

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

経済協力開発機構

1960年12月14日パリで署名され、1961年9月30日に発行した条約の条項1に従って、経済協力開発機構(OECD)は次に掲げることのために立案された方針を促進する。

- 継続可能な最も高度な経済成長を達成し、加盟国における生活水準を向上させるとともに、金融の安定とそれによる世界経済の発展に貢献すること。
- 経済発展のプロセスにおいて、非加盟国のみならず加盟国の健全な経済の拡大に貢献すること。
- 国際的な責務に合致した、多国的主義、非差別主義に基づき、世界貿易の拡大に貢献すること。

OECDの設立当初の原加盟国は、オーストリア、ベルギー、カナダ、デンマーク、フランス、ドイツ、ギリシャ、アイスランド、アイルランド、イタリア、ルクセンブルグ、オランダ、ノルウェイ、ポルトガル、スペイン、スウェーデン、スイス、トルコ、英国、米国である。その後、次に掲げるの国が、後に示す日付による承認を経て、加盟国になった。日本(1964年4月28日)、フィンランド(1969年1月28日)、オーストラリア(1971年6月7日)、ニュージーランド(1973年5月29日)、メキシコ(1994年5月18日)、チェコ(1995年12月21日)、ハンガリー(1996年5月7日)、ポーランド(1996年11月22日)、韓国(1996年12月12日)、スロバキア(2000年12月14日)。欧州共同体の委員会は、OECDの活動に参加する(OECD条約 条項13)。

はしがき

現在の情報システム及びネットワークのセキュリティのためのガイドライン - セキュリティ文化の普及に向けて - は、2002年7月25日の第1037回会合でOECD理事会の勧告として採択された。

はじめに

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

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

性質、量及び取扱いの注意度が大きく拡大してきた。

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

I. セキュリティ文化の普及に向けて

このガイドラインは、セキュリティ文化(すなわち、情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること)の発展を促進することによって、絶えず変化を続けるセキュリティの環境に対応するものである。このガイドラインは、ネットワーク及びシステムの安全な設計及び利用が後知恵の結果であったことが余りにも多かった時代との明確な決別の合図である。参加者は情報システム、ネットワーク及び関連するサービスに一層依存するようになっており、これらすべてが信頼でき、かつ安全なものであることが必要となっている。すべての参加者の利益、並びにシステム、ネットワーク及び関連するサービスの性質を適切に考慮したアプローチのみが、効果的なセキュリティを提供し得る。

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

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

II. 目的

このガイドラインは次に掲げることを目的とする。

- 情報システム及びネットワークを保護する手段として、すべての参加者の間にセキュリティ文化を普及させること。
- 情報システム及びネットワークに対するリスク、それらのリスクに対処するために有効な方針、実践、手段及び手続並びにそれらの導入及び実施の必要性について、認識を高めること。
- すべての参加者の間に、情報システム及びネットワーク並びにそれらの提供及び利用の形態における一層大きな信頼を醸成すること。
- 情報システム及びネットワークのセキュリティのための首尾一貫した方針、実践、手段及び手続の開発並びに実施において、参加者のセキュリティの課題に関する理解及び倫理的価値の尊重を助ける全般的な考え方の枠組みを創造すること。

- セキュリティの方針、実践、手段及び手続の開発並びに実施においてすべての参加者の間の協力及び情報共有を適切に促進すること。
- 標準類の策定及び施行に関与するすべての参加者の間で重要な目的としてセキュリティが考慮されることを促進すること。

III. 原則

次の9つの原則は互いに補い合うものであり、一体のものとして読まれるべきである。それらは、方針及び運用のレベルを含む、すべてのレベルで参加者に関係する。このガイドラインの下で、参加者の責任は、彼らの役割に応じて変化する。すべての参加者は、セキュリティのより良い理解及び実践の採用を導き得る認識、教育、情報共有及び訓練によって助けられる。情報システム及びネットワークのセキュリティを強化させる努力は、民主主義社会の価値、特に公開された自由な情報の流通の必要性及び個人のプライバシーに対する基本的な関心と合致すべきである¹。

1 このセキュリティガイドラインに加えて、OECDは、世界の情報社会にとって重要な他の課題についてのガイドラインに関する互いに補い合う勧告を策定してきた。それらはプライバシーに関するもの(1980年OECDプライバシー保護と個人データの国際流通についてのガイドライン)及び暗号に関するもの(1997年OECD暗号政策ガイドライン)である。このセキュリティガイドラインは、これらと併せて読まれるべきである。

1) 認識(Awareness)

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

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

2) 責任(Responsibility)

すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

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

3) 対応(Response)

