

応用情報技術者試験の午前・午後で頻出する主要なセキュリティ用語は、「攻撃手法」「防御・管理概念」「認証・暗号技術」の3つに分類して覚えるのが効果的です。

1. 攻撃手法・マルウェア

- **ゼロデイ攻撃**：ソフトウェアの脆弱性が公表され、修正パッチが提供される前に行われる攻撃。
- **クロスサイトスクリプティング (XSS)**：掲示板などに悪意あるスクリプトを埋め込み、閲覧者のブラウザで実行させる攻撃。
- **SQL インジェクション**：入力欄に不正な SQL 文を混入させ、データベースを不正操作・閲覧する攻撃。
- **クロスサイトリクエストフォージェリ (CSRF)**：ログイン状態の利用者に意図しないリクエスト（操作）を送信させる攻撃。
- **ファイルレス攻撃**：ファイルを残さずメモリ上でマルウェアを実行し、検知を逃れる手法。
- **リスト攻撃 (パスワードリスト攻撃)**：他から流出した ID・パスワードのリストを使い、別サイトへの不正ログインを試みる手法。
- **ランサムウェア / Emotet (エモテット)**：データを暗号化して身代金を要求するマルウェア、および巧みなメール返信型で感染を拡大させるウイルス。 [[1](#), [2](#), [3](#)]
- **リバースブルートフォース攻撃**：パスワードを1つに固定し、多数のユーザーID を総当たりで変えて侵入を狙う手法。
- **DMZ (DeMilitarized Zone)**：インターネット（外部）と社内ネットワーク（内部）のどちらにも属さない独立した中間領域のこと。

2. 防御・セキュリティ管理概念

- **ゼロトラスト**：「社内ネットワークだから安全」といった境界防御をせず、すべてのアクセスを信頼せず検証する考え方。
- **SIEM (Security Information and Event Management)**：各種ログを収集・統合管理し、不審な動きを検知・通知するシステム。
- **CASB (Cloud Access Security Broker)**：社内から利用するクラウドサービスを一元管理し、セキュリティポリシーを適用する仕組み。
- **サプライチェーン攻撃**：セキュリティが脆弱な委託先や関連企業を踏み台にして、本命の標的組織を狙う攻撃。

- **デジタルフォレンジック**：不正アクセスの原因や被害範囲を特定するため、電子データの法的証拠を収集・解析すること。
- **WAF**：Web アプリケーションへの不正なアクセスや攻撃を検知・防御する仕組み。
- **EDR**：PC などのエンドポイント端末を常時監視し、不審な挙動の検知や隔離を行う仕組み。
- 機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の3つ。：**情報セキュリティ3要素**

3. 認証・暗号・その他

- **多要素認証（MFA）**：「知識（パスワード）」「所持（スマホ等）」「生体（指紋等）」から2つ以上を組み合わせて認証する方式。
- **PKI（Public Key Infrastructure）**：公開鍵暗号方式を安全に運用するための基盤（認証局やデジタル証明書など）。
- **ペネトレーションテスト**：実際にシステムへ攻撃を試みて、脆弱性がないかを検査する手法。