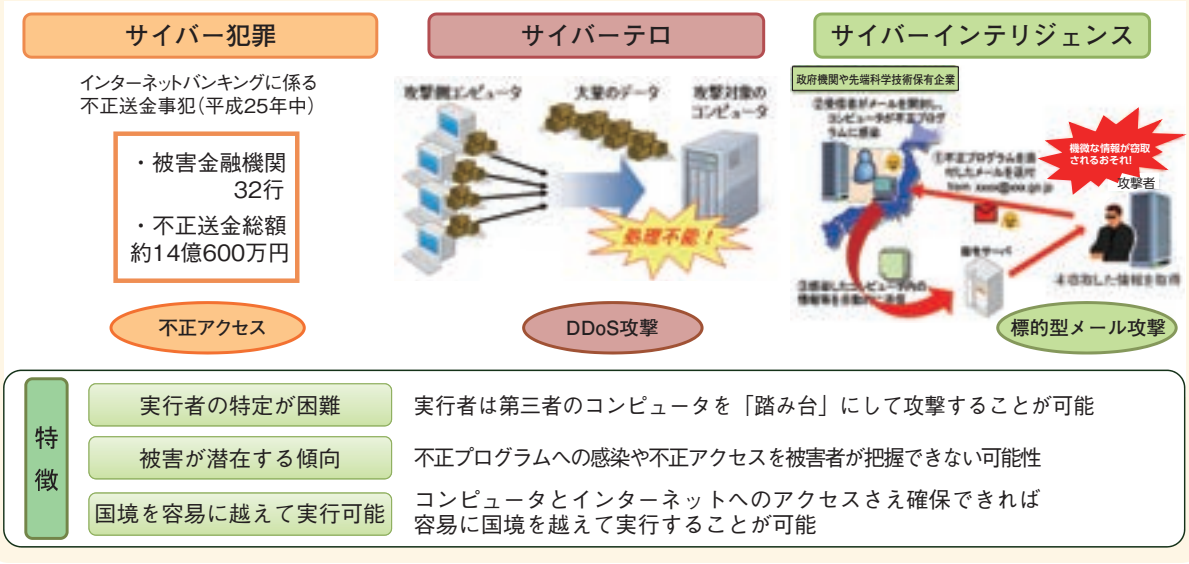
サイバー空間の安全の確保

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(注1)が多発しているほか、重要インフラ(注2)の基幹システム(注3)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4)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。

図表3－1 サイバー空間における脅威



1 サイバー犯罪の情勢

(1) サイバー犯罪の検挙状況

平成25年中のサイバー犯罪の検挙件数は8,113件と、前年より779件(10.6%)増加し、過去最多を記録した。また、インターネットバンキングに係る不正送金事犯が多発し、被害額は約14億600万円と大幅に増加したほか、不正アプリによる個人情報の収集事案等が発生しており、サイバー犯罪による被害は深刻さを増している。

① 不正アクセス禁止法違反

25年中の不正アクセス禁止法違反の検挙件数は980件と、前年より437件(80.5%)増加した。また、検挙人員は147人と、前年より7人(4.5%)減少した。

② コンピュータ・電磁的記録対象犯罪等

25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(以下「コンピュータ・ウイルスに関する罪」という。)の検挙件数は478件と、前年より300件(168.5%)増加した。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27件であった。

注1:高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪
2～4:108頁参照

③　ネットワーク利用犯罪 (注1)

25年中のネットワーク利用犯罪の検挙件数は6,655件と、前年より42件（0.6%）増加し、過去最多となった。特にわいせつ物領布等及び著作権法違反については、21年中と比較すると、検挙件数がそれぞれ約5.6倍及び約3.9倍となっており、著しく増加している。

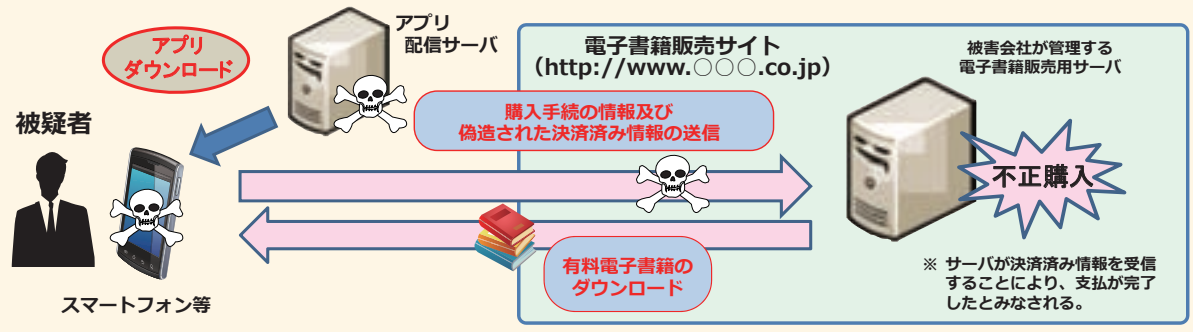
図表３－２　サイバー犯罪の検挙件数の推移（平成21～25年）

区分＼年次	21	22	23	24	25
合計(件)	6,690	6,933	5,741	7,334	8,113
不正アクセス禁止法違反	2,534	1,601	248	543	980
コンピュータ・電磁的記録対象犯罪等	195	133	105	178	478
ネットワーク利用犯罪	3,961	5,199	5,388	6,613	6,655
詐欺	1,280	1,566	899	1,357	956
児童買春・児童ポルノ禁止法違反(児童ポルノ)	507	783	883	1,085	1,124
わいせつ物頒布等	140	218	699	929	781
青少年保護育成条例違反	326	481	434	520	690
著作権法違反	188	368	409	472	731
児童買春・児童ポルノ禁止法違反(児童買春)	416	410	444	435	492
出会い系サイト規制法(注2)違反	349	412	464	363	339
商標法違反	126	119	212	184	197
その他	629	842	944	1,268	1,345

