

平成13年度
OECD 情報セキュリティガイドライン
に関する調査



情報処理振興事業協会

セキュリティセンター

- 目次 -

1 . OECD 情報セキュリティガイドラインに関わる基礎資料の調査	3
1 . 1 OECD 情報セキュリティガイドライン	3
1 . 1 . 1 制定の経緯と見直しについて.....	3
1 . 1 . 2 ガイドラインの構成.....	3
1 . 1 . 3 ガイドライン本文各章の概要.....	3
1 . 1 . 4 ガイドライン付録（説明のための覚書）	5
1 . 2 その他国際機関等の活動について	6
1 . 2 . 1 欧州委員会（European Committee）	6
1 . 2 . 2 BIAC（Business and Industry Advisory Committee to the OECD）	6
2 . OECD セキュリティガイドラインワークショップ関連事項の調査	7
2 . 1 ワークショップについて	7
2 . 2 ワークショップでの主張および提言内容の検討.....	7
2 . 3 ワークショップクロージングステートメントについて.....	9
3 . 主要なセキュリティ関連ガイドライン	11
3 . 1 ISO/IEC TR 13335（GMITS）	11
3 . 2 ISO/IEC 17799（JIS X-5080, BS7799 Part I）	14
3 . 3 金融業務における情報セキュリティガイドライン ISO/TR 13569	16
3 . 4 情報処理サービス業情報システム安全対策実施事業所認定制度の改革と ISMS 適合性 評価制度.....	17
4 . 国内外における情報通信システムに対する脅威の動向	22
4 . 1 情報システムのセキュリティを取り巻く環境の変化.....	22
4 . 2 セキュリティ基盤に関する動向.....	26
4 . 2 . 1 不正アクセス.....	26
4 . 2 . 2 ウィルス.....	30
4 . 3 情報システムのセキュリティに対する脅威の変化	32
4 . 3 . 1 技術の発展と脅威	32
4 . 3 . 2 社会、生活、経済と脅威.....	41
4 . 4 情報セキュリティ対策コストとセキュリティ関連製品 / サービスの市場規模	44
4 . 4 . 1 企業や組織におけるインシデントの発生と被害	44
4 . 4 . 2 組織におけるセキュリティ対策とそのコスト.....	46
4 . 4 . 3 情報セキュリティビジネスマーケット動向	48
4 . 5 情報セキュリティにおける課題.....	48
5 . 国内におけるニーズ調査.....	50
6 . OECD 情報セキュリティガイドラインの見直しの検討	52
6 . 1 研究会委員	52
6 . 2 研究会における審議の経緯.....	53
6 . 3 研究会における審議の概要.....	53

6 . 4 見直しにおける論点.....	55
7 . ガイドラインの見直しに関する提案.....	57
8 . 付録.....	60
8 . 1 付録1 1992年OECDセキュリティガイドライン(本文/和訳対訳)	60
8 . 2 付録2 英字略語表.....	86

1 . OECD 情報セキュリティガイドラインに関わる基礎資料の調査

1 . 1 OECD 情報セキュリティガイドライン

1 . 1 . 1 制定の経緯と見直しについて

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初めて登場したものである。

ガイドラインの制定作業の場として 1991 年 1 月に専門家会議が組織され、合計 6 回の専門家会議が開催された。ガイドラインは 1992 年 11 月 26 日の理事会において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。見直しの結果は、変更の必要なし、とのことであった。2002 年の第 2 回の見直しに向けて、検討作業が現在行われている。

1 . 1 . 2 ガイドラインの構成

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」、及び付録としての「説明のための覚書 (Explanatory Memorandum)」の 3 部構成となっている。

勧告本文では、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和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。

勧告の内容は、(1)付属文書に記述された情報システムに関する原則を反映した対策、実践、手続きの確立、(2)ガイドラインの実施における国際的な協議、協調、協力、(3)ガイドライン適用に関わる協議への合意、(4)原則の普及、(5)OECD ガイドラインの 5 年毎の見直し、の 5 項目である。

1 . 1 . 3 ガイドライン本文各章の概要

ガイドライン本文は、「I . 目的 (AIMS)」、「II . 適用範囲 (SCOPE)」、「III . 定義 (DEFINITIONS)」、「IV . セキュリティの目的 (SECURITY OBJECTIVE)」、「V . 原則 (PRINCIPLES)」、「VI . 実施 (IMPLEMENTATION)」の 6 章で構成されている。

「I . 目的」では、ガイドラインの目的を、「情報セキュリティにおけるリスク対応の必要性の認識を高めること」、「対策に関する一般的な枠組みを提供すること」、「対策にお

ける公共部門と民間部門の協力を推進すること」「情報システムの信頼性を高めること」「情報システムの国際的な利用を促進すること」「情報セキュリティを達成するために国際的協力を推進すること」としている。

「II．適用範囲」では、ガイドラインの適用対象を「公共部門及び民間部門」の「全ての情報システム」としている。

「III．定義」では、「IV．セキュリティの目的」の表現に必要な概念を定義している。特に、可用性（Availability）、機密性（Confidentiality）、完全性（Integrity）の3つの概念を定義していることが注目される。

「IV．セキュリティの目的」では、それまで一般的には漠然と語られていたセキュリティの目的に対し、「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、明確な定義を立て、いわゆる CIA の意識（Confidentiality、Integrity、Availability）を広く世に知らしめたことが重要である。

「V．原則」では、以下の9つの原則を示し、以後の情報セキュリティに関する諸規格に影響を与えている。9つの原則とは次の通り

(i) 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。

(ii) 情報提供の原則（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。

(iii) 倫理性の原則（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。

(iv) 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。

(v) 比例性の原則 (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、広がりには比例したものであるべきである。

(vi) 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。

(vii) 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。

(viii) 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。

(ix) 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。

「VI. 実施」では、ガイドラインに示される目的の達成、原則の実施にあたって、「適切な法律、行政、自主規範その他の対策及び実践、手続き、規則の確立及び確立の推進、支援が求められる」とし、「政策」、「教育及び訓練」、「法の執行及び補償」、「情報の交換」、「協力」の各項目に区分して活動指針を提示している。

1. 1. 4 ガイドライン付録 (説明のための覚書)

ガイドラインの全6章は、ガイドラインとしての性質上、冗長性を排し、広範囲な適応性をもたせるための抽象的な記述を採用している。その理解を助けるために、ガイドライン付録として「説明のための覚書 (Explanatory Memorandum)」が付けられている。説明のための覚書では、ガイドライン制定に至る歴史的な経緯から始まり、情報セキュリティ確保の重要性を示す背景情報、セキュリティの目的の定義に関する詳細な議論、及び、9個の原則、5個の実施指針に関して、具体例を交えた解説が展開されている。

1.2 その他国際機関等の活動について

1.2.1 欧州委員会 (European Committee)

欧州委員会は 2001 年 7 月に情報セキュリティに関する政策の方向性を示すものとして「Network and Information Security: Proposal for a European Policy Approach (ネットワークと情報のセキュリティ：欧州政策アプローチのための提案)」というタイトルの文書を公表している。同文書の要旨は以下のとおり。

- (1) ネットワークの進展に際して、セキュリティは経済・社会発展のための重要な要素となりつつある。
- (2) 複雑なネットワーク化の進展は、十分なセキュリティ対策の実施を難しくしている。
- (3) セキュリティに関する法律の規定は、環境の変化にあわせて適切に適用していく必要がある。また、セキュリティの欠陥について個別の対策を行うことは、市場を強化し、法的枠組みの機能を改良するものである。
- (4) ネットワーク及び情報セキュリティは、サイバー犯罪、データ保護及び通信フレームワークと相互に関係している。
- (5) セキュリティにおける脅威には、以下のようなものがある。
 - ・ 電気通信が傍受され、データのコピー及び改ざんがなされる。
 - ・ 不正アクセスにより悪意のあるデータのコピー、改ざん及び破壊がなされる。
 - ・ インターネットの破壊行為は一般的になり、将来電話回線も脆弱になる。
 - ・ ウィルス等の悪意のあるソフトウェアにより、システムの破壊、データの改ざんが行われる。
 - ・ なりすましは消費者等にとって甚大なダメージを起こす。
 - ・ 多くのセキュリティインシデントは、予期できない、意図しないものが原因となる。
- (6) 提案する施策は次の通り。
 - ・ 意識の啓発
 - ・ 欧州での警告 / 情報提供システム (CERT (Computer Emergency Response Team) との連携)
 - ・ 技術開発
 - ・ マーケットベースの基準認証のサポート (IPv6、IPSec、認証の相互承認)
 - ・ 法的枠組み (適切な法の整備、暗号製品の自由な流通等)
 - ・ 政府利用 (電子署名、セキュリティ要件の強化)
 - ・ 国際連携 (国際的な組織及びパートナーとの意見交換の強化)

1.2.2 BIAC (Business and Industry Advisory Committee to the OECD)

- ・ OECD における産業界側の公式の諮問機関である BIAC (Business and Industry Advisory Committee to the OECD) は、OECD セキュリティガイドラインの見直しに関する取り組みに積極的に協力している。

2 . OECD セキュリティガイドラインワークショップ関連事項の調査

2 . 1 ワークショップについて

2001 年 9 月 12 日及び 13 日に、東京において、OECD、日本国政府、及び情報処理振興事業協会（IPA）の共催の下、「情報セキュリティに関するワークショップ（Information Security in a Networked World）」が開催された。OECD 加盟国を含む 24 カ国・地域（うち OECD 加盟国は 16 カ国。他はマレーシア、ロシア、中国等）から、政府、産業界、アカデミア、消費者団体等の情報セキュリティに携わる専門家約 250 名が参加し、パネルディスカッションを中心に活発な議論を行った。

本ワークショップは、GBDe（Global Business Dialogue on Electronic Commerce）の第三回東京会合と踵を接して開催され、政府と産業界の相互理解を促進した。

古屋経済産業省副大臣（日本政府代表）、ピーター・フォード OECD WPISP（Working Party on Information Security and Privacy）議長、及びマイケル・オボーン OECD 事務局科学技術産業局次長がそれぞれ冒頭挨拶を行った。キーノートスピーチとパネルディスカッションで構成される 5 つのセッションに分かれて、新たな脅威、電子商取引における安全性及び信頼性、技術動向、教育・倫理、マネジメント・人的要因、技術標準、法的問題、各主体の役割、セキュリティガイドラインのあり方等に関して発表及び活発な議論が行われた。これらを通じて、新たな脅威の性質、それへの対応、またとられるべき政府の政策やアプローチ方法等に関して、参加者間で共通の認識を形成する点において、価値ある進展が見られた。また、今回の結果は、来年度予定されている OECD セキュリティガイドラインの見直しに貢献することが期待されており、今回のワークショップを契機として、ガイドライン見直しに関する議論の活発化が想定される。

2 . 2 ワークショップでの主張および提言内容の検討

「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」（詳細は第 6 章参照）のメンバが、上記ワークショップのパネルセッションに参加し講演を行った。これに関連し、9 月 6 日に開催された同研究会第 2 回では、各メンバのワークショップでの主張および提言内容について検討を行っており、表 2-1 にその要旨を示す。

表 2-1 ワークショップでの主張および提言内容の検討

セッションタイトル （【】内は研究会委員名）	要旨
Plenary Session 2 : Information System: New Threats, New Responses (9/12) 【山口委員】	<ul style="list-style-type: none">・ ブロードバンドの普及を背景に、家庭を如何に守るかという観点急速にクローズアップされている。・ セキュリティを守るためには、テクノロジーによる手段が重要。法や規制はテクノロジーの発展に細かい注文をつけるべきではない。そうでない場合は、法や規制を柔軟に変えられるスキームを持つ必要がある。・ 政府の役割は、プラクティカルでリーズナブルな規制の策定や司法機関への教育の提供であり、産業界や学术界との対話を進めることが重要。

セッションタイトル (【】内は研究会委員名)	要旨
Tracking Session Track A : Role of Technical Standards (9/13) 【苗村委員】	<ul style="list-style-type: none"> ・ セキュリティに関するテクニカルスタンダードには、2つのユニークな問題がある。標準化が進むと、攻撃する者も含め全ての人に情報が公開になるため脆弱性が増加する。また、標準化された技術が破られると、すべてのシステムが攻撃の対象になってしまう ・ SC27 で策定された GMITS (TR13335)を紹介。GMITS ではセキュリティの目的として、CIA (Confidentiality, Integrity, Availability)の他に Reliability、Authenticity、Accountability が追加されている。 ・ 将来の課題として、国の制約条件といったものをどうやって取り入れていくのかということも問題になる。
Tracking Session Track A : Management & human factors (9/13) 【中尾委員】	<ul style="list-style-type: none"> ・ 今日のビジネス環境における危険の露呈を背景に、情報セキュリティマネジメントが必要になる。 ・ 国際標準化の観点から、ISO/IEC SC27 の構成や、ISO/IEC 17799、ISO/IEC TR 13335(GMITS)の概念について紹介。 ・ 日本の取り組みとして ISMS 制度について、パイロット事業や審査基準等について説明。
Tracking Session Track B : Policy & legal issues including privacy protection (9/13) 【室町委員】	<ul style="list-style-type: none"> ・ 1992 年からの環境変化について、法律の観点から説明。インターネット普及、暗号技術や VPN をはじめとするテクノロジーの進化、国際的な協調や標準化など。 ・ プライバシーの保護と追跡可能性、あるいは、セキュリティと利便性など、利益の対立が起こってきており、その調整が困難になっている。 ・ セキュリティの問題と reliability の問題は今後融合する。
Plenary Session 4 : Action For Information Security The Role of Stakeholders (9/13) 【大野経済産業省室長】	<ul style="list-style-type: none"> ・ OECD も含めた各者の役割ということと、国際協力としてはどのようなニーズがあるのかについて網羅的に指摘。 ・ 主体について、従来の政府、ビジネスに加え、individual といった新しい主体が出現している。ビジネスにおいても、ISP や Web サイトオペレータなどがある。CSIRT (緊急対応チーム) といったものも新しく出てきており、注目すべき点である。各主体がそれぞれの役割を果たしていくことが重要 ・ 政府の役割については、ルールや標準の設定、研究開発の推進、国際協力の推進、法執行、CSIRT の援助、意識の向上などが重要。特に日本の場合は、電子政府を構築していく過程での経験をベストプラクティスとして示していくことが求められている。
Plenary Session 5 : The OECD Guidelines in the Networked World (9/13) 【石田委員】	<ul style="list-style-type: none"> ・ 技術と運用の変化に対応した EM の修正が必要。 ・ 情報セキュリティは、国家安全保障、公共安全、及び、経済的安定の3領域を包含する。 ・ 各国政府は、民間部門との情報共有メカニズムを確立すること、ベストプラクティスを適用すること、サイバー 犯罪法を実施し、そして、セキュリティの事前研究をサポートすべきであることを奨励すべきである。 ・ OECD は、産業界による自主的でプライベートなベストプラクティスの開発のサポートに集中するべきである。

2.3 ワークショップクロージングステートメントについて

ピーター・フォード議長より、クロージングステートメントとして「ネットワークで結ばれた世界の情報セキュリティ (Information Security in a Networked World)」が宣言された。クロージングステートメントでは、ワークショップの成果として、各ステークホルダ間の情報の交換と共有を報告するとともに、OECD セキュリティガイドライン見直しへの期待感を表明している。

以下に、クロージングステートメントの仮訳を示す。

OECD ワークショップ：“ネットワークで結ばれた世界の情報セキュリティ”

背景

日本国政府の寛大なる支援を得て、“ネットワークで結ばれた世界の情報セキュリティ”と名付けられた OECD ワークショップは、2001 年 9 月 12 日 13 日の両日、東京お台場において成功裡に開催された。

本会議は、OECD、及び、日本国政府によって共同で計画されたものであり、日本情報処理振興事業協会(IPA)の支援を得ている。

ワークショップの目的は、インターネット時代における情報セキュリティに影響を及ぼす進展を評価し、情報通信技術の全てのユーザのために安全なサイバースペース環境を作成するに際して、国家のそしてまたグローバルなステークホルダ(利害関係者)の役割を探究することであった。

ワークショップは、OECD 加盟国および非加盟国の双方からと同様、政府の代表、企業、及び、一般の社会の広い範囲から参加者を得た。約 250 人の人々が、世界中で 27 ヶ国から集まった。この中には、政府、及び、ビジネス代表と同様に、消費者、ユーザーグループ、及び、セキュリティエキスパートが含まれる。

行政組織、及び、ビジネスセクタの間でのシナジー効果を高めるために、ワークショップは、9 月 14 日に同じ場所で開かれる GBDe (Electronic Commerce でのグローバルなビジネスダイアログ)と踵を接して開催された。

現在のポジション

1992 年における OECD 評議会の「情報システムのセキュリティに関するガイドラインについての勧告」の採択以来の 10 年の間に、OECD 加盟国の経済及び社会は、情報通信システムやネットワークの可用性、信頼性及びセキュリティにますます依存するようになった。

1997 年に行われた OECD セキュリティガイドラインの正式レビュー以来、インターネットによって象徴されるネットワーク技術、及び、電子商取引 (EC) を含む商慣習は変化し続け、情報通信システムの経済的及び社会的重要性を変えた。ウィルス、ハッキング、コンピュータ犯罪、及び、その他のサイバー脅威は、高い優先順位を有する政策関心事になった。政府と民間部門関係者間の協力は非常に重要になっている。

現在のレビューの完了は、喫緊の課題として待たれているところである。

ワークショップの結果

政府、民間部門代表、及び、他のステークホルダは、ワークショップを通じて情報、知識、及び、意見の交換と共有を行った。ワークショップの焦点は、インターネットに代表されるグローバルに遍在するネットワークによって結ばれた世界において、情報システムのセキュリティに影響を及ぼす現在及び潜在的な進展にあった。情報セキュリティに対する認識された脅威、及び、戦略、及び、政府の政策に対するそれらの影響における最近の展開が考慮された。我々の社会に影響を及ぼすかもしれない移動体通信、及び、他の科学技術上の傾向が、同じく考察された。脅威、方針、及び、アプローチの性質に関する共通の理解に向けて、参加者によって価値ある進歩がなされた。

ワークショップの結果は、この問題に関係する多くのフォーラムでの考察方針に影響を与えると期待される。

特に、全ての異なるステークホルダが一同に会して行った討論の成果は、ガイドラインの見直しの 2002 年完成に向けて、WPISP によって現在行われている 1992 年 OECD ガイドラインのレビューに大いに貢献すると期待される。

ピーター・フォード 議長
2001 年 9 月 13 日

3 . 主要なセキュリティ関連ガイドライン

IT 化が我々の経済、社会、生活に深く浸透するにつれて、情報セキュリティの確保は、自らの情報資産の保護のみならず、他者に対する信頼基盤の重要な要素となりつつある。国境のないインターネットにおいては、国際的に認められたスタンダードやガイドラインへの準拠性が、企業や組織の情報セキュリティに対する信頼の拠り所となることが期待される。

このような状況のもと、ISO を中心とする国際標準化機関において、情報セキュリティに関する各種の標準化が行われており、我が国においても、国際標準に対応した国内規格の制定や関連する制度の整備が進められている。

本章では、情報セキュリティに関する標準化動向のキャッチアップを目的として、以下のセキュリティ関連ガイドライン等について整理する。

- ・ ISO/IEC TR 13335 (GMITS)
- ・ ISO/IEC 17799 (JIS X-5080, BS7799 Part I)
- ・ 金融業務における情報セキュリティガイドライン ISO/TR 13569
- ・ 情報処理サービス業情報システム安全対策実施事業所認定制度 / ISMS 適合性評価制度

3 . 1 ISO/IEC TR 13335 (GMITS)

(1) 制定の経緯

1990 年の ISO/IEC JTC 1/SC 27 会合において、ヨーロッパ側からこの GMITS (Guidelines for the Management of IT Security) の構想が提案され、1991 年から GMITS 開発プロジェクトが開始された。1996 年から逐次、技術報告書 (Technical Report : TR) として公開されてきた。2001 年に JIS TR X 0036-1 から TR X 0036-4 の 4 部構成として制定されている。JIS TR 0036-5 は現在審議中である。

(2) 制定の背景

JIS TR X 0036-1 の 6 章では、この背景として「政府及び商業組織は、事業活動を行う際に情報の使用に大きく依存している。情報及びサービスの機密性、完全性、可用性、責任追跡性、真正性、及び信頼性が欠けると、組織に悪影響を及ぼすことになる。従って、組織内で、情報の保護と IT システムのセキュリティマネジメントが不可欠である。この情報保護の要件は、今日の環境で特に重要である。なぜなら、IT システムのネットワークによって多くの組織が内部的及び外部的に接続されているからである。」として、IT セキュリティマネジメントの重要性を捉えている。続けて、IT セキュリティマネジメントを「IT セキュリティマネジメントは、適切なレベルの機密性、完全性、可用性、責任追跡性、真正性、及び信頼性を達成して維持するためのプロセスである。」と、定義している。ここに述べられているとおり、TR X 0036(GMITS)においては、セキュリティの目的を、OECD 情報セキュリティガイドラインの定義：CIA (機密性(confidentiality)、完全性 (integrity)、可用性 (availability)) の確保、に加えて、「責任追跡性 (accountability)、真正性(authenticity)、信頼性(reliability)」を挙げていることが注目

される。(ここでの accountability は、OECD ガイドラインの第一原則に掲げられている Accountability Principle の概念とは異なる概念であることに注意が必要である。)

(3) 各シリーズの構成

(a) 第1部 ITセキュリティの概念及びモデル

第1部では、

- ・ ITセキュリティ、ITセキュリティマネジメントの概念及びモデルの概要
- ・ ITセキュリティの要素の吟味
- ・ ITセキュリティの管理に使用されるプロセスの検討
- ・ 概念の理解に役立つ幾つかのモデルの概要の説明、

の順でTRが構成されている。

特に、ITセキュリティマネジメント機能については、以下の9つの要素を掲げ、それぞれの重要性を提示している。

- ・ 組織のITセキュリティの目的、戦略、及び対策の決定
- ・ 組織のITセキュリティ要件の決定
- ・ 組織内のIT資産に対する、セキュリティ上の脅威の識別および分析
- ・ リスクの識別および分析
- ・ 適切なセーフガードの指定
- ・ 組織内の情報とサービスを費用対効果に優れた方法で保護するために必要な、セーフガードの実施および稼働の監視
- ・ セキュリティ意識向上プログラムの開発および実装
- ・ 偶発事件の検出および対応

更に、セキュリティマネジメントとは、構成マネジメント、変更管理、リスクマネジメント、リスク分析、モニタリングなどの個々のプロセスによって構成される継続型のプロセスである、と定義し、各プロセスを詳述している。

最後に、そこまでに述べられた各概念を用いて、(資産、価値、脆弱性、脅威、リスク、保護要求事項、セーフガード)の7つの要素を用いて、セキュリティ要素の関係、およびリスクマネジメントにおける関係等、幾つかのモデルを提示している。

(b) 第2部 ITセキュリティのマネジメント及び計画

第2部は、ITセキュリティの効果的なプログラムとそれにかかわるマネジメントプロセス及び責任についての検討に充てられている。この検討は、ITセキュリティマネジメントに登場する幾つかの主要なプロセス及び機能を、管理者に良く知ってもらうことを目的としてなされている。

一方、第2部が提供する情報は、全ての組織にそのままの形で適用できるものでは

ないかもしれないという認識を示し、特に、小規模の組織などのように、説明した機能を完全に実行するための資源を全て持っている場合が少ないような状況では、基本的な概念及び機能を組織に適した方法で取り扱うことが重要である、としている。

(c) 第3部 ITセキュリティマネジメントのための手法

第3部では、ITセキュリティマネジメントにとって重要な幾つかの手法の検討に充てられている。これらの手法は、第1部で提供された概念とモデル及び第2部で考察したマネジメントプロセスと責任に基づくものである。標準情報(TR)群のこのパートにおける考察では、リスク分析を行うに当たってとりうる4つの戦略(ベースラインアプローチ、非形式的アプローチ、詳細リスク分析、組み合わせアプローチ)のメリット及びデメリットがそれぞれ示されている。そして、その実施に役立つ組み合わせアプローチ及び幾つかの手法が詳細に記述されている。

一部の組織、特に小規模組織では、第3部で提供された全ての手法を、正確に記述したとおりの方法で実施することは出来ないかもしれない、という認識は第2部と同様であり、これらの手法それぞれをその組織に適した方法で実施することが重要である、とする点も同様である。

(d) 第4部 セーフガードの選択

第4部では、ベースライン保護を達成するために使用できるセーフガード、すなわち第3部に記述した技法をサポートするセーフガードの各種の選択方法が説明されている。また、第4部では、上記のどのアプローチをとっても使用できる共通のセーフガードや、これらのセーフガードについての詳細な記述がある各種ベースラインセーフガードマニュアルへの参照も記載されている。最後に、全組織規模のベースラインの開発方法、他の方法の優劣についても説明が加えられている。第4部は、規模の大小を問わず、ITシステムの保護のためのセーフガードを選択しようとしているあらゆる組織で使用することが出来る、としているが、これはセーフガードという方法論の適用に関するTRであるから、当然のことであろう。

(e) 第5部 マネジメントガイダンス

ISO/IEC TR 13335では、第5部として、ネットワークセキュリティ上のマネジメントガイダンス(Management guidance on network security)が掲げられている。(JIS化は検討中)内容は、

- ・ コーポレートITセキュリティ要件のレビュー
- ・ ネットワークアーキテクチャとアプリケーションのレビュー
- ・ ネットワーク接続の種類判定
- ・ ネットワーキングアーキテクチャと関連信頼関係のレビュー
- ・ セキュリティリスクの種類判定
- ・ 適切な能力のセーフガード領域

- ・ 文書化とセキュリティアーキテクチャオプションのレビュー
- ・ セーフガード選択設計実装保守の再検討の準備

等である。

3.2 ISO/IEC 17799 (JIS X-5080, BS7799 Part I)

(1) 制定の経緯

英国 DTI (Department of Trade and Industry) は、1990 年代初め、情報セキュリティマネジメントに関する作業グループを産業界と組織し、有効とされる実践規範 (code of practice) を抽出した。これを BS 7799 の基礎として、BSI(British Standards Institute)が 1995 年に発表した。

BS 7799 は次の 2 部構成である。

- ・ BS 7799-1 (Part1): 「情報セキュリティマネジメントのための実践規範 (Code of practice for information security management)」
- ・ BS 7799-2 (Part 2): 「情報セキュリティマネジメントシステムのための仕様 (Specification for information security management systems)」

1999 年には、2 部とも改訂され、このうち BS 7799-1 だけが SC 27 において審議され、2000 年 9 月の投票手続きの後 11 月に ISO 標準として認められた。

ISO/IEC 17799 については、2001 年 4 月のオスロ会合にて早期見直しが採決され、現在、見直し作業が進行中である。また日本国内においては 2001 年 9 月に、ISO/IEC 17799 を翻訳した JIS X 5080 が日本規格協会の情報技術専門委員会で承認された。

(2) 制定の目的

コンピュータシステムによる情報処理・データ交換・保存処理は、ドッグイヤーとも形容される情報化社会の進展速度に促される形で、各企業及び組織の活動の中に根深く入り込み、いまや IT (情報技術) なしでの組織の活動は考えられなくなってきている。企業及び組織がコンピュータで扱う情報の中に高度な機密情報及び個人情報が含まれるのも珍しいことではない。このため、これらの IT 資産 (情報やコンピュータシステム) を、不正使用或いは外部からの攻撃などから保護する仕組み (情報セキュリティの維持) の重要性が高まっている。日本においても 2000 年初頭から頻発している Web サイトのページ改ざん、コンピュータシステムへの不正侵入及び運用妨害など、悪意の攻撃が規模及び深刻度を増して行政や民間組織の活動全般に大きく影響を与えるものとなりつつある。このように、情報セキュリティは、もはや脅威に対抗するコンピュータ技術やシステム管理担当者だけの課題ではなくなり、経営層の参画も必要とし、経営、管理の面を含めた総合的な対処を必要とするものになっている。

この状況を受け、情報処理システムのセキュリティ上のリスクに対して、対抗のためのシステムティックなセキュリティ管理対策を提供する仕組みの構築が要求されるよう

になってきた。ISO/IEC 17799 は、それが提供するセキュリティ管理対策指針を、情報処理システムの管理者、運用者、業務者が実施することで、より安全なシステムの運用が可能になることを目的として制定されている。

(3) 概要

BS7799 は part I、part II の 2 部構成になっているが、そのうち、part I のみが ISO/IEC 17799 として ISO 標準になっている。

ISO/IEC 17799 は「IT セキュリティ管理実施基準」として、IT セキュリティ管理項目の内容を規定している。

IT セキュリティ管理項目は次の 10 個の管理分野 (security domain) が規定されている。

- ・ セキュリティ基本方針 (3. Security policy)
- ・ 組織のセキュリティ (4. Organizational security)
- ・ 資産の分類及び管理 (5. Asset classification and control)
- ・ 人的セキュリティ (6. Personnel security)
- ・ 物理的及び環境的セキュリティ (7. Physical and environmental security)
- ・ 通信及び運用管理 (8. Communications and operations management)
- ・ アクセス制御 (9. Access control)
- ・ システムの開発及び保守 (10. Systems development and maintenance)
- ・ 事業継続管理 (11. Business continuity management)
- ・ 適合性 (12. Compliance)

上記 () 内は、現国際規格の項番と名称

この 10 個の管理分野の中に、36 個のセキュリティ目的 (security objectives) があり、さらに、その対策方針の中に合計 127 個の管理方策 (controls) が規定されている。

本規格の Introduction 「情報セキュリティの基本及びこの規格の位置づけ」において、「情報セキュリティの基本は、リスクアセスメントを実施してセキュリティ要求事項を識別し、その上で、リスクを受容可能なまで低減する管理方策を選択して実施することである」と規定していることが注目される。セキュリティ対策に対するこの思想は、OECD 情報セキュリティガイドラインの第 5 原則：比例性の原則 (Proportionality Principle) と軌を一にするものであろう。

その上で、重要な主張として、次の 2 点を挙げることができる。

第 1 に、この規格に基づく情報セキュリティマネジメントは、それを適用する情報システムそれぞれに、リスクアセスメントに基づき 127 個の管理方策の中から適切なものを選択してセキュリティ対策を実施していくこと、さらには、企業及び組織が選択すべき管理方策は、この規格が掲げている 127 個の管理方策のなかに限定されるものではないとしている点、第 2 に、これまでの情報セキュリティ対策は、情報システム部門が実

施するものであり、またハードウェアを中心に対処されるものと受け止められてきたのに対して、この規格では、経営層が関与して策定したセキュリティ基本方針を起点とした、職員をはじめ外部委託業者なども参加する幅広い活動として計画し実践することを推奨している点である。

この基本方針に基づき、各企業及び組織は、関連する諸手順及びそれぞれの運用の責任体制を定め、物理的な面と管理的な面との両面からの管理方策を計画、実施し、その効果を監視して、情報の保護を継続的に維持、改善していくことを推奨している。

