**セキュリティ対策資料**

[1 情報セキュリティ管理 1](#_Toc414621947)

[1.1 情報資産 2](#_Toc414621948)

[1.2 情報セキュリティポリシ 2](#_Toc414621949)

[1.3 情報セキュリティマネジメントの要素 3](#_Toc414621950)

[2 リスク管理 3](#_Toc414621951)

[（1） リスクの特定 3](#_Toc414621952)

[（2） リスクの分析 3](#_Toc414621953)

[（3） リスクの評価 4](#_Toc414621954)

[（4） リスクの対策 4](#_Toc414621955)

[2.2 情報セキュリティマネジメントシステム 5](#_Toc414621956)

[2.3 情報技術セキュリティ評価基準 6](#_Toc414621957)

[2.4 セキュリティ規定 6](#_Toc414621958)

[3 脅威と脆弱性 7](#_Toc414621959)

[3.1 人的脅威 7](#_Toc414621960)

[3.2 技術的脅威 8](#_Toc414621961)

[3.3 物理的脅威 8](#_Toc414621962)

[3.4 脆弱性 9](#_Toc414621963)

# 情報セキュリティ管理

企業などでは、個人情報や機密情報などのさまざまな情報が扱われたり、コンピューターを利用した情報の共有化が行われていたりします。

このような「情報」は、企業や団体、教育機関などの立場にかかわらず、大切な「資産」です。これらの資産は厳重に管理する必要があります。

## 情報資産

「情報資産」とは、データやソフトウェア、コンピューターやネットワーク機器などの守るべき価値のある資産のことです。組織が保有する情報資産の価値を認識し、正しく運用することが大切です。

情報資産は、「有形資産」と「無形資産」に分類できます。有形資産は、物理的に存在する機器のことで、「物理的資産」とも呼ばれます。無形資産は、論理的なデータやソフトウェアのことで、「ソフトウェア資産」とも呼ばれます。

有形資産と無形資産の例は、次のとおりです。

## 情報セキュリティポリシ

「情報セキュリティポリシ」とは、組織全体で統一の取れた情報セキュリティ対策を実施するために、技術的な対策だけでなくシステムの利用面や運用面、組織の体制面など、組織における基本的なセキュリティ方針を明確にしたものです。組織内の重要な情報資産を明確にした上で、どのように守るのかという対策を立てます。

情報セキュリティポリシは「基本方針」、「対策基準」、「実施手順」で構成されますが、通常は「基本方針」と「対策基準」の2つを指して情報セキュリティポリシといいます。

|  |  |
| --- | --- |
| **名称** | **説明** |
| 基本方針 | 組織の情報セキュリティに関しての取り組み方を、経営トップの方針として示す。経営トップは、なぜそのような取り組みが必要なのかを社員に対して説明する必要がある。 |
| 対策基準 | 基本方針にもとづき、“どの情報資産を、どのような脅威から、どの程度守るのか”といった具体的な守るべき行為や判断基準を設ける。 |
| 実施手順 | 対策基準に定められた内容を個々の具体的な業務や情報システムにおいて、どのような手順で実行していくのかを示す。 |

## 情報セキュリティマネジメントの要素

「情報セキュリティマネジメント」とは、情報資産に対するさまざまな脅威を防止し、「機密性」、「完全性」、「可用性」を確保するものです。この3つの要素をバランスよく持ち合わせることが求められます。

|  |  |
| --- | --- |
| **名称** | **説明** |
| 機密性（Confidentiality） | アクセスを許可された者だけが、確実に情報にアクセスできる。 |
| 完全性（Integrity） | 情報および処理方法が正確であること、および完全であることを保護する。 |
| 可用性（Availability） | 認可された利用者が必要なときに、情報および関連する資産に確実にアクセスできる。 |

参考　情報システムのセキュリティに関するガイドライン

経済協力開発機構（OECD）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」では、情報セキュリティを「情報資産の機密性、完全性及び可用性を維持すること。」と定義している。

また、ISO/IEC JTC 1/SC 27によるガイドラインでは、システムやデータの身元が主張どおりである「真正性（Authenticity）」、形跡をたどれる「責任追跡性（Accountability）」、動作と結果に整合性がある「信頼性（Reliability）」を加えて定義している。

