ISSUE BRIEF

情報セキュリティの現状と課題

国立国会図書館 ISSUE BRIEF NUMBER 443 (Mar.10,2004)

経済産業課

（横内（よこうち） 律子（りつこ））

調査と情報

第 443 号

はじめに

現在、わが国では、ブロードバンドの整備・普及が目覚しく、政府や企業においても IT 化が急速に進んでいる。こうした中で重要性を増しているのが、情報セキュリティの問題である。今後、電子政府の構築、電子商取引の活発化等、社会の IT 化が更に進めば、ウイルス等の情報セキュリティへの脅威がもたらす影響は、一層強まるものと考えられる。そこで、その対策としては、高度で幅広い対応が求められている。

本稿は、こうした状況に鑑み、わが国の情報セキュリティの現状についてまとめたものである。まず、情報セキュリティとは何かを整理した上で、我が国における情報セキュリティへの脅威の現状と現在のセキュリティ対策について述べ､最後に今後の課題を挙げた。

なお、情報セキュリティ関連の組織名や用語等は、通常アルファベットの略称で表記される場合が多い。本稿でも正式名称は初出のみ併記しているが、一見しただけでは分かりにくい場合もあるため、文中の略称とその正式名称を巻末に一括して挙げた。適宜参照していただきたい。

Ⅰ 情報セキュリティとは

情報セキュリティとは、データや情報システム等を、正当な利用者のみが必要な時に利用できるよう、正確で完全な状態に保つことである[1]。この情報セキュリティを脅かす主な原因を、表 1 にまとめた。まず、外部からの脅威として、不正アクセス、サービス妨害、コンピュータ・ウイルス等がある。これに加えて、ソフトウェアのセキュリティ上の脆弱性等、被害者側に内在する要因もある。

近年、情報セキュリティに対する脅威として「サイバー攻撃」「サイバーテロ」という言葉もしばしば使われる。「サイバー攻撃」という用語は、一般に、不正アクセスやサービス妨害、コンピュータ・ウイルス等の、情報システムやネットワークを使った電子的な攻撃が、特に政治的な意図を持って行われた場合に用いられることが多い。

「サイバーテロ」についても、現時点で明確な定義はない[2]。一般に、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス[3]といった「国家又は社会の重要な基盤」に対して不正アクセスやサービス妨害等を行い、国民生活や社会経済に深刻な被害を与える行為を「サイバーテロ」と呼ぶ。サイバーテロの特徴は、①地理的・時間的制約がない、②専門的技術者さえいれば十分で、攻撃のコストが低い、③匿名性・無痕跡性があり、罰則等による抑止が困難である、④経済・社会に多大な影響を与える、等である[4]。

---

[1]「OECD(経済協力開発機構）情報セキュリティのためのガイドライン」（1992）では、「情報の機密性（Confidentiality)、完全性（Integrity）及び可用性（Availability）を保護すること」と定義されている。

[2] 警察庁「情報セキュリティ政策大系」2000.2. ＜http://www.npa.go.jp/hightech/sec_taikei/taikei.htm＞では、「コンピュータ・ネットワークを通じて各国の国防、治安等をはじめとする各種分野のコンピュータ・システムに侵入し、データを破壊、改ざんする等の手段で国家又は社会の重要な基盤を機能不全に陥れるテロ行為」と述べられている。どのような程度・性質の攻撃を言うのか等はいまだ明確に定まっていない。

[3] 情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」2000.12. ＜http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/1215actionplan.html＞では、当面これらの分野を重要インフラとすることが述べられている。

[4] 警察庁技術対策課「サイバー犯罪の現状と課題」2002.12.19.

