SSCP®

システムセキュリティ認定実務者

ISC2 Certification

認定試験要綱

施行日：2025年10月1日

ISC2™

SSCPについて

The Systems Security Certified Practitioner（SSCP）は、IT運用の役割において実証済みの技術スキルと実践的なセキュリティ知識を持つ人にとって理想的な認定資格です。この資格を取得することで、実務者に対するデータ、機密性、整合性、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インフラを実装、監視、管理する適性が認められます。

SSCP の知識体系には幅広いトピックが含まれているため、情報セキュリティ領域におけるあらゆる分野にわたる関連性を保証します。試験に合格した受験者は、次の7つのドメインに関して十分な適性を有しています：

- セキュリティの概念と実践
- アクセス制御
- リスクの識別、監視、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

求められる経験

認定を受ける受験者は、現行SSCP認定試験の概要の7つのドメインのうち1つ以上で合計1年以上のフルタイムの実務経験が必要です。コンピュータサイエンス、情報テクノロジー（IT）または関連分野での学士または修士の学位を取得することで、必要な経験年数のうち、最大一年間までを満たすことができます。パートタイム勤務およびインターンシップ期間も経験要件に計上できる場合があります。

認定

SSCPはANSI米国適合性認定機関（ANAB）ISO/IEC規格17024の厳しい要件に準拠しています。

作業タスク分析（JTA）

ISC2は、その会員に対してSSCPの妥当性を維持する義務を負っています。定期的に実施される、ジョブタスク分析（JTA）は、SSCPが定めたプロフェッショナルな業務に従事するセキュリティ専門家によって職務が実行されていることを判断する体系的でかつ極めて重要なプロセスです。JTAの結果は試験の改善に活用されます。このプロセスは、情報セキュリティ専門家の今日の実務における役割と責任に関連する項目や領域に関して、受験者が確実に審査されるようにします。

SSCP CAT試験情報

SSCP試験では、英語、日本語、現代スペイン語の試験において、コンピュータ適応型テスト（CAT）を使用しています。SSCP CATについては、www.isc2.org/certifications/computerized-adaptive-testing で詳細をご覧ください。

試験時間	2時間
出題数	100 - 125
出題形式	選択式問題と発展的問題
合格ライン	1000点満点中700点
試験で使用される言語	英語、日本語、スペイン語
受験会場	ピアソンVUEテストセンター

SSCP CAT試験の比重

ドメイン	比重の平均
1. セキュリティの概念と実践	16%
2. アクセス制御	15%
3. リスクの識別、監視、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：
セキュリティの概念と実践

1.1 倫理規定への準拠

» ISC2の倫理規定
» 組織倫理規定

1.2 セキュリティコンセプトの理解

» 機密保持
» 整合性
» 可用性
» 説明責任
» 否認防止
» 最小特権
» 業務の分掌（SoD）

1.3 セキュリティコントロールの特定と実装

» 技術的管理（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）など）
» 物理的コントロール（例：マントラップ、カメラ、ロック）
» 行政的コントロール（例：セキュリティポリシー、規格、手続き、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
» 予防制御
» 発見制御
» 修正制御
» 補償制御

1.5 資産管理ライフサイクル（ハードウェア、ソフトウェア、データなど）をサポートして実施

» プロセス、計画、設計、開始
» 開発／獲得（DevSecOps、試験など）
» インベントリーとライセンス（オープンソース、クローズドソースなど）
» 実施および評価
» オペレーション／メンテナンス／エンド・オブ・ライフ（EOL）
» アーカイブと保持要件
» 廃棄と破棄

1.6 変更管理ライフサイクルのサポートおよび／または実施

» 変更管理（例：役割、責任、プロセス）
» セキュリティインパクト分析
» 構成管理（CM）

1.7 セキュリティ意識向上およびトレーニング（ソーシャルエンジニアリング／フィッシング／卓上演習／意識向上コミュニケーションなど）をサポートおよび／または実施

1.8 物理的セキュリティ運用（データセンター／施設の評価、バッジングと訪問者管理、個人デ バイスの制限など）と連携

ドメイン2：アクセス制御

2.1 認証方法の実装と維持

» 単要素/多要素認証（MFA）
» シングルサインオン（SSO）（例：アクティブディレクトリフェデレーションサービス（ADFS）、OpenIDコネクト）
» デバイス認証（証明書、メディアアクセス制御（MAC）アドレス、信頼性の高いプラットフォームモジュール（TPM）など）
» フェデレーションアクセス（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を理解してサポート