3.3 金融業務における情報セキュリティガイドライン ISO/TR 13569

(1) 制定の経緯

ISO/TR 13569 の第 1 版は 1996 年 11 月に制定され、暗号技術の利用に関する記述の追加等が行われた第 2 版が 1997 年 10 月に制定された。

1998 年 12 月には、第 2 版の一部を改訂する「修正第 1 号 (Amendment 1)」を発表した。修正第 1 号では、アクセス管理の手段として、公開鍵証明書を用いた方法やバイオメトリックスを利用する際の留意点が追加されたほか、暗号技術について、共通鍵暗号や公開鍵暗号における推奨最短鍵長が盛り込まれた。

さらに ISO/TC68/SC2 では、ISO/TR 13569 第 2 版の見直しにあたって、ISO/IEC TR 13335 (GMITS) の内容を取り込む方向で作業が進められている。新たに、情報セキュリティポリシー、情報セキュリティ手段の選択、セキュリティに対する意識向上などに関する項目が追加、編成される予定である。

(2) 制定の目的

ISO/TR 13569 は、銀行、証券会社等の金融機関が情報セキュリティ対策を実施する際の指針を提供する技術報告書 (Technical Report : TR) であり、ISO/TC68/SC2 において策定された。

ISO/TR 13569 策定の目的として、以下の 3 点が挙げられている。

- ・ 情報セキュリティプログラムの構造 / 構成要素について解説する。
- ・ 情報セキュリティ対策を講じるための手段を選択する際の指針となる情報を提供する。
- ・ 既存の標準規格との整合性だけでなく、策定段階にある標準規格案との整合性もとれた情報セキュリティ対策を実現可能にする。

(3) 概要

ISO/TR 13569 は、情報セキュリティポリシーや情報セキュリティプログラムを作成する際の指針について規定する部分と、情報セキュリティプログラムを作成した上で、具体的な情報セキュリティ対策の実施方法を検討する際の指針を与える部分、の 2 つのパートに大別することができる。

ISO/TR 13569 では、情報セキュリティプログラムの構成要素として以下の項目を定

めている。

- ・ 情報セキュリティポリシーの策定
- ・ 情報セキュリティ管理専門部署の設置方針
- ・ 役職員への情報セキュリティに関する研修プログラム
- ・ 災害情報等の情報伝達 / 復旧プラン
- ・ 情報セキュリティプログラムから逸脱した事象の発見 / 対応手続き
- ・ 監査、保険、法務部門との連絡手続き
- ・ 情報セキュリティプログラムの見直し手続き
- ・ 監査記録の作成 / 管理方法

情報セキュリティプログラムに関する規定に続く章では、具体的な情報セキュリティ製品 / システムを管理する際の指針を提供する。指針の内容は以下の通り。

- ・ 基本的な情報管理手段（必要度や機密度による情報の分類、アクセス管理、システム運用記録の管理、システム変更時の管理）
- ・ コンピュータやネットワーク等具体的な情報セキュリティ製品の管理方法
- ・ 暗号技術を利用する際の指針

3.4 情報処理サービス業情報システム安全対策実施事業所認定制度の改革と ISMS 適合性評価制度

(1) ISMS 適合性評価制度制定の経緯

情報処理サービス業を行う事業所を対象とした安全対策認定制度として、「情報処理サービス業情報システム安全対策実施事業所認定制度（以下「安対制度」）」が昭和 56 年より運用されてきた。同制度は、情報システムに関して一定の安全対策が施されている（認定基準に合致している）事業所を国が認定することにより、情報処理サービス業における安全対策の実施の促進を図ることを目的とするものである。現在約 200 事業所が認定事業者として認定を受けている。

経済産業省（当時 通商産業省）は 2000 年 7 月、インターネットの世界的な普及と情報セキュリティ管理に関する国際スタンダードの必要性の高まりを背景に、国際的にも信頼を得られる情報システムのセキュリティ管理に関する第三者適合性評価制度の確立を目指し、安対制度の見直しを行った。

これに伴い、国際的な規格等に沿った基準類（JIS 等）を策定するとともに、当該 JIS 等をベースとした民間による適合性評価制度として「情報セキュリティマネジメントシステム（ISMS）適合性評価制度（以下「ISMS 適合性評価制度」）」を制定した。2001 年には ISMS 適合性評価制度のパイロット事業が行われており、2002 年 4 月から本格的に運用が開始される予定である。また、従来実施してきた安対制度は 2001 年 3 月をもって廃止されている。

(2) ISMS 適合性評価制度の概要

ISMS 適合性評価制度の対象範囲は、従前の安対制度に準じて「情報処理サービス業を営む者」と規定されている。ISMS 適合性評価制度では、新しい形態の情報処理サービス事業者をカバーすることを検討するとともに、将来的には情報処理サービス事業者以外への適用も視野に入れている。

安対制度が、主として設備等の物理的な対策に重点を置いた認定基準であったのに対し、ISMS 適合性評価制度では、設備 / 運用面をバランスよく盛り込むとともに、情報セキュリティマネジメントの観点からの管理策を付加した点が特徴となっている。

ISMS 適合性評価制度における、事業者の適合性を評価する認証基準は、国際標準 ISO/IEC 17799 を基にし、英国規格 BS7799-2 を参考として作成された。またこの評価基準は、国際標準の JIS 化の動向等や JIS 化後の周知状況を踏まえ、より時代に適合したものにするため見直し改訂を図ることとしている。

(3) ISMS (Information Security Management System : 情報セキュリティマネジメントシステム) の概念

情報セキュリティマネジメントシステム (ISMS) とは、情報セキュリティに関わる問題について個別の技術対策を行うとともに、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して、情報システムを運用することである。

組織が保護すべき情報資産について、機密性、完全性、可用性をバランスよく維持し改善することが、ISMS の要求する主要なコンセプトである。

ISMS のポイントは、組織が情報セキュリティ対策の方針を示したポリシーを作成することから始まり、ポリシーを基に以下の Plan-Do-Check-Action のサイクルを継続的に繰り返し、情報セキュリティレベルの向上を図ることにある。

- ・ Plan : 情報セキュリティ対策の具体的計画、目標を策定。
- ・ Do : 計画に基づいて対策の実施 / 運用を行う。
- ・ Check : 実施した結果の監査を行う。
- ・ Action : 経営陣による見直しを行い、改善する。

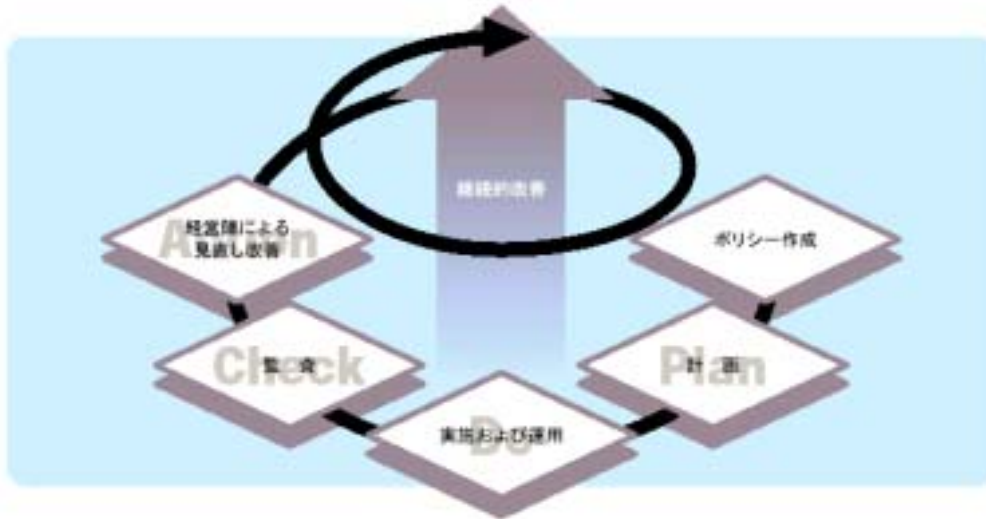


図 3-1 ISMS の Plan-Do-Check-Action のサイクル（出典：日本情報処理開発協会資料）

（４）ISMS におけるマネジメント枠組みの確立

ISMS では要求事項として、「マネジメント枠組みの確立」について定めている。マネジメント枠組みの確立では、管理目的及び管理策の内容を明確にし、その目的及び内容を文書化するために以下の作業を実施することとしている。

- （ a ） 情報セキュリティポリシーの策定
- （ b ） ISMS の対象範囲の決定
- （ c ） リスク評価
- （ d ） リスクマネジメントの対象範囲の決定
- （ e ） 管理策の選択
- （ f ） 適用宣言書の作成

また、上記の各項目について定期的または必要に応じて見直すことと定めている。

図 3-2 に標準的な ISMS 構築スキームを示す。図中の各ステップは、上記の各項目に対応している。

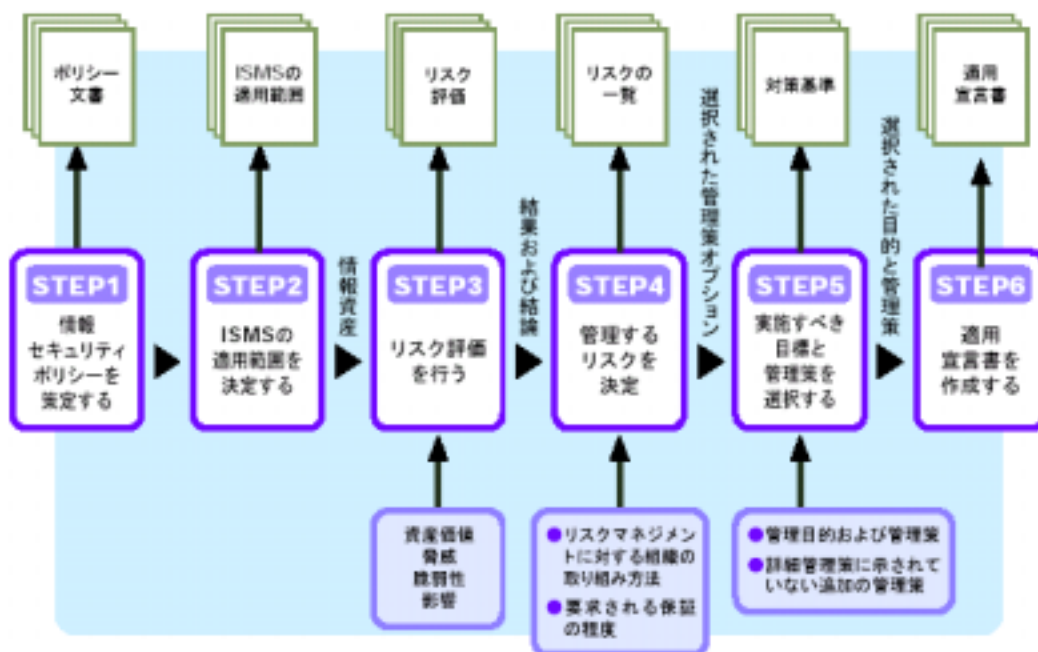


図 3-2 ISMS 確立のステップ (出典：日本情報処理開発協会資料)

(4) ISMS 適合性評価制度のスキーム

ISMS 適合性評価制度は、認証を希望する組織（事業者）と利害関係を持たない第三者（財団法人 日本情報処理開発協会によって指定された審査登録機関）によって審査が行われる、第三者認証制度である。

第三者認証の場合には、第一社（自社）の実施する内部監査や第二者（取引先等）に依頼して実施する外部監査に比べて、審査における客観性、審査結果の信憑性が確保でき、顧客やビジネス上の関係者に対して情報セキュリティマネジメントの有効性を主張するのに役立つと考えられている。

ISMS 制度における各機関、事業者の役割は以下のとおりである。

(a) 財団法人 日本情報処理開発協会（JIPDEC）

- ・ 本制度全体を運用するとともに、維持管理する。
- ・ 本制度の審査登録機関を指定するとともに、審査登録機関を登録管理する。
- ・ 必要に応じて審査登録機関の審査業務をオブザーブ（観察）する。
- ・ 審査登録機関より評価希望事業者の審査結果の報告を受けるとともに、認証された事業者を登録する。
- ・ 段階的に ISO/IEC Guide 61(JIS Z 9361)の要求事項をクリアする。

(b) 審査登録機関

- ・ 指定基準[ISO/IEC Guide 62(JIS Z 9362) を準用]に基づき審査登録機関を整備する。
- ・ 評価希望事業者の申請を受付けるとともに、ISMS 認定基準により審査を実施

する。

- ・ 審査結果により評価希望事業者を認証する。
- ・ 審査結果は JIPDEC へ届出（審査報告）をする。

(c) 評価希望事業者

- ・ 本制度の認証を希望する事業者は、審査登録機関に対して申請することができる。
- ・ 申請適用範囲の ISMS を確立する。
- ・ 本制度の ISMS 認証基準に基づき審査を受けることができる。
- ・ 審査結果に基づき認証登録を受けることができる。
- ・ 認証を受けた場合には、本制度の規程にしたがってマークを付することができる。

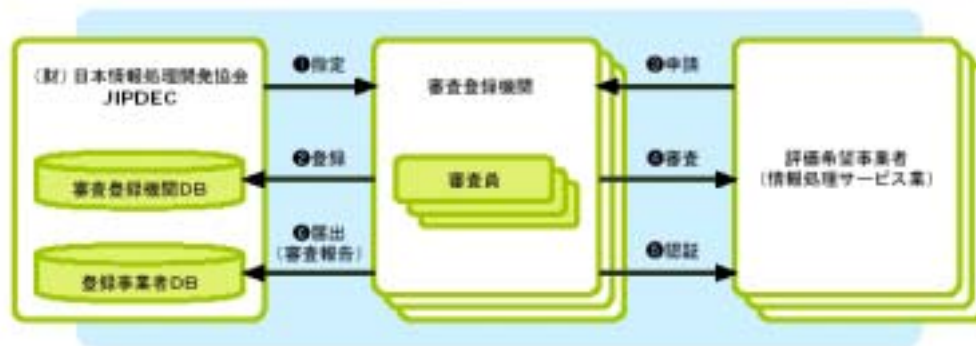


図 3-3 ISMS 適合性評価制度のスキーム

4 . 国内外における情報通信システムに対する脅威の動向

1992 年に OECD 情報システムセキュリティガイドラインが作成されてから 10 年、情報システムのセキュリティを取り巻く環境は劇的に変化を遂げている。

この間、インターネットは飛躍的に発展し、学術 / 研究の分野から、公的部門および民間企業、さらには一般の生活者へと普及してきた。また近年では、携帯電話や無線ネットワークなど新規技術が成熟し、広く一般に浸透している。ネットワークを含む情報システムは、今日の社会を支えるインフラストラクチャとして、また、世界経済の原動力として、その重要性はますます大きくなっているといえる。

こういった環境変化を背景として、情報システムのセキュリティに対する脅威も変化しており、経済や社会に及ぼす影響やその範囲も格段に大きくなっている。その意味で、今日の脅威は、以前にも増してより深刻な存在になっているといえる。

ここでは、1992 年当時からの情報システムのセキュリティに対する脅威に関する環境の変化、脅威に対する取り組みの動向、および今後の課題について分析する。

4 . 1 情報システムのセキュリティを取り巻く環境の変化

1990 年代以降、インターネットの社会・経済・生活のあらゆる場面に爆発的な勢いで浸透してきた。それに伴って、情報システムのパラダイムそのものが変化するとともに、情報システムに関わるステークホルダの種類とその役割も以前とは大きく異なるものとなっている。

ここでは、情報システムのセキュリティを取り巻く背景はどのように変化してきたかについて、以下の観点から整理する。

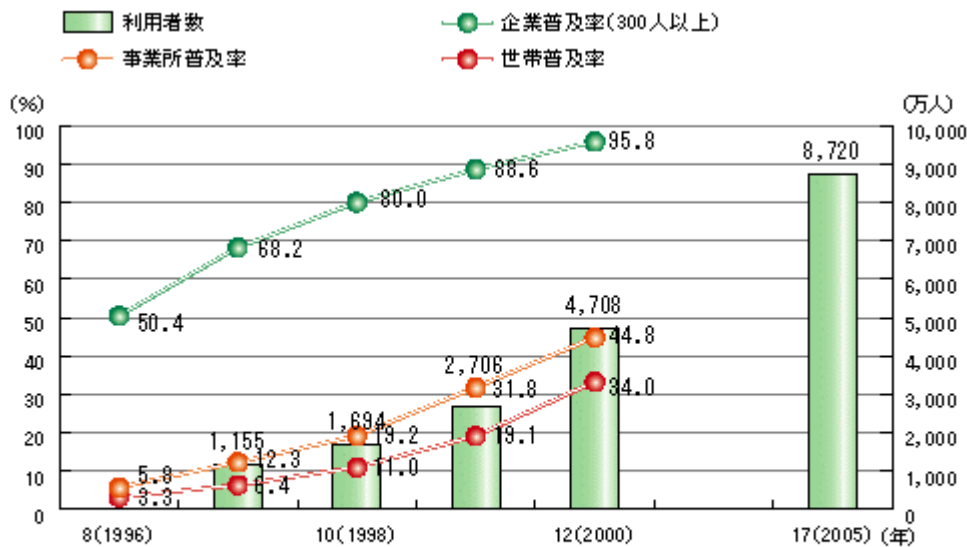
- ・ インターネットの爆発的普及とインパクト
- ・ 情報システムに関わるステークホルダの拡大
- ・ 情報システムのパラダイムの変化

(1) インターネットの爆発的普及

米 Network Wizards は、DNS(Domain Name Service)にもとづき、インターネットに接続する世界のホスト・コンピュータの台数を定期的に公表している。この資料によると、1992 年 1 月当時 72 万台程度であった全世界のインターネットホスト数は、2001 年 7 月の時点で、1 億 2 千 5 百万台に指数的に増加していることがわかる。また、インターネットの利用者数をみると、2001 年の 8 月現在、世界のインターネット人口は 5 億 1 千万人を超えている (NUA 調査) 。地域別に見ると、米国・カナダの 1 億 8,068 万人が最も多く、ヨーロッパの 1 億 5,463 万人、アジア / パシフィックの 1 億 4,399 万人と続く。以前は北米が半数を占めていたが、近年アジア / パシフィックを中心としたその他の地域におけるインターネット人口の増加が著しい。インターネットは、世界のあらゆる地域へと拡大しているといえる。

我が国においては、平成 12 年末時点のインターネット利用者が 4,708 万人となってお

り、対前年比で 74%増加した（平成 13 年度版 情報通信白書）。ここで、「インターネット利用者」とは、インターネットを自宅・自宅外を問わず、パソコン、携帯電話、携帯情報端末、ゲーム、インターネット接続テレビにより利用している人を含む。特に、1999 年頃よりインターネット接続サービスが開始された携帯電話や PHS からの利用者数の急激な伸びが、インターネット利用者数の増加を押し上げる要因となっている。



※1 事業所は全国の(郵便業及び通信業を除く。)従業員数5人以上の事業所。
 ※2 「企業普及率(300人以上)」は全国の(農業、林業、漁業及び鉱業を除く。)従業員数300人以上の企業。

「生活の情報化調査」、「通信利用動向調査」(総務省)より作成

図 4-1 我が国におけるインターネットの普及状況

(出典：平成 13 年度版 情報通信白書)

インターネットが 1990 年代に入って商用開放されたのを契機に、金融、製造、流通等の分野でのインターネット上での電子商取引が発展してきた。それと同時に、インターネット上における経済の発展は、雇用の創出にも寄与し、産業構造の変化をもたらしている。

テキサス大学電子商取引研究センターが定期的公表しているインターネット経済に関する調査レポートによると、1998 年にインターネット利用により得られた米国の総収益は推定で 3,014 億ドルにのぼり、120 万人分の雇用が創出されたという。この総収益はすでにエネルギー産業、自動車、電気通信といった旧来の産業に匹敵する水準に成長している。

我が国においても、インターネット上の電子商取引が急速に拡大しており、今後もこの傾向は続くと予想される。電子商取引推進協議会 (ECOM) が NTT データ経営研究所及び経済産業省と共同で行った「平成 13 年度電子商取引に関する市場規模・実態調査」によると、2001 年の B to B / B to C の電子商取引市場規模はそれぞれ 34.0 兆円 / 1 兆 4,840 億円と億円となっている。B to B については、1998 年以降 3 年間で 4 倍、年

率約 60%の急成長を遂げ、一方、B to C についても 2001 年に 1 兆円を突破するなど大幅な拡大基調を継続している。同調査では、2005 年には B to B / B to C 市場規模は、それぞれ 98 兆円 / 12.5 兆円に成長すると予測している（図 4-2）。

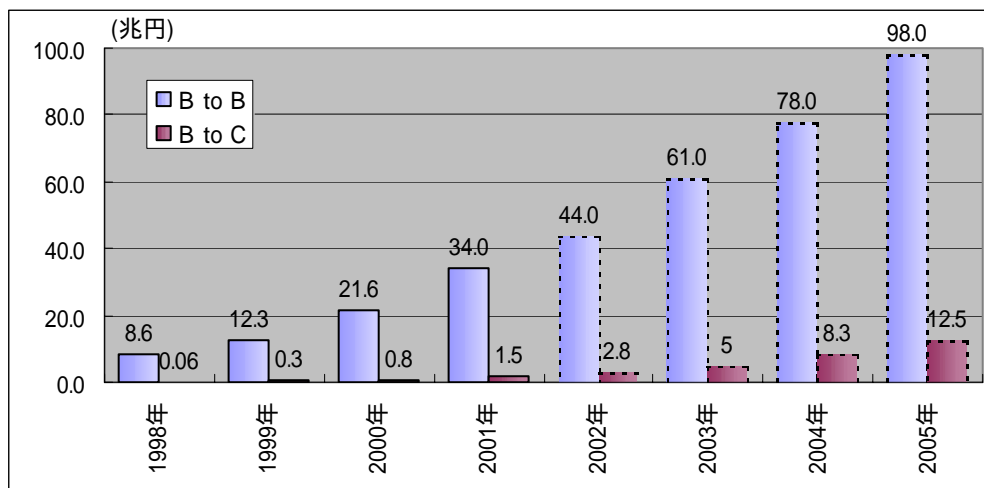


図 4-2 B to B / B to C の電子商取引市場規模推移（2002 年以降は予測）
（ECOM「平成 13 年度電子商取引に関する市場規模・実態調査」より作成）

（2）情報システムのパラダイムの変化

インターネットに代表される情報技術（IT）の進化が、あらゆるセクターの情報システムのパラダイムそのものに変化をもたらしている。特に、インターネットをベースとしたアプリケーション / サービスの種類は、電子メールや FTP（File Transfer Protocol）から、World Wide Web（WWW）や Voice over IP へと多様化してきている（図 4-3）。

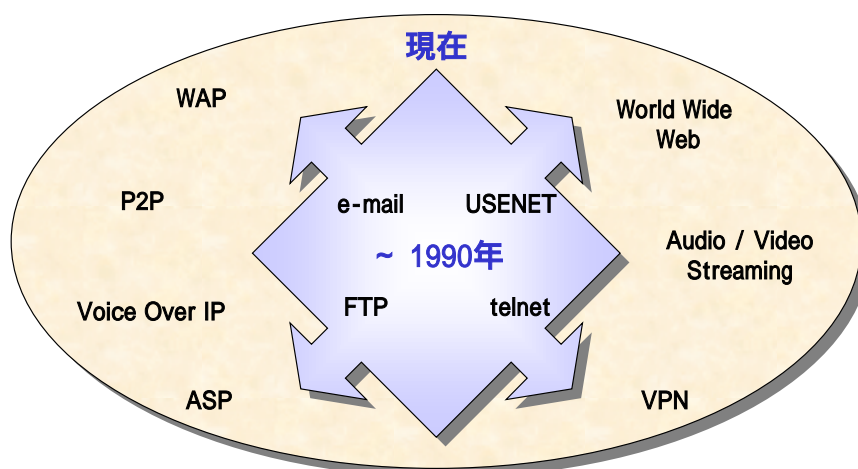


図 4-3 多様化するインターネットのアプリケーション / サービス

企業や政府機関等の組織の情報システムは、1980年代後半よりそれまでの主流であったメインフレームを中核とした集中型システムから、PC や WS などのオープンシステムへとダウンサイジングが進んできた。この背景には、CPU やメモリ、ハードディスクなどハードウェアの性能価格比の飛躍的な向上と、UNIX や Windows といった OS 及びその上で動作するアプリケーションなど、ソフトウェア技術の進化によるところが大きい。このような技術革新に加えて、Linux や Apache ウェブサーバなど、いわゆるフリーソフトウェアが、ビジネスの場面でも使用されるようになってきており、多様化する情報システムのひとつの流れとなっている。(図 4-4)

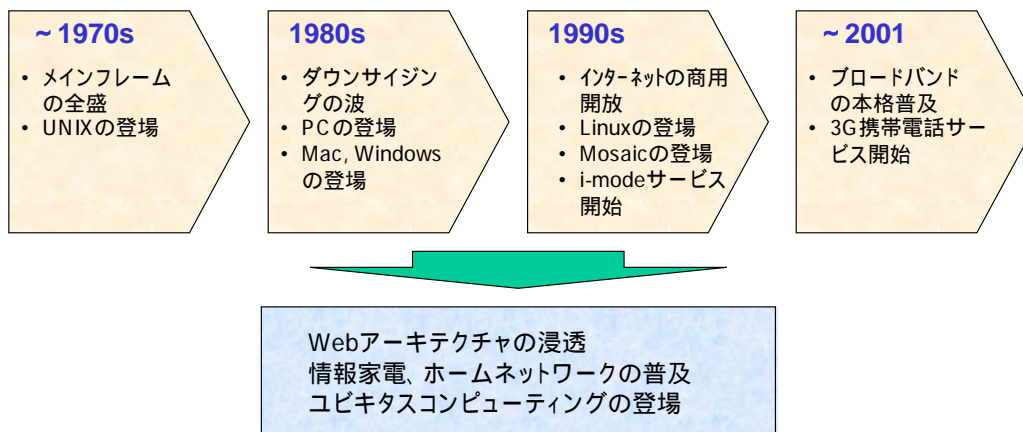


図 4-4 情報システムのパラダイムの変化

加えて、情報システム同士のネットワーク化の進展が、企業や組織の情報システムの方向性に大きなインパクトを与えている。組織内のシステム同士が、LAN (Local Area Network) で接続されると同時に、組織を超えた情報システム同士が相互に接続されるようになってきている。さらに、インターネットバンキングなどにみられるように、フロントエンドのインターフェースに Web ブラウザを利用し、バックエンドの基幹システムやデータベースとのアクセスを提供する「Web アーキテクチャ」が多くの企業システムにおいて採用されるようになってきた。また、Java や ActiveX といったネットワーク上でプログラムを配信可能とするソフトウェア技術により、Web は単なる情報閲覧を超えて、よりインタラクティブなアプリケーションを実行できるようになっている。

最近では、XML (eXtensible Markup Language) や CORBA (Common Object Request Broker Architecture) といった技術により、より大規模なシステム間の連携が可能になっている。企業の枠を超えてネットワーク上で電子データの交換を行う EDI (Electronic Data Interchange) も、B to B の電子商取引の基盤を形成する技術となっている。

企業や組織の情報化が進む一方、PC やインターネットが家庭においても普及し家庭内の情報が着実に進んでいる。また、最近では情報家電やホームエレクトロニクスといったネットワークに対応した家電製品の登場が注目を集めている。さらに今後、いつでも、

どこからでもネットワークにつながり、各種のサービスにアクセスする「ユビキタスコンピューティング」が現実的なものとなってくることが予想される。

情報システムのセキュリティについて議論する場合においても、テクノロジーの進化に合わせて情報システムそれ自体が多様化、複雑化している状況を考慮することが重要になっているといえる。

(3) 情報システムに関わるステークホルダの拡大

インターネットの普及によって、情報システムは社会や生活のなかに深く浸透してきており、情報システムに関わるステークホルダも、個人利用者、スモールビジネス、学校など多様化してきた。

「平成 13 年度版 情報白書」の調査結果(図 4-1)によると、2000 年におけるインターネットの世帯普及率は 34.0%に達している。また、従業員 5 人以上の事業所においても、1996 年から 2000 年の 5 年間で、5.8%から 44.8%へと急速に拡大しているのがわかる。

国の IT 関連政策の進展と相まって、情報ネットワークの運用主体は、これまで大半を占めてきた各種プロバイダ、大学、民間企業に加えて、個人や教育機関、行政機関の比重が増大していく。

1994 年に始まった「100 校プロジェクト」以来、インターネットやその他の情報技術を活用する教育の情報化が進められてきた。関係省庁のイニシアチブの下、2001 年度中に全ての公立小中高等学校等がインターネットに接続されるよう整備が進められており、さらに 2005 年度までに概ね全ての公立学校が高速インターネットに常時接続可能にする方針が打ち出されている。

また、国の IT 政策の方向性を定める「e-Japan 戦略」(2001 年 1 月策定)を受け、2001 年 3 月に発表された「e-Japan 重点計画」では、基本方針の柱の一つとして「行政の情報化及び公共分野における情報通信技術の活用の推進」がかかげられ、申請・届出等手続のオンライン化、入札・開札の電子化および関連法令の見直し等に関する目標が設定されている。

さらに今後は、急速に利用者を増やしているオークションサイトや e マーケットプレイスといった電子商取引の仲介者のプレゼンスも大きくなることが予想される。

4.2 セキュリティ基盤に関する動向

わが国における情報通信のセキュリティ基盤に関する動向に関連して、不正アクセスやウィルス等の現状について整理する。

4.2.1 不正アクセス

2001 年の年間届出件数は 550 件となり、前年(2000 年)の届出件数 143 件に対して約 3.8 倍まで急増した(図 4-5)。

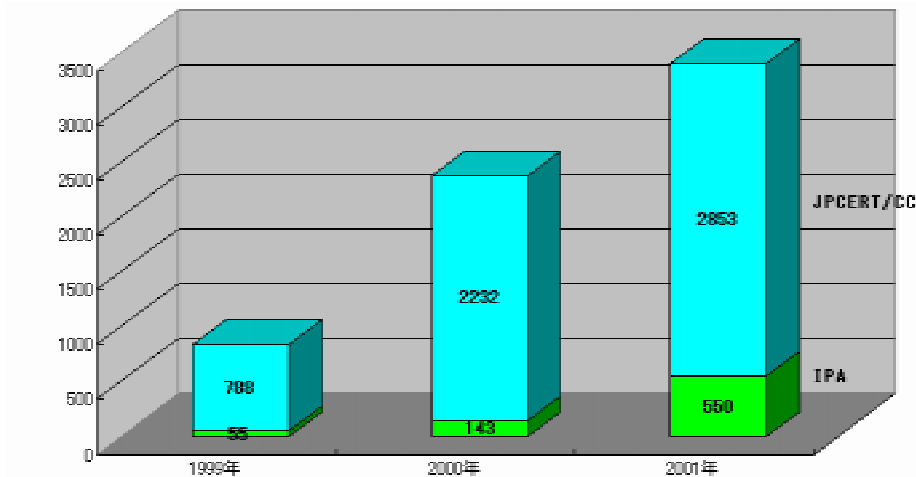


図 4-5 不正アクセス届出件数の年別推移 (1999年～2001年)(出典：IPA)

