CISSP®

Certified Information Systems Security Professional

ISC2 Certification

認定資格の試験の概要

実施日：2024年4月15日

ISC2™

CISSPについて

認定情報システムセキュリティ専門家（CISSP）は、情報セキュリティ市場で最も世界的に認知されている認定資格です。CISSPでは組織のセキュリティ体制を効果的に設計、エンジニアリング、管理する情報セキュリティの専門家の専門的技術と管理の知識と経験を確認します。

CISSPの知識体系には幅広いトピックが含まれているため、情報セキュリティ領域におけるのあらゆる分野における関連性を確実にします。合格した受験者は次の8つのドメインに関して十分な適性を備えています。

- セキュリティとリスクマネジメント
- 資産のセキュリティ
- セキュリティ アーキテクチャとエンジニアリング
- 通信とネットワークセキュリティ
- IDおよびアクセス管理（IAM）
- セキュリティの評価とテスト
- セキュリティ運用
- ソフトウェア開発セキュリティ

求められる経験について

認定を受ける受験者は、現行CISSP認定試験概要の8つのドメインのうち、2つ以上のドメインで5年以上のフルタイムの累積実務経験が必要です。コンピュータ サイエンス、情報テクノロジー（IT）、または関連分野で高等教育後の学位 (学士または修士) の取得、または、ISC2 承認リストから追加の資格証明書の取得により、必要な経験年数のうち、最大一年間までを満たすことができます。パートタイム勤務およびインターンシップ期間も経験要件に計上できる場合があります。

CISSPに必要な経験がない受験者でも、CISSP試験に合格することでISC2 Associateになることができます。ISC2 Associateでは、必要な5年分の経験を積むために6年間の猶予が与えられます。CISSPの経験要件と、パートタイム勤務期間の計算方法やインターンシップについての詳細は、
www.isc2.org/Certifications/CISSP/experience-requirementsをご覧ください。

認定

CISSPはANSI/ISO/IEC規格17024の厳しい要件を満たす、情報セキュリティの分野において最初の資格証明書でした。

作業タスク分析（JTA）

ISC2はメンバーに対して、CISSP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、CCSP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で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。

CISSP CAT試験情報

CISSP試験では、英語、ドイツ語、現代スペイン語、日本語、簡体字中国語の試験において、コンピュータ適応型テスト（CAT）を使用しています。CISSP CATの詳細については、www.isc2.org/certificatons/CISSP-CATをご覧ください。

試験時間	3時間
出題数	100 - 150
出題形式	選択方式、高度で革新的な問題
合格ライン	1000点満点中700点
試験に用いられる言語	中国語、英語、ドイツ語、日本語、スペイン語
試験センター	ISC2認定PPCおよびPVTCセレクト ピアソン VUE テストセンター

CISSP CAT試験の比重

ドメイン	比重の平均
1.セキュリティとリスクマネジメント	16%
2.資産のセキュリティ	10%
3.セキュリティ アーキテクチャとエンジニアリング	13%
4.通信とネットワークセキュリティ	13%
5.IDおよびアクセス管理（IAM）	13%
6.セキュリティの評価とテスト	12%
7.セキュリティ運用	13%
8.ソフトウェア開発セキュリティ	10%
合計：	**100%**

ドメイン1：
セキュリティとリスクマネジメント

1.1 職業倫理の理解、遵守、推進

» ISC2職業倫理規定
» 組織倫理規定

1.2 セキュリティの概念の理解、適用

» 機密性、完全性、可用性、真正性、否認防止（情報セキュリティの5つの柱）

1.3 セキュリティガバナンス原則の評価および適用

» 事業戦略、目標、使命、目的に合わせたセキュリティ機能の調整
» 組織プロセス（買収、売却、ガバナンス委員会など）
» 組織の役割と責任
» セキュリティ制御フレームワーク（例：国際規格化機構（ISO）、国立規格技術研究所（NIST）、情報および関連テクノロジーのためのコントロール目標（COBIT）、シャーウッド応用企業安全保障アーキテクチャ（SABSA）、クレジットカード業界（PCI）、連邦リスク及び認証管理プログラム（FedRAMP））
» 相当な注意/精査

1.4 情報セキュリティに関連する法律、規制、コンプライアンスの問題に対する総合的な観点からの理解

» サイバー犯罪とデータ侵害
» ライセンスと知的財産（IP）の要件
» インポート/エクスポートの管理
» 国境を越えたデータの流れ
» プライバシーに関連する問題（例：一般データ保護規則（GDPR）、カリフォルニア消費者プライバシー法、個人情報保護法、個人情報保護法）
» 契約、法的、業界標準および規制要件

