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2)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。

図表３－１ サイバー空間をめぐる脅威

注：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

（１）サイバー犯罪の検挙状況

平成27年中のサイバー犯罪の検挙件数は8,096件と、前年より191件（2.4%）増加した。

不正アクセス禁止法(注3)違反の検挙件数は373件と、前年より９件（2.5%）増加した。また、検挙人員は173人と、前年より３人（1.8%）増加した。

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240件と、前年より48件（25.0%）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45件であった。

ネットワーク利用犯罪の検挙件数は7,483件と、前年より134件（1.8%）増加した。

図表３－２ サイバー犯罪の検挙件数の推移（平成23～27年）

区分＼年次	H23	H24	H25	H26	H27
合計（件）	5,741	7,334	8,113	7,905	8,096
不正アクセス禁止法違反	248	543	980	364	373
コンピュータ・電磁的記録対象犯罪等	105	178	478	192	240
ネットワーク利用犯罪	5,388	6,613	6,655	7,349	7,483
児童買春・児童ポルノ禁止法違反（児童ポルノ）	883	1,085	1,124	1,248	1,295
詐欺	899	1,357	956	1,133	951
うちオークション利用詐欺	389	235	158	381	511
わいせつ物頒布等	699	929	781	840	835
著作権法違反	409	472	731	824	693
青少年保護育成条例違反	434	520	690	657	593
児童買春・児童ポルノ禁止法違反（児童買春）	444	435	492	493	586
脅迫	81	162	189	313	398
商標法違反	212	184	197	308	304
出会い系サイト規制法違反	464	363	339	279	235
その他	944	1,268	1,345	1,567	1,593

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
２：18頁参照
３：不正アクセス行為の禁止等に関する法律

（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。我が国では、これまで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。

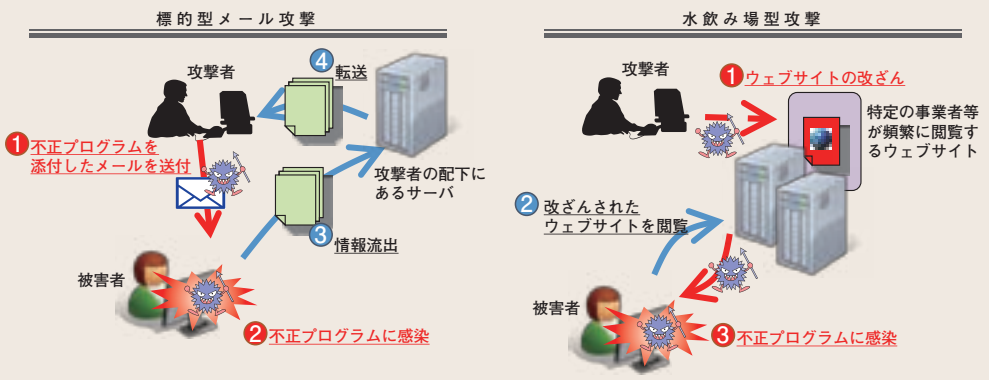
②　サイバーインテリジェンスの情勢

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、我が国に対する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。

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手口によ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。

図表３－３　サイバーインテリジェンスの手口



事例 Case

平成27年６月、アメリカの政府職員の個人情報を管理する米国連邦人事管理局は、サイバー攻撃により、政府職員等に関する氏名、住所、社会保障番号等の個人情報420万人分が流出したと発表した。

さらに、同年７月、その後の調査の結果、政府職員等約2,150万人分の個人情報が流出していたことが新たに判明した。

事例 Case

27年６月、日本年金機構に対するサイバー攻撃により、同機構が保有する個人情報の一部が流出したことが判明した。また、同事案の発生が判明した後、我が国の複数の機関、団体、民間企業等において、同種の被害が発生していたことが明らかとなった。

