サイバー空間の安全の確保

第3章
CHAPTER 3

第1節 サイバー空間における脅威

サイバー空間は、地域や年齢、性別を問わず、全国民が参加し、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、金融、航空、鉄道、医療等といった国民生活や社会経済活動を支える基盤となる機能から、警察や防衛といった治安や安全保障に関わる国家機能に至るまで、あらゆる場面で実空間とサイバー空間との融合が進んでいる。

こうした中、政府機関、交通機関、金融機関等の重要インフラ事業者等に対するDDoS攻撃(注1)によるものとみられる被害が確認されるとともに、情報窃取を目的としたサイバー攻撃や国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案、生成AI等の高度な技術を悪用した事案等が発生しているほか、企業・団体等の事業活動に大きな影響を与えるランサムウェア被害も相次いでいる。また、クレジットカード不正利用被害が過去最多となっているほか、インターネットバンキングに係る不正送金被害が引き続き高水準で推移している。さらに、インターネット上では児童ポルノや規制薬物の広告等の違法情報や、自殺誘引等情報(注2)、爆発物・銃砲等の製造方法、殺人や強盗の請負等の有害情報が氾濫するなど、サイバー空間をめぐる脅威は、引き続き極めて深刻な情勢にある。

1 サイバー事案等の検挙状況

（1）サイバー事案(注3)の検挙件数

令和６年（2024年）中のサイバー事案の検挙件数は、3,611件であった。

（2）不正アクセス禁止法違反

令和６年中の不正アクセス禁止法違反の検挙件数は563件と、前年より42件（8.1％）増加し、検挙人員は259人と、前年と同数であった。不正アクセス禁止法違反として検挙した不正アクセス行為の手口別内訳をみると、他人の識別符号を無断で入力する「識別符号窃用型」が511件（90.8％）と最多であった。

また、令和６年中の不正アクセス行為の認知件数(注4)は5,358件であり、これを不正アクセス行為後の行為別にみると、「インターネットバンキングでの不正送金等」が4,342件（81.0％）と最多であった。

（3）コンピュータ・電磁的記録対象犯罪(注5)

令和６年中のコンピュータ・電磁的記録対象犯罪の検挙件数は1,155件と、前年より155件（15.5％）増加した。

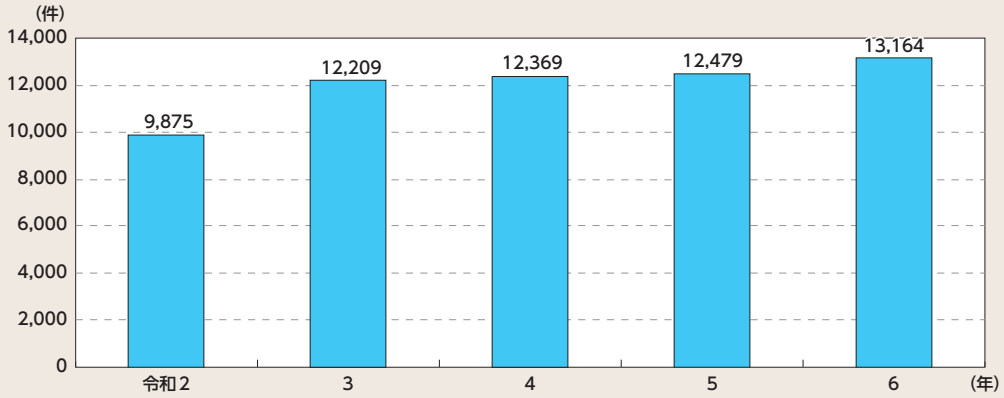
（4）サイバー犯罪(注6)の検挙件数の推移

最近５年間のサイバー犯罪の検挙状況は、図表３－１のとおりである。

サイバー犯罪の検挙件数は増加傾向にあり、令和６年中の検挙件数は１万3,164件と、前年より685件（5.5％）増加し、過去最多を記録した。

注１：Distributed Denial of Serviceの略。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
２：他人を自殺に誘引・勧誘する情報等
３：サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案。サイバー事案への対策については121頁参照
４：不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を認知した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合その他関係資料により不正アクセス行為の事実を確認することができた場合において、被疑者が行った犯罪構成要件に該当する行為の数
５：刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪
６：不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

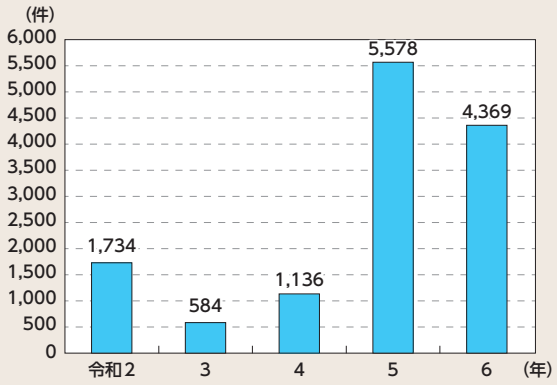
図表３－１　サイバー犯罪の検挙件数の推移（令和２年～令和６年）



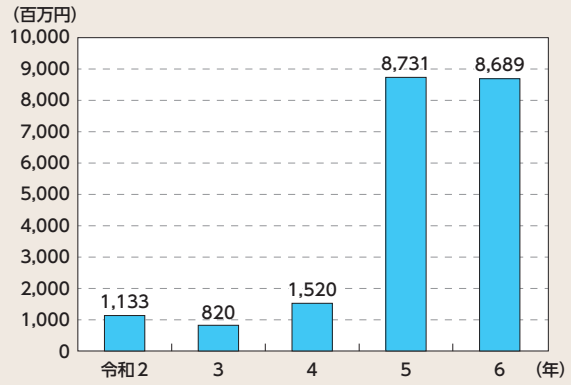
2　インターネットバンキングに係る不正送金事犯の情勢

令和６年におけるインターネットバンキングに係る不正送金事犯の発生件数は4,369件、被害額は約86億8,900万円と、過去最高であった前年に比べ、それぞれ減少した。その被害の多くは、金融機関等を装ったフィッシング(注)によるものと考えられる。

図表３－２　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の推移（令和２年～令和６年）



図表３－３　インターネットバンキングに係る不正送金事犯の被害額の推移（令和２年～令和６年）

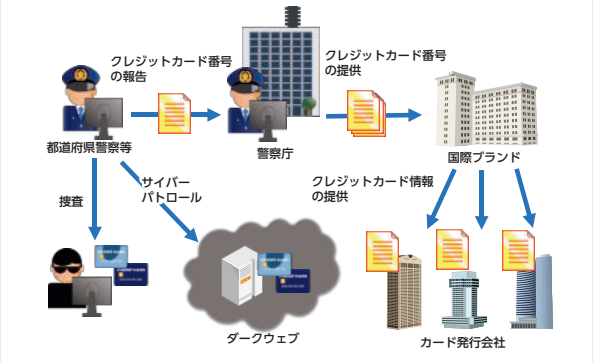


memo　不正に入手されたクレジットカード番号の国際ブランドへの提供

フィッシングは、クレジットカード番号等の窃取にも用いられ、クレジットカードの不正利用被害にもつながっている。

警察では、クレジットカードの不正利用被害の拡大防止のための取組を推進しており、令和６年12月には、「国民を詐欺から守るための総合対策」（令和６年６月18日犯罪対策閣僚会議決定）においてクレジットカード不正利用情報提供の効率化が掲げられたことを踏まえ、各都道府県警察が捜査等を通じて把握したクレジットカード番号を警察庁で集約し、カード発行会社を含む決済システム全体を統括する国際ブランド各社にそれぞれ一括して提供する仕組みを構築した。

図表３－４　国際ブランドに対する不正クレジットカード番号の提供による被害拡大防止



注：実在する企業・団体等や官公庁を装うなどしたメール又はショートメッセージサービスを送り、その企業等のウェブサイトに見せかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するように誘導し、当該フィッシング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

