情報処理安全確保支援士
試験
（レベル４）
シラバス

ー知識・技能の細目　ー

Ver. 2.1

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

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　情報セキュリティマネジメントの推進又は支援に関すること	1-1　情報セキュリティ方針の策定	経営者による情報セキュリティ方針の策定及び改定について，必要な指導・助言を行い，支援する。	・情報セキュリティガバナンス及びITガバナンスに関する知識 ・マネジメントシステム（ISMS，BCMSなど）に関する知識 ・組織マネジメントに関する知識	・組織内外の利害関係者のニーズと期待，組織内の経営戦略，事業戦略によって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 ・法令，規制，契約，情報セキュリティに関する動向などによって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 ・経営者とコミュニケーションする能力
	1-2　情報セキュリティリスクアセスメント	リスク基準の確立及び維持について，必要な指導・助言を行い，支援する。 リスク特定，リスク分析，リスク評価のプロセスの実施について，必要な指導・助言を行い，支援する。	・情報の特性（機密性，完全性，可用性，真正性，責任追跡性，否認防止，信頼性など）に関する知識 ・リスク，リスク基準，リスク源，脆弱性及び脅威に関する知識 ・情報セキュリティリスクアセスメントのプロセス（特定，分析，評価）に関する知識 ・脅威分析（STRIDE分析，アタックツリー分析（ATA）など）に関する知識	・情報資産損失の大きさ（失われる資産の価値，原因究明及び復旧の費用，社会的説明の費用）を算定し，評価する能力 ・リスク源，脆弱性及び脅威を，新たなITに関するものも含めて列挙する能力 ・情報資産とリスクを関連付けて整理する能力 ・リスクを優先順位付けする能力
	1-3　情報セキュリティリスク対応	情報セキュリティリスクアセスメントの結果に基づく適切な管理策の選定，情報セキュリティリスク対応計画の策定について，必要な指導・助言を行い，支援する。	・リスク対応の選択肢（リスク低減，リスク共有，リスク回避，リスク保有など）に関する知識 ・管理策の実施に要する費用の算定に関する知識 ・サイバー保険に関する知識	・リスクごとに，リスク対応の選択肢を選定する能力 ・リスク対応の実施に適切な管理策を選定する能力 ・情報セキュリティリスク対応計画を作成し，残留リスクと併せて説明する能力
	1-4　情報セキュリティ諸規程の策定	情報セキュリティに関連する諸規程の策定及び改定について，必要な指導・助言を行い，支援する。 事業継続に関する計画の策定及び改定について，必要な指導・助言を行い，支援する。	・法令，規制，規格に関する知識 ・ITの動向（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，AI（生成AIを含む），ビッグデータ，IoTなど）及びその情報セキュリティへの影響に関する知識 ・事業継続に関する知識	・業務プロセス，業務手順を踏まえた上で，情報セキュリティ諸規程で定めるべき事項を検討する能力 ・検討した事項及びその必要性を説明する能力 ・法令，規制，規格の変化やITの動向を踏まえて情報セキュリティ諸規程をレビューする能力

