SSCP®

Systems Security Certified Practitioner

認定試験の概要

発効日：2018年11月

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

SSCPについて

システムセキュリティ認定従事者（SSCP）はIT担当の業務において実証された技能、そして実践的かつ実地的なセキュリティ知識を有する方々にとって理想的な認定です。これはデータの機密性、完全性及び可用性を確実にするための情報セキュリティポリシー及び手順に沿ったITインフラストラクチャの利用、監視及び管理における従事者の能力を確認するものです。

SSCPの共通知識体系（CBK）に含まれる広範な知識項目は情報セキュリティの現場における全ての分野に関係するものです。認定要件を満たす受験者は以下の7ドメインにおいて十分な能力を有します。

- アクセス制御
- セキュリティ運用及び管理
- リスクの特定、監視及び分析
- インシデント対応及び復旧
- 暗号
- ネットワーク及び通信セキュリティ
- システム及びアプリケーションセキュリティ

経験要求

受験者は、7つのSSCP CBKドメインにおいて少なくとも1つかそれ以上における最低で累積1年間の実務経験を有すること。サイバーセキュリティプログラムにおける学位（学士号あるいは修士号）を取得した受験者は1年分の実務経験相当の必修要件を満足していると認められます。

所要の経験を有しない受験者がSSCPに認定されるため、SSCP試験を合格することで(ISC)²準会員になることもできます。(ISC)²準会員には、1年分の所要の経験を積むための期間として2年間が与えられます。

認定

SSCPはANSI/ISO/IEC規格17024の厳格な要求に則っています。

業務タスク分析（JTA）

(ISC)²は会員がSSCPとの関連性を維持することに義務を負います。業務タスク分析(JTA)は、SSCPが定義する職種に従事するセキュリティ専門家により定期的に実施されるもので、タスクを確認する体系的かつ極めて重要な手順です。JTAの結果は認定試験の更新に使用されます。この手順は、受験者が今日の情報セキュリティ専門家が有する役割と責任に関連した分野の項目で試験されることを確実にします。

SSCP試験概要

試験時間	3 時間
出題数	125問
問題形式	選択式
合格基準	1000点中700点以上
試験言語	英語、日本語、またはブラジルポルトガル語
試験会場	ピアソンVUE試験センター

SSCP試験問題配分

ドメイン	配分
1. アクセス制御	16%
2. セキュリティ運用及び管理	15%
3. リスクの特定、監視及び管理	15%
4. インシデント対応及び復旧	13%
5. 暗号	10%
6. ネットワーク及び通信セキュリティ	16%
7. システム及びアプリケーションセキュリティ	15%
合計	**100%**

ドメイン 1:
アクセス管理

1.1 認証方式の実装と維持

» 単一／複数要素による認証
» シングルサインオン
» デバイス認証
» 連携されたアクセス

1.2 内部ネットワーク信頼構造の支援

» 信頼関係（例：一方向、双方向、推移型）
» エクストラネット
» 第三者接続

1.3 Participate in the identity management lifecycle

» 認可
» プルーフィング
» プロビジョニング／非プロビジョニング
» 保守
» 資格付与
» アイデンティティ及びアクセス管理（IAM）システム

1.4 アイデンティティ管理ライフサイクルへの参画

» 強制
» 非任意
» 任意
» ロールベース
» 属性ベース
» サブジェクトベース
» オブジェクトベース

ドメイン 2:
セキュリティ運用及び管理

2.1 倫理規定の順守

» (ISC)²倫理規定
» 組織の倫理規定

2.2 セキュリティ概念の理解

» 機密性
» 完全性
» 可用性
» 責任追跡性
» プライバシー
» 否認防止
» 最小権限
» 職務の分離

2.3 機能的なセキュリティ制御の文書化、実装及び維持

» 抑止制御
» 予防制御
» 検知制御
» 是正制御
» 補償制御

2.4 資産管理への参画

» ライフサイクル（ハードウェア、ソフトウェア及び情報）
» ハードウェア一覧
» ソフトウェア一覧及びライセンス
» データストレージ

2.5 セキュリティ制御の実装及び遵守度の評価

» 技術的制御（例：セッションタイムアウト、パスワード劣化）
» 物理的制御（例：侵入者捕獲装置、カメラ、錠前）
» 管理的制御（例：セキュリティポリシー、規格、手順及びベースライン）
» 定期監査及びレビュー

2.6 変更管理への参画

» 変更管理手順の遂行
» セキュリティインパクトの特定
» パッチ、修正及びアップデート実装の試行（例：オペレーティングシステム、アプリケーション、SDLC）

2.7 セキュリティ意識喚起及び訓練への参画

2.8 物理セキュリティ運用への参画（例：データセンターの評価、バッジ管理）

ドメイン 3:
リスクの特定、監視及び分析

3.1 リスク管理手順の理解

» リスクの可視化及び報告（例：リスクの登録、脅威インテリジェンスの共有、共通脆弱性評価システム（CVSS））
» リスク管理の概念（例：インパクト評価、脅威モデリング、ビジネスインパクト分析（BIA））
» リスク管理フレームワーク（例：ISO、NIST）
» リスク処理（例：受容、移転、緩和、退避、改変

3.2 セキュリティ評価活動の実施

» セキュリティテストへの参画
» スキャニング及びテスト結果の解釈及び報告
» 妥当性確認の修正
» 監査指摘事項に基づく修正

3.3 監視システムの運用及び管理（例：継続監視）

» 関係するイベント（例：異常、侵入、認可されていない変更、遵守度の監視）
» ログ
» ソースシステム
» 法規及び法令上の懸念（例：司法、制限及びプライバシー）

3.4 監視結果の分析

» セキュリティベースライン及び異常
» 可視化、定量化及び傾向（例：ダッシュボード、時系列）
» イベントデータ分析
» 文書及びコミュニケーション上の気づき（例：エスカレーション）

