# 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

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、親ロシア派ハッカー集団によるものとみられるDDoS攻撃(注1)により、政府機関や重要インフラ事業者のウェブサイトの閲覧障害が断続的に発生するとともに、中国を背景とするサイバー攻撃グループにより、情報窃取を目的としたサイバー攻撃が行われていることが確認された。また、ランサムウェア被害が依然として高水準で推移していることに加え、クレジットカード不正利用被害が急増し、インターネットバンキングに係る不正送金被害が過去最多となっているほか、インターネット上では児童ポルノや規制薬物の広告等の違法情報や、自殺誘引等情報(注2)、爆発物・銃砲等の製造方法、殺人や強盗の請負等の有害情報が氾濫するなど、サイバー空間をめぐる脅威は、引き続き極めて深刻な情勢にある。

## 1 サイバー事案等の検挙状況

### （1）サイバー事案(注3)の検挙件数

令和５年（2023年）中のサイバー事案の検挙件数は、3,003件であった。

### （2）不正アクセス禁止法違反

令和５年中の不正アクセス禁止法違反の検挙件数は521件と、前年より１件（-0.2%）減少し、検挙人員は259人と、前年より２人（0.8%）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475件（91.2%）と最多であった。

また、令和５年中の不正アクセス行為の認知件数(注4)は6,312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5,598件（88.7%）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５年中のコンピュータ・電磁的記録対象犯罪の検挙件数は1,000件と、前年より52件（5.5%）増加した。

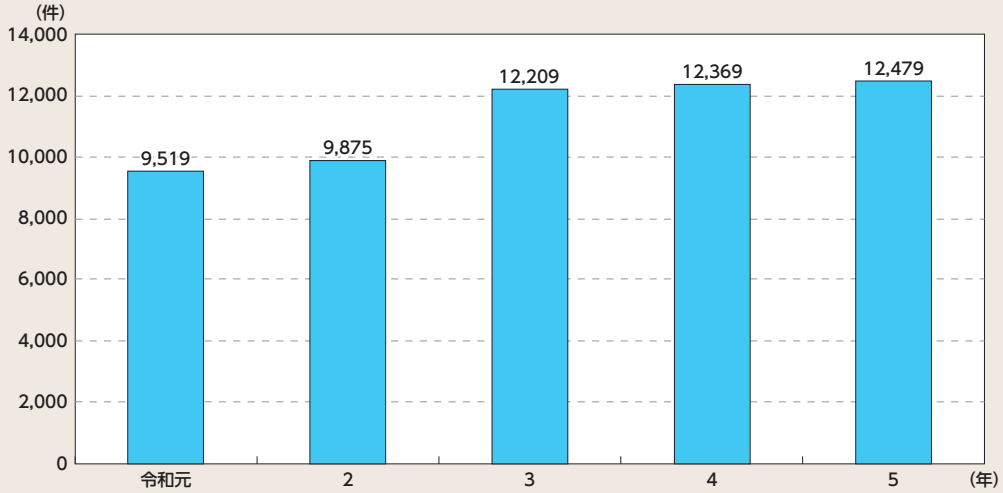
### （4）サイバー犯罪(注6)の検挙件数の推移

最近５年間のサイバー犯罪の検挙状況は、図表３－１のとおりである。

サイバー犯罪の検挙件数は増加傾向にあり、令和５年中の検挙件数は１万2,479件と、前年より110件（0.9%）増加し、過去最多を記録した。

注１：Distributed Denial of Serviceの略。特定のコンピュータに対し、複数のコンピュータから大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃
２：他人を自殺に誘引・勧誘する情報等
３：116頁参照
４：不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を認知した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合その他関係資料により不正アクセス行為の事実を確認することができた場合において、被疑者が行った犯罪構成要件に該当する行為の数
５：刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪
６：不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

