情報セキュリティ監査実施手順の策定手引書

平成 29 年 4 月

内閣官房 内閣サイバーセキュリティセンター

目　次

第 1 部　情報セキュリティ監査実施手順の策定手引書の使い方

第 2 部　情報セキュリティ監査実施手順

第１部　情報セキュリティ監査実施手順の策定手引書の使い方

1.　情報セキュリティ監査実施手順の策定手引書の使い方

1.1.　情報セキュリティ監査実施手順の策定手引書の目的

情報セキュリティ監査実施手順の策定手引書（以下「策定手引書」という。）は、「政府機関の情報セキュリティ対策のための統一規範（平成28年８月31日 サイバーセキュリティ戦略本部決定)」（以下「統一規範」という。）に基づき、府省庁が実施する情報セキュリティ監査の実施手順として、情報セキュリティ監査に係る実施手順を整備するための手引書である。

府省庁においては、統一規範に基づき、自組織の特性を踏まえた府省庁基本方針及び「政府機関の情報セキュリティ対策のための統一基準（平成28年８月31日サイバーセキュリティ戦略本部決定)」（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となる府省庁対策基準を定めることが求められている。統一基準においては、府省庁対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順として実施手順を整備することが規定されている（図1.1-1「策定手引書と統一基準群との関係」を参照)。

情報セキュリティの確保のためには、府省庁基本方針及び府省庁対策基準が適切に策定され、かつ、情報セキュリティ関係規程（府省庁対策基準及び実施手順の総称）が適切に運用されることにより、その実効性を確保することが重要であって、その準拠性及び対策の妥当性が確認されなければならない（図1.1-2「情報セキュリティ監査の目的について」を参照)。そのためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を実施することが必要である。

情報セキュリティ監査実施手順は、情報セキュリティ監査責任者（以下「監査責任者」という。）等が情報セキュリティ監査を行うに当たり、監査責任者等が情報セキュリティ監査実施手順に従うことにより、統一規範に基づく情報セキュリティ監査を遵守することを想定している。

これらの背景の下で策定手引書は、情報セキュリティ監査実施手順に含めるべき事項を具体的に示し、もって準拠性及び妥当性の観点から、適切な情報セキュリティ関係規程の整備に資することを目的とする。

なお、策定手引書の対象とする情報セキュリティ監査は、サイバーセキュリティ基本法に基づきサイバーセキュリティ戦略本部が実施する監査を指すものではない。

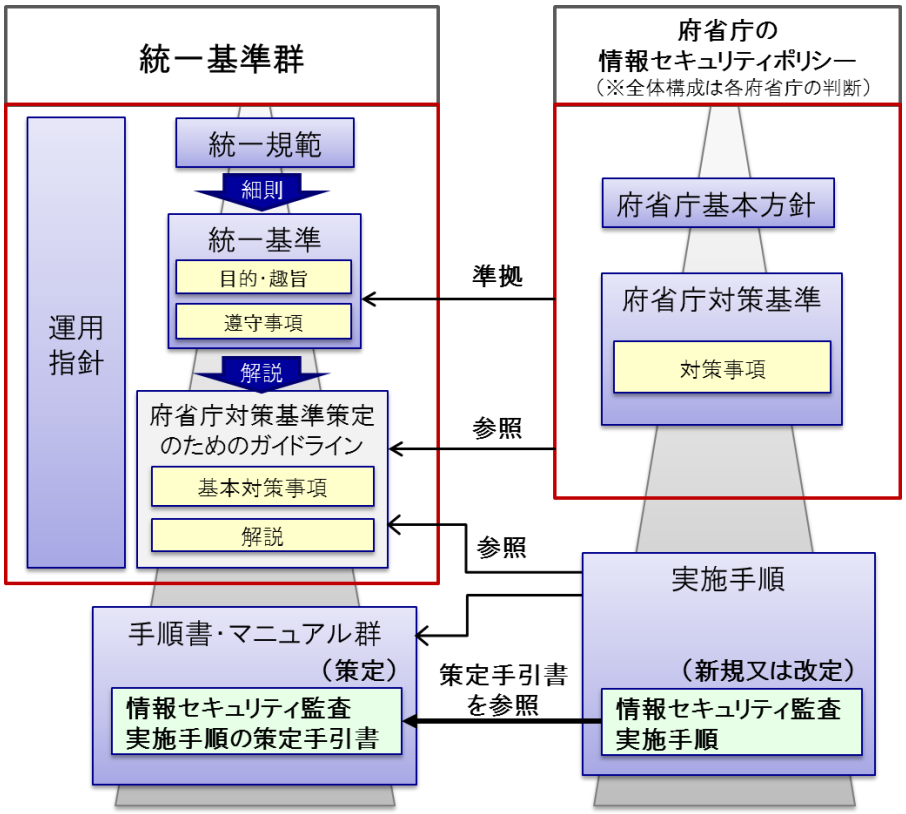

図 1.1-1　策定手引書と統一基準群との関係

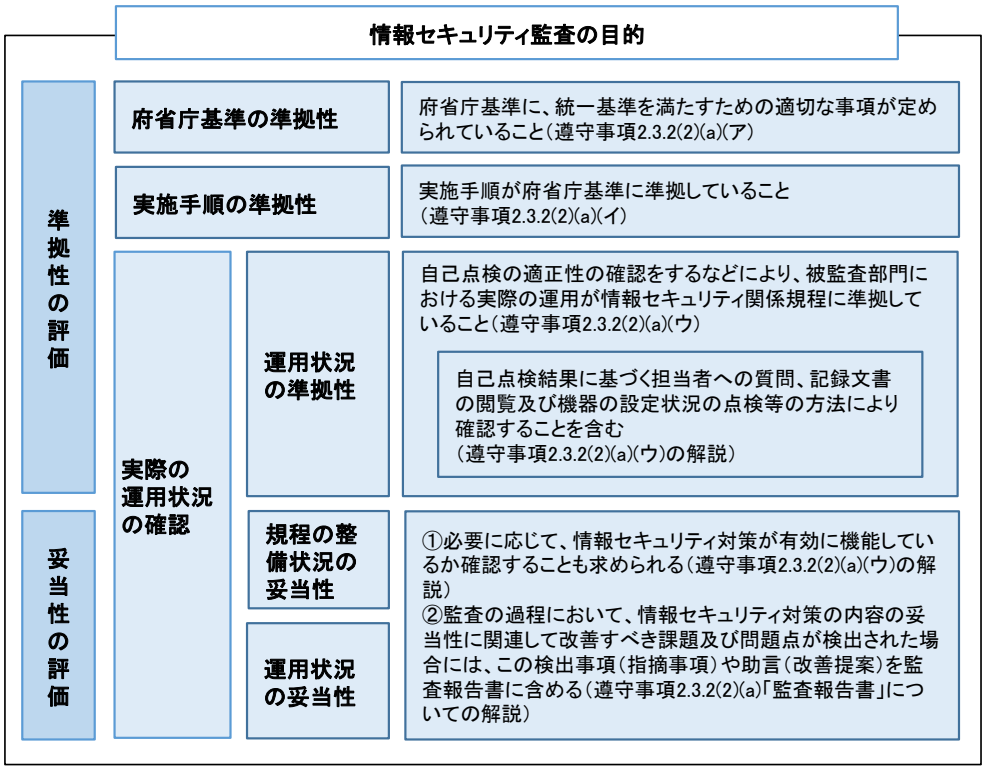

図 1.1-2　情報セキュリティ監査の目的について

1.2. 情報セキュリティ監査実施手順に含めるべき事項

情報セキュリティ監査実施手順には、以下の事項を具体化させて記載する。

(1) 統一基準（平成28年度版）に定める情報セキュリティ監査実施手順に係る遵守事項

2.1.1 組織･体制の整備（３）情報セキュリティ監査責任者の設置
2.3.2 情報セキュリティ監査（１）監査実施計画の策定
2.3.2 情報セキュリティ監査（２）監査の実施
2.3.2 情報セキュリティ監査（３）監査結果に応じた対処

(2) 情報セキュリティ監査の実施に係るその他の留意事項

(1) に示す遵守事項のほか、情報セキュリティ監査の実施に係る留意事項として、以下の項目を考慮する。

・情報セキュリティ監査の府省庁内での位置付けの明確化（府省庁内規程の作成等）
・情報セキュリティ監査の実効性の確保（監査チームの編成及び監査人の行動原則の明確化等）
・情報セキュリティ監査実施の効率化（自己点検結果の活用及びリスクアプローチの監査等）