# リスク管理

「リスク管理」とは、リスクを特定・分析し、それらのリスクの発生頻度と影響度の観点から評価したあと、リスクの種類に応じて対策を講じることです。

リスク管理の手順は、次のとおりです。

### リスクの特定

「リスクの特定」では、リスク分析の対象となる情報資産が、どこに、どのように存在しているのかを特定します。

### リスクの分析

「リスクの分析」では、公開情報か非公開情報か、その情報資産にはどのような価値があるのか、その情報資産をどの範囲で人が利用するのかを分析します。その際、機密性、完全性、可用性の側面から重要度のランク付けをします。

参考　公開情報と非公開情報

「公開情報」とは、製品カタログやWebページに掲載する情報などの、一般に公開している情報や、公開しても問題のない情報のこと。

「非公開情報」とは、新製品開発情報などのように公開することで不利益が発生するような機密情報や、顧客情報、住所情報などのような個人情報のこと。

### リスクの評価

「リスクの評価」では、脅威が発生するとどれだけの影響があるのかを評価し、予測される発生頻度や損失額の大きいものから優先順位を決定します。

その際、損失が発生するメカニズムを理解しておくことが大切です。

参考　ハザード

「ハザード」とは、損失を発生させる間接的要因のこと。道徳意識の低下が間接的要因になることを「モラルハザード」という。

参考　ペリル

「ペリル」とは、ハザードによって引き起こされる事故や、損失を発生させる直接的原因のこと。

### リスクの対策

「リスクの対策」では、リスクの評価結果にもとづいて、情報セキュリティを維持するための具体的な対策を決定します。

その際、損失の発生を防止または軽減するための手法として、「リスクコントロール」があります。また、損失が発生した場合の経済的損失を補てんするための手法を「リスクファイナンス」といいます。

|  |  |  |
| --- | --- | --- |
| **種類** | | **説明** |
| リスクコントロール | リスク回避 | リスクが発生しそうな状況を避ける。情報資産をインターネットから切り離したり、情報資産を破棄したりする。 |
| リスク分離 | 損失をまねく原因や情報資産を複数に分割し、影響を小規模に抑える。情報資産を管理するコンピューターや人材を、複数に分けて管理する。 |
| リスク集中 | 損失をまねく原因や情報資産をひとつに集約する。ひとつにまとめることで、より専門的かつ堅牢な管理ができる。 |
| リスクファイナンス | リスク移転 | 契約などにより、他者に責任を移転する。情報資産の管理を外部委託したり、保険に加入したりする。 |
| リスク保有 | 自ら責任を負い、損失を負担する。リスクがあまり大きくない場合に採用されるもので、引当金や補償金を用意して対処する。 |

参考　リスク最適化

「リスク最適化」とは、リスクの大きさを小さくすること。

## 情報セキュリティマネジメントシステム

「情報セキュリティマネジメントシステム」とは、情報システムの機密性、完全性、可用性のバランスを維持し改善するために、組織のリスク管理により必要なセキュリティバランスを定め、プランに沿って運用するしくみのことです。「ISMS（Information Security Management System）」とも呼ばれます。

情報セキュリティマネジメントシステムでは、リスク管理の結果にもとづいて、具体的な情報セキュリティの基本方針や目標を策定します。その上で、技術的対策のほかに人的・物理的対策を含んだ情報セキュリティ対策を実施します。その結果を検証して対策を見直すことによって、継続的な情報セキュリティの改善を目指します。

情報セキュリティマネジメントシステムは、「ISO/IEC 27001」として国際標準化されており、日本では「JIS Q 27001」としてJIS化されています。また、情報セキュリティマネジメントシステムの認証基準（システム仕様）となる規格として「ISO/IEC 27002」が国際標準化され、日本では「JIS Q 27002」としてJIS化されています。

## 情報技術セキュリティ評価基準

「情報技術セキュリティ評価基準」とは、IT製品やシステムのセキュリティ品質を客観的に評価するための基準のことです。「CC」、「コモンクライテリア」とも呼ばれます。コンピューターシステムのネットワーク化や分散化にともない、情報システムのセキュリティの重要性が高まっています。その中で、個々の情報処理製品（データベース管理、ファイアウォール、ICカードなど）や情報処理システム（インターネットバンキング、認証サービスなど）のセキュリティ完備状況を評価するための制度が必要とされています。

