情報処理安全確保支援士試験
（レベル４）
シラバス　追補版（午前Ⅱ）

－ 午前Ⅱにおける知識の細目 －

Ver. 4.0

○○○：追加　~~○○○~~：削除

※記載順序の変更，表記の軽微な変更などは表示を省略。

IPA 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。

目　次

■ はじめに

「情報処理安全確保支援士試験」の出題範囲及びシラバス[1)]を補足するものとして，午前Ⅱの知識の幅と深さを体系的に整理，明確化した「シラバス 追補版」（午前Ⅱにおける知識の細目）を策定しましたので，公表します。

本シラバスが，試験の合格を目指す受験者の方々にとっての学習指針として，また，企業，学校の教育プロセスにおける指導指針として，有効に活用されることを期待するものです。

なお，本シラバスは，技術動向などを踏まえて，内容の追加，変更，削除など，適宜見直しを行っていきますので，あらかじめご承知おきください。

■ シラバスの構成

本シラバスは，「共通キャリア・スキルフレームワーク」の知識体系（BOK：Body of Knowledge）に沿って，「情報処理安全確保支援士試験」の午前Ⅱの出題範囲を，次の図 1 のとおり，小分類ごとに学習の目標とその具体的な内容を示したものです。

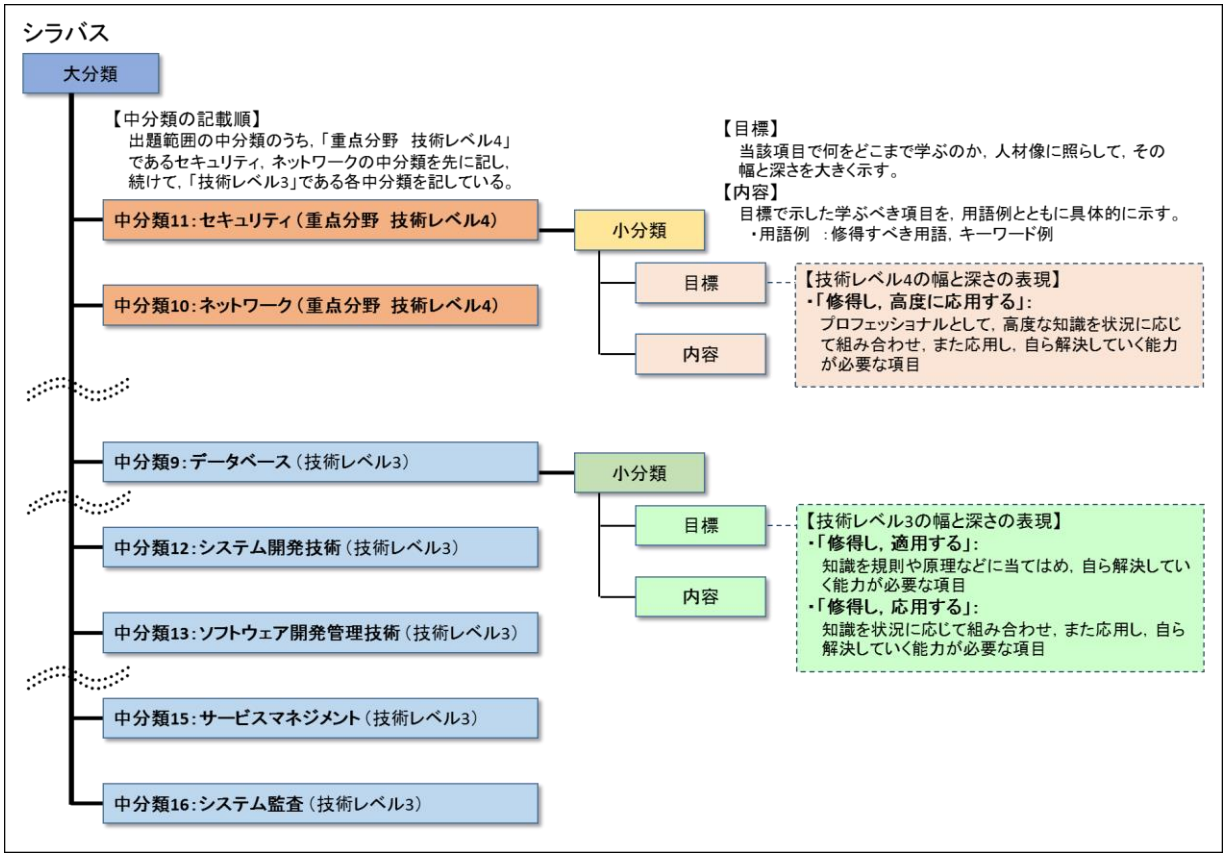

図 1　シラバスの構成

注 1)「情報処理安全確保支援士試験」シラバス　https://www.ipa.go.jp/shiken/syllabus/gaiyou.html

テクノロジ系

大分類 3：技術要素　中分類 11：セキュリティ（重点分野　技術レベル 4）

1.　情報セキュリティ

【目標】
- 情報セキュリティの目的，考え方，重要性を修得し，高度に応用する。
- 情報資産に対する脅威，脆弱性と主な攻撃手法の種類を修得し，高度に応用する。
- 情報セキュリティに関する技術の種類，仕組み，特徴，その技術を使用することで，どのような脅威を防止できるかを修得し，高度に応用する。

(1) 情報セキュリティの目的と考え方

情報の機密性（Confidentiality），完全性（Integrity），可用性（Availability）を確保，維持することによって，様々な脅威から情報システム及び情報を保護し，情報システムの信頼性を高めることを理解する。

用語例　機密性（Confidentiality），完全性（Integrity），可用性（Availability），真正性（Authenticity），責任追跡性（Accountability），否認防止（Non-Repudiation），信頼性（Reliability），多層防御，セキュリティバイデザイン（セキュアバイデザイン），プライバシーバイデザイン~~，OECD セキュリティガイドライン（情報システム及びネットワークのセキュリティのためのガイドライン）~~

(2) 情報セキュリティの重要性

社会のネットワーク化に伴い，企業にとって情報セキュリティの水準の高さが企業評価の向上につながること，情報システム関連の事故が事業の存続を脅かす可能性があることから，情報セキュリティの重要性を理解する。

用語例　情報資産，脅威，脆弱性，サイバー攻撃

(3) 脅威

① 脅威の種類

情報資産に対する様々な脅威を理解する。

用語例　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），権限昇格，誤操作，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，故意，過失，誤謬，内部不正，妨害行為，SNS の悪用，踏み台，迷惑メール（スパム），AI に対する脅威，攻撃ベクトル（Attack Vector），攻撃対象領域（アタックサーフェス：Attack Surface）

② マルウェア・不正プログラム

マルウェア・不正プログラムの種類とその振る舞いを理解する。

用語例　コンピュータウイルス，マクロウイルス，ワーム，ボット（ボットネット，遠隔操作型ウイルス（RAT：Remote Access Trojan），C&C サーバ），コネクトバック，リバースシェル，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，ステルス技術（ポリモーフィック型，メタモーフィック型ほか），ファイルレスマルウェア，エクスプロイトコード，エクスプロイトキット

(4) 脆弱性

情報システムの情報セキュリティに関する欠陥，行動規範・職務分掌の組織での未整備，従業員への不徹底などの脆弱性を理解する。

用語例　バグ，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，バッファエラー，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，認証の欠如，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

(5) 不正のメカニズム

不正行為が発生する要因，内部不正による情報セキュリティ事故・事件の発生を防止するための環境整備の考え方を理解する。

用語例　不正のトライアングル（機会，動機，正当化），状況的犯罪予防，割れ窓理論，防犯環境設計

(6) 攻撃者の種類，攻撃の動機

悪意をもった攻撃者の種類，及び攻撃者が不正・犯罪・攻撃を行う主な動機，流れ，パターンを理解する。

用語例　スクリプトキディ，ボットハーダー，内部犯，愉快犯，詐欺犯，故意犯，ダークウェブ，金銭奪取，二重脅迫（ダブルエクストーション），ハクティビズム，サイバーテロリズム，リークサイト，脅威モデリング，サイバーキルチェーン，MITRE ATT&CK，MITRE CAPEC（Common Attack Pattern Enumeration and Classification）

(7) 攻撃手法

情報システム，組織及び個人への不正な行為と手法を理解する。

用語例
- 辞書攻撃，総当たり（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，パスワードリスト攻撃（クレデンシャルスタッフィング）
- クロスサイトスクリプティング（反射型，格納型，DOM ベース），クロスサイトリクエストフォージェリ，クリックジャッキング，ドライブバイダウンロード，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，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
- 中間者（Man-in-the-middle）攻撃，MITB（Man-in-the-browser）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（スミッシングほか），セッションハイジャック，セッション ID の固定化（Session Fixation）攻撃，リプレイ攻撃，ドメインフロンティング攻撃，多要素認証疲労攻撃（Multi-Factor Authentication Fatigue Attack）
- DoS（Denial of Service：サービス妨害）攻撃，DDoS 攻撃（マルチベクトル型ほか），DRDoS 攻撃，~~電子メール爆弾，~~ICMP Flood 攻撃，Smurf 攻撃，リフレクション攻撃，DNS 水責め攻撃（ランダムサブドメイン攻撃），クリプトジャッキング
- 標的型攻撃（APT（Advanced Persistent Threat），水飲み場型攻撃，やり取り型攻撃ほか），SEO ポイズニング
- ゼロデイ攻撃，サイドチャネル攻撃（テンペスト攻撃，プローブ攻撃，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（RLO（Right-to-Left Override）の悪用，オープンリゾルバの悪用ほか），バージョンロールバック攻撃

・AI を悪用した攻撃（標的型攻撃・フィッシング・なりすましの巧妙化，マルウェア（バリアント（亜種））の生成，システムの脆弱性発見の効率化ほか），ディープフェイク，敵対的サンプル（Adversarial Examples），プロンプトインジェクション，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

・攻撃の準備（フットプリンティング，ポートスキャンほか），RaaS（Ransomware as a Service），ラテラルムーブメント

（8）情報セキュリティに関する技術

① 暗号技術

脅威を防止するために用いられる暗号技術の活用を理解する。また，暗号化の種類，代表的な暗号方式の仕組み，特徴を理解する。

用語例 CRYPTREC 暗号リスト，暗号方式（暗号化（暗号鍵），復号（復号鍵），共通鍵暗号方式（共通鍵），公開鍵暗号方式（公開鍵，秘密鍵）），RSA 暗号，楕円曲線暗号（ECDSA），鍵共有，Diffie-Hellman（DH）鍵共有方式，前方秘匿性（PFS：Perfect Forward Secrecy），ハイブリッド暗号，認証暗号（認証付き暗号，AEAD：Authenticated Encryption with Associated Data），秘密分散（電子割符），秘密計算（秘密分散方式，準同型暗号方式），量子暗号，耐量子暗号（PQC（Post Quantum Cryptography：耐量子計算機暗号）ほか），ハッシュ関数（SHA-256（SHA-2），SHA-3，一方向性，第二原像発見困難性，衝突発見困難性ほか），ブロック暗号（AES（Advanced Encryption Standard），Camellia ほか），暗号利用モード（CBC，CTR ほか），ストリーム暗号（KCipher-2 ほか），軽量暗号，鍵生成，疑似乱数，乱数生成，疑似乱数生成器（PRNG），鍵管理，ストレージ暗号化，ファイル暗号化，危殆化，ゼロ知識証明，ブロックチェーン，SSL/TLS 暗号設定ガイドライン，ワンタイムパッド，計算量（オーダー記号），暗号強度（ビットセキュリティ），情報量的安全性，計算量的安全性

② 認証技術

認証の種類，仕組み，特徴，脅威を防止するためにどのような認証技術が用いられるか，認証技術が何を証明するかを理解する。

用語例 デジタル署名（署名鍵，検証鍵），XML デジタル署名，ブラインド署名，グループ署名，トランザクション署名，タイムスタンプ（時刻認証），メッセージダイジェスト，メッセージ認証，MAC（Message Authentication Code：メッセージ認証符号），HMAC，CMAC，フィンガプリント，チャレンジレスポンス認証，リスクベース認証，コードサイニング，エンティティ認証

③ 利用者認証

利用者認証のために利用される技術の種類，仕組み，特徴を理解する。

用語例 ログイン（利用者 ID とパスワード），アクセス管理，IC カード，PIN コード，Kerberos 方式，LDAP サーバでの認証，ワンタイムパスワード，多要素認証（記憶，所有，生体），多段階認証，パスワードレス認証（FIDO UAF，FIDO U2F，FIDO2，WebAuthn，Passkeys），EMV 3-D セキュア（3D セキュア 2.0），アイデンティティ連携（OpenID Connect，SAML），IdP（Identity Provider），IDaaS（Identity as

a Service), シングルサインオン，CAPTCHA，AAA（認証，認可，アカウンティング), eKYC（electronic Know Your Customer）

④ 生体認証技術

利用者確認に利用される技術の一つである生体認証技術の種類，仕組み，特徴を理解する。

用語例 身体的特徴（静脈パターン認証，虹彩認証，顔認証，網膜認証ほか），行動的特徴（声紋認証，署名認証ほか），本人拒否率（FRR），他人受入率（FAR）

⑤ 公開鍵基盤

PKI（Public Key Infrastructure：公開鍵基盤）の仕組み，特徴，活用場面を理解する。

用語例 PKI（Public Key Infrastructure：公開鍵基盤），デジタル証明書（公開鍵証明書），ルート証明書，トラストアンカー（信頼の基点），中間 CA 証明書，サーバ証明書，クライアント証明書，コードサイニング証明書，CRL（Certificate Revocation List：証明書失効リスト），OCSP，CA（Certification Authority：認証局），VA（Validation Authority），GPKI（Government Public Key Infrastructure：政府認証基盤），BCA（Bridge Certification Authority：ブリッジ認証局），ITU-T X.509，証明書パス検証，サブジェクト，CP/CPS（Certificate Policy/Certification Practice Statement），CAA（Certificate Authority Authorization），証明書自動発行（SCEP：Simple Certificate Enrollment Protocol，ACME：Automatic Certificate Management Environment），CA/Browser Forum

2. 情報セキュリティ管理

【目標】

- 情報セキュリティ管理の考え方を修得し，高度に応用する。
- リスク分析と評価などの方法，手順を修得し，高度に応用する。
- 情報セキュリティ継続の考え方を修得し，高度に応用する。
- 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）の目的，考え方を修得し，高度に応用する。
- 情報セキュリティマネジメントシステム（ISMS）や情報セキュリティに関係するその他の基準の考え方，情報セキュリティ組織・機関の役割を修得し，高度に応用する。

(1) 情報セキュリティ管理

組織の情報セキュリティ対策を包括的かつ継続的に実施するために，情報セキュリティ管理の考え方，情報資産などの保護対象を理解する。

用語例 情報セキュリティポリシーに基づく情報の管理，情報資産，リスクマネジメント（JIS Q 31000），監視，情報セキュリティ事象，情報セキュリティインシデント，アカウント管理，利用者アクセス権の管理（need-to-know（最小権限）の原則ほか），クラウドサービスの責任共有モデル，セキュリティエコノミクス，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，サイバーハイジーン

(2) リスク分析と評価

① 情報資産の調査

情報セキュリティリスクアセスメント及び情報セキュリティリスク対応に当たり，情報資産（情報システム，データ，文書ほか）を調査して特定することを理解する。

② 情報資産の重要性による分類

機密性，完全性，可用性の側面から情報資産の重要性を検討し，情報資産を保護するために，定められた基準に基づいて情報資産を分類することを理解する。

用語例　機密性，完全性，可用性，情報資産台帳

③ リスクの種類

調査した情報資産を取り巻く脅威に対するリスクの種類を理解する。

用語例　財産損失，責任損失，純収益の喪失，人的損失，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，地政学的リスクほか），ペリル，ハザード，モラルハザード，年間予想損失額，得点法，コスト要因

④ 情報セキュリティリスクアセスメント

リスクを特定し，そのリスクの生じやすさ及び実際に生じた場合に起こり得る結果を定量的又は定性的に把握してリスクレベルを決定し，組織が定めたリスク受容基準に基づく評価を行うことを理解する。

用語例　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），リスク忌避，リスク選好，リスクの定性的分析，リスクの定量的分析

⑤ 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を考慮して，適切な情報セキュリティリスク対応の選択肢を選定し，その選択肢の実施に必要な管理策を決定することを理解する。

用語例　リスクコントロール，リスクヘッジ，リスクファイナンシング，サイバー保険，リスク回避，リスク共有（リスク移転，リスク分散），リスク保有，リスク集約，残留リスク，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

(3) 情報セキュリティ継続

組織が困難な状況（例えば，危機又は災害）に陥る事態に備えて，情報セキュリティ継続（継続した情報セキュリティの運用を確実にするためのプロセス）を組織の事業継続マネジメントシステムに組み込む必要性を理解する。