事例1 Case

団体職員の男（33）らは、電子書籍をスマートフォンで購入する際、実際には決済がなされていないにもかかわらず決済がなされている旨の虚偽の情報を被害会社のサーバに送信するスマートフォン等のアプリを使用するなどして、多数の電子書籍を不正に入手した。警視庁外６府県警察は、25年12月までに、電子計算機使用詐欺で男ら15人を検挙した。

図表３－３　スマートフォン等のアプリを用いた電子書籍の詐取事案の概要



事例2 Case

サイト運営会社役員の男（59）らは、スマートフォンの電話帳データを不正に取得するコンピュータ・ウイルスを作成し、電池を長持ちさせるアプリと偽って、事情を知らない者にダウンロードさせてコンピュータ・ウイルスを供用した。25年９月、不正指令電磁的記録供用罪等で男ら６人を逮捕した（京都、大分）。

事例3 Case

電気設備修理業の男（50）らは、インターネット上に、有料である衛星放送を無料で視聴できるように不正に改造されたＢ－ＣＡＳカードの販売サイトを立ち上げ、当該Ｂ－ＣＡＳカードを販売した。栃木県警察外８道県警察は、25年９月までに、私電磁的記録不正作出等で販売に関わった男ら７人を逮捕したほか、多数の購入客を不正作出私電磁的記録供用罪で検挙した。

注１：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：インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律

2 サイバー攻撃の情勢

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で、我が国の政府機関、民間企業等に対するサイバー攻撃が発生している。特に、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、社会機能を麻痺させる電子的攻撃であるサイバーテロ(注3)や、情報通信技術を用いた諜報活動であるサイバーインテリジェンスの脅威は、国の治安や安全保障に影響を及ぼすおそれのある問題となっている。

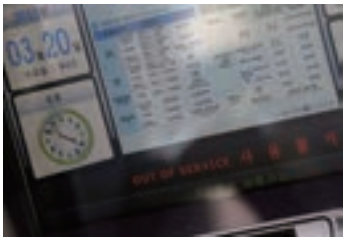
（1）サイバーテロの情勢

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によりインフラ機能の維持やサービスの供給が困難となり、国民の生活や社会経済活動に重大な被害をもたらすサイバーテロの脅威は正に現実のものとなっている。これまで、我が国では重要インフラの基幹システムに対する電子的攻撃により社会的混乱が生じるようなサイバーテロの被害は生じていないが、海外では、金融機関のシステムや原子力発電所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。

サイバーテロに用いられるおそれのある手口としては、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。

事例 Case

平成25年3月、韓国では、複数の放送局及び金融機関において、不正プログラムが同時多発的に作動し、数万台に及ぶコンピュータが機能不全を起こした。その結果、ＡＴＭやオンラインバンキングが停止するなど、社会経済活動に大きな影響が生じた。この事案では、不正プログラムを大量のコンピュータに潜伏させ、これらが所定の期日に一斉に活動を開始するよう指示を出すなど、時限爆弾のような仕組みが用いられたとされている。

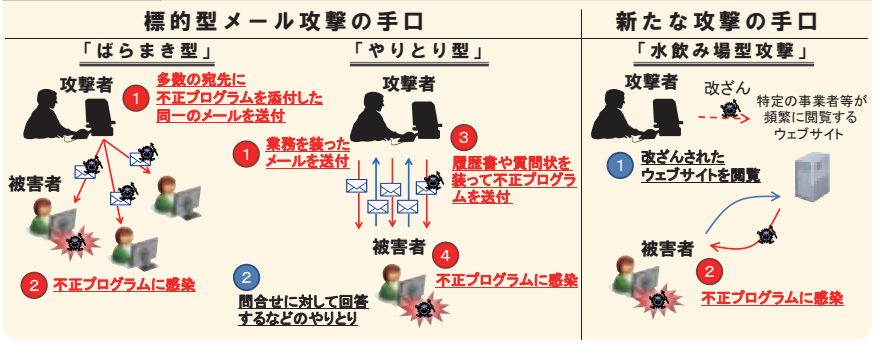


機能不全を起こした韓国金融機関のATM（ロイター／アフロ）

（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。

図表３－４　不正プログラムに感染させる手口



最近では、「ばらまき型」攻撃の件数が減少する一方で、採用活動や取引等の業務との関連を装った通常のメールのやりとりを何通か行うことにより、添付ファイル付きのメールが送付されても不自然ではない状況を作った上で、不正プログラムを添付したメールを送付する「やりとり型」攻撃の件数が

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対する電子的攻撃による可能性が高いもの

増加している。また、送りつけた不正プログラムを受信者に実行させるため、画面上の表示を一般的な文書ファイルや画像ファイルのものに偽装したものが増加している。こうした標的型メール攻撃のほか、標的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という、「水飲み場型攻撃」と呼ばれる手口も出現しており、サイバー攻撃の手口はますます巧妙になっている。

事例１ Case

平成25年５月、農林水産省が設置した第三者委員会による調査結果の中間報告が発表され、同省の職員が使用する複数のコンピュータが不正プログラムに感染し、24年１月から同年４月までの間、業務上の情報や個人情報を含む124点の行政文書等が外部に流出した可能性があること等が明らかになった。

