はじめに

情報セキュリティ専門家には幅広い知識とスキルが必要とされており、その知識とスキルを有していることがセキュリティ担当者や専門家として認められる条件となっています。その一つの基準が、(ISC)² の CBK(Common Body of Knowledge：共通知識分野)です。CBK は、それを理解していることを証明する資格である CISSP と共に、多くの国や企業、組織で認められたグローバルな内容として注目を浴びています。

本書では、CISSP 認定保持者が知っておくべき 8 ドメインについて紹介します。

(ISC)² とは

(ISC)²(International Information Systems Security Certification Consortium：アイエスシー・スクエア)は、安全で安心できるサイバーセキュリティの世界を実現することを目的とした国際的な非営利団体です。高い評価を得ている CISSP(Certified Information Systems Security Professional)を始めとした各種資格を提供することにより、セキュリティに対して(ISC)² は網羅的、そして計画的にアプローチしています。サイバー・情報・ソフトウェア・インフラストラクチャセキュリティの専門家から成り立つ 14 万人を超える資格保持者は、その資格によって他との差別化を図るとともに、業界の発展に貢献しています。

(ISC)²は、情報セキュリティの共通言語となる CBK を策定し、情報セキュリティ人材評価におけるゴールドスタンダードとなる認証制度を開発、提供しています。あわせて、世界中の情報セキュリティ専門家を教育、認定することによって、CBK をグローバルでより良いものとし続けています。

CISSP とは

CISSP(Certified Information Systems Security Professional)は、(ISC)²が認定を行うベンダーフリー・カントリーフリーの情報セキュリティの専門家資格です。CISSP には、情報セキュリティにおける理論やメカニズムを理解するだけでなく、その知識を体系的かつ構造的に整理し、状況に応じた適切な判断を行うための、合理的かつ実践的な「知識」と「理解度」が求められます。

資格取得のためには業務経験が必要です。試験合格後の認定登録手続きで業務経験を明記した職務経歴書とエンドースメント(推薦状)を提出し、それを証明する必要があります。認定期間は 3 年間となっており、3 年毎の認定継続要件をパスすることが必要です。

ANSI(米国規格協会)より、ISO/IEC 17024 の認証を受けた厳正な資格開発、運用、運営、維持に加え、米国国防総省のキャリアパスにおいて取得が義務付けられている資格の一つにも認定されており、CISSP は知識と実務経験を兼ね備えた、常に最新の知識をもった情報セキュリティプロフェッショナルであることを証明します。

CBK とは

CBK は、(ISC)² CBK 委員会が、CISSP 認定試験の作成に先駆け、情報セキュリティ専門家が理解すべき知識を国際規模で収集し、分野(ドメイン)別に体系的にまとめたものです。

情報セキュリティの共通言語である CBK をベースとすることで、CISSP をはじめとする情報セキュリティ専門家は、地域や専門分野を問わず、円滑なコミュニケーションが可能となります。CBK は毎年、多くの世界各国のセキュリティのプロフェッショナルへの定期的なヒアリング調査を行い、「最新の知識」として更新、維持されています。その中で CISSP に必要とされるものをまとめたのが CISSP CBK 8 ドメインであり、CISSP 認定試験の範囲として活用されています。

CISSP の CBK は、2018 年 4 月にコンテンツを更新し、新たな知識が追加されました。

目次

CISSP CBK の8ドメイン

CISSP CBK は、以下の 8 ドメインから構成されています。

1．セキュリティとリスクマネジメント
2．資産のセキュリティ
3．セキュリティアーキテクチャとエンジニアリング
4．通信とネットワークのセキュリティ
5．アイデンティティとアクセスの管理
6．セキュリティの評価とテスト
7．セキュリティの運用
8．ソフトウェア開発セキュリティ

CISSP CBK 8ドメインは、機能だけではなく、保証についても説明されています。また、実際のシステムに実装できるように、具体的に記載されたものとなっています。

情報セキュリティの具体策となる「管理策(Control)」は、運用においてモニタリングされており、その結果が方針の策定にフィードバックされることで定期的な改善が行われます。

CISSP CBK 8 ドメインのキーとなるのは「アクセス制御」です。物理(環境)セキュリティにおける設計も、ネットワークの物理設計、論理設計、そしてファイルサーバ上での権限管理などもすべてアクセス制御として実装されます。具体的にどの管理策を採用するか、その決定においては「情報の分類」などの方針に沿って、「脅威」、「脆弱性」、「事業影響度」などが考慮されます。

CISSP には、情報セキュリティ専門家として、相応の知識とスキルが求められます。技術的な内容に関する知識だけでなく、方針を決定する判断力も必要とされます。管理策の選択においては、それぞれのメリット・デメリット、そして費用対効果などを比較対照して提示する力が必要になります。さらに、判断のためには情報収集する力も必要になります。情報収集のソースは、ネットワークの利用状況の結果や、コンプライアンスの遵守状況の結果です。そういった情報収集を行うという意味では、フォレジック捜査やインシデントレスポンスなども運用セキュリティの一環としてとらえられるべきでしょう。

国内においては JIS Q 27001 を基盤として情報セキュリティ専門家の育成をしていることが多く、情報セキュリティマネジメントをキーとして捉えがちですが、CISSP はマネジメントの仕組みを作るというより、情報セキュリティ全体をどのように具現化していくのか、どのように維持していくのかに重点を置いています。ISMS の構築をどのように行うのかだけではなく、その前段階となる設計、そして運用、管理における判断力が求められています。8 ドメインを学習する際には、何が優先事項であるかを考えながら内容を理解していくことが重要です。

1．セキュリティとリスクマネジメント

「セキュリティとリスクマネジメント」ドメインでは、情報セキュリティの基本的な考え方となるセキュリティ原則に関する知識が求められます。機密性、完全性、可用性などの原則を理解することと、幅広く一般的な情報セキュリティとリスクマネジメントに関する知識が必要です。

このドメインでは、セキュリティガバナンスとコンプライアンス分野をベースに知識とスキルを積み上げていかなければいけません。

CISSP には、情報セキュリティポリシーの策定やセキュリティ機能を実践するための手順を策定するスキルが求められます。それは、セキュリティ機能が慎重かつ一様に適用されるための成功要因となります。この他にも、情報と要件の収集、ビジネス影響度分析、目標復旧時点の設定を含む、事業継続計画におけるあらゆる側面が求められます。

本ドメインの中心はリスクマネジメントです。リスク分析、対策の選択と実施、モニタリング、報告、リスクフレームワークについての知識が求められます。さらに、脅威モデルの導入、ハードウェア、ソフトウェア、サービスの調達や運用に関する契約や管理など、リスクマネジメントの統合的な考え方も求められます。

人的セキュリティについては、ポリシー策定、セキュリティ教育や訓練、意識向上(気づき)トレーニングの計画、実行を含む維持管理のスキルが求められます。

最後に、(ISC)^2 が提供しているその他の資格と同様に、CISSP でも一般的な倫理考慮事項についての知識が求められ、更に資格所有者として求められる(ISC)^2 倫理規約について理解していなければなりません。情報セキュリティ専門家は自らの技能が、独立的で信頼され、一貫して倫理的かつ健全であることが求められることも理解しておく必要があります。

ドメインの主題となるキーワードと関連する要素

■機密性・完全性・可用性の概念の理解と適用
- 機密性
- 完全性
- 可用性

■セキュリティガバナンスの原則の適用
- リスクマネジメント
- ポリシーとセキュリティ対策の実装
- セキュリティ対策の有効性のモニタリング
- 意識向上(Awareness)
- 学習と成長
- 予算
- 評価基準
- リソース
- 役割と責任
- ガバナンスフレームワーク
- デューケア
- デューデリジェンス
- ISO/IEC 27000 シリーズ
- COBIT
- COSO
- ITIL

