CCSP®

Certified Cloud Security Professional

ISC2 Certification

認定資格の試験の概要

実施日：2022年8月1日

ISC2™

CCSPについて

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へのコンプライアンスに関して必要な知識、スキル、能力を確実に備えていることを証明するために、ISC2はCertified Cloud Security Professional（CCSP）資格認定証明書を創設しました。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 アーキテクチャ、設計、運用、サービス オーケストレーションにおける適性を実証します。この専門的な適性は世界的に認められている知識体系に基づいて評価されます。

CCSP 知識体系に含まれるトピックは、クラウドセキュリティ領域におけるあらゆる分野における関連性を確実にします。試験に合格した受験者は、次の6つのドメインに関して十分な適性があります。

- クラウドの概念、アーキテクチャ、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

求められる経験について

受験者は、情報テクノロジー（IT)分野で少なくとも5年間のフルタイム累積実務経験が必要です。
3年間はサイバーセキュリティにおいて、1年間は現行のCCSP認定試験のアウトラインに含まれるの6つのドメインの、最低1つの分野における経験が必要です。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。ISC2承認リストに記載されている追加の資格証明書を取得することで、CCSP認定試験の概要の6つのドメインのうち1つ以上のドメインで、1年間の経験に置き換えることができます。CISSP認定資格を取得することで、CCSPの経験要件すべてを満たすことになります。パートタイム勤務やインターンシップも、経験要件に考慮される場合があります。

CCSPになるために必要な経験を有していない受験者でも、CCSP試験に合格することでISC2 Associateになることができます。ISC2 Associateでは、必要な5年分の経験を積むために6年間の猶予が与えられます。CCSPの経験要件と、パートタイム勤務期間の計算方法やインターンシップについての詳細は、
www.isc2.org/Certifications/CCSP/experience-requirementsをご覧ください。

認定

CCSPはANSI/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、そのメンバーシップに対してCCSP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作業タスク分析（JTA）は、CCSP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、クラウドテクノロジーに重点を置い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テーマに関して、受験者が確実に審査されるようにします。

CCSP試験情報

試験時間	3時間
出題数	125
出題形式	選択方式
合格ライン	1000点満点中700点
試験で使用される言語	英語、中国語、ドイツ語、日本語
受験会場	ピアソンVUEテストセンター

CCSP試験の比重

ドメイン	比重
1.クラウドの概念、アーキテクチャ、設計	17%
2.クラウド データセキュリティ	20%
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	16%
6.法務、リスク、コンプライアンス	13%
合計：	**100%**

ドメイン1：
クラウドの概念、アーキテクチャ、設計

1.1 クラウド コンピューティングの概念に対する理解

» 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と責任（例：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、規制当局）

» 主要なクラウド コンピューティングの特性（例：オンデマンドのセルフサービス、広範なネットワークアクセス、マルチテナント、迅速な弾力性と拡張性、リソースプーリング、計測可能サービス）

» ビルディング ブロック テクノロジー（例：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）

1.2 クラウド リファレンス アーキテクチャに関する説明

» 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（例：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種類（例：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））

» クラウドの展開モデル（例：パブリック、プライベート、ハイブリッド、コミュニティ、マルチクラウド）

» クラウド共有の考慮事項（例：相互運用性、ポータビリティ、可逆性、可用性、セキュリティ、プライバシー、回復力、パフォーマンス、ガバナンス、メンテナンスとバージョン管理、サービスレベルとサービスレベル契約（SLA）、監査可能性、規制、アウトソーシング）

» 関連テクノロジーの影響（データ サイエンス、機械学習、人工知能 （AI）、ブロックチェーン、モノのインターネット（IoT）（IoT）、コンテナ、量子コンピューティング、エッジコンピューティング、機密コンピューティング、DevSecOps）

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の理解

» 暗号化と鍵管理

» IDとアクセス制御（例：ユーザーアクセス、特権アクセス、サービスアクセス）

» データおよびメディアのサニタイゼーション（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、トラフィック検査、ジオフェンシング、ゼロトラストネットワーク）