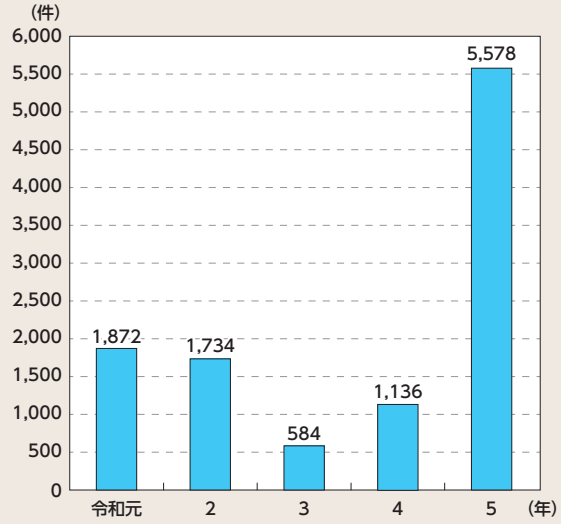
図表３－１　サイバー犯罪の検挙件数の推移（令和元年～令和５年）



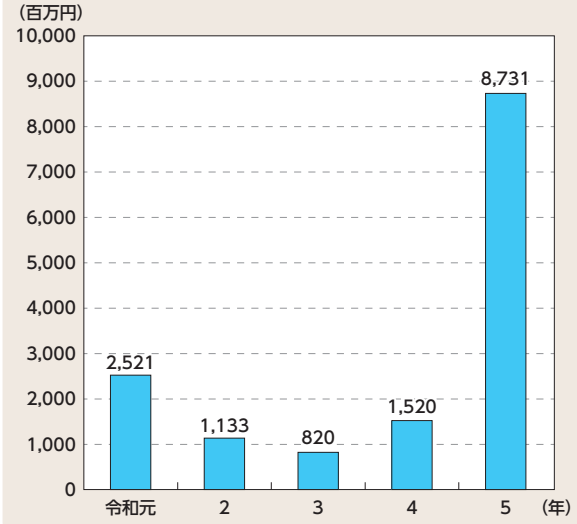

## 2　インターネットバンキングに係る不正送金事犯の情勢

令和５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5,578件、被害額は約87億3,130万円と、過去最高となった。その被害の多くは、金融機関等を装ったフィッシング(注)によるものと考えられる。

図表３－２　インターネットバンキングに係る不正送金事犯の発生件数の推移（令和元年～令和５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（令和元年～令和５年）




注：８頁参照（特集）

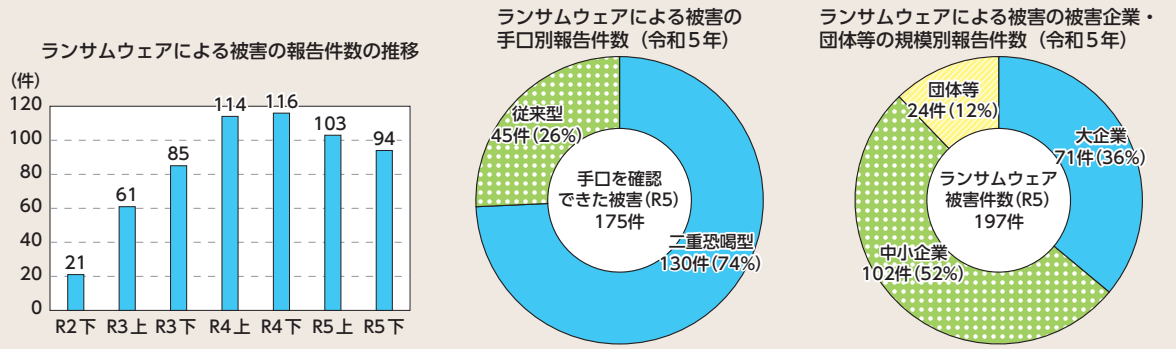
## 3 ランサムウェアの情勢

令和５年中のランサムウェアによる被害の報告件数(注１)は197件（令和５年上半期103件、下半期94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175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130件であり、74％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71件、中小企業は102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115件のうち、VPN機器(注３)が利用されて侵入された事例は73件（63％）、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21件（18％）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５年中30件確認されている。

図表３－４　ランサムウェアによる被害の報告件数




**CASE**

令和５年７月、名古屋港運協会は、名古屋港のコンテナターミナルにおけるコンテナの船積み・船卸や搬出入の作業等を一元的に管理するシステムがランサムウェアに感染し、同システムのサーバが暗号化されたことにより、システム障害が発生したと発表した。これにより、同ターミナルにおけるコンテナの搬出入等が約３日間停止し、物流に大きな影響が生じた。

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

# 4 サイバーテロ・サイバーエスピオナージの情勢

重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロ(注)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。

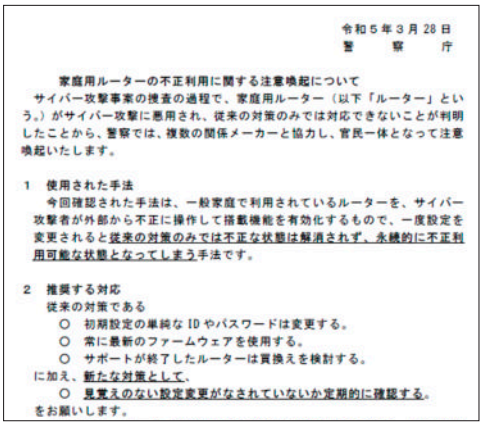
## （2）サイバーエスピオナージの情勢

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 家庭用ルーターの不正利用に関する注意喚起

警察における捜査の過程で、家庭用ルーターが、初期設定のID・パスワードの変更や最新のソフトウェアへのアップデートなどの従来の対策では対応することができない手法で、サイバーエスピオナージ等に悪用されていることが判明した。そこで、令和５年３月、警察庁及び警視庁において、複数の関係メーカーと協力し、注意喚起を実施した。

同注意喚起では、各家庭で所有するルーターについて、従来の対策に加え、新たな対策として、見覚えのない設定変更がなされていないか確認するよう呼び掛けを行った。



令和５年３月28日
警　察　庁

家庭用ルーターの不正利用に関する注意喚起について

サイバー攻撃事案の捜査の過程で、家庭用ルーター（以下「ルーター」という。）がサイバー攻撃に悪用され、従来の対策のみでは対応できないことが判明したことから、警察では、複数の関係メーカーと協力し、官民一体となって注意喚起いたします。

