SSCP®

Systems Security Certified Practitioner

An (ISC)² Certification

認定試験の概要

発効日：2021年11月

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

SSCPとは

Systems Security Certified Practitioner（SSCP®）は、実証された技術スキル、そして運用ITの役割における実践的で実務的なセキュリティ知識を持つ方にとって理想的な認定資格です。データの機密性、完全性、可用性を確保するための情報セキュリティポリシーと手順に従って、ITインフラストラクチャを実装、監視、管理する能力の認定を行います。

SSCP Common Body of Knowledge（CBK®）に含まれる広範なトピックは、情報セキュリティ分野のあらゆる分野における関連性を保証します。合格した受験者は、以下の7つのドメインで優れた技能を有していることになります。

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

経験要件

受験者は、SSCP CBKの7つのドメインのうち1つ以上で合計1年以上の実務経験を有している必要があります。サイバーセキュリティプログラムで学位（学士または修士）を取得した受験者は、1年間の経験要件の免除が受けられます。

SSCPになるために必要な経験がない受験者は、SSCP試験に合格することで、(ISC)²の準会員になることができます。(ISC)²の準会員は、2年間で1年間の必要な経験を積むことができます。SSCPの経験要件、アルバイトやインターンシップを計上する方法については、www.isc2.org/Certifications/SSCP/experience-requirementsをご覧ください。

認定

SSCPは、ANSI/ISO/IEC規格17024の厳しい要件に準拠しています。

ジョブタスク分析（JTA）

(ISC)²は、SSCPの関連性を維持する義務があります。定期的に実施されるジョブタスク分析（JTA）は、SSCPによって定義された職務に従事するセキュリティ専門家が実行するタスクを決定するための方法論的かつ重要なプロセスです。JTAの結果をもとに、試験の更新を行います。このプロセスにより、受験者は、今日の実践的な情報セキュリティ専門家としての役割と責任に関連するトピック領域について試験されます。

SSCP試験情報

験時間、	3時間
問題数、	125
問題形式、	複数選択
合格点	1000点満点中700点
試験言語、	英語、日本語、ブラジルポルトガル語、
テストセンター	ピアソンVUEテストセンター

SSCP試験の配点

ドメイン	配点
1.セキュリティの運用と管理	16%
2.アクセス制御	15%
3.リスク特定、モニタリング、分析	15%
4.インシデントレスポンスとリカバリ	14%
5.暗号化	9%
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%
合計：	**100%**

ドメイン 1:
セキュリティの運用と管理

1.1 倫理規約の遵守

» (ISC)²倫理規約
» 組織の倫理規約

1.2 セキュリティの概念を理解する

» 機密性
» 完全性
» 可用性
» 説明責任
» プライバシー
» 否認防止
» 最小特権
» 職務の分離（SoD）

1.3 セキュリティ管理の特定と実施

» 技術的コントロール（例：セッションのタイムアウト、パスワードのエージング）
» 物理的コントロール（例：マントラップ、カメラ、ロック）
» 管理的コントロール（例：セキュリティポリシー、基準、手順、ベースライン）
» コンプライアンスの評価
» 定期的な監査とレビュー

1.4 機能的なセキュリティ管理の文書化と維持

» 抑止的コントロール
» 予防的コントロール
» 検出的コントロール
» 是正的コントロール
» 補償的コントロール

1.5 資産マネジメントのライフサイクル（ハードウェア、ソフトウェア、データ）への参加

» プロセス、計画、設計、開始
» 開発／取得
» インベントリとライセンス
» 実施／評価
» 運用／メンテナンス
» アーカイブと保存の要件
» 廃棄／破壊

1.6 変更管理ライフサイクルへの参加

» 変更管理（例：役割、責任、プロセス）
» セキュリティの影響分析
» 構成管理（CM）

1.7 セキュリティの認識とトレーニングの実装に参加する（例：ソーシャルエンジニアリング／フィッシング）

1.8 物理的なセキュリティの運用との連携（例：データセンターの評価、バッジ付け）

ドメイン 2: クセス制御

2.1 認証方法の実装と維持

» 単一／多要素認証（MFA）
» シングルサインオン（SSO）（例：Active Directoryフェデレーション サービス（ADFS）、OpenID Connect（オープンIDコネクト））
» デバイス認証
» フェデレーテッドアクセス（例：オープン認証2（OAuth2）、セキュリティ・アサーション・マークアップ言語（SAML））

