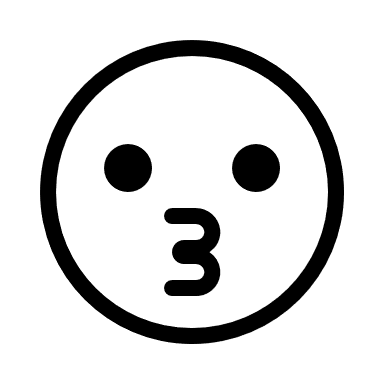
**システムの脆弱性**

**セキュリティホールとは**

ソフトウェア製品の欠陥により、権限がないと本来できないはずの操作がユーザにも実行できてしまったり、見えるべきではない情報が第三者にも見えてしまうような不具合のこと

どのような製品にも存在する可能性があり、OS、Webサーバ、DBサーバからも日々発見されている

  
  
  
  
  
  
  
  
発見されたセキュリティホールは脆弱性情報データベースで保管され、一般公開されているためシステム管理者はその情報を参照することで地震の管理するシステムのセキュリティホールを知ることができる

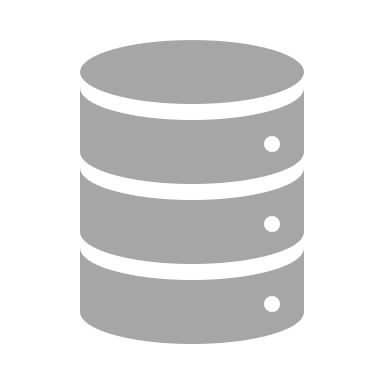
それぞれに脆弱性が存在しうるため完全になくすことは困難

ファイアウォール



APサーバ

Java、Tomcatなど



Webサーバ

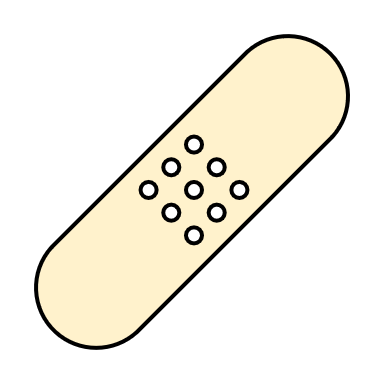
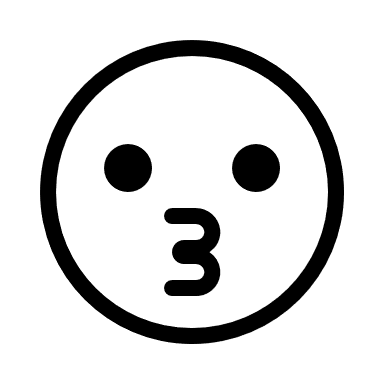
IIS、Apacheなど



DBサーバ

Oracle、MySQLなど

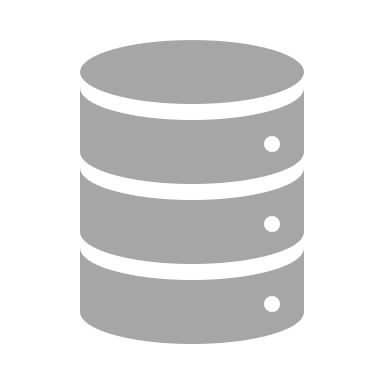
また、ソフトウェアの開発元はセキュリティホールが発見されると直ちに修正プログラムを開発し、利用者に配布することで被害の拡散を防ぐ

