情報処理技術者試験

試験要綱

Ver 2.0

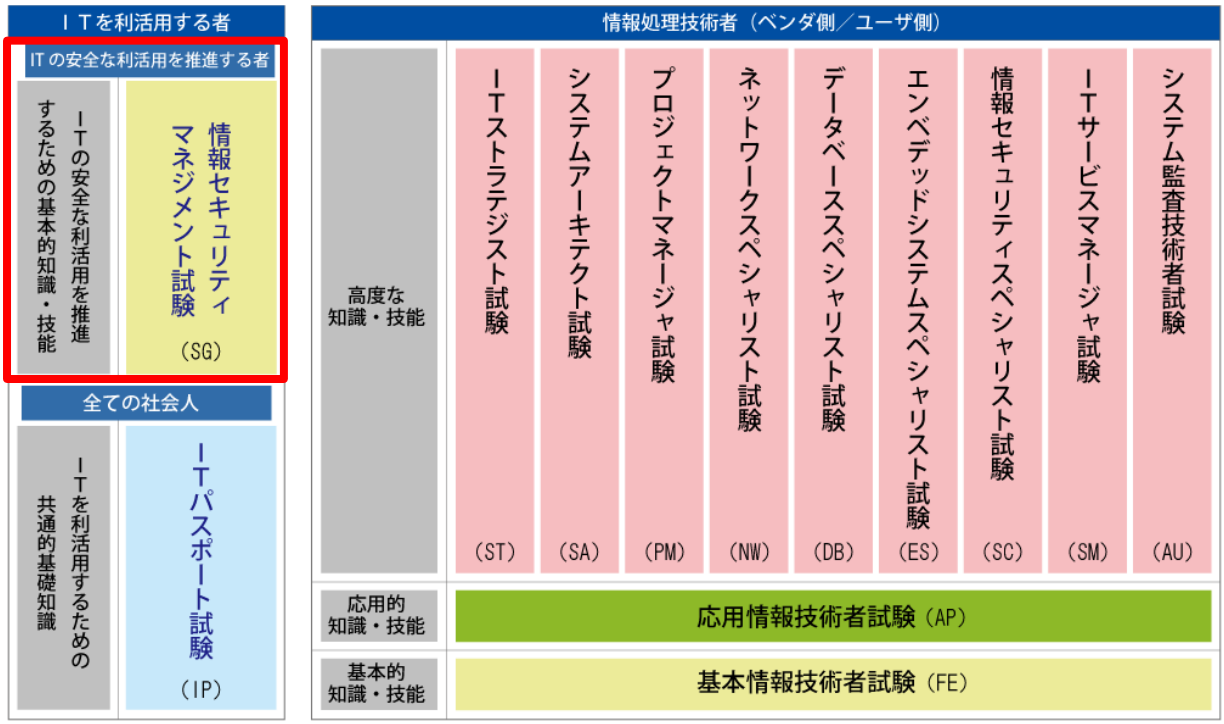
情報セキュリティマネジメント試験
抜粋版

平成 27 年 10 月 16 日

IPA 独立行政法人情報処理推進機構
IT人材育成本部 情報処理技術者試験センター

1. 実施する試験区分

情報処理技術者試験は，「IT パスポート試験」，「情報セキュリティマネジメント試験」，「基本情報技術者試験」，「応用情報技術者試験」及び「高度試験」9 区分の計 13 区分から構成する。



2. 試験の対象者像

情報セキュリティマネジメント試験の対象者像，役割と業務，期待する技術水準及びレベル対応を次に示す。

○情報セキュリティマネジメント試験（SG：Information Security Management Examination）

対象者像	情報システムの利用部門にあって，情報セキュリティリーダとして，部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し，情報及び情報システムを安全に活用するために，情報セキュリティが確保された状況を実現し，維持・改善する者
業務と役割	情報システムの利用部門において情報セキュリティが確保された状況を実現し，維持・改善するために，次の業務と役割を果たす。 ① 部門における情報資産の情報セキュリティを維持するために必要な業務を遂行する。 ② 部門の情報資産を特定し，情報セキュリティリスクアセスメントを行い，リスク対応策をまとめる。 ③ 部門の情報資産に関する情報セキュリティ対策及び情報セキュリティ継続の要求事項を明確にする。 ④ 情報システムの調達に際して，利用部門として必要となる情報セキュリティ要求事項を明確にする。また，業務の外部委託に際して，情報セキュリティ対策の要求事項を契約で明確化し，その実施状況を確認する。 ⑤ 部門における情報セキュリティを確実に運用する。 ⑥ 部門のメンバの情報セキュリティ意識，コンプライアンスを向上させ，内部不正などの情報セキュリティインシデントの発生を未然に防止する。