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

情報システム及びネットワークが相互接続されていること並びに急速でかつ広範な被害の可能性があることを認識し、参加者はセキュリティの事件に対処するために、適切な時期に協力的な方法で行動すべきである。参加者は脅威及び脆弱性についての情報を適切に共有するとともに、セキュリティの事件に対する予防、検出及び対応を目的とした迅速で効果的な協力を行う手続を整備すべきである。なお、許容される場合には、これらの行動に国境を越えた情報の共有と協力を含めることができる。

4) 倫理 (Ethics)

参加者は、他者の正当な利益を尊重するべきである。

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

5) 民主主義 (Democracy)

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

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

6) リスクアセスメント (Risk assessment)

参加者は、リスクアセスメントを行うべきである。

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

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

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

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

8) セキュリティマネジメント (Security management)

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

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

9) 再評価(Reassessment)

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

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

OECD理事会の勧告

理事会は、

1960年12月14日のOECD条約、特に、条項1 b)、1 c)、3 a)、及び5 b)を考慮し、

1980年9月23日のプライバシー保護と個人データの国際流通に関するガイドラインに関する理事会勧告[C(80)58/Final] を考慮し、

1985年4月11日のOECD加盟国政府によって採択されたデータの国際流通に関する宣言[Annex to C(85)139] を考慮し、

1997年3月27日の暗号政策ガイドラインに関する理事会勧告[C(97)62/FINAL] を考慮し、

1998年12月7-9日のグローバルなネットワークにおけるプライバシーの保護に関する閣僚宣言[Annex to C(98)177/FINAL] を考慮し、

1998年12月7-9日の電子商取引のための認証に関する閣僚宣言 [Annex to C(98)177/FINAL] を考慮し、

情報システム及びネットワークは、政府、企業、その他の組織及び個人利用者にとってその利用と価値がますます増大していることを認識し、

情報システム及びネットワークの役割が重要性を増し、また、安定的で効率的な国内経済及び国際貿易のために情報システム及びネットワークへ依存すること、また社会的、文化的及び政治的生活において情報システム及びネットワークへ依存することが一層増大していることが、情報システム及びネットワークにおける信頼を保護し促進する特別な努力を要求していることを認識し、

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

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

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

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

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

また、更に、この勧告の付属文書に規定される「情報システム及びネットワークのセキュリティのためのガイドライン:セキュリティ文化の普及に向けて」は強制的なものではなく、国家の主権に影響を及ぼさないことを認識し、

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

情報システム及びネットワークを開発、所有、提供、管理、サービス提供及び使用する政府、企業、その他の組織及び個人利用者に、この「情報システム及びネットワークのセキュリティのためのガイドライン:セキュリティ文化の普及に向けて」を推奨する。

OECD加盟国に次に掲げることを勧告する。

「情報システム及びネットワークのセキュリティのためのガイドライン:セキュリティ文化の普及に向けて」に規定されたセキュリティ文化を取り入れ、普及させることによって、このガイドラインを反映し、かつ考慮した政策、実践、手段及び手続を新たに確立し、又は、既存のものを改正すること。

このガイドラインを実施するために国内及び国際レベルで協議し、調整し、かつ協力すること。

セキュリティ文化を普及させ、またすべての関係者が責任を負い、個々の役割に応じた適切な方法で、このガイドラインを実施するための必要な措置を講じることを奨励するために、政府、企業、その他の組織及び個人利用者を含む公共及び民間セクターを通じて、このガイドラインを普及させること。時宜を得た、適切な方法でこのガイドラインを非加盟国において利用可能にすること。

情報システム及びネットワークのセキュリティに関する課題についての国際的な協力を促進するため、5年毎にこのガイドラインを見直すこと。

OECD情報・コンピュータ・通信政策委員会にこのガイドラインの実施を促進するよう指示する。

この勧告は、1992年11月26日の情報システムのセキュリティのためのガイドラインに関する理事会勧告(C(92)188/FINAL)に代替する。

手続の歴史

セキュリティガイドラインは、1992年に初めて策定され、1997年に見直された。今回の見直しは、情

報・コンピュータ・通信政策委員会(ICCP)から与えられた権限に従って情報セキュリティ・プライバシー作業部会(WPISP)によって、2001年に着手され、9月11日の悲劇の余波を受けて作業が早められた。草案は2001年12月10日及び11日のワシントンDC、2002年2月12日及び13日のシドニー、並びに2002年3月4日及び6日のパリで会合が開催されたWPISPの専門家グループによって起草された。WPISPは2002年3月5日及び6日、2002年4月22日及び23日、並びに2002年6月25日及び26日にパリで開催された。

現在の情報システム及びネットワークのセキュリティのためのガイドライン - セキュリティ文化の普及に向けては、2002年7月25日の第1037回会合でOECD理事会の勧告として採用された。