**情報システムの整備と運用管理を調達する際の情報セキュリティ対策として考慮すべき要件メモ**

2016年4月12日

中山正樹

目次

[**情報システムの整備と運用管理を調達する際の情報セキュリティ対策として考慮すべき要件メモ** 1](#_Toc514852288)

[1. 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」より 1](#_Toc514852289)

[1.1. プロジェクトの管理 1](#_Toc514852290)

[1.1.1. プロジェクト管理要領の記載内容（プロジェクト計画書等の作成） 1](#_Toc514852291)

[1.2. 業務の見直し 6](#_Toc514852292)

[1.2.1. 業務要件の定義 6](#_Toc514852293)

[1.3. 要件定義 7](#_Toc514852294)

[1.3.1. 非機能要件（要件定義書の記載事項） 7](#_Toc514852295)

[1.4. 設計・開発 9](#_Toc514852296)

[1.4.1. 設計・開発実施要領の記載内容（設計・開発実施計画書等の作成） 9](#_Toc514852297)

[1.5. 業務の運営と改善 9](#_Toc514852298)

[1.5.1. 日常運営における業務改善の実施方法（日常運営における業務改善） 9](#_Toc514852299)

[1.6. 運用及び保守 10](#_Toc514852300)

[1.6.1. 運用実施要領の作成・記載内容（運用開始前の準備） 10](#_Toc514852301)

[1.6.2. 保守実施要領の作成・記載内容（運用開始前の準備） 10](#_Toc514852302)

[1.7. システム監査の計画 11](#_Toc514852303)

[1.7.1. システム監査計画の策定 11](#_Toc514852304)

