経済産業省委託事業

平成 24 年度情報セキュリティ対策推進事業

(情報セキュリティ人材の育成指標等の策定事業)

事業報告書

～ 第４編 ～

情報セキュリティに関する認定・資格調査結果

平成 25 年 3 月

みずほ情報総研株式会社

国内/
国家資格

情報セキュリティスペシャリスト

資格の概要

情報処理技術者試験は、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験である。情報システムを構築・運用する「技術者」から情報システムを利用する「エンドユーザ（利用者）」まで、ITに係わる全ての人を対象としたベンダーフリーの試験である。

「情報セキュリティスペシャリスト」は、セキュリティ機能の企画・要件定義・開発・運用・保守を推進又は支援する業務、若しくはセキュアな情報システム基盤を整備する業務を主導的に行うとともに、下位者を指導する役割を持つ人材を認定する。

開始年度	2009年	実施団体名	独立行政法人 情報処理推進機構		
受験者数（H24春期）	19,711名	合格者数（H24春期）	2,707名	資格保持者数（平成21年度春期～）	11,044名
目的	セキュリティ機能の企画・要件定義・開発・運用・保守を推進又は支援する業務、若しくはセキュアな情報システム基盤を整備する業務を主導的に行うとともに、下位者を指導する役割を持つ人材を認定する。				
対象者像	高度IT人材として確立した専門分野をもち、情報システムの企画・要件定義・開発・運用・保守において、情報セキュリティポリシに準拠してセキュリティ機能の実現を支援し、又は情報システム基盤を整備し、情報セキュリティ技術の専門家として情報セキュリティ管理を支援する者				
認定条件	情報処理技術者試験「情報セキュリティスペシャリスト試験」への合格				
更新条件	なし				
URL	http://www.jitec.ipa.go.jp/1_11seido/sc.html				

活用状況

・企業における活用

社団法人情報サービス産業協会発行の「賃金データ」平成22年度調査によると回答企業116社中107社が、情報処理技術者試験の少なくとも一つ以上の試験区分に対して一時金又は資格手当を支給している。

・公的機関における活用

官公庁、地方公共団体の情報システム開発の競争入札参加申請（北海道、大分県、静岡県、岩手県など）において、申請書の一つに、情報処理技術者試験合格者数の記入を求めている。或いは、情報処理技術者試験合格者を雇用していることが要件の場合もある。

・国家試験などにおける優遇制度など

情報処理技術者試験合格者は教員採用選考試験（一部の県市）で試験の一部免除を実施。また弁理士試験の一部免除を実施。コンピュータ犯罪捜査官（警視庁）、サイバー犯罪捜査官（群馬県警）の応募資格の一つとなっている。

認知度・浸透度

・国家試験。昭和44年にプログラマを対象とした「情報処理技術者認定試験制度」を通商産業省告示により発足させ、第一種情報処理技術者認定試験と第二種情報処理技術者認定試験が実施。昭和45年に情報処理技術者試験が法制化。昭和59年より試験事務が公益法人に委譲。平成16年より「独立行政法人 情報処理推進機構（IPA）」に移管。

・株式会社日経BP IT Pro「いる資格、いらない資格」（http://itpro.nikkeibp.co.jp/article/COLUMN/20120412/390758/）にて、情報処理技術者試験の中で、ITベンダーの人事担当者が自社の技術者に「取得させたい」資格第3位、ユーザー企業のシステム部長が自社のシステム部員に「取得させたい」資格第3位、システム部員が「取得したい」資格第2位。

スキル要件・シラバス

受験条件

下位試験に「ITパスポート」「基本情報技術者」「応用情報技術者」があるが、当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲

特定の製品やソフトウェアに関する試験ではなく、情報技術の背景として知るべき原理や基礎となる技能について、幅広い知識を総合的に評価する。出題形式は筆記試験（多肢選択式、記述式）である。

1. 情報システムの脆弱性・脅威分析

情報資産の評価、リスクの特定（脆弱性・脅威の検出）、リスクの算定、リスクの評価、リスク対応の選択

2. セキュリティ要件定義

セキュリティ要件定義のための情報収集・分析、セキュリティアーキテクチャの設計、セキュリティ要件の決定、セキュリティ要件定義書の作成、セキュリティ要件定義書の評価とレビュー

3. セキュリティ機能の設計

セキュリティ機能方式の決定と評価、セキュリティ実装の設計、セキュリティ実装テスト仕様の作成

4. 開発の管理に関すること

セキュリティ機能の実装、システムテストの支援、関連文書の更新

5. 情報セキュリティ関連の法的要求事項などに関すること

開発対象システムの本番移行の支援、開発対象システムの受け入れ検査支援、運用担当者の教育・訓練及び支援、システム利用者対応

6. 情報セキュリティ面からのレビュー

開発対象システムのセキュリティレビュー

7. 情報システム運用時のセキュリティ管理の支援

セキュリティ管理体制の確立の支援、セキュリティ侵入の監視の支援と状況分析の支援、セキュリティ強度の確認の支援、セキュリティ侵入への対応の支援、セキュリティの評価の支援

8. 開発プロジェクトの管理

開発ライフサイクル管理、セキュリティ違反への対処。セキュリティパッチの運用作業、システム文書管理、人的管理

9. 情報セキュリティマネジメントの支援

情報セキュリティ基本方針の策定支援、情報セキュリティ対策基準の策定支援、情報セキュリティの見直しの支援

URL:http://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf

認定団体について

■ 情報処理推進機構 ■ 独立行政法人。「暮らしを支えるITの安全性・信頼性の向上」「国際競争に勝ち抜けるIT産業の創造」「世界で活躍できる優れたIT人材の育成」の三つをミッションに掲げる。国家試験である情報処理技術者試験を実施。

URL:http://www.ipa.go.jp/

設立年	2004年
所在国	日本
団体種別	独立行政法人
参加者	職員（169名）

国内/
国家資格

システム監査技術者

資格の概要

情報処理技術者試験は、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験である。情報システムを構築・運用する「技術者」から情報システムを利用する「エンドユーザ（利用者）」まで、ITに係わる全ての人を対象としたベンダーフリーの試験である。

「システム監査技術者」は、被監査対象から独立した立場で、情報システムや組込みシステムを監査する業務を主導的に行うとともに、下位者を指導する役割を持つ人材を認定する。

開始年度	1994年	実施団体名	独立行政法人 情報処理推進機構		
受験者数（H24春期）	3,216名	合格者数（H24春期）	468名	資格保持者数（平成21年度春期～）	8,885名
目的	被監査対象から独立した立場で、情報システムや組込みシステムを監査する業務を主導的に行うとともに、下位者を指導する役割を持つ人材を認定する。				
対象者像	高度IT人材として確立した専門分野をもち、被監査対象から独立した立場で、情報システムや組込みシステムに関するリスク及びコントロールを総合的に点検、評価し、監査結果をトップマネジメントなどに報告し、改善を勧告する者				
認定条件	情報処理技術者試験「システム監査技術者試験」への合格				
更新条件	なし				
URL	http://www.jitec.jp/1_11seido/au.html				

活用状況

・企業における活用

社団法人情報サービス産業協会発行の「賃金データ」平成22年度調査によると回答企業116社中107社が、情報処理技術者試験の少なくとも一つ以上の試験区分に対して一時金又は資格手当を支給している。

・公的機関における活用

官公庁、地方公共団体の情報システム開発の競争入札参加申請（北海道、大分県、静岡県、岩手県など）において、申請書の一つに、情報処理技術者試験合格者数の記入を求めている。或いは、情報処理技術者試験合格者を雇用していることが要件の場合もある。

・国家試験などにおける優遇制度など

情報処理技術者試験合格者は教員採用選考試験（一部の県市）で試験の一部免除を実施。また中小企業診断士試験、弁理士試験で試験の一部免除を実施。サイバー犯罪捜査官（千葉県警、群馬県警）の応募資格の一つとなっている。

認知度・浸透度

・国家試験。昭和44年にプログラマを対象とした「情報処理技術者認定試験制度」を通商産業省告示により発足させ、第一種情報処理技術者認定試験と第二種情報処理技術者認定試験が実施。昭和45年に情報処理技術者試験が法制化。昭和59年より試験事務が公益法人に委譲。平成16年より「独立行政法人 情報処理推進機構（IPA）」に移管。

・株式会社日経BP IT Pro「いる資格、いらない資格」（http://itpro.nikkeibp.co.jp/article/COLUMN/20120412/390758/）にて、情報処理技術者試験の中で、ユーザー企業のシステム部長が自社のシステム部員に「取得させたい」資格第6位、システム部員が「取得したい」資格第6位。

スキル要件・シラバス

受験条件

下位試験に「ITパスポート」「基本情報技術者」「応用情報技術者」があるが、当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲

特定の製品やソフトウェアに関する試験ではなく、情報技術の背景として知るべき原理や基礎となる技能について、幅広い知識を総合的に評価する。出題形式は多肢選択式、記述式、論述式である。

1. システム監査の計画

中長期計画書の作成、年度計画書の作成、個別計画書の作成

2. システム監査の実施

実施準備、
予備調査（(1) 関連資料の収集，インタビューなどによる情報収集　(2) 現状把握）、
監査手続書の作成、
本調査（(1) 現地調査　(2) インタビュー　(3) ドキュメントレビュー　(4) その他のシステム監査技法）、
実施結果の記録（監査調書の作成監査意見の明確化（監査判断の形成）、
評価・結論の総合検討、
監査報告書案の作成

3. システム監査の報告

指摘事項の記載、改善勧告の記載、補足事項の記載
監査報告書の提出、監査報告会の開催
フォローアップの実施、年度監査報告書の作成

4. システム監査業務の管理

進捗管理、品質管理、監査業務の改善、監査体制の整備

URL:http://www.jitec.ipa.go.jp/1_13download/syllabus_au_ver2_0.pdf

認定団体について

■ 情報処理推進機構 ■　独立行政法人。「暮らしを支えるITの安全性・信頼性の向上」「国際競争に勝ち抜けるIT産業の創造」「世界で活躍できる優れたIT人材の育成」の三つをミッションに掲げる。国家試験である情報処理技術者試験を実施。

URL:http://www.ipa.go.jp/

設立年	2004年
所在国	日本
団体種別	独立行政法人
参加者	職員（169名）

国内/
国家資格

応用情報技術者

資格の概要

情報処理技術者試験は、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験である。情報システムを構築・運用する「技術者」から情報システムを利用する「エンドユーザ（利用者）」まで、ITに係わる全ての人を対象としたベンダーフリーの試験である。

「応用情報技術者」は、基本戦略立案又はITソリューション・製品・サービスを実現する業務に従事し、需要者の課題をITを活用して解決する戦略の立案、あるいはシステムの設計・開発、又は汎用製品の最適組合せによって信頼性・生産性の高いシステムを構築し、またその安定的な運用サービスを実現する人材を認定する。

開始年度	2009年	実施団体名	独立行政法人 情報処理推進機構		
受験者数（H24春期）	35,072名	合格者数（H24春期）	7,945名	資格保持者数（平成21年度春期～）	33,831名
目的	基本戦略立案又はITソリューション・製品・サービスを実現する業務に従事し、需要者の課題をITを活用して解決する戦略の立案、あるいはシステムの設計・開発、又は汎用製品の最適組合せによって信頼性・生産性の高いシステムを構築し、またその安定的な運用サービスを実現する人材を認定する。				
対象者像	高度IT人材となるために必要な応用的知識・技能をもち、高度IT人材としての方向性を確立した者				
認定条件	情報処理技術者試験「応用情報技術者試験」への合格				
更新条件	なし				
URL	http://www.jitec.jp/1_11seido/ap.html				

活用状況

・企業における活用

社団法人情報サービス産業協会発行の「賃金データ」平成22年度調査によると回答企業116社中107社が、情報処理技術者試験の少なくとも一つ以上の試験区分に対して一時金又は資格手当を支給している。

・公的機関における活用

官公庁、地方公共団体の情報システム開発の競争入札参加申請（北海道、大分県、静岡県、岩手県など）において、申請書の一つに、情報処理技術者試験合格者数の記入を求めている。或いは、情報処理技術者試験合格者を雇用していることが要件の場合もある。

・国家試験などにおける優遇制度など

情報処理技術者試験合格者は教員採用選考試験（一部の県市）で試験の一部免除を実施。また中小企業診断士試験、弁理士試験の一部免除を実施。コンピュータ犯罪捜査官（警視庁）、サイバー犯罪捜査官（千葉県警、群馬県警）の応募資格の一つとなっている。

認知度・浸透度

・国家試験。昭和44年にプログラマを対象とした「情報処理技術者認定試験制度」を通商産業省告示により発足させ、第一種情報処理技術者認定試験と第二種情報処理技術者認定試験が実施。昭和45年に情報処理技術者試験が法制化。昭和59年より試験事務が公益法人に委譲。平成16年より「独立行政法人 情報処理推進機構（IPA）」に移管。

・株式会社日経BP IT Pro「いる資格、いらない資格」（http://itpro.nikkeibp.co.jp/article/COLUMN/20120412/390758/）にて、情報処理技術者試験の中で、ITベンダーの人事担当者が自社の技術者に「取得させたい」資格第2位、ITベンダーの技術者が「取得済み」、「取得したい」資格第2位、ユーザー企業のシステム部員が「取得済み」、「取得したい」資格第2位。

スキル要件・シラバス

受験条件

下位試験に「ITパスポート」「基本情報技術者」があるが、当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲

特定の製品やソフトウェアに関する試験ではなく、情報技術の背景として知るべき原理や基礎となる技能について、幅広い知識を総合的に評価する。出題形式は多肢選択式、記述式である。

1. 基礎理論

（1）基礎理論：離散数学、応用数学、情報に関する理論、通信に関する理論、計測・制御に関する理論
（2）アルゴリズムとプログラミング：データ構造、アルゴリズム、プログラミング、プログラム言語、その他の言語

2. コンピュータシステム

（1）コンピュータ構成要素：プロセッサ、メモリ、バス、入出力デバイス、入出力装置
（2）システム構成要素：システムの構成、システムの評価指標
（3）ソフトウェア：オペレーティングシステム、ミドルウェア、ファイルシステム、開発ツール
（4）ハードウェア：ハードウェア

3. 技術要素

（1）ヒューマンインタフェース：ヒューマンインタフェース技術、インタフェース設計
（2）マルチメディア：マルチメディア技術、マルチメディア応用
（3）データベース：データベース方式、データベース設計、データ操作、トランザクション処理、データベース応用
（4）ネットワーク：ネットワーク方式、データ通信と制御、通信プロトコル、ネットワーク管理、ネットワーク応用
（5）セキュリティ：情報セキュリティ、情報セキュリティ管理、セキュリティ技術評価、情報セキュリティ対策、セキュリティ実装技術

4. 開発技術

（1）システム開発技術：システム要件定義、システム方式設計、ソフトウェア要件定義、ソフトウェア方式設計・ソフトウェア詳細設計、ソフトウェアコード作成及びテスト、ソフトウェア結合・ソフトウェア適格性確認テスト、システム結合・システム適格性テスト、ソフトウェア導入、ソフトウェア受入れ、ソフトウェア保守
（2）ソフトウェア開発管理技術：開発プロセス・手法、知的財産適用管理、開発環境管理、構成管理・変更管理

5. プロジェクトマネジメント

（1）プロジェクトマネジメント：プロジェクト統合マネジメント、プロジェクト・タイム・マネジメント、プロジェクト・コスト・マネジメント、プロジェクト品質マネジメント、プロジェクト人的資源マネジメント、プロジェクト・コミュニケーション・マネジメント、プロジェクト・リスク・マネジメント、プロジェクト調達マネジメント

6. サービスマネジメント

（1）サービスマネジメント：サービスマネジメント、運用設計・ツール、サービスサポート、サービスデリバリ、サービスマネジメント構築、ファシリティマネジメント
（2）システム監査：システム監査、内部統制

