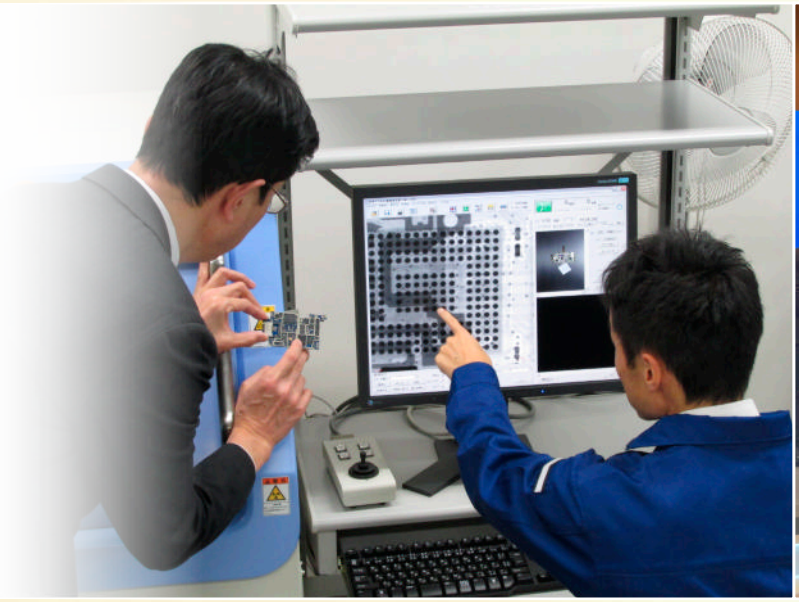
サイバー空間の安全の確保

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の融合が進んでいる。

こうした中、国内において被害が拡大を続けるランサムウェアの感染被害では、サプライチェーン全体の事業活動や地域の医療提供体制に影響を及ぼす事例が確認されるとともに、我が国の暗号資産関連事業者を標的としたサイバー攻撃や、学術関係者・シンクタンク研究員等を標的としたサイバーインテリジェンス(注1)が明らかになり、また、フィッシング報告件数が増加する中でインターネットバンキングに係る不正送金被害が一時的に急増するなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。

1 サイバー事案等の検挙状況

（1）サイバー事案(注2)の検挙件数

令和４年（2022年）中（４月から12月まで）(注3)のサイバー事案の検挙件数は、1,844件であった。

（2）不正アクセス禁止法違反

令和４年中の不正アクセス禁止法違反の検挙件数は522件と、前年より93件（21.7%）増加し、検挙人員は257人と、前年より22人（9.4%）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482件（92.3%）と最多であった。

また、令和４年中の不正アクセス行為の認知件数(注4)は2,200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1,096件（49.8%）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４年中のコンピュータ・電磁的記録対象犯罪の検挙件数は948件と、前年より219件（30.0%）増加した。

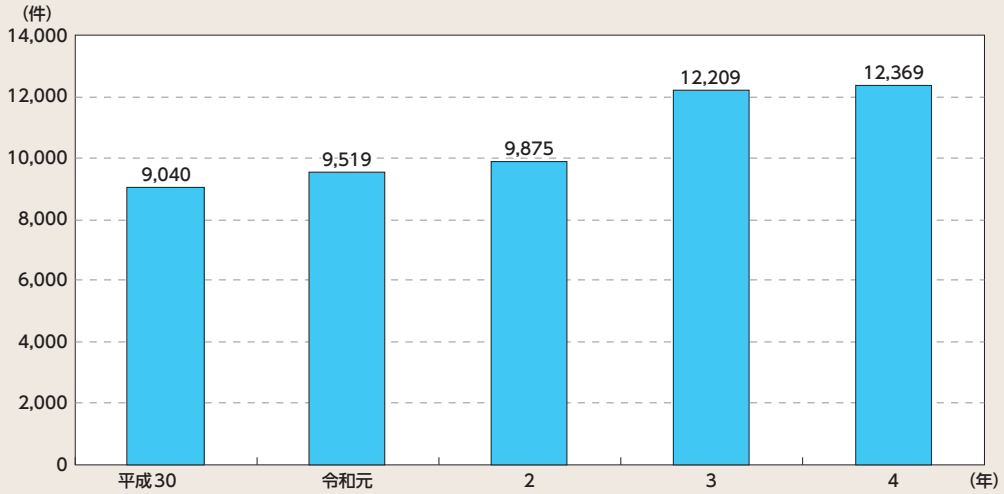
（4）サイバー犯罪(注6)の検挙件数の推移

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４年中の検挙件数は１万2,369件と、前年より160件（1.3%）増加し、過去最多を記録した。

注１：107頁参照
２：108頁参照
３：法令上の用語としての「サイバー事案」は、令和４年４月１日に施行された警察法の一部を改正する法律による改正後の警察法において新たにが定義されたものであることから、同年１月から３月までに検挙されたサイバー事案については計上していない。
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

