

情報セキュリティマネジメント試験 シラバス（案）

－ 情報処理技術者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。



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

Beyond Digital

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。

■ はじめに

本シラバスは、情報セキュリティマネジメント試験の出題範囲案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〕の分類ごとに主な用語例を示しています。

「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。

1. 本シラバスにおいて示す内容

【目標とする知識（重点分野）】※科目 A の出題範囲の細目。

大分類○：XXXXXXXXXX 中分類○：XXXXXXXXXX		
【内容】 ・XX		
小分類	項目	用語例
大分類○：XXXXXXXXXX 中分類○：XXXXXXXXXX		
【内容】 ・XX		
小分類	項目	用語例

【目標とする知識（その他の分野）】※科目 A の出題範囲の細目。

大分類○：XXXXXXXXXX 中分類○：XXXXXXXXXX		
【内容】 ・XX		
小分類	項目	用語例
大分類○：XXXXXXXXXX 中分類○：XXXXXXXXXX		
【内容】 ・XX		
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	目標とする技能の例

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（重点分野）】

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】

- ・日々の業務で起こり得る情報セキュリティの脅威や攻撃の内容を把握し、部門のメンバーからマルウェア感染などの疑いが報告された際に適切に判断して対応するために必要な、情報セキュリティの脅威に関する基本的な知識を問う。

小分類		項目	用語例
1	脅威と脆弱性 ^{ぜい}	脅威の種類と動向	事故，災害，故障，破壊，盗難，侵入，不正アクセス，盗聴，なりすまし，改ざん，エラー，クラッキング，ビジネスメール詐欺（BEC），アクセス権の誤設定，紛失，破損，盗み見，不正利用，ソーシャルエンジニアリング，情報漏えい，内部不正，踏み台，情報セキュリティ 10 大脅威
		マルウェア・不正プログラム	コンピュータウイルス，マクロウイルス，ボット，ボットネット，トロイの木馬，スパイウェア，ランサムウェア，キーロガー，ルートキット，バックドア，ファイルレスマルウェア
		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
		不正の動機・メカニズム	ダークウェブ，ハクティビズム，サイバーテロリズム，リークサイト，不正のトライアングル，RaaS（Ransomware as a Service），二重恐喝（多重恐喝），状況的犯罪予防，割れ窓理論
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，偵察（フットプリンティング，ポートスキャン など），ラテラルムーブメント
		資格情報・セッション管理の不備を狙った攻撃	辞書攻撃，総当たり攻撃（ブルートフォース攻撃），リバースブルートフォース攻撃，クレデンシャルスタッフィング，セッションハイジャック，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，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，クロスサイトリクエストフォージェリ（CSRF），ディレクトリトラバーサル，バッファオーバーフロー，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	中間者（Man-in-the-middle）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，標的型攻撃，水飲み場型攻撃，SEO ポイズニング
		サービスの妨害を狙った攻撃	DoS 攻撃，DDoS 攻撃
		AI を悪用した攻撃	マルウェア亜種の自動生成，フィッシング文面の巧妙化，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，データポイズニング

		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
		その他・特殊・高度な攻撃	ゼロデイ攻撃，サービス及びソフトウェアの機能の悪用
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】 ・部門において取扱う情報資産の情報セキュリティを維持するために必要な，情報セキュリティマネジメントに関する基本的な知識を問う。 ・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，リスク対応策を検討・提案するために必要な，リスクマネジメントに関する基本的な知識を問う。			
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），ゼロトラスト，セキュリティバイデザイン，プライバシーバイデザイン
		情報セキュリティマネジメントの考え方	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・生成 AI 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，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）
		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，リスクヘッジ，リスクファイナンス，リスク対応計画，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
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），情報セキュリティ目的，情報セキュリティ対策基準，情報管理規程，秘密情報管理規程，文書管理規程，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，情報セキュリティ教育の規程，プライバシーポリシー（個人情報保護方針），職務規程，罰則の規程，対外説明の規程，例外の規程，規則更新の規程，規程の承認手続，ソーシャルメディアガイドライン（SNS 利用ポリシー）

