

試験範囲	
<p>4. 保守、変更管理、移行</p>	<p>(5) サービスレベル管理</p> <ul style="list-style-type: none"> イ SLA ロ SLAの評価項目 ハ 評価指標と目標値 <p>(6) 費用の管理</p> <ul style="list-style-type: none"> イ 費用の発生時期による分類 ロ ハードウェア費用の特徴と費用削減の視点 ハ ソフトウェア費用の特徴と費用削減の視点 ニ ハードウェア保守費用の特徴と費用削減の視点 ホ ソフトウェア保守費用の特徴と費用削減の視点 ヘ 施設設備の費用の特徴と費用削減の視点 ト サービス利用の特徴と費用削減の視点 チ クラウドサービスにおける契約 リ 委託業務に関するセキュリティの要求事項 ヌ その他の費用の特徴と費用削減の視点 <p>(7) 報告</p> <ul style="list-style-type: none"> イ 報告先 ロ 項目(例) ハ 報告時期 <p>(8) インシデントの管理</p> <ul style="list-style-type: none"> イ インシデントの管理の概略 ロ インシデントの管理の活動 <p>(9) 利用者の支援</p> <ul style="list-style-type: none"> イ サービスデスクの役割 ロ 受信する要求の分類 ハ サービス品質の維持・向上への取り組み <p>(1) 保守の活動の概要</p> <ul style="list-style-type: none"> イ 保守の管理対象 ロ 保守の要因 ハ 保守の種類 ニ 保守契約 <p>(2) IT資源の種類ごとの特徴</p> <ul style="list-style-type: none"> イ ハードウェアの保守 ロ ソフトウェアの保守 <p>(3) 変更管理</p> <ul style="list-style-type: none"> イ 変更の分類 ロ 変更管理の手順 <p>(4) 移行(リリースおよび展開)</p> <ul style="list-style-type: none"> イ 移行(リリースおよび展開)の概要 ロ 移行方式 ハ 移行作業の検証 ニ 移行テストの評価項目

試験範囲	
<p>4. ビジネスツールの活用</p>	<p>(3) eメール(電子メール)</p> <ul style="list-style-type: none"> イ eメールのしくみ ロ 導入効果 ハ さまざまなeメール ニ eメールの運用 <p>(4) クラウドサービス</p> <ul style="list-style-type: none"> イ クラウドサービスの概要 ロ クラウドサービスの技術基盤 ハ いろいろなクラウドサービス ニ 特徴・効果と課題 <p>(5) ソーシャルメディア</p> <ul style="list-style-type: none"> イ SNS(Social Networking Service) ロ マーケティングへの活用 <p>(6) グループウェア</p> <ul style="list-style-type: none"> イ グループウェアとは ロ 主な機能 <p>(7) EC:Electronic Commerce</p> <ul style="list-style-type: none"> イ B to B(企業間取引) ロ B to C(企業・消費者間取引) ハ C to C(個人間取引) ニ バーチャルモール ホ ポータルサイト <p>(8) 企業間連携</p> <ul style="list-style-type: none"> イ EDI ロ EOS ハ SCM <p>(1) 文書作成ソフトウェア</p> <ul style="list-style-type: none"> イ 文書作成ソフトウェアの利用シーンの変化 ロ 文書作成時の表示方法 ハ 校正機能 ニ データの挿入 ホ データのコンバート ヘ 表形式の変換 ト 文書データのセキュリティ <p>(2) 表計算ソフトウェア</p> <ul style="list-style-type: none"> イ 表計算ソフトウェアの利用 ロ シミュレーション的な利用 ハ グラフとの連動 ニ 表計算ソフトウェアでのデータの共有 ホ 表計算での分析 ヘ ゴールシーク ト 保存形式

試験範囲	
<p>5. データの活用</p>	<p>(3)プレゼンテーションソフトウェア イ プレゼンテーションソフトウェアの日常 ロ 表現の基本 ハ スライド全体のデザイン ニ 関係の表示 ホ スライドで使う画像 ヘ アニメーション ト 音声の取り込みと動画資料の作成 チ スライドの再生方法 リ 配布資料</p> <p>(1)統計 イ 平均と期待値 ロ 差の見つけ方 ハ t検定 ニ 相関 ホ 統計的仮説検定 ヘ 主成分分析 ト クラスター分析 チ テキストマイニング</p> <p>(2)意思決定の支援 イ 意思決定と意志決定 ロ 組み合わせ問題へのアプローチ ハ 重みづけ ニ 重要点領域の設定 ホ データの独り歩きに注意する</p> <p>(3)マーケティングで使われる指標例 イ 回転率 ロ ショッピングバスケット分析 ハ RFM分析 ニ 行動ターゲティング</p>
<p>Ⅲ. 評価</p> <p>1. 情報化の効果の考え方</p>	<p>(1)経営戦略との連動性 イ 経営戦略の再確認 ロ 情報化戦略の再確認 ハ 対象情報システムの役割確認</p> <p>(2)評価の前提となる外部環境、内部環境 イ 外部環境分析 ロ 内部環境分析 ハ SWOT分析による重要成功要因(CSF)抽出</p> <p>(3)評価の対象や項目(ヒト、モノ、カネなどの視点) イ 財務の視点 ロ 顧客の視点 ハ 業務プロセスの視点 ニ 学習と成長の視点</p> <p>(4)評価の範囲 イ 対象となる事業・業務 ロ 対象ビジネスプロセス ハ 対象となる情報システム</p>

