サイバー空間の安全の確保

第3章
CHAPTER 3

第1節 サイバー空間の脅威

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し、今や、サイバー空間は国民の日常生活の一部となっている。こうした中、インターネットバンキングに係る不正送金事犯等のサイバー犯罪が多発しているほか、重要インフラ(注1)の基幹システム(注2)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3)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頻発するなど、サイバー空間における脅威は深刻化している状況にある。

（1）サイバー犯罪の検挙状況

平成29年中のサイバー犯罪の検挙件数は9,014件と、前年より690件（8.3%）増加し、過去最多を記録した。

① 不正アクセス禁止法(注4)違反

29年中の不正アクセス禁止法違反の検挙件数は648件と、前年より146件（29.1%）増加した。また、検挙人員は255人と、前年より55人（27.5%）増加した。

② コンピュータ・電磁的記録対象犯罪等

29年中の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及び不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウイルスに関する罪）の検挙件数は355件と、前年より19件（5.1%）減少した。このうち、コンピュータ・ウイルスに関する罪の検挙件数は75件であった。

③ ネットワーク利用犯罪(注5)

29年中のネットワーク利用犯罪の検挙件数は8,011件と、前年より563件（7.6%）増加した。特徴として、青少年保護育成条例違反の検挙件数が858件と、前年より242件（39.3%）増加した一方、著作権法違反の検挙件数は398件と、前年より188件（32.1%）減少した。

図表3－1 サイバー犯罪の検挙件数の推移（平成25～29年）

区分＼年次	25	26	27	28	29
合計（件）	8,113	7,905	8,096	8,324	9,014
不正アクセス禁止法違反	980	364	373	502	648
コンピュータ・電磁的記録対象犯罪等	478	192	240	374	355
ネットワーク利用犯罪	6,655	7,349	7,483	7,448	8,011
児童買春・児童ポルノ禁止法違反（児童ポルノ）	1,124	1,248	1,295	1,368	1,432
詐欺	956	1,133	951	828	1,084
うちオークション利用詐欺	158	381	511	208	212
青少年保護育成条例違反	690	657	693	616	858
児童買春・児童ポルノ禁止法違反（児童買春）	492	493	586	634	793
わいせつ物頒布等	781	840	835	819	769
著作権法違反	731	824	593	586	398
脅迫	189	313	398	387	376
ストーカー規制法違反	113	179	226	267	323
商標法違反	197	308	304	298	302
名誉毀損	122	148	192	215	223
その他	1,260	1,206	1,410	1,430	1,453

注1：情報通信、金融、航空、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、石油の各分野における社会基盤
2：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
3：重要インフラの基幹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
4：不正アクセス行為の禁止等に関する法律
5：その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

（２）サイバー攻撃の情勢

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。

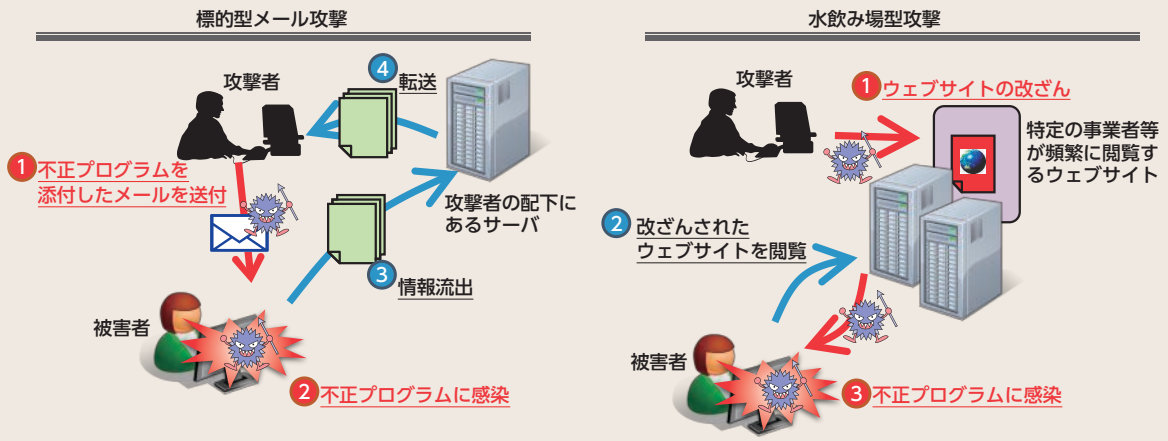
サイバーテロに用いられる手口としては、セキュリティ上のぜい弱性を悪用するなどして攻撃対象のコンピュータに不正に侵入するもの、不正プログラムに感染させることにより管理者や利用者の意図しない動作をコンピュータに命令するものなどがある。