情報技術セキュリティ評価基準では、個々の情報処理製品や情報処理システムのセキュリティ機能と品質を、設計書やプログラム、テスト結果、マニュアルなどの内容のチェック、テストの実施などによって検査し、問題がないことを証明します。

情報技術セキュリティ評価基準は、「ISO/IEC 15408」として国際標準化されており、日本では「JIS X 5070」としてJIS化されています。

## セキュリティ規定

「セキュリティ規定」とは、組織におけるセキュリティ管理について、管理体制や内規を定めたものです。セキュリティ規定には、組織がどのように情報セキュリティを維持するのかを具体的に定め、誰がどのように責任を負い、どのように対策するのかを記します。それぞれのセキュリティ規定は、互いに連関するよう、組織全体で体系立てて作成することが重要です。

セキュリティ規定で定める文書には、次のようなものがあります。

# 脅威と脆弱性

現在、多くの企業などにおいてシステムやインターネットが活用されています。誰でも素早く簡単に情報を利用できるメリットがある反面、コンピューターウイルスに感染したりシステムに不正にアクセスされたりする事例があとを絶ちません。これらのリスクから情報資産を守って安全に活用するためには、取り巻くさまざまな脅威や脆弱性を把握して適切な対策を講じていくことが重要です。

## 人的脅威

人的・物理的な手口によって重要な情報を入手し、その情報を悪用することをセキュリティの世界では「ソーシャルエンジニアリング」といいます。技術的な手口を知らなくても、人間の心理的な弱点を突くことで誰でも簡単に情報を悪用できるため、警戒が必要です。

## 技術的脅威

技術的脅威として、Webサーバーやメールサーバーなどの外部からアクセスできるサーバーに対してさまざまな手口を使って、サーバー内のデータを盗み見たり改ざんしたり、サーバーに過負荷をかけて停止させたりすることがあります。このような攻撃を行う者を「クラッカー」といいます。

代表的な技術的脅威として、次のようなものがあります。

|  |  |
| --- | --- |
| **種類** | **説明** |
| コンピューターウイルス | 利用者の知らない間にコンピューターに侵入し、コンピューター内のデータを破壊したり、ほかのコンピューターに増殖したりするなどを目的に作られた、悪意のあるプログラム。ネットワークに接続されたコンピューターに対して、次々と自己増殖していく「ワーム」もコンピューターウイルスのひとつ。ネットワークの負荷によって、被害を増大させる。 |
| バッファオーバーフロー攻撃 | コンピューター上で動作しているプログラムで確保しているメモリ容量（バッファ）を超えるデータを送り、バッファをあふれさせクラッカーが意図する不正な処理を実行させる。 |
| クロスサイトスクリプティング | ソフトウェアのセキュリティホールのひとつで、悪意のあるWebサイトを閲覧したときに、埋め込まれているコードを介して個人情報が盗み出されたり、コンピューター上のファイルが破壊されたりする。 |
| DoS（Denial of Service）攻撃 | サーバーに過負荷をかけ、その機能を停止させる。一般的には、サーバーが処理することができないくらいの大量のパケットを送る方法が使われる。DoS攻撃によってネットワークが混雑することで、一般の利用者がサーバーを利用できなくなる場合もある。 |

## 物理的脅威

自然災害や、破壊・妨害行為、事故や故障（エラー）などによって、情報にアクセスできなかったり情報が壊れてしまったりすることで、業務の遂行やサービスの提供に支障をきたしてしまうことがあります。これらの脅威の発生を抑制するのは難しく、脅威の発生後の対応を含めた対策が必要となります。

## 脆弱性

「脆弱性」とは、情報セキュリティに関する欠陥や弱点のことをいいます。

代表的な脆弱性として、次のようなものがあります。

|  |  |
| --- | --- |
| **種類** | **説明** |
| セキュリティホール | 開発段階では想定していないセキュリティ上の脆弱性。セキュリティホールを悪用されると、コンピューターウイルスに感染させられたり、外部から攻撃を受けたりする恐れがある。 |
| 人為的脆弱性 | 組織や個人に対する、行動規範の不徹底や未整備に起因する脆弱性。セキュリティ規定の作成や、教育訓練の徹底が求められる。 |