CCSP ドメインガイドブック

CCSP®

Certified Cloud
Security Professional

ISC2 Certification

はじめに

情報セキュリティ実務担当者や専門家には幅広い知識とスキルが必要とされており、その知識とスキルを有していることがセキュリティ実務担当者や専門家として認められる条件となっています。その一つの基準が、ISC2 の CBK (Common Body of Knowledge：共通知識分野)です。CBK は、それを理解していることを証明する資格である CCSP と共に、多くの国や企業、組織で認められたグローバルな内容として注目を浴びています。

本書では、CCSP 認定保持者が知っておくべき 6 ドメインについて紹介します。

ISC2 とは

ISC2(International Information Systems Security Certification Consortium：アイエスシー・スクエア)は、安全で安心できるサイバーセキュリティの世界を実現することを目的とした国際的な非営利団体です。高い評価を得ているCISSP(Certified Information Systems Security Professional)を始めとした各種資格を提供することにより、セキュリティに対してISC2は網羅的、そして計画的にアプローチしています。サイバー・情報・ソフトウェア・インフラストラクチャセキュリティの専門家から成り立つ16万人を超える資格保持者は、その資格によって他との差別化を図るとともに、業界の発展に貢献しています。

ISC2は、情報セキュリティの共通言語となるCBKを策定し、情報セキュリティ人材評価におけるゴールドスタンダードとなる認証制度を開発、提供しています。あわせて、世界中の情報セキュリティ専門家を教育、認定することによって、CBKをグローバルでより良いものとし続けています。

CCSP とは

CCSP(Certified Cloud Security Professional)は、ISC2 が認定を行うベンダーフリー・カントリーフリーのクラウドセキュリティ資格です。CCSP は、クラウドセキュリティと重要な資産の保護について理解していることを証明したいと考えている、IT および情報セキュリティのリーダーに最適です。クラウド上のデータ、アプリケーション、インフラストラクチャを設計、管理、セキュリティを確保する高度な技術的スキルと知識を持っていることを、CCSP が証明します。

資格取得のためには業務経験が必要です。試験合格後の認定登録手続きで業務経験を明記した職務経歴書とエンドースメント(推薦状)を提出し、それを証明する必要があります。認定期間は 3 年間となっており、3 年毎の認定継続要件をパスすることが必要です。

ANSI (米国規格協会)より、ISO/IEC 17024 の認証を受けた厳正な資格開発、運用、運営、維持に加え、米国国防総省のキャリアパスにおいて取得が義務付けられている資格の一つにも認定されており、情報セキュリティ &IT 実務者がグローバルの共通言語と知識を保有している事を証明できる資格になっています。

CBK とは

CBK は、ISC2 CBK 委員会が、各種認定試験の作成に先駆け、情報セキュリティ実務担当者及び専門家が理解すべき知識を国際規模で収集し、分野(ドメイン)別に体系的にまとめたものです。

情報セキュリティの共通言語である CBK をベースとすることで、CCSP をはじめとするクラウドセキュリティ専門家は、地域や専門分野を問わず、円滑なコミュニケーションが可能となります。CBK は毎年、世界各国の多数のセキュリティのプロフェッショナルに定期的なヒアリング調査を行い、「最新の知識」として更新、維持しています。その中で CCSP に必要とされるものをまとめたのが CCSP CBK 6 ドメインで

あり、CCSP 認定試験の試験範囲として活用されています。

CCSP の CBK は、2022 年８月にコンテンツを更新し、新たな知識が追加されました。

目次

CCSP CBK の６ドメイン

CCSP CBK は、以下の６ドメインから構成されています。

1. クラウドの概念、アーキテクチャ、設計
2. クラウドデータセキュリティ
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
4. クラウドアプリケーションセキュリティ
5. クラウドセキュリティオペレーション
6. クラウドガバナンス-法務、リスク、コンプライアンス