１　使用された手法
今回確認された手法は、一般家庭で利用されているルーターを、サイバー攻撃者が外部から不正に操作して搭載機能を有効化するもので、一度設定を変更されると従来の対策のみでは不正な状態は解消されず、永続的に不正利用可能な状態となってしまう手法です。

２　推奨する対策
従来の対策である
○　初期設定の単純なIDやパスワードは変更する。
○　常に最新のファームウェアを使用する。
○　サポートが終了したルーターは買換えを検討する。
に加え、新たな対策として、
○　見覚えのない設定変更がなされていないか定期的に確認する。
をお願いします。


注意喚起文の一部と警視庁が公表したリーフレット

注：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

# 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

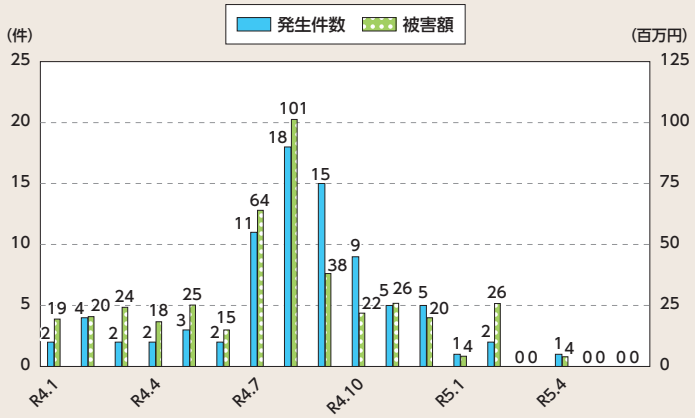
警察では、不正アクセス行為の犯行手口の分析に基づき、関係機関等とも連携し、広報啓発等の不正アクセスを防止するための取組を実施しているほか、不正アクセス行為による被害防止のための広報啓発に資することを目的として、毎年、民間企業や行政機関等に対する「不正アクセス行為対策等の実態調査」(注1)及び「アクセス制御機能に関する技術の研究開発状況等に関する調査」(注2)を行っている。

### （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。このほか、令和４年（2022年）７月から８月にかけてSIMスワップ(注4)による不正送金事犯が急増した状況を踏まえ、令和４年９月、大手携帯電話事業者に対し、販売店における本人確認の強化についての要請を総務省と連携して行ったところ、令和５年２月までに、各事業者において要請に基づき本人確認が強化された結果、令和５年上半期におけるSIMスワップによる不正送金事犯の被害が激減した。

図表３－５ SIMスワップに係る不正送金発生状況




注１：令和５年の調査は、同年８月23日から９月15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、618件の回答を得た。

２：令和５年の調査は、同年８月23日から９月15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、1,844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、214件の回答を得た。

３：Japan Cybercrime Control Centerの略

４：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

## memo 「キャッシュレス社会の安全・安心の確保に関する検討会」の開催

クレジットカードの不正利用及びインターネットバンキングに係る不正送金事犯の被害が過去最多となっている状況を踏まえ、警察庁において、「キャッシュレス社会の安全・安心の確保に関する検討会」を、令和５年11月から令和６年２月にかけて開催した。同検討会では、最先端技術の活用等によるフィッシング対策の高度化・効率化や、クレジットカードの不正利用に関する関係事業者との情報共有による被害防止対策・捜査の推進等に関し、これらの知見を有する金融業界やセキュリティ関係団体等の有識者の間で幅広い議論が行われ、令和６年３月、被害に遭わないための環境整備等を内容とする報告書が取りまとめられた。

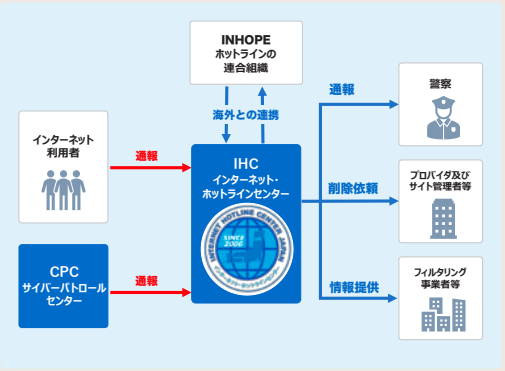
## （３）インターネット上の違法情報・有害情報対策

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。

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

警察庁では、一般のインターネット利用者等から違法情報や、重要犯罪密接関連情報(注１)、自殺誘引等情報(注２)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５年中、IHCでは1,913件の違法情報の削除依頼を行い、そのうち1,645件（86.0%）が削除されたほか、3,379件の重要犯罪密接関連情報の削除依頼を行い、そのうち2,411件（71.4%）が、6,609件の自殺誘引等情報の削除依頼を行い、そのうち3,851件（58.3%）が、それぞれ削除された。IHCに通報された違法情報等の中には、外国のサーバにそのデータが蔵置されているものがあるところ、このうち児童ポルノについては、各国のホットライン相互間の連絡組織であるINHOPE(注３)の加盟団体に対し、削除に向けた措置を依頼している。