7. システム戦略

（1）システム戦略：情報システム戦略、業務プロセス、ソリューションビジネス、システム活用促進・評価
（2）システム企画：システム化計画、要件定義、調達計画・実施

8. 経営戦略

（1）経営戦略マネジメント：経営戦略手法、マーケティング、ビジネス戦略と目標・評価、経営管理システム
（2）技術戦略マネジメント：技術開発戦略の立案、技術開発計画
（3）ビジネスインダストリ：ビジネスシステム、エンジニアリングシステム、e-ビジネス、民生機器、産業機器

9. 企業と法務

（1）企業活動：経営・組織論、OR・IE、会計・財務
（2）法務：知的財産権、セキュリティ関連法規、労働関連・取引関連法規、その他の法律・ガイドライン・技術者倫理、標準化関連

URL:http://www.jitec.ipa.go.jp/1_13download/syllabus_ap_ver2_0.pdf

認定団体について

■ 情報処理推進機構 ■ 独立行政法人。「暮らしを支えるITの安全性・信頼性の向上」「国際競争に勝ち抜けるIT産業の創造」「世界で活躍できる優れたIT人材の育成」の三つをミッションに掲げる。国家試験である情報処理技術者試験を実施。

URL:http://www.ipa.go.jp/

設立年	2004年
所在国	日本
団体種別	独立行政法人
参加者	職員（169名）

国内/
国家資格

基本情報技術者

資格の概要

情報処理技術者試験は、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験である。情報システムを構築・運用する「技術者」から情報システムを利用する「エンドユーザ（利用者）」まで、ITに係わる全ての人を対象としたベンダーフリーの試験である。

「基本情報技術者」は、基本戦略立案又はITソリューション・製品・サービスを実現する業務に従事し、上位者の指導の下、需要者が直面する課題に対するITを活用した戦略立案への参加、もしくはシステムの設計・開発又は汎用製品の最適組合せによる、信頼性・生産性の高いシステムの構築、またはその安定的な運用サービスの実現に貢献する人材を認定する。

開始年度	2001年	実施団体名	独立行政法人 情報処理推進機構		
受験者数（H24春期）	52,582名	合格者数（H24春期）	12,437名	資格保持者数（平成21年度春期～）	227,917名
目的	基本戦略立案又はITソリューション・製品・サービスを実現する業務に従事し、上位者の指導の下、需要者が直面する課題に対するITを活用した戦略立案への参加、もしくはシステムの設計・開発又は汎用製品の最適組合せによる、信頼性・生産性の高いシステムの構築、またはその安定的な運用サービスの実現に貢献する人材を認定する。				
対象者像	高度IT人材となるために必要な基本的知識・技能をもち、実践的な活用能力を身に付けた者				
認定条件	情報処理技術者試験「基本情報技術者試験」への合格				
更新条件	なし				
URL	http://www.jitec.jp/1_11seido/fe.html				

活用状況

・企業における活用

社団法人情報サービス産業協会発行の「賃金データ」平成22年度調査によると回答企業116社中107社が、情報処理技術者試験の少なくとも一つ以上の試験区分に対して一時金又は資格手当を支給している。

・公的機関における活用

官公庁、地方公共団体の情報システム開発の競争入札参加申請（北海道、大分県、静岡県、岩手県など）において、申請書の一つに、情報処理技術者試験合格者数の記入を求めている。或いは、情報処理技術者試験合格者を雇用していることが要件の場合もある。

・国家試験などにおける優遇制度など

情報処理技術者試験合格者は教員採用選考試験（一部の県市）で試験の一部免除を実施。コンピュータ犯罪捜査官（警視庁）の応募資格の一つとなっている。

認知度・浸透度

・国家試験。昭和44年にプログラマを対象とした「情報処理技術者認定試験制度」を通商産業省告示により発足させ、第一種情報処理技術者認定試験と第二種情報処理技術者認定試験が実施。昭和45年に情報処理技術者試験が法制化。昭和59年より試験事務が公益法人に委譲。平成16年より「独立行政法人 情報処理推進機構（IPA）」に移管。

・株式会社日経BP IT Pro「いる資格、いらない資格」（http://itpro.nikkeibp.co.jp/article/COLUMN/20120412/390758/）にて、情報処理技術者試験の中で、ITベンダーの技術者が「取得済み」、「取得したい」資格第1位、ユーザー企業のシステム部長が自社のシステム部員に「取得させたい」資格第1位、システム部員が「取得済み」、「取得したい」資格第1位。

スキル要件・シラバス

受験条件　下位試験に「ITパスポート」があるが、当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　特定の製品やソフトウェアに関する試験ではなく、情報技術の背景として知るべき原理や基礎となる技能について、幅広い知識を総合的に評価する。出題形式は多肢選択式である。

1. 基礎理論

（1）基礎理論：離散数学、応用数学、情報に関する理論、通信に関する理論、計測・制御に関する理論
（2）アルゴリズムとプログラミング：データ構造、アルゴリズム、プログラミング、プログラム言語、その他の言語

2. コンピュータシステム

（1）コンピュータ構成要素：プロセッサ、メモリ、バス、入出力デバイス、入出力装置
（2）システム構成要素：システムの構成、システムの評価指標
（3）ソフトウェア：オペレーティングシステム、ミドルウェア、ファイルシステム、開発ツール
（4）ハードウェア：ハードウェア

3. 技術要素

（1）ヒューマンインタフェース：ヒューマンインタフェース技術、インタフェース設計
（2）マルチメディア：マルチメディア技術、マルチメディア応用
（3）データベース：データベース方式、データベース設計、データ操作、トランザクション処理、データベース応用
（4）ネットワーク：ネットワーク方式、データ通信と制御、通信プロトコル、ネットワーク管理、ネットワーク応用
（5）セキュリティ：情報セキュリティ、情報セキュリティ管理、セキュリティ技術評価、情報セキュリティ対策、セキュリティ実装技術

4. 開発技術

（1）システム開発技術：システム要件定義、システム方式設計、ソフトウェア要件定義、ソフトウェア方式設計・ソフトウェア詳細設計、ソフトウェアコード作成及びテスト、ソフトウェア結合・ソフトウェア適格性確認テスト、システム結合・システム適格性テスト、ソフトウェア導入、ソフトウェア受入れ、ソフトウェア保守
（2）ソフトウェア開発管理技術：開発プロセス・手法、知的財産適用管理、開発環境管理、構成管理・変更管理

5. プロジェクトマネジメント

（1）プロジェクトマネジメント：プロジェクト統合マネジメント、プロジェクト・タイム・マネジメント、プロジェクト・コスト・マネジメント、プロジェクト品質マネジメント、プロジェクト人的資源マネジメント、プロジェクト・コミュニケーション・マネジメント、プロジェクト・リスク・マネジメント、プロジェクト調達マネジメント

6. サービスマネジメント

（1）サービスマネジメント：サービスマネジメント、運用設計・ツール、サービスサポート、サービスデリバリ、サービスマネジメント構築、ファシリティマネジメント
（2）システム監査：システム監査、内部統制

7. システム戦略

（1）システム戦略：情報システム戦略、業務プロセス、ソリューションビジネス、システム活用促進・評価
（2）システム企画：システム化計画、要件定義、調達計画・実施

8. 経営戦略

（1）経営戦略マネジメント：経営戦略手法、マーケティング、ビジネス戦略と目標・評価、経営管理システム
（2）技術戦略マネジメント：技術開発戦略の立案、技術開発計画
（3）ビジネスインダストリ：ビジネスシステム、エンジニアリングシステム、e-ビジネス、民生機器、産業機器

9. 企業と法務

（1）企業活動：経営・組織論、OR・IE、会計・財務
（2）法務：知的財産権、セキュリティ関連法規、労働関連・取引関連法規、その他の法律・ガイドライン・技術者倫理、標準化関連

URL:http://www.jitec.ipa.go.jp/1_13download/syllabus_fe_ver2_0.pdf

認定団体について

■ 情報処理推進機構 ■　独立行政法人。「暮らしを支えるITの安全性・信頼性の向上」「国際競争に勝ち抜けるIT産業の創造」「世界で活躍できる優れたIT人材の育成」の三つをミッションに掲げる。国家試験である情報処理技術者試験を実施。

URL:http://www.ipa.go.jp/

設立年	2004年
所在国	日本
団体種別	独立行政法人
参加者	職員（169名）

国内/
国家資格

ITパスポート

資格の概要

情報処理技術者試験は、「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験である。情報システムを構築・運用する「技術者」から情報システムを利用する「エンドユーザ（利用者）」まで、ITに係わる全ての人を対象としたベンダーフリーの試験である。

「ITパスポート」は、職業人として備えておくべき、情報技術に関する共通的な基礎知識を習得した者であり、担当する業務に対して情報技術を活用し、「利用する情報機器及びシステムの把握、活用」、「担当業務の理解、その業務における問題の把握及び必要な解決の実行」、「安全な情報の収集や活用」、「上位者の指導の下での、業務の分析やシステム化の支援」等の活動を行う人材を認定する。

開始年度	2009年	実施団体名	独立行政法人 情報処理推進機構		
受験者数（H24春期）	48,482名	合格者数（H24春期）	21,714名	資格保持者数（平成21年度春期～）	72,352名
目的	職業人として備えておくべき、情報技術に関する共通的な基礎知識を習得した者であり、担当する業務に対して情報技術を活用し、「利用する情報機器及びシステムの把握、活用」、「担当業務の理解、その業務における問題の把握及び必要な解決の実行」、「安全な情報の収集や活用」、「上位者の指導の下での、業務の分析やシステム化の支援」等の活動を行う人材を認定する。				
対象者像	職業人が共通に備えておくべき情報技術に関する基礎的な知識をもち、情報技術に携わる業務に就くか、担当業務に対して情報技術を活用していこうとする者				
認定条件	情報処理技術者試験「ITパスポート試験」への合格				
更新条件	なし				
URL	http://www.jitec.jp/1_11seido/ip.html				

活用状況

・企業における活用

社団法人情報サービス産業協会発行の「賃金データ」平成22年度調査によると回答企業116社中107社が、情報処理技術者試験の少なくとも一つ以上の試験区分に対して一時金又は資格手当を支給している。

・公的機関における活用

官公庁、地方公共団体の情報システム開発の競争入札参加申請（北海道、大分県、静岡県、岩手県など）において、申請書の一つに、情報処理技術者試験合格者数の記入を求めている。或いは、情報処理技術者試験合格者を雇用していることが要件の場合もある。

・国家試験などにおける優遇制度など

情報処理技術者試験合格者は教員採用選考試験（一部の県市）で試験の一部免除を実施。コンピュータ犯罪捜査官（警視庁）の応募資格の一つとなっている。

認知度・浸透度

・国家試験。昭和44年にプログラマを対象とした「情報処理技術者認定試験制度」を通商産業省告示により発足させ、第一種情報処理技術者認定試験と第二種情報処理技術者認定試験が実施。昭和45年に情報処理技術者試験が法制化。昭和59年より試験事務が公益法人に委譲。平成16年より「独立行政法人 情報処理推進機構（IPA）」に移管。

・株式会社日経BP IT Pro「いる資格、いらない資格」（http://itpro.nikkeibp.co.jp/article/COLUMN/20120412/390758/）にて、情報処理技術者試験の中で、ITベンダーの人事担当者が、ユーザー企業のシステム部員に「取得してほしい」資格第1位、ユーザー企業のシステム部長が自社のシステム部員に「取得させたい」資格第2位、システム部員が「取得済み」の資格第3位。

スキル要件・シラバス

受験条件　当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　特定の製品やソフトウェアに関する試験ではなく、情報技術の背景として知るべき原理や基礎となる技能について、幅広い知識を総合的に評価する。出題形式は多肢選択式である。

1. 企業と法務

（1）企業活動：経営・組織論、OR・IE、会計・財務
（2）法務：知的財産権、セキュリティ関連法規、労働関連・取引関連法規、その他の法律・ガイドライン・技術者倫理、標準化関連

2. 経営戦略

（1）経営戦略マネジメント：経営戦略手法、マーケティング、ビジネス戦略と目標・評価、経営管理システム
（2）技術戦略マネジメント：技術開発戦略の立案・技術開発計画
（3）ビジネスインダストリ：ビジネスシステム、エンジニアリングシステム、e-ビジネス、民生機器、産業機器

3. システム戦略

（1）システム戦略：情報システム戦略、業務プロセス、ソリューションビジネス、システム活用促進・評価
（2）システム企画：システム化計画、要件定義、調達計画・実施

4. 開発技術

（1）システム開発技術：システム開発技術
（2）ソフトウェア開発管理技術：開発プロセス・手法

5. プロジェクトマネジメント

（1）プロジェクトマネジメント：プロジェクトマネジメント

6. サービスマネジメント

（1）サービスマネジメント：サービスマネジメント、サービスサポート、ファシリティマネジメント
（2）システム監査：システム監査、内部統制

7. 基礎理論

（1）基礎理論：離散数学、応用数学、情報に関する理論、通信に関する理論
（2）アルゴリズムとプログラミング：データ構造、アルゴリズム、プログラミング・プログラム言語、その他の言語

8. コンピュータシステム

（1）コンピュータ構成要素：プロセッサ、メモリ、入出力デバイス
（2）システム構成要素：システムの構成、システムの評価指標
（3）ソフトウェア：オペレーティングシステム、ミドルウェア、ファイルシステム、開発ツール、オープンソースソフトウェア
（4）ハードウェア：ハードウェア（コンピュータ・入出力装置）

9. 技術要素

（1）ヒューマンインタフェース：ヒューマンインタフェース技術、インタフェース設計
（2）マルチメディア：マルチメディア技術、マルチメディア応用
（3）データベース：データベース方式、データベース設計、データ操作、トランザクション処理
（4）ネットワーク：ネットワーク方式、通信プロトコル、ネットワーク応用
（5）セキュリティ：情報セキュリティ、情報セキュリティ管理、情報セキュリティ対策・情報セキュリティ実装技術

URL:http://www.jitec.ipa.go.jp/1_13download/syllabus_ip_ver2_0.pdf

認定団体について

■ 情報処理推進機構 ■ 独立行政法人。「暮らしを支えるITの安全性・信頼性の向上」「国際競争に勝ち抜けるIT産業の創造」「世界で活躍できる優れたIT人材の育成」の三つをミッションに掲げる。国家試験である情報処理技術者試験を実施。

URL:http://www.ipa.go.jp/

設立年	2004年
所在国	日本
団体種別	独立行政法人
参加者	職員（169名）

国内/
民間資格

CSBM
（Certified Security Basic Master）

資格の概要

日本発のベンダーニュートラルなセキュリティ資格である。セキュリティ・リーダを目指す人材のために、情報セキュリティ全般の知識(IPA情報セキュリティスキルマップのレベル1)を網羅した教育を行う。また、ITスキル標準(ITSS)の情報セキュリティ分野レベル2～3に対応した教育となっている。日々のオペレーションに情報機器を使う人から、高度なネットワークの設計・構築・運用をする人まで、情報セキュリティ知識を効果的に修得することが可能である。
主に経験2～3年のITエンジニアを対象としているが、IT企業ではセキュリティの広範な知識は技術者以外の職種にも必要な知識であることから、営業やマーケティングの人材の受験実績もある。

開始年度	2009年	実施団体名	SEA/J		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年8月現在）	6,055名
目的	セキュリティ・リーダを目指す人のために、情報セキュリティ全般の知識(下図：IPA情報セキュリティスキルマップのレベル1)を網羅した教育を行う。				
対象者像	情報セキュリティに関係する初級技術者およびシステム関係企業の従業員				
認定条件	CSBM（Certified Security Basic Master）試験の合格				
更新条件	なし				
URL	http://www.sea-j.net/curriculum/basic.html				

活用状況

・官公庁の入札案件に、作業者の必要セキュリティ資格の一つとして記載されることもあるほか、ISMS審査員などの継続研修として利用されている。（http://allabout.co.jp/gm/gc/52719/2/）

