ネットワークセキュリティ基礎

学習内容

セキュリティの土台となる重要概念を順序立てて学習します。

1. はじめに：セキュリティの全体像
2. CIAの3要素と脅威の分類
3. アクセスと認証に関する基本用語
4. マルウェアと攻撃手法の理解
5. 防御技術（FW, IDS, WAF）の役割
6. まとめとCCNAへの接続

01

Chapter 1：セキュリティの全体像とCIAの3要素

ネットワークセキュリティの全体像

外部からの脅威と内部からのリスク、両輪での対策が必要です。

セキュリティとは？

デジタル資産を安全に保つ一連の仕組みと運用

外部対策

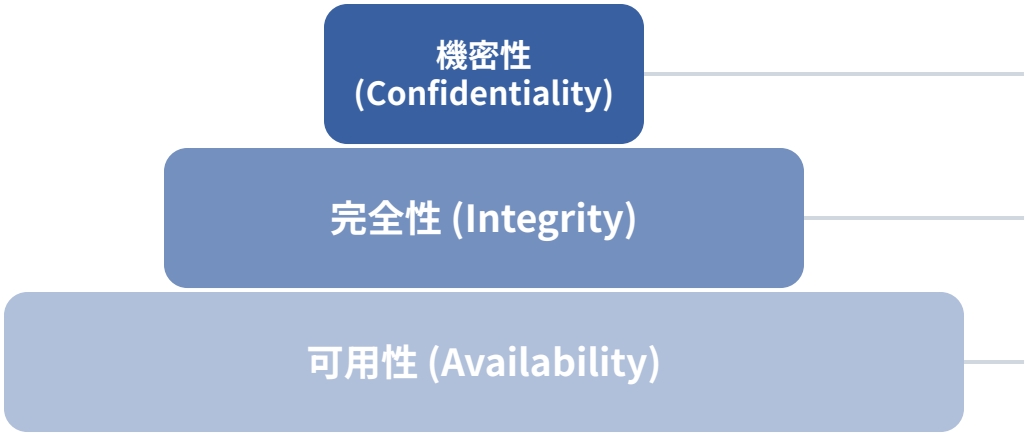
クラッキングやマルウェア流入を防ぐ技術的な防御

内部対策

内部不正や誤操作による情報漏えいを抑える運用統制

システムが守るべき三本柱：CIAの3要素

この3要素のバランスを保つことがセキュリティの究極の目的です。



見てよい人だけが見られること（暗号化、アクセス制御）

情報が正しく保たれていること（改ざん・欠損がない状態）

必要なときにシステムが使えること（停止しない設計）

セキュリティを壊しうる要因：脅威の三分類

脅威は発生源によって3つに分類され、それぞれ対策が異なります。

技術的脅威

- 不正アクセス
- 盗聴・改ざん
- DoS攻撃
- マルウェア

物理的脅威

- 火災、停電
- 機器の故障
- 盗難、紛失

人的脅威

- 操作ミス
- 内部不正
- ソーシャルエンジニアリング

02

Chapter 2：アクセスと認証に関する基本用語

アクセス管理の土台となる用語

「誰か」と「何ができるか」を分けて管理します。

アカウント	認証 (Authentication)	認可 (Authorization)
サービスに入場するための**入館証**。ユーザ名とパスワードの組み合わせ	**誰であるか**を確かめるプロセス（例：パスワード入力）	認証されたユーザに**何ができるか**を与える権限（閲覧・変更など）

認証の三要素と多要素認証 (MFA)

異なる種類の要素を組み合わせることでセキュリティが大幅に向上します。

要素	説明	代表的な例
知識情報	本人だけが知っている情報	パスワード、PIN、秘密の質問
所持情報	本人だけが所持する物や端末	スマホ、ICカード、ワンタイムコード
生体情報	身体的特徴	指紋、顔、網膜、静脈

二要素認証と二段階認証の違い

混同しやすい用語ですが、セキュリティ上の意味合いは大きく異なります。

二要素認証 (2FA)	二段階認証
異なる種類の要素を2つ使う	認証の手順が2回あること
「知識 + 所持」など、性質の異なる組み合わせ	「パスワード + 秘密の質問」など、同じ種類でも成立する
セキュリティレベルが高い	セキュリティレベルが低い場合もある

