CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

認定試験の概要

発効日：2021年5月1日

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

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は世界で最も認められている認定資格です。CISSPは、情報セキュリティ専門家が、組織の全体的なセキュリティ態勢の効果的な設計、エンジニアリング、および管理をするための深い技術的および管理的な知識と経験を持つことを認証するものです。

CISSP共通知識体系（CBK®）は広範囲のテーマを網羅するため、情報セキュリティの全分野に関連することが保証されます。合格者は、次の8ドメインで能力を有すると認められます。

- 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
- アイデンティティとアクセスの管理（IAM）
- セキュリティの評価とテスト
- セキュリティの運用
- ソフトウェア開発セキュリティ

業務経験の要件

受験者は、CISSP CBKの8個のドメインのうち2個以上において、5年以上の有給の業務経験があることが必要です。4年制大学の学士号か各地域でこれに相当するもの、または(ISC)²が承認したリストに記載された追加の資格を取得していれば、1年分の経験が免除されます。教育による業務経験の免除は、1年分のみとします。

CISSPになるために必要な経験を満たしていない受験者は、CISSP試験に合格後、(ISC)²の準会員になることができます。(ISC)²の準会員の期間は6年間であり、その間に必要な5年間の業務経験を満たすようにしてください。CISSPの経験要件とアルバイト・インターンの扱いの詳細については、www.isc2.org/Certifications/CISSP/experience-requirementsをご覧ください。

認証

CISSPは、情報セキュリティ分野において、ANSI/ISO/IEC規格17024の厳格な要求事項に適合した最初の認証資格です。

ジョブタスク分析（JTA）

(ISC)²は、会員に対して、CISSP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、CISSP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方法であり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で確実に試験されます。

CISSP CAT試験情報

CISSP試験では、すべての英語試験にコンピュータ適応型テスト（CAT）を使用しています。他のすべての言語（英語以外の言語）のCISSP試験は、固定フォームの連続問題式で実施されます。CISSP CAT試験の詳細については、www.isc2.org/certificatons/CISSP-CATをご覧ください。

試験時間	4時間
問題数	125 - 175
問題形式	複数選択、高度な革新的項目
合格基準	1000点中700点
対応言語	英語
試験会場	(ISC)²が認定したPPCおよびPVTCセレクトピアソンVUEテストセンター

CISSP CAT試験出題比率

ドメイン	出題比率
1.セキュリティとリスクマネジメント	15%
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.セキュリティの運用	13%
8.ソフトウェア開発セキュリティ	11%
合計：	**100%**

CISSP連続問題式試験

試験時間	6時間
問題数	250
問題形式	複数選択、高度な革新的項目
合格基準	1000点中700点
対応言語	中国語、ドイツ語、韓国語、日本語、スペイン語
試験会場	(ISC)²が認定したPPCおよびPVTCセレクトピアソンVUEテストセンター

CISSP連続問題式試験の出題比率

ドメイン	出題比率
1.セキュリティとリスクマネジメント	15%
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.セキュリティの運用	13%
8.ソフトウェア開発セキュリティ	11%
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 職業倫理を理解し、遵守し、促進する

» (ISC)²職業倫理規約
» 組織倫理規定

1.2 セキュリティの概念を理解し、適用する

» 機密性、完全性、可用性、真正性、否認防止

1.3 セキュリティガバナンスの原則を評価し、適用する

» セキュリティ機能の事業戦略、目標、ミッション、目的への合致
» 組織におけるプロセス（買収、会社分割、ガバナンス委員会等）
» 組織における役割と責任
» セキュリティコントロールフレームワーク
» デューケア/デューデリジェンス

