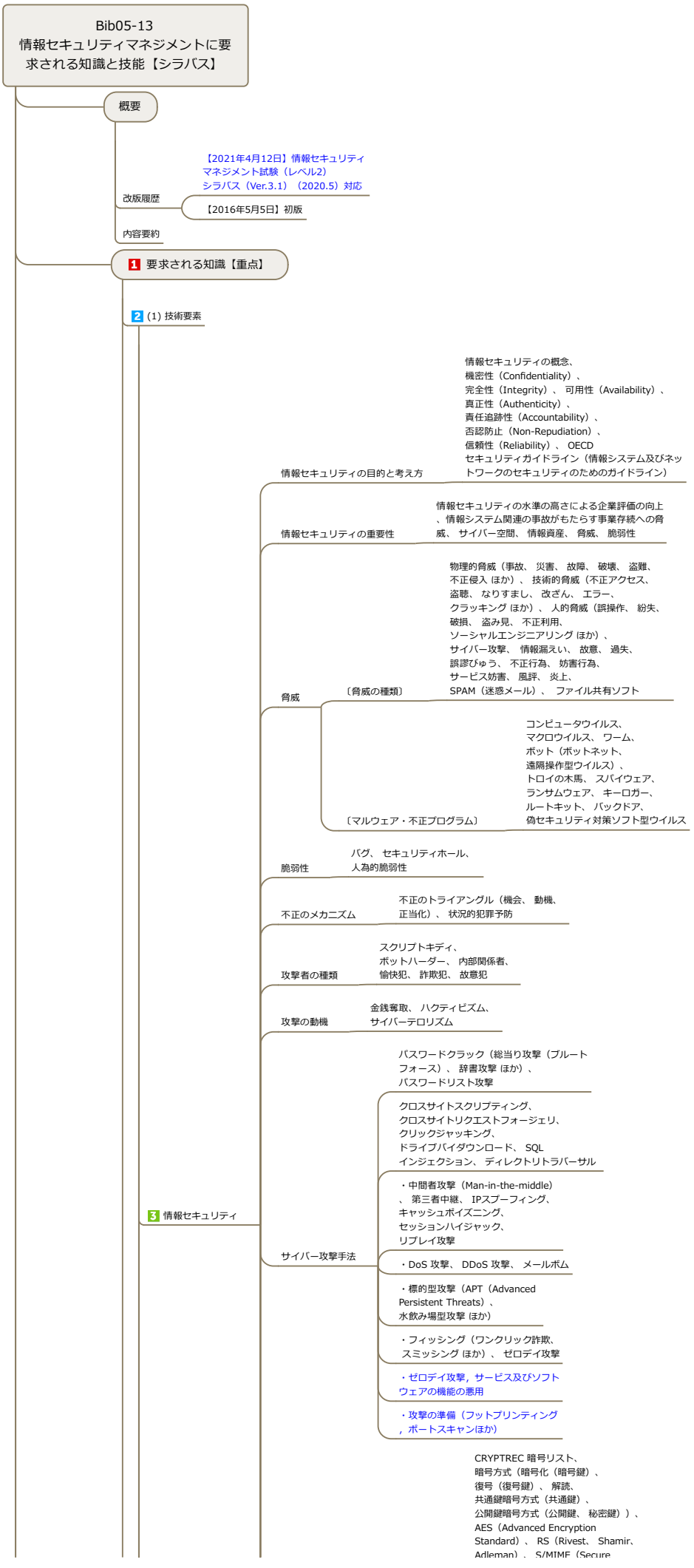

Bib05-13
情報セキュリティマネジメントに要求される知識と技能【シラバス】
概要
改版履歴
【2021年4月12日】情報セキュリティマネジメント試験（レベル2）シラバス（Ver.3.1）（2020.5）対応
【2016年5月5日】初版
内容要約
1 要求される知識【重点】
2 (1) 技術要素
情報セキュリティの目的と考え方
情報セキュリティの概念、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）、真正性（Authenticity）、責任追跡性（Accountability）、否認防止（Non-Repudiation）、信頼性（Reliability）、OECD 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）
情報セキュリティの重要性
情報セキュリティの水準の高さによる企業評価の向上、情報システム関連の事故がもたらす事業存続への脅威、サイバー空間、情報資産、脅威、脆弱性
脅威
〔脅威の種類〕
物理的脅威（事故、災害、故障、破壊、盗難、不正侵入 ほか）、技術的脅威（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 ほか）、人的脅威（誤操作、紛失、破損、盗み見、不正利用、ソーシャルエンジニアリング ほか）、サイバー攻撃、情報漏えい、故意、過失、誤謬びゅう、不正行為、妨害行為、サービス妨害、風評、炎上、SPAM（迷惑メール）、ファイル共有ソフト
〔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、ワーム、ボット（ボットネット、遠隔操作型ウイルス）、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、偽セキュリティ対策ソフト型ウイルス
脆弱性
バグ、セキュリティホール、人為的脆弱性
不正のメカニズム
不正のトライアングル（機会、動機、正当化）、状況的犯罪予防
攻撃者の種類
スクリプトキディ、ボットハーダー、内部関係者、愉快犯、詐欺犯、故意犯
攻撃の動機
金銭奪取、ハクティビズム、サイバーテロリズム
サイバー攻撃手法
パスワードクラック（総当り攻撃（ブルートフォース）、辞書攻撃 ほか）、パスワードリスト攻撃
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、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、ディレクトリトラバーサル
・中間者攻撃（Man-in-the-middle）、第三者中継、IPスプーフィング、キャッシュポイズニング、セッションハイジャック、リプレイ攻撃
・DoS 攻撃、DDoS 攻撃、メールボム
・標的型攻撃（APT（Advanced Persistent Threats）、水飲み場型攻撃 ほか）
・フィッシング（ワンクリック詐欺、スミッシング ほか）、ゼロデイ攻撃
・ゼロデイ攻撃，サービス及びソフトウェアの機能の悪用
・攻撃の準備（フットプリンティング，ポートスキャンほか）
3 情報セキュリティ
CRYPTREC 暗号リスト、暗号方式（暗号化（暗号鍵）、復号（復号鍵）、解読、共通鍵暗号方式（共通鍵）、公開鍵暗号方式（公開鍵、秘密鍵））、AES（Advanced Encryption Standard）、RS（Rivest、Shamir、Adleman）、S/MIME（Secure

