

# 警察庁情報セキュリティ政策大系 - 2004

～サイバー犯罪・サイバーテロに立ち向かう警察～

平成16年8月  
警察庁

## 目次

はじめに	1
背景	2
1 高度情報通信ネットワーク社会の進展	2
2 サイバー犯罪・サイバーテロの脅威	3
(1) サイバー犯罪の検挙状況	
(2) インターネット・オークションにおける盗品等の処分	
(3) いわゆる出会い系サイトに関係した事件の検挙状況	
(4) サイバー等に関する相談の受理状況	
(5) サイバー空間におけるその他の脅威	
3 情報セキュリティ対策の現状	8
(1) 政府における情報セキュリティ対策	
(2) 産業界等における情報セキュリティ対策	
(3) 国際的な動向	
4 「緊急治安対策プログラム」について	15
5 「犯罪に強い社会の実現のための行動計画」について	15
政策大系	18
1 サイバー犯罪の取締り等の推進	18
(1) 体制の整備	
(2) 取締りの強化	
(3) 外国関係機関との連携強化	
2 サイバーテロ対策の推進	21
(1) 体制の整備	
(2) 緊急対処能力並びに関連情報の収集及び分析能力の強化	
(3) 人材育成・資機材の充実強化	
(4) 重要インフラ事業者等との連携強化	
(5) 外国関係機関との連携強化	
3 高度情報通信ネットワーク社会における情報セキュリティの向上	23
(1) 警察の情報通信システムにおけるセキュリティの確保	
(2) 高度情報通信ネットワーク社会における警察の基盤の確立に向けた取組み	
(3) 産業界・関係機関等との連携強化	
(4) 広報啓発の推進	
参考資料	29

## はじめに

平成 12 年 2 月に策定した「警察庁情報セキュリティ政策大系」(以下、旧大系という。)に基づき、警察は、サイバー犯罪対策、サイバーテロ対策等高度情報通信ネットワーク社会の治安維持に係る情報セキュリティ施策に重点的に取り組んできた。

その間、高度情報通信ネットワーク社会推進戦略本部(IT 戦略本部)を中心とした内閣のリーダーシップの下、「我が国が 2005 年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」、IT の戦略的な利活用を軸に「元気・安心・感動・便利」社会を目指す「e-Japan 戦略」等に基づく各種の計画が策定され、官民総力を挙げて我が国の IT 革命に対する各種の取組みが図られてきた。これを受け、国民がその利便性を十分享受できる高度情報通信ネットワーク社会の着実な形成を図るためには、情報セキュリティの確保が欠かせないことから、警察においても、「高度情報通信ネットワークの安全性及び信頼性の確保」のための各種施策を推進してきたところである。

このように官民を挙げて IT 施策を進めた結果、平成 15 年 12 月末で総人口の 60%以上がインターネットを利用するに至り、情報通信ネットワークが社会・経済活動の根幹に必要なインフラとなったが、その一方で、サイバー犯罪・サイバーテロ等の脅威は、国民の生活基盤をゆるがしかねない社会問題となっている。サイバー犯罪の検挙件数は、年々増加の一途をたどっているほか、平成 15 年中のサイバー犯罪等に関する相談受理件数は、41,754 件となり、前年に比べて約 2.2 倍に増加している。また、韓国で特に甚大なインターネット接続障害を生じさせたスラマーワームの発生やブラスターワームのような感染スピードの速いワームがまん延するなど、いわゆるコンピュータ・ウイルスの猛威もいまだ衰えてはいないばかりか、世界規模でインターネットのデータの流れを制御するルート DNS サーバに対する DDoS 攻撃が発生するなど、サイバーテロの脅威も現実のものとなっている。

こうした現状にかんがみ、また、旧大系を定めて 4 年を経過したこともあり、近年のサイバー空間の情勢に対応した情報セキュリティ政策の方向性と具体的な施策を明確化するため、旧大系を見直して、新たに「警察庁情報セキュリティ政策大系 - 2004」を策定し、サイバー犯罪・サイバーテロに立ち向かう警察としての情報セキュリティ施策を推進することとした。

## 背景

### 1 高度情報通信ネットワーク社会の進展

「2005年までに世界最先端のIT国家となる」との目標を掲げ、平成13年1月に策定された「e-Japan戦略」及び同戦略を具体化した年次計画である「e-Japan重点計画」に掲げられた施策等により、インターネット利用人口は、着実に増加し、平成15年末には7,730万人となり、人口普及率は60.6%と初めて6割を超えた(図1)ほか、ブロードバンド回線<sup>(\*)</sup>の利用率が前年の29.6%から47.8%へと大幅に増加した(図2)。政府の高度情報通信ネットワーク社会推進戦略本部(IT戦略本部)は、平成15年7月にITの戦略的な利活用を軸に「元気・安心・感動・便利」社会を目指す「e-Japan戦略」さらには平成16年2月にはそれを加速化するための「e-Japan戦略 加速化パッケージ」を策定し、平成16年6月には2006年以降に向けての布石を含む「e-Japan重点計画-2004」が策定されている。

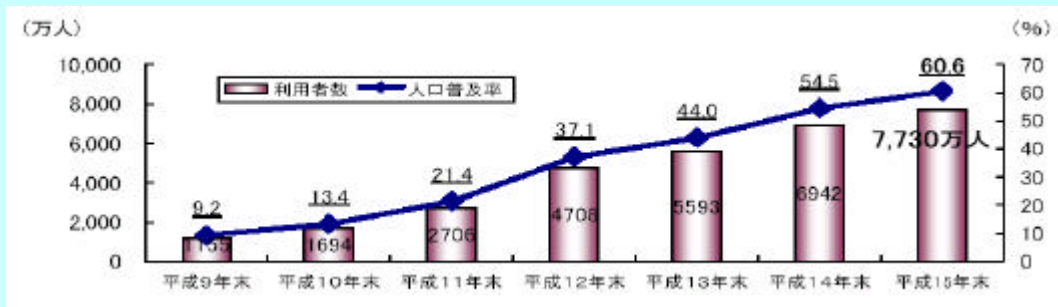


図1 インターネットの人口普及状況<sup>(\*)</sup> (出典：総務省「平成15年通信利用動向調査」)

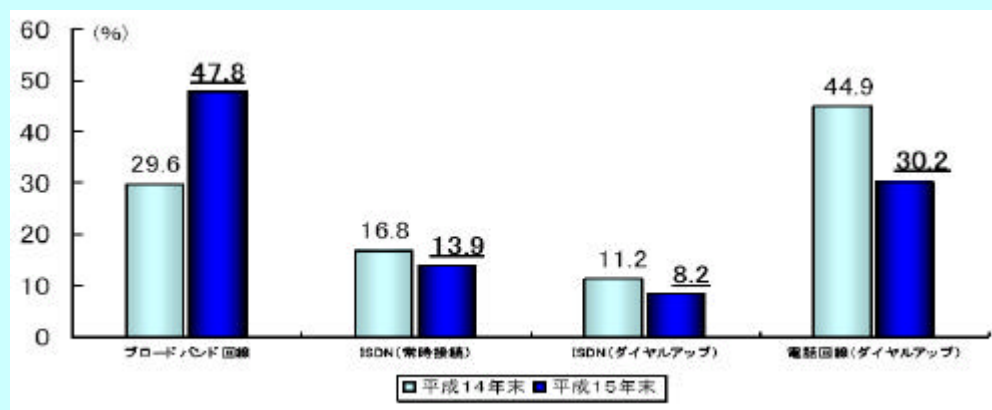


図2 パソコンからのインターネットへの接続方法の推移 (出典：総務省「平成15年通信利用動向調査」)

(\*) DSL(デジタル加入者線)、ケーブルインターネット、無線(FWA等)及び光ファイバー

(\*\*) ここでいう利用者とは、パソコン・携帯電話・PHS・携帯情報端末、ゲーム機・TV機等のうち、1つ以上の機器からインターネットを利用している6歳以上の者をいう。

このように、IT 基盤の整備に伴う高度情報通信ネットワーク社会への移行は着実に進展しており、インターネット・ショッピングやインターネット・オークション等の電子商取引が活発化しているほか、自治体においても、申請・届出等手続のオンライン化や行政の情報化推進体制を進めており、また、住民基本台帳ネットワークにおける IC カードの導入を開始するなど、IT の利活用が図られている。

さらに、「いつでも・どこでも・何でも・誰でも」ネットワークにアクセス可能なユビキタス・ネットワーク社会の実現に向けた取組みが進められ、新たなインターネット関連技術が次々と出現していることから、高度情報通信ネットワーク社会の進展はますます加速している。

## 2 サイバー犯罪・サイバーテロの脅威

### (1) サイバー犯罪の検挙状況

高度情報通信ネットワーク社会の光の部分が進展するに伴い、その陰の部分も露呈してきており、サイバー犯罪<sup>(\*)</sup>及びサイバーテロの脅威の増大は、国民の生活基盤をゆるがしかねない社会問題となっている。

警察では、サイバー犯罪を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、コンピュータ・電磁的記録対象犯罪及びネットワーク利用犯罪に分類し、その傾向を把握するとともに、各種対策を講じてきたところであるが、サイバー犯罪の検挙件数は年々増加しており、平成 15 年中は 1,849 件と、前年と比べて 243 件増加した(図 3、表 1)。