■コンプライアンス
- リスクマネジメント
- プライバシー関連法

■ガバナンス
- セキュリティガバナンス
- セキュリティ組織
- 役割と責任
- セキュリティ責任者
- セキュリティ担当者
- システム管理責任者
- 資産管理責任者
- セキュリティ管理フレームワーク
- ISO/IEC 27001
- ISO/IEC 27002
- COBIT
- ITIL
- RMF
- CSA STAR
- コンピュータ犯罪

■リスクマネジメント
- 資産
- 資産価値

- 事業影響度分析(BIA)
- 脅威
- 脆弱性
- リスク分析
- リスク評価
- リスク対応
- セキュリティ対策
- モニタリング
- 評価基準
- リスクフレームワーク
- サプライチェーンマネジメント
- リスクベース管理
- 脅威モデル
- 最低限のセキュリティ要件
- サービスレベル要件

■コンプライアンス要件

- プライバシー
- 監査
- サイバー犯罪
- データ流出
- 知的財産
- デジタル著作権保護
- GDPR
- セキュリティポリシー
- セキュリティ標準
- セキュリティ手順
- セキュリティガイドライン

■人的セキュリティ

- 採用時のセキュリティ
- 雇用中のセキュリティ
- 解雇・退職時のセキュリティ
- サードパーティのセキュリティ
- 教育
- 訓練
- 気づき

■事業継続管理

- 事業継続
- 災害復旧
- 最大許容停止時間
- 復旧目標時間
- 復旧目標時点

ドメインで求められるスキルの例

- 機密性、完全性、および可用性の概念を説明できる
- 機密性、完全性、可用性の違いを説明できる
- セキュリティガバナンスの原則を理解している
- 組織のセキュリティ機能が、その組織のビジネス戦略、目標、使命、目的にどのように整合するかを説明できる
- 組織内のセキュリティに関連するさまざまな役割と責任を説明できる
- 組織内のガバナンスプロセスを理解し、それらがセキュリティにどのように影響するかを説明できる
- フレームワークについての概要を理解し、目的に応じてセキュリティフレームワークを適切に特定できる
- デューケアとデューデリジェンスの概念とそれぞれの違いを理解している
- 資産の評価、関連する課題、利益への貢献を理解している
- 脅威と脆弱性の違いを理解し、説明できる
- リスク評価と分析の一般的な手法を理解し、説明できる
- リスク管理の一般的な 4 つの手法を理解している
- リスク管理の一般的な 4 つの手法から選択する方法を理解している
- セキュリティ管理策を選択するための共通の手法を理解している
- さまざまなタイプ、クラスのセキュリティ管理策のカテゴリを列挙できる
- セキュリティ計画とコントロールのモニタリングと測定の重要性と、これらをなぜ継続的に実施するのかを説明できる
- 共通のリスクフレームワークを理解している
- リスクベースのセキュリティ管理をサプライチェーンに適用し、サードパーティを使用してリスク評価とモニタリングを行うことができる
- 標準的な脅威モデルの概念を理解している
- 脅威モデリング手法を適用できる
- 共通の脅威とリスクを理解している
- サービスレベルアグリーメントの目的、契約をどのように強化するのか、それぞれにどの項目を含めるべきかを理解している
- 最低限のセキュリティ要件を決定し文書化できる
- コンプライアンス要件(法律、規制、基準、契約)のさまざまな形態を理解している

- 特にコンプライアンスのコンセプトを、最新のプライバシー要件との関連で理解し、実際に遭遇する典型的な規制を理解している
- 知的財産を保護するデジタル著作権管理(DRM)ソリューションの役割を理解している
- データおよび IT ツールの輸出入に関する近代的な国際法的規制を理解している
- 世界中の現在の個人情報保護法で使用されている共通のプライバシー条項を識別できる
- 文書化されたガバナンス(ポリシー、スタンダード、ガイドライン、プロシージャ)の階層を説明できる
- 共通の方針と手順を含む、人事のセキュリティ目標をサポートするためのさまざまな手段を理解している
- 現代の法的枠組みがどのように国際的なデータの流れに影響し、情報セキュリティ業界が多くのコンプライアンス要件をどの程度担当するかを説明できる
- セキュリティの訓練、教育、気づきの重要性と、それらの要素を区別する方法を説明できる
- 事業継続性(BC)と災害復旧(DR)機能の必要性を説明し、基本的な概念を理解している
- (ISC)^2 のメンバーが期待される行動基準および実績基準だけでなく、専門のセキュリティ実践者が守ることが期待される倫理基準を理解している
- リスク評価、リスク分析、データ分類、およびセキュリティ意識向上の概念を理解し、適用できる

2．資産のセキュリティ

「資産のセキュリティ」ドメインでは、情報のライフサイクル全体を通じた資産の入手、取り扱い、保護についての知識とスキルが求められます。情報分類と資産の取り扱いをベースに、情報、システム、ビジネス・プロセスなどの所有権についての理解も求められます。

データ化された個人情報の収集やストレージサービスが急速に発展した結果として、プライバシーに考慮した情報の管理も求められるようになりました。プライバシーについては、データオーナー、データ利用者、データの残留性の観点からの考慮が必要とされ、情報の収集やストレージの取り扱いに影響を与えるものとなっています。

情報の収集とストレージについて考慮する際には、データの保有についてのルールを明確にしておく必要があります。保有については、組織のルールだけではなく、法規制の観点からも考慮する必要があります。

CISSP には、適切なデータセキュリティ対策を選択できることが求められるため、特にこの分野については詳細な知識とスキルが必要です。

データの取り扱いについてはライフサイクルに従って取り扱い要件を理解しなければいけません。特にラベル付けや廃棄などの要件を評価し、これに基づいてポリシーや手順を策定できる知識とスキルが求められます。

ドメインの主題となるキーワードと関連する要素

■情報と資産
- 資産
- リソース
- 価値
- 資産の分類
- インベントリ
- オーナーシップ
- 保護
- 取り扱い

■資産のライフサイクル
- 分類
- カテゴリ化
- 分類ポリシー

■資産のオーナーシップ
- データサブジェクト
- データオーナー
- カストディアン
- スチュワード
- 個人データ
- データ制御
- データ処理
- 情報オーナー

■プライバシー保護
- プライバシー
- OECD プライバシーガイドライン
- 収集の制限

■資産の保有
- 情報ガバナンス
- 保有ポリシー

■データセキュリティ
- ベースライン
- ベースライン保護
- ベースラインカタログ
- 範囲の決定
- テーラリング
- NIST SCAP
- サイバーセキュリティフレームワーク
- データの状態
- データ保護
- リンク暗号化
- エンドツーエンドの暗号化

■取り扱い要件
- メディア
- マーキング
- 取り扱い
- 保管
- 記録保持
- 残留データ
- クリアリング
- パージング
- 破壊
- SSD
- クラウド上の残留データ