用語例　緊急事態の区分，緊急時対応計画（コンティンジェンシー計画），復旧計画，災害復旧，バックアップによる対策，被害状況の調査手法

(4) 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）

情報セキュリティ管理における情報セキュリティポリシーの目的，考え方，情報セキュリティポリシーに従った組織運営を理解する。また，組織の情報セキュリティ目的，資産の分類・管理手順，情報セキュリティ対策基準などを体系的に定めることを理解する。

用語例　情報セキュリティ方針，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ほか），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）

(5) 情報セキュリティマネジメントシステム（ISMS）

組織体における情報セキュリティ管理の水準を高め，維持し，改善していく ISMS

（Information Security Management System：情報セキュリティマネジメントシステム）の仕組みを理解する。

用語例　ISMS 適用範囲，リーダーシップ，計画，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ほか），改善（不適合及び是正処置，継続的改善），管理目的，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，検知，対応，復旧），有効性，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におけるインシデント管理

インシデント発生時から解決までの一連のフローであるインシデント管理を理解する。

用語例　インシデントハンドリング（検知／連絡受付，トリアージ，インシデントレスポンス（対応），報告／情報公開），テイクダウン

（7）情報セキュリティ組織・機関

不正アクセスによる被害受付の対応，再発防止のための提言，情報セキュリティに関する啓発活動などを行う情報セキュリティ組織・機関の役割，及び関連する制度を理解する。

用語例
- 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），~~ホワイト~~エシカルハッカー
- サイバーセキュリティ戦略本部，内閣サイバーセキュリティセンター（NISC），IPA セキュリティセンター，CRYPTREC，米国国立標準技術研究所（NIST），MITRE，FIRST（Forum of Incident Response and Security Teams），JPCERT コーディネーションセンター，J-CSIP（サイバー情報共有イニシアティブ），サイバーレスキュー隊（J-CRAT），Trusted Web 推進協議会
- 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，ソフトウェア等の脆弱性関連情報に関する届出制度，情報セキュリティサービス基準，情報セキュリティサービス審査登録制度，情報セキュリティサービス基準適合サービスリスト，ISMAP（政府情報システムのためのセキュリティ評価制度），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），NOTICE，SECURITY ACTION，情報セキュリティ早期警戒パートナーシップ，ISAC（Information Sharing and Analysis Center：セキュリティ情報共有組織）

（8）情報セキュリティに関する基準

情報セキュリティに関する基準，指針を理解する。

用語例　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，ソフトウエア製品等の脆弱性関連情報に関する取扱規程，政府機関等の情報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，IoT セキュリティガイドライン，サイバー・フィジカル・セキュリティ対策フレームワーク，金融機関等コンピュータシステムの安全対策基準・解説書，PCI DSS，サイバーセキュリティフレームワーク（CSF），NIST SP 800 シリーズ

3. セキュリティ技術評価

【目標】
- セキュリティ技術評価の目的，考え方，適用方法を修得し，高度に応用する。

(1) セキュリティ評価基準

情報資産の不正コピーや改ざんなどを防ぐセキュリティ製品の，セキュリティ水準を知るためのセキュリティ技術評価の目的，考え方，適用方法を理解する。

用語例　評価方法，セキュリティ機能要件，セキュリティ保証要件，保証レベル，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），耐タンパ性，IT 製品の調達におけるセキュリティ要件リスト

(2) ISO/IEC 15408, ISO/IEC 18045

情報技術セキュリティの観点から，情報技術に関連した製品及びシステムが適切に設計され，正しく実装されていることを評価する ISO/IEC 15408（コモンクライテリア）の適用方法を理解する。

用語例　CC（Common Criteria：コモンクライテリア, ISO/IEC 15408），~~ST（Security Target：セキュリティターゲット），~~PP（Protection Profile：プロテクションプロファイル），CEM（Common Methodology for Information Technology Security Evaluation：共通評価方法, ISO/IEC 18045），EAL（Evaluation Assurance Level：評価保証レベル），JISEC（IT セキュリティ評価及び認証制度）

(3) 制御システムのセキュリティ評価

組織の産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）を対象とした CSMS（Cyber Security Management System：サイバーセキュリティマネジメントシステム）など，制御システム及び重要インフラのセキュリティの仕組みを理解する。

用語例　CSMS 適合性評価制度，CSMS 認証基準（IEC 62443-2-1），EDSA 認証，重要インフラのサイバーセキュリティを向上させるためのフレームワーク

(4) 脆弱性評価~~の指標~~

情報システムの脆弱性に対する評価手法を理解する。

用語例　JVN（Japan Vulnerability Notes），CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム），CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子），CWE（Common Weakness Enumeration：共通脆弱性タイプ一覧），SCAP（Security Content Automation Protocol：セキュリティ設定共通化手順），CPE（Common Platform Enumeration），KEV（Known Exploited Vulnerability），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）

(5) セキュリティ情報共有技術

サイバー攻撃活動に関する情報を記述，交換するための技術仕様を理解する。

用語例　TAXII（Trusted Automated eXchange of Indicator Information：検知指標情報自動交換手順），STIX（Structured Threat Information eXpression：脅威情報構造化記述形式），TLP（Traffic Light Protocol），IoC（Indicator of Compromise），脅威インテリジェンス（OSINT など）の利用

4. 情報セキュリティ対策

【目標】
- 人的，技術的，物理的セキュリティの側面から情報セキュリティ対策を修得し，高度に応用する。

(1) 情報セキュリティ対策の種類

① 人的セキュリティ対策

人的セキュリティ対策として，人的ミス，不正行為，盗難，ソーシャルエンジニアリングなどのリスクを軽減するための教育と訓練，事件や事故に対して被害を最小限にするための対策を理解する。

用語例 組織における内部不正防止ガイドライン，情報セキュリティ啓発（教育，資料配付，メディア活用），情報セキュリティ訓練（標的型メールに関する訓練，レッドチーム演習ほか），認証情報の割当て及び管理，UBA（User Behavior Analytics），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

② 技術的セキュリティ対策

技術的セキュリティ対策として，ソフトウェア，データ，PC，サーバ，ネットワークなどに技術的対策を実施することによって，システム開発，運用業務などに被害が発生することを防ぐことを理解する。

用語例〔技術的セキュリティ対策の種類〕

クラッキング対策，不正アクセス対策，情報漏えい対策，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ほか），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，WORM（Write Once Read Many）機能，イミュータブルバックアップ），マルウェア検出手法（パターンマッチング法，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，静的解析ほか），~~出口対策，入口対策，~~秘匿化，匿名化の手法（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），アクセス制御，特権的アクセス権の管理，ログ管理，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，ソフトウェア構成分析（SCA：Software Composition Analysis），SBOM（Software Bill of Materials）を利用した脆弱性管理ほか），ネットワーク監視，アクセス権の設定，侵入検知，侵入防止，DMZ（非武装地帯），検疫ネットワーク，電子メール・Web のセキュリティ（メール無害化，メール誤送信対策，URL フィルタリング（Web フィルタリング），コンテンツフィルタリング，プロキシ認証），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，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），SED（Self Encrypting Drive：自己暗号化ドライブ），TNC（Trusted Network Communications：高信頼ネットワーク）），セキュアブート（UEFI：Unified Extensible Firmware Interface），データマスキング，暗号化消去（CE：Cryptographic Erase），クラウドサービスのセキュリティ，IoT のセキュリティ，制御システムのセキュリティ，電子透かし，デジタルフォレンジックス（証拠保全ほか），AI を使ったセキュリティ技術（AI for Security），AI そのものを守るセキュリティ技術（Security for AI），連合学習，要塞化（ハードニング），ゼロトラストアーキテクチャ，脅威ハンティング（Threat Hunting）

〔セキュリティ製品・サービス〕

マルウェア対策ソフト，EDR（Endpoint Detection and Response），XDR（Extended Detection and Response），MDR（Managed Detection and Response），DLP（Data Loss Prevention），SIEM（Security Information and Event Management），ファイアウォール，WAF（Web Application Firewall），RASP（Runtime Application Self-Protection），IDS（Intrusion Detection System：侵入検知システム），IPS（Intrusion Prevention System：侵入防止システム），UTM（Unified Threat Management：統合脅威管理），許可リスト（パスリスト），拒否リスト（ブロックリスト），シグネチャ型，アノマリ型，フォールスネガティブ，フォールスポジティブ，SSL/TLS アクセラレーター，MDM（Mobile Device Management），CASB（Cloud Access Security Broker），CSPM（Cloud Security Posture Management），SSPM（SaaS Security Posture Management），CWPP（Cloud Workload Protection Platform），SASE（Secure Access Service Edge），Web アイソレーション，SOAR（Security Orchestration，Automation and Response），MSS（Managed Security Service）

③ 物理的セキュリティ対策

物理的セキュリティ対策として，外部からの侵入，盗難，水害，落雷，地震，大気汚染，爆発，火災などから情報システムを保護し，情報システムの信頼性，可用性を確保するための対策を理解する。

用語例 RASIS（Reliability，Availability，Serviceability，Integrity，Security），RAS 技術，耐震耐火設備，UPS，多重化技術，ストレージのミラーリング，ハウジングセキュリティ，セキュリティゾーニング，監視カメラ，セキュリティゲート，アンチパスバック，インターロック，施錠管理，入退室管理，機械警備，クリアデスク・クリアスクリーン，遠隔バックアップ，USB キー，セキュリティケーブル，記憶媒体の管理，装置のセキュリティを保った処分又は再利用

5. セキュリティ実装技術

【目標】
- システムの開発，運用におけるセキュリティ対策やセキュア OS の仕組み，実装技術，効果を修得し，高度に応用する。
- ネットワーク，データベースに実装するセキュリティ対策の仕組み，実装技術，効果を修得し，高度に応用する。
- アプリケーションセキュリティの対策の仕組み，実装技術，効果を修得し，高度に応用する。

(1) セキュアプロトコル

通信データの盗聴，不正接続を防ぐセキュアプロトコルの種類と効果を理解する。

用語例 IPsec（ESP，AH，IKE），SSL/TLS，STARTTLS，SSH，HTTP over TLS（HTTPS），QUIC，WPA2，WPA3，PSK（Pre-Shared Key），Enhanced Open，SMTP over TLS

(2) 認証~~プロトコル~~・認可技術

なりすましによる不正接続，サービスの不正利用を防ぐ認証・認可技術の種類と効果を理解する。

用語例 スパム対策（ベイジアンフィルタリング，送信元ドメイン認証，SPF，DKIM，DMARC，SMTP-AUTH，OP25B，IP25B，PGP（Pretty Good Privacy），S/MIME（Secure MIME）ほか），OAuth，DNSSEC，IEEE 802.1X，EAP（Extensible Authentication Protocol），EAP-TLS，PEAP，RADIUS，Diameter

(3) OS のセキュリティ

OS のセキュリティや，セキュリティを強化した OS であるセキュア OS の仕組み，実装技術，効果を理解する。

用語例　MAC（Mandatory Access Control：強制アクセス制御），RBAC（Role-Based Access Control：ロールベースアクセス制御），最小特権，トラステッド OS

(4) ネットワークセキュリティ

ネットワークに対する不正アクセス，不正利用，サービスの妨害行為などの脅威に対する対策の仕組み，実装方法，効果を理解する。

用語例　パケットフィルタリング，ステートフルパケットフィルタリング，MAC アドレス（Media Access Control address）フィルタリング，アプリケーションゲートウェイ方式，ネットワークトラフィック分析，認証サーバ，NAT，IP マスカレード（NAPT），認証 VLAN，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），リバースプロキシ，DNSBL，DHCP スヌーピング，ネットワーク脆弱性検査，ポートスキャンによる検査

(5) データベースセキュリティ

データベースに対する不正アクセス，不正利用，破壊などの脅威への対策の仕組み，実装方法，効果を理解する。

用語例　データベース暗号化，データベースアクセス制御，データベースバックアップ，ログの取得

(6) アプリケーションセキュリティ

アプリケーションソフトウェアに対する攻撃を抑制するアプリケーションセキュリティの対策の仕組み，実装方法，効果を理解する。

用語例　Web システムのセキュリティ対策，セキュアプログラミング，脆弱性検査技術（ソースコード静的検査（SAST：Static Application Security Testing），プログラムの動的検査（DAST：Dynamic Application Security Testing），インタラクティブアプリケーションセキュリティ検査（IAST：Interactive Application Security Testing），Web アプリケーションソフトウェアの脆弱性検査，ファジングほか），コンテナセキュリティ，Same Origin Policy，CORS（Cross-Origin Resource Sharing），パスワードクラック対策（ソルト，ストレッチングほか），バッファオーバーフロー対策，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（プレースホルダほか），cookie の Secure 属性指定，HSTS（HTTP Strict Transport Security），HSTS プリロード，CSP（Content Security Policy），~~UUID（Universally Unique Identifier）の利用~~

(7) マルウェア解析

マルウェア解析環境の仕組み，マルウェア検体の解析手法を理解する。また，解析をマルウェアが回避，妨害する仕組みを理解する。

用語例　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，バイナリ解析ツール，逆アセンブル，アンパック，解析の回避（パッカー，難読化，デバッガの検知，マルウェア対策ソフトの停止ほか），PE（Portable Executable）ファイル，PE ヘッダー

(8) IoT システムの設計・開発におけるセキュリティ

IoT システム，IoT 機器の設計・開発について策定された各種の指針・ガイドラインを理解する。

用語例 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，IoT セキュリティガイドライン

大分類 3：技術要素　中分類 10：ネットワーク（重点分野　技術レベル 4）

1.　ネットワーク方式

【目標】
- LAN と WAN の仕組み，特徴，電気通信事業者が提供するサービスの種類，特徴を修得し，高度に応用する。
- 有線 LAN と無線 LAN，交換方式の仕組み，特徴を修得し，高度に応用する。
- 回線速度，データ量，転送時間の関係を修得し，高度に応用する。
- インターネット技術の必要性，特徴を修得し，高度に応用する。

(1) 通信ネットワークの役割

通信ネットワークが果たす役割と効果，ネットワーク障害が発生した場合の社会的影響の大きさを理解する。

用語例　ネットワーク社会，ICT（Information and Communication Technology：情報通信技術）

(2) ネットワークの種類と特徴

LAN と WAN の仕組み，特徴，構成要素，運用費用を理解する。また，WAN を構成する場合に利用する電気通信事業者から提供されているサービスの種類と特徴を理解する。

用語例　インターネットサービスプロバイダ（ISP），従量制，月額固定料金，IDF（Intermediate Distribution Frame），MDF（Main Distribution Frame），パケット交換網，回線交換網，センサーネットワーク

(3) 有線 LAN

有線 LAN の仕組み，構成要素，特徴を理解する。

用語例　同軸ケーブル，より対線，光ファイバケーブル

(4) 無線 LAN

無線 LAN の仕組み，構成要素，特徴を理解する。

用語例　電波，赤外線，無線 LAN アクセスポイント，インフラストラクチャモード，アドホックモード，SSID，BSSID，隠れ端末問題，さらし端末問題

(5) 交換方式

回線交換とパケット交換の仕組み，特徴を理解する。

用語例　パケット，VoIP（Voice over Internet Protocol），SIP

(6) 回線に関する計算

回線速度，データ量，転送時間の関係を理解し，与えられた回線速度，データ量，回線利用率からの転送時間の算出方法を理解する。また，発生するトラフィック量から必要な回線速度を算出する方法を理解する。

用語例　転送速度（伝送速度），bps（bit per second：ビット／秒），回線容量，ビット誤り率，トラフィック理論，呼量，呼損率，アーランB式（アーランの損失式），アーラン，トラフィック設計，性能評価

(7) インターネット技術

ノードには，世界で一意となる IP アドレスが割り当てられることによって，相互通信が可能となっていること，アドレスを構成するネットワークアドレスとホストアドレスの役割，

IP パケットのルーティングの動作，IPv6 の必要性と特徴を理解する。

用語例　IPv4，IPv6，アドレスクラス，グローバル IP アドレス，プライベート IP アドレス，IP マスカレード，NAT，オーバーレイネットワーク，DNS，ドメイン，FQDN，TLD，QoS（Quality of Service：サービス品質），ユビキタス，パーベイシブ，セキュリティプロトコル，ファイアウォール，RADIUS

2.　データ通信と制御

【目標】
- ネットワークアーキテクチャの考え方，重要性，効果を修得し，高度に応用する。
- 伝送方式と回線の種類，特徴を修得し，高度に応用する。
- ネットワーク接続装置の種類，特徴を修得し，高度に応用する。
- ネットワークにおける代表的な制御機能の仕組み，特徴を修得し，高度に応用する。

(1) ネットワークアーキテクチャ

① ネットワークトポロジ

代表的なネットワーク構成の種類，特徴，端末，制御機器がどのような形態で接続されるかや，ネットワーク構成図の作成方法を理解する。また，各構成における信頼性と障害時の動作の違いを理解する。