# 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」より

## プロジェクトの管理

### プロジェクト管理要領の記載内容（プロジェクト計画書等の作成）

#### リスク管理

* リスク顕在時の報告先、報告内容、リスクの管理手法等を記載する
* 情報セキュリティリスクについては、自組織の情報セキュリティポリシーを参照
* 趣旨
  + プロジェクトの目標達成を阻害する予期し得ない事態をリスクという。多種多様なリスクについて、その顕在化前から発生の要因分析と影響、確率を評価するとともに、予防策や顕在化した際の原因追及、プロジェクトへの影響の把握、対応策の実施及び結果を評価するため、リスクの管理手法等を記載するものである。
  + リスクには、プロジェクト遂行上発生するおそれがあることがプロジェクトの計画段階で判断可能なもの、遂行中に新たに発生するおそれがあることが判明又は顕在化するもの、レビュー制度において判明するものがある。
  + 段階別では、下記のようなリスクが存在するため、PJMOはこれらを把握し、分析・評価結果を踏まえて適切な対応を指示する必要がある。
    - 計画策定段階のリスク（政策等の要求による非常に短期の開発スケジュールを要因とするリスク等）
    - 要件定義段階のリスク（適切な要件を網羅できない又は過剰な事項まで要件としてしまうリスク等）
    - 調達リスク（適切な事業者が選定できないリスク、調達したハードウェア等の瑕疵、情報システム等に内在する情報セキュリティリスク等）
    - 制度改定、関連法令等への遵守に関係するリスク（コンプライアンスのリスク）
  + また、PJMOは、プロジェクトの各工程において発生する可能性のある全てのリスク（）も把握する。
    - プロジェクト遅延リスク
    - 成果物の瑕疵リスク
    - コスト増大リスク
    - サービスレベルの低下リスク
    - 情報セキュリティリスク等
  + そのリスクの分析・評価結果を踏まえて適切な対応を指示する必要がある。リスク対応策は、リスクの内容に応じて、リスク管理に関する会議やPJMOが決定する。
  + リスク対応の結果については、PJMOがPMOに報告し承認を得る。
  + 上記について、PJMOは、その都度、統括してリスク管理簿注）にまとめ、適切に管理するとともに、プロジェクト関係者間で常に共有する。特にリスク対応の状況については、継続的なフォローを行い、適時に対応状況の報告を受ける。
  + 注）実務手引書「第３編第２章別紙２－４　６．リスク管理簿の例」参照。
* リスク管理の要点
  + 個々のリスクの要因や特徴、発生頻度等の網羅的な把握により、プロジェクトを遂行することに影響する重要なリスクが適切に識別、分析、管理及び報告されるとともに、対策の実行及びその有効性に関する評価が行われることとなる。
  + PJMOは、政策目的・目標の達成を阻害するリスク、各事業者は、契約に定めた目標の達成（成果物の完成、業務品質水準の達成等）を阻害するリスクについて、それぞれ管理する責任があるため、PJMOは、自らが責任を負うべきリスク管理を実施するとともに、各事業者においても適切なリスク管理の実施を要求し、その状況を把握する。
* リスク管理の活動
  + リスク管理は次の活動から構成される。
  + (1)データの収集
    - プロジェクトを遂行することに関わるリスクの効果的な特定、分析及び報告ができるように、関連するデータの特定と収集を行う。
    - 各種リスクに関する事象のタイプ、リスクのカテゴリ、発生要因に関して、当該プロジェクトに関係するリスクに関わるデータを収集、分類及び分析するための方法を確立し、適宜見直しを行う。
    - 当該プロジェクトを遂行することにおけるリスクの管理において、プロジェクトの対象となっている業務及び情報システムの実行に影響する内外の環境に関するデータを収集する。また、この際、過去のプロジェクトからの経験についても調査を行う注）。
    - 注）実務手引書「第３編第２章別紙２－４　１ リスクの要因」参照。
  + (2)リスクの分析及び対応策の検討
    - リスクの要因及び業務の関連性を考慮して、リスクに関する対応を決定するために必要な情報を取りまとめる。
    - このために、リスクの要因及び業務に対する重要性を考慮し、リスク分析を行う範囲及び深さについて検討を行い、費用対効果も考慮したリスク分析の範囲を設定する。
    - リスクは、単独の事象としてだけではなく、一連の事象として連鎖して発生することも多いことを考慮し、脅威の種類、リスクの原因となる行為を行う可能性のある者、発生する可能性のある事象、影響を受ける可能性のある資産等、発生のタイミング等をリスクシナリオとしてまとめ、その影響及び頻度（発生確率）を推定する注）。
    - リスクシナリオについて、そのコントロール及び対策並びに残存リスクについて評価を行い、残存リスクについて、更なる対策を検討する必要性の有無を検討する。
    - 費用対効果の分析を行い、回避、低減・軽減、移転・共有及び受容といった、最適なリスク対応策をまとめる。なお、ISO 31000又はJIS Q 31000（リスクマネジメント－原則及び指針）を参照することは有用である。
    - 取りまとめたリスク対応策について、レビューを行う。
    - リスクを必要十分なレベルまで低減するため、対応策の優先順位付けを行って、実行を管理する。
    - 注）実務手引書「第３編第２章別紙２－４　２ リスク分析を実施する際の検討項目」、同「第３編第２章別紙２－４　３ リスク分析を行う分野の例」及び同「第３編第２章別紙２－４　４ リスク評価を行う際の書式（リスクシナリオ）例」参照。
  + （参考：クラウドコンピューティングサービスの利用を考慮する場合）
    - 利用によるメリットとリスクのバランスの考察（リスクの最適化）
      * クラウドコンピューティングサービスを利活用することによるメリットとしてどのようなものがあるのかを理解し、利用によって生じ得るリスクと、利用しないことによって生じるリスクを理解して、その二つの面から、適切に判断することが肝要である。
      * クラウドコンピューティングサービスの利活用のメリットの例（これらは、利活用しない場合のリスクの項目と対応する。）
        + 情報システム基盤を調達せずに、既に実績のあるサービスを利用できるため、政策課題への迅速な対応、調達費用の最小化等が期待できる
        + 利用量に応じた課金となっているため、利用に係るコストの最適化を行うことが期待できる
        + 災害時における復旧を速やかに行うことが期待できる
        + 規模の拡張若しくは縮小が容易である　等
      * クラウドコンピューティングサービスを利用することによって生じ得るリスクの例
        + サービスレベルはベンダーが提示するものに固定される
        + データセンタが海外に存在する場合、日本の法規制が適用されない
        + サービス形態によっては、システム監査を実施できない
        + データの所有権の帰属が曖昧になることがある　等
    - リスクへの対応