表１：情報セキュリティへの脅威

	名称	定義・内容	引き起こされる被害の例	特徴
外部からの加害	不正アクセス	システム利用者が、与えられた権限によって許されていない行為を、ネットワークを通じて意図的に行うこと。	なりすまし、改ざん、盗聴、破壊、不正プログラムの埋め込み	他のコンピュータからのリアルタイムの攻撃であること。
	サービス妨害	外部からサーバへの攻撃	DoS 攻撃(サーバに大量のデータを送り過大な負荷をかける）によるパフォーマンスの極端な低下やサーバダウン。	
	ウイルス（広義）	他者のプログラムやデータベースに意図的に被害を及ぼすように作られたプログラムで、①自己伝染、②潜伏、③発病機能のうち、1つ以上を持つもの	情報の消失、改ざん、漏洩、パソコンの操作不能、起動不能	
	ウイルス（狭義）	①～③の機能をすべて持つ。		
	ワーム	②～③の機能を持つ。プログラム等の媒体に寄生せず、単独で増殖する。		
	トロイの木馬	②～③の機能を持つ。寄生・増殖せず、有用なプログラムを装い裏で被害を起こす。		
内在する要因	セキュリティホール	ソフトウェアのセキュリティ上の問題点（脆弱性）等	メールソフトの脆弱性を突いたウイルス攻撃	攻撃対象とされることで、被害の原因となる。
	セキュリティ概念・モラルの欠如		情報漏洩	

（出典）IPA/ISEC「情報セキュリティ読本」2002.6.
＜http://www.ipa.go.jp/security/awareness/management/dokuhon.pdf＞ などをもとに作成。

II わが国の情報セキュリティ侵害の状況

1 発生状況（届け出ベース）

●コンピュータ・ウイルス

情報処理推進機構[5]セキュリティセンター（IPA/ISEC）によると、コンピュータ・ウイルスの発見・届出件数は、90 年代を通じて増加傾向にあったが、平成 13 年の 24,261 件をピークに減少に転じている。また、発見・届出件数のうち実際に感染被害があった割合も、年々減少している。これは、ワクチンソフトの導入等、セキュリティに関する意識の向上が見られるためとされている[6]。企業・自治体の状況をみると、平成 14 年に一度でもウイルスに感染した割合は 35.4%であり、発見のみのケースを含めた遭遇率は 80.2% に

[5] 経済産業省の関係機関。平成 16 年 1 月、独立行政法人へ移行した。
[6] 情報処理推進機構セキュリティセンター（IPA/ISEC）「2003 年ウイルス届出状況」2004.1.8.
＜http://www.ipa.go.jp/security/txt/2004/2003-all-virus.pdf＞

上る[7]。企業におけるウイルスの被害総額は、約 3,027 億円[8]とも約 4,400 億円[9]とも推計されている。また、個人のインターネット利用者の被害総額は約 384 億円[10]とみられている。

ウイルスは不特定多数を標的とするため、件数・被害額が多大になる傾向がある。ウイルスの攻撃手段は近年、多様化・高度化しており、メール機能を悪用し感染を広げるもの、ソフトウェアのセキュリティ上の欠陥を悪用して感染させるものが目立っている。また、ウイルスが、不正アクセスやサービス妨害の手段として使われるようになってきている点も近年の傾向である。

●不正アクセス

警察活動[11]及び警察への届け出等による不正アクセスの認知（不正アクセス行為の事実が確認された）件数、及び関係団体（IPA/ ISEC 及び JPCERT コーディネーションセンター（JPCERT/CC）[12]）への届け出状況をみると、いずれも平成 13 年までは増加傾向にあり、14 年は減少または横ばいとなっている。警察の 14 年の認知件数は 329 件で、13 年に比べ 924 件の大幅減となった。この原因は、13 年に多発したセキュリティホールの攻撃による不正アクセスが、修正プログラムの普及等によって激減したためとされている[13]。

2 発生状況（監視ベース）

これまでに挙げた件数は、警察又はセキュリティ関係団体への届け出等に基づく数字であり、実際の件数は更に多いと考えられる。攻撃の状況をより正確に把握するため、警察庁は、平成 14 年 7 月から、全国の警察施設のインターネット接続点 57 ヵ所に侵入検知装置を設置し、24 時間体制で特定の侵入パターンを対象にサイバー攻撃の監視を行っている。

これによる検知件数は、ほぼ 3 ヶ月につき 5 万件台で推移していたが、平成 15 年 4～6 月には、当時流行したワームの被害もあり、3 ヶ月で約 12 万件、1 日当たり約 1,300 件に達し、以後ほぼ同水準を維持している[14]。なお、攻撃内容としては、不正アクセス、サービス妨害、ウイルス等に加え、攻撃初期の準備段階も含まれており、平成 15 年 7～9 月には、ウイルス（ワーム）とポートスキャン（侵入の予備行為）が、全体の約 8 割を占めた。不正アクセスやサービス妨害を意図した本格的な攻撃は、全体の 1 割強程度と見られる[15]。

