情報処理安全確保支援士
試験
（レベル４）
シラバス

－知識・技能の細目　－

Ver 1.0

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

本シラバスに記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，本シラバスでは，® 及び TM を明記していません。

大項目	小項目	概　要	要求される知識	要求される技能
1　情報システムの脆弱性・脅威分析	1-1　情報資産の評価	開発対象システムを分析し，リスクを考える上で対象となる情報資産（システム，データ，人材，ドキュメントなど）を整理し，文書精査，ヒアリングなどを通じて，情報セキュリティの観点（機密性，完全性，可用性，システムの稼働に与える影響度）から，資産の価値を明確にする。	・情報収集の手法，手順，実践に関する知識 ・関連法令（不正アクセス禁止法，特定電子メール送信適正化法，個人情報保護法，電子署名法，サイバーセキュリティ基本法など），標準，ガイドラインなどに関する知識 ・組織のIT資産に関する知識 ・組織の情報システム及びネットワーク構成に関する知識 ・IT資産の評価及び計量化の手法に関する知識 ・文書化に関する知識	・調査に関する目標とスコープを設定する能力 ・組織のIT資産に対し，細部にまで気がつく能力 ・組織内におけるIT資産のフローを理解する能力 ・IT資産を合理的に整理する能力
	1-2　リスクの特定（脆弱性・脅威の検出）	開発対象システムについて，情報資産のリスク因子（脆弱性，脅威など）に関する情報を分析し，発現した際にシステムに重大な影響をもたらすと懸念されるリスク，及び結果として生じる損失の大きさが確定できないリスクを特定する。	・情報収集の手法，手順，実践に関する知識 ・IT資産が関係した事件・事故の事例に関する知識 ・リスク因子及び評価に関する知識 ・情報システム及びネットワークのアーキテクチャ，技術と運用，ハードウェア，ソフトウェアに関する知識 ・IT資産に関する知識 ・新しいプラットフォーム（クラウドコンピューティング，仮想化，モバイル，組込みシステム，Web技術）に関する知識	・IT資産損失の大きさ(失われた資産価値，原因究明及び復旧費用，社会的説明費用)を算定・評価する能力 ・調査に関する目標とスコープを設定する能力 ・組織のIT資産に関してリスクを漏れなく列挙する能力 ・IT資産とリスクを関係付けて合理的に整理する能力 ・情報収集を継続的に行う能力 ・脆弱性及び脅威を合理的に把握する能力 ・新しいプラットフォームにおけるリスク因子（脆弱性，脅威）を合理的に摘出する能力
	1-3　リスクの算定	特定したリスクについて，各リスクが発現する確率及びリスクが発現した場合の影響の大きさを，定量的又は定性的に把握することによって，リスクの大きさを算定する。	・リスクの発現する確率についての経験的データに関する知識 ・確率及び統計に関する知識 ・セキュリティ対策のコスト算定に関する知識	・IT資産損失の大きさ(失われた資産価値，原因究明及び復旧費用，社会的説明費用)を算定・評価する能力 ・調査に関する目標とスコープを設定する能力 ・継続的に情報収集を行う能力
	1-4　リスクの評価	特定した各リスクについて，追加の対応が必要か否かを判断するためのリスク受容基準[1)]を作成する。その上で，算定したリスクの大きさをリスク受容基準に照らして，対策を追加すべきリスクを明らかにすると	・セキュリティ対策のコストに関する知識 ・リスク受容基準に関する知識	・リスク受容基準を作成する能力 ・対策を優先順位づけする能力

大項目	小項目	概　要	要求される知識	要求される技能
		ともに，それらの対応すべきリスクの優先順位を決定する。		
	1-5　リスク対応の選択	リスク対応には，リスク回避，リスク移転，リスク最適化及びリスク保有がある。組織の情報セキュリティポリシに従い，リスクの種類に応じて，適切な対策を策定し組み合わせて選択する。また，緊急時，災害時といった異常事態に対する管理策を考慮する。	・ リスク対応に関する知識 ・ 情報システム及びネットワークのアーキテクチャ，ハードウェア，ソフトウェア，運用に関する知識 ・ 情報収集の手法，手順，実践に関する知識	・ 組織のIT資産に関してリスクを漏れなく列挙する能力 ・ リスクと対応を合理的に整理する能力 ・ 調査結果を分析する能力
2　セキュリティ要件定義	2-1　セキュリティ要件定義のための情報収集・分析	セキュリティ要件を明らかにするため，組織の情報セキュリティポリシに基づく要求，現行システムの問題点及び新しい要求を分析する。その際には，調査範囲の検討，調査の実施，調査結果の整理，セキュリティ対策ニーズの整理，前提条件・制約条件の整理，概要業務フローの整理，解決策・システム化範囲の検討などを実施する。	・ 業務内容，用語に関する知識 ・ 情報収集方法に関する知識 ・ 業務分析手法に関する知識 ・ モデル化技法に関する知識 ・ システム工学に関する知識 ・ ハードウェアに関する知識 ・ ソフトウェアに関する知識 ・ ネットワークに関する次の知識 　・ プロトコル 　・ トポロジ 　・ 経路制御 ・ 運用管理に関する知識 ・ データベースに関する知識 ・ セキュリティに関する次の知識 　・ パスワード，アカウント管理 　・ 暗号技術，認証技術，ディジタル署名技術，PKI 　・ マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 　・ アプリケーションセキュリティ対策 　・ データベースセキュリティ対策 　・ ネットワークセキュリティ対策 　・ システムセキュリティ対策 　・ 物理的セキュリティ対策 　・ ログ管理技術 　・ アクセス制御 　・ 特権の最小化 　・ 攻撃手法（なりすまし，盗聴，改ざん，	・ 情報収集の手法，手順を実践に移す能力 ・ 調査に関する目標とスコープを設定する能力 ・ 要求及び制約条件を明確にする能力 ・ 業務をモデル化し，分析する能力 ・ システム化に当たってのニーズ，前提条件，制約条件を分類する能力 ・ アプリケーションシステムの分析を行う能力 ・ 情報システムで対応できるか否かを判断する能力 ・ セキュリティ上の問題点を的確に把握する能力 ・ ネットワークアーキテクチャの分析を行う能力 ・ セキュリティに関する事件・事故，技術動向を適切に収集し，その影響度を分析する能力