大項目	小項目	概　要	要求される知識	要求される技能
	1-5　情報セキュリティ監査	情報セキュリティ監査及びシステム監査において，監査人を技術的な側面から支援する。 情報セキュリティ監査及びシステム監査の後の監査対象組織による改善計画策定及び改善活動について，必要な指導・助言を行い，支援する。	・情報セキュリティ監査，システム監査，内部監査，業務監査に関する知識 ・監査のプロセス，関連文書（監査計画書，監査調書，監査報告書など）に関する知識 ・監査証拠（システム，ネットワークのログなど）に関する知識	・組織が利用しているセキュリティ技術及び導入している情報セキュリティ対策が十分か，並びに適切に実施されているかを評価する能力 ・事業，業務，情報システム上の制約を考慮した上で，実現可能な管理策を検討し，指導・助言する能力
	1-6　情報セキュリティに関する動向・事例の収集と分析	情報セキュリティに関する事件・事故，傾向と背景，攻撃の手口，脅威，脆弱性及び対策，セキュリティ技術などの情報を収集する。 情報セキュリティに関する法令，規制，規格類の制定・改廃や社会通念の変化，コンプライアンス上の新たな課題などについて把握する。 収集した各情報について，組織内への影響，対応の緊急性，対応の費用・効果・必要性を評価し，報告する。	・JIS，ISO，IEC，IEEE，NISTなどのセキュリティ関連の規格の動向に関する知識 ・業界標準，ガイドラインの動向に関する知識 ・サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）に関する知識 ・攻撃の手口に関する知識 ・攻撃の分析モデル（サイバーキルチェーン，ATT&CKなど）に関する知識 ・脅威インテリジェンス（OSINTなど）に関する知識	・国内外の様々な情報源（公的機関，セキュリティ機関，ベンダからの発表，カンファレンス，論文など）から，必要な情報を，迅速にかつ継続的に収集する能力 ・収集した情報の信頼性，正確さを検証する能力 ・収集した情報を整理し，関係者に伝達する能力 ・収集した情報に関して，組織内への影響などを評価する能力
	1-7　関係者とのコミュニケーション	組織内の課題及び必要な対策といった情報セキュリティに関する情報を，経営層ほか組織内の各層に伝達し，コミュニケーションを促進する。 組織内の情報システムに影響を及ぼす情報を情報システム部門に伝達し，必要な検討，調整が行われるようにする。 外部のセキュリティ機関，情報共有コミュニティ，組織内外の関係者との連絡窓口となって，情報の入手及び提供を行う。	・セキュリティ機関（JPCERT/CC，警察，監督官庁，NISC，IPAなど）に関する知識 ・サイバー情報共有イニシアティブ（J-CSIP），サイバーレスキュー隊（J-CRAT）に関する知識 ・情報セキュリティ早期警戒パートナーシップに関する知識	・情報セキュリティのコミュニティ，イベントに参加し，情報の入手及び提供を行う能力 ・様々な立場の関係者とコミュニケーションする能力 ・連絡窓口として，組織内外の情報連携を担う能力 ・ISAC，他のCSIRTなどと情報共有する，及び共有した情報を活用する能力

大項目	小項目	概　要	要求される知識	要求される技能
2　情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	2-1　企画・要件定義（セキュリティの観点）	調達又は開発するシステムのニーズ及び制約並びに脅威分析の結果からのセキュリティ要件の定義について，必要な指導・助言を行い，支援する。 調達又は開発の仕様書のレビューについて，セキュリティの観点から必要な指導・助言を行い，支援する。	・セキュリティ要件に関する知識 ・セキュリティバイデザイン，プライバシーバイデザインに関する知識 ・システム及びソフトウェア製品の品質要求及び評価（SQuaRE）に関する知識	・調達又は開発するシステムのニーズ及び制約からセキュリティ要件を定義する能力 ・脅威分析の結果からセキュリティ要件を定義する能力 ・仕様書をレビューする能力
	2-2　製品・サービスのセキュアな導入	システム全体又はその一部を構成する製品・サービスの調達について，セキュリティの観点から必要な指導・助言を行い，支援する。 調達した製品・サービスへのセキュアな設定の実施について，必要な指導・助言を行い，支援する。	・製品・サービスの種類と特徴に関する知識 ・ネットワーク機器，サーバの設定に関する知識 ・要塞化（ハードニング）に関する知識 ・セキュリティの投資対効果の評価に関する知識	・製品・サービスの仕様書とセキュリティ要件とを照らして，製品･サービスを選定する能力 ・セキュリティの投資対効果を最適化する能力
	2-3　アーキテクチャの設計（セキュリティの観点）	システム及びネットワークのアーキテクチャの設計，インタフェース，利用する各技術の評価について，セキュリティの観点から必要な指導・助言を行い，支援する。	・システム開発技術，アーキテクチャの設計に関する知識 ・データベース，ネットワークに関する知識 ・信頼性設計（フェールセーフ，フェールソフトなど）に関する知識 ・仮想化，コンテナ技術に関する知識	・アーキテクチャの設計書をレビューする能力 ・システム及びネットワークのアーキテクチャ，インタフェース，利用する各技術がセキュアであるかどうかを評価する能力
	2-4　セキュリティ機能の設計・実装	セキュリティ要件及びアーキテクチャに基づくセキュリティ機能の設計・実装について，必要な指導・助言を行い，支援する。	・セキュリティ機能（認証，アクセス制御，暗号化，ログの取得，セッション管理など）に関する知識 ・ソフトウェア，ハードウェアに関する知識 ・ITセキュリティ関連の規格（CC/CEM，FIPS 140など）に関する知識 ・ITセキュリティ関連の認証制度（JISEC，JCMVPなど）に関する知識 ・耐タンパ性，サイドチャネル攻撃に関する知識	・セキュリティ機能の設計書，テスト計画書をセキュリティの観点からレビューする能力 ・セキュリティ機能の実装方式を設計する能力

