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。

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28年中のサイバー犯罪の検挙件数は8,324件と、前年より228件（2.8%）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

28年中の不正アクセス禁止法違反の検挙件数は502件と、前年より129件（34.6%）増加した。また、検挙人員は200人と、前年より27人（15.6%）増加した。

②　コンピュータ・電磁的記録対象犯罪等

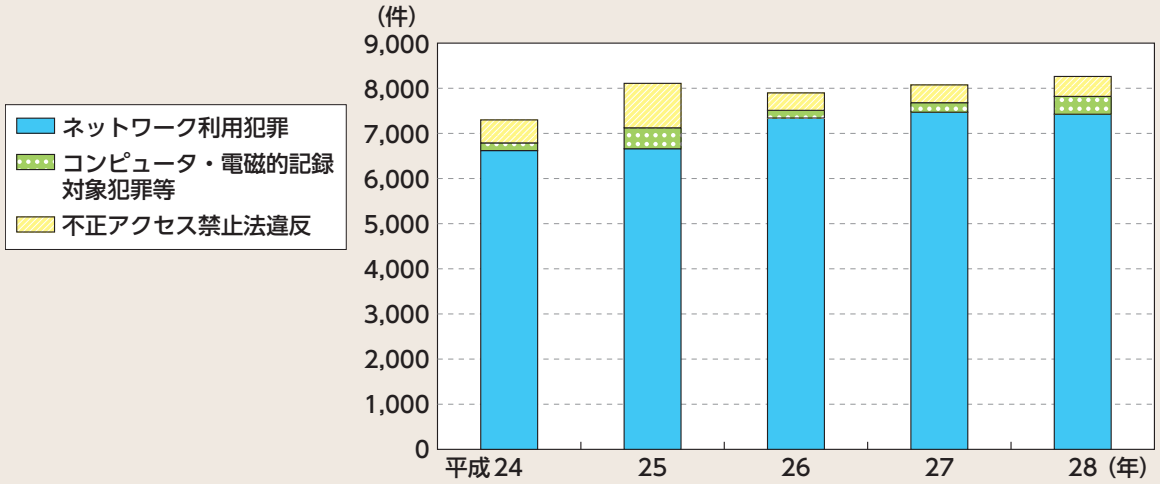
28年中の刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪及び不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウイルスに関する罪）の検挙件数は374件と、前年より134件（55.8%）増加した。このうち、コンピュータ・ウイルスに関する罪の検挙件数は58件であった。

③　ネットワーク利用犯罪(注5)

28年中のネットワーク利用犯罪の検挙件数は7,448件と、前年より35件（0.5%）減少した。特徴として、ストーカー規制法違反の検挙件数が267件と、前年より41件（18.1%）増加した一方、詐欺の検挙件数は828件と、前年より123件（12.9%）減少した。

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

図表３－２　サイバー犯罪の検挙件数の推移（平成24~28年）



区分＼年次	24	25	26	27	28
合計（件）	7,334	8,113	7,905	8,096	8,324
不正アクセス禁止法違反	543	980	364	373	502
コンピュータ・電磁的記録対象犯罪等	178	478	192	240	374
ネットワーク利用犯罪	6,613	6,655	7,349	7,483	7,448
児童買春・児童ポルノ禁止法違反（児童ポルノ）	1,085	1,124	1,248	1,295	1,368
詐欺	1,357	956	1,133	951	828
うちオークション利用詐欺	235	158	381	511	208
わいせつ物頒布等	929	781	840	835	819
児童買春・児童ポルノ禁止法違反（児童買春）	435	492	493	586	634
青少年保護育成条例違反	520	690	657	693	616
著作権法違反	472	731	824	593	586
脅迫	162	189	313	398	387
商標法違反	184	197	308	304	298
ストーカー規制法違反	78	113	179	226	267
出会い系サイト規制法(注)違反	363	339	279	235	222
その他	1,028	1,043	1,075	1,367	1,423

注：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

コラム　身代金要求型ウイルス「ランサムウェア」

近年、「ランサムウェア」と呼ばれるコンピュータ・ウイルスによる被害が発生している。同ウイルスに感染したコンピュータは、機能が制限され、コンピュータの利用者は、その制限の解除と引換えに金銭を要求される。

平成29年５月、世界各国において政府機関、病院、銀行、企業等のコンピュータが、「WannaCry」等と呼ばれるランサムウェアに感染させられる事案が発生し、国内でも被害が確認された。