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、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て行われる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。

サイバーインテリジェンスに用いられる手口としては、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図る標的型メール攻撃が代表的である。また、このほかにも、対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる水飲み場型攻撃も発生するなど、その手口はますます巧妙化・多様化している。さらに、我が国に対する国際テロの脅威が現実のものとなっていることを踏まえると、物理的なテロの準備行為として、重要インフラ事業者等のシステムに侵入し警備体制に関する情報を窃取するなどのサイバーインテリジェンスが行われるおそれがある。

図表３－２　サイバーインテリジェンスの手口



CASE

平成29年（2017年）５月、フランス大統領選挙に関連して、マクロン候補（当時）の陣営がサイバー攻撃を受け、大量の電子メールや会計資料等の情報がインターネット上に流出したことが報道された。

第2節 サイバー空間の脅威への対処

1 総合的なサイバーセキュリティ対策の強化

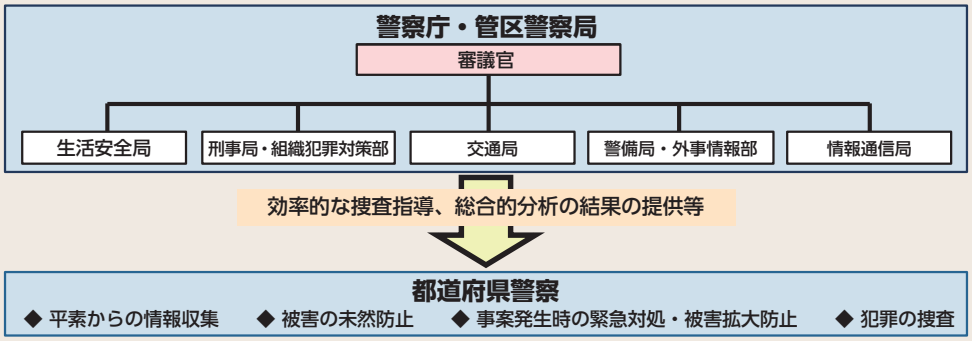
（1）警察におけるサイバー空間の脅威への対処体制

サイバー空間の脅威への対処は警察のいずれの部門にとっても大きな課題となっており、統一的な戦略の下で警察全体の対処能力を強化する必要があることから、警察庁では、サイバーセキュリティ対策全般の司令塔としての機能を強化するため、サイバーセキュリティの確保に向けた各種取組の総括・調整を行う審議官が、

- サイバーセキュリティ戦略の策定
- サイバー空間の脅威への総合的な対処方針の策定
- 捜査員等の人材育成に関する指針の立案
- 民間事業者、外国機関等との連絡の総括
- サイバー空間の情勢の総合的な分析
- 部門横断的な捜査支援・技術支援の調整
- 装備資機材の効果的な整備・活用の調整

といった取組を推進している。

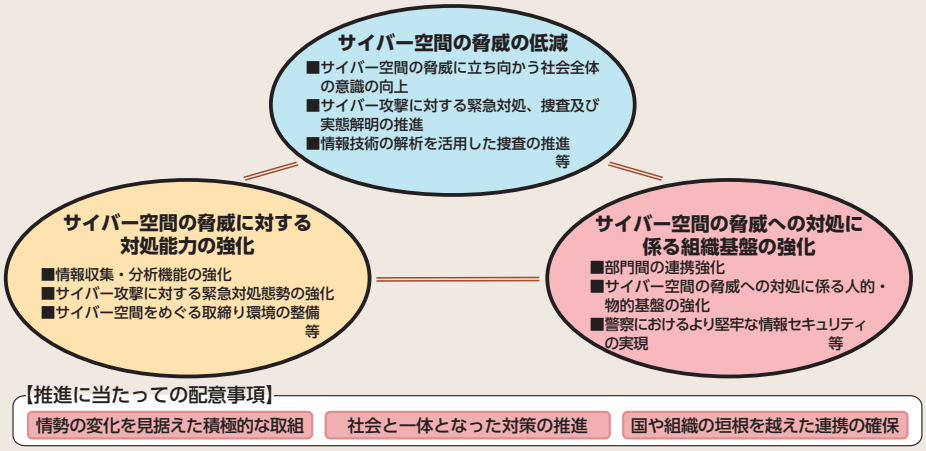
図表３－３ 警察におけるサイバー空間の脅威への対処体制



（2）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、平成27年に制定された「警察におけるサイバーセキュリティ戦略」に基づき、サイバー空間の脅威への対処に係る組織基盤を強化するなど、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。

