情報処理安全確保支援士試験
シラバス（案）

－ 情報処理安全確保支援士試験における出題範囲の細目 －

Ver.0.1

- 本資料の内容は公表時点の検討状況に基づくものであり，変更する可能性があります。

Beyond Digital
独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

■ はじめに

本シラバスは，情報処理安全確保支援士試験の出題範囲 [1] を詳細化し，目標とする知識，技能の幅と深さを明確化したものです。

知識及び技能の習得を目指して試験を受験する方々にとっての学習指針として，また，組織（企業，学校など）における人材育成及び教育の指導指針として活用されることを想定しています。

なお，本シラバスは，ビジネス環境の変化，デジタル技術の動向などを踏まえて，内容の追加，変更，削除などの見直しを適宜行います。

■ シラバスの構成

本シラバスは，前半部に「目標とする知識」を，後半部に「目標とする技能」を記しています。

「目標とする知識」では，全試験区分共通の体系である〔科目 A の出題範囲〕の分類ごとに，科目 A-2 の主な用語例を示しています。専門知識において，中分類の記載順は「大分類 6：セキュリティ」を先に記しています。

「目標とする技能」では，各試験区分の〔科目 B の出題範囲〕の項目ごとに，具体的な内容を示しています。

なお，科目 A-1 の用語例については，「プロフェッショナルデジタルスキル試験（仮称）及び情報処理安全確保支援士試験 共通知識　シラバス（案)」で示します。

1．本シラバスにおいて示す内容

【目標とする知識（専門知識)】※科目 A-2 の出題範囲の細目。

大分類〇：XXXXXXXXXX　中分類〇：XXXXXXXXXX		
【内容】 ・XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
小分類	項目	用語例

【目標とする知識（その他の知識)】※科目 A-2 の出題範囲の細目。

大分類〇：XXXXXXXXXX		
【内容】 ・XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
小分類	項目	用語例

【目標とする技能】※科目 B の出題範囲の細目。

大項目	小項目	概要	目標とする技能の例

2．「プロフェッショナルデジタルスキル試験（仮称）及び情報処理安全確保支援士試験 共通知識　シラバス（案)」において示す内容

【目標とする知識（共通知識)】※科目 A-1 の出題範囲の細目。

大分類〇：XXXXXXXXXX		
【内容】 ・XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
小分類	項目	用語例

注 [1]「情報処理技術者試験・情報処理安全確保支援士試験 出題範囲等の改定案
https://www.ipa.go.jp/shiken/syllabus/henkou/2025/rcu1hd0000008574-att/shinshiken-hani-kaiteian.pdf

【目標とする知識（専門知識）】

大分類 6：セキュリティ　中分類 23：情報セキュリティの脅威			
【内容】 ・組織の事業，業務及び情報システムを取り巻く様々なリスクの動向を把握し，管理面と技術面における適切なセキュリティ対策を検討するために必要な，情報セキュリティの脅威，脆弱性及び攻撃手法に関する専門的な知識を問う。			
小分類		項目	用語例
1	脅威と脆弱性	脅威の種類と動向	事故，災害，破壊，盗難，侵入，不正アクセス，盗聴，なりすまし，改ざん，ビジネスメール詐欺（BEC），アクセス権の誤設定，ソーシャルエンジニアリング，情報漏えい，踏み台，攻撃ベクトル，攻撃対象領域（アタックサーフェス），脅威モデリング（STRIDE　など），脅威シナリオ，情報セキュリティ 10 大脅威
		マルウェア・不正プログラム	遠隔操作型ウイルス（RAT），リバースシェル，ランサムウェア，ステルス技術（ポリモーフィック型，メタモーフィック型　など），ファイルレスマルウェア，エクスプロイトコード
		脆弱性	セキュリティホール，人的脆弱性，内部統制の不備，シャドーIT，認可・権限・アクセス制御の不備，不適切な入力確認，パスワードのハードコード，認証バイパス，重要情報の平文での保存・送信，レースコンディション，OWASP Top 10，OWASP Top 10 for LLM Applications，OWASP API Security Top 10
		不正の動機・メカニズム	ダークウェブ，ハクティビズム，不正のトライアングル，RaaS（Ransomware as a Service），イニシャルアクセスブローカー，二重恐喝（多重恐喝）
2	攻撃手法	攻撃のライフサイクルとフレームワーク	サイバーキルチェーン，MITRE ATT&CK（戦術，技術，手順（TTP）），偵察（フットプリンティング，ポートスキャン　など），初期侵入，権限昇格，永続化，ラテラルムーブメント，C2（Command and Control），持ち出し（Exfiltration）
		資格情報･セッション管理の不備を狙った攻撃	ブルートフォース攻撃，リバースブルートフォース攻撃，レインボーテーブル攻撃，クレデンシャルスタッフィング，MFA 疲労攻撃（Multi-Factor Authentication Fatigue Attack，プッシュ通知爆撃（Push Bombing）），セッションハイジャック，セッション固定化攻撃（Session Fixation），リプレイ攻撃
		アプリケーションの不備を狙った攻撃	SQL インジェクション，HTTP ヘッダインジェクション，OS コマンドインジェクション，クロスサイトスクリプティング（反射型，格納型，DOM 型（DOM-based）），クロスサイトリクエストフォージ