- 情報セキュリティ技術（暗号技術）
  - MIME）、 PGP（Pretty Good Privacy）、
    ハイブリッド暗号、
    ハッシュ関数（SHA-256 ほか）、
    鍵管理、 ディスク暗号化、
    ファイル暗号化、 危殆化
- 情報セキュリティ技術（認証技術）
  - ディジタル署名（署名鍵、
    検証鍵）、
    タイムスタンプ(時刻認証)、
    メッセージ認証、 MAC（Message
    Authentication
    Code：メッセージ認証符号）、
    チャレンジレスポンス認証，リスクベース認
    証
- 情報セキュリティ技術（利用者認証）
  - 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、
    ワンタイムパスワード、
    多要素認証、 シングルサインオン、
    CAPTCHA、 パスワードリマインダ、
    パスワード管理ツール
- 情報セキュリティ技術（生体認証技術）
  - 静脈パターン認証、 虹彩認証、
    声紋認証、 顔認証、 網膜認証、
    署名認証、 本人拒否率、 他人受入率
- 情報セキュリティ技術（公開鍵基盤）
  - PKI（Public Key
    Infrastructure：公開鍵基盤）、
    ディジタル証明書（公開鍵証明書）、
    ルート証明書、 サーバ証明書、
    クライアント証明書、
    CRL（Certificate Revocation
    List：証明書失効リスト）

3 情報セキュリティ管理

- 情報セキュリティ管理
  - 情報セキュリティポリシに基づく情報
    の管理、 情報、 情報資産、
    物理的資産、 ソフトウェア資産、
    人的資産（人、
    保有する資格・技能・経験）、
    無形資産、 サービス、
    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
- リスク分析と評価（情報資産の調査・分類）
  - 情報資産の調査、
    情報資産の重要性による分類と管理、
    情報資産台帳
- リスク分析と評価（リスクの種類）
  - 財産損失、 責任損失、
    純収益の喪失、 人的損失、
    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、
    モラルハザード、 年間予想損失額、
    得点法、 コスト要因
- リスク分析と評価（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
- リスク分析と評価（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、
    リスクファイナンシング、
    情報化保険、 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
- 情報セキュリティ継続
  - 緊急事態の区分、
    緊急時対応計画（コンティンジェンシープラン）、 復旧計画、 災害復旧、
    障害復旧、 バックアップ対策、
    被害状況の調査手法
- 情報セキュリティ諸規程（情報セキュリティポリシを含む組織内規程）
  - 情報セキュリティポリシに従った組織運営，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（個人情報保護方針），雇用契約，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）
- ISMS 適用範囲、 リーダシップ、
  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、
  管理策（情報セキュリティインシデン

- 情報セキュリティマネジメントシステム（ISMS）
  - ト管理、情報セキュリティの教育及び訓練、法的及び契約上の要求事項の順守ほか）、 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（ISO/IEC 27014）
- 3 セキュリティ技術評価
  - セキュリティ評価
    - PCI DSS、 CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）、脆弱性検査、ペネトレーションテスト
- 3 情報セキュリティ対策
  - 人的セキュリティ対策
    - 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、訓練、 資料配付、 メディア活用）、パスワード管理、利用者アクセスの管理（アカウント管理、 特権的アクセス権の管理、need-to-know（最小権限）ほか）、 ログ管理、 監視
  - 技術的セキュリティ対策
    - 〔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，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），出口対策，入口対策，多層防御，秘匿化，アクセス制御，脆弱性管理（OSアップデート，脆弱性修正プログラムの適用ほか），ネットワーク監視，ネットワークアクセス権の設定，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（SPAM 対策，URLフィルタリング，コンテンツフィルタリング），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，無線LANセキュリティ，クラウドサービスのセキュリティ，IoTのセキュリティ，電子透かし，ディジタルフォレンジックス（証拠保全 ほか）
    - 〔セキュリティ製品・サービス〕
      - マルウェア対策ソフト，DLP（Data Loss Prevention），SIEM（Security Information and Event Management），ファイアウォール，WAF（Web Application Firewall），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），ホワイトリスト，ブラックリスト，フォールスネガティブ，フォールスポジティブ，SSLアクセラレータ，MDM（Mobile Device Management）
  - 物理的セキュリティ対策
    - 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，監視カメラ，施錠管理，入退室管理，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
- 3 セキュリティ実装技術
  - セキュアプロトコル
    - IPsec，TLS，SSL/TLS，SSH，HTTP over TLS（HTTPS），WPA2，WPA3，PGP（Pretty Good Privacy），S/MIME（Secure MIME），SPF
  - ネットワークセキュリティ
    - 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、認証サーバ、 認証VLAN、VPN（Virtual Private Network：仮想私設網）、セキュリティ監視、 ハニーポット、リバースプロキシ
  - データベースセキュリティ
    - 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
  - アプリケーションセキュリティ
    - Web システムのセキュリティ対策、セキュリティバイデザイン，プライバシーバイデザイン，セキュアプログラミング、バッファオーバフロー対策、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
- 2 (2) 企業と法務
- 3 知的財産権
  - 知的財産権
    - 著作権法（著作権、 権利侵害、保護対象）、 コピープロテクト外し
  - 不正競争防止法
    - 営業秘密、 ドメイン名の不正取得
- サイバーセキュリティ基本法
  - サイバーセキュリティ基本法
    - サイバーセキュリティ基本法，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
    - アクセス制御機能、不正アクセス行為