	⑦　情報セキュリティインシデントの発生又はそのおそれがあるときに，情報セキュリティ諸規程，法令・ガイドライン・規格などに基づいて，適切に対処する。 ⑧　部門又は組織全体における情報セキュリティに関する意見・問題点について担当部署に提起する。
期待する技術水準	情報システムの利用部門において情報セキュリティが確保された状況を実現し，維持・改善するために，次の知識・実践能力が要求される。 ①　部門の情報セキュリティマネジメントの一部を独力で遂行できる。 ②　情報セキュリティインシデントの発生又はそのおそれがあるときに，情報セキュリティリーダとして適切に対処できる。 ③　情報技術全般に関する基本的な用語・内容を理解できる。 ④　情報セキュリティ技術や情報セキュリティ諸規程に関する基本的な知識をもち，情報セキュリティ機関，他の企業などから動向や事例を収集し，部門の環境への適用の必要性を評価できる。
レベル対応	共通キャリア・スキルフレームワークのレベル 2 に相当

3. 試験時間・出題形式・出題数・解答数

試 験 区 分	午　前		午　後	
	9:30～11:00 （90 分）		12:30～14:00 （90 分）	
	出題形式	出題数 解答数	出題形式	出題数 解答数
情報セキュリティマネジメント試験	多肢選択式 (四肢択一)	50 問 50 問	多肢選択式	3 問 3 問

4. 採点方式・配点・合格基準

(1) 採点方式は，午前・午後とも素点方式を採用する。

(2) 合格基準は，午前，午後の得点がともに基準点以上の場合に合格とする。

(3) 配点（満点）及び基準点は次のとおりとする。なお，試験結果に問題の難易差が認められた場合には，基準点の変更を行うことがある。

〔配点及び基準点〕

試験区分	時間区分	配点	基準点
情報セキュリティマネジメント試験	午前	100点満点	60点
	午後	100点満点	60点

(4) 問題別配点割合は，次のとおりとする。

〔問題別配点割合〕

試験区分	午前			午後		
	問番号	解答数	配点割合	問番号	解答数	配点割合
情報セキュリティマネジメント試験	1～50	50	各 2 点	1～3	3	各 34 点 [1)]

注 [1)] 得点の上限は 100 点とする。

5. 試験の実施方法・実施時期

(1) 情報セキュリティマネジメント試験はペーパ方式によって実施する。
(2) 情報セキュリティマネジメント試験は春期・秋期（4月・10月 第3日曜日）の年2回実施する。

〔各試験区分の試験実施時期〕

試験区分		実施時期	
ITパスポート試験		随時	
情報セキュリティマネジメント試験		春期	秋期
基本情報技術者試験		春期	秋期
応用情報技術者試験		春期	秋期
高度試験	ITストラテジスト試験		秋期
	システムアーキテクト試験		秋期
	プロジェクトマネージャ試験	春期	
	ネットワークスペシャリスト試験		秋期
	データベーススペシャリスト試験	春期	
	エンベデッドシステムスペシャリスト試験	春期	
	情報セキュリティスペシャリスト試験	春期	秋期
	ITサービスマネージャ試験		秋期
	システム監査技術者試験	春期	

6. 出題範囲

情報セキュリティマネジメント試験では，受験者の能力が期待する技術水準に達しているかを，午前の試験では知識を問うことによって，午後の試験では技能を問うことによって評価する。