大項目	小項目	概　要	要求される知識	要求される技能
			SQLインジェクション,クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・ セキュリティエコノミクスに関する知識 ・ ITの技術動向（IoT，ビッグデータ，AIなどを含む）に関する知識	
	2-2　セキュリティアーキテクチャの設計	開発対象システムのセキュリティ要件を実現するために，関連するハードウェア，ソフトウェア，ネットワーク，運用管理の全体構造をセキュリティアーキテクチャとして設計する。	・ ハードウェア（仮想化技術を含む）に関する知識 ・ ソフトウェア（クラウドコンピューティング技術を含む）に関する知識 ・ ネットワークに関する次の知識 　・ プロトコル 　・ トポロジ 　・ 経路制御 ・ 運用管理に関する知識 ・ データベースに関する知識 ・ セキュリティに関する次の知識 　・ パスワード・アカウント管理 　・ 暗号技術，認証技術，ディジタル署名技術，PKI 　・ マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 　・ アプリケーションセキュリティ対策 　・ データベースセキュリティ対策 　・ ネットワークセキュリティ対策 　・ システムセキュリティ対策 　・ 物理的セキュリティ対策 　・ ログ管理技術 　・ アクセス制御 　・ 特権の最小化 　・ 攻撃手法（なりすまし，盗聴，改ざん，SQLインジェクション,クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・ ISO/IEC 15408（JIS X 5070）に関する知	・ 暗号技術，認証技術，ディジタル署名技術などのセキュリティ技術を統一のとれた観点で一つの情報システムにまとめ提案する能力 ・ 情報セキュリティ対策基準からハードウェア，ソフトウェアに関するセキュリティ要件を導出する能力 ・ リスク分析で行ったIT資産の評価に従って，適切な物理的セキュリティ対策を適用する能力 ・ 物理的に重要なIT資産を隔離できるように情報システムを統合化する能力 ・ セキュリティシステムの設計要件からネットワークの設計要件を導出する能力 ・ セキュリティシステムを実現するセキュリティ製品を選択する能力 ・ 費用対効果を考慮して適切なセキュリティ製品を選択する能力

大項目	小項目	概　要	要求される知識	要求される技能
			識 ・ 信頼性設計に関する知識 ・ 実装方式及び要求事項の文書化に関する知識 ・ セキュリティ関連標準化に関する知識	
	2-3　セキュリティ要件の決定	脆弱性・脅威分析の結果として決められた，優先度の高いリスクへの対応を中心に，開発対象システムの問題点，新しい要求事項から，開発対象システムにおけるセキュリティ要件を決定する。開発対象システムがネットワークシステムであれば，例えばファイアウォール，侵入検知装置の導入などが要件となり，開発対象システムが業務アプリケーションであれば，利用者認証機構，権限定義に基づいたアクセス制御機構などがセキュリティ要件となる。	・ 情報システムの機能とオペレーションに関する知識 ・ 開発プロセスと開発技術に関する知識 ・ ソフトウェアの品質要件に関する知識 ・ 品質保証に関する知識 ・ セキュリティ技術に関する知識 ・ ソフトウェアのテストに関する知識 ・ ミドルウェア，ツール及びプログラム言語などの開発環境に関する知識 ・ コスト見積りに関する知識 ・ データベースに関する知識 ・ ネットワークに関する知識 ・ 運用管理に関する知識 ・ 情報システムの構築目的に関する知識 ・ 情報システムの基本機能に関する知識 ・ 情報システムのプロトタイピングに関する知識 ・ 情報システムのテスト手法に関する知識 ・ 情報システムの移行に関する知識 ・ 情報システムの運用及び保守に関する知識	・ システム要求事項とセキュリティ要件とを関連づける能力 ・ 情報セキュリティ対策基準から，認証と権限に関するシステム要件を導出する能力 ・ 認証と権限の関係の整合性を保って，論理的に組み立てる能力 ・ 利用者の要求をセキュリティ要件として翻訳する能力 ・ 相反する要求を認識し，総合的な解決策を提示する能力 ・ 要求事項に対して効果的な技術を適用する能力 ・ データの重要度について分析する能力 ・ 情報の正確性，一貫性について分析する能力 ・ 効率的なテスト手法を選択する能力 ・ 効果的なプロトタイプを設計する能力
	2-4　セキュリティ要件定義書の作成	決定したセキュリティ要件を実現するセキュリティ対策に関する次に示す項目を定義し，セキュリティ要件定義書として提示するための文書化を行う。 ・セキュリティ対策の目標と範囲 ・セキュリティ機能と性能 ・業務・組織・利用者への要求事項 必要に応じて，ハードウェア，ソフトウェア，ネットワーク，運用管理それぞれの要求作成を検討する。	・ システム開発環境，システム運用環境に関する知識 ・ システム要件定義書に盛り込むべき事項，及び注意点に関する知識	・ 重点事項を明確に記述する能力
	2-5　セキュリテ	開発対象システムにおける利用者の要求と	・ レビューの進め方に関する知識	・ システム要件定義レビューに適したコミ