認知度・浸透度

・情報セキュリティ教育事業者連絡会（ISEPA）「情報セキュリティ資格マップ」（2011年5月）に掲載
http://www.jnsa.org/isepa/outputs/research.html
・内閣官房「人材育成・資格制度体系化専門委員会報告書(2007年1月23日)」で「主な情報セキュリティ資格」として取り上げられている。

スキル要件・シラバス

受験条件　当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　情報セキュリティ全般の知識(IPA情報セキュリティスキルマップのレベル1)を網羅、ITスキル標準(ITSS)の情報セキュリティ分野レベル2～3に対応した教育となっている。

1. 情報セキュリティマネジメント	**9. 認証**
情報セキュリティの構成要素、情報セキュリティマネジメントシステム 、リスク 、情報セキュリティポリシー 、教育・訓練、情報セキュリティ監査	ID管理と認証、パスワード認証、バイオメトリクス認証、認証デバイス 、認証プロトコル、シングルサインオン、アクセス制御手法
2. セキュリティ運用	**10. プログラミング**
物理的セキュリティ、人的セキュリティ	プログラム、言語、バッファオーバーフロー、オブジェクト指向技術
3. インフラセキュリティ	**11. 不正プログラム**
TCP/IP基礎、VPN、無線LAN	不正プログラムの種類 、不正プログラムの感染経路、不正プログラムの活動、検出方法
4. 不正アクセス	**12. 暗号**
犯罪との関係、情報収集、不正侵入	暗号の基礎知識、共通鍵暗号、公開鍵暗号、その他の暗号
5. ファイアウォール	**13. 電子署名**
ファイアウォールの概念、ネットワークアクセスコントロール、NA、ファイアウォールの導入・運用	電子署名の必要性、改ざん検知、電子署名の仕組み
6. 侵入検知	**14. PKI**
IDS概要、IDSの構成、検知アルゴリズム、関連技術	電子証明書、認証局、PKI
7. アプリケーションセキュリティ	**15. セキュリティプロトコル**
DNS、電子メール、Web	セキュリティプロトコル、代表的なセキュリティプロトコル
8. OSセキュリティ	**16. 法令・規格**
サービス管理、ファイルシステム管理、アカウント管理、ネットワーク保護、修正プログラム管理、ログ管理、監査機能、TrustedOS	標準規格、法令

URL:http://www.sea-j.net/curriculum/basic.html

認定団体について

■ SEA/J ■　日本における情報セキュリティ知識の普及と技術者育成を目的とし、"情報セキュリティ教育には製品やベンダーに偏らない体系的なプログラムが必要である"との考えに賛同したセキュリティベンダー等によって共同で設立された団体。
正会員はITベンダー、システムプロバイダ、インテグレータなど計7社。日本独自の体系的な教育プログラムを開発し、「認定教育コース」と「認定資格試験」を提供する。

URL:http://www.sea-j.net/about/index.html

設立年	2002年
所在国	日本
団体種別	任意団体
参加者	正会員7社

国内/
民間資格

CSPM of Technical
（Certified Security Professional Master OF Technical）

資格の概要

Certified Security Professional Master(CSPM)OF Technicalは、日本発のベンダーニュートラルなセキュリティ資格である。ネットワークセキュリティのシステム構築・運用を実施する人のために、情報セキュリティテクニカル系の知識（IPA情報セキュリティスキルマップのレベル2）に対応した教育を行う。また、ITスキル標準（ITSS）の情報セキュリティ分野レベル2～4に対応した教育となっている。ファイアウォール、侵入検知システム、VPNなどのアクセスコントロールや機密性確保に必要な知識を習得する。

開始年度	2009年	実施団体名	SEA/J		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年8月現在）	650名
目的	ネットワークセキュリティのシステム構築・運用を実施する人のために、情報セキュリティテクニカル系の知識（IPA情報セキュリティスキルマップのレベル2）に対応した教育を行う。				
対象者像	システム/セールスエンジニア、情報システム管理者、ITコンサルタント				
認定条件	Certified Security Professional Master(CSPM)OF Technical試験の合格				
更新条件	なし				
URL	http://www.sea-j.net/curriculum/technical.html				

活用状況

・官公庁の入札案件に、作業者の必要セキュリティ資格の一つとして記載されることもあるほか、ISMS審査員などの継続研修として利用されている。（http://allabout.co.jp/gm/gc/52719/2/）

認知度・浸透度

・情報セキュリティ教育事業者連絡会（ISEPA）「情報セキュリティ資格マップ」（2011年5月）に掲載
http://www.jnsa.org/isepa/outputs/research.html
・内閣官房「人材育成・資格制度体系化専門委員会報告書(2007年1月23日)」で「主な情報セキュリティ資格」として取り上げられている。

スキル要件・シラバス

受験条件　当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　分野は情報セキュリティテクニカル系の知識(IPA情報セキュリティスキルマップのレベル2)に対応し、レベルはITスキル標準(ITSS)の情報セキュリティ分野レベル2～4に対応した教育となっている。

1. 脅威	**6. アプリケーション Web**
セキュリティ事故と犯罪の関係（インシデント事例、原因と対策）、調査・不正アクセス（不正アクセスの対象、対象の洗い出し、情報収集）。情報漏洩、攻撃手法（プログラム不備の悪用、パスワードの不正入手、攻撃手法の多様化）、アクセスコントロール	Webサービスの仕組み（静的コンテンツと動的コンテンツ、Webアプリケーション、セッション管理）、Webサーバの実装、アクセスログの解析
2. OS Windows	**7. ファイアウォール設計**
Windows OSの特徴、Windows ネットワーク（Windowsネットワークの機能、Windowsネットワークで使用されるプロトコル、匿名接続）、統合管理機能、サービスの管理、アカウント管理、ファイルシステム、セキュリティポリシー機能、アップデート	ファイアウォールポリシー設計、ネットワークにおけるセキュリティ（ファイアウォールの種類と技術、各サーバや装置の配置）
3. OS UNIX	**8. IDS運用**
UNIX OSの特徴、プロセスの管理、サービスの起動と停止、アカウント管理、パーミッション、セキュアOS	導入目的の明確化、NIDSとHIDSの違い、運用
4. アプリケーション DNS	**9. VPN**
DNSの構造と名前解決、DNSの実装、DNSにおけるセキュリティ（キャッシュの書き換え、ゾーン転送の制限、DDoS、DNSサーバ認証、サーバの設置場所）	VPNの要素と種類（VPNを構成する要素、カプセル化、VPNの種類）、セキュリティプロトコルの種類、IPsec（暗号化と認証、IPsecのモード、セッションの管理情報、鍵管理プロトコル、NAPTとの関係）
5. アプリケーション メール	**10. PKI**
電子メール配信の仕組み、電子メールサーバの実装、電子メールの不正中継、電子メール配信におけるセキュリティ	PKIを構成する要素、認証局、電子証明書の検証

URL:http://www.sea-j.net/curriculum/basic.html

認定団体について

■ SEA/J ■　日本における情報セキュリティ知識の普及と技術者育成を目的とし、"情報セキュリティ教育には製品やベンダーに偏らない体系的なプログラムが必要である"との考えに賛同したセキュリティベンダー等によって共同で設立された団体。
正会員はITベンダー、システムプロバイダ、インテグレータなど計7社。日本独自の体系的な教育プログラムを開発し、「認定教育コース」と「認定資格試験」を提供する。

URL:http://www.sea-j.net/about/index.html

設立年	2002年
所在国	日本
団体種別	任意団体
参加者	正会員7社

国内/
民間資格

CSPM of Management
（Certified Security Professional Master OF Management）

資格の概要

Certified Security Professional Master(CSPM)OF Managementは、日本発のベンダーニュートラルなセキュリティ資格である。セキュリティ・マネジメントを実施する人のために、情報セキュリティマネジメント系の知識（IPA情報セキュリティスキルマップのレベル2～3）に対応した教育を行う。また、ITスキル標準（ITSS）の情報セキュリティ分野レベル2～4に対応した教育となっている。情報セキュリティマネジメント・リスク分析の考え方や、情報セキュリティポリシー策定の基本、対策計画を立てるために必要な知識を習得する。

開始年度	2009年	実施団体名	SEA/J		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年8月現在）	497名
目的	セキュリティ・マネジメントを実施する人のために、情報セキュリティマネジメント系の知識（IPA情報セキュリティスキルマップのレベル2～3）に対応した教育を行う。				
対象者像	情報システム管理者、セキュリティ監査員、法務担当				
認定条件	Certified Security Professional Master(CSPM)OF Management試験の合格				
更新条件	なし				
URL	http://www.sea-j.net/curriculum/management.html				

活用状況

・官公庁の入札案件に、作業者の必要セキュリティ資格の一つとして記載されることもあるほか、ISMS審査員などの継続研修として利用されている。（http://allabout.co.jp/gm/gc/52719/2/）

認知度・浸透度

・情報セキュリティ教育事業者連絡会（ISEPA）「情報セキュリティ資格マップ」（2011年5月）に掲載
http://www.jnsa.org/isepa/outputs/research.html
・内閣官房「人材育成・資格制度体系化専門委員会報告書(2007年1月23日)」で「主な情報セキュリティ資格」として取り上げられている。

スキル要件・シラバス

受験条件　当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　分野は情報セキュリティマネジメント系の知識（IPA情報セキュリティスキルマップのレベル2～3）に対応し、レベルはITスキル標準（ITSS）の情報セキュリティ分野レベル2～4に対応した教育となっている。

1. 情報セキュリティとは何か	7. 詳細リスク分析
セキュリティには2つの意味がある、何をセキュアする（安全にする）のか、情報セキュリティの種類、物理的セキュリティと論理的セキュリティ	詳細リスク分析の手順、情報資産を分類する、分類のときに持つべき「目」、情報資産調査の準備をする、どこまで情報資産調査を行うのか、情報資産をカテゴライズする、情報資産調査表のまとめ方、脅威と脆弱性・管理策、リスクの大きさの評価、どの手法を使うか
2. 情報セキュリティーの構成要素	8. リスクマネジメント
情報セキュリティのCIA、機密性[Confidential]とは？、完全性[Integrity]とは？、可用性[Availability]とは？、真正性[Authenticity]とは？、責任追跡性[Accountability]とは？、信頼性[Reliability]とは？、3大要素のバランスと活用、情報セキュリティ対策の考え方、情報セキュリティ対策の4つの機能、「抑止機能」脆弱さをカバーする環境作り、「防衛機能」抑止できない脅威からの防御、「検知機能」トラブルをいち早く察知し被害を最小限に食い止める、「回復機能」機能とデータを速やかに修復	リスクマネジメントのプロセス、リスク処理の概要、リスクコントロールの手法、リスクファイナンスの手法
3. 脅威と脆弱性	9. 情報セキュリティポリシーの概要
100%のセキュリティはありえない、「地震、雷、障害、オヤジ …」、人ほど怖いものはない、ソーシャルエンジニアリングの脅威、クリアデスク・クリアスクリーン	「ルール」がセキュリティを作る、内的効果と外的効果、セキュリティポリシーが果たす役割、情報セキュリティーポリシーの位置付け、情報セキュリティーの構成
4. 情報セキュリティマネジメント	10. 情報セキュリティポリシーの策定
情報セキュリティにおける「PDCAサイクル」、さまざまな情報セキュリティマネジメント	策定のための委員会を設置する、情報セキュリティポリシーの策定手順、策定において注意すべきこと
5. リスクの概念	11. 情報セキュリティ監査制度
情報セキュリティにおけるリスクとは、期待される効果が得られないとき、損失には3つのタイプがある、リスクを構成する要素 ●事例● 個人情報漏えいで「32億円」 ・JOモデルと使って想定損害賠償額を計算する ・宇治市事故と想定損害賠償額	うわべだけのセキュリティ対策になっていないか、監査なきセキュリティは無意味である、3本柱で信頼ある監査を、情報セキュリティ監査制度、監査が情報セキュリティマネジメントを高める、情報セキュリティ管理基準、「JIS X 5080」と「情報セキュリティ管理基準」 、組織にあった個別の管理基準、我が社の管理基準を策定する、コントロールを選定する、「現実的かつ理想的」がコントロール選定の目安、サブコントロールを選定する、「サブコントロールは、具体的な表現で 」、技術的検証の必要性、個別の管理基準を完成させる、個別管理基準を使いやすく分類する、個別管理基準を利用する前に、技術的検証と監査結果を活用するために 、外部監査の利点
6. リスク分析の概要	12. 情報セキュリティ関連法規
リスク分析の必要性、リスク分析の目的と効果、リスク分析の種類、ベースラインアプローチ、非形式アプローチ、詳細リスク分析、組み合わせアプローチ	電子計算機損壊等業務妨害、電子計算機使用詐欺、不正アクセス禁止法、電子署名法、個人情報保護法、知的財産権、工業所有権に関する法律、特許法、著作権法、不正競争防止法、その他の法律

URL:http://www.sea-j.net/curriculum/basic.html

認定団体について

■ SEA/J ■　日本における情報セキュリティ知識の普及と技術者育成を目的とし、“情報セキュリティ教育には製品やベンダーに偏らない体系的なプログラムが必要である”との考えに賛同したセキュリティベンダー等によって共同で設立された団体。
正会員はITベンダー、システムプロバイダ、インテグレータなど計7社。日本独自の体系的な教育プログラムを開発し、「認定教育コース」と「認定資格試験」を提供する。

URL:http://www.sea-j.net/about/index.html

設立年	2002年
所在国	日本
団体種別	任意団体
参加者	正会員7社

国内/
民間資格

公認情報セキュリティ主任監査人

資格の概要

経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、資格を認定する。「公認情報セキュリティ監査人」の資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められる。

開始年度	2004年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2013年2月時点、登録者数）	57名
目的	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査チームを編成し監査を実施する場合に監査チームリーダとなって、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、公認情報セキュリティ監査人がOJTとして監査チームリーダを務める場合は、これを指導し評価する。				
対象者像	民間企業や政府、地方自治体等の情報セキュリティ対策の監査を目的とする者				
認定条件	• 情報技術分野で少なくとも4年以上の業務経験があること。その内、情報セキュリティ関連分野で少なくとも2年以上の業務経験があることが必須であり、その業務経験内容について推薦者の推薦文・署名を記した「業務経験及び監査実施経験に対する推薦書」を提出することにより、情報セキュリティ監査を実施するために必要な専門分野の前提知識を備えていることを証明する。（なお、他資格の保有で情報セキュリティ関連分野の業務経験を代替することも可能とする。） • 協会認定の2日間研修コースを受講、履修し協会所定の研修終了試験に合格すること。 • 協会認定の3日間トレーニングコースを履修し協会所定のトレーニング終了試験に合格すること。 • 協会認定の監査経験確認試験に合格すること。 • 過去3年以内に最低4回延べ20日間の監査メンバーとしての監査実施経験（うち2回以上は情報セキュリティ監査制度に基づく助言型監査又は保証型監査）があること。 • 過去2年以内に最低3回延べ15日間は、主任情報セキュリティ監査人の指導のもとでの監査チームリーダとしての監査実施経験（うち2回以上は情報セキュリティ監査制度に基づく助言型監査又は保証型監査）があること。 • 「公認情報セキュリティ監査人」の実証能力に加えて、資格認定委員会委員による面接審査に合格すること。 ※内部監査人資格を取得済みの場合、2007年4月末日までに小論文試験を受験し、トレーニングを修了したと認定された者はこの限りではない。				
更新条件	有効期間は年度を前期（4月1日から9月30日）と後期（10月1日から3月31日）に分け、資格認定月を基準にして3年後の当該半期の末日まで。資格維持には、活動実績をポイント換算し、一定水準以上を満たす必要がある。				
URL	http://www.jasa.jp/qualification/about.html				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・監査人資格制度は、ISO/IEC17024（適合性評価－要員の認証を実施する機関に対する一般要求事項）に則っている

スキル要件・シラバス

受験条件

「認定条件」の欄を参照。

出題範囲

監査人として必要とされる情報セキュリティ監査の基本的な知識と、情報セキュリティ監査の「実践に必要な知識」を備えていることを問う。出題形式は筆記試験（多肢選択式、論述式）である。また、「実証された能力」を問うために、面接審査を行う。

