サイバー空間の安全の確保

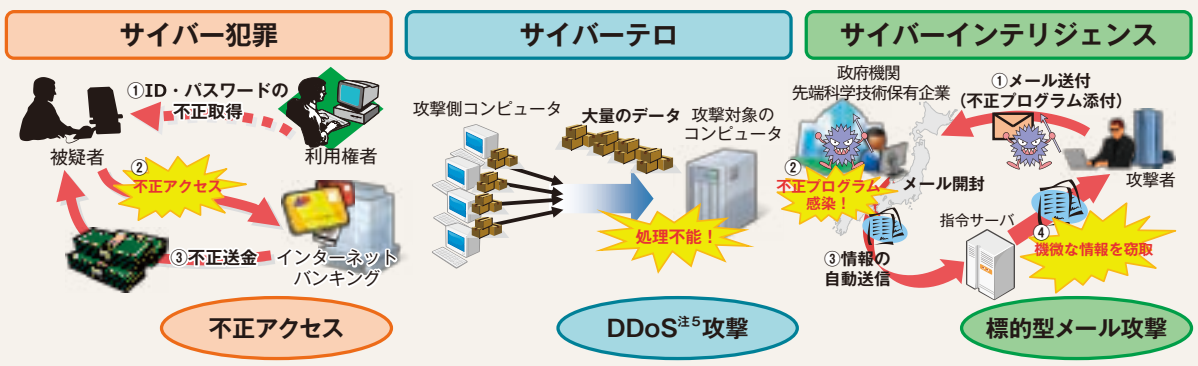
第３章
CHAPTER 3

第1節 サイバー空間の脅威

1 サイバー空間をめぐる脅威の特徴

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。平成26年中は、インターネットバンキングに係る不正送金事犯や標的型メール攻撃等における手口の悪質・巧妙化や、悪質な中継サーバを始めとするサイバー空間における犯罪インフラの存在が確認された。また、個人がウェブサイトからダウンロードした銃の設計図を基に3Dプリンタを用いて手製拳銃を製造する事件が発生するなど、サイバー空間とつながりを持ち、犯罪のツールとして悪用される危険をはらんだ新たな技術・サービスの出現や、不正ログイン攻撃、インターネットを通じた私事性的画像記録の提供による被害等、インターネットの利用によって犯罪に巻き込まれるリスクの拡大といった特徴もみられた。警察では、このようなサイバー空間をめぐる脅威の情勢を的確に見定め、適切な対策を講じていくこととしている。

図表3－1 サイバー空間をめぐる脅威



事例 Case

26年11月、米国ソニー・ピクチャーズ・エンターテインメントが、不正プログラムによるシステムの破壊を伴うサイバー攻撃を受けたことが判明した。本攻撃により、数千台のコンピュータが動作不能となり、同社の企業活動が阻害されるとともに、従業員の個人情報等が窃取された。FBI(注6)は、本攻撃で使用されたツールが、25年３月に発生した韓国の銀行等に対するサイバー攻撃事案(注7)において使用されたものと類似していることや、不正プログラム内に記録されていたIPアドレスと北朝鮮のインフラに関連がみられることなどから、北朝鮮政府が本件攻撃に責任を有すると結論付けたことなどを発表した。


サイバー攻撃を受けたコンピュータに表示された画像

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
２～４：128頁参照
５：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
６：Federal Bureau of Investigation（米国司法省連邦捜査局）の略
７：韓国政府は北朝鮮の関与を指摘している。

2 サイバー犯罪の情勢

（1）サイバー犯罪の検挙状況

平成26年中のサイバー犯罪の検挙件数は7,905件と、前年より208件（2.6%）減少した。

① 不正アクセス禁止法違反

26年中の不正アクセス禁止法（注1）違反の検挙件数は364件と、前年より616件（62.9%）減少した。一方、検挙人員は170人と、前年より23人（15.6%）増加した。

② コンピュータ・電磁的記録対象犯罪等

26年中の刑法に規定されている不正指令電磁的記録に関する罪（コンピュータ・ウイルスに関する罪）及びコンピュータ又は電磁的記録を対象とした犯罪の検挙件数は192件と、前年より286件（59.8%）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28件であった。

③ ネットワーク利用犯罪（注2）

26年中のネットワーク利用犯罪の検挙件数は7,349件と、前年より694件（10.4%）増加し、過去最多となった。特徴として、オークション利用詐欺の検挙件数が381件と、前年より223件（141.1%）増加する一方、出会い系サイト規制法（注3）違反の検挙件数は279件と、前年より60件（17.7%）減少した。

