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、フィッシング(注2)に起因するとみられる証券口座に係る不正取引が多発したほか、クレジットカード不正利用被害及び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、規制薬物の広告、犯罪実行者募集情報等の違法情報や、自殺誘引等情報(注3)、爆発物の製造方法、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4)の検挙件数

令和７年（2025年）中のサイバー事案の検挙件数は、4,154件であった。

（2）不正アクセス禁止法違反

令和７年中の不正アクセス禁止法違反の検挙件数は431件と、前年より132件（23.4%）減少し、検挙人員は248人と、前年より11人（4.2%）減少した。検挙件数を不正アクセス行為の手口別内訳でみると、他人の識別符号を無断で入力する「識別符号窃用型」を手口とする不正アクセス行為の検挙件数が399件（92.6%）と最多であった。

また、令和７年中の不正アクセス行為の認知件数(注5)は7,190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4,747件（66.0%）と最多であった。

（3）コンピュータ・電磁的記録対象犯罪(注6)

令和７年中のコンピュータ・電磁的記録対象犯罪の検挙件数は1,253件と、前年より98件（8.5%）増加した。

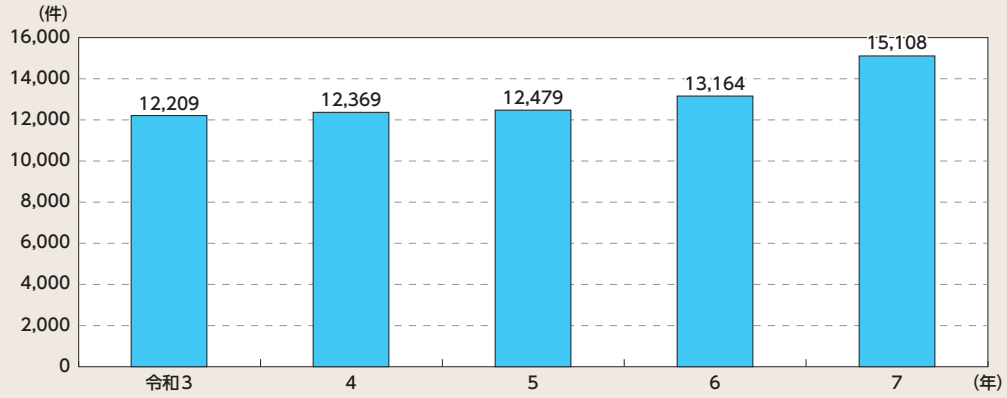
注１：Distributed Denial of Serviceの略。特定のコンピュータに対し、複数のコンピュータから大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃
２：２頁参照（特集）
３：他人を自殺に誘引・勧誘する情報等
４：サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案。サイバー事案への対策については130頁参照
５：不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を認知した場合、報道を踏まえて事業者等に不正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
６：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

（４）サイバー犯罪(注１)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７年中の検挙件数は１万5,108件と、前年より1,944件（14.8%）増加し、過去最多を記録した。

図表３－１　サイバー犯罪の検挙件数の推移（令和３年～令和７年）



memo　少年によるサイバー犯罪

令和７年に不正アクセス禁止法違反で検挙された248人の被疑者のうち、14歳から19歳までの者が81人（32.7%）であるなど、少年が実行するサイバー犯罪が目立っており、以下のような事例が発生している。

CASE

サイバーパトロールによる取締りを行った結果、大学生の男（19）が、令和６年５月から令和７年５月にかけて、オンラインカジノを利用したほか、同年１月から同年２月にかけて、内閣総理大臣の登録を受けないでオンラインカジノの利用者の電子マネー等を暗号資産に交換していたことが判明した。同年10月、同男を常習賭博罪、資金決済に関する法律違反等で逮捕した。同取締りの結果、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）らを常習賭博罪で児童相談所に通告するなど、合計20人を常習賭博罪等で検挙又は児童相談所に通告した（警視庁）。

CASE

高校生の少年（17）は、令和７年１月、情報を窃取するプログラムを、生成ＡＩを悪用して作成し、それを利用してインターネットカフェ運営会社にサイバー攻撃を行うことで、正常な業務の遂行を困難にさせ、その業務を妨害した。同年12月、同少年を不正アクセス禁止法違反（不正アクセス行為）及び偽計業務妨害で逮捕した（警視庁）。

