サイバー空間の安全の確保

第１節　サイバー空間における脅威
第２節　サイバー空間における脅威への対処

第3章
CHAPTER 3





第1節 サイバー空間における脅威

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着する中、新型コロナウイルス感染症の感染拡大防止の観点から、行政手続のオンライン化やテレワークの積極的な実施が進められ、業務や取引に関するデータをオンラインで取り扱う機会が増加したことで、今やサイバー空間は、全国民が参画し、重要な社会経済活動を営む公共空間となっている。こうした中で、国内では、キャッシュレス決済サービスの普及等を背景として、令和３年（2021年）中にサイバー犯罪の検挙件数が１万2,209件と過去最多を記録しており、インターネットバンキングに係る不正送金事犯による被害は前年に比べて減少したものの、ランサムウェアによる被害が拡大するなど、その手口を深刻化・巧妙化させたサイバー事案が多数発生している。また、不正アクセスによる情報流出や、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明らかになるなど、サイバー空間における脅威は極めて深刻な情勢が続いている。

1 サイバー事案の検挙状況

（1）不正アクセス禁止法違反

令和３年中の不正アクセス禁止法違反の検挙件数は429件と、前年より180件（29.6%）減少し、検挙人員は235人と、前年より５人（2.2%）増加した。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類型別内訳をみると、他人の識別符号を無断で入力する「識別符号窃用型」が398件（92.8%）と最多であった。

また、令和３年中の不正アクセス行為の認知件数(注1)は1,516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693件（45.7%）と最多であった。

（2）コンピュータ・電磁的記録対象犯罪(注2)

令和３年中のコンピュータ・電磁的記録対象犯罪の検挙件数は729件と、前年より166件（29.5%）増加した。

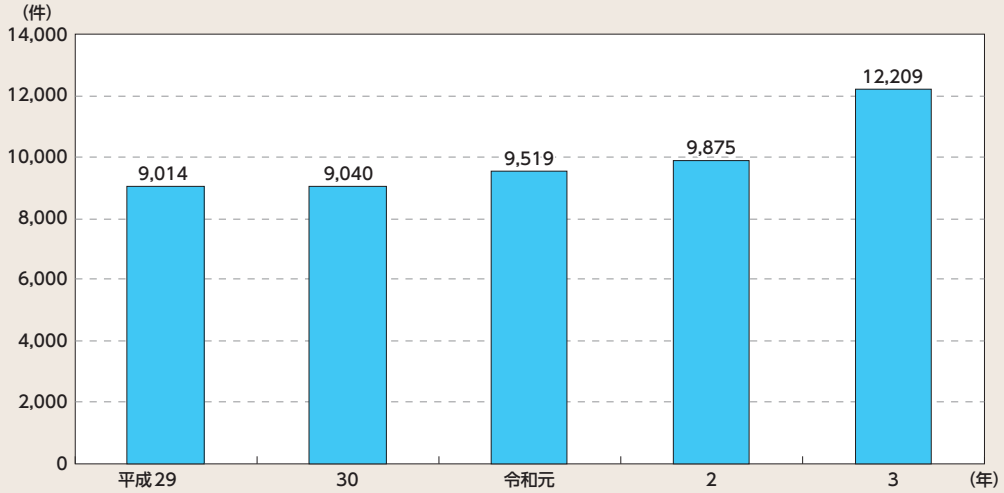
（3）サイバー犯罪(注3)の検挙件数の推移

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３年中の検挙件数は１万2,209件と、前年より2,334件（23.6%）増加し、過去最多を記録した。

注１：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
２：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
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

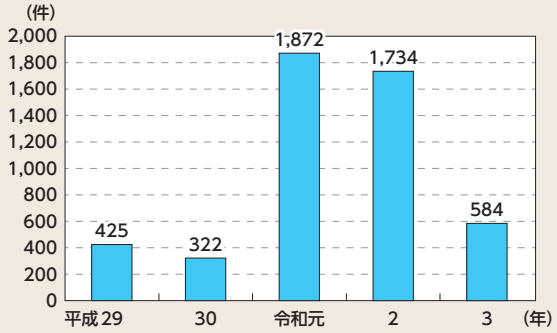
図表３－１　サイバー犯罪の検挙件数の推移（平成29年（2017年）～令和３年）



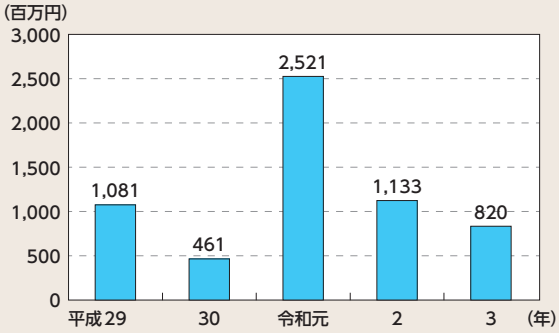
2　インターネットバンキングに係る不正送金事犯の情勢

令和３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584件、被害額は約８億2,000万円と、前年に比べて減少した。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（平成29年～令和３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（平成29年～令和３年）