» 仮想化セキュリティ（例：ハイパーバイザーセキュリティ、コンテナセキュリティ、エフェメラルコンピューティング、サーバーレステクノロジー）

» 一般的な脅威

» セキュリティ ハイジーン（例：パッチング、ベースライニング）

1.4 安全なクラウド コンピューティングの設計原則に対する理解

» クラウドの安全なデータのライフサイクル

» クラウドベースの事業継続性（BC）および災害復旧（DR）の計画

» 事業インパクト分析（BIA）（例：費用対効果分析、投資利益率（ROI））

» ファンクショナル セキュリティ要件（例：ポータビリティ、相互運用性、ベンダーロックイン）

» さまざまなクラウドカテゴリ（例：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）のセキュリティに関する考慮事項と責任

» クラウド設計パターン（例：SANSセキュリティ原則、Well-Architectedフレームワーク、クラウド セキュリティアライアンス（CSA）企業アーキテクチャ）

» DevOpsセキュリティ

1.5 クラウド･サービス･プロバイダーの評価

» 基準に照らした検証（例：国際規格化機構/国際電気規格会議（ISO/IEC）27017、ペイメントカード業界データセキュリティ規格（PCI DSS））

» システム/サブシステム製品認定（例：一般基準（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 クラウドデータに関する概念の説明

» クラウドデータに関するライフサイクルのフェーズ
» データの分散
» データフロー

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

» ストレージの種類（例：長期、一時、ローストレージ）
» 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 テクノロジーと戦略の設計と適用

» 暗号化と鍵管理
» ハッシュ化
» データの難読化（例：マスキング、匿名化）
» トークン化
» データ損失防止（DLP）
» キー、シークレット、認証の管理

2.4 データ ディスカバリーの実装

» 構造化データ
» 構造化データ
» 半構造化データ
» データ ロケーション

2.5 データ分類の計画と実装

» データ分類ポリシー
» データマッピング
» データラベリング

2.6 情報権限管理（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（例：証明書の発行と失効）

2.7 データの保持、削除、アーカイブのポリシーの計画および実装

- データ保持ポリシー
- データ削除の手順とメカニズム
- データアーカイブの手順とメカニズム
- 法的保全

2.8 データイベントの監査可能性、追跡可能性、説明責任の設計および実装

- イベントソースの定義とイベント属性の要件（例：ID、インターネットプロトコル（IP） アドレス、地理位置情報）
- データイベントのログ、保存、分析
- 保管管理と否認防止

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セキュリティ

3.1 クラウド インフラ ストラクチャとプラットフォーム コンポーネントの理解

- 物理的環境
- ネットワークと通信
- コンピューティング
- 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の設計

- 論理設計（例：テナント分割、アクセス制御）
- 物理設計（例：場所、購入、構築）
- 環境設計（例：暖房、換気、および空調（HVAC）、マルチベンダー経路接続）
- 設計耐性

3.3 クラウド インフラ ストラクチャとプラットフォームに関連するリスクの分析

- リスク評価（例：識別、分析）
- クラウドの脆弱性、脅威、攻撃
- リスク軽減戦略

3.4 セキュリティ管理の計画と実装

- 物理的および環境的保護（例：オンプレミス）
- システム、ストレージ、通信の保護
- クラウド環境における識別、認証、認可
- 監査メカニズム（例：ログ収集、相関関係、パケットキャプチャ）

3.5 事業継続性（BC）および災害復旧（DR）の計画

- 事業継続性（BC）/災害復旧（DR）戦略
- 事業要件（例：目標復旧時間（RTO）、復旧点目標（RPO）、復旧サービスレベル）
- 計画の作成、実施、テスト

ドメイン4：
クラウド アプリケーションセキュリティ

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意識向上の提唱

» クラウド開発の基本
» よくある落とし穴
» 一般的なクラウドの脆弱性（例：オープンWebアプリケーションセキュリティプロジェクト（OWASP）Top-10、SANS Top-25）

