ＫＷ備忘録

■メールとDNSキャッシュのセキュリティ一覧

**（１）メール関連**

**1. SPF（Sender Policy Framework）**

SPFは、送信ドメインのDNS（Domain Name System）に、正当な送信元IPアドレスの情報を登録し、受信側がその情報を基に送信者の正当性を検証する仕組みです。これにより、なりすまし**メール**の受信を防止します。

**2. DKIM（DomainKeys Identified Mail）**

DKIMは、電子**メール**に電子署名を付与し、受信側がその署名を検証することで、**メール**の送信者が正当であり、内容が改ざんされていないことを確認する技術です。これにより、**メール**の信頼性を向上させます。

（２）DNSキャッシュのセキュリティ

**3. DNSSEC（DNS Security Extensions）**

DNSSECは、DNSの応答にデジタル署名を追加することで、DNS情報の正当性と完全性を保証する拡張機能です。これにより、DNSキャッシュポイズニング攻撃などを防止します。

**4. ソースポートランダマイゼーション（Source Port Randomization）**

ソースポートランダマイゼーションは、DNSキャッシュサーバが権威DNSサーバに名前を問い合わせる際、送信元ポート番号を問い合わせごとにランダムに変更する手法です。これにより、DNS問合せへの不正な応答を防止します。

以下の表に、これらの技術の違いをまとめます。

|  | **技術名** | **主な目的** | **OSI参照モデル** | **IP**  **アドレス** | **デジタル**  **証明** | **ポート**  **番号** |
| --- | --- | --- | --- | --- | --- | --- |
| **メールの信頼性** | **SPF（Sender Policy Framework）** | りすまし**メール**の防止 | アプリケーション層 | **利用** | × | × |
| **DKIM（DomainKeys Identified Mail）** | **メール**の送信者認証と内容の改ざん検知 | アプリケーション層 | × | **利用** | × |
| **DNSキャッシュの信頼性** | **DNSSEC（DNS Security Extensions）** | DNS情報の正当性と完全性の保証 | アプリケーション層 | **利用** | **利用** | × |
| **ソースポートランダマイゼーション** | DNS問合せへの不正な応答の防止 | トランスポート層 | 利用 | × | **利用** |

※覚え方

SPF　IPアドレス

Dがつくものは、デジタル証明を使用する。

DKIM　メールの送信者の認証（デジタル証明）

ソースポートらダ枚ゼーション　ポート番号利用

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 部品名 | 直流を通す | 交流を通す | 変換する | 直流（DC）の特徴 | 交流（AC）の特徴 | 変換の役割（インバータ・コンバータ） |
| 半導体 | 〇 | 〇 | ◎ | 直流をスイッチングで制御 | 高周波信号の増幅や処理 | インバータでは直流をスイッチングして交流を生成する。コンバータではPWM制御で直流を調整。 |
| **パワー半導体** | 〇 | 〇 | **◎** | 高電圧・高電流の直流をスイッチング制御 | 高周波交流を生成または制御 | インバータでは直流→交流、コンバータでは交流整流や直流変換を行う。 |
| **ダイオード** | **〇（片方向）** | **×** | **◎** | 電流を一方向のみに流す | 整流には使用されるが交流そのものは通さない | コンバータでは整流（交流→直流）に使用される。 |
| **コンデンサー** | **×** | **〇** | × | 直流は遮断（充電後、電流を流さない） | 交流は通し、周波数が高いほど通りやすい | インバータでは高周波信号の平滑化、コンバータではリップル電圧除去に使用される。 |
| 抵抗器 | 〇 | 〇 | × | 電流を制限 | 周波数に影響されず動作 | スイッチング回路の電流制御や電圧分圧に使用される。 |



■エクスプロイトキット（exploit kit）は、OSやアプリケーションソフトウェアの脆ぜい弱性を悪用して攻撃するツールである。

■プロジェクトマネジメント・オフィス（PMO）」は、プロジェクトに関連するガバナンスのプロセスを標準化し、資源、方法論、ツール、及び技法の共有を促進するものとされている。したがって（ウ）が正解である。