図表３－４ 警察におけるサイバーセキュリティ戦略の概要

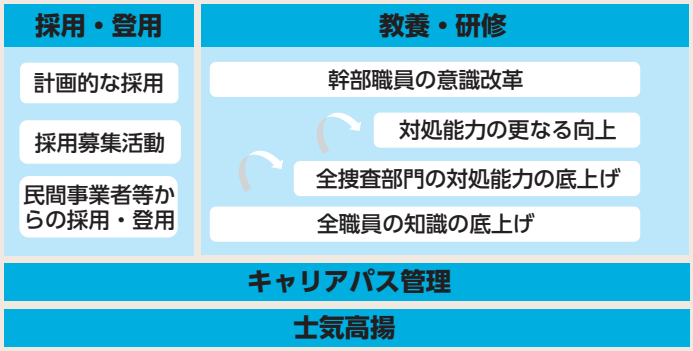


（３）サイバー空間の脅威への対処に係る組織基盤の強化

①　サイバー空間の脅威への対処に係る人材の確保・育成

警察では、サイバー空間の脅威への対処に係る人的基盤を強化するため、平成27年に策定した「サイバー空間の脅威への対処に係る人材育成方針」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。また、28年に「警察庁サイバー人材確保・育成計画」を策定し、サイバー空間の脅威への対処に係る人材の裾野の拡大及び能力の向上を図ることとしている。

図表３－５　サイバー空間の脅威への対処に係る人材育成



さらに、警察庁では、各都道府県警察の捜査員等を対象に、サイバー空間の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。

サイバーセキュリティコンテストの状況

②　サイバーセキュリティ対策研究・研修センターの取組

警察大学校に設置されているサイバーセキュリティ対策研究・研修センターは、解析研究室と捜査研修室の２室で構成され、両室は相互に連携しつつ、以下の取組を実施している。

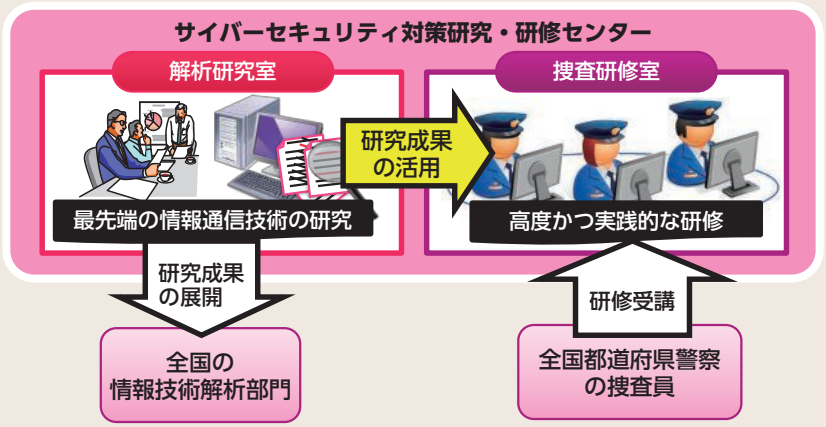
ア　犯罪の取締りのための情報技術の解析に関する研究

解析研究室においては、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及び各種電子機器等の解析手法の確立に向けた研究を行うとともに、研究成果を全国の情報技術解析部門に展開している。

イ　警察全体の対処能力向上に必要な研修

捜査研修室においては、解析研究室で得られた成果を活用しつつ、各都道府県警察においてサイバー犯罪対策やサイバー攻撃対策に専従する捜査員をはじめとする全部門の捜査員を対象に、実際の事案を想定した高度かつ実践的な研修を行っている。

図表３－６　サイバーセキュリティ対策研究・研修センター



2 サイバー犯罪への対策

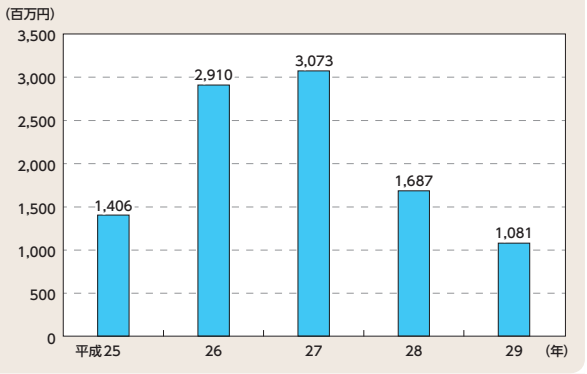
（1）インターネットバンキングに係る不正送金事犯への対策

① 発生状況

不正送金事犯の被害額は、平成27年に過去最多の約30億7,300万円となったが、28年に被害額は大きく減少し、29年の被害額は約10億8,100万円と、前年より約6億600万円（35.9%）減少した。

