第1部　特集・トピックス

深刻化するサイバー空間の脅威と警察の新たなる展開

特集に当たって

本年の警察白書の特集のテーマは「深刻化するサイバー空間の脅威と警察の新たなる展開」です。

今日、我が国は戦後最も厳しく複雑な安全保障環境に直面しており、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、重大な事態へと急速に発展するリスクをはらんでいます。特に、サイバー空間の匿名性を悪用したサイバー攻撃は、実空間で行われる犯罪と比べて露見しにくく攻撃者側が優位にあることから、その脅威が急速に高まっています。具体的には、国家を背景としたサイバー攻撃が平素から行われているとされているほか、ロシアによるウクライナ侵略前に行われたサイバー攻撃等、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、今後さらに高度化・巧妙化すると考えられています。

また、近年、社会全体のデジタル化の進展に伴い、サイバー空間は、地域や年齢を問わず、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ており、地理的・時間的制約の少ないサイバー空間は、社会に様々な便益をもたらしている反面、その匿名性があらゆる犯罪において悪用されています。特に昨年は、特殊詐欺や証券口座に係る不正取引、企業・団体等に対するランサムウェア事案等が発生し、国民生活や経済活動に対して大きな影響を与えました。

このような情勢において、国民の生命、身体及び財産の保護の任に当たる警察は、あらゆる手段を駆使して、平時から有事に至るまでシームレスに、サイバー空間をめぐる脅威に対処する必要があります。

この特集では、第１節で、重大サイバー事案の対処を担うサイバー特別捜査部（設置当初はサイバー特別捜査隊）が設置から５年の節目を迎えることを契機に、同部におけるこれまでの取組について紹介します。第２節では、能動的サイバー防御等の導入を目的として令和７年５月に成立したサイバー対処能力強化法及び同整備法について概観します。そして、第３節では、これらを踏まえて、今後、警察が進めていくべき対策の在り方について展望します。

今回の特集が、深刻化するサイバー空間の脅威に対する警察の取組について、デジタル社会に生きる国民の皆様の理解を深めるとともに、社会全体で国民の安全・安心を守っていくための対策の在り方について考えていただく一助となれば幸いです。

第1節 重大サイバー事案に対処するサイバー特別捜査部

1 サイバー特別捜査部の設置に至るまでの警察の取組の軌跡

（1）令和４年（2022年）の警察法改正までの主な組織改正と法令の制定

コンピュータが社会の各分野に普及し、国民生活に大きな利便をもたらしてきた反面、昭和50年代から、不法な利益を得ることを目的とした不正データの入力等のコンピュータを利用した不正行為や、コンピュータの機能妨害等が重大な社会問題となり始めた。これに対して、警察においては、コンピュータ犯罪(注1)の発生実態の分析と、捜査及び防犯上の対策を進めてきた。また、昭和62年（1987年）６月には、刑法等の一部を改正する法律が施行され、電磁的記録不正作出等の罪、電子計算機損壊等による業務妨害罪及び電子計算機使用詐欺罪が新設されたことを受け、警察においては、こうした違法行為の取締りも実施してきた。

こうした中で、平成10年（1998年）５月に開催されたバーミンガム・サミットのコミュニケにおいては、「ハイテク犯罪と闘うための原則と行動計画」を迅速に実施することが宣言された。当時、我が国でも、不正アクセスを手口とする事案が多発しており、警察庁は、同年６月、急増するハイテク犯罪(注2)に的確に対処するため、「ハイテク犯罪対策重点推進プログラム」を策定・公表し、体制及び法制の整備等の取組を推進した。これを踏まえ、平成11年４月には、警察庁情報通信局に電磁的記録の解析等に関する事務をつかさどる技術対策課が設置された。また、同年８月には不正アクセス禁止法が成立し、平成12年２月に施行された。

その後も、サイバー犯罪(注3)の検挙件数は増加し、平成16年頃には、インターネットを悪用した詐欺事犯等が新たな社会問題となった。このような情勢に対処することを目的として、サイバー犯罪の予防及び捜査を一体的に推進するため、同年４月、警察庁生活安全局に情報技術犯罪対策課が設置された。また、技術支援体制の整備のため、警察庁情報通信局技術対策課は情報技術解析課と改称されたほか、総合的なサイバーテロ対策を推進するため、警察庁警備局、生活安全局及び情報通信局の職員により構成されるサイバーテロ対策推進室も設けられた。

それ以降も、コンピュータ・ウイルスがまん延し、フィッシング(注4)を手口とする不正アクセス行為が深刻化していた情勢の中で、平成23年７月、情報処理の高度化等に対処するための刑法等の一部を改正する法律の施行により、不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウイルスに関する罪）が新設されたほか、平成24年５月には、不正アクセス禁止法の一部を改正する法律が施行され、フィッシング行為が禁止されるなど、不正アクセス行為につながる一連の行為に対する規制が強化された。

警察庁では、平成24年７月、サイバー空間における脅威への戦略的かつ全庁的な対応を強化するため、サイバーセキュリティ戦略を統括する長官官房審議官（サイバーセキュリティ戦略担当）を設置した。さらに、平成25年５月、サイバー攻撃に係る情報収集・分析や捜査の高度化等を実施するため、警察庁警備局警備企画課にサイバー攻撃対策官を設置したほか、平成26年４月、サイバーセキュリティ対策全般の司令塔としての機能を強化するため、長官官房審議官（サイバーセキュリティ戦略担当）が担当する事

注１：コンピュータ犯罪の定義は、当初は「コンピュータ・システムに向けられた犯罪又はこれを悪用した犯罪」であったが、昭和62年６月の刑法の一部改正を契機に、その対象の範囲が見直され、「コンピュータ・システムの機能を阻害し、又はこれを不正に使用する犯罪（過失、事故等を含む。）」となった。

２：コンピュータ技術及び電気通信技術を悪用した犯罪

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を指す。それまでは、コンピュータ技術及び電気通信技術を悪用した犯罪を「ハイテク犯罪」と呼称していたが、国際的動向等を踏まえて「サイバー犯罪」と呼称することとした。

４：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

務を変更し、長官官房審議官（サイバーセキュリティ担当）としてサイバーセキュリティに関する各種取組の総括・調整を行うこととした上で、新たに長官官房参事官（サイバーセキュリティ担当）を設置した。

（2）令和４年の警察法改正以降の主な組織改正

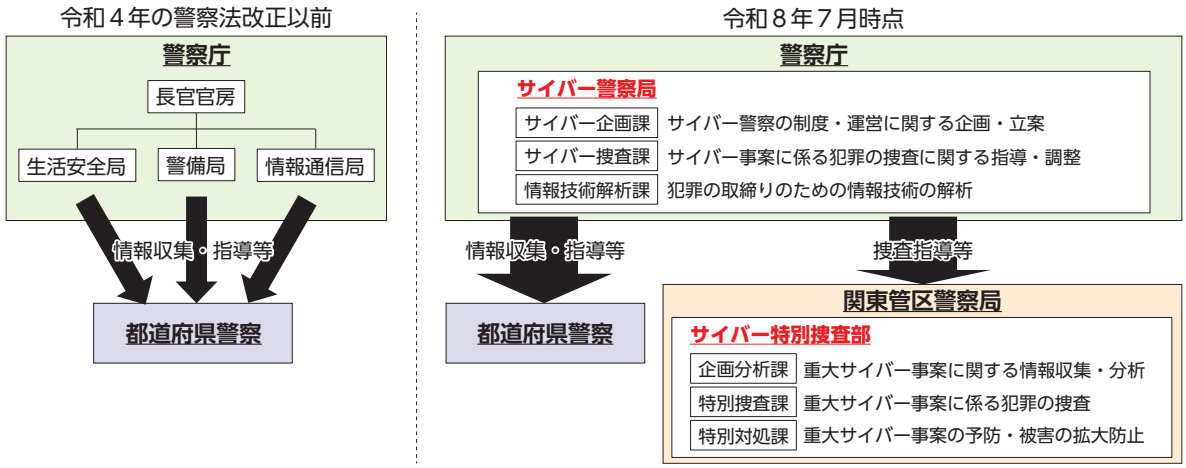
近年、サイバー空間は、全国民が参画し、重要な社会経済活動を営む場となっている。一方で、サイバー空間を利用した犯罪や国家を背景としたサイバー攻撃がその手口を深刻化・巧妙化させつつ多数発生しており、サイバー空間をめぐる脅威は、極めて深刻な情勢となっている。警察庁では、サイバー関係の業務に関する事務を生活安全局、警備局及び情報通信局がそれぞれ所掌した上、長官官房においてその調整等を行うなどして対応してきたが、サイバー空間をめぐる情勢が深刻化する中、情報の集約や関係省庁との連携等に課題が生じていた。また、重大なサイバー事案(注１)への対処に不可欠である外国捜査機関等との連携を強化する必要もあった。

そこで、警察法等を改正し、令和４年４月、警察庁に新たにサイバー警察局を設置してサイバー関係事務を所掌している部門を統合し、当該事務を一元的に所掌することとしたほか、重大サイバー事案(注２)へ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ことで、サイバー事案への対処能力を強化した。

サイバー警察局・サイバー特別捜査隊発足式

重大サイバー事案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。こうした事案に対応するため、令和６年４月、サイバー特別捜査隊は発展的に改組され、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及び特別捜査課が置かれた。これにより、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、整理及び横断的・俯瞰（ふかん）的な分析等を行う体制が強化された。また、令和７年４月、同部の下に特別対処課が置かれ、重大サイバー事案の発生の予防及び当該事案による被害の拡大の防止に係る体制が強化された。

図表特－１　サイバー空間の脅威に対処する警察の体制



注１：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
２：サイバー事案のうち、国若しくは地方公共団体の重要な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

2 設置から５年目を迎えるサイバー特別捜査部の取組

（１）国際連携の中での特徴的な取組

サイバー特別捜査部は、自ら又は都道府県警察が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うことで被疑者を検挙するとともに、分析・解析の結果を外国捜査機関等と共有して国際共同捜査を行うことで事件検挙を遂げるなど、全国の捜査におけるハブとしての役割に加えて、国内捜査と国際捜査の結節点としての役割も果たしている。

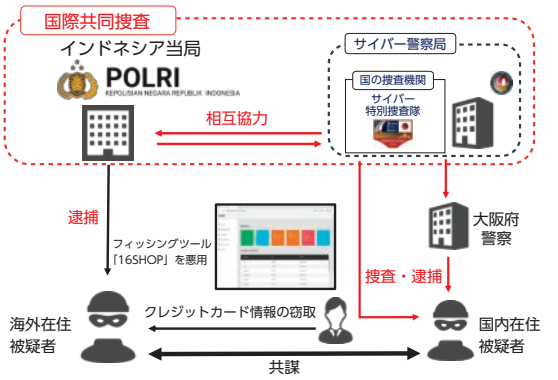
❶ フィッシングに係る国際共同捜査

フィッシングに起因する不正送金被害等が深刻化する中、サイバー特別捜査部では、国際共同捜査をはじめとする国際的なネットワークを活用しフィッシング事案に対処している。

