ネットワーク防御技術

学習内容

ネットワーク防御を構成する主要なシステム

1. ファイアウォール（FW）の基本機能と動作
2. 侵入検知システム（IDS）と侵入防止システム（IPS）
3. ファイアウォール導入時の構成とトラフィックルール
4. FWの高度な機能：ステートフルインスペクションとフェールオーバー
5. 統合脅威管理（UTM）の概要と役割

01

ファイアウォール（FW）の基本機能と動作

ファイアウォール（FW）：ネットワークの門番

外部からの不正アクセスを防ぐための必須システム

役割

外部ネットワークからの社内LANへの**侵入を防ぐ**システム

実装方法

ルータ機能の一部または**専用ハードウェア**として設置

基本動作

外部からのトラフィックを拒否し、内部から外に出た通信の戻りだけを許可

FWの限界：攻撃の善悪は見分けられない

IDSやIPSと併用が必要な理由

ファイアウォールは「**この通信を許可するか拒否するか**」だけを判断する仕組み

パケットが**悪意あるものかどうか**までは判断できない

DoS攻撃やワーム、Webアプリケーションの脆弱性を狙った不正なリクエストは防ぎきれない

防御の堅牢性を高めるには、侵入検知・防止システム（**IDSやIPS**）との併用が必須

02

IDSとIPS：侵入の「検知」と「防止」

IDS vs IPS：役割と対応のスピード

シグネチャによる検知・防御の違いを理解する

IDS（侵入検知システム）

ネットワーク通信を監視し、攻撃を検知

検知した情報を管理者に**通知**

検知には「シグネチャ」データベースを使用

防御はできず、管理者が対応するまで待つ必要がある

IPS（侵入防止システム）

IDSと同じく攻撃パターンを検知

検出した時点でパケットを破棄・切断し**即座に防御**

自動で防御を行うため、リアルタイムな対応が可能

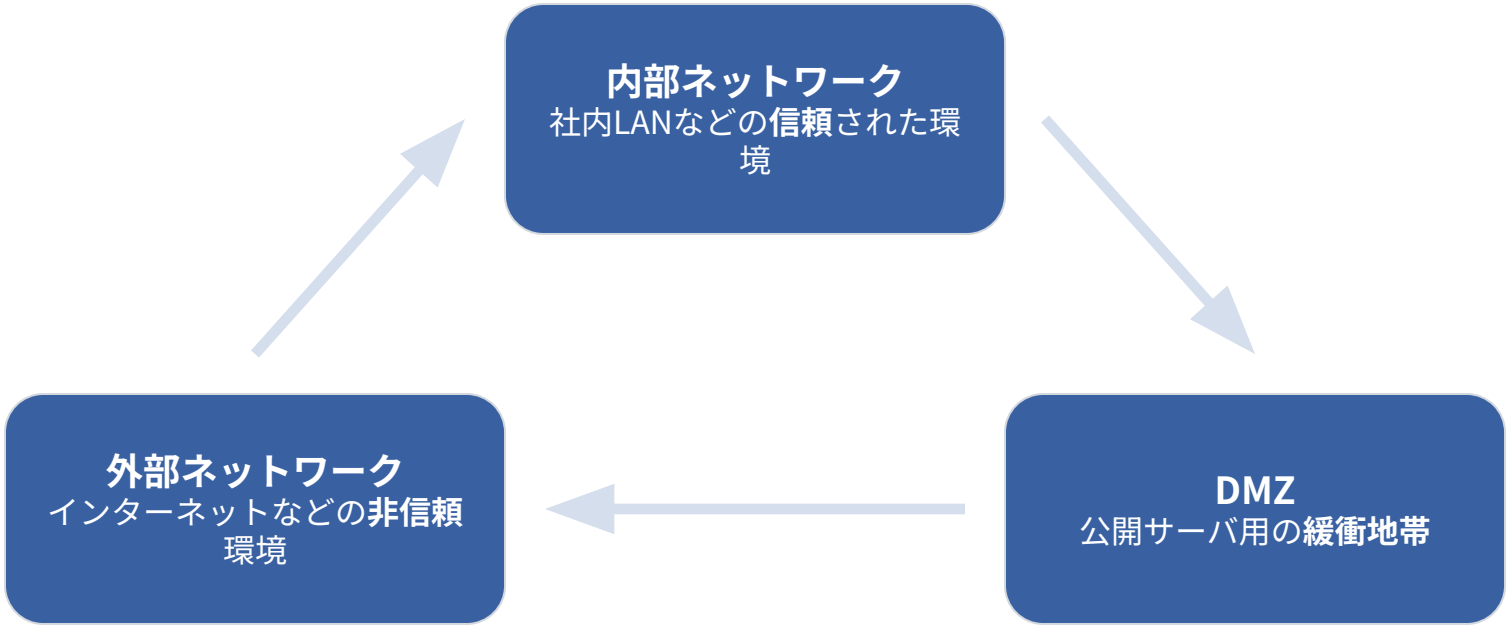
ファイアウォールと並ぶネットワーク防御の**要**となる

03

ファイアウォール導入時の構成

標準的なネットワークセグメント構成

セキュリティを確保するための3つの領域



DMZの役割とセキュリティ上のメリット

公開サーバの配置による内部ネットワーク保護

DMZ（DeMilitarized Zone）は、内部と外部の**中間**に置かれる公開サーバ用ネットワーク

WebサーバやメールサーバをDMZに配置する

仮にDMZのサーバが攻撃で侵入されても、**内部ネットワークへ直接到達できない**ように防御

DMZは「内部への侵入を防ぐための緩衝地帯」としての役割を持つ

セグメント間のトラフィック基本ルール

必要最低限の通信のみを許可する原則

通信方向	ルール（許可するもの）
内部 → 外部	設計ポリシーに従い必要な通信のみ許可
外部 → 内部	内部からの戻り通信のみ許可
外部 → DMZ	公開サーバに必要な通信のみ許可
DMZ → 内部	内部からの戻り通信のみ許可

04

FWの高度な機能

ステートフル機能の重要性

単なるフィルタリングを超えたFWの役割

ステートフルインスペクション		ステートフルフェールオーバー
通信状態の記録・照合	機能	通信状態の引継ぎ・継続
戻り通信だけを許可	役割	障害時のセッション維持
外部からの**一方的な通信を拒否**	動作	アクティブ/スタンバイのリアルタイム同期

05

統合脅威管理（UTM）の概要

UTM（統合脅威管理）のコンセプト

複数のセキュリティ機能を一つの製品に統合

STEP 1	ファイアウォール
STEP 2	IPS（侵入防止システム）
STEP 3	アンチウイルス・アンチスパム
STEP 4	Webフィルタリング・アプリケーション制御

UTMのメリットとデメリット

導入前に考慮すべき点

メリット
運用の**簡素化**とコスト削減

メリット
複数のセキュリティ対策を**一台**でカバー

デメリット
処理負荷増大による**通信速度の低下**リスク

デメリット
大規模ネットワークでは**機能分離**が推奨される場合がある

CCNA試験対策：覚えておくべき要点

知識の定着に役立つ重要なチェックポイント

Q. FW、IDS、IPSの違いは？

A. FWは許可/拒否判断のみ。IDSは検知/通知のみ。IPSは検知/リアルタイム防御を行う。

Q. DMZの役割は？

A. 内部と外部の中間に位置し、公開サーバを配置して内部への侵入を防ぐ緩衝地帯。

Q. ステートフルインスペクションの動作は？

A. 通信の状態を記録し、内部からの戻り通信だけを許可し、外部からの一方的な開始を拒否。