INSPIRING A SAFE AND SECURE CYBER WORLD.

SSCP®

SSCP 7 ドメインガイドブック

SSCP®
Systems Security
Certified Practitioner

(ISC)²®

はじめに

情報セキュリティ実務担当者や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実務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SSCP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、SSCP認定保持者が知っておくべき7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。

SSCPとは

SSCP (Systems Security Certified Practitioner)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資格です。SSCPは、情報セキュリティが専業ではないものの、ネットワークやシステムの開発・運用などに従事し、技術的な観点だけではなく「組織」という観点から情報セキュリティを理解し、情報セキュリティ専門家や経営陣とコミュニケーションを図れることを目指す人材を認定します。また、情報セキュリティ専業で経験年数が少ない方にとっては、より実践に近い内容をグローバルの標準に則った内容で理解していることを証明できる資格でもあります。

SSCPは、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、情報セキュリティ&IT実務者がグローバルの共通言語と知識を保有している事を証明できる資格になっています。

CBKとは

CBKは、(ISC)² CBK委員会が、各種認定試験の作成に先駆け、情報セキュリティ実務担当者及び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、SSCPをはじめとする情報セキュリティ実務担当者や専門家は、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、世界各国の多数のセキュリティのプロフェッショナルに定期的なヒアリング調査を行い、「最新の知識」として更新、維持しています。その中でSSCPに必要とされるものをまとめたのがSSCP CBK 7ドメインであり、SSCP認定試験の試験範囲として活用されています。

SSCPのCBKは、2018年11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

SSCP CBK の７ドメイン

SSCP CBK は、以下の７ドメインから構成されています。

1．アクセス制御
2．セキュリティの運用と管理
3．リスクの特定、モニタリングと分析
4．インシデントレスポンスとリカバリ
5．暗号
6．ネットワークと通信のセキュリティ
7．システムとアプリケーションセキュリティ

情報システムセキュリティの中心はアクセス制御であり、これを実現するための様々な方策を論理的、物理的に展開していきます。SSCP では論理的アクセス制御を中心に構成されていますが、物理セキュリティの知識もアクセス制御に含まれます。

具体的な対策としてのネットワークと通信、暗号、アプリケーションについては、専門家がこれまでに経験した内容をカテゴリごとにまとめ、実際に対策を選択するときや、インシデントレスポンスにおける分析や対応を行う際、活用しやすいように体系化されています。

正しい管理策を実施しているかどうかは、機能面だけではなく、その効果についても測定しなければいけません。そのための情報を収集する手段として分析とモニタリング(監視)があり、情報セキュリティの目的と合致しているかどうか確認することが求められます。

情報セキュリティの目的や方針などは情報セキュリティの運用と管理のドメインで、その詳しい手順などはインシデントレンスポンス・リカバリのドメインにまとめられています。この中には情報セキュリティのライフサイクルだけではなく、事業継続計画や、災害復旧計画なども含まれており、情報セキュリティ管理者からの指示を適切に判断し、管理策を提案していくために必要な知識と手順が示されています。

SSCP CBK は、CISSP CBK には含まれている法律、倫理、セキュリティアーキテクチャやコーポレートガバナンスに関連する内容は含まれていません。一方で、SSCP と CISSP は同じセキュリティ戦略を共有するため、情報セキュリティの概念は両方の CBK に含まれています。

SSCP CBK では、現場の作業者や専門家が理解しておくべき情報セキュリティの知識がまとめられています。SSCP CBK では、情報セキュリティポリシーを作成するスキルよりも、そのポリシーに従ってセキュリティ機能要件を実装し、IT に特化したセキュリティを保証していくためのスキルに重点が置かれています。

1. アクセス制御

論理的なアクセス制御を中心に、アクセス制御の方針から具体的な管理策まで理解します。アクセス制御の４つの要素である、識別、認証、認可、説明責任を理解し、機能要件となるシステムの提供、そしてアイデンティティマネジメントなどのソリューションについて理解します。

ドメインの主題となるキーワードと関連する用語

アクセス制御の実装

- サブジェクト
- オブジェクト
- リファレンスモニター
- 情報管理モデル(IMM)
- 許可
- 強制アクセス制御(MAC)
- 非任意アクセス制御(NDAC)
- 任意アクセス制御(DAC)
- ルールベースのアクセス制御
- 役割ベースのアクセス制御(RBAC)
- ビューベースのアクセス制御(VBAC)
- コンテンツ依存型アクセス制御(CDAC)
- 一時アクセス制御
- 属性ベースのアクセス制御(ABAC)

アイデンティティマネジメントライフサイクル

- 新規ユーザーの登録
- プロビジョニング
- 証明
- 識別
- 認証
- 単一要素認証(知識ベース)
- 多要素認証
- 認証の種類
- 所有権ベースの認証
- 認可
- メンテナンス
- パスワード
- 所有権
- トークン
- 時刻同期パスワード
- 属性(バイオメトリック認証)
- バイオメトリックの分類
- バイオメトリックの精度
- サービス拒否
- 資格
- アカウンティング
- 特権アクセス

認証方法の実装と維持

- 分散型アクセス制御
- 集中型アクセス制御
- シングルサインオン(SSO)
- ケルベロス
- IDaaS
- セキュリティアサーションマークアップ言語(SAML)
- オープン認証(OAuth)
- ネットワーク、コミュニケーション、トラスト
- 信頼パス
- ネットワークアクセス制御の管理
- ネットワークアクセス保護
- 802.1x 標準
- 802.1x シングルサインオン
- リモート認証ダイヤルインユーザーサービス(RADIUS)
- RADIUS の脆弱性
- ターミナルアクセス制御システム

ドメインで求められるスキルの例

- リファレンスモニターを説明できる
- 情報マネジメントモデル(IMM)を説明できる
- アクセス制御モデルを説明できる
- 自組織に相応しいアクセス制御モデルの選び方を説明できる
- 職務の分離を説明できる
- アイデンティティマネジメントを説明できる