■ITIL®1) (Information Technology Infrastructure Library) 2011 editionの

サービス・パッケージの「パッケージ」とは、「一式」という意味である。

サービス・パッケージは次のように構成されている。

サービス・パッケージ＝ コアサービス＋支援サービス（実現サービス＋強化サービス）

つまり、顧客の成果に直接つながり、サービスの核となる基本的なサービスである「コアサービス」、コアサービスのためのサービスである「実現サービス」、及び魅力的な品質を実現するための追加サービスである「強化サービス」の組合

せで構成された、特定の種類の顧客ニーズへのソリューションを提供する複数のサービスの集まり（一式）がサービス・パッケージである。

■要件定義プロセスは、システムの開発以前の超上流工程であり、そこで行うアクティビティ（活動）としては、ユーザがシステムに要求する機能要件と非機能要件の明確化、利害関係者の識別、要件の識別、要件の抽出、制約条件の定義などが掲げられている。選択肢の中では、「利害関係者の識別」が、要件定義プロセスで行うことである。

■TLO（Technology Licensing Organization）とは、技術移転機関の略称である。

大学にはたくさんの研究成果があるものの、その成果が産業に十分に活用されてこなかった現状や、特許の管理を行う組織があまり存在してこなかったことを受け、TLOの設立を政策的に支援するための「大学等技術移転促進法」が制定されTLOが整備されるようになってきている。TLOは大学の研究成果を特許化し、それを企業へ技術移転するための法人である。

■生産管理のIE（Industrial Engineering）分析手法に関する問題である。

ワークサンプリング法は、事務作業のように定量化しにくい作業について、ある作業状況に対して定期的な観測を何回も行い、得られた観測記録から作業量を分析する手法である。

■システム監査基準

〇ウォークスルー法とは、データの生成から入力、処理、出力、活用までのプロセス、及び組み込まれているコントロールを、書面上で、又は実際に追跡する技法をいう」と記載されている。

〇テストデータ法（あらかじめシステム監査人が準備したテスト用データを監査対象プログラムで処理し、期待した結果が出力されるかどうかを確かめる技法）～などが利用されることもある」と記載されている。

〇インタビュー法とは、監査対象の実態を確かめるために、システム監査人が、直接、関係者に口頭で問い合わせ、回答を入手する技法をいう」と記載されている。

〇「ドキュメントレビュー法とは、監査対象の状況に関する監査証拠を入手するために、システム監査人が、関連する資料及び文書類を入手し、内容を点検する技法をいう」と記載されている。

■バリューチェーン分析は、製品やサービスを提供する企業活動を、購買物流、製造、出荷物流、マーケティングと販売、サービスの五つの主活動と、主活動を支援する調達活動、技術開発、人的資源管理、全般管理の四つの支援活動に分け、各活動が生み出す価値と各活動に要するコストを把握して、企業が顧客に提供する製品やサービスの利益が、どの活動で生み出されているかを分析する手法である。

■3C分析……マーケティングを成功させるために、顧客（Customer）、競合他社（Competitor）、自社（Company）について分析する手法である。分析対象の顧客、競合他社、自社の頭文字を取って3C分析と呼ばれている。

■SWOT分析……企業の戦略立案において使用される分析手法であり、組織がもつ強み（Strengths）と弱み（Weaknesses）、組織の外的環境にある機会（Opportunities）と脅威（Threats）を評価する。

■ファイブフォース分析……企業が置かれている外部環境を、二つの外的要因（新規参入、代替品）と三つの内的要因（競争企業間の敵対関係、買い手、供給業者の交渉力）の五つの視点（外部環境の五つの力）で検討する分析手法である。ファイブフォース分析は競争戦略の策定に活用される。