事例２ Case

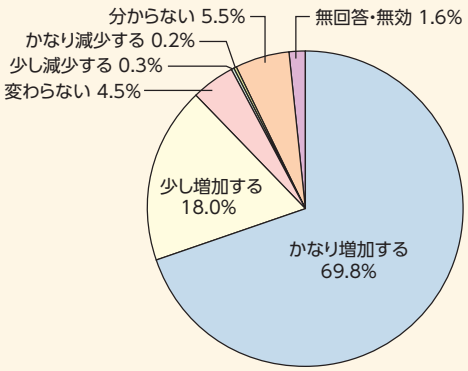
25年４月、宇宙航空研究開発機構（ＪＡＸＡ）において、職員のＩＤとパスワードにより、同機構管理のサーバが不正アクセスされ、国際宇宙ステーション日本実験棟「きぼう」及び国際宇宙ステーション補給機「こうのとり」に関する情報等が流出した可能性があることが明らかになった。

コラム ①サイバー空間の安全・安心に関する国民の意識

警察庁では、平成25年12月、都道府県警察を通じて、サイバー空間の安全・安心に関する国民の意識調査（注）を行った。

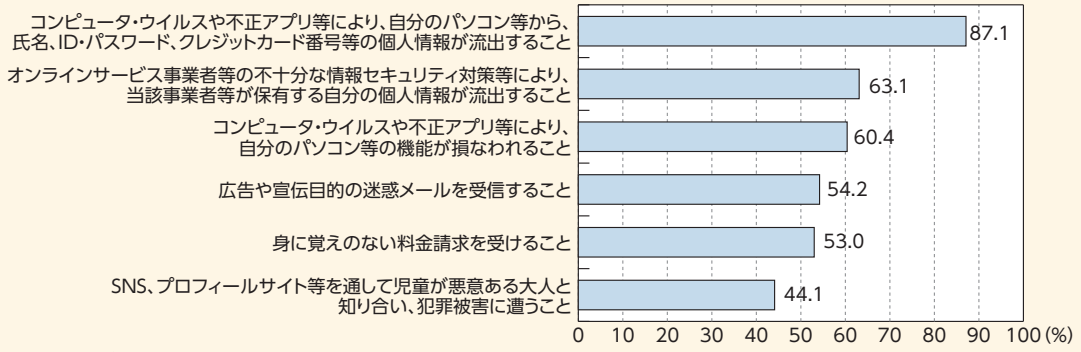
サイバー空間を安全に安心して利用できるかについては、56.8%の者が「そう思わない・どちらかといえばそう思わない」と回答したほか、インターネットを利用した犯罪については、今後「かなり増加する・少し増加する」と回答した者が87.8%を占めるなど、サイバー空間の安全・安心に対する不安感が大きいことがうかがわれた。インターネットを利用していて不安に感じることについては、自分のパソコン等から個人情報が流出することに対する不安を回答した者が87.1%、事業者等が持っている個人情報が流出することに対する不安を回答した者が63.1%と、個人情報の流出が多く挙げられた。

図表３－５ インターネット利用犯罪は増加するか



出典：サイバー空間の安全・安心に関する国民の意識調査

図表３－６ インターネットを利用していて不安に感じること



出典：サイバー空間の安全・安心に関する国民の意識調査

注：全国の運転免許試験場等において、運転免許証の更新に訪れた方を対象に、警察庁において作成した質問票を配付し回答を求める形式で実施
（有効回答数3,462人のうち、インターネットを利用しないと回答した308人を除く3,154人について分析）

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

情報通信技術の進展と共に、サイバー空間では次々と新たなサービスや技術が現れており、その利便性が向上している反面、これらを悪用したサイバー犯罪・サイバー攻撃の手口も日々新たなものが現れている。警察では、こうしたサイバー空間の脅威に的確に対処するべく総合的な対処能力の強化を図っている。

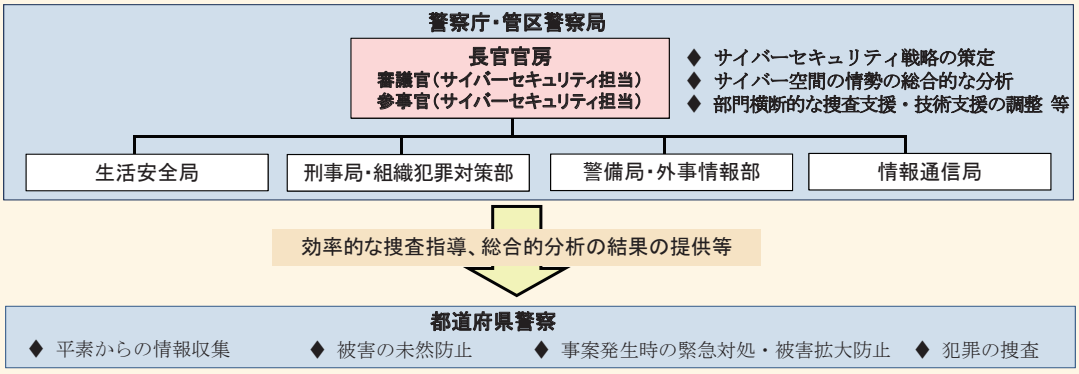
（1）サイバーセキュリティ対策の司令塔機能の強化

サイバー空間の脅威への対処が警察のいずれの部門にとっても大きな課題となっていることを踏まえ、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、平成26年4月、サイバーセキュリティに関する各種取組の総括・調整を行う長官官房審議官（サイバーセキュリティ担当）及び長官官房参事官（サイバーセキュリティ担当）を設置した。同審議官及び同参事官は、