1.5 調査の種類の要件の理解（行政、刑事、民事、規制、業界の標準など）

1.6 セキュリティポリシー、規格、手続き、ガイドラインを開発、文書化、実装

1.7 事業継続性（BC）要件の特定、分析し、評価、優先順位付け及び実施

» 事業インパクト分析（BIA）
» 外的な依存関係

1.8 人事セキュリティのポリシーと手続きへの貢献と執行

- 受験者の選考と採用
- 雇用契約およびポリシーに基づく要件
- オンボーディング、異動、解雇のプロセス
- ベンダー、コンサルタント、請負業者との契約と管理

1.9 リスク管理の概念の理解および適用

- 脅威と脆弱性の識別
- リスク分析、アセスメント、およびスコープ
- リスク対応と処置（例：サイバーセキュリティ保険）
- 適用可能な管理の種類（例：予防、発見、是正）
- コントロール評価（例：セキュリティとプライバシー）
- 監視と測定
- 報告（例：内部、外部）
- 継続的な改善（例：リスク成熟度モデリング）
- リスクフレームワーク（例：国際規格化機構（ISO）、国立規格技術研究所（NIST）、情報および関連テクノロジーのためのコントロール目標（COBIT）、シャーウッド応用企業安全保障アーキテクチャ（SABSA）、クレジットカード業界（PCI））

1.10 脅威モデリングの概念と方法論の理解および適用

1.11 サプライチェーンリスク管理（SCRM）に関する概念の適用

- サプライヤーやプロバイダーからの製品やサービスの取得に関連するリスク（例：製品の改ざん、偽造品、インプラント）
- リスク軽減策（例：第三者による評価と監視、最低セキュリティ要件、サービスレベル要件、シリコンルートオブトラスト、物理的に複製不可能な機能、ソフトウェアの部品構成表）

1.12 セキュリティ意識、教育、トレーニングプログラムの確立および維持

- 意識とトレーニングを提示するための方法とテクニック（例：ソーシャル エンジニアリング、フィッシング、セキュリティ チャンピオン、ゲーミフィケーション）
- 新興技術やトレンドを含む定期的なコンテンツのレビュー（例：暗号通貨、人工知能（AI）、ブロックチェーン）
- プログラムの有効性評価

ドメイン2：資産のセキュリティ

2.1 情報と資産を特定及び分類

» データの分類
» 資産の分類

2.2 情報と資産の取り扱い要件の確立

2.3 情報と資産を安全な提供

» 情報と資産の所有権
» 資産インベントリ（有形、無形など）
» 資産管理

2.4 データ ライフサイクルの管理

» データの役割（所有者、管理責任者、保管責任者、処理責任者、ユーザー/対象者）
» データ収集
» データ ロケーション
» データ メンテナンス
» データ保持
» データの残留
» データ破棄

2.5 適切な資産保持の確保（例：エンド オブ ライフ（EOL）、サポート終了（EOS））

2.6 データセキュリティ管理とコンプライアンス要件の決定

» データの状態（使用中、転送中、保存中など）
» 範囲指定と調整
» 規格の選択
» データ保護方法（例：デジタル著作権管理（DRM）、データ損失防止（DLP）、クラウドアクセスセキュリティブローカー（CASB））

ドメイン3：
セキュリティ アーキテクチャとエンジニアリング

3.1 安全な設計原則を使用したエンジニアリングプロセスの調査、実装、管理

- 脅威モデリング
- 最小特権
- 多層防御
- セキュアデフォルト
- フェイルセキュア
- 業務の分掌（SoD）
- シンプルでコンパクトに保つ
- ゼロトラストまたは信頼するが検証する
- プライバシー バイ デザイン
- 共有責任
- セキュアアクセスサービスエッジ（SASE）