CCSP は、クラウドサービスを安全に利用するために必要となる知識を体系化したものです。クラウドサービスのセキュリティを理解するには、クラウドアーキテクチャ、IaaS/PaaS/SaaS というサービスモデル、データの保存場所などの法律・規制要件、安全なアプリケーション設計・配備など、様々な知識を必要とします。また、それを実践していくには、様々な状況下におけるベストプラクティスを理解する必要があります。

CCSP の６ドメインは、クラウドサービスの専門家として、まずクラウドそのものを定義することから始めます。そして、クラウドセキュリティとして必要となる幅広い知識を４つのドメイン（ドメイン 2～ドメイン 5）で学んでいきます。その上で、運用におけるクラウドセキュリティの考え方を理解します。

CCSP の６ドメインを通して、クラウドセキュリティを体系的に理解すると同時に、実務に役立つ知識として身に着けていきます。

1．クラウドの概念、アーキテクチャ、設計

「クラウドの概念、アーキテクチャ、設計」ドメインでは、クラウドコンピューティングの定義および関連する概念について説明します。クラウドセキュリティを考える前に、そもそものクラウドコンピューティングそのものを定義します。日々使っているクラウドという用語に対して、標準の定義に基づいてクラウドコンピューティングを理解します。

クラウドコンピューティングの定義における主な要素は、クラウドの特徴、一般的なアーキテクチャの要素、役割、および、配備モデルになります。また、クラウドの例として参照アーキテクチャを理解することで、クラウドとは何か、どのようなことができるのか、また、クラウドの制限は何かについて理解します。

また、本ドメインでは、クラウドコンピューティングの考慮事項として、クラウドの経済性、クラウドサービスプロバイダーの評価方法、責任共有モデルに基づくクラウドセキュリティの考え方の概要について理解します。

ドメインの主題となるキーワードと関連する要素

1.1 クラウドコンピューティングの概念の理解

- NIST 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特性
- クラウドの基盤となるサービスおよびデータセンターの構造

1.2 クラウドリファレンスアーキテクチャ

- ISO/IEC17789 クラウドコンピューティング参照アーキテクチャ
  - ユーザビュー、機能ビュー、実装ビュー、配備ビュー
  - クラウドサービスが提供する機能
  - クラウドサービスカテゴリー
- NIST クラウドコンピューティング参照アーキテクチャ
  - NIST クラウド参照モデル
  - アクター、クラウドサービスモデル、クラウド配備モデル
- ISO/IEC17789 と NIST の参照モデルの比較
- クラウドコンピューティングの責任共有モデルにおける考慮事項
- クラウド関連技術の概要
  - 機械学習
  - 人工知能
  - ブロックチェーン
  - IoT
- クラウドの経済性
  - プライベートクラウド経済性
  - パブリッククラウドの経済性
  - クラウドコンピューティングの ROI,KPI

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概念

- クラウドに適用するセキュリティの 3 原則
- CISO の責務
- リスク管理フレームワーク
- ガバナンス・リスク・コンプライアンス（GRC）

1.4 セキュアなクラウドコンピューティングの設計原則

- 責任共有モデルの理解
- サービスモデル（IaaS, PaaS, SaaS）ごとのセキュリティの考慮事項

1.5 クラウドサービスプロバイダーの評価

- クラウドサービスプロバイダーとの契約文書
  - クラウドサービス契約書
  - 利用規定
  - サービスレベル合意書

2. クラウドデータセキュリティ

データセキュリティは、クラウドセキュリティの中核となる要素です。「クラウドデータセキュリティ」ドメインでは、クラウドデータセキュリティの概念として、Cloud Security Alliance (CSA)のセキュリティガイダンスで説明されているデータセキュリティライフサイクルを使用し、データセキュリティライフサイクルの各フェーズに関連する管理策をマッピングするとともに、クラウドの特徴であるデータの移動性、多様なアクセス方法にどのように対応するかを説明します。また、クラウドデータセキュリティの基本として、クラウドにおけるデータストレージの概念、クラウドにおける暗号化と鍵管理の考え方、また、クラウドデータセキュリティを支える様々なツールとして、データディスカバリ、DLP、難読化/匿名化技術、IRMなどについて説明します。さらに、クラウドデータセキュリティ戦略として必要となる、データの保持/削除/アーカイブに関するポリシー、監査について説明します。

