# 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、取り巻く様々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様々な手口を使って、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。ネットワークに過負荷をかけて、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。 |