（午前の試験）

午前の出題範囲は次のとおりとする。

〔試験区分別出題分野一覧表〕

分野	大分類		中分類		ITパスポート試験	情報セキュリティマネジメント試験	基本情報技術者試験	応用情報技術者試験	高度試験 午前Ⅰ（共通知識）	高度試験 午前Ⅱ（専門知識） ITストラテジスト試験	システムアーキテクト試験	プロジェクトマネージャ試験	ネットワークスペシャリスト試験	データベーススペシャリスト試験	エンベデッドシステムスペシャリスト試験	情報セキュリティスペシャリスト試験	ITサービスマネージャ試験	システム監査技術者試験
テクノロジ系	1	基礎理論	1	基礎理論														
			2	アルゴリズムとプログラミング														
	2	コンピュータシステム	3	コンピュータ構成要素							○3		○3	○3	◎4		○3	
			4	システム構成要素		○2					○3		○3	○3	○3		○3	
			5	ソフトウェア											◎4			
			6	ハードウェア											◎4			
	3	技術要素	7	ヒューマンインタフェース														
			8	マルチメディア														
			9	データベース		○2					○3			◎4		○3	○3	○3
			10	ネットワーク		○2					○3		◎4		○3	◎4	○3	○3
			11	セキュリティ		◎2				○3	○3	○3	◎4	○3	○3	◎4	○3	○3
	4	開発技術	12	システム開発技術	○1		○2	○3	○3		◎4	○3	○3	○3	◎4	○3		○3
			13	ソフトウェア開発管理技術							○3	○3	○3	○3	○3	○3		
マネジメント系	5	プロジェクトマネジメント	14	プロジェクトマネジメント		○2						◎4					◎4	
	6	サービスマネジメント	15	サービスマネジメント		○2						○3				○3	◎4	○3
			16	システム監査		○2										○3	○3	◎4
ストラテジ系	7	システム戦略	17	システム戦略		○2				◎4	○3							
			18	システム企画		○2				◎4	◎4	○3						
	8	経営戦略	19	経営戦略マネジメント						◎4								○3
			20	技術戦略マネジメント						○3								
			21	ビジネスインダストリ						◎4								
	9	企業と法務	22	企業活動		○2				◎4								○3
			23	法務		◎2				○3		○3					○3	◎4

注記 1　○は出題範囲であることを，◎は出題範囲のうちの重点分野であることを表す。
注記 2　1，2，3，4 は技術レベルを表し，4 が最も高度で，上位は下位を包含する。

〔情報セキュリティマネジメント試験　午前の出題範囲〕

➢ 重点分野

共通キャリア・スキルフレームワーク							知識項目例 （情報セキュリティマネジメント試験は「IT を利活用する者」を主な対象とすることから，技術的な項目は除外している）
分野	大分類		中分類		小分類		
テクノロジ系	1	技術要素（セキュリティ）	1	セキュリティ	1	情報セキュリティ	情報の機密性・完全性・可用性，脅威，マルウェア・不正プログラム，脆弱性，不正のメカニズム，攻撃者の種類・動機，サイバー攻撃（SQL インジェクション，クロスサイトスクリプティング，DoS 攻撃，フィッシング，パスワードリスト攻撃，標的型攻撃ほか），暗号化技術（共通鍵，公開鍵，秘密鍵，RSA，AES，ハイブリッド暗号，ハッシュ関数ほか），認証技術（ディジタル署名，メッセージ認証，タイムスタンプほか），利用者認証（ID・パスワード，多要素認証ほか），生体認証技術，公開鍵基盤（PKI，ディジタル証明書ほか）　など
					2	情報セキュリティ管理	情報資産とリスクの概要，情報資産の調査・分類，リスクの種類，情報セキュリティリスクアセスメント及びリスク対応，情報セキュリティ継続，情報セキュリティ諸規程（情報セキュリティポリシを含む組織内規程），ISMS，管理策（情報セキュリティインシデント管理，法的及び契約上の要求事項の順守ほか），情報セキュリティ組織・機関（CSIRT，SOC（Security Operation Center），ホワイトハッカーほか）　など
					3	セキュリティ技術評価	PCI DSS，CVSS，脆弱性検査，ペネトレーションテスト　など
					4	情報セキュリティ対策	情報セキュリティ啓発（教育，訓練ほか），組織における内部不正防止ガイドライン，マルウェア・不正プログラム対策，不正アクセス対策，情報漏えい対策，アカウント管理，ログ管理，脆弱性管理，入退室管理，アクセス制御，侵入検知/侵入防止，検疫ネットワーク，多層防御，無線 LAN セキュリティ（WPA2 ほか），携帯端末（携帯電話，スマートフォン，タブレット端末ほか）のセキュリティ，セキュリティ製品・サービス（ファイアウォール，WAF，DLP，SIEM ほか），ディジタルフォレンジックス　など
					5	セキュリティ実装技術	セキュアプロトコル（IPSec，SSL/TLS，SSH ほか）ネットワークセキュリティ，データベースセキュリティ，アプリケーションセキュリティ　など
ストラテジ系	2	企業と法務（法務）	2	法務	1	知的財産権	著作権法，不正競争防止法（営業秘密ほか）　など
					2	セキュリティ関連法規	サイバーセキュリティ基本法，不正アクセス禁止法，刑法（ウイルス作成罪ほか），個人情報保護法，特定個人情報の適正な取扱いに関するガイドライン，プロバイダ責任制限法，特定電子メール法，コンピュータ不正アクセス対策基準，コンピュータウイルス対策基準　など
					3	労働関連・取引関連法規	労働基準法，外部委託契約，ソフトウェア契約，ライセンス契約，守秘契約（NDA），労働者派遣法　など
					4	その他の法律・ガイドライン・技術者倫理	コンプライアンス，情報倫理，技術者倫理　など
					5	標準化関連	JIS，ISO，IEEE などの関連機構の役割，標準化団体など