			エリ（CSRF），ディレクトリトラバーサル，バッファオーバーフロー，オープンリダイレクトの悪用，クリックジャッキング，ドライブバイダウンロード
		信頼を悪用した攻撃	第三者中継（オープンリレー），IP スプーフィング，DNS キャッシュポイズニング，フィッシング（スミッシング　など），標的型攻撃，SEO ポイズニング
		サービスの妨害を狙った攻撃	DDoS 攻撃（マルチベクトル型　など），リフレクション攻撃（DNS アンプ攻撃　など）
		AI を悪用した攻撃	AI による攻撃の高度化（マルウェア亜種の自動生成，フィッシング文面の巧妙化，脆弱性発見の効率化，偵察の自動化），ディープフェイク・音声クローンによるなりすまし
		AI システムに対する攻撃	プロンプトインジェクション（直接，間接），ジェイルブレイク，敵対的サンプル（Adversarial Examples），データポイズニング，モデルインバージョン攻撃，メンバーシップ推測攻撃，モデル窃取（Model Extraction），システムプロンプトの窃取
		サプライチェーンを狙った攻撃	ソフトウェアサプライチェーン攻撃（アップデート配信経路の悪用　など），ビルド環境・CI/CD パイプラインの侵害，依存関係混同（Dependency Confusion），タイポスクワッティング，OSS メンテナアカウントの乗っ取り
		その他・特殊・高度な攻撃	サイドチャネル攻撃（タイミング攻撃，電力解析攻撃　など），エアギャップに対する攻撃，サービス及びソフトウェアの機能の悪用（オープンリゾルバの悪用　など），ダウングレード攻撃（バージョンロールバック攻撃）

大分類 6：セキュリティ　中分類 24：情報セキュリティマネジメント

【内容】

・事業活動における情報資産の機密性，完全性，可用性を維持する観点から情報セキュリティリスクをアセスメントし，その対応として管理策を適用するために必要な，情報セキュリティマネジメントに関する専門的な知識を問う。

・国内外の規格，基準，ガイドライン，ベストプラクティスなどを踏まえて組織的に情報セキュリティを確保するために必要な，情報セキュリティ関連組織及び関連制度に関する専門的な知識を問う。

・組織の情報セキュリティ方針及び情報セキュリティ目的を明確にし，要求事項に適合する情報セキュリティマネジメントシステムを確立し，実施し，維持し，継続的に改善するために必要な，情報セキュリティマネジメントシステムに関する専門的な知識を問う。

小分類		項目	用語例
1	情報セキュリティの考え方	情報セキュリティの考え方	機密性，完全性，可用性，真正性，責任追跡性，否認防止，信頼性，多層防御（Defense in Depth），セキュリティ・バイ・デザイン，セキュア・バイ・デフォルト，最小権限の原則，フェイルセーフ／フェイルセキュア，攻撃対象領域の最小化

		情報セキュリティマネジメントの考え方	リスクマネジメント（JIS Q 31000），情報セキュリティ事象，情報セキュリティインシデント，利用者アクセス権の管理（need-to-know の原則　など），クラウドサービスの責任共有モデル，外部委託やクラウドサービスの利用時における情報セキュリティ
2	リスクマネジメント	情報資産とリスク	情報資産台帳，情報資産を取り巻く脅威，リスクの種類（オペレーショナルリスク，サプライチェーンリスク，外部サービス利用のリスク，SNS による情報発信のリスク，地政学的リスク　など），年間予想損失額（ALE），単一損失予想額（SLE），年間発生率（ARO），リスク分析のアプローチ（ベースラインアプローチ，非形式的アプローチ，詳細リスク分析，組合せアプローチ），ISO/IEC 27005
		情報セキュリティリスクアセスメント	リスク基準（リスク受容基準，情報セキュリティリスクアセスメントを実施するための基準），リスクレベル，リスクマトリックス，リスク所有者，リスク源，リスクアセスメントのプロセス（リスク特定，リスク分析，リスク評価），リスク態度（リスク選好，リスク回避的態度），リスクの定性的分析，リスクの定量的分析
		情報セキュリティリスク対応	リスクコントロール，リスク対応計画，リスク登録簿，リスクコミュニケーション，リスク対応の選択肢（リスク回避，リスク低減（軽減），リスク移転（共有），リスク保有（受容）），残留リスク，リスク受容の承認
3	情報セキュリティ諸規程	情報セキュリティポリシーを含む組織内規程	情報セキュリティ方針（情報セキュリティポリシー），情報セキュリティインシデント対応規程，マルウェア感染時の対応，プライバシーポリシー（個人情報保護方針）
4	情報セキュリティ関連組織・関連制度	情報セキュリティに関する組織・機関	〔組織内の体制・窓口〕 情報セキュリティ委員会，情報セキュリティ関連組織（CSIRT，PSIRT，SOC（Security Operation Center）），組織への設置が推奨されている窓口（abuse@ドメイン名，noc@ドメイン名，security@ドメイン名） 〔国のサイバーセキュリティ推進体制〕 サイバーセキュリティ戦略本部，国家サイバー統括室（NCO） 〔調整・情報共有を担う機関〕 JPCERT コーディネーションセンター，FIRST(Forum of Incident Response and Security Teams)，セキュリティ情報共有組織（ISAC） 〔標準化・技術評価を担う機関〕 CRYPTREC，米国国立標準技術研究所（NIST），MITRE

		情報セキュリティに関する制度・基準	〔脆弱性・インシデントの届出及び公表〕 コンピュータ不正アクセス届出制度，コンピュータウイルス届出制度，情報セキュリティ早期警戒パートナーシップガイドライン，ソフトウェア製品開発者の脆弱性開示（ISO/IEC 29147），脆弱性情報取扱手順（ISO/IEC 30111），サイバー攻撃被害に係る情報の共有・公表ガイダンス 〔評価・登録の制度〕 情報セキュリティサービス基準，サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度），ISMAP（政府情報システムのためのセキュリティ評価制度） 〔対策の指針となる基準・フレームワーク〕 政府機関等のサイバーセキュリティ対策のための統一基準群，サイバーセキュリティ経営ガイドライン，中小企業の情報セキュリティ対策ガイドライン，NIST サイバーセキュリティフレームワーク，NIST SP 800 シリーズ（SP 800-53，SP 800-61，SP 800-171，SP 800-207　など） 〔分野別の規格・指針〕 JIS Q 27701（ISO/IEC 27701），ISO/IEC 42001（AI マネジメントシステム），AI 事業者ガイドライン，つながる世界の開発指針，IoT 開発におけるセキュリティ設計の手引き
5	情報セキュリティマネジメントシステム	情報セキュリティマネジメントシステム	ISMS 適用範囲，情報セキュリティ管理策，管理策タイプ（予防，検知，是正），ISMS 適合性評価制度，ISMS 認証，JIS Q 27001（ISO/IEC 27001），JIS Q 27002（ISO/IEC 27002），情報セキュリティガバナンス（JIS Q 27014（ISO/IEC 27014）），JIS Q 27017（ISO/IEC 27017）
6	情報セキュリティ管理策	組織的管理策	〔組織的管理〕 情報セキュリティのための方針群，情報セキュリティの役割及び責任，職務の分離，管理層の責任，関係当局との連絡，専門組織との連絡，脅威インテリジェンス，プロジェクトマネジメントにおける情報セキュリティ 〔資産管理〕 情報及びその他の関連資産の目録，情報及びその他の関連資産の許容される利用，資産の返却，情報の分類，情報のラベル付け，情報の転送 〔アクセス権管理〕 アクセス制御，識別情報の管理，認証情報，アクセス権 〔供給者管理〕 供給者関係における情報セキュリティ，供給者との合意における情報セキュリティの取扱い，

