



# サーバ攻撃と対策



## 主な手口のしくみと守り方

Webサーバをねらう攻撃にはパターンがある。  
攻撃のまねではなく、守るために仕組みを知ろう。

### 1 DDoS (大量アクセス)

大量の通信を一気に送り、サーバをパンクさせて止める。

通信を分散(CDN)

あやしい通信を遮断

つねに監視



### 2 SQLインジェクション

入力欄に命令を混ぜ、データベースを不正に操作しようとする。

入力を検証する

命令と値を分ける

権限は最小限に



### 3 XSS (スクリプト混入)

ページに悪いスクリプトを埋め込み、見た人のブラウザで動かす。

出力をエスケープ

入力を検証

CSPで制限



### 4 パスワード総当たり

パスワードを次々に試して、ログインを破ろうとする。

強いパスワード

多要素認証(MFA)

試行回数を制限



### 5 フィッシング(なりすまし)

本物そっくりの偽サイトで、パスワード等をだまし取る。

URLをよく確認

鍵マーク(HTTPS)を見る

あやしいリンクは開かない



仕組みを知れば守れる:

検証・MFA・監視