1. 協会認定研修

- 情報セキュリティ監査概論
  監査の概念、監査におけるリスク、情報セキュリティ監査の概念と定義
- 情報セキュリティ監査の基準
  情報セキュリティ監査基準、情報セキュリティ管理基準
- 情報セキュリティ監査の技法
  監査技法の種類、監査手続、監査証拠、リスク分析と成熟度モデル
- 情報セキュリティ監査のプロセス
  監査実施まで、契約フェーズ、方針フェーズ、計画フェーズ、実施フェーズ、意見フェーズ、報告フェーズ、その他

2. 協会認定トレーニング

- 監査を実施するために必要な情報を収集し、理解すること
- 監査手続を作成すること
- 監査チェックリストを作成すること
- 監査技法（ヒアリング、閲覧、観察、再実施）、技術的検証を用いて監査を実施すること
- 報告書作成に必要かつ十分な証跡を収集すること
- 適切な監査報告書を作成すること

3. 監査経験確認

- 情報セキュリティ監査の各プロセスにおいて、いずれかのプロセスの実施内容につき説明
  - ➢ その監査プロセスにおいて重要な事項（キーワード）を含んでいること
  - ➢ 記述の論旨が一貫していること。
  - ➢ 題意に沿った記述になっていること（記述を求められているプロセスについて記述していることが必要）
- 経験を踏まえた自身の考え
  - ➢ 監査人としてどのような監査を行うべきか
  - ➢ 情報セキュリティ監査はどうあるべきかなど

4. 面接

- 資格制度運営細則 第8条3. 公認情報セキュリティ主任監査人「実証された能力」を確認

URL:http://www.jasa.jp/qualification/acquisition.html?key=lead_auditor

認定団体について

■日本セキュリティ監査協会■ 特定非営利活動法人。2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行され、この制度を着実に浸透させていくための運営体として設立。

http://www.jasa.jp/index.html/

設立年	2003年
所在国	日本
団体種別	特定非営利活動法人
参加者	53団体（正会員） ※2011年4月時点

国内/
民間資格

公認情報セキュリティ監査人

資格の概要

経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、資格を認定する。「公認情報セキュリティ監査人」の資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められる。

開始年度	2004年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2013年2月時点、登録者数）	129名
目的	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、上位の監査人の指導のもとで、OJTとして監査チームリーダを務め、経験を積んで、公認情報セキュリティ主任監査人をめざすことができる。加えて、情報セキュリティ監査人補がOJTとして監査に参加している場合は、これを指導し評価する。				
対象者像	民間企業や政府、地方自治体等の情報セキュリティ対策の監査を目的とする者				
認定条件	• 情報技術分野で少なくとも4年以上の業務経験があること。その内、情報セキュリティ関連分野で少なくとも2年以上の業務経験があることが必須であり、その業務経験内容について推薦者の推薦文・署名を記した「業務経験及び監査実施経験に対する推薦書」を提出することにより、情報セキュリティ監査を実施するために必要な専門分野の前提知識を備えていることを証明する。（なお、他資格の保有で情報セキュリティ関連分野の業務経験を代替することも可能とする。） • 協会認定の2日間研修コースを受講、履修し協会所定の研修終了試験に合格すること。 • 協会認定の3日間トレーニングコースを履修し協会所定のトレーニング終了試験に合格すること。 • 協会認定の監査経験確認試験に合格すること。 • 過去3年以内に最低4回延べ20日間の監査メンバーとしての監査実施経験（うち2回以上は情報セキュリティ監査制度に基づく助言型監査又は保証型監査）があること。 • 監査人、主任監査人、主席監査人又は協会会員からの推薦があること。（会員企業の社員は推薦は不要） ※内部監査人資格を取得済みの場合、2007年4月末日までに小論文試験を受験し、トレーニングを修了したと認定された者はこの限りではない。				
更新条件	有効期間は年度を前期（4月1日から9月30日）と後期（10月1日から3月31日）に分け、資格認定月を基準にして3年後の当該半期の末日まで。資格維持には、活動実績をポイント換算し、一定水準以上を満たす必要がある。				
URL	http://www.jasa.jp/qualification/about.html				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・監査人資格制度は、ISO/IEC17024（適合性評価－要員の認証を実施する機関に対する一般要求事項）に則っている

スキル要件・シラバス

受験条件

「認定条件」の欄を参照。

出題範囲

監査人として必要とされる情報セキュリティ監査の基本的な知識と、情報セキュリティ監査の「実践に必要な知識」を備えていることを問う。出題形式は筆記試験（多肢選択式、論述式）である。

1. 協会認定研修

- 情報セキュリティ監査概論
  監査の概念、監査におけるリスク、情報セキュリティ監査の概念と定義
- 情報セキュリティ監査の基準
  情報セキュリティ監査基準、情報セキュリティ管理基準
- 情報セキュリティ監査の技法
  監査技法の種類、監査手続、監査証拠、リスク分析と成熟度モデル
- 情報セキュリティ監査のプロセス
  監査実施まで、契約フェーズ、方針フェーズ、計画フェーズ、実施フェーズ、意見フェーズ、報告フェーズ、その他

2. 協会認定トレーニング

- 監査を実施するために必要な情報を収集し、理解すること
- 監査手続を作成すること
- 監査チェックリストを作成すること
- 監査技法（ヒアリング、閲覧、観察、再実施）、技術的検証を用いて監査を実施すること
- 報告書作成に必要かつ十分な証跡を収集すること
- 適切な監査報告書を作成すること

3. 監査経験確認

- 情報セキュリティ監査の各プロセスにおいて、いずれかのプロセスの実施内容につき説明
  - その監査プロセスにおいて重要な事項（キーワード）を含んでいること
  - 記述の論旨が一貫していること。
  - 題意に沿った記述になっていること（記述を求められているプロセスについて記述していることが必要）
- 経験を踏まえた自身の考え
  - 監査人としてどのような監査を行うべきか
  - 情報セキュリティ監査はどうあるべきかなど

URL:http://www.jasa.jp/qualification/acquisition.html?key=auditor

認定団体について

■日本セキュリティ監査協会■ 特定非営利活動法人。2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行され、この制度を着実に浸透させていくための運営体として設立。

http://www.jasa.jp/index.html/

設立年	2003年
所在国	日本
団体種別	特定非営利活動法人
参加者	53団体（正会員） ※2011年4月時点

国内/
民間資格

情報セキュリティ監査人補

資格の概要

経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、資格を認定する。「情報セキュリティ監査人補」の資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められる。

開始年度	2004年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2013年2月時点、登録者数）	323名
目的	情報セキュリティ監査制度に対する知識と経験を有し、OJTとして監査に参加する。監査経験を積んで、公認情報セキュリティ監査人をめざすことができる。				
対象者像	民間企業や政府、地方自治体等の情報セキュリティ対策の監査を目的とする者				
認定条件	• 協会認定の2日間研修コースを受講、履修し協会所定の研修終了試験に合格すること。 • 協会認定の3日間トレーニングコースを履修し協会所定のトレーニング修了試験に合格すること。 ※内部監査人資格を取得済みの場合、2007年4月末日までに小論文試験を受験し、トレーニングを修了したと認定された者はこの限りではない。				
更新条件	有効期間は年度を前期（4月1日から9月30日）と後期（10月1日から3月31日）に分け、資格認定月を基準にして3年後の当該半期の末日まで。資格維持には、活動実績をポイント換算し、一定水準以上を満たす必要がある。 ·監査実績 情報セキュリティに関連する外部監査への従事 情報セキュリティに関連する内部監査への従事 ·監査人の学習 JASAが主催する研修・セミナー等の受講、JASA会員・後援団体が主催する研修・セミナー等の受講、他の団体が主催し、協会が認める研修・セミナー等の受講、協会が認める自己学習等 ※上記いずれも情報セキュリティ監査、情報セキュリティに関する研修、セミナーであること。 ·社会貢献 委員会・タスク・WG活動への参加、協会が主催、または、協会が認める講演・講師活動、協会が公募する課題に応募、協会活動が求める研究等の成果物作成に貢献、協会が主催するその他の社会貢献活動、その他、協会が社会貢献に意義があると認める活動の実施				
URL	http://www.jasa.jp/qualification/about.html				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・監査人資格制度は、ISO/IEC17024（適合性評価ー要員の認証を実施する機関に対する一般要求事項）に則っている

スキル要件・シラバス

受験条件

「認定条件」の欄を参照。

出題範囲

監査人として必要とされる情報セキュリティ監査の基本的な知識と、情報セキュリティ監査の「実践に必要な知識」を備えていることを問う。出題形式は筆記試験（多肢選択式）である。

1. 協会認定研修

- 情報セキュリティ監査概論
  監査の概念、監査におけるリスク
- 情報セキュリティ監査の概念と定義
- 情報セキュリティ監査の基準
  情報セキュリティ監査基準、情報セキュリティ管理基準
- 情報セキュリティ監査の技法
  監査技法の種類、監査手続、監査証拠、リスク分析と成熟度モデル
- 情報セキュリティ監査のプロセス
  監査実施まで、契約フェーズ、方針フェーズ、計画フェーズ、実施フェーズ、意見フェーズ、報告フェーズ、その他

2. 協会認定トレーニング

- 監査を実施するために必要な情報を収集し、理解すること
- 監査手続を作成すること
- 監査チェックリストを作成すること
- 監査技法（ヒアリング、閲覧、観察、再実施）、技術的検証を用いて監査を実施すること
- 報告書作成に必要かつ十分な証跡を収集すること
- 適切な監査報告書を作成すること

URL: http://www.jasa.jp/qualification/acquisition.html?key=assistant&step=1

認定団体について

■ 日本セキュリティ監査協会 ■ 特定非営利活動法人。2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行され、この制度を着実に浸透させていくための運営体として設立。

http://www.jasa.jp/index.html/

設立年	2003年
所在国	日本
団体種別	特定非営利活動法人
参加者	53団体（正会員） ※2011年4月時点

国内/
民間資格

情報セキュリティ監査人アソシエイト

資格の概要

経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、資格を認定する。「情報セキュリティ監査アソシエイト」の資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められる。

開始年度	2004年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2013年3月時点、登録者数）	322名
目的	監査チームリーダの要請によりチームの一員として専門知識にもとづく助言を行う。				
対象者像	民間企業や政府、地方自治体等の情報セキュリティ対策の監査を目的とする者				
認定条件	• 専門分野（分野は問わない）での3年以上の業務経験を有すること、又は業務経験を代替する資格を保有すること。 • 協会認定の2日間研修コースを受講、履修し協会所定の研修終了試験に合格すること。 ※内部監査人資格を取得済みの場合、2007年4月末日までに小論文試験を受験し、トレーニングを修了したと認定された者はこの限りではない。				
更新条件	有効期間は年度を前期（4月1日から9月30日）と後期（10月1日から3月31日）に分け、資格認定月を基準にして3年後の当該半期の末日まで。資格維持には、活動実績をポイント換算し、一定水準以上を満たす必要がある。 ·監査実績 情報セキュリティに関連する外部監査への従事 情報セキュリティに関連する内部監査への従事 ·監査人の学習 JASAが主催する研修・セミナー等の受講、JASA会員・後援団体が主催する研修・セミナー等の受講、他の団体が主催し、協会が認める研修・セミナー等の受講、協会が認める自己学習等 ※上記いずれも情報セキュリティ監査、情報セキュリティに関する研修、セミナーであること。 ·社会貢献 委員会・タスク・WG活動への参加、協会が主催、または、協会が認める講演・講師活動、協会が公募する課題に応募、協会活動が求める研究等の成果物作成に貢献、協会が主催するその他の社会貢献活動、その他、協会が社会貢献に意義があると認める活動の実施				
URL	http://www.jasa.jp/qualification/about.html				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・監査人資格制度は、ISO/IEC17024（適合性評価－要員の認証を実施する機関に対する一般要求事項）に則っている

スキル要件・シラバス

受験条件　「認定条件」の欄を参照。

出題範囲　監査人として必要とされる情報セキュリティ監査の基本的な知識と、情報セキュリティ監査の「実践に必要な知識」を備えていることを問う。出題形式は筆記試験（多肢選択式）である。

1. 協会認定研修

1. 情報セキュリティ監査概論
　監査の概念
• 監査の一般的性質
• 二重責任の原則　など
　監査におけるリスク
• 監査における「リスク・アプローチ」
• 監査リスクと「監査リスクモデル」など
　情報セキュリティ監査の概念と定義
• 保証の概念
• 設計監査と実装・運用監査　など
2. 情報セキュリティ監査の基準
　情報セキュリティ監査基準
• 独立性、客観性と職業倫理
• 監査企業としての品質管理　など
　情報セキュリティ管理基準
• 情報セキュリティ管理基準 マネジメント編
• 情報セキュリティ管理基準 管理策編　など
3. 情報セキュリティ監査の技法
　監査技法の種類
• 監査技法
• サンプリングによる試査の手順
• 技術的検証の留意事項　など
　監査手続
• 監査手続ガイドライン
• 詳細管理策のパターンと監査技法の選択　など
　監査証拠
• 監査証拠と証拠能力
• 証拠の十分性と適切性
• 電子的監査証拠　など
　リスク分析と成熟度モデル

4. 情報セキュリティ監査のプロセス
　監査実施まで
• 保証型監査実施までの流れ
• 言明（監査手続）の策定～保証　など
　契約フェーズ
• 監査契約の締結
• 保証型監査の業務契約　など
　方針フェーズ
• 監査基本方針の策定
• リスク情報の収集と評価　など
　計画フェーズ
• 監査実施計画の立案
　実施フェーズ
• 監査手続の実施
• 入手した監査証拠の適切性と十分性の判断　など
　意見フェーズ
• 監査調書の作成
• 監査意見の形成
　報告フェーズ
• 監査報告書の作成
• 保証意見の表明方法　など
　その他
• 監査品質管理のための体制とプロセス
• 監査調書体系整備と保管体制　など

URL: http://www.jasa.jp/qualification/acquisition.html?key=associate

認定団体について

■ 日本セキュリティ監査協会 ■　特定非営利活動法人。2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行され、この制度を着実に浸透させていくための運営体として設立。

http://www.jasa.jp/index.html/

設立年	2003年
所在国	日本
団体種別	特定非営利活動法人
参加者	53団体（正会員） ※2011年4月時点

国内/
民間資格

公認システム監査人
(Certified Systems Auditor)

資格の概要

システム監査の普及と発展を図るため、特定非営利活動法人 日本システム監査人協会 は、「公認システム監査人(Certified Systems Auditor)」および「システム監査人補 (Associate Systems Auditor) 」の資格制度を創設した。システム監査技術者試験の合格者である「システム監査技術者」を対象に、一定の継続教育を受けることを条件として「システム監査人補」に認定し協会に登録する。また、「システム監査人補」を対象に、2年以上のシステム監査の実務経験を審査し、「公認システム監査人」に認定し協会に登録する。

開始年度	2002年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	(不明)	合格者数	(不明)	資格保持者数 (2012年12月時点)	349名
目的	「システム監査技術者」を中心に、実務に応じられるシステム監査人を認定し、システム監査の実績をさらに積上げ、情報化社会の健全な発展に寄与するもの。				
対象者像	システム監査技術者試験合格者もしくは同等の能力を有し、且つ一定の実務経験を重ねた者				
認定条件	①公認システム監査人の認定を受けようとするシステム監査人補 認定申請書に実務経験を裏付ける小論文(A4版・2000字程度)を添付して提出し、公認システム監査人となるに必要な資質と実務経験の審査ならびに面接試験を受ける。 ②公認システム監査人の認定を受けようとするシステム監査人補でない者 認定申請書に実務経験に基づく小論文および「今後、継続教育要件を満たす旨」の宣誓書を添付して提出し、公認システム監査人となるに必要な資質と実務経験の審査ならびに面接試験を受けることができる。				
更新条件	• 公認システム監査人の認定の有効期限は2年とする。 • 公認システム監査人の認定の更新を受けようとする者は、別途に定める更新に必要な継続教育を受けていることを報告する書類を、2年分まとめて提出しなければならない。 • 公認システム監査人の認定の更新を受けようとする者は、申請書に一定の継続教育を受けたことを報告する書類を添付して、有効期限満了時に申請しなければならない。 • 公認システム監査人の認定を受けた後の原資格の失効は、本認定には影響しない。				
URL	http://www.saaj.or.jp/csa/shosai.pdf				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・他の監査人資格に比べると資格取得者の層は幅広く、金融、公共団体、学校等の出身者も存在すると協会は認識している。