1.3. 本策定手引書の利用方法

(1) 本策定手引書の構成

策定手引書は、第１部「情報セキュリティ監査実施手順の策定手引書の使い方」と第２部「情報セキュリティ監査実施手順」から構成されている。

第２部「情報セキュリティ監査実施手順」は、実施手順のひな形となるように作成されている。また、実施手順の利用者の理解を深めるために解説を加えている。

(2) ひな形の手直しポイント

統一基準に基づき策定された府省庁対策基準に準拠した情報セキュリティ監査実施手順を新規に策定又は改定する場合には、策定手引書の事項を踏まえて作業を行うことが望ましい。

第２部「情報セキュリティ監査実施手順」は、府省庁が実施手順を策定する際のひな形として利用することを想定しているが、府省庁の特性に合わせて実施手順を修正することが望ましい（図1.1-1「策定手引書と統一基準群との関係」を参照）。

特に、本文中において《　》で囲まれている部分については、府省庁において適切な内容に変更することが望ましい。

また、府省庁が策定手引書を利用せず、府省庁の特性に合わせて独自の実施手順を策定することを妨げない。

1.4. 参考資料

「情報セキュリティ監査実施手順」の策定に際しては、本策定手引書の他、以下のような資料が参考となる。

(1) 経済産業省「情報セキュリティ監査基準Ver1.0」
(2) 経済産業省「情報セキュリティ監査基準　実施基準ガイドラインVer1.0」
(3) 経済産業省「情報セキュリティ監査基準　報告基準ガイドラインVer1.0」
http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
(4) 特定非営利活動法人 日本セキュリティ監査協会「情報セキュリティ監査制度普及啓発活動報告」
http://www.jasa.jp/information/result.html?key=2004
(5) 日本公認会計士協会　監査基準委員会報告書500「監査証拠」
(6) 日本公認会計士協会　監査基準委員会報告書530「監査サンプリング」
(7) 日本公認会計士協会　監査・保証実務委員会研究報告書第19号「重要な虚偽表示のリスクの評価方法」

第２部　情報セキュリティ監査実施手順

1.　情報セキュリティ監査実施手順の概要

1.1.　情報セキュリティ監査実施手順の目的

情報セキュリティ監査実施手順（以下「監査実施手順」という。）は、統一規範に準拠して、情報セキュリティ監査（以下「監査」という。）を実施するに当たり、監査の各段階における監査実施手順を策定し、実効性のある監査を実施することを目的とする。

1.2.　用語の定義

監査実施手順において使用する用語の定義は、次に定めるところによる。

【あ】

【か】

- 「監査項目」とは、監査の評価を実施する単位をいう。
- 「監査項目に対する評価」とは、監査実施計画において立案した監査項目について、その整備状況及び運用状況を評価するために実施する監査業務をいう。
- 「監査実施計画」とは、監査において実施すべき事項の計画をいう。
- 「監査証拠」とは、監査項目に対する評価の結果を導くために利用する全ての情報をいう。

  監査人は、監査項目に対する評価の結果を導くに足る、十分かつ適切な監査証拠を入手する。
- 「監査対象」とは、情報セキュリティ対策が適切に実施されているか否かを正しく把握するために、監査項目に対する監査手続を実施する単位をいう。監査対象としては、監査で確認するために選択した組織、情報システム又は業務等が考えられる。
- 「監査調書」とは、監査業務の記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、適正に監査実施計画を策定し、監査を実施したという証拠、その他関連資料等をいう。情監査実施者自らが直接に入手した資料や監査手続の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。
- 「監査手続」とは、監査証拠を入手するために実施する手続であって、単独又は複数の監査技法を組み合わせたものをいう。
- 「監査責任者」とは、情報セキュリティ監査責任者をいう。
- 「監査実施者」とは、監査責任者が、監査実施計画に基づき、監査を実施させるために選任するものをいう。
- 「監査を支援する専門家」とは、監査責任者又は監査実施者が必要に応じて支援を求める、監査対象システムの詳細情報を有する組織又は府省庁内の情報システム部門等

の専門家をいう。

- 「監査人」とは、監査責任者、監査実施者及び監査を支援する専門家を含む総称をいう。
- 「監査ファイル」とは、紙媒体、電子媒体等に特定の監査業務に関連する監査調書をとりまとめたファイルをいう。

【さ】

- 「指摘事項」とは、監査の過程で発見された発見事項であり、監査報告書に含められて報告される事項をいう。
- 「情報セキュリティ監査責任者」とは、監査に関する事務を統括する者として、統一基準群が最高情報セキュリティ責任者に設置を求めるものをいう。
- 「実施手順」とは、府省庁対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
- 「情報セキュリティ関係規程」とは、府省庁対策基準及び実施手順を総称したものをいう。

【た】

【な】

【は】

- 「発見事項」とは、監査の過程における、準拠性に関する評価又は情報セキュリティ対策の内容の妥当性に関する評価において発見された事実をいう。
- 「府省庁対策基準」とは、府省庁における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。

【ま】

【や】

【ら】

【わ】

1.3. 監査実施手順の対象者

監査実施手順は、監査責任者、監査実施者及び監査を支援する専門家を対象とする。

1.4. 監査の基本的考え方

(1) 監査の実施は、府省庁対策基準に根拠を置く。

(2) 監査の実施に係る府省庁内規程等を作成し、監査業務及び手続に関する府省庁内での位置付けを明確化する。

(3) 監査は、監査実施計画に基づき、最高情報セキュリティ責任者の指示により実施する。
(4) 監査の客観性、実効性を確保するために、監査責任者は以下のことに配慮する。
  (a) 監査実施者の選任に当たっては、所属する課室長等と協議をした上で、府省庁内から広く選定することとし、原則として任期は《2 年》とする。
  (b) 専任の監査実施者の確保が困難であることを考慮し、併任により監査実施者を任命する場合には、監査業務が他の業務から影響を受けないよう、監査実施者に指示する。
  (c) 監査責任者及び監査実施者等で、府省庁内における監査チームの組織を編成することを検討する。
  (d) 監査実施者には、自らが直接担当している業務や情報システムの監査を実施させない。
  (e) 監査実施者に対して、監査で知り得たことを監査業務以外では利用しないよう、周知徹底する。
  (f) 必要に応じて、監査業務の外部委託の活用を合わせて検討する。
(5) 監査調書又は監査報告書を含む監査関連文書は、府省庁内の文書管理規程規定及び監査の重要性等に鑑みて、情報の格付を実施するなど適切に取り扱うとともに、決定した保管方法、保管者、保存期間等に従い適切に保管する。

