OECD 情報セキュリティガイドライン

見直しに関する調査

調査報告書

本資料は2003年5月に公開した資料ですが、
原典が2015年10月に改訂されましたので、
本資料は歴史的資料としてのみご利用ください。

情報処理振興事業協会
セキュリティセンター

はじめに

OECD（Organisation for Economic Cooperation and Development：経済協力開発機構）では、ネットワーク社会の発達に伴い、安全で信頼性の高い電子商取引の環境を整備する観点から 1992 年に「OECD 情報セキュリティに関するガイドライン（OECD Guidelines for the Security of Information Systems）」を制定している。本ガイドラインは 5 年ごとの見直しが決まっているが、2002 年が 2 回目の見直しの時期にあたり、OECD に設置された専門家による会合において、見直しの検討作業が進められてきた。

昨年度、IPA では、「OECD 情報セキュリティガイドライン見直しに関する研究会」を開催し、国内専門家らによる検討を行った。2001 年 9 月には「OECD 情報セキュリティに関するワークショップ」を東京で開催し、政府、産業界、学術界、消費者団体等の情報セキュリティに携わる専門家を中心に活発な議論が行われた。

上記研究会では、ガイドライン見直しに向けて、我が国としての対処方針の検討を行った。検討にあたっては、情報セキュリティに関わる実態や他のガイドライン等の状況を整理するとともに、国内関係機関へのヒアリングを実施し、意見の反映に努めた。

本年度においても研究会を継続し、見直しの方向性とそれに基づく我が国の対処方針を維持しつつ、OECD 会合における改訂作業において我が国の対処方針のインプットを図ってきた。その結果、2002 年 7 月 25 日の OECD 理事会において新しいガイドラインである「OECD 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（OECD Guidelines for the Security of Information Systems and Networks : TOWARDS A CULTURE OF SECURITY）」が承認されたところである。

本調査は、新ガイドラインが策定されたことを踏まえて、ガイドライン見直しの経緯や新しいガイドラインの概要等についてまとめるものである。あわせて、新ガイドラインに基づく我が国の実施方策案、新ガイドラインの普及施策並びに 2003 年以降の情報セキュリティに関する OECD ワークプログラムに対する我が国の提案の論点について整理する。

－ 目　　次 －

１．OECD 情報セキュリティガイドラインの見直しについて

OECD 情報セキュリティガイドラインの見直し作業は、OECD の WPISP（Working Party on Information Security and Privacy）及びその専門家会合により 2001 年に着手され、2002 年 7 月 25 日の OECD 理事会にて新しいガイドライン「OECD 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（OECD Guidelines for the Security of Information Systems and Networks : TOWARDS A CULTURE OF SECURITY）」が承認された。本章では、新ガイドラインの見直しの経緯及びその概要、並びに本年度の「OECD 情報セキュリティガイドライン見直しに関する研究会」の活動状況について報告する。

１．１ OECD 情報セキュリティガイドラインの見直し

１．１．１ 経緯とガイドラインの構成

OECD 情報セキュリティのためのガイドラインは、1992 年情報システムセキュリティガイドラインに関する理事会（THE COUNCIL concerning Guidelines for the Security of Information Systems）による勧告及びその付属文書として発表された。発表当時においては、情報システムのセキュリティに関する各国政府・公共部門及び民間機関の組織的かつ整合性のとれた協調的対応を可能とする枠組みを示す文書として登場したものとしては早い方に属する。

ガイドライン制定のため 1991 年 1 月に専門家会議が組織され、以後合計 6 回の専門家会議での検討を経て、1992 年 11 月 26 日の理事会においてガイドラインは勧告として正式に採択された。

勧告本文の第 5 項には、5 年毎にガイドラインの見直しを行う旨が記されており、これにより、1997 年に第 1 回の見直し作業がおこなわれた。見直し作業の結果は、変更の必要なし、ということであった。

制定後 10 年目にあたる 2002 年の第 2 回の見直しでは、大幅な改訂が行われた。見直し作業は 2001 年 12 月以後 4 回開催された WPISP の専門家グループ会議により起草され、2002 年 3 月以後 3 回の WPISP 会議での討議を経て 2002 年 7 月 25 日の第 1037 回会合で OECD 理事会の勧告として採用された。2001 年 9 月 11 日のアメリカ合衆国における同時多発テロの発生を受け、改訂ガイドラインの検討と発表は当初のスケジュールを前倒しで実施する形で行われた。2002 年版の正式名称は、「OECD 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（OECD Guidelines for the Security of Information Systems and Networks : TOWARDS A CULTURE OF SECURITY）」である。

1992 年版ガイドラインは、「勧告本文」、付属文書としての「ガイドライン」、および付録としての「説明のための覚書」の 3 部構成であったが、2002 年版では、「説明のための覚書」はなくなっている。

特に、1992 年当時は、インターネットの商用利用が公式に認められるようになるかなら

ぬかの瀬戸際の頃であり、一般の人々の情報システムおよびネットワークのセキュリティに関する知識の普及の不足や関心の低さを反映して、ガイドラインそのものの意義やガイドライン中に述べられている 9 つの原則に対して、それを原則として掲げなければならない情勢や必要性を説明する詳細な「説明のための覚書」を準備しておかなければならなかった状況があった。2002 年版においては、既にそのような改めての説明は敢えて必要とはしないとするところに、情報社会の状況の変化を見て取ることができる。

1992 年版においては、「情報セキュリティとは何か」について、「所謂 CIA（情報システムの Confidentiality、Integrity、Availability）の欠如に起因する危害から情報システムを利用するユーザを守ること」という定義を述べ、情報セキュリティの概念を確固とするところから出発したが、その後 10 年間の情報システムとネットワークの技術的進展や応用の深まりは、情報セキュリティの把握の仕方において上記 CIA の確保に留まるものではなくなっていることを認識させるに到っている。従って、2002 年版においては、「情報セキュリティ」を現象面から捉える定義は行なわず、「セキュリティの文化」という概念を提示し、情報システムとネットワークを人間社会の活動を主に捉えた上での総合的な把握を目指しているようである。

１．１．２ 改訂の方向

（1）1992 年版の概観

1992 年版ガイドラインでは、情報システムの価値、利用の世界的な高まりを受け、ネットワーク化の進展に伴う世界的な広がりと社会全体の情報システムに対する依存性の増加に伴い、情報システムの信頼性を高める特別な取り組みが必要である、と指摘し、そのために、適正なセキュリティ措置のない情報システムの脆弱性がもたらすリスクへの対処、および、情報システムに関わる種々の権利・義務の内容を明確にし、もって、情報システムセキュリティを推進する共通の利益に関する国際協調を進めたいとの認識のもと、勧告をおこなっている。

勧告本文の中では、情報システムのセキュリティについての一般の理解を深めるために、基本概念として「可用性：Availability」、「機密性：Confidentiality」、「完全性：Integrity」を説明(注)し、この 3 概念を使って情報セキュリティの目的を「情報システムセキュリティの目的は、情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護することである。」と定義している。

（注：可用性：データ、情報、情報システムが、適時に、必要な様式に従い、アクセスでき、利用できること。機密性：データ及び情報が、権限ある者が、権限ある時に、権限ある方式に従った場合のみ開示されること。完全性：データ及び情報が正確（accurate）で完全（complete）であり、かつ正確さ（accuracy）、完全さ（completeness）が維持されること）

情報セキュリティの概念をこのように捉えた上で、公共部門・民間部門のすべての情報システムに適用されるガイドラインとして、次の 9 つの原則を掲げている。

① **責任の原則**（Accountability Principle ）

情報システムの所有者、提供者、利用者その他情報システムセキュリティに関わる者の任務および責任を明確にすべきである。

② **認識の原則**(Awareness Principle)

情報システムへの信頼を高めるため、情報システムの所有者、提供者、利用者その他関係者は、セキュリティ維持と矛盾のないように、情報システムセキュリティのための手段、慣行および、手続の存在と、およその範囲について容易に適切な知識を得ることができるようにすべきであり、また、知らされるべきである。

③ **倫理の原則**(Ethics Principle)

情報システムおよび情報システムセキュリティは、他の者の権利と合法的な利益を尊重して提供され利用されるべきである。

④ **多面的考慮の原則**(Multidisciplinary Principle)

情報システムセキュリティのための手段、慣行および、手続は、技術、行政、組織、運営、営業、教育および、法律を含むその問題に関連するあらゆる考え、視点を考慮し、斟酌すべきである.

⑤ **比例の原則**(Proportionality Principle)

セキュリティへの要求は、個々の情報システムによって異なるのであって、セキュリティのレベル、コスト、手段、慣行および、手続は、適正であり、かつ情報システムの価値と要求される信頼度、セキュリティが破れた場合の被害の深刻度、発生の可能性、広がりに比例したものであるべきである。

⑥ **統合の原則**(Integration Principle)

情報システムセキュリティのための手段、慣行および、手続は、一貫したシステムセキュリティ創出のため、相互に、かつ、組織内の他の手段、慣行および、手続と調和的、統合的に行われるべきである。

⑦ **適時性の原則**(Timeliness Principle)

情報システムセキュリティへの侵害を防止し、かつ、それに対応するため、公共部門および民間部門は、国内・国際の両レベルにおいて、時宜に応じ協調的に行動すべきである。

⑧ **再評価の原則**(Reassessment Principle)

情報システムおよびそれに対するセキュリティの要求は時と共に変わるため、情報システムセキュリティは定期的に再評価されるべきである。

⑨ 民主主義の原則(Democracy Principle)

情報システムセキュリティは、民主主義社会におけるデータと情報の合法的な利用および流通と整合のとれたものとすべきである。

各原則の間に対象読者の不統一感（対象読者は情報システムの開発者か、所有者か、提供者か、管理者か、利用者か）や、記述粒度の不統一感は見て取れるが、これら 9 原則は 2002 年版で再構成され、その精神は継承されている。

更に、勧告文には実施施策として、政府及び公共部門、民間部門は、情報システムを保護し、このガイドラインの原則に従ったセキュリティを提供するため、情報システムに関する「政策」、「教育及び訓練」、「法の執行及び補償」、「情報の交換」、「協力」の 5 分野において努力すべきであるとしている。

（2）2002 年版の改訂のポイント

2002 年改訂版では、従来のガイドラインと比べて、以下のような点が新しくなっている。

（ａ）「セキュリティ文化」の提唱

2002 年改訂版では、情報セキュリティの重要性を広く認識させるために、「セキュリティ文化（a culture of security）」という新しい概念を提唱している。「セキュリティ文化」を「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」と定義し、これを取り入れ、普及することを提案するとともに、このガイドラインを「セキュリティ文化」の普及に向けたものと位置付けている。

（ｂ）情報通信ネットワーク社会を前提

従来のガイドラインでは、主として情報システムを対象としていた。近年のインターネットの浸透や携帯電話などの新しい通信手段の普及を受け、新ガイドラインは、名称を「Guidelines for the Security of Information Systems and Networks」とするなど、情報通信ネットワーク社会を前提とした内容になっている。

（ｃ）個人を含むすべての参加者が責任を負う

従来のガイドラインでは、対象者として政府や企業を主に念頭に置いていたが、新ガイドラインでは、個人も含めて情報セキュリティに関わる人すべてを「参加者（participants）」（注）と呼び、すべての参加者が責任を負うことを規定している。

（注）新ガイドラインでは、「参加者」を「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」としている。

（d）情報セキュリティマネジメントの概念の導入

情報システムやネットワークを取り巻く環境の変化は激しく、絶えず新たな脅威が出現している。情報セキュリティを確保するためには総合的な対策を選択、実施し、継続的に改善していくことが重要である。新ガイドラインでは、このような情報セキュリティマネジメントの概念を導入し、「セキュリティマネジメントの原則」を新たに設けたほか、「リスクアセスメントの原則」「セキュリティの設計及び実装の原則」「再評価の原則」といった、情報セキュリティマネジメントのプロセスに関連する原則を規定している。

（e）従来のガイドラインとの対応関係

従来のガイドラインにおける各原則は、図 1-1のような対応関係により、新ガイドラインに取り入れられている。

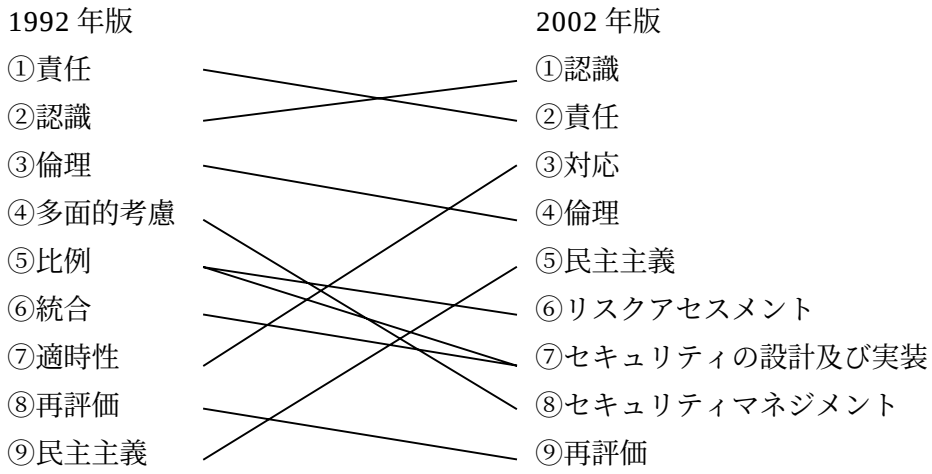

図 1-1　従来ガイドラインと新ガイドラインの原則の対応関係

１．１．３ 新ガイドラインの概要

１．１．３．１ 目的

ガイドラインは次の 6 項目を勧告の目的として掲げている。

（1）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。
（2）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。
（3）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。
（4）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。
（5）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、すべての参加者間の協力及び情報共有を適切に促進すること。
（6）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。

「セキュリティ文化」とは、前節に紹介した通り、「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」であり、それを受けて、このガイドラインは、情報システムとネットワークを、所有し、開発し、利用し、管理するすべての参加者に、それが現代社会に有する重要性の理解の上で「セキュリティ文化」の意識をもたせることを目的としている。この情報システムとネットワークの重要性については、「１．１．３．２ 状況認識」に表現されている。また、このガイドラインの意味を、ネットワーク及びシステムの安全な設計及び利用が余りにもしばしば後追いでしか作られていなかった時代との明確な決別の合図であるとして、情報セキュリティの積極的な創生を提唱している。

１．１．３．２ 状況認識

ガイドラインは、次の 9 項目を、勧告するに当っての状況認識としている。

（1）情報システム及びネットワークは、政府、企業、その他の組織及び個人利用者にとってその利用と価値がますます増大していること
（2）情報システム及びネットワークの役割が重要性を増し、また、安定的で効率的な国内経済及び国際貿易のために情報システム及びネットワークへ依存すること、また社会的、文化的及び政治的生活において情報システム及びネットワークへ依存することが一層増大していることが、情報システム及びネットワークにおける信

頼を保護し促進する特別な努力を要求していること

（3）情報システム及びネットワーク、並びにそれらの世界的な急増が、新しく、かつ増加し続けるリスクを伴ってきていること

（4）情報システム及びネットワークを経由して保存され、伝送されるデータや情報は、様々な手段による権限のないアクセス、利用、横領、変更、悪意のあるコード伝送、サービスの妨害、又は破壊の脅威にさらされており、適切な安全防護措置が求められていること

（5）情報システム及びネットワークのリスク並びにそのリスクに対応するために利用可能な方針、実践、手段及び手続についての認識を高める必要があること、並びにセキュリティ文化の発展に向けた決定的な措置としての適切な行動を奨励する必要があること

（6）現在の方針、実践、手段及び手続を、それらが情報システム及びネットワークに対する脅威によってもたらされる難題の展開に確実に対応するように、見直す必要があること

（7）「セキュリティ文化」は、セキュリティ面での障害から生じる潜在的な損害によってもたらされる、国内経済及び国際貿易、並びに社会的、文化的及び政治的な生活への参画に対する難題に対応するための国際的な調整及び協力を促進するものであり、この「セキュリティ文化」によって情報システム及びネットワークのセキュリティを促進することに共通の利益が存在すること

（8）また、更に、この勧告の付属文書に規定される「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」は強制的なものではなく、国家の主権に影響を及ぼさないこと

（9）このガイドラインは、セキュリティのためにある一つの解決策が存在すること、又はある特別な状況に適した方針、実践、手段及び手続が何であるかを提案することを意図するものではなく、参加者が、どのようして「セキュリティ文化」の発展から利益を得、また、その発展にどのように貢献するかについてより良い理解を促すために、原則の枠組みを提供するものであること

１．１．３．３ 原則

上記 6 目的と 9 状況認識のもと次の 9 原則を掲げている。

（1）認識の原則（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。
Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

情報セキュリティを確保するためには、リスクと安全防護措置について認識することがまず必要である。情報システムやネットワークはつねに組織内外のリスクにさらされており、セキュリティ面での障害は自らの情報システムのみならず、他人にも損

害を与えることになることを認識するべきである。

利用する情報システムの構成がどうなっていてネットワーク内でどういう位置付けにあるのか、更新情報（ソフトウェアの修正パッチ等）をどうすれば利用できるのか、実施可能な対策はあるのか、他の参加者が何を求めているのかを認識するべきである。

（2）責任の原則（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。
All participants are responsible for the security of information systems and networks.

参加者は、相互接続された情報システムやネットワークのセキュリティに関する自らの責任を理解するとともに、個々の役割にふさわしい方法で責任を負うべきである。またセキュリティの方針、手段等は定期的に見直し、それらが適切か否かを評価するべきである。

IT 製品やサービスの開発者等は、情報システムやネットワークのセキュリティに取り組むとともに、利用者が製品やサービスのセキュリティ機能と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、更新情報を含む適切な情報をタイムリーに提供するべきである。

（3）対応の原則（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。
Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

参加者は、情報システムやネットワークが相互接続されていることにより急速で広範な被害が生じるおそれがあることを認識し、セキュリティ上の事件（不正アクセス等）に対してタイムリーに協力するべきである。

また参加者は、脅威や脆弱性の情報の共有や不正アクセスの予防、検出、対応のための協力関係を築くべきである。

（4）倫理の原則（Ethics）

参加者は、他者の正当な利益を尊重するべきである。
Participants should respect the legitimate interests of others.

情報システムやネットワークが社会に普及していることから、自らの行為が他人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。それゆえに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と採用に努め、セキュリティの必要性を認識するとともに、他人の正当な利益を尊重することに努めるべきである。

（5）民主主義の原則（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。
The security of information systems and networks should be compatible with essential values of a democratic society.

セキュリティは、思想や理念を交換する自由、情報の自由な流通、情報・通信の秘密、個人情報の適切な保護、公開性・透明性といった、民主主義社会において認められる価値と合致するような方法で実践されるべきである。

（6）リスクアセスメントの原則（Risk assessment）

参加者は、リスクアセスメントを行うべきである。
Participants should conduct risk assessments.

リスクアセスメントとは、セキュリティ上の脅威と脆弱性を識別し、リスクの許容できるレベルの決定やリスクを管理するための措置の選択を支援するものである。リスクアセスメントは、技術、物理的・人的な要因、セキュリティの方針（ポリシー）、セキュリティと関わりを持つ第三者のサービスといった、内外の要因を広く含むものであるべきである。

また、他人から受ける、又は、他人に対して与える、潜在的な損害についても考慮するべきである。

（7）セキュリティの設計及び実装の原則（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。
Participants should incorporate security as an essential element of information systems and networks.

情報システム、ネットワーク及びセキュリティの方針（ポリシー）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。適切な安全防護措置や解決策の設計・採用が重要で、これらは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、情報システムやネットワークの設計・構造に不可決な部分であるべきである。

一方、エンドユーザの場合は、自分が使用するシステムのために、適切な製品やサービスを選択し、構成するべきである。

（8）セキュリティマネジメントの原則（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。
Participants should adopt a comprehensive approach to security management.