CASE

サイバー特別捜査隊（当時）と大阪府警察の合同捜査本部は、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・利用事案について、ＩＣＰＯ(注1)が主導するインドネシア国家警察との国際共同捜査であるオペレーション「Kingfisher（キングフィッシャー）」を実施した。同捜査本部は、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サイトで不正に注文を行ったとみられるインドネシアに所在する同国籍の男（40）を特定し、その結果として、令和５年７月、インドネシア国家警察が同男を逮捕した。本事案は、国際共同捜査の結果としてフィッシング事案の国外被疑者を逮捕した初の事例となった。

図表特－２ 事案概要



❷ ＤＤｏＳ攻撃(注2)に係る国際共同捜査

重要インフラ事業者等に対するＤＤｏＳ攻撃によるものとみられる被害が確認されている中、サイバー特別捜査部では、国際共同捜査による被疑者の検挙や犯罪インフラの解体等を行っている。

CASE

日本警察は、ＥＵＲＯＰＯＬ(注3)が主導する国際共同捜査であるオペレーション「PowerOFF（パワーオフ）」に参画し、ＤＤｏＳ攻撃を実行するための機能を提供するウェブサービスに関する捜査及び対策を推進している。同オペレーションでは、外国治安機関が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示す「スプラッシュページ」を表示させたほか、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行っており、日本国内でも、サイバー特別捜査部と関係都道府県警察が当該ウェブサービスの利用者を検挙した。

PowerOFFに係るスプラッシュページ

また、警察庁では、令和８年４月、当該国際共同捜査を受けて、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、広報啓発活動を実施した。

注１：International Criminal Police Organization（国際刑事警察機構）の略
２：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
３：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。

❸ 組織的詐欺等に係る国際共同捜査

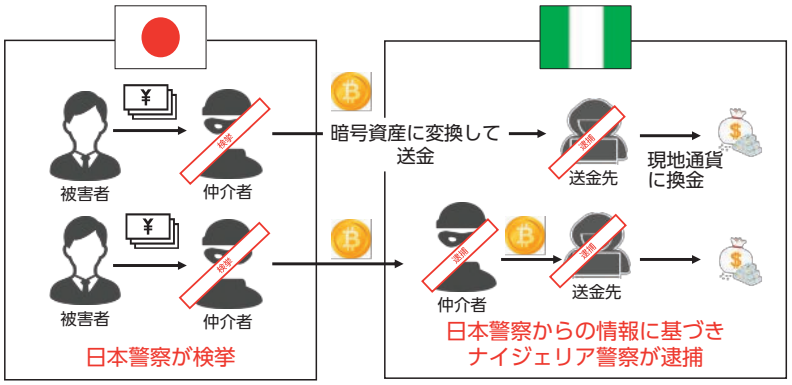
ＳＮＳ型投資・ロマンス詐欺をはじめとした特殊詐欺の被害が急増する中、サイバー特別捜査部では、国境を越える組織的詐欺等の犯罪に対処している。

CASE

西アフリカの組織犯罪グループによる金融犯罪に対し、ＩＣＰＯが主導する国際共同捜査であるオペレーション「Jackal（ジャッカル）」が進められている。日本警察も令和６年４月から同オペレーションに参画しており、サイバー特別捜査部では、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によって得られた情報を横断的に分析するとともに、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。

同情報をナイジェリア警察に提供することで、同警察が同国内の被疑者を逮捕するとともに、日本国内でも関係都道府県警察において送金の仲介者を検挙した。

図表特－３　事案概要

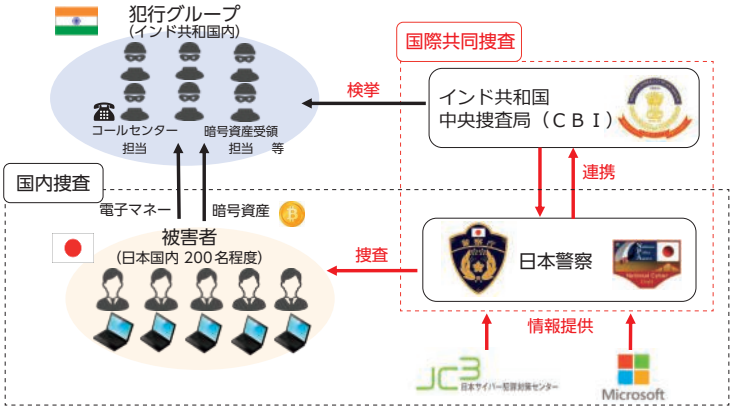


MEMO　捜査における官民連携

警察と民間事業者は、サイバー空間の安全・安心の確保に向けて緊密に連携しているが、このことは犯罪の予防のみならず、被疑者の検挙にもつながっている。

日本人を標的としたいわゆる「サポート詐欺(注1)」事件について、一般財団法人日本サイバー犯罪対策センター（ＪＣ３(注2)）とマイクロソフト社が分析した情報が警察庁に提供されたことを端緒とし、サイバー特別捜査部では暗号資産の移転状況を追跡するなどの捜査を行った。同部が特定したインド人被疑者らの情報や、警視庁をはじめとする都道府県警察が把握した捜査情報をインド共和国の中央捜査局（ＣＢＩ）に対して提供するなどした結果、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。

図表特－４　インド共和国との国際共同捜査の概要



当該被疑者グループの犯行による日本国内の被害件数は少なくとも200件、総被害額は約１億8,000万円であったが、本件検挙後の令和７年６月中に独立行政法人情報処理推進機構（ＩＰＡ）に寄せられた「ウイルス検出の偽警告」に関する相談件数は85件（前月比353件（80.6%）減少）と、前月より著しく減少した。本件は、警察と民間事業者による連携した検挙が、その後の事案発生の抑止に効果があることを示す先駆的な事例となった。

注１：パソコン等の画面にウイルスに感染したかのような警告を表示し、サポートの名目で金銭等をだまし取る詐欺
　２：Japan Cybercrime Control Centerの略

❹ ランサムウェアに係る国際共同捜査

企業・団体等におけるランサムウェア被害が相次いでいる中、サイバー特別捜査部は、国際共同捜査を通じた被疑者の検挙や暗号化されたデータの復号等に貢献している。

MEMO ランサムウェア攻撃事案に係る復号ツール開発

Lockbitに係るスプラッシュページ

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サイバー攻撃グループ「LockBit（ロックビット）」について、サイバー特別捜査隊（当時）と関係都道府県警察は、ＥＵＲＯＰＯＬ等との国際共同捜査であるオペレーション「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人を逮捕したほか、同グループが使用するサーバ等のテイクダウン（機能停止）を実施し、流出した情報等が掲載されていたリークサイト上に「スプラッシュページ」を表示させた。また、関係国の捜査機関が、同年５月、ランサムウェアの開発・運営を行っていた被疑者の資産を凍結するとともに起訴し、同年10月、関連被疑者４人を逮捕した。

この事案では、サイバー特別捜査隊（当時）が、LockBitにより暗号化されたデータを復号するツールを独自開発し、国内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。その結果、少なくとも24の被害企業等が同ツールを活用し、約1,290万件の被害データの復号に成功している。

MEMO ランサムウェア攻撃グループ「Phobos」及び「8 Base」に係る国際共同捜査

㋐ 概要

「Phobos」及び「8 Base」に係るスプラッシュページ

平成30年12月頃から、他のランサムウェア攻撃と比べて少額の身代金を、多数の中小規模の組織等に要求するランサムウェア攻撃を仕掛けることが特徴とされる「Phobos（フォボス）」グループによる被害が、欧米において確認され始めた。さらに、令和４年３月頃には、同グループの関連組織「8 Base（エイトベース）」による被害も確認され始めた。我が国においても、これらのグループによるものと考えられる被害が認知されたことから、令和５年11月、日本警察は、これらのグループの取締りを目的とした米国等との国際共同捜査に参画した。

同国際共同捜査の結果、令和６年11月、米国司法省は、「Phobos」グループの運営者とみられるロシア人を起訴したことを発表し、令和７年２月までに、米国司法省及びスイス連邦警察が、「8 Base」グループ運営者等とみられる男ら４人を検挙した。

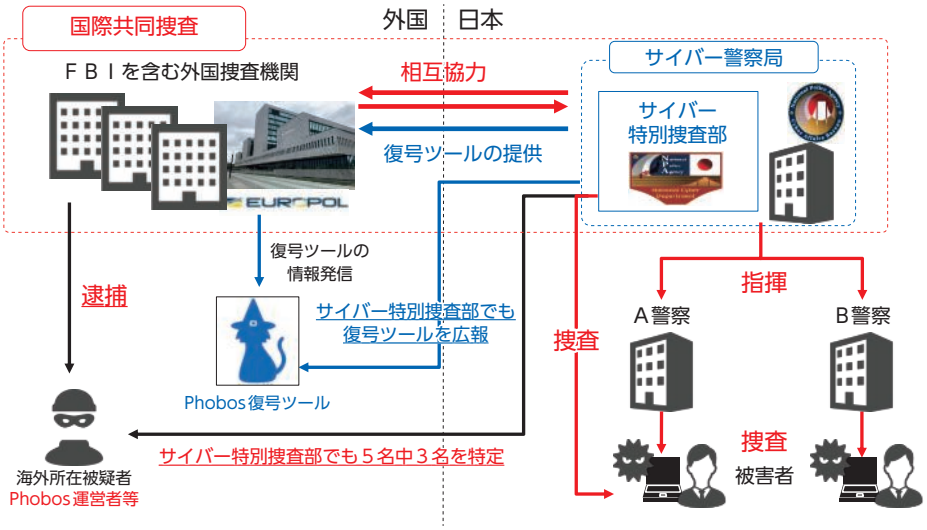
㋑ 日本警察による貢献

サイバー特別捜査部は、ＩＰアドレス等の捜査により、「Phobos」グループの運営者及び同人の居場所の特定に成功し、米国をはじめとする関係国の捜査機関に情報を提供した。また、外国捜査機関から提供された被疑者の暗号資産に関する情報について、詳細な分析を実施した結果、「8 Base」グループの暗号資産の移転先となる暗号資産アカウントから同グループ運営者らの特定に成功し、関係国の捜査機関に情報提供した。

さらに、サイバー特別捜査部では、米国が押収した被疑者のパソコン等のデータの提供を受けて分析を行い、ランサムウェア「Phobos」により暗号化されたデータを復号するツールの開発に成功した。同ツールは、同部の技術部門と捜査部門が緊密に連携し、１年以上にわたって当該ランサムウェアのプログラムの解析を