ドメインの主題となるキーワードと関連する要素

2.1 クラウドデータセキュリティの概念

- データセキュリティライフサイクルの各フェーズの管理策
- クラウド環境におけるデータの移動性と様々なアクセス方法
- データアクセス管理

2.2 クラウドデータストレージアーキテクチャ

- IaaS のストレージタイプ
  - オブジェクトストレージ
  - ボリュームストレージ
- PaaS のストレージタイプ
  - データベース
  - Big data as a Service
  - アプリケーション
- SaaS のストレージタイプ
  - SaaS アプリケーションの情報保存
  - コンテンツ/ファイルストレージ
  - CDN
- クラウド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および戦略

- マスキング、難読化、匿名化、トークン化の特徴と違い
- データ損失防止(DLP)
  - DLP アーキテクチャのコンポーネント
  - DLP アーキテクチャのトポロジー

2.4 暗号

- 暗号化技術
  - 対象暗号化
  - 非対称暗号化
  - ハッシュ関数
  - PKI
- クラウド環境での暗号化の利用方法
  - 移動中のデータ（data in motion: DIM）
  - 保存中のデータ（data at rest: DAR）
  - 使用中のデータ（data in use: DIU）
- クラウドデータ暗号化の課題
- クラウドデータ暗号化のアーキテクチャとオプション
  - 暗号化エンジン
  - 暗号化鍵
  - データ
- IaaS/PaaS/PaaS におけるデータ暗号化
  - インスタンスベースの暗号化
  - ファイルレベルの暗号化
  - アプリケーションレベルの暗号化
  - データベースの暗号化
- 暗号化鍵の管理、鍵管理オプション、鍵管理に関する考慮事項

- 鍵管理に関する課題
- 鍵管理のオプション
- 鍵管理における考慮事項

- FIPS 140-2
  - FIPS 140-2 標準の目的
  - FIPS のレベル
- 新しい暗号化技術の理解
  - ビット分割
  - 準同型暗号
  - 量子コンピューティング
  - ニューラルネットワーク
- データ削除と媒体のサニタイジング
  - サニタイジングのオプション

2.5 データディスカバリと分類の技術

- データディスカバリのアプローチ手法
  - ビッグデータ
  - リアルタイム分析
  - アジャイル分析、アジャイルビジネスインテリジェンス
- データディスカバリの課題
  - データ品質
  - 分析方法の正確性
  - データの場所の特定、データへのアクセス
  - データの保全とメンテナンス
- データ分類と分類カテゴリー
  - 分類カテゴリー
  - 機微データの分類
  - プライバシーデータの分類カテゴリーと管理策

2.6 情報著作権管理の概要

- 情報著作権管理（IRM）の設計と実装
  - IRM、DRM
  - コンシューマ DRM、エンタープライズ DRM
  - DRM の目的
- クラウド環境における DRM の課題
  - DRM リソースアクセスポリシーのプロビジョニング
  - ローカル DRM エージェント
  - DRM に対応した reader ソフトウエア
  - DRM 互換性

2.7 クラウドデータの保持、削除、およびアーカイブに関するポリシー

- データ保持ポリシーとメカニズム
  - 保持期間
  - データ形式
  - データセキュリティ
  - データ検索手順
- データ保持ポリシーのコンポーネント
  - 法律、規制、標準の要件
  - データの分類
  - データ保持手順
  - 監視と保守
- データ削除ポリシー
  - 法規制
  - ビジネス要件と技術要件
- データアーカイブポリシー
  - データ暗号化手順
  - データ監視手順
  - 電子情報開示と粒度の高い検索
  - バックアップと災害復旧
  - データ形式とメディアオプション
  - データ復元手順

