６．高度情報通信ネットワークの安全性及び信頼性の確保

＜目標＞

我が国の高度情報通信ネットワークの安全性及び信頼性を世界最先端の IT 国家にふさわしいものにするため、特に、電子政府、電子商取引、重要インフラ等のうち国民生活や社会経済活動に大きな影響を及ぼすものについて、情報セキュリティの不備により不正アクセス、コンピュータ・ウイルス、DoS 攻撃(Denial of Service;サービス不能攻撃)等の高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止をゼロとすることを目標とする。

（１）現状と課題

インターネット等の情報通信ネットワークにおいては、常に不正アクセス行為、コンピュータ・ウイルス、DoS 攻撃[1]などの脅威にさらされており、超高速インターネット網の整備やインターネット常時接続の実現、電子商取引の発展や電子政府の実現等によって、これらの脅威は、政府機関や企業などに限らず、すべての国民にとっても、詐欺等の犯罪行為やプライバシー侵害等のかたちで、現実の差し迫ったものとして現れてくることが懸念される。

また、エネルギー供給、交通、政府・行政サービス等の国民生活や経済・社会活動に大きな影響を与えるいわゆる重要インフラ関連サービス活動の多くは、情報システムにますます依存するようになってきており、今後、更に加速的な情報化・ネットワーク化の進展が見込まれるなか、いわゆるサイバーテロの脅威が現実のものとなってきている。こうした状況は、自然災害等の緊急事態発生時の危機管理や国家安全保障に関わる事案についても同様であり、安全で信頼できる情報通信ネットワークの構築は経済社会全般の安全性・信頼性を確保する上で必須の課題である。

しかし、我が国の現在の情報セキュリティ水準は、不正アクセス防止に有効とされる一般的方法の一つであるファイアウォール[2]の設置率が 50%程度(米国では約 80%)にとどまっているなど、いまだ世界最高水準のものとは言い難いため、これを 2005 年までに世界最先端の IT 国家にふさわしい水準に引き上げることが必要である。

このため、情報の自由な流通と民間の自由な活動の確保を大前提としつつ、情報通信に関する安全性及び信頼性の確保とプライバシーの保護に万全を期する。あわせて、国際的な連携、治安、防災、安全保障、さらには、災害時等における情報システムのバックアップ体制や高度なセキュリティが求められる施設には、光ファイバー等を用いるなどの十分な配慮が必要である。

---

[1] DoS 攻撃：Denial of Service 攻撃(サービス不能攻撃)の略称。コンピュータやネットワークに不正に負荷をかけたり、セキュリティホールを突くなどして業務を妨害する攻撃。

[2] ファイアウォール：主に内部ネットワークと外部(インターネット等)との境界に設置し、外部からの不正アクセス等の攻撃を防ぎ、内部ネットワークを保護するシステム。

＜主要指標（1999 年 12 月）＞

政府・企業等における情報セキュリティポリシー策定率	**18.9%**
政府・企業等におけるファイアウォール設置率	**50.7%**
政府・企業等におけるバックアップシステム設置率	**24.3%**

（２）施策の意義

情報セキュリティ対策の推進は、高度情報通信ネットワークの発展に必要不可欠なものであるが、IT に係る技術革新の速度が極めて速いなかで、ますますその攻撃手法等が進化を遂げていることや、国境が無いというサイバー空間の特徴により、国内のみならず世界のどこからでも瞬時かつ隠密にサイバー攻撃を受ける可能性があることなどから、その対応は困難さを増している。このため、それに対処するための安全対策についても不断の見直しが必要である。高度情報通信ネットワークの安全性及び信頼性の確保は、世界最先端の IT 国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。

（３）具体的施策

①　情報セキュリティに係る制度・基盤の整備

刑事基本法制、情報セキュリティに関する客観的な判断基準等、情報セキュリティ対策における制度・基盤の整備を推進する。

ア）刑事基本法制の整備（法務省）

IT 経済社会における刑事の基本法制について、高度情報通信ネットワーク社会の安全性及び信頼性の確保に資するため、法的基盤の整備を行う。

ⅰ）2001 年中に、支払用カードの偽造等の犯罪に関する罰則の整備について刑法の一部を改正する法律案を国会に提出する。

ⅱ）2005 年までに、各種のハイテク犯罪に対する罰則、情報通信ネットワークに関する捜査手続について、適切な処罰を確保するため必要に応じた法整備を行う。

イ）情報通信ネットワークの安全・信頼性対策（総務省）

2001 年中に、移動体通信のインターネット利用の急増に伴う新たな脅威等に対

処するため、次世代移動通信ネットワークの安全・信頼性対策について検討を行い、所要の制度整備を行う。

ウ）暗号技術の標準化の推進（総務省及び経済産業省）

客観的にその安全性が評価され、実装性で優れた暗号技術を採用するため、2002 年度までに、ISO[3]、ITU 等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

