CCSP®

Certified Cloud Security Professional

ISC2 Certification

認定試験要綱

施行日： 2026年8月1日

ISC2™

CCSPについて

ISC2では、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へのコンプライアンスに関する必要な知識、スキル、能力を確実に備えていることを証明するために、Certified Cloud Security Professional (CCSP) 資格認定証明書を開発しました。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、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。

CCSP認定試験要綱で取り上げられているトピックは、クラウドセキュリティ分野のあらゆる領域において、一貫した内容で構成されています 。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能力があります。

- 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

受験者は、情報テクノロジー（IT）において最低5年間のフルタイム累積実務経験を有していなければなりません。3年間はサイバーセキュリティ分野における経験、1年間は現行のCCSP認定試験要綱の6つのドメインのうち、最低1つのドメインにおける経験が必要です。コンピュータサイエンス、IT、または関連分野の高等学位（学士号または修士号）を取得している場合は、必要な経験を1年まで満たすことができます。CSAのCCSK認定資格の取得は、1年間の経験に代替可能です。免除されるのは、1年間の経験のみです。有効なCISSP認定資格を取得することで、CCSPの全経験要件を満たせます。また、パートタイム勤務や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。

CCSPに必要な経験を持たない受験者は、CCSP試験に合格することで、ISC2準会員（アソシエイト）になることができます。ISC2準会員は、その後5年間の必要な実務経験を6年かけて積んでいきます。CCSPの経験要件、パートタイム勤務やインターンシップ期間の計上方法については、www.isc2.org/Certifications/CCSP/experience-requirementsをご覧ください。

認定

CCSPは、ANSI国家認定委員会（ANAB）ISO/IEC規格17024の厳格な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ジョブ・タスク分析（JTA）は、CCSPが定義した専門職に従事するセキュリティ専門家が遂行している業務を特定する、体系的かつ極めて重要なプロセスです。JTAの結果は、本試験の更新に活用されます。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するためのものです。

CCSP CAT試験情報

CCSP試験では、英語、簡体字中国語、ドイツ語、日本語の試験において、コンピュータ適応型テスト（CAT）を使用しています。CCSP CATについては、www.isc2.org/certifications/computerized-adaptive-testingをご覧ください。

試験時間	3時間
試験問題数	100 ～ 150
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、中国語、ドイツ語、日本語
試験会場	ピアソンVUEテストセンター

CCSP CAT試験出題比重

ドメイン	比重の平均
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	16%
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： 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（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、規制当局など）
» クラウドコンピューティングの主要な特性（オンデマンドセルフサービス、広範なネットワークアクセス、マルチテナンシー、迅速な弾力性と拡張性、リソースプーリング、測定サービスなど）
» 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関する説明

» クラウドコンピューティングでの作業
» クラウドサービス機能（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など）
» クラウドサービスのカテゴリー（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）
» クラウドの展開モデル（パブリック、プライベート、ハイブリッド、コミュニティ、マルチクラウドなど）
» クラウド共有の考慮事項（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、アウトソーシングなど）
» 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）、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など）

1.3 クラウドコンピューティング関連のセキュリティ概念に対する理解

» 暗号技術と鍵管理
» IDとアクセス制御（ユーザーアクセス、特権アクセス、サービスアクセスなど）
» データおよびメディアのサニタイゼーション（上書き、暗号消去など）
» 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、アイソレーションなど）
» 一般的なクラウドの脅威
» セキュリティハイジーン（パッチング、ベースライニング、不変アーキテクチャ、ハードニングなど）

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）計画
» 事業インパクト分析（BIA）（費用対効果分析、投資利益率（ROI）など）
» 機能的セキュリティ要件（ポータビリティ、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ー（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）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（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、セキュア・バイ・デザインなど）
» DevOpsセキュリティ

1.5 クラウドサービスプロバイダー（CSP）に対する評価

» 基準に照らした検証
» システム/サブシステム製品の認証（コモンクライテリア（CC）、連邦情報処理標準（FIPS）140-2など）

1.6 人工知能（AI）/機械学習（ML）に対する理解

» クラウド脅威の検出と分析
» データソースの検証と確認
» セキュリティ・オーケストレーション、自動化、レスポンス（SOAR）
» 倫理的懸念
» 規制要件

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関する説明

» クラウドデータに関するライフサイクルフェーズ
» 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（長期、一時、ローストレージ、オブジェクトストレージ、ボリュームストレージなど）
» 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

» 暗号化と鍵の管理
» ハッシュ化（データの完全性、否認防止など）
» データの難読化（マスキング、匿名化など）
» トークン化
» データ損失防止（DLP）
» 鍵、機密、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
» 非構造化データ
» 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
» データのラベリングとタグ付け

2.6 情報権限管理（IRM）の設計と実装

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

2.7 データ保持、削除、アーカイブポリシーの計画と実装

- 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（許可されたアクセス、削除防止など）

2.8 データイベントの監査可能性、追跡可能性、説明責任の設計と実装

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

2.9 人工知能（AI）および機械学習（ML）のデータ保護に対する理解

- データセットとモデルのプライバシー
- データセットとモデルのセキュリティ（検証、妥当性確認など）

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のコンポーネントに対する理解

- 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（テナント分割、アクセス制御など）
- 物理的設計（場所、購入、構築など）
- 環境設計（暖房、換気、および空調（HVAC）、マルチベンダー経路接続性など）
- 設計の回復力（電力、暖房、換気、および空調（HVAC）、接続性など）

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（識別、分析など）
- 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（オンプレミスなど）
- 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（ログ収集、相関関係、パケットキャプチャなど）