大項目	小項目	概　要	要求される知識	要求される技能
	2-5　セキュアプログラミング	ソフトウェア実装でのコーディング標準，セキュアプログラミングなどについて，必要な指導・助言を行い，支援する。	・セキュアプログラミングの原則，実践規範に関する知識 ・OS 及びコンパイラでの攻撃防止技術に関する知識 ・統合開発環境に関する知識 ・プログラム言語，データベース言語，マークアップ言語に関する知識	・ソフトウェア実装について，セキュアプログラミングの原則，実践規範と照らしてレビューする能力 ・コーディング標準に沿ったセキュアプログラミングを実践する能力
	2-6　セキュリティテスト	実装したセキュリティ機能のテスト，並びにソフトウェア及びシステムのテストについて，セキュリティの観点から必要な指導・助言を行い，支援する。 運用フェーズのソフトウェア及びシステムを対象に行う脆弱性診断について，必要な指導・助言を行い，支援する。	・ソフトウェア及びシステムの，セキュリティの観点でのテスト（ソースコード静的検査，プログラム動的検査，ファジングなど）の実施方法に関する知識 ・脆弱性診断，ペネトレーションテストの実施方法に関する知識 ・脆弱性検査ツール（Webアプリケーションソフトウェア検査用，ネットワーク検査用など）に関する知識	・テスト対象に応じて，必要なテストの種類及びその実施方法を計画する能力 ・実施するテストの種類に適したツールを選択する能力 ・手動テストとツールによる自動テストを組み合わせ，効果的かつ効率的なテストを計画する能力 ・テストで検出したエラーを識別し，修正，解消する能力
	2-7　運用・保守（セキュリティの観点）	システムの運用・保守について，セキュリティの観点から必要な指導・助言を行い，支援する。 運用・保守の関連文書のレビュー，システム運用担当者に対する教育・訓練の実施について，セキュリティの観点から必要な指導・助言を行い，支援する。	・サービスマネジメント，ITSMS，SLAに関する知識 ・サービスデスクに関する知識 ・システム及びネットワークの監視手順，情報セキュリティインシデントが発生した場合の運用手順に関する知識	・運用・保守の関連文書（作業計画書，作業手順書，利用者向けのマニュアルなど）を，セキュリティの観点からレビューする能力 ・運用担当者の能力水準の目標に合わせて教育・訓練の目標を設定する能力
	2-8　開発環境のセキュリティ確保	開発環境のセキュリティを確保するために必要な対策について，必要な指導・助言を行い，支援する。 リポジトリの管理及びそのバージョン管理について，セキュリティの観点から必要な指導・助言を行い，支援する。 開発業務を外部に委託する場合の契約に記載する要求事項，委託先からの成果物の確認について，セキュリティの観点から必要な指導・助言を行い，支援する。	・ソフトウェア開発管理技術（開発プロセス，開発環境管理，構成管理，変更管理など）に関する知識 ・開発プロジェクトのマネジメントに関する知識 ・ソフトウェアの仕様書，ソースコード，テストデータなどを含むリポジトリの管理及びそのバージョン管理のためのツールに関する知識	・開発対象のソフトウェアの仕様書，ソースコード，テストデータなどのセキュアな管理方法をレビューする能力 ・開発業務を外部に委託する場合のリスクを認識し，必要な対策を設計する能力

