CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

認定試験の概要

発効日：2019年8月1日

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

CCSPについて

(ISC)²とCloud Security Alliance(CSA)は、クラウドセキュリティの専門家がクラウドセキュリティの設計、実装、アーキテクチャ、運用、制御、規制フレームワークの遵守に必要な知識、スキル、および能力を持つことを証明することを目的に、Certified Cloud Security Professional(CCSP)資格を開発しました。CCSPは、情報セキュリティの専門知識をクラウドコンピューティング環境に適用し、クラウドセキュリティのアーキテクチャ、設計、運用、およびサービスオーケストレーションにおける能力を実証します。この専門的能力は、世界的に認められた知識体系に対して評価されます。CCSPは、(ISC)²の認定情報システムセキュリティプロフェッショナル(CISSP)およびCSAのクラウドセキュリティ知識証明書(CCSK)を含む、既存の資格情報および教育プログラムを補完および構築するスタンドアロン資格情報です。

CCSP Common Knowledge of Knowledge(CBK)に含まれるトピックは、クラウドセキュリティの分野のすべての分野にわたってその関連性を保証します。成功した候補者は、次の6つのドメインで有能です。

- クラウドの概念、アーキテクチャ、および設計
- クラウドデータセキュリティ
- クラウドプラットフォームとインフラストラクチャセキュリティ
- クラウドアプリケーションのセキュリティ
- クラウドセキュリティオペレーション
- 法務、リスク、コンプライアンス

実務要件

候補者は、最低5年の情報技術の累積有給実務経験が必要です。そのうち3年は情報セキュリティ、1年はCCSP CBKの6つのドメインの1つ以上で実務経験があることが求められます。CSAのCCSK証明書を取得すると、CCSP CBKの6つのドメインの1つ以上での1年間の経験に置き換えることができます。CISSP 資格取得者は、CCSP実務要件が免除されます。

CCSPになるために必要な経験がない候補者は、CCSP試験に合格すると、(ISC)²のアソシエイトになることができます。(ISC)²のアソシエイトは、6年間の5年間の経験を積むことができます。CCSPの経験要件とパートタイムの仕事とインターンシップを説明する方法の詳細については、www.isc2.org / Certifications / CCSP / experience-requirementsをご覧ください。

認定

ANSI / ISO / IEC規格17024の厳しい要件に準拠するためのANSIレビューに基づくCCSP。

ジョブタスク分析(JTA)

(ISC)²は、CCSPの関連性を維持するために、そのメンバーシップに対して責任を負います。定期的に実施されるジョブタスク分析(JTA)は、CCSPによって定義された専門職に従事するセキュリティ専門家によって実行されるタスクを決定するための系統的かつ重要なプロセスです。JTAの結果は、試験の更新に使用されます。このプロセスにより、最新のクラウドテクノロジーに焦点を合わせた情報セキュリティ専門家の役割と責任に関連するトピック領域で候補者がテストされることが保証されます。

CCSP試験情報

試験時間3時間

質問の数125

質問形式 多肢選択式

1000点満点で700点合格

受験可能言語 英語、日本語

テストセンター ピアソンVUEテストセンター

CCSP試験配分

ドメイン	配分
1. クラウドの概念、アーキテクチャ、および設計	17%
2. クラウドデータセキュリティ	19%
3. クラウドプラットフォームとインフラストラクチャセキュリティ	17%
4. クラウドアプリケーションセキュリティ	17%
5. クラウドセキュリティオペレーション	17%
6. 法務、リスク、コンプライアンス	13%
合計I:	100%

ドメイン1
クラウドの概念、アーキテクチャ、および設計

1.1 クラウドコンピューティングの概念を理解する

» クラウドコンピューティングの定義
» クラウドコンピューティングの役割（クラウドサービスの顧客、クラウドサービスプロバイダー、クラウドサービスパートナー、クラウドサービスブローカーなど）
» 主要なクラウドコンピューティングの特性（例：オンデマンドセルフサービス、ブロードネットワークアクセス、マルチテナンシー、スピーディな拡張性とスケーラビリティ、リソースプーリング、従量制サービス）
» ビルディングブロックテクノロジー（仮想化、ストレージ、ネットワーキング、データベース、オーケストレーションなど）