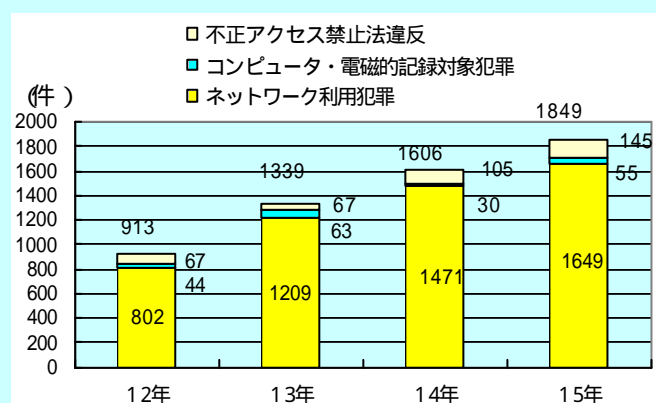


図 3 サイバー犯罪の検挙件数の推移

(\*) 情報技術を利用する犯罪を指す。従来、警察庁では、コンピュータ技術や電気通信技術を悪用した犯罪を「ハイテク犯罪」と表していたが、国際的動向等を踏まえ、現在は「サイバー犯罪」と表すこととしている。

	H12	H13	H14	H15	増減			
不正アクセス禁止法違反	67	67	105	145	+ 40			
コンピュータ・電磁的記録対象犯罪	44	63	30	55	+ 25			
電子計算機使用詐欺	33	48	18	34	+ 16			
電磁的記録不正作出・毀棄	9	11	8	12	+ 4			
電子計算機損壊等業務妨害	2	4	4	9	+ 5			
ネットワーク利用犯罪	802	1,209	1,471	1,649	+ 178			
児童買春 児童ポルノ法違反(買春)	8	121	117	268	269	371	+ 1	- 37
" (ポレノ)	113	128	245	140	408	102	371	- 38
詐欺	306	485	514	521				+ 7
わいせつ物頒布等	154	103	109	113				+ 4
青少年保護育成条例違反	2	10	70	120				+ 50
脅迫	17	40	33	38				+ 5
著作権法違反	80	86	66	87				+ 21
名誉毀損	30	42	27	46				+ 19
その他	92	198	244	353				+ 109
合 計	913	1,339	1,606	1,849				+ 243

表 1 サイバー犯罪の検挙件数の内訳

## ア 不正アクセス禁止法違反

サイバー犯罪のうち、不正アクセス禁止法違反の検挙は、同法が施行された平成 12 年から一貫して増加している。平成 15 年中は 58 事件（145 件）<sup>(\*)4</sup> 検挙している（図 4）が、このうち 26 事件（77 件）が、ID 等から容易に推測されるパスワードの利用等、利用権者の設定・管理の甘さにつけ込んで ID やパスワードを入手し、不正アクセス行為を行ったものであった。また、プログラムの脆弱性を利用したホームページの改ざんのように、セキュリティの脆弱性を突くセキュリティ・ホール攻撃型も引き続きみられたほか、キーロガー<sup>(\*)5</sup> を使用して ID・パスワードを入手するなど、高度なコンピュータ技術を悪用したものもあった。

<sup>(\*)4</sup> 事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合も 1 事件と数える。件数とは、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。不正アクセス行為の件数の計上については、一つのアクセス制御機能に対する一つの手口による侵害行為が 1 回あったことをもって 1 件としている。ただし、被疑者が異なる場合（共犯を除く。）はそれぞれ 1 件として計上し、短期間に一つのアクセス制御機能に対して同一手口による侵害が連続的に行われ、実質上 1 回の行為とみなしうる場合は包括して 1 件としている。

<sup>(\*)5</sup> インストールしたパソコン端末において、キーボードでどの文字を打鍵したかを記録するプログラムのこと。

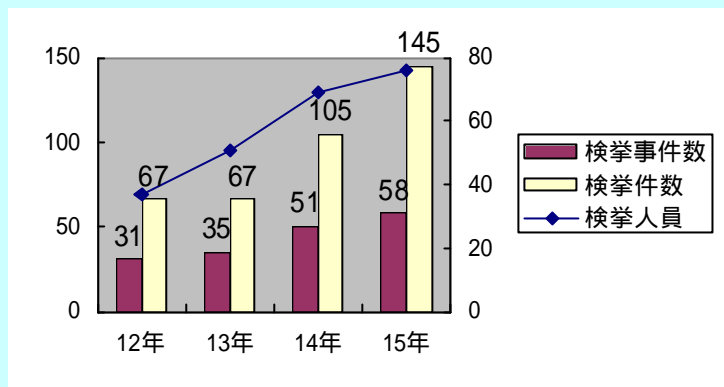


図4 不正アクセス禁止法違反の検挙状況の推移

## イ ネットワーク利用犯罪

ネットワーク利用犯罪<sup>(\*6)</sup>は、サイバー犯罪の検挙件数のうち最も多くを占める犯罪であり、平成15年中は1,649件（全体の約89%）を検挙している。ネットワーク利用犯罪では、いわゆる出会い系サイトを利用した児童買春や青少年保護育成条例違反、インターネット・オークションを利用した詐欺やわいせつ物頒布、著作権法違反、電子掲示板を利用した名誉毀損や脅迫が多くを占めている。

また、平成15年中にインターネットを利用して取引されたけん銃の押収丁数は、201丁で前年より86丁増加し、過去最高を更新したほか、薬物をインターネット上で取引する薬物事犯等も発生しており、サイバー空間が犯罪に悪用されないよう適切な対策を講じていく必要がある。

### (2) インターネット・オークションにおける盗品等の処分

インターネット・オークションにおいては、詐欺事件だけでなく、盗品等を処分する事例も見られ、平成15年中の盗品等の処分件数は338件であった。このうち、古物営業法に基づく業務の実施の方法の認定を受けていないオークションでの処分が336件と99.4%を占めている。インターネット・オークションの出品物について、盗品等であると疑うに足りる相当な理由がある場合においては、警察本部長等は、そのインターネット・オークション事業者に対して、競りの中止（出品物の削除）を命ずることができることされており、平成15年9月1日の改正古物営業法の施行以降、平成16年3月31日までの間に3件の命令が発出されている。

### (3) いわゆる出会い系サイトに関係した事件の検挙状況

いわゆる出会い系サイトについては、ネットワーク利用犯罪には当たらない

(\*6) 犯罪の構成要件に該当する行為についてネットワークを利用した犯罪、又は、構成要件該当行為ではないものの、犯罪の敢行に必要不可欠な手段としてネットワークを利用した犯罪をいう。

いものも含め、これに関係した事件<sup>(\*)</sup>として、平成15年中に1,743件を検挙している。中でも、重要犯罪（殺人、強盗、強姦、略取誘拐、強制わいせつ）が、137件と前年に比べて37件（37%）増加しているほか（図5、表2）、被害者1,510人のうち18歳未満の児童が1,278人と約85%を占めており、事件の凶悪化や出会い系サイトを利用して犯罪にまきこまれる児童の増加が懸念されている。また、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、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。）違反事件は、平成15年9月の同法の施行から平成16年6月末までに20件検挙している。

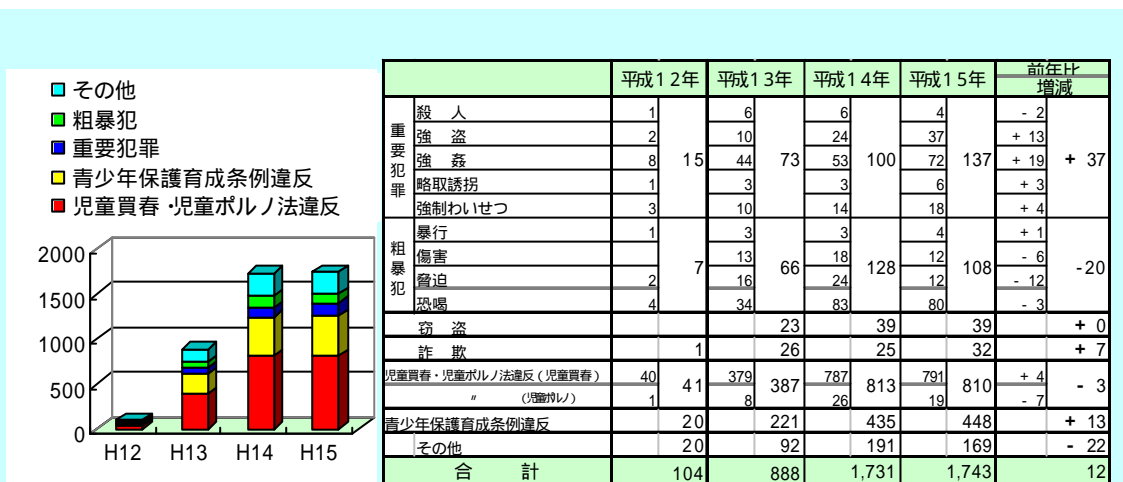


図5 出会い系サイトに関係した事件の推移 表2 出会い系サイトに関係した事件の内訳

#### (4) サイバー犯罪等に関する相談の受理状況

サイバー空間の脅威の増大は、サイバー犯罪の検挙等だけでなく、サイバー犯罪等の相談受理件数の急増にも表れており、平成15年中に全国の警察で受理したサイバー犯罪等に関する相談件数は、41,754件と前年の約2.2倍となっている。中でも、利用した覚えのない有料サイトの料金を請求されるいわゆる架空請求メール等の詐欺・悪質商法に関する相談が20,738件と前年の約6.5倍に急増したほか、インターネット・オークションに関する相談も年々増加しており、前年の約1.5倍、平成12年の約4.6倍となってい

(\*) 対象は、インターネット上で異性間の出会いの場を提供する電子掲示板、チャット等のいわゆる出会い系サイトに関係した事件として警察庁に報告のあったもの。

なお、出会い系サイトに関係した事件には、出会い系サイトをきっかけとして被疑者と被害児童が知り合い、その後、ネットワーク以外の手段でのやりとりを経て買春を行った場合など、ネットワーク利用犯罪にはあたらぬものも含まれている。

