第 12 章　午後試験対策

本章について

本章では試験要綱の「午後の出題範囲」及びシラバスの「要求される技能」を基に，午後試験で求められる知識・スキルを列記します．また「要求される技能」の「用語例」に記載された用語について，本書第 1～11 章の該当項目を挙げますので，理解度の確認に利用してください．

12.1　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

12.1.1　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ことが求められます．
- **情報資産，価値（重要度）**　1.2.2（情報資産の重要性による分類と管理）参照．
- **3特性（機密性，完全性，可用性）**　1.1.1（情報セキュリティの目的と考え方）参照．
- **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こと，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ことが求められます．
- **情報資産受入れ，変更管理**　1.1.2（情報資産の重要性による分類と管理）参照．
- **利用管理，廃棄管理，管理体制**　1.1.2（情報資産台帳）参照．
- **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，作成できることが求められます．
- **情報資産台帳**　1.2.2（リスク分析と評価（情報資産の調査・分類））参照．
- **資産の棚卸**　1.2.2（情報資産の調査）参照．

12.1.2　情報セキュリティリスクアセスメント及びリスク対応

- **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こと，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ことが求められます．加えて，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，同様に評価できることが求められます．

- **脅威** 1.1.3（脅威脅威の種類），1.1.4（脅威マルウェア・不正プログラム）参照．
- **脆弱性** 1.1.5（脆弱性）参照．
- **サイバー攻撃（標的型攻撃，ゼロデイ攻撃ほか）** 1.1.9（サイバー攻撃手法）参照．
- **資産の価値** 1.2.2（情報資産の重要性による分類と管理）参照．
- **物理的な要因** 1.1.3（物理的脅威）参照．
- **技術的な要因** 1.1.3（技術的脅威）参照．
- **人的な要因** 1.1.3（人的脅威）参照．
- **事象の起こりやすさ，結果（損害の大きさ）** 10.1.1（リスクの発生頻度・影響・範囲）参照．
- **リスク受容基準** 1.2.4（リスク基準）参照．
- **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こと，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ことが求められます．加えて，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ことが求められます．
- **リスク対応策** 1.2.5（リスク分析と評価）参照．
- **物理的対策** 1.4.4（物理的セキュリティ対策）参照．
- **人的（管理的）対策** 1.4.1（人的セキュリティ対策）参照．
- **技術的対策** 1.4.2，1.4.3（技術的セキュリティ対策）参照．
- **残留リスク** 1.2.5（リスク分析と評価）参照．
- **リスク対応計画の策定** 検討したリスク対応策の優先順位を基に，リスク対応計画を作成する目的，及び記載する内容（実施項目，資源，責任者，完了予定時期，実施結果の評価方法ほか）を理解し，リスク対応計画を作成できることが求められます．
- **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** 1.2.5（リスク分析と評価）参照．

12.1.3 情報資産に関する情報セキュリティ要求事項の提示

- **物理的及び環境的セキュリティ** 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ことが求められます．

- **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** 1.4.4（物理的セキュリティ対策）参照．
- **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** 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ことが求められます．要求事項には，次のような項目があります．

  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
  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

- 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ことが求められます．
- **アクセス制御，利用者アクセスの管理** 1.4.2（技術的セキュリティ対策）参照．
- **業務上の要求事項，情報セキュリティ要求事項** 1.1.2（情報セキュリティの重要性）参照．
- **開発及びサポートプロセス** 9.2.1（業務プロセスの改善と問題解決）参照．
- **受入れテスト，試験データ** 7.2.2（サービスの設計・移行）参照．

12.1.4 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示

- **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** 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ことが求められます．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）を提案できることが求められます．
- **障害，災害，事業継続マネジメント** 11.1.3（リスクマネジメント）参照．
- **情報セキュリティ継続** 1.2.6（情報セキュリティ継続）参照．

12.2 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

12.2.1 情報資産の管理

- **情報資産台帳の維持管理** 情報資産台帳に記載する内容，及び台帳の維持管理の必要性，手順を理解した上で，情報セキュリティポリシ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ことが求められます．
- **情報セキュリティポリシ** 1.2.7（情報セキュリティ諸規程）参照
- **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** 7.2.2（サービスの設計・移行）参照．
- **廃棄** 9.4.2（情報システム廃棄）参照．
- **媒体の管理** 情報セキュリティインシデント（以下，インシデントという）を発生させないために必要な，可搬媒体の管理（部門の執務場所と外部との間での持込み・持出し，廃棄）の方法，手順を理解し，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ことが求められます．
- **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）** 1.4.4（物理的セキュリティ対策）参照．
- **利用状況の記録** 情報資産を管理することの必要性，方法，手順を理解した上で，対象資産の利用状況を把握し，また，その配置，管理者，構成の変更などを追跡し，情報資産の利用状況を記録できることが求められます．
- **情報資産の配置，管理者，構成の変更** 7.2.2（サービスの設計・移行）参照．