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。

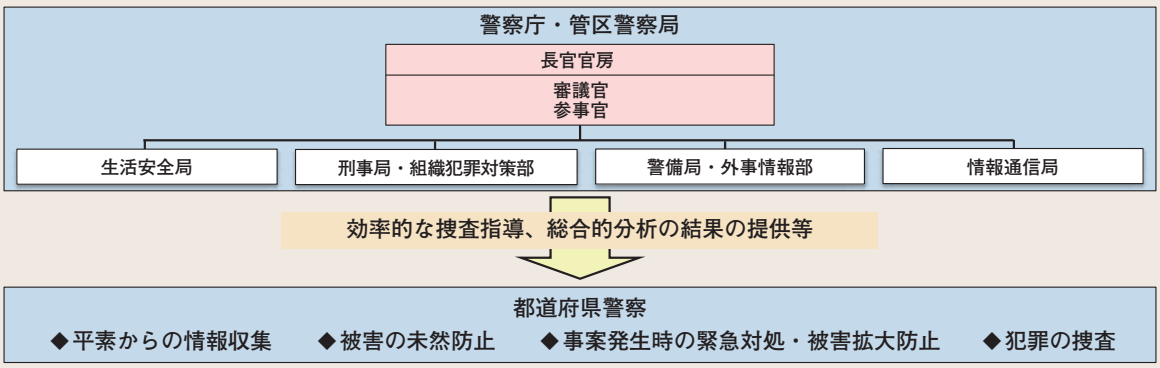
（1）サイバーセキュリティ対策の司令塔機能の強化

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・調整を行う長官官房審議官及び長官官房参事官を設置している。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。

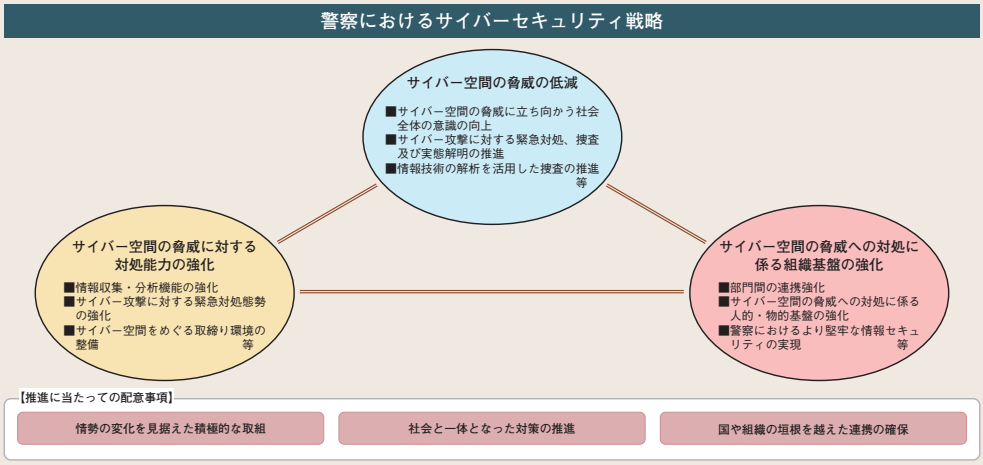
図表３－４ 警察におけるサイバー空間の脅威への対処態勢



（2）警察におけるサイバーセキュリティ戦略の制定

警察庁では、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、平成27年９月、「警察におけるサイバーセキュリティ戦略」を制定した。警察では、同戦略に基づき、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くこととしている。

図表３－５　警察におけるサイバーセキュリティ戦略の概要

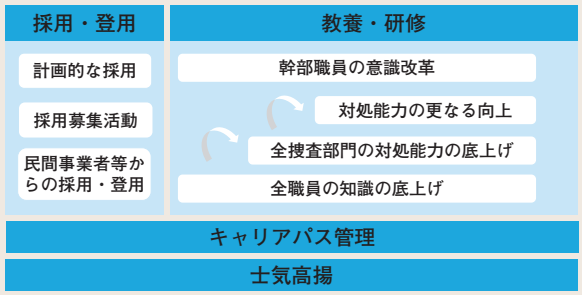


（３）サイバー空間の脅威への対処に係る組織基盤の強化

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12月に策定した「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、教養・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することで、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３－６　サイバー空間の脅威への対処に係る人材育成