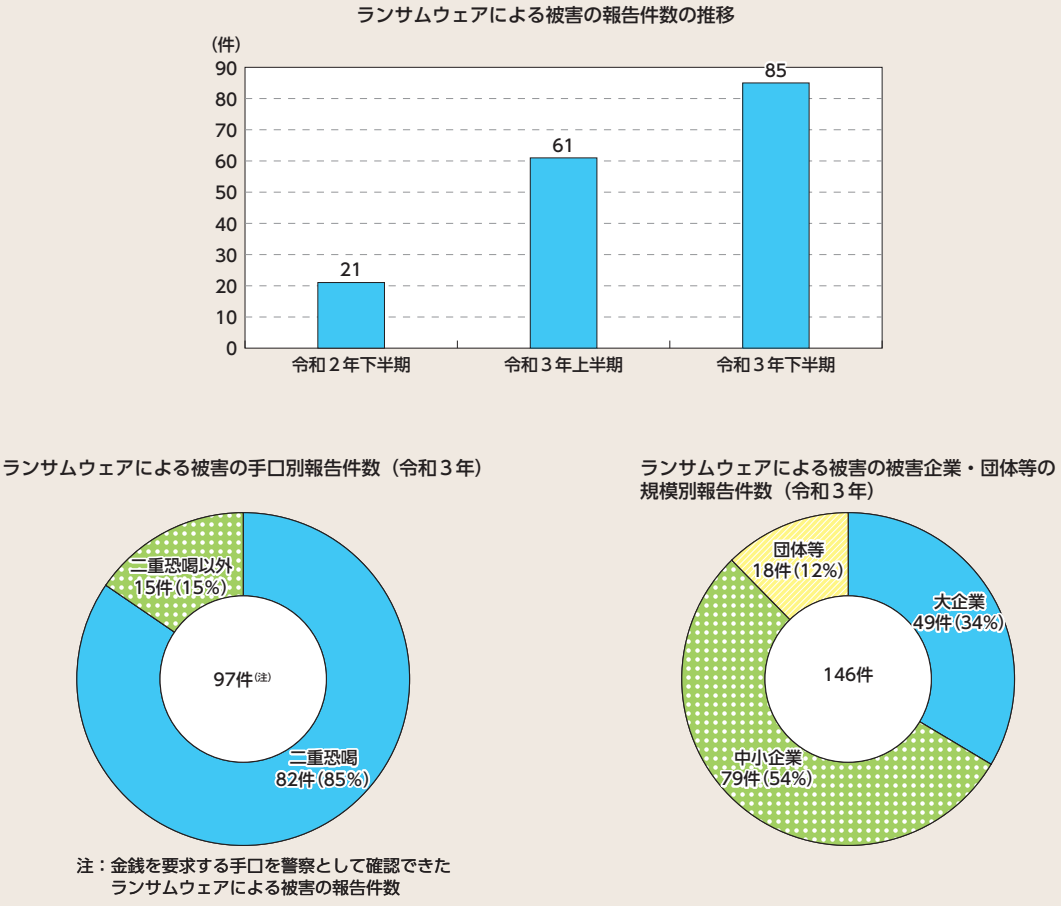
注：銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトに見せかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するよう誘導し、当該サイトでクレジットカード番号や識別符号を入力させて金融情報や個人情報を不正に入手する行為

3 ランサムウェアの情勢

令和３年中のランサムウェアによる被害の報告件数(注１)は146件（令和３年上半期61件、下半期85件）であり、令和２年下半期（21件）以降、連続して増加している。金銭を要求する手口を警察として確認できた、ランサムウェアによる被害の報告件数97件のうち、ダブルエクストーション（二重恐喝）(注２)の手口によるものは82件であり、85％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について、被害企業・団体等の規模別(注３)にみると、大企業は49件、中小企業は79件と、被害企業の規模を問わず、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・団体等を対象に、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76件のうち、VPN機器(注４)を利用して侵入された事例は41件（54％）、リモートデスクトップサービス(注５)を利用して侵入された事例は15件（20％）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。

図表３－４　ランサムウェアによる被害の報告件数



注：金銭を要求する手口を警察として確認できた
ランサムウェアによる被害の報告件数

注１：３頁参照（特集）
２：３頁参照（特集）
３：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。
４：５頁参照（特集）
５：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 サイバー攻撃の情勢

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インテリジェンス（サイバーエスピオナージ）といったサイバー攻撃が、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。我が国では、社会的混乱が生じるようなサイバーテロは発生していないものの、海外では、不正プログラムによって金融機関のシステムや原子力関連施設の制御システムの機能不全を引き起こす事案が発生している。

（２）サイバーインテリジェンスの情勢

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、新型コロナウイルス感染症に関連する研究等の機密情報の窃取を目的としたサイバーインテリジェンス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インテリジェンス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インテリジェンスが発生している。

CASE

令和３年４月、内閣府は、内閣官房、内閣府、個人情報保護委員会及び復興庁の職員が使用するファイル共有ストレージ(注２)が不正アクセスを受け、231名分の個人情報が流出した可能性がある旨を公表した。

CASE

原子力規制庁では、令和元年８月から９月にかけて、原子力規制委員会のネットワークシステムが不正アクセスを受け、職員及び請負業者の認証用パスワード等の情報が窃取されたほか、令和２年10月には、窃取されたと思われる認証用パスワード等の情報を利用した不正アクセスを受け、更にデータを窃取されたことなどが判明し、令和３年９月、調査結果を公表した。

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４年６月17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、クレジット及び石油の14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：外部との間でファイルの送受信を行うため、内閣府が構築しているLANの外側に別個のものとして設置された機器

第2節 サイバー空間における脅威への対処

1 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3)）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。特に、SMSによってフィッシングサイトへ誘導する手口であるスミッシングによる被害を防止するため、フィッシングサイトへ誘導するSMSを利用者が受信すること自体を阻止する仕組みの構築に向けた大手携帯電話事業者等による検討に参画し、令和４年（2022年）３月、JC3の協力の下、フィッシングサイトへ誘導するSMSの受信を自動で拒否する機能が大手携帯電話事業者により提供されるようになった。

CASE

令和３年１月、警視庁と共同対処協定を締結している金融機関に開設された口座を送金元とする不正送金被害の急増を受けて、警視庁では、当該金融機関と連携して、速やかに犯行手口を分析の上、モニタリング(注4)やインターネットバンキングへのログイン時における認証の強化等の被害防止対策を要請し、当該金融機関において、これらの対策を実施したところ、同年２月中旬には、当該金融機関に開設された口座を送金元とする不正送金被害は確認されなくなった。

（3）インターネット上の違法情報・有害情報対策

インターネット上には、児童ポルノ、規制薬物の広告に関する情報等の違法情報や、違法情報には該当しないが、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有害情報が多数存在している。

注１：令和３年の調査は、同年８月23日から９月21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、2,950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、716件の回答を得た。