■パテントプールとは、企業や研究機関が特許権をもち寄り、特許権を一括管理することで特許利用分野の拡大やライセンス料の管理をする仕組み

■EDI（Electronic Data Interchange）とは、異なる企業間における商取引のためのデータを、ネットワークを介してコンピュータ間でやり取りすることである

■SoE（System of Engagement）とは、エンゲージメントが意味するとおり**、“思い入れ”、“愛着”**など、お客様とのつながりを構築するためのシステム。

SoEの事例としては、購買履歴や閲覧履歴などに基づいてレコメンデーションをするショッピングサイトがある。

■定量発注方式とは、在庫量が事前に定めた水準を下回った時に一定量を発注する発注方式

■デルファイ法は、複数の専門家にアンケート調査を行い、その結果をフィードバックすることで、他の専門家の意見などを参考にしながら、集団としての意見を収束させていく手法である。

・ワークアラウンド

・ARP、RARP

・フォワードプロキシ、リバースプロキシ

IPS（Intrusion Prevention System；侵入防止システム）

チャレンジレスポンス認証方式とWPA2-PSK（Wi-Fi Protected Access 2 Pre-Shared Key）の比較

■ペトリネットは、並行して動作する機能間の同期を表現するものであり、その構造はプレース（状態）とトランジション（事象）という2種類の節点をもつ有向2部グラフで表される。

レビュー技法

1. インスペクション

- 作業成果物の作成者以外の第三者（モデレータ）が主導

- 公式な記録と分析を実施

- ソースプログラムだけでなく、各工程の文書なども対象

- 最も形式的で厳格なレビュー手法

2. ウォークスルー

- 作業成果物の作成者自身が主導

- インスペクションより非公式

- 開発メンバー間の相互チェックとして機能

- 技術水準の向上や意識統一にも効果的

3. パスアラウンド

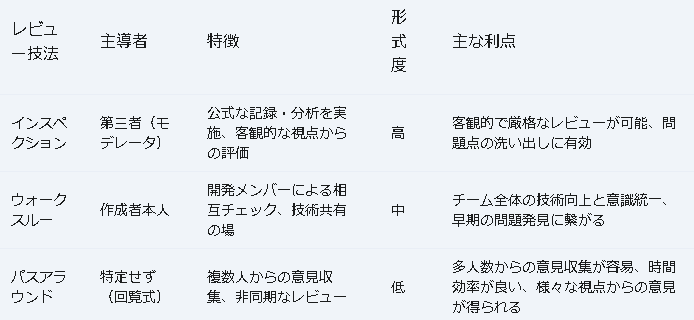
- 複数のレビューアに成果物を回覧して意見を収集

- 電子メールなどでの実施も可能

- 多人数からの意見収集に適している

- 時間的制約がある場合に効果的

以下、表形式で整理します：



 **クラッシング (Crashing)**

* **定義**: 作業全体の完成までにかかる期間を短縮する技法。
* **手法**: クリティカルパス上の作業に追加の人員や資金を投入して所要期間を短縮する。
* **適用範囲**: クリティカルパス上の作業に限定され、作業の順序は変更しない。

 **ファストトラッキング (Fast Tracking)**

* **定義**: 工程が完了する前に次の工程に着手することで全体の所要時間を短縮する技法。
* **手法**: 工程間の依存関係が緩やかな場合に、一部の工程を並行して実施する。
* **適用範囲**: 工程間の依存関係が緩やかで、並行実行が可能な場合に適用される。