2.8 データイベントの監視機能、追跡機能、説明責任

- IaaS/PaaS/SaaS におけるデータセキュリティ関連のイベントソース
  - インフラストラクチャレベルのログ
  - OWASP のログ取得推奨事項
  - データアクセス要件
- データイベントロギングおよびイベント属性
  - OWASP Proactive Controls v3.0
- データイベントの保存と分析
  - 証拠保全
  - 監査ログの保護、保持、ライフサイクル管理
  - 安全な廃棄

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

「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」ドメインでは、クラウド利用者およびクラウドプロバイダとしての物理的環境、論理的環境、仮想環境に対するリスクと対応策について説明します。また、クラウド環境のリソースへのアクセスを管理するためのアイデンティティとアクセス管理、特に、クラウド環境におけるアイデンティティの特性である複数のクラウドへのアクセスを扱うためのフェデレーションについて説明します。さらに、クラウド環境における事業継続性および災害復旧戦略を説明するとともに、クラウドベースの事業継続性計画および災害普及計画の方法について説明します。

ドメインの主題となるキーワードと関連する要素

クラウドインフラストラクチャコンポーネントの理解

- ネットワーク機能とクラウドサービスの関係
  - NFV, SDN, SD-WAN
- コンピュート、ストレージとクラウドサービスの関係
  - コンピュートリソース
  - SAN, NAS, クラウドストレージ（オブジェクトストレージ、ボリュームストレージ）
  - ハイパーコンバージドインフラストラクチャ（HCI）
- 管理プレーンと仮想化機能
  - タイプ 1 ハイパーバイザー、タイプ 2 ハイパーバイザー
  - 管理コンソール
  - 管理プレーンの API

3.2 安全なクラウドデータセンターの設計

- データセンターの論理設計
  - 相互運用性
  - 移植容易性
- データセンターの物理設計
  - ISO/IEC 22237
  - データセンターの施設の要件と仕様
  - 保護クラス、可用性クラス
  - Uptime Institute のデータセンターサイト Infrastructure Tier Standard
  - 防火、火災の検知、消化
- データセンターの環境設計
  - 暖房、換気、エアコン（HVAC）

3.3 クラウドインフラストラクチャに関連するリスクの分析

- クラウド環境に対するリスクと対策
  - IaaS/SaaS の観点のリスク
  - 仮想化リスク
  - 対策方針としてのゼロトラストモデル、サイバーキルチェーン

3.4 物理的および論理的なクラウドインフラストラクチャ向けのコントロールセキュリティの設計及び計画

- ハードウエア固有のセキュリティ構成要件
  - TPM
  - 仮想化管理ツール
- 仮想ハードウエア固有のセキュリティ構成要素
  - VPC
  - セキュリティグループ
  - 管理プレーン
  - クラウドオーケストレーション

3.5 適切なアイデンティティ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 管理
  - SAML, OAuth, OpenID Connect
  - アイデンティティプロバイダ、リライングパーティー
  - SSO, RSO

3.6 災害復旧(DR)と事業継続性(BC)の計画

- 事業継続性と災害復旧戦略
  - ISO/DIS22301:2019 BCMS の構成要素とプロセス
  - BC/DR 戦略のリスク
  - ビジネス要件、MTPD, RTO, RPO
- クラウドベースの災害復旧および事業継続性計画
  - オンプレミスとクラウド
  - プライマリプロバイダ BCDR
  - 代替プロバイダーBCDR
- 復元と復旧
  - フェールオーバー
  - フェールバック
- 計画の作成、実施およびテスト
  - 計画の範囲
  - 計画の作成、リスクアセスメント
  - 計画の実施
  - テストのタイプ、カオスエンジニアリング

4. クラウドアプリケーションセキュリティ

「クラウドアプリケーションセキュリティ」ドメインでは、クラウドでのセキュアなアプリケーションの設計、開発、配備について説明します。クラウドセキュリティでは、ID アクセス管理、インフラセキュリティなどにフォーカスされるケースが多いですが、アプリケーションセキュリティも重要です。アプリケーションがセキュアでなければ、クラウドで実行しているすべてのプロセスがセキュアでは無くなります。本ドメインでは、ソフトウエア開発ライフサイクル(SDLC)を通して、クラウドでのアプリケーションをセキュアにするプロセスについて説明します。

