CC®

Certified in Cybersecurity

ISC2 Certification

認定試験要綱

発効日：2026年9月1日

ISC2™

サイバーセキュリティ認定資格について

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、雇用主に証明するものです。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つのドメインが対象になっています。

- セキュリティ原則
- セキュリティ・ガバナンス
- IDおよびアクセス管理（IAM）の概念
- ネットワーキングとクラウドセキュリティの概念
- セキュリティ運用とインシデント対応

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。受験者には、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。受験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すが、これには業界での経験が必要です。

認定

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

ジョブ・タスク分析（JTA）

ISC2は、会員に対して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ジョブ・タスク分析（JTA）は、CC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、今日の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。

CC CAT試験情報

CC試験は、英語、簡体字中国語、日本語、ドイツ語、スペイン語（現代）試験すべてにおいて、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

試験時間	2時間
出題数	100〜125
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
試験で使用されれる言語	英語、中国語、日本語、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

CC CAT 試験の配点

ドメイン	比重の平均
1. セキュリティ原則	24%
2. セキュリティ・ガバナンス	17.3%
3. IDおよびアクセス管理（IAM）の概念	20%
4. ネットワーキングとクラウドセキュリティの概念	21.3%
5. セキュリティ運用とインシデント対応	17.3%
	合計:100%

ドメイン1：セキュリティ原則

1.1 サイバーセキュリティの概念に対する理解

» 機密性
» 完全性
» 利用可能性
» 認証、認可、アカウンティング（AAA）
» 否認防止
» プライバシー

1.2 リスク管理の概念に対する理解

» リスク管理のライフサイクル
» リスク管理プロセス

1.3 ガバナンスの概念に対する理解

» 規制と法律
» フレームワークとガイドライン
» ポリシー、規格（例：国際規格化機構（ISO）、インターネットセキュリティセンター）、手順

1.4 サイバーセキュリティ制御に対する理解

» 技術的制御
» 管理的制御
» 物理的制御

1.5 専門家としての倫理的行動の維持

» 専門家としての行動規範
» デューケアとデューディリジェンス
» ISC2倫理規定

ドメイン2：
セキュリティ・ガバナンス

2.1 ガバナンス、リスク、コンプライアンス（GRC）の計画

» 目的
» 重要性
» フレームワークとツール

2.2 冗長性に対する理解

» 事業継続（BC）
» 災害復旧（DR）

2.3 セキュリティ意識向上トレーニングに対する理解

» 組織文化（例：セキュリティの重要性、セキュリティ・リーダーシップ）
» 概念（例：ソーシャルエンジニアリング、パスワード保護、フィッシング）

2.4 サイバーセキュリティの有効性の測定

» 重要な指標、重要なリスク指標（KRI）
» ダッシュボード、スコアカード、レポート

ドメイン3：
IDおよびアクセス管理（IAM）の概念

3.1 IDライフサイクル管理に対する理解

» 役割の定義
» プロビジョニング
» レビュー
» デプロビジョニング
» フレームワークとツール

3.2 論理的アクセス制御に対する理解

» 最小権限の原則（PoLP）
» 職務分掌（SoD）
» アクセス制御モデル

ドメイン4：
ネットワーキングとクラウドセキュリティの概念

4.1 ネットワークセキュリティに対する理解

- ネットワーク（例：オープンシステム間相互接続（OSI）モデル、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）、仮想プライベートネットワーク（VPN））
- ファイアウォール（例：ポート、アプリケーション）
- ワイヤレス（例：Wi-Fi、Bluetooth）
- 組込みシステム（例：産業用制御システム（ICS））、モノのインターネット（IoT）

4.2 ネットワークセキュリティ・アーキテクチャに対する理解

- ネットワークセグメンテーション（例：ファイアウォールゾーン、仮想ローカルエリアネットワーク（VPN））、マイクロセグメンテーション）に対する理解
- 多層防御
- ゼロトラスト（ZT）

4.3 クラウドセキュリティに対する理解

- 特徴（例：広範なネットワークアクセス、迅速な伸縮性、測定されたサービス、オンデマンドセルフサービス、リソースプーリング）
- サービスモデル
- 展開モデル
- 共有セキュリティモデル（例：役割と責任）

ドメイン5：
セキュリティ運用とインシデント対応

5.1 データセキュリティに対する理解

» データの取り扱い（例：分類、ラベリング、マスキング、サニタイズ）
» 暗号化（例：対称暗号、非対称暗号、ハッシュ化、量子耐性暗号）

5.2 セキュリティオペレーションに対する理解

» セキュリティイベントのログ記録と監視
» セキュリティイベントのトリアージ（例：インシデントのユースケース、優先順位付け、相関関係）
» 脅威アクター（例：タイプ、動機）
» サイバー脅威インテリジェンス
» 脅威のフレームワーク

5.3 インシデント対応（IR）に対する理解

» インシデント対応計画（IRP）を実装するデータ取り扱いポリシー
» インシデント対応（IR）演習（例：テスト、テーブルトップ）

5.4 資産保護に対する理解

» 資産ライフサイクル管理（例：End Of Life（EOL）ソフトウェアおよびデバイス）
» 構成および変更管理

5.5 セキュリティテストに対する理解

» セキュリティ準備テスト（例：ブルーチーミング、パープルチーミング、レッドチーミング）
» アプリケーションテスト（例：脆弱性スキャン、静的分析、動的分析、脅威モデリング）
» 物理的侵入テスト（例：フィッシング、尾行、なりすまし）

追加の試験情報

補足参考資料

受験者は、CC試験概要に関連する資料に目を通し、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、自身の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については、ISC2.org/certifications/Referencesをご覧ください。

試験ポリシーと手続き

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

お住まいの地域の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