

セキュリティ文化専門委員会報告書

- 企業・個人の情報セキュリティ対策強化に向けて -

2005年11月17日

情報セキュリティ政策会議
セキュリティ文化専門委員会

目次

はじめに	2
委員名簿	5
1 企業・個人の情報セキュリティ対策に係る現状認識	6
(1) 背景	6
ア ITの普及状況	
イ 企業・個人の情報セキュリティ対策強化が今求められる理由	
ウ 企業・個人の情報セキュリティ対策推進上の課題	
(2) 進むべき方向	10
(参考) 環境問題における取組みのフレームワーク	
2 企業・個人の情報セキュリティ問題の所在	12
(1) 関係する主体の整理と留意点	12
(2) 企業・個人の情報セキュリティ対策強化に係る問題の所在	13
ア 企業の情報セキュリティ対策強化に係る問題の所在	
イ 個人の情報セキュリティ対策強化に係る問題の所在	
(3) メディアに期待される役割と問題の所在	16
(4) 基盤形成に係る問題の所在	16
3 企業・個人の情報セキュリティ問題の解決の方向性と具体的方策	18
(1) 解決の方向性と具体的方策	18
ア 企業の情報セキュリティ対策強化のための方策	
イ 個人の情報セキュリティ対策強化のための方策	
ウ メディアの協力を得るための環境整備の方策	
エ 基盤形成	
(ア) 法制度等の検討	
(イ) 犯罪の取締り及び権利利益の保護・救済	
オ 評価体制の確立	
(2) 今後さらに検討すべき課題	23
ア グローバル(国際的)な視点からの情報セキュリティ対策の検討	
(参考) 有害情報問題	
(別紙1) 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	
(別紙2) サイバーセキュリティの国際的文化の創出に関する総会決議	
(参考) セキュリティ文化専門委員会報告書までの検討の経緯	

はじめに

2000年からe-Japan戦略及びe-Japan戦略IIに基づいて進められてきた我が国における高度情報通信ネットワーク社会実現の取組みは、ITが国民生活・経済活動の多種多様な場面で積極的に活用されるようになるなど大きな成果を生み出している。また、我が国は世界一のブロードバンド基盤環境を持ち、携帯電話等に代表される洗練された先端ITを使いこなしているマーケットを抱えるなど、世界に先駆けてITの社会化が進んでいる。しかし、我が国のIT基盤が真に依存可能な基盤として機能するための取組みはいまだ十分とは言えない。この取組みにおいては、単に基盤技術の高度化により信頼性を改善するだけではなく、利用者が安全に、そして安心してITを利用できるようにすることが重要である。

ここで大きな役割を担うのが情報セキュリティである。情報セキュリティの確保に当たっては、ITに関する技術の変化の速さを理解することは当然ながら、ITが展開されている領域の変化の速さや、ITの適用の状況を的確に把握し、継続的に、かつ、変化に先回りできる体制で取組みを実施することが必要であることは言うまでもない。

しかしながら、ここには大きな問題が存在する。情報セキュリティ確保の取組みを行う主体は一体誰なのかということである。この答えは、高度情報通信ネットワーク社会の基盤であり主要構成要素であるインターネットの特性から導き出すことができると考えられる。インターネットは開放型ネットワークによりエンドユーザの各システムを相互接続する世界規模のコンピュータ・ネットワークである。この特性は、情報セキュリティの観点からは、情報セキュリティに対する理解が均一でないエンドユーザの各システムがネットワーク基盤の一部を構成していることを表しており、そこに大きな脅威が存在することを意味している。このことから分かるように、情報セキュリティ確保のための取組みは、IT基盤に関わるすべての当事者において実施する必要がある。すなわち、公共セクタだけではなく、民間セクタにおいても、また、国民それぞれが個人のレベルにおいても取組みを実施すべきである。

このような考え方にに基づき、我が国の情報セキュリティへの取組みについての設計と実施を2004年より積極的に展開してきた。内閣官房においては、情報セキュリティ問題に関する我が国の全体像を検討するにあたっては、これまで、対策に取り組むべき当事者の領域を、概ね、政府機関、重要インフラ（地方公共団体を含む）、企業、個人に分け、それぞれの特性に応じた対策の在り方を検討する手法を採ってきた。2004年7月には、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）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（委員長；金杉明信 日本電気㈱代表取締役 執行役員社長）を設置し、情報セキュリティに対する我が国の新たな取組みについて

の検討を開始した。現在までに、政府機関の対策については2004年11月に第1次提言¹⁾、重要インフラの対策については2005年4月に第2次提言²⁾として公表され、これを受けた政府としての取組みも開始されている。具体的には、2005年4月には、まず、内閣官房に政府における情報セキュリティ確保の取組みについて中心的役割を果たす内閣官房情報セキュリティセンター(NISC)が設置され、2005年5月には、IT戦略本部の下に情報セキュリティ政策会議が設置された。そして政府の情報システムにおける情報セキュリティ確保についての取組み、重要インフラにおける情報セキュリティ確保のためのフレームワーク作り等が行われている状況にある。

一方、企業、個人という領域における対策の在り方については、政府全体としての取組みの検討が未着手のままになっていたことから、本委員会では、これらの領域を射程とした検討を行うこととした。

政府機関や重要インフラにおける情報セキュリティは、政府としてより直接的な取組みが必要な領域であるのに対し、企業や個人における情報セキュリティは、企業や個人としての行動原理に沿った自主的な取組みが主体的役割を果たし、政府はこれを積極的に支援する取組みが必要である領域と考えられる。そこで、本委員会では、かかる取組みが個別の企業や個人のみ委ねられる特殊なものではなく、各主体のセキュリティに関する理解と役割分担の調整に基づき構築される、常識、マナーあるいは社会的慣習を「セキュリティ文化」と定義し、セキュリティ文化醸成の大前提となる、企業・個人が「何のために情報セキュリティ対策を行うのか」という点についての共通認識を形成するにはどのようにしたらよいか議論を進めてきた。

本報告書の構成は以下のようになっている。

1. 企業・個人の情報セキュリティに係る現状認識
2. 企業・個人の情報セキュリティ問題の所在
3. 企業・個人の情報セキュリティ問題解決の方向性と具体的方策

本委員会での検討の過程では、2002年にOECDが策定した「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 - セキュリティ文化の普及に向けて -」(以下「OECDガイドライン」、外務省仮訳として別紙1参照)及び2003年に国連総会が決議した「サイバーセキュリティの国際的文化的創出に関する総会決議」(別紙2参照)を強く意識し、議論を進めてきた。これらの文書に示された9原則は、情報システム及びネットワークの利用者を含むすべての者が情報セキュリティの責任者としての自覚を持って準拠すべき原則として定められ、多くの示唆を含んでいる。また、同じ内容が国連総会決議

1) 情報セキュリティ基本問題委員会第1次提言(2004年11月16日) <http://www.bits.go.jp/conference/kihon/index.html#teigen>

2) 情報セキュリティ基本問題委員会第2次提言(2005年4月22日) <http://www.bits.go.jp/conference/kihon/index.html#2teigen>

にも採用されたという意味で広く世界的に合意されたものである。本報告書の根底に流れる概念を理解するためには、この原則を理解することが必須である。さらに、本報告書で述べる問題解決の方向性と具体的方策では、この 9 原則を踏まえ、我が国の IT 化進展の現状を勘案し、企業・個人をめぐる情報セキュリティ問題に対する解決方法を提示している。

本報告書で示す解決の方向性と具体的方策の検討過程においては、特に問題解決に取り組む政府の積極的な姿勢が重要であることが多くの委員から指摘された。特に、政府が行うべき環境整備及び国際展開について積極的な取り組みが必要であるということが合意されている。具体的には、環境整備については、政府は、企業・個人などのすべての当事者が情報セキュリティに対して強い関心を持つ環境を整備していくことが必要であり、例えば、すべての組織体がリスクに応じて行う情報セキュリティ対策への取り組みについて客観的指標をもって評価していくような取り組みが求められる。また、国際展開では、諸外国においては情報セキュリティ管理の手法開発、その国際標準化、さらには実施主体となる認証機関設立を通じてビジネス化する戦略的な例が見られ、政府は、情報セキュリティに関する国際標準制定における我が国のプレゼンス確保を明確に意識しなければならない。

この報告書に盛り込まれた具体的方策は、各実施主体において直ちに着手・実行されるべきものとして、本専門委員会は考えており、政府はもとより、企業、個人においても主体的かつ積極的に取り組むことが、我が国の高度情報通信ネットワーク社会の基盤強化に直結し、いわゆるセキュリティ文化の醸成につながると確信している。

