資産口座に送金、暗号資産を取得し、取得した暗号資産の一部を国外暗号

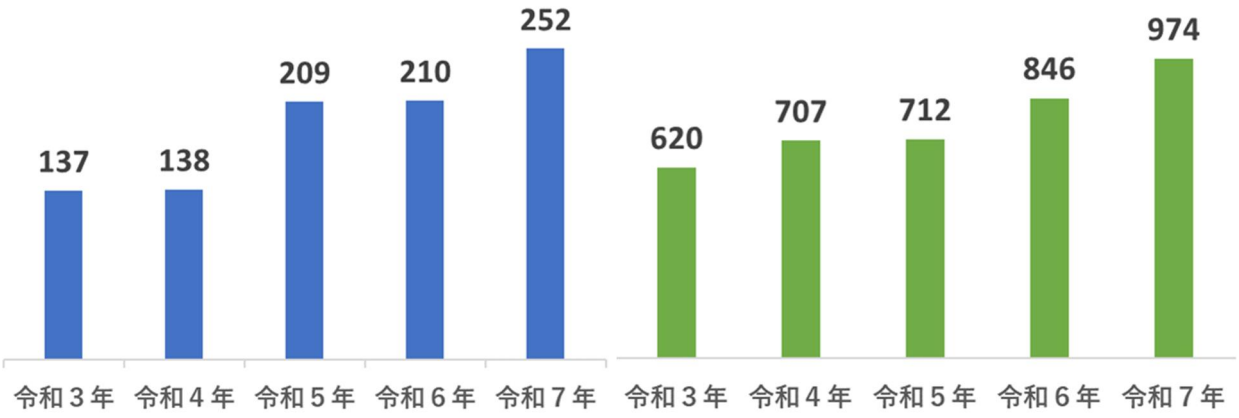
資産取引所に開設されたアカウントに紐付くコインアドレスに移転し、犯罪収益を隠匿したとして、令和７年９月、同人を含む４名を組織犯罪処罰法違反で逮捕した。

この事案では、福井県警察の組織犯罪対策部門から支援要請を受け、サイバー部門が暗号資産に交換された被害金の追跡を支援し、同人らの犯行を裏付けた。（福井）

また、警察庁及び全国の情報通信部に設置された情報技術解析課においては、都道府県警察等に対し、捜索・差押の現場でコンピュータ等を適切に差し押さえるための技術的な指導、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、高性能な解析用資機材を整備し、破損した電磁的記録媒体からの情報の抽出・可視化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。

【図表 40：高度情報技術解析センターにおける解析件数・相談対応件数】



【CASE：焼損したスマートフォンからのデータ抽出】

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

【CASE：破損した電磁的記録媒体からのデータ抽出】

令和７年５月から同年６月にかけて、警察庁高度情報技術解析センターは、無職の

男（36）による、未成年に対する性犯罪事件に関し、破損して通常の方法では認識されない状態で押収したＵＳＢメモリ及びハードディスクを機能回復し、データを抽出できる状態にした。その結果、当該ＵＳＢメモリ及びハードディスクから犯行の動機や余罪を裏付ける電磁的記録を抽出することができ、同事件の全容解明に貢献した。

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

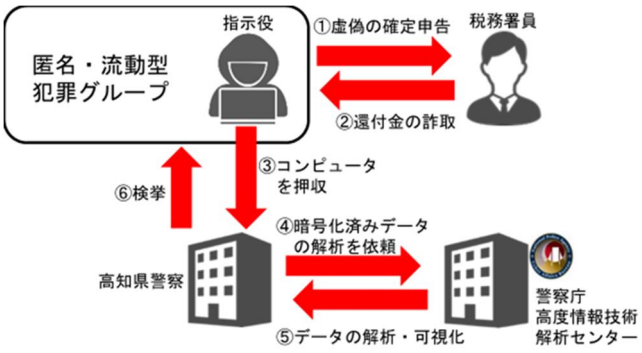
コラム：解析能力向上のための資機材の整備

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・複雑化も顕著であることから、警察捜査を支えるためには、データの暗号化や破損、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。

警察庁高度情報技術解析センターでは、高速演算装置及び解析基盤装置を始めとする高度な解析用機器を整備し、暗号により隠ぺいされたデータ、破損した電子機器等の高度な解析に対して、技術支援を行っている。

○暗号化されたデータの抽出が検挙につながった事例

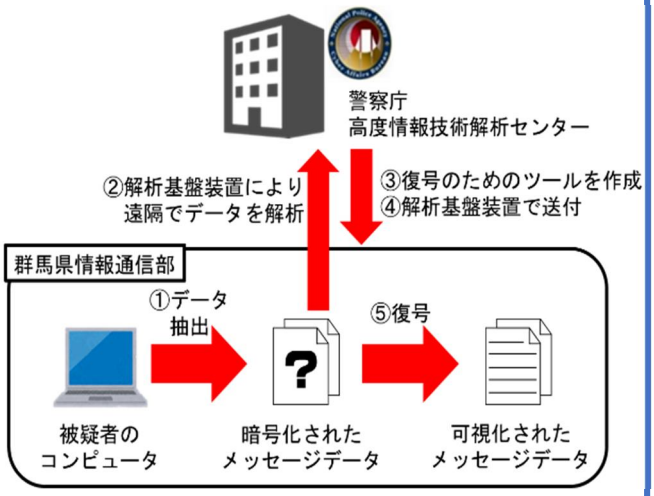
【検挙までの流れ】



デザイン業の男（40）らは、令和６年４月から令和７年３月にかけて、虚偽の内容による確定申告を行い、税務署員にその旨誤信させ、口座に還付加算金を振込入金させた。当初、同男は犯行を否認しており、証拠品として押収されたコンピュータ内のデータも暗号化されていたが、警察庁高度情報技術解析センターにおいて当該データの解析を行った結果、当該コンピュータから、虚偽の内容が含まれた確定申告に係る電磁的記録や、犯行に関与した者に関する電磁的記録等を発見した。警察では、当該解析結果等を元に同男を指示役とする匿名・流動型犯罪グループの犯行であることを解明し、令和７年５月までに、同男ら 10 人を詐欺罪等で逮捕した（高知）。

○遠隔支援により暗号化されたデータを復号した事例

【遠隔支援の流れ】



令和７年 12 月、ベトナム国籍の男（50）らによる有印公文書偽造事件に関し、警察庁高度情報技術解析センターは、解析基盤装置を活用することで、同男が使用していたメッセージアプリの暗号化されたデータを遠隔で解析し、これを復号するためのツールを作成した。群馬県情報通信部において当該ツールを使用した結果、犯罪収益の処分状況を裏付ける記録を抽出することができ、事件の真相解明に貢献した。

(3) 国際連携

サイバー事案の多くは国境を越えて敢行されるため、そうした事案への対処には国際連携が重要であるところ、警察においては、サイバー空間における脅威に関する情報の共有、国際捜査共助に関する連携強化、情報技術解析に関する知識・経験等の共有等のため、多国間における情報交換や協力関係の確立等に積極的に取り組んでいる。

警察庁サイバー警察局では、令和７年中、Ｇ７ローマ／リヨン・グループに置かれたハイテク犯罪サブグループ、サイバー犯罪条約（通称：ブダペスト条約）の締約国等が参加するサイバー犯罪条約委員会会合、EUROPOL が主催する欧州警察長官会議等の国際会議に参加し、各国におけるサイバー犯罪対策への取組みについて議論を行うなど、国際的な情報共有の更なる強化を推進している。特に、このような国際会議においてハイレベルな幹部間協議を行うことは、国際連携強化という面で非常に重要であることから、幹部職員の積極的な海外出張・国際会議出席は、今後、ますます必要になると見込まれる。

また、ICPO 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等に関する研修に我が国の警察職員を派遣したほか、外国治安機関等の捜査員等を日本に招へいし、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、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 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。

加えて、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いる。

コラム：サポート詐欺に対する国際共同捜査

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

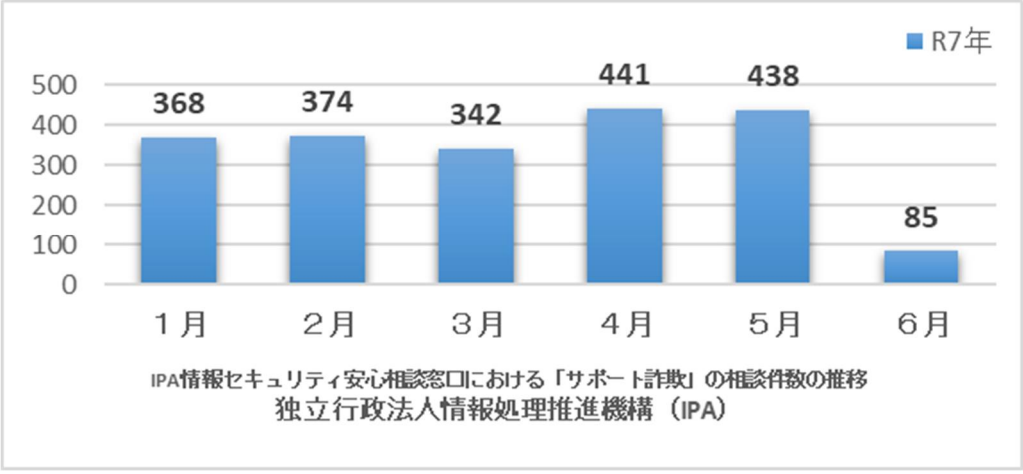
本件は、被疑者グループが生成 AI を悪用し、標的の特定やポップアップウィンドウの作成、日本語への翻訳を行うなど、犯行に AI が使用された事案ではあったが、JC３や Microsoft 社による独自の取組に基づく協力に加え、日本警察と CBI との緊密な連携により被疑者の逮捕に至ったものであり、国際的な官民連携の新たなリーディングケースとなった。

また、本件検挙後の令和７年６月中に IPA（独立行政法人情報処理推進機構）に寄せられた「ウイルス検出の偽警告」に関する相談は 85 件であり、大幅に減少した。

令和８年１月、警察庁サイバー警察局サイバー捜査課長が CBI を訪問し、CBI の次長（サイバー担当）に対して捜査協力への感謝状を手交するとともに、今後の国際連携の更なる強化を確認した。

【サイバー捜査課長が感謝状を手交する状況】

【図表 41：サポート詐欺に係る報告件数の推移】



【CASE：オンライン上の児童ポルノ事犯の取締りに係る国際共同捜査】

令和７年２月から３月にかけて、警察（生活安全部門）は、国際連携強化の一環として、６つの国と地域（日本、シンガポール、韓国、香港、タイ及びマレーシア）において、オンライン上の児童ポルノ事犯の取締りに係る国際共同捜査を実施した（合計で 544 人の被疑者を検挙）。

【児童ポルノ事犯被疑者検挙の様子】

２　被害の未然防止・拡大防止に向けた取組

サイバー空間の安全・安心を確保するため、警察では、サイバー事案の検挙に向けた取組のみならず、攻撃者・犯行手口等の実態解明、被害の未然防止・拡大防止対策等を推進している。

(1)　情報発信

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

①　国際連携を通じた情報発信

国家を背景とするサイバー攻撃等、高度な技術を悪用したサイバー攻撃への対策においては、攻撃者の検挙に向けた捜査を推進するのみならず、サイバー攻撃を受けたコンピュータ等を解析し、攻撃者及び手口に関する実態解明を進めており、未然防止対策等に関する注意喚起を実施している。例えば、令和７年１月、警察庁及び NISC は、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から日本国内の組織、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。

このほか、我が国としてサイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止するパブリック・アトリビューションを実施している。例えば、同年８月には中国を背景とするサイバー攻撃グループ「Salt Typhoon」に関するパブリック・アトリビューションを実施した。

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

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

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。

コラム：豪州主導国際文書への共同署名

令和７年10月、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」（”Foundations for modern defensible architecture”）の共同署名に加わった。本文書は、情報システムを設計などする技術者に対して、サイバー空間における脅威に対応したシステムの構築等のために役立つアプローチを提供するものである。

② 関係機関との連携を通じた情報発信

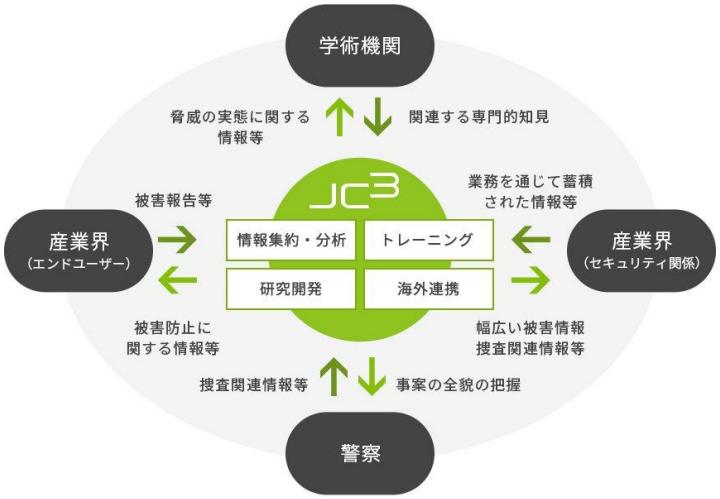
警察では、様々な関係機関と連携した情報発信を行っており、特に一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center の略）との連携を推進している。

JC3 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[16] に類似の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、指摘されたことを受け、日本版 NCFTA として産学官の情報や知見を集約・分析し、その結果等を還元することにより、国民が安全かつ安心してインターネットを利用できる環境の構築に貢献することを目的として設立され、平成 26 年 11 月に業務を開始した。

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

JC3 では、利用者がだまされて不正なスマートフォンアプリを導入することが原因で、個人のスマートフォンから身に覚えのない大量の SMS を配信し、料金が高額になる等の事象が確認されていることから、こうした悪性の SMS が存在することを認識し、安易な URL リンクへのアクセスやアプリの導入に危険が伴うことについて注意喚起している。さらに最近では、偽 SMS の文面の作成に生成 AI を悪用したとみられる事象を確認するなど、攻撃手法が高度化していることについての注意喚起も行っている。

【図表 42：日本サイバー犯罪対策センター（JC3）の概要】



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

また、各都道府県警察においては、金融機関、暗号資産交換事業者、医療機関、商工会議所、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。

さらに、警察庁においては、ランサムウェア等のサイバー事案の未然防止及び発生時における被害拡大防止のため、VPN 機器等のぜい弱性対策や認証情報の適切な管理、バックアップやログの適切な取得、サイバー攻撃を想定した業務継続計画（BCP）の策定、被害発生時における速やかな警察への通報・相談等について、特に被害が増加傾向にある中小企業を主な対象としつつ、幅広く周知・啓発に取り組んでいる。そのほか、関係省庁と連携した業界団体及び事業者等への周知、サイバーセキュリティ月間 2025 における NISC と連携した中小企業向けセミナー、内閣府政府広報室や損害保険会社との連携による広報啓発記事・動画の制作等を行った。（ランサムウェア対策を紹介する広報啓発動画に関しては、特集 II を参照。）

加えて、各都道府県警察や重要インフラ事業者等で構成される「サイバーテロ対策協議会」を全ての都道府県に設置し、サイバー攻撃事案の知見を踏まえた共同対処訓練等を実施しているほか、警察及び全国約 8,800 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（CCI ネットワーク：Counter Cyber Intelligence Network）の枠組みを通じ、情報窃取を企図したとみられるサイバー攻撃に関する各種情報を集約するとともに、事業者等に対し注意喚起等を実施している。

令和 7 年 1 月には、大阪・関西万博開催に備え、大阪府警察及び大阪・関西万博関係事業者と共同で、実際のサイバー攻撃への対処を想定したインシデント対応訓練を実施した（警察庁主催）。訓練では、架空の企業のセキュリティ対応チームの一員として、サイバー攻撃に対する実機を使用した実践訓練に加え、顧客対応や警察への被害報告等が行われた。このほか、警察庁において大阪・関西万博関係事業者をはじめとした全国の重要インフラ事業者等からの依頼に基づきセキュリティ診断を実施し、診断結果に基づく注意喚起を実施した。こうした取組が功を奏し、令和 7 年 4 月から 10 月まで開催された大阪・関西万博は、運営に支障をきたすサイバー攻撃を許さず、成功裏に終わった。

コラム： JC3 によるランサムウェア対策のポッドキャスト

令和７年 12 月、JC３は、弁護士、民間のセキュリティ技術者、サイバー犯罪捜査官、検事等、ランサムウェアの脅威に最前線で立ち向かう専門家たちとの対話を通じて、今後のランサムウェアの被害者になり得る人々のセキュリティリテラシーを高めることを目的とした「JC３ポッドキャスト ランサムウェア・ダイアログ」の配信を開始しており、このような取組を通じた被害の未然防止を推進している。

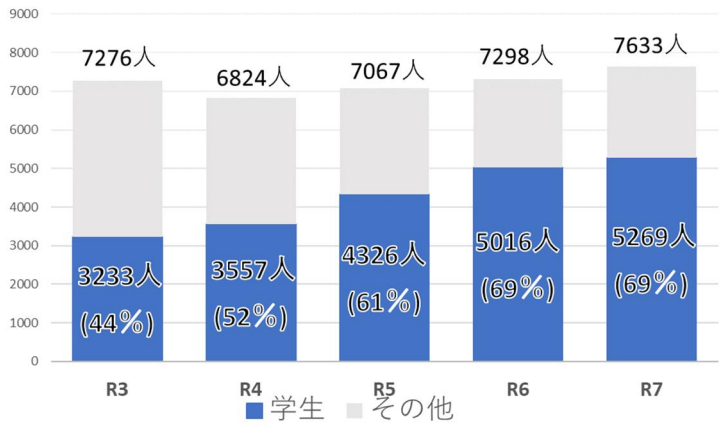
※ 内容には個人的意見を含んでおり、出演者所属組織やJC3の公式見解とは異なることがあります。

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

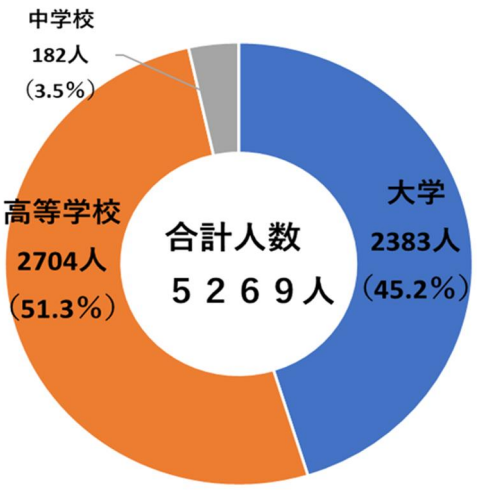
サイバー防犯ボランティアは、「自分たちの利用するインターネットの安全は自分たちで守る。」というコンセプトの下、安全で安心して利用できるインターネット空間を作るための自主的な防犯活動のことを言い、全国で 332 団体、7,633 人（令和７年 12 月末現在）が、「被害防止のための教育活動」、「広報啓発活動」、「サイバー空間の浄化活動（サイバーパトロール）」を柱とする活動を行っており、警察ではその活動の拡大・活性化に向けた支援を行っている。

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。

【図表 43：サイバー防犯ボランティア数の推移】



【図表 44：サイバー防犯ボランティアの学生別内訳】



コラム： 金沢工業大学サイバー防犯ボランティアの取組

金沢工業大学（石川県）においては、学生同士がセキュリティを始めとする様々な知識の共有を行う場である「情報セキュリティ・スキルアッププロジェクト」の中で、地域におけるサイバー防犯活動にも取り組んでいる。

具体的な活動内容としては、

○ 小中学生を対象としたセキュリティ教室の開催

○ 被害防止のための広報啓発動画の制作

○ 小学生から高校生、その保護者を対象としたサイバーセキュリティ学習用のゲームサイトの制作、運用

等を行っている。

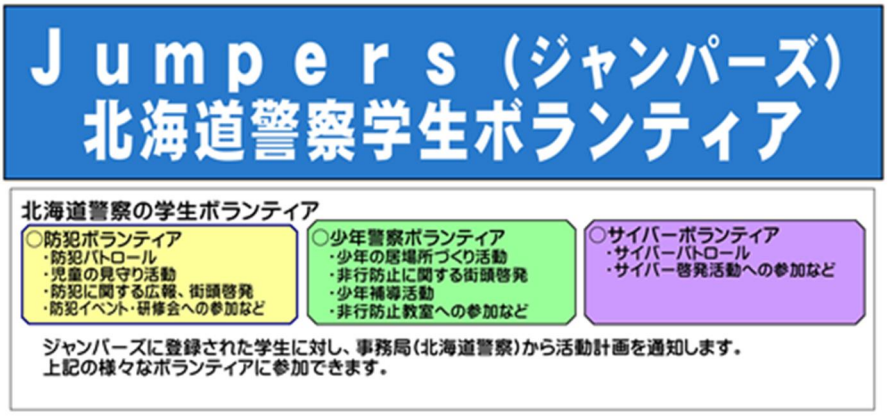
令和７年 11 月には、これまでの防犯活動における功績により、内閣総理大臣から「安全安心なまちづくり関係功労者表彰」を授与されている。

【金沢工業大学サイバー防犯ボランティアの様子】

コラム： サイバー防犯ボランティアの拡大・活性化への支援

北海道警察では、複数のボランティア活動への参加・登録手続を一元化し、学生が各種活動に参加しやすい環境を作ることを目的として、各ボランティアを統合した「Ｊｕｍｐｅｒｓ」という新たな学生ボランティア組織を設立し、運営している。「Ｊｕｍｐｅｒｓ」に登録すれば、様々なボランティア活動の中から、希望する活動に参加できるなど、積極的なボランティア活動への参加促進に寄与している。

また、北海道警察や広島県警察では、一部の警察官採用試験において、一定程度のボランティア活動歴を有している者に対して加点措置を実施するなど、サイバー防犯ボランティアの拡大・活性化に向けた施策に取り組んでいる。



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。

(2) 犯罪インフラへの対処

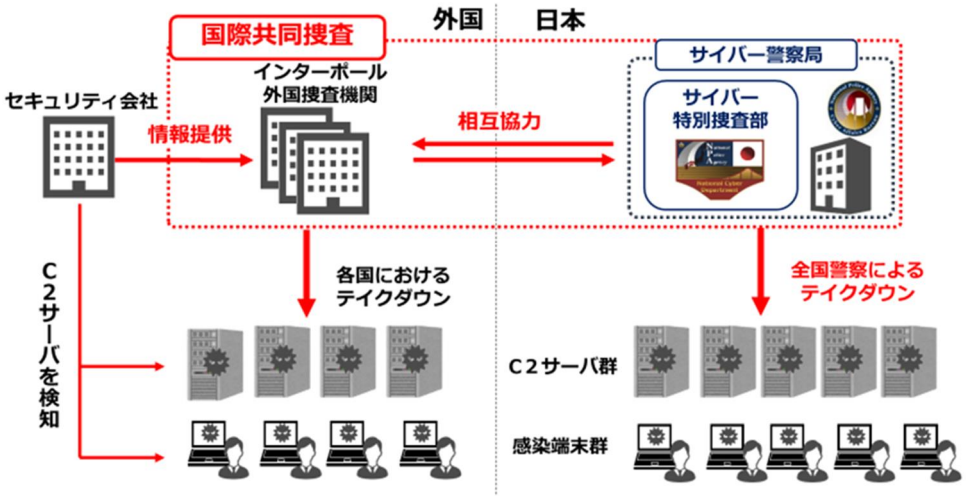
サイバー事案による被害を防止するためには、犯罪インフラへの対処が必要であるところ、この対処に当たっては、警察による取組のみならず、民間事業者、学術機関、関係省庁等も含めた社会全体における対策が重要である。特に、新たなサービスや技術が、その欠陥を突かれるなどして悪用される例が認められることから、その悪用防止に向けては、産学官の連携による効果的な対策を実施している。

① 高度な技術を悪用したサイバー攻撃に関するインフラへの対処

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C2サーバとして機能している国内のサーバを把握し、当該C2サーバの不正な機能を停止するよう、サーバを管理する事業者等に依頼するなどして、C2サーバの対策を継続的に実施するなどしている。

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。

【図表 45：インフォスティーラーに対する INTERPOL との国際共同捜査】



② インターネット空間を悪用した犯罪に関するインフラへの対処

○ フィッシングサイト対策

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

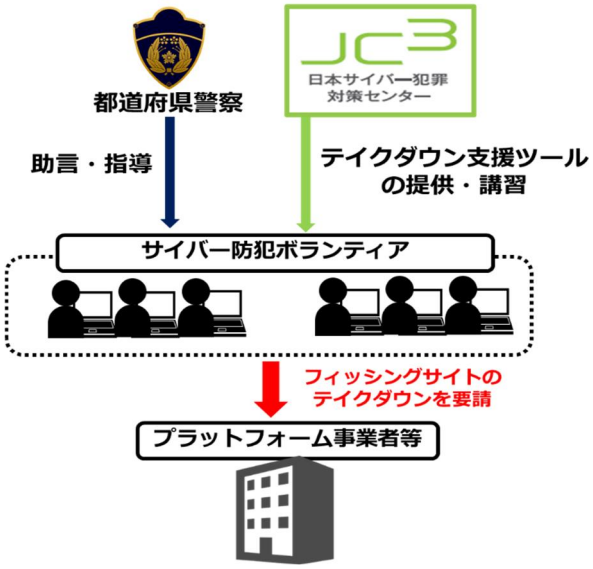
また、１つの IP アドレス上に、数百のフィッシングサイトが構築されているといったフィッシングサイトの特性を踏まえた先制的な対策として、警察庁において、同一の IP アドレスに紐づくドメイン情報を独自に収集し、未把握のフィッシングサイトを発見・提供している。

さらに、フィッシングの手口が巧妙化し、被害が急増している情勢に鑑み、利用者保護のため、フィッシングサイトにアクセスさせないための対策として、「なりすましメールを防ぐ技術（DMARC[17]等）への対応促進」を始め、「フィッシングサイトの閉鎖促進」や「パスワードに代わって生体認証等により簡単かつ安全にログインできる認証方法（パスキー）の普及促進」について、所管省庁を通じ、事業者に対する対策の要請を実施した。

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

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

【図表 46：フィッシングサイト撲滅チャレンジカップ】

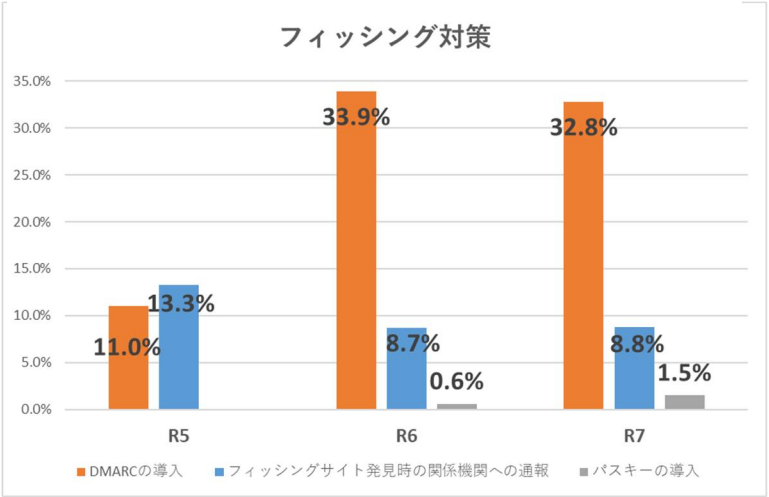


コラム：民間企業等における不正アクセス行為対策の調査結果

警察庁において、無作為に抽出した民間企業や行政機関等に対して不正アクセス行為対策等に関する調査を実施した結果、民間企業等のフィッシング対策として、DMARC 導入率は令和 6 年に大きく増加した。

また、民間企業等が過去 1 年間で受けたサイバー攻撃は、過去 10 年間で比較すると DDoS 攻撃は半減し、マルウェア設置・感染は大幅に減少した。さらに、民間企業等における対応マニュアルや要領の策定状況については、約 55%が策定済みで、過去 10 年で増加傾向であった。(統計編 158 頁参照)

【図表 47：民間企業におけるフィッシング対策の推移】



※パスキーの導入は、令和 6 年から調査項目に追加。

○　インターネットバンキングに係る不正送金対策

警察庁は、令和７年 11 月からボイスフィッシングによる法人口座の不正送金被害が再び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及び一般財団法人日本サイバー犯罪対策センター（JC3）と連名で、広報啓発資料「サイバー警察局便り」を作成した上で、警察庁ウェブサイト等にて公開し、その手口の詳細や対策に関する注意喚起を実施した。

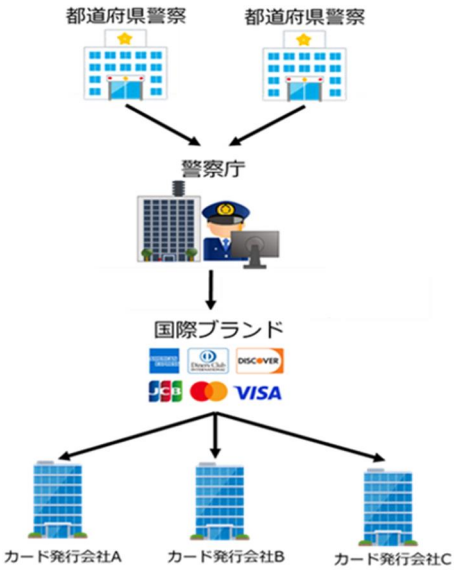
○　証券口座不正取引対策

証券口座不正取引の被害情勢を踏まえ、警察庁は、令和７年５月、ウェブサイト等において証券会社をかたるフィッシングについて注意喚起を行ったほか、同年７月には、金融庁と連名で、日本証券業協会を含む金融関係協会に対して、被害を踏まえた具体的なフィッシングの手口やその対策を示した上で、顧客口座・アカウントの不正アクセス・不正取引対策の強化について要請した。（資料編 106 頁参照）

○　クレジットカード不正利用対策

各都道府県警察で把握した、悪用されたクレジットカード番号を警察庁で速やかに集約し、カード発行会社を含む決済システム全体を統括する国際ブランド各社に対し、一括して提供しており、クレジットカード発行会社における不正利用対策に活用されているところ、令和７年は、約 187 万件のクレジットカード番号を国際ブランド各社に提供した。

【図表 48：国際ブランドに対する不正クレジットカード番号情報提供】



③　違法・有害情報に関するインフラへの対処

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

○　インターネット・ホットラインセンター（IHC）における取組

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

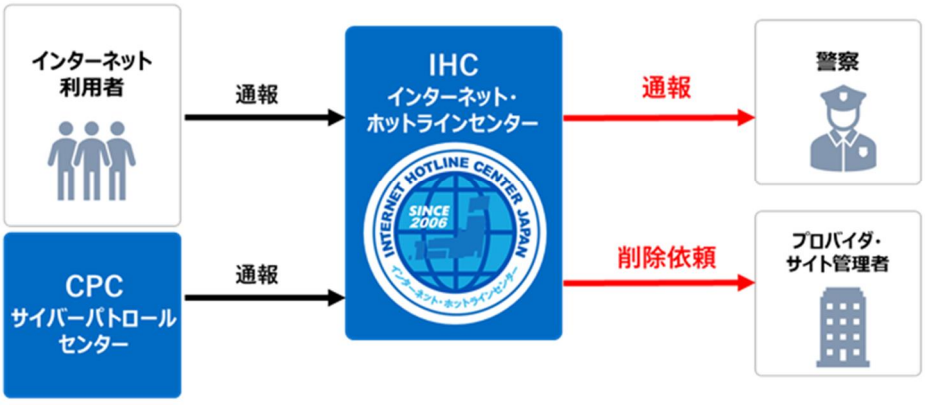
犯罪密接関連情報及び自殺誘引等情報を収集し、IHC に通報するサイバーパトロールセンター（CPC）を事業委託している。

令和 7 年の IHC の受理件数のうち、運用ガイドラインに基づいて 63 万 3,036 件を分析した結果、違法情報を 10 万 5,553 件、重要犯罪密接関連情報を 1,538 件、自殺誘引等情報を 5,321 件と判断した。

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

さらに、同年 6 月、ギャンブル等依存症対策基本法の一部を改正する法律が成立し、インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為等が禁止されたことから、同年 9 月の法施行に合わせて IHC の運用ガイドラインを改定し、これら情報を新たに違法情報として取扱範囲に追加するなど、社会問題となっているこれら情報の流通防止に向けた取組を強化した。（37 頁参照）

【図表 49：インターネット・ホットラインセンターの仕組み】



○　警察における取組

警察庁では、IHC 等の取組について周知を図るとともに、違法・有害情報の削除の実効性を確保するため、令和 7 年 10 月、国内のプロバイダ事業者等

に対して、違法・有害情報に関する削除への引き続きの協力を依頼した。都道府県警察においても、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ており、令和７年は、約 53 万件の違法・有害情報の削除依頼等を行った。

また、ＳＮＳ事業者に対し、警察が認知したＳＮＳ型投資・ロマンス詐欺及び特殊詐欺の犯行に利用されたアカウントの利用停止や削除等を促すための情報提供を行う仕組みを運用しているところ、令和７年は、1 万 8,500 件を超える情報提供を実施した。

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・オフェ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、各種施策を推進している。（資料編 108 頁参照）。

３　基盤整備

(1)　体制の拡充

警察庁サイバー警察局は、令和７年度の定員数が 260 名（前年比＋14 名）であり、関東管区サイバー特別捜査部の定員数が 185 名（前年比＋56 名）と年々体制を拡充している。

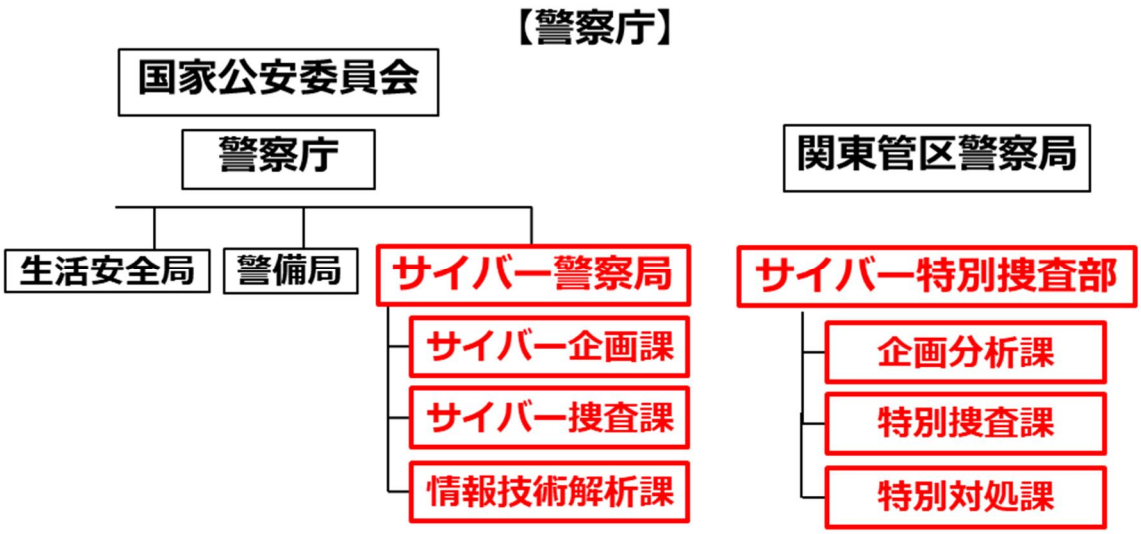
令和４年４月、警察法を改正し、重大サイバー事案の対処を担う国の捜査機関として、関東管区警察局にサイバー特別捜査隊を設置した。

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

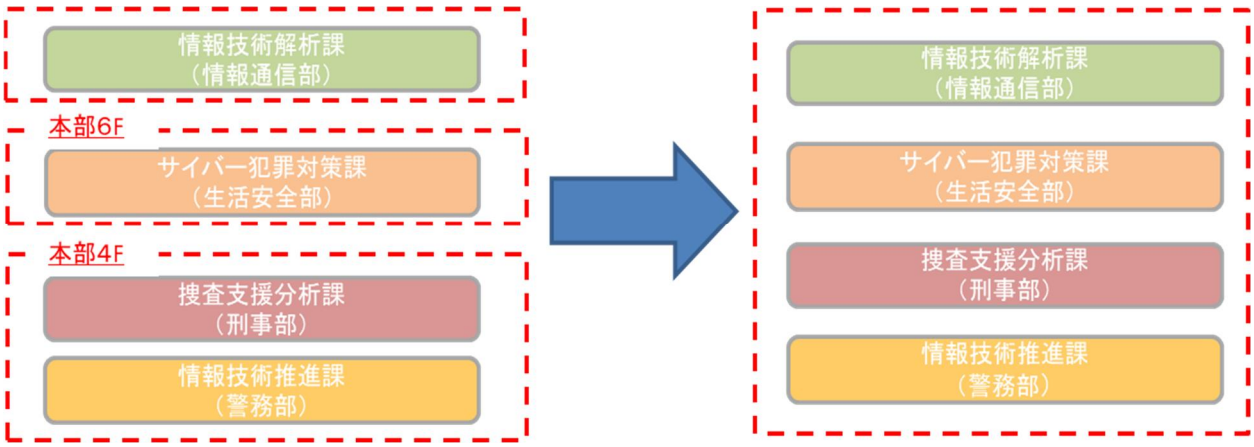
れらにより、捜査はもとより、重大サイバー事案の対処に必要な情報の収集、整理及び事案横断的な分析、事案発生の予防及び被害の拡大防止等を行う体制が強化された。これは、都道府県警察が捜査により得た膨大な情報をサイバー特別捜査部に集約し、同部が、外国治安機関等との情報交換や独自の捜査により得た情報と併せて高度な分析・解析を行うことにより、犯罪グループの中枢被疑者の特定や実態解明等を一層推進するためのものである。

【図表 50：サイバー警察局及びサイバー特別捜査部の概要】



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

【図表 51：山口県警察におけるフロアー体化の例】



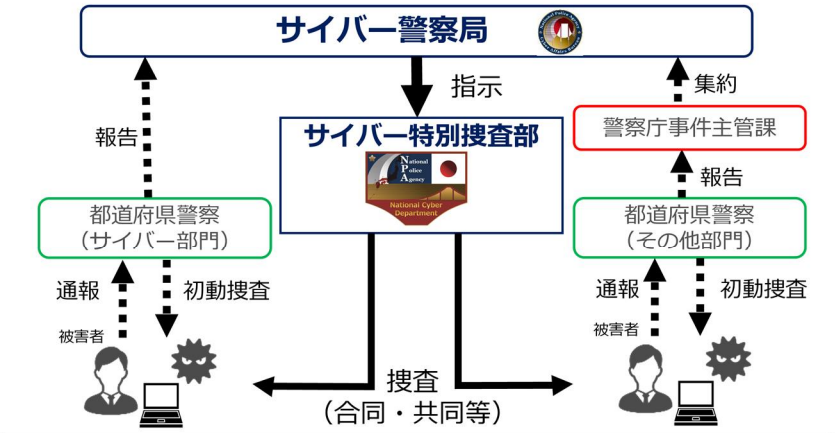
コラム：重大サイバー事案捜査における各警察組織の関係

個々のサイバー事案は、発生時点ではその事案を生起した主体やその意図、背景、関連性が明らかでない。そこで、犯罪組織による組織的な犯行や国家を背景とする安全保障に関わるサイバー攻撃等をあぶり出し、的確に対処するには、個々のサイバー事案の捜査を着実に推進してその実態を解明するとともに、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ことが不可欠である。

そのため、警察においては、個々のサイバー事案に対して治安責任を有する都道府県警察が一次的に捜査を推進し、被疑者や当該事案に用いられたインフラの特定等を進めるとともに、これらの情報をサイバー特別捜査部に集約し、同部が「情報のハブ」として、俯瞰的・横断的な分析を行うことにより、主体やインフラの共通性等の事案間の関連性を明らかにし、その組織性や国家の関与を解明している。