情報セキュリティマネジメントは、参加者の活動のすべてを含む包括的で、動的なものであるべきである。また情報セキュリティマネジメントには、セキュリティ上の事件の予防、検出、対応やシステムの復旧、保守、レビュー、監査等が含まれるべきである。

セキュリティの方針（ポリシー）、手段等は、首尾一貫したセキュリティシステムを構築するために調和が図られ、統合されるべきである。

（9）再評価の原則（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。
Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

新たな脅威や脆弱性が絶えず発見されている。参加者は、これらのリスクに対処するために、セキュリティのすべての面のレビュー、再評価を行うとともに、セキュリティの方針（ポリシー）、手段等を適切に修正する必要がある。

１．２ OECD 情報セキュリティガイドライン見直しに関する研究会について

OECD 情報セキュリティガイドラインの見直し作業にあたって、国内の検討組織として「OECD 情報セキュリティガイドライン見直しに関する研究会」を開催した。上記研究会では、見直しに向けた我が国対処方針の検討のほか、新ガイドラインの制定後は、その仮訳案の作成並びに実施方策案の検討等の活動を行なった。以下に、研究会の構成及び活動経緯について整理する。

１．２．１ 研究会委員

上記研究会の委員及び事務局は以下のとおり。

（委員はアイウエオ順、所属・肩書きは第１回委員会開催時のもの）

（委員）

石田　喬也	三菱電機（株）　開発本部顧問（ＢＩＡＣ日本代表窓口）
歌代　和正	(株)インターネットイニシアティブ　システム技術部部長
佐野　晋	（社）日本ネットワークインフォメーションセンター　理事
土居　範久	慶應義塾大学理工学部情報工学科　教授（座長）
苗村　憲司	慶應義塾大学環境情報学部　教授
中尾　康二	（株）ＫＤＤＩ研究所　コンピュータセキュリティグループグループリーダー
中原　志郎	日本電信電話（株）　第五部門担当部長
西尾　秀一	ＮＴＴデータ・セキュリティ（株）　コンサルティング部長
堀部　政男	中央大学法学部教授
丸橋　透	富士通（株）法務・知的財産権本部法務部　法務企画部担当課長
室町　正実	弁護士（東京丸の内法律事務所）
山口　英	奈良先端科学技術大学院大学情報科学研究科教授

（事務局）

大野　秀敏	経済産業省 商務情報政策局 情報セキュリティ政策室長
山本　文土	経済産業省 商務情報政策局 情報セキュリティ政策室 課長補佐
金澤　祐治	経済産業省 商務情報政策局 情報セキュリティ政策室 技術係長
矢田　健一	情報処理振興事業協会 セキュリティセンター
宮川　寧夫	情報処理振興事業協会 セキュリティセンター
佐藤　能行	（株）富士総合研究所 情報セキュリティ評価研究室
冨田　高樹	（株）富士総合研究所 情報セキュリティ評価研究室
佐久間　敦	（株）富士総合研究所 情報セキュリティ評価研究室

１．２．２ 研究会及び OECD 会合等の開催状況

表 1-1 に研究会及び国内の動向並びに OECD 会合等の開催状況について示す。

表 1-1　国内研究会及び OECD 会合等の開催状況（2001.12～2003.1）

年月日	国内	OECD 会合等
2001 年 12 月 10 日, 11 日		専門家会合（第 1 回） - 新ガイドラインの審議着手
2002 年 2 月 12 日, 13 日	―	専門家会合（第 2 回） - 新ガイドラインの審議
3 月 4 日	―	専門家会合（第 3 回） - 新ガイドラインの審議
3 月 5 日, 6 日	―	WPISP - 新ガイドラインの審議
3 月 6 日	―	専門家会合（第 4 回） - 新ガイドラインの審議
4 月 22 日, 23 日		WPISP - 新ガイドラインの審議
5 月 31 日	第 1 回研究会	―
6 月 25 日, 26 日	―	WPISP 臨時会合 - 新ガイドラインの承認（英語版、仏語版） - 実施計画案、及びコミュニケーション計画案の審議
6 月 26 日	―	ICCP 臨時会合 - 新ガイドラインの承認
7 月 23 日	第 2 回研究会	―
7 月 25 日	―	OECD 理事会 - 新ガイドラインの承認
9 月	経済産業省、外務省等より新ガイドラインの仮訳公表	―
2003 年 1 月 14 日～17 日	―	OECD-APEC Global Forum

(略語は６．３を参照)

１．２．２．１ 第 1 回研究会（2002 年 5 月 31 日）

第 1 回研究会における議題は以下の通り。

（1）ガイドライン改訂案について
（2）今年度の研究会の進め方について
（3）ガイドライン（改訂版）に関する実施方策の検討

１．２．２．２ 第 2 回研究会（2002 年 7 月 23 日）

第 2 回研究会における議題は以下の通り。

（1）Ad hoc WPISP Meeting／Ad hoc ICCP Meeting（6/24-26）報告
（2）ガイドライン改訂版及び仮訳の検討
（3）ガイドライン改訂版に関する実施方策の検討

１．２．３ 仮約の検討

新しい OECD 情報セキュリティガイドラインが 2002 年 7 月 25 日に OECD 理事会で承認されたことを受け、研究会において日本語仮約の検討を行なった。その後、経済産業省に研究会仮約案が提出され、関係省庁における審議を経て、2002 年 9 月に外務省より日本政府仮約として公表されている。対訳形式の仮約を６．１に示す。

また、仮約は以下の URL でも公開されている。

- 経済産業省ホームページ： http://www.meti.go.jp/policy/netsecurity/oecd2002.htm
- 外務省ホームページ： http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html

2．OECD 情報セキュリティガイドラインの実施方策

1992 年版 OECD 情報セキュリティガイドラインでは、政府及び公共部門、民間部門の情報セキュリティ保護に関して果たすべき事項として、以下観点から OECD 情報セキュリティガイドラインの各原則に掲げる理念を実施することを求めている。

- 政策
- 教育及び訓練
- 法の執行及び補償
- 情報の交換
- 協力

しかし、昨年度研究会における検討や関連団体へのヒアリング調査では、1992 年版 OECD 情報セキュリティガイドラインの国内における実施については、十分な成果を見たとは言い難いとの指摘も少なくなかった。これは主に以下の理由によるものと考えられる。

- OECD 情報セキュリティガイドライン自体の認知度の不足
- OECD 情報セキュリティガイドラインの対象とする者が明確でない
- 既存の制度、慣行や他のガイドライン等における参照の少なさ

一方、2002 年に改訂された OECD 情報セキュリティガイドライン（以下本章において、特に指定しない場合は、単に「新ガイドライン」と呼ぶ）では、各原則に沿った実施方策に関連する勧告として、

- 新たな方針、実践、施策、手続きの確立または既存のものの修正
- 国内／国外レベルでの調整／協調
- 公的／民間セクターへの新ガイドラインの普及
- 関連機関の責任の明確化と実施の奨励

といった項目を掲げており、具体的な政策や取り組みのレベルでの実施方策を通じて、各国が情報セキュリティに対する国際的な共通理念である「セキュリティ文化（culture of security）」を自国の中で醸成し、普及させていくことを求めている。

今年度 OECD セキュリティガイドライン研究会では、上記の OECD の勧告の方向性を踏まえ、我が国の民間部門／政府部門における、新ガイドラインの実効的な実施方策のあり方について検討を行った。

２．１ 実施方策の対象となる参加者（participants）について

新ガイドラインでは、「情報システム及びネットワークの開発、所有、提供、管理、サービス提供及び使用に関与し、情報セキュリティに重大な関心を払うべき者」として、以下のような例示をしている（PREFACE（序文）より）。

- 政府（governments）
- 企業（business）
- 組織（organization）
- 個人利用者（individual user）

実施方策の対象をより具体的に想定するため、本調査では、我が国における情報システムに関わる者の構成やその関与のし方を考慮し、表 2-1 に示す参加者に分類した。

表 2-1　情報システムに関わる参加者

参加者	具体例
(a) 政府	・ 中央省庁／地方自治体 ・ 関連機関
(b) ベンダー	・ ソフトウェア／ハードウェアメーカ ・ システムインテグレータ／システムコンサルタント ・ セキュリティ関連製品／サービスベンダー
(c) xSP	・ インターネットサービスプロバイダ（ISP） ・ アプリケーションサービスプロバイダ（ASP） ・ インターネットデータセンタ（iDC） ・ Web 運営者（ショッピングモール、オークションサイト等を含む）
(d)ユーザ	・ 企業／組織内の情報システム管理部門 ・ 企業／組織内の一般ユーザ ・ SOHO ユーザ ・ 個人ユーザ（一般世帯ユーザ）
(e) 地域／学界	・ 研究機関／学会 ・ 大学／大学院 ・ 初等／中等教育機関 ・ コミュニティ（NPO 等を含む）
(f) CSIRT	・ IRT（Incident Response Team：緊急対応チーム） ・ 情報セキュリティや情報システム／ネットワーク等に関連する業界団体 ・ 関連公的機関
(g) 国際機関	・ OECD ・ 関連国際機関

２．２ 各原則に対応した実施方策

新ガイドラインの定める各原則ごとに、実施方策として想定される項目、その実施方策に関わりをもつ参加者（participants）並びに各実施方策に関連する既存の取り組み等について整理する。

各原則に関わる実施方策として想定される項目は以下のとおりである。また、【】内は、実施方策として想定される各項目に関連する参加者を示す。

２．２．１ 認識の原則に関わる実施方策

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るべきである。
Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

（1）セキュリティ対策の必要性の広報、啓発【政府、ベンダー、xSP、地域／学界、ユーザ】

全ての参加者の間で、セキュリティに対する意識の向上させ、その対策の必要性について認識することがセキュリティ文化の普及の第一歩となる。そのために、セキュリティ対策の必要性に対する広報や啓発が不可欠である。

特に、政府においては、ベンダー、xSP、地域／学界等と協力しつつ、企業、学校及び個人のユーザに対して、情報セキュリティの普及啓蒙のための各種のイニシアティブを推進することが求められる。具体的な実施方策としては、セキュリティ対策に関するパンフットや CD-ROM 等を関係団体や自治体等を通じて配布することが考えられる。

また、個人ユーザにおいては、携帯電話やブロードバンドの浸透等を背景にパソコンやインターネットの利用者層が拡大していることから、個人ユーザに対するセキュリティ対策の必要性の啓発については、政府、ベンダー、xSP による取り組みのほか、地域の NPO やコミュニティによる支援が望まれる。

（関連する既存の取り組み）

- 「読者層別：情報セキュリティ対策実践情報（ソフトウェア開発者、情報システム部門責任者、システム管理者、エンドユーザー、SOHO、ネットワークサービス事業者）」（IPA）

（2）脆弱性、インシデントの情報提供【ベンダー、xSP、CSIRT】

ベンダーや xSP は、提供する製品／サービスの脆弱性やインシデントに関する情報と、セキュリティパッチを含む対策実践情報を適切なタイミングでユーザに提供することが求められる。

CSIRT は、脆弱性、インシデント等の状況の把握に努めるとともに、ユーザがこれらの情報にアクセスできるような環境を整備する必要がある。

（関連する既存の取り組み）

- ウイルス／不正アクセスの報告の受付と対策情報の提供（IPA）
- インシデントの報告の受付と対策情報の提供（JPCERT/CC）
- 「ネットワークセキュリティ脆弱性データベース（V-STAF）」（NPO 法人 ネットワークリスクマネジメント協会）

（3）教育（職員向け、一般向け）【政府、ベンダー、xSP、ユーザ、地域／学界】

政府や企業、組織のユーザは、情報システムやネットワークのユーザとして、自身の組織の職員や従業員に対して、セキュリティに関して必要な教育を行うことが必要である。ベンダー、xSP は、自身の提供する製品／サービスのユーザに対して、セキュリティのレベルが適正に保たれるように、必要に応じて情報の提供や教育・訓練の提供を行うべきである。

一方、セキュリティ文化をより広範に普及させるためには、初等中等教育の早い時期から、教育の機会が提供されることが望まれる。また、高齢者も含め幅広い層にパソコンやインターネットの利用が広まりつつあることから、自治体が実施する IT 講習会を含む地域における情報リテラシ教育等において、セキュリティに関する教育・訓練が提供されることが望まれる。また、個人ユーザの場合、セキュリティ対策について自らが学習することに努めることも含まれる。

2．2．2 責任の原則に関わる実施方策

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。
All participants are responsible for the security of information systems and networks.

（1）民事・刑事のルールの整備【政府、ベンダー、xSP、ユーザ、地域／学界】

政府は、情報セキュリティに関する民事及び刑事のルールの整備を推進することが求められる。特に、ベンダー、xSP に関しては、提供する製品／サービス等におけるセキュリティホールに関する役割・責任の見直しやハイテク犯罪の発生時における捜査当局への協力あり方（データの緊急保全等を含む）について、ルールの整備の機運が高まりつつある。関連する話題としては、知的財産権や個人情報保護の分野において、xSP 等ののユーザ（会員等）が第三者に対して行なった権利侵害や犯罪における、xSP の責任の範囲と制限についてのルール整備が進められている。

ルール整備にあたっては、セキュリティやハイテク犯罪は国境を超えて行なわれることもあることから、国際的に整合を図ることが必要である。ただし、ベンダーや xSP を含む事業者に過度の負担を負わせないように配慮がなされなければならない。

（関連する既存の取り組み）

- 「サイバー犯罪に関する条約」（欧州評議会 2001 年 11 月 8 日採択。我が国も同

年 11 月 23 日署名）
・ 「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（通称：プロバイダ責任法　2002 年 5 月施行）

（2）情報セキュリティマネジメントの実施【政府、ユーザ、（ベンダー、xSP）】

政府や企業、組織のユーザは、自身の情報資産（情報システム、ネットワーク、データ等を含む）の保護に対する責任がある。これらの者は、（必要のある場合はベンダーや xSP の支援を得て）適切なセキュリティポリシーを定め、各種の実践規範、セキュリティ対策手段及び手続等を整備し、実施していくことが求められる。上記の活動は、政府や企業、組織における情報セキュリティマネジメントの中に組み入れられるべきである。（セキュリティマネジメントの実施にあたっては、新ガイドラインの「セキュリティマネジメントの原則」を参照）

なお、個人ユーザの場合の情報セキュリティマネジメントとは、所有するパソコンへのウイルスソフト等の実装、といったセキュリティ対策の実施とその継続に相当する。

（関連する既存の取り組み）
・ 「ISMS 適合性評価制度」
・ 「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議　平成 12 年 7 月 18 日）
・ 「情報セキュリティポリシーサンプル」（NPO 法人 日本ネットワークセキュリティ協会）

（3）脆弱性、インシデントの情報提供【ベンダー、xSP】

脆弱性やインシデントの情報提供については、「認識の原則」においても実施方策として掲げているが、主として、ユーザに対してセキュリティ対策の必要性を啓発することがその目的である。

これに対して、「責任の原則」の観点からは、近年セキュリティホールを悪用したウイルスや不正アクセスが増加してきたことを背景に、製品／サービス等におけるセキュリティホールに対するベンダー、xSP の責任のあり方が問われている。

ベンダーや xSP は、セキュアな製品やサービスの開発及び提供に努めるとともに、セキュリティパッチの提供を含む時宜を得た情報提供を行うべきであり、責任の範囲や免責の要件等について、必要なルールの整備に政府等ともに主体的に取り組むべきである。

（関連する既存の取り組み）
・ ウイルス／不正アクセスの報告の受付と対策情報の提供（IPA）
・ インシデントの報告の受付と対策情報の提供（JPCERT/CC）
・ 「ネットワークセキュリティ脆弱性データベース（V-STAF）」（NPO 法人 ネッ

トワークリスクマネジメント協会）

（4）アクセス制御、認証、暗号利用の促進【政府、ベンダー、xSP、ユーザ】

ネットワーク上での不正アクセスの防止のため、認証技術・暗号技術の研究開発の推進及びその法的な効力の担保等についてルールを整備する必要がある。一方、企業や組織のユーザまたは個人のユーザにおいては、これらの技術の実装に努めるべきである。

今日の情報システムはネットワークによって結ばれており、一箇所セキュリティレベルの低い箇所があると、その影響を受けて情報システム全体のレベルが低下する。そのため、上記の技術に対しては、一定の水準を満たすことを評価・認定する制度を活用することが望ましい。

（関連する既存の取り組み）

- 「不正アクセス行為の禁止等に関する法律」（平成 12 年 2 月 13 日施行）
- 「電子署名及び認証業務に関する法律」（平成 13 年 4 月 1 日施行）
- 「暗号技術評価（CRYPTREC）」

２．２．３ 対応の原則に関わる実施方策

③ 対応（Response）
参加者は、セキュリティの事件・事故に対する予防、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るべきである。
Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

（1）インシデント対応体制の整備【政府、ベンダー、xSP、CSIRT、ユーザ】

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インシデントの発生に備えて、対策の立案に必要な調査・助言等を行うための危機管理体制の整備が不可欠である。同時に、政府機関や民間企業の情報システムのユーザ組織は、インシデント発生時には速やかに CSIRT 等へ報告することが求められる。

また、政府においては、インシデントへの対応に関する国際協調のあり方についての検討や国内におけるより迅速な対応体制の確立に向けた CSIRT 等の支援なども課題となっている。

（関連する既存の取り組み）

- 緊急対応支援チーム（通称 NIRT; National Incident Response Team）の設置（内閣官房情報セキュリティ対策推進室　平成 14 年 4 月 1 日）
- ウイルス／不正アクセスの報告の受付と対策情報の提供（IPA）
- インシデントの報告の受付と対策情報の提供（JPCERT/CC）
- FIRST（Forum of Incident Response and Security Teams）

・ APSIRC（Asia Pacific Security Incident Response Coordination）

（2）重要インフラ防護【政府、ベンダー、xSP、ユーザ】

情報システムは、重要インフラ分野（情報通信、金融、航空、鉄道、電力、ガス、地方公共団体を含む政府・行政サービス）においても、国民生活や社会経済活動に不可欠なサービスの安定的に供給し、公共の安全を確保するために重要な役割を果たすようになってきている。サイバーテロ等から重要インフラを防護するために、政府は目標や計画を策定し、必要な対策を講じる必要がある。加えて、政府は、民間重要インフラ事業者等が計画の実施をする際には、必要な協力を行うことが求められる。

（関連する既存の取り組み）

・ 「重要インフラのサイバーテロ対策に係る特別行動計画」（内閣官房情報セキュリティ対策推進室　平成 12 年 12 月 15 日）
・ 「サイバーテロ対策に係る官民の連絡・連携体制について」（内閣官房情報セキュリティ対策推進室　平成 13 年 10 月 2 日）

（3）脆弱性、インシデントの情報提供【ベンダー、xSP、CSIRT】

ベンダーや xSP は、提供する製品／サービスにおいてセキュリティホールが発見された場合には、速やかにユーザや CSIRT 等に対して情報提供することが求められる。また、セキュリティパッチ等を含む対策実践情報は、必要な人が必要な時に入手できるような状態にしておく必要がある。

CSIRT は、国境を越えて発生するインシデントにより迅速かつ正確に対応するため、インシデント対応に関する国際的な協調において主導的な役割を果たすことが期待される。

（関連する既存の取り組み）

・ ウイルス／不正アクセスの報告の受付と対策実践情報の提供（IPA）
・ インシデントの報告の受付と対策実践情報の提供（JPCERT/CC）
・ 「ネットワークセキュリティ脆弱性データベース（V-STAF）」（NPO 法人 ネットワークリスクマネジメント協会）

２．２．４ 倫理の原則に関わる実施方策

④ 倫理（Ethics） *参加者は、他者の正当な利益を尊重するべきである。* ***Participants should respect the legitimate interests of others.***

（1）倫理的な対応の必要性の広報、啓発【政府、ベンダー、xSP、ユーザ、地域／学界】

政府、ベンダー、xSP、CSIRT の取り組みとして、自身の職員や従業員または組織

／個人のユーザを対象とした啓蒙普及活動を通じて、ネットワーク上での倫理に関する意識の向上に貢献することが期待される。具体的な取り組みの例としては、セキュリティに関するルールやマナーに関するガイドライン等を提供することなどがある。

（関連する既存の取り組み）

- 「インターネットを利用する方のためのルール&マナー集」（財団法人 インターネット協会）
- 「インターネット接続サービス等に係る事業者の対応に関するガイドライン」（社団法人 テレコムサービス協会）

（2）教育（職員向け、一般向け）【政府、ベンダー、xSP、ユーザ、地域／学界】

教育機関における情報リテラシ教育の一環として、ネットワーク上の社会での倫理の重要性について啓蒙を図ることが求められる。特に若年層に対する倫理教育の実施は重要な課題である。

政府や企業、組織のユーザにおいては、職務規程や社内手続等において、倫理の重視を盛り込むとともに、パンフレットや CD-ROM 等の教材の配布、研修の実施等を通じた啓蒙活動の実践が期待される。

一方、個人ユーザの場合、ネットワーク上のルールやマナーについて自ら学習ことが相当する。

2．2．5 民主主義の原則に関わる実施方策

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るべきである。
The security of information systems and networks should be compatible with essential values of a democratic society.

（1）個人情報保護のルールの整備【政府、ベンダー、xSP、ユーザ、地域／学界】

電子商取引や電子政府等の普及に伴い、個人のユーザはネットワーク上でやり取りされる自身の個人情報の保護について、高い関心を持つようになってきている。政府は、必要な個人情報保護に関するルールを整備することが求められる。

（関連する既存の取り組み）

- 個人情報保護法制度の整備
- 「プライバシーマーク制度」（財団法人 日本情報処理開発協会）

（2）紛争処理に係る制度／体制の整備【政府、ベンダー、xSP、ユーザ、地域／学界】

政府は、情報の自由な流通を促進するために、紛争（著作権侵害、名誉毀損等を含む）の解決のためのルールを整備するとともに、簡便、迅速かつ柔軟な解決を図るための紛争処理の体制を整備する必要がある。

（関連する既存の取り組み）

- ADR（裁判外紛争解決）の整備
- 「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（通称：プロバイダ責任法、 2002 年 5 月施行）

(3) 脆弱性、インシデントの情報提供【ベンダー、xSP、CSIRT】

ベンダーや xSP では、製品／サービスに関わる脆弱性やインシデントに関わる情報を開示することは、これらの者の事業とってマイナスのイメージを招くことから、あまり積極的になれない場合もある。しかし、情報の公開性及び透明性の観点からは、ベンダー、xSP は時宜に応じた適切な情報の提供に努めるべきである。CSIRT には、これらの情報を収集し、公開することで、被害の拡散を防止する役割を果たすことが期待される。加えて、公開性、透明性に配慮しつつ、脆弱性に関する適正な情報開示ルールのあり方について議論することが必要である。

（関連する既存の取り組み）

- ウイルス／不正アクセスの報告の受付と対応情報の提供（IPA）
- インシデントの報告の受付と対応情報の提供（JPCERT/CC）
- 「ネットワークセキュリティ脆弱性データベース（V-STAF）」（NPO 法人 ネットワークリスクマネジメント協会）

(4) アクセス制御、認証、暗号利用の促進【政府、ベンダー、xSP、ユーザ】

情報の自由な流通と情報・通信の秘密を両立するため、アクセス制御、認証、暗号等の技術の利用促進は不可欠である。政府は、ベンダーや xSP との協働のもと、利用促進に向けたイニシアティブを主導する役割が期待される。

（関連する既存の取り組み）

- 「不正アクセス行為の禁止等に関する法律」（平成 12 年 2 月 13 日施行）
- 「電子署名及び認証業務に関する法律」（平成 13 年 4 月 1 日施行）
- 「暗号技術評価（CRYPTREC）」

2．2．6 リスクアセスメントの原則に関わる実施方策

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。
Participants should conduct risk assessments.

