CC SM

サイバーセキュリティ認定

ISC2 Certification

認定試験要綱

施行日：2025年10月1日

ISC2

認定サイバーセキュリティ資格について

サイバーセキュリティ認定（CC）は、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役職に必要な基礎的な知識、スキル、および能力を持っていることを雇用主に証明します。これにより、基本的なセキュリティのベストプラクティス、ポリシー、手順に関する理解と、さらに学び成長する意欲と能力を雇用主に示すことができます。

試験では5つのドメインがカバーされています。

- セキュリティ原則
- ビジネス継続性（BC）、災害復旧（DR）、およびインシデント対応の概念
- 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

試験を受けるための特定の前提条件はありません。 候補者には基本的な情報技術（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職務経験や、正式な教育の修了証書/学位は必要ありません。候補者の次のキャリアステップは、ISC2の専門家レベルの認定を取得することであり、これには業界での経験が必要です。

認定

CCは、ANSI全国認定委員会（ANAB）のISO/IEC規格17024の厳格な要件に準拠しています。

作業タスク分析（JTA）

ISC2は、CCの関連性を維持する責任があります。定期的に実施される職務タスク分析（JTA）は、CCで定義された職業に従事しているセキュリティ専門家が実行するタスクを特定するための体系的で重要なプロセスです。JTAの結果は、試験の更新に使用されます。このプロセスにより、候補者は今日の実務に従事している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領域についてテストされることが保証されます。

CC CAT 試験情報

CC試験は、すべての英語、簡体字中国語、日本語、ドイツ語、スペイン語（現代）試験においてコンピュータ適応型テスト（CAT）を使用します。CC CATについての詳細は www.isc2.org/certifications/computerized-adaptive-testing をご覧ください。

試験時間	2時間
出題数	100 - 125
項目形式	選択式問題と発展的問題
合格ライン	1000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、スペイン語
受験会場	ピアソンVUEテストセンター

CC CAT 試験の比重

ドメイン	比重の平均
1. セキュリティ原則	26%
2. ビジネス継続性（BC）、災害復旧（DR）、およびインシデント対応の概念	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 情報保証のセキュリティ概念を理解する

» 機密性
» 完全性
» 利用可能性
» 認証（例：認証方法、マルチファクター認証（MFA））
» 否認防止
» プライバシー

1.2 リスク管理プロセスを理解する

» 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、評価および対応

1.3 セキュリティ制御を理解する

» 技術的制御
» 管理的制御
» 物理的制御

1.4 ISC2倫理規定を理解する

» プロとしての行動規範

1.5 ガバナンスプロセスを理解する

» ポリシー
» 手順
» 規格
» 規制と法律

ドメイン2：
ビジネス継続性（BC）、災害復旧（DR）、およびインシデント対応の概念

2.1 ビジネス継続性（BC）を理解する

» 目的
» 重要性
» コンポーネント

2.2 災害復旧（DR）を理解する

» 目的
» 重要性
» コンポーネント

2.3 インシデント対応を理解する

» 目的
» 重要性
» コンポーネント

ドメイン3：
アクセス制御の概念

3.1 物理的アクセス制御を理解する

» 物理的セキュリティ制御（例：バッジシステム、ゲート入場、環境設計）
» 監視（例：警備員、閉回路テレビ（CCTV）、警報システム、ログ）
» 許可された者と許可されていない者

3.2 論理的アクセス制御を理解する

» 最小特権の原則
» 職務分掌
» 任意アクセス制御（DAC）
» 強制アクセス制御（MAC）
» 役割ベースのアクセス制御（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キングを理解する

» ネットワーク（例：オープンシステム間相互接続（OSI）モデル、トランスミッション制御プロトコル/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を理解する

» 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）、サイドチャネル攻撃）

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

» 防止（例：アンチウイルス、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を理解する

» オンプレミス（例：電源、データセンター／クローゼット、空調（HVAC）、環境、消火設備、冗長性、了解覚書（MOU）/合意覚書（MOA））

» 設計（例：ネットワーク分割（非武装地帯（DMZ）、仮想ローカルエリアネットワーク（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、モノのインターネット（IoT）向けの分割））

» クラウド（例：サービスレベル契約（SLA）、マネージド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（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を理解する

» 暗号化（例：対称、非対称、ハッシュ化）
» データ取扱い（例：破棄、保管、分類、ラベリング）
» セキュリティイベントのログ記録と監視

5.2 システムの強化を理解する

» 構成管理（例：ベースライン、更新、パッチ）

5.3 ベストプラクティスのセキュリティポリシーを理解する

» データ取扱ポリシー
» パスワードポリシー
» 適正使用ポリシー (AUP)
» 自分のデバイス持参ポリシー (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を理解する

» 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

追加の試験情報

補足参考文献

候補者は、自身の学歴や経験を補完するために、以下の資料を確認することを推奨します。
追加で学習が必要な分野を特定することで 教育や経験を補完することが推奨されます。

補足参考資料の全リストは、www.isc2.org/certifications/References をご覧ください。

試験のポリシーと手続き

ISC2は、受験者が試験に登録する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。この重要な情報の詳細については、www.isc2.org/Register-for-Exam でご確認ください。

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

お住まいの地域のISC2受験者サービス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：+852-5803-5662
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