用語例　ポイントツーポイント（2 地点間接続），ツリー型，バス型，スター型，リング型

② OSI 基本参照モデル

ISO が策定した 7 層からなるネットワークアーキテクチャである OSI 基本参照モデルの各層の機能，各層の間の関係を理解する。

用語例　物理層，データリンク層，ネットワーク層，トランスポート層，セション層，プレゼンテーション層，アプリケーション層

③ 標準化の実例

WAN における通信プロトコルの標準化が ITU-T において策定されていることを理解する。

用語例　X シリーズ，V シリーズ，I シリーズ

(2) 伝送方式と回線

ネットワークで使用される回線の種類，通信方式，交換方式の種類と特徴を理解する。

用語例　単方向，半二重，全二重，WDM（Wavelength Division Multiplexing：波長分割多重），TDMA，CDMA，OFDMA，リンクアグリゲーション，回線交換，パケット交換，公衆回線，専用線，電力線通信（PLC）

(3) ネットワーク接続

LAN 内接続，LAN 間接続，LAN-WAN 接続の装置の種類，特徴，各装置の機能が，OSI 基本参照モデルのどの層に対応するかを理解する。

用語例　リピータ，ハブ，カスケード接続，Automatic MDI/MDI-X，スイッチングハブ，ルータ，回線接続装置，レイヤー2（L2）スイッチ，レイヤー3（L3）スイッチ，ブリッジ，ゲートウェイ，プロキシサーバ，リバースプロキシサーバ，ロードバランサー，スパニングツリー，VRRP

(4) 伝送制御

送受信者の間でデータを確実に伝送するための制御機能である伝送制御の仕組み，特徴を

理解する。

用語例　データリンク制御，ルーティング制御，フロー制御，輻輳制御，ベーシック手順，コンテンション方式，ポーリング／セレクティング方式，HDLC，マルチリンク手順，相手固定，交換方式，コネクション方式，コネクションレス方式，パリティチェック，CRC，ハミング符号，ビット誤り率，SYN 同期，フラグ同期，フレーム同期

(5) メディアアクセス制御

データの送受信方法や誤り検出方法などを規定する MAC（Media Access Control：メディアアクセス制御）の仕組みと特徴を理解する。また，アクセス制御の目的，アクセス制御手法の代表的な種類と仕組みを理解する。

用語例　CSMA/CD，CSMA/CA，トークンパッシング，衝突

3. 通信プロトコル

【目標】
- 代表的なプロトコルである TCP/IP が OSI 基本参照モデルのどの階層の機能を実現しているか，その役割は何かを修得し，高度に応用する。

(1) プロトコルとインタフェース

① TCP/IP

TCP/IP を OSI 基本参照モデルの 7 階層と対比させながら，各層が果たす役割，提供しているインタフェースを理解する。また，代表的なサービスのポート番号（ウェルノウンポート）などを理解する。

用語例　パケット，ヘッダー

② データリンク層のプロトコル

ARP など，TCP/IP ネットワークにおいて使用されるデータリンク層レベルのプロトコルの役割，機能を理解する。

用語例　RARP（Reverse Address Resolution Protocol：逆アドレス解決プロトコル），L2TP，PPP，PPPoE（Point to Point Protocol over Ethernet），IPoE（IP over Ethernet），VLAN，IEEE 802.1Q，プロキシ ARP

③ ネットワーク層のプロトコル

IP の役割，機能を理解する。

用語例　IP アドレス，サブネットアドレス，サブネットマスク，物理アドレス，ルーティング，ユニキャスト，ブロードキャスト，マルチキャスト，ICMP（Internet Control Message Protocol），ICMPv6，IGMP，CIDR（Classless Inter Domain Routing），IPv6，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，6to4）

④ トランスポート層のプロトコル

TCP と UDP の役割，機能を理解する。

用語例　ポート番号，ウィンドウ制御，確認応答，サブミッションポート

⑤ アプリケーション層のプロトコル

HTTP，SMTP，POP，FTP，DNS などの役割，機能を理解する。

用語例　TELNET，DHCP，IMAP，NTP，SOAP，RTP，HTTP/2，HTTP/3

⑥ ルーティングプロトコル
ルーティングプロトコルの役割，機能を理解する。

用語例　OSPF，RIP，RIPng，BGP，MPLS

⑦ LAN と WAN のインタフェース
イーサネット，無線 LAN，ISDN，PRI（Primary Rate Interface：1 次群インタフェース）など，LAN と WAN で使用される代表的なインタフェースの役割，機能を理解する。

用語例　10BASE-T，100BASE-TX，1000BASE-T，10GBASE-T，IEEE 802.11a/b/g/n/ac/ad/ax，Wi-Fi 4/5/6/6E，メッシュ Wi-Fi

⑧ CORBA
CORBA はプログラム言語やネットワークプロトコルに依存せず，異機種分散環境におけるシステム統合の基盤の考え方として利用できることを理解する。

用語例　分散オブジェクト技術，クライアント，オブジェクトサービス，リクエストアプリケーションオブジェクト

4.　ネットワーク管理

【目標】
- ネットワーク運用管理の管理項目，管理方法を修得し，高度に応用する。
- ネットワーク管理のためのツール，プロトコルの機能，仕組み，利用法を修得し，高度に応用する。

(1) ネットワーク運用管理

① 構成管理
構成情報を維持し，変更を記録する構成管理の管理方法を理解する。

用語例　ネットワーク構成，バージョン

② 障害管理
障害の検出，分析，対応を行う障害管理の管理方法を理解する。

用語例　情報収集，障害の切分け，障害原因の特定，復旧措置，記録，死活監視

③ 性能管理
トラフィック量と転送時間の関係の分析などによるネットワークの性能の管理方法，並びにネットワーク及びサーバの負荷分散手法を理解する。

用語例　トラフィック監視，負荷分散（DNS ラウンドロビン，DNS ゾーン転送ほか）

(2) ネットワーク運用管理ツール
ネットワークの運用管理に利用されているツールやユーティリティの機能，仕組みを理解する。

用語例　ping，ifconfig，arp，netstat，nslookup，ip，ss，dig，traceroute，syslog，IPFIX（Internet Protocol Flow Information Export），パケットアナライザー（tcpdump，Wireshark ほか）

(3) SNMP

ネットワークを構成する機器を集中管理するためのプロトコルである SNMP と MIB (Management Information Base：管理情報ベース) を使用したトラフィック解析方法を理解する。

用語例　SNMP エージェント，SNMP 管理ステーション，MIB (Management Information Base：管理情報ベース)，get 要求，put 要求，trap 要求

(4) 仮想ネットワーク

ネットワークの仮想化の仕組み，特徴，構成要素を理解する。

用語例　トンネリング，SDN (Software-Defined Networking)，SD-WAN (Software Defined WAN)，OpenFlow，NFV (Network Functions Virtualization)，VXLAN

5. ネットワーク応用

【目標】
- インターネットで利用されている電子メールや Web などの仕組み，特徴，機能を修得し，高度に応用する。
- イントラネットとエクストラネットの仕組み，特徴を修得し，高度に応用する。
- ネットワーク OS の仕組み，特徴，機能を修得し，高度に応用する。
- 代表的な通信サービスの種類，特徴，機能，留意事項を修得し，高度に応用する。
- モバイルシステムの仕組み，特徴を修得し，高度に応用する。

(1) インターネット

① 電子メール

電子メールシステムはメールサーバとメールクライアントで構成されており，送信したメールはメールサーバからメールサーバへリレー方式で配送される仕組みであること，電子メールシステムの特徴，機能を理解する。

用語例　SMTP，POP3，IMAP4，MIME，base64，HTML メール (MHTML)，Web メール

② Web

WWW はインターネット上で提供されるハイパーテキストのシステムであり，Web サーバとクライアント (Web ブラウザ) を利用してアクセスすること，Web ページは HTML，XML などのマークアップ言語で記述され，ハイパーリンクで簡単に別のページを参照できることや，Web アプリケーションシステムの仕組み，特徴，機能を理解する。

用語例　HTTP，HTTP over TLS (HTTPS)，CGI，cookie，URL，セッション ID，REST，WebDAV，QUIC (Quick UDP Internet Connection)

③ ファイル転送

FTP サーバとクライアントの仕組みや Web への組込み方式の仕組み，特徴，機能を理解する。

用語例　アップロード，ダウンロード，アクティブモード，パッシブモード，TFTP (Trivial File Transfer Protocol)

④ 検索エンジン

Web の環境で利用される代表的な検索エンジンの仕組み，特徴を理解する。

用語例　全文検索型，~~ディレクトリ型，~~ロボット型

(2) イントラネット

インターネットの技術を企業内ネットワークの構築に応用したイントラネットの仕組み，特徴，機能を理解する。

用語例　VPN，相手固定接続，プライベート IP アドレス，NAT

(3) エクストラネット

企業のイントラネットを相互接続したエクストラネットの仕組み，特徴，機能を理解する。

用語例　EC（Electronic Commerce：電子商取引），EDI

(4) ネットワーク OS

ネットワーク管理や通信サービスの提供を専門に行うソフトウェアであるネットワーク OS の仕組み，特徴，機能を理解する。

用語例　ピアツーピア形式，クライアントサーバ形式

(5) 通信サービス

代表的な通信サービスの種類，特徴，機能，利用条件，サービス選択上の留意事項を理解する。

用語例　専用線サービス，回線交換サービス，パケット交換サービス，IP 電話，IP セントレックス，IP-PBX，xDSL，FTTH，衛星通信サービス，国際通信サービス，広域 Ethernet，IP-VPN，ベストエフォート，マルチホーミング

(6) モバイルシステム

① モバイル通信サービス

モバイル通信サービスの種類，特徴，サービス選択上の留意事項を理解する。

用語例　移動体通信事業者，仮想移動体通信事業者（MVNO：Mobile Virtual Network Operator），LTE，VoLTE，5G（第 5 世代移動通信システム），ローカル 5G，SA（Stand Alone）方式，NSA（Non-Stand Alone）方式，ネットワークスライシング，キャリアアグリゲーション，SIM カード，eSIM（embedded SIM），IMEI，ISM バンド，サブ GHz 帯

② モバイルシステム構成要素

モバイルシステムの構成要素，特徴，機能を理解する。

用語例　基地局，フェムトセル，携帯端末（携帯電話，スマートフォン，タブレット端末ほか），テザリング，テレマティクス

③ モバイル通信技術

無線 LAN も含め，無線通信で用いられる基盤技術の特徴を理解する。

用語例　ハンドオーバー，ローミング，MIMO，モバイル通信の省電力化技術（間欠受信，eDRX，ビームフォーミング，ドーマント（プリザベーション），PSM ほか）

④ IoT システムのネットワーク

IoT システムに適したネットワークの特徴，適合する技術を理解する。

用語例　LPWA（LTE-M，NB-IoT，Wi-SUN，LoRaWAN），IEEE 802.11ah（Wi-Fi HaLow），軽量プロトコル（CoAP，MQTT），NB-IoT（Narrow Band-IoT），カテゴリ 0，カテゴリ M，IoT エリアネットワーク

（補足）
「技術レベル 3」の中分類の知識の幅と深さは応用情報技術者試験（AP）と同等です。
以下は AP シラバスの内容をそのまま掲載しています。

大分類 3：技術要素　中分類 9：データベース（技術レベル 3）

1.　データベース方式

【目標】
- データベースの種類，特徴，データベースのモデル，3 層スキーマの考え方を修得し，応用する。
- データベース管理システムの目的，機能を修得し，応用する。

(1) データベース

① データベースの種類と特徴
代表的なデータベースの種類，データ構造の表現，レコード間の関連付けの方法など種類ごとの特徴，与えられた要件に応じて最適なデータベースを選択し，設計に活用することを理解する。

用語例　RDB（Relational Database：関係データベース），構造型データベース，HDB（Hierarchical Database：階層型データベース），NDB（Network Database：網型データベース），~~CODASYL（Conference on Data Systems Languages）型データベース，~~OODB（Object Oriented Database：オブジェクト指向データベース），~~オブジェクト関係データベース，ハイパーテキストデータベース，マルチメディアデータベース，~~XML データベース，分散データベース，ドキュメント指向データベース，列指向データベース，グラフデータベース，キーバリュー型データベース，インメモリデータベース

② データベースの 3 層スキーマアーキテクチャ（3 層スキーマ構造）
データベースでは，システムの利用者やプログラムから見たデータの定義（外部スキーマ），論理的なデータ構造（概念スキーマ），物理的なデータ構造（内部スキーマ）の 3 層を区別することでデータの独立性を高めていること，各スキーマの表現方法を理解する。

用語例　概念スキーマ，外部スキーマ（副スキーマ），内部スキーマ（記憶スキーマ）

③ データベースのデータモデル
データベースの論理的なデータ構造を表現するためのデータモデルの種類，特徴，利点，表現できる内容，特徴を理解する。

用語例　論理データモデル，物理データモデル，関係モデル，階層モデル，ネットワークモデル（網モデル），グラフ型のデータモデル（プロパティグラフ，トリプルストア）

④ 関係モデル
関係モデルにおいて，データがどのように表されるのか，表の構成，考え方，複数の表の関係付けを理解する。また，与えられた要件に応じて，規定の表記法を使用してデータ構造を表現することを理解する。

用語例　関係（リレーション），タプル（行，組），属性（列，フィールド），実現値，定義域（ドメイン），関係スキーマ

(2) データベース管理システム

① データベース管理システムの目的
DBMS の目的，代表的な機能とともに，DBMS にも階層型，網型，関係型があること，DBMS のマネジメント機能をデータベース開発や保守に利用することを理解する。

用語例　データベース定義機能，データベース操作機能，データベース制御機能，保全機能，データ機密保護機能

② 同時実行制御（排他制御）
複数のトランザクションが一つのデータベースに同時にアクセスするときに必要な制御方法を理解する。

用語例　トランザクション，ロック，デッドロック，ACID 特性，データ辞書

③ 障害回復
データベースに障害が発生した場合の障害回復機能と回復手順を理解する。

④ データセキュリティ
データを共有する際に重要となるセキュリティ確保のための方法を理解する。

⑤ データベース管理システムの種類と特徴
代表的なデータベース管理システムの種類と特徴，関係データベース管理システムと NoSQL のデータベース管理システムとの違い，取り扱う上での留意事項，関連する機能を理解する。

用語例　関係データベース（MySQL，PostgreSQL，SQLite ほか），NoSQL データベース（Apache Cassandra，Apache CouchDB，MongoDB，Redis，Neo4j ほか）

2. データベース設計

【目標】
- データの分析の考え方を修得し，応用する。
- データベースの設計の考え方，手順，手法を修得し，応用する。
- データの正規化の目的，手順を修得し，応用する。
- データベース作成の手順，評価方法を修得し，応用する。
- ~~オブジェクト指向データベースの考え方を修得し，応用する。~~

(1) データ分析

対象業務にとって必要なデータは何か，各データがどのような意味と関連をもっているかなどの分析と整理，異音同義語，同音異義語の発生を抑えるデータ項目の標準化など，データ分析を行う際の考え方を理解する。また，データモデルの作成手法であるトップダウンアプローチとボトムアップアプローチを理解する。

用語例　データ重複の排除，メタデータ，データディクショナリ

(2) データベースの設計

① データベース開発工程
開発計画立案，外部設計，内部設計，プログラム作成，テスト，移行に至るまでのデータベース開発の工程と手順，手法を理解する。

用語例　システム分析，要求定義，企業データモデル，データモデル，概念データモデル，

論理データモデル，物理データモデル，副次索引，分割法，DOA（Data Oriented Approach：データ中心アプローチ）

② データベースの概念設計

概念設計では，要求定義で定義されたデータ項目と，システム機能設計の際に発生したデータ項目をまとめ，データ項目全体を設計することを理解する。また，DBMS に依存しないデータの関連を表現する手法として，E-R 図や UML を使用した構成要素，属性，関連の表し方，特徴，カーディナリティ（1 対 1，1 対多，多対多）などを理解する。

用語例　概念データモデル，バックマン線図，エンティティ，属性，リレーションシップ

③ データベースの論理設計

データの重複や矛盾が発生しないテーブル（表）設計の考え方，主キー，外部キーなどの概念，一貫性制約（一意性制約，参照制約，検査制約など）の制約を理解する。また，ビューの機能と定義を理解する。

用語例　論理データモデル，配置モード，親子集合順序，親子集合，索引，フィールド（項目），レコード，ファイル，NULL，一意性制約，サロゲートキー

(3) データの正規化

正規化の目的と手順，第 1 正規形，第 2 正規形，第 3 正規形などを理解する。また，正規化の考え方に従った，具体的な設計案に対して更新容易性や性能面などから評価し，最適な設計を行うことを理解する。

用語例　完全関数従属，部分関数従属，推移関数従属

(4) データベースのパフォーマンス設計

処理の高速化のためにあえて正規化を行わず，表の結合にかかる時間を短縮するなど，パフォーマンスを考慮したデータベース設計の考え方を理解する。

用語例　非正規化

(5) データベースの物理設計

データベースの物理設計では，アクセス効率，記憶効率の側面からデータベースの最適化を図ることを理解する。また，磁気ディスク上に記憶される形式や論理データ構造の物理データ構造へのマッピングなど，データベースの物理的構造を設計する際の留意事項を理解する。

用語例　ディスク容量見積り，論理データ構造のマッピング，ファイル編成，最適ブロック設計，物理入出力，性能評価，コンプレッション，デコンプレッション，性能改善ポイント，インメモリデータベース