2005年11月17日

情報セキュリティ政策会議
セキュリティ文化専門委員会委員長
安田 浩

セキュリティ文化専門委員会 委員名簿

【委員長】

安田 浩 東京大学国際・産学共同研究センター教授

【委員】

稲垣 隆一 弁護士
岡村 久道 弁護士
志波 幹雄 (株)電通アカウント・プランニング計画局エグゼクティブ・プロジェクト・マネージャ
下村 正洋 NPO 日本ネットワークセキュリティ協会事務局長
((株)ディアイティ代表取締役社長)
関口 和一 日本経済新聞編集委員兼論説委員
田邊 則彦 慶應義塾湘南藤沢中・高等部教諭
経沢 香保子 トレンダーズ(株)代表取締役
土居 範久 中央大学教授
苗村 憲司 情報セキュリティ大学院大学教授
廣川 聡美 横須賀市企画調整部情報政策担当部長
藤原 静雄 筑波大学大学院教授
村上 輝康 (株)野村総合研究所理事長 ((社)日本経済団体連合会・IT ガバナンスに関する WG 座長)
吉川 誠司 WEB110 代表
若槻 絵美 弁護士

(五十音順、敬称略)

1 企業・個人の情報セキュリティ対策に係る現状認識

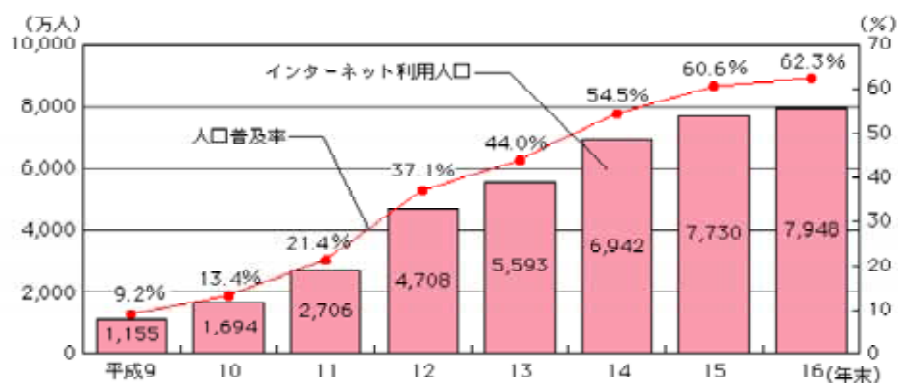
(1) 背景

ア ITの普及状況

2001年1月にIT戦略本部により設定された「5年以内に我が国を世界最先端のIT国家にする」(e-Japan戦略)という目標は概ね達成されつつある。

例えば、我が国のインターネット利用人口は、近年急速なスピードで増加しており、2004年(平成16年)末時点で約8000万人、人口普及率は62.3%となり(図1参照)すべての世代で情報収集手段、通信手段等としてインターネット等が用いられるなど、IT基盤は国民生活・経済活動に不可欠な存在になってきたといえる。

また、電子署名及び認証業務に関する法律等のITに係る法制度の整備や情報セキュリティ監査制度等の導入等、ITを組み込んだ社会制度の構築も徐々に進みつつあるところである。



- ※1 上記のインターネット利用人口は、パソコン、携帯電話・PHS・携帯情報端末、ゲーム機・TV機器等のうち、1つ以上の機器から利用している6歳以上の者が対象
- ※2 平成16年末の我が国の人口普及率(62.3%)は、本調査で推計したインターネット利用人口7,948万人を、平成16年10月の全人口推計値1億2,764万人(国立社会保障・人口問題研究所「我が国の将来人口推計(中位推計)」)で除したものの(全人口に対するインターネット利用人口の比率)
- ※3 平成9～12年末までの数値は「情報通信白書(平成12年までは通信白書)」より抜粋。平成13～16年末の数値は、通信利用動向調査の推計値
- ※4 推計においては、高齢者及び小中学生の利用増を踏まえ、対象年齢を年々上げており、平成12年末以前の推計結果については厳密に比較出来ない(平成11年末までは15～69歳、平成12年末は15～79歳、平成13年末から6歳以上)

図1 インターネット利用人口及び人口普及率

出所：平成17年版情報通信白書

イ 企業・個人の情報セキュリティ対策強化が今求められる理由

その一方で、現在、サイバー犯罪、個人情報や営業秘密等の情報漏えい等のトラブルも急増している(図2、図3参照)。情報漏えいについてはセキュリティの不備を突いた外部からの侵入によるものもあるが内部の者によるものも多く、個人についてもインターネットに接続された家庭のパソコンの不適切な取扱いが原因でコンピュータウイルスが一瞬にしてインターネット上で蔓延したり、パソコンがサイバー攻撃の踏み台に利用されて無意識のうちに加害者として被害の拡大を助長してしまう可能性があるなど、国民生活・経済活動に支障を及ぼすおそれがある。

今後、我が国の IT 基盤が健全な発展を遂げていくためには、「国民全体が IT を安心・安全かつ快適に利用できる」との観点、「IT による我が国の社会経済活動の持続的発展と国際競争力の維持を図る」との観点から、企業・個人の情報セキュリティ対策を強化していくことが必須の課題である。

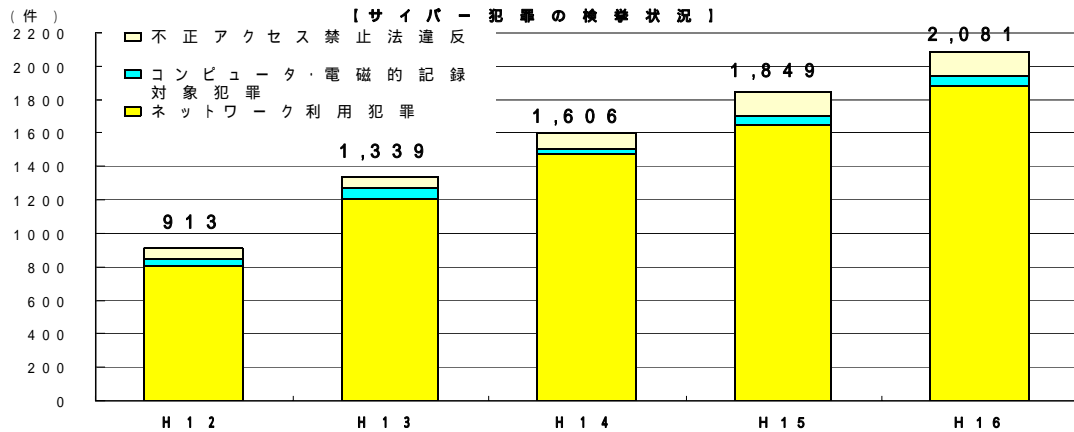


図2 サイバー犯罪の検挙状況

出所：警察庁「平成16年のサイバー犯罪の検挙及び相談受理状況等について」

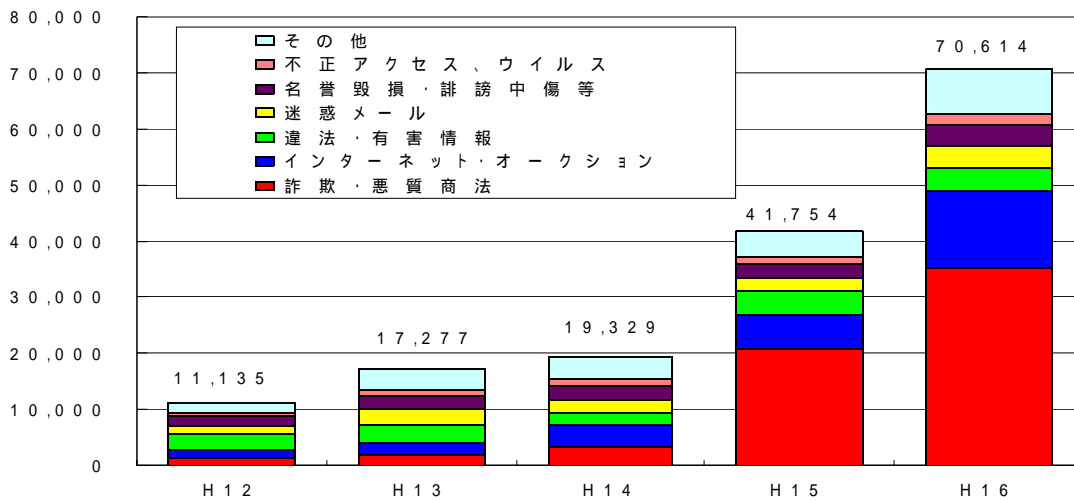


図3 サイバー犯罪等に関する相談受理状況

出所：警察庁「平成16年のサイバー犯罪の検挙及び相談受理状況等について」

ウ 企業・個人の情報セキュリティ対策推進上の課題

企業・個人を総体的に見ると、「情報セキュリティの必要性・重要性がわからない」(図4、図5参照)「情報セキュリティ対策を行おうとしても、何をどこまですべきかがわからない」(図6、図7参照)という状況となっている。すなわち、現状では、企業及び個人が、自発的に情報セキュリティの必要性・重要性を認識し、その上で必要な対策を自ら検索、特定して実施するところまで至っていない場合が多く、このままの環境では、企業・個人の情報セキュリティ対策を強化していくこ