- アイデンティティマネジメントコンポーネント群を比較対照できる
- 認証手法の評価を説明できる
- 権限の段階を説明できる
- アカウンティングを説明できる
- IDaaS を説明できる
- シングルサインオンの利用を説明できる
- トラストモデルを説明できる
- WAN(Wide Area Network)をベースにした認証オプションにおける比較対照できる
- アクセス制御スタンダードとプロトコルを説明できる

2. セキュリティの運用と管理

情報セキュリティマネジメントにおける実行責任者として、関連文書の構築、運用、管理手法を理解します。情報セキュリティ責任者からの指示を的確に理解し、情報分類、完全性の確保、意識向上プログラムなど、現場における作業を統括し、実行できるスキルを身につけます。このドメインでは、物理セキュリティと倫理を取り扱います。

ドメインの主題となるキーワードと関連する用語

セキュリティ原則の理解

- よくある誤解
- 論点
- フォーカス
- ギャップを埋める
- 資産の保護
- 分類と資産価値
- 情報セキュリティの原則
- 機密性
- 機密データへのアクセス
- データ保護(知る必要)
- 保護された情報
- センシティビティ
- 完全性
- 否認防止
- 可用性
- クリティカル
- プライバシー
- 最小特権
- 職務の分離
- 多層防御

資産マネジメント

- 資産カテゴリ
- 資産の識別
- IT 資産管理(ITAM)
- 資産保護
- 資産リスク管理の責任
- 資産ライフサイクル
- 焦点を合わせる資産
- ハードウェア/ソフトウェアデバイス管理
- ハードウェア
- ハードウェアのインベントリ
- ハードウェアの調達
- ハードウェアの実装
- ハードウェアの運用とメンテナンス
- ハードウェアの廃棄(HDD)
- ハードウェアの廃棄(SSD)
- ソフトウェア
- ソフトウェアのインベントリ
- 構成管理
- 情報
- 情報の分類
- 分類プロセス
- プライバシー
- 情報の所有権
- 運用・メンテナンス
- 第三者/アウトソーシングへの影響
- サービスレベル契約(SLA)
- リスクと資産価値
- サードパーティ/アウトソーシングへの影響
- リスクと資産価値
- 人事
- 雇用
- 人材開発
- 退職
- 物理
- 訪問者
- 資産保護
- コントロールの選択

機能的セキュリティ管理策(ドキュメント、実装、維持)

- セキュリティ戦略
- セキュリティコンディション
- セキュリティプログラムの成熟度
- ポリシー
- ポリシーに関する基本的な考慮事項
- 機能的ポリシー
- ポリシー実装のサポート
- プロシージャー
- 標準とベースライン
- ガイドライン
- コントロール
- 定義されたコントロール
- 最初に提案された概要
- 予防的コントロール
- 反応的コントロール
- 補正的コントロール
- 階層化されたコントロール
- 実施／評価
- セキュリティ運用レビュー

変更管理

- 構成管理
- 変更管理
- 変更管理委員会
- リリース管理
- リリースマネージャ
- ベースライン
- 構成管理データベース
- コード署名
- リリース管理ツール
- システム保証とコントロールの検証
- パッチ管理
- ロールアウト
- 不正な変更の検出
- ファイル整合性チェック

物理セキュリティの運用

- 物理的セキュリティの目標
- 多層防御
- ドア
- ビル
- 訪問者のコントロール
- ドアロック
- ロックの種類
- ハイテク鍵
- ターンスタイル
- マントラップ
- 鍵のコントロール
- 窓
- ガラスの種類
- 道路
- CPTED
- 火災
- 消火
- ガス消火
- 音響
- ポータブル消火器
- 電力
- UPS と発電機
- その他の物理的セキュリティの考慮事項
- 暖房、換気、および空調(HVAC)
- 空気汚染
- 湿度
- 水
- 通信とサーバールーム
- 雷からの保護
- センサーと制御
- 照明とカメラ
- 金庫、金庫室、コンテナ

セキュリティ意識トレーニング

- 用語
- セキュリティ意識向上トレーニング
- セキュリティ意識向上プログラムの提供
- 重要な成功要因
- メッセージ
- 一般的なセキュリティ意識
- トレーニング
- 潜在的なトレーニングトピック
- ソーシャルエンジニアリング
- ソーシャルエンジニアリング攻撃
- セキュリティトレーニングプロバイダ
- 倫理
- (ISC)^2 倫理規約
- 倫理規約の序文
- 倫理規約の基準

ドメインで求められるスキルの例

- セキュリティの基本的な概念を説明できる
- CIA (セキュリティの３原則)の定義を説明できる
- 資産の保護を説明できる
- プライバシーの必要要件を説明できる
- 否認防止の必要性を説明できる
- 多層防御を説明できる
- 資産の定義方法について説明できる
- IT 資産管理(ITAM)について説明できる
- ハードウェア/ソフトウェアインベントリの作成手法について説明できる
- ハードウェア/ソフトウェアのライフサイクルについて説明できる
- ハードウェア/ソフトウェアインベントリについて説明できる
- 継続的な診断とリスク低減の利点について説明できる
- 安全なデータ消去を比較対照できる