- 不正アクセス禁止法
  - 不正アクセス行為を助長する行為
- 個人情報保護法
  - 個人情報保護に関するガイドライン，個人情報取扱事業者，安全管理措置，要配慮個人情報，特定個人情報の適正な取扱いに関するガイドライン，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），個人情報保護委員会，JIS Q 15001，プライバシーマーク，OECDプライバシーガイドライン（プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告），プライバシー影響アセスメント（PIA），プライバシーフレームワーク，一般データ保護規則（GDPR），オプトイン，オプトアウト，第三者提供，匿名化手法（サンプリング，k-匿名化），匿名加工情報
- 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
- その他のセキュリティ関連法規
  - 電子署名及び認証業務等に関する法律（認定認証事業者、 電子証明書）、プロバイダ責任制限法、特定電子メール法
- 情報セキュリティに関する基準
  - 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，ソフトウェア等脆弱性関連情報取扱基準，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，コンシューマ向けIoT セキュリティガイド，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，スマートフォン安全安心強化戦略

3 セキュリティ関連法規

- 労働関連の法規（労働基準法
  - 就業規則
- 労働関連の法規（労働者派遣法）
  - 労働者、 派遣先、 派遣元、派遣契約、 雇用契約、 指揮命令
- 企業間の取引にかかわる契約
  - 準委任契約、 請負契約、 守秘契約、ソフトウェア使用許諾契約（ボリュームライセンス契約、コピーレフト（Copyleft））、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）

3 労働関連・取引関連法規

3 その他の法律・ガイドライン・技術者倫理

- その他の法律・ガイドライン・技術者倫理
  - その他の法律（IT 基本法、e-文書法（電磁的記録）、電子帳簿保存法）、コンプライアンス、情報倫理・技術者倫理

3 標準化関連

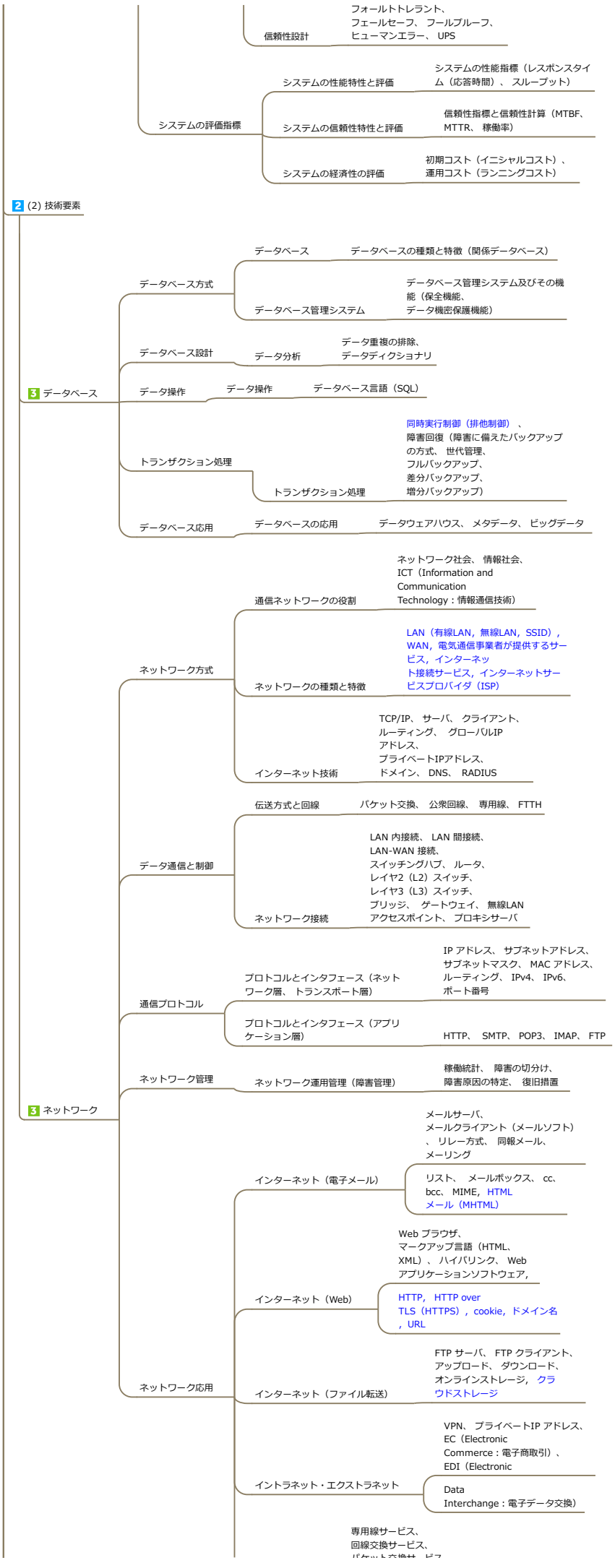
- 標準・規格と標準化団体
  - JIS（Japanese Industrial Standards：日本工業規格）、IS（International Standards：国際規格）、ISO（International Organization for Standardization：国際標準化機構）、IEEEなどの関連機構の役割、デジュレスタンダード、デファクトスタンダード