家庭におけるインターネット接続が普及するに伴って、個人等がセキュリティ侵害による被害を受けるケースも急増している。IPAによると、不正アクセスに関する個人からの届出の割合が2000年の4%から2001年は一気に47%まで増加している(図4-6)。IPAではこの要因として、個人ユーザにおけるADSLなどの常時接続環境の普及とパーソナルファイアウォールの家庭への導入が寄与していると分析している。

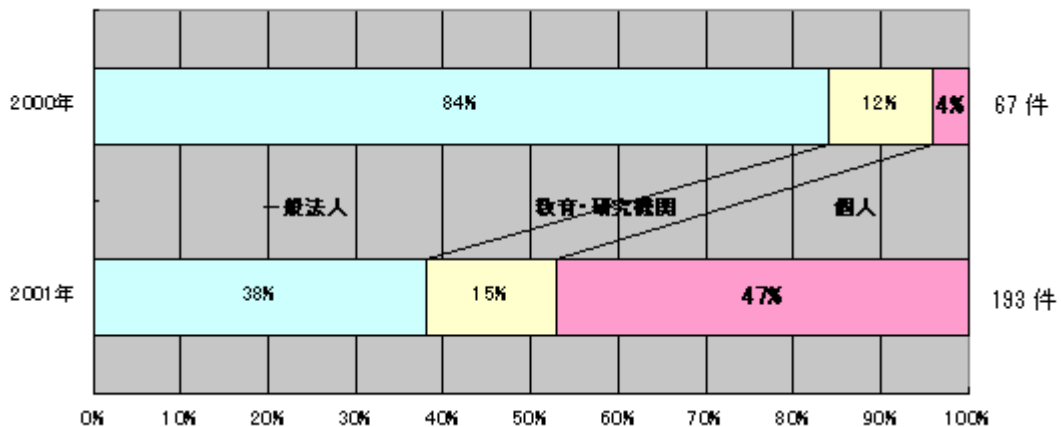


図 4-6 不正アクセス届出別推移 (出典：IPA)

以下に2001年における不正アクセス届出の傾向を示す。

- ・ 実際に被害に及んだケースが約7割。
- ・ 特に2001年は、Sadmind/IIS、CodeRed、Nimdaなど既知のセキュリティホールを悪用したワームの出現により、ワーム感染及びワーム形跡(未感染)に関するものが全体の約46%を占めた
- ・ 被害内容の分類については、半数近くがWWWサーバの書き換えの被害であり、

その要因としては、ワーム感染 によるものが多く全体の約 4 割。ワームに感染した場合には、自らが感染元となり、 被害者から加害者へ立場が逆転する場合も。
(図 4-7)

- ・ 原因別分類では、「古いバージョン、パッチ未導入など」「設定不備」など基本的な(既知の)対策をとっていれば被害を未然に防げたケースが全体の約 8 割。
- ・ 特にワーム感染においては、Microsoft 社の IIS (Web サーバ) や Internet Explorer(ブラウザ)などのセキュリティホールが原因の被害が多く届出された。

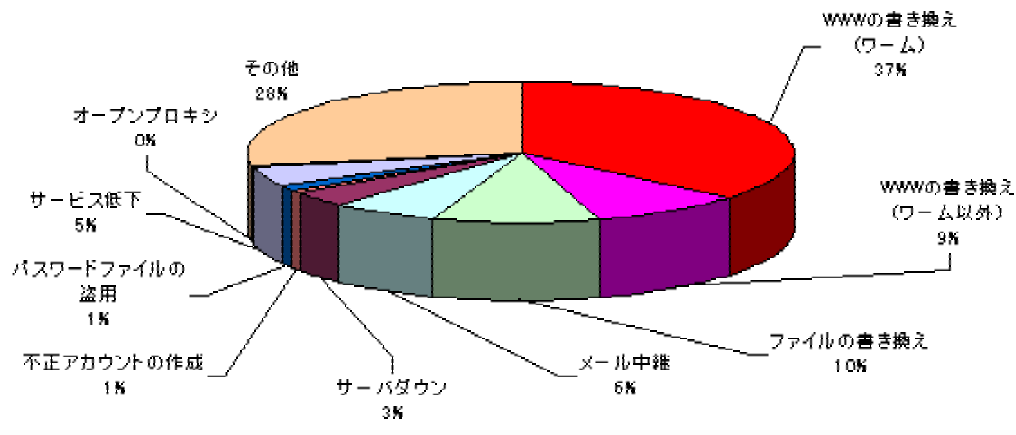


図 4-7 2001 年不正アクセス被害内容分類 (出典 ; IPA)

警察庁の報告によると、2001 年中の不正アクセス行為は、計 1,253 件で、前年の不正アクセス行為と比較して約 12 倍となった。このうち、海外から不正アクセス行為が行われたことが判明しているものは 448 件で、前年の約 18 倍となっている。

警察庁では、不正アクセス行為の大幅に増加した要因として、特に以下の事案の発生が寄与したと分析している (図 4-8)。

- ・ ホームページ書換えプログラムによるホームページ書換え事案 (813 件)
- ・ 自己増殖型不正プログラムによる事案 (94 件)
- ・ 攻撃予告に関連すると思われるセキュリティホール攻撃型の不正アクセス行為の連続発生事案 (以下「攻撃予告に絡む事案」という。)(55 件)
- ・ 自己増殖型 DoS 攻撃プログラム及び自己増殖型バックドア作成プログラムによる事案 (28 件)

2001 年中に、不正アクセスの被害を被ったサーバ管理者の業種をみると、一般企業が 429 件 (2000 年 25 件) と最も多く、次いでプロバイダ 182 件 (同 59 件)、大学、研究機関等 101 件 (同 8 件) の順となっている。全ての業種において、大幅に増加している状況がわかる。

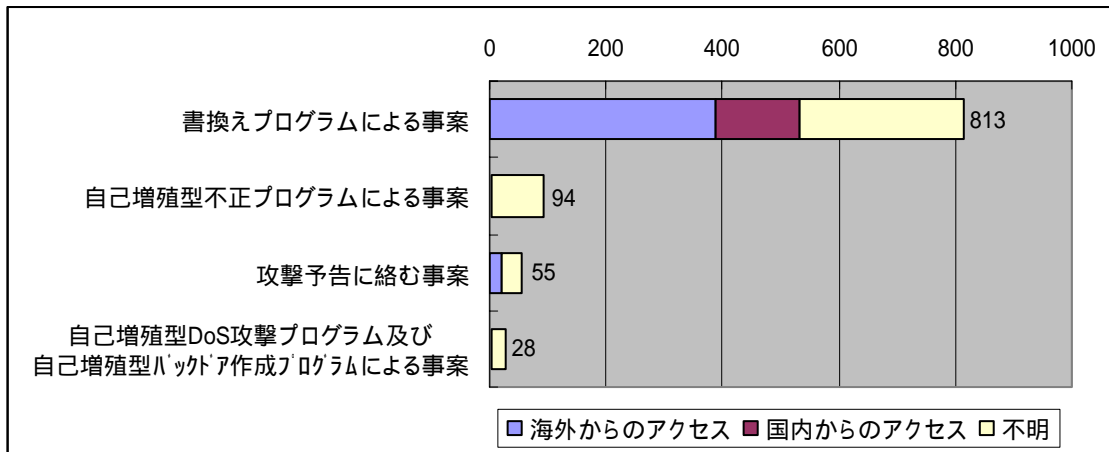


図 4-8 平成 13 年 (2001 年) に顕著だった不正アクセス行為事案 (警察庁資料より作成)

2000 年中の不正アクセス禁止法違反の検挙件数は 35 事件 (67 件)、検挙人員は 51 人で、前年に比べ検挙事件数は 4 事件増加し (検挙件数は変わらず)、検挙人員は 14 人増加した。内訳は、不正アクセス行為が 35 事件 (66 件)、51 人であり、不正アクセス助長行為が 1 事件 (1 件)、1 人であった。

不正アクセス行為の態様については、33 事件 (52 件) が識別符号窃用型 (不正アクセス禁止法第 3 条第 2 項第 1 号の他人の識別符号を無断で入力する行為) であり、3 事件 (14 件) がセキュリティホール攻撃型となっている。

なお、検挙人員 51 人中 49 人が成人であり、2 人が少年であったという。

表 4-1 平成 13 年 (2001 年) の不正アクセス禁止法違反事件の検挙状況 (警察庁資料より作成)

事犯別		平成 13 年	平成 12 年
不正アクセス行為	検挙事件数	35	30
	検挙件数	66	62
	検挙人員	51	34
不正アクセス助長行為	検挙事件数	1	4
	検挙件数	1	5
	検挙人員	1	5
計	検挙事件数	35 (重複 1)	31 (重複 3)
	検挙件数	67	67
	検挙人員	51 (重複 1)	37 (重複 2)

4.2.2 ウィルス

2001年にIPAへ届けられたウィルスは、24,261件となり、年間過去最多を記録した(図4-9)。この数字は、前年(2000年)の届出件数の2倍を超えるものである。

表4-2をみると、個人からの届出が著しく増加していることがわかる。

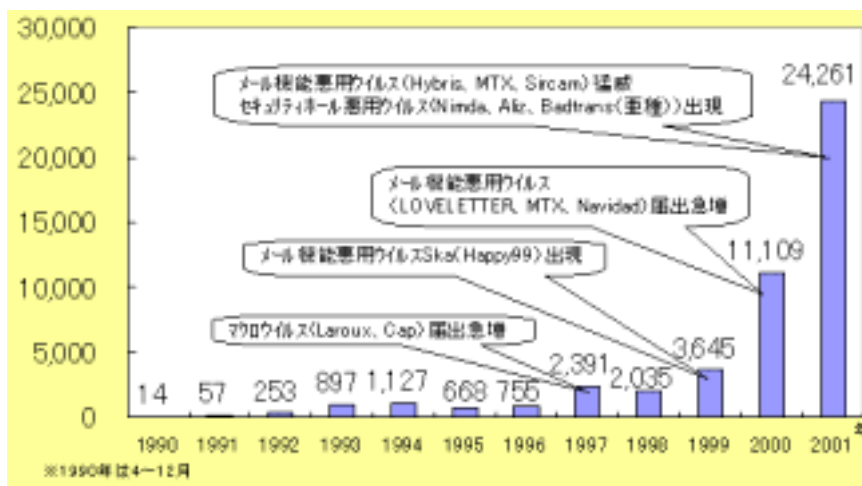


図 4-9 ウィルス届出件数の年別推移 (出典: IPA)

表 4-2 届出人別ウィルス届出件数 (2000年~2001年) (出典: IPA)

	2000年				2001年			
	届出件数		実害件数		届出件数		実害件数	
一般法人	9,975件	89.80%	1,480件	14.8%	17,332件	71.4%	2,793件	16.1%
個人	920件	8.30%	601件	65.3%	5,643件	23.3%	1,479件	26.2%
教育研究機関	214件	1.90%	101件	47.2%	1,286件	5.3%	404件	31.4%
合計	11,109件		2,182件(19.6%)		24,261件		4,676件(19.3%)	

以下に2001年におけるウィルス被害届出の傾向を示す。

- ・ 届出されたウィルスは112種類
- ・ 2001年に初めて届出されたウィルスは22種類(11,712件)
- ・ 2000年に引き続き、メール機能悪用ウィルスが多く届出、2001年は、W32/Aliz、W32/Badtrans(亜種)等、セキュリティホールを悪用して感染を拡げるタイプのウィルスの届出が急増(表4-3)

表 4-3 タイプ別ウイルス届出件数（2000年～2001年）（出典：IPA）

	2000年		2001年		代表的なウイルス
	件数	割合	件数	割合	
メール機能悪用ウイルス	6,692件	60.2%	14,263件	58.8%	Hybris、Sircam、MTX
セキュリティホール悪用ウイルス	507件	4.6%	6,338件	26.1%	Badtrans、Aliz、Nimda
マクロウイルス	3,393件	30.5%	2,812件	11.6%	Laroux、Divi
その他のウイルス	528件	4.7%	848件	3.5%	QAZ、Funlove
合計	11,120件		24,261件		

届出件数が急増する一方、実際に情報システムがウイルスに感染したケースは19%にとどまった（図4-10）。1998年の調査では、「感染被害あり」と回答した者が80%であったことから、企業や組織において、アンチウイルスソフトを導入するなど、適切なウイルス対策が実施されている状況がうかがえる。

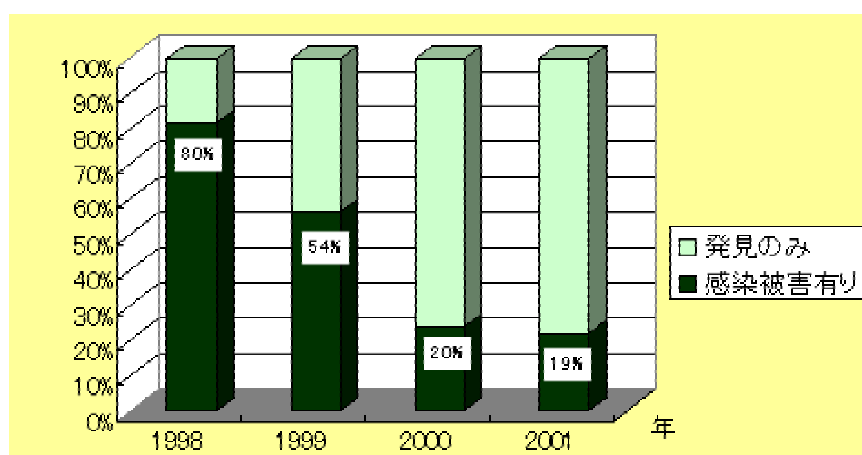


図 4-10 ウィルス感染被害の割合の推移（1998～2001）（出典：IPA）

4.3 情報システムのセキュリティに対する脅威の変化

4.1 に示したように、情報システムやネットワークの技術が飛躍的な進歩とそれを取り巻く環境の変化に伴い、脅威の技術的な性質やセキュリティ侵害の対象となる情報システムの種類が大きく変わってきた。

同時に、情報システムがわれわれの社会のより広範な分野に浸透してきたことによって、情報セキュリティに対する脅威が社会、生活、経済に及ぼす影響は拡大しつつある。

ここでは、情報システムのセキュリティに対する脅威の変化について、以下の2つの観点から分析する。

- ・ 技術の発展と脅威
- ・ 社会、生活、経済と脅威

4.3.1 技術の発展と脅威

この10年間における情報システムのセキュリティに対する脅威の変化には、インターネットの発展や情報システムに関する技術（ソフトウェア/ハードウェア）の進化が大きく寄与している。特に、WWW や電子メールをはじめとするインターネットの利用の拡大に伴い、インターネット関連技術のセキュリティホールを攻撃するインシデントが多発している。

また、インターネットに接続できる携帯電話、PHS や無線 LAN といった無線ネットワークが普及しており、今後脅威にさらされる危険が高まることが予想される。

以下に技術の発展からみられた脅威の変化について整理する。

(1) 攻撃方法の高度化

情報システムのセキュリティに対する脅威は、技術の発展に合わせて攻撃方法を高度化させ、その影響を拡大させてきた。特に近年、ウィルスやトロイの木馬をはじめとする不正プログラムは、インターネットに繋がった情報システムを攻撃対象にすると同時に、不正プログラムを流布させる媒介としてインターネットを悪用するケースが顕在化してきた。特に、以下のような傾向が顕著である。

(a) 攻撃ツールの自動化/高度化

攻撃ツールが、攻撃の準備を含め高度に自動化していることに加えて、扱い易い GUI (グラフィカルユーザインターフェース) を備えるものが増えてきている。

そのため、コンピュータやネットワークの技術に関してそれほど高い知識を持たない者も使用できるようになってきており、脅威の裾野が拡大しているといえる。

CERT/CC では、攻撃の高度化と攻撃を行うために必要な知識の関係について分析している。図 4-11 では、攻撃ツールが自動化され、扱い易くなることによって、より高度な攻撃が可能になると同時に、攻撃を実行するために必要となる知識はむしろ少なくなっている現状を示している。

Attack Sophistication vs. Required Intruder Knowledge

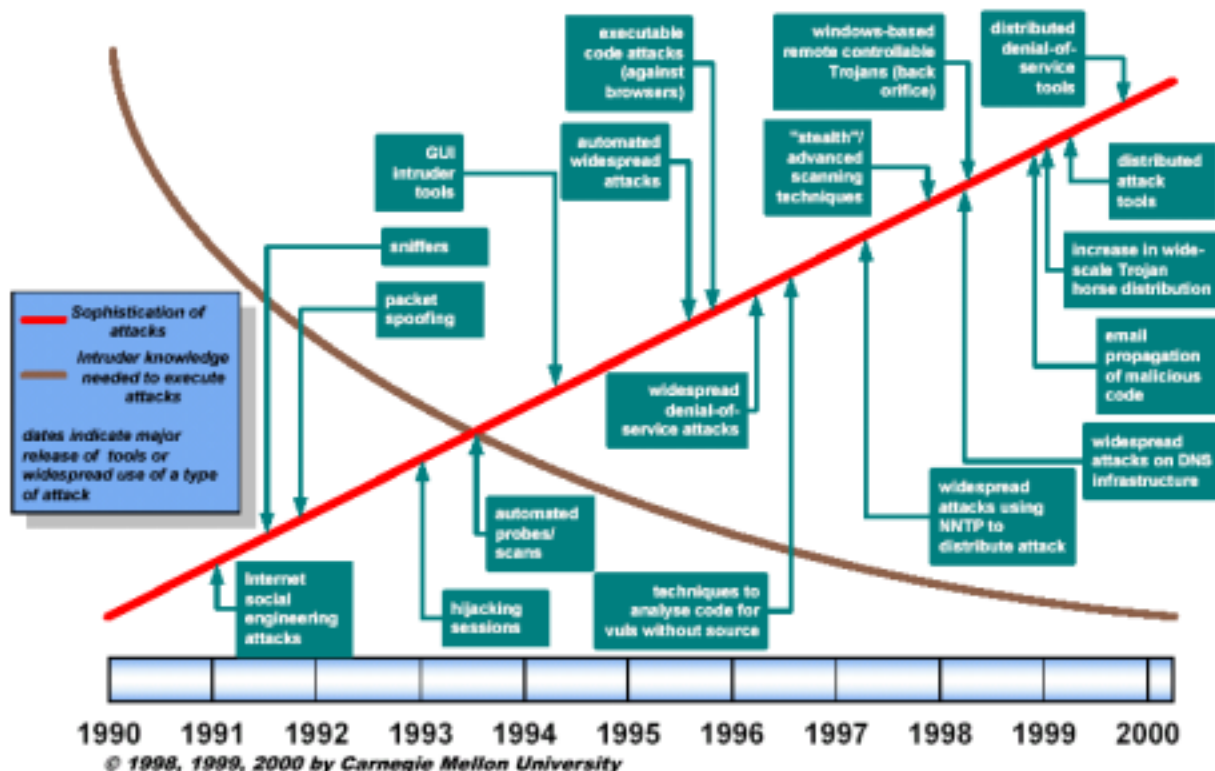


図 4-1-1 攻撃の高度化と必要となる知識（出典：CERT/CC）

また、この10年の間、コンピュータの処理速度が飛躍的に増加していると同時に、ネットワークの帯域幅も広がってきている。セキュリティ侵害の観点からみると、これらの攻撃ツールによって被る単位時間辺りの被害情報量は増加しているといえる。

(b) インターネットを媒介としたウィルスの流行

ウィルスの種類については、1986年の時点で確認されたウィルスは4種類であったのが、1990年代以降急速に増加している。米セキュリティソフト大手シマンテックによると、亜種を含めて毎日3種類以上のウィルスが作成されており、1カ月当たり平均では110もの新ウィルスの登場しているという。現在世界で確認されているウィルスの数は数千種類以上ともいわれる。

ウィルスの形態の傾向をみると、1990年後半よりeメールを媒介としたウィルスの急増が顕著である。ICSA Labsのウィルス発生状況に関するサーベイ2000年版によると、ウィルスの感染経路は、1998年頃よりそれまで主流であったディスクによる感染が減少するのと同時に、eメールによるものが急増している（図4-1-2）。

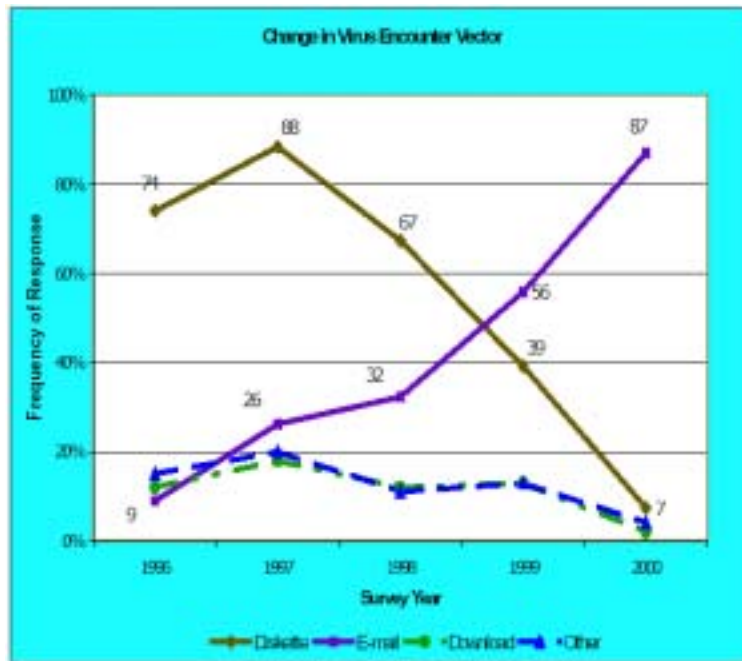


図 4-1 2 ウィルスの感染経路の変化(1996～2000年)

(出典：ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000)

上記 ICSA Labs サーベイによると、ウィルスの感染先からみたウィルスのタイプについては、1990 年代中頃より DOS ファイルやシステムのブートセクタに感染するものに代わって、Microsoft Word や Excel 文書のマクロに感染する「マクロウィルス」が急増している傾向が顕著になっている。

さらに 1990 年代末～2000 年代に入って、ウィルスはより巧妙な手口を使うようになっており、それに伴う被害の拡大も著しい。

2000 年 9 月から 10 月ごろにかけて発見された「Hybris ウィルス」は、インターネット上のニュースグループからプラグインをダウンロードして、ウィルス自身をアップデートする機能を持つ。このため、アンチウィルスソフトのパターンファイルの更新を少しでも怠ると、ウィルスを検出できない可能性がある。

2001 年 7 月に発見された「Code Red ワーム」は、マイクロソフト社の Internet Information Server (IIS) の脆弱性を利用するワームである。猛烈な勢いで感染する点が特徴で、9 時間で 25 万台のサーバが感染したという報告もある。Code Red は、感染した Web サーバのホームページを書き換えたり、米国ホワイトハウスに DDoS 攻撃を仕掛けたりする。感染力を強化した亜種も報告されている。

2001 年 9 月に猛威をふるった「W32/Nimda ウィルス」は、複数の感染手法を使うことで、国内においても被害が一気に拡大した。Nimda は、(1) 電子メール経由、(2) クライアントから Web サーバ (3) Web サーバからクライアント、(4) 共有ネットワーク (SMB) 経由、(5) Nimda に感染した実行ファイルの交換 - で感染を広げる。公開 Web サーバが感染した場合、サーバ上の HTML 文書が、ウィルスをダウンロードするように改ざんされるため、ブラウザによっては、HTML 文書を

表示させただけで自動的にそのウィルスを実行してしてしまう場合がある。

また近年、VBScript や Java Script 等のスクリプト言語を悪用した不正プログラムである「スクリプトウィルス」によるインシデントも顕在化している。スクリプトウィルスの特徴は、比較的プログラミングが簡単であり、そのため亜種の作成が容易である点あげられる。2000 年 5 月に発見された「ラブレッターウィルス (VBS_LOVELETTER)」では、短時間の間に複数の亜種が出回り、被害を拡大させる原因となった。

(c) DDoS (Distributed Denial of Service) 攻撃による被害の拡大

コンピュータによって提供されるサービスを妨害する攻撃である DoS 攻撃の一種に、インターネットプロトコルの特性を攻略して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを停止させてしまう攻撃がある。DDoS (Distributed Denial of Service : 分散サービス妨害) 攻撃は、このような DoS 攻撃を複数のホストから一斉に実行するものであり、標的とされるコンピュータにかけられる負荷はより大きなものとなる (図 4-13)。

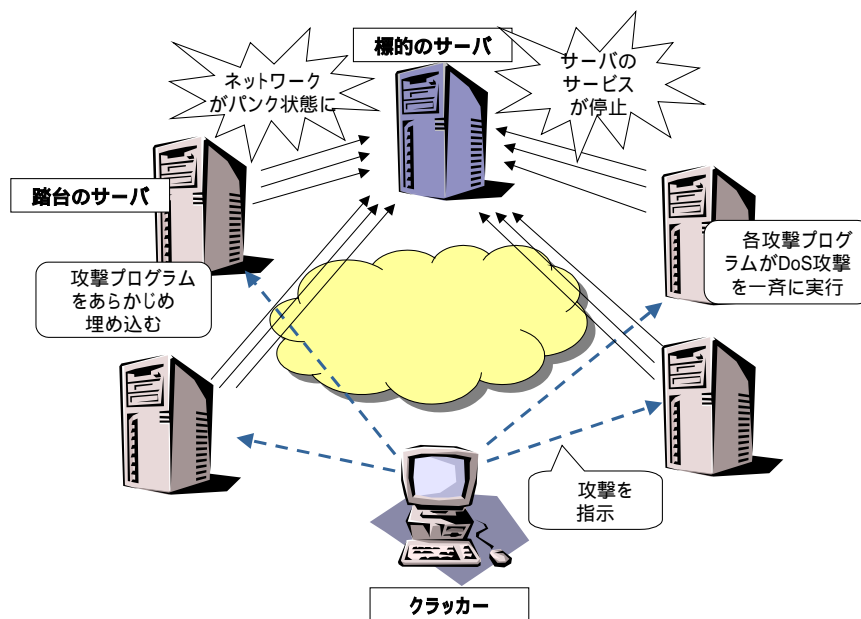


図 4-13 DDoS 攻撃の仕組み

(日経インターネットテクノロジー資料等をもとに作成)

近年、この DDoS 攻撃によるインシデントが多発しており、2000 年 2 月には Yahoo!、eBay、Amazon.com といった米国の著名ポータルサイトが次々と DDoS 攻撃を受け、各サイトは一時的にサービス停止に追い込まれた。米アスタ・ネットワークスが 2001 年 5 月に公開した調査結果によると、調査を行った 3 週間に世界中で発生した DDoS 攻撃は 1 万 2000 件以上。週平均で 4000 件以上も被害が発生しているという。

DDoS 攻撃では、攻撃元が攻撃者自身とは限らず、攻撃者（クラッカー）が事前に標的以外の複数サイトに、攻撃プログラムを仕掛けておいて、遠隔から攻撃を仕掛ける操作を行う場合もある。この場合、元々の攻撃者の所在を追跡するのが難しくなる。

(d) Web 関連技術を対象とした脅威の出現

Web の利用の拡大に伴い、Web 関連技術のセキュリティホールを突く不正プログラムの脅威が顕在化しつつある。

2001 年夏には、ユーザが特定のホームページを見た後、悪意ある Java スクリプトの実行によって、PC が立ち上がらなくなる被害情報が報告されている。これは、Java VM（バーチャルマシン）の実装の脆弱性を突いたものであり、Windows において、アプリケーションの起動、設定変更、システムの終了が出来なくなるといった現象を引き起こす。利用者の多いオークションサイトに仕掛けられたため、被害が拡大した。

また、現在稼働中の多く Web サービス（ショッピングサイト、インターネットバンキングなど）における「クロスサイトスクリプティング」と呼ばれる脆弱性が指摘されている。クロスサイトスクリプティングとは、Web サイトでのデータ・チェックが不十分なため、不正なスクリプトをユーザの Web ブラウザに送信してしまうという問題である。これにより、悪意ある第三者に、ユーザの Cookie 情報を読み取られてしまう場合がある。

独立行政法人 産業技術総合研究所の研究グループが 2001 年 10 月に発表した報告によると、大手の銀行および証券サイトから 23 サイトを抽出して調査した結果、少なくとも 21 サイト（91%）がクロスサイトスクリプティング対策を実施していなかったという。経済産業省は 2001 年 10 月、多数の EC サイトなどにセキュリティ上の問題が指摘されているとして、関係団体へ対応を要請している。

(2) 脅威の対象の拡大

インターネットに接続する携帯電話や PHS を含め情報システムの利用場面が拡大するにつれて、脅威の対象が拡大している。また、P-to-P（Peer-to-Peer）プログラムや情報家電、ホームネットワークといった先進の技術が、今後脅威の対象になることも懸念されている。

特に、以下にあげるような対象へと脅威が拡大することが指摘されている。

(a) 無線 LAN

オフィスや家庭などで無線 LAN を利用するケースが増えており、世界の無線 LAN 市場全体では、2000 年には 330 万だった出荷台数が 2005 年には 2360 万まで成長すると見られている（データリソース社調査）。

無線 LAN の規格である 802.11b とその暗号プロトコルである WEP（Wired Equivalent Privacy）にいくつかの脆弱性が指摘されている。場合によっては、第

三者が建物の外から企業内 LAN を盗聴することも可能という。

(b) 携帯電話 / PHS

携帯電話や PHS がインターネットに接続されるようになってきていることから、これらの機器を対象としたウイルスやワームをはじめとする不正プログラムの危険性が指摘されている。平成 13 年度版 情報通信白書によると、携帯電話や PHS からインターネットにアクセスするユーザは 2,364 万人となっており、数年の間に急激な伸びをみせている。

現時点で、我が国のインターネット接続携帯電話や PHS を標的にしたウイルスはまだ報告されていないが、スペインでは、携帯電話のいわゆるショートメッセージサービス(SMS)を利用して感染するワームが発見されている。

また、シマンテックの AntiVirus Research Center の報告によると、無線デバイスの通信プロトコルである WAP (Wireless Application Protocol) に関して、現時点ではウイルスや不正プログラムを実行する可能性は低いものの、技術の進化の方向から潜在的な脅威はむしろ高まっていることが指摘されている。

携帯電話や PHS を含む無線デバイスからのインターネット接続は、世界に先駆けて我が国が先行しているが、他の国や地域でも普及しつつあることから、今後ウイルスやトロイの木馬などの不正プログラムが登場し、攻撃の対象となる危険性は高い。

(c) インスタントメッセージング

「インスタントメッセージング」とは、オンライン上のユーザ同士で、メッセージのやりとりやチャット、ファイルの送受信などの機能を実行するメッセージ交換サービスである。簡便なコミュニケーションツールとして、一般ユーザのみならず、企業内でも利用されるようになってきた。調査会社ジュピターメディアメトリクスによると、国内のインスタントメッセージングのユニークユーザは、2001 年 4 月時点での 321.7 万人となっており、インターネット利用人口の約 6 人に 1 人が使用していることになるという。