			ICT サプライチェーンにおける情報セキュリティの管理，供給者のサービス提供の監視・レビュー・変更管理，クラウドサービスの利用における情報セキュリティ 〔インシデント管理・事業継続〕 情報セキュリティインシデント管理の計画策定及び準備，情報セキュリティ事象の評価及び決定，情報セキュリティインシデントへの対応，情報セキュリティインシデントからの学習，証拠の収集，事業の中断・阻害時の情報セキュリティ，事業継続のための ICT の備え 〔コンプライアンス管理〕 法令・規制・契約上の要求事項，知的財産権，記録の保護，プライバシー及び PII の保護，情報セキュリティの独立したレビュー，情報セキュリティのための方針群・規則・標準の順守，操作手順書
		人的管理策	〔人的管理〕 選考，雇用条件，情報セキュリティの意識向上・教育・訓練，懲戒手続，雇用の終了又は変更後の責任，秘密保持契約又は守秘義務契約，リモートワーク，情報セキュリティ事象の報告
		物理的管理策	〔物理的領域の管理〕 物理的セキュリティ境界，物理的入退，オフィス・部屋・施設のセキュリティ，物理的セキュリティの監視，物理的及び環境的脅威からの保護，セキュリティを保つべき領域での作業，クリアデスク・クリアスクリーン 〔装置の管理〕 装置の設置及び保護，構外にある資産のセキュリティ，記憶媒体，サポートユーティリティ，ケーブル配線のセキュリティ，装置の保守，装置のセキュリティを保った処分又は再利用
		技術的管理策	〔情報アクセスの管理〕 利用者エンドポイント機器，特権的アクセス権，情報へのアクセス制限，ソースコードへのアクセス，セキュリティを保った認証 〔情報資産運用に関する管理〕 容量・能力の管理，マルウェアに対する保護，技術的脆弱性の管理，構成管理，情報の削除，データマスキング，データ漏えい防止，情報のバックアップ，情報処理施設・設備の冗長性，ログ取得，監視活動，クロックの同期，特権的なユーティリティプログラムの使用，運用システムへのソフトウェアの導入

			〔情報システムの適正利用の管理〕 ネットワークセキュリティ，ネットワークサービスのセキュリティ，ネットワークの分離，ウェブフィルタリング，暗号の利用 〔情報システム開発・導入の管理〕 セキュリティに配慮した開発のライフサイクル，アプリケーションセキュリティの要求事項，セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則，セキュリティに配慮したコーディング，開発及び受入れにおけるセキュリティテスト，外部委託による開発，開発環境・テスト環境・本番環境の分離，変更管理，テスト用情報，監査におけるテスト中の情報システムの保護

大分類 6：セキュリティ　中分類 25：情報セキュリティ対策

【内容】

・情報資産及び情報システムを様々な脅威から保護する上で幅広くセキュリティ対策を検討して，それらの必要性及び期待効果を関係者に説明し，適切な情報セキュリティ対策の適用・維持を推進するために必要な，情報セキュリティ対策に関する専門的な知識を問う。

小分類		項目	用語例
1	組織的管理策に関する技術・手法	脅威インテリジェンス	OSINT（公開情報）の利用，IoC（Indicator of Compromise），脅威情報構造化記述形式（STIX），検知指標情報自動交換手順（TAXII），TLP（Traffic Light Protocol），脅威ハンティング（Threat Hunting），テイクダウン
		インシデント管理	インシデントハンドリング，インシデント対応プロセス（準備，検知・分析，封じ込め・根絶・復旧，事後対応），トリアージ，インシデントレスポンス計画（IRP），CSIRT の構築・運用（CSIRT マテリアル），法令に基づく報告及び本人への通知，関係機関への届出，公表の判断及び広報対応，サイバー保険，事後レビュー
		事業継続とレジリエンス	バックアップからの復旧手順の検証，復旧目標（RTO，RPO）に基づく復旧設計，代替サイト（ホットサイト，コールドサイト）
2	人的管理策に関する技術・手法	人的管理	組織における内部不正防止ガイドライン，情報セキュリティ訓練（標的型メールに関する訓練，レッドチーム演習，机上演習　など），UEBA（User and Entity Behavior Analytics），セキュリティクリアランス，秘密保持契約・誓約書
3	物理的管理策に関する技術・手法	物理的領域の管理	セキュリティゾーニング，入退管理システム，アンチパスバック