2.2 インターネットワーク・トラスト・アーキテクチャの支援

» トラスト関係（例：1WAY、2WAY、過渡、ゼロ）
» インターネット、イントラネット、エクストラネット
» 第三者との接続

2.3 アイデンティティ管理のライフサイクルへの参加

» 認可
» 証明
» プロビジョニング／プロビジョニング解除
» メンテナンス
» 資格
» アイデンティティとアクセス管理（IAM）システム

2.4 アクセス制御の理解と適用

» 必須
» 裁量
» 役割ベース（例：属性ベース、主題ベース、対象ベース）
» ルールベース

ドメイン 3:
リスク特定、モニタリング、分析

3.1 リスクマネジメントプロセスの理解

» リスクの可視化と報告（例：リスク登録、脅威インテリジェンスの共有／妥協の指標（IOC）、一般的な脆弱性スコアリングシステム（CVSS））
» リスクマネジメントの概念（例：影響評価、脅威のモデル化）
» リスクマネジメントの枠組み（例：国際規格化機構（ISO）、国立規格技術研究所（NIST））
» リスク許容度（食欲など）
» リスク対応（例：受容、移転、緩和、回避、無視）

3.2 法的および規制上の考慮事項（例：管轄権、制限、プライバシー）の理解

3.3 セキュリティアセスメントや脆弱性管理活動への参加

» セキュリティテスト
» リスクレビュー（例：内部、サプライヤー、アーキテクチャ）
» 脆弱性管理のライフサイクル

3.4 セキュリティプラットフォームの運用と監視（例：継続的な監視）

» ソースシステム（例：アプリケーション、セキュリティアプライアンス、ネットワークデバイス、ホスト）
» 関心のあるイベント（例：異常、侵入、不正な変更、コンプライアンス監視）
» ログ管理
» イベントの集約と相関関係

3.5 モニタリング結果の分析

» セキュリティのベースラインと異常
» 可視化、メトリクス、トレンド（例：通知、ダッシュボード、タイムライン）
» イベントデータ分析
» 発見事項の文書化と伝達（例：エスカレーション）

ドメイン 4:
インシデントレスポンスとリカバリ

4.1 インシデントライフサイクルの支援（例：国立規格技術研究所（NIST）、国際規格化機構（ISO））

» 準備
» 検出、分析、エスカレーション
» 封じ込め
» 根絶
» リカバリ
» 教訓／新対策の実施

4.2 フォレンジック調査の理解と支援

» 法律（例：民事、刑事、行政）と倫理原則
» 証拠の取り扱い（例：初期対応、トリアージ、過程の管理、現場の保存）
» 分析の報告

4.3 事業継続計画（BCP）と災害復旧計画（DRP）活動の理解と支援

» 緊急時対応計画と手順（例：情報システムのコンティンジェンシー、パンデミック、自然災害、危機管理）
» 中間的または代替的な処理戦略
» 復旧計画
» バックアップと冗長化の実装
» テストと訓練

ドメイン 5: 暗号化

5.1 暗号化の理由と要件の理解

» 機密性
» 完全性と信頼性
» データセンシティビティ（例：個人情報（PII）、知的財産（IP）、保護された健康情報（PHI））
» 規制および業界のベストプラクティス（例：ペイメントカード業界データセキュリティ規格（PCI-DSS）、国際規格化機構（ISO））

5.2 暗号の概念の適用

» ハッシュ
» ソルト
» 対称／非対称暗号化／楕円曲線暗号化（ECC）
» 否認防止（例：電子署名／証明書、ハッシュベースのメッセージ認証コード（HMAC）、監査証跡）
» 暗号化アルゴリズムと鍵の強度（例：新暗 号化規格 （AES）、リベスト-シャミール-アデルマン（RSA）、256／512／1024／2048ビット鍵）
» 暗号攻撃、暗号解析、対策（例：量子コンピューティング）

5.3 セキュアプロトコルの理解と実装

» サービスとプロトコル（例：インターネットプロトコルセキュリティ（IPsec）、トランスポート層のセキュリティ（TLS）、セキュア／多目的インターネットメール拡張（S/MIME）、ドメインキーが識別したメール（DKIM）
» 一般的な使用例
» 制限と脆弱性

5.4 公開鍵基盤（PKI）システムの理解と支援

» » 基本的な鍵管理の概念（例：保存、回転、構成、生成、破壊、交換、失効、エスクロー）
» ウェブオブトラスト（WOT）（例：良好なプライバシー保護（PGP）、GNUプライバシーガード（GPG）、ブロックチェーン）

ドメイン 6:
ネットワークと通信のセキュリティ

6.1 ネットワークの基本的な概念の理解と適用

» オープンシステム間の相互接続（OSI）そして、伝送制御プロトコル/インターネットプロトコル（TCP / IP）モデル
» ネットワークトポロジー
» ネットワーク関係（例：ピアツーピア（P2P）、クライアントサーバ）
» 伝送メディアの種類（例：有線、無線など）
» ソフトウェア定義ネットワーキング（SDN）（例：ソフトウェア定義の広域ネットワーク（SD-WAN）、ネットワーク仮想化、自動化）
» 一般的に使用されるポートとプロトコル

6.2 ネットワーク攻撃（例：分散型サービス拒否（DDoS）、man-in-the-middle（MITM）、ドメインネームシステム（DNS）ポイズニング）とその対策（例：コンテンツ配信ネットワーク（CDN））