- セキュリティポリシーを説明できる
- スタンダード及びベースラインにおけるポリシーの評価を説明できる
- コントロールに対する評価を説明できる
- 異なるタイプのコントロールを説明できる
- 構成管理について説明できる
- 変更管理委員会について説明できる
- 変更管理の目標の分析について説明できる
- リリースマネージャの役割について説明できる
- リリース管理の定義について説明できる
- リリース管理方針について説明できる
- リリースプロセスについて説明できる
- コード署名について説明できる
- システム保証の定義について説明できる
- パッチ管理について説明できる
- 不正な変更の検出について説明できる
- ファイルの整合性チェックについて説明できる
- 多層防御の要素について説明できる
- 鍵の種類と鍵の管理について説明できる
- ターンスタイルとマントラップを比較対照できる
- アンチパスバックについて説明できる
- ガラスの種類の評価について説明できる
- 火災検知と火災抑制技術について説明できる
- 音響衝撃について説明できる
- 電源の評価について説明できる
- 暖房換気と空調(HVAC)について説明できる
- 空気汚染と湿度について説明できる
- 物理的セキュリティ要素の推奨について説明できる
- セキュリティ意識向上トレーニングについて説明できる
- 成功要因について説明できる
- トレーニング手法について説明できる
- トレーニングトピックの定義について説明できる
- ソーシャルエンジニアリングの評価について説明できる
- (ISC)^2 倫理規約について説明できる

3. リスクの特定、モニタリングと分析

リスクマネジメントや分析の手順に加え、コンプライアンスマネジメントの重要な要素である改善提案のための情報収集、分析手法について理解します。監査における法的順守事項などについても理解し、公正で適切な手順を理解し、実施できるようにします。また、そのために必要となる技術的手順について理解します。

ドメインの主題となるキーワードと関連する用語

リスクマネジメントプロセスの理解

- プロセス
- リスクマネジメントの体制
- フレームリスク
- リスクマネジメントプロセス
- 脅威
- 脆弱性
- 影響
- 発生の可能性
- リスクを評価する
- リスク評価要因
- リスク対応
- リスクのモニタリング
- 継続的/コンプライアンスモニタリング
- モニタリング
- リスク管理のためのデータソース
- ソースシステムまたはレコードシステム(SOR)
- 脆弱性の識別
- 脆弱性評価
- 共通脆弱性評価システム(CVSS)

リスクマネジメントプロセス-対応

- プロセス-対応
- リスク評価プロセス
- 己の敵を知る
- リスク評価の難しい部分
- リスクプロファイル
- 定性的および定量的リスク評価の方法論
- リスクの可視性
- リスクレジスタ
- リスク耐性
- リスク対応の選択肢
- セキュリティ投資の利点
- 費用対効果
- その他の考慮事項
- セキュリティ予算
- リスク対応の選択肢
- 行動計画
- リスク受容レベル
- リスク評価のフローチャート
- リスク対応
- リスク回避
- リスク低減/低減プロセス
- リスク受容度
- 共有/移転リスク
- 残存リスク
- コントロールの有効性を評価する
- リスクの変化を監視する
- 新しい脆弱性

モニタリングシステムの運用と維持

- モニタリング用語
- 継続的監視およびその他の監視システムの運用と維持
- 主要分野のモニタリング
- 監査計画
- 継続的モニタリング
- センサーとセンサーネットワーク
- 物理センサー
- SCADA
- 侵入検知と侵入防止
- NIDS/NIPS
- ホストベースセンサー
- 検出エンジン(IDS/IPS)
- アプリケーションログ
- モニタリングの実装上の問題
- モニタリングの種類
- モニタリングの課題
- ロギング
- アプリケーションログ
- クリッピング
- ログ統合
- ログを保護する
- IP フロー
- イベント相関システム(SIEM)
- ネットワークセキュリティの強化と IT /セキュリティ運用の向上
- フルパケットキャプチャ
- データ損失防止

セキュリティアセスメント活動の実践

- セキュリティ評価
- テスト戦略
- テストの基本
- 脆弱性評価
- データ収集
- 脆弱性レポート
- SCAP
- 脆弱性テストのメリット
- 脆弱性テストのデメリット
- 潜在的な問題
- ホストスキャン
- ホストセキュリティ
- ネットワークトラフィックの種類
- セキュリティゲートウェイの種類
- 無線ネットワークテスト
- ペネトレーションテスト
- フェーズ 1: 準備
- フェーズ 2: 情報収集(偵察とネットワークマッピング手法)
- フェーズ 3: 情報評価とリスク分析
- フェーズ 4: 侵入活動
- フェーズ 5: 分析と報告
- ペネトレーションテストの高度な手順
- 監査結果
- セキュリティコンプライアンス
- コンプライアンス監査
- 調査結果の報告
- 可視化

ドメインで求められるスキルの例

- リスクマネジメントプロセスについて説明できる
- リスクフレームワークについて説明できる
- リスク概念の定義(例：脅威、脆弱性)について説明できる
- 共通脆弱性評価システム(CVSS)について説明できる
- モニタリング結果からレポートの結果を理解し説明できる
- ソースシステムの識別について説明できる
- リスクプロファイルについて説明できる
- 組織のリスク受容度/耐性の評価について説明できる
- 定量的および定性的リスクアセスメントについて比較対照できる
- リスク用語について説明できる
- リスク可視化について説明できる
- モニタリング用語を列挙できる
- 継続的モニタリングの設計について説明できる
- 監査計画手順の作成について説明できる
- センサーの種類と配置について説明できる
- ロギングプロセスの作成について説明できる
- セキュリティ情報とイベント管理(SIEM)システムについて説明できる
- パケットのキャプチャと分析について説明できる
- データ損失防止(DLP)ソリューションの評価について説明できる
- セキュリティアセスメント要件について説明できる
- テスト戦略の設計について説明できる
- 脆弱性評価について説明できる
- ホストスキャンについて説明できる
- ネットワークトラフィックの種類を比較対照できる
- セキュリティゲートウェイについて説明できる
- 無線テストについて説明できる
- ウォーダイヤリング/ドライビング/フライングを比較対照できる
- ペネトレーションテストを説明できる
- テスト結果を説明できる

4. インシデントレスポンスとリカバリ

事故対応分析などの活動に実際に参加するために、それぞれの活動における基本的な考え方や手順を理解します。それに伴い、事業継続計画や災害復旧計画などにおいて、実践的な提案をできるようになるための知識とスキルも身につけます。

