セキュリティ

SaaS(Software as a service) -> 完成したソフトウェアをインターネット経由で提供するサービス　ユーザーの責任範囲はなし

PaaS (Platform as a Service) -> アプリケーション開発に必要なプラットフォームとインフラを提供するサービス　ユーザーの責任範囲はアプリケーション開発・運用

IaaS (Infrastructure as a Service) -> 仮想サーバー、ストレージ、ネットワークなどのインフラを提供　ユーザーの責任範囲はOSやミドルウェアのインストール、アプリケーション開発・運用　HaaS(hardware as a service) と同義

・チャレンジレスポンス方式は、平文のパスワードの代わりにサーバーからチャレンジを送信して、クライアントにチャレンジとパスワードからレスポンスと利用者IDを返すので、パスワードを盗まれる事を防止している

・ SSL(Secure Sockets Layer)/TLS(Transport Layer Security)
SSLは通信プロトコル。インターネット上で「安全な通信路（トンネル）」を作るための仕組み。その中で、**どんな暗号アルゴリズムを使うか** を取り決める。例：鍵交換にRSAやECDH、データ暗号化にAESなどを組み合わせる。TLSはSSLの後継。
仕組みは、
サーバー証明書 を使って「このサイトは正しい相手だよ」と確認できる。
公開鍵暗号と共通鍵暗号 を組み合わせて、安全に暗号通信を始められる。
以降の通信（リクエストやレスポンス）は全部暗号化され、途中で盗み見されても内容はわからない。

暗号化プログラム
・ DES -> Data Encryption Standard、鍵長が56bit
・ **AES -> Advanced Encryption Standard、2000年台から主流、**鍵長128bit / 192bit / 256bitから選べる。より詳しい解説を後述。

・ WAF -> Web Application firewall
通常のファイアウォールは**IPアドレスやポート番号** を基準にブロック/許可

WAFはWebアプリのリクエストやレスポンスの **中身（HTTPリクエストの内容）** を見て、不正を検知・遮断

WAFは次の不正を防げる

・SQLインジェクション
入力フォームに「' OR '1'='1」みたいな文字列を入れてデータベースを不正操作する攻撃。
・XSS（クロスサイトスクリプティング）
悪意あるJavaScriptを入力部分に入力して、ユーザーのCookieやセッションを盗む攻撃。
・OSコマンドインジェクション

サーバー側で任意のコマンドを実行させようとする攻撃。
・不正なBOTアクセス
スクレイピングや脆弱性スキャンをしてくる不審なリクエスト。

WAFは、
1. **リバースプロキシ型**
   ユーザーとWebサーバーの間にWAFを置き、すべての通信を検査する（CloudflareやAWS WAFなど）。
2. **ソフトウェア型**
   サーバー内にモジュールとして組み込む（Apacheの mod_security など）。
3. **アプライアンス型**
   専用のハードウェアとして導入する。

として導入できる。

目的は、
・ロードバランシング　複数のサーバーに処理を分散して、負荷を軽くする。
・セキュリティ　本当のサーバーのIPアドレスを隠して、攻撃を防ぐ。
・キャッシュ　よく使われるコンテンツをリバースプロキシが保存して、サーバーに負荷をかけずに返せる。
・SSL終端（TLS終端）　HTTPSの暗号化通信をリバースプロキシで処理して、裏のサーバーは平文でやり取りできる。

・リバースプロキシ -> サーバーの前段に立って、クライアント（ユーザー）からのリクエストを一度受け取り、その後ろにある実際のサーバー（Webサーバーやアプリケーションサーバーなど）に代わりに転送する仕組み

・DNS(Domain Name System)
ドメイン名とIPアドレスを結びつける仕組み。DNSサーバは、この対応関係を管理・検索してくれるサーバー。DNSキャッシュポイズニングは偽のドメイン情報をDNSサーバに送って、偽サイトに誘導する攻撃手法。

・OCSP(Online Certificate Status Protocol)
リアルタイムでデジタル証明書の失効情報をチェックしてくれるプロトコル。

・デジタルフォレンジックス

ディジタルフォレンジックスとは
コンピュータやネットワークに関連する証拠を科学的に収集・分析する技術・手法のこと
不正アクセス、マルウェア感染、情報漏えいなどの事件・事故が起きたときに、
証拠を改ざんされない形で収集し、原因究明や法的手続きに利用する。