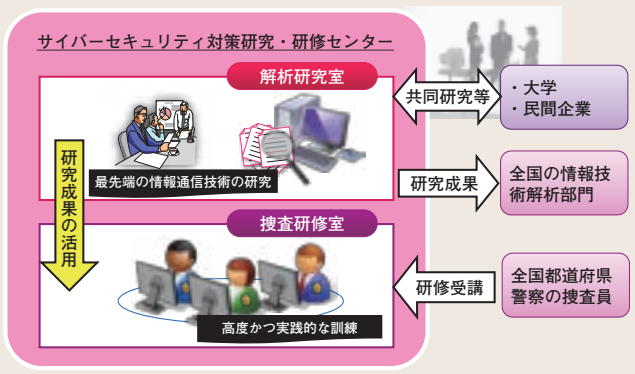
②　サイバーセキュリティ対策研究・研修センターの取組

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　情報技術の解析の高度化・効率化に資する研究

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、警察外部の機関との共同研究を行うなど、警察・民間双方の知見を融合・活用した研究活動を行っている。

図表３－７　サイバーセキュリティ対策研究・研修センター



イ　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

捜査研修室においては、解析研究室で得られた研究成果を活用しつつ、全国の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高度かつ実践的な訓練等を行っている。

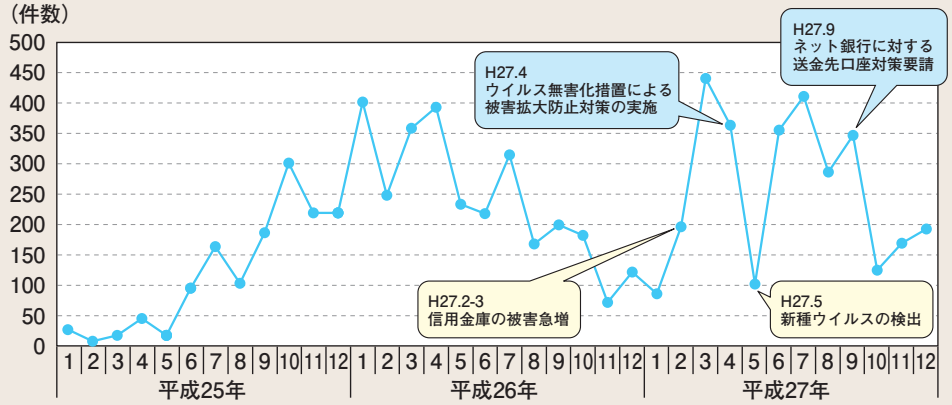
2 サイバー犯罪への対策

（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25年に約14億600万円と急増し、26年は約29億1,000万円となった。26年下半期は被害がやや減少していたものの、27年上半期は再び増加に転じ、27年中の被害額は約30億7,300万円で、過去最高となった。また、27年は、信用組合、農業協同組合等に被害が拡大し、特に信用金庫の法人名義口座に係る被害が急増したほか、４月以降は都市銀行での被害が多発するなど、深刻な状況にある。このほか、不正送金先の口座名義人については中国籍の者の割合が高いことが特徴として挙げられる。

図表３－８　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状況の推移（平成25～27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、27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160人を検挙している。

イ　金融機関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、資金移動業者に対する国外送金の審査強化に関する働き掛け等を行っている。

（2）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。

（３）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、不正プログラムの無害化措置、ボットネット（注１）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」への参加、外国捜査機関と連携した不正プログラムの通信先サーバの停止等を行ったほか、サイバー犯罪に悪用される中継サーバへの対策を実施するなど、積極的な被害防止対策を推進している。