ドメインの主題となるキーワードと関連する用語

インシデントライフサイクル

- インシデント対応
- 共通言語による会話
- 事業継続とインシデント対応
- インシデント対応の概要
- 準備
- インシデント対応ポリシーの要素
- インシデント管理計画のステップ
- ポリシー要素
- インシデント対応計画
- インシデントレスポンスチーム
- トレーニング
- インシデント対応ツール
- インシデントと)データが元の適正な状
- コミュニケーション計画
- 効果的なインシデントハンドリングのための要件
- インシデントの定義
- 検出と分析
- インシデント分析
- 情報ソース
- インライン SSL 復号デバイス
- インシデント文書
- インシデント管理計画のステップ
- 対応
- 封じ込め戦略に関する考慮事項
- 発見
- エスカレーション
- トリアージ、通知、封じ込め、回復および根絶
- 報告とフィードバックのループ(学んだ教訓)
- インシデント対応
- 管理策の実施

事業継続計画と災害復旧計画の理解

- 緊急時対応計画とプロシージャー
- 事業継続計画
- BCP と DRP の比較
- ビジネス影響分析(BIA)
- BIA プロセス
- ビジネス影響分析メトリクス
- 継続性復旧の要件
- BIA プロジェクトステージ
- 復旧戦略の選択
- 災害復旧計画
- 災害復旧計画- 情報技術の復旧
- 復旧戦略の選択
- バックアップと冗長性の実装
- 電子金庫(オンラインストレージ)
- リモートジャーナリング
- ハードウェア保護
- RAID
- 計画書の作成
- 回復
- 計画のテスト、保守、および実施
- 計画の確認とメンテナンス

フォレンジック調査の理解

- フォレンジック調査
- フォレンジックガイドライン
- 犯罪現場の説明
- インシデントレスポンスチーム
- 一般的なガイドライン
- 経験則
- 犯罪行為
- 主要なポイント
- 現場を保護する
- 証拠収集
- ロカールの交換原理
- ハッシュアルゴリズム
- 刑事責任
- ドキュメンテーション
- 5 つの証拠規則
- 分析
- NIST の推奨事項の説明
- 法的およびプライバシー上の懸念
- データのプライバシーと国境を越えた管理
- インタビュー

ドメインで求められるスキルの例

- インシデント対応の定義について説明できる
- 事業継続計画(BCP)のサブセットとしてインシデント対応について説明できる
- 準備フェーズについて説明できる
- インシデント対応ポリシー要素の定義について説明できる
- インシデント管理計画の作成について説明できる
- 通信プロセスの作成について説明できる
- インシデントの定義について説明できる
- 検出技術を比較対照できる
- ドキュメントの作成について説明できる
- 対応プロセスについて説明できる
- 封じ込め戦略の評価について説明できる
- 封じ込め、根絶および回復プロセスの設計について説明できる
- 管理策を比較対照できる
- 情報システムの危機管理計画について説明できる
- 事業継続計画(BCP)について説明できる
- 重要な指標の認識について説明できる
- DR 計画、種類、および資産の評価について説明できる
- 復旧サイトの評価について説明できる
- バックアップの種類と場所を比較対照できる
- ハードウェア保護の選択肢について説明できる
- テスト計画の設計と評価について説明できる
- フォレンジックについて説明できる
- 証拠の収集、調査および提示について説明できる
- インシデント対応チームのフォレンジックトレーニング要件を説明できる
- フォレンジックに関する一般的なガイドラインについて説明できる
- 現場を保全すること(封じ込め)の重要性について説明できる
- ロカールの原則について説明できる
- 5 つの証拠規則について説明できる
- 異なる種類の分析を比較対照できる
- 法的な影響について説明できる
- 国境を越えたデータの流れとその関連性について説明できる

5. 暗号

データ管理および通信における暗号技術について全般的に理解します。暗号が利用される環境について想定し、どのような暗号技術を利用するのが良いのかを判断するのに十分な知識を身につけます。

ドメインの主題となるキーワードと関連する用語

暗号の基本的概念の理解

- 暗号化プロセス
- 用語
- 初期化ベクター(IV)
- XOR
- 暗号システムのカテゴリ
- 暗号化の利点
- データセンシティビティと規制要件
- シャノンの法則
- 暗号に関する法的問題
- ユーザートレーニング
- セキュリティ意識トレーニングのトピック

暗号アルゴリズム

- 暗号アルゴリズムの評価
- 対称アルゴリズム
- 対称アルゴリズムのバージョン
- 対称アルゴリズムのメリットとデメリット
- ストリーム暗号
- ブロック暗号
- ECB
- CBC
- CFB
- OFB
- CTR
- ストリーム暗号とブロック暗号の比較
- DES
- 2DES
- 3DES
- AES
- CCMP を使用したカウンターモード
- 非対称アルゴリズム
- 非対称アルゴリズムの利点
- 非対称アルゴリズムの欠点
- Diffie-Hellman
- El Gamal
- Rivest – Shamir – Adleman(RSA)
- 楕円曲線暗号(ECC)
- 暗号の使用方法
- ハイブリッド暗号
- セッションキー

PKI

- 完全性
- ハッシュ
- 完全性チェック
- セキュアハッシュアルゴリズム(SHA-3)
- ハッシュアルゴリズムとメッセージ認証コードへの攻撃
- 誕生日のパラドックスとレインボーテーブル
- ソルト
- デジタル署名
- PKI
- 認証局(CA)
- X-509 証明書
- 証明書の失効
- Web of Trust

鍵の管理

- 基本的な鍵管理の概念
- ケルクホフの原理
- 鍵管理の進化
- 主な課題
- 鍵の数に関する課題
- 鍵の作成
- 鍵長
- 鍵クラスタリング
- 鍵管理
- 鍵配布
- 鍵の保管
- 鍵の破壊
- 鍵リカバリ
- 鍵エスクロー