図表３－２ サイバー犯罪の検挙件数の推移（平成22～26年）

区分＼年次	22	23	24	25	26
合計(件)	6,933	5,741	7,334	8,113	7,905
不正アクセス禁止法違反	1,601	248	543	980	364
コンピュータ・電磁的記録対象犯罪等	133	105	178	478	192
ネットワーク利用犯罪	5,199	5,388	6,613	6,655	7,349
児童買春・児童ポルノ禁止法違反（児童ポルノ）	783	883	1,085	1,124	1,248
詐欺	1,566	899	1,357	956	1,133
うちオークション利用詐欺	677	389	235	158	381
わいせつ物頒布等	218	699	929	781	840
著作権法違反	368	409	472	731	824
青少年保護育成条例違反	481	434	520	690	657
児童買春・児童ポルノ禁止法違反（児童買春）	410	444	435	492	493
脅迫	67	81	162	189	313
商標法違反	119	212	184	197	308
出会い系サイト規制法違反	412	464	363	339	279
その他	775	863	1,106	1,156	1,254

事例 Case

自営業の男（43）らは、女性を装ってチャットサイトで知り合った被害者に、画像閲覧用のアプリと偽って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・ウイルスをダウンロードさせ、電話帳データを窃取した。また、同被害者が送信したわいせつな動画を「抜き取った電話帳データを使ってばらまく」などと言って脅し、現金20万円を喝取した。26年４月、同自営業の男ら２人を不正指令電磁的記録供用罪及び恐喝罪で逮捕した（千葉）。

注１：不正アクセス行為の禁止等に関する法律
２：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
３：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

3 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、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1）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（注2）の基幹システム（注3）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。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は発生していないが、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。

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。

事例 Case

平成27年４月、フランスの国際放送局が、ISILの賛同者とみられる「CyberCaliphate」と称する者によるサイバー攻撃を受けた。

この攻撃により同局の番組が放送できない状態となったほか、公式ウェブサイトや同局のSNSアカウントが一時的に乗っ取られ、フランス軍のISILに対する空爆を非難する声明文等が同ウェブサイトや同局のアカウントに掲示される被害が発生した。

フランス政府は、この攻撃の犯人を特定し起訴するために全力を尽くすと表明し、捜査を進めるとともに、国内メディアの幹部を集めた会議を開催し、通信ネットワーク等のセキュリティに関する警戒レベルを引き上げる必要性を指摘した。

放送不可能となったフランスの国際放送局

乗っ取られた国際放送局のSNSアカウント

注１：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
２：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
３：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

（2）サイバーインテリジェンスの情勢

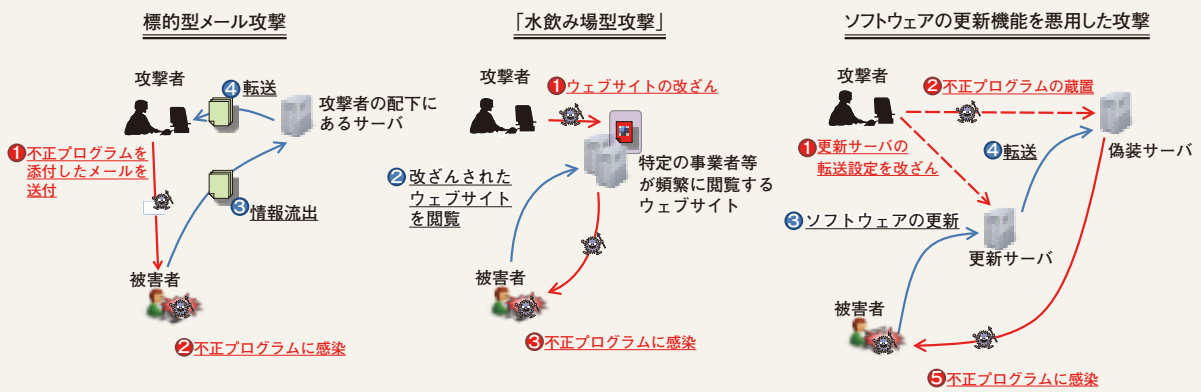
近年、情報を電子データの形で保有することが一般的となっている中、軍事技術への転用も可能な先端技術や、外交交渉における国家戦略等の機密情報の窃取を目的として行われるサイバーインテリジェンスの脅威が、世界各国で問題となっている。

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。

最近の標的型メール攻撃の傾向としては、近年減少傾向にあった「ばらまき型」攻撃が平成26年下半期に急増しており、その内容としては、商品代金請求等の業務上の連絡を装った英文のものが多くみられる。また、日本の制度を踏まえて受信者が違和感を感じにくい内容のメールを送信するなど、手口がより巧妙化しており、例えば、企業等の健康保険組合からの医療費の通知を装った手口が新たに確認された。標的型メール攻撃の送信先アドレスについては、インターネット上で公開されていないものが約７割を占めていることから、攻撃者が対象組織や職員について深く調査し、周到な準備を行った上で攻撃を実施していることがうかがわれる。

こうした標的型メール攻撃のほか、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手口による「水飲み場型攻撃」や、無償ソフトウェアの更新機能を悪用して不正プログラムに感染させるといった攻撃も発生するなど、サイバー攻撃の手口はますます巧妙化・多様化している。