ドメインの主題となるキーワードと関連する要素

4.1 アプリケーションセキュリティのトレーニングと認識

- クラウドベースのアプリケーションの潜在的な課題
  - フォークリフト、リフト＆シフト
  - Web サービスを使用するためのトレーニング
  - 暗号化依存の意識
  - マルチテナンシー
  - サードパーティ管理
- クラウド環境における一般的な脆弱性
  - OWASP Top10「The Top Ten Most Critical Web Application Security Risks」

4.2 セキュアなソフトウエア開発ライフサイクル(SDLC)プロセス

- SDLC の各フェーズと方法論
  - 定義、セキュリティ要件
  - デザイン、脅威モデリング
  - 開発、静的解析
  - テスト、動的テスト、回帰テスト、受入テスト
  - 配備/運用、監視、WAF
  - メンテナンス、更新
  - 廃棄、クリプトシュレッディング
- セキュアなクラウドアプリケーションの要件
  - ISO/IEC 27034-1
  - Microsoft　セキュリティ開発ライフサイクル
  - NIST SP800-64
- ソフトウエア開発モデル
  - ウオーターフォールモデル
  - 検証・妥当性確認モデル
  - プロトタイプモデル
  - 反復増分モデル
  - スパイラルモデル
  - アジャイル
  - DevOps/DevSecOps
  - CI/CD
  - エクストリーム・プログラミング

4.3 安全なソフトウエア開発ライフサイクル(SDLC)の適用

- 脅威モデル
  - STRIDE 脅威モデル
- ソフトウエアの構成管理とバージョン管理
  - Puppet
  - Chef
  - Ansible
  - Salt

4.4 クラウドソフトウエア保証および妥当性確認の適用

- アプリケーションセキュリティテスト手法
  - 機能テスト
  - ブラックボックステスト
  - ホワイトボックステスト
  - SAST
  - DAST
  - 脆弱性評価
  - ペネトレーションテスト
  - セキュアコードレビュー

- OWASP テスティングガイド

4.5 検証済みの安全なソフトウエアの使用

- アプリケーションプログラミングインターフェース
  - REST
  - SOAP
- サプライチェーン管理
  - サードパーティ製ソフトウエアの管理
  - 検証済みオープンソースソフトウエア

4.6 クラウドアプリケーションアーキテクチャの詳細

- クラウドアプリケーションアーキテクチャ
  - サンドボックス、アプリケーション仮想化、マイクロサービス、コンテナ、Infrastructure as Code(IaC)

5. クラウドセキュリティオペレーション

「クラウドセキュリティオペレーション」ドメインでは、クラウドセキュリティの運用を構成するツール、プロトコル等を説明します。また、クラウド利用者とクラウドプロバイダの間の共通の基盤に対して、誰が責任を持ち、誰がすべての関連する活動に対して説明責任を持つかを定義し、それを契約やSLAに規定していく方法について説明します。さらに、クラウドセキュリティの運用において必要とされる運用管理の標準、セキュリティ運用の管理として必要となるSOCの要件およびログ管理等の要件について説明します。

ドメインの主題となるキーワードと関連する要素

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運用と管理

- リモートアクセス管理用のツール、プロトコル
  - KVM, RDP, SSH, DHCP, DNS
- 安全なネットワーク構成と追加コンポーネント
  - VXLAN, VPN, TLS, IPSec
  - ファイアウォール、侵入検知/侵入防止システム
- ベースラインの適用による OS のセキュリティ強化
  - ベースラインの設定
  - ベースラインの取得
  - CIS コントロール、SCAP、STIG
- ホストクラスタリングの概念
  - ストレージクラスタ
  - 動的リソース共有
  - メンテナンスモードの考え方