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
- ビジネス要件（復旧時間目標（RTO）、復旧点目標（RPO）、復旧サービスレベルなど）
- 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（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）Top10、アプリケーションセキュリティ検証規格（ASVS）、アプリケーションプログラミングインターフェース（API）Top10、大規模言語モデルアプリケーションTop10、SANS Top25など）

4.2 安全なソフトウェア開発ライフサイクル（SDLC）プロセスに関する説明

» ビジネス要件

» フェーズと方法論（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など）

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（共有技術の問題、クラウド・サービス・プロバイダー（CSP）の内部脅威、可視性と制御の欠如、法律や管轄権の問題など）

» 脅威モデル（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）など）

» 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（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規格（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）など）

» ソフトウェア構成管理（CM）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（継続的インテグレーションと継続的デリバリー（CI/CD）プロセスなど）

» セキュリティテスト方法論（ブラックボックス、ホワイトボックス、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）、静的なアプリケーションのセキュリティテスト（SAST）、動的なアプリケーションのセキュリティテスト（DAST）など）

» 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）の保護
» サプライチェーン管理（ベンダー評価、完全性、真正性、ライセンスなど）
» サードパーティ製ソフトウェアの管理
» 検証済み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に対する理解と適用

» 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フェース（API）ゲートウェイなど）
» 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（マイクロサービス、コンテナ、ドッカー、Kubernetesなど）

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ID
» IDプロバイダー（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、鍵、認証の管理

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（ハードウェアセキュリティモジュール（HSM）、信頼性の高いプラットフォームモジュール（TPM）など）

» セキュア・バイ・デフォルト

» 管理プレーン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）、ハイパーバイザータイプ1および2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の運用と維持

» ローカルおよび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)、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、シングルサインオン（SSO）など）

» 安全なネットワーク構成（仮想ローカルエリアネットワーク（VLAN)、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）など）

» ネットワークセキュリティ制御（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、セグメンテーションなど）

» ベースライン、モニタリング、修復の適用によるオペレーティングシステム（OS）の強化（Windows、Linux、VMwareなど）

» パッチ管理

» クラスタ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、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）など）

» ゲストオペレーティングシステム（OS）の可用性

» パフォーマンスとキャパシティのモニタリング（ネットワーク、コンピュート、ストレージ、レスポンスタイムなど）

» ハードウェア監視（ディスク、中央処理装置（CPU)、ファン速度、温度など）

» ホストと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（スケジューリング、オーケストレーション、メンテナンスなど）

5.3 運用管理および標準の導入（米国国立標準技術研究所（NIST）、国際標準化機構（ISO）、医療保険の携行性と責任に関する法律（HIPPA）、情報および関連テクノロジーのためのコントロール目標（COBIT）、インターネットセキュリティセンター（CIS）コントロール、スポンサー組織委員会（COSO）、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など）

- 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
- インシデント管理
- 問題管理
- リリース管理
- 配備管理
- 構成管理（CM）
- 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 セキュリティ業務の管理

- 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（ファイアウォール、侵入検知システム（IDS）、侵入防御システム（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）など）
- ログのキャプチャと分析（セキュリティ情報およびイベント管理（SIEM）、ログ管理、脅威インテリジェンスなど）
- インシデント対応（IR）
- 脆弱性評価
- 侵入テスト

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化

- 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（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）ガイダンスなど）
- フォレンジック要件（クラウドセキュリティアライアンス（CSA）、国際規格化機構/国際電気規格会議（ISO/IEC）27037:2012/27041:2015/27042:2015/27043:2015など）

6.2 プライバシー要件に対する理解

- 契約上の個人データおよび規制された個人データの違い（保護された健康情報（PHI）、個人情報（PII）など）
- 個人データに関連する各国固有の法律（家族の教育権利とプライバシー法（FERPA）、個人情報保護及び電子文書法（PIPEDA）、一般データ保護規則（GDPR）、医療保険の携行性と説明責任に関する法律（HIPPA）、デジタル個人データ保護法など）
- 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（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）など）
- 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に対する理解

» 内部および外部監査管理
» 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（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）など）
» 監査範囲に関する声明の制限（認証業務の基準に関する声明（SSAE）、保証契約に関する国際規格（ISAE）など）
» ギャップ分析（コントロール分析、ベースライン・リスク、コントロールの自己評価など）
» 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制御システム
» 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識別と関与
» 高度に規制された業界向けの特殊なコンプライアンス要件（北米電気信頼性公社/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）など）
» 分散型情報テクノロジー（IT）モデルの影響（多様な地理的位置や法的管轄区域の横断など）

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の評価（コントロール、方法論、ポリシー、リスクプロファイル、リスクアペタイトなど）
» データの役割の違い（所有者、管理者、カストディアン、処理者、スチュワードなど）
» 規制の透明性要件（違反通知、サーベンス・オクスリー法（SOX法）、一般データ保護規則（GDPR）など）
» リスク処理（回避、軽減、移転、共有、受け入れなど）
» 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（サービス、ベンダー、インフラストラクチャ、ビジネスなど）

6.5 アウトソーシングとクラウドの契約設計に対する理解

» ビジネス要件（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）など）
» ベンダー管理（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、エスクローなど）
» 契約管理（監査権、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、データ所有権、セキュリティ要件など）
» サプライチェーン管理（国際規格化機構/国際電気規格会議（ISO/IEC）27036など）

追加の試験情報

補足参考資料

受験者は、CCSP 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奨励されます。

補足参考資料の全リストについては、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、受験者に対し、試験の登録前に試験のポリシーと手続きを確認することを推奨しています。この重要な情報の包括的な詳細については、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先

各地域の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
Eメール：membersupport@isc2.org

アジア太平洋

電話: +(852) 5803-5662
Eメール：isc2asia@isc2.org

ヨーロッパ、中東、アフリカ

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