		装置の管理	モバイル機器（ノート PC，スマートフォン，タブレット端末　など）のセキュリティ，MDM（Mobile Device Management），サポートユーティリティ（電源，空調，給水　など）の保守
4	技術的管理策に関する技術・手法（情報アクセスの管理）	情報へのアクセス制限	強制アクセス制御（MAC），任意アクセス制御（DAC），ロールベースアクセス制御（RBAC），属性ベースアクセス制御（ABAC），最小特権，特権アクセス管理（PAM），セキュア OS，ストレージ暗号化，ファイル暗号化，データベース暗号化
		認証・署名	デジタル署名，メッセージ認証符号（MAC），HMAC，コードサイニング，エンティティ認証，DNSSEC
		利用者の認証・認可・ID 連携	多要素認証，多段階認証，リスクベース認証，フィッシング耐性のある認証，Kerberos 方式，LDAP サーバでの認証，アイデンティティ連携（OpenID Connect，SAML，OAuth 2.0，IdP（Identity Provider)），PKCE，アクセストークン，リフレッシュトークン，JWT（JSON Web Token），シングルサインオン（SSO），IDaaS（Identity as a Service）
		生体認証	身体的特徴，行動的特徴，本人拒否率（FRR），他人受入率（FAR），等価誤り率（EER），ライブネス検知（アクティブ検知，パッシブ検知）
		パスワードレス認証	FIDO（FIDO2，WebAuthn，CTAP，パスキー），ワンタイムコード
5	技術的管理策に関する技術・手法（情報資産運用に関する管理）	マルウェアに対する保護	〔マルウェア・不正プログラム対策〕 ビヘイビア法（振る舞い検知），ヒューリスティック法，未知マルウェア検出手法，動的解析，静的解析 〔ランサムウェア対策〕 バックアップ分離，3-2-1 ルール，WORM（Write Once Read Many）機能，イミュータブルバックアップ，カナリアファイル，暗号化挙動検知
		脆弱性管理・データ保護	脆弱性情報の収集と適用判断，パッチ管理，資産インベントリの継続的把握，ASM／EASM（外部攻撃対象領域管理），DLP（Data Loss Prevention），Web 分離（Web アイソレーション），情報の削除及びデータマスキングの実装
		ログ管理・監視・検知及び対応	〔ログの管理〕 ログ設計（取得範囲，保存期間，改ざん防止（WORM，追記のみ），時刻同期（NTP）とタイムスタンプ），ログの相関分析 〔検知の方式と精度〕 シグネチャ型，アノマリ型，偽陽性（フォールスポジティブ），偽陰性（フォールスネガティブ） 〔検知・対応の基盤及び製品〕

			SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), NDR(Network Detection and Response),XDR(Extended Detection and Response),SOAR(Security Orchestration, Automation and Response) 〔運用体制及び外部サービスの活用〕 SOC の運用(アラートトリアージ,誤検知の低減),MSS(Managed Security Service),MDR(Managed Detection and Response)
6	技術的管理策に関する技術・手法（情報システムの適正利用の管理）	ネットワークセキュリティの方式・制御	〔防御の考え方〕 境界防御，ゼロトラストの実装技術（マイクロセグメンテーション，ZTNA，継続的な検証） 〔境界における通信の制御〕 ファイアウォール（パケットフィルタリング型，ステートフルインスペクション型，アプリケーションゲートウェイ型），IDS／IPS（NIDS，HIDS），VPN（リバースプロキシ方式，ポートフォワーディング方式，L2 フォワーディング方式） 〔内部ネットワークへの接続の制御〕 検疫ネットワーク,端末健全性検証によるネットワークアクセス制御(NAC,TNC(Trusted Network Connect))，MAC アドレスフィルタリング，DHCP スヌーピング 〔公開サービスの保護〕 リバースプロキシ，DDoS 対策（CDN，スクラビングセンター，Anycast，レート制限），Bot 対策（CAPTCHA，レート制限） 〔監視及び検査〕 ネットワークトラフィック分析，ネットワーク脆弱性検査，ポートスキャンによる検査
		ネットワークセキュリティの技術規格・プロトコル	〔通信の暗号化〕 TLS（TLS 1.2，TLS 1.3，暗号スイート，SSL 及び TLS 1.0／1.1 の廃止），STARTTLS，SMTP over TLS，IPsec（ESP，AH，IKE），QUIC，DoH，DoT 〔認証基盤〕 IEEE 802.1X，RADIUS，EAP（Extensible Authentication Protocol），EAP-TLS 〔無線 LAN セキュリティ〕 PSK（Pre-Shared Key），WPA3（Personal，Enterprise，Enhanced Open） 〔電子メールセキュリティ〕

			SMTP-AUTH, OP25B, 送信ドメイン認証 (SPF, DKIM, DMARC (ポリシー (none, quarantine, reject), 集約レポート)), S/MIME (Secure MIME), 添付ファイルの無害化 (サニタイズ)
		ネットワークセキュリティの製品・サービス	〔境界防御・アプリケーション保護〕 統合脅威管理 (UTM), WAF (Web Application Firewall) 〔クラウド・SaaS〕 CASB (Cloud Access Security Broker), CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), SASE (Secure Access Service Edge)
7	暗号技術 (技術的管理策のうち「暗号の利用」に対応)	暗号方式の種類・鍵管理	〔暗号方式の種類〕 共通鍵暗号方式, 公開鍵暗号方式 (RSA 暗号, DSA など), ハイブリッド暗号, 楕円曲線暗号, ECDSA (楕円曲線 DSA) 〔鍵交換〕 Diffie-Hellman 鍵交換 (DH), ECDH, 前方秘匿性 (PFS) 〔鍵と乱数の管理〕 鍵生成, 鍵管理, 鍵のライフサイクル (生成, 配送, 保管, 更新, 廃棄), HSM (Hardware Security Module), 鍵管理システム (KMS), 擬似乱数生成器 (PRNG), 量子乱数生成器 (QRNG), 危殆化 〔安全性の評価尺度〕 暗号強度 (ビットセキュリティ)
		ハッシュ関数	SHA-2 (SHA-256 など), SHA-3, 原像計算困難性 (一方向性), 第二原像発見困難性, 衝突発見困難性, MD5 及び SHA-1 の危殆化
		共通鍵暗号	ブロック暗号 (AES (Advanced Encryption Standard) など), ストリーム暗号 (KCipher-2 など), 暗号利用モード (CBC, CTR など), 認証暗号 (認証付き暗号, AEAD (Authenticated Encryption with Associated Data)), 軽量暗号
		公開鍵基盤	公開鍵基盤 (PKI), 認証局 (CA), 政府認証基盤 (GPKI), CP/CPS (Certificate Policy/Certification Practice Statement), CA/Browser Forum, ITU-T X.509, 証明書パス検証, 証明書失効リスト (CRL), OCSP, コードサイニング証明書, 証明書自動発行 (ACME), CAA (Certification Authority Authorization)
		応用的な暗号技術	秘密分散, 準同型暗号, ゼロ知識証明, TEE (Trusted Execution Environment), 量子鍵配送 (QKD), 耐量子計算機暗号 (PQC, ML-KEM, ML-DSA), 暗号アジリティ (Crypto Agility)