5.2 運用上のコントロールと標準の実装

- IT サービスマネージメント
  - ISO/IEC 20000-1
  - ITIL v4

5.3 関係者とのコミュニケーション管理

- サプライチェーンベンダーのカテゴリー
- プロバイダーと利用者の責任の分担

5.4 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）
  - ISO/IEC 18788-2 セキュリティオペレーション管理システム（SOMS）のフロー
- セキュリティコントロールの監視
- パフォーマンス、容量、ハードウエアの監視
  - SNMP
  - クラウド監視ログの取得と分析
- ログ及びシステム情報収集の推進要因
  - ログ管理の推奨事項
  - ログ管理ツール、SIEM の特徴

6. クラウドガバナンス-法務、リスク、コンプライアンス

「クラウドガバナンス-法律、リスク、コンプライアンス」ドメインでは、ガバナンスの主要な要素であるポリシー、スタンダード、プロシージャを誰が行うのか、また、どのような役割を持つのかを包括的に確立することを目的とします。その際に、クラウドに適用する法律・規制を明確にする必要があります。また、コンプライアンス要件として、クラウドサービスプロバイダーとクラウドサービス利用者の双方が、責任共有モデルに基づいて役割を果たしていくことが必要となります。

本ドメインでは、クラウドサービスに影響を与える法的枠組み、クラウドに適用する司法ツールである電子情報開示（e-Discovery）、デジタルフォレンジックを理解するとともに、クラウドにおける法律/規制上重要になるプライバシーについて理解します。また、クラウドにおける監査として、監査プロセス、方法論、クラウドへの適応について理解します。

ドメインの主題となるキーワードと関連する要素

6.1 クラウド環境における法的要件と固有のリスクの明確化

- クラウド環境における法的枠組み
- クラウド環境における法的リスク

6.2 デジタルフォレンジックのサポート

- 電子情報開示とデジタルフォレンジック
- デジタル証拠

6.3 プライバシーの問題の理解

- データプライバシーの進化と歴史
- 一般データ保護規則(GDPR)、および、個人データに関連する国別の法律
- プライバシー要件に関する標準

6.4 クラウド環境の監査プロセス、方法論、必要となる適応の理解

- 内部監査、外部監査、監査要件、監査範囲等、監査プロセス
- クラウドに関する保証の課題と特定
  - フレームワーク： STAR, SOC, ISMS, NIST SP800-53, PCI DSS 等

6.5 エンタープライズリスクマネジメントに対するクラウドの影響の理解

- データコントローラとデータプロセッサの違い
- インシデント発生時の規制要件
- リスク管理フレームワーク
  - ISO31000, NIST サイバーセキュリティフレームワーク(CSF), NIST SP800-37 リスク管理フレームワーク, FedRAMP
- 定性的リスク評価、定量的リスク評価のためのマトリックス
- リスク対応方法
  - 修正、保持、回避、共有
- システム/サブシステム認定
  - コモンクライテリア

6.6 アウトソーシングとクラウド契約設計の理解

- ベンダー管理
- 契約管理
- 契約基準
  - クラウド契約の主要コンポーネント
- デューデリジェンス、デューケア
- サプライチェーン管理

確認問題

CCSP の問題は以下のように 4 択で出題されます。CBK の内容を理解する際の「気づき」として活用してください。

問題の正答は本書内には記載していません。CCSP に求められる判断力を知るために、考え方の一例として取り上げています。

1. あなたの会社はデータストレージをクラウドへ移行させることを決定しました。CSPのデータストレージ戦略についてレビューしたところ、あなたは会社が共有ストレージを利用していることを知りました。会社のデータを他のテナントから適切に保護するために最も良いソリューションは、次のうちどれでしょうか？

   A. 事前定義されたビジネスルールに基づくアクセス制御ルールの適用
   B. 会社のデータを別のストレージに保存することを求める
   C. 会社のデータが暗号化されていることを確認する
   D. CSPのアプリケーションを利用し、データをローカルに保存するハイブリッドクラウド戦略を活用する