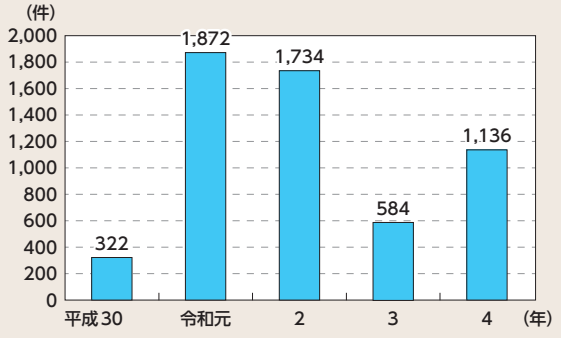
図表３－１　サイバー犯罪の検挙件数の推移（平成30年（2018年）～令和４年）



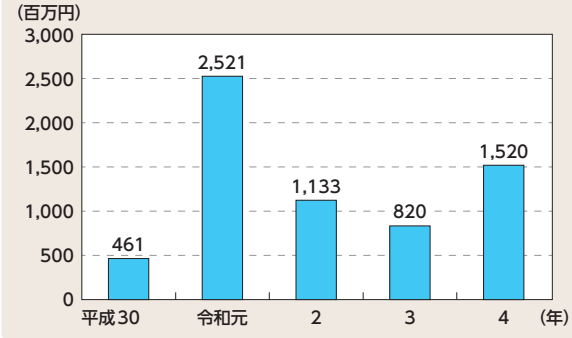
2　インターネットバンキングに係る不正送金事犯の情勢

令和４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1,136件、被害額は約15億2,000万円と、前年に比べて増加した。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30年～令和４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30年～令和４年）



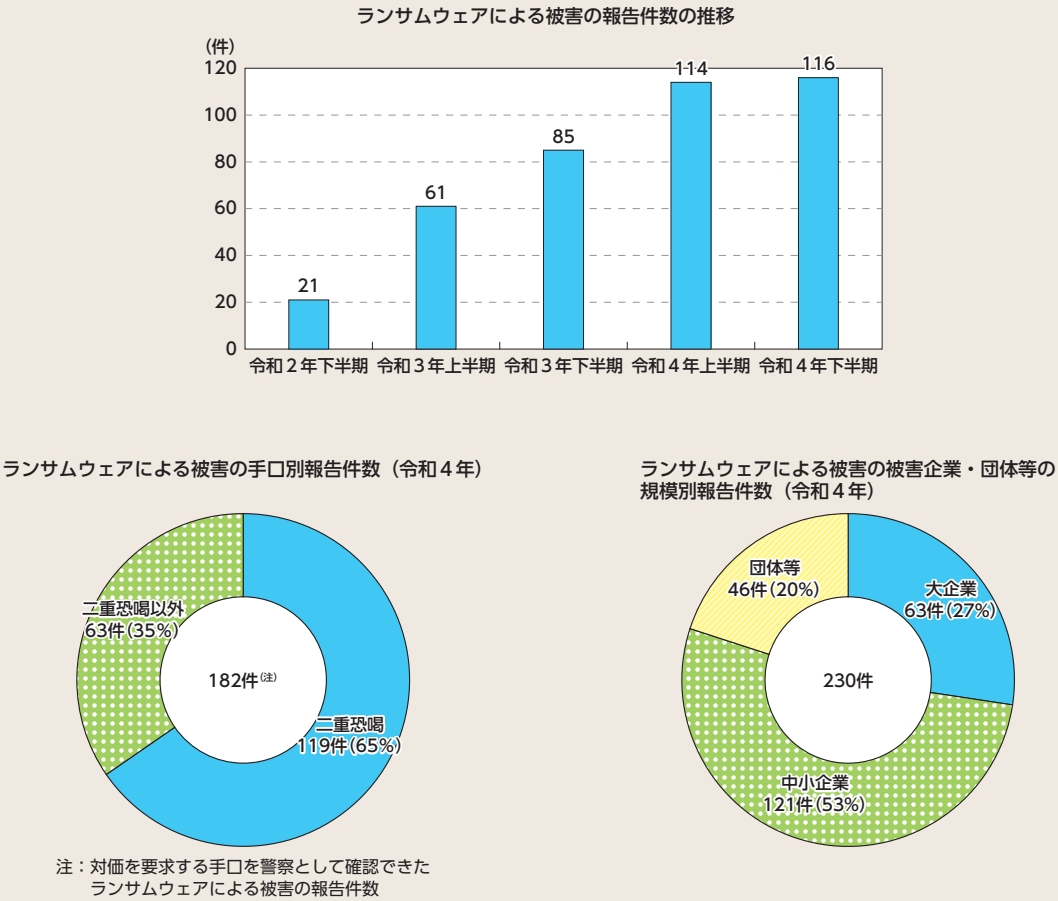
注：銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトにみせかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するよう誘導し、当該サイトでクレジットカード番号や識別符号を入力させて金融情報や個人情報を不正に入手する行為

3 ランサムウェアの情勢

令和４年中のランサムウェアによる被害の報告件数(注１)は230件（令和４年上半期114件、下半期116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。従来の被害においては、暗号化したデータを復元する対価として企業等に金銭や暗号資産を要求する手口が一般的であったが、最近の事例では、データを窃取した上で、企業等に対し「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ダブルエクストーション（二重恐喝）という手口が認められる。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182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119件であり、65％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63件、中小企業は121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102件のうち、VPN機器(注３)を利用して侵入された事例は63件（62％）、リモートデスクトップサービス(注４)を利用して侵入された事例は19件（19％）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：対価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：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・サイバーインテリジェンスの情勢

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(ひ)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）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。

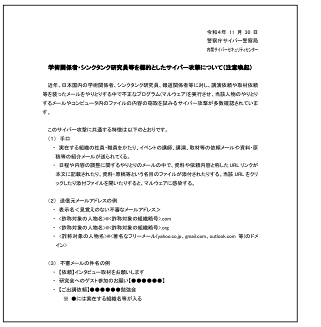
（２）サイバーインテリジェンスの情勢

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。

memo 学術関係者・シンクタンク研究員等を標的としたサイバーインテリジェンスに対する注意喚起

近年、日本国内の学術関係者、シンクタンク研究員等を標的として、講演依頼や取材依頼等を装ったメールのやりとりをする中で不正なプログラムを実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバーインテリジェンスが行われた例が多数確認されている。