ドメインで求められるスキルの例

- 資産、情報、データ、リソースなどの重要な資産用語を理解している
- セキュリティ管理策が情報などの資産の価値によってどのように決まるかを説明できる
- 情報およびデータが、組織に対する資産価値に基づいて保護する必要がある貴重な資産の一例であることを理解している
- 資産分類が価値に基づいた資産保護の決定に役立つことを説明できる
- 資産のライフサイクルを説明できる
- データの分類が資産のライフサイクルにどのように適用されるかを理解している
- 資産や情報の所有および管理に関する責任と、責任の証明の重要性を理解している
- 所有者、カストディアン、スチュワード、コントローラ、およびプロセッサによる資産保護の責任と説明責任について説明できる
- 資産保護に関連する主要な用語を説明できる
- 今日の技術によって、個人情報およびプライバシーがどのように影響を及ぼすかを理解している
- プライバシーに関する法律および規制に従って情報主体の期待を説明できる
- 経済協力開発機構(OECD)のプライバシー保護に関するガイドラインの重要性を説明できる
- OECD ガイドラインに従って、プライバシー保護のための 8 つの原則を説明できる
- プライバシーに適用される収集制限の概念を理解し、説明できる
- 組織の要件によって、資産の保持と保持ポリシーの実装方法を理解している
- コンプライアンスや組織の要件を含む、データの保存と記録の保持の理由を説明できる
- 資産の長期保管に関する課題を理解している
- ベースライン保護を説明できる
- 組織が貴重な資産に関連する最低限のセキュリティを達成するために何ができるかを説明できる
- ベースラインにセキュリティコントロールがどのように含まれているか、およびそれらを実装する方法を理解している
- 資産保護に関して、ベースラインの保護とスコープとテーラリングを説明できる
- さまざまなデータの状態を理解し、それぞれにおいて保護する方法を説明できる
- 動作中のデータに関連するエンドツーエンドとリンク暗号化の違いを説明できる
- メディアごとに必要なコンテンツの保護方法を説明できる
- 資産の分類における表示要件とマーキング要件を理解している
- 分類されたメディアおよび資産の取り扱いが、許可されたものにのみ実施されるべきであることを理解している
- 資産の保管、利用、廃棄は、分類によってどのように指示されるかを理解している
- データの残存性とその資産価値への影響を理解している
- クリア、パージ、および破壊を含む、データの廃棄方法の違いについて説明できる
- データをクリア、パージ、および破壊するために使用される手法を説明できる

3．セキュリティアーキテクチャとエンジニアリング

「セキュリティアーキテクチャとエンジニアリング」ドメインでは、様々な問題(例えば、悪意のある行為、人的エラー、ハードウェアの故障や自然災害によるトラブルなど)が発生しても、必要なビジネス機能を続行する情報システムおよびそれに関連するアーキテクチャを構築することができる知識やスキルが求められます。これは、システムエンジニアリングにおける情報セキュリティ原則の適用ができるかどうかというスキルに関連します。

CISSP はセキュアな設計の概念や原則について理解している必要があります。

セキュリティモデルの基本的な概念を理解し、組織のビジネス要件とセキュリティポリシーに基づいた設計要件を満たすセキュリティ対策の選択ができるスキルが求められます。これらを実践するためには、情報システムにおけるセキュリティの制限と能力を正しく把握する必要があるため、それらに関する知識も求められます。

CISSP は継続的に情報システムの脆弱性を評価し、低減するための知識とスキルも求められます。具体的には、クライアントとサーバの脆弱性、データベースに関するセキュリティ要件、分散システムやクラウドに関するセキュリティや暗号システム、産業用の制御システムなどが対象となります。また、ウェブアプリケーションやモバイルデバイス、組込みシステムなどの脆弱性についても把握できる知識とスキルが必要です。

暗号は機密性、完全性、真正性を確保することが目的であり、情報の意図しない変更からの保護に有効な対策であるため、本ドメインでも詳細な知識が求められます。一般的な暗号の概念だけではなく、暗号のライフサイクル、システム、公開鍵基盤、鍵管理の実践、デジタル署名およびデジタル著作権管理の広範囲にわたる知識が求められます。また、セキュリティ専門家として暗号解読の攻撃手法(ソーシャルエンジニアリング、総当たり、暗号文、既知平文、頻度分析、選択暗号、実装攻撃など)を十分に理解しておく必要があります。

セキュリティエンジニアリングに関する知識は、情報システムの開発に限定されることなく、施設や設備の設計などの物理的なセキュリティに関する設計の原則についても知識が求められます。

ドメインの主題となるキーワードと関連する要素

■セキュリティアーキテクチャの原則
- エンジニアリングプロセス
- NIST SP800-160
- ISO/IEC 15026
- ISO/IEC/IEEE 15288
- INCOSE

■セキュリティモデル
- セキュリティモデル
- Bell-LaPadula
- Biba
- Brewer and Nash
- Clark-Wilson
- Graham-Denning
- Harrison, Russo, Ulman

■システムセキュリティ要件
- セキュリティ管理策
- 予防
- 検知
- 是正
- 管理策の選択
- ISO/IEC 27001
- NIST SP800-53
- COBIT
- ISO/IEC 62443
- 評価のクライテリア

■情報システムのセキュリティ機能
- アクセス制御
- プロセッサの状態
- メモリ管理
- プロセスの分離
- データの隠蔽
- 抽象化レイヤ
- セキュリティカーネル
- 暗号
- コード署名
- 監査

- 監視
- 仮想化
- サンドボックス
- ハードウェアセキュリティモジュール
- ファイルシステム属性

■セキュリティアーキテクチャにおける脆弱性

- ハッキング
- ソーシャルエンジニアリング
- マルウェア
- フィッシング
- クライアントベースシステム
- サーバベースシステム
- データベースシステム
- 産業制御システム
- クラウドベースシステム
- 分散システム
- IoT システム
- ウェブベースシステム
- モバイルシステム
- 組込みシステム

■ 暗号

- 機密性
- 完全性
- 信頼性
- 否認防止
- アクセス制御
- 鍵暗号
- 平文
- 暗号文
- 暗号システム
- アルゴリズム
- 暗号化
- 復号
- 鍵
- 暗号解読
- 暗号学
- コリジョン
- 鍵空間
- 初期化ベクタ
- エンコーディング
- デコーディング
- 置換
- 変換
- 転置
- 混乱
- 拡散
- アバランシェ
- キークラスタリング
- 同期
- 非同期
- ハッシュ
- デジタル署名
- 対称鍵
- 非対称鍵
- 電子認証
- 認証局
- 登録局
- ストリーム暗号
- ブロック暗号
- XOR
- 鍵長
- ブロックサイズ
- ケルクホフスの法則
- ワークファクタ
- 置換暗号
- 転置暗号
- ランニングキー
- ワンタイムパッド
- ステガノグラフィ
- ヌル暗号
- 共通鍵暗号
- DES
- 3DES
- CCMP
- ラインダール
- AES
- IDEA
- CAST-128
- SAFER
- Blowfish
- Twofish
- RC4/5/6
- 公開鍵暗号
- RSA
- Diffie-Hellman
- ElGamal
- 楕円曲線暗号
- MIC
- メッセージダイジェスト
- MAC
- HMAC
- ハッシュ化
- MD5
- SHA-1
- SHA-3
- HAVAL
- RIPEMD-160
- PKI
- X-509
- KEK
- ブルートフォース
- 暗号文単独攻撃
- 既知平文攻撃
- 選択平文攻撃
- 選択暗号文攻撃
- 差分解読
- リプレイ攻撃
- バースデーアタック

- 素因数分解攻撃

■物理的セキュリティ
- サイトデザイン
- ファシリティデザイン
- 境界セキュリティ
- ワイヤリングクローゼット
- 制限エリア
- ユーティリティ
- HVAC
- 火災予防
- 火災検知
- 防火／消火
- 災害