とは、困難な状況にあると考えられる。

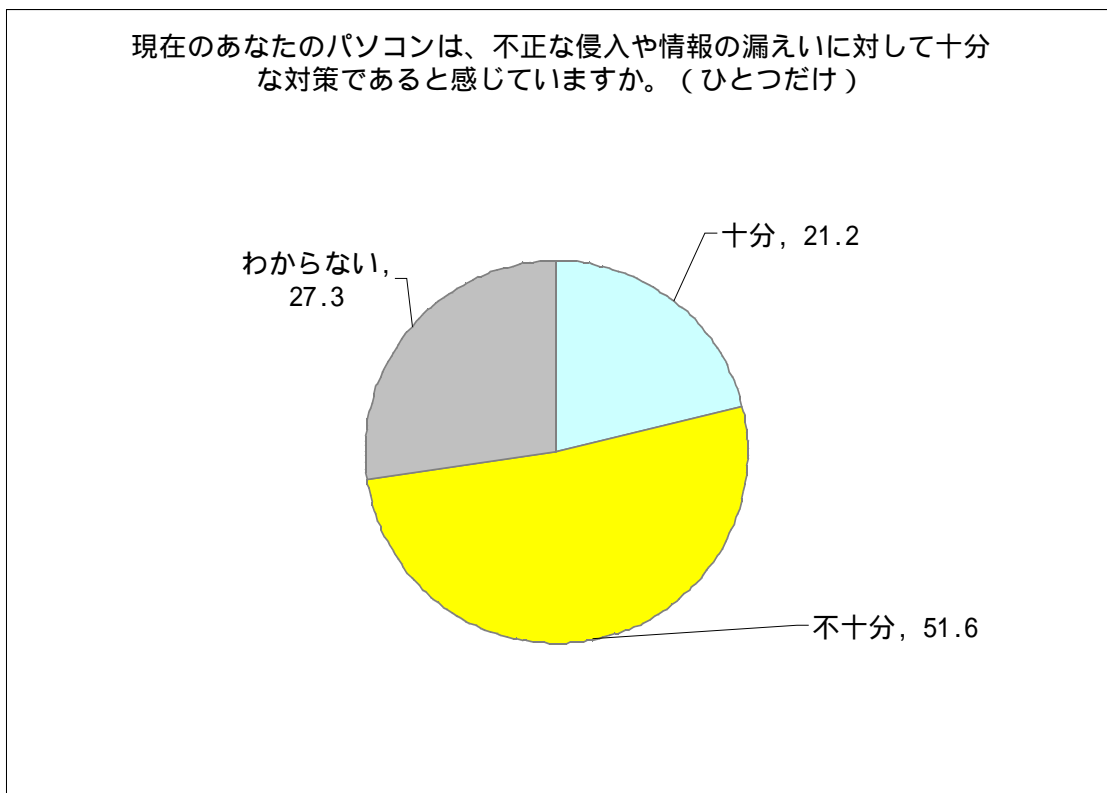


図4 個人のパソコンのセキュリティ対策意識

出所：NRI セキュアテクノロジーズ「個人情報保護に関する消費者意識調査 2005」

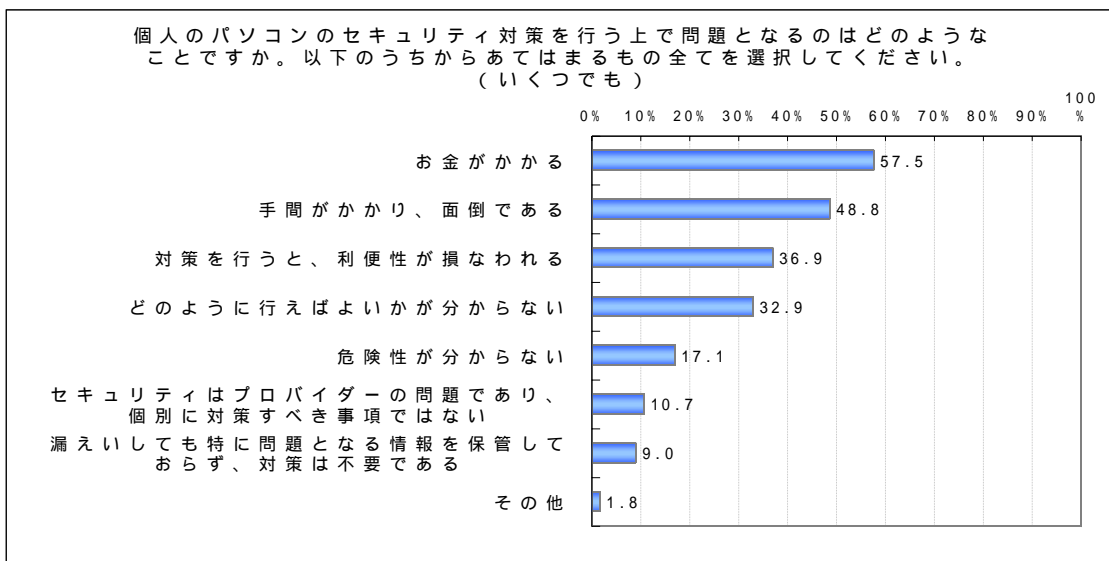


図5 個人のパソコンのセキュリティ対策阻害要因

出所：NRI セキュアテクノロジーズ「個人情報保護に関する消費者意識調査 2005」

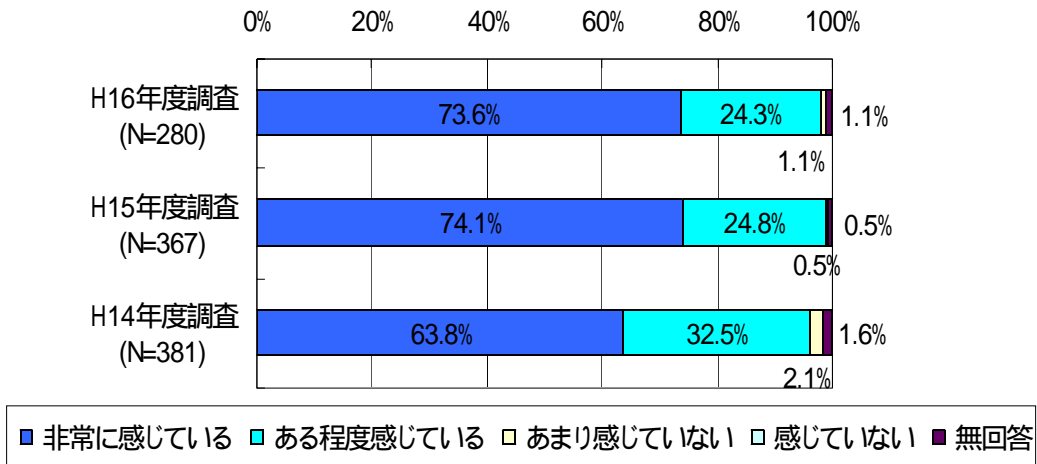


図6 大手・中堅企業（重要インフラ業種を除く）における情報セキュリティの必要性

出所：警察庁「不正アクセス行為対策等の実態調査」より内閣官房作成

「どこまで行えば良いのか基準が示されていない」を選択した企業の割合

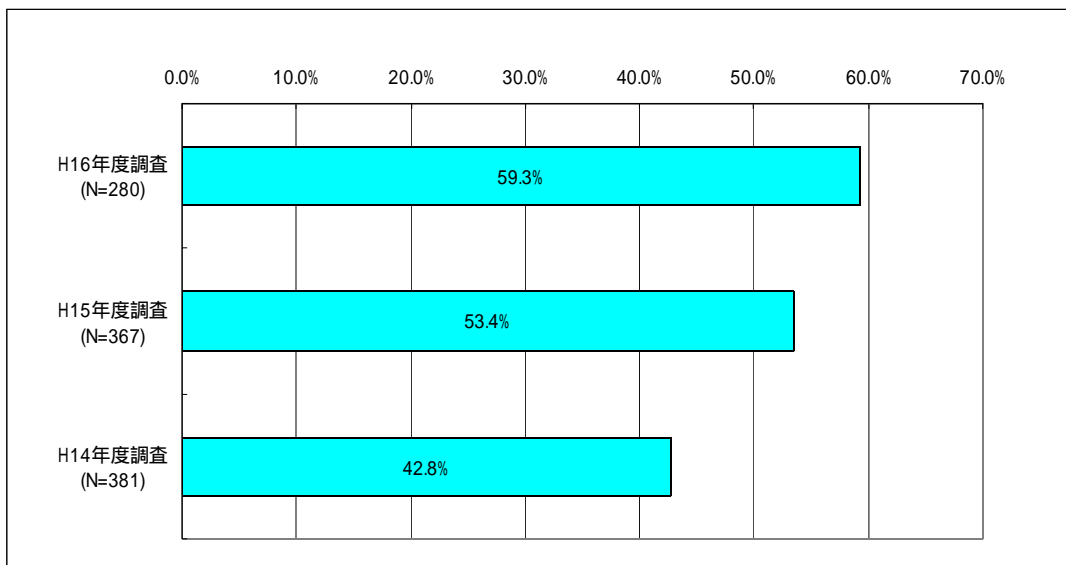


図7 大手・中堅企業（重要インフラ業種を除く）における情報セキュリティ対策実施上の問題点

出所：警察庁「不正アクセス行為対策等の実態調査」より内閣官房作成

(2) 進むべき方向

(1) のウで述べた課題を解決するためには、それぞれの企業・個人によって自律的に対策が実施されることが必要である。そのためには、政府等関係する主体によって、企業・個人が、それぞれの特性に応じ、自律的に適切な行動を行うこととなる環境が構築されることが必要である。

