**IDSとIPS**

**IDSとIPSとは**

ファイアウォールで防ぎきれない攻撃を防ぐ手段

どちらもネットワーク上を流れる通信を監視し、不正アクセスとみられる通信や普段と異なる異常な通信を検知する装置

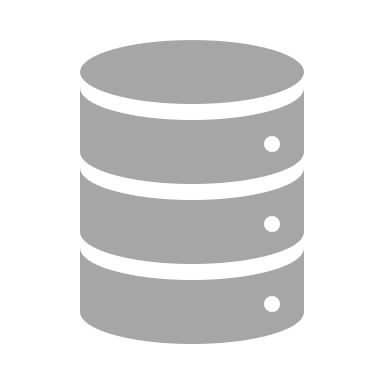
通信を監視するネットワーク型とサーバ上のユーザの動きを監視するホスト型の2種類ある

・IDS…異常な通信があったことをシステム管理者にメールなどで通知する

・IPS…通知のほかに即座に該当する通信の遮断を行う

IPSの方が強固なセキュリティを実現できるが、不正な通信だけを正確に検知することは難しく正常な通信を不正な通信と誤認してしまうこともある

通信の中身まではチェックしないため、クロスサイトスクリプティングやSQLインジェクションのような一見正常な通信に見えるものの、ユーザから送信されてくるデータに悪意のあるデータが含まれる攻撃は防ぐことができない