ドメインで求められるスキルの例

- セキュリティアーキテクチャの原則を使用してエンジニアリングプロセスを実装・管理できる
- セキュリティモデルの目的を識別できる
- 一般的なセキュリティモデルを識別できる
- セキュリティ要件とセキュリティ管理策を区別できる
- 管理策の種類を特定する
- 共通または継承可能な管理策を特定できる
- 適切なセキュリティ管理策を選択できる
- 主要なコントロールフレームワークを識別できる
- セキュリティ管理策を調整できる
- セキュリティ管理策の評価基準を識別できる
- システムセキュリティ機能の種類を識別できる
- 統合されたセキュリティ要素を採用できる
- クライアントベースのシステムにおける脆弱性と低減策を識別できる
- サーバベースのシステムにおける脆弱性と低減策を識別できる
- データベースシステムの脆弱性と低減策を識別できる
- 産業制御システム(ICS)の脆弱性と低減策を識別できる
- クラウドベースのシステムにおける脆弱性と低減策を識別できる
- 分散システムにおける脆弱性と低減策を識別できる
- Internet of Things(IoT)の脆弱性と低減策を識別できる
- Web ベースのシステムにおける脆弱性の評価と低減策を識別できる
- モバイルシステムの脆弱性を評価し低減策を識別できる
- 組込みシステムの脆弱性を評価し低減策を識別できる
- 暗号に関連する主要用語を理解している
- 機密性、完全性、真正性、否認防止性、アクセス制御などのセキュリティサービスが、暗号によってどのように実装されているかを理解している
- 対称および非対称の基本的な暗号の概念を理解している
- ハッシュアルゴリズムとデジタル署名を説明できる
- 鍵管理の重要性を理解している
- 暗号解読の手法を理解している
- セキュリティの原則を施設設計に適用できる
- 物理的なセキュリティ対策を実装し、管理できる
- ワイヤリングクローゼットおよび中間物流施設における物理的管理を実施および管理できる
- サーバルームやデータセンターの物理的な制御を実装し、管理できる
- 施設におけるセキュリティの導入と管理を実施できる
- 資産の保管庫におけるセキュリティの実装と管理を実施できる
- 制限区域・作業区域の物理的管理を実施し、管理できる
- ユーティリティと電力に関するセキュリティ管理の導入および環境管理ができる
- 空調(HVAC)の実装と管理について理解している
- 環境セキュリティの実装と管理ができる
- 防火、検出、抑制のための環境セキュリティの実装と管理について理解している

4．通信とネットワークのセキュリティ

「通信とネットワークセキュリティ」ドメインでは、ネットワークアーキテクチャ、伝送方法、トランスポートプロトコル、制御デバイスのほかオープンなネットワークやクローズなネットワークを介して送信される情報の機密性、完全性、可用性を維持するために利用されるセキュリティ対策の理解が求められます。

CISSP は、ネットワークの基礎(トポロジー、アドレス、セグメンテーション、スイッチングやルーティング、無線、OSI や TCP/IP モデルおよびプロトコルスイートなど)を十分に理解していることが求められます。また、セキュアなネットワークを実装するための暗号、ネットワーク機器のセキュリティ対策など広範なトピックについても理解しておかなければなりません。ネットワーク機器の(スイッチ、ルータ、無線 LAN アクセスポイントなど)の安全な設置と維持管理に関する知識とスキルが求められます。ネットワークにおけるアクセス制御、エンドポイントのセキュリティ、コンテンツ配信ネットワーク(CDN)についての知識も必要です。

CISSP はネットワークを利用した多くのアプリケーション(データ、音声、リモートアクセス、マルティメディアなど)の利用を推進するために様々な技術を利用して、セキュアな通信チャネルを設計および実装できるスキルが求められます。また、これらのアプリケーションに対する攻撃ベクトルの知識や、それらを防止、低減する知識やスキルについても求められます。

ドメインの主題となるキーワードと関連する要素

■ネットワーク設計

- ISO/IEC 7498
- OSI モデル
- TCP/IP モデル
- 物理層
- ネットワークトポロジ
- CSMA/CD、CSMA/CA
- コンセントレータ
- マルチプレクサ
- ハブ
- リピータ
- トークンリング
- FDDI
- ツイストペア
- 同軸ケーブル
- 光ファイバ
- DSL
- ケーブルモデム
- WiFi
- Bluetooth
- WiMAX
- 衛星チャネル
- CDMA
- GSM
- データリンク層
- MAC アドレス
- LLC
- ARP
- FCoE
- MPLS
- ブリッジ
- スイッチングハブ
- VLAN
- ネットワーク層
- ユニキャスト
- マルチキャスト
- ブロードキャスト
- IP
- IP アドレス
- IPv6
- ICMP
- IGMP
- OSPF
- ルータ
- ファイアウォール
- トランスポート層
- QoS
- TCP
- UDP
- ポート番号
- セッション層
- PAP
- PPTP
- RPC
- ISO 7498-2
- プレゼンテーション層
- ASCII
- EBCDIC

- Unicode
- アプリケーション層
- DHCP
- DNS
- SNMP
- LDAP
- HTTP

■サービスにおける考慮事項
- リモート会議
- PVC
- SVC
- 回線交換ネットワーク
- パケット交換ネットワーク
- 仮想ネットワーク
- SDN

■セキュアネットワークの要素
- ファイアウォール
- IDS/IPS
- ホワイトリスト／ブラックリスト
- プロキシ
- ポートアドレス変換

■セキュアネットワークチャネルの設計
- VoIP
- SIP
- P2P
- インスタントメッセンジャー
- IRC
- VPN
- L2TP
- IPSEC
- SSL/VPN

ドメインで求められるスキルの例

- OSI および TCP/IP のそれぞれのネットワークモデルのレイヤを説明できる
- OSI と TCP/IP ネットワークモデルの違いや共通点を説明できる
- OSI モデルの 7 つのレイヤに関連する技術および実装システム、プロトコルを定義する概念とアーキテクチャについて説明できる
- OSI モデルの 7 つのレイヤに関連する脅威を識別し、動作するシステムとプロトコルの適切な対策を説明できる
- モビリティとコラボレーションをサポートするサービスを提供する技術的な実装を識別できる
- 基礎となるコンポーネントやインフラストラクチャを抽象化して仮想化し、サービスメリットを関連付けるさまざまなネットワークサービスを説明できる
- 通信を保護し、要件に基づいて用途ごとに使用される関連ネットワークコンポーネントを認識できる
- OSI モデルの 7 つのレイヤに関連する特定の脅威に対応するための対策として、安全なネットワークコンポーネントの利用を実証できる
- リモートアクセスサービスとコラボレーションをサポートする安全な通信チャネルを定義できる

5．アイデンティティとアクセスの管理

「アイデンティティとアクセスの管理」ドメインでは、情報セキュリティに不可欠な、人と情報システムの相関、情報システム同士の相関、さらには情報システムの個々のコンポーネント間の相関に利用されるアイデンティティとアクセス権のプロビジョニングや管理に関連した知識が求められます。これらのセキュリティが損なわれると、攻撃者の不正アクセスによって機密性が侵害されます。情報セキュリティ専門家はこの問題に多大な時間を費やすため、この分野の知識やスキルも必要です。

このドメインでは、利用者、システムおよびサービスの識別と認可を扱います。CISSP には、ID 管理システム、単一要素認証や多要素認証、説明責任、セッション管理、ID 登録とその証明、ID フェデレーション、およびクレデンシャル(資格情報)管理システムに関する知識も求められます。

クラウドベースによる ID 管理やアクセス制御、またそれらと社内の ID 管理サービスとの統合についての知識も求められます。CISSP は認可に関する仕組み(ロールベース、ルールベース、強制アクセス制御、任意アクセス制御など)の実装と管理に関するスキルも求められます。

他のドメインと同様に、本ドメインでもシステムに対する攻撃やライフサイクルにわたる攻撃の防止や低減についての知識も求められます。

ドメインの主題となるキーワードと関連する要素

■資産への物理的・論理的アクセス
- アクセス制御
- 論理アクセス制御システム
- 物理アクセス制御システム

■プロビジョニングとライフサイクル
- ユーザアカウント
- システムアカウント
- プロビジョニング

■人、デバイス、サービスの識別と認証
- 識別
- 認証
- 認可
- 説明責任
- セッション管理
- RFC2965
- NIST SP800-63-3

■ID 管理の実装
- ID 連携管理
- SAML
- OAuth
- IdP
- SP

■認可の仕組みの実装と管理
- 任意アクセス制御
- 強制アクセス制御
- 非任意アクセス制御
- 役割ベースのアクセス制御
- ルールベースのアクセス制御
- 属性によるアクセス制御