る(図6)。

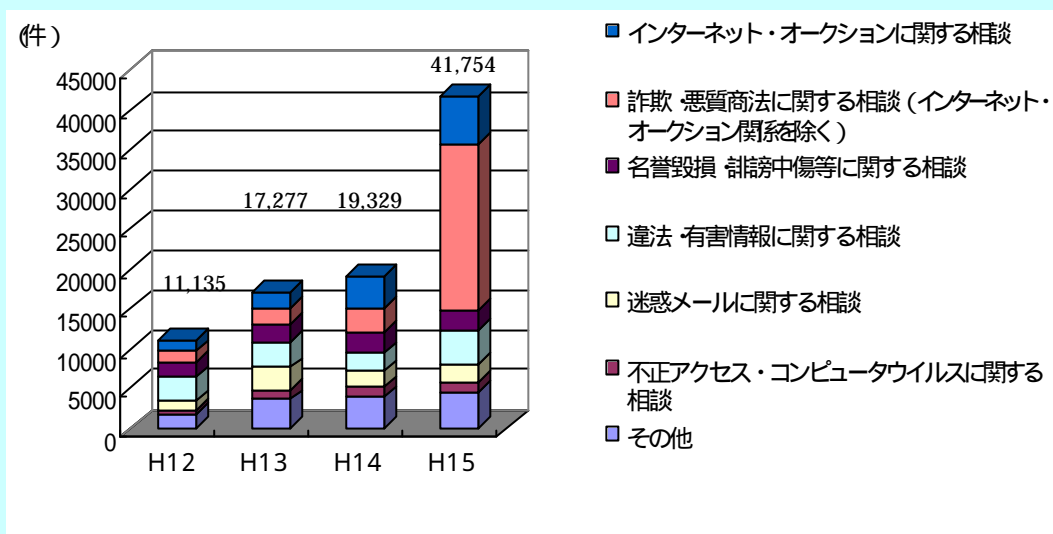


図6 サイバー犯罪等に関する相談受案件数の推移

#### (5) サイバー空間におけるその他の脅威

我が国においては、ここ数年、中央省庁等のホームページ改ざん、歴史教科書問題をめぐるアクセス集中等による関係ホームページ攻撃事案が発生するなど、通信ネットワークや情報システムを利用した電子的な攻撃、いわゆるサイバー攻撃も恒常的に行われている。

平成14年10月に発生したルートDNSサーバ<sup>(\*)8)</sup>に対するサイバー攻撃事案では、我が国や米国等世界13か所に設置された当該サーバに対し一斉にDDoS攻撃<sup>(\*)9)</sup>が敢行され、7か所のサーバで情報処理能力が大幅に低下し、他の2か所では一時的に機能が停止するという事態に至った。また、平成15年1月には、いわゆるスラマーワーム<sup>(\*)10)</sup>が発生し、ブロードバンド(大容量・高速)通信先進国の一つである韓国において大規模なインターネット

(\*)8) インターネットのドメイン名とIPアドレスを対応させるための情報を提供するネームサーバは世界中に無数に存在し、ドメイン名に対応した階層構造をなしているが、その最上位に位置するサーバのこと。

(\*)9) DoS(Denial of Service)攻撃とはコンピュータに対し、想定していないほど大量のアクセスの繰り返し等を行い、コンピュータのサービス提供を不可能にするなどの攻撃手法であり、サイバー攻撃の一つ。DDoS(Distributed Denial of Service)攻撃は、多数のマシンから同時にDoS攻撃を行う分散型DoS攻撃のこと。

(\*)10) 特定のデータベースサーバソフトの脆弱性を利用してサーバに侵入し、さらに他の任意のサーバへ同様の侵入を繰り返すことによりネットワークの通信量を増大させ、コンピュータ・システムの機能停止を引き起こすコンピュータ・ウイルス。

接続障害が発生したほか、同年 8 月には、特定のコンピュータに対してサイバー攻撃を行うようプログラムされていたいわゆるブラスタースターム<sup>(\*)11)</sup>が世界規模でまん延し、一部の日本の行政機関では当該ワームがシステムに感染するのをおそれ、運用を停止するという事態が起こっている。

このように深刻なサイバー攻撃事案が散見されることや、世界中にまん延する可能性のあるコンピュータ・ウイルスが次々に発生していることなどから、サイバーテロの脅威は我が国においても現実のものとなっている。

また、現在の法体系においては、必ずしも犯罪にはあたらないものの、昨今多発している情報漏えい事案も、情報セキュリティ上、看過できない社会問題となっており、個人情報の保護を含め、インターネット上における国民の権利保護に係る取組みが求められている。

### 3 情報セキュリティ対策の現状

高度情報通信ネットワーク社会の利便性を享受するためには、情報通信ネットワークや情報システムの安全性・信頼性を確保することが必要不可欠である。

サイバー空間の安全と秩序の維持を図るため、政府及び産業界等においては、以下のとおり、情報セキュリティ対策の推進に努めている。

#### (1) 政府における情報セキュリティ対策

情報セキュリティ対策に係る我が国政府の取組みは、高度情報通信社会推進本部（平成 6 年 8 月内閣に設置。内閣総理大臣が本部長。）が「高度情報通信社会推進に向けた基本方針」を策定した平成 7 年 2 月に始まるが、同基本方針は、情報技術の進展及び社会情勢にかんがみ、平成 10 年 11 月に改訂されており、その中では、高度情報通信社会の実現に向けた課題の一つとして「ハイテク犯罪対策・セキュリティ対策・プライバシー対策」が掲げられ、具体的には、コンピュータ・ウイルス対策、不正アクセス対策、暗号技術の不正利用対策、個人情報の管理の在り方等の諸問題について検討することとされた。

その後、平成 11 年 9 月、官民のコンピュータ・システムを違法・不正行為から守るための対策全般を政府全体として総合的に推進するため、内閣官房副長官を議長とする「情報セキュリティ関係省庁局長等会議」が設置され、必要とされる法制度の検討、ハッカー対策等の基盤整備、サイバーテロ対策等について検討することとされた。このうち、ハッカー対策については、平成 12 年 1 月、同会議は、我が国政府の情報セキュリティ政策の方向性を示

---

(\*)11) 特定のコンピュータ基本ソフト（OS）の脆弱性を有するコンピュータに侵入し、そのプログラムが実行されることによりコンピュータの異常終了を生じさせ、さらに同様の脆弱性を有する他のコンピュータを探し、感染を繰り返すことにより感染の被害が拡大するコンピュータ・ウイルス。

した「ハッカー対策等の基盤整備に係る行動計画」を策定し、政府機関の安全対策の推進、民間重要インフラの安全対策の推進、国際的な連携等に積極的に取り組んでいくこととした。さらに、同会議を発展的に改組することにより平成12年2月に設置された「情報セキュリティ対策推進会議」は、同行動計画に掲げられた各事項の具体化を積極的に進め、これまでに、セキュリティポリシーに関するガイドラインの策定や内閣官房における緊急対応支援チーム（NIRT：National Incident Response Team）<sup>(\*12)</sup>の設置等を行っている。同会議は、サイバーテロ対策に関しても、平成12年12月に「重要インフラのサイバーテロ対策に係る特別行動計画」を策定、当該特別行動計画のフォローアップを積極的に実施してきている<sup>(\*13)</sup>。

また、高度情報通信ネットワークの安全性及び信頼性の確保のためには、省庁横断的な政府内の連携が不可欠であることから、内閣官房を中心に、同会議その他あらゆる場を通じた情報セキュリティに係る省庁間の情報共有を進めており、情報セキュリティ事案に係る政府内の連絡体制を確立しているほか、内閣官房、警察庁、総務省及び経済産業省の4省庁が協同して、コンピュータ・ウイルスの被害に遭わないよう注意喚起を実施するなど、政府内の連携を強化している。

## (2) 産業界等における情報セキュリティ対策

対象を特定しないサイバー攻撃は高度情報通信ネットワーク上で恒常的に行われており、家庭や企業を問わず常時接続されたコンピュータ・システムは常にその脅威にさらされているため、不断の情報セキュリティ対策が重要である。しかしながら、現状における情報セキュリティ文化は未だ発展途上にあるといえる。前項で取り上げた韓国のスラマーワーム事案では、当該ワームは特定のデータベースサーバソフトの安全上の欠陥（セキュリティ・ホール）を突いて自己増殖するものであったが、その発生より前に、必要なパッチファイル<sup>(\*14)</sup>は既に公開されており、ユーザーレベルでの情報セキュリティ対策が適切に講じられていれば被害はこれほど拡大しなかったと考えられる。

---

(\*12) 電子政府や民間重要インフラ事業者等の情報システムへのサイバーテロ等の国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案に対し、各省庁等における情報セキュリティ対策の立案に必要な調査・助言等を行うために設置された組織。

(\*13) 「重要インフラのサイバーテロ対策に係る特別行動計画のフォローアップについて」（平成14年3月）  
「重要インフラのサイバーテロ対策に係る特別行動計画に基づく取組みの推進について」（平成14年11月）

(\*14) ソフトウェアの不具合の修正や小規模なバージョンアップを行うためのデータ又はプログラム。無料で提供されていることが多い。

我が国における情報セキュリティ対策の進展状況については、警察庁が平成15年に、全国の企業、医療機関、教育機関及び行政機関等2,000団体を対象に（うち、回答を得たのは732団体）実施したアンケート調査<sup>(\*15)</sup>によれば、情報セキュリティポリシー<sup>(\*16)</sup>を策定済みの団体は、金融機関では88.6%、エネルギー関連企業で71.4%に達しているが、教育機関では16.5%にとどまっているほか、医療機関に至っては、7.7%しか策定していないとの結果が得られており、業種による取組みの格差は依然として大きい（図7）。