こうしたサイバーインテリジェンスの中で、一定の共通点を有する事案を把握するに至ったところ、情報窃取の被害の発生が深く懸念されることに鑑み、令和４年11月、警察庁は、内閣サイバーセキュリティセンター（NISC(注２)）と連名で注意喚起を行った。



令和4年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム（マルウェア）を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

このサイバー攻撃に共通する特徴は以下のとおりです。

（1） 手口
- 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
- 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称した URL リンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該 URL をクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。

（2） 送信元メールアドレスの例
- 表示名＜見覚えのない不審なメールアドレス＞
- <詐称対象の人物名>@<詐称対象の組織略号>.com
- <詐称対象の人物名>@<詐称対象の組織略号>.org
- <詐称対象の人物名>@<著名なフリーメール（yahoo.co.jp、gmail.com、outlook.com 等）のドメイン>

（3） 不審メールの件名の例
- 【依頼】インタビュー取材をお願いします
- 研究会へのゲスト参加のお願い【●●●●●●】
- 【ご出講依頼】●●●●●●勉強会

※ ●には実在する組織名等が入る

注意喚起文の一部

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：National center of Incident readiness and Strategy for Cybersecurityの略

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４年８月下旬から９月までにかけて、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害が急増した。これを受けて、警察庁では、令和４年９月、警察庁ウェブサイトにおいて注意喚起を行うとともに、金融庁と連携して、一般社団法人全国銀行協会等の団体等に対し、フィッシング対策の強化を要請した。

（3）インターネット上の違法情報・有害情報対策

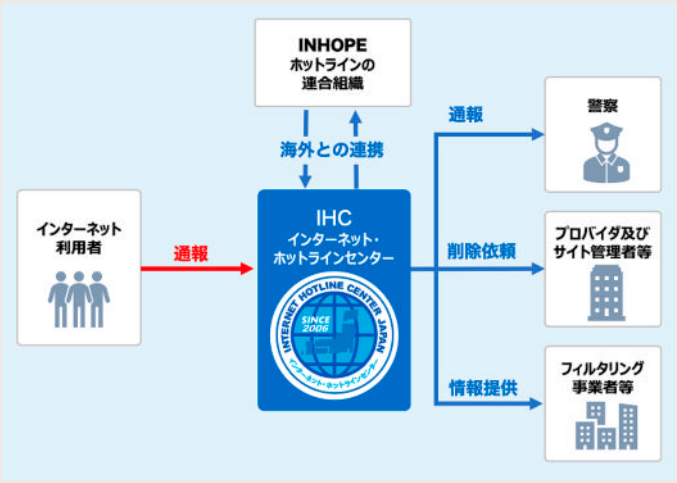
インターネット上には、児童ポルノ、規制薬物の広告に関する情報等の違法情報や、違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない有害情報が多数存在している。

注１：30頁参照（トピックス４）
２：令和４年の調査は、同年９月９日から10月17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、227件の回答を得た。
３：Japan Cybercrime Control Centerの略

①　インターネット・ホットラインセンターの運用

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、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４年中、IHCでは2,433件の違法情報の削除依頼を行い、そのうち2,026件（83.3%）が削除された。また、2,687件の自殺誘引等情報の削除依頼を行い、そのうち1,634件（60.8%）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。

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



②　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

インターネットを通じて銃砲等の設計図、製造方法等に関する情報を容易に入手することができる現代社会の特性を踏まえ、インターネット上の違法情報・有害情報対策を強化するため、令和５年２月、IHCにおいて取り扱う情報の範囲に、個人の生命・身体に危害を加えるおそれが高い重要犯罪等と密接に関連する情報（重要犯罪密接関連情報）を追加した。

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。

重要犯罪密接関連情報に関する広報啓発資料

（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、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ずるよう注意喚起を行っている。

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：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)

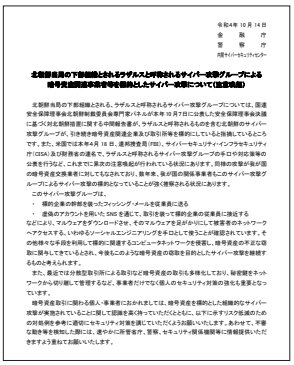
（5）サイバー攻撃対策

警察では、サイバー攻撃に適切に対処するため、サイバー警察局、サイバー特別捜査隊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 ラザルスに対するパブリック・アトリビューション

北朝鮮当局の下部組織であるとされるラザルスと呼称されるサイバー攻撃集団が、数年来、国内の暗号資産関係事業者を標的としたサイバー攻撃を行っていると強く推察される状況にあることが、関係警察やサイバー特別捜査隊の捜査等によって判明した。

ラザルスによるものとみられる暗号資産の窃取を目的としたサイバー攻撃は、今後も継続すると考えられる。また、最近においては、暗号資産取引が、事業者を介さず個人間でも行われるようになってきていることから、個人も標的とされるおそれがある。こうした状況を踏まえ、警察庁は令和４年10月、金融庁及びNISC(注1)との連名で注意喚起を行い、暗号資産取引に関わる個人や事業者に対し、組織的なサイバー攻撃が行われているという認識を持って適切なサイバーセキュリティ対策を講じるよう呼び掛けた。



令和４年10月14日
金融庁
警察庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年１０月７日に公表した安全保障理事会決議に基づく北朝鮮制裁に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年４月１８日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者をこのサイバー攻撃グループによるサイバー攻撃の標的としていることが強く推察される状況にあります。

このサイバー攻撃グループは、

・　標的企業の幹部を装ったフィッシングメールを従業員に送る
・　虚偽のアカウントを用いたSNSを通じて、取引を装って標的企業の従業員に接近する

などにより、マルウェアをダウンロードさせ、そのマルウェアを足がかりにして標的者のネットワークへアクセスする、いわゆるソーシャルエンジニアリングを手口として使うことが確認されています。その他様々な段階を利用して標的に関連するコンピュータネットワークを探索し、暗号資産の不正な窃取に関与しているとされ、今後このような暗号資産の窃取を目的としたサイバー攻撃を継続するものと考えられます。