種類もあって、

コンピュータフォレンジックス
- PCやサーバのハードディスク、メモリの解析
- 削除ファイルの復元、タイムスタンプの調査

ネットワークフォレンジックス
- 通信ログやパケットを収集・解析
- 攻撃経路の追跡、不正通信の特定

モバイルフォレンジックス
- スマホ・タブレットからの証拠収集
- 通話履歴、位置情報、SNSの痕跡

マルウェアフォレンジックス
- 不審なファイルを解析して挙動や感染経路を特定

・NAPT(Network Address Port Transition、IPマスカレード) -> グローバルIPとローカルIPを紐づける技術。
ブロードバンドルータはこの機能を持っている。
ブロードバンドルータ は、家庭やオフィスで **インターネット回線と複数の端末をつなぐための装置**

主な機能

1. **ルーティング機能**
   - LAN内の端末とインターネットとの通信を中継する
2. **NAT / IPマスカレード**
   - グローバルIPアドレスをLAN内の複数端末で共有可能にする
3. **DHCPサーバ**
   - 端末に自動でプライベートIPアドレスを割り当てる
4. **ファイアウォール機能**
   - 不正アクセスや不要な通信を遮断してセキュリティを確保
5. **無線LAN (Wi-Fi) 機能**（内蔵タイプの場合）
   - スマホやPCをワイヤレス接続

DMZ (DeMilitarized Zone, 非武装地帯) とは、インターネットと内部ネットワークの**中間に置かれるネットワーク領域** のこと。つまり、外部公開サーバーを隔離して配置する「緩衝地帯。

Wi-Fiの暗号化方式

1. 暗号化アルゴリズム

- **WEP (Wired Equivalent Privacy)**
  初期の方式。脆弱性が多くて、今は実質使用禁止。
- **WPA (Wi-Fi Protected Access)**
  WEPの次。暗号化に **TKIP** を採用。改良されたが今は非推奨。
- **WPA2**
  AES（CCMPモード）を採用して、強固になった。現在も広く使われる。
- **WPA3**
  さらに強化された最新規格。辞書攻撃や総当たり攻撃に強い。

2. **認証方式**
Wi-Fiに「誰が入れるか」を決める仕組み。主に2つある。

- **PSK (Pre-Shared Key) 方式**
  - 共通のパスフレーズ（Wi-Fiのパスワード）を全員で共有する。
  - 家庭用や小規模オフィスで一般的。
  - 例：**WPA2-PSK**（AES暗号化 + 事前共有鍵）
- **Enterprise方式 (802.1X/EAP認証)**
  - RADIUSサーバーを使って、ユーザーごとにID・パスワードや証明書で認証する。
  - 大企業や大学などで使われる。
  - 例：**WPA2-Enterprise**
  -

3、暗号アルゴリズム (各仕組みの中身)

🔑 1. RC4

- 種類：**ストリーム暗号**
- 特徴：1文字ずつ（ビットやバイト単位）暗号化していく方式。
- WEPや初期のTLS（SSL）で使われた。
- 問題点：設計上の脆弱性が見つかり、**今では安全でない**とされて廃止。

🔑 2. TKIP (Temporal Key Integrity Protocol)

- 種類：暗号プロトコル（WPA用に登場）
- 中身は基本的に **RC4を改良して使っている。**
- 改良点：
  - 鍵をパケットごとに変える（WEPは固定鍵だった）。
  - 鍵長を128bitにした。
- 問題点：
  - RC4ベースなので根本的に古い。
  - 2010年代以降は非推奨。

🔑 3. AES (Advanced Encryption Standard)

- 種類：**ブロック暗号**（128bit単位でまとめて暗号化）
- 特徴：
  - 2001年に米国標準規格として採用。
  - 鍵長は128/192/256bit。
  - いまだに強固で、Wi-Fi（WPA2, WPA3）やVPN、TLSでも現役。
- セキュリティ評価：
  - **現在も世界標準で安全とされている。**
  - 将来的には量子コンピュータ対策の新しい暗号（ポスト量子暗号）に置き換わる可能性はある。

・メールのプロトコル

1. POP3（Post Office Protocol）

- メールをサーバーから **端末にダウンロード** して保存する方式。
- ダウンロード後はサーバーから削除されるのが基本（最近は残す設定も可能）。
- → メールを1台のPCだけで管理したい場合に向く。

2. IMAP(Internet Message Access Protocol)

- メールを **サーバーに残したまま** 管理。
- 複数端末（PC・スマホ・タブレット）から同じメールボックスを使える。
- → GmailやOutlook.comなど、今の主流。

CRL -> Certificate Revocation List(証明書失効リスト)。もう使ってはいけない証明書一覧表。

SSH -> Secure Shell。安全なリモート接続プロトコル

SBOM -> Software Bill of Matrials(ソフトウェア部品表)
ソフトウェアを構成する、ライブラリ、モジュール、依存関係、バージョン、ライセンス情報などを一覧化したリスト