1 要求される知識【その他の分野】

2 (1) コンピュータシステム

3 システム構成要素

- システムの処理形態・利用形態
  - 集中処理、 分散処理、 対話型処理、利用形態（バッチ処理、リアルタイム処理）
- システムの構成
  - システム構成
    - 機能配分，冗長構成，負荷分散，デュアルシステム，デュプレックスシステム，クラスタ，主系（現用系），従系（待機系），クライアントサーバシステム（クライアント，サーバ），シンクライアント，仮想化，VM（Virtual Machine：仮想マシン），VDI（Virtual Desktop Infrastructure：デスクトップ仮想化），Web システム（Web ブラウザ，Web サーバ），ピアツーピア，クラウドコンピューティング，SaaS，PaaS，IaaS，エッジコンピューティング
  - ストレージの構成
    - RAID、 NAS、 SAN


信頼性設計
フォールトトレラント、
フェールセーフ、 フールプルーフ、
ヒューマンエラー、 UPS
システムの評価指標
システムの性能特性と評価
システムの性能指標（レスポンスタイム（応答時間）、 スループット）
システムの信頼性特性と評価
信頼性指標と信頼性計算（MTBF、MTTR、 稼働率）
システムの経済性の評価
初期コスト（イニシャルコスト）、
運用コスト（ランニングコスト）
2 (2) 技術要素
3 データベース
データベース方式
データベース
データベースの種類と特徴（関係データベース）
データベース管理システム
データベース管理システム及びその機能（保全機能、
データ機密保護機能）
データベース設計
データ分析
データ重複の排除、
データディクショナリ
データ操作
データ操作
データベース言語（SQL）
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）、
障害回復（障害に備えたバックアップの方式、 世代管理、
フルバックアップ、
差分バックアップ、
増分バックアップ）
データベース応用
データベースの応用
データウェアハウス、 メタデータ、 ビッグデータ
3 ネットワーク
ネットワーク方式
通信ネットワークの役割
ネットワーク社会、 情報社会、
ICT（Information and Communication
Technology：情報通信技術）
ネットワークの種類と特徴
LAN（有線LAN，無線LAN，SSID），
WAN，電気通信事業者が提供するサービス，インターネット
ト接続サービス，インターネットサービスプロバイダ（ISP）
インターネット技術
TCP/IP、 サーバ、 クライアント、
ルーティング、 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、 DNS、 RADIUS
データ通信と制御
伝送方式と回線
パケット交換、 公衆回線、 専用線、 FTTH
ネットワーク接続
LAN 内接続、 LAN 間接続、
LAN-WAN 接続、
スイッチングハブ、 ルータ、
レイヤ2（L2）スイッチ、
レイヤ3（L3）スイッチ、
ブリッジ、 ゲートウェイ、 無線LAN
アクセスポイント、 プロキシサーバ
通信プロトコル
プロトコルとインタフェース（ネットワーク層、 トランスポート層）
IP アドレス、 サブネットアドレス、
サブネットマスク、 MAC アドレス、
ルーティング、 IPv4、 IPv6、
ポート番号
プロトコルとインタフェース（アプリケーション層）
HTTP、 SMTP、 POP3、 IMAP、 FTP
ネットワーク管理
ネットワーク運用管理（障害管理）
稼働統計、 障害の切分け、
障害原因の特定、 復旧措置
ネットワーク応用
インターネット（電子メール）
メールサーバ、
メールクライアント（メールソフト）、 リレー方式、 同報メール、
メーリング
リスト、 メールボックス、 cc、
bcc、 MIME，HTML
メール（MHTML）
インターネット（Web）
Web ブラウザ、
マークアップ言語（HTML、XML）、 ハイパリンク、 Web
アプリケーションソフトウェア，
HTTP，HTTP over
TLS（HTTPS），cookie，ドメイン名
，URL
インターネット（ファイル転送）
FTP サーバ、 FTP クライアント、
アップロード、 ダウンロード、
オンラインストレージ，クラウドストレージ
イントラネット・エクストラネット
VPN、 プライベートIP アドレス、
EC（Electronic
Commerce：電子商取引）、
EDI（Electronic
Data
Interchange：電子データ交換）
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、
インターネットサービス、 IP電話、
モバイル通信、
移動体通信規格（LTE など）、
デザリング、 広域Ethernet、
IP-VPN、 インターネットVPN、
VoIP（Voice over Internet
Protocol）、 ベストエフォート