一方、29年中は、新たな不正送金ウイルスが検出されたほか、インターネットバンキングのID・パスワード等を不正に入手し、電子決済サービスを利用して仮想通貨交換業者へ不正送金を行う新たな手口が出現するなど、予断を許さない状況にある。また、不正送金先の口座名義人の国籍についてはベトナムの割合が高いことが特徴として挙げられる。

図表３－７ 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25～29年）



② 不正送金事犯に対処するための取組

ア 不正送金事犯に関与した者の検挙状況

警察では、29年中、不正送金事犯に関連して、金融機関のサーバに不正アクセスして不正送金を行った者をはじめ、他人に利用させる意図を隠して口座を開設した者、口座を売買した者、不正に送金された資金を引き出した者、現金を回収した者、これらを指示した者等合計77人を検挙した。

イ 金融機関等と連携した抑止対策

警察では、銀行、仮想通貨交換業者等の金融機関に対し、モニタリング(注1)、ワンタイムパスワード(注2)及び二経路認証(注3)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。

CASE

警視庁は、JC3(注4)と連携し、インターネットバンキングの利用時に正規の画面を装った偽の画面を表示させてワンタイムパスワードを入力させ、自動的に他人の口座へ不正送金を行うコンピュータ・ウイルスの機能を解明したことから、29年3月、インターネットバンキングの利用者や金融機関等に対して注意喚起を実施した。また、JC3では、同ウイルスの感染の有無を確認できるウェブページを公開した。

（2）コンピュータ・ウイルス対策

警察では、コンピュータ・ウイルスに関する罪の取締りを推進するとともに、民間事業者と連携したコンピュータ・ウイルスによる被害拡大防止のための対策を講じている。

警察庁では、犯罪捜査の過程で警察が把握した新たなコンピュータ・ウイルスに関する情報をウイルス対策ソフト事業者等に提供し、当該コンピュータ・ウイルスによる被害の拡大防止を図るための枠組み(注5)を構築している。

CASE

男子中学生（14）は、平成29年1月から同年4月にかけて、他人のコンピュータに保存されているファイルを暗号化して、同ファイルの利用を不可能にするとともに、人の電子計算機における実行の用に供する目的で、「法律に違反するファイルが検出されたためこのコンピュータのファイルを暗号化しました。解除するには罰金をお支払い頂く必要があります。」等と表示するランサムウェアを作成し、自宅に保管していた。同年6月、同男子中学生を不正指令電磁的記録作成罪等で逮捕した（神奈川）。

注1：金融機関が、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
2：インターネットバンキング等における認証用の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、識別符号を盗まれても次回の利用時に使用できないこととなる。
3：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
4：129頁参照
5：128頁参照

（3）不正アクセス対策

① 発生状況等

平成29年における不正アクセス行為の認知件数(注1)は1,202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」が442件（36.8%）と最多であった。

また、検挙した不正アクセス禁止法違反における不正アクセス行為の手口は、「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が230件（38.4%）と最多であった。

図表３－８ 不正アクセス行為後の行為別認知件数（平成28年及び29年）

区分＼年次	28	29
合計（件）	1,840	1,202
インターネットバンキングでの不正送金等	1,305	442
仮想通貨交換業者等での不正送信		149
メールの盗み見等の情報の不正入手	91	146
インターネットショッピングでの不正購入	172	133
知人になりすましての情報発信	25	110
オンラインゲーム・SNSの不正操作	124	83
インターネット・オークションの不正操作	34	28
ウェブサイトの改ざん・消去	6	14
その他	83	97

図表３－９ 検挙した不正アクセス禁止法違反における不正アクセス行為の犯行手口の内訳（平成28年及び29年）

区分＼年次	28	29
合計（件）	462	599
識別符号窃用型(注)	457	545
利用権者のパスワードの設定・管理の甘さにつけ込んだもの	244	230
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もの	61	113
他人から入手したもの	20	74
言葉巧みに利用権者から聞き出した又はのぞき見たもの	49	42
スパイウェア等のプログラムを使用して識別符号を入手したもの	34	37
フィッシングサイトにより入手したもの	3	2
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したもの	4	0
その他	42	47
セキュリティ・ホール攻撃型	5	54

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

② 不正アクセス防止対策に関する官民連携

不正アクセス防止対策に関する官民意見集約委員会(注2)における「不正アクセス防止対策に関する行動計画」に基づき、情報セキュリティに関する情報を掲載した情報セキュリティ・ポータルサイト「ここからセキュリティ！」(注3)を公開するなど、不正アクセスを防止するための官民連携した取組を実施している。