図表３－６　インターネット・ホットラインセンターにおける取組




重要犯罪密接関連情報に関する広報啓発資料

また、警察庁では、インターネット上の重要犯罪密接関連情報等を収集し、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、令和５年９月、重要犯罪密接関連情報を自動収集してその該当性を判定するAI検索システムを導入し、サイバーパトロールの高度化を図っている。

### ②　インターネット・ホットラインセンター等における取組の強化

近年、著しく高額な報酬の支払いを示唆して犯罪の実行者を直接的かつ明示的に誘引等（募集）する情報（犯罪実行者募集情報）が、インターネット上に氾濫していることを踏まえ、「SNS上で実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」（令和５年３月17日犯罪対策閣僚会議決定）では、この種の情報の排除に向けた更なる取組の推進が掲げられた。こうしたことを受け、令和５年９月、IHC及びCPCにおいて取り扱う情報の範囲に犯罪実行者募集情報を追加した。

注１：12頁参照（特集）
２：112頁参照
３：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

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

#### ③　効果的な違法情報等の取締り

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

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

### （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)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。

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

#### memo　BlackTechに対するパブリック・アトリビューション

中国を背景とするサイバー攻撃グループBlackTechが、平成22年頃以降、日本を含む東アジア及び米国の政府機関や工業、科学技術、メディア、エレクトロニクス、電気通信分野の事業者を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認された。

これを受け、令和５年９月、警察庁は、内閣サイバーセキュリティセンター（NISC）、米国国家安全保障局（NSA）、米国連邦捜査局（FBI）及び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）との連名で注意喚起を行い、BlackTechの手口を説明したほか、リスク低減のための対処例について呼び掛けた。


Cybersecurity Advisory

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

注：警察庁ウェブサイト「ランサムウェア被害防止対策」
(https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html)

# 2 技術支援と解析能力の向上

## （1）サイバーフォースの役割

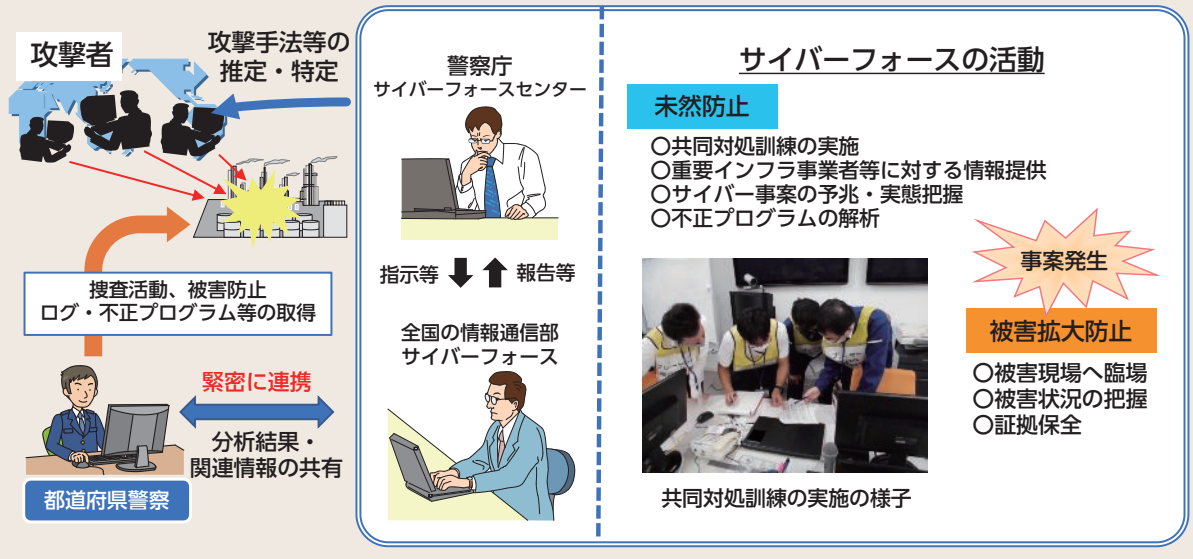
警察では、深刻化するサイバー事案に対処するため、攻撃の対象となったサイバーセキュリティ上のぜい弱性に関する情報や、標的型メール攻撃等の犯行手口に関する情報等を、捜査活動及び事業者との情報交換を通じて把握・分析し、被害の未然防止及び拡大防止に努めている。