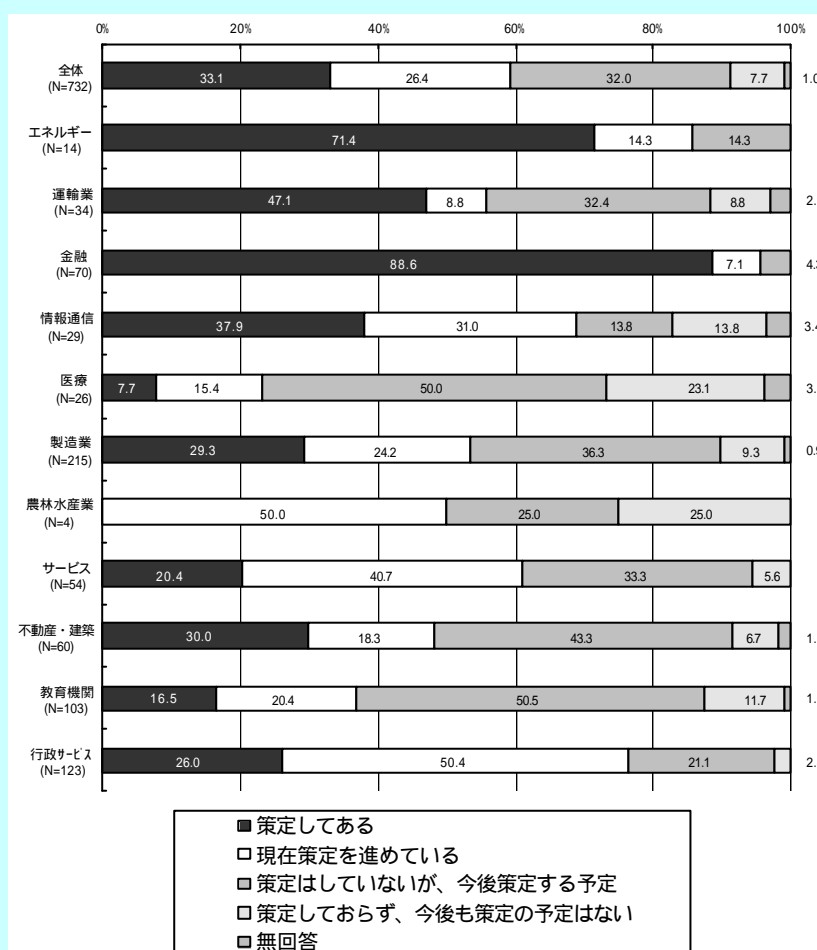


図7 業種別情報セキュリティポリシーの策定状況

(\*15) 「不正アクセス行為対策等の実態調査」(平成15年12月公表。調査結果については、警察庁サイバー犯罪対策ホームページ (<http://www.npa.go.jp/cyber/>) に掲載している。)

(\*16) どのような情報資産をどのような脅威からどのようにして守るかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用等を定めた規定。

また、全体としては、情報セキュリティポリシーを策定済み又は策定中の団体は約60%に増加したものの、一方で、セキュリティポリシーに情報セキュリティ教育を規定している団体のうち、34.2%が実際には実施しておらず(図8)、同様にセキュリティポリシーにセキュリティ監査を規定している団体のうち、40.6%が実際には実施していないことが分かっており(図9)、情報セキュリティポリシーを策定するだけでなく、その実行が求められる。

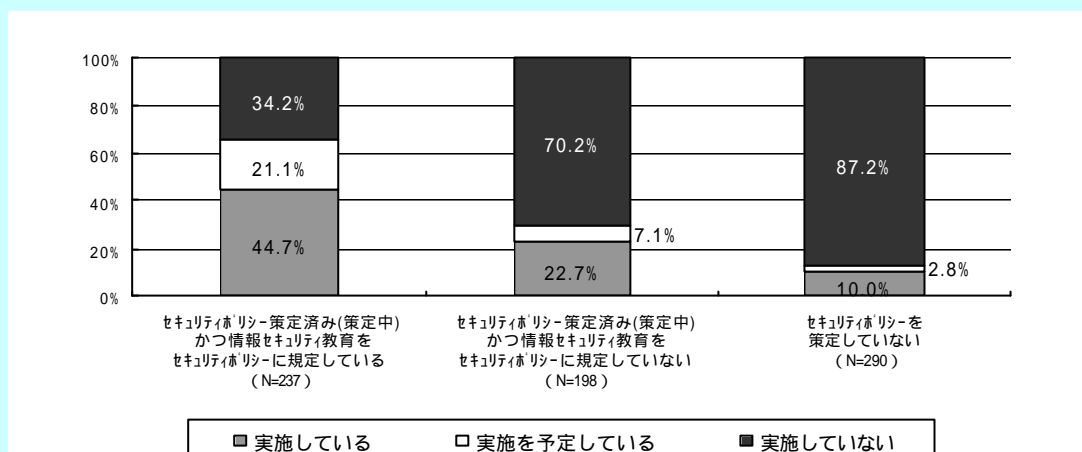


図8 情報セキュリティ教育の実施状況

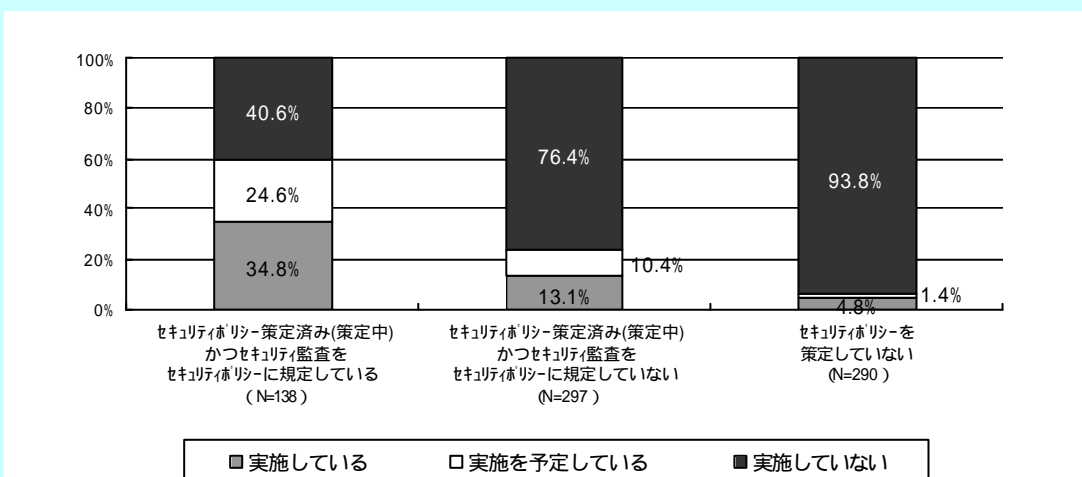


図9 セキュリティ監査の実施状況

また、無線 LAN<sup>(\*\*17)</sup>については、ESS-ID の適切な設定、暗号化、MAC アドレス認証<sup>(\*\*18)</sup>のすべてを実施している団体は、無線 LAN を利用している団体のうち 14.9%と、取組みが進んでいるとは言えない状況となっている（図 10）。

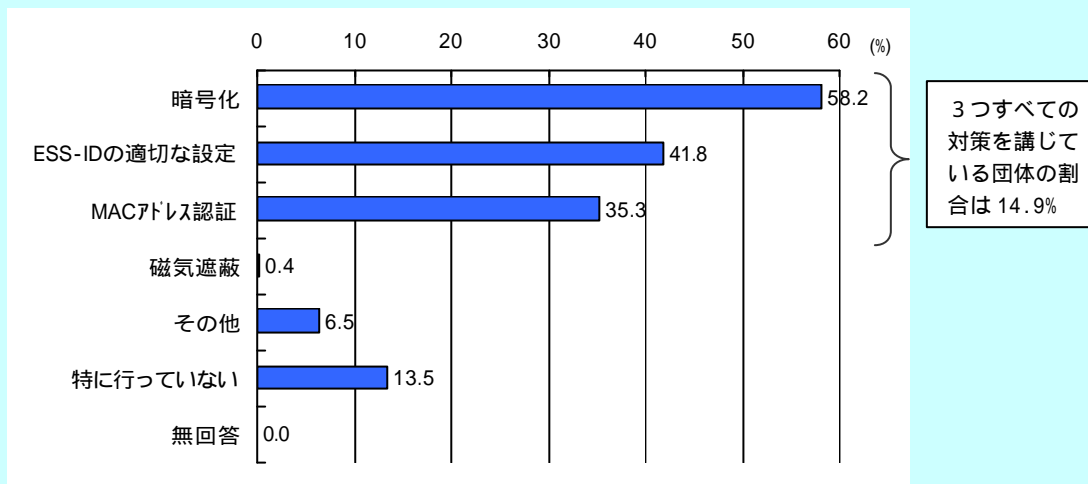


図 10 無線 LAN のセキュリティ対策状況

コンピュータ・ウイルス感染防止対策については、全体の 91.5%でクライアント（利用者）端末にウイルス対策ソフトを使用しており、年々取組みは進んでいるものの（図 11）情報セキュリティに関する被害状況についての回答では、過去 1 年間において情報セキュリティに関する何らかの被害に遭ったと回答した団体は、全体の 61.4%に上り、そのうち 91.5%がコンピュータ・ウイルス感染による被害であったことから（図 12）、引き続き、サーバへのウイルス対策ソフトの導入やパターンファイルの頻繁な更新等により、ユーザのセキュリティ意識の向上等を含めた総合的な対策を進めていく必要がある。