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)), エシカルハッカー 〔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, サイバーレスキュー隊 (J-CRAT), FIRST (Forum of Incident Response and Security Teams) 〔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, ソフトウェア等の脆弱性関連情報に関する届出制度, コンピュータウイルス対策基準, 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届出制度 〔評価・登録の制度〕 情報セキュリティサービス基準, ISMAP (政府情報システムのためのセキュリティ評価制度), SECURITY ACTION 〔対策の指針となる基準・フレームワーク〕 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, PCI DSS, NIST サイバーセキュリティフレームワーク (CSF)
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, 運用, パフォーマンス評価 (内部監査, マネジメントレビュー など), 不適合及び是正処置, 継続的改善, 情報セキュリティ管理策 (組織的管理策, 人的管理策, 物理的管理策, 技術的管理策), 管理策タイプ (予防, 検知, 是正), サイバーセキュリティ概念 (識別, 防御), 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, 脅威インテリジェンス

			〔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，情報の分類，情報のラベル付け，情報の転送 〔アクセス制御〕 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 〔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への対応，証拠の収集，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，プライバシー及び PII の保護
		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，クリアデスク・クリアスクリーン
		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 〔情報資産運用に関する管理〕 マルウェアに対する保護，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，ログ取得

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】

・部門の情報セキュリティ確保に貢献するために必要な，情報セキュリティ対策に関する基本的な知識を問う。

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，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, トリアージ, 法令に基づく報告及び本人への通知, 関係機関への届出, サイバー保険
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, 机上演習 など), 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)
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	最小特権, 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 (署名鍵, 検証鍵), メッセージダイジェスト, メッセージ認証
		利用者の認証・認可・ID 連携	ログイン (利用者 ID とパスワード), アクセス管理, PIN コード, ワンタイムパスワード, 多要素認証, 多段階認証, リスクベース認証, シングルサインオン, eKYC, EMV 3-D セキュア (3D セキュア 2.0)
		生体認証	身体的特徴 (静脈パターン認証, 虹彩認証, 顔認証 など), 行動的特徴, 本人拒否率 (FRR), 他人受入率 (FAR)
		パスワードレス認証	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〕 マルウェア対策ソフトの導入, マルウェア定義ファイルの更新, マルウェア検出手法 (パターンマッチング法, ピヘイピア法 (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 〔ランサムウェア対策〕 データのバックアップ, 3-2-1 ルール, イミュータブルバックアップ
		脆弱性管理・データ保護	脆弱性管理 (OS アップデート, 脆弱性修正プログラム (セキュリティパッチ) の適用), 脆弱性情報の収集
		ログ管理・監視・検知及び対応	取得範囲, 保存期間, 時刻同期 (NTP) とタイムスタンプ, SIEM (Security Information and Event Management), EDR (Endpoint 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	境界防御，ファイアウォール，IDS（侵入検知システム）／IPS（侵入防止システム），VPN，検疫ネットワーク，リバースプロキシ，CAPTCHA
ネットワークセキュリティの技術規格・プロトコル		TLS，IPsec，RADIUS，WPA3，SMTP-AUTH，OP25B，送信ドメイン認証（SPF，DKIM）	
ネットワークセキュリティの製品・サービス		WAF（Web Application Firewall），許可リスト（アローリスト／パスリスト），拒否リスト（ブロックリスト），URL フィルタリング（Web フィルタリング）	
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	共通鍵暗号方式，公開鍵暗号方式（RSA 暗号 など），ハイブリッド暗号，鍵管理，危殆化
		ハッシュ関数	SHA-2（SHA-256 など），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）
大分類 7：倫理・コンプライアンス 中分類 29：プライバシー関連法規			
【内容】			
・個人情報の漏えいやプライバシーの侵害が組織に深刻な影響を与えることを理解するとともに，部門において取扱う個人情報やプライバシーに関わる情報を適切に管理するために必要な，プライバシー関連法規に関する基本的な知識を問う。			
小分類		項目	用語例
1	プライバシー保護に関する法規・ガイドライン	個人情報保護・プライバシー保護に関する法規・ガイドライン	個人情報保護法，個人情報取扱事業者，安全管理措置，個人情報，個人データ，保有個人データ，個人識別符号，要配慮個人情報，匿名加工情報，仮名加工情報，個人情報データベース等，マイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律），特定個人情報の適正な取扱いに関するガイドライン，個人情報保護委員会，JIS Q 15001，一般データ保護規則（GDPR）
2	プライバシー保護に関する手法・技法	個人情報保護・プライバシー保護に関する手法・技法	オプトイン，オプトアウト，第三者提供，プライバシー影響評価（PIA），プライバシーフレームワーク，情報漏えい対策，データマスキング，電子透かし，項目削除／レコード削除／セル削除，トップ（ボトム）コーディングなどの一般的な手法のほか，k-匿名化などの高度な手法を含む