スキル要件・シラバス

受験条件

- システム監査技術者試験の合格者である「システム監査技術者」を対象に、一定の継続教育を受けることを条件として「システム監査人補」に認定されていること。
  (ただし、システム監査技術者試験と関連性のある資格の所有者については、特別認定制度により、一定の教育を受けることなどを条件として同様に認定する。)
- システム監査人補が、所定の実務経験を示して認定申請することにより、面接の上、審査し、認定する。
  (認定条件の①の場合)
- 公認システム監査人とシステム監査人補は同時に申請が可能である。(認定条件の②の場合)

出題範囲

- 認定審査は、小論文に基づき公認システム監査人となる実務経験を有していることを審査する。
- 面接試験は、公認システム監査人となるに必要な資質、倫理規定の理解、実務経験を、複数の試験委員により確認する。

システム監査人倫理規定

(目的)
第1条　この規定は、システム監査人が最低限遵守すべき職業倫理の規範を定めることを目的とする。
(使命)
第2条　システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。
(責務)
第3条　システム監査人は、情報システムを総合的かつ客観的に点検・評価し、関係者に助言・勧告するものとする。
(監査基準・手続き)
第4条　システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。
(監査報告)
第5条　システム監査人は、監査結果の報告にあたって、知り得た全ての重要な事実を明らかにするものとする。
(守秘義務)
第6条　システム監査人は、正当な理由なく業務の遂行に伴い知り得た機密情報を他に漏洩し、または窃用してはならない。
(独立性)
第7条　システム監査人は、常に独立の立場を堅持しつつ、適切な注意と判断によって業務を遂行し、特定人の要求に迎合するようなことがあってはならない。
(公正不偏)
第8条　システム監査人は、業務を誠実に果たし、常に公正不偏の態度を保持しなければならない。
(社会的信頼の保持)
第9条　システム監査人は、自らの使命の重要性に鑑み、高い社会的信頼を保持するよう努めなければならない。
(名誉と信義)
第10条　システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。
(システム監査人間の規律)
第11条　システム監査人は、みだりに他のシステム監査人を誹謗し、名誉を傷つける等の行為をしてはならない。
(自己研鑽)
第12条　システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。
(規定の改廃)
第13条　この規定の改廃は、理事会の承認を得なければならない。

URL: http://www.saaj.or.jp/csa/panf.pdf

認定団体について

■ 日本システム監査人協会 ■ システム監査を社会一般に普及させるとともに、システム監査人の育成、認定、監査技法の維持・向上を図り、よって、健全な情報化社会の発展に寄与することを目的としている。

http://www.saaj.or.jp//

設立年	1987年
所在国	日本
団体種別	特定非営利活動法人
参加者	904名(正会員・団体) 34社(正会員・個人) ※2011年12月末時点

国内/
民間資格

システム監査人補
(Associate Systems Auditor)

資格の概要

システム監査の普及と発展を図るため、特定非営利活動法人 日本システム監査人協会 は、「公認システム監査人(Certified Systems Auditor)」および「システム監査人補 (Associate Systems Auditor) 」の資格制度を創設した。システム監査技術者試験の合格者である「システム監査技術者」を対象に、一定の継続教育を受けることを条件として「システム監査人補」に認定し協会に登録する。

開始年度	2002年	実施団体名	特定非営利活動法人日本セキュリティ監査協会		
受験者数	(不明)	合格者数	(不明)	資格保持者数(2012年12月時点)	145名
目的	「システム監査技術者」を中心に、実務に応じられるシステム監査人を認定し、システム監査の実績をさらに積上げ、情報化社会の健全な発展に寄与するもの。				
対象者像	システム監査技術者試験合格者もしくは同等の能力を有し、且つ一定の実務経験を重ねた者				
認定条件	• システム監査技術者試験の合格者である「システム監査技術者」を対象に、一定の継続教育を受けることを条件として「システム監査人補」に認定されていること。 (ただし、システム監査技術者試験と関連性のある資格の所有者については、特別認定制度により、一定の教育を受けることなどを条件として同様に認定する。) ・ 「継続教育を受ける旨」の宣誓書をつけて、認定申請することにより、審査し、認定する。				
更新条件	• システム監査人補の認定の有効期限は2年とする。 • システム監査人補の認定の更新を受けようとする者は、別途に定める更新に必要な継続教育を受けていることを報告する書類を、2年分まとめて提出しなければならない。 • システム監査人補の認定の更新を受けようとする者は、申請書に一定の継続教育を受けたことを報告する書類を添付して、有効期限満了時に申請しなければならない。 • システム監査人補の認定を受けた後の原資格の失効は、本認定には影響しない。				
URL	http://www.saaj.or.jp/csa/shosai.pdf				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。

認知度・浸透度

・他の監査人資格に比べると資格取得者の層は幅広く、金融、公共団体、学校等の出身者も存在すると協会は認識している。

スキル要件・シラバス

受験条件

- システム監査技術者試験の合格者である「システム監査技術者」を対象に、一定の継続教育を受けることを条件として「システム監査人補」に認定されていること。
(ただし、システム監査技術者試験と関連性のある資格の所有者については、特別認定制度により、一定の教育を受けることなどを条件として同様に認定する。)

出題範囲

- 認定申請書に「今後、継続教育要件を満たす旨」の宣誓書を添えて提出する。

システム監査人倫理規定

(目的)
第1条　この規定は、システム監査人が最低限遵守すべき職業倫理の規範を定めることを目的とする。
(使命)
第2条　システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。
(責務)
第3条　システム監査人は、情報システムを総合的かつ客観的に点検・評価し、関係者に助言・勧告するものとする。
(監査基準・手続き)
第4条　システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。
(監査報告)
第5条　システム監査人は、監査結果の報告にあたって、知り得た全ての重要な事実を明らかにするものとする。
(守秘義務)
第6条　システム監査人は、正当な理由なく業務の遂行に伴い知り得た機密情報を他に漏洩し、または窃用してはならない。
(独立性)
第7条　システム監査人は、常に独立の立場を堅持しつつ、適切な注意と判断によって業務を遂行し、特定人の要求に迎合するようなことがあってはならない。
(公正不偏)
第8条　システム監査人は、業務を誠実に果たし、常に公正不偏の態度を保持しなければならない。
(社会的信頼の保持)
第9条　システム監査人は、自らの使命の重要性に鑑み、高い社会的信頼を保持するよう努めなければならない。
(名誉と信義)
第10条　システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。
(システム監査人間の規律)
第11条　システム監査人は、みだりに他のシステム監査人を誹謗し、名誉を傷つける等の行為をしてはならない。
(自己研鑽)
第12条　システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。
(規定の改廃)
第13条　この規定の改廃は、理事会の承認を得なければならない。

URL: http://www.saaj.or.jp/csa/panf.pdf

認定団体について

■ 日本システム監査人協会 ■ システム監査を社会一般に普及させるとともに、システム監査人の育成、認定、監査技法の維持・向上を図り、よって、健全な情報化社会の発展に寄与することを目的としている。

http://www.saaj.or.jp//

設立年	1987年
所在国	日本
団体種別	特定非営利活動法人
参加者	904名(正会員・団体) 34社(正会員・個人) ※2011年12月末時点

国内/
民間資格

ネットワークセキュリティ基礎資格 /ネットワークセキュリティ実践資格 / サーバセキュリティ実践資格 /セキュリティ監視実践資格 / セキュリティポリシー実践資格 / セキュリティ監査実践資格

資格の概要

ハッカー、不正アクセス、コンピュータウイルス等から情報通信ネットワークとその利用者を防御するための専門知識を持つ技術者を育成し、情報通信サービスを提供する事業者に配置することを目的に創設された。資格を取得するには、認定講習の受講と講習最終日に実施される認定試験にパスすることが必要となる。

開始年度	2001年	実施団体名	ネットワーク情報セキュリティマネージャー推進協議会		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月現在）	約1,100（6資格合計）
目的	ハッカーやサイバーテロの脅威に対処するため、情報セキュリティに関する専門家を育成・配置すること				
対象者像	・ IPやOS等の基本知識（事前確認レベル）はあるものの、セキュリティに関する業務経験や関連知識が少ない者 ・ 基礎コースを終了、または終了と同等のレベルを有する方で、セキュリティシステムの構築を体験した者 ・ ネットワークセキュリティ実践レベル、もしくはセキュリティシステムの構築体験がある者を対象に、より専門的なスキルの習得を目指す者				
認定条件	NISM推進協議会が実施する資格認定のための講習(認定講習)を受講し、一定のレベルに達したものを有資格者として認定する。				
更新条件	資格の有効期間は2年（翌々年度の3月末日まで）とする。資格を更新する者は、NISM推進協議会が実施する更新手続きを行わなければならない。 •「ネットワークセキュリティ基礎資格 /ネットワークセキュリティ実践資格 /サーバセキュリティ実践資格 /セキュリティ監視実践資格 / セキュリティポリシー実践資格 / セキュリティ監査実践資格」は何れの組み合わせでも同時に更新することができる。また、更新年度が合わない場合、前倒しでその年度に更新する科目と同時に更新することができる。 ·「ネットワークセキュリティ基礎資格」更新年度に「ネットワークセキュリティ実践資格」を取得することで「ネットワークセキュリティ基礎資格」も同時に更新されたこととなる。 ·「ネットワークセキュリティ基礎資格」を更新することより、「ネットワークセキュリティ実践資格」の取得を推奨。その後は「ネットワークセキュリティ実践資格」の更新のみで、「基礎、実践」両資格が更新される				
URL	http://www.nism.jp/info.html				

活用状況

・自社の研修カリキュラムの中に当資格の研修を組み込んでいる企業や、社内の推奨資格として取得者には報奨金を出す企業がある。

認知度・浸透度

・資格の取得者は、会員企業に所属する、ITベンダーやIT機器関連の企業の実務者、通信キャリアでネットワーク構築を行う技術者などが多い。会員企業はある程度の規模と認知度のある企業が多いため、規模の小さい企業や、設立間もない企業からの受験は少ない。

スキル要件・シラバス

受験条件

「NISM推進協議会」を構成する団体に加盟する事業者に所属し、当該事業者が推薦する者または、加盟はしていないが、上司または管理するものが推薦する者であって、かつ「NISM推進協議会」が承認した者。

出題範囲

機器及びネットワークの情報セキュリティはもとより、最新の内容を追加する、ケーススタディを増やす等要素が組み込まれている。

1. ネットワークセキュリティ基礎	4. セキュリティ監視実践
1. NISM講習復習 2. 最新セキュリティ動向	1. NISM講習復習 2. 最新セキュリティ動向 – 不正アクセスの動向 – セキュリティインシデントの動向 – セキュリティ監視の動向 – IDSシステムの動向
2. ネットワークセキュリティ実践	**5. セキュリティポリシー実践**
1. NISM講習復習 2. 最新セキュリティ動向 – セキュリティインシデント紹介 – コンピュータウイルスの動向 – 標準化動向 – 関連法規概要	1. NISM講習復習 2. 最新セキュリティ動向 – グローバル・スタンダードの動向 – 評価/認証制度の動向 – セキュリティ関連法規の動向 – セキュリティポリシー策定の動向
3. サーバセキュリティ実践	**6. セキュリティ監査実践**
1. NISM講習復習 2. 最新セキュリティ動向 – オペレーティングシステムの動向 – セキュリティホールの動向 – セキュリティ対策の動向 – サーバアプリケーションの動向	1. NISM講習復習 2. 最新セキュリティ動向 – セキュリティインシデントの動向 – セキュリティ監査の動向 – 技術的検証の動向

URL: http://www.nism.jp/kousin2.html

認定団体について

■ネットワーク情報セキュリティマネージャー推進協議会■ NISMにかかる資格制度に関し、次の業務を行う。なお、協議会において決定する事項及び協議会へ報告する事項は、別に定める。
(1) 制度の基本的な事項についての協議、決定
(2) 制度の運営状況の管理・監督
(3) 制度の普及、定着及び発展のための施策の検討、推進
(4) その他の重要事項についての協議、決定

URL:http://www.nism.jp/nismtowa.html

設立年	2001年
所在国	日本
団体種別	協議会
参加者	7団体

国内/
民間資格

情報セキュリティプランナー

資格の概要

2005年の個人情報保護法の施行に応じたISMS審査員の増加の中で、「主導的な立場のauditorにならない人材がどういった教育を受けるべきか分からない」というニーズがあり、「リスクアセスメントの計画から実行を担当する現場の人材に対する実践的教育が不足している」という問題意識から創設された資格である。勉強会に近い要素もあり、実際に使えるスキルを学び身につけることを重視している。

開始年度	2005年	実施団体名	株式会社ディアイティ		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月時点）	約200名
目的	情報セキュリティ対策の上流工程のプロフェッショナルとして、「ビジネスを前提とした」リスク分析を実施し、中期的な情報セキュリティ対策計画について企画、構築、提案できる人、また、情報セキュリティ対策におけるプロビジョンを明確にし、実装の提案ができる人をPlanning Expert for Information Security（情報セキュリティプランナー）として認定する。				
対象者像	情報セキュリティ計画を構築、運用する専門の方やお客様の組織にあった計画を支援出来るようなスキルを持った営業担当（営業推進担当）を目指す方 （CIO、CISO、CSO等の下で実務を行う人材を対象とした資格である。セキュリティポリシーを策定する人材ではなく、セキュリティポリシーに基づいた対策を立案する人材を対象としている。）				
認定条件	2日間の「情報セキュリティプランナー育成研修」を行う。内容は座学の研修とケーススタディである。研修の最後に行う確認テストの合格者に対し資格認定が与えられる。				
更新条件	なし				
URL	http://www.dit.co.jp/training/infosec_planner/index.html				

活用状況

・株式会社ディアイティでは、合格者に対して、CISSPの受験料を5万円程度安くしている。

認知度・浸透度

・前身はNTTの4日間の営業研修であり、これは過去4000名程度の受講実績がある。

スキル要件・シラバス

受験条件

特になし。誰でも受験可能である。

出題範囲

情報セキュリティプランナー育成研修の内容に基づいた試験。研修としては、主にISMSにおける「Plan」と、「Check」を考慮した「Do」の段階に対応している。

1. 情報セキュリティプランナー育成研修

- 第1章　情報セキュリティの考え方
- 第2章　脅威とぜい弱性、リスク
- 第3章　業務フローの洗い出しとリスク分析
- 第4章　情報セキュリティ対策の選択
- 第5章　事業継続と費用対効果
- 第6章　情報セキュリティ対策の4つのフェーズとPDCAサイクル
- 第7章　ケーススタディ(グループ演習)
- 第8章　提案発表会
- 第9章　確認テスト

2. 成果物

- 業務フロー作成による手順書の実装
- 年間損失予測を前提とした提案書
- 情報セキュリティ対策計画

URL: http://www.dit.co.jp/training/infosec_planner/index.html

認定団体について

■株式会社ディアイティ■ 「安全・安心な高度情報通信ネットワーク社会」を目指している。その実現のために、技術・製品・サービスを提供するだけでなく、情報セキュリティと安定した情報ネットワークを、社会インフラとして確立するための あらゆる活動を行っている。

http://www.dit.co.jp/company/index.html

設立年	1985年
所在国	日本
団体種別	株式会社
参加者	100名（グループ計） ※2010年4月時点

海外/
民間資格

CISSP
（Certified Information Systems Security Professional）

資格の概要

CISSP℠認定資格とは、(ISC)²℠が認定を行っている、国際的に認められたベンダーフリーの情報セキュリティ・プロフェッショナル認証資格である。CIO、CISOを始めとする管理職、技術職、コンサルタント、営業など幅広い職種でIT業務に取組む人が取得している。(ISC)²認定資格「SSCP」の上位資格にあたる。

