CISSP®

Certified Information Systems Security Professional

認定試験概要

発行日: 2018年4月

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

CISSPについて

CISSP (Certified Information Systems Security Professional) は、国際的に認められた情報セキュリティの認証資格です。CISSPは、情報セキュリティプロフェッショナルの技術と管理に関わる深い知識、及び組織におけるセキュリティ態勢全般の効果的な設計、技術、管理の経験について検証します。

CISSPの共通知識分野（CBK）に含まれる広範囲なトピックスは情報セキュリティ分野の広範な領域にわたって関連性を確保しています。受験志願者が合格するには、以下の８ドメインについての能力が求められます。

- 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
- セキュリティの評価とテスト
- セキュリティの運用
- ソフトウエア開発セキュリティ

業務経験の要件

受験志願者は、CISSP CBKの8個のドメインのうち、2個以上において、有給での常勤セキュリティプロフェッショナルとしての業務経験が累計で5年以上なければなりません、. 4年制大学の学士号、各地域でこれに相当するものの取得、もしくは(ISC)²が承認するリストに掲載されている有効な認証を保持している場合には、1年間の経験の免除を受けることができます。経験が免除されるのは、合計で1年までです。

CISSP試験の合格者で、CISSPに必要とされる職務経験のない受験志願者は、試験合格後 (ISC)² 準会員として登録することができます。 (ISC)² 準会員の期間は6年間までとなり、それまでに必要とされる5年の経験年数を満たすようにして下さい。

認証

CISSPは、 ANSI/ ISO/IEC スタンダード 17024.の厳格な要求に適合した最初の情報セキュリティ認証資格です。

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。 一定の間隔で実施されるジョブタスク分析は、CISSPにて定義された業務に従事するセキュリティプロフェッショナルが、実際に行っているタスクを把握する上で重要なプロセス／方法です。ＪＴＡの結果は、試験を更新する際に利用されます。このプロセスは、受験志願者が本日の情報セキュリティプロフェッショナルが担う役割と責任に関連する領域についてテストされる事を確保します。

CISSP CAT 試験について

CISSPの全ての英語の試験は、CAT（Computerized Adaptive Testing）で実施します。他言語によるCISSPの試験は 固定フォームにより実施されます。CISSP CAT試験については www.isc2.org/certificatons/CISSP-CAT. をご参照下さい

試験時間	3 時間
出題数	100 - 150
出題形式	複数選択・高度な革新的設問
合格基準	1000点中700点
対応言語	英語
試験会場	(ISC)² に認められたPPC およびPVTC Selectのピアソン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管理	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	14%
5. アイデンティティとアクセスの管理(IAM)	13%
6. セキュリティアセスメントとテスト	12%
7. セキュリティの運用	13%
8. ソフトウエア開発のセキュリティ	10%
合計	**100%**

CISSP 連続問題式 試験について

試験時間	6 時間
出題数	250
出題形式	複数選択・高度な革新的形式
合格基準	1000点中700点
対応言語	フランス語, ドイツ語, ブラジル系ポルトガル語,スペイン語, 日本語、簡体字中国語, 韓国語
試験会場	(ISC)² に認められたPPC およびPVTC Selectのピアソン VUEテストセンター

CISSP 連続問題式 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管理	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	14%
5. アイデンティティとアクセスの管理(IAM)	13%
6. セキュリティアセスメントとテスト	12%
7. セキュリティの運用	13%
8. ソフトウエア開発のセキュリティ	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 機密性、完全性および可用性の概念の理解と適用

1.2 セキュリティガバナンスの原則を適用する

- 事業戦略、目標、ミッションおよび目的とセキュリティ機能の合致
- 組織におけるプロセス (買収、会社分割、ガバナンス委員会など)
- 組織におけるセキュリティの役割と責任
- セキュリティコントロールフレームワーク
- 妥当な注意/デューディリジェンス

1.3 コンプライアンス要件を決定する

- 契約, 法令, 業界標準、および規制の要求
- プライバシー関連の要求

1.4 情報セキュリティに関連する法的および規制の問題をグローバルな文脈で理解する

- サイバー犯罪と情報漏洩
- ライセンス供与および知的財産における要件
- 輸入/輸出管理
- 越境データフロー
- プライバシー

1.5 職業倫理を理解する

- (ISC)² 倫理規約
- 組織の倫理規約

1.6 文書化されたセキュリティポリシー、スタンダード、プロシージャ、およびガイドラインを策定し導入する

1.7 事業継続要件を理解する

- 範囲および計画を策定し文書化する
- 事業影響度分析

1.8 人的セキュリティポリシーへの貢献

- 雇用志願者の審査
- 雇用契約とポリシー
- 雇用の採用と終了のプロセス
- 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

1.9 リスクマネジメントの概念と理解の適用

- 脅威認識と脆弱性
- リスク評価／分析
- リスクレスポンス
- 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)
- セキュリティ管理策の測定 (SCA)
- 監視と測定
- 資産評価
- 報告
- 継続的改善
- リスクフレームワーク

1.10 脅威のモデリングを理解し適用する

- 脅威のモデリングと方法
- 脅威のモデリングとコンセプト

1.11 調達戦略および実行にセキュリティリスクに関する考慮事項を取り入れる

- ハードウエア、ソフトウエア、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

1.12 情報セキュリティの教育、トレーニング、および意識向上策を構築し管理する

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

ドメイン 2: 資産のセキュリティ

2.1 情報および資産を分類する

- » データの分類
- » 資産の分類

2.2 情報と資産の所有者を決定し維持する

2.3 プライバシーを保護する

- » データオーナー
- » データ処理者
- » データの残留
- » 収集制限

2.4 適切なデータ保持を確実にする

2.5 データセキュリティ管理を決定する

- » データの状況理解
- » 範囲とテーラリング
- » スタンダードの選定
- » データ保護の方法

2.6 情報と資産の取り扱い要件を確立する

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導入し管理する

3.2 セキュリティモデルの基本概念を理解する

3.3 システムセキュリティ要件に基づき管理策を選択する

3.4 情報システムのセキュリティ能力を理解する (メモリ保護、信頼できるプラットフォームモジュール、暗号化／復号化)