通信サービス

2 (3) プロジェクトマネジメント

3 プロジェクトマネジメント

プロジェクトマネジメント

プロジェクト，プロジェクトマネジメント，プロジェクトの環境，プロジェクトガバナンス，
プロジェクトライフサイクル，プロジェクトの体制，プロジェクトの自己管理（変更管理，
問題発見，問題報告，対策立案，文書化）

PDCAサイクルがなくなる

3 プロジェクトの統合

プロジェクトの統合

プロジェクト憲章の作成，プロジェクト作業の管理，プロジェクトフェーズ又はプロジェクトの終結，得た教訓の収集，ベースライン

3 プロジェクトのステークホルダ

プロジェクトのステークホルダ

ステークホルダの特定，ステークホルダのマネジメント

3 プロジェクトのスコープ

プロジェクトのスコープ

スコープの定義，WBSの作成，活動の定義，スコープの管理

3 プロジェクトの資源

プロジェクトの資源

資源の対象群が含むプロセス（資源の見積り，プロジェクトチームのマネジメント）

3 プロジェクトの時間

プロジェクトの時間

時間の対象群が含むプロセス（活動の順序付け，活動期間の見積り，スケジュールの作成），
活動リスト，PERT

3 プロジェクトのコスト

プロジェクトのコスト

コストの管理，コストベースライン

3 プロジェクトのリスク

プロジェクトのリスク

プロジェクトの全体リスクと個別リスク，リスクの対象群が含むプロセス（リスクの特定，
リスクの評価，リスクへの対応，リスクの管理）

3 プロジェクトの品質

プロジェクトの品質

品質管理の遂行，検査報告書

3 プロジェクトの調達

プロジェクトの調達

調達の対象群が含むプロセス（調達の計画，供給者の選定，調達の運営管理）

3 プロジェクトのコミュニケーション

プロジェクトのコミュニケーション

コミュニケーションのマネジメント，
代表的な情報配布の方法（双方向コミュニケーション，
プッシュ型コミュニケーション，プル型コミュニケーション，電子メール，
ボイスメール，
テレビ会議，紙面）

2 (4) サービスマネジメント

サービスマネジメント

SLA

サービスレベル合意書（SLA），顧客満足，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，サービスマネジメントシステム

サービスマネジメントシステムの計画及び運用

サービスの計画

サービスの要求事項

サービスカタログ管理

サービスカタログ

資産管理，構成管理

資産管理，ライセンスマネジメント，
構成管理，構成品目（CI）

事業関係管理，サービスレベル管理，
供給者
管理

サービス満足度，サービスレベル管理，サービスレベル目標，供給者管理，
外部供給者，契
約，内部供給者

需要管理，容量・能力管理

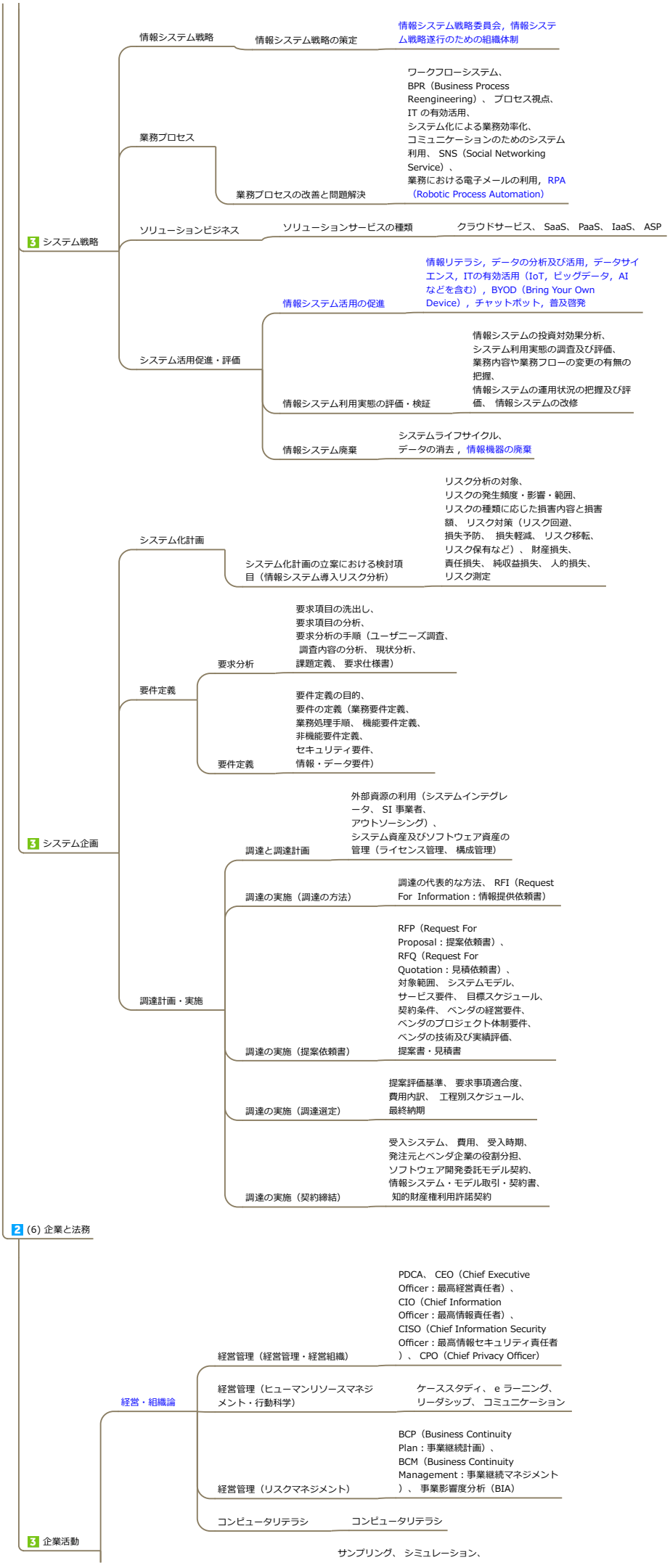
需要管理，容量・能力（キャパシティ）管理，監視，管理指標（CPU
使用率，メモリ使用率，
ディスク使用率，ネットワーク利用率），しきい（閾）値