注記 1　出題上の配慮から，重点分野（セキュリティ，法務）を先頭に配置している。

注記 2　「試験区分別出題分野一覧表」（P4）のうち，出題範囲に含まない分野（基礎理論，開発技術など）の分類番号は前詰めしている。

➢ **その他の分野**

共通キャリア・スキルフレームワーク							知識項目例 （情報セキュリティマネジメント試験は「IT を利活用する者」を主な対象とすることから，技術的な項目は除外している）
分野	大分類		中分類		小分類		
テクノロジ系	3	コンピュータシステム	3	システム構成要素	1	システムの構成	システムの処理形態，システムの利用形態，クライアントサーバシステム，Web システム，シンクライアントシステム，フォールトトレラントシステム，RAID，NAS，SAN，P2P，クラスタ　など
					2	システムの評価指標	システムの性能指標，システムの性能特性と評価，信頼性計算，信頼性指標，信頼性特性と評価，経済性の評価　など
	4	技術要素（セキュリティ以外）	4	データベース	1	データベース方式	データベースの種類と特徴，DBMS　など
					2	データベース設計	データ分析　など
					3	データ操作	データベースを操作するための言語（SQL ほか）　など
					4	トランザクション処理	排他制御，リカバリ処理　など
					5	データベース応用	データウェアハウス，メタデータ，ビッグデータ　など
			5	ネットワーク	1	ネットワーク方式	ネットワークの種類と特徴（WAN/LAN，有線･無線ほか），インターネット技術，パケット交換網，RADIUS　など
					2	データ通信と制御	伝送方式と回線，LAN 間接続装置　など
					3	通信プロトコル	プロトコルとインタフェース，HTTP，IPv6　など
					4	ネットワーク管理	障害管理　など
					5	ネットワーク応用	インターネット，イントラネット，エクストラネット，モバイル通信，通信サービス　など
マネジメント系	5	プロジェクトマネジメント	6	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，プロジェクトマネジメント，プロジェクトの環境　など
					2	プロジェクト統合マネジメント	プロジェクト憲章の作成，プロジェクト計画の作成，プロジェクト作業の指揮，プロジェクト作業のコントロール，変更のコントロール，プロジェクトフェーズ又はプロジェクトの終結，学んだ教訓の収集　など
					3	プロジェクトステークホルダマネジメント	ステークホルダの特定，ステークホルダの管理　など
					4	プロジェクトスコープマネジメント	スコープの定義，WBS の作成，アクティビティの定義，スコープのコントロール　など
					5	プロジェクト資源マネジメント	プロジェクトチームの結成，資源の見積り，プロジェクト組織の決定，プロジェクトチームの育成，資源のコントロール，プロジェクトチームの管理　など
					6	プロジェクトタイムマネジメント	アクティビティの順序付け，アクティビティ期間の見積り，スケジュールの作成，スケジュールのコントロール　など
					7	プロジェクトコストマネジメント	コストの見積り，予算の編成，コストのコントロール　など
					8	プロジェクトリスクマネジメント	リスクの特定，リスクの評価，リスクへの対応，リスクのコントロール　など
					9	プロジェクト品質マネジメント	品質の計画，品質保証の実施，品質コントロールの実施　など