エ）情報セキュリティマネジメント規格の確立（経済産業省）

2001 年度中に、情報セキュリティマネジメントに関する国際規格(ISO/IEC[4]13335、ISO/IEC17799)を JIS 等へ国内規格化するとともに、情報処理サービス業を対象とした事業所認証制度を創設することにより、情報通信ネットワークの安全性及び信頼性を確保する。

② 政府部内における情報セキュリティ対策

各府省において情報セキュリティポリシー[5]の継続的な評価・見直しを実施し、情報セキュリティポリシーの水準を一層向上させるとともに、電子政府の基盤構築に資する情報セキュリティ評価・認証基盤の整備を行う。

また、情報セキュリティ水準の高い製品等の利用、重要システムのバックアップ、擬似アタックを含めた情報セキュリティ評価の実施等、国民に信頼される電子政府の構築を推進する。

ア）情報セキュリティポリシーの評価・見直しの実施（内閣官房及び全府省）

2003 年度までに、「情報セキュリティポリシーに関するガイドライン」(2000 年 7 月、情報セキュリティ対策推進会議決定)に基づき、全府省は、情報セキュリティポリシーの運用・評価・見直しを実施するとともに、必要に応じ重要シス

---

[3] ISO：International Organization for Standardization（国際標準化機構）の略称。物資及びサービスの国際交換を容易にし、知的、科学的、技術的及び経済的活動分野における国際間の協力を助長するために、世界的な標準化及びその関連活動の発展開発を図ることを目的とした国際機関。

[4] IEC：International Electrotechnical Commission（国際電気標準会議）の略称。電気及び電子の技術分野における標準化のすべての問題及び関連事項に関する国際協力を促し、これによって国際的意志疎通を図ることを目的とした国際会議。

[5] 情報セキュリティポリシー：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の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、組織及び運用を含めた規定。

テムのバックアップ、擬似アタックを含めた情報セキュリティ評価を行い、電子政府の実現のための情報セキュリティを確保するのに十分な水準に引き上げる。

イ）政府におけるセキュリティ水準の高い製品等の利用の促進（全府省）

2001 年度より、政府における情報セキュリティに関する信頼性の高いシステムの構築のため、「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」(2001 年 3 月、行政情報化推進各省庁連絡会議)を踏まえた政府調達を行う。

ウ）情報セキュリティ技術評価・認証事業の実施（経済産業省）

2001 年度中に、情報機器等の情報セキュリティ関連国際規格(IS0/IEC15408)に基づいた評価・認証事業を開始するとともに、2003 年度までに、政府レベルでの認証に係る国際相互承認スキームへの参加を目指す。

③　個人情報保護

＜前掲（４．電子商取引等の促進）＞

④　民間部門における情報セキュリティ対策及び普及啓発

情報セキュリティ対策を推進するための税制、融資等の支援を実施し、民間部門の情報セキュリティ水準の一層の向上を図るとともに、情報セキュリティ対策に係る相談業務や情報交換・発信について機能の充実を行う。

ア）情報セキュリティ意識の向上（警察庁）

2001 年度中に、国民に対する情報セキュリティに関する研修・意見交換を実施するための情報セキュリティコミュニティセンター(仮称)を全都道府県警察に設置する。また、2004 年度までに、ハイテク犯罪[6]に関する相談、広報啓発活動等に従事する情報セキュリティアドバイザーを都道府県警察に配置し、その能力向上のための研修を行う。

イ）産業界との連携の強化（警察庁）

2001 年度中に、産業界との連携を強化するため、産業界からの参加者を含む会

[6] ハイテク犯罪：コンピュータ技術及び電気通信技術を悪用した犯罪で、電子計算機使用詐欺、ネットワークを利用したわいせつ物頒布、不正アクセス禁止法違反等が挙げられる。