2001 年 12 月に発見された「W32.Goner (別名: PENTAGONE)」ウイルスは、広く利用されているインスタントメッセージングソフトである ICQ のファイル転送機能を利用して感染する。他にも MSN Messenger を介しての感染を行う「Choke」といったウイルスも報告されている。

現在ウイルスの感染経路は e メールによるものが最も多くなっているが(図 4-12)、今後、インスタントメッセージングを含めウイルスの感染経路が拡大することが懸念される。

(d) P-to-P プログラム

P-to-P (Peer-to-Peer) プログラムは、ファイル共有プログラムとも呼ばれ、デジタル音楽ファイルの交換を行う Napster や Gnutella などの登場により注目を集め

た。P-to-P プログラムでは、ユーザの PC のハードディスクや CPU をネットワーク上で共有することが可能になり、分散コンピューティングの新形態として期待されている。

その一方で、P-to-P プログラムにおいては、トロイの木馬などの悪意あるソフトウェアに対して、プログラムの性質上脆弱であることが指摘されている。既に、一部のファイル共有プログラムに感染し、ユーザのコンピュータから個人情報を収集して転送するトロイの木馬が報告されている。

(d) 情報家電

家庭内の電化製品を家庭内ネットワーク（ホームネットワーク）で結び、さらにインターネットなど外部のネットワークと接続する「情報家電」が注目されている。例えば、外出先から携帯電話ビデオの録画を予約したり、電子レンジがインターネット上のサイトから、レシピや調理方法に関するデータをダウンロードしたりすることが可能になる。

このような情報家電では、誰もが安心して利用できるような環境を提供することが重要である。悪意ある者がこれらの機器を不正に操作し、火災や事故等を引き起こすことも懸念される。それゆえ、通常のコンピュータネットワークと同様あるいはそれ以上のセキュリティ対策が必要となる。

(3) セキュリティリスクを拡大させる要因の変化

情報システムの技術の進化と適用領域の拡大が、セキュリティに対する脅威をより深刻なものとしていることに加え、情報システムを取り巻く環境の変化が脅威を直接的、間接的に増長させる要因にもなっている。

セキュリティリスクの拡大につながるとして、近年その危険性が顕著になりつつあると指摘されている要因には、以下のようなものがある。

(a) デフォルトインストールと脆弱性

米 SANS (System Administration, Networking, and Security) 研究所と米国家インフラ保護センター (NIPC) は 2001 年 10 月、「The Twenty Most Critical Internet Security Vulnerabilities (もっとも危険なインターネットセキュリティの脆弱性 20)」と題したリストを公開している。同リストは、コンピュータシステムの脆弱性を危険度が高い順から記述したものであり、もっとも危険とされたのが「デフォルトインストール」となっている。

OS やアプリケーションをインストールする際、作業を軽減するため、ベンダから提供されるインストールプログラムを利用することがある。このとき、既定の設定のままインストールすると、不要な機能がインストールされてしまう。

この場合、ユーザは自分の使っていない機能に対して、セキュリティパッチを含むメンテナンスの手間を嫌う傾向があることに加え、実際に何がインストールされたか把握できずに、セキュリティホールが残ってしまう危険がある。攻撃者は、こ

これらの脆弱性を熟知しており、効果的で広範に利用可能なツールを使って攻撃を成功させている。SANS 研究所と NIPC は、インストール時に不要なサービスやソフトウェアの削除を含め問題箇所を修正しない限り、インターネット上で脆弱なシステムを走査して仕掛けられる無差別攻撃に頻繁にさらされることになる、と警告している。

デフォルトインストールの問題と同じく、発見された脆弱性に対してセキュリティパッチを当てるなどのセキュリティ対応の実施も重要である。被害に遭わないため、また、被害の拡大を招かないためにも、迅速かつ継続的に行うことが求められる。

しかしながら、各種の調査の結果を見ると、企業や組織の対応は遅れ気味である現状がうかがえる。日経インターネットテクノロジーの調査によると、外部 Web サーバのソフトウェアにセキュリティパッチを「提供され次第あてている」と答えた企業は 30.9%に過ぎなかった。また、「いくつかまとめてあてている」17.7%、「ときどきあてている」15.6%となっている。一方、「ほとんどあてていない」9.9%、「まったくあてていない」9.9%となっており、約 20%の企業でセキュリティパッチ適用されていない状況である（図 4-14）。

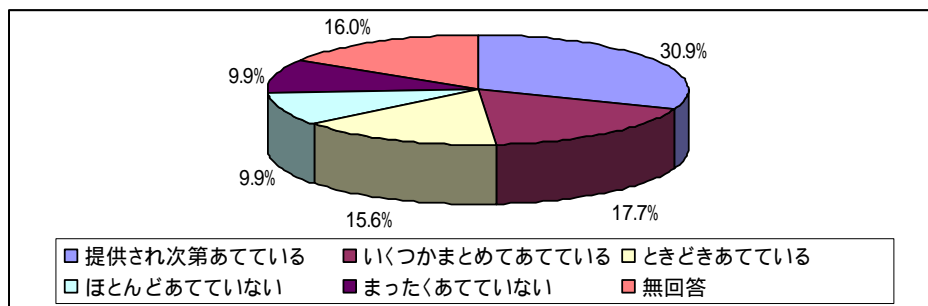


図 4-14 企業における外部公開の Web サーバへのセキュリティパッチの適用状況

（出典：日経インターネットテクノロジー「企業のインターネット利用状況調査」2001年）

（b）インターネットを媒介とした攻撃ツールや関連する情報の流布

攻撃のためのツールや不正プログラム等は、インターネット上のサイトで簡単に手に入れられることが指摘されている。加えて、このようなツールの使った劇の方法や、脆弱性のある情報システムや Web サイトの情報についても、ハッカーやクラッカーのあいだで交換されているという。

上記のツールや情報がネット上で簡単に得られる状況は、好奇心を持つ者をセキュリティ侵害行為に駆り立てる一つの要因にもなっている。最近の甚大な被害をもたらしたインシデントが若年者によって行われたということも、この傾向とつながりがあると考えられる。前述の米国著名 Web サイトの DDoS 攻撃は、「マフィアボーイ」を名乗るカナダの 15 歳の少年によるものとされている。

しかし、その一方で、これらのツールや情報は、防御する側がセキュリティを検

証する際などにも有用な場合があり、完全に排除するべきかについては議論がある点考慮すべきである。

(c) ソフトウェア開発の産業構造と脅威

情報システムに対する脅威を増長するその他の要因として、情報システム開発産業やソフトウェア開発産業の産業構造がある。

情報システムの開発を受注した会社が、他の会社に再委託、再々委託する場合も多い。2000年2月に、オウム真理教(アレフに改称)関連のコンピュータソフト開発会社が、防衛庁などの6つの官公庁や大手企業約80社にソフトを納入していたことが、警視庁公安部の調べで判明した。このうち防衛庁には、全国10カ所の陸上自衛隊駐屯地のコンピュータネットワークを接続するためのシステムを納入した。ネットワークには不正アクセスを防ぐファイアウォール(防護壁)が設けられていたが、教団関連のソフト開発会社はソフト納入の際、正規のアクセス方法を把握しており、サーバに侵入される可能性もあった。他にも、ソフトウェア開発の国際分業化が進んでいることも、脅威の拡大につながる危険性として指摘されている。

4.3.2 社会、生活、経済と脅威

10年前と比較して、PCの普及やインターネットの進展など、我々が情報システムと直接的、間接的に触れる機会が多くなってきた。また、ビジネスの現場においても、電子メールやWWWは欠かせないツールとして定着している。

サイバーワールドの社会的、経済的重要性が増すにつれ、ネット上の脅威が我々の社会、生活、経済に深刻な影響を及ぼすようになってきている。特に最近、政治目的によるWebサイトへのサイバー攻撃の発生や、インターネットを悪用した犯罪の増加など、情報ネットワーク化社会の負の面を強調する出来事が相次いでいる。

さらに、現代社会の基盤である情報通信、金融、航空、鉄道、電気、ガス、政府・行政サービス（地方公共団体を含む）といった「重要インフラ分野」における情報システムの保護は、我が国を含む各国共通の課題となっている。

以下に社会、生活、経済に影響を与える脅威の変化について整理する。

(1) Webサイトを標的とするサイバー攻撃の発生

近年、政治的な目的から政府関連機関等のWebサイトを書き換えたり、DoS攻撃を行う「サイバー攻撃」のインシデントが増加している。これらのサイバー攻撃は、政治的なメッセージ性を協調して「サイバープロテスト」と呼ぶこともある。

1999年のコソボ紛争の時には、米国政府内の部門や機関のWebサイトが書き換えられ、停止に追い込まれた。損害は致命的、恒久的なものではなかったが、サイバー攻撃が米国のシステムに及ぼす影響の大きさを示すことになった。また、我が国においても、2000年1月から2月にかけて多数の中央省庁系のサイトが不正侵入および改ざんの被害を受けている。

NIPC（National Infrastructure Protection Center：全米インフラ防衛センター）の調査報告によると、政治目的のサイバー攻撃（サイバープロテスト）はより組織化され、洗練された方法で攻撃を試みる傾向が顕著となっている。

また、政治的な緊張下にある国や地域の人あるいは組織が、サイバー攻撃の応酬をする事態に発展するケースも少なくない。最近では、2001年9月11日の多発テロ以降、親米派／反米派双方が相手国の政府や企業のWebサイトの書き換えを企て、多くの被害をもたらしている。

NIPCの報告は、これらの書き換え行為自体の被害はそれほど大きくないものの、政府機関や重要インフラ分野の企業がより深刻な攻撃を受ける危険性は、むしろ増加しつつあると警告している。

(2) 電子商取引とトラブルの増加

インターネット上の電子商取引の利用が一般利用者の間に広まるにつれて、トラブルも急増している。これらのトラブルの中には、情報システムのセキュリティと直接的には関係のないものも少なくないが、電子商取引の健全な発展に影響を与える問題といえる。

国民生活センターに寄せられたインターネット関連の苦情件数は、平成8年から11

年の間に 10 倍以上に増加した。特に、インターネットオークションにおける詐欺の増加やマルチまがい商法等が目立っている。また、特に、勧誘目的の迷惑メールは、電子メールを送受信できる携帯電話や PHS が増加に伴い、社会問題としてクローズアップされている。

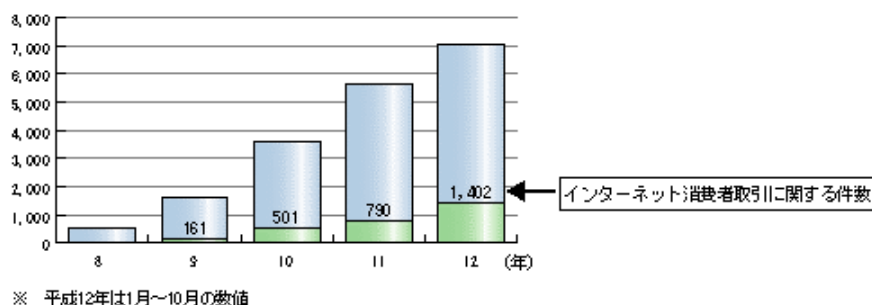


図 4-15 インターネット関連の苦情件数の推移

(出典：国民生活センター資料)

また、全米消費者連盟 (National Consumers League : NCL) は 2001 年 11 月、同団体のインターネット詐欺監視組織「Internet Fraud Watch」(IFW) に寄せられた詐欺被害をまとめた。2001 年 1-10 月の被害総額は 430 万ドル、1 人当たりの平均被害額が 636 ドルに達したという。昨年 1 年間の被害総額は 330 万ドル、1 人当たりの平均被害額は 427 ドルで、今年 10 カ月間だけで既に前年を上回っている。

消費者のオンラインでのプライバシーやセキュリティに対する懸念は依然根強い。調査会社の米ジュピターによると、一般消費者の 60% が、セキュリティに対する不安のためにインターネット・ショッピングをしたことがないという。また、ギャロップ社の調査によると、60% のアメリカ人は法的な文書や税金の申告に関する情報、電話番号情報にいたるまでインターネット上で漏洩することを心配している。

(3) 増加するハイテク犯罪とその傾向

「ハイテク犯罪」は、コンピュータ技術及び電気通信技術を悪用した犯罪と定義される。匿名性の高さや国境を超えることが容易な点がハイテク犯罪の特徴であり、この特徴ゆえ、捜査が難しくなる場合も多い。

また、インターネットを悪用した犯罪のもう一つの特徴は、被害者の人数や被害額が拡大しやすい点である。米証券取引委員会 (Securities and Exchange Commission : SEC) は 2002 年 1 月、100 万ドルの投資詐欺を行ったとして 17 歳の高校生を摘発した。SEC は、このような犯罪がインターネットにより高校生でも容易に行えるようになった点を指摘している。

近年我が国においても、個人や企業などがハイテク犯罪に巻き込まれるケースが多発している。警察庁によると、平成 13 年度中のハイテク犯罪の検挙件数は 810 件であり、前年(559 件)と比較して 45% 増加している (表 4-4)。

表 4-4 ハイテク犯罪の検挙件数（平成 13 年）

	平成 13 年	平成 12 年	増 減
コンピュータ、電磁的記録対象犯罪	63 件	44 件	19 件
電子計算機使用詐欺	48 件	33 件	15 件
電磁的記録不正作出・毀棄	11 件	9 件	2 件
電子計算機損壊等業務妨害	4 件	2 件	2 件
ネットワーク利用犯罪	712 件	484 件	228 件
児童買春・児童ポルノ法違反	245 件	121 件	124 件
わいせつ物頒布等	103 件	154 件	51 件
詐欺	103 件	53 件	50 件
名誉毀損	42 件	30 件	12 件
脅迫	40 件	17 件	23 件
著作権法違反	28 件	29 件	1 件
その他	151 件	80 件	71 件
不正アクセス禁止法違反	35 件	31 件	4 件
合 計	810 件	559 件	251

（出典：警察庁資料）

また、インターネットが犯罪のきっかけとなるケースも急増している。警察庁生活安全企画課のまとめによると、インターネット上で男女間の出会いの場を提供する「出会い系サイト」がきっかけになった事件が 2001 年上半期（1～6 月）だけで、前年 1 年間の 104 件より約 3 倍増の 302 件に上ったとされている。

その他には、インターネットがテロリストの犯行の連絡に利用されたとする調査報告もある。

4.4 情報セキュリティ対策コストとセキュリティ関連製品/サービスの市場規模

企業や組織におけるセキュリティ対策の現状に関して、インシデントの発生とその被害額、および情報セキュリティ対策コストについて整理する。また、セキュリティ関連の製品やサービスの市場規模に関する各種の調査結果から、企業や組織のセキュリティ対策の動向について分析する。

4.4.1 企業や組織におけるインシデントの発生と被害

(1) インシデントの経験

4.2にみたように、ブロードバンドの普及に伴う個人ユーザのインターネット利用の急増を背景として、2001年のIPAへのウィルスおよび不正アクセスの届出件数は、ウィルス、不正アクセスともに過去最多を記録している。

企業を対象とした調査では、日経インターネットテクノロジーが2001年11月に国内の主要企業(回答:1,053社)におけるインターネットの利用状況調査を行っている。調査結果によると、今までに社内のコンピュータがウィルス(あるいはワーム)に感染した経験は77.9%、また、不正アクセスを受けた経験のある企業は38.3%となっている。また、上記調査では、不正アクセスやウィルス害を受けた企業のうち、「JPCERT/CCあるいはIPAに報告した」と回答した企業は2割に満たない。実際に起きているインシデントの数は、JPCERT/CCやIPAといった緊急対応機関に報告されている件数より大幅に多いものとみられる。

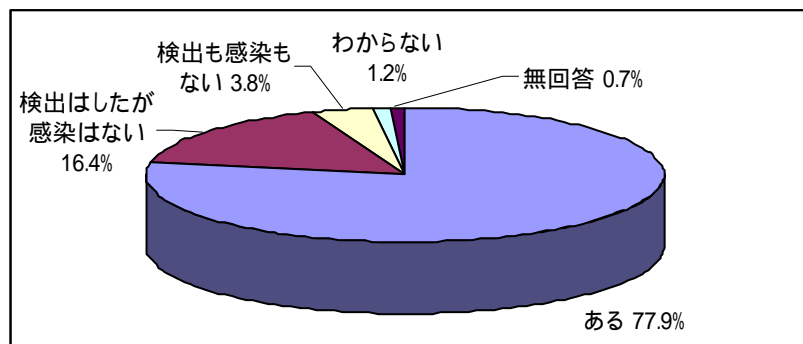


図 4-16 企業のウィルス被害の経験 (出典:日経インターネットテクノロジー資料)

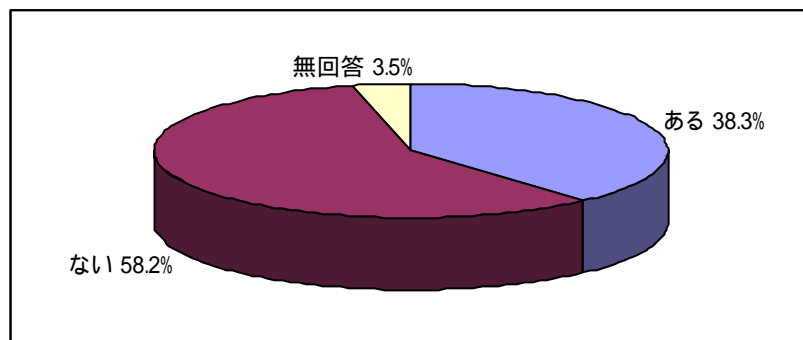


図 4-17 企業の不正アクセスの経験 (出典:日経インターネットテクノロジー資料)

(2) 企業におけるセキュリティ侵害による被害額

各種の調査によると、インターネットを利用している企業の間では、セキュリティ技術を増強しているにもかかわらず、侵入行為やサイバー犯罪の被害が増加している。セキュリティ侵害による被害額を正確に測ることは難しいが、これらの調査は脅威の傾向を把握するのに役立つ。

米 CSI (Computer Security Institute) と FBI による「The 2001 Computer Crime and Security Survey」によると、2001 年の被害額を算定した 186 企業で、各種サイバー犯罪による損失額の合計が 3 億 7800 万ドルにのぼった。1 社あたりの平均被害額をみると約 200 万ドルとなっており、249 社が回答した 2000 年の調査結果の約 2 倍に跳ね上がっている。図 4-18 に被害の経験の割合及びその被害額をタイプ別に示す (回答数は、「被害の経験」: 483、「被害額」: 186)。被害額の多い順にみると「企業秘密の盗難」が被害額の全体 (378M\$) の半分を占め、以下「金融詐欺」「ウイルス」「内部のネット悪用」と続いている。図 4-18 をみると、ウイルスや外部からのハッキング行為は、被害の経験の割合に比べて被害額は小さく、逆に機密情報漏洩や金融詐欺行為は、被害数は少ないものの被害額は深刻であることがわかる。

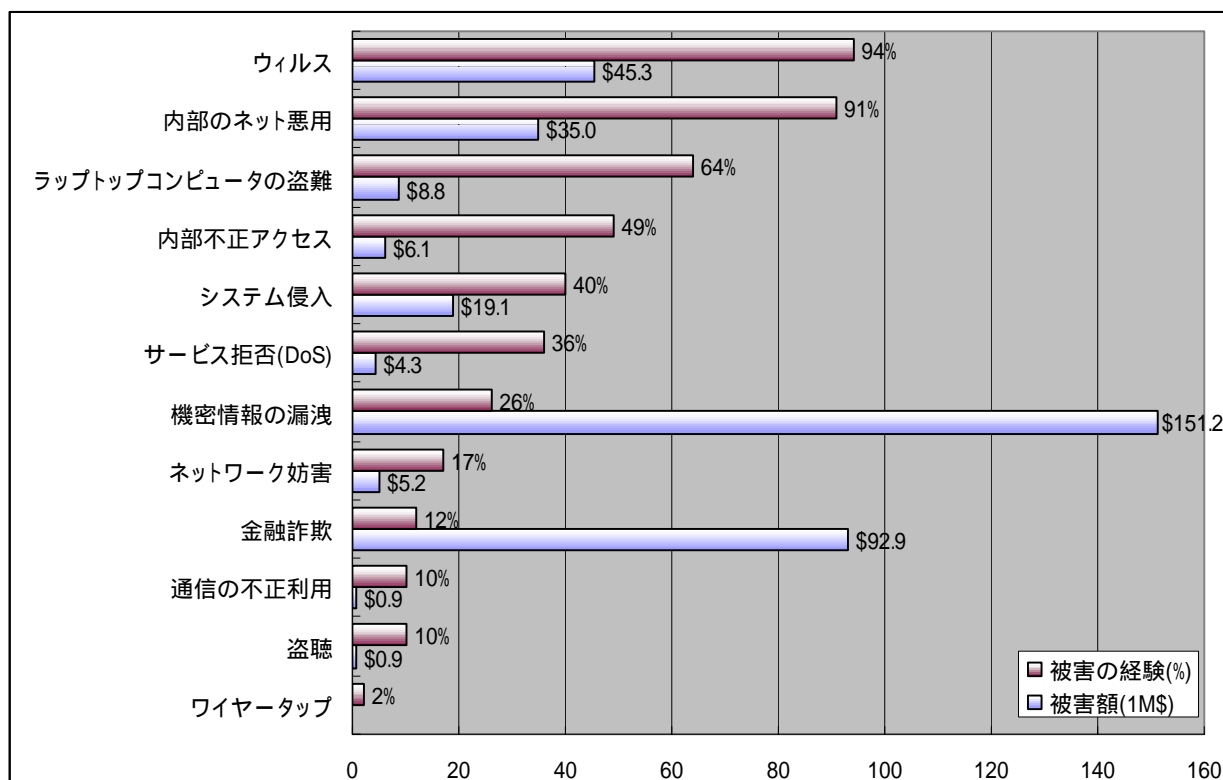


図 4-18 米国企業におけるセキュリティ侵害による被害の経験と被害額

(CSI/FBI The 2001 Computer Crime and Security Survey をもとに作成)

また、上記調査では、インターネットからの攻撃を受けた組織は、1996 年の調査時の 38% から 2001 年には 70% へと増加しており、企業や組織におけるインターネット

につながった情報システムの弱点が顕在化していることを指摘している。

米調査会社コンピュータエコノミクスでは、悪意あるコードが全世界の経済に与えたインパクトに関する統計を発表している。同調査によると、2001年にもっとも被害額の大きかったのは「コード・レッド」の26億2000万ドル。「サーカム」が11億5000万ドル、「ニムダ」が6億3500万ドルとなっている。また、ここ数年間でもっとも被害額の大きかったのは、「I love you (Love Bug)」の87億5000万ドルであったとしている(表4-5)。

表 4-5 ウィルスによる被害額

年	コードの名称	被害額 (\$U.S.)
2001	Nimda	\$635 Million
2001	Code Red(s)	\$2.62 Billion
2001	SirCam	\$1.15 Billion
2000	Love Bug	\$8.75 Billion
1999	Melissa	\$1.10 Billion
1999	Explorer	\$1.02 Billion

(米コンピュータエコノミクス資料をもとに作成)

4.4.2 組織におけるセキュリティ対策とそのコスト

(1) 組織におけるセキュリティ対策

日本ベリサインが2000年に実施した「ネットワーク・セキュリティに関する意識調査」によると、70%がセキュリティに不安を感じていながらもセキュリティ専任者のいる企業はまだ50%程度となっているなど、セキュリティ対策のための体制が整っていない企業も多い。

同調査によると、セキュリティの被害を防ぐために企業がとっている対策では、「ウィルス対策ソフトの導入」(81.1%)と「ファイアウォールの設置」(59.6%)の割合が高い。「SSLによるサーバ認証」などその他の対策は2割を切り、「盗聴」「改ざん」「なりすまし」「否認防止」など高度な通信・商取引に欠かせない対策の実施については低い結果となっている(図4-19)。

ネットワークセキュリティに関して専任の管理者を設置している企業は5割弱で、セキュリティポリシーを設定している企業は4割となっている。また企業規模が大きくなるにつれてセキュリティ管理者設置の割合が高くなる傾向がみられる。

また、サーバ認証の導入率については、金融・保険関連業の実施率が高く、公共団体で対策が遅れがみられると分析している。「SSLによるサーバ認証」で分析すると、既の実施しているという回答は「金融・保険・不動産関連」(25%)「コンピュータ関連製造」(18%)、「電力・ガス・運輸」(16.7%)、「ソフトウェアハウス、SI」(15.6%)「機械製造」(12.2%)「通信サービス」(11.7%)。一方、「教育、医療、官公庁、団体」は実施率が8%を切るという結果が出ており、民間に比べ、ウェブサイトのセキュリティなど基本的なセキュリティ対策が遅れていることがうかがえる。

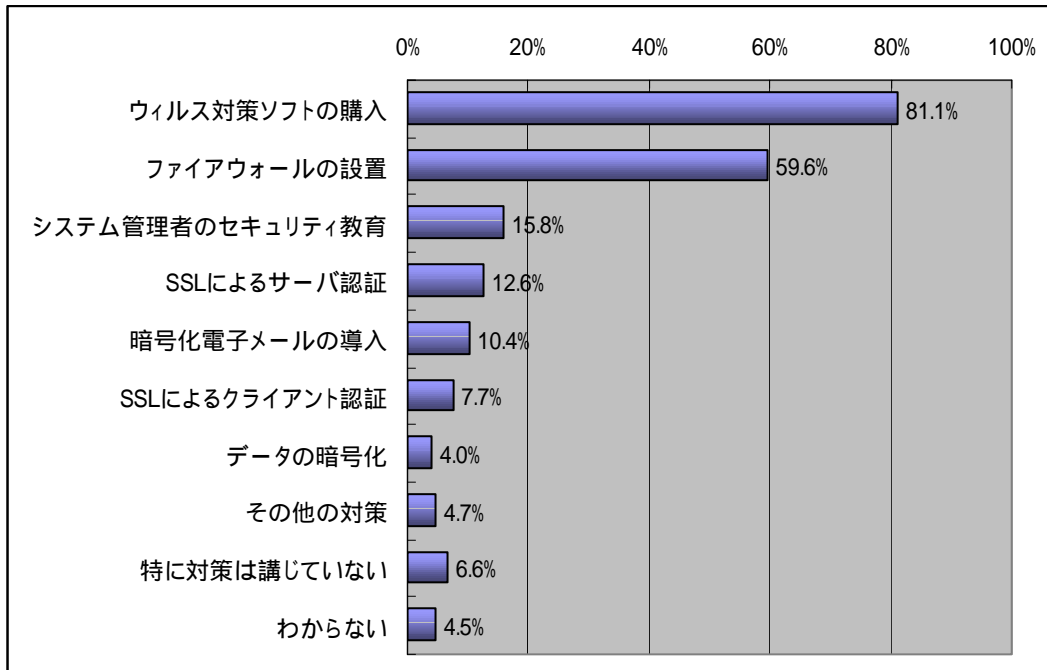


図 4-19 組織におけるセキュリティ対策の状況

(出典：日本ベリサイン「ネットワーク・セキュリティに関する意識調査」)

(2) 企業におけるセキュリティ投資

米国を中心にテロリストやその他のセキュリティへの脅威から情報システムを保護する機運が高まっており、企業におけるセキュリティ投資も今後数年間で大幅に伸びる見通しである。

米調査会社ガートナーの調査によると、現在米国企業が IT 関連のセキュリティに充てている費用（件費、ハードウェア、ソフトウェア、外部委託サービス費、社内におけるセキュリティ管理費を含む）は、平均して売上高の 0.4% となっている。同調査によると、10 年後の 2011 年にはこの割合は、売上高の約 4% 程度にまで高まると予測している。

米 RBC Capital Markets の調査によると、2005 年には世界中の企業や政府機関が情報セキュリティに 300 億ドルを投資するようになるという。2000 年はネットワークでの機密漏洩、ウィルス、クラッカー（悪意のあるハッカー）による損害額が 150 億ドルに及び、企業と政府機関をあわせた情報セキュリティ費用は合計 100 億ドル程度であったとしている。また、同調査によると、2001 年 9 月の米国多発テロ以降、企業や政府機関では、予算項目における情報セキュリティの優先順位を軒並み引き上げている状況がみられる。

国内企業を対象としたものとしては、(財)インターネット協会が Networld+Interop の来場者を対象とした調査を行っている。2001 年に実施した調査によると、企業のセキュリティ関連製品予算の平均は 2,500 万円強。内訳は、「災害復旧/メディア防御」(852.1 万円)、「アクセス制御/個人認証」(505.2 万円)、「イ

「インターネット/ネットワークセキュリティ」(335.0万円)の順番となっている(図4-20)。

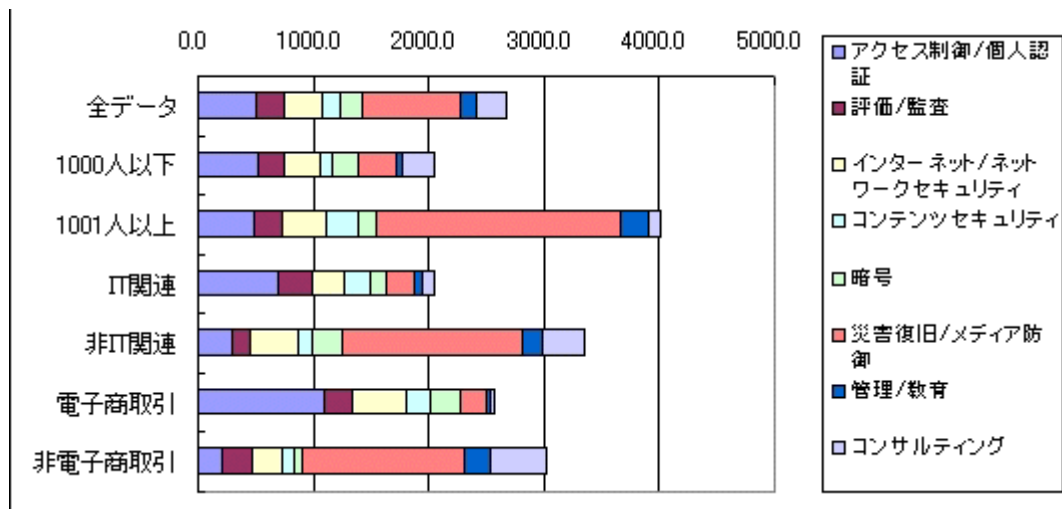


図 4-20 セキュリティ製品予算平均 (単位: 万円)

(出典: インターネット協会 セキュリティサーベイ報告書)

4.4.3 情報セキュリティビジネスマーケット動向

企業のセキュリティ対策が今後本格化する傾向は、情報セキュリティビジネスマーケット動向の予測調査の結果からも裏付けられる。

情報処理振興事業協会 (IPA) が 2001 年 3 月にまとめた「情報セキュリティビジネスに関する調査報告」によると、1999 年の日本の情報セキュリティ市場は、製品市場が 235 億円、サービス市場が 291 億円、合計 526 億円と推計されるという。5 年後の 2004 年にはそれぞれ市場は順調に拡大し、製品市場が 858 億円、サービス市場が 1,136 億円の合計 1,994 億円になると予測している。