CASE

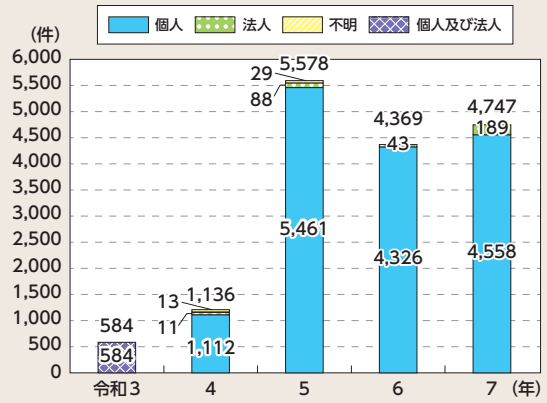
ＳＮＳを通じて結び付いた14歳から16歳までの中学生及び高校生の少年らは、生成ＡＩを悪用して作成した、自動的に電気通信事業者が管理するサーバコンピュータにアクセスした上でｅＳＩＭ(注２)の契約を行うことができるプログラムを利用し、令和６年５月から同年８月にかけて、それぞれ不正に取得した他人のＩＤとパスワードを用いて不正にｅＳＩＭを契約し、転売した。令和７年１月から同年２月にかけて、同少年ら３人を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺罪で逮捕した（警視庁）。

注１：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
２：Embedded Subscriber Identity Moduleの略。契約者情報等をオンラインで書き込むことができるＳＩＭであって、携帯電話端末に組み込まれているもの

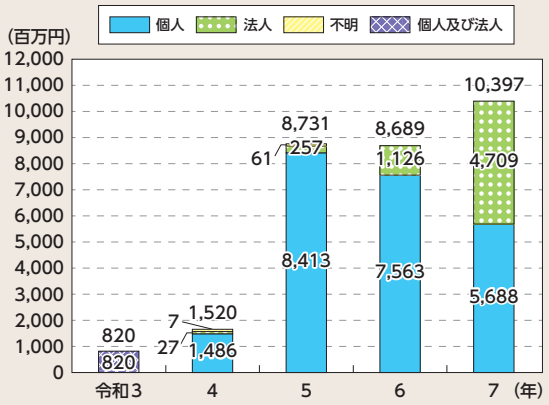
2 インターネットバンキングに係る不正送金事犯の情勢

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件と、依然として高い水準で推移している。また、ボイスフィッシング(注)による法人口座の不正送金被害が急増したことなどにより、被害額は約103億9,700万円と、過去最高となった。

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３年～令和７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３年～令和７年）

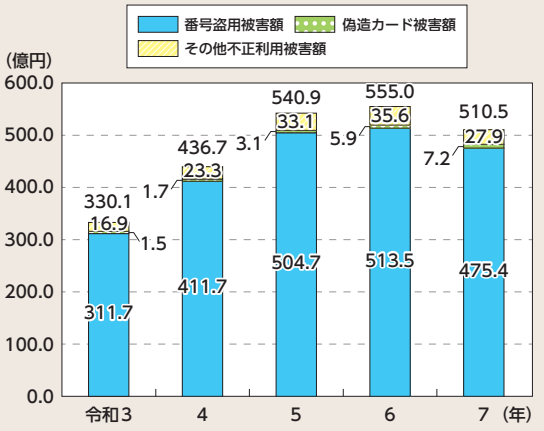


注：単位未満は四捨五入しているため、個々の数字の合計と総額は一致しない場合がある。

3 クレジットカードに係る不正利用被害の情勢

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に係る不正利用被害総額は約510億5,000万円と、依然として深刻な状況にある。そのうち、番号盗用による被害額は約475億4,000万円であり、その被害の多くは、クレジットカード会社等を装ったフィッシングによるものと考えられる。

図表３－４ クレジットカードの不正利用被害額の推移（令和３年～令和７年）



注：「クレジットカード不正利用被害の発生状況」（一般社団法人日本クレジット協会）から作成した。

注：138頁参照

4 ランサムウェアの情勢

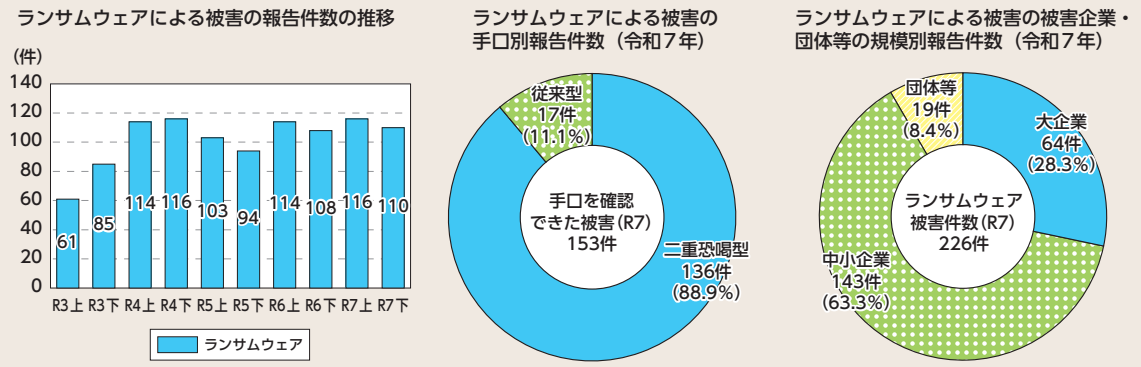
令和７年中のランサムウェアによる被害の報告件数(注１)は226件（令和７年上半期116件、下半期110件）であり、引き続き高い水準で推移している。こうした被害において、暗号化したデータを復元する対価として企業等に金銭等を要求する手口のほか、データを企業等から窃取した上で「対価を支払わなければ当該データを公開する」などと対価を要求する手口であるダブルエクストーション（二重恐喝）が認められる。対価を要求する手口を警察として確認したランサムウェアによる被害の報告件数153件のうち、ダブルエクストーションの手口によるものは136件であり、88.9%を占めている。

