特集に当たって

本年の警察白書の特集テーマは「安全・安心なインターネット社会を目指して」である。

我が国においては、「2005年度までに世界最先端のIT国家となる」との目標を掲げたe-Japan戦略等の５年間において、ブロードバンドインフラの整備と利用の広がり等の面で世界最先端を実現するなど、国民生活の利便性が飛躍的に向上し、情報通信ネットワークが社会・経済活動上、極めて重要なインフラとなった。

一方で、国民生活の安全を脅かすサイバー犯罪は年々増加し、その手口も高度化、多様化している。また、インターネット上に違法・有害情報が氾濫し、これが人の行動や意識に悪影響を及ぼしているとみられる事件も発生している。

さらに、証券取引や航空管制に関するシステムに障害が発生し、国民生活に多大な影響を及ぼすなど、サイバーテロが発生した際の影響の大きさをうかがわせる事案も発生している。

このように、サイバー空間はそれだけで完結した世界ではなく、現実社会に様々な影響を与える存在となっている。このことは、今後の我が国の治安を確保する上で、サイバー空間と現実社会とを別々のものとしてではなく、一体として捉えることが不可欠であることを示している。

そこで、インターネット社会の負の側面を明らかにするとともに、これまで講じられてきた対策の現状と課題を示し、今後、社会全体でインターネット社会の在り方についての真剣な議論を進めるための契機となることを期待して、この特集を組むこととした。

第１節では、インターネット上に氾濫する違法・有害情報による国民生活、とりわけ少年の健全育成に与える悪影響、各種犯罪におけるインターネットの悪用、サイバーテロの脅威の顕在化等のインターネット社会の諸問題について、一般のインターネット利用者の意識に触れつつ記述した。

第２節では、インターネット社会の安全確保に向けた取組みについて記述した。

第３節では、社会全体としての違法・有害情報への対応、巧妙化するサイバー犯罪への対応及び公共の安全を維持するための取組みの強化といった、今後、重点的に推進すべき課題を取り上げ、その方向性等について記述した。

本特集を通じ、サイバー空間の安全確保に向けた取組みに対する国民一人一人の理解が深まり、安全・安心なインターネット社会が実現することを切に願うものである。

第１節　国民の生活を脅かすインターネット社会の現実

近年めざましい発展を遂げている情報通信ネットワークは、国民生活の利便性を向上させ、社会・経済の根幹を支えるインフラとして機能するようになった一方で、わいせつ画像、規制薬物の売買情報、爆弾の製造方法等の違法・有害情報がインターネット上に氾濫し、これがインターネット利用者に悪影響を与え、犯罪の引き金になる事件も多発している。

特に、少年の健全育成に悪影響を与えかねないインターネット上の情報に少年が気軽にアクセスできる状況が放置されており、実際に少年が児童買春等の被害に遭うといった事件が後を絶たない。

また、最近は、スパイウェア等の高度な技術を利用した犯罪が発生し、社会問題化する一方で、インターネット社会自体がインターネット・オークションを利用した詐欺や知的財産権侵害事犯のような新たな形態の犯罪を生み出している。

さらに、インターネットの急速な普及に伴って、国際テロ組織や国際テロリストも様々な形でインターネットを利用するようになっており、顕在化するサイバーテロの脅威とともに我が国の公共の安全の維持にとって大きな問題となっている。

この節では、インターネット社会が国民生活を脅かしているこのような現実について記述する。

（１）インターネット上の違法・有害情報のもたらす脅威

インターネットには、テレビ、ラジオ、新聞、雑誌等の他の媒体と異なり、インターネットに接続することができる環境にあれば、だれもが自由に情報を発信し、受信することができるという特徴がある。このことが、インターネット上に、国民生活にとって有益な情報ばかりではなく、社会に悪影響を与える様々な情報が氾濫する状況を招いている。

①　様々な違法情報

インターネット上には、児童ポルノ画像、わいせつ画像、覚せい剤等規制薬物の販売に関する情報等の違法情報（情報自体が違法である情報）を掲載するウェブサイトや電子掲示板（インターネット上の電子掲示板をいう。以下同じ。）が多数存在し、だれもがアクセスできる状態に置かれている。

事例１　無職の男（３４）は、平成１７年３月、自ら管理する電子掲示板に他の者が撮影して投稿した児童ポルノ画像を公然と陳列した。同年１２月、電子掲示板を管理する無職の男及び児童ポルノ画像を投稿した男ら８人を児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律（以下「児童買春・児童ポルノ法」という。）（児童ポルノ公然陳列）違反で逮捕した（愛知）。

事例２　コンピュータプログラマーの男（３１）は、１７年６月、他人に譲渡する目的で覚せい剤を所持していた。同月、覚せい剤取締法違反（営利目的所持）で逮捕するとともに、同年９月、国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律違反（薬物犯罪のあおり、唆し）で追送致した。男は、携帯電話からアクセスすることのできる電子掲示板に覚せい剤等を販売する旨を掲載し、連絡してきた客に覚せい剤等を密売していた（静岡、群馬）。

②　氾濫する有害情報

ア　国民生活を脅かす有害情報

インターネット上には、

- 爆発物の製造方法や運転免許証その他の公的証明書の偽造方法等を教示する情報
- 殺人、脅迫等の違法行為の請負、仲介等に関する情報
- いわゆる自殺サイトに掲載されている他人を自殺に勧誘する情報

といった有害情報（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のできない情報）が氾濫している。

これらの情報は、インターネット上に掲載すること自体は違法とまでは言えないが、次の事例のように、実際に爆発物の製造に必要な知識の取得や犯罪の共犯者の募集に利用されるなどしており、現実の国民生活への大きな脅威となっている。

このほか、インターネット上には、殺人等の残虐な画像や人を誹謗・中傷する情報、盗撮画像等が氾濫している。このうち、盗撮画像については、盗撮された者のプライバシーを侵害するなど大きな社会問題となっている。現在、警察では、盗撮行為について、軽犯罪法、いわゆる迷惑防止条例等を適用して取締りを進めているが、盗撮行為は違法であっても、それによって得られた盗撮画像を提供する行為は、当該画像が違法でない限り禁止されておらず、インターネット上に提供された当該画像がわいせつ画像、児童ポルノ画像等違法な画像である場合には刑法や児童買春・児童ポルノ法等を適用することとしている。

事例1　高校生の少年（18）は、17年6月、爆発物の製造方法に関する情報を掲載するウェブサイトを閲覧して、そこで得た情報を基にガラス瓶に火薬を詰めた爆発物を製造し、これを自らが在籍する高等学校の教室で爆発させて、同級生28人を負傷させた。傷害罪で現行犯逮捕するとともに、同年7月、爆発物取締罰則違反（爆発物の所持）で再逮捕した（山口）。

事例2　会社員の男（32）は、17年2月、モデルガンを改造したけん銃を所持していた。同月、銃砲刀剣類所持等取締法違反（所持）で逮捕するとともに、改造けん銃3丁を押収した。男は、改造けん銃を、インターネット・オークションを利用して密売していた（愛知、警視庁）。

事例3　無職の少年（17）は、17年5月、携帯電話からアクセスすることのできる電子掲示板を通じてひったくりの共犯者を募り、同電子掲示板を通じて知り合った塗装工の男（27）と共謀し、同年6月、道路を通行していた女性から手提げバッグを奪った。同年７月までに、窃盗罪で逮捕した（警視庁）。

事例4　無職の男（49）は、17年12月、その長男（25）と共謀して、電子掲示板に「半殺し50万円。殺したら100万円。年内に達成なら倍額」等と実父の殺害を依頼する書き込みをし、これを見て連絡してきた派遣会社社員の男（36）に実父を殺害させた。18年2月までに、殺人罪で逮捕した（長野）。

押収した改造けん銃

「闇の職業安定所」と称する電子掲示板における違法行為の共犯者の募集の例（本文の事件とは関係ない。）

コラム 1 インターネットで殺人依頼～復讐サイトの落とし穴～

Ａ子（32）は、職場の上司の男と不倫関係にあった。いずれは男が妻と別れて自分と一緒になってくれると信じ交際を続けていたが、男は自分の妻が身ごもると、Ａ子の前で妻を大切にするような言動をとるようになり、Ａ子に対しては暴力を振るうようになった。

Ａ子は「裏切られた」と感じた。男への愛情は復讐心へと変わり、そして「奥さんやお腹の子どもがいなくなれば男に復讐できる」と考えるようになった。

折しも、Ａ子は、インターネット上の有償で他人に対する恨みを晴らすと宣伝する「復讐代行サイト」を見付け、男の妻の殺害を依頼した。このサイトの管理者は、着手料と称して165万円を受け取り、自称探偵業の男を紹介した。しかし、そのサイト管理者と自称探偵業の男は当初から殺害する意図などなく、殺害計画や必要経費をでっち上げ、Ａ子から数回にわたり合計で約1,500万円をだまし取った。Ａ子は、消費者金融から借金をしてまで請求された費用を払い続けたが、いつになっても殺害が実行されることがなかったことから、「だまされているのではないか」と疑念を抱いて警察に相談し、一連の事件が発覚した。

Ａ子は暴力行為等処罰ニ関スル法律違反（犯罪請託罪）で逮捕され、起訴猶予となったものの、職場を解雇された。不倫相手の男は、Ａ子に対する傷害罪で逮捕され、50万円の罰金刑に処され、同じく職場を解雇された。

また、サイト管理者と自称探偵業の男は、それぞれ詐欺罪で逮捕・起訴され、サイト管理者は懲役1年6か月、執行猶予4年の判決、自称探偵業の男は懲役2年6か月の実刑判決を受けた。

イ　子どもに対する暴力的性犯罪の誘発

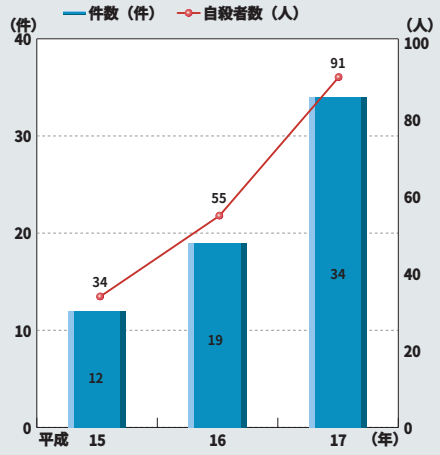
インターネット上には、子どもの裸体画像や性的虐待画像が氾濫している。これらはそれ自体が違法であることもあるが、時として、これらの情報が影響して子どもに対する暴力的性犯罪を誘発するといった事例もみられ、子どもをこれらの犯罪から守る上で深刻な問題となっている。

例えば、小学生の女児を車に乗せて連れ去り、わいせつ行為をして逮捕された被疑者が、日ごろから児童と性交をする場面を撮影した画像や児童の裸体画像等をウェブサイトから多数ダウンロードして収集するなどしていた事案等が発生している。

ウ　社会問題となっているいわゆる自殺サイト

近年、いわゆる自殺サイトにおける自殺の予告や呼び掛けを通じて知り合った者同士が自殺を敢行する事案が増加しており、17年中のいわゆる自殺サイトで知り合った者による自殺事案の発生件数は34件（前年比15件（78.9%）増）、自殺者数は91人（前年比36人（65.5%）増）と、いずれも前年より大幅に増加した。また、いわゆる自殺サイトを通じて知り合った女性を一緒に自殺するかのように装って呼び出し、殺害した事件が発生するなど、いわゆる自殺サイトの存在が大きな社会問題となっている。

図1-1　いわゆる自殺サイトで知り合った者による自殺事案の発生状況（平成15～17年）



事例1　いわゆる自殺サイトで知り合った男2人A（28）、B（23）と少女（17）は、17年8月、自殺するためA宅に集まり、密閉した室内で炭の入ったこんろを使用し、一酸化炭素中毒により死亡した（愛知）。

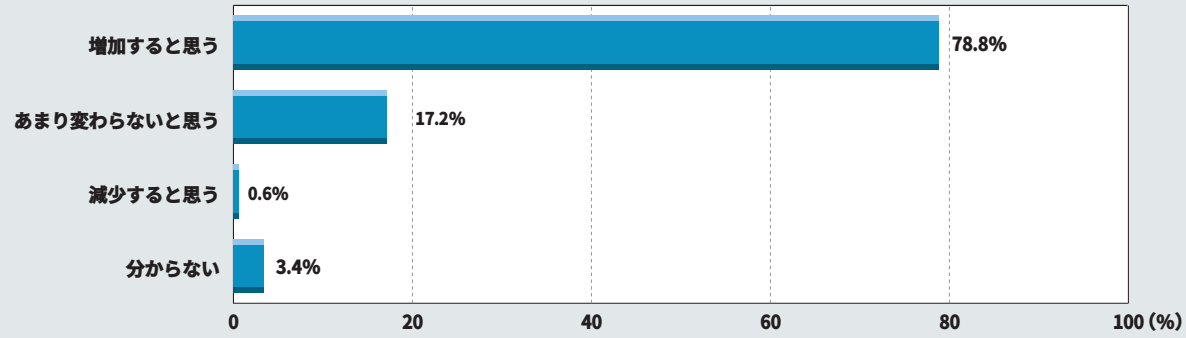
事例2　派遣会社社員の男（36）は、人が窒息して苦もんする表情を見て性的快感を得ようと考え、17年2月、いわゆる自殺サイトで知り合った女性を、駐車場に止めた車両内で殺害し、その死体を河川敷に遺棄した。同年8月、殺人罪及び死体遺棄罪で逮捕した（大阪）。

③　インターネット上の違法・有害情報に関する国民の意識

警察庁では、18年３月、インターネット利用者を対象にインターネット利用に関する意識調査(注)を行った。

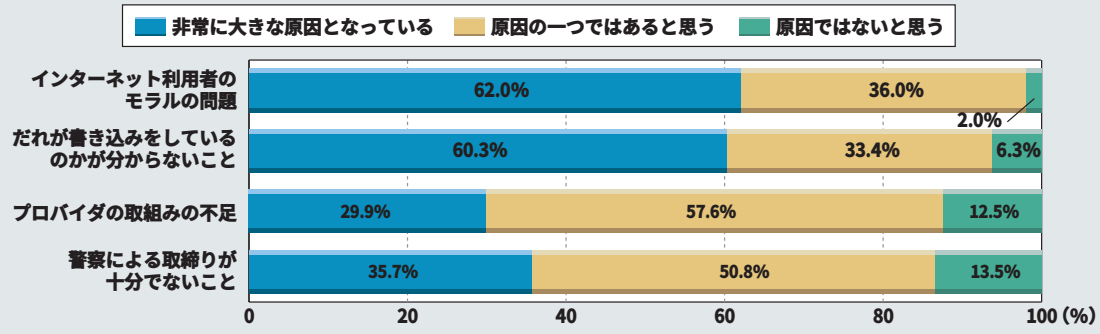
インターネット上の違法・有害情報に起因する事件が、今後、増加するかどうかについて質問したところ、78.8%の者が「増加すると思う」と回答している。

図1 - 2　インターネット上の違法・有害情報が氾濫している原因



また、インターネット上に違法・有害情報が氾濫している原因について質問したところ、「非常に大きな原因となっている」ものとして、62.0%の者が「インターネット利用者のモラルの問題」を、60.3%の者が「だれが書き込みをしているのかが分からないこと」を回答している。

図1 - 3　今後、インターネット上の情報に起因する事件は増加すると思うか



このように、多くのインターネット利用者が、違法・有害情報に起因する事件の増加を懸念し、違法・有害情報が氾濫しているのは、利用者のモラルの欠如やインターネット上の匿名性にあると考えていることが分かる。

注：全国のインターネット利用者男女1,000名を対象に、調査を委託した民間事業者のウェブサイト上に警察庁において作成した質問票を掲示して回答を求める形式で実施

（2）少年に与える悪影響

現在、多数の少年が自由に使える携帯電話を持っており、出会い系サイト(注1)の利用を通じた児童買春・児童ポルノ法違反、いわゆる青少年保護育成条例違反等の性的被害に遭う事件が多発しているなど、出会い系サイトの利用が少年の健全育成に悪影響を及ぼしている。また、少年が、保護者の監督の及ばない所で携帯電話によりインターネットを利用し、違法・有害情報に直接アクセスできる状況が放置されているという問題が指摘されている。近年、これらの情報に影響を受けたとみられる少年による凶悪事件が発生するなど、性や暴力に関する情報が少年に深刻な悪影響を与えている。

①　出会い系サイトの危険性

ア　児童による出会い系サイトの利用実態

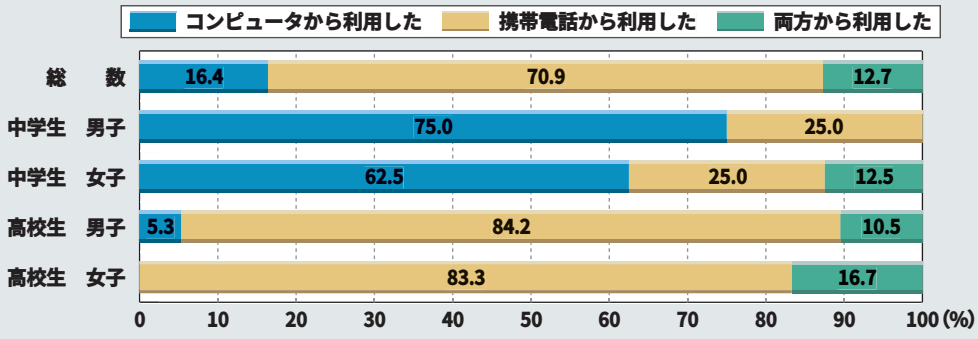
17年11月、警察庁は中学生、高校生及びその保護者を対象にインターネット利用に関する意識調査(注2)を行った。

中学生及び高校生に対し、自由に使える携帯電話を持っているかどうかについて質問したところ、70.9%の者が「持っている」と回答しており、特に、高校生については「持っている」と回答した者の割合は男子で94.2%、女子で98.0%に上るなど、大多数の高校生が携帯電話を保有し、自由に使用することができる環境に置かれている。

次に、出会い系サイトを利用した経験の有無について質問したところ、2.6%の者が実際に出会い系サイトを「利用したことがある」と回答した。中学生、高校生とも、女子による利用が多く（中学生の女子1.9%、高校生の女子4.2%）、特に高校生の女子については、利用したことのある者の割合が高かった。

また、出会い系サイトを「利用したことがある」と回答した者に対し、出会い系サイトを利用する手段について質問したところ、70.9%の者が「携帯電話から利用した」と回答しており、携帯電話及びコンピュータの「両方から利用した」ことがあると回答した者（12.7%）を合わせると83.6%の者が出会い系サイトの利用に際して携帯電話を使用している。

図1 - 4　出会い系サイトの利用形態

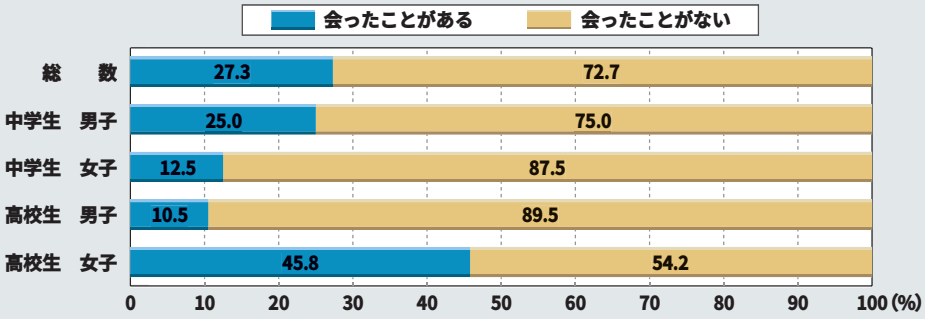


注1：面識のない異性との交際（以下「異性交際」という。）を希望する者（以下「異性交際希望者」という。）の求めに応じ、その異性交際に関する情報をインターネットを利用して公衆が閲覧することができる状態に置いてこれに伝達し、かつ、当該情報の伝達を受けた異性交際希望者が電子メールその他の電気通信を利用して当該情報に係る異性交際希望者と相互に連絡することができるようにする役務を提供するウェブサイト

2：インターネット人口普及率（人口に対するインターネット利用者数の比率）等を考慮して、６都県を選定し、それぞれ中学校及び高等学校１校ずつ（合計12校）の生徒計2,271名及び保護者計2,196名を対象に、あらかじめ作成した調査票を配布、回収する形式で実施

さらに、出会い系サイトを利用して知り合った相手と実際に会ったことがあるかについて質問したところ、３割近くの者が実際に「会ったことがある」と回答し、特に、高校生の女子については、半数近くが実際に「会ったことがある」と回答している。

図1 - 5　いわゆる出会い系サイトを利用して知り合った者との接触状況



このように、相当数の少年が、携帯電話を利用して出会い系サイトにアクセスするだけでなく、出会い系サイトを通じて知り合った相手と実際に会っている。

出会い系サイトへの書き込みの例

イ　出会い系サイトに関係した犯罪の発生状況

出会い系サイトに関係した犯罪の検挙件数は、15年の1,743件をピークにほぼ横ばいで推移しており、17年中は1,581件と、前年より１件（0.1%）減少した。

そのうち、児童買春・児童ポルノ法違反の検挙件数は707件（前年比61件（7.9%）減）、児童福祉法違反の検挙件数は71件（前年比16件（18.4%）減）とそれぞれ減少しているものの、いわゆる青少年保護育成条例違反の検挙件数は460件（83件（22.0%）増）と増加しており、依然として児童（18歳未満の者をいう。）の性的犯罪の被害が目立っている。また、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（以下「出会い系サイト規制法」という。）違反の検挙件数は18件（前年比13件（41.9%）減）と減少し、うち児童によるものは５件（前年比１件（16.7%）減）であった。

表1-1　出会い系サイトに関係した事件の検挙件数の推移

区分＼年次	13	14	15	16	17
児童買春・児童ポルノ法違反（件）	387	813	810	768	707
青少年保護育成条例違反	221	435	448	377	460
児童福祉法違反	16	117	82	87	71
重要犯罪（殺人・強盗・強姦等）	73	100	137	95	98
粗暴犯（暴行・傷害・脅迫・恐喝）	66	128	108	58	72
出会い系サイト規制法違反	-	-	5	31	18
その他	125	138	153	166	155
合　　計	888	1,731	1,743	1,582	1,581

出会い系サイトに関係した犯罪の被害者数に占める児童の割合は約８割以上の高水準で推移しており、被害者となった児童のほとんどを女性が占めている。また、17年中の被害者のうち、小学生、中学生、高校生の人数を見ると、約６割を高校生が占めているが、約４割を中学生が占め、少数ではあるが小学生の被害児童もみられるなど、出会い系サイトによる被害は低年齢層にも着実に広がっていることが分かる。

表1-2　出会い系サイトに関係した犯罪の被害者数の推移

区分＼年次		13	14	15	16	17
被害者数（人）		757	1,517	1,510	1,289	1,267
	うち女性	699（92%）	1,398（92%）	1,395（92%）	1,194（93%）	1,163（92%）
児　童		584（77%）	1,273（84%）	1,278（85%）	1,085（84%）	1,061（84%）
	うち女性	574（98%）	1,255（99%）	1,262（99%）	1,076（99%）	1,052（99%）
18歳以上		173（23%）	244（16%）	232（15%）	204（16%）	206（16%）
	うち女性	125（72%）	143（59%）	133（57%）	118（58%）	111（54%）

表1-3　被害者のうち小学生・中学生・高校生の人数（平成17年中）

（人）

	小学生	中学生	高校生	計
計	3　（0.4%）	347　（42.0%）	477　（57.7%）	827
女性	3　（0.4%）	345　（42.0%）	473　（57.6%）	821
男性	0　（0.0%）	2　（33.3%）	4　（66.7%）	6

また、出会い系サイトについては、必ずしも異性交際を目的として利用されるばかりではなく、次の事例のように知り合った相手に危害を加えたり、性風俗店で稼働させる者を探すためにも利用されている。これらの者は、異性交際が目的であるかのように装い、本来の目的を隠して児童と接触することが多いため、警戒心が乏しく、判断能力が未熟な児童が安易に出会い系サイトを利用すると犯罪に巻き込まれる危険性が高い。