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

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

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

図表3－7　サイバーフォースの役割と活動

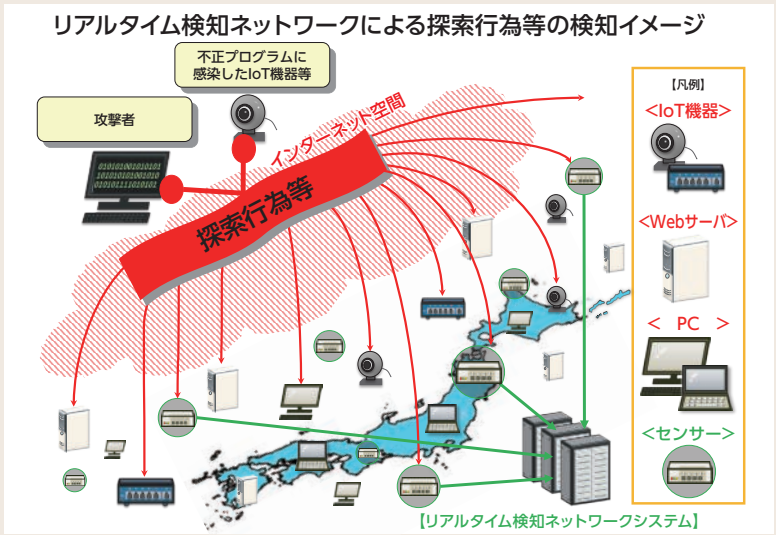



注1：管区警察局情報通信部（四国警察支局情報通信部を含む。以下同じ。）、東京都警察情報通信部、北海道警察情報通信部、府県情報通信部（四国警察支局の管轄区域内の県情報通信部を含む。以下同じ。）及び方面情報通信部
2：126頁参照

## （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３－８　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。

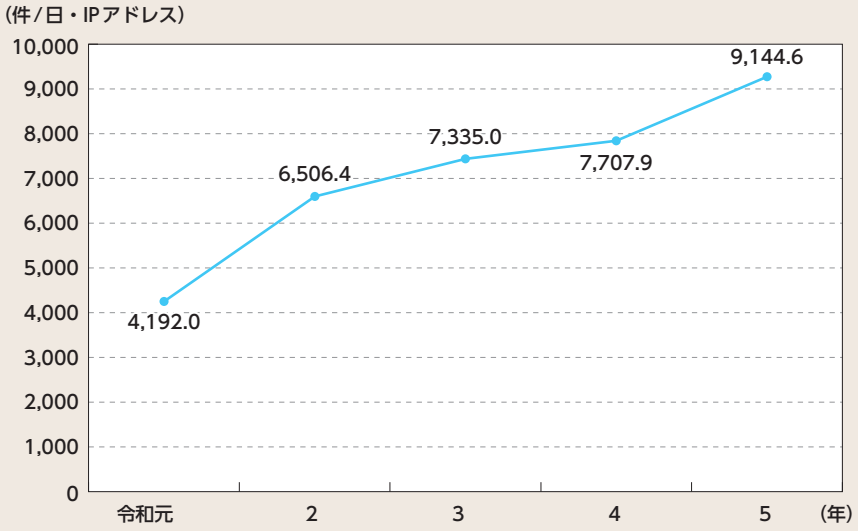
サイバーフォースセンターでは、本システムから得られる情報を用いて、24時間体制でサイバー事案の予兆・実態等を把握し、インターネット利用者がサイバー事案の危険性を正しく認識し、適切な対策を自主的に講じられるよう、分析結果を警察庁ウェブサイトにおいて広く一般に公開している。

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５年中のインターネット観測結果

令和５年中、リアルタイム検知ネットワークシステムのセンサーにより、一つのセンサー当たり約9.4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。

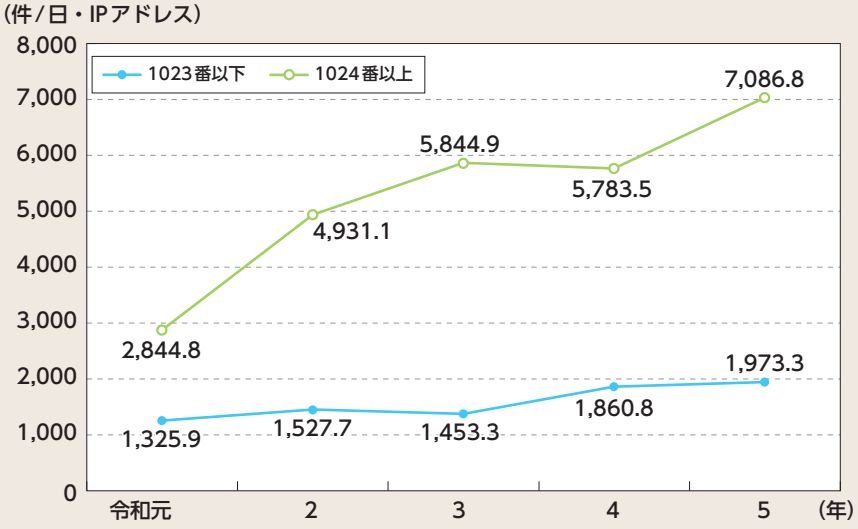
図表３－９　リアルタイム検知ネットワークシステムにおいて検知した一つのセンサーに対する１日当たりの不審なアクセス件数の推移（令和元年～令和５年）




検知した不審なアクセスについて、宛先ポート番号(注)に着目すると、1024番以上のポート番号へのアクセスが大きな割合を占めている。IoT機器では、標準設定として1024番以上のポート番号が使用されているものも多く、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。

