特集2 サイバー空間の安全の確保

第1節 サイバー空間の脅威をめぐる情勢

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場となっている。近年、サイバー犯罪・サイバー攻撃はその手口を深刻化・巧妙化させつつ多数発生しており、サイバー空間における脅威は極めて深刻な情勢となっている。

1 サイバー犯罪の情勢

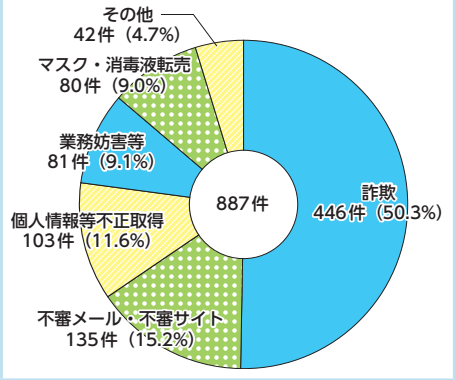
（1）令和２年（2020年）中のサイバー犯罪の情勢

令和２年中の警察によるサイバー犯罪の検挙件数は、過去最多となった。また、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・被害額も、引き続き高水準で推移している。これらの被害の多くは、金融機関を装ったフィッシング(注1)によるものと考えられる。このほか、スマートフォン決済サービスの不正振替事案(注2)や、いわゆる「SMS認証代行」(注3)を用いて不正にアカウントを取得させる事案が確認されている。

（2）新型コロナウイルス感染症に関連するサイバー犯罪の情勢

新型コロナウイルス感染症に関連するサイバー犯罪であると疑われる事案として、令和２年中に都道府県警察から警察庁に報告のあった件数は887件であった。その内訳としては、詐欺が446件で全体の50.3%と最も多く、次いで不審メール等が135件で全体の15.2%を占めており、マスクの販売に関連した詐欺、新型コロナウイルス感染症への感染者情報に関連した虚偽情報の流布等の事例がみられた。

図表特２－１ 新型コロナウイルス感染症に関連するサイバー犯罪であると疑われる事案の報告件数(令和２年)



（3）サイバー犯罪の検挙状況

❶ 不正アクセス禁止法違反

令和２年中の不正アクセス禁止法違反の検挙件数は609件と、前年より207件（25.4%）減少し、検挙人員は230人と、前年より４人（1.7%）減少した。同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、識別符号をフィッシングサイトにより入手したものが172件（29.4%）と最多であった。

また、令和２年中の不正アクセス行為の認知件数(注4)は2,806件であり、不正アクセス後に行われた行為別に内訳をみると、「インターネットバンキングでの不正送金等」が1,847件（65.8%）と最多であった。

CASE

アルバイトの男（32）は、平成31年（2019年）１月から同年２月までの間、元勤務先会社のID・パスワードを無断で使用してインターネット通販サイトへ不正アクセスし、電子マネーのギフト券を不正に注文し窃取した。令和２年２月、同男を不正アクセス禁止法違反（不正アクセス行為）等で逮捕した（京都）。

注１：17頁参照
２：18頁参照
３：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。18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

図表特２－２　検挙した不正アクセス行為の類型別内訳（令和元年及び令和２年）

区分＼年次	令和元	2
合計（件）	787	585
識別符号窃用型 (注)	785	576
フィッシングサイトにより入手	1	172
利用権者からの聞き出し又はのぞき見	20	115
利用権者のパスワードの設定・管理の甘さにつけ込んで入手	310	99
他人から入手	182	78
識別符号を知り得る立場にあった元従業員や知人等による犯行	161	67
スパイウェア等のプログラムを使用して入手	5	3
インターネット上に流出・公開されていた識別符号を入手	3	1
その他	103	41
セキュリティ・ホール攻撃型	2	9

注：アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

図表特２－３　不正アクセス後に行われた行為別内訳（令和元年及び令和２年）

区分＼年次	令和元	2
合計（件）	2,960	2,806
インターネットバンキングでの不正送金等	1,808	1,847
メールの盗み見等の情報の不正入手	329	234
インターネットショッピングでの不正購入	376	172
オンラインゲーム・SNSの不正操作	60	81
知人になりすましての情報発信	30	26
暗号資産交換業者等での不正送信	22	18
ウェブサイトの改ざん・消去	19	10
インターネット・オークションの不正操作	47	6
その他	269	412

（認知件数）

❷ コンピュータ・電磁的記録対象犯罪(注)

令和２年中のコンピュータ・電磁的記録対象犯罪の検挙件数は563件と、前年より127件（29.1％）増加した。

CASE

元会社員の男（35）は、令和２年３月、当時の職場の同僚のメールを盗み見る目的で、同僚の使用する社内パソコンに、キーボード等からの入力情報等を秘密裏に記録する不正プログラムを仕掛け、同僚らが使用するメールアカウント等のID・パスワードを盗み取り、メールアカウント等へ不正アクセスした。同年７月、同男を不正指令電磁的記録供用罪及び不正アクセス禁止法違反（不正アクセス行為）で逮捕した（福井）。

❸ サイバー犯罪の検挙件数の推移

最近５年間のサイバー犯罪の検挙状況は、図表特２－４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２年中の検挙件数は9,875件と、前年より356件（3.7％）増加した。

図表特２－４　サイバー犯罪の検挙件数の推移（平成28年～令和２年）

区分＼年次	平成28	29	30	令和元	2
合計（件）	8,324	9,014	9,040	9,519	9,875
不正アクセス禁止法違反	502	648	564	816	609
コンピュータ・電磁的記録対象犯罪	374	355	349	436	563
児童買春・児童ポルノ禁止法違反	2,002	2,225	2,057	2,281	2,015
詐欺	828	1,084	972	977	1,297
著作権法違反	586	398	691	451	363
上記以外の罪種	4,032	4,304	4,407	4,558	5,028

注：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）インターネットバンキングに係る不正送金事犯の状況

❶ 情勢

令和２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1,734件、被害額は約11億3,300万円と、前年に比べて被害額は大幅に減少したものの、発生件数はやや減少という状況であり、引き続き高水準で推移している。その被害の多くは、金融機関等を装ったフィッシング(注１)によるものと考えられる。

❷ 特徴的な手口

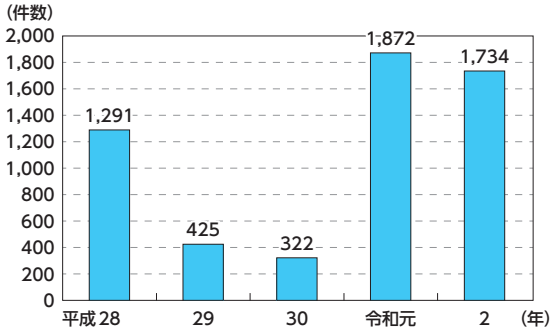
ア　フィッシングサイトへの誘導

金融機関、宅配事業者等を装ったSMS等によって、フィッシングサイトへ誘導し、そこで窃取したID・パスワード等を用いて被害者の銀行口座等から不正に送金するものが多数確認されている。

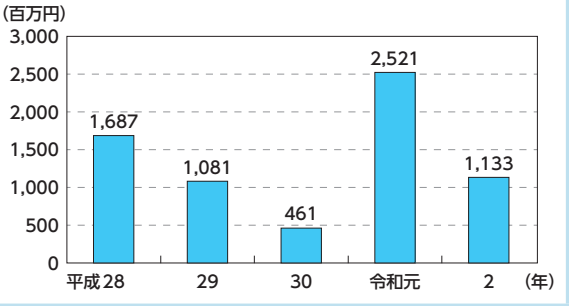
イ　不正プログラムの感染

コンピュータやスマートフォン等に感染した不正プログラム「Emotet」(注２)が、インターネットバンキングの情報窃取等を目的とした別の不正プログラムを、これらの感染した端末にダウンロードし、ID・パスワード等を窃取したと疑われるものが確認されている。

図表特２－５　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28年～令和２年）



図表特２－６　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28年～令和２年）

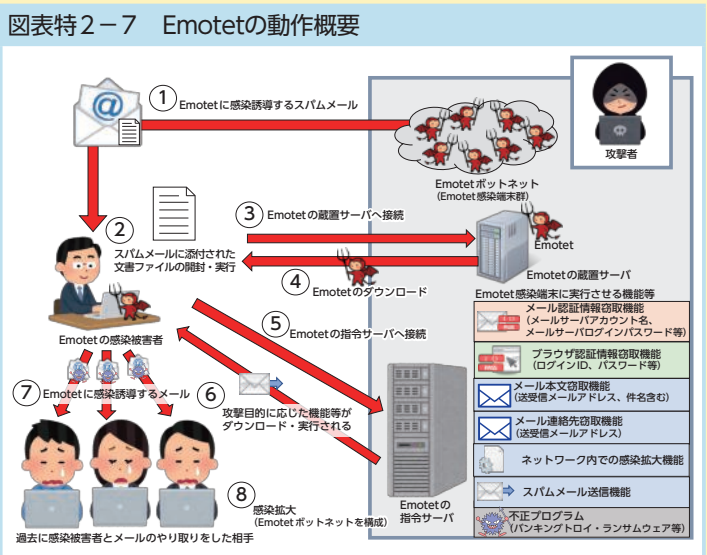


MEMO　特徴的な不正プログラムの脅威

近年、急速に被害が広がっている「Emotet」について、パスワード付きzipファイルを悪用した新たな拡散の手口が認められた。このようなファイルは、ウイルス対策ソフト等による検知をすり抜けてしまうことから、メールの受信前に不正プログラムを駆除できないおそれがあり、こうした手口による被害の拡大が引き続き懸念されている。

