

「警察庁情報セキュリティ重点施策プログラム-2005」

第1 背景

1 警察庁におけるこれまでの取組み

我が国においては、平成 13 年 1 月に高度情報通信ネットワーク社会推進戦略本部（以下「IT 戦略本部」という）において決定された「e-Japan 戦略」、「e-Japan 戦略」等により、「2005 年までに世界最先端の IT 国家となる」との目標を掲げ、官民一体となって IT 施策を推進してきた。その結果、情報通信ネットワークが、国民生活から社会・経済活動に至るまで必要不可欠なインフラとなり、国民がその恩恵を享受することとなった。

他方、こうした社会の IT 化は、国民の利便性を向上させる反面で、サイバー犯罪やサイバーテロといった新たな脅威を顕在化させ、国民生活や社会・経済活動に大きな被害を生じさせている。警察庁では、平成 12 年 2 月に「警察庁情報セキュリティ政策大系」を策定するなど、情報セキュリティ対策につき先駆的に取り組んできたところであるが、サイバー犯罪の増加・多様化及びサイバーテロの脅威の顕在化といった現状から、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に「警察庁情報セキュリティ政策大系-2004」を平成 16 年 8 月に策定したところである。

2 政府における情報セキュリティ対策の強化

サイバー犯罪やサイバーテロに係る脅威の増大を踏まえ、平成 16 年 7 月、IT 戦略本部情報セキュリティ専門調査会の下に「情報セキュリティ基本問題委員会」を新たに設置して、政府及び重要インフラにおける情報セキュリティ対策に係る検討を行った。

ここでの検討結果を踏まえ策定された「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（平成 16 年 12 月 7 日付け IT 戦略本部決定）では、情報セキュリティの問題への政府の取組みの不足が、国民の生命・財産の損失につながりかねないリスクを増大させているとして、政府として早急に抜本的な対策に着手すべきとしている。

当該IT戦略本部決定では、我が国における情報セキュリティ政策に関する基本戦略及び各府省庁の情報セキュリティを確保するための安全基準の策定・推進等の機能強化を図るために、IT戦略本部の下に「情報セキュリティ政策会議」^{*1}を置くほか、当該基本戦略の立案、各省庁の情報セキュリティ対策促進及び各省庁の事案対処支援のための統一的・横断的な総合調整機能を強化するために、内閣官房に「情報セキュリティセンター」^{*2}を置くこととされている。

その後策定された「IT政策パッケージ2005」(平成17年2月24日付けIT戦略本部決定)では、e-Japan戦略の目標の年である2005年を迎えた後も、引き続き世界最先端であり続けるための取組みを行っていく必要があるとし、従来からのサイバー犯罪・サイバーテロ対策の推進に加え、ITがもたらす新たな社会問題を克服するため、フィッシング及び迷惑メール対策等の強化を進めていくこととされている。

また、違法・有害情報がもたらす新たな社会問題への対応も課題となっており、内閣官房において「インターネット上における違法・有害情報等対策関係府省局長級会議」が開催されるなど、これに対する取組みが強化されている。

IT社会において安全で安心して暮らせる社会を実現するためには、現実社会とサイバー空間における安全が総合的に確保されることが重要である。「世界一安全な国、日本」の復活を目指し策定された「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決定)においても、サイバー犯罪対策が治安回復のために取り組むべき重要施策の一つとして取り上げられている。今後、情報セキュリティ政策会議においては、情報セキュリティに関する我が国の中長期の基本戦略(「第一次情報セキュリティ基本計画(仮称)」)を策定することとしており、警察庁としても、現実社会とサイバー空間における「安全・安心」が総合的に確保されるよう、内閣官房、関係省庁等と緊密に連携しつつ、警察庁の有する組織力、技術力を最大限に活用して、情報セキュリティに関する取組みを推進し、サイバー空間に関しても「世界一安全な国、