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
- 暗号化システム
- 産業制御システム
- クラウドベースシステム
- ディストリビューテッドシステム
- モノのインターネット (IoT)

3.6 ウェブベースシステムにおける脆弱性を評価し軽減する

3.7 モバイルシステムにおける脆弱性を評価し軽減する

3.8 組み込みデバイスにおける脆弱性を評価し軽減する

3.9 暗号化を適用する

- 暗号化のライフサイクル (鍵管理, アルゴリズムの選択)
- 暗号化の方法(対称、非対称、楕円曲線)
- 公開鍵インフラストラクチャ (PKI)
- 鍵管理の実務
- デジタル署名
- 否認防止
- 完全性 (ハッシュ)
- 暗号解読攻撃の方法
- デジタル著作権管理 (DRM)

3.10 事業所および施設の設計に安全な原則を適用する

3.11 事業所および施設へのセキュリティ管理を導入する

- 配線用ボックス/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冷暖房空調設備 (HVAC)
- 環境の問題
- 防火、火災検知および消火

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

- » OSIおよびTCP/IP モデル
- » IP ネットワーク
- » マルチレイヤプロトコルの意味
- » コンバージドプロトコル
- » ソフトウエア定義ネットワーク
- » 無線ネットワーク

4.2 安全なネットワークコンポーネント

- » ハードウエアのオペレーション
- » 伝送媒体
- » ネットワークアクセスコントロールデバイス
- » エンドポイントセキュリティ
- » コンテンツ配信ネットワーク

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

ドメイン 5: アイデンティティとアクセスの管理 (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

5.2 人とデバイスの特定および認証を管理する

- アイデンティティ管理の実装
- 単一／多要素認証
- 説明責任
- セッション管理
- アイデンティティの登録と確認
- フェデレーテッドＩＤ管理 (FIM)
- 信用管理システム

5.3 サードパーティのサービスとしてアイデンティティを統合する

- オンプレミス
- クラウド
- フェデレーテッド

5.4 承認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)
- 任意アクセス制御 (DAC)
- 属性ベースアクセス制御 (ABAC)

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

- ユーザーアクセスの確認
- システムアカウントアクセスの確認
- プロビジョニングとプロビジョニング解除

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 セキュリティ制御テストを実施する

» 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
» テスト範囲の分析
» インターフェーステスト

6.3 セキュリティプロセスデータを収集する (運用制御および管理など)

» アカウント管理
» 管理レビューと承認
» KPIおよびリスク指標
» バックアップ確認データ
» トレーニングと意識向上
» 災害復旧(DR)と事業継続(BC)

6.4 テスト結果を分析し報告する

6.5 施設のセキュリティ監査を実施する

» 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、支援する

- 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

7.2 捜査タイプ毎の要件を理解する

- 運用上
- 刑事上
- 民事上
- 規制上
- 業界標準

7.3 ロギングと監視活動を実施する

- 侵入検知と防止
- セキュリティ情報とイベント管理 (SIEM)
- 継続的な監視
- 漏洩の監視

7.4 リソースのプロビジョニングを保護する

- 資産インベントリ
- 資産管理
- 構成管理

7.5 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／最小特権
- 職務および責任の分離
- 特権アカウント管理
- ジョブローテーション
- 情報ライフサイクル
- サービスレベルアグリーメント (SLA)

7.6 リソース保護手法を採用する

- 媒体管理
- ハードウエアおよびソフトウエア資産管理

7.7 インシデント管理を実施する

- 検知
- 対応
- 軽減
- 報告
- リカバリ
- 是正
- 学んだ教訓

7.8 検知および防止策を運用し維持する

- ファイアウォール
- 侵入検知と防止システム
- 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

7.9 パッチ及び脆弱性管理を実施しサポートする

7.10 変更管理プロセスに参加し理解する

7.11 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、サービスの質 (QoS), およびフォルトトレランス

7.12 災害復旧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

7.13 災害復旧計画をテストする

- » リードスルー／テーブルタップ
- » ウォークスルー
- » シミュレーション
- 並列作業テスト
- 完全断

7.14 事業継続計画の立案および行使に参加する

7.15 物理的セキュリティを実装し管理する

- 境界のセキュリティ管理
- 内部のセキュリティ管理

7.16 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: ソフトウエア開発のセキュリティ

8.1 ソフトウエア開発のライフサイクル(SDLC)におけるセキュリティを理解し適用する

- 開発方法
- 成熟度モデル
- 運用と保守
- 変更管理
- 統合製品チーム

8.2 開発環境においてセキュリティ制御を認識し執行する

- ソフトウエア環境のセキュリティ
- 安全なコーディングの側面としての構成管理
- コードリポジトリのセキュリティ

8.3 ソフトウエアセキュリティの有効性を評価する

- 変更と監査のロギング
- 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

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のセキュリティ
- セキュアコーディングの実践

試験情報(追記)

参照

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、新たに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。参照情報リストについては www.isc2.org/certifications/References. をご確認下さい。

試験のポリシーと手順

(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. をご確認下さい。

リーガル情報

(ISC)²'のリーガル ポリシーについてのご質問は、(ISC)² 法務部(legal@isc2.org)までお問合せ下さい。

お問い合わせ

(ISC)² Candidate Services (受験志願者向けサービス)
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org