このほか、Wi-Fiルーターを対象とした不審なアクセスが複数観測された。観測されたアクセスは、Wi-Fiルーターのぜい弱性を狙ったもののほか、Wi-Fiルーターの設定変更等を行うための管理用のポートに対してユーザ名・パスワードを送信してログインを試行したと疑われるものであった。

図表３－10　ポート番号1023以下及び1024以上のポートへのアクセス件数の推移（令和元年～令和５年）



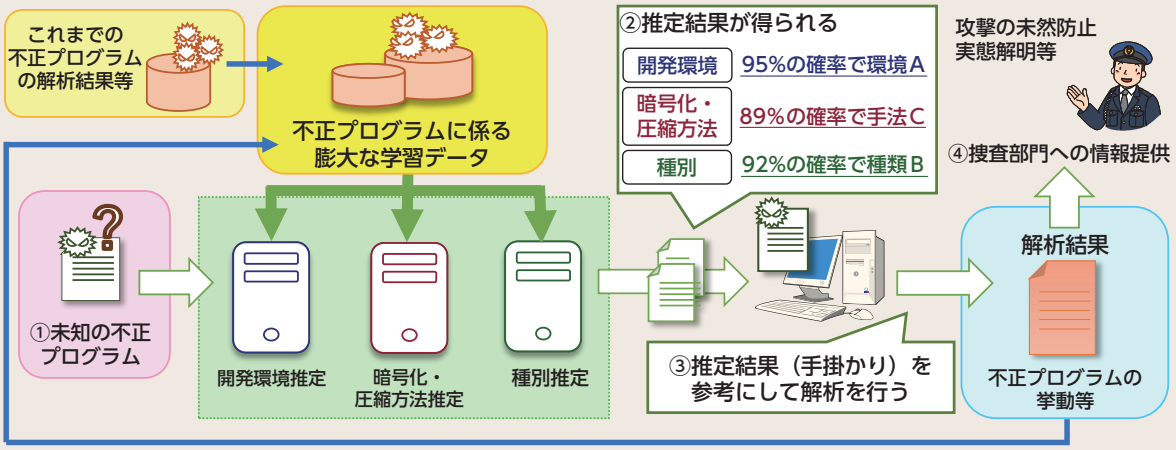

注：TCP/IP通信（インターネット等で用いられるネットワーク上でデータを交換する際の取決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。