セキュアプロトコル

- セキュアな通信の実装
- S/MIME
- S/MIME の利点
- SSL / TLS
- ステガノグラフィ
- NULL 暗号
- IPSec
- SA

- トランスポートモードとトンネルモード
- インターネット鍵交換(IKE)
- リモートアクセス
- 仮想ネットワークターミナルサービス
- 仮想プライベートネットワーク(VPN)
- VPN の種類
- 暗号解読
- 暗号解読攻撃の方法
- クリッピングレベル
- ステガナリシス

ドメインで求められるスキルの例

- 暗号について説明できる
- 暗号用語について列挙できる
- XOR 関数について説明できる
- 攪乱、拡散、アバランシェについて説明できる
- 暗号の利点について説明できる
- データ分類の定義について説明できる
- 法律と暗号の関連性について説明できる
- トレーニングの要件について説明できる
- 暗号の手法について説明できる
- 対称及び非対称暗号アルゴリズムについて比較対照できる
- 対称及び非対称暗号アルゴリズムのメリットとデメリットについて説明できる
- 保存されたメッセージと転送中のメッセージの違いについて説明できる
- ストリーム暗号とブロック暗号アルゴリズムの違いについて説明できる
- アウトバウンド鍵配送について説明できる
- 発信証明について説明できる
- PKI 及びその構成要素について説明できる
- 証明書の項目について説明できる
- Web of Trust について説明できる
- 完全性チェックの適用について説明できる
- ハッシュアルゴリズムについて説明できる
- 誕生日のパラドックスについて説明できる
- ソルトの利点について説明できる
- MAC と HMAC の違いについて説明できる
- 鍵管理の概念について説明できる
- ケルクホフスの原理について説明できる
- XML と ANSI の規格について説明できる
- 鍵マネジメントの要件について説明できる
- 鍵ストレージと破壊の課題について説明できる
- エスクローサービスについて説明できる
- 鍵破壊オプションについて比較対照できる
- 鍵防御技術について説明できる
- セキュアプロトコルについて説明できる
- SSL と TLS について説明できる
- IPSec とその実装について説明できる
- ステガノグラフィについて説明できる
- 暗号解読及びステガナリシスについて説明できる
- 異なるタイプの攻撃について比較対照できる

6. ネットワークと通信のセキュリティ

ネットワークにおける物理的および論理的な構成を知り、情報セキュリティに関わる問題点を特定できる知識を身につけます。ネットワークにおける、機密性、完全性、可用性、そして認証について理解し、攻撃に対する管理策や適正なプロトコルの選択などができるようなスキルを身につけます。

ドメインの主題となるキーワードと関連する用語

ネットワークの構成要素

- OSI と TCP/IP モデル
- OSI モデル
- OSI モデルの各レイヤとその機能
- レイヤ２フレーム
- IP
- レイヤ３パケット
- ルーティングプロトコル
- レイヤ４セグメント
- UDP
- TCP
- TCP ３ウェイハンドシェイク
- レイヤ５
- レイヤ７プロトコル
- データグラムの構築

ポートとプロトコル

- プロトコル
- ARP
- ネットワーククラス
- DHCP リース
- DNS
- グローバル DNS 構造
- DNSSEC と新しいレコードタイプ
- TCP
- UDP
- 伝送タイプ
- ICMP
- RPC
- ネットワークトポロジー
- トポロジーモデル
- メディアアクセス制御方法
- 伝送メディア
- 一般的に使用されるポートとプロトコル
- ウェルノウンポートとプロトコル
- SNMP
- HTTP プロキシ
- SCADA
- SCADA への攻撃

ネットワークへの攻撃と管理策

- サービスモデル
- 攻撃の方法
- 盗聴
- ネットワークへの攻撃
- プロトコルベースの攻撃
- SCADA への攻撃
- IP への攻撃
- TCP シーケンス番号への攻撃
- SYN フラッディング
- スマーフ攻撃
- フラッグル攻撃
- NFS 攻撃
- DNS 攻撃
- トラフィックシェーピング
- ネットワークアーキテクチャ
- オープンメールリレー
- DoS / DDoS
- SIP フラッディング攻撃

ネットワークセキュリティの管理

- ネットワークデバイスの識別
- レイヤ１デバイス(物理)
- レイヤ２デバイス(データリンク)
- レイヤ３デバイス(ネットワーク)
- ルータとスイッチ
- セグメンテーション(VLAN、ACL)
- VLAN
- 動作中の VLAN
- VLAN の利点
- MACsec(IEEE 802.1AE)
- MACsec の機能
- ネットワークベースのセキュリティデバイスに関する運用と設定
- 要塞化されたネットワーク
- ファイアウォールとプロキシ
- NAT
- PAT
- 様々なプロキシ技術
- VPN

- トンネリングプロトコル
- トンネリングファイアウォールとその他の制限
- ネットワーク侵入検知/防止システム
- SDN
- SDN とアーキテクチャ

無線ネットワークの設定と運用

- 無線技術の種類
- 衛星放送とマイクロ波
- bluetooth
- Wireless LAN
- WiMAX
- 無線通信の管理
- ワイヤレスセキュリティの問題
- アドホックモード
- インフラストラクチャモード
- WEP
- WPA
- TKIP
- WPA2
- WPA3
- 「駐車場」攻撃
- シェアードキー認証の欠陥
- SSID の欠陥
- WEP プロトコルの脆弱性
- TKIP への攻撃
- 無線デバイス
- 展開アプローチ

ネットワークアクセス制御

- コンピュータ通信
- PBX
- 携帯電話
- 交換回線
- X.25、フレームリレー、ATM
- MPLS
- MPLS のオプション
- ソフトウェアベースのテレフォニー
- コンバージド コミュニケーション
- VoIP
- SIP
- H.323
- パケット損失隠蔽
- FCoE
- iSCSI
- セキュアなデバイス管理
- 構成管理
- 攻撃と管理策