アンチウィルスソフトやファイアウォールをはじめとするセキュリティ製品は、軍の需要が大きい米国やイスラエルの企業の製品が世界市場の大半を占めている。

IPA の上記調査によると、1999 年の米国の情報セキュリティ市場は、製品市場が 2,069 百万ドル、サービス市場が 2,509 百万ドル、合計 4,578 百万ドルと推計される。5 年後の 2004 年には、製品市場が 5,328 百万ドル、サービス市場が 7,351 百万ドルの合計 12,679 百万ドルになると予測している。

4.5 情報セキュリティにおける課題

情報システムの利用者の増加と利用場面の拡大に伴い、脅威が増大している。情報セキュリティにおける課題としては、以下のような項目の重要性が高まっているといえる。

(1) セキュリティに対する意識の向上

セキュリティに関する教育、訓練から経営層トップの啓発まで、一貫したセキュリテ

ィに対する社会の意識の向上が急務である。

初等中等教育においては、教育の情報化が国のイニシアチブのもと進められているが、情報のリテラシのみならず、セキュリティやプライバシーの保護の方法及びルールやマナーといった倫理面の教育も不可欠となる。また、高等教育機関においては、セキュリティ保護技術の研究開発とともに、専門家の育成が重要になる。

一方、企業のセキュリティ担当者の多くは、経営層の理解が得られないためにセキュリティ対策が不十分になっていることを指摘している。前述の「The 2001 Computer Crime and Security Survey」(CSI/FBI)の調査結果にみられるように、セキュリティ侵害による企業 1 社あたりの被害額が増加する傾向にあることから、経営者層のセキュリティに対する意識の啓発は今後より重要になるといえる。

(2) ベンダ・ユーザのセキュリティ対応の促進

マーケットベースのセキュリティ技術の開発と製品の対応の促進が重要になる。また、セキュリティに対する一定の水準を保つ目安として標準化の推進が求められている。

米セキュリティ機関の SANS 研究所と米国家インフラ保護センター (NIPC) が指摘しているように、情報システムをデフォルトインストールのまま使用することがセキュリティ侵害を招く一番の要因となっている。ベンダ側は、セキュリティホールに対するパッチ等を速やかに公表するとともにユーザが容易に情報を得られるような環境を整備することが望ましい。ユーザサイドにおいても、インシデントやセキュリティパッチに迅速に対応できる体制を整えるとともに、自組織のセキュリティを定期的に見直していく、セキュリティマネジメントが不可欠となる。

また、これと歩調を併せて、各ステークホルダ (ベンダ・サービスプロバイダ・ユーザ等) の責任についての議論が求められるといえる。

(3) 健全な電子商取引の発展に向けた環境整備

各種調査にみられるように、オンライン上でのプライバシー・セキュリティに対する消費者の懸念は依然根強い。電子商取引の健全な発展に向けて、実効的なプライバシー・セキュリティ保護のための技術・規制等が望まれる。

その一方で、テロリズム・ハイテク犯罪等への対抗手段としてのナショナルセキュリティとプライバシー保護とのバランスについては、慎重な議論が必要とする意見も多い。

電子商取引の信頼性を確保するため、オンライン上で行う取引において、取引相手の認証や改ざん、否認の防止のための基盤を整備することが重要となる。公開鍵基盤 (Public Key Infrastructure : PKI) はこのような目的を達成するための重要な技術と認識されている。PKI においては、インターネット上の電子商取引は国境を越えて行われることから、国または地域間で相互に利用可能であることが求められる。

5 . 国内におけるニーズ調査

OECD セキュリティガイドラインの見直しにあたり、情報セキュリティガイドライン一般、及び国際機関の情報セキュリティガイドライン、OECD の情報セキュリティガイドライン等に関するニーズを調査した。

調査の対象は、情報セキュリティに関わる活動を行っている国内関連機関数団体である。

表 5-1 に、ヒアリング調査結果の概要について公表の許諾を得られたものについて示す（団体名は伏せてある）。

表 5-1 ヒアリング調査概要（順不同）

	団体 A	団体 B	団体 C
<p>セキュリティの現状に関する認識</p> <p>(インターネットの進展に伴う新たな脅威の出現、民間・政府における対応の現状および課題、既存法制度等の対応の現状および課題等)</p>	<ul style="list-style-type: none"> セキュリティにはコストがかかり、問題が顕在化するまでは避けようとしがちなため、何らかの強制力が必要。 セキュリティは危機管理的な要素が強い。そのため、トップの意識が変わらないとダメではないか。 製品レベルで規格に準拠していても、システム化すると、無規格製品が入るなど不都合が出てくる。このため、システム全体としてもセキュリティの考慮が必要。 	<ul style="list-style-type: none"> ブロードバンド化の進展と、それに伴う常時接続環境の拡大によって、個人ユーザへもセキュリティ問題が拡大することを懸念。 個人からの苦情や相談、通報に対応する組織や団体のコストと人材の確保が問題になる。 インターネットそのものを重要なインフラと位置づけ、税金による施策がなされるべき。 ネットワークセキュリティそのものを重要なインフラと位置づけ、ある程度公的な資金による施策がなされるべき。例えば、税制措置等の活用が考えられる。 	<ul style="list-style-type: none"> IT の浸透で IT ガバナンスはコーポレートガバナンスに接近。もはやセキュリティはシステム内に閉じ得ない。 知っている人が限られている時代から、多くの人が理解すべき時代へ。 システムのバラ売りはまともにインテグレートしないとうまく動かない。あるいは利用者が意識する必要がある。 未知の他者との直結に際して第3者による認証の必要性が生じている。
<p>OECDセキュリティガイドラインについて</p> <p>(OECDセキュリティガイドラインへの取り組み、見直しに向けた見解・意見等)</p> <p>9原則(数字で対応) 責任の原則 情報提供の原則 倫理性の原則 多面的考慮の原則 比例性の原則 統合の原則 適時性の原則 再評価の原則 民主主義の原則</p>	<ul style="list-style-type: none"> まずガイドライン自体の認知度が低いのが問題ではないか。周知させ、機能させることが肝心である。 情報公開は原則ではなく、公開が社会に不利益になる場合は避けるべき。 バランスの中で、運用責任への言及要。 見直し期間は対象により変わることを考慮。 OECD の役割は、文化の統一ができない中で相互配慮を促すことではないか。 		<ul style="list-style-type: none"> 一般的に、従来のルールは開発サイドの視点とその視点から見たシステムリスクが主体の場合が多いといった感じがする。もしそうであれば、昨今の状況変化を反映していない。現在、開発者はマイノリティと言っても過言でない程度であり、ユーザ等他の関係者の視点を加えるべきである。 92 年当時のメインフレーム前提からミッドレンジ主体の現在への流れを反映した変更が必要。 関係するがコントロールできない他者には awareness は使えず、disclose しかない。こうした関係者の責任関係に言及すべき。 時間が見えてこない。世の中に流れがあることを示すべき。 途上国を意識した文言が含まれていると感じる。重心が途上国に移る中、米英のガバナンスが通用しない国に向けたガイドラインの重要性は増大するはず。
<p>その他</p> <p>(国内 / 国外関連機関との協調・連携、標準化への取り組み等、その他関連する事項)</p>	<ul style="list-style-type: none"> セキュリティ規格作成に参加。 評価認証をビジネスとしてどう成り立たせるべきか。日本ではサービスはタダとの認識が強く有償化の浸透には時間がかかるのではないか。 	<ul style="list-style-type: none"> IPsec の相互運用実験等に関して、IETF の会合に参加した実績がある。また、同様のテーマでセミナー開催を予定。 	
<p>備考</p>	<ul style="list-style-type: none"> Y2K のときなど、自国にメーカーのない国が責任を全てメーカーに帰属させる法律をつくるケースあり。 今のネットワーク社会はあまりに急成長した結果、セキュリティの観点から見ると特に秩序の維持が追いついていない状況にある。 		<ul style="list-style-type: none"> 日本で監査として行う事務検査は inspection であって audit ではない場合が多い。米国では外側の立場から大枠の仕掛けを見るといった考え方が定着している。

6 . OECD 情報セキュリティガイドラインの見直しの検討

OECD セキュリティガイドラインに見直しにあたって、「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」において検討を行ってきた。

以下に研究会における審議の経緯と概要について整理する。

6 . 1 研究会委員

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委員および事務局は以下の通り（委員はあいうえお順、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）開発本部技師長（B I A C日本代表窓口）
歌代 和正	（株）I I J技術本部システム技術部長
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	慶応義塾大学理工学部情報工学科教授（座長）
苗村 憲司	慶応義塾大学環境情報学部教授
中尾 康二	（株）K D D I研究所ネットワーク管理グループグループリーダー
中原 志郎	日本電信電話（株）第五部門法務部担当部長
西尾 秀一	（株）N T Tデータビジネス企画開発本部 ITセキュリティ推進センター
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
久米 孝	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
山本 文士	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
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 社会システム研究室
富田 高樹	（株）富士総合研究所 社会システム研究室
佐久間 敦	（株）富士総合研究所 社会システム研究室

6.2 研究会における審議の経緯

表 6-1 に研究会における審議の経緯及び OECD の会合（WPISP、専門家会合）の開催状況について示す。

表 6-1 研究会における審議の経緯

	H13.8	9	10	11	12	H14.1	2	3
研究会の開催	第 1 回 (8.1)	第 2 回 (9.6)	第 3 回 (10.2)	第 4 回 (11.20)			第 5 回 (2.21)	
東京ワーク ショップ		9/12 - 13						
OECD 会合			WPISP 会合 (10.9-10)		専門家 会合 (12.11-12)		専門家 会合 (2.12-13)	WPISP 会合 / 専門家 会合 (3.4-6)

6.3 研究会における審議の概要

研究会における審議に概要について、各回次の主要な議題とその要旨を以下に示す。

第 1 回議題：

(1) ワークショップについて

- ・ セキュリティに関する活動領域には、主に以下の 3 種類があることを確認。
(1) national security、(2) public safety、(3) economic security。
- ・ BIAC、GBDe のセキュリティガイドラインの見直しに関する意向を確認。
- ・ OECD、METI 及び IPA 共催の 9 月のワークショップでは、OECD の役割、セキュリティガイドラインの役割を踏まえての議論が重要。

(2) 情報セキュリティガイドライン見直しについて

- ・ 現在盛んに発行され続けている数多の RFC (Request For Comments) が指し示すルール of 把握、技術進展により生ずる新たな脅威の分析が重要。
- ・ 技術的進展の中でのガイドラインそれ自体のライフサイクルを見誤らないようにしなければならない。

第 2 回議題：

(1) ワークショップについて

- ・ ワークショップに参加する委員から、講演の概要に関してそれぞれ解説及び、それに関する質疑応答があった。テーマは表 6-2 のとおり。

表 6-2 講演テーマ（一覧）

- | |
|--|
| <ul style="list-style-type: none">・ セキュリティマネジメントの重要性・ ブロードバンドの普及による一般家庭に対する脅威の増加・ 法・規制とテクノロジーの間の柔軟な関係の重要性・ プライバシーの保護とセキュリティの調和、技術の展開と脅威の増大・ 標準化の推進が生み出す脆弱性の増加・ セキュリティの目的：定義の展開（CIA（Confidentiality, Integrity, Availability）から CIARAA（Confidentiality, Integrity, Availability, Reliability, Authenticity, Accountability）へ）・ ステークホルダの役割 |
|--|

(2) 情報セキュリティの現状に関する調査報告

- ・ 最新の情報セキュリティの現状に関する、統計データに基づく傾向と規格化の動向についての調査報告および質疑。
- ・ 国内情報セキュリティ関連団体のヒアリング結果に関する報告と質疑。

(3) ガイドライン見直しについて

- ・ ガイドラインが何を目的とするかで、セキュリティの目的は大きく変わる。
- ・ 技術的な立場と法律的な立場では、言葉も考え方も変わる。
- ・ ガイドラインと OECD 加盟国、非加盟国の関係について。

第3回議題：

(1) ワークショップ実施報告について

- ・ OECD非加盟の6カ国と2地域も含め24の国と地域から参加、250名の登録。
- ・ プレス発表では、新たな脅威の性質とそれへの対応、取られるべき政府の対策やアプローチの方法等に関して、参加者間で共通の認識を形成する点において価値ある進展が見られたと評価。

(2) ガイドラインの見直しについて

- ・ セキュリティの目的に対する authenticity、accountability、reliability の追加が引き起こす問題点について：語の妥当性、語の格（階層・抽象度）、概念の錯綜、等
- ・ 9原則のそれぞれに対する意見の交換。
- ・ 原則の追加に関する試案の検討：国際連携/協力、市場に基くソリューション、適正な費用負担について議論。

第4回議題：

(1) ガイドラインの見直し原案作成について

- ・ 原案趣旨作成についての意見の交換が行われた。

(2) 調査報告「情報セキュリティの脅威に関する動向」の進め方(案)

- ・ 脅威の原因や、セキュリティホールに関する分析を加える。
- ・ 公開の原則とからめ情報をどう扱うべきか、が情報セキュリティに対する脅威に関する課題になる。被害の実際は、国ごとに認識が異なる、という問題がある。
- ・ 第1回に出た(1) national security、(2) public safety、(3) economic security のバランスは、9月11日のテロ以降、大きく変化している。

第5回議題：

(1) 今後のガイドライン見直しの方向性

- ・ 以下のような論点もしくは検討課題が明らかになっているが、さらに議論を重ねる必要がある。

原則のあり方

9原則についてどのように解釈するかについて議論。

ガイドライン全体構成

ガイドライン全体の構成について議論。

適用範囲の問題

「ユーザ」の範囲はどこまでか。

各関係主体が責任を担う範囲をどのように考えるべきか。

(2) 調査報告「情報セキュリティの脅威に関する動向」

- ・ 現状における脅威の特徴と原因に関する分析結果の報告。
- ・ 本報告書のドラフトに関する検討。

6.4 見直しにおける論点

研究会を通じて得られた、ガイドライン見直しにおける論点を以下に整理する。

(1) セキュリティの種類

- ・ セキュリティに関する活動領域には、主に以下の3種類がある。
(1) national security、(2) public safety、(3) economic security。
- ・ 本ガイドラインが対象とするセキュリティは、OECDの担う役割に応じて決まってくるものと考えられる。

(2) ガイドラインの対象としている関係主体

- ・ ガイドライン本文によれば「関係する者すべて」である。
- ・ 実質的には、OECDに加盟する各国政府が主として想定されていると考えられる。
- ・ 見直しに関しては、誰を対象とするかにより内容は大きく変わってくる。

(3) ガイドラインが想定する情報システム

- ・ 制定当時(1992年)の状況を考えると、closedなネットワークを介した情報システムを主としたものであると考えられる。
- ・ ただし1997年に結果的に見直しを行わなかった経緯としては、インターネットに象徴されるオープンなネットワークを含めた想定が1992年時点でなされてい

たとの判断によるものとされる。

(4) 考慮すべき状況変化

- ・ 本文にみられる「provider」の用語は現在の ISP、ASP ほかのいわゆる「サービスプロバイダ」を指すものと解釈されがちであるが、その多くはここ数年で登場してきたサービスであり、ガイドラインの指示する内容が妥当かどうかは議論を要するのではないか。
- ・ 同様に「users」が指す範囲も再考すべきである。企業ユーザは当然として、home user の扱いをどうするか。一定の責任を負うべきとの意見と、現実的には無理との意見がある。

(5) ガイドラインの構成

- ・ OECD が提供する他のガイドライン（個人情報保護、暗号政策ほか）と比較して、全体の構成がわかりにくく、また、EM(Explanatory Memorandum)に書かれている内容が細かく、ガイドラインとしての指導性に欠ける面がある。

(6) 実効性あるガイドラインとするための今後の方策

- ・ 開かれたネットワーク環境に対応した本人確認（認証）を行う Authenticity の強化が必要ではないか。
- ・ ネットワーク社会に対応できるより実効性のある Security Management に対応した原則の導入を行う必要があるのではないか。
- ・ 上記、方策を実現するための IMPLEMENTATION 記述の強化と EM 記述の具体化が必要ではないか。

7. ガイドラインの見直しに関する提案

1992年に制定されたOECD情報セキュリティガイドラインは、情報セキュリティの目的として、現在他の多くのガイドラインからも参照されている「CIA（Confidentiality(機密性)、Integrity(完全性)、Availability(可用性)）」の概念をもたらした意味において画期的であったといえる。また、ガイドラインに掲げられた9つの原則は、情報セキュリティに関わる諸問題に対して、技術、法制の両面をバランスよく網羅し、その普遍性において今なお指導原理として有効に機能していると評価できる。

一方、この10年間に情報システムを取り巻く環境は大きく変化してきている。特に、今日のインターネットの爆発的な普及は、1992年当時には予見されていなかった事象である。情報システムそれ自体の変化と歩調を合わせるかのように、情報システムに対する脅威も大きく変化している。「4. 国内外における情報通信システムに対する脅威の動向」にみたように、脅威の技術的な進化が、社会、経済、生活に深刻な影響を及ぼすようになっている。加えて、今やIT（情報技術）の進化は「ドッグイヤー」と形容されるほどスピードが速く、技術の進歩と、それと表裏一体である脅威の進化を正確に予測することは困難なことになっている。

OECD情報セキュリティガイドラインは、5年ごとに見直しを図ることが決まっているが、次回2007年までの5年間に情報セキュリティに対する要求はどのように変化していくのだろうか。2002年に予定されているOECD情報セキュリティガイドラインの見直しにおいては、今日の状況に対応しつつ、この時間の試練に耐えうるものとなる必要があり、以下の観点が重要になると考える。

(1) ガイドラインの実施の促進

企業や組織あるいは行政機関等において、セキュリティに関わる方針や政策を検討する際の規範として、OECD情報セキュリティガイドライン自体を明確な形で実施したケースは多くはないのが現状である。無論、セキュリティマネジメントの概念やISOをはじめとする情報セキュリティの標準化は、OECD情報セキュリティガイドラインが掲げる理念に礎を置いていることは間違いないが、ガイドラインそのものに対する認知度は、10年を経た現在でもそれほど高まっているわけではない。

本調査の一環として実施した国内のセキュリティ関連団体に対するヒアリング調査においても、OECD情報セキュリティガイドラインについて知識をもつ企業や組織は多くはない、との意見が複数の関係者から聞かれた。

OECD情報セキュリティガイドラインが、情報セキュリティに関する高次の指導原理としてその役割を果たすためには、実施をより具体的に意識した形に整理されることが望ましい。特に、OECD情報セキュリティガイドラインの「実施(Implementation)」の項は、各原則を実際のセキュリティ確立の現場に適用する方針を記述している部分であり、影響力の高い箇所といえる。しかしながら、現行のガイドラインにおける記述は網羅性と最近の状況変化への対応という点で十分とは言いがたく、加盟各国の状況を踏まえつつ、本項を充実させることでガイドラインの実効力をさらに高めることが期待される。

(2) 情報セキュリティに対する意識の向上と普及啓蒙

政府、民間、個人といった社会のあらゆるセクターにおいて、また、若年層から企業・組織のトップまであらゆる階層に対して、情報セキュリティの目的に対する理解とその実践の必要性について意識を向上させ、普及啓蒙に努めることが重要となる。

企業や組織における情報セキュリティの現場では、セキュリティ選任担当者の設置を含むセキュリティ対策のコスト負担についてトップマネジメントのコミットメントが得られないことを、自組織のセキュリティ向上を阻む要因としてあげる声は根強く残っている。経営者、政策担当者等に対する普及啓蒙は、今なお課題であるといえる。

一方、企業、組織のみならず学校や家庭の情報化は今後一層進むことが予想されている。学校教育から企業、組織における情報リテラシ訓練に至るまで、情報システムのユーザに対しては、必要に応じたセキュリティ教育の機会が提供されるべきである。

OECD 情報セキュリティガイドラインは、情報セキュリティに関する普及啓蒙と教育訓練をより明確な形で奨励すべきである。

また、情報システムの利用者に対する啓蒙においては、セキュリティを保護する側だけでなく、セキュリティを侵害しようとする者への視点も含めて議論することは有効だろう。

2000年2月に発生した米国著名サイトへのDDoS攻撃事件をはじめ、若年層によるセキュリティ侵害やインターネットを悪用した犯罪が急増している。年少の頃より、倫理性や自己の責任に対する自覚が身につくような環境の整備が求められているといえる。

このような背景のもと、OECD 情報セキュリティガイドラインにおいても、セキュリティに対する社会全体の意識を向上させるため、普及啓蒙と教育訓練の推進について明確な支持を打ち出すべきである。現行のガイドラインにおいては、「説明のための覚書 (Explanatory Memorandum)」に「Education and Training (教育と訓練)」の項を設け、その重要性を説いているが、より積極的に原則やそれに準じる形に整理することが望ましいと考える。

(3) 情報セキュリティに関わるステークホルダの多様化への対応

情報システムに利用局面が広がり、ベンダ、プロバイダ、事業者、行政担当者、個人等を含め、情報システムにかかわるステークホルダ (関係者) が多様化している。ネットワーク社会における信頼性の確保のために、各者は適正な責任分担と役割を負うことを認識することが必要である。

家庭でのブロードバンド化の進展や、携帯電話、PHS など普及により、個人ユーザにおいても IT はより身近なものになっている。もはや、情報セキュリティに対する脅威は個人ユーザにとっても無関係なものではなく、セキュリティ対策のコストや、ネットワークに繋がった他者に対する責任について、意識の向上を促すことが重要になる。

また、各国において電子政府、電子自治体に向けた取り組みが進行中であり、今後政府機関は情報システムの大規模ユーザであると同時に、情報システムによるサービス提供者の側面を併せ持つことになる。

他方、ベンダやサービスプロバイダにおいては、インシデントの急増と影響の拡大を背景として、製品のセキュリティホール等の脆弱性とそれへの対処に対する責任が、今後議論の

対象としてクローズアップしてくるものと思われる。ただし、電子商取引を含めたインターネット経済の健全な発展のために、自由な情報の流通を支持し、これを妨げないように十分な配慮が必要である。

このようなステークホルダの多様化と各者の役割の変化に対して、現在のガイドラインで想定している対象が漠然とした印象があり、「誰が」「何を」すべきなのかを直感的に把握しにくい問題があるといえる。原則の中で書き分けるのは煩雑ないし冗長になる懸念があるため、現行の「実施(Implementation)」の項あるいは「覚書(Explanatory Memorandum)」などにおいて、想定されるステークホルダごとに各原則をどう扱うべきかを記述することで、読者の理解を容易にする効果が期待できるものと考えられる。

(4) 国際協調の推進

国境のないインターネットにおいて、脅威の進化のスピードと影響の深刻さが格段に高まっている現在、各国間における情報とベストプラクティスの共有の促進が不可欠である。加えて、セキュリティ施策が倫理の尊重や、公平性や開放性といった民主主義社会における価値との整合性を図る点において、ガイドラインが加盟各国間の協調に向けて方向性を示すことが望ましい。これを支援する意味において、OECD の役割として、加盟各国や関係者間の協調を促し、それを支援する機会の提供を表明することも有効であると思われる。

現行のガイドラインに記述されている概念や用語については、加盟各国間での法制度、文化的相違や、国内あるいは域内のガイドラインや規格との整合等の事情が作用しており、完全な整合が得られない側面もある。より普遍的かつ認知性の向上を目指し、改良を加えていく必要があるものと考えられる。特に、インターネットに繋がる人の多様性を考慮し、非英語圏の読者も意識しつつ、より広く理解が得られる形に再整理されることが望ましい。

一方、政府機関や企業の情報システムを対象とした脅威に関しては、政治的な意図をもった攻撃が増加しているとの見解もある。このようなサイバーテロやサイバー戦争の危険は高まりつつあるといえ、プライバシー保護を含む国際的な情報セキュリティと一国の安全保障(ナショナルセキュリティ)と整合を如何に確保するかについては、今後重要な検討課題になるとと思われる。

加えて、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いる。また、情報セキュリティの全体のレベルは、もっとも低い箇所の影響を受けることが指摘されている。今後、OECD 非加盟国やインターネット途上国に対して、OECD 情報セキュリティガイドラインへの対応を含めたセキュリティ施策の推進をどのように支援していくかが、国際的な課題としてよりクローズアップされてくるだろう。

(了)

8 . 付録

8 . 1 付録1 1992年 OECD セキュリティガイドライン (本文 / 和訳対訳)

<p>RECOMMENDATION OF THE COUNCIL concerning Guidelines for the Security of Information Systems (adopted by the Council at its 793rd Session on 26-27 November 1992)</p> <p>THE COUNCIL, HAVING REGARD TO:</p> <ol style="list-style-type: none">1.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;2.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)];3.the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [C(85)139,Annex]; <p>RECOGNISING:</p> <ol style="list-style-type: none">1. the increasing use and value of computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance (all hereinafter referred to collectively as "information systems");2. the international nature of information systems and their worldwide proliferation;3. that the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems;4. that, in the absence of appropriate safeguards, data and information in information systems acquire a distinct sensitivity and vulnerability, as compared with paper documents, due to risks arising from available means of unauthorised access, use, misappropriation, alteration, and destruction;5. the need to raise awareness of risks to information systems and of the safeguards available to meet those risks;6. that present measures, practices, procedures and institutions may not adequately meet the challenges posed by information systems and the concomitant need for clarity, predictability, certainty, and uniformity of rights and obligations, of enforcement of rights, and of recourse and	<p>情報システムセキュリティガイドラインに関する委員会勧告 1992年11月26日</p> <p>委員会は、以下の事柄を考慮し、</p> <ol style="list-style-type: none">1. 1960年12月14日のOECD協定、特に1(b)、1(c)、3(a)、5(b)2. 1980年9月23日のプライバシー及び個人データの越境データ流通の保護に関するガイドライン [C(80)58(最終版)]3. 1985年4月11日にOECD加盟国政府によって採択された越境データ流通宣言 [C(85)139, 付属文書] <p>以下の事柄を認識し、</p> <ol style="list-style-type: none">1. コンピュータ、通信施設、コンピュータ通信網、及びそれらにより蓄積又は処理され、検索され、伝送されるデータ及び情報(それらデータ及び情報にはプログラムや仕様、保守・運用・使用手順を含む)の価値及び利用が高まりつつあること(以後、集散的に情報システムと呼ぶ)2. 情報システムの国際的性格及び世界的な広がり3. 情報システムが重要な役割を果たすようになり、OECDにおける経済・貿易または社会的、文化的、政治的分野で情報システムへの依存が高まりつつあるため、情報システムの信頼性を高めるための特別な取り組みが必要であること4. 情報システムにおける全てのデータ及び情報は、適正なセキュリティ障壁無しでは、紙に書かれた文書に比較して、無権限のアクセス、使用、悪用、改変及び破壊による危険が大きいため、明らかに害を受けやすく、無防備であること5. 情報システムへのリスクについて周知させる必要性、及びそのようなリスクに対処するために利用可能な対策について周知させる必要性6. 情報システムに関して提起されてくる問題に、現在の対策や実践、手続、規則は充分に対応できず、権利及び義務、権利の行使、情報システム及び情報システムセキュリティに関する権利の侵害に対する請求及び補償の内容を明確にし、
---	---

<p>redress for violation of rights relating to information systems and the security of information systems;</p> <p>7. the desirability of greater international co-ordination and co-operation in meeting the challenges posed by information systems, the potential detrimental effects of a lack of co-ordination and co-operation on national and international economies and trade and on participation in social, cultural and political life, and the common interest in promoting the security of information systems;</p> <p>AND FURTHER RECOGNISING:</p> <p>1. that the Guidelines do not affect the sovereign rights of national governments in respect of national security and public order ("ordre public"), subject always to the requirements of national law;</p> <p>2. that, in the particular case of federal countries, the observance of the Guidelines may be affected by the division of powers in the federation;</p> <p>RECOMMENDS THAT MEMBER COUNTRIES:</p> <p>1. establish measures, practices and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Appendix to this Recommendation, which is an integral part hereof;</p> <p>2. consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures for the security of information systems;</p> <p>3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;</p> <p>4. disseminate extensively the principles contained in the Guidelines;</p> <p>5. review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems.</p>	<p>予見可能のものとし、必然的なものとし、統一的なものとする必要があること</p> <p>7. 情報システムに関して提起されてくる問題、各国協調的な手段を採らない場合に国内・国際経済、貿易、及び社会・文化・政治の場での参加に及ぼすであろう悪影響、情報システムセキュリティを推進する共通の利益、に対処するため、国際協調を更に進めたいこと</p> <p>また、さらに次のことを認識し、</p> <p>1. ガイドラインは国家安全保障及び公衆の安寧に関する国家主権を侵すものではなく、常に国内法の要請に従うこと</p> <p>2. 連邦国家の場合ガイドラインの遵守が地方分権によって影響を受け得ること</p> <p>以下の事柄を勧告する。</p> <p>1. この勧告と一体をなす附属文書であるガイドラインに規定されている、情報システムセキュリティに関する原則を反映した、対策、実践、手続きを確立すること</p> <p>2. ガイドラインの実施にあたり、協議、協調、協力を進める。これには、情報システムセキュリティのための互換性のある標準、対策、実践、手続きの策定のための国際協力を含む</p> <p>3. ガイドラインの適用のための特別の決議に関し、可能な限り迅速に合意すること</p> <p>4. ガイドラインに含まれる原則の普及に大いに努めること</p> <p>5. 情報システムセキュリティに関する問題についての国際協力を改善するという観点から、OECD ガイドラインを5年毎に見直す。</p>
---	---

<p style="text-align: center;">Annex to the Recommendation of the Council of 26 November 1992</p> <p style="text-align: center;">GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS</p> <p style="text-align: center;">26 November 1992</p>	<p style="text-align: center;">1992 年 11 月 26 日委員会勧告付属文書</p> <p style="text-align: center;">情報システムのセキュリティ のためのガイドライン</p> <p style="text-align: center;">1992 年 11 月 26 日</p>
<p style="text-align: center;">I. AIMS</p> <p>The Guidelines are intended:</p> <ul style="list-style-type: none"> • To raise awareness of risks to information systems and of the safeguards available to meet those risks; • To create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems; • To promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures; • To foster confidence in information systems and the manner in which they are provided and used; • To facilitate development and use of information systems, nationally and internationally; and • To promote international co-operation in achieving security of information systems. 	<p style="text-align: center;">I. 目的</p> <p>このガイドラインは以下のことを目的とする。</p> <ul style="list-style-type: none"> • 情報システムに対するリスク及びそれらリスクに対処するための利用可能なセキュリティ障壁に対する認識を高める • 情報システムセキュリティのための一貫した対策、実践、手続きの開発及び実施のため、公共及び民間部門の責任者の助けとなる一般的な枠組みを策定する • そのような対策、実践、手続きの開発及び実施にあたっての、公共部門と民間部門との協力を推進する • 情報システム及びそれが提供され利用される形式に対する信頼性を高める • 情報システムの国際的な展開及び利用を促進する • 世界的情報システムセキュリティを達成するための国際的な協力を推進する
<p style="text-align: center;">II. SCOPE</p> <p>The Guidelines are addressed to the public and private sectors.</p> <p>The Guidelines apply to all information systems.</p> <p>The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.</p>	<p style="text-align: center;">II. 適用範囲</p> <p>ガイドラインは公共部門及び民間部門を対象とする</p> <p>ガイドラインは全ての情報システムに適用される</p> <p>ガイドラインには、情報システムセキュリティ提供のための更なる実践、手続きが追加され得る</p>
<p style="text-align: center;">III. DEFINITIONS</p> <p>For the purposes of these Guidelines:</p> <ul style="list-style-type: none"> • "data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means; • "information" is the meaning assigned to data by means of 	<p style="text-align: center;">III. 定義</p> <p>このガイドラインの目的のため、以下の表現はそれぞれ次の意味を持つこととする。</p> <ul style="list-style-type: none"> • データとは、事実又は概念、命令が、人間又は自動的手段による通信、翻訳、処理に適した形式になっているものを言う • 情報とは、現在習慣的にデータとされているもの