CASE

男子高校生（16）は、28年7月から同年10月にかけて、SNSを装ったフィッシングサイトをインターネット上に公開し、同サイトを閲覧した者のID・パスワードの入力を不正に要求して、他人のID・パスワードを不正に取得した。29年6月、同男子高校生を不正アクセス禁止法違反（識別符号取得等）で逮捕した（宮城、福井）。

（4）通信事業者における通信履歴等（ログ）の保存

通信履歴等（ログ）は、サイバー空間における事後追跡可能性を確保するために必要であるが、我が国では事業者に平素からログの保存を義務付ける制度が存在しておらず、サイバー犯罪捜査等を行う上で大きな課題となっている。

警察では、ログの保存が許容される期間を具体的に例示した総務省による「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」の解説を踏まえ、総務省と連携し、関係事業者における適切な取組が推進されるよう、必要な対応を行っている。

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をいう。

2：23年に、警察庁、総務省及び経済産業省が主体となって、社会全体としての不正アクセス防止対策の推進に当たって必要となる施策に関して、現状の課題や改善方策について官民の意見を集約するため、民間事業者等と共に設置した委員会

3：https://www.ipa.go.jp/security/kokokara/

（5）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、被害防止対策の重要性が高まっていることから、警察では、民間事業者や外国捜査機関等と連携し、都道府県警察が相談等で受理した海外の偽サイト等(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。

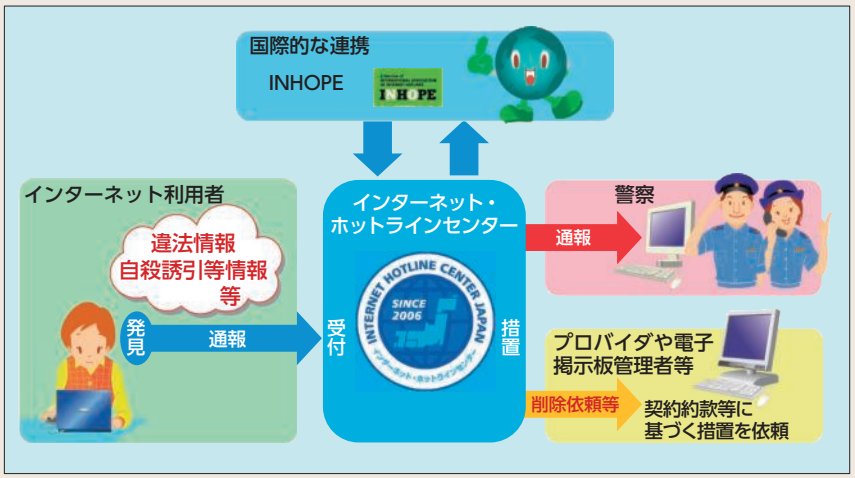
（6）インターネット上の違法情報・有害情報対策

インターネット上には、児童ポルノや覚醒剤等規制薬物の販売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氾濫している。

①　インターネット・ホットラインセンターにおける取組等

警察庁では、一般のインターネット利用者等から、違法情報等に関する通報を受理し、警察への通報や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。平成29年中にIHCが削除依頼を行った2,187件のうち1,778件（81.3%）が削除された。

図表３－10　インターネット・ホットラインセンターにおける取組



IHCに通報された違法情報等の中には、外国のサーバに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、IHCからの通報に対して全国協働捜査方式を活用し、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。

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

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。11年に設立され、30年４月末現在、IHCを含む55団体（49の国・地域）から構成される国際組織

3 サイバー攻撃への対策

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、各部門が連携し、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。また、各国治安情報機関との捜査や情報収集に関する協力を強化したり、民間事業者等との協力関係を確立して被害の未然防止を図ったりするなど、サイバー攻撃をめぐる新たな情勢に対処するための対策に取り組んでいる。