12.2.2 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ことが求められます．
- **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** 1.1.4（脅威〔マルウェア・不正プログラム〕）参照．
- **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ことが求められます．
- **バックアップ（取得サイクル，保持場所），リストア** 1.5.3（データベースセキュリティ）参照．
- **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ことが求められます．
- **ログの監視，記録，分析，保持方法** 1.5.3（データベースセキュリティ）参照．

- **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ことが求められます．
- **電子メール，ファイル，閲覧サイト** 1.4.2（技術的セキュリティ対策）参照．
- **機器の持込み・持出し** 1.4.4（物理的セキュリティ対策）参照．
- **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ことが求められます．
- **脆弱性管理，パッチ管理，パッチ適用基準** 1.4.2（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））参照．
- **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ことが求められます．
- **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，IC カード，トークン，アクセス権限** 1.1.12（情報セキュリティ技術（利用者認証））参照．
- **生体認証** 1.1.13（情報セキュリティ技術（生体認証技術））参照．
- **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ことが求められます．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ことが求められます．
- **情報セキュリティポリシ，監視** 1.2.7（情報セキュリティ諸規程）参照
- **測定，分析，評価** 10.1.1（情報システム導入リスク分析）参照
- **脆弱性検査，侵入検査** 1.3.1（セキュリティ評価）参照

12.2.3 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ことが求められます．また，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こと，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ことが求められます．
- **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** 10.3.1（調達と調達計画）参照
- **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ことが求められます．そして，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ことが求められます．また，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ことが求められます．

- **不正防止・機密保護，機密保持契約**　10.3.1（調達と調達計画）参照
- **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ことが求められます．また，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ことが求められます．
- **検収，廃棄，システムライフサイクル，データの消去**　10.3.1（調達と調達計画）参照

12.2.4 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ことが求められます．
- **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**　1.2.1（情報セキュリティ管理）参照
- **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ことが求められます．

  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．

- **情報セキュリティインシデント，インシデント対応，事故**　1.2.1（情報セキュリティ管理）参照
- **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ことが求められます．

  情報システム部門の協力を受けて，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．

- **操作記録，アクセス記録**　1.4.1（利用者アクセスの管理）参照
- **原因の切分け**　1.2.6（情報セキュリティ継続）参照

- **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ことが求められます．
- **再発防止，業務手順の見直し** 1.2.6（情報セキュリティ継続）参照
- **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，保持を実施できることが求められます．
- **証拠，ディジタルフォレンジックス** 1.4.2（技術的セキュリティ対策）参照

12.2.5 情報セキュリティの意識向上

- **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ことが求められます．

  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．

- **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** 1.2.7（情報セキュリティ諸規程）参照
- **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ことが求められます．
- **FAQ** 7.4.1（サービスの運用）参照
- **ナレッジ** 9.2.1（業務プロセスの改善と問題解決）参照
- **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ことが求められます．
- **教育・訓練計画** 1.2.7（情報セキュリティ諸規程）参照
- **内部不正防止ガイドライン** 1.4.1（人的セキュリティ対策）参照
- **不正のトライアングル（機会，動機，正当化），状況的犯罪予防** 1.1.6（不正のメカニズム）参照

12.2.6 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ことが求められます．

  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．

- **情報セキュリティポリシ** 1.2.7（情報セキュリティ諸規程）参照
- **コンプライアンス，法令，規格，情報倫理規程** 2.4.1（その他の法律・ガイドライン・技術者倫理）参照
- **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ことが求められます．

  自部門又は業務監査部門が定期的に行う，法令，規格，規範及び情報セキュリティ諸規程の順守状況の点検，評価に対応する．
  第三者（外部を含む）による情報セキュリティ監査に協力し，必要な文書をそろえ，インタビューに応じる．
  監査部門からの指摘事項に関して，改善のために必要な方策を活動計画として取りまとめ，実施する．

- **情報セキュリティ監査** 8.1.2（情報セキュリティ監査）参照
- **内部監査，自己点検，指摘事項** 1.2.8（情報セキュリティマネジメントシステム（ISMS））参照

12.2.7 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ことが求められます．

  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．

- **情報セキュリティポリシ** 1.2.7（情報セキュリティ諸規程）参照
- **業務分析，レビュー技法，ブレーンストーミング** 11.2.2（業務分析・業務計画）参照
- **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ことが求められます．

- **PDCA サイクル**　11.1.1（経営管理（経営管理・経営組織））参照
- **規程の改廃**　1.2.8（情報セキュリティマネジメントシステム（ISMS））参照

12.2.8 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ことが求められます．

  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．

- **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**　1.2.9（情報セキュリティ組織・機関）参照