SSCP®

Systems Security Certified Practitioner

ISC2 Certification

認定試験要綱

発効日: 2024年9月

ISC2™

SSCPについて

Systems Security Certified Practitioner (SSCP®) は、実証済みの技術スキルと運用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有する人材にとって最適な資格認定です。データの機密性、完全性、可用性を確保する情報セキュリティ・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、管理する実務者の能力を確認します。

SSCPの知識体系に含まれる広範なトピックは、情報セキュリティ分野のすべての部門にわたる関連性を確保します。合格者には、次のドメインでの能力が求められます。

- セキュリティの概念と実践
- アクセス制御
- リスクの特定、モニタリング、分析
- インシデントへの対応と復旧
- 暗号
- 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のセキュリティ

実務経験要件

必要な実務経験:受験者は、現在のSSCP要綱の1つ以上のドメインにおける1年以上のフルタイムの実務経験が必要です。コンピューターサイエンス、情報技術 (IT)、または関連分野で中等教育後の学位 (学士号または修士号) を取得すると、必要な実務経験の最長1年を満たすことができます。パートタイムの業務やインターンシップも実務経験要件に含まれる場合があります。

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)

ISC2 は会員に対して、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 (JTA)」 は、SSCPで定義された専門分野に従事するセキュリティプロフェッショナルが実行するタスクを決定する、体系的かつ重要なプロセスです。JTAの結果は審査の更新に用いられます。このプロセスにより、受験者は、今日の実務を担う情報セキュリティプロフェッショナルの役割と責任に関連するトピック分野の試験を確実に受けることができます。

SSCP試験情報

試験時間	3時間
問題数	125問
出題形式	四者択一
合格点	1000点中700点
受験可能言語	英語、日本語、スペイン語テストセンターピアソンVUEテストセンター

SSCP試験の重み付け

ドメイン	重み付け
1.セキュリティの概念と実践	16%
2.アクセス制御	15%
3.リスクの特定、モニタリング、分析	15%
4.インシデントへの対応と復旧	14%
5.暗号	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のセキュリティ	15%
合計:	**100%**

ドメイン1:
セキュリティの概念と実践

1.1 倫理規約の遵守

» ISC2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
» 否認防止
» 最小権限
» 職務分掌 (SoD)

1.3 セキュリティ・コントロールの特定と実施

» 技術的管理(例:ファイアウォール、侵入検知システム (IDS)、アクセス制御リスト (ACL))
» 物理的コントロール(例：マントラップ、カメラ、ロック)
» 管理コントロール(例：セキュリティポリシー、標準、手順、ベースライン)
» コンプライアンス要件の評価
» 定期的な監査とレビュー

1.4 機能的なセキュリティ・コントロールの文書化と維持

» 抑止制御
» 予防的コントロール
» 検出コントロール
» 是正的コントロール
» 補正コントロール

1.5 資産管理ライフサイクル(つまりハードウェア、ソフトウェア、データ)のサポートと実装

» プロセス、計画、設計、開始
» 開発・取得(例:DevSecOps、テスト)
» インベントリとライセンス(例:オープンソース、クローズドソース)
» 実装/評価
» 運用/保守/エンド・オブ・ライフ（EOL)
» アーカイブと保存の要件
» 処分と破壊

1.6 変更管理ライフサイクルのサポートおよび/または実装

» 変更管理(例えば、役割、責任、プロセス、コミュニケーション、監査)
» セキュリティ影響分析
» 構成管理 (CM)

1.7 セキュリティ意識とトレーニング(例:ソーシャルエンジニアリング/フィッシング/机上演習/認識コミュニケーション)のサポートおよび/または実装

1.8 物理的なセキュリティ・オペレーション(例:データセンター/施設の評価、バッジと訪問者の管理、パーソナルデバイスの制限)との連携

ドメイン2:
アクセス制御

2.1 認証方式の実装および維持

» 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)
» デバイス認証（例：証明書、メディア・アクセス・コントロール（MAC）アドレス、トラステッド・プラットフォーム・モジュール（TPM））
» フェデレーションアクセス(例:Open Authorization 2 (OAuth2)、Security Assertion Markup Language (SAML))

2.2 インターネットワーク信頼アーキテクチャの理解とサポート

» 信頼関係(例:1方向、双方向、推移的、ゼロトラスト)
» インターネット、イントラネット、エクストラネット、および非武装地帯 (DMZ)
» サードパーティとの接続(例：アプリケーションプログラミングインターフェイス (API)、アプリ拡張機能、ミドルウェア)

2.3 アイデンティティ管理ライフサイクルのサポートおよび/または実装

» 認可
» 立証
» プロビジョニング/プロビジョニング解除
» 監視、レポート作成、維持(例：役割の変更、新しいセキュリティ標準)
» エンタイトルメント(例：継承された権利、資源)
» IDおよびアクセス管理 (IAM) システム