1.4 コンプライアンスおよびその他の要件を決定する

» 契約、法律要件、業界標準、規制要件
» プライバシー要件

1.5 情報セキュリティに関連する法的および規制上の問題を総合的に理解する

» サイバー犯罪とデータ漏洩
» ライセンス供与および知的財産（IP）における要件
» 輸入/輸出管理
» 越境データフロー
» プライバシー

1.6 調査の各種類（すなわち、行政、刑事、民事、規制、業界標準）の要件を理解する

1.7 セキュリティポリシー、標準、手順、およびガイドラインを策定、文書化し、実施する

1.8 事業継続（BC）要件を特定し、分析し、優先順位付けする

» 事業インパクト分析
» 範囲と計画を作成し、文書化する

1.9 人員のセキュリティポリシーと手順に貢献し、実施する

» 雇用候補者の審査と採用
» 雇用契約とポリシー
» 雇用の採用、異動、終了のプロセス
» ベンダー、コンサルタント、委託の合意と管理
» コンプライアンスポリシーの要件
» プライバシーポリシーの要件

1.10 リスクマネジメントの概念を理解し、適用する

» 脅威と脆弱性の特定
» リスク評価/分析
» リスク対応
» 対策の選択と導入
» 適用管理策の形式（防止的、検知的、是正的等）
» コントロールの評価（セキュリティとプライバシー）
» 監視と測定
» 報告
» 継続的改善（リスク成熟度モデリング等）
» リスクフレームワーク

1.11 脅威モデリングの概念と手法を理解し、適用する

1.12 サプライチェーンリスク管理の概念を適用する

» ハードウエア、ソフトウェア、およびサービスに関わるリスク
» サードパーティの評価および監視
» 最低限のセキュリティ要件
» サービスレベル要件

1.13 セキュリティ意識、教育、トレーニングプログラムを確立し、維持する

» 意識向上とトレーニングの方法と技術（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等）
» 内容の定期的なレビュー
» プログラム有効性評価

ドメイン2：
資産のセキュリティ

2.1 情報と資産を特定し、分類する

» 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を確立する

2.3 リソースを安全にプロビジョニングする

» 情報と資産の所有権
» 資産インベントリ（有形、無形等）
» 資産管理

2.4 データライフサイクルを管理する

» データの役割（すなわち、所有者、管理者、保管者、処理者、ユーザー/対象者）
» データの収集
» データの場所
» データの維持
» データの保持
» データの復元
» データの破棄

2.5 適切な資産保持を確実にする（保守期限（EOL）、サポート期限（EOS）等）

2.6 データセキュリティ管理とコンプライアンス要件を決定する

» データの状態（使用中、転送中、静止中等）
» 範囲とテーラリング
» 基準の選定
» データ保護の方法（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）等）

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てエンジニアリングプロセスを調査し、導入し、管理する

» 脅威モデリング
» 最小限の特権
» 多層防御
» 安全な初期値
» フェイルセキュア
» 職務分離（SoD）
» 単純化
» ゼロトラスト
» プライバシー・バイ・デザイン
» 信頼せよ、されど確認せよ
» 共有責任

3.2 セキュリティモデルの基本概念を理解する（Biba、Star Model、Bell-LaPadula等）

3.3 システムのセキュリティ要件に基づき管理策を選択する

3.4 情報システム（IS）のセキュリティ能力を理解する（メモリ保護、トラステッドプラットフォームモジュール（TPM）、暗号／復号）

3.5 セキュリティアーキテクチャ、設計、およびソリューション要素の脆弱性を評価し軽減する

» クライアントベースシステム
» サーバーベースシステム
» データベースシステム
» 暗号システム
» 産業制御システム（ICS）
» クラウドベースシステム（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）等）
» 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
» 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（HPC）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を選択し、決定する

» 暗号のライフサイクル（キー、アルゴリズムの選択等）
» 暗号の方法（対称、非対称、楕円曲線、量子等）
» 公開鍵基盤（PKI）
» 鍵管理の実務
» デジタル署名とデジタル証明書
» 否認防止
» 完全性（ハッシュ等）

3.7 暗号解読攻撃の方法を理解する

» ブルートフォース攻撃
» 暗号文単独攻撃
» 既知平文攻撃
» 頻度分析攻撃
» 選択暗号文攻撃
» 実装攻撃
» サイドチャネル攻撃
» 故障注入攻撃
» タイミング攻撃
» 中間者 (MITM)攻撃
» パス・ザ・ハッシュ
» ケルベロスの悪用
» ランサムウェア