また、ランサムウェアによる被害の深刻化・手口の悪質化も世界的に問題となっている。従来は、暗号化したデータを復元する対価として企業等に金銭を要求していたが、最近の事例では、データを窃取した上、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」などと金銭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。さらに、ランサムウェアや二重恐喝の手口そのものが闇サイト上で販売されるなど、こうした悪質な手口が拡散している状況もみられる。

図表特２－７　Emotetの動作概要



注１：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

２：コンピュータの利用者が送受信したメールの宛先、本文等の情報を窃取し、当該情報を基になりすましのメールを作成・送信することで感染を拡大させる機能を持つ不正プログラム

（5）キャッシュレス決済サービスをめぐるサイバー犯罪の状況

キャッシュレス決済(注1)の普及が進む中、スマートフォン決済(注2)サービスと銀行口座の連携時における本人確認方法のぜい弱性を悪用した事例や、サービス利用時の本人認証として広く用いられているSMS認証を不正に代行し、第三者に不正にアカウントを取得させる事例等が発生している。

図表特２－８　スマートフォン決済サービスの不正振替のイメージ

CASE

令和２年９月、ある事業者が提供するスマートフォン決済サービスに関して、同社と業務提携する金融機関に開設された口座情報を不正に入手・連携し、不正な振替（チャージ）を行う事例が確認された。警察では、関係機関・団体等と連携し、被害実態の把握と犯行手口の解明に向け、捜査を実施している（埼玉、警視庁、宮城、福島、岐阜、愛知、三重、滋賀、京都、和歌山、鳥取、岡山）。

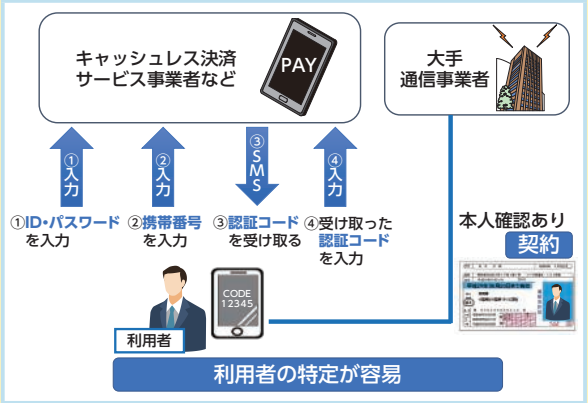
MEMO

SMS認証の不正な代行の実態

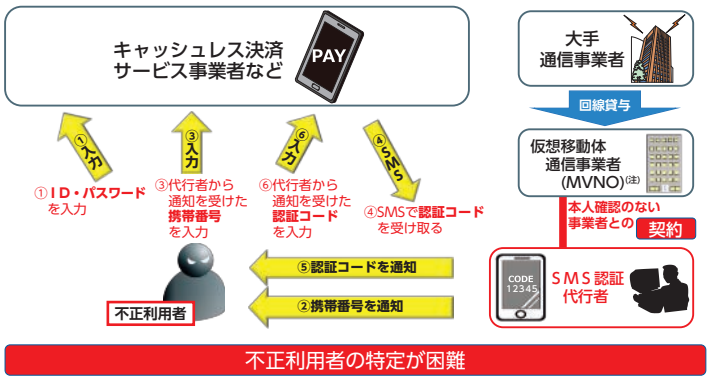
本人認証の実効性を高めるため、サービス利用時等において、SMS認証が広く導入されている一方、SMS認証の不正な代行を行い、第三者に不正にアカウントを取得させる事案が発生している。

埼玉県警察は、スマートフォン決済サービスのSMS認証を代行し、第三者に不正にアカウントを取得させたとして、令和２年６月、無職の女（40）らを私電磁的記録不正作出・同供用の罪で逮捕した。

図表特２－９　SMS認証の仕組み



図表特２－10　SMS認証の不正な代行の概要



注　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

注１：現金を使用せずにお金を支払うこと。クレジットカード、電子マネー、デビットカード、スマートフォンやインターネット等を使った支払がある。
２：スマートフォンを使ってお金を支払うこと。NFC（非接触IC）搭載のスマートフォンを読み取り機にかざす方式や、QRコード®やバーコードを使う方式がある。

2 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は世界的規模で発生しており、令和２年中は、ソフトウェアやシステムのぜい弱性を悪用した攻撃や、標的型メール攻撃を通じて不正プログラムに感染させるなどの事案が多数発生した。国外では、米国の大手ITインフラ管理ソフトウェア会社が提供する製品のぜい弱性を悪用し、同国の政府機関等を標的としたサイバー攻撃の被害等が確認された。国内においても、複数の防衛関連企業、大手電気通信事業者が、外部からの不正アクセスを受け情報が流出した可能性があると公表したほか、大手製造業者からも、従業員が在宅勤務時に社用端末からSNSを利用した際に不正プログラムに感染させられる手口により個人情報等が流出したとの発表が行われた。こうした事案の中には国家の関与が疑われるものもみられるなど、国内外で政府機関、重要インフラ事業者等を標的としたサイバー攻撃が激しさを増している。

また、警察庁が国内で検知した、サイバー空間における探索行為等とみられるアクセスの件数についても増加の一途を辿っており、サイバー攻撃の準備行為とみられる活動が広がりをみせている状況がうかがわれる(注2)。

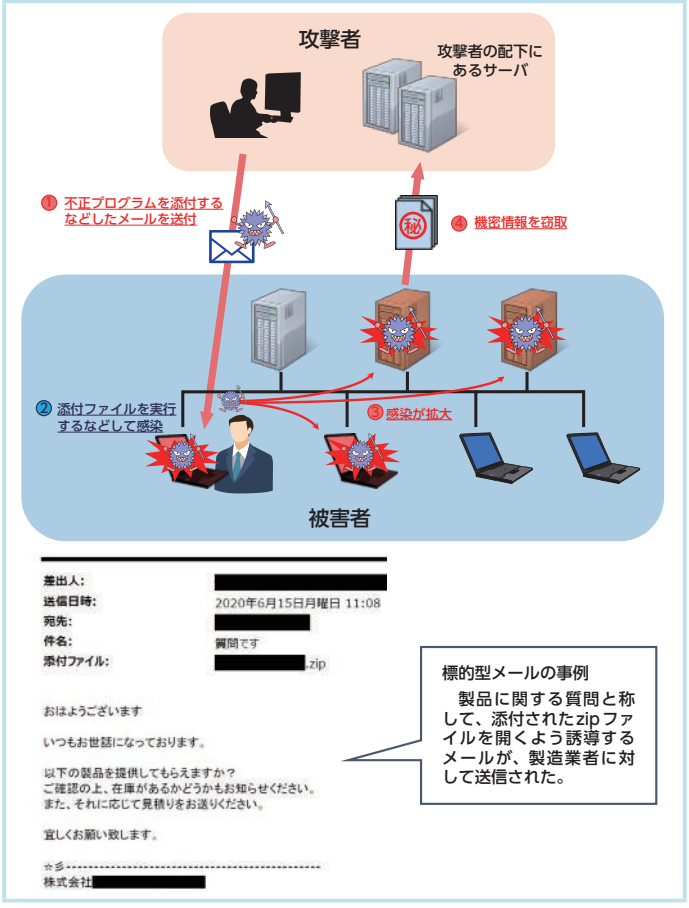
（1）新型コロナウイルス感染症に関連したサイバー攻撃の情勢

新型コロナウイルス感染症に関連した特徴的なサイバー攻撃としては、国内外で医療機関や研究機関等に対する攻撃が確認されている。これらの攻撃は、ワクチンの開発、医療機関・研究機関の研究状況等の把握や、研究成果の窃取等を目的としている可能性が考えられる。新型コロナウイルス感染症の感染拡大やこれに乗じた関連事案による社会への影響は極めて大きく、攻撃者が攻撃対象として新型コロナウイルス感染症に関連した機関等を狙う傾向は今後も継続する可能性がある。

また、我が国でも多数発生し、しばしば情報窃取やサーバ乗っ取り等の更なるサイバー攻撃等の端緒となっている標的型メール攻撃についても、新型コロナウイルス感染症に関連しただまし文句を用いる事例が報告されている。

さらに、新型コロナウイルス感染症の感染拡大防止のため、各事業者等でテレワークの積極的な実施が進められているなど、業務環境が変化していることに伴い、テレワークに用いるオンライン会議システム等のぜい弱性を悪用したとみられる事例も確認されている。一部の事業者においては、テレワークを実施するために十分なセキュリティ上の措置が講じられていないシステムや端末が用いられていたり、テレワーク等によりシステム監視の体制がぜい弱となり社内システムに対するサイバー攻撃被害への対応が遅れたりするなどの状況が生じているものとみられる。