大項目	小項目	概　要	要求される知識	要求される技能
	ィ要件定義書の評価とレビュー	の一貫性，システム設計上の実現可能性，テスト計画性，運用・保守の実現可能性，組織の情報セキュリティポリシへの準拠性を考慮して，システム設計者と共同でレビューを実施する。	・システム開発環境，システム運用環境に関する知識 ・システム要件定義書に盛り込むべき事項，及び注意点に関する知識	ュニケーション方法を選択する能力 ・対立意見を適切に評価する能力 ・問題点を明確化し，解決策を導き出す能力
3　セキュリティ機能の設計	3-1　セキュリティ機能方式の決定と評価	セキュリティ要件を実現するために，セキュリティアーキテクチャを前提にして，ハードウェア，ソフトウェア，ネットワーク，運用管理のそれぞれに対し，セキュリティ機能の実装方式を検討する。開発対象システムにおける利用者の要求との一貫性，システム設計上の実現可能性，テスト計画性，運用・保守の実現可能性を考慮して，システム設計者と共同でレビューを実施した上で，セキュリティ実装方式設計書として文書化し，全体システム設計書に組み込む。	・ハードウェアに関する知識 ・ソフトウェアに関する知識 ・ネットワークに関する次の知識 　・プロトコル 　・トポロジ 　・経路制御 ・運用管理に関する知識 ・データベースに関する知識 ・セキュリティに関する次の知識 　・パスワード・アカウント管理 　・暗号技術，認証技術，ディジタル署名技術，PKI 　・マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 　・アプリケーションセキュリティ対策 　・データベースセキュリティ対策 　・ネットワークセキュリティ対策 　・システムセキュリティ対策 　・物理的セキュリティ対策 　・ログ管理技術 　・アクセス制御 　・特権の最小化 　・攻撃手法（なりすまし，盗聴，改ざん，SQLインジェクション，クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・システム方式設計の概念及び技術に関する知識 ・システム方式設計書の記述事項に関する知識 ・運用及び保守に関する知識	・システム方式の内容について正確に文書化する能力 ・システム化案の各候補を評価し，関係者に対して説明する能力 ・システム方式に関して，システムのコアとなる要件を識別する能力 ・費用対効果を配慮して，技術的な選択を行う能力 ・一貫した基準でシステム要件を割り振る能力 ・システム要求事項を解釈し，システム方式と関連付ける能力 ・情報システムの論理的一貫性を分析し，組み立てる能力 ・問題点の核心を把握し，解決する能力 ・ソフトウェア要求事項を正確に文書化する能力 ・ソフトウェアの使用条件を明確化する能力 ・利用者のニーズを的確に把握し，システムに反映する能力 ・業務を理解する能力 ・業務運用に必要な事項を把握する能力 ・運用及び保守をシミュレーションする能力 ・脅威を分析し，対策を選定する能力 ・必要となるネットワーク構成をまとめる能力 ・システム要件及びシステム設計を解釈し，ソフトウェア要求事項と関連付ける能力