行う中で開発されたものである。令和７年７月、警察庁では同ツールを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各国の被害企業等の被害回復が可能となるよう、国際的に広く周知した(注)。令和８年４月現在、少なくとも17の被害企業等が約717万件の被害データの復号に成功しており、その復号成功率は99.9%を超えている。

図表特－５　国際共同捜査における日本警察の役割



オペレーションに参加した捜査員の手記

・捜査に携わった捜査員

国際的なサイバー犯罪者は、ダークウェブ、ＶＰＮ、暗号資産等の匿名化の手段を多用し犯行に及んでいます。そのような状況の中、一国の情報収集能力や捜査では対処が困難であり、国際共同捜査の重要性が増してきています。ランサムウェア事案では、被害者から得られる情報は非常に少なく、例えるなら、犯行現場が犯行後に放火されているような状態で、残された情報は「燃えかす」程度しかないといったイメージです。そのような中で、少ない情報を基に情報の源をたどり、他国とも協調しながら捜査を広げ、データを入手し、空雑巾を絞るような努力をして被疑者にたどり着く一本の糸を紡いでいく作業を行っています。そういった捜査の中で成果を出せることができた理由の一部は、日本警察のデジタル・フォレンジック能力や情報分析能力の高さと、日本人の真面目な気質に由来するのではないかと考えています。

Phobos/８Base事案でも、数万件のＩＰアドレスの中に含まれるごく僅かの手がかりを抽出し、そのＩＰアドレスから被疑者の人物像を推定し、特定に成功しました。また、同事案では、他国では追跡が不可能であった暗号資産の高度な匿名化措置に対して、捜査的な観点や得られた情報を基にして仮説を立てて追跡することで、日本独自の暗号資産追跡方法を確立し、被疑者へとつながる資金移動の解明に至りました。国際的なサイバー捜査というと華やかなイメージがあるかもしれませんが、実際は、多くのデータと実直に向き合い真実を求めるという執念に近い地道な捜査が行われています。日本警察のそういった姿勢や実績に対する国際的な評価の高まりを感じています。

・復号ツールを作成した捜査員

私はこの度、関東管区警察局サイバー特別捜査部において、ランサムウェア「Phobos」によって暗号化された被害データを復号するツール開発に携わりました。また、令和７年７月、世界中の被害企業等の被害回復が可能となるよう、警察庁及びＥＵＲＯＰＯＬから当該ツールが公開されました。Phobosは、私が初めてマルウェアの検体に触れたランサムウェアでもあり、それがこのような形で結実したことは、非常に感慨深いです。

復号ツールの開発の道のりは、決して平坦なものではありませんでした。必要な情報が欠けた状態で１年以上の時間が経過し、完成することはないかもしれないとの焦燥感にかられる中、米国の協力でもたらされたデータから有益な情報を発見し、「最後のピースがはまった」と得も言われぬ感覚を覚えたことをいまだに鮮明に記憶しています。被害企業からは、「民間調査会社に依頼しても、費用がかかるのに復元できる保証がないため、復号ツールが警察によって公開されて大変助かった」などとの声も届き、職員としての誇り

注：https://www.npa.go.jp/bureau/cyber/countermeasures/ransom/phobos.html

と使命感を実感できました。このような素晴らしい結果を得られたことは、海外のカウンターパートを含む関係者の協力の成果であるといえます。今後も周囲の皆様のお力を借りながら、自分に課せられた業務に精一杯取り組みたいと思います。

㊦ 他国の捜査員による国際オペレーションでの日本の存在感や特徴についての寄稿

European Cybercrime Centre（ＥＣ３）オペレーション部長　Schuurbiers氏からの寄稿

ＥＣ３オペレーション部長
Schuurbiers氏

サイバー犯罪に関していえば、近年、日本の法執行機関とヨーロッパの関係機関との協力が顕著に増加しています。ランサムウェアに対する各種オペレーションや複数のＤＤｏＳ攻撃のためのインフラやその利用者に対するオペレーション等の共同オペレーションの成果をみれば、世界的なサイバー犯罪の撲滅を成功させるには、信頼性の高い、先制的な国際協力が不可欠であることは明らかです。質の高いオペレーション情報の提供、各種調整や高度な技術的専門知識の共有に至るまで、日本の貢献のおかげで、これら取組による協働の成果が一貫して底上げされているのです。

あわせて、有意義な貢献といえるのが、ＥＵＲＯＰＯＬとＥＵ加盟国に対する日本の戦略的な働き掛けです。度々オペレーションに参加して持続的に戦略上の対話を重ねるなど、連携強化に向けた日本の精力的な姿勢のおかげで、共通の状況認識の確立が大いに促進されました。このような連携における継続的なアプローチが、より効果的な優先順位の決定、信頼関係の醸成や国境なき犯罪の脅威に対峙する真に世界的な行動の構築につながっています。

ＥＵＲＯＰＯＬは、この国際協力を通じて日本警察が示してくれている専門性、オープンな姿勢と信頼性を高く評価しています。日本に積極的に参加してもらえることで、オペレーション上の影響が大きいだけでなく、サイバー犯罪から国際社会を守るという使命に長期的に取り組んでいくという気概を感じます。この協力が拡大し続けていく中で、ＥＵＲＯＰＯＬは、この強固な協力関係を更に強化し、今後これまで以上に大きな協働の成果を上げることを期待しています。

（２）匿名性の打破に向けた取組

❶ 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

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移行している中、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(注)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るほか、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も確認されている。また、匿名・流動型犯罪グループは、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させるなどして資金の流れを仮装・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。

❷ 暗号資産の匿名性の仕組みと捜査への障壁

暗号資産取引の特徴の一つとして、その利用者の匿名性の高さが挙げられる。暗号資産取引の際には、取引明細に相当するトランザクションがブロックチェーン上に記録・公開されるものの、これらの情報だけでは特定のコインアドレスの使用者を特定することは困難である。

図表特－６　暗号資産におけるコインアドレス・トランザクション（イメージ図）

TXID:1a2b3c4d5e6f7g8h9i10j11k12l13m14n1
5o16p17q18r19s20t21u22v23w24x2

20XX-XX-XX XX:XX:XX (UTC)	2.026
From:	To
aB3dE5fG7hJk9LmN2pQrStUv	G7kP2bV9xR4tZ6mQe1NfY8sW
WxYz0XXXXX	3cD0aXXXXX

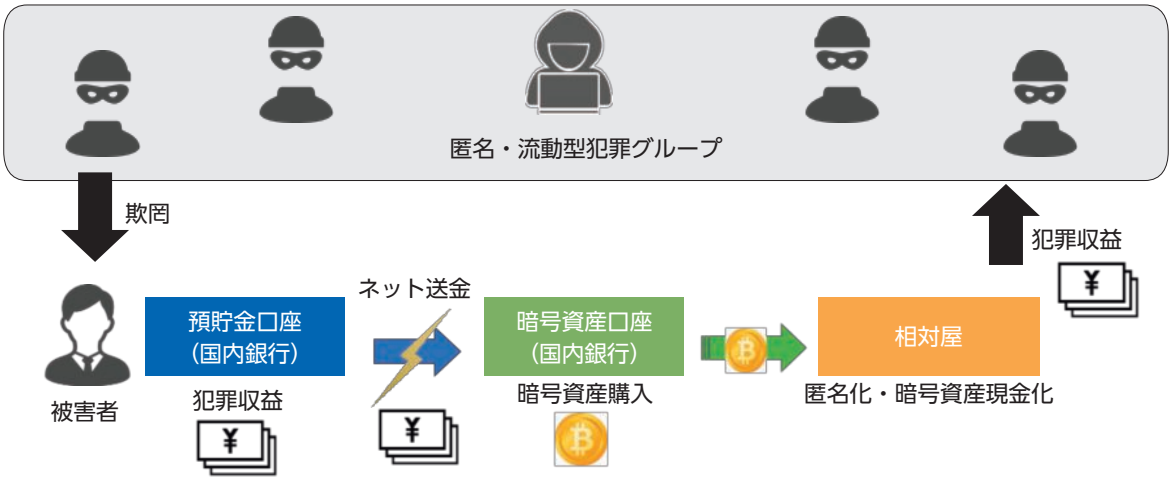
これはFromのアドレスからToのアドレスへ20XX年X月X日XX時XX分XX秒（UTC）2.026ビットコインを送信したという記録である。
TXIDはトランザクションハッシュという取引の固有値である。

また、暗号資産に対する規制は各国において異なることから、暗号資産交換業者が所在する国・地域の中には、本人確認等の措置が義務付けられていないものがあるほか、海外の暗号資産交換業者で取

注：28頁参照（トピックスⅠ）

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、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」を経由しながら送金を行ったり、様々な手段を利用して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」等の匿名性向上技術を用いたりするなどして、暗号資産取引がマネー・ローンダリングに悪用されている実態がある。

図表特－７　暗号資産を悪用したマネー・ローンダリングのイメージ



❸ 匿名性を打破するための取組

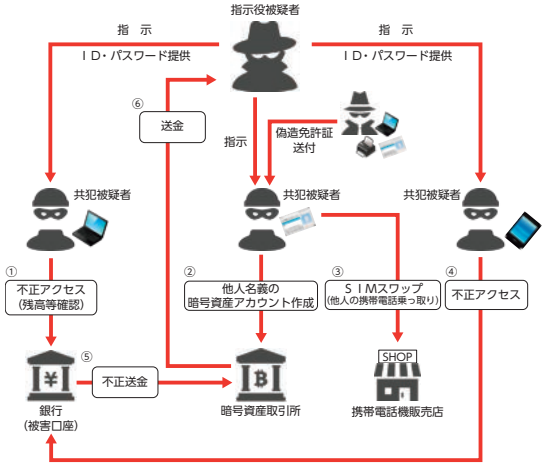
サイバー特別捜査部では、こうした犯罪に悪用される暗号資産の移転状況を追跡するとともに、追跡結果の横断的・俯瞰（ふかん）的な分析を行い、その結果を都道府県警察と共有している。こうした分析により、従来の捜査では必ずしも明らかにならなかった複数事案同士の関連性や背景にある組織性及び上位被疑者を浮き彫りにすることができる。

また、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、増強した職員については、警察庁に設置された匿名・流動型犯罪グループ情報分析室(注１)の分析業務も担うこととなった。当該職員は、同室が有する他の情報も含めた大量の情報の多角的な分析を行うことにより、サイバー空間の匿名性を打破して、匿名・流動型犯罪グループの中核的人物の検挙につなげられるよう、取組を一層強化している。