事例1　地方公務員の男（27）は、16年11月、当初から殺害する目的で、携帯電話からアクセスすることのできる出会い系サイトを通じて知り合った少女に「8万円を払う」などと交際を持ちかけて、待ち合わせ場所に現れた少女を殺害し、死体を雑木林に遺棄した。17年9月までに、殺人罪及び死体遺棄罪で逮捕した（愛知）。

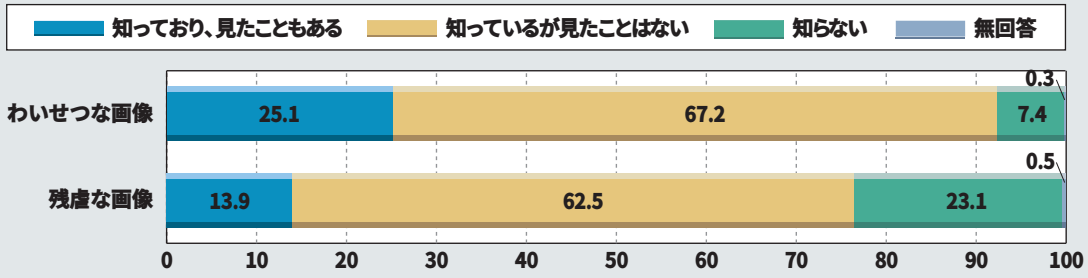
事例2 性風俗店経営の男（32）は、17年5月から同年6月にかけて、携帯電話からアクセスすることのできる出会い系サイトを通じて知り合った少女3人を、同人が経営する性風俗店で稼働させ、客相手にみだらな行為をさせるなどした。17年11月、児童福祉法違反（児童に淫行をさせる行為）で逮捕した（新潟）。

②　違法・有害情報対策に関する保護者の意識

ア　少年による違法・有害情報へのアクセスの状況

現在、多数の少年が携帯電話を保有しており、自由に使用している状況にある。警察庁が実施した意識調査(注1)において、中学生及び高校生に対し、コンピュータや携帯電話を使ってわいせつな画像を見ることができるのを知っているか質問したところ、「知っているが見たことはない」と回答した者が67.2%、「知っているし、見たこともある」と回答した者が25.1%を占めている。同様に、残虐な画像を見ることができるのを知っているか質問したところ、「知っているが見たことはない」と回答した者が62.5%、「知っているし見たこともある」と回答した者が13.9%であった。このように、ほとんどの少年がコンピュータや携帯電話により、性や暴力に関する情報を入手できることを知っており、実際にそのような画像を見たことのある少年も多くいる。

図1-6　わいせつ画像及び残虐な画像の認知・閲覧経験



イ　フィルタリングに関する保護者の認識不足

このような違法・有害情報から少年を守るため、現在、コンピュータ用だけでなく、携帯電話用のフィルタリング・ソフト又はサービス(注2)の提供も行われているが、保護者に対して、こうしたコンピュータ及び携帯電話のフィルタリング・ソフト又はサービスを知っているかどうか等について質問したところ、「知らなかった」と答えた者が57.7%を占める一方で、「知っていて、利用したこともある」と答えた者は7.7%にとどまった。また、フィルタリング・ソフト又はサービスの利用の意向の有無について質問し、「利用したくない」と答えた保護者が34.6%いたことから、その保護者に対して理由を質問したところ、「子どもが有害な情報を見ないと思うから」と答えた者が46.4%、「利用する方法が分からないから」と答えた者が38.0%に上った。

注1：６頁の意識調査と同一のもの
2：ウェブサイト上の違法・有害情報へのアクセスを制御するために、受信者側でこれらの情報を受信するかどうかを選択できるソフトウェア又はサービス

図1 - 7　フィルタリング・ソフト又はサービスの認知度

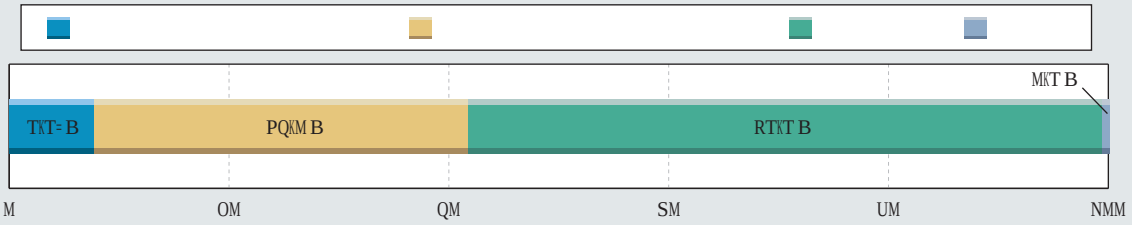
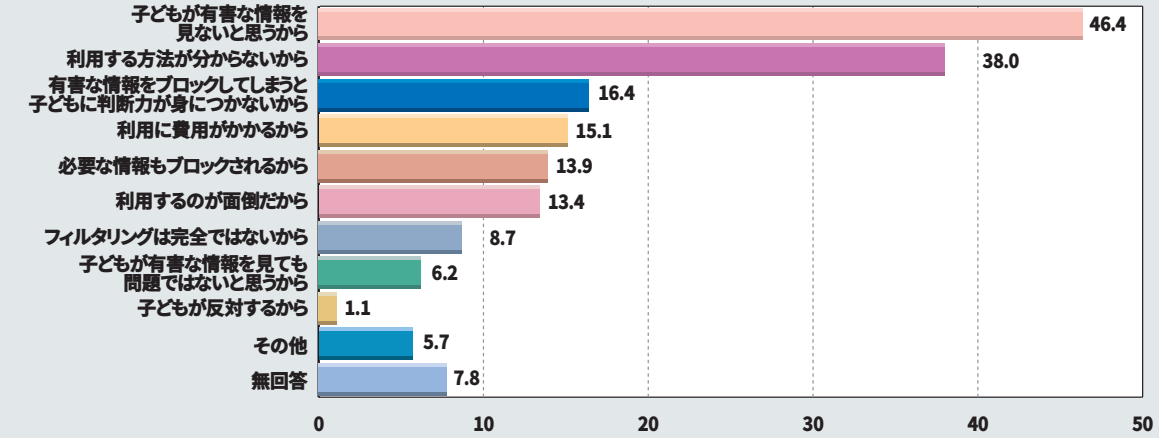
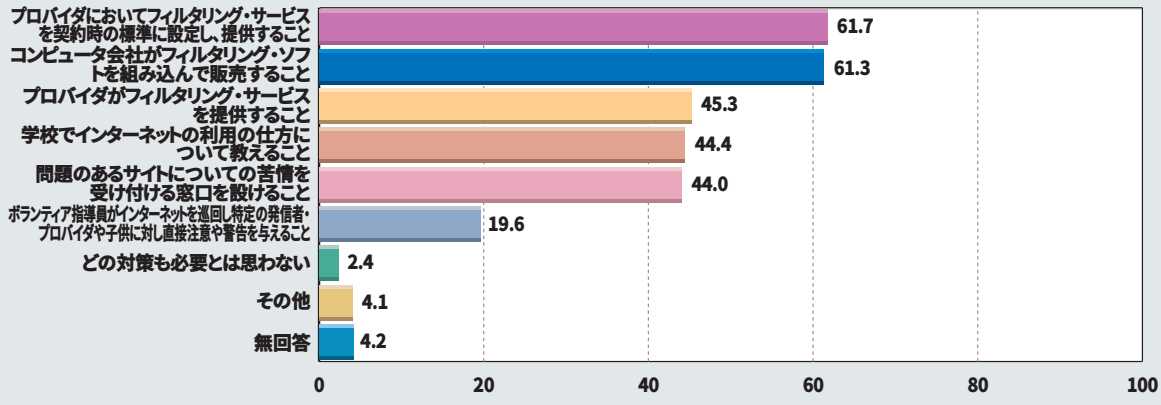


図1 - 8　フィルタリング・ソフト又はサービスを利用しない理由



保護者に対して出会い系サイトやインターネット上の違法・有害情報に対して必要だと思う対策について質問したところ、「プロバイダにおいてフィルタリング・サービスを契約時に設定し、標準機能として提供すること」と答えた者が61.7%、「コンピュータにフィルタリング・ソフトを組み込んで販売すること」と答えた者が61.3%と、契約又は販売時においてフィルタリング機能の初期設定が必要であると回答した保護者が６割を超えている。また、「プロバイダがフィルタリング・サービスを提供すること」と答えた者は45.3%、「学校でインターネットの利用の仕方について教えること」と答えた者も44.4%に上った。

図1 - 9　必要な対策

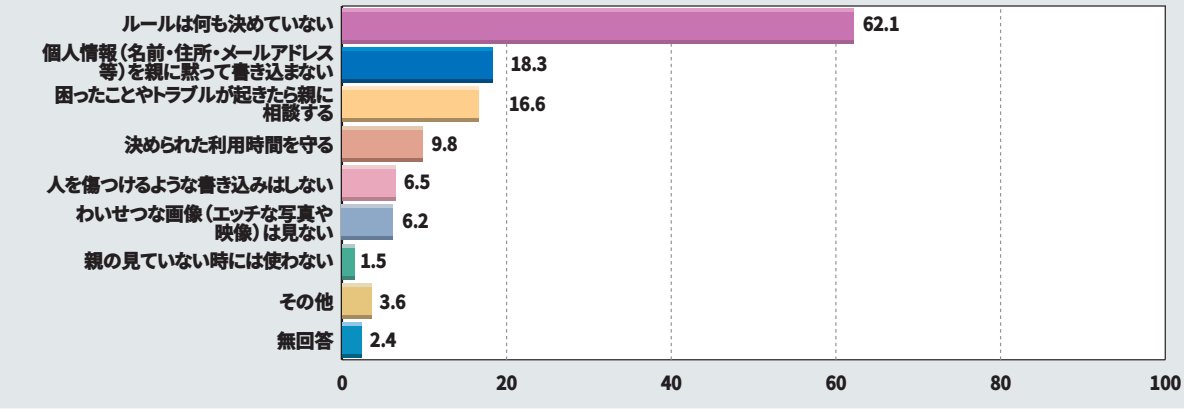


ウ　ルール無き子どものインターネット利用

中学生及び高校生に対して、インターネット利用に係る家庭でのルールについて質問したところ、「ルールは何も決めていない」と答えた者が62.1%に上った。

また、保護者に対して、子どもがインターネットを利用するときの保護者の態度について質問したところ、「何もせず、自由に使わせている」と答えた者が49.2%に上った。

図1 - 10　家庭でのルール



以上の意識調査の結果から、少年がインターネット上の違法・有害情報に容易にアクセスし得る状況が放置されているのは、コンピュータや携帯電話にフィルタリング・ソフト又はサービスを付加せずに、子どもにインターネットを自由に使用させているなど、保護者の意識や取組みが不十分であることが一因となっていることが分かる。

③　性や暴力に関する情報が少年に与える悪影響

インターネット上には、児童ポルノ、わいせつ画像等の性に関する情報や、人が殺害される画像、死体画像等の暴力に関する情報が氾濫しているが、少年がコンピュータや携帯電話によりインターネットを利用して、これらの情報に容易にアクセスすることができる状況となっている。

そのため、ウェブサイトで、女児への性的ないたずら、盗撮等の体験談等を読んだことで触発されたとみられる少年による性犯罪や、殺人・暴力に関するウェブサイトに影響を受けたとみられる少年による凶悪事件が発生するなど、性や暴力に関する情報が少年に与える悪影響が深刻な状況となっている。

事例　中学生の男子（14）は、15年12月、自宅において、鉄製の棒で実妹を数回殴打し、頭部等を負傷させた。同月、殺人未遂罪で逮捕した。この男子は、幼児期より家族の跡継ぎとして親や地域に期待されてきたことなどのストレスを感じてきたが、思春期に差し掛かり、学業や人間関係に行き詰まりを覚えて人間不信に陥り、人に殺されたり人を殺したりする悪夢を見て不眠に相当期間悩まされていたところ、殺人に関するウェブサイトに触発されて、些細なきっかけで敢行したものである（茨城）。

④　その他の少年に悪影響を及ぼす情報

出会い系サイト、性や暴力に関する情報以外にも、ウェブサイト上には、モデル、性風俗営業の営業所等で働く者等を募集するサイト、家出した少女に対し生活の方法等を教えるサイト、使用済み下着を販売するサイト等、少年の健全育成上問題のある情報や、少年を非行や犯罪被害に巻き込むおそれのある様々な情報に少年が容易にアクセスできるほか、電子掲示板等への書き込みに起因したトラブルも発生しており、その結果、少年が犯罪に巻き込まれた事件も発生している。

事例1　自営業の男（42）は、17年3月、携帯電話からアクセスすることのできる電子掲示板に、モデル募集目的の求人広告を掲載し、応募してきた中学生の女子（15歳）に対して、現金3万円を供与する約束をして性交し児童買春するとともに、同女子の裸体をビデオカメラで撮影して、児童ポルノを製造した。同年10月、同自営業の男を児童買春・児童ポルノ法違反（児童買春、児童ポルノ製造）で逮捕した（埼玉）。

事例2　小学生の女児（11）は、16年6月、小学校において同級生の女児の首をカッターナイフで切りつけ、殺害した。加害者の女児は、交換ノートや電子掲示板に記載された内容を見ているうちに、自分が馬鹿にされ、批判されているように感じて、怒りを募らせ、殺害しようと決意するに至ったものである（長崎）。

コラム 2　家出サイト

家出サイトとは、家出中に収入を得る方法や宿泊地を探す方法等家出を助長する情報を掲載しているウェブサイトであり、家出をしようとする者とこれを受け入れることを希望する者との間で情報交換をするための電子掲示板を設けているウェブサイトも存在する。この電子掲示板を利用して家出をした少女を受け入れた男が、少女に対してわいせつな行為をする事案が発生するなど、少年の健全な育成を図る観点からも問題があると指摘されている。

（3）インターネット社会が生み出した新たな犯罪

情報通信ネットワークの発展に伴い、インターネットが国民に身近なものとなる一方で、サイバー犯罪(注)の検挙件数及びインターネット上でのトラブル等に関する相談件数は増加傾向にあり、犯罪の手口についても高度化・多様化している状況にある。

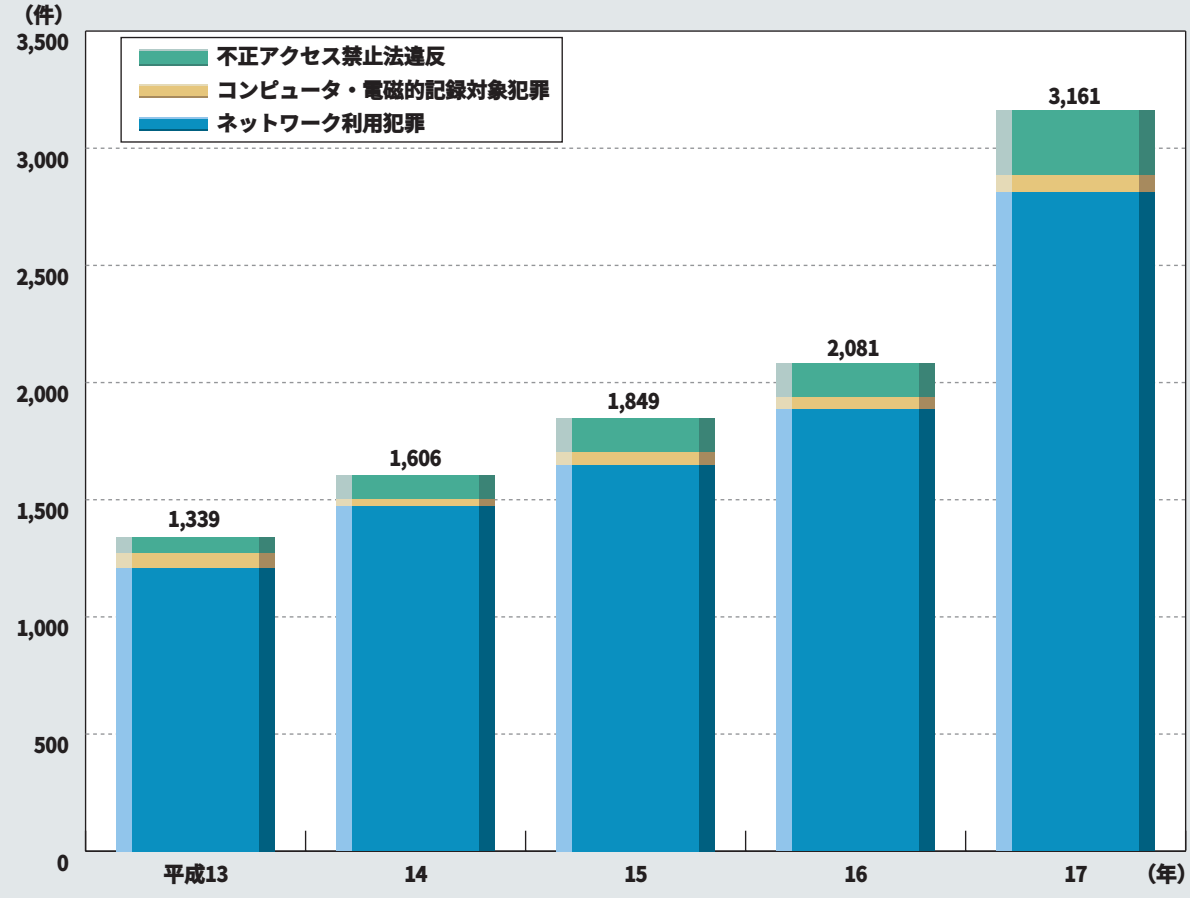
①　犯罪の手段として利用されるインターネット

サイバー犯罪は、①匿名性が高い、②痕跡が残りにくい、③地理的・時間的制約を受けることなく、短期間のうちに不特定又は多数の者に被害を及ぼすといった特徴を有しており、犯罪を行う者にとっては、その所在を特定されにくいなど、インターネットは極めて好都合な犯行の手段となっている。実際に相手の顔が見えないやり取りの中で、抵抗感なく犯罪に手を染めている者もいる。

ア　経済的利益を追求したサイバー犯罪の増加

サイバー犯罪の検挙件数は、年々増加しており、17年中の検挙件数は3,161件と、前年より1,080件（51.9%）増加し、過去最高となった。近年は、詐欺等経済的利益を追求したサイバー犯罪が増加する傾向が顕著である。

図1 - 11　サイバー犯罪の検挙件数の推移



注：インターネット等の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、情報技術を利用した犯罪

表1-4　サイバー犯罪の検挙件数の内訳（平成13～17年）

罪名＼年	13	14	15	16	17
不正アクセス禁止法違反　（件）	67	105	145	142	277
コンピュータ・電磁的記録対象犯罪	63	30	55	55	73
電子計算機使用詐欺	48	18	34	42	49
電磁的記録不正作出・毀棄	11	8	12	8	17
電子計算機損壊等業務妨害	4	4	9	5	7
ネットワーク利用犯罪	1,209	1,471	1,649	1,884	2,811
詐欺	485	514	521	542	1,408
児童買春・児童ポルノ法違反（児童買春）	117	268	269	370	320
児童買春・児童ポルノ法違反（児童ポルノ）	128	140	102	85	136
青少年保護育成条例違反	10	70	120	136	174
わいせつ物頒布等	103	109	113	121	125
著作権法違反	86	66	87	174	128
商標法違反	31	37	95	82	109
脅迫	40	33	38	58	39
名誉毀損	42	27	46	26	47
その他	167	207	258	290	325
合　計	1,339	1,606	1,849	2,081	3,161

（ア）　ネットワーク利用犯罪

17年中のネットワーク利用犯罪(注)の検挙件数は2,811件と、前年より927件（49.2%）増加した。特に、詐欺の検挙件数が、前年の2.6倍と急増しており、中でもインターネット・オークションを利用した詐欺等の経済的利益を追求したサイバー犯罪の検挙件数が多くを占めている。

事例1　無職の男（36）ら2人は、16年9月から同年10月にかけて、インターネット・オークションにおいて家電製品を売ると偽り、164人から約1,500万円をだまし取った。17年1月、詐欺罪で逮捕した（千葉）。

事例2　無職の男（34）は、電子掲示板を通じて共犯者を募り、17年6月から18年5月にかけて、フィッシング詐欺の手法を用いて、実在するインターネット・オークション運営会社を装って不特定多数の者に電子メールを送り、同社のウェブサイトに見せ掛けて作成した偽のウェブサイトを閲覧するよう誘導し、これを本物のウェブサイトであると誤信した者に識別符号（ＩＤ、パスワード等）を入力させてこれを不正に取得した上、無職の女（41）らにこの識別符号を使って不正アクセスさせ、他人になりすまして商品を架空に出品させ、落札した者から代金をだまし取った。18年5月、無職の男ら8人を詐欺罪及び不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）違反（不正アクセス行為）で逮捕した。共犯者である女らは、この詐欺をインターネット上で行うことから、容易に逮捕されることはないだろうと考え、電子掲示板の募集に気軽に申し込んできたものである（京都、静岡、熊本）。

注：その実行に必要不可欠な手段として情報通信ネットワークを利用する犯罪

また、インターネット上には偽ブランド品や海賊版のＣＤ、ＤＶＤ等の販売に関する情報が氾濫している。中でも、最近はインターネット・オークションを利用した偽ブランド品や海賊版のＣＤ、ＤＶＤ等の出品が増加している傾向にあり、17年中の知的財産権侵害事犯の約３割がインターネットを利用したもので、そのうちの約９割がインターネット・オークションを利用したものであった。

事例3　無職の男（21）は、17年7月から同年８月にかけて、携帯電話からアクセスすることのできるインターネット・オークションを利用して偽ブランド品を販売した。17年8月、商標法違反（販売目的所持、販売譲渡）で逮捕した（徳島）。

コラム 3　インターネット上の知的財産権侵害に対する事業者の取組み

ヤフー株式会社においては、インターネット上の違法・有害情報対策として次の取組みを推進している。

○　サイトの監視及び知的財産権を侵害する情報の削除等の措置

インターネット・オークションサイトにおいて知的財産権を侵害する情報を把握するため、24時間体制で自社において運営するサイトを監視している。

また、同社では法務部門において作成した厳格な判断基準にのっとり、削除等の措置を講じており、17年中にはインターネット・オークションサイトにおいて、知的財産権を侵害する出品52万398件（商標法違反36万8,816件、著作権法違反15万1,582件。全出品数の0.3％）について自主的に削除措置を行った。

○　ＩＤを取得する際の本人確認の強化及び利用者のモラル啓発

インターネット・オークションを利用するために必要なＩＤを取得する際には、他人名義や架空名義での登録を防止するため、配達証明郵便を利用した本人確認を導入するなど、本人確認を強化している。

また、インターネット・オークションの利用者に対して、ウェブサイト上において知的財産権侵害を行わないよう呼び掛けるなど、利用者のモラルを啓発する活動を推進している。

（イ）　不正アクセス禁止法違反

17年中の不正アクセス禁止法違反の検挙件数は277件と、前年より135件（95.1％）増加し、過去最高を記録した。不正アクセス行為は他の犯罪を実行するための手段として用いられることが多く、17年中の不正アクセス禁止法違反のうち不正アクセス行為に係る検挙件数は271件であったが、このうち「不正に金を得るため」を動機とするものが167件に上り、前年の５倍以上に増加している。このように、不正アクセス行為の多くが経済的利益を追求したサイバー犯罪の手段として用いられていることが分かる。

また、「顧客データの収集等情報を不正に入手するため」を動機とするものも23件と、前年の1.9倍に増加している。

事　例　大学生の男（27）は、17年3月、他人の個人情報を入手する目的で、旅行会社が設置・管理するウェブサーバを経由して、個人情報を管理するデータベース・サーバに、ＳＱＬインジェクションと呼ばれる不正アクセス行為を約19万回行い、同社の会員の氏名、住所、パスワード等の個人情報約16万件を不正に入手し、販売した。17年6月、不正アクセス禁止法違反（不正アクセス行為）で逮捕した（警視庁）。