1.5.　監査の目的及び位置付け

監査には、準拠性評価を目的とした監査と妥当性評価を目的とした監査がある。

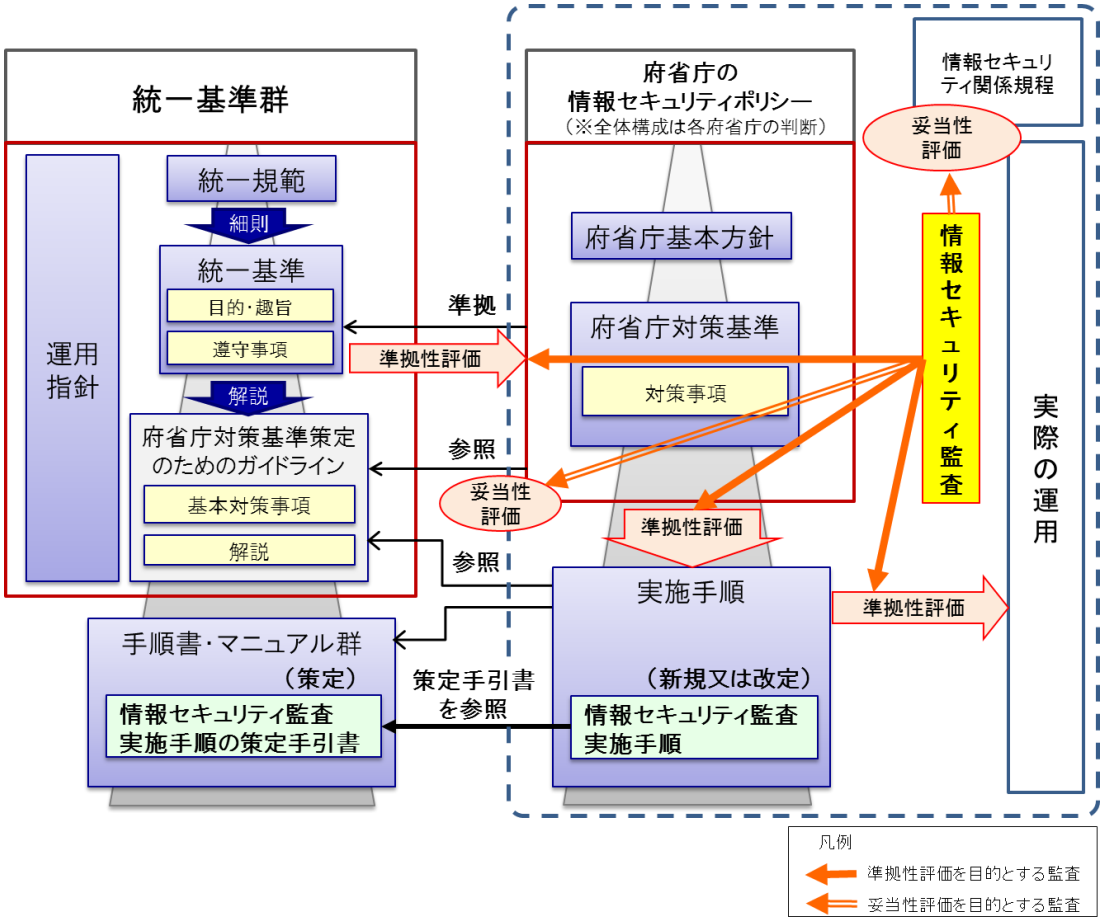

図 1.5-1　統一基準における監査の目的及び位置付け

(1)　準拠性評価を目的とする監査

監査責任者は、統一基準の 2.3.2 (1) 監査実施計画の策定の遵守事項により、以下の事項を監査するために、準拠性の評価を目的として監査を実施し、準拠性違反がある場合には改善提案を行う。

(a)　府省庁対策基準が統一基準に準拠しているかを評価する。

(b)　実施手順が府省庁対策基準に準拠しているかを評価する。

(c)　情報セキュリティ対策の運用が情報セキュリティ関係規程に準拠しているかを評価する。

(2)　妥当性評価を目的とする監査

監査責任者は、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点を発見した場合には、その指摘事項と合わせて改善提案

を行う。また、必要に応じて、情報セキュリティ対策が有効に機能しているかという観点から監査を実施する。

（解説）

- **1.5. (2) 情報セキュリティ対策の内容の妥当性**

  統一基準の遵守事項 2.3.2(2)(a)「監査報告書」についての解説により、監査責任者は、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点が発見された場合には、この指摘事項や改善提案を監査報告書に含めることが望ましい。

  情報セキュリティ対策の内容の妥当性とは、府省庁対策基準等が統一基準や JIS Q 27002 等の基準や府省庁の情報セキュリティを取り巻く状況等に照らし、府省庁として必要な水準を満たしていることである。

- **1.5. (2)「情報セキュリティ対策が有効に機能しているか」について**

  統一基準の「遵守事項 2.3.2(2)(a)(ウ)の「実際の運用」について」の解説により、監査責任者は、必要に応じて、情報セキュリティ対策が有効に機能しているか確認することが望ましい。

  情報セキュリティ対策が有効に機能しているとは、府省庁対策基準等が、府省庁のおかれた状況に照らして、情報セキュリティ対策を効果的かつ効率的に実施できるものになっていることである。

  例えば、情報セキュリティ対策が有効に機能していることの評価とは、次のことをいう。

  （整備状況の有効性評価）

  情報セキュリティ対策の整備状況の有効性評価とは、府省庁の特性を踏まえて、評価対象となる対策が、情報セキュリティに係るリスクの発生を十分に低減できる設計になっていることを確かめることである。

1.6.　監査業務の全体像

監査業務は、図 1.6-1「監査業務の全体像について」の流れに従って進める。

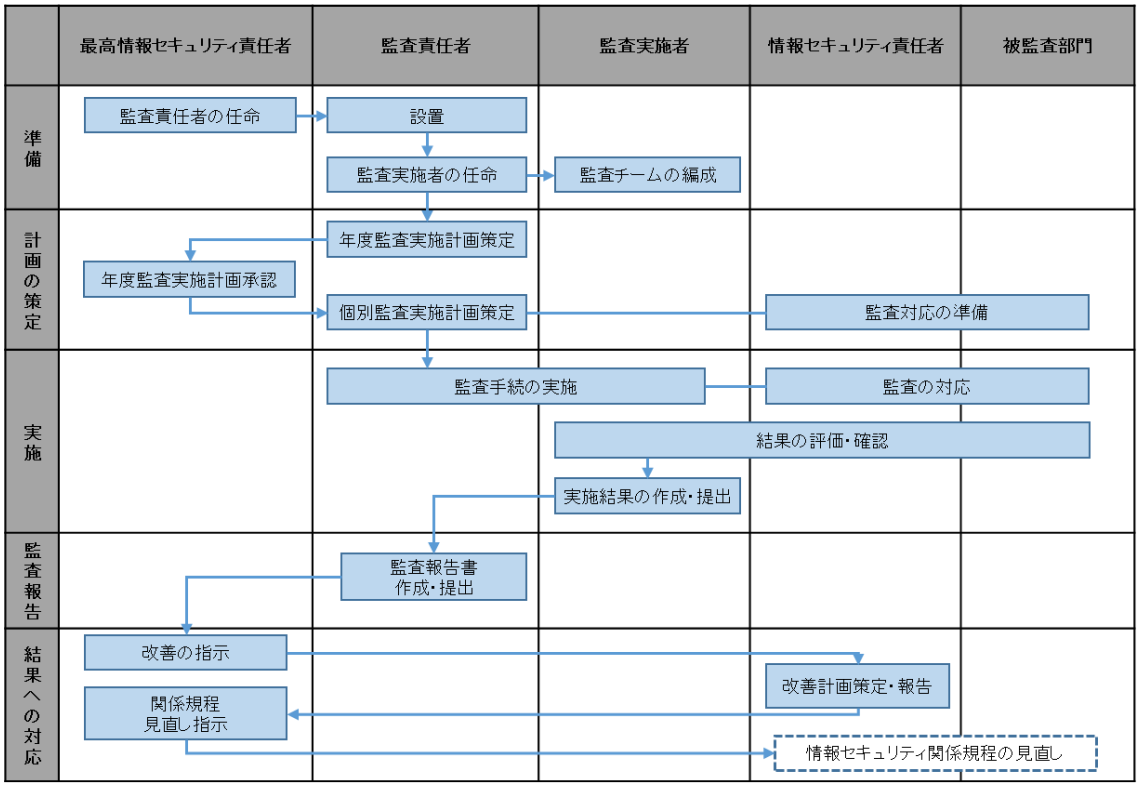

図 1.6-1　監査業務の全体像について

2.　監査実施に当たっての前提及び準備

2.1.　監査責任者の役割及び権限

(1) 監査責任者は、最高情報セキュリティ責任者の指示に基づき、監査に関する事務を統括する。
(2) 監査責任者は、年度監査実施計画及び個別監査実施計画を策定し、監査を実施する。
(3) 監査責任者は、監査実施者を選任し、監査チームを編成する。
(4) 監査責任者は、監査調書に基づき、監査の結果を監査報告書として作成し、最高情報セキュリティ責任者に報告する。
(5) 監査責任者は、監査実施計画の立案、監査マニュアルの整備及び監査調書のレビュー等のプロセスを通じて、監査業務の品質を管理する。
(6) 監査責任者は、情報セキュリティ委員会への出席や各情報セキュリティ責任者への質問等により、継続的に情報セキュリティ関係規程の整備状況や対策の実施状況、情報セキュリティ事案や違反の発生状況等の情報収集に努める。

（解説）

- **2.1. (5)「監査業務の品質」について**

  監査業務の品質とは、実施された監査が、府省庁対策基準、実施手順及び外部委託に係る契約書等の監査の基準に準拠して適切に行われているという監査業務の信頼性及び有効性のことをいう。