CASE

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、関係都道府県警察の捜査情報をサイバー特別捜査部で集約・分析し、関係被疑者のＳＮＳアカウントに係る捜査を実施した結果、被疑者らがＳＩＭスワップ(注２)と呼ばれる手口を用いて組織的に不正送金を行っていた実態を明らかにした。また、犯罪収益である暗号資産の移転状況は、ミキシングにより追跡が困難な状態であったが、サイバー特別捜査部の高度な技術によってその追跡に成功し、犯行グループの指示役とみられる無職の男（44）を特定した。令和６年８月までに、同男ら９人を不正アクセス禁止法違反（不正アクセス行為）等で逮捕した（サイバー特別捜査部、警視庁、広島、北海道、宮城、茨城、群馬、千葉、静岡、大阪、兵庫、奈良、岡山、愛媛、福岡、長崎及び熊本）。

図表特－８　事案概要



本件は、サイバー特別捜査部において、日本国内に所在する被疑者を逮捕した初の事案である。

注１：30頁参照（トピックスⅠ）
２：実在する人物になりすまして店舗に来店し、本人確認資料として偽造した運転免許証等を用い、MNP（携帯電話番号ポータビリティ）又はＳＩＭカードの再発行を行うことで、携帯電話番号を乗っ取る手口

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、関係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・分析する中で、匿名性の高い暗号資産（モネロ）に換えられた犯罪収益の流れを解明した。その結果、同グループの首謀者の男（26）を特定し、令和６年10月、同男を電子計算機使用詐欺罪で逮捕した。

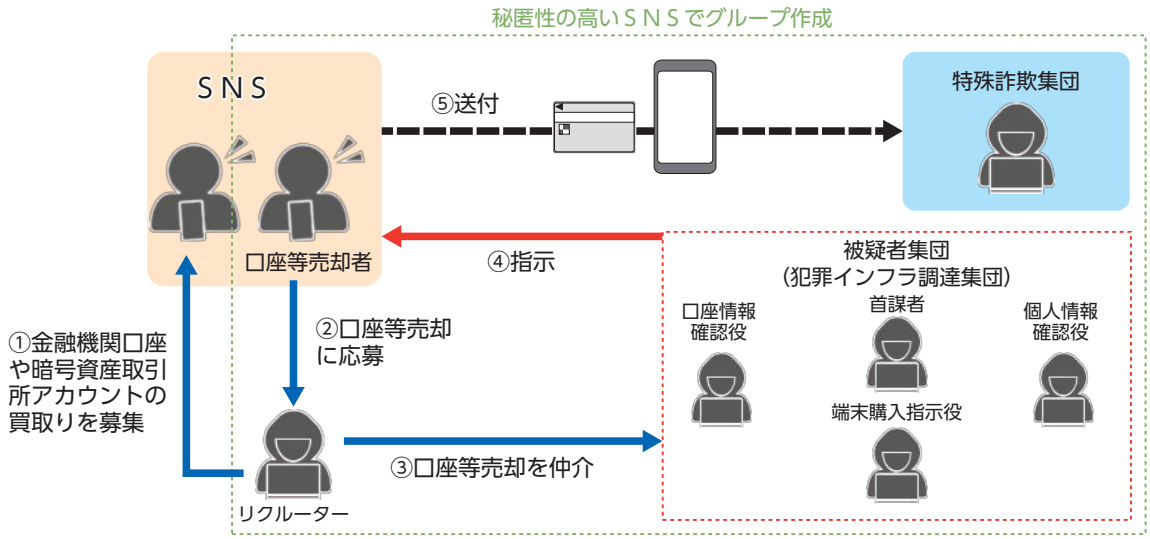
また、本件の関連被疑者については、首謀者の男の指示により、収受した犯罪収益で暗号資産を購入したとして電子計算機使用詐欺罪を適用して逮捕した上、首謀者の男が管理していた犯罪収益である暗号資産の追徴保全を行った（サイバー特別捜査部、青森、宮城、埼玉、滋賀、京都、福岡、佐賀、長崎及び熊本）。

図表特－９　事案概要

CASE

いわゆる「闇バイト」[注]として口座の売買を行う者を募り、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、特殊詐欺集団らに対して販売していた犯罪集団について、関係道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、都道府県警察やＪＣ３から提供された情報を集約・分析するとともに、高度な専門的知識・技術を用いて暗号資産を追跡したことなどにより、関連被疑者を特定した。令和７年10月、首謀者の男（32）ら７人を詐欺罪及び犯罪収益移転防止法違反（なりすまし目的・有償による譲受け）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）。

図表特－10　事案概要



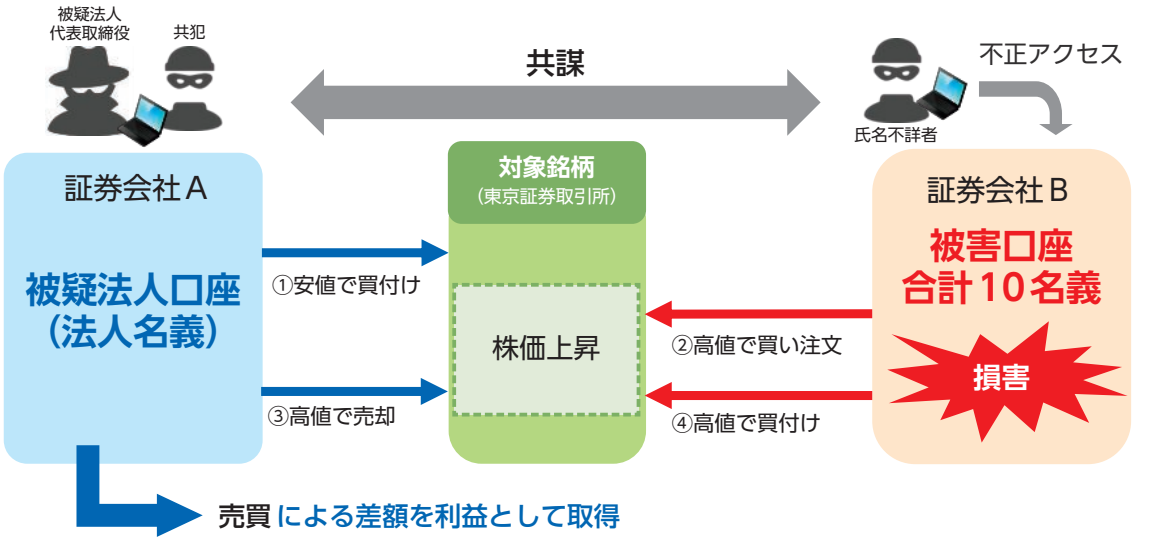
注：28頁参照（トピックスⅠ）

CASE

令和７年３月以降、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た。これを受けて、関係機関の協力を得て、関係都府県警察が捜査を推進した結果、令和７年11月、中国籍の男（38）らを金融商品取引法違反（相場操縦）及び不正アクセス禁止法違反（不正アクセス行為）で逮捕した（警視庁、サイバー特別捜査部、埼玉、千葉、神奈川、山梨、愛知、大阪、兵庫、奈良及び広島）。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。）を大量に買い付けた後、他人の証券口座に不正アクセスし、その証券口座に保有されていた株を売却するなどして資金を確保した上で、対象株を大量に買い付け、株価を上昇させた。その後、同男が保有していた対象株について、高値で売り注文を行うとともに、不正アクセスした他人の証券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、対象株の購入額と売却額の差額を利益として得ていた。

サイバー特別捜査部は、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関し、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、全国で発生した同種事案の情報集約・分析等により、関係都道府県警察による捜査に貢献している。

図表特－11　事案概要



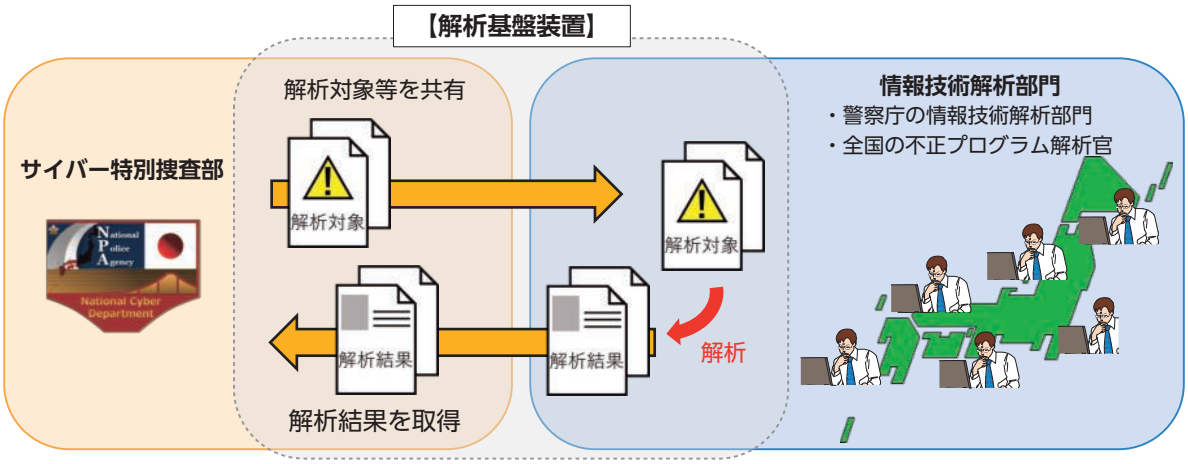
（3）捜査支援

サイバー特別捜査部では、捜査の過程で押収した不正プログラムや犯行に利用されたサーバ等を解析し、被疑者検挙につながる情報や被害回復に有用な情報等を捜査している。

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、不正プログラム等の解析には極めて高い技術力が求められている。このような状況に対応するため、警察庁は、全国の情報通信部に設置された情報技術解析課の中から、不正プログラムの解析に関し特に高い素養を有する職員を不正プログラム解析官として指定しており、サイバー特別捜査部は、必要に応じてこれらの不正プログラム解析官と連携して捜査を実施している。

また、警察庁では、技術支援体制の強化に向け、全国の情報技術解析部門の限られた人的・物的資源を効率的かつ最大限に活用するため、全国を結ぶネットワークを通じて、高度な解析を実施するためのソフトウェアの共有・利用や相互支援を可能とする解析基盤装置を運用しており、サイバー特別捜査部、警察庁の情報技術解析部門及び不正プログラム解析官の間で、技術的知見や解析結果を共有している。

図表特－12 サイバー特別捜査部・警察庁・不正プログラム解析官の連携体制



3 捜査のための基盤整備

（1）人材確保

❶ 都道府県警察からの出向・派遣

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・育成に取り組んでいる。特に、サイバー特別捜査部においては、都道府県警察から、サイバー分野の知見を豊富に持つ人材を登用している。

全国の重大サイバー事案への対処に日々当たるサイバー特別捜査部への出向・派遣は、当該捜査員の能力の向上につながり、ひいては当該捜査員の帰任後の都道府県警察全体のサイバー事案対処能力向上に寄与するものとなっている。警察では、こうした出向・派遣の意義を踏まえ、同部への出向・派遣を都道府県警察の捜査員のキャリアパスの一つと位置付け、出向・派遣に向けた各種研修等を通じて捜査員を計画的に育成するとともに、出向・派遣後も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を構築するよう取り組んでいる。