3 ランサムウェアの情勢

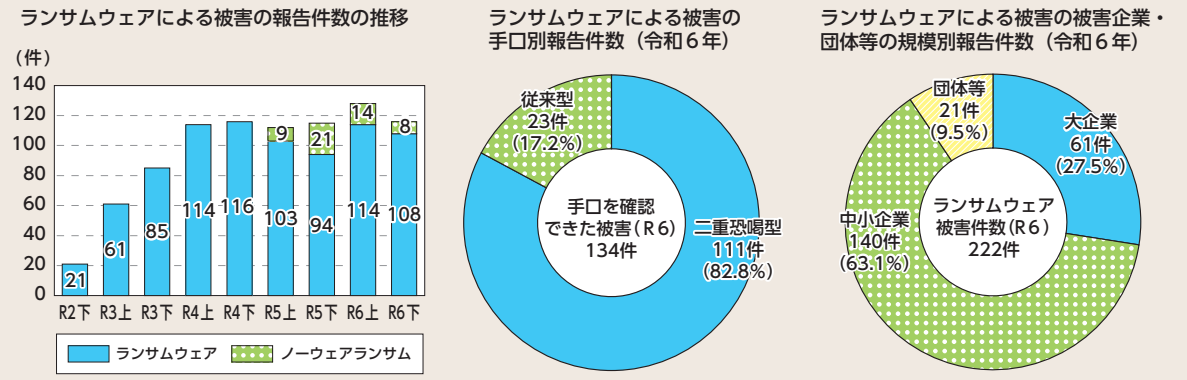
令和６年中のランサムウェアによる被害の報告件数(注１)は222件（令和６年上半期114件、下半期108件）であり、引き続き高い水準で推移している。こうした被害において、暗号化したデータを復元する対価として企業等に金銭等を要求する手口のほか、データを企業等から窃取した上で「対価を支払わなければ当該データを公開する」などと対価を要求する手口であるダブルエクストーション（二重恐喝）が認められる。対価を要求する手口を警察として確認したランサムウェアによる被害の報告件数134件のうち、ダブルエクストーション（二重恐喝）の手口によるものは111件であり、82.8％を占めている。

また、ランサムウェアによる被害の報告件数を被害企業・団体等の規模別(注２)にみると、大企業は61件、中小企業は140件と、企業・団体等の規模を問わず被害が発生している。

さらに、企業・団体等におけるランサムウェア被害の実態を把握するため、被害企業・団体等を対象としてランサムウェアの感染経路に関するアンケート調査を実施したところ、有効回答数100件のうち、VPN機器(注３)を利用されて侵入された事例は55件（55.0％）、リモートデスクトップサービス(注４)が利用されて侵入された事例は31件（31.0％）と、テレワークに利用される機器等のぜい弱性や強度の弱い認証用パスワード等の情報を利用して侵入したと考えられるものが大半を占めている。

加えて、企業・団体等のネットワークに侵入し、データを暗号化することなくデータを窃取した上で対価を要求する手口（ノーウェアランサム）による被害が、令和６年中22件確認されている。

図表３－５　ランサムウェアによる被害の報告件数



注１：企業・団体等におけるランサムウェアによる被害として都道府県警察から警察庁に報告のあった件数
２：中小企業基本法第２条第１項に規定する中小企業者の範囲を踏まえて分類した。
３：Virtual Private Networkの略。インターネットや多人数が利用する閉域網を介して、暗号化やトラフィック制御技術により、プライベートネットワーク間が、あたかも専用線接続されているかのような状況を実現するための機器
４：職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータ等から閲覧・操作等できるサービス

4 サイバーテロ・サイバーエスピオナージの情勢

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(注１)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事案が、世界的規模で発生している。

（１）サイバーテロの情勢

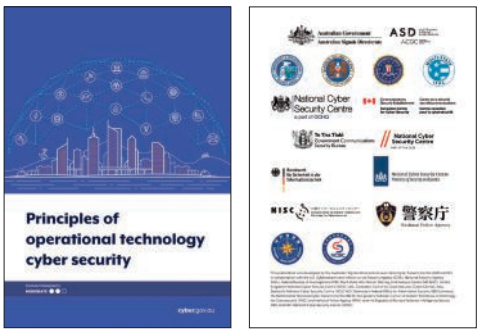
情報通信技術が浸透した現代社会において、重要インフラの基幹システムに対する電子的攻撃は、インフラ機能の維持やサービスの供給を困難とし、国民の生活や社会経済活動に重大な被害をもたらすおそれがある。海外では、電力会社がサイバーテロの被害に遭い、広範囲にわたって停電が発生するなど国民に大きな影響を与える事案が発生している。

（２）サイバーエスピオナージの情勢

近年、情報を電子データの形で保有することが一般的となっている中で、軍事技術への転用も可能な先端技術や、外交交渉における国家戦略等の機密情報の窃取を目的としたサイバーエスピオナージの脅威が世界各国で問題となっている。また、我が国に対するテロの脅威が継続していることを踏まえると、現実空間でのテロの準備行為として、重要インフラ事業者等の警備体制等の機密情報を窃取するためにサイバーエスピオナージが行われるおそれもある。我が国においても、不正プログラムや不正アクセスにより、機密情報が窃取された可能性のあるサイバーエスピオナージ事案が発生している。

memo 「OT(注2)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、内閣サイバーセキュリティセンター（NISC(注3)）のほか、米国や英国をはじめとする関係機関と共に、豪州通信情報局（ASD(注4)）豪州サイバーセキュリティセンター（ACSC(注5)）が策定した文書「OTサイバーセキュリティの原則」の共同署名に加わった。本文書は、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）の管理等に係る意思決定を行う際に、指針とするべき６つの原則をその具体例と共に示し、事業者をサイバーセキュリティの観点から支援することを目的としている。



「OTサイバーセキュリティの原則」

memo サイバー攻撃グループ「MirrorFace」に関する注意喚起

警察庁は、MirrorFaceと呼称されるサイバー攻撃グループが、令和元年頃から国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信や、ソフトウェアのぜい弱性を悪用した標的ネットワーク内への侵入により、情報窃取を目的としたサイバー攻撃を行っていることを確認した。令和７年１月には、これらの攻撃が、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、内閣サイバーセキュリティセンター（NISC）との連名で、同グループの手口や未然防止対策等に関する注意喚起を実施した。

注１：重要インフラ（「重要インフラのサイバーセキュリティに係る行動計画」（令和６年３月８日サイバーセキュリティ戦略本部決定）において、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道、物流、化学、クレジット、石油及び港湾の15分野が指定されている。）の基幹システム（国民生活又は社会経済活動に不可欠な役務の安定的な供給、公共の安全の確保等に重要な役割を果たすシステム）に対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの
2：Operational Technologyの略。重要インフラ等の基幹システムや設備を制御・運用するための技術
3：National center of Incident readiness and Strategy for Cybersecurityの略
4：Australian Signals Directorateの略
5：Australian Cyber Security Centreの略

第2節 サイバー空間における脅威への対処

1 重大サイバー事案対処に係る警察の取組

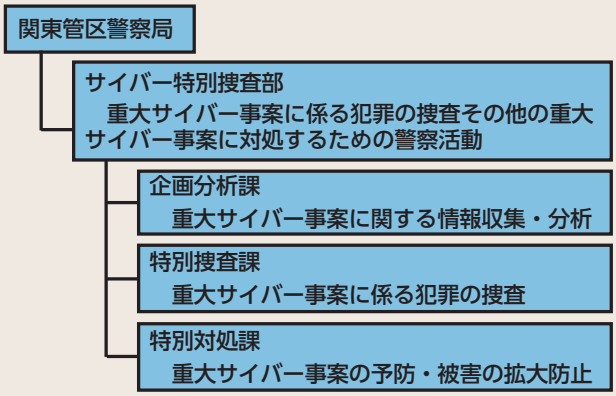
（1）サイバー特別捜査部による重大サイバー事案への対処

サイバー空間をめぐる脅威は極めて深刻な情勢にあり、中でも、重大サイバー事案(注)が一たび発生すれば、物流、医療等の人々の暮らしに不可欠な社会機能に影響が及んだり、先端技術を有する企業が情報を窃取されることなどにより国家と国民の安全が脅かされたりするおそれがあるなど、その脅威は深刻である。

こうした状況を踏まえ、警察では、重大サイバー事案への対処を担う国の捜査機関として関東管区警察局に設置されているサイバー特別捜査部において、全国警察からサイバー分野の知識や経験を豊富に持つ人材を登用するとともに、高度な資機材を整備し、重大サイバー事案に係る捜査や実態解明を推進している。