警察では、ランサムウェアによる被害の実態把握に努めるとともに、被害拡大防止対策に取り組んでいる。

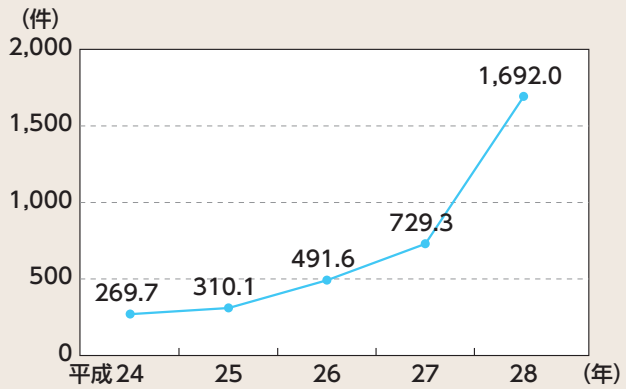
（2）サイバー攻撃の情勢

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、インターネット上で観測される不審なアクセスの件数が年々増加しているほか、実際に我が国の政府機関、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　サイバー空間における探索行為等

警察庁がリアルタイム検知ネットワークシステム(注1)により観測した不審なアクセスの件数は増加傾向にあり、平成28年中は、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50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。これは前年の約2.3倍の頻度となっている。

図表３－３　１つのセンサーに対する１日当たりの不審なアクセスの件数の推移（平成24～28年）



特に、28年中は、インターネットに接続されたデジタルビデオレコーダー、ウェブカメラ等の家電等の機器が発信元とみられる不審なアクセスの増加が顕著であり、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機器を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(注2)攻撃等に悪用されるおそれがある。

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、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電力会社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（2015年）12月、ウクライナにおいて大規模な停電が発生した。ウクライナ政府は、同停電がサイバー攻撃によるものとした上で、同国の電力会社の一社がシステムへの不正な侵入を受け、30か所の変電所との通信を切断されたことにより、８万の顧客が停電の影響を受けたと発表した。また、平成28年（2016年）12月、これに関連するとみられるサイバー攻撃による停電が同国の首都・キエフ近郊で発生したと報道された。

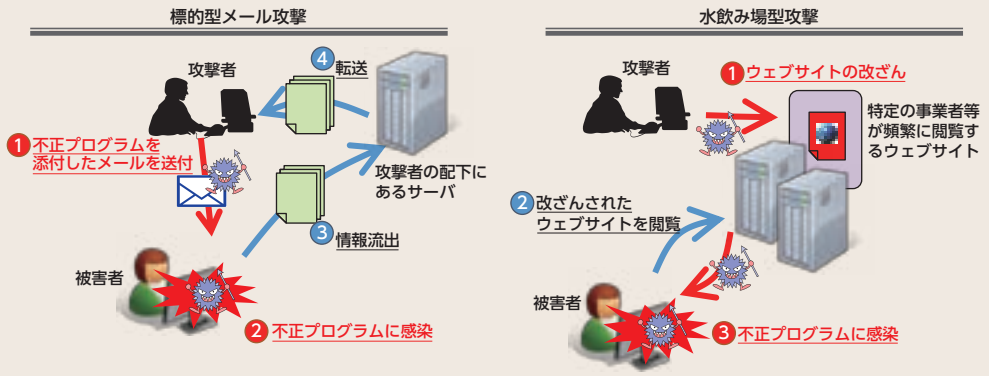
注１：141頁参照
２：Denial of Serviceの略。特定のコンピュータに対し、大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃

③　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正に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３－４　サイバーインテリジェンスの手口



事例 Case

平成28年（2016年）６月、北朝鮮が、平成26年（2014年）７月から平成28年（2016年）２月にかけて、複数の韓国企業等のコンピュータ約13万台に不正プログラムを感染させ、軍事情報を含む４万件以上の文書を窃取していたと報道された。

事例 Case

平成28年（2016年）６月、米国大統領選挙に関連して、民主党全国委員会に対するサイバー攻撃により、共和党のトランプ候補（当時）に関する調査資料等が窃取されたことが報道された。また、同年７月には、民主党のクリントン候補（当時）の陣営がサイバー攻撃を受けていたことが報道された。