事例 Case

平成26年に検挙した中継サーバ事業者から押収したコンピュータから、大量のインターネットサイトのID・パスワード等を把握したことから、当該サイトの運営会社にID・パスワード等を提供し、不正アクセス事案等の未然防止を要請した（警視庁・埼玉）。

事例 Case

悪質な中継サーバへの対策として、警察庁及び警視庁が総務省及び大手通信事業者に対して、不正アクセス行為に使用された通信回線の契約の強制解約を要請した結果、27年12月、大手電気通信事業者が契約約款を改正し、要請に応じて契約を解除することとなった。

（４）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２）を構築している。

事例 Case

無職の少年（18）は、平成27年６月、人の電子計算機における実行の用に供する目的で、身代金要求型ウイルス「ランサムウェア（注３）」の作成ツールを保管した。27年８月、少年を不正指令電磁的記録保管罪で検挙した（警視庁）。

（５）不正アクセス対策

①　発生状況等

平成27年における不正アクセス行為の認知件数は2,051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1,531件（74.6%）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係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117件（35.2%）と最多であった。

図表３－９　不正アクセス行為に係る犯行手口の内訳の推移（平成26、27年）

区分＼年次	26	27
識別符号窃用型（注）（件）	336	331
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	84	117
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	34	57
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	47	51
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	53	46
フィッシングサイトにより入手したもの	71	24
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	6	15
他人から入手したもの	25	13
その他	16	8
セキュリティ・ホール攻撃型（件）	2	1
合計（件）	338	332

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４）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５）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。

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
２：132頁参照
３：感染したコンピュータの機能を制限し、その制限の解除と引き替えに金銭を要求するウイルス
４：23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
５：http://www.ipa.go.jp/security/kokokara/

（6）インターネット上の違法情報・有害情報対策

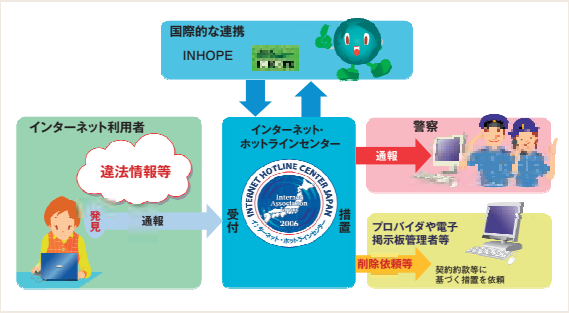
インターネット上には、児童ポルノ画像や覚醒剤等規制薬物の販売に関する情報等の違法情報や、違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない有害情報が氾濫している。

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）を運用している。平成27年中にIHCが削除依頼を行った違法情報のうち９割以上の３万359件が削除された。

通報された違法情報の中には、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、各国のホットライン相互間の連絡組織であるINHOPE（注１）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

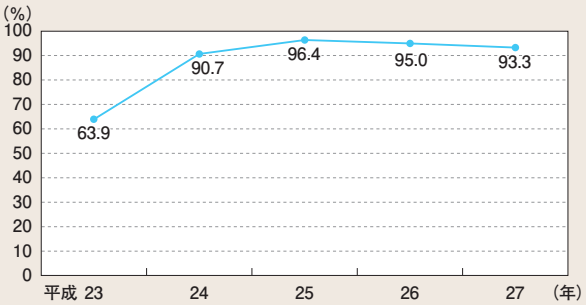


②　効果的な違法情報・有害情報の取締り

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。

また、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る。

図表３－11　インターネット・ホットラインセンターが削除依頼を行った違法情報の削除率の推移（平成23～27年）



（7）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３）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（注４）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５）に起因して犯罪被害に遭った児童の数は、平成20年以降増加傾向にある。また、27年中、フィルタリングの利用の有無が判明した被害児童のうち、９割以上がフィルタリングを利用していなかった。