また、都道府県警察においては、サイバー特別捜査部への出向・派遣も念頭に置きつつ、中途採用・特別採用によって、高度な専門的知識及び技術を有するサイバー人材の採用を推進している。例えば、転職サイトを通じたＩＴ人材の募集活動や、サイバー分野に関連のある大学、高等専門学校、工業高校等を対象とした説明会の開催、合同企業説明会への積極的な参加等、効果的な採用募集活動を行っている。さらに、学生が参加することのできるサイバーコンテストの開催やサイバー防犯ボランティア(注1)に対する支援を通じて人材の発掘にも努めている。

❷ サイバー採用

警察庁では、令和７年度から、高度な専門的知識及び技術を有するサイバー人材の確保のための新たな取組として、高度な民間試験(注2)の合格者等を対象に、警察庁独自の採用試験を実施し、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採用する、サイバー採用を開始した。

サイバー採用によって採用された技術系職員は、採用後、警察学校及び職場における教育訓練を通じて、重大サイバー事案への対処等に必要な知識・能力を早期に習得した上で、その専門性を生かし、主として警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において勤務することとなる。

MEMO 高度なサイバーセキュリティ技術を有する民間人材の採用

深刻化するサイバー空間上の脅威への対応に当たり、警察組織の能力強化を目的として、特に高度な技術を有する民間人材を非常勤の国家公務員として採用する取組が開始された。令和８年６月に重大サイバー事案対策戦略官として採用された小河哲之氏は、民間企業での勤務を継続しながら、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において、重大サイバー事案に関する技術的知見の提供や警察組織における人材育成に関する助言等の幅広い業務に取り組んでいる。

新たに採用された小河重大サイバー事案対策戦略官

注１：138頁参照（第３章）
　２：情報処理安全確保支援士試験又は情報処理技術者試験（高度試験又は応用情報技術者試験）

MEMO 中途採用・官民人事交流制度により採用した幹部警察官の活躍

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を指揮している。

サイバーセキュリティ関連企業出身の濵石佳孝警視正は、官民人事交流制度により平成31年４月及び令和５年10月の２度にわたって警察庁に採用された。現在は、民間企業で培った最新の知見を生かし、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・分析業務の一層の高度化に取り組んでいる。


事件捜査を指揮する丸山篤警視正


分析業務に従事する濵石佳孝警視正

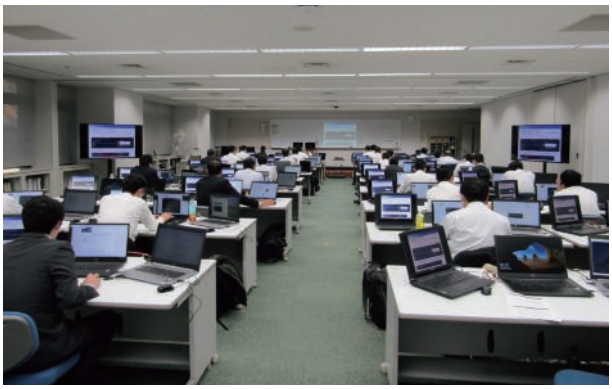
（2）人材育成

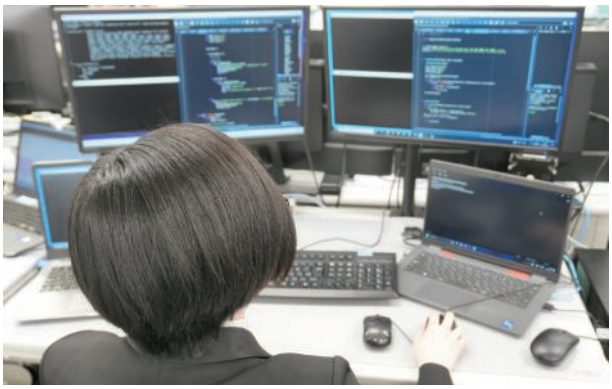
サイバー人材を確保・育成する取組は部門横断的に推進する必要があるところ、警察庁では、都道府県警察等の指導体制をリードしていくための司令塔的存在として、指導・人材育成部門の体制強化を図っている。

また、平成30年度以降、警察大学校にサイバーレンジ(注)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、最新の手口によって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の実施を可能としている。同サイバーレンジは、高度な専門的知識・技術を必要とするサイバー事案への対処能力を習得するために活用されている。

さらに、あらゆる犯罪にサイバー空間が悪用されていることから、深刻化するサイバー空間の脅威に的確に対処し、組織を挙げて全職員の対処能力の向上を図るため、都道府県警察からも同サイバーレンジを遠隔利用できるようにネットワークを整備するとともに、全ての警察職員を対象として、初級、中級及び上級に区分したサイバー対処能力検定を実施している。

加えて、都道府県警察では、警察学校及び職場における教育訓練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、警察学校での教育訓練を通じてサイバー人材を育成する観点から、警察学校に、サイバー事案捜査に関する教育訓練を実施できる教官の配置を推進している。


サイバーレンジによる捜査演習

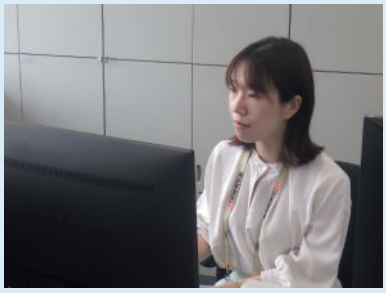

サイバーレンジによる遠隔訓練

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

MEMO 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。

茨城県警察本部生活安全部サイバー捜査課に所属していた溝井由樹子巡査長（当時）は、育児を行いながらサイバー分野について深く学び、令和７年度に開催したサイバーコンテストの「デジタル・フォレンジック(注)部門」で上位入賞した。その後、高度な専門的知識・技術を習得した経験を生かして、関東管区警察局茨城県情報通信部情報技術解析課に技官として出向し、デジタル・フォレンジックを活用した技術支援の第一線で活躍している。



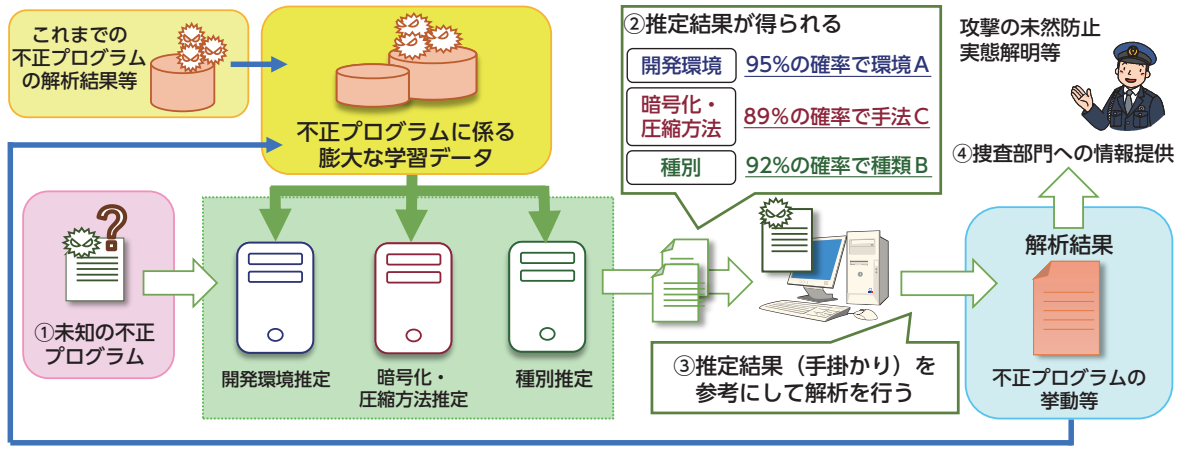
関東管区警察局茨城県情報通信部
情報技術解析課にて活躍する溝井技官

（3）資機材の整備と新技術の導入

重大サイバー事案や匿名・流動型犯罪グループによるサイバー空間の匿名性を悪用した犯罪を含むサイバー事案では、被疑者等の所在地と被害発生地の地理的関連性が希薄であるほか、捜査を要するサーバの設置場所等も全国に散在しているため、複数の都道府県警察が共同して捜査活動を行わなければ事案の解明が困難である。そこで、サイバー特別捜査部では、サイバー事案の手口や暗号資産の取引情報等の被疑者の特定や犯罪組織の実態解明に資する情報を、全国的に集約・分析するとともに、そのための資機材を整備している。

また、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を用いたサイバー事案が発生している。こうした状況を踏まえ、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。

図表特－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



MEMO 生成ＡＩを悪用するマルウェア

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を悪用して不正な命令を生成することが確認された。

注：犯罪の立証のための電磁的記録の解析技術及びその手続

第2節 能動的サイバー防御の導入に向けて

1 重大なサイバー攻撃の発生と対処事例

（1）重大なサイバー攻撃の発生事例

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である一方で、サイバー空間をめぐる脅威は、極めて深刻な情勢にあり、世界各地で機密情報や暗号資産の窃取、重要インフラの機能停止等を企図したとみられるサイバー攻撃が相次いで発生している。

❶ 機密情報の窃取を企図したとみられるサイバー攻撃

令和６年（2024年）７月、米国連邦捜査局は、英国、韓国等の関係機関と共に、北朝鮮を背景とするサイバー攻撃グループ「Andariel」によるサイバー攻撃に関する注意喚起を行った。同サイバー攻撃グループは、北朝鮮の軍事・原子力施策を発展させる目的で、米国、英国、韓国を含む世界各国の防衛、航空宇宙、原子力等の産業分野を標的として、機密情報等を窃取したとみられている。

❷ 暗号資産の窃取を企図したとみられるサイバー攻撃

令和６年（2024年）３月に発表された国際連合安全保障理事会北朝鮮制裁委員会専門家パネル(注１)による最終報告書では、北朝鮮における外貨収入の約半分はサイバー攻撃により獲得され、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ている。

また、令和７年（2025年）10月、多国間制裁監視チーム（ＭＳＭＴ(注２)）は、令和６年（2024年）１月から令和７年（2025年）９月にかけて、北朝鮮が少なくとも28億米国ドル相当の暗号資産を窃取した旨の報告書を公表した。

❸ 重要インフラの機能停止等を企図したとみられるサイバー攻撃

令和４年（2022年）５月、EUやウクライナ等は、ウクライナ侵略の約１時間前にロシアが行った、国際衛星通信へのサイバー攻撃について非難声明を発表した。当該サイバー攻撃は、ウクライナの公共機関等に通信障害を引き起こすなど、軍事的侵略を助長したとされている。