(1) セキュリティマネジメントの実施【政府、ユーザ、（ベンダー、xSP）】

政府や企業・組織のユーザにおいて、リスクアセスメントは、情報セキュリティマネジメントの実践の最初のステップとして組み込まれるべきである。これらの者は、

自身の情報システムやネットワークを含む情報資産について、その脆弱性や組織の内外からの脅威を評価し、望まれるセキュリティレベルとそのコストのバランスについて検討する必要がある。

個人ユーザの場合は、自身の使用するシステムやネットワークにどのようなセキュリティ上の脅威があり、どのようなセキュリティ対策を実施すればよいのか、考慮することが求められる。

（関連する既存の取り組み）

- 「ISMS 適合性評価制度」
- 「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議　平成 12 年 7 月 18 日）
- 「情報セキュリティポリシーサンプル」（NPO 法人 日本ネットワークセキュリティ協会）

（2）情報セキュリティに係る評価の推進【政府、ベンダー、ユーザ】

政府においては、情報システムや IT 製品等を調達する際に、個々の製品・システム等のセキュリティの保証レベルを定めた国際規格に基づき評価または認証された製品の利用を進めることが求められている。

また、社会全体のセキュリティレベル向上のため、企業や他の組織においても、情報セキュリティの評価・認定制度等を積極的に活用することが望まれる。

（関連する既存の取り組み）

- 「IT セキュリティ評価・認証制度」
- IT セキュリティ評価・認証制度に係る国際相互承認（CCRA：Common Criteria Recognition Arrangement）への参加
- 「暗号技術評価（CRYPTREC）」

（3）脆弱性、インシデントの情報提供【ベンダー、xSP、CSIRT】

ベンダーや xSP は、提供する製品／システム／サービス等について評価を行い、脆弱性、インシデント及び対策などの情報を適切なタイミングでユーザや CSIRT 等に提供することが求められる。

CSIRT の役割の 1 つとして、散在する脆弱性、インシデント、対策実践方法等に関する情報を集約、整理し、ユーザがリスクアセスメントを行う際のリファレンス情報として提供することが期待される。

（関連する既存の取り組み）

- ウイルス／不正アクセスの報告の受付と対応情報の提供（IPA）
- インシデントの報告の受付と対応情報の提供（JPCERT/CC）
- 「ネットワークセキュリティ脆弱性データベース（V-STAF）」（NPO 法人 ネッ

トワークリスクマネジメント協会）

２．２．７ セキュリティの設計及び実装の原則に関わる実施方策

⑦ セキュリティ設計及び実施（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。* *Participants should incorporate security as an essential element of information systems and networks.*

（1）アクセス制御、認証、暗号利用の促進【政府、ベンダー、xSP、ユーザ】

ベンダーや xSP は、提供する製品、システム、サービス等において、その必要不可分な構成要素としてセキュリティに関する機能や仕組みの導入に努めるべきである。特に、アクセス制御技術、認証技術、暗号技術の利用の促進は、ネットワークのセキュリティレベル向上の観点から課題となっている。

（関連する既存の取り組み）

- 「不正アクセス行為の禁止等に関する法律」（平成 12 年 2 月 13 日施行）
- 「電子署名及び認証業務に関する法律」（平成 13 年 4 月 1 日施行）
- 「暗号技術評価（CRYPTREC）」

（2）情報セキュリティに係る評価の実施【政府、ベンダー、ユーザ】

ベンダーは、情報システムの個々の製品・システム等のセキュリティ機能に関する客観的な評価基準の活用が望まれる。

政府では、情報システム等の IT 製品の調達仕様において、可能な限り評価・認定を受けた製品を導入することとしており、企業・組織のユーザにおいても、情報システムを導入する際の重要な要件として、これらの評価基準等を活用することが望ましい。

（関連する既存の取り組み）

- 「IT セキュリティ評価・認証制度」
- IT セキュリティ評価・認証制度に係る国際相互承認（CCRA：Common Criteria Recognition Arrangement）への参加
- 「暗号技術評価（CRYPTREC）」

（3）技術の標準化の推進 【政府、ベンダー、ユーザ】

政府は、情報セキュリティ関連技術の研究開発および標準化を推進し、ベンダー等に対して必要な協力を行うべきである。さらに、ユーザに対しては、標準化への対応を促進することで、ネットワーク全体のセキュリティの向上を図ることが期待される。

２．２．８ セキュリティマネジメントの原則に関わる実施方策

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。* *Participants should adopt a comprehensive approach to security management.*

（1）情報セキュリティマネジメントの実施【政府、ベンダー、xSP、ユーザ】

政府は、電子政府や重要インフラにおいて、情報セキュリティマネジメントに関する方針を定め、推進するとともに、情報セキュリティマネジメントに関するベストプラクティスを官民の間に広めていくことが求められる。また、官民における情報セキュリティマネジメントの普及促進のため、評価制度等を促進することも重要である。

政府、企業、その他の組織において情報セキュリティマネジメントを実施するにあたっては、他のすべての原則の実施方策との整合を図るように配慮する必要がある。

個人ユーザの場合の情報セキュリティマネジメントには、ウイルスソフトの実装等のセキュリティ対策の実施とその継続が含まれる。

（関連する既存の取り組み）

- 「ISMS 適合性評価制度」
- 「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議　平成 12 年 7 月 18 日）
- 「情報セキュリティポリシーサンプル」（NPO 法人 日本ネットワークセキュリティ協会）

（2）アクセス制御、認証、暗号利用の促進【政府、ユーザ、（ベンダー、xSP）】

情報セキュリティマネジメントは、運用・体制の整備と技術的な防護方策の両面から検討することが不可欠である。特に、近年、ネットワーク上のインシデントが急増し、サイバーテロ等の脅威が懸念されていることから、アクセス制御、認証、暗号技術の利用の促進が求められている。政府は、必要な法制度や技術開発等の推進を行う必要がある。

（関連する既存の取り組み）

- 「不正アクセス行為の禁止等に関する法律」（平成 12 年 2 月 13 日施行）
- 「電子署名及び認証業務に関する法律」（平成 13 年 4 月 1 日施行）
- 「暗号技術評価（CRYPTREC）」

２．２．９ 再評価の原則に関わる実施方策

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るべきである。* ***Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.***

（1）情報セキュリティマネジメントの実施【政府、ユーザ、（ベンダー、xSP）】

政府や企業・組織のユーザは、情報セキュリティマネジメントの一部として、セキュリティ方策、対策実践方法、手続等を継続的に再検討し、必要な見直しを行う必要がある。

（関連する既存の取り組み）

- 「ISMS 適合性評価制度」
- 「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議　平成 12 年 7 月 18 日）
- 「情報セキュリティポリシーサンプル」（NPO 法人 日本ネットワークセキュリティ協会）

（2）情報セキュリティ監査の実施【政府、ユーザ、（ベンダー、xSP）】

再評価の実施にあたっては、客観的かつ包括的に組織全体のセキュリティについて評価・監査することが必要であり、可能である場合は外部の第三者機関に情報セキュリティ監査の実施を委託することも検討するべきである。政府は、一定の水準を満たす情報セキュリティの監査の基準について、整備することが求められる。

個人ユーザの場合、セキュリティ対策のアップデート及び見直しを継続的に行うことが必要であり、専門的な知識がなくても簡単に対策ができるように、自動化ツール等がベンダーや xSP から提供され、使用が促進されることが期待される。

（関連する既存の取り組み）

- 情報セキュリティ監査制度の検討

２．３ 全般を通じた対策

新ガイドラインの全体を通じて、実施方策として想定される項目、その実施方策に関わりをもつ参加者（participants）並びに各実施方策に関連する既存の取り組み等について整理する。

【】内は、実施方策として想定される各項目に関連する参加者を示す。

（1）目標／計画の策定【政府】

政府は、我が国の情報通信ネットワーク及び情報システム全体の安全性及び信頼性の向上に向けて、必要な目標／計画を策定し、施策を実施していく必要がある。

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）が 2002 年 6 月に定めた「e-Japan 重点計画-2002」では、重点政策 5 分野の 1 つとして「高度情報通信ネットワークの安全性及び信頼性の確保」を掲げており、具体的な施策として「① 政府の情報セキュリティ確保」「② 重要インフラのサイバーテロ対策」「③ 民間部門における情報セキュリティ対策及び普及啓発」「④ 情報セキュリティに係る制度・基盤の整備」「⑤ 個人情報の保護」「⑥ 情報セキュリティに係る研究開発」「⑦ 情報セキュリティに係る人材育成」「⑧ 情報セキュリティに係る国際連携」を設定している。

（関連する既存の取り組み）

- 「e-Japan 重点計画-2002」（IT 戦略本部　2002 年 6 月 18 日）

（2）技術開発【政府、ベンダー、xSP、ユーザ、地域／学界】

不正アクセスやサイバーテロの予防、検知等に関する技術のほか、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、情報セキュリティに関する基盤技術の研究開発を推進することが求められている。

また、情報システムやネットワークの利用が個人ユーザや小規模事業者（SOHO 等）にも広がっていることから、自動的にセキュリティパッチやアップデートを適用できるような個人向けツール等の研究開発も不可欠である。

（3）人材育成【政府、ベンダー、xSP、ユーザ、地域／学界】

政府部門及び民間部門において、基本的な情報リテラシの向上とセキュリティに関する専門技術者の両面から、人材の育成を行う必要がある。

情報システムの利用者部門（政府機関、一般企業等）では、職員及び従業員に対して、基礎的な情報セキュリティ教育／研修を実施するとともに、組織においてセキュリティポリシーを定め、それに則って情報セキュリティマネジメントの実践を主導する人材の確保が不可欠となる。

一方、ベンダーや xSP 等の現場では、情報セキュリティの専門技術者が質量共に不足しており、人材の供給側である教育機関における専門家育成が課題となっている。

また、情報セキュリティの専門技術者の育成にあたっては、セキュリティ関連業務に必要とされる技能（スキル）に関する標準を策定するとともに、当該標準に基づく人材

育成プログラム等の整備を推進することが望まれる。

（関連する既存の取り組み）
- 「情報セキュリティアドミニストレータ試験」
- 情報セキュリティ技能の標準化

２．４ 国際機関の役割

OECD をはじめとする情報通信や情報セキュリティに関連のある各種国際機関の役割について整理する。

(1) 国際的な連携と協力

サイバーテロやハイテク犯罪等は、国境を越えて行なわれる可能性も高いことから、インシデントの発生時の連絡や情報の共有、捜査における協力体制の整備等が望まれる。国際機関は、情報セキュリティに関する国際的な連携と協力における調整を主導する役割が期待される。

国際協調・連携の推進にあたっては、国内における「対応の原則」の実施方策（２．２．３参照）と密接な関係があり、両者の整合が図られることが重要である。

(2) ベストプラクティスの提示

国際機関は、各国で取り組んでいる実施方策について情報を収集し、実効性に優れるものをベストプラクティスとして、共有できる環境を整備することが望まれる。

(3) セキュリティに対する意識の向上

新ガイドラインの提唱する「セキュリティ文化」が国際的な共通理念として普及するためには、非加盟国や情報通信分野における発展途上国においても、セキュリティに対する意識を向上させていくことが重要である。国際機関の役割として、これらの国に対しても新ガイドラインの周知を図っていくことが期待される（「３．２ OECD 非加盟国への周知方策の提案」を参照）。

３．OECD 情報セキュリティガイドラインの普及

OECD 情報セキュリティガイドラインは、情報システムに関わる全ての者の共通理念である「セキュリティ文化」の普及を目指すものである。そのために、国内はもとより、OECD 非加盟国に対して、OECD 情報セキュリティガイドラインの認知度の向上と普及を促進していくことが求められている。

以下本章では、OECD 情報セキュリティガイドラインの普及に向けた活動や方策について提案する。

３．１ OECD 情報セキュリティガイドライン普及啓発用パンフレットの作成

OECD 情報セキュリティガイドラインは、OECD 独自のフォーマットや用語が使われており、一般には馴染みにくい部分もある。ガイドラインが掲げる 9 原則の理念や改訂の経緯等について簡潔にまとめた、一般向けの普及啓発用パンフレットの作成を行った。IPA や経済省等が開催するイベント等や関係機関等への配布を通じて、OECD 情報セキュリティガイドラインの周知を図っていくことを想定している。作成したパンフレットについては、本報告書の付録として添付している。

パンフレットの作成に際して、その仕様について検討した結果、以下に示す方針のもとで実施するものとした。

(1) パンフレットの目的の設定

これまでのところ、情報セキュリティに関して OECD ガイドラインが存在することに対する一般的な認知度はきわめて低い。IT 分野の専門家の場合は、ガイドラインが存在すること自体は認知されているものの、彼らの議論や著作においてガイドラインの原則が引用されることは、OECD において作成されたプライバシー保護、暗号政策の 2 つのガイドラインと比較しても明らかに少ない傾向が見受けられる。この原因としては、以下の 2 点が挙げられる。

（ａ）ガイドラインのターゲットがつかみにくい

1992 年制定のガイドラインは、「情報システムのセキュリティ」を対象としている。これは、プライバシーや暗号政策といったテーマを絞ったガイドラインと比較すると、その適用範囲や影響を把握しにくく、議論における判断材料としての活用は容易とは言えない。また、ガイドラインの対象者も政府や企業が中心であり、情報システムにたずさわることのない人々にとっては当事者意識を抱きにくいこともこの傾向を助長している。

（ｂ）ガイドラインの翻訳文書が普及していない

プライバシーおよび暗号政策の各ガイドラインについては、翻訳文書が普及しているのに対し、1992 年制定のガイドラインについては、日本国内での統一的な翻訳が作成されなかったこともあって、翻訳されたガイドラインが広く流通することはこれま

でなかった。

（c）インターネットの普及前後のギャップ

1992 年制定のガイドラインは、特定の組織内ないし用途に閉じた情報システムを対象としており、ガイドラインの認知が必要となる範囲は限られていた。

こうした経緯により、改正前のガイドラインは普及しているとは言えないが、ガイドラインの対象が一般ではなかったこともあり、その悪影響を懸念する必要性は必ずしも高くなかった。これに対して、今回改正されたガイドラインにおいては、改正のポイントとして、

- 「セキュリティ文化」の提唱
- 個人を含むすべての参加者が責任を負う

の 2 点が強調されていることもあり、一般における認知度と理解を高めることがガイドラインを有効に機能させるために欠かせない。そこで、パンフレットの作成に際しては、その目的を「一般におけるガイドラインへの認知度と理解を高めること」に置くものとする。

(2) 対象読者の想定

パンフレットの読者としては、情報セキュリティの専門家から、電気製品の操作は概して苦手という人々まで様々に想定することが可能である。このとき、上述の目的を踏まえ、適切な読者の想定を行う必要がある。

読者の想定として、情報システムやネットワークに関する知識がほとんどない人々を対象にすると、原理的にはすべての人々が理解可能なパンフレットを作成することができる。ただし、ガイドラインで言及している内容のすべてについて平易な解説を用意することは、パンフレットのボリュームを増すだけでなく、一定以上の知識を有する読者にとって、記述事項におけるポイントをつかみにくくしてしまう恐れがある。また、ガイドラインの各原則において言及されている内容は、情報システムやネットワークにおける具体的な操作方法の指針となるものではなく、むしろそうしたインタフェースを構築するために何を考えればよいのかを説く性質が強いものであって、ガイドラインの理念上の対象者がすべての参加者であっても、実際にガイドラインを常に意識すべき層は絞られるものと考える必要がある。

一方、情報システムやネットワーク、情報セキュリティの専門家に対してガイドラインの改正内容とその意図を簡潔に伝えることにも意義はあるが、こうした専門家はガイドラインの原文や別途公開されている仮訳で内容の把握は可能あり、パンフレットを通じた啓発を行う必要性は必ずしも高くない。

そこで、今回作成するパンフレットの対象読者としては、改正されたガイドラインにおいてその目的とされている「セキュリティ文化」の普及と、すべての参加者がセキュ

リティに関する責任を負うことの自覚を促すことを最も効果的に実現させるため、以下に示すような読者をターゲットとして作成するものとする。

（ａ）マネジメント層、公共政策担当者

これまで情報セキュリティの知識は必ずしも求められこなかったと想定される。昨今の IT 活用を必須とする時勢のもとで、IT 導入に合わせてセキュリティポリシーの作成やマネジメントサイクルの構築が必要となることを理解する際の参考としてもらう。

（ｂ）情報システムやネットワーク事業の従事者

これまで日本語による解説が得られなかったことで、ガイドラインの中身を知る機会がなかったと想定される。パンフレットを通じて、情報システムやネットワークの構築や運用を考えるにあたってのガイドラインで言及している事項の重要性に対する自覚をより高めてもらう。

３．２ OECD 非加盟国への周知方策の提案

インターネットの世界には国境はなく、脅威が国際化する傾向が顕在化してきている。また、情報セキュリティはもっとも防御の弱いところから影響を受けることが知られている。OECD 非加盟国やインターネット途上国に対しても、OECD 情報セキュリティガイドラインの提唱する「セキュリティ文化」を普及させていくことが、情報化社会全体のセキュリティレベルの向上につながる。そのため、新ガイドラインにおいても、勧告の中で以下の 2 点を掲げ、国際的な協調の必要性を支持している。

- このガイドラインを実施するために国内及び国際レベルで協議し、調整し、かつ協力すること（Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines.）。
- 時宜を得た、適切な方法でこのガイドラインを非加盟国において利用可能にすること。（Make the Guidelines available to non-member countries in a timely and appropriate manner.）

特に、近年インターネットユーザ数が加速度的に増加しているアジア地域においては、我が国は OECD 情報セキュリティガイドラインの普及を含め、情報セキュリティに関する国際的な施策の推進や地域のセキュリティレベルの向上に向けてリーダーシップを発揮することが求められている。

「３．１ OECD 情報セキュリティガイドライン普及啓発用パンフレットの作成」で紹介したような普及・広宣のためのパンフレット等を作成し、国際的なカンファレンスやイベント、学会等の機会を捉えて、OECD 情報セキュリティガイドラインを広く周知していくことも有効な方策の一つになるものと思われる。

上記のような取り組みの一例として、2003 年 1 月に行なわれた「OECD-APEC Global

Forum: Policy Frameworks for the Digital Economy」では、「ネットワーク社会のためのセキュリティ文化（A Culture of security for the Networked Society）」というタイトルで1 セッションが設けられた。同会合は、グローバルなデジタル社会のための一貫性のある政策フレームワークの必要性に焦点を当てたものであり、OECD と APEC（Asian Pacific Economic Cooperation Conference：アジア太平洋経済協力閣僚会議）の共同で開催された。

この中で、OECD 情報セキュリティガイドラインについての紹介が行なわれたところである。

４．OECD ワークプログラム提案に向けた課題の整理

OECD 情報セキュリティガイドラインが改訂されたことを受けて、その中で提唱された「セキュリティ文化（culture of security）」の理念をグローバルなレベルで広めていくことが必要となる。OECD 事務局では、加盟国の協調のもと、セキュリティ文化促進のために、効果的なフォローアップ作業の重要性を認識しており、2003 年以降、具体的なワークプログラムを策定し、推進していくことを検討している。OECD 情報セキュリティガイドラインの見直し作業の過程では、以下のようなフォローアップ施策が提案された。

- WPISP において全体討議型の情報交換を実施
- OECD 加盟国における OECD 情報セキュリティガイドラインの実施状況の把握
- 情報交換を通じたベストプラクティスによるベンチマーキング

本年度の研究会においても、日本から OECD ワークプログラムの提案に向けた検討の必要性が指摘されている。本調査では、検討の過程で指摘された以下の 4 項目について、関連する団体等へヒアリング調査や各種文献調査を中心に課題の整理を行なった。

1. セキュリティ方策に関するベストプラクティスの共有に向けた検討
2. 最新の情報通信技術におけるセキュリティ方策の検討
3. 情報セキュリティ監査のあり方の検討
4. セキュリティホールに対する関係者間の役割と責任分担のあり方の検討

４．１ セキュリティ方策に関するベストプラクティスの共有に向けた検討

セキュリティ方策を国際的な協調のもとで推進していくため、各国それぞれの取り組みについての情報交換を進め、ベストプラクティスとして共有化していくことが望まれる。

インターネットの発祥の地である米国では、官民それぞれのレベルで取り組みが進められている。政府においては、重要インフラの保護や国防の観点を中心にセキュリティ方策を推進している。2002 年 10 月には「米国サイバーセキュリティ国家戦略（National Strategy to Secure Cyberspace）」のドラフトを発表し、政府としての取り組みのロードマップを示している。

このように、政府も情報セキュリティに関する施策に力を入れてきているが、これまで米国では民間団体が情報セキュリティ方策の推進において中心的な役割を果たしてきた。情報セキュリティにかかわる各分野において、米国の事情を反映した特徴的なモデルを生み出し、活動を行ってきている。

本調査研究では、「3. ガイドラインの実施方策」でも重要な課題として指摘されている以下の 2 テーマについて、米国の民間団体にヒアリング調査を行った。

- 脅威や脆弱性等に関する情報流通のための体制整備（ヒアリング先：Internet Security Alliance）
- 情報セキュリティ教育と資格試験制度のあり方（ヒアリング先：International Information System Security Certifications Consortium, Inc.）

４．１．１ 脅威や脆弱性等に関する情報流通のための体制整備

４．１．１．１ 背景

情報システムやネットワークの利用者が、適切なセキュリティレベルを維持しつづけるために、自身が使用している製品における脆弱性や発生したインシデント等に対して迅速かつ適切に対応する必要がある。そのために、脅威や脆弱性等に関する情報が、必要な時に、必要な人に対して、適切な形で提供され、流通する体制が不可欠である。新しい OECD 情報セキュリティガイドラインにおいても「対応の原則（Response）」の中で「参加者は、セキュリティの事件・事故に対する予防、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るべきである」とし、「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・事故に対する予防、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る」ことを要求している。