| No. | 対応の選択肢 | 対応の内容 |
| --- | --- | --- |
| １ | 回避 | 利用によって生じると考えられるリスクを検討した結果、利用をやめる場合。クラウドコンピューティングサービスを利用しないため、これによるリスクは発生しない |
| ２ | 低減・軽減 | データセンタの場所が国内であって、利用者がシステム監査を実施可能であるサービスを選定し、システム監査の条項を含む契約を結ぶことができるベンダーを選定する場合。適切な運用管理が行われているか否かを確認し、問題があれば改善等を要求し、リスクを低減する |
| ３ | 移転・共有 | 何らかの問題が発生し損害が発生した場合には、賠償責任をベンダーが負うことについて、契約に明記し、その損害をカバーする場合等 |
| ４ | 受容 | 既に適切な対策が実施されており、残存リスクが小さいと判断される場合に、残存リスクがあることを承知した上で、特別に新たな対策を取らないことを意思決定した上で、利用する場合 |

* + (3) リスクとその属性についての情報を最新の状態に維持
    - リスクに適切に対応するためには、次の事項について明確化しておくことが望ましい。
    - 既知のリスクとその属性（予想される頻度、潜在的な影響及び対応）
      * リスクが影響する資源
      * リスクに対応する組織の力
      * 現状におけるリスクをコントロールする活動の状況
    - このためには、各計画書や構成管理等の資料を活用する。また、他において顕在化したリスクに関する情報を集め、リスクとその属性に関する情報を最新の状態に維持する。
    - これらの情報を基に、定期的にリスクへの対応策の見直し、優先順位付けの変更等について必要性を判断し、変更を行う。
  + (4) リスクに関する理解の促進
    - 適切にリスクに対応するために、必要な関係者に対して、適時に、リスクの発生により顕在化する状況について情報を提供する。
    - このため、影響を受ける関係者にとって具体的かつ理解しやすい形式で、またリスクの影響と発生確率に係る根拠も含めてリスク分析結果を取りまとめる。さらに、最悪で、かつ、最も発生可能性の高いリスクシナリオ、コンプライアンス上の重要事項等も取りまとめる。
    - 取りまとめたものは、リスク管理プロセスの有効性、コントロールの有効性、現状における問題点等を整理し、関係者で共通理解を得る。
    - 必要に応じて、第三者の評価、システム監査、工程レビュー等の結果を評価して、更なるリスク分析を実行する必要性を判断する。
  + (5) リスクのモニタリングと対応策の見直し
    - リスクを低減するための一連のコントロール活動を整理し、その有効性等を評価して、対応策及びコントロール活動の優先順位を定義する。リスクに関するモニタリングを継続的に実施し、コントロールの有効性を判断し、適宜見直しを行う。
  + (6)リスク顕在時の対応
    - リスク顕在時に適切に対応するためには、次の事項を考慮しておくことが望ましい。
    - 予兆の検出
      * 地震等の突発的自然災害等によるリスクを除くと、リスクが顕在化する前には予兆が発生していることが多いため、PJMOは、府省CIO補佐官等の助言を受けつつ、日常的に注意深く、プロジェクト実行現場の状況や、プロジェクトに影響を与え得る外部環境の変化を把握することが必要である。
    - 対応の準備
      * リスクに関するインシデント（事象）が発生した場合、その影響を最小化するために適切に対応するためには、あらかじめ対応の計画を準備し、その更新とテストを行う中で、インシデントが発生したときの対応の手続も点検しておく必要がある。
    - リスクの顕在化時（インシデント発生時）の対応
      * 実際にインシデントが発生した場合は、影響を最小化するため、事前に計画において定めた手順により速やかに対応を行う。
  + (7)リスク対応結果の評価とその後の対応
    - リスク対応を行った後、過去の有害事象等の情報等も参照しつつ、インシデント発生の根本原因、追加対策、対応手続の改善等について取りまとめ、関係者に報告を行う。
    - リスク対応及びその結果は、当該リスクの性格に応じて、工程管理、品質管理、課題管理、変更管理、構成管理等に影響を与えるため、PJMOは、リスクへの対応の計画に基づき、それぞれの個別管理における対応へと引き継ぐべき事項を判断し、適切に対処する。
    - また、PJMOは、PMOに対応結果を報告するとともに、必要に応じてプロジェクト計画書等の修正等を行う。
  + (8)留意事項
    - (2)で述べたように、リスクは連鎖するものであるという認識が重要である。
    - 例えば、個人情報の漏えいといった情報セキュリティ上のリスクが顕在化した場合に、初期対応を誤ると、最終的には当該情報システムを利用している業務そのものに対する国民からの信頼を失墜するリスクにまでつながりかねない。
    - 一つのリスクの顕在化を発端として、各種のリスクへとつながる可能性があることを認識し、連鎖する可能性のあるリスクについてあらかじめ十分に検討し、対策を検討しておくことが肝要である。