2.2.　監査実施体制の確立及び監査実施者の選任

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を府省庁内から広く選定し、監査実施体制を確立する。
(2) 監査責任者は監査実施者を選任する際に、監査責任者自らの所管する部署又は府省庁内の各部局からメンバーを選定する。監査責任者は、必要に応じ監査実施者に対する兼務発令や業務指示を発効する。
(3) 監査責任者は、必要に応じ、監査責任者と監査実施者等で構成する監査チームを編成する。
(4) 監査責任者は、監査対象となる情報システムや業務、情報資産の運用に直接携わる者に、監査実施者として当該情報システム等を対象とする監査を実施させないようにする。
(5) 監査責任者又は監査実施者は、必要に応じて、監査対象システムの詳細情報を有する組織、府省庁内の情報システム部門等の専門家の支援を受ける。

(6) 監査責任者は、監査の一部業務を外部に委託した場合でも、府省庁内に相当程度の監査実施者を確保する必要があることに留意の上、監査実施体制を検討する。

(7) 監査責任者は、組織内に監査を実施する者又は監査遂行能力が不足していると判断した場合、必要に応じて監査の一部業務の外部委託を検討する。

(8) 監査責任者は、外部委託をする場合、委託先の選定に当たり、被監査部門との独立性及び監査遂行能力を有している者を選択する。

（解説）

- **2.2. (3)「監査チームを編成する」について**

  監査チーム編成において、次の事項に配慮する。

  - 各監査実施者の通常業務と監査業務の負荷バランス
  - 監査実施者間の相互チェック機能の確保
  - 適切な職務の分担による監査対象からの独立性の確保

- **2.2. (6)「監査実施体制を検討する」について**

  監査に必要な人的リソースの目安として、監査対象とする項目や情報システム、業務の数及び実施する監査の方法により、必要となる監査実施者の人数や能力を明らかにする。

  この一部の人員を外部委託することにより確保した場合でも、府省庁内にかなりの人的リソースを確保しなければならないことに留意の上、計画を立てることが重要である。

- **2.2. (7)「監査遂行能力」について**

  監査遂行能力とは、監査に関する能力や経験と監査対象業務及び情報セキュリティに対する知識・技術等からなる。

- **2.2. (8)「委託先の選定」について**

  監査業務の委託先の選定に関する事項として、委託先の選定に当たっては、「情報セキュリティ監査企業台帳」に登録されている企業や情報セキュリティ監査又は情報システム監査に係る各種資格の保有者等の参画を要件とすることも一案である。

2.3. 監査人の行動原則

監査人は、自らを律し、その職責を果たすため、以下の事項に留意する。

(1) 誠実性

監査人は、常に誠実に行動しなければならず、次のような報告又は情報であると認識

しながら、その作成や報告に関与してはならない。

（ア）　重要な指摘事項を、正当な理由なく指摘事項として取り扱わない報告等

（イ）　重要な誤びゅうが含まれている報告等

（ウ）　必要な情報を省略する又は曖昧にすることにより誤解を生じさせるような場合において、当該情報を省略する又は曖昧にする報告等

(2)　外観上の独立性

監査人は、監査を客観的に実施するために、監査対象から独立していなければならない。外観上の独立性とは、監査の関係者（監査報告書の利用者を含む）から、監査人の誠実性及び精神上の独立性が阻害されているのではないかと推測される次のような事実や環境をさけることをいう。

（ア）　経済的利害関係

（イ）　独立性を疑われる不適切な外観

(3)　精神上の独立性

監査人は、監査の実施に当たり、偏向を排し、常に公正かつ客観的に判断を行わなければならない。

(4)　注意義務

監査人は、監査の全ての過程において、府省庁における情報セキュリティ対策の状況に対して予断を持つことなく、他の慎重な監査人であれば払うであろうと想定される注意を払う。

(5)　専門的能力

監査人は、情報セキュリティ及び監査に関連する知識、技能、その他の能力を、監査に必要とされる水準に維持するよう努めなければならない。

（解説）

- **2.3. (1)「誠実性」について**

  誠実性とは、公平であること及び正直であることを意味する。

- **2.3. (2)（イ)「独立性を疑われる不適切な外観」について**

  監査人は、当該監査人が実施する監査の対象となる行政事務や情報システムに現に関与する者でないように留意する。また、次のような状況にある場合は、外観上の独立性が確保できているか慎重に検討する必要がある。

  - 監査人が、最近まで監査の対象となる行政事務に関与していた場合
  - 監査人が、監査の対象となる情報セキュリティ対策の策定、導入その他整備及び運用に関与していた場合
  - 監査人が、近々、監査の対象となる機関の行政事務に関与することが予定されている

（次頁に続く）

場合

・ 監査人が、近々、監査の対象となる情報セキュリティ対策の策定、導入その他整備及び運用に関与することが予定されている場合

- **2.3. (3)「偏向を排し、常に公正かつ客観的に判断を行わなければならない」について**

偏向を排しとは、監査人の判断を歪めるおそれのある諸要因から影響を受けない精神状態を維持していることをいう。

常に公正かつ客観的に判断を行うとは、客観性を確保し、専門家としての公正普遍な態度を堅持できる状態を保持していることをいう。

- **2.3. (4)「他の慎重な監査人であれば払うであろうと想定される注意」について**

監査の実施において払うべき注意は、監査人によって相違するものではなく、同一の状況下において、他の慎重な又は平均的な監査人であれば払うであろうと想定される注意を指す。

- **2.3. (5)「監査に必要とされる水準」について**

監査に関連する専門領域は多岐に亘ることから、その全てについて十分な知識、技能、その他の能力を有する人材は稀有であり、監査人がその習得を試みることは現実的ではない。一方で、個別の専門領域に限定すれば、そのいくつかについては、外部に十分な水準の業務を提供できる専門家が存在している。このため、現実的には、監査人自らが全ての監査業務を実施するのではなく、外部の専門家の利用を検討することが想定される。

外部の専門家を利用する場合においても、監査人は、監査に関連する全ての専門領域について、少なくとも、専門家の業務及びその適切性を理解できる水準の知識、技能、その他の能力を有することが求められる。

【監査に必要とされる専門領域】

監査に求められる専門領域としては、次のものが挙げられる。

・ 監査
・ リスクマネジメントシステム
・ リスク評価
・ 情報セキュリティ上のリスクの動向
・ 情報ネットワーク
・ オペレーティングシステムとアプリケーション
・ 情報セキュリティ上のリスクに対する主なコントロール
・ インシデント対応体制
・ 事業継続計画

3. 監査実施計画

監査実施計画には、年度計画となる「年度監査実施計画」と個別の監査対象ごとの計画となる「個別監査実施計画」の２つがある。

3.1. 年度監査実施計画の目的と位置付け

年度監査実施計画の目的は、監査チーム内で情報を共有することにより、府省庁内における監査業務を円滑に実施することである。

統一基準においては、対策推進計画に監査の取組の方針・重点及びその実施時期を含めることとされていることから、当該記載に基づき、年度監査実施計画を策定する。この際、対策推進計画に監査の目的、対象、実施時期及び管理体制等を記載することにより、当該記載をもって年度監査実施計画とすることができる。

中・長期計画を策定する場合、監査責任者は、当該年度の監査計画の策定に当たり、必要に応じて、3 ヵ年程度以上の中・長期計画を策定し、重点監査対象の年度展開及び当該年度に実施すべき監査の水準・詳細度等を設定する。

3.2. 年度監査実施計画の策定手順

(1) 監査責任者は、《毎年 2 月末日》までに、翌年度の年度監査実施計画を策定する。

(2) 監査責任者は、年度監査実施計画の策定に当たり、対策推進計画における当該記載と整合性を確保した上で、監査を効果的かつ効率的に実施するため、府省庁を取り巻く環境を概括的に把握し（予備調査）、それに基づいて情報セキュリティに関連するリスク等を重視した年度監査実施計画を策定する（リスクアプローチの監査）。
監査責任者は、当該年度に実施する監査対象、監査項目及び監査目標を明確化する。

(3) 中・長期計画を策定している場合は、当該中・長期計画に沿って当該年度における年度監査実施計画を策定する。

(4) 監査責任者は、実施時期の調整や内容の重複の回避等に配慮し、計画を策定する。

(5) 監査責任者は、年度監査実施計画に次の事項を記載する。
  (a) 監査方針
  (b) 府省庁の概要
  (c) 情報セキュリティに関連する動向
  (d) 過去の監査の内容と指摘事項
  (e) 監査対象（業務、情報システム、段階等）、監査項目及び監査目標（例えば、機密性、情報漏えい防止、不正アクセス防止等）
  (f) 監査スケジュール