大項目	小項目	概　要	要求される知識	要求される技能
			・ レビュー方法（ピアレビュー，ウォークスルーレビュー，インスペクションなど）に関する知識 ・ 性能予測に関する知識 ・ テスト手法に関する知識	
	3-2　セキュリティ実装の設計	ハードウェア，ソフトウェア，ネットワーク，運用管理のそれぞれに対し，セキュリティ要件定義の実現に必要な機能の設計を行う。また，セキュリティ実装に関する作業計画を作成し，他システム設計者と共同でレビューを行う。	・ ソフトウェア設計技法に関する知識 ・ 利用可能なプラットフォームに関する知識 ・ 構造化設計に関する知識 ・ オブジェクト指向設計技法に関する知識 ・ 情報システム構成に関する知識 ・ アルゴリズムに関する知識 ・ ソフトウェア詳細設計に関する知識 ・ プログラムロジックを正確に文書化するための表現技法に関する知識 ・ CASEツール，統合開発環境に関する知識 ・ プログラム言語に関する知識 ・ レビュー方法（ピアレビュー，ウォークスルーレビュー，インスペクションなど）に関する知識	・ システム仕様書の内容を理解でき，サブシステムをコンポーネントに分解する能力 ・ コンポーネント間のインタフェースを矛盾なく設計できる能力 ・ 要求品質を具現化する能力 ・ 拡張性，汎用性，信頼性などの構造を実現する能力 ・ ソフトウェアコンポーネントをシステム仕様に対して矛盾なく設計する能力 ・ 検討事項を整理し，詳細仕様としてまとめる能力 ・ 最適な設計技法を選択する能力 ・ 情報システムに最適な開発環境を選択する能力
	3-3　セキュリティ実装テスト仕様の作成	テスト要件に基づき，ソフトウェアであればコンポーネントテスト仕様及びユニットテスト仕様，ネットワークであれば接続テスト仕様などの作成を行う。	・ ユニットテスト仕様の設計に関する知識 ・ テストツールに関する知識 ・ 開発プロセスに関する知識 ・ 運用環境に関する知識 ・ プログラム言語に関する知識 ・ 実装環境に関する知識	・ ユニットテスト計画を作成する能力 ・ コンポーネントテスト計画を作成する能力 ・ システムテスト計画を作成する能力
4　セキュリティ機能の実装とテスト	4-1　セキュリティ機能の実装	ハードウェア，ソフトウェア，ネットワーク，運用管理のそれぞれに対し，セキュリティ機能の実装を行う。ソフトウェア実装においては，セキュアプログラミングの手法を用いることが求められる。ネットワーク実装においては，ファイアウォール，侵入検知システム，認証 VLAN，検疫ネットワークなどのセキュリティ対策装置の採用を検討する。	・ コードの開発方法論に関する知識 ・ SQLプログラミングに関する知識 ・ 解読容易性，効率性，保守容易性などプログラム品質に関する知識 ・ 該当アプリケーションシステムの開発に適したプログラム言語の選択に関する知識 ・ 既存コンポーネントの再利用に関する知識 ・ オブジェクト指向設計技法に関する知識 ・ レビュー方法（ピアレビュー，ウォーク	・ 詳細仕様を踏まえて，プログラム作成指針を明確化する能力 ・ 処理内容を簡潔に文書化する能力 ・ 複雑で難易度の高いロジックに対して代替のコードを作成し，比較評価する能力 ・ 情報システムの体系／階層を理解する能力 ・ 要求されるソフトウェア品質を実装する能力 ・ 拡張性，汎用性，信頼性などをもったプログラム構造を提供する能力

大項目	小項目	概　要	要求される知識	要求される技能
			スルーレビュー，インスペクションなど）に関する知識 ・ セキュアプログラミングに関する知識（プログラム言語，ウェブアプリケーション開発，ソフトウェア脆弱性対策技術など） ・ ネットワークプロトコル，トポロジ，経路制御，ネットワークハードウェアに関する知識	
	4-2　システムテストの支援	開発するセキュリティ機能のユニットテスト，コンポーネントテストを主体的に実施するとともに，システムテストを支援する。さらに開発対象システムについて，脆弱性テストやセキュリティ侵入テストを実施する。	・ ユニットテスト手続に関する知識 ・ コンポーネントテスト手続に関する知識 ・ システム要件テスト手続に関する知識 ・ システムテスト手続に関する知識 ・ ソフトウェアが仕様どおりに実装されていることを確認する手法に関する知識 ・ 情報システムが仕様どおりに実装されていることを確認する手法に関する知識 ・ 反復テストプロセスに関する知識 ・ エラー分析と解決プロセスに関する知識 ・ セキュリティ侵入テストを実施するための攻撃手法，脆弱性に関する知識 ・ セキュリティ評価テスト技法に関する知識（ホワイトボックス，ブラックボックス，ペネトレーションテスト，マルウェア解析など）	・ 不具合や障害を識別し，解決，是正する能力 ・ 状況を調査，分析し，解決策を提案する能力 ・ システムの体系や階層を理解する能力 ・ プロセスと結果を体系的に整理し，詳細な裏付け文書として文書化する能力 ・ 技術的又はシステム的欠陥によって，利用者が求める要件を満足できない場合の代替案を考案する能力 ・ セキュリティ侵入テストを漏れなく計画，実施する能力
	4-3　関連文書の更新	利用者マニュアル及びこれまでに実装したセキュリティ機能に関するシステム文書類（外部設計書，内部設計書，機能仕様書など）の更新を行う。また，必要があれば，その結果を組織の情報セキュリティポリシにフィードバックする。	・ 利用者マニュアルの書き方に関する知識 ・ システム文書の書き方に関する知識 ・ 文書の更新手続きに関する知識 ・ 情報システムの運用に関する知識	・ 関係者に対して，利用者マニュアルの変更点及び変更理由について明快に説明する能力 ・ 情報システムの設計又は実装の変更内容を既存のシステム文書に適切に反映する能力
5　セキュリティ機能の本番移行	5-1　開発対象システムの本番移行の支援	組織の情報セキュリティポリシに準拠して，開発対象システムの移行計画の作成及び移行を支援する。	・ 情報セキュリティポリシを理解するための知識 ・ 利用者の既存システムに関する知識 ・ ソフトウェアの導入に関する知識 ・ 既存システムとの並行運転に関する知識	・ 情報セキュリティポリシを理解する能力 ・ 利用者の業務への影響を最小にしてソフトウェアを移行する計画を立てる能力 ・ 立ち上げ作業時に利用者を支援する能力
	5-2　開発対象システムの受	発注者による，開発対象システムの受入れレビュー及び受入れ検査の実施を支援す	・ システムテスト及びシステム要件テストの結果の検査に関する知識	・ 利用者の要求する受入れ支援業務を実施する能力