同年10月、米国政府は、ロシア政府が米国大統領選挙の妨害を企図して、これらのサイバー攻撃を指示していたという旨の声明を発表し、同年12月、オバマ大統領（当時）は、ロシアに対する制裁措置を発表した。

事例 Case

28年10月、富山大学水素同位体科学研究センターに対するサイバー攻撃により、同大学職員のコンピュータが不正プログラムに感染し、外部のサーバとの間で不審な通信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

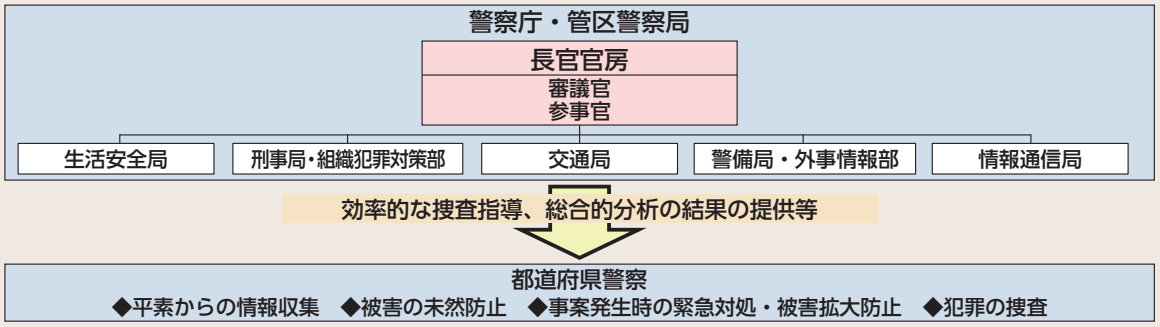
（1）警察におけるサイバー空間の脅威への対処体制

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。

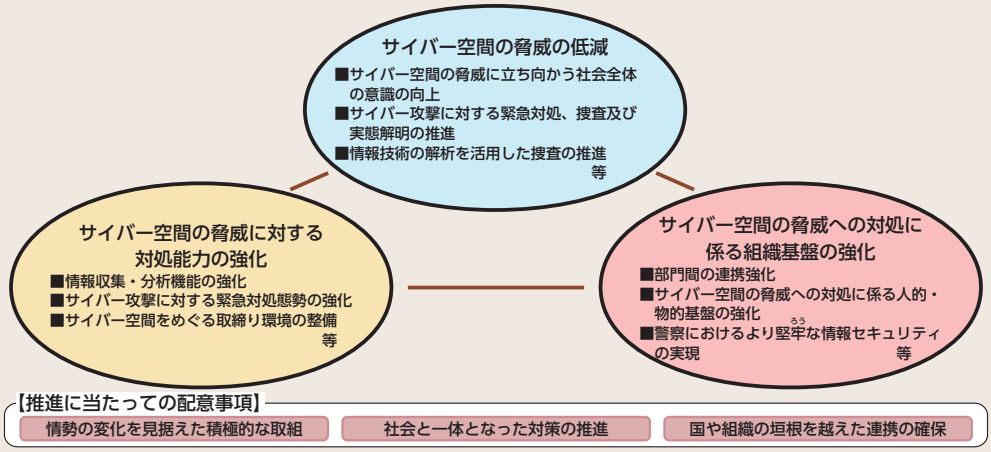
図表３－５ 警察におけるサイバー空間の脅威への対処体制



（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９月に制定された「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３－６ 警察におけるサイバーセキュリティ戦略の概要

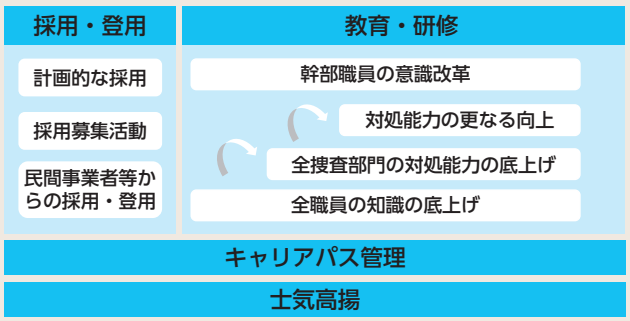


（３）サイバー空間の脅威への対処に係る組織基盤の強化

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８月、「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３－７　サイバー空間の脅威への対処に係る人材育成