また、最近では分散型取引所による取引など暗号資産の取引も多様化しており、秘密鍵をネットワークから切り離して管理するなど、事業者だけでなく個人のセキュリティ対策の強化も重要となっています。

暗号資産取引に関わる個人・事業者におかれましては、暗号資産を標的とした組織的なサイバー攻撃が実施されていることに関して認識を高めていただくとともに、以下に示すリスク低減のための対策例を参考に適切にセキュリティ対策を講じていただくようお願いいたします。あわせて、不審な動きを検知した際には、速やかに所管省庁、警察、セキュリティ関係機関等に情報提供いただきますよう重ねてお願いいたします。

警察庁、金融庁及びNISCによる注意喚起文

memo サイバー特別捜査隊の活動状況

サイバー空間における極めて深刻な脅威の情勢を踏まえ、令和４年４月、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サイバー特別捜査隊が設置された。

重大サイバー事案について、サイバー特別捜査隊が都道府県警察と共同で捜査を進める中、サイバー特別捜査隊による情報の集約・分析や、その結果に基づく外国捜査機関との情報交換等を通じ、外国に被疑者が存在するなど検挙が困難とみられたような事案についても、捜査が着実に進められつつある。

外国捜査機関等との会議の状況

実際、上記のラザルスによるものと推察される暗号資産の窃取を目的としたサイバー攻撃についても、サイバー特別捜査隊の捜査等が実態解明に寄与したほか、米国におけるランサムウェア事案について、サイバー特別捜査隊等の捜査で得られた情報をFBIに提供するなどの協力を行った結果、令和５年５月、米国司法省から被疑者の１人を起訴した旨の発表があり、捜査に当たって日本警察の支援が有益であったとの言及があった。また、サイバー保険を名目とした架空料金請求詐欺事件について、サイバー特別捜査隊において暗号資産追跡の支援を行い、令和５年５月、愛知県警察等の５県警察による合同捜査本部が被疑者２人を逮捕した。

CASE サイバー防衛演習「ロックド・シールズ2023」への参加

令和５年４月に開催されたNATOサイバー防衛協力センター主催のサイバー防衛演習「ロックド・シールズ2023」において、オーストラリアと我が国の合同チームが編成され、防衛省等と共に、警察庁からも職員が参加した。

注１：107頁参照
２：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 技術支援と解析能力の向上

（1）サイバーフォースの役割

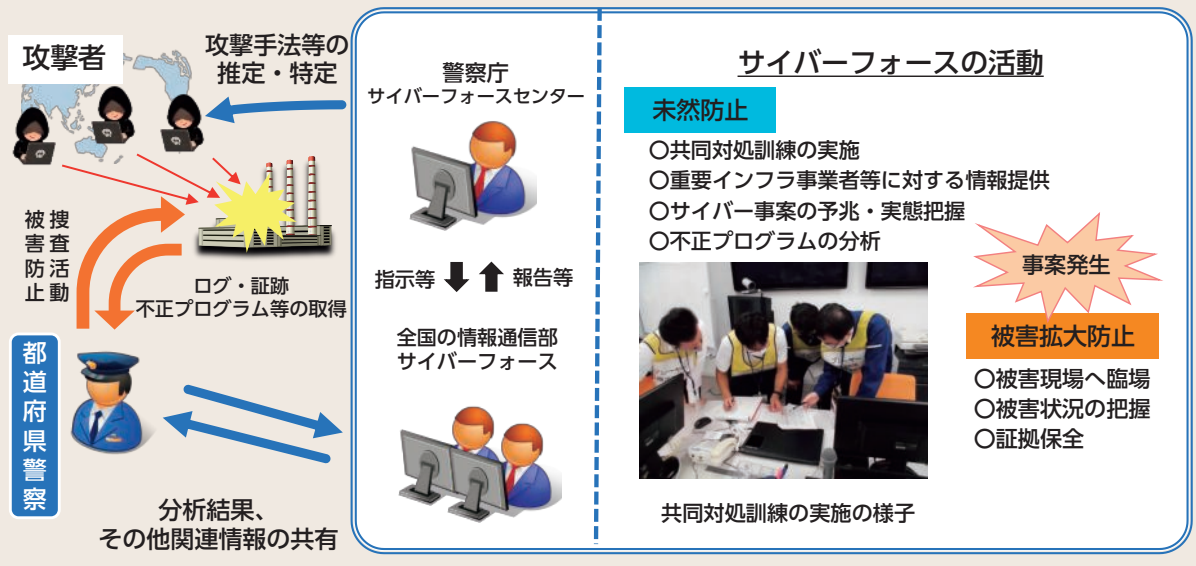
警察では、深刻化するサイバー事案に対処するため、攻撃の対象となったサイバーセキュリティ上のぜい弱性に関する情報や、標的型メール攻撃等の犯行手口に関する情報等を、捜査活動及び事業者との情報交換を通じて把握・分析し、被害の未然防止及び拡大防止に努めている。

