CCSP®

# Certified Cloud Security Professional

An (ISC)² Certification

# 認定試験の概要

発効日：2022年8月1日

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

# CCSPについて

(ISC)²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、統制、および規制フレームワークへの準拠に必要な知識、スキル、能力を確実に身に付けられるように、CCSP（Certified Cloud Security Professional）資格を開発しました。CCSPは、情報セキュリティの専門性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するものです。この専門的な能力は、世界的に認められている知識体系と照らし合わせて測定されます。

CCSP Common Body of Knowledge（CBK）は、それに含まれるトピックにより、クラウドセキュリティのすべての分野に対応しています。資格取得者は、次の6つの領域に関する能力を有すると評価されます。

- 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、およびインフラストラクチャのセキュリティ
- 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
- 法律、リスク、およびコンプライアンス

## 必要な経験

受験者は、情報技術分野において最低5年の（報酬有り）累積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つの領域の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つの領域のうち、1つ以上の領域での1年間の経験に置き換えることができます。(ISC)² CCSPの資格取得者は、CCSP実務要件が免除されます。

CCSPになるために必要な経験を満たしていない受験者は、CCSP試験に合格後、(ISC)² 準会員になることができます。(ISC)² 準会員の期間は6年間です。その間に必要な5年間の業務経験を満たすようにしてください。CCSPの経験要件とアルバイト・インターンの扱いの詳細については、www.isc2.org/Certifications/CCSP/experience-requirementsをご覧ください。

## 認証

CCSPは、ANSI/ISO/IEC規格17024の厳格な要求事項に適合した認証資格です。

## ジョブタスク分析（JTA）

(ISC)²は、会員に対してCCSPとの関連性を維持する義務があります。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が行うタスクを決定するための系統的で重要なプロセスです。JTAの結果は、試験を更新するために使用されます。受験者は、このプロセスにより、クラウド技術における今日の実践的な情報セキュリティ専門家の役割と責任に関連するテーマ領域について試験を受けることができます。

# CCSP試験情報

| | |
|---|---|
| 試験時間 | 4時間 |
| 問題数 | 150問 |
| 問題形式 | 多肢選択 |
| 合格基準 | 1000点中700点 |
| 対応言語 | 英語、日本語、中国語、韓国語、ドイツ語、スペイン語 |
| 試験会場 | ピアソンVUEテストセンター |

# CCSP試験の配点

| 領域 | 出題比率 |
|---|---|
| 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 | 20% |
| 3. クラウドプラットフォーム、および<br>インフラストラクチャのセキュリティ | 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. 法律、リスク、およびコンプライアンス | 13% |
| 合計: | 100% |

# 領域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徴（例：オンデマンドセルフサービス、幅広いネットワークアクセス、マルチテナンシー、迅速な拡張性とスケーラビリティ、リソースプーリング、測定されたサービス）

» 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ついて説明する

» クラウドコンピューティングアクティビティ

» 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）

» クラウドサービスカテゴリ（例：SaaS（サービスとしてのソフトウェア）、IaaS（サービスとしてのインフラストラクチャ）、PaaS（サービスとしてのプラットフォーム）

» クラウド展開モデル（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）

» クラウド共通の考慮事項（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、レジリエンス、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（例：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）

## 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

» 暗号技術と鍵管理

» 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（例：ネットワークセキュリティグループ、トラフィックの検査、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

» セキュリティ衛生（例：パッチ適用、ベースライン）

## 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

» クラウドのセキュアデータライフサイクル

» クラウドベースの事業継続（BC）計画および災害復旧（DR）計画

» 事業影響分析（BIA）（例：費用便益分析、投資利益率（ROI））

» 機能的なセキュリティ要件（例：移植性、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：SaaS（サービスとしてのソフトウェア）、IaaS（サービスとしてのインフラストラクチャ）、PaaS（サービスとしてのプラットフォーム））のセキュリティに関する考慮事項と責任

» クラウドデザインパターン（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）のエンタープライズアーキテクチャ）

» DevOpsセキュリティ

## 1.5 クラウドサービスプロバイダーを評価する

» 基準に対する検証（例：ISO/IEC（国際標準化機構/国際電気標準会議）27017、PCI DSS（ペイメントカード業界データセキュリティ基準））

» システム/サブシステム製品の認証（例：コモンクライテリア（CC）、米国連邦情報処理規格（FIPS）140-2）

# 領域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を説明する

» クラウドデータの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を設計および実装する

» ストレージの種類（例：長期ストレージ、一時ストレージ、RAW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技術と戦略を設計および適用する

» 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）
» 鍵、シークレット、および証明書の管理

## 2.4 データディスカバリを実装する

» 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 データ分類を計画および実装する

» 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 情報権限の管理（IRM）を設計および実装する

» 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：証明書の発行や失効）

## 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、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、ジオロケーション）
» データイベントのログ記録、ストレージ、分析
» 証拠保全および否認防止

# 領域3：
# クラウドプラットフォーム、および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
» 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（例：場所、購入か構築か）
» 環境設計（例：（暖房、換気、空調（HVAC）、マルチベンダーパス接続）
» レジリエンスのある設計