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64件、中小企業は143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92件のうち、ＶＰＮ機器(注３)を利用されて侵入された事例は61件（66.3%）、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19件（20.7%）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７年中17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機器の略。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

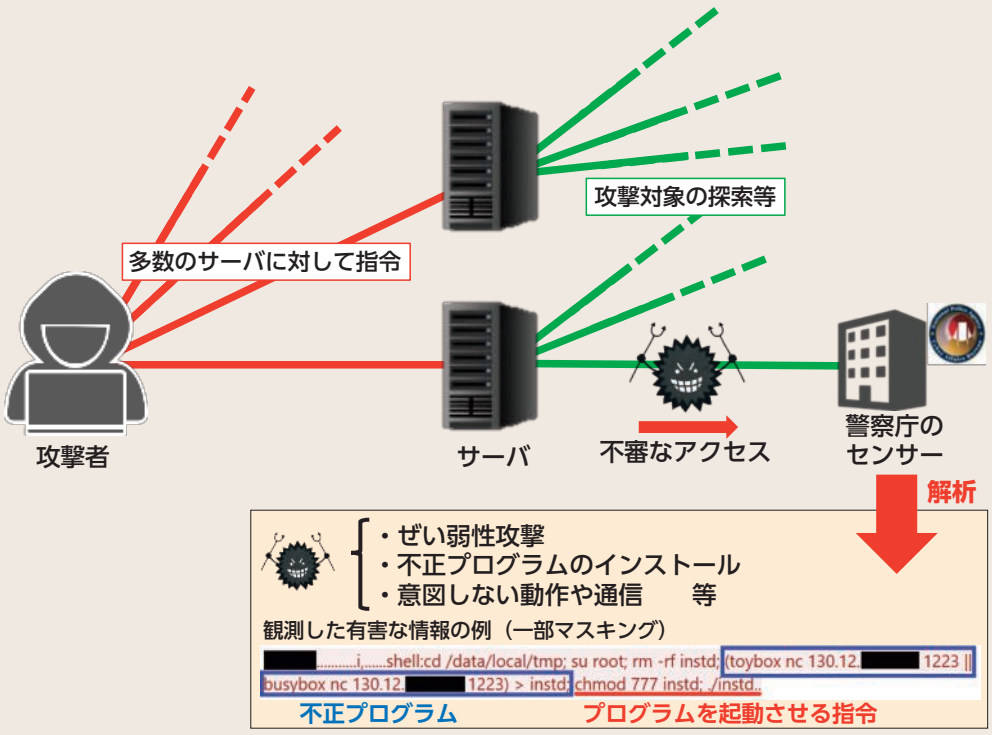
5 警察庁が検知した不審なアクセス

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(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。したがって、このセンサーを利用することで、ぜい弱性を有するＩｏＴ機器を攻撃者が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、不審な通信パケットを観測することができる。

このような不審なアクセスは、引き続き観測されており、中には、ＩｏＴ機器の設定変更等を行うための管理用のポート番号(注2)を宛先として、ユーザ名・パスワードを送信してＩｏＴ機器へのログインを試行したことが疑われる動向も観測されている。

警察では、こうした通信パケットを分析することで、サイバー攻撃の予兆となるぜい弱性の探索行為やサイバー攻撃の内容、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、これらの分析結果から、攻撃者の活動実態等を把握する取組を推進している。

図表３－６　不審な通信アクセス観測のイメージ



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：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。

6 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 「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、警察庁及び国家サイバー統括室（ＮＣＯ(注2)）は、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(注3)）豪州サイバーセキュリティセンター（ＡＣＳＣ(注4)）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(注5)」の共同署名に加わった。本文書は、情報システムに関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・維持・更新・強化に役立つアプローチを提供するものである。

「最新の防御可能なアーキテクチャのための基礎」

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：National Cybersecurity Officeの略
３：Australian Signals Directorateの略
４：Australian Cyber Security Centreの略
５：https://www.cyber.gov.au/sites/default/files/2025-10/foundations-for-modern-defensible-architecture.pdf

第2節 サイバー空間における脅威への対処

1 検挙に向けた取組

（1）検挙活動

警察では、サイバー空間をめぐる脅威に対処するため、検挙に向けた取組を推進している。都道府県警察のサイバー部門では、管轄する地域において必要な捜査を行っているほか、国の捜査機関であるサイバー特別捜査部では、都道府県警察と連携しながら、重大サイバー事案(注1)に対処している。また、電子機器やネットワークを利用したサービスが普及・多様化し、あらゆる犯罪に悪用されている中、サイバー部門では他部門の捜査力のみでは対処が困難な場合等における支援を推進している(注2)。