1.2 クラウドリファレンスアーキテクチャについて説明する

» クラウドコンピューティング活動
» クラウドサービス機能（つまり、アプリケーション機能タイプ、プラットフォーム機能タイプ、インフラストラクチャ機能タイプ）
» クラウドサービスのカテゴリ（サービスとしてのソフトウェア（SaaS）、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）など）
» クラウド展開モデル（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）
» クラウド共有の考慮事項（例：相互運用性、移植性、可逆性、可用性、セキュリティ、プライバシー、復元力、パフォーマンス、ガバナンス、保守とバージョン管理、サービスレベルとサービスレベルアグリーメント（SLA）、監査性、規制）
» 関連テクノロジーの影響（例：機械学習、人工知能、ブロックチェーン、モノのインターネット（IoT）、コンテナー、量子コンピューティング）

1.3 クラウドコンピューティングに関連するセキュリティの概念を理解する

» 暗号化とキー管理
» アクセス制御
» データとメディアのサニタイズ（例：上書き、暗号消去）
» ネットワークセキュリティ（ネットワークセキュリティグループなど）
» 仮想化セキュリティ（ハイパーバイザーセキュリティ、コンテナーセキュリティなど）
» 一般的な脅威

1.4 安全なクラウドコンピューティングの設計原則を理解する

» クラウドの安全なデータライフサイクル
» クラウドベースの災害復旧（DR）とビジネス継続性（BC）の計画
» 費用便益分析
» 機能的セキュリティ要件（移植性、相互運用性、ベンダーロックインなど）
» さまざまなクラウドカテゴリのセキュリティに関する考慮事項（サービスとしてのソフトウェア（SaaS）、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）など）

1.5 クラウドサービスプロバイダーを評価する

» 基準に対する検証（例：国際標準化機構/ International Electrotechnical Commission（ISO / IEC）27017、Payment Card Industry Data Security Standard（PCI DSS））
» システム/サブシステム製品の認定（例：Common Criteria（CC）、Federal Information Processing Standard（FIPS）140-2）

ドメイン2
クラウドデータセキュリティ

2.1 クラウドデータの概念について説明する

» クラウドデータのライフサイクルのフェーズ
» データ分散

2.2 クラウドデータストレージアーキテクチャの設計と実装

» ストレージのタイプ（例：長期、短期、ローディスク）
» ストレージタイプに対する脅威

2.3 データセキュリティ技術と戦略の設計と適用

» 暗号化とキー管理
» ハッシュ
» マスキング
» トークン化
» データ損失防止（DLP）
» データ難読化
» データの匿名化（例：匿名化）

2.4 データ検出を実装する

» 構造化データ
» 非構造化データ

2.5 データ分類を実装する

» マッピング
» ラベリング
» 機密データ（保護された健康情報（PHI）、個人識別情報（PII）、カード所有者データなど）

2.6 Information Rights Management（IRM）の設計と実装

» 目的（例：データの権利、プロビジョニング、アクセスモデル）
» 適切なツール（証明書の発行や失効など）

2.7 データの保持、削除、アーカイブポリシーを計画および実装する

» データ保持ポリシー
» データ削除手順とメカニズム
» データのアーカイブ手順とメカニズム
» 訴訟ホールド

2.8 データイベントの監査可能性、追跡可能性、および説明責任を設計および実装する

» イベントソースの定義とID属性の要件
» データイベントのロギング、保存、分析
» 監護の連鎖と否認防止

ドメイン3
クラウドプラットフォームとインフラストラクチャのセキュリティ

3.1 クラウドインフラストラクチャコンポーネントを理解する

- 物理的環境
- ネットワークと通信
- 計算する
- 仮想化
- ストレージ
- 管理プレーン

3.2 安全なデータセンターを設計する

- 論理設計（例：テナントのパーティション分割、アクセス制御）
- 物理的な設計（場所、購入、構築など）
- 環境設計（暖房、換気、空調（HVAC）、マルチベンダーパス接続など）

3.3 クラウドインフラストラクチャに関連するリスクを分析する

- リスク評価と分析
- クラウドの脆弱性、脅威、攻撃
- 仮想化のリスク
- 対策戦略

3.4 セキュリティ管理の設計と計画

- 物理的および環境的保護（オンプレミスなど）
- システムと通信の保護
- 仮想化システムの保護
- クラウドインフラストラクチャでの識別、認証、および承認
- 監査メカニズム（ログ収集、パケットキャプチャなど））

3.5 災害復旧（DR）とビジネス継続性（BC）の計画

- クラウド環境に関連するリスク
- ビジネス要件（例：目標復旧時間（RTO）、目標復旧ポイント（RPO）、復旧サービスレベル（RSL））
- ビジネス継続性/災害復旧戦略
- 計画の作成、実装、およびテスト