開始年度	1995年	実施団体名	（ISC）²（International Information Systems Security Certification Consortium）		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月現在）	1,272名
目的	国際的、普遍的レベルで必要な情報セキュリティの知識体系「CBK」を理解している情報セキュリティ・プロフェッショナルを認定する。				
対象者像	情報セキュリティにかかわる人材（コンサルタント、管理職、技術職、監査員など）。セキュリティ業務従事者から管理職者が対象。				
認定条件	試験における1,000点中700点以上のスコアの取得、業務経験（「受験条件」欄参照）、業務経験が事実であることの証明及び「(ISC)²倫理規約（Code of Ethics）」への同意、現役の(ISC)²認定資格保持者の推薦状の提出、無作為に行われる業務経験に関する監査への合格、犯罪に関連した履歴に関する4つの質問事項への正しい回答				
更新条件	あり（3年間に120ポイント・かつ毎年最低20ポイントのCPEクレジットの取得、年会費の支払、(ISC)²倫理規約の遵守） ※CPEクレジットはイベントの参加やオンラインセミナーの受講等で獲得可能				
URL	https://www.isc2.org/japan/what_index.html				

活用状況

・企業における活用
Novell、Deloitte Touche Tohmatsu、大手ヘルスケアサービス企業その他主要企業において、CISSP認定資格の取得が情報セキュリティ関連業務従事者の必須事項とされている。シスコシステムズ社では800人以上のシステムエンジニアとプリセールスエンジニアを教育し、700人以上がCISSP認定を保持している。日本企業でも、ラック、NTTコミュニケーションズ、日本ユニシス、日本オラクルなど多くの企業で資格取得が推進されている。
・公的機関における活用
米国において、NSA（国家安全保障局）がCISSP取得義務付けと上位資格（ISSEP）の提供、DoD（国防総省）で取得必須資格要件化、米国従軍軍人省でCISSP取得費用の負担を実施。
英国スコットランドヤードのコンピュータ犯罪局やインターポール（国際警察機構）においても、情報テクノロジー犯罪の専門家のCISSP取得が進んでいる他、英国政府のInfoSec Training Paths and Competencies（ITPC）（英国政府機関、認定契約機関及び関連組織における機密情報を管理する情報セキュリティ専門家のために設けられたトレーニングプログラム・資格認定の仕組み）で、CISSP認定保持者を自動的に資格認定することを決定。

認知度・浸透度

・国際的に最も権威あるセキュリティ プロフェッショナル認証資格の一つともいわれる。2004年6月には、米国規格協会（ANSI）よりISO/IEC17024の認証を受け、資格制度の全てのプラクティスがグローバルに認められ、認定資格試験としての信頼度がより高まった。
・日本では内閣官房「人材育成・資格制度体系化専門委員会報告書(2007年1月23日)」で「主な情報セキュリティ資格」として取り上げられるなどして認知度が上昇。

スキル要件・シラバス

受験条件　CISSP CBKの10ドメインのうち、2つもしくはそれ以上のドメインにおいて5年以上（大卒者または（ISC）²が認める資格の取得者は4年以上）の「プロフェッショナルとしての」業務経験があること。

出題範囲　国際的、普遍的レベルで必要な情報セキュリティの知識体系として、1989年に作成された『(ISC)²公式CISSP CBK℠（Common Body of Knowledge：共通知識分野）』（下表）がベースとなる。出題形式は多肢選択式である。

1. 情報セキュリティとリスクマネジメント
機密性、完全性、可用性を軸にしたセキュリティマネジメントを行うために必要なポリシー、スタンダード、プロシージャ、ガイドラインの策定、文書化、実施方法、およびそのマネジメントを有効に実施するための、情報の分類、リスクの特定、リスク評価、リスク分析（定性的・定量的）等の手段を用いてセキュリティの脅威を特定し、資産を分類し、システムの脆弱性を評価する方法

2. セキュリティアーキテクチャと設計
企業組織におけるネットワークインフラを設計し、モニターし、セキュリティを確保にするための概念、原則、構造、規格・標準（ハードウェア、ソフトウェア、オペレーティングシステムとそれに関わる全ての機能、アプリケーション、ユーティリティ、ネットワーク環境、セキュリティ意識の向上とトレーニング、ポリシー・プロシージャ・ベースライン、および標準・規格に基づく情報システムセキュリティを含む）

3. アクセス制御
組織の情報へのアクセスを制御するさまざまな情報セキュリティシステム（アクセス制御の原則・基本概念、脅威の特定、アクセス制御の種類及び分類、アクセス制御技術とモデル、監視システム、監査方法等）

4. アプリケーションセキュリティ
ソフトウェア（オペレーティングシステムソフトウェアとアプリケーションソフトウェアを含む）アプリケーションに適用される重要なセキュリティ概念、アプリケーションレベルの脅威、ソフトウェアの設計と開発に必要な環境の概要、情報システムセキュリティでソフトウェアが果たす重要な役割

5. 運用セキュリティ
ハードウェア、記録媒体、およびこれらのリソースにアクセス権を持つオペレーターや管理者等を管理する方法、運用上の違反行為の特定、検出方法、対処策、運用システムの種類と必要性、データセンター・サーバールーム・コンピュータルームの必要性、アクセス権の管理

6. 暗号学
完全性・機密性・信頼性を確保するための暗号化の原則、手段及び方式（暗号技術の歴史、さまざまな暗号方式・アルゴリズムの原則・特徴、公開鍵・共通鍵のアルゴリズム、PKI、システム上の暗号化アーキテクチャ、暗号への脅威等）

7. 通信とネットワークのセキュリティ
ネットワーク構造や伝送（トランスミッション）方式、伝送（トランスポート）形式、可用性・完全性・機密性を提供するために使用されるセキュリティ手段、専用通信網・公衆通信網・メディア上の通信の認証技術、ネットワーク上の脅威およびその防護策

8. 物理（環境）セキュリティ
外部周辺エリアから内部のデータセンターやサーバールームを含むオフィスエリアにおけるすべての情報資産やその施設全体の物理的な保護技術（階層化モデル、環境設計、施設の場所、施設建設の影響、インフラサポート設備）

9. 事業継続と災害復旧の計画
正常な事業運営機能が停止した場合の業務の維持と復旧について

10. 法、規則、コンプライアンス、捜査
組織および人員に関わる法律・コンピュータ犯罪法・規制、及び、犯罪が行われたかどうかを判断するために使用する捜査手段と技術、犯罪事件の捜査、証拠の収集方法、法執行機関への連絡方法（※特定の国に依存する法ではなく、グローバルで通用する、またはグローバルで共通した法（ライセンス問題、知的所有権、輸出・輸入問題等）について取り扱う）

URL:https://www.isc2.org/japan/what_domain.html

認定団体について

■ (ISC)²（International Information Systems Security Certification Consortium）■
全世界の情報セキュリティプロフェッショナルに対し認証資格を開発・提供するほか、CBKに基づく教育プロダクトやトレーニングサービスの提供、CBKの維持・更新を実施する。日本法人である(ISC)²Japanにて、日本語化された公式セミナーや試験等を提供。

URL:https://www.isc2.org/ （日本）https://www.isc2.org/japan/Default.aspx

設立年	1989年
本拠地	米国
団体種別	NPO法人
参加者	会員（世界62,000名以上）

海外/
民間資格

SSCP
（Systems Security Certified Practitioner）

資格の概要

（ISC)²が提供するベンダーフリー・カントリーフリーの情報セキュリティ実務者向け資格。ネットワーク・システム開発や運用などに従事し、通常は情報セキュリティを専業としていないが、情報セキュリティの知見を技術としての観点だけではなく、「組織」という観点から理解し、情報セキュリティ専門家や経営陣とコミュニケーションを図れることを目指している人材を認証する。

情報セキュリティ専業で経験年数が少ない人材にとっても、より実践に近い内容をグローバルの標準に則った内容で理解していることを証明できる資格である。

開始年度	2000年	実施団体名	（ISC）²（International Information Systems Security Certification Consortium）		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月現在）	（日本）41名
目的	通常は情報セキュリティを専業としていないが、情報セキュリティの知見を技術としての観点だけではなく、「組織」という観点から理解し、情報セキュリティ専門家や経営陣とコミュニケーションを図れることを目指している人材を認証する。				
対象者像	情報セキュリティを専業とせず、ネットワーク・システム開発や運用などに従事するアプリケーションプログラマー、システム/ネットワーク/データベースアドミニストレーター、システムアナリスト等のIT実務者。				
認定条件	試験における1,000点中700点以上のスコアの取得、業務経験（「受験条件」欄参照）、業務経験が事実であることの証明及び「(ISC)²倫理規約（Code of Ethics）」への同意、現役の(ISC)²認定資格保持者の推薦状の提出、無作為に行われる業務経験に関する監査への合格、犯罪に関連した履歴に関する4つの質問事項への正しい回答				
更新条件	あり（3年間に60ポイント、かつ毎年最低10ポイントのCPEクレジットの取得、年会費の支払、(ISC)²倫理規約の遵守） ※CPEクレジットはイベントの参加やオンラインセミナーの受講等で獲得可能				
URL	https://www.isc2.org/sscp-domains/Default.aspx				

活用状況

・公的機関における活用
米国国防総省のキャリアパスにおいて取得が 義務付けられている資格の一つに認定。

認知度・浸透度

・米国規格協会（ANSI）よりISO/IEC17024の認証を受けている。
・ニュースサイト「COMPUTER WORLD」(2011年08月25日)にて、情報セキュリティ分野の有望資格として紹介
http://www.computerworld.jp/topics/570/200610
・情報セキュリティ教育事業者連絡会（ISEPA）「情報セキュリティ資格マップ」（2011年5月）に掲載
http://www.jnsa.org/isepa/outputs/research.html

スキル要件・シラバス

受験条件　CISSP CBKの7ドメインのうち、1つもしくはそれ以上のドメインにおいて、1年以上の情報セキュリティ関連の実務経験があること。

出題範囲　（ISC)²作成の「SSCP CBK」（下表）の7分野より出題される。出題形式は多肢選択式である。

1. Access Controls（アクセス制御）
Logical Access Controls - Subjects & Objects、Authentication Mechanisms、Access Control Concepts、Internetwork Trust Architectures、Identity Management 、Cloud Computing
2. Security Operations and Administration（セキュリティの運用と管理）
Code of Ethics, Security Administration, Change Management, Security Evaluation and Assistance, Security Awareness, Information Communication Technology Infrastructure, Endpoint Device Security, Data Management Policies, Security Concepts
3. Monitoring and Analysis（分析とモニタリング）
Continuous Monitoring, Analysis of Monitoring Results
4. Risk, Response and Recovery（リスク、対応、復旧）
Risk Management Process, Security Assessment Activities, Incident Handling Analysis, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP)
5. Cryptography（暗号学）
Concepts & Requirements of Cryptography, Certificate and Key Management, Secure Protocols
6. Networks and Communications（ネットワークと通信）
Networks, Telecommunications, Remote Access, Firewalls & Proxies, Wireless & Cellular Technologies
7. Malicious Code and Activity（不正なコード、不正行為）
Malicious Code, Malicious Code Countermeasures, Malicious Activity, Malicious Activity Countermeasures

URL:https://www.isc2.org/sscp-domains/Default.aspx

認定団体について

■ (ISC)²（International Information Systems Security Certification Consortium）■
全世界の情報セキュリティプロフェッショナルに対し認証資格を開発・提供するほか、CBKに基づく教育プロダクトやトレーニングサービスの提供、CBKの維持・更新を実施する。日本法人である(ISC)²Japanにて、日本語化された公式セミナーや試験等を提供。

URL:https://www.isc2.org/ （日本）https://www.isc2.org/japan/Default.aspx

設立年	1989年
本拠地	米国
団体種別	NPO法人
参加者	会員（世界62,000名以上）

海外/
民間資格

日本行政情報セキュリティプロフェッショナル（JGISP）

資格の概要

「JGISP（Japan Government Information Security Professional：日本行政情報セキュリティ・プロフェッショナル）」は、住民基本台帳ネットワークシステム（住基ネット）やGPKI（Government Public Key Infrastructure：政府認証基盤）を含め、CISSPがカバーしていない日本独自の情報セキュリティ要件を包括的に網羅し、行政組織の事業遂行に関わる人材を認定する。CISSPの上位資格にあたる。前身は、2006年から提供されていたCISSPの上位資格「CISSP-行政情報セキュリティ」である。

開始年度	2009年	実施団体名	（ISC）² Japan		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月現在）	（日本）61名
目的	CISSP認定資格がカバーしていない日本独自の情報セキュリティ要件について包括的に網羅し、特に行政組織の事業遂行に関わる人材を認証する。				
対象者像	行政組織の事業遂行に関わる人材。				
認定条件	試験における1,000点中700点以上のスコアの取得、業務経験（「受験条件」欄参照）、業務経験が事実であることの証明及び「(ISC)²倫理規約（Code of Ethics）」への同意、現役の(ISC)²認定資格保持者の推薦状の提出、無作為に行われる業務経験に関する監査への合格、犯罪に関連した履歴に関する4つの質問事項への正しい回答				
更新条件	あり（3年間に60ポイント、かつ毎年最低10ポイントのCPEクレジットの取得、年会費の支払、(ISC)²倫理規約の遵守） ※CPEクレジットはイベントの参加やオンラインセミナーの受講等で獲得可能				
URL	https://www.isc2.org/japan/other_jgisp.html				

活用状況

・JGISPは当初CISSPの上位資格として創設したが、二つの資格の取得が必須となるためハードルが高く、なかなか浸透しなかった。よって、CISSPを必須とせず、JGISPを単独の資格として提供する現在の形式に変更した。CISSP認定資格がカバーしていない日本独自の情報セキュリティ要件について包括的に網羅し、特に行政組織の事業遂行に関わる人材を認証することを目的としている。公的機関や企業における活用情報については不明である。

認知度・浸透度

・ニュースサイト「COMPUTER WORLD」(2011年08月25日)にて、情報セキュリティ分野の有望資格として紹介
http://www.computerworld.jp/topics/570/200610
・情報セキュリティ教育事業者連絡会（ISEPA）「情報セキュリティ資格マップ」（2011年5月）に掲載
http://www.jnsa.org/isepa/outputs/research.html
・世界ではじめて特定の国の情報セキュリティ要件に特化した認定資格であり、日本ネットワークセキュリティ協会（JNSA）の協力のもと開発した。

スキル要件・シラバス

受験条件　日本行政情報セキュリティプロフェッショナルCBK4ドメインのうち、最低1ドメインで、2年間の業務経験があること

出題範囲　日本行政情報セキュリティプロフェッショナルCBK 4ドメイン（下記表）がベースとなる。出題形式は多肢選択式である。

1. 組織と政策・制度
日本国の情報セキュリティに関わる政府や関連機関などの組織、およびそれら組織に対応する政策や制度などを対象とする。
2. 法
情報セキュリティに関わる日本国の法令を対象とする。
3. 倫理と慣行
日本国独自の文化に根ざしたビジネス上の倫理・慣行、及び、日本国独自の規制・基準に則ったシステムの見積・運用・保守の手法、ならびに、日本国の法制度の枠組みを理解するための基礎知識を対象とする。
4. 技術
主に政府機関・地方公共団体の情報セキュリティにおける日本特有の技術インフラと内容を理解するための基礎知識を対象とする。

URL:https://www.isc2.org/japan/other_jgisp.html

認定団体について

■（ISC）² Japan■
（ISC）²の日本法人。2004年より日本語テキストでのCBKレビューセミナーや本語・英語併記でのCISSP提供を開始。2005年より日本人(ISC)2認定講師によるレビューセミナー講義開催、CISSP認定試験公式ガイドブック(英語版の日本語訳)出版。