(g)　監査業務の管理体制
(h)　外部委託による監査及び外部専門家の活用の必要性及び範囲
(i)　リソース管理（監査予算、人材育成計画等）

(6) 策定した年度監査実施計画は、最高情報セキュリティ責任者の承認をもって、《当該年度４月１日より》発効する。

(7) 監査責任者は、年度監査実施計画の策定後、情報セキュリティに関連するリスクの大きな変動等があった場合には、適宜本計画を修正し、最高情報セキュリティ責任者の承認を得る。

（解説）

- **3.2. (2)「監査を効果的かつ効率的に実施するため、府省庁を取り巻く環境を概括的に把握し（予備調査）、それに基づいて情報セキュリティに関連するリスク等を重視した年度監査実施計画を策定する（リスクアプローチの監査）」について**

監査において、府省庁の情報セキュリティ対策を網羅的にチェックすることは、限られた監査資源（人、時間）のために形式的なチェックとなり重要な問題を見逃す可能性がある。また、重要な情報セキュリティ対策とそうでない対策を区別なく一律にチェックすることは、監査上重視すべきポイントについて深く追及できない可能性がある。そのため、監査を効果的かつ効率的に実施するためには、情報セキュリティに関連するリスク等を重視して、そのリスクに対して監査資源を割り当てることが大切である。このように監査上重要なリスクを重視した監査をリスクアプローチの監査という。

監査責任者は、監査上重要と考えられる「情報セキュリティに関連するリスク等」を識別するため、府省庁の概要及び情報セキュリティに関連する動向を把握し、府省庁を取り巻く情報セキュリティに関連するリスクを暫定的に評価する。この暫定的な評価は、監査により検証するための仮説として監査責任者の判断により識別されたリスクであり、府省庁の公式な情報セキュリティのリスク評価ではないことに留意する。

当年度の監査の終了までに、年度監査実施計画に重要な影響を与える事象が発生した場合には、当該影響について分析・検討し、暫定的に評価した情報セキュリティに関連するリスクを修正し、年度監査実施計画を更新する。このため監査実施計画は、監査終了時に確定することに留意する。

- **3.2. (2)「監査対象、監査項目及び監査目標」について**

①　監査対象

監査対象とは、監査で確認するために選択した組織、情報システム又は業務等である。

（次頁に続く）

監査責任者は、府省庁の概要及び情報セキュリティに関連する動向に基づき、顕在化することによって府省庁の有する情報資産又は情報システムの機密性、完全性及び可用性に影響が生じる可能性の高いリスクを評価して、監査対象を決定する。リスクの評価に当たっては、例えば次の事項を検討する。

・ 機密性の高い情報資産に関連するリスクであるかどうか
・ 発生の蓋然性の高い脅威に関連するリスクであるかどうか

② 監査項目

監査項目は、選択した監査対象に対して確かめたい事項であり、例えば次のものである。

・ 府省庁対策基準に統一基準を満たすための適切な事項が定められていること
・ 実施手順が府省庁対策基準に準拠していること
・ 実際の運用が府省庁対策基準及び実施手順に準拠していること

③ 監査目標

監査目標とは、監査対象及び監査項目を対象にした監査において確かめたい立証命題である。一つの監査項目に対して、複数の監査目標を挙げてもよい。監査項目に統一基準の項目を利用した場合には、統一基準の内容が監査目標として想定される。このように、監査項目の内容により監査目標が明確な場合には、あえて監査目標を明示しなくてもよい。

監査対象、監査項目、監査目標の例

監査対象	監査項目	監査目標
府省庁対策基準及び実施手順	（ア）府省庁対策基準に統一基準を満たすための適切な事項が定められていること （イ）実施手順が府省庁対策基準に準拠していること （ウ）実際の運用が府省庁対策基準及び実施手順に準拠していること並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当であること	・府省庁対策基準の統一基準群への準拠性 ・実施手順の府省庁対策基準への準拠性 ・課室情報セキュリティ責任者の設置 ・CSIRT の体制　等
情報セキュリティ管理体制	情報システム対策の導入・計画、運用、点検見直しの整備・運用状況	情報セキュリティ管理体制が整備され、有効に機能していること等

（次頁に続く）

○○局の情報格付業務	情報の取扱いに係る整備・運用状況	○○局の情報の機密性が確保されていること等
府省庁内 LAN	府省庁内 LAN の運用状況	不正アクセスの防止対策が有効に機能していること等

- **3.2. (3)「中・長期計画を策定している場合」について**

  中・長期計画を策定している場合とは、例えば次のような中・長期計画に沿って当該年度における年度監査実施計画を策定する。

  ・ 初年度　：府省庁内情報セキュリティ対策の実施状況の把握及び評価
  ・ ２年度目：情報セキュリティ対策実施に関する日常業務への浸透
  ・ ３年度目：情報セキュリティ対策の定着化及び府省庁内セキュリティレベルの底上げ

- **3.2. (5)「年度監査実施計画に次の事項を記載する」について**

  監査責任者は、監査対象及び監査対象に係る監査項目並びに監査業務の実施に係る体制とスケジュールを検討した過程を監査調書に記録し、その内容を取りまとめて年度監査実施計画書を策定する。

- **3.2. (5) (a)「監査方針」について**

  対策推進計画に記載した監査の基本的な方針を前提として、府省庁を取り巻く環境を踏まえて、年度の監査方針を記載する。

- **3.2. (5) (b)「府省庁の概要」について**

  情報セキュリティ対策は、組織の目的、規模、編成や情報システムの構成、取り扱う情報の内容、用途等といった府省庁の特性を勘案しつつ、自らの組織が如何なる手段を採れば情報セキュリティが最も適切に確保されるのかとの視点から検討する。

  監査責任者は、年度監査実施計画の策定に当たり、情報セキュリティの観点からこれらの特性を判断するため、次の項目を含む情報を収集し、監査調書に記録するとともに、その内容を取りまとめて年度監査実施計画に簡潔に記載する。特に、前年度から重要な変化が見られた項目がある場合は、それによって新たな情報セキュリティ対策を講じる必要性を生じさせることがあることに留意する。

（次頁に続く）

①　基礎情報

次のものを含む府省庁に関する基礎情報を記載する。特に、前年度から大きく変化した項目については、その旨が明らかになるように記録する。

- 年度予算等規模に関する情報
- 構成員の概数
- 地方拠点の有無等拠点に関する情報
- 外局や所管法人等関連する機関に関する情報

公開ウェブサーバ等に情報が記載されている場合は、当該情報と現状に大きな乖離がない場合に限り、当該情報のスクリーンコピー等を調書化することで代替することも考えられる。

構成員数の増加や地方拠点の変更は、端末管理の仕組みやネットワーク構成の変更等を伴う場合が多い。また、新たな拠点の場合は、他の拠点とは異なる物理的セキュリティ対策を導入していることも考えられる。

②　所掌事務

府省庁が所掌する事務に関する情報を記載する。事務分掌表等を調書化することで代替することもできる。特に関連する法令等の制改定によって所掌事務に変化がある場合は、当該法令等の名称及び変化の内容が明らかになるように記録する。

③　重要な情報資産

府省庁が有する情報資産について記載する。府省庁が取り扱う情報資産は、その所掌事務によって規定されるという側面があるため、所掌事務と関連付けて把握することが望ましい。

また、重要な情報資産は、機密性 3 情報に限るものではない。当該情報の漏えいが府省庁に対して大きな影響を与えると府省庁が判断する場合は、当該情報が機密性 2 情報に区分されるものであっても、重要な情報資産として把握する。

④　情報システムに対する資源の状況

情報システムに対して確保されている予算に関連する情報として、情報システムの更改の状況や情報システムの管理要員の規模について記載する。

情報システムの更改や統廃合は、業務の流れや情報セキュリティに関連するコントロール、外部委託の状況等に影響を与える。対象となる情報システムの規模によっては、更改等に数年を要することも考えられることから、記載対象とする期間は直近に限定することなく、本監査の計画策定に影響を与える範囲を検討する必要がある。