ドメインで求められるスキルの例

- 物理的および論理的アクセス制御をセキュリティの実践に関連する環境に適用するための標準用語を特定できる
- 物理的および論理的アクセス制御を、セキュリティプラクティスに関連する環境に適用できる
- ユーザとシステムのアクセスレビューのプロセスを定義できる
- アイデンティティのプロビジョニングと抹消に必要な管理手法と種類を説明できる
- 人、デバイス、およびサービスの管理に使用する、識別、認証、認可の技術を分類できる
- ID フェデレーションをサポートする言語とプロトコルを説明できる
- ビジネス要件を満たし、フェデレーション環境を確立するための適切なテクノロジーとプロトコルを選択できる
- ビジネスにおけるセキュリティ要件を満たすさまざまなアクセス制御モデルを評価できる
- 識別、認証、認可との関係におけるアカウンタビリティの重要性を理解している

6．セキュリティの評価とテスト

「セキュリティの評価とテスト」のドメインでは、情報資産やそれに関わるインフラの評価をさまざまな技術やツールを用いて実施する知識とスキルが求められます。これらの評価は構造的な問題や設計上の欠陥、設定のミスやハードウェアやソフトウェアの脆弱性、コーディングのミス、その他の欠陥など、情報システムが期待通りに機能するために、リスクの識別や低減を状況に応じて実施します。CISSP には、組織における情報セキュリティの計画、ポリシー、プロセスおよび手順が適用されていることに関する継続な検証も求められます。

CISSP には、評価とテストの戦略を検証し、これらのテストを実行できるスキルが求められます。脆弱性検査、ペネトレーションテスト、代理トランザクション、コードレビューやコードテスト、ミスユースケース、およびインタフェース試験についての知識も求められます。

CISSP にはセキュリティポリシーとそれに伴う手順を継続的に、かつ一様に適用することが求められます。また、障害復旧や事業継続計画を維持管理、必要に応じて更新し、災害発生時にはそれらが目的に応じて確実に機能するようにしなければなりません。このため、本ドメインではセキュリティ運用におけるデータ収集に関する知識が求められます。アカウント管理、マネジメントレビュー、パフォーマンスとリスクの指標、バックアップの検証、セキュリティ訓練と意識向上(気づき)トレーニングおよび障害復旧と事業継続に関する知識も求められます。

セキュリティ評価とテストにおいては、適切なリスク低減戦略を策定し、実施できるだけの綿密な分析と、評価結果の報告がなければ意味をなしません。CISSP にはテスト結果の分析と報告を行うスキルが求められます。また、内部監査や第三者監査を実施または補助するスキルも求められます。

ドメインの主題となるキーワードと関連する要素

■評価、テスト、監査の戦略
- 内部テスト
- 外部テスト
- サードパーティテスト

■セキュリティ管理策のテスト
- 脆弱性テスト
- ペネトレーションテスト
- ログレビュー
- ログのセキュリティ
- 代理トランザクション
- リアルユーザモニタリング
- コードレビュー
- ユースケース／ミスユースケース
- ポジティブテスト／ネガティブテスト
- インタフェーステスト

■セキュリティプロセスデータ
- アカウント管理
- マネジメントレビュー
- KPI
- COSO

■テストの報告とレポートの作成
- テストデータの保護
- 個人識別情報

■セキュリティ監査
- SOC 1/2/3

ドメインで求められるスキルの例

- テストおよび監査の戦略を設計および検証するための主要な方法を説明できる
- ビジネス要件をサポートするテストおよび監査機能を設計および検証するための適切な戦略を選択できる
- セキュリティ制御テストに関連するログを保持する手法と、関連するレビューと保護のためのロギングシステムを準備する手法を説明できる
- アプリケーション開発および提供に関連するさまざまなセキュリティ制御テスト手法を分類できる
- アカウント管理およびプロセス承認に関連するテストおよび評価をサポートするセキュリティ関連手続きのデータ管理を選択できる

- 組織のシステムに対して内部的および外部的に使用するセキュリティ制御テスト手法を適切に適用できる
- 組織のガバナンス、コンプライアンス、ポリシー、および能力に合わせたトレーニングと気づきの重要な要素を説明できる
- テストデータを利用する際に重要な情報を保護するための手順を説明できる
- サービスプロバイダ監査のプロセスを説明できる
- ビジネスサポート要件に基づいて、適切な監査タイプを選択できる

7．セキュリティの運用

「セキュリティの運用」ドメインは、エンタープライズコンピューティングシステムの運用に対する情報セキュリティのコンセプトとベストプラクティスの適用に関わる広範なトピックを含んでいます。

情報セキュリティの専門家が、日常的に実行することが要求されるタスクおよびその状況を示すことを目的としています。

フォレンジック調査に関する知識およびそれらを指揮したりサポートしたりする能力についてのトピックが含まれ、様々な調査コンセプトの概念(証拠の収集と取り扱い、文書化と報告、調査手法およびデジタルフォレンジックを含む)に関する知識が求められます。また、運用状況、犯罪、市民、および規制の観点から調査の要件を理解する必要があります。

ロギングとモニタリングの仕組みづくりは、セキュリティの基盤となる機能です。フォレンジック調査のサポートに加えて、ログ取得記録とモニタリングは、インフラストラクチャの日常業務を俯瞰するのに役立ちます。侵入検知防御、セキュリティ情報とイベントモニタリングシステム SIEM(Security Information and Event Monitoring system)、および漏えいからの保護が含まれます。

また、「セキュリティの運用」ドメインでは、リソースのプロビジョニングとそれらのリソースのライフサイクル全体を通じた管理と保護も扱っており、リソースの保護に関するセキュリティ運用基盤についての知識も求められます。保護制御(ファイアウォール、侵入防止システム、アプリケーションホワイトリスト、アンチマルウェア、ハニーポットとハニーネットおよびサンドボックスを含む)の運用と維持ならびにサードパーティのセキュリティサービス契約と管理を行うことに関するスキルも求められます。パッチ、脆弱性および変更管理についての知識も必要になります。

さらに、インシデント対応と回復復旧、障害・災害復旧、および事業継続も含まれます。CISSP には、インシデント管理などに関するスキルについて、および障害・災害復旧プロセスの実装とテストを行い事業継続計画に参加する知識とスキルが求められます。物理的セキュリティと人と個人の安全に関するトピックも含まれています。