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。11年に設立され、28年３月末現在、IHCを含む52団体（46の国・地域）から成る国際組織

２：IHCから警察庁に通報された違法情報について効率的な捜査を進めるため、違法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。23年７月から本格実施している。

３：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

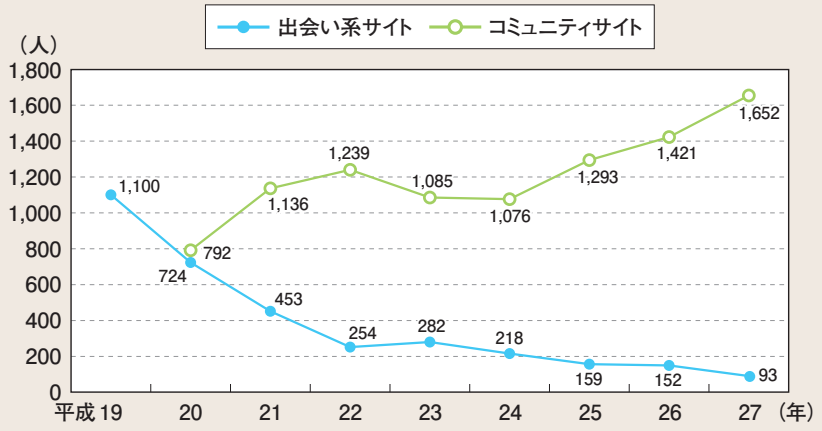
４：インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律

５：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

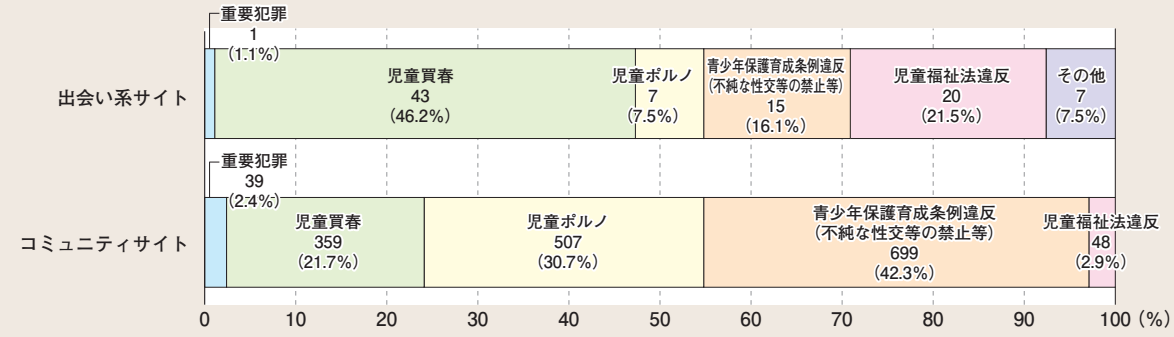
②　被害児童の状況

27年中、被害児童の最も多い罪種は、出会い系サイトに起因する事犯では、児童買春43人（全体の46.2%）、コミュニティサイトに起因する事犯では、青少年保護育成条例違反699人（全体の42.3%）となっている。

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の被害児童数の推移（平成19～27年）



図表３－13　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罪種別の被害児童数及び割合（平成27年）



事例 Case

大学生の男（34）は、27年１月及び同年２月の２回にわたり、コミュニティサイトで知り合った女子児童（15）が児童であることを知りながら、ホテルにおいて買春をした。27年４月、男を児童買春・児童ポルノ禁止法違反で逮捕した（警視庁）。

③　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１）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２）の導入に向けた働き掛けを推進している。

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３）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促進や児童、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と情報共有を推進している。

（８）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224団体（平成27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：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
２：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、大人と児童との間のミニメールの送受信や検索を制限すること
３：99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。