大分類 6：セキュリティ　中分類 26：セキュリティ実装技術・評価

【内容】

・システム及びソフトウェアの要求事項を踏まえて，セキュリティに配慮したシステムアーキテクチャを設計し，システム及びソフトウェアのセキュリティ機能を実装するために必要な，セキュア開発に関する専門的な知識を問う。

・インシデント発生時の証拠保全やマルウェア解析について他の専門家に協力し，原因究明及び再発防止に対応するために必要な，フォレンジックに関する専門的な知識を問う。

・システム及びソフトウェアの脆弱性やセキュリティ製品の適合性を，評価基準に基づいて評価するために必要な，セキュリティ評価に関する専門的な知識を問う。

小分類		項目	用語例
1	セキュア開発・実装	セキュリティに配慮したシステムアーキテクチャ及びシステム構築	ゼロトラストアーキテクチャ（ZTA，NIST SP 800-207，ポリシー決定ポイント（PDP），ポリシー実施ポイント（PEP）），AI を使ったセキュリティ技術（AI for Security）
		AI システムを守るための対策（Security for AI）	プロンプトインジェクション対策（プロンプト分離，エージェントの権限分離），LLM の脅威への対策（システムプロンプトの強化，機密情報のシステムプロンプトからの分離，入力されたプロンプトの検証，外部参照データの検証，外部参照データの分離，RAG 用のデータ及びデータストアへのアクセス制御），AI のセキュリティ確保のための技術的対策に係るガイドライン
		アプリケーション開発のセキュリティ	〔セキュア開発の進め方〕 セキュアプログラミング，セキュアコーディングの指針（安全なウェブサイトの作り方　など），脆弱性検査技術（ソースコード静的検査（SAST），プログラムの動的検査（DAST），Web アプリケーションソフトウェアの脆弱性検査，ファジング　など） 〔脆弱性への実装上の対策〕 出力時のエスケープ処理（出力エンコーディング），クロスサイトスクリプティング対策，SQL インジェクション対策（プレースホルダ　など），CSRF トークン，バッファオーバーフロー対策，パスワードクラック対策（ソルト，ストレッチング　など） 〔ブラウザが備える防御機構と指示〕 Same Origin Policy，CORS（オリジン間リソース共有），cookie の属性指定（Secure，HttpOnly，SameSite），HSTS（HTTP Strict Transport Security），CSP（Content Security Policy），SRI（Subresource Integrity） 〔ソフトウェアサプライチェーン及び実行環境の保護〕 シークレット管理（シークレットストア，ハードコードの排除），依存ライブラリの更新管理，

			署名付きコミット，成果物の署名検証，SLSA，要塞化（ハードニング）
		クラウド・コンテナのセキュリティ	責任共有モデルに基づく役割分担，クラウドのアイデンティティ・アクセス管理，クラウドの設定不備（公開設定，権限設定），インスタンスメタデータサービスの保護，コンテナイメージの脆弱性管理，コンテナオーケストレーションのアクセス制御（RBAC，ネットワークポリシー），IaC（Infrastructure as Code）のセキュリティスキャン
		ハードウェアのセキュリティ	セキュアエレメント，TPM（Trusted Platform Module），自己暗号化ドライブ（SED），セキュアブート（UEFI），耐タンパ性
		IoT・制御システムのセキュリティ	IoT のセキュリティ，制御システムのセキュリティ，IEC 62443（産業用オートメーション及び制御システムのセキュリティ），サイバーセキュリティマネジメントシステム（CSMS），ISASecure CSA 認証（IEC 62443-4-2），JC-STAR（セキュリティ要件適合評価及びラベリング制度），Purdue モデル，IT／OT 境界の DMZ，一方向ゲートウェイ，ファームウェアのセキュアアップデート，IT 製品の調達におけるセキュリティ要件リスト
2	フォレンジック	デジタルフォレンジック	証拠保全，揮発性データの収集順序，ディスクイメージの取得と書込み防止，ハッシュ値による同一性の証明，Chain of Custody（証拠保全の連鎖），タイムライン分析，メモリフォレンジック
		マルウェア解析	サンドボックス，ハニーポット，ハニーネット，パケットキャプチャ，バイナリファイルの解析，逆アセンブル，アンパック，解析やセキュリティ検知を回避する技術（パッカー，難読化，デバッガ検知（アンチデバッグ），マルウェア対策ソフトの停止　など）
3	セキュリティ評価	脆弱性評価	ソフトウェア構成分析（SCA），SBOM を利用した脆弱性管理，JVN（Japan Vulnerability Notes），共通脆弱性評価システム（CVSS），共通脆弱性識別子（CVE），共通脆弱性タイプ一覧（CWE），セキュリティ設定共通化手順（SCAP），KEV（Known Exploited Vulnerability），EPSS（Exploit Prediction Scoring System），SSVC（Stakeholder-Specific Vulnerability Categorization），脆弱性診断，ペネトレーションテスト，脆弱性報奨金制度（バグバウンティプログラム）
		コモンクライテリア	ISO/IEC 15408，コモンクライテリア（CC），プロテクションプロファイル（PP），ISO/IEC 18045，共通評価方法（CEM），評価保証レベル（EAL），JISEC（IT セキュリティ評価及び認証制度）
		暗号モジュールの評価	JCMVP（暗号モジュール試験及び認証制度），暗号モジュールのセキュリティ要求事項（FIPS 140），電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）