*1 平成17年5月30日に設置。

*2 平成17年4月25日に設置。

日本」の実現に努めることが重要である。

3 警察における情報セキュリティに係る取組みの強化

前記の「警察庁情報セキュリティ政策大系-2004」において、警察として中長期的に取り組むべき情報セキュリティ対策の方向性を示したところであるが、昨今の犯罪情勢等から、当面重点的に取り組むべき項目を選定し、及びこれらを推進するための具体的方策等を定める必要がある。さらに、政府としての情報セキュリティ対策を推進する体制が整備されたことに伴い、内閣官房や他省庁、重要インフラ事業者等と協調して、これを支えていくことが求められている。

そこで、「情報セキュリティ政策大系-2004」を踏まえつつ、引き続き「国民が安心して暮らせる安全な社会の確立」を目指し、「警察庁情報セキュリティ重点施策プログラム-2005」を策定し、警察庁として当面、具体的に取り組むべき重点施策及びその内容を次のとおり定めることとしたものである。

第2 重点施策

1 情報セキュリティ対策の推進体制の整備

(1) 情報セキュリティ政策機能の強化

サイバー空間上の治安情勢を的確に把握し、また、中長期的な視点から情報セキュリティ対策に関する戦略を策定する部門を明確化する。

(2) 情報セキュリティに関する教養体系の見直し

情報セキュリティ対策に必要な技術力の醸成に資する体制等を整備するとともに、国際的に通用する情報セキュリティに関する資格の適用も視野に入れ、部内の情報セキュリティに関する技術レベルの評価手法等の導入に努める。

2 サイバー犯罪の根絶に向けた取組みの強化

(1) サイバー犯罪対策のための捜査体制等の充実・強化

広域性を有するサイバー犯罪に対し、より効率的な合同・共同捜査等を推進するため、警察庁及び管区警察の調整能力の強化を図る。また、都道府県警察における体制の充実を図る。

(2) 不特定多数の者を対象とするサイバー犯罪への対策の強化

フィッシングや架空・不当請求メール、不正プログラム等、多数の国民に被害を及ぼすおそれのあるサイバー犯罪に対する取締りを強化し、同種事犯の発生を抑止を推進する。

(3) インターネット上の違法・有害情報対策の推進

児童ポルノ等の違法・有害情報に対するサイバーパトロール等の強化及び海外治安機関等との情報共有を推進し、把握した情報については、適宜、プロバイダ等の関係者に対する指導・連絡・要請等の措置を講じるとともに、その取締りを強化する。

(4) 電磁的記録の解析能力の強化

最新の情報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、電磁的記録の解析業務を担う体制及び資機材の充実・

強化を図る。また、今次の刑法・刑訴法改正^{*3}により創設される新たな手続について、解析手順及び使用するツール等の検証・評価を行い、国際捜査共助等の場面でも通用する手法を確立する。

(5) コンピュータ・フォレンジック^{*4}に係る取組みの強化

電磁的記録の解析手順や捜査現場におけるコンピュータの取扱手法等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始めとして、コンピュータ・フォレンジックに係る研究を行い、警察活動に支障のない範囲で、当該技術の民間への移転を進める。

3 サイバーテロ対策の抜本的強化

(1) 緊急対処能力の強化

全国の政府機関、自治体を含めた重要インフラ事業者と緊密に連携したサイバーテロ対策を実施するため、警察庁における予防及び初動対応に係る体制の抜本的な強化を図る。また、重要インフラ事業者を対象とした「サイバーテロ対策協議会」やプロバイダ等の通信事業者を対象とした「プロバイダ等連絡協議会」等都道府県警察における民間事業者との連携の枠組み拡大に向けた取組みを強化する。

(2) サイバー攻撃の予兆把握の機能強化

サイバー攻撃の予兆を、早期かつ正確に把握するため、リアルタイム検知ネットワークの機能及び運用体制を強化する。また、重要インフラ事業者及び同様の観測体制を有する他の機関との連携を図り、高精度な予兆把握を可能とする手法を検討する。