URL:https://www.isc2.org/ （日本）https://www.isc2.org/japan/Default.aspx

設立年数	2004年
本拠地	日本
団体種別	NPO法人
参加者	会員 （会員数不明）

海外/
民間資格

CompTIA Security+

資格の概要

セキュリティエンジニアの基本レベルのセキュリティスキルおよび知識を評価するために作成された、ワールドワイドで提供されているベンダーニュートラルの認定資格。
CompTIA Network+に相当するネットワーク環境の実務経験を持つ技術者に必須となるセキュリティスキルを評価するために設計され、セキュリティの一般概念、インフラストラクチャセキュリティ、暗号技術、業務・組織面でのセキュリティ策定など、セキュリティに関連する知識と改善能力、問題解決能力などが幅広く問われる。

開始年度	1993年	実施団体名	CompTIIA		
受験者数	（不明）	合格者数	（不明）	資格保持者数（世界）	約60,000名
目的	セキュリティインシデントに対応するためのセキュリティ概念、ツール、対応手順に関連する知識やスキルを評価するだけではなく、セキュリティインシデントの発生を予防するため定期的、日常的に実施されるべき運用セキュリティ、セキュリティの脅威や脆弱性についての知識やスキルについても評価する。				
対象者像	セキュリティアーキテクト、セキュリティエンジニア、セキュリティコンサルタント、情報保証に携わるエンジニア、セキュリティ管理者、上級システムアドミニストレータ、およびネットワーク管理者。 以下の条件を満たすITセキュリティプロフェッショナルを対象としている（受験条件ではない）。 ・セキュリティ関連のネットワーク管理における最低2年間の業務経験 ・日常的な技術情報セキュリティにおける経験 ・試験分野に挙げられた項目を含む、セキュリティ上の問題や実装に関する幅広い知識				
認定条件	認定資格試験（100～900のスコア形式）における750スコア以上の得点				
更新条件	有効期限：3年間（2011年1月1日以降。それ以前に認定された資格は生涯資格の扱い） 継続教育プログラム（CE プログラム）を登録（資格取得と同時）後3年以内に完了する。 【CEプログラムの完了条件】 ・CompTIA Continuing Education Program Ethics Policy（倫理ポリシー）への同意 ・CE プログラムの登録をした認定資格で必要とされるCEU の取得 ・CE プログラムの登録をした認定資格のCE プログラムの登録費用の全額の支払い 【CEUの対象となる活動】 ・最新バージョンのCompTIA 認定資格試験の合格 ・関連する内容の教育、講義、プレゼンテーション ・コース（学位課程ではない）、またはコンピュータベーストレーニングへの参加 ・関連する内容のカンファレンスやイベントへの参加 ・CompTIA 試験開発のワークショップへの参加 ・関連する内容について記事、ホワイトペーパー、ブログ、本の記載または出版 ・学位を付与する教育機関での関連する内容のコースの修了　など				
URL	http://www.comptia.jp/cont_certif_04.html				

活用状況

・米国国防総省の情報保証に関連している全ての人材に対し、CompTIA Security+は必須資格とされている。

認知度・浸透度

・ANSI認定（ANSI/ISO/IEC17024、ISO/IEC 17011）を取得。

スキル要件・シラバス

受験条件　受験条件は特に設けられていない。

出題範囲　セキュリティ概念について、「知っている」「理解している」だけではなく「How to(どのようにするべきか)」を理解することにより重点が置かれている。従って、新しい出題範囲では「適切な手順を実行する」「異なる認証モデルを展開する」といった表現が見られる。

1. ネットワークセキュリティ

1.1 ネットワーク機器と技術におけるセキュリティの機能と目的について説明することができる。
1.2 安全なネットワーク管理ポリシーを適用、実装することができる。
1.3 ネットワーク設計の要素とコンポーネントを識別し、分類することができる。
1.4 共通プロトコルを実装、利用することができる。
1.5 一般的に使用されるネットワークポートを識別することができる。
1.6 安全な手法を用いて無線ネットワークを実装することができる。

2. コンプライアンスと運用セキュリティ

2.1 リスクに関連する概念を説明することができる。
2.2 適切なリスク軽減戦略を実践することができる。
2.3 適切なインシデント対応手順を実行することができる。
2.4 セキュリティを認識することとトレーニングの重要性を説明することができる。
2.5 事業継続の側面から比較し、対応することができる。
2.6 環境管理を適切に実行し、影響を説明することができる。
2.7 ビデオ監視災害復旧計画（DRP:Disaster Recovery Plan）を立て、実行することができる。
2.8 機密性、完全性、可用性（CIA）コンセプトを実証することができる。

3. 脅威と脆弱性

3.1 マルウェアの各種タイプを解析、分類することができる。
3.2 攻撃の各種タイプの解析、分類することができる。
3.3 ソーシャル・エンジニアリング攻撃の各種タイプを解析、分類することができる。
3.4 無線攻撃の各種タイプを解析、分類することができる。
3.5 アプリケーション攻撃の各種タイプを解析、分類することができる。
3.6 リスク軽減と抑止技術の各種タイプを解析、分類することができる。
3.7 セキュリティの脅威と脆弱性を発見する技術とツールを実装することができる。
3.8 脆弱性の評価において、侵入テスト（ペネトレーションテスト）と脆弱性スキャンの適切な使用を説明することができる。

4. 情報セキュリティマネジメント

4.1 アプリケーション・セキュリティの重要性を説明することができる。
4.2 ホストセキュリティを確立するための適切な手順と実装をすることができる。
4.3 データ・セキュリティの重要性を説明することができる。

5. リスクの概要

5.1 認証サービスの目的と機能を説明することができる。
5.2 認証、認可、アクセスコントロールに関連する基本的なコンセプトとベストプラクティスを説明することができる。
5.3 アカウント管理を行う際に適切なセキュリティコントロールを実装することができる。

6. リスク分析の概要

6.1 一般的暗号化のコンセプトを理解し、確認することができる。
6.2 適切な暗号化ツールと製品を使用することができる。
6.3 PKI の主なコンセプトを説明することができる。
6.4 PKI、証明書の管理と関連したコンポーネントを実装することができる。

URL:http://www.comptia.jp/pdf/Securityplus_jp_sy0-301_ver1.3.pdf

認定団体について

■ CompTIA ■　EDI(Electronic Data Interchange)が様々な規格で利用され情報が飛び交う中、ISOやIEEEに対し標準化を提言するため、各社が集まる場として設立されたIT業界団体。欧米を中心とし14拠点を持ち、日本では2001年4月に支局が開設。IT業界や各種団体、教育機関など100ヶ国22,000機関以上が会員として活動に参加。（2009年1月現在）CompTIA認定資格は、各「業務」の基盤となる技術知識やスキル、問題解決や状況判断などの実務能力を評価する。現在12の業務分野の認定資格をグローバルに提供している。

URL:http://www.comptia.org/home.aspx

設立年数	1982年
所在国	米国
団体種別	任意団体
参加者	IT業界や各種団体、教育機関など 22,000機関以上

海外/
民間資格

CISA
(Certified Information Systems Auditor /公認情報システム監査人)

資格の概要

情報システム監査およびコントロールの専門家資格としては最も長い歴史を持ち、かつ最も国際的に普及している資格である。情報システム監査に関わる専門家自身による団体が認定しており、欧米の企業社会では既に広く認知されている。日本には約10年前に紹介され、その後徐々に存在が知れ渡ってきている。また、認定後の維持条件が厳しいことが「専門能力を常にアップデイトしている」証明として受け止められ、名前だけではない実践的資格として評価を受けている。

開始年度	1978年	実施団体名	ISACA		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月時点）	約2,700名（国内）
目的	情報システムの監査および、セキュリティ、コントロールに関する高度な知識、技能と経験を有するプロフェッショナルを認定する				
対象者像	情報システムの監査および、セキュリティ、コントロールの実務を行っている者				
認定条件	以下5つの条件を全て満たす必要がある。 1.CISA試験に合格すること 2.所定の実務 経験を持っていること 最低5年間の情報システム監査、コントロール（管理）、セキュリティ分野のいずれかの実務経験を証明する経歴証明を提出すること。但し、所定の経験により、この5年間の実務経験の一部を代替することが可能。 3.協会制定 の「職業倫理規定」を遵守すること 情報システムコントロール協会（The Information Systems Audit and Control Association, Inc.）の職業倫理規定は、協会の会員やCISA（公認情報システム監査人）に対して、専門家および個人としての行為のガイドラインを提供している。 4.協会が採用するIS監査基準に従うこと 5.協会の継続専門教育方針に従うこと				
更新条件	以下3つの条件を全て満たす必要がある。 1.毎年、所定時間以上の「継続教育活動」を実践し、報告すること CISAは、この資格をもつ専門家が常に最新の知識と能力を保有していることを証明するために、継続教育プログラムをもっている。最低単位時間（1単位50分計算で1年20単位時間、3年で120単位時間）の継続教育の受講が必要である。 2.毎年、CISA維持手数料を納付すること 3.協会制定の「職業倫理規定」を遵守すること				
URL	http://www.isaca.gr.jp/cisa/index.html#cisa4 （ISACA Tokyo Chapter）				

活用状況

・米国国防総省(DoD)では情報保証局員に対して、DoD の承認した民間の認定資格の取得を義務付けており、CISAは、この承認を得た認定資格である。

認知度・浸透度

・ANSI(米国規格協会)より、ISO（国際標準化機構）/IEC（国際電気標準会議）17024の認証を受けた、情報システムの監査、コントロール、保証およびセキュリティの専門家向けの資格である。

スキル要件・シラバス

受験条件

年齢、学歴等の条件は何もない。

出題範囲

IS監査原則や実践および技術的内容の領域に関する知識、評価、および適用の側面から出題。5 つの実務領域に関する多肢選択方式の問題200 問で構成され、4 時間かけて実施される。問題は、ある特定の状況と質問を記述し、これについて、「最も適当な」、あるいは「最も関係しない」解答を 選ばせるというものが一般的。問題数や問題は、これまでの試験結果や統計的な数値に基づき、受験者の能力を適切に判断できるように工夫されている。

実務領域

1. 情報システム監査のプロセス (14%)
   IT 監査基準に従って、組織における情報システムの保護とコントロールを支援するための監査サービスを提供する。
2. ITガバナンスとマネジメント (14%)
   目標を達成し、組織の戦略を支援するために必要とされるリーダーシップ、組織構造、およびプロセスを備えているという保証を提供する。
3. 情報システムの取得、開発、導入 (19%)
   情報システムの調達、開発、テスト、導入の各業務が組織の戦略と目標を満たしているという保証を提供する。
4. 情報システムの運用、保守、サポート (23%)
   情報システムの運用、保守、およびサポートのプロセスが、組織の戦略と目標を満たしているという保証を提供する。
5. 情報資産の保護 (30%)
   組織のセキュリティポリシー、基準、手順、コントロールが、情報資産の機密性、完全性、可用性を確保しているという保証を提供する。

URL: http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Register-for-the-Exam/Documents/CISA-BOI-June-2013-Japanese.pdf

認定団体について

■ ISACA ■ 情報システムのアシュアランスとセキュリティ、ITガバナンス、システム運用、そしてIT関係のリスクやコンプライアンスにおける、知識、資格認定、コミュニティ作り、支援活動、教育機会等を、グローバルで先導的な立場で提供している。

https://www.isaca.org/Pages/default.aspx

設立年	1969年
所在国	米国
団体種別	非営利団体
参加者	100,000人以上（全世界会員数）

海外/
民間資格

CISM
(Certified Information Security Manager /公認情報セキュリティマネージャー)

資格の概要

企業の情報セキュリティの管理、設計および監督を行う人を対象としてる。CISM 資格はセキュリティ管理が中心となるが、セキュリティ実務に携わっている情報システムの専門家すべてに有用である。CISM 資格は国際的な慣行を促進しており、この認定資格を得た者は効果的なセキュリティ管理とコンサルティング・サービスを提供するのに必要な経験と知識を持っていることが経営トップに保証される。CISM 資格の取得者は、セキュリティ管理のエリートネットワークの一員となり、比類のない技術を持ったプロとして世界で認められる。

開始年度	2003年	実施団体名	ISACA		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年12月時点）	約350名（国内）
目的	経験豊富な情報セキュリティマネージャーと情報セキュリティ管理責任者を認定する				
対象者像	企業・団体等の情報セキュリティプログラムに係る、マネージメント、設計、監督を行う、以下のプロフェッショナルの者 ・セキュリティマネージャー（Security managers） ・セキュリティ担当役員（Security directors） ・セキュリティ担当役職者（Security officers） ・セキュリティコンサルタント（Security consultants）				
認定条件	以下4つの条件を全て満たす必要がある。 1.CISM試験に合格すること 2.所定の実務経験を持っていること 5 年以上の情報セキュリティの実務経験が必要。その内、3 つ以上の実務分野で、少なくとも3年間は情報セキュリティの管理業務を経験が必須。一般的な情報セキュリティの実務経験を代替することはできるが、情報セキュリティ管理の実務経験は代替できない。但し、他のセキュリティ資格や情報システム管理の経験は、最大で2 年まで情報セキュリティ管理の実務経験として認められる。 3.協会制定 の「職業倫理規定」を遵守すること 協会の会員および当該資格保有者のプロフェッショナルまたは個人としての行動規範となる職業倫理規定を定めている。協会の継続専門教育方針に従うこと				
更新条件	以下3つの条件を全て満たす必要がある。 1.毎年、所定時間以上の「継続教育活動」を実践し、報告すること CISAは、この資格をもつ専門家が常に最新の知識と能力を保有していることを証明するために、継続教育プログラムをもっている。最低単位時間（1単位50分計算で1年20単位時間、3年で120単位時間）の継続教育の受講が必要である。 2.毎年、CISA維持手数料を納付すること 3.協会制定の「職業倫理規定」を遵守すること				
URL	http://www.isaca.gr.jp/cism/index.html （ISACA Tokyo Chapter）				

活用状況

・国内の情報セキュリティマネジメントに関する資格はCISMだけである。現在、情報セキュリティマネージャーの配備が不十分、専門知識が不足していると言われており、今後取得者増加の余地があるとされている。

認知度・浸透度

・ANSI(米国規格協会)より、ISO（国際標準化機構）/IEC（国際電気標準会議）17024の認証を受けた、情報システムの監査、コントロール、保証およびセキュリティの専門家向けの資格である。

スキル要件・シラバス

受験条件

年齢、学歴等の条件は何もない。

出題範囲

課題に関連する実践的な知識に基づいて出題。4 つの実務領域に関する多肢選択方式の問題200 問で構成され、4 時間かけて実施される。問題は、ある特定の状況と質問を記述し、これについて、「最も適当な」、あるいは「最も関係しない」解答を 選ばせるというものが一般的。問題数や問題は、これまでの試験結果や統計的な数値に基づき、受験者の能力を適切に判断できるように工夫されている。

実務領域

1. 情報セキュリティガバナンス(24%)
   情報セキュリティガバナンスのフレームワークと支持プロセスを確立し維持して、確実に情報セキュリティ戦略が組織の目標と目的を調和し、情報リスクが適切に管理され、プログラム・リソースが責任を持って管理されるようにする。
2. 情報リスクの管理とコンプライアンス(33%)
   情報リスクを許容できるレベルまで管理して、組織の事業要件とコンプライアンス要件を満たす。
3. 情報セキュリティプログラムの開発と管理(25%)
   情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し管理する。
4. 情報セキュリティのインシデントの管理(18%)
   情報セキュリティのインシデントの検知、調査、対応、および復旧を行う能力の計画、確立、および管理を行って、ビジネスへの影響を最小限にとどめる。

※試験問題は定期的に更新される。実務領域および付随する課題と知識の記述は、広範な調査と各国の当該問題の専門家によるフィードバックに基づいて作成されている。

URL: http://www.isaca.org/About-ISACA/History/Documents/CISM-CandGuide-2013-Japanese.pdf