また、サイバー特別捜査部では、都道府県警察の捜査により得られた情報、暗号資産の追跡等の高度な専門的知識・技術に基づく支援により得られた情報等を集約することにより、俯瞰的・横断的な分析を行っている。さらに、サイバー特別捜査部は、こうした分析を生かして外国捜査機関等との国際共同捜査により事件検挙を遂げるなど、国内捜査と国際捜査の結節点であるとともに、全国の捜査におけるハブとしての役割も果たしている。

図表３－６　関東管区警察局サイバー特別捜査部の体制



サイバー特別捜査部のロゴマーク

CASE

オンラインのフリーマーケットサービスへの架空出品や他人名義のクレジットカード情報の不正利用を行っていた犯行グループについて、サイバー特別捜査部が匿名性の高い暗号資産の取引の流れを解明したことにより、同グループの首魁の男（26）を特定し、令和６年（2024年）10月20日、同男を電子計算機使用詐欺罪で逮捕した（サイバー特別捜査部、青森、宮城、埼玉、滋賀、京都、福岡、佐賀、長崎及び熊本）。

注：国若しくは地方公共団体の重要な情報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

memo 能動的サイバー防御の導入と警察の取組

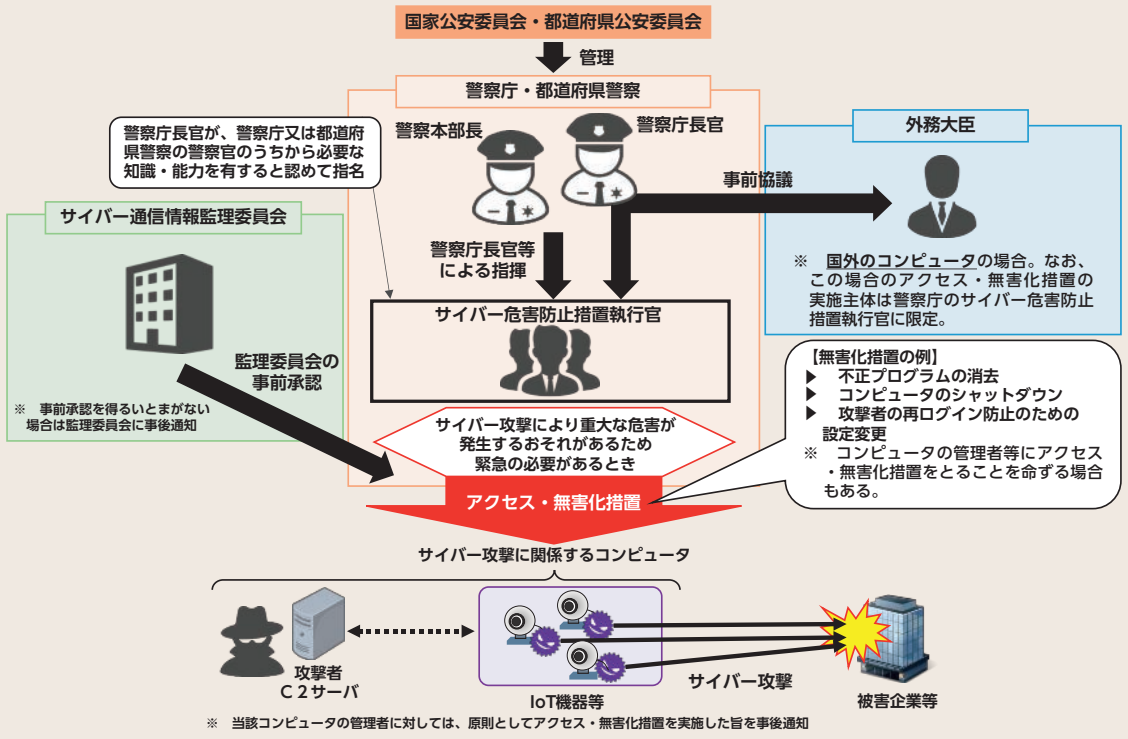
令和４年12月に閣議決定された国家安全保障戦略において、重大なサイバー攻撃による被害の未然防止・拡大防止を図るため、能動的サイバー防御を導入することとされた。

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。

こうした情勢の下、令和７年５月、第217回国会において、サイバー対処能力強化法（以下「強化法」という。）及び同整備法（以下「整備法」という。）が成立した。

強化法及び整備法は、「官民連携の強化」、「通信情報の利用」及び「攻撃者のサーバ等へのアクセス・無害化措置」の３つを取組の柱としている。このうち警察関係では、整備法により、警察官職務執行法の一部が改正され、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新たに設けられた(注)。警察では、同規定の施行に向け、関係機関・団体等と緊密に連携しながら、人材の確保・育成や資機材の整備等により、サイバー空間における対処能力の更なる強化を図っていくこととしている。

図表３－７　改正警察官職務執行法の概要



注：アクセス・無害化措置に関する規定については、令和８年11月までに施行することとされている。アクセス・無害化措置の実施に当たっては、国家安全保障との整合性の観点等から、内閣官房国家サイバー統括室や内閣官房国家安全保障局等の関係機関と緊密に連携していくこととしている。

（2）重大サイバー事案に対処する人材の確保・育成

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、民間での勤務経験を有する者の中途採用や任期付き採用を推進するなど、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いる。サイバー特別捜査部においても、警察庁をはじめ全国警察から登用された多彩な経歴や資格を持つ職員たちが、日々、重大サイバー事案対処に当たっている。

（3）外国捜査機関等との連携の推進

国境を越えて実行される重大サイバー事案に対処するためには、外国捜査機関等との緊密な連携が不可欠である。

警察庁サイバー警察局では、令和４年から、国際共同捜査の実施等における我が国と欧州各国との橋渡し役として、サイバー事案対策に専従する連絡担当官をEUROPOL(注１)に常駐させ、外国捜査機関等との連携を強化している。また、海外におけるサイバー事案の手口や技術の動向等について、平素から外国捜査機関等との情報交換を推進している。

EUROPOL

サイバー特別捜査部では、都道府県警察が初動捜査により収集した証拠について、高度な技術を用いて分析や解析を行い、その結果を外国捜査機関等と共有するなどして、国境を越えて実行される重大サイバー事案に対し、国際共同捜査をはじめとする国際的なネットワークの下で対処している。

CASE

我が国を含め世界各国の企業等に対してランサムウェア被害を与えている攻撃グループ「Phobos（フォボス）」について、サイバー特別捜査部と関係都道府県警察は、EUROPOL等との国際共同捜査を推進している。その結果、令和６年（2024年）11月、米国司法省は、同グループの運営者とみられるロシア人の男（42）を起訴したことを発表した。

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

memo

外国捜査機関等と連携したサイバー事案対策の取組

警察では、EUROPOLが主導する国際共同捜査に参画し、DDoS攻撃(注２)ウェブサービスに関する捜査及び対策を推進している。同国際共同捜査では、DDoS攻撃に用いられるドメイン等をテイクダウン（機能停止）し、テイクダウンの実施を告げる「スプラッシュページ」を表示させている。また、当該ドメイン等の管理者の逮捕や当該ウェブサービスの利用者の特定も進められており、サイバー特別捜査部と関係都道府県警察でも、日本国内の利用者を検挙した。

警察庁では、令和６年12月、公式SNSアカウントやグーグルの広告機能を活用してDDoS攻撃に関する注意喚起を行うなど、関係する外国捜査機関等と同時に広報啓発活動を実施した。

スプラッシュページ

注１：European Union Agency for Law Enforcement Cooperationを指す。欧州連合（EU）の法執行機関であるが、捜査権限はなく、加盟国間の情報交換の促進や収集した情報の分析等が主な任務である。
２：114頁参照

2 サイバー事案への対策

（1）不正アクセス対策

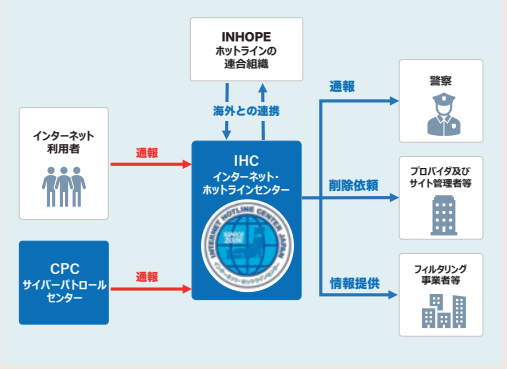
警察では、不正アクセス行為の犯行手口の分析に基づき、関係機関等とも連携し、広報啓発等の不正アクセスを防止するための取組を実施しているほか、不正アクセス行為による被害防止のための広報啓発に資することを目的として、毎年、民間企業や行政機関等に対する「不正アクセス行為対策等の実態調査」(注１)及び「アクセス制御機能に関する技術の研究開発の状況等に関する調査」(注２)を行っている。