コラム　サイバーセキュリティコンテストの開催

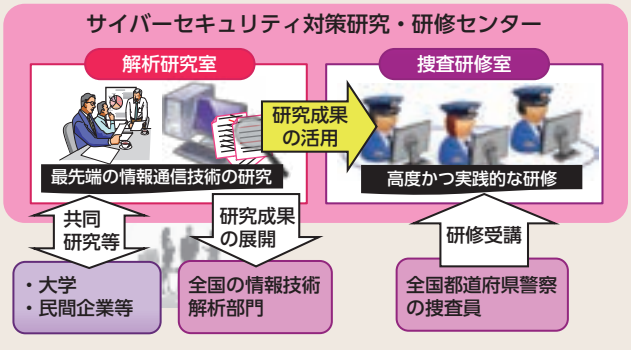
警察庁では、平成28年11月から29年２月にかけて、各都道府県警察の捜査員等を対象に、サイバー空間の脅威への対処に関する知識・技能を競うサイバーセキュリティコンテストを初めて開催した。同コンテストを通じて、捜査員等の知識・技能の向上を図るほか、全国の優秀な人材の発掘に取り組んでいる。

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究室の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。

図表３－８　サイバーセキュリティ対策研究・研修センター



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、大学、民間企業等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。

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研修を行っている。

2 サイバー犯罪への対策

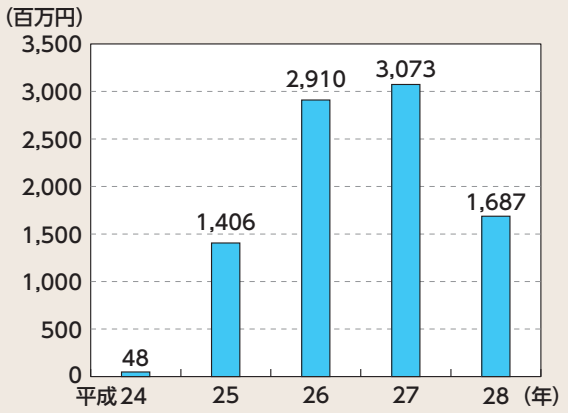
（1）インターネットバンキングに係る不正送金事犯への対策

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、26年に約29億1,000万円と急増し、27年には約30億7,300万円と、過去最高となった。しかし、不正プログラムに感染したコンピュータからのアクセスを検知するウイルス対策ソフトを活用した対策等による信用金庫の被害の減少等を受けて、28年の被害額は大きく減少し、約16億8,700万円（前年比45.1％減少）となった。

一方、28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電子決済サービスにおいて電子マネー等が不正に購入されるといった被害が多発するなど、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３－９　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24～28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、28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始め、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117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、金融機関に対し、フィッシングサイト対策やモニタリング(注1)等の被害防止対策の強化を要請しているほか、不正送金に利用されたレンタルサーバや口座に関する情報、JC３(注2)と連携して把握したフィッシングサイトに関する情報等を提供するなどしている。

（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3)を構築している。

事例 Case

男子中学生（14）は、平成27年６月から同年８月にかけて、匿名掲示板に不正送金ウイルスや遠隔操作ウイルス等を販売する旨の書き込みを行って顧客を募り、購入を申し込んだ少年らにコンピュータ・ウイルスを提供するなどした。同年11月から28年３月にかけて、同男子中学生を不正指令電磁的記録提供罪等で逮捕するとともに、コンピュータ・ウイルスの提供を受けた少年ら６人を不正指令電磁的記録取得罪で検挙した。また、同年５月、同男子中学生の依頼を受けて、コンピュータ・ウイルスの動作の検証等を行った大学職員の男（26）を、不正指令電磁的記録提供幇助罪等で逮捕した（警視庁、福島、千葉、愛知、滋賀）。

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。
２：145頁参照
３：144頁参照

（３）不正アクセス対策

①　発生状況等

平成28年における不正アクセス行為の認知件数(注１)は1,840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1,305件（70.9%）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244件（52.8%）と最多であった。

図表３－10　不正アクセス行為後の行為別認知件数（平成27、28年）

区分＼年次	27	28
合計（件）	2,051	1,840
インターネットバンキングでの不正送金	1,531	1,305
インターネットショッピングでの不正購入	167	172
オンラインゲーム、コミュニティサイトの不正操作	96	124
メールの盗み見等の情報の不正入手	92	91
インターネット・オークションの不正操作	20	34
知人になりすましての情報発信	83	25
ウェブサイトの改ざん・消去	34	6
その他	28	83