変更管理，サービスの設計及び移行，
リリー
ス及び展開管理

変更管理，変更によるサービスへの影響，サービス受入れ基準，サービス設計書，非機能要
件，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，リリース及び展開
管理

インシデント管理，インシデント，影響，サービス要求，エスカレーション，回避策，重大
なインシデント，ヒヤリハット，サービス要求管理，問題管理（問題，既知

- 3 サービスマネジメント
  - 【削除】サービスの設計・移行
    - サービスの設計・移行
      - サービス受入れ基準、サービス設計書、 非機能要件、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
  - 【削除】サービスマネジメントプロセス
    - サービスレベル管理
      - サービスレベル管理、サービス目標、 レビュー、サービス改善計画、サービスカタログ
    - サービスの報告
      - サービスの報告、サービス目標に対するパフォーマンス、 傾向情報
    - サービス継続及び可用性管理
      - サービス継続及び可用性管理、サービス継続計画、 RTO、 RPO、復旧（障害復旧、 災害復旧）、コールドスタンバイ、ホットスタンバイ、 可用性、信頼性、 保守性
    - キャパシティ管理
      - キャパシティ管理、 監視、管理指標（CPU 使用率、メモリ使用率、 ファイル使用量、ネットワーク利用率）、しきい（閾）値
    - 供給者管理
      - 供給者管理、 供給者、 契約、内部グループ、運用レベル合意書（OLA）
    - インシデント及びサービス要求管理
      - インシデント及びサービス要求管理、インシデント、 影響範囲、サービス要求、 段階的取扱い、回避策、 重大なインシデント、ヒヤリハット
    - 問題管理・構成管理・変更管理・リリース及び展開管理
      - 問題管理（問題、 既知の誤り、根本原因、 予防処置、 傾向分析）、構成管理（資産管理）、変更管理（変更管理、変更によるサービスへの影響）、リリース及び展開管理（構成管理及び変更管理との連携）
  - パフォーマンス評価及び改善
    - パフォーマンス評価
      - パフォーマンス評価，サービスの報告，（サービスレベル目標に対する）パフォーマンス，傾向情報
    - 改善
      - 不適合及び是正処置，継続的改善
  - サービスの運用
    - サービスの運用
      - システム運用管理、運用オペレーション（システムの監視・操作・状況連絡、 作業指示書、操作ログ）、サービスデスク（利用者からの問合せ）
  - ファシリティマネジメント
    - ファシリティマネジメント
      - ファシリティマネジメント、施設管理、設備管理（電源・空調設備ほか）、UPS
- 3 システム監査
  - システム監査
    - システム監査の目的と手順
      - 情報システムの総合的な点検・評価・検証（安全性，信頼性，準拠性，戦略性，効率性，有効性），システム監査の体制整備，システム監査人の独立性・客観性・慎重な姿勢，システム監査計画策定，システム監査実施（監査証拠の入手と評価ほか），システム監査報告とフォローアップ
    - 情報セキュリティ監査
      - 情報セキュリティ監査基準、情報セキュリティ管理基準
    - コンプライアンス監査
      - 行動指針、 倫理、 透明性、権利侵害行為への指摘、労働環境における問題点への指摘
  - 内部統制
    - 内部統制
      - 職務分掌，相互牽制（職務の分離），実施ルールの設定，チェック体制の確立，ITが内部統制に果たす役割，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統制（IT全般統制，IT業務処理統制），ITガバナンス，EDMモデル
    - 法令順守状況の評価・改善
      - 基準・自社内外の行動規範の順守状況の継続的な評価、 内部統制の整備、CSA（Control Self Assessment：統制自己評価）
- 2 (5) システム戦略