大項目	小項目	概　要	要求される知識	要求される技能
3　情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-1　暗号利用及び鍵管理	暗号の利用，鍵管理の設計及び暗号関連諸規程の策定及び改定について，必要な指導・助言を行い，支援する。	・暗号アルゴリズム，暗号利用モードに関する知識 ・公開鍵基盤（PKI）に関する知識 ・デジタル署名に関する知識 ・セキュアプロトコル，認証プロトコルに関する知識 ・暗号を利用する場合のリスクに関する知識 ・暗号解読方法に関する知識 ・暗号の安全性などの評価（CRYPTREC暗号リスト）に関する知識 ・ハードウェアセキュリティモジュール（HSM），TPMに関する知識	・暗号を利用すべき情報・機能を特定する能力 ・適切な暗号技術を選択する能力 ・鍵管理の仕組みを設計する能力
	3-2　マルウェア対策	情報及び情報システムをマルウェアから保護するためのマルウェア対策ソフト及び他のセキュリティソリューションの導入，運用（マルウェア定義ファイルの更新を含む），並びにマルウェア感染を防止するための諸規程の策定及び改定について，必要な指導・助言を行い，支援する。 マルウェア感染の疑いがある事象の報告手順，初動対応手順の設計について，必要な指導・助言を行い，支援する。	・マルウェアの種類と特徴（ボット，ランサムウェア，ファイルレスマルウェアなど）に関する知識 ・マルウェア感染の経路・方法（標的型攻撃など）に関する知識 ・既知及び未知のマルウェアを検知，隔離又は無害化する技術 ・マルウェアによる攻撃（C&C通信，ファイル暗号化など）に対する多層防御に関する知識 ・検疫ネットワーク，サンドボックスに関する知識	・マルウェア感染のリスクを分析する能力 ・情報システム，ネットワーク構成及びその利用方法に応じたマルウェア対策を設計する能力 ・マルウェア対策ソフトを効果的に適用し，マルウェアからの保護の有効性を高める能力 ・マルウェア感染の初動対応手順を設計する能力
	3-3　バックアップ	データのバックアップ及び復旧の計画の策定及び改定，並びに手順の設計について，必要な指導・助言を行い，支援する。 データのバックアップのテスト，データの復旧のテストについて，必要な指導・助言を行い，支援する。 システムの冗長化，バックアップシステムの確保について，必要な指導・助言を行い，支援する。	・データのバックアップの方式及び頻度に関する知識 ・遠隔地保管に関する知識 ・データの復旧に関する知識	・データのバックアップの範囲，頻度，保管期間，保管場所などを，組織内の業務上の要求事項，事業継続に対しての重要度，目標復旧時間などを考慮して設計する能力 ・バックアップ媒体の適切な保管方法を設計する能力 ・データの復旧方法を設計する能力

大項目	小項目	概　要	要求される知識	要求される技能
	3-4　セキュリティ監視並びにログの取得及び分析	情報セキュリティインシデントの検知と調査を可能にするためのログの取得，保管，定期的なレビューについて，必要な指導・助言を行い，支援する。 ログに時刻を正確に記録するための機器の時刻同期について，必要な指導・助言を行い，支援する。 ネットワーク機器，IPS/IDS，Web サーバ，プロキシサーバ，DNS，DHCP のログなどの多種多様なログの効果的な保管，監視及び分析について，必要な指導・助言を行い，支援する。	・セキュリティ監視（制御システム，IoT機器の監視を含む），SOCに関する知識 ・ログ（OSのログ，ネットワーク機器のログ，サービスのログなど）に関する知識 ・ログの取得，保管に関する知識 ・ログの分析方法（相関分析など）に関する知識 ・脅威インテリジェンスの共有のための標準（STIX/TAXIIなど）に関する知識 ・SIEMに関する知識 ・時刻同期プロトコル（NTP）に関する知識	・セキュリティ監視方法を設計する能力 ・取得すべきログを設計する能力 ・ログの分析方法を設計する能力 ・ログの保護について設計する能力 ・セキュリティ監視及びログ分析における脅威インテリジェンスの利用を設計する能力 ・ログのモニタリング及びレビューにおいて情報セキュリティインシデントの疑いがある事象を検知した場合の対応を設計する能力
	3-5　ネットワーク及び機器のセキュリティ管理	ネットワーク及び通信（電子メールの送受信など）におけるセキュリティの確保について，必要な指導・助言を行い，支援する。 ネットワークの管理手順及び利用手順並びに通信データの保護方法のレビューについて，必要な指導・助言を行い，支援する。 利用者エンドポイント機器利用及びリモートワークにおけるセキュリティ対策について，必要な指導・助言を行い，支援する。	・ネットワーク通信プロトコル（DNS，ICMP，ARP，DHCP，HTTP，SMTPなど）に関する知識 ・Webアクセスのセキュリティに関する知識 ・電子メールのセキュリティに関する知識 ・DNSのセキュリティに関する知識 ・無線LANのセキュリティに関する知識 ・ネットワークセキュリティ技術（ファイアウォール，IPS/IDS，WAFなど）に関する知識 ・利用者エンドポイント機器利用及びリモートワークのセキュリティ（物理的保護，遠隔でのデータ消去・ロック，VDIなど）に関する知識	・ネットワークの物理的又は論理的な分割を設計する能力 ・利用するネットワークサービスのセキュリティ（認証，暗号化，ネットワーク接続管理など），サービスレベルなどの妥当性を確認する能力
	3-6　脆弱性への対応	情報システム及びコンポーネントの構成管理，脆弱性情報収集及び脆弱性対応について，必要な指導・助言を行い，支援する。 脆弱性修正プログラムの適用基準の設計，利用者によるソフトウェアのインストールを管理するための諸規程の策定及び改定並びに利用者への周知について，必要な指導・助言を行い，支援する。	・脆弱性情報の入手（脆弱性診断結果，外部からの情報収集など）に関する知識 ・脆弱性情報（JVN，CVE，CVSS，CWEなど）に関する知識 ・セキュリティ設定共通化手順（SCAP）に関する知識 ・脆弱性ハンドリングに関する知識 ・バグバウンティプログラムに関する知識	・効果的な構成管理，脆弱性情報収集を設計する能力 ・脆弱性修正プログラムの適用の要否，優先度を評価する能力 ・必要な回帰テストなどを計画する能力