大分類 7 : 倫理・コンプライアンス 中分類 30 : セキュリティ関連法規

【内容】

- ・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、法令に基づいて適切に判断・対応するために必要な、セキュリティ関連法規に関する基本的な知識を問う。

小分類		項目	用語例
1	刑法・不正アクセス禁止法	刑法	不正指令電磁的記録に関する罪（ウイルス作成罪），電子計算機使用詐欺罪，電子計算機損壊等業務妨害罪，電磁的記録不正作出及び供用罪，支払用カード電磁的記録不正作出等罪
		不正アクセス禁止法	アクセス制御機能，不正アクセス行為，不正アクセス行為を助長する行為
2	その他セキュリティ関連法規	その他のセキュリティ関連法規	サイバーセキュリティ基本法，サイバーセキュリティ，サイバーセキュリティ戦略，サイバーセキュリティ協議会，特定電子メール法，サイバー対処能力強化法（能動的サイバー防御），重要経済安保情報保護法

【目標とする知識（その他の分野）】

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】

・サービスに関するインシデントや問合せが発生したときにサービス提供者と適切に連携するために必要な、サービスマネジメントに関する基本的な知識を問う。

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, SLA
2	サービスマネジメントの活動	サービス事業の確立, 維持及び改善	顧客満足, サービス満足度, サービスレベル管理, 供給者管理, サービスの報告, 継続的改善, 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, サービス受入れ基準, 移行, 運用引継ぎ, リリース及び展開管理, 資産管理, 構成管理, 構成品目 (CI), 需要管理
		サービス要求の実現	サービスデスク, 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, サービス要求管理, サービス要求, 問題管理, 既知の誤り, 傾向分析, 根本原因, 予防処置
		サービスの保証	サービス可用性管理, コールドスタンバイ, ホットスタンバイ, サービス継続管理, サービス継続計画

大分類 2：データ・AI の利活用 中分類 9：データ分析・データ利活用

【内容】

・データサイエンティストなどの高度なデータ分析を行う担当者からの要請や分析結果を正しく理解し、実務の観点から円滑に連携・協力するために必要な、データ基盤及びデータ分析に関する基本的な知識を問う。

・組織から提供されたデータや分析ツール（BI ツールなど）を自らの担当業務に適用し、業務プロセスの改善（効率化、品質向上など）や日々の業務遂行における判断の根拠として役立てるために必要な、業務分析及びデータ利活用に関する基本的な知識を問う。

小分類		項目	用語例
2	データ分析・データ利活用	データの種類と特徴	1 次データ, 2 次データ, ビッグデータ, オープンデータ, パーソナルデータ
		データの加工・分析	スクレイピング, データマイニング, テキストマイニング, シミュレーション
		データ分析における統計的手法	統計的バイアス, 認知バイアス
3	業務分析	業務分析・業務計画	QC 七つ道具, 新 QC 七つ道具, ブレーンストーミング, デルファイ法

大分類 2：データ・AI の利活用 中分類 10：AI 利活用			
【内容】 ・ AI を価値創造や意思決定のための活動に効果的に活用するために必要な，AI の活用領域及び活用目的，AI の信頼性を保って利用する方法（自律性と人間の関与，ガードレールなど）に関する基本的な知識を問う。			
小分類		項目	用語例
2	識別 AI 利活用	識別 AI の活用領域及び活用目的	教師あり学習による予測，教師なし学習によるグルーピング，強化学習による支援
3	生成 AI 利活用	生成 AI の活用領域及び活用目的	マルチモーダル AI，ランダム性の制御，RAG による知識連携，プロンプトエンジニアリング
4	AI エージェント利活用	AI エージェントの活用領域及び活用目的	AI エージェント，自律性と人間の関与（最終承認，例外処理 など），ガードレール（安全性への配慮，倫理的配慮，法令順守 など）
大分類 3：組織活動 中分類 11：経営・組織論			
【内容】 ・ 担当業務と事業・組織全体の関係性，人や金の動き・流れを理解し，広い視野で業務を遂行するために必要な，経営・組織論に関する基本的な知識を問う。			
小分類		項目	用語例
2	経営管理	経営管理・経営組織	PDCA，最高経営責任者（CEO），最高デジタル責任者（CDO），最高情報セキュリティ責任者（CISO），最高プライバシー責任者（CPO），最高情報責任者（CIO）
		ヒューマンリソースマネジメント	ケーススタディ，リスクリング
		事業継続計画	事業継続計画（BCP），事業継続マネジメント（BCM），事業影響度分析（BIA）
3	会計・財務	売上と利益の関係	利益，粗利益，営業利益，費用，固定費，変動費，原価，損益分岐点
		財務諸表	貸借対照表，損益計算書，キャッシュフロー計算書，流動資産，固定資産，有形固定資産，無形固定資産，繰延資産，流動負債，固定負債，純資産
大分類 3：組織活動 中分類 12：ガバナンス・監査			
【内容】 ・ 監査対象部門の立場として，監査時に関係者と連携を図るとともに，情報セキュリティに関する指摘事項・改善提案への対応を適切に行うために必要な，ガバナンス及び監査に関する基本的な知識を問う。			
小分類		項目	用語例
1	コーポレートガバナンス	コーポレートガバナンス	コーポレートガバナンス，コンプライアンス
2	内部統制・デジタル	内部統制・デジタルガバナンス	内部統制の限界（合理的保証・デジタル／AI リスク考慮），職務分掌，実施ルールの設定，チェッ