図表３－３　サイバーインテリジェンスの手口



事例 Case

26年１月、福井県に所在する独立行政法人（現：国立研究開発法人）日本原子力研究開発機構において、高速増殖原型炉「もんじゅ」の発電課当直員が使用する事務処理用パソコンが、動画再生用ソフトウェアの更新機能を悪用した手口により不正プログラムに感染したことが判明した。その後の調査により、パソコン内のファイルやフォルダの名称や、ユーザーアカウント名等のデータが窃取されたことが明らかになった。

事例 Case

26年９月、法務省民事局及び法務局のサーバ等が不正アクセスを受けたことが判明した。その後の調査の結果、当該不正アクセスにより、法務省が業務上保有する情報の一部が外部に送信された可能性があることが明らかになった。

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

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。

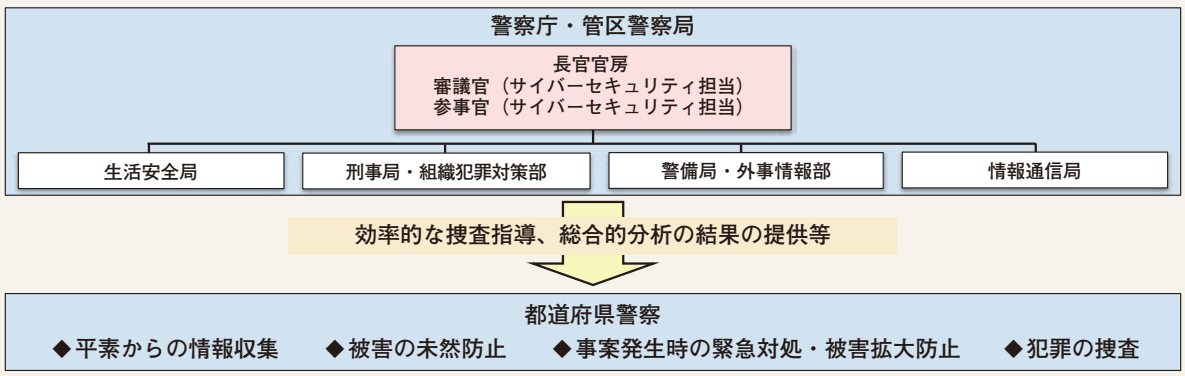
（1）サイバーセキュリティ対策の司令塔機能の強化

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

といった取組を推進している。

図表３－４ 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重点施策の策定

警察では、平成25年１月、当面緊急に推進すべき施策として、「サイバー犯罪対処能力の強化等に向けた緊急プログラム」を策定し、各種施策を推進してきたが、同プログラムの策定から時間が経過したことから、警察庁では、新たな手口や技術の出現等、サイバー空間をめぐる最近の情勢を踏まえ、今後注力して取り組むべき施策として、26年９月、「サイバーセキュリティ重点施策2014-2015」を策定した。

今後、新たな産学官連携の枠組みとして業務を開始したJC3 (注) 等との連携による情報収集・分析や、事後追跡可能性の確保に向けた施策等を着実に実施し、サイバー空間の安全・安心の確保に努めることとしている。

注：53頁参照

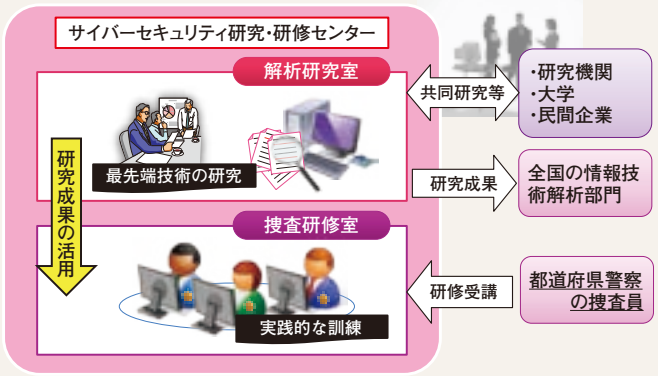
（３）サイバーセキュリティ研究・研修センターの取組

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。

①　情報技術解析の高度化・効率化に資する研究

解析研究室では、外部の研究機関等と共同研究を行うなど、民間の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っている。このほか、電子機器等の解析手法の確立に向けた研究も行うなど、警察・民間双方の知見を融合・活用した研究活動を展開している。

図表３－５　サイバーセキュリティ研究・研修センター



②　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

捜査研修室では、解析研究室で得られた研究成果を踏まえて、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っている。