図1 - 12　不正アクセス禁止法違反の検挙状況

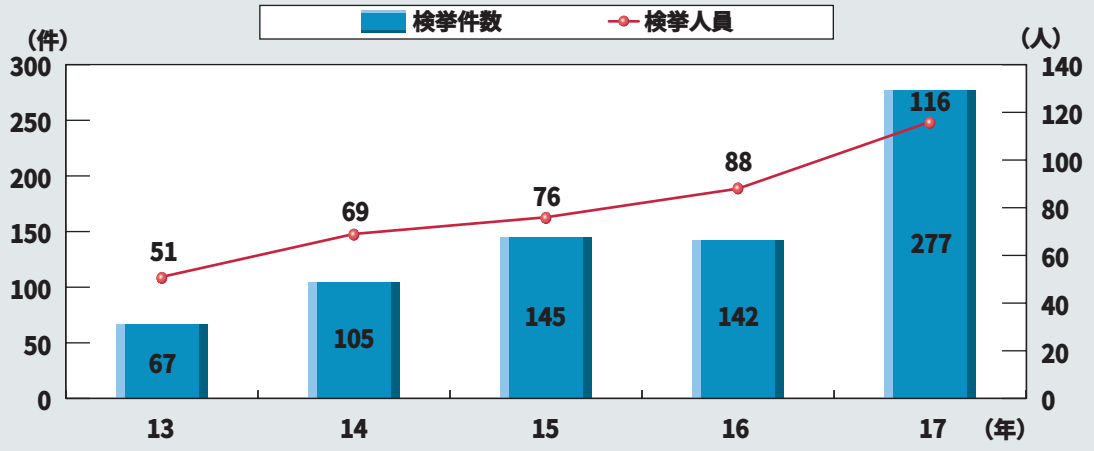


表1 - 5　不正アクセス行為の動機

動　機	16	17
不正に金を得るため	32	167
嫌がらせや仕返しのため	35	31
オンラインゲームで不正操作を行うため	31	25
顧客データの収集等情報を不正に入手するため	12	23
好奇心を満たすため	23	20
自分の技量を計るため	0	2
その他	9	3

注：不正アクセス禁止法第４条違反（不正アクセス助長行為）の検挙件数（16年中０件、17年中６件）は含まない。

コラム 4　ＳＱＬインジェクション

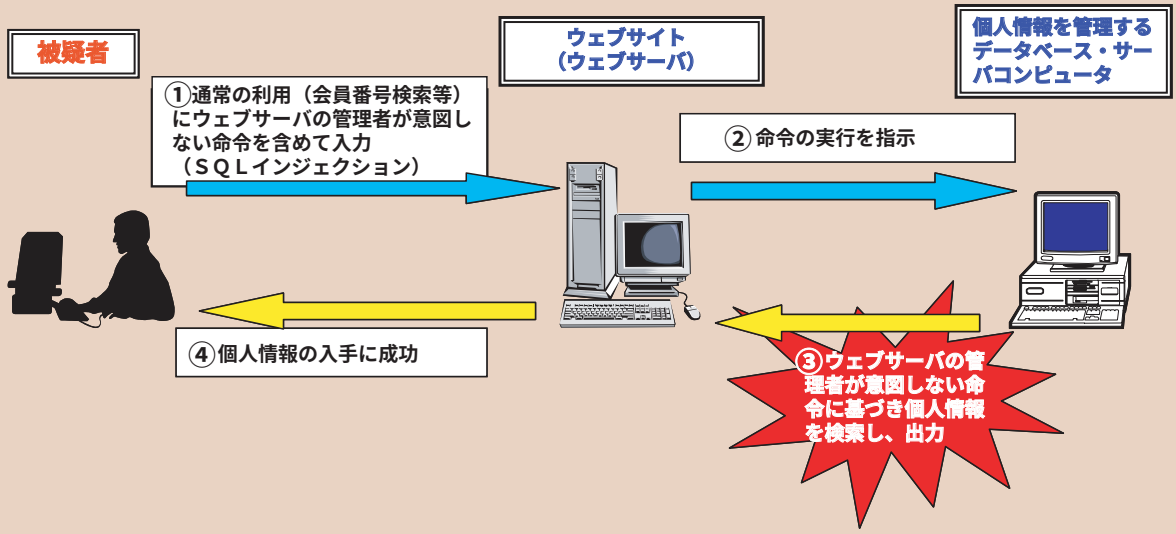
ＳＱＬインジェクションとは、ＳＱＬ(注)というプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

ＳＱＬは、データベースに記録された会員情報を閲覧したり、更新したりするウェブサイト上で用いられるが、ウェブサーバの管理者の意図しない命令が入力された場合、システム上の脆弱性を突かれ、データベース内の個人情報等が不正に取得される。

データベースは大量のデータを管理するのに便利であるが、このような手段によって、大量の情報が流出する可能性があるため、ウェブサーバの管理者は十分な注意が必要である。

注：Structured Query Languageの略で、データベースの構造設計やデータの検索、更新等を行うためのプログラム言語の一種

図1 - 13　ＳＱＬインジェクションによる不正アクセス行為



イ　経済的利益を目的とするサイバー犯罪に関する相談の増加

17年中のサイバー犯罪等に関する相談の受理件数は８万4,173件と、５年間で4.9倍に増加し、過去最高となった。このうち、「利用した覚えのない利用料金を請求する電子メールが携帯電話に送り付けられて困っている」、「ウェブサイトを閲覧し、画面上のボタンをクリックしただけで『会員登録されたので料金を振り込め』等と表示された」等の詐欺・悪質商法に関する相談が21.1倍、「インターネット・オークションで落札し、代金を振り込んだが商品が送られてこない」等のインターネット・オークションに関する相談が8.3倍に増加するなど、経済的利益を目的とするサイバー犯罪の被害に関する相談が全体の70.0%を占めている。

表1 - 6　サイバー犯罪等に関する相談の内訳（平成13～17年）

区分＼年	13	14	15	16	17
詐欺・悪質商法に関する相談（インターネット・オークション関係を除く。）	1,963	3,193	20,738	35,329	41,480
インターネット・オークションに関する相談	2,099	3,978	5,999	13,535	17,451
名誉毀損、誹謗中傷等に関する相談	2,267	2,566	2,619	3,685	5,782
違法・有害情報に関する相談	3,282	2,261	4,225	4,157	5,317
迷惑メールに関する相談	2,647	2,130	2,329	3,946	3,975
不正アクセス、コンピュータ・ウイルスに関する相談	1,335	1,246	1,147	2,160	3,965
その他	3,684	3,955	4,697	7,802	6,203
合　　計	17,277	19,329	41,754	70,614	84,173

コラム 5 インターネットを利用した架空請求に注意

インターネットを利用した架空請求の被害に遭わないためには、日ごろから、

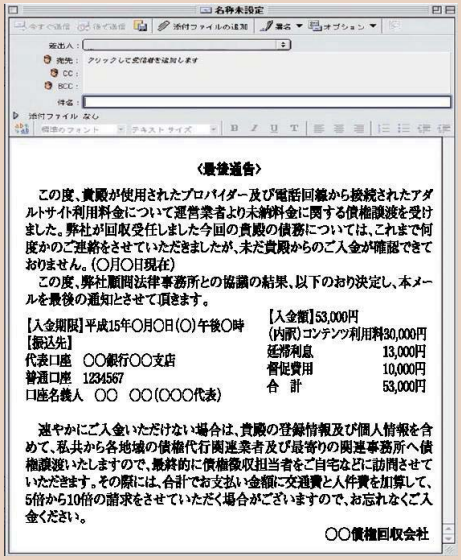
・　心当たりのないアドレスからの電子メールは開かない
・　利用規約は必ず確認する

といったことを心掛けてインターネットを利用する。

また、インターネットを利用している際に、架空請求をされた場合には、

・　請求をしてきた相手に電子メールや電話等で問い合わせや連絡をしない
・　請求内容を確認し、証拠を保存しておく
・　判断に迷う場合には、消費生活センターや最寄りの警察署等に相談する

ことが適切である。



〈最後通告〉

この度、貴殿が使用されたプロバイダー及び電話回線から接続されたアダルトサイト利用料金について運営業者より未納料金に関する債権譲渡を受けました。弊社が回収受任しました今回の貴殿の債務については、これまで何度かのご連絡をさせていただきましたが、未だ貴殿からのご入金が確認できておりません。(〇月〇日現在)

この度、弊社顧問法律事務所との協議の結果、以下のとおり決定し、本メールを最後の通知とさせて頂きます。

【入金期限】平成15年〇月〇日(〇)午後〇時
【振込先】
代表口座　〇〇銀行〇〇支店
普通口座　1234567
口座名義人　〇〇　〇〇(〇〇〇代表)

【入金額】53,000円
(内訳)コンテンツ利用料30,000円
延滞利息　13,000円
督促費用　10,000円
合　計　53,000円

速やかにご入金いただけない場合は、貴殿の登録情報及び個人情報を含めて、私共から各地域の債権代行関連業者及び最寄りの関連事務所へ債権譲渡いたしますので、最終的に債権徴収担当者をご自宅などに訪問させていただきます。その際には、合計でお支払い金額に交通費と人件費を加算して、5倍から10倍の請求をさせていただく場合がございますので、お忘れなくご入金ください。

〇〇債権回収会社

架空請求の例（見本）

コラム 6 インターネット・オークションを利用した詐欺の被害に遭わないために

インターネット・オークションを利用した詐欺の被害に遭わないためには、

・　出品者の評価を確認する（ただし、出品者が自ら評価を操作している可能性があるので注意する）
・　取引をする前に電話で連絡を取り、住所や連絡先を確認する
・　利用するインターネット・オークションサイトのトラブルリスト（トラブルの多い出品者や預貯金口座番号等のリスト）を確認する
・　少しでも不安を感じたときは、取引をやめる

といった点に留意する必要がある。

②　情報通信技術の発展に伴う新たな脅威

情報通信技術の発展に伴い、サイバー犯罪の手口も高度化・多様化しており、ワーム型のコンピュータ・ウイルス(注)がまん延し、スパイウェア、フィッシングといった高度な技術を利用した犯罪も発生している。

ア　コンピュータ・ウイルス

コンピュータ・ウイルスとは、コンピュータに感染して、利用者の意図する動作をさせなかったり、意図に反する動作をしたり、コンピュータの機能を破壊したりするプログラムをいう。

コンピュータ・ウイルスは、電子メールやＣＤ－ＲＯＭ等に添付されるなどしてコンピュータ内に侵入するほか、コンピュータの脆弱性等を利用して侵入するもの、他のファイルに偽装し、ファイル共有ソフト等を通じて感染を広げるものもある。また、コンピュータに感染後、自動的に感染を繰り返す自己増殖型のコンピュータ・ウイルスも発生しており、その感染力は高く、一国のインターネット網を一次的に麻痺させた事例（第１章第１節（４）①ア事例４（25頁）参照）もある。17年中は、ソバー（Sober）、ゾトブ（Zotob）といったコンピュータ・ウイルスの発生が確認されているほか、最近では、ファイル共有ソフトを介して感染したコンピュータの情報を流出させるコンピュータ・ウイルスによる被害が多方面で発生している。

一般的に、コンピュータ・ウイルスが出現してからそのコンピュータ・ウイルスの対策ソフトが更新されるまでには一定の時間がかかることから、最新のコンピュータ・ウイルス対策ソフトを利用していても、新たなコンピュータ・ウイルスが出現した場合、対策ソフトの更新が間に合わず、感染してしまう可能性は常に存在する。

今後も、このような新たな機能を有するコンピュータ・ウイルスが発生する可能性があり、その被害の拡大に関して、十分に注意する必要がある。

コラム 7　ファイル共有ソフトを介して情報流出させるコンピュータ・ウイルス

いわゆるファイル共有ソフトは、同種のソフトウェアを利用する不特定多数のコンピュータの中から特定の情報を持つコンピュータを探し出し、特定のサーバコンピュータを経由せずに、不特定多数の者が相互に直接情報を共有するものであるが、このソフトウェアを利用して著作権法に違反する情報共有を行っていた事件も検挙されている。

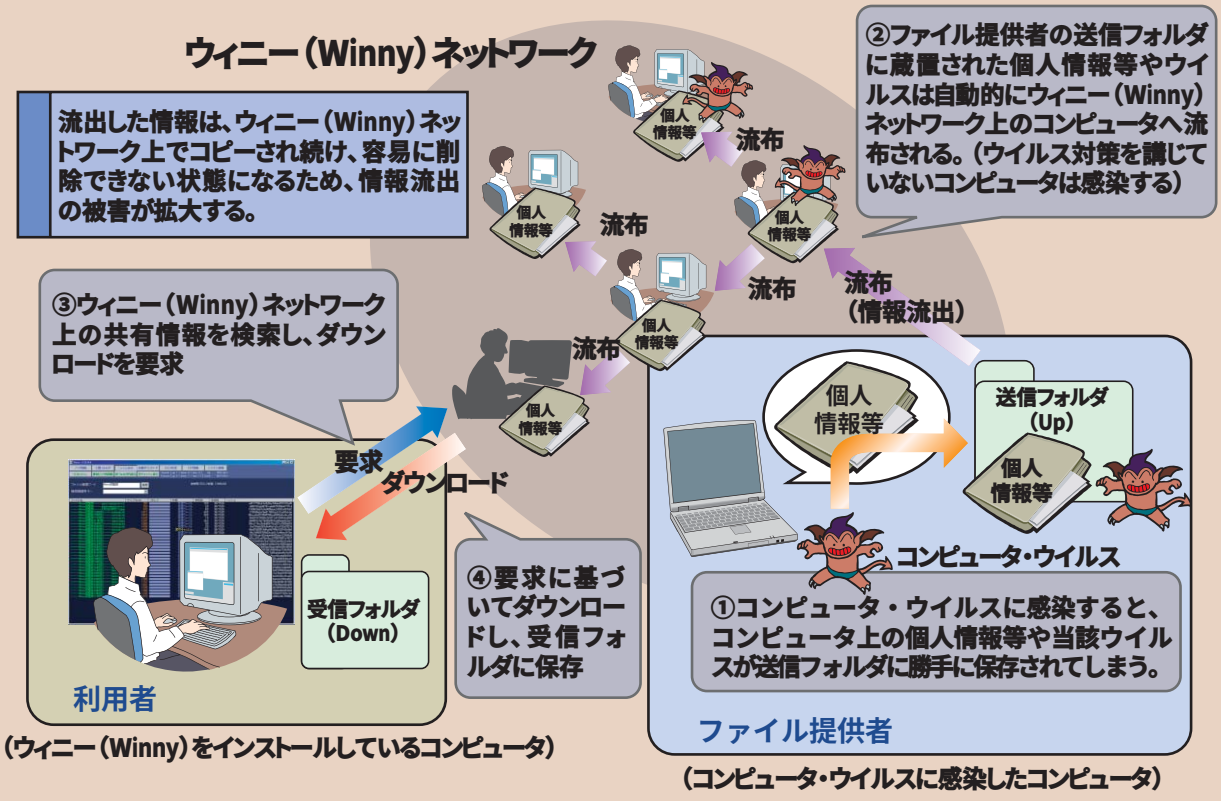
また、近年、ファイル共有ソフトを介して感染を拡大するコンピュータ・ウイルスの出現によって、多くの情報流出事案が発生し、社会問題化している。特に、ウィニー（Winny）と呼ばれるファイル共有ソフトでは、一たび情報が流出すると、同種ソフトウェアを利用する不特定多数の者のコンピュータを経由しながら情報が拡散するため、当該情報を削除することが非常に困難となる。さらに、情報と共に流出したコンピュータ・ウイルスが更に多数の者に感染し、被害を拡大することとなる。

最近では、ウィニー（Winny）に類するファイル共有ソフトであるシェア（Share）においても、同種のコンピュータ・ウイルスによる情報流出事案が発生している。

ウィニー（Winny）やシェア（Share）だけでなく、ファイル共有ソフトには様々な種類が存在しており、今後、同種のコンピュータ・ウイルスによる情報流出事案の発生も懸念される。

注：コンピュータ・ネットワークを利用して他のホストコンピュータに自分自身のコピーを送り込んで自己増殖し、ファイルには感染せずに、単独のプログラムとして動作するコンピュータ・ウイルス

図1 - 14　ウィニー（Winny）上で感染するコンピュータ・ウイルスによる情報流出



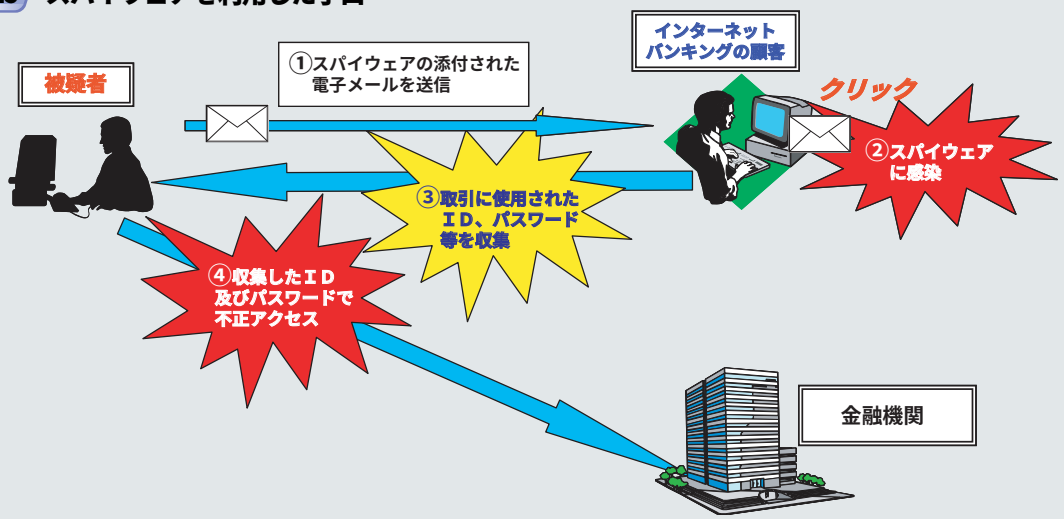
イ　スパイウェア

スパイウェアとは、コンピュータのハードディスク等に記録された情報やキーボードの操作（入力）情報、表示画面の情報等を外部に流出させる機能を有するプログラムをいう。

このようなプログラムは、プログラム自体がコンピュータ上で動作していることを隠ぺいする機能を備えているものもあり、専用のソフトウェアを用いなければ削除等を行うのが困難なものもある。

インターネット・バンキングやオンラインショッピング等インターネットを通じて預貯金口座番号やクレジットカード番号等の情報を入力する機会が増加していることから、スパイウェアによりこれらの情報が流出した事案も発生している。

図1 - 15　スパイウェアを利用した手口



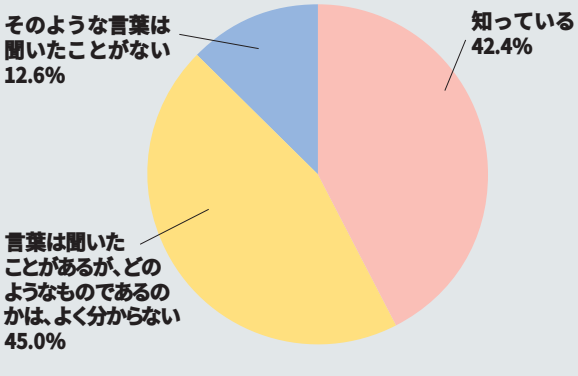
事例５　無職の男（３４）らは、１７年６月から７月にかけて、インターネット・バンキングを使用している会社に対して、取引上の苦情を装った電子メールにスパイウェアを添付して送りつけ、同社がインターネット・バンキングにアクセスするために必要な識別符号を取得し、インターネット・バンキングに不正アクセスして同社の預貯金口座から男の管理する他人名義の預貯金口座に対して約２１万円を送金する操作を行った。１７年１１月、電子計算機使用詐欺罪及び不正アクセス禁止法違反（不正アクセス行為）で逮捕した（警視庁）。

警察庁では、18年３月、インターネット利用者を対象にインターネット利用に関する意識調査(注)を行った。

スパイウェアというソフトウェアはどのようなものか知っているかと質問したところ、「言葉は聞いたことがあるが、どのようなものかよく分からない」又は「そのような言葉は聞いたことがない」と回答した者が57.6%と過半数を占めていた。

既にスパイウェアを悪用した犯罪が発生していることを踏まえ、新たな犯罪被害を防止する観点から、スパイウェアの危険性について国民に対する広報啓発等を徹底する必要がある。

図1 - 16　スパイウェアの認知度



注：５頁の意識調査と同一のもの

コラム 8 スパイウェア対策

スパイウェアについては、従来は
- ウェブサイトを閲覧した際
- ソフトウェアをインストールした際

に自分のコンピュータにインストールされる事例が見られたが、最近ではこれらに加え、
- 送付されてきた電子メールの添付ファイルを開いた際
- 郵送されてきたCD-ROMを利用した際

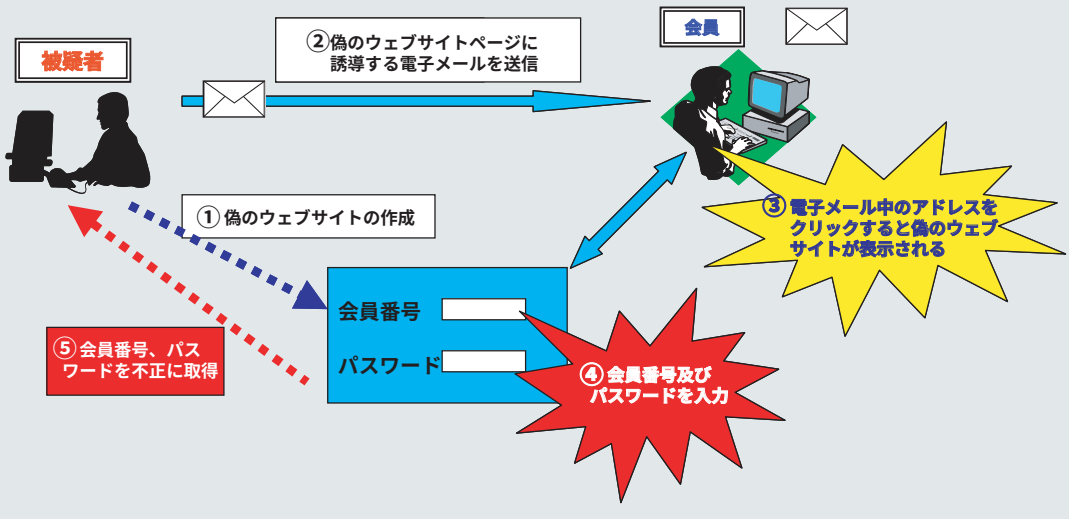
等にインストールされる事例が見られている。スパイウェアを間違ってインストールしないようにするためには、
- 不審なウェブサイトにはアクセスしない
- 不審なソフトウェアはインストールしない
- 不審なCD-ROMを使用しない
- 不審な電子メールの添付ファイルは開かない

ことが重要である。また、オペレーティング・システム等のソフトウェアをアップデートしたり、ウイルス対策ソフトやファイアウォールを利用したりするなどの防御策を重層的に講ずることが有効である。

ウ　フィッシング（Phishing）(注)

フィッシングとは、銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトに見せかけて作成した偽のウェブサイトを受信者が閲覧するよう誘導し、そこにクレジットカード番号、インターネット上で個人を識別するためのＩＤ、パスワード等を入力させて、金融情報や個人情報を不正に入手する行為をいう。日本においても、17年中、大手プロバイダのウェブサイトを装った偽のウェブサイトが確認されており、今後、同じような事案が増加することが懸念される。

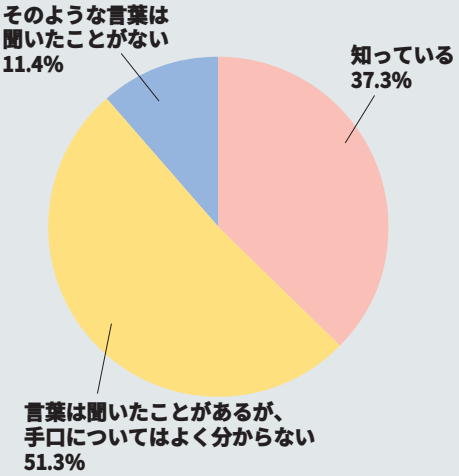
図1-17 フィッシングの手口



注：「Phishing」という英語のつづりは、利用者を「釣る」という意味の「fishing」と、その手口が「洗練されている」という意味の「sophisticated」を合わせた造語であるなどといわれている。