	ガバナンス		ク体制の確立，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，IT への対応（IT 環境への対応，IT の利用，IT に係る全般統制，IT に係る業務処理統制）
3	監査	情報システムに係る監査	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，内部監査
		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，監査の独立性と客観性の保持，情報システムの利活用に係る検証・評価，システム監査基準，システム管理基準
		システム監査の実施	監査プロセス（予備調査，本調査，結論），監査証拠の提供，監査報告書，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 15：クラウド

【内容】

・部門においてクラウドサービス利用の要望などがあった際に，組織の情報セキュリティのルールに照らした上で，意見や問題点を提起するために必要な，クラウドに関する基本的な知識を問う。

小分類		項目	用語例
1	クラウドサービス	クラウドサービスの特徴	クラウドサービス（SaaS，PaaS，IaaS など），クラウドサービスの提供形態（パブリッククラウド，プライベートクラウド，ハイブリッドクラウド，マルチクラウド など），ソブリッククラウド，オンプレミスとクラウドとの違い，データ保持の方法，リージョン
2	基盤技術	クラウド・仮想化基盤技術	仮想化（ホスト型，ハイパーバイザー型，コンテナ型），クラスタ，シンクライアント

大分類 4：デジタル技術 中分類 16：ネットワーク

【内容】

・部門においてインターネットサービス利用の要望などがあった際に，組織の情報セキュリティのルールに照らした上で，意見や問題点を提起するために必要な，ネットワークに関する基本的な知識を問う。

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	LAN，WAN，インターネットサービスプロバイダ（ISP），有線 LAN，無線 LAN（無線 LAN アクセスポイント，SSID など）
		インターネット技術	IPv4，IPv6，グローバル IP アドレス，プライベート IP アドレス，ドメイン，ファイアウォール，RADIUS
2	データ通信と制御	ネットワーク接続装置	スイッチングハブ，ルータ，ゲートウェイ，プロキシサーバ，リバースプロキシサーバ
3	通信プロトコル	プロトコルの種類と特徴	IP アドレス，サブネットアドレス，サブネットマスク，ルーティング，ポート番号，HTTP，HTTP over TLS（HTTPS），SMTP，POP3，FTP，DNS，DHCP，IMAP

		インタフェースの種類と特徴	イーサネット, 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] MIME, HTML メール, Web メール [Web ブラウジング] cookie, URL [通信サービス] IP-VPN, インターネット VPN
		モバイル通信・IoT 通信の特徴	LTE, 5G (第 5 世代移動通信システム), テザリング
5	ネットワーク管理	ネットワーク運用管理	障害の切分け, 障害原因の特定, 復旧措置
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】 ・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ために必要な, セキュリティ実装技術及び評価に関する基本的な知識を問う。			
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	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, RAG 用のデータ及びデータストアへのアクセス制御
		アプリケーション開発のセキュリティ	セキュアプログラミング, 安全なウェブサイトの作り方, 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, バッファオーバーフロー対策
		IoT・制御システムのセキュリティ	IoT のセキュリティ, JC-STAR (セキュリティ要件適合評価及びラベリング制度)
3	セキュリティ評価	脆弱性評価	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), 脆弱性診断, ペネトレーションテスト