図表特２－11　標的型メール攻撃による情報窃取の例



注１：重要インフラ（「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月サイバーセキュリティ戦略本部決定、令和２年１月改定）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

２：29頁参照

（2）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。

（3）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、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 警察のアトリビューションにより国家レベルの関与を明らかにしたサイバー攻撃事案

1　レンタルサーバ不正契約事件被疑者の検挙

中国共産党員の男（30代）は、平成28年９月から平成29年４月までの間、合計５回にわたり、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行った。警視庁公安部は、令和３年４月、同男を私電磁的記録不正作出罪・同供用罪で検挙した。

2　一連のサイバー攻撃に関与した背景組織の特定

本事件の捜査を通じ、警察では、同男が不正に契約したレンタルサーバが宇宙航空研究開発機構（JAXA）等に対するサイバー攻撃に悪用されたことを把握するとともに、同攻撃の実態解明の過程で、同一の攻撃者が関与している可能性が高いサイバー攻撃が約200の国内企業等に対して実行されたことを把握した。

本事件被疑者・関係者の供述をはじめ数多くの証拠を積み上げた結果、これらのサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行されたものであり、このTickの背景組織として山東省青島市を拠点とする中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った。

3　被害企業等に対する注意喚起

警察では、これらの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た(注1)。

また、一連のサイバー攻撃は、日本製ソフトウェアのぜい弱性が悪用されたゼロデイ攻撃(注2)であったことから、このソフトウェアの開発企業と協力し、ぜい弱性の存在と有効な対応策について広く周知した。

注１：令和３年４月時点、これら被害企業等において情報流出等の被害は確認されていない。
２：OSやアプリケーションのぜい弱性に対応するパッチがソフトウェアの開発企業等から提供される前に、そのぜい弱性を悪用して行われる攻撃の総称

第2節 サイバー空間の脅威への対処

1 サイバー犯罪への対策

（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、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)を例年行っている。

（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、手口が巧妙化している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、不正プログラムへの感染が疑われる端末の解析等、早期の実態解明と必要な取締りを推進している。令和２年（2020年）中は、不正送金事犯に関連して、他人に利用させる意図を隠して口座を開設した者、口座を譲渡した者、不正に送金された資金を引き出した者等合計157人を検挙した。

また、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の被害防止のため、関係機関と連携した効果的な広報啓発、ウイルス対策ソフト事業者等に対するフィッシングサイト情報の迅速な共有等を行っている。さらに、金融機関等に対し、モニタリング(注3)の強化、ワンタイムパスワード(注4)及び二経路認証(注5)の利用、本人確認の徹底等の被害防止対策の強化を要請している。

（3）キャッシュレス決済サービスをめぐるサイバー犯罪への対策

警察庁では、令和２年10月、身に覚えのないスマートフォン決済サービスを通じて銀行口座から不正に出金される手口に関し、金融庁等と連携し、警察庁ウェブサイト等で被害防止のための注意喚起を実施した。

また、令和３年３月、金融機関及びスマートフォン決済サービス提供事業者に対し、犯罪捜査の過程で判明した手口等について情報提供するとともに、それらを踏まえた被害防止対策の強化について要請した。

CASE

ベトナム国籍の男（23）は、令和２年３月、他人の口座情報を不正に利用し、自身が使用するスマートフォン決済サービスのアカウントに紐付く振替口座として登録し、同口座から合計２万8,000円を不正に振替（チャージ）した。同年11月、同男を電子計算機使用詐欺罪で逮捕した（岡山）。

注１：令和２年の調査は、同年８月26日から９月25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、2,928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、622件の回答を得た。

２：令和２年の調査は、同年８月26日から９月25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、1,822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、204件の回答を得た。

３：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

４：インターネットバンキング等における認証用パスワードであって、認証のたびにそれを構成する文字列が変わるもの。これを導入することにより、ID・パスワード等を盗まれても次回の利用時に使用できないことになる。

５：インターネットバンキング等において、コンピュータ（第一経路）で振り込み等の取引データを作成した後、スマートフォン等（第二経路）で承認を行うことで取引を成立させる認証方式

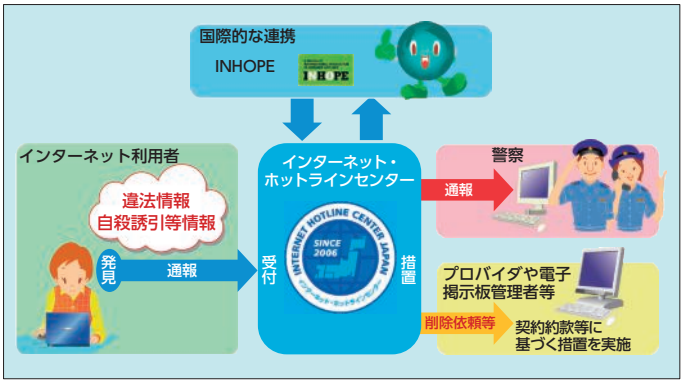
（4）インターネット上の違法情報・有害情報対策

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。

❶ 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２年中、IHCでは2,161件の違法情報の削除依頼を行い、そのうち1,787件（82.7%）が削除された。また、4,218件の自殺誘引等情報の削除依頼を行い、そのうち1,733件（41.1%）が削除された。

図表特２－12　インターネット・ホットラインセンターにおける取組



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。

❷ 効果的な違法情報等の取締り

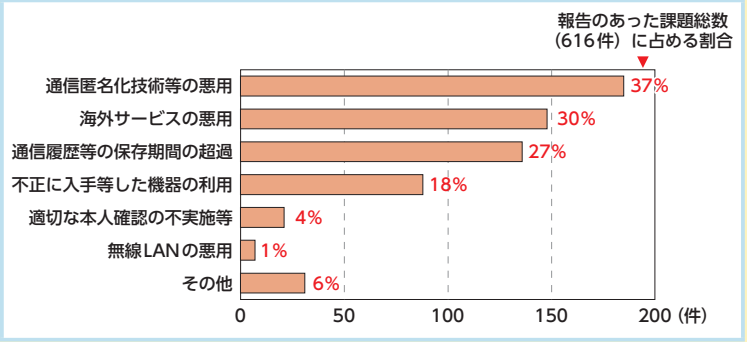
警察では、サイバーパトロール等により違法情報・有害情報の把握に努めるとともに、効率的な違法情報の取締り及び有害情報を端緒とした取締りを推進している。

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ている。

MEMO　サイバー犯罪捜査における犯人の事後追跡上の課題

サイバー犯罪捜査における犯人の事後追跡可能性について、都道府県警察本部のサイバー犯罪対策担当課に対し、令和元年中に認知したサイバー犯罪事件に関し、犯人の事後追跡上の課題となったものを調査したところ(注3)、プロキシ等の「通信匿名化技術等の悪用」が最も多く、次いで、「海外サービスの悪用」、捜査の時点で通信履歴（ログ）が保存されていないなどの「通信履歴等の保存期間の超過」が多かった。

図表特２－13　サイバー犯罪捜査における事後追跡上の課題



こうした課題に対処するため、警察では、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。

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：調査は、都道府県警察本部のサイバー犯罪対策課等において管理している、令和元年中に認知したサイバー犯罪事件（495件）を対象とした。捜査に支障を来す要因となった事後追跡上の課題について選択肢（複数回答可）を設けて調査し、616件の報告があった。

（5）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262団体、8,161人（令和２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。