情報システム戦略
情報システム戦略の策定
情報システム戦略委員会，情報システム戦略遂行のための組織体制
業務プロセス
業務プロセスの改善と問題解決
ワークフローシステム、BPR（Business Process Reengineering）、プロセス視点、IT の有効活用、システム化による業務効率化、コミュニケーションのためのシステム利用、SNS（Social Networking Service）、業務における電子メールの利用，RPA（Robotic Process Automation）
ソリューションビジネス
ソリューションサービスの種類
クラウドサービス、SaaS、PaaS、IaaS、ASP
3 システム戦略
システム活用促進・評価
情報システム活用の促進
情報リテラシ，データの分析及び活用，データサイエンス，ITの有効活用（IoT，ビッグデータ，AIなどを含む），BYOD（Bring Your Own Device），チャットボット，普及啓発
情報システム利用実態の評価・検証
情報システムの投資対効果分析、システム利用実態の調査及び評価、業務内容や業務フローの変更の有無の把握、情報システムの運用状況の把握及び評価、情報システムの改修
情報システム廃棄
システムライフサイクル、データの消去，情報機器の廃棄
システム化計画
システム化計画の立案における検討項目（情報システム導入リスク分析）
リスク分析の対象、リスクの発生頻度・影響・範囲、リスクの種類に応じた損害内容と損害額、リスク対策（リスク回避、損失予防、損失軽減、リスク移転、リスク保有など）、財産損失、責任損失、純収益損失、人的損失、リスク測定
要件定義
要求分析
要求項目の洗出し、要求項目の分析、要求分析の手順（ユーザニーズ調査、調査内容の分析、現状分析、課題定義、要求仕様書）
要件定義
要件定義の目的、要件の定義（業務要件定義、業務処理手順、機能要件定義、非機能要件定義、セキュリティ要件、情報・データ要件）
3 システム企画
調達計画・実施
調達と調達計画
外部資源の利用（システムインテグレータ、SI 事業者、アウトソーシング）、システム資産及びソフトウェア資産の管理（ライセンス管理、構成管理）
調達の実施（調達の方法）
調達の代表的な方法、RFI（Request For Information：情報提供依頼書）
調達の実施（提案依頼書）
RFP（Request For Proposal：提案依頼書）、RFQ（Request For Quotation：見積依頼書）、対象範囲、システムモデル、サービス要件、目標スケジュール、契約条件、ベンダの経営要件、ベンダのプロジェクト体制要件、ベンダの技術及び実績評価、提案書・見積書
調達の実施（調達選定）
提案評価基準、要求事項適合度、費用内訳、工程別スケジュール、最終納期
調達の実施（契約締結）
受入システム、費用、受入時期、発注元とベンダ企業の役割分担、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、知的財産権利用許諾契約
2 (6) 企業と法務
経営・組織論
経営管理（経営管理・経営組織）
PDCA、CEO（Chief Executive Officer：最高経営責任者）、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）、CPO（Chief Privacy Officer）
経営管理（ヒューマンリソースマネジメント・行動科学）
ケーススタディ、e ラーニング、リーダシップ、コミュニケーション
経営管理（リスクマネジメント）
BCP（Business Continuity Plan：事業継続計画）、BCM（Business Continuity Management：事業継続マネジメント）、事業影響度分析（BIA）
コンピュータリテラシ
コンピュータリテラシ
3 企業活動
サンプリング、シミュレーション、

- 検査手法・品質管理手法
  - QC 七つ道具、 新QC 七つ道具
- OR・IE
- 業務分析・業務計画
  - データマイニング、ブレーンストーミング、デルファイ法、 デシジョンツリー
- 企業活動と会計
  - 固定費、 変動費、 原価、 利益、粗利益、 営業利益、 変動費率、損益分岐点、 減価償却、 リース、レンタル
- 会計・財務
- 財務諸表
  - 貸借対照表、キャッシュフロー計算書、資産（純資産、 流動資産、固定資産、 繰延資産、 有形資産、無形資産）、 負債（流動負債、固定負債）、 流動比率

1 要求される技能

2 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

3 情報資産管理の計画

- 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、 文書精査、ヒアリングなどによって価値を明確化できる。
  - 用語知識：情報資産、価値（重要度）、 3特性（機密性、完全性、 可用性）
- 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、部門における情報資産の管理方針と管理体制を検討できる。
  - また、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、自らルールを検討して提案できる。
  - 用語知識：情報資産受入れ、変更管理、 利用管理、 廃棄管理、管理体制
- 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、作成できる。
  - 用語知識：情報資産台帳、資産の棚卸

3 情報セキュリティリスクアセスメント及びリスク対応

- 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、物理的な要因、 技術的な要因、人的な要因の側面から分析する、また、 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、組織が定めたリスク受容基準に基づく評価を実施できる。
  - また、 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も、 それらを特定し、同様に評価できる。
  - 用語用語：脅威、 脆弱性、サイバー攻撃（標的型攻撃、ゼロデイ攻撃ほか）、 資産の価値、物理的な要因、 技術的な要因、人的な要因、 事象の起こりやすさ、結果（損害の大きさ）、リスク受容基準
- 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、 それぞれ物理的対策、人的（管理的）対策、技術的対策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、リスク対応策を検討できる。 また、検討した対応策について、現状の実施状況を把握できる。
  - 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、（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できる。
  - 用語知識：リスク対応策、物理的対策、 人的（管理的）対策、技術的対策、 残留リスク

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、
リスク対応計画を作成できる。

リスク対応計画の策定

用語知識：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、
情報化保険、 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、 リスク対応計画

情報資産を保護するための物理的及び環境的セキュリティの考え方、
仕組みを理解した上で、
執務場所への入退管理方法、
情報資産の持込み・持出し管理方法、
ネットワークの物理的な保護方法、
情報セキュリティを維持すべき対象（モバイル機器を含む）の範囲を検討し、
リスク対応計画に基づく要求事項の取りまとめを実施できる。

物理的及び環境的セキュリティ

用語知識：入退管理方法、
持込み・持出し管理、
ネットワーク、 モバイル機器

情報資産を保護するための技術的及び運用のセキュリティの考え方、
仕組みを理解し、
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できる。