認定団体について

■ ISACA ■ 情報システムのアシュアランスとセキュリティ、ITガバナンス、システム運用、そしてIT関係のリスクやコンプライアンスにおける、知識、資格認定、コミュニティ作り、支援活動、教育機会等を、グローバルで先導的な立場で提供している。

https://www.isaca.org/Pages/default.aspx

設立年	1969年
所在国	米国
団体種別	非営利団体
参加者	100,000人以上（全世界会員数）

海外/
民間資格

GIAC
（Global Information Assurance Certification）

資格の概要

GIACは、実社会で真に通用するコンピュータ、ネットワーク、およびソフトウェアセキュリティのスキルを認定するものである。また、GIACは能力確認テストであり、理論や用語の知識だけに限らず、実際に情報セキュリティ・コンピュータ・サーバ操作、監査、タスク管理の実用的な知識・スキルを試験し、認定を行う。試験領域は、Security Essentials、セキュリティ監査、侵入検知、インシデント・ハンドリング、ファイアウォール、フォレンジック、Windows OS、Unix/Linux OSなど、入門レベルから高度な専門性を要求される分野までのすべてをカバーしている。2012年11月14日現在35のトレーニングコースと、それに対応する23の認定資格が存在する。

開始年度	1999年	実施団体名	SANS Institute		
受験者数	（不明）	合格者数	（不明）	資格保持者数（2012年11月現在）	45,764名（世界）
目的	情報セキュリティの分野において必要な知識やスキルを、当該個人が有していることを証明すること				
対象者像	セキュリティプロフェッショナルやITマネージャ				
認定条件	資格試験への合格				
更新条件	認定の有効期間は4年間。認定を継続するためには、再受験あるいは有効期間の後半の2年間で継続認定ポイント（CMU）を36ポイント取得することが求められる。				
URL	http://www.giac.org/certifications/why-certify http://sans-japan.jp/index.html				

活用状況

・米国ではカーネギーメロン大学の優秀な学生70名程度がGIACのコースを受講している。
・米国の政府関係者（軍、FBI、CIAなども含む）は年間15,000名程度がコースを受講している。

認知度・浸透度

・情報セキュリティ関連業務経験年数が20年以上の回答者が挙げた、役立つ資格の上位25のうち、15以上がGIACの資格であり、プロフェッショナルに支持される資格である。
・ガートナーグループは、情報セキュリティの分野における最上位の認定はGIACであるとの調査結果を公表している
・Foote Partnersは、GIAC認定を受けた個人は、情報セキュリティに関して最も高いスキルを有すると認められ、高いサラリーとボーナスを得ているとの調査結果を公表している。
・NSA（米国・国家安全保障局）は、SANSのSEC-401について、NSTISSI 4013（情報セキュリティのトレーニング標準）を完全に満たしているとの見解を示している。
・ANSI(米国規格協会)より、ISO（国際標準化機構）/IEC（国際電気標準会議）17024の認証を受けた、情報セキュリティプロフェッショナル向けの資格であり、同分野における世界的標準となっている。

スキル要件・シラバス

受験条件　当試験の受験必須要件は特に設けられておらず、誰でも受験可能である。

出題範囲　分野は「Security Administration」「Forensics」「Management「Audit」「Software Security」「Legal」の6つに分けられ、「How to do the job（知識やスキルを業務においてどう活用するか）」、つまり実務能力を重視した試験になっている。

資格とトレーニングコースの関係（左：資格、右トレーニングコース）

GSEC: GIAC Security Essentials	SEC401: Security Essentials Bootcamp Style
GCIH: GIAC Certified Incident Handler	SEC504: Hacker Techniques, Exploits & Incident Handling
GCIA: GIAC Certified Intrusion Analyst	SEC503: Intrusion Detection In-Depth
GPEN: GIAC Penetration Tester	SEC560: Network Penetration Testing and Ethical Hacking
GCFW: GIAC Certified Firewall Analyst	SEC502: Perimeter Protection In-Depth
GWAPT: GIAC Web Application Penetration Tester	SEC542: Web App Penetration Testing and Ethical Hacking
GCWN: GIAC Certified Windows Security Administrator	SEC505: Securing Windows and Resisting Malware
GAWN: GIAC Assessing and Auditing Wireless Networks	SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
GCUX: GIAC Certified UNIX Security Administrator	SEC506: Securing Linux/Unix
GISF: GIAC Information Security Fundamentals	SEC301: Intro to Information Security
GCED: GIAC Certified Enterprise Defender	SEC501: Advanced Security Essentials – Enterprise Defender
GXPN: GIAC Exploit Researcher and Advanced Penetration Tester	SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking
GCFA: GIAC Certified Forensic Analyst	FOR508: Advanced Computer Forensic Analysis and Incident Response
GREM: GIAC Reverse Engineering Malware	FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GCFE: GIAC Certified Forensic Examiner	FOR408: Computer Forensic Investigations – Windows In-Depth
GSLC: GIAC Security Leadership	MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression
GISP: GIAC Information Security Professional	MGT414: SANS +S Training Program for the CISSP Certification Exam
GCPM: GIAC Certified Project Manager	MGT525: IT Project Management, Effective Communication, and PMP Exam Prep
GSNA: GIAC Systems and Network Auditor	AUD507: Auditing Networks, Perimeters, and Systems
GSSP-JAVA: GIAC Secure Software Programmer-Java	DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
GWEB: GIAC Certified Web Application Defender	DEV522: Defending Web Applications Security Essentials
GSSP-.NET: GIAC Secure Software Programmer- .NET	DEV544: Secure Coding in .NET: Developing Defensible Applications
GLEG: GIAC Legal Issues in Information Technology & Security	LEG523: Law of Data Security and Investigations

認定団体について

■ SANS Institute■ 米国メリーランド州ベセスダに本部を置く産学官の連携横断的な調査研究・教育機関。情報セキュリティのコミュニティ形成・発展をテーマに「Content and Community」と「Training and Certification」の2つのミッションを持つ。

URL:http://www.sans.org/

設立年	1989年
所在国	米国
団体種別	調査研究・教育機関
参加者	40万人以上（プログラム利用者）

海外/
民間資格

ISMS審査員補

資格の概要

ISMS（情報セキュリティマネジメントシステム）審査員とは、ISMS認証基準への適合性を審査する要員であり、要員認証機関であるJRCAが評価登録している。ISMS適合性評価制度は、組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。

ISMS審査員資格は、主任審査員、審査員、審査員補の3段階に分かれ、審査員補はISMS主任審査員のアシスタントとして審査の実務に加わる。

開始年度	1984年	実施団体名	日本規格協会 マネジメントシステム審査員評価登録センター（JRCA）、国際審査員登録機構（IRCA）		
受験者数	（不明）	合格者数	（不明）	資格保持者数	約2,400名（日本）
目的	ISMS認証基準への適合性を審査する要員を認証する。				
対象者像	ISMS審査員補の登録要件を満たすとJRCAが評価し登録した者であり、審査の補助者として当センター登録のISMS 主任審査員（ｺﾝﾋﾟﾃﾝｽ）の同行、同席の下で審査の実務を行うことができる。				
認定条件	・学歴 高等学校卒業又はこれと同等以上の学歴を有していること。もしくはそれと同等の教育を修了した者、又は豊富な経験を持ち、あるいは専門的な教育訓練を受けている者で、JRCAが承認する者とする。 ・情報技術分野の実務経験 情報技術分野において4年以上の常勤（派遣・委託を含む）による実務経験があること。また、2年以上の情報セキュリティ技術に関連した役割又は職務に就いていること。 ・審査技術の習得 JRCAが承認した情報セキュリティマネジメントシステム審査員（ｺﾝﾋﾟﾃﾝｽ）研修コース（フォーマルコース又は資格拡大コース）において個人的特質の継続的評価および実技評価に合格し、研修コースを修了していること。 ・力量試験の合格 ・申請期限 上記研修コースの修了証記載の終了日から5年以内に申請すること。 ・審査員倫理綱領の遵守				
更新条件	登録有効期間：登録日又は更新日から3年 【資格登録維持】 維持登録日前の1年間において実施した以下の一つを報告すること。 【資格登録更新】 更新登録日前の1年間において実施した以下の一つを報告すること。 ・教育実績5 時間以上 ・有効な審査実績、あるいは内部監査実績7 時間以上 ・継続的専門能力開発（CPD）5時間以上　※別途経費等が必要				
URL	http://www.jsa.or.jp/jrca/seido-2.asp				

活用状況

・官公庁、自治体等の情報セキュリティ監査の入札や公募において、を資格要件の1つとして含めている場合がある。
・大企業や中堅のソフトウェアハウスで内部監査人として、審査員補資格の取得を社員に求める企業は多い。
(第三者認証を受ける際にも、外部の審査員と対等な立場で話ができるように、社内に審査員補資格を取得している人材がいた方が良いと考えられているため)

認知度・浸透度

・認証機関は全国に400機関以上存在する。ISMS審査員はほぼ全員が認証機関に所属している。日本は世界的に見てISMS認証の取得数が多い方である。

スキル要件・シラバス

受験条件　一定の実務経験に加え、認定コースの受講が求められる。

出題範囲　ISMS適合性評価制度に基づく研修コース（内容は下記参照）と力量試験を合格修了することで、ISMS審査員登録申請に必要な合格証明書が授与される。

＊研修コース内容

・ISMS適合性評価制度概要
・ISO27001（JISQ27001）の解説
・リスクアセスメントの理解
・セキュリティ技術の解説
・ISMS審査技法概説
・ISMS審査技法演習（文書審査、審査計画書作成／発表、実地審査ロールプレイ、是正処置要求書作成、審査報告書作成／発表）
URL:http://www.gtc.co.jp/semn/isc/ila.html

（参考）継続的専門能力開発（CPD）テーマ例

① ISMS規格及び他の関連する基準文書
② 情報技術
③ 情報セキュリティ技術
④ リスクアセスメント、リスクマネジメント
⑤ ISMS関連法規制、要求事項
⑥ ISMSに関連する監査の原則
⑦ ISMSの有効性のレビュー
⑧ 管理策の有効性の測定
⑨ ISMS審査技術
URL:http://www.jsa.or.jp/jrca/isms-pdf/jrca-ai-110.pdf

認定団体について

■ 日本規格協会 マネジメントシステム審査員評価登録センター（JRCA）■
品質マネジメントシステム審査員、情報セキュリティマネジメントシステム審査員、並びに航空宇宙産業向け審査員の評価登録を行っている要員認証機関。マネジメントシステム審査について一定水準以上の知識と経験からくる力量を持ち合わせていることを当センターが評価し、「マネジメントシステム審査員」として資格を与える。

URL:http://www.jsa.or.jp/jrca/seido-2.asp

設立年数	1945年
所在国	日本
団体種別	＊＊
参加者	＊＊

■ 国際審査員登録機構（IRCA）■ 世界初、最大規模のマネジメントシステム審査員国際登録組織。本部はロンドン。世界150カ国、14,750人以上の審査員が登録している。マネジメントシステム審査員の登録と、研修機関および審査員研修コースの認定を担う。

URL:http://www.irca.org/home.html

設立年数	1984年
所在国	英国
団体種別	＊＊
参加者	審査員 世界150カ国、14,750人以上

海外/
民間資格

CIW Web Security Professional / CIW Web Security Specialist / CIW Web Security Associate

資格の概要

CIW Web Security Professional / CIW Web Security Specialistの認定者は、Webセキュリティについて、「信頼性のあるセキュアなデータ通信技術とその実装」「システムのセキュリティを確保する技術とその実装」「様々なシステム攻撃の手法と実践的な対処方法」の知識・スキルを身につけたとみなされる。

CIW Web Security Associateの認定者は、ネットワークセキュリティとファイアウォールについての理解を深め、ネットワークやシステムのセキュリティを確保するための専門知識・スキルを身につけたとみなされる。

開始年度	2001年	実施団体名	CIW Japan		
受験者数	（不明）	合格者数	（不明）	資格保持者数	（不明）
目的	・ Web上において最も必要とされるセキュリティ技術について専門知識と実践スキルを持ち合わせていることを証明する（CIW Web Security Professional / CIW Web Security Specialist） • ネットワークやシステムのセキュリティを確保するための専門知識・スキルを持ち合わせていることを証明する（CIW Web Security Associate）				
対象者像	• CIW Web Security Professional / CIW Web Security Specialist アプリケーション開発者、ソフトウェア開発者、アプリケーションプログラマ、クライアント/サーバ開発者、Webアーキテクト • CIW Web Security Associate ネットワークサーバアドミニストレータ、ファイアウォールアドミニストレータ、システムアドミニストレータ、アプリケーションデベロッパ、ITセキュリティ担当者、その他、ビジネス上でWebセキュリティに関わる方や上記職種を目指される方				
認定条件	• CIW Web Security Professional / CIW Web Security Specialist 1. CIW Web Security Associate資格の取得 2. 資格同意書の提出 3. CIW以外の関連資格の取得（「CIW Web Security Specialist」では他団体の認定証は1種類、「CIW Web Security Professional」では2種類必要。） • CIW Web Security Associate CIW Web Security Associate試験に合格すること				
更新条件	なし				
URL	http://www.ciw-japan.com/curriculum/CIW_Web_Security_Professional.html http://www.ciw-japan.com/curriculum/CIW_Web_Security_Specialist.html http://www.ciw-japan.com/curriculum/CIW_WebSecurityAssociate.html				

活用状況

・国内外の企業において、研修への導入や、昇進の条件の一つに設定されるといった形で活用されている。
（http://www.ciw-japan.com/ciw/adoption.html）

認知度・浸透度

・米国では各州単位で教育政策やジョブトレーニングが行われており、現在16の州でCIWの教育プログラムが採用されている。

スキル要件・シラバス

受験条件

年齢、学歴等の条件は何もない。

出題範囲

企業のネットワークセキュリティポリシー、認証手続、暗号化標準と実装、ハッカーが操作するポートとプロトコル、積極的な検出と回答/報告メソッド、ハッカー侵入の防止と管理について出題される。受験言語は英語。問題数は62問。試験時間は90分。合格基準は76%。

What Is Security?	Protocol Layers and Security
• Network Security Background • What Is Security? • Hacker Statistics, etc..	• TCP/IP Security Introduction • OSI Reference Model Review • Data Encapsulation, etc.
Elements of Security	Securing Resources
• Security Elements and Mechanisms • The Security Policy • Determining Backups, etc.	• TCP/IP Security Vulnerabilities • Implementing Security • Resources and Services, etc.
Applied Encryption	Firewalls and Virtual Private Networks
• Reasons to Use Encryption • Creating Trust Relationships • Symmetric-Key Encryption, etc.	• Access Control Overview • Definition and Description of a Firewall • The Role of a Firewall, etc.
Types of Attacks	Levels of Firewall Protection
• Network Attack Categories • Brute-Force and Dictionary Attacks • System Bugs and Back Doors, etc.	• Designing a Firewall • Types of Bastion Hosts • Hardware Issues, etc.
Recent Networking Vulnerability Considerations	Detecting and Distracting Hackers
• Networking Vulnerability Considerations • Wireless Network Technologies and Security • IEEE 802.11 Wireless Standards, etc.	• Proactive Detection • Distracting the Hacker • Deterring the Hacker, etc.
General Security Principles	
• Common Security Principles • Be Paranoid • You Must Have a Security Policy, etc.	• Creating an Incident Response Policy • Determining If an Attack Has Occurred • Executing the Response Plan, etc.

URL: http://www.ciwcertified.com/proddesc/COURSE_DESC/CCN02CAWSAAPR1012.pdf

認定団体について

■CIW Japan■ CIW本部は米国Certification Partner社にあり、CIW-Japanは同社の100%出資子会社であるCPジャパンによって運営されている。国内におけるCIWサービスの提供業務を担っている。

http://www.ciw-japan.com/about_us.html

設立年	2012年
所在国	日本
団体種別	運営団体
参加者	職員数不明