3.2 セキュリティモデルの基本概念の理解（例：Biba、Star Model、Bell-LaPadula）

3.3 システムのセキュリティ要件に基づくコントロールの選択

3.4 情報システム（IS）のセキュリティ機能の理解（メモリ保護、信頼性の高いプラットフォームモジュール（TPM）、暗号化/復号化など）

3.5 セキュリティ アーキテクチャ、設計、ソリューション要素の脆弱性の評価および軽減

- クライアントベースのシステム
- サーバーベースのシステム
- データベースシステム
- 暗号化システム
- 工業制御システム（ICS）
- クラウドベースシステム（例：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））
- 分散システム
- モノのインターネット（IoT）
- マイクロサービス (アプリケーション プログラミング インターフェース （API）など)
- コンテナ化
- サーバーレス
- 組み込みシステム
- 高性能コンピューティングシステム
- エッジコンピューティングシステム
- 仮想化システム

3.6 暗号ソリューションの選択と決定

- 暗号化のライフサイクル（鍵、アルゴリズムの選択など）
- 暗号化手法（対称、非対称、楕円曲線、量子など）
- 公開キー基盤（PKI）（例: 量子キー配送センター）
- 主要な管理慣行 （例: ローテーション）
- デジタル署名とデジタル証明書（例：否認防止、完全性）

3.7 暗号解読攻撃の手法の理解

- ブルートフォース
- 暗号文のみ
- 既知の平文
- 頻度解析
- 選択された暗号文
- 実装攻撃
- サイドチャネル
- フォールト インジェクション
- タイミング
- 中間者（MITM）
- パス ザ ハッシュ攻撃
- ケルベロスの悪用
- ランサムウェア

3.8 セキュリティ原則のサイトと施設の設計への適用

3.9 現場および施設のセキュリティ管理の設計

- 配線クローゼット/中間分配施設
- サーバールーム/データセンター
- メディアストレージ施設
- 証拠保管
- 制限区域と作業エリアのセキュリティ
- 公共施設および暖房、換気、および空調（HVAC）
- 環境問題（例：自然災害、人為的災害）
- 火災の予防、検知、および鎮火
- 電源（冗長、バックアップなど）

3.10 情報システムのライフサイクルを管理する

- 利害関係者のニーズと要件
- 要件分析
- アーキテクチャ デザイン
- 開発/実装
- 統合
- 検証と妥当性確認
- 移行/展開
- 運用と保守/維持
- 償却/廃棄

ドメイン4：
通信とネットワークセキュリティ

4.1 ネットワーク アーキテクチャに安全な設計原則を適用する

» 開放型システム間相互接続（OSI）および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 (IP) バージョン 4 および 6 (IPv6) （例：ユニキャスト、ブロードキャスト、マルチキャスト、エニーキャストなど）
» 安全なプロトコル (例: インターネット プロトコル セキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケット層(SSL)/転送層セキュリティ (TLS)
» 多層プロトコルの影響
» 統合プロトコル (例:インターネット小型コンピュータシステムインターフェース (iSCSI)、ボイスオーバーインターネットプロトコル(VoIP)、InfiniBand over Ethernet(IBoE)、Compute Express Link（CXL）
» トランスポートアーキテクチャ (例: トポロジ、データ/コントロール/管理プレーン、カットスルー/ストア アンド フォワード)
» パフォーマンス指標 (帯域幅、遅延、ジッター、スループット、信号対雑音比など)
» トラフィックの流れ (例: 南北、東西)
» 物理的セグメンテーション（例：インバンド、アウト･オブ･バンド、エアギャップ）
» 論理的セグメンテーション（例：仮想ローカルエリアネットワーク（LAN)、仮想プライベートネットワーク（VPN）、仮想ルーティング/転送、仮想ドメイン）
» マイクロ セグメンテーション（例：ネットワークオーバーレイ/カプセル化、分散型ファイアウォール、ルーター、侵入検知システム（IDS）/侵入防止システム（IPS）、ゼロトラスト）
» エッジネットワーク（例：イングレス/エグレス、ピアリング）
» ワイヤレスネットワーク（例：ブルートゥース、Wi-Fi、Zigbee、衛星）
» 携帯電話/モバイルネットワーク（例：4G、5G）
» コンテンツ配信ネットワーク（CDN）
» ソフトウェア定義ネットワーク（SDN）（例：アプリケーションプログラミングインターフェース（API）、ソフトウェア定義広域ネットワーク、ネットワーク機能の仮想化）
» 仮想プライベートクラウド（VPC）
» 監視と管理（例：ネットワーク可観測性、トラフィックフロー/シェイピング、容量管理、障害検出と処理）

4.2 安全なネットワークコンポーネント

» ハードウェアの運用（例：冗長電源、保証、サポート）
» 伝送媒体（例：メディアの物理的セキュリティ、信号伝播の品質）
» ネットワークアクセス制御（NAC）システム（例：物理的および仮想的なソリューション）
» エンドポイントセキュリティ（例：ホストベース）