- 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

を行うこととしている。

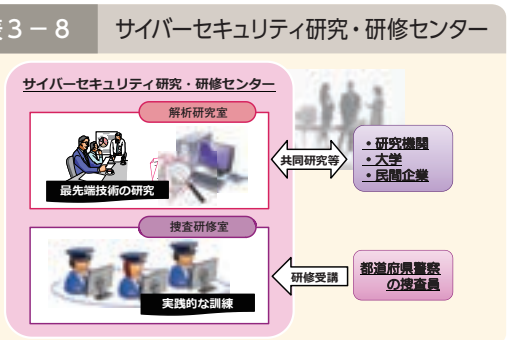
図表３－７ 警察におけるサイバー空間の脅威への対処体制



（2）サイバーセキュリティ研究・研修センターの設置

警察庁では、平成26年4月、警察大学校にサイバーセキュリティ研究・研修センターを設置した。同センターでは、民間の優れた知見を取り入れつつ、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ついて研究を行うとともに、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始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実践的な訓練等を行うなど、サイバー空間における警察全体の対処能力向上に必要な研修を行うこととしている。

図表３－８ サイバーセキュリティ研究・研修センター



2 サイバー犯罪への対策

（１）コンピュータ・ウイルス対策

近年、解析ソフトによる解析を妨害する機能を備えたものが確認されるなど、コンピュータ・ウイルスの高機能化が認められ、また、これらのコンピュータ・ウイルスを感染させる手口として、有用なアプリに偽装したコンピュータ・ウイルスをダウンロードさせる手法等の巧妙かつ多様な手法が確認されている。その結果、個人情報や機密情報の窃取、データの損壊等、被害の多様化・深刻化が懸念される。

そこで、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、平成25年3月、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提供事業者等に提供し、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1)を構築した。

（２）不正アクセス対策

①　発生状況の公表及び共同対処協定の締結

警察庁では、毎年、不正アクセス行為の発生状況を取りまとめ、総務省及び経済産業省と共に公表するとともに、利用権者、アクセス管理者等が不正アクセス行為による被害を防ぐために講じるべきパスワードの適切な設定・管理を始めとする措置について、具体的な注意喚起を行っている。

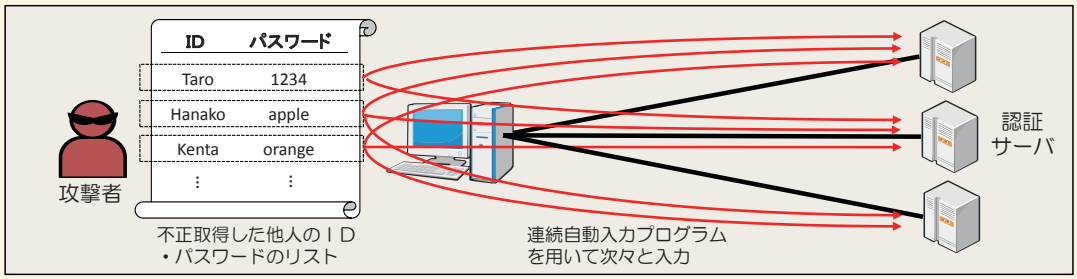
②　不正アクセス防止対策に関する官民意見集約委員会

平成23年12月、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)において「不正アクセス防止対策に関する行動計画」が取りまとめられ、24年9月には、同計画に基づいた取組の成果の一部として、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。

コラム　②連続自動入力プログラムによる不正ログイン攻撃

連続自動入力プログラムによる不正ログイン攻撃とは、インターネット利用者の多くが複数サイトで同一のＩＤ・パスワードを使い回している状況に目を付け、不正取得した他人のＩＤ・パスワードのリストに基づき、インターネットで各種サービスを提供する企業等のサイトに対し、次々とＩＤ・パスワードを自動に入力するプログラムを用いてＩＤ・パスワードを入力し、不正アクセス行為を敢行するものである。このようなプログラムは、大手電気通信事業者や大手通信販売事業者等に対する不正アクセス事案で用いられたことが確認されている。

図表３－９　連続自動入力プログラムによる不正ログイン攻撃



注１：118頁参照
２：平成23年６月、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：http://www.ipa.go.jp/security/kokokara/

（３）インターネット上の違法情報・有害情報対策

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

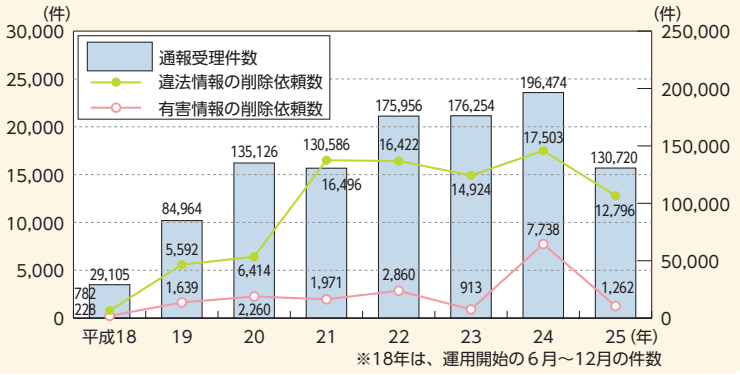
インターネット上には、児童ポルノ画像や覚醒剤等規制薬物の販売に関する情報等の違法情報や、違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない有害情報が氾濫している。

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・有害情報に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行うインターネット・ホットラインセンター（ＩＨＣ）の運用を、平成18年６月から開始した。25年中にＩＨＣが削除依頼を行った情報のうち、違法情報については12,341件が、有害情報については964件が削除された（削除率は、それぞれ96.4%、76.4%）。