このような問題に対応するため、産業界や各国政府、学術界などの各セクターにおいて「CSIRT（Computer Security Incident Response Team）」と呼ばれる機関が組織されている。CSIRT は、情報セキュリティのインシデントに対応する活動を行う組織体の総称であり、情報セキュリティに関する情報交換、インシデントへの対応、国内外の関連機関とのコーディネーション等の活動を行なっている。CSIRT の運営形態やサービス内容はそれぞれ異なっており、設立や活動の母体についても、民間団体、政府機関、大学・研究機関など各国によって事情は異なっている。CSIRT は表 ４-１のように分類することができる。

表 4-1　各国の CSIRT の分類

独立系	CERT/CC、JPCERT/CC
学術系	CERT-NL（蘭）、DFN-CERT（独）
政府外郭団体系	CERT-KR（韓）、IPA/ISEC
軍	AFCERT（米国空軍）、NAVCIRT（米国海軍）、DOD-CERT（米国防省）
大学	OxCERT、GTCERT
企業	MSCERT（Microsoft）、ISS
会員制	AusCERT（豪）

（出典：JPCERT/CC「InternetWeek2002」資料をもとに作成）

米国における脅威や脆弱性等に関する情報流通に関する体制としては、米国カーネギーメロン大学のソフトウェア工学研究所（SEI：Software Engineering Institute）に設置された CERT/CC（Computer Emergency Response Team Coordination Center）が、インターネット上のインシデントへの対応に関する中心的な調整機関として 1988 年より活動を行ってきた。また、米国政府の取り組みとしては、重要インフラ分野の保護を目的として 1998 年 5 月に発令された PDD（Presidential Decision Directive：大統領決定指令）63 にもとづき、サイバー攻撃の脅威に対する警告、分析、対応等を担う NIPC（国家インフラ防護センター）が設置されたほか、政府と民間の連携組織として情報共有分析センター（ISAC：Information Sharing and Analysis Center）が金融、電気通信、情報技術、電力、ガス、水道、電力、ガス、水道、運輸などの産業分野ごとに設立され、活動を行なっている。

政府による取り組みが進む一方、米国では民間の団体や企業などが積極的に活動を行なっており、それぞれのアプローチで取り組んでいる。そこで本調査では、上記のテーマに対して米国の民間団体の動向について把握するため、複数の団体にヒアリングの依頼を行なった。このうち、依頼に応じて頂いた「Internet Security Alliance（ISA）」に訪問し、ヒアリングを行なった。

４．１．１．２ ヒアリング調査結果概要

（1）調査の目的

脅威や脆弱性等に関する情報流通のための体制整備の状況に関して、主に以下の調査テーマについて知見を得る。

- ISA の活動
- 脆弱性や脅威に関する情報流通のあり方
- 情報セキュリティにかかわる米国内の動向

（2）組織概要

ISA は、米国の電子機器産業の業界団体である Electronic Industries Alliance（EIA）と CERT/CC によりに 2001 年 4 月に設立された。産業界主導の情報セキュリ

ティに関するベストプラクティスの推進組織として活動を行ってきている。ISA の組織概要は表 4-2の通り。

表 4-2 ISA の概要

名称	Internet Security Alliance（ISA）
所在地	Virginia 州 Arlington
設立	2001 年 4 月
活動目的	・ 脆弱性、脅威等に関する会員向けの情報提供サービス及びソリューションサービス ・ 米国の情報セキュリティ政策に対する産業界としての提言
会員企業数	Sponsors： 20 社 Members： 7 社 Associate Members：15 社
従業員数	5 名（フルタイム）

会員種別は以下の 3 種類。メンバーシップのランクが高くなるにつれて、CERT/CC が提供するデータベースへのアクセス数や増えるほか、カンファレンス、出版物、トレーニングコース等の料金がディスカウントされる。

表 4-3 ISA の会員種別

種別	主な特典	年会費
Sponsors	・ メンバー認定書： 28 ライセンス ・ カンファレンス、CERT/CC のコース受講料等の 25%ディスカウント ・ Executive Committee（執行委員会）への参加 ・ ワーキンググループの議長権	US$70,000
Members	・ メンバー認定書： 5 ライセンス ・ カンファレンス、CERT/CC のコース受講料等の 10%ディスカウント	US$25,000
Associates	・ メンバー認定書： 1 ライセンス ・ カンファレンス、CERT/CC のコース受講料等の 5%ディスカウント	US$3,000

（3）ISA の主要な活動

ISA では、カーネギーメロン大学及び CERT/CC との協力のもと、脆弱性や脅威に関する最新情報である「Threat and Vulnerability First-Alert」を会員企業に提供している。ISA の会員企業は、ベンダー企業等から CERT/CC へ報告された、あるいは CERT/CC のメンバーらが発見した脆弱性や脅威に関する情報を、一般に先駆けて提供を受けることができる。加えて、脆弱性や脅威に対してどのように対処すればよいかのガイダンスを受けられる。

会員からの年会費の半分は CERT/CC の活動に充てられる。CERT/CC は国防総省、連邦調達局（General Services Administration：GSA）、その他の米政府機関からも資金提供を受けているが、その使用用途は制限されている。民間からの資金提供を受

けることで CERT/CC はよりサービスを拡充できると ISA は説明している。

会員のメリットの一つに、サイバーテロ保険のディスカウントが受けられる特典がある。ISA の会員企業であれば保険料が 10%割引になり、さらに ISA の推奨するベストプラクティスを実行している場合には割引率は 15%になる。サイバーテロ保険は一般に高額なものも多いと言われているが、会員企業は会費以上の経済的なメリットが得られるとのことである。

(4) 脅威や脆弱性等に関する情報流通のあり方について

ISA では、社会の情報セキュリティレベルの向上は、民間主導のもとで行われることが望ましいと考えている。そのため、フィロソフィーとして政府からは金銭的、人的な支援は受けていない。

また、脆弱性に関する情報の流通については、

（ａ）脆弱性が発見された場合、ただちにすべての人に対して公表する
（ｂ）脆弱性が発見されても、ベンダーがその対応策等に関する情報を自ら発表するまで一切公開しない
（ｃ）上記の中間またはコンビネーション

といった三種類のモデルが考えられるが、ISA は、自身のモデルは（ｃ）の立場を採っていると説明している。ISA では、脆弱性が発見された場合、会員企業と政府機関に対して脆弱性情報が一般に公開される前に防御策を取る機会を与え、しかるべき時間が経過した後に、一般に公表するというスタンスをとっている。過去のケースでは、一般公開される 6 ヶ月前に ISA の会員に情報提供がされたこともある。一方、ISA の会員は、厳しい機密保持契約に同意することが求められる。この契約により、会員は自分の運営するシステムやネットワークを守る目的以外に提供された脆弱性情報を利用できないようになっている。

(5) ベストプラクティスガイドラインについて

会員向けのサービスの一環として「Common Sense Guide for Senior Managers － Top Ten Recommended Information Security Practices（邦題：上級管理者のための常識ガイド － 実行したいセキュリティプラクティストップ 10)」を 2002 年 7 月に策定している（2002 年 10 月には日本語版も作成)。

このガイドラインは、企業の情報セキュリティにおける 10 の最優先事項及び推奨されるベストプラクティスを整理したものであり、組織内の上級管理者クラスへのインストラクションとチェックリスト形式の質問文から構成されている。

ISA ベストプラクティスガイドラインの項目は表 4-4 のとおりである。

表 4-4　ISA ベストプラクティスガイドライン

Practice	主な内容
#1：一般的な管理	・ 情報セキュリティにおける役割と責務の定義と割り当て ・ 組織内の管理者クラスの責務 ・ セキュリティポリシーの規定と見直し
#2：ポリシー	・ セキュリティポリシーの重要事項（セキュリティ危機管理、重要資産の識別、物理セキュリティ、ネットワーク管理、認証と権限、脆弱性管理インシデント対応、認識向上と訓練、プライバシー等） ・ 標準手続き、業務、訓練
#3 危機管理	・ 重要資産に対する危機が発生した場合の影響の見積もり ・ 情報セキュリティ評価に基づく危機緩和プランの策定と実施
#4：セキュリティ構造とデザイン	・ ネットワーク及びシステムの多層化と業務形態の変更 ・ 多様な通信手段予備システムの導入
#5：ユーザの問題	
#5.1：責務と訓練	・ ユーザのセキュリティに対する認識の向上 ・ ユーザアカウント取得時における教育 ・ ポリシー違反や法的違反に対する制裁や社会的影響
#5.2：相応の知識	・ 情報セキュリティの専門技術に精通した人間を組織の内外に常駐させること
#6：システム及びネットワーク管理	
#6.1：アクセスコントロール	・ ネットワーク、システム、ファイル、アプリケーションのアクセスコントロール ・ 必要に応じた暗号と VPN の使用 ・ ファイアウォールを含めたセキュリティアプリケーションの使用 ・ 重要データの物理的保護のための可搬式メディアの使用 ・ パソコン等の破棄手順の確立
#6.2：ソフトウェアの完全性	・ ウイルス、ワーム、トロイの木馬等に対する定期的なチェック ・ すべてのファイルと及びディレクトリ内の暗号化したチェックサムの定期的な確認
#6.3：安全な資産の形態	・ パッチの適用 ・ コンピュータ及びサービスの最低限必要な状態の標準の策定と保持 ・ ネットワーク構成図の作成 ・ ログの収集 ・ システムの脆弱性の定期的な査定
#6.4：バックアップ	・ バックアップ前後のソフトウェア及びデータの確認 ・ バックアップによる復旧能力の確認
#7：認証と権限	
#7.1：ユーザの認証と権限	・ ユーザの組織の内外からのアクセス字の認証と権限の対策 ・ 上記の対策は、セキュリティポリシーや手続き、特定資産へのアクセス制限のレベル等と首尾一貫したものであること
#7.2：リモートアクセス及び第三者に対する認証と権限	・ ネットワークから離れた場所で働くユーザや契約業者、サービスプロバイダ等の第三者に対してネットワークアクセスを提供する際の重要資産の保護
#8：モニタと監査	・ システム及びネットワークのモニタリングツールの定期的な使用 ・ フィルタリング及び分析ツールの定期的な使用 ・ 怪しい行動に気づいたときの連絡先の周知
#9：物理的セキュリティ	・ 必要に応じ、物理的アクセスコントロール（バッチ、バイオメトリクス、鍵等）を使用すること ・ パスワードによってロックし、時間外にコンピュータにログインできないようにすること ・ ハードウェア資産（ルータ、ファイアウォール、サーバ、メールハブ）へのアクセスのコントロール
#10：継続プラントと災害復旧プラン	・ 重要資産に関する業務継続プランと災害復旧プランの作成と定期的なテストの実施

（6）OECD 情報セキュリティガイドラインへの関与

2002 年の OECD 情報セキュリティガイドラインの見直し作業に対しては、FTC（Federal Trade Commission：連邦取引委員会）を通して米国内の意見の取りまとめ作業に参加した。

ISA 関係者の話によると、新しい OECD 情報セキュリティガイドラインに対して現時点では具体的なアクションは取っていないが、今後 ISA の活動に何らかの影響をもたらすものと思われることから、内部で検討する予定があるとのこと。

４．１．１．３ 課題の整理

ISA のモデルは、民間のリーダーシップと資金で情報セキュリティに関する方策の推進を図るものである。1990 年代の商用解放以降、インターネットは民間主導で発展してきた。情報セキュリティにかかわる問題がインターネットの健全な発展を阻害しないために、米国の産業界は自らの社会的責任を意識し、強い意志をもってこの問題に取り組んでいくこと表明している。さらに、2001 年 9 月の米国同時多発テロ以降、米国連邦政府が「The National Strategy For Homeland Security」「The National Strategy to Secure Cyberspace」といった情報セキュリティにも関連する国家戦略を相次いで打ち出すなど、情報セキュリティ分野の政策の方向性を転換させてきている。このような状況に対して、産業界の影響力を確保しようとする意図が含まれているともいえる。

日米の企業における公共分野への関与の仕方の違いや文化的な背景の相違などがあり、ISA のモデルがそのまま我が国で通用するわけではないが、一つの方向性を示すものといえるだろう。脅威や脆弱性等に関する情報流通のための体制整備に関しては以下のような点が課題になる。

- 各国によって脅威や脆弱性等に関する情報流通の体制が異なっている（政府主導、民間主導、学術界主導、等）状況において、どのような国際的なパートナーシップが望ましいか。
- 我が国において、脅威や脆弱性等に関する情報流通のための体制については、どのようなモデルが適切か。特に、産業界、政府、学術界および独立機関の連携はどうあるべきか。
- 脅威や脆弱性等に関する情報流通のための体制整備において、政府に求められる役割は何か。

４．１．２ 情報セキュリティ教育と資格試験制度のあり方

４．１．２．１ 背景

IT 関連製品の開発メーカや情報システムのインテグレータ、ネットワークサービスなど、情報システムの供給者側においては、情報セキュリティに関する知識に精通した技術者や開発者を育成し、確保していくことが課題となっている。一方、情報システムの使用者側では、情報システムやネットワークを含む企業の情報資産に対する情報セキュリティマネジメントの策定及び実施を担当する人材の不足が認識されており、教育、訓

練の必要性は高い。新しい OECD 情報セキュリティガイドラインでは「認識の原則（Awareness)」において「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付け、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るべき」としており、啓発や意識向上の観点から、教育、訓練の必要性を支持している。

しかし、情報セキュリティに関連する技術は変化が早く、教育や訓練の難しさが指摘されている。加えて、情報セキュリティは、技術知識だけでなく、経営管理やリスクマネジメント、法令などの幅広い分野ともかかわりがあるうえ、不測の事態への対応など、知識だけでなく実際に実践できる能力や経験等が求められる場合も多い。

情報セキュリティにたずさわる人材の技術知識や実務能力に関する客観的な指標として、資格試験制度が運用されている。わが国においても情報セキュリティ関連の資格制度として、国家試験である情報処理技術者試験の「情報セキュリティアドミニストレータ試験」や（社）電気通信事業者協会など民間の 7 事業者団体により運営される「ネットワーク情報セキュリティマネージャー」が 2001 年から開始されている。また、ベンダーでは自社製品等に関する独自の資格認定制度を運用している企業もある。

米国においては、民間の団体や企業等において資格試験が運用されている（表 4-5）。情報セキュリティの重要性の高まりを受け、これらの資格試験の受験者も増加しているという。

表 4-5　米国の情報セキュリティ関連資格

実施団体・企業	資格名	必要科目	コスト
International Information Systems Security Certification Consortium (ISC)2	Certified Information System Security Professional（CISSP）	1 科目(250 問／6 時間）	$450
	Systems Security Certified Practitioner（SSCP）	1 科目(125 問／3 時間）	$295
Prosoft	Master CIW(Certified Internet Webmaster) Administrator	CIW Security Professional を含む必須 4 科目	$500(1 科目$125)
	CIW Master Security Analyst	ネットワーク系資格（MCSE, CNE, LPI etc.）＋ CIW Security Professional	$125(CIW Security Professional のみ)
SANS	GIAC Security Engineer	7 科目	$1750(1 科目$250)
Information Systems Audit and Control Association2（ISACA）	Certified Information Security Manager（CISM）	1 科目	$465
BrainBench	Brainbench Internet Security Certification	1 科目	$25
	Brainbench Network Security Certification	1 科目	$25
CompTIA	Security+	1 科目	$199
Security Certified Program	Security Certified Network Professional	2 科目	$300(1 科目$150)
	Security Certified Network Architect	2 科目	$360(1 科目$180)

(各種資料をもとに作成)

そこで本調査では、上記のテーマに対して米国の民間団体の動向について把握するため複数の団体にヒアリングの依頼を行なった。このうち、依頼に応じて頂いた「International Information System Security Certifications Consortium, Inc.（(ISC)² ：「ISC スクエア」と発音する）」に訪問し、ヒアリングを行なった。

４．１．２．２ ヒアリング調査結果概要

（1）調査の目的

米国における情報セキュリティ教育及び資格試験の状況に関して、主に以下の調査テーマについて知見を得る。

- (ISC)² の活動
- 情報セキュリティ教育のあり方
- 情報セキュリティに関する資格制度のあり方

（2）組織概要

(ISC)² は、民間の非営利のコンソーシアムとして、1989 年に設立された。情報セキュリティプロフェッショナルの資格認定試験と教育・トレーニング等のサービスを提供している。(ISC)² のフィロソフィーとして、政府機関からは直接的な資金援助は受けていない。(ISC)² の組織概要は表 4-6 のとおり。

表 4-6 (ISC)² の概要

名称	International Information System Security Certifications Consortium, Inc.（(ISC)²）
所在地	Virginia 州 Vienna
設立	1989 年
活動目的	情報セキュリティ資格試験 CISSP 試験／SSCP 試験の運営、教育／セミナーの提供
従業員数	35 名（フルタイム）のほか、CISSP 取得者のボランティア 300～400 名が全世界で活動を支援

(ISC)² は、12 名の理事会（Board of Directors）及び委員会（Committee）と呼ばれる組織が設置されており、それぞれの活動は CISSP 資格の取得者のボランティアによって支えられている。理事会は、(ISC)² の全体を統括及び戦略策定に権限を持つ。また、資格試験の知識体系である「Common Body of Knowledge」（後述）の策定及びアップデート、資格試験問題の策定などの実作業は、それぞれの委員会のメンバーが担当する。

（3）CISSP 試験と SSCP 試験

(ISC)² の活動の重要なコンポーネントの一つは、情報セキュリティプロフェッショナルを対象とした資格認定制度の運用である。

(ISC)² では、以下の 2 タイプの資格認定試験を提供している。

（ａ）CISSP（Certified Information Systems Security Professional）
　情報セキュリティポリシーの策定に携われるマネージャクラスを対象とした試験
（ｂ）SSCP（System Security Certified Practitioner）
　組織内で情報セキュリティを実施する専門技術者（practitioner）を対象とした試験

CISSP 試験については、現在 72 カ国で受験可能であり、2002 年 12 月の時点で約 15,000 人が資格を取得している。資格取得者数は、過去 4 年間に年率 100%で伸びてきているという)。また、アジア・太平洋地域の資格取得者は約 2,000 人となっている。なお、SSCP 試験については、昨年より開始された新しい試験区分であるため、現時点ではまだ実数は把握されていないとのこと。ただ、今後は SSCP 試験の方がよりニーズが高くなることを見込んでいるという。

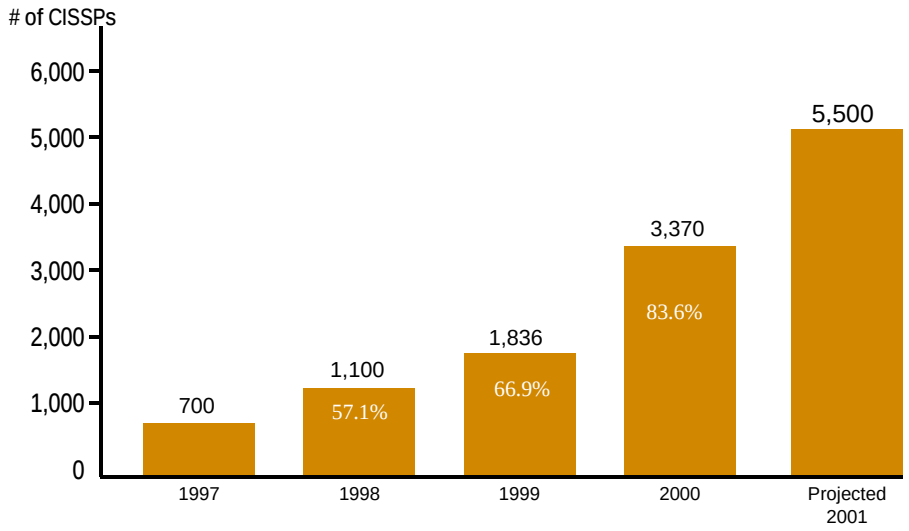

図 4-1　CISSP の資格取得者数（1997～2001: 2002.12 には 15000 になる見込み）

試験問題は、特定のベンダーに依存しない情報セキュリティに共通的な項目となっている。また、受験者の能力をより科学的に分析するため、心理学に基づいたテスティング手法（Psychometric Testing）を取り入れている。

受験資格の一つとして 3 年以上の業務経験を証明することが求められる。また、資格の有効期限は 3 年間となっており、その間に 120 時間の継続教育を受講しているか、ボランティアとして(ISC)² の委員会等の活動に参加していれば再試験は免除される。

情報セキュリティにたずさわる人材に対しては、特に倫理性が求められることから、資格取得の適格要件として、(ISC)² の定める倫理規範（Code of Ethics）の遵守が求められる。資格取得者が倫理規範に反する行為を行った場合、資格及び将来の受験資格が剥奪される場合がある。

（4）Common Body of Knowledge

(ISC)²では、「Common Body of Knowledge（CBK）」は情報セキュリティ関連の知識を体系化したデータベースである。CBK は、CISSP を取得したメンバーが世界各国の企業から、現場で必要とされる知識やスキルを収集して策定される。技術の変化に対応するため、CBK の内容は毎年更新されている。

CISSP 試験と SSCP 試験の試験や教育カリキュラムは、CBK に基づいて行なわれる。CISSP 試験と SSCP 試験とで CBK の内容は異なっており、その大分類（ドメイン）はそれぞれ以下のとおりである。

（ａ）CISSP 試験

- セキュリティマネジメントプラクティス（Security Management Practices）
- セキュリティアーキテクチャとモデル（Security Architecture and Models）
- アクセスコントロールシステムと方法論（Access Control Systems & Methodology）
- アプリケーション開発のセキュリティ（Application Development Security）
- 運用のセキュリティ（Operations Security）
- 物理セキュリティ（Physical Security）
- 暗号（Cryptography）
- 電気通信、ネットワーク、インターネットのセキュリティ（Telecommunications, Network, & Internet Security）
- ビジネス継続計画（Business Continuity Planning）
- 法律、捜査、倫理（Law, Investigations, & Ethics）