また、令和６年（2024年）２月、米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（ＣＩＳＡ(注３)）及び複数国の関係機関は、中国を背景とするサイバー攻撃グループ「Volt Typhoon」による米国の重要インフラ事業者への侵害が確認されたことを公表し、注意喚起を行った。同サイバー攻撃グループは、有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークにアクセスできるようにしている。また、同サイバー攻撃グループは、そのためにLiving Off The Land戦術(注４)等を用いるなど、サイバー攻撃の検知を回避するための高度な能力を有しているとみられている。

Volt Typhoonに対する注意喚起(注５)

注１：北朝鮮に関する安保理決議の実効性を向上させるため、安保理決議1874号に基づき設置されたが、令和６年３月、マンデート更新に関する安保理決議案にロシアが拒否権を行使したため、専門家パネルは同年４月で活動を終了した。
２：Multilateral Sanctions Monitoring Teamの略。国際連合安全保障理事会北朝鮮制裁委員会専門家パネルの活動が終了したことを受け、日米韓をはじめとする同志国によって設立された。
３：Cybersecurity and Infrastructure Security Agencyの略
４：不正に侵入したシステム内に組み込まれている正規の機能等を用いることで、正規の操作との区別がつきにくくなり、当該サイバー攻撃の検知を困難にする戦術
５：https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

注５

（2）重大なサイバー攻撃への対処事例

欧米主要国等では、重大なサイバー攻撃への対策として、サイバー攻撃グループに関与しているとみられる企業に対する制裁や、被害の未然防止・拡大防止に向けた注意喚起、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を実施しているほか、サイバー攻撃グループが攻撃に悪用しているボットネット(注1)等に対する無害化措置を実施している。

❶ 制裁、注意喚起及びパブリック・アトリビューション

令和７年（2025年）１月、米国財務省外国資産管理局は、中国四川省を拠点とするサイバーセキュリティ企業が、中国を背景とするサイバー攻撃グループ「Salt Typhoon」の活動に関与したとして、同企業に対する制裁を公表した。

また、令和７年（2025年）７月、英国外務・英連邦・開発省（ＦＣＤＯ(注2)）等は、欧州各国を標的としたサイバー攻撃に関与したとして、ロシア軍参謀本部情報総局（ＧＲＵ）の部隊及びＧＲＵの幹部職員を含む関係者18人に対する制裁を公表した。さらに、英国国家サイバーセキュリティセンター（ＮＣＳＣ(注3)）は、ＧＲＵの部隊に属するサイバー攻撃グループ「APT28」が、マイクロソフト社が提供するサービスへのアクセスを行うための認証情報等を窃取する「AUTHENTIC ANTICS」という高度なマルウェアを使用していたとして注意喚起を実施した。

❷ 無害化措置

令和６年（2024年）９月、米国司法省は、中国を背景とするサイバー攻撃グループ「Flax Typhoon」が情報窃取等を目的としたサイバー攻撃に用いているとされているボットネットを無害化するオペレーションを実施したと公表した。

また、令和７年（2025年）６月、ＩＣＰＯは、アジア・南太平洋地域における情報窃取型マルウェアの「Infostealer」の捜査・対策を行うための国際共同捜査であるオペレーション「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連携し、関係サーバの管理者に働き掛けるなどして、サーバのテイクダウン（機能停止）を実施した旨を公表した。


PRESS RELEASE

Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers

Wednesday, September 18, 2024

For Immediate Release
Office of Public Affairs

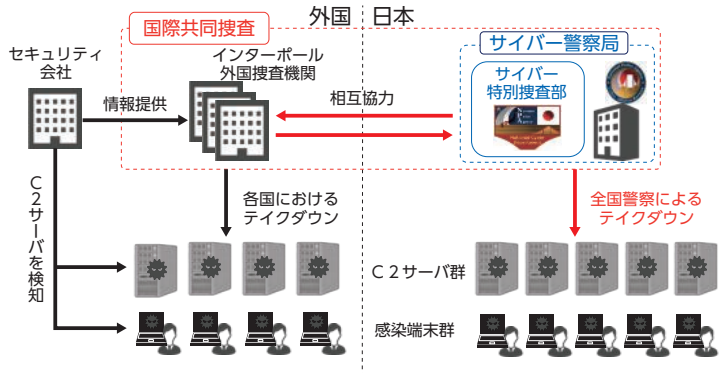
Actors Unsuccessfully Sought to Prevent FBI's Disruption of Botnet

The Justice Department today announced a court-authorized law enforcement operation that disrupted a botnet consisting of more than 200,000 consumer devices in the United States and worldwide. As described in court documents unsealed in the Western District of Pennsylvania, the botnet devices were infected by People's Republic of China (PRC) state-sponsored hackers working for Integrity Technology Group, a company based in Beijing, and known to the private sector as "Flax Typhoon."

The botnet malware infected numerous types of consumer devices, including small-office/home-office (SOHO) routers, internet protocol (IP) cameras, digital video recorders (DVRs), and network-attached storage (NAS) devices. The malware connected these thousands of infected devices into a botnet, controlled by Integrity Technology Group, which was used to conduct malicious cyber activity disguised as routine internet traffic from the

ボットネットの無害化に係る広報状況(注4)

図表特－14　Infostealerに対するテイクダウンの概要



注１：攻撃者の命令に基づき動作する不正プログラム（ボット）に感染したコンピュータ及びこれらのコンピュータに攻撃者の命令を送信する命令サーバから成るネットワーク
２：Foreign, Commonwealth & Development Officeの略
３：National Cyber Security Centreの略
４：https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

注４

2 日本における能動的サイバー防御の必要性の高まり

（1）国内のサイバー空間における治安課題

日本国内においても、機密情報や暗号資産の窃取、重要インフラの機能停止等を企図したとみられるサイバー攻撃が発生している。警察では、こうしたサイバー攻撃に適切に対処するため、迅速かつ的確な捜査を推進するとともに、パブリック・アトリビューションをはじめとする被害の未然防止・拡大防止に向けた取組を推進している。

❶ 国内におけるサイバー攻撃

令和７年１月、警察庁は、「MirrorFace」と呼ばれるサイバー攻撃グループが、令和元年頃から、日本国内のシンクタンク、政府、政治家、報道機関に関係する個人及び組織に対し、情報窃取を目的としたサイバー攻撃を行っていることを確認するとともに、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、注意喚起を実施した。

また、令和５年８月、内閣サイバーセキュリティセンター（ＮＩＳＣ(注1)）（令和７年７月に内閣官房国家サイバー統括室（ＮＣＯ(注2)）に改組）及び気象庁は、電子メール関連機器のぜい弱性を悪用したとみられる不正アクセスを受け、メールデータの一部が外部に漏えいした可能性があると発表した。

❷ 警察庁が実施したパブリック・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3)）及び米国国防省サイバー犯罪センター（ＤＣ３(注4)）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約482億円相当の暗号資産を窃取したことを特定し、連名で公表した。

TraderTraitorに対するパブリック・アトリビューション(注5)

また、令和７年８月、警察庁及び国家サイバー統括室は、中国を背景とするサイバー攻撃グループ「Salt Typhoon」が、中国の情報機関に製品やサービスを提供している複数の中国企業と連携して悪意ある活動を実施しており、当該活動を通じて取得されたデータによって、対象者の通信や移動等を追跡することが可能となっていると評価されたことを受け、米国、英国等の関係機関と共に、当該活動に関する「国際アドバイザリー」に共同署名した。

Salt Typhoonに対するパブリック・アトリビューション(注6)

注１：National center of Incident readiness and Strategy for Cybersecurityの略
２：National Cybersecurity Officeの略
３：Federal Bureau of Investigationの略
４：Department of Defense Cyber Crime Centerの略
５：https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom
６：https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf

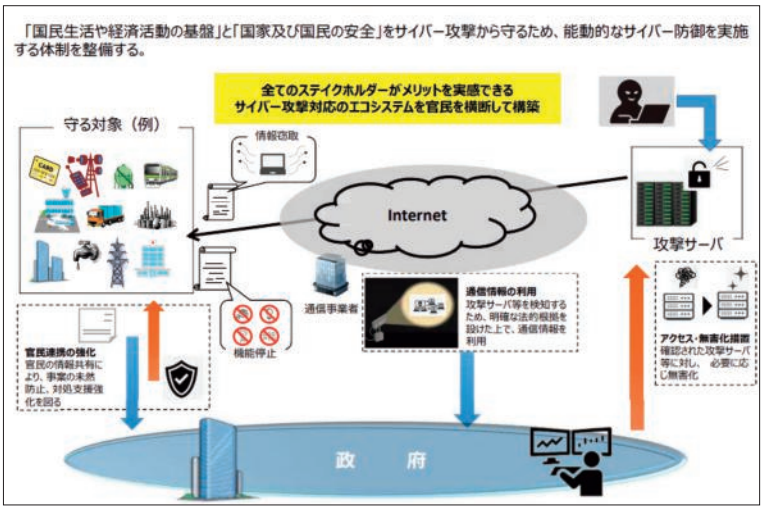
注５ 注６

（2）サイバー対処能力強化法及び同整備法の成立

安全保障上の課題として、サイバー攻撃による機密情報や暗号資産の窃取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おり、特に、重要インフラの機能停止、破壊等を目的とした国家を背景とするサイバー攻撃は世界的規模で発生している。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」ことが目標に掲げられ、重大なサイバー攻撃の未然の排除やサイバー攻撃発生時の被害拡大防止のための能動的サイバー防御を導入すべく、実現に向けた検討を進めることとされた。

同戦略に基づき、政府は、令和６年６月から約６か月間にわたり、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、経済界、アカデミア、法曹界、メディア等の有識者による「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」を開催した。また、同年11月には、「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、「官民連携の強化」、「通信情報の利用」及び「アクセス・無害化措置」の３つの取組について実現すべき具体的な方向性が示された。このうち、アクセス・無害化措置に関しては、警察官職務執行法（以下「警職法」という。）を参考に危害防止のための措置を即時的に実施できる法制度とすべきことや、警察や防衛省・自衛隊が保有する能力・機能を十全に活用すべきこと等が提言された。

第４回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
（首相官邸ウェブサイト）



注：国家サイバー統括室作成資料より抜粋
有識者会議における提言の全体イメージ

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。

3 強化法及び整備法

（1）強化法及び整備法の全体像

強化法及び整備法では、サイバーセキュリティが害された場合に、国家及び国民の安全を害したり、国民生活又は経済活動に多大な影響を及ぼしたりするおそれのある国等の重要な電子計算機に対する不正な行為による被害の防止を図るために、「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。