CASE

無職の男（36）らは、令和６年６月及び同年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ＩＤやパスワードといった識別符号を保管した。本件では、生成ＡＩを悪用して当該フィッシングサイトの改修が行われ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(注3)）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）。

（2）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・相談の促進

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4)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、インターネットからサイバー事案に関する通報・相談をすることができる一元的な窓口を運用している。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１：３頁参照（特集）
２：令和７年中のサイバー事案の検挙件数については124頁参照。令和７年中のサイバー犯罪の検挙件数については125頁参照
３：５頁参照（特集）
４：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

（３）犯罪の取締りのための技術支援体制

情報化社会の進展は、匿名性が高く、追跡が困難なサイバー空間を利用した様々な犯罪の実行を容易にさせており、こうした犯罪の取締りにおいては、高度な技術的な知見が必要となっている。

このため、警察では、警察庁及び全国の情報通信部に情報技術解析課を設置し、都道府県警察等に対し、捜索・差押えの現場でスマートフォンやコンピュータ等の電子機器を適切に差し押さえるための技術的な指導や、押収した電子機器から証拠となる情報を取り出すための解析の実施についての技術支援を行っている。

また、犯罪捜査の過程で押収した電子機器は、変形、燃焼、水没等により破損していることが少なくない。そこで、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、破損した電子機器の機能回復及び情報の抽出・可視化等を行っている。

図表３-７　犯罪の取締りへの技術支援体制

CASE

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、破損した状態で押収した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、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たことで、同事件の全容解明に貢献した。

（４）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７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)が主催するサイバー犯罪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や、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７年６月、警察庁サイバー警察局では、欧州等からデジタル・フォレンジックの専門家を招へいし、破損機器の解析等に関する意見交換を実施したほか、同年９月、オランダ国家警察との間で、サイバー空間をめぐる脅威の情勢等について、サイバー犯罪対策部門の長等を交えたハイレベルな意見交換を行った。また、同年11月には、ＥＵＲＯＰＯＬから暗号資産追跡の専門家を招へいし、日本の捜査員向けに暗号資産の高度な追跡方法等の講演及び実習を行った。さらに、同年12月には、外国捜査機関の捜査員等を招へいし、関係各国との国際共同捜査に関する捜査情報の交換等を行った。

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。

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。

３：４頁参照（特集）

４：４頁参照（特集）

５：Forum of Incident Response and Security Teamsの略

６：Japan International Cooperation Agencyの略

memo ＡＩとデジタル・フォレンジックに係る国際会議の開催

近年のサイバー事案では、生成ＡＩ等の最新の技術が悪用されるなど、従来の手法による捜査では対処が困難になってきている。

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、外国捜査機関、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(注)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。

国際会議「Interpol Conference on AI in Digital Forensics」の様子

注：ＡＩ技術を応用して偽の動画や音声等を作る技術

2 被害の未然防止・拡大防止に向けた取組

（1）サイバー空間における脅威に係る対策

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・団体とも連携し、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。

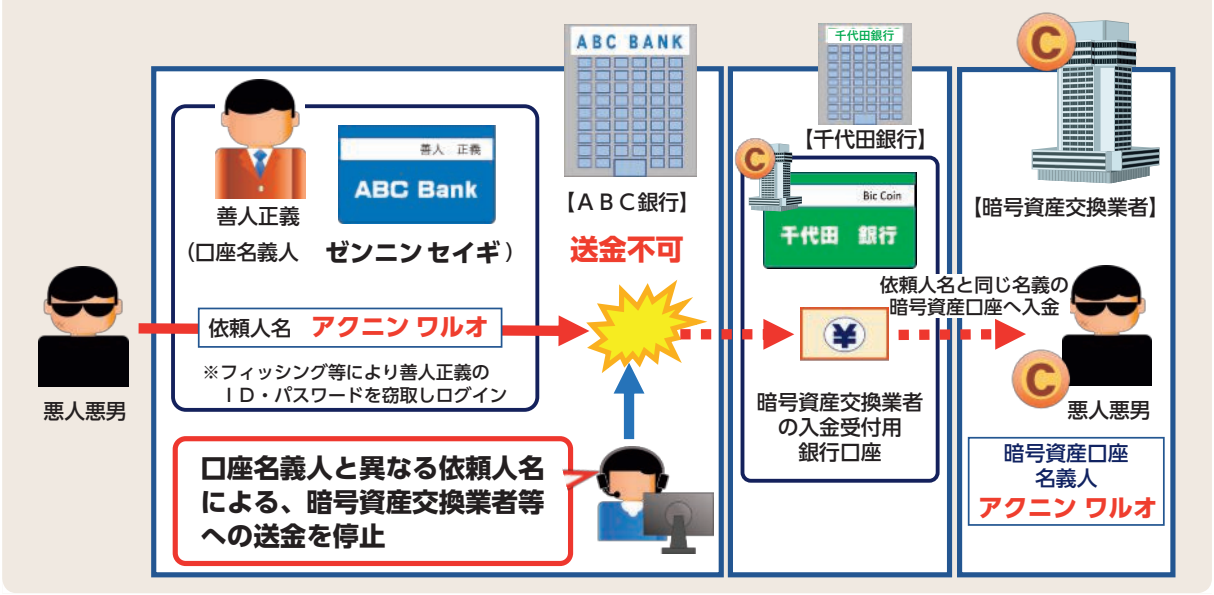
② インターネットバンキングに係る不正送金事犯への対策

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・団体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、ＪＣ３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。