警察庁が実施した意識調査(注)において、フィッシングの手口を知っているかと質問したところ、「言葉は聞いたことがあるが、手口についてはよく分からない」又は「そのような言葉は聞いたことがない」と回答した者が62.7%と過半数を占めた。犯罪被害を防止する観点から、今後、フィッシングの危険性について国民に対する広報啓発等を徹底する必要がある。

図1-18　フィッシングの認知度



事例6　会社員の男（42）は、17年2月、プロバイダが会員に付与した識別符号を不正に入手する目的で、同社が著作権を有するウェブサイトに酷似した偽のウェブサイトをインターネット上に公開し、これを本物のウェブサイトであると誤信した者が入力した識別符号を不正に取得し、これを用いて不正アクセス行為を行った。17年6月、著作権法違反（著作権侵害）及び不正アクセス禁止法違反（不正アクセス行為）で逮捕した（警視庁）。

コラム9　フィッシング対策

フィッシングによる被害に遭わないようにするためには、

- 電子メールやウェブサイトで個人情報の入力を求められても安易に応答しない
- 金融機関等の名前で不審な電子メール等が来たときは、その電子メール等に記載された連絡先を信用せず、その金融機関等の連絡先を電話番号案内等で確認した上で、直接問い合わせる

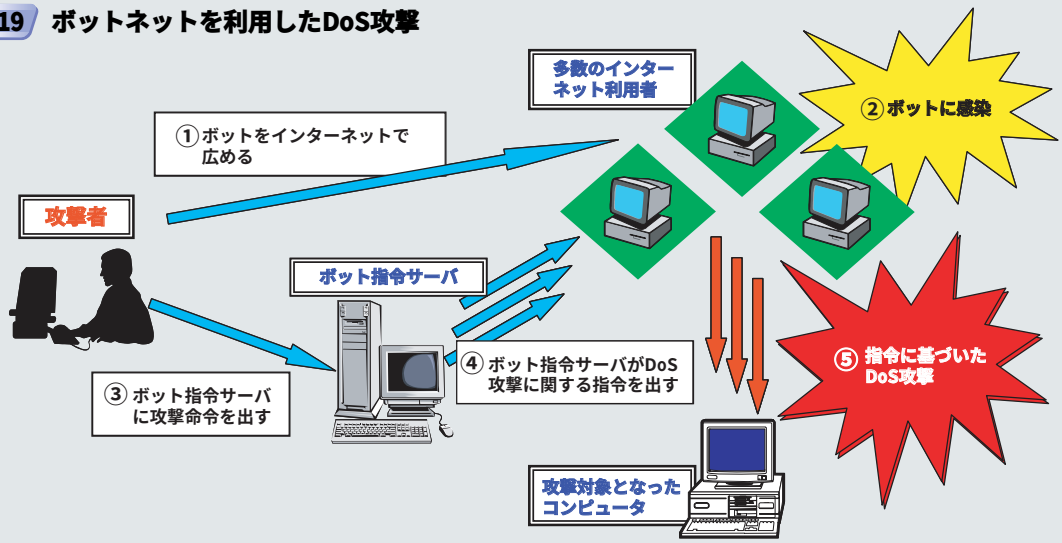
ことが重要である。

注：５頁の意識調査と同一のもの

エ　ボットネット

ボットネットとは、攻撃者の命令に基づき動作するプログラム（ボット）に感染したコンピュータ及び攻撃者の命令を送信する指令サーバ（ボット指令サーバ）からなるネットワークであり、中には数万台規模のコンピュータ等からなるボットネットも確認されている。攻撃者は一度の命令で多数のコンピュータを操作することができるので、例えば、特定のコンピュータに対して同時に多数のアクセスを行う命令を出せば、容易にDoS攻撃(注1)を行うことができる。この場合、多数のコンピュータが攻撃を行っているため、開始された攻撃を停止させるのは困難である。

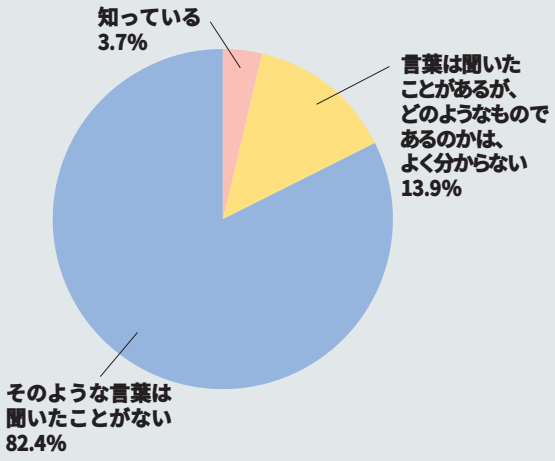
図1 - 19　ボットネットを利用したDoS攻撃



警察庁が実施した意識調査(注2)において、ボットネットを知っているかと質問したところ、「知っている」と回答した者は3.7%にとどまった。

ボットネットは、一般のインターネット利用者を不正な攻撃に関与させることになり、その社会的危険性は極めて大きいことから、今後、更にインターネット利用者に対する注意喚起を行う必要がある。

図1 - 20　ボットネットの認知度



注1：Denial of Service攻撃の略。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
2：５頁の意識調査と同一のもの

（4）公共の安全を害するサイバーテロ等の脅威

①　サイバーテロ(注1)の脅威

ア　サイバーテロが発生し得るネットワーク環境の現状

情報通信ネットワークの発展により、国民生活や社会・経済活動の基盤（重要インフラ(注2)）において、情報通信技術の利用が急速に進んでいる。特に、株式売買システム、銀行の勘定系システム、航空管制システム、列車運行制御システム、送配電システム等は、重要インフラにおける基幹システムとして、安定的なサービスを供給する上で重要な役割を果たしている。サイバー攻撃等によってその機能が損なわれた場合、国民生活や社会・経済活動に大きな混乱をもたらし、公共の安全と秩序の維持に重大な影響を与えかねない。また、サイバーテロは、コンピュータとネットワークへのアクセスが確保できれば、時と場所を選ばず実行が可能であることから、社会に大きな被害を与えるテロの敢行を利する巧妙な手法であると指摘されている。

平成15年３月及び17年11月に基幹システムにおいて発生した機能障害事案は、サイバーテロに起因するとは認められないものの、国民生活や社会・経済活動に混乱を生じさせた。

事例1　15年3月、国土交通省東京航空交通管制部にある航空管制システムの一部が停止した。これにより、約20分間、全国の空港において航空機が離陸できなくなった。システムの復旧後も航空機の離陸を制限する措置がとられ、その影響は約30万人に及んだ。

事例2　17年11月、東京証券取引所の株式売買システムが起動せず、午前中の取引が行えなかった。

他方、16年８月のウェブサーバに対するDoS攻撃事案、15年１月の大規模なインターネット接続障害事案は、基幹システムに対する攻撃ではなく、いずれもサイバーテロとは認められないが、これらの事案で用いられた手法は、サイバーテロに容易に利用されるおそれがある。

事例3　16年8月、首相官邸や警察庁を始めとする政府機関や靖国神社等のウェブサーバに対して、DoS攻撃が行われ、これらのウェブサイトが一時的に閲覧困難な状態となった。

事例4　2003年（15年）1月、データベースサーバ用のプログラムの欠陥（セキュリティ・ホール）を利用して攻撃するコンピュータ・ウイルスが、インターネットを通じて急速に世界的に拡散した。感染したサーバは、即座にコンピュータ・ウイルスを複製し、他のサーバへの送信を繰り返すため、インターネットの負荷が急増し、特に韓国では、インターネットが約9時間にわたって麻痺(ひ)状態に陥った。

重要インフラの基幹システムにおける重大な機能障害の発生や、サイバーテロに容易に利用される手段を用いたサイバー攻撃事案の発生は、サイバーテロが発生した時の影響の大きさを表すとともに、サイバーテロが現実に発生し得るものであることを示している。このように、現代社会は正にサイバーテロの脅威にさらされていると言える。

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
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、物流の各分野における社会基盤

イ　サイバーテロに用いられる手段

（ア）　不正アクセス行為（第１章第１節（３）①ア（イ）（15頁）参照）

17年中、世界で使用されるソフトウェアに関し、不正アクセス行為を許すなどの脆弱性があるとして、米国において、国土安全保障省（DHS）(注1) が設置した米国コンピュータ緊急対応班（ＵＳ-ＣＥＲＴ）(注2) に報告された件数は5,198件であった。その脆弱性を修正するためのプログラム（パッチ）が提供されるまでには、一定の時間を要することから、その間に不正アクセス行為を手段としたサイバーテロが敢行される可能性の高い状態が続くこととなる。

（イ）　不正プログラム

a　コンピュータ・ウイルス（第１章第１節（３）②ア（19頁）参照）

コンピュータ・ウイルスは、多数のコンピュータに感染し、その機能を停止させたり、情報を破壊したりして、被害を拡大するほか、膨大な数のコンピュータ・ウイルスがインターネットを行き交うことによって、回線を圧迫し、ネットワーク自体を麻痺させてしまうこともある。

また、コンピュータ・ウイルスは、外部記録媒体等を介して感染を拡大する危険性があり、インターネットに接続されていない重要インフラの基幹システムであっても、感染を完全に回避することは困難である。

世界中で、毎年、約1,000種 (注3) もの新たなコンピュータ・ウイルスが発生しており、ウイルス対策ソフトの更新には一定の時間を要することから、サイバーテロを引き起こすことを目的としたコンピュータ・ウイルスが作成された場合には、当該コンピュータ・ウイルスへの対策プログラムが作成されるまでの間はコンピュータ・ウイルスによるサイバーテロ発生の危険性が高い状態が続くこととなる。

b　ボットネット（第１章第１節（３）②エ（24頁）参照）

ボットネットを悪用すれば、ボットに感染した多数のコンピュータから、特定のコンピュータに対して、DoS攻撃等を仕掛けることができる。このため、重要インフラの基幹システムに対してボットネットによる攻撃が行われれば、機能停止等の事態を引き起こす危険性がある。

また、ボットネットは、短期間のうちに規模や形態を変えていくため、実態を把握することが困難であり、対策を講ずることが難しいことから、ボットネットを悪用したサイバーテロの発生は大きな脅威となっている。

コラム 10　ボットネットの観測結果

図１－21に示すように、17年中、警察庁が認知しただけでも、国内で延べ約15万、国外も含めると約134万ものコンピュータがボットに感染し、(注) これらが悪意ある利用者に自由に操作され得る状態にあった。ボットは指令サーバから指示された特定の範囲のＩＰアドレスに対して感染を拡大することがあるため、その影響を受けて、警察庁が観測に使用しているＩＰアドレスから比較的近い中国や韓国における感染数が多く検知されているものと推測される。

図１－22は、17年中に観測された「エスディーボット（Sdbot）」というボットの亜種の観測結果である。ボットネットはボットの感染と共に急速に規模を拡大するが、すぐに減少し始め、最終的に観測できなくなっている。これは、ボットネット自体が消滅したのではなく、指令サーバを通じてボットのプログラムが更新され、別の指令サーバの配下にボットが移されたためである。このように、ボットネットは、その規模や形態を短期間に変えるため、継続して観測及び分析することが困難である。そこで、サイバーフォースセンターでは、リアルタイム検知ネットワーク上のボットネット観測システムの高度化等を図り、動向を把握するための取組みを強化している。

注：ＩＰアドレス数から計算

注1：Department of Homeland Securityの略
2：United States Computer Emergency Readiness Teamの略。米国において、インターネット上の脅威やソフトウェアの脆弱性を分析することなどを行う団体
3：警察庁において把握した数

図1 - 21　ボットに感染したコンピュータの延べ数の国別比較（認知数）（平成17年）

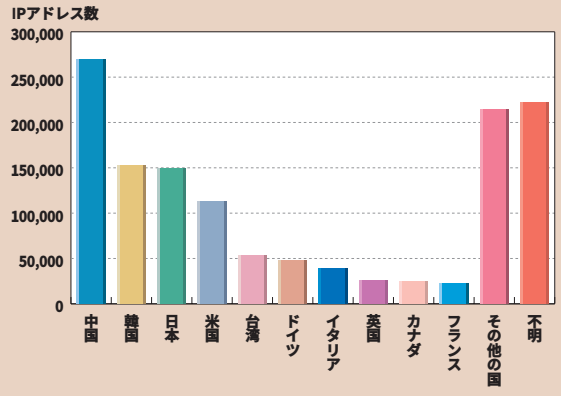
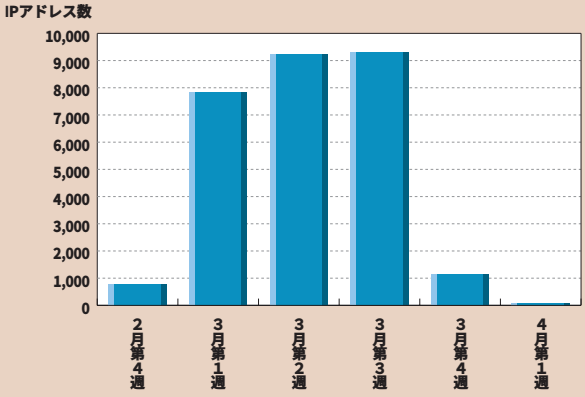


図1 - 22　ボットネットの観測例（平成17年）



ウ　サイバーテロに関する国民の意識

18年３月、警察庁が実施したインターネット利用に関する意識調査(注)において、サイバーテロの脅威を感じているかと質問したところ、30.6%の者が「いつ発生してもおかしくない現実のものとして、大変な脅威を感じている」と回答しており、「漠然とではあるが、脅威を感じている」と回答した者を加えると、84.9%の者がサイバーテロに対する脅威を少なからず感じていることが分かった。

また、サイバーテロ対策には何が必要かと質問したところ、88.1%の者が「重要インフラ事業者による対策」を、また、90.2%の者が「重要インフラ事業者と警察、所管省庁等公的機関の連携・協力」を、それぞれ更に強化すべきと回答した。

このように、サイバーテロはこれまで認知されていないが、多くの国民がサイバーテロに対して不安を抱き、その対策の必要性を感じている。そして、重要インフラ事業者による対策だけでなく、公的機関と重要インフラ事業者が連携してサイバーテロ対策に取り組むことが期待されている。

注：５頁の意識調査と同一のもの

図1 - 23　サイバーテロの脅威を感じているか

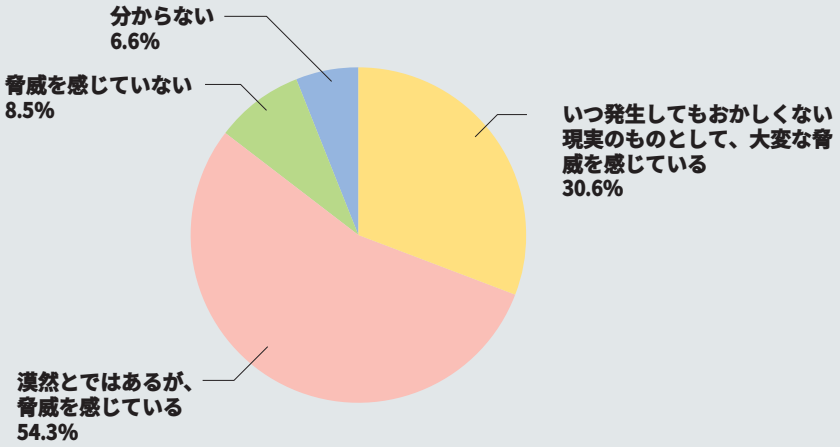
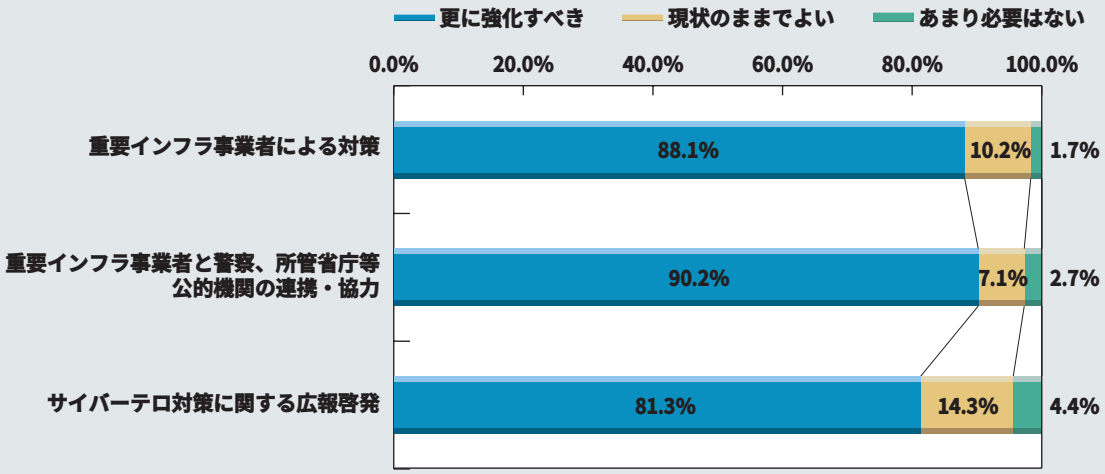


図1 - 24　サイバーテロ対策には何が必要か



②　国際テロ組織等によるインターネットの利用

インターネットの急速な普及に伴い、国際テロ組織や国際テロリストが、様々な形でインターネットを利用している。

ア　宣伝・勧誘を目的とした利用

多くの国際テロ組織等が、ウェブサイトを開設するなどして、自らの主張や活動の宣伝、新たなテロリスト等の勧誘を行っている。これは、多額の費用をかけることなく不特定又は多数の者に対し瞬時に働き掛けることができるインターネットの特性を利用したものとみられる。

例えば、国際テロ組織「アル・カーイダ」は、インターネットを通じて、指導者オサマ・ビンラディンやアイマン・アル・ザワヒリのものとされる声明を発し、米国に対する批判やジハード（聖戦）の呼び掛けを行っており、我が国をテロの対象として名指しした声明をインターネット上に公開したこともある。「よど号」グループのように、支援者がウェブサイトを開設し、活動の宣伝等を行っている例もみられる。

また、国際テロ組織等は、インターネットを通じて頻繁に犯行声明等を発している。例えば、2004年（16年）10月にイラクにおいて邦人旅行者が殺害された事件に関し、武装グループが邦人を人質とし、同国に派遣している自衛隊を撤退させるよう我が国に要求した映像等を、2005年（17年）５月に同国において武装グループが邦人の勤務する民間警備会社車列を襲撃し、同社の邦人社員が行方不明となった事件に際し、武装グループが邦人の勤務する民間警備会社の車列を襲撃する映像等を、それぞれインターネット上に公開した。

イ　相互の連絡を目的とした利用

国際テロ組織等は、テロの計画や準備に関する連絡・調整のため、電子メール、電子掲示板等を利用している。利用に際しては、暗号を用いて、情報内容の隠ぺいを図ることも多い。また、インターネットは、世界各地から利用できるため、活動地域や所属組織にとらわれず、広くテロリストの間で情報交換が行われていることが指摘されている。

例えば、「アル・カーイダ」、中東等においてテロ活動を実行してきた「ヒズボラ」等が、電子メール等を各種の活動のために利用していると指摘されている。

また、国際テロ組織等が、ウェブサイトに掲載した音声や画像等のデータに、一般には分からないようにメッセージを埋め込んで隠すステガノグラフィーという手法を利用していることも指摘されている。

ウ　情報収集を目的とした利用

インターネット上には、重要インフラ施設に関する情報や、爆発物、ＮＢＣ兵器(注)の製造方法、武器の入手方法等、テロの実行を容易にする情報が公開されている。国際テロ組織等は、こうした情報をインターネットを通じて入手しているものとみられる。

例えば、2005年（17年）に米国において未然に阻止された米軍関連施設、イスラエル権益等を対象としたテロ計画では、テロリストがテロの標的を選定するためにインターネットを利用していたとされている。

エ　資金獲得を目的とした利用

国際テロ組織等が、自己のウェブサイト上で人道支援を名目とした寄附を募り、得られた資金の一部をテロに活用するなど、インターネットをその資金獲得活動のためにも利用している。

例えば、2002年（14年）、「アル・カーイダ」等に対して支援を行っていたとして国際連合安全保障理事会決議に基づき資産凍結措置の対象に指定され、我が国も同様の措置を講じている「グローバル・リリーフ・ファウンデーション（ＧＲＦ）」が、インターネットを通じて寄附金を集めていたと指摘されている。

注：N（Nuclear：核）、B（Biological：生物）、C（Chemical：化学）物質を使用した兵器

第２節　サイバー空間の安全確保に向けた取組み

この節では、サイバー空間の安全を確保するための取組みについて紹介する。

（１）違法・有害情報対策

前節で述べたとおり、インターネット上における違法・有害情報の氾濫が深刻な社会問題となっていることから、警察では、サイバーパトロール等を通じた取締りを行うとともに、関係機関と連携して国民への広報啓発に努めている。また、プロバイダ等と協力して自殺予告事案への対応を図るなど違法・有害情報対策を推進している。

①　サイバーパトロールを通じた取締りの実施等

都道府県警察では、ウェブサイトや電子掲示板等を閲覧して違法・有害情報が掲載されていないかどうかを調査するサイバーパトロールを実施している。実施に当たっては、警察職員自らが行うほか、都道府県警察から委嘱されたサイバーパトロールモニター等や、特定非営利活動法人（ＮＰＯ法人）、消費生活センター等の関係機関・団体と連携している。

警察職員及びサイバーパトロールモニターから報告される情報並びに関係機関から寄せられる相談及び情報は、警察本部のサイバーパトロール担当者が一元的に把握して、その詳細を調査・分析している。これにより、インターネット上の違法・有害情報の発信状況を確認し、違法行為を検挙するほか、プロバイダや電子掲示板の管理者等に対して削除等の措置を講ずるよう要請するなど、違法・有害情報の氾濫とそれらによる被害の防止対策を推進している。

②　出会い系サイトに係る広報啓発

出会い系サイトによる子どもの犯罪被害を防止するため、平成17年９月、リーフレットを作成し、また、同年12月、中学生、高校生、保護者、出会い系サイト利用者や出会い系サイト事業者ごとの犯罪防止のための情報をウェブサイト（http://www.npa.go.jp/cyber/deai/index.html）で公開し、広報啓発活動を推進している。

出会い系サイト犯罪予防ウェブサイト

③　自殺予告事案への対応

近年、いわゆる自殺サイトにおいて自殺を予告する事案や自殺の呼び掛けを通じて知り合った者同士が自殺する事案が増加しており、深刻な社会問題となっている。

17年10月、業界団体では、警察庁及び総務省と連携し、インターネット上における自殺予告事案への対応に関するガイドラインを策定・公表した。このガイドラインを踏まえ、都道府県警察がプロバイダ等と連携して円滑に対応できるようにするため、インターネット上での自殺予告に係る対処要領を定めた。これらに基づき、都道府県警察は、17年10月５日から18年３月31日にかけてプロバイダや電子掲示板の管理者等から開示を受けた自殺を予告する者等に関する情報を基に、インターネット上の自殺予告事案に対応し、19人の自殺を行うおそれのあった者について説諭等の自殺の防止に係る措置をとった。

コラム 1　政府全体で取り組む違法・有害情報対策

政府では、17年2月、インターネット上における違法・有害情報等に関する関係省庁連絡会議（ＩＴ安心会議）(注)を内閣官房に設置し、インターネット上の違法・有害情報対策を検討している。特に、いわゆる自殺サイトで知り合った者同士が集団で自殺する事案が継続して発生している状況に加え、高校生がウェブサイトを見て爆発物を製造・使用した傷害事件が発生するなど、インターネット上の違法・有害情報が社会に及ぼす悪影響が問題視されたことから、これらに対する政府としての具体的な対処方針として、同年6月、「インターネット上における違法・有害情報対策について」を取りまとめた。

この対策における主要な項目は次のとおりである。

- フィルタリング・ソフトの普及
- プロバイダ等による自主規制の支援
- 違法・有害情報対策に関するモラル教育の充実
- 相談窓口の充実

注：インターネットの普及に伴い違法・有害情報の入手が容易となったことが、犯罪や人権侵害等の情報通信技術に関係する新たな社会問題の発生を助長しているとみられることから、この会議では、関係省庁の緊密な連携の下、国内外のインターネット上の違法・有害情報等に関連する様々な社会問題の実態把握やその対処、国民への周知等を推進している。

