情報システム及びネットワークのセキュリティのためのガイドライン：
セキュリティ文化の普及に向けて

新OECD情報セキュリティ・ガイドラインの概要

経済産業省 商務情報政策局 情報セキュリティ政策室
情報処理振興事業協会 セキュリティセンター（IPA/ISEC）

新ガイドライン発表までの道のり

OECD（経済協力開発機構）は2002年（平成14年）8月に、「OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security（情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて）」を発表しました。

情報セキュリティを取り巻く状況

今日、情報通信は私たちに多くの利便性をもたらし、経済、行政、生活のあらゆる場面で、情報システムやネットワークは欠くことのできない基盤となっています。その反面、コンピュータウィルスや不正アクセスによる被害、重要な社会インフラを狙ったサイバーテロ(注)の危険性といった脅威にどう対処していくかが課題となっています。情報システムやネットワークをこれらの脅威から守り、安全性と信頼性を確保すること、即ち、情報セキュリティを確保することが、情報通信社会におけるすべての人の共通の課題といえます。

（注）「重要インフラのサイバーテロ対策に係る特別行動計画」（2000年12月 情報セキュリティ対策推進会議決定）においては、このような重要インフラ分野を、当面、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）としています。

初めて策定されたのは1992年

情報セキュリティに対する国際的な関心の高まりを受けて、OECD（経済協力開発機構）は1992年に「 Guidelines for the Security of Information Systems（情報システムのセキュリティに関するガイドライン）」を策定し、その普及に努めてきました。このガイドラインは、あくまで加盟国が尊重すべき指針であり、強制力はありません。OECDでは、刻々変化する情報を取り巻く環境に対応するため、ガイドラインの5年ごとの見直しを定めています。1997年には見直しのためのレビューが行われましたが、内容の改正は行われませんでした。2回目の見直し時期である2002年に向け、2001年からガイドラインの改正についてOECDの専門家会合等において検討がなされ、2001年9月の米国同時多発テロの発生を受けてスケジュールを前倒ししながら、今回の全面改正が実現しました。

OECDについて

1948年に設立されたOEEC（欧州経済協力機構）を改組して、1961年に発足。日本は1964年に加盟し、2002年9月現在で30カ国が加盟。本部所在地はフランス（パリ）。

OECDが制定した情報セキュリティ関連のガイドライン

制定年	ガイドライン名
1980	*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* プライバシー保護と個人データの国際流通に関するガイドライン
1992	*Guidelines for the Security of Information Systems* 情報システムのセキュリティのためのガイドライン（2002年に改正）
1997	*Guidelines for Cryptography Policy* 暗号政策ガイドライン

新ガイドラインの原則とその解説

（注）解説 は新ガイドラインの各原則に記載されている解説の概要です。

1 認識の原則 Awareness

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

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

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

2 責任の原則 Responsibility

すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

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

IT 製品やサービスの開発者等は、情報システムやネットワークのセキュリティに取り組むとともに、利用者が製品やサービスのセキュリティ機能とセキュリティに関する自らの責任をよりよく理解できるように、更新情報を含む適切な情報をタイムリーに提供するべきです。

3 対応の原則 Response

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

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

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

4 倫理の原則 Ethics

参加者は、他者の正当な利益を尊重するべきである。

解説 情報システムやネットワークが社会に普及していることから、自らの行為が他人に損害を与えるおそれがあることを認識する必要があります。それゆえに倫理的な行動が極めて重要であり、参加者はベストプラクティスの形成と採用に努め、セキュリティの必要性を認識するとともに、他人の正当な利益を尊重することに努めるべきです。

5 民主主義の原則 Democracy

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

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

6 リスクアセスメントの原則
Risk assessment

参加者は、リスクアセスメントを行うべきである。

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

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

7 セキュリティの設計及び実装の原則
Security design and implementation

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

解説 情報システム、ネットワーク及びセキュリティの方針（ポリシー）は、セキュリティを最適なものとするために、適切に設計され、実装され、かつ調和が図られる必要があります。適切な安全防護措置や解決策の設計・採用が重要で、これらは情報の価値と比例するべきです。

セキュリティは、すべての製品、サービス、情報システムやネットワークの設計・構造に不可決な部分であるべきです。

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

8 セキュリティマネジメントの原則
Security management

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

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

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

9 再評価の原則
Reassessment

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

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

●新ガイドラインの全文はここで見ることができます

OECD（英語、フランス語）
http://www.oecd.org/

経済産業省（英語と日本語の対訳）
http://www.meti.go.jp/policy/netsecurity/

情報処理振興事業協会 セキュリティセンター
http://www.ipa.go.jp/security/index.html

新ガイドラインのポイント

従来のガイドラインと比べて、以下のような点が新しくなっています。

「セキュリティ文化」の提唱

新ガイドラインでは、情報セキュリティの重要性を広く認識させるために、「セキュリティ文化（a culture of security）」という新しい概念を提唱しています。「セキュリティ文化」を「情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」と定義し、これを取り入れ、普及することを提案するとともに、このガイドラインを「セキュリティ文化」の普及に向けたものと位置付けています。

情報通信ネットワーク社会を前提

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

個人を含むすべての参加者が責任を負う

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

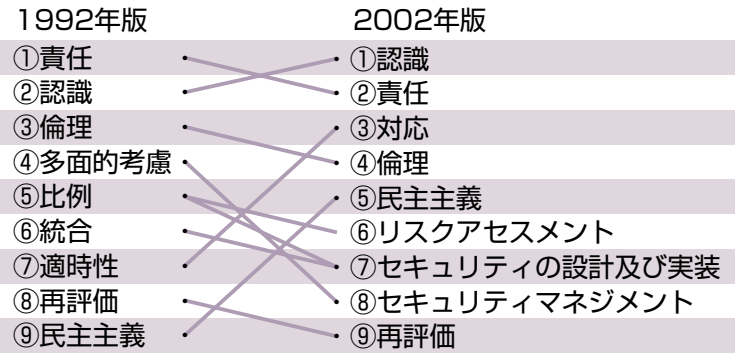
（注）「参加者」を「情報システム及びネットワークを開発、所有、提供、管理、サービス提供及び使用する政府、企業、その他の組織及び個人利用者」としています。

情報セキュリティマネジメントの概念の導入

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

従来のガイドラインとの対応関係

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



お問い合わせは‥

経済産業省 商務情報政策局 情報セキュリティ政策室
電　　話　03-3501-0397（直通）
ファクシミリ　03-3501-6639
電子メール　it-security@meti.go.jp

情報処理振興事業協会 セキュリティセンター（IPA/ISEC）
電　　話　03-5978-7508（直通）
ファクシミリ　03-5978-7518
電子メール　isec-info@ipa.go.jp