2. 会社がクラウドへ移行させたい2つ目の業務プロセスは、人事システムです。その際にSaaS型クラウドサービスモデルを選択しました。SaaS型クラウドサービスモデルを利用する場合、会社のデータのセキュリティを確保するために最も効果的なツールは何でしょうか？

   A. 会社の全データが暗号化されていることを確認する
   B. 自社の監査権を確保する
   C. 会社のデータの存在が許可される地理的な制限を定義する
   D. CSPと会社の役割および責任を規定した契約書を作成する

3. 会社のリスク管理戦略の一環として、ビジネスプロセスをクラウドに移行する際、リスクを適切に対処できるようにする必要があります。次のうち、移行プロセスの際に考慮する必要がないものはどれでしょうか？

   A. そのプロセスが不正に操作された場合、ビジネスはどのような悪影響を受けでしょうか？
   B. クラウドに含まれる情報が公開されてしまった場合、ビジネスに影響を与えるでしょうか？
   C. そのプロセスをクラウドに移行することで、どのようなコストが発生するでしょうか？
   D. そのプロセスが使えなくなった場合、ビジネスにどのような影響があるのでしょうか？

4. 会社は利用したリソース以外には料金を支払いたくないと考えています。しかし、リソースの需要が急激

に増加する休日や高需要期にも対応できるようにしたいとも考えています。次のうち、どのコンセプトがこのビジネス要件を満たすでしょうか？

A. 負荷バランス
B. クラウドバースト
C. 高可用性
D. クアッドプロセッサー

5. クラウドバーストのビジネス要件に最も適合する導入モデルはどれでしょうか？

A. プライベートクラウド
B. コミュニティクラウド
C. ハイブリッドクラウド
D. パブリッククラウド

6. SaaS型サービスモデルでは、ユーザーはコンピューティング環境の技術的な制御をクラウドサービスプロバイダーに移管します。ユーザーが負う責任は次のうちどれしょうか？

A. アプリケーションの構成
B. データの遠隔地におけるバックアップ
C. オペレーティングシステムのパッチ適用
D. データ保護に関する責任と法的責任

7. さまざまなクラウド導入配備モデルについて検討した結果、会社は専用のクラウド導入配備モデルの購入は費用対効果が低いと判断しました。一方で、クラウド導入配備モデルを利用するすべての企業が既知の企業であり、同じPCI-DSS要件を遵守していることを確認したいと考えています。この要件に最も適合する導入配備モデルはどれでしょうか？

A. ハイブリッド
B. コミュニティ
C. プライベート
D. パブリック

8. あなたは、SaaSプロバイダーになることを望むスタートアップ企業に勤めています。あなたの会社は、資本支出コストを最小限に抑えながら、アプリケーションの利用を開発し、販売したいと考えています。この要件に最も適合するサービスモデルはどれでしょうか？

A. SaaS
B. IaaS
C. PaaS
D. オンプレミス

9. あなたの会社では、多くの金融顧客にサービスを提供するカスタムアプリケーションを利用しています。このアプリケーションは、プライベートデータセンター内に存在する会社のサーバーでホストされています。会社のサーバーすべてで、特定の構成とソフトウェアファイアウォールを実行しています。会社は両環境の構成設定が同じになるように、環境をできるだけ制御できるテスト環境を求めていますが、それと同時に、環境のセットアップにかかるコストと時間は最小限に抑えたいと考えています。このビジネス要件に最も適合するサービスモデルはどれでしょうか？

A. SaaS/プライベート
B. IaaS/パブリック
C. PaaS/ハイブリッド
D. IaaS/プライベート
E. SaaS/パブリック
F. PaaS/パブリック

10. あなたの会社は、ビジネスプロセスをクラウドに移行したいと考えています。そのビジネスプロセスと関連データには、厳しい規制要件が課せられています。そのため会社は、管理制御の所有権を保持し、データが特定の地理的位置に保管されていることを確認する必要があります。このビジネス要件に最も適合する配備モデルはどれでしょうか？

A. パブリック
B. プライベート
C. ハイブリッド
D. コミュニティ

CCSP 受験から認定までの流れと認定維持

CCSP 認定試験

申込み(実施機関)