6.3 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制御、標準およびプロトコル（例：IEEE 802.1X、リモート認証ダイヤルインユーザーサービス（RADIUS）、ターミナルアクセスコントローラアクセス制御システムプラス（TACACS+））
» リモートアクセスの操作と設定（例：シンクライアント、仮想プライベートネットワーク（VPN））

6.4 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論理的および物理的配置（例：インライン、パッシブ、バーチャル）
» セグメンテーション（例：物理／論理、データ／コントロールプレーン、仮想ローカルエリアネットワーク（VLAN）、アクセス制御リスト（ACL）、ファイアウォールゾーン、マイクロセグメンテーション）
» 安全なデバイス管理

6.5 ネットワークベースのセキュリティデバイスの操作と設定

» ファイアウォールとプロキシ（例：フィルタリング方法、ウェブアプリケーションファイアウォール（WAF））
» 侵入検知システム（IDS）侵入防止システム（IPS）
» ルーターとスイッチ
» トラフィックシェーピングデバイス（例：広域ネットワーク（WAN）の最適化、負荷分散）

6.6 安全な無線通信

» 技術（例：セルラーネットワーク、Wi-Fi、Bluetooth、近距離通信（NFC）
» 認証および暗号化プロトコル（例：有線相当のプライバシー（WEP）、Wi-Fi保護アクセス（WPA）、拡張認証プロトコル（EAP））
» モノのインターネット（IoT）

ドメイン 7: システムとアプリケーションセキュリティ

7.1 悪意のあるコードと活動の特定と分析

» マルウェア（ルートキット、スパイウェア、スケアウェア、ランサムウェア、トロイの木馬、ウイルス、ワーム、トラップドア、バックドア、ファイルレス）
» マルウェア対策（例：スキャナ、マルウェア対策、コード署名）
» 悪意のあるアクティビティ（内部脅威、データ盗難、分散型サービス拒否（DDoS）、ボットネット、ゼロデイエクスプロイト、Webベースの攻撃、高度な持続的脅威（APT））
» 悪意のある活動に対する対策（例：ユーザーの認識、システムの強化、パッチ適用、検疫、データ損失防止（DLP））
» ソーシャルエンジニアリング（フィッシング、なりすましなど）
» 行動分析（例：機械学習、人工知能（AI）、データ分析）

7.2 エンドポイントデバイスのセキュリティの実装と運用

» ホストベース侵入防止システム（HIPS）
» ホストベースのファイアウォール
» アプリケーションホワイトリスト
» エンドポイント暗号化（例：ディスク全体の暗号化）
» トラステッドプラットフォームモジュール（TPM）
» 安全なブラウジング
» エンドポイント検出と対応（EDR）

7.3 モバイルデバイス管理（MDM）の管理

» プロビジョニング技術（例：企業所有、個人利用可（COPE）、自分のデバイスを持参（BYOD））
» コンテナ
» 暗号化
» モバイルアプリケーション管理（MAM）

7.4 クラウドセキュリティの理解と設定

» 配置モデル（例：パブリック、プライベート、ハイブリッド、コミュニティ）
» サービスモデル（例：サービスとしてのインフラストラクチャ（IaaS）、サービスとしてのプラットフォーム（PaaS）、
» サービスとしてのソフトウェア（SaaS））
» 仮想化（例：ハイパーバイザー）
» 法的および規制上の考慮事項（例：プライバシー、監視、データ所有権、管轄権、eDiscovery）
» データの保存、処理、伝送（例：アーカイブ、リカバリ、レジリエンス）
» 第三者／アウトソーシングの要件（例：サービスレベル契約（SLA）、データポータビリティ、データ破棄、監査）
» 共有責任モデル

7.5 安全な仮想環境の運用と維持

» ハイパーバイザー
» 仮想アプライアンス
» コンテナ
» 継続性とレジリエンス
» 攻撃と対策
» 共有ストレージ

追加の試験情報

参考文献の補足

受験者は、CBKに関連する関連資料を確認し、さらに注意を払う必要がありそうな研究分野を特定することで、知識を身に着けて経験を補うことが奨励されます。

補足文献の全リストは www.isc2.org/certifications/References でご覧いただけます。

試験の方針と手続き

(ISC)²は、SSCP受験者が受験申請を行う前に、試験の方針や手順を確認することを推奨していますこの重要な情報に関する包括的な内容は、www.isc2.org/Register-for-Exam でご覧い

法務情報

(ISC)²の法的方針に関するご質問は、(ISC)2法務部 (legal@isc2.org) までお問い合わせくださ

質問はございませんか?

(ISC)² Americas
電話:+1.866.331.ISC2(4722)
Eメール : info@isc2.org

(ISC)² Asia Pacific
電話:+(852)28506951
Eメール : isc2asia@isc2.org

(ISC)² EMEA
電話:+44(0)203 300 1625
Eメール : info-emea@isc2.org