大項目	小項目	概　要	要求される知識	要求される技能
	3-7　物理的セキュリティ管理	物理的及び環境的脅威への対策について，必要な指導・助言を行い，支援する。	・物理的及び環境的脅威（故障，サポートユーティリティの不具合，破壊，盗難，物理的不正アクセス，電力供給の妨害，通信妨害，電磁波放射，自然災害，火災，水，塵埃，振動など）に関する知識 ・入退管理に関する知識 ・装置，情報又はソフトウェアの持込み・持出しの管理及び物理的保護に関する知識 ・物理的な侵入に対する警報，監視装置（監視カメラなど）に関する知識	・物理的セキュリティ境界を定義し，オフィス，部屋及び施設に対する物理的セキュリティを設計する能力 ・記憶媒体の廃棄・再利用，無人状態にある機器の保護，紙の書類の管理，複合機の利用などの情報セキュリティを設計する能力
	3-8　アカウント管理及びアクセス管理	情報及び情報システム並びにネットワークサービスのアクセス制御方針のレビューについて，必要な指導・助言を行い，支援する。 アカウント管理，認証情報の割当て及び管理並びにアクセス管理に関するプロセスの確立，特権的アクセス権の割当て及び利用の制限と管理について，必要な指導・助言を行い，支援する。 アカウント及びアクセス権のレビューについて，必要な指導・助言を行い，支援する。	・アクセス制御の種類と特徴（ロールベースアクセス制御など）に関する知識 ・need-to-know，need-to-use，最小権限の原則に関する知識 ・認証情報の割当て及び管理に関する知識 ・アカウント及びアクセス権のレビューが必要になるタイミング（利用者の異動，業務担当者の変更，雇用又は契約の終了など）に関する知識	・アクセス制御方針，アカウント及びアクセス権をレビューする能力 ・責任追跡性を確保するための，特権的アクセスのログの記録，保護及びレビューの手順を設計する能力 ・情報システムの重要性に応じた認証情報の割当て及び管理を設計する能力
	3-9　人的管理	従業員の雇用前，雇用期間中，雇用の終了・変更の対応について，セキュリティの観点から必要な指導・助言を行い，支援する。 セキュリティ教育・訓練の計画・実施について，必要な指導・助言を行い，支援する。 情報セキュリティ諸規程の順守状況に関する自己点検の計画・実施について，必要な指導・助言を行い，支援する。 情報セキュリティ違反に対する懲戒手続の策定及び改定について，必要な指導・助言を行い，支援する。	・内部不正及びそのメカニズムに関する知識 ・内部不正防止に関する知識 ・職務規程，雇用契約，守秘義務協定に関する知識 ・セキュリティクリアランスに関する知識 ・セキュリティ教育・訓練の方法に関する知識 ・自己点検に関する知識	・内部不正防止を設計する能力 ・人的管理に関する諸規程をセキュリティの観点からレビューする能力 ・効果的なセキュリティ教育・訓練を計画する能力
	3-10 サプライチ	ビジネスパートナー・委託先との契約への	・サプライチェーンに関する知識	・契約に盛り込むべきリスク低減のための