❶ 官民連携の強化

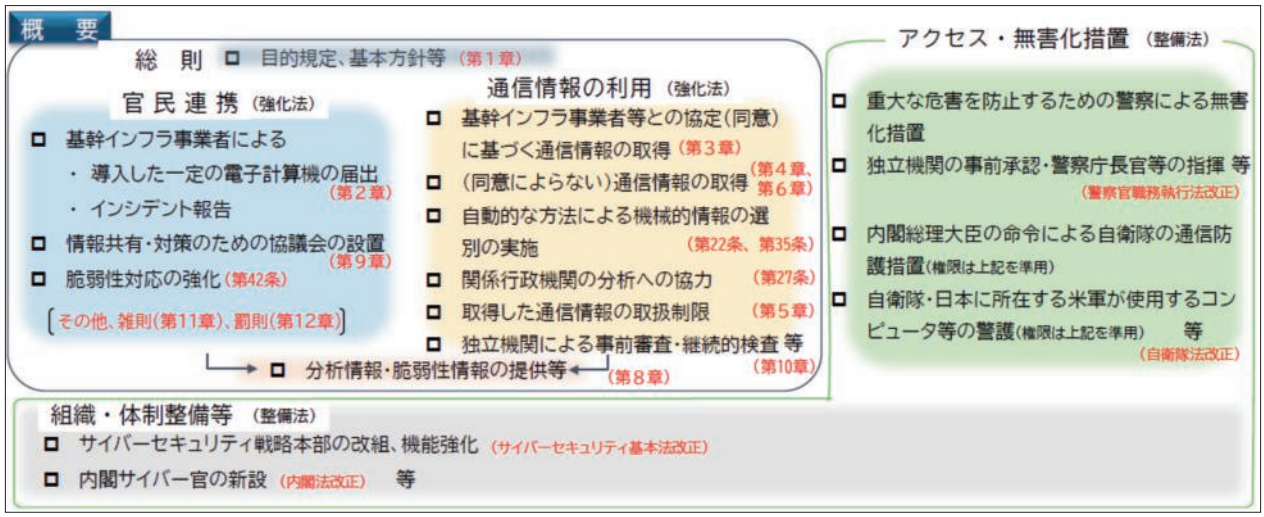
国家を背景とするサイバー攻撃グループ等による、高度なサイバー攻撃に対しては、官のみ又は民のみでの対策では限界があるため、官民が連携し、一体となって我が国全体のサイバー防御能力を高めることが必要である。このため、強化法において、基幹インフラ事業者がサイバー攻撃を受けた場合の政府への報告や、被害の防止のための情報共有及び対策に関する協議会の設置等、官民の連携を強化するための規定が設けられた。

❷ 通信情報の利用

重大なサイバー攻撃においては、攻撃者が、攻撃元を隠蔽（いんぺい）するため、ボットネットを用いてサイバー攻撃を行うのが通例である。このようなサイバー攻撃の詳細を事前に把握するため、強化法において、基幹インフラ事業者等から提供された通信情報を利用する規定が設けられた。その通信情報の利用に当たっては、憲法が保障する通信の秘密を不当に侵害することのないよう、サイバー攻撃に関係があると認めるに足りる機械的情報を自動的に選別することとされた。

❸ 攻撃者のサーバ等へのアクセス・無害化措置

日常的かつ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・無害化措置をはじめとする新たな施策を組み合わせるなど、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。そこで、整備法において、攻撃者のサーバ等へのアクセス・無害化措置を実施するための規定が設けられた。



注：国家サイバー統括室作成資料より抜粋

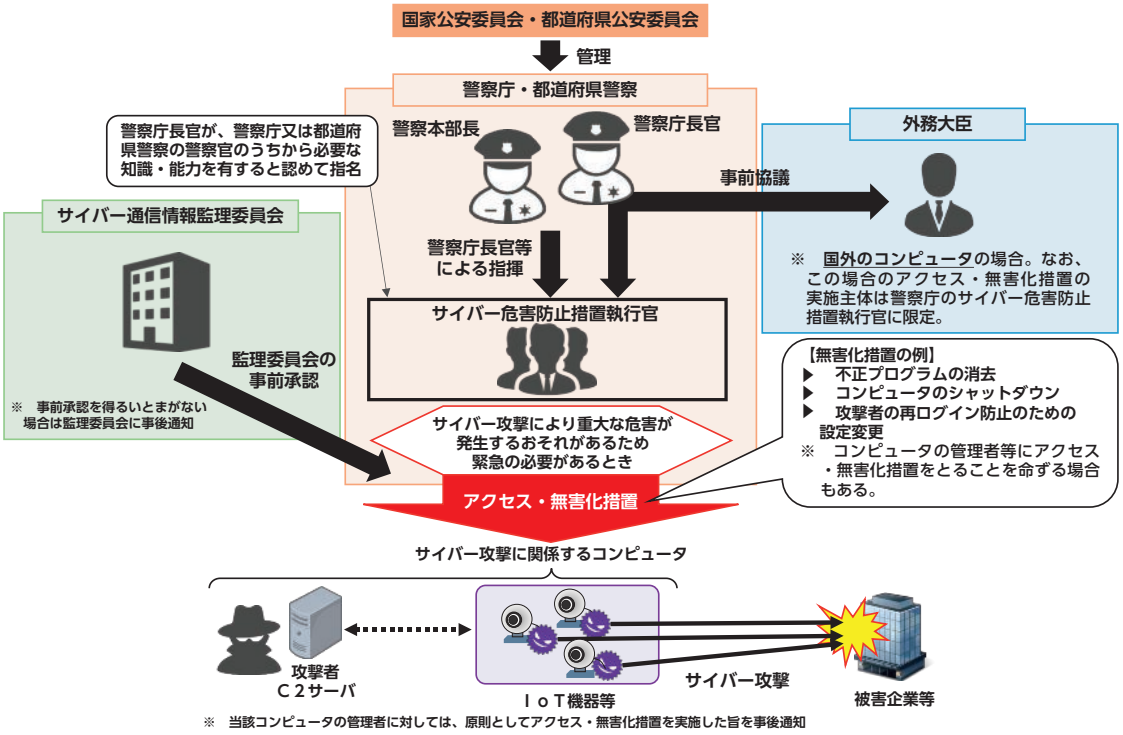
強化法及び整備法の概要

（2）改正警職法によるアクセス・無害化措置

重要インフラ等の機能停止や機微な情報の窃取といった重大なサイバー攻撃を未然に防止し、また、実際に発生した場合にその被害の拡大を防止する措置は、個人の生命、身体及び財産を保護し、その他公共の安全と秩序の維持に当たることを責務とする警察において実施することとなる。そこで、整備法により警職法の一部が改正され、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。同規定では、サイバーセキュリティを害することその他情報技術を用いた不正な行為に用いられる加害関係電気通信等を認めた場合であって、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にアクセス・無害化措置をとることが可能とされている。そのほか、アクセス・無害化措置の適正な実施を確保するため、サイバー通信情報監理委員会の事前承認や外務大臣との協議等についても定められている。

警察は、整備法の施行日(注)以降、アクセス・無害化措置を担うこととなる。措置の実施に当たっては、基幹インフラ事業者から提供された情報等を収集・分析し、サイバー攻撃に悪用されているサーバ等（以下「攻撃サーバ等」という。）を特定した上で、以下に掲げるような必要な手続を経て、攻撃サーバ等にアクセスし、無害化措置を講ずることとなる。

図表特－15　改正警職法の概要



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10月１日に施行される。

❶ サイバー危害防止措置執行官の指名

アクセス・無害化措置の実施に当たっては、警察庁長官が、サイバー特別捜査部に所属する警察官をはじめとするアクセス・無害化措置に必要な知識及び能力を有する警察官を、「サイバー危害防止措置執行官（以下「執行官」という。）」として指名し、その者に限ってアクセス・無害化措置を実施することとされている。

❷ 外務大臣との協議

攻撃サーバ等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、アクセス・無害化措置が国際法上許容される範囲内で実施されることを確保する観点から、事前に外務大臣と協議することとされている。

❸ サイバー通信情報監理委員会の承認

執行官が行うアクセス・無害化措置は、原則として、事前に、独立機関として設置されたサイバー通信情報監理委員会の承認を得て実施することとされている。これは、アクセス・無害化措置が、警職法の要件を満たした上で実施されることを担保するためである。

なお、現に攻撃サーバ等からサイバー攻撃を受けているなど、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、事前にサイバー通信情報監理委員会の承認を得ずにアクセス・無害化措置を実施することが可能となっている。このような場合であっても、アクセス・無害化措置が適正に実施されたことを明らかにするため、当該措置の実施後速やかに、サイバー通信情報監理委員会へ通知を行い、確認を受けることとされている。

❹ アクセス・無害化措置の実施

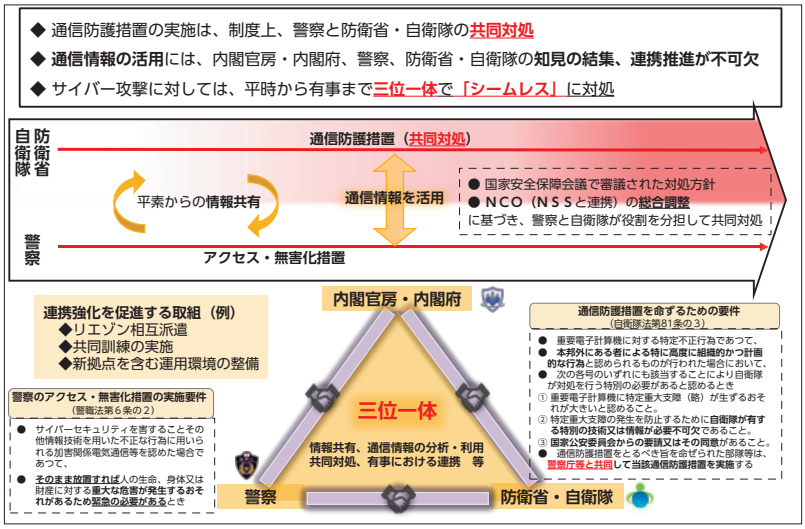
以上のような手続を経て初めて、執行官がアクセス・無害化措置を実施することとなる。具体的には、攻撃サーバ等に対し、ネットワークを介してアクセスした後、不正プログラムの消去、攻撃者の利用しているアカウントの削除等の通常必要と認められる措置を実施することとなる。

❺ 攻撃サーバ等の管理者への事後通知

アクセス・無害化措置は、ネットワークを介して遠隔地の攻撃サーバ等に対して実施することとなるため、攻撃サーバ等の管理者が認知しないまま、アクセス・無害化措置を実施することが可能となる。そこで、実施したアクセス・無害化措置が、執行官の正当な職務又は命令によるものであることを相手方が確認できるようにするため、攻撃サーバ等の管理者の所在が不明であるなどの一部の場合を除き、遅滞なく、アクセス・無害化措置を実施したことを攻撃サーバ等の管理者に通知することとされている。