違法情報・有害情報の中には、外国のウェブ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、ＩＨＣが、19年３月に各国のホットライン相互間の連絡組織として設置されたＩＮＨＯＰＥ（注1）に加盟し、ＩＮＨＯＰＥ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３－10　インターネット・ホットラインセンターにおける取組

図表３－11　ＩＨＣの通報受理件数及びＩＨＣからの削除依頼数の推移（平成18～25年）



ＩＨＣからの削除依頼に応じない悪質なサイト管理者の中には、違法情報・有害情報を自らのサイトに掲載し、サイトへのアクセス数を増やすことで、広告料収入を得ている者がみられた。こうした状況への対策として、ＩＨＣから広告業界に対して、違法情報・有害情報の削除依頼に応じない悪質サイトに関する情報を提供し、広告業界において悪質サイトへの広告配信の停止等の措置を講ずる新たな取組が26年3月から開始されている。

②　効果的な違法情報・有害情報の取締り

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からの通報に基づく全国協働捜査方式（注2）の活用等により、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。25年中のＩＨＣからの通報に基づく違法情報の検挙件数は1,452件と、10月に全国協働捜査方式の試行を開始した22年中の検挙件数（405件）と比べて約3.6倍に増加している。

注１：旧名称であるInternet Hotline Providers in Europe Associationの略。現在の名称はInternational Association of Internet Hotlines。平成11年に設立され、26年3月末現在、IHCを含む49団体（43の国・地域）から成る国際組織

２：ＩＨＣから警察庁に通報される違法情報・有害情報について効率的な捜査を進めるため、違法情報・有害情報の発信元を割り出すための初期捜査を警視庁が一元的に行い、捜査すべき都道府県警察を警察庁が調整する捜査方式。違法情報については23年7月から、有害情報については24年4月から、それぞれ本格実施している。

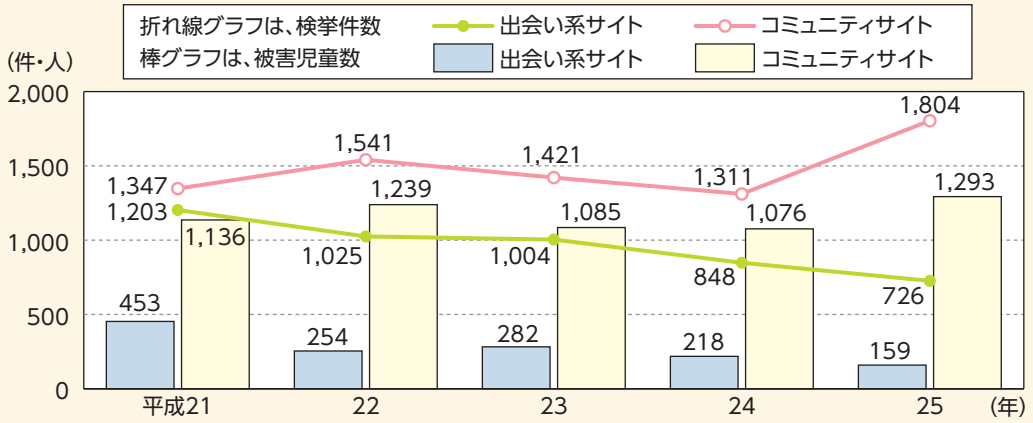
また、ＩＨＣ等から削除依頼がなされたにもかかわらず、削除されなかった違法情報・有害情報が相当数インターネット上に流通したままになっている。警察では、合理的な理由もなく違法情報の削除依頼に応じない悪質なサイト管理者については、検挙を始めとした積極的な措置を講じていくこととしている。

（４）コミュニティサイト等に起因する事犯への対策

①　コミュニティサイト等に起因する事犯の発生状況

出会い系サイト(注1)に起因して犯罪被害に遭った児童（18歳未満の者をいう。以下同じ。）の数は、平成20年の出会い系サイト規制法の改正以降減少傾向にある。一方、コミュニティサイト(注2)に起因して犯罪被害に遭った児童の数は、23年から減少に転じていたが、25年中は、無料通話アプリのＩＤを交換する掲示板に起因する犯罪被害が増加したことにより、再び増加に転じた。

図表３－12　出会い系サイト及びコミュニティサイトに起因する事犯の検挙件数及び被害児童数の推移（平成21～25年）



②　コミュニティサイト等への対策

警察では、コミュニティサイト等に起因する事犯の検挙を推進するとともに、コミュニティサイトに起因する児童被害の防止に向けた対策として、サイト事業者に対するミニメール(注3)の内容確認を始めとするサイト内監視の強化や実効性あるゾーニング(注4)の早期導入に向けた働き掛け、関係省庁、事業者及び関係団体と連携した更なるフィルタリングの普及徹底、児童、保護者、学校関係者等に対する広報啓発等を推進している。

（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等に通報する取組や講演活動等を行うサイバー防犯ボランティアは全国で141団体（平成26年４月現在）に増加しており、警察ではこうした活動を行う団体を育成するため、研修会の開催等の支援を行っている。

注１：面識のない異性との交際（以下「異性交際」という。）を希望する者（以下「異性交際希望者」という。）の求めに応じ、その異性交際に関する情報をインターネットを利用して公衆が閲覧することができる状態に置いてこれを伝達し、かつ、当該情報の伝達を受けた異性交際希望者が電子メールその他の電気通信を利用して当該情報に係る異性交際希望者と相互に連絡することができるようにする役務を提供するウェブサイト等
２：ＳＮＳ、プロフィールサイト等、ウェブサイト内で多数人とコミュニケーションがとれるウェブサイト等のうち、出会い系サイトを除いたものの総称
３：コミュニティサイト内において、会員同士でメッセージの送受信ができる機能
４：サイト内において悪意ある大人を児童に近づけさせないように、携帯電話事業者の保有する契約者年齢情報を活用し、大人と児童とのミニメールの送信や検索を制限すること