認定試験は、Pearson VUE にて実施されます。試験の申込みや会場などに関する情報は、Pearson VUE Web サイトを参照してください。

https://www.pearsonvue.co.jp/Clients/ISC2.aspx

出題範囲

- CCSP CBK 6 ドメイン

問題数

- 150 問／4 択 Computer Based Testing(CBT)(日本語・英語併記)
  150 問中、50 問は調査のために入っており、採点対象とはなりません。

時間

- 4 時間(途中休憩可・途中退出可)
  - 試験開始前に 30 分程度の試験説明があります。この説明を受けないで受験をすることはできません。
  - 試験監督の監視のもとでの休憩となります。
  - 途中退出後は、試験会場に戻ることはできません。

受験料

- 599 米ドル

必須持ち物(忘れると受験不可)：

写真・署名付公的身分証明書と署名付身分証明書(計 2 点)

合格点

- 1000 点満点中 700 点で合格
  (スケールドスコアなので、各問題の配点は同じとは限りません)
- 受験後に会場で合否がわかります(非公式)。
  6 週間～8 週間後に公式な結果が電子メールで通知されます。
  不合格の場合には、6 ドメインについて、最もスコアがよかったドメインから最もスコアが悪かったドメインまでの 1～6 の順位が記載されます。

CCSP 試験ドメインの各ドメイン出題比率

ドメイン	出題比率
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. クラウドガバナンス-法務、リスク、コンプライアンス	13%
	100%

CCSP 認定要件

CCSP に認定されるには、下記要件をすべて満たすことが必要です。

- CCSP 認定試験での合格(1000 点中 700 点以上で合格)
- IT に関する業務に従事した経験が 5 年以上あること
- 上記 5 年の内、 情報セキュリティに関する業務が 3 年以上、また CCSP の 6 ドメインのいずれかに関する業務が 1 年以上(もしくは CCSK 合格) あること
  ※ CISSP 資格保持者は、上記経験年数に関係なく、CCSP 認定試験に合格することで資格が認定されます。
- 実務経験が事実であることの証明及び倫理規約に合意すること
- ISC2 認定資格保持者(CISSP, SSCP, CCSP, CSSLP)からの推薦
- 無作為に行われる業務経験に関する監査に合格すること
- 犯罪に関連した履歴に関する 4 つの質問事項に正しく答えること(試験登録時の申込書にて)

認定登録手続

- 推薦状(エンドースメント)と職務経歴書(英語)を米国 ISC2 本部に送付
  - 推薦状書式は合格通知の電子メールに記載の URL からダウンロードして記入します。ISC2 認定資格保持者(CISSP, SSCP, CCSP, CSSLP)からの推薦の署名をもらう必要があります。
  - 職務経歴書は、業務経験年数を明確に記載し、また経験年数に含む業務が CCSP CBK に関連した業務であることを明確に記載する必要があります。
- 手続き完了後、米国 ISC2 本部から認定証パッケージが希望した住所に郵送されます。
  - パッケージに入っているもの
    - 認定証
    - CCSP ラペルピン購入クーポン

CCSP 認定継続要件

- ISC2 倫理規約に従い行動する
- 年会費の支払(125 米ドル／年・複数の資格を保有している場合でも同額)
- 継続教育単位(CPE クレジット)を 3 年間で 90 ポイント取得する

その他

記載している情報は 2022 年 9 月現在の内容です。最新情報は ISC2 ホームページにてご覧ください。

ISC2 日本語 Web サイト	https://japan.isc2.org/
CCSP 認定試験案内	https://japan.isc2.org/examination_ccsp.html
公式 CCSP CBK トレーニング案内	https://japan.isc2.org/ccsp_training.html

本書の取り扱いについて

CCSP ドメインガイドブック

2022 年 12 月 1 日 第 1 版発行

お問い合わせ先

ISC2

E-mail: infoisc2-j@isc2.org

TEL: 03-5322-2837

URL: https://japan.isc2.org/