（ｂ）SSCP 試験

- アクセスコントロール（Access Controls）
- 管理（Administration）
- 監査とモニタリング（Audit and Monitoring）
- 暗号（Cryptography）
- データ通信（Data Communications）
- 悪意あるコード／ソフトウェア（Malicious Code/Malware）
- リスク、対応、回復（Risk, Response and Recovery）

CBK は非常に大きなドキュメントセットであり、(ISC)² の知的財産であることから、一般に公開はされていない。(ISC)² の教育サービス機関である「(ISC)² Institute」が提供する「CBK Seminar」を受講することで CBK の内容の講義が受けられる。

（5）米国における情報セキュリティにたずさわる人材の現状

(ISC)² 関係者によると、数年前までは米国の企業では情報セキュリティは「IT プロ

フェッショナル」業務の一部としてみなされることが多かったが、情報セキュリティの重要性の高まりを受けて、現在では「情報セキュリティプロフェッショナル」としてエキスパートが担当すべき分野であると認識されるようになってきているという。そのため、情報セキュリティプロフェッショナルのためのキャリアパスを設定している企業も多い。情報セキュリティプロフェッショナルに対する需要は高く、キャリアマーケットとして成立している状況がうかがえる。実際、IT 分野一般のエンジニアの給料が低下傾向にあるにもかかわらず、情報セキュリティ関連のエンジニアや管理者の給料水準は上昇を続けている。米国の資格情報誌「Certification Magazine」によると、CISSP を含め情報セキュリティ関連の資格取得者の給与は、IT 関連の資格取得者の中で上位にランクされている。

企業におけるセキュリティポリシーの策定とその実践にあたっては、シニアレベルのプロフェッショナルが担当する必要があると認識されている。そのような人材に大しては、技術知識だけではなく、法律、システム運用プランニング、ビジネスプロセスやヒューマンリソースのマネジメントなど幅広いスキルが要求されている。

（6）情報セキュリティの教育及び資格制度のあり方について

(ISC)² の目標は、情報セキュリティ分野において、その資格を持たないとその職種に事実上就けないような「職業資格」のデファクトスタンダードを確立することにある。それによって、資格取得のインセンティブにもつながると、(ISC)² では考えている。

また、情報セキュリティの教育及び資格制度においては、技術の変化が非常に早いことに対応していくことが重要な要件であり、継続的な教育が不可欠である。CISSP 試験／SSCP 試験では、3 年間の有効期限を設けており、その間に研修を一定時間受講することを義務付けている。我が国の情報処理技術者試験は一度合格すると終身で認定され、この点が大きく異なっている。

加えて、情報セキュリティ教育においては、共通的な知識と特定の製品に関する知識のバランスを如何に図るかが重要になるが、企業では、情報セキュリティやそのベースとなる IT やネットワークに関する基礎的な教育を体系的に教えるのは、時間、コスト、講師の問題から難しい場合も多い。その意味で、基礎的な情報セキュリティ教育の場として、大学等の教育機関に対する期待は大きい。

近年、米国においても情報セキュリティエンジニア向けのキャリアコースの必要性が認識され、採用されるようになってきており、大学院の修士号取得コースの設置が増えているという。ヒアリングを行なった(ISC)² 関係者の話によると、(ISC)² では大学とのアライアンスを検討しているところであり、CBK の内容を大学のコースとして教えることも計画しているとのことである。

４．１．２．３ 課題の整理

ヒアリングを行った(ISC)² を含め、米国では民間の団体や企業による情報セキュリティ関連の資格が認知されており、これらの資格の取得が給与水準に直接反映されること

もあって、受験者数は大きく伸びている。これらの試験の多くは、情報セキュリティ分野の技術や知識の変化のスピードが速いことから資格の更新制度を取り入れている。また、試験実施団体は、資格試験とリンクした形で教育サービスを提供し、資格取得後も継続教育サービスを行うビジネスモデルを確立している。

我が国においては、国が認定する情報処理技術者試験など国による試験制度が運用されており、企業においても重視されている。一方で、我が国の企業では人材の能力開発は OJT が中心になっており、資格は人材の能力を測る付加的な要素にとどまっているケースも多い。加えて、厳しい経済環境のもと、情報セキュリティの専門技術者や専任担当者による情報セキュリティに対する対応体制を整備する余裕がない企業も多く、情報セキュリティにたずさわる人材の採用や育成が進んでいないことが指摘されている。情報セキュリティ教育と資格試験制度のあり方に関しては以下のような点が課題になるといえる。

- 我が国の資格試験制度において、継続教育と資格の更新制度をどのように位置付けるか。
- 民間部門や地方自治体における情報セキュリティにたずさわる人材の充実に向けて、政府の果たすべき役割は何か。
- 我が国の資格試験制度において、国際的な整合性を如何に確保するか。

４．２ 最新の情報通信技術におけるセキュリティ方策の検討

E to E（エンド・トゥ・エンド）通信、ワイアレス通信、常時接続などの普及は、今後の情報セキュリティのあり方を検討する上での影響が大きいものと思われる。

本節では、社団法人電子情報技術産業協会(JEITA)会員企業ならびに電気通信事業者へのヒアリング結果をもとに、上記の分野の状況について俯瞰し、情報セキュリティ上の課題を整理する。

４．２．１ EtoE 通信、常時接続、ワイアレス通信、モバイル環境の状況について

EtoE 通信、ワイアレス通信、常時接続等のキーワードで表される、主として個人ユーザの先進的通信技術によるネットワーク接続が盛んになっている。ADSL に代表される高速大容量回線の普及がこの流れを支えている。DSL 加入者数の急激な増加は、2000 年 12 月末 9,723 件、2001 年 12 月末 1,524,564 件、2002 年 12 月末 5,645,728 件という累積加入者数の伸びが示している。2003 年 1 月の 1 ヶ月だけで 50 万件弱の加入者数を数えるが、前年同月の加入者数は僅か 1 万 8 千件であった（総務省調べ)。また、平成 14 年 9 月には、それまでの ISDN 接続加入者が DSL 移行のためにアナログ回線に復帰するに際し同番移行が可能となり、同時に DSL 接続業者の新規参入と定額料金の低価格化により、以後の加入者数は急増している。制度変更が、利用者動向に影響を与える格好の例である。また、2002 年末からは、光ファイバー接続サービス提供が本格化したことで、今後の大容量・高速回線利用者数は一層の増加を見せることであろう。

さて、接続料の低価格化とともに、一般公衆回線を用いたダイヤルアップ接続による従量制から定額制への課金体制の移行が、大量のネットワーク加入者数の生起理由であると見られるが、利用者は接続時間の増加による回線使用料の高額化という恐怖に怯えることなく、ネットワーク接続を継続できるようになることで、安価もしくは無料で配布・ダウンロードされているコンテンツ流通を支える高機能のアプリケーション・ソフトウェアが利用可能になるなどの、応用面での裏支えも大きい。ネットワークを介したファイルの共有化、常時接続の利点を最大限に生かしたチャットルームやメーッセージ交換ソフトに代表されるリアルタイムな情報交換機能の実現は、容易にインターネットによる EtoE 通信を可能にした。またバージョンアップの都度より便利になっていく WEB ブラウザーや、電子メールソフトウェアが、ネットワークに接続されたコンピュータを日常生活の中の通常の道具に変化させた。コンピュータが常に動作している（ネットワークに接続中）家庭も多いことであろうことは容易に想像できる。また、光ファイバー網利用による、動画配信もこれからますます盛んになるであろう。

一方、無線 LAN に代表されるワイアレス通信では、米国市場の例であるが、2002 年の無線 LAN 関係の小売売上が前年の 4 倍、平均小売価格は低下したとの調査報告が出されている（NPDTechworld)。同様に米国市場の例であるが、2002 年の企業向け出荷無線 LAN 製品の台数は、前年比 65%増、一方、家庭用無線 LAN 製品の出荷台数は、同 160%の伸びの見込みとの調査報告も伝えられている(In-Stat/MDR)。この分野での過去の例からみて、米国市場の動向は、程なく日本の動向につながるものとしてよいから、日本においても、それほどの時間を経ることなく、多くの企業、家庭において無線

LAN・ワイアレス通信が常態になるものと思われる。

上の通り、昨年から今年にかけての爆発的利用者増加を示しているこれら先端的情報通信技術は、インターネットの利用環境を劇的に変化させる可能性をもった強力な技術である。それゆえに、セキュリティを蔑ろにしてメリットにのみ注目した場合の被害の評価が重要である。現状のセキュリティ対策は、セキュリティ意識の高い層が自発的・自助努力的に行っているのが実態である。一般利用者の意識の啓発が必要であるとの指摘がある。セキュリティ対策は、生産財としての情報処理基盤ツールをセキュアに運用する道具であり、それ自体はなんらの生産を行うものではないところに、一般企業・利用者の積極的な関与を誘えない弱点がある。またそれは情報システムとネットワーク利用の足枷になる惧れもある。セキュリティと利用促進のバランスをとった施策が要求される。特にある程度の資金力を有する公共部門・民間大企業のセキュリティ対策は昨今の状況から見て比較的進められているということができるが、中小組織、一般家庭に同様の対策を期待するのは無理がある。しかし、ネットワークに接続されたコンピュータに向けられた脅威には、その所有者による差異はなく、結果的に弱いところからネットワーク全体に綻びが広がることが予想される。現在のインターネットはその程度の脆弱なものでしかない、ということを認識しておくことが重要である。とりわけ、情報家電と呼ばれる所謂白物家電とコンピュータネットワークとの接続は一般家庭の物理的存在の制御と直接に関係する方向で進んでおり、単にネットワークを流通する情報のみのセキュリティでは済まないところに、大きな危険が潜んでいる。少なくともセキュリティ対策を施した上でネットワークに接続しているという意識を高め、かつ一定のセキュリティ水準を有する情報機器を利用できる、という面で、現在進められている幾つかのセキュリティ標準化認証対策は意味があると言える。また対象となる組織・個人に対応した推奨セキュリティ対策案の啓示は有意義ではあるが、それが単なる意識の啓発活動に終わってしまわないようにすることが必要である。コンピュータ専門家ではない一般人が行うセキュリティ対策は、物理的世界のセキュリティ対策（火の元に注意し、窓を閉め、玄関の鍵を掛けて外出する(3 ステップ)。自動車のエンジンを止め、ドアに鍵を掛けてクルマから離れる(2 ステップ)）と同程度の複雑性に止めておく必要があるのではないかと思われる。

常時接続・無線 LAN の一つの将来形として、ユビキタスコンピューティングという概念があるが、そのセキュリティを考えたとき、＜ユビキティ＞と＜セキュリティ＞は相反する概念であることは認識しておく必要がある。情報セキュリティは、ある意味で利用を制限し禁止する方向のベクトルをもった概念であり、ユビキティは何時でも何処でも誰でも使えることを目指した汎化概念である。両者のバランスを求めた活動は永遠に続くものである。

４．２．２ 最新の情報通信技術におけるセキュリティの現状と課題

常時接続環境、無線 LAN 環境における情報セキュリティ対策は、市場創生初期段階、利用開始初期段階の通例にもれず、後回しになっているのが現状のようである。メーカー・ベンダーは市場そのものの開拓・立ち上がり・当該市場における占有率の確保、を

第一義として、サービスのポジティブ面のみの強調に走り勝ちであり、またセキュリティ機能等の付加操作を製品操作性の低下要因とみなす傾向が強い。また、利用者においては、情報セキュリティの脅威に対する注意力が不足気味であり、同時に、セキュリティ強化処理の設定の煩雑さから、ないがしろにし勝ちである傾向が見える。

広く指摘される、常時接続・無線 LAN についての情報セキュリティの脅威に対する課題は、悪意のハッカー・クラッカー等の攻撃からの防禦、信頼できる認証系の構築（成りすまし・誤接続の回避・盗用）、情報の秘密を守る機能の整備（盗聴・漏洩（傍受）の回避）をあげることができる。これらは、一般論として指摘されれば、メーカー・ベンダー・ユーザーは等しく認めるところであるが、対策が進んでいるとは言い難い現状がある。

OECD 情報セキュリティガイドラインの 9 原則に照らせば、すべての原則に当てはめて対策を施さねばならない現状であることがみてとれる。

特に喫緊の課題として、

- メーカー・ベンダーに対するセキュリティ対策を施した製品・サービスの提供を促す制度上の課題
- 通信回線提供者に対する、セキュリティ品質を高めた回線提供を促す制度上の課題
- ユーザに対するセキュリティ認識の向上を目指した、教育・訓練（特に、OECD 情報セキュリティガイドラインの 9 原則中、認識、責任、倫理の原則）上の課題
- 利用が簡便なセキュリティツールの開発支援上の課題

等をあげることができる。

サイバー犯罪に特徴的なことは、一般的国内法に基づく刑事罰による犯罪抑止力は期待できないことである。その意味で、

- サイバー犯罪に対する国際協力対応の緊密化

は早急に対処にしなければならない課題である。

４．３ 情報セキュリティ監査のあり方の検討

今後重要性が一層高まると考えられる情報セキュリティ監査について、国内外における関連情報の収集ならびに関係者へのヒアリングの実施を通じて、そのあり方についての検討を行なった。

なお本テーマについては、本調査と並行して平成 14 年 8 月から 15 年 3 月にかけて経済産業省により「情報セキュリティ監査研究会」が開催され、今後の監査制度のあり方についての検討がなされている。ここでは OECD 情報ガイドラインの原則論の観点から、研究会の成果を踏まえた分析を行っている。

４．３．１ 情報セキュリティ監査と関連する検査の現状

情報セキュリティ監査については、後述するように現在わが国においてその準拠対象とすべき明確な基準が存在しないため、現時点で「情報セキュリティ監査」と称されている活動の範囲は必ずしも明確ではない。厳密な解釈によれば、情報資産を対象とするマネジメントサイクルの実現状況を評価することのみが情報セキュリティ監査となり、このような解釈を行った場合は、現状では該当する活動がほとんど行われていない結果となる可能性が高い。

そこで、監査の対象をその構成要素の 1 つである脆弱性検査に相当するものまで拡大した範囲での実施の動向について、以下の団体、事業者にヒアリング調査を実施した結果を整理する。

- 特定非営利活動法人 情報ネットワークセキュリティ協会(JNSA)
  （情報セキュリティ監査サービス事業者の参加団体）
- 株式会社ヒューコム
  （情報セキュリティ監査サービスの提供事業者）

(1) 情報セキュリティ監査に関するニーズ

情報セキュリティ監査の現状について、需要側ニーズをもとに整理した結果を示す。

（ａ）情報セキュリティ監査と脆弱性検査の切り分けについて

現状において、情報セキュリティ監査と脆弱性検査等との切り分けは必ずしも明確ではない。提供するメニューの中から、これだけ揃えれば監査などと分類されているわけではなく、大まかなところでは現状であるがままの脆弱性を診断するのが検査サービス、セキュリティ運用体制やポリシーの有効性・準拠性の評価まで含めたものが監査サービスといった区分がなされている。

（ｂ）情報セキュリティ監査の実施状況

脆弱性検査については民間企業のほか、官庁、自治体など、幅広い利用がある。ただし、情報セキュリティ監査として機能させるためには、セキュリティポリシーやマネジメントシステムが整備されている必要があるが、自治体などでは未整備の

組織が大半であるため、現在のところ監査として実施可能なところは少ない。

（2）サービス提供側事業者の状況

（ａ）情報セキュリティ監査の実施主体

現在、監査に取組もうとしている事業者としては、会計法人系、コンサル系、技術系の 3 種類の流れがあるが、すべてを 1 社でできるところはない。どのような業態で、どのようなところまで対象とするのかの分担が今後できてくるものと考えられている。

（ｂ）脆弱性検査のコストの考え方

脆弱性検査のコストは、商用ツールの使用に要するコストに依存する部分が少なくない。こうした商用ツールを使用するにあたっては、検査対象とするネットワークの IP アドレスの数だけツールを使うための専用のライセンスキーを購入する必要があり、検査対象の規模が大きくなるのに比例してコストも増大することになる。

４．３．２ ガイドラインや各種制度の整備等に関する国内外における動向

情報セキュリティ監査に関するガイドラインや各種制度について、国内ならびに海外における動向の調査結果を整理する。

（1）日本国内の動向

前述したように、経済産業省において「情報セキュリティ監査研究会」が実施されている。この研究会において、下記に示すような諸制度の策定が検討されている。なお、ここに示す名称ならびに定義は 2003 年 2 月時点のものであり、最終的には変更となる可能性がある。

- 情報セキュリティ管理基準
- 情報セキュリティ監査基準
- 個別管理基準（監査項目）策定ガイドライン
- 実施基準ガイドライン
- 報告基準ガイドライン
- 情報セキュリティ監査企業台帳
- 電子政府情報セキュリティ管理基準モデル
- 電子政府情報セキュリティ監査基準モデル

（2）海外における動向

米国内の例として、GAO(Government Accounting Office)が連邦政府についてのセキュリティ監査基準を定義しているものが挙げられる。内容については、NIST（National Istitute of Standard and Technology：米国国立標準技術研究所）など各種の機関で分担した結果が反映されており、その中には侵入テストの実施方法のガイ

ドラインも含まれている。

Federal Information System Controls Audit Manual:
Volume I Financial Statement Audits. AIMD-12.19.6, June 2001.[1]
Appendix III 3.4 SYSYTEM SOFTWARE
（侵入テストの対象に指定されている機器の例）

- on-line transaction monitors
- database software
- on-line editors
- online direct-access storage devices
- on-line operating system datasets
- exits related to the operating system, security, and program products
- controls over batch processing

４．３．３ 情報セキュリティ監査のあり方をめぐる論点

情報セキュリティ監査の現状と今後の方向性において、課題となりうる事項について論点として以下に列挙し、OECD 情報セキュリティガイドラインの原則が示す方向性をもとにその解決のあり方について展望する。

（1）ISMS 認証との差異について

ISMS 認証制度は、その認証を受けることにより情報セキュリティに関する一定のレベルを確保していることを保証する手段として極めて有効な制度である。

ただし、ISMS の認証を得るためには現状での一般的なセキュリティの水準と比較して、相当に高いレベルが要求され、これはすべての事業者にとって適切であるとはいえない。また、ISMS の適合性認証の判定においては、既定された水準に達しているか否かを判断するのみであり、中間的な段階を表現することができない。これは ISMS 制度では想定されていない用途であり、こうした用途で活用するのであれば、別途制度を検討する必要がある。

情報セキュリティ監査においては、現在検討されている制度によれば、BS7799 part2 に準拠して対象とする組織の妥当性を診断することになっており、この部分のみを比較すれば、ISMS 認証と大きな違いはない。ただし、ISMS 認証制度における上述の不足要素を満足するようにすることで、ISMS 認証を得ることが現実的ではない組織の情報セキュリティに関する水準を段階的に評価、保証することができる制度とすることが可能になる。これは、OECD 情報セキュリティガイドラインにおけるリスクアセスメントの原則の附属文書において言及されている「リスクの許容レベル」を反映する意味で重要な効果を及ぼすものと期待される。

具体的には、以下の事項について今後分析していく必要がある。

[1] http://www.gao.gov/special.pubs/ai12.19.6.pdf

・ 実用性の観点から、段階的な水準を設けるべき対象は何か。
・ 段階的な設定と評価のあり方はいかにすべきか。

（2）監査とコンサルティングの分離の問題を含む監査モラルのあり方

上述の「情報セキュリティ監査研究会」報告書案においては、電子政府の監査を行う場合を例に、従事者としての独立性として以下の条件を満たすべきことが提案されている。

・ 監査を実施する企業ないし全ての監査従事者が、過去 3 年以内において被監査主体における情報システム（関連業務を含む）の企画、開発、運用及び保守に係る業務を行っていないこと。
・ 監査を実施する企業ないし全ての監査従事者が、過去 3 年以内において被監査主体における情報セキュリティのマネジメントや、マネジメントにおけるコントロール（関連業務を含む）の企画、運用、及び保守に係る業務を行っていないこと。
・ 監査従事者の中に、現在または過去において、被監査主体の在職者であるものが含まれないこと。

ただし、構築を担当していない別事業者に監査を委託する場合、システムの内部情報をすべて把握する必要があるため、それ自体がリスクを招くのではないかという指摘がなされている。また、情報セキュリティ監査を、監査対象におけるマネジメントやコントロールの状態の適切性を示す「保証型監査」と、問題点を指摘と改善提案を行うことを主体とする「助言型監査」の 2 種類に分類したとき、「助言型監査」とコンサルティングについては、分離するとはいえ両者の業務範囲が重なる部分も少なくないものと推定される。

今後の監査モラルの検討に際しては、OECD 情報セキュリティガイドラインにおける倫理の原則「参加者は、他者の正当な利益を尊重すべきである」をもとに、関係者の正当な利益が守られることを念頭に置いた基準作りが求められるものと考えられる。

（3）ユーザ側意識の向上の必要性

現時点においては、情報セキュリティ監査の制度自体が存在しないこと、セキュリティポリシーやマネジメントシステムの未整備などの理由により、情報セキュリティ監査はほとんど実施されていない状況にある。今後、制度的な整備が図られていくに伴い、公的機関としての責任上、監査の実施が求められる自治体等においては監査制度が急速に広まるものと考えられるが、民間事業者においては、どのような監査を行うかは事業者の自主性に委ねられることになる。

今後の情報セキュリティ施策においては、OECD 情報セキュリティガイドラインにおける、認識、リスクアセスメント、セキュリティの設計及び実装、セキュリティマネジメント、再評価の各原則の趣旨をもとに、利用者に対して情報セキュリティ監査制度の積極的な利用を促すような施策の立案、推進が不可欠になるものと想定される。