---

[7] IPA/ISEC「『国内におけるコンピュータウイルス被害状況調査』報告書」2003.3.
[8] 総務省『情報通信白書 平成 15 年版』2003,p.121.
[9] IPA/ISEC「『被害額算出モデル』報告書」2003.3.
＜http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf＞
[10] 前掲注（8）
[11] インターネット上を巡回し、違法な行為を発見するサイバーパトロールや、被疑者の取り調べ等。
[12] 経済産業省の支援を受けた民間の非営利団体。平成 15 年には、インターネット定点観測システムを導入している。
[13] 国家公安委員会・総務省・経済産業省「不正アクセス行為の発生状況」2003.2.20.
＜http://www.soumu.go.jp/s-news/2003/030220_2.html#01＞
ここでの不正アクセス件数には、ウイルス（ワーム）、サービス妨害等の一部も含まれるとみられる。
[14] 警察庁「我が国におけるインターネット治安情勢の分析について」
＜http://www.cyberpolice.go.jp/detect/index.html＞
[15] 「コンピューターへの攻撃 3 ヵ月で 5 万 8000 件」『日本経済新聞』2003.2.6,夕刊

3 サイバーテロの脅威

確実にサイバーテロと呼ぶべき被害は、世界的にみても、いまだ発生していない。しかし、平成 12 年に起きた中央省庁等の Web ページ改ざん事件は、サイバーテロの脅威を示唆するものであり、政府によるセキュリティ対策の推進に影響を与えたといわれている[16]。

III 情報セキュリティ対策の現状

情報セキュリティに関する対策の主なものは、以下のように分類できる。
①セキュリティを脅かす犯罪の「取り締まり」や緊急時の対応
②セキュリティ関連の情報を把握する「情報収集」
③セキュリティ関連「技術」の評価、研究
④情報システムの適切な「運用」
⑤情報セキュリティに資する「人材育成」の推進
⑥国境を越えて広がるセキュリティ上の脅威に対応するための「国際連携」

これらは、おおよそ次のような体制で進められている。コンピュータを悪用した犯罪の取り締まりは警察庁、サイバー攻撃への対処手法の研究等は防衛庁、技術的対策は経済産業省や総務省、運用基準の作成・評価は経済産業省が主に行っている。そして、省庁横断的な企画・調整や緊急時の対策支援等は、内閣官房情報セキュリティ対策推進室（以下「推進室」という。）が担当している。推進室は、IT 戦略本部に置かれた全省庁の局長級から成る情報セキュリティ対策推進会議の事務局でもある。なお、各省庁自体のセキュリティ対策や管轄下の重要インフラ企業との連携は、各省庁が個別に行い推進室が統括している。

以下では、上記①～⑥の対策の概略について述べる。

1 取り締まり

不正アクセス等の犯罪の取り締まりや、サイバーテロ等の緊急事態への対応など、主に、事後的な対策としては、次のようなものがある。

●法律・条約

不正アクセスについては、「不正アクセス行為の禁止等に関する法律」（平成 11 年法律第 128 号）により、権限のない者のアクセスやコンピュータ侵入とそれらを助長する行為が、規制されている。侵入後に業務妨害やなりすまし等を行った場合は、刑法により処罰の対象となる。ウイルスに関しては、現在、ウイルス自体を規制する法律は存在しない。ウイルスによって業務妨害や破壊行為をすれば、刑法が適用されるが、現行法ではウイルスの作成等の行為を取り締まることは困難である。

国際的な枠組みとしては、サイバー犯罪（不正アクセス、ウイルスの他、コンピュータを利用した詐欺等の犯罪も含む。）に関する国際的なガイドラインや協力関係の原則を示す、「サイバー犯罪に関する条約」がある。この条約は欧州評議会において検討され、平成 13

[16] IPA/ISEC「情報セキュリティの現状 2002 年版 個別詳細編」2002.
＜http://www.ipa.go.jp/security/fy13/report/security_state/sec2002detail.pdf＞

年に、わが国を含む 31 カ国が署名している。現在、わが国では、条約批准に向けた国内法の整備の一環として、刑法等の改正が検討されている。改正が行われれば、ウイルスの作成や配布等も処罰の対象になる見込みである。なお、この条約に関しては、プライバシーの侵害等につながることを懸念する意見もある[17]。