（2）サイバー犯罪対策

増加するサイバー犯罪に対応するため、サイバー犯罪対策に必要な法令の整備、態勢の強化に努め、取締りの徹底を図るとともに、国民に対する広報啓発、適切な相談対応等サイバー犯罪の未然防止等のための施策を推進している。

①　法令の整備

ア　風俗営業等の規制及び業務の適正化等に関する法律

平成10年５月、風俗営業等の規制及び業務の適正化等に関する法律が改正され、専ら性的好奇心をそそるため性的な行為を表す場面や衣服を脱いだ人の姿態の映像をインターネット等により有料で見せる営業を映像送信型性風俗特殊営業として規制の対象とし、この営業を営もうとする者に都道府県公安委員会への届出義務を課すほか、18歳未満の者を客とすることを禁止し、客が18歳未満でないことを確認する義務等を課すこととした（17年12月末現在、映像送信型性風俗特殊営業の届出件数は全国で2,575件で、年々増加している。）。

また、映像送信型性風俗特殊営業を営む者にウェブサーバを提供しているプロバイダ等には、このウェブサーバに映像送信型性風俗特殊営業を営む者がわいせつな映像又は児童ポルノ映像を記録したことを知ったときに、これらの映像の送信を防止するため必要な措置を講ずる努力義務が課せられ、当該プロバイダ等が努力義務を遵守していないと認められるときは、都道府県公安委員会は、これを遵守するよう当該プロバイダ等に勧告することができることとされた。

イ　不正アクセス禁止法

11年12月、他人の識別符号を不正に入力し、情報通信ネットワークを通じてコンピュータにアクセスする不正アクセス行為が多発し、社会問題となっていたことを踏まえ、不正アクセス禁止法が制定された。これにより、不正アクセス行為やそれを助長する行為を禁止するとともに、不正アクセス行為の被害を受けたアクセス管理者からの申出により、都道府県公安委員会が再発防止のために必要な資料の提供、助言、指導等の援助を行うこととされた。

ウ　古物営業法

14年11月、古物営業法が改正され、インターネット・オークションにおいて盗品その他犯罪によって領得された物（以下「盗品等」という。）が売買されることを防止するため、インターネット・オークションを営もうとする者の届出、義務、盗品等の疑いがある場合の申告義務、出品者の確認並びに取引記録の作成及び保存に関する努力義務、競りの中止命令に関する規定等が設けられたほか、盗品等の売買防止に資する業務方法を採用している事業者の認定制度が創設された（18年３月現在、13事業者を認定）。

エ　出会い系サイト規制法

15年６月、出会い系サイトの利用に起因する犯罪で多くの児童が深刻な被害を受けるようになったことを踏まえ、出会い系サイト規制法が制定された。これにより、出会い系サイトを利用して、18歳未満の児童を相手方とする性交等や対償を伴う異性交際を誘引することなどを禁止するとともに、事業者に対しては、児童の利用を防止するため、児童が利用してはならないことの明示及び利用者が児童でないことの確認を義務付け、これに違反した場合は、都道府県公安委員会が必要な措置を講ずるよう命ずることができることなどとされた。

オ　警察法

11年４月、増加するサイバー犯罪に的確に対処するため、情報通信の技術についての人的、物的資源を組織的に保有する部局である警察庁情報通信局に、電磁的記録の解析その他情報通信の技術を利用する犯罪の取締りのための情報通信の技術的事項を集約し、横断的に所掌させることとした。また、16年４月、サイバー犯罪に悪用される技術がますます高度化・複雑化し、その取締りには高度の技術的知見が必要とされるようになったことを踏まえ、サイバー犯罪捜査に対する技術支援を国が統轄し、全国的に技術水準を維持向上させることを国の責務として明確にするとともに、警察庁の情報通信部門に現場活動を中心とした技術支援を行わせることとされた。

なお、８年６月、警察庁長官は、特定のサイバー犯罪を含む広域組織犯罪等に対処するために必要があると認めるときは、都道府県警察に対し、広域組織犯罪等に対処するための警察の態勢に関する事項について必要な指示をすることができることとされた。

②　サイバー犯罪の未然防止に向けた取組み

ア　広報啓発活動

警察では、情報セキュリティに関する国民の知識及び意識の向上を図るため、警察やプロバイダ連絡協議会等が主催する研修会、学校関係者等からの依頼による講演会、地域の各種セミナー、情報通信技術関連イベント等において、犯罪手口の実演を交えるなどして、サイバー犯罪の現状、対策等についての周知を図っている。

また、広報啓発用パンフレットを配布するほか、情報セキュリティ対策ビデオをケーブルテレビで放映したり、警察署や図書館等で貸し出したり、警察庁ウェブサイト（http://www.npa.go.jp/）において、新たなサイバー犯罪の手口を紹介したりして、インターネットを利用する際の注意喚起を行っている。

さらに、毎年４月及び５月をサイバー犯罪防止のための情報セキュリティ対策に関する広報啓発の重点期間とし、集中的な広報啓発を実施している。

警察庁ウェブサイト

情報セキュリティ対策ビデオ

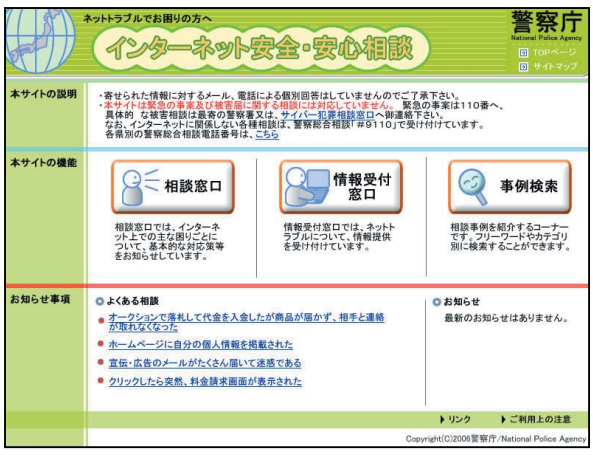
イ　相談対応

都道府県警察では、サイバー犯罪相談窓口を設け、情報セキュリティ・アドバイザー等の専門の職員によりサイバー犯罪等の相談に対する対応を推進している。

また、16年12月には、フィッシング事案に関する部外との窓口となる「フィッシング110番」を各都道府県警察に設置し、フィッシング事案に関する相談や情報提供を受け付けている。

さらに、警察庁において、サイバー犯罪等に関する相談の増加（第１章第１節（３）①イ（17頁）参照）に的確に対応し、インターネット利用者の被害防止を推進するため、17年６月、インターネット安全・安心相談システム（http://www.cybersafety.go.jp/）の運用を開始した。

このシステムでは、利用者の困りごとに応じた基本的な対応策等を自動的に回答するとともに、利用者からの情報提供を受け付けている。



インターネット安全・安心相談システム

③　サイバー犯罪の取締り

ア　サイバー犯罪対策のための態勢の強化

警察庁では、サイバー犯罪対策を的確に推進するための態勢の強化を図っており、９年４月には、電子商取引等の新たな社会的インフラに対する安全対策を確立するため、生活安全局生活安全企画課にセキュリティシステム対策室を設置した。

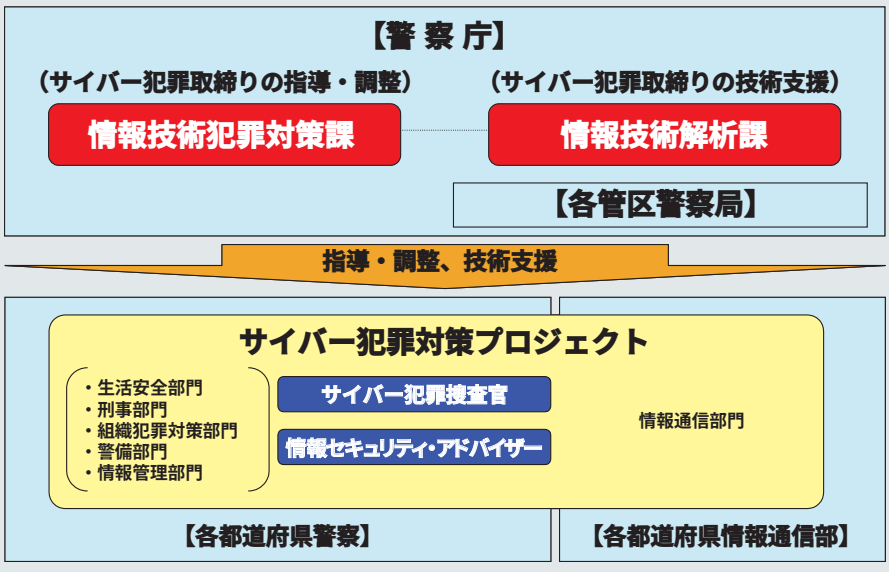
また、情報通信技術の発展に伴い、サイバー犯罪に悪用される技術が高度化し、その取締りには高度な技術的知見が必要とされるようになったことから、警察庁では、11年４月、サイバー犯罪対策に関し都道府県警察を技術的に指導する組織として情報通信局に技術対策課（現情報技術解析課）を設置するとともに、その技術的な中核組織として、同課に警察庁技術センターを開設した。さらに、13年４月には、管区警察局情報通信部に技術対策課（現情報技術解析課）を設置した。16年４月には、都道府県（方面）情報通信部に情報技術解析課を設置した。

その後、サイバー犯罪の検挙件数が増加するとともに、被害が複数の都道府県警察にわたるため、捜査が重複するという問題等が顕著になってきたことから、16年４月、生活安全局に情報技術犯罪対策課を設置し、都道府県警察が行うサイバー犯罪捜査に関する指導・調整を行うとともに、産業界や外国関係機関等との連携、広報啓発活動、相談対応等の施策を推進するなど、サイバー犯罪の捜査と予防に関する施策を一体的に推進することとした。また、都道府県警察が行うサイバー犯罪捜査に関する指導・調整能力の向上を図るため、18年４月、同課に情報技術犯罪捜査指導官を設置した。

一方、都道府県警察では、サイバー犯罪対策を効率的に進めるため、関係部門が連携の上、サイバー犯罪対策に関する知識及び技能を有する捜査員等により構成されるサイバー犯罪対策プロジェクトを設置している。

また、サイバー犯罪捜査に必要な専門的技術・知識を有する捜査員を育成したり、民間企業でシステム・エンジニアとして勤務した経験を有する者をサイバー犯罪捜査官として採用したりしているほか、サイバー犯罪等に関する相談への対応、情報セキュリティに関する広報啓発活動等サイバー犯罪の予防のための施策を推進する情報セキュリティ・アドバイザーを配置するなど、サイバー犯罪対策のための態勢の強化に努めている。

図1－25　サイバー犯罪対策のための態勢



コラム 2　警察庁技術センターの活動

警察庁技術センターには、特に高度かつ専門的な知識及び技能を有する職員を配置するとともに、高性能の解析用資機材を整備し、都道府県（方面）情報通信部で対応が困難な暗号等により隠ぺいされた情報、破損したハードディスク等に記録された情報等の抽出・解析、コンピュータ・ウイルス等の不正プログラムの動作の解析等を行っている。

非破壊検査装置を使った解析手法検討


クリーンルームでの精密作業

事例　中国人留学生の男（26）は、17年3月、オンラインゲーム運営会社がゲームサーバの負荷を軽減させるために外国からのアクセスを禁止していたにもかかわらず、中国からのアクセスを国内で中継してゲームサーバへのアクセスを可能とするサービスを提供することにより、接続料を徴収するなどして収益を得ようと企て、自宅等にプロキシサーバ(注)を設置してこれらのアクセスを不正に中継したことで、オンラインゲーム運営会社のゲームサーバに過度の負荷を与えて、同社の業務を妨害した。同年7月、電子計算機損壊等業務妨害罪で逮捕した。香川県情報通信部情報技術解析課では、押収されたコンピュータ等の解析等の技術支援を実施し、事件の全容解明に貢献した（香川）。


大量押収した解析対象コンピュータ

注：ウェブサイトの参照等を本来のコンピュータに代わって行うコンピュータであり、参照したウェブサイトのデータを記憶しておき、利用者からの同一のウェブサイトの閲覧要求があった場合、記憶しているデータを閲覧させることでネットワークの通信量を減らすことなどを目的として設置される。

イ　都道府県警察間の情報共有

複数の都道府県にまたがって敢行されるサイバー犯罪については、被害の拡大防止を図るため、早期に被疑者を特定し、検挙することが必要であるが、このような事案については、各都道府県警察において捜査している事件に競合が生じやすいことや捜査範囲が多数の都道府県にまたがることなどから、一の都道府県警察で捜査を遂行することが困難となっている。

このような状況に的確に対処するためには、従来、各都道府県警察において個別に把握していた捜査情報の共有を図り、各都道府県警察における捜査の競合を回避することにより、迅速に合同捜査・共同捜査を実施することが必要となる。

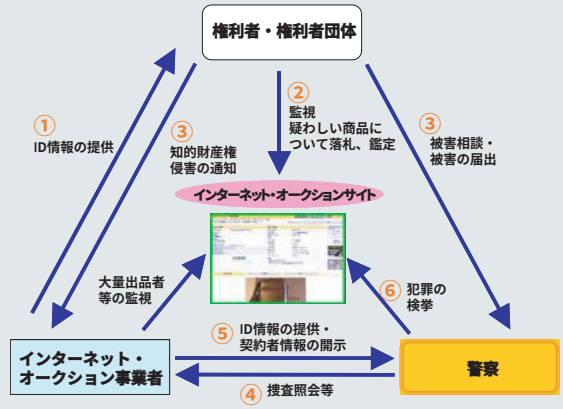
このため、各管区警察局及び各都道府県警察にサイバー犯罪捜査共助官を設置し、サイバー犯罪の捜査に関する連絡調整に当たらせることにより、サイバー犯罪の合同捜査及び共同捜査を推進している。

事例　無職の男（28）ら12人は、16年4月から同年12月にかけて、他人の識別符号を使用してインターネット・オークションサイトに不正アクセスし、携帯電話やブランド品等を架空に出品し、落札者から金銭をだまし取るなどしていた。警察では、被害者が33都道府県に及んだことを踏まえ、関係都県警察による合同捜査本部を設置し、捜査を実施した。17年6月までに詐欺罪、不正アクセス禁止法違反（不正アクセス行為）等で検挙した（大分、宮城、警視庁、茨城、兵庫、熊本）。

ウ　関係機関・団体との情報共有による取締り

近年、インターネット・オークションを利用した偽ブランド品や海賊版のＣＤ、ＤＶＤ等の出品が増加している傾向にある。既に著作権等の権利者や権利者団体では、自主的に出品状況を監視し、インターネット・オークション事業者に対し、違法出品の削除を要請するなどの対策を講じているが、出品する側も出品の宣伝において隠語を用いて知的財産権侵害品であることを分かりにくくするなど、その手口は巧妙化している。

図1-26　情報共有のための仕組み



これらの状況を踏まえ、16年度には、警察庁において開催した総合セキュリティ対策会議において、違法出品の把握、出品者への警告、捜査機関への通報、検挙といった一連の措置を円滑に実施するため、権利者・権利者団体、インターネット・オークション事業者及び警察の間の情報共有のための仕組みを構築した。現在、これを活用して、インターネット・オークションを利用した知的財産権侵害事犯の取締りを推進している。

事例 無職の男（37）は、17年8月から18年1月にかけて、インターネット・オークションにおいて複数の識別符号を用いてコンピュータソフトの海賊版を出品し、約1万5,000人に対しＣＤ－Ｒ約2万枚を販売して約3,000万円の収益を得た。兵庫県警察は、権利者団体から提供を受けた違法出品に関する情報を基に捜査を行い、18年1月、著作権法違反（頒布）で逮捕した。

コラム 3 快適なインターネット社会を目指して

警視庁ハイテク犯罪対策総合センター　　吉田 浩子　巡査部長

私は、警視庁のコンピュータ犯罪特別捜査官として採用され、前職で携わっていた大手都市銀行のシステム開発の経験や知識をいかし、日々、新たな手口が登場するハイテク犯罪の捜査に取り組んでいます。

インターネット社会の利便性とそこに潜む危険性については、警視庁のウェブサイトやハイテク犯罪防止教室等あらゆる機会を通して多くの方に呼び掛けをしていますが、最も効果的に多くの方に呼び掛けられるのは、ハイテク犯罪事件を解決し、それを新聞、テレビ等で報道していただくことだと思っています。

年々増加するハイテク犯罪事件を数多く検挙し、その手口を解明することで、インターネットを利用する多くの人々に注意を喚起しながら、快適なインターネット社会ができることを願っています。

コラム 4 見えない敵との戦い

香川県高松北警察署生活安全課　　藤本 芳明　警部補
（当時、香川県警察本部生活安全部生活環境課勤務）

「パソコンの調子が悪くなった」、「ホームページが見えない」といった相談の裏には犯罪のにおいがするものです。16年1月、一人の少年から、「オンラインゲームですべてのアイテムが盗まれた」という相談を受けました。「におい」がしたため地道に捜査を続けたところ、日本国内のプロキシサーバを利用した国外からの不正アクセスであることが分かりました。捜索に着手すると30台を超えるプロキシサーバがあり、中国語の画面と格闘しながら検証したものの、この時には実行行為者を特定することはできませんでした。

しかし、被害者の悔しさに思いを致し、あきらめずに裏付け捜査を積み重ねたところ、最終的には、オンラインゲーム運営会社に対する業務妨害事件 (注) により、プロキシサーバを設置していた被疑者を検挙することができました。

インターネット社会の秩序はでき上がっていません。だれもが安心してインターネットを利用することができる社会の実現を目指して、新たな形態のサイバー犯罪捜査に挑み続けていきたいと思っています。

注：第1章第2節（2）③アの事例（35頁）参照

（3）公共の安全を害するサイバーテロ等に対する取組み

①　サイバーテロ対策のための態勢の整備

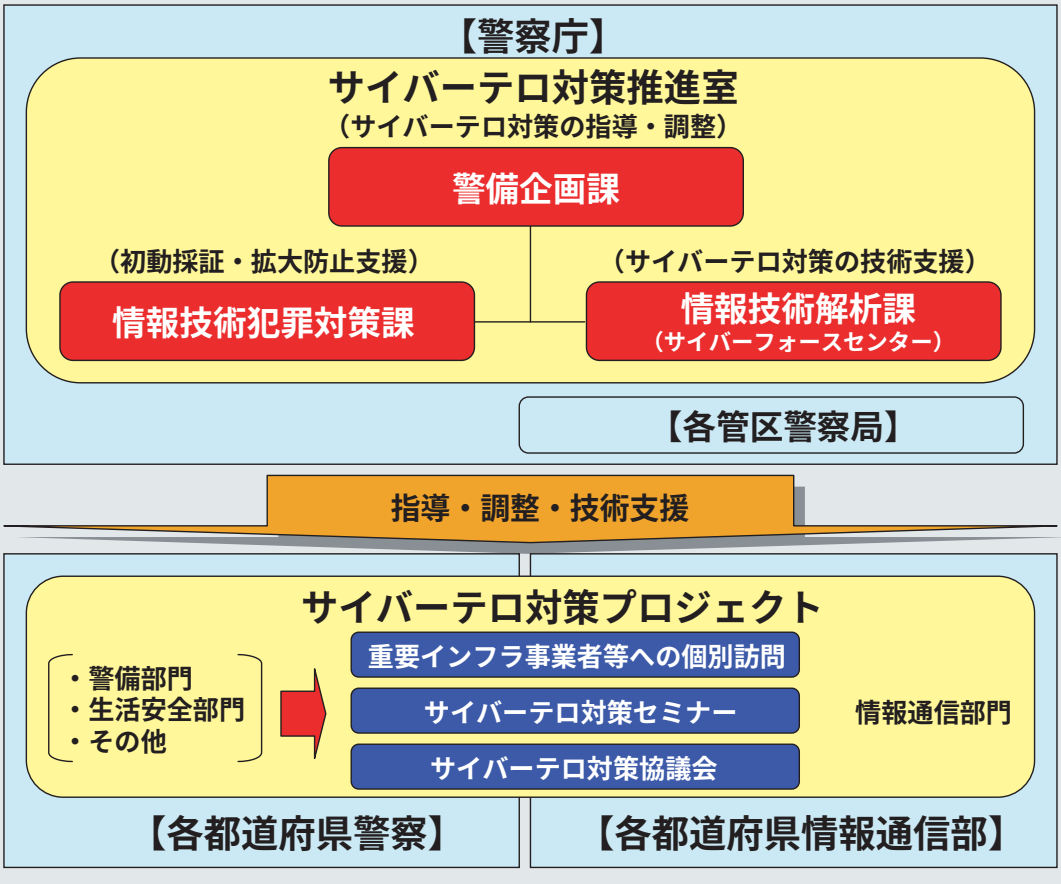
サイバーテロは、一たび発生すれば国民生活及び社会・経済活動に大きな被害を与える可能性があることから、できる限り早期に把握し、被害の未然防止と拡大防止を図ることが重要である。そのためには、平素から重要インフラ事業者等と連携し、サイバーテロの予兆の把握に努めるとともに、サイバーテロが発生した際には、速やかに対策を講ずることのできる態勢を確保する必要がある。

ア　平素の措置

警察庁では、平成16年４月、警備局、生活安全局及び情報通信局の職員により構成されるサイバーテロ対策推進室を設けた。同室では、重要インフラ事業者を会員とする業界団体に対し、サイバーテロの脅威や警察のサイバーテロ対策を説明し、各業界内で警察と連携した対策を推進するよう要請している。このほか、サイバーテロ対策に従事する都道府県警察の職員に対する教育訓練や、都道府県警察におけるサイバーテロ対策に関する指導を行うなど、総合的なサイバーテロ対策を推進している。

都道府県警察でも、警察庁の取組みに準じ、関係部局の職員により構成されるサイバーテロ対策プロジェクトの体制の充実を図っている。同プロジェクトでは、重要インフラ事業者等への個別訪問、サイバーテロ対策セミナー、サイバーテロ対策協議会等の開催（第１章第２節（４）②（45頁）参照）を通じて、セキュリティ水準向上のための情報提供、事案発生時における警察の捜査への迅速な協力の要請等、サイバーテロ対策を推進するための官民連携の強化に努めている。

図1 - 27　平素の措置のイメージ

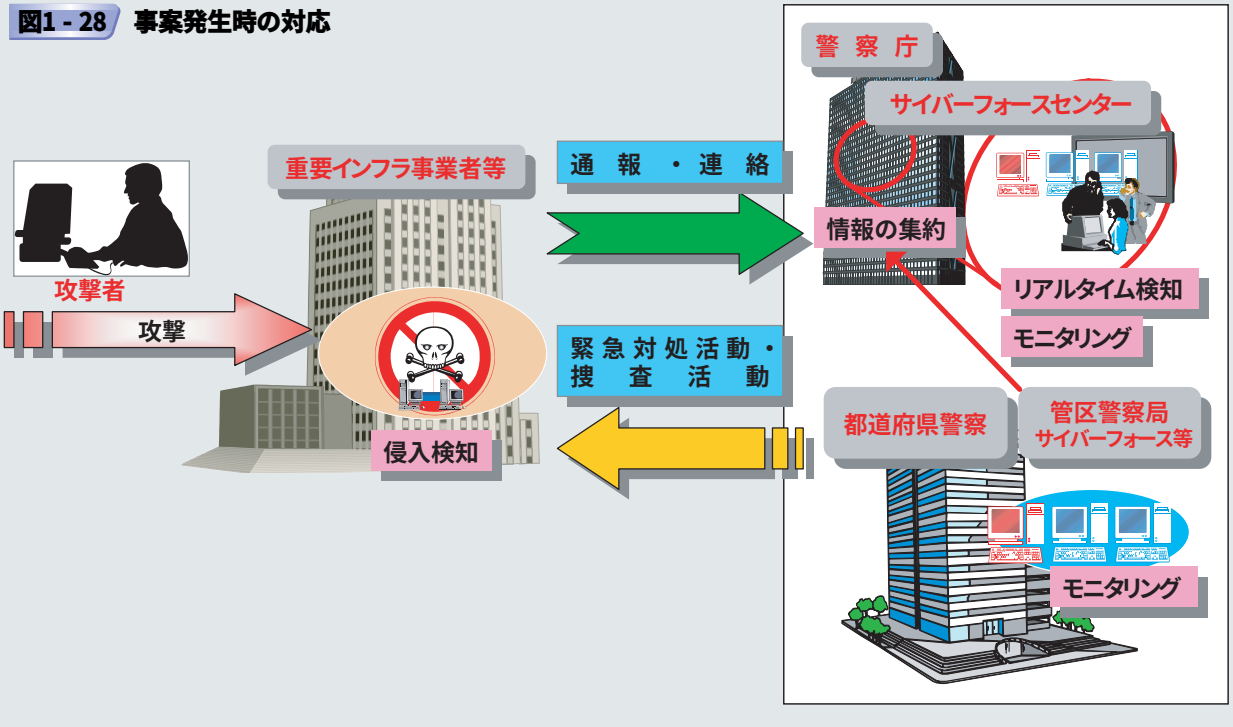


イ　事案発生時の対応

平素からの警察と重要インフラ事業者等との間で構築された連絡体制やリアルタイム検知ネットワークシステム（第１章第２節（３）②イ（ア）（41頁）参照）でのサイバーテロの予兆把握等により、サイバーテロ又はそのおそれがある事案を認知した場合、警察庁、関係管区警察局及び関係都道府県警察では、警備部門、情報通信部門を中心としたサイバーテロ対処本部を設け、情報の収集・分析を行うこととしている。同時に、都道府県警察のサイバーテロ対処本部の要員が、警察庁又は当該府県を管轄する管区警察局情報通信部等のサイバーフォースと共に現場に急行し、被害の状況を把握するとともに、サイバー攻撃を受けた基幹システムに対して、被害拡大の防止、証拠保全等の緊急対処活動を迅速に行うほか、速やかに捜査活動に当たることとしている。なお、サイバーテロは外国から敢行される可能性もあることから、その際は、警察庁を通じて、関係国に対して協力を要請することとしている。