## 3.3 クラウドインフラストラクチャおよびプラットフォームに関連するリスクを分析する

» 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 セキュリティ制御の計画および実装

» 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（例：ログ収集、相関関係、パケットキャプチャ）

## 3.5 ビジネス継続性（BC）および災害復旧（DR）を計画する

» 事業継続（BC）/災害復旧（DR）戦略
» ビジネス要件（例：目標復旧時間（RTO）、目標復旧時点（RPO）、復旧サービスレベル（RSL））
» 計画の作成、実装、およびテスト

# 領域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（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）トップ10、SANSトップ25）

## 4.2 セキュアソフトウェア開発ライフサイクル（SDLC）プロセスを説明する

» ビジネス要件
» フェーズおよび方法論（例：設計、コーディング、テスト、保守、ウォーターフォールとアジャイル）

## 4.3 セキュアソフトウェア開発ライフサイクル（SDLC）を適用する

» クラウド特有のリスク
» 脅威モデリング（例：なりすまし、改ざん、否 認、情報漏洩、サービス拒否、および特権の昇 格（STRIDE）、被害、再現可能性、悪用可能性、影響を受けるユーザー、および発見可能性（DREAD）、アーキテクチャ、脅威、攻撃対象 領域、および軽減策（ATASM）、攻撃シミュレ ーションと脅威分析のプロセス（PASTA））
» 開発における一般的な脆弱性を回避する
» セキュアコーディング（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））
» 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および検証を適用する

» 機能テストと非機能テスト
» セキュリティテストの方法論（例：ブラックボックス、ホワイトボックス、静的、動的、ソフトウェア構成分析（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を使用する

» アプリケーションプログラミングインターフェイス（API）の保護
» サプライチェーンマネジメント（例：ベンダー評価）
» サードパーティのソフトウェア管理（例：ライセンス供与）
» 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

» 補完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）、データベースアクティビティ監視（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イス（API）ゲートウェイ）
» 暗号技術
» 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（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）ソリューションを設計する

» 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）
» シークレット管理

# 領域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構築および実装する

» 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）とトラステッド・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&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を運用および保守する

» 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）、安全な端末アクセス、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（VLAN）、転送層セキュリティ（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セキュリティ拡張機能（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（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）
» ベースラインの適用、監視、修復によるオペレーティングシステム（OS）の強化（例：Windows、Linux、VMware）
» パッチ管理
» IaC（コードとしてのインフラストラクチャ）戦略
» クラスター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（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（HA））
» 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：スケジューリング、オーケストレーション、メンテナンス）

## 5.3 運用管理と標準を実装する（例：情報技術インフラストラクチャライブラリ（ITIL）、ISO/IEC（国際標準化機構/国際電気標準会議）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
- インシデント管理
- 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
- キャパシティ管理

## 5.4 デジタルフォレンジックをサポートする

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

## 5.5 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
- 顧客
- パートナー
- 規制当局
- その他の利害関係者

## 5.6 セキュリティオペレーションを管理する

- 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知的監視（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）など）
- ログのキャプチャと分析（例：セキュリティ情報とイベント管理（SIEM）、ログ管理）
- インシデント管理
- 脆弱性の評価

# 領域6：
# 法律、リスク、およびコンプライアンス

## 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：ISO/IEC（国際標準化機構/国際電気標準会議）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）、個人を識別することができる情報（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）、個人情報（PII））
» データプライバシーの司法管轄の違い
» 標準のプライバシー要件（例：ISO/IEC（国際標準化機構/国際電気標準会議）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））
» プライバシー影響評価（PIA）

## 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統制
» 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：認証業務の基準に関する声明（SSAE）、サービス組織統制（SOC）、保証契約に関する国際規格（ISAE））
» 監査範囲ステートメントの制限（例：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））
» ギャップ分析（例：統制分析、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制御システム
» 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：北米電力信頼度協議会の重要インフラ保護基準（NERC/CIP）、医療保険の相互運用性と説明責任に関する法律（HIPAA）、経済的および臨床的健全性のための医療情報技術（HITECH）に関する法律、支払いカード業界（PCI））
» 分散情報技術（IT）モデルの影響（例：地理的な場所の多様性や法的管轄区域の越境）

## 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：統制、方法論、ポリシー、リスクプロファイル、リスク選好）
» データ所有者/コントローラーとデータカストディアン/処理者の違い
» 規制の透明性要件（例：侵害通知、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（つまり、回避、軽減、移転、共有、受容）
» 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（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 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（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、ベンダーの実行可能性、エスクロー）
» 契約管理（例：監査する権利、測定基準、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）
» サプライチェーン管理（例：ISO/IEC（国際標準化機構/国際電気標準会議）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ご確認ください。

## 試験ポリシーと手続き

(ISC)²は、受験申し込みの前にCCSP受験者が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。www.isc2.org/Register-for-Examにアクセスし、試験情報をご確認ください。

## 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）までお問い合わせください。

## お問い合わせ先

(ISC)² アメリカ大陸
Tel：+1-727-785-0189
Email：info@isc2.org

(ISC)² アジア太平洋
Tel：+852-5803-5662
Email：isc2asia@isc2.org

(ISC)² ヨーロッパ・中東・アフリカ
Tel：+44 (0)203-960-7800
Email：info-emea@isc2.org