さらに、インターネットバンキングに係る不正送金事犯において、暗号資産交換業者の入金受付用の金融機関口座が送金先となっている実態を踏まえ、令和７年９月、警察庁は、金融庁と連携し、一般社団法人全国銀行協会等に対して、送金元口座名義人名と異なる依頼人名で行われる暗号資産交換業者等の金融機関口座への送金取引を拒否することといった対策に取り組むよう、金融機関等へ周知するよう要請した。

図表３－８　暗号資産交換業者への不正送金対策



注１：令和７年の調査は、同年８月27日から同年９月19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、588件の回答を得た。

２：令和７年の調査は、同年８月27日から同年９月19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。

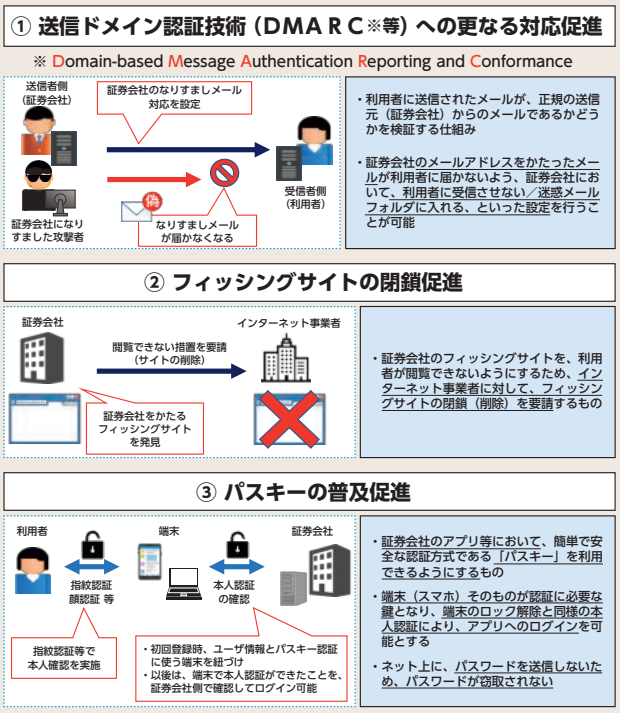
加えて、フィッシングの手口が巧妙化し、被害が急増している情勢に鑑み、利用者保護を目的として、フィッシングメールが届かない環境の整備やフィッシングサイトにアクセスさせないための対策について、「国民を詐欺から守るための総合対策2.0」(注１)に基づいた取組を進めるため、関係機関と連携して、各事業者等に働き掛けを行っている。

memo 証券口座不正取引への対策

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。

こうした事態を受け、同年７月、警察庁は、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、①送信ドメイン認証技術（ＤＭＡＲＣ等）への更なる対応促進、②フィッシングサイトの閉鎖促進、③パスキーの普及促進（図表３－９参照）等について要請を行った。証券会社におけるインターネット取引時の利用者認証の強化や警察庁及び金融庁による注意喚起をはじめとした各種対策が講じられて以降、証券口座の不正取引被害は大幅に減少した。

図表３－９　フィッシング対策

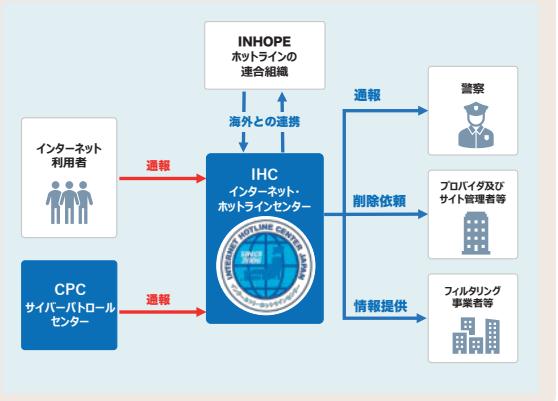


③　インターネット上の違法情報・有害情報対策

ア　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、重要犯罪密接関連情報(注２)及び自殺誘引等情報(注３)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７年中、ＩＨＣでは国内外のプロバイダ等に対して５万7,185件の違法情報の削除依頼を行い、そのうち２万7,032件（47.3%）が、1,227件の重要犯罪密接関連情報の削除依頼を行い、そのうち1,072件（87.4%）が、5,192件の自殺誘引等情報の削除依頼を行い、そのうち4,241件（81.7%）が、それぞれ削除された。