ドメイン4
クラウドアプリケーションのセキュリティ

4.1 アプリケーションのセキュリティに関するトレーニングと認識を提唱する

» クラウド開発の基本
» 一般的な落とし穴
» 一般的なクラウドの脆弱性

4.2 セキュアソフトウェア開発ライフサイクル（SDLC）プロセスの説明

» ビジネス要件
» フェーズと方法論

4.3 セキュアソフトウェア開発ライフサイクル（SDLC）の適用

» 開発中に一般的な脆弱性を回避する
» クラウド固有のリスク
» 品質保証
» 脅威モデリング
» ソフトウェア構成管理とバージョン管理

4.4 クラウドソフトウェアの保証と検証を適用する

» 機能テスト
» セキュリティテストの方法論

4.5 検証済みの安全なソフトウェアを使用する

» 承認済みのアプリケーションプログラミングインターフェイス（API）
» サプライチェーンマネジメント
» サードパーティのソフトウェア管理
» 検証済みのオープンソースソフトウェア

4.6 クラウドアプリケーションアーキテクチャの詳細を理解する

» 補足的なセキュリティコンポーネント（Webアプリケーションファイアウォール（WAF）、データベースアクティビティ監視（DAM）、Extensible Markup Language（XML）ファイアウォール、アプリケーションプログラミングインターフェイス（API）ゲートウェイなど）
» 暗号化
» サンドボックス化
» アプリケーションの仮想化とオーケストレーション

4.7 適切なIDおよびアクセス管理（IAM）ソリューションを設計する

» フェデレーションID
» IDプロバイダー
» シングルサインオン（SSO）
» 多要素認証
» クラウドアクセスセキュリティブローカー（CASB）

ドメイン5
クラウドセキュリティオペレーション

5.1 クラウド環境の物理的および論理的インフラストラクチャを実装および構築する

- ハードウェア固有のセキュリティ構成要件（たとえば、仮想化のための基本入出力システム（BIOS）設定とTrusted Platform Module（TPM）、ストレージコントローラー、ネットワークコントローラー）
- 仮想化管理ツールのインストールと構成
- 仮想ハードウェア固有のセキュリティ構成要件（ネットワーク、ストレージ、メモリ、中央処理装置（CPU）など）
- ゲストオペレーティングシステム（OS）仮想化ツールセットのインストール

5.2 クラウド環境の物理的および論理的インフラストラクチャを運用する

- ローカルアクセスとリモートアクセスのアクセス制御を構成する（例：セキュアキーボードビデオマウス（KVM）、コンソールベースのアクセスメカニズム、リモートデスクトッププロトコル（RDP））
- 安全なネットワーク構成（例：仮想ローカルエリアネットワーク（VLAN）、トランスポート層セキュリティ（TLS）、動的ホスト構成プロトコル（DHCP）、ドメインネームシステム（DNS）、仮想プライベートネットワーク（VPN））
- ベースラインの適用によるオペレーティングシステム（OS）の強化（例：Windows、Linux、VMware）
- スタンドアロンホストの可用性
- クラスター化されたホストの可用性（分散リソーススケジューリング（DRS）、動的最適化（DO）、ストレージクラスター、メンテナンスモード、高可用性など）
- ゲストオペレーティングシステム（OS）の可用性

5.3 クラウド環境の物理的および論理的インフラストラクチャを管理する

- リモートアクセスのアクセス制御（リモートデスクトッププロトコル（RDP）、Secure Terminal Access、Secure Shell（SSH）など）
- オペレーティングシステム（OS）ベースラインコンプライアンスの監視と修正
- パッチ管理
- パフォーマンスと容量の監視（ネットワーク、コンピューティング、ストレージ、応答時間など）
- ハードウェア監視（例：ディスク、中央処理装置（CPU）、ファン速度、温度）
- ホストおよびゲストオペレーティングシステム（OS）のバックアップおよび復元機能の構成
- ネットワークセキュリティコントロール（ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS）、ハニーポット、脆弱性評価、ネットワークセキュリティグループなど）
- 管理プレーン（例：スケジューリング、オーケストレーション、メンテナンス）

5.4 運用管理と標準の実装（例：情報技術インフラストラクチャライブラリ（ITIL）、国際標準化機構/国際電気標準会議（ISO / IEC）20000-1）

- 変更管理
- 継続性管理
- 情報セキュリティ管理
- 継続的なサービス改善管理
- 事故管理
- 問題管理
- リリース管理
- 展開管理
- 構成管理
- サービスレベル管理
- 可用性管理
- 容量管理