なお、（1）でも述べたように、ISMS 的なマネジメントシステムと現状とのギャップは大きいため、その差を埋めるための段階的なアプローチが求められることになろう。

４．４ セキュリティホールに対する関係者間の役割と責任分担のあり方の検討

対策の重要性が指摘されながら、これまで普遍的な対策方針の定まっていなかったセキュリティホールに関する関係者間の役割と責任の分担のあり方について、現状や事例についての情報収集ならびに関係者へのヒアリング調査をもとに分析を行った結果を示す。

４．４．１ セキュリティホール情報に関するこれまでの経緯と課題

これまでに論議のあった内容について、セキュリティホールに関わる各参加者(participants)における考え方と、参加者相互の関わり（製品の購入、利用、連絡、対応など）における課題を整理する。

(1) 各参加者における考え方

セキュリティホール情報の公開ならびに流通について、参加者ごとの利害や意向はおおむね以下のように整理される。

（ａ）開発者、ソフトウェアベンダー

ソフトウェア上の脆弱性の責任を負う参加者である。脆弱性情報の公開に際してはそれを速めることにメリットはないが、脆弱性が既知であるにもかかわらず、ユーザにその情報を伝える努力を怠った場合は問題となる可能性がある。

実際、2003 年 1 月のいわゆる SQL Slammer ワームで大きな被害を被った韓国においては、原因となった製品のベンダーである米国 Microsoft 社を提訴する動きが生じている。ただし、現時点の解釈では、製造物責任の範囲は媒体のみであり、ソフトウェアのような無形物に対してメーカに責任を問うことはできないとの判断が世界的にも主流となっている。

（ｂ）システムインテグレータ

システムで用いるソフトウェアの利用者としてのユーザ側ニーズと、システムの提供者としてのベンダー側ニーズが混在する。システムの構築方法に依存する脆弱性についてはインテグレータが責任を有する。

（ｃ）サービス提供者のニーズ

脆弱性があることを認識した状態でサービスを提供することは、利用者への背任になるため脆弱性情報を知る権利と対応義務の両方を有する。このとき、サービス事業者は自らのサービスを停止することにより脆弱性の影響を回避することが可能であるため、パッチ等による脆弱性への対策手段が準備できていない段階でも、脆弱性情報の開示を望む声がある。

（ｄ）セキュリティサービス事業者、セキュリティ研究者

脆弱性情報の発見者となった場合、それを公表することは自らの技術力の PR 手段となりうるため評価されることを望むが、反面脆弱性情報を公開することで犯罪

者扱いされない権利が保証されるべきである。よって、ガイドラインの制定へのニーズが最も高い参加者とみなすことができる。

（ｅ）ユーザ側のニーズ

提供されるサービスを利用するだけのユーザの場合、単純に考えれば脆弱性の開示に支障はないことになるが、実際にはユーザの個人情報等を管理している事業者において適切な対応が期待できないと想定される場合は、安易な開示は好ましくないことになる。

（2）参加者相互の利害の不一致と中立機関の役割

以上の各参加者の意識について整理した結果を表 4-7 に示す。

これによれば、脆弱性情報の公開に関するベンダーとユーザの利害は一致しておらず、ベンダー側のみの意向で制定されたガイドラインでは、情報システムとネットワークに関する脆弱性からユーザを保護するには不十分であることが想定される。この対応策としては、ガイドラインの策定に全ての参加者が参加し、中立かつ合理的な運用ルールを導入することができれば望ましいが現実的ではない。そこで、中立的な第三者機関における脆弱性情報の管理・提供が重要となる。

代表的な第三者機関である米国 CERT/CC の場合、様々な経緯を経て現在は独自のポリシー[2]のもとで脆弱性情報の公開を行っている。その概要を以下に示す。

- CERT/CC に報告されたあらゆる脆弱性情報は、報告のあった日から 45 日後に、影響を受けたベンダーからのパッチあるいは回避策の存在ないし利用可能性にかかわらず一般に公表する。
- ただし、攻撃手段の有無や影響の深刻さ、既存の標準的な状況の変更が必要となる状況の発生の有無などにより、公表までの期間を増減させることがある。

ここで既定された 45 日後の公表ルールに反した例としては、2002 年 2 月の SNMP (Simple Network Management Protocol)に関する脆弱性情報について、公表が再度にわたって延期となったケースが知られている。このときは、SNMP を用いている製品の数が多く、影響が広範囲にわたることが確実であったことが、公表延期の原因となっている。

[2] The CERT/CC Vulnerability Disclosure Policy: http://www.kb.cert.org/vuls/html/disclosure

表 4-7　セキュリティホール情報の流通制度の整備に関する各参加者（participants）の意向の整理

	現在の不満･ニーズ (情報流通への期待)	懸念材料 (情報流通の悪影響)	各参加者 (participants) 別の要望 (左欄の主体による上欄の参加者へ) と施策ニーズ (矢印部分)				
			ソフトウェアベンダー	インテグレータ	事業者	セキュリティ研究者	一般ユーザ
ソフトウェアベンダー	• 対応する前に脆弱性情報を開示される。 • 自社以外のソフトウェアとの組合せで生じるものは対応できない。	• 了承なしに勝手に自社製品の情報が流通するのは困る。		• 発信する情報へはインテグレータの責任で対応してほしい。 **→コンセンサス醸成**	• 古いバージョンに対応する情報はいつまでも発信できない。 **→コンセンサス醸成**	• 勝手に情報開示しないでほしい。 **→報告･開示ルールの制定**	• 初心者向けに都度丁寧な説明をするのは困難。 **→セキュリティ啓発**
インテグレータ	• パッチへの対応が困難な場合がある。 • 過去の製品の脆弱性への対応が不十分なことがある。	• 顧客 (事業者) が対応する前に情報がオープンになるのは困る。	• 脆弱性の生じにくい製品の開発。 • より速やかな情報発信。 **→コンセンサス醸成**		• 継続的サポートの重要性の認識。 **→コンセンサス醸成**	• 勝手に情報開示しないでほしい。 **→報告･開示ルールの制定**	(接点は少ない)
事業者 (民間･電子政府など)	• 複雑なシステムの場合自らは脆弱性の影響を評価できない。 • パッチへの対応が困難な場合がある。	• 自分達が対応する前に情報がオープンになるのは困る。	• 脆弱性の生じにくい製品の開発。 • インテグレータとの連携の強化。 **→コンセンサス醸成**	• 瑕疵対応責任。 **→コンセンサス醸成**		• 勝手に情報開示しないでほしい。 **→報告･開示ルールの制定**	• セキュリティに対する意識を高めてほしい。 **→セキュリティ啓発**
セキュリティ研究者	• セキュリティホール発見の報告をしても反応がない。犯罪者的な扱いを受けることがある。	• 一般ユーザに有益な情報がベンダーの意向で開示できなくなる恐れはないか。	• 報告に対する責任ある対応と姿勢。 **→報告･開示ルールの制定**	• 報告に対する責任ある対応と姿勢。 **→報告･開示ルールの制定**	• 報告に対する責任ある対応と姿勢。 **→報告･開示ルールの制定**		• セキュリティに対する意識を高めてほしい。 **→セキュリティ啓発**
一般ユーザ	• 情報が専門的で理解や対応が難しい。	• 情報の開示でかえって弱者が脅威に晒されることはないか。	• 脆弱性の生じにくい製品の開発。 • 対応の容易性の向上。	(接点は少ない)	• 対象サービスと脆弱性の関係についてのわかりやすい説明。	• 一般ユーザの立場も考慮した行動と倫理性。	

表 4-8　ソフトウェアのセキュリティホールに対する関係者間の役割と責任の分担に関する各国の状況

	ソフトウェアベンダー	サービス提供者 (各種プロバイダ)	行政･公的機関	セキュリティ関連団体(CSIRTほか)	セキュリティ研究者	サービス利用者
責任の分担						
法制度化されているもの	日) 製造物責任は媒体のみ 独) パッケージソフトには製造物責任が及ぶとの議論あり	日) アクセス制御の管理義務	日) 被害状況の把握		日) 不正アクセス防止法	日) 不正アクセス防止法
慣習的･商業上のもの						
自己責任レベルのもの						
セキュリティホールの発見時における役割　(非常時)						
セキュリティホールの発見と報告		(被害･痕跡の発見) (ベンダーへの報告)			(脆弱性の検証) (ベンダーへの報告)	
セキュリティホール修正	(修正版、パッチ作成)	(修正、サービス一時停止)			(修正版、パッチ作成)	(パッチ適用、設定変更)
セキュリティホールの当事者への支援		(被害･不具合情報の提供)			(問題箇所･原因の提案)	(被害･不具合情報の提供)
情報の交換			(影響を受ける諸機関への通知)		(被害回避方法の提案)	
情報の発信 (アナウンス)	(Web･メール等による通知) (アップデートサービス)	(ユーザ向けアナウンス)	(影響拡大防止のための周知)	(影響範囲と対策のアナウンス)		
情報の蓄積			(インシデント情報の蓄積管理)	(インシデント情報の蓄積管理)		
セキュリティホールの防止に向けた役割　(平常時)						
セキュリティホール発生の未然防止	(安全な言語･コンパイラの使用)	(脆弱性検査の実施)	米) セキュア版Linux (NSA) 世) 行政システムへのオープンソース製品の採用		(安全な言語･コンパイラの使用) 世) OpenBSDプロジェクト	
セキュリティホールの悪用事例の早期発見		(ログの常時監視)				
一方的公開や助長行為に関する規制	(セキュリティ窓口への連絡要請)		日) 不正アクセス防止法 世) サイバー犯罪条約		(発見時のルールの作成と遵守)	
開発者への啓発･教育	(開発者向け社内教育) (ベンダー資格制度の提供)	(セキュリティ要件の発注仕様への記載)	日) 各種資格･スキル標準の制定		(開発コミュニティ内の相互レビュー)	
利用者への啓発･教育	(ソフトウェアの自動更新機能の提供) (各種情報サービス)					
対応組織の設立	米) OIS	世) プライベートCSIRT	米) FedCERC 日) NIRT	米) CERT/CC 日) JPCERT/CC	米) Sardonix Audit Portal (政府支援のコードレビュー組織)	

凡例：カッコ内は一般的な対応例。ゴシック体は各国の政策事例。ただし世＝複数国によるもの。

４．４．２ ソフトウェアベンダーやセキュリティ事業者における取り組みの状況

前項までに示した各参加者について、セキュリティホール等による脆弱性の影響を抑制、防止するための取り組みや制度について、これまでの状況を整理した結果を、表４-８に示す。

以下ではこれらの参加者のうち、ソフトウェアの開発当事者、およびセキュリティサービスを商用ベースで提供している事業者が、脆弱性の発生の防止に向けて取り組んでいる状況について整理する。

４．４．２．１ セキュリティサービス事業者における取り組みの事例

脆弱性の発見に関する活動を実施している国内では実質的に唯一の事業者である、株式会社ラックに対してヒアリングを行った結果をもとに整理する。

(1) 脆弱性情報の発信活動の状況

ラック社が発見した脆弱性情報の公開媒体である SNS Advisory の発行を中心として、脆弱性情報の発信活動の状況は以下に示す通りである。

（ａ）脆弱性の発見活動の経緯について

脆弱性発見の活動を行うことになった経緯として、以下の 2 点が指摘されている。

- セキュリティ事業を行うに当たり、例えばファイアウォールの機能を評価する際には、攻撃側と同等以上の技術を身に付けておく必要があり、こうした技術を養うための手段として有効であるため。
- 脆弱性情報を発信することを通じて、他社との技術力の差をアピールすることが可能なため。

（ｂ）脆弱性の発見時の対応について

脆弱性を発見した場合、まず対象となる製品のベンダーに連絡し、対応を待った上で情報を発信するというルールは遵守されている。ベンダーの状況によっては、ベンダーへの連絡のみで、一般へ公表は行われないことも少なくない。また、脆弱性情報の発見活動は商用サービスと位置付けられておらず、コンサルティングと連携させることで収益を得るなどの対応は全く想定されていない。

脆弱性情報の連絡時の対応姿勢はベンダーにより様々であり、積極的な対応を行うところもあれば、連絡に対して好意的反応を示さないところもあると指摘されている。

（ｃ）脆弱性発信に対する反応について

ラック社が脆弱性情報を発信していることに対し、国内の行政、民間を含めた情報セキュリティ関係者の反応は必ずしも高くない。海外のセキュリティベンダーからは多くの問い合わせや情報提供の依頼がある。こうした傾向の差が生じる原因と

しては、脆弱性に対する問題意識の差が影響しているものと考えられる。

(2) 脆弱性情報のデータベース事業について

同社で提供している脆弱性情報データベース SNSDB に関して、その事業上の位置付けや状況は以下に示す通りである。

（a）脆弱性情報データベースの位置付けについて

一般公開を前提としている SNS Advisory と逆に、SNSDB は有料の契約者向けサービスである。SNSDB 事業自体による利益は他の中核となっている事業（検査、監視、構築、コンサルティング等）によるものと比較すると今のところまだまだ少ない。ただし、SNSDB の対象としている情報は同社自身の活動のためにも必要であるため、その必須経費と考えれば、自社の事業用の情報を外部にも売っているという視点で見れば収益性は悪くないことになる。

（b）CERT Advisory の日本語化について

SNSDB に載せるための情報の 1 つとして、CERT Advisory の日本語への翻訳が CERT/CC の許可のもとで実施されている。これも自社に有効に活用することが第一であり、外部への公開は副次的な活動とみることができる。

（c）脆弱性情報データベースについて

脆弱性情報データベースについては他社からも提供されているが、全ての情報を日本語化した上に、対象についての検証情報も提供するものは SNSDB のみであり、こちらについても差別化が実現されている。

(3) 脆弱性情報に関する他の参加者との関係

ヒアリングを通じて、脆弱性情報の扱いに関する他の事業者における現状での課題と要望について、以下に示すような意見が得られている。

（a）システムインテグレータ、ソフトウェア事業者

ラック社以外のデータベースを含め、脆弱性情報の購入を行っている事業者は必ずしも多くないようであるが、自社で同じ情報を集めようとしてもコストがかかるはずであり、その手間を考えれば脆弱性情報の購入には合理性がある。こうした情報を参照せずにシステム構築を行っている事業者が多いことに、根本的な問題があるのではないか。

（b）行政機関

ラック社で脆弱性を発見していることに対する、行政機関からの直接的な問い合わせなどはあまり多くはない。また、ラック社のほうから情報提供などを行うこともしていない。これは、関心があれば Bugtraq などのメーリングリストを参照して

いるはずであり、あえて別の情報流通のルートを作る必要性は見受けられないとの判断に基づく。

現在、それ以上の情報収集を積極的に行い、セキュリティ対策を主導的に進める段階にはないと推測される。

（c）ユーザ企業

自社のセキュリティポリシーを作成する際に、リスク分析に時間をかけるあまり、情報セキュリティ対策の実施が止まってしまうケースがみられる。現実のリスクに対処するためには、自社の情報資産は予め把握できていてしかるべきである。

４．４．２．２ ソフトウェアの提供者による取り組みの事例

ソフトウェアの提供側において、脆弱性による被害の抑制に向けて実施されている取り組みとして、世界最大のソフトウェアベンダーである米国 Microsoft 社と、オープンソース開発コミュニティの 1 つである OpenBSD プロジェクトの事例を示す。

（1）Microsoft 社の Trustworthy Computing

米国 Microsoft 社が 2002 年 1 月に今後の方針として、事業戦略においてセキュリティを重視することをアピールする際に用いた概念である。かつては、Microsoft 社においても、セキュリティホールに関する連絡をしても対応が曖昧であり、対策のリリースまでに時間を要するなど、世界最大のソフトウェアベンダーとしての責任を自覚していないとの批判が数多く見られた。

"Trustworthy Computing"の活動と、それ以前を含めてアプリケーションにおける脆弱性による被害の防止のため、Microsoft 社が実施している活動としては以下のようなものが挙げられる。

- 脆弱性情報の連絡窓口の設置
- 脆弱性情報の連絡窓口の設置
- 既知の脆弱性とその対策についての定期的な情報発信
  （Web サイト、メーリングリスト）
- 知識の高くないユーザに向けた脆弱性対策についての解説ページの設置
- セキュリティを高めるためのツールキットの提供
  （Strategic Technology Protection Program）
- 製品出荷時の脆弱性調査の強化とセキュリティ対策の優先対応
  （Secure Windows Initiative）

こうした活動の結果、同社の姿勢はこの概念を打ち出した頃より相当に改善の傾向が示されているというのが、一般的な認識となりつつある。ただし、既知の脆弱性に対し、すべての対策が公開されておらず、脆弱性が放置されていると指摘されるものが未だに存在するほか、2003 年 1 月に発生した同社の製品を対象とするワーム（SQL

Slammer）の蔓延の際、同社から半年以上前に対策パッチが公開されているにもかかわらず、同社内でも感染がみられたことなどは、依然として批判の対象となっている。

（2）OpenBSD プロジェクト

OpenBSD プロジェクト[3]は、Linux や FreeBSD などと同様に、UNIX と互換性のあるオペレーティングシステムをオープンソースによって開発しようとするコミュニティの 1 つであるが、プロジェクトの特徴としてセキュリティの重視を提唱している点に特徴がある。こうした特徴が実際の活動に反映している例を以下に示す。

（ａ）フルディスクロージャーによる対応

OpenBSD の場合、セキュリティを意識したコーディングを行っていることで、脆弱性が発見した場合でも速やか（Web サイト上では大半が 30 分程度と記載）に対応が可能なため、対応への準備をしている間、情報を伏せておくなど余計なプロセスの必要がなく、フルディスクロージャーが可能であるとの主張がなされている。

（ｂ）監査プロセスの存在

OpenBSD では 1996 年以来、6～12 人のメンバーがソースコードの監査作業に従事しており、脆弱性の事前の発見を可能にしている。この成果は、他のプロジェクトで脆弱性が発見された際でも、OpenBSD においてはすでに対応済みであった例が多い実績などにより裏付けられているとされる。なお、こうしたプロセスによっても脆弱性を皆無にできるわけではなく、過去 7 年間で少なくとも 1 件の脆弱性が、外部からの指摘で明らかになっている。

（ｃ）デフォルト時の高セキュリティ

オープンソースの OS においても、インストール用メディアの作成時にはユーザの利便性を考え、標準的なインストールを行った場合は実際に必要になるかどうかにかかわらず、各種のアプリケーションが OS の基本部分のインストールと同時にインストールされるように設定されていることが多い。ただしこの傾向は、実際に使わないアプリケーションはユーザが意識することも少ないため、セキュリティ上の盲点となりやすい欠点も有している。

OpenBSD プロジェクトではこうした問題点を考慮し、標準的なインストールを行った場合は必要最低限の機能のみが実装され、しかも利便性に支障があってもセキュリティを保つ設定が初期値として与えられる仕組みとなるよう配慮されている。

４．４．２．３ 脆弱性情報の開示に向けたルール策定の取り組み

脆弱性情報の開示に際し、対象となるソフトウェアの提供者と通報者、その他関係者にわたるルールの策定の動きについて、以下に整理する。

[3] http://www.openbsd.org/

（1）脆弱性情報の開示に関する IETF（Internet Engineering Task Force）ドラフトの提案

責任ある開示プロセスについてのベストプラクティスを提示することを目的として 2002 年 2 月に提案された。この提案者は後述の（2）に示す OIS(Organization for Internet Safety)の中心メンバーと同一である。ただし、提案は実施、公開されたものの、脆弱性情報の開示というテーマが IETF の扱うテーマではないということで却下の扱いとなっている。

提案されたルールの概要を以下に示す。

- ソフトウェアベンダーはセキュリティホールの報告者から脆弱性情報を受け取った場合、7 日以内に受信の旨を返答する必要がある。自動応答システムを用意している場合は、10 日以内に対処方針等を報告者に報告する必要がある。
- セキュリティホールの報告者は、ソフトウェアベンダーにその脆弱性情報を報告してから、一般に公開するまで少なくとも 30 日間の期間を置くことが求められる。
- 以下の場合、報告者はソフトウェアベンダーに対し、情報の公開までの期間に関して 30 日に限らない時間的猶予を与える必要がある：
  （ａ）問題が安全でない設計に由来している場合
  （ｂ）問題が影響するハードウェアや OS、製品の範囲が多数に及ぶ場合
  （ｃ）ソフトウェアベンダーのセキュリティ技術に関するスキルが不十分の場合。

（2）OIS(Organization for Internet Safety)

米国内のセキュリティサービス事業者と Microsoft 社を含むソフトウェアベンダー計 11 社が 2002 年 9 月に設立した団体である。セキュリティ情報の発表方法に関するルールの策定を目的としているが、設立についての報道発表後の目立った動きは見られない。

（3）Vulnerability Disclosure Guidelines（脆弱性開示ガイドライン）

米国のセキュリティサービス事業者 ISS が 2002 年 11 月 18 日に公表したもの。こうしたガイドラインがセキュリティサービス事業者によって提供された背景には、過去にフリーの Web サーバである Apache に関する脆弱性の情報公開において議論となったことが挙げられる。これは、2002 年 6 月に ISS が通知後わずかの期間で脆弱性情報を公開したため、Apache の開発元のみならず各方面から ISS が非難を受けたこと、を指す。ISS ではこうした指摘に対し、この脆弱性はアンダーグラウンドのコミュニティでも既知であったため、警告する必要があったと説明している。