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新設するなど体制の強化を行ったほか、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、外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。

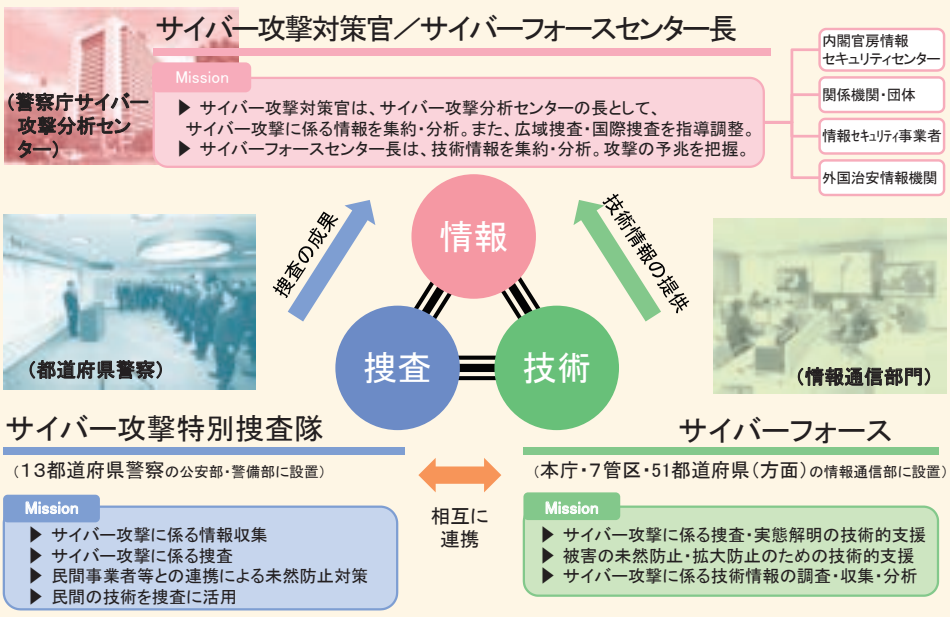
（１）体制の強化

警察庁では、平成25年5月、サイバー攻撃対策官を設置し、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らせるとともに、これを長とするサイバー攻撃分析センターを設置し、サイバー攻撃に係る情報の集約・分析機能を強化している。

また、同年４月、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13都道府県警察に、サイバー攻撃特別捜査隊を設置した。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、全国のサイバー攻撃事案に対する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、サイバーテロへの対処態勢を強化するために、各種訓練に取り組んでいる。同年には、重要インフラ事業者がサイバー攻撃を受けたとの想定の下、初動対処机上訓練を全国の都道府県警察において実施した。

図表３－13　サイバー攻撃対策の推進体制



（２）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不正プログラムを解析するなどして、攻撃者及び手口に係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（国際刑事警察機構）を通じるなどして、海外の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。

（３）技術的基盤の整備

①　サイバーフォース

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1)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は、サイバーフォースセンターとして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緊急対処(注2)の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３－14　サイバーフォースの体制

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対するアクセス情報等を集約・分析することで、ＤｏＳ(注3)攻撃の発生やコンピュータ・ウイルス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。平成26年1月には、情報の集約・分析能力の一層の強化を図るため、同システムの更新・高度化を行った。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、警察庁セキュリティポータルサイト「＠police」(注4)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

コラム　③平成25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25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対して、一つのセンサー当たり約４分40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、25年中は、重要インフラ事業者等のウェブサイトの改ざんを121件（前年比80件増）観測した。これらの中には、目視では改ざんが確認できなくとも、当該ウェブサイトを閲覧すると他の悪意あるウェブサイトへ強制的に接続される仕組みになっているものもあり、そのパソコンが不正プログラムに感染し、思わぬ被害を受ける可能性がある。こうした被害を防ぐためには、インストールされたソフトウェアを最新の状態にしておくとともに、ウイルス対策ソフトを導入するなど、適切なセキュリティ対策を行うことが重要である。

注１：30頁参照
２：被害状況の把握、被害拡大の防止、証拠保全等
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：http://www.npa.go.jp/cyberpolice/

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、携帯電話等の電子機器が普及するとともに、情報通信技術の進展によりスマートフォンのような新たな電子機器が登場し、あらゆる犯罪に悪用されるようになってきており、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(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、押収した携帯電話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。

図表３－15　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）対応力強化に向けた取組

①　海外製スマートフォンへの対応

スマートフォンの急速な普及に伴い、その解析の需要が年々増大している。解析の対象となるスマートフォンの半数以上は海外製のものであることから、警察では、関係機関と連携して海外製スマートフォンの解析を行うなど、海外製スマートフォンへの対応力を更に強化している。

②　最先端の情報通信技術への対応

警察では、急速に進展する情報通信技術に対応するため、最新の電子機器や通信履歴（ログ）の解析等に対応するための解析用資機材の充実、インターネット観測技術の高度化やデジタルフォレンジックを取り巻く課題とその対応に関する調査研究の外部委託等、解析能力の向上を図る取組を推進している。また、警察大学校サイバーセキュリティ研究・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の研究を行っている。

研究例　匿名化通信技術に関する研究

匿名化通信技術は、インターネット上で匿名性を確保し、利用者の発信元を特定されずに通信を行うために使用される技術である。この技術が犯罪に悪用されれば、犯行に使用されたコンピュータを追跡することが困難となる。そこで、サイバーセキュリティ研究・研修センターでは、この技術が悪用された際の発信元の特定につながる手掛かりを発見するための解析手法や、悪用による被害を防止するためのアクセス防御手法について研究を行っている。