<p>conventions applied to that data;</p> <ul style="list-style-type: none"> • "information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance; • "availability" means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner; • "confidentiality" means the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner; • "integrity" means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. <p style="text-align: center;">IV. SECURITY OBJECTIVE</p> <p>The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.</p> <p style="text-align: center;">V. PRINCIPLES</p> <p>1. Accountability Principle The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.</p> <p>2. Awareness Principle In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.</p> <p>3. Ethics Principle Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.</p> <p>4. Multidisciplinary Principle Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal..</p> <p>5. Proportionality Principle Security levels, costs, measures, practices and procedures</p>	<ul style="list-style-type: none"> • 情報システムとは、コンピュータ、通信施設、コンピュータ通信網、及びそれらにより蓄積又は処理され、検索され、伝送されるデータ及び情報を言い、それらデータ及び情報にはプログラムや仕様、保守・運用・使用手順を含む • 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 <p style="text-align: center;">・セキュリティの目的</p> <p>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。</p> <p style="text-align: center;">V. 原則</p> <p>1. 責任の原則 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。</p> <p>2. 情報提供の原則 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。</p> <p>3. 倫理性の原則 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。</p> <p>4. 多面的考慮の原則 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。</p> <p>5. 比例性の原則 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</p>
--	---

<p>should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.</p> <p>6. Integration Principle Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.</p> <p>7. Timeliness Principle Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.</p> <p>8. Reassessment Principle The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.</p> <p>9. Democracy Principle The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.</p>	<p>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、広がりには比例したものであるべきである。</p> <p>6. 統合の原則 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。</p> <p>7. 適時性の原則 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。</p> <p>8. 再評価の原則 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。</p> <p>9. 民主主義の原則 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るべきである。</p>
<p style="text-align: center;">VI. IMPLEMENTATION</p> <p>Governments, the public sector and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative, self-regulatory and other measures, practices, procedures and institutions for the security of information systems. Where provision has not already been made, they should, in particular:</p> <p>Policy Development Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:</p> <ul style="list-style-type: none"> • harmonized worldwide technical standards, methods and codes of practice; • promotion of expertise and best practice in the security of information systems; • formation and validity of contracts and other documents created and executed in or by means of information systems; 	<p style="text-align: center;">VI. 実施</p> <p>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、努力すべきである。このガイドラインに示される目的の達成及び原則の実施にあたり、政府及び公共部門、民間部門には、情報システムのセキュリティのため、適切な、法律、行政、自主規範その他対策及び実践、手続き、規則の確立及び確立の推進・支援が求められる。規定がまだ策定されていない場合、以下のことをなすべきである。</p> <p>政策 以下の事柄に関する規定を含む、適正な政策、法、政令、規範、国際協定の採択及び採択の推進を図る。</p> <ul style="list-style-type: none"> • 世界的に調和した技術標準、手段及び行為規範 • 情報システムセキュリティのための専門的知識及び最良の実践の普及 • 情報システムの中で、又は情報システムによって生成され履行される契約その他の書類の構造、有効性

<ul style="list-style-type: none"> • allocation of risks and liability for failures of the security of information systems; • penal, administrative or other sanctions for misuse of information systems; • jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies; • mutual assistance, extradition and other international co-operation in matters relating to the security of information systems; and • means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings. <p>Education and Training Promote awareness of the necessity for and the goals of security of information systems, including:</p> <ul style="list-style-type: none"> • ethical conduct in the use of information systems; and • adoption of good security practices. <p>Provide and foster education and training of:</p> <ul style="list-style-type: none"> • developers, owners, providers and users of information systems; • specialists and auditors of information systems; • specialists and auditors of security of information systems; and • law enforcement authorities, investigators, attorneys and judges. <p>Enforcement and Redress Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.</p> <p>Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.</p> <p>Exchange of Information Facilitate the exchange of information relating to the Guidelines and their implementation.</p> <p>Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.</p>	<ul style="list-style-type: none"> • 情報セキュリティが破れたときのリスク及び責任の分散 • 情報システムの悪用に対する刑事罰、行政罰その他刑罰 • 国外裁判権に関する規則を含む裁判所の司法適格性及び他の機関の行政適格性 • 相互援助、犯罪人引渡その他刑事事件における国際協力 • 刑事裁判、民事裁判及び行政審判で使用される証拠を情報システムの中で獲得できる方法、及び刑事裁判、民事裁判及び行政審判における、そのような証拠の認容性 <p>教育及び訓練 情報システムセキュリティの目的及び必要性の周知を推進する。</p> <ul style="list-style-type: none"> • 情報システムの利用における倫理的行動 • 良きセキュリティの実践を採用 <p>以下の者に対する教育及び訓練の提供、及び教育及び訓練の推進</p> <ul style="list-style-type: none"> • 情報システムの開発者、所有者、提供者、ユーザ • 情報システムの専門家、監査人 • 情報システムセキュリティの専門家、監査人 • • 法執行者、捜査官、弁護士、裁判官 <p>法の執行及び補償 ガイドラインの実施に基づく権利の行使及び執行のため、及びそれら権利の侵害に対する請求及び補償のため、利用し易く、合理的で、適切な手段を提供する。</p> <p>情報システムセキュリティの破壊に関する裁判及び捜査においては迅速に支援する。</p> <p>情報の交換 ガイドライン及びその実施に関する情報交換を促進する</p> <p>情報システムセキュリティ及びガイドラインの遵守のため採択された対策、実践、手続きについては一般的に広報する</p>
--	--

Co-operation

On national and international levels, consult, co-ordinate and co-operate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonize as completely as possible measures, practices and procedures for the security of information systems.

EXPLANATORY MEMORANDUM

to Accompany the Guidelines for the Security of Information Systems

PREFACE

In October 1988, the Committee for Information, Computer and Communications Policy (ICCP) of the OECD approved the preparation by the OECD Secretariat of a study on the subject of security of information systems. The report, entitled Information Network Security, was submitted to the ICCP Committee in October 1989. Following review of the Secretariat document, the ICCP Committee endorsed the convocation of a meeting of experts to explore in greater depth the issues raised in the report.

Based upon the advice of the experts, the ICCP Committee, in March 1990, approved the creation of a Group of Experts to draft Guidelines for the Security of Information Systems. The Group of Experts included governmental delegates, scholars in the fields of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users. The Group of Experts was chaired by the Hon. Michael Kirby, President of the Court of Appeal, Supreme Court of New South Wales, Australia. The Secretariat of the Information, Computer and Communications Policy Division of the OECD's Directorate for Science, Technology and Industry drafted the Recommendation, the Guidelines and the Explanatory Memorandum, based upon the deliberations of the Expert Group at its meetings.

The Group of Experts met six times between January 1991 and September 1992 to prepare the Recommendation of the Council concerning Guidelines for the Security of Information Systems, the Guidelines for the Security of Information Systems, and the Explanatory Memorandum to Accompany the Guidelines.

The OECD is well-positioned to play a central role in building awareness of the need for security of information systems and of measures that might be undertaken to meet that end. OECD membership encompasses North America, the Pacific region and Europe. The lion's share of development and exploitation of information systems occurs in OECD Member countries. Through the ICCP Committee, the OECD provides direction and coalesces opinion at an early stage on issues related to information, computer and communications technologies and policies and their effects on society, with a view to raising

協力

ガイドラインの実施及び情報システムのセキュリティのための対策及び実践、手続きを可能な限り一致させるため、政府及び民間部門は、国内・国際レベルにおいて他の政府、政府内、及び民間部門と協議し、調整し、協力する。

説明のための覚書

情報システムのセキュリティに関するガイドラインに添えて

前書き

1988年10月、OECDの情報コンピュータ通信政策(ICCP)委員会は、OECD事務局が情報システムのセキュリティに関する報告書を作成することを承認した。「情報ネットワークセキュリティ」と題するこの報告書は、1989年10月にICCP委員会に提出された。この委員会文書の再検討に従い、ICCP委員会は、専門家を召集して会議を開き、報告書で提起された問題点をさらに深く探求することを指示した。

専門家の勧告に基づいて、ICCP委員会は、1990年3月に、専門家グループによる情報システムのセキュリティに関するガイドライン草稿の作成を承認した。この会議に参加したのは、政府代表者、法律、数学およびコンピュータ科学の研究者、ならびにコンピュータや通信に関連する製品やサービスの提供者およびユーザを含む民間部門の代表などである。オーストラリア New South Wales の最高裁判所である Appeal 裁判所の首席判事である Hon. Michael Kirby 氏が専門家グループの議長を務めた。OECD の科学・技術・産業に関する理事会の ICCP の事務局が、勧告、ガイドラインおよび説明用覚書のドラフトを、専門家会合における検討に基づいて作成した。

専門家グループは1991年1月から1992年9月にかけて6回会議を開き、「情報システムのセキュリティに関するガイドラインに関する委員会勧告」、「情報システムのセキュリティに関するガイドライン」、および「説明のための覚書 - ガイドラインに添えて」を作成した。

OECD は、情報システムのセキュリティの必要性について、またその目的を果たすために講ずべき手段について、注意を喚起し認識させるにあたって中心的な役割を果たすのに適した立場にある。OECD 加盟国は北米、太平洋地域から、ヨーロッパまでと、広範にわたっている。情報システムの開発と利用によって最大の利益を得ているのは、これら OECD 加盟各国である。OECD は、ICCP 委員会を通して情報、コンピュータ、および通信の技術と施策、ならびにこれらが社会に及ぼす影響に関連する問題に関して早い段階で指示を与え、意見をとりまとめ、国際的に周知を喚起し政府や民間部門による審議を援助す

awareness on an international level and assisting governments and the private sector as they undertake national deliberations.

The Guidelines for the Security of Information Systems are intended to provide a foundation from which countries and the private sector, acting singly and in concert, may construct a framework for security of information systems. The framework will include laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities. It is hoped that the Guidelines will serve as a benchmark against which governments, the public sector, the private sector and society may measure their progress.

INTRODUCTION

A computer, a computer program and data constitute basic elements of an information system. The computer may be connected by communication equipment and devices into a network with terminals or other computers or communication facilities. A network may be a private local area network (LAN), an extended private network, such as a wide area network (WAN) or global network, or an external communication link open to anyone with the technological means to gain access to it. Many networks are composed of a combination of internal and external links. Communication networks include data communication, telephone and facsimile. Other ancillary equipment, printers, for example, may be attached to the computer and communications hardware. The computer programs might include operating system and application software, which may be custom-designed or purchased ready-made. The software may be installed in the computer or stored on magnetic, optical or other media. Paper manuals and documentation support the operation, use and maintenance of the hardware and software. This entire structure is created for the purpose of storing, processing, retrieving and transmitting data and information. These various elements may be combined to form an information system. (The dynamism of information and communication technologies dictates that this description of information systems may serve only to give an indication of the present situation and that new technological developments will arise to augment the potentialities of information systems).

Expanding Uses and Benefits of Information Systems

The significance of computer and communications technologies, economically, socially and politically, is widely accepted. They are key technologies not only in their own right but also as conduits for and components of other goods, services and activities.

Recent years have witnessed:

- proliferation of computers;
- increase of computing power with simultaneous decrease in costs;

る。

情報システムのセキュリティに関するガイドラインは、各国および民間部門が単独あるいは協力して情報システムのセキュリティの枠組みを構築できる土台を提供することを意図したものである。この枠組みには、法律、実施綱領、技術対策、管理部とユーザの訓練、公教育および宣伝活動が含まれるだろう。このガイドラインが、政府、公共部門、民間部門および社会が進捗を判断するためのベンチマークとなることが望まれる。

はじめに

コンピュータ、コンピュータプログラムおよびデータが、情報システムを構成する。コンピュータは、通信装置によって、端末または他のコンピュータを含むネットワークもしくは通信施設と接続される。ネットワークには、プライベートなローカル・エリア・ネットワーク(LAN)から、ワイド・エリア・ネットワーク(WAN)やグローバル・ネットワークなどの拡張私設ネットワーク、さらに、アクセスする技術的手段さえ持っていれば誰でも利用できるよう開放されている外部通信リンクまで様々ある。ネットワークの多くは、内部リンクと外部リンクを組み合わせた構成となっている。通信ネットワークには、データ通信、電話およびファクシミリが含まれる。コンピュータと通信ハードウェアには、たとえば、印刷装置などの他の補助装置を取り付けてもよい。コンピュータ・プログラムには、オペレーティング・システム(OS)やアプリケーション・ソフトウェアが含まれ、これらは、受注設計品であっても既製品を購入してもよい。これらのソフトウェアは、コンピュータ内に格納されるか、磁気媒体上に保存される。印刷された取り扱い説明書と文書を介して、ハードウェアとソフトウェアの使用、保守管理および保護をサポートする。この構成全体は、データと情報の保存、処理、検索および伝送のために作成される。これらの要素のすべてが組み合わせられて、1つの情報システムを形成する。(情報技術と通信技術は進歩し続けているため、情報システムに関するこの記述は現状を示すに過ぎず、新しい技術開発製品が出現して情報システムの潜在的可能性が増すであろう。)

情報システムの利用の拡大と利便性

コンピュータ技術および通信技術の経済的、社会的ならびに政治的重要性については広く認識されている。これらの技術はそれ自体が重要な鍵となるものであるばかりではなく、他の製品、サービスおよび活動を導き出すもの、またそれらの構成要素としても重要である。

近年、下記の出来事が見られる。

- コンピュータの急激な普及。
- 計算能力の増強と、それと同時に削減されたコスト。

<ul style="list-style-type: none"> • convergence of computer and communication technologies; • greater interconnectivity and inter-operability of computer and communication systems; • increasing decentralisation of computing and communication functions; and • growth of computer use to the point that, in many countries, every individual is an actual or potential user of computer and communication networks. <p>The global information society has arrived. It is borderless, unconstrained by distance or time. Our economies, politics and societies are based less on geography and physical infrastructure than previously, and increasingly on information system infrastructures.</p> <p>Information systems benefit governments, international organisations, private enterprise and individuals. They have become integral to national and international security, trade, and financial activity. They are widely used by government administrations, fiscal authorities, business organisations and research institutions. They are critical to the provision of health care, energy, transport, and communications. Information systems may be used for trading, voting, learning and leisure. Expanded use of information systems offers possibilities of greater access to resources, experience, learning, and participation in cultural and civic life.</p> <p>Dependency</p> <p>Every person, enterprise and government is affected by information systems and has become dependent on their continued proper functioning. For example, increased use of information systems has wrought fundamental changes in internal organisational procedures and has altered the way that organisations interact. In the event of an information system failure, it may not be possible to continue present procedures without information systems nor practicable to return to former methods. There may not be sufficient paper records, staff skills or even numbers of staff to permit an organisation to continue to work as productively as it does with its information system in operation, and as effectively as its competitors. Consider, for example, the effect of information system failure on the functioning and efficiency of airlines, banks or securities exchanges.</p> <p>Dependence on information systems is growing. Concomitant is a mounting need for confidence that they will continue to be available and to operate in the expected manner.</p> <p>Vulnerability</p> <p>As use of information systems has increased enormously, generating many benefits, it has, in its wake, created an ever larger gap between the need to protect systems and the degree of protection presently utilised. Society, including business, public services and individuals, has become very dependent on</p>	<ul style="list-style-type: none"> • コンピュータ技術と通信技術の集中。 • コンピュータと通信システムの相互接続性と相互操作性(インターオペラビリティ)の増大。 • 計算機能と通信機能の分散化の進展。 • 多くの国で、誰もがコンピュータおよび通信ネットワークの実際のユーザとなるか、ユーザになりうるような状態にまでコンピュータの利用が増大。 <p>地球規模の情報化社会が到来した。これは、国境がなく、距離にも時間にも制約されない社会である。我々の経済、政治および社会は、以前ほど地理的物理的なインフラストラクチャに基づいてはおらず、ますます情報システムのインフラストラクチャに基づくようになりつつある。</p> <p>情報システムは、政府、民間企業および個人に利益をもたらす。情報システムは、国内および国際的な安全保障、貿易および金融活動に組み込まれており、政府管理、財政当局、事業体、研究機関などで広く利用されている。保健、エネルギー、交通、および通信の提供にはなくてはならないものである。ビジネス、投票、学習、レジャーなどのすべてが、情報システムを利用して行える。情報システムの利用が拡大すると、資源、経験および教育へのアクセスと、文化生活や都市生活への参加の可能性が広がる。</p> <p>依存性</p> <p>個人、企業および政府は、それぞれ情報システムによる影響を受けており、情報システムが正しく機能することに依存するようになっている。たとえば、情報システムの利用が増大したことから、組織内部の手続きに根本的な変化がもたらされ、組織間の相互作用にも変化が生じてきた。情報システムに障害があるからといって、情報システムなしには現在の手続きを今後も続けることはできないであろうし、かといって昔の方法に戻るといっても現実的ではないだろう。組織が情報システムを利用して可能な限り高い生産性をもって運営し、また競争力を効率的に存続するには、書類上の記録、スタッフの技能、あるいはスタッフの数さえも十分でないかもしれない。たとえば、情報システムに障害が発生した場合に、航空、銀行または証券取引所の機能や効率性がどのようなものになるか考えていただきたい。</p> <p>情報システムへの依存性は、いまやますます大きくなっている。それに付随して、情報システムを今後とも利用し続けられること、また期待どおりに動くことに対する信頼性がますます強く求められている。</p> <p>脆弱性</p> <p>情報システムの利用が大きく拡大し、多くの利便性もたらされるにつれて、システムを保護する必要と、実際に利用されている保護の程度との間に、大きなギャップが生じている。商業、公共サービスおよび個人を含む社会は、十分信頼しうるとはいえない技術に大いに頼るようになってきた。上掲の情報システムの</p>
---	--

technologies that are not yet sufficiently dependable. All the uses of information systems identified above are vulnerable to attacks upon or failures of information systems. There are risks of loss from unauthorised access, use, misappropriation, modification or destruction of information systems, which may be caused accidentally or result from purposeful activity. Certain information systems, both public and private, such as those used in military or defence installations, nuclear power plants, hospitals, transport systems, and securities exchanges, offer fertile ground for anti-social behaviour or terrorism.

The developments identified above, proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, while enhancing the utility of information systems, also increase system vulnerability. It may be harder to locate a system problem and its causes, to correct it in balance with other system functions and requirements, and to prevent its recurrence or the occurrence of other lapses. As systems decentralise and grow larger, it is important to keep account of their interdependent components, which, increasingly, may come from multiple vendors and sources. Moreover, the growing interconnectivity of network systems and use of external networks multiply points of possible information system failures. These externalities lie outside the direct control of the system operators and the rights and duties of the parties in the event of breaches may be unclear.

Technical change is uneven. It leaps ahead in some areas while lagging in others. Inability to adapt to and absorb technological developments at the same rate at which they occur, such as failure adequately to test or co-ordinate system changes, may lead to system problems. Technological developments may be implemented before all their ramifications and relations to existing technologies are understood. Unequal distribution of system capabilities may give some persons more control of and access to information systems than is intended or desirable. Increasing numbers of users have access to information systems, while, at the same time, they are decreasingly directly controlled by system owners or providers.

Failures of information systems may result in direct financial loss, such as loss of orders or payment, or in losses that are more indirect or perhaps less quantifiable by, for example, disclosure of information that is personal, important to national security, of competitive value, or otherwise sensitive or confidential.

The evolution of the law is not always in step with technological progress. It is sometimes insufficient at the national level and in a number of cases still undeveloped at the international level. Harmonization of legislation is an important goal to be actively pursued.

Building Confidence

Users must have confidence that information systems will operate as intended without unanticipated failures or problems.

利用は、いずれもが、情報システムに対する攻撃や、情報システムの障害に弱い。不正アクセス権や非公認の情報システムへのアクセス、不正使用、悪用、または変更の危険が存在する。これらは、偶然に発生する場合もあるが、故意の行動の結果であることもある。軍事施設または防衛施設、原子力プラント、病院、交通システムおよび証券取引所で使用される情報システムは、反社会的活動やテロリズムの格好の標的になっている。

上述のような発展、コンピュータの普及、計算能力の増強、相互接続性、分散化、ネットワークの成長およびユーザ数の増加は、情報システムの活用度を高める一方で、システムの脆弱性も増加させている。システムの問題とその原因を突き止め、システムの他の機能や要件と調和をとりながら訂正し、再び同じことが起こったりあるいは別の間違いが生じるのを防ぐことが、これまで以上に困難になっている。システムの分散化が進みいっそう巨大になるにつれて、ベンダや供給源が多重化するため、相互依存の構成要素について常に把握しておくことが重要になる。さらに、ネットワーク・システムの相互接続性が高まり、外部ネットワークを利用することも多くなると、情報システムの障害が発生し得る箇所も増える。このような外的要因は、システム・オペレータの直接管理の範囲外にあり、違反があった場合でも、誰に権利と義務があるのかが明らかでないことがある。

技術は、すべての領域で均等に变化していくわけではない。ある領域では急激に進歩するが、べつの領域では停滞していることもある。システムの変更を適切に試験したり調整できないなど、技術開発と同じ速度で技術の進歩に適合し、これを吸収できないと、システムに問題が生じるだろう。既存の技術がもたらした成果やそれに関連する事項すべてについて理解しないうちに、さらに新たな技術の開発が行われる。システムの能力が均等に分散されているのではないことから、本来意図された、あるいは適切だと思われる以上に情報システムを管理したり情報システムにアクセスすることになる人もいるかもしれない。ますます大勢のユーザが情報システムにアクセスするようになっているが、それと同時にこれらのユーザは、システムの所有者や提供者から直接に管理されなくなりつつある。

情報システムの障害は、注文や支払いを受け損なったりという直接的な財務上の損失をもたらすことがある。一方、たとえば競争上重要な情報、個人情報、国家安全保障上重要かさなければ機密の情報などが開示されることによって、むしろ間接的ではあるがおそらく数量的には評価することのできないような損失がもたらされることがある。

技術の進歩に比べて、法的ガイダンスはかなり遅れている。国内レベルでも十分でなく、国際的なレベルではほとんど存在しない。法的な調整が達成されるべき重大な目標である。

信頼性の確立

情報システムが本来意図したとおりに動き、予想外の障害、または問題がないということをユーザが信頼できなければならない。

Otherwise, the systems and their underlying technologies may not be exploited to the extent possible and further growth and innovation may be inhibited. Access to secure networks and establishment of security standards have already emerged as general user requirements. Loss of confidence may stem equally from outright malfunction or from functioning that does not meet expectations.

Uncertainties may be met and confidence fostered by building consensus about use of information systems. Accepted procedures and rules are needed to provide conditions to increase the reliability of information systems. Developers, operators and users of information systems deserve reassurance as to their rights and obligations, including responsibility for system failures. Clear, uniform, predictable rules should be in place to ease and encourage growth and exploitation of information systems.

The security of information systems is an international issue because information systems and the ability to use them frequently cross national boundaries. It is a problem that may be ameliorated by international co-operation. Indeed, given the disregard of information systems for geographical and jurisdictional boundaries, agreements are best promulgated and accepted on an international level.

Experience in other sectors involving new technologies with the potential for serious harm reveals a three-part challenge: developing and implementing the technology; providing for avoiding and meeting the failures of the technology; and gaining public support and approval of use of the technology. The air transport industry has been fairly successful in implementing safety techniques and requirements. They facilitate the smooth functioning of air transport and inspire public confidence. Similarly, the shipping industry has successfully used ship certification systems to rank safety of vessels. The field of biotechnology is now grappling to meet the requirements of permitting technological development and preventing harm from exploitation of the technology and subsequent loss of public support. For information and communication technologies, the goal of avoiding and meeting failures of the technology includes the additional task of preventing and handling actual or potential intrusions to information systems.

SECURITY OF INFORMATION SYSTEMS

Security of information systems is the protection of availability, confidentiality and integrity. Availability is the characteristic of information systems being accessible and usable on a timely basis in the required manner. Confidentiality is the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner. Integrity is the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. The relative priority and significance of availability, confidentiality and integrity vary according to the information system.

そうでなければ、システムとその基礎技術は、可能性があってもより以上の開発は望めないだろうし、また進歩と革新が妨げられるかもしれない。ユーザの一般的な要求として、安全なネットワークへのアクセスおよびセキュリティの標準の確立がすでに浮き彫りになっている。信頼性は、明らかな誤動作によっても、期待どおりの機能をしないことによっても、同様に失われる。

情報システムの利用に関しては、コンセンサスを形成することで、不確実性を減らし、人々の信頼を築くことができよう。情報システムへの信頼性を増大させるには、一般的に受け入れられる手続きと規則が必要である。情報システムの開発者、オペレータ、およびユーザは、当然のことながら、システム障害に関する責任を含む自らの権利と義務を再確認すべきである。明瞭で統一がとれ、しかも予測可能な規則を設定して、情報システムの一層の進歩と開発を容易にし、促進すべきである。

情報システムのセキュリティは、情報システムそのものならびにそれを利用する能力が頻繁に国境を越えるものであることから、国際的な問題である。こうした問題は、国際的な協力によって、改善可能である。実際、情報システムは地理的境界や管轄権による境界を無視しているため、協定を国際レベルで広め、承認するのがもっとも好ましい。

新たな技術によって危害がもたらされる可能性を有している他の部門における経験から、3つの部分から成る課題が明らかになった。「技術の開発および実施」、「技術に含まれる障害を回避しまたこれに対処するための備え」、および、「技術の使用に対する公衆の支持と承認の取得」である。航空運輸業界は、安全技術を実現し要件を満たすのにかなり成功を収めている。同業界は空輸が円滑に行われるようにし、公衆に信頼感を抱かせている。同じように海運業界も、船舶登録システムをうまく活用して、船舶の安全性のランク付けを行っている。バイオテクノロジーの分野は、技術開発を許可し、技術開発がもたらす生じる危害や、それによって公衆の支持を失うのを防ぐための要件を満たそうと、現在奮闘中である。情報技術および通信技術の場合、技術の障害を防止し、要件を満たすという目標には、情報システムへの実際の侵入またはその恐れを防止し、処理するという作業が加わる。

情報システムのセキュリティ

情報システムのセキュリティとは、可用性、信頼性、および完全性の保護である。可用性とは、情報システムが必要なときに即時にアクセスでき利用できることである。信頼性とは、許可されている時に許可された方法で、公認された人物、実体およびプロセスに対してのみデータと情報が開示されるということである。完全性とは、情報システムが正確かつ完全であること、かつ正確さと完全性が保たれることである。可用性、信頼性、および完全性の相対的な優先度と重要性は情報システムにより変化する。

Threats to Information Systems

Technological development, technical problems, extreme environmental events, adverse physical plant conditions, human frailty, and inadequacies of social, political and economic institutions all present challenges to the smooth functioning of information systems. Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. They range from cataclysmic events to minor, daily inefficiencies. Down-times, for example, may be caused by one large break-down or frequent slow-ups or service degradations. The frequency and duration of disturbances, however minor, should be considered when planning for security. Large and small events may be equally disruptive to system functioning and use and equally debilitating to the organisation's effective operation.

Technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They may be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads or other operational or quality problems. The difficulty may arise in an internal system component (system hardware and peripherals, such as a memory unit, a networked collection of computer systems or a distributed system; application and operating system software, such as a compiler or editor; LANs), an external system component (telecommunication circuits, satellites) or from the interaction of different parts of the system.

Technical problems may be caused by intentional attacks on the system. Viruses, often introduced into the system via infected software, parasites, trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort or destroy normal system functions.

The difficulty of providing security for networks and information is compounded in multiple-vendor environments. For example, a significant problem is the availability of access-control software, a commonly-used security measure, that is compatible with the entire system in a multiple-vendor environment. In order to facilitate development of effective security for information systems, standards bodies, governments, and vendors and users of information systems must agree on standards for security measures.

Physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms, and excessive heat and humidity. The information system may be housed in a building, in which, in addition to computers and communication lines located throughout the building, there may be dedicated computer rooms and data storage rooms. Connections for power supply and communication may lead to and from the building. Adverse physical plant conditions may arise from breach of physical security measures, power failures or surges, air conditioning malfunction, water leaks, static electricity and

情報システムに対する脅威

技術開発、技術上の問題点、極度の環境事象、物理的施設条件、人間の欠点、社会的、政治的および経済的な施設の不適合は、いずれも情報システムの円滑な機能を阻害する要因である。情報システムに対する脅威は、意図的な行為または故意でない行為から生じ、内部または外部からもたらされる。これらの脅威は、社会的大変動をもたらすような事象から、ごく些細な日常的な非効率までと、実に幅広い。たとえばダウンタイムは、1回の大規模な故障によることもあれば、頻繁なスローアップまたはサービスの低下によることもある。セキュリティに関する計画を立てる際には、たとえ些細なものであっても、妨害の頻度と継続時間を考慮に入れるべきである。大きな事件であっても小さな事柄であっても、システムの操作や利用に与える損害は同等の場合もあり、また組織の機能の効率を低下させる点では同じである。

情報システムを失敗に陥らせる技術的な要因は多数あり、よく理解されていない場合もある上、常に変化し続けている。バグ、オーバーロード、その他の操作上または品質上の問題点が原因で起こるコンピュータや通信のハードウェアまたはソフトウェアの障害もしくは誤動作もこうした要因の一部である。問題は、内部のシステム構成要素(メモリ・ユニット、コンピュータシステムのネットワーク化による集合、分散システムなどのシステム・ハードウェアおよび周辺装置、コンパイラやエディタなどのアプリケーションやオペレーティング・システム・ソフトウェア、LAN)または外部のシステム構成要素(通信回線、衛星)からくることもある。システムの様々な部分が相互に作用しあって問題を起こすこともある。

システムが意図的に攻撃されて技術上の問題点ももたらされることもある。正常なシステム機能を崩壊させたり歪めたり破壊するのに使われる技術的手段としては、感染したソフトウェアを通じてシステムに持ち込まれることが多いウィルス、寄生虫、トラップ・ドア、トロイの木馬、ワーム、論理爆弾などがある。

ネットワークおよび情報に対するセキュリティ対策はただでさえ難しいが、複数ベンダの製品を使用している場合にはさらに困難となる。たとえば、一般にセキュリティ手段としてよく利用される、複数ベンダ製品で構成されるシステム全体と互換性を持つアクセス制御ソフトウェアおよび一般的なセキュリティ手段が手に入るかどうかは深刻な問題となる。情報システムの効率的なセキュリティの開発を容易にするためには、セキュリティ手段に関する標準について、情報システムの標準化団体、政府、ベンダ、およびユーザが合意をしなければならぬ。

情報システムに対する物理的脅威は、「極度の環境事象」と、「不完全な物理的施設条件」の2つに大きく分けられる。極度の環境事象としては、地震、火災、洪水、雷雨、過度の熱や湿度が挙げられる。コンピュータおよび通信回線が建物全体に設置されている上に、専用のコンピュータ室やデータ格納室を持つ建物に情報システムが収容されている場合がある。電源や通信のための接続は、建物の外部と通じている。不完全な物理的施設条件は、物理的セキュリティ手段の不履行、電源異常やサージ、空調の機能不全、水滴れ、静電気、塵埃などから生じ得る。ある組織は、その構内での誤りによって直接に影響を受ける場合もあれば、電源供給や電気通信チャネルなど外部の致命的な箇所でのミスによって間接的に影響を受ける場合もある。

dust. An organisation may be affected by lapses either directly at its premises or indirectly at a vital point outside the organisation, such as power supply or telecommunication channels.