●ガイドライン

通商産業省（当時）等は、不正アクセスやウイルスについてシステム管理者やユーザが行うべき対策等のガイドラインを定めている[18]。情報セキュリティ対策推進会議等は、政府のシステムのセキュリティ確保やサイバーテロ対策の行動計画等の策定を進めてきた[19]。

●具体的対応の体制

警察庁は平成 13 年、サイバーテロ等の犯罪捜査支援のため、機動的技術部隊であるサイバーフォースを設置した。現在、中心的施設のサイバーフォースセンターを始め、全国に約 60 名が配置されている。Ⅱの 2 で述べたように、全国の警察施設に設置した検知装置によって監視を行い、攻撃手法等の情報の収集・分析、防御手段の開発・研究を行っている。技術的支援や助言等を通じた重要インフラ事業者との連携強化も図っている。

また、平成 14 年には、情報セキュリティ対策推進室に緊急対応支援チーム（NIRT）が設置された。NIRT は、官民の専門家 17 名から成る非常勤チームで、サイバーテロ等に際して、被害の状況を正確に把握し、拡大防止や復旧のための技術的対応策を検討し、実施を支援する。平成 16 年には、インターネットの常時監視チームを、内閣官房に設立する動きもある。さらに、経済産業省は、サイバーテロ等を想定し、重要インフラに関して実践的な模擬演習を、平成 16 年度から行う予定である。

2 情報収集

情報セキュリティ上の事故や事件に早期に対応するために、被害等に関する情報を収集・共有し、分析を行う、各種の組織が設立されている。

●IPA/ISEC と JPCERT/CC

わが国の代表的な情報収集機関としては、ウイルス対策を中心に行ってきた IPA/ISEC と、不正アクセス対策を中心に行ってきた JPCERT/CC とがある。これらの機関は、情報セキュリティ関連の被害や対策についての情報を収集し、分析・蓄積・研究を行い、結果を一般に提供することで、普及啓発の役割も果たしている。

●ISAC（情報共有・分析センター）

ISAC は、元々は米国の重要インフラを担う各業界で組織された、セキュリティ情報の共有と緊急時の連絡窓口の役割を果たす非営利団体である。わが国もこれに倣い、平成 14 年、総務省の主導で、初の ISAC であるインシデント情報共有・分析センター

---

[17]「批准作業進むサイバー犯罪条約」Mainichi INTERACTIVE 2003.9.2.
＜http://www.mainichi.co.jp/digital/coverstory/archive/200309/02/1.html＞

[18] 郵政省「情報通信ネットワーク安全・信頼性基準」
＜http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_0203.html＞
通商産業省「情報システム安全対策基準」「コンピュータウイルス対策基準」「コンピュータ不正アクセス対策基準」＜http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm＞
国家公安委員会「情報システム安全対策指針」＜http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm＞

[19] 内閣官房情報セキュリティ対策推進室「情報セキュリティ施策の展開」＜http://www.bits.go.jp/sisaku＞

（Telecom-ISAC Japan）が設立された。情報通信業者によって組織された Telecom-ISAC Japan は、通信サービスを妨げるセキュリティ上の事故情報を収集・分析・共有することで、情報通信基盤の安全性確保を目指している。また、他の対応組織（NIRT・IPA/ISEC・JPCERT/CC 等、及び海外の類似組織）との連携も重視している。米国では 10 以上の業種に ISAC が置かれているが、わが国の状況は極めて手薄で、現在、他業種での設立が検討されている。

●今後の体制強化

わが国では、セキュリティ情報を収集・分析する体制が弱く、IPA/ISEC 等も、米国の専門機関等からの情報を基にウイルスの危険性などを判断しているのが現状である。そこで総務省は、国内ネットワークを常に監視し、セキュリティ情報を収集する「広域モニターシステム」を平成 16 年度内に構築し、Telecom-ISAC Japan によって運用することを計画している。経済産業省も、平成 16 年 1 月に、ソフトの欠陥やウイルスの攻撃手法、対策手段等を分析・提供する「情報セキュリティ技術ラボラトリ」を IPA 内に設置した。