ドメインの主題となるキーワードと関連する要素

■セキュリティ運用
- 知る必要性
- 最小特権
- 責務の分離
- ジョブローテーション
- アカウント管理
- サービスレベルアグリーメント

■セキュアなプロビジョニングリソース
- 資産管理
- インベントリ管理
- 構成管理
- 変更管理
- パッチ管理
- 脆弱性管理

■リソース保護の技術
- メディア管理
- ハードウェア資産
- ソフトウェア資産

■検知と予防
- 脅威インテリジェンス
- サンドボックス
- ハニーポット
- ハニーネット
- マルウェア対策

■インシデント管理
- インシデント管理のフェーズ
- 検知
- 対応
- 緩和
- 報告
- 復旧
- 修復
- 学習と成長

■調査
- 証拠の収集と取り扱い
- 報告と文書化
- フォレンジック

■ログの取得とモニタリング
- 侵入検知
- 侵入防止
- SIEM
- 継続的モニタリング

■復旧戦略
- バックアップストレージ
- 復旧サイト
- 複合処理サイト
- レジリエンス
- フォールトトレランス

■事業計画と訓練
- 事業継続計画
- 事業継続テスト
- 災害復旧
- 災害復旧テスト

■人命の安全
- 旅行時のセキュリティ
- 緊急管理
- 脅迫

ドメインで求められるスキルの例

- 知る必要性、職務遂行、職務分離、最小特権など、基本的な情報セキュリティの実践の特徴を説明できる
- 特権アカウントと通常のユーザアカウントを保護するために使用される方法を区別できる
- 情報ライフサイクルの各段階のフェーズを説明できる
- SLA の目的と使用方法を説明できる
- 資産管理の目的と実践を説明できる
- 構成管理および変更管理を実施する目的と手法を説明できる
- パッチ管理を実装する利点、課題、および最良の方法を説明できる
- 物理的、論理的、管理的な対策の視点から、メディア(およびそれに含まれるデータ)を保護するための技術を説明できる
- ハードウェアおよびソフトウェア資産を保護することに関する一般的な脅威やリスクと、それらに対抗するための共通の対策を説明できる
- 第三者ベンダーに任せることができる組織のセキュリティの一般的な内容と、その関係を保護するためのベストプラクティスについて包括的に理解している
- サンドボックス、ハニーポット、ハニーネット、マルウェア対策ソリューションの使用など、一般的なセキュリティ対策の利点と課題を説明できる
- 共通のインシデント管理モデルのフェーズを列挙し、各フェーズに関連する利点や課題を説明できる
- 様々なタイプの調査(行政、民事、刑事、規制など)に共通する特徴を説明し、一般的な調査基準を説明できる
- 証拠の収集と取扱いに関連する課題と共通の活動を説明できる
- 望ましい証拠の特性を説明できる
- デジタルフォレンジックの実践を含む一般的な証拠処理技術を説明できる
- IDS や IPS の特性と目的を説明できる
- SIEM システムの構築および運用に関する目的と課題を説明できる
- 継続的なモニタリングの目的と、その目的を達成するために現在一般的に使用されているツール(データ損失防御(DLP)など)を説明できる
- 一般的なバックアップ戦略とさまざまな技術に関連する利点と課題を説明できる
- 一般的なバックアップ施設の特徴を説明できる
- RAID システムのレベルごとの特性など、高可用性環境に関連する技術と技法について説明できる
- ビジネス継続性と災害復旧のための適切な訓練と認識と、対応行動、関係者、コミュニケーション戦略、評価と回復に関連するプロセスの不可欠な要素を説明できる
- ビジネス継続性と災害復旧計画における演習の課題を説明できる
- ビジネス継続性と災害復旧におけるテストの一般的なタイプの特徴を説明できる
- 人事に関連する業務上の懸案事項と共通的なセキュリティを説明できる
- 集中環境および分散環境おける情報処理資産の保護と制御を説明できる
- セキュリティサービスの確実かつ効率的な運用を継続するために必要な毎日のタスクを実行できる

8．ソフトウェア開発セキュリティ

「ソフトウェア開発セキュリティ」ドメインは、ソフトウェアの開発、およびソフトウェアの開発環境に対するセキュリティコンセプト概念とベストプラクティスの適用に関わっています。ソフトウェア開発者や、ソフトウェアセキュリティエンジニアが環境内で運用しているソフトウェアに関するセキュリティ制御を評価、実行します。CISSP は、この目的を達成するためにソフトウェア開発のライフサイクルに照らしてセキュリティを理解し適用しなければなりません。CISSP は、ソフトウェア開発手法、成熟度モデル、運用および保守、変更管理、統合された製品開発チームの必要性を理解する必要があります。

また CISSP は、ソフトウェア開発環境においてセキュリティ管理策制御を実行できなければなりません。CISSP は、ソフトウェア開発ツール、ソースコードの弱点と脆弱性、構成管理のセキュリティを含む(これは、ソースコード開発、コードリポジトリのセキュリティおよびアプリケーションプログラミングインターフェースのセキュリティに関連しています)この領域分野のいくつかのトピックについての理解が求められます。

また CISSP は、ソフトウェア保護統制評価の領域分野についても知っている必要があります。この領域分野のトピックには、監査とログ記録(これは変更管理に関連しています)、リスクの分析と低減(これはソフトウェアセキュリティに関連しています)および取得されたソフトウェアのセキュリティ上の影響が含まれます。

ドメインの主題となるキーワードと関連する要素

■ソフトウェア開発ライフサイクル
- システムライフサイクル
- ソフトウェア開発ライフサイクル
- テストデータの要件
- 認証と認定
- 廃棄
- 運用
- 保守
- ソフトウェア開発手法
- 反復開発
- CMM
- SW-CMM
- DevOps

■セキュアコード
- プログラム言語
- 世代
- アセンブラ
- コンパイラ
- インタプリタ
- オブジェクト指向
- ポリインスタンス
- CORBA
- ライブラリ
- ツールセット
- ランタイム
- API
- REST
- 統合開発環境
- ソースコード分析ツール
- OWASP
- TCB
- リファレンスモニタ
- セキュリティカーネル
- メモリ管理
- 隠れチャネル
- TOC/TOU

■開発環境
- オープンソース
- DBMS
- リレーショナルデータベース
- SQL
- オブジェクトデータベース
- XML
- メタデータ
- OLAP
- ロック制御
- OLTP
- ナレッジマネジメント
- マルウェア
- ウイルス
- コードリポジトリ

■ソフトウェアセキュリティ
- NIST SP800-37
- RMF
- ログ
- 監査

- コード署名
- 再帰テスト
- 受入テスト

ドメインで求められるスキルの例

- 様々な開発手法について説明できる
- 組織が、機能成熟度モデル(CMM)などの成熟度モデルをソフトウェア開発に適切に対応させる方法を説明できる
- 運用と保守を理解している
- 変更管理の仕組みと、それがソフトウェア開発にどのように適用されるかを理解している
- DevOps を含む統合製品チーム(IPT)の価値を理解している
- 安全なコーディング標準とガイドラインを理解している
- プログラミング言語の進化と、それがセキュリティとどのように関係しているかを説明できる
- ライブラリとツールセットの利点を説明できる
- 統合開発環境とランタイムシステムの価値を理解している
- ソースコードレベルでセキュリティの弱点と脆弱性を理解している
- アプリケーションプログラミングインターフェイス(API)におけるセキュリティの具体的な実装と安全なコーディング手法を説明できる
- セキュリティを理解し、それがソフトウェア環境でどのように適用されるかを理解している
- コードリポジトリを保護することの重要性を説明できる
- セキュアなコーディングの側面としての構成管理の重要性を理解している
- ソフトウェアに対するすべての変更の監査とロギングの重要性を理解している
- ソフトウェアセキュリティにリスク分析とリスク低減がどのように適用されるかを理解している
- 取得したソフトウェアのセキュリティへの影響を評価する方法を説明できる