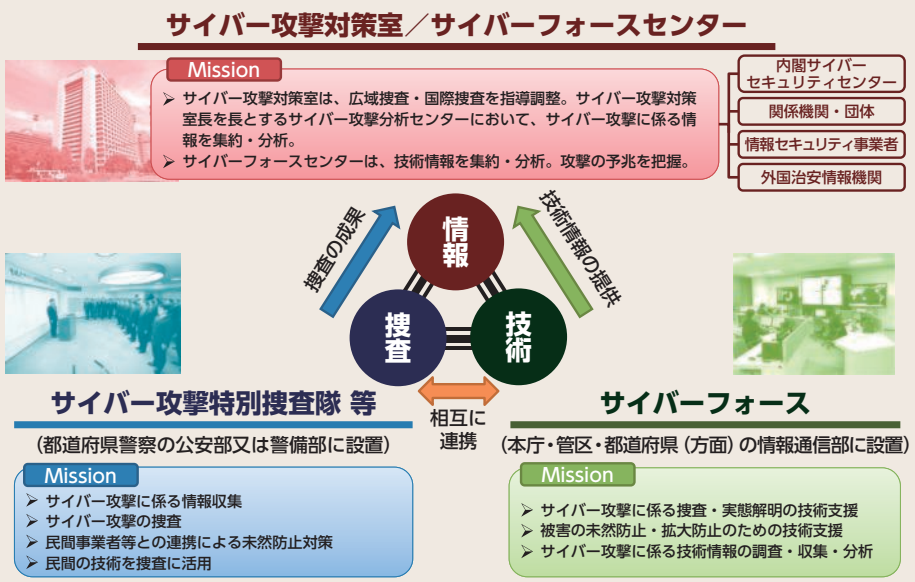
（1）サイバー攻撃対策の推進体制

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、官民連携や各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、サイバー攻撃に係る情報の集約・分析を実施している。

また、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、サイバー攻撃に係る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。

さらに、警察では、サイバー攻撃対策の技術的基盤として、警察庁及び地方機関(注)にサイバーフォースと呼ばれる技術部隊を設置しており、都道府県警察に対する技術支援を実施している。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、サイバー攻撃発生時においては技術的な被害状況の把握、被害拡大の防止、証拠保全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等の分析、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3－11 サイバー攻撃対策の推進体制



注：管区警察局情報通信部、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）サイバー攻撃の予兆・実態の把握

①　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、各国治安情報機関との情報交換を行うとともに、ICPO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)。

CASE

警察では、平成29年3月、インターネットに接続されたコンピュータを不正プログラムに感染させ、同コンピュータに接続した外部記録媒体に保存されている情報を窃取する手口を把握したことから、警察庁ウェブサイト「@police」(注2)において、適切な被害防止対策を講ずるよう注意喚起を行った。

②　リアルタイム検知ネットワークシステム

サイバーフォースセンターでは、インターネットとの接続点に設置したセンサーにおいて検知したアクセス情報等を集約・分析することで、DoS(注3)攻撃の発生や不正プログラムに感染したコンピュータの動向等の把握を可能とするリアルタイム検知ネットワークシステムを24時間体制で運用している。このシステムにより分析した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の情報提供に活用するほか、警察庁ウェブサイト「@police」で広く一般に公開している。

サイバーフォースセンターにおける
リアルタイム検知ネットワークシステムの運用状況

「@police」

MEMO　平成29年中のインターネット観測結果

サイバーフォースセンターでは、平成29年中に、インターネットとの接続点に設置したセンサーにおいて、一つのセンサー当たり約46秒に1回の割合という高い頻度で日本国内のみならず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。

特に、29年4月以降、マイクロソフト社が提供するOSのぜい弱性を悪用する攻撃ツールを用いて、探索行為又は攻撃を行っているとみられる不審なアクセスを観測し、同年5月には、同ツールを用いた「WannaCry」等と呼ばれるランサムウェアに感染したコンピュータが発信元とみられる不審なアクセスを観測した。

また、同年6月には、同ランサムウェアの亜種に感染したコンピュータが発信元とみられる不審なアクセスを観測しており、これらのアクセスは、他のコンピュータを同亜種に感染させることを企図した攻撃とみられ、同亜種の感染が拡大した場合には、システム障害が発生するおそれや、感染したコンピュータが第三者に遠隔操作され、更に感染が拡大するおそれがある。

警察庁では、コンピュータが不正プログラムに感染することを未然に防止するため、コンピュータの利用者に対し、修正プログラムを適用してOSを最新の状態にするなど、適切なセキュリティ対策を講じるよう注意喚起を行っている。

注1：外国捜査機関等との連携の推進については、48頁（トピックスⅠ　サイバー犯罪・サイバー攻撃対策に関する国際連携の推進）参照
2：https://www.npa.go.jp/cyberpolice/
3：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