大項目	小項目	概　要	要求される知識	要求される技能
	け入れ検査支援	る。	・ 受入れレビューに関する知識 ・ 受入れ検査に関する知識	
	5-3　運用担当者の教育・訓練及び支援	開発されたセキュリティ機能に関して，システム運用担当者の教育・訓練プログラムを開発し，実際の教育・訓練を支援する。	・ 運用担当者が必要とするソフトウェア操作に関する知識 ・ 外部のセキュリティ診断サービスに関する知識 ・ セキュリティ事件・事故に関する知識 ・ ネットワーク攻撃に関する知識 ・ システムログ，アクセスログに関する知識	・ 運用担当者のソフトウェア操作能力に応じた教育・訓練及び支援を計画する能力 ・ 運用担当者の教育・訓練及び支援を実施する能力 ・ セキュリティ事件・事故の原因を分析する能力 ・ システムログ，アクセスログを分析する能力 ・ 習得した技術をセキュリティシステムの運用管理に適用させる能力
	5-4　システム利用者対応	利用者に対するサポートの範囲を決定し，具体的なサポート内容を提示する。特に，利用者に対する教育訓練の計画と実施，ヘルプデスクの設置と対応に重点を置く。実施したサポートに関しては，記録するとともに，問題点を明確にし，改善策を実施する。	・ セキュリティ事件・事故に関する知識 ・ IT資産へのリスクに関する知識 ・ 社内規則及びセキュリティポリシに関する知識 ・ 文書化及びその蓄積に関する知識 ・ セキュリティツールに関する知識 ・ 利用者が用いるOS，アプリケーションシステム，ネットワークシステムに関する知識 ・ 利用者が必要とするネットワーク設定に関する知識 ・ 情報収集方法に関する知識 ・ 利用者のニーズに関連する技術情報，ノウハウ，資料に関する知識	・ 業務遂行によって蓄積されたノウハウ，実績などを制度化及び文書化する能力 ・ 保守手順の概要を記述する能力 ・ ニーズを認識，分析し，ニーズを充足する解決策を提供する能力 ・ 教育訓練内容について，正確，簡潔に記述する能力 ・ 利用者の能力を評価し，適合する教育目標を設定する能力 ・ 教育・訓練環境を整備する能力 ・ 理解度・技術レベルに合わせて指導，助言する能力
6　情報セキュリティ面からのレビュー	6-1　開発対象システムのセキュリティレビュー	開発対象システムで採用された各技術方式，プロトコルについて，情報セキュリティ面から見た安全性，信頼性を検証し，さらに，組織の情報セキュリティポリシへの準拠性を確認して，各レビュー依頼者にフィードバックする。	・ ハードウェアに関する知識 ・ ソフトウェアに関する知識 ・ ネットワークに関する次の知識 　・ プロトコル 　・ トポロジ 　・ 経路制御 ・ 運用管理に関する知識 ・ データベースに関する知識 ・ セキュリティに関する次の知識 　・ パスワード・アカウント管理 　・ 暗号技術，認証技術，ディジタル署名技術，PKI	・ システム方式の内容について正確に理解する能力 ・ システム化案の各候補を評価する能力 ・ システム方式に関して，システムのコアとなる要件を識別する能力 ・ 費用対効果を配慮して，技術的な選択を行う能力 ・ システム要求事項を解釈し，システム方式と関連付ける能力 ・ 情報システムの論理的一貫性を分析し，組み立てる能力 ・ 問題点の本質を把握し，解決する能力

大項目	小項目	概　要	要求される知識	要求される技能
			・ マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 ・ アプリケーションセキュリティ対策 ・ データベースセキュリティ対策 ・ ネットワークセキュリティ対策 ・ システムセキュリティ対策 ・ 物理的セキュリティ対策 ・ ログ管理技術 ・ アクセス制御 ・ 特権の最小化 ・ 攻撃手法（なりすまし，盗聴，改ざん，SQLインジェクション，クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・ レビュー方式に関する知識 ・ フィードバックに関する知識	・ 新たな攻撃手法に関する情報を収集し，その影響度を評価する能力
7　情報システム運用時のセキュリティ管理の支援	7-1　セキュリティ管理体制の確立の支援	組織の情報セキュリティポリシに基づく，システム運用時のセキュリティ管理体制の確立，管理規程の策定を支援する。また，セキュリティ侵入に対する技術的な防止策の立案，実施について，情報セキュリティ管理者を支援する。さらに，利用者に対するセキュリティ教育計画の作成を支援する。	・ セキュリティ要件に関する知識 ・ 不測事態対応計画，業務継続計画に関する知識 ・ 潜在的なリスクに関する知識 ・ セキュリティ侵入の発生事例に関する知識 ・ セキュリティ対策技術と実施事例に関する知識 ・ セキュリティ対策手法のコストに関する知識 ・ ハードウェアに関する知識 ・ ソフトウェアに関する知識 ・ ネットワークに関する次の知識 　・ プロトコル 　・ トポロジ 　・ 経路制御 ・ 運用管理に関する知識 ・ データベースに関する知識 ・ セキュリティに関する次の知識 　・ パスワード・アカウント管理	・ 組織におけるセキュリティ侵入の可能性を識別する能力 ・ 組織の情報セキュリティポリシ，及び情報システムに組み込まれたセキュリティを理解する能力 ・ セキュリティ対策に関わる費用対効果を算定する能力 ・ 物理的セキュリティ対策，技術的セキュリティ対策，及び管理的セキュリティ対策の立案を支援する能力