» トラスト関係（例：1方向、2方向、推移、ゼロ）
» インターネット、イントラネット、エクストラネット、非武装地帯（DMZ）
» サードパーティ接続（アプリケーションプログラミングインターフェース（API）、アプリの拡張機能、ミドルウェアなど）

2.3 識別管理ライフサイクルのサポートおよび／または実施

» 認証
» 実証
» プロビジョニング/デプロビジョニング
» モニタリング、レポーティング、メンテナンス（役割の変更、新しいセキュリティ基準など）
» 権利（継承された権利、資源など）
» 識別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
» 裁量
» 役割ベース（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）など）
» ルールベース
» 属性ベース

ドメイン3：
リスクの識別、監視、分析

3.1 リスク管理の理解

» リスクの可視化とレポート（リスク登録、脅威インテリジェンスの共有、侵害指標（IOC）、一般的な脆弱性スコアリングシステム（CVSS）、社会化、MITRE/ATT&CKモデルなど）
» リスク管理コンセプト（例：インパクト評価、脅威モデリング）
» リスク管理の枠組み（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（アペタイト、リスク定量化など）
» リスク処理（例：受入、転送、軽減、回避、無視）

3.2 法的および規制上の懸念事項（例：管轄区域、制限、プライバシー）の理解

3.3 セキュリティ評価と脆弱性管理活動の実施

» リスク管理フレームワークの実施
» 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（スキャン、レポート、分析、修復など）

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）
» 関心のある事象（エラー、脱落、異常、不正変更、コンプライアンス違反、ポリシー違反など）
» ログ管理（ポリシー、整合性、保存、アーキテクチャ、構成、集約、チューニングなど）
» セキュリティ情報および事象管理（SIEM）（リアルタイム監視、分析、追跡、監査など）

3.5 監視結果の分析

» セキュリティベースラインと異常（相関、ノイズ除去など）
» 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
» 調査結果の文書化と伝達（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復旧

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

» 準備（役割の定義、トレーニングプログラムなど）
» 検知、分析、エスカレーション（インシデントコミュニケーション、広報など）
» 封じ込み
» 根絶
» 復旧（インシデントの文書化など）
» インシデント後の活動（教訓、新たな対策、継続的改善など）

4.2 フォレンジック調査の理解とサポート

» 法的原則（例：民事、刑事、行政）および倫理原則
» 証拠の取り扱い（例：初期対応者、トリアージ、保管過程、現場の保存）
» 分析結果の報告
» 組織のセキュリティポリシー遵守

4.3 事業継続計画（BCP）および災害復旧計画（DRP）活動への理解とサポート

» 緊急対応計画と手順（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）
» 暫定または代替の処理戦略
» 復旧計画（復旧時間目標（RTO）、復旧ポイント目標（RPO）、最大許容ダウンタイム（MTD）など）
» バックアップと冗長性の実装
» テストと訓練（プレイブック、テーブルトップ、災害復旧訓練、スケジュール管理など）

ドメイン5：
暗号化

5.1 暗号化の理由と要件への理解

» 機密保持
» 誠実さと信頼性
» データの機密性（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））
» 暗号エントロピー（量子暗号、量子鍵配布など）

5.2 暗号化の概念の適用

» ハッシュ化
» ソルト化
» 対称/非対称暗号/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キーの強度（例：新暗号化規格（AES）、リベスト-シャミア-エーデルマン（RSA）など）
» 暗号攻撃と暗号解読

5.3 安全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）、転送層セキュリティ（TLS）、セキュア/多目的インターネットメール拡張（S/MIME）、DomainKey識別メール（DKIM））
» 一般的な使用例（クレジットカード処理、ファイル転送、ウェブクライアント、仮想プライベートネットワーク（VPN）、PIIデータの送信など）
» 制限と脆弱性

5.4 公開キー基盤（PKI）システムの理解とサポート

» 基本的なキー管理の概念（例：ストレージ、ローテーション、構成、生成、破棄、交換、失効、エスクロー）
» Web of Trust（WOT）（良好なプライバシー保護（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