セキュリティホールをうまく利用することで攻撃可能に

製品の開発元から提供される修正プログラム(セキュリティパッチ)を適用することで対策

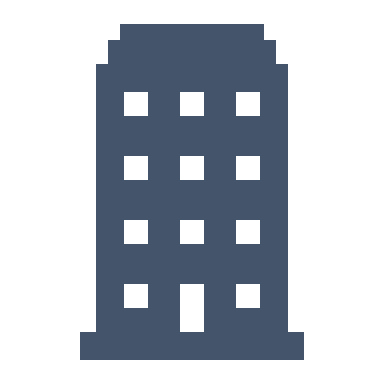
情報セキュリティを脅かすソフトウェアのバグ=セキュリティホール



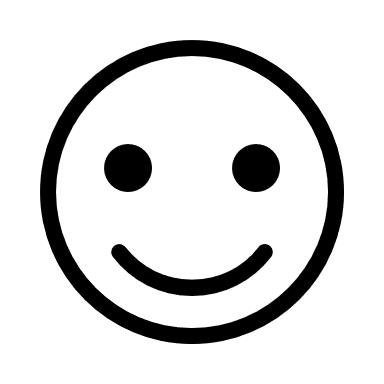
Webサーバ

IIS、Apacheなど

セキュリティパッチの提供



開発元



システム管理者

ファイアウォール



APサーバ

Java、Tomcatなど



DBサーバ

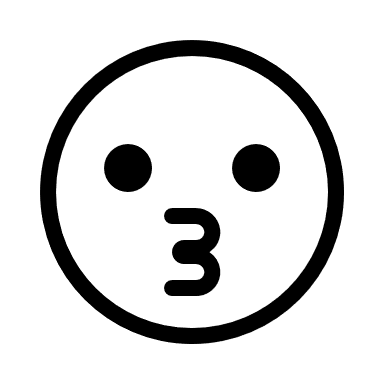
Oracle、MySQLなど

**ゼロデイ攻撃**

発見されたセキュリティホールに対する修正プログラムが開発される前に、そのセキュリティホールを利用した攻撃を仕掛けること

はっきりとした対策がなく、システム管理者にとっては最も対策が難しい攻撃となる

セキュリティホールの発見頻度が少なく信頼できる製品や、セキュリティホールへの対応が早い製品を選定することが一つの対策になる

最近では、脆弱性データベースの情報を利用し、正式なセキュリティパッチが開発されるまで一時的にゼロデイ攻撃の可能性のある通信を遮断するようなセキュリティ製品も開発されている

ファイアウォール



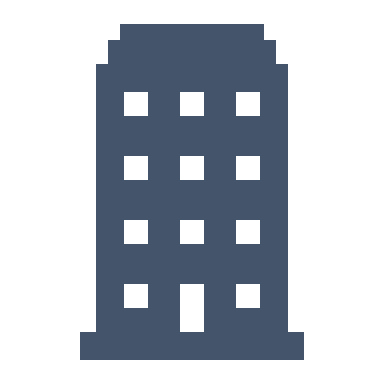
APサーバ

Java、Tomcatなど

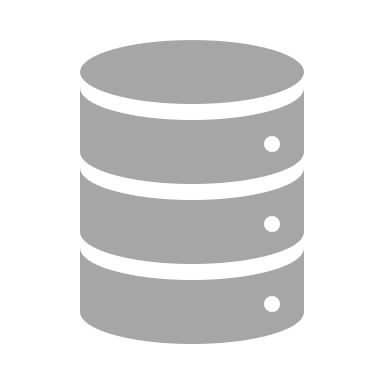


DBサーバ

Oracle、MySQLなど



開発元



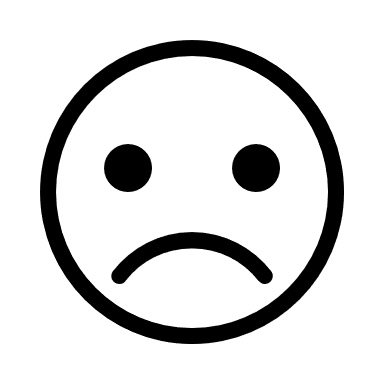
Webサーバ

IIS、Apacheなど

セキュリティパッチが開発されるまでに

セキュリティホールを利用した攻撃を行う

セキュリティパッチが提供されるまでは対策できない



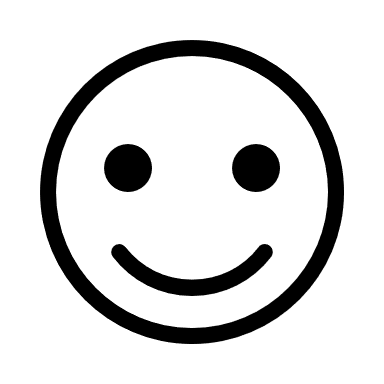
システム管理者

セキュリティパッチの提供には時間がかかる

**ペネトレーションテスト**

実際にサイバー攻撃と同じ手法でWebシステムにアクセスを試みるなど疑似的に攻撃を行うことで脆弱性の有無を確認するテスト

Webシステム全体としての脆弱性を確認するため、実施することでWebアプリケーションだけでなくOSやミドルウェアの脆弱性も同時に調査することができる

  
  
  
  
  
  
  
  
  
脆弱性が発見された場合、その脆弱性への対策が必要になる。Webアプリケーションの場合は該当箇所の修正で対応することになり、OSやミドルウェアは基本的には修正プログラムを適応したり脆弱性のないバージョンにすることになる

SQLインジェクション

DoS攻撃

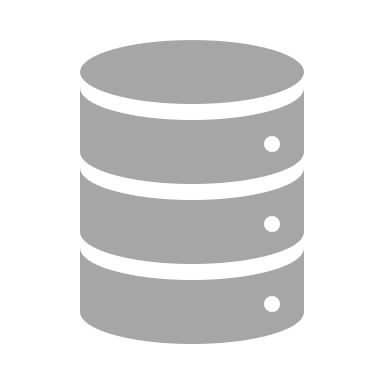
ディレクトリトラバーサル

成功した攻撃があれば対策が必要

ファイアウォール

自分の管理するシステムに対し、

疑似的に攻撃を仕掛けてみる



Webサーバ

IIS、Apacheなど



APサーバ

Java、Tomcatなど



DBサーバ

Oracle、MySQLなど

ただしバージョンアップを行うと、Webアプリケーションの稼働する環境が変わるため十分な検討が必要