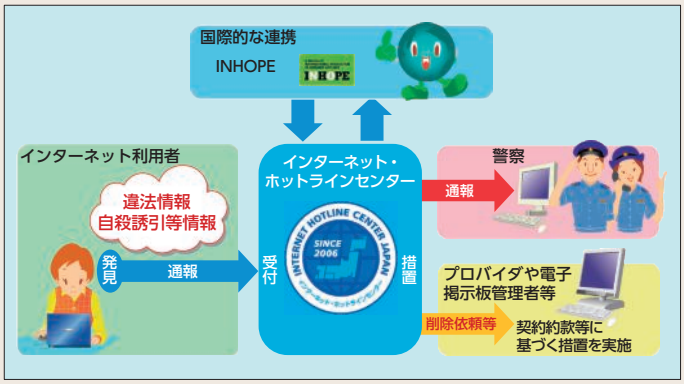
２：令和３年の調査は、同年８月23日から９月21日までの間に、市販のデータベースに掲載された企業のうち業種分類が「情報・通信」、「サービス」、「電気機器」又は「金融」であるもの及び国公立・私立大学のうち理工系学部又はこれに準ずるものを設置するものから、1,843件を無作為に抽出し、調査票を郵送で配布して実施した。電子メール又は郵送により、299件の回答を得た。

３：Japan Cybercrime Control Centerの略

４：金融機関等が、顧客があらかじめ登録した口座以外への送金等について、不正なものであるかどうかを確認すること。

① インターネット・ホットラインセンターにおける取組

図表3－5　インターネット・ホットラインセンターにおける取組



警察庁では、一般のインターネット利用者等から、違法情報、自殺誘引等情報(注1)等に関する通報を受理し、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３年中、IHCでは2,206件の違法情報の削除依頼を行い、そのうち1,846件（83.7%）が削除された。また、2,199件の自殺誘引等情報の削除依頼を行い、そのうち942件（42.8%）が削除された。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。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2)の加盟団体に対して、削除に向けた措置を依頼している。

② 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、サイバー保険(注3)を取り扱う損害保険会社等との連携や民間事業者等との共同対処協定(注4)の締結を通じて、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ほか、警察庁ウェブサイト(注5)において、ランサムウェアによるサイバー攻撃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。

memo　医療機関におけるランサムウェアによる被害の防止対策

国内外の医療機関においてランサムウェアによる被害が発生している状況を受け、警察では、厚生労働省、医療機関等と連携した被害防止対策を推進している。

富山県警察では、サイバー事案による被害の防止に向けて、同県内の公的医療機関により構成される富山県公的病院長協議会と共同対処協定を締結し、同協議会と連携して同県内の公的医療機関におけるサイバーセキュリティに対する意識の向上やサイバー事案認知時における警察への通報体制の確立に向けた取組を推進している。



協定の締結式（富山県警察）

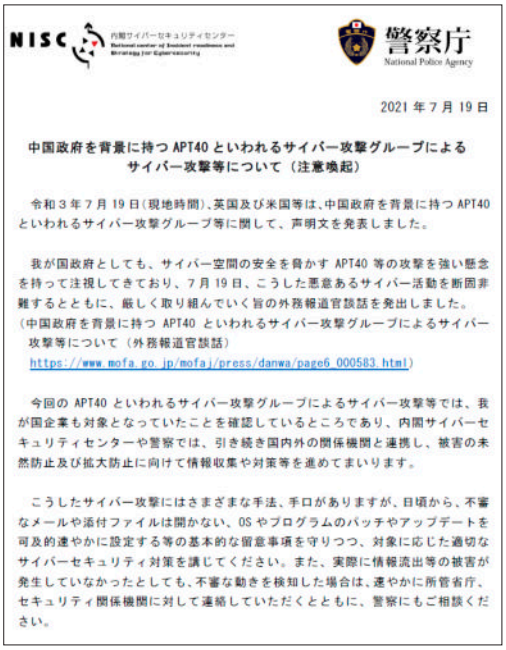
注１：他人を自殺に誘引・勧誘する情報等
２：現在の名称はInternational Association of Internet Hotlinesであるが、旧名称のInternet Hotline Providers in Europe Associationの略称を現在も使用している。平成11年（1999年）に設立され、平成31年１月末現在、IHCを含む52団体（47の国・地域）から構成される国際組織
３：サイバー事案等により企業に生じた損害等を補償する保険
４：令和３年12月末までに、金融機関や暗号資産交換業者等、全国で602事業者・団体と本協定を締結している。
５：**警察庁ウェブサイト「ランサムウェア被害防止対策」**(https://www.npa.go.jp/cyber/ransom/index.html)

（5）国境を越えて敢行されるサイバー攻撃への対策

警察では、国境を越えて敢行されるサイバー攻撃に適切に対処するため、新設されたサイバー警察局、サイバー特別捜査隊(注1)等と都道府県警察が緊密に連携して、迅速かつ的確な国際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 APT40に関するパブリック・アトリビューション及び注意喚起

令和３年（2021年）７月、英国、米国等の発表(注2)に関連して、我が国はAPT40と呼ばれるサイバー攻撃集団が中国政府を背景に持つ可能性が高いと評価した上で、悪意あるサイバー活動を断固非難する旨の外務報道官談話を発表した。また、警察庁及び内閣サイバーセキュリティセンター（NISC(注3)）は、事業者等に対し、適切なサイバーセキュリティ対策を講ずるとともに、システムの不審な動作を検知した場合には実際に情報流出等の被害が発生していなかったとしても、速やかにJC3等の関係機関・団体等に連絡するほか、警察に相談するよう注意喚起を行った。また、警察では、APT40によるサイバー攻撃を認知後、被害企業等に対し、速やかに不正プログラムへの感染可能性や有効な対応策について個別に情報提供を実施し、被害拡大防止のための措置を講じた(注4)。



NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity　警察庁 National Police Agency

2021年7月19日

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等について（注意喚起）

令和３年７月19日（現地時間）、英国及び米国等は、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等に関して、声明文を発表しました。

我が国政府としても、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念を持って注視してきており、７月19日、こうした悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を発出しました。
（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等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html）

今回の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等では、我が国企業も対象となっていたことを確認しているところであり、内閣サイバーセキュリティセンターや警察では、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めてまいります。