４．４．３ 情報流通と緊急時対応のための組織による取り組み

国内の CSIRT(Computer Security Incident Response Team)として分類される組織による対応について、以下に整理する。

４．４．３．１ JPCERT/CC における取り組みの事例

日本における代表的 CSIRT 機関として知られる、JPCERT/CC へのヒアリング調査をもとに整理した結果について示す。

（1）JPCERT/CC による発信情報の種類

JPCERT で発信する情報の種類を、表 ４-９に示す。

表 ４-９　JPCERT/CC が発信する情報の種類

種類	情報発信の根拠
緊急報告	実際に多くの被害が寄せられている場合。個々にメールで対応するより、同じ内容であれば文書を公開したほうが望ましいと判断されるときに発行する。
注意喚起	概ね以下の条件のいずれかが満たされた場合に出すが、基準についてはケースバイケースであり、都度判断している。 • 広範囲にわたる脆弱性、もしくは特定のアプリケーションを対象とするものでも、影響するユーザが多いもの(例：Apache, IIS) • 攻撃用の手法が明らか、ないしは攻撃用のツールが既に出回ってしまっているもの • ワークアラウンドでもよいので対策、ないし回避策があるもの（回避策がない場合は待つ）
技術メモ	TIPS 集。個別に依存しないもの。必ずしも技術的なものばかりでなく、ポリシー的なものも含まれる。
レポート	ほぼ週に１回、定期的に発行。

（2）JPCERT/CC における情報の収集方法

JPCERT/CC が参加している IRT 組織の団体である FIRST (the Forum of Incident Response and Security Teams)のメーリングリストが主たる情報源となっている。この内容は参加組織限りの扱いとなっており、公開前の情報が流通する。このほか、ベンダー、民間コミュニティの協力者からの情報や、一般の Web サイトで公開されている情報についても収集対象となっている。

（3）JPCERT/CC が発信する情報の利用のされ方

現在の情報発信のタイミングでは、情報システムやネットワークの運用にたずさわっている現場の技術者にとって、JPCERT/CC から情報が出てから慌てて対応するようでは間に合わないのが実情である。これに対して、エンジニアが対策を実施した旨の報告を上部に行う際の根拠として、JPCERT/CC のような機関から出た日本語の情報の利用価値が高いことから、結果的に技術者層だけでなく、経営者層向けに役立っているとの指摘もある。

（4）JPCERT/CC とソフトウェアベンダーとの関係

ソフトウェアベンダーの JPCERT/CC への対応の姿勢はこの 1〜2 年で飛躍的に改善されている。これは、CodeRed、 Nimda などの騒動以降のことである。ベンダーにおける JPCERT/CC との付き合いの仕方が、単にユーザとして情報を使うだけの関係から、もっとプロアクティブに活用する方向に変化していると分析されている。情報開示の重要性の認識のもと、ユーザへの真摯な姿勢の表明の手段として、非営利中立機関をうまく使おうと考えているものとみられる。

ただし、協力的でないベンダーも未だに数多いとの指摘が得られている。米国ソフトウェアベンダーの日本法人の場合は、日本には販売窓口の機能しかなく、脆弱性に関する報告や問い合わせがあっても対応できないなど、状況として止むを得ないと判断されるものもあるとはいえ、協力的なベンダーとそうでないベンダーとの差が拡大する傾向が見受けられるようである。

（5）運営上の課題

現在は経済産業省等の支援により運営されているが、今後の運営のあり方については以前から議論が続けられている。米国 CERT/CC の場合、国防総省からの資金と４．１．１に示した ISA を経由した民間の会費による資金で運営されているが、日本でそのままの形で適用可能かどうかは疑問との意見が出されている。日本でもこれまで会員制度は検討されたものの、その時点では断念せざるを得なかったとされる。ただし、上述のように最近ではソフトウェアベンダーの姿勢が急速に変化しつつあり、今後は運営方法の見直しに向けた検討が進む可能性もある。

４．４．３．２ 行政による取り組み

行政組織による CSIRT の構築、運用に関する取り組みの事例について、以下に整理する。

（1）NIRT の役割と実施の状況

NIRT(National Incident Response Team)は、内閣官房情報セキュリティ対策推進室内に 2002 年 4 月に設置された緊急対応支援チームである。この組織の特徴を以下に整理する。なお、本記述は NIRT の総括・指導担当の大野浩之氏が 2002 年 12 月に JPCERT/CC セミナーにおいて講演した内容に主として基づいている。

（ａ）ミッション

政府機関においてインシデントが発生した際に、事態の正確な把握、被害の拡大防止、復旧、再発防止のための技術的対応策の検討、対策の実施に関する支援を行う。

（b）体制

官民のコンピュータセキュリティ専門家により構成される。

（c）活動状況

現在の活動としては、各種体制の構築、訓練と研修の実施、国際会議への参加などが報告されている。

(2) IPA/ISEC の役割と実施の状況

情報処理振興事業協会セキュリティセンター(IPA/ISEC)は経済産業省における情報セキュリティ政策を担う行政組織として、内外の情報セキュリティに関わる情報の収集、発信の中心的な役割を担っている。IPA の Web サイトにて公開されている内容をもとに、主たる活動の状況を以下に整理する。

（a）ミッション

わが国において情報セキュリティ対策の必要性・重要性についての認識を啓発・向上し、具体的な対策実践情報・対策手段を提供するとともに、セキュアな情報インフラストラクチャ整備に貢献する。

（b）体制

40 名弱の人員からなり、以下の各組織で構成される。

- RPG (Research and Planning Group)
- ORG (Outreach Group)
- Alert TF（緊急対策情報タスクフォース）
- CRYPT (Cryptography research and evaluation group)
- SECIA (Security Evaluation & Certification and Information Assurance group)

（c）活動状況

大別して以下に示すような活動を行っている。

- 情報セキュリティに関する啓発と対策実践情報の提供
- コンピュータウイルス、不正アクセスに関する届出受理と相談対応
- 情報セキュリティ対策調査・技術調達と成果の普及
- 暗号技術調査・評価事業
- 情報技術セキュリティ標準・セキュリティ保証関連事業
- 重要インフラストラクチャ情報セキュリティ対策

(3) Telecom-ISAC Japan の役割と実施の状況

Telecom-ISAC JAPAN は 2002 年 7 月に設立され、平成 14 年度中の活動開始を目標に、総務省の主導のもとで構築が進められている CSIRT 組織である。その概要を以下に示す。

（ａ）ミッション

システムの脆弱性情報などのセキュリティ対策を実施する上で有益な情報の分析・共有等を通して、ISP 事業者の情報セキュリティ対策を支援する。

（ｂ）体制

ISP 事業者を主たる会員とする。

（ｃ）活動状況

現在のところまだ開始されていないが、以下の活動が計画されている。

- システムの脆弱性に関する報告及び情報交換
- 対抗策及びそのベストプラクティスの提供
- サイバー攻撃、コンピュータ犯罪等の脅威及び被害情報の提供

４．４．３．３ 民間事業者による取り組み

ISP、ソフトウェアベンダーなどの事業者が、自らの事業におけるインシデント対応を行うため、社内にプライベートな CSIRT 組織を設置する傾向が徐々に見られるようになりつつある。

これには以下に示すようなメリットがあり、JPCERT/CC においても設置を推奨している。

（1）情報共有と体制整備の強化

情報セキュリティは事業者内の複数の部署の協力無しには実現し得ないが、既存組織相互の連携では主導権の問題なども生じやすく、うまくいかない場合が多い。これに対して、情報セキュリティを目的とする組織が主導するのであれば、各部署においても目的に応じた連携方法をとりやすく、合理的な対応が可能となる。

なお、CSIRT はインシデント対応が中心と考えられがちであるが、プライベート CSIRT の場合、通常時における情報セキュリティを意識するための活動において効果を発揮することも多く、通常時、緊急時（インシデント発生時）それぞれの役割を考慮して CSIRT 組織を検討する必要がある。

（2）情報セキュリティを通じた対外活動の容易化

CSIRT 組織を名乗ることにより、社外の同業種、他業種の CSIRT 組織と、情報セキュリティを共通のテーマに交流を行うことが容易になる。さらに、一定の条件をみたすことができれば前述の FIRST のような国際組織への加入も可能となり、メンバー

限りの情報が得られるなどもメリットも期待できる。

４．４．３．４ 研究機関による取り組み

現在、国内大学における情報セキュリティ研究活動の一環として、以下の 2 件の取り組みが実践されている。

（1）V-STAF[4]

米国 ISS 社およびその日本法人の協力のもと、同社の X-Force データベースを日本語化した脆弱性情報データベースの構築を行っている。早稲田大学村岡研究室が、特定非営利活動法人ネットワークリスクマネジメント協会(NRA)と共同で実施している。主な特徴は以下の通りである。

- 運営は早稲田大学の学生および NRA 会員企業のボランティアによって実施。
- 情報の番号および脆弱性が及ぼす危険度については、米国 ISS 社の X-Force データベースのものに対応。
- X-Force データベースに記載された内容の翻訳と、検索環境の提供がサービスのポイントとなっている。

（2）JPCERT/CC Vendor Status Notes (JVN)[5]

国内で利用されているソフトウェアや装置を対象に、国内の各ベンダーが提供する対策情報や更新情報へのリンクを提供する。2003 年 2 月に一般向けの公開利用が開始された。おもな特徴は以下の通りである。

- JPCERT/CC の支援のもと、慶應義塾大学の土居・高田研究室において情報の整備、公開等の作業を実施。
- 脆弱性情報の基準として CERT Advisory を使用し、その ID 毎に本プロジェクトに協力するベンダーが提供する日本語情報へのリンク集を提供。
- 脆弱性情報についての加工を行うのではなく、その付加価値として日本語情報へのリンクを体系的に整理した情報を提供することがサービスのポイントとなっている。

４．４．３．５ CSIRT 組織の連携

以上で示した各 CSIRT 組織をいかにして相互に連携し、ソフトウェアのセキュリティホールに代表される脆弱性への対応能力を強化させるかが、今後の課題となる。このとき、日本における CSIRT 機関の草分けであり、創設以来積極的にその中立性を維持している JPCERT/CC に、その核としての役割を期待する指摘は多い。

---

[4] http://www.v-staf.org/
[5] http://jvn.doi.ics.keio.ac.jp/

なお本件については、2003 年 1 月のいわゆる SQL Slammer ワームの被害に関する総括として経済産業省より発表されたレポートの中で、以下の 2 点に対して JPCERT/CC の強化が提案されており、今後の展開が注目される。

- 情報収集・相談窓口の強化
- 定点観測システムの構築

４．４．４ 行政によるソフトウェアの脆弱性に向けた取り組み

行政による脆弱性情報に関する取り組みとして、米国における政策動向、および海外諸国における対策事例について整理する。

４．４．４．１ 米国における政策事例

米国における脆弱性情報による被害発生の防止に向けた取り組みに関連する政策として、以下の事例が挙げられる。

（1）National Strategy to Secure Cyberspace

米国政府によるサイバーセキュリティの強化計画である。セキュリティに関する主たる責任は、“ Cyberspace ”のすべての利用者が負うべきものとし、以下の 5 つの重点(Priority)を定めている。

- セキュリティ対応システムの整備
- 脅威と脆弱性の減少に向けた取り組み
- セキュリティの啓発とトレーニングの取り組み
- 政府の電子化における安全の確保
- セキュリティに関する国内外の協力

この戦略は米国内 IT ベンダー等からは概ね支持されているが、セキュリティを自発的な行動に依存させている点への批判も見られる。パブリックコメントの募集期間を経たのち、2003 年 2 月 14 日に公表された。

（2）Computer Security Enhancement Act（コンピュータセキュリティ強化法）

連邦政府のネットワーク内のセキュリティを確保することを目的として、NIST（National Istitute of Standard and Technology：米国国立標準技術研究所）が連邦政府に対する指導と情報提供を行うとともに、行政向けの暗号技術や認証技術の標準化と普及の役割を担う。

（3）上院 2182 号法案

連邦政府が使用するすべてのコンピュータに適切な「最善のセキュリティ対策」を

施すよう義務付けるものである。

４．４．４．２ ソフトウェアの脆弱性に対する各国での対策事例

米国の事例と同様、脆弱性の発生の抑制および脆弱性情報の流通に向けた取り組みとして、オープンソースソフトウェアの採用と CSIRT 組織の構築の例を示す。

(1) オープンソースソフトウェア採用の動き

各国・地域におけるオープンソースソフトウェアの活用事例として、以下を挙げる。なお、オープンソースソフトウェアに対する各国政府の施策については、情報処理振興事業協会セキュリティセンターによる「オープンソースソフトウェアのセキュリティ確保に関する調査」の中で国別に詳細な分析がなされている。ここでは、情報セキュリティの観点から着目すべき事例を挙げ、分析を行うものとする。

（ａ）米国 NSA によるセキュリティ強化 Linux(Security-Enhanced Linux)の開発

米国 NSA (National Security Agency: 国家安全保障局)は、政府で用いる暗号の選定を行うなど、米国連邦政府における情報セキュリティ政策に重要な役割を果たす機関であるが、この機関内で機密情報を扱うために安全性の高いオペレーティングシステム(OS)が必要とのニーズをもとに開発されたものである。本来の Linux はその互換性の対象となった OS である UNIX と同様、特権ユーザ（スーパーユーザ）の立場を得ると事実上アクセス制御の対象外となるため、この欠点を克服するための機能を強化するための改良を、NSA が Secure Computing 社ならびにユタ大学との共同研究により実装したのが、この Security-Enhanced Linux (SELinux)[6]である。

現在の SELinux は研究用プロトタイプの位置付けであり、実用性から見た完成度は十分とはいえない。また Trusted OS の条件も満たしていないなど、情報セキュリティの向上の視点からはまだ有用とは言いがたい。ただし、将来的には Common Criteria(CC)の認定を受ける予定もあるなど、実用化に向けた取り組みを進めている途上にあるものとみることができる。

（ｂ）欧州委員会による eEurope アクションプラン

欧州連合(EU)の行政を司る機関である欧州委員会(European Commission)が 2000 年の 6 月に公表した施策：“ eEurope2002－An Information Society For All ”のアクションプラン[7]の中で、2002 年を実施目標とするオープンソフトウェアの普及促進の方針が示された。具体的な施策は以下の通りである。

・ 官民共同による、オープンソースソフトウェアを用いたセキュリティプラッ

6 http://www.nsa.gov/selinux/
7 http://europa.eu.int/information_society/eeurope/index_en.htm

トフォームの開発と展開。

・ 各国政府機関における手続きの電子化（電子政府）における、オープンソースソフトウェアの導入。

上例のうち後者に関しては、コストダウンの手段としてオープンソースを導入することのメリットが説かれているため、情報セキュリティとしての色彩は必ずしも強くないが、前者において開発されたプラットフォームの普及を通じて脆弱性の発生を抑制することで、情報セキュリティの確保を目指した期待した施策であるとみることが可能である。

（c）中国政府による Red Flag Linux の開発支援

中国政府は Microsoft 社などの米国企業により自国の安全保障が左右されることへの懸念から、Linux の独自のディストリビューションの開発支援を実施している。このディストリビューションは「Red Flag（紅旗）Linux」[8]と呼ばれ、中国政府において数多く導入されているとされる。なお、脆弱性対策という視点では、Red Flag Linux の Web サイト上では既知の脆弱性への対応に関する情報が表示されておらず、実際の状況は明らかではない。

（2）各国における CSIRT 組織の整備の動向

米国以外の CSIRT 組織についての整備の動向として、アジア太平洋地域における状況を示す。これらの各国は APSIRC (Asia Pacific Security Incident Response Coordination)に参加しており、その運営に際しては JPCERT/CC が主導的な役割を果たしている。

（a）オーストラリア

オーストラリアを代表する CSIRT 組織である AusCERT は、大学で発足した CSIRT をベースにしている点で米国 CERT/CC と類似している。ただし、現在は有料会員の会費による完全な民間組織となっており、米国国防総省の経済的支援を受けている CERT/CC とは異なる運用形態となっている。

（b）中国

中国国内に CSIRT は数多く存在する。ただし、FIRST には CNCERT/CC が中国全体を代表して参加し、CNCERT/CC のヒエラルキーのもとで、CSIRT 相互の情報交換が密になされている。

（c）韓国

韓国の場合は、CERTCC-KR が国際的な窓口になり、CONCERT という韓国内

[8] http://www.redflag-linux.com/eindex.html

の CSIRT の集まり（フォーラム）が束ねる形となっている。この CONCERT には JPCERT/CC もスピーカーとして招かれ、発表も行っている。

４．４．５ 解決すべき課題と今後の展望

セキュリティホールに代表される脆弱性情報に対する関係者間の役割と責任分担のあり方に関して、現状における解決すべき課題を整理するとともに、今後取り組むべき方向について展望する。

(1) 脆弱性情報の発信主体と責任のあり方について

これまでの調査結果をもとに、課題として次の事項が挙げられる。

（ａ）セキュリティサービス事業者における課題

米国 OIS や ISS の例に見られるように、脆弱性情報の公開に関するガイドラインの策定の動きは見られるものの、広範な合意を得るには至っていない。これは、後述するようにソフトウェアベンダー毎に脆弱性に対する姿勢に大きな開きがあり、適切な対応期間にも差が生じざるをえないこと、現在提案されているガイドラインは、セキュリティサービス事業者に都合のよいものとなっていることなどが原因となっているものと考えられる。脆弱性情報の公開・非公開の判断は原則として民間セクターの問題であり、製品やサービスが複数国にまたがることも多いため、行政による規制や制度化はなじまない分野といえるものの、脆弱性情報の公開ガイドラインを議論する場に多くの立場からの参加者の意見が反映されるような支援を行うことが望ましい。脆弱性情報の公開ガイドラインの策定に際しては、その内容が OECD 情報セキュリティガイドラインにおける責任、対応、倫理、民主主義の各原則を満足するものであることが望まれる。

（ｂ）ソフトウェアベンダーにおける課題

４．４．２．２にて示した Microsoft 社における事例に見られるように、最近 2 年程度の間で一部ソフトウェアベンダーの脆弱性への対応の姿勢は急速に向上しつつある。ただし、対応に改善がみられないベンダーに関しては変化がなく、結果的にベンダー間での対応の差が拡大する傾向がみられる。これは、オープンソースコミュニティにおいても同様であり、同じ Linux のディストリビューションでも、脆弱性情報の公開があってから対応が完了するまでの時間にはかなりの開きがある。現状ではこうした対応までの時間の差よりも、ユーザにおいてパッチ等の対策を実施しているかどうかのほうが脅威への影響としては重大であるため、こうした差が目立つ状況にはなっていないが、将来的にパッチの適用が一般化、ないし可能な限り自動化されるようになった場合には問題として顕在化する恐れがある。OECD 情報セキュリティガイドラインにおける責任および対応の原則の指示する内容のもとで、それぞれの役割に応じた責任の分担が可能となるような、脆弱性への対応ルールについても今後求められていくものと考えられる。

（2）脆弱性情報の流通のあり方について

情報の流通の仕組みについては、４．４．３．４にて記述した大学でのボランタリな取り組みに解決の萌芽が見受けられる。今後は、こうした動きをどのように支援していくかが問題になろう。2 種類の取り組みがいずれも大学でのボランタリな対応という形式で始まった背景としては、こうした活動には利害関係を超越するような中立的な姿勢が欠かせないことを示唆していると考えることもできる。脆弱性情報の流通の仕組みとして、発信、制御、共有、伝達などの個々のプロセスに対応した望ましい組織と運用体制のあり方について、今後検討を進める必要がある。それぞれのプロセスについて、OECD 情報セキュリティガイドラインにおける認識、責任、対応、倫理、民主主義、リスクアセスメントなどの各原則を考慮し対応を図ることが望ましい。

（3）組織間の連携のあり方について

セキュリティホールへの対応に限らず、情報セキュリティを確保するために多様な参加主体の関与が欠かせないことに関しては、今後も変わらずに続くと考えられる。ただし、ベンダー、ユーザ、行政機関など性質の異なる多様な組織の間で連携関係を構築、維持することの困難さは改めて言及するまでもないだろう。

こうした状況の中で、各組織において CSIRT に相当する組織ないし役目を設定することは、親に相当する組織の性質が大きく異なっても、同じ目的で設立されている子に相当する組織間では比較的容易に連携が可能というメリットが生ずることが想定され、有益な成果を生み出し得るものと推察される。この場合、OECD 情報セキュリティガイドラインにおける責任、対応、倫理の各原則の示す方向性のもとで、効果的な連携が実現されるよう、各方面からの支援を検討することが求められる。

５．「セキュリティ文化」の普及に向けた提言

新しい OECD 情報セキュリティガイドラインでは、加盟国に対して「セキュリティ文化（Culture of Security）」を自国の中で普及させるために、必要なアクションをとることを求めている。

本章では、本調査のまとめとして「セキュリティ文化」の普及に向けて、我が国の情報セキュリティ政策の方向性について、以下の 3 つの観点から提言を行う。

1. 個人ユーザに向けた情報セキュリティ意識の啓発
2. 脅威および脆弱性に関する情報の流通と責任のあり方
3. 情報セキュリティ関連人材の育成と環境整備

５．１ 個人ユーザに向けた情報セキュリティ意識の啓発

新しい OECD 情報セキュリティガイドラインでは、第 1 番目の原則として「認識（Awareness）」をかかげている。「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。（Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.）」として、情報システムやネットワークを利用する者が、そのリスクと利用可能な対応策について認識することが、情報セキュリティ対策の第一歩であることを主張している。

特に、近年インターネットは家庭や職場の中にも浸透し、子供から高齢者までより多くの人がネットワークで結ばれるようになっており、この層の意識啓発は「セキュリティ文化」の普及において最重要の課題となっているといえる。新ガイドラインにおいても、情報セキュリティにかかわる「参加者（participants）」として、産業界、政府機関、学術機関等に加え、個人ユーザも対象として明確に位置付けている。

我が国においては、ブロードバンドの急速な普及によって、情報システムやネットワークの技術にあまり精通していない初心者レベルの人達へも利用者層が拡大している。コンピュータやインターネットを使いはじめる最初の段階で、情報セキュリティの必要性とそのために何ができるのかを啓発することが求められる。

具体的には、情報セキュリティ対策に関する個人ユーザ向けのガイドラインやパンフレットなどの作成、配布などのほか、初等中等教育や生涯教育の現場での情報セキュリティに関する授業の実施、個人の情報セキュリティ対策を支援する非営利団体や地域ボランティアの活動の支援などが考えられる。