(6) データベースの作成手順

データベース環境の準備，入力データの準備，データベースの定義，データの登録，データベースの検証などの一連のデータベースの作成手順を理解する。

用語例　データベース定義情報，レコード形式，親子関係，キー順，存在制約，インバーテッドファイル

(7) データベースの評価・運用

データベースの性能評価方法を理解し，評価結果によってはチューニングや再編成などの対応策が必要であることを理解する。

用語例　データベースの運用・保守

3. データ操作

【目標】
- 関係データベースのデータの操作を修得し，応用する。
- データベース言語の種類，SQL 文を修得し，応用する。

(1) データベースの操作

関係データベースのデータの操作として，集合演算（和，差，積（共通）），関係演算（選択，射影，結合，商，直積）などを理解する。

用語例　関係代数

(2) データベース言語

① データベース言語の種類

データベース言語は，DDL（Data Definition Language：データ定義言語）と DML（Data Manipulation Language：データ操作言語）などに大別されること，また，これらには SQL を単独で使用する独立言語方式と，他のプログラム言語から使用する親言語方式があることを理解する。

用語例　会話型SQL，埋込みSQL，モジュール言語，コマンド方式，フォーム，問合せ（クエリ）

② データベース言語（SQL）

(a) データ定義言語

スキーマ，テーブル，ビュー，処理権限を定義する SQL 文を理解する。また，データ型，列制約，表制約の定義方法，ビューの更新（更新可能なビューと更新不可能なビュー）を理解する。

用語例　実表，ビュー表，文字型，数値型，日付型，一意性制約，参照制約，検査制約，非 NULL 制約，アクセス権, CASCADE, TRIGGER

(b) データ操作言語（SELECT 文）

要求されるデータを選択するために，SELECT 文による問合せの方法，条件を指定した特定行や列の選択，表の結合，BETWEEN や IN などの述語指定，集合関数，グループ化，ウィンドウ，並べ替えなどを理解する。

用語例　集約関数，パターン文字列，相関名，副問合せ，相関副問合せ, ウィンドウ関数

(c) その他のデータ操作言語

INSERT 文，UPDATE 文，DELETE 文, GRANT 文などの SQL 文を理解する。

(d) 埋込み SQL

カーソル操作，非カーソル操作，親言語との接続など，埋込み SQL によるデータ操作の仕組み，利点，利用法を理解する。また，カーソル操作において，カーソルの宣言，操作の開始，終了，読込みを行うなどの SQL 文を理解する。

用語例　カーソル

4. トランザクション処理

【目標】
- データベースの同時実行制御（排他制御），障害回復の考え方，仕組みを修得し，応用する。
- トランザクション管理，アクセス効率向上のための考え方を修得し，応用する。
- データに対するアクセス制御の必要性，代表的なアクセス権限を修得し，応用する。

(1) 同時実行制御（排他制御）

データの整合性を保つために，複数のトランザクションが同時にデータベースのデータを更新することが起こらないようにする同時実行制御（排他制御）の考え方を理解する。また，ロック方式，セマフォ方式，コミットメント制御，多版同時実行制御（MVCC）の仕組みを理解する。

用語例　専有ロック，共有ロック，ロック粒度，2 相ロッキングプロトコル，デッドロック，Wait-Die 方式，Wound-Wait 方式，~~1 相コミットメント，~~2 相コミットメント，ダーティリード，ノンリピータブルリード，ファントムリード，隔離性水準，補償トランザクション，TCC パターン，Saga パターン，スキュー（skew）

(2) 障害回復

障害に備えたバックアップの方式，世代管理の考え方，障害発生直前の状態まで回復を図るリカバリ処理の仕組み，データベースの利用環境の準備，アクセス効率の向上のための再編成などの考え方，仕組みを理解する。

用語例　フルバックアップ，差分バックアップ，増分バックアップ，ダンプファイル，リストア，データディレクトリ，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），シャドウページ法，ウォームスタート，コールドスタート

(3) トランザクション管理

データベースは複数の利用者が同時にアクセスするので，トランザクション処理には ACID 特性が求められること，四つの特性の意味を理解する。

(4) データベースの性能向上

データベースへのアクセス効率向上のために，インデックスを有効に活用する考え方を理解する。

用語例　インデックス数，負荷，ユニークインデックス，クラスタ化インデックス，B-tree インデックス，ビットマップインデックス，ハッシュインデックス，カバリングインデックス，転置インデックス

(5) データへのアクセス制御

利用者ごとに，データに対するアクセス制御を行う必要性があること，アクセス権限としてはデータベースに接続する権限，データを検索する権限，データを新規登録する権限，データを更新する権限などがあること，SQL による権限の定義と変更の方法を理解する。

用語例　参照権限，挿入権限，削除権限

5. データベース応用

【目標】
- データベースの応用対象，応用方法を修得し，応用する。
- 分散データベースの特徴，機能を修得し，応用する。
- データ資源管理の仕組みとして，リポジトリ，データディクショナリを修得し，応用する。

(1) データベースの応用

データウェアハウス，データマート，OLAP（Online Analytical Processing），データマイニングなど，データを分析して有効活用する技術の特徴，これらの技術が企業会計システム，在庫管理システムなどで使われていること，その応用方法を理解する。

用語例 OLTP（Online Transaction Processing），ETL（Extract/Transform/Load），ELT（Extract/Load/Transform），データクレンジング，ビッグデータ，文書管理システム，営業支援システム

(2) 分散データベース

複数のサイトに配置された分散データベースの特徴，利点，取り扱う上での留意事項，サイト間でのデータ同期の仕組み，関連する機能，集中型データベースとの違いを理解する。

用語例 透過性，クライアントキャッシュ，コミットメント制御，2 相コミットメント，コミットシーケンス，同時実行制御，レプリケーション，水平分散，垂直分散，表の分散（水平，垂直），分散問合せ，結合演算，分散トランザクション，スプリットブレイン，OSI-RDA（Open Systems Interconnection-Remote Database Access：開放型システム間相互接続-遠隔データベースアクセス）プロトコル，ブロックチェーンにおけるデータベース関連技術（コンセンサスアルゴリズム，ファイナリティほか），分散処理フレームワーク（Apache Hadoop，Apache Spark ほか），CAP 定理，BASE 特性，結果整合性，シャーディング

(3) データ資源管理

データの属性，意味内容，格納場所など，データを管理するための情報（メタデータ）を収集，管理したデータディクショナリや，ソフトウェア開発と保守における様々な情報を一元的に管理するリポジトリを理解する。

用語例 IRDS（Information Resource Dictionary System：情報資源辞書システム），分散ファイルシステム（HDFS（Hadoop Distributed File System），Ceph，GlusterFS ほか），ファクトデータベース，リファレンスデータベース，データベースサービス，構造化データ，半構造化データ，非構造化データ，ストリーミングデータ，データレイク，大規模データセットのクエリエンジン（Apache Hive，Presto ほか）

大分類 4：開発技術　中分類 12：システム開発技術（技術レベル 3）

1.　システム要件定義・ソフトウェア要件定義

【目標】
- システム及び／又はソフトウェア要件定義の考え方，手順，手法，留意事項を修得し，適用する。

(1) システム要件定義のタスク

システム要件定義では，システムの境界の定義，システム要件の定義，システム要件の評価，システム要件の共同レビューを実施することを理解する。

(2) システムの境界の定義

① システムの境界の定義の目的

利害関係者要件として定義された，利用の状況及び運用シナリオに基づいて機能的な境界を定義することを理解する。

用語例　利用の状況，運用シナリオ，API，GUI，インタフェースファイル，サービス

② システム化の目標と対象範囲

システム化の目標，対象範囲（対象業務，対象部署）をまとめることを理解する。

(3) システム要件の定義

① システムの機能及び能力の定義

システムの機能要件，性能要件をまとめることを理解する。

用語例　システム機能仕様，レスポンスタイム，スループット

② 業務・組織及び利用者の要件

利用者の業務処理手順，入出力情報要件，操作要件（システム操作イメージ）の定義など，業務，組織，利用者からの要求事項をシステム開発の項目に対応させ，明確に定義することを理解する。また，開発対象システムの具体的な利用法を調査，分析して要件を抽出し，5W2H（Why，When，Where，Who，What，How，How much）の観点から明確に文書化することを理解する。

用語例　性能要件，データベース要件，テスト要件，セキュリティ要件，移行要件，運用要件，運用手順，運用形態，保守要件，可用性，障害対応，教育，訓練，費用，保守の形態，保守のタイミング，CRUD マトリクス

③ その他の要件

システム構成要件，設計及び実装の制約条件，UX（User Experience）を考慮した要件の定義，適格性確認要件（開発するシステムが利用可能な品質であることを確認する基準）の定義，開発環境の検討などを行うことを理解する。

用語例　実行環境要件，周辺インタフェース要件，品質要件，機能要件，非機能要件，達成する遂行能力・性能・運用時の実績に対する要件（パフォーマンス要件），UX デザイン，イネーブリングシステム

(4) システム要件の評価及びレビュー

システム要件を評価する際の基準を理解する。また，システム要件定義書の作成後，システムの取得者及び供給者が共同でレビューを行うことを理解する。

用語例　双方向の追跡可能性（双方向のトレーサビリティ），一貫性，テスト可能性，システム設計の実現可能性，運用及び保守の実現可能性，レビュー参加者，レビュー方式，アシュアランスケース

(5) ソフトウェア要件定義のタスク

ソフトウェア要件定義では，ソフトウェアの境界の定義，ソフトウェア要件の定義，ソフトウェア要件の評価，ソフトウェア要件の共同レビューを実施することを理解する。

(6) ソフトウェアの境界及び要件の定義

① ソフトウェアの境界及び要件の定義の目的

ソフトウェア要件定義では，業務モデル，論理データモデルを作成して，システムを構成するソフトウェアの境界，ソフトウェアに求められる機能，能力，インタフェースなどを決定し，ソフトウェア要件を定めることを理解する。また，要件定義のための業務分析には，DFD，E-R 図，UML などの分析，表現方法を使用することを理解する。

用語例　要件の属性（根拠，優先順位，ソフトウェア要素・テストケース・情報項目への追跡可能性（トレーサビリティ），検証手法），トレーサビリティマトリクス，UX デザイン，使用性（usability）

② ソフトウェアの機能仕様とそのインタフェースの仕様の識別

ソフトウェアの機能仕様とそのインタフェースの仕様を識別する一連の活動と留意事項を理解する。

用語例　ユースケース，ユーザーストーリー，シナリオ，DFD，E-R 図，UML，運用の状態又はモード，サブシステム分割，サブシステム機能仕様定義，サブシステムインタフェース定義，サブシステム関連図，サービスの定義，実装制約条件，品質特性，IoT

③ 業務モデルとデータモデルの識別

業務フローやサブシステム間の関係から業務モデルとデータモデルを作成する一連の活動と留意事項，データモデルの種類と各々の特徴を理解する。

用語例　論理モデル，物理モデル，業務モデリング，IoT，画面設計，帳票設計，伝票設計，データモデリング，システム業務フロー，データ要素，データ構造，データ形式，データベース又はデータ維持の要件，ユーザーインタフェース，利用者用文書類，利用者の教育訓練

④ セキュリティ要件の識別

企業の情報セキュリティポリシーに即したセキュリティ機能に関する設計原則及び設計特性を選定して優先順位をつける活動と留意事項を理解する。

用語例　情報セキュリティ方針，セキュリティ要件，セキュリティ実現方式，安全性対策，信頼性対策，設計原則（最小限の原則，多層防御，システムサービスへのアクセス制限，システムへの攻撃にさらされる境界面の最小化及び防御），設計特性（アベイラビリティ，障害許容性（耐故障性），復元性（resilience））

⑤ 保守性の考慮

運用開始後の新機能の追加及び既存機能の変更に必要な工数を抑え，機敏性を獲得するための設計上の配慮の必要性を理解する。

用語例　無矛盾性，自己記述性，構造性，簡潔性，拡張性，移植性

(7) ソフトウェア要件の評価及びレビュー

決定したソフトウェア要件がシステム要件に合致しているか，実現可能かなど，ソフトウェア要件を評価する際の基準，ソフトウェア要件定義書の作成後，システムの取得者及び供給者が共同でレビューを行うことを理解する。

用語例　双方向の追跡可能性（双方向のトレーサビリティ），外部一貫性，内部一貫性，テスト可能性，ソフトウェアシステムの実現可能性，トレーサビリティマトリクス，運用及び保守の実現可能性，レビュー参加者，レビュー方式，アシュアランスケース

(8) 業務分析や要件定義に用いられる手法

① ヒアリング

ソフトウェアに何が要求されているかを明らかにし，理解するためには，利用者からのヒアリングが有効であること，ヒアリング実施の手順，考え方を理解する。

用語例　ヒアリング計画，ヒアリング議事録

② ユースケース

ユースケースは，一つの目標を達成するための利用者とシステムのやり取りを定義するために用いること，その特徴，目的，ユースケースを描く方法を理解する。

用語例　アクター，振舞い，ユースケース図

③ モックアップ及びプロトタイプ

ソフトウェア要求分析において，外部仕様の有効性，仕様の漏れ，実現可能性などの評価を行い，手戻りを防ぐためにモックアップ及びプロトタイプを作成することがあること，モックアップ及びプロトタイピングの特徴を理解する。

用語例　プロトタイプ版評価，垂直型プロトタイプ，水平型プロトタイプ

④ DFD

業務プロセスをデータの流れに着目して表現する場合に，DFD を使用することを理解する。

用語例　データストア，データフロー，プロセス，源泉と吸収，外部実体，コンテキストダイアグラム，ミニスペック，段階的詳細化，構造化分析法，アクティビティ

⑤ E-R 図

業務で扱う情報を抽象化し，実体（エンティティ）と実体間の関連（リレーションシップ）を表現する場合に，E-R 図を使用することを理解する。

用語例　実体，関連，データ中心設計

⑥ UML

オブジェクト指向設計の標準化された表記法として UML があること，UML で用いる図式の種類，特徴，UML を用いてシステムの仕組みを表現する方法を理解する。

用語例　クラス図，操作，属性，ロール名，パッケージ図，アクティビティ図，ユースケース図，ステートマシン図，シーケンス図，コミュニケーション図，イベントフロー分析，バックトラック，コントロールフロー，分析と設計の役割分担，エージェント指向，モデル，フレームワーク

⑦ ユーザーストーリー

ソフトウェア要件を記述する方法としてユーザーストーリーがあることを理解する。

用語例　エピック，ユーザーストーリー，ストーリーポイント，プロダクトバックログ

⑧ その他の手法
その他，業務分析や要件定義に用いられる手法を理解する。

用語例　決定表（デシジョンテーブル），SysML，状態遷移図，状態遷移表

2. 設計

【目標】
- システム及び／又はソフトウェア設計の考え方，手順，手法，留意事項を修得し，適用する。

(1) システム設計のタスク

システム設計では，システム設計，利用者用文書類（暫定版）の作成，システム設計の評価，システム設計の共同レビューを実施することを理解する。

(2) システム設計

① システム設計の目的
システム設計では，システム要件をハードウェア，ソフトウェア，手作業に振り分け，それらを実現するために必要なシステムの構成品目を決定すること，システム要求仕様が実現できるか，リスクなどを考慮した選択肢の提案は可能か，効率的な運用及び保守ができるかなど，システムを設計する際に考慮すべき点を理解する。

用語例　ハードウェア構成品目，ソフトウェア構成品目，サービス，手作業，機能要件，非機能要件

② ハードウェア・ソフトウェア・サービス・手作業の機能分割
ハードウェア，ソフトウェア，サービス，手作業の機能分割を，業務効率，作業負荷，作業コストなどの観点から検討し，決定することを理解する。

用語例　利用者作業範囲

③ ハードウェア構成の決定
信頼性や性能要件に基づいて，冗長化やフォールトトレラント設計，サーバの機能配分，信頼性配分などを検討し，ハードウェア構成を決定することを理解する。

用語例　アーキテクチャ，ハードウェア要素，IaaS，PaaS，SaaS

④ ソフトウェア構成の決定
システムの供給者が自社で全て開発するか，ソフトウェアパッケージなどを利用するかなどの方針，使用するミドルウェアの選択などを検討し，ソフトウェア構成を決定することを理解する。

用語例　アーキテクチャ，ソフトウェアシステム要素，ソフトウェア要素

⑤ システム処理方式の決定
業務に応じて集中処理，分散処理を選択すること，Web システム，クライアントサーバシステムなど，システムの処理方式を検討し，決定することを理解する。

用語例　集中処理，分散処理，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，Web システム，クライアントサーバシステム，プロトタイプ，データモデル，擬似コード，E-R 図，ユースケース，利用者の役割及び特権のマトリックス，インタフェース仕様，サービス記

述，手順

⑥ データベース方式の決定

システムで使用するデータベースの種類，信頼性を考慮して冗長化したレプリケーションなどを検討し，決定することを理解する。

用語例 RDB（Relational Database：関係データベース），NDB（Network Database：網型データベース），OODB（Object Oriented Database：オブジェクト指向データベース），XML データベース，インメモリデータベース，分散データベース，NoSQL データベース