 **クリティカルチェーン法 (Critical Chain Method)**

* **定義**: リソース（人員や設備）に基づいてスケジュールを調整する技法。
* **手法**: アクティビティの順序をリソースに基づいて調整し、リソース不足による遅延を防ぐ。
* **適用範囲**: アローダイアグラム上では並行可能な作業でも、リソース不足で順次実行する場合の最適化。

| **技法名** | **定義** | **手法** | **適用範囲** |
| --- | --- | --- | --- |
| **クラッシング** | 作業全体の所要期間を短縮する技法 | クリティカルパス上の作業に追加のリソースを投入 | クリティカルパス上の作業 |
| **ファストトラッキング** | 工程を並行して実施し全体期間を短縮する技法 | 工程完了を待たず次工程を開始 | 工程間の依存関係が緩やかな場合 |
| **クリティカルチェーン法** | リソースに合わせてスケジュールを調整する技法 | リソースに基づき作業順序を最適化 | リソース不足で順次実行が必要な作業 |

ソートのアルゴリズム

**1. クイックソート**

データを「中間に位置する適当な値」xx を**基準**として、並びを「**前半部**」（xx 以下）と「**後半部**」（xx 以上）に分けます。この分割を「再帰的に繰り返す」ことで整列を実現します。分割と再帰が特徴であり、大量のデータを効率的に処理するのに適しています。

**2. 基数ソート**

「有限**桁**の数値や文字列」を対象とし、まず「最下位**桁**」からデータを整列します。その後、「上（前）の桁」の値で順に整列を進め、最終的に「最上位**桁**」まで繰り返すことでデータを完全に整列します。桁ごとに分類して処理するのが特徴です。

**3. 選択ソート**

「対象のデータ」からまず「**最小値**」を選んで「**先頭に置く**」操作を行います。その後、「それ以外のデータ」から再び「最小値」を選び、「先頭の次」に置く。この操作を繰り返しながら整列を進めます。「最小値を選ぶ」プロセスが特徴です。

**4. 挿入ソート**

「新たなデータ」を「**整列済み**のデータ列中の**適切な位置に挿入**」する操作を繰り返します。この操作を通じて、整列済み範囲を「広げながら整列」していきます。「適切な位置への挿入」に焦点を当てて進むのが特徴です。

**違いのまとめ**

1. **クイックソート**は**分割**と再帰を用いて効率よく整列します。
2. **基数ソート**は**桁**ごとに分類しながら整列します。
3. **選択ソート**は**最小値**を見つけて順に並べます。
4. **挿入ソート**は新しいデータを適切な位置に追加していきます。

それぞれの特徴を理解することで、目的に応じて適切なソート方法を選べます。

■DisplayPortは、VESAが策定したPCと周辺機器を接続するデジタル映像インタフェースで、**1本のケーブルで映像と音声をパケット化**して**シリアル伝送**できる規格です。

■キャパシティプランニングとは、ユーザの要求や需要を分析し、システム資源や性能を見積もり、経済性や拡張性を考慮して最適なシステム構成を計画・構築するプロセスです。**現在の負荷状況**だけでなく、**将来の負荷や利用形態も予測**し、サービス水準を維持する構成を立案します。

以下は、フェールトレランスを含めた信頼性向上技術の解説です。

**1. フォールトアボイダンス**

「故障を未然に防ぐ」ことを目的とした技術と考え方です。「品質管理」や「システム構成要素の信頼性向上」によって、問題が発生しないように設計・管理します。故障が起きる前の段階で対策を講じる「回避（avoidance）」が特徴です。

**2. フェールセーフ**

システムに故障が発生した場合、「安全（セーフ）」を最優先する設計思想です。例として「道路の信号制御システム」があり、故障時には「全ての信号機を赤」にして運転を停止することで、重大な事故を防ぎます。「停止」または「制限された動作」を通じて安全性を確保するアプローチです。

**3. フォールバック（縮退運転）とフェールソフト**

「フォールバック」とは、システムの一部機能を縮退させながら「稼働を継続」する技術です。たとえば、部分的な性能低下を許容しつつ、システム全体の停止を回避します。  
これを可能にする設計思想を「フェールソフト」と呼び、完全停止よりも稼働継続を優先するのが特徴です。