5.5 デジタルフォレンジックをサポート

- 法医学データ収集方法論
- 証拠管理
- デジタル証拠を収集、取得、保存する

5.6 関連当事者とのコミュニケーションを管理する

- ベンダー
- お客さま
- パートナー
- 規制当局
- その他の利害関係者

5.7 セキュリティ操作を管理する

- セキュリティオペレーションセンター（SOC）
- セキュリティ制御の監視（例：ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS）、ハニーポット、脆弱性評価、ネットワークセキュリティグループ）
- ログのキャプチャと分析（セキュリティ情報とイベント管理（SIEM）、ログ管理など）
- 事故管理

ドメイン6
法務、リスク、コンプライアンス

6.1 法的要件とクラウド環境内の固有のリスクを明確に示す

- 矛盾する国際法
- クラウドコンピューティングに固有の法的リスクの評価
- 法的枠組みとガイドライン
- 電子情報開示（例：国際標準化機構/国際電気標準会議（ISO / IEC）27050、クラウドセキュリティアライアンス（CSA）ガイダンス）
- 法医学の要件

6.2 プライバシーの問題を理解する

- 契約上のプライベートデータと規制されたプライベートデータの違い（例：保護された健康情報（PHI）、個人を特定できる情報（PII））
- 個人データに関連する国固有の法律（例：保護された健康情報（PHI）、個人識別情報（PII））
- データプライバシーの管轄権の違い
- 標準のプライバシー要件（例：国際標準化機構/国際電気標準会議（ISO / IEC）27018、一般に認められたプライバシー原則（GAPP）、一般データ保護規則（GDPR））

6.3 監査プロセス、方法論、およびクラウド環境に必要な適応について理解する

- 内部および外部の監査管理
- 監査要件の影響
- 仮想化とクラウドの保証の課題を特定する
- 監査レポートのタイプ（例：アテステーションエンゲージメントの標準に関するステートメント（SSAE）、サービス組織統制（SOC）、国際的なスタンダードのアシュアランスエンゲージメント（ISAE））
- 監査範囲ステートメントの制限（例：アテステーションエンゲージメントの標準に関するステートメント（SSAE）、アシュアランスエンゲージメントに関する国際標準（ISAE））
- ギャップ分析
- 監査計画
- 内部情報セキュリティ管理システム（ISMS）
- 内部情報セキュリティ管理体制
- ポリシー（組織、機能、クラウドコンピューティングなど）
- 関連する利害関係者の特定と関与
- 高度に規制された業界向けの特別なコンプライアンス要件（例：北米電気信頼性公社/重要インフラ保護（NERC / CIP）、医療保険の相互運用性と説明責任に関する法律（HIPAA）、支払いカード業界（PCI））
- 分散情報技術（IT）モデルの影響（たとえば、地理的な場所の多様性や法的管轄区域の境界）

6.4 クラウドがエンタープライズリスク管理に与える影響を理解する

- プロバイダーのリスク管理プログラムを評価する（例：コントロール、方法論、ポリシー）
- データ所有者/管理者とデータ管理者/処理者の違い（例：リスクプロファイル、リスク選好度、責任）
- 規制の透明性要件（違反通知、Sarbanes-Oxley（SOX）、一般データ保護規則（GDPR）など）
- リスク対応（つまり、回避、変更、共有、保持）
- さまざまなリスクフレームワーク
- リスク管理の指標
- リスク環境の評価（サービス、ベンダー、インフラストラクチャなど）

6.5 アウトソーシングとクラウド契約設計を理解する

- ビジネス要件（サービスレベルアグリーメント（SLA）、マスターサービスアグリーメント（MSA）、作業明細書（SOW）など）
- ベンダー管理
- 契約管理（例：監査する権利、測定基準、定義、解約、訴訟、保証、コンプライアンス、クラウド/データへのアクセス、サイバーリスク保険）
- サプライチェーン管理（例：国際標準化機構/国際電気標準会議（ISO / IEC）27036）

追加試験情報

参考資料

受験者は自身の学習や実務経験の補足として、CBKに関連する参考情報の確認や、追加で情報収集が必要と思われる分野を把握しておくことが推奨されます。
www.isc2.org/certifications/Referencesにアクセスし、試験分野の参考情報を確認してください。

審査方針と手続き

(ISC)²は、受験申し込みの前にCCSP候補者が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。
www.isc2.org/Register-for-Examにアクセスし、それらの情報を確認してください。

法的情報

(ISC)²の法的ポリシーに関する質問については、(ISC)²法務部門(legal@isc2.org)にお問い合わせください

お問合せ先

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

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