2.4 アクセス制御の理解と管理

» 必須
» 随意
» 役割ベース(例：サブジェクト・ベース、オブジェクト・ベース、特権アクセス管理 (PAM))
» ルールベース
» 属性ベース

ドメイン3:
リスクの特定、モニタリングおよび分析

3.1 リスク管理を理解する

» 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、侵害指標 (IOC)、共通脆弱性評価システム (CVSS)、社会化、MITRE/ATT&CKモデル)
» リスクマネジメントの考え方(例：影響評価、脅威のモデル化、適用範囲)
» リスク管理の枠組み(例:国際標準化機構 (ISO)、米国商務省標準技術局 (NIST))
» リスク許容度（例：リスク選好、リスクの定量化)
» リスク対応(例：受け入れる、移転させる、軽減する、回避する、無視する)

3.2 法的および規制上の懸念事項の理解(例：管轄権、制限、プライバシー)

3.3 セキュリティ評価および脆弱性管理アクティビティの実行

» リスク管理体制の整備
» セキュリティテスト
» リスクレビュー(例:社内、サプライヤ、アーキテクチャ)
» 脆弱性管理ライフサイクル(例:スキャン、レポート、分析、修復)

3.4 セキュリティプラットフォームの運用・監視(例:継続的モニタリング)

» 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:エラー、欠落、異常、不正変更、コンプライアンス違反、ポリシー失敗)
» ログ管理(例:ポリシー、完全性、保存、アーキテクチャ、構成、集約、チューニング)
» セキュリティ情報およびイベント管理 (SIEM) (例：リアルタイムの監視、分析、追跡、監査)

3.5 監視結果の解析

» セキュリティベースラインと異常(例：相関、ノイズ低減)
» 視覚化、測定基準、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
» 知見の文書化と伝達(例：エスカレーション)

ドメイン4:
インシデントへの対応と復旧

4.1 インシデント対応ライフサイクルの理解とサポート(例:米国商務省国立標準技術研究所(NIST)、国際標準化機構 (ISO))

» 準備(例：役割の定義、研修プログラム)
» 検出、分析、エスカレーション(例:インシデントコミュニケーション、広報)
» 封じ込め
» 根絶
» 復元(例：:インシデントの文書化)
» インシデント後の活動(例：得られた教訓、新たな対策、継続的改善)

4.2 フォレンジック調査の理解とサポート

» 法的(例：民事、刑事、行政)および倫理的原則
» 証拠の取り扱い(例：第一応答者、トリアージ、証拠の管理連鎖、現場の保全))
» 分析のレポート
» 組織のセキュリティポリシーコンプライアンス

4.3 ビジネス継続性計画 (BCP) および災害復旧計画 (DRP) 活動の理解とサポート

» 緊急時対応計画及び手順(例：情報システムの不測の事態、パンデミック、自然災害、危機管理)
» 中間処理又は代替処理戦略
» 復旧計画(例:目標復旧時間 (RTO)、目標復旧時点 (RPO)、最大許容ダウンタイム (MTD))
» バックアップと冗長性の実装
» テストと訓練(例：プレイブック、テーブルトップ、災害復旧演習、スケジュール設定)

ドメイン5: 暗号

5.1 暗号の理由と要件の理解

» 機密性
» 完全性と信頼性
» データセンシティブ(例:個人を特定できる情報 (PII)、知的財産 (IP)、保護された医療情報 (PHI))
» 規制および業界のベスト・プラクティス(例:PCI-DSS (Payment Card Industry Data Security Standards)、国際標準化機構 (ISO))
» 暗号エントロピー(例；量子暗号、量子鍵配送)

5.2 暗号の概念の適用

» ハッシング
» 塩漬け
» 対称/非対称暗号化/楕円曲線暗号 (ECC)
» 否認防止(例：デジタル署名/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暗号鍵の強化 (例：高度暗号化標準(AES)、リベスト・シャミア・アドルマン (RSA))
» 暗号攻撃と暗号解読

5.3 セキュアな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・レイヤー・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）、ドメインキー識別メール（DKIM）)
» 一般的なユースケース(例:クレジット・カード処理、ファイル転送、Webクライアント、仮想プライベート・ネットワーク (VPN)、PIIデータの伝送)
» 制限事項と脆弱性

5.4 公開鍵インフラストラクチャ (PKI) システムの理解とサポート

» 鍵管理の基本概念(例：保管、ローテーション、組成、生成、破棄、交換、失効、エスクロー)
» Web of Trust (WOT) (例:Pretty Good Privacy (PGP)、GNU Privacy Guard (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 ネットワーキングの基本概念の理解と適用

» 開放型システム間相互接続 (OSI) および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

» 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)

» 伝送メディアタイプ(例:有線、無線)

» ソフトウェア定義ネットワーキング (SDN) (例:Software-Defined Wide Area Network 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 ネットワーク攻撃の理解(例:分散型サービス妨害 (DDoS)、中間者攻撃 (MITM)、ドメインネームシステム (DNS) キャッシュポイズニング)

» 対策(例:コンテンツ配信ネットワーク (CDN)、ファイアウォール、ネットワークアクセス制御、侵入検出および防止システム (IDPS))

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、プロトコル(例:Institute of Electrical and Electronics Engineers (IEEE) 802.1X、Remote Authentication Dial-In User Service (RADIUS)、Terminal Access Controller Access-Control System Plus (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)、仮想デスクトップインフラストラクチャ)