その結果に基づき、外国治安機関等との国際共同捜査を通じた被疑者の特定・検挙、パブリック・アトリビューションの実施、また、今後は令和８年 10 月１日に施行予定のアクセス・無害化措置に係る権限を適切に行使するなど、犯罪から安全保障に関わる事案までシームレスに対処し、サイバー空間における安全・安心の確保に取り組んでいる。

【サイバー事案における各警察組織の関係】



(2)　人材確保・育成

○　人材確保

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

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

コラム：中途採用・官民人事交流制度により採用された幹部警察官

○　サイバー特別捜査官として採用された幹部警察官

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

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

事件捜査を指揮する
丸山　篤　警視正

○　官民人事交流制度により採用された幹部警察官

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

令和 5 年 10 月、同制度により、改めて警察庁に採用され、民間の最新の知見をいかし、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
濵石　佳孝　警視正

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

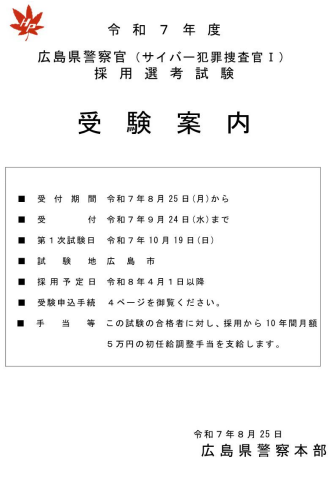
また、高度なサイバー人材の確保の取組として、官民人事交流制度による民間人材の登用を進めており、サイバー警察局では、同局設置の令和４年以降、官民人事交流制度により、民間企業から高度な知識・技術を有する８名を採用しているほか、令和８年度からは、専らサイバー事案の対処等に係る事務に従事する技術系職員２名の採用を予定している（サイバー採用）。

コラム：サイバー人材の新たな確保方策

警察庁では、サイバー空間の脅威に的確に対処していくため、令和８年度から、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を２名採用予定である（いわゆる「サイバー採用」）。同採用は、令和８年度採用が初めての試みであり、情報処理に関する応用的知識・技能を有する者を対象に、警察庁独自の採用試験を行うなど、警察庁でサイバー部門の業務を専門的に担う技官の採用選考を実施したものである。

サイバー採用により採用された技術系職員は、その専門的知識をいかすべく、主として警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において勤務することとなる。警察庁では、このように専門分野の技術力伸長を意識した人事配置を実施することで、高度な専門的知識を有する人材が活躍できるキャリアパスの構築を強力に推進している。令和８年度採用に引き続き、令和９年度サイバー採用の募集を実施している。

また、広島県警察においては、令和７年度から、令和８年度以降採用予定のサイバー犯罪捜査官の募集を開始したところであるが、高度かつ専門的な知識及び技能を有するサイバー人材への優遇措置として、応用情報技術者以上の試験合格者に対し、採用の日から 10 年間月額５万円を支給する初任給調整手当を導入することとし、本年度の採用区分（サイバー犯罪捜査官Ⅰ）の採用試験において１名が合格・内定している。また、採用区分（サイバー犯罪捜査官Ⅱ）の採用試験において、サイバー防犯ボランティア経験者に対する試験加点も導入している。



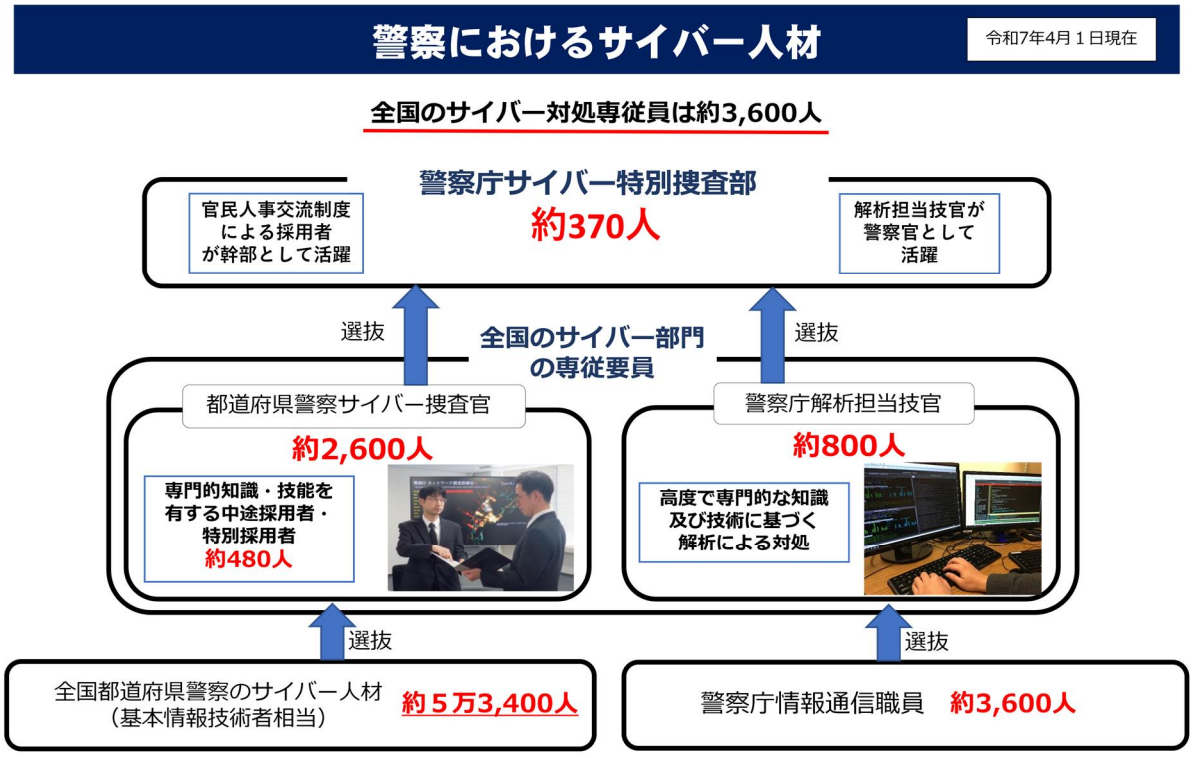
令和７年度
広島県警察官（サイバー犯罪捜査官Ⅰ）
採用選考試験

受験案内

■ 受付期間　令和７年８月25日(月)から
■ 受　　付　令和７年９月24日(水)まで
■ 第１次試験日　令和７年10月19日(日)
■ 試験地　広島市
■ 採用予定日　令和８年４月１日以降
■ 受験申込手続　４ページを御覧ください。
■ 手当等　この試験の合格者に対し、採用から10年間月額５万円の初任給調整手当を支給します。

令和７年８月25日
広島県警察本部

【図表 52：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370人には、定員185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3,600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480人のうち、サイバー部門以外に所属する約230人については、都道府県警察サイバー捜査官の約2,600人に含めていない。

○　人材育成

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

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

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

このほか、サイバー空間はあらゆる犯罪に悪用され得るところ、サイバ

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

なお、高度な知識・技能に係る情報処理資格である情報処理安全確保支援士の登録資格取得者数及び CISSP[1]の資格取得者数は、令和７年４月現在、それぞれ、情報処理安全確保支援士が約 700 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。）。

このように、極めて深刻な情勢が続いているサイバー空間をめぐる脅威に的確に対処するため、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の拡充が予定されており、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。

また、サイバー人材を確保・育成する取組を部門横断的に推進する必要があることから、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ることとしている。

コラム：サイバーレンジ

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を実施することで、サイバー事案への対処能力の向上を図っている。

【サイバーレンジによる捜査演習】

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

コラム：サイバーコンテスト

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「オフェンシブ・セキュリティ部門」を新たに創設した。

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特別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。

【福島県警におけるサイバーコンテストの状況】

(3)　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、資機材の整備、高度な解析技術を持つ職員の育成だけではなく、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、機械学習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を使用した簡易解析の仕組みを取り入れている。この仕組みは、全国の情報技術解析部門において活用しており、令和７年は警察庁において 5,808 件、地方機関において 591 件利用している。

【CASE：ランサムウェア「VanHelsing」の解析】

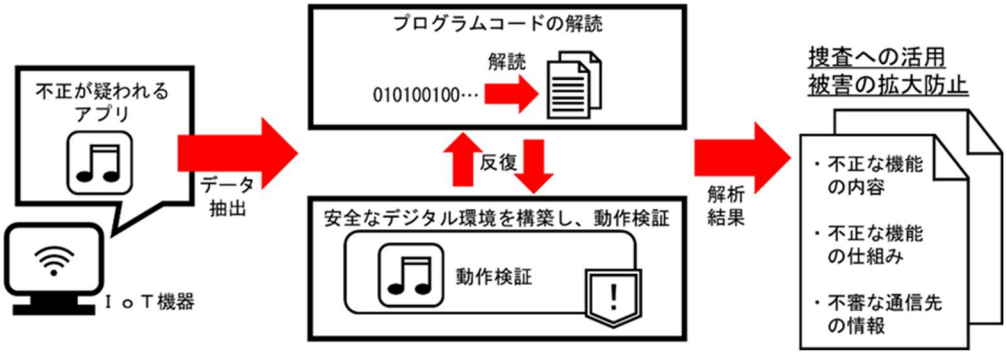
令和７年５月、警察庁情報技術解析部門は、同年３月に登場したランサムウェア「VanHelsing」のソースコードを解析し、ランサムウェアで使用されている暗号アルゴリズム、暗号化鍵の生成方法、暗号化ファイルの構造等を解明した。

コラム：不正アクセスの踏み台となる不正プログラムの解析

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（IoT 機器）について、機器の所有者の認識しないところで踏み台として悪用される事案が多発している。（34 頁参照）情報技術解析部門では、IoT 機器やプログラムを解析することで、こうしたサイバー事案の詳細な手口を調査し、被害の未然防止・拡大防止に活用している。

令和７年、警察庁情報技術解析課が IoT 機器向けの音楽配信アプリの解析を実施したところ、当該アプリには、プロキシ[18]機能等が組み込まれていることが判明したため、全国の警察にその旨周知した。この周知を踏まえ、長野県警察が、捜査中の事件に関連して IoT 機器と当該アプリを確認した結果、実際に踏み台として悪用されていたことが判明した。そこで、アプリストアに対応を要請したところ、当該アプリの配信が停止するに至った。

【不正プログラム解析の流れ】



[18] プロキシとは、ネットワーク接続を代行する機能のこと。ＩｏＴ機器がプロキシとして機能した場合、接続先には当該ＩｏＴ機器のＩＰアドレスが記録されるため、なりすましやサイバー攻撃元の匿名化に悪用される事例がある。

コラム：自動運転システムの解析に関する研究

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、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っている。

例えば、自動運転システムを搭載した車両には、車両外部との接続環境が備わっており、これらを悪用したセキュリティ侵害事案が発生した場合、重大な事件・事故につながるおそれがある。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、これらの脅威に備え、自動運転システムに関する研究を実施している。

令和７年度は、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、学術機関と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。

【自動運転システムの解析に関する研究状況】

(4)　資機材の整備

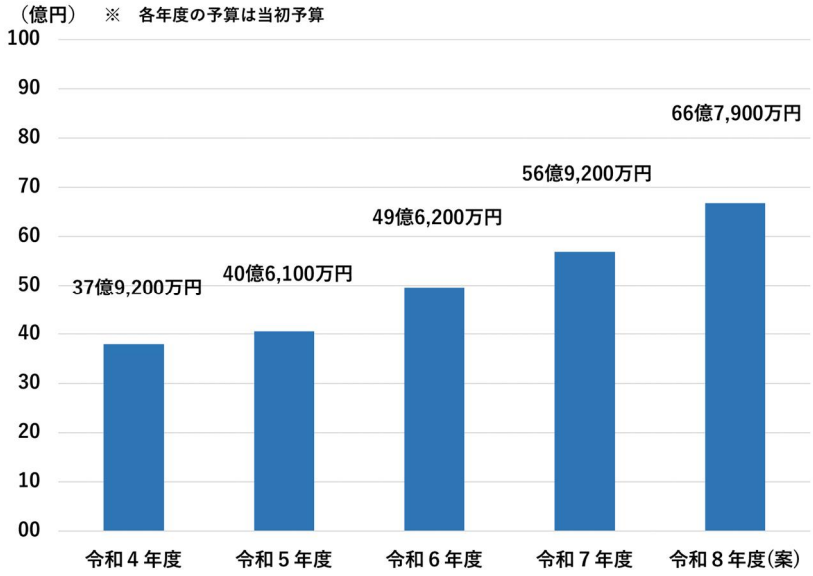
深刻化するサイバー空間の脅威に的確に対処するためには、資機材の整備・高度化が急務であることから、警察庁においては、サイバー特別捜査部を中心とした国の機関への集中的な資機材整備を推進している。例えば、匿名・流動型犯罪グループの検挙や重大なサイバー攻撃による被害の未然防止・拡大防止に寄与する資機材として、暗号資産分析ツール、サイバー捜査分析用資機材、スマートフォン解析用資機材、解析基盤装置及び高速演算装置等を整備するとともに、サイバー人材を育成するための人材育成基盤装置（サイバーレンジ）を整備しているほか、令和８年 10 月１日にアクセス・無害化措置に係る改正警察官職務執行法が施行される予定であることを踏まえ、能動的サイバー防御の実施に資する資機材等にあっても整備を進めている。

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。

なお、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（案）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、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、官民連携及び国際連携の推進に係る予算は５億 8,800 万円となっている。

【図表 53：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】



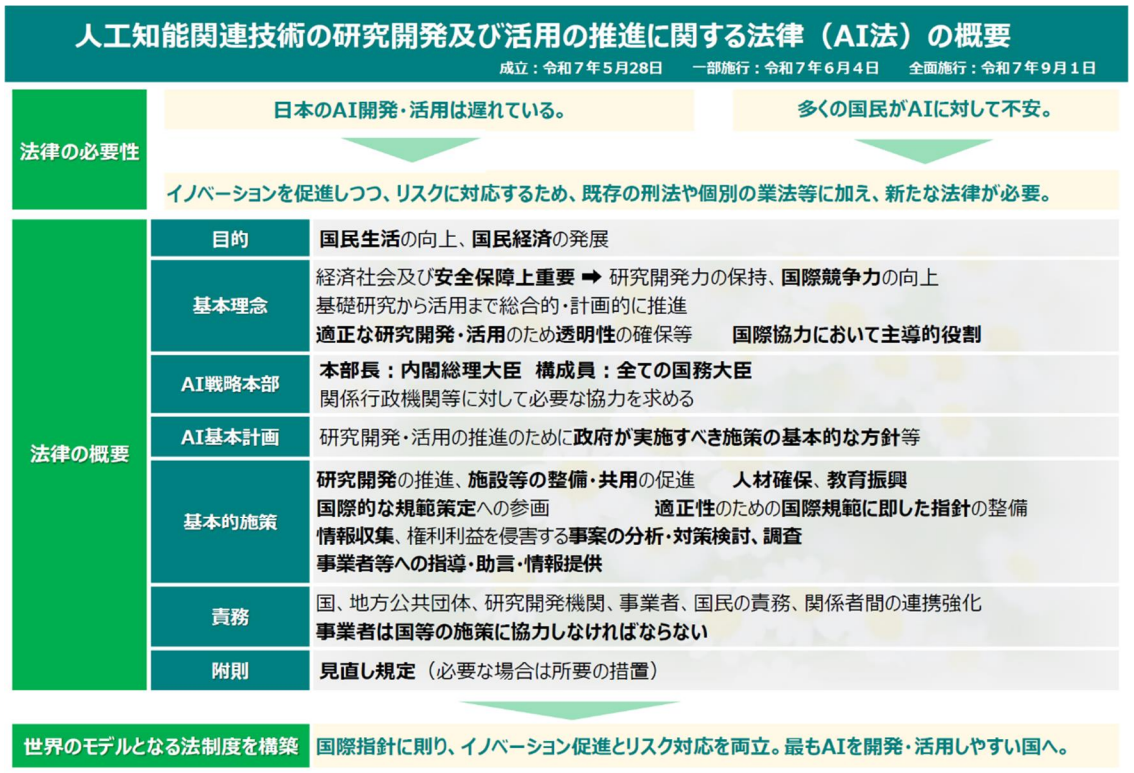
なお、トピックスⅠ「国家安全保障におけるサイバー警察の役割」で記載したとおり、サイバー攻撃は、その性質上、事案発生時点では、その攻撃主体や目的等を即座に判断できるものではなく、サイバー警察の全ての対処能力をもって判明させていくものであることから、サイバー空間の脅威への対処に係る予算は、全て、サイバー安全保障関連経費と整理されている。

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。

資料編

（「特集Ⅰ：AI をめぐる脅威の情勢と警察の取組」関連）

AI 法及び AI 基本計画・AI 指針



※　出典：内閣府

- **人工知能基本計画（令和７年 12 月 23 日閣議決定）（抄）**
  - 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。
  - 技術開発の進展とともに、ディープフェイクなど AI を悪用した問題が顕在化している。これらや国民生活への影響について、AI 法第 16 条に基づく調査研究等を実施し、リスクへの対応等を適切に行う。
  - 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や詐欺を始めとする各種の犯罪等への対応を図る。

- **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（抄）**

AI を悪用したサイバー攻撃や詐欺をはじめとする各種犯罪その他の違法行為が行われるリスクを特定・評価し、適切な対策を講じる。

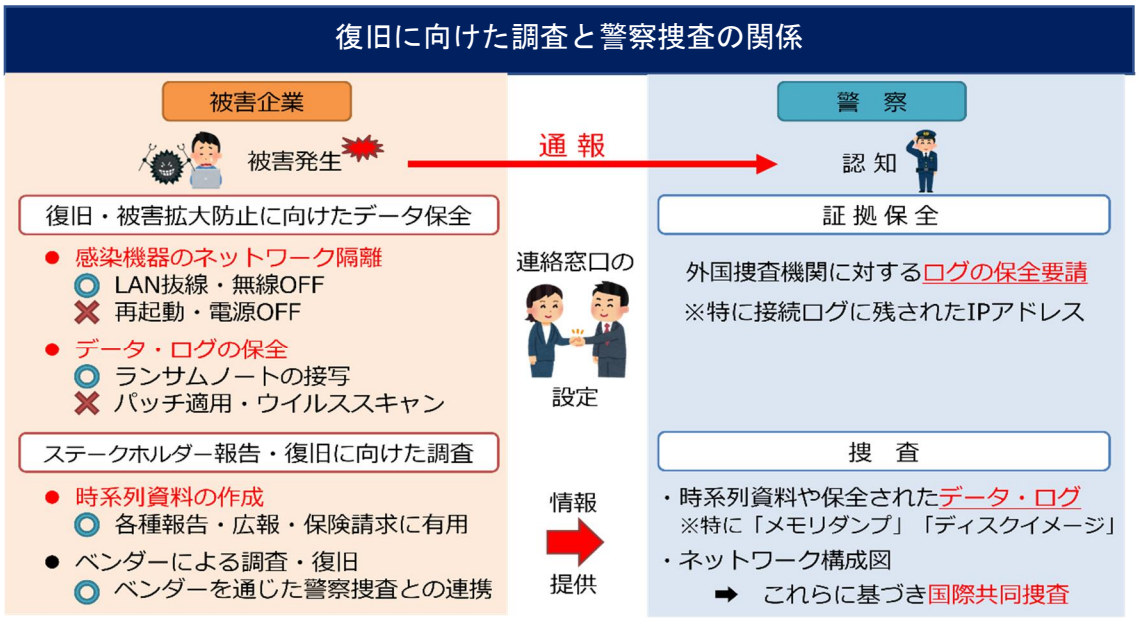
また、ハルシネーションや偏見・差別の助長、偽・誤情報等（ディープフェイク技術によるフェイク動画、性的加工画像等）の拡散等につながる AI による不適切な出力の抑制、AI の意図しない動作や誤作動の防止をするため、最新の技術と知見を駆使して、解決、改善に向けて取り組む。

（「特集Ⅰ：AIをめぐる脅威の情勢と警察の取組」関連）

令和７年におけるAIを悪用した不正アクセス事件一覧（抄）

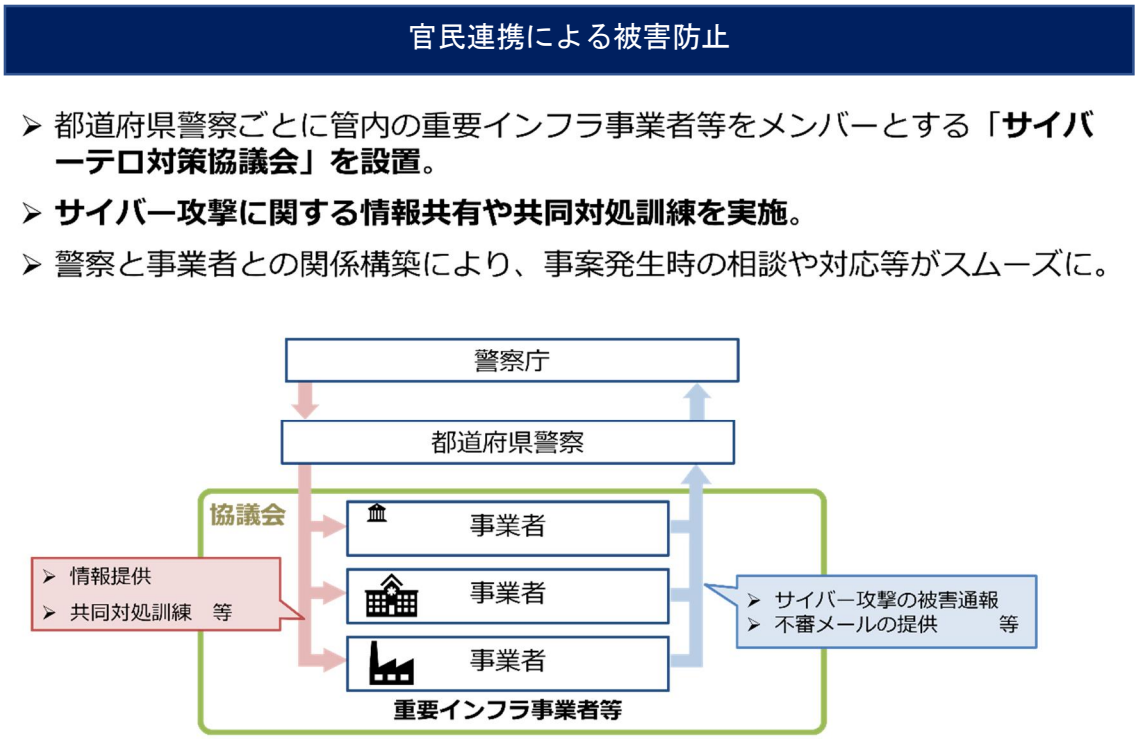
検挙年月	被疑者の属性、罪名	概要
R7.1	10代学生 電子計算機使用詐欺・不正アクセス禁止法違反	被疑者ら３名は、電気通信事業者のeSIM契約システムにぜい弱性を認め、生成AIを使用して作成した自作プログラムにより他人名義の通信回線契約を複数行った。（警視庁）
R7.8	10代学生 私電磁的記録不正作出・詐欺・不正アクセス禁止法違反	被疑者は、生成AIを使用して作成したツールでアクセス先を選定し、ネットショッピングサイトに不正アクセスして、自分の個人情報に書き換えた上で購入商品の代金返還を求めて、金券等を詐取した。（新潟）
R7.11	10代無職 不正アクセス禁止法違反	被疑者は、生成AIを使用してフィッシングサイトを作成し、銀行口座のID・パスワードを詐取した。（千葉等）
R7.12	10代無職 不正アクセス禁止法違反	被疑者は、生成AIを使用して作成した不正プログラム等でパスワードリスト攻撃を行い、不正アクセスを行って、ログイン可能なアカウントを抽出していた。（愛知）
R7.12	10代学生 偽計業務妨害・不正アクセス禁止法違反	被疑者は、複合カフェのアプリサーバに生成AIを使用して作成した攻撃プログラムで不正な指令を送信して会員情報を漏洩させ、同アプリ機能の一部の停止させる等し、同カフェ運営会社の業務を妨害した。（警視庁）
R7.12	30代無職 不正アクセス禁止法違反・割賦販売法違反・電算詐欺・組織犯罪処罰法違反事件	被疑者は、フィッシングサイトを構築する際、生成AIを使用してアップデートを繰り返し、フィッシングサイトのクオリティを高めていた。（大阪）

（「特集Ⅱ：ランサムウェアをめぐる脅威の情勢と警察の取組」関連）



<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。



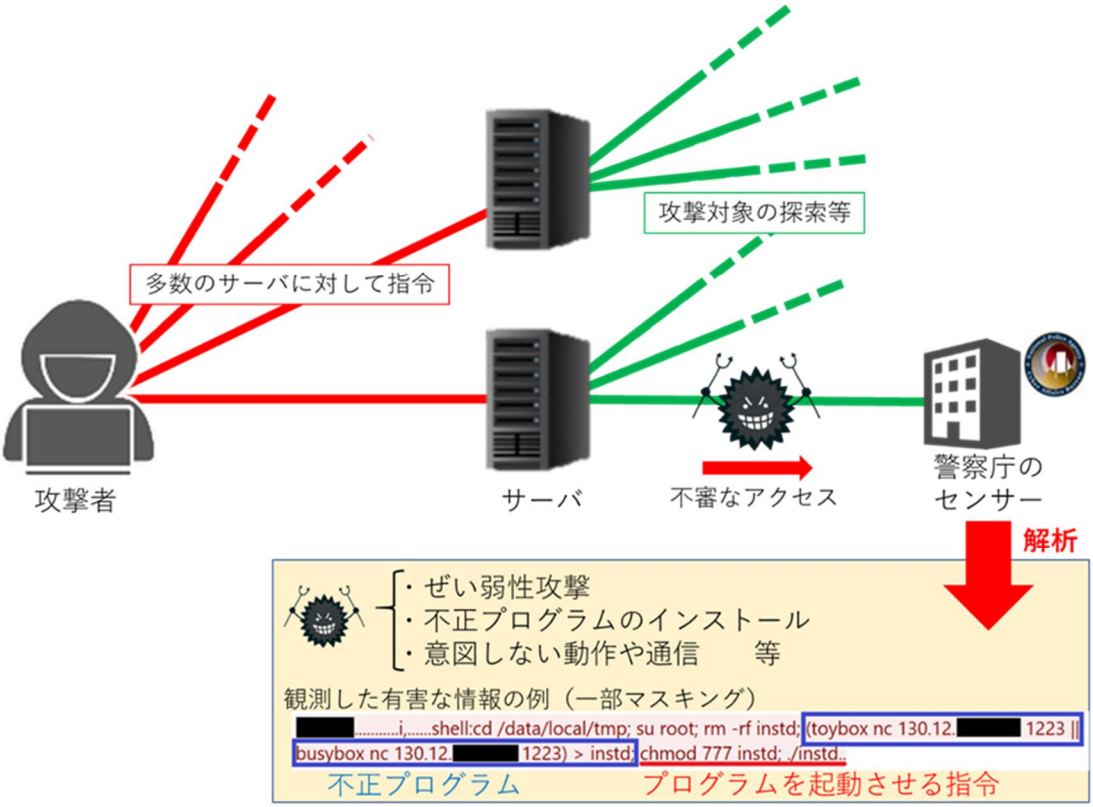
（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

警察庁が設置したセンサーによる不審な通信パケットの観測

警察庁では、インターネット上にセンサーを設置し、当該センサーに対して送られてくる通信パケットを収集している。このセンサーは、外部に対して何らサービスを提供していないため、本来であれば外部から通信パケットが送られてくることはない。このセンサーを利用することで、攻撃者が攻撃対象を探索する場合等に、不特定多数のＩＰアドレスに対して無差別に送信する、不審な通信パケットを観測することができる。

警察では、この通信パケットを分析することで、インターネットに接続された各種機器のぜい弱性の探索行為、当該ぜい弱性を悪用した攻撃、不正プログラムに感染したコンピュータの動向等を把握している。また、観測されたパケットからは送信元情報が得られるほか、ぜい弱な機器に対しマルウェアをダウンロードさせる内容が含まれている場合があり、この内容を基にダウンロードしたマルウェアを調べることで、マルウェアが通信する宛先の情報を収集することができる。収集した情報を多角的に分析することで、攻撃インフラ同士のつながりやマルウェア同士の関連性把握への活用が期待できる。

【不審な通信アクセス観測のイメージ】



（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

国別の不審なアクセス件数

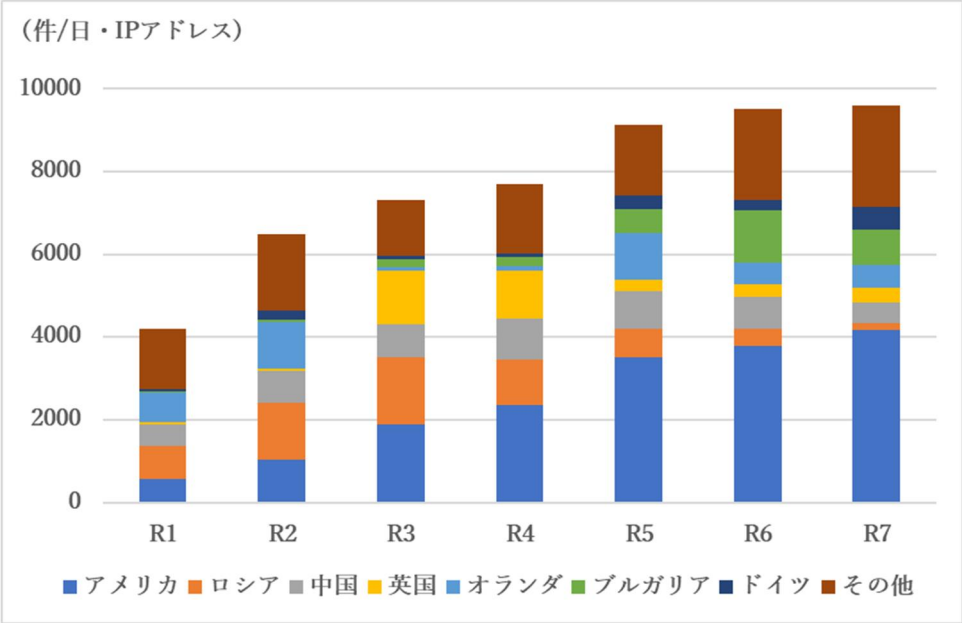
本文図表１「警察庁が検知した不審なアクセス件数」を送信元国・地域別[1]で色付けしたものが以下の図表である。

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

令和６年と令和７年を比較すると、全体としては高水準で推移しているが、ブルガリアの件数が減少している。これは、令和６年の２月から３月にかけて、ブルガリアの特定のＩＰアドレスから広範な宛先ポートに対してアクセスするといった特徴を含む大量のアクセスが観測されたためであり、令和７年については、当該アドレスからのアクセスは大幅に減少した。一方で、令和７年下半期のブルガリアの件数は増加傾向にあり、10月にはウェブサーバとの通信で利用される特定のポートを宛先とするアクセスの増加を観測した。

上記の特徴を含むアクセスはインターネット上で稼働する機器やサービスの探索を行う手段として用いられることが多く、今後も継続的に観測をしていく。

【不審なアクセス件数の国別の推移（年別、送信元国・地域別）】



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

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

令和７年における主なサイバー攻撃事例 ①

● 金融機関等に対する DDoS 攻撃被害とみられるウェブサイトの閲覧障害

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

● 保険大手企業に対するランサムウェア攻撃事案

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

● 研究開発機関に対する情報窃取目的とみられるサイバー攻撃

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

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

令和７年３月から４月にかけて、政府要人の個人ウェブサイトにおいて、DDoS 攻撃による被害とみられる閲覧障害が複数発生した。同じ頃、SNS 上に、ハクティビストのものと思われるアカウントから、それらの犯行をほのめかす投稿が確認された。

● 大手システム事業者に対する情報窃取目的とみられるサイバー攻撃

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

（第１部１「高度な技術を悪用したサイバー攻撃の脅威情勢」関連）

令和７年における主なサイバー攻撃事例 ②

● **電力事業者に対する情報窃取目的とみられるサイバー攻撃**

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

● **国際総合物流企業に対するランサムウェア攻撃**

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

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

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

● **機器製造業者に対する情報窃取目的とみられるサイバー攻撃**

令和７年６月、先端技術を有する機器製造業者は、自社で管理するサーバに不正アクセスを受け、個人情報等が漏洩した可能性があると発表した。

● **情報通信事業者に対する情報窃取目的とみられるサイバー攻撃**

令和７年７月、情報通信事業者は、ネットワーク機器に対するゼロデイ攻撃による不正アクセスを受け、個人情報等が漏洩した可能性があると発表した。

● **情報通信事業者に対する情報窃取目的とみられるサイバー攻撃**

令和７年 11 月、情報通信事業者は、クラウドサーバサービスの構築や運用に係る専用ネットワークに接続しているサーバに対して外部から不正アクセスを受け、個人情報等が漏洩した可能性があると発表した。

● **教育機関に対する情報窃取目的とみられるサイバー攻撃**

令和７年 12 月、教育機関は、外部から不正アクセスを受け、同機関が提供するメールサービスにおける個人情報等が漏洩した可能性が高いと発表した。

（第２部トピックスⅠ「国家安全保障におけるサイバー警察の果たす役割」関連）

警察におけるサイバーセキュリティ対策

巧妙化・高度化するサイバー攻撃

- ランサムウェア攻撃（試算上、R6年中で約129億円以上の調査・復旧費が発生）
- 国家を背景とした暗号資産や機密情報の窃取（R6年、約482億円相当の暗号資産が窃取）
- AIの悪用

サイバー攻撃は、その背後に国家がいることもあり、放置すれば、
サイバー安全保障の危機

警察におけるサイバーセキュリティ対策の取組

【警察におけるサイバーセキュリティ対策の取組】

① 民間事業者等との緊密な連携
② 脅威情報の収集、分析等による実態解明
③ 注意喚起、パブリック・アトリビューション等の実施
④ サイバー事案の捜査
⑤ アクセス・無害化措置の実施

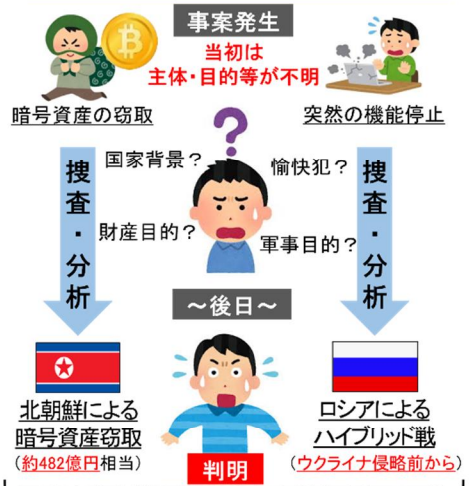
○ 高度な知見を有する人材の確保・育成
○ 先端技術を活用した対処能力の強化

【警察組織の強み】
- 全国47都道府県警による広域な情報網と捜査網
- 民間事業者等との緊密な信頼関係
- 同盟国・同志国との緊密な連携
- 捜査権を有する組織としてサイバー捜査を実施

巧妙化・高度化するサイバー攻撃の抑止のため、警察が、計画的・安定的に上記対策を推進し、サイバー攻撃への対処能力を継続して強化・高度化することが不可欠

サイバー空間の脅威への対処

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が含まれている

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

警察の取組

官民連携
- ○ 平素からの民間事業者等との情報共有や広報啓発活動等

～サイバー攻撃の発生～

捜査
- ○ 被害事業者等からの通報・相談
- ○ 実態解明による潜在的な被害の発掘
- ○ 外国治安機関等との国際共同捜査

情報の収集・分析／実態解明
- ○ 脅威情報の収集・把握及び当該情報を多角的・総合的に分析
- ○ 国家の関与、攻撃インフラ等の解明

これらの活動により、初めて国家の関与が特定

注意喚起／PA
- ○ 注意喚起、パブリックアトリビューション（PA）等の実施

アクセス・無害化措置
- ○ アクセス・無害化措置の実施

※ 攻撃手段の高度化を受け、今後は、「AI」等の先端技術を活用した対処能力の高度化等が必須

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

（第２部トピックスⅠ「国家安全保障におけるサイバー警察の果たす役割」関連）

国家安全保障戦略（令和４年 12 月 16 日）（抄）

【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。

（第２部トピックスⅠ「国家安全保障におけるサイバー警察の果たす役割」関連）

サイバー対処能力強化法

法の全体像

6

- 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

P7 総　則 ◻ 目的規定、基本方針等（第１章）

P8 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））

P11 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）

P16 ◻ 分析情報・脆弱性情報の提供等（第８章）

P18 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）

P21 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

施行期日 P22 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

■　本手続について、国家サイバー統括室が国家安全保障局と連携しつつ総合調整（警察・自衛隊の役割分担等）

国家安全保障会議（4大臣会合※）
要請を受けた警護の実施判断に関する審議
※サイバー安全保障担当大臣・国家公安委員会委員長も参加
← 米軍からの警護の要請

重大なサイバー攻撃の発生・予兆の認知（平素よりサイバー攻撃や脅威の情勢等の情報を集約・分析）

1 国外への対処の場合・国内への対処であって国家安全保障に関わる場合
2 自衛隊又は在日米軍が使用するコンピュータを警護する場合
3 国内への対処であって国家安全保障に関わらない場合

国家安全保障会議（4大臣会合※）　対処方針を審議
※　サイバー安全保障担当大臣・国家公安委員会委員長も参加

警察・自衛隊による共同対処を実施することとされた場合
→ 国家公安委員会からの要請又は同意
→ 国家安全保障会議（9大臣会合※）・閣議（※サイバー安全保障担当大臣も参加）
→ 内閣総理大臣による通信防護措置命令

警察単独で対処することとされた場合

自衛隊単独で実施

警察単独で実施

外務大臣との協議（国外のコンピュータを対象とする場合等）

サイバー通信情報監理委員会への申請と承認（いとまがない場合は事後通知）

アクセス・無害化措置（※1）

措置の対象としたコンピュータの管理者への通知（※2）

対処終了

実施した措置（1 2）については適時に国家安全保障会議に報告

（※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除く。

出典：内閣官房

改正警察官職務執行法（抄）

【改正警察官職務執行法（抄）】

（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理委員会の承認を得なければならない。ただし、当該加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、当該確認の結果に基づき、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。

改正自衛隊法（抄）

【改正自衛隊法（抄）】

（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をいう。次号において同じ。）が生ずるおそれが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。

三　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十一項までの規定は、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。

（第２部トピックスⅠ「国家安全保障におけるサイバー警察の果たす役割」関連）

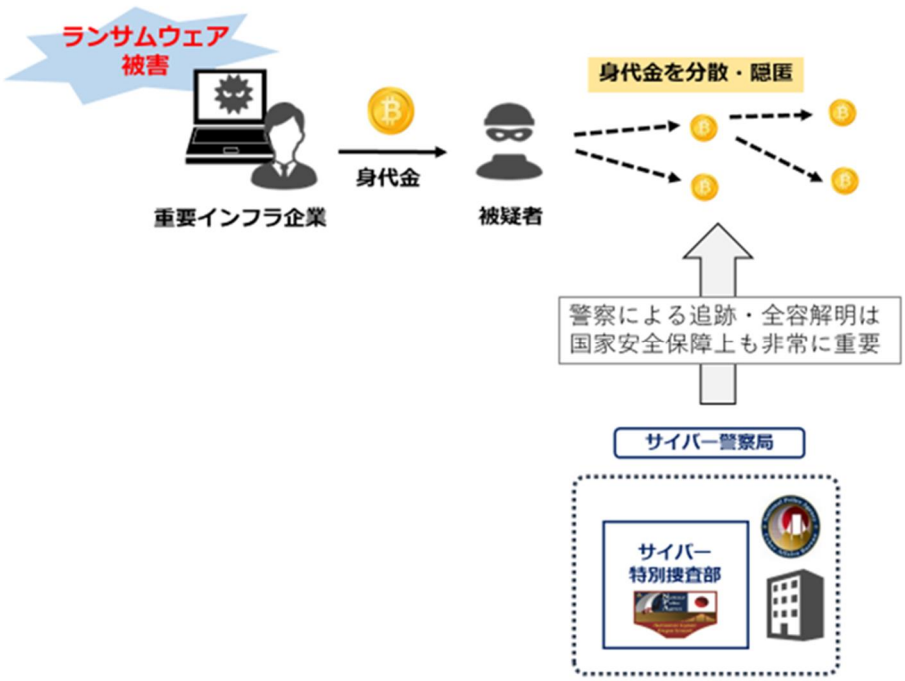
安全保障上の脅威に対する暗号資産追跡の重要性

令和３年（2021年）５月、米国最大手の石油パイプライン企業のシステムがロシアを拠点とするランサムウェアグループ「DarkSide」によるランサムウェア攻撃を受け、パイプラインの操業を６日間停止する事態となり、市民生活に大きな影響を与えた。