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。

図表３－11　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27、28年）

区分＼年次	27	28
合計（件）	332	462
識別符号窃用型(注)	331	457
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	117	244
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	51	61
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	46	49
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	15	34
他人から入手したもの	13	20
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	57	4
フィッシングサイトにより入手したもの	24	3
その他	8	42
セキュリティ・ホール攻撃型	1	5

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

事例 Case

無職の少年（17）らは、28年１月から同年５月にかけて、他人のID・パスワードを用いるなどして、佐賀県教育情報システムに不正アクセスを行った。同年６月、同少年ら２人を不正アクセス禁止法違反（不正アクセス行為の禁止）で検挙した。また、佐賀県教育委員会にシステムのぜい弱性に関する情報を提供するなど、被害の再発防止対策を推進した（警視庁、佐賀）。

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

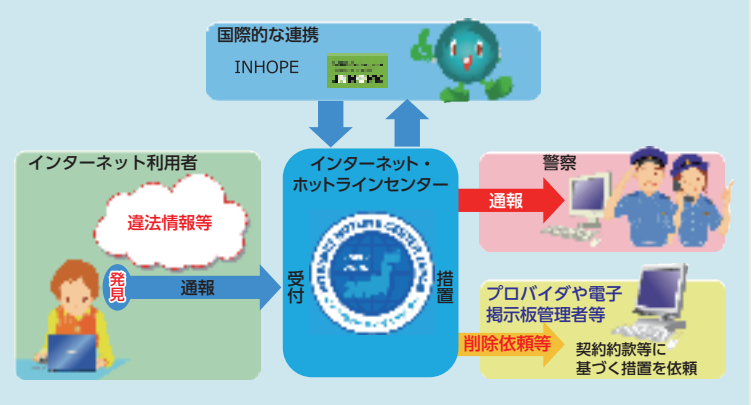
（5）インターネット上の違法情報・有害情報対策

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28年中にIHCが削除依頼を行った違法情報１万7,106件のうち１万6,838件（98.4%）が削除された。

図表３－12　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。

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(注２)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、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。

（6）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

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、平成20年以降増加傾向にあり、28年中の被害児童数は1,736人で、過去最多となった。

一方、出会い系サイト(注４)に起因して犯罪被害に遭った児童の数は、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り、28年中の被害児童数は42人となった。

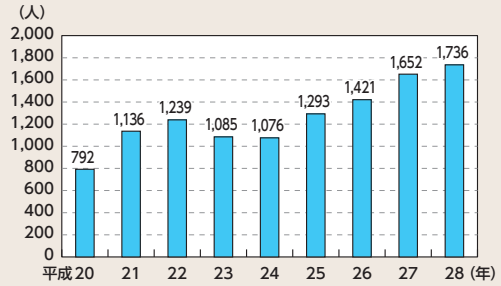
注１：現在の名称はInternational Association of Internet Hotlinesであるが、旧名称のInternet Hotline Providers in Europe Associationの略称を現在も使用している。11年に設立され、29年５月末現在、IHCを含む52団体（47の国・地域）から成る国際組織

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。

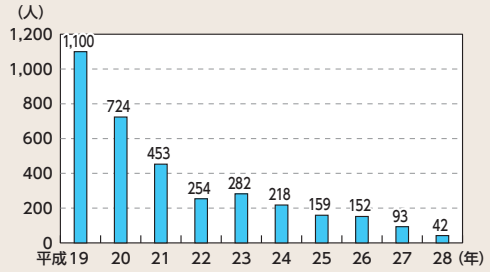
３：SNS、プロフィールサイト等、ウェブサイト内で多数人とコミュニケーションがとれるウェブサイト等のうち、出会い系サイトを除いたものの総称