すなわち、企業・個人のセキュリティ対策を強化するためには、情報セキュリティに対する理解が均一でないエンドユーザの各システムがネットワーク基盤の一部を構成していること、そこに大きな脅威が存在すること、したがって、情報セキュリティ確保のための取組みは IT 基盤に関わるすべての当事者において実施する必要があることを踏まえ、企業・個人が「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成を行うことが必要である。こうした企業・個人における共通認識の形成を行う環境を政府等関係する主体が、協力して構築することが必要であり、その際、政府は、OECD ガイドラインの民主主義(Democracy)原則を踏まえた取組みを行うことが重要である(別紙1参照)。

この取組みは、OECD ガイドラインで定義された「セキュリティ文化」(OECD ガイドラインによれば「情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」¹⁾とされる)を実現するための基盤を我が国にも醸成していくことに他ならず、国際社会におけるセキュリティ文化の実現にも寄与するものである。

1) OECD ガイドラインの原文では、"...a culture of security - that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" とある。

(参考) 環境問題における取組みのフレームワーク

以上のような企業・個人が「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成が行われるような取組みについては、以下に示すような環境問題への取組みのフレームワークその他人材、資金等の社会的リソースの配分に関する既存の制度的枠組みも参考となる。

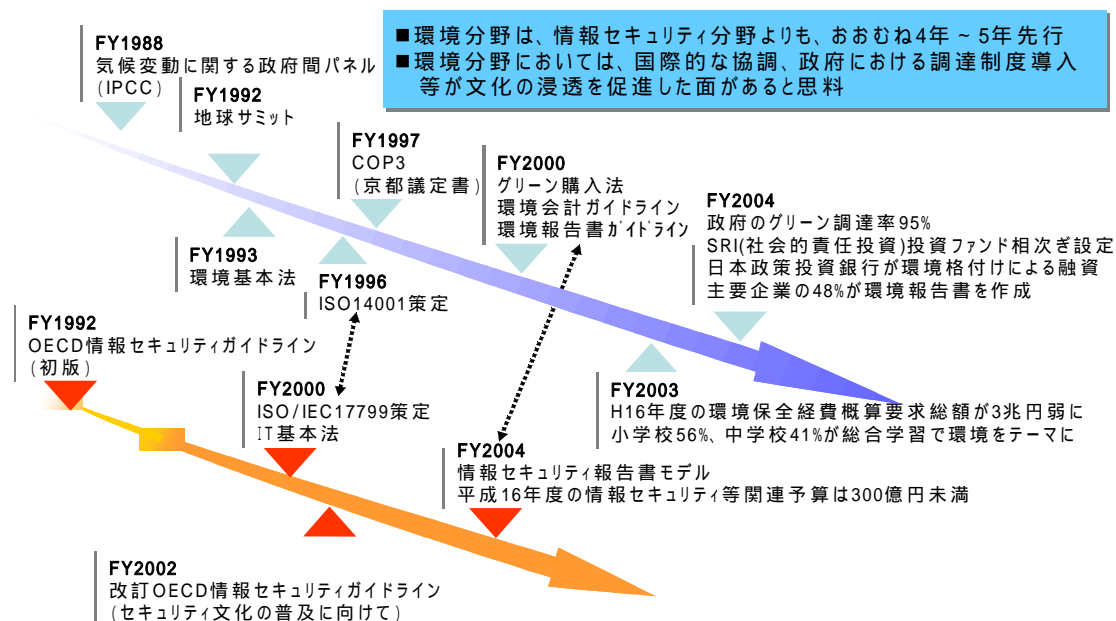


図8 環境分野と情報セキュリティ分野の歴史の流れ¹⁾

1)なお、情報セキュリティ分野については、2005年10月15日に英国標準 BS7799 part2 に相当する国際規格 ISO/IEC27001 が発行され、27000 シリーズとして展開することが明確になった。

2 企業・個人の情報セキュリティ問題の所在

本章では、前章で示した現状認識に基づき、企業・個人がそれぞれ「何のために情報セキュリティ対策を行うのか」という点についての共通の認識の形成を行うことができるために必要な、すなわち、企業・個人の情報セキュリティ対策強化のための方策を検討するにあたっての問題の所在を、より具体的に提示する。

(1) 関係する主体の整理と留意点

問題の所在を提示する前提として、まず、企業・個人の情報セキュリティ対策強化のための方策を検討するにあたって関係する主体と留意点を整理する。

対策を行うべき主体として、本委員会において取り上げる企業・個人については、まず、企業・個人としての行動原理や自主的な取組みを前提とすることが重要であり、そのためには、OECD ガイドラインに言う「責任原則 (Responsibility)」の徹底を、その出発点とすることが必要である。すなわち、企業・個人は、IT 基盤に既に深く依存していること、IT 基盤のセキュリティに対して自らが責任を負っていることを理解し、それぞれに相応しい方法で、責任を負うことが期待される。

ところで、企業・個人と一口に言っても、企業には大企業もあれば中小企業もあり、個人も児童から高齢者まで様々な者を含んでいるなど、そのすべてを一括りに捉えることはできないが、「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成がそれぞれの特性に応じて行われるようにするためには、原則として、以下のような点に留意することが必要である。

* 企業については、企業自身の存続・発展だけを考えるのではなく、市場（顧客や投資家等）との関係に配慮する必要があること、企業の社会的責任（CSR;Corporate Social Responsibility）に係る社会の関心が高まっていること、IT により重要な情報の集積度合が高まっていること等を認識した上で、共通認識の形成を行っていくことが必要である。

* 個人については、8000 万人のインターネット利用者の情報セキュリティに対する理解が世代間で違うなど均一ではないという現状を認識した上で、各対象に配慮するなどして、共通認識の形成を目指していくことが必要である。

一方、企業・個人以外の主体にも、企業・個人の情報セキュリティ対策の強化や「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成を支援する者が存在する。これらの者の役割と働きも同時に重要である。政府のほかに、直接、企業・個人に支援することができる者としては、

企業・個人に対し、直接、情報セキュリティ教育を行う教育機関

企業・個人に対し、直接、製品・サービスを提供する情報関連製品・サービス提供者

がある。は企業・個人に対し、情報セキュリティの重要性とその具体的対策についてまとめてインプットすることが可能な存在であり、は利用者の負担を軽減し、利用者自体の知識等に依らずに情報セキュリティ機能を活用できる製品・サービスの提供を行うことが可能な存在である。

また、メディア（媒体）（新聞、テレビ、ラジオ等の報道機関を指すものとする）は、その活動を通じて、企業・個人の「何のために情報セキュリティ対策を行うのか」

という点についての共通認識の形成に大きな影響を与える存在であり、メディアに期待されている役割は何か、情報セキュリティ対策について適切な情報がメディアにより取り上げられるために関係する主体は何をすべきかを検討することが必要である。

さらに、これらのすべての土台となる社会全体の基盤形成についても、官民による持続的かつ強固な取組みを継続させるためにすべきことは何かを検討することが必要である。

(2) 企業・個人の情報セキュリティ対策強化に係る問題の所在

(1) で提示した留意点を踏まえつつ、企業・個人のそれぞれの特性等に応じ、それぞれの対策強化を行うにあたって阻害要因となっている点、すなわち、企業・個人の「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成ができていない原因を整理すると以下の通りである。

ア 企業の情報セキュリティ対策強化に係る問題の所在

前掲の図6に示すように、企業においては、昨今の相次ぐ情報セキュリティ問題の発生等により、「情報セキュリティ対策を実施しなければならない」との認識は高まっているといえる。しかしながら、実態としては、コンピュータウイルス対策ソフト、ファイアウォール等の導入による対策が中心であり、セキュリティポリシーの策定や情報セキュリティ監査の導入といった組織面からの対策は十分に行われていない状況にある(図9参照)。多くの企業においては、自己責任原則の下で費用対効果に見合った情報セキュリティ対策を講じるという行動原理がある中で、実際に被害が発生しない限り、何をどこまで行えばよいか判断が難しいという悩みを抱えている状況が続いていると言える。