Human beings and the institutions they establish to reflect their values, whether social, economic or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users -- employees, consultants, customers, competitors or the general public -- and their various levels of awareness, training and interest compound the potential difficulties of providing security.

Lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users may not be aware of the potential for harm from system misuse. Poor security practices abound. Operators and users may not take even the most rudimentary security measures.

The choice of a password, a nearly universal user activity and usually a user's first activity on a system, provides a striking example. Although passwords are employed to control access to most information systems, few users are instructed on the need for password security, on the manner in which to create a password or on penalties for misuse of the system. Without guidance, many users choose obvious passwords that may be easily ascertained, such as family or pet names, joke words or words related to the task. After logging in to the system, untrained users may leave active terminals connected to network systems unattended, display passwords on the side of terminals, fail to create backup data files, share user identification codes and passwords, and leave open access-control doors into high security areas. These are threshold security problems that arise from entering a room, switching on a computer or terminal, possessing a password and logging in.

Errors and omissions may occur in gathering, creating, processing, storing, transmitting, and deleting data and information. Failure to back up critical files and software multiplies the negative effects of errors and omissions. If files have not been backed up, the organisation may incur significant expense in time and money in recreating them.

Intentional misuse of authorised system access and unauthorised system access ("hacking") for the purposes of mischief, vandalism, sabotage, fraud or theft are additional serious threats to system and organisational viability. Unauthorised copying of software (software piracy), for example, is widespread. Popular conception holds that the greater part of threats to information systems comes from external sources. On the contrary, persons who have been granted authorised access to the system may pose a larger threat to information systems. They may be honest, well-intentioned employees who, owing to fatigue, inadequate

人間や、人間の社会的、経済的または政治的な価値観を反映するものとして人間が設定した制度、またそのような制度の欠如も、セキュリティにとって問題をもたらす。システム・ユーザは、従業員、コンサルタント、顧客、競争他社あるいは一般大衆など実に多彩であり、またかれらの意識、訓練および関心のレベルも様々であることから、セキュリティを提供することが一層困難になる。

セキュリティおよびその重要性に関する訓練やフォローアップが行われないと、情報システムの適切な利用に対していつまでも無関心な状態が続く。オペレータやユーザは、適当な訓練を受けなければ、システムの誤った利用によって危害を蒙る可能性があることを意識しない。つまり、セキュリティにとって好ましくないような使い方がはびこってしまう。オペレータやユーザは、ごく初歩的なセキュリティ手段ですらとらないかもしれない。

パスワードの選択は、ほとんどすべてのユーザが行い、しかもたいていはシステム上で最初に行う作業であるが、これについて印象的な例が見られる。ほとんどの情報システムで、それに対するアクセスを制御するためにパスワードが使用されているにもかかわらず、パスワードのセキュリティの必要性、パスワードの決め方、システム誤用に対する罰則に関して、なんらかの指示を受けたユーザはごくわずかしかない。指針を与えられなければ、ユーザの多くは、家族やペットの名前、冗談のような言葉、仕事に関連する語などの簡単に突き止められる明白なパスワードを選択する。システムにログインした後にも、訓練を受けていないユーザは、ネットワーク・システムに接続した活動状態の端末をそのままにして席を離れる、端末の側面にパスワードを表示しておく、バックアップ・データ・ファイルの作成を怠る、ユーザ識別コードやパスワードを共用する、セキュリティの必要性が高い領域へのアクセスの入り口を開いたままにしておく、といったことをしでかすかもしれない。これらは、部屋に入る、コンピュータまたは端末のスイッチを入れる、パスワードを与えられる、ログインするといった活動から生じる初歩的なセキュリティの問題点である。

エラーや怠慢は、情報やデータの収集、作成、処理、保存、伝送、および削除といった作業において生ずることがある。重大なファイルやソフトウェアのバックアップを作成しそこなうと、エラーや怠慢の悪影響がさらに大きくなる。ファイルのバックアップを怠っていた場合、組織はそれを作成し直すのに相当な時間と金銭を費やすことになる。

いたずら、破壊行為、妨害行為、詐欺、または盗みの目的で、権限が与えられているシステム・アクセスの意図的悪用および無権限システム・アクセス(「ハッキング/クラッキング」)を行うことも、システムの能力や組織の可能性に深刻な脅威を及ぼすことになる。一般には、情報システムに対する脅威のかかなりの部分は外部からくると考えられている。しかし、それに反して、システムへのアクセス権を与えられている人の方が、情報システムにとってより大きな脅威となる可能性がある。アクセス権を与えられている人たちは、誠実で悪意のない社員が、疲労、不十分な訓練、または不注意のために、うっかり大量のデータを消してしまう場合がある。また、不満を抱いていたり不誠実な社員が、許可

<p>training or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorised access to tamper deliberately with the system for their own enrichment or to the detriment of the organisation.</p> <p>Computer programs are an important element of information systems and a potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality and integrity of that system by overloading the system, changing the list of authorised users of certain parts of the system or altering data or information in the system. Violations of provisions of licensing agreements relating to the information system (e.g., software licensing agreements, database licensing agreements) may pose an additional security threat. Unauthorised alteration of the licensed program, for example, may trigger malfunctions as the modified software interacts with other parts of the system. Disclosure of proprietary information may damage an organisation's competitive position.</p> <p>Proper procedures must extend beyond the computer terminal and communication lines to the entire information arena. Improper handling of data and information storage media (whether paper, magnetic or other) and improper handling and disposal of discarded computer printouts may lead to security breaches. Computer printouts may contain proprietary or competitive information or clues regarding system access. Yet, many companies have no policy for their disposal. Once used for the organisation's purpose, they are considered worthless and discarded along with the day's used envelopes and pencil shavings. There may, however, be no expectation of privacy in trash, at least in trash that is outside the premises.</p> <p>Insufficient use of systems may also lead to security problems, such as maintaining information availability or integrity in the event of shortages of qualified personnel, whether as a result of employees changing jobs, the introduction of new technologies requiring new skills, or work slowdowns, stoppages or strikes.</p> <p>Social, political and economic institutions have not kept pace with technological development and growth in use of information systems. The price is uncertainty and lack of uniformity, which increase expense, cause delays and, if permitted to continue, might impede future growth. There is a glaring deficiency of codes of practice, standards, and legal guidance and apportionment of legal rights and obligations.</p> <p>Harm Resulting From Security Failures</p> <p>Security failures may result in direct and consequential losses. Direct losses are those to: the hardware, including processors, workstations, printers, disks and tapes and communication equipment; software, including systems and applications software for central and remote devices; documentation, including specifications, user manuals and operating</p>	<p>されたアクセス権を悪用または濫用し、自分の利益のためや組織に損害を与えるためにシステムに故意に変更を加える可能性もある。</p> <p>コンピュータプログラムは情報システムの重要な要素であり、情報システムに対する脅威の温床となる恐れがある。ウィルスが入ったプログラムが情報システムの中に持ち込まれると、システムがオーバーロードになったり、システムの特定の部分について権限のあるユーザのリストが変更されたり、システムに入っているデータや情報が変更されたりすることによって、そのシステムの可用性、機密性、完全性が影響を受ける。ソフトウェア・ライセンス契約の規定違反も、セキュリティに対する脅威になりうる。たとえば、ライセンス・プログラムを許可なしに変更すると、変更後のソフトウェアがシステムの他の部分と影響しあって誤動作を招くことがある。専有情報の開示は、競争における組織の立場を損なうことにもなる。</p> <p>コンピュータ端末や通信回線の範囲にとどまらず情報の領域全体で、適切な手順をとるようにしなければならない。磁気媒体の取り扱いが不適切であったり、不用になったコンピュータの印刷出力の取り扱いや廃棄方法が不適切であると、セキュリティの違反につながる可能性がある。コンピュータの印刷出力には、財産と見てよい専有情報や競争上重要な情報が入っていたり、システム・アクセスの鍵となる情報が載っていたりする。ところがほとんどの会社は、その廃棄処分に関する方針を定めていない。いったん会社が目的とする事柄に利用してしまえば、それらは価値のないものとみなされ、毎日出てくる使用済み封筒や鉛筆の削り屑といっしょに捨てられる。ただし、ごみ箱の中、少なくとも施設外のごみ箱の中にはプライバシーを期待することはできない場合もある。</p> <p>システムを十分利用しないことも、セキュリティ上の問題につながる可能性がある。たとえば、従業員の職務変更、新たな技能を必要とするような新技術の導入、あるいは怠業、作業中止、ストライキなどいずれの結果であれ、有資格要員の不足が生じたような場合における情報の可用性または完全性の維持といった問題が生じる。</p> <p>社会的、政治的および経済的な制度は、技術開発や情報システムの利用の伸びと歩調を揃えてきたわけではない。価格は不確実であり、統一性を欠いている。そのため支出がかさみ、遅れの原因となり、またその継続を許可される場合には将来の成長を妨げることにもなりうる。実施規則、標準、ならびに法的権利と義務の法律的指導や配分といった面での欠陥が目につく。</p> <p>セキュリティの欠如によって生じる被害</p> <p>セキュリティが欠如していると、直接的および間接的な損害がもたらされることがある。直接的な損害とは、プロセッサ、ワークステーション、プリンタ、ディスクおよびテープ、通信装置などのハードウェア、中央およびリモート装置のシステム・ソフトおよびアプリケーション・ソフトなどのソフトウェア、仕様書、ユーザ・マニュアル、操作手順書などの文書、オペレータ、ユーザ、管理、技</p>
--	---

<p>procedures; personnel, including operators, users, and managerial, technical and support staff; and physical environment, including computer rooms, communications rooms, air conditioning and power supply equipment. Although direct losses may account for a small percentage of total losses arising from a security failure, nonetheless, the absolute investment in developing and operating the system will usually have been significant. The system requires protection in its own right as the container and channel for the data and information. The need to protect the system and the manner of doing so are inextricably linked to protecting the data and information that the system stores, processes and transmits in order both to preserve the availability, confidentiality and integrity of the data and information and to prevent alteration or damage of the container and channel through introduction of data and information, such as viruses, that may have a deleterious effect on operation and use of the system.</p> <p>A consequential loss may occur when an information system fails to perform as intended. Consequential losses arising from security failures may include: loss of goods, other tangible assets, funds or intellectual property; loss of valuable information; loss of competitive advantage; reduction in cash flow; loss of orders or business; loss of production efficiency, effectiveness or safety; loss of customer or supplier goodwill; penalties from violation of statutory obligations; and public embarrassment and loss of business credibility. Consequential losses account for most of the losses arising from security lapses. In light of this fact, protection against consequential loss, which, above all, means protecting the data and information, must be a top priority.</p> <p>Enhancing Security</p> <p>The goals of confidentiality, integrity and availability must be balanced both against other organisational priorities, such as cost-efficiency, and against the negative consequences of security breaches. The cost must not exceed the benefit. Similarly, from the viewpoint of deterring those who would attempt to enter information systems to view, manipulate or obtain information, security controls should be sufficient to render the costs or the amount of time required greater than the possible value to be gained from the intrusion.</p> <p>Adequate measures for security of information systems help to ensure the smooth functioning of information systems. In addition to the commercial and social benefits of information systems already mentioned, security of information systems may assist in the protection of personal data and privacy and of intellectual property in information systems. Similarly, protection of personal data and privacy and of intellectual property may serve to enhance the security of information systems.</p> <p>The use of information systems to collect, store and cross-reference personal data has increased the need to protect such systems from unauthorised access and use. Methods to protect information systems include user verification or authentication, file access control, terminal controls and network monitoring.</p>	<p>術およびサポート・スタッフなどの要員、コンピュータ室、コミュニケーション室、空調装置、電源装置などの物理環境に対する損害である。直接的な損害は、セキュリティの失敗から生じる損害全体のうちのわずかな比率を占めるに過ぎない。それにもかかわらず、システムの開発と稼働に対して制限なく投資することは重要な意味を持つだろう。システムは、データおよび情報の格納容器として、また情報のチャネルとして、それ自体の権利に対する保護を必要とする。情報の可用性、信頼性、一貫性を保護すると同時に、システムの動作と使用に有害な影響を与えるウイルスなどのデータおよび情報の持ち込みによって情報の格納容器およびチャネルが変更または損傷されるのを防止するために、システムを保護する必要性および保護の仕方は、システムが保存し、処理し、伝送するデータおよび情報の保護と切っても切れない関係がある。</p> <p>間接的な損失は、情報システムが当初の目的どおりに働かなかったときに生じるかもしれない。セキュリティの失敗から生じる間接的な損失は次の事項を含む。： 物品およびその他物理的な資産、資金、知的財産権の損失； 価値の高い情報の損失； 競争上優位の失墜； キャッシュフローの減少； 注文や取引の損失； 生産における効率性、安全性の低下； 顧客や供給者の信用の失墜、法的義務の違反による懲罰、公共の混乱とビジネス上の信頼の失墜。間接的な損失は、セキュリティの失敗から生じる損失のほとんどを占める。この事実を考えると、間接的損失に対する防護、とりわけデータと情報の保護は、最優先すべき事柄と言える。</p> <p>セキュリティの強化</p> <p>機密性、完全性および可用性の目標は、費用効率など組織の他の優先順位とセキュリティ侵害の悪影響の両方と対照して考えなければならない。費用は利益を超えてはならない。同様に、情報を調べたり、操作したり、入手したりするために情報システムに入り込もうとする者を阻止するという見地から、セキュリティ・コントロールは十分なもので、侵入によって得られる価値を超える費用や時間がかかるものでなければならない。</p> <p>情報システムのセキュリティに対する適切な手段があると、情報システムの円滑な機能を確保するのに役立つ。上述したように、情報システムには商業的利益や社会的利益があるが、それに加えて、情報システムのセキュリティは、パーソナル・データおよびプライバシーならびに情報システムの知的所有権を保護する際の支援となりうる。同様に、パーソナル・データおよびプライバシーならびに知的所有権の保護は、情報システムのセキュリティを保護する助けとなる。</p> <p>パーソナル・データの収集、保存、相互参照に情報システムが使われることによって、システムを無権限のアクセスや使用から保護する必要が増している。情報システムを保護する方法には、ユーザの確認または認証、ファイルのアクセス・コントロール、端末コントロールおよびネットワーク監視などがある。このよ</p>
---	--

Such measures generally contribute both to the security of information systems and to the protection of personal data and privacy. It is possible that certain measures adopted for the security of information systems might be misused so as to violate the privacy of individuals. For example, an individual using the system might be monitored for a non-security-related purpose or information about the user made available through the user verification process might permit computerised linking of the user's financial, employment, medical and other personal data. The principles of the Guidelines (for example, the Proportionality Principle and the Ethics Principle) and those of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data give guidance in achieving compatible realisation of the goals of security of information systems and protection of personal data and privacy.

Information systems may include hardware, computer programs, databases, layout designs for semiconductor chips, data and information, elements of which may be protected by intellectual and industrial property laws. Intellectual property in information systems is intangible, may cross borders virtually imperceptibly, and may be vulnerable to theft by the effort of one finger in a matter of seconds without taking the original and without leaving a trace. Security of information systems may reinforce the protection of intellectual property by limiting unauthorised access to components of the system, such as software or competitive information.

Since contracts, transactions and disputes relating to information systems may involve parties, actions and evidence in many different jurisdictions, it may be useful to clarify existing rules or presumptions or to establish new ones with regard to the law applicable in matters relating to the security of information systems. Given that disputes related to the security of information systems may involve complex factual situations as well as parties, actions and evidence that may be situated in multiple jurisdictions, it may also be advisable to develop non-judicial means, including arbitration, for resolution of disputes.

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

Aims

This section of the Guidelines sets forth the purposes to be served by their formulation and adoption by governments and the private sector. The Guidelines are intended to assist the further development and use of information systems. In order to do so, it is viewed as necessary to raise awareness of risks to information systems and to provide reassurance as to the reliability of information systems and their provision and use. In recognition of the ubiquity of information systems, governments and the private sector are urged to co-operate to create an international framework for security of information systems.

うな対策は一般には、情報システムのセキュリティとパーソナル・データおよびプライバシーの保護の両方に対して効果がある。しかし、情報システムのセキュリティのために採用した対策が、個人のプライバシーを侵害するように誤用される可能性もある。たとえば、システムを使用している個人がセキュリティ以外の目的のために監視されたり、ユーザ確認処理によって入手できるユーザ情報によってユーザの金融、雇用、医療その他のパーソナル・データをコンピュータでリンクすることができる。ガイドラインの各原則(たとえば比例原則、倫理原則など)と「プライバシー保護およびパーソナル・データのトランスボーダ・フローに関する OECD のガイドライン」の原則は、情報システムのセキュリティとパーソナル・データおよびプライバシーの目標の両立可能な関係を実現する手引きとなる。

情報システムには、ハードウェア、コンピュータプログラム、データベース、半導体チップのレイアウト設計、データおよび情報、知的財産権および工業所有権法によって保護されているものなどがある。情報システムにおける知的財産権は無形であり、実際には感知できない形で越境して侵入して行くことがあり、しかもオリジナルには手をつけず、跡も残さずに、ほんの数秒で指 1 本使うだけで容易に盗まれてしまうことがある。情報システムのセキュリティは、ソフトウェアや競争情報など、システムのコンポーネントに対する無権限アクセスを制限することによって知的財産権の保護を強化することができる。

情報システムに関する契約、取引および紛争には、実に様々な管轄権下にある当事者、行為、および証拠が関わってくるがあるので、情報システムのセキュリティに関する事項に適用しうる法律に関して、既存の規則または推定を明らかにしたり、新たな規則や推定を確立することが有用かもしれない。情報システムのセキュリティに関する紛争には、複雑な実情や、複数の管轄権下にある当事者、証拠、行為が関与することが多いとすれば、特に国際的レベルでの仲裁など、非司法的な紛争解決手段を確立することが望ましい。

情報システムのセキュリティに関するガイドライン

目的

ガイドラインの第 1 部は、政府および民間セクタによるガイドラインの公的活用と採用の目的に供することである。ガイドラインは、情報システムのさらなる発展と利用を援助する目的のものである。そのためには、必要に応じて、情報システムに対するリスクについての周知を喚起し、情報システムの信頼性とそのための手段やその利用について再確認を行う。情報システムが様々な場で利用されていることを認識し、政府と民間セクタに、共同して情報システムのセキュリティのための国際的な枠組みを作成するよう推奨する。

It is hoped that the Guidelines will contribute to increasing awareness of the importance of security of information systems and to dispelling reluctance to report security breaches, which might permit the compilation of more national and international statistics.

Scope

The Guidelines are intended to apply to all information systems, whether owned, operated or used by public or private entities or for public or private purposes. The information systems may be of a public or private nature and elements of them may be protected by intellectual property or industrial property laws or other laws (e.g., trade secrets, official secrets). The Guidelines are not intended to supersede or otherwise affect the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The objective of the Guidelines is full application at all levels. In particular, parties should strive to avoid the evolution of a dual approach, one for information systems related to national security and one for all other information systems. Notwithstanding these intentions, it is fully accepted that governments may find it necessary to depart from the Guidelines. This is the case in the areas of national security and maintenance of public order ("ordre public"). The fact that governments have the sovereign right to do what they must in these vital areas is recognised in the Recommendation of the Council Concerning Guidelines for the Security of Information Systems. However, it is expected that any departure from the Guidelines will relate more to the section on implementation than to the nine principles. The general idea is that exceptions to the Guidelines would be few and, since they relate to "sovereign" matters, would be of the highest order of importance. Furthermore, it was foreseen that appropriate information relating to departures from the Guidelines, whether involving a public or private information system, would generally be made known to the public and all interested parties.

Definitions

The definition of information systems includes: computer hardware; interconnected peripheral equipment; software, firmware and other means of expressing computer programs; algorithms and other specifications either embedded within or accessed by such computer programs; manuals and documentation on paper, magnetic, optical and other media; communication facilities, such as terminal/customer premises equipment and multiplexers, on the information system side of the network termination point of public telecommunication transport networks as well as equipment for private telecommunication networks not offered to the public generally; security control parameters; storage, processing, retrieval, transmission and communication data, such as check digits and packet switching codes, and procedures; data and information about parties accessing information systems; and user identification and verification measures (whether

「ガイドラインの目的」およびこの「説明のための覚書」の他の部分で述べているガイドラインのその他の目的に加えて、このガイドラインがハッカーおよびハッカーの活動の許容度を抑止するためと、セキュリティ侵害について報告したがる傾向をなくして国内および国際的な統計をさらに収集するために役立つことが望まれる。

範囲

ガイドラインは、公共または民間の実体により、公共目的または私的な目的のために、所有、運用、または使用されているすべての情報システムに適用されることを意図している。これらの情報システムは、公共物または私有物であってよく、これらの要素は、知的財産権法または工業所有権法もしくは他の法律（たとえばトレード・シークレットやオフィシャル・シークレットなど）で保護することができる。このガイドラインはプライバシー保護および個人情報の国外流出に関する1980年のOECDガイドラインに取って代わったり、何らかの効力を及ぼすことを意図したものではない。ガイドラインは、あらゆるレベルで完璧に適用されることを目標とする。特に、当事者は国家安全保障に関連する情報システム用とその他の情報システム用の二重のアプローチを展開することを避ける努力をしなければならない。これらの目的にもかかわらず、政府が特に国家安全保障および社会秩序（「治安」）の維持の領域において、このガイドラインから逸脱する必要があると判断することは、全面的に受け入れられる。政府がこれらの重大な領域で行わなければならない主権を有しているという事実は、「会議勧告」で認められている。ただし、ガイドラインからの逸脱は、9項目の基本原則よりも履行に関する部分に関係すると予想される。専門家の見解によれば、ガイドラインの例外はほとんどなく、また、例外は「主権」問題であるため、最高位の重要度を持つものであろうとのことだった。さらに、ガイドラインからの逸脱に関する適切な情報は、公共の情報システムにかかわるものであるか個人の情報システムにかかわるものであるかを問わず、公衆およびすべての関係者に通知されるであろうの見通しだった。

定義

情報システムとして定義されるものの中には、ハードウェア；周辺装置；ソフトウェア；ファームウェア；およびコンピュータプログラムを表すその他の手段；コンピュータプログラムの内部に格納されたり、アクセスされるアルゴリズムとその他の仕様；印刷媒体および電子媒体に記録されたマニュアルおよび文書；一般に公共には提供されないプライベートの通信網と同様の、公共通信網のネットワーク終端点の情報システムサイドに関する端末や顧客敷地内の装置や多重化装置といった通信設備；セキュリティコントロールパラメータ；チェックディジットやパケットスイッチングコード、手順といった、記憶、処理、検索、伝送、および通信データ；情報システムにアクセスする当事者に関するデータと情報；情報、ユーザを識別したり検証する手段（知識ベース、トークンベース、バイオメトリック、行動、その他のいかなる手段でもよい）がある。この定義は、財産たる専有のデータおよび情報があれば、非専有のものもあり、公的なものも私的なものもサービスかもしれない。この定義は、システムによって伝送されたデータと

<p>knowledge-based, token-based, biometric, behavioural or other). This definition may include elements that are proprietary or non-proprietary, public or private. This definition applies to elements whether or not they interact with the data being transmitted by the system or are necessary for the operation, use and maintenance of the other components of the system.</p> <p>Confidentiality and integrity apply to data and information. The words data and information are repeated in the definition of availability, even though the term "information systems" includes them, in order to emphasise that availability also covers data and information. Confidentiality, integrity and availability may be important for reasons of competitive advantage, national security or in order to fulfil legal, regulatory or ethical obligations, such as fiduciary duties, protection of personal data and privacy or medical confidentiality. Examples of availability are up-time and response time of the information system.</p> <p>Security Objective</p> <p>The Principles of the Guidelines, which follow the Security Objective, express essential concepts to be considered in protecting information systems and providing for their security. The Principles are preceded by a simple declaration of the purpose and goals of security of information systems. Security of information systems is the protection of availability, confidentiality and integrity. In the absence of sufficient security, information systems and, more generally, information and communication technologies may not be used to their full potentials. Lack of security or lack of confidence in the security of information systems may act as a brake on information system development and use and on development and use of new information and communication technologies. One goal, therefore, is the protection of individuals and organisations from harm resulting from failures of security. All individuals and organisations potentially rely on the proper functioning of information systems. Clear examples are the information systems in hospitals, air traffic control systems and nuclear power plants. Security, therefore, is directed at preserving the effectiveness of information systems. In addition to the goal of ensuring that the level of availability, confidentiality and integrity of information systems is not eroded, the security of information systems and the Guidelines are directed toward facilitating the development and use of information systems by individuals and for new and different purposes than those for which they are presently employed as well as toward facilitating the development and exploitation of information and communication technologies.</p> <p>Principles</p> <p>The Guidelines identify nine principles in connection with security of information systems. They are: the Accountability Principle; the Awareness Principle; the Ethics Principle; the Multidisciplinary Principle; the Proportionality Principle; the Integration Principle; the Timeliness Principle; the</p>	<p>の関わりにおいても、システムの他のコンポーネントの操作、利用、保守に必要なものにも適用される。</p> <p>信頼性および完全性は、データおよび情報に適用される。「情報システム」という用語にはデータおよび情報が含まれるにもかかわらず、可用性がデータおよび情報も対象としていることを強調するために、可用性の定義ではデータおよび情報という言葉が繰り返される。信頼性、完全性および可用性は、競争上有利な立場を保つため、国家安全保障のため、または、受託者としての義務あるいはプライベート・データやプライバシーの保護もしくは医療の信頼性など、法律、規則または倫理上の義務を満たすために重要である。可用性を測る指標としては、情報システムの使用可能時間と応答時間の2つがある。</p> <p>セキュリティの目的</p> <p>「セキュリティの目的」に続く「ガイドラインの原則」は、情報システムの保護とそのセキュリティの保持において考慮すべき必須概念を示すものである。情報システムのセキュリティの目的と最終目標の簡単な宣言を、「原則」の前に記載しておけば役立つはずである。情報システムのセキュリティとは、可用性、信頼性、完全性の保護である。セキュリティが十分でない、情報システムおよび、より一般的に言えば、情報および通信技術を最大限に利用することができない。セキュリティが保持されていなかったり、情報システムのセキュリティを信頼できないと、情報システムの開発および使用と、新しい情報技術および通信技術の開発に抑制がかけられる。したがって、1つの目標は、個人および組織をセキュリティの欠如による損害から保護することである。すべての個人および組織は潜在的に、情報システムが正常に機能することに依存している。その明白な例は、病院、航空管制システム、および原子力プラントで使用されている情報システムである。したがって、セキュリティは情報システムの効果を保つことに向けられる。さらに、情報システムの可用性、信頼性、および一貫性のレベルが下がらないようにするという目標に加えて、情報システムのセキュリティとガイドラインは、個人が情報システムを現在の採用目的とは異なる新しい目的のために開発し使用するよう促進すること、情報技術および通信技術の開発と利用を促進する方向にも向けられる。</p> <p>原則</p> <p>ガイドラインでは、情報システムのセキュリティに関して9つの原則を挙げる。9つの原則とは、責任の原則、情報提供の原則、倫理性の原則、多面的考慮の原則、比例性の原則、統合の原則、適時性の原則、再評価の原則、および民主主義の原則である。</p>
--	--

Reassessment Principle; and the Democracy Principle.

Accountability Principle

There should be an express and timely apportionment of responsibilities and accountability with respect to the security of information systems among owners, providers and users of information systems and others. The phrase "other parties concerned with the security of information systems" includes executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and internal and external information system auditors.

Awareness Principle

This principle is meant to assist those with a legitimate interest to learn of or be informed about security of an information system. It is not intended as an opening to gain access to the information system or specific security measures and should not be construed as tending to jeopardise security. The level of information sought pursuant to this principle should be able to be obtained without compromising security.

Owners and providers are included in the Awareness Principle for there may be circumstances in which they, too, may need to acquire information about the security of a system. For example, an owner of a network may enter into an agreement whereby another organisation would use the network to provide services for third parties. The owner may require, as part of the agreement, that certain levels of security be offered or available. In this circumstance, the owner may wish to be able to be informed of the security of the information system. Similarly, an organisation that contracts with a computer or network owner to provide services may desire assurances as to security and the ability independently to verify security. Users are also included in the Awareness Principle. For example, a customer choosing a bank may have a legitimate interest in being generally informed about the existence of security policies and programs of various banks. Depending upon customer demand, security might even come to be used as a marketing tool.

Ethics Principle

Information systems pervade our societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information systems. This principle supports the development of social norms in these areas. Important aspects are the expression of these norms to all members of society and inculcation of these concepts from a very young age.