当該被害企業は、ランサムウェアグループに対して身代金として約75ビットコインを支払ったものの、同年６月、米国司法省は、支払われた身代金のうち約63.7ビットコイン（当時約230万ドル相当）を被疑者側のウォレットから押収したことを公表した。

ランサムウェアグループ「DarkSide」は、被害企業が支払った身代金を、複数の暗号資産アドレスを経由して分散するなどして隠匿していたが、FBI等が身代金の移転状況を追跡することで、その一部について特定・押収に至ったものである。日本警察においても、本事案について独自にその移転状況を分析しており、身代金の移転を解明している。

このように、重要インフラに対するサイバー攻撃は、国家安全保障上の深刻な脅威であるところ、暗号資産の移転状況を追跡することは、犯罪捜査だけでなく、安全保障上の脅威を解明する上でも必要不可欠な取組である。警察では、犯罪捜査はもとより、国家安全保障という観点からも、サイバー特別捜査部を中心に、暗号資産追跡能力の向上に努めている。



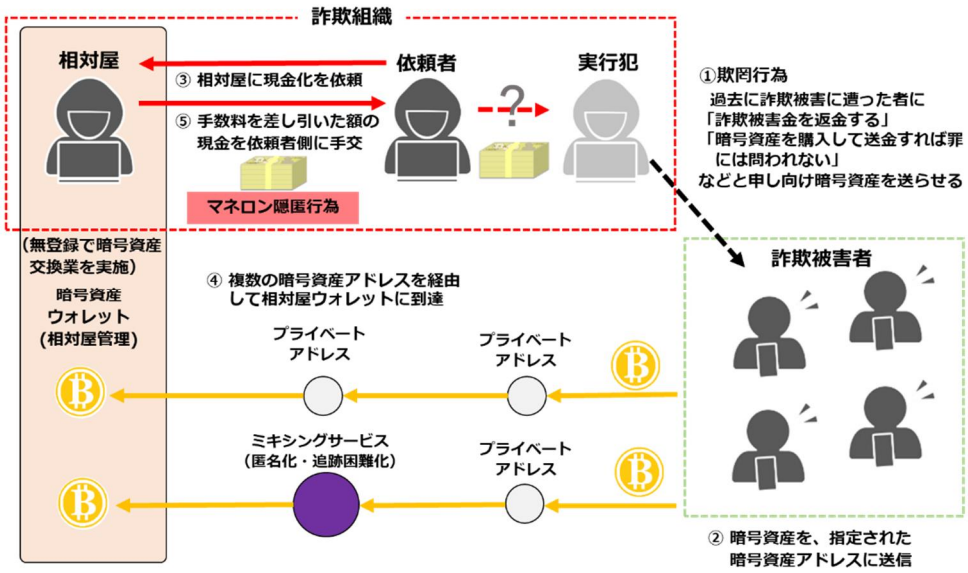
（第２部トピックスⅡ「サイバー空間の匿名性の打破に向けた取組」関連）

サイバー空間の匿名性を悪用した「相対屋」の検挙

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「相対屋（あいたいや）」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）

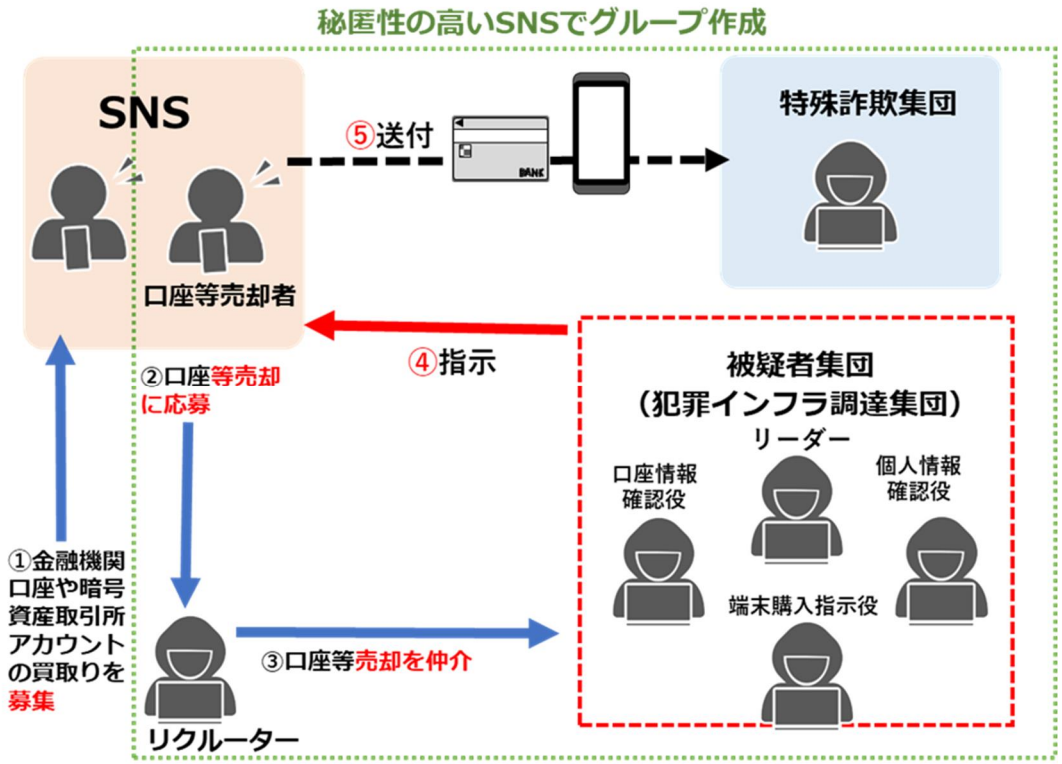
本件においては、特殊詐欺の被害金である暗号資産の移動に、匿名性を高める「ミキシングサービス」が利用されていたところ、サイバー特別捜査部の高度な分析により、被疑者名義のアカウントに被害金が流れていることを解明し、当該アカウントを都道府県警察からサイバー特別捜査部に集約された情報と照合することで、他県での被害との関係性を浮き彫りにするなど、事件構図の解明に貢献した。



（第２部トピックスⅡ「サイバー空間の匿名性の打破に向けた取組」関連）

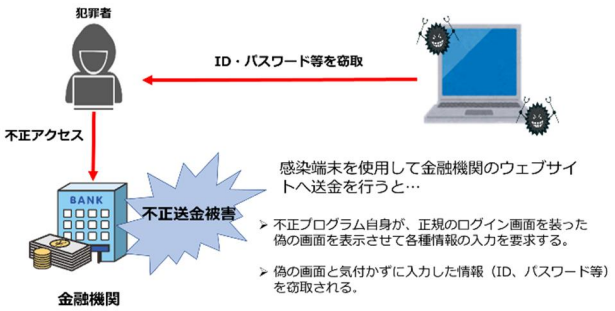
サイバー空間の匿名性を悪用した「道具屋」の検挙

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（なりますまし目的・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）。



サイバー警察局設置前における国際共同捜査の主な事案一覧 ①

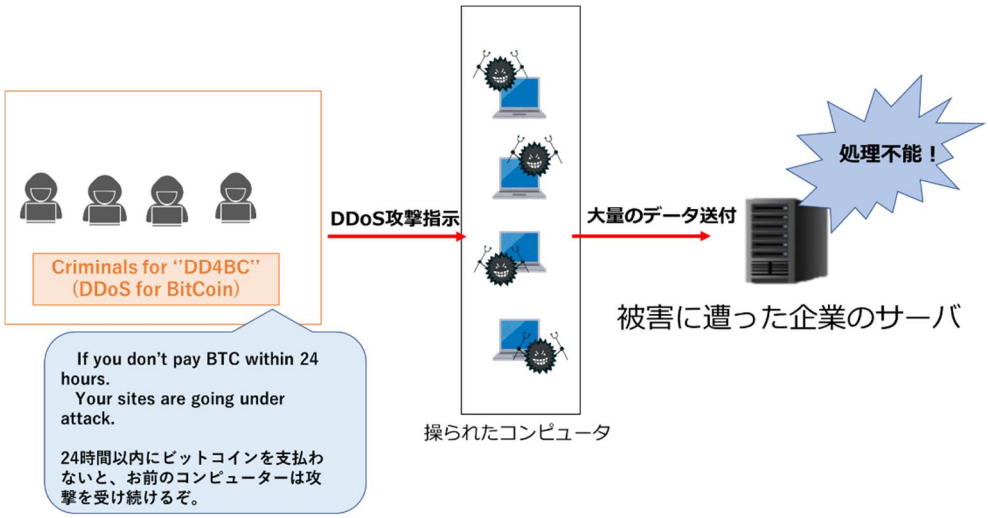
● 国際的なボットネットを利用した不正送金事案



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。

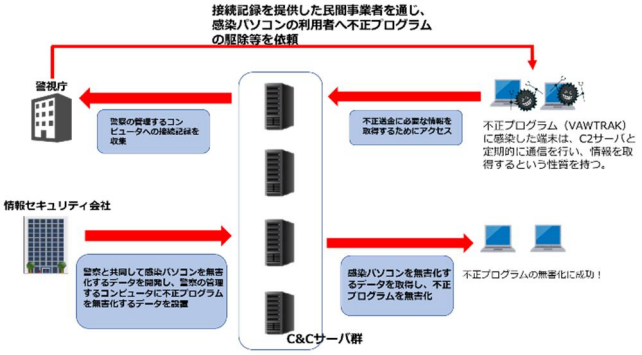


サイバー警察局設置前における国際共同捜査の主な事案一覧 ②

● 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

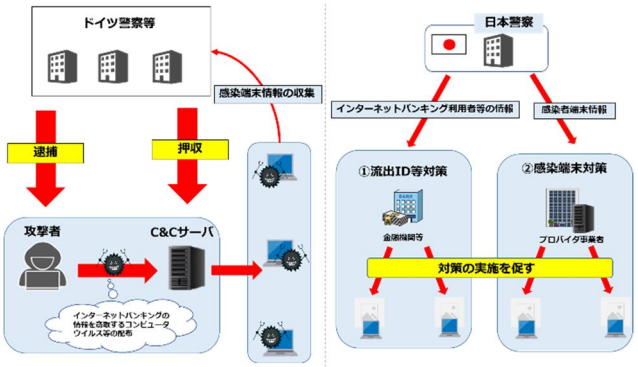
平成 27 年４月、警視庁は、インターネットバンキングに係る不正送金事犯に利用されるＣ２サーバの動作を観測することにより、国内外において約８万 2,000 台の端末が不正プログラム「VAWTRAK（ボートラック）」に感染していることを把握し、不正プログラムによる被害の拡大防止措置を実施した。警視庁は、プロバイダを通じた国内の感染端末の利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供に加え、被害拡大防止措置として、不正プログラムの無害化措置の実施にも成功した。

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



● 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。

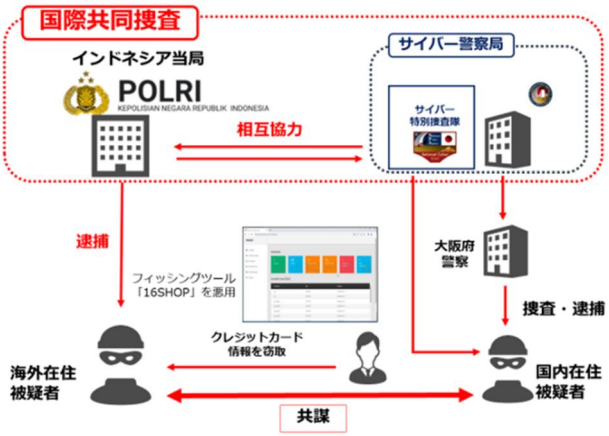


（第２部１「検挙に向けた取組」関連）

サイバー警察局設置後における国際共同捜査の主な事案一覧 ①

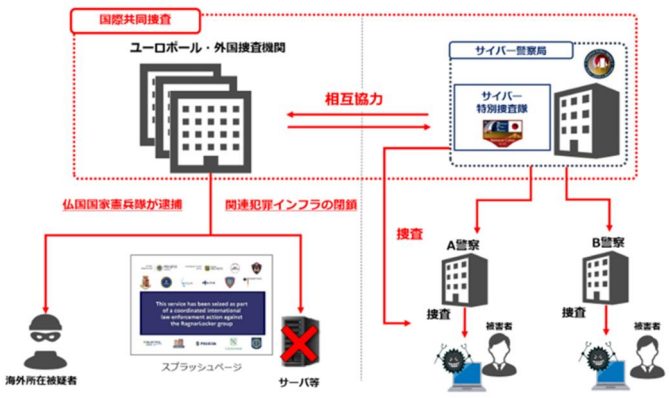
● 「16SHOP」を用いたクレジットカード情報不正取得・利用事案

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

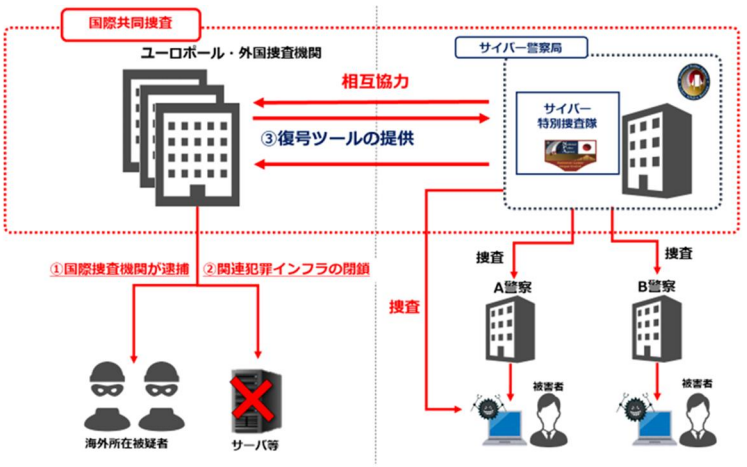
ランサムウェア攻撃グループ「Ragnar Locker」に係る国際共同捜査「オペレーション Talpa（タルパ）」においては、サイバー特別捜査隊（当時）等による国内捜査により得られた情報を関係国捜査機関等に提供するなどした結果、令和５年（2023 年）10 月、関係国捜査機関により「Ragnar Locker」の開発者であると考えられている被疑者が逮捕されたほか、同グループが使用するサーバ等の犯罪インフラがテイクダウン（機能停止）された。テイクダウンに当たっては、同グループが使用していたリークサイト上に、テイクダウンの実施を告げるスプラッシュページが表示された。同ページには、我が国を含む関係国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の主な事案一覧 ②

● 「LockBit」によるランサムウェア攻撃事案

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



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

【スプラッシュページ】

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

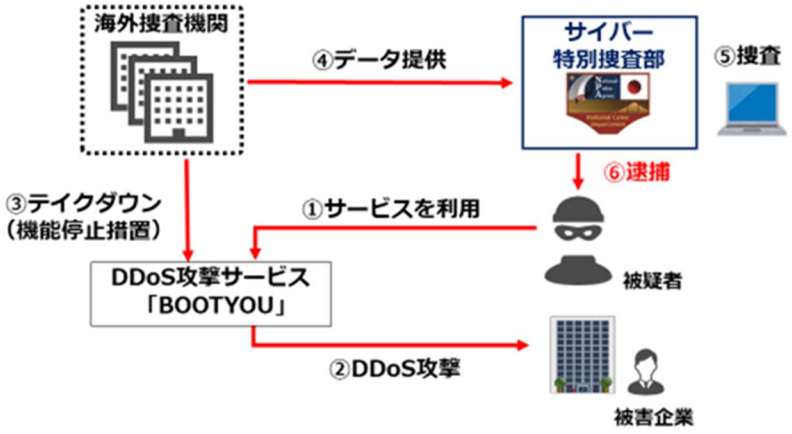
（第２部１「検挙に向けた取組」関連）

サイバー警察局設置後における国際共同捜査の主な事案一覧 ③

● 海外の DDoS 攻撃ウェブサービスを利用した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。

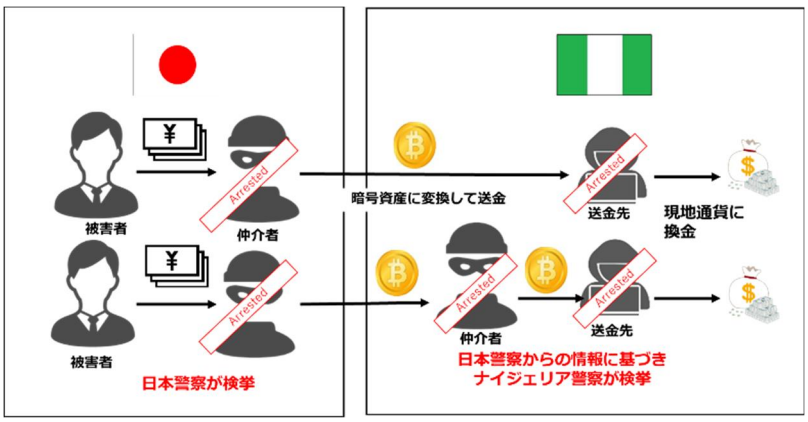
また、令和６年 12 月には、本国際共同捜査の一環として実施された広報啓発キャンペーンに参画した。



● 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の主な事案一覧 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。

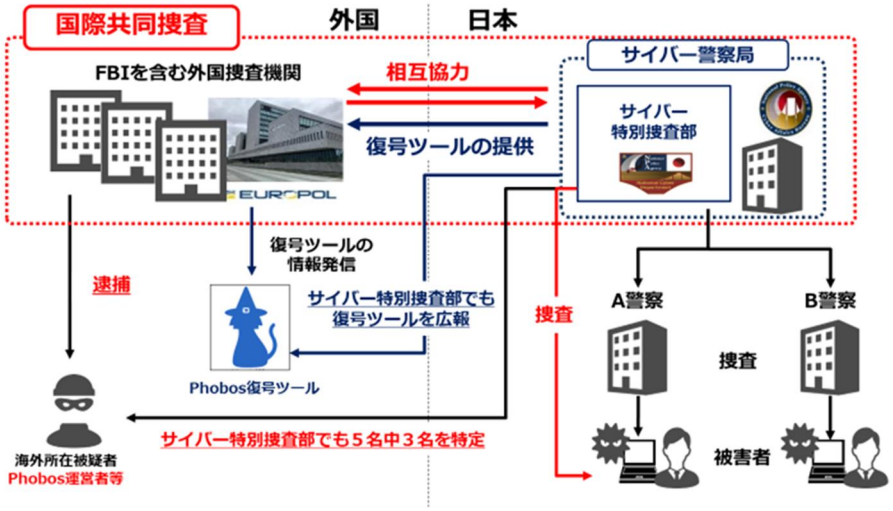
令和６年 11 月、米国は、「Phobos」グループの運営者とみられるロシア人の男（42）を起訴したことを発表したほか、令和７年２月、米国及びスイスは、「Phobos」の関連組織である「８Base」グループ運営者等とみられる男ら４名を検挙したことを発表した。

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

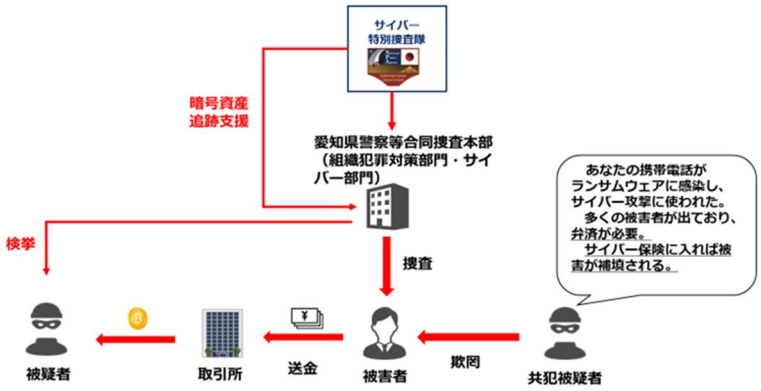


（第２部１「検挙に向けた取組」関連）

サイバー特別捜査部等合同捜査本部による国内における主な捜査事例①

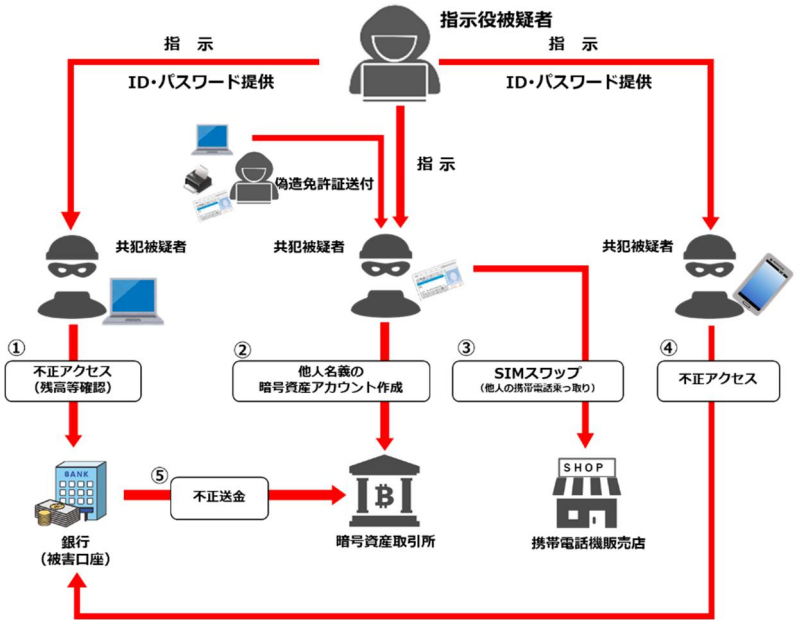
● サイバー保険名目の架空料金請求詐欺事案

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等合同捜査本部による国内における主な捜査事例②

●　クレジットカード不正利用事案

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

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

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

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

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

パブリック・アトリビューションの事例一覧 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。

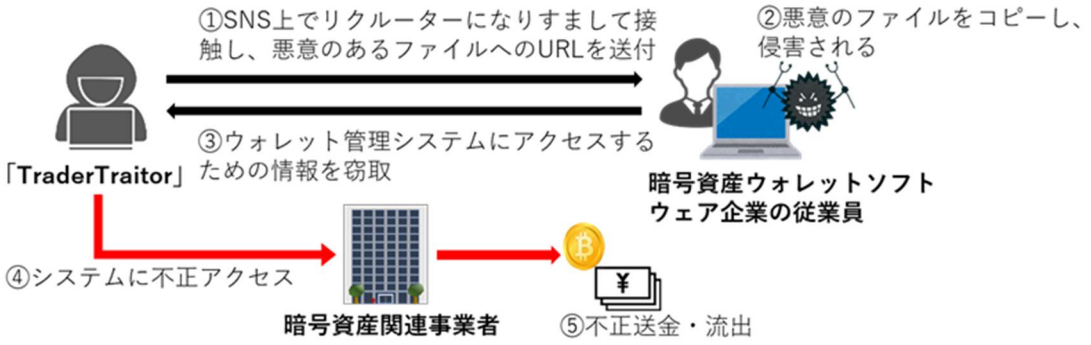
パブリック・アトリビューションの事例一覧②

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

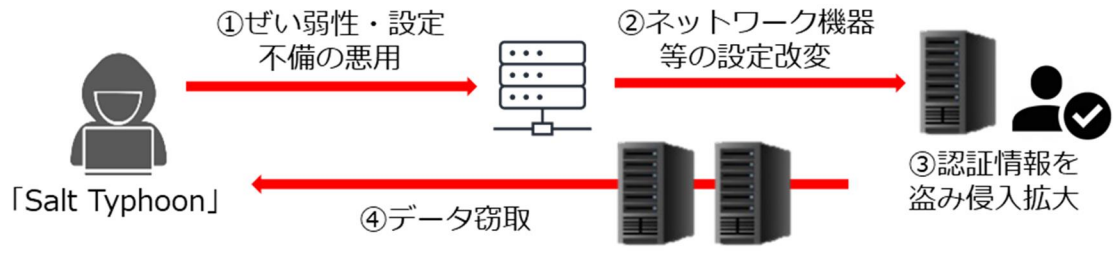
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー警察局設置後のサイバー攻撃に対する主な注意喚起 ①

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



● 中国を背景とするサイバー攻撃グループ Salt Typhoon は、ネットワーク機器等に存在する既知のぜい弱性や機器の設定不備を悪用し、初期アクセスを確立する。次に、ネットワーク機器の設定等を改変することで攻撃対象ネットワークへの永続的なアクセスを維持する。さらに、侵入を拡大するために、攻撃対象ネットワーク内部のアクセス認証に関する情報を狙い、最終的にはデータ窃取まで実行する。



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー警察局設置後のサイバー攻撃に対する主な注意喚起 ②

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

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

● 家庭用ルーターの不正利用に関する注意喚起

令和５年３月、警察庁及び警視庁は、捜査の過程で、家庭用ルーターがサイバー攻撃に悪用されており、従来の対策のみでは対応できないことが判明したことから、複数の関係メーカーと協力し、官民一体となって注意喚起を実施した。

● DDoS 攻撃に関する注意喚起

令和５年５月、警察庁は、NISC と連名で、重要インフラ事業者等のウェブサイトへの DDoS 攻撃に関する注意喚起を行い、令和４年９月に発生した国内の政府関連や重要インフラ事業者等のウェブサイトに対する一連の DDoS 攻撃に関する分析結果を示すとともに、リスク低減に向けたセキュリティ対策の実施を呼び掛けた。

● サイバー特別捜査隊をかたる不審メールに関する注意喚起

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

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー警察局設置後のサイバー攻撃に対する主な注意喚起 ③

● 豪州主導国際文書「OT サイバーセキュリティの原則」への共同署名

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

● MirrorFace によるサイバー攻撃に関する注意喚起

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

● 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

令和７年 10 月、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」（“Foundations for modern defensible architecture”）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した。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

DDoS 攻撃対策に関する注意喚起

ＤＤｏＳ攻撃対策のお願い

警察庁
National Police Agency
令和7年12月

- 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<u>DDoS攻撃対策の設定の再確認</u>**
  - ・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<u>冗長化</u>**
- **<u>本社・支社使用のIoT機器の再確認</u>**（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

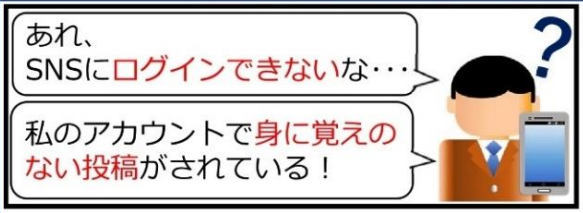
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

アカウントの乗っ取りに関する注意喚起

サイバー警察局便り

Cyber Police Agency Letter 2025 Vol. 5 (R7.8)

SNS等の アカウントの乗っ取りに警戒を!!



ちょっと待って！
アカウントが乗っ取られていませんか？

令和６年に検挙した不正アクセス禁止法違反の手口別検挙件数のうち、
・パスワードの設定・管理の甘さにつけ込んで入手（34.1%）
・利用権者(※)からの聞き出し、のぞき見（10.0%）
などが多くみられました。以下、対策ができているかチェックしましょう！
※当該アカウントの利用について、サービス提供者等から許諾を得た利用者

アカウント乗っ取り防止・早期発見のためのチェック項目

- ☐ 短くて簡単なパスワードにしていませんか？
- ☐ 同じパスワードを他のアカウントでも使っていませんか？
- ☐ 誰かにパスワードを教えていませんか？
- ☐ 多要素認証を設定していますか？
- ☐ ログイン通知を有効化していますか？

もしもアカウントを乗っ取られたら

- ☐ ログインできる場合は、パスワードを変更し、見覚えのない端末を全てログアウトする
- ☐ サービス提供会社に相談する
- ☐ 友人・フォロワー等に注意喚起する
- ☐ **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

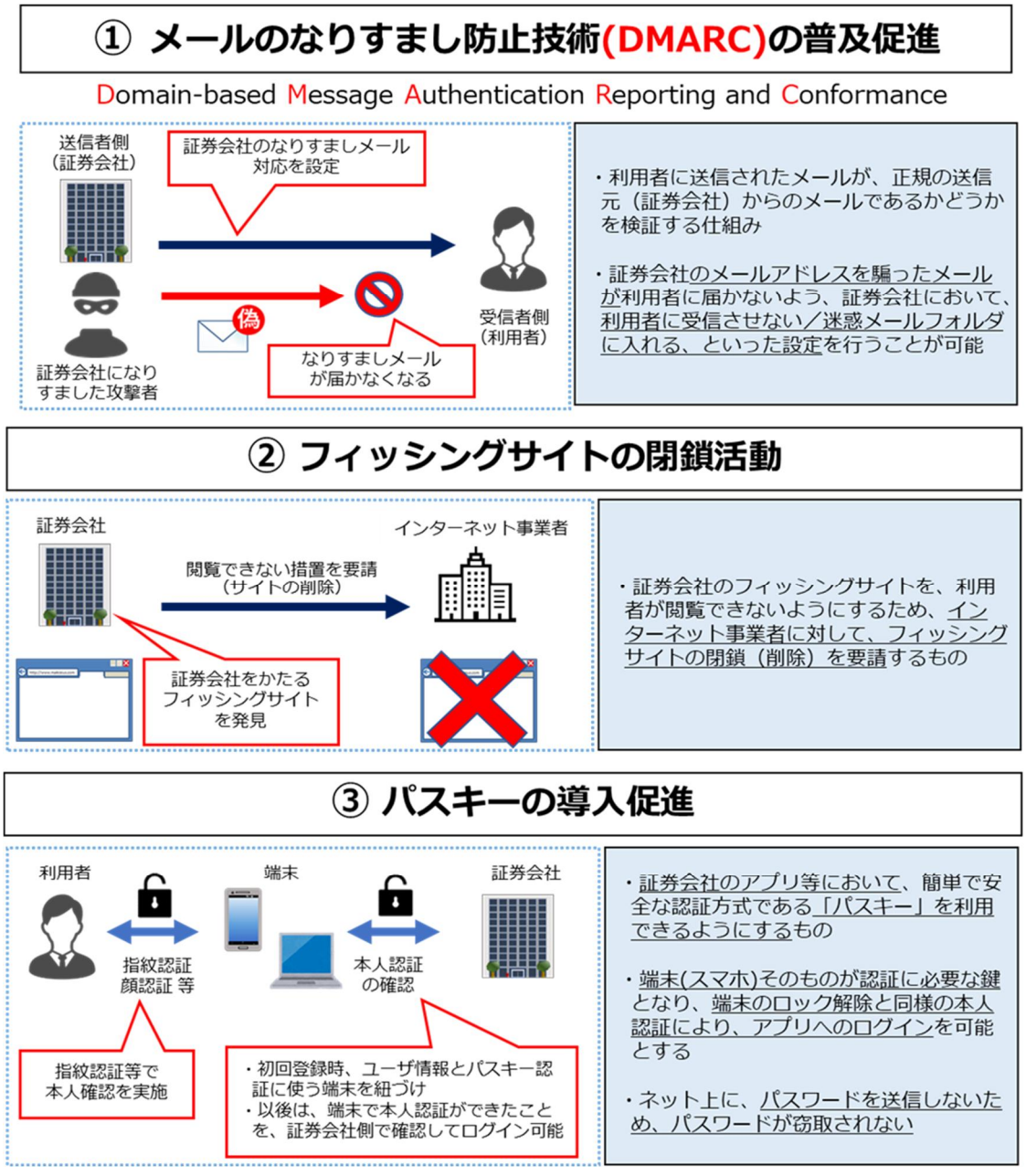
★詳しくは、警察庁HP「基本的なセキュリティ対策」「不正アクセス対策」等を参照してください。 https://www.npa.go.jp/bureau/cyber/index.html

警察庁
National Police Agency

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

日本証券業協会等に対する不正アクセス・不正取引対策の要請

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



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

メールのなりすまし防止技術（ＤＭＡＲＣ）について

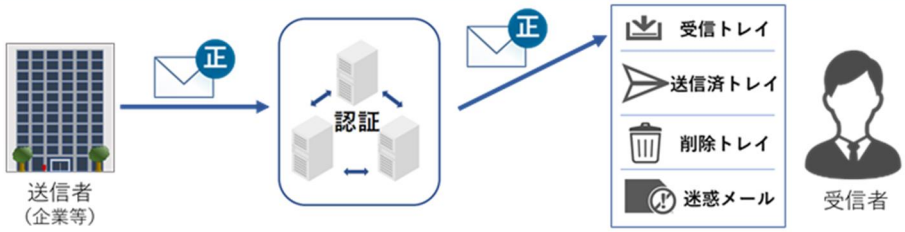
Domain-based Message Authentication Reporting andConformance

ＤＭＡＲＣとは･･･

- 実在する企業等を装って送信されるなりすましメールの受信を防ぐための認証技術で、受信者に送信されたメールが、正規の送信元からのメールであるかどうかを検証する仕組み
- 事前に送信者側において、受信者側で認証に失敗したなりすましメールをどう処理するか設定することができる（ＤＭＡＲＣポリシーの設定）
- 設定内容は、そのまま受信（Ｎｏｎｅ）、隔離（Ｑｕａｒａｎｔｉｎｅ）、拒否（Ｒｅｊｅｃｔ）の３態様

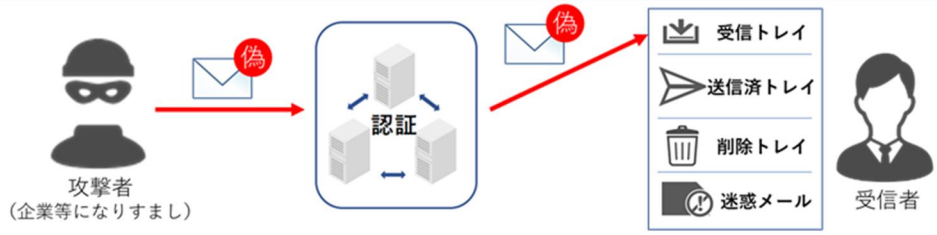
★ＤＭＡＲＣを導入した企業等（送信者側）

➡ 企業等が送信した正規メールは受信者側で認証に成功し、受信者に届く



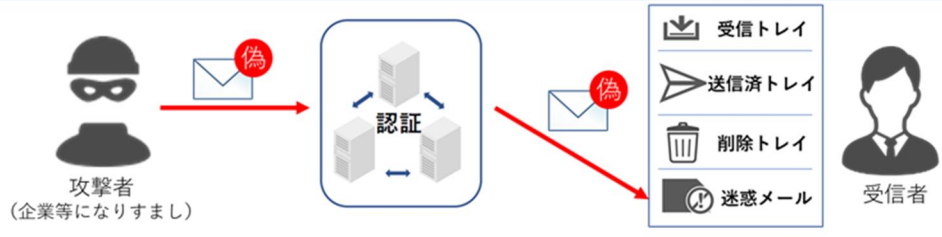
●送信者側のＤＭＡＲＣを「そのまま受信（Ｎｏｎｅ）」に設定

➡ 企業等のなりすましメールは受信者側で認証に失敗するが、設定に基づき、そのまま受信者に届く



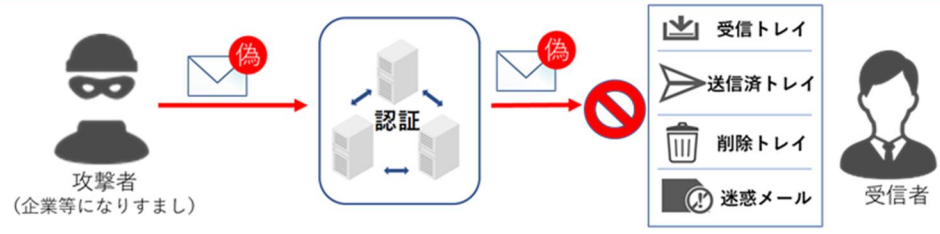
●送信者側のＤＭＡＲＣを「隔離（Ｑｕａｒａｎｔｉｎｅ）」に設定

➡ 企業等のなりすましメールは受信者側で認証に失敗し、受信者の迷惑メールフォルダに隔離



●送信者側のＤＭＡＲＣを「拒否（Ｒｅｊｅｃｔ）」に設定

➡ 企業等のなりすましメールは受信者側で認証に失敗し、受信が拒否され受信者に届かない



（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

国民を詐欺から守るための総合対策 2.0

「国民を詐欺から守るための総合対策2.0」における主な施策

1 SNS型投資・ロマンス詐欺対策 ／ 2 特殊詐欺対策

（１） 犯行準備段階への対策

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

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

（２） 着手段階への対策

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

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

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

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

（３） 欺罔段階への対策

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

（４） 金銭等の交付段階への対策

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

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

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

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

（５） 犯行後の捜査段階における対策

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

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

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

3 ID・パスワード等の窃取・不正利用対策

（１） フィッシングサイトへの対策

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

（２）・(3) ID・パスワードやクレジットカード情報の不正入手・利用対策

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

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

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

（５） 犯行後の捜査段階における対策

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

4 治安基盤の強化等

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

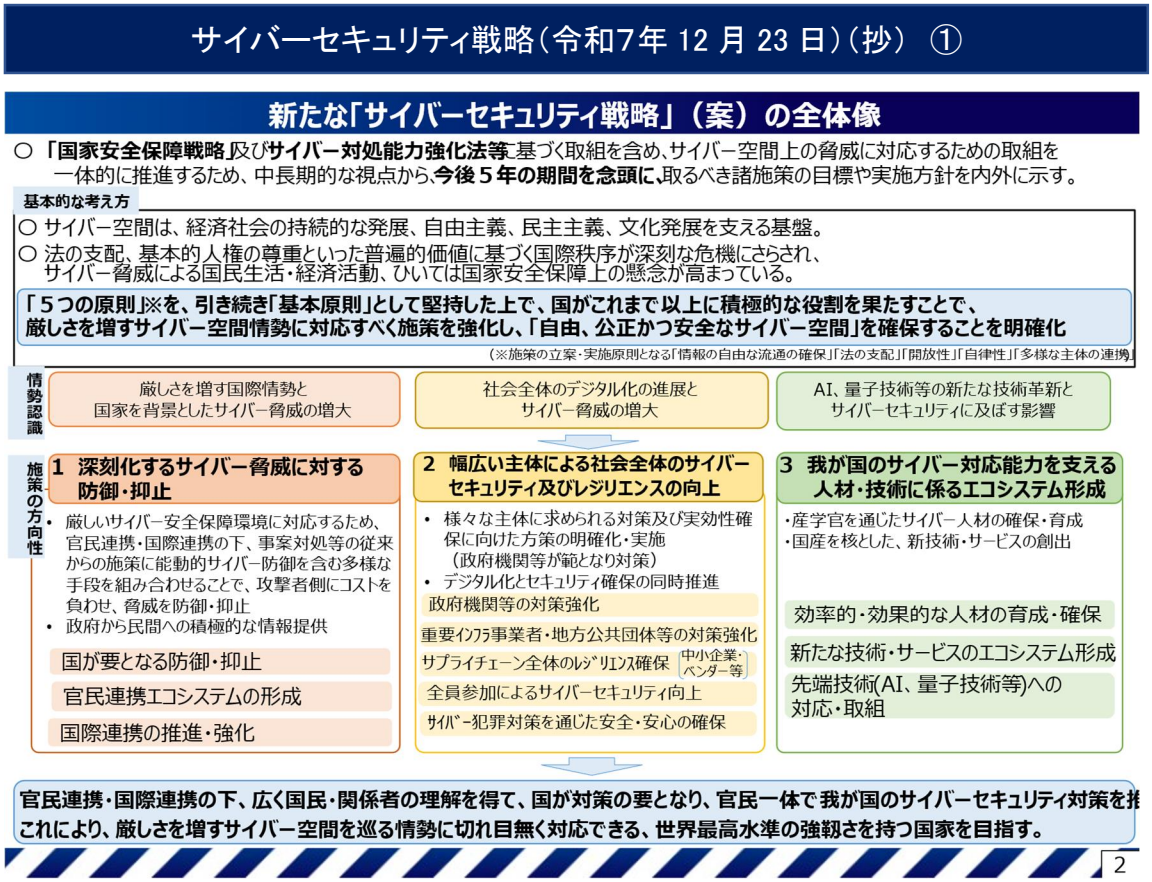
○ スマートフォン端末等の解析能力の強化、捜査に必要な情報収集の効率化のため、警察・検察の装備資機材の充実強化を推進。