図表３－10　インターネット・ホットラインセンターにおける取組



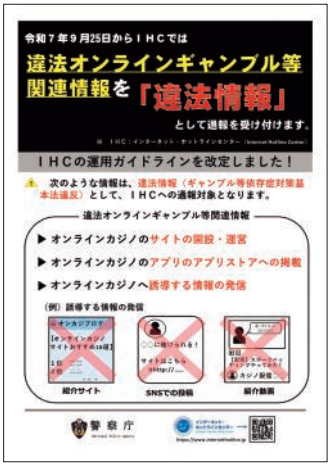
注１：32頁参照（トピックスⅠ）
２：個人の生命・身体等に危害を加えるおそれが高い重要犯罪等と密接に関連する情報。具体的には、例えば、爆発物の製造を直接的かつ明示的に助長等していると認められる情報、殺人等を直接的かつ明示的に請負等する情報等をいう。
３：他人を自殺に誘引・勧誘する情報等

ＩＨＣに通報された児童ポルノのうち、外国のサーバにそのデータが蔵置されているものについては、各国のホットライン相互間の連絡組織であるＩＮＨＯＰＥ(注1)の加盟団体に対し、削除に向けた措置を依頼している。

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、犯罪実行者募集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。

イ　インターネット・ホットラインセンターにおける取組の強化

令和７年９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の施行に合わせて、ＩＨＣの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」を違法情報に追加するなど、ＩＨＣにおける取組を強化した。



違法オンラインギャンブル等関連情報に関する広報啓発資料

ウ　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。

④　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、中小企業を主な対象として、ＶＰＮ機器等のセキュリティ対策や認証情報の適切な管理、オフラインを含むバックアップの取得、ログの保存、サイバー攻撃を想定した業務継続計画（ＢＣＰ(注2)）の策定等について幅広く広報啓発活動に取り組んでいる。

さらに、警察庁ウェブサイト(注3)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じ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ている。

⑤　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。

注１：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８年２月末現在、ＩＨＣを含む57団体（52の国・地域）から構成される国際組織

２：Business Continuity Planの略

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

（２）官民連携の推進

①　サイバーフォースの活動

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。

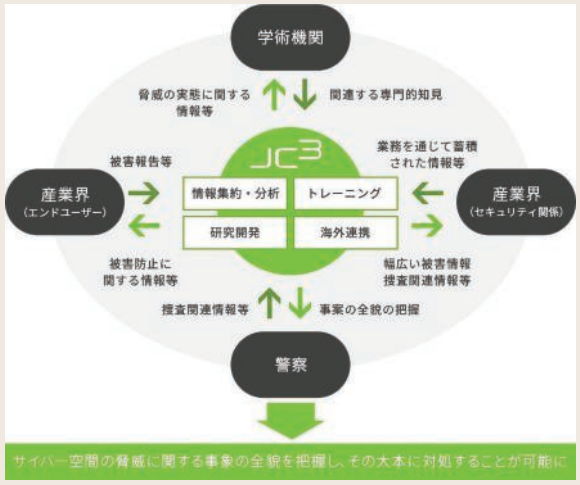
このような情勢に対応するため、警察では、都道府県警察のサイバー事案対策部門に技術的な面から支援を行う部隊であるサイバーフォースを、警察庁及び全国の情報通信部(注１)にそれぞれ設置している。サイバーフォースは、個々の重要インフラ事業者等に対する脅威情報の提供や助言、サイバーテロ対策協議会(注２)での講演、サイバー事案発生を想定した共同対処訓練を実施するなどして、官民連携の強化に努めている。また、サイバー事案発生時には、都道府県警察と連携し、被害状況の把握、被害拡大の防止、証拠保全等について技術的な緊急対処を行っている。

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、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。

②　日本サイバー犯罪対策センター（ＪＣ３）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３－11　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。

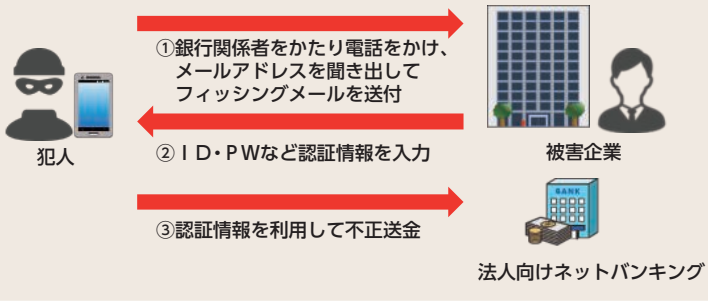
また、ＪＣ３では、サイバー防犯ボランティア等が同ツールを活用し、フィッシングサイトのテイクダウン件数等を競う「フィッシングサイト撲滅チャレンジカップ」を開催しており、警察庁がこれを後援している。令和７年12月と令和８年１月の２回に分けて開催された第３回大会では、55団体が参加し、2,828件のフィッシングサイトがテイクダウンされた。