4.2 安全な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（例：設計、コード、テスト、保守、ウォーターフォールとアジャイル）

4.3 安全なソフトウェア開発ライフサイクル（SDLC）の適用

» クラウド固有のリスク
» 脅威モデル（例：なりすまし、改ざん、否認、情報漏えい、サービス拒否、特権の昇格（STRIDE）、災害、再現性、悪用可能性、影響を受けるユーザーと 発見可能性（DREAD）、アーキテクチャ、脅威、攻撃対象領域と緩和策（ATASM）、攻撃のシミュレーションと脅威の分析のためのプロセス（PASTA））
» 開発中に一般的な脆弱性を回避する
» 安全なコーディング（例：オープンWebアプリケーションセキュリティプロジェクト（OWASP）、アプリケーションセキュリティ検証基準（ASVS）、卓越したコードのためのソフトウェア保証フォーラム（SAFECode））
» 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の適用

» 機能テストと非機能テスト
» セキュリティ テスト方法（例：ブラックボックス、ホワイトボックス、静的、動的、ソフトウェア構造解析（SCA）、対話型アプリケーションのセキュリティテスト（IAST））
» 品質保証（QA）
» 悪用ケーステスト

4.5 検証済みの安全なソフトウェアの使用

» アプリケーション プログラミン グインターフェース（API）のセキュリティ保護
» サプライチェーン管理（例：ベンダー評価）
» サードパーティのソフトウェア管理（例：ライセンス）
» 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の理解

» 補足的なセキュリティ コンポーネント（例：Webアプリケーションファイアウォール（WAF）、データベース活動監視（DAM）、拡張可能なマークアップ言語（XML）ファイアウォール、アプリケーション プログラミング インターフェース（API） ゲートウェイ）
» 暗号化
» サンドボクシング
» アプリケーションの仮想化とオーケストレーション （例：マイクロサービス、コンテナ）

4.7 適切なIDおよびアクセス管理（IAM）ソリューションの設計

» フェデレーション アイデンティティ
» IDプロバイダ（IdP）
» シングルサインオン（SSO）
» 多要素認証（MFA）
» クラウド アクセス セキュリティブローカー（CASB）
» 機密管理

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の構築と実装

» ハードウェア固有のセキュリティ構成要件（例：ハードウェア セキュリティ モジュール（HSM）および信頼性の高いプラットフォーム モジュール（TPM））

» 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（例：ネットワーク、ストレージ、メモリ、中央処理装置(CPU)、ハイパーバイザー タイプ1および2）

» 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の運用および維持

» ローカルおよびリモートアクセスのアクセス制御（例：リモートデスクトッププロトコル（RDP）、セキュア ターミナル アクセス、セキュアシェル（SSH）、コンソールベースのアクセス メカニズム、ジャンプボックス、仮想クライアント）

» 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（LAN）、転送層セキュリティ（TLS）、ダイナミックホスト構成プロトコル（DHCP）、ドメインネーム システムセキュリティ拡張（DNSSEC）、仮想プライベートネットワーク（VPN））

» ネットワークセキュリティ制御（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、要塞ホスト）

» オペレーティングシステム（OS）ベースライン、監視、修復の適用による強化（例：Windows、Linux、VMware）

» パッチ管理

» コードとしてのインフラストラクチャ（IaC）戦略

» クラスタ化されたホストの可用性（例：分散リソーススケジューリング、動的最適化、ストレージクラスタ、メンテナンスモード、高可用性（HA））

» ゲストオペレーティングシステムの可用性（OS）

» パフォーマンスと容量の監視（例：ネットワーク、コンピューティング、ストレージ、応答時間）

» 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の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

» 管理プレーン（例：スケジュール、オーケストレーション、メンテナンス）

5.3 運用管理と標準の導入（例：情報テクノロジー インフラストラクチャ ライブラリ（ITIL）、国際規格化機構/国際電気規格会議（ISO/IEC）20000-1）