（2）インターネット上の違法情報・有害情報対策

① インターネット・ホットラインセンター及びサイバーパトロールセンターの運用

警察庁では、一般のインターネット利用者等から違法情報や、重要犯罪密接関連情報(注３)、自殺誘引等情報(注４)に関する通報を受理して、警察への通報、サイト管理者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）を運用している。令和６年中、IHCでは2,186件の違法情報の削除依頼を行い、そのうち1,991件（91.1%）が削除されたほか、9,488件の重要犯罪密接関連情報の削除依頼を行い、そのうち8,024件（84.6%）が、6,359件の自殺誘引等情報の削除依頼を行い、そのうち4,986件（78.4%）が、それぞれ削除された。IHCに通報された違法情報等の中には、外国のサーバにそのデータが蔵置されているものがあるところ、このうち児童ポルノについては、各国のホットライン相互間の連絡組織であるINHOPE(注５)の加盟団体に対し、削除に向けた措置を依頼している。

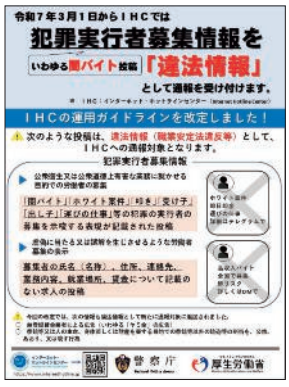
図表３－８ インターネット・ホットラインセンターにおける取組



また、警察庁では、インターネット上の違法情報等を収集し、IHCに通報するサイバーパトロールセンター（CPC）を運用している。CPCでは、違法情報等を自動収集してその該当性を判定するAI検索システムを導入し、サイバーパトロールの高度化を図っている。

② インターネット・ホットラインセンター等における取組の強化

「いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策」（令和６年12月17日犯罪対策閣僚会議決定）を受けて、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において犯罪実行者募集情報を違法情報と位置付けるとともに、同年３月、体制を増強した。



犯罪実行者募集情報に関する広報啓発資料

注１：令和６年の調査は、８月28日から９月20日までの間に、市販のデータベースに掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市区町村等）、独立行政法人及び特殊法人から2,951件を無作為に抽出し、調査票を郵送で配布して実施した。電子メール又は郵送により、634件の回答を得た。

２：令和６年の調査は、同年８月28日から９月20日までの間に、市販のデータベースに掲載された企業のうち業種分類が「情報・通信」、「サービス」、「電気機器」又は「金融」であるもの及び国公立・私立大学のうち理工系学部又はこれに準ずるものを設置するものから、1,884件を無作為に抽出し、調査票を郵送で配布して実施した。電子メール又は郵送により、225件の回答を得た。

３：19頁（特集）参照

４：114頁参照

５：現在の名称はInternational Association of Internet Hotlinesであるが、旧名称のInternet Hotline Providers in Europe Associationの略称を現在も使用している。平成11年（1999年）に設立され、令和７年１月末現在、IHCを含む55団体（51の国・地域）から構成される国際組織

また、大手SNS事業者と個別に面談し、違法情報・有害情報に係る削除依頼への迅速な対応を要請するなど削除の実効性を確保するための取組を推進している。

③　効果的な違法情報等の取締り

警察では、サイバーパトロール等により違法情報・有害情報の把握に努めるとともに、効率的な違法情報の取締り及び有害情報を端緒とした取締りを推進している。

また、合理的な理由もなく違法情報の削除依頼に応じないサイト管理者については、検挙を含む積極的な措置を講じることとしている。

（3）ランサムウェア対策

警察では、ランサムウェア等による被害に関する警察への通報・相談を促進し、サイバー事案の潜在化を防止するとともに、捜査活動の効率化及び再発防止を図っている。特に、国民生活に大きく影響を及ぼすおそれのある医療機関等における被害の未然防止及び拡大防止を図るため、医療機関等に対する講演や個別訪問等を実施している。

また、警察庁ウェブサイト(注1)において、ランサムウェア事案の手口に関する情報等を公開し、被害の未然防止対策等を講ずるよう注意喚起を行っているほか、ランサムウェア等のサイバー事案の発生に備えた警察への連絡体制の整備等について、関係機関を通じて事業者等に周知した。

（4）サイバー攻撃対策

警察では、サイバー攻撃に適切に対処するため、警察庁サイバー警察局、サイバー特別捜査部等と都道府県警察が緊密に連携して、迅速かつ的確な捜査を推進することとしている。また、サイバー攻撃を受けたコンピュータやサイバー攻撃に使用された不正プログラムを解析し、その結果や犯罪捜査の過程で得た情報等を総合的に分析するなどして、攻撃者及び手口に関する実態解明を進めており、これらの情報等は、被害の未然防止・拡大防止に向けた取組のほか、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、いわゆるパブリック・アトリビューションにも活用されている。

memo　TraderTraitorに対するパブリック・アトリビューション

令和６年12月、警察庁は、サイバー特別捜査部及び警視庁による捜査及び分析の結果を総合的に評価し、米国連邦捜査局（FBI(注2)）及び米国国防省サイバー犯罪センター（DC３(注3)）と共に、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交換業者から暗号資産を窃取したことを特定し、連名で公表した。また、警察庁では、内閣サイバーセキュリティセンター（NISC(注4)）及び金融庁との連名で、標的となる事業者等に対し、TraderTraitorの手口例と緩和策に関する文書を発出し、注意喚起を行った。


FBI News

Washington, D.C.
FBI National Press Office
(202) 324-3691

December 23, 2024

FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com

The Federal Bureau of Investigation, Department of Defense Cyber Crime Center, and National Police Agency of Japan are alerting the public to the theft of cryptocurrency worth $308 million U.S. dollars from the Japan-based cryptocurrency company DMM by North Korean cyber actors in May 2024. The theft is affiliated with TraderTraitor threat activity, which is also tracked as Jade Sleet, UNC4899, and Slow Pisces. TraderTraitor activity is often characterized by targeted social engineering directed at multiple employees of the same company simultaneously.

In late March 2024, a North Korean cyber actor, masquerading as a recruiter on LinkedIn, contacted an employee at Ginco, a Japan-based enterprise cryptocurrency wallet software company. The threat actor sent the target, who maintained access to Ginco's wallet management system, a URL linked to a malicious Python script under the guise of a pre-employment test located on a GitHub page. The victim copied the Python code to their personal GitHub page and was subsequently compromised.

After mid-May 2024, TraderTraitor actors exploited session cookie information to impersonate the compromised employee and successfully gained access to Ginco's unencrypted communications system. In late-May 2024, the actors likely used this access to manipulate a legitimate transaction request by a DMM employee, resulting in the loss of 4,502.9 BTC, worth $308 million at the time of the attack. The stolen funds ultimately moved to TraderTraitor-controlled wallets.

The FBI, National Police Agency of Japan, and other U.S. government and international partners will continue to expose and combat North Korea's use of illicit activities—including cybercrime and cryptocurrency theft—to generate revenue for the regime.