**4. フェールトレランス**

「フェールトレランス」とは、故障が発生しても、システム全体の機能が「影響を受けない」ように設計された耐障害性技術です。冗長化された部品や並列処理を活用し、故障した部品を別の部品で補完します。たとえば、航空機の制御システムでは、複数のコンピュータが同時に同じ処理を行い、1台に障害が発生しても機能を維持するように設計されています。

**違いのポイント**

1. **フォールトアボイダンス**：故障そのものを「未然に防ぐ」ことを重視。
2. **フェールセーフ**：故障時に「安全性」を優先し、停止も含めた設計。
3. **フォールバックとフェールソフト**：故障後に縮退運転で「稼働を継続」。
4. **フェールトレランス**：故障が発生しても「機能を維持」できる耐障害設計。

これらの技術は、異なる状況で信頼性を高めるために適用されます。たとえば、安全が最優先される場合はフェールセーフ、稼働継続が重要な場合はフェールトレランスやフォールバックが適用されることが多いです。

■チャレンジレスポンス方式とWPA2-PSKの違いについて

### ****1. チャレンジレスポンス方式****

#### ****概要****

* サーバがクライアントにランダムなデータ（チャレンジコード）を送信します。
* クライアントはチャレンジコードとユーザーが持つパスワードを連結し、そのハッシュ値（レスポンス）を計算してサーバに送信します。
* サーバ側では、クライアントから受け取ったレスポンスと自分で計算した値を比較し、一致すれば認証を成功とします。

#### ****特徴****

* パスワード自体はネットワーク上を送信しないため、盗聴されても直接的にパスワードが漏洩するリスクは低い。
* 動的に生成されるチャレンジコードを使用することで、リプレイ攻撃（過去の通信データを再利用する攻撃）への耐性を持っています。

### ****2. WPA2-PSK****

#### ****概要****

* 無線LANのセキュリティ仕様の一つで、アクセスポイントと端末の相互認証、および通信フレームの暗号化と改ざん検出を行います。
* 相互認証では、アクセスポイントと端末の両方が同じSSID（ネットワーク名）とPre-Shared Key（PSK、事前共有鍵）を設定していることが必要です。
* 認証の際に、アクセスポイントまたは端末のMACアドレスと乱数をPSKによって暗号化して認証情報を作成し、通信相手に送信します。

#### ****特徴****

* 無線通信の暗号化にはAES（Advanced Encryption Standard）が使用され、通信内容の盗聴や改ざんを防ぎます。
* **PSKを事前に共有している端末だけがネットワークに接続可能**であり、SSIDとPSKが一致していない端末からの接続をブロックします。

### ****比較表****

| **項目** | **チャレンジレスポンス方式** | **WPA2-PSK** |
| --- | --- | --- |
| **目的** | サーバとクライアント間の認証を行うための方式 | 無線LANのセキュリティ仕様（相互認証と通信の暗号化を実現） |
| **認証方法** | サーバから送られたチャレンジコードを基に、ハッシュ値（レスポンス）を生成して認証 | PSK Pre-Shared Key（PSK、事前共有鍵）を用いてアクセスポイントと端末の相互認証を行う |
| **暗号化対象** | **認証情報のみ**（通信内容は対象外） | **無線通信全体をAESで暗号化** |
| **リプレイ攻撃耐性** | チャレンジコードがランダムであるため高い耐性を持つ | WPA2仕様により高い耐性を持つ |
| **主な使用範囲** | ネットワーク認証プロトコル（例：CHAP） | 無線LAN（家庭用やオフィス用ネットワークで広く利用） |
| **脆弱性** | パスワードそのものが漏洩した場合、認証の安全性が損なわれる可能性がある | 共有鍵が漏洩するとネットワーク全体が危険にさらされる |

以上のように、**チャレンジレスポンス方式は認証そのものを目的とし、パスワードを安全に扱う技術**であり、**WPA2-PSKは無線LAN通信のセキュリティを包括的に保護する技術**です。役割と使用範囲が異なるため、それぞれの特徴を理解して適切に選択することが重要です。