3 技術

技術的対策としては、電子署名・暗号等のセキュリティ技術や攻撃に強いシステムの利用が考えられる。そのためには、それらの安全性の評価や、研究・開発を行う必要がある。

●電子署名の普及

電子署名とは、従来の捺印や手書き署名と同様のものを電子的に実現する技術であり、安全な電子商取引の基盤となる。平成 13 年には、「電子署名および認証業務に関する法律」（平成 12 年法律第 102 号）が施行された。この法律は、電子文書等に本人による一定の電子署名があれば、手書き署名と同様に通用すると定めている。また、署名が本人のものであること等を証明する認証業務のうち、一定の基準を満たしたものは、国の認定が受けられることになっており、これが認証業務の信頼性判断の目安となっている。

●暗号技術の評価

総務省、経済産業省、通信・放送機構（TAO）及び IPA/ISEC は、セキュリティの基盤技術である暗号技術の安全性を客観的に評価する、暗号技術評価事業（CRYPTREC）を共同で行っている。CRYPTREC の一環として、平成 15 年には、電子政府での利用を推奨する暗号のリストと、調達のためのガイドブックが作成された。各府省は可能な限り、リスト上の暗号を利用する方針である。

●IT 製品の技術評価

経済産業省は、「IT セキュリティ評価・認証制度」を平成 13 年から開始した。これは、IT 製品やシステムのセキュリティについて、国際的な技術基準に基づく評価・認証を行う制度である。制度の利用を促進するため、各省庁は、この制度で認証された製品やシステムを優先的に調達することで合意している。

●オープンソース OS 導入の検討

オープンソース OS とは、ソフトウェアの設計図であるソースコードが公開され、改良して利用することが可能な OS[20]のことである。中身が明らかであるため、セキュリティ上の問題に対応しやすいと見られている。現在わが国で使われている OS は、Windows が大

[20] Operating System の略。ハードウェアと応用ソフトの仲介をし、ユーザがコンピュータを利用できるようにするという、基本的な機能を持つソフトウェアのこと。Windows や Mac OS などがある。

半を占めているため、Windows にセキュリティ上の欠陥があった際には被害が大きくなる可能性もある。オープンソース OS の導入には、多様な OS の利用促進の意味もある。経済産業省は、オープンソース OS 等の利用状況の調査結果と導入検討のガイドラインを公表し[21]、セキュリティ強化の技術や電子政府での採用に必要な機能についての調査研究も計画している。総務省も、電子政府等へのオープンソース OS の導入に関するセキュリティ上の利点・問題点等について、研究[22]している。

●研究・開発の推進

現在、電子署名・暗号等の技術については多様な研究がなされているが、ネットワークやソフトウェア等に関するセキュリティ技術の研究は遅れているといわれる。こうした研究は TAO、IPA/ISEC、通信総合研究所（CRL）、産業技術総合研究所（AIST）、大学等で行われているが、これら機関の強化と連携、中核的研究開発拠点の整備等が進んでいる[23]。

4 運用

セキュリティ維持のため、企業等は、システム全体を適切に運用する必要がある。具体的には、対策方針や実施計画の作成、それに基づく管理を継続的に行わなくてはならない。

平成 14 年、「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」が開始された。これは、第三者が国際的な規格をもとに、企業のセキュリティ管理が適切か評価する制度であり、日本情報処理開発協会（JIPDEC）が運営している。

経済産業省は、企業や政府のセキュリティ対策を専門家が客観的に評価する情報セキュリティ監査を普及させるため、監査の方法や内容の基準と監査を請け負う企業の登録リストを柱とする「情報セキュリティ監査制度」を、平成 15 年に開始した。この制度は、企業等の部門全体ではなく、特定の業務のみへの適用も可能であるし、評価のみならず助言的な監査も重視している。また、現状では、政府の情報セキュリティを対象とした監査の具体的な指針がないため、「電子政府における利用モデル」を提示しているのも特徴である。

現在、これらの制度については、実施体制の強化や利用促進が図られている。経済産業省は、情報セキュリティ監査制度をベースに、企業等におけるセキュリティ対策のレベルを評価し、格付けする制度も検討中である。

5 人材育成

情報セキュリティの維持には、専門的な知識や技術を持つ人材が不可欠である。しかし現状では、企業において、セキュリティ分野の専門的な人材は、約 12 万人不足している。

---

21 経済産業省「オープンソースソフトウエアの利用状況調査／導入検討ガイドラインの公表について」2003.8.15. ＜http://www.meti.go.jp/kohosys/press/0004397/＞