(\*17) 無線を利用して構築される LAN（企業内、ビル内等のある限定された空間において、コンピュータやプリンタ等の機器を接続するネットワーク）。

(\*18) ESS-ID は、無線 LAN ネットワークの ID であり、同じ ID を設定しているコンピュータのみ通信できる。よって、ESS-ID を設定することにより、同じ設定をしていないコンピュータからの接続を排除できる。また、MAC アドレス認証を行っていると、あらかじめアクセスポイントに登録してある MAC アドレス（のコンピュータ）のみ接続を許可される。ESS-ID、暗号化、MAC アドレス認証は、ほとんどの無線 LAN に実装されている機能であり、無線 LAN の基本的セキュリティ対策とされている。

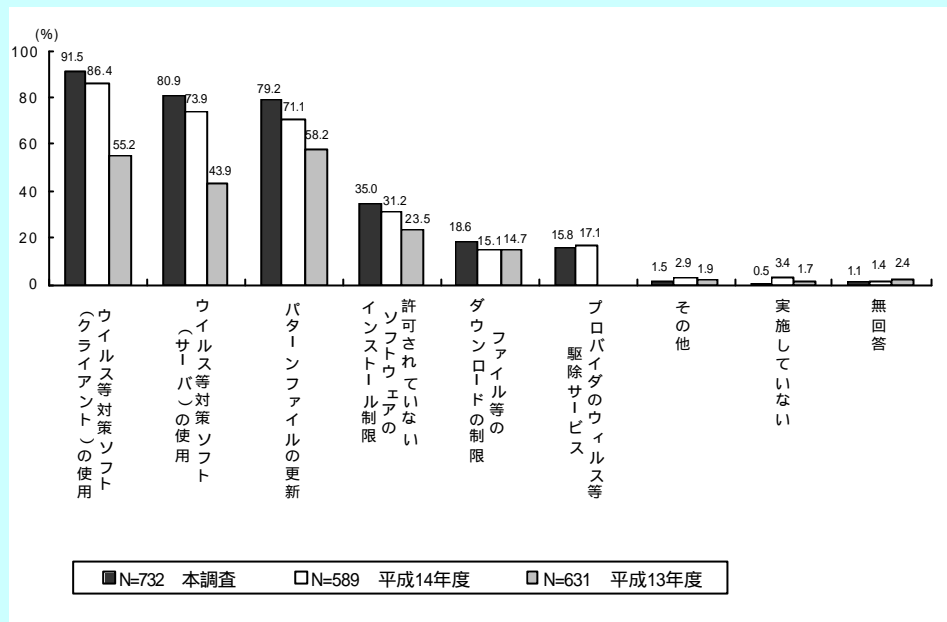


図 11 コンピュータ・ウイルス等の不正プログラムに対する対策の取組み状況

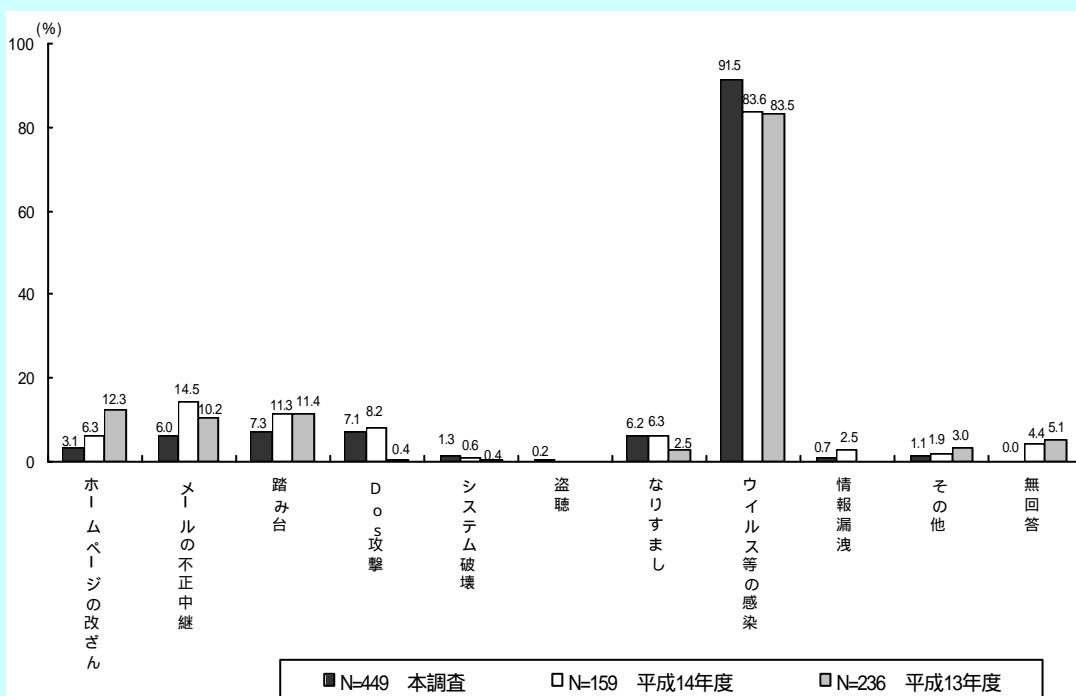


図 12 過去 1 年間で情報セキュリティに関する被害に遭った団体の被害内容

こうした調査結果からは、我が国における情報セキュリティ対策は必ずしも十分でないことが見受けられることから、高度情報通信ネットワーク社会を構成する者それぞれが、サイバー空間の脅威に対して情報セキュリティ対策を講じるべきである、という情報セキュリティ文化の醸成を図る必要があ

る。

### (3) 国際的な動向

世界的にも IT 化の波がひろがりつつある一方で、サイバー犯罪・サイバーテロの脅威もまた深刻化しているとともに、サイバー空間には国境がないことから、サイバー犯罪・サイバーテロに的確に対処するためには、国際的な連携が必要不可欠であり、多様な枠組みでの議論がなされている。

G8 リヨン・グループのハイテク犯罪サブグループでは、平成 9 年 12 月の G8 司法・内務閣僚級会合で策定された「ハイテク犯罪と闘うための原則と行動計画」等に基づき、国際捜査協力、各国国内の法制度や捜査手法及び産業界との連携等についての議論がなされており、平成 14 年 5 月の G8 司法・内務閣僚級会合においては、サイバー犯罪捜査の特殊性に一層的確に対応すべく、24 時間コンタクト・ポイント<sup>(\*19)</sup>の拡充が合意された。また、平成 13 年 9 月に発生した米国同時多発テロ事件以後は、サイバーテロ対策も重要な議題の一つとなっており、平成 14 年 5 月の同会合では、国際的な情報通信ネットワークを使用する犯罪者等の所在確認及び本人確認を迅速に行うための「テロ・犯罪捜査における国境を越えたネットワーク・コミュニケーション追跡のための勧告」が承認され、平成 15 年 5 月の同会合では「G8 重要インフラ防護に関する原則」が承認された。

経済協力開発機構（OECD）では、不正アクセスやコンピュータ・ウイルス等の脅威から情報システムと通信ネットワークを保護するため、政府機関、企業、個人を含むすべてのネットワーク参加者が、この脅威と予防策を適切に理解し、自己責任でセキュリティ強化のための措置をとる必要があるとして、平成 14 年 7 月に「情報システム及びネットワークのセキュリティのためのガイドライン」<sup>(\*20)</sup>を改訂し、各加盟国に情報セキュリティ文化の醸成に向けて取り組むよう勧告している。

また、欧州評議会では、サイバー犯罪の地理的無制約性その他の特性にかんがみ、国際的な法的枠組みの構築のため、平成 13 年 11 月 8 日、サイバー犯罪に関する実体法、刑事手続法及び国際捜査協力に関する規定を含んだ世界初の包括的な国際条約として「サイバー犯罪に関する条約」が採択され、我が国は署名開放と同時に本条約に署名した。なお、本条約は第 159 回国会で承認されている。

このように、国際社会においては、各国政府がサイバー犯罪・サイバーテロに対して適正な対策を講じつつ、関係各機関と連携し情報セキュリティ文化を醸成するといった流れが着実に形作られてきているといえる。

---

(\*19) サイバー犯罪捜査に関する国際捜査協力について 24 時間常時対応できる連絡窓口。

(\*20) 全文については、OECD ホームページ（<http://www.oecd.org/>）に掲載している。

#### 4 「緊急治安対策プログラム」について

緊急治安対策プログラム<sup>(\*21)</sup>は、刑法犯認知件数の増加、特に街頭犯罪や侵入犯罪の急増、少年犯罪・重要凶悪犯罪の増加等により、国民の日常生活に多大な不安を抱かせ、さらには我が国の社会・経済にも影響を与えていることに加え、社会のグローバル化・IT化に伴い、国際テロやサイバー犯罪・サイバーテロ等の新たな脅威に直面していることを踏まえ、犯罪の増加基調に早急に歯止めをかけ、国民の不安を解消するため、警察が、緊急かつ重点的に取り組んでいく治安対策のプログラムとして平成15年8月に策定したものである。同プログラムの3つの基本課題の一つとして、「新たな脅威への対応（組織犯罪・サイバー犯罪対策の強化とテロの未然防止）」を挙げており、警察全体として、サイバー犯罪及びサイバーテロ対策を重点的に取り組むこととしている。