ドメインで求められるスキルの例

- OSI 参照モデル(OSI) と TCP/IP モデルを比較対照できる
- 7 層の機能について説明できる
- OSI に適応される主要なネットワーキングプロトコルについて説明できる
- ルーティングプロトコルについて比較対照できる
- 信頼できるパケット配信に要求されるステップを説明できる
- 主要なネットワーキングプロトコルについて説明できる
- ネットワーククラスについて説明できる
- IPv4 と IPv6 の違いについて説明できる
- DHCP と DORA 方式について説明できる
- DNS について説明できる
- 一般的に使用されるプロトコルについて説明できる
- 一般的なポートについて説明できる
- ネットワークトポロジーについて比較対照できる
- 異なるネットワークメディアについて比較対照できる
- プロキシタイプについて比較対照できる
- SCADA にリスクについて説明できる
- 攻撃の方法について説明できる
- OSI 層の攻撃について説明できる
- 異なる攻撃種類について比較対照できる
- ネットワークデバイス(ハブ、スイッチ、ルータなど)について説明できる
- セグメンテーション技術について比較対照できる
- MACsec について説明できる
- ネットワークの要塞化について説明できる

- SDN について説明できる
- トンネリングの利点について説明できる
- ワイヤレスコミュニケーション技術について説明できる
- ワイヤレスモジュレーション方式について比較対照できる
- ワイヤレスセキュリティの問題について説明できる
- ワイヤレスセキュリティプロトコルについて比較対照できる
- セキュアなワイヤレスネットワーク設計について説明できる
- アナログ電話回線(POTS)と PBX に関して説明できる
- コンバージド・コミュニケーションについて説明できる
- 交換回線網に関して比較対照できる
- 携帯電話ネットワークについて説明できる
- X.25 とフレームリレーについて説明できる
- MPLS について説明できる
- VoIP の問題について説明できる
- QoS と CoS について比較対照できる
- セキュアデバイスマネジメントについて説明できる
- 攻撃と管理策について説明できる

7. システムとアプリケーションセキュリティ

セキュアなソフトウェアを開発、取得する方法を理解し、セキュリティプロトコルの使用方法や安全なリモートユーザー環境を理解します。また、不正なコードやモバイルコードの概念や種類を幅広く知り、これらの攻撃に対する対処法などを適切に選択できるような知識を身につけます。攻撃を受けた際の対処法や再発防止策などの提案ができるようなスキルを身につけます。

ドメインの主題となるキーワードと関連する用語

ソフトウェア保護

- 保護対象の理解
- 誤った認識
- システムとアプリケーションのセキュリティ
- アーキテクチャの脆弱性
- アーキテクチャデザイン
- ソフトウェア
- SLC と SDLC
- SDLC ウォーターウォール
- SDLC のセキュリティ担当者への懸念
- 開発/取得/プロビジョニング
- ソフトウェアの種類
- 市販品(COTS)
- オープンソースソフトウェア
- エスクローサービス
- ソフトウェアライセンス
- シャドウ IT
- ソフトウェア制限ポリシー
- SaaS
- SaaS の利点
- データセキュリティ
- マスキング/難読化と匿名化
- トークン化
- データ保持ポリシー
- データの完全性の保護
- ランタイムアプリケーションの自己保護
- 表示されたデータの保護
- スワイプ攻撃
- 明白なチャネルと隠しチャネル
- データ削除の手順とメカニズム
- データアーカイブ

不正なコードと挙動の特定と分析

- 主要な概念
- マルウェアの種類
- ソーシャルエンジニアリング攻撃
- 攻撃者
- ゼロデイエクスプロイト
- Web アプリケーションベースの脆弱性
- OWASP
- CERT
- ハードニング
- マルウェアの検出と防止
- 管理策を展開する
- アプリケーションホワイトリスト
- アプリケーションホワイトリストのメリット
- アプリケーションホワイトリストのデメリット
- スキャナー
- 次世代型アンチウイルススキャンソフトウェア
- ジェネリック検知技術
- ビヘイビアブロックソフトウェア
- コード署名

エンドデバイスセキュリティの実装と運用

- トラステッドコンピューティングベース(TCB)
- トラステッドプラットフォームモジュール(TPM)
- MDM ソフトウェア
- リモートワーク
- テレワーク
- BYOD ポリシーに関する考慮事項
- IoT
- IoT 分野の成長
- 仮想マシン
- ハイパーバイザー
- テスト結果をセキュリティに加える
- 脆弱性スキャン
- 脆弱性テストソフトウェアカテゴリ
- 脆弱性テストの品質
- ホストセキュリティの考慮事項
- ファイアウォールとルータのテスト
- セキュリティ監視のテスト

クラウドセキュリティの設定と運用

- タイプ 1:ネイティブまたはベアメタルハイパーバイザー
- タイプ 2：ホスト型ハイパーバイザー
- 仮想化の種類

- サーバー仮想化
- ネットワーク仮想化
- デスクトップ仮想化
- アプリケーション仮想化
- ストレージ仮想化
- セキュリティ
- デスクトップ仮想化セキュリティ
- ネットワーク仮想化セキュリティ
- 仮想化ストレージの種類
- 仮想化ストレージ
- ホストベースの仮想化ストレージ
- ストレージデバイスベースの仮想化ストレージ
- ネットワークベースの仮想化ストレージ
- アーカイブとオフラインの仮想化ストレージ
- サンドボックスの仮想化ストレージ
- 他のストレージタイプ
- PaaS
- IaaS
- 仮想化環境への攻撃
- リスク低減の戦略