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

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

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

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）



【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

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】

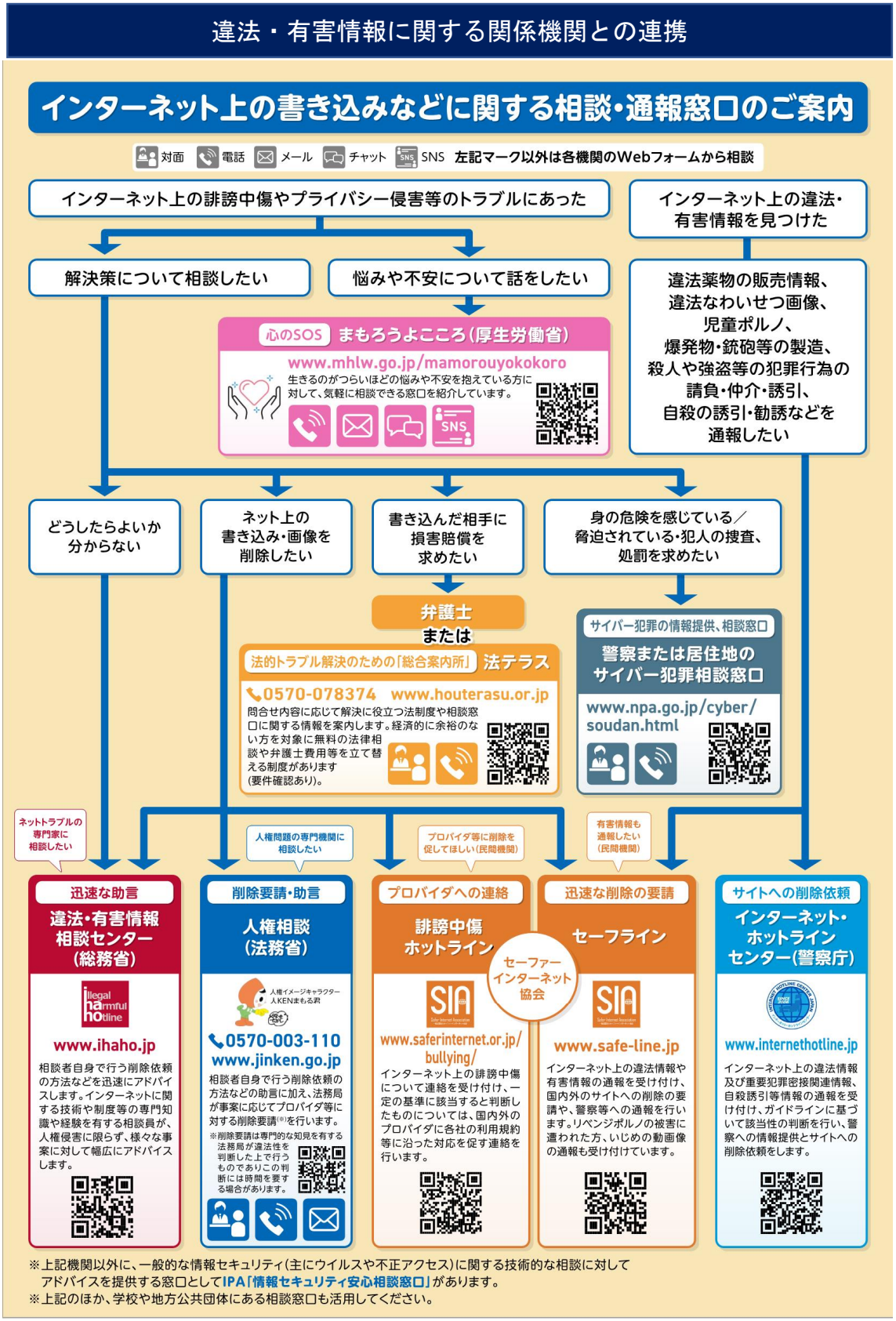
サイバー空間が、あらゆる主体が参画する公共空間へと進化していることを踏まえ、実空間と変わらぬ安全・安心を確保するため、国は、暗号資産、SNS 等のサイバー空間の匿名性を悪用する犯罪者や犯罪者グループ、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

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。


違法・有害情報に関する関係機関との連携
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にアドバイスします。
削除要請・助言
人権相談（法務省）
人権イメージキャラクター人KENまもる君
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(※)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
セーファーインターネット協会
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、いじめの動画像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。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

情報流通プラットフォーム対処法に係る広報啓発

サイバー警察局便り

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

大規模プラットフォーム事業者が提供するＳＮＳや動画投稿サイト等について

誹謗中傷等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

引用元：総務省ウェブサイト

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）、MetaPlatforms,Inc（Facebook、Instagram、Threads）等）　（総務省ウェブサイト）

※　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（令和３年法律第137号）

警察庁 National Police Agency

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

インターネット・ホットラインセンターの変遷

年　月	概　要
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。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

政府広報におけるランサムウェア注意喚起

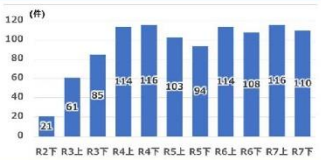
サイバー警察局便り

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/

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

政府広報オンライン動画一覧

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も慌てないで！
「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

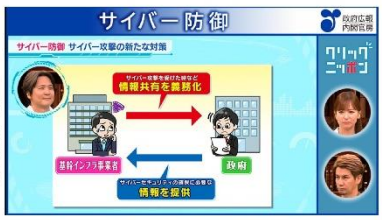
サイバーセキュリティ

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-portal.cyber.go.jp/cybersecuritymonth/2026/

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指示。

サイバー人材の確保

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

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

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

サイバー人材の育成

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

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

サイバー人材のキャリアパス管理

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

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

上記方針に基づき本部長の指揮の下すべての都道府県警察が施策を推進

情報通信部門におけるサイバー人材確保・育成方針

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

サイバー人材の確保

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

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

サイバー人材の育成

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

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

サイバー人材のキャリアパス管理

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

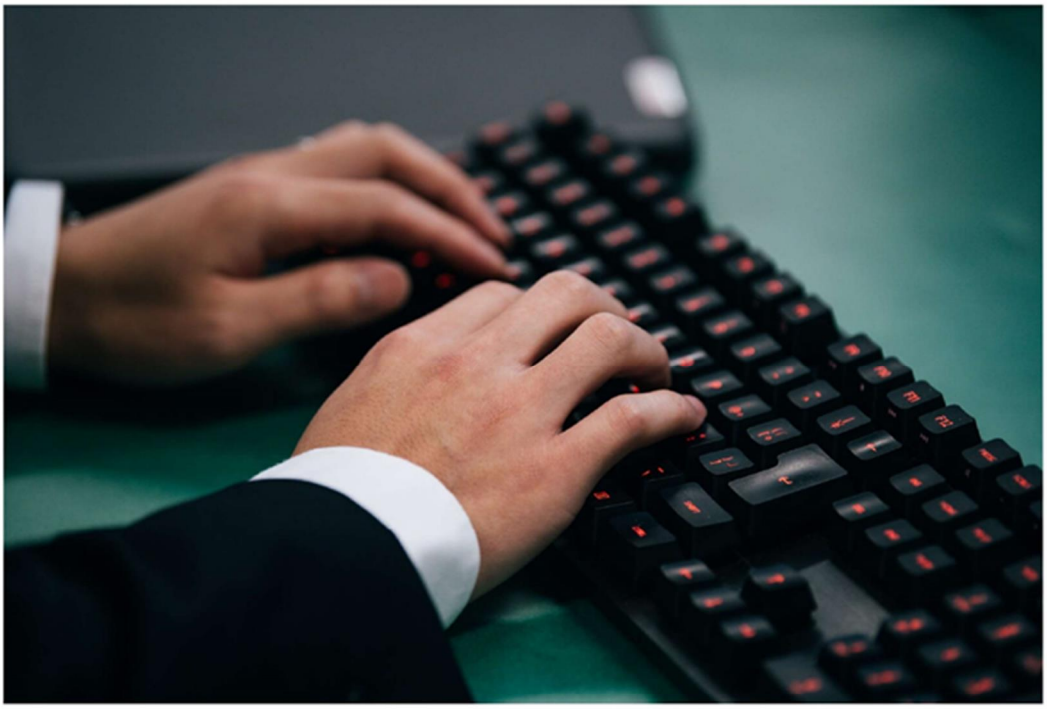
2　キャリアパス管理に基づく職員の配置等
- ✓ 高度サイバー人材については能力をいかせるポストへの配置に配意
- ✓ ハイブリッド人材育成の観点から都道府県警察サイバー部門に積極的に出向、情管への出向も検討
- ✓ 警察庁サイバー警察局・サイバー特別捜査部に長期勤務も念頭に配置、特に優秀な者については幹部ポストに登用

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

（第２部３「基盤整備」関連）

サイバー人材の確保・育成 ②

サイバー犯罪捜査官(都道府県警察)・技術職員(警察庁)募集



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

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

そこで、警察では、

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

サイバー警察局サイト

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

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

（第２部３「基盤整備」関連）

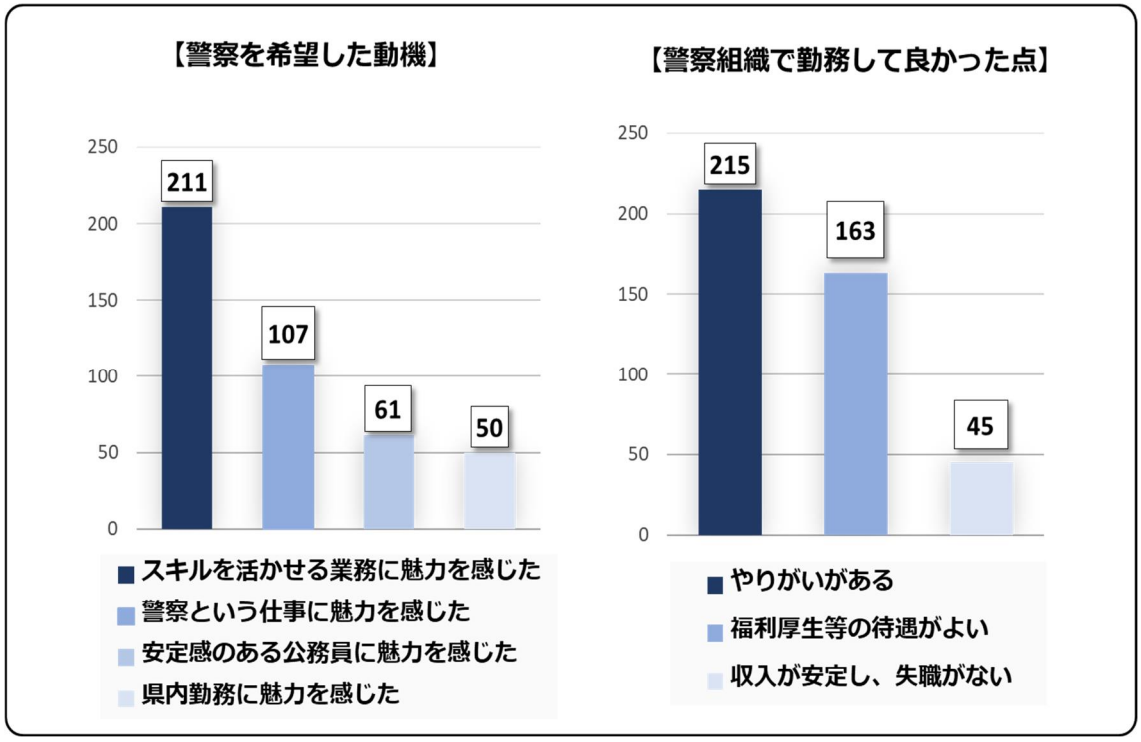
サイバー人材の確保・育成 ③

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】



（第２部３「基盤整備」関連）

サイバー部門の変遷

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

統計編[1]

---

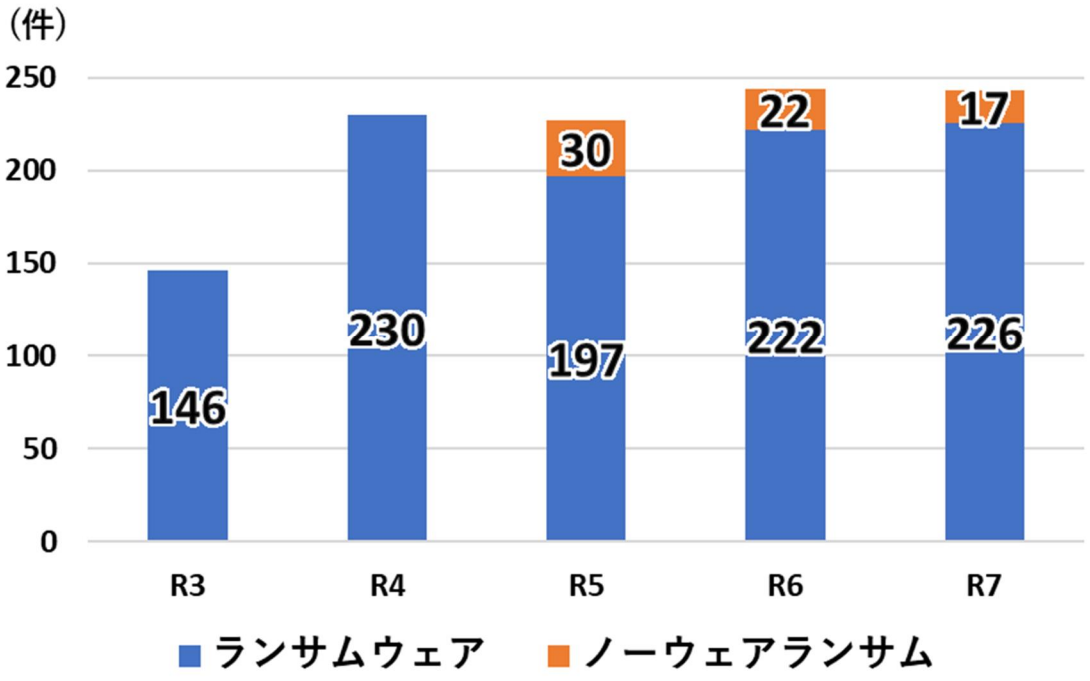
[1] 統計編中のグラフについては、特段の記載がない限り、令和７年の状況を示している。

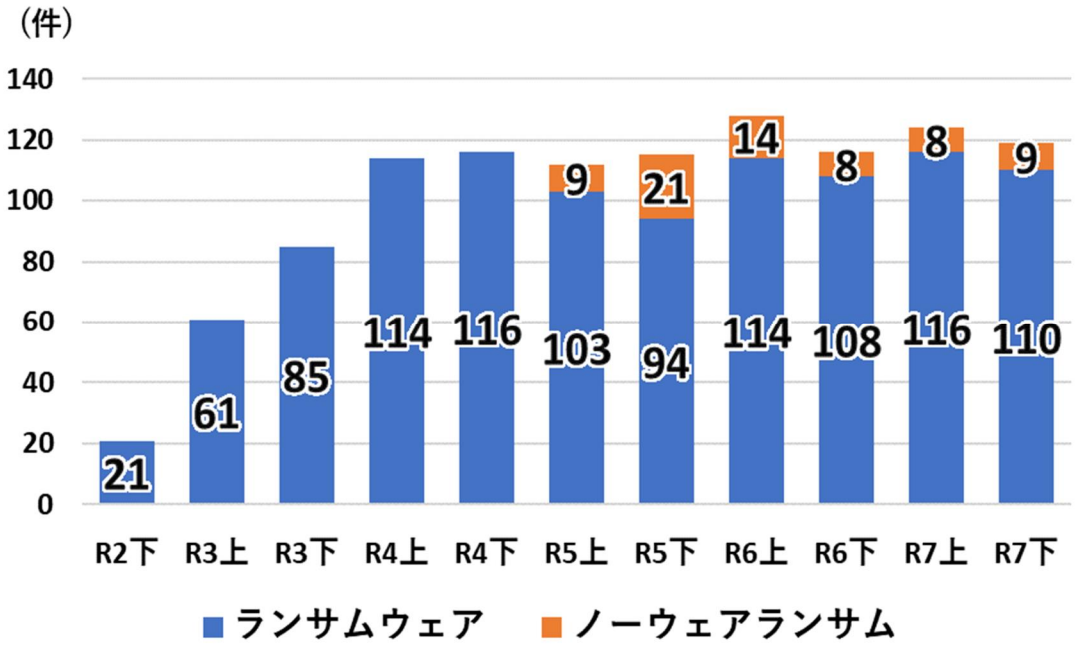
（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ランサムウェア被害報告件数等 ①

1　企業・団体等における被害の報告件数の推移

※ノーウェアランサムの被害については、令和５年上半期から集計。

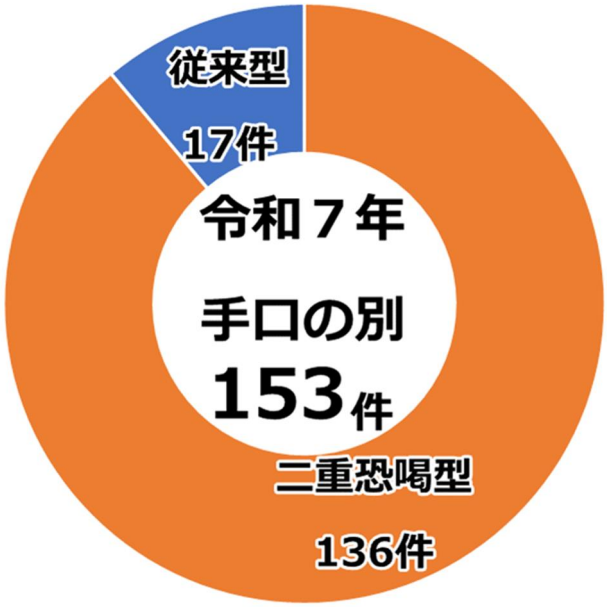


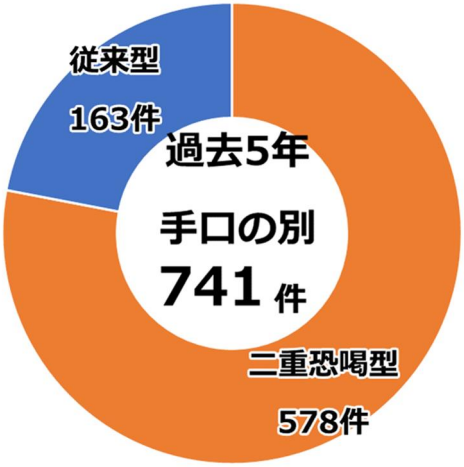


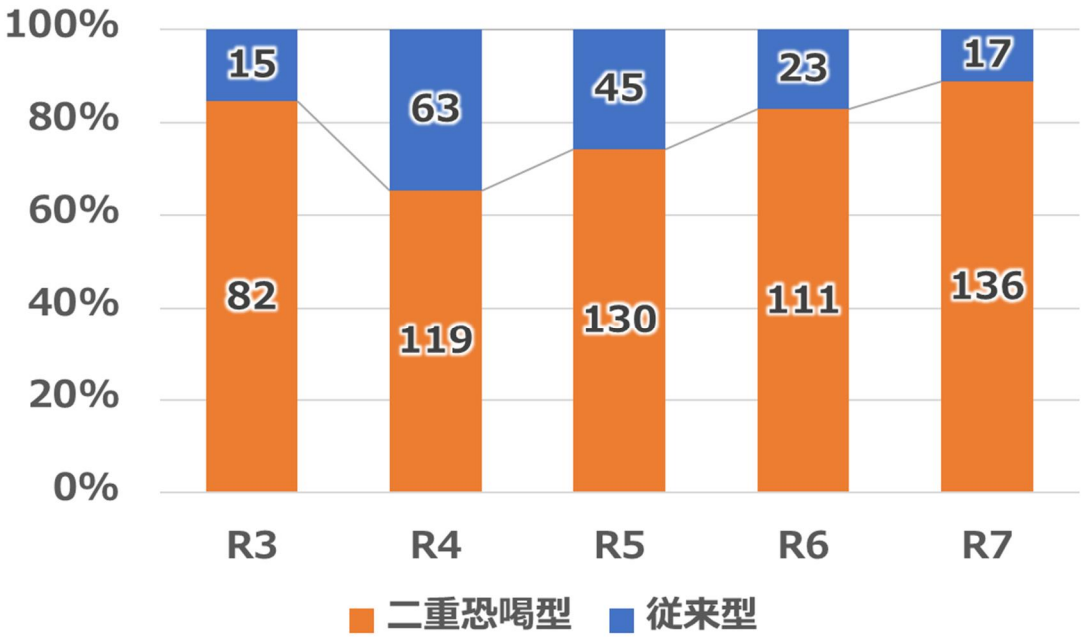
（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ランサムウェア被害報告件数等 ②

２　手口別報告件数





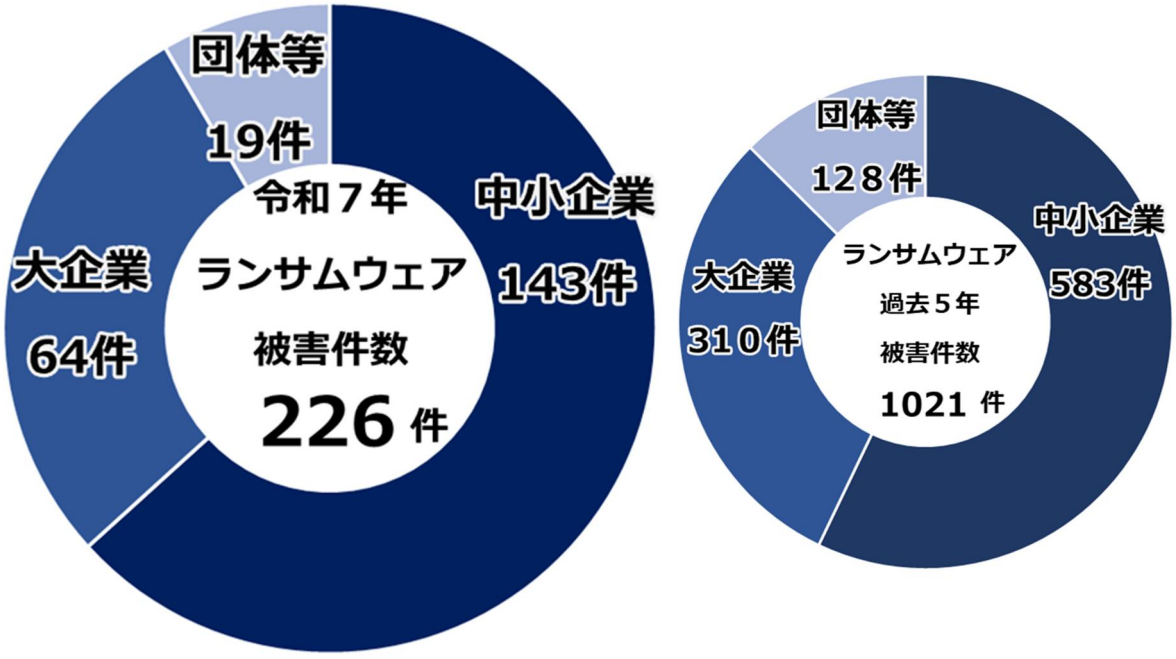


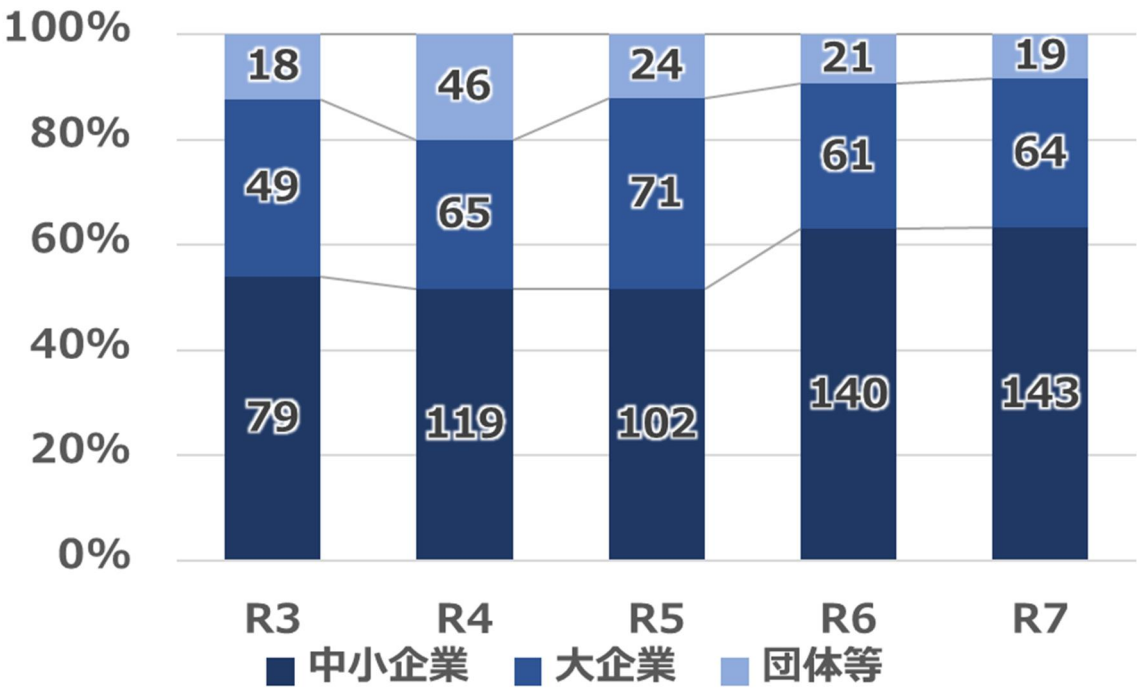
※　手口が判明した数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

被害企業・団体等の種別 ①

３　被害企業・団体等の規模別報告件数



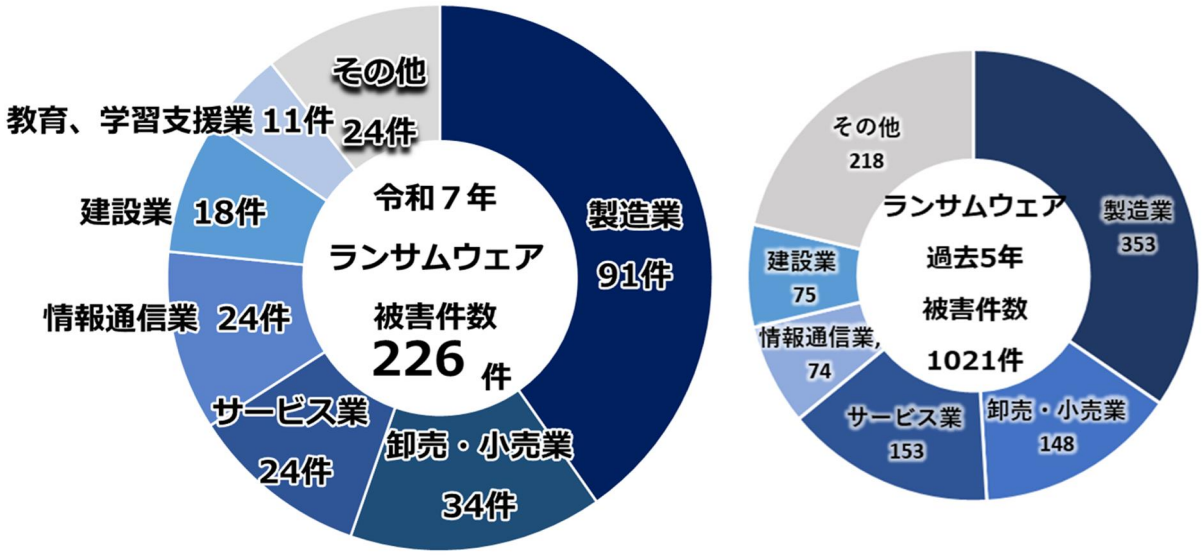


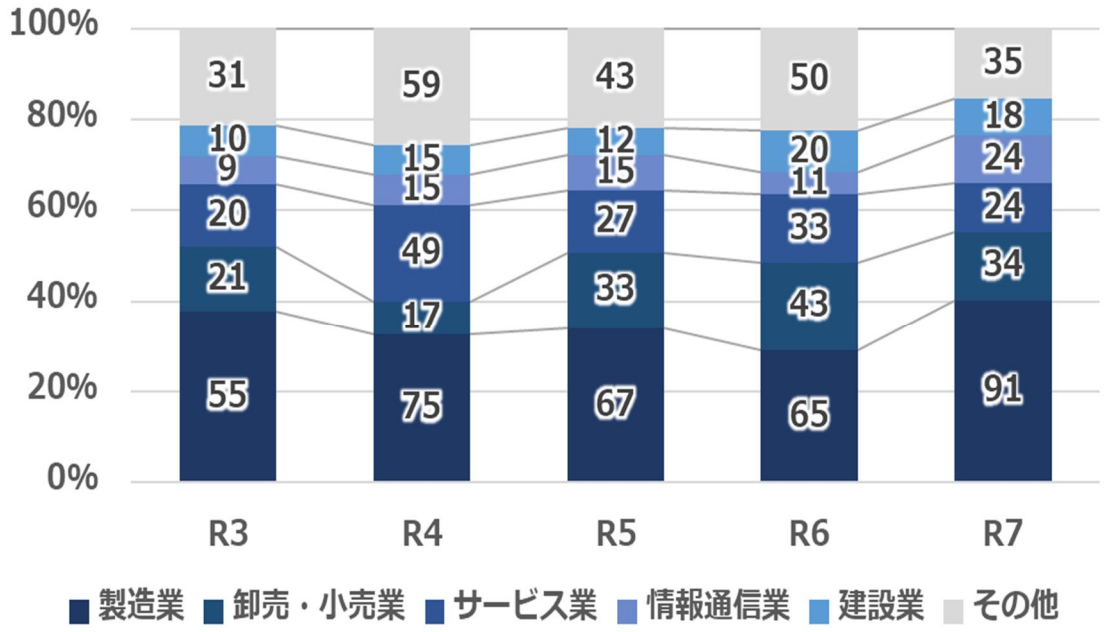
※　発生件数の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

被害企業・団体等の種別 ②

４　業種別報告件数





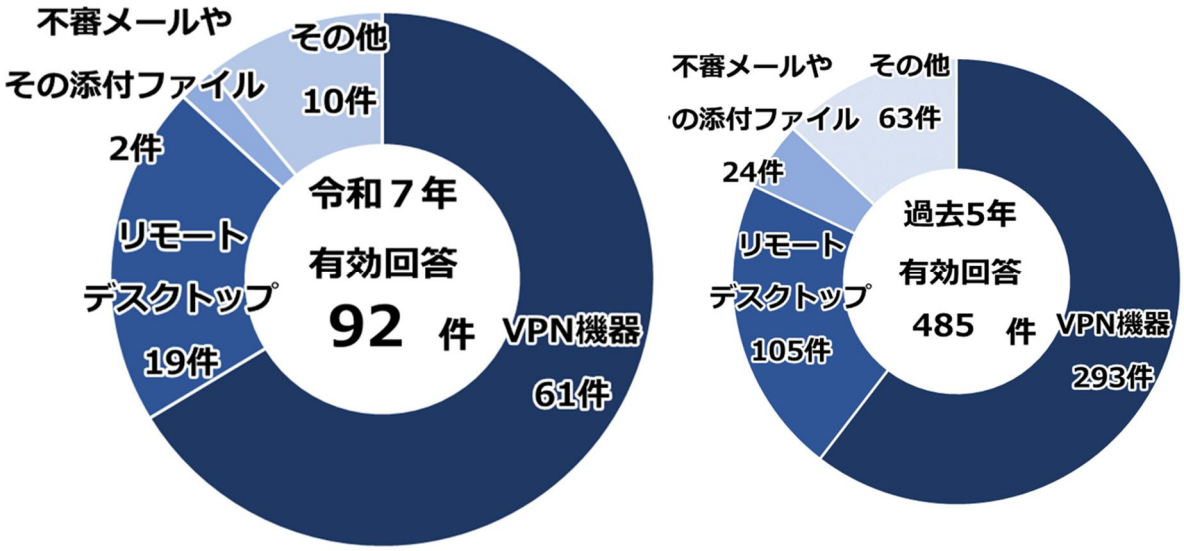
※　発生件数の数値が異なるため、各年の合計数値は異なる。

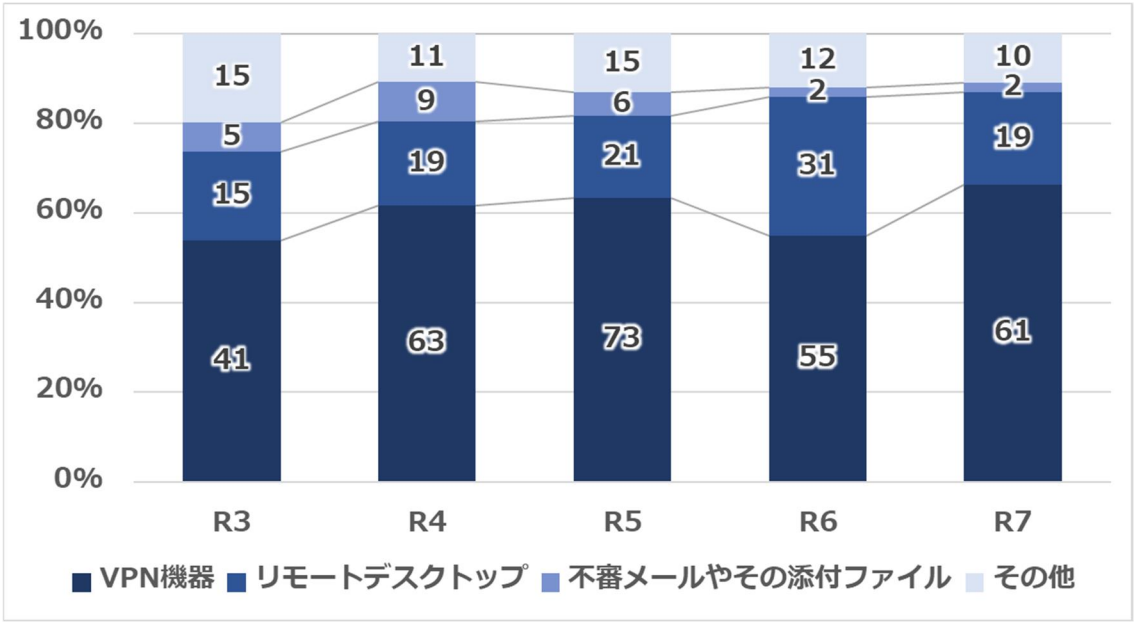
（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ランサムウェア感染経路

５　ランサムウェア被害にあった企業・団体等へのアンケート調査の回答結果

● 感染経路



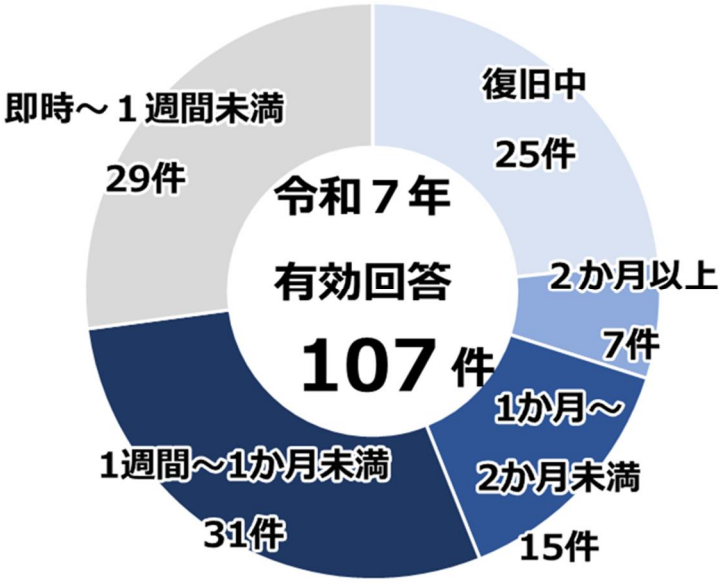


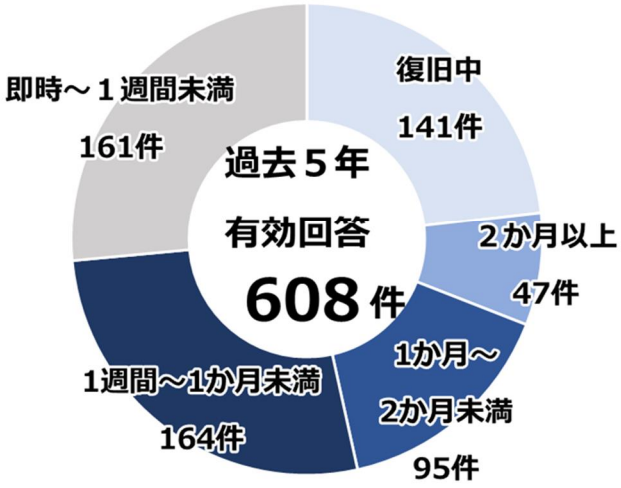
※　有効回答の数値が異なるため、各年の合計数値は異なる。

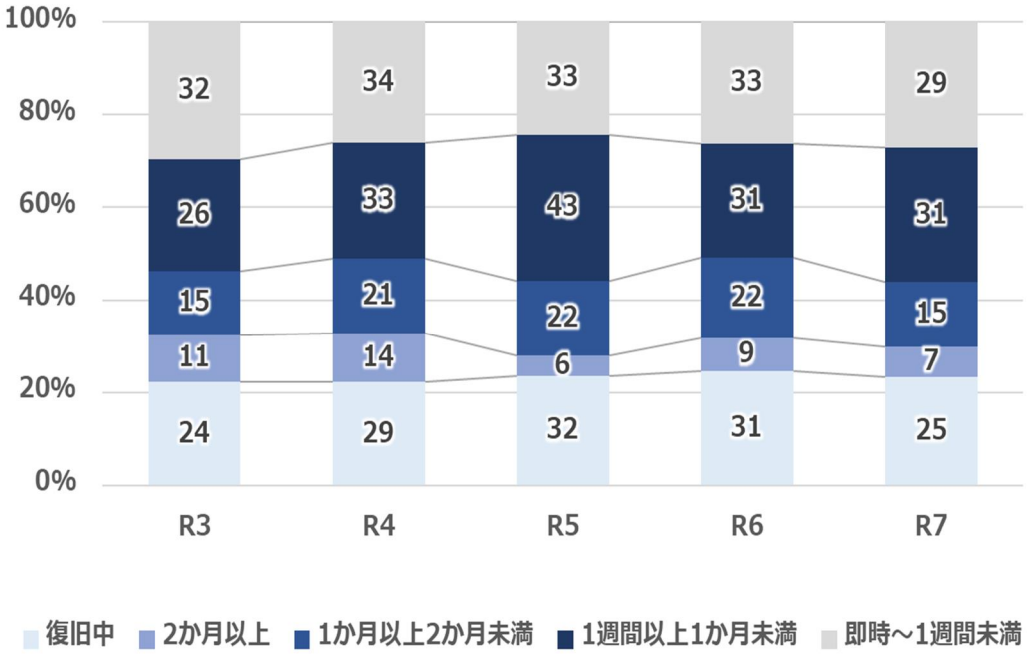
（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