（6）民間事業者、外国捜査機関等と連携した被害防止対策

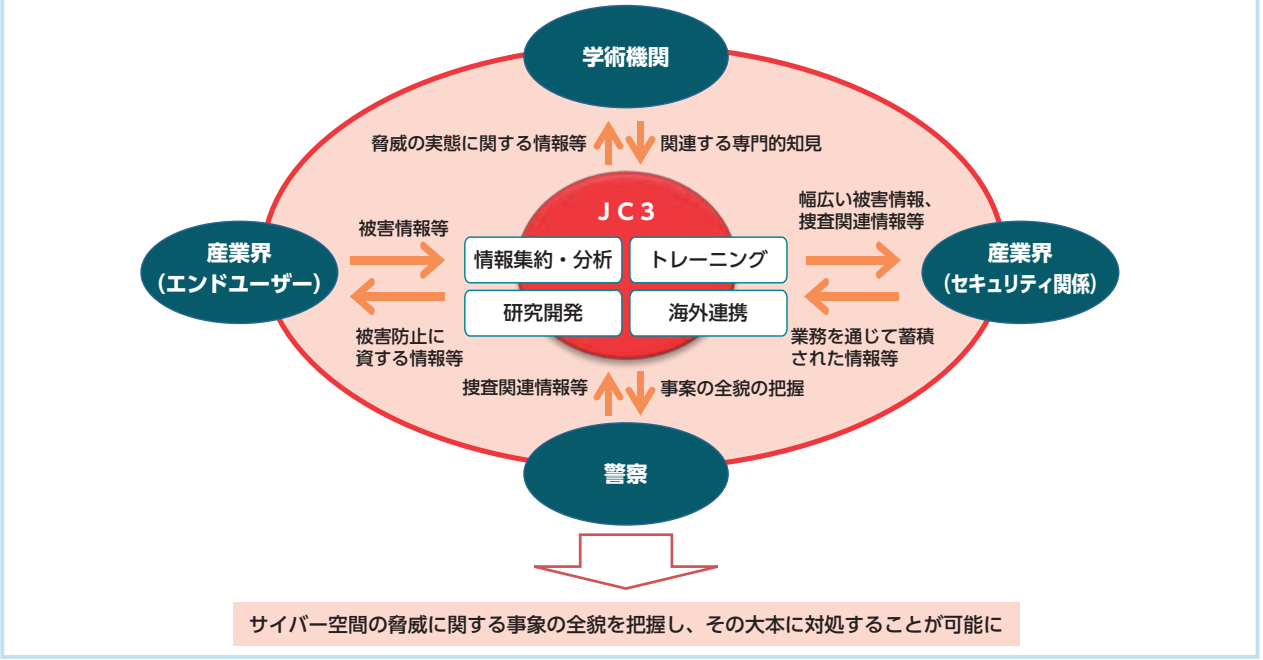
サイバー犯罪における手口が悪質・巧妙化する中、警察では、民間事業者、外国捜査機関等と連携し、都道府県警察が相談、犯罪捜査の過程等で把握した不正プログラムに関する情報、海外の偽サイト等(注１)に関する情報をウイルス対策ソフト事業者等に提供するなど、積極的な被害防止対策を推進している。

また、サイバー犯罪の潜在化の防止、捜査活動の効率化及び再発防止を図るため、警察では、民間事業者等との共同対処協定の締結を推進している。事業者と信頼関係を構築し、サイバー犯罪の警察への通報の促進等を図るため、令和２年12月末までに、金融機関や暗号資産交換業者等、全国で581事業者・団体と本協定を締結している。

（7）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一般財団法人日本サイバー犯罪対策センター（ＪＣ３(注２)）においては、産学官の情報や知見を集約・分析し、その結果等を還元することで、脅威の大本を特定し、これを軽減及び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。

図表特２－14　ＪＣ３の概要



注１：海外のサーバに開設された、実在する企業のウェブサイトを装ったウェブサイトや、インターネットショッピングを利用した詐欺や偽ブランド品の販売を目的とするウェブサイト等
２：Japan Cybercrime Control Centerの略

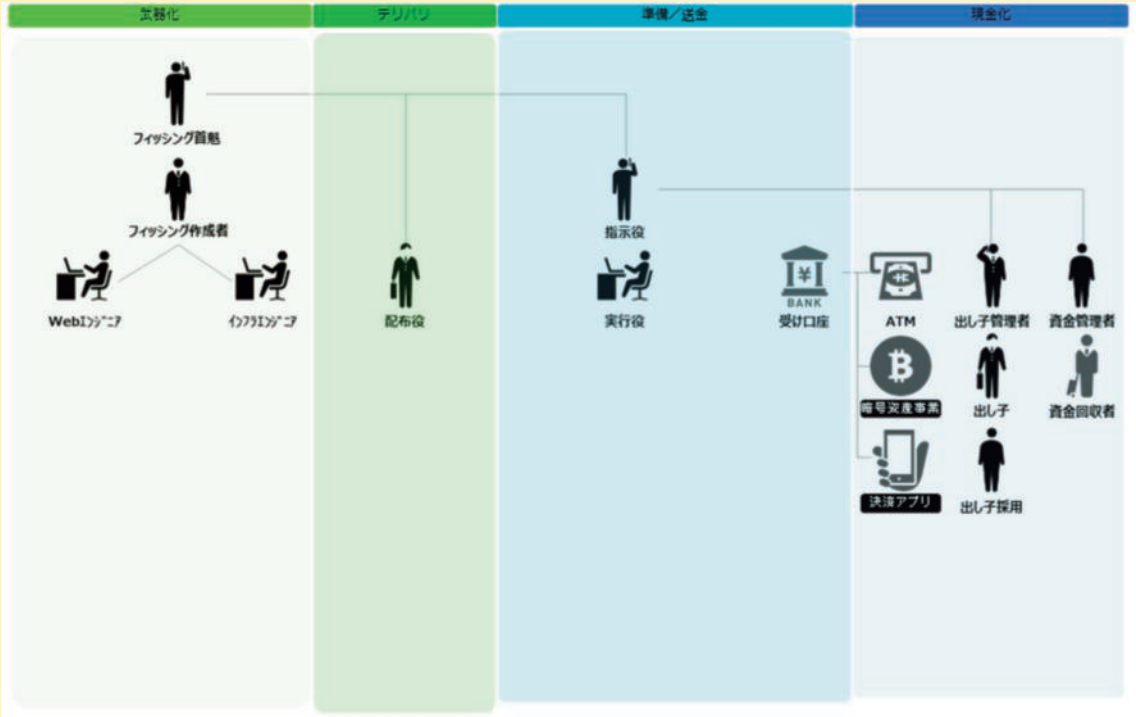
CASE

サイバー犯罪の捜査において押収されたコンピュータから、ID・パスワードのリストを用いて、様々なオンラインサービスへのログインを試みるリスト型攻撃のツールが多数発見された。警察では、ＪＣ３と連携して当該ツールを解析し、その仕組みや攻撃の手口を解明するとともに、企業等に対し情報提供を行い、犯罪被害防止対策の推進を要請した。また、ＪＣ３では、当該解析結果等に基づき、ウェブサイトにおいて、リスト型攻撃の手口やパスワードの使いまわしの危険性について注意喚起を行った（千葉・茨城）。

中国語圏で利用されているとみられるリスト型攻撃ツールの画面

MEMO ＪＣ３と連携した分析

警察庁では、ＪＣ３と連携して、犯行手口等から犯行グループを分類し、各犯行グループの詳細な分析により、犯罪の実態解明を進めている。例えば、インターネットバンキングに係る不正送金事犯については、ID・パスワード等を不正に取得するフィッシングサイトを作成する者、不正アクセスにより送金を行う者、不正に送金された資金を引き出す者等といった犯行の分業化等が行われており、こうした犯罪の実態や犯行手口の解明に向け分析を進めている。こうした分析結果は、都道府県警察や連携する民間企業へ情報提供され、都道府県警察における捜査活動や産業界における被害防止対策の推進に貢献している。



犯行グループの構造のイメージ（ＪＣ３提供）

2 サイバー攻撃への対策

（1）警察におけるサイバー攻撃対策

警察庁及び各都道府県警察では、サイバー攻撃対策を担当する組織を設置しているほか、関係機関等と連携し、サイバー攻撃の実態解明や被害の未然防止等を推進している。

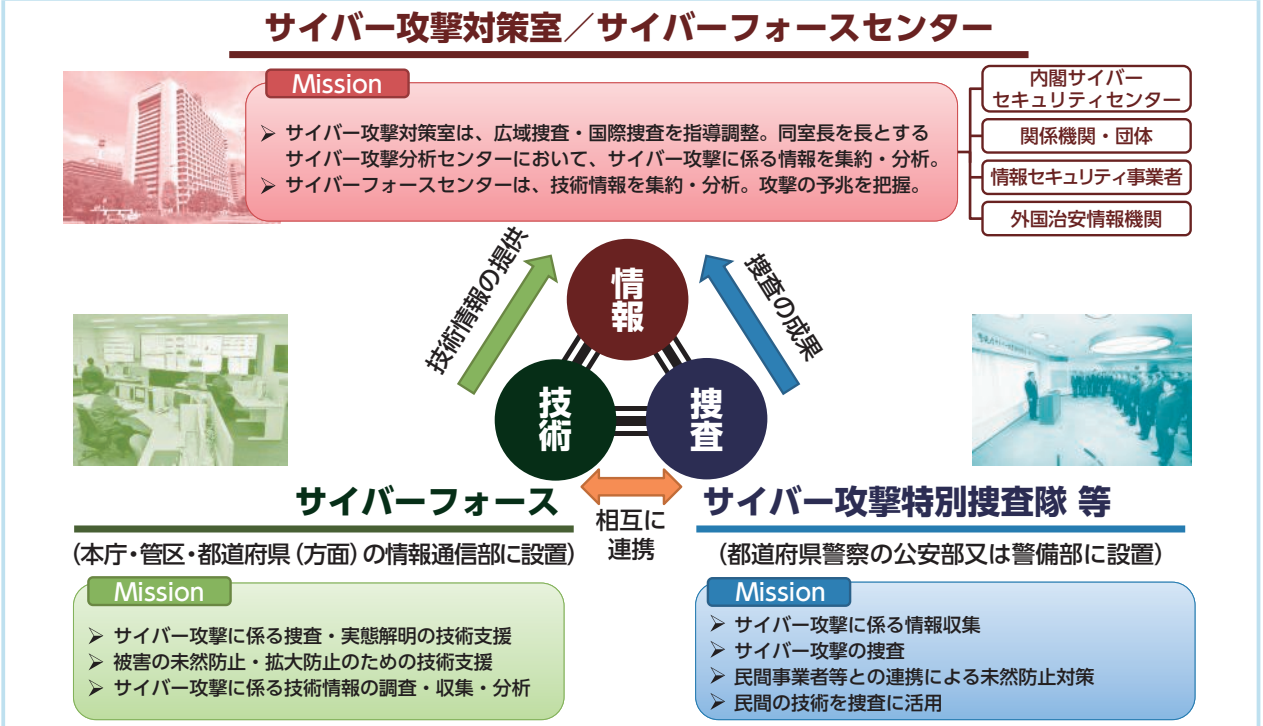
❶ 推進体制

警察庁では、サイバー攻撃対策室が、都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換に当たるとともに、サイバー攻撃対策室長を長とするサイバー攻撃分析センターにおいて、サイバー攻撃に関する情報の集約・分析を実施している。