大分類 7：倫理・コンプライアンス 中分類 27：情報倫理・AI 倫理

【内容】

・業務遂行においてデータや AI（生成 AI など）を利用する際に、社会や組織に対して及ぼす影響を考慮し、実務担当者として適切に振る舞うために必要な、情報倫理及び AI 倫理に関する基本的な知識を問う。

小分類		項目	用語例
1	情報倫理・情報モラル	情報倫理・情報モラル	倫理的・法的・社会的な課題（ELSI：Ethical, Legal and Social Issues）、同報メールの適切な利用（TO, CC, BCC, メーリングリスト）、メール誤送信、デジタルタトゥー、フェイクニュース、ファクトチェック、エコーチェンバー、フィルターバブル、悪意ある情報（マルインフォメーション）、偽情報（ディスインフォメーション）、誤情報（ミスインフォメーション）、フィルタリング
2	AI 倫理・AI ガバナンス	AI 倫理・AI ガバナンス	説明可能な AI（XAI：Explainable AI）、ヒューマンインザループ（HITL）、AI サービスのオプトアウトポリシー、AI 倫理アセスメント、AI ガバナンス、AI 利用ポリシー
		AI のリスク・脅威	セキュリティ・プライバシーへの懸念（生成 AI への機密情報・個人情報の入力）、フロンティア AI によるリスクと脅威、ハルシネーション、シャドーAI、ディープフェイク

大分類 7：倫理・コンプライアンス 中分類 28：ビジネス関連法規

【内容】

・他者の権利の侵害、契約・取引上のトラブルなどが起きないように留意しながら、安心して業務を遂行するために必要な、ビジネス関連法規に関する基本的な知識を問う。

小分類		項目	用語例
1	知的財産権	著作権法	著作権、著作権法、引用
2	労働関連法規	労働関連法規	労働基準法、労働者派遣法（雇用契約、派遣契約、指揮命令、偽装請負）、公益通報者保護法
3	取引関連法規	不正競争防止法	営業秘密、営業秘密の 3 要件（秘密管理性、有用性、非公知性）、限定提供データ、ドメイン名の不正取得、コピープロテクト外し
		取引関連法規	民法（準委任契約、請負契約）、中小受託取引適正化法（取適法）
		企業間の取引に関わる契約	外部委託契約、守秘契約（NDA）、ソフトウェア使用許諾契約（ライセンス契約）、ボリュームライセンス契約、ソフトウェア開発契約、ソフトウェア開発委託モデル契約、情報システム・モデル取引・契約書
5	その他デジタル関連法規・ガイドライ	その他デジタル関連法規	デジタル社会形成基本法、官民データ活用推進基本法、人工知能関連技術の研究開発及び活用の推進に関する法律（AI 基本法）、情報流通プラットフォーム対処法、e-文書法、電子帳簿保存法

	ン		
		標準化関連	デファクトスタンダード，デジュレスタンダード

【目標とする技能】

大項目	小項目	目標とする技能の例
Ⅰ 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	1-1. 情報資産の特定及び価値の明確化	・ 部門で利用する情報資産（情報システム、データ、文書、施設、人材など）を特定することの必要性、方法、手順を理解し、また、機密性、完全性、可用性の三つの側面からそれらの価値（重要度）を明確化することの必要性、方法、手順を理解した上で、文書精査、ヒアリングなどによって情報資産の価値を明確化するスキル
	1-2. 管理責任及び利用の許容範囲の明確化	・ 情報資産の管理責任者の役割を理解した上で、部門における情報資産の管理方針と管理体制を検討するスキル ・ 組織と部門が定めた方針に基づき、情報資産の受入れと確認、利用の許容範囲の明確化、変更管理、廃棄管理などについて、必要性、方法、手順を理解した上で、自らルールを検討して提案するスキル
	1-3. 情報資産台帳の作成	・ 情報資産台帳を作成することの必要性、方法、手順を理解した上で、情報資産台帳を作成するスキル
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	2-1. リスクの特定・分析・評価	・ 部門で利用する情報資産について、脅威、脆弱性、資産の価値を、組織的な要因、人的な要因、物理的な要因、技術的な要因の4つの側面から分析するスキル ・ リスクについて、事象の起こりやすさ、及びその事象が起きた場合の結果を定量的又は定性的に把握してリスクの大きさを算定するための考え方、手法を理解した上で、組織が定めたリスク受容基準に基づく評価を実施するスキル ・ 新種の脅威の発生、情報システムの変更、組織の変更に伴う新たなリスクについて、それらを特定し、評価するスキル
	2-2. リスク対応策の検討	・ 特定・分析・評価した全てのリスクに対して、組織的管理策、人的管理策、物理的管理策、技術的管理策のそれぞれの区分でのリスク対応の考え方、必要性、方法、手順を理解した上で、リスク対応策を検討するスキル