具体的な施策としては、最初に、県境、国境のないサイバー犯罪の特殊性を考慮し、都道府県警察における捜査等の重複を避けるため、予防、捜査を一体として警察庁においてこれを指導調整する体制を確立することを挙げているほか、平成13年に署名した「サイバー犯罪に関する条約」を履行するための援助体制を整備し、関係国の機関との連携体制を構築することとしている。また、サイバーテロ対策については、情報収集、分析態勢の強化、要員の教育訓練の充実、重要インフラ事業者との連携強化を推進することとしている。

さらに、いわゆる出会い系サイト対策として、平成15年に制定された出会い系サイト規制法に基づき、出会い系サイトに係る少年の犯罪被害の防止及び少年の規範意識の向上等を図ることとしているほか、犯罪抑止のため、インターネット等を通じた国民への情報提供を推進することとしている。

#### 5 「犯罪に強い社会の実現のための行動計画」について

犯罪に強い社会の実現のための行動計画<sup>(\*22)</sup>は、刑法犯の認知件数の増加等の治安水準の悪化と体感治安の悪化による国民の不安感の増大を背景として、「国民が自らの安全を確保するための活動の支援」、「犯罪の生じにくい社会環境の整備」、「水際対策を始めとした各種犯罪対策」の3つの視点から、「世界一安全な国、日本」の復活を目指し、内閣に設置された犯罪対策閣僚会議において、平成15年12月に策定したものである。

前述の3つの視点を前提として、同行動計画では、現下の犯罪情勢の特徴的傾向に即した5つの重点課題、「平穏な暮らしを脅かす身近な犯罪の抑止」

---

(\*21) 全文については、巻末参考資料及び警察庁ホームページ（<http://www.npa.go.jp/>）に掲載している。

(\*22) 全文については、巻末参考資料及び首相官邸ホームページ（<http://www.kantei.go.jp/>）に掲載している。

「社会全体で取り組む少年犯罪の抑止」、「国境を越える脅威への対応」、「組織犯罪等からの経済、社会の防護」、「治安回復のための基盤整備」を設定しており、このうち、「組織犯罪等からの経済、社会の防護」の中で、サイバー犯罪対策の推進を施策の一つとして取り上げ、具体的には、次の6つの施策を掲げている。

第1に挙げているのは、情報セキュリティに関する知識及び対策の普及啓発であり、セミナーの開催やホームページの充実、相談窓口の設置等を通じて国民や事業者等の情報セキュリティ対策に関する意識を向上させ、サイバー犯罪による被害発生の防止に必要な知識及び対策の普及を図ることとしている。

第2は、インターネット上の防犯技術の開発・普及であり、不正アクセス行為により他人になりすましてインターネット・オークションで詐欺を行うなどの事案が多発していることを踏まえ、官民連携の下、低コストで利用できるより高度な本人確認技術その他の防犯技術の開発を行い、その普及を図ることとしている。

第3は、情報通信ネットワーク等の安全性及び信頼性の確保であり、産学官の連携の下、サイバー攻撃の予防、検知、分析等に関する技術、認証技術、暗号技術等に関する総合的な研究開発を推進するとともに、コンピュータ・ウイルスや不正アクセスに対する情報システム・IT製品の脆弱性を低減させるための技術開発等を実施し、情報通信ネットワーク等の安全性及び信頼性を向上させることとしている。

第4には、重要インフラを標的としたサイバー攻撃への的確な対応を挙げ、国民生活を支える重要インフラを標的としたサイバー攻撃に的確に対処するため、こうしたサイバー攻撃に関する情報収集・分析能力を向上させるとともに、関係する公益事業者、公共交通機関、金融機関、行政機関等との連携及び連絡体制を強化するほか、サイバー攻撃からの重要インフラ防護に関する国際的な協力体制を拡充することとしている。

第5としては、サイバー犯罪の徹底検挙と捜査の高度化を掲げ、サイバー犯罪の捜査に携わる警察職員の技能水準の向上や警察組織の見直し、体制の強化を図るとともに、捜査に用いられる装備資機材を最新のIT技術を駆使した犯行にも対応可能なものとすることにより、複雑・高度化するサイバー犯罪を徹底検挙するほか、先進各国の捜査技術、証拠化手法、技術基準等を参考にしながら、サイバー犯罪捜査の高度化を推進することとしている。

最後に第6として、サイバー犯罪条約の早期締結及び関連刑事法の整備を取り上げており、世界的に形成されたコンピュータ・ネットワークを利用して敢行される犯罪等のサイバー犯罪に的確に対処するとともに、サイバー犯罪条約を早期に締結し、国際間協力の下にサイバー犯罪の防圧を図るため、コンピュータ・ウイルスの作成・供用等の罪の新設、わいせつ物頒布罪の構成要件の拡

充、電磁的記録に係る記録媒体に関する証拠の収集、電磁的記録の没収等に関する国内法の整備を行うこととしている。

このほか、情報セキュリティに関連する施策としては、「少年の非行防止につながる健やかな育成への取組み」の中で、インターネット上の有害コンテンツ対策の推進を挙げており、出会い系サイト対策の推進、民間事業者が主体となった「コンテンツ安心マーク」(仮称)制度の創設に関する検討・協力、携帯電話・PHS 端末向けフィルタリング機能<sup>(\*23)</sup>の実現、少年の情報活用能力(メディアリテラシー)等の育成、少年及び保護者に対する各種啓発活動の推進等により、少年をインターネット上の有害なコンテンツから保護することとしているほか、少年及び保護者に対する相談活動の強化として、各種行政機関、民間ボランティアによる相談活動に、インターネット等を活用するなどとしている。

また、「薬物乱用、銃器犯罪のない社会の実現」の中では、インターネットの利用等薬物の密売手口の巧妙化に適切に対処するための対策を講じること、いわゆる脱法ドラッグについてインターネットの広告監視等を実施すること及び社会への銃器拡散を防止するためインターネット上の銃器取引に関する情報の収集及び取締りを推進することを取り上げている。

---

(\*23) ユーザーによる有害なコンテンツの閲覧を禁止する機能。

## 政策大系

警察としては、「背景」で述べた情報セキュリティをめぐる諸情勢を踏まえ、高度情報通信ネットワーク社会の治安維持に向けた警察活動の核たる「サイバー犯罪の取締り等の推進」、「サイバーテロ対策の推進」に加え、「高度情報通信ネットワーク社会における情報セキュリティの向上」を重点項目とし、以下の施策を迅速かつ重点的に実施することとする。

### 1 サイバー犯罪の取締り等の推進

#### (1) 体制の整備

##### 警察庁における体制の強化

サイバー犯罪は、匿名性が高い、こん跡が残りにくい、不特定多数の者に被害が及びやすい、地理的・時間的制約が少ないなどの特性があり、県境・国境もないことから、複数の都道府県警察や複数の部門にわたって取締りの重複が生じるという問題がある。

そこで、前項で触れた緊急治安対策プログラムにもあるとおり、サイバー犯罪の予防及び捜査を一体化してサイバー犯罪対策を強化するため、警察庁では、平成16年4月、生活安全局に情報技術犯罪対策課を設置し、同課において都道府県警察による取締りの調整を行うほか、産業界等や諸外国との連携強化等を推進している。

また、高度化・複雑化するサイバー犯罪に対応するには、高度な技術的知見が必要とされるため、同じく平成16年4月に、都道府県（方面）情報通信部に情報技術解析課を設置し、サイバー犯罪捜査を技術的に支援する全国的な体制を整備したところである。あわせて、都道府県警察のサイバー犯罪の取締りに対して、一定水準以上の技術的な支援を継続して提供するためには、それらの体制の下支えとなる職員らの技術力の向上が欠かせないことから、引き続き人的基盤の維持、強化に努めることとする。

##### 都道府県警察における体制整備

各都道府県警察においても、サイバー犯罪捜査を効率的に進めるため、警察部内の各部門が連携し、サイバー犯罪に関する知識及び技能を有する者により構成するサイバー犯罪対策プロジェクトを設置して、サイバー犯罪対策の強化を図っているところである。また、企業等におけるコンピュータ関連の専門職等情報技術に精通した者をサイバー犯罪捜査官として中途採用しているほか、サイバー犯罪捜査の防止のための広報啓発等を行う情報セキュリティ・アドバイザーを配置している。

しかし、情報技術の進歩は非常に速く、これを利用した犯罪も、次々に新しい手口が出現することから、今後もこうした特別な採用を推進するとともに、サイバー犯罪の取締り等に従事する全国の警察職員に対し、新し

い情報技術及びサイバー犯罪の手口等に関する知識を習得させるための教育訓練を行い、人材育成を図る。

#### サイバー犯罪捜査のための資機材の充実・強化

最新の技術を利用した犯罪や新しい手口を用いたサイバー犯罪に的確に対応するため、サイバー犯罪捜査等に必要となる資機材の充実・強化を図る。

不正アクセス事犯への対応能力を強化するため、既存の専用資機材の性能を向上させるほか、インターネットのセキュリティサイト等で公開されている情報から不正アクセスに悪用されるおそれのあるツール及び不正アクセス等の原因となるセキュリティ・ホール等の情報を検索・収集し、その対処策を蓄積するためのデータベースの機能強化を図る。

また、現場活動用に、大容量化・多様化する電磁的記録媒体に対応した各種記録媒体の複製機、リモートストレージ<sup>(\*24)</sup>に蔵置されている電磁的記録を差し押えるために必要となる解析装置等の充実・強化を図る。特に、都道府県（方面）情報通信部情報技術解析課が第一線の活動において必要とする資機材の整備を進める。