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。

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

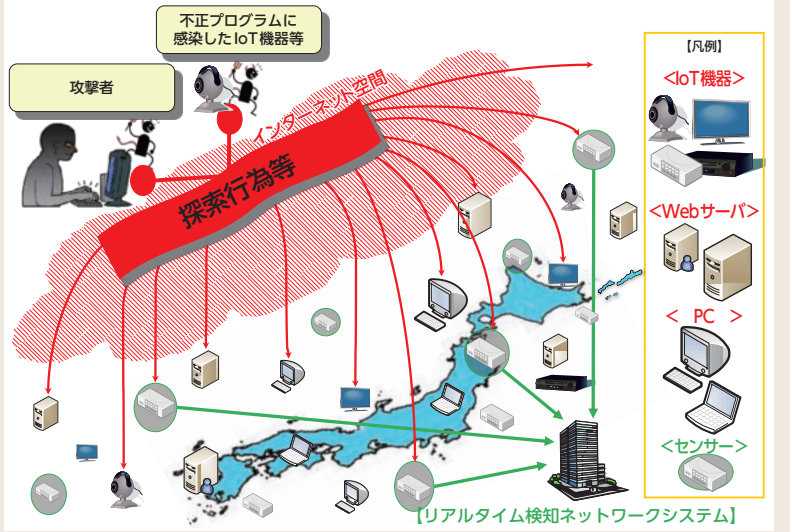


注１：管区警察局情報通信部（四国警察支局情報通信部を含む。以下同じ。）、東京都警察情報通信部、北海道警察情報通信部、府県情報通信部（四国警察支局の管轄区域内の県情報通信部を含む。以下同じ。）及び方面情報通信部
２：119頁参照

（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、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。

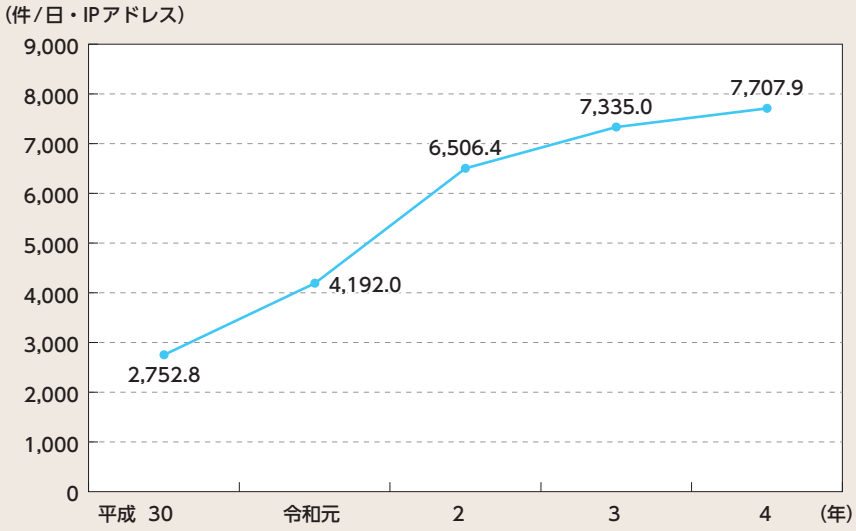
サイバーフォースセンターでは、本システムから得られる情報を用いて、24時間体制でサイバー事案の予兆・実態等を把握し、インターネット利用者がサイバー事案の危険性を正しく認識し、適切な対策を自主的に講じられるよう、分析結果を警察庁ウェブサイトにおいて広く一般に公開している。

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４年中のインターネット観測結果

令和４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11.2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。

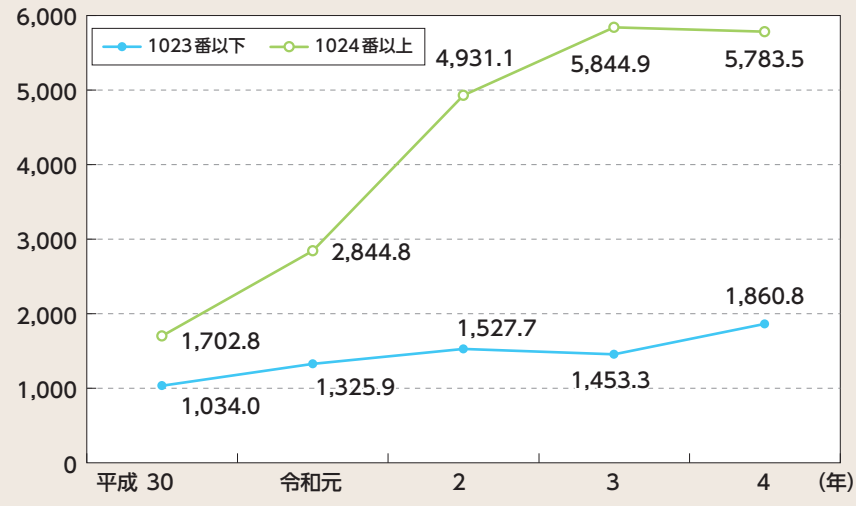
図表３－８　リアルタイム検知ネットワークシステムにおいて検知した一つのセンサーに対する１日当たりの不審なアクセス件数の推移（平成30年～令和４年）



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く、こうしたアクセスの多くは、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であるとみられる。

そのほか、リモートデスクトップサービスの稼働状況を調べることが目的と思われるアクセスの増加が観測された。テレワークが社会的に浸透し、リモートデスクトップサービス(注２)を利用する機会が増加していることに伴い、それらが攻撃の対象となり得るリスクも増しているものと考えられる。