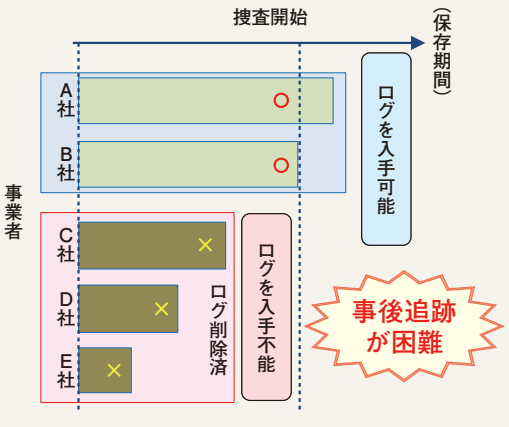
コラム　通信履歴等（ログ）の保存について

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なものである。しかし、我が国では、プロバイダ等の事業者において、ログを平素から保存しなければならないこととする制度が存在しないため、犯人の追跡が困難になるなど、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。

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」、26年11月に成立した私事性的画像記録の提供等による被害の防止に関する法律の附則等において、ログの保存の在り方について検討を行うこととされていた。

ログの保存が許容される期間を具体的に例示することを内容とする総務省による「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」の解説の改正を踏まえ、警察庁では、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。

図表３－６　サイバー犯罪捜査等における事後追跡上の課題



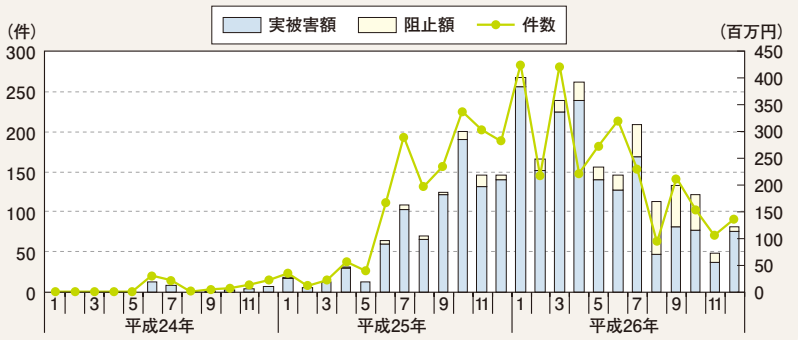
2 サイバー犯罪への対策

（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23年から24年にかけて減少したが、25年に約14億600万円と急増し、26年は過去最多となる約29億1,000万円となった。また、26年は、多くの地方銀行や信用金庫等に被害が拡大したほか、法人名義口座に係る被害も増加するなど、深刻な状況にある。

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月別発生件数の推移（平成24～26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、平成26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や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計233人を検挙している。

イ 民間事業者等と連携した抑止対策

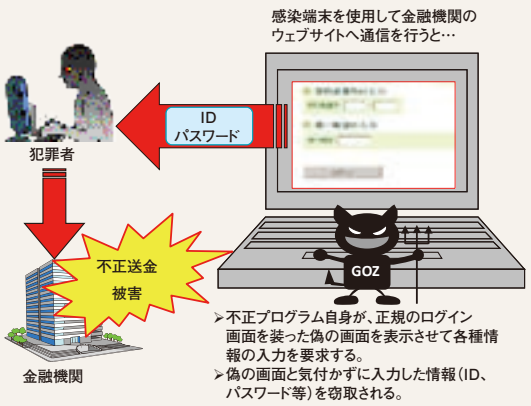
警察では、金融機関に対するインターネットバンキングのセキュリティ機能強化のための注意喚起、不正送金に悪用される口座を凍結するための口座情報・凍結口座名義人情報の提供、資金移動業者への国外送金の審査強化に関する働き掛け等を行っている。

また、ウイルス対策ソフト事業者との情報交換を通じて、不正送金事犯に悪用されているボットネット（注１）の情報を入手し、金融機関と連携した口座停止措置を行うなどの対策を行っている。

コラム 国際的なボットネットのテイクダウン作戦

不正送金事犯に使用されているとみられる不正プログラム「Game Over Zeus」が世界的にまん延した（注２）ことから、26年５月、FBI及びEUROPOL（注3）を中心に、日本を含む協力国の法執行機関が連携して同プログラムに感染した端末の情報を収集し、当該端末を特定した上で、プロバイダ等を通じて当該端末の利用者に対して不正プログラムの駆除を促し、ネットワークを崩壊させる「国際的なボットネットのテイクダウン作戦」を決行した。

図表３－８ Game Over Zeusの脅威



注１：攻撃者の命令に基づき動作する不正プログラム（ボット）に感染したコンピュータ及びこれらのコンピュータに攻撃者の命令を送信する命令サーバから成るネットワーク
２：不正プログラムに感染した端末が世界中に50～100万台存在し、そのうち約20％が日本に所在しているとされる。
３：European Police Office（欧州刑事警察機構）の略

