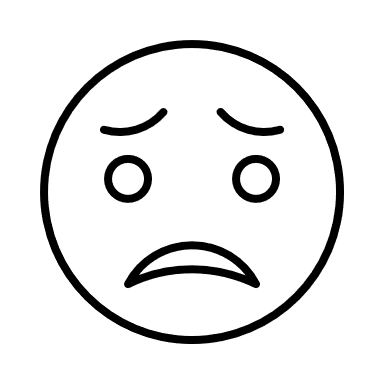
**ファイアウォール**

**ファイアウォールとは**

インターネットと内部ネットワークの間に設置し、送受信されるデータを監視して通信の許可・拒否を行うもの

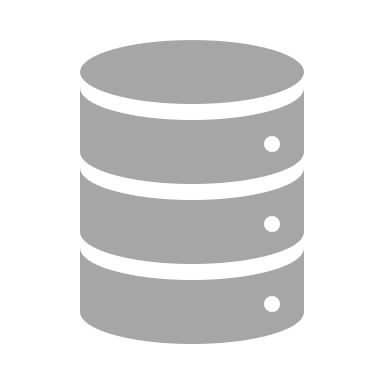


攻撃者

インターネット

攻撃の手段が限られる

インターネットから直接アクセスするサーバは必要な通信のみ通す



Webサーバ



APサーバ



DBサーバ

内部ネットワーク

ファイアウォール

**パケットフィルタ型ファイアウォール**

最も広く使われているファイアウォールの方式

ネットワーク層(第3層)で動作する

送受信されるデータ(パケット)のIPアドレスとポート番号をチェックし通信の許可・拒否の判断を行う

また、内部からインターネット向けの通信を遮断することもできるため、ウイルスに感染したサーバが外部にデータを送信してしまうという状況も未然に防ぐことが可能

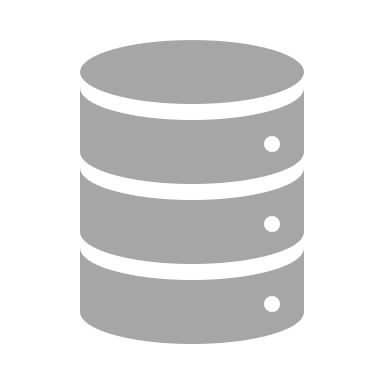
ただし、ファイアウォールで許可したIPアドレスやポート番号を利用した通信を使っての攻撃は防げないため、ほかのセキュリティ対策も併せて行われることが多い