(3) 安全・安心ホームページ制度

サイバーテロの攻撃の対象となる可能性のある重要インフラ事業者等の開設するホームページ等を重点的に監視し、各種の攻撃が警察において検知された場合には、連絡窓口を通じ、電子メール等を利用して速やかに管

*3 「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）」において、コンピュータ・ウイルスの作成、供用等の罪の新設等[刑法]、電磁的記録に係る記録媒体に関する証拠収集手続の整備等[刑訴法]が新たに規定される。刑法は公布後二十日、刑訴法は1年以内の政令で定める日をもって施行。

*4 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

理者に対して状況を通報する「安全・安心ホームページ制度」を確立する。

また、対策を実施する上で必要となる技術情報等を集約した支援ツール（再発防止及び攻撃の痕跡の保全に有効なソフトウェア等）の研究開発を進め、重要インフラ事業者等における利用を促進する。

4 官民一体となった安全・安心への取組みの強化

(1) 民間における情報セキュリティ活動支援

警察部内の資格制度（前記第1(2)を参照）については、その制度を導入する過程で蓄積された各種のノウハウを民間とも共有し、民間における情報セキュリティ技術の向上を促進する。また、民間への技術移転も視野に入れ、市販の情報セキュリティ機器を警察独自の視点から評価・認定する制度や手法について検討を行う。

(2) 民間有識者との交流の枠組みの拡大

ア 技術者の交流促進

治安維持に資する技術的な課題を議論するため、民間有識者と警察の技術者らで構成する研究会等を設置する。また、大学の研究室等、最先端の研究を実施している部門に職員を派遣し、共同研究を進めるなど、技術者の交流を促進する。

イ 民間の有識者との議論の場の拡大

情報セキュリティ政策に関する将来的な課題について、官民の双方の立場から自由に議論できる場を設定する。

(3) 関係機関との連携強化

インターネット・カフェ等の匿名性の高い利用環境に対する防犯対策、インターネット・オークション等における知的財産権侵害事犯の取締り、違法なインターネット異性紹介事業者の取締り、児童ポルノ等のインターネット上の違法・有害情報対策、インターネット上での自殺予告・殺害予告事案等への対応を推進するため、プロバイダを始めとする関係業界との連携の枠組みを確立するなど、協力関係を醸成する。

(4) 教育機関等との連携強化

学校等の教育機関と連携し、学校教育の中で子供が情報セキュリティに

ついて学ぶ機会を提供する。また、学校、保護者等による地域社会における取組みの活性化を支援する。

(5) 広報啓発・相談活動の推進

サイバー犯罪等に係る国民からの相談に適切に対応するため、ホームページ等を積極的に活用した情報提供の枠組みを確立する。また、都道府県警察のセキュリティ・アドバイザーを拡充し、国民に対する広報啓発の取組みを推進する。

5 国際連携の強化

(1) 国際会議等の枠組みの拡大

G 8 等の国際的な枠組みにおいて、我が国から情報セキュリティに係る新たな議題及びそれを検討する場の設置を提案する。また、我が国が主催する国際会議への参加国を増やし、日本を中心とした情報共有の枠組みの拡大を図る。

(2) 人事交流の促進

ア 関係国への職員派遣の推進等

欧米のIT先進国に職員を長期に派遣し、当該国との連携強化を図るとともに、事案対処等を速やかに行える枠組みの確立を図る。

イ 海外治安機関からの職員の受入れの推進

情報セキュリティ対策に関する高度な知見を有する海外治安機関からの職員を受け入れ、技術の共有等を行う。

(3) 技術基盤の醸成

ICPO等との連携を視野に入れつつ、我が国のサイバー犯罪捜査技術等を海外治安機関と共有するための研修プログラムを策定する。