確認テスト

CISSP の問題は以下のように 4 択で出題されます。CBK の内容を理解する際の「気づき」として活用してください。

問題の正答は本書内には記載していません。CISSP に求められる判断力を知るために、考え方の一例として取り上げています。

1. インシデントレスポンスの最も重要な目的は、次のうちのどれか？

   A) 犯人の逮捕
   B) 情報漏洩の阻止
   C) ポリシー違反の発見
   D) 被害の最小化

2. コンピュータインシデント下におけるフォレンジック手順で最初にとるべき行動は次のうちのどれか？

   A) メモリ情報の取得
   B) システムの緊急停止
   C) 記憶装置の複製
   D) 事故現場の確保

3. BCP/DRP を策定する前にしておくべきことは何か？

   A) 予算の配分
   B) SLA の見直し
   C) 自組織の事業の分析
   D) バックアップシステムのアップデート

4. BCP/DRP に関する分析では、どんな要素に焦点をおくべきか？

   A) 情報システムの完全性
   B) 情報システムの可用性
   C) ビジネス機能の有効性
   D) ビジネス機能の可用性

5. 復旧(Recovery)計画では、何に焦点を置くべきか？

   A) 通常活動の再開
   B) クリティカル機能の再開
   C) クリティカルな資産の保護
   D) 代替サイトへの移行

6. BCP/DRP に関するテストでは、どんな要素に焦点をおくべきか？

   A) 基準への準拠性
   B) 業務の効率性
   C) 計画の有効性
   D) 情報システムの可用性

7. 以下の出入り口に関する物理的保護のうち、最も重要となる要素はどれか？
   A) 緊急時の非常口の確保
   B) 警備員の配置
   C) 耐火性に優れた素材の使用
   D) 入退室記録が自動的に収集できる仕組み

8. 物理セキュリティの目標として、一番関連性が低いのは次のうちのどれか？
   A) 遅延
   B) 検知
   C) 分割
   D) 判断

9. 防犯環境設計の観点から最も効果が高いものは、次のうちのどれか？
   A) 出入り口を目立たないようにする
   B) フェンスで囲う
   C) 窓に強化ガラスを使用する
   D) 無停電電源装置(UPS)の設置

10. 火災を検知したときに、最初にとるべき措置は次のうちのどれか？
    A) 従業員に避難を勧告する
    B) 火災抑止システムを起動する
    C) 災害復旧担当者に知らせる
    D) 防火扉の解除を起動する

11. 検出できない不正行為が発生しないように、責任の分担を推奨している原則は次のうちのどれか？
    A) 職務の分離
    B) 相互排除
    C) 知る必要性
    D) 最小特権

12. 運用セキュリティの検知的制御で例外が発生したとき、何が考えられるか？
    A) 誰かが印刷された機密レポートを不正に見ている
    B) 誰かが秘密レポートを不正に廃棄している
    C) 認可されたオペレーターが、認可されていない作業を行っている
    D) 認可されたオペレーターが、重要なコンソールのメッセージに対処していない

13. 構成管理は、コンピュータシステムに加えられる全ての変更が、特定可能で管理できる環境で行われるようにすると同時に、以下のどれを保証しているか？
    A) アプリケーションソフトウェアへの変更は、システムのセキュリティ機能をバイパスしないようにする
    B) 変更がセキュリティポリシーに悪影響を及ぼさないようにする
    C) オペレーティングシステムへの変更は、第三者の妥当性確認と検証を前提としている
    D) 技術文書内の変更は、高信頼コンピュータ基盤を正確に保っている

14. クリッピングレベルは、違反行為の追跡と分析にどのように役立つか？

A) クリッピングレベルは、通常のユーザエラーの基準を設定し、そのしきい値を超える違反行為は記録され、違反行為が発生した理由の分析に使われる
B) クリッピングレベルを使用すると、セキュリティ管理者は監査証跡を変更して、セキュリティに関係しているとみなされる違反行為のみを記録することができる
C) クリッピングレベルを使用すると、セキュリティ管理者は監査証跡を変更して、特権ステータスで利用者コードにアクセスしたユーザの活動のみを記録することができる
D) クリッピングレベルを使用すると、セキュリティ管理者は違反行為を受けたユーザコードに対して設定されたすべてのセキュリティレベルの減少を見ることができる

15. 効果的なアクセス制御を実施するために最も必要なものは、次のうちのどれか？

A) リファレンスモニタ
B) 資産の分類
C) 適切なアクセス制御リスト(ACL)を設計する技術
D) 幅広い製品の知識

16. 銀行の ATM では数字 4 桁を暗証番号として利用している。セキュリティの観点から最も適切に説明しているのは次のうちのどれか？

A) 現在、認証方法を生体認証に切り替える活動を行っている
B) 誕生日などを使わず、鍵空間を広く取ることでセキュリティを確保している
C) キャッシュカードとの併用によりセキュリティを確保している
D) 提供されるセキュリティは不十分なまま使われ続けている

17. 従業員が不正アクセスをしたことを特定するために必要なものは、次のうちのどれか？

A) 当事者の犯罪歴
B) ログの取得
C) 他の社員による目撃証言
D) 当事者の業務報告

18. セキュアであると信頼できるシステムは、次のうちのどれか？

A) システムの開発者が安全性を正確に説明できるもの
B) 組織の中で長い時間使われ続けたもの
C) 攻撃の対象にならないマイナーなもの
D) ペネトレーションテストの結果、欠陥や不備がなかったもの

19. サーバを攻撃されにくくするために、最も効果的な方法は次のうちのどれか？

A) OS の種類やバージョンを返さないようにする
B) ワンタイムパスワードを利用する
C) ログの削除を行う
D) 脆弱性の分析を行う

20. 法体系と第一次法源の組み合わせが適切なものは、次のうちのどれか？

A) コモンロー：神が創ったとされる法典
B) シビルロー：有識者が作成した法典
C) 慣習法：宗教体系に基づく法典
D) 混合法：法典と過去の判例を混ぜたもの

21. 数年以上にわたる長期計画において、セキュリティ計画上で最も必要なものは、次のうちのどれか？

    A) コーポレートガバナンス
    B) セキュリティポリシー
    C) エンタープライズアーキテクチャ
    D) システムセキュリティアーキテクチャ

22. OS の機能で確実に保護しなければならない要素は、次のうちのどれか？

    A) コンピュータへのウイルス感染
    B) メモリ内の情報漏洩
    C) アプリケーションにおけるバッファオーバーフロー
    D) 高可用性のハードディスク

23. セキュアなコンピューティングシステムで使用される論理的な分離を説明しているのは、次のうちのどれか？

    A) プロセスは、入力装置と出力装置に、異なるレベルのセキュリティを使用する
    B) 各プロセスは、許可されたドメイン外のオブジェクトにアクセスできないように制約されている
    C) プロセスは、外部プロセスによるアクセスを禁止するために、データと計算処理を隠す
    D) プロセスは、制御されているオブジェクトの粒度に基づき、アクセスを許可される

24. 導入を検討しているシステムのセキュリティについて、信頼性が高いと判断するには、次のうちのどの要素が必要か？

    A) システムの開発者が信頼性の高さを文書にまとめたもの
    B) 世界中で最も多く使われたシステムであること
    C) 組織のセキュリティポリシーに準拠していること
    D) 共通の基準に基づく監査により保証されること

25. 暗号の実装に関して最も注意すべき点は、次のうちのどれか？

    A) AIC の全てを提供すること
    B) アルゴリズムが公開されていない暗号を選択すること
    C) 広い鍵空間を利用するものを提供すること
    D) 最も長い鍵長を利用できるものを提供すること

26. ネットワークを構築する際に、最も優先されるべき事項は次のうちのどれか？

    A) 複数のファイアウォールを選択する
    B) 単一障害点を少なくする
    C) 高いスループット
    D) 暗号化の実装

27. ネットワークを分割(ゾーニング)する主な理由は次のうちのどれか？

    A) ネットワークアクセス制御を実装するため
    B) 情報資産を分類するため
    C) 異なるネットワークトポロジを接続するため
    D) ビジネスユニットとしてまとめるため

28. ルーティングプロトコルの主要な役割は次のうちのどれか？

A) 運用負荷を軽減する
B) ネットワーク機器をグループ化する
C) ネットワーク障害を回避する
D) パフォーマンスを向上させる

29. 共通鍵暗号 AES と公開鍵暗号 RSA は必ず解読できる。その理由は次のうちのどれか？

A) 解読はできない
B) 人類の技術は今後大きく進歩するから
C) すでに解読方法が見つかっているから
D) 暗号は時間稼ぎに過ぎないから

30. 信頼性をもって安全といえる暗号とは、次のうちのどれか？

A) 暗号アルゴリズムの作者が、安全な理由を公表したもの
B) 暗号解読の結果、解けなかったもの
C) 暗号アルゴリズムの利用者が、安全な理由を公表したもの
D) 法で定められた期間、事故が起きなかったもの