また、警察庁及び全国の情報通信部(注1)には、都道府県警察のサイバー攻撃対策部門に対する技術支援を行うサイバーフォースを設置している(注2)。

さらに、政府機関、重要インフラ事業者、先端技術を有する事業者等が多く所在する14都道府県警察には、サイバー攻撃特別捜査隊を設置している。サイバー攻撃特別捜査隊は、サイバー攻撃の捜査に関する専門的な知識、技能及び経験をいかし、設置された都道府県におけるサイバー攻撃対策のみならず、他の都道府県警察に対して技能・技術・体制面の支援を行うことにより、サイバー攻撃事案に対する警察全体の捜査能力の向上を図っている。このほか、情報収集活動の推進や民間事業者等との協力関係の確立においても、中核的な役割を果たしている。

図表特2－15　サイバー攻撃対策の推進体制



❷ 実態解明の推進

警察では、違法行為に対する捜査を推進するとともに、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いる。また外国治安情報機関との情報交換を行うとともに、ICPO(注3)を通じるなどして、外国捜査機関との間で国際捜査協力を積極的に推進している。

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。組織図については65頁参照（第1章）
2：サイバーフォースの活動等については27頁参照
3：International Criminal Police Organization（国際刑事警察機構）の略

（2）官民連携の推進

❶ サイバーテロ対策協議会

警察では、各都道府県警察、サイバー攻撃の標的となるおそれのある重要インフラ事業者等とで構成するサイバーテロ対策協議会を全ての都道府県に設置し、サイバー攻撃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、参加事業者間の意見交換や情報共有を行っているほか、サイバー攻撃の発生を想定した共同対処訓練等を行っている。

CASE

鳥取県警察では、令和２年10月、「鳥取県サイバーテロ対策協議会第10回総会」を開催した。同協議会では、事例紹介、講師による講演等を通してセキュリティ意識の向上を図った。

協議会会長による挨拶


別会場からの参加の様子

❷ 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攻撃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。

❸ 不正プログラム対策協議会

警察では、警察庁とウイルス対策ソフト提供事業者等とで構成す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。

❹ 不正通信防止協議会

警察では、警察庁と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とで構成す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。

❺ 高度な研究開発を行う大学に対するサイバー攻撃への対策の推進

近年、高度な研究開発を行う大学に対するサイバー攻撃が発生していることから、警察では、このようなサイバー攻撃に関する情報収集・分析を強化するとともに、大学と連携し、サイバー攻撃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、サイバー攻撃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に対するサイバー攻撃への対処能力の強化を図っている。

3 技術支援と解析能力の向上

（1）サイバー攻撃対策におけるサイバーフォースの役割

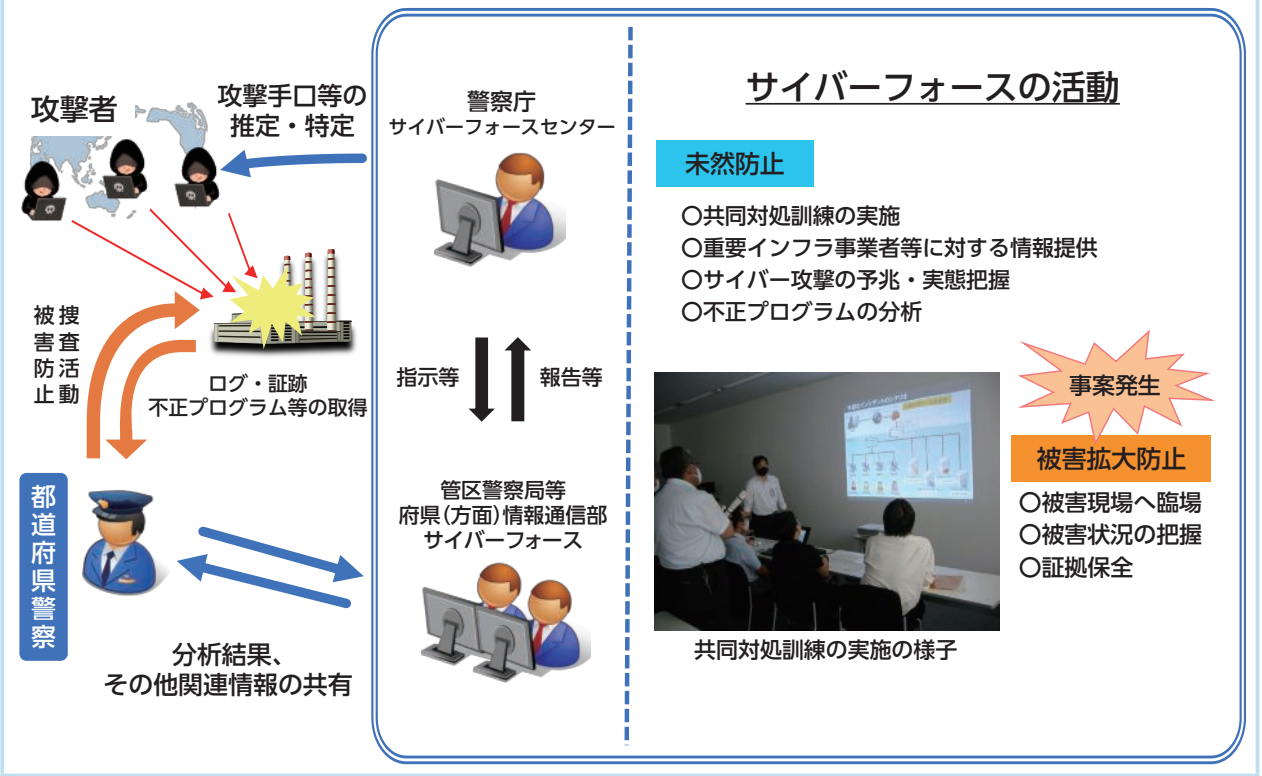
警察では、深刻化するサイバー攻撃に対応するため、攻撃の対象となったサイバーセキュリティ上のぜい弱性に関する情報や標的型メール攻撃等の犯行手口に関する情報等を捜査活動や事業者との情報交換を通じて把握・分析し、被害の未然防止や拡大防止に努めている。

近年のサイバー攻撃は、国家を背景とす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、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、警察庁及び全国の情報通信部(注1)に都道府県警察のサイバー攻撃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、サイバー攻撃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、サイバー攻撃事案発生時には、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、サイバー攻撃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攻撃の予兆・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。

図表特2－16　サイバーフォースの役割と活動

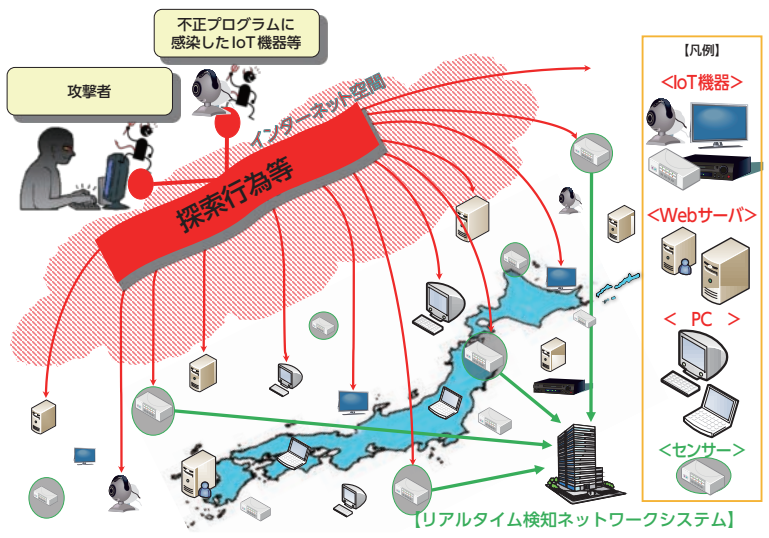


注1：25頁参照
　2：26頁参照

（2）サイバー攻撃の予兆・実態等の把握

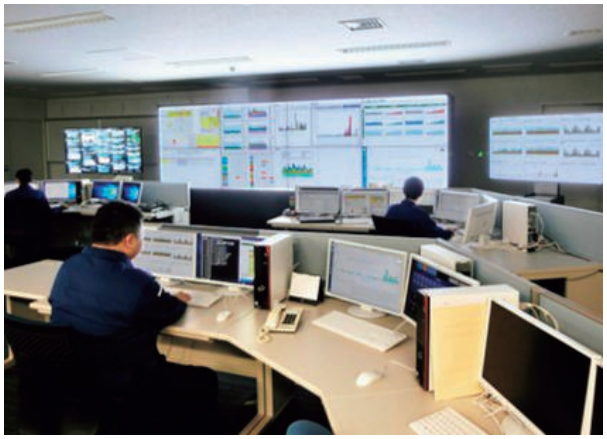
❶ リアルタイム検知ネットワークシステムの運用

図表特２－17　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、サイバー攻撃の予兆・実態等を把握することを目的に、リアルタイム検知ネットワークシステムを平成14年から運用している。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が、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やそれらを悪用した攻撃、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。