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30年～令和４年）



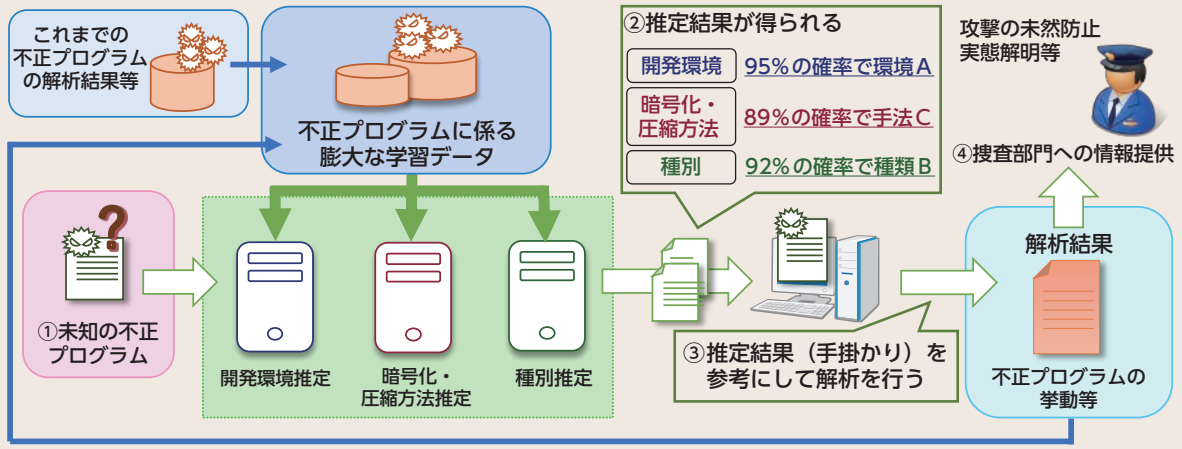
注１：TCP/IP通信（インターネット等で用いられているネットワーク上でデータを交換する際の取決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。
２：ネットワークで接続された他のコンピュータのデスクトップ環境を操作する機能