22 総務省「セキュア OS に関する調査研究会」
＜http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/s_os/index.html＞

23 総合科学技術会議「情報セキュリティの課題と方向性」＜http://www8.cao.go.jp/cstp/project/export/ITPT-B/ITPT1/shiryo.1-1-4.pdf＞；「通信総合研究所情報セキュリティセンターの設置について」
＜http://www2.crl.go.jp/pub/whatsnew/press/031225/031225.html＞

中でも、特に高度な専門性を持った人材の不足は約 9 万人に上るといわれる[24]。多くの企業は、セキュリティの高度な知識と技術を持った人材の不足を感じている。「セキュリティ確保のために、どのような人材が必要か明確にできない」、「人材評価の方法が分からない」など、人材を確保する上での問題を抱えている企業も多い[25]。

このような現状に鑑み、IPA/ISEC は、人材の評価・教育への利用を想定し、情報セキュリティに携わるために必要な知識や技術をまとめた「スキルマップ」を作成した。経済産業省は、セキュリティ管理の現場責任者に必要な知識や技術を養う国家試験「情報セキュリティアドミニストレータ試験」を行っている。総務省も、民間の研修を強化するため、多額の初期投資が必要な施設整備や教材開発への支援等をしている。

なお、現在、情報セキュリティ学科を持つ大学はないが、中央大学、筑波大学、早稲田大学、大阪大学等で、セキュリティに関する研究・教育環境を強化する動きが見られる。

6 国際連携

情報セキュリティへの脅威は、国境を越えて広がるという特徴があるため、国際的に連携して対策を進めることが不可欠である。現在、行われている取組みを、表 2 にまとめた。

表 2 ： 国際連携に関する取組み

	関係省庁・団体	内　　容
取り締まり・緊急対応	警察庁、総務省、法務省、外務省、経済産業省	G8 リヨングループハイテク犯罪サブグループに参加、ハイテク犯罪からの重要インフラの保護について、各国と情報交換
	内閣官房、警察庁、総務省、外務省、経済産業省等	OECD の 1992 年情報システムセキュリティガイドライン見直し作業に参加
	警察庁	アジア各国のハイテク犯罪の技術対応担当者を対象とする国際会議を実施、ネットワークを活用して情報を共有・交換
	防衛庁	2000 年度より、米国国防総省等と、政策協議や情報交換を行うための IT フォーラムを開催
	内閣官房	2002 年 3 月、米国の情報セキュリティ対策担当者との日米政府間討議を開催。将来の連携も目指している。
情報収集	JPCERT/CC	2003 年、アジア太平洋コンピュータ緊急対応チーム（APCERT）設立
		世界の CSIRT（コンピュータセキュリティ問題対応チーム）の連携を目的とする国際フォーラムに加盟
技術	総務省	アジア太平洋電気通信共同体（APT）の研究会において、情報セキュリティ分野での協力体制の強化で合意
		国際電気通信連合電気通信標準化部門（ITU-T）における、情報セキュリティに関する標準化活動を推進
	情報システム関連企業、商社等（経済産業省が支援）	アジア地域の国々に対する統括的な PKI（公開鍵暗号方式による暗号技術）を実現するため、アジア PKI フォーラムを設立
	製品評価技術基盤機構（NITE）、経済産業省	IT 製品やソフトウェアの安全性を評価・認証する国際基準、共通基準相互認証制度（CCRA）への加盟

（出典）総務省情報通信ソフト懇談会セキュリティ WG「中間報告書」2003.7.25、情報セキュリティ対策推進会議「『重要インフラのサイバーテロ対策に係る特別行動計画』のフォローアップ等について」2002.3.28.などをもとに作成。

[24] 情報通信ソフト懇談会「人材育成ワーキンググループ中間報告書」2003.7.25.
＜http://www.soumu.go.jp/s-news/2003/030725_5a.html＞
[25] IPA/ISEC「情報セキュリティプロフェッショナル育成に関する調査研究」2003.4.
＜http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html＞

Ⅳ 今後の課題

これまでに、IT 戦略本部、総合科学技術会議、情報通信ソフト懇談会等は、セキュリティに関する課題の検討や対応策の提言を行ってきた。また、産業構造審議会は平成 15 年、わが国初の包括的な「情報セキュリティ総合戦略」を答申している[26]。これらの提言を表３にまとめた。Ⅲでみたように、その多くは既に取組みが始められているが、各種対策を横断する課題として、省庁間の調整、セキュリティ意識の啓発等が挙げられている。