議を警察庁において開催し、産業界との連携に関する基本方針を策定するとともに、全都道府県警察に、プロバイダー、民間企業等とのハイテク犯罪情勢や犯罪手口等の犯罪実態に係る情報交換を行うための協議会を設置する。

ウ）電気通信システムの信頼性を向上する施設の導入支援の強化（総務省）

2001 年中に、自然災害等の非常時における通信手段の確保及びコンピュータウイルス等に対する情報セキュリティの向上を図るため、電気通信基盤充実臨時措置法の改正法案を国会に提出し、同法による支援対象となる「信頼性向上施設」に、新たに「コンピュータウイルス監視装置」等を追加することによって、これらの施設の導入を行う民間事業者に対する税制優遇措置等の支援を行う。

エ）情報通信ネットワークにおける情報セキュリティ評価手法の確立（総務省）

2003 年度までに、情報通信ネットワークに関して事業者の規模にあったセキュリティ評価項目等の検討を行い、ITU に対し国際標準提案を行うとともに、事業者における情報セキュリティ対策のレベルを的確に判断するための評価手法を確立する。

オ）不正アクセス対策・ウイルス対策等に関する情報提供体制の強化（経済産業省）

2003 年度までに、不正アクセス、ウイルス等に関する情報収集・分析に係る機能を具体的に担っている情報処理振興事業協会(IPA)及びコンピュータ緊急対応センター(JPCERT/CC)の充実強化・連携及び海外の関係機関との連携を図り、情報セキュリティ情報提供機能の向上を行うことにより、広く一般利用者がこれらの情報提供を享受できる環境を整備する。

⑤　重要インフラのサイバーテロ対策

「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 年 12 月、情報セキュリティ対策推進会議決定）を踏まえ、重要インフラの基幹をなす情報システムについて、リスク評価、情報セキュリティポリシーの策定及びこれらに基づく情報セキュリティ対策を推進するとともに、政府や民間事業者等との連絡・連携体制の構築及び緊急対処能力の向上を行う。

ア）官民の連絡・連携体制の構築（内閣官房及び全府省）

2001 年中に、官民共同で、情報通信ネットワークの脆弱性を克服するため、

既存の連絡体制を活用しつつ、重要インフラ（情報通信、金融、航空、鉄道、電力、ガス、政府及び地方公共団体)における連絡・連携体制の構築を行う。

イ）内閣官房における緊急対処体制の整備（内閣官房）

2001 年度中に、情報セキュリティ事案に対処するための緊急時対応マニュアルを作成するほか、2003 年度までに、情報セキュリティ対策業務支援システムを整備するなど、内閣官房における緊急対処体制の整備を行う。

ウ）警察における緊急対処体制の整備（警察庁）

ⅰ）2001年度中に、いわゆるサイバーテロ発生時の被害防止や攻撃元の追跡等を行う機動的技術部隊の創設及びサイバー攻撃の発生を認知するためのリアルタイム検知ネットワークシステムの構築を行うほか、要員の訓練・研究環境等必要な装備資機材を整備するなど、いわゆるサイバーテロの未然防止及び発生時の緊急対処のための体制を構築する。

ⅱ）2003年度までに、テロ組織等に関する情報収集体制の整備、警察と重要インフラ管理者との連携強化、要員の技術の向上を図る。

エ）防衛庁における緊急対処体制の整備（防衛庁）

2003 年度までに、防衛庁・自衛隊の保有する情報システムについて、情報セキュリティを確保しつつ運用を行うための運用ガイドラインの策定等を行うほか、情報システムに対する常時監視、システム監査、緊急事態対処等の各種機能を有した組織(部隊)体系の構築を行う。

⑥　情報セキュリティに係る研究開発

ア）国防・治安に係る情報セキュリティ技術の研究開発の推進（警察庁及び防衛庁）

2002 年度までに、警察庁においては、強力なファイアウォールの研究開発を行い、警察が保有するネットワークの情報セキュリティを強化する。

また、2003 年度までに、防衛庁において、サイバー攻撃に対する対処手法の実証的研究等を行い、防衛庁が保有するネットワークの情報セキュリティを強化する。

イ）情報セキュリティに関する基盤技術の研究開発の推進（警察庁、総務省及び経済産業省）

2005 年度までに世界最先端の IT 国家にふさわしい技術水準を確保するため、現在想定されているあらゆる脅威等に対する情報セキュリティ技術の研究開発を推進し、次の研究開発について 2005 年度までに実用化を目指すこととする。