さらに、サイバー攻撃手法の手口を解明するため、各種サーバや OS、アプリケーションソフト、無線 LAN など、疑似インターネット環境を整備するほか、インターネット上に日々流通する、ネットワークセキュリティ関連情報、コンピュータ・ウイルス関連情報等に関するニュースソースを自動的かつ網羅的に集約し、それらの中からサイバー犯罪対策等に有用な情報を抽出・分析するためのシステムの能力強化を図る。

## (2) 取締りの強化

### 不正アクセス事犯の取締りの推進

不正アクセス事犯に関しては、ソフトウェアの安全上の欠陥（セキュリティ・ホール）を突いたサイバー攻撃による事犯、財産・個人情報・企業機密情報の窃取を狙う犯罪等、悪質な事犯に重点を置いて取締りの強化を図る。

### 児童買春・児童ポルノ事犯等の取締りの推進

インターネットを利用した児童ポルノ事犯等に対し、児童ポルノ画像自動検索システム（CPASS：Child-Pornography Automatic Searching System）<sup>(\*25)</sup>の運用による取締りを推進する。

また、出会い系サイトを利用した児童買春事犯を取り締まるとともに、

---

(\*24) 本大系では、搜索差押現場のパーソナルコンピュータ等とネットワークにより接続され、別の場所に設置された外部記憶装置を指す。

(\*25) インターネット上に存在する児童ポルノ画像を自動的に検索するシステム。

出会い系サイト規制法の適正な運用により、児童による出会い系サイトの利用及び犯罪被害を防止する。

#### 薬物・銃器密売事犯の取締りの推進

インターネットを利用した密売事犯については、インターネット上の薬物・銃器取引についての早期情報収集を一層強化するとともに、捜査手法の確立に努めるほか、広域にわたる捜査に備えて都道府県警察間の連絡体制を強化する。

また、既存の情報提供窓口を活用して情報を収集するほか、インターネット利用者からも幅広く情報提供を求めていく。

#### その他インターネットを利用した各種事犯の取締りの推進

インターネットを利用した架空請求事犯、インターネット・オークションやホームページ等を利用した、知的財産権侵害事犯、詐欺事犯、わいせつ物頒布等事犯等の各種事犯の取締りに当たっては、事犯が広域性を有するおそれが高いため、必要に応じて、警察庁において指導調整を実施し、捜査の競合を排除するほか、共同・合同捜査の実施等により、迅速かつ的確な取締りを推進する。

#### サイバーパトロールの強化

サイバーパトロール活動を強化し、インターネット上の薬物・銃器の取引、わいせつ物等の禁制品等に関する情報、詐欺・悪質商法・児童買春等に関する違法・有害情報を把握して、その取締りや関係者に対する指導、連絡、要請等の適宜の措置を講ずる。

### (3) 外国関係機関との連携強化

#### 諸外国との連携強化

「背景」の3(3)で記述した国際的動向を踏まえ、警察庁では、G8 リヨン・グループのハイテク犯罪サブグループに係る会合や、平成12年5月(パリ)及び平成13年5月(東京)に開催されたG8ハイテク犯罪対策政府・産業界合同会合に積極的に参画してきた。今後も、サイバー犯罪に関する国際的会合に積極的に参加し、諸外国の関係機関との協調関係構築に向け、サイバー犯罪捜査における国際協力、サイバー犯罪対策の専門家の育成等を目的とした相互交流等を行う。また、第159回国会で承認されたサイバー犯罪条約の締結に向けた所管法の整備を進めるとともに、サイバー犯罪条約締結後の国際捜査協力の促進について検討する。

#### サイバー犯罪対策のための技術情報共有ネットワークの活用

警察庁では、アジア地域の法執行機関における技術情報の共有、そして技術者交流を促進するため、「サイバー犯罪技術情報ネットワークシステ

ム<sup>(\*26)</sup>」及び「アジア地域サイバー犯罪捜査技術会議」を主導しているところであるが、より実働に資する技術情報の共有を実現するため、トレーニングコースの開設及びトレーナーの選出・派遣などを含めた所要の環境の整備を図る。

## 2 サイバーテロ対策の推進

サイバーテロの脅威が現実のものとなっている現在、警察では、サイバーテロへの的確な対応に向け、「重要インフラの基幹システム<sup>(\*27)</sup>に対する電子的攻撃」及び「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」を対象事案に掲げ、各種施策を講じている。

### (1) 体制の整備

平成 16 年 4 月、警察庁において、情報技術を利用した犯罪に的確に対処するための組織改編が行われたことを受け、平素においてサイバーテロ対策を推進する警察庁サイバーテロ対策推進室の体制の見直しを行ったほか、各管区警察局に管区警察局サイバーテロ対策推進室を設置した。さらに、都道府県警察においては、サイバーテロ対策プロジェクトの体制の見直しを行うなど、全国的な体制を整備している。

また、事案発生時には、警察庁に警察庁サイバーテロ対処本部を設置するほか、関係管区警察局及び関係都道府県警察に対し、状況に応じサイバーテロ対処本部の設置を指示することとしており、迅速かつ的確な対応を可能としている。

### (2) 緊急対処能力並びに関連情報の収集及び分析能力の強化等

サイバーフォース<sup>(\*28)</sup>は、24 時間体制でインターネット上の治安情勢の把握に努めているところであるが、世界規模で感染を拡大するコンピュータ・ウイルスや DoS 攻撃などが横行するようになり、それらに対処するためには、より早期に、かつ正確に予兆を把握し、関係機関との情報共有を推進することが求められている。そこで、サイバー攻撃手法の収集・分析能力の高度化、リアルタイム検知ネットワーク<sup>(\*29)</sup>の検知センサー部の拡張などにより、緊

---

(\*26) サイバー犯罪の技術的手口やデジタル証拠の解析手法、警察庁においてモニターしているインターネット上の悪意ある活動（コンピュータ・ウイルス等）について情報共有を行うため、アジア諸国 9 か国・1 地域（日本を含む。）の法執行機関を結んだネットワークシステムのこと。

(\*27) 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス等、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情報システムをいう。

(\*28) サイバーテロ対策の技術的中核として警察庁に設置した機動的技術部隊の通称名。

(\*29) 全国の警察機関のネットワークとインターネットとの接続点に設置された不正侵入検知装置を 24 時間オンラインで監視するシステムのこと。

急対処能力の強化を図ることとする。

また、悪質・巧妙化するサイバー攻撃手法及び緊迫化する国際テロ情勢に対応するため、外国治安機関等との連携強化、国内外のサイバーテロに関する情報収集・分析能力の強化等を行う。

これらにより収集された情報及び分析結果のうち有益なものについては、「我が国におけるインターネット治安情勢」として取りまとめ、警察庁セキュリティポータルサイト( @police )<sup>(\*30)</sup>を通じて、広く国民へ公表するほか、重要インフラ事業者等に訪問するなどして注意喚起を実施する。

### (3) 人材育成・資機材の充実強化

日進月歩の情報通信技術を悪用したサイバー攻撃に適切に対処していくためには、高度な専門知識を備えた人材の育成が必要不可欠である。それら技術を習得させるため、以下に挙げる教育・訓練及びそのための環境の整備を進める。

また、サイバーテロ事案発生 of 未然防止及び発生した際の的確な緊急対処活動それぞれに資する資機材の充実・強化を図る。あわせて、それら資機材の高度化、効率化に資する調査研究を行うこととする。

#### サイバーテロ対策要員に対する教育・訓練の実施

各都道府県警察におけるサイバーテロ対策要員の能力向上のため、サイバー攻撃及びその防御の手法並びにサイバー攻撃の有無の確認等に資する知識・技能を習得するための実習を中心とした民間委託教養を含む教育・訓練を実施する。

#### 外国治安機関における実践的訓練の実施

サイバーテロ等の対処の分野において高い技術レベルを有する米国、英国等の治安機関にサイバーテロ対策技術要員を派遣し、OJT<sup>(\*31)</sup>等実践的な訓練を実施する。

#### サイバーテロ事案に対応した資機材の整備

サイバーテロ事案捜査に用いる各種記録媒体の複製機等の資機材を整備するほか、オープンソースソフトウェア<sup>(\*32)</sup>を導入したサーバ等を標的としたサイバーテロへの緊急対処用資機材の充実・強化を図る。

#### サイバーテロ対策に資する調査・研究

サイバーテロに用いられる手法、その防御策等について、調査・研究を行うための環境整備を行う。また、リアルタイム検知ネットワークシステムのデータ収集機能及び分析機能の高度化を図るための調査・研究を実施

---

(\*30) ホームページアドレスは、<http://www.cyberpolice.go.jp/>である。

(\*31) On the Job Training の略。仕事の現場で、業務に必要な知識や技術を習得する実地研修。

(\*32) ソースコードが公開されているコンピュータ基本ソフト( OS )のこと。

する。

#### (4) 重要インフラ事業者等との連携強化

都道府県警察のサイバーテロ対策プロジェクト及びサイバーフォースは、重要インフラ事業者等への訪問を通じて、警察との連携窓口の設置及び緊急時の連絡に係る要請等を行いつつ緊密な協力関係の醸成に努めるとともに、その枠組みを拡大していく。

また、警察庁において収集・分析した各種技術情報の提供、脆弱性試験の実施及び警察と重要インフラ事業者等との情報共有のためのメーリングリストの開設など、官民一体となったサイバーテロ対策を実現するための各種施策を推進する。

これら施策の実効を図り連携を深める場として、サイバーテロ対策協議会を適切に運営するとともに、重要インフラ事業者等を対象とした情報セキュリティ技術セミナーを積極的に実施する。