図表特2－18　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、平成16年に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攻撃被害観測機能を、平成22年に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を、それぞれ開発・導入している。また、平成31年１月には、本システムを更新し、インターネット上の事象の変化等に応じた観測機能を強化した。

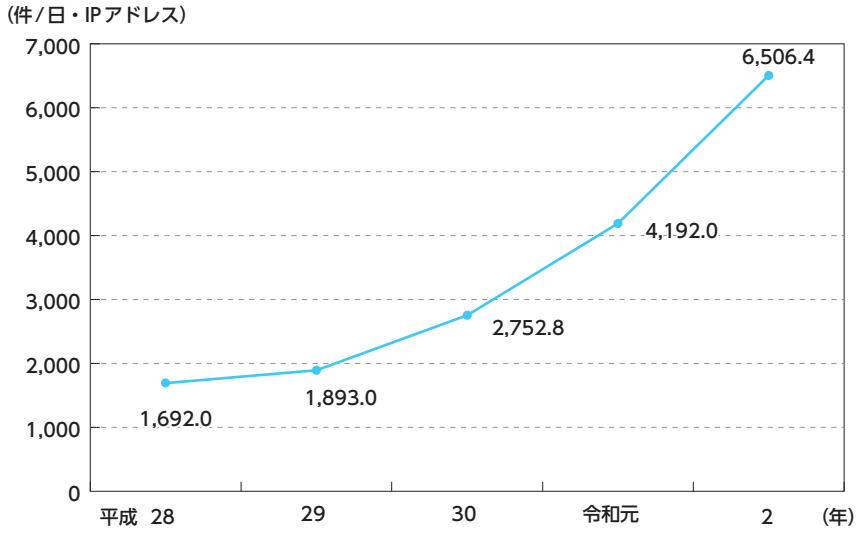
サイバーフォースセンターでは、本システムから得られる情報を用いて24時間体制でサイバー攻撃の予兆・実態等を把握し、分析結果をインターネット観測結果として重要インフラ事業者等へ情報提供しているほか、インターネット利用者がサイバー攻撃の危険性を正しく認識し、適切な対策を自主的に講じられるよう、警察庁ウェブサイト「@police」(注3)において広く一般に公開している。

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/)

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

令和２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おいては、一つのセンサー当たり約13.3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年々増加傾向にあり、サイバー攻撃情勢が深刻化していることがうかがわれる。

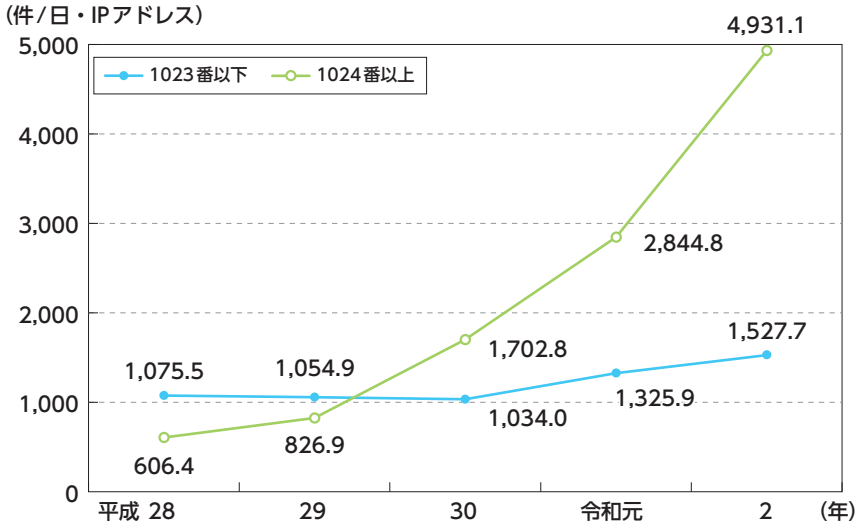
図表特２－19　リアルタイム検知ネットワークシステムにおいて検知した１つのセンサーに対する１日当たりの不審なアクセス件数の推移（平成28年～令和２年）



検知した不審なアクセスの宛先ポート番号(注１)に着目すると、1024番以上のポートへのアクセス件数が増加し続けており、アクセス全体の総数が増加している大きな要因となっている。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２年上半期には、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。

図表特２－20　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28年～令和２年）



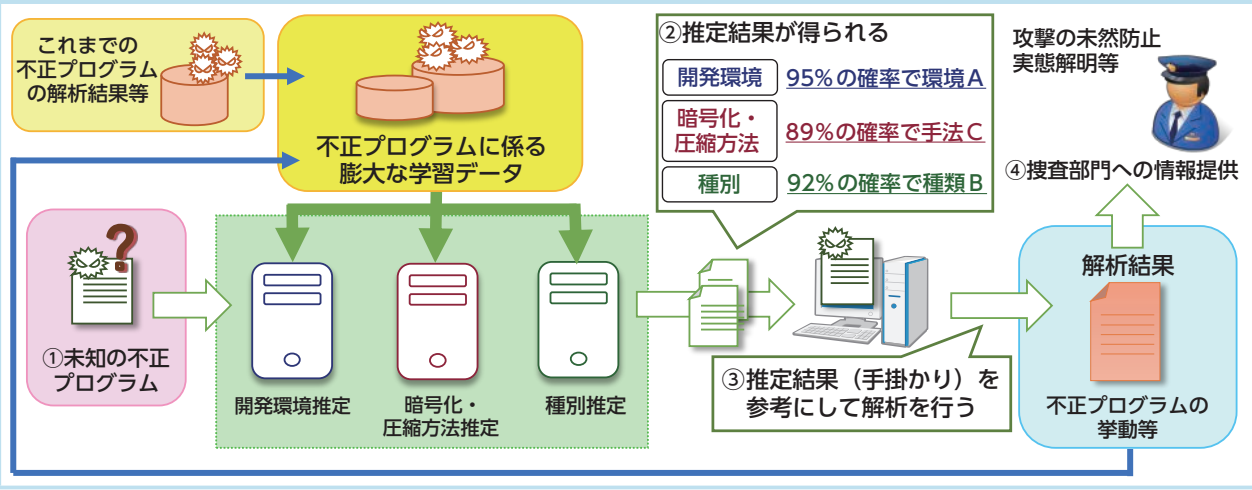
注１：TCP/IP通信（インターネット等で用いられているネットワーク上でデータを交換する際の取り決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。
２：IoT機器等に感染しDoS攻撃等を行う不正プログラムの一種

（3）サイバー攻撃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攻撃事案が発生しているほか、発電所や化学プラント等の重要インフラの制御・監視を行う産業制御システム等を標的として身代金を要求する不正プログラムを用いた事案等が発生している。

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。

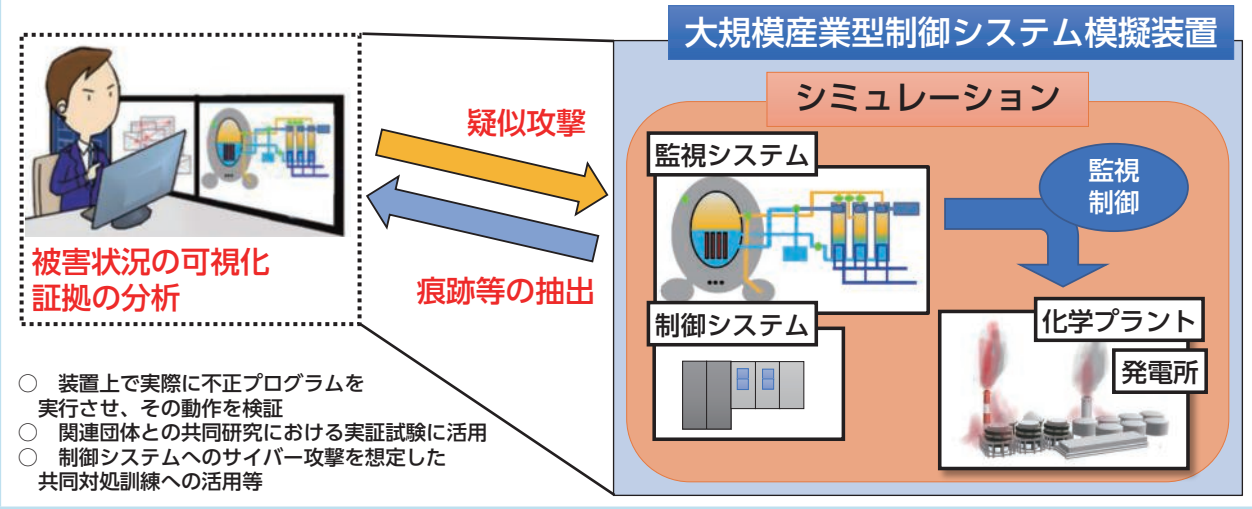
図表特２－21　機械学習を活用した不正プログラム解析の高度化･効率化のイメージ



特に、産業制御システムに対するサイバー攻撃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痕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、産業制御システムのぜい弱性の検証を行うほか、当該装置を活用して関係機関・団体等とのサイバー攻撃の未然防止・被害拡大防止対策の共同研究や産業制御システムへのサイバー攻撃を想定した共同対処訓練等を実施している。