APT-> Advanced Persistent Threat 長期的に特定の企業を　　執拗に狙う攻撃

ゼロデイ攻撃 (修正前の脆弱性を突く攻撃) などがよく使われるらしい。

TPM -> Trusted Platform Module
PCのマザーボードについているセキュリティチップ。暗号化、復号、鍵ペアの生成、管理、ハッシュ値の計算、乱数生成、デジタル署名の生成、検証など色々やってくれる。

CA -> Certification Authorityは認証局で、公開鍵暗号を用いたデータ通信において、公開鍵の正当性を保証するデジタル証明書を発行してくれる。

エクスプロイトコード -> ソフトウェアの脆弱性を悪用した不正な動作を再現するために作成されたスクリプトやプログラム

CVSS -> Common Vulnerability Scoring System
情報システムの脆弱性の深刻度を同一の基準のもとで定量的に評価する手法

CCE -> Common Configuration Enumeration
コンピュータのセキュリティ設定項目ごとにつけられた識別子

CWE -> Common Weakness Enumeration
ソフトウェアの脆弱性の種類を識別する基準

CVE -> Common Vulnerabilities and Exposures
脆弱性に名付けられている識別子

SPF -> Sender Policy Framework

メールが「本当にそのドメインから送られてきたものか」を検証する仕組み

耐タンパ性
機器やデータが改ざんされたり、不正にアクセス

SAML(Security Assertion Markup Language)
XMLベースのメッセージのやり取りによって、複数のシステムで認証情報、属性情報、権限の認可情報を交換する

サンドボックス
外部から受け取ったプログラムを保護させた領域で動作させることによって、システムが不正に操作されるのを防ぎ、セキュリティを向上させる仕組み

リゾルバ
リゾルバとは、利用者からの名前解決要求に対して、ネームサーバに問い合わせをして、結果をクライアントに返すソフトウェア
オープンリゾルバは、インターネット上で公開されている、外部の不特定多数からの問い合わせに対しても、名前解決を処理するようになっているDNSサーバ。

基本構造（デジタル署名）

1. **送信者が秘密鍵で署名する**
    - メッセージ本文からハッシュ値を計算する
    - そのハッシュを送信者の「秘密鍵」で暗号化 → 署名データ
2. **受信者が公開鍵で検証する**
    - 署名を「公開鍵」で復号してハッシュ値を得る
    - 自分で計算したメッセージ本文のハッシュと一致するか確認

🔷 **物理的・管理的セキュリティ対策 一覧**

対策名	内容
クリアスクリーンポリシー (Clear Screen Policy)	席を離れるときに画面をロックし、第三者に情報を見られないようにする。
クリアデスクポリシー (Clear Desk Policy)	席を離れるときに機密文書やUSBメモリを机に放置しない。机上は整理整頓。
アクセス制御 (Access Control)	入退室管理カード、ICカード、バイオメトリクスなどで許可された人だけ入れるようにする。
パスワード管理 (Password Management)	強固なパスワードポリシーを設定し、定期変更や多要素認証と組み合わせる。
画面覗き見防止 (Shoulder Hacking対策)	覗き見防止フィルタの使用、座席配置の工夫。
記録媒体管理 (Media Control)	USBメモリ・外付けHDDなどの持ち出しを制限、暗号化して管理。

廃棄管理 (Disposal Management)	機密文書はシュレッダーで破棄、HDDは物理破壊や完全消去ソフトで処理。
監視カメラ・警備員 (Surveillance)	重要区域に監視カメラを設置、警備員による巡回。
セキュリティゾーニング (Security Zoning)	機密度に応じてエリアを分け（執務室／サーバ室など）、入室を制限。
ワークエリアセキュリティ (Work Area Security)	社外での作業時に情報を保護（VPN利用、公衆Wi-Fi回避、画面ロック）。
持ち込み・持ち出し管理 (Device Control)	個人PCやスマホの社内持ち込みを制限。データ持ち出しは承認制。
教育・訓練 (Security Awareness Training)	従業員に対して情報セキュリティポリシーや注意事項を教育。
ログ監査 (Log Audit)	入退室やシステム利用ログを記録し、不正利用を監視。

🔷 **TCPとUDPの比較表**

項目	TCP	UDP
通信方式	コネクション型（接続確立が必要）	コネクションレス型（接続不要）
信頼性	高い（到達保証、順序保証、再送制御あり）	低い（保証なし）
速度	遅め（オーバーヘッド大）	速い（軽量）
データ指向	ストリーム指向（連続したバイト列）	メッセージ指向（独立したデータ単位）
ヘッダ長	20バイト以上	8バイト
主な用途	Web、メール、ファイル転送	音声通話、動画配信、DNS、ゲーム