大項目	小項目	概　要	要求される知識	要求される技能
			・暗号技術，認証技術，ディジタル署名技術，PKI ・マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 ・アプリケーションセキュリティ対策 ・データベースセキュリティ対策 ・ネットワークセキュリティ対策 ・システムセキュリティ対策 ・物理的セキュリティ対策 ・ログ管理技術 ・アクセス制御 ・特権の最小化 ・攻撃手法（なりすまし，盗聴，改ざん，SQLインジェクション，クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・サプライチェーンリスクに関する知識 ・情報セキュリティ教育に関する知識 ・ユーザセキュリティ管理に関する知識 ・システム開発（オフショア開発環境）におけるセキュリティ管理に関する知識	
	7-2　セキュリティ侵入の監視の支援と状況分析の支援	セキュリティ侵入の監視情報を収集し，状況を分析して，情報セキュリティ管理者に報告する。報告に際して，「新種のウイルス情報」，「セキュリティ対策事例」など，セキュリティ関連情報を添付する。	・セキュリティ侵入の種類及び個々の特性に関する知識 ・セキュリティ侵入の発見技術に関する知識 ・過去のセキュリティ侵入事例に関する知識 ・セキュリティ侵入対策実施に関する知識 ・情報システムの利用モニタリングに関する知識 ・脆弱性のチェックを行うツールに関する知識 ・運用手続上の例外に関する知識 ・組織内の連絡体制及び責任体制に関する知識	・セキュリティ侵入の兆候を判別する能力 ・些細な記録から，重大な攻撃の事実を発見したり，予測したりする能力 ・セキュリティ侵入の兆候がセキュリティ侵入にまで至るかどうかを判定する能力 ・発生したセキュリティ侵入の重大度を判定する能力 ・発生したセキュリティ侵入の業務への影響度を判定する能力 ・運用手続の抜け道を発見し，悪用を阻止する能力 ・セキュリティ違反を速やかに発見する能力 ・システムログ，アクセスログを分析する

大項目	小項目	概　要	要求される知識	要求される技能
			・ 事故の公表に関する知識 ・ 情報セキュリティポリシに関する知識 ・ リスク分析の結果，IT資産の重要度に関する知識 ・ 情報システム及びネットワークシステムに関する知識 ・ システム運用に関する知識 ・ セキュリティ監視データの分析に関する知識 ・ 事故原因の追求手順に関する知識 ・ ディジタルフォレンジックスに関する知識	能力
	7-3　セキュリティ強度の確認の支援	脆弱性テストやセキュリティ侵入テストの実施による定期的なセキュリティ強度の分析・評価を支援する。問題点を発見した場合は，強度向上のための対策を立案する。	・ セキュリティ攻撃ツールに関する知識 ・ 脆弱性に関する知識 ・ セキュリティ勧告に関する知識 ・ セキュリティ機能の検証又は脆弱性のチェックを行うツールに関する知識 ・ 情報システム及びネットワークシステムのアーキテクチャに関する知識 ・ ネットワーク攻撃に関する知識	・ 脆弱性及びセキュリティの情報を継続的に収集する能力 ・ ネットワーク攻撃を行う能力 ・ 様々な攻撃ツールを駆使して強度を確認する能力 ・ 発見された脆弱性に対して速やかに対処する能力
	7-4　セキュリティ侵入への対応の支援	システムログ，システムエラーログ，アラーム記録，トラフィックパターンの分析，システムの整合性チェックによって，不正侵入などのセキュリティ侵入を発見する技術的支援を行う。 セキュリティ侵入による被害状況や被害範囲を調査し，損失の大きさを評価する。セキュリティ情報，侵入に関する様々な情報，システムログ，アクセスログなどを収集して，侵入原因の特定を支援する 同様のセキュリティ侵入が発生しないように，恒久的な再発防止策を検討し，提案する。必要に応じて，システムの再構築の支援を行う。	・ ネットワークアーキテクチャ，トポロジ，ハードウェア及びソフトウェアに関する知識 ・ 監視の手順に関する知識 ・ 不正侵入検知ツールに関する知識 ・ セキュリティ侵入を受けたときの対処に関する知識 ・ 脆弱性と対策パッチに関する知識 ・ マルウェアに関する知識	・ セキュリティ侵入時に適切な対応を取る能力 ・ ネットワーク監視や不正侵入検知ツールを利用する能力 ・ ワクチンツールを利用する能力 ・ 事故原因から適切な対処方法を選択する能力 ・ 事故の緊急性，早期復旧への方策を迅速に判断する能力 ・ 初動処理を適切に行う能力 ・ IT資産の重要度から，処置の優先順位を決定する能力 ・ JPCERT/CC,IPAなどと連絡をとって適切な処理が行える能力 ・ 事実を正確に記録し連絡する能力
	7-5　セキュリティの評価の支援	最新の脅威，脆弱性及び侵入についての情報を収集し，さらにシステムの脆弱性，情報セキュリティポリシの遵守状況を評価す	・ 脆弱性情報やセキュリティ勧告及びパッチ情報に関する知識 ・ セキュリティテスト項目に関する知識	・ 脅威，脆弱性及び侵入に関する情報を漏れなく収集する能力 ・ 外部のサービスの優劣を判断する能力