匿名化通信技術に関する研究

注：30頁参照

5 国際的なサイバー犯罪捜査協力の推進

（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、サイバー犯罪に関する条約（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に対処している。

（２）国際会議・協議等

警察庁では、Ｇ８ローマ／リヨン・グループ（注4）に置かれたハイテク犯罪サブグループ、ＩＣＰＯが主催するサイバー犯罪に関するユーラシア地域作業部会等の国際会議に参加し、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いる。

また、外国捜査機関等との二国間における協議を通じ、国際捜査共助に係る連携強化や技術情報の共有等を推進している。

第14回アジア大洋州地域サイバー犯罪捜査技術会議

さらに、アジア大洋州地域サイバー犯罪捜査技術会議を平成12年度から毎年度開催し、解析技術やサイバー犯罪捜査に係る知識・経験等の共有を図っている。25年度は、アジア大洋州地域の国等の情報技術解析担当官やサイバー犯罪捜査官のほか、この分野で先進的な取組を行うＮＦＩ（注5）や米国パデュー大学、国内外の民間事業者の専門家が参加し、電磁的記録媒体の解析技術等に関する発表・討議、国際捜査及び官民連携に関する発表・討議、携帯端末解析の演習等を実施した。

このほか、警察庁では、外国捜査機関等との連携を強化するため、25年には米国のＮＣＦＴＡ（注6）が同国内外の捜査機関等の捜査員を対象として実施している捜査実習に職員を派遣したほか、26年度中に海外にリエゾンオフィサーを派遣することとしている。

注１：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11月1日に我が国について発効した。
２：捜査共助の実施を条約上の義務とすることで捜査共助の一層確実な実施を期するとともに、捜査共助の実施のための連絡を外交当局間ではなく、条約が指定する中央当局間で直接行うことにより、手続の効率化・迅速化を図るもの
３：９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」に基づき設置されたもので、26年1月現在、66の国・地域に設置されている。
４：昭和53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年にハリファックス・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13年の米国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。
５：Netherlands Forensics Institute（オランダ国立法科学研究所）の略
６：National Cyber-Forensics & Training Allianceの略。サイバー空間の脅威を効率的に特定及び軽減するため、９年に米国ピッツバーグに設立された非営利団体で、法執行機関、民間企業、学術団体を構成員としている。

第3節 サイバー空間の脅威に対する官民の連携の推進

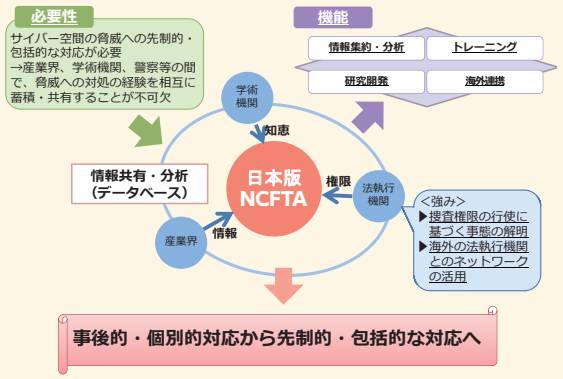
1 サイバー空間の脅威に対する官民の連携の推進

（1）日本版ＮＣＦＴＡの創設に向けた検討

サイバー空間の安全・安心を達成する上では、産学官が連携し、それぞれの知見を活用した取組を推進していく必要がある。米国ではＮＣＦＴＡ(注1)という非営利団体が設立され、産学官における情報共有と協力を促進し、三者が一体となった取組が行われている。

これを踏まえ、平成25年12月に閣議決定された「「世界一安全な日本」創造戦略」(注2)に日本版NCFTAの創設が盛り込まれ、26年1月には、総合セキュリティ対策会議(注3)において「サイバー空間の脅威に対処するための新たな産学官連携の在り方～日本版ＮＣＦＴＡの創設に向けて～」と題する報告書が取りまとめられた。この報告書では、サイバー空間の脅威への対処をより効果的なものとするため、産学官(警察)が持つ経験を全体で蓄積・共有し、警察による捜査権限の行使を始めとする先制的・包括的な対応を可能とする産学官連携の新たな枠組みとして日本版ＮＣＦＴＡを創設する必要性が指摘されている。警察庁では、これらを踏まえ、その創設に向けた実務的・具体的な検討を加速させることとしている。

図表３－16 日本版ＮＣＦＴＡの概要



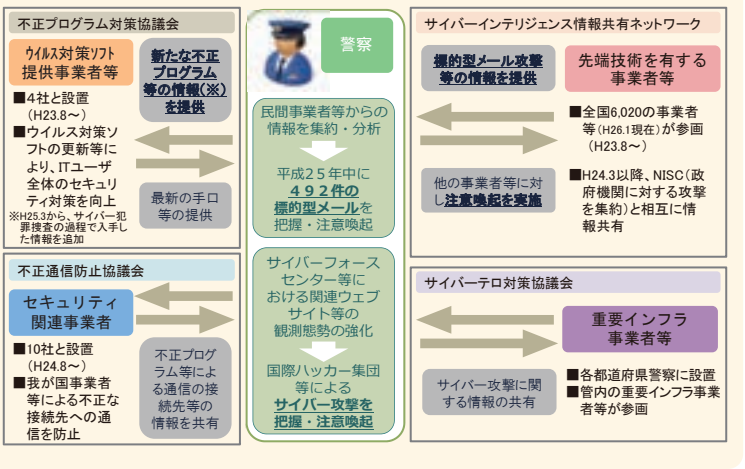
（2）官民の連携のための枠組み

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不可欠であり、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　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。