大項目	小項目	目標とする技能の例
		・ 検討した対応策について，現在の実施状況を把握するスキル ・ リスクの大きさ，リスク対応策の実施に要するコスト，及び対応策を実施しても残留するリスクへの対処の考え方，方法，手順を理解した上で，（それらのリスクを許容できるか否かを考慮した）リスク対応策の優先順位を検討するスキル
	2-3. リスク対応計画の策定	・ 検討したリスク対応策の優先順位を基に，リスク対応計画を作成する目的，及び記載する内容（実施項目，資源，責任者，完了予定時期，実施結果の評価方法ほか）を理解した上で，リスク対応計画を作成するスキル
3. 情報資産に関する情報セキュリティ要求事項の提示	3-1. 部門の情報システムの調達・利用に関する組織的・人的・物理的・技術的な要求事項の提示	・ 情報資産を保護するための管理策の考え方を理解した上で，情報システム部門の技術的支援を受けながら，リスク対応計画に基づく要求事項の取りまとめを実施するスキル 〔要求事項の項目の例〕 ✓アクセス制御に関する業務上の要求事項，利用者アクセスの管理，利用者の責任 ✓執務場所への入退管理，情報資産の持込み・持出し管理，ネットワークの物理的な保護 ✓部門で調達（取得）又は開発し，利用する情報システムに関する情報セキュリティ要求事項，開発及びサポートプロセスにおける情報セキュリティ，試験データの取扱いなど ✓運用の手順及び責任 ・ 情報システム部門が所有する情報システムのうち，部門が利用する情報システムに関しても，必要に応じて同様に要求事項を取りまとめて提案するスキル
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	4-1. 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	・ 障害，災害など困難な状況の発生時において，部門の情報セキュリティを継続的に確保するために必要な情報セキュリティ要求事項を理解した上で，それらの事項が事業継続計画に盛り込まれていることを確認するスキル ・ 過不足がある場合に，改善（必要事項を計画に盛り込み，追加の手順を定めて文書化する）

大項目	小項目	目標とする技能の例
		を提案するスキル
II 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		
5. 情報資産の管理	5-1. 情報資産台帳の維持管理	・ 情報資産台帳に記載する内容、及び台帳の維持管理の必要性、手順を理解した上で、情報セキュリティポリシーを含む組織内諸規程（以下、情報セキュリティ諸規程という）及び部門で定めたルールに従い、情報資産の受入れ、配置、管理者変更、構成変更、他部門への移転及び廃棄を適切に反映して、情報資産台帳を維持管理するスキル
	5-2. 媒体の管理	・ 情報セキュリティインシデント（以下、インシデントという）を発生させないために必要な、可搬媒体の管理（部門の執務場所と外部との間での持込み・持出し、廃棄）の方法、手順を理解した上で、あらかじめ定められた手順を部門のメンバーが適切に実施するためのアドバイスを行うスキル
	5-3. 利用状況の記録	・ 情報資産を管理することの必要性、方法、手順を理解した上で、対象資産の利用状況を把握し、また、その配置、管理者、構成の変更などを追跡し、情報資産の利用状況を記録するスキル
6. 部門の情報システム利用時の情報セキュリティの確保	6-1. マルウェアからの保護	・ マルウェアのタイプ、及びマルウェアからの情報資産の保護の目的、仕組みを理解した上で、マルウェアやマルウェア対策ソフトについて、部門のメンバーの理解を深め、情報セキュリティ諸規程の順守を促進するスキル
	6-2. バックアップ	・ 重要なデータの消失を防ぐために、バックアップの考え方、方法、手順を理解した上で、バックアップの重要性について、部門のメンバーの理解を深め、情報セキュリティ諸規程に従ったバックアップの実施を促進するスキル
	6-3. ログ取得及び監視	・ 情報システムに関連するシステムログ、システムエラーログ、アラーム記録、利用状況ログなどのログの種類と、ログを取得する目的を理解した上で、それらの記録、定期的な分析を基に、不正侵入などの情報セキュリティ事故や情報セキュリティ違反を監視するスキル
	6-4. 情報の転送における情報セキュリティの維持	・ 情報の転送における情報セキュリティの維持の考え方、仕組みを理解した上で、情報セキュリティ諸規程と、情報システムが提供する機能に従って、部門のメンバーが転送する情

