Domain 1：Security Architecture Modeling and Concepts（25問）

以下は、CISSP-ISSAP Domain 1「Security Architecture Modeling and Concepts」から25問のサンプル問題です。各設問には選択肢、正答、解説を掲載し、日本語訳と英語原文を併記しています。

問1.1

設問：データの機密保持（Confidentiality）を最重視するシステムで採用すべきセキュリティモデルはどれか？

A. Biba 完全性モデル（Integrity）
B. Clark-Wilson 商取引モデル（Transaction Integrity）
C. Bell-LaPadula 機密保持モデル（Confidentiality）
D. Brewer-Nash コンプライアンスモデル（Conflict-of-Interest）

解答：C

解説：

- Bell-LaPadulaモデルは「機密保持（Confidentiality）」を目的とし、ノン・リードアップ（no read up）／ノン・ライトダウン（no write down）で情報漏えいを防止する【Official (ISC)² Guide to the CISSP CBK, 5th Edition, Domain 1】。
- BibaはIntegrity、Clark-Wilsonは商取引の完全性、Brewer-Nashは利益相反防止に特化。

問1.2

設問：システムの完全性（Integrity）を重視する環境で適用すべきセキュリティモデルはどれか？

A. Bell-LaPadula 機密保持モデル
B. Biba 完全性モデル
C. Clark-Wilson 商取引モデル
D. Graham-Denning アクセス制御モデル

解答：B

解説：

- Bibaモデルは「Integrity」を中心に、ノン・ライトアップ（no write up）／ノン・リードダウン（no read down）で改ざんリスクを低減。
- Clark-Wilsonは業務トランザクション権限管理、Graham-Denningはアクセス制御行為のモデル化に利用。

問1.3

設問：企業全体のセキュリティアーキテクチャを体系的に策定する際、ビジネス要件・制約から始め、技術ソリューションへ落とし込むフレームワークはどれか？

A. Zachman Framework
B. TOGAF ADM (Architecture Development Method)
C. SABSA (Sherwood Applied Business Security Architecture)
D. COBIT (Control Objectives for Information and Related Technologies)

解答：C

解説：

- SABSAはビジネス要求→リスク分析→セキュリティソリューションの流れで6つの層を持つアーキテクチャフレームワーク。
- TOGAFはエンタープライズアーキテクチャ全般、Zachmanは情報システム構造の分類、COBITはガバナンス／管理目的に特化。

問1.4

設問：SABSAアーキテクチャの「コンセプト層（Conceptual）」に該当するものはどれか？

A. セキュリティサービスの技術実装
B. リスクマトリクスとビジネスモデル
C. 利用者認証フローの詳細設計
D. ネットワークセグメンテーションポリシー

解答：B

解説：

- コンセプト層はビジネスニーズとリスク戦略をマッピングする抽象レベル。
- 他の層：論理層→アーキテクチャ設計、物理層→技術実装。

問1.5

設問：セキュリティアーキテクチャ設計で「Defense in Depth（多層防御）」の適用例として最も適切なのはどれか？

A. 単一のファイアウォールでDMZを保護
B. IDS/IPS→ファイアウォール→アンチウイルスの多段防御
C. エンドポイントの暗号化のみ実施
D. ネットワークとアプリケーションを同一ゾーンに配置

解答：B

解説：

- 多層防御とは、複数の異なる制御を重ね、単一障害点をなくす原則。
- IDS/IPS、ファイアウォール、アンチウイルスを組み合わせ、異なるレイヤーで防御。

問1.6

設問：システム間の「信頼境界（Trust Boundary）」を明確化する主な目的はどれか？

A. ネットワーク帯域幅の最適化
B. セキュリティ制御配置と責任範囲の明確化
C. アプリケーション性能向上
D. サービスレベル合意（SLA）の交渉

解答：B

解説：

- Trust Boundaryは異なる信頼レベルを分離し、各境界でどの制御を適用するかを決定するために用いる。
- ネットワーク図やデータフロー図（DFD：Data Flow Diagram）で可視化。

問1.7

設問：脅威モデリング手法STRIDEの「R」は何を示すか？

A. Relevance（関連性）
B. Repudiation（否認）
C. Reliability（信頼性）
D. Resilience（回復力）

解答：B

解説：

- STRIDEはSpoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilegeの頭文字。
- Repudiationは行為否認を防ぐための非否認性ログや署名制御を意味。