図表特２－22　大規模産業型制御システム模擬装置の活用例



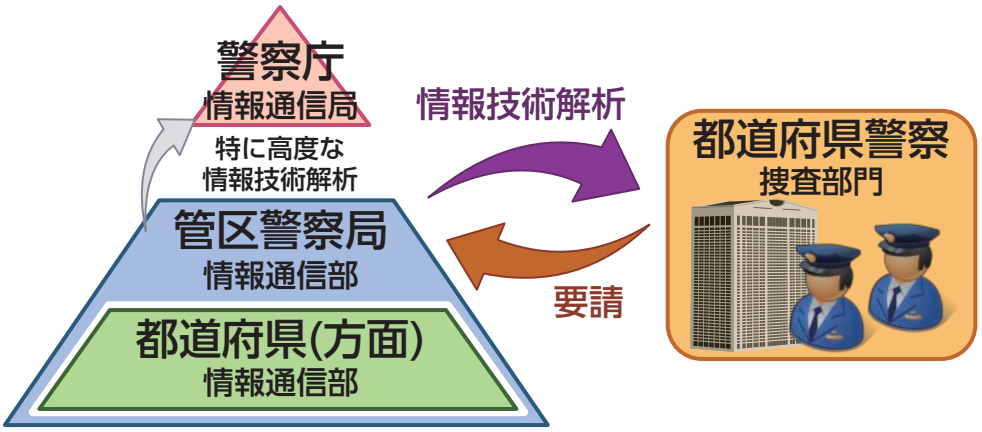
（4）サイバー犯罪の取締りへの技術支援

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て、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。

図表特２－23　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犯罪・サイバー攻撃が多発する中、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。

そのため、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。

スマートフォン解析の様子

注：25頁参照

4 国際連携の推進

（1）国際捜査共助

国境を越えて行われるサイバー犯罪・サイバー攻撃について、国内における捜査で犯人を特定できない場合は、外国捜査機関の協力を求める必要がある。

警察庁では、サイバー犯罪条約(注1)、刑事共助条約（協定）(注2)、ICPO、サイバー犯罪に関する24時間コンタクトポイント(注3)等の国際捜査共助の枠組みを活用し、国境を越えて行われるサイバー犯罪・サイバー攻撃に対処している。

（2）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２年中は、サイバー犯罪条約の締約国等が参加するサイバー犯罪条約委員会会合、ICPO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、サイバー空間の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。

（3）国際協力の推進

警察庁では、サイバー空間の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）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、サイバー空間の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6)。

令和元年度JICA課題別研修
（サイバー犯罪対処能力向上）

注１：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。
２：227頁参照（第６章）
３：平成９年（1997年）12月のＧ８司法内務閣僚会合で策定された「ハイテク犯罪と闘うための原則と行動計画」等に基づき設置されたもので、令和２年10月現在、88の国・地域に設置されている。
４：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。
５：Forum of Incident Response and Security Teamsの略
６：令和２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 警察におけるサイバーセキュリティ戦略及び人材育成の推進

（1）警察におけるサイバーセキュリティ戦略

社会情勢等の変化に的確に対応しつつ、サイバー空間の脅威に先制的かつ能動的に対処するため、警察では、「警察におけるサイバーセキュリティ戦略」（平成27年９月策定、平成30年９月改定）に基づき、警察における組織基盤の更なる強化を図るなど、警察組織の総合力を発揮した効果的な対策を推進している。

（2）サイバー空間の脅威への対処に係る人材育成方針

都道府県警察では、サイバー犯罪・サイバー攻撃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、警察本部等にこうした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、その知識や技能をいかして活躍している。

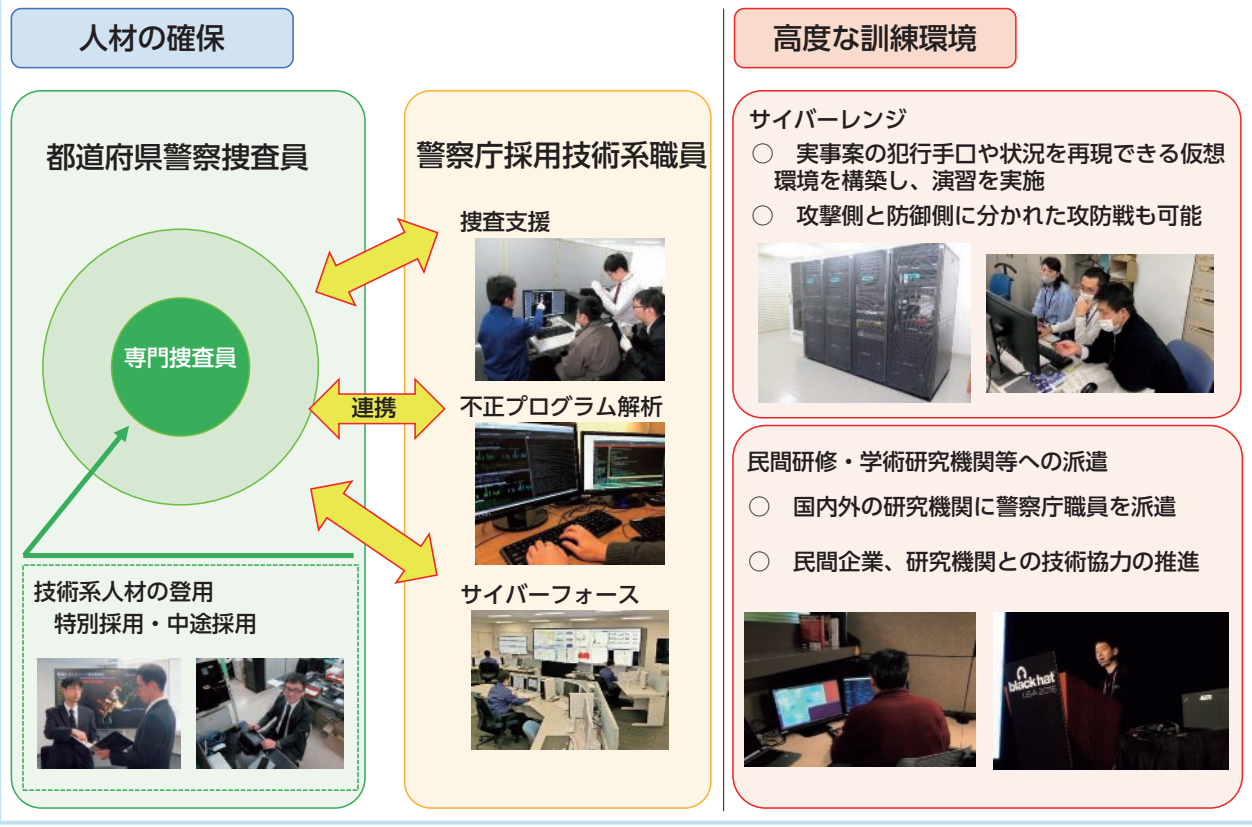
これらサイバー空間の脅威への対処のための人的基盤を強化するため、警察では、「サイバー空間の脅威への対処に係る人材育成方針」（平成27年12月策定、平成31年４月改定）に基づき、職員の採用・登用、教育・研修、キャリアパスの管理等を部門横断的かつ体系的に実施している。

（3）捜査員等に対する実践的研修

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。

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。

図表特２－24　サイバー空間の脅威への対処に係る人材育成



注：サイバー攻撃等に対する実践的な訓練を行うためのサイバー演習環境

MEMO サイバー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

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サイバー犯罪等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。

①電子機器の解析に関する研究

事件関係者が使用したスマートフォン等の電子機器には、犯罪捜査に有用な情報が記録されている可能性があることから、スマートフォン等の電子機器の解析に関する研究を行っている。令和２年度は、スマートフォン等からのデータ抽出及び抽出したデータの可視化・可読化手法に関する研究を行った。

電子機器の解析に関する研究状況

②自動運転システムの解析に関する研究

特定条件の範囲内で、人ではなくシステムが自動車の運転操作を行うSAEレベル３(注)の自動運転システムを備えた自動車が令和３年３月に発売された。自動運転システム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、令和元年度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２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開始した。