大項目	小項目	目標とする技能の例
		報の内容確認、閲覧する Web サイトの管理、機器の持込み・持出しなどの管理を実施するスキル
	6-5. 脆弱性管理	・脆弱性管理の考え方、必要性、方法、手順を理解した上で、部門の情報システムの使用状況に基づいてパッチ情報を入手し、組織が定めたパッチ適用基準に基づいてパッチ適用を促進するスキル
	6-6. 利用者アクセスの管理	・情報システムや執務場所その他における情報資産へのアクセス管理の考え方、必要性、方法、手順を理解した上で、部門メンバーに割り当てられたアクセス権が、担当職務の変更、雇用・退職を含む人事異動などを反映して適切に設定されていることを定期的に確認するスキル
	6-7. 運用状況の点検	・部門の情報システムの運用状況について、点検の必要性、方法、手順を理解した上で、情報セキュリティ諸規程に沿って情報セキュリティが確保されていることを確認するスキル ・不適切と思われる事項を発見した場合に、上位者に報告・相談し、適切に対処するスキル
7. 業務の外部委託における情報セキュリティの確保	7-1. 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について、調査の必要性、方法、手順を理解した上で、情報取扱いルールなど、委託先に求める情報セキュリティ要求事項と委託先における現状との乖離を、契約担当者と協力しながら事前確認するスキル ・委託先の現状に関する事前確認の結果を踏まえて、是正の必要があれば、その対応方法、時期、対応費用の取扱いを含め、委託先との調整を、契約担当者と協力しながら実施するスキル ・委託開始時と更新時には、情報セキュリティが担保されていることを、契約担当者と協力しながら確認するスキル
	7-2. 外部委託先の管理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管理を実施することの必要性、方法、手順を理解した上で、委託業務の実施に関連する情報セキュリティ要求事項の委託先責任者への説明、契約内容との齟齬(そご)の解消を、契約担当者と協力しながら実施するスキル ・契約締結後は、不正防止・機密保護などの実施状況を、契約担当者と協力しながら確認する

大項目	小項目	目標とする技能の例
		るスキル ・ 委託業務の実施内容と契約内容に相違がある場合は、齟齬の発生理由と課題の明確化，措置の実施による是正を，契約担当者と協力しながら実施するスキル
	7-3. 外部委託の終了	・ 外部委託の終了時に必要な措置についての考え方を理解した上で，委託先に提示した資料やデータの回収又は廃棄の指示，実施結果の確認を，契約担当者と協力しながら実施するスキル ・ 資料やデータの委託先からの回収又は廃棄の状況を文書に取りまとめ，上位者に報告するスキル
8. 情報セキュリティインシデントの管理	8-1. 発見	・ 情報セキュリティインシデントを発見するための方法，手順を理解した上で，情報セキュリティ事象の中からインシデントを発見するスキル
	8-2. 初動処理	・ 情報セキュリティインシデントの初動処理の考え方，方法，手順を理解した上で，初動対応を実施するスキル 〔初動対応の対応事項〕 ✓ インシデントの発見時には，上位者や関係部署に連絡して指示を仰ぐ。 ✓ 上記の指示の下，事故の影響の大きさと範囲を想定して対応策の優先順位を検討し，被害の拡大を回避する処置を提案し実行する。 ✓ 事故に対する初動処理を記録し，状況を報告する。
	8-3. 分析及び復旧	・ 情報セキュリティインシデントの分析及び復旧の考え方，方法，手順を理解した上で，情報システム部門の協力を受けて，分析及び復旧を実施するスキル 〔分析及び復旧の対応事項〕 ✓ 事故による被害状況や被害範囲を調査し，損害と影響を評価する。 ✓ セキュリティ情報，事故に関する様々な情報，部門で収集した操作記録，アクセス記録などを基に，事故の原因を特定する。