セキュリティ上の「良くない出来事」に関する用語

問題発生の事象と、それに対処する技術・人の役割を整理します。

Q. インシデントとは何ですか？

A. セキュリティ上の**対処が必要な**良くない出来事の総称（マルウェア感染、情報漏洩など）

Q. クラッカーとは誰ですか？

A. 不正侵入や改ざんを行う**悪意ある攻撃者**（ハッカーは必ずしも悪意を持たない）

Q. ロギングの重要性は何ですか？

A. 出来事を時系列に記録すること。トラブル時の**タイムライン作り**に必須

03

Chapter 3：マルウェアと攻撃手法の理解

マルウェアの主要分類と特徴

感染方法と目的によって分類されます。

ウィルス

宿主プログラムに**寄生**して広がる

ワーム

単独で複製し、ネットワーク経由で広がる

トロイの木馬

無害に見せかけ、**侵入後に悪さ**をする

ランサムウェア

ロックや暗号化で身代金を要求する

スパイウェア

ユーザー情報を**密かに抜き取る**

マルウェア検出：シグネチャ法 vs 振る舞い法

それぞれ長所・短所があり、組み合わせて利用するのが一般的です。

シグネチャ法		振る舞い（ビヘイビア）法
既知のマルウェア	検出対象	未知のマルウェア
指紋データとの照合	検出原理	実行中の不審な挙動の監視
高速かつ高精度	長所	未知の脅威に対応可能
未知の攻撃に弱い	短所	誤検知の可能性

攻撃の三つのステップ

防御策を講じるためには、攻撃者がたどる順序を理解することが不可欠です。

Step 1: 調査

Pingスイープやポートスキャンでターゲットの弱点を探す

Step 2: アクセス

辞書攻撃やブルートフォースで不正侵入し、バックドアを設置

Step 3: 攻撃

DoS、DDoS、マルウェアなどで直接的な被害を与える

攻撃手法に関する重要用語

攻撃の目的や手口を知り、適切な防御策につなげます。

脆弱性 (ぜいじゃくせい)

設計や実装の不備で生じた**弱点**。パッチで修正する

エクスプロイト

脆弱性を突く**具体的な攻撃コード**やその行為

フィッシング

偽サイトに誘導し、**認証情報**を盗み出す手口

サービス不能攻撃 (DoS) の代表例

システムを使えなくする『可用性つぶし』の攻撃です。

大規模攻撃：DDoS vs DRDoS

攻撃元の規模と手法に大きな違いがあります。

DDoS (分散型DoS)

多数の機器（ボットネット）から**直接**攻撃

攻撃元から標的に向けてパケットを大量送信

攻撃パケットの流量が多い

DRDoS (分散反射型DoS)

第三者サーバを**踏み台（反射）**にして攻撃

小さなリクエストで大きな応答を標的に集中させる

増幅（アンプリフィケーション）の特性を利用

04

Chapter 4：防御技術の役割と仕組み

境界防御を担う主要な装置

それぞれの装置が、異なる層の防御を受け持ちます。

ファイアウォール (FW)	IDS / IPS	WAF
不正な通り道をふさぐ**門番**。パケットフィルタリングを行う	**IDS**は検知・通知、**IPS**は検知・遮断（インライン配置が前提）	Webアプリの弱点（SQLi, XSS）を守る**Web専用の盾**

DMZの役割とセグメント設計

社内と外部の中間に設けられた「緩衝地帯」です。

DMZ（DeMilitarized Zone）は内部と外部の中間に置く**緩衝地帯**のサブネット

Webサーバーやメールサーバーなど、**外部に公開するサービス**を配置する

内部ネットワークへ直接アクセスされないよう、ファイアウォールで厳密に制御する

ネットワーク形態別のセキュリティ要点

環境に応じてリスクの種類と対策の優先度が変わります。

オープンネットワーク

外部からの不正アクセスやマルウェア流入対策が主眼

クローズドネットワーク

内部不正、なりすまし、媒体持ち出しへの備えが主眼

VPN (Virtual Private Network)

社外からの安全な通信経路。2FAとの併用で認証を強化

802.1Xによる端末接続の制御

正規の端末だけをネットワークに接続させる仕組みです。

ポートベース認証とも呼ばれ、**正規の端末だけ**をポートに通すことで、見知らぬ端末からの不正接続を防ぎます。

特に証明書を用いるEAP-TLSは、端末と認証サーバーが相互に検証しあうため、セキュリティ強度が非常に高いです。

【試験のポイント】

ポートベース認証＝802.1X

証明書ベース＝EAP-TLS