FBI、DC３及び警察庁による公表

注１：警察庁ウェブサイト「ランサムウェア被害防止対策」
(https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html)
２：Federal Bureau of Investigationの略
３：Department of Defense Cyber Crime Centerの略
４：117頁参照

3 技術支援と解析能力の向上

（1）サイバーフォースの役割

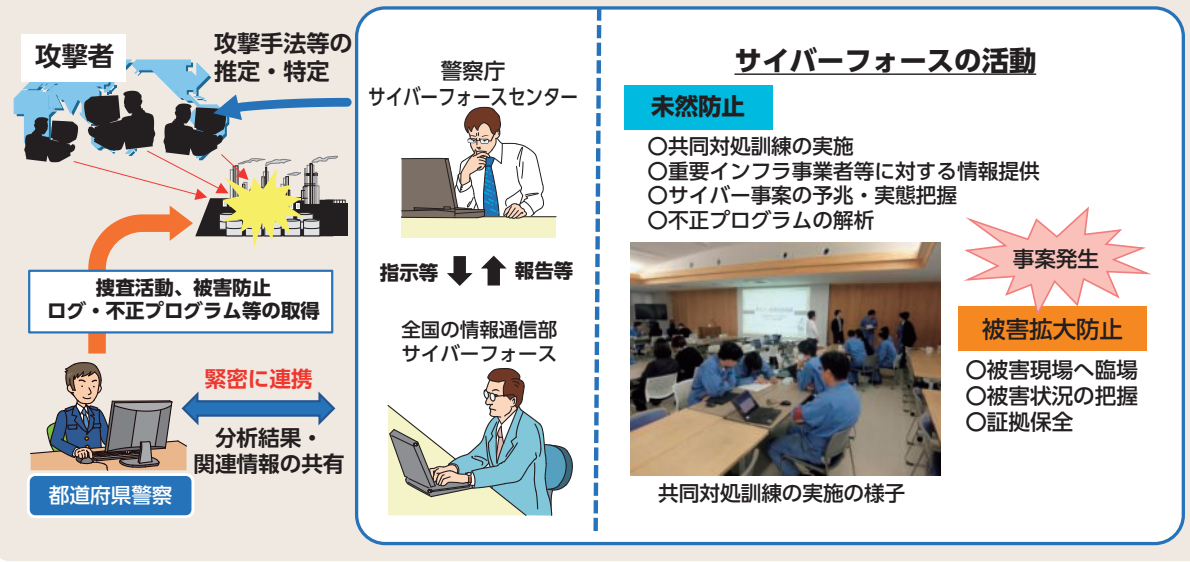
警察では、深刻化するサイバー事案に対処するため、攻撃の対象となったサイバーセキュリティ上のぜい弱性に関する情報や、標的型メール攻撃等の犯行手口に関する情報等を、捜査活動及び事業者との情報交換を通じて把握・分析し、被害の未然防止及び拡大防止に努めている。

近年のサイバー事案をみると、国家を背景に持つサイバー攻撃集団による高度な攻撃が引き続き発生しているほか、新たなぜい弱性とその対策が日々発見されており、それに応じて用いられる手口も次々と変化している。

このような情勢に対応するため、警察では、都道府県警察のサイバー事案対策部門に技術的な面から支援を行う部隊であるサイバーフォースを、警察庁及び全国の情報通信部(注1)にそれぞれ設置している。サイバーフォースは、個々の重要インフラ事業者等に対する脅威情報の提供や助言、サイバーテロ対策協議会(注2)での講演、サイバー事案発生を想定した共同対処訓練を実施するなどして、官民連携の強化に努めている。また、サイバー事案発生時には、都道府県警察と連携し、被害状況の把握、被害拡大の防止、証拠保全等について技術的な緊急対処を行っている。

さらに、警察庁のサイバーフォースセンターは、全国のサイバーフォースの司令塔の役割を担っており、サイバー事案発生時には被害状況の把握等を行う拠点として機能するほか、24時間体制でのサイバー事案の予兆・実態把握、標的型メールに添付された不正プログラムの解析、全国のサイバーフォースに対する指示等を行っている。

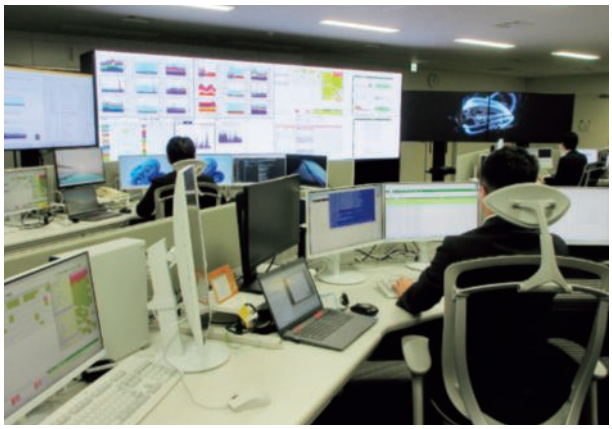
図表3－9 サイバーフォースの役割と活動



注1：15頁（特集）参照
2：131頁参照

（2）サイバー事案の予兆・実態等の把握

①　リアルタイム検知ネットワークシステムの運用



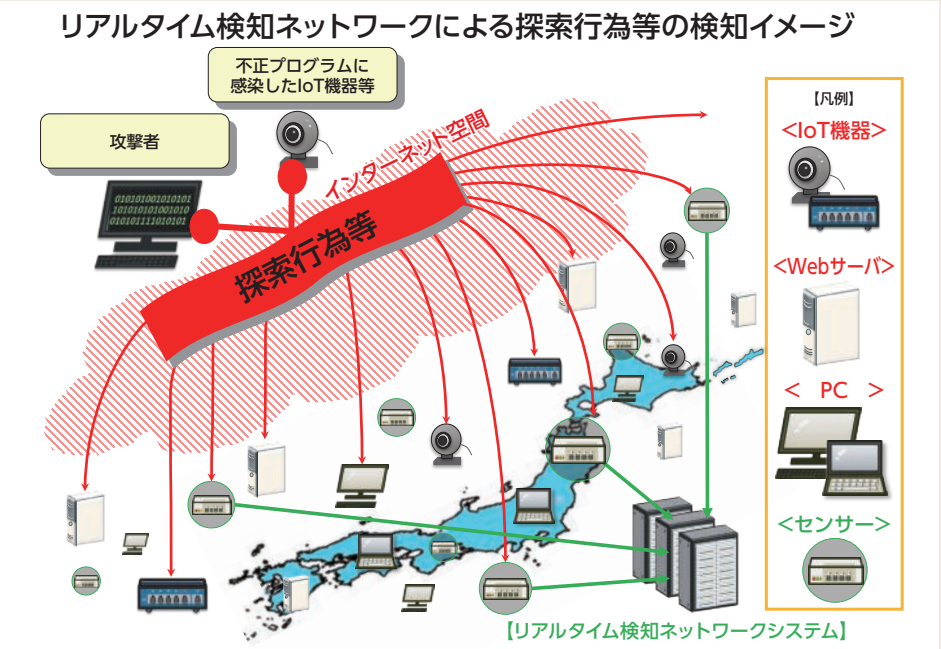
リアルタイム検知ネットワークシステムの運用状況

サイバーフォースセンターでは、サイバー事案の予兆・実態等を把握することを目的として、平成14年からリアルタイム検知ネットワークシステムを運用している。本システムでは、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(注1)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とから、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される、通信パケットを観測することができる。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、インターネット上で発生している各種事象を把握することができる。

本システムは、インターネット上で発生するDoS攻撃(注2)を早期に検知するDoS攻撃被害観測機能や、犯罪の温床となっているダークウェブの実態を把握するためにダークウェブ上の情報を収集・分析する機能を備えており、インターネット上の事象の変化等に応じて機能の強化を行っている。

サイバーフォースセンターでは、本システムから得られる情報を用いて、24時間体制でサイバー事案の予兆・実態等を把握し、インターネット利用者がサイバー事案の危険性を正しく認識し、適切な対策を自主的に講じられるよう、分析結果を警察庁ウェブサイトにおいて広く一般に公開している。

図表３－10　リアルタイム検知ネットワークシステムの概要



注１：ネットワークを通して送信される際に分割されるデータのかたまりのことであり、各パケットには、送信先や送信元のIPアドレス等の情報が付加されている。
　２：Denial of Serviceの略。特定のコンピュータに対し、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

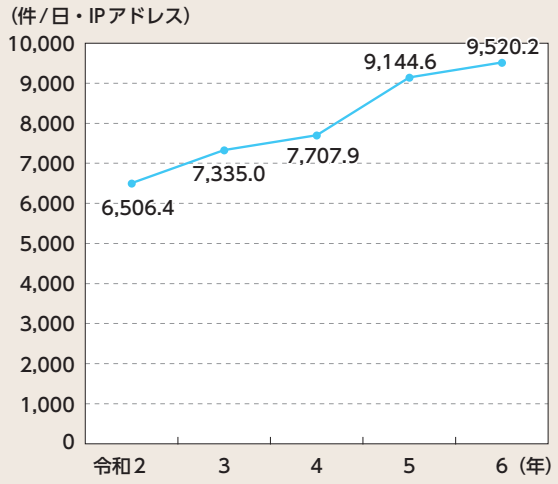
②　リアルタイム検知ネットワークシステムによる令和６年中のインターネット観測結果