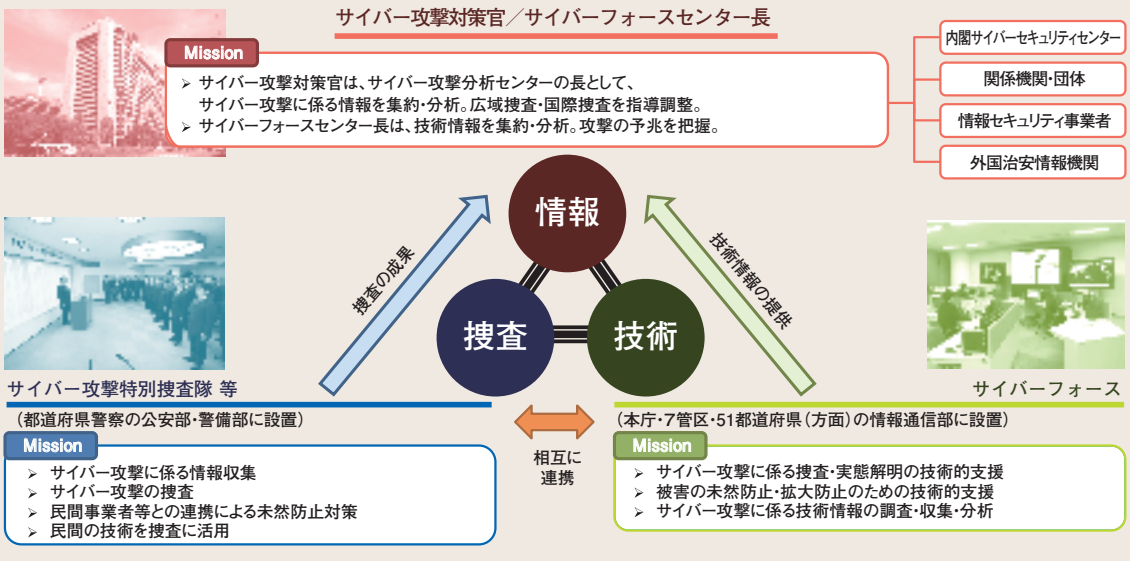
（1）サイバー攻撃対策の推進体制

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３－14　サイバー攻撃対策の推進体制



注：206頁参照

（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。

事例 Case

我が国の政府機関に対する不正アクセス事件に関して警視庁が捜査を進めたところ、犯行に使用されたレンタルサーバの契約に際し、当時日本に留学生として滞在していた中国人の男が、氏名、住所、生年月日等を偽って会員登録を行っていた事実が判明したことから、27年11月、同男を私電磁的記録不正作出・同供用罪により検挙した。また、同男は、これまで1,000台以上のレンタルサーバを契約した上、主に海外に居住する利用者に転売して利益を上げていたとみられ、転売されたレンタルサーバのなかには、他のサイバー攻撃において踏み台として悪用されたとみられるものが含まれていることから、実態の解明を進めている。

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１）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２）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27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27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２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、27年中は、インターネット接続が可能な家電等の機器を発信元とする不審なアクセスの増加が顕著であった。これらのアクセスを分析したところ、発信元の機器と同様のインターネットに接続された家電等の機器を主な標的として、不正プログラムに感染させることを企図したとみられる攻撃が行われていることが判明した。この攻撃を受けて家電等の機器が不正プログラムに感染すると、当該機器は攻撃者の命令に基づいて動作する「ボット」となり、不正プログラムの更なる感染拡大や、DoS攻撃等に悪用されるおそれがある。

今後、インターネット接続が可能な家電等の更なる普及に伴い、このような攻撃の脅威が一層高まると予想されることから、警察庁においては、これらの機器の利用者に対して、意図せず攻撃に加担しないよう、利用する機器のソフトウェアを最新に保つなど、適切なセキュリティ対策を講じるよう注意を呼びかけている。