ドメイン 4:
インシデント対応及び復旧

4.1 インシデントライフサイクルの支援

» 準備
» 検知、分析及びエスカレーション
» 封じ込め
» 根絶
» 復旧
» 教訓／新しい対策の実装

4.2 フォレンジック調査の理解と支援

» 法規及び倫理原則
» 証拠ハンドリング（例：第一対応者、トリアージ、過程管理、現場の保全）

4.3 事業継続計画（BCP）及び災害復旧計画（DRP）活動の理解と支援

» 緊急対応計画及び手順（例：情報システム非常事態計画）
» 暫定または代替手順の戦略
» 復旧計画
» バックアップ及び冗長性の実装
» テスト及び訓練

ドメイン 5:
暗号

5.1 暗号の基本的な概念の理解

» ハッシュ
» ソルト
» 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、HMAC、監査証跡）
» 暗号化アルゴリズム（例：AES、RSA）
» 鍵強度（例：256、512、1024、2048ビット鍵）
» 暗号攻撃、暗号分析及び対策

5.2 暗号化の理由と要件の理解

» 機密性
» 完全性及び真正性
» データの重要度（例：PII、知的所有、PHI）
» 規制

5.3 セキュアプロトコルの理解と支援

» サービス及びプロトコル（例：IPSec、TLS、S/MIME、DKIM）
» 共通利用ケース
» 制約及び脆弱性

5.4 公開鍵基盤（PKI）システムの理解

» 基本的な鍵管理の概念（例：鍵のローテーション、鍵の組成、鍵の作成、交換、廃止、供託）
» ウェブの信頼性（WOT）（例：PGP、GPG）

ドメイン 6:
ネットワーク及び通信セキュリティ

6.1 基本的なネットワーク概念の理解と適用

» OSI及びTCP/IPモデル
» ネットワークトポグラフィ（例：リング型、スター型、バス型、メッシュ型、ツリー型）
» ネットワーク関係性（例：ピアツーピア、クライアントサーバ）
» 伝送メディア種類（例：光ファイバー、有線、無線）
» 共用ポート及びプロトコル

6.2 ネットワーク攻撃及び対策の理解（例：DDoS、中間者攻撃、DNSポイズニング）

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及び監視（例：修正、検疫、入場）
» ネットワークアクセス制御規格及びプロトコル（例：IEEE 802.1x、Radius、TACACS）
» リモートアクセス運用及び構成（例：シンクライアント、SSL VPN、IPSec VPN、テレワーク）

6.4 ネットワークセキュリティの管理

» 論理的及び物理的なネットワークデバイスの配置（例：インライン、パッシブ）
» 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、VLAN、ACLs）
» セキュアデバイス管理

6.5 ネットワーク上のセキュリティデバイスの運用及び構成

» ファイアウォール及びプロキシ（例：フィルタリング）
» ネットワーク侵入検知／予防システム
» ルータ及びスイッチ
» トラフィック形成デバイス（例：WAN最適化、負荷平準化）

6.6 ワイヤレス技術の運用及び構成（例：ブルートゥース、NFC、WiFi）

» 伝送セキュリティ
» 無線セキュリティデバイス（例：WIPS、WIDS）

ドメイン 7:
システム及びアプリケーションセキュリティ

7.1 悪質なコード及び活動の特定及び分析

» マルウェア（例：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、ウイルス、ワーム、トラップドア、バックドア及びリモートアクセス　トロイの木馬）
» 悪質なコードへの対策（例：スキャナ、アンチマルウェア、コードサイニング、サンドボックス）
» 悪質な活動（例：内部の脅威、データ盗難、DDoS、ボットネット）
» 悪質な活動への対策（例：ユーザ注意喚起、システム堅固化、パッチ、サンドボックス、アイソレーション）

7.2 エンドポイントデバイスセキュリティの実装及び運用

» HIDS
» ホストベースファイアウォール
» 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
» トラステッド・プラットフォーム・モジュール（TPM）
» モバイルデバイス管理（MDM）（例：COPE、BYOD）
» セキュアブラウジング（例：サンドボックス）

7.3 クラウドセキュリティの運用及び構成

» モジュールのデプロイ（例：パブリック、プライベート、ハイブリッド及びコミュニティ）
» サービスモジュール（例：IaaS、PaaS及び SaaS）
仮想化（例：ハイパーバイザ）
» 法規及び規制上の懸念（例：プライバシー、調査、データ所有権、司法、eDiscovery）
» データストレージ及び伝送（例：アーカイブ、復旧、回復）
» 第三者／外部委託要件（例：SLA、データの可搬性、データの破壊、監査）
» 責任共有モデル

7.4 仮想環境の運用及び保全

» ソフトウェアで定義されたネットワーク
» ハイパーバイザ
» 仮想アプライアンス
» 継続性及び回復力
» 攻撃及び対策
» 共有ストレージ

試験に関する追加情報

補足情報

受験者は、CBKに付随する関連情報を熟読し、追加の配慮が必要な専攻分野を特定することによって、教育及び経験を補完することが奨励されます。

全ての補足情報は www.isc2.org/certifications/References. をご覧ください。

試験ポリシー及び手順

(ISC)²はSSPC受験者に対し、受験登録前に試験ポリシー及び手順を熟読することを推奨いたします www.isc2.org/Register-for-Exam. 細かく網羅された重要な情報をお読み取りください。

法務情報

(ISC)²の法令ポリシー に関するいかなる質問は、(ISC)2法務部門 legal@isc2.org. にご連絡ください。

質問がありますか?

(ISC)² 受験者サービス窓口
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² アメリカ
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² アジアパシフィック
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² ヨーロッパ
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org