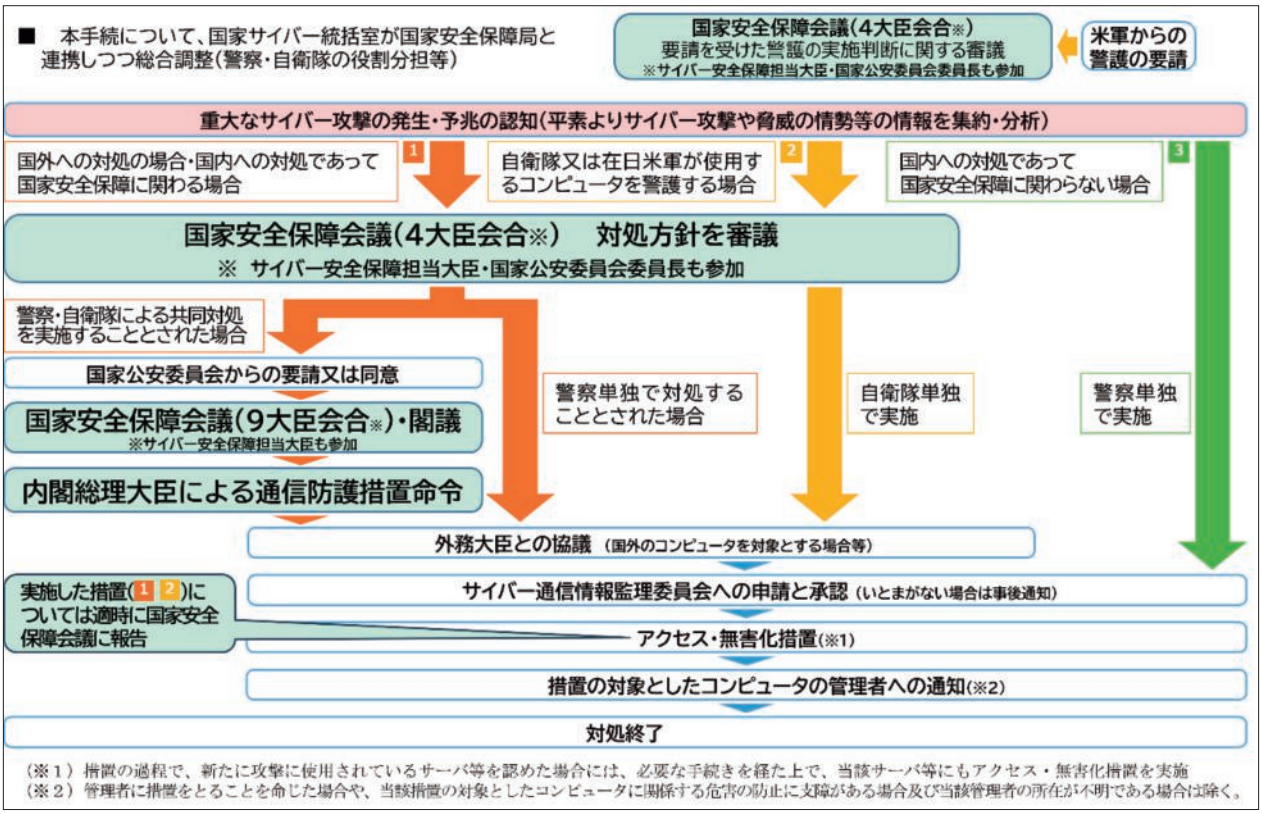
4 施行に向けた警察の取組

アクセス・無害化措置は、警察に新たに課せられた重要な任務であり、当該措置の対象となるサイバー攻撃は、一義的には警察が対処を行うこととなる。他方、こうしたサイバー攻撃の中には国家安全保障に関わる事案が含まれ得るほか、自衛隊が有する特別の技術又は情報が必要不可欠である事案もあり、こうした事案においては警察が自衛隊と共同して対処することとなる。これらを踏まえると、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となってシームレスな対応を行うことにより、サイバー攻撃による被害の防止を図る必要がある。



内閣官房・内閣府、警察、防衛省・自衛隊の三位一体の対処

警察庁では、強化法及び整備法の施行に向けて、人材の確保・育成や資機材の整備といった人的・物的基盤の強化による体制整備を図るなど諸準備を進めている。警察は、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」を踏まえつつ、引き続き、ＡＩを活用した資機材の導入等を含め、運用開始に向けた諸準備を継続し、サイバー対処能力の一層の向上を図っていくこととしている。



注：国家サイバー統括室作成資料より抜粋

アクセス・無害化措置の運用に関する指針

第3節 今後の展望

地理的・時間的制約の少ないサイバー空間が社会に様々な便益をもたらしている反面、サイバー空間を取り巻く情勢が一層深刻化していることは、これまで述べたとおりである。サイバー空間の匿名性を悪用した犯罪やサイバー攻撃は、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かつ致命的な影響を及ぼすおそれがあるため、警察としてこれに対処することは急務である。

このため、警察では、「警察におけるサイバー戦略」(注)（令和８年４月改定）に基づき、今後、次のような取組を推進することとしている。

（１）検挙に向けた取組

国家を背景とするサイバー攻撃や匿名・流動型犯罪グループによる特殊詐欺をはじめとした様々な犯罪が深刻化していることを踏まえ、被疑者の特定や暗号資産の形で隠匿された犯罪収益の解明等を含め、高度な専門的知識・技術に基づく捜査に取り組んでいく。その上で、得られた情報をサイバー特別捜査部に集約し、横断的・俯瞰（ふかん）的分析を行うことで、各事案の関連性や背景にある組織性、犯罪グループの上位被疑者等を浮き彫りにし、更なる検挙を推進していく。

また、被疑者が国内に所在しない場合であっても、警察庁を通じた国際共同捜査による検挙を目指して捜査を徹底していく。そのために、警察庁では、国際共同捜査への積極的な参画に向けて、外国治安機関等とのハイレベルの調整や情報・運用面を含めた協力関係の強化に取り組んでいく。

さらに、平素からの官民連携の推進によって、民間企業等による警察への通報・相談を促進するほか、サイバー事案の捜査に当たっては適正性の確保に配意する。

（２）未然防止・拡大防止に向けた取組

サイバー空間の匿名性を悪用した事案による被害の未然防止・拡大防止のため、被疑者の検挙を通じた将来の事案の抑止を図っていくほか、パブリック・アトリビューション等を通じた情報発信や、地域に根差した官民連携による広報啓発活動等を推進していく。

また、事件検挙を通じたいわゆる「道具屋」（不正に調達した預貯金口座等を犯罪グループに提供する者）や「相対屋」（暗号資産交換を個人が無登録で業として行う者）等の解体、サイバー攻撃の攻撃元であるサーバ等の閉鎖、サイバー事案の踏み台とされている家庭用インターネット通信機器に関する対策、ＳＮＳ事業者等への情報提供を通じた違法・有害情報への対処の推進等、サイバー空間の悪用を容易にする犯罪インフラへの対処を推進していく。

さらに、警察では、サイバー特別捜査部に全国の人的・物的リソースを集約した上、国家安全保障上の脅威をはじめとしたあらゆる情報を集約し、内閣官房や防衛省等と緊密に連携しつつ、アクセス・無害化措置の効果的な実施を図ることとしている。

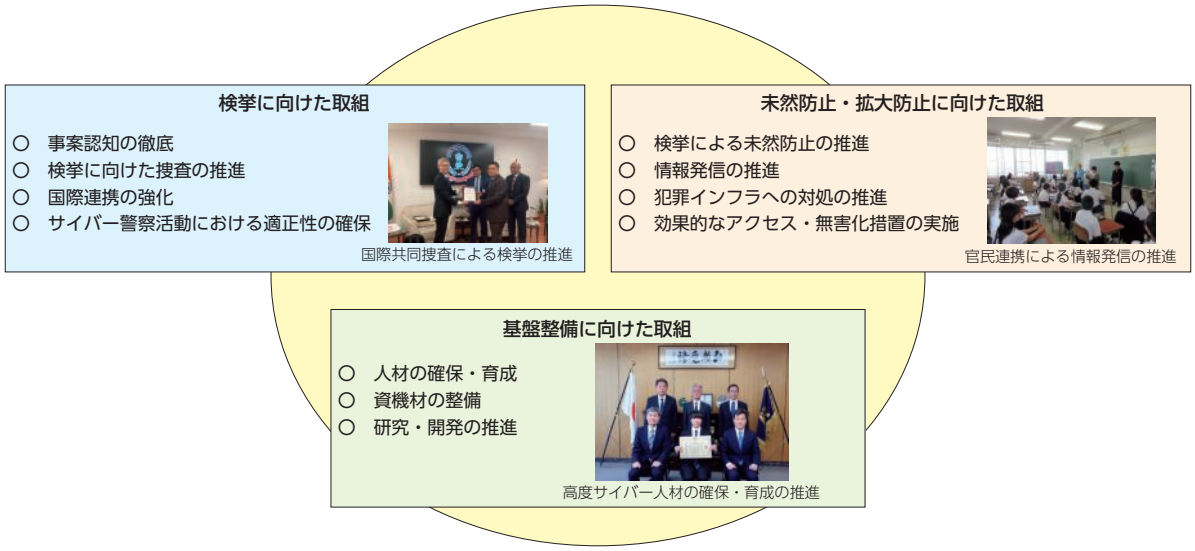
注：https://www.npa.go.jp/bureau/cyber/pdf/20260402.pdf

（3）基盤整備に向けた取組

あらゆる種類の犯罪にサイバー空間が悪用されていることから、（1）及び（2）のような取組の推進のため、全警察職員のサイバー対処能力の向上を図るとともに、アクセス・無害化措置をはじめとする能動的サイバー防御を担い得る高度なサイバー人材の確保・育成に組織を挙げて取り組んでいく。

また、ＡＩを活用した資機材や捜査に不可欠な解析用資機材等の高度な資機材の効果的かつ効率的な整備・運用を行うほか、ランサムウェアに係る復号ツールの開発等、研究・開発を推進していく。

図表特－16　警察におけるサイバー戦略



（1）から（3）までの取組の実施主体として、サイバー特別捜査部を含めた警察庁及び都道府県警察がこれまで以上に緊密に連携していくことが重要である。警察では、将来を見据えた警察組織の構造改革(注)を推進しているところ、都道府県警察においては、（1）から（3）までの取組を更に効果的に進めるため、サイバー部門の一元化組織の整備を検討することとした。具体的には、令和８年５月、警察法施行令に規定される警視庁及び道府県警察本部の内部組織の基準が改正され、サイバー警察事務を一元的に所掌する組織を設置できることが示された。

都道府県警察においては、各都道府県の実情を踏まえた上で、ますます巧妙化するサイバー事案への対処を部門横断的に推進する司令塔となる、適切な組織を整備する。

警察では、深刻化するサイバー空間の脅威に対して、全国隅々にまで張り巡らされた体制に裏付けられた対処能力を駆使し、今後も国民の期待と信頼に応えていく。

注：254頁参照（第７章）