16年８月、複数の政府機関等のウェブサーバに対してDoS攻撃が行われ、これらのウェブサイトが一時的に閲覧困難な状態となった際には、連絡を受けた警視庁及び警察庁サイバーフォースは、被害状況の確認、侵入検知装置の設置による攻撃状況の検知、被害の拡大を防止するためのファイアウォールの設定に関する指導・助言等を行った。

図1 - 28　事案発生時の対応



ウ　サイバーテロ対策に従事する要員の育成

サイバーテロ対策を行うためには、サイバーテロに用いられる手段や重要インフラの基幹システムに関する専門的知識も必要となる。そのため、都道府県警察のサイバーテロ対策に従事する要員については、警察大学校及び各管区警察学校におけるサイバーテロ対策のための教育訓練のほか、民間企業に委託して技術的な教育訓練を実施している。

サイバーテロ対策に従事する要員の育成

②　サイバーテロ対策に係る技術的基盤の強化

ア　サイバーフォースの創設

12年には、中央省庁等のウェブサイト改ざん事案や米国有名ウェブサイトへのDoS攻撃が発生するなど、サイバーテロの脅威は現実のものとなった。サイバーテロが発生した場合には、その影響が大きく、また、時間的・地理的な制約を受けないことから、警察は他の警察活動と比べてより迅速かつ広域的に展開しなければならず、そのための体制整備が喫緊の課題となっていた。このため、警察庁は、サイバーテロの予兆把握、被害の拡大防止のための緊急対処に係る都道府県警察への技術支援等を行うため、13年４月、警察庁情報通信局技術対策課（現情報技術解析課）にサイバーテロ対策技術室を設置したほか、警察庁及び管区警察局情報通信部の技術対策課（現情報技術解析課）に、サイバーテロ対策に当たる専門の技術部隊であるサイバーフォースを創設した。

サイバーフォースでは、都道府県警察の実施するサイバーテロ対策を技術的に支援するため、都道府県警察と連携して次のような活動を行っている。

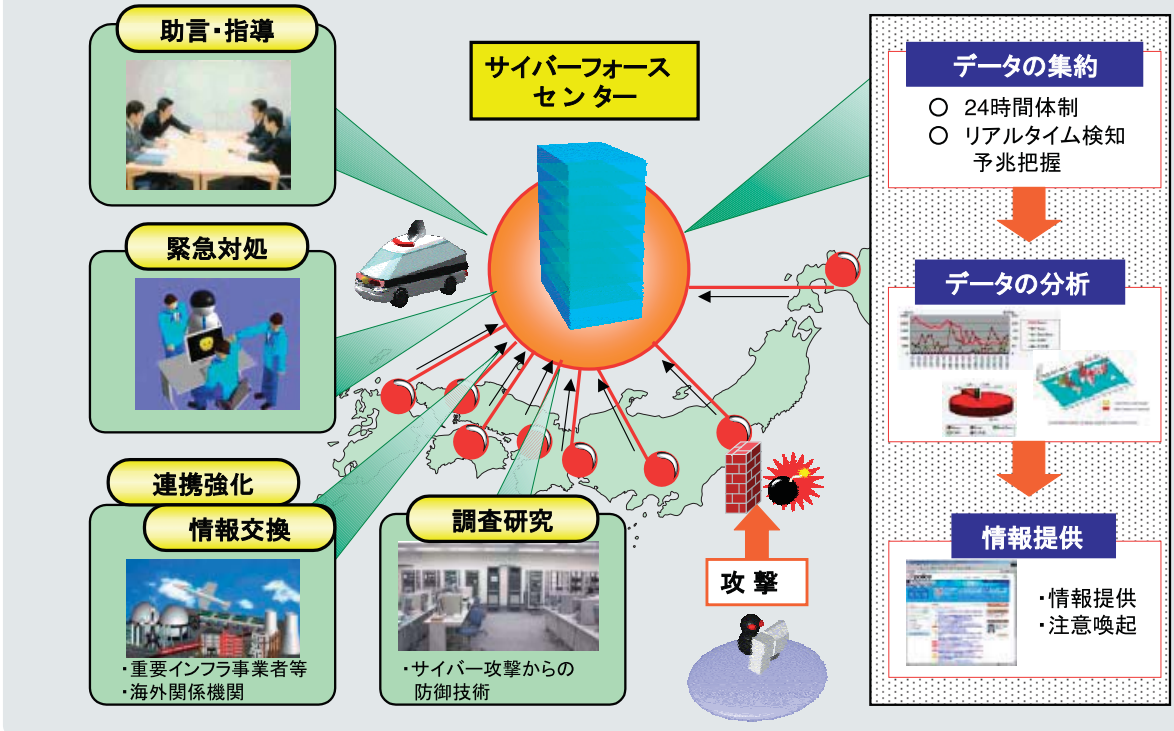
○　重要インフラ事業者への個別訪問を通じての技術情報の提供、助言
○　サイバー攻撃の予兆把握、早期検知
○　サイバー攻撃発生時の緊急対処
○　サイバー攻撃対策の調査研究

イ　サイバーフォースセンターの機能

全国のサイバーフォースの司令塔として警察庁に設置されたサイバーフォースセンターは、警察におけるサイバーテロ対策の技術的中核と位置付けられており、サイバー攻撃の予兆把握、事案認知及び事案発生時の緊急対処の拠点として機能している。

サイバーフォースは、全国の警察職員から選抜された、高度かつ専門的な知識と経験を有する者で構成されているが、その中でも、サイバーフォースセンターは、24時間体制でサイバーテロの予兆把握を行うための大規模かつ高度な情報システムを運営するとともに、集約された情報の分析、全国のサイバーフォースの指導等を実施している。

図1-29　サイバーフォースセンターの機能



（ア）　リアルタイム検知ネットワークシステムを活用したサイバーテロの予兆把握等

サイバーフォースセンターでは、警察の有するインターネットとの接続点（全国で57か所）に設置したセンサーからの情報を24時間体制で集約・分析するためのリアルタイム検知ネットワークシステムを整備・運用している。このシステムを用い、コンピュータ・ウイルスの感染の拡大やサイバー攻撃等の発生状況を観測し、サイバーテロの予兆把握に努めている。

リアルタイム検知ネットワークシステム

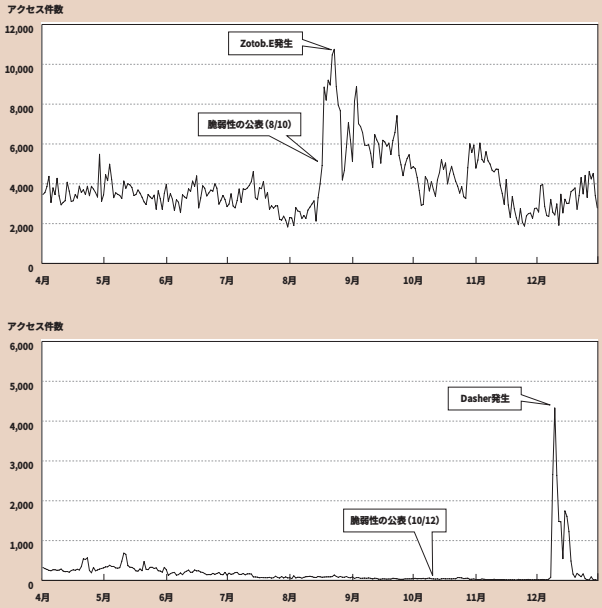
このシステムは、日々進化しており、例えば16年10月には、DoS攻撃被害観測システムを開発・導入し、インターネット上で発生するDoS攻撃を早期に検知することが可能となり、また、17年１月には、ボットネット観測システムを開発・導入し、ボットに感染したコンピュータの動向を把握することが可能となっている。

サイバーテロの予兆を把握し、速やかに重要インフラ事業者等に情報を提供することができれば、被害の未然防止や拡大防止に資することができることから、サイバーフォースでは、重要インフラ事業者等に対して、分析結果を電子メールにより配信するとともに、個別訪問を通じて対策のための各種情報を提供している。また、これらの分析結果の一部は、警察庁セキュリティポータルサイト「@police」（http://www.cyberpolice.go.jp/）を通じて、広く国民にも提供している。

コラム 5 リアルタイム検知ネットワークシステムにおける観測結果

図1－29は、リアルタイム検知ネットワークシステムにおける観測データから、2種類のコンピュータ・ウイルスに関係するアクセス件数の推移をそれぞれ示したものである。上の図では、17年8月中旬頃にアクセス件数が増加していることがわかる。これは、同年8月10日に公表されたソフトウェアの脆弱性を悪用して感染する「ゾトブ（Zotob)」というコンピュータ・ウイルス及びその亜種によるものと推測される。また、下の図では、17年12月中旬頃に急激なアクセス件数の増加がみられる。これは、同年10月12日に公表されたソフトウェアの脆弱性を悪用して感染する「ダッシャー（Dasher)」というコンピュータ・ウイルス及びその亜種によるものと推測される。このように、リアルタイム検知ネットワークシステムの観測データを分析することにより、コンピュータ・ウイルスやサイバー攻撃等の発生を早期に認知できるだけでなく、その動向を詳細に把握することが可能となる。このような分析結果は、重要インフラ事業者だけでなく国民にとってもサイバーテロ対策を講ずる上で有用であることから、サイバーフォースセンターにおいて、積極的に情報提供を行うこととしている。

図1－30 リアルタイム検知ネットワークシステムに対するアクセス件数の推移の例



（イ） 調査研究

サイバーテロに的確に対処するためには、サイバーフォースの活動を支える技術基盤の強化が不可欠である。そこで、サイバーフォースセンターでは、サイバー攻撃から重要インフラの基幹システムを防御するための技術、サイバーテロを敢行した者を特定するための技術等について調査研究等を行っている。

研究開発システム

（ウ） サイバーテロ対処訓練

サイバーフォースは、サイバーテロ対策に必要な高度かつ専門的な知識を常に修得している必要がある。そこで、サイバーフォースセンターに、様々な種類のコンピュータ等を組み合わせることにより重要インフラ事業者等のシステムを模擬的に構築できるサイバーフォース用訓練システムを整備し、サイバーフォースに対し、実際にサイバーテロが発生した場合に現場で必要となる実践的な技術を修得させるための訓練を実施している。

サイバーフォース用訓練システム

コラム 6　インターネット利用者への情報提供

インターネット利用者がサイバーテロ等の危険性を正しく認識するとともに、適切な対策が自主的に講じられるよう、15年3月から警察庁セキュリティポータルサイト「@police」（http://www.cyberpolice.go.jp/）を開設し、警察が集約した情報セキュリティに関する情報をいち早く公開している。このウェブサイトでは、新たにコンピュータ・ウイルスが発見されたり、各種プログラムの脆弱性が明らかとなったりした際に、これを速やかに公開するほか、インターネットの安全な利用方法について学習できる「@police セキュリティ講座」、警察施設に設置したリアルタイム検知ネットワークシステムの観測データを一定時間ごとに自動的に集計・分析して表示する「インターネット定点観測」等を公開している（第1章第2節（3）②イ（ア）コラム5（42頁）参照）。

警察庁セキュリティポータルサイト「@police」

③　国際テロ組織等によるインターネット利用に対する取組み

国際テロ組織等のインターネットの利用形態や扱われている情報を把握することは、国際テロ組織等の動向把握やテロの未然防止等、国際テロ対策上も有益である。また、各国の取組みは、我が国における対策の検討に資することから、警察庁においては、外国治安情報機関等との連携等により、国際テロ組織等のインターネット利用及びその対策に関する情報収集を行っている。

（4）産業界、関係機関等との連携強化

サイバー空間の安全を確保するためには、警察の取組みに加え、産業界や学校、教育委員会等との連携が不可欠であることから、警察においては、これらと連携した施策を推進している。

①　産業界、関係機関等と連携した違法・有害情報対策等

ア　学校、教育委員会等と連携した対策

都道府県警察では、学校で開催する非行防止教室や、少年、保護者及び学校職員等を対象とする講演等を通じ、フィルタリング・システムの導入を勧めるとともに、インターネット上の違法・有害情報の実態、インターネットに起因した犯罪や少年が被害者となった事件の具体的な事例を紹介するなどの広報啓発活動を進めている。

非行防止教室を通じた広報啓発活動

イ　産業界と連携した対策

警察庁では、インターネット上における薬物、銃器の取引の未然防止を図るため、複数の検索サイトを運営する事業者に依頼し、17年６月から、インターネットで薬物や銃器に関連する特定の用語を検索した場合、検索結果表示画面の上部に「薬物乱用は犯罪です」、「けん銃を所持することは犯罪です」等と記載した広告を掲示することにより、インターネット利用者への注意喚起等を行っている。

また、警察においては、インターネット上の違法・有害情報対策としてサイバーパトロールを強化しており、例えば、警視庁では、17年８月から、サイバーパトロールを通じて蓄積した違法・有害情報のデータベースをフィルタリング・ソフトの開発事業者に提供するなど、産業界と連携した取組みを推進している。

ウ　総合セキュリティ対策会議

警察庁では、13年度から、有識者、関連事業者、ＰＴＡの代表者等で構成する総合セキュリティ対策会議を開催し、情報セキュリティに関する産業界と政府の連携の在り方等について検討を行っている。

16年度は、インターネット上の自殺予告事案への対応の在り方について検討を行い、人命保護等の観点から緊急の対応を必要とする事案であり、プロバイダや電子掲示板の管理者等が緊急避難に該当すると判断できるものが認知された場合には、プロバイダ等は自殺を予告する者等に関する情報を警察に開示することができることとするなど、自殺予告事案への対応の在り方についての提言を取りまとめた。

平成１７年度総合セキュリティ対策会議

17年度は、インターネット上の違法・有害情報への対応における官民連携の在り方について検討を行い、その検討の結果をインターネット上の「ホットライン」（第１章第３節（１）①（52頁）参照）の必要性及びその運用の在り方に関する提言として取りまとめた。

エ　民間企業等との連携

警察からの要請に速やかに対応するため、15年12月、マイクロソフト株式会社に、都道府県警察からの照会に対応するための専用窓口が設置された。また、捜査の過程で押収した電磁的記録媒体の解析作業を行う上で、民間企業が有する技術情報等が必要になることから、17年４月、同社と技術協力に関する協定を締結し、同社からプログラム上の欠陥や脆弱性等に関して、非公開情報を含む各種技術情報の提供を受けられる協力関係を構築した。

プロバイダ連絡協議会

また、都道府県警察では、関係行政機関、プロバイダ、消費者団体等で構成されるプロバイダ連絡協議会等を設置し、サイバー犯罪の情勢や手口、サイバー犯罪被害防止等に関する情報交換を行っているほか、講習会等の実施、一般向け広報資料の作成等を行っている。

事例　熊本県警察は、17年5月から同年6月にかけて、熊本県情報セキュリティ推進協議会と共同で、出会い系サイトやサイバー犯罪から子どもたちを守るために、中学生を対象とした熊本県青少年サイバー犯罪対策作文コンクールを開催した。

さらに、常時、不特定多数の者がインターネットを利用することができる環境にあり、その利用者を特定することが困難であるインターネットカフェ等については、サイバー犯罪を敢行する者に悪用されやすいことから、各都道府県警察においては、インターネットカフェ等の事業者に働き掛け、連絡協議会を設立するなど、防犯意識の向上に努めている（18年６月現在、４道県・３地区において連絡協議会が設置）。

②　サイバーテロ対策に関する官民連携

ア　重要インフラ事業者等への個別訪問

都道府県警察では、重要インフラ事業者等への個別訪問を通じて、重要インフラにおけるサイバーテロ対策を支援するなどの取組みを推進している。具体的には、

- リアルタイム検知ネットワークシステムの分析結果、コンピュータ・ウイルスやソフトウェアの脆弱性情報等、インターネット上の治安情勢に関する情報提供
- サイバーテロ発生時の警察への速やかな通報及び平素からの連絡窓口の設置の要請
- サイバーテロを敢行した者を特定するための捜査に対する協力要請

等を実施し、サイバーテロ対策の重要性について理解を求めている。

イ　サイバーテロ対策セミナー

都道府県警察では、重要インフラ事業者等の基幹システムの運用等に携わる情報セキュリティ担当者等を対象としたサイバーテロ対策セミナーを実施している。このセミナーでは、DoS攻撃等代表的なサイバー攻撃の手法を実演し、その防御手法を解説するなど、サイバー攻撃に対処するための具体的な情報提供に努めている。

参加者からは、「サイバーテロ対策を身近な問題としてとらえることができた」、「事例紹介や攻撃手法の実演を通じてネットワークの危険性について実感できた」などの意見が寄せられており、参加者の意識向上に役立っている。

サイバーテロ対策セミナー

ウ　サイバーテロ対策協議会

重要インフラ事業者や地方公共団体等から構成されるサイバーテロ対策協議会は、サイバーテロ対策に関する警察からの情報提供、参加者間の意見交換・情報共有を行う場として設置されている。この協議会では、重要インフラ事業者等から、実際にサイバー攻撃を受けた際の対応状況に関する経験も発表されるなど、活発な意見交換が行われている。

現在、協議会は、東京都、大阪府、広島県及び香川県の４都府県に設置されている。

サイバーテロ対策協議会

エ　共同研究

情報通信技術の発展に伴い、これを悪用した新たなサイバー攻撃の手段が次々と顕在化している。これらに適切に対応していくためには、情報通信分野の最新の技術動向を把握していかなければならない。そこで、サイバーフォースでは、大学、民間企業等と協力し、共同でサイバーテロ対策のための技術に関する調査及び研究開発を実施している。

コラム 7　情報セキュリティに係る政府全体の取組み

コンピュータ・ウイルスのまん延、サイバー犯罪の急激な増加、国民生活や社会・経済活動を支える重要インフラにおける情報システム障害等、我が国を取り巻く情報セキュリティ問題は深刻である。このような情勢の下、政府においては、官民における統一的・横断的な対策の推進を図るため、17年4月、内閣官房に情報セキュリティセンター（ＮＩＳＣ）を、同年5月、ＩＴ戦略本部（議長：内閣総理大臣）に情報セキュリティ政策会議（議長：内閣官房長官）をそれぞれ設置した。

NISCでは、情報セキュリティ政策会議の下で、我が国の情報セキュリティ対策に関する基本戦略を立案し、政府機関における総合対策、重要インフラの情報セキュリティ対策を促進するとともに、政府機関に対するサイバー攻撃等が発生した際の事案対処支援等を行っている。警察においては、NISCや関係省庁との連携の下、サイバー犯罪やサイバーテロ対策等の情報セキュリティ問題に対して、その技術力、機動力をいかした取組みを推進し、政府における情報セキュリティ対策に貢献している。

（5）国際連携（第６章第１５項（２８０頁）参照）

①　国際的なサイバー犯罪捜査協力の推進

ア　Ｇ８ハイテク犯罪サブグループにおける取組み

サイバー犯罪及びサイバーテロは、容易に国境を越えて行われ、一国だけでは解決できない問題であることから、様々な多国間協議の場で捜査機関相互の協力や各国国内の体制整備に関する議論が行われている。

主要８か国（Ｇ８）(注1) 各国がサイバー犯罪に対して共通して講ずるべき対策を検討するため、Ｇ８ローマ/リヨン・グループの下に置かれたハイテク犯罪サブグループでは、1997年（平成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、国際捜査協力や各国国内の体制整備に関する議論がなされている。

「ハイテク犯罪と闘うための原則と行動計画」には、サイバー犯罪に関する国際捜査協力について24時間対応できる連絡窓口である24時間コンタクトポイントの指定が含まれているが、これは、国際的なサイバー犯罪に対する適時・効果的な対応確保のため、この分野に精通した職員からなるコンタクトポイントを通じて、迅速かつ信頼できる通信手段により連絡をとることを想定したもので、現在43か国・地域まで拡張され、サイバー犯罪の国際捜査協力に大きな役割を果たしている。我が国では、警察庁に24時間コンタクトポイントを設置し、国際的な対応を必要とする事件への対応の円滑化を図るとともに、二国間での情報交換を積極的に行うなど、サイバー犯罪の取締りに関する国際的な捜査協力を推進している。

また、ハイテク犯罪サブグループにおいては、重要インフラを防護するための各国の取組みに関する意見交換、情報の共有の在り方等についての議論が行われている。これらを踏まえ、Ｇ８各国を中心とした18か国（18年６月現在）による重要インフラの防護に関する情報を交換するための連絡窓口が設置されている。

さらに、2005年（17年）５月、Ｇ８各国の法執行機関が中心となった重要インフラの防護に関する図上訓練が実施され、警察庁も訓練に参加し、各国との連携強化に努めた。

イ　その他の取組み

警察庁は、国際刑事警察機構（ICPO-Interpol）における捜査手法に関する情報の交換や関係国の取締能力の向上についての検討に積極的に参加し、国際的な連携の強化に努めている。

17年９月には、アジアの近隣諸国・地域との間でサイバー犯罪に関する捜査機関相互の連携を強化するため、中国、韓国、タイ、香港等の７か国・地域からサイバー犯罪捜査機関の幹部を招き、第７回アジア・南太平洋IT犯罪作業部会をICPOと共催した。

また、18年４月には、児童ポルノ事犯等児童を被害者とするサイバー犯罪の国際的な動向について理解を共有するとともに、その捜査手法や捜査技術について習熟を図ることを目的として、アジア等の６か国からサイバー犯罪捜査担当者を招き、インターネット利用児童ポルノ事犯捜査セミナーをICPO及び児童失踪・児童虐待国際センター（ICMEC）(注2) と共催した。

第７回アジア・南太平洋IT犯罪作業部会

注1：日本、米国、英国、フランス、ドイツ、カナダ、イタリア及びロシア
2：International Center for Missing & Exploited Children

さらに、警察庁は、二国間の捜査協力の一環として、同年５月に、英国の重大組織犯罪対策庁（SOCA）(注1) 電子犯罪部との間で、ネットワーク情報その他の情報技術解析に関する協力を含めたサイバー犯罪の防止及び取締りのための国際協力を推進することを内容とする合意文書に署名した。

②　国際的なサイバー犯罪捜査技術協力の推進

サイバー犯罪の国際捜査協力やサイバーテロに係る国際協力を進める上で、各国は、電磁的記録の解析手順や解析に使用するソフトウェア、電磁的記録媒体の取扱い等において、同等の技術水準を確保していることが望ましい。そこで警察庁では、技術水準の維持向上のため、各国の法執行機関等との情報共有や人材育成のための国際連携を推進している。