４：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

図表３－13　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20～28年）



図表３－14　出会い系サイトに起因する事犯の被害児童数の推移（平成19～28年）

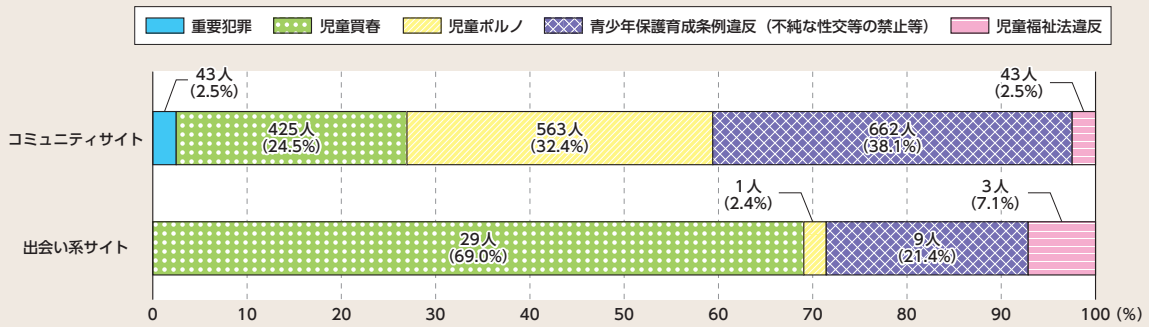


②　被害児童の状況

28年中、被害児童の最も多い罪種は、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662人（38.1％）、出会い系サイトに起因する事犯では、児童買春29人（69.0％）となっている。

また、28年中、コミュニティサイトに起因する事犯では、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、約９割がフィルタリングを利用していなかった。

図表３－15　コミュニティサイト及び出会い系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28年）



③　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に起因する児童の犯罪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、投稿内容の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１)の導入に向けた働き掛けを推進している。また、出会い系サイトに起因する児童の犯罪被害の防止に向けた対策として、無届け等の悪質出会い系サイト事業者や、出会い系サイトにおいて禁止誘引行為(注２)を行った者に対する取締り等を徹底している。

さらに、コミュニティサイト等において、サイバー補導(注３)を実施しているほか、関係機関・団体等と連携し、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の犯罪被害の防止に関する広報啓発等の取組を推進している。

（７）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や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202団体、8,598人（平成28年末現在）となっており、警察では、研修会の開催等を通じて、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。

注１：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、利用者年齢情報を活用し、大人と児童の間のやり取りや検索を制限すること。
２：出会い系サイト規制法第６条各号に掲げる行為
３：109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、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。

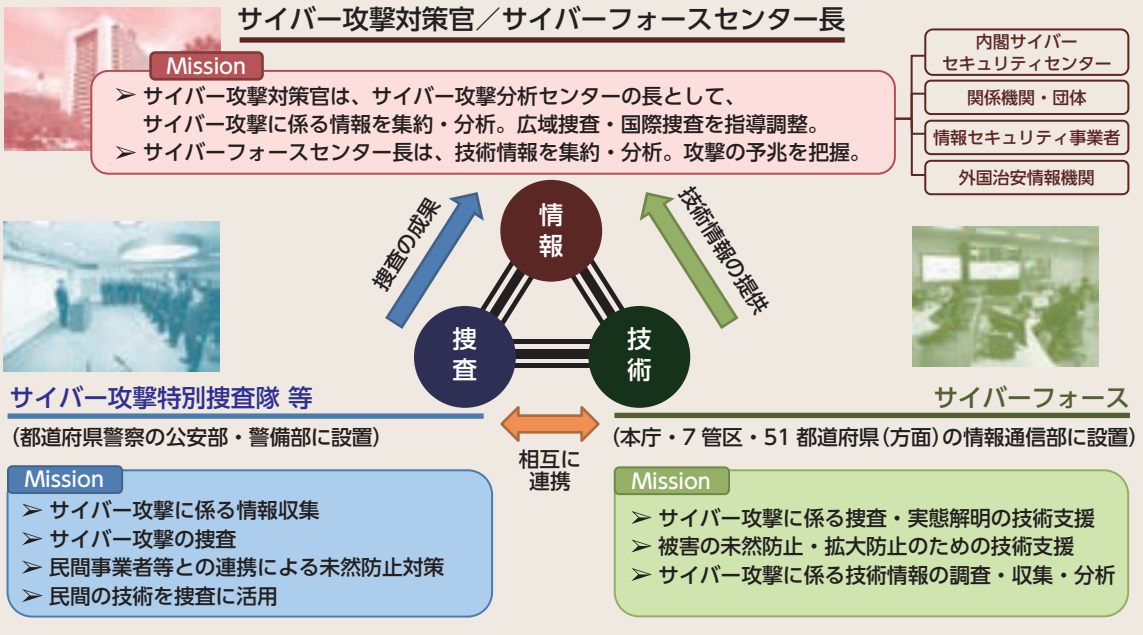
（1）サイバー攻撃対策の推進体制

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、官民連携や各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、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３－16　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、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、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