## 業務の見直し

### 業務要件の定義

#### 情報セキュリティ

業務において取り扱われる情報の格付・取扱制限等に応じた情報セキュリティ対策の基本的な考え方

* 情報セキュリティ対策の基本的な考え方等の定義方法
* (1)本項目の趣旨
  + 見直し後の業務を実施する上で必要な情報セキュリティ対策の基本的な考え方を明らかにするものである。
  + この段階で見直し後の業務における情報の取扱いに関する考え方を明らかにすることにより、要件定義段階において、情報システムに求める機能要件及び非機能要件を漏れなく定義することができる。
* (2)定義手順
  + 情報セキュリティ対策の対象となる情報を明確化するために、実務手引書に係る解説及び取扱情報の洗い出し結果を確認する。
  + また、要件定義の段階で情報セキュリティ上のリスクを特定し、その対策を機能要件及び非機能要件として定義できるように、情報セキュリティ対策の対象となる情報について、自組織の情報セキュリティポリシーに準拠した格付の区分及び取扱制限を明確化する。特に、新たな業務を開始するに当たって情報システムを新規に整備する場合や、既存の業務の見直しに伴って新たに取り扱う情報がある場合を中心として行うが、従来の格付についても必要に応じて見直しを行う。
  + 情報漏えい等による個人のプライバシーの侵害や、国民・組織に財産上の被害を与える等、情報の機密性保護に係るリスクに対する対策は特に重要であるが、情報の改ざんや情報システムの停止による利用者への影響についても考慮する必要がある。

【表４－33】(参考)機密性についての格付の区分注）

|  |  |
| --- | --- |
| 格付の区分 | 分類の基準 |
| 機密性３情報 | 行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報 |
| 機密性２情報 | 行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報 |
| 機密性１情報 | 機密性２情報又は機密性３情報以外の情報 |

注）政府機関の情報セキュリティ対策のための統一基準群を引用しているが、自組織が定める情報セキュリティポリシーに従うこと。また、完全性、可用性の格付の区分についても同様に自組織が定める情報セキュリティポリシーに従うこと。

* + さらに、情報の取扱いについて定められている根拠法令（例えば行政機関個人情報保護法、番号法等）が存在する場合は、要件定義の段階で当該法令を遵守するために必要な情報セキュリティ対策に漏れが生じないよう適切に要件を定める必要があるため、当該法令の存在について確認する。
  + また、実務手引書において情報の漏えい、改ざん等の情報セキュリティに係る問題点が洗い出されている場合は、実務手引書及び問題点を踏まえたものとなっているかを確認する。
  + 業務で取り扱う情報の格付及び取扱制限について整理した結果が、この段階における情報セキュリティ対策の基本的な考え方となる。