問1.8

設問：Zachmanフレームワークで「What / How / Where / Who / When / Why」の問いを管理するセルの目的は何か？

A. セキュリティ要件を技術実装に落とす
B. エンタープライズアーキテクチャの多次元的ドキュメント化
C. 開発プロジェクト管理
D. 運用インシデント管理

解答：B

解説：

- Zachmanは6×6マトリクスで、異なる利害関係者（Planner ~ Subcontractor）が6つの問いを扱う。
- エンタープライズ全体を可視化し、整合性を保つ。

問1.9

設問：「最小権限（Least Privilege）」原則の主な効果として誤っているものはどれか？

A. インサイダーリスクの低減
B. 攻撃者の横展開（Lateral Movement）の抑制
C. 管理者の操作負荷の大幅軽減
D. 誤操作による被害範囲の限定

解答：C

解説：

- 最小権限は必要最小限の権限付与だが、権限管理の厳格化により管理者の操作負荷は増える場合がある。
- A, B, Dはいずれも最小権限によるメリット。

問1.10

設問：ISO/IEC 27001の「A.13 ネットワークセキュリティ管理」に沿ったネットワーク境界制御の例として最適なのはどれか？

A. ネットワーク境界にWAF（Web Application Firewall）を配置
B. クライアントPCにVPNクライアントを強制インストール
C. サーバーOSのパッチ適用
D. 無線LANのSSIDを非表示設定

解答：A

解説：

- A.13ではDMZや境界でのファイアウォール、IDS/IPS、WAFなどの導入を推奨。
- VPNクライアントやOSパッチ、SSID非表示は別の管理領域に該当。

問1.11

設問：「セキュリティゾーニング（Security Zoning）」の目的として最も適切なのはどれか？

A. ネットワークを複数の物理セグメントに分割
B. データ分類レベルに応じてアクセス制御を段階的に適用
C. 全社標準のアンチウイルス定義を一括管理
D. アプリケーションごとに別々のOSを使用

解答：B

解説：

- セキュリティゾーニングでは、ネットワーク上の仮想 / 物理ゾーンに機密度（Classification）を割り当て、境界制御を設計。
- 物理的分割のみではゾーニングの意義を十分に果たせない。

問1.12

設問：防御層（Layered Security）において「技術的制御（Technical Control）」に該当するものはどれか？

A. 安全な設計方針の文書化
B. アクセス制御リスト（ACL）
C. セキュリティ研修
D. インシデント対応手順

解答：B

解説：

- 技術的制御はシステム / ネットワークで動作する制御で、ACL、ファイアウォールルール、暗号化などを指す。
- 方針、教育、手順はそれぞれ管理的 / 人的 / 手続き的制御。

問1.13

設問：企業のネットワーク設計で「Air Gap（エアギャップ）」を適用する主なユースケースはどれか？

A. 開発環境と本番環境の統合
B. 機密性の高い研究データを外部ネットワークから完全隔離
C. VPN経由で社外からアクセス可能にする
D. クラウドサービスへの接続性を担保

解答：B

解説：

- Air Gapは物理的にネットワークを分断し、外部からの通信経路を完全に遮断する。
- 開発−本番統合、VPNアクセス、クラウド接続は相反。

問1.14

設問：MITRE ATT&CKフレームワークの「Tactic（戦術）」に該当する例はどれか？

A. Credential Dumping
B. Defense Evasion
C. CVE識別子
D. IOC（Indicators of Compromise）

解答：B

解説：

- Tacticsは攻撃者が達成しようとする目的レベル（例：Initial Access, Defense Evasion）。
- Techniquesは具体的手法（Credential Dumping）、CVEは脆弱性、IOCは痕跡情報。

問1.15

設問：リスク対応の一種「リスク転嫁（Risk Transfer）」の代表例はどれか？

A. インシデント発生時の保険加入
B. リスクを受容（Accept）すること
C. 予防的なパッチ適用
D. IDS/IPS導入による検知

解答：A

解説：

- Risk Transferは保険などの第三者を介し、損失を資金的に移転する方法。
- Acceptは受容、Patchは改修、IDS/IPSは検知（Mitigation）。

問1.16

設問：Business Impact Analysis（BIA）で求められる「RTO（Recovery Time Objective）」とは何か？

A. 最大許容データ損失時間
B. サービス復旧までに許容される最大時間
C. バックアップ実行間隔
D. コスト回収期間

解答：B

解説：

- RTOはシステム停止後、業務を復旧するまでに許容されるダウンタイムの上限。
- 最大許容データ損失はRPO（Recovery Point Objective）。