令和６年中、リアルタイム検知ネットワークシステムのセンサーにより、一つのセンサー当たり約9.1秒に１回という高い頻度で不審なアクセスが行われていることを観測し、その大部分は海外を送信元とするアクセスで占められていた。不審なアクセス件数は増加の一途をたどっており、引き続きサイバー空間をめぐる脅威の情勢は極めて深刻であることがうかがわれる。

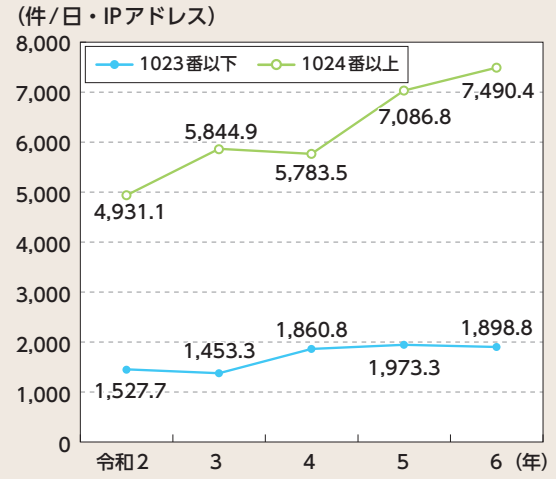
検知した不審なアクセスについて、宛先ポート番号(注)に着目すると、1024番以上のポート番号へのアクセスが大きな割合を占めている。IoT機器では、標準設定として1024番以上のポート番号が使用されているものも多いことから、ぜい弱性を有するIoT機器の探索行為やIoT機器に対するサイバー攻撃の脅威が高まっているとみられる。

また、Wi-Fiルーター等を対象とした不審なアクセスが引き続き観測されており、Wi-Fiルーター等のソフトウェアのぜい弱性を狙ったもののほか、設定変更等を行うための管理用のポートに対してユーザ名・パスワードを送信してログインを試行したと疑われるものが観測されている。

図表３－11　リアルタイム検知ネットワークシステムにおいて検知した一つのセンサーに対する１日当たりの不審なアクセス件数の推移（令和２年～令和６年）



図表３－12　ポート番号1023以下及び1024以上のポートへのアクセス件数の推移（令和２年～令和６年）



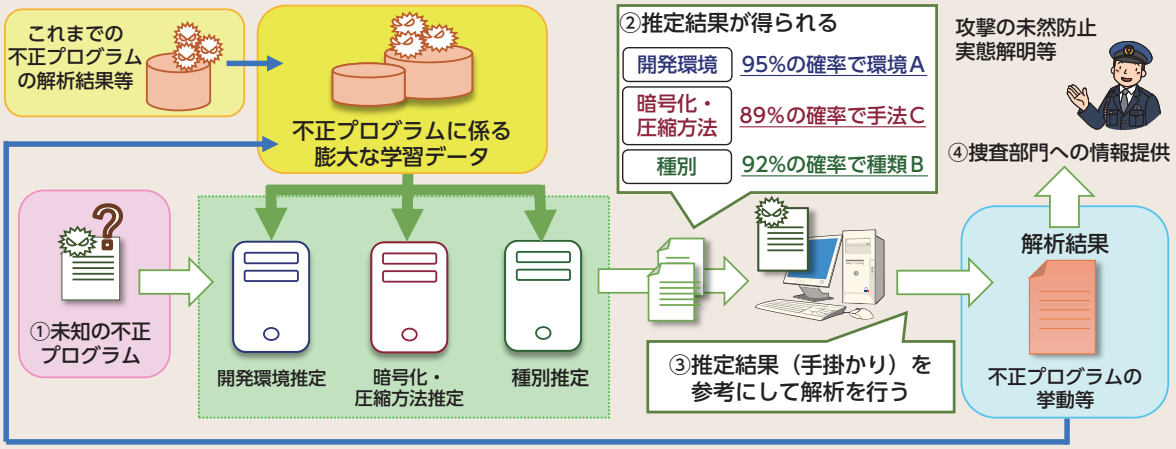
注：TCP/IP通信（インターネット等で用いられるネットワーク上でデータを交換する際の取決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。

（3）不正プログラムの解析

近年、標的型メールに添付された不正プログラムを用いたサイバー事案が発生しているほか、病院、発電所、化学プラント等の重要インフラの基幹システム等を標的としたランサムウェア(注)を用いたサイバー事案が発生している。

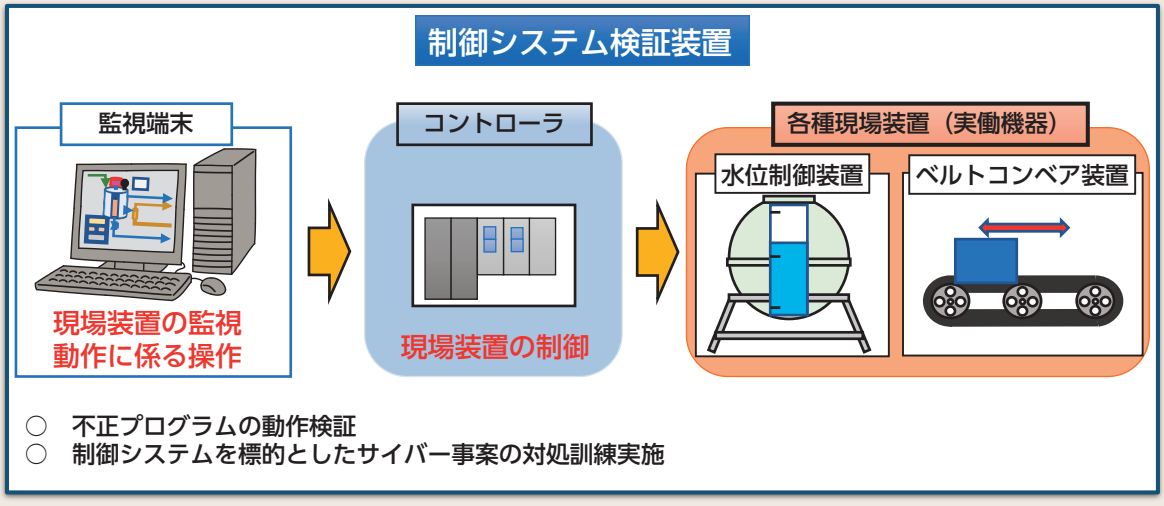
警察庁では、不正プログラムの動作解析や攻撃手口の解明等に資する情報の収集・分析及び機械学習を活用した不正プログラム解析の高度化・効率化に取り組んでいる。

図表３－13　機械学習を活用した不正プログラム解析の高度化・効率化のイメージ



特に、重要インフラの制御・監視を行う産業制御システムを標的としたサイバー事案への対処能力の強化を図るため、制御システム検証装置等を整備し、実際に不正プログラムを実行させ、その動作を検証するとともに、不正プログラムが動作することで残される証跡等を調査することにより、事案発生時における迅速な原因特定・対処に万全を期している。また、産業制御システムを標的としたサイバー事案を想定した対処訓練に当該装置を活用しているほか、当該装置による検証の結果を踏まえ、関係機関・団体とサイバー事案の未然防止・被害拡大防止対策のための情報交換を実施している。

図表３－14　制御システム検証装置の活用例



注：116頁参照

4 警察における人材育成の推進

（1）サイバー空間における脅威への対処に係る人材育成

都道府県警察では、サイバー事案に的確に対処するため、事案発生時には、多数の捜査員を従事させるとともに、警察本部等にサイバー事案への対処について高度な知見を有するサイバー犯罪捜査官等の専門捜査員を配置している。サイバー犯罪捜査官等は、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・特別採用をした警察官等であり、その知識や技能を生かして捜査の第一線で活躍している。

また、警察庁では、従前から情報通信に関する専門的な技術を有する者を技術系職員として採用し、実践的な研修を実施するなどして育成しており、これらの職員は、その専門知識を生かして、情報技術解析等の第一線で活躍している。