こうしたサイバー攻撃にはさまざまな手法、手口がありますが、日頃から、不審なメールや添付ファイルは開かない、OSやプログラムのパッチやアップデートを可及的速やかに設定する等の基本的な留意事項を守りつつ、対象に応じた適切なサイバーセキュリティ対策を講じてください。また、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

警察庁及びNISCによる注意喚起文

注１：４頁参照（特集）
２：４頁参照（特集）
３：National center of Incident readiness and Strategy for Cybersecurityの略
４：令和３年７月時点では、これら企業において情報流出等の被害は確認されなかった。

2 技術支援と解析能力の向上

（1） サイバー事案対策におけるサイバーフォースの役割

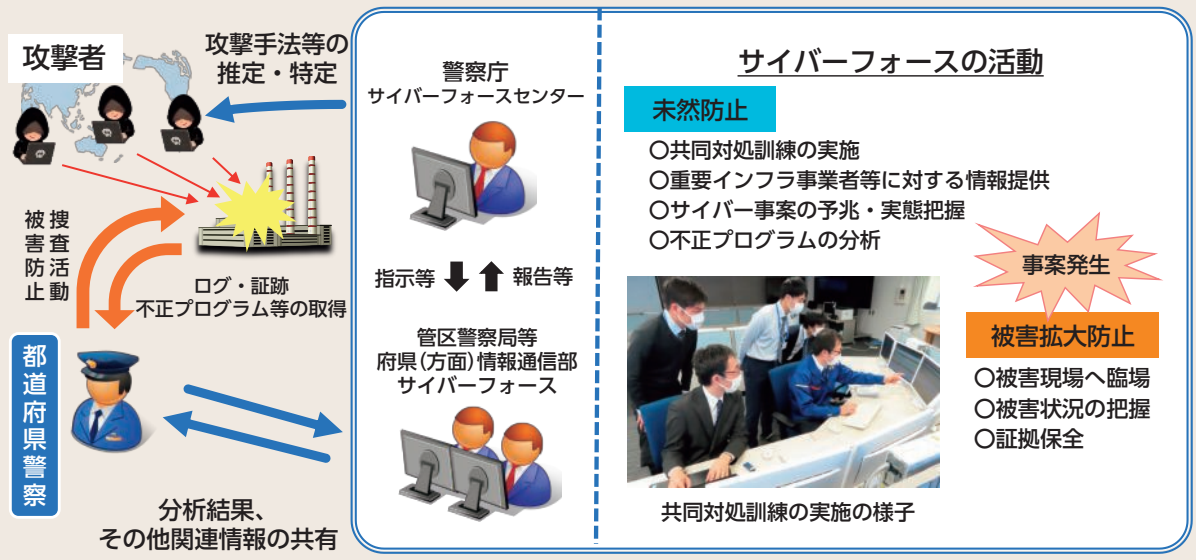
警察では、深刻化するサイバー事案に対処するため、攻撃の対象となったサイバーセキュリティ上のぜい弱性に関する情報や、標的型メール攻撃等の犯行手口に関する情報等を、捜査活動及び事業者との情報交換を通じて把握・分析をし、被害の未然防止及び拡大防止に努めている。

近年のサイバー事案については、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へ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)に設置している。サイバーフォースは、警備部門や生活安全部門と連携し、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。

また、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3－6 サイバーフォースの役割と活動

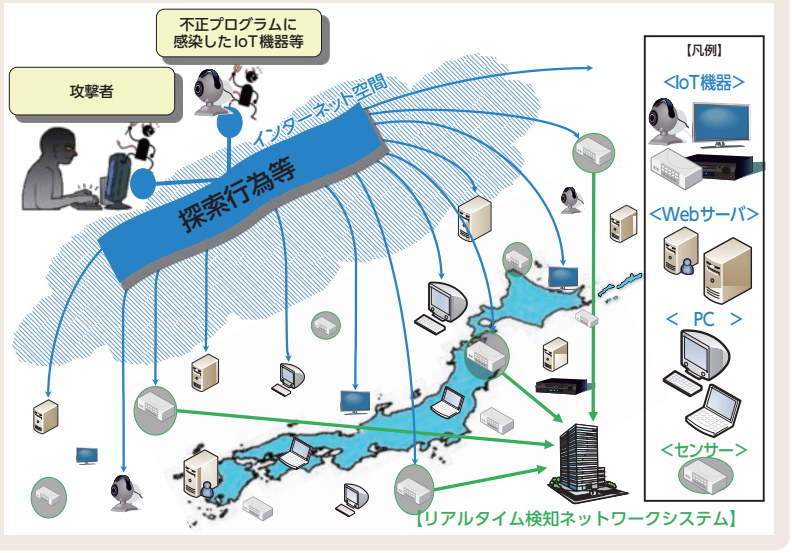


注1：管区警察局情報通信部（四国警察支局情報通信部を含む。以下同じ。）、東京都警察情報通信部、北海道警察情報通信部、府県情報通信部及び方面情報通信部
2：123頁参照

（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

図表３－７ リアルタイム検知ネットワークシステムの概要



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。


リアルタイム検知ネットワークシステムの運用状況

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、ファイル共有ソフトによるファイルの流通状況等の実態を把握するファイル共有ネットワーク観測機能等を備えており、インターネット上の事象の変化等に応じて観測機能の強化を行っている。また、近年では、各種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、ダークウェブ上の情報の収集・分析ができる機能の開発・導入を行い、ダークウェブ上のウェブサイトを分析しているほか、同機能の強化に向けた研究を進めている。

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、分析結果をインターネット観測結果として重要インフラ事業者等へ情報提供しているほか、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、警察庁ウェブサイト「@police」(注3)において広く一般に公開している。

