CC SM

Certified in Cybersecurity

ISC2 Certification

認定資格の試験の概要

実施日：2022年8月29日

ISC2

サイバーセキュリティ認定資格の認定について

サイバーセキュリティ認定資格（CC）に認定されることで、エントリーレベルまたはジュニアレベルのサイバーセキュリティの職務に求められる基礎知識、スキル、能力を備えていることを雇用主に証明することができます。また、セキュリティに関する基本的なベストプラクティス、ポリシー、手順についての理解、加えて、学習を継続し、職務上の知識を伸ばす意欲と能力を示すことができます。

この試験がカバーしているドメインは5つあります。

- セキュリティ原則
- 事業継続性（BC）、災害復旧（DR）およびインシデント レスポンスの概念
- アクセス制御の概念
- ネットワークセキュリティ
- セキュリティ運用

求められる経験について

受験資格は特にありません。 受験者に基本的な情報テクノロジー（IT）の知識があることが推奨されます。 サイバーセキュリティに関する実務経験や正式な終了証書 学位は必要ありません。受験者のキャリアにおける次のステップは、ISC2のエキスパートレベルの認定資格取得で、この資格を取得するには現場での経験が必要です。

作業タスク分析(JTA)

ISC2は、そのメンバーシップに対してCC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、CC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、情報セキュリティ専門家の今日の実務における役割と責任に関連する項目や領域に関して、受験者が確実に審査されるようにします。

CC試験情報

試験時間	2時間
出題数	100
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、日本語、ドイツ語
受験会場	ピアソンVUEテストセンター

CC試験内容の比重

ドメイン	比重の平均
1. セキュリティ原則	26%
2.事業継続性（BC）、災害復旧（DR）およびインシデント レスポンスの概念	10%
3.アクセス制御の概念	22%
4.ネットワークセキュリティ	24%
5.セキュリティ運用	18%
合計	**100%**

ドメイン1：セキュリティ原則

1.1 情報保証におけるセキュリティ概念の理解

» 機密保持
» 整合性
» 可用性
» 認証（例：認証方法、多要素認証（MFA））
» 否認防止
» プライバシー

1.2 リスク管理プロセスの理解

» リスク管理（例：リスクの優先順位、リスク許容度）
» リスクの識別、評価、処理

1.3 セキュリティコントロールの理解

» 技術的コントロール
» 管理的コントロール
» 物理的コントロール

1.4 (ISC)²倫理規定の理解

» 職業上の行動規範

1.5 ガバナンスプロセスの理解

» ポリシー
» 手順
» 規格
» 規制と法律

ドメイン2：
事業継続性 (BC)、災害復旧(DR)およびインシデント レスポンスの概念

2.1 事業継続性(BC)の理解

» 目的
» 重要性
» 構成内容

2.2 災害復旧(DR)の理解

» 目的
» 重要性
» 構成内容

2.3 インシデント レスポンスの理解

» 目的
» 重要性
» 構成内容

ドメイン3：
アクセス制御の概念

3.1 物理的なアクセス制御の理解

» 物理的セキュリティコントロール（例：バッジシステム、ゲートエントリー、環境設計）
» 監視（例：警備員、閉鎖型テレビ（CCTV）、警報システム、ログ）
» 権限のある担当者と権限のない担当者

3.2 論理的なアクセス制御の理解

» 最小特権の原則
» 業務の分掌
» 裁量アクセス制御（DAC）
» 強制アクセス制御（MAC）
» ロールベースアクセス制御（RBAC）

ドメイン4：
ネットワークセキュリティ

4.1 コンピュータネットワークの理解

» ネットワーク（例：オープンシステム間相互接続（OSI）モデル、転送制御プロトコル/インターネットプロトコル（TCP/IP）モデル、インターネットプロトコル バージョン4（IPv4）、インターネットプロトコル バージョン6（IPv6）、WiFi）

» ポート

» アプリケーション

4.2 ネットワークの脅威と攻撃の理解

» 脅威の種類（例：分散型サービス拒否（DDoS）、ウイルス、ワーム、トロイの木馬、中間者攻撃（MITM）、サイドチャネル）

» 識別（例：侵入検知システム（IDS）、ホストベース侵入検知システム（HIDS）、ネットワーク侵入検知システム（NIDS））

» 防止（例：ウイルス対策、スキャン、ファイアウォール、侵入防止システム（IPS））

4.3 ネットワーク セキュリティ インフラストラクチャの理解

» オンプレミス（例：電力、データセンター/クローゼット、暖房、換気、および空調（HVAC）、環境、消火、冗長性、諒解書（MOU）/合意覚書（MOA））

» 設計（例：ネットワーク セグメンテーション（非武装地帯（DMZ）、仮想ローカルエリアネットワーク（LAN）（VLAN）、仮想プライベートネットワーク（VPN）、マイクロ セグメンテーション）、多層防御、ネットワークアクセス制御（NAC）（組み込みシステム、インターネット セグメンテーション、モノのインターネット（IoT）（IoT））

» クラウド（例：サービスレベル契約（SLA）、管理サービスプロバイダー（MSP）、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）、ハイブリッド）

ドメイン5：
セキュリティ運用

5.1 データセキュリティの理解

» 暗号化（例：対称、非対称、ハッシュ）
» データ処理（例：破棄、保存、分類、ラベル付け）
» セキュリティイベントのログ記録と監視

5.2 システム強化の理解

» 構成管理（例：ベースライン、アップデート、パッチ）

5.3 セキュリティポリシーのベストプラクティスに対する理解

» データ処理ポリシー
» パスワードポリシー
» 許容利用ポリシー（AUP）
» 自分のデバイスを持参（BYOD）ポリシー
» 変更管理ポリシー（例：文書化、承認、ロールバック）
» プライバシーポリシー

5.4 セキュリティ意識向上トレーニングに対する理解

» 目的/概念（例：ソーシャルエンジニアリング、パスワード保護）
» 重要性

試験に関するその他の情報

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、試験に申し込む前に試験の方針や手続きの確認を推奨しています。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)
メール：membersupport@isc2.org

アジア太平洋

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

ヨーロッパ、中東、アフリカ

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