表３ ： 情報セキュリティに関する提言

		IT 戦略本部	総合科学技術会議	情報通信ソフト懇談会	情報セキュリティ総合戦略
省庁間の調整･体制整備		政府の体制整備	対策を統括する組織の設置又は拡充		内閣機能の強化、統一的な推進体制の整備
普及啓発		セキュリティ文化定着のため、啓発や注意喚起	セキュリティ文化を定着させるための啓発の強化	ネットワーク利用者の教育・啓発	義務教育段階からの教育の実践等による、意識の向上
取り締まり	緊急時対処	体制強化。関係者間の連携強化			関係者間の情報共有体制見直し。ガイドライン整備
	不正行為の取り締まり	セキュリティ関連の不正行為対策推進。法整備の検討			セキュリティ関連の法制度上の問題点に係る検討。犯罪対策の推進
情報収集		情報収集･分析能力の強化		Telecom-ISAC Japan の活動強化	セキュリティ情報収集・分析体制の強化
技術	セキュリティ技術の研究開発	国においても、先導的基盤技術の研究開発を推進	研究開発の強化。攻撃の防御･対処に加え、ネットワーク自体の安全性向上	サイバーテロ対策技術・ネットワーク自体の安全性向上等の研究推進、体制の充実	技術開発の促進
	安全な製品・サービス	セキュリティに配慮した多様な製品等の提供促進	安全･信頼性の高いソフトウェアの開発		安全性向上に向けた技術・製品・サービスの開発
	オープンソースの検討	オープンソースソフトウェアの評価等	オープンソースソフトウェアの開発・利用促進		単一の OS に依存するリスク回避のための代替案確保
	技術評価	情報セキュリティ評価・認証制度の普及			技術評価の促進
	運用	関連制度の普及促進			セキュリティマネンジメントの促進
人材育成		十分な知識･技術を持つ専門家の育成	高度な人材の育成・流動化の促進	専門的・高度な人材の育成	高度人材の育成

（出典）IT 戦略本部「e-Japan 重点計画-2003」2003.8.8、総合科学技術会議ソフトウェア懇話会「ソフト的な分野において推進すべき事項」2003.7.1、セキュリティ WG「中間報告書」、「情報セキュリティ総合戦略」をもとに作成。

1 省庁間の調整

わが国の情報セキュリティ対策は、分野ごとに複数の省庁が推進しており、一部には、省庁による「主導権争い」ともいえる状況が見られる。例えば、オープンソース OS の導入については、経済産業省と総務省が、事前の調整なしで似たような政策を行っている[27]。この一因は、省庁横断的なセキュリティ関連組織は推進室のみであること、しかも推進室

[26] 経済産業省「情報セキュリティ総合戦略」2003.10.10.
＜http://www.meti.go.jp/policy/netsecurity/strategy.htm＞
[27]「国の情報セキュリティー政策 『船頭』定まらず 迷走」『日経新聞』2003.11.8.

が非常勤職員中心の小規模な組織であり、企画・調整を行うのみで実効性に乏しいことにある。現在様々な組織が担当している電子政府のセキュリティ維持、情報収集、技術・運用の評価や開発等を一元的に行う独立の組織を新設すべきである[28]との指摘もある。

こうした現状の改善に向けて、情報セキュリティ総合戦略の検討段階には、内閣官房、内閣府、警察庁、防衛庁、総務省がオブザーバーとして参加している。また、戦略は、推進室を強化し、政策の推進体制間の総合的な調整・進捗管理をはじめ、情報収集体制の構築や各省庁へのセキュリティ監査等を行わせることを提言している。IT 戦略本部も、内閣官房に、セキュリティ対策の助言を行う補佐官を平成 16 年に置くことを発表している。

2 普及啓発

これまでの様々な取組みにもかかわらず、依然として企業や個人ユーザのセキュリティ意識は低いうえ、実際の対応も充分ではない。企業等を対象とした調査によれば、セキュリティ管理部署を設置している割合は約 60%だが、専従の担当者の設置は約 5%、教育の実施は約 16%、セキュリティポリシーの策定は約 28%にとどまっている[29]。別の調査でも、ウイルス対策部門・担当者を設置している割合、及び対策教育を行っている割合は約 6 割であり、米国の約 8 割に比べ対策が遅れていることが分かる[30]。また、総務省の調査によると、個人のインターネット利用者の約 3 割がセキュリティ対策を行っていないという[31]。