試験範囲	
2. 評価方法	(1) 会計的評価法 (2) バランスト・スコアカード (3) 戦略マップ (4) 成熟度モデル (5) IT投資マネジメント (6) 情報化企画書の効果評価例
3. モニタリング・コントロール	(1) モニタリング・コントロールの意義 イ モニタリング・コントロールとは ロ モニタリング・コントロールの対象範囲 (2) モニタリングの対象となるプロセス イ モニタリング対象領域の知識 ロ モニタリング・コントロールの手順 (3) モニタリング実施方法 イ モニタリングの指標管理 ロ 実態把握 ハ 報告書
IV. 対策	
1. 対策の概念	(1) リスクマネジメント (2) 内部統制 イ 内部統制に関する基準および用語定義 ロ 内部統制の基本的計画および方針 ハ 3点セット文書 ニ 内部統制の管理体制 ホ 内部統制のモニタリング (3) 情報セキュリティ管理 イ 情報セキュリティ管理に関する基準 ロ 情報セキュリティ関連の用語定義 ハ 情報セキュリティポリシーと対策基準 ニ 組織体制 ホ モニタリング
2. 対策の管理システムの詳細	(1) 内部統制の構築・管理 イ 統制環境の整備 ロ リスク評価 ハ リスク対応 ニ 統制活動 ホ ITへの対応 へ 情報と伝達 ト モニタリング (2) 情報セキュリティ管理 イ 情報セキュリティ管理に対する要求事項 ロ リスクアセスメント ハ リスク対応 ニ モニタリング ホ 改善

試験範囲	
<p>3. 対策の管理策の詳細</p>	<p>(1) 組織的なセキュリティ</p> <ul style="list-style-type: none"> イ 情報セキュリティの役割および責任 ロ 情報資産の管理 ハ 職務の分離 ニ 専門組織および関係当局との連絡 ホ 供給者関係のための情報セキュリティの管理 ヘ 情報セキュリティインシデント管理および事業継続計画 ト 法令・規制・契約上の義務の要求事項の遵守(コンプライアンス) <p>(2) 人的資源のセキュリティ</p> <ul style="list-style-type: none"> イ 雇用条件 ロ 情報セキュリティの意識向上、教育および訓練 <p>(3) 物理的および環境的セキュリティ</p> <ul style="list-style-type: none"> イ 災害対策 ロ オフィスや施設のセキュリティ ハ 装置のセキュリティ ニ バックアップ <p>(4) 通信およびシステム運用のセキュリティ</p> <ul style="list-style-type: none"> イ LANのセキュリティ設定 ロ ユーザー認証 ハ 通信の暗号化 ニ 電子メールのフィルタリング ホ セキュリティホールなどのぜい弱性対策 ヘ ファイアウォール ト コンピュータウイルスなどのマルウェア対策 チ ネットワークのアクセス制御 リ ネットワーク不正アクセスの検知 ヌ システム運用管理のセキュリティ ル システムの開発・取得・保守のセキュリティ
<p>4. 対策の応用と動向</p>	<p>(1) セキュリティ管理の実践</p> <ul style="list-style-type: none"> イ トップマネジメント(経営者)の責任 ロ 情報セキュリティの方針 ハ 情報セキュリティの適用範囲 ニ 情報セキュリティ対策基準の策定 ホ 情報セキュリティの目標 ヘ 情報資産の洗い出し ト リスクアセスメントとリスク対応 チ 情報セキュリティの運用 リ 情報セキュリティの監視 ヌ 情報セキュリティの改善 <p>(2) 関連するリスクマネジメントの基準</p> <ul style="list-style-type: none"> イ COSO改訂ERMフレームワーク

試験範囲	
	<p>(3) 関連する情報セキュリティの基準</p> <ul style="list-style-type: none"> イ IPAによる情報セキュリティに関する情報提供、問い合わせ、相談 ロ PCI DSS ハ 金融機関等コンピュータシステムの安全対策基準(FISC) ニ サイバーセキュリティ経営ガイドライン ホ CSIRT へ IoTへのサイバー攻撃の脅威に対する対応 ト 産業用オートメーションおよび制御システムを対象としたサイバーセキュリティマネジメント(CSMS) チ EU一般データ保護規則(GDPR)