さらに、サイバー特別捜査部においては、全国警察からサイバー分野の知見を持つ有為な人材を登用して重大サイバー事案対処に当たっており、同部での経験は、捜査員の能力を向上させ、帰任後の都道府県警察全体の対処能力向上にも寄与している。

こうしたサイバー空間における脅威への対処のための人的基盤を強化するため、警察では、高度な専門的知識・技術を有する人材を確保・育成するための取組を計画的に推進するとともに、高度な専門的知識・技術を有するサイバー人材が、その専門性を継続的に生かすことができるようなキャリアパスの管理等を部門横断的かつ体系的に実施している。

CASE

徳島県警察では、サイバー犯罪捜査官（中途採用・特別採用）の採用枠として、技術・経験に応じた採用区分を設け、幅広い人材の登用に努めている。令和６年度には、特に高度な技術・経験を有する者１人を捜査幹部となる警部として採用し、サイバー部門において業務に従事させている。

徳島県警察採用募集ポスター

memo

官民人事交流制度を活用した情報集約・分析業務の高度化

警察庁では、官民人事交流制度により、サイバーセキュリティ関連企業出身の職員を幹部警察官として採用し、当該職員が民間企業で培った最新の知見を、警察庁サイバー警察局及びサイバー特別捜査部におけるサイバー事案に関する情報集約・分析業務の一層の高度化に生かしている。

（2）サイバーコンテストの開催

警察庁では、全国の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。


警察庁サイバーコンテスト

CASE

和歌山県警察では、令和６年10月、サイバーコンテストを開催し、県下12警察署の警察官が出場した。同コンテストでは、会場として、令和５年度に整備された研修訓練施設である「サイバー人材育成トレーニングルーム」を活用し、サイバー空間における脅威への対処能力の向上及び素養のある人材の発掘を図った。

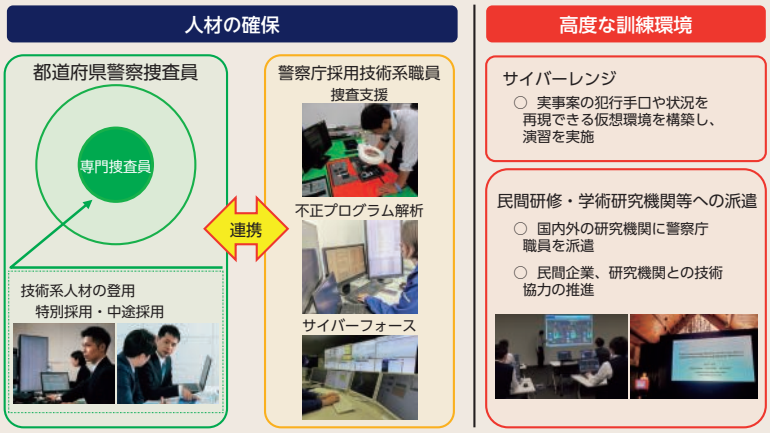
和歌山県警察サイバーコンテスト

（３）捜査員等に対する実践的教育訓練

サイバー空間の利用が広がる中、どのような捜査分野においてもサイバー関係の知識が不可欠となってきており、サイバー部門のみならず全ての部門の幹部警察官にサイバーリテラシーに関する十分な知識を身に付けさせることが必須となっている。

こうした状況を踏まえ、令和７年４月、警察大学校にサイバー部門に係る研修・訓練に特化したサイバー警察教養部を新設した。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実践的な研修のほか、都道府県警察の各部門の幹部警察官に対するサイバーリテラシーに係る研修等を体系的・効果的・一元的に実施している。

図表３－15　サイバー空間における脅威への対処に係る人材育成



また、警察大学校では、平成30年度以降、サイバーレンジ(注)を導入し、仮想環境下において実際の犯行手口や被害状況を再現することにより、最新の手口により行われるサイバー事案に対する実践的な捜査演習や、大規模なサイバー攻撃の被害事案を想定した訓練等を実施している。

さらに、警察庁では、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。

memo　サイバーセキュリティ対策研究センターにおける取組

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。

自動運転システムの解析に関する研究

自動運転システムを備えた自動車の中には、車載装置と外部のビーコンやサーバとの双方向通信による情報を基に運行するものが開発されているが、こうした通信を介して車載装置のぜい弱性を悪用された場合には、重大な事件・事故につながるおそれがある。こうした場合、当該自動車に記録された情報が捜査に必要となり得ることから、サイバーセキュリティ対策研究センターでは、自動運転システムに関する研究を行っている。令和６年度は、自動車に対するサイバー攻撃に備え、学術機関及び民間企業の知見を活用し、自動車におけるセキュリティインシデントの解明に関する共同研究を行った。

自動運転システムの解析に関する研究状況

注：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

5 国際連携の推進

（１）外国捜査機関等との連携の推進

警察庁では、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おり、令和６年中は、Ｇ７ローマ／リヨン・グループ(注１)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）(注２)の締約国等が参加するサイバー犯罪条約委員会会合、EUROPOL(注３)とハンガリー国家警察とが共催する欧州警察長官会議等の国際会議に参加した。また、ICPO(注４)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が参加するなど、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等を推進している。

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(注５)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。

memo 外国捜査機関との連携強化に資する取組

令和６年９月、警察庁サイバー警察局では、オランダ国家警察との間で、共同オペレーション等について、サイバー犯罪対策部門の幹部等を交えたハイレベルな意見交換を行ったほか、同年10月に開催されたＧ７ローマ／リヨン・グループ会合におけるハイテク犯罪サブグループでは、サイバー空間をめぐる脅威の情勢、暗号資産を悪用した犯罪の捜査等について議論が行われ、Ｇ７各国の捜査機関との緊密な連携を図った。また、令和７年２月、ドイツの治安機関との間で、自動車に搭載されたシステムの解析手法等について意見交換を実施した。

（２）国際協力の推進

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、外国捜査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(注６)）と連携して外国捜査機関等に対する支援を行っている。平成26年度からは、外国捜査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ほか、平成29年度からは、ベトナム公安省の職員を受け入れて、サイバーセキュリティ対策等に関する知識・技術の習得を目的とした研修を行っている。

注１：昭和53年（1978年）にボン・サミットを契機に発足したＧ８テロ専門家会合（Ｇ８ローマ・グループ）と平成７年（1995年）にハリファクス・サミットで設置されたＧ８国際組織犯罪対策上級専門家会合（Ｇ８リヨン・グループ）が、平成13年（2001年）の米国における同時多発テロ事件以降合同で開催されているもので、国際組織犯罪対策やテロ対策等について検討している。なお、平成26 年（2014年）３月から、Ｇ７として実施している。
２：サイバー犯罪に関する条約。サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定している。平成24年に我が国について発効した。
３：120頁参照
４：19頁（特集）参照
５：Forum of Incident Response and Security Teamsの略
６：Japan International Cooperation Agencyの略

6 官民連携の推進

（1）インターネットバンキングに係る不正送金事犯への対策

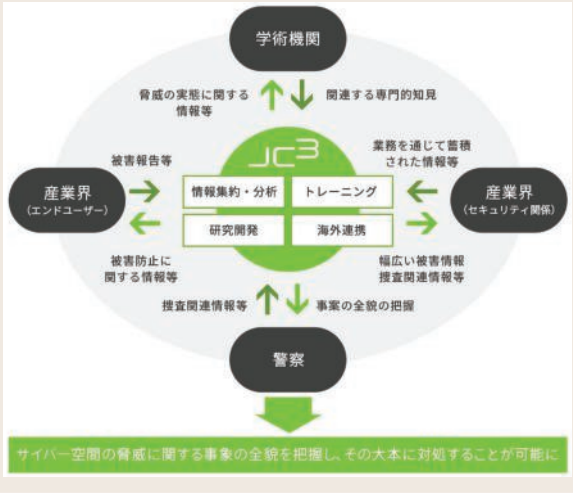
警察では、インターネットバンキングに係る不正送金事犯に対し、関係機関と連携したフィッシング被害の実態把握や、フィッシングサイトに関する分析及び関係事業者への照会等、早期の実態解明と必要な取締りを推進している。