- リスク管理
- 継続性マネジメント
- 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
- 導入管理
- 構成管理
- サービスレベル管理
- 可用性管理
- キャパシティ管理

5.4 デジタル フォレンジックのサポート

- フォレンジックデータの収集方法
- 証拠管理
- デジタル証拠の収集、取得、保存

5.5 関係者とのコミュニケーションの管理

- ベンダー
- 顧客
- パートナー
- 規制
- その他のステークホルダー

5.6 セキュリティ運用の管理

- 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インテリジェント監視（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、ネットワーク セキュリティ グループ、人工知能（AI））
- ログのキャプチャと分析（例：セキュリティ情報及びイベント管理（SIEM）、ログ管理）
- 事故管理
- 脆弱性評価

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特有のリスクの明確な説明

» 矛盾する国際法
» クラウド コンピューティング特有の法的リスクの評価
» 法的枠組みとガイドライン
» eDiscovery（例：国際規格化機構/国際電気規格会議（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）
» フォレンジック要件

6.2 プライバシーの問題の理解

» 契約上の個人データと規制された個人データの違い（例：保護された健康情報（PHI）、個人情報（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）、個人情報（PII））
» データプライバシーにおける管轄区域の違い
» 標準的なプライバシー要件（例：国際規格化機構/国際電気規格会議（ISO/IEC） 27018、一般に認められているプライバシー原則（GAPP）、一般データ保護規則（GDPR））
» プライバシー影響評価（PIA）

6.3 監査プロセス、方法論、クラウド環境に必要な適応の理解

» 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上の課題の特定
» 監査報告書の種類（例：認証業務の基準に関する声明（SSAE）、サービス組織管理（SOC）、保証契約に関する国際規格（ISAE））
» 監査範囲の制限ステートメント（例：認証業務の基準に関するステートメント（SSAE）、保証契約に関する国際規格（ISAE））
» ギャップ分析（例：コントロール分析、ベースライン）
» 監査計画
» 内部情報セキュリティ管理システム
» 内部情報セキュリティ管理システム
» ポリシー （例：組織、機能、クラウド コンピューティング）
» 関連する利害関係者の識別と関与
» 高度に規制された業界に特化したコンプライアンス要件（例：北米電力信頼度協議会 /重要インフラストラクチャ保護（NERC / CIP）、医療保険の携行性と責任に関する法律（HIPAA）、経済臨床衛生法のための医療情報テクノロジー（HITECH）に関する法律、クレジットカード業界（PCI））
» 分散型情報テクノロジー（IT)モデルの影響 （例：多様な地理的場所や法的管轄区域の横断）

6.4 企業リスク管理に対するクラウドの影響への理解

» 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、リスク プロファイル、リスクアペタイト）
» データ所有者/管理者とデータ管理者/処理者の違い
» 規制の透明性要件 （例：違反通知、サーベンス・オクスリー法（SOX）、一般データ保護規則（GDPR））
» リスク処理（回避、軽減、移転、共有、受け入れ）
» 多様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 （例：サービス、ベンダー、インフラストラクチャ、ビジネス）

6.5 企業のリスク管理に対するクラウドの影響の理解

» ビジネス要件（例：サービスレベル契約（SLA）、マスターサービス契約（MSA）、作業明細書（SOW））
» ベンダー管理（例：ベンダー評価、ベンダーロックインリスク、ベンダー存続可能性、エスクロー）
» 契約管理（例：監査の権利、指標、定義、終了、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 マネジメント（例：国際規格化機構/国際電気規格会議（ISO/IEC） 27036）

追加の試験情報

補足参考資料

受験者は、CBKに関連するリソースを確認し、注意が必要な研究分野を特定することで、教育と経験を補うことが奨励されます。

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) 58035662
メール：isc2asia@isc2.org

ヨーロッパ、中東、アフリカ

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