注１：131頁参照
　２：138頁参照

memo 官民連携によるボイスフィッシングへの注意喚起の実施

警察庁は、令和６年秋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急増したことを受け、金融庁、全国銀行協会及びＪＣ３と連名で、広報啓発資料「サイバー警察局便り」の作成・公開を行い、その犯行手口や被害防止対策等に関する注意喚起を実施した。

図表３－12　ボイスフィッシングの流れ



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332団体、7,633人（令和７年12月末現在）となっており、警察では、全国のサイバー防犯ボランティアの研鑽の場として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。

また、警察庁においては、サイバー防犯ボランティア広報啓発コンテストを開催し、その入賞作品を渋谷スクランブル交差点等に設置されたデジタルサイネージで放映するなどの取組を実施している。

デジタルサイネージで放映されている入賞作品

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。

3 警察活動の基盤の強化に向けた取組

（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。

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７年度には、サイバー防犯ボランティア及び徳島県高校対抗サイバーセキュリティコンテストの参加者から２人をサイバー犯罪捜査官として採用した。

福井県警察では、サイバー防犯ボランティアの一環として、県内の大学でデザインを専攻する学生らが授業で制作した、サイバー犯罪捜査官の採用募集ポスターや、サイバー犯罪対策課のウェブサイトに掲載する画像及びキャッチコピーを、警察活動に活用している。

福井県警察採用募集ポスター

（2）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、サイバー部門に係る研修・訓練に特化した警察大学校サイバー警察教養部では、都道府県警察のサイバー部門においてサイバー事案の対処に当たる捜査員等を対象とした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。

また、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。

（3）解析能力向上のための取組

コンピュータやスマートフォン等の電子機器やＳＮＳ等のネットワークを利用したサービスが普及・多様化する中、警察捜査を支えるため、電子機器等に保存された電磁的記録やネットワークの通信状況等の解析の重要性が一層高まっている。

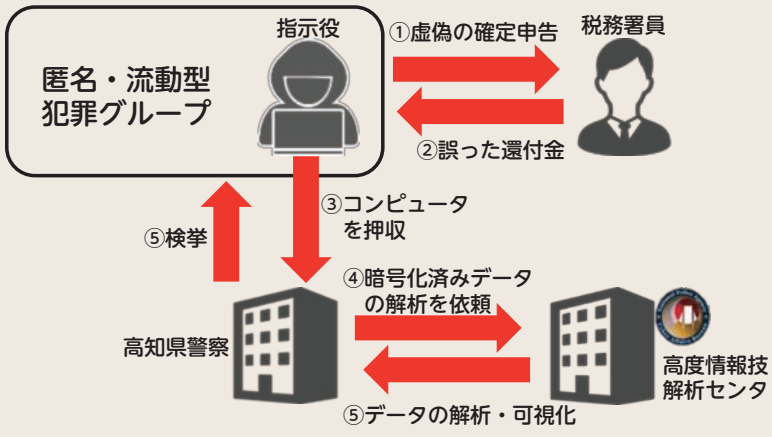
犯罪に悪用された電子機器等に保存されている電磁的記録は、犯罪捜査において重要な客観証拠となり得るため、警察では、押収した電子機器から、通信履歴、位置情報、写真等の証拠となる情報を取り出すための解析を実施している。犯人は、犯行に利用していた電磁的記録に暗号化処理を施す、電子機器を破壊するなど、証拠隠滅による捜査妨害を図ることが多い。また、ＩｏＴ機器をはじめとする新たな電子機器やそれに関連するサービスの社会への定着、スマートフォン等のアプリの多様化・複雑化、自動運転システムの実現に向けた技術開発等が進んでいる。これらのことから、警察捜査を支えるためには、暗号化済みデータや破損した電子機器、最新の技術に対応した解析能力の向上を図っていく必要がある。

このため、警察では、解析手法の開発や資機材の整備、高度な解析技術を持つ職員の育成のほか、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。また、技術的中核となる警察庁高度情報技術解析センターには、高速演算装置や解析基盤装置をはじめとする高度な解析用機器を整備しており、都道府県警察において解析が困難な場合に、これらの機器を使用し、暗号により隠蔽されたデータを解析したり、破損した電子機器等からデータを抽出・解析したりするなどの技術支援を行っている。

CASE

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。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は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解析・可視化した。その結果、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。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６月までに、同男ら10人を詐欺罪等で逮捕した（高知）。

図表３－13　犯罪とその検挙までの流れ（イメージ）



memo 高度な専門性を有する警察庁職員による支援

コンピュータやスマートフォン等の電子機器の普及、ＩｏＴ機器等の新たな電子機器の登場、情報通信サービスの多様化により、解析の対象となる物の範囲が拡大している。また、解析の対象となる物は様々な要因により破損している場合があるため、解析には高度な専門性が必要となる。