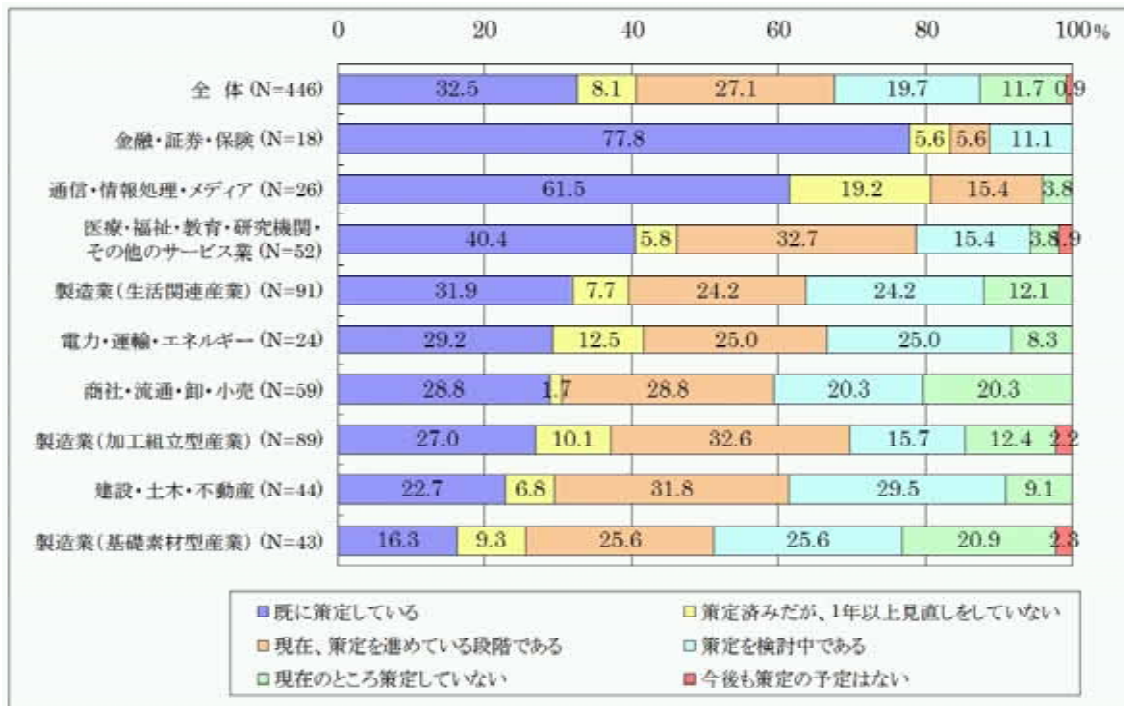


図9 上場企業・各種団体におけるセキュリティポリシーの策定状況

出所：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査 2005 報告書」より

こうした状況に陥っている原因としては、主に以下の2点に集約できると考えられる。

企業の情報セキュリティ対策と市場評価の非直結

情報セキュリティ対策を行うことの必要性は、トラブルを未然に防ぐという観点からは理解されつつあるものの、情報セキュリティ対策を行うことが、顧客や投資家といった市場から積極的に評価される環境ではない。

また、情報セキュリティのリスクが明確ではなく、どこまでの対策を行えば良いか（適正な情報セキュリティ投資）についての判断基準が十分でない。

企業における情報セキュリティ人材の不足等

情報セキュリティ対策を行うにも、各企業においてその対策の実施等を、情報システム開発・運用委託先に依存せざるを得ない状況であるなど、経営トップ等の理解が不足しており、また、現場のエンジニア等企業内における情報セキュリティ人材が不足している。

イ 個人の情報セキュリティ対策強化に係る問題の所在

個人においても、前掲の図4に示すように、情報セキュリティ対策実施の必要性についての認識は高まっていると言える。しかしながら、専ら自宅におけるホームページの閲覧や電子メールの送受信のみの利用ではあるもののブロードバンドに接

続している個人が増大する中、自らが利用するパソコンへのコンピュータウイルス対策ソフトの導入、無線 LAN 利用に際しての利用者限定のための設定等の最低限の対策すら行っていないものも多く存在し、たとえば、米国や韓国と比べても、その取組みが遅れている面がある（図 10 参照）。

あなたはどのようなコンピュータウイルス対策や不正アクセス対策を行っていますか。
（いくつでも）

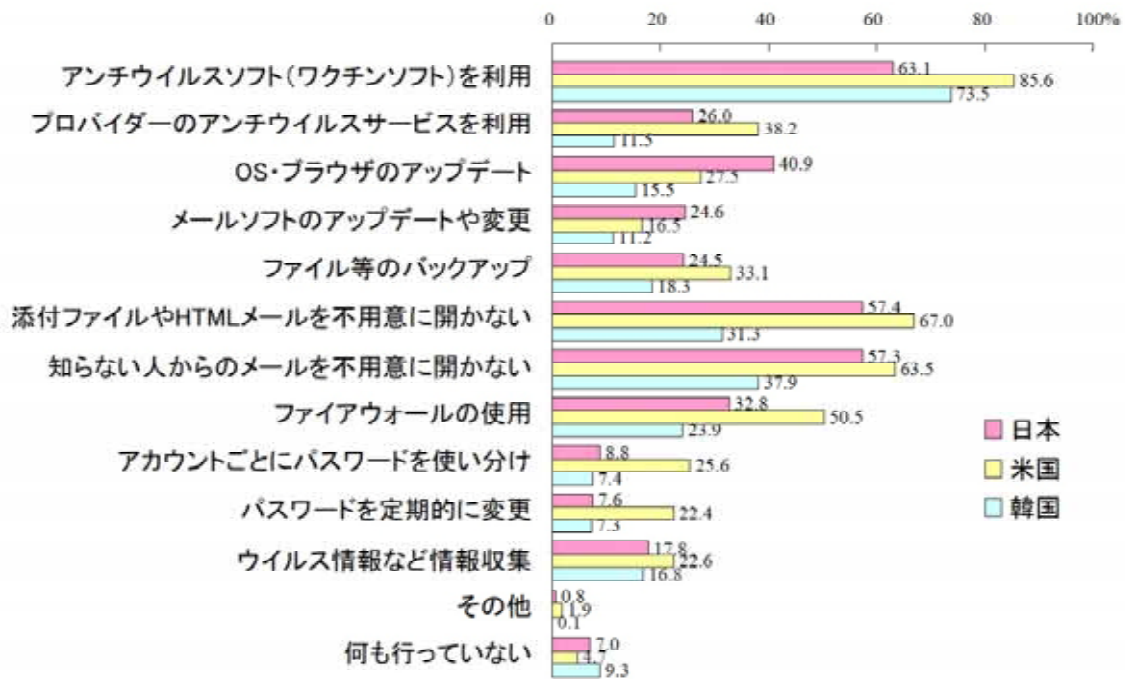


図 10 個人の情報セキュリティ対策の現状

出所：総務省「ネットワークと国民生活に関する調査」(平成 17 年 3 月)より

こうした状況に陥っている原因としては、主に以下の 2 点に集約できると考えられる。

「当たり前のこと」であることが認識できる環境にない

各個人にとっては、被害者とならない限り、自らが情報セキュリティ対策を行わないことが、実は他人に迷惑をかけているといった点の認識が薄く、そうした認識が醸成される環境にない。すなわち、「知らない人に付いていけない」、「道路に急に飛び出さない」、「ペースメーカー等の利用者と近接するような場所（例：満員電車）では携帯電話の電源を切る」等といった極めて一般的な安全に対する認識と同等レベルの意識がまず必要であるにもかかわらず、義務教育課程の教育プログラムに埋め込まれていない、そもそもそれを教えられる人材がいなかった問題や、各種主体による広報啓発・普及活動が行われているものの、広く国民全体に効果を与えるような広報啓発・普及活動は極めて困難である、といった問題点が指摘されている。

ITの分かりにくさと個人の「自己責任」の限界

個人が意識や危機感を持って情報セキュリティ対策を行おうにも、通常は、個人のレベルでは、ソフトウェアのインストール一つとっても、技術的に理解が困難であり、対策を行おうとする入口でつまずいてしまう場合が多い。各個人は、自己責任の下で自らの対策を行うことが原則となるが、こうしたITの分かりにくさをみると、個人が情報セキュリティ対策を行っているという負担感なく製品やサービスを利用できるような環境が、いまだ不足していると言える。

(3) メディアに期待される役割と問題の所在

(2) に述べた問題について、メディアは、企業・個人に対して直接情報発信するという機能を持っていることから、企業・個人がそれぞれ「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成に当たって期待される役割は非常に大きいと言える。

そこで、メディアに期待される役割と、その役割を果たすにあたっての問題を整理する。

ア メディアに期待される役割

メディアが行う報道の基本的な役割は、「起きている事象をありのまま正確に伝える。」ということにある。しかしながら、情報漏えい事案等の情報セキュリティに係る事件・事故を報道することにより、被害の拡大を防止する効果や、警鐘を鳴らすという効果を追加的にもたらすことも期待することができる。

同時に、事件・事故だけでなく、情報セキュリティ対策の好事例等が積極的に取り上げられることにより、企業・個人の情報セキュリティに関するインセンティブの高まりが期待できるなど、メディアには、社会全体の情報セキュリティの意識を高めるための様々な効果を期待することができる。