大項目	小項目	概　要	要求される知識	要求される技能
	ェーンの情報セキュリティの推進	セキュリティ関連の要求事項の追加，及びビジネスパートナー・委託先での要求事項への対応状況の評価について，必要な指導・助言を行い，支援する。	・委託での情報セキュリティリスクに関する知識 ・製品・サービスのサプライチェーンのリスクに関する知識 ・取引関連法規，企業間の契約に関する知識	要求事項を設計する能力 ・ビジネスパートナー・委託先での要求事項への対応状況を評価する能力
	3-11 コンプライアンス管理	情報セキュリティ及び個人情報保護に関連する法令，規制並びに契約上の義務を考慮した組織内の情報セキュリティ諸規程の策定及び改定について，必要な指導・助言を行い，支援する。 また，法令，規制，契約に関する従業員向け意識向上プログラムの利用について，必要な指導・助言を行い，支援する。	・法令（刑法，不正アクセス禁止法，個人情報保護法，マイナンバー法，不正競争防止法など）及び公的なガイドラインに関する知識 ・契約，倫理，公益通報者保護制度に関する知識 ・意識向上プログラムに関する知識	・法令，規制などを考慮して，情報セキュリティ諸規程を策定し，改定する能力 ・契約上の義務を確実に遂行する方法を設計する能力 ・コンプライアンス管理の重要性を関係者に伝達する手段を設計する能力
4 情報セキュリティインシデント管理の推進又は支援に関すること	4-1 情報セキュリティインシデントの管理体制の構築	組織内 CSIRT の構築について，必要な指導・助言を行い，支援する。 情報セキュリティインシデントの管理に関する規程の策定及び改定について，必要な指導・助言を行い，支援する。	・CSIRTの構築（体制の構築，規程の整備，メンバの訓練など）に関する知識 ・CSIRT活動の設備（執務スペース，通信設備，データの管理・廃棄のための設備，インシデントトラッキングシステムなど）に関する知識 ・PSIRTに関する知識	・情報セキュリティインシデントの管理に関する規程を検討する能力 ・情報セキュリティ事象を情報セキュリティインシデントとするかの判断基準，及び対応の優先順位の判断基準を設計する能力
	4-2 情報セキュリティ事象の評価	情報セキュリティ事象の検知時又は連絡受付時の初動対応について，必要な指導・助言を行い，支援する。 事実関係（いつ，どこで，何が，どのように，など）の確認について，必要な指導・助言を行い，支援する。 事象を情報セキュリティインシデントとするかの判断，及び対応の優先順位の判断について，必要な指導・助言を行い，支援する。	・情報セキュリティ事象及び情報セキュリティインシデントに関する知識 ・トリアージに関する知識	・初動対応を設計する能力 ・事実関係を確認し，整理する能力 ・情報セキュリティインシデントの連絡・報告のフローを設計する能力 ・判明している事象，事実から，情報セキュリティインシデントの原因，被害を客観的に分析し，対応を検討する能力
	4-3 情報セキュ	情報セキュリティインシデントによる被	・被害・損失の評価に関する知識	・根本原因を特定し，再発防止を設計する

大項目	小項目	概　要	要求される知識	要求される技能
	リティインシデントへの対応	害・損失の評価，情報セキュリティインシデントの根本原因の特定，復旧・回復策の実施，再発防止，対応改善などについて，必要な指導・助言を行い，支援する。 顧客，監督官庁及び関係者への報告，報道機関への公表及び一般に向けた情報公開について，必要な指導・助言を行い，支援する。 マルウェア検知時のマルウェア解析について，必要な指導・助言を行い，支援する。	・システム，ネットワーク，ソフトウェアの調査方法に関する知識 ・監督官庁などへの報告，報道機関などへの公表に関する知識 再発防止に関する知識 ・マルウェア解析の手順，マルウェアが解析を回避する仕組み，マルウェア検体の安全な取扱いに関する知識	能力 ・外部の組織と連携して対応する能力 ・インシデント対応を評価し，対応手順を改善する能力 ・再発防止及び対応改善のための教訓を教育・訓練に反映する能力 ・マルウェア解析を支援する能力
	4-4　証拠の収集及び分析	証拠保全の手順及びツールについて，必要な指導・助言を行い，支援する。 専門性を必要とする状況における，デジタルフォレンジックスの専門家，法的措置の専門家などへの依頼について，必要な指導・助言を行い，支援する。	・証拠保全すべき対象に関する知識 ・証拠保全の手順及びツールに関する知識 ・Chain of Custody（証拠保全の一貫性）に関する知識 ・法的措置（弁護士又は警察への相談など）に関する知識	・証拠保全の対象（デスクトップPC，ノートPC，サーバ，記憶媒体），電源の状態などに応じた証拠保全方法を設計する能力 ・証拠を分析する能力

■情報処理安全確保支援士試験（レベル 4）
シラバス（Ver.2.1）

独立行政法人情報処理推進機構
〒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：https://www.ipa.go.jp/shiken/

2023.12