大項目	小項目	概　要	要求される知識	要求される技能
		る。	・ 外部のセキュリティ診断サービスに関する知識 ・ システム監査（のセキュリティ側面）に関する知識	
8 開発プロジェクトの管理[2)]	8-1 開発ライフサイクル管理	企画，要件定義，開発・調達，運用・保守といった情報システムのライフサイクルの各ステージにおいて，開発プロジェクトのセキュリティを維持するために有効なセキュリティ対策を行う。この対策には，開発において機密性，完全性，可用性が失われた際の影響の識別及び分類，開発対象システムにおける情報セキュリティポリシから見た要求事項の検討，セキュリティコストの検討，情報セキュリティを維持するための計画策定（構成管理，緊急時対応，教育，リスクアセスメントなど），詳細管理策の立案，情報セキュリティの評価（管理策の有効性の評価），継続的な監視，記録媒体の廃棄，ハードウェア，ソフトウェアの処分などが含まれる。	・ リスク因子に関する知識 ・ セキュリティ対策のコスト算定に関する知識 ・ 危機管理に関する知識 ・ 機密漏えいに関する知識 ・ 事業継続管理に関する知識 ・ 機密情報の管理手順に関する知識 ・ ハードウェアに関する知識 ・ ソフトウェアに関する知識 ・ ネットワークに関する知識 ・ 運用管理に関する知識 ・ データベースに関する知識 ・ セキュリティに関する次の知識 　・ パスワード・アカウント管理 　・ 暗号技術，認証技術，ディジタル署名技術，PKI 　・ マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術 　・ アプリケーションセキュリティ対策 　・ データベースセキュリティ対策 　・ ネットワークセキュリティ対策 　・ システムセキュリティ対策 　・ 物理的セキュリティ対策 　・ ログ管理技術 　・ アクセス制御 　・ 特権の最小化 　・ 攻撃手法（なりすまし，盗聴，改ざん，SQLインジェクション，クロスサイトスクリプティング，DoS/DDoS攻撃，フィッシング，ソーシャルエンジニアリング，標的型攻撃，ランサムウェアなど） ・ 文書管理に関する知識 ・ バックアップツールに関する知識	・ IT資産損失の大きさ（失われた資産価値，原因究明及び復旧費用，社会的説明費用）を算定，評価する能力 ・ バックアップデータやセキュリティ監視データの保管方法を決定する能力 ・ 情報セキュリティ対策基準を基にセキュリティシステムを実際に運用する場面で用いる手続を作成する能力 ・ リスクと対策を合理的に整理する能力

大項目	小項目	概　要	要求される知識	要求される技能
			・ リスクアセスメントに関する知識 ・ 教育計画に関する知識 ・ 構成管理に関する知識 ・ 緊急時対応に関する知識 ・ 記録媒体の処分に関する知識	
	8-2　セキュリティ違反への対処	開発対象プロジェクトで使用するシステム環境において，システムの使用状況，システムログ，アクセスログ，アラーム，トラフィックパターンを監視，記録し，セキュリティ違反を検出する。	・ 緊急時対応マニュアルの作成に関する知識 ・ 障害復旧計画，復旧対策に関する知識 ・ 脆弱性情報の収集に関する知識 ・ セキュリティ侵入報告機関に関する知識 ・ ディジタルフォレンジックスに関する知識 ・ 不正アクセス対策に関する知識 ・ インシデント対応に関する知識 ・ マルウェア（ウイルス，スパイウェア，ボット，ワーム，悪意あるアドウェア，クラックツールなど）対策技術に関する知識	・ 些細な記録から重大な攻撃の事実を発見したり，予測したりする能力 ・ セキュリティ違反者に対し，適切に警告を行う能力 ・ IT資産の重要度から，処置の優先順を決定する能力 ・ 事故内容についての詳しい記録を残す能力 ・ 事故の緊急性，早期復旧への方策を短期間で判断し対処する能力 ・ 発見された脆弱性に対して速やかに対処する能力 ・ 慎重にネットワーク攻撃状況を調査分析する能力
	8-3　セキュリティパッチの適用作業	開発対象プロジェクトで使用するハードウェアのファームウェア，ソフトウェア（特に，OS，ウイルス対策ソフト，ウイルス定義ファイルなど）に関するセキュリティパッチの適用作業を支援する。	・ 脆弱性情報公開機関に関する知識 ・ セキュリティパッチの適用手順に関する知識 ・ バックアップの取得と復旧に関する知識 ・ ハードウェアのファームウェアを更新する手法に関する知識 ・ ハードウェア，ソフトウェアのライセンス契約に関する知識 ・ ハードウェア，ソフトウェアベンダサポートに関する知識	・ ハードウェア，ソフトウェア，ネットワークに必要なパッチ情報を選択する能力 ・ パッチ処理（ハードウェアのファームウェアの更新を含む）を障害を起こさずに行う能力
	8-4　システム文書管理	開発上の機密事項，顧客データ（個人情報を含む）などの外部流出を防ぐため，プロジェクトで作成，利用する文書の管理を行う。	・ レビュー手順に関する知識 ・ 紙ファイルの電子化に関する知識 ・ アクセス制限に関する知識 ・ クリアデスク，クリアスクリーンに関する知識 ・ 文書管理に関する知識 ・ 構成管理に関する知識 ・ 記録媒体に関する知識 ・ バックアップツールに関する知識	・ バックアップ手順を作成する能力 ・ バックアップデータの保管方法を決定する能力 ・ 管理規則を文書化し周知する能力