イ 問題の所在

情報セキュリティへの脅威が年々多岐にわたり、その構造が複雑化しているにも関わらず、「ニュース性」を追う余り、表層的な事象の追跡に終始している報道等も見受けられる。これは、報道に対して問題の本質についての分かりやすい情報を、的確かつ幅広く提供する環境が不足しているという要因も大きいものと考えられる。

(4) 基盤形成に係る問題の所在

企業・個人がそれぞれ「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成を促進するためには、その土台となる社会全体の基盤を形成することが必要である。しかしながら、基盤の形成にあたって、現状では以下のような問題が指摘されている。

ア 各主体の責任・役割等の位置づけ

我が国における情報セキュリティに係る具体的な取組みや各主体の責任・役割について、我が国の法制度等の中に明確に位置づけられていない。

イ サイバー犯罪等

急増するサイバー犯罪等の取締りや予防対策が不十分である。

ウ 急速に変化するサイバー空間の情勢への対応

情報セキュリティ対策のための法制度等の整備が急速に変化するサイバー空間の情勢に対応できていない面がある。

3 企業・個人の情報セキュリティ問題の解決の方向性と具体的方策

(1) 解決の方向性と具体的方策

本章では、企業・個人の情報セキュリティ対策の強化、すなわち我が国の情報セキュリティ政策と整合するような共通認識を形成するために必要な方策について、前章で示した問題点を踏まえて、その方向性と具体策を提示する。政府を中心に各主体は、それぞれの役割に応じて、以下の具体的方策のすべての項目について 2006 年度までに着手すべきである。

ア 企業の情報セキュリティ対策強化のための方策

< 解決の方向性 >

企業の対策を促進するためには、企業の社会的責任（CSR）も含めた自らの責任を持つという「責任原則」の下で、適切な内部統制に基づき情報セキュリティ対策を自主的に行うような環境の整備が必要である。すなわち、2(2)アで示した2つの問題点を解決する取組み - 企業の情報セキュリティ対策が市場評価に繋がる環境の整備、企業における情報セキュリティ人材の確保・育成のための取組み - を、我が国全体として行っていくことが必要である。

なお、政府の果たすべき役割は、企業による自主的な情報セキュリティ対策の取組みを促す環境整備を支援することにあることに留意が必要である。

< 具体的方策 >

具体的には、以下の方策を講じることが適当である。

企業の情報セキュリティ対策が市場評価に繋がる環境の整備

a 政府調達への各種制度の活用

各種政府調達においては、十分な広報等を行いつつ、受注候補先企業の情報セキュリティ対策レベルの評価（「情報セキュリティ対策ベンチマーク」「ISMS 認証」「情報セキュリティ監査」「情報セキュリティ報告書」「事業継続計画」の活用等）を入札条件等の一つとするための環境整備を行う。

【政府が実施】

b 企業における各種制度活用の推進

各企業において、「情報セキュリティ対策ベンチマーク」の利用、ISMS 認証の取得、情報セキュリティ監査の実施、事業継続計画の策定等の、自主的な取組みが行われるよう環境整備に努める。また、それらの実施状況に関する「情報セキュリティ報告書」の作成の推進をはじめとする、情報セキュリティ対策への取組み状況の自主的な開示を推進する。【企業が自主的に実施することを期待、事業者団体等が制度の普及促進を自主的に実施することを期待、政府は制度の普及促進・継続的な見直しを実施】

c 企業の対応策との関係を考慮した情報セキュリティリスク明確化に向けた取組み

情報セキュリティ関係の事件事例を踏まえつつ、企業における情報セキュリティをめぐるリスクに対する定量的評価手法の研究を推進する。

なお、その際、方法論的には困難が予想されるが、リスクの定量的評価

と企業の対応策を関係付け、事故の発生時及び事故後に生ずる社会等へのインパクトの大きさを企業の対応策の差に即した形で迅速に評価し、その評価の結果がメディアを含む社会の幅広い層に受け入れられる環境を整備することについても、官民が連携して検討することが重要である。また、同様の取組みは、個人情報漏えい対策についても行われるべきである。【企業・事業者団体の協力を得て政府が実施、事業者団体等が自主的に実施することも期待】

d 表彰制度の整備

情報セキュリティ対策に積極的に取り組む企業に対する表彰制度を整備する。【政府が実施、事業者団体等が自主的に実施することも期待】

企業における情報セキュリティ人材の確保・育成

を通じて経営トップ等の情報セキュリティへの理解を普及させるとともに、企業の情報システム担当者等に対する全国的規模での広報啓発・普及活動を実施する。【政府が実施、事業者団体等が自主的に実施することも期待】

各企業において情報セキュリティ対策を行っている担当者のモチベーションの維持のための取組みを推進する。【企業が自主的に実施することを期待】

イ 個人の情報セキュリティ対策強化のための方策

<解決の方向性>

個人の対策を促進するためには、個人の自己責任を原則としながらも、2(2)イで示した2つの問題点を解決する取組み - 「当たり前のこと」であることが認識できる環境の整備、個人が負担感なく情報関連製品・サービスを利用できる環境の整備 - が必要である。

その際、に当たっては、老弱男女を問わず各人がその状況に応じて情報セキュリティに関するリテラシーを向上させることを支援する方策に加え、ここでは、特に、初等中等教育及び社会教育からの底上げとともに、企業が対策を行うことによって個人の情報セキュリティに関する意識に間接的に影響を及ぼすという循環を作ることも重要である。

<具体的方策>

具体的には、以下の方策を講じることが適当である。

「当たり前のこと」であることが認識できる環境の整備

a 情報セキュリティ教育の強化・推進

(a) 初等中等教育からの情報セキュリティ教育の推進

初等中等教育（特に義務教育）における情報セキュリティ教育を推進する。このため、学習指導要領の見直し、技術的・専門的視点を踏まえた、発達段階に応じた情報セキュリティ教育コンテンツ等の教育支援体制の整備の推進、義務教育を行う機関のIT教育環境における情報セキュリティの確保の支援等に取り組む。また、情報セキュリテ

イ関連の高等教育（大学・大学院）の充実・強化への主体的な取組みを促す。【政府が実施】

さらに、教員研修、リカレント教育（学校教育を終了した社会人や職業人がいつでも必要に応じて職場や家庭から学習の場に戻って、生涯にわたって繰り返し学習すること）への情報セキュリティ教育の導入等により、教員の意識改革を促進し、情報セキュリティ教育を行うことができる者の育成・拡充を推進する。【政府が実施】

(b) 世代横断的な情報セキュリティ教育の推進

情報セキュリティ関連のリカレント教育の実施等により、世代横断的な情報セキュリティリテラシー形成のための生涯教育を推進する。また、青少年を保護育成する者の啓発も推進する。【政府が実施、事業者団体等が自主的に実施することも期待】

b 広報啓発・情報発信の強化・推進

(a) 全国的規模での広報啓発・情報発信の継続的实施

国民から見て分かりやすい形での広報啓発と情報発信、メディアへの分かりやすい説明、事故発生時の情報発信の迅速化に配慮しつつ、全国的規模での広報啓発と情報発信を継続的に実施する。その際、予防策に加えて、事故が発生した場合の対応方法に係る広報啓発と情報発信も実施する。また、小学生をはじめとする若年層に向けた広報啓発・情報発信も実施する。【政府が実施、事業者団体、非営利組織等が自主的に実施することも期待】

(b) ランドマーク的イベントの実施

国民全体により注意を喚起する方策として、「情報セキュリティの日」の創設、情報セキュリティ関連表彰制度の整備等を行う。【政府が実施、非営利組織等が自主的に実施することも期待】

(c) 日常からの世論喚起の仕組みの構築

日常から情報セキュリティの重要性を世論に呼びかけ、理解を深めるための仕組み（例：人々が安心して情報セキュリティに関する情報を迅速に得ることができるような場（「情報セキュリティ天気予報（仮称）」）の検討）を構築する。【政府が実施、メディア等が自主的に実施することを期待】

(d) 我が国の情報セキュリティの基本戦略の国内外への発信

情報セキュリティ問題全体を俯瞰した我が国としての中長期の基本戦略を積極的に国内外へ発信・周知するための取組みを推進する。【政府が実施】

個人が負担感なく情報関連製品・サービスを利用できる環境整備

電子認証基盤の普及、事業者によるネットワークを介したセキュリティサポートの取組みの促進、セキュアプログラミング手法の研究の活用促進等を

通じたソフトウェアのセキュリティホールを低減する取組みの推進等により、情報関連製品・サービス提供者が、個人が負担感なく利用できる製品やサービス（「情報セキュリティ・ユニバーサルデザイン」）を開発・供給する環境を整備する。また、これらを実現するための継続的な技術開発・実証実験の実施を推進する。【政府が実施、事業者団体等が自主的に実施することも期待】