（2）コンピュータ・ウイルス対策

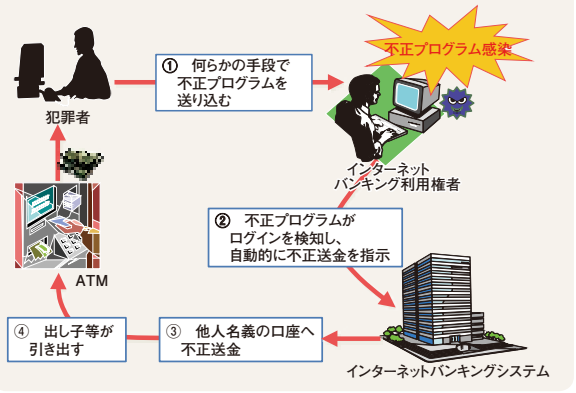
警察では、コンピュータ・ウイルスに関する罪の取締りを推進するとともに、民間事業者と連携したコンピュータ・ウイルスによる被害拡大防止のための対策を講じている。

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１）を構築している。

コラム MITB攻撃による不正送金

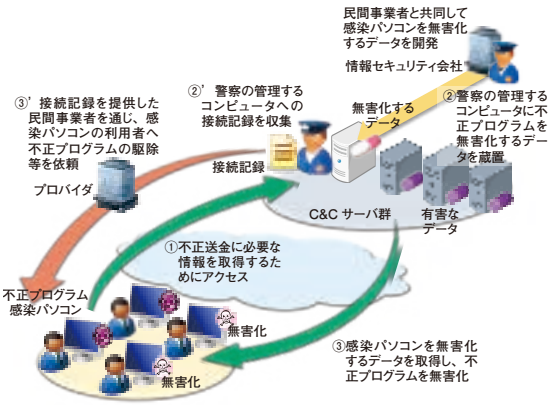
平成26年中に過去最大の被害額を記録したインターネットバンキングに係る不正送金事犯について、海外では以前から多くの被害をもたらしていたMITB（注２）攻撃と呼ばれる手口による被害が同年上半期に国内で初めて確認された。この手口は、パソコンに感染した不正プログラムが、正規の利用権者がインターネットバンキングへログインしたことを検知し、自動的に他人名義の口座へ不正送金するものである。

図表３－９　MITB攻撃の概要



コラム インターネットバンキングに係る不正送金事犯に係る不正プログラムによる被害の拡大防止措置

平成27年４月、警視庁は、インターネットバンキングに係る不正送金に利用されるC&Cサーバ（注３）の動作を観測することにより、国内外において約８万2,000台の端末がワンタイムパスワード（注４）の入力を誘導するための入力画面を表示させ、不正送金を自動で行うといった機能を有する不正プログラムに感染していることを把握したことから、被害の拡大防止措置を実施した。



具体的には、プロバイダを通じた国内の感染端末の利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供に加え、画期的な被害拡大防止措置として、不正プログラムの無害化措置にも成功した。

不正プログラムの無害化については、C&Cサーバと定期的に通信を行うことで不正送金に必要な情報を入手するというこの不正プログラムの性質を逆手に取り、その代わりに無害なデータを取得させることにより行われた。

注１：140頁参照
２：Man In The Browserの略。あたかも人がウェブブラウザの中で監視を行っているかのように、不正プログラムが不正な通信を行うもの。
３：Command and Control serverの略。攻撃者の命令に基づいて動作する不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと
４：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、識別符号が盗まれても次回の利用時に使用できないこととなる。

（3）不正アクセス対策

①　発生状況の公表

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ず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1）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2）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。

（4）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

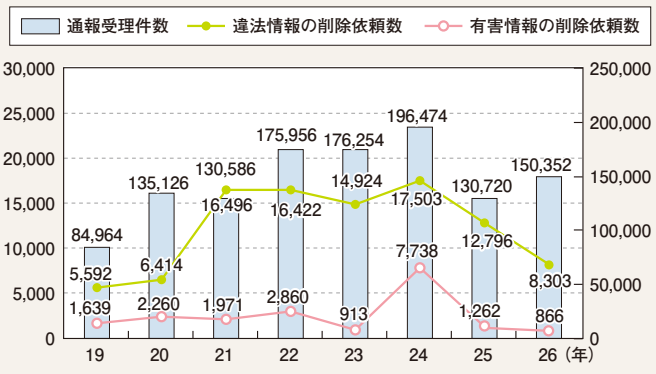
インターネット上には、児童ポルノ画像や覚醒剤等規制薬物の販売に関する情報等の違法情報や、違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない有害情報が氾濫している。

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。26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7,890件が、有害情報については564件が削除された（削除率は、それぞれ95.0%、65.1%）。

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3）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19～26年）



注１：23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
２：http://www.ipa.go.jp/security/kokokara/
３：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。11年に設立され、27年3月末現在、IHCを含む51団体（45の国・地域）から成る国際組織

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１）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。