また、警察では、一般財団法人日本サイバー犯罪対策センター（JC３(注)）等との間における官民連携の枠組みも活用して把握したフィッシングサイトの情報をウイルス対策ソフト事業者等に提供するなど、積極的な被害防止対策を推進している。

（2）日本サイバー犯罪対策センターとの連携

我が国における産学官連携の枠組みとして平成26年から業務が開始されたJC３では、産学官の情報や知見の集約・分析をし、その結果等を還元することで、脅威の大本を特定し、これを軽減し、又は無効化することにより、以後の事案発生の防止を図ることとしている。警察では、捜査関連情報等をJC３において共有し、産学におけるサイバーセキュリティに関する取組に貢献するとともに、JC３において共有された情報を警察活動に迅速・的確に活用し、安全で安心なサイバー空間の構築に努めている。

図表３－16　JC３の概要



memo　フィッシングサイト撲滅チャレンジカップの開催

JC３では、専門的な知識を持たない人でもプラットフォーム事業者等に対してフィッシングサイトのテイクダウン（機能停止）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している。

また、JC３では、サイバー防犯ボランティア等が同ツールを活用し、フィッシングサイトのテイクダウン件数等を競う「フィッシングサイト撲滅チャレンジカップ」を開催しており、警察庁がこれを後援している。令和６年７月に開催された第２回大会では、46団体が参加し、2,201件のフィッシングサイトがテイクダウンされた。

（3）サイバー防犯ボランティアに対する支援

サイバーパトロールにより発見した違法情報・有害情報をIHC、サイト管理者等に通報する取組やインターネット利用者に対する講演活動等を行うサイバー防犯ボランティアは、全国で301団体、7,298人（令和６年12月末現在）となっており、警察では、研修会を開催するなどして、こうした活動を行う団体の拡大と取組の活性化を図っている。

サイバー防犯ボランティアの活動

注：Japan Cybercrime Control Centerの略

memo サイバー防犯ボランティアによる犯罪実行者募集への対策に関する活動

警察では、サイバー防犯ボランティアと連携し、社会情勢に応じた活動を展開している。都道府県警察では、いわゆる「闇バイト」による強盗事件等の発生を受け、学生に対する犯罪実行者募集の実態に関する講演等を通じ、これらに加担しないよう注意喚起を実施しているほか、学生ボランティアが自ら犯罪実行者募集情報を発見し、IHC等に通報するサイバーパトロール活動を実施している。

（４）サイバーテロ対策協議会

警察では、各都道府県警察及びサイバー事案の標的となるおそれのある重要インフラ事業者等で構成される「サイバーテロ対策協議会」を全ての都道府県において設置し、サイバー事案の脅威やサイバーセキュリティに関する情報提供、民間の有識者による講演及び参加事業者間の意見交換・情報共有を行っているほか、サイバー事案の発生を想定した共同対処訓練等を行っている。

サイバーテロ対策協議会

（５）サイバーインテリジェンス情報共有ネットワーク

警察では、情報窃取の標的となるおそれの高い先端技術を有する事業者等との間で、情報窃取を企図したとみられるサイバー事案に関する情報共有を行う「サイバーインテリジェンス情報共有ネットワーク」を構築しており、事業者等から提供された情報等を集約・分析し、事業者等に対し、分析結果に基づく注意喚起を行っている。

（６）高度な研究開発を行う大学を標的としたサイバー事案への対策の推進

近年、高度な研究開発を行う大学を標的としたサイバー事案が発生していることから、警察では、当該サイバー事案に関する情報収集・分析を強化するとともに、大学と連携し、サイバー事案をめぐる最新の情勢や被害防止対策等に関する情報共有及びサイバー事案の発生を想定した共同対処訓練を実施することなどにより、高度な研究開発を行う大学を標的としたサイバー事案への対処能力の強化を図っている。

（７）被害の潜在化防止に向けた取組の推進

①　関係機関と連携した通報・相談の推進

サイバー事案対処に当たっては、警察への通報・相談を一層促進し、国民・事業者等からの情報を広範に収集することが求められる一方、被害者自身に対する社会的評価の悪化の懸念等から通報・相談そのものがためらわれる傾向があり、いわゆる「被害の潜在化」が課題となっている。警察では、関係機関・団体、サイバー保険(注)を取り扱う損害保険会社をはじめとする民間事業者等との連携、民間事業者等との共同対処協定の締結等を通じて、サイバー事案による被害に関する警察への通報・相談を促進している。

②　通報・相談しやすい環境整備

警察庁では、令和６年３月、インターネットから通報・相談をすることができる一元的な窓口を整備した。また、ウェブサイト等における発信を通じて、サイバー事案に関する警察への通報・相談を促す広報を行うなどの取組を実施している。

さらに、サイバー事案に関する通報・相談に適切に対応するため、採用時教養、昇任時教養等において、サイバー事案対処に関する講義を実施するなど警察職員全体の対処能力の向上に向けた人材育成を推進している。

注：サイバー事案等により企業に生じた損害等を補填する保険

警察活動の最前線

進化する脅威に立ち向かうサイバー犯罪対策を目指して

前　福島県警察本部生活安全部サイバー犯罪対策課サイバー対策係長（現　同課サイバー犯罪捜査第四係長）
五十嵐　貴子

私は、育児休暇を取得した後、深刻化するサイバー犯罪を何とかしたいと考え、情報処理安全確保支援士試験に合格し、サイバー犯罪対策課に配属されました。現在はサイバー対策係として、広報や講演、官民連携等を通じてサイバー犯罪の防止に取り組んでいます。

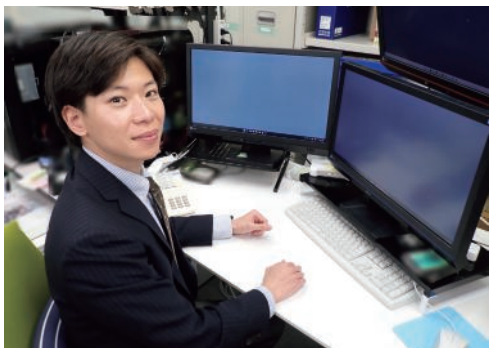
サイバー犯罪は日々巧妙化し、新たな手口が次々と生まれます。そのため、常に最新の知識と技術を学びながら、講演では具体的な事例を交えて分かりやすく伝えることを心掛けています。また、参加者に質問を投げかけ、一緒に考えてもらうといったインタラクティブな方法を取り入れることで、誰もがサイバー犯罪を「自分ごと」として捉えられるよう工夫しています。

サイバー犯罪対策は、新たな手口との攻防戦ですが、犯罪の手口を分析し、対策を考えることで自分の知識や技術を深化させられるところに醍醐味があります。対策の効果は目に見えにくいものの、「被害が発生しないことこそが成功の証」であり、犯罪を未然に防ぐことが人々の安心につながると信じています。

今後も新たな脅威に対応できるよう自己研鑽に努め、関係機関と連携しながら、社会全体でサイバー犯罪に立ち向かう機運を高めていきたいです。

社会問題化するSNS関連犯罪の早期解決により被害拡大を防止

京都府警察サイバー対策本部サイバー捜査課情報・指導係
亀井　瞭



令和５年春、京都府警察では、サイバー空間における脅威に的確に対処するため、サイバー事案捜査や技術支援に特化したサイバー捜査課が発足しました。私は、初代課員として捜査係に配置となり、サイバーパトロールや府民から寄せられるサイバー相談等を端緒とした事件捜査に従事しています。

令和５年、「登録するだけで数万円分のポイントが貰える」などとインフルエンサーにSNSで宣伝させてフォロワーをだまし、消費者金融の借入用アカウントを作成させた上、そのアカウントに不正アクセスして借入れを装って金員を窃取する事案が発生し、その被害は全国に及びました。この事案では、当初、不正アクセスについて立件が困難とされていましたが、犯行に使われた消費者金融のアプリの通信状況を疑似的に再現するなどの手法を駆使してこれを打破し、事案解決につながりました。

私は、この事件を通じ、「困難な事件でも創意工夫を凝らし犯人を検挙する」という取組姿勢を学びました。今後もサイバー空間の脅威は深刻な情勢が続くと思われますが、私は京都府警察の取組姿勢を受け継ぐとともに、将来、サイバー捜査をけん引できるようスキルアップに全力を尽くしたいと思っています。