## 要件定義

### 非機能要件（要件定義書の記載事項）

#### 情報セキュリティに関する事項

* 情報システムの情報セキュリティ対策に関する事項について記載する。特に、「第４章５．8) 情報セキュリティ」において検討した内容に照らし、過度にならないよう適切な要件とすること。また、記載に当たっては、自組織の情報セキュリティポリシーを参照のこと
* (1)本項目の趣旨
  + 情報セキュリティは、自組織が扱う情報を適切に保護し、業務の継続性の確保、業務に対する信頼の維持のために重要な事項である。自組織の情報セキュリティポリシーを踏まえ、当該情報システムにおいて実現しなければならない情報セキュリティに関する事項を、当該業務の特性を踏まえて整理し、要件定義書に記載するものである。
* (2)記載方法
  + 情報セキュリティ対策要件の記載方法及び記載例は、次のとおりである。
  + 情報セキュリティ対策要件
    - 自組織において定められた情報セキュリティポリシーを遵守するために必要な情報セキュリティ対策の内容について、具体的に記載する。
    - 記載に当たっては、自組織の情報セキュリティポリシーを参照するとともに、必要に応じて「政府機関の情報セキュリティ対策のための統一基準群」及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（平成23年４月28日内閣官房情報セキュリティセンター）等を参照し、必要な対策を漏れなく記載する。
    - 情報セキュリティ対策
      * 本情報システムにおいて実現すべき情報セキュリティ対策を記載する。記載事項は、上記基準等及びその他の情報セキュリティ対策要件に準拠するよう定める。ただし、不必要に過度な対策とならないよう、必要性を十分検討した上で記載する。
      * 例：
        + 主体認証
        + アクセス制御
        + 権限管理
        + ログ取得及びログ管理
        + 暗号化及び電子署名
        + ソフトウェアの脆弱性対策
        + 不正プログラム対策
        + サービス不能攻撃対策
        + 標的型攻撃対策
    - 対策に係る要件
      * 上記基準等及びその他の情報セキュリティ対策要件を参照し、上記情報セキュリティ対策ごとに、情報システムにおいて提供する業務及び取り扱う情報の特性等に応じた対策要件を具体的に記載する。
    - 補足
      * 基本要件のみを記載し具体的な方式の提案を求めるもの、代替手法による対策の提案を許容するもの等の補足事項について記載する。また、特定の基準等への準拠を求めるものについては、当該基準等を補足欄において指定する。

## 設計・開発

### 設計・開発実施要領の記載内容（設計・開発実施計画書等の作成）

#### 情報セキュリティ

設計・開発における情報漏えい対策等について記載する。

* 本項目の趣旨
  + 本項目は、設計・開発業務を遂行する上での情報セキュリティに対する基本的な考え方、情報セキュリティの管理方法等について記載するものである。
* 記載内容
  + 要件定義の情報セキュリティに関する事項注１）及び調達仕様書における情報セキュリティに係る内容注２）に基づき、「政府機関の情報セキュリティ対策のための統一基準群」及び自組織の情報セキュリティポリシーに準拠して、次に示す例を参考に情報セキュリティ確保に必要な対策を定めて記載する。
  + 注１）実務手引書「第３編第５章２．1)ウj) 情報セキュリティに関する事項」参照。
  + 注２）実務手引書「第３編第６章２．1)カ 作業の実施に当たっての遵守事項」参照。
* （設計・開発に係る情報セキュリティ対策の例）
  + 情報・データ管理（情報・データの授受、廃棄等の管理、特に実データ、実帳票の管理方法）
  + アクセス管理方法（主体認証情報管理、アクセス権限管理等）
  + 不正アクセス監視
  + ログ管理、ログ分析
  + 開発用ＰＣの管理方法（開発終了時のファイルの完全削除等）
  + 作業環境の物理的セキュリティ対策（入退室管理等）
  + 守秘義務同意書の作成
  + 脆弱性対策等の情報セキュリティ対策の実施状況の管理　等

## 業務の運営と改善

### 日常運営における業務改善の実施方法（日常運営における業務改善）

#### リスク及び課題とその原因

* 情報セキュリティ対策の徹底
  + 情報の紛失、漏えい、改ざん等のおそれが生じている場合
  + サービス利用者等からのプライバシー保護等に関する要求が現状と大きく乖離している場合
* 実施方法
  + 対応すべきリスクや課題のうち、改善及び見直しの手段が情報システムの運用又は保守に関するものについては、PJMOのうち情報システム部門の管理者・担当職員が中心となって、運用及び保守作業の改善注１）や運用計画及び保守作業計画の見直し注２）を実施する。
  + また、日常運営における業務改善や情報システムの運用及び保守の改善だけでは対応できない残存課題・リスクについては、情報システムの見直し注３）の必要性について検討する。
  + 注１）実務手引書「第３編第９章４．運用及び保守作業の改善」参照。
  + 注２）実務手引書「第３編第９章６．運用計画及び保守作業計画の見直し」参照。
  + 注３）標準ガイドライン「第３編第１１章 情報システムの見直し又は廃止」参照。