図表３－17 官民連携のための枠組み



注1 ：117頁参照
2 ：210頁参照
3 ：警察庁において、情報通信ネットワークの安全性・信頼性を確保することを目的として平成13年度から開催し、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について有識者等による検討を行っているもの

②　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。

③　サイバーインテリジェンス情報共有ネットワーク

警察は、情報窃取の標的となるおそれの高い先端技術を有する全国6,020の事業者等（平成26年1月現在）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いる。警察では、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。

④　サイバーテロ対策協議会

警察は、サイバーテロ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ている。また、この協議会の枠組み等を通じ、個別訪問によるサイバーテロの脅威や情報セキュリティに関する情報提供、民間有識者による講演、参加事業者間の意見交換や情報共有等を行っている。さらに、サイバーテロの発生を想定した共同訓練やサイバーテロ対策セミナーを実施し、サイバー攻撃のデモンストレーションや事案対処シミュレーション等を行うことにより、緊急対処能力の向上に努めている。

このほか、警察では平素から、事業者等に対し、事案発生時における警察への通報を要請するとともに、我が国の事業者等に対するサイバー攻撃の呼び掛け等を警察が認知した場合は、攻撃対象とされた事業者等に対して速やかに注意喚起を行い、被害の未然防止を図っている。

（３）民間事業者と連携した対策

①　海外の偽サイト等(注1)に係る被害拡大防止対策

警察庁では、都道府県警察が相談等で受理した海外の偽サイト等のＵＲＬ等の情報を集約し、ウイルス対策ソフト提供事業者等に提供して、これらのサイトを閲覧しようとする利用者のコンピュータ画面に警告表示等を行う対策を平成25年12月に開始した。

②　民間事業者と連携したボットネット対策

25年7月、ウイルス対策ソフト提供事業者から、インターネットバンキングに係る不正送金事犯で悪用されているボットネット(注2)の指令サーバに関する情報が提供された。当該指令サーバのログを解析したところ、15,000以上ものＩＰアドレスからアクセスが行われていたことが判明した。そこで、これらのＩＰアドレスを管理する全国の約300の通信事業者等にこれらの情報を提供し、契約者を特定して注意喚起を行うよう依頼した。

③　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、24年7月から、警察では、民間事業者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、25年末までに、オンラインゲーム事業者や銀行等、全国で355事業者・団体と本協定を締結している。

注1：海外のサーバを通じてインターネット上に掲載された、実在する企業のサイトを模したサイトや、インターネットショッピングに係る詐欺や偽ブランド品販売を目的とするサイト
2：51頁参照

警察活動の最前線

インターネット回線の向こう側には

埼玉県警察本部生活安全部サイバー犯罪対策課
中村（なかむら）　和貴（かずき）　警部補

「貴方が罪を犯したのはインターネットの世界ではない。インターネット回線の向こう側には現実に泣いている人が存在する」

これは、インターネット上に偽サイトを作り、クレジットカード情報等をだまし取っていた犯人に向けて私が発した言葉です。

サイバー犯罪の犯人の多くは、現実感の希薄さから、罪悪感を持たず、インターネットの匿名性を盲信し、安易な考えで犯罪に手を染めています。この犯人の供述からも、「こんなことぐらいで捕まるなんて」という軽い気持ちが感じられました。

しかし、サイバー犯罪は、パソコンが行う仮想犯罪ではありません。人が行う現実の犯罪なのです。

サイバー犯罪捜査においては、犯人を捕まえることはもちろん、犯人に「インターネット回線の向こう側は現実世界である」ことを認識させ、現実に引き戻すことも重要な仕事の一つです。

また、高度な技術を悪用した組織的な犯罪も後を絶たず、これらの悪質なサイバー犯罪に立ち向かうには、一人の捜査員の力だけでは解決することはできません。今後、県内はもちろん、全国の捜査員と連携し、切磋琢磨することで、インターネットを悪用する犯人を検挙し、皆さんが安心して使える安全なインターネット空間を実現していきたいと思っています。

サイバー攻撃の現状を目の当たりにして

近畿管区警察局兵庫県情報通信部情報技術解析課
大西（おおにし）　健一（けんいち）　技官

私は、情報技術解析部門の一員として、兵庫県警察サイバー攻撃特別捜査隊と協力して、県内のサイバーテロ・サイバーインテリジェンス対策に取り組んでいます。普段は、県内重要インフラ事業者等への個別訪問や、セキュリティセミナーの開催等によりセキュリティ意識の向上を図るなど、サイバー攻撃の未然防止を図りながら有事に備えています。

平成25年9月、海外の掲示板に日本の各政府機関を含む国内ウェブサーバへの攻撃を示唆する書き込みがありました。この事案では、サイバー攻撃特別捜査隊と連携した情報の収集及び収集した情報の解析を行い、日本に対し行われているサイバー攻撃手法の一部を解明しました。また、同時期に起きたホームページの改ざん事案では、改ざん前から、不特定多数の者がサーバへ不正アクセスしていることや、多くの不正なファイルが置かれていることを確認し、サイバー攻撃の現状を目の当たりにしました。

現在、サイバー空間は、目に見えるサイバーテロ、目に見えないサイバーインテリジェンスが活発に行われ、現実社会における警察活動に匹敵するほどの取組がサイバー空間でも望まれています。私は、知見の限りを尽くし、サイバー空間における治安の維持を守る一員として、安全・安心な社会の実現に寄与したいと思います。

注：掲載されているキャラクターは、都道府県警察のマスコットキャラクターです。