問1.17

設問：企業がデータを「パブリック / インターナル / 機密 / 秘密」の4分類する際に利用する枠組みはどれか？

A. Data Classification Scheme
B. Data Loss Prevention（DLP）ポリシー
C. Information Lifecycle Management
D. ISO 27018（クラウド個人情報保護）

解答：A

解説：

- Data Classification Schemeは機密度に応じてデータを分類し、アクセス制御や保護レベルを定義する枠組み。
- DLPは検知・防止技術、ILMはライフサイクル管理。

問1.18

設問：セキュリティアーキテクトが「共通セキュリティパターン」を利用する主なメリットはどれか？

A. すべての脅威を自動的に排除
B. 再利用可能な設計テンプレートで品質と効率を向上
C. ランタイムのパフォーマンスを必ず最適化
D. ビジネス要件の策定を不要にする

解答：B

解説：

- パターンは検証済みの設計手法を再利用でき、短期間で高品質なアーキテクチャを構築可能。
- 脅威排除やパフォーマンス最適化はパターンの副次効果ではあるが保証されない。

問1.19

設問：TOGAF ADM（Architecture Development Method）の「フェーズ A：アーキテクチャビジョン」で行う作業はどれか？

A. 詳細設計仕様の作成
B. 初期ビジネスケースとスコープの定義
C. ソリューション移行計画の構築
D. 実装ガバナンスの確立

解答：B

解説：

- フェーズ Aではビジネスドライバー、ステークホルダー、ハイレベル要件をまとめ、アーキテクチャのビジョンとスコープを定義。
- 詳細設計はフェーズ C/D、移行計画はフェーズ F/G、ガバナンスはフェーズ H。

問1.20

設問：セキュリティアーキテクチャ設計で「ミクロセグメンテーション（Micro-segmentation）」を適用する最大のメリットはどれか？

A. ネットワーク全体の帯域幅増加
B. ワークロード間の細かい通信制御で横展開を抑制
C. 単一のファイアウォールで全トラフィックを制御
D. 運用コストの劇的な削減

解答：B

解説：

- Virtual Network（Azure VNet）内でマイクロセグメントを作り、NSGやAzure Firewallでワークロード間の通信を厳格管理。
- 帯域幅増加やコスト削減は副次的効果。

問1.21

設問：セキュリティアーキテクチャの文書化に必須な「アーキテクチャビュー」に含まれないものはどれか？

A. ロジックビュー
B. 開発ビュー
C. プロセスビュー
D. パフォーマンスビュー

解答：D

解説：

- 標準的な4つのビュー：ロジック（機能）、プロセス（動的振る舞い）、開発（コンポーネント構造）、展開（物理配置）。
- パフォーマンスは別ドキュメントで管理することが多い。

問1.22

設問：クラウドプロバイダーの「セキュリティ責任共有モデル（Shared Responsibility Model）」において、インフラ層で顧客が負う責任はどれか？

A. ハイパーバイザーのパッチ適用
B. ゲストOSのセキュリティ設定
C. データセンターファシリティの物理セキュリティ
D. ネットワーク機器の保守

解答：B

解説：

- IaaSではゲストOSやアプリケーションのセキュリティは顧客責任。プロバイダーはハイパーバイザー、物理、ネットワーク機器を管理。

問1.23

設問：システム開発ライフサイクル（SDLC）における「セキュリティ設計レビュー（Security Design Review）」を行う適切なタイミングはどれか？

A. 要件定義フェーズ終了直後
B. コーディング完了直後
C. 運用移行フェーズ開始時
D. 障害対応後

解答：A

解説：

- セキュリティ設計レビューは要件定義から詳細設計フェーズへの移行前に実施し、要件と設計の整合性 / リスクを早期検出する。

問1.24

設問：TPM（Trusted Platform Module）が提供する主要機能として誤っているものはどれか？

A. システム起動時のセキュアブートサポート
B. ハードウェアベースの乱数生成
C. エンドポイントのアンチウイルス制御
D. キーの安全な保管と使用

解答：C

解説：

- TPMはハードウェアベースのセキュアブート、鍵管理、乱数生成、プラットフォーム認証などを提供。
- アンチウイルスはソフトウェア制御であり、TPM固有ではない。

問1.25

設問：システムアーキテクチャ文書で「信頼度レベル（Assurance Level）」を示す目的はどれか？

A. 開発言語のバージョン管理
B. 実装コンポーネントのセキュリティ保証範囲の明確化
C. 運用マニュアルの目次作成
D. プロジェクト予算の算出

解答：B

解説：

- Assurance Levelはシステムやコンポーネントがどの程度のセキュリティ保証を満たすかを示し、テスト範囲や監査対象を明確化する。