ア　サイバー犯罪技術情報ネットワークシステム

警察庁では、13年３月から、犯罪の取締りに関する技術情報を共有し、相互の技術水準の向上を図ることを目的として、アジア地域の法執行機関を結ぶサイバー犯罪技術情報ネットワークシステム（CTINS）(注2) を整備・運用しており、18年６月現在、11の国・地域が参加している。ICPOアジア・南太平洋IT犯罪作業部会においても、この作業部会に参加する国・地域間の情報共有手段の一つとして活用されることが期待されている。

イ　アジア地域サイバー犯罪捜査技術会議

警察庁では、CTINSに参加する国・地域との円滑な情報共有を推進するとともに、国際連携の強化を図るため、サイバー犯罪の捜査等に当たる技術者等を集めアジア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ている。この会議では、各国が実施しているサイバー犯罪への技術的対策について発表、議論及び意見交換を行い、各国の相互理解を深めている。

アジア地域サイバー犯罪捜査技術会議

注1：Serious Organized Crime Agencyの略。違法薬物取引、人身取引、詐欺のほか、サイバー犯罪、通貨偽造、銃器犯罪等の組織犯罪を担当する英国の法執行機関。2006年（18年）４月１日に、国家犯罪捜査庁(NCS:National Crime Squad)、国家犯罪情報部（NCIS:National Criminal Intelligence Service)、歳入税関局の薬物取引及び金融犯罪捜査部門並びに入国管理局の組織的不法移民犯罪担当部門を統合して発足

2：Cybercrime Technology Information Network Systemの略。電子メール、電子掲示板及びデータベースの機能を備え、暗号化されたネットワークにより、各国の担当官が安全に情報を共有できる手段を提供している。

ウ　人材育成

17年３月、警察庁は、電磁的記録媒体を解析するソフトウェアの使用方法等を指導するため、インドネシア国家警察に解析技術に精通した専門家を派遣した。また、18年１月には、ICPO及び国際協力機構（JICA）と共に、サイバー犯罪捜査技術に関して各国の指導的立場にある者の捜査技術の更なる向上のため、アジア地域等18か国のサイバー犯罪捜査担当者等を集めた、ICPO・IT犯罪捜査技術に関するトレーナー育成ワークショップを開催し、実践的な教育訓練を行った。

他方、警察庁では、サイバーフォース要員を外国の法執行機関等に派遣して実地訓練を受けさせるなど、国際的なサイバーテロ対策の動向を見据えた訓練を実施している。

インドネシア国家警察に対する技術支援

③　FIRSTへの参加

警察庁では、サイバーフォースを、情報セキュリティに関する最新の技術情報を共有し、適切な事案対処の促進を目的とする世界的な枠組みである事案対処及びセキュリティ組織のフォーラム（FIRST）(注) に参加させている。FIRSTには、世界各国から170以上の組織が官民を問わず参加しており、一般に公開されていない技術情報を共有している。警察庁のサイバーフォースは、17年11月、警察機関としては世界で初めてFIRSTに加盟することが認められた。

注：Forum of Incident Response and Security Teamsの略

コラム 8 都道府県警察官と情報通信部職員の連携

警察庁には、地方機関として7の管区警察局と、府県ごとに府県情報通信部が置かれている。また、これとは別に、東京都警察情報通信部及び北海道警察情報通信部が置かれ、北海道警察情報通信部には、4の方面ごとに方面情報通信部が置かれている。これら都道府県（方面）情報通信部は、都道府県警察の行う捜査活動を技術的に支援するとともに、災害等の事案に際しては、機動警察通信隊を派遣し、現場活動に必要不可欠な通信の確保に努めるなど、都道府県警察と連携して様々な事案に対応している。

ここでは、都道府県警察官と情報通信部職員が連携してサイバー犯罪の解決に当たった事例を、実際に捜査に従事した者の手記により紹介することとする。

事例1 無職の男（39）は、平成16年6月から同年12月にかけて、インターネット・オークションにおいて家電製品を売ると偽り、延べ約500人の落札者から代金として合計約1億2,000万円を預貯金口座に振り込ませてだまし取った。17年6月、詐欺罪で逮捕した（北海道）。

北海道旭川方面旭川東警察署生活安全課　　中村 哲也　巡査部長

インターネット・オークションサイトなど利用したことのない私にとっては、この事件をどのように解決すればよいのか、途方に暮れていました。そんな中、情報通信技術のスペシャリストである旭川方面本部情報通信部情報技術解析課の協力を得て、被疑者の使用していたコンピュータに残されていた記録を解析し、その中から重要な資料を発見することができたのです。それが、それまで否認していた被疑者の供述の矛盾点を突くことになり、その結果としてこの事件の真相解明につながったのでした。

サイバー犯罪は技術の進歩とともにその手口も進化します。私自身、流れに乗り遅れないよう日々研鑽（さん）するとともに、今後もサイバー犯罪の捜査に当たって常に情報通信部との連携を深めていきたいと思っています。

西井技官（左）と中村巡査部長（右）

北海道警察情報通信部旭川方面情報通信部情報技術解析課　　西井 謙介　技官

インターネット・オークションは、だれでも気軽に参加できるというメリットがあるものの、被害に巻き込まれる可能性をなくすことができないのが実際のところです。

この事件の技術支援に当たっては、捜査員に同行し、捜索すべき場所や差し押さえるべき物を特定するために技術的な観点から助言をしたり、捜査員の指示の下でコンピュータに残されていた記録を解析したりしました。特にこの事件で使用されていたコンピュータは、非常に特殊な仕様であったため、解析作業は困難を極めました。しかし、様々な手法を用いて試行錯誤を繰り返した結果、最終的に解析を成功させ、事件の早期解決に貢献することができました。

このように、私たちが持っている技術や専門知識によって犯罪捜査の端緒情報や証拠資料を得ることができ、事件の早期解決に役立つことができたときの喜びは、何事にも代え難く、正に「技術屋」として誇りに思い、生きがいを感じた瞬間でもあります。

サイバー犯罪の技術は日々進歩しています。私たち「技術屋」も、日々自己研鑽に励まなければなりません。今後も、最新の技術に対応できるよう努力を重ねていきます。

事例2 出会い系サイトを運営する男（38）は、15年12月ころ、不特定多数の者に自己のウェブサイトを宣伝する内容を記載した迷惑メールを大量に送信した。男は、送信する際、迷惑メールが他の電気通信事業者から送信されたものであるかのように装い、当該事業者の使用するドメイン名を不正に使用して送信したため、あて先が不明となった電子メールが当該事業者に大量に返信され、その管理するサーバの機能を麻痺させた。17年5月、有線電気通信法違反（通信妨害）で逮捕した（京都）。

京都府警察本部生活安全部生活経済課ハイテク犯罪対策室　　安達 茂樹　警部補

この事件の捜査の過程では、被疑者が経営するアダルトサイト会社を捜索しましたが、社内に200台以上のコンピュータが設置されており、この大量のコンピュータの中から、この事件に使用されたものを特定することは非常に困難でした。

しかし、被疑者を検挙するという捜査員の執念と、情報通信部職員の高度な技術力が見事に結実して、そのコンピュータを特定することができ、そしてこれが突破口となって、この困難な事件を一気に解決することができました。

今から振り返れば、この捜査員と情報通信部職員との連携なくして、この事件の解決はあり得ませんでした。

情報化の進展に伴いサイバー犯罪は、今後、ますます悪質・巧妙化する傾向にあります。捜査力に一層磨きをかけ、また、情報通信部との連携を緊密にして、このような犯罪の検挙に全力を注いでいく覚悟です。

近畿管区警察局京都府情報通信部情報技術解析課　　谷口 優生　技官

私は現在、事件の捜索・差押え時の捜査員に対する技術支援や押収されたコンピュータを始めとする電子機器の解析を行っています。

捜索現場において技術支援を行うことは、この事件が初めてでしたが、事前の打合せでは、捜査員の方が非常に熱意を持って説明されていて、事件解決への意気込みを強く感じました。

捜索当日は、大量のコンピュータの中から事件に直接関与したコンピュータを探し出さなければなりませんでしたが、捜査員の気迫に押され、粘り強くコンピュータの特定作業に取り組み、結果としてそのコンピュータの特定及び事件全体の解明に大きく貢献することができました。

この事件の捜査では、捜査員の方に大変に感謝されました。このように感謝してもらえることは技術者として、無上の喜びであり、また、この事件の捜査を通じて、この種の事件を解決するためには、捜査員と技術支援員の両方の力を結集することの必要性を強く感じました。私としても、ここで得られた経験をいかし、今後とも、事件解決のため頑張っていくつもりです。

第３節　今後の課題

（１）社会全体で取り組む違法・有害情報への対応

第１節で述べたとおり、現在、インターネット上には様々な違法・有害情報が氾濫し、これらの情報に起因した犯罪が実際に発生するなど、インターネットの負の部分が深刻な問題となっている。これに対処するため、警察では、サイバーパトロールを通じて違法・有害情報の把握に努め、違法情報については被疑者を検挙し、有害情報についてはプロバイダや電子掲示板の管理者に削除を依頼するなどの取組みを進めてきたところであるが、対象が広範囲にわたることなどから、警察だけの取組みでは限界がある。

こうした現状を踏まえ、インターネット上の違法・有害情報対策を推進していくためには、これまでの取組みを更に推進するとともに、新たな取組みについて検討を行う必要がある。

今後、国民のニーズを踏まえつつ、警察の取締りの強化によるインターネット上からの違法・有害情報の排除のほか、次のような対策を重点的に推進していくこととしている。

①　ホットラインの適切な運用

インターネット上に違法・有害情報が氾濫している状況を踏まえ、平成17年度総合セキュリティ対策会議において、ホットラインの必要性及びその運営の在り方について検討を行い、「インターネット上の『ホットライン』の必要性及びその運営の在り方等に関する提言」を取りまとめた。ホットラインとは、インターネット利用者からインターネット上の違法・有害情報に関する通報を受け付け、一定の基準に基づいて選別した上、違法情報については、警察に通報するとともにプロバイダや電子掲示板の管理者等に対して削除を依頼し、有害情報については、プロバイダや電子掲示板の管理者等に対して利用者との契約約款等に基づく削除等を依頼する仕組みのことである。現在、米国、英国、ドイツ、フランスを始めとする諸外国において既に運用されており、1999年（11年）にはホットライン相互間の連絡組織であるINHOPE(注)が設置されている。INHOPE加盟国においては、インターネット上の違法情報が外国に所在するウェブサーバに蔵置されている場合、INHOPEを通じて外国のホットラインに削除を依頼するといった取組みもなされている。我が国では、18年６月、警察庁が（財）インターネット協会にホットラインに関する業務を委託し、我が国のホットラインとして、インターネット・ホットラインセンターの運用が開始されたところである。

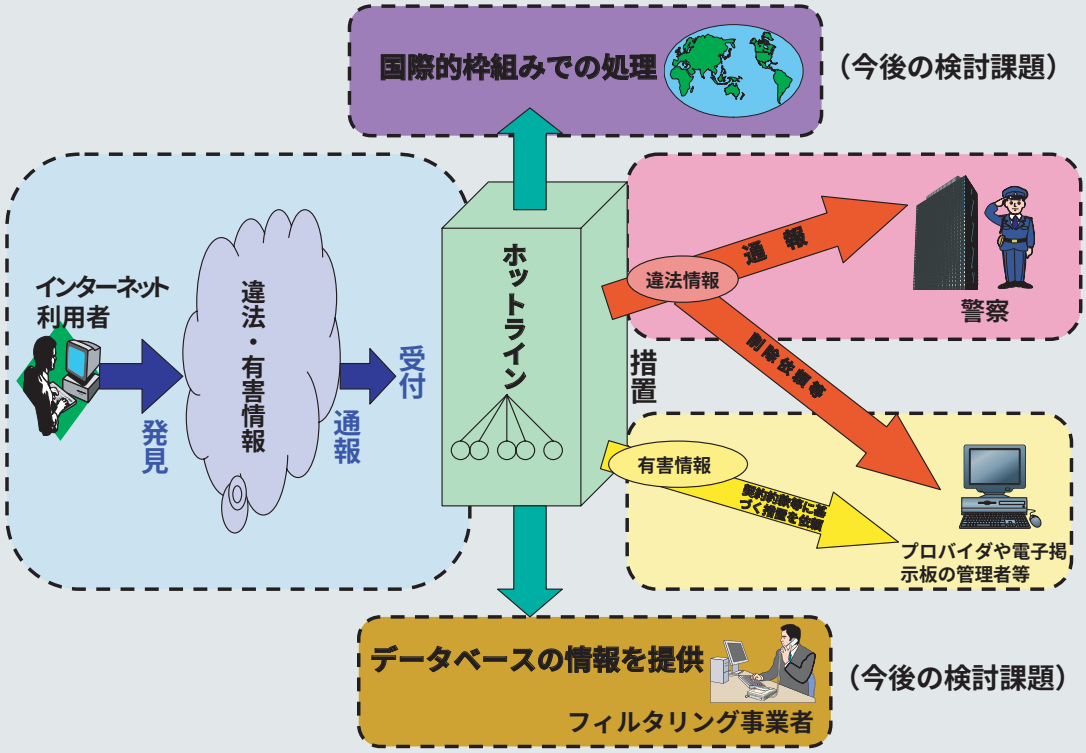
ホットラインは、通報を寄せるインターネット利用者、依頼を受けて対応するプロバイダや電子掲示板の管理者等の理解や協力を得て初めてその目的が達成されるものである。したがって、今後、その活動内容や活動実績について、様々な媒体、手段を利用して周知を図るとともに、取り扱う違法・有害情報の範囲やその判断基準についても、広く国民の意見を集約し、最新の情勢に対応したものとしていく必要がある。

また、我が国では、違法情報が外国に所在するウェブサーバに蔵置されている場合、警察が外国の警察機関を通じ、プロバイダや電子掲示板等の管理者に当該情報の削除を依頼することとしているが、今後、違法情報については、原則として警察機関を通じて対応することとしつつも、我が国がＩＮＨＯＰＥに加盟した際は、現在の運用を補完するものとして、ＩＮＨＯＰＥを通じた仕組みの活用についても検討していく必要がある。

さらに、ホットラインには様々なインターネット上の違法・有害情報に関する通報が寄せられていることから、フィルタリング・システムの精度の向上のために必要な情報をフィルタリング・ソフトの開発業者に提供するなど、他の違法・有害情報対策に貢献するための取組みについて更に検討していく必要がある。

注：Internet Hotline Providers in Europe Associationの略。2006年（18年）３月現在、23か国・地域の25団体が加盟している。

図1 - 31　「ホットライン」の仕組み



コラム 1　インターネット・ホットラインセンターが扱う違法・有害情報の範囲

インターネット・ホットラインセンターがプロバイダや電子掲示板の管理者等に対して削除依頼を行う違法・有害情報の具体的範囲は、次のとおりとされている。

＜違法情報＞

- ○ わいせつ物公然陳列
- ○ 児童ポルノ公然陳列
- ○ 売春防止法違反の広告
- ○ 出会い系サイト規制法違反の誘引行為
- ○ 規制薬物の濫用を公然とあおり又は唆す行為
- ○ 規制薬物の広告
- ○ 預貯金通帳等の譲渡の誘引等
- ○ 携帯電話の匿名貸与営業等の誘引等

＜有害情報＞

- ○ 違法行為（けん銃等の譲渡、爆発物の製造、児童ポルノの提供、公文書偽造、殺人、脅迫等）の直接的かつ明示的な請負・仲介等に関する情報
- ○ 違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報
- ○ 人を自殺に勧誘・誘引する情報（集団自殺の呼び掛け等）

②　学校等と連携したインターネット利用に係る被害防止対策やマナー等の周知

17年11月、警察庁が中学生、高校生及びその保護者に対して実施した意識調査(注1)の結果から、学校で、不審なウェブサイトにアクセスしたり、心当たりのない電子メールに返信したりしない、電子掲示板等に他人の悪口を書き込んだり、いわゆるチェーンメール（複数の者に同内容の電子メールを送信することを求める電子メール）を送ったりしないといったインターネットを利用する際の被害防止対策やマナー等についての教育への保護者の期待の高さがうかがえる（第１章第１節（２）②イ（９頁）参照)。警察では、非行防止教室やインターネットに関する講習会等の場を通じて、少年に対してこのような教育を実施しているところであるが、今後は、学校その他の関係機関との連携を深めつつ、教育内容を充実させるとともに、開催回数と参加者数の増加を図り、その普及・促進に一層努めていくこととしている。

③　保護者に対する意識啓発

上記意識調査によれば、フィルタリング・ソフト又はサービスを知らない保護者が６割近くおり、また、これを「利用したくない」と答えた保護者の中には、フィルタリング・ソフト又はサービスの利用方法が分からないことを理由にしている者が４割近くいることから（第１章第１節（２）②イ（９頁）参照)、警察では、保護者に対し、フィルタリング・ソフト又はサービスの利用方法について情報提供を行い、保護者の理解を深めていくこととしている。

また、インターネット上の違法・有害情報の影響から少年を守るためには、各家庭における教育が重要であるが、上記意識調査の結果から、保護者が子どものインターネットや電子メールの利用状況を十分把握しておらず、少年が違法・有害情報に触れないようにする取組みに対する保護者の意識が十分でないことがうかがえる。したがって、警察では、学校その他の関係機関と連携し、非行防止教室やインターネットに関する講習会等への保護者の参加を積極的に促すとともに、インターネット上の違法・有害情報に起因する犯罪や少年の犯罪被害の発生状況について実例を示しつつ、違法・有害情報から少年を守るため、保護者の責務の自覚を促すための意識啓発を進めていくこととしている。

④　違法・有害情報の排除に向けたネット安全・安心国民運動の展開

我が国のインターネット社会の安全・安心を確保するためには、広報啓発活動を進めるほか、違法・有害情報を排除し、インターネット社会の健全化に協力する民間ボランティアの取組みを支援するとともに、違法・有害情報から子どもを守るためのネット安全・安心国民運動とも言うべき活動による国民的気運の醸成が不可欠である。このため、警察では、シンポジウムや講演会の開催やインターネットを通じた広報啓発の推進等により、違法・有害情報を排除し、インターネット社会の健全化を推進する気運を全国的に波及・向上させ、国民の意識と理解を深めるための国民運動を展開することとしている。

⑤　産業界における自主的取組みの強化に向けた働き掛け

インターネット上に氾濫する違法・有害情報への対策を推進するためには、プロバイダによる違法・有害情報の排除のための自主的取組みが重要である。

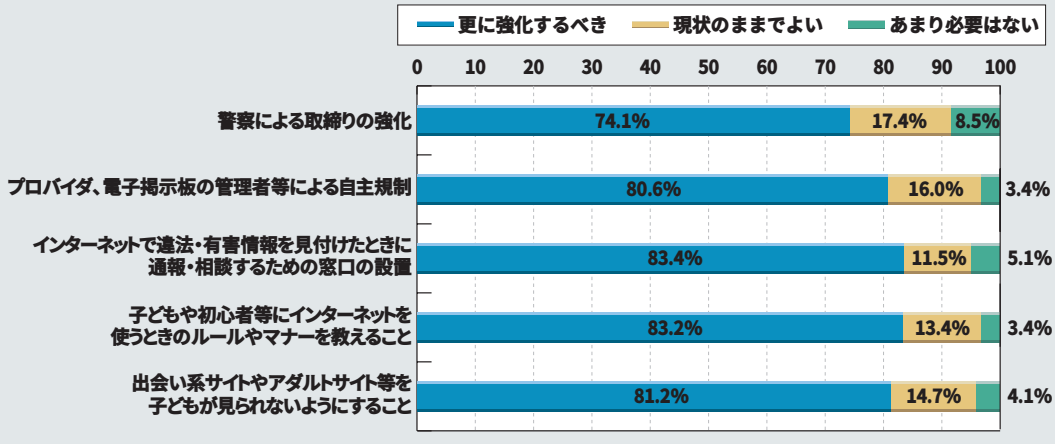
しかしながら、18年３月、警察庁がインターネット利用者を対象に行ったインターネット利用に関する意識調査(注2)において、９割近くの者がプロバイダの取組み不足を違法・有害情報氾濫の原因とし、８割以上の者がインターネット上から違法・有害情報をなくすための対策として、「プロバイダ、電子掲示板の管理者による自主規制」を「更に強化すべき」としており、また、次に示す東京都による調査結果からも、一般にプロバイダや電子掲示板の管理者、関連機器の販売店等による取組みは十分とは認識されていないことから、警察としても関連事業者に対して自主的な取組みを促していくこととしている。

もっとも、プロバイダの中には、インターネット上の違法・有害情報の氾濫について強い問題意識を有し、自己の管理するウェブサイトやその電子掲示板を定期的に監視するなどして違法・有害情報の把握に努め、警察への通報や削除措置等を講ずるなどの取組みを推進しているところもある。

今後、警察としては、このようなプロバイダにおける先進的な取組みが業界全体において一層推進されるようプロバイダ連絡協議会等の機会を活用して、業界に対して協力を求めていくこととしている。

注1：６頁の意識調査と同一のもの
**　2：５頁の意識調査と同一のもの**

図1 - 32　インターネット上の違法・有害情報対策として必要な取組み



コラム 2　フィルタリングに関する実態調査

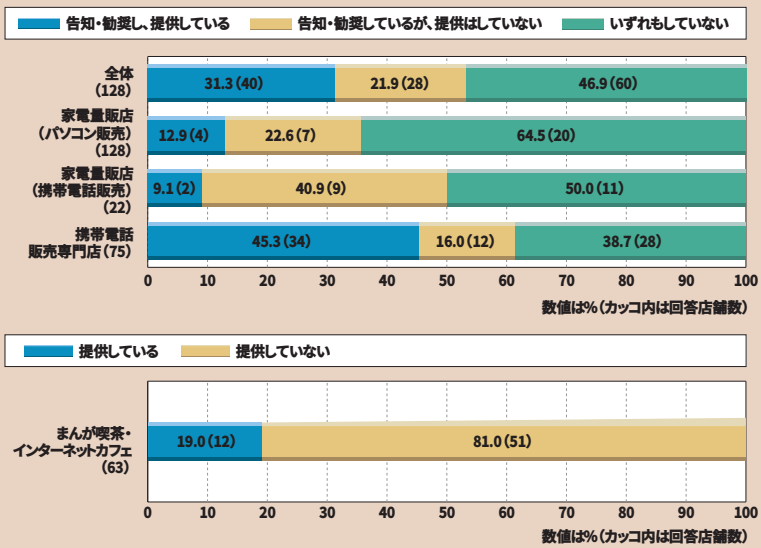
東京都青少年・治安対策本部は、平成17年3月に改正した東京都青少年の健全な育成に関する条例（第1章第3節（1）コラム3（56頁）参照）の施行状況を調査するため、18年2月から3月にかけて、東京都内に所在する家電量販店（パソコン販売部門）、家電量販店（携帯電話機器販売部門）、携帯電話機器販売専門店及びまんが喫茶・インターネットカフェを対象として「フィルタリングに関する実態調査」を行った(注)。

まず、青少年がコンピュータや携帯電話等を購入する際、フィルタリング・サービスを告知・勧奨し、提供しているかどうかについて質問したところ、31.3%（40店）の店舗が「告知・勧奨し、提供している」と回答したが、21.9%（28店）の店舗が「告知・勧奨しているが、提供はしていない」と回答したほか、「いずれもしていない」と回答した店舗は46.9%（60店）に上った。

店舗形態別にみると、携帯電話機器販売専門店では45.3%（34店）の店舗が「告知・勧奨し、提供している」と回答したものの、家電量販店のうち携帯電話機器販売部門については50%（11店）、コンピュータ販売部門については64.5%（20店）が、「いずれもしていない」と回答した。

まんが喫茶・インターネットカフェでは81.0%（51店）の店舗がフィルタリングサービスを「提供していない」と回答した。

注：調査対象数1,695のうち有効回答数は247であり、回答率は14.6%であった。



⑥　バーチャル社会の弊害から子どもを守るための取組み

インターネット上には、少年が簡単にアクセスできる状態で性や暴力に関する情報が氾濫しており、少年の健全育成を図る上で深刻な状況となっている。さらに、携帯電話等を通じたインターネット等へののめり込みが、少年の精神的な成長に悪影響を与える可能性を指摘する者もいる。