クラウドセキュリティと仮想化の設定と運用

- クラウドの 5 つの重要な特徴
- 展開モデル
- サービスモデル
- クラウド展開時の考慮事項
- クラウドストレージへのデータ分散
- ストレージタイプごとの脅威
- クラウド上のデータ損失防止に関する考慮事項
- ベストプラクティス
- 法的およびプライバシー上の懸念
- 管轄権および準拠法
- 共通のプライバシー規約
- 個人識別情報への定義済みコントロールの適用
- プライバシーレベル契約(PLA)
- クラウドセキュリティアライアンスクラウドコントロールマトリックス(CCM)
- CCM セキュリティドメイン
- データの保存と転送
- クラウド暗号化の課題
- クラウド内の鍵保管
- ソフトウェア環境における鍵管理

ドメインで求められるスキルの例

- ソフトウェアに関するよくある誤解について説明できる
- システムライフサイクル(SLC)及びシステム開発ライフサイクル(SDLC)の違いについて説明できる
- ソフトウェア開発、取得、プロビジョニングについて説明できる
- 市販品(COTS) について説明できる
- オープンソースとプロプライエタリ・ソフトウェアについて比較対照できる
- ソフトウェア・エスクローについて説明できる
- ライセンス問題に関する理解及び問題の解決策について説明できる
- SaaS について説明できる
- アプリケーションに属するデータセキュリティににについて説明できる
- 明白なチャネルと隠れチャネルの定義について説明できる
- ランタイムアプリケーション自己保護(RASP)ににについて説明できる
- 異なるタイプのマルウェアについて説明できる
- ウイルス、ワーム、トロイの木馬の違いについて説明できる
- ソーシャルエンジニアリング攻撃の異なるタイプの違いについて説明できる
- ボットネットとゾンビ PC について説明できる
- ウェブアプリケーションの欠点について説明できる
- サート(CERT)の役割について説明できる
- 異なる管理策の違いについて説明できる
- トラステッド・コンピューティング・ベース(TBC) について説明できる
- トラステッド・プラットフォーム・モジュール(TPM)のセキュリティ適用について説明できる
- モバイル・デバイス・マネジメント(MDM)について説明できる
- リモートワークのリスクについて説明できる
- IoT に関連するリスクの分析について説明できる
- 仮想化及びハイパーバイザーの役割について説明できる
- セキュリティアセスメント及び脆弱性テストについて説明できる
- 仮想化について説明できる

- タイプ 1 及タイプ 2 のハイパーバイザーについて説明できる
- 異なる仮想化オプションについて説明できる
- NaaS について説明できる
- DaaS について説明できる
- PaaS について説明できる
- IaaS について説明できる
- 仮想化ストレージについて説明できる
- 仮想化への攻撃方法に関する討論
- 仮想化セキュリティオプションに関する評価
- クラウドコンピューティングの概念について説明できる
- 異なるデプロイメントモデルとサービスモデルについて説明できる
- 法律とプライバシー問題について説明できる
- 発見されたセンシティブデータの分類について説明できる
- 個人識別情報(PII)に要求されるコントロールについて説明できる
- コントロールの定義とマッピングについて説明できる
- データの保存と転送について説明できる
- クラウド暗号化について説明できる
- クラウドにおける主要なマネジメントについて説明できる
- クラウド上のデータ損失保護について説明できる

確認問題

SSCP 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。SSCP 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. TACACS の 3 つの機能分野として知られている AAA ではないものは、次のうちのどれか？

A) 認証

B) 認可

C) 可用性

D) アカウンティング

2. Biba 完全性モデルの主要な 3 つのルールではないものは、次のうちのどれか？

A) アクセス制御サブジェクトは、より高い完全性レベルのアクセス制御オブジェクトにアクセスすることはできない

B) アクセス制御サブジェクトは、より低い完全性レベルのアクセス制御オブジェクトにアクセスすることはできない

C) アクセス制御サブジェクトは、より高い完全性レベルのアクセス制御オブジェクトを変更することはできない

D) アクセス制御サブジェクトは、より高い完全性レベルのアクセス制御オブジェクトからサービスを要求することはできない

3. アクセス制御システムの定常的モニタリングで考慮すべきことは、次のうちのどれか？

A) アクセスの変更の定期的なモニタリングは、不正使用や不正アクセスのリスクを軽減するのに役立つ

B) アクセス制御システム内のアカウントのすべての変更が、定期的に記録され、見直しされるべきである

C) 新規アカウント作成や、既存アカウントへの追加での特権付与について、きちんと承認されているかどうかに対して特別な注意をはらわなければならない

D) 上記の全て

4. セキュリティ管理の主要な目的は何か？

A) 不正なソースから情報を保護するため

B) ユーザーに高いレベルのシステムの可用性を提供するため

C) 不慮の操作から情報を保護することを確実にするため

D) 上記の全て

5. ユーザーが、タスクを実行するための許可された最小レベルだけを与えられていることを何というか？

A) 限定された権限

B) 制限付きの特権

C) 責任の分離

D) 最小特権

6. 「完全性」とは何か？

A) データが元の適正な状態から、不適切に、あるいは不注意・不正のいずれかによる変更や破壊がなく、保管・処理され伝送されていることの保証

B) 必要な時に権限のあるユーザーがリソースに正常にアクセスできることの保証

C) データが非公開に保たれ、権限のある個人に制限されていることの保証

D) 上記のいずれでもない

7. セキュリティモニタリングの必要性とは何か？

A) 攻撃者がシステムにアクセスしたり変更したりする手順を示す活動を記録することができるから

B) ログファイルは、フォレンジック捜査でイベントのタイムラインを形成し、相関性を表すことができる

C) ログファイルは、セキュリティポリシーからの逸脱を示すことができる

D) 上記の全て

8. セキュリティテストに含まれない活動は、次のうちのどれか？

A) 稼動しているサービスをチェックするためにポートスキャンを実行する

B) 公に入手可能な情報を収集する

C) 敵対するものを特定するカウンター攻撃のシステム

D) 権限のない情報を得るための技術的なサポートのふりをする

9. システムに対するリスクを低減するものに含まれないものは次のうちのどれか？

A) 意識向上トレーニング

B) 論理的または技術的なコントロール

C) 管理者用コントロール

D) 物理的なコントロール

10. 最もコストがかかる一方、100%の可用性が担保される代替サイトはどれか？

A) Cold Site

B) Warm Site

C) Multiple Processing Sites

D) Mobile Site

11. バックアップ計画を策定するときに最も関連性の深い指標はどれか？

A) RTO(Recovery Time Objective)