3 情報資産に関する情報セキュリティ要求事項の提示

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

要求事項には、
次のような項目がある。

部門で開発・取得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

部門の情報システムに関する技術的及び運用のセキュリティ

また、
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できる。

用語知識：アクセス制御、
業務上の要求事項、
利用者アクセスの管理、
情報セキュリティ要求事項、
開発及びサポートプロセス、
受入れテスト、 試験データ

障害又は災害発生時において、
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、
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できる。

3 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

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

もし過不足がある場合は、
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）を提案できる。

用語知識：障害、 災害、
事業継続マネジメント、
情報セキュリティ継続

2 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

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できる。

情報資産台帳の維持管理

用語知識：情報セキュリティポリシ、
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、 廃棄

3 情報資産の管理

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、
あらかじめ定められた手順を部門のメンバが適切に実施するためのアドバイスができる。

媒体の管理

用語知識：媒体の持込み・持出し、
廃棄、 可搬媒体（USB メモリ、
DVD、 ハードディスクなど）

情報資産を管理することの必要性、

- 利用状況の記録
  - 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できる。
  - 用語知識：情報資産の配置、
    管理者、 構成の変更
- 3 部門の情報システム利用時の情報セキュリティの確保
  - 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、
      マルウェアやウイルス対策ソフトについて、 部門のメンバの理解を深め、
      情報セキュリティ諸規程の順守を促進できる。
    - 用語知識：マルウェア、
      コンピュータウイルス、
      トロイの木馬、 ワーム、
      ウイルス対策ソフト
  - 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、
      バックアップの重要性について、
      部門のメンバの理解を深め、
      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できる。
    - 用語知識：バックアップ（取得サイクル、
      保持場所）、 リストア
  - 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、
      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できる。
    - 用語知識：ログの監視、 記録、
      分析、 保持方法
  - 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、
      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、
      部門のメンバが転送する情報の内容確認、
      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できる。
    - 用語知識：電子メール、 ファイル、
      閲覧サイト、 機器の持込み・持出し
  - 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、
      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できる。
    - 用語知識：脆弱性管理、
      パッチ管理、 パッチ適用基準
  - 利用者アクセスの管理
    - 情報システムや執務場所その他の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、
      部門メンバ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できる。
    - 用語知識：認証方式、 パスワード、
      パスワード強度、 変更サイクル、
      変更手法、 生体認証、 IC カード、
      トークン、 アクセス権限
  - 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、
      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できる。
    - また、
      不適切と思われる事項を発見した場合は、 上位者に報告・相談し、
      適切に対処することができる。
    - 用語知識：情報セキュリティポリシ、
      監視、 測定、 分析、 評価、
      脆弱性検査、 侵入検査
  - 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、
      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かい離を、
      契約担当者と協力しつつ事前確認できる。
    - 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つつ実施できる。
    - 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つつ確認できる。
- 用語知識：委託先管理、情報取扱いルール、情報セキュリティ要求事項

- 業務の外部委託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の実施
    - 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、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、 契約内容との齟齬の解消を、契約担当者と協力しつつ実施できる。
    - 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つつ確認できる。
    - 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つつ実施できる。
    - 用語知識：委託先管理、不正防止・機密保護、 機密保持契約
  - 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、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つつ実施できる。
    - 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、上位者に報告できる。
    - 用語知識：検収、 廃棄、システムライフサイクル、データの消去

- 情報セキュリティインシデントの管理
  - 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、情報セキュリティ事象の中からインシデントを発見できる。
    - 用語知識：情報セキュリティ事象、情報セキュリティインシデント、インシデント対応
  - 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、次の事項を実施できる。
      - 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。
    - 用語知識：情報セキュリティインシデント、 インシデント対応、 事故
  - 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、次の事項を実施できる。
      - 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。
    - 用語知識：操作記録、アクセス記録、 原因の切分け
  - 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、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できる。
    - 用語知識：再発防止、業務手順の見直し
  - 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、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、 保持を実施できる。
    - 用語知識：証拠、ディジタルフォレンジックス

- 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、 次の事項を実施できる。
    - 情報セキュリティポリシ、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。
  - 用語知識：情報セキュリティポリシ、情報セキュリティ意識、教育・訓練計画、 教育資料、成果の評価

- 情報セキュリティの意識向上
  - 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、情報セキュリティを維持した運用を行うため、部門のメンバへアドバイスができる。
    - 用語知識：FAQ、 ナレッジ
  - 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、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できる。
    - 用語知識：教育・訓練計画、内部不正防止ガイドライン、不正のトライアングル（機会、動機、 正当化）、 状況的犯罪予防
- コンプライアンスの運用
  - 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、次の事項を実施できる。
      - 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。
    - 用語知識：情報セキュリティポリシ、 コンプライアンス、 法令、 規格、情報倫理規程
  - 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、次の事項を実施できる。
      - 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案を活動計画として取りまとめ、 実施する。
    - 用語知識：情報セキュリティ監査、内部監査、 自己点検、 指摘事項
- 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
    - 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、 次の事項を実施できる。
      - 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、現行の規程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、現行の規程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。
    - 用語知識：情報セキュリティポリシ、 業務分析、 レビュー技法、ブレーンストーミング
  - 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、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できる。
    - 用語知識： PDCA サイクル、 規程の改廃
- 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
    - 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、次の事項を実施できる。
      - ・情報セキュリティ機関や製品ベンダから提供されるセキュリティ情報を収集し、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、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。
    - 用語知識： 情報セキュリティ機関（NISC、JPCERT/CC、 IPA）、 事例研究、グループ学習、 セミナー