復旧期間・費用 ①

● 復旧等に要した期間





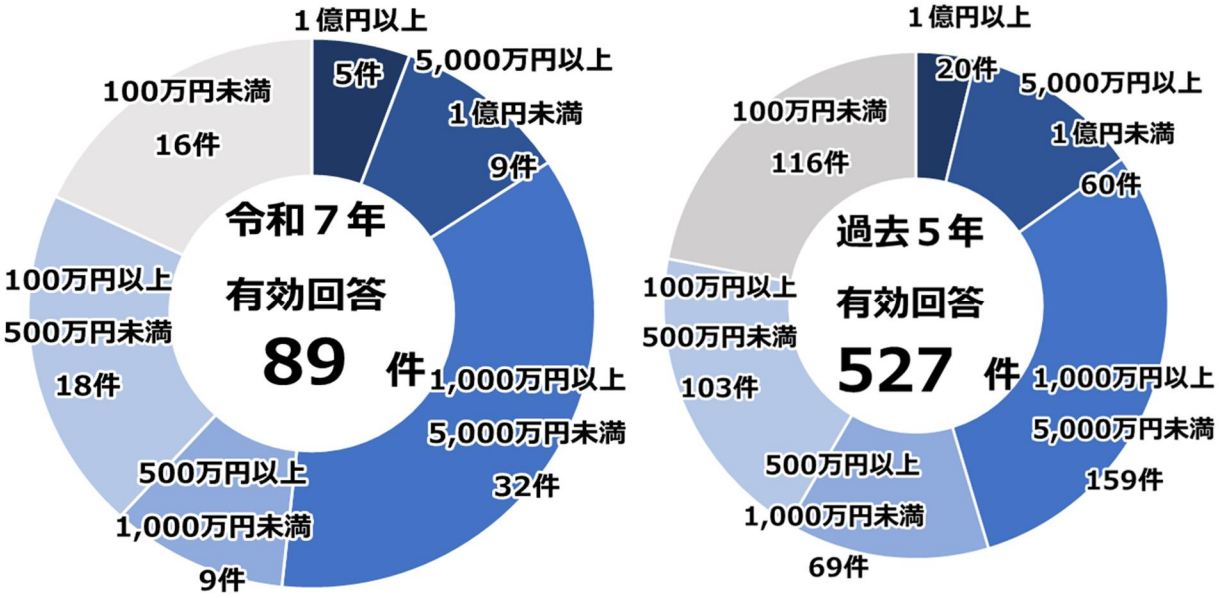


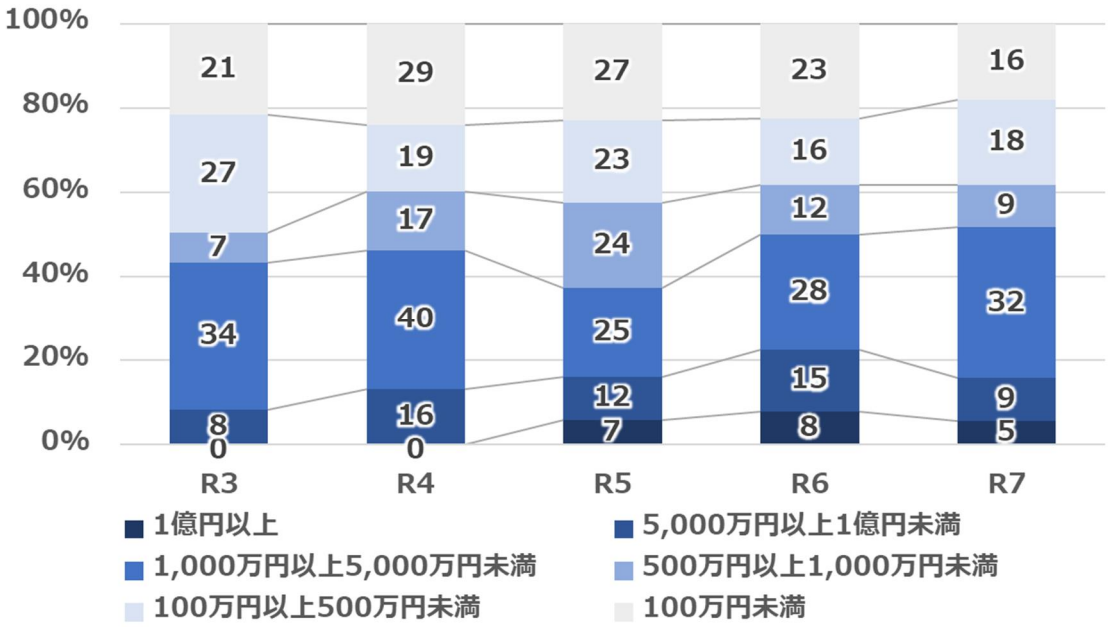
※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

復旧期間・費用 ②

● 調査・復旧費用の総額





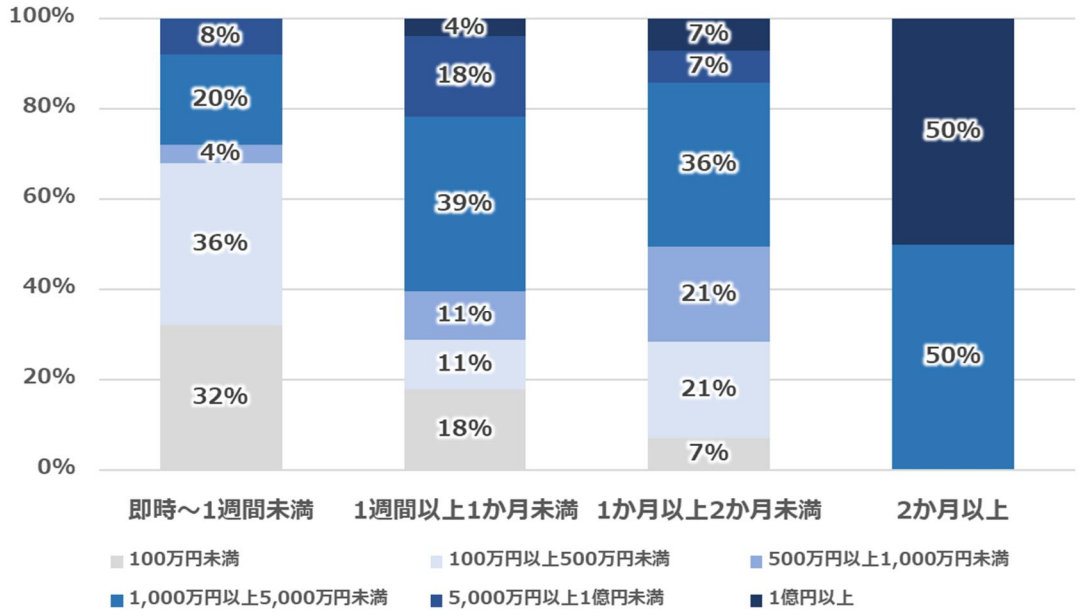
※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

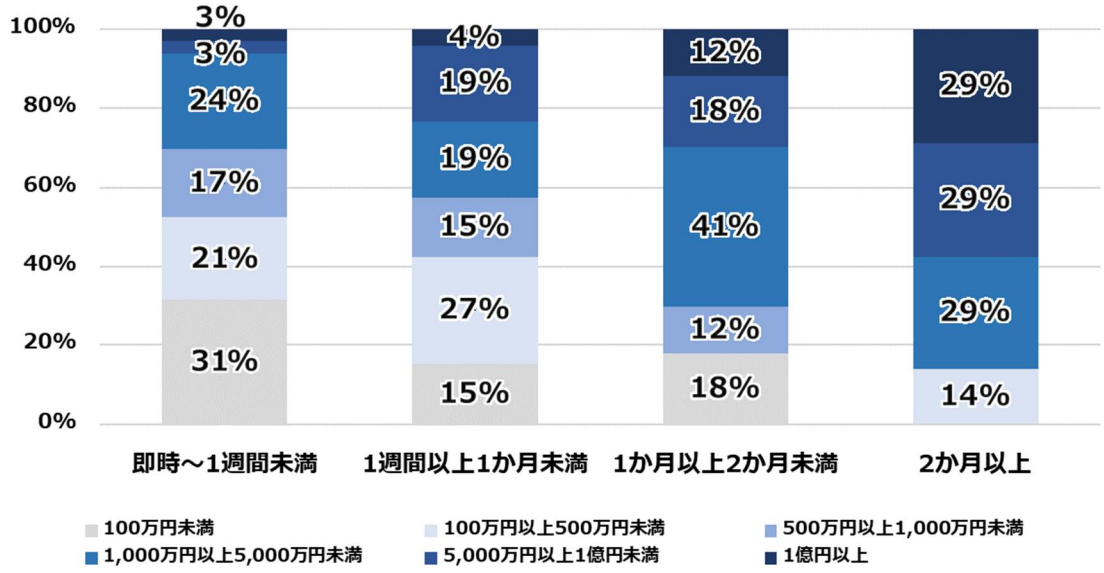
復旧期間・費用 ③

● 復旧期間と費用の関係性

【令和７年　アンケート調査結果】



【令和６年アンケート調査結果】

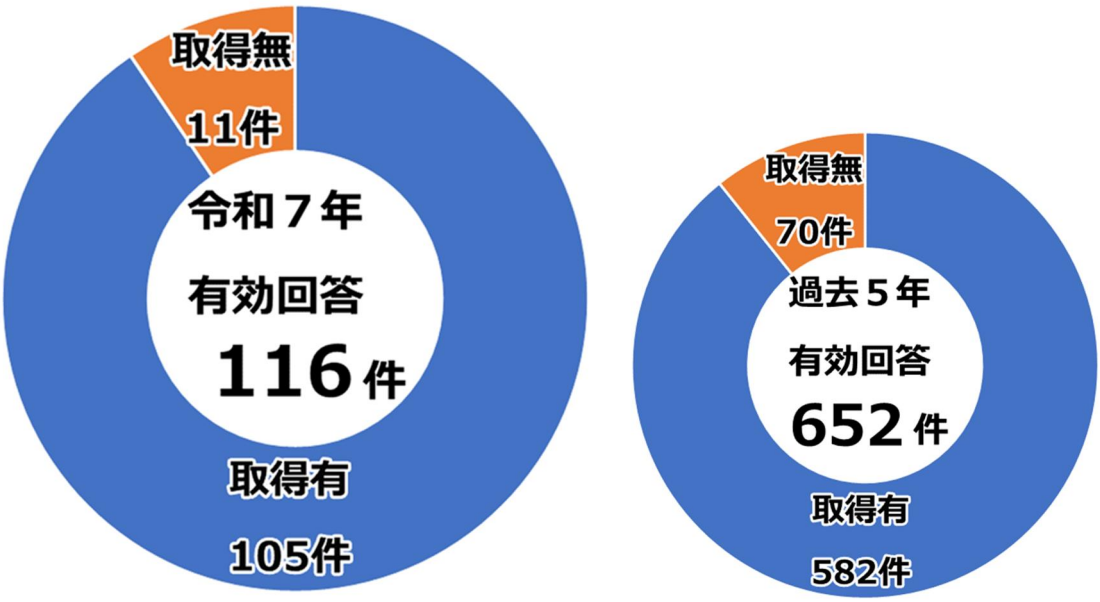


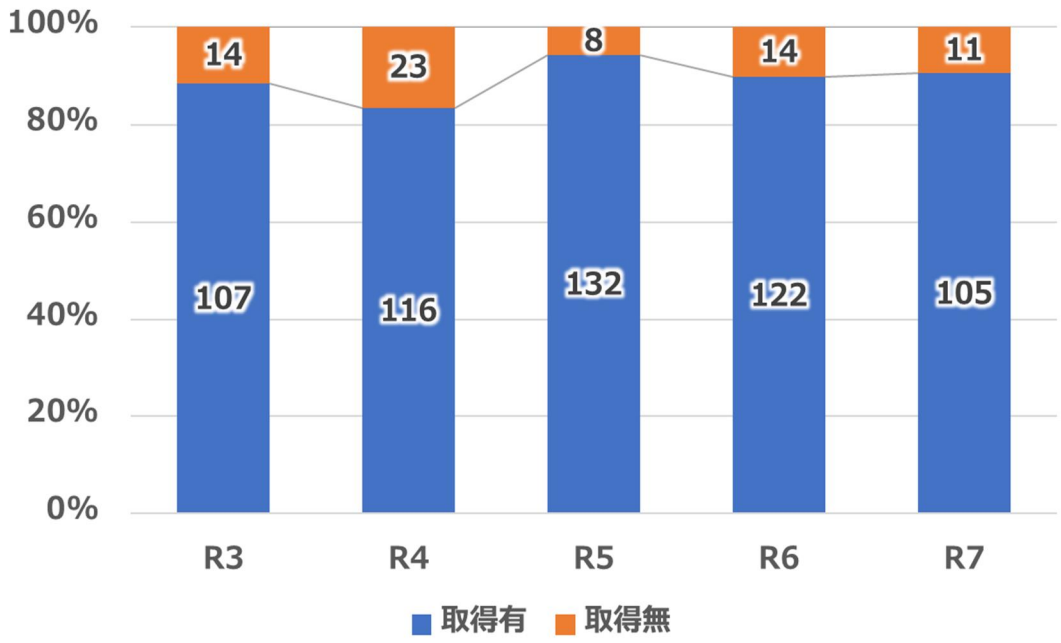
※　図中の割合は小数第１位以下を四捨五入しているため、統計が必ずしも 100 にならない。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

バックアップ ①

● バックアップの取得状況



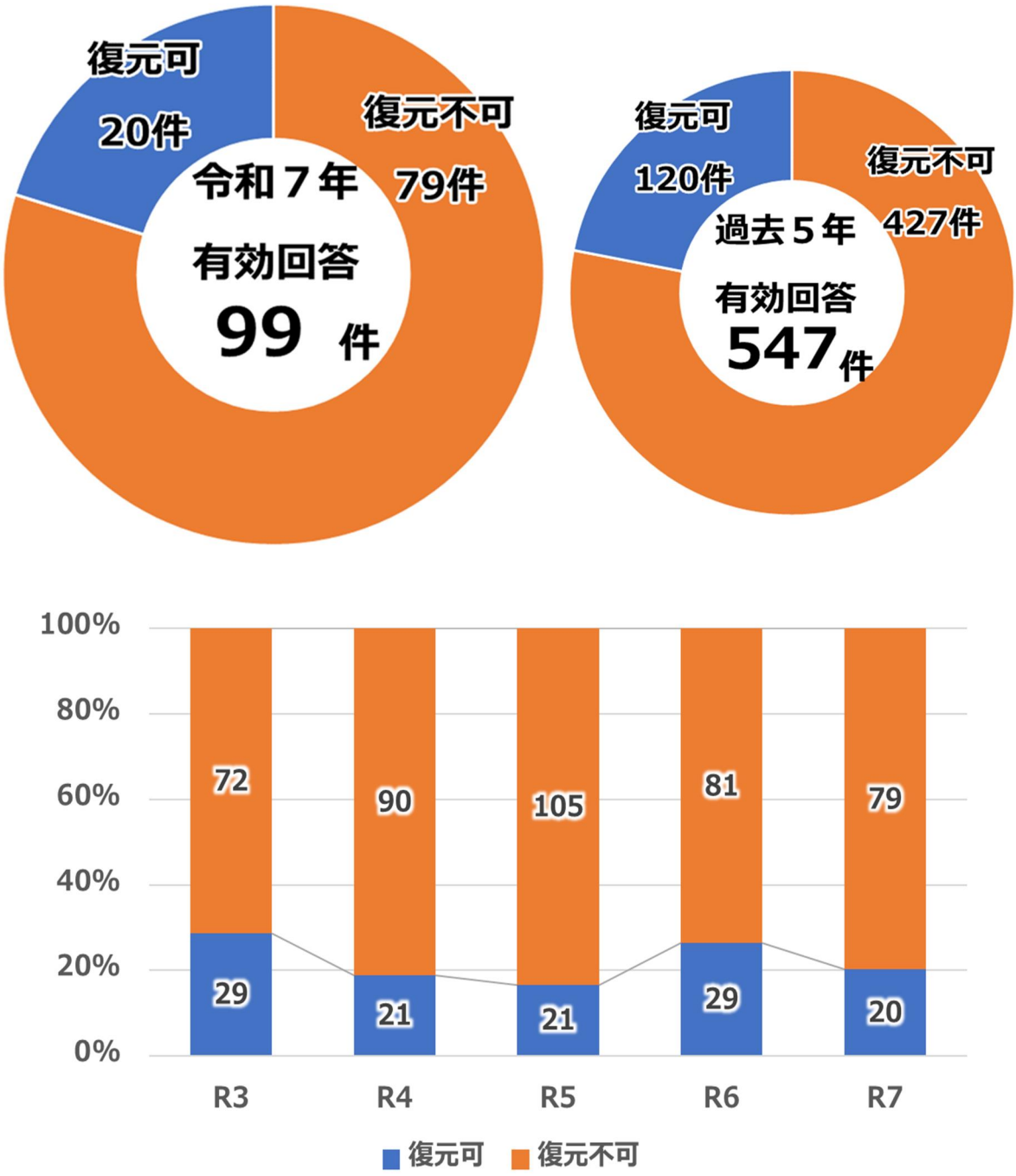


※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

バックアップ ②

●バックアップからの復元結果

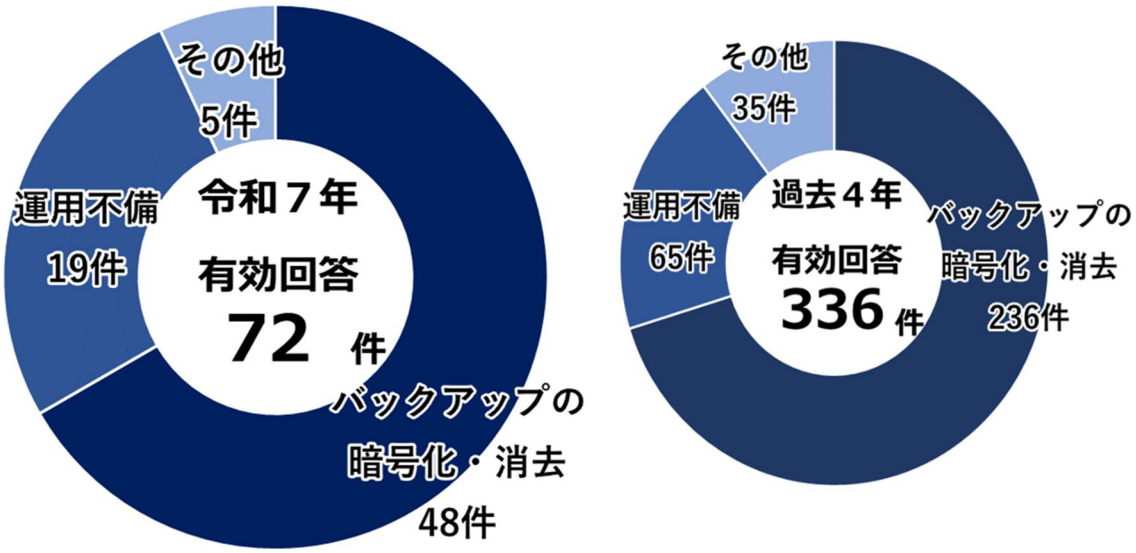


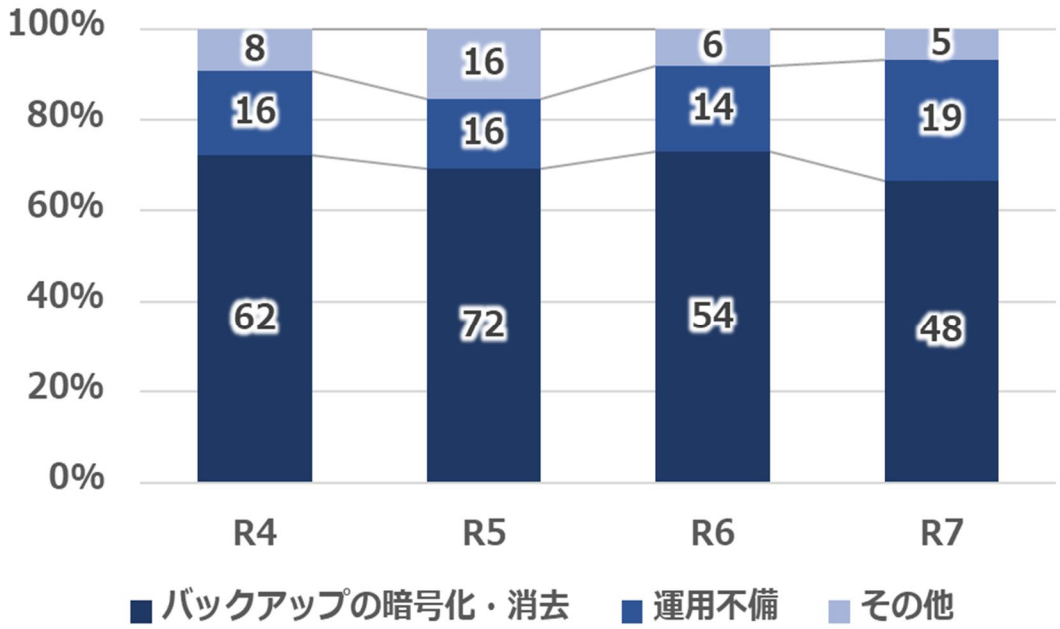
※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

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





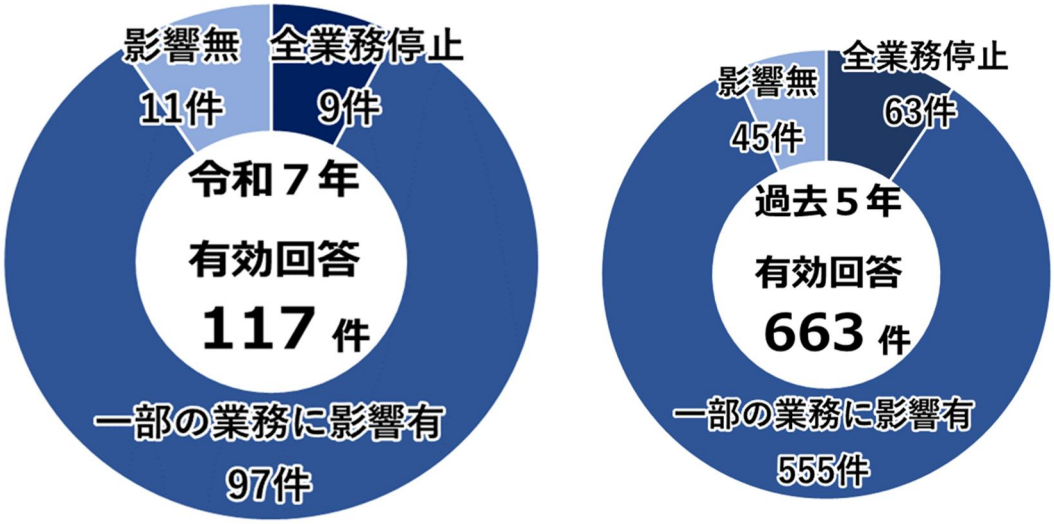
※ 令和４年から集計。

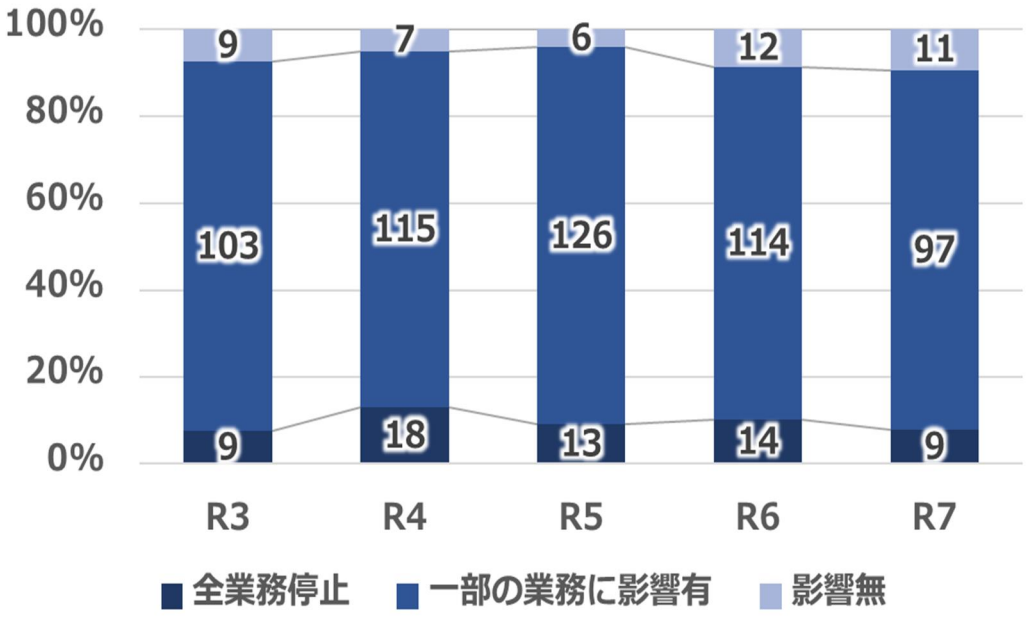
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ランサムウェアが業務に与えた影響

● ランサムウェア被害が業務に与えた影響の程度



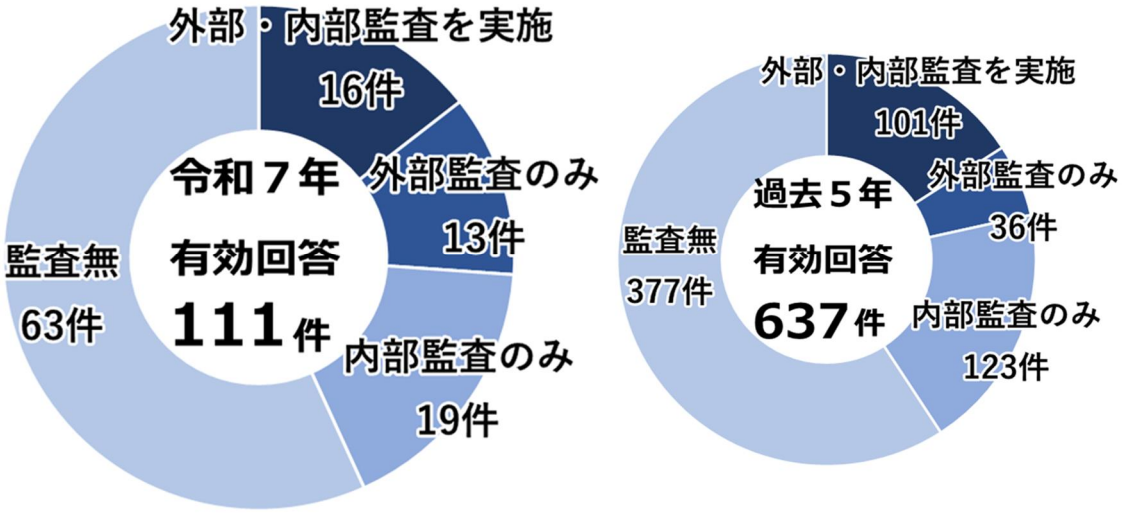


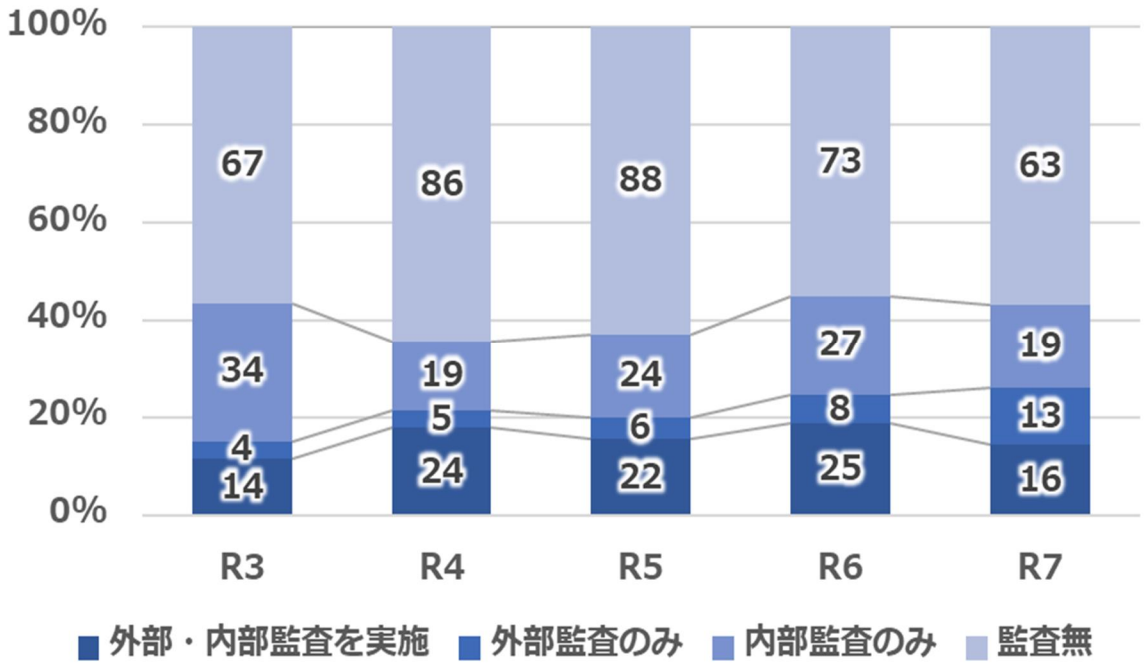
※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

情報セキュリティ監査の実施状況

● 被害企業・団体等の情報セキュリティ監査の実施状況



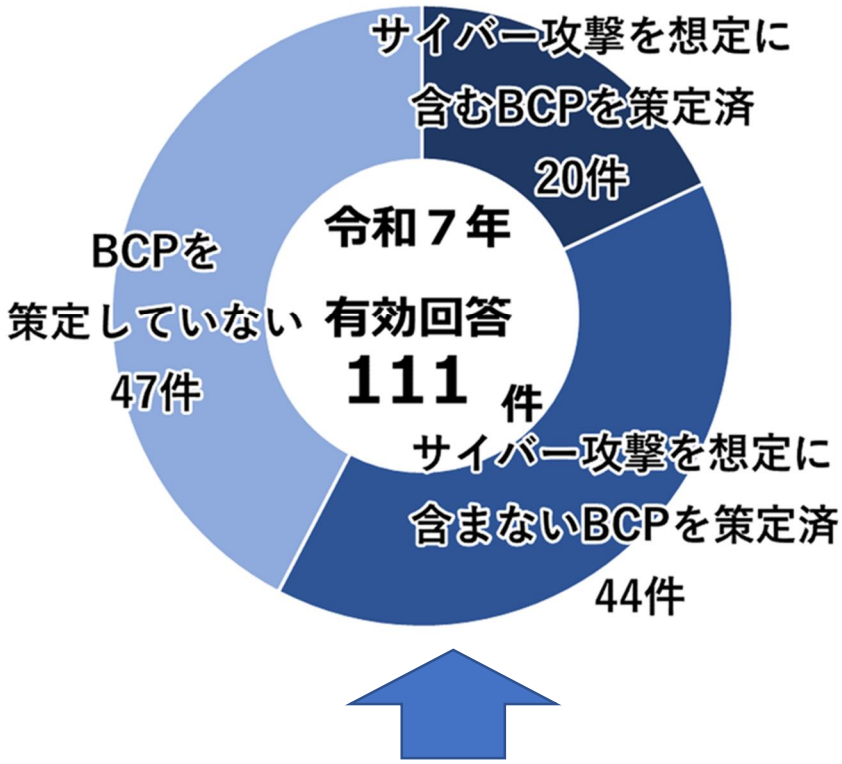


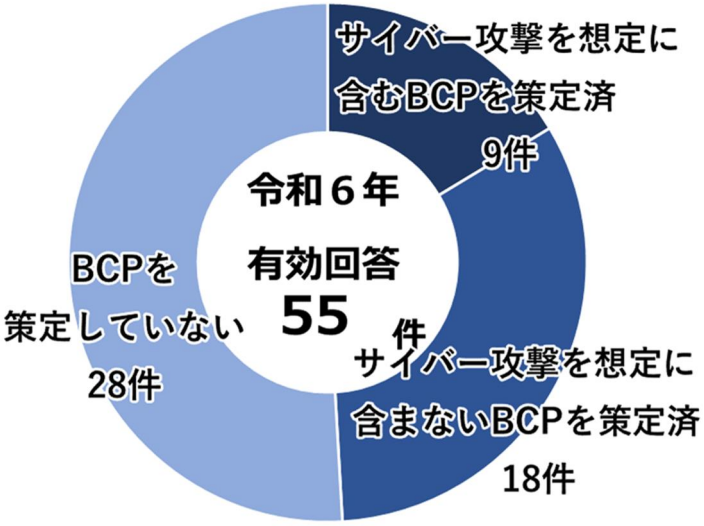
※　有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

業務継続計画（BCP）の策定状況

● 被害企業・団体等における業務継続計画（BCP）の策定状況





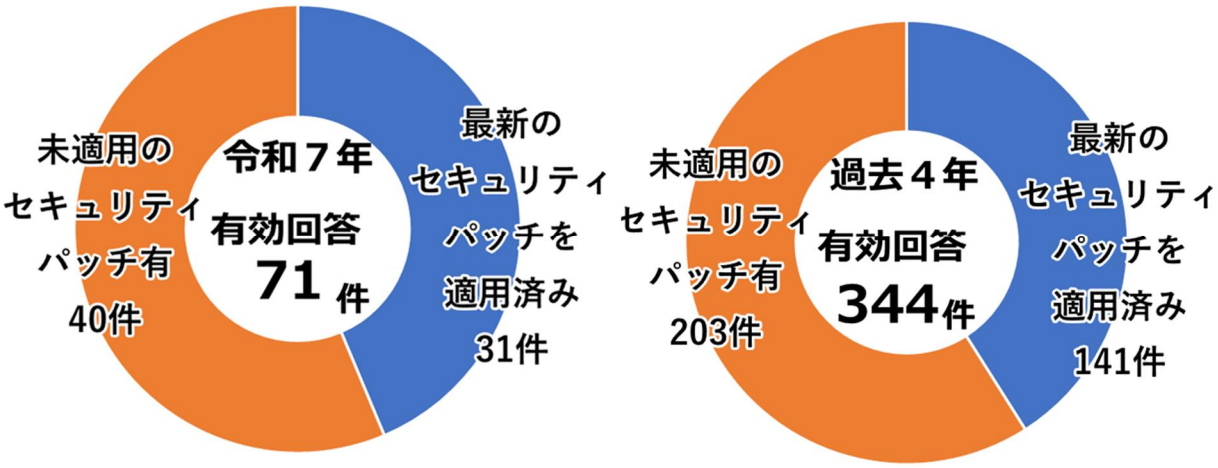
※ 令和６年から集計。

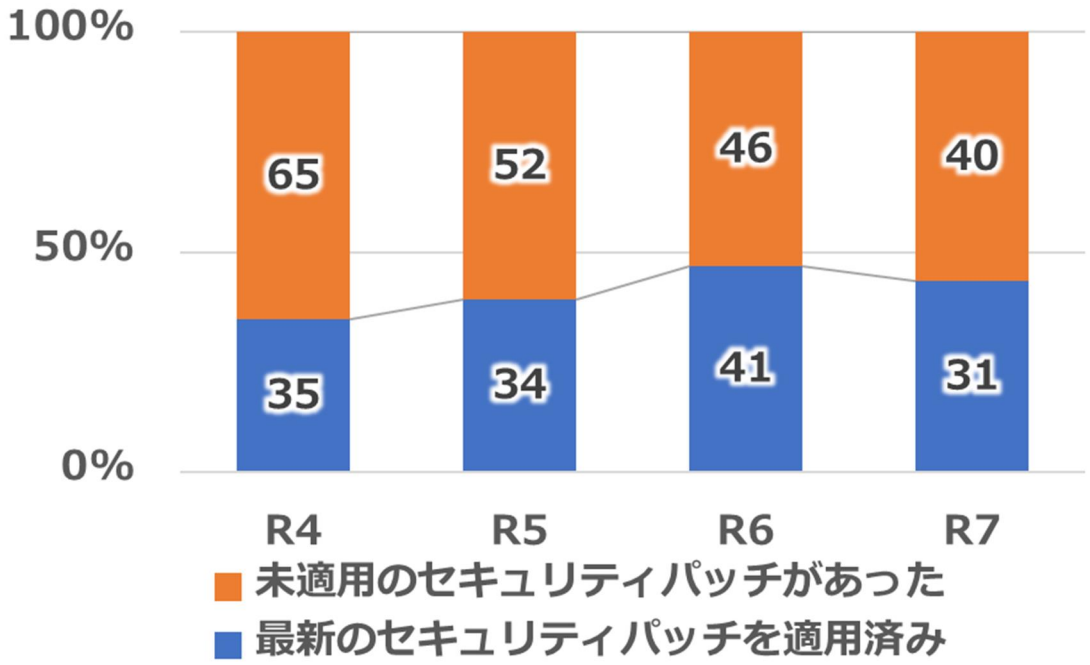
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

セキュリティパッチ、ウイルス対策ソフト ①

● 侵入経路とされる機器のセキュリティパッチの適用状況





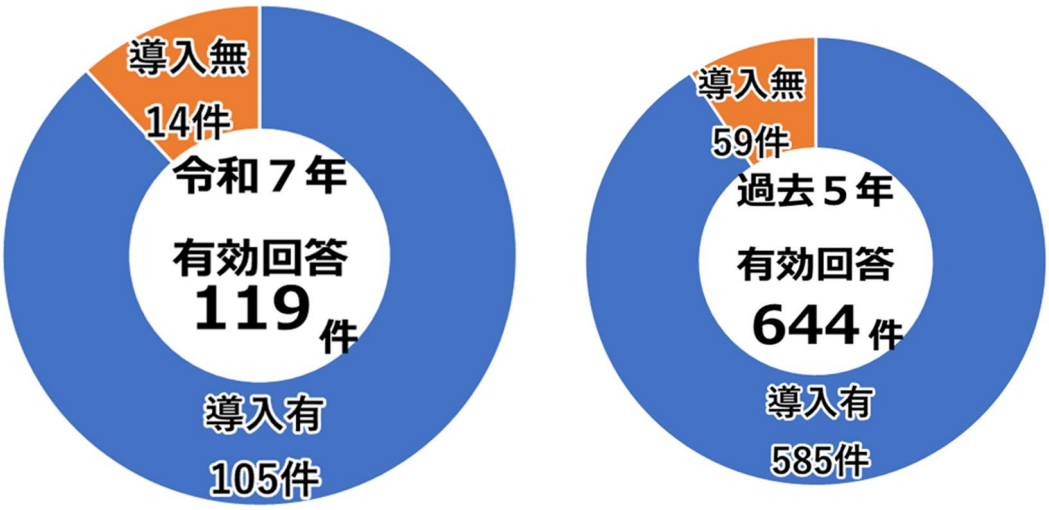
※ 令和４年から集計。

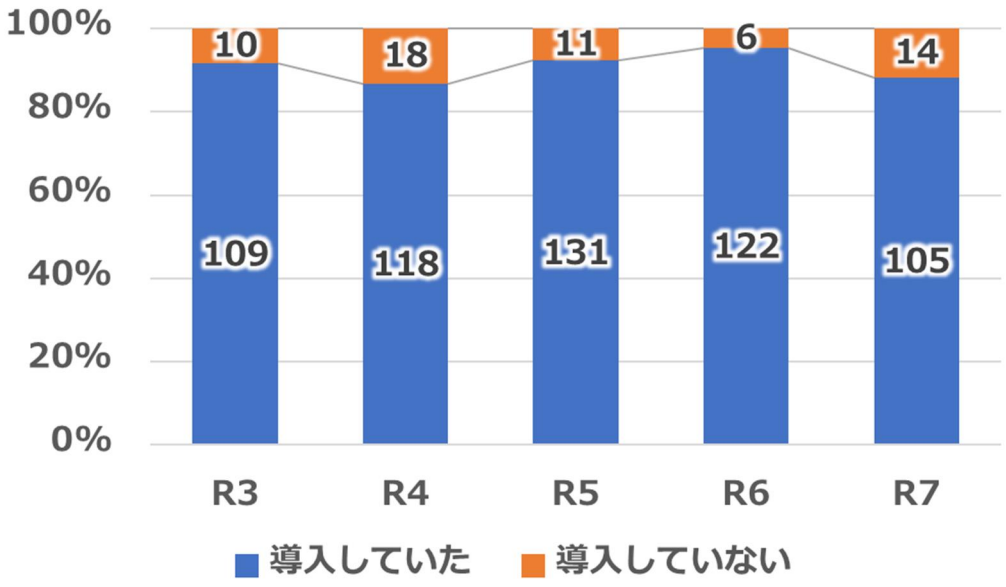
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