大分類 4：デジタル技術　中分類 16：ネットワーク

【内容】

・ネットワークシステムの要求事項を踏まえてセキュリティの観点から必要な指導・助言を行い，ネットワークシステムの構築・維持を支援するために必要な，ネットワークに関する専門的な知識を問う。

小分類		項目	用語例
1	ネットワーク方式	ネットワークの種類と特徴	センサーネットワーク，有線 LAN，無線 LAN（隠れ端末問題，さらし端末問題，SSID　など）
		インターネット技術	NAT，NAPT，オーバーレイネットワーク，TLD
2	データ通信と制御	伝送方式と回線の種類	波長分割多重（WDM），OFDMA，リンクアグリゲーション
		ネットワーク接続装置	レイヤー2 スイッチ（L2 スイッチ），レイヤー3 スイッチ（L3 スイッチ），ロードバランサー，VRRP，CSMA/CA
3	通信プロトコル	プロトコルの種類と特徴	〔データリンク層のプロトコルの種類と特徴〕 ARP，IPoE，IEEE 802.1Q 〔ネットワーク層のプロトコルの種類と特徴〕 IP，ICMP，ICMPv6，NDP，IGMP，ルーティング，エニーキャスト，IPv4/IPv6 共存技術（IPv4/IPv6 トランスレーション，IPv4/IPv6 デュアルスタック） 〔トランスポート層のプロトコルの種類と特徴〕 TCP，QUIC，ポート番号，ウィンドウ制御，確認応答 〔アプリケーション層のプロトコルの種類と特徴〕 HTTP，DNS，DHCP 〔ルーティングプロトコル〕 OSPF，BGP，MPLS
		インタフェースの種類と特徴	イーサネット，Wi-Fi，1000BASE-T，10GBASE-T，メッシュ Wi-Fi
4	ネットワーク応用	インターネットサービスの種類と特徴	〔電子メール〕 SMTP，POP3，IMAP4 〔Web ブラウジング〕 cookie，REST，GraphQL 〔通信サービス〕 衛星通信サービス，国際通信サービス，広域 Ethernet，IP-VPN，インターネット VPN，マルチホ

			ーミング
		モバイル通信・IoT 通信の特徴	〔モバイル通信サービス〕 移動体通信事業者（MNO），LTE，ネットワークスライシング 〔モバイルシステム構成要素〕 IMEI，SA（Stand Alone）方式，NSA（Non-Stand Alone）方式 〔IoT システムのネットワーク〕 LPWA（LTE-M（Cat-M1），NB-IoT（Narrow Band-IoT），Wi-SUN，LoRaWAN）
5	ネットワーク管理	ネットワーク運用管理	負荷分散（DNS ラウンドロビン　など），syslog，パケットアナライザー，SNMP（管理情報ベース（MIB））

【目標とする知識（その他の知識）】

大分類 1：ビジネス変革　中分類 4：サービスマネジメント

【内容】

・サービスの要求事項を踏まえてセキュリティの観点から必要な指導・助言を行い，継続性・可用性の高いサービスの提供を支援するために必要な，サービスマネジメントに関する応用的な知識を問う。

小分類		項目	用語例
1	サービスマネジメント	サービスマネジメントの目的と考え方	サービス，サービスマネジメント
		サービス事業の確立，維持及び改善	事業関係管理，サービス満足度，サービスレベル管理，サービスレベル合意書（SLA），サービスレベル指標（SLI），サービスレベル目標（SLO），供給者管理，外部供給者，内部供給者，サービスポートフォリオ管理，サービスポートフォリオ，サービスカタログ管理，サービスの報告，継続的改善，サービス品質，サービスの要求事項
		サービスの設計，構築及び移行	変更管理，変更要求（RFC），変更のカテゴリー（標準変更，通常の変更，プロジェクト変更，緊急変更　など），サービスの設計及び移行，サービス受入れ基準，移行，運用テスト，リリース及び展開管理，緊急リリースを含むリリースの種類，資産管理，構成管理，構成品目（CI），構成情報，構成ベースライン，サービスの予算業務及び会計業務，需要管理，容量・能力管理，容量・能力（キャパシティ），パフォーマンス
		サービス要求の実現	インシデント管理，インシデント，重大なインシデント，エスカレーション（機能的エスカレーション，階層的エスカレーション），サービス要求管理，問題管理，問題，既知の誤り，傾向分析，根本原因，予防処置，優先順位付け，モニタリング
		サービスの保証	サービス可用性管理，サービス可用性，MTBF，MTTR，サービス継続管理，ビジネス・インパクト分析（BIA），サービス継続計画

大分類 3：組織活動　中分類 12：ガバナンス・監査

【内容】

・情報セキュリティに関連するガバナンス確保，監査について他の専門家に協力し，情報セキュリティに関する指摘事項・改善提案に対する対応策の検討を支援するために必要な，ガバナンス・監査に関する応用的な知識を問う。

小分類		項目	用語例
2	内部統制・デジタルガバナンス	内部統制・デジタルガバナンス	内部統制の限界（合理的保障・デジタル／AI リスク考慮），内部統制報告制度（J-SOX），財務報告に係る内部統制の評価及び監査の基準，財務報告に係る内部統制の評価及び監査に関する実施基準，内部統制の基本的要素（統制環境，リスクの評価と対応，統制活動，情報と伝達，モニタリング，IT への対応）
3	監査	情報システムに関係する監査	監査の形態（システム監査，情報セキュリティ監査，個人情報保護監査，コンプライアンス監査，マネジメントシステム監査），統制自己評価（CSA），システム監査基準，システム管理基準，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制度，保証型監査と助言型監査
		システム監査の目的	システム監査人の権限と責任等，監査人の倫理，誠実性，専門的能力の保持と向上，正当な注意と秘密の保持，情報システムの利活用に係る検証・評価，保証・助言
		システム監査の計画・体制整備	システム監査計画の策定（リスクアプローチ，監査対象範囲，監査の方法）
		システム監査の実施	監査プロセス（予備調査，本調査，結論），予備調査の実施，監査手続書の作成，監査証拠の入手と評価（運用・保守の記録，アクセスログ，トランザクションログ，オーディットトレイル（監査証跡），監査証拠　など），改善提案のフォローアップ