平成27年11月、地方公共団体が管理していたウェブサイトが、大量のアクセスにより閲覧が不可能になる事案（DoS攻撃事案）が発生した。28年５月、電子計算機損壊等業務妨害罪で男子高校生（16）を検挙した（大阪）。

コラム　世界的会合等における情報交換

警察では、サイバー攻撃の実態解明に資する情報の収集等のため、国内外のサイバーセキュリティに関する会合に参加するなどして、積極的な情報交換を行っている。

平成28年８月、警察庁職員が、サイバーセキュリティに関する世界最大級の会合である「Black Hat USA 2016」において、標的型メール攻撃に使用される文書ファイル形式の不正プログラムの従来とは異なる効果的な検出手法について講演するとともに、参加者との情報交換を行った。

講演の状況

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」(注)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」

注：https://www.npa.go.jp/cyberpolice/

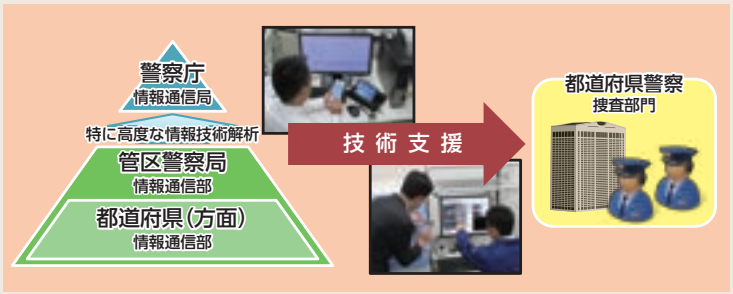
4 技術支援と解析能力の向上

（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1)。

図表３－17　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の研究

近年、最先端の情報通信技術を用いた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、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及び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１：98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(注１)。

警察庁では、サイバー犯罪に関する条約(注２)、刑事共助条約（協定）(注３)、ICPO、サイバー犯罪に関する24時間コンタクトポイント(注４)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28年中は、シンガポール内務省等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５)に置かれたハイテク犯罪サブグループ、ICPO及びEuropol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、日米サイバー対話や日韓サイバー協議等の関係省庁の代表が参加する国際会議や、オランダ国立法科学研究所を始めとする外国捜査機関等との二国間における協議等を通じ、サイバー空間の脅威に関する情報の共有や、国際捜査共助に係る連携強化等を推進している。

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。28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フランス国家憲兵隊、ICPO、FBI(注６)、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人材育成、国際連携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。

加えて、海外にリエゾンオフィサーを派遣するなどして、外国捜査機関等との連携を強化している。

注１：平成28年中の外国捜査機関との連携によるサイバー犯罪・サイバー攻撃への被害防止対策の事例については、53頁（トピックスⅠ　サイバー犯罪・サイバー攻撃への被害防止対策）参照
２：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。24年11月１日に我が国について発効した。
３：214頁参照
４：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、29年１月現在、73の国・地域に設置されている。
５：昭和53年（1978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（1995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、平成13年（2001年）の米国における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、平成26年（2014年）３月より、G7として実施している。
６：Federal Bureau of Investigation（米国司法省連邦捜査局）の略

6 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(注)。

（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。

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全国7,520の事業者等（平成29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