共通キャリア・スキルフレームワーク							知識項目例 （情報セキュリティマネジメント試験は「IT を利活用する者」を主な対象とすることから，技術的な項目は除外している）
分野	大分類		中分類		小分類		
					10	プロジェクト調達マネジメント	調達の計画，サプライヤの選定，調達の管理　など
					11	プロジェクトコミュニケーションマネジメント	コミュニケーションの計画，情報の配布，コミュニケーションの管理　など
	6	サービスマネジメント	7	サービスマネジメント	1	サービスマネジメント	サービスレベル合意書（SLA），サービス及びプロセスのパフォーマンス　など
					2	サービスの設計・移行	サービスの設計・開発，移行，サービス受入れ基準，運用引継ぎ　など
					3	サービスマネジメントプロセス	サービスレベル管理，サービスの報告，サービス継続及び可用性管理，キャパシティ管理，供給者管理，インシデント及びサービス要求管理，問題管理，構成管理，変更管理，リリース及び展開管理　など
					4	サービスの運用	システム運用管理，運用オペレーション，サービスデスク，システムの監視と操作　など
					5	ファシリティマネジメント	設備管理（電源・空調設備ほか），施設管理　など
			8	システム監査	1	システム監査	システム監査の意義と目的，システムの可監査性，システム監査の品質評価，情報セキュリティ監査　など
					2	内部統制	内部統制の意義と目的，相互けん制（職務の分離），IT ガバナンス，CSA（統制自己評価）　など
ストラテジ系	7	システム戦略	9	システム戦略	1	情報システム戦略	情報システム戦略の意義と目的，情報化推進体制　など
					2	業務プロセス	BPR，業務改善　など
					3	ソリューションビジネス	ソリューションビジネスの種類とサービス形態，ASP，クラウドコンピューティング（SaaS，PaaS，IaaS ほか）　など
					4	システム活用促進・評価	システム利用実態の評価・検証，システム廃棄　など
			10	システム企画	1	システム化計画	情報システム導入リスク分析　など
					2	要件定義	要求分析，ユーザニーズ調査，現状分析，課題定義，業務要件定義，機能要件定義，非機能要件定義　など
					3	調達計画・実施	調達計画，提案依頼書（RFP），提案評価基準，見積書，提案書，調達選定　など
	8	企業と法務（法務以外）	11	企業活動	1	経営・組織論	経営管理，PDCA，経営組織（CIO，CEO ほか），ヒューマンリソース（ケーススタディほか），行動科学（リーダシップ，コミュニケーションほか），リスクマネジメント，BCP　など
					2	OR・IE	検査手法（サンプリング，シミュレーションほか），品質管理手法（QC 七つ道具，新 QC 七つ道具ほか）　など
					3	会計・財務	財務諸表，減価償却，損益分岐点，原価，リースとレンタル　など

〔情報セキュリティマネジメント試験　午後の出題範囲〕

1　情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること

（1）情報資産管理の計画

情報資産の特定及び価値の明確化，管理責任及び利用の許容範囲の明確化，情報資産台帳の作成　など

（2）情報セキュリティリスクアセスメント及びリスク対応

リスクの特定・分析・評価，リスク対応策の検討，リスク対応計画の策定　など

（3）情報資産に関する情報セキュリティ要求事項の提示

物理的及び環境的セキュリティ，部門の情報システムに関する技術的及び運用のセキュリティ　など

（4）情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示

2　情報セキュリティマネジメントの運用・継続的改善に関すること

（1）情報資産の管理

情報資産台帳の維持管理，媒体の管理，利用状況の記録　など

（2）部門の情報システム利用時の情報セキュリティの確保

マルウェアからの保護，バックアップ，ログ取得及び監視，情報の転送における情報セキュリティの維持，脆弱性管理，利用者アクセスの管理，運用状況の点検　など

（3）業務の外部委託における情報セキュリティの確保

外部委託先の情報セキュリティの調査，外部委託先の情報セキュリティ管理の実施，外部委託の終了　など

（4）情報セキュリティインシデントの管理

発見，初動処理，分析及び復旧，再発防止策の提案・実施，証拠の収集　など

（5）情報セキュリティの意識向上

情報セキュリティの教育・訓練，情報セキュリティに関するアドバイス，内部不正による情報漏えいの防止　など

（6）コンプライアンスの運用

順守指導，順守状況の評価と改善　など

（7）情報セキュリティマネジメントの継続的改善

問題点整理と分析，情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の見直し　など

（8）情報セキュリティに関する動向・事例情報の収集と評価

参考　シラバス（情報処理技術者試験における知識・技能の細目）について

情報セキュリティマネジメント試験の出題範囲を詳細化し，求められる知識の幅と深さを体系的に整理・明確化した「シラバス」（情報処理技術者試験における知識・技能の細目。各項目の学習目標，内容，用語例等から構成）を公開しているので，学習又は教育の指針として活用されたい。

http://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.html

Ver 2.0　平成 27 年 10 月 16 日

■情報処理技術者試験　試験要綱（情報セキュリティマネジメント試験 抜粋版）

IPA 独立行政法人 情報処理推進機構
IT人材育成本部 情報処理技術者試験センター

〒113-8663　東京都文京区本駒込 2-28-8
文京グリーンコートセンターオフィス 15 階
TEL 03-5978-7600（代表）
FAX 03-5978-7610

詳しくは･･･
http://www.jitec.ipa.go.jp