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。

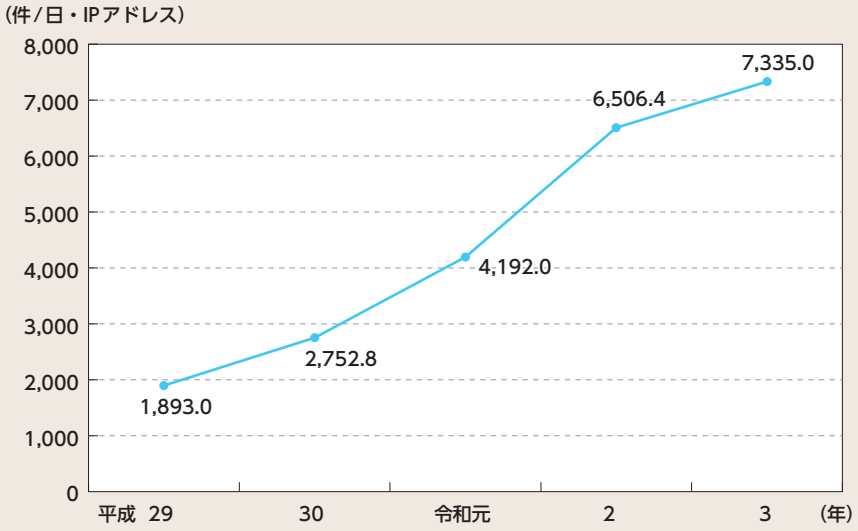
２：Denial of Serviceの略。特定のコンピュータに対し、大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃

３：**警察庁ウェブサイト「@police」**(https://www.npa.go.jp/cyberpolice/)

②　リアルタイム検知ネットワークシステムによる令和３年中のインターネット観測結果

令和３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11.8秒に１回という高い頻度で世界中から不審なアクセスが行われていることを観測した。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。

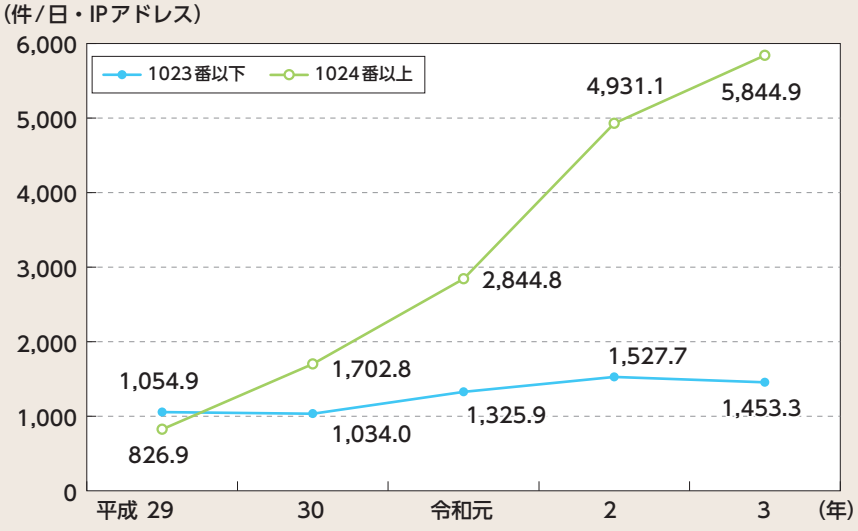
図表３－８　リアルタイム検知ネットワークシステムにおいて検知した一つのセンサーに対する１日当たりの不審なアクセス件数の推移（平成29年～令和３年）



検知した不審なアクセスについて、宛先ポート番号(注１)に着目すると、1024番以上のポートへのアクセスが大きな割合を占めている。1024番以上のポートは、主にIoT機器が標準設定として使用しているものであることから、こうしたアクセスの多くはIoT機器に対するサイバー攻撃やぜい弱性を有するIoT機器の探索行為であるとみられる。

令和３年上半期にも、本システムにおいて、不正プログラム「Mirai」(注２)の探索行為による不審なアクセスを多数観測したことから、警察庁ウェブサイト「@police」を通じて、IoT機器等の利用者に対し、ユーザ名及びパスワードを推測されにくいものに変更するなどのセキュリティ対策を講じるよう注意喚起を行った。

図表３－９　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（平成29年～令和３年）



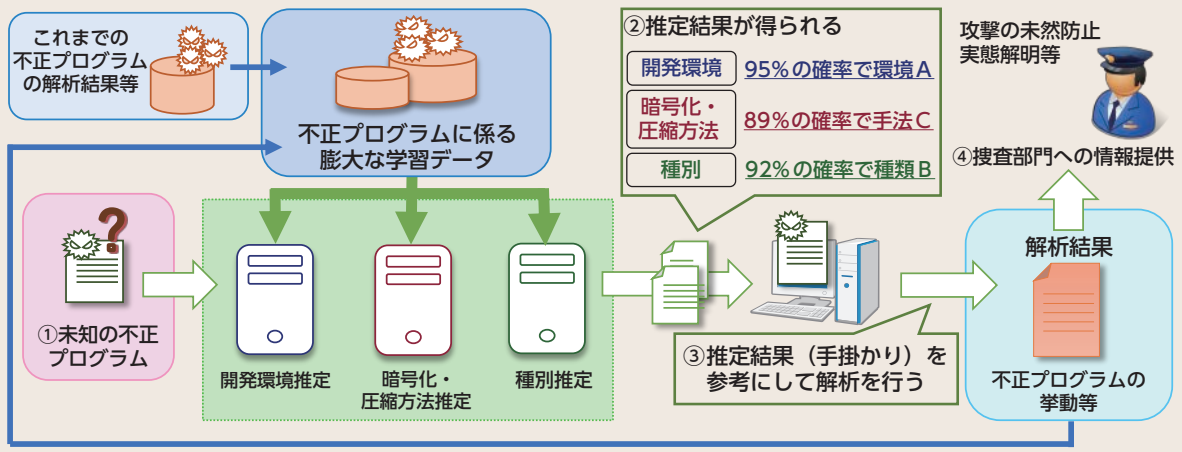
注１：TCP/IP通信（インターネット等で用いられているネットワーク上でデータを交換する際の取決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。
２：IoT機器等に感染しDoS攻撃等を行う不正プログラムの一種