3.8 拠点および施設の設計に安全な原則を適用する

3.9 拠点および施設へのセキュリティ管理を設計する

» 配線用クローゼット/中間配電盤
» サーバールーム/データセンター
» 媒体保管施設
» 証拠保管
» 立入禁止区域および作業区域のセキュリティ
» ユーティリティおよび暖房、換気、および空調（HVAC）
» 環境の問題
» 防火、火災検知および消火
» 電源（冗長、バックアップ等）

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評価し、適用する

» オープンシステム相互接続（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）ネットワーク（インターネットプロトコルセキュリティ（IPSec）、インターネットプロトコル（IP）v4/6等）
» 安全なプロトコル
» マルチレイヤプロトコルの影響
» コンバージドプロトコル（ファイバーチャネルオーバーイーサネット（FCoE）、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）等）
» マイクロセグメンテーション（ソフトウェア定義ネットワーク（SDN）、仮想拡張可能ローカルエリアネットワーク（VXLAN）、カプセル化、ソフトウェア定義の広域ネットワーク（SD-WAN）等）
» 無線ネットワーク（Li-Fi、Wi-Fi、Zigbee、衛星等）
» セルラーネットワーク（4G、5G等）
» コンテンツ配信ネットワーク（CDN）

4.2 安全なネットワークコンポーネント

» ハードウエアの運用（冗長電源、保証、サポート等）
» 伝送媒体
» ネットワークアクセス制御（NAC）デバイス
» エンドポイントセキュリティ

4.3 安全な通信チャネルを設計し構築する

» 音声
» マルチメディアコラボレーション
» リモートアクセス
» データ通信
» 仮想化ネットワーク
» サードパーティの接続

ドメイン5：IDおよびアクセス管理（IAM）

5.1 資産への物理的および論理的アクセスを制御する

» 情報
» システム
» デバイス
» 施設
» アプリケーション

5.2 人、デバイス、サービスの特定および識別を管理する

» アイデンティティ管理（IdM）の実装
» 単一/多要素認証（MFA）
» 説明責任
» セッション管理
» アイデンティティの登録、証明、確認
» フェデレーションアイデンティティ管理（FIM）
» 認証情報管理システム
» シングルサインオン（SSO）
» ジャスト・イン・タイム（JIT）

5.3 サードパーティの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 認可の仕組みを実装し管理する

» ロールベースアクセス制御（RBAC）
» ル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制御（ABAC）
» リスクベースアクセス制御

5.5 アイデンティティおよびアクセスプロビジョニングのライフサイクルを管理する

» アカウントアクセスの審査（ユーザー、システム、サービス等）
» プロビジョニングとプロビジョニング解除（入退社と異動等）
» 役割の定義（新しい役割に割り当てられた人員等）
» 権限のエスカレーション（管理サービスアカウント、sudoの使用、使用の最小化等）

5.6 認証システムを実装する

» オープンIDコネクト（OIDC）/オープン認証（Oauth）
» セキュリティアサーションマークアップ言語（SAML）
» ケルベロス
» リモート認証ダイヤルインユーザーサービス（RADIUS）/ターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）

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、監査戦略を設計し、検証する

» 内部
» 外部
» サードパーティ

6.2 セキュリティコントロールテストを実施する

» 脆弱性評価
» ペネトレーションテスト
» ログレビュー
» 代理トランザクション
» コードレビューとテスト
» 悪用ケーステスト
» テストカバレッジの分析
» インターフェーステスト
» 侵害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を収集する（技術、管理等）

» アカウント管理
» 経営層のレビューと承認
» 重要業績指標とリスク指標
» 検証データのバックアップ
» トレーニングと意識向上
» 災害復旧（DR）と事業継続性（BC）

6.4 テスト出力を分析し、レポートを生成する

» 修復
» 例外処理
» 倫理的開示

6.5 セキュリティ監査を実施または促進する

» 内部
» 外部
» サードパーティ

ドメイン7：
セキュリティの運用

7.1 調査を理解し、遵守する

» 証拠の収集と取り扱い
» 報告および文書化
» 調査手法
» 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（コンピュータ、ネットワーク、モバイルデバイス等）