🔷 SPF（Sender Policy Framework）

仕組み

- 送信ドメインのDNSに「このドメインからメールを送ってよいメールサーバのIPアドレス」を登録しておく
- 受信側は、送信元メールサーバのIPとDNSに登録されたSPFレコードを照合して正当性を確認

🔷 DKIM（DomainKeys Identified Mail）

仕組み

- 送信サーバがメール本文＋ヘッダに **電子署名** を付ける
- 公開鍵はDNSに登録
- 受信サーバはDNSから公開鍵を取得し、署名を検証 → 改ざんされていないか確認

🔷 PTR レコード（Pointer Record）

- DNS の **逆引きレコード**
- IP アドレス → ドメイン名 を解決するために使う
- メール送信時、受信サーバは送信元の IP アドレスに対して PTR を引いて「正しいドメイン名か」を確認することが多い

🔷 MX レコード（Mail Exchanger Record）

- DNS における **メール配送先サーバ** の指定レコード
- 「このドメイン宛のメールはどのサーバに送ればよいか」を定義する

🔷 SMTP（Simple Mail Transfer Protocol）

- メール送受信に使う **アプリケーション層プロトコル**
- TCP ポート 25（送信）、587（Submission）、465（SMTPS）で使われることが多い
- **送信時の流れ**：
  1. 送信者のメールクライアント（MUA）が SMTP で送信サーバ（MSA）へ送信
  2. サーバ間で SMTP を使ってメールを配送
  3. 受信側のメールサーバ（MX で指定されたもの）が受け取り、ユーザーは POP3/IMAP で読む

午後試験のミス

社外にモバイル PC 持ち出し時->ウイルス対策ソフトが最新か確認すること

ランサムウェアにバックアップを感染させない -> 社内 LAN に接続するのはバックアップ時のみにする

🔷 NTP とは

- TCP/IP ネットワーク上で **時計合わせを行う仕組み**
- OSI 参照モデルの **アプリケーション層** に属する
- UDP ポート **123 番** を使用
- インターネット上の「NTP サーバ」と通信して、自分の PC やサーバの時計を合わせる

バックドア通信と普通の通信の見分けはつかない

マルウェアが大量アクセス -> おそらく総当たり攻撃

認証プロキシを導入した場合、ユーザーID やパスワードがブラウザに保存されていると意味がない
なので、ブラウザのオートコンプリート機能を無効にする必要がある。

NTPはインターネット上のNTPサーバと通信して時計を合わせてくれる。
なので、NTPが稼働していないと、各機器のログに記録された事象の時系列の把握が困難になってしまう

🔷 **公開鍵暗号方式（Public-key Cryptography）**
公開鍵暗号には **2つの使い方** があります。
① 秘密性の確保（暗号化通信）

- **受信者の公開鍵で暗号化**
- **受信者の秘密鍵で復号**

② 認証・改ざん検知（デジタル署名）

- **送信者の秘密鍵で署名**
- **送信者の公開鍵で検証**

🔷 **ハイブリッド暗号方式（Hybrid Encryption）**
公開鍵暗号と共通鍵暗号を組み合わせた実用的な方式。

1. **共通鍵暗号**
    - 実際のメッセージは高速な共通鍵暗号（AESなど）で暗号化
2. **公開鍵暗号**
    - その共通鍵を「受信者の公開鍵」で暗号化して安全に送る

情報セキュリティマネジメントで維持すべき3つ要素として、機密性、完全性、可用性がある。

多層防御 -> 複数の異なる防御手段を組み合わせて総合的にセキュリティを強化

パスワードのさらなるテクニック

ペッパー -> 全ての利用者で共通の固定値をパスワードに追加しハッシュ化

ソルト -> 利用者ごとに異なるランダムな値をパスワードに追加し、ハッシュ化。

ペッパーのいいところは、ペッパーの値を別のところで保管する為、会員テーブルを取られてもペッパーは取られていないから大丈夫な状態にできる。

【権威DNSサーバー】
権威DNSサーバは特定のドメイン名に関する「正式な」情報を持っているサーバーを指します。
ted.comというドメイン名の情報はどのサーバーにて管理されているのか、その情報を持っているのは権威DNSサーバーとなります。
【キャッシュDNSサーバー】
キャッシュDNSサーバーは、DNSの情報を一時的な「キャッシュ」として保存しておくサーバー

共通鍵の方が暗号の処理は高速