大項目	小項目	概　要	要求される知識	要求される技能
			・機密漏えいに関する知識	
	8-5　人的管理	プロジェクトメンバによる不正行為を防止するため，抑止，防止，検出，回復のそれぞれの対策を実施する。各メンバの情報セキュリティに対する責任を明確化し，共有する。適切な情報セキュリティ教育を行うことで不正行為を未然に防ぐ。	・セキュリティ教育に関する知識 ・内部不正防止に関する知識 ・人的管理手法に関する知識 ・雇用契約に関する知識 ・職務規定に関する知識 ・守秘義務協定に関する知識 ・プライバシ保護，個人情報保護に関する知識 ・セキュリティに関する外部教育サービスに関する知識	・ルールの普及と定着を推進する能力 ・教育訓練内容について，正確，簡潔に記述する能力 ・教育訓練ニーズ・人員の能力を評価し，適合する教育目標を設定する能力 ・セキュリティ上の責任を的確に割り当てる能力 ・不正行為を検知，識別する能力
9　情報セキュリティマネジメントの支援	9-1　情報セキュリティ基本方針の策定支援	組織の情報セキュリティ基本方針の策定又は改定に関して，情報資産の評価，脅威の認識，リスクの識別，対策の整理と調査，リスクの評価を技術的な側面から支援する。	・組織の情報セキュリティポリシに関する知識 ・組織の経営戦略，事業戦略に関する知識 ・組織の情報セキュリティ管理体制に関する知識 ・事業継続管理に関する知識 ・内部統制に関する知識	・事業戦略，事業計画を情報セキュリティポリシに具体化する能力 ・事業継続の観点から情報セキュリティ活動の問題点を分析する能力
	9-2　情報セキュリティ対策基準の策定支援	組織の情報セキュリティ対策基準の策定又は改定を支援するため，組織の活動一般に関する情報セキュリティ関連規定の作成を技術的な側面から支援する。	・情報セキュリティ基本方針に関する知識 ・情報セキュリティ対策基準の標準に関する知識 ・組織の規則体系に関する知識 ・法令，省令又はガイドライン及び法的手続に関する知識 ・雇用契約に関する知識 ・職務規定に関する知識 ・守秘義務協定に関する知識 ・プライバシ保護，個人情報保護に関する知識 ・危機管理に関する知識 ・機密漏えいに関する知識 ・事業継続管理に関する知識 ・機密情報の管理手順に関する知識 ・セキュリティに関する事件・事故の事例に関する知識 ・基準の作成及び更新に関する知識 ・文書管理及び文書変更の手続に関する知識	・対策基準の作成を適切に支援する能力 ・セキュリティに関係する事件・事故の事例を継続的に収集する能力 ・情報セキュリティに関する法令，ガイドライン，規則，規格を継続的に収集する能力

大項目	小項目	概　要	要求される知識	要求される技能
	9-3　情報セキュリティの見直しの支援	組織の情報セキュリティに関する，技術情報の収集と評価，運用上の問題点整理と分析，技術上の問題点整理と分析，新たなリスクの整理と分析を行い，情報セキュリティの見直しを技術的な側面から支援する。	・ セキュリティ事件・事故に関する知識 ・ ベンダ情報，セキュリティ調査機関情報に関する知識 ・ 情報収集の手法，手順，実践に関する知識 ・ 組織の情報システム，ネットワーク構成，運用に関する知識	・ セキュリティ技術関連情報を収集する能力 ・ 情報システム及びネットワークに関係する脆弱性情報，セキュリティ技術を評価選択する能力 ・ 情報セキュリティの運用に関するアンケート調査票を作成し，アンケート調査を実施する能力 ・ 整理されたアンケート調査結果から，システム運用，ネットワーク運用上の情報セキュリティポリシ（方針，基準）の問題点を分析する能力 ・ 分析された問題点に対応した情報セキュリティポリシの見直しを支援する能力 ・ 分析された問題点に対し，経営上対処すべき内容を経営層に報告するための報告資料作成を支援する能力

注 1)　リスク受容基準とは，リスクの重要性の度合いを評価するときに参考とする条件。関連経費，法律及び法令による要求，社会経済及び環境に関する側面，関係者の関心並びにアセスメントに対する優先順位などを要素として含む。

2)　開発プロジェクトの管理においては，上記のタスクに加えて，情報システム運用時のセキュリティ管理の支援に含まれるタスクについても担当することになる。

■情報処理安全確保支援士試験（レベル 4）
シラバス（Ver 1.0）

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
ホームページ：http://www.jitec.ipa.go.jp/

2016.10