一方、情報システムの管理要員の規模は、情報システムの規模との関係性において、その運用状況の有効性に影響を与える。府省庁全体の情報システムに関するセキュリティを統括する部署、要員、専任又は兼務の別、担当者の情報セキュリティに係る知識や技能その他の能力、委託会社の利用の有無及びその内容（人数や常駐の有無等）等、関連する状況を把握する必要がある。また、情報システムの管理要員の異動は、情

（次頁に続く）

報セキュリティに係る知識や技能、その他の能力が大きく変動する場合や、属人的な運用に関して十分な引継ぎがなされていない場合等、情報セキュリティ上のリスクが高まる要因となることがある。

⑤　情報システムの概要及び構成

次のものを含む、府省庁が保有する情報システムに関する基礎情報を収集する。

- 情報システムの名称
- 情報システムにおいて取り扱う情報資産
- 情報システムの責任者
- 情報システムを構成する主要なハードウェア、ソフトウェア、OS、データベース、ネットワーク機器及び回線等

政府情報システム管理データベース（ODB）や政府情報システム改革ロードマップ、ネットワーク構成図等を上記の補足資料とすることも考えられる。

小規模な情報システムやスタンドアロンの情報システムが大量に存在する場合や、多数のハードウェアやソフトウェアから構成される大規模な情報システムの場合には、その内容を網羅的かつ精緻に把握、記載することが困難な場合があるが、必ずしも網羅的かつ精緻な記載を要するものではない。

情報システムの在り様は、府省庁の情報セキュリティに係るリスク及び情報セキュリティ対策の水準に大きな影響を与える。特に、情報システムの導入や更改は、設計の不備や作業時のミス等により情報セキュリティ上のリスクが高まる要因となることがある。したがって、情報システムの更改や統廃合等、前年度から重要な変更がある場合は、監査人は、個別に監査調書を作成してその内容を記載することを検討することとする。

⑥　委託管理の状況

府省庁の有する重要な情報を取り扱う業務に係る外部委託について、その管理の整備状況及び管理体制並びに当該管理体制の運用状況の概要について記載する。

委託管理の整備状況及び管理体制には、調達段階における外部委託の可否の検討、委託先に対する情報セキュリティ対策に係る要求事項の選定、契約時における要求事項の充足に係る点検及び契約後の継続的なモニタリングといった管理策だけではなく、委託管理に係る規程の見直しの実施等、府省庁全体としての委託管理に係るマネジメントシステムも含まれる。

⑦　委託会社が提供する業務

次のものを含む府省庁が外部に委託している行政事務に関する基礎情報を収集する。

- 委託会社の名称
- 委託業務において取り扱う情報資産
- 委託業務の責任者
- 委託業務の内容

（次頁に続く）

委託会社が提供する業務に係る記載は、特に重要な情報を取り扱うものは網羅性を確保できるよう努める。重要な情報を取り扱う委託業務は、システム開発や運用管理等、主として情報システムに関連するものになるが、必ずしも情報システムに関連するとは限らないことに留意する。例えば、重要な情報を委託会社で処理させる場合等がこれに該当する。

委託業務は、府省庁の行政事務を構成する一部の業務を外部に委託するものである。この観点から、当該業務についても府省庁の行政事務と同等又は同等以上の情報セキュリティ対策の水準が確保されている必要がある。一方、委託会社は府省庁と独立した外部の組織であり、情報セキュリティ対策を含む統制に係る府省庁の影響が及びにくい。したがって、委託会社の業務の状況及びそれに対する府省庁の管理体制は、総体として府省庁の情報セキュリティに係るリスク及び情報セキュリティ対策の水準に大きな影響を与える。このため、新規の委託業務や委託先の変更等、前年度から重要な変更がある場合は、監査人は、個別に監査調書を作成してその内容を記載することを検討することとする。

- **3.2. (5) (c)「情報セキュリティに関連する動向」について**

監査責任者は、サイバー攻撃の動向等、情報セキュリティに関連する世の中の動向について概括的に把握し、その結果を監査調書に記録するとともに、その内容を取りまとめて年度監査実施計画書に簡潔に記載する。概括的に把握すべき情報セキュリティに関連する動向には、次の事項が含まれる。

①　情報セキュリティに関連する政府の動向

情報セキュリティに関連する法令等の施行や情報セキュリティに関連する重要な戦略等の決定の事実について記載する。

政府における情報セキュリティ対策や個人情報等の秘匿性の高い情報の保護に係る法令の施行又は制改定、サイバーセキュリティ戦略及びそれに基づく年次計画その他情報セキュリティに関連する方針や施策の決定は、府省庁が実施すべき情報セキュリティ対策に広く影響を及ぼす可能性がある。

②　情報セキュリティ上のリスクを高める社会の動向

政府機関に対するサイバー攻撃が発生する蓋然性を高めるようなイベントや動向について記載する。例えば、次のような事象は政府機関に対するサイバー攻撃のリスクを高める可能性がある。

・ オリンピックや万国博覧会等、全世界的なイベントの開催
・ サミット等各国の要人が一堂に会する国際会議の開催

このような事象のうち、府省庁の業務の特性やそれに関連する特定の状況により、特に府省庁に係る情報セキュリティ上のリスクを高める可能性のあるものは、その旨を記載する。

（次頁に続く）

③　情報セキュリティに係る重大な事案の動向

情報セキュリティに係る重大な事件や事案に関する近年の全体的な動向について記載する。

対象とする事件や事案には、外部からのサイバー攻撃だけではなく、関係者による機密情報の不正利用等の内部不正や、機密情報を保存した USB メモリの紛失等の事案を含む。また、府省庁で発生したものに加え、民間や海外で発生した重要な事案も対象とする。後者のうち、府省庁において同様の事案が生じるおそれが高いものについては、当該事件や事案の概要、規模、原因、終息状況、課題点等の具体的な内容を記載することも考えられる。

④　情報セキュリティに関する新しい脅威や脆弱性

サイバー攻撃に係る技術的又は社会的な手法に関する動向や、ソフトウェアの脆弱性に関して直近に判明した社会的影響の大きいものに関する情報等、情報セキュリティ上の脅威又は間接的に脅威になりうる脆弱性の情報について記載する。

サイバー攻撃の手法には一定の流行があり、重大な事案の動向と並んで、これらの情報を把握することは府省庁におけるリスク評価及びそれに対する情報セキュリティ対策の状況を検討するのに役立つ。このような情報には、内閣サイバーセキュリティセンターから提供されるものを含む。

- **3.2. (5) (d)「過去の監査の内容と指摘事項」について**

監査責任者は、府省庁が過去に実施した監査に関する情報を監査調書に記録し、その内容を取りまとめて年度監査実施計画書に簡潔に記載する。監査調書に記録する情報は、次の事項が含まれる。

①　監査対象及び監査項目並びにその結果

これらの情報は、監査の対象及び監査項目の検討に資するため、当該結果が現在においても有効であると判断される場合に限り、その判断根拠とともに記載する。

例えば、過去に情報システムの運用状況を監査対象とし、適切な運用がされていると結論付けられている場合、当該結論付けた時点から現在に至るまで当該情報システム及びその運用体制に大きな変更がないのであれば、当該情報システムの運用状況に係るリスクは十分に低減された状況にあると判断し、監査対象から除外できる可能性がある。

②　是正されたことが確かめられていない指摘事項

情報セキュリティ水準の自律的かつ継続的な向上を実現するため、監査で指摘された事項は、確実に是正される必要がある。このため、過去の監査における是正事項のうち、監査の枠組みで是正が確かめられていないものについては、その是正状況をフォローアップするため、一覧化して記載する。

（次頁に続く）

- **3.2. (5) (f)「監査スケジュール」について**

  監査責任者は、監査対象、監査項目及び監査手続並びに監査の実施体制に基づき、監査業務に係る所要日数を検討する。検討に当たっては、監査項目に対する評価手続に留まることなく、事前準備、監査証拠の整理、監査報告の案の作成及び監査対象との協議、監査報告書の承認を含む、監査業務全体に要する概算の日数を算定する。

  また、実施時期については、所掌事務の繁忙期等他の業務との重複に配慮し、過度な負担が生じないように調整する。

【例】年度監査実施計画のひな形

作成日：○○年○○月○○日
（情報セキュリティ監査責任者）
氏　　名

○○年度　○○省情報セキュリティ監査実施計画書

１．監査方針

情報セキュリティ対策を向上させるため、政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）に準拠して適切に対策基準を整備し、その対策基準に準拠して適切に運用していること、また対策基準とその運用が組織の特性に照らして妥当であることを確かめていること等について監査する。

