Certified in Cybersecurity

An (ISC)² Certification

認定試験概要

発効日：2022年8月29日

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

Certified in Cybersecurity 認定について

Certified in Cybersecurity（CC）は、初級または基礎レベルのサイバーセキュリティの職務に必要な基礎知識、スキル、能力を有していることを雇用者に証明できる資格です。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と、さらに学習を続けて仕事で成長しようとする意欲と能力を示すことができます。

試験は5つのドメインをカバーしています。

- セキュリティ原則
- 事業継続（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
- セキュリティの運用

必要な経験

受験にあたり、前提条件は特にありません。基本的な情報技術（IT）の知識を持っていることを推奨します。サイバーセキュリティに関する実務経験や、正式な教育課程の修了・学位は必要ありません。次のステップとして、この分野の実務経験を必要とする(ISC)²専門家レベルの認定資格の取得を目指していただくことになります。

ジョブタスク分析（JTA）

(ISC)²は、会員に対してCC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、CC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、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。

CC 認定試験情報

試験時間	2時間
問題数	100
問題形式	多肢選択式
合格基準	1000点満点中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

CC試験の重み

ドメイン	出題比率
1.セキュリティ原則	26%
2. 事業継続(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. セキュリティの運用	18%
合計:	**100%**

ドメイン1:
セキュリティ原則

1.1 情報セキュリティの概念を理解する

» 機密性
» 完全性
» 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 リスクマネジメントプロセスを理解する

» リスクマネジメント（例：リスクの優先順位、リスク許容度）
» リスクの特定、評価、処置

1.3 セキュリティ制御を理解する

» 技術コントロール
» 管理コントロール
» 物理コントロール

1.4 (ISC)²の倫理規約を理解する

» 専門家としての行動規範

1.5 ガバナンスプロセスを理解する

» ポリシー
» 手順
» 標準
» 規則と法律

ドメイン2:
事業継続(BC)、災害復旧(DR)およびインシデント対応の概念

2.1 事業継続（BC）を理解する

» 目的
» 重要性
» 要素

2.2 災害復旧（DR）を理解する

» 目的
» 重要性
» 要素

2.3 インシデント対応の概念を理解する

» 目的
» 重要性
» 要素

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を理解する

» 物理的なセキュリティ制御（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、監視カメラ、警報システム、ログ）
» 許可された人と許可されていない人

3.2 論理的なアクセス制御を理解する

» 最小権限の原則
» 職務分掌
» 任意アクセス制御（DAC）
» 裁量アクセス制御（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 コンピューターネットワーキングについて理解する

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

» 防御（例：アンチウイルス、スキャン、ファイアウォール、侵入防御システム（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、暖房・換気・空調（HVAC）、環境、消火、冗長性、覚書（MOU）/合意書（MOA））

» 設計（例：ネットワークの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（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）（組込みシステム向けセグメンテーション、IoT（モノのインターネット））

» 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:
セキュリティの運用

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）
» データの取り扱い（例：破壊、保管、分類、ラベリング）
» セキュリティイベントのログ取得・監視

5.2 システムのハードニングについて理解する

» 構成管理（例：ベースライン、更新、パッチの適用）

5.3 セキュリティポリシーのベストプラクティスを理解する

» データ取扱ポリシー
» パスワードポリシー
» 許容利用ポリシー（AUP）
» BYOD（Bring Your Own Device）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 セキュリティ意識の向上に関する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

その他の試験に関する情報

試験のポリシーと手順

(ISC)²は、受験志願者が、Certified in Cybersecurityの試験登録前に試験のポリシーと手順を確認する事を推奨します。試験に関する重要な情報が包括的に記載されていますので、Register-for-Exam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

あなたの地域の(ISC)²受験サービスまでお問い合わせください。

アメリカ地域

電話：+1-866-331-ISC2 (4722)
メール：info@isc2.org

アジア・太平洋地域

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

ヨーロッパ、中東、アフリカ地域

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