加えて、トラブルが起こった場合の情報セキュリティサポートを、非営利組織等が実施する。【非営利組織等が自主的に実施することを期待】

ウ メディアの協力を得るための環境整備の方策

2（3）を踏まえ、情報セキュリティに関する幅広い情報が企業・個人に直接届きやすくなるような環境を整備することが必要である。

<解決の方向性>

報道の自由の原則を踏まえた上で、事件・事故だけでなく、サイバー犯罪や個人情報漏えい等のトラブルの予防、被害拡大防止等の、社会全体の情報セキュリティの意識を高める幅広い情報がメディアにより取り上げられるための取組みを行う環境整備が必要である。その際、犯罪や不正行為に悪用される恐れがある情報をどこまで個人に知らせるべきかについても配慮できるようにするものとする。

<具体的方策>

具体的には以下の方策を講じることが適当である。

メディアへの情報の提供

メディアによる情報セキュリティに関する理解・報道を支援するために、情報セキュリティに関する一般情報を的確かつ幅広くメディアに提供する仕組みを構築する。【政府が実施、政府以外のすべての主体が自主的に実施することを期待】

エ 基盤形成

2（4）を踏まえ、基盤形成にあたっての問題を解決するためには、（ア）法制度等の検討、（イ）犯罪の取締り及び権利利益の保護・救済、に取り組むことが必要である。

（ア）法制度等の検討

<解決の方向性>

法制度等の検討にあたっては、企業・個人がそれぞれ「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成をなす前提となる各種基盤の構築を目指すことが必要である。

<具体的方策>

具体的には以下の方策を講じることが適当である。

位置づけ明確化・普及促進のための法制度整備を含めた幅広い検討
我が国における情報セキュリティの位置づけを明確化する、あるいは情報セキュリティ対策の普及を促進するための、法制度整備を含めた幅広い検討を行う。【政府が実施】

新たな脅威・問題発生時の法制度整備等の検討
情報セキュリティ上の新たな脅威・問題が社会に発生した際に、公法・私法等幅広い範囲での法制度整備等について、その必要性も含め迅速に検討することとする。【政府が実施】

(イ) 犯罪の取締り及び権利利益の保護・救済

<解決の方向性>

企業・個人がそれぞれ「何のために情報セキュリティ対策を行うのか」という点についての共通認識の形成を担保するためには、サイバー犯罪を未然に防ぐ、サイバー犯罪を行った者が検挙される、サイバー空間で権利や利益を侵害された者が保護・救済されるなど、サイバー空間が安心して安全かつ快適に利用することのできるものとするのが重要である。そのため、情報セキュリティに対する侵害を予防し、犯罪を行った者を確実に特定・検挙するための仕組みを整備・強化することが必要である。

<具体的方策>

サイバー犯罪の取締り及び権利利益の保護・救済のための基盤整備
サイバー空間における実態に対応した、法執行機関のサイバー犯罪捜査の技能水準の向上や体制の強化を図るとともに、サイバー犯罪条約の締結に伴う法制度の改正や国際協力の強化により、サイバー犯罪の取締りを強化する。あわせて、IT 障害やサイバー空間における不正行為から権利利益を擁護するため、他の権利利益である通信の秘密をはじめとする基本的人権に十分配慮しつつ、官民連携を容易にし、権利利益の保護と迅速な救済を促進するための技術・産業・司法基盤のさらなる整備に努める。【政府が実施】

サイバー空間の安全性・信頼性を向上させる技術の開発・普及
通信相手が誰なのかを全ての通信当事者の承認の下に確認可能とするための認証技術の開発・普及を行う。また、認証技術の他にも、サイバー空間の安全性及び信頼性を向上させるための技術の開発・普及を行う。【政府が実施、その他の主体による自主的な実施を期待】

オ 評価体制の確立

企業・個人の行動規範までも含めた一つの基盤の形成の度合を測る指標の検討と、その評価体制の確立が必要であり、今後、内閣官房情報セキュリティセンターを中心に、形成の度合を測る指標の策定、導入及び定期的な評価状況の公表の実施

並びに本報告書に記載された解決の方向性と具体的方策の内容の見直し・更新を検討する。【政府が実施】

(2) 今後さらに検討すべき課題

本委員会は、企業・個人の情報セキュリティ対策の強化のための具体的方策を検討してきたが、以下の課題については、さらに時間をかけて結論を得ることが妥当であると思料されることから今後さらに検討すべき課題として提示し、政府の検討・取組みを促すこととする。

ア グローバル(国際的)な視点からの情報セキュリティ対策の検討

情報セキュリティ政策は、情報セキュリティの脅威に国境がないことから、一国で完結するものではなく、関係国で密接に協調して政策を平準化して、実施する必要性が高い。

企業・個人にあっても、国際社会にその責任を負っていることを自覚し、IT 基盤を利活用していくことが求められる。

しかしながら、ここでこれまで述べてきた方策は、我が国の中で実施されるものが中心であったことから、今後は、現時点で国際的に見てより進んだ取組みを行っている国との情報交流や情報共有を進めつつ、国際社会におけるセキュリティ文化の平準化、セキュリティに関する国際規範として重要な位置を占める国際標準開発への貢献と我が国事情の反映、セキュリティに関する JIS 規格の整備、さらには国際社会におけるセキュリティ文化の一層の醸成に向けた我が国としての取組みを行うべく、政府はさらに検討すべきである。

(参考) 有害情報問題

インターネット上には様々な情報が散在しているところ、社会にとって有用な情報と同時に社会に悪影響を及ぼしかねない情報も存在する。

たとえば、サイバー犯罪の具体的手法を知ることができる又は犯罪に利用されやすいツールをダウンロードできるサイト、青少年に悪影響を及ぼしかねないアダルト・サイト、自殺希望者が集まり集団自殺の実行を助長するサイト等、違法ではないが有害といえる情報が国内外において広く存在するところである。

有害情報問題、すなわち、これらのサイトへの対応は、表現の自由との関係や世界各国の文化的・経済的・政治的背景の違い等から、困難な問題である。しかしながら、有害情報問題は情報セキュリティ対策と関連を持つ部分もあり、政府は、この問題への取組みについての検討を行っているところ、今後とも検討を継続していくべきである。

(別紙 1) 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
セキュリティ文化の普及に向けて
(2002年7月25日)
(外務省仮訳)

はしがき

現在の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 - セキュリティ文化の普及に向けて - は、2002年7月25日の第1037回会合でOECD理事会の勧告として採択された。

はじめに

OECDが初めて「情報システムのセキュリティのためのガイドライン」を発表した1992年以来、情報システム及びネットワークの利用と情報技術を取りまく全体的な環境は、劇的に変化してきた。これらの継続的な変化は、大きな利益をもたらす一方、情報システム及びネットワークを開発、所有、提供、管理、サービス提供及び使用する政府、企業、その他の組織及び個人利用者(「参加者」)がセキュリティを一層重視することを要求している。

一層強力になるパーソナルコンピュータ、技術の収れん、及びインターネットの広範な利用が、主として閉鎖的だったネットワークにおける地味で外部との接続のないシステムに取って代わった。今日、参加者の相互接続は増加し、その接続は国境を越えている。加えて、インターネットは、エネルギー、交通及び金融のような重要インフラを支え、企業がビジネスを行い、政府が市民及び企業にサービスを提供し、また、個々の市民が通信し情報交換する方法において主要な役割を果たしている。通信及び情報インフラを構成する技術の性質及び方式も著しく変化してきた。通信及び情報インフラに対するアクセス機器の数が増加するとともに、その性質も多様化し、固定型、ワイヤレス型及びモバイル型の機器が含まれるようになり、また、「常時」接続によるアクセスの割合が増大している。その結果、交換される情報の性質、量及び取扱いの注意度が大きく拡大してきた。

相互接続の増加の結果として、情報システム及びネットワークは、今や一層増加し、かつ多様化している脅威及び脆弱性にさらされている。これは、セキュリティに関する新しい課題を提起している。これらの理由により、このガイドラインは、新しい情報社会のすべての参加者に適用され、セキュリティの課題に対する一層の認識及び理解の必要性、並びに「セキュリティ文化」を発展させることの必要性を提唱する。

I. セキュリティ文化の普及に向けて

このガイドラインは、セキュリティ文化(すなわち、情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること)の発展を促進

することによって、絶えず変化を続けるセキュリティの環境に対応するものである。このガイドラインは、ネットワーク及びシステムの安全な設計及び利用が後知恵の結果であったことが余りにも多かった時代との明確な決別の合図である。参加者は情報システム、ネットワーク及び関連するサービスに一層依存するようになっており、これらすべてが信頼でき、かつ安全なものであることが必要となっている。すべての参加者の利益、並びにシステム、ネットワーク及び関連するサービスの性質を適切に考慮したアプローチのみが、効果的なセキュリティを提供し得る。

各参加者は、セキュリティを確実にするための重要な担い手である。参加者は、自らの役割に応じて、関連するセキュリティリスクと予防の手段を認識し、責任を持って、情報システム及びネットワークのセキュリティを強化するための措置をとるべきである。