B) RPO(Recovery Point Objective)

C) MTD(Maximum Tolerable Downtime)

D) BIA(Business Impact Analysis)

12. BCP および DRP のテスト手法では無いものは次のどれか？

A) チェックリストテスト

B) シミュレーションテスト

C) フルインタラプションテスト

D) 構造化インタラプションテスト

13. シーザー暗号を説明しているものは次のうちのどれか？

A) 別のメッセージに正しいメッセージを隠す

B) 換字暗号

C) 転字暗号

D) 多換字暗号

14. デジタル署名が提供するのは、次のうちのどれか？

A) 個人の機密データを暗号化する機能を提供する

B) 個人のプライバシーを確保する

C) ソースを識別し、データの完全性を検証する

D) 法律や手続きのためのフレームワークを提供する

15. 非対称鍵暗号の利点は、次のうちのどれか？

A) 鍵の配布が比較的容易であること

B) 両方の鍵が同じであること

C) ハードウェアに簡単に実装できること

D) 実行が非常に速いこと

16. アクセスポイントの基本的な役割は何か？

A) ワイヤレスで接続されたコンピュータやその他デバイスとの間にネットワークを構築するために、有線または無線のブリッジとして動作する

B) ネットワークのアクセスポイントでアクセス制御ポリシーを適用する

C) ランダムな WEP キーを生成する

D) ランダムな MAC アドレスを生成する

17. IPSec がしないものは、次のうちのどれか？

A) データの発信元の認証

B) コネクションレスの完全性

C) 無制限のトラフィックフローの機密性

D) リプレイ攻撃からの保護

18. モニタリングの対象となる可能性のあるローカルエリアネットワーク上のトラフィックのセキュリティ確保を支援することができるセキュリティ技術は、次のうちのどれか？

A) IPSec の実装

B) 伝送に暗号化を追加

C) バスの両端にアッテネータを提供し、データの盗難を防止する

D) すべてのコンピュータへのアクセスコントロールの追加

19. 「生産性と性能に対する攻撃」の例は、次のうちのどれか？

A) 機密データの不正操作

B) コンピュータのウイルス感染

C) 総当たり攻撃

D) サービス拒否(DoS)

20. ハッカーが DNS と ICMP のツール、またはポートスキャナやマッパーを使用するのは、次のうちの攻撃のどの段階か？

A) サービス拒否(DoS)

B) 窃取

C) アクセスと権限の昇格

D) 偵察

21. 「NetBus」や「BackOrifice」は、どんな悪意のあるコードの分類の例か？

A) ワーム

B) マルチパータイトウイルス

C) バックドアのトロイの木馬

D) アドウェア

SSCP 受験から認定までの流れと認定維持

SSCP 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、Perason 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

- SSCP CBK 7 ドメイン

問題数

- 125 問／4 択 Computer Based Testing(CBT)(日本語・英語併記)
  125 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。

時間

- 3 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。この説明を受けないで受験をすることはできません。
  - 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

- 250 米ドル

必須持ち物(忘れると受験不可)：

写真・署名付公的身分証明書と署名付身分証明書(計 2 点)

合格点

- 1000 点満点中 700 点で合格
  (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、7 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 1～7 の順位が記載されます。

SSCP 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. アクセス制御	16%
2. セキュリティの運用と管理	15%
3. リスクの特定、モニタリングと分析	15%
4. インシデントレスポンスとリカバリ	13%
5. 暗号	10%
6. ネットワークと通信のセキュリティ	16%
7. システムとアプリケーションセキュリティ	15%
	100%

SSCP 認定要件

SSCP 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。

- SSCP 認定試験での合格(1000 点中 700 点以上で合格)
- SSCP CBK7 ドメインのうち 1 ドメインに関連した 1 年以上の業務経験
- 実務経験が事実であることの証明及び倫理規約に合意すること
- (ISC)^2 認定資格保持者(CISSP, CAP, SSCP, CSSLP)からの推薦
- 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
- 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(試験登録時の申込書にて)

認定登録手続

- 推薦状(エンドースメント)と職務経歴書(英語)を米国(ISC)^2 本部に送付
  - 推薦状書式は合格通知の電子メールに記載の URL からダウンロードして記入します。(ISC)^2 認定資格保持者(CISSP, CAP, SSCP, CSSLP)からの推薦の署名をもらう必要があります。
  - 職務経歴書は、業務経験年数を明確に記載し、また経験年数に含む業務が SSCP CBK に関連した業務であることを明確に記載する必要があります。
- 手続き完了後、米国(ISC)^2 本部から認定証パッケージが希望した住所に郵送されます。
  - パッケージに入っているもの
    - 認定証
    - カード型の認定証
    - SSCP ラペルピン購入クーポン

SSCP 認定継続要件

- (ISC)^2 倫理規約に従い行動する
- 年会費の支払(125 米ドル／年・複数の資格を保有している場合でも同額)
- 継続教育単位(CPE クレジット)を 3 年間で 60 ポイント取得する

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 ホームページ	https://japan.isc2.org/
SSCP 認定試験案内	https://japan.isc2.org/sscp_examination.html
SSCP 7 ドメイン公式セミナー案内	https://japan.isc2.org/sscp_training.html

本書の取り扱いについて

SSCP 7ドメインガイドブック

2019年4月1日発行

お問い合わせ先

(ISC)²

E-mail: infoisc2-j@isc2.org

TEL: 03-5322-2837

URL: https://japan.isc2.org/