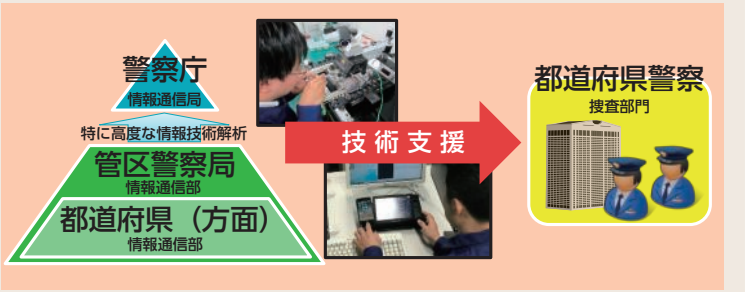
4 技術支援と解析能力の向上

（１）犯罪の取締りへの技術支援

コンピュータ、スマートフォン等の電子機器が普及し、これらがあらゆる犯罪に悪用されており、こうした犯罪の取締りにおいても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、警察庁及び地方機関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(注)。

図表３－12　犯罪の取締りへの技術支援



また、近年、不正プログラムを悪用したサイバー犯罪・サイバー攻撃の多発等により、不正プログラムの解析の需要が増大していることに加え、手口の巧妙化・多様化により、その解析には極めて高い技術力が求められていることから、警察では、警察庁高度情報技術解析センターを中心に、組織の総合力を発揮して不正プログラムの解析に取り組んでいる。

（２）解析能力の向上に向けた取組

①　スマートフォン等への対応

スマートフォン等の記憶容量の増大やアプリの多様化・複雑化により、これらの解析がますます困難になっているところ、警察では、最新の電子機器に対応できる資機材の充実や関係機関と連携した解析手法の開発を進めるなど、スマートフォン等への対応力を強化している。

②　最先端の情報通信技術等の研究

近年、最先端の情報通信技術を用いたサイバー犯罪・サイバー攻撃への対応が求められているところ、警察では、警察大学校サイバーセキュリティ対策研究・研修センターにおいて、犯罪に悪用され得る最先端の情報通信技術等の研究を行っている。

③　国内外研究機関への職員派遣

警察では、電子機器の解析やサイバー犯罪・サイバー攻撃への対策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、最新の電子機器及び不正プログラムの解析手法や、今後悪用され得る情報システム、インターネット上のサービス等に関する調査及び研究を実施し、解析能力の向上に努めている。

注：112頁参照

5 官民連携の推進

サイバー空間の脅威に対処するためには、民間事業者との連携が重要であり、警察では、人事交流や新種の不正プログラムの情報共有枠組みの構築等の各種取組を行っている。

（1）サイバーテロ対策協議会

警察では、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の間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

愛媛県警察では、平成29年8月、四国管区警察局及び香川県警察と連携し、現に稼働中の原子力発電所において、サイバー攻撃の発生を想定した電気事業者との共同対処訓練を実施した。同訓練の実施に当たっては、原子力規制庁の助言を受けて作成した想定シナリオを使用するなど実践的な内容とすることで、事案対処能力の向上を図った。

サイバー攻撃の発生を想定した共同対処訓練

（2）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。

（3）不正プログラム対策協議会

警察では、ウイルス対策ソフト提供事業者等との間で、不正プログラム対策協議会を設置しており、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。

（4）不正通信防止協議会

警察では、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の間で、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を設置しており、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。