(3) システム統合テストの設計

システム設計に対し，システム統合テストの範囲，テスト計画，テスト手順などの方針を検討し，システムが機能を全て満たしているかどうかを確認するシステム統合テスト仕様書を作成することを理解する。

用語例 テスト要求事項

(4) アーキテクチャ及びシステム要素の評価及びレビュー

決定したアーキテクチャ及びシステム要素がシステム要件に合致しているか，実現可能かなど，システム要素を評価する際の基準を作成し，システムの取得者及び供給者が共同でレビューを行うことを理解する。

用語例 双方向の追跡可能性（双方向のトレーサビリティ），一貫性，設計標準や方法の適切性，ソフトウェア要素の実現可能性，運用及び保守の実現可能性，レビュー参加者，レビュー方式，クリーンアーキテクチャ

(5) ソフトウェア設計のタスク

ソフトウェア設計では，ソフトウェア設計，利用者用文書類（暫定版）の作成，ソフトウェア設計の評価，ソフトウェア設計の共同レビューを実施することを理解する。

(6) ソフトウェア設計

① ソフトウェア設計

ソフトウェア設計では，ソフトウェア要件定義書を基に，開発側の視点からソフトウェアの構造とソフトウェア要素の設計を行うこと，ソフトウェア要素をソフトウェアユニット（プログラム）まで分割し，各ソフトウェアユニットの機能，ソフトウェアユニット間の処理の手順や関係を明確にすること，ソフトウェア設計書作成の構成，記述上の留意事項を理解する。

用語例 構造化，ソフトウェア要素，ソフトウェアユニット，ソフトウェアユニット分割，ソフトウェアユニット機能仕様決定，ソフトウェアユニット間インタフェース設計，ソフトウェア統合のためのテスト要件，基本機能，部品，入出力設計，物理データ設計，部品化，再利用

② インタフェース設計

インタフェース設計では，ソフトウェア要件定義書を基に，操作性，応答性，視認性，ハードウェア及びソフトウェアの機能，処理方法を考慮して，入出力装置を介して取り扱われるデータに関する物理設計を行うことを理解する。

用語例 入出力詳細設計，GUI，画面設計，帳票設計，伝票設計，レイアウト設計，インタフェース設計基準，タイミング設計，インタフェース条件，ソフトウェアユニット間インタフェース，インタフェース項目，UXデザイン，~~ヒューマン~~ユーザーインタフェース，画面構成，フォームオーバーレイ，リミットチェック，IoT

③ ソフトウェアユニットのテストの設計
ソフトウェアユニット機能仕様書で提示された要件を全て満たしているかどうかを確認するために，テストの範囲，テスト計画，テスト方式を定義し，ソフトウェアユニットのテスト仕様書を作成することを理解する。

用語例　テスト要件，チェックリスト，ホワイトボックステスト

④ ソフトウェア統合テストの設計
ソフトウェア設計書で提示された要件を全て満たしているかどうかを確認するために，テストの範囲，テスト計画，テスト方式を定義し，ソフトウェア統合テスト仕様書を作成することを理解する。

用語例　ソフトウェア統合テスト仕様，テスト要件，チェックリスト，ブラックボックステスト

(7) ソフトウェア要素の評価及びレビュー

ソフトウェア要素がソフトウェア要件に合致していること，ソフトウェア要素間やソフトウェアユニット間の内部一貫性などのソフトウェア要素を評価する際の基準を理解する。また，ソフトウェア設計書について，作成後にレビューを行うことを理解する。

用語例　双方向の追跡可能性（双方向のトレーサビリティ），外部一貫性，内部一貫性，設計方法や作業標準の適切性，テストの実現可能性，運用及び保守の実現可能性，レビュー参加者，レビュー方式

(8) ソフトウェア品質

JIS X 25010 で規定されているシステム及びソフトウェア製品の品質特性を理解し，要件定義や設計の際には品質特性を考慮することを理解する。

用語例　JIS X 25010，ISO 9000

① 利用時の品質モデル
システムとの対話による成果に関係する五つの特性である，利用時の品質モデルを理解する。

用語例　有効性，効率性，満足性，リスク回避性，利用状況網羅性

② 製品品質モデル
システム及び／又はソフトウェア製品の品質特徴（品質に関係する測定可能な特徴とそれに伴う品質測定量）を八つに分類した製品品質モデルを理解する。また，各特性は関連する副特性の集合から構成されていることを理解する。

用語例　機能適合性，性能効率性，互換性，使用性（習得性，運用操作性，アクセシビリティほか），信頼性（可用性，回復性ほか），セキュリティ，保守性（解析性，試験性ほか），移植性

(9) ソフトウェア設計手法

① プロセス中心設計
プロセス中心設計手法によるソフトウェア設計の考え方と手順を理解する。

② データ中心設計
データ中心設計手法によるソフトウェア設計の考え方と手順を理解する。

用語例　DOA（Data Oriented Approach：データ中心アプローチ），E-R 図，実体，関連，正規化，一事実一箇所

③ 構造化設計

(a) 機能分割と構造化

機能分割と構造化の手順（機能の洗い出し，データフローの明確化，機能のグループ化，階層構造化，プログラム機能の決定，機能仕様の文書化），構造化設計による機能分割の利点，留意事項を理解する。

用語例　階層，段階的詳細化，複合設計

(b) 構造化設計の手法

構造化設計で用いられる手法として，流れ図，DFD，構造化チャート，状態遷移図などがあることを理解する。

用語例　順次，選択，繰返し，NS（Nassi-Shneiderman：ナッシュナイダマン）図，HIPO（Hierarchy plus Input Process Output），ブロック図，バブルチャート，階層構造図，イベントトレース図，ジャクソン法，ワーニエ法

(c) プログラムの構造化設計

プログラムの構造化設計の目的，基本的な考え方，手順を理解する。

用語例　品質特性，モジュール分割

④ オブジェクト指向設計

オブジェクト指向設計の考え方，手順，手法を理解する。

用語例　ソフトウェア設計原則（SOLID），クラス，抽象クラス，スーパークラス，インスタンス，属性，メソッド，カプセル化，サブクラス，継承（インヘリタンス），部品化，再利用，クラス図，多相性，パッケージ，関連，派生関連，派生属性，コレクション，汎化，特化，分解，集約

⑤ ドメイン駆動設計（DDD）

ドメイン駆動設計の考え方，手順，手法を理解する。

用語例　ドメイン，ドメインモデル，ドメインロジック，コンテキストマップ，ユビキタス言語，エンティティ，値オブジェクト，サービス

(10) ソフトウェア要素の設計

① ソフトウェア要素分割の考え方

ソフトウェア要素を分割する際の基準には，処理パターン適用，処理タイミングの違い，処理効率の違い，同時使用可能資源，入出力装置の特徴などがあることを理解する。また，基準ごとの特徴を理解する。

用語例　ファイルの統合，ファイルの分割，レコード処理，処理の周期

② プログラム分割基準

プログラム分割の基準を理解する。

用語例　分かりやすさ，安全性，開発の生産性，運用性，処理能力，保守性，再利用性

(11) モジュールの設計

① 分割手法

分割手法には，データの流れに着目した手法とデータ構造に着目した手法があり，内部

処理の形態に応じて複数の分割手法を組み合わせること，分割手法の種類，特徴を理解する。

用語例　STS（Source Transform Sink）分割，TR（Transaction：トランザクション）分割，共通機能分割，論理設計，領域設計，サブルーチン，再帰プログラム

② 分割基準

モジュールの独立性の評価基準として，モジュールの結束性（強度），結合度，それらと独立性との関係，分割量の評価基準，部品化と再利用のための評価基準を理解する。

用語例　モジュールの制御領域，モジュールの影響領域，分割量，モジュール再分割，従属モジュール，機能的結束性，情報的結束性，データ結合，制御結合

③ モジュール仕様の作成

各モジュール仕様の作成の考え方，手順，モジュール仕様の作成に用いられる手法を理解する。

用語例　流れ図，PSD（Program Structure Diagram），DSD（Design Structure Diagram），SPD（Structured Programming Diagrams），HCP（Hierarchical and Compact description）チャート，PAD（Problem Analysis Diagram），決定表（デシジョンテーブル），ワーニエ法，ジャクソン法，NS 図，論理構造図，プログラミングテーブル

（12）部品化と再利用

ソフトウェアの部品化と再利用の必要性，部品の種類と特徴，部品設計の留意事項，ソフトウェアパッケージの利用法を理解する。

用語例　コンポーネントウェア，ホワイトボックス型，ブラックボックス型，クラスライブラリ，デザインパターン，レガシーラッピング，COTS（Commercial Off-The-Shelf）

（13）アーキテクチャパターン

アーキテクチャパターンはソフトウェア構造のパターンであることなどの特徴を踏まえて，アーキテクチャパターンを利用する利点，留意事項を理解する。

用語例　MVC モデル

（14）デザインパターン

デザインパターンは主にオブジェクト指向設計に用いられ，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の 3 種類に分類されることなどの特徴を踏まえて，デザインパターンを利用する利点，留意事項を理解する。

用語例　生成，構造，振舞い，GoF

（15）レビュー

① レビューの目的と手順

プロジェクト活動の状況や成果物を適宜評価するためのレビューの目的を理解する。また，レビューは文書の作成，レビューの実施（レビュー方式の決定，レビューの評価基準の決定，レビュー参加者の選出），レビュー結果の文書への反映作業という手順で行われることを理解する。

② レビューの対象と種類

レビューの対象，実施タイミング，種類を理解する。

用語例　コードレビュー，テスト仕様レビュー，利用者マニュアルレビュー，ピアレビュー，デザインレビュー，インスペクション，モデレーター，文書化手法，ウォークスルー，共同レビュー

③ 妥当性評価の項目
レビューで確認する妥当性評価の項目を理解する。

用語例　機能，性能，容量・能力，信頼性，操作性，安定性，運用の容易性，技術的整合性，合目的性，実現可能性，開発の合理性，経済性，投資効果

④ その他の妥当性評価手法
測定器やテストプログラムの利用によるデータ実測，利用者の意見や感想の収集など，レビュー以外の妥当性評価の手法を理解する。

用語例　ヒアリング，アンケート，チェックリスト

3. 実装・構築

【目標】
- ソフトウェア構築の考え方，手順，手法，留意事項を修得し，応用する。

(1) 実装・構築のタスク

実装・構築では，ソフトウェアユニットの作成，テスト手順及びテストデータの作成，ソフトウェアユニットのテストの実施，利用者用文書類の更新，ソフトウェア統合テスト要件の更新，ソフトウェアコード及びテスト結果の評価を実施することを理解する。

用語例　コーディング，プログラム言語，プログラム書法

(2) ソフトウェアユニットの作成

定められたコーディング標準，プログラム言語の仕様に従い，ソフトウェアユニット機能仕様書に基づいてプログラミングを行うことを理解する。

用語例　セグメント化，制御構造，制御セグメント，プログラム設計，アルゴリズム，データ処理，データベース，加工セグメント，構造化プログラミング，モジュール分割，モジュール仕様，論理型プログラミング，並列処理プログラミング，アスペクト指向プログラミング

(3) ソフトウェアコード及びテスト結果の評価基準

ソフトウェアコードとテスト結果を評価する際の基準を理解する。また，ソフトウェアユニットの作成，ソフトウェアユニットのテスト実施後，レビューを行うことを理解する。

用語例　追跡可能性，外部一貫性，内部一貫性，テスト網羅性，コーディング方法及び作業標準の適切性，ソフトウェア統合及びテストの実現可能性，運用及び保守の実現可能性

(4) コーディング標準

コーディング標準の目的を理解する。また，コーディング標準には具体的にどのような内容を含めるか，コーディング標準を守らない場合にどのような弊害が起こるかを理解する。

用語例　インデンテーション，ネスト，命名規則，使用禁止命令

(5) コーディング支援手法

コーディング支援手法の特徴と，利用する利点，留意事項を理解する。

用語例　コード補完，オートインデント，コードオーディター，シンタックスハイライト，

ブレークポイント

(6) コードレビュー

コードレビューの目的，方法を理解する。また，コーディング標準を守っているか，ソフトウェア詳細設計書に基づいているか，効率性や保守性が適切かなどを確認することを理解する。

用語例 メトリクス計測，コードインスペクション，ピアコードレビュー，ウォークスルー，サイクロマティック複雑度

(7) デバッグ

デバッグの方法，留意事項，机上デバッグと実際にソフトウェアを動作させて行うデバッグの特徴，各種開発ツールを用いたデバッグ方法を理解する。

用語例 デバッグ環境，静的解析，動的テスト，アサーション，デバッガ，トレーサー，スナップショット

(8) ソフトウェアユニットのテスト

① テストの目的

ソフトウェアユニットのテストは，ソフトウェア設計で定義したテスト仕様に従って行い，要求事項を満たしているかどうかを確認することを理解する。

用語例 障害，欠陥，障害分析，使用性（usability）

② テストの手順

テストの目的，方針，スケジュール，体制，使用するテストツールなどを決定してテスト計画を立て，次にテスト項目，テストデータの作成，テスト環境の用意などのテスト準備を行い，テストを実施し，テスト結果を評価するという一連の手順を理解する。

用語例 テスト方法論，テスト範囲，テスト準備（テスト環境，テストデータなど），テストオラクル，テスト実施者，ユニットテスト，チェックシートの作成，シミュレーター，プロトタイプ

③ テストの実施と評価

テストの目的，実施方法，留意事項，テストで使用されるテストツールの役割を理解する。また，テストの実行後には，テスト結果の記録，結果分析，プログラムの修正や改良作業を行うことを理解する。

用語例 デバッガ，ドライバ，スタブ，テストデータジェネレーター，テスト設計と管理手法（バグ曲線，エラー除去，バグ管理図），テスト自動化，テストの網羅度，テスト密度，欠陥密度（バグ密度），トレーサビリティ要件，ソフトウェア要件又はソフトウェア設計との一貫性，ユニットの要件内の一貫性

④ テストの手法

テストで用いられるブラックボックス法，ホワイトボックス法のテストデータの作成方法を理解する。

用語例 メトリクス計測，テストケース，命令網羅，条件網羅，判定条件網羅（decision coverage），複数条件網羅（multiple condition coverage），経路組合せ網羅，網羅率，カバレージ，限界値分析法，同値分析法，原因結果グラフ法，エラー埋込法，実験計画法，ミューテーションテスト，ドメイン分析テスト

4. 統合・テスト

【目標】
- システム及び／又はソフトウェア統合・システム及び／又はソフトウェア検証テストの考え方，手順，手法，留意事項を修得し，応用する。

(1) ソフトウェア統合のタスク

ソフトウェア統合では，ソフトウェア統合計画の作成，ソフトウェア統合，ソフトウェア統合テストの実施，利用者用文書類の更新，ソフトウェア統合の評価，ソフトウェア統合の共同レビュー，ソフトウェア検証テストの準備を実施することを理解する。

用語例　テスト要件，テスト手順，テストデータ

(2) ソフトウェア検証テストのタスク

ソフトウェア検証テストでは，ソフトウェア検証テストの実施，利用者用文書類の更新，ソフトウェア検証テストの評価，ソフトウェア検証テストの共同レビューの実施，監査の支援，納入ソフトウェア製品の準備を実施することを理解する。

用語例　ソフトウェア要件，監査

(3) ソフトウェア統合

ソフトウェア統合では，統合する順序に基づいてソフトウェア統合計画を作成し，構築されたソフトウェアを統合することを理解する。

用語例　統合する順序，再帰戦略（回帰戦略）

(4) ソフトウェア統合テスト

ソフトウェア統合テストはソフトウェア設計で定義したテスト仕様に従って行い，ソフトウェアの動作を確認すること，ソフトウェア統合テストの実施時期，実施手順，評価の基準を理解する。

用語例　テスト計画，テスト準備（テスト環境，テストデータなど），ソフトウェア統合テスト報告書，トップダウンテスト，ボトムアップテスト，ドライバ，スタブ，テストベッド，統合テスト報告書，テスト結果の文書化，文書化基準

(5) ソフトウェア検証テスト

ソフトウェア検証テストはソフトウェア要件定義で定義したソフトウェア要件に従って行い，ソフトウェアが要件どおりに実現されているかを検証することを理解する。

用語例　テストの種類（機能テスト，非機能要件テスト，性能テスト，負荷テスト，セキュリティテスト，回帰テスト（リグレッションテスト）など），ファジング，ソフトウェア検証テスト報告書

(6) ソフトウェア統合及びソフトウェア検証テスト結果の評価

① テスト実施後のタスク

テストの実施後には，テスト結果の記録，結果の分析及び評価，プログラムの修正や改良作業を行い，必要に応じてソフトウェア設計書，利用者用文書類を更新することを理解する。