Multidisciplinary Principle

When devising and maintaining measures, practices and procedures for the security of information systems, it is important to review the full spectrum of security needs and

責任の原則

情報システムの所有者、提供者、ユーザ及びその他の者の間で、情報システムのセキュリティに関して責任 (responsibilities & accountabilities) の明確な割当てが必要である。「情報システムのセキュリティに関係する他の当事者」という句には、経営幹部、プログラマ、保守管理者、情報システム管理者 (ソフトウェア管理者、オペレーション管理者およびネットワーク管理者)、ソフトウェア開発管理者、情報システムのセキュリティに関して責任を負う管理者、および内外の情報システムの監査人が含まれる。

情報提供の原則

この原則は、情報システムのセキュリティについて学習したり知ることに関し、正当な興味を有する人物の援助を目的としている。これは、情報システムまたは特定のセキュリティ手段へのアクセス取得の端緒となることを意図したものではなく、また、結果的にセキュリティを危険にさらすものと解釈してはならない。この原則に従って得られる情報の水準は、セキュリティを危うくすることなしに取得できるものでなければならない。

所有者と提供者は、システムのセキュリティに関する情報を得る必要がありえるので、情報提供の原則に含める。たとえば、ネットワークの所有者は、別の組織がそのネットワークを使用して第三者にサービスを提供する旨の協定を結ぶ場合がある。所有者は、この協定の一部として、特定の水準のセキュリティの提供または使用を要求してよい。この状況において、所有者は、この情報システムのセキュリティについて情報を得たい旨を希望してよい。同様に、コンピュータ所有者またはネットワーク所有者に対してサービスの提供を契約する組織は、セキュリティに関する保証と、単独でセキュリティを検査する能力を希望するかもしれない。ユーザもまた、情報提供の原則に取り込まれる。たとえば、銀行を選択しようとしている顧客は、様々な銀行のセキュリティの方針とプログラムに関して、一般的な情報を与えられるべく当然の興味を抱くかもしれない。顧客の要求によっては、セキュリティが、マーケティング・ツールとして使用されるようになるかもしれない。

倫理性の原則

情報システムは、我々の社会と文化に広く浸透している。情報システムと情報システムのセキュリティを適切に実現し、使用することに関して、規則が生まれつつあり、期待も膨らんでいる。この原則は、これらの領域での社会的規範の発展を支持するものである。重要な側面の1つに、これらの規範を社会の成員全員に示し、これらの概念をごく若い年齢のうちから説き聞かせることがある。

多面的考慮の原則

情報システムのセキュリティの手段、実施方法、手順、および指示を考案し維持する時には、セキュリティの全範囲にわたる必要性と使用可能なセキュリティ手段を再検討することが重要で

available security options. In an organisation, for example, this would involve consultation with technical personnel, management, the legal department, users and others. All these groups will have different perspectives, requirements and resources that should be consulted and combined to produce an optimal level of security for the information system. Similarly, on a policy level, technical standards, codes of practice, legislation, public awareness, education and training for security of information systems may be mutually reinforcing.

From another aspect, this principle acknowledges that information systems may be used for very different purposes and that the security requirements may vary as a result. For example, the civil and military branches of government may have dissimilar needs for security as may different types of businesses or the commercial sector and private individuals.

Proportionality Principle

Every information system does not require maximum security. As it is important that systems not be insufficiently secure, so is it futile to provide security beyond the reasonable requirements of the system. Rather, there is a hierarchy of information systems and their security needs that differs for each organisation. For this reason, there is no one security solution.

In assessing security needs, the information should first be identified and a value assigned. Possible security measures, practices and procedures available to protect the various elements of the information system should be enumerated and the costs of implementing and maintaining each of the security options calculated. The level and type of security should then be weighed against the severity and probability of harm and its costs as well as the cost of the security measures. This analysis should be carried out for the information system in the context of all other relevant procedures and systems, including other information systems.

Integration Principle

Security of information systems is best considered when the system is being designed. Measures for security may be formulated and tested to avoid incompatibility. Overall costs of security may also be reduced. Security is required at all phases of the information cycle -- gathering, creating, processing, storing, transmitting and deleting. Security is only as good as the weakest link in the system.

Timeliness Principle

In the environment of the interconnected information systems that span the globe, the importance of time and place are diminished. It is possible to gain access to information systems regardless of physical location. The Timeliness Principle acknowledges that, due to the interconnected and transborder nature of information systems and the potential for damage to systems to occur rapidly, parties may need to act together

ある。たとえば、ある組織内では、このために技術担当者、管理部門、法律部門、およびユーザに諮問することになるだろう。これらのグループはそのいずれもが、情報システムに最適な水準のセキュリティを産み出すために諮問して組み合わせる必要のある異なる見通し、要件、および資源を有しているだろう。同様に、政策レベルでは、情報システムのセキュリティに関する技術標準、実践規則、法制定、公衆の啓蒙、教育および訓練が、互いに補強しあう関係にあるかもしれない。

別の側面から見ると、この原則は、情報システムを非常に異なる目的のために使用できること、またセキュリティ要件が、結果として変化しうることを示すものでもある。たとえば、政府の文官と軍部は、異なるタイプのビジネスや商業部門および個人の場合と同様に、セキュリティに対するニーズが異なるかもしれない。

比例性の原則

情報システムのすべてが、最大のセキュリティを必要としているわけではない。システムが十分に安全であることが重要であるのと同様に、システムが必要としている以上のセキュリティを提供しても無益である。むしろ、情報システムとそのセキュリティの必要性には階層性があり、それは組織ごとに異なるものである。そのため、1 つですべてを解決するセキュリティ対策というものは存在しない。

セキュリティの必要性を評価するには、まず情報を確認し、それにある価値を割り当てなければならない。情報システムの様々な要素を保護するのに利用可能なセキュリティ手段、実施方法、手順、および指示を列挙し、そのセキュリティ手段のそれぞれを実行し維持していくのにどれだけ費用がかかるかを計算しなければならない。それから、危害の深刻度と可能性およびその被害額、ならびにセキュリティ対策の費用を考慮して、セキュリティの水準とタイプを評価しなければならない。この分析を、その情報システムについて、他のあらゆる関連手順および他の情報システムを含むシステムとの関連において実施しなければならない。

統合の原則

情報システムのセキュリティは、システムの設計中に検討すると最もよい。互換性がなくなることをないように、セキュリティ手段を設計し、試験することができる。セキュリティの全体的な費用も削減される。セキュリティは、情報の収集、作成、処理、保存、伝送および削除といった情報サイクルのあらゆる段階で必要である。セキュリティの効果は、そのシステムのうちで最も弱体なリンクにおいて発揮される。

適時性の原則

地球的規模の相互接続情報システムの環境下では、時間と場所の重要性が低くなる。物理的な場所に関係なく、情報システムにアクセスすることができる。適時性の原則は、情報システムの相互接続された越境性と、システムに急速に損害が生ずる可能性があるため、情報システムのセキュリティを達成するように当事者たちが迅速に協力する必要があることを認識したものである。セキュリティの侵害によっては、該当する当事者が、公共

swiftly to meet challenges to the security of information systems. Depending upon the security breach, the relevant parties may be members of the public and private sectors and may be located in different countries or jurisdictions. This principle recognises the need for the public and private sectors to establish mechanisms and procedures for rapid and effective co-operation in response to serious security breaches.

Reassessment Principle

This principle recognises that information systems are dynamic. System technology and users, the data and information in the system and, accordingly, the security requirements of the system are ever-changing. The information systems, their value, and the severity, probability and extent of potential harm should, therefore, undergo periodic reassessment. Follow-up is as important as implementation, especially in light of new technological developments, whether those adopted by the system owner or those available for use by others.

Democracy Principle

The security interests of owners, developers, operators and users of information systems must be weighed against the legitimate interests in the use and flow of information with the aim of striking a balance in accordance with the principles of a democratic society. Those unfamiliar with security of information systems may presuppose that security of information systems may lead only to restrictions to access to and movement of data and information. On the contrary, security may enhance access and flow of data and information by providing more accurate, reliable, and available systems. For example, harmonization of technical security standards will help to prevent data and information islands and other barriers to data and information flows.

Implementation

National governments should strive to ensure that territorial subdivisions in their countries are aware of the Guidelines and their implications for areas within the competence of the subdivisions. They should communicate at political level to all territorial subdivisions the text of the Guidelines, undertake every effort to urge their implementation, and consult as to difficulties that may arise.

Self-regulation may take the form of codes of conduct or practice developed and adopted by individual organisations, industry or professional associations or public sector agencies.

Policy Development

Worldwide harmonization of standards

There is a need for creation of appropriate technical security standards (including product and system evaluation criteria) with the widest possible geographic range of applicability. Their development should be the product of collaboration between,

部門および民間部門の構成員である場合もあり、異なる国または管轄下にある場合もある。そのため、同原則は、深刻なセキュリティ侵害に対処するため公共機関および民間企業が迅速かつ効率的に協力する組織や手順を策定することの必要性を認めている。

再評価の原則

この原則は、情報システムが動的であることを認識したものである。システム技術およびシステム・ユーザと、そのシステムによって操作されるデータおよび情報は、常に変化している。情報システムとその価値、起こりうる危害の深刻度と確率と範囲は、定期的に再評価されなければならない。フォローアップすることは、実行と同じくらい重要である。特に新たな技術開発のことを考えると、それがシステム所有者が採用したものであれ、他者に広く利用されるものであれ、フォローアップが重要となる。

民主主義の原則

情報システムの所有者や開発者、オペレータ、ユーザのセキュリティに対する関心は、民主主義社会の原則にのっとったバランスを保つ目的で情報を利用し、流通させることに対する合理的な利益に集中するであろう。情報システムのセキュリティに詳しくない人は、情報システムのセキュリティが、データおよび情報へのアクセスと、これらの移動に対する制限をもたらすだけだと予想するかもしれない。その反対に、セキュリティは、より正確で信頼性の高い、可用性の高いシステムを提供することによって、データと情報のアクセスとフローを拡張しうるのである。たとえば、技術的なセキュリティ標準を調和させると、データと情報の孤立化を防ぎ、データと情報のフローに対するその他の障壁を取り除くのに役立つ。

実施

各国の政府は、それぞれの領土内に所属する地域に対してガイドラインおよびその地域の権限の範囲に関係する事項を周知させるべきである。地域全土に対して、ガイドライン全文を政治的レベルで通知し、その実施を促すためあらゆる努力を払い、生じる可能性のある問題点について協議すべきである。

自主規制は、個々の組織、産業組合、または公共機関が開発し採用する実施規則、実践規則の形態としてもよい。

施策の開発

全世界での標準の整合性

地理的にできる限り広い範囲に適用できるような、適切な技術的セキュリティ標準(製品およびシステムの評価基準も含む)を作成する必要がある。それは、政府、標準団体、および情報技術関連のベンダとユーザの協力の中から生まれたものでなけれ

among others, governments, standards bodies, and vendors and users of information systems.

While seeking harmonized standards, it should be recalled that, as to individual situations, there can be no one security solution. Security needs vary considerably from sector to sector, company to company, department to department, and, as to given information systems, over time. Lack of an informed and balanced understanding of users' needs may create a significant risk of "off-target" technology standardisation. A productive first step is recognition of the inherent diversity and heterogeneity of users' needs for information system safeguards.

Promotion of expertise and best practice

Governments, public sector agencies, industry and professional associations and organisations should work together to promote expertise and to develop and promote awareness of concepts of "best practice" in the field of security of information systems. This may include notions of risk analysis, risk management, insurance, or audits. The particular program adopted may vary from organisation to organisation and from sector to sector. The security requirements of the banking sector, for example, may differ from those of other sectors.

Contract formation and validity

The goals of parties to an electronic transaction are not very different from those in a paper transaction. Generally, the participants in an information transfer, whether electronic or non-electronic, want to know that the information came from the person who purports to have sent it, that it is received only by persons intended to receive it, and that it arrived in the intended form, unaltered and unmanipulated. While the goals of parties to electronic and non-electronic transactions may be basically the same, the manner of achieving these aims are not. They differ as a function of the means of creation, use, transmission, storage, and access to electronic and non-electronic information. The manners in which the two types of information are protected perforce differ as well.

The challenge is to bring to electronic dealings the same level of confidence that presently exists for paper transactions. This may be accomplished in several ways. First, existing rules may be applicable to electronic situations. As necessary, existing rules may be modified and new ones developed. Technological means may also be employed. Further study and refinement of commercial laws involving electronic transactions might be useful, including rules relating to the validity of electronic signatures, the formation and validity of contracts created and executed in information systems, and enforcement of and liability for such contracts.

Allocation of risks and liability

There seems to be a dearth of rules relating to allocation of risks and liability for damage arising from security lapses. The relevant parties may include vendors, distributors, telecommunication operators, service providers and users. Several systems may be involved in an information transfer, often including systems outside the ownership or control of the

ばならない。

整合性のとれた標準を求める一方で、個々の状況に関しては、1 つですべてを解決できるようなセキュリティ対策などないことを思い出さなければならない。セキュリティのニーズは、部門ごと、会社ごと、部署ごとに、また一定の情報システムであっても時によって、実に大きく異なる。ユーザのニーズについての知識がなく、他のものに比べて十分理解されていないために、「的はずれの」技術標準化が行われる危険性が大きくなることもある。情報システムのセキュリティに関するユーザのニーズが本質的に多様であり、均質ではないことを認識することが、実現へ向けての第 1 歩である。

専門技術の促進と最適行動

政府、公共機関、産業組合、および組織は、協力して情報システムのセキュリティの分野における専門技術を促進し、「最適行動」の概念を作成する必要がある。これには、リスク分析、リスク管理、保険、または監査の概念などがある。採用するプログラムは、組織や部門によって異なる。たとえば銀行業界には、他の部門とは異なるセキュリティ要件がある。

契約書の作成および有効性

電子的取引の当事者が目標とするところは、書類による取引における目標とそれほど違わない。一般に、情報伝送に参加する者は、それが電子によるものであれ電子以外によるものであれ、送ったという人から実際に情報が送られていること、受け取るべき人だけが情報を受け取っていること、また意図された通りの形式で、変更されず、操作もされないで着いたことを確認したがる。電子的取引および電子以外の取引の当事者たちの目標とするところは基本的には同じかもしれないが、その目的達成の方法は同じではない。電子的情報と電子以外による情報とは、作成、利用、伝送、保存、および情報へのアクセスの手段が異なるのに応じて違ってくるのである。この 2 種類の情報の保護の仕方も、当然のことながら違ってくる。

課題とされるのは、電子的取引の信頼性水準を、現在の書類による処理と同じ水準にすることである。これを達成する方法はいくつか考えられる。まず、電子的状況に既存の規則を適用できるかも知れない。また必要に応じて既存の規則を修正し、新しい規則を作ることができる。技術的手段を採用することもできる。電子署名の有効性、情報システムで作成され実行される契約の作成と有効性、このような契約の実施と義務に関する規則など、電子的取引にかかわる商法の詳細な研究および改正が役に立つだろう。

リスクの配分と失敗に対する責任

リスクの配分と、セキュリティの失敗から生じた損害に関する責任に関する規則が不足している。関係当事者としては、ベンダ、配給業者、公衆電気通信業者、サービス提供者、およびユーザなどがある。ある情報を伝送するには、複数のシステムが関与することがあり、その情報を処理したり伝送したりする者の所有権や管理の範囲外の外部システムが含まれることも多

<p>information processor or transmitter. The rights and duties of the parties involved may be unclear in cases of mistakes, omissions, failures of the various systems or other mishaps.</p> <p>The need for such rules exists and is illustrated when funds that are electronically transferred between two financial institutions are lost or stolen. Such transfers may involve vast amounts of money, are common financial practice, and are made almost instantaneously and across international boundaries. Where existing rules are not sufficient, further development and refinement on the national and international levels on the manner in which to assign liability in cases of fraudulent or negligent wire transfers is supported.</p> <p>Sanctions</p> <p>Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime (See, e.g.: Organisation for Economic Co-operation and Development (1986), Computer-Related Crime: Analysis of Legal Policy , ICCP Series No. 10; Council of Europe (1989), Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems; United Nations (1990), Statement on Computer-related Crime, Report of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August-7 September; and International Chamber of Commerce (1988), Computer Related Crime and Criminal Law: An International Business View , Position Paper No. 11, June). National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.</p> <p>At the same time, it is recognised that many factors may aggravate or mitigate the seriousness of the conduct: the specific intent of the actor, the type of data affected (e.g., national security or medical data), the extent of the harm, and the extent to which the actor exceeded authorisation. For minor violations, the use of administrative sanctions, such as the imposition of non-penal fines by an administrative agency, is considered by some nations (especially in the area of data protection) to be sufficient. Other types of sanctions may include, for example, disciplinary measures against civil servants or civil sanctions.</p> <p>The development of legislation in OECD Member countries has</p>	<p>い。誤りや怠慢、各種システムの故障またはその他の問題が起きた場合に、関係当事者の権利と義務がはっきりしていないことがある。</p> <p>このような規則に対するニーズが示されるのは、2つの金融機関の間で電子送金された資金が喪失したかあるいは盗まれたというような場合である。この種の伝送には多額の金に関与し、しかも金融業ではよく行われることであり、国境を越えてほとんど瞬間的に行われている。既存の規制では不十分で、不正または怠慢な電信が行われた場合に責任をどう割り振るかについては、国内レベルと国際レベルのいずれでも、さらなる開発、改良が必要である。</p> <p>制裁</p> <p>情報システムの濫用に対する制裁は、情報システムに依存している人の利益を情報システムおよびそのコンポーネントの可用性、機密性、および完全性に対する攻撃による損害から保護する重要な手段である。このような攻撃の例としては、ウィルスやワームの混入、データの改変、データへの不法アクセス、コンピュータによる詐欺または偽造、コンピュータプログラムの無許可複製により、情報システムに損害を与えたり破壊したりすることなどが挙げられる。このような損害に対抗して、各国は様々な方法で違反行為を規定し対応する決定を行ってきた。各国の刑法が適用されるべきコンピュータ関連犯罪の中核について、国際協定が生まれつつある。これは、最近20年間のOECD加盟国におけるコンピュータ犯罪とデータ保護に関する法律制裁と、OECD及びその他の国際団体のコンピュータ関連犯罪に対抗する立法作業に反映されている(参照:経済協力開発機構、コンピュータ関連犯罪:法的制裁の分析、ICCPシリーズ第10号、1986年;欧州会議、コンピュータ関連犯罪に関する勧告および犯罪問題に関する欧州委員会の最終報告第R(89)号、1989年;国連、コンピュータ関連犯罪、犯罪防止および犯罪人の扱いに関する第8回国連会議報告書、キューバ、ハバナ、1990年8月27日~9月7日;国際商工会議所、コンピュータ関連犯罪および刑法:国際経営ビュー、政策方針第11号、1988年6月)。国の法律は、情報システムから生ずる危険に十分に適合しているか確認するため、定期的に見直す必要がある。</p> <p>それと同時に、行為者の特定の意図、影響を受けたデータのタイプ(たとえば国家機密や医療データなど)、損害の程度、行為者がどの程度権限を超えたかなど、多くの要因によって罪が重くなったり軽くなったりすることが認められている。軽微な違反の場合は、行政機関による罰金などの行政制裁の適用で十分と考える国もある(特にデータ保護の分野)。この他のタイプの制裁として、たとえば公務員に対する懲戒処分や民事制裁などがある。</p> <p>OECD加盟各国における立法措置はすでに、特にOECDなど</p>
---	---

already led, particularly under the influence of international organisations, including the OECD, to a certain degree of harmonization. In order to further international co-operation in penal matters (including in the areas of mutual assistance, extradition and other international co-operation described below), this harmonization process should be supported and taken into account by countries when reviewing their legislation.

Jurisdictional competence

In addition to the jurisdictional competence of courts in matters relating to the security of information systems, some countries may wish to grant certain administrative agencies rights to impose administrative sanctions.

The transborder character of data flow on the one hand and the mobility of offenders on the other hand may create problems in prosecuting computer criminals. Ideally, there should be harmonized rules on extraterritorial jurisdiction. However, pending the development of such rules, individual countries should review the suitability of their domestic jurisdictional rules to deal with transborder offences. In countries where the doctrine of ubiquity (a crime is committed where one of its elements takes place) is not acknowledged, difficulties arise as to the application of national computer crime laws. In such countries, it may be necessary to introduce special jurisdictional rules, as, for instance, was done in the United Kingdom, where the Computer Misuse Act 1990 claims jurisdiction when the hacker or computer is in the United Kingdom or where the interference makes use of a computer in the United Kingdom.

If a national of a state commits a computer-related crime in another state, problems may also arise when the crime is detected and the perpetrator is in the home country. Many countries do not extradite nationals. In such situations, an extension of the existing rules of extraterritorial jurisdiction (or the possibility of transfer of proceedings (see the following paragraph)) should be considered with a view to creating the necessary prerequisites for a successful prosecution in at least one state.

Mutual assistance and extradition

Mutual assistance agreements, extradition laws, recognition and reciprocity provisions, transfer of proceedings and other international co-operation in matters relating to the security of information systems may facilitate assistance to other countries in their investigations.

Evidence

Improved security of information systems, by enhancing the accuracy, completeness and availability of data and information in the information system and, accordingly, by increasing the ability to rely on data and information in the system, may assist the introduction and use of such evidence in legal and administrative proceedings. Similarly, in legal systems with special formal requirements regarding evidence, clear rules of evidence in both penal and civil legal and administrative proceedings may make information systems more secure by

の国際組織の影響を受けてある程度の協調を実現している。刑罰問題における国際協力(以下で述べる相互援助、外国犯罪人引き渡し及びその他の国際協力)を推進するために、この協調プロセスを維持し、各国が自国の法を見直す際に考慮に入れるべきである。

管轄権限

情報システムのセキュリティに関する問題における裁判所の管轄権限に加えて、特定の行政機関に、行政罰を課する権利を認めてもよい。

データの流れには国境を越える性質がある一方で犯罪者が移動するため、コンピュータ犯罪の訴追に障害が生ずることがある。治外法権に関する一致した規則があるのが理想的である。しかし、このような規則の制定まで、各国が国際犯罪を処理するための国内の管轄規則の適合性を再検討しなければならない。遍在原則(犯罪を構成する要素の1つが行われた場所に犯罪を委ねる)が認められていない国では、コンピュータ犯罪法の適用について困難が生ずる。このような国では、たとえば英国のように特別な管轄権規則を導入する必要がある。英国では1990年のコンピュータ悪用に関する法律で、ハッカーまたはコンピュータが英国に所在するか、あるいは英国にあるコンピュータを利用した犯罪である場合は、管轄権を主張している。

一国の国民が他国でコンピュータ関連犯罪を犯した場合で、本国で犯罪が発覚し犯人が本国にいたときも問題が生ずる可能性がある。多くの国は国民を引き渡さない。このような場合には、少なくとも一国で起訴できる必要条件を作るために、治外法権に関する既存の規則の拡大(または裁判手続きの移転の可能性(次段参照))を考慮しなければならない。

相互援助と犯罪人引渡し

自由な犯罪人引渡しに関する法律、相互援助協定、および情報システムのセキュリティに係る刑事上の事項に関する承認および相互規定、裁判手続きの移転及びその他の国際協力は、他国の調査を援助するだろう。

証拠

情報システム内のデータおよび情報の正確さ、完全さおよび可用性を強化することにより、したがって、システム内のデータと情報に依存する能力を向上させることによって、情報システムにおいてセキュリティを改良すると、訴訟手続きおよび行政手続きにおける上記の証拠の提出と使用の助けになる。同様に、刑法および民法の手続きと行政手続きの双方において証拠に関する要件が明瞭になれば、セキュリティの失敗または不履行を伴う活動の予測可能性が増すことと、このような活動を予防する効果の可能性によって、システムがさらに安全になる。

providing more predictability in actions involving failures or breaches of security and by the potentially deterrent effect of such actions.

At present, electronic records may present problems for existing laws of evidence. For European continental countries, which have civil law systems, the admissibility of evidence in court is based upon the principle of free introduction and free evaluation of evidence. This is also the situation in Japan with respect to non-penal matters. In theory, under such legal systems, a court may admit any material as evidence, including computer records, but it must then decide the value such material will be afforded as evidence.

In common law countries, however, the admissibility of evidence is subject to objection and governed by complex rules. Computer records, like any other documents, may present two issues. The first is authentication: Are the documents accurate and genuine? Are the printouts from the computer admissible either as "originals" or "copies" of the data in the system? In the United States, for example, the federal rules expressly allow authentication and admission of computer records. The second issue that common law systems must address with respect to any document is whether it contains hearsay. This pertains not to the form of the document (whether electronic data or handwritten) but to its content. Generally, it is possible to testify only about matters of which one has direct knowledge and not about something learned from secondary sources. This rule applies to documents as well as to individuals and, while the hearsay rule has many exceptions (the business records rule, for example), this issue must be recognised and anticipated.

Education and Training

An overarching task is the increase of awareness at every level of society, in governments and the private sector and among individuals, of the necessity for and the goals of security of information systems and good security practices. Promotion of awareness should also include awareness of the risks to information systems and of safeguards available to meet those risks. It is important to develop social consensus about proper use of information systems.

In building awareness, it is essential to have the co-operation of users of information systems and the commitment of management, especially senior management, to providing for security of information systems.

Education and training should be included in school curricula and should be provided for users, executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and auditors of information systems and of security of information systems, both internal and independent auditors. Trained, professionally qualified auditors should inspect and evaluate an information system. Information system auditors should possess knowledge of planning, development and operation of information systems

現在のところ、電子的な記録は、既存の証拠法に問題を提起することがある。ヨーロッパ大陸諸国といった大陸法(私法)制度を有する国については、証拠が法廷において許容されるかどうかは、証拠の提出の自由および証拠の評価の自由の原則に基づいている。日本においても、刑事事件以外については同じ状況である。理論的には、このような法律制度の下では、法廷はいかなるものでも証拠として認めることができるが、後にそれが証拠たりうるものかどうかといった価値を判断しなければならない。

しかしながら、コモン・ローの国々では、証拠が許容されるかが問題となり、複雑な規則が適用される。コンピュータによる記録には、他の文書と同様に、2つの問題があり、それに対処する法執行を用意しなければならない。最初の問題は、その文書が正確で真正であるかという、立証である。コンピュータから出力された印刷物が、システムに記録されているデータの「原本」と認められるのか「写し」と認められるのか。たとえばアメリカでは、連邦規則によってコンピュータによる記録の立証と承認が明白に認められている。コモン・ロー方式があらゆる文書に関して処理しなければならない2番目の問題は、その文書の中に伝聞が含まれているかどうかである。これは文書の形式ではなく内容に関することである。一般に、人は直接知ったことについてのみ真実であると証言し、二次的情報源から知ったことについては証言できない。この規則は書類だけでなく人にも適用され、伝聞規則には多くの例外があるが(たとえば業務規則など)、検察官はこの問題を知り、予期して対処する必要がある。

教育と訓練

何よりも重要な仕事は、政府および民間部門そして個人といった、社会のあらゆるレベルで、情報システムのセキュリティおよびよいセキュリティ実践の必要性とその目的に対する理解を深めさせることである。理解の促進としては、情報システムに対するリスクの理解と、そのリスクに対処するために利用できる保護策の理解も含めるべきである。情報システムの正しい使い方について社会的コンセンサスを確立することが重要である。

認識を形成する際には、情報システムのユーザの協力と情報システムのセキュリティを実現することについての管理部門の約束が何よりも重要である。

教育と訓練は、学校のカリキュラムに取り入れられるべきであり、ユーザ、経営幹部、プログラマ、保守管理提供者、情報システム管理者(ソフトウェア管理者、オペレーション管理者およびネットワーク管理者)、ソフトウェア開発管理者、および情報システムのセキュリティに関して責任を負う管理者、内部と外部の双方を含む情報システムの監査員および情報システムのセキュリティの監査員に対して提供すべきである。訓練を受けたプロフェッショナルの独立した監査員が、情報システムを検査し評価すべきである。情報システムの監査員は、情報システムの計画、開発および動作の知識と監査全般の知識を持っていなければならない。情報システム監査を実際に実行した経験が必要である。

and of general auditing and should have actual experience in performing information system audits. It is equally important that law enforcement authorities, including police and investigators, and attorneys and judges receive adequate education and training.

Enforcement and Redress

There should be provided accessible and adequate means for exercise and enforcement of rights related to the security of information systems and for recourse and redress of violations of such rights. This includes access to courts and provision of means for adequate investigative powers. Security breaches include failures and violations of security of information systems. There is a need for better cross-education, communication, co-operation and sharing of information among law enforcement agencies, communications operators and service providers, and banks at national and international levels. Law enforcement authorities should co-operate to facilitate investigations in other countries.

Exchange of Information

Governments, the public sector and the private sector should exchange information and establish procedures to facilitate the exchange of information relating to the Guidelines and their implementation. As part of their efforts, they should publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems. It is desirable that national governments make known to the OECD, other international bodies and other governments their activities and those of their territorial subdivisions relating to the security of information systems, the Guidelines and their implementation.

Co-operation

Governments, the public sector and the private sector should develop measures, practices and procedures that are simple and compatible with those of other parties that comply with the Guidelines, taking into consideration in their development the measures, practices and procedures developed by others, so as to avoid, where possible, conflicts or obstacles. All laws adopted on regional, national or provincial levels should be harmonized to meet the challenges of a worldwide technology.

警察、調査官、弁理士及び判事などを含む法執行機関が十分な教育と訓練を受けることも同様に重要である。

実施と損害補償

情報システムのセキュリティに関する権利の履修と実施、およびそれらの権利を侵害した場合の損害補償の適切な手段が提供されるべきである。それには、法廷へのアクセス、適切な調査能力を提供する手段が含まれる。不履行としては、情報システムのセキュリティの失敗と違反が含まれる。国内および国際的レベルで、法執行機関、通信業者や通信サービス提供者、および銀行の間で、相互教育、通信、協力、および情報の共用をいっそう進める必要がある。法執行機関は、他の国において調査を実施する際に援助を必要とする。

情報の交換

政府、公共部門および民間部門は、ガイドラインおよびその実行に関する情報を交換しなければならず、情報交換を容易にするための手続きを確立しなければならない。その作業の一環として、ガイドラインに従い、情報システムのセキュリティのために設定された手段、実施方法、手続き、及び機関を一般に発表する。各国の政府は、情報システム、ガイドライン、およびガイドラインの実行に関して自国および国内の各地域で行われている活動について、OECD、その他の国際団体、及びその他の政府に対して通知するのが望ましい。

協力

政府、公共機関および民間部門は、簡単でしかもガイドラインに準拠した他の主体のものと矛盾しないような手段と実施方法、手順および指示を作成しなければならない。その際、他の主体が採用している手段、実施方法、手順の発展を考慮しなければならない。可能であれば争いや障害を回避するために、地域、国または地方自治体レベルで採用される法律はすべて、世界的な技術がもたらす課題を解決できるように、整合性のとれたものとすべきである。

8 . 2 付録2 英字略語表

ADSL	Asymmetrical Digital Subscriber Line
ASP	Application Service Provider
BIAC	Business and Industry Advisory Committee to the OECD
B to B	Business-to-Business
CERT	Computer Emergency Response Team
CIA	Confidentiality / Integrity / Availability
CORBA	Common Object Request Broker Architecture
CSI	Computer Security Institute
CSIRT	Computer Security Incident Response Team
B to C	Business to Consumer
DNS	Domain Name Service
DoS	Denial of Service
DDoS	Distributed Denial of Service
EC	Electronic Commerce
EDI	Electronic Data Interchange
FTP	File Transfer Protocol
GBDe	Global Business Dialogue on Electronic Commerce
GMITS	ISO/IEC TR 13335 Guidelines for the Management of IT Security
GUI	Graphical User Interface
ICCP	(Committee for) Information, Computer and Communications Policy
IFW	Internet Fraud Watch
ISMS	Information Security Management System
LAN	Local Area Network
NCL	National Consumers League
NIPC	National Infrastructure Protection Center
OECD	Organization for Economic Cooperation and Development
PKI	Public Key Infrastructure
P to P	Peer-to-Peer
SANS Institute	System Administration, Networking, and Security Institute
SEC	Securities and Exchange Commission
SSL	Secure Sockets Layer
TR	Technical Report
USENET	UNIX User's Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WPISP	Working Party on Information Security and Privacy
WWW	World Wide Web
XML	eXtensible Markup Language