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。

（５）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への対策

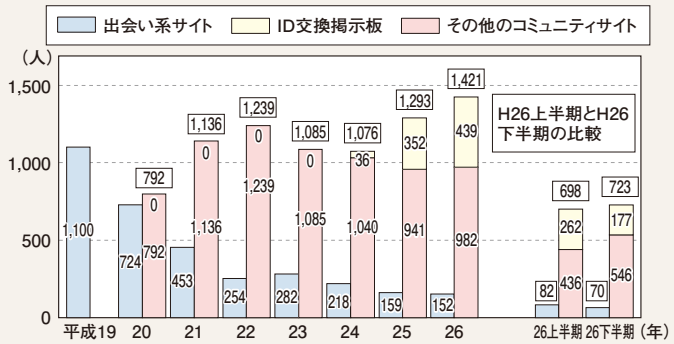
①　出会い系サイト及びコミュニティサイトに起因する事犯の発生状況

出会い系サイト（注２）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、届出制の導入により事業者の実態把握が促進されたことや、事業者の被害防止措置が義務化されたことなどにより減少傾向にある。一方、コミュニティサイト（注３）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年以降、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等が増加したことにより、増加傾向にある。

②　出会い系サイト及びコミュニティサイトへの対策

警察では、出会い系サイトに起因する児童被害の防止に向けた対策として、悪質出会い系サイト事業者や禁止誘引行為等の書き込み違反者に対する取締り等を徹底している。また、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、サイト事業者の規模や提供しているサービスの態様に応じて、ミニメール（注４）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５）の導入に向けた働き掛けを推進している。

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に係る被害児童数の推移（平成19～26年）



※コミュニティサイトの統計は平成20年から取り始めた。

さらに、出会い系サイト及びコミュニティサイトにおいて、サイバー補導（注６）を実施しているほか、関係省庁、事業者及び関係団体と連携し、スマートフォンを中心としたフィルタリングの普及徹底や児童、保護者、学校関係者等に対する児童被害の防止に関する広報啓発を推進している。

（６）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199団体（平成26年12月末現在）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：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。
２：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
３：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
４：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
５：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利用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
６：107頁参照

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、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。

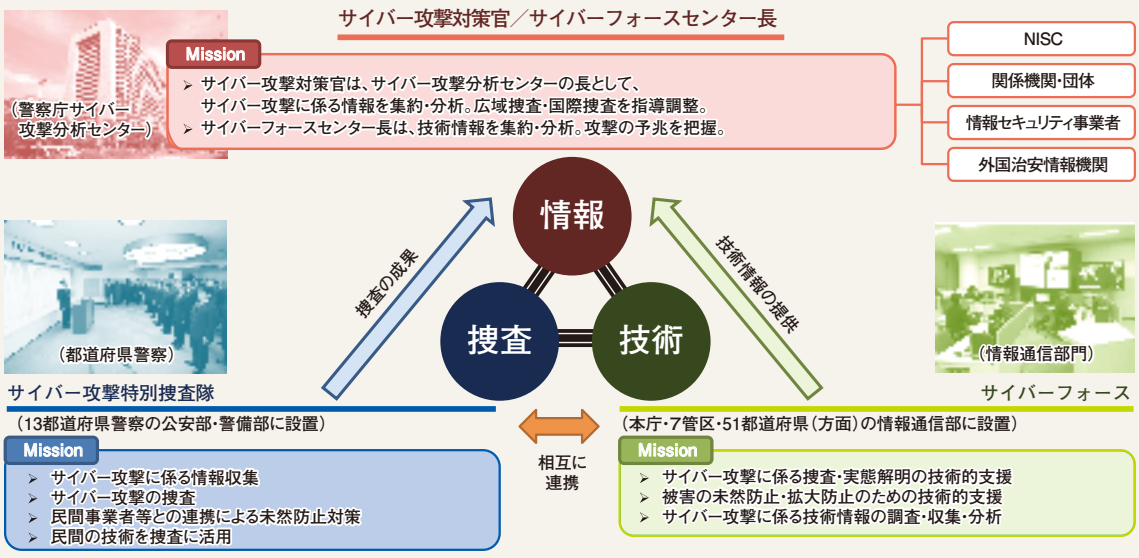
（1）サイバー攻撃対策の推進体制

警察庁では、サイバー攻撃対策官が、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、これ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13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、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、サイバー攻撃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。平成26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、共同対処訓練を複数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



注：National center of Incident readiness and Strategy for Cybersecurity（内閣サイバーセキュリティセンター）の略。情報通信ネットワーク又は電磁的記録媒体を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析、行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明のための調査等を行う機関。