大項目	小項目	目標とする技能の例
	8-4. 再発防止策の提案・実施	・ 情報セキュリティインシデントの再発防止の考え方を理解した上で、同様な事故が発生しないようにするための恒久的な再発防止策を検討するスキル
	8-5. 証拠の収集	・ 情報セキュリティインシデントの証拠収集の考え方、方法、手順を理解した上で、あらかじめ定めた手順に従って、証拠となり得る情報の特定、収集、取得、保持を実施するスキル
9. 情報セキュリティの意識向上	9-1. 情報セキュリティの教育・訓練	・ 情報セキュリティの意識向上の重要性、意識向上に必要な教育と訓練を理解した上で、情報セキュリティの教育・訓練を実施するスキル 〔情報セキュリティの教育・訓練の対応事項〕 ✓情報セキュリティポリシー，職務に関する組織の方針と手順，情報セキュリティの課題とその影響を理解するための教育・訓練計画を検討し，提案する。 ✓組織による部門への教育・訓練を支援する。
	9-2. 情報セキュリティに関するアドバイス	・ 情報セキュリティに関するアドバイスの方法・手順を理解した上で、情報セキュリティを維持した運用を行うため、部門のメンバーへアドバイスするスキル
	9-3. 内部不正による情報漏えいの防止	・ 内部不正による情報漏えいの防止の考え方を理解した上で、組織の定めた内部不正防止ガイドラインに従って、抑止、予防、検知のそれぞれの対策を実施するスキル
10. コンプライアンスの運用	10-1. 順守指導	・ コンプライアンスの運用（順守指導）の考え方を理解した上で、順守指導を実施するスキル 〔順守指導の対応事項〕 ✓関連法令，規格，規範及び情報セキュリティ諸規程の順守を徹底するために，組織が定めた年間教育計画に従って，対象となる法令，規格，規範及び情報セキュリティ諸規程を関係者に伝達し，周知に努める。 ✓繰り返して伝達（リカレント教育）を実施し，コンプライアンス意識の定着を目指す。
	10-2. 順守状況の評価と改善	・ コンプライアンスの運用（順守状況の評価・改善）の考え方を理解した上で、順守状況の

大項目	小項目	目標とする技能の例
		評価・改善を実施するスキル 〔順守状況の評価・改善の対応事項〕 ✓自部門又は業務監査部門が定期的に行う、法令、規格、規範及び情報セキュリティ諸規程の順守状況の点検、評価に対応する。 ✓第三者（外部を含む）による情報セキュリティ監査に協力し、必要な文書をそろえ、インタビューに応じる。 ✓監査部門からの指摘事項に関して、改善のために必要な方策を活動計画として取りまとめ、実施する。
11. 情報セキュリティマネジメントの継続的改善	11-1. 問題点整理と分析	・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）の考え方を理解した上で、問題点整理と分析を実施するスキル 〔問題点整理と分析の対応事項〕 ✓情報セキュリティ運用で起こり得る問題（例えば、利用者の反発、非現実的なルールに起因する情報セキュリティ違反者の続出など）を整理し、情報セキュリティ諸規程の関係する箇所を抽出し、現行の規定の妥当性を確認する。 ✓情報セキュリティ新技術、新たな情報システムの導入に際して、情報セキュリティ諸規程の関係する箇所を抽出し、現行の規定の妥当性を確認する。 ✓情報システム利用時の情報セキュリティが確保されていることを確認する。
	11-2. 情報セキュリティ諸規程の見直し	・情報セキュリティマネジメントの継続的改善の必要性、プロセスを理解した上で、見直しの必要性があれば、情報セキュリティ諸規程の見直しを実施するスキル
12. 情報セキュリティに関する動向・事例情報の収集と評価	12-1. 情報セキュリティに関する動向・事例情報の収集と評価	・情報セキュリティに関する動向・事例情報の収集と評価の必要性、手段を理解した上で、動向・事例情報の収集と評価を実施するスキル 〔動向・事例情報の収集と評価の対応事項〕 ✓情報セキュリティ機関や製品・サービスのベンダーから提供されるセキュリティ情報

大項目	小項目	目標とする技能の例
		を収集し、緊急性と組織としての対策の必要性を評価する。 ✓最新の脅威と事故に関する情報を情報セキュリティ機関、ベンダー、その他の企業から収集する。 ✓最新のセキュリティ情報や情報セキュリティ技術情報及び情報セキュリティ事故例を、報道、学会誌、商業誌などから収集し、分析、評価して、情報システムへの適用の必要性や費用対効果を検討する。 ✓情報セキュリティに関する法令、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の情報を収集する。

■情報セキュリティマネジメント試験
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/>