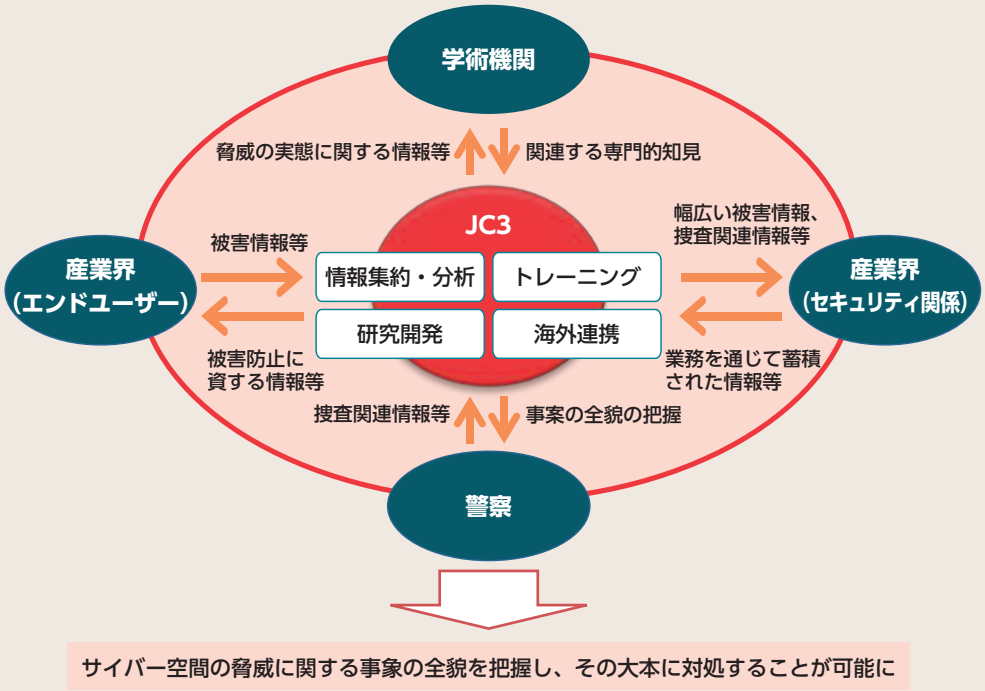
（5）共同対処協定の締結

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、平成29年末までに、オンラインゲーム事業者や銀行等、全国で582事業者・団体と本協定を締結している。

（６）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)）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・的確に活用することにより、安全で安心なサイバー空間の構築に努めている。

図表３－13　日本サイバー犯罪対策センター（JC3）の概要



（７）都道府県警察における産学官連携による中小事業者対策

警察では、中小事業者が有する先端技術に関する情報の窃取や、中小事業者の保有するサーバ等がサイバー攻撃の踏み台として悪用されることなどを防止するため、商工会議所、学術機関、地方公共団体等と連携し、中小事業者における適切な対策を促すための広報啓発活動等を実施している。

（８）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、当該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。

注：Japan Cybercrime Control Centerの略

警察活動の最前線

上州くん
みやまちゃん

サイバー空間の安全のために

群馬県警察本部生活安全部サイバー犯罪対策課特別捜査係（現　群馬県伊勢崎警察署生活安全課生活安全係）
大須賀（おおすが）　智彦（ともひこ）　警部補

私は、大学卒業後、民間のシステム開発企業に勤めていましたが、自分の知識や技術をより世の中のために役立てたいと思い、群馬県警へ転職しました。

警察官としての最初の担当業務は、サイバー犯罪による被害に遭った方の相談対応に加えて、企業のシステム担当者や学生に対し、サイバー犯罪による被害防止策について防犯講話を行うことでした。

相談対応を担当して、日々受理する相談の種類や件数の多さに驚くとともに、サイバー犯罪による被害は誰にでも起こり得ることなのだと実感しました。

「自分は犯罪被害に遭わないと思ってはいけない。しかし、今や社会基盤となったインターネットの利用を避けることはできない。だからこそ、犯罪被害に遭うかも知れないという怖さを知った上でインターネットを利用してほしい。」

民間企業にいたときは考えもしなかったことです。

防犯講話では、サイバー犯罪による被害者を一人でも減らしたいという思いで、実感を持ちづらいサイバー空間の脅威について、民間企業で培った知識をいかし、企業や学生の方にも分かりやすく説明しながら、私の思いを参加者の方々に伝え続けました。

これからも、自分の経験と知識を最大限に活用して、サイバー空間における安全の確保に邁進（まいしん）していきます。

サイバー攻撃対策に向けた取組

九州管区警察局沖縄県情報通信部情報技術解析課解析係（現　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）
夜差（やざし）　章浩（あきひろ）　警部補

私は、主に技術的な側面から、沖縄県警察におけるサイバー攻撃対策等に取り組んでいます。

具体的には、県内の重要インフラ事業者等を対象としたセキュリティセミナーでの講演や、警察職員に対する不正プログラム等に関する講義、押収したスマートフォンから証拠となる情報を取り出すための解析といった犯罪の取締りのための技術支援等を行っています。

サイバー空間をめぐる情勢は、日々変化しており、平成29年５月には、世界的規模で「WannaCry」等と呼ばれるランサムウェア(注)に感染させられる事案が発生し、日本でも被害が確認されるなど、サイバー空間の脅威は深刻化しています。

このような状況の中、サイバー攻撃による被害を防止するためには、民間の方々のセキュリティ意識の向上を図ることが重要となります。

そこで私は、ランサムウェアの最新の手口や脅威の実態を分かりやすく説明できるよう、ランサムウェアに感染したコンピュータの様子を疑似的に再現するプログラムを作成しました。講演等において、コンピュータの画面上に脅迫文等が表示され、コンピュータの機能が制限される様子を壇上で実演することで、ランサムウェアの脅威をより実感してもらい、セキュリティ意識の向上を図ることができたと感じています。

警察は、サイバー空間の脅威に対処するため、部門を横断し、一丸となってサイバーセキュリティ対策に取り組んでいます。私もその一員として、今後も警察組織の総合力を発揮した効果的なサイバーセキュリティ対策に寄与していきたいと思います。

注：48頁参照