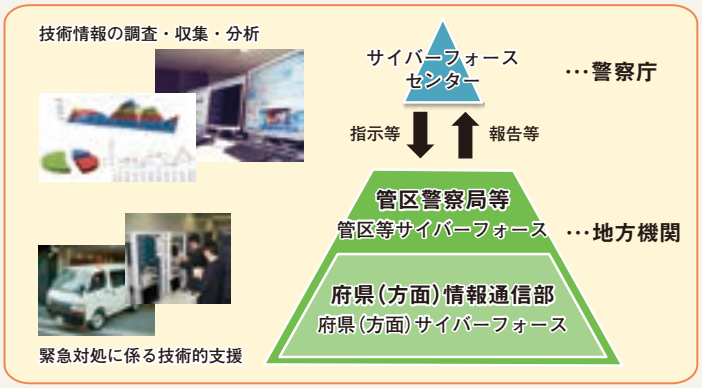
（2）実態解明の推進

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

図表３－14　サイバーフォースの体制



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。

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２）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、警察庁セキュリティポータルサイト「@police」（注３）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　平成26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26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３分に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、26年中は、インターネットショッピング、インターネットバンキング等で幅広く使用される通信の暗号化等のセキュリティを確保するためのソフトウェアであるOpenSSLに深刻なぜい弱性があることが明らかとなり、このぜい弱性が存在するサーバ等を探索していると考えられるアクセスを断続的に検知した。このぜい弱性が悪用された場合には、暗号に用いる秘密鍵、パスワード等のサーバ内の重要な情報が漏えいするおそれがある。このような被害を防止するためには、サーバの管理者が、ぜい弱性が存在する旧バージョンのOpenSSLを使用しているサービスがないかを確認し、存在する場合にはアップデートを速やかに実施するなど、適切なセキュリティ対策を行うことが重要である。

注１：93頁参照
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：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、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（注1）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　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。特に、その記憶容量の増大、アプリの多様化・複雑化を踏まえ、警察では、関係機関と連携して解析手法の開発を行うなど、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

近年、最先端の技術が導入された海外製電子機器の解析や社会経済活動に大きな影響を与えるサイバー攻撃への対応が求められている。そこで、警察では、最新の電子機器や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（注2）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、匿名化通信技術（注3）等の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。

③　海外研究機関への職員派遣

警察では、国内における取組にとどまらず、電子機器の解析や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海外の研究機関に職員を派遣し、海外製電子機器からのデータの抽出手法や最新の不正プログラムの解析手法、今後悪用され得る情報システムやインターネット上のサービスに関する調査及び研究を実施し、最先端の技術の取得に努めている。

注1・2：93頁参照
3：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

5 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、G7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。

ベトナムにおける協議の様子

また、日米サイバー対話や日・ASEANサイバー犯罪対策対話等の政府横断的な代表が参加する国際会議にも積極的に参加している。

さらに、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。特に、技術協力の推進を目的とした意図表明文書に署名しているNFI（注5）との間では、情報交換を行うなどして、緊密な関係を築いている。

加えて、アジア大洋州地域サイバー犯罪捜査技術会議を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。26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FBIやアイルランドダブリン大学、国内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、情報技術解析に関する演習等を実施した。

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、26年には海外にリエゾンオフィサーを派遣した。

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。
2：37頁参照
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」等に基づき設置されたもので、27年５月現在、70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。なお、26年3月より、G7として実施している。
5：Netherlands Forensics Institute（オランダ国立法科学研究所）の略

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）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。

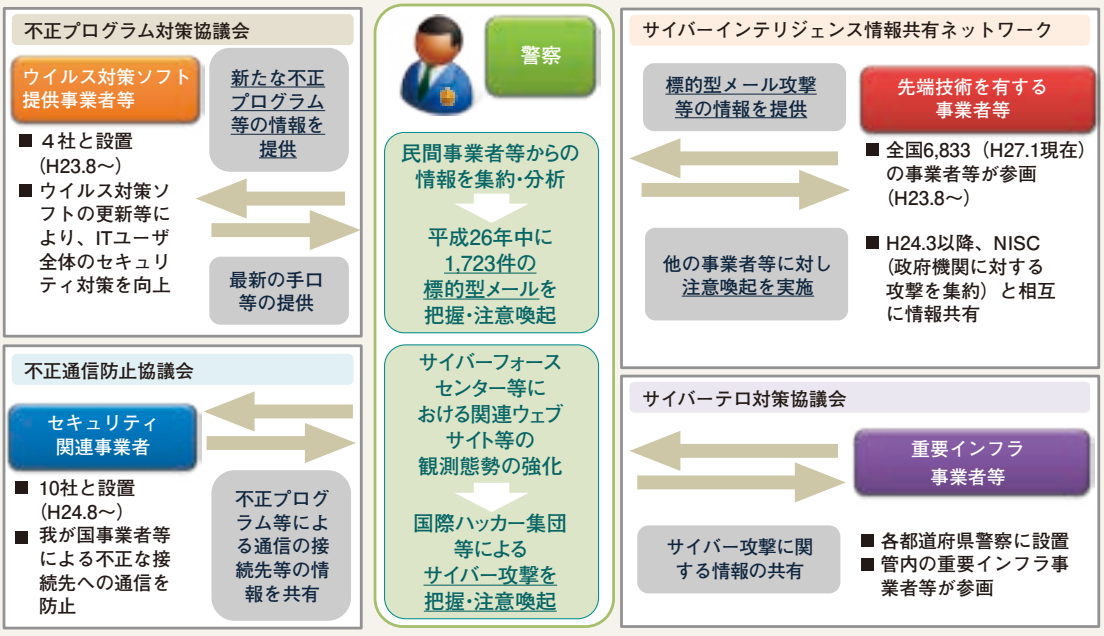
② 不正通信防止協議会

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6,833の事業者等（平成27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。