大分類 4：デジタル技術　中分類 17：データベース

【内容】

・データベースシステムの要求事項を踏まえてセキュリティの観点から必要な指導・助言を行い，データベースシステムの構築・維持を支援するために必要な，データベースに関する応用的な知識を問う。

小分類		項目	用語例
1	データベース方式	データベースの概要	データアーキテクチャ（集中型アーキテクチャ，分散型アーキテクチャ，ハイブリッド型アーキテクチャ），データベースの 3 層スキーマアーキテクチャ，データモデル，グラフ型のデータモデル，関係モデル，ドキュメント指向データベース
2	データベース設計	データベースの設計	〔データベースの概念設計〕

			概念データモデル，E-R 図，UML，カーディナリティ 〔データベースの論理設計〕 論理データモデル，一貫性制約（一意性制約，参照制約，検査制約　など），主キー，外部キー，サロゲートキー
		正規化とパフォーマンス設計	正規化，データベースの性能評価，チューニング，再編成，データベースの運用・保守
3	データ操作	データベースの操作	集合演算，関係演算，関係代数
		データベース言語	DDL（データ定義言語），DML（データ操作言語）
4	トランザクション処理	トランザクション処理	同時実行制御（排他制御），コミットメント制御，2 相ロッキングプロトコル，デッドロック，2 相コミットメント，ACID 特性 〔障害回復〕 ジャーナルファイル（ログファイル），チェックポイント，フォワードリカバリ（ロールフォワード），バックワードリカバリ（ロールバック）
5	データベース応用	分散データベース	コミットシーケンス，レプリケーション，水平分散，垂直分散，表の分散（水平，垂直），結果整合性，シャーディング

大分類 5：システムの開発・運用　中分類 20：システムライフサイクルプロセス

【内容】

・システム及びソフトウェアの開発プロジェクトやシステム運用業務の各活動においてセキュリティ確保を推進又は支援するために必要な，システムライフサイクルプロセスに関する応用的な知識を問う。

小分類		項目	用語例
1	開発プロセスの概要	ライフサイクルプロセス	システムライフサイクルプロセス，ソフトウェアライフサイクルプロセス（SLCP），テクニカルプロセス
2	システム要件定義・ソフトウェア要件定義	システム要件の定義	システムの機能要件，システムの性能要件，入出力情報要件，データベース要件，テスト要件，セキュリティ要件，運用要件，保守要件，可用性，障害対応，保守の形態，保守のタイミング，設計及び実装の制約条件，システム要件の評価及びレビュー
		ソフトウェアの境界及び要件の定義	ソフトウェアの機能仕様，サブシステム分割，サービスの定義，セキュリティ要件の識別，保守性の考慮，ソフトウェア要件の評価及びレビュー
3	設計	システム設計	ハードウェア・ソフトウェア・サービス・手作業の機能分割，機能要件，非機能要件，ハードウェア構成の決定，ソフトウェア構成の決定，システム処理方式の決定（マイクロサービスアーキテク

			チャ，サービスメッシュ，サーキットブレーカー，サーバレスアーキテクチャ）
		ソフトウェア設計	ソフトウェアの構造の設計，ソフトウェアユニット分割，ソフトウェアユニットのテストの設計，ソフトウェア統合テストの設計
		ソフトウェア品質	品質特性モデル（機能適合性，信頼性，セキュリティ，保守性，安全性　など）
		モジュール設計	モジュール分割基準（モジュール強度，モジュール結合度）
4	実装・構築	ソフトウェアユニットの作成	コーディング標準，構造化プログラミング，並列処理プログラミング，コードレビュー（メトリクス計測，コードインスペクション）
		ソフトウェアユニットのテスト	ドライバ，スタブ，テスト設計と管理手法，ホワイトボックステスト，ブラックボックステスト
5	統合・テスト	ソフトウェア統合・ソフトウェア検証	ソフトウェア統合計画，ソフトウェア統合テスト，トップダウンテスト，ボトムアップテスト，統合テスト報告書，ソフトウェア検証テスト，ソフトウェア検証テストの評価，性能テスト，負荷テスト，セキュリティテスト，ソフトウェア検証テスト報告書
		システム統合・システム検証	システム統合テスト，システム統合の評価
6	導入・受入れ支援	導入	導入作業，リプレース
		受入れ支援	受入れ基準，教育訓練計画
		妥当性確認テスト	妥当性確認される要件（要求事項），妥当性確認テストの目的，成功基準（期待される結果），不具合の根本原因
7	運用	システム運用	障害発生時の運用計画，AIOps，運用安全及び業務安全に関する安全戦略
8	保守・廃棄	保守	保守テスト，是正保守，改良保守，予防保守，適応保守，完全化保守，システム信頼性のための解析技法（FTA，FMEA　など）

大分類 5：システムの開発・運用　中分類 21：開発・運用の方法論

【内容】

・システム及びソフトウェアの開発，品質管理，運用保守の業務をセキュリティの観点から推進又は支援するために必要な，システムの開発及び運用の方法論や手法・技法に関する応用的な知識を問う。

小分類		項目	用語例
1	開発の手法・方法論	アジャイル開発	エクストリームプログラミング（XP），スクラム，リーンソフトウェア開発，テスト駆動開発（TDD）
		DevOps	SRE（Site Reliability Engineering：サイト信頼性エンジニアリング），エラーバジェット，継続的インテグレーション（CI），継続的デリバリー（CD），継続的デプロイ，カオスエンジニアリング，オブザーバビリティ（可観測性），DevSecOps