警察庁高度情報技術解析センターでは、電子機器から抽出したデータや、電子機器の詳細な状態を示す顕微鏡画像、欠損した電磁的記録等を、解析基盤装置を活用して遠隔で確認し、破損箇所の特定、解析手法の検討、解析に伴うリスク判断等を行った上で、全国の情報通信部に対して助言を行っている。

図表３－14　遠隔での支援のイメージ

memo スマートフォンの解析

近年、スマートフォンが、様々なコンテンツやアプリケーションの利用が可能なモバイル端末として普及している中、犯罪に悪用されたスマートフォンに保存されている情報は、犯罪捜査において重要な客観証拠となり得る。このため、警察では、押収したスマートフォンから、通信履歴、位置情報、写真等の証拠となる情報を取り出すための解析を実施している。

警察庁高度情報技術解析センターでは、スマートフォンアプリに記録された暗号化済みデータを可視化する手法を開発するなど、新たな解析手法の開発等に取り組んでいる。

図表３－15　スマートフォンの解析の概要

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及び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。

不正プログラム解析の高度化に関する研究

不正プログラムを悪用したサイバー事案の実態解明のためには、不正プログラム解析の高度化が必要となる。サイバーセキュリティ対策研究センターでは、生成ＡＩを活用した不正プログラム解析の高度化に関する研究を行っており、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。

学会での発表の様子

警察活動の最前線

デジタル・フォレンジック最前線

近畿管区警察局情報通信部情報技術解析課支援分析第二係
和木　将晃

情報技術解析課では、電子機器等の解析や捜査への技術支援を行っています。その中でも、私はマルウェアやスマートフォンの解析に従事しており、それらの高度な技術を担う人材の育成にも力を入れています。

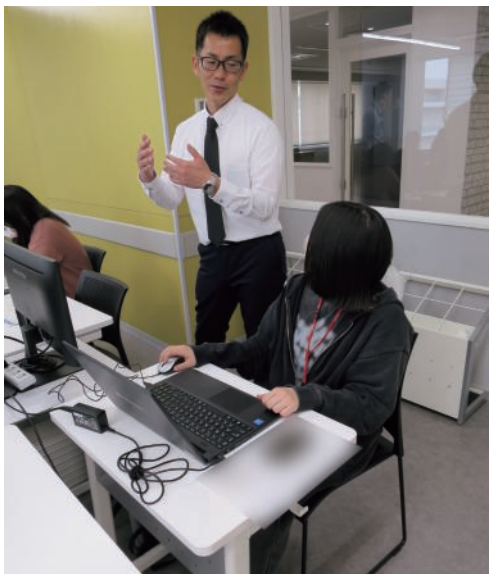
近年、どのような犯罪であってもスマートフォンをはじめとする様々な電子機器等が使用されています。デジタル・フォレンジックという業務は、一般にはあまり知られていませんが、犯罪に使用された電子機器等を解析できるかどうかが、捜査の行方に大きく影響するため、非常に重要な仕事となっています。特に、秘匿された電磁的記録や暗号化された電磁的記録の可視化は、解析者の腕の見せ所です。私が独自に開発した可視化のための解析ツールは、全国の警察で利用され、多くの捜査に役立てられています。

また、これらのツールの有用性が認められ、検察庁や税関といった関係機関でも導入されるようになりました。

解析が困難と思われた電磁的記録を解析できたとき、成功の喜びと社会貢献の達成感を同時に得ることができます。ＩＴ技術は日進月歩で、今ある技術もいずれは通用しなくなるため、新たな困難に対するチャレンジがずっと続きますが、日々成長できることに満足しています。

持続可能なサイバー防犯ボランティアの育成

広島県警察本部生活安全部サイバー犯罪対策課官民連携推進係
鷹村　陽一



サイバー犯罪対策課官民連携推進係では、サイバー犯罪の未然防止と対処能力の向上を図るため、サイバー防犯ボランティアの活動について、大学や専門学校と連携し、学生を中心とした委嘱・拡大を推進しています。

サイバー防犯ボランティア活動を実質的なものにするため、ＷＥＢ会議等を活用した合同パトロールや防犯イベント等の主体的な企画を促進し、更なる活性化を図るとともに、次世代ボランティアを含めた継続的な育成に取り組んでいます。これらの取組により、学生による総合的かつ自主的なボランティア活動が定着し、安全・安心なまちづくりの功労により当県のサイバー防犯ボランティア団体が「内閣総理大臣賞」を受賞するなど、地域全体の防犯意識の向上に寄与しています。

また、サイバー防犯ボランティア活動を通じて警察の業務に魅力を感じた学生が警察官として採用されるなど、人材の好循環が創出され、持続可能な官民連携モデルの構築が図られています。

「サイバー防犯ボランティア出身者の声」

大学在籍時から警察のサイバー犯罪捜査に関心を持ち、県警が開催したインターンシップに参加したことを契機にサイバー防犯ボランティア活動を開始しました。現在は広島県警察職員として、希望していたサイバー犯罪対策課で勤務しています。