31. デジタル署名だけを利用した場合の、最大の問題点は次のうちのどれか？

A) デジタル署名から秘密鍵を推測される
B) 選択暗号文攻撃に弱い
C) 処理に時間がかかるため可用性に大きく影響する
D) デジタル署名の送り手が本人かどうかわからない

32. 情報を分類し、特定の保護手段をとる最終的な責任は誰にあるか？

A) セキュリティ管理者
B) 経営陣
C) データオーナー
D) データ管理者

33. デューケアの説明として、適切なものは次のうちのどれか？

A) 競合会社よりも高いレベルのセキュリティを維持すること
B) AIC 三要素をバランスよく向上させること
C) 他者が同じ立場に立ったときに行うと考えられる行動をとること
D) 組織としてのベストプラクティスを常に選択すること

34. セキュリティ計画を作成する組織が最初に行うことは、次のうちのどれか？

A) 組織の目標と目的の理解
B) 組織の情報資産の洗い出し
C) 組織の既存のセキュリティ対策の確認
D) 組織が準拠しなければならない法律の理解

35. 特定のリスク軽減コントロールを実施すべきかどうかを最も明確に示すことができる手法は、次のうちのどれか？

A) 脅威および脆弱性の分析
B) リスク評価
C) 年次損失予測(ALE)の計算
D) 対策の費用対効果分析

36. セキュリティ意識向上プログラムのひとつの目的は、何を修正することであるか？

A) 従業員の態度とアプローチ
B) 経営陣のアプローチ
C) 機密データを所持する従業員の態度
D) データ保護に関する企業の態度

37. システム開発ライフサイクル(SDLC)において、最初の段階からのセキュリティ活動が必要とされるのはなぜか？

A) セキュリティ活動の必要性を特定するため
B) 要件定義を有効にするため
C) 正確な実装をするため
D) SDLC を効率的、効果的にするため

38. ソフトウェアの変更管理が、厳格なプロセスで実施されるべき理由は何か？

A) 変更の効果の最大化
B) 変更の効果の保証
C) 変更による影響の緩和
D) 変更管理プロセスの確立

39. DBMS におけるセキュリティのテストは、どのような目的で実施されるべきか？

A) デッドロックの回避
B) アクセスコントロールの評価
C) トランザクションの記録
D) 変更管理の評価

40. Web アプリケーションが攻撃のターゲットとされやすい理由は、次のうちのどれか？

A) 攻撃が比較的容易である
B) 痕跡が全く残らない
C) ファイアウォールや IDS を回避できる
D) 脆弱性の解決手段がない

CISSP 受験から認定までの流れと認定維持

CISSP 認定試験

- **申込み(実施機関)**
  認定試験は、Pearson VUE にて実施されます。試験の申込みや会場などに関する情報は、Pearson VUE Web サイトを参照してください。
  https://www.pearsonvue.co.jp/Clients/ISC2.aspx

- **出題範囲**
  CISSP CBK 8 ドメイン

- **問題数**
  250 問／4 択 Computer Based Testing(CBT)(日本語・英語併記)
  250 問中、25 問は調査のために入っており、採点対象とはなりません。

- **試験時間**
  6 時間(途中休憩可・途中退出可)
  ・試験開始前に 30 分程度の試験説明があります。(必須)
  ・試験監督の監視のもとでの休憩となります。
  ・途中退出後は、試験会場に戻ることはできません。

- **受験料**
  699 米ドル

- **必須持ち物(忘れると受験不可)**
  写真・署名付き公的身分証明書と署名付き身分証明書(計 2 点)

  合格点
  1000 点満点中 700 点以上で合格
  (スケールドスコアなので、各問題の配点は同じとは限りません)
  受験後に会場で合否がわかります(非公式)。
  6 週間～8 週間後に公式な結果が電子メールで通知されます。不合格の場合には、8 ドメインについて、最もスコアがよかったドメインから最もスコアが悪かったドメインまでの 1～8 の順位が記載されます。

- **CISSP 試験ドメインの各ドメイン出題比率**

ドメイン	出題比率
1. セキュリティとリスクマネジメント	15%
2. 資産のセキュリティ	10%
3. セキュリティアーキテクチャとエンジニアリング	13%
4. 通信とネットワークセキュリティ	14%
5. アイデンティティとアクセスの管理	13%
6. セキュリティの評価とテスト	12%
7. セキュリティの運用	13%
8. ソフトウェア開発セキュリティ	10%
	100%

- **CAT(Computer Adaptive Testing)について**
  CISSP 英語版試験のみ CAT による試験が行われます。日本語を選択した場合には該当しません。
  CAT の詳細はこちらをご覧ください。
  https://www.isc2.org/Certifications/CISSP/CISSP-CAT

CISSP 認定要件

- CISSP に認定されるには、下記要件をすべて満たすことが必要です。

1. CISSP 認定試験に合格すること
2. CISSP CBK 8 ドメインのうち 2 ドメインに関連した 5 年以上の業務経験があること
   下記どちらかに該当する方は、1 年分の経験が免除され、4 年の業務経験で認定可能です。(免除は最長で 1 年分)
   ・大学卒業学位取得者
   ・(ISC)² が認める資格の取得者
   対象資格は https://www.isc2.org/Certifications/CISSP/Prerequisite-Pathway 参照
3. 実務経験が事実であることを証明すること
4. (ISC)² の倫理規約に合意すること
5. (ISC)² 認定資格保持者(CISSP, CAP, SSCP, CSSLP)から推薦されること
6. 無作為に行われる業務経験に関する監査に合格すること
7. 犯罪に関連した履歴に関する 4 つの質問事項に正しく答えること(試験登録時)

認定登録手続

- 推薦状(エンドースメント)をオンライン上で提出
  試験合格者は、CISSP として認定されるために、ご自身のプロフェッショナル経験を証明することのできる、現役の(ISC)² 認定資格保持者(CISSP, SSCP, CSSLP など)からのエンドースメント(推薦)を提出する必要があります。合格者に試験後 2 日以内に配信されるメールに、試験結果およびオンラインエンドースメント(推薦状)プロセスについての記載があります。

- 認定パッケージ
  手続き完了後、米国(ISC)² 本部から以下のものを含む認定パッケージが登録した住所に郵送されます。

  • 認定証
  • カード型の認定証
  • CISSP ラペルピン購入クーポン

CISSP 認定継続要件

- CISSP の資格を維持するためには、下記要件をすべて満たすことが必要です。

1. (ISC)² 倫理規約に従い行動する
2. 年会費を支払う(125 米ドル／年・複数の資格を保有している場合でも同額)
3. 継続教育単位(CPE)を 3 年間で 120 ポイント取得する
   (ISC)² 認定 CPE サブミッターによるトレーニングの受講や、その他ベンダーによる情報セキュリティ関連セミナー受講等で CPE を取得することができます(1 時間の教育受講で CPE 1 ポイント)。CPE は監査を受けることがあります。

その他

記載している情報は 2019 年 4 月現在の内容です。最新情報は(ISC)² ホームページにてご覧ください。

(ISC)² 日本語Webサイト	https://japan.isc2.org/
CISSP認定試験案内	https://japan.isc2.org/examination_cissp.html
(ISC)² 公式 CISSP CBK レビュートレーニング案内	https://japan.isc2.org/cissp_training.html

本書の取り扱いについて