こういった現状は問題視されてはいたものの、この問題の深刻さ、解決策等については、いまだに議論の一致をみていない。

バーチャル社会の弊害から
子どもを守る研究会

そのため、警察庁は、18年４月、有識者から成る「バーチャル社会の弊害から子どもを守る研究会」を立ち上げ、出会い系サイトの利用が少年にもたらす悪影響、子どもを性の対象とするアニメがもたらす社会的弊害について幅広く議論しているところであり、今後、バーチャル社会が子どもの成長に与える様々な影響について、社会に問題提起していくこととしている。

コラム 3　地方公共団体におけるインターネット上の有害情報への対応

東京都は、17年3月、東京都青少年の健全な育成に関する条例を改正し、インターネット上の有害情報への対応に関して、事業者、保護者及び青少年の育成にかかわる者の責務を次のように規定している（同年10月施行）。なお、18年4月1日現在、東京都のほか、17府県の条例において、同様の規定が設けられている。

○　事業者の責務
- インターネット事業者は、フィルタリングを利用したサービスの開発及び提供に努めること。
- インターネット事業者は、利用者と契約を行う際に、青少年にフィルタリングを利用したサービスを提供していることを告知し、利用の勧奨等に努めること。
- インターネットカフェの経営者は、青少年にフィルタリング付きの機器の提供に努めること。

○　保護者等の責務
- 青少年にフィルタリングを利用させるよう努めること。
- インターネットの利用の危険性及び過度の利用による弊害等について、青少年に対する教育に努めること。

（２）巧妙化するサイバー犯罪への対応

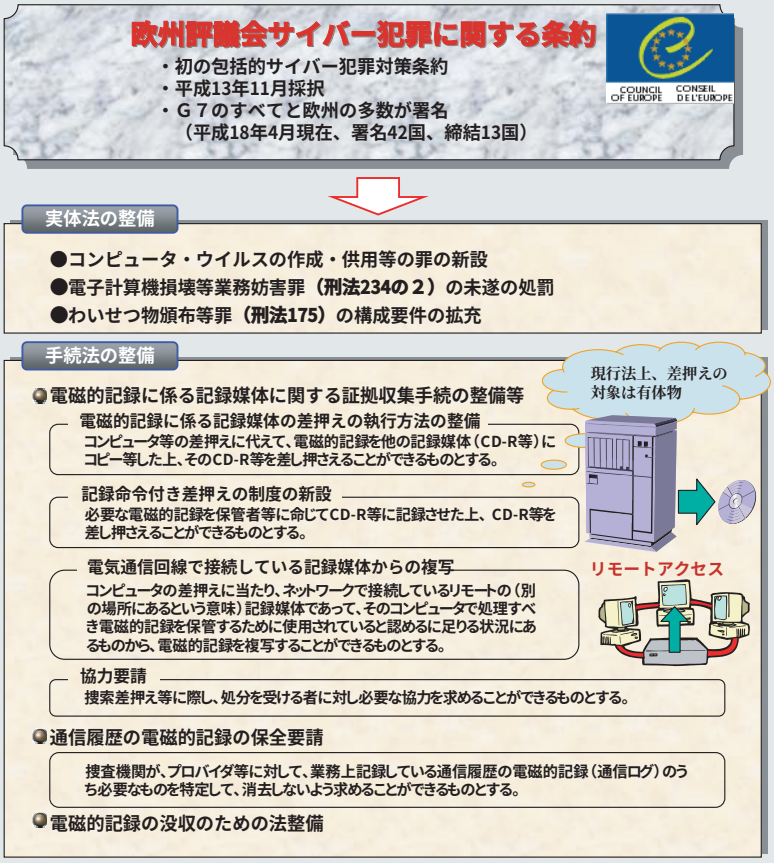
サイバー犯罪の増加、手口の高度化・多様化に対応するため、必要な法制を整備するとともに、サイバー犯罪捜査態勢の一層の強化、効果的な捜査手法の確立及び技術力の一層の高度化が必要である。

①　サイバー犯罪条約締結に向けた国内法の整備

2001年（平成13年）11月、欧州評議会で、サイバー犯罪に関する刑事実体法に関する規定、刑事手続法に関する規定及び国際協力に関する規定を含んだ世界初の包括的な国際条約である、サイバー犯罪に関する条約が採択されたことから、我が国においても、16年４月、同条約の締結について国会の承認を得、現在、その締結に向けた国内法の整備のため、不正アクセス禁止法、刑法及び刑事訴訟法の改正を含む犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案が国会に上程され、審議されている。

サイバー犯罪は、その特性上、容易に国境を越えて敢行されることから、一国の取組みによって発生を抑止し、被害の拡大を防ぐことが困難であり、国際的に協調して有効な手段をとる必要があるため、早急に国内法を整備してサイバー犯罪に関する条約を締結することが求められる。

図1 - 33　国内法の整備の概要



②　新たな犯罪への的確な対応

第１章第１節（３）②（19頁）で述べたとおり、情報通信技術の発展に伴い、コンピュータ・ウイルスがまん延し、また、スパイウェア、フィッシング、ボットネット等といった高度な技術を利用した犯罪が発生している。警察は、これらの新たな脅威から国民を守るため、これまで以上に迅速かつ的確に対応していくことが求められている。

コンピュータ・ウイルスやスパイウェアを利用した不正アクセス事犯等の捜査に当たっては、情報通信部門において個別にコンピュータ・ウイルスやスパイウェアの解析を実施しているが、犯罪に利用される技術の高度化・複雑化のために、その解析は困難になりつつある。他方、コンピュータ・ウイルスやスパイウェアの作成・供用については、サイバー犯罪条約締結に向けた国内法が整備された場合、不正指令電磁的記録作成・供用罪として処罰の対象となる。このような状況を踏まえ、警察庁では、今後、不正プログラムについてデータベースを構築することなどにより、不正プログラムに関する事案の捜査を的確に推進するための仕組みを構築することとしている。

また、国内の金融機関等を装った偽のウェブサイトがアジアやヨーロッパ等の外国のウェブサーバに設置されるなどのフィッシング事案も発生しており、今後、より高度な技術を利用した国際的な犯罪が次々と新たに生み出される可能性がある。警察庁では、24時間コンタクトポイントを活用するとともに、外国において発生した新たな手口を早期に把握し、被害の拡大防止や捜査手法の開発に反映させていくため、情報収集を更に強化していくこととしている。

③　サイバー犯罪捜査態勢の更なる強化

サイバー犯罪は国民のだれもが被害者となり得、しかも瞬時にかつ広域的に被害が発生することから、すべての都道府県警察がこれに的確に対応することができるよう十分な捜査力を備え、かつ効率的に対応するための態勢を整備することが重要である。

そこで、サイバー犯罪の捜査力を更に充実させるため、警察では、実際の捜査活動を通じてサイバー犯罪捜査に必要な知識・技能の共有を進めるとともに、専門分野別の研修等により各捜査員が最新の手口のサイバー犯罪に対応した捜査手法やコンピュータの解析手法等、自らの捜査能力向上に必要な知識・技能を選択して修得できるようにするなど、人材育成の多様化・高度化の実現に向けて取り組むこととしている。

また、巧妙化し、広域的に敢行されるサイバー犯罪に効率的に対応するという観点から、アクセスログ（以下「ログ」という。）の確保や各種照会等の捜査活動がプロバイダや関係企業等が集中する主要都市等を中心に行われている現状を踏まえ、サイバー犯罪捜査に従事している各都道府県警察の捜査員を一定地域ごとに集中して運用するなど、効率的なサイバー犯罪捜査態勢の在り方についても検討していくこととしている。

コラム 4　英国、フランス及びドイツにおけるサイバー犯罪捜査態勢

英国では、全国43の地方警察においてサイバー犯罪の捜査を行っているが、高度化・国際化するサイバー犯罪に対して的確に対処するため、2001年（13年）に全国的又は国際的な重大かつ組織的なサイバー犯罪について直接捜査を行う権限を有するとともに、個別事件に関して各地方警察に対して情報分析及び捜査の観点から必要な支援を行うことを任務とする国家ハイテク犯罪捜査局（NHTCU）(注) を創設した。現在、NHTCUの所掌事務は2006年（18年）4月に発足した重大組織犯罪対策庁（SOCA）電子犯罪部に引き継がれている（第1章第2節（5）①イ（48頁）参照）。

フランスでは、パリ警視庁及び全国19の管区司法警察局がサイバー犯罪捜査を担当する一方で、警察の中央機関である中央司法警察局の経済・金融犯罪捜査部に設置された情報技術犯罪対策中央本部が国際捜査共助や地方機関の行う捜査活動の総合調整等を行うだけでなく、複数の管区にまたがるサイバー犯罪についてその複雑性、重大性等を勘案した上で直接捜査を行うこともある。

また、ドイツでは、連邦刑事庁は各国の警察機関との情報交換や州警察の行う捜査活動の総合調整を行うとともに、一定の重大な事件について独自の捜査権限を有しており、例えば、サイバー攻撃が（ア）ドイツ連邦共和国の内的、外的安全を脅かすような場合や、（イ）非常に重要な施設であって、損失したり破壊されたりすれば人間の健康や生命に重大な脅威となるようなもの又は公共組織の機能にとって欠くことのできないものの弱点を脅かすような場合には、同庁が直接捜査を行うことができることとされている。

注：National Hi-Tech Crime Unitの略。国家犯罪捜査庁（NCS:National Crime Squad）の一部局として、全国又は国際的規模の重大かつ組織的なハイテク犯罪対策を行うことを任務としていた法執行機関

④　効果的な捜査手法の確立

ア　情報収集分析体制の強化

国民をサイバー犯罪による被害から守るためには、犯罪の手口や発生状況について迅速に情報を入手し、これを的確に分析して捜査や防犯対策を推進することが必要である。

警察では、現在もサイバー犯罪相談窓口において国民からの相談を受けるとともに、サイバーパトロールを行い、サイバー犯罪に関する情報の入手に努めている。また、プロバイダ連絡協議会を

始めとする様々な機会を通じて事業者等からも情報が寄せられている。

今後は、インターネットに流通する情報量が膨大であることや、犯罪の手段が短期間に変化し、又は巧妙化・高度化するなどの状況を踏まえ、インターネット上に流通する違法情報を自動的に検索するシステムや発見された不正プログラムを解析・分析し、データベース化する仕組みを構築し、活用するなど、情報収集分析機能の一層の高度化を図ることとしている。

また、インターネット安全・安心相談システム、インターネット利用者から違法・有害情報に関する通報を受け付けるインターネット・ホットラインセンターを通じて寄せられた国民からの情報についても、これを効果的に活用し、防犯対策や捜査活動を推進していくこととしている。

イ　捜査技術の高度化・デジタルフォレンジックの強化

コンピュータ、携帯電話等の電子機器が一般に普及し、あらゆる犯罪に悪用されるようになってきている中、犯罪の取締りに当たっては、各種電子機器に保存されている電子データの解析が捜査に必要不可欠となってきている。また、今後、法律や技術の専門家ではない一般国民が刑事裁判に参加する裁判員制度が導入され、客観的証拠の収集が必要とされることとなる。このため、破損したハードディスク等、あらゆる状態の電子機器から電子データを抽出、解析することとなり、これまで以上に高度かつ多様な解析技術が求められることとなり、消去、改ざん等が容易である電子データの解析手続や手法について、その適正を確保することが一層重要となる。

さらに、サイバー犯罪条約が締結された場合、外国の法執行機関から電子データの押収や解析等に係る捜査共助の要請等を受けることが予想され、その際、我が国の解析手続や手法が要請元において適切であると認められなければ、解析結果は当該国において証拠として採用されず、犯罪の立証に重大な支障を及ぼしかねない。

犯罪の立証のための電子データの解析手続や手法については、デジタルフォレンジックと呼ばれ、外国の法執行機関や研究機関において科学的な検証、評価等が行われつつある。各国の法執行機関が集まる国際会議等においても、当該研究成果が共有され、国際的な統一基準の策定に向けた議論が行われている。

このような情勢の下、警察においては、国際的な技術動向を踏まえつつ、これまで蓄積してきた解析技術に関する知見を集約、体系化した上で、法的な観点からの検討や科学的な検証を行うなど、デジタルフォレンジックの確立に向けた取組みを推進することとしている。

ウ　追及可能性の強化

近年、サイバー犯罪においては、プロキシサーバやセキュリティ対策が十分でないコンピュータを不正に中継したり、外国のネットワークを経由したりするなど容易に身元が判明しないような手法が用いられる傾向にある。このように巧妙化したサイバー犯罪に対して、警察ではインターネット上の通信記録であるログを分析し、コンピュータに記録された犯人の足跡を追跡する捜査を行っている。

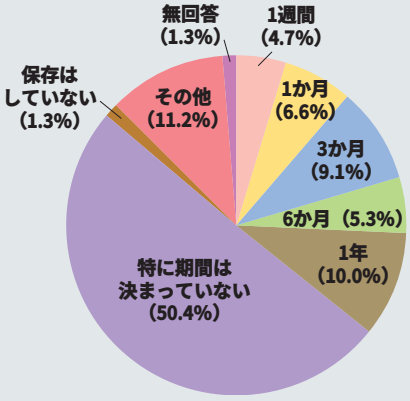
しかしながら、ログは、機器の仕様や運用管理者の設定により保存される内容に差異があり、現実には犯罪の立証に不可欠なログが捜索・差押えの際に記録・保存されていない場合も少なくない。また、国際的なサイバー犯罪捜査においては、外国の捜査機関からログの差押えに関する捜査共助を求められる場合も少なくなく、我が国においてログが保存されていない場合は国際捜査協力に支障を及ぼすこととなる。

このようにますます巧妙化するサイバー犯罪の捜査を確実に進めるためには、犯罪が行われた時点のログが保存されていることが必要不可欠であることから、今後、犯罪の立証に必要となるログが一定期間保存される仕組みについて検討を進めていくこととしている。

コラム 5 ログ保存の実態

警察庁が、17年11月に実施した不正アクセス行為対策等の実態調査によれば、ログの保存期間について1年間保存すると回答している事業者が10.0％存在するものの、特に保存期間を決めていない事業者が過半数（50.4％）を占めた。また、少ない割合ながらもログを保存していない事業者が1.3％存在していることが判明した。

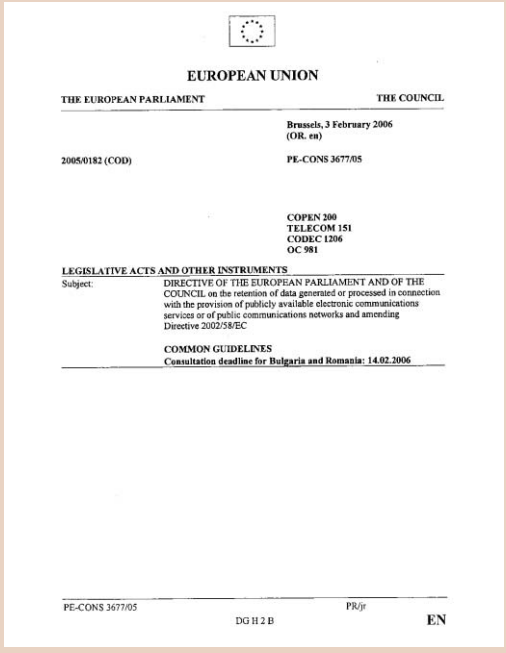
図1 - 34 ログの保存期間



コラム 6 ＥＵにおける追及可能性の確保に向けた取組み

欧州連合（ＥＵ）は、2006年（18年）2月、プロバイダ等に対してインターネットを使ったサービス等を提供する際にはＩＰアドレスを含む通信記録の保存を義務付ける指令を閣僚理事会において承認し、2007年（19年）8月までに加盟各国に対して指令内容の実施に必要な措置を講ずるよう求めることとした。

これにより、重大犯罪の捜査に際して、ＥＵ加盟国の各捜査当局は、各国の法律により保存が義務付けられる期間内（最低6か月以上2年まで）であれば、だれが、だれに、いつ、どこから通信を行ったのかなどについての情報を確実に入手することができるようになり、犯罪捜査がログが記録・保存されていないことで途切れることがなくなるものと期待されている。



EUROPEAN UNION

THE EUROPEAN PARLIAMENT — THE COUNCIL

Brussels, 3 February 2006
(OR. en)

2005/0182 (COD) — PE-CONS 3677/05

COPEN 200
TELECOM 151
CODEC 1206
OC 981

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

COMMON GUIDELINES
Consultation deadline for Bulgaria and Romania: 14.02.2006

PE-CONS 3677/05 — PR/jr
DG H 2 B — EN

エ　インターネット利用時の匿名性等への対応

インターネットの匿名性を利用したサイバー犯罪に的確に対処していくためには、どのコンピュータにおいて犯罪が行われたかを特定することとともに、そのコンピュータをだれが使用していたのかを明らかにし、被疑者を特定することが必要である。

特に、被疑者が、不特定多数の者が利用することのできるフリースポット(注)や購入時に身分確認が不要なプリペイド式データ通信カードを利用してインターネットを利用した場合、その特定は非常に困難であり、現実にこの匿名性を利用した事案の発生もみられる。警察からの要請に基づき、本人確認を強化する事業者も存在するが、取組み状況はいまだ十分なものではない。

また、インターネットカフェ等では、事業者が利用者の本人確認を行い、その使用状況を記録していなければ、犯行に利用されたコンピュータを使用していた者を特定することが困難であり、現実にこの匿名性を悪用した事案の発生もみられる。業界団体に加盟している事業者は、会員制度の導入や防犯カメラの設置等の利用者の匿名性を排除するための措置を盛り込んだ運営ガイドラインを策定するなど、自主的な取組みを進めているが、全体としては、事業者による取組み状況はいまだ十分なものではない。

さらに、出会い系サイトやアダルトサイト等では、利用の際に年齢制限が設けられているが、利用者の年齢をチェックするシステムが不十分であるとの問題も指摘されている。

今後、インターネットカフェ等を運営する事業者による利用者の本人確認に向けた自主的取組みを引き続き支援するとともに、利用者の本人確認が確実に行われるための方策についても検討を進めることとしている。

⑤　技術水準の維持・向上

ア　官民連携の強化

最新の技術等を悪用した新たな手口に対応するためには、それらに関する技術情報の収集が必要不可欠である。特に、民間企業が開発した技術や製品に係る欠陥（セキュリティ・ホール）を突いた新たな犯罪手口等の迅速な解明のためには、それらを開発した民間企業との技術協力が非常に有効である。このため、民間企業と技術情報の提供等に係る協力関係を構築するなど、官民連携を更に強化していく必要がある。

イ　解析用資機材の充実・強化

情報家電等、新たな技術が活用された機器が次々と開発されており、中には、従来の機器とは互換性がないものもある。それらの最新の機器が犯行に使用された場合には、既存の解析用資機材では、情報の抽出、分析等ができない可能性があることから、常に最新の技術に対応した解析用資機材を整備していく必要がある。

注：無線ＬＡＮでインターネットへの接続環境を提供するサービス

（3）公共の安全を害するサイバーテロ等に対する取組みの強化

①　サイバーテロ対策の強化

サイバーテロ対策を推進するためには、警察だけでなく、サイバーテロの対象となり得る重要インフラ事業者等においても、サイバーテロ対策を講ずることが重要である。

ア　対処態勢等の強化

サイバーテロを未然に防止し、また、その被害を最小限に食い止めるためには、平素から、警察だけでなく官民が連携して事案対処の能力を向上させる必要があることから、今後は、重要インフラ事業者等に対して訓練への参加を促し、実際にサイバーテロが発生した際の対処態勢を更に強化するための取組みを進める必要がある。

コラム 7　米国における業種横断的なサイバー攻撃対処訓練

2006年（平成18年）2月、米国では、国土安全保障省（DHS）が主催し、連邦捜査局（FBI）等の法執行機関を含む公的機関や民間事業者等、115の組織が参加して、重要インフラに対してサイバー攻撃が行われたとの想定の下、官民の相互連携、情報共有の手法、システムの復旧手順等についての訓練を行った。

イ　官民連携体制の更なる強化

サイバーテロが発生した場合、サイバーテロの対象となった基幹システムと同様の基幹システムを保有する他の重要インフラ事業者等においても同様の被害が発生する可能性があるため、警察と重要インフラ事業者等の連携のほか、重要インフラ事業者等相互の連携を更に深めることが重要である。そこで警察では、重要インフラ事業者等への個別訪問、サイバーテロ対策セミナー及びサイバーテロ対策協議会について、その内容を質量ともに充実させるよう努めることとしている。

②　サイバー攻撃等の予兆把握機能及び事案発生時の緊急対処能力の強化

情報通信技術の発展は日進月歩であり、サイバー攻撃の手口等も高度化・複雑化してきている。特に、近年、ボットネットという新たな脅威も発生しており、これを利用したサイバー攻撃の発生も懸念されている。それらを的確に検知・分析することにより、サイバーテロの予兆を早期に把握するとともに、事案発生時には、被害拡大防止のため、迅速な緊急対処を行う必要がある。

ア　体制の充実強化

警察では、サイバーテロの予兆把握のため、インターネット上で発生する事象の観測・分析を行っているところであるが、サイバーテロの手段となり得る新たなサイバー攻撃等を迅速に把握するため、それらに対応できるように継続的な観測機能の更なる高度化や分析体制の強化を進めていくこととしている。

イ　サイバーフォースの技術力の向上

新たなサイバー攻撃の手口が次々と登場している中、事案の未然防止のための技術的助言や事案発生時の緊急対処等を的確に実施するため、サイバーフォース要員に対して、今後も外国の法執行機関での実地訓練等を継続的に実施するほか、最先端の技術を持つ大学、民間企業等と連携した技術の研究開発等を推進することとしている。

③　国際テロ組織等のインターネット利用に対する今後の取組み

国際テロ組織等によるインターネットの利用は、インターネットの普及や情報通信技術の進展に伴い、今後一層拡大するものと考えられることから、引き続き、国際テロ組織等のインターネット利用に関する情報収集を行っていくこととしている。また、2006年（18年）６月、Ｇ８司法内務閣僚会合において、国際テロ組織等によるインターネット利用の脅威が認識され、インターネットを通じたテロ活動への支援、新たなテロリスト等の勧誘等への対策について検討することが合意されたことから、我が国としても積極的に参画していくこととしている。

（4）安全・安心なインターネット社会を目指して

情報通信技術を利用したシステムは、サイバー空間におけるコミュニティの形成や知的生産を促進する機能を有するに至り、個人や組織の社会・経済活動に深くかかわるようになった反面、様々な違法・有害情報がインターネット上にあふれ、昨今の携帯電話の普及により少年が違法・有害情報に容易にアクセスできる状態が放置されるなど、システムが生み出す弊害も露呈している。また、新たな技術を悪用した犯罪が多発し、さらには我が国の社会・経済活動の基盤をも揺るがしかねないサイバーテロの脅威も現実のものとなっている。

情報通信ネットワークに関する様々な脅威から国民・社会を守り、安全に、かつ、安心して情報通信技術を利用できる環境を整備することは、現下の我が国の重要な課題であり、警察にとっても重要な責務である。警察では、現在、インターネット上に氾濫する違法・有害情報の悪影響から国民生活を守り、サイバー犯罪に立ち向かい、そしてサイバーテロの脅威から社会を守るための取組みを進めている。

しかしながら、サイバー空間及びそれと一体化した現実社会の安全は、警察の力だけで確保できるものではない。産業界、学界、関係機関・団体はもとより、インターネットを利用する組織や個人と警察が連携を強化し、力を合わせて対策を進めることが必要である。そして、更にこれを効果あるものとするためには、何より、インターネット社会のもたらす利便性を享受するだけでなく、違法・有害情報の氾濫等、その負の側面をも正しく認識し、事業者、保護者を始めとしたインターネットにかかわるすべての者が果たすべき役割を自ら果たさなければならない。このように、インターネットにかかわる広範な人々が、現状の問題について認識を共有し、新たな時代に対応した規範を形成し、そしてそれを行動に結び付けていくとき、安全・安心なインターネット社会は、初めて実現するのではなかろうか。

サイバー空間と現実社会の安全のため、多くの方々と共に、警察は今後も全力を尽くしていく決意である。今回の特集が、一人一人の方により良いインターネット社会について考えていただく契機となれば幸いである。