図表3－16 官民連携のための枠組み



④　サイバーテロ対策協議会

警察は、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攻撃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、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃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。

サイバー攻撃の発生を想定した共同対処訓練

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。

（２）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　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、26年末までに、オンラインゲーム事業者や銀行等、全国で468事業者・団体と本協定を締結している。

③　民間事業者と連携したボットネット対策

25年10月、サイバー犯罪に対する共同対処協定を締結している民間事業者から、インターネットバンキングに係る不正送金事犯に利用されるC&Cサーバ（注２）が国内に存在する旨の情報が提供された。同サーバのデータを入手して解析したところ、不正に入手したとみられるID・パスワード等の口座情報が大量に保存されていることが判明したことから、26年３月までに、約１万3,000件の当該口座情報を全国の16金融機関に提供し、当該口座情報に係るインターネットバンキングの利用を停止するように要請した。

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
２：133頁参照

警察活動の最前線

安心・安全なサイバー空間の実現を目指して

和歌山県警察本部生活安全部生活環境課
サイバー犯罪対策室
岡本（おかもと）　進吾（しんご）　警部補

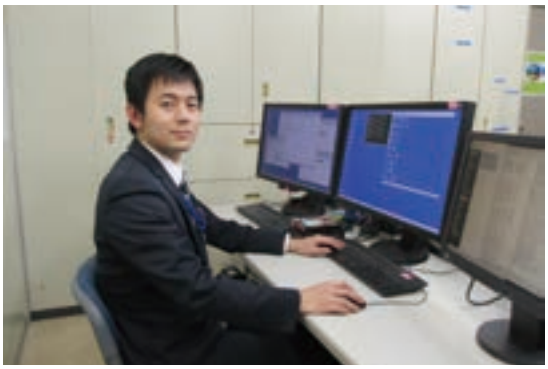
私が初めてサイバー犯罪の捜査に携わっていた平成15年当時は、まだ「ハイテク犯罪」という名称が一般的な時代でした。この10年ほどでスマートフォンの爆発的な普及等を通じてインターネットはさらに国民の生活に浸透し、一方でこれを悪用した犯罪についても、手口の巧妙化が進み、犯人を特定することが困難になっています。

最近では、発信元を匿名化するソフトを使用した威力業務妨害、脅迫事件の捜査に携わりました。この事件では、犯人の発信元につながる情報が完全に偽装されていたことから、捜査は困難を極めましたが、紙にして１万ページにも及ぶ膨大な通信記録を１つ１つ緻密に精査することで、犯人を検挙することができました。サイバー犯罪捜査といえば、一見華やかな印象を受けますが、実際には、姿の見えない犯人を追い詰めるため、電子機器の解析や通信記録の精査等の地道な捜査を粘り強く行うことが要求されるのです。

これからも、巧妙化するサイバー犯罪に対応するため、新たな技術や知識を習得し、一人でも多くの皆さんが安心・安全なサイバー空間を実感できるよう、サイバー犯罪の検挙・撲滅を目指したいと思います。

サイバー攻撃対策に向けた取組について

東京都警察情報通信部情報技術解析課
貞包（さだかね）　篤（あつし）　技官



私は現在、サイバー攻撃対策プロジェクトの一員としてサイバーテロ、サイバーインテリジェンス対策に取り組んでいます。サイバー空間上の治安を維持するためには、民間事業者の協力が必要不可欠であることから、普段は都内の重要インフラ事業者に対して、情報セキュリティ対策に対する助言、不正プログラムの感染等のインシデント対策の訓練や情報セキュリティに関する講演を行っています。

平成26年中は特に、インターネットで広く利用されている様々なソフトウェアに、サイバー攻撃に結びつくおそれのある重大なぜい弱性が次々に発見されました。このぜい弱性による被害を防止するため、事業者を個別に訪問し、ぜい弱性がもたらす危険について丁寧に説明を行い、これに迅速に対処するための組織づくりを促すことで、重大事案の発生を防ぐことができました。このように、一つ一つの活動はとても地道なものですが、現実の世界での地道な取組が、サイバーテロの防止には不可欠なのです。

サイバー空間をめぐる情勢は常に変化しており、安全への対策にもゴールはありません。そのような環境にあるからこそ、サイバー空間の治安を守る一員として、官民一体となった取組を通じて社会の安全の実現に寄与していきたいと思っています。

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。