Webサーバ

内部ネットワーク

ネットワーク型

IDS、IPS

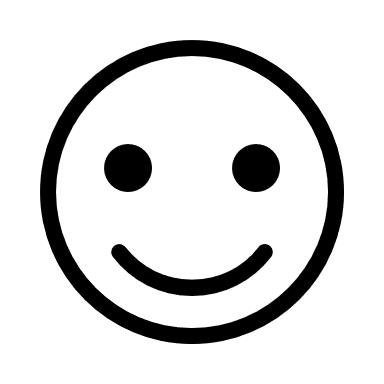
ファイアウォール

ファイアウォールで通過してきた通信をIDSやIPSで監視

インターネット

**動作の違い**

・IDS

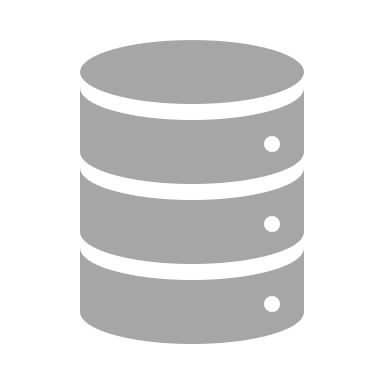


管理者

ショッピングサイトのように、

IPSの誤検知で遮断された場合、販売機会が大きく損なわれる恐れがあるため、採用する選択肢が出てくる

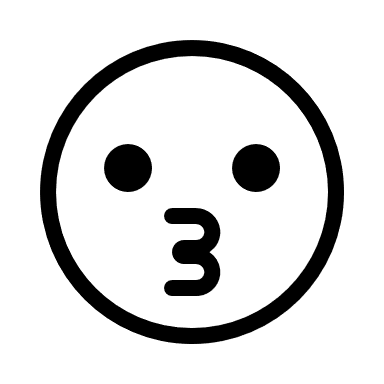
可用性を重視



Webサーバ

内部ネットワーク

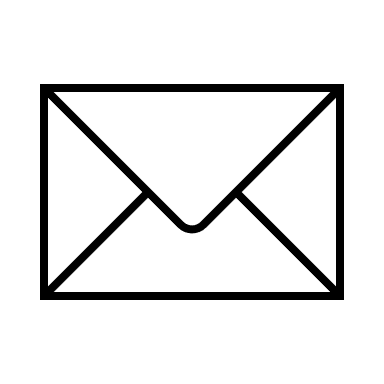
IDS



攻撃者

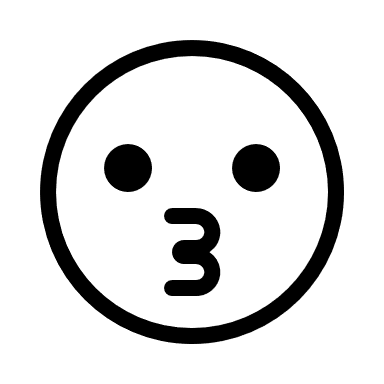
通信はそのまま通す

異常検知

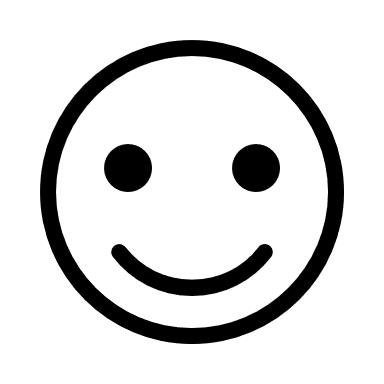


・IPS

IPS



攻撃者

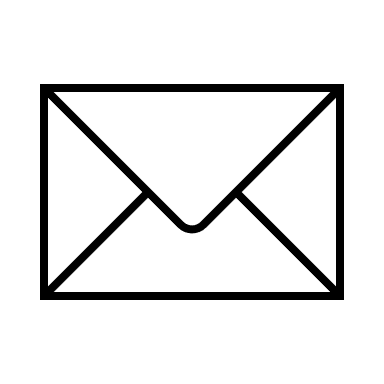


管理者

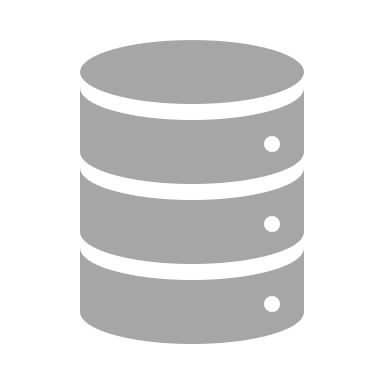
異常検知

攻撃を受けた際のリスクが非常に大きいサイトで採用されることが多い

機密性・完全性を重視



該当の通信を遮断



Webサーバ

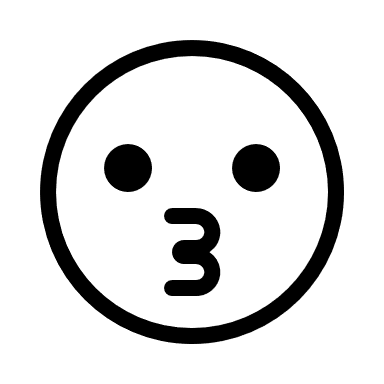
内部ネットワーク

**不正アクセスの検知方法**

・シグネチャ型(不正検知型)…監視対象の通信とシグネチャを比較し、シグネチャに登録されたパターンと一致する通信 を不正アクセスと判断

SYN Flood攻撃のような特徴的な通信を行う攻撃を検出できる  
  
  
  
  
  
  
  
・アノマリー型(異常検知型)…普段の通信とは大きく異なる通信や、通常は発生しないような通信を不正アクセスと判 断する検知方法

IDS、IPS



攻撃者

シグネチャ

不正アクセスと判断

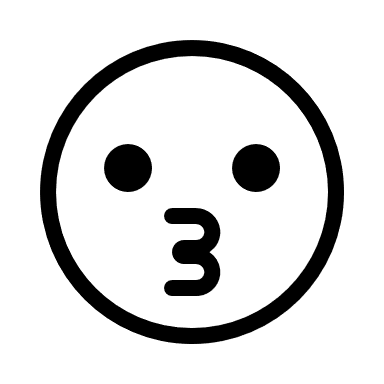
シグネチャのパターンと同じ

通信内容には不審な点がないもののアクセス量が急増するF5攻撃などを検出できる

いつもとパターンが違う

不正アクセスと判断

IDS、IPS



攻撃者

**WAF(Web Application Firewall)とは**

やりとりされるパケットの中身を見て悪意のあるデータが含まれていないかチェックするもの

・ブラックリスト型…特定のパターンのデータを持つ通信を遮断する。新たな攻撃手法が発見された場合はブラックリストに そのパターンが追加されるまでは対応できない。

・ホワイトリスト型…正常なデータのパターンを登録しておき、それに適合する通信のみを通す。Webサイトへの正常な 通信が誤って遮断されないようにすべての通信パターンをあらかじめ登録しておく必要があり、運用に コストがかかる。