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な配置(例:インライン、パッシブ、仮想)

» 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・アプライアンスおよびサービスの操作と構成

» 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)、クラウドアクセスセキュリティブローカ (CASB))

» 侵入検知システム (IDS) および侵入防止システム (IPS)

» ルータおよびスイッチ

» トラフィックシェーピングデバイス(例:ワイドエリアネットワーク (WAN) の最適化、負荷バランシング)

» ネットワークアクセス制御 (NAC)

» 情報漏洩対策 (DLP)

» 統合脅威管理 (UTM)

6.6 安全なワイヤレス通信

» テクノロジー(例:携帯電話ネットワーク、Wi-Fi、Bluetooth、近距離無線通信 (NFC))

» 認証および暗号化プロトコル(例:Wi-Fi Protected Access (WPA)、Extensible Authentication Protocol (EAP)、Wi-Fi Protected Access 2 (WPA2)、Wi-Fi Protected Access 3 (WPA3))

6.7 モノのインターネット (IoT) のセキュリティ保護と監視 (例:構成、ネットワーク分離、ファームウェア更新、エンド・オブ・ライフ (EOL) 管理)

ドメイン7: システムとアプリケーションのセキュリティ

7.1 悪意のあるコードとアクティビティの特定と分析

- 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、アプリ/コード/オペレーティング システム (OS)/モバイル コードの脆弱性など)
- マルウェア対策 (例: スキャナー、マルウェア対策、封じ込めと修復、ソフトウェア セキュリティ)
- 悪意のあるアクティビティの種類 (例: 内部関係者の脅威、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、高度な永続的脅威 (APT))
- 悪意のあるアクティビティの対策 (例: ユーザーの意識向上/トレーニング、システムの強化、パッチ適用、隔離、データ損失防止 (DLP)
- ソーシャル エンジニアリング手法 (例: スパム電子メール、フィッシング/スミッシング/ビッシング、なりすまし、希少性、捕鯨)
- 行動分析 (機械学習、人工知能 (AI)、データ分析など)

7.2 エンドポイントデバイスセキュリティの実装と運用

- ホストベースの侵入防止システム (HIPS)
- ホストベースの侵入検知システム (HIDS)
- 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登録
- エンドポイントの暗号化(フルディスク暗号化など)
- トラステッドプラットフォームモジュール (TPM) (例: ハードウェアセキュリティモジュール管理)
- 安全なブラウジング(デジタル証明書など)
- エンドポイントの検出と応答 (EDR)

7.3 エンドポイントの検出と応答 (EDR)

- プロビジョニングの手法(例:企業所有、個人所有 (COPE)、個人所有デバイスの持ち込み (BYOD)、モバイルデバイス管理 (MDM))
- コンテナ化
- 暗号化
- モバイルアプリケーション管理

7.4 クラウドセキュリティの理解と構成

- デプロイメントモデル(パブリック、プライベート、ハイブリッド、コミュニティなど)
- サービスモデル(例:Infrastructure as a Service (IaaS)、Platform as a Service (PaaS)、Software as a Service (SaaS))
- 仮想化(例:ハイパーバイザ、Virtual Private Cloud (VPC))
- 法的および規制上の懸念(例:プライバシー、監視、データの所有権、管轄権、電子情報開示、シャドウ情報テクノロジー (IT))
- サードパーティ/アウトソーシングの要件(例:サービスレベルアグリーメント (SLA)、データポータビリティ/プライバシー/破壊/監査)
- 責任分担モデル
- データの保存、処理、および送信(アーカイブ、バックアップ、リカバリ、回復性など)

7.5 セキュアな仮想環境の運用と保守

- ハイパーバイザ(タイプ1 (例: ベアメタル)、タイプ2 (ソフトウェアなど))
- 仮想アプライアンス
- コンテナ
- 継続性と回復力
- ストレージ管理(例: データドメイン)
- 脅威・攻撃・対策(例:ブルートフォース攻撃、仮想マシンエスケープ、脅威ハンティング)

追加の試験情報

補足資料

受験者は、さらに注意を払う必要があると思われる研究分野を特定するために、知識体系に関連する関連資料に目を通し、自らの教育と経験を補うことが奨励されます。

補足資料の完全なリストについては、www.ISC2.org/certifications/Referencesを参照してください。

審査の方針及び手続

ISC2では、受験者が試験に登録する前に、試験のポリシーと手順を確認することを推奨しています。この重要な情報の詳細については、www.ISC2.org/Register-for-Examを参照してください。

法的情報

ISC2の法的ポリシー に関するご質問については、ISC2法務部legal@isc2.orgまでお問い合わせください。

質問はございますか?

お住まいの地域のISC2候補サービスにお問い合わせください。

南北アメリカ

電話:+1.866.331。ISC2 (4722)、1を押してください。
電子メール: membersupport@isc2.org

アジア太平洋

電話:+852-5803-5662
電子メール: isc2asia@isc2.org

欧州、中東、アフリカ

電話:+44 (0) 203-960-7800
電子メール: info-emea@isc2.org