## （3）不正プログラムの解析

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

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

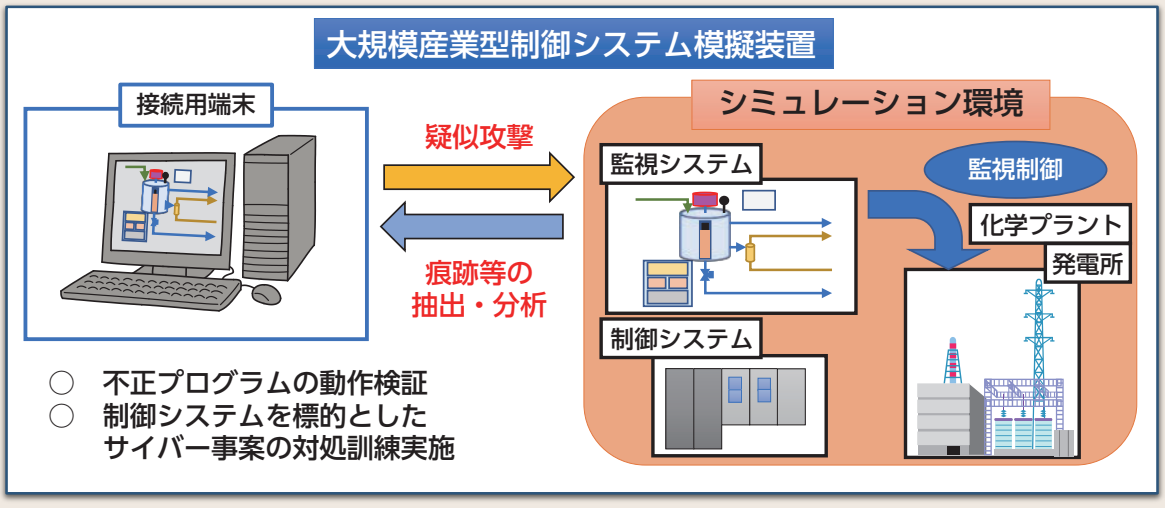
図表３－11　機械学習を活用した不正プログラム解析の高度化・効率化のイメージ




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３－12　大規模産業型制御システム模擬装置の活用例




注：114頁参照

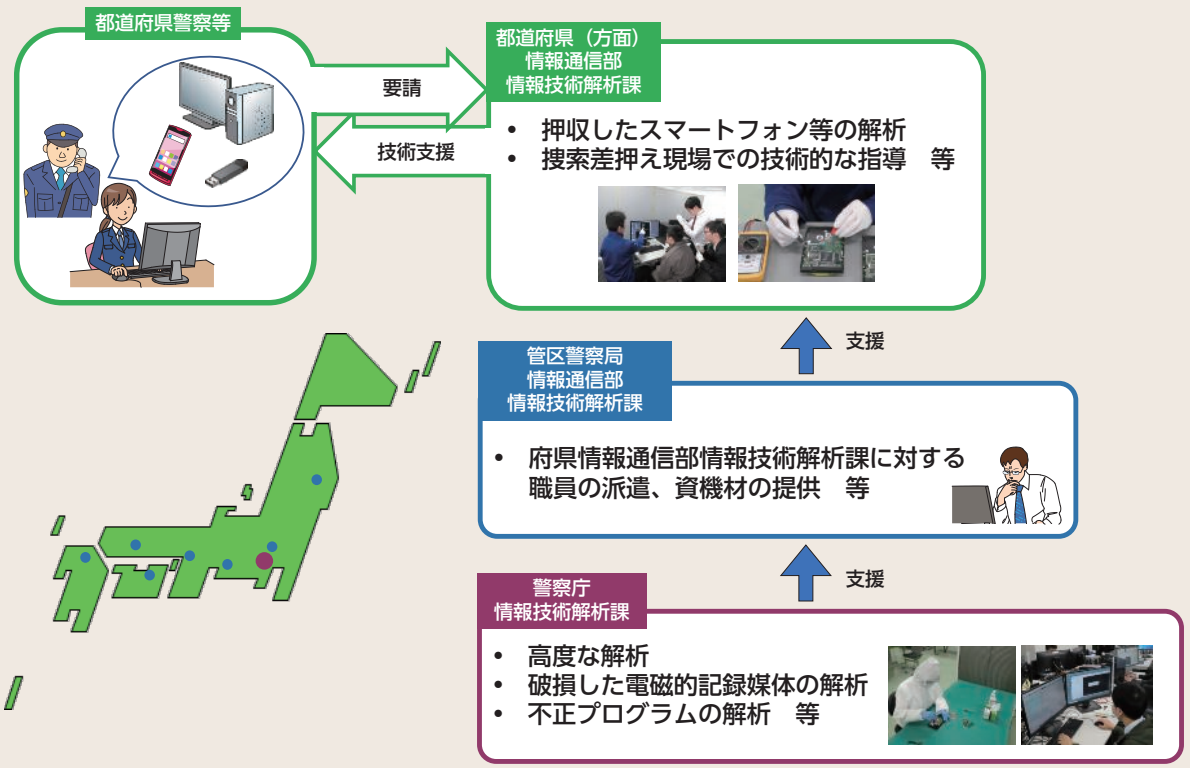
## （４）犯罪の取締りのための技術支援体制

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３－13　犯罪の取締りへの技術支援体制




さらに、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、令和５年５月から運用している。また、最新の資機材の整備を進めるなど、サイバー事案の対処に必要な資機材の整備・高度化を推進している。

## （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：119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

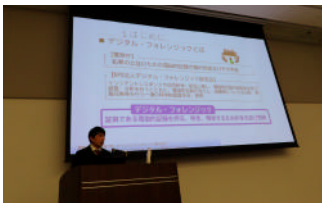
警察大学校サイバーセキュリティ対策研究・研修センター捜査研修室では、都道府県警察の捜査員等を対象とした高度な実践的研修を実施している。平成30年度以降、サイバーレンジ(注)を導入し、仮想環境下において実際の犯行手口や被害状況を再現することにより、最新の手口により行われるサイバー事案に対する実践的な捜査演習や、大規模なサイバー攻撃の被害事案を想定した訓練等を実施している。

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。

図表３－14　サイバー空間における脅威への対処に係る人材育成


### memo　サイバーセキュリティ対策研究・研修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・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。


学会における発表

**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５年度は、自動車に対するサイバー攻撃に備え、学術機関及び民間企業の知見を活用し、自動車におけるセキュリティインシデントの解明に関する共同研究を行った。

### 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・技能の向上を図るとともに、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５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、FBI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４)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５年９月、警察庁サイバー警察局では、英国及びイタリアの捜査機関との間で、サイバー空間をめぐる脅威情勢等について、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ほか、同年11月、外国捜査機関のデジタル・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。また、令和５年10月に我が国で開催されたG7ローマ／リヨン・グループ会合におけるハイテク犯罪サブグループでは、サイバー空間をめぐる脅威情勢や暗号資産を悪用した犯罪の捜査等について議論し、G7各国の捜査機関との緊密な連携を図った。