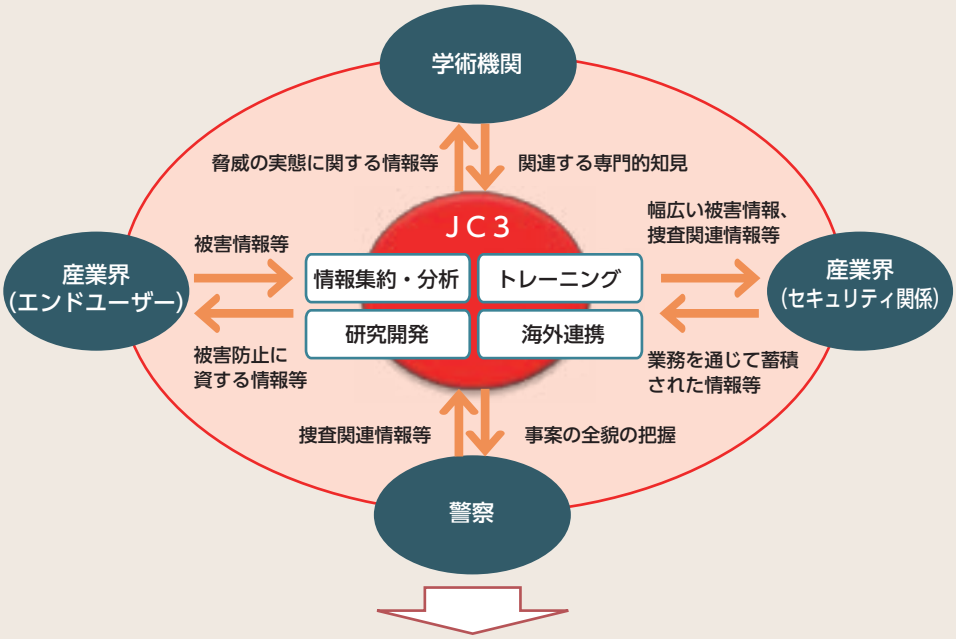
サイバー犯罪の潜在化の防止、捜査活動の効率化及び再発防止を図るため、平成24年７月から、警察では、民間事業者等との共同対処協定の締結を推進している。事業者と信頼関係を構築し、サイバー犯罪の警察への通報の促進等を図るため、28年末までに、オンラインゲーム事業者や銀行等、全国で554事業者・団体と本協定を締結している。

注：平成28年中の民間事業者との連携によるサイバー犯罪・サイバー攻撃への被害防止対策の事例については、52頁（トピックスⅠ　サイバー犯罪・サイバー攻撃への被害防止対策）参照

（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、安全安心なサイバー空間の構築に努めている。

図表３－18　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等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

サイバー空間の安全安心を目指して

福ぼうしくん
福ぼうしさん

福島県警察本部生活安全部生活環境課サイバー犯罪特捜第一係
松﨑（まつざき）　則夫（のりお）　警部補

私は、現在サイバー犯罪の捜査を行っており、これまでウェブサイトの改ざん、インターネットバンキングに係る不正送金事犯、動画投稿サイトを利用した著作権法違反等の事件を担当してきました。

サイバー犯罪は、犯行現場で犯人の姿を確認することはできません。また、犯人によって犯行の痕跡を消去されることがあるほか、時には国境を越えた先にいるであろう犯人までたどり着くことができず、悔しい思いをすることもありました。したがって、他の都道府県警察の捜査員と共に捜査を行い、それぞれが持つ知恵を出し合うことによって犯人にたどり着き、犯人を検挙できたときの喜びは格別なものがあります。

最近では、コンピュータをウイルスにより使用できない状態にさせ、そのコンピュータを直すために金銭を要求する手口のサイバー犯罪が発生するなど、その犯行手口はますます巧妙になっています。インターネットが生活に不可欠な基盤となっている中で、深刻化するサイバー犯罪を徹底的に検挙し、インターネット利用者の被害防止を図るため、日々業務に励んでいきたいと考えています。

サイバー攻撃対策の推進と堅牢な情報セキュリティの実現

関東管区警察局神奈川県情報通信部情報技術解析課技術支援第一係（現　警察庁情報通信局情報通信企画課）
柳原（やなぎわら）　忠明（ただあき）　技官

右側が本人

私は神奈川県警察サイバー攻撃対策プロジェクトチームの一員として、サイバーテロ対策及びサイバー犯罪対策に取り組んでいます。近年は政府機関、地方公共団体、企業等を狙ったサイバー攻撃が多発し、サイバー空間の脅威に対する対処能力の強化が喫緊の課題となっています。

このような状況の中、平成28年に、神奈川県警察のCSIRT（シーサート）(注)が、全国に先駆け、県警察の部門を横断してサイバー攻撃対処訓練を実施しました。私たちの部署は、日頃は県警察と共に重要インフラ事業者等に対する個別訪問や標的型攻撃メール対策の共同対処訓練、情報セキュリティ研修等を実施していますが、県警察を対象とする訓練は初めての試みでした。私は、今回の訓練の実施に先立つ自らの経験や知識をいかし、訓練参加者に技術的な指導や助言を行うことで、より実践的な訓練に寄与することができたと思います。

警察のみならず、産学官が連携して、このような訓練を行ってサイバー空間の脅威に対する対処能力の強化を図り、より堅牢な情報セキュリティを実現することで、安全安心なサイバー空間を構築できるものと信じています。

注：199頁参照