セキュリティ文化を普及させるためには、リーダーシップと広範な参画の双方が必要となる。また、セキュリティ文化の普及により、すべての参加者の間でセキュリティの必要性が理解されるとともに、セキュリティの計画及びマネジメントに高い優先順位が与えられるべきである。セキュリティの課題は、政府及び企業のすべてのレベルにとって、またすべての参加者にとって関心を持ち、責任を持つべき事項である。このガイドラインは、社会全体でセキュリティ文化の普及に向けた取り組みが行われるための基礎をなすものである。これにより、参加者がすべての情報システム及びネットワークの設計及び利用にセキュリティを組み込むことが可能になる。このガイドラインは、すべての参加者が、情報システム及びネットワークの運用について考え、評価し、影響を与える方法として、セキュリティ文化を取り入れ、普及することを提案する。

II . 目的

このガイドラインは次に掲げることを目的とする。

- 情報システム及びネットワークを保護する手段として、すべての参加者の間にセキュリティ文化を普及させること。
- 情報システム及びネットワークに対するリスク、それらのリスクに対処するために有効な方針、実践、手段及び手続並びにそれらの導入及び実施の必要性について、認識を高めること。
- すべての参加者の間に、情報システム及びネットワーク並びにそれらの提供及び利用の形態における一層大きな信頼を醸成すること。
- 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首尾一貫した方針、実践、手段及び手続の開発並びに実施において、参加者のセキュリティの課題に関する理解及び倫理的価値の尊重を助ける全般的な考え方の枠組みを創造すること。
- セキュリティの方針、実践、手段及び手続の開発並びに実施においてすべての参加者の間の協力及び情報共有を適切に促進すること。
- 標準類の策定及び施行に関与するすべての参加者の間で重要な目的としてセキュリティが考慮されることを促進すること。

III . 原則

次の9つの原則は互いに補い合うものであり、一体のものとして読まれるべきである。それらは、方針及び運用のレベルを含む、すべてのレベルで参加者に関係する。このガイドラインの下で、参加者の責任は、彼らの役割に応じて変化する。すべての参加者は、セキュリティのより良い理解及び実践の採用を導き得る認識、教育、情報共有及び訓練によって助けられる。情報システム及びネットワークのセキュリティを強化させる努力は、民主主義社会の価値、特に公開された自由な情報の流通の必要性及び個人のプライバシーに対する基本的な関心と合致すべきである。

(1) 認識 (Awareness)

参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。

リスクと利用可能な安全防護措置に関する認識が、情報システム及びネットワークのセキュリティにとっての最初の防衛線である。情報システム及びネットワークは、内部及び外部双方のリスクによって影響を受けるおそれがある。参加者は、セキュリティ面での障害が自らの管理下にあるシステム及びネットワークに著しい損害を与えるおそれがあることを理解すべきである。参加者は、また、相互接続及び相互依存の結果として他者に損害を与えるおそれがあることを認識すべきである。参加者は、自らのシステムの構成及びそのシステムのために利用可能な更新情報、ネットワークの中での位置づけ、セキュリティを強化するために自らが実施し得る良い慣行、並びに他の参加者のニーズを認識すべきである。

(2) 責任 (Responsibility)

すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

参加者は、相互接続されたローカルな、及びグローバルな情報システム及びネットワークに依存しており、情報システム及びネットワークのセキュリティに対する自らの責任を理解すべきである。参加者は、個々の役割にふさわしい方法で、責任を負うべきである。参加者は、自らの方針、実践、手段及び手続を定期的に見直し、それらが自らの環境に適したものであるか否かを評価すべきである。製品若しくはサービスを開発、設計又は供給する者は、システム及びネットワークのセキュリティに取り組み、利用者が製品又はサービスのセキュリティ機能及びセキュリティに関する自らの責任をよりよく理解できるように、適切な時期に、更新情報を含む適切な情報を頒布すべきである。

(3) 対応 (Response)

参加者は、セキュリティの事件に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。

情報システム及びネットワークが相互接続されていること並びに急速でかつ広範な被害の可能性のあることを認識し、参加者はセキュリティの事件に対処するために、適切な時期に協力的な方法で行動すべきである。参加者は脅威及び脆弱性についての情報を適切に

共有するとともに、セキュリティの事件に対する予防、検出及び対応を目的とした迅速で効果的な協力を行う手続を整備すべきである。なお、許容される場合には、これらの行動に国境を越えた情報の共有と協力を含めることができる。

(4) 倫理 (Ethics)

参加者は、他者の正当な利益を尊重すべきである。

情報システム及びネットワークが我々の社会に普及していることから、参加者は自らの作為又は不作為が、他者に損害を与えるおそれがあることを認識する必要がある。それゆえ、倫理的な行動が極めて重要であり、参加者は、ベストプラクティスの形成及び採用に努め、かつセキュリティの必要性を認識し他者の正当な利益を尊重する行動を促進することに努めるべきである。

(5) 民主主義 (Democracy)

情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。

セキュリティは、思想及び理念を交換する自由、情報の自由な流通、情報及び通信の秘密、個人情報の適切な保護、公開性及び透明性を含む、民主主義社会によって認識される価値と合致する方法で実施されるべきである。

(6) リスクアセスメント (Risk assessment)

参加者は、リスクアセスメントを行うべきである。

リスクアセスメントは、脅威と脆弱性を識別するものであり、技術、物理的及び人的要因、方針並びにセキュリティと関わりを持つ第三者のサービスのよう、重要な内的及び外的要因を包含できるよう十分に広範であるべきである。リスクアセスメントは、保護すべき情報の性質と重要性に照らして、リスクの許容できるレベルの決定を可能にし、情報システム及びネットワークに対する潜在的な損害のリスクを管理するために、適切な制御を選択することを支援する。情報システムの相互接続が増加しているため、リスクアセスメントは、他者に起因する、また、他者に対してもたらされる潜在的な損害についての考慮を含むべきである。

(7) セキュリティの設計及び実装 (Security design and implementation)

参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。

システム、ネットワーク及び方針は、セキュリティを最適なものとするために、適切に設計され、実装され、かつ調和が図られる必要がある。この努力の主要な、しかし唯一ではない焦点は、識別された脅威及び脆弱性から生じる潜在的な損害を、回避又は限定するための、適切な安全防護措置及び解決策を設計し、採用することにある。技術的及び非技術的安全防護措置及び解決策が必要であり、かつ、これらは組織のシステム及びネットワーク上の情報の価値と比例するべきである。セキュリティは、すべての製品、サービス、システム及びネットワークの基本的要素であるべきであり、システムの設計及び構造に不

可欠な部分であるべきである。エンドユーザにとって、セキュリティの設計及び実装とは、主として自らのシステムのために製品及びサービスを選択し、構成することである。

(8) セキュリティマネジメント (Security management)

参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。

セキュリティマネジメントは、参加者の活動のすべてのレベル及び運用のすべての局面を包含しリスクアセスメントに基づき、かつ、動的であるべきである。セキュリティマネジメントは、出現する脅威に対する将来を見越した対応を含み、事件・事故の予防、検出、対応、システムの復旧、継続的な保守及び監査を扱うべきである。情報システム及びネットワークのセキュリティの方針、実践、手段及び手続は、首尾一貫したセキュリティシステムの創造のために調和が図られ、統合されるべきである。セキュリティマネジメントの要件は、関与のレベル、参加者の役割、含まれるリスク及びシステムの要件に依存する。

(9) 再評価 (Reassessment)

参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

新しく、かつ変化する脅威及び脆弱性が絶えず発見されている。参加者は、これらの展開するリスクに対処するために、セキュリティのすべての局面のレビュー、再評価及び修正を継続的に行うべきである。



General Assembly

Distr.: General
31 January 2003

Fifty-seventh session
Agenda item 84 (c)

Resolution adopted by the General Assembly

[on the report of the Second Committee (A/57/529/Add.3)]

57/239. Creation of a global culture of cybersecurity

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the information society,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Aware also that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society,

Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity through the support of national efforts aimed at the enhancement of

human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all,

Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies,

1. *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;

2. *Invites* all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;

3. *Invites* Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005;

5. *Stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity.

*78th plenary meeting
20 December 2002*

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks (“participants”) must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(a) *Awareness*. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(b) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(c) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(d) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(e) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(f) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(g) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(h) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(i) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

(参考) セキュリティ文化専門委員会報告書までの検討の経緯

【情報セキュリティ政策会議】

2005年 7月14日 第1回会合

セキュリティ文化専門委員会及び技術戦略専門委員会の設置
について

2005年 9月15日 第2回会合

「第1次情報セキュリティ基本計画(仮称)」の骨子と方向
性について

【情報セキュリティ政策会議セキュリティ文化専門委員会】

2005年 8月10日 第1回会合

- (1) セキュリティ文化専門委員会及び技術戦略専門委員会の設置について
- (2) 会議の公開等について
- (3) 情報セキュリティ政策会議の概要について
- (4) セキュリティ文化に関する問題意識について
- (5) 「我が国にとってのセキュリティ文化とは何か」ということについての検討

2005年 9月 9日 第2回会合

セキュリティ文化醸成のための方向性の検討

2005年10月 5日 第3回会合

セキュリティ文化専門委員会報告書骨子(案)の検討

2005年10月25日 第4回会合

セキュリティ文化専門委員会報告書(案)の検討