2	開発関連の設計手法	アーキテクチャパターン	レイヤードアーキテクチャ，クリーンアーキテクチャ，MVC，マイクロサービスアーキテクチャ，SOA（Service-Oriented Architecture）
		デザインパターン	GoF，生成に関するパターン，構造に関するパターン，振る舞いに関するパターン
		オブジェクト指向設計	ソフトウェア設計原則（SOLID），カプセル化，多相性（ポリモーフィズム），汎化，特化，クラス図，アクティビティ図，ステートマシン図
4	開発プラットフォーム・開発ツール	開発環境	ソースコード管理（SCM），ステージング環境，設計データ管理，統合開発環境（IDE）
		OSS	オープンソースライブラリ，オープンソースライセンシング，GPL（General Public License）
5	Web アプリケーション開発	Web デザイン	モバイルファースト，レスポンシブ Web デザイン
		Web プログラミング	サーバサイドプログラミング，SPA（Single Page Application），WebAssembly
		モバイル Web アプリケーション	プログレッシブウェブアプリ（PWA），パーミッション要求
9	施設管理技術	施設管理技術	建物管理（免震装置，アレスタなどのサージ防護デバイス，防災防犯設備，安全管理関連知識　など），消火設備（泡消火設備，ハロゲン化物消火設備，不活性ガス消火設備　など），電気設備（UPS，自家発電設備　など）

【目標とする技能】

大項目	小項目	概　要	目標とする技能の例
1. 情報セキュリティマネジメントの組織的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。	・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。 クラウドサービス，AI などの安全な導入・利用に関する指針・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	・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，規格の変化や情報セキュリティ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	目標とする技能の例
		要な指導・助言を行い，支援する。	
	1-5 セキュリティ運用状況の点検	セキュリティ運用状況の点検（情報資産管理，システム利用状況管理などの点検）について，必要な指導・助言を行い，支援する。 情報セキュリティマネジメントシステムの運用・適合性確認について，必要な指導・助言を行い，支援する。	・業務プロセス，手順，運用見直し，リスクなどの状況を踏まえた上で，セキュリティ運用状況を点検する能力 ・ログ分析による設定不備や不正の検出，及び点検結果に基づく是正・改善を行う能力 ・内部監査の実施，是正措置の管理，及び経営層への報告を行う能力
	1-6. サプライチェーンの情報セキュリティの推進	ビジネスパートナー・委託先との契約への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。	・契約に盛り込むべきリスク低減のための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
	1-7. コンプライアンス管理	情報セキュリティ，個人情報保護及び AI に関連する法令，規制，ガイドライン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。 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作成及び利用について，必要な指導・助言を行い，支援する。 AI 関連のガイドラインの遵守について，必要な指導・助言を行い，支援する。	・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
	1-8. 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	・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

大項目	小項目	概　要	目標とする技能の例
		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。	
	1-9. 情報セキュリティ監査及びデジタルガバナンス確保への対応	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。 DX 推進に向けたデジタルガバナンス体制の構築・運用において，情報セキュリティの観点から指導・助言を行い，支援する。	・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
	1-10. 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。 脅威インテリジェンスや脆弱性収集ツールを活用し，検出・対応・予防策を強化する。 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	・脅威インテリジェンスや脆弱性収集ツールを活用して，必要な情報を迅速かつ継続的に収集する能力 ・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，最先端の情報を収集する能力 ・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

大項目	小項目	概　要	目標とする技能の例
		緊急性，対応の費用・効果・必要性を評価し，報告する。	
	1-11. 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，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。	・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
2. 情報システムのライフサイクルプロセスにおける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）	情報システムのライフサイクルプロセスについて，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。	・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（IoT，クラウドサービスを含む）へのセキュリティ確保の実施について，必要な指導・助言を行い，支援する。	・仕様書とセキュリティ要件とを照らして，また，制度・ガイドラインも踏まえて，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	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	・アーキテクチャの設計書をレビューする能力

大項目	小項目	概　要	目標とする技能の例
	の観点）	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
	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。	・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。	・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。	・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	・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	目標とする技能の例
		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。	
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及び他のセキュリティソリューションのマルウェア検知・防御能力を評価し，効果的に適用する能力
	3-3. データ保護	情報の削除及びデータマスキングについて，必要な指導・助言を行い，支援する。 データ漏えい防止対策のシステムやネットワークへの適用について，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。	・媒体特性に応じたデータ消去を行う能力 ・データマスキングの運用を行う能力 ・情報漏えい対策の運用を行う能力 ・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	目標とする技能の例
		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。	
	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，分析について，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。 クラウド環境におけるセキュリティ管理について，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 ・クラウド環境における設定不備や過剰な権限付与を持続的に検出し，是正策を設計する能力
	3-6. 技術的脆弱性への	情報システム及びコンポーネントの構成管理，脆弱	・効果的な構成管理，脆弱性情報収集を設計する能力

大項目	小項目	概　要	目標とする技能の例
	対応	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
	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，オフィス内外の機器の保護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
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対応体制の構築	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。 サイバー攻撃などによる被害を想定し，サイバーレ	・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 ・サイバー攻撃などを想定した具体的な復旧訓練を計画・評

大項目	小項目	概　要	目標とする技能の例
		ジリエンスの実現に必要な指導・助言を行い，支援する。	価する能力 ・情報セキュリティインシデント対応手順を設計する能力 ・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
	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。	・事実関係を確認し，整理する能力 ・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. 情報セキュリティインシデントへの対応	情報セキュリティインシデントによる被害・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。	・根本原因を特定し，再発防止を設計する能力 ・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	・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

大項目	小項目	概　要	目標とする技能の例
		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。	・証拠を分析する能力

■情報処理安全確保支援士試験
シラバス（案）

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）
ホームページ：https://www.ipa.go.jp/shiken/