（3） サイバー事案への対処のための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。

サイバーフォースセンターでは、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。

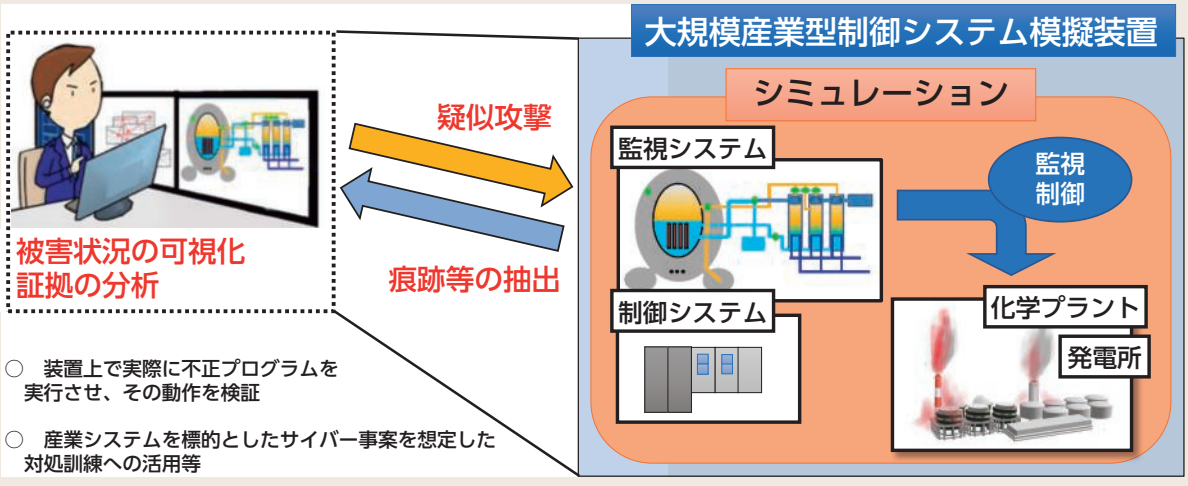
図表３－10　機械学習を活用した不正プログラム解析の高度化・効率化のイメージ



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、大規模産業型制御システム模擬装置を整備し、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、事案発生時に迅速な原因特定・対処ができるようにしている。

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・団体等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３－11　大規模産業型制御システム模擬装置の活用例



注：３頁（特集）

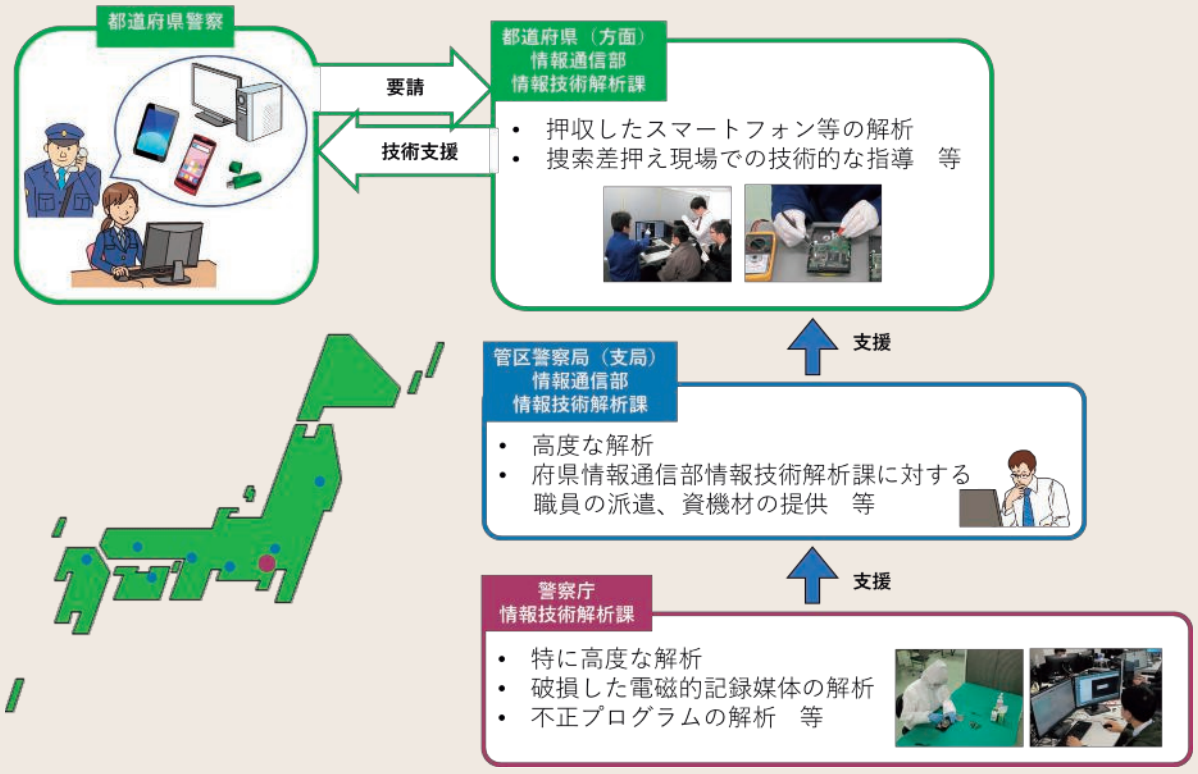
（4）サイバー事案の取締りへの技術支援

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敢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(注)に情報技術解析課を設置し、都道府県警察に対し、捜索差押え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や、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を実施する、技術支援を行っている。

また、警察庁に設置された高度情報技術解析センターは、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、不正プログラムの解析等を行っている。

図表３－12　犯罪の取締りへの技術支援



（5）解析能力向上のための取組

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いる。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む中、警察捜査を支えるためには、最新の技術に対応した解析能力の向上を図っていく必要がある。

このため、警察では、解析手法の開発や資機材の整備、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。

注：115頁参照

3 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・特別採用されており、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。