府省庁対策基準の統一基準群への準拠性、実施手順の府省庁対策基準への準拠性及び実際の運用の実施手順への準拠性並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当性を評価し、当該評価結果に基づく指摘事項に関して改善提案を行う。

２．府省庁の概要

３．情報セキュリティに関連する動向

４．過去の情報セキュリティ監査の内容と指摘事項

５．監査対象、監査項目及び監査目標

(1) 重点監査対象等

監査対象	監査項目	監査目標
府省庁対策基準及び実施手順	（ア）府省庁対策基準に統一基準を満たすための適切な事項が定められていること （イ）実施手順が府省庁対策基準に準拠していること （ウ）実際の運用が府省庁対策基準及び実施手順に準拠していること並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当であること	・府省庁対策基準の統一基準群への準拠性 ・実施手順の府省庁対策基準への準拠性 ・課室情報セキュリティ責任者の設置 ・CSIRT の体制　等
情報セキュリティ管理体制	情報システム対策の導入・計画、運用、点検見直しの整備・運用状況	情報セキュリティ管理体制が整備され、有効に機能していること等

（次頁に続く）

○○局の情報格付業務	情報の取扱いに係る整備・運用状況	○○局の情報の機密性が確保されていること等
府省庁内 LAN	府省庁内 LAN の運用状況	不正アクセスの防止対策が有効に機能していること等

(2) その他の監査対象

インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

６．監査の実施体制：別紙のとおり

７．監査スケジュール：別紙のとおり

８．監査業務の管理体制：別紙のとおり

９．外部委託による監査の範囲及び必要性

(1) 外部委託の範囲及び必要性

① 範囲

インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

② 必要性

脆弱性スキャン、システム侵入テスト等専門的技術を要するため

(2) 委託契約の必要性の要否：要

１０．リソース管理

(1) 監査予算：別紙のとおり

(2) 人材育成計画：詳細別紙のとおり

① 目標：監査スキルの向上と要員の確保

② 監査業務基礎講座：4 月 1 日～4 月 30 日の 2 週間程度

③ 情報セキュリティ基礎講座：5 月 1 日～5 月 30 日の 2 週間程度

別紙

●監査業務の管理体制

（体制図の挿入）

（次頁に続く）

●監査スケジュール

監査業務のプロセス	監査対象	作業フェーズ	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
準備		監査チームの編成												
計画の策定		年度計画策定												
		個別監査実施計画策定												
実施	府省庁対策基準及び実施手順	往査												
		結果の評価・確認												
		実施結果の作成・提出												
	情報セキュリティ管理体制	往査												
		結果の評価・確認												
		実施結果の作成・提出												
	○○局の情報の格付	往査												
		結果の評価・確認												
		実施結果の作成・提出												
	府省庁内LAN	往査												
		結果の評価・確認												
		実施結果の作成・提出												
監査報告		監査報告書の作成・提出												
結果への対応		改善の指示等												

●監査予算

予算項目	項目概要	予算費目	金額	実施時期	実施担当者
出張費					
宿泊費					
外部委託費					
・・・					

●人材育成計画

育成内容	実施時期	実施方法	対象者	実施担当者
監査業務基礎講座	4/1~4/30	座学	全行政事務従事者	△△△△
・・・				
・・・				
・・・				

4. 個別監査実施計画

4.1. 個別監査実施計画の目的及び位置付け

(1) 個別監査実施計画は、監査対象や監査項目、監査手続を含む監査事務の詳細な計画であって、被監査部門を含む府省庁内の監査関係者と情報を共有することにより、監査の円滑な実施に資することを目的とする。

4.2. 個別監査実施計画の策定手順

(1) 監査責任者は、年度監査実施計画及び情報セキュリティの状況の変化に応じた最高情報セキュリティ責任者からの指示に基づき、個別の監査対象ごとの個別監査実施計画を策定する。

(2) 監査責任者は、府省庁対策基準等の規定文書の内容確認を行った上で、十分かつ適切な監査証拠を入手するために、情報セキュリティ上のリスク及びその他の個々の状況を考慮し、以下の単独又は複数の監査技法を組み合わせて監査手続を作成する。

【監査技法】

(a) 記録・文書又はシステム設定の閲覧（紙媒体、電子媒体その他の媒体による記録や文書を確かめる技法、以下のように情報システム機器等の設定情報を確かめる技法を含む。）

(ア) システム設定の閲覧（情報システムの設定情報を閲覧し、評価基準に整合した対策となっていることを確かめる技法）

(イ) ログの閲覧（情報システムのログを閲覧し、利用者や管理者の操作内容の妥当性、セキュリティ機能の有効性、インシデントの兆候の有無等を確かめる技法）

(b) 観察（監査人自らが業務の実施されている現場に赴き、その状況を目視によって確かめる技法）

(c) 質問（監査対象に関係すると考えられる者に問い合わせて、説明又は回答を求める技法。公式な書面による質問のみでなく、インタビュー等口頭による質問も含まれる。）

(d) 再実施（業務において実施している手順を再現することで、その有効性を確かめる技法）

(ア) プログラムテスト（情報システムのアプリケーションを実行し、意図したとおりに動作しているか、目標とした水準の品質を確保できているか、想定外の挙動を示さないかを確かめる技法）

(イ) データ整合・完全性テスト（情報システムに対して検証用データを入力し、デ

ータが漏れなく意図したとおりに処理されることを確かめる技法）

(ウ) ペネトレーションテスト（情報システムに対して様々な手法により実際に侵入や攻撃を試み、情報システムに脆弱性がないかを確かめる技法）

(3) 監査手続の作成に当たり、十分かつ適切な監査証拠の入手方法について検討する。

情報セキュリティ対策の整備状況の評価については、業務の流れに沿って、抽出した１～数件のサンプルにより確かめることができる。

情報セキュリティ対策の運用状況の評価については、通常、試査（母集団から一部のサンプルを抽出する方法）により監査証拠を入手する。その場合、監査実施者は、サンプル件数の決定方法等の監査サンプリングの計画を作成する。

(4) 監査責任者は、個別監査実施計画に次の事項を記載する。

(a) 監査目的
(b) 背景（直前の情報セキュリティの状況認識）
(c) 監査対象
(d) 被監査部門及びその責任者
(e) 監査実施責任者及び実施担当者
(f) 監査の実施時期
(g) 監査の実施場所
(h) 監査項目及び監査手続
(i) 監査の進捗管理手段
(j) 外部委託先との役割分担（外部委託を行う場合）

（解説）

- **4.2. (2)「十分かつ適切な監査証拠」について**

監査人は、監査項目に対する評価の結果を導くために、当該監査項目に応じた十分かつ適切な監査証拠を入手する。十分かつ適切な監査証拠を入手したかどうかは、監査人の判断に係る事項である。

監査証拠の十分性と適切性は独立した概念であるが、相互に関連することに留意する。

監査証拠の十分性とは、監査証拠の量、すなわち、監査項目に対する評価の結果を導くためにどれくらいの監査証拠が必要かという問題である。監査証拠の量が少なすぎれば、監査の有効性を損なうこととなり、監査証拠の量が多すぎれば、監査の効率性を損なうこととなる。

監査証拠の適切性とは、監査証拠の質、すなわち、監査項目に対する監査証拠の適合性（監査証拠が監査項目に合致していること）と証明力（監査証拠として利用する情報の信頼性）の問題である。

（次頁に続く）

- **4.2. (2) (a)「記録・文書又はシステム設定の閲覧」について**

記録・文書又はシステム設定の閲覧は、監査人が入手した情報セキュリティに関連する記録や文書又はシステム設定の内容を確かめる監査技法であり、質問と並んで監査の全ての過程で利用される。閲覧する記録や文書は、府省庁内部のポリシーや運用記録だけではなく、インターネット上で取得できる公開情報等を含む。

記録や文書の性質や情報源等によって、監査人が記録や文書の閲覧により入手する監査証拠の証明力は大きく異なる。したがって、記録や文書の閲覧によって監査証拠を入手する場合には、明らかに不要な場合を除き、監査調書に当該記録や文書の作成過程、入手経路その他証明力を評価できる情報を記載することが重要である。

記録や文書の閲覧は、監査項目に関連する部分だけを対象とすることがある。例えば、端末の持出に係る承認プロセスの運用状況の評価を目的として実施する場合、申請書における承認の有無を中心として記録を確かめることがある。