一般への啓発の意味も込めて、本調査の活動の一環として OECD 情報セキュリティガイドラインの普及啓発用パンフレットを作成した（３．１を参照）。個人ユーザに対しては、より具体的な対応策がわかりやすく整理されたガイドライン等が提供されることが望ましい。IPA では一般家庭や SOHO（Small Office Home Office）のユーザが行うべき情報セキュリティ対策をまとめた「SOHO・家庭向けの情報セキュリティ対策マニュアル」を公開しているが、このような情報がより広く普及することが求められる。

また近年、家庭や学校においてインターネットが急速に普及してきたことにともない、子供や未成年者がネットワークにアクセスする機会が格段に増えている。早い時期からインターネットを利用するうえでのリスクや自身の責任について認識させるとともに、他人への配慮などを含む倫理面での教育が必要となる。初等中等教育においては、学習指導要領が見直され、小中学校では平成 14 年度から開始された「総合的学習の時間」においてコンピュータや情報通信ネットワークを活用されることになっており、高等学校では平成 15 年度より教科「情報」が開始される予定である。これらの授業や教科のなかで情報セキュリティについて必要な教育がされることが望ましい。教育の現場では、情報セキュリティについて教えられる教師の数が少ないことが指摘されているが、場合によっては情報関連の大学院生や民間企業のエンジニア、地域のコミュニティなどの人材を柔軟に活用することも考えられる。

一方、政府は平成 13 年度末までに、全国で約 550 万人程度の国民に対して、IT の基礎技能（パソコンの基本操作、文書の作成、インターネットの利用及び電子メールの送受信）を身に付けるための「IT 基礎技能講習事業」を実施している。多くの自治体が、この事業の成果をもとにそれぞれの地域で講習事業を継続しているほか、国においても、IT 基礎技能講習事業のフォローアップとして、講習を受けた地域住民が自宅等で IT を利用する際のサポートをするために、「地域 IT リーダー」の育成、派遣および地域センターのヘルプデスク機能を整備する「IT 基礎技能習得等住民サポート事業」を平成 14 年度より実施している。これらの事業は、主に地域住民の情報リテラシの向上を目的としているが、情報セキュリティにおいても、講習等で基礎的な知識をレクチャーしたうえで、日々の情報セキュリティ対策や事件・事故等の発生時に連絡・相談を受け付ける窓口機能が整備されることが望まれる。その際、人員や資源を有効に活用するために、国や自治体は地域のコミュニティや NPO 等の活力を支援するべきである。

５．２ 脅威および脆弱性に関する情報の流通と責任のあり方

「４．１ セキュリティ方策に関するベストプラクティスの共有に向けた検討」および「４．４ セキュリティホールに対する関係者間の役割と責任分担のあり方の検討」にみたように、脅威や脆弱性の情報を流通に関しては、国や地域によって異なるモデルが運用されている。米国では、重要インフラを中心とする産業セクターごとに官民の情報共有体制である情報共有分析センター（ISAC：Information Sharing and Analysis Center）設置されており、また、韓国や中国などのアジア地域では、国またはその外郭団体が中核となる CSIRT を運営する形態がみられる。特に、米国政府の情報セキュリティ政策の戦略を定める「The National Strategy to Secure Cyberspace」では、ISAC の重要性を認識し、各セクターで設立すること、および、各 ISAC と政府機関との連携について言及している。同時に、ISAC の設立、運用は、資金面、人材面等で課題を抱えており、ISAC 間の連携も必要であることについても触れている。

我が国の脅威および脆弱性に関する情報の流通の体制として、どのようなモデルが日本の環境に馴染むのか検討する必要がある。特に、以下のような観点について、国内関係者間で議論を深める必要があるだろう。

- 製品に脆弱性が発見された場合、ベンダーの情報開示のルールはどうあるべきか
- その情報を共有すべき関係者は誰か
- 脆弱性情報を一般に公開するタイミングはどうあるべきか
- FIRST (Forum of Incident Response and Security Teams：世界中の CSIRT 同士の情報交換、インシデント対応の協力関係の構築などを目的とした国際フォーラム)の枠組みにおいて、我が国の CSIRT（JPCERT/CC 等）の果たすべき役割は何か

国はこの分野においてリーダーシップを発揮し、基本的な方向性を示すとともに、自らの CSIRT 機能（内閣官房 緊急対応支援チーム（NIRT： National Incident Response Team）等）のベストプラクティスモデルを示すことが求められる。

脅威や脆弱性の情報を流通体制の整備とあいまって、情報システムやサービスの提供者側、利用者側双方を含む各参加者が、脅威および脆弱性に対して、どのような範囲において、どのような責任を持ち、どのような役割を果たすべきか議論する必要がある。この場合、IT セキュリティ評価制度や情報セキュリティ監査制度等の既存あるいは現在策定の進む諸制度との整合を考慮する必要がある。

５．３ 情報セキュリティ関連人材の育成と環境整備

総務省が 2002 年 9 月に公表した「情報セキュリティ対策の状況調査～世界的に情報セキュリティ対策の関心が高まる中で～」調査報告書によると、情報システムを使用している企業においては、情報セキュリティ管理ために専任部署や専任担当者を置くなどの体制を整備している企業は少数にとどまっている（図 5-1 参照)。一般企業や行政機関など、情報システムやネットワークを導入し、使用する側である、いわゆる「ユーザ企業（ユーザ組織)」においては、エンドユーザに向けた情報セキュリティ意識の啓発に加えて、社内で情報セキュリティの担当者の確保と育成が課題である。一方、ユーザ企業が使用する情報システムやネットワークを提供する側の「ベンダー企業」においても、セキュアな製品やサービスを提供するため、情報セキュリティに関する高度な技術や知識をもった開発者やシステムエンジニア等を育成することが急務である。

情報セキュリティにたずさわる人材に求められる知識やスキル、実務能力は、上記のユーザ企業、ベンダー企業によって異なるほか、同じベンダー企業においても、例えばウイルスソフトやファイアウォール製品を開発する技術者と、それらのパッケージ製品を組み合わせ顧客のセキュリティシステムを構築するインテグレータとで、要求される知識の内容やレベルが違っている。情報セキュリティの教育においては、これらの多様性を踏まえつつ、教育する側および教育を受ける側が一定のゴールを共通に認識できるモデルキャリアを複数設定し、それに対応した教育カリキュラムやコース等が整備されることが必要である。また、情報セキュリティに関する資格試験制度においても、このようなモデルキャリアに即した形で整備されることが望ましい。

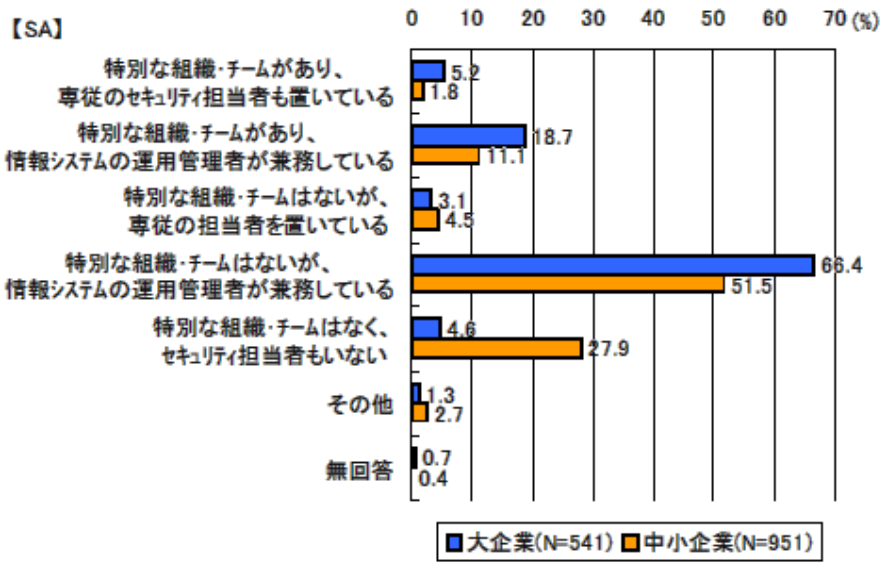

図 5-1　セキュリティ管理のための社内組織・チームの設置
（出典：総務省「情報セキュリティ対策の状況調査～世界的に情報セキュリティ対策の関心が高まる中で～」調査報告書）

「４．１．２ 情報セキュリティ教育と資格試験制度のあり方」でみたように、米国では民間の団体や企業が情報セキュリティ関連の資格試験を運用しており、資格取得が就職や昇進、昇給に大きな影響を及ぼすなど、その権威が一般に認められている。各団体は、資格試験と教育プログラムをリンクさせたビジネスモデルを確立しており、一般企業から連邦職員まで資格取得者の裾野を広げている。その一方で、情報セキュリティ関連の資格試験を運用する団体が増え、資格間で対象者の重複がみられるようになり、受験者側の負担が増すとの懸念もある。

我が国においても、情報セキュリティ関連の資格制度の充実は情報セキュリティレベルの向上において、非常に有効なスキームである。今後、国家試験と民間試験の役割分担を含め資格試験制度の枠組みについて議論する必要があるだろう。

また、情報セキュリティは特に変化のスピードが速い分野であり、常に最新の知識レベルを保つため、継続的な教育や資格の更新制度が不可欠である。しかし、継続的に教育を実施することは企業や組織にとって大きな負担となるうえ、強力なインセンティブが必要である。そのため、資格試験においても継続教育の仕組みが組み込まれていることが望まれるが、現在の情報処理技術者試験では継続教育や資格更新の義務は課せられていない。継続教育も含め情報セキュリティの専門教育のあり方について、民間と大学・専門学校等の教育機関との役割分担はどうあるべきか、また、国や自治体はそのような取り組みをどのようにして支援していけばよいか、検討する必要がある。

また、国や自治体は、電子政府や電子自治体の取り組みが進んでおり、2002 年 8 月からは住民基本台帳ネットワークの運用がスタートしている。今後、国や自治体での情報シス

テムやネットワークの利用の拡大に伴い、情報セキュリティにたずさわる人材を確保していくことが不可欠となる。国や自治体の一般職員に対する情報セキュリティ教育のあり方および情報セキュリティ担当者の育成について、継続教育と資格制度の導入も含め方向性を検討する必要があるだろう。

（了）

６．付録

６．１ 2002 年版 OECD 情報セキュリティガイドライン仮訳

OECD Guidelines for the Security of Information Systems and Networks
TOWARDS A CULTURE OF SECURITY
OECD 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
(仮訳)

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT	**経済協力開発機構**
Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:	1960 年 12 月 14 日パリで署名され、1961 年 9 月 30 日に発行した条約の条項 1 に従って、経済協力開発機構 (OECD) は次に掲げることのために立案された方針を促進する。
To achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy.	継続可能な最も高度な経済成長を達成し、加盟国における生活水準を向上させるとともに、金融の安定とそれによる世界経済の発展に貢献すること。
To contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and	経済発展のプロセスにおいて、非加盟国のみならず加盟国の健全な経済の拡大に貢献すること。
To contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.	国際的な責務に合致した、多国的主義、非差別主義に基づき、世界貿易の拡大に貢献すること。
The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).	OECD の設立当初の原加盟国は、オーストリア、ベルギー、カナダ、デンマーク、フランス、ドイツ、ギリシャ、アイスランド、アイルランド、イタリア、ルクセンブルグ、オランダ、ノルウェイ、ポルトガル、スペイン、スウェーデン、スイス、トルコ、英国、米国である。その後、次に掲げるの国が、後に示す日付による承認を経て、加盟国になった。日本 (1964 年 4 月 28 日)、フィンランド (1969 年 1 月 28 日)、オーストラリア (1971 年 6 月 7 日)、ニュージーランド (1973 年 5 月 29 日)、メキシコ (1994 年 5 月 18 日)、チェコ (1995 年 12 月 21 日)、ハンガリー (1996 年 5 月 7 日)、ポーランド (1996 年 11 月 22 日)、韓国 (1996 年 12 月 12 日)、スロバキア (2000 年 12 月 14 日)。欧州共同体の委員会は、OECD の活動に参加する (OECD 条約条項 13)。
FOREWORD	**はしがき**
The present OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture	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－

of Security were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.	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。
PREFACE The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the Guidelines for the Security of Information Systems. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks ("participants").	**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と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。
Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.	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。
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. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".	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. TOWARDS A CULTURE OF SECURITY These Guidelines respond to an ever changing security environment by promoting the development of 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. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are	**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

becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.	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。
Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.	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。
Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.	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. AIMS These Guidelines aim to:	**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。
Promote a culture of security among all participants as a means of protecting information systems and networks.	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。
Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.	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。
Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.	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。
Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.	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。
Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.	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。
Promote the consideration of security as an important objective among all participants involved in the devel-	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

opment or implementation of standards.	進すること。
III. PRINCIPLES The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy[1].	**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]。
1 In addition to these Security Guidelines, the OECD has developed complementary recommendations concerning guidelines on other issues important to the world's information society. They relate to privacy (the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) and cryptography (the 1997 OECD Guidelines for Cryptography Policy). These Security Guidelines should be read in conjunction with them.	1 このセキュリティガイドラインに加えて、OECD は、世界の情報社会にとって重要な他の課題についてのガイドラインに関する互いに補い合う勧告を策定してきた。それらはプライバシーに関するもの（1980 年 OECD プライバシー保護と個人データの国際流通についてのガイドライン）及び暗号に関するもの（1997 年 OECD 暗号政策ガイドライン）である。このセキュリティガイドラインは、これらと併せて読まれるべきである。
1) Awareness *Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.* Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.	*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付け、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) Responsibility *All participants are responsible for the security of information systems and networks.* Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks.	*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、

They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.	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) Response *Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.* Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.	*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があることを認識し、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) Ethics *Participants should respect the legitimate interests of others.* Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.	*4) 倫理 (Ethics)* ***参加者は、他者の正当な利益を尊重するべきである。*** 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) Democracy *The security of information systems and networks should be compatible with essential values of a democratic society.* Security should be implemented in a manner consistent with the values recognised 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.	*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、公開性並びに透明性を含む、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) Risk assessment	*6) リスクアセスメント (Risk assessment)*

Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be 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. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.	***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な、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) Security design and implementation *Participants should incorporate security as an essential element of information systems and networks.* Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.	*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) Security management *Participants should adopt a comprehensive approach to security management.* Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of	*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つつ、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、レビュー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、

security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.	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) Reassessment *Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.* New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.	*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。
RECOMMENDATION OF COUNCIL OF THE OECD THE COUNCIL,	**OECD 理事会の勧告** 理事会は、
Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof;	1960 年 12 月 14 日の OECD 条約、特に、条項 1 b)、1 c)、3 a)、及び 5 b)を考慮し、
Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(FINAL)];	1980 年 9 月 23 日のプライバシー保護と個人データの国際流通に関するガイドラインに関する理事会勧告 [C(80)58/FINAL] を考慮し、
Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];	1985 年 4 月 11 日の OECD 加盟国政府によって採択されたデータの国際流通に関する宣言 [Annex to C(85)139] を考慮し、
Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];	1997 年 3 月 27 日の暗号政策ガイドラインに関する理事会勧告[C(97)62/FINAL] を考慮し、
Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];	1998 年 12 月 7-9 日のグローバルなネットワークにおけるプライバシーの保護に関する閣僚宣言[Annex to C(98)177/FINAL] を考慮し、
Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];	1998 年 12 月 7-9 日の電子商取引のための認証に関する閣僚宣言 [Annex to C(98)177/FINAL] を考慮し、
Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;	情報システム及びネットワークは、政府、企業、その他の組織及び個人利用者にとってその利用と価値がますます増大していることを認識し、
Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;	情報システム及びネットワークの役割が重要性を増し、また、安定的で効率的な国内経済及び国際貿易のために情報システム及びネットワークへ依存すること、また社会的、文化的及び政治的生活において情報システム及びネットワークへ依存することが一層増大していることが、情報システム及びネットワークにおける信頼を保護し促進する特別な努力を要求していることを認識し、
Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;	情報システム及びネットワーク、並びにそれらの世界的な急増が、新しく、かつ増加し続けるリスクを伴ってきていることを認識し、
Recognising that data and information stored on and transmitted over information systems and networks are	情報システム及びネットワークを経由して保存され、伝送されるデータや情報は、様々な手段による権限のな

subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;	いアクセス、利用、横領、変更、悪意のあるコード伝送、サービスの妨害、又は破壊の脅威にさらされており、適切な安全防護措置が求められていることを認識し、
Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;	情報システム及びネットワークのリスク並びにそのリスクに対応するために利用可能な方針、実践、手段及び手続についての認識を高める必要があること、並びにセキュリティ文化の発展に向けた決定的な措置としての適切な行動を奨励する必要があることを認識し、
Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;	現在の方針、実践、手段及び手続を、それらが情報システム及びネットワークに対する脅威によってもたらされる難題の展開に確実に対応するように、見直す必要があることを認識し、
Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;	セキュリティ文化は、セキュリティ面での障害から生じる潜在的な損害によってもたらされる、国内経済及び国際貿易、並びに社会的、文化的及び政治的な生活への参画に対する難題に対応するための国際的な調整及び協力を促進するものであり、このセキュリティ文化によって情報システム及びネットワークのセキュリティを促進することに共通の利益が存在することを認識し、
And further recognising that the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;	また、更に、この勧告の付属文書に規定される「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」は強制的なものではなく、国家の主権に影響を及ぼさないことを認識し、
And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;	このガイドラインは、セキュリティのためにある一つの解決策が存在すること、又はある特別な状況に適した方針、実践、手段及び手続が何であるかを提案することを意図するものではなく、参加者が、どのようしてセキュリティ文化の発展から利益を得、また、その発展にどのように貢献するかについてより良い理解を促すために、原則の枠組みを提供するものであることを認識し、
COMMENDS these Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;	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に、この「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」を推奨する。
RECOMMENDS that Member countries: Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security by adopting and promoting a culture of security as set out in the Guidelines;	OECD 加盟国に次に掲げることを勧告する。 「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」に規定されたセキュリティ文化を取り入れ、普及させることによって、このガイドラインを反映し、かつ考慮した政策、実践、手段及び手続を新たに確立し、又は、既存のものを改正すること。
Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;	このガイドラインを実施するために国内及び国際レベルで協議し、調整し、かつ協力すること。
Disseminate the Guidelines throughout the public and private sectors, including to governments, business,	セキュリティ文化を普及させ、またすべての関係者が責任を負い、個々の役割に応じた適切な方法で、このガ

other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;	イドラインを実施するための必要な措置を講じることを奨励するために、政府、企業、その他の組織及び個人利用者を含む公共及び民間セクターを通じて、このガイドラインを普及させること。
Make the Guidelines available to non-member countries in a timely and appropriate manner;	時宜を得た、適切な方法でこのガイドラインを非加盟国において利用可能にすること。
Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;	情報システム及びネットワークのセキュリティに関する課題についての国際的な協力を促進するため、5 年毎にこのガイドラインを見直すこと。
INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.	OECD 情報･コンピュータ･通信政策委員会にこのガイドラインの実施を促進するよう指示する。
This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].	この勧告は、1992 年 11 月 26 日の情報システムのセキュリティのためのガイドラインに関する理事会勧告(C(92)188/FINAL)に代替する。
PROCEDURAL HISTORY The Security Guidelines were first completed in 1992 and were reviewed in 1997. This current review was undertaken in 2001, by the Working Party on Information Security and Privacy (WPISP) pursuant to a mandate from the Committee for Information, Computer and Communication Policy (ICCP) and accelerated in the aftermath of the September 11 tragedies.	**手続の歴史** セキュリティガイドラインは、1992 年に初めて策定され、1997 年に見直された。今回の見直しは、情報･コンピュータ･通信政策委員会(ICCP)から与えられた権限に従って情報セキュリティ･プライバシー作業部会(WPISP)によって、2001 年に着手され、9 月 11 日の悲劇の余波を受けて作業が早められた。
Drafting was undertaken by an Expert Group of the WPISP which met in Washington DC on 10 and 11 December 2001, Sydney on 12 and 13 February, 2002 and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5-6 March 2002, 22 and 23 April, 2002 and 25 and 26 June, 2002.	草案は 2001 年 12 月 10 日及び 11 日のワシントン DC、2002 年 2 月 12 日及び 13 日のシドニー、並びに 2002 年 3 月 4 日及び 6 日のパリで会合が開催された WPISP の専門家グループによって起草された。WPISP は 2002 年 3 月 5 日及び 6 日、2002 年 4 月 22 日及び 23 日、並びに 2002 年 6 月 25 日及び 26 日にパリで開催された。
The present OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.	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用された。

６．２ OECD 情報セキュリティガイドライン普及啓発用パンフレット

※ 別添資料を参照

６．３ 略語一覧

ADR	Alternative Dispute Resolution
ADSL	Asymmetrical Digital Subscriber Line
ASP	Application Service Provider
BIAC	Business and Industry Advisory Committee to the OECD
CBK	Common Body of Knowledge
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CISSP	Certified Information System Security Professional
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DSL	Digital Subscriber Line
EIA	Electronic Industries Alliance
FIRST	the Forum of Incident Response and Security Teams
GSA	General Services Administration
ICCP	(Committee for) Information, Computer and Communications Policy
IETF	Internet Engineering Task Force
IRT	Incident Response Team
ISA	Internet Security Alliance
ISAC	Information Sharing and Analysis Center
ISMS	Information Security Management System
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center
LAN	Local Area Network
NIPC	National Infrastructure Protection Center
NIST	National Istitute of Standard and Technology
NIRT	National Incident Response Team
NPO	Non-profit Organization
OECD	Organization for Economic Cooperation and Development
OIS	Organization for Internet Safety
PKI	Public Key Infrastructure
SOHO	Small Office / Home Office
SSCP	Systems Security Certified Prac-titioner
V-STAF	Vulnerabilities database conStructing TAsk Force
WPISP	Working Party on Information Security and Privacy
(ISC)2	International Information System Security Certifications Consortium, Inc.