» オープンシステム間相互接続（OSI）および転送制御プロトコル/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（ピア・ツー・ピア（P2P）、クライアントサーバーなど）
» 伝送メディアの種類（例：有線、無線）
» 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）、中間者攻撃（MITM）、ドメインネームシステム（DNS）ポイズニングなど）の理解

» 対策（コンテンツ復旧ネットワーク（CDN）、ファイアウォール、ネットワークアクセス制御、侵入検知・防止システム（IDPS）など）

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：電気電子学会（IEEE）802.1X、リモート認証ダイヤルインユーザーサービス（RADIUS）、Terminal Access Controller Access-Control System Plus（TACACS+））
» リモートアクセスの操作と構成（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、仮想）
» セグメンテーション（例：物理的/論理的、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設定

» ファイアウォールとプロキシ（フィルタリング方法、Web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ー（CASB）など）
» 侵入検知システム（IDS）と侵入防止システム（IPS）
» ルーターとスイッチ
» トラフィック シェイピング デバイス（広域ネットワーク（WAN）の最適化、負荷分散など）
» ネットワークアクセス制御（NAC）
» データ損失防止（DLP）
» 統合脅威管理（UTM）

6.6 安全な無線通信

» テクノロジー（例：携帯電話ネットワーク、Wi-Fi、ブルートゥース、近距離無線通信（NFC））
» 認証および暗号化プロトコル（Wi-Fi Protected Access（WPA）、Extensible Authentication Protocol（EAP）、Wi-Fi Protected Access 2（WPA2）、Wi-Fi Protected Access 3（WPA3）など）

6.7 モノのインターネット（IoT）の安全確保と監視（構成、ネットワーク分離、ファームウェア 更新、終息（EOL）管理など）

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（スキャナ、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など）
- 悪意のあるアクティビティの種類（例：内部関係者による脅威、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、持続的標的型攻撃（APT））
- 悪意のあるアクティビティの対策（例：ユーザーの認識、システムの強化、パッチの適用、隔離、データ損失防止（DLP））
- ソーシャルエンジニアリングの手法（SPAM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、ホエーリングなど）
- 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）
- ホストベース侵入検出システム（HIDS）
- ホストベースのファイアウォール
- アプリケーションのホワイトリスト化
- エンドポイント暗号化（例：ディスク全体の暗号化）
- 信頼性の高いプラットフォームモジュール（TPM）（ハードウェアセキュリティモジュール管理など）
- 安全な閲覧（電子証明書など）
- エンドポイント検出と対応（EDR）

7.3 エンドポイント検出と対応（EDR）

- プロビジョニング技術（企業所有、個人使用可能（COPE）、BYOD（Bring Your Own Device）、モバイルデバイス管理（MDM）など）
- 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

- 展開モデル（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（ハイパーバイザー、仮想プライベートクラウド（VPC）など）
- 法的および規制上の懸念事項（プライバシー、監視、データ所有権、管轄権、eDiscovery、シャドー情報技術（IT）など）
- サードパーティ／アウトソーシング要件（サービスレベル契約（SLA）、データポータビリティ／プライバシー／破壊／監査など）
- 共有責任モデル
- データのストレージ、処理、送信（例：アーカイブ、リカバリ、回復力）

7.5 安全な仮想環境の運用と維持

- ハイパーバイザー（タイプ1（ベアメタルなど）、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（データドメインなど）
- 脅威、攻撃、対策（ブルートフォース攻撃、仮想マシンエスケープ、脅威ハンティングなど）

追加の試験情報

補足参考資料

受験者は、SSCP試験要綱に関連する関連資料に目を通し、さらに注意が必要と思われる学習分野を特定することで、自らの教育と経験を補うことが推奨されます。

補足参考資料の全リストについては、www.ISC2.org/certifications/References をご覧ください。

試験のポリシーと手続き

ISC2では認定を受ける受験者に対して、試験に登録する前に試験の方針や手続きを確認することを推奨しています。この情報については、www.ISC2.org/Register-for-Exam をご覧ください。

法的情報

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

質問などのお問い合わせ

お近くのISC2 Candidate Servicesにお問い合わせください：

アメリカ大陸
電話：+1.866.331.ISC2 (4722)、「1」を押してください
メール：membersupport@isc2.org

アジア太平洋
電話：+852-5803-5662
メール：isc2asia@isc2.org

ヨーロッパ、中東、アフリカ
電話：+44 203-960-7800
メール：info-emea@isc2.org