注１：Denial of Serviceの略。特定のコンピュータに対し、大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃
２：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、情報通信技術の急速な進展に伴い、これを用いたサイバー攻撃への対応や、最先端の技術が導入された海外製電子機器の解析が求められている。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１）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対策研究・研修センターにおいて、匿名化通信技術（注２）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　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、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１：90頁参照
　２：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・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・サイバー攻撃に対処している。

（2）国際会議・協議等

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、平成27年中は、内閣府が主催したサイバーセキュリティに関する国際会議のほか、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た。

サイバーセキュリティに関する国際会議における国家公安委員会委員長の講演

また、日米サイバー対話や日中韓サイバー協議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。27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オランダ国家警察、FBI、エストニア法務省、国内外の学術機関等が参加し、不正プログラム等の解析技術や、サイバー犯罪対策に係る国際連携・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、27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。
２：216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11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

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7,333の事業者等（平成28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。

サイバー攻撃の発生を想定した共同対処訓練

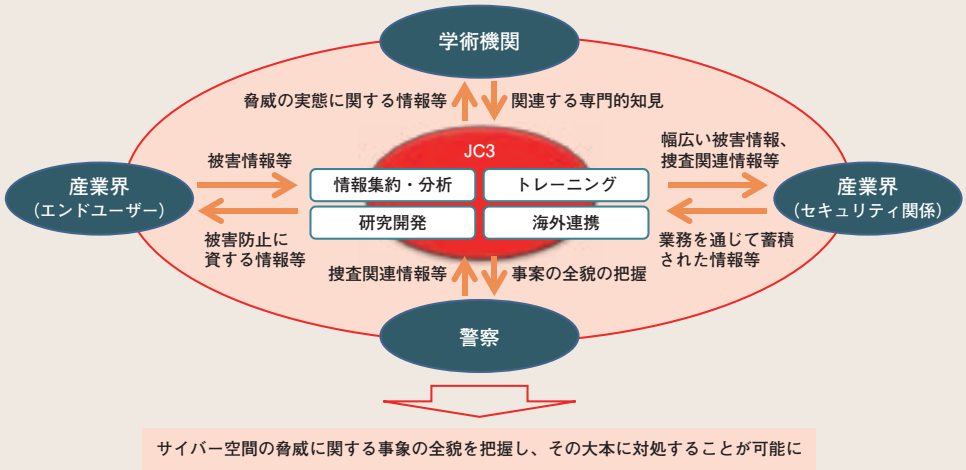
（5）共同対処協定の締結

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、平成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、27年末までに、オンラインゲーム事業者や銀行等、全国で525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。警察としては、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、安全安心なサイバー空間の構築に努めている。

図表３－16　日本サイバー犯罪対策センター（JC3）の概要

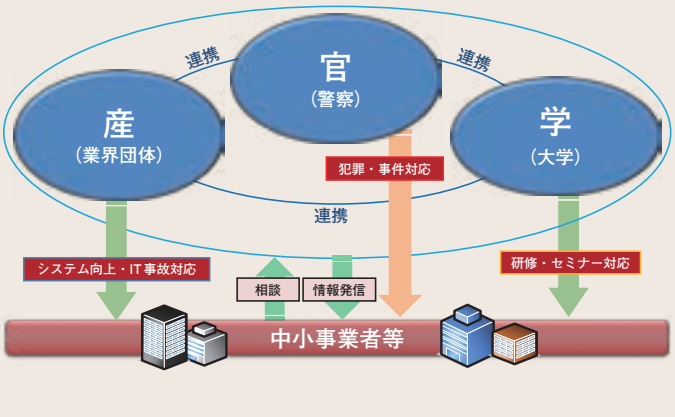


コラム　都道府県警察における産学官連携による中小事業者対策

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、地方自治体等と連携し、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。