4.3 設計に従った安全な通信チャネルの実装

» 音声、ビデオ、およびコラボレーション（例：会議、Zoomルーム）
» リモートアクセス（例：ネットワーク管理機能）
» データ通信（例：バックホールネットワーク、衛星）
» 第三者の接続性（例：通信事業者、ハードウェアサポート）

ドメイン5：IDおよびアクセス管理（IAM）

5.1 物理的アクセス制御および論理的アクセス制御

- 情報
- システム
- デバイス
- ファシリティ
- アプリケーション
- サービス

5.2 識別と認証戦略の設計（例：人、デバイス、サービス）

- グループとロール
- 認証、認可、およびアカウンティング（AAA）（例：多要素認証（MFA）、パスワードレス認証）
- セッション管理
- アイデンティティの登録、証明、確立
- フェデレーションID管理（FIM）
- 資格情報管理システム（例：パスワードボールト）
- シングルサインオン（SSO）
- ジャスト・イン・タイム

5.3 サードパーティサービスとのフェデレーション アイデンティティ

- オンプレミス
- クラウド
- ハイブリッド

5.4 認可メカニズムの実装と管理

- ロールベースアクセス制御（RBAC）
- ロールベースアクセス制御
- 強制アクセス制御（MAC）
- 裁量アクセス制御（DAC）
- 属性ベースのアクセスコントロール（ABAC）
- リスクベースアクセス制御
- アクセスポリシーの強制（例：ポリシー定義ポイント、ポリシー施行ポイント）

5.5 IDとアクセスプロビジョニングのライフサイクルの管理

- アカウントアクセスのレビュー（例：ユーザー、システム、サービス）
- プロビジョニングとプロビジョニング解除（例：オンボーディング/オフオンボーディングおよび移動）
- サービスアカウントの管理
- ロールの定義と移行（例：新しいロールに割り当てられた人）
- 特権昇格（例：sudoの使用、その使用の監査）

5.6 認証システムの導入

ドメイン6：
セキュリティの評価とテスト

6.1 評価、テスト、および監査戦略の設計、検証

- 内部（例：組織内の制御）
- 外部（例：組織外の制御）
- 第三者（例：企業の外部の制御）
- 場所（例：オンプレミス、クラウド、ハイブリッド）

6.2 セキュリティ コントロールのテストの実施

- 脆弱性評価
- ペネトレーションテスト（例：レッド、ブルー、および/またはパープルチームの演習）
- レビューの記録
- 合成トランザクション/ベンチマーク
- コードのレビューとテスト
- 悪用ケーステスト
- カバレッジ分析
- インターフェースのテスト (例: ユーザー インターフェース、ネットワーク インターフェース、アプリケーション プログラミング インターフェース (API))
- 侵入攻撃シミュレーション
- コンプライアンス チェック

6.3 セキュリティ プロセスデータの収集（例：技術的および管理的）

- アカウント管理
- 管理レビューと承認
- キーパフォーマンスとリスクインジケータ
- バックアップ検証データ
- トレーニングと啓発
- 災害復旧（DR）と事業継続性（BC）

6.4 テスト結果の分析とレポートの作成

- 改善
- 例外処理
- 倫理的開示

6.5 セキュリティ監査の実施または推進

- 内部（例：組織内の制御）
- 外部（例：組織外の制御）
- 第三者（例：企業の外部の制御）
- 場所 (例：オンプレミス、クラウド、ハイブリッドなど)

ドメイン7：セキュリティ運用

7.1 調査に関する理解と遵守

- 証拠の収集と処理
- 報告と文書化
- 調査技法
- デジタル フォレンジック ツール、戦術、および、手順
- アーティファクト（例：データ、コンピュータ、ネットワーク、モバイルデバイス）

7.2 ログ記録およびモニタリング活動の実施

- 侵入検知と防止 (IDPS)
- セキュリティ情報及びイベント管理（SIEM）
- 継続的な監視とチューニング
- エグレス モニタリング
- ログ管理
- 脅威インテリジェンス（例：脅威フィード、脅威ハンティング）
- ユーザーと事業体の行動分析（UEBA）