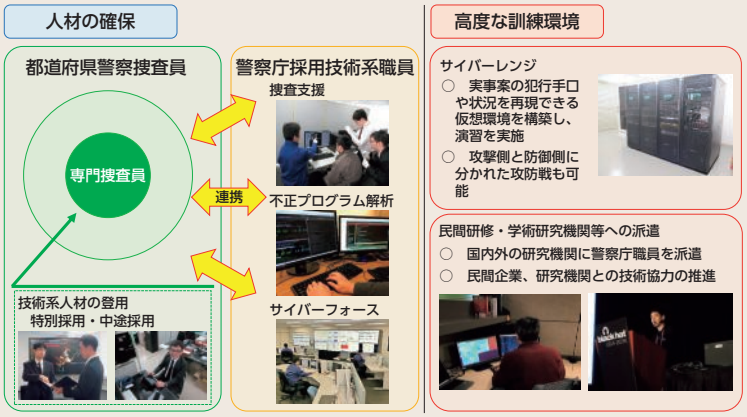
また、警察庁では、従前から情報通信に関する専門的な技術を有する者を技術系職員として採用し、各種研修を実施するなどして育成しており、これらの職員は、その専門知識を生かして、情報技術解析等の第一線で活躍している。

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、職員の採用・登用、教育・研修、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。

（2）捜査員等に対する実践的研修

警察大学校サイバーセキュリティ対策研究・研修センター捜査研修室では、都道府県警察の捜査員等を対象とした高度な実践的研修を実施している。平成30年度からは、新たにサイバーレンジ(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犯罪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。

図表３－13　サイバー空間への脅威に係る人材育成



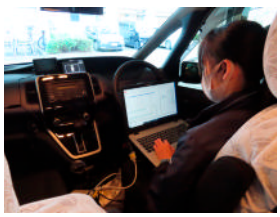
さらに、警察庁では、高度な解析技術を持つ職員の育成を行うため、最新の技術を有する民間企業や研究機関との技術協力を推進している。

memo　サイバーセキュリティ対策研究・研修センター解析研究室における取組

警察大学校サイバーセキュリティ対策研究・研修センター解析研究室では、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にはカメラやレーダー等が搭載されており、同システムには事件・事故等の捜査に必要な情報が記録されている可能性があることから、自動運転システムの解析に関する研究を行っている。令和３年度は、車載ネットワーク及び自動運転ソフトウェアからのデータの抽出及び可視化のための研究を行うとともに、民間の知見を活用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

memo　サイバーセキュリティコンテストの開催

警察庁では、各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セキュリティ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・技能の向上を図っているほか、全国の優秀な人材の発掘に取り組んでいる。

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

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３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(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、ICPO(注３)及びEUROPOL(注４)が共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等が主催するワークショップ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 ランサムウェアに関するG7高級実務者会合

ランサムウェアの脅威への対処に関するG7各国の連携を強化するため、令和３年12月、ランサムウェアに関するG7高級実務者会合がオンラインで開催され、G7各国の法執行機関、サイバーセキュリティ当局等の関係機関に加え、ICPO、EUROPOL等の国際機関が参加し、我が国からは警察庁長官官房サイバーセキュリティ・情報化審議官（当時）が政府代表として出席した。同会合では、ランサムウェアの脅威の情勢、対策状況等について議論を行い、G7各国等が連携してランサムウェアの脅威に優先的かつ継続的に対処することの必要性について認識が一致した。



G7高級実務者会合の様子

（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関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７)。

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：International Criminal Police Organization（国際刑事警察機構）の略

４：European Union Agency for Law Enforcement Cooperationの略。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。

５：Forum of Incident Response and Security Teamsの略

６：Japan International Cooperation Agencyの略

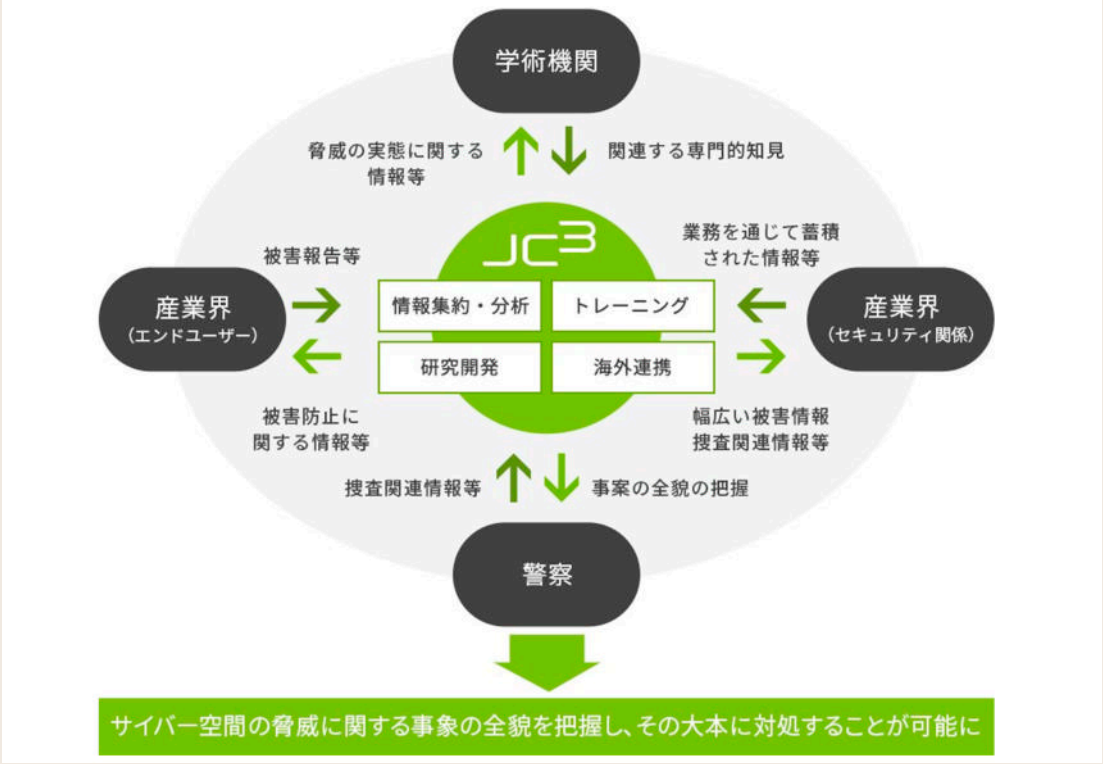
７：令和２年度及び３年度については、新型コロナウイルス感染症の感染拡大の影響により中止となった。