京都府警察では、平成27年10月、府内の行政機関、経済団体及び大学教授と共に「京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）」を設立した。同ネットワークでは、中小事業者を対象とした情報漏えい等に関する相談窓口を開設しているほか、そこに寄せられるセミナー等への講師派遣依頼に対応するとともに、従来各機関等が独自に実施してきた広報活動等の諸対策を連動させ、より効果的なサイバーセキュリティに関する啓発活動の実施を図るなど、府内の中小事業者のサイバー空間の脅威への対策を推進している。

図表３－17　産学官連携による中小事業者対策（イメージ）



注：Japan Cybercrime Control Centerの略

警察活動の最前線

より安全なサイバー空間を目指して


カモンくん

山形県警察本部生活安全部生活環境課
サイバー犯罪対策室サイバー犯罪特捜係
田中（たなか）　秀典（ひでのり）　巡査長

私が、サイバー犯罪捜査係として勤務を始めてから、２年が経過しました。この２年間で、サイバー犯罪は、巧妙化、悪質化の一途を辿り、特に、平成27年中の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は、全国で30億円を超え過去最悪を更新しました。

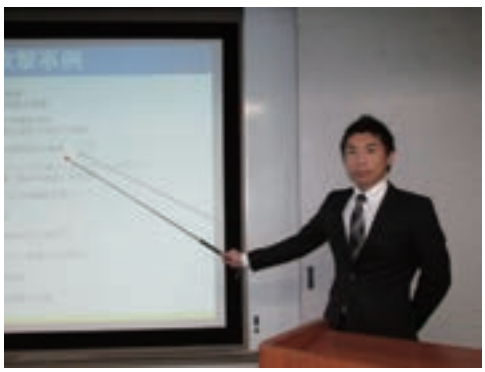
私は、平成26年に、複数の都道府県警察の合同捜査によるインターネットバンキング不正送金事件捜査に従事した際に、インターネット技術が日々進化するのに伴って新たな手口の不正アクセスや不正プログラムの悪用も急速に進んでおり、サイバー犯罪が年々、悪質巧妙化し、サイバー空間の脅威が拡大していることを思い知らされました。

今や、犯罪は、実空間からサイバー空間へと広がり、様々な犯罪がインターネットと関わりを持つようになってきております。これら犯罪に対処するには、警察職員一人一人が、サイバー犯罪に対する対処能力を身に付けるとともに、全国規模で敢行されるサイバー犯罪に対しては、全国警察の捜査能力と技術を結集し、一丸となって対処しなければならないと思っております。

私も、サイバー空間を暗躍する犯罪者の取締りに向け、日々精進し、より安全なサイバー空間の確保に努めていきたいと考えております。

サイバー攻撃対策の現状～見えざる敵と戦うために～

近畿管区警察局奈良県情報通信部
情報技術解析課技術指導係（現　同課解析係）
古谷（ふるや）　洋惣（ひろふさ）　技官



私は、奈良県警察サイバーセキュリティ対策プロジェクトの一員として、関係部署と協力して、重要インフラ事業者等への個別訪問や訓練・研修を実施し、サイバー攻撃対策に取り組んでいます。具体的には、近年、事業者が持つ情報の窃取等を目的とした「標的型メール攻撃」が増加傾向にあるため、事業者に対し、実際に模擬の標的型メールを送付した上での共同対処訓練やセキュリティ研修を実施しています。そのほか、サイバー攻撃の危険性に対する理解やセキュリティ意識の向上を図るため、その時々で話題となっている攻撃手法やマルウェア等セキュリティ上の脅威について、デモンストレーションを交えた講演を実施しています。講演を行うに当たっては、対象者の職種やセキュリティ意識が様々な中、事業者の要望に沿いつつ、いかに分かりやすく、脅威が実感できる内容にできるか工夫を加えています。

サイバー攻撃の手口については、日々、高度化・巧妙化しているため、この種の攻撃による被害を防止するためには、システムのセキュリティ対策だけではなく、利用者のセキュリティ意識をいかに高めるかが重要です。今後も、工夫を凝らした講演や訓練を実施し、サイバー攻撃による被害の未然防止に努めていきます。

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。