セキュリティパッチ、ウイルス対策ソフト ②

● 被害企業・団体等のウイルス対策ソフト等導入状況



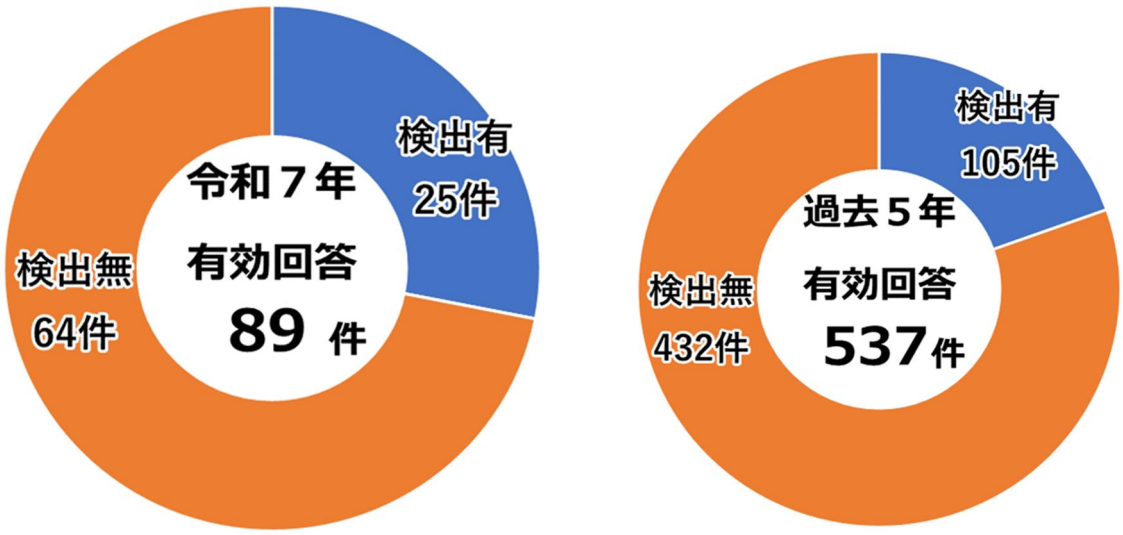


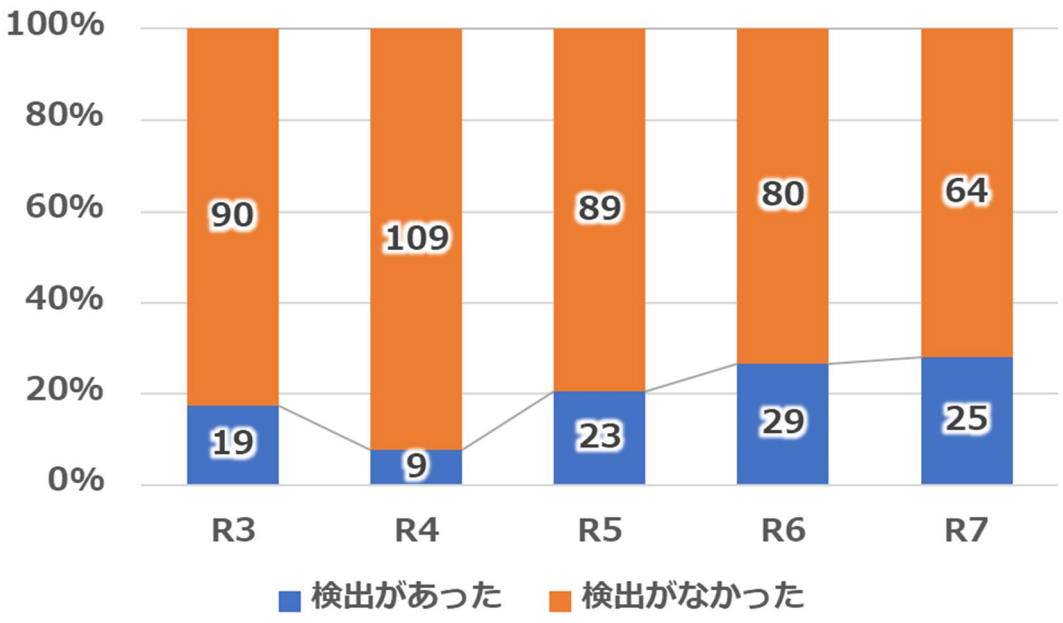
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

セキュリティパッチ、ウイルス対策ソフト ③

● 被害企業・団体等のウイルス対策ソフト検出状況



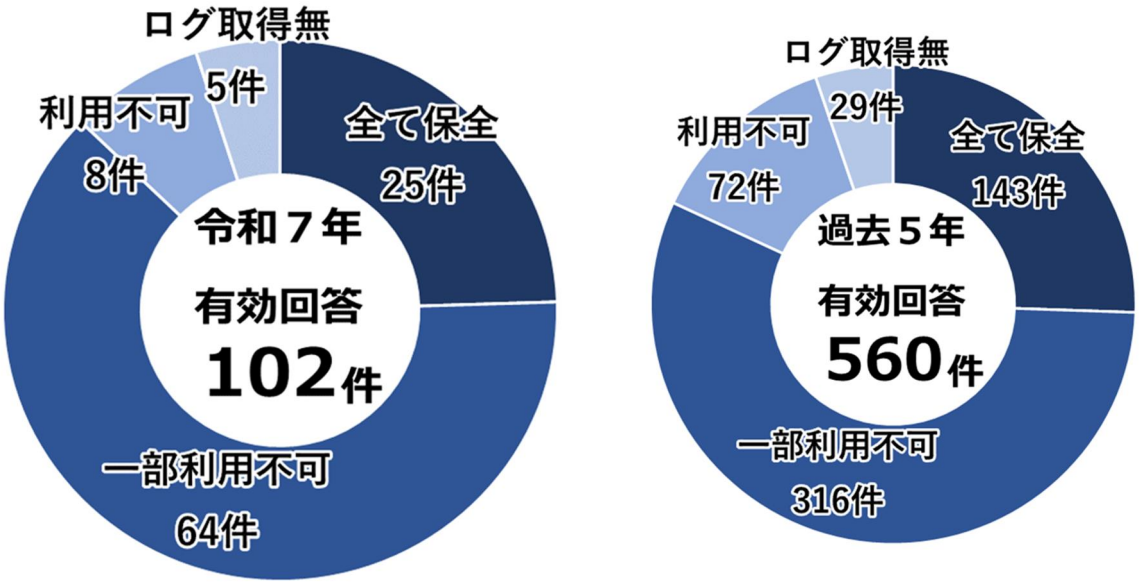


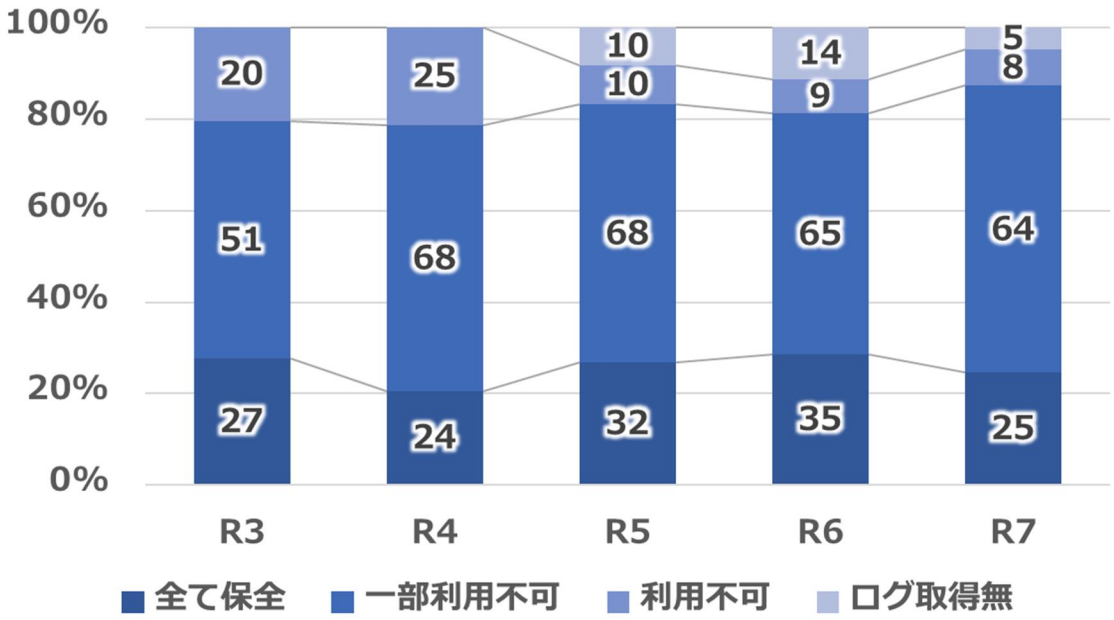
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ログ ①

● 被害企業・団体等のログ保全状況



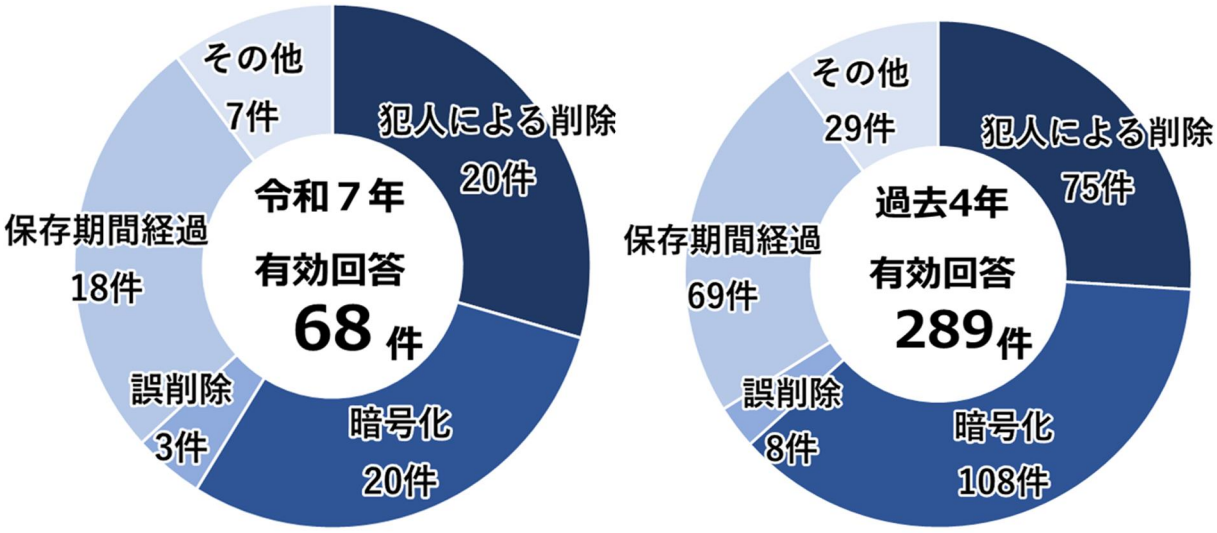


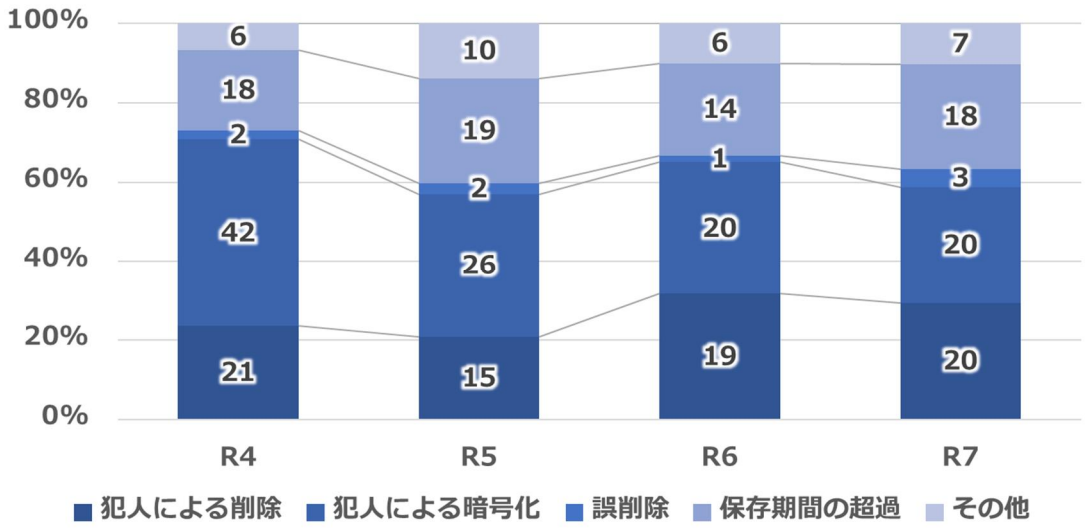
※ 有効回答の数値が異なるため、各年の合計数値は異なる。

（特集Ⅱ「ランサムウェアをめぐる脅威の情勢と警察の取組」関連）

ログ ②

● ログが使用できなくなっていた原因





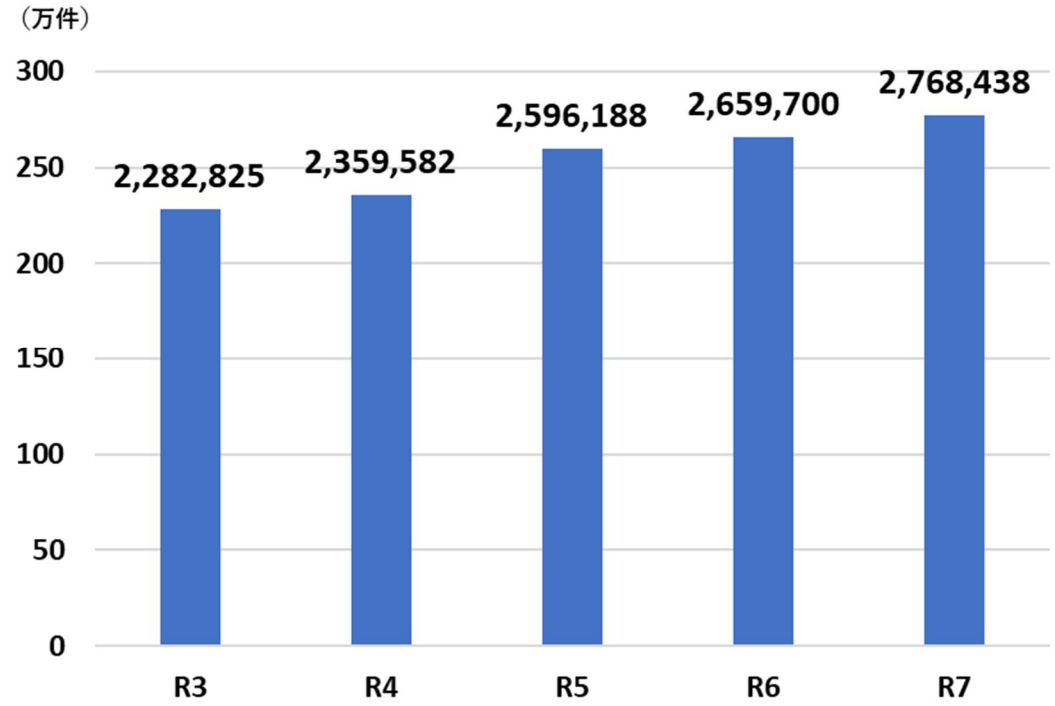
※ 令和４年から集計。

※ 有効回答の数値が異なるため、各年の合計数値は異なる。

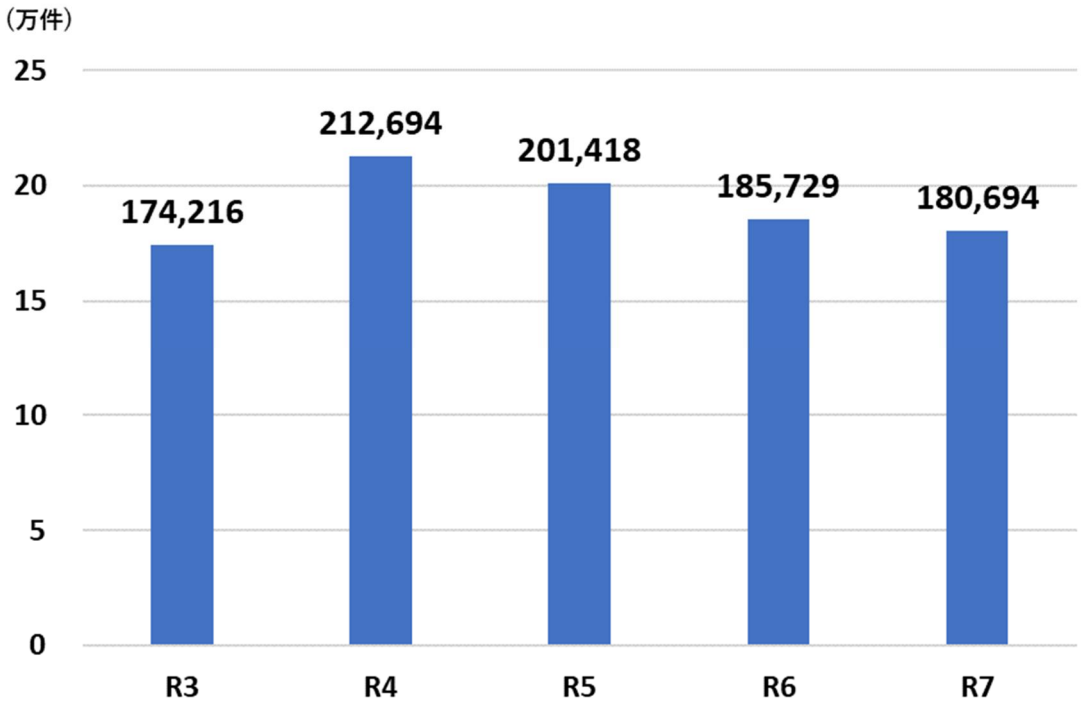
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

警察に対する相談

１　警察で取り扱った相談件数の推移



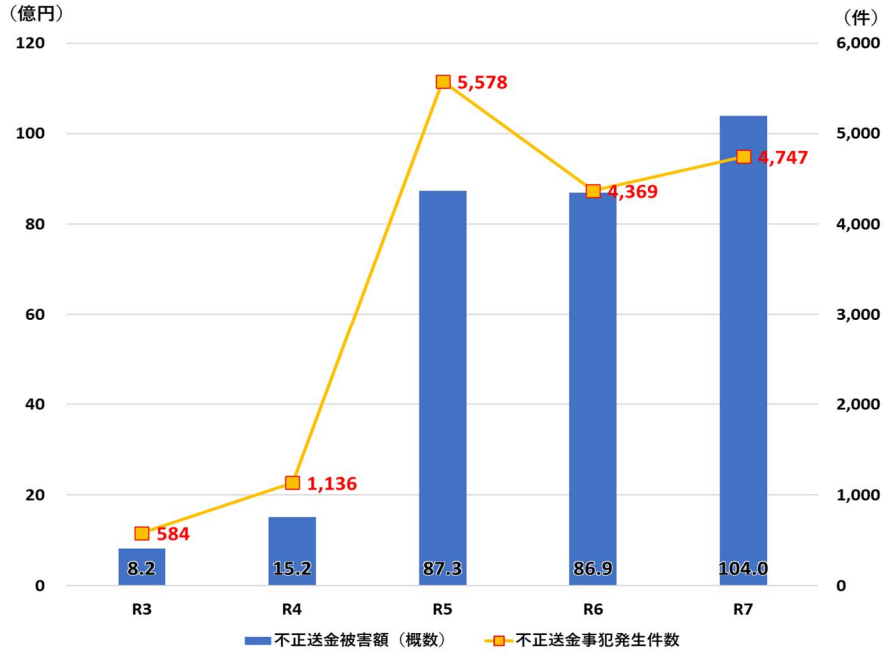
２　警察で取り扱ったサイバー関係の相談件数の推移



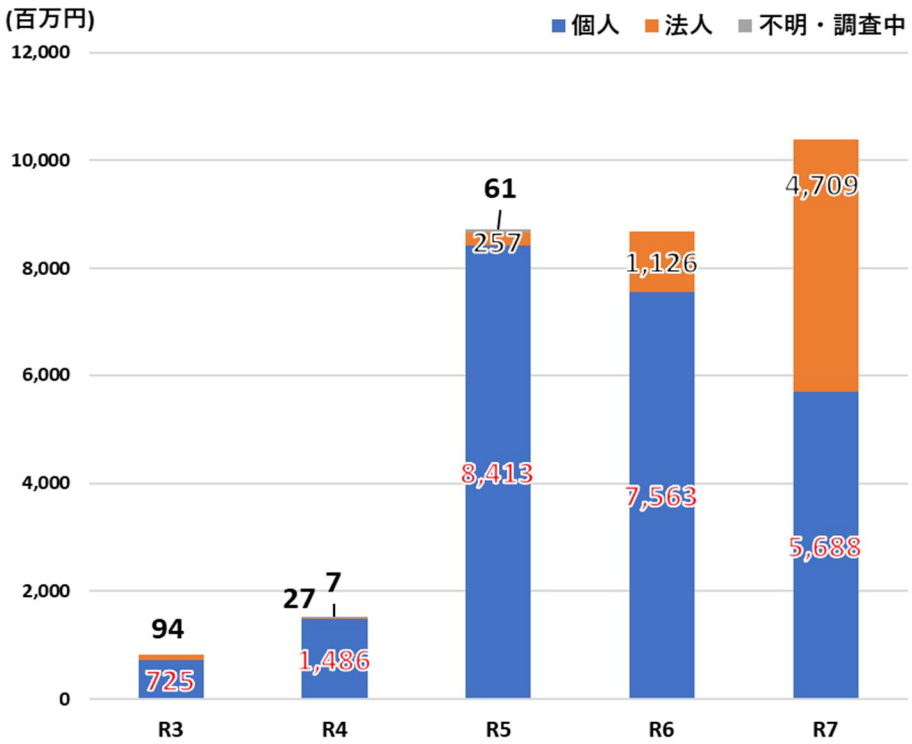
（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯 ①

１　インターネットバンキングに係る不正送金事犯発生件数及び被害額の推移



２　インターネットバンキングに係る不正送金被害額の推移（個人・法人別）

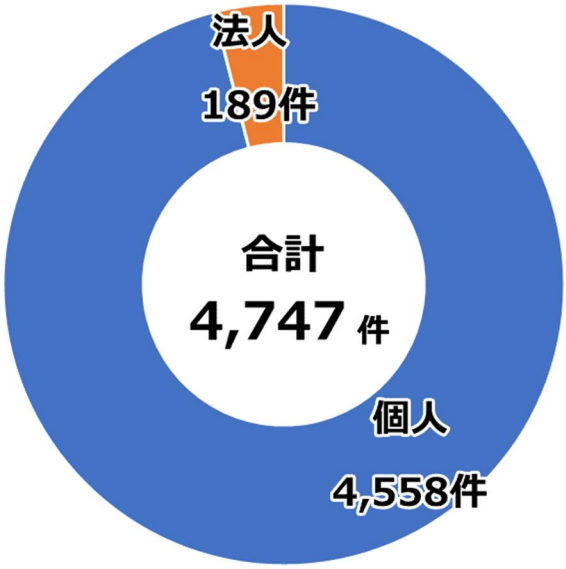


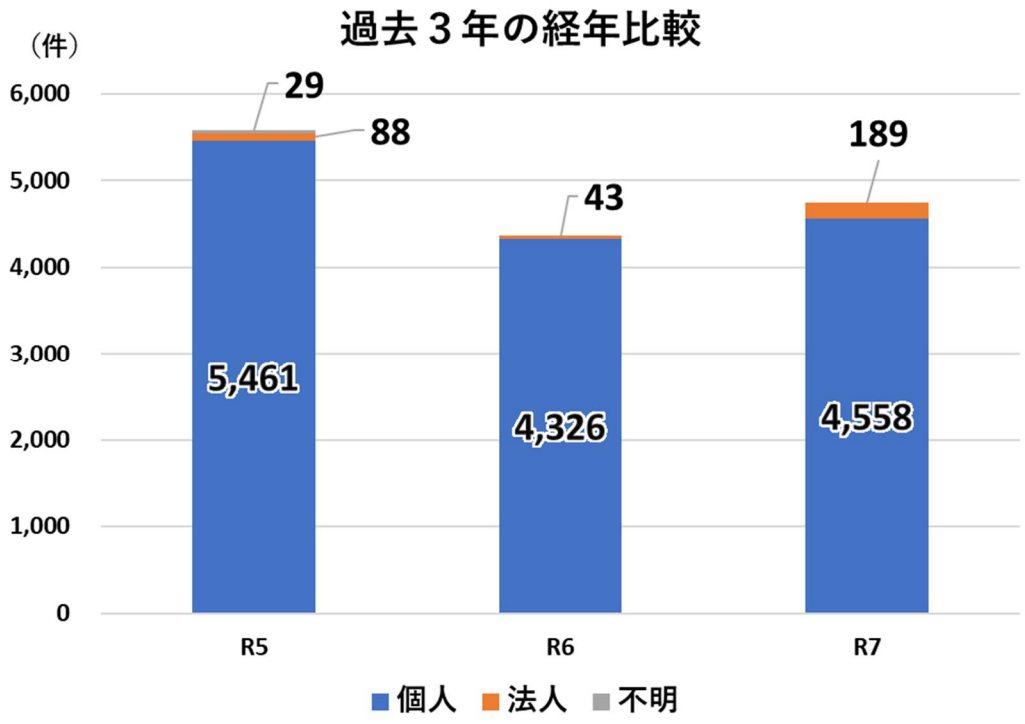
※　令和７年中に法人被害が急増した背景として、ボイスフィッシングによる法人口座の不正送金被害が急増したことが挙げられる。

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯 ②

３　インターネットバンキングに係る不正送金発生件数（個人・法人別）



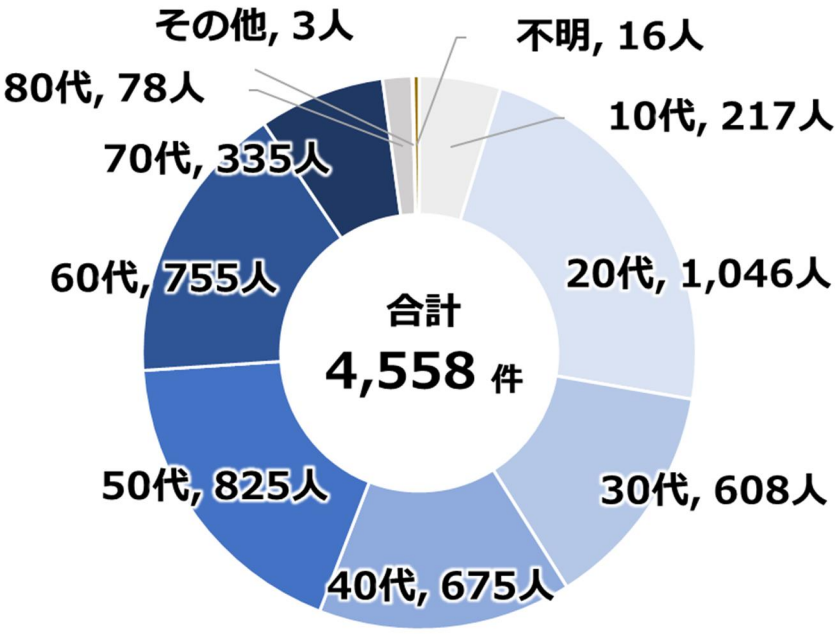


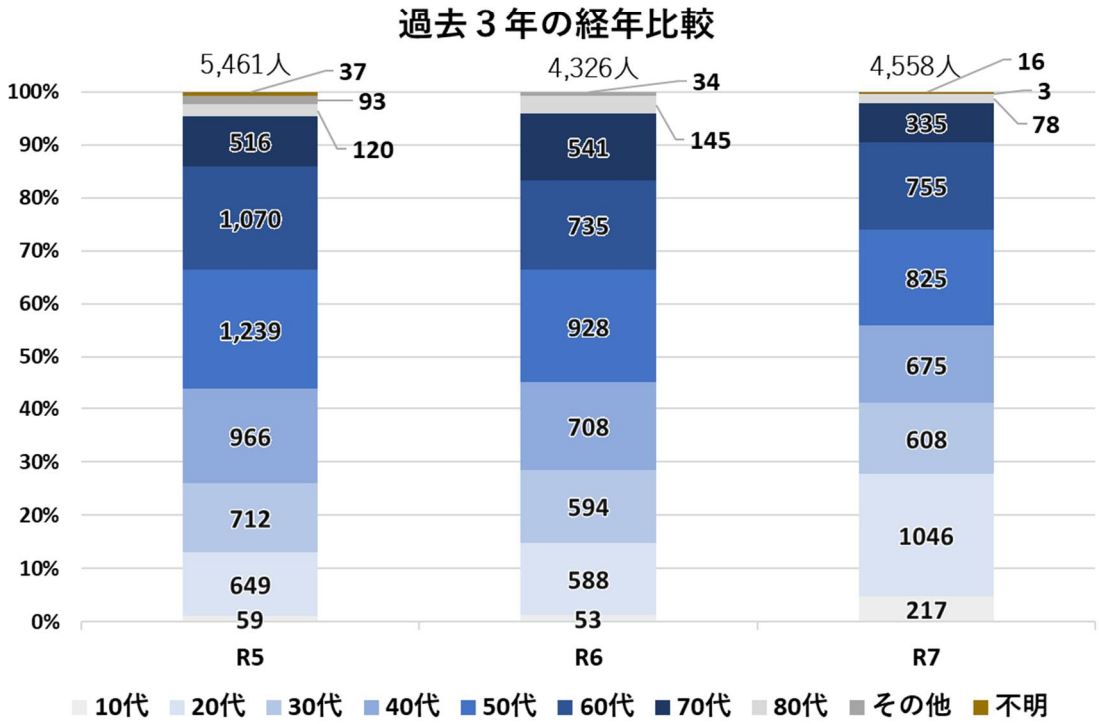
※　発生件数が異なるため、各年の合計数値は異なる。

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯 ③

４　個人のインターネットバンキングに係る年齢別の不正送金被害者数



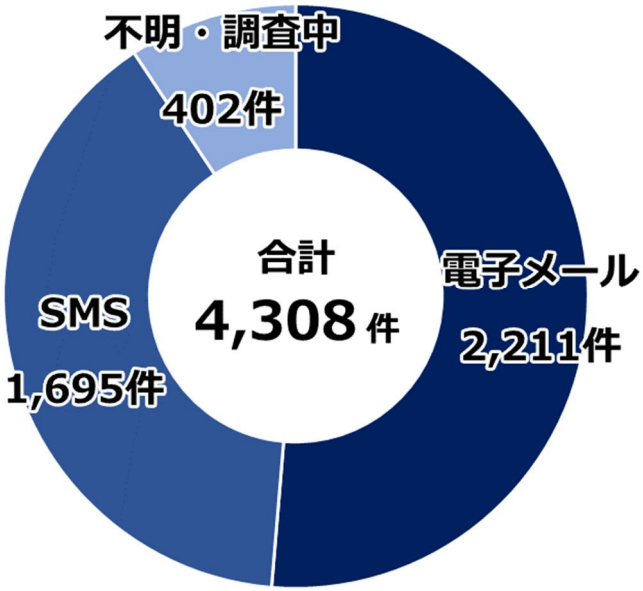


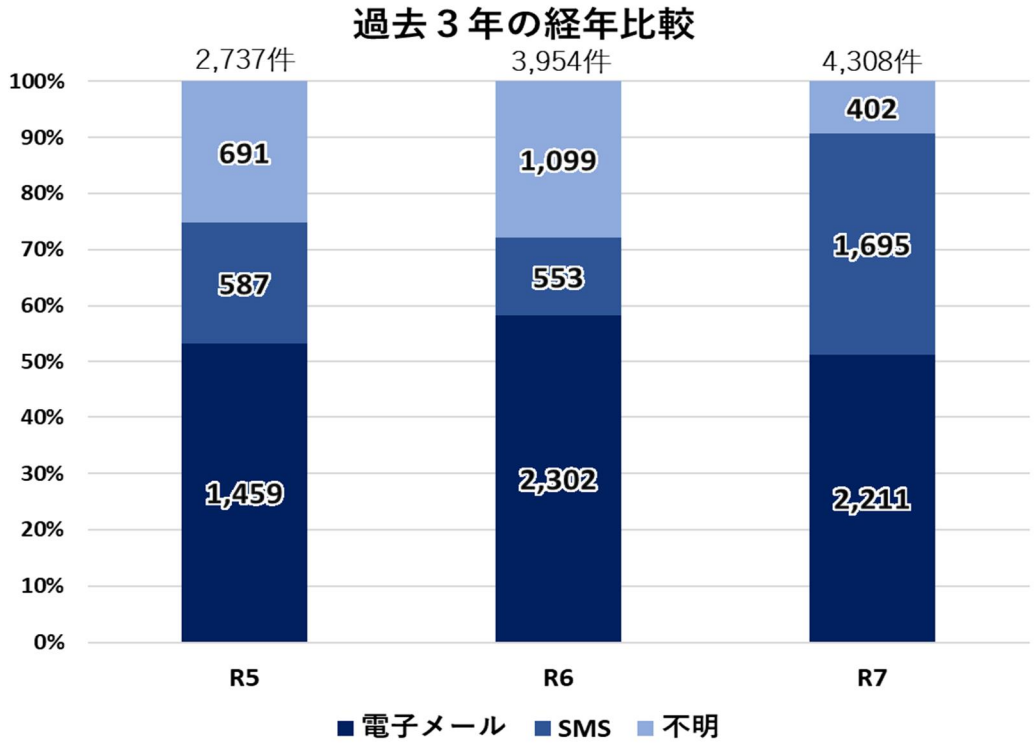
※　発生件数が異なるため、各年の合計数値（被害者数）は異なる。

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯 ④

５　フィッシングサイトへ誘導する手口別の不正送金発生件数





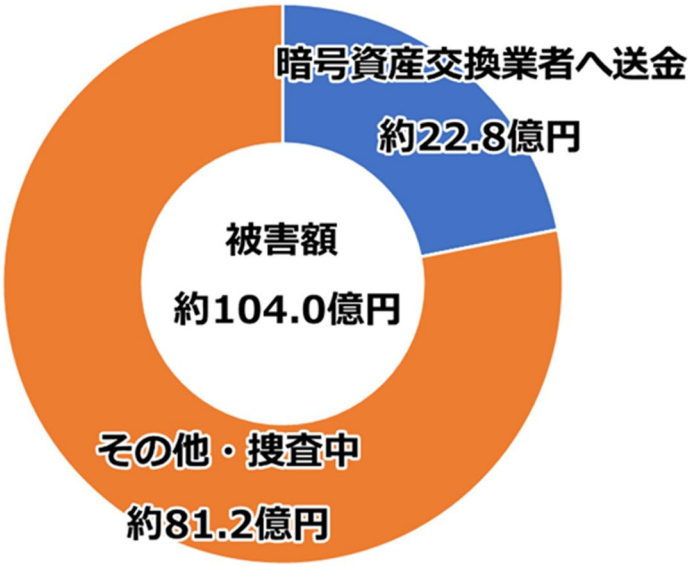
※　発生件数が異なるため、各年の合計数値は異なる。

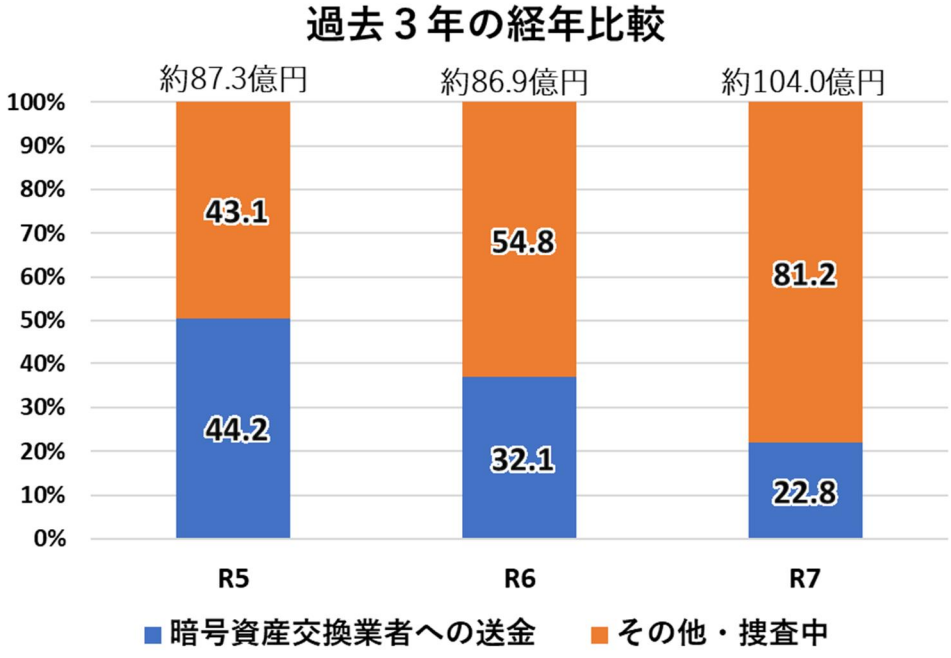
※　令和７年中に SMS が増加した要因として、モバイルマルウェアに感染した端末を悪用して、フィッシングサイトへ誘導する悪性な SMS を大量配信されていることが考えられる。

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

インターネットバンキングに係る不正送金事犯 ⑤

６　不正送金被害額のうち暗号資産交換業者名義の金融機関口座へ送金された額[2]





※　被害額が異なるため、各年の合計数値は異なる。

[2] 暗号資産交換業者の金融機関口座へ送金された後は、そのほとんどが暗号資産に変換されているものと考えられる。「その他」は、暗号資産交換業者の金融機関口座へ送金される前に被疑者等により使用されたもの、金融機関口座間の資金移動中に口座が凍結されたものを含む。また、捜査に一定の時間を要しており、「捜査中」の一部は暗号資産交換業者の金融機関口座へ送金されているものと考えられる。