（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。

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。

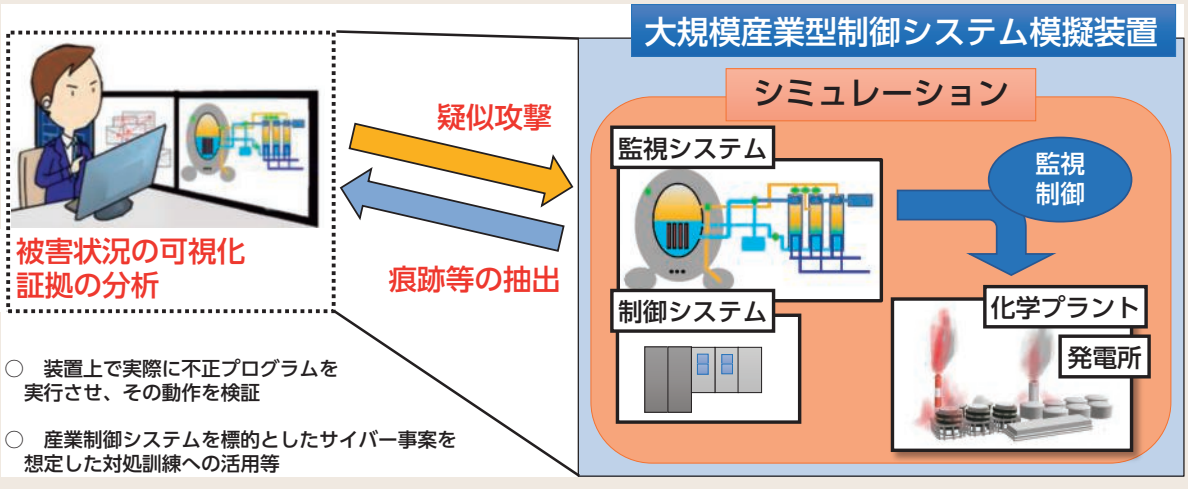
図表３－10　機械学習を活用した不正プログラム解析の高度化・効率化のイメージ



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：106頁参照

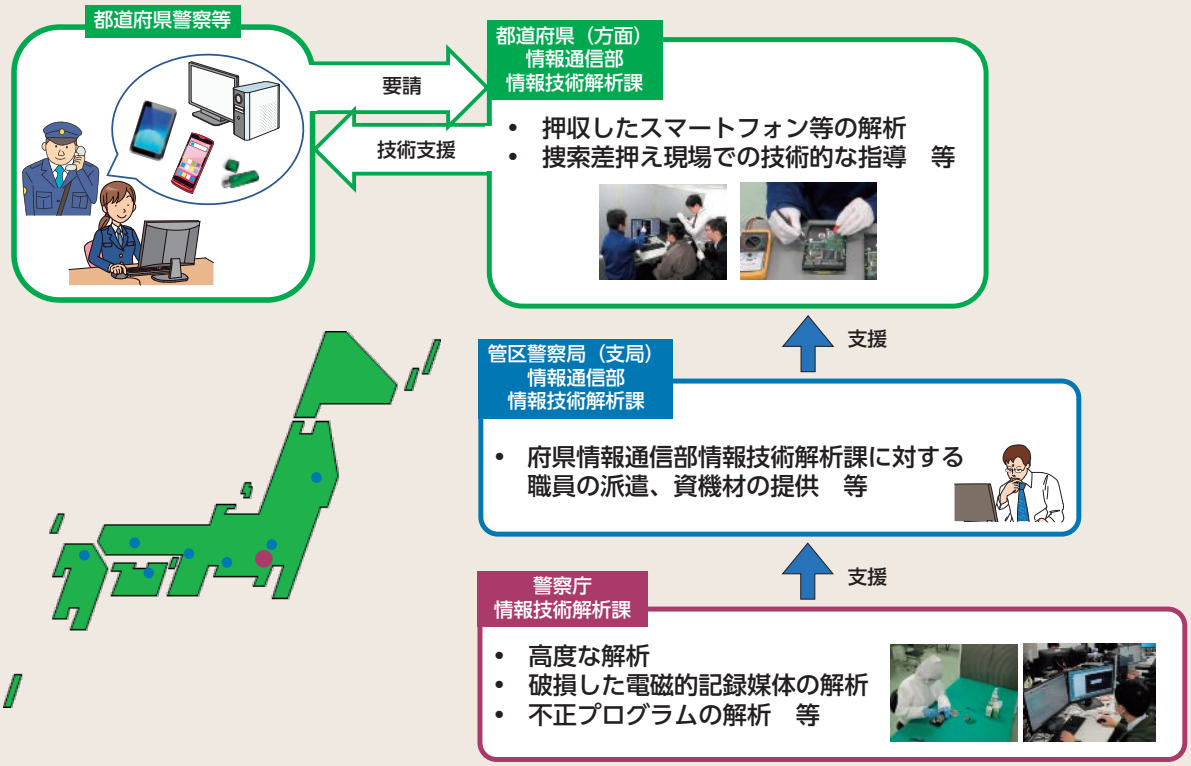
（４）犯罪の取締りのための技術支援体制

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、都道府県警察等に対し、捜索・差押えの現場でコンピュータ等を適切に差し押さえるための技術的な指導や、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の実施についての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体制



（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：111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、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。

図表３－13　サイバー空間における脅威への対処に係る人材育成

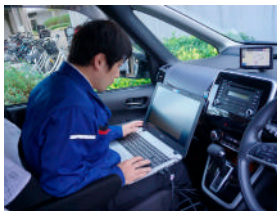
さらに、警察庁では、高度な解析技術を持つ職員の育成を行うため、最新の技術を有する民間企業や研究機関との技術協力を推進している。

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４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

memo　サイバーコンテストの開催

警察庁では、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

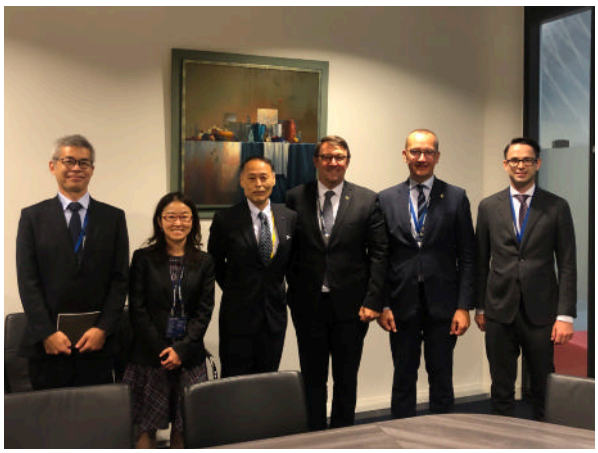
警察庁では、多国間における情報交換や協力関係の確立等に積極的に取り組んでおり、令和４年中は、G7ローマ／リヨン・グループ(注１)に置かれたハイテク犯罪サブグループ、サイバー犯罪条約(注２)の締約国等が参加するサイバー犯罪条約委員会会合、EUROPOL(注３)が主催するサイバー犯罪会議等の国際会議に参加した。また、FBI(注４)が主催する各国の捜査機関職員を対象としたサイバー犯罪対策等に関する研修に我が国の警察職員を派遣するなど、サイバー空間における脅威に関する情報の共有や、国際捜査共助に関する連携強化等を推進している。

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(注５)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６)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 欧州各国との連携強化の推進

警察庁においては、令和４年６月から、欧州各国の捜査機関との緊密な連携を図るため、サイバー事案対策に専従する連絡担当官をEUROPOLに初めて常駐させ、信頼関係の構築を進めている。

令和４年10月には、サイバー警察局長がEUROPOLにおいて開催された欧州警察長官会議に出席するとともに、フランス、オランダ及びドイツの３か国の捜査機関を訪問し、サイバー犯罪対策部門の長等とサイバー空間をめぐる脅威情勢、ランサムウェア対策、連絡担当官を通じた連携強化等について協議を行った。



サイバー警察局長によるEUROPOL訪問

（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７)）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。

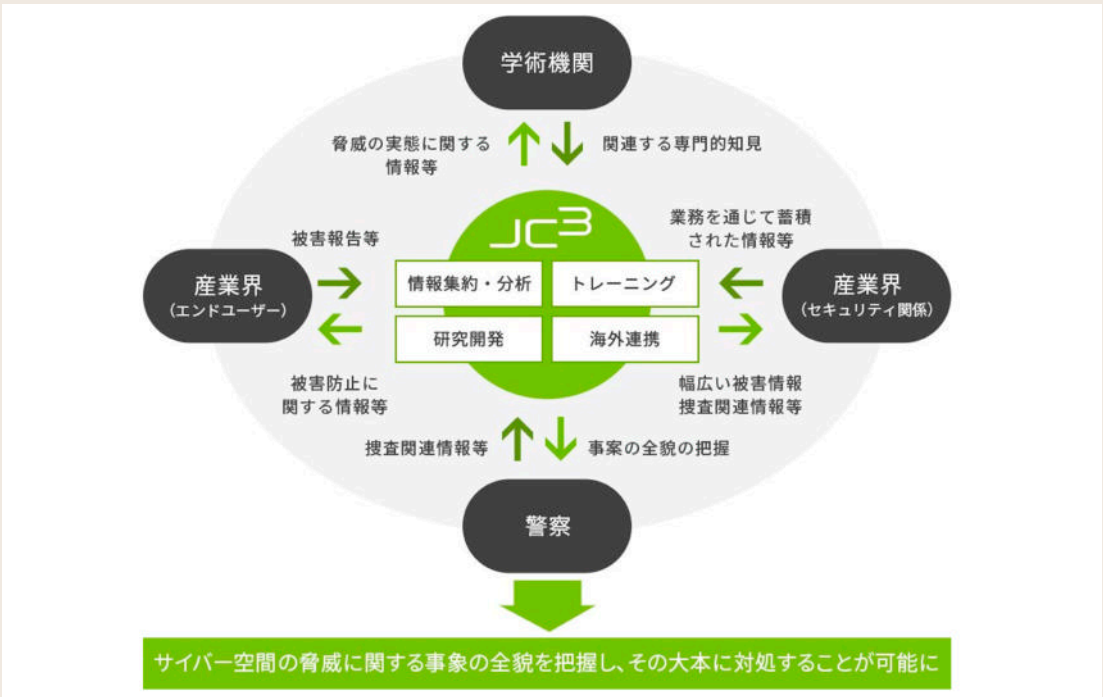
注１：昭和53年（1978年）にボン・サミットを契機に発足したG8テロ専門家会合（G8ローマ・グループ）と平成７年（1995年）にハリファクス・サミットで設置されたG8国際組織犯罪対策上級専門家会合（G8リヨン・グループ）が、平成13年（2001年）の米国における同時多発テロ事件以降合同で開催されているもので、国際組織犯罪対策やテロ対策等について検討している。なお、平成26年（2014年）３月から、G7として実施している。
２：サイバー犯罪に関する条約。サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な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：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。
４：Federal Bureau of Investigation（米国連邦捜査局）の略
５：International Criminal Police Organization（国際刑事警察機構）の略
６：Forum of Incident Response and Security Teamsの略
７：Japan International Cooperation Agencyの略