○社内ユーザ向けWebシステムの場合

○不特定多数向けWebシステムの場合

そもそもアクセスできない

社内のIPアドレスとポート番号のみ許可する

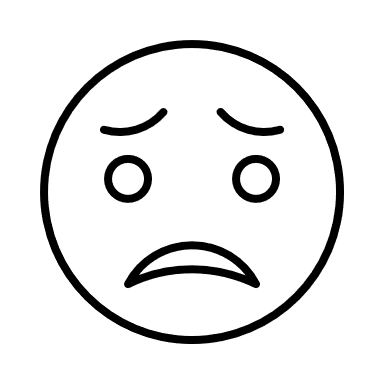


Webサーバ

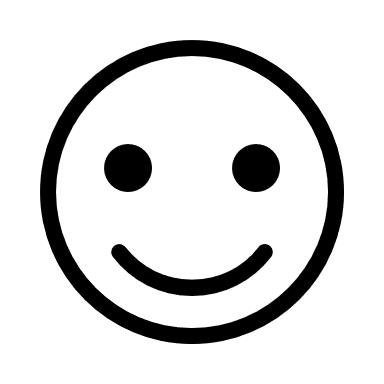
内部ネットワーク

インターネット

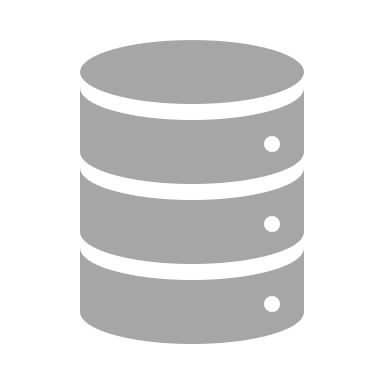
ファイアウォール



攻撃者



一般ユーザ



Webサーバ



APサーバ

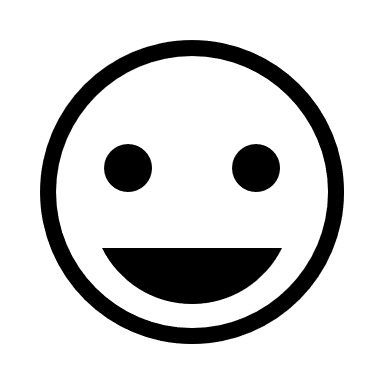


DBサーバ

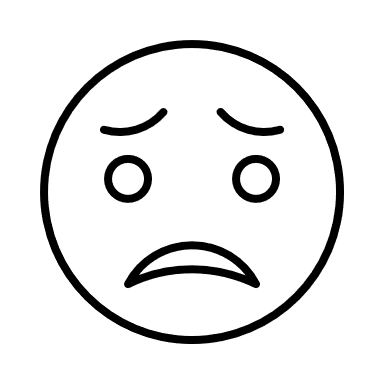
内部ネットワーク

許可されたポート番号でしかアクセスできないので攻撃の手段が限られる

不特定多数向けなのでIPアドレス単位での遮断は難しい



一般ユーザ



攻撃者

ファイアウォール

インターネット

**アプリケーションゲートウェイ型ファイアウォール**

アプリケーション型ファイアウォールとも呼ばれる

通信を中継するプロキシ(代理)プログラムを使い、社内ネットワークとインターネットを切り離す方式

ゲートウェイ上でHTTPやFTPなどのアプリケーションレベルのフィルタリングを行い、データを中継する

アプリケーションごとにきめ細かい制御ができる反面、プロキシプログラムが各アプリケーションに対応している必要がある

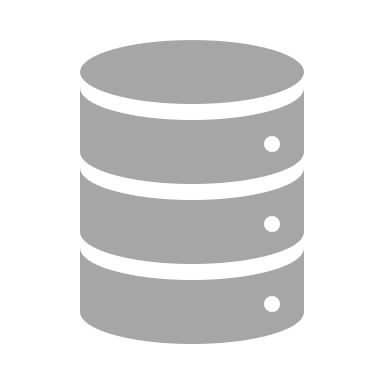
また、処理速度はパケットフィルタ型ファイアウォールより遅い

アプリケーション層(第7層)で動作する

プロキシ…企業などの内部ネットワークとインターネットの境界にあり、内部のコンピュータの代理としてインターネット上のコ ンピュータへ接続を行うコンピュータ、またはそのような機能を持つサーバソフトウェア

プロキシサーバを使用して

特定のWebサイトで閲覧を制限する



Webサーバ



APサーバ



DBサーバ

社内ネットワーク

ファイアウォール

インターネット

一度取得した外部サーバのデータを自らのストレージ内に保存しておくキャッシュ機能があり、再び同じデータに取得要求があったとき、自らが保管しているデータを代理として渡す場合がある。これにより外部サーバの負荷が軽減されるほか、内外を結ぶ通信回線の混雑を緩和することができる

また、内外を流通するデータをアプリケーションレベルで把握することができるため、望ましくない接続先を設定して内部からの中継を拒否する[フィルタリング](http://e-words.jp/w/%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%AA%E3%83%B3%E3%82%B0.html)を行なったり、外部から[ウイルス](http://e-words.jp/w/%E3%82%B3%E3%83%B3%E3%83%94%E3%83%A5%E3%83%BC%E3%82%BF%E3%82%A6%E3%82%A4%E3%83%AB%E3%82%B9.html)など不正なデータが流入することを検知・抑止する。

**サーキットレベルゲートウェイ型ファイアウォール**

パケットフィルタリングのIPパケットによるフィルタリングに加え、TCPのセッション単位で任意のポートに関する通信の許可・拒否を制御できる

トランスポート層(第4層)で動作する

**パーソナルファイアウォール**

家庭や個人のコンピュータ利用者向けに開発・提供されているファイアウォール

コンピュータ上で動作するソフトウェアの形で提供され、接続設定に基づいてコンピュータが送受信するパケットを監視し、不審な通信があればパケットを破棄する

あらかじめいくつか推奨設定を組み込んでおき、利用環境に合わせて選択できるようにしたりコンピュータ内の個々のソフトウェア単位で通信を許可・拒否するといった形で設定できるようになっている製品が多い

単体の製品やフリーソフトウェアのほか、アンチウイルスソフトなどと共イン統合セキュリティソフトウェアの一部として提供している場合があり、Windowsでは「Windows Defender ファイアウォール」などOSの機能の一部として標準で組み込まれている