## （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。

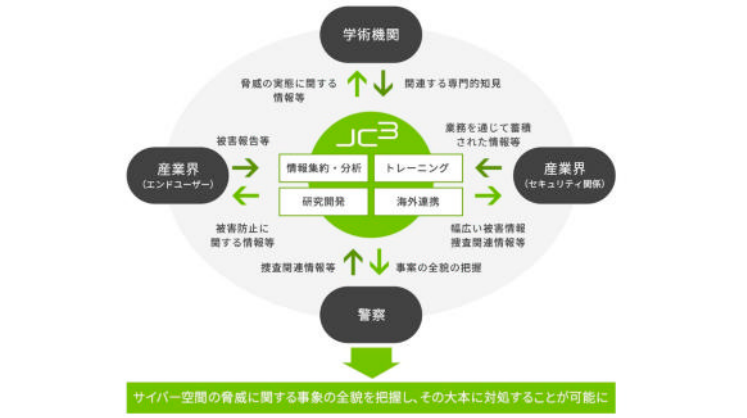
注１：昭和53年（1978年）にボン・サミットを契機に発足したG8テロ専門家会合（G8ローマ・グループ）と平成７年（1995年）にハリファクス・サミットで設置されたG8国際組織犯罪対策上級専門家会合（G8リヨン・グループ）が、平成13年（2001年）の米国における同時多発テロ事件以降合同で開催されているもので、国際組織犯罪対策やテロ対策等について検討している。なお、平成26年（2014年）３月から、G7として実施している。
２：サイバー犯罪に関する条約。サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な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。
３：31頁参照（トピックスⅢ）
４：18頁参照（特集）
５：Forum of Incident Response and Security Teamsの略
６：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)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３－15　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308団体、7,067人（令和５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６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。「ID・パスワードの設定と管理」又は「サポート詐欺対策」をテーマとした広報動画を募集し、警察庁X（旧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授与した。

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

## （3）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

注：116頁参照

### （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）被害の潜在化防止に向けた取組の推進

#### ①　関係機関と連携した通報・相談の推進

サイバー事案対処に当たっては、警察への通報・相談を一層促進し、国民・事業者等からの情報を広範に収集することが求められる一方、被害者自身に対する社会的評価の悪化の懸念等から通報・相談そのものがためらわれる傾向があり、いわゆる「被害の潜在化」が課題となっている。こうした状況を踏まえ、警察庁では、サイバー事案の被害に関する通報・相談の促進に向け、令和５年４月、医療機関との連携について日本医師会との間で、同年６月、クレジットカード番号等の漏えいへの対応として経済産業省との間で、それぞれ覚書を締結した。また、警察では、関係機関・団体、サイバー保険(注１)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(注２)の締結等を通じて、サイバー事案による被害に関する警察への通報・相談を促進している。

#### ②　通報・相談しやすい環境整備

警察庁では、令和４年度に開催した「サイバー事案の被害の潜在化防止に向けた検討会」において取りまとめられた報告書を踏まえ、令和６年３月、インターネットから通報・相談をすることができる一元的な窓口を整備した。また、ウェブサイト等における発信を通じて、サイバー事案に関する警察への通報・相談を促す広報を行うなどの取組を実施している。

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

注１：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
　２：令和５年12月末までに、金融機関や暗号資産交換事業者等、全国で739事業者・団体と本協定を締結している。

# 警察活動の最前線


## 大学との連携による安全・安心なサイバー空間の実現について

福岡県警察本部生活安全部サイバー犯罪対策課特別対処係
古賀　淳

私は、サイバー犯罪に悪用される情報技術に関する調査・研究を行う業務を担当しています。

以前、マルウェアによりフィッシングメールが大量送信される事案を認知し、マルウェアの解析を行うに際し、知見を有する福岡県内の大学に協力を求め、その挙動を解明できたことがありました。

以降、同大学とサイバーセキュリティに関する対処協定を締結し、サイバー犯罪に悪用される情報技術に関する共同研究を進めています。

その成果の一つとして、未把握のフィッシングサイトを検知する仕組みを共同で開発しました。国際論文誌IEEE Accessにおいて成果を公表したほか、検知したフィッシングサイトの閲覧防止措置等の被害防止対策に活用しています。

近年のサイバー犯罪は、最新の情報通信技術を悪用するなど複雑化･巧妙化しており、その対策を講じるには、産･学・官の様々な機関・団体が緊密に連携することが不可欠となっています。

今後も、新たな知識・技術の習得に努めるとともに、関係機関・団体との更なる連携を積極的に進め、安全・安心なサイバー空間の実現に貢献していきたいと思います。

## 日々巧妙化する不正プログラムの解析経験を通して

近畿管区警察局京都府情報通信部情報技術解析課技術支援係
松尾　優希奈


私が所属する情報技術解析課では、京都府警察からの要請を受け、捜索･差押え等における技術的な支援や、押収された電子機器に記録された電磁的記録の抽出・可視化、不正プログラムの解析等を行っています。

これまでの解析経験の中でも、「表面上は不正な動作を行わない不正プログラム」の動作の解析業務が、特に印象に残っています。このプログラムは、自身が動作するパソコンの環境の情報を検知し、その環境によって動作を停止するといった、解析を妨害する耐解析機能を有していました。そこで、このプログラムを段階的に実行しては停止させ、その都度詳細な動作を確認する作業を繰り返し行うことで、解析の妨害を免れる方法を特定し、隠されていた不正な動作を見つけ出すことに成功しました。結果として、このプログラムはパソコンの遠隔操作に悪用できることが分かり、後の捜査に大きく貢献することができました。

不正プログラムは、用いられる技術・手口が日々多様化・巧妙化しており、その解析には、より高度かつ最新の技術が求められます。これからも、解析手法の検討や技術の調査を行いながら自らの技術･知識のアップデートに努め、技術の変化に即した解析を行っていきます。