5 官民連携の推進

（1）日本サイバー犯罪対策センターとの連携

我が国における新たな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(注)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３－14　JC3の概要



（2）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264団体、7,276人（令和３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の様子

CASE

香川県警察では、令和３年11月、JC3と連携して、サイバー防犯ボランティアに対する研修会を開催した。JC3の職員が、参加した大学生ボランティア約20人に対し、産業界から集約した情報や知見を踏まえたサイバーパトロールのポイント等について、講師として指導することにより、大学生ボランティアの技術や意識の向上等が図られた。


研修会の様子

注：112頁参照

（３）サイバーテロ対策協議会



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設置し、サイバー事案の脅威や情報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。

（４）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、このネットワークを通じて事業者等から提供された情報を集約するとともに、これらの事業者等から提供された情報及びその他の情報を総合的に分析し、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。

（５）不正プログラム対策協議会

警察では、警察庁及びウイルス対策ソフト提供事業者等で構成される不正プログラム対策協議会において、不正プログラム対策に関する情報共有を行っている。特に、警察からは、市販のウイルス対策ソフトで検知できない新たな不正プログラムに関する情報や未知のぜい弱性に関する情報を提供し、情報セキュリティ対策の向上を図っている。

（６）不正通信防止協議会

警察では、警察庁及びセキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者で構成されるサイバーインテリジェンス対策のための不正通信防止協議会において、標的型メール攻撃等に利用される不正プログラムの接続先等の情報を共有することにより、我が国の事業者等が不正な接続先へ通信を行うことを防止している。

（７）高度な研究開発等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。

（８）事後追跡可能性の確保に向けた取組の推進

捜査における犯人の事後追跡可能性を確保するため、関係事業者等に対し、総務省の「電気通信事業者における個人情報保護に関するガイドライン」を踏まえた通信履歴の適切な保存、適切な本人確認・認証等の実施を要請している。

また、近年、MVNO(注１)が本人確認をせずに契約したSMS機能付きデータ通信専用SIMカードが、サイバー事案等に悪用された事例が確認されていることなどを踏まえ、都道府県警察では、SMS認証の代行に伴う違法行為(注２)の取締りを強化しているほか、警察庁では、令和３年１月、総務省と連携して、一般社団法人テレコムサービス協会MVNO委員会に対し、SMS機能付きデータ通信契約時の確実な本人確認の実施を要請した。同要請を受け、同委員会加盟事業者は、自主的な取組として、SMS機能付きデータ通信契約時の本人確認を実施することを申し合わせた。

注１：２頁参照（特集）
　２：２頁参照（特集）

警察活動の最前線

犯罪捜査に資する情報技術の解析手法を模索し続ける

警察庁サイバー警察局情報技術解析課解析第三係
鮫島（さめしま）　優太（ゆうた）



私は、被疑者等が破壊を試み、損傷したスマートフォン等の修復やデータの抽出等の情報技術の解析を担当しています。私の所属する情報技術解析課高度情報技術解析センターには全国警察から激しく損傷した特に高度な解析を要する証拠品が持ち込まれるため、私は、高性能な解析用資機材を用いて微細な部品が密集した回路基板の調査・修復を行い、データの抽出を行っています。

昨年、ある県警の捜査員から「盗撮事犯の被疑者が証拠隠滅を図り、焼いたり、水に漬けるなど、様々な手法で破壊が試みられたスマートフォンを１週間以内に修復してほしい」という相談を受け、解析を実施したことがありました。

このような事例は初めてだった上に期限も短く、さらに、内部が激しく損傷しているとのことだったため、修復できないかもしれないと不安でした。

しかし、これで諦めるわけにはいきません。私は、期間内に修復するために必要となる解析方法等を調査し、懸命に対応したところ、３日間で修復することができました。

その後、捜査員から、私が修復に成功したスマートフォンから証拠となるデータを発見することができ、被疑者の検挙に至ったと連絡があり、改めてやりがいを感じました。

激しく損傷したスマートフォンの修復は非常に困難であり、修復まで長期間を要することもあるなど、つらいこともありますが、技術の進展に対応し続けることができるよう、最新の解析手法に関する情報の収集に不断に努めるとともに、粘り強く解析を実施することで犯罪捜査により一層貢献できるよう常に心掛けています。

サイバー空間の安全・安心の確保に貢献する仕事

東京都警察情報通信部情報技術解析課技術支援第二係
蒔苗（まかなえ）　博充（ひろみつ）



私は、警視庁と連携して東京都内の重要インフラ事業者等を訪問し、最新の技術動向等の情報提供やセキュリティ対策の助言等を行っているほか、サイバー事案対策に関する講演や共同対処訓練に参画するなど、サイバー空間の安全・安心を守るための業務を担当しています。

最近は、企業や自治体等が不正アクセスを受け、ランサムウェアに感染するなどの被害に遭ったというニュースを目にする機会が特に増加していると感じています。実際にサイバー事案による被害に遭った場合、その企業や自治体等の活動が単に停止するだけでなく、国民生活に支障を来すということを企業や自治体等がしっかりと認識し、被害を最小限にとどめるためのセキュリティ対策を講じることが大変重要です。

そのためには、現に発生しているサイバー事案がどのようなものかを理解してもらうことが重要であり、講演や訓練を企画する際には、解析によって得られたマルウェアの機能や特徴のほか、不正アクセスの侵入経路等の情報を整理して盛り込むなど、可能な限り実例を反映させるよう工夫して取り組んでいます。

私の業務は、サイバー空間の安全・安心を守るために技術的な知識や経験を生かして貢献することができる大変重要な仕事であると認識しています。日々の地道な努力を積み重ねて、安心・安全を実感できる社会の実現に向けて取り組んでいきたいと考えています。