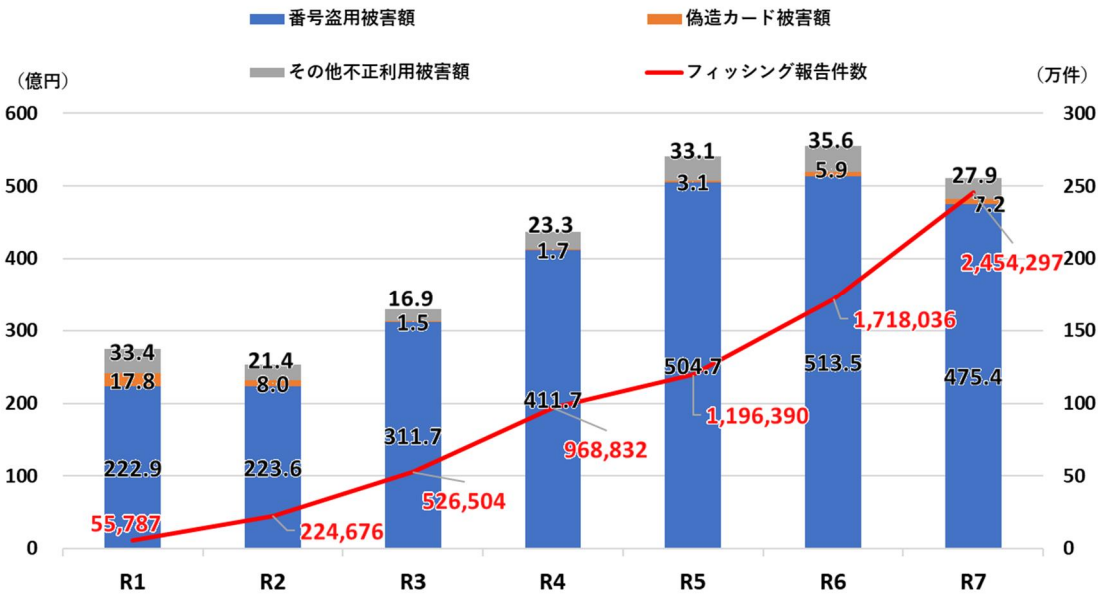
統計編

（第１部２「インターネット空間を悪用した犯罪に係る脅威情勢」関連）

（第２部１「検挙に向けた取組」関連）

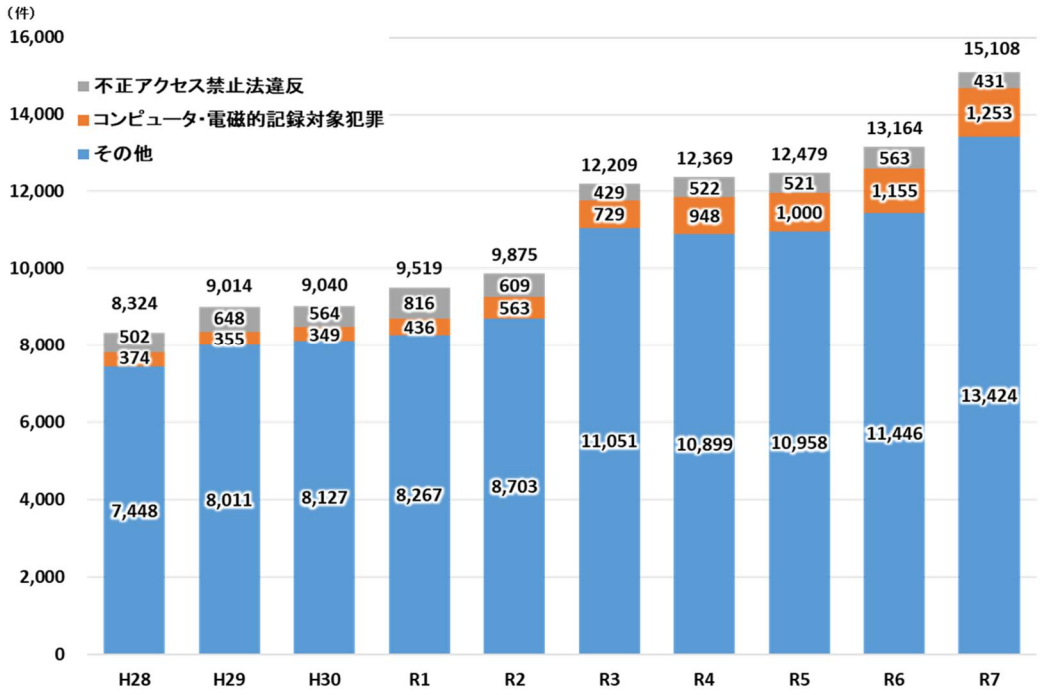
フィッシング報告件数及びクレジットカード不正利用被害額

１　フィッシング報告件数及びクレジットカード不正利用被害額の推移



サイバー犯罪・サイバー事案 ①

１　サイバー犯罪[3]の検挙件数の推移

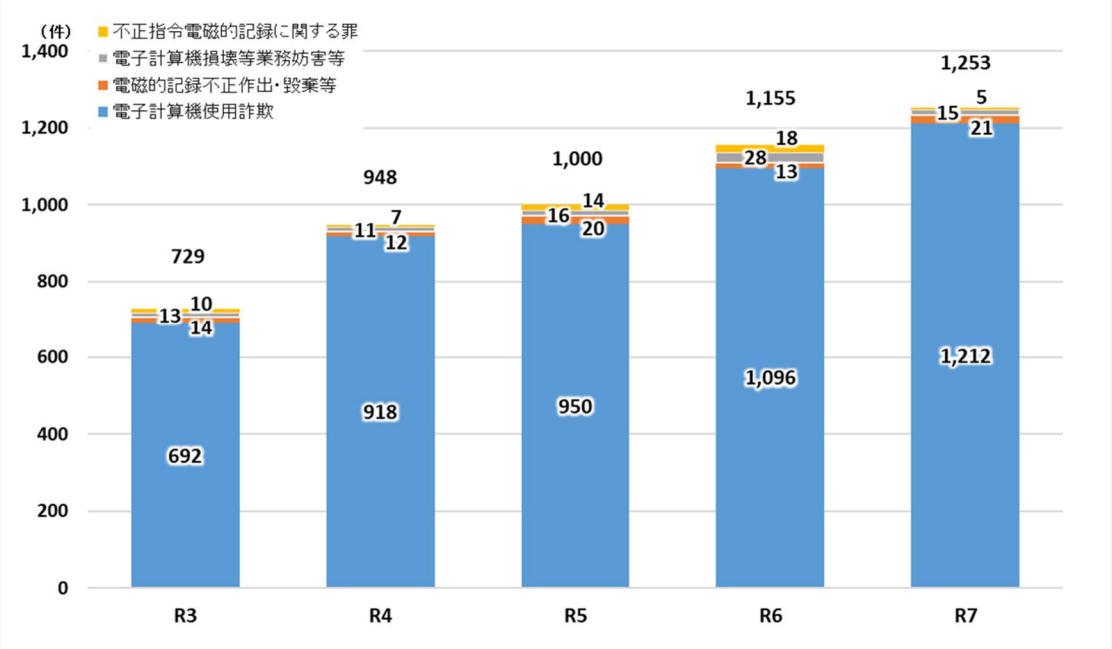


[3] 不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

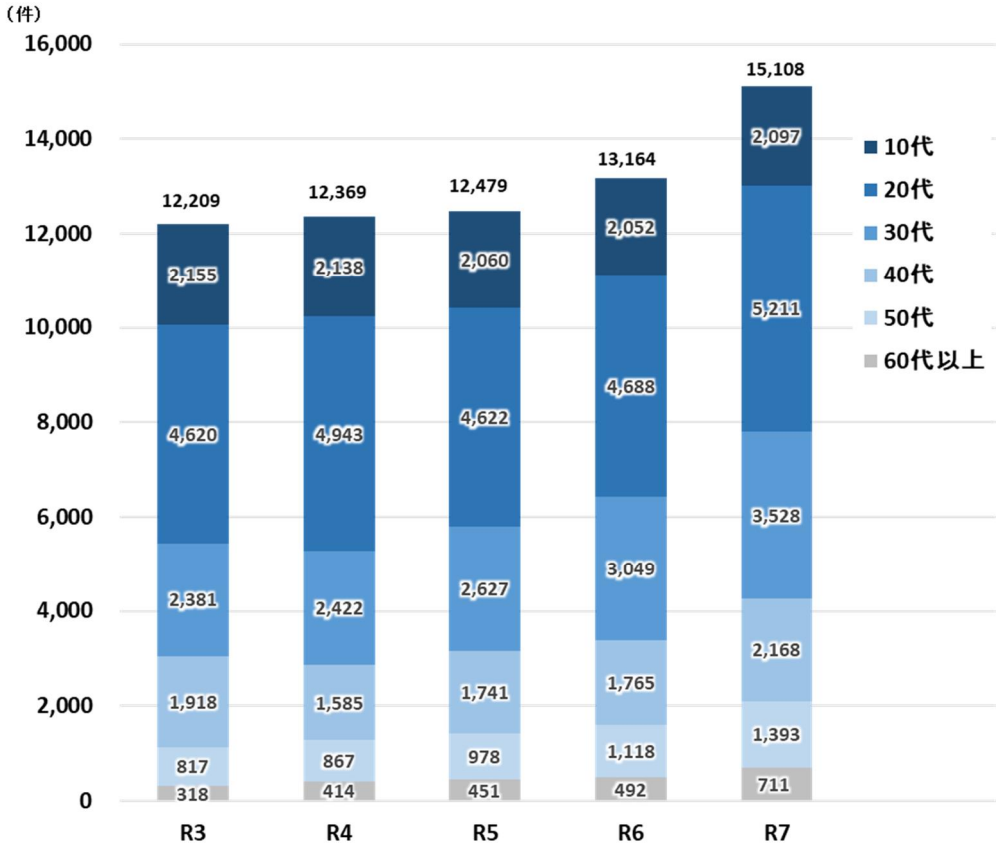
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案 ②

２　前記１中、コンピュータ・電磁的記録対象犯罪の検挙件数の推移



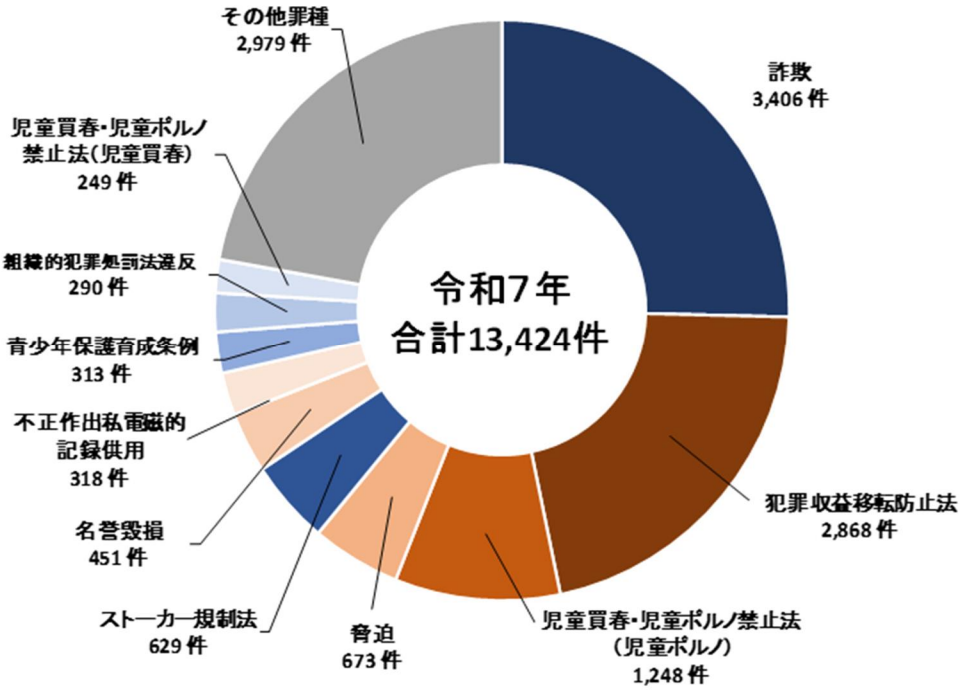
３　サイバー犯罪の検挙数の年齢構成

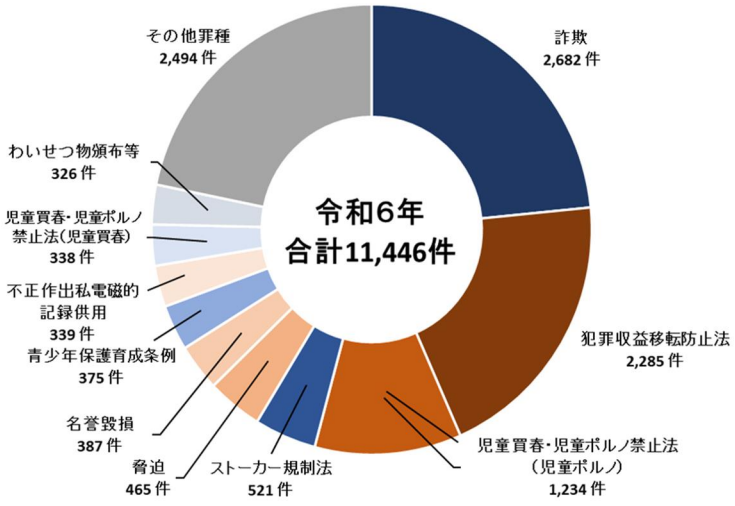


（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案 ③

４　前記１中、「その他」の検挙状況



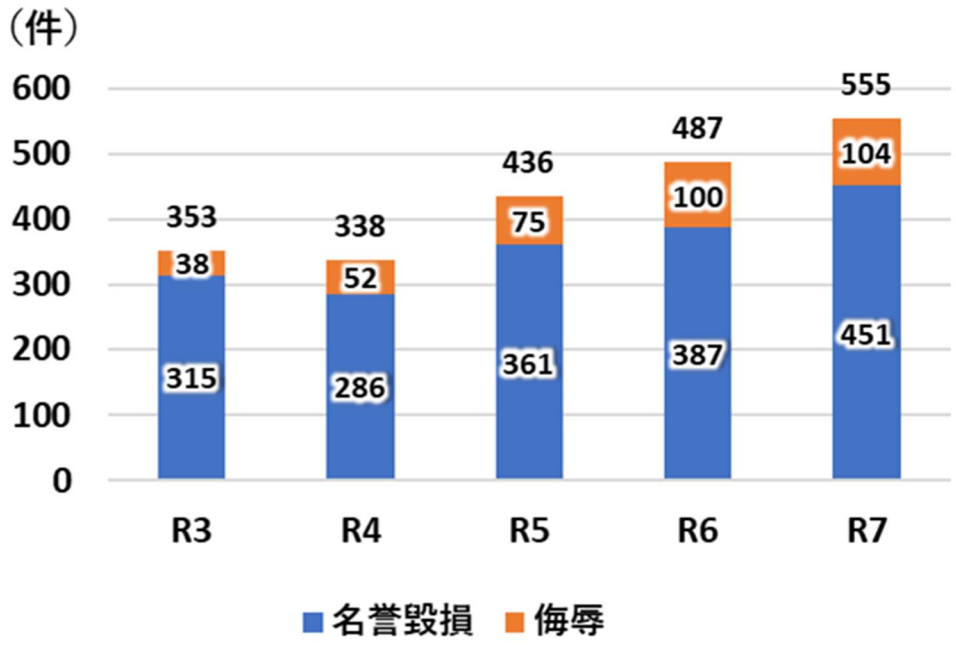


※　前記１中、「その他」の合計値が異なるため、各年の合計数値は異なる。

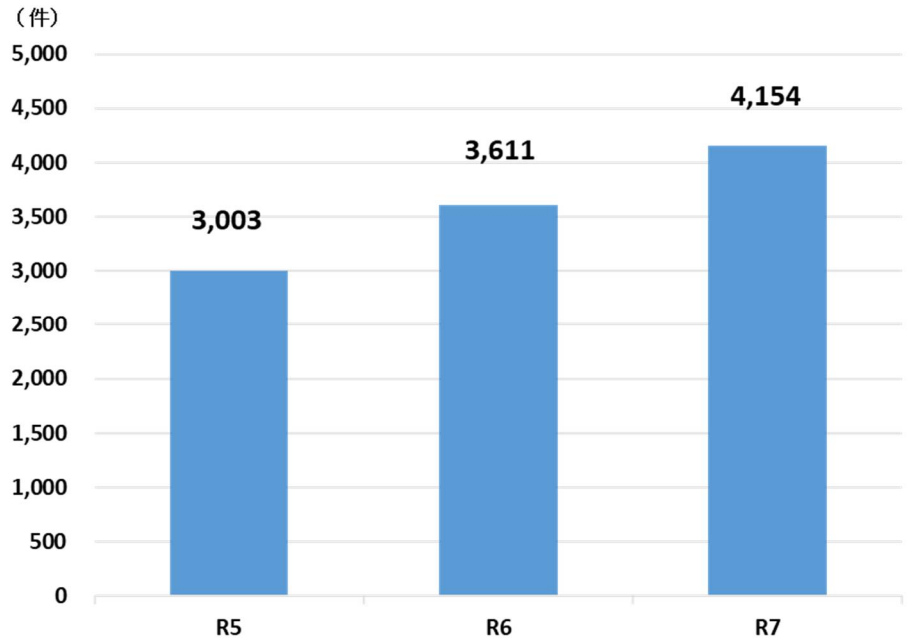
（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案 ④

４　令和７年中のインターネット上での名誉毀損罪及び侮辱罪の検挙件数



５　サイバー事案[4]の検挙件数の推移

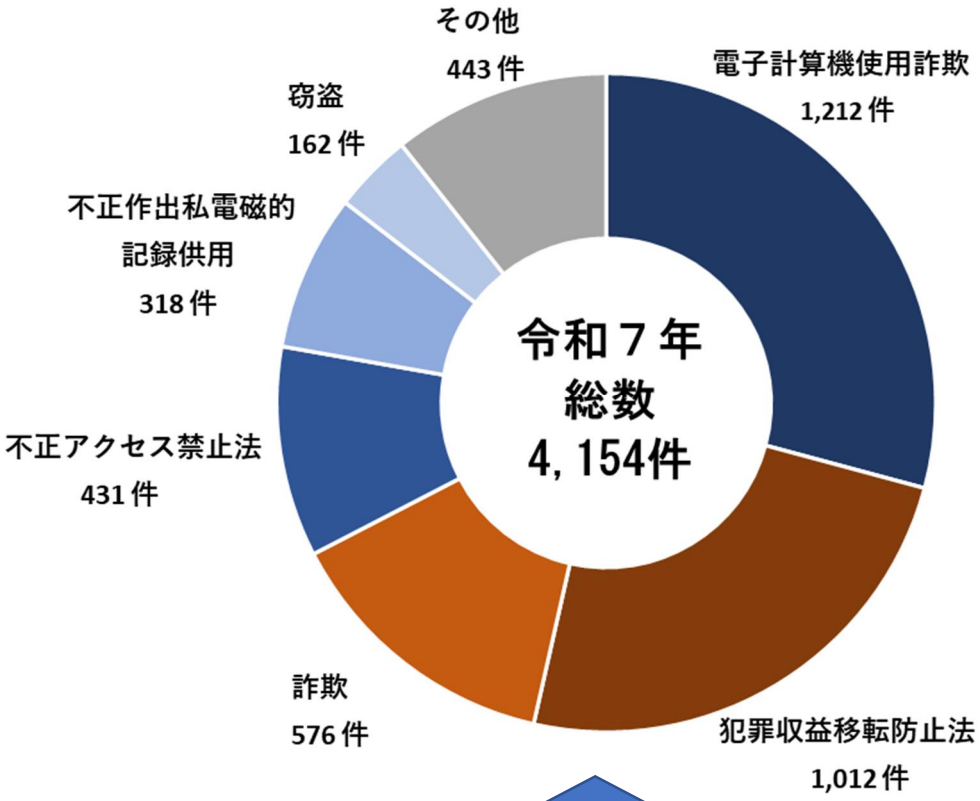


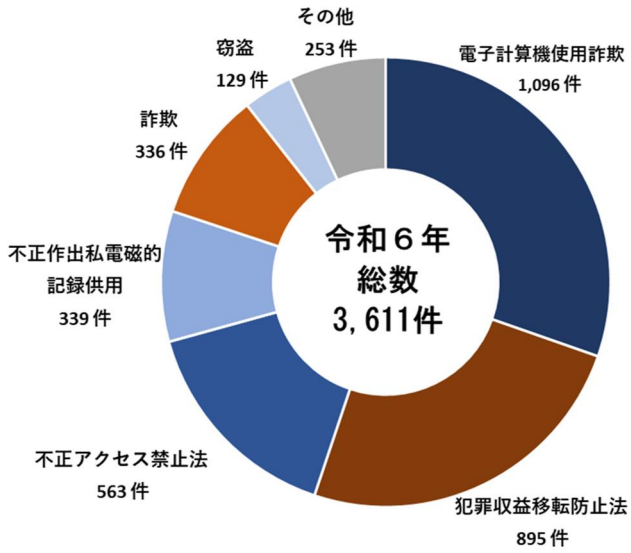
[4] サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。

（第２部１「検挙に向けた取組」関連）

サイバー犯罪・サイバー事案 ⑤

６　サイバー事案の検挙状況



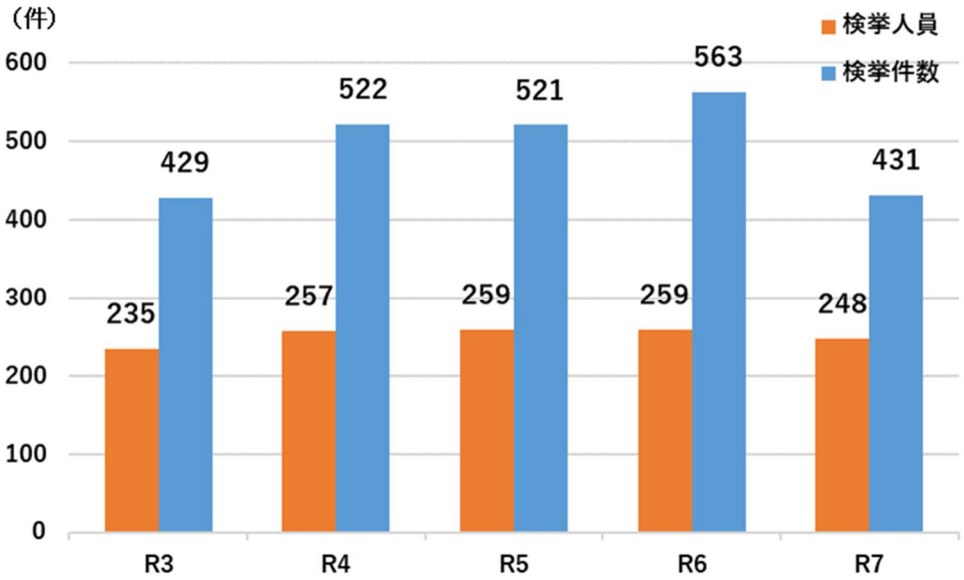


※　検挙総数が異なるため、各年の合計数値は異なる。

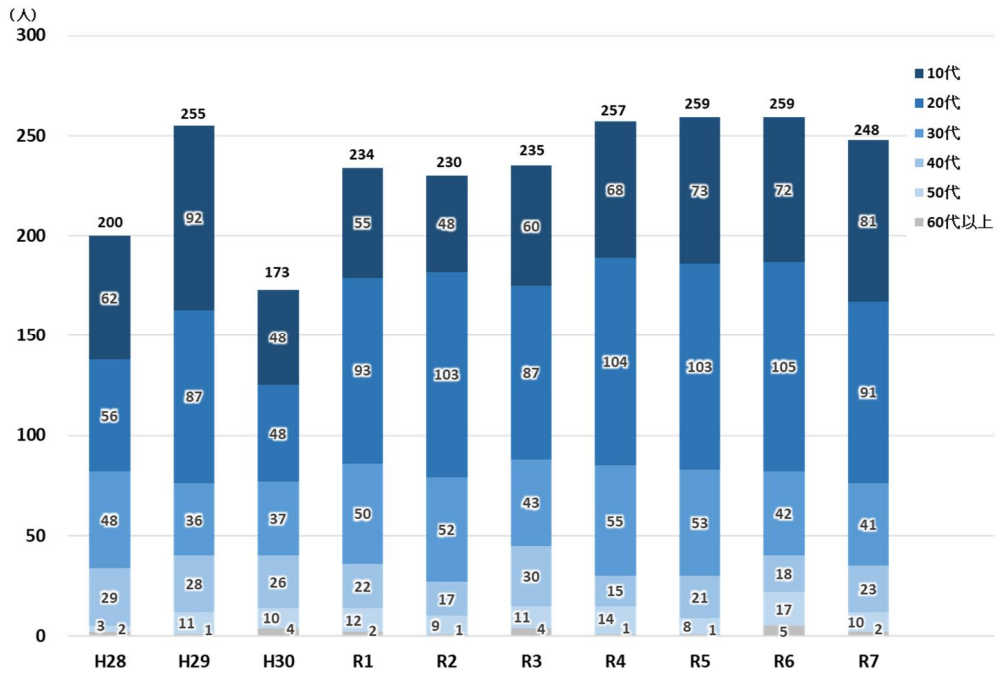
（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ①

７　不正アクセス禁止法違反の検挙件数の推移



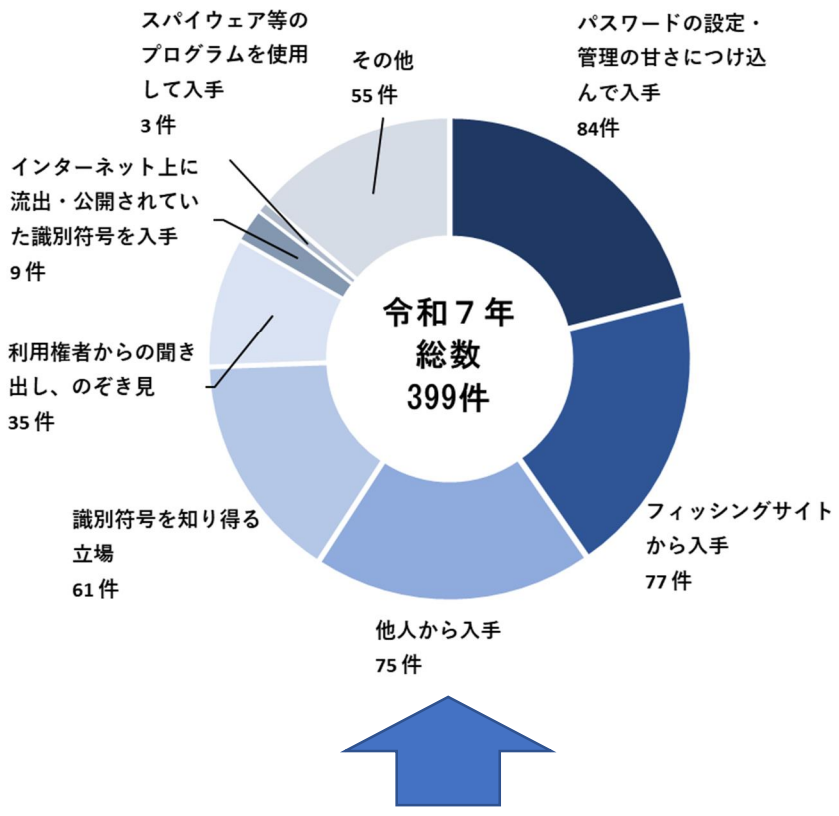
８　不正アクセス禁止法違反の検挙人員の年齢構成

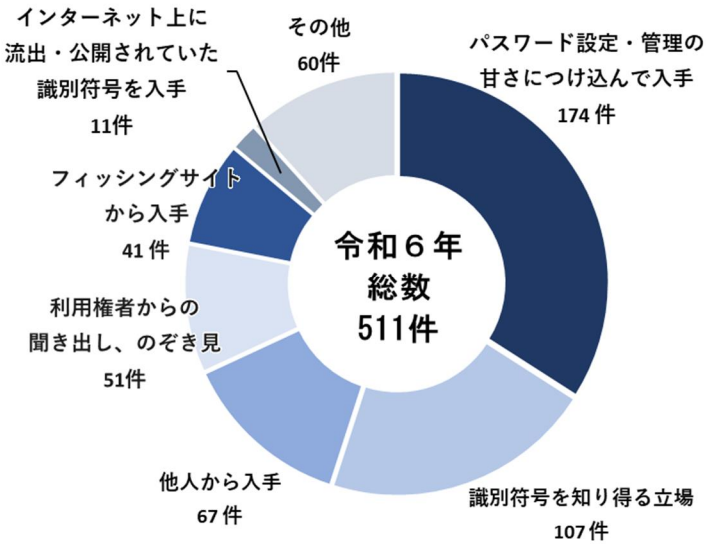


（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ②

９　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



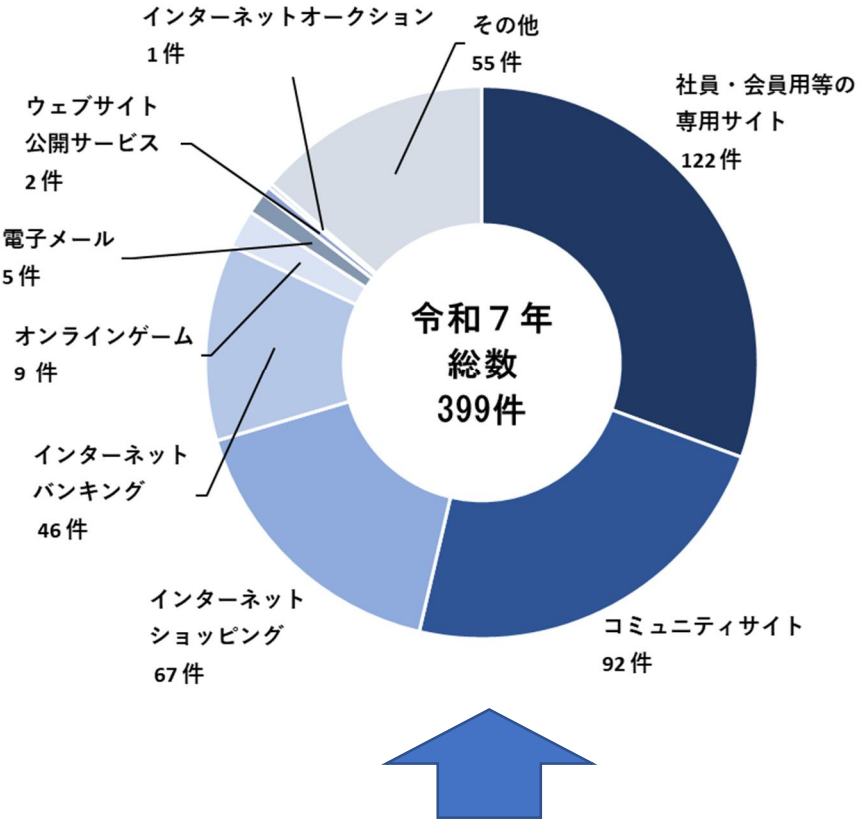


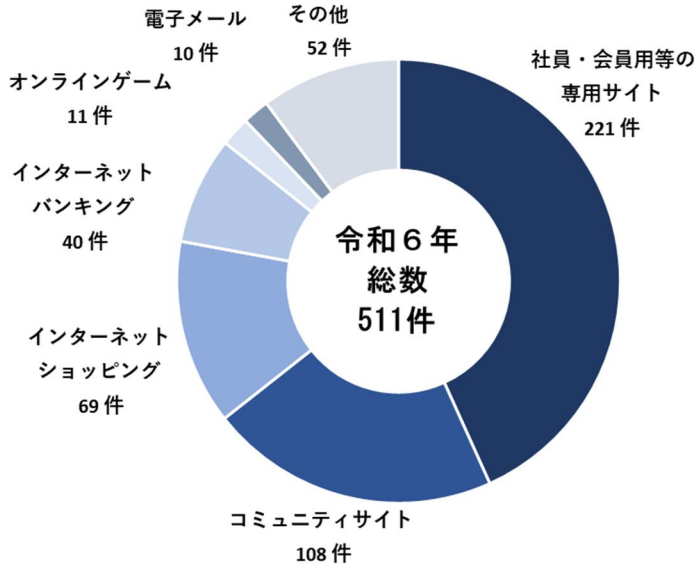
※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ③

10　不正に利用されたサービス別検挙件数（識別符号窃用型）



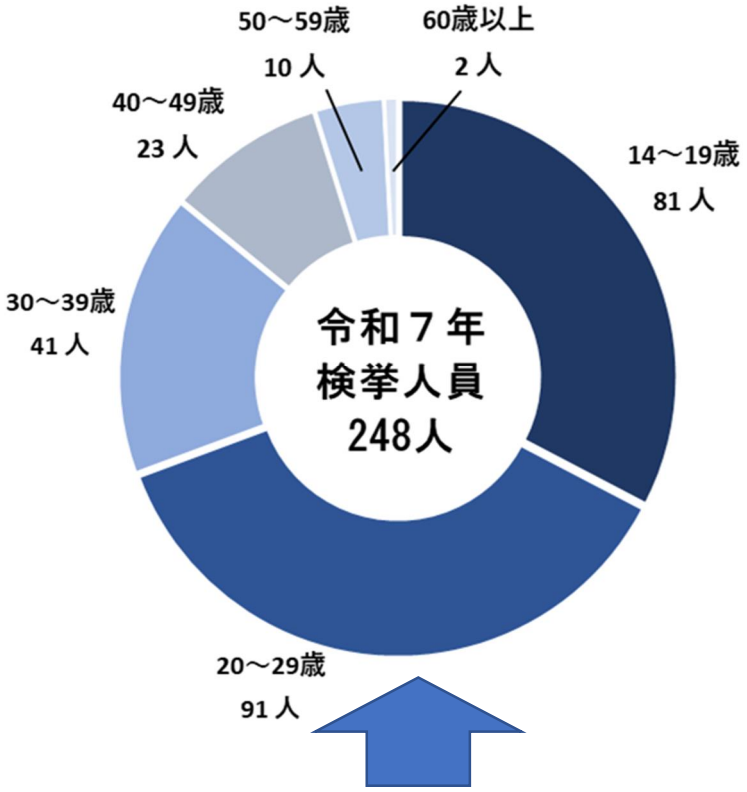


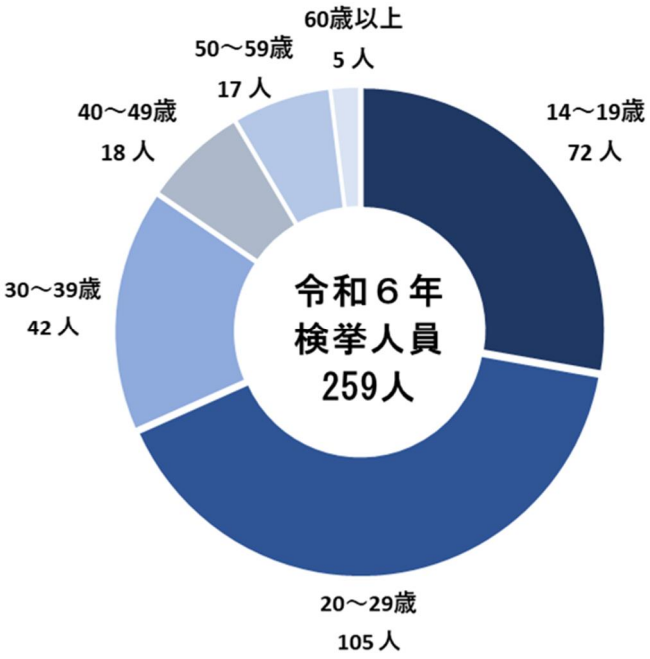
※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ④