自動運転システムの解析に関する研究状況

MEMO 国内外研究機関への職員派遣

警察では、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、最新の技術情報を継続的に収集しているほか、電子機器の解析やサイバー犯罪・サイバー攻撃への対処に資する最先端の研究を行っている国内外の研究機関に職員を派遣し、不正プログラムの解析手法や、今後犯罪に悪用される可能性のある、ネットワークを利用したサービス等に関する調査を実施し、解析能力の向上に努めている。

国内研究機関における調査の様子

注：182頁参照（第４章）

第3節 今後の取組

近年、新型コロナウイルス感染症に関連するサイバー犯罪の発生や「Emotet」(注)のような感染力の強い特徴的な不正プログラムの出現など、日々新たな手口のサイバー犯罪が登場しているほか、国内防衛関連企業等から機密情報が流出した可能性のあるサイバー攻撃事案が発生するなど、サイバー空間における脅威は極めて深刻な情勢となっている。

その一方で、サイバー空間は国民の日常生活の一部として重要な社会経済活動が営まれる公共空間へと変貌を遂げており、サイバー空間の安全安心の確保は、国民にとって安全安心なデジタル社会の実現のためにこれまで以上に重要かつ必要不可欠なものとなると考えられる。

警察では、これまでもサイバー犯罪・サイバー攻撃の取締り、不正プログラムの解析をはじめとした情報解析技術の活用、外国捜査機関等との連携等、サイバー空間の脅威への対策を講じてきたところである。今後、デジタル社会が進展し、サイバー空間の役割が拡大していく中、国民の安全安心な暮らしを守る責務を担う警察は、サイバー空間の安全安心の確保に向けた取組においても、これまで以上に中心的な役割を果たすことが求められている。

MEMO 令和２年度サイバーセキュリティ政策会議の開催

警察庁においては、「サイバーセキュリティ政策会議」が令和２年（2020年）10月から令和３年３月にかけて5回開催された。同会議では、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」をテーマとして、新型コロナウイルス感染症の感染拡大やデジタル化の進展等により大きく変化するサイバー空間の脅威について、幅広い分野の有識者とともに幅広い議論が行われ、同月、報告書が取りまとめられた。

報告書では、スマートフォン決済サービスの不正振替のように、令和２年中に深刻な被害を生じさせた新たな脅威がサイバー空間で顕在化している点や、以前から確認されているフィッシングや不正プログラムによる攻撃の犯行手口等の悪質化、国家の関与が疑われるサイバー攻撃の被害の深刻化等が生じている点等、サイバー空間の脅威が極めて深刻な情勢にあることが共有されるとともに、今後、サイバー空間は、全国民が参画し、重要な社会経済活動が営まれる、これまで以上に重要かつ公共性の高い場へと変貌を遂げていくとの認識が示された。

また、サイバー空間の新たな脅威に対処していくための新たな基本理念として、「公共空間としての安全性確保」が提示され、サイバー空間においても、実空間と同水準の安全性の実現、すなわち、誰もが安心して参画できるサイバー空間の実現を目指していくべきであるとの提言がなされ、そのための課題と今後の取組として、以下３点の方向性が示された。

ア　犯行主体の特定を通じた犯罪対策・安全保障

今後のサイバー空間において実空間と同水準の安全性を実現するため、法治国家として、犯罪についてその行為者に帰責するという健全な社会認識を醸成していく必要がある。そのためには、警察における犯人の事後追跡可能性の向上や犯行主体やその手口、目的を特定する活動（アトリビューション）の強化・活用を図るため、犯罪インフラを提供する悪質事業者の摘発強化等の取組が必要である。

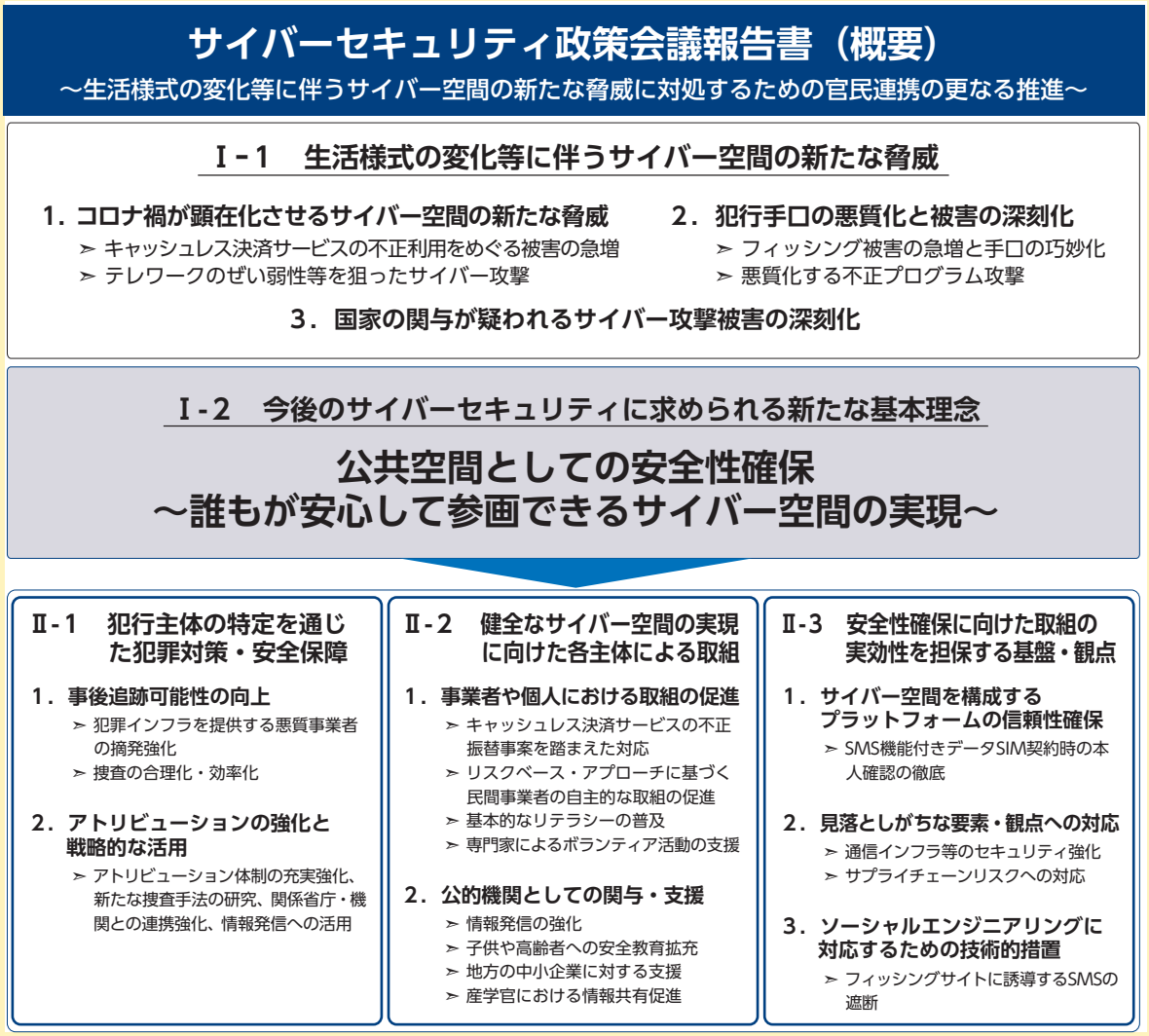
注：17頁参照

イ　健全なサイバー空間の実現に向けた各主体による取組

健全なサイバー空間の実現に向けた各主体におけるサイバー・ハイジーン(注1)の実践を促すため、事業者や個人における具体的な取組の促進、公的機関としての警察による情報発信の強化等の取組が必要である。

ウ　安全性確保に向けた取組の実効性を担保する基盤・観点

安全なサイバー空間の基盤となるスマートフォン等における本人確認等の信頼性を確保するため、SMS機能付きデータSIMを契約する際の本人確認を徹底することのほか、ソーシャルエンジニアリング(注2)に対応するための技術的措置として、フィッシングサイトに誘導するSMSを遮断するための仕組みを構築することが必要であり、これらについて、必要な対策等が講じられるよう関係事業者に対して働き掛けを行うことが重要である。



警察庁では、これまで述べてきたように、サイバー空間の脅威が極めて深刻な情勢にあること、包括的なサイバーセキュリティ対策の必要性等についてサイバーセキュリティ政策会議から提言を受けたことなどを踏まえ、サイバー犯罪・サイバー攻撃への対処能力の向上を図るため、警察の組織体制の在り方等について必要な検討を行っている。今後、令和４年度を目途とした警察組織の見直しも視野に入れた上で、令和３年度末までに一定の方向性を示すこととしている。

注１：ソフトウェアに適切にパッチが適応されているかを確認する、定期的にデータのバックアップを取得するといった、基本的な行動に平時から取り組むこと
２：人間の心理的な隙や行動のミスにつけ込み、情報通信技術を使用せずに、ID・パスワード等を窃取する方法