## 運用及び保守

### 運用実施要領の作成・記載内容（運用開始前の準備）

#### 情報セキュリティ対策

運用における情報漏えい対策等について記載する。

* 趣旨
  + 本項目は、運用業務を遂行する上で、情報セキュリティポリシーを遵守するための基本的な考え方、情報セキュリティの管理方法等について記載するものである。
* 記載内容
  + 要件定義の情報セキュリティに関する事項注１）及び調達仕様書における情報セキュリティに係る内容注２）に基づき、情報セキュリティ確保のための管理項目やその内容について記載する。なお、各管理項目における具体的な手順等は、作業手順書として別途作成する。特に、異常検知時の報告所要時間やログの点検間隔等、定量的に記載できるものは定量的に記載することが望ましい。
  + 注１）実務手引書「第３編第５章２．1)ウj) 情報セキュリティに関する事項」参照。
  + 注２）実務手引書「第３編第６章２．1)カ 作業の実施に当たっての遵守事項」参照。
  + （情報セキュリティ確保のための管理項目の例）
    - 情報・データ管理（情報・データの授受、廃棄等の管理）
    - アクセス管理（主体認証情報管理、アクセス権限管理等）
    - 不正アクセス監視
    - ログ管理、ログ分析
    - 脆弱性対策等の情報セキュリティ対策の実施状況の管理　等

### 保守実施要領の作成・記載内容（運用開始前の準備）

#### 情報セキュリティ対策

保守における情報漏えい対策等について記載する。

* 本項目の趣旨
  + 本項目は、保守業務を遂行する上で、情報セキュリティポリシーを遵守するための基本的な考え方、情報セキュリティの管理方法等について記載するものである。
* 記載内容
  + 要件定義の情報セキュリティに関する事項注１）及び調達仕様書における情報セキュリティに係る内容注２）に基づき、情報セキュリティ確保のための管理項目やその内容について記載する。なお、各管理項目における具体的な手順等は、作業手順書として別途作成する。特に、脆弱性改善のためのソフトウェア更新の間隔等、定量的に記載できるものは定量的に記載することが望ましい。
  + 注１）実務手引書「第３編第５章２．1)ウj) 情報セキュリティに関する事項」参照。
  + 注２）実務手引書「第３編第６章２．1)カ 作業の実施に当たっての遵守事項」参照。
* （情報セキュリティ確保のための管理項目の例）
  + 情報・データ管理（情報・データの授受、廃棄等の管理）
  + アクセス管理（主体認証情報管理、アクセス権限管理等）
  + 不正アクセス監視
  + ログ管理、ログ分析
  + 脆弱性対策等の情報セキュリティ対策の実施状況の管理　等

## システム監査の計画

### システム監査計画の策定

* 概要
  + 本節では、各府省がシステム監査計画を策定（PMOが案を作成し、情報化推進委員会等に諮って確定）し、当該計画に基づいて監査を実施することを求める。なお、PMO又はPJMOは、必要に応じて、システム監査計画に記載していない監査を実施することができる注）。
  + 注）実務手引書「第３編第10章１．システム監査」参照。
  + また、本節は、各府省の情報セキュリティポリシーに基づいて実施する情報セキュリティをテーマとした監査（以下「情報セキュリティ監査」という。）と標準ガイドラインに基づくシステム監査との関係を示すものである。
* 情報セキュリティ監査との関係
  + 情報セキュリティは、システム監査におけるテーマの一つである。したがって、標準ガイドラインに基づくシステム監査においても、情報セキュリティがプロジェクトの重大なリスクとして位置付けられる場合には、情報セキュリティをテーマとした監査を実施する必要がある。
  + 一方で、このような監査を実施した場合、その内容が情報セキュリティ監査で実施し、又は実施する予定の内容と重複する可能性がある。この場合、PMOは、情報セキュリティをテーマとする監査を計画するに際し、情報セキュリティ監査の責任者等と協議し、無駄な重複が発生しないように調整するものとする。なお、その際には、システム監査の目的に照らして、情報セキュリティ監査の内容、範囲、実施方法等が十分なものであるか否かを確認した上で、重複を排除する必要がある。
  + また、標準ガイドラインに基づくシステム監査の実施により、情報セキュリティ監査の一部を兼ねようとする場合には、両監査の実施主体、監査対象、監査目的等が異なるため、情報セキュリティ監査の監査責任者と十分な協議を行った上でシステム監査計画を策定する必要がある。