② ソフトウェア統合の評価

ソフトウェア統合を評価する際の基準を理解する。

用語例　双方向の追跡可能性（双方向のトレーサビリティ），外部一貫性，内部一貫性，テスト網羅性，テスト標準及び方法の適切性，ソフトウェア検証テストの実現可

能性，運用及び保守の実現可能性

③ ソフトウェア検証テストの評価
ソフトウェア検証テストを評価する際の基準を理解する。

用語例　期待した結果に対する適合性，システム統合及びテストの実現可能性

(7) システム統合のタスク

システム統合では，システム統合計画の作成，システム統合，システム統合テストの実施，利用者用文書類の更新，システム統合の評価，システム統合の共同レビュー，システム検証テストの準備を実施することを理解する。

用語例　ハードウェア構成品目，ソフトウェア構成品目，手作業

(8) システム検証テストのタスク

システム検証テストでは，システム検証テストの実施，システムの評価，システム検証テストの共同レビューの実施，利用者用文書類の更新，監査の支援，納入可能なシステムの準備，運用及び保守に引き継ぐシステムの準備を実施することを理解する。

用語例　システム要件

(9) システム統合

システム統合では，統合する順序に基づいてシステム統合計画を作成し，構築されたシステムを統合することを理解する。

用語例　統合する順序，再帰戦略（回帰戦略）

(10) システム統合テスト

システム統合テストはシステム設計で定義したテスト仕様に従って行い，ソフトウェア構成品目，ハードウェア構成品目，手作業及び必要に応じてほかのシステムを全て統合したシステムが要件を満たしているかどうかを確認すること，システム統合テストの実施時期，実施手順，評価の基準を理解する。

用語例　テスト計画，テスト準備（テスト環境，テストデータなど），システム統合テスト報告書，テスト結果の文書化，文書化基準

(11) システム検証テスト

システム検証テストはシステム要件定義で定義したシステム要件に従って行い，システムが要件どおりに実現されているかどうかを確認することを理解する。

用語例　テストの種類（機能テスト，非機能要件テスト，性能テスト，負荷テスト，セキュリティテスト，回帰テスト（リグレッションテスト），探索的テストなど），システム検証テスト報告書

(12) システム統合及びシステム検証テスト結果の評価

① テスト実施後のタスク
テストの実施後には，テスト結果の記録，結果の分析及び評価，システムのチューニングを行い，必要に応じて文書の更新を行うことを理解する。

② システム統合の評価
システム統合を評価する際の基準を理解する。

用語例　テスト網羅性，テスト方法及び作業標準の適切性，期待した結果への適合性，システム検証テストの実現可能性，運用及び保守の実現可能性，レビュー

③ システム検証テストの評価
システム検証テストを評価する際の基準を理解する。

用語例　テスト方法及び作業標準の適切性

5.　導入・受入れ支援

【目標】
- システム及び／又はソフトウェアの導入及び受入れ支援の考え方，手順，手法，留意事項を修得し，応用する。
- 妥当性確認テストの考え方，手順，手法，留意事項を修得し，応用する。

(1) システム及び／又はソフトウェアの導入のタスク

システム及び／又はソフトウェアの導入（インストール）では，システム及び／又はソフトウェアの導入計画の作成，導入を実施することを理解する。

(2) システム及び／又はソフトウェアの受入れ支援のタスク

システム及び／又はソフトウェアの受入れ支援では，取得者の受入れレビューや受入れテストの支援，納入，取得者への教育訓練及び支援を実施することを理解する。

用語例　納品

(3) 妥当性確認テストのタスク

妥当性確認テストでは，妥当性確認テストの実施，妥当性確認テストの結果の管理を行うことを理解する。

(4) 導入

① システム及び／又はソフトウェアの導入計画の作成
システム及び／又はソフトウェアの導入に先立って，実環境への導入及び新旧のシステム及び／又はソフトウェアの移行をどのように実施するのか，データ保全や業務への影響などの留意事項は何か，スケジュールや体制はどのようにするかなど，導入計画を作成，文書化することを理解する。

用語例　導入要件，移行要件（プロセス及びデータの移行，移行保守の取組方法及びスケジュール），導入可否判断基準，インストール計画の作成，導入作業，リプレース，並行稼働対応，導入文書，一斉移行，段階移行，移行リハーサル，移行システム，カナリアリリース，ブルーグリーンデプロイメント

② システム及び／又はソフトウェアの導入の実施
システム及び／又はソフトウェアの導入計画に従って導入を行うこと，その際の留意事項を理解する。また，システム及び／又はソフトウェア，データベースなどを契約で指定されたとおりに初期化などを行い，実行環境を整備すること，導入時の作業結果を文書化することを理解する。

用語例　導入手順，導入体制，利用部門，システム運用部門，運用サイト，仮想環境，通信用資源，ソフトウェア導入

③ 利用者支援
システム及び／又はソフトウェアの導入に当たり，利用者を支援する作業を理解する。

用語例　教育訓練資料，教育訓練システム（e-Learning，Web Based Training），ロジスティクス支援パッケージ

(5) 受入れ支援

① システム及び／又はソフトウェアの受入れレビューとテスト
システム及び／又はソフトウェアの供給者は，取得者による受入れレビューやテストを支援すること，受入れレビューやテストの目的，どのように実施するのかを理解する。また，取得者は，供給者の受入れ支援を受け，共同レビュー，システム及び／又はソフトウェアの妥当性確認テストの結果を考慮して，受入れの準備，受入れレビュー，テストを行い，結果を文書化することを理解する。

用語例　受入れ手順，受入れ基準，受入れテスト，検収，検収基準

② システム及び／又はソフトウェアの納入と受入れ
システム及び／又はソフトウェアの供給者，取得者は，契約で示されたとおりにシステム及び／又はソフトウェアが完成していることを相互に確認して納入し，受け入れることを理解する。

用語例　受入れ体制，利害関係者の合意，双方向の追跡可能性（双方向のトレーサビリティ）

③ 教育訓練
システム及び／又はソフトウェアの供給者は，取得者に対して，初期及び継続的な運用のための教育訓練，支援を提供すること，取得者は供給者の支援を受けて体制の整備，教育訓練の計画，実施を行うことを理解する。また，教育訓練の目的，内容，準備，体制，結果の評価方法を理解する。

用語例　教育訓練計画，教育訓練の準備，教育訓練体制，教育訓練結果の評価方法，教育訓練システム（e-Learning，Web Based Training），カークパトリックの教育効果の 4 段階モデル

④ 利用者用文書類（利用者マニュアル）
システム及び／又はソフトウェアの取得者の業務，コンピュータ操作，システム運用などの手順を利用者用文書類（利用者マニュアル）として文書化すること，利用者用文書類（利用者マニュアル）はシステム設計時又はソフトウェア設計時に暫定版を作成し，開発の進行に従って適宜更新することを理解する。

用語例　運用規程，~~利用者マニュアル，~~利用者用文書類（ウィザード，学習書（チュートリアル），オンラインヘルプ），組込文書類，分離形文書類，システム利用文書，ソフトウェア利用文書，文書類のテスト

(6) 妥当性確認テスト

① 妥当性確認テストの実施
定義した環境において妥当性確認テストの手順を実施することを理解する。

用語例　妥当性確認される要件（要求事項），関連する作成物，妥当性確認テストの目的，成功基準（期待される結果），適用する妥当性確認テストの技法，必要とするイネーブリングシステム（施設・設備・機器），各妥当性確認テストを実施するための環境条件

② 妥当性確認テストの結果の管理
妥当性確認テストによって識別されたインシデント及び問題を記録し，それらの解決を追跡すること，及び妥当性確認されたシステム要素のトレーサビリティを維持することを理解する。

用語例　不具合の根本原因，是正処置，欠陥修正，改善作業，学んだ教訓の記録，双方向の追跡可能性（双方向のトレーサビリティ）

③ 妥当性確認テストの手法又は技法
妥当性確認テストで用いる手法又は技法を理解する。

用語例　使用性テスト，ソフトウェアの試行利用（ベータテスト，運用操作テスト，利用者テスト，受入れテスト），分析，相似性・類似性，自演による実証，シミュレーション

6. 保守・廃棄

【目標】
- 保守の考え方，タイプ及び形態，手順，留意事項を修得し，応用する。
- 廃棄の考え方，手順，留意事項を修得し，応用する。

(1) 保守のタスク

保守の目的やサービスレベルなどの保守を受ける側の要求，保守を提供する側の実現性や費用を考慮して，保守要件を決定することを理解する。また，保守では問題の発生，改善，機能拡張要求などへの対応として，既存システム及び／又は既存ソフトウェアの安全性を維持しつつ修正や変更を行うことを理解する。

用語例　保守手順，保守体制，保守の実現可能性，保守テスト，回帰テスト（リグレッションテスト），リファクタリング，リバースエンジニアリング

(2) 廃棄のタスク

廃棄では，運用及び保守の組織によって実施中の支援を終えるか，又は影響を受けるシステム若しくはソフトウェアを最終の状態にし，かつ，廃棄しても運用に支障のない状態にして，起動不能にしたり，解体したり，取り除いたりすることを理解する。

用語例　組織の運用の完整性（integrity）

(3) 保守のタイプ及び形態

保守をどのように実施するか，保守のタイプ及び形態，その際の留意事項，実施内容，方法の違いなどを理解する。

用語例　保守契約，保守要件の定義，ハードウェア保守，日常点検，是正保守，改良保守，予防保守，適応保守，完全化保守，オンサイト保守，遠隔保守，ライフサイクルの評価

(4) 保守の手順

① 保守プロセス開始の準備
保守業務開始のための準備を行うことを理解する。

用語例　開発プロセスからの保守に必要な成果物の引継ぎ，計画及び手続の作成，問題管理手続の確立，修正作業の管理，保守のための文書作成

② 問題把握及び修正の分析
保守対象のシステム及び／又はソフトウェアの問題や改善要求を解決する過程を理解する。

用語例　問題報告又は修正依頼の分析，問題の再現又は検証，修正実施の選択肢の用意

③ 修正の実施

修正部分が決まった後，修正を実施する過程を理解する。

用語例 修正するシステム及び／又はソフトウェアや関連文書の決定，機能追加，性能改良，問題の是正

④ 保守レビュー及び／又は受入れ

修正されたシステム及び／又はソフトウェアの動作確認や完了の承認を行うことを理解する。

用語例 修正されたシステム及び／又はソフトウェアの完整性（integrity）

⑤ 再発防止策の実施

問題の再発防止のため，特性要因分析などを実施することによって，根本原因の抽出，類似事故の発生の可能性を検討し，システム及び／又はソフトウェアの改善やマニュアルなどの改訂を行うことを理解する。

用語例 システム信頼性のための解析技法（FTA，FMEA，STAMP/STPAほか），双方向の追跡可能性（双方向のトレーサビリティ）

⑥ 移行

システム移行及び／又はソフトウェア移行の手順，システム及び／又はソフトウェアの完全性の維持，業務への影響など移行の際の留意事項を理解する。

用語例 移行計画の文書化と検証，関係者全員への移行計画などの通知，新旧環境の並行運用と旧環境の停止，関係者全員への移行の通知，移行結果の検証，移行評価，旧環境関連データの保持と安全性確保

(5) 廃棄

システム及び／又はソフトウェアの導入や更新などに伴い，不要となったシステム及び／又はソフトウェアの廃棄の手順を理解する。

用語例 廃棄計画の立案，廃棄計画などの利用者への通知，新旧環境の並行運用と利用者の教育訓練，関係者全員への廃棄の通知，廃棄関連データの保持とアクセス可能性の確保

大分類 4：開発技術　中分類 13：ソフトウェア開発管理技術（技術レベル 3）

1.　開発プロセス・手法

【目標】
- ソフトウェア開発プロセスに関する手法の考え方，特徴を修得し，応用する。
- アジャイルの概要，アジャイルソフトウェア開発手法の考え方，特徴を修得し，応用する。

(1) ソフトウェア開発手法

① ソフトウェア開発モデル

ソフトウェア開発の効率化や品質向上のために用いられるソフトウェア開発モデルの考え方，必要性を理解し，ソフトウェア開発モデルの特徴を理解する。

用語例　ウォーターフォールモデル，プロトタイピングモデル，アジャイル，DevOps，MLOps，ソフトウェアプロダクトライン，段階的モデル（Incremental Model），進展的モデル（Evolutionary Model）

② アジャイル

迅速かつ適応的にソフトウェア開発を行う軽量な開発手法であるアジャイルの特徴を理解する。

(a) アジャイルの概要

アジャイルの概要として，アジャイルソフトウェア開発手法の種類などを理解する。

用語例　アジャイルソフトウェア開発宣言，アジャイルソフトウェアの 12 の原則，XP（エクストリームプログラミング），スクラム，リーンソフトウェア開発，ユーザー機能駆動開発（FDD），テスト駆動開発（TDD），ペルソナ，インセプションデッキ，ユーザーストーリー，INVEST，プランニングポーカー，タイムボックス，バーンダウンチャート，ベロシティ，モブプログラミング，リファクタリング，ふりかえり（レトロスペクティブ），KPT（Keep，Problem，Try），継続的インテグレーション（CI)），継続的デリバリー（CD），エンタープライズアジャイル（SAFe，LeSS（Large-Scale Scrum），Scrum of Scrums），DA（Disciplined Agile）

(b) XP（エクストリームプログラミング）の特徴

XP（エクストリームプログラミング）の特徴を理解する。

用語例　五つの価値（コミュニケーション，シンプル，フィードバック，勇気，尊重），共同のプラクティス，開発のプラクティス（テスト駆動開発（TDD），ペアプログラミング，リファクタリング，ソースコードの共同所有，継続的インテグレーション（CI），YAGNI），管理者のプラクティス，顧客のプラクティス，イテレーション

(c) スクラムの特徴

スクラムの特徴を理解する。

用語例　スクラムチーム（プロダクトオーナー，開発~~チーム~~者，スクラムマスター），スプリント，スプリントプランニング，デイリースクラム，スプリントレビュー，スプリントレトロスペクティブ，プロダクトバックログ，スプリントバックログ，インクリメント

③ DevOps

開発チームと運用チームが連携し，迅速かつ柔軟にソフトウェア開発を行う DevOps の特徴を理解する。

用語例 CALMS フレームワーク（Culture（文化），Automation（自動化），Lean（リーン），Measurement（測定），Sharing（共有）），SRE（Site Reliability Engineering：サイト信頼性エンジニアリング），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，テスト駆動開発（TDD），カオスエンジニアリング，Four Keys（デプロイの頻度，変更のリードタイム，変更障害率，平均修復時間（MTTR）），オブザーバビリティ（可観測性），OpenTelemetry，DevSecOps

④ ローコード／ノーコード開発

専門的なコーディングの知識や経験がなくてもソフトウェアの開発が可能となるローコード／ノーコード開発の特徴，利点，留意事項を理解する。

~~③~~⑤ ソフトウェア再利用

ソフトウェアの開発生産性や品質向上のためには，部品化や再利用が必要であり，部品化を進める際には，部品は再利用されるという前提に立って設計や作成に取り組む必要があること，ソフトウェアパッケージを活用することによって，開発生産性や品質向上が可能になることなどを理解する。また，ソフトウェア部品の種類，特徴，部品設計のポイントを理解する。

(a) 部品の種類と特徴

ソフトウェア部品の種類と特徴を理解する。

用語例 関数部品，オブジェクト部品（クラスライブラリ），データ部品，プロセス部品，常駐部品と組込み部品，ブラックボックス部品，ホワイトボックス部品，パラメトリック部品，ノンパラメトリック部品，クローズドシステム部品，オープンシステム部品

(b) 部品設計の基準

部品の利用用途に応じた，設計基準の目的，内容を理解する。

用語例 モジュールの独立性，カスタマイズ，ライブラリ，命名規則

~~④~~⑥ リバースエンジニアリング

既存のソフトウェアを解析して，仕様や構成部品などの情報を得るリバースエンジニアリングがあること，リバースエンジニアリングの結果に基づいて，元のソフトウェアの権利者の許可なくソフトウェアを開発，販売すると，元の製品の知的財産権を侵害する可能性があること，利用許諾契約によっては，リバースエンジニアリングを禁止している場合もあることなどを理解する。

用語例 互換性，コールグラフ

~~⑤~~⑦ マッシュアップ

マッシュアップは，複数の提供元による API を組み合わせることで，新しいサービスを構築する手法であることを理解する。また，マッシュアップの考え方，生産性，品質面での特徴，留意事項を理解する。

用語例 プレゼンテーションマッシュアップ，データマッシュアップ，ロジックマッシュアップ

~~⑥~~⑧ モバイルアプリケーションソフトウェア開発

モバイルアプリケーションソフトウェア開発の手順，留意事項を理解する。

用語例 モバイル用 Web アプリケーションソフトウェア，ネイティブアプリケーションソフトウェア，ハイブリッドアプリケーションソフトウェア，PWA（Progressive Web Apps：プログレッシブウェブアプリ），User-Agent，パーミッション要求，端末仕様（ディスプレイサイズほか）の多様性への対応，アプリケーションソフトウェア動作中の圏外時・着信時の対応，アプリケーションソフトウェア審査，アプリケーションソフトウェア配布