政府の政策や対策の方法についての企業等の知識不足も問題である。企業・自治体対象の調査（平成 15 年調査）では、通商産業省（当時）の「コンピュータウイルス対策基準」を「知らない」とする回答が 3 割以上を占める[32]。届け出機関としての IPA/ISEC の認知度は約 60%だが、近年ほとんど増加しておらず、ウイルス被害を届け出ない理由は「方法が不明なため」が約 45%に上る。また、前述の総務省の調査では、対策を行っていない個人ユーザの約 65%が、その理由を、具体的な方法が分からないためとしている。

このような現状への対策として、情報セキュリティ総合戦略では、企業関係者への研修や、個人利用者に対する義務教育段階からのセキュリティ教育の実践等を提言している。

おわりに

以上のように、IT 化が進む現代において、情報セキュリティの確保は危急の課題である。しかし、その対策には様々な要素が絡み、一朝一夕には大幅な向上は期待できない。Ⅳで触れた情報セキュリティ総合戦略についても、全ての対策の実現は難しいという見方もある[33]。セキュリティ促進のためには、今後さらに、継続的に力を注ぐことが求められる。

28「『電子』安全保障を整備せよ」『日経コンピュータ』572 号,2003.4.21,pp.42-57；
ソフトウェア懇話会「ソフト的な分野において推進すべき事項」

29 警察庁「不正アクセス行為対策の実態調査」2003.5.

30 IPA/ISEC「『海外におけるコンピュータウイルス被害状況調査』報告書」2003.3.

31 総務省 前掲注（8）,p.122.

32 IPA/ISEC 前掲注（7）

33「政府が包括的な情報セキュリティ戦略」『日経コンピュータ』585 号,2003.10.20,pp.16-17；
「壮大な計画、どこまで実現できるか」Mainichi INTERACTIVE 2003.10.17.
＜http://www.mainichi.co.jp/digital/coverstory/archive/200310/17/1.html＞

略称表（アルファベット順）

略称･略語	日本語名称	英語名称	関係省庁
AIST	産業技術総合研究所	National Institute of Advanced Industrial Science and Technology	経済産業省
APT	アジア・太平洋電気通信共同体	Asia-Pacific Telecommunity	総務省
APCERT	アジア太平洋コンピュータ緊急対応チーム	Asia Pacific Computer Emergency Response Team	経済産業省
CCRA	共通基準相互認証制度(共通基準承認アレンジメント)	Common Criteria Recognition Arrangement	経済産業省
CRL	通信総合研究所	Communications Research Laboratory	総務省
CRYPTREC	暗号技術評価事業（経済産業省、総務省及び関係団体が、暗号技術検討会と暗号技術評価委員会（＝CRYPTREC）で行ってきた事業を指す。）	Cryptography Research and Evaluation Committees	経済産業省、総務省
CSIRT	コンピュータセキュリティ問題（インシデント）対応チーム	Computer Security Incident Response Team	
IPA/ISEC	情報処理推進機構セキュリティセンター	Information-technology Promotion Agency/ Information-technology Security Center	経済産業省
ISAC	情報共有・分析センター	Information Sharing and Analysis Center	
ISMS	情報セキュリティマネンジメントシステム	Information Security Management System	
ITU-T	国際電気通信連合 電気通信標準化部門	ITU(International Telecommunication Union) Telecommunication Standardization Sector	総務省
JIPDEC	日本情報処理開発協会	Japan Information Processing Development Corporation	経済産業省
JPCERT/CC	JPCERT コーディネーションセンター	Japan Computer Emergency Response Team / Coordination Center	経済産業省
NIRT	緊急対応支援チーム	National Incident Response Team	内閣府
NITE	製品評価技術基盤機構	National Institute of Technology and Evaluation	経済産業省
PKI	公開鍵基盤	Public Key Infrastructure	
TAO	通信・放送機構	Telecommunications Advancement Organization	総務省
Telecom-ISAC Japan	インシデント情報共有・分析センター	Telecom-ISAC(Information Sharing and Analysis Center) Japan	総務省