#### (5) 外国関係機関との連携強化

G8 の司法・内務閣僚会合等において、重要情報インフラ防護が議題の一つに挙げられ、国際的な連携強化や政府と民間部門の情報共有が重要な課題とされている。

警察庁では、サイバーテロ対策を議論するための国際会議等へ参加することはもちろんのこと、欧米のネットワーク先進国を訪問し、技術担当者とのミーティング等を通じて、法執行機関で標準的に利用されているソフトウェアツール等の技術やサイバーテロ等の具体的な事例と最適な技術対応方策（ベストプラクティス）に係る情報共有を行う。また、技術担当者の人材育成（教育訓練等）に係る情報交換や技術情報共有のための窓口の設置等に係る調整等の活動を行うこととする。

### 3 高度情報通信ネットワーク社会における情報セキュリティの向上

安全・安心な高度情報通信ネットワーク社会の構築に資するため、警察の情報通信システムに係るセキュリティの確保を進め、また、技術の進歩に対応した警察活動のための調査研究や基盤整備への取組みのほか、産業界・関係機関等との連携を強化し、効果的な広報啓発活動等を実施することにより、社会全体の情報セキュリティの向上を図る。

#### (1) 警察の情報通信システムにおけるセキュリティの確保

警察が取り扱う情報通信システムは、それ自体が警察活動に必須な重要インフラであることから、これへのサイバー攻撃や不正アクセスによる大規模機能障害の発生等を未然に防ぐための措置を講ずる。また、警察は、捜査情報等の保秘を要する情報資産を有しているため、これらの情報資産の保護及び適切な取扱いに向けた施策を推進する。

なお、これらの施策を通じて得られた知識・技術等については、民間への情報提供や政府全体の取組みの際に積極的に活用する。

#### セキュリティ水準の高い情報通信システムの整備

警察では、警察庁から各都道府県警察本部、警察署、パトカー、第一線の警察官にまで及ぶ全国的な情報通信ネットワークを構築し、24時間間断無く行われる警察活動に必要な情報を伝達している。このため、最新の暗号技術の導入や暗号の運用方法の改善による機密性の飛躍的な改善と利便性向上、さらに可用性を大幅に向上させた新たな警察移動通信システムの全国整備を進める。

#### 情報セキュリティ監査の活用

警察情報システムに情報セキュリティ監査を実施することにより、警察庁及び都道府県警察の情報セキュリティの実態を把握し、その結果に基づきセキュリティ対策の評価・指導を行うことにより警察全体のセキュリティレベルの向上を図る。

#### システムに対する脆弱性試験の実施

警察庁ホームページ等の公開サーバが外部からの攻撃に対して安全かどうか、実際に攻撃手法を試しながら安全性の検証を行う脆弱性試験を定期的実施することにより、情報セキュリティ上の問題点の詳細把握及び対策の徹底に努める。

#### システムの脆弱性に係る対応の迅速化

警察庁 WAN<sup>(\*33)</sup>システム及び霞ヶ関 WAN 用 LAN<sup>(\*34)</sup>システムの端末について、プログラムの脆弱性が発見されてから修正プログラムが適用されるまでの期間を最小化するとともに、確実にすべての端末に当該プログラムを適用するために、修正プログラムを自動適用するシステム等を導入する。

#### コンピュータ・ウイルス対策の強化

警察庁 WAN システムにおけるコンピュータ・ウイルス対策について、すべての端末を一元的に管理・監視するためのシステムを導入し、コンピュータ・ウイルスによる被害の未然防止を図る。

#### 障害発生時の対応についての検討

情報処理センターの機能に支障が生じた場合を想定し、緊急時の対応方策、バックアップの確保方策に係る調査検討を実施するとともに、その検討結果について、同センターに勤務する職員に周知徹底する。

#### 情報セキュリティに関する教養の推進

---

(\*33) 警察庁の職員間でやり取りされる電子メール、電子掲示板等に利用されている。

(\*34) インターネット及び霞ヶ関 WAN に接続され、電子メールの送受信、ホームページの提供・閲覧等に利用されている。

警察情報セキュリティポリシーが正しく理解され、これが確実に実施されるようにするため、警察情報システムを運用・管理する職員のみならず、すべての職員に対し、同ポリシーに関する知識の普及及び啓発に努める。

## (2) 高度情報通信ネットワーク社会における警察の基盤の確立に向けた取組み

サイバー犯罪捜査やサイバーテロ対策に限らず、あらゆる警察活動において情報通信技術に係る高度な知見が必要となっている。そこで、以下のとおり最先端の情報通信技術に係る調査研究を行い、警察活動に資する技術の高度化、体系化を図るとともに、統一的な技術基準の策定など全国警察を支える基盤技術の醸成に努める。

また、高度情報通信ネットワーク社会での的確な警察活動を確保するため、必要となる基盤整備に積極的に取り組むこととする。

### 情報技術解析に関する研究

電磁的記録の解析等のための手順や捜査現場におけるコンピュータの取扱いなどを定めた標準的な作業要領及び使用するツール等の統一化を図るため、コンピュータ・フォレンジック<sup>(\*35)</sup>に関する調査研究を行う。また、当該作業要領及びツール等の取扱いに係る技術を全国で共有するとともに、作業に携わる警察職員の能力向上のための教育訓練を実施する。

### 緊急対処活動に関する研究

サイバーテロの未然防止・被害拡大防止のための緊急対処活動（インシデント・レスポンス）の高度化を図るため、海外の技術動向調査やリアルタイム検知技術、防御技術等に係る調査研究を行う。

### IP 電話対応 110 番通報受理システムに必要な技術に関する研究

普及が進む IP 電話からの 110 番通報を直接受理する際に必要となる技術の調査研究を行うとともに、サイバー攻撃等の IP 電話網特有の脅威に対応した 110 番通報受理システムのセキュリティ対策について、モデルシステムを用いて検討する。

## (3) 産業界・関係機関等との連携強化

### 総合セキュリティ対策会議の開催

警察庁において、官民の協調による情報セキュリティの確保に努めるため、情報セキュリティに関する有識者らで構成する「総合セキュリティ対策会議」を開催し、産業界等と政府機関との連携の在り方、特に警察との連携の在り方について検討を行う。

### プロバイダ等連絡協議会の設置・活用

都道府県警察において、官民一体となって情報セキュリティ対策を推進するため、プロバイダ等の企業や行政機関等により構成するプロバイダ等

---

(\*35) 計算機科学等を利用して、デジタルの世界の証拠性を確保し、法的問題の解決を図る手段。

連絡協議会を設置し、具体的な取締りの過程で発生した問題点等を踏まえて、サイバー犯罪情勢や犯罪手口等の犯罪実態に係る情報を提供するとともに意見交換を行う。

#### 学校等教育機関との連携

インターネットを利用する少年が増加し、少年がサイバー犯罪の被害者又は加害者となる事案やインターネットにまつわるトラブルも発生していることから、少年がサイバー犯罪に巻き込まれないよう、また、出会い系サイトへの違法な書込み等インターネットを利用した違法行為を行うことがないよう、少年の情報セキュリティ意識の向上を図るため、学校等教育機関を積極的に訪問して講習会等を実施するなど、学校等教育機関と連携した広報啓発を実施する。

#### インターネット・オークション事業者等に対する指導

「古物営業法の一部を改正する法律」が平成15年9月1日から施行されたことに伴い、インターネットを利用した無許可古物営業の排除を図るほか、インターネット・オークションを利用した盗品等の処分を防止することにより、犯罪の防止と被害の回復を図る。

### (4) 広報啓発の推進

#### 国民の情報セキュリティ意識の向上

情報セキュリティコミュニティセンター<sup>(\*)36)</sup>及び警察庁セキュリティポータルサイト (@police) 等を活用し、国民がサイバー犯罪の被害に遭わないよう、犯罪の最新の手口を踏まえた情報提供を実施するとともに、各種研修会等を実施するなど、広報資料や様々なメディアを活用した広報啓発活動を推進し、国民の情報セキュリティ意識の向上に努める。特に、迅速な情報提供を行うため、インターネット等を通じた広報啓発活動を強化する。

また、インターネット上の違法・有害情報から少年を保護するため、出会い系サイト等少年に有害な情報の危険性に関する広報啓発やフィルタリングシステムを普及させるための広報啓発活動を行う。

#### サイバー犯罪に関する相談への適切な対応の推進

ホームページ等によりサイバー犯罪に関する相談窓口を広報するとともに、各種相談機関との連携を保ち、相談者の立場に立った適切な対応に努める。また、相談業務を通じて把握した新たな手口等については、その対策等を広報するなどして被害の拡大防止に努める。

#### インターネットカフェ等を利用したサイバー犯罪等の防止

---

(\*)36) 警察からサイバー犯罪の予防のための助言・指導を行い、自主的な情報セキュリティ対策を促すための情報提供の場のこと。

インターネットカフェ、フリースポット<sup>(\*37)</sup>、公共施設等の不特定多数の者が利用できるインターネット環境におけるネットワークセキュリティを始めとした防犯対策の実施状況等の把握に努め、管理者及び利用者に対し、こうした環境がサイバー犯罪に利用されないよう広報啓発を実施する。

---

(\*37) 本大系においては、不特定多数の者が接続できる無線 LAN のアクセスポイントをいう。



## 参考資料一覧

- 1 **重要インフラのサイバーテロ対策に係る行動計画**  
(平成12年12月、情報セキュリティ対策推進会議)
- 2 **緊急治安対策プログラム**  
(平成15年8月、警察庁)
- 3 **犯罪に強い社会の実現のための行動計画**  
(平成15年12月、犯罪対策閣僚会議)
- 4 **サイバー犯罪に関する条約**