(2) 構造化手法

大規模なシステムや複雑な処理内容に対して適切な品質を確保し，また，プログラムの保守を容易にするために構造化手法が用いられること，構造化手法の考え方，特徴，手順，効果，留意事項を理解する。

用語例 階層構造化，段階的詳細化，構造化チャート，状態遷移図，HIPO（Hierarchy plus Input Process Output），DFD，ソフトウェア構造

(3) 形式手法

形式手法（Formal Method）は，形式仕様記述言語を使用してルールに従って厳密に記述し，ソフトウェアの品質を高めるための手法であること，モデルの状態を記述することに重点をおいていること，その仕様記述言語である VDM-SL（Vienna Development Method - Specification Language），VDM++の考え方，特徴を理解する。

用語例 モデル検査，VDMTools，Z 言語，SPIN

(4) 開発プロセス

① ソフトウェアライフサイクルプロセス

SLCP（Software Life Cycle Process：ソフトウェアライフサイクルプロセス）の目的と全体像を理解する。

用語例 JIS X 0160，JIS X 0170，プロセス，アクティビティ，タスク，合意プロセス，組織のプロジェクトイネーブリングプロセス，テクニカルマネジメントプロセス，テクニカルプロセス，プロセス修整（Tailoring），完全適合，修整適合，SLCP-JCF（共通フレーム）

② プロセス成熟度

開発と保守のプロセスを評価，改善するに当たって，システム開発／ソフトウェア開発を行う組織~~と~~のプロセス成熟度の水準を~~モデル化した CMMI があること，~~識別するための成熟度モデルがあること，プロセス~~成熟度~~の能力を ~~5~~6 段階~~のレベル~~で定義~~するなど CMMI の考え方~~して進化の道筋を示した能力水準や進化レベルの内容，より高次のレベルに達するために必要な方策を理解する。

用語例 JIS X 33001，JIS X 33020，組織の標準プロセス，プロセス改善，不完全なプロセス，実施されたプロセス，管理されたプロセス，確立されたプロセス，予測可能なプロセス，革新しているプロセス，CMMI

2. 知的財産適用管理

【目標】
- ソフトウェア開発工程で必要となる知的財産権の取得，管理の目的，考え方を修得し，応用する。
- ソフトウェア開発工程で発生した知的財産権の保護のための手順を修得し，応用する。

(1) 著作権管理

開発するソフトウェアの著作権の帰属の考え方を理解し，プログラムを外注する場合の留意事項を理解する。

用語例　プログラムの著作者，職務著作

(2) 特許管理

ソフトウェア開発工程で発生した発明を保護するための手順を理解する。ソフトウェア開発時に他者のもつ特許を利用する必要が生じた場合は，使用許諾を受ける必要があることを理解する。

用語例　特許権，専用実施権，通常実施権

(3) ライセンス管理

ソフトウェア開発時に，自社が権利を所有しないソフトウェアを利用する必要が生じた場合はライセンスを受ける必要があること，獲得したライセンスについては使用実態や使用人数がライセンス契約で託された内容を超えないよう管理する必要があることを理解する。

用語例　ライセンサー，ライセンシー

(4) 技術的保護

ソフトウェアやコンテンツなどの知的財産を技術的に保護する手法の特徴，効果，留意事項を理解する。

用語例　コピーガード，DRM，アクティベーション，CPRM，AACS

3.　開発環境管理

【目標】
- 開発環境の目的，考え方，管理対象，手法を修得し，応用する。

(1) 開発環境構築

効率的な開発のためには，開発用ハードウェア，ソフトウェア，ネットワーク，シミュレーターなどの開発ツールを開発要件に合わせて準備することを理解する。

用語例　構成品目，ソフトウェアライセンス，SCM（Source Code Management：ソースコード管理），ステージング環境

(2) 管理対象

① 開発環境稼働状況管理

効率的な開発のためには，コンピュータ資源，開発支援ツールなど適切な開発環境の準備が必要であること，また資源の稼働状況を適切に把握，管理することを理解する。

用語例　資源管理，運用管理

② 設計データ管理

設計に関わる様々なデータのバージョン管理，プロジェクトでの共有管理，安全管理など，設計データを管理することを理解する。また，企業機密や個人情報が含まれているデータは，誰がいつ何の目的で利用したのか，不適切な持出しや改ざんがないかなどを厳重に管理することを理解する。

用語例　更新履歴管理，アクセス権管理，検索，リポジトリ

③ ツール管理

多数の人が開発に携わる場合，開発に利用するツールやバージョンが異なることによって，作成したソフトウェアの互換性の問題が生じるおそれがあることを理解する。また，ツールに起因するバグやセキュリティホールの発生など，ツールの選択によって開発対象のソフトウェアの信頼性に影響を及ぼすおそれがあるので，使用するツールやバージョンの統一などツールを管理することを理解する。

用語例　構成品目，バージョン管理

④ ライセンス管理

ライセンス条項に違反した利用は不正利用に当たり，不正利用は違法行為として法的処罰の対象となることを理解する。また，ライセンスの内容を理解し，定期的にインストール数と保有ライセンス数を照合確認するなど，適正に使用しているかどうかを確認することを理解する。

用語例　不正コピー，バージョン管理，棚卸

4.　構成管理・変更管理

【目標】
- 構成管理と変更管理の目的，考え方，手順を修得し，応用する。

(1) 構成管理

構成管理では，ソフトウェア全体がどのような構成品目の組み合わせで構成されているかという構成識別体系を確立し，その構成識別体系の管理の方法を明らかにした上で管理を行うことを理解する。

用語例　ソフトウェア構成管理，ソフトウェア構成品目，SLCP（Software Life Cycle Process：ソフトウェアライフサイクルプロセス），構成管理計画，ベースライン，SBOM（Software Bill of Materials）

(2) 変更管理

① 構成状況の記録

基準になっているソフトウェア構成品目について，状況や履歴を管理し文書化すること，プロジェクトにおける変更回数，最新のバージョン，移行状況などの当該文書に記録する内容を理解する。

② ソフトウェア構成品目の完全性保証

ソフトウェア構成品目の機能的な完全性と物理的な完全性を決定，保証することであること，及びその必要性を理解する。

用語例　一貫性，正確性

③ リリース管理及び出荷

ソフトウェア構成品目の完全性が保証された後は，ソフトウェアや関連文書の新しい版の出荷などの手続を行うこと，ソフトウェアのコードや文書はソフトウェアの寿命のある間保守することを理解する。

用語例　バージョン管理，保管期間

マネジメント系

大分類 6：サービスマネジメント　中分類 15：サービスマネジメント（技術レベル 3）

1.　サービスマネジメント

【目標】
- サービスマネジメントの目的，考え方を修得し，適用する。
- サービスマネジメントシステムの確立，実施，維持及び継続的改善の考え方を修得し，適用する。

(1) サービスマネジメントの目的と考え方

サービスマネジメントは，価値を提供するため，サービスの計画立案，設計，移行，提供及び改善のための組織の活動及び資源を，指揮し，管理する，一連の能力及びプロセスであることを理解する。

用語例　サービス，サービスコンポーネント，サービス品質，サービスマネジメント，サービスライフサイクルの段階（計画立案，設計，移行，提供，改善）

(2) サービスマネジメントシステムの確立，実施，維持及び継続的改善

サービス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の組織に対する要求事項について，JIS で規定していることを理解する。

用語例　サービスマネジメントシステム，サービスの要求事項，顧客，サービス提供者，JIS Q 20000 の規格群（ISO/IEC 20000 シリーズ）

(3) ITIL

サービスマネジメントのフレームワークで，現在，デファクトスタンダードとして世界で活用されている ITIL（Information Technology Infrastructure Library）の目的，考え方を理解する。

(4) SLA

サービスレベル合意書（SLA：Service Level Agreement）は，サービス及びその合意されたパフォーマンスを特定した，組織と顧客との間の合意文書であることを理解する。また，代表的なサービスレベル目標を理解する。

用語例　SLA，SLO，SLI，サービス可用性，信頼性，サービス時間，応答時間，サービス及びサービスマネジメントシステムのパフォーマンス

2.　サービスマネジメントシステムの計画及び運用

【目標】
- サービスマネジメントシステムの計画及び運用の要求事項を修得し，適用する。

(1) サービスマネジメントシステムの計画と支援

サービスマネジメントシステムの計画を作成，実施及び維持することを理解する。また，サービスマネジメントシステム及びサービスの運用を支援するために必要な知識を決定し，維持することを理解する。

用語例　PDCA，JIS Q 9001，マネジメントシステム，資源，力量，認識，コミュニケーション，文書化した情報，知識

(2) サービスの計画

サービスの要求事項を決定し，利用可能な資源を考慮して，変更要求及び新規サービス又はサービス変更の提案の優先順位付けを行う。

用語例　サービスの要求事項，変更要求，サービスポートフォリオ，サービス・パイプライン，サービスの状態（計画中，開発中，稼働中，廃止など）

(3) サービスカタログ管理

顧客に提供するサービスについての文書化した情報として，サービスの意図した成果及びサービス間の依存関係を説明する情報を含めて，サービスカタログを作成し，維持することを理解する。また，顧客，利用者及びその他の利害関係者に対して，サービスカタログの適切な部分へのアクセスを提供することを理解する。

用語例　サービスカタログ

(4) 資産管理

サービスマネジメントシステムの計画における要求事項及び義務を満たすため，サービスを提供するために使用されている資産を確実に管理することを理解する。

用語例　資産管理（IT アセットマネジメント（ITAM：IT asset management)），ソフトウェアアセットマネジメント（SAM)，ライセンスマネジメント，JIS X 0164 シリーズ

(5) 構成管理

構成品目を識別，記録，制御，追跡及び検証し，サービスに関連する構成情報を管理することを理解する。また，定められた間隔で，構成情報の正確性を検証すること，必要に応じて，構成情報を他のサービスマネジメント活動で利用可能とすることを理解する。

用語例　構成管理，構成品目（CI)，構成情報，文書化された構成情報（例：構成管理データベース（CMDB))，版（バージョン)，構成ベースライン，構成識別，構成監査

(6) 事業関係管理

顧客関係を管理し，顧客満足を維持し，顧客及び他の利害関係者との間のコミュニケーションのための取決めを確立することを理解する。また，サービスのパフォーマンス傾向及びサービスの成果のレビューを行い，サービス満足度の測定，サービスに対する苦情の管理を行うことを理解する。

用語例　事業関係管理，顧客関係，顧客満足，サービス満足度，苦情

(7) サービスレベル管理

サービスレベルを定義，合意，記録及び管理するために，顧客と提供するサービスについて SLA を合意することを理解する。また，あらかじめ決められた間隔で，サービスレベル目標に照らしたパフォーマンス及び実績の周期的な変化を監視し，レビューし，報告する。

用語例　サービスレベル管理，サービスレベル目標，サービスレベル指標，パフォーマンス

(8) 供給者管理

外部供給者の管理として，外部供給者との関係，契約及び外部供給者のパフォーマンスを監視することを理解する。内部供給者及び供給者として行動する顧客の管理として，サービスレベル目標及び関係者間のインタフェースを定義するための合意文書を作成し，合意すること，及びパフォーマンスを監視することを理解する。

用語例　供給者管理，外部供給者，内部供給者，供給者として行動する顧客，契約，アウトソーシングの利用，SaaS，PaaS，IaaS などのクラウドサービスの利用

(9) サービスの予算業務及び会計業務

財務管理の方針及びプロセスに従ってサービスの予算業務及び会計業務を行うこと，費用はサービスに対して効果的な財務管理及び意思決定ができるように予算化すること，及びあらかじめ定めた間隔で，予算に照らして実際の費用を監視・報告し，財務予測をレビューし，費用を管理することなどを理解する。

用語例　サービスの予算業務及び会計業務，財務管理，予算業務，会計業務，課金，配賦，費用，直接費，間接費，減価償却，総所有費用（TCO）

(10) 需要管理

あらかじめ定めた間隔で，サービスに対する現在の需要を決定し，将来の需要を予測すること，及びサービスの需要及び消費を監視し報告することを理解する。

用語例　需要，需要管理，需要予測

(11) 容量・能力管理

資源の容量・能力の要求事項を，決定し，サービスに対する需要に基づいた現在及び予測される容量・能力を計画し，提供することを理解する。また，容量・能力の利用を監視し，容量・能力及びパフォーマンスデータを分析し，パフォーマンスを改善するための機会を特定することを理解する。

用語例　容量・能力（キャパシティ），容量・能力計画，容量・能力管理，監視，しきい（閾）値，管理指標（CPU 使用率，メモリ使用率，ディスク使用率，ネットワーク使用率ほか）

(12) 変更管理

① 変更管理方針

変更管理が管理するサービスコンポーネント及び他の品目，緊急の変更を含む変更のカテゴリ及び管理の方法，及び顧客又はサービスに重大な影響を及ぼす可能性のある変更を判断する基準を定義することを理解する。

用語例　変更管理，変更管理方針

② 変更管理の開始

変更管理の開始では，サービスの追加，廃止又は提案を含む変更要求を記録・分類し，“サービスの設計及び移行”又は“変更管理の活動”のどちらで変更の管理を行うかを決定することを理解する。

用語例　変更要求（RFC）

③ 変更管理の活動

変更管理の活動では，主に次を行うことを理解する。

- 変更要求の優先度を決定する。
- リスク，事業利益，実現可能性及び財務影響を考慮し，変更要求を承認する。
- 承認された変更を，計画，開発（構築）及び試験する。
- 成功しなかった変更を戻す又は修正する活動を計画し，可能であれば試験する。
- 試験された変更は，リリース及び展開管理に送られ，稼働環境に展開する。

用語例　優先度，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），ロールバック（切り戻し），変更諮問委員会（CAB），変更実施後のレビ

ュー（PIR）

（13）サービスの設計及び移行

① 新規サービス又はサービス変更の計画

サービス計画で決定した新規サービス又はサービス変更についてのサービスの要求事項を用いて，新規サービス又はサービス変更の計画を立案することを理解する。

用語例 サービスの設計及び移行，新規サービス又はサービス変更の計画

② 設計

サービス計画で決定したサービスの要求事項を満たすように，設計し，文書化することを理解する。また，SLA，サービスカタログ，契約書などの新設，更新を行うことを理解する。

用語例 サービス受入れ基準，設計・開発，サービス設計書，非機能要件

③ 構築及び移行

文書化した設計に適合する構築を行い，サービス受入れ基準を満たしていることを検証するために，試験することを理解する。リリース及び展開管理を使用して，新規サービス又はサービス変更を，稼働環境に展開することを理解する。

用語例 構築，継続的インテグレーション，移行，運用サービス基準，業務及びシステムの移行，移行計画，移行リハーサル，移行判断，移行の通知，移行評価，運用テスト，受入れテスト，運用引継ぎ

（14）リリース及び展開管理

新規サービス又はサービス変更，及びサービスコンポーネントの稼働環境への展開について計画し，実施することを理解する。また，リリースの成功又は失敗を監視し，改善の機会を特定するために，分析から導き出された結果をレビューすること，及びリリースの成功又は失敗に関する情報や将来のリリース期日についての情報を，適切な他のサービスマネジメント活動のために利用可能にすることを理解する。

用語例 リリース及び展開管理，リリース，緊急リリースを含むリリースの種類，展開，リリースの受入れ基準，受入れ試験環境，稼働環境，リリースの配付，継続的デリバリー，継続的デプロイ

（15）インシデント管理

① インシデントの対応

インシデントとは，サービスに対する計画外の中断，サービスの品質の低下，又は顧客又は利用者へのサービスに影響していない事象のことであり，次の事項を実施することを理解する。

a）記録し，分類する。
b）影響及び緊急度を考慮して，優先順位付けをする。
c）必要であれば，エスカレーションする。
d）解決する。
e）終了する。

用語例 インシデント管理，インシデント，記録，分類，影響，緊急度，優先順位，解決目標時間，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），解決，回避策，終了，インシデントモデル

② 重大なインシデントの対応

重大なインシデントを特定する基準を決定することを理解する。また，重大なインシデントは，文書化された手順に従って分類し，管理し，トップマネジメントに通知することを理解する。

用語例　重大なインシデント

(16) サービス要求管理

サービス要求に対して，次の事項を実施することを理解する。

a) 記録し，分類する。
b) 優先順位付けをする。
c) 実現する。
d) 終了する。

また，サービス要求の実現に関する指示書を，サービス要求の実現に関与する要員が利用できるようにすることを理解する。

用語例　サービス要求管理，サービス要求，記録，分類，緊急度，優先順位，実現，終了，サービス要求の実現に関する指示書

(17) 問題管理

問題を特定するために，インシデントのデータ及び傾向を分析すること，及び根本原因の分析を行い，インシデントの発生又は再発を防止するための処置を決定することを理解する。問題管理は，次の事項を実施することを理解する。

a) 記録し，分類する。
b) 優先順位付けする。
c) 必要であれば，エスカレーションする。
d) 可能であれば，解決する。
e) 終了する。

問題管理に必要な変更は，変更管理の方針に従って管理することを理解する。また，根本原因が特定されたが問題が恒久的に解決されていない場合，問題がサービスに及ぼす影響を低減又は除去するための処置を決定すること，及び既知の誤りを記録することを理解する。