11　不正アクセス禁止法違反被疑者の年齢構成



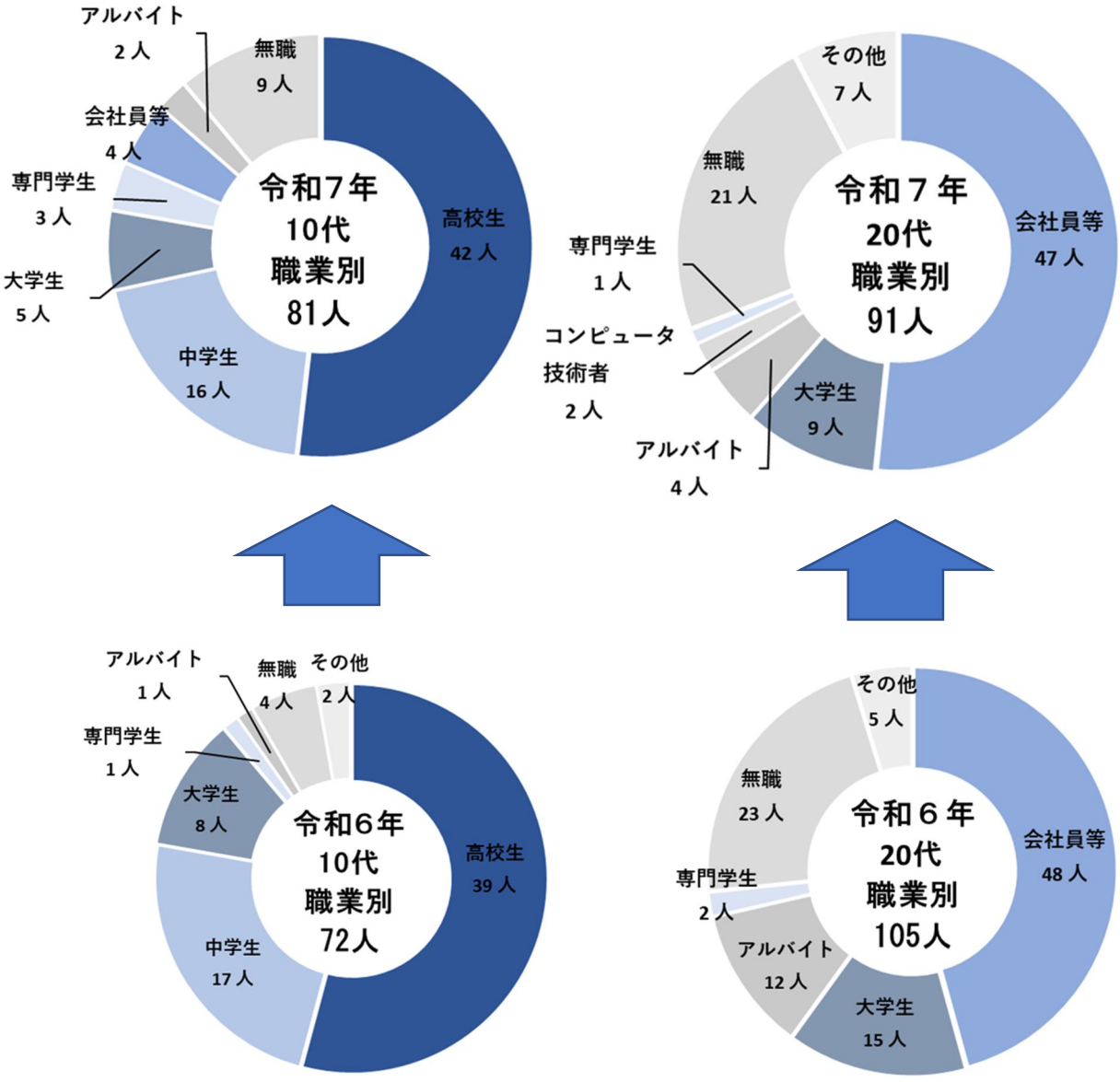


※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ⑤

12　不正アクセス禁止法違反被疑者の 10 代～20 代における職業別

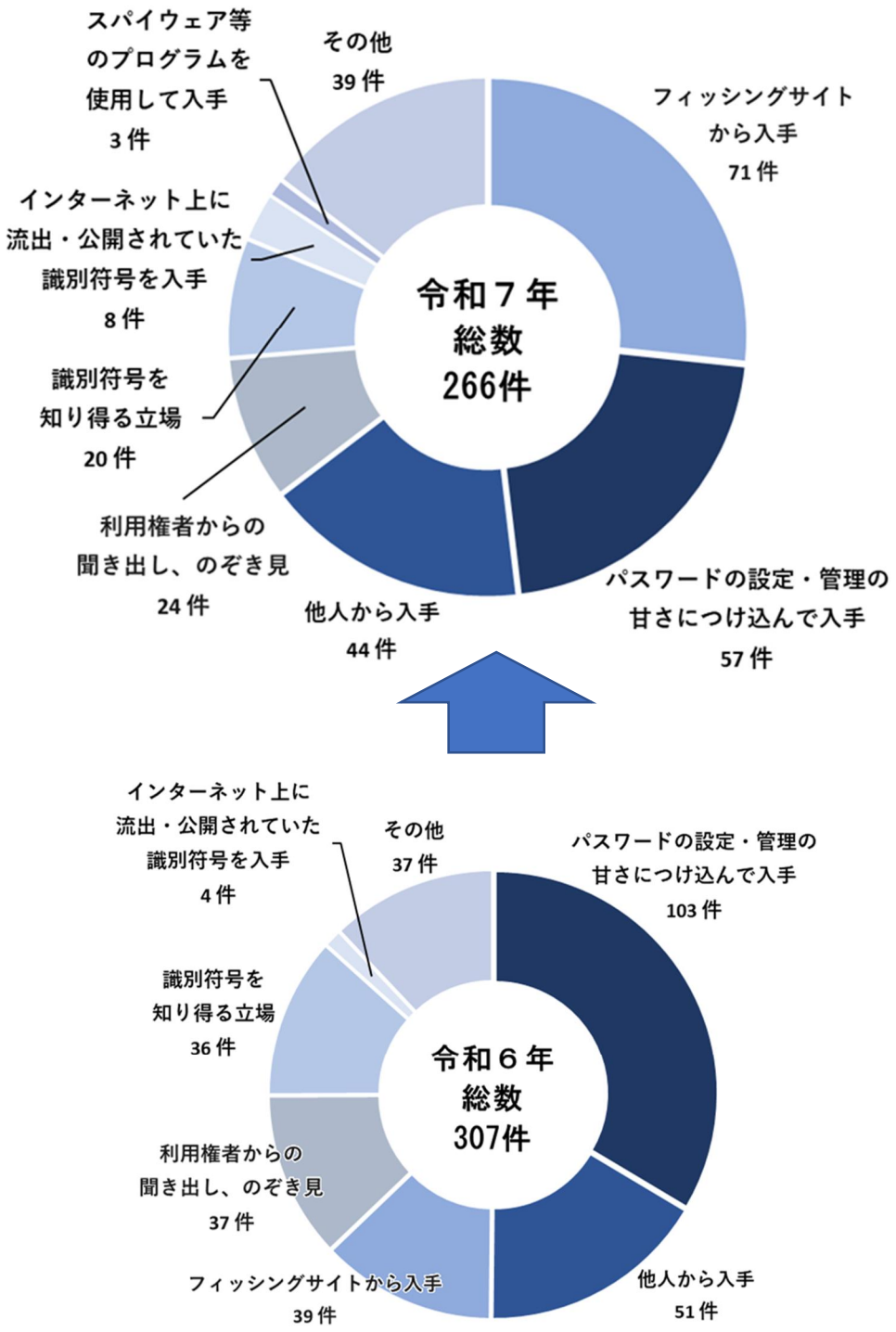


※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ⑥

13　10 代～20 代における不正アクセス行為（識別符号窃用型）に係る手口別検挙件数

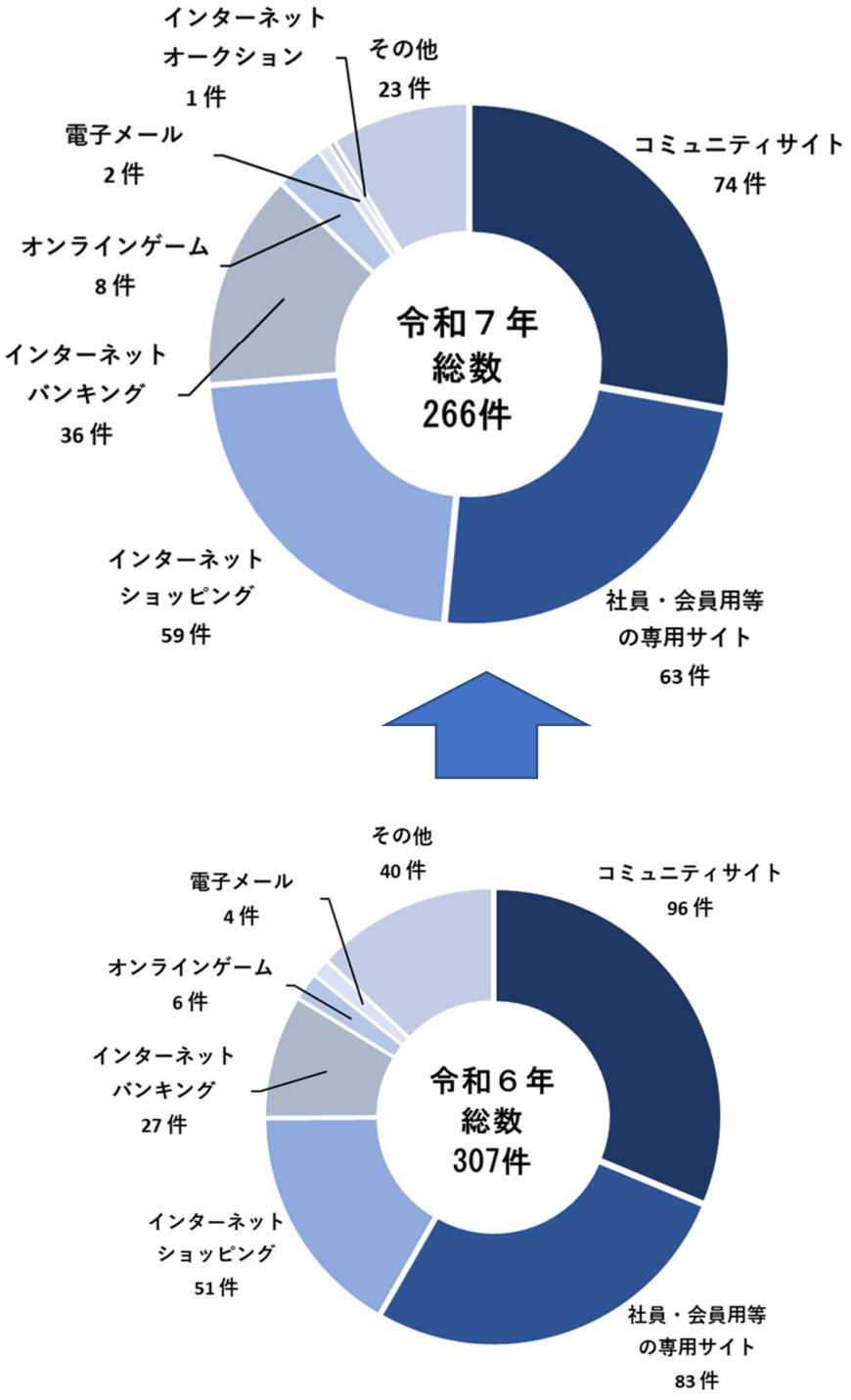


※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部１「検挙に向けた取組」関連）

不正アクセス禁止法違反 ⑦

14　10 代～20 代における不正に利用されたサービス別検挙件数（識別符号窃用型）の推移

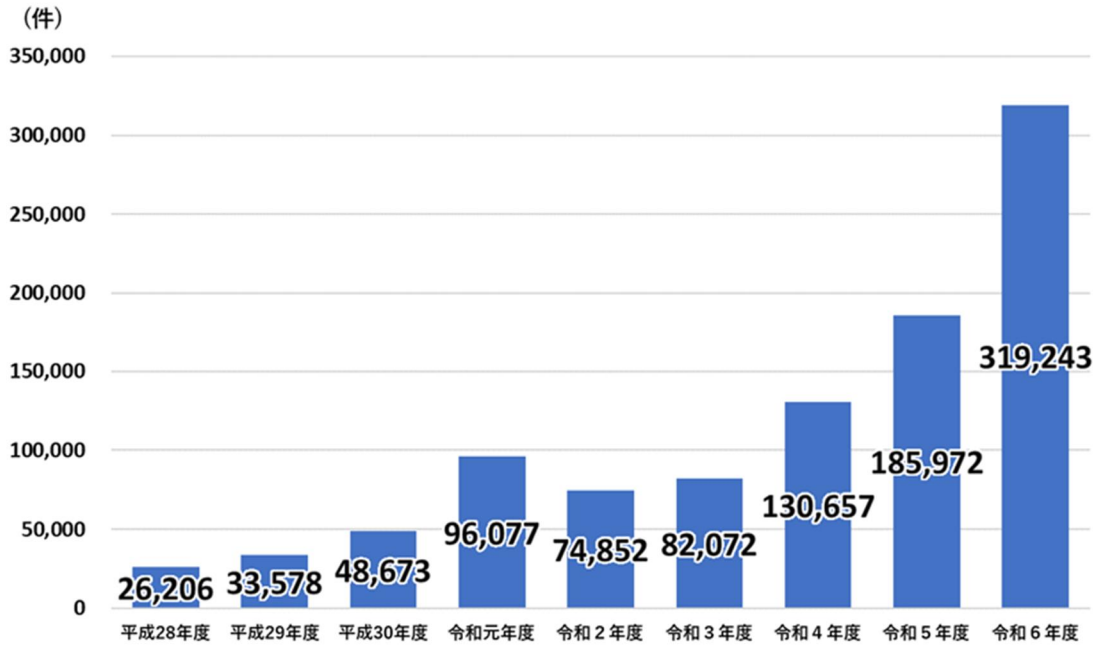


※　検挙した総数が異なるため、各年の合計数値は異なる。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

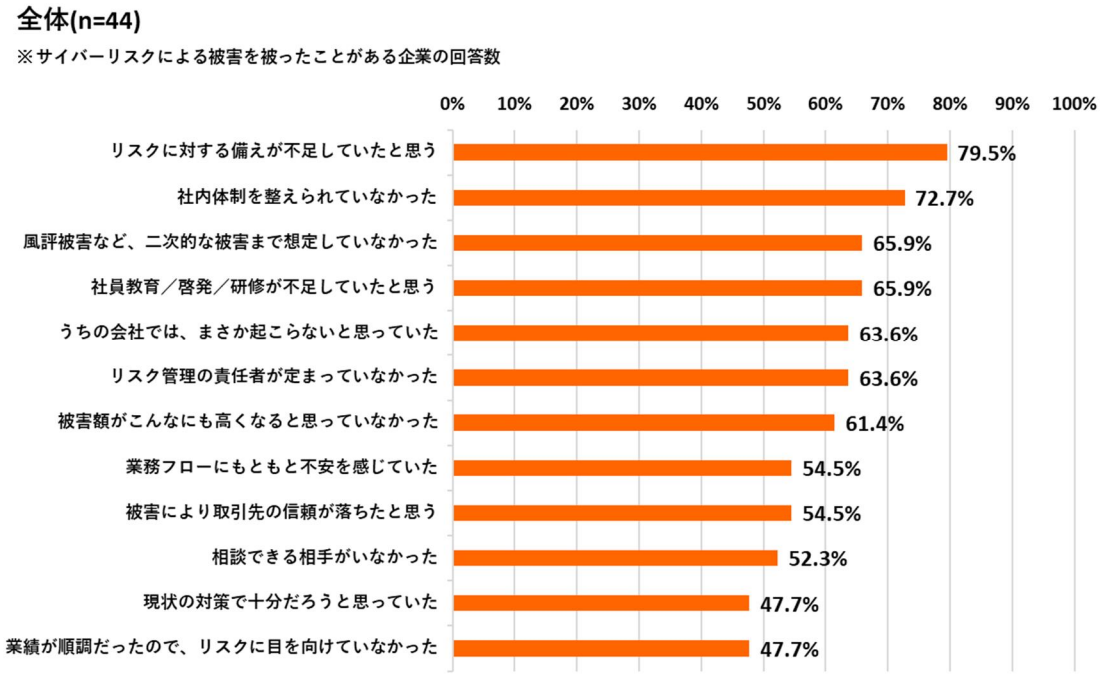
サイバー保険契約に関する日本損害保険協会による調査結果

１　サイバー保険の契約件数の推移



※一般社団法人日本損害保険協会の調査による。

２　サイバーリスクによる被害にあった企業の認識

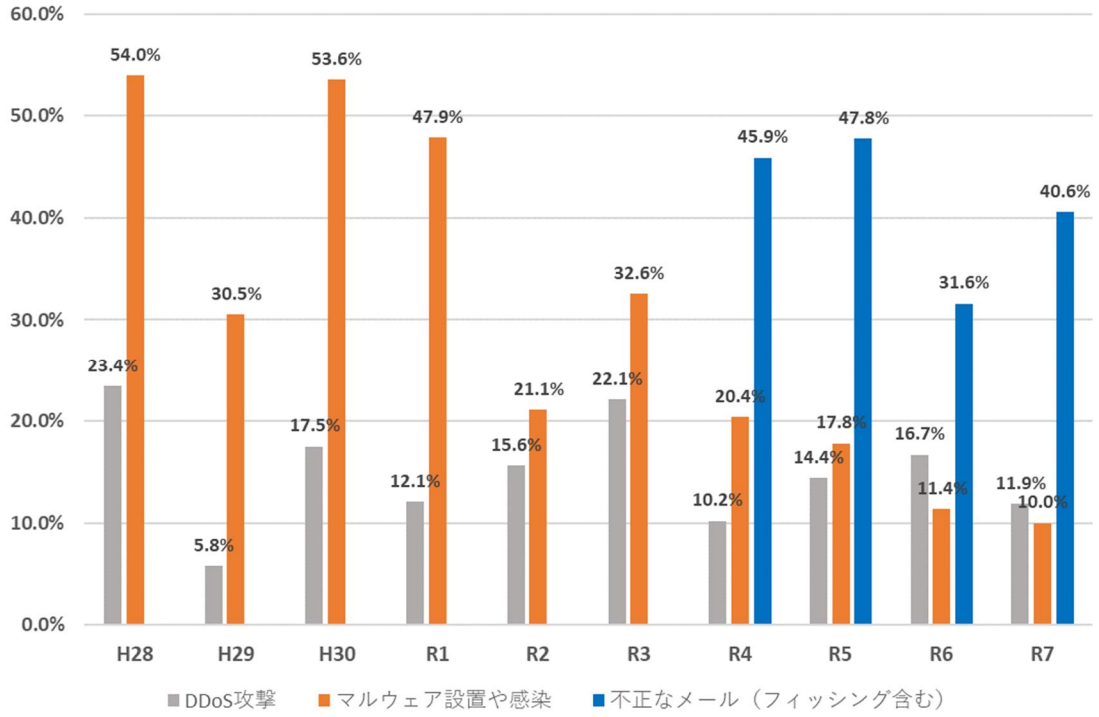


※一般社団法人日本損害保険協会の調査による。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

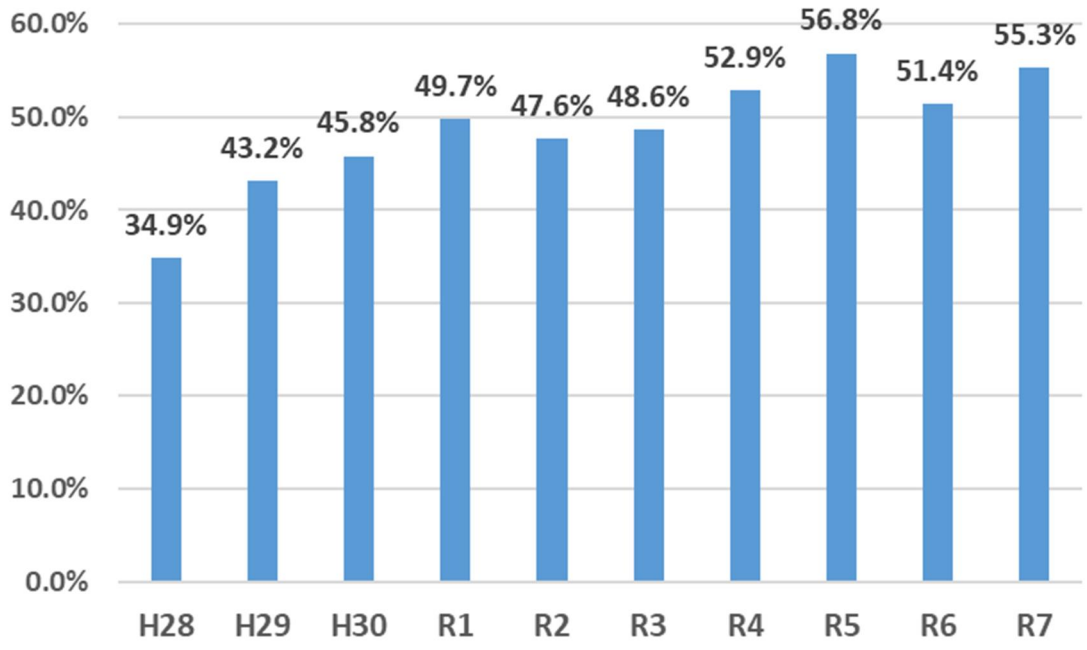
民間企業等における不正アクセス行為対策等調査結果

１　過去１年間に受けたことのある攻撃



※不正なメールは令和４年から調査項目に追加

２　情報セキュリティ侵害事案発生時の対応マニュアル策定状況

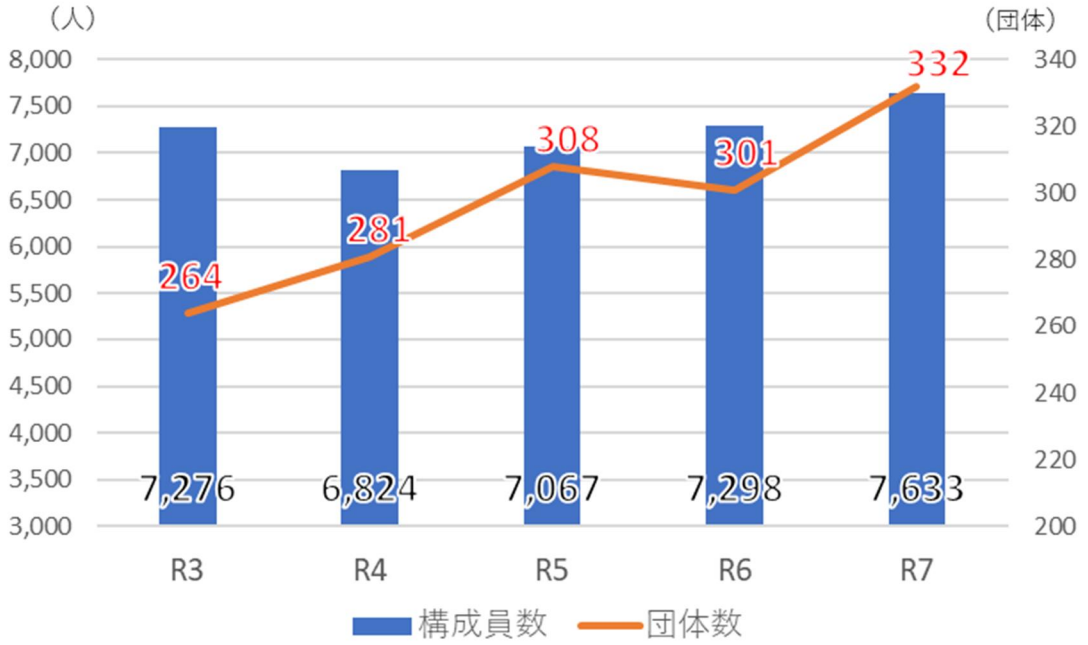


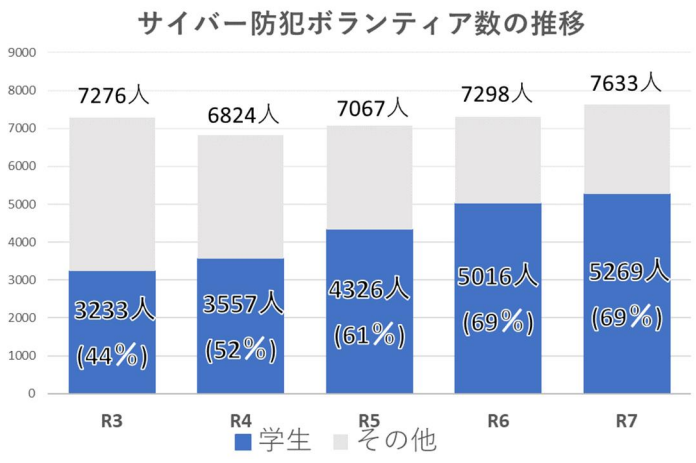
統計編

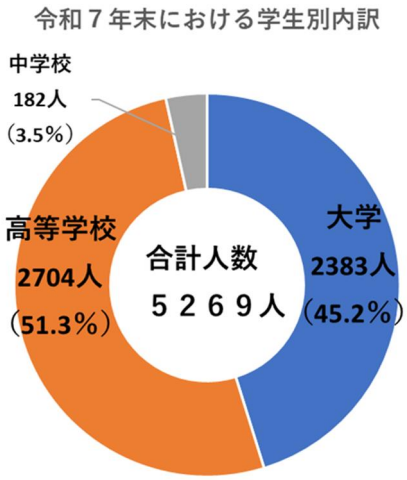
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

サイバー防犯ボランティア団体数及び構成員数の推移

１　サイバー防犯ボランティア団体数及び構成員数の推移







（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

インターネット・ホットラインセンターに関する統計 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１月１日現在

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

【振り込め詐欺等関連情報】
- 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

【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

【犯罪実行者募集関連情報】
- 犯罪実行者の募集

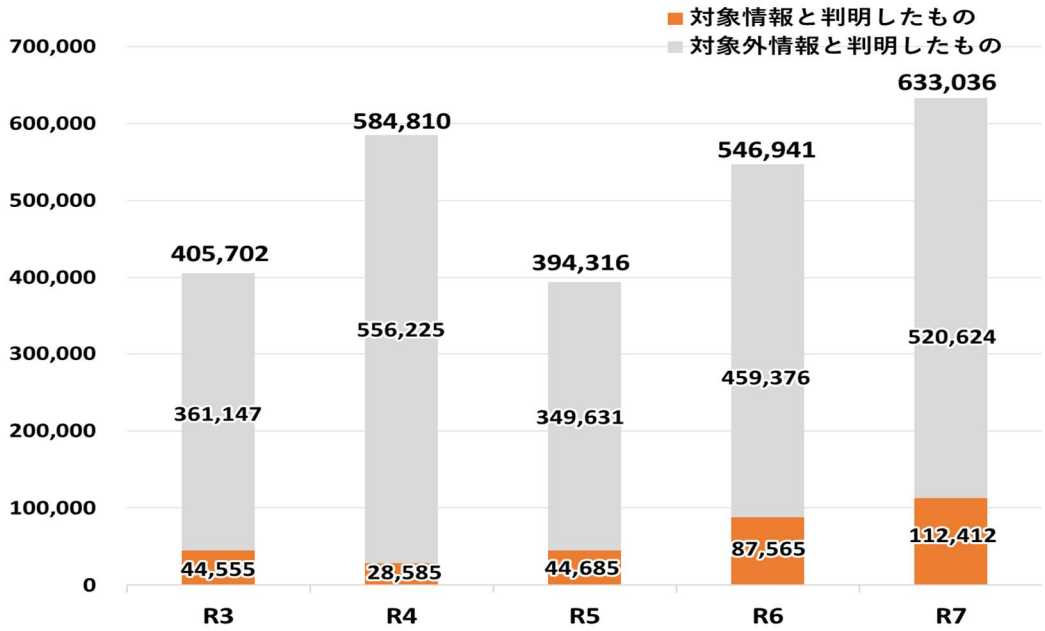
【違法オンラインギャンブル等関連情報】
- 国内にある不特定の者に対し違法オンラインギャンブル等ウェブサイト又は違法オンラインギャンブル等プログラムを提示する行為
- インターネットを利用して国内にある不特定の者に対し違法オンラインギャンブル等に誘導する情報を発信する行為

【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
- 臓器売買
- 人身売買
- 硫化水素ガスの製造
- ストーカー行為等

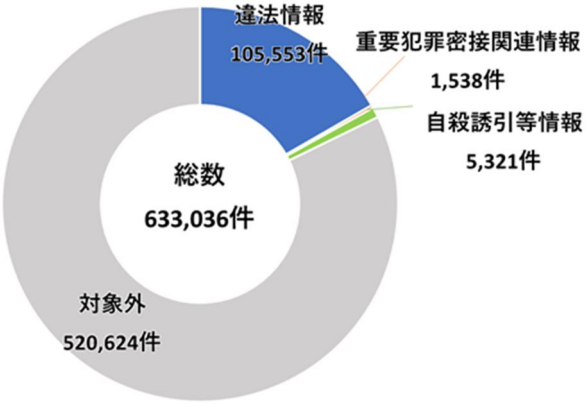
１　違法情報等の分析件数の推移



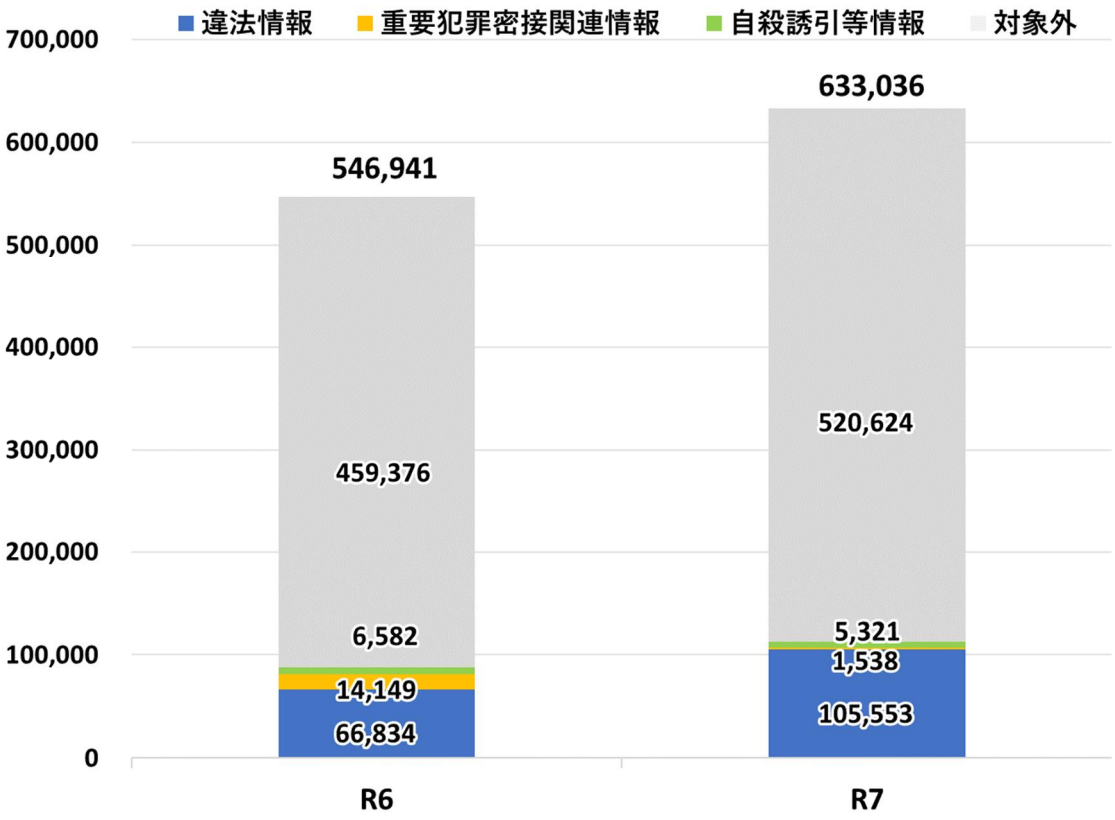
（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

インターネット・ホットラインセンターに関する統計②

２　分析結果[5]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。

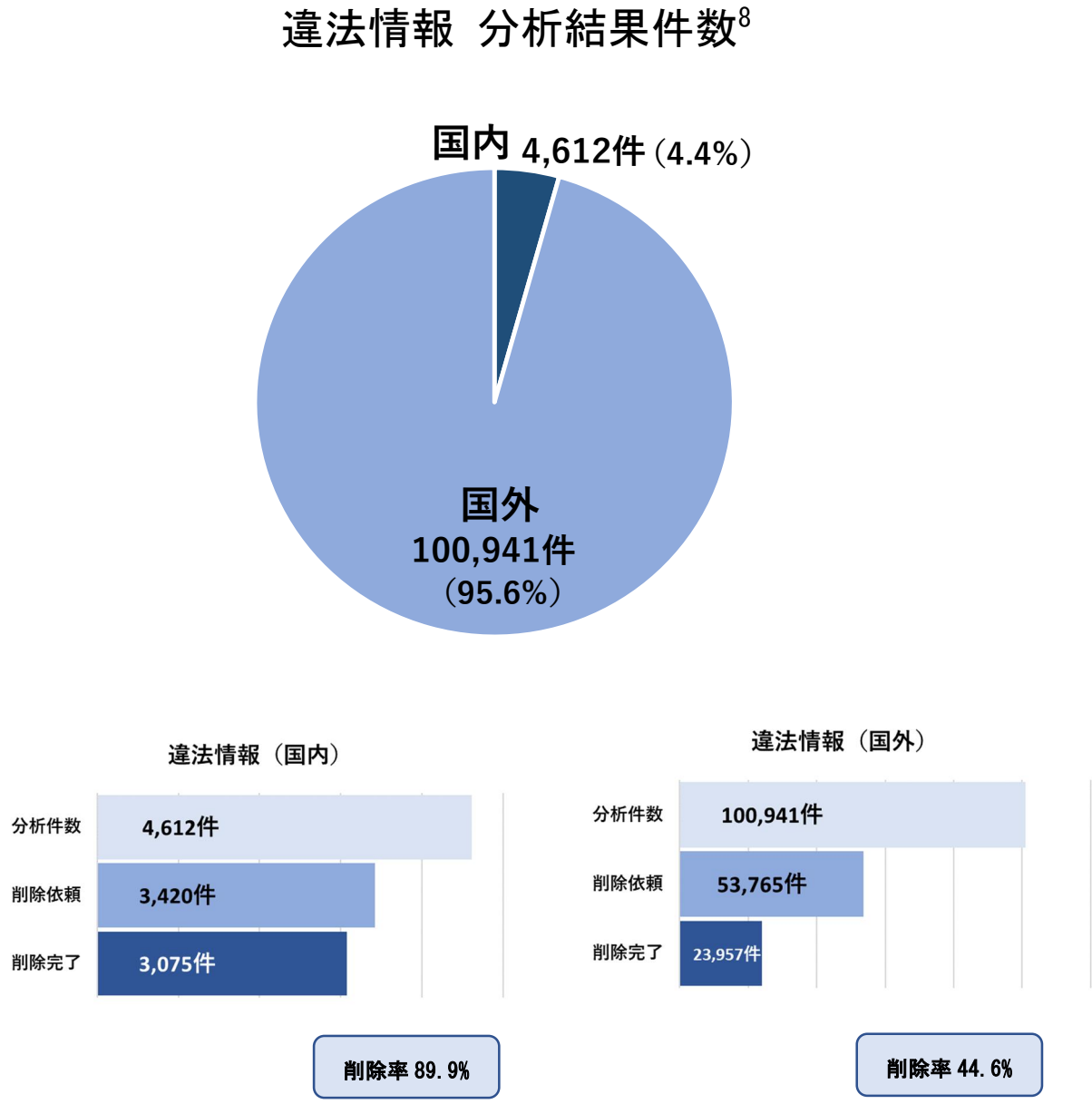


[5] インターネット・ホットラインセンターにおいて運用ガイドラインに基づいて分析した結果、「違法情報」又は「重要犯罪密接関連情報」若しくは「自殺誘引等情報」として分類された件数。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

インターネット・ホットラインセンターに関する統計③

３　分析結果件数と処理結果[6] [7]



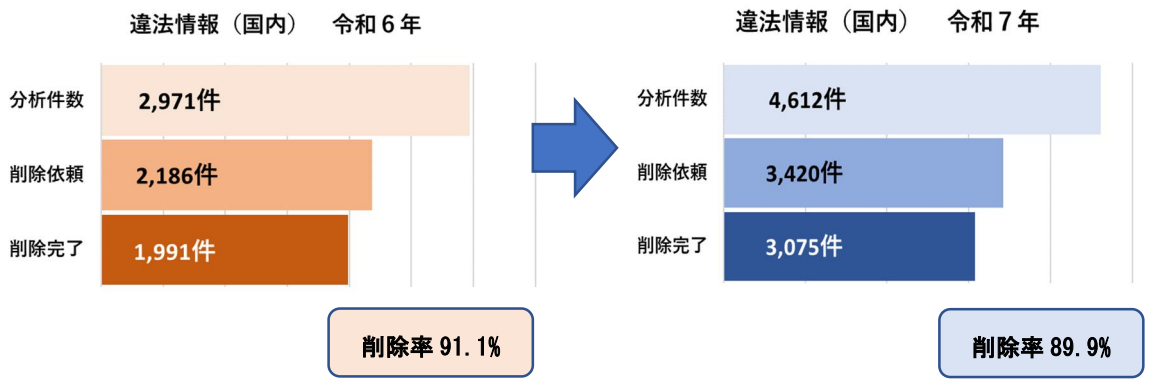
[6] 削除完了の件数については、削除依頼から５営業日後に確認した際の件数。

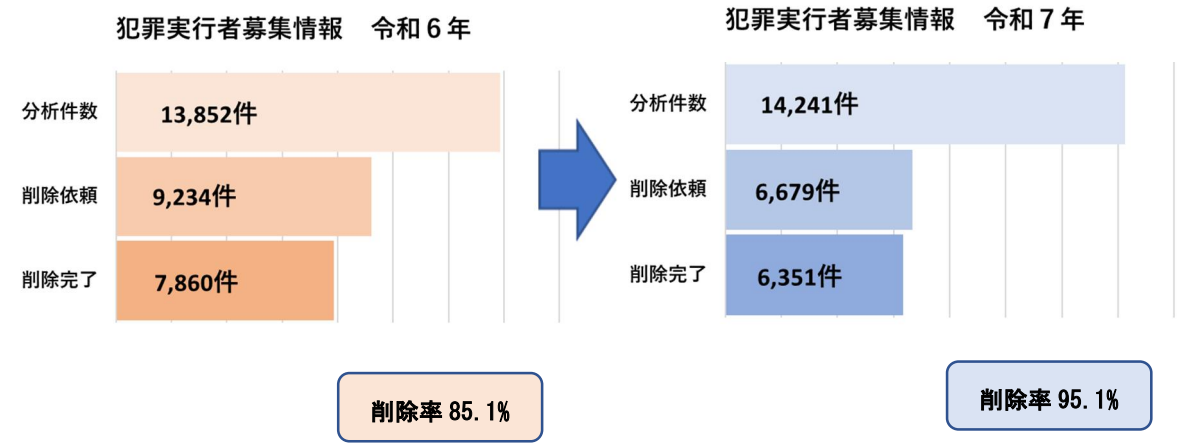
[7] 警察が行うリプライ警告等により、削除依頼前に削除されるものもあるため、削除依頼に至らないものがある。

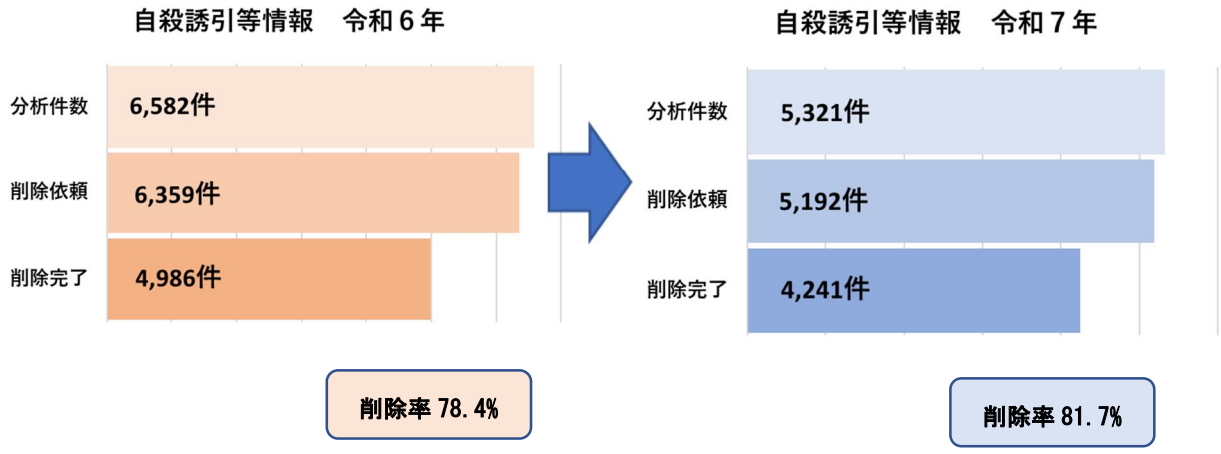
[8] 「国外」とは、プロバイダ等の所在地が不明又は国外に所在し、かつ国外に所在するサーバに蔵置されている場合をいい、「国内」とは、情報が日本国内のプロバイダ及びウェブサイト等に係るものである場合をいう。

（第２部２「被害の未然防止・拡大防止に向けた取組」関連）

インターネット・ホットラインセンターに関する統計④

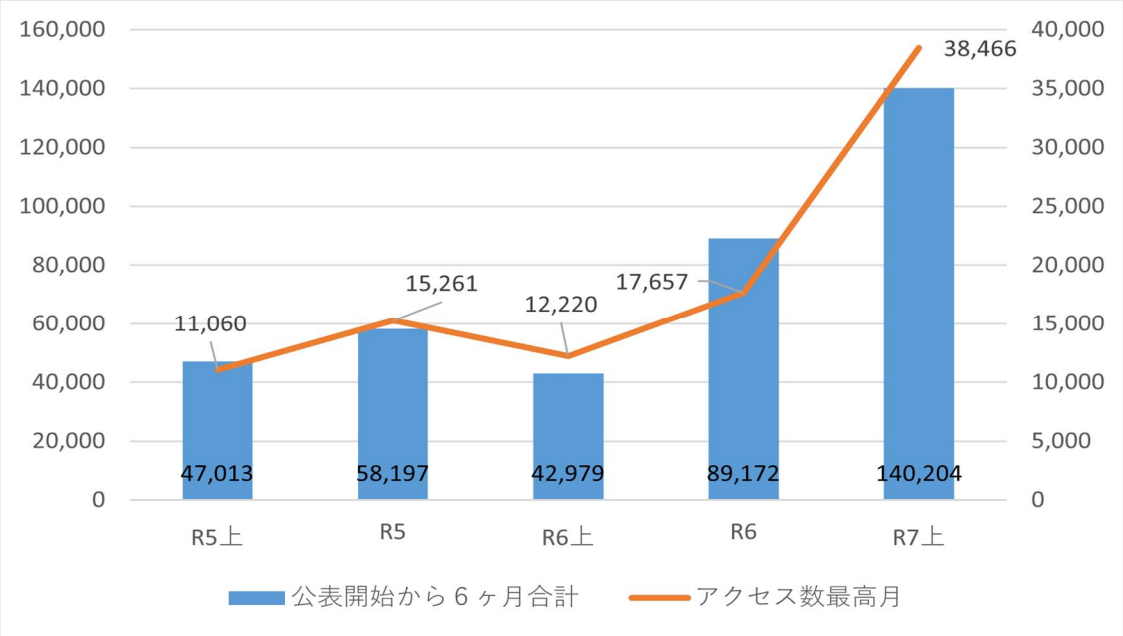






（その他）

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」へのアクセス数推移



※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）

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。

令和７年中に公表した「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」及び「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」へのアクセス数は右肩上がりであり、国民からの関心が高くなっていることが認められる。

特に、令和７年９月に公表した「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」にあっては、同年 10 月に月間アクセス数 38,466 件を記録したところであるが、これは、同年９月末と同年 10 月に国内大手企業で立て続けにランサムウェア事案が発生したことに伴い、ランサムウェア等のサイバー空間における脅威に対する国民からの関心が一層高まったことが関係しているとも考えられる。