ⅰ）不正アクセスやいわゆるサイバーテロの予防、検知等に関する研究開発

不正アクセスやいわゆるサイバーテロ等の脅威から情報通信ネットワークを守るため、これらの脅威を検知し、迅速かつ適切な対処を可能とするために必要な技術開発を行う。

ⅱ）情報通信ネットワークの安全性及び信頼性の確保に関する研究開発

情報の自由な流通を確保するため、暗号技術、電子署名等の認証技術、セキュリティ評価・認証技術等の情報通信ネットワークの安全性及び信頼性の確保に必要な技術開発を行う。

⑦　情報セキュリティに係る人材育成

研究開発、研修事業、資格制度の導入等を通じ、高いレベルの情報セキュリティ技術を有する人材を十分に確保するための多面的な育成を行う。

ア）ハイテク犯罪対策に係る人的基盤の整備

ⅰ）2004 年度までに、ハイテク犯罪捜査官の配置、サイバーパトロールモニターの委嘱、ハイテク犯罪捜査に従事する全国の警察職員への部内外の研修の実施等、ハイテク犯罪対策に必要な人材の確保や民間との協力体制の整備を行う。（警察庁）

ⅱ）2001 年度中に、地方検察庁の捜査官のネットワーク及び情報セキュリティに関する高度な専門的知識の習得を促進し、複雑高度化するハイテク犯罪に適正かつ迅速に対応できる体制の整備を行う。（法務省）

イ）防衛庁における情報セキュリティ等に係る人材教育（防衛庁）

2003 年度までに、防衛庁職員を米国等へ派遣を行い、緊急事態対処等の高度な情報セキュリティ技術等を習得した中核的な技術専門要員を確保し、部内におけ

る技術要員の教育及び作戦情報などの秘匿性の高い情報を扱う防衛庁のネットワークの情報セキュリティの確保を行う。

ウ）情報セキュリティに関する資格制度の整備（総務省及び経済産業省）

2001年度中に、電気通信主任技術者試験に情報セキュリティに関する試験科目の追加、情報処理技術者試験に情報セキュリティ・アドミニストレーター試験の導入を行うとともに、情報セキュリティに関する講習の実施等及び情報セキュリティ評価関係技術者育成のための研修事業に対する助成を実施する。

⑧　情報セキュリティに係る国際連携の強化

G8、OECD等における情報セキュリティ係る取組に加え、開発途上地域への支援等国際的な取組に積極的な貢献を行う。

ア）ハイテク犯罪対策に係る国際連携の強化（警察庁、総務省、外務省、法務省及び経済産業省）

2001年度に、我が国が主催予定である第2回G8ハイテク犯罪対策官民合同ハイレベル会合等の機会を通じて、国際的なレベルでの官民の協議を行うとともに、ハイテク犯罪に関する迅速な捜査協力のためのルール作りについて協議する。

イ）各国警察機関との連携強化（警察庁）

2001年度に、アジア・太平洋ハイテク犯罪対策担当実務者会議の開催、アジア諸国警察機関との連絡のための24時間コンタクトポイントシステムの有効活用等を通じ、各国警察機関との連携を強化するとともに、ハイテク犯罪対策に係る技術的指導等を行う。

ウ）米国国防総省等との連携強化（防衛庁）

2003年度までに、米国防総省との間における政策協議等の意見交換(ITフォーラム等)を通じて、防衛庁としての情報保証[7]を確立するとともに、これらのノウハウ・技術等について、国防上支障のない限り部外に公表する。

[7] 情報保証：ここでは、現在、米国防総省が実施しているコンピュータ・システム等の安全に関する各種施策の総称(Information Assurance)。

エ）情報セキュリティに関するグローバル情報交換ネットワークの構築（経済産業省）

2003年度までに、不正アクセス・ウイルス等の発生状況・分析等情報セキュリティに関する情報集積を行っているCERT/CC等諸外国の官民関係機関との情報交換のため、JPCERT/CCにおける関係諸機関との連携強化、民間各層におけるネットワーク構築の支援等を行い、情報セキュリティに関する迅速かつ正確な情報提供、対応及び施策への反映ができる環境を整備する。