用語例　問題管理，問題，傾向分析，根本原因，予防処置，記録，分類，優先順位付け，エスカレーション，解決，終了，既知の誤り，回避策，解決策

(18) サービス可用性管理

サービス可用性のリスクのアセスメントを行うこと，及びサービス可用性の要求事項及び目標を決定することを理解する。また，サービス可用性を監視し，結果を記録し，目標と比較すること，計画外のサービス可用性の喪失を調査し，必要な処置をとることを理解する。

用語例　サービス可用性管理，サービス可用性，信頼性，回復力，保守性，MTBF，MTTR，MTBSI，MTRS

(19) サービス継続管理

サービス継続のリスクのアセスメントを行うこと，及びサービス継続の要求事項を決定し，サービス継続計画を作成し，実施し，維持することを理解する。また，サービス継続計画は，あらかじめ定めた間隔又はサービス環境に重大な変更があった場合，試験することを理解する。

用語例　事業継続計画（BCP），サービス継続計画，復旧，RTO（目標復旧時間），RPO（目標復旧時点），RLO（目標復旧レベル），コールドスタンバイ，ホットスタンバイ，ウォームスタンバイ

(20) 情報セキュリティ管理

情報セキュリティ方針，情報セキュリティ管理策，情報セキュリティインシデントに関す

る事項を実施することを理解する。
なお，ISO/IEC 27000 シリーズ（及びそれに基づき制定されている JIS 規格群）は，情報セキュリティマネジメントシステムの要求事項を規定し，導入及び運用を支援するための手引を提供している。

3. パフォーマンス評価及び改善

【目標】
- パフォーマンス評価及び改善を修得し，適用する。

(1) パフォーマンス評価

① 監視，測定，分析及び評価
サービスマネジメントの目的に照らしてサービスマネジメントシステムのパフォーマンスと有効性を評価すること，また，サービスの要求事項に照らして，サービスの有効性を評価することを理解する。

② サービスの報告
報告の要求事項及び目的を決定し，サービスマネジメントシステム及びサービスのパフォーマンス並びに有効性に関する報告を作成することを理解する。

用語例 サービスの報告，パフォーマンス，有効性，傾向情報

(2) 改善

① 不適合及び是正処置
不適合が発生した場合に，不適合を管理し修正するための処置をとること，不適合によって起こった結果に対処すること，不適合が再発しないようにするための処置の必要性を評価すること，必要な処置を実施することを理解する。

用語例 不適合，是正処置

② 継続的改善
サービスマネジメントシステム及びサービスの適切性，妥当性及び有効性を継続的に改善すること，改善の機会に対して適用する評価基準を決定すること，承認された改善活動を管理することを理解する。

用語例 継続的改善，プロセス能力水準（プロセス成熟度水準），プロセスアセスメント，ギャップ分析，CSF（Critical Success Factors：重要成功要因），KPI（Key Performance Indicator：重要業績評価指標），KGI（Key Goal Indicator：重要目標達成指標）

4. サービスの運用

【目標】
- 運用計画や資源管理といったシステム運用管理の役割，機能を修得し，適用する。
- システムの操作やスケジューリングといった運用オペレーションの役割，機能を修得し，適用する。
- サービスデスクの役割，機能を修得し，適用する。

(1) システム運用管理

システムの運用管理では，日常の運用計画，障害発生時運用を適切に行うための計画，運用負荷低減のための改善計画などに加えて，容量・能力管理，情報セキュリティ管理，サー

ビス可用性管理及びサービス継続管理の方針を受けて実施する活動があることを理解する。また，運用の資源管理では，サービスを構成する設備，コンピュータシステム，データ，マニュアル，作成した成果物，及びシステムを運用する要員を，組織の目標と適合するように維持，運用する一連の活動であることを理解する。

用語例　システム運用管理，運用の資源管理（要員などの人的資源及びハードウェア，ソフトウェア，データ，ネットワークなどインフラストラクチャの技術的資源），仮想環境の運用管理，ジョブの管理，データ管理，利用者の管理，コールドスタート，ウォームスタート，AIOps

(2) 運用オペレーション

システムを安定稼働させるために，定められた手順に沿ってシステムの監視・操作・状況連絡を実施することを理解する。システムの操作に当たっては，作業指示書に従って実施することを理解する。また，ジョブスケジューリング，アウトプット管理，バックアップといった運用オペレーションの内容を理解する。

用語例　運用オペレーション，スケジュール設計，ジョブスケジューリング，バックアップ，システムの監視と操作，アウトプットの管理，ジョブの復旧と再実行，運用支援ツール（監視ツール，診断ツール），業務運用マニュアル

(3) サービスデスク

サービスデスクは，サービスの利用者からの問合せに対して単一の窓口機能を提供し，適切な部署への引継ぎ，対応結果の記録，記録の管理などを行う一連の活動であることを理解する。

用語例　サービスデスク，SPOC（Single Point Of Contact），コールセンター，CTI（Computer Telephony Integration），FAQ，応対マニュアル，知識ベース，一次サポート，二次サポート及び三次サポート，サービスデスク組織の構造（ローカルサービスデスク，バーチャルサービスデスク，中央サービスデスク，フォロー・ザ・サン），AI の活用（チャットボットなど）

5. ファシリティマネジメント

【目標】
- ファシリティマネジメントの目的，考え方，施設や設備の管理，維持保全における留意事項を修得し，適用する。

(1) ファシリティマネジメント

① ファシリティマネジメントの目的と考え方

コンピュータシステムやネットワークの施設基盤の設計，構築の管理及び運営におけるファシリティマネジメントの目的，考え方を理解する。

用語例　ファシリティマネジメント

② 施設管理・設備管理

データセンターなどの施設やコンピュータ，ネットワークなどの設備の管理によって，費用の削減，快適性，安全性などを確保することを理解する。また，電源や回線の冗長化，バックアップ環境の整備，電源，空調設備，建物などのアクセス管理などを理解する。

用語例　施設管理，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，安全管理関連知識ほか），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，自家発電設備ほか），空調設備（空調機器，エアフロー，コールドアイル，ホットアイルほか），通信設備（MDF，

IDF ほか), データファシリティスタンダード（ティア（Tier）基準）

③ 施設・設備の維持保全

施設・設備を適正な状態に維持保全することを理解する。また，水道光熱費，保守・メンテナンス費，修繕費などを含めたライフサイクル費用の削減を目指して，修繕計画を立案し，施設・設備の長寿命化を図るなど，施設・設備の維持保全の一連の活動を理解する。

用語例 施設・設備の維持保全

④ 環境側面

地球環境に配慮した IT 製品やインフラストラクチャ，環境保護や資源の有効活用につながる IT 利用を理解する。

用語例 環境側面，グリーン IT，データセンター総合エネルギー効率指標（GEC，PUE，ITEE，ITEU ほか), ZEB（net Zero Energy Building），LEED（Leadership in Energy & Environmental Design）認証，GHG プロトコル

大分類 6：サービスマネジメント　中分類 16：システム監査（技術レベル 3）

1.　システム監査

【目標】
- 監査の目的，種類を修得し，適用する。
- システム監査の目的，手順，対象業務についての考え方を修得し，適用する。
- システム監査の計画・実施・報告・フォローアップ，システム監査の体制整備の考え方を修得し，適用する。
- 情報システムに関係する監査で参照される代表的な基準，法規などを修得し，適用する。

(1) 監査業務

情報システムに関係する監査の目的，種類を理解する。

用語例　会計監査，業務監査，システム監査，情報セキュリティ監査，法定監査，任意監査，内部監査，外部監査，立入監査，保証を目的としたシステム監査，助言を目的としたシステム監査

(2) システム監査の目的と手順

① システム監査の目的

システム監査の目的は，情報システムに係るリスク（情報システムリスク）に適切に対応しているかどうかを，高い倫理観をもった，独立かつ客観的な立場のシステム監査人が検証・評価し，もって保証や助言を行うことを通じて，組織体の経営活動と業務活動の効果的かつ効率的な遂行，さらにはそれらの変革を支援し，組織体の目標達成に寄与すること，及び利害関係者に対する説明責任を果たすことであることを理解する。

用語例　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，システム監査に対するニーズの把握と品質の確保，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

② システム監査の流れ

システム監査は，監査計画の策定，監査の実施，監査報告とフォローアップという流れで行われることを理解する。

用語例　リスクの評価に基づく監査計画の策定（リスクアプローチ），監査証拠の入手と評価，監査調書の作成と保管，監査の結論の形成，監査報告書の作成と報告，改善提案のフォローアップ

(3) システム監査の対象業務

システム監査の対象業務は，情報システムのコントロールとマネジメントだけでなく，ガバナンスにまで及ぶことを理解し，さらに，情報システムの企画・開発（アジャイル開発を含む）・運用・保守・廃棄のプロセス，外部サービスの調達・利活用のプロセスなどに及ぶことから，各プロセスで評価する内容を理解する。また，システム監査を実施する目的及び対象範囲は，監査規程，契約書などの文書，監査計画によって明確に定めることを理解する。

用語例　企画プロセスの妥当性，開発・運用・保守プロセスの信頼性・効率性，リスク，コントロール，準拠性，適時性，情報セキュリティ，内部監査規程，システム監査委託契約書

(4) システム監査計画の策定

有効かつ効率的な監査を行うために，システム監査人は監査の目的・テーマ，監査対象範

囲，監査の方法，実施時期，実施体制，実施スケジュールなどの監査計画を策定することを理解する。

用語例 中長期計画，年度計画，個別監査計画

(5) システム監査の実施（予備調査，本調査，評価，結論）

① 予備調査，本調査，結論
予備調査，本調査，結論の形成の一連の監査プロセスを理解する。

② 監査手続の適用
システム監査手続で利用される，代表的なシステム監査技法を理解する。

用語例 チェックリスト法，ドキュメントレビュー法（文書及び記録の収集・閲覧），インタビュー法（質問書・調査票），ウォークスルー法，突合・照合法，現地調査法，統計的サンプリング

③ コンピュータ支援監査技法（CAAT）
監査ソフトウェアなどを利用してシステム監査を実施する，コンピュータ支援監査技法を理解する。

用語例 監査ソフトウェア，データサンプリング，データ分析，テストデータ法，監査モジュール法，ペネトレーションテスト法

④ 監査証拠の入手と評価
監査証拠とは，システム監査人の監査の結論を裏付けるために必要な情報であることを理解する。また，監査の結論を裏付けるためには，適切かつ慎重に監査手続を実施し，十分かつ適切な監査証拠を入手する必要があることを理解する。監査の実施において監査証拠を監査人が円滑に入手できるように，情報システムが構築，整備されていることが望ましいことを理解する。また，監査対応のためだけのドキュメント作成を開発現場に求めるような負荷をかけないよう考慮することが望ましいことを理解する。

用語例 インシデント報告書，進捗管理資料，運用・保守の記録，アクセスログ，トランザクションログ，監査証跡，監査証拠

⑤ 監査調書の作成と保管
システム監査人は，調査，収集，検証・評価した情報を，監査の結論に至った過程が分かるよう整理して文書化した監査調書を作成，保管し，監査報告書を作成するときの基礎資料や監査結果の裏付けとすることを理解する。

⑥ 他の監査との連携・調整
システム監査は，公認会計士による監査，監査役などによる監査，内部監査人による監査などと関係があることを理解する。

用語例 法定監査，任意監査，金融商品取引法監査，会社法監査，経営監査，業務監査，会計監査，内部監査，外部監査，内部監査基準，専門職的実施の国際フレームワーク（IPPF）

(6) システム監査の報告とフォローアップ

システム監査人は，監査目的に応じた適切な形式で，監査結果を監査の依頼者や適切な関係者に報告すること，報告書に記載した改善提案又は監査対象先が作成した改善計画について，所要の措置が適切かつ適時に実施されているかどうかのフォローアップを行うことを理解する。

用語例　システム監査報告書，指摘事項，保証を目的としたシステム監査，助言を目的としたシステム監査，改善提案，改善計画，フォローアップ，フォローアップ報告書

(7) システム監査の体制整備

システム監査に対するニーズを満たしているかどうかを含め，一定の監査品質を確保するための体制の整備・運用が必要であることを理解する。

用語例　システム監査人の権限と責任などの明確化，専門的能力の保持と向上，正当な注意と秘密の保持，システム監査に対するニーズの把握と品質の確保，監査の独立性と客観性の保持

(8) その他のシステム関連の監査

① 情報セキュリティ監査

情報セキュリティ監査の目的，役割を理解する。

用語例　情報セキュリティ監査基準，情報セキュリティ管理基準，クラウド情報セキュリティ管理基準

② 個人情報保護監査

個人情報保護監査の目的，役割を理解する。

用語例　個人情報の保護，情報漏えいリスク

③ コンプライアンス監査

コンプライアンス監査の目的，役割を理解する。

用語例　行動指針，職務分掌，倫理，透明性

④ マネジメントシステム監査

品質，環境，サービス，情報セキュリティ，事業継続などの各種マネジメントシステムを対象とするマネジメントシステム監査の目的，役割を理解する。

用語例　JIS Q 19011（マネジメントシステム監査のための指針）

(9) 情報システムに関係する監査関連法規

① システム監査基準・システム管理基準

システム監査における監査人の倫理は，経済産業省が策定したシステム監査基準によって規定されていることを理解する。また，システム監査の判断尺度を確定する際の客観的な参照基準として，経済産業省が策定したシステム管理基準などを用いることができることを理解する。

用語例　監査人の倫理，システム監査上の判断尺度，監査の独立性と客観性の保持，正当な注意と秘密の保持

② 情報セキュリティ関連法規

情報セキュリティに関する法律，情報セキュリティ監査の対象組織，情報システムに及ぼす影響を理解する。

用語例　刑法（電磁的記録不正作出及び供用，電子計算機損壊等業務妨害，電子計算機使用詐欺），不正アクセス行為の禁止等に関する法律，電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律，電子署名及び認証業務

に関する法律，JIS Q 27001，ISMS 適合性評価制度

③ 個人情報保護関連法規
個人情報保護に関する法律やガイドライン，個人情報保護におけるシステム監査の役割を理解する。

用語例 個人情報保護法，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，JIS Q 15001，プライバシーマーク制度

④ 知的財産権関連法規
知的財産権に関する法律，システム監査では権利侵害行為を指摘する必要性があることを理解する。

用語例 著作権法，特許法，不正競争防止法，営業秘密管理指針

⑤ 労働関連法規
労働に関する法律，システム監査では法律に照らして労働環境における問題点を指摘する必要があることを理解する。

用語例 労働基準法，労働者派遣法，男女雇用機会均等法

⑥ 法定監査関連法規
システム監査は法定監査との連携を図りながら実施する必要があることを理解する。

用語例 金融商品取引法，会社法

2. 内部統制

【目標】
➢ 企業などにおける内部統制，IT ガバナンスの目的，考え方を修得し，適用する。

(1) 内部統制

内部統制とは，健全かつ効率的な組織運営のための体制を企業などが自ら構築し運用する仕組みであり，実現には業務プロセスの明確化，職務分掌，実施ルールの設定，チェック体制の確立が必要であることを理解する。また，IT が内部統制に果たす役割，内部統制の六つの基本的要素を理解する。

用語例 内部統制の限界，内部統制報告制度，財務報告に係る内部統制の評価及び監査の基準，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），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），システム管理基準追補版（財務報告に係る IT 統制ガイダンス），全社的な内部統制，業務プロセスの明確化，職務分掌，実施ルールの設定，チェック体制の確立，コンプライアンス，COSO（Committee of Sponsoring Organizations of the Treadway Commission）フレームワーク，ERM（全社的リスクマネジメント）

(2) IT ガバナンス

IT ガバナンスとは，組織体のガバナンスの構成要素で，取締役会等がステークホルダのニーズに基づき，組織体の価値及び組織体への信頼を向上させるために，組織体における IT の利活用のあるべき姿を示す IT 戦略と方針の策定及びその実現のための活動であることを理解する。また，システム監査，情報セキュリティ監査，ソフトウェア資産管理など IT ガバナンスを実現するための取組を理解する。また，IT ガバナンスの評価のために使用されるフレームワークを理解する。

用語例　JIS Q 38500，CIO（Chief Information Officer：最高情報責任者），CISO（Chief Information Security Officer：最高情報セキュリティ責任者），IT 統制，データガバナンス，コーポレートガバナンス，COBIT，PRM-IT（Process Reference Model for IT），成熟度モデル

(3) 法令遵守状況の評価・改善

情報システムの構築・運用は，当該業務システムに関わる法令を遵守して行わなければならないこと，適切なタイミングと方法で法令，基準，自社内外の行動規範の遵守状況を継続的に評価し，改善していく必要があること，内部統制を整備することが法令遵守の体制を確立する上で有効であることを理解する。

用語例　会社法，金融商品取引法，コンプライアンス監査，CSA（Control Self Assessment：統制自己評価）

情報処理安全確保支援士試験
シラバス 追補版（午前Ⅱ）　Ver.4.0

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/

2023.12