7.2 ログ取得と監視活動を実施する

» 侵入検知および防止
» セキュリティ情報およびイベント管理（SIEM）
» 継続的な監視
» 出力監視
» ログ管理
» 脅威インテリジェンス（脅威フィード、脅威ハンティング等）
» ユーザとエンティティティの行動分析（UEBA）

7.3 構成管理（CM）の実行（プロビジョニング、ベースライン、自動化等）

7.4 基礎的なセキュリティ運用概念を理解し適用する

» 知る必要性/最小限の特権
» 職務分離（SoD）と責任
» 特権アカウント管理
» ジョブローテーション
» サービスレベル契約（SLAs）

7.5 リソース保護手法を適用する

» 媒体管理
» 媒体保護技術

7.6 インシデント管理を実施する

» 検知
» 対応
» 緩和
» 報告
» 復旧
» 修復
» 教訓

7.7 検知および防止策を運用し維持する

» ファイアウォール（次世代、Webアプリケーション、ネットワーク等）
» 侵入検知システム（IDS）および侵入防止システム（IPS）
» ホワイトリスティング／ブラックリスティング
» サードパーティのセキュリティサービス
» サンドボックス
» ハニーポット/ハニーネット
» マルウエア対策
» 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を実施しサポートする

7.9 変更管理プロセスを理解し参加する

7.10 復旧戦略を実施する

» バックアップストレージ戦略
» 復旧サイト戦略
» 複数処理サイト
» システム障害許容力、高可用性、サービス品質（QoS）、 およびフォルトトレランス

7.11 災害復旧（DR）プロセスを導入する

» 対応
» 人員
» 通信
» 評価
» 復元
» トレーニングと意識向上
» 教訓

7.12 災害復旧計画（DRP）をテストする

» 読み合わせ/机上
» ウォークスルー
» シミュレーション
» 並行
» 完全な中断

7.13 事業継続性（BC）の立案および行使に参加する

7.14 物理的セキュリティを実装し管理する

» 境界セキュリティ制御
» 内部セキュリティ制御

7.15 個人の安全に関する懸念への対処に参加する

» 出張
» セキュリティトレーニングと意識向上
» 緊急管理
» 強要

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）においてセキュリティを理解し統合する

» 開発手法（アジャイル、ウォーターフォール、DevOps、DevSecOps等）
» 成熟度モデル（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）等）
» 運用と保守
» 変更管理
» 統合製品チーム（IPT）

8.2 開発エコシステムにおいてセキュリティ制御を識別し適用する

» 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（IDE）
» 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）
» セキュリティのオーケストレーション、自動化、対応（SOAR）
» ソフトウェア構成管理（SCM）
» 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（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）等）

8.3 ソフトウェアセキュリティの有効性を評価する

» 変更の監査とログ取得
» リスク分析と軽減

8.4 取得したソフトウエアのセキュリティインパクトを評価する

» 市販品（COTS）
» オープンソース
» サードパーティ
» マネージドサービス（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）等）

8.5 セキュアコーディング規定とガイドラインを定義し適用する

» ソースコードレベルで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
» セキュアコーディングの実践
» ソフトウェア定義のセキュリティ

追加の試験情報

参考文献

受験志願者は、共通知識分野（CBK）に関連するリソースを見直し、追加で注目すべき学習領域を認識することで、これまでの教育および経験を補うことが奨励されます。

参考文献の完全なリストはwww.isc2.org/certifications/Referencesをご確認ください。

試験のポリシーと手続き

(ISC)²は、受験志願者が、CISSP 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、www.isc2.org/Register-for-Examをご確認ください。

法務情報

(ISC)²のリーガルポリシーに関するご質問は、(ISC)²法務部（legal@isc2.org）までお問い合わせください。

お問い合わせ先

(ISC)² Candidate Services
625 N. Washington Street, Suite 400
Alexandria, VA 22314

(ISC)² Americas
Tel: +1-866-331-ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org