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1)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281団体、6,824人（令和４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

警察庁では、令和５年２月から３月にかけて、サイバー防犯ボランティアを対象とした広報啓発コンテストを実施した。サイバー防犯ボランティアから、「フィッシング対策」又は「ランサムウェア対策」をテーマとした広報動画を募集し、警察庁Twitterへの掲載等により審査を行い、テーマごとに、最優秀作品にはサイバー警察局長賞を、次点の優秀作品にはサイバー審議官賞を、それぞれ授与した(注2)。

サイバー防犯ボランティア広報啓発コンテスト最優秀作品

注１：108頁参照
２：警察庁ウェブサイト「サイバー防犯ボランティア広報啓発コンテストの実施結果について」(https://www.npa.go.jp/bureau/cyber/koho/news/csvolunteer_contest.html)

（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。

（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することができない新たな不正プログラムに関する情報をはじめとする不正プログラム対策に資する情報を提供し、サイバー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

警察では、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「電気通信事業における個人情報等の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、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本人確認の実施について働き掛けを行ってきた。この働き掛けを受けて、令和３年１月、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：Mobile Virtual Network Operatorの略。自ら無線局を開設・運用せずに移動通信サービスを提供する電気通信事業者
２：通信当事者以外の第三者が、SMS認証に用いる携帯電話番号や当該認証のための認証コードを当該通信当事者に提供する行為

警察活動の最前線

安全・安心なサイバー空間の実現を目指して

前　沖縄県警察本部生活安全部サイバー犯罪対策課サイバー犯罪特捜係（現　沖縄県警察本部警務部監察課監察第一係）
仲眞　克美

サイバー犯罪は、年々その手口を深刻化・巧妙化させています。その一つとして、インターネットバンキングに係る不正送金が挙げられます。

私が捜査に携わった事案では、不正に入手した利用者のID・パスワードを用いた不正送金が全国17都府県で発生し、現金の引き出し場所が沖縄県内だけでも100か所以上に及ぶとともに、被害額も多額に上っていることが確認できました。

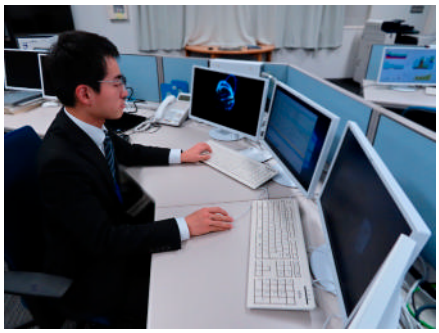
そこで、９県警察による合同捜査体制を構築し、各県連携した一斉捜査を行うことで、指示役を含む多数の上位被疑者を逮捕するに至りました。

その後、約３年半に及ぶ捜査により、指定暴力団組員を含む数十名を検挙するとともに、徹底したスマートフォンのデータ解析、IPアドレスの差押え、解析等を重ね、海外で不正アクセスを敢行しているグループや本件の首魁等犯罪グループの実態を解明しました。

私は沖縄県警察の捜査員の一人にすぎませんが、今回の９県警察による合同捜査で得た貴重な経験を生かし、県境も国境も関係なく発生するサイバー空間における犯罪に敢然と立ち向かっていきたいと思います。

サイバー事案の予兆を見逃すな！

警察庁サイバー警察局情報技術解析課情勢把握第二係
後藤　隆文



私が所属しているサイバーフォースセンターでは、サイバー空間の安全・安心の確保に向けて、インターネット上に設置したセンサーで検知した情報から、インターネット上で発生している脅威を分析しています。このような脅威の中には、日本の重要インフラ事業者等に対するサイバー攻撃やその予兆となるものが含まれていることがあることから、収集した情報の高度な分析により、サイバー事案の予兆の把握に努めています。

企業などで使われるネットワーク機器やシステム等のぜい弱性は日々出現しており、サイバー事案に悪用される手法も常に変化しています。サイバー事案の実態を把握するには、警察庁で設置しているセンサーだけでなく、インターネット上に公開されているあらゆる情報源からデータを収集･分析する必要があります。私は､このようなサイバー事案に関係する情報をインターネット上から自動で収集するプログラムを作成し、分析業務の効率化に役立てています。

あらゆるモノがインターネットにつながる昨今、サイバー空間における攻撃者の目的や手法は変化し続けており、新たな情報の収集や分析が欠かせません。これからも、自分自身の知識や技能を常にアップデートしながら、分析技術の向上、高度化にもまい進していきます。