7.3 構成管理（CM）の実行（例：プロビジョニング、ベースライン化、自動化）

7.4 基本的なセキュリティ運用概念の適用

- Need-to-know/最小特権の原則
- 業務の分掌（SoD）と責任
- 特権アクセス管理
- ジョブローテーション
- サービスレベル契約（SLA）

7.5 リソース保護の適用

- メディア管理
- メディア保護技術
- 保存中のデータ/転送中のデータ

7.6 インシデント管理の実施

- 検出
- 対応
- 軽減
- 報告
- 復旧
- 改善
- 教訓

7.7 検出および予防措置の運用および維持

- ファイアウォール（例：次世代、ウェブアプリケーション、ネットワーク）
- 侵入検知システム（IDS）と侵入防止システム（IPS）
- ホワイトリスト化/ブラックリストへ化
- サードパーティが提供するセキュリティサービス
- サンドボクシング
- ハニーポット/ハニーネット
- マルウェア対策
- 機械学習と人工知能（AI）ベースのツール

7.8 パッチおよび脆弱性管理の実施とサポート

7.9 変更管理プロセスの理解と参加

7.10 復旧戦略の実施

- バックアップ ストレージ戦略 (例: クラウド ストレージ、オンサイト、オフサイト)
- 復旧サイト戦略 (例: コールドとホット、リソース容量の契約)
- 複数の処理サイト
- システムの復元力、高可用性（HA）、サービス品質（QoS）、およびフォールトトレランス

7.11 災害復旧（DR）プロセスの実装

- 対応
- 人員
- コミュニケーション (例: メソッド)
- 評価
- 復元
- トレーニングと啓発
- 教訓

7.12 災害復旧計画（DRP）のテスト

- リードスルー／テーブルトップ
- ウォークスルー
- シミュレーション
- 並列処理
- フル インタラプション
- コミュニケーション (例: 利害関係者、テスト状況、規制当局)

7.13 事業継続性（BC）計画と演習への参加

7.14 物理セキュリティの実施と管理

- 境界セキュリティ管理
- 内部セキュリティ管理

7.15 人員の安全とセキュリティの懸念への対処

- トラベル
- セキュリティのトレーニングと意識向上 (例: 内部関係者の脅威、ソーシャル メディアの影響、二要素認証 (2FA) 疲労攻撃)
- 危機管理
- 強迫

ドメイン8：
ソフトウェア開発セキュリティ

8.1 ソフトウェア開発ライフサイクル（SDLC）におけるセキュリティの理解、統合

» 開発方法論（例：アジャイル、ウォーターフォール、DevOps、DevSecOps、Scaled Agile Framework）
» 成熟度モデル（例：能力成熟度モデル（CMM）、ソフトウェア保証の成熟度モデル（SAMM））
» 運用および保守
» 変更管理
» 統合製品チーム

8.2 ソフトウェア開発エコシステムにおけるセキュリティ制御の特定、適用

» プログラミング言語
» ライブラリ
» ツールセット
» 統合開発環境
» ランタイム
» 継続的インテグレーションと継続的デリバリー（CI/CD）
» ソフトウェア構成管理（CM）
» コードリポジトリ
» アプリケーション セキュリティ テスト (例: 静的アプリケーション セキュリティ テスト (SAST)、動的アプリケーション セキュリティ テスト (DAST)、ソフトウェア構造解析、対話型アプリケーションのセキュリティテスト (IAST)

8.3 ソフトウェアセキュリティの有効性の評価

» 変更の監査とログ記録
» リスク分析と軽減

8.4 取得したソフトウェアのセキュリティへの影響の評価

» 商用オフザシェルフ（COTS）
» オープンソース
» サードパーティ
» マネージド サービス (例：エンタープライズアプリケーションなど)
» クラウドサービス（例：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））

8.5 安全なコーディングのガイドラインと標準の定義、適用

» ソースコードレベルのセキュリティの弱点と脆弱性
» アプリケーション プログラミング インターフェース（API）のセキュリティ
» 安全なコーディングの実践
» ソフトウェア定義セキュリティ

追加の試験情報

補足参考資料

受験者は、CBKに関連するリソースを確認し、注意が必要な研究分野を特定することで、教育と経験を補うことが奨励されます。

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

試験のポリシーと手続き

ISC2では認定を受ける受験者に対して、試験に登録する前に試験の方針や手続きを確認することを推奨しています。全体的に分類された重要な情報は、isc2.org/register-for-examでご確認いただけます。

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)、「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 (0) 203-960-7800
メール：info-emea@isc2.org

ISC2