システム設定の閲覧については、次の「システム設定の閲覧」を参照する。

- **4.2. (2) (a)（ア）「システム設定の閲覧」について**

システム設定の閲覧は、府省庁に導入されている情報システムの設定情報を入手し、その内容を確かめる監査技法であり、記録や文書の閲覧の一種である。

システム設定の閲覧の対象となる設定情報は、IP アドレスやトランスポート層のポートによるアクセスコントロール、Web サーバの認証設定、メールサーバの SPF（Sender Policy Framework）認証設定、ファイルサーバの共有設定等が挙げられる。

システム設定の閲覧の方法として、詳細設計書やパラメータシート等の閲覧により設計レベルで確かめる方法と、機器やソフトウェアに対して現に設定されている設定情報を確かめる方法がある。いずれの方法においても高い技術的専門性を必要とするが、特に後者は特定の機器やソフトウェアに関する知識が要求されるため、当該手続が必要となった場合には、外部の専門家に請け負わせることを検討する必要がある。

- **4.2. (2) (a)（イ）「ログの閲覧」について**

ログの閲覧は、システムで取得されたログ（システムの利用者や管理者の当該システムに対する操作内容を、当該操作が実行された日時と実行した者を特定できる情報とともに記録したもの）を解析する監査技法であり、記録や文書の閲覧の一種である。

ログの閲覧は、例えば次のようなことを評価する目的で実施することがある。

・ 利用者や管理者の情報セキュリティ対策に係る操作内容や頻度が適切か
・ 導入済の情報セキュリティ対策に係るシステムが有効に機能しているか
・ インシデントの兆候はないか

ログの閲覧の対象となるログは、一般的に CSV や通常のテキストであり、膨大な行数になることが多い。このため、その解析には、スプレッドシートやデータベース、テキスト処

（次頁に続く）

理の専用ツールや高度な技能が要求される。したがって、当該手続が必要となった場合には、外部の専門家に請け負わせることを検討する必要がある。

- **4.2. (2) (b)「観察」について**

観察は、行政事務従事者等が情報セキュリティに関連する手順を実施している現場に赴き、その内容を確かめる監査技法であり、対象となる手順の運用に関する監査証拠を入手できる。しかし、観察を行った時点に関する監査証拠に限定され、また、当該手順の実施は観察されているという事実により影響を受けることがあることに留意する必要がある。

視察や立会といった監査技法は、観察の一種である。視察は、特定の手順に限定することなく執務室に赴き、業務の状況から情報セキュリティに関連する全体的な状況を把握する技法であり、担当者への質問を伴うことが多い。一方、立会は、重要な情報セキュリティ対策について担当者が実施する現場に同行する監査技法であり、委託先管理におけるオンサイト点検への同行等が挙げられる。

- **4.2. (2) (c)「質問」について**

質問は、監査人が情報セキュリティに関連する府省庁内外の関係者に情報を求める監査技法であり、質問以外の監査手続と組み合わせて監査の全ての過程で利用される。質問の方法は、質問管理表を利用した公式な書面による質問からインタビューを通じた質問、非公式な口頭による質問まで様々である。

質問に対する回答から、監査人は、新たな情報又は既に入手していた監査証拠を裏付ける情報を入手することがある。また、執務室に対する入退室管理の状況について、担当者による事前の説明とその他の行政事務従事者の説明が異なるなど、質問に対する回答から、監査人は既に入手した情報とは大きく異なる情報を入手することがある。質問に対する回答によっては、監査人は実施する手続を修正することや、監査手続を追加して実施することが必要となる。

質問は、多くの監査手続の一部を構成する主要な監査技法であるものの、その証明力は高いものではない。したがって、質問を通じて入手した監査証拠を他の監査手続等によって裏付け評価することは、質問を実施する上で必要不可欠なプロセスである。

- **4.2. (2) (d)「再実施」について**

再実施は、情報セキュリティに関して部局が実施しているコントロールの運用状況を評価するために、監査人自らが当該コントロールを試行することで、その妥当性や適否を確かめる監査技法である。例えば、ID カードによる入退室管理が行われている場合、ゲストカード等のアクセス権が付与されていないこととなっているカードを利用し、監査人自らがエラーとなることを確かめることや、システム利用時に認証エラーが一定の閾値を超えるとアカウントが凍結される場合、実際に認証エラーを発生させてアカウントの凍結状況

（次頁に続く）

を確かめること等が再実施に該当する。後者の例では、観察と組み合わせ、担当者に認証エラーの発生を依頼することも考えられる。

再実施による監査証拠は、監査人自らがコントロールを試行してその状況を確かめることにより入手するため、極めて高い証明力を有する。一方で、当該監査証拠は、監査人が試行した範囲、すなわち、監査人が試行した ID カードやアカウント、監査人が試行した日時等に限定した証拠能力しか持たない。すなわち、これらのコントロールが他の ID カードやアカウントにおいても有効であるか、あるいは、継続して適切な運用がなされているかについて評価しなければならない場合、再実施は必ずしもその目的に適合しないことに留意する必要がある。

- **4.2. (2) (d)（ア）「プログラムテスト」について**

プログラムテストは、開発したプログラムに組み込まれている情報セキュリティに係るコントロールが、要求された通りの機能を有しており、実際に機能していることを確かめる監査技法である。

運用開始後の情報システムに対するプログラムテストは、再実施の一種として実施されることが多いと考えられる。

- **4.2. (2) (d)（イ）「データ整合性・完全性テスト」について**

データ整合・完全性テストは、開発したプログラムに対して検証用データを入力し、その処理結果が期待されていたものと一致するか確かめる監査技法であり、プログラムテストの一種である。

データ整合・完全性テストの目的は、その名称からも明らかなとおり、情報システムによるデータの完全性を確かめることであり、高い整合性、完全性を求められるデータを処理するシステムの評価に適用することが想定される。例えば、テキストを流し込むと自動的に整形するような CMS（Content Management System; Web サーバのコンテンツ管理システム）が導入されている場合、当該整形によって意図しない情報の欠落や改変が生じないことを確かめる監査手続等が考えられる。

- **4.2. (2) (d)（ウ）「ペネトレーションテスト」について**

ペネトレーションテストは、システムに対して実際に侵入や攻撃を試みる監査手法であり、プログラムテストの一種である。システムへの影響を考慮し実際の侵入までは行わず脆弱性の有無の調査だけを実施する場合、脆弱性診断と呼ぶ場合がある。

ペネトレーションテストで用いる攻撃手法は既知のものであり、その種類は評価内容によって異なる。例えば、公開する意図のない情報を摂取できるか調べる場合には、外部からの不正アクセスによって脆弱性を利用することが多い。一方、システムが提供するサービスの可用性を評価する場合には、疑似的な DoS 攻撃を利用することとなる。いずれにして

（次頁に続く）

も、サイバー攻撃を取り巻く環境は日々変化しており、過去に本監査技法を適用したシステムであっても、その重要性に応じて定期的に実施することが望ましい。また、どのような手法を利用する場合でも高い技術的専門性が必要となるため、当該手続が必要となった場合には、外部の専門家に請け負わせることを検討する必要がある。この場合、事業者ごとに検査や有する技術が異なることから、毎回異なる事業者に請け負わせることで、新たな事項を検出できる可能性が高まる場合がある。

- **4.2. (3)「試査」について**

試査は、監査項目に関連する母集団を構成する全ての項目から一部を抽出し、監査手続の対象とする方法である。一般的に、監査項目に関連する全ての情報を入手し監査手続を実施することは、監査の効率性の観点から実務的ではない。このため、試査により監査手続の対象となる項目を抽出することが多い。

- **4.2. (3)「サンプル件数の決定方法等の監査サンプリングの計画を作成する」について**

運用状況の監査手続においては、サンプリングにより監査証拠を入手する。

サンプル件数については、対策の重要性、複雑さ、担当者が行う判断の性質、対策の実施者の能力、前年度の評価結果やその後の変更の状況を考慮して、サンプル件数を増加、あるいは減少させる。なお、サンプル件数については、以下の表が参考になる。

表 4.2.(3)　会計監査で使われているサンプリング数の例

母集団の数	サンプル件数
12 以下	2 件
13～24 以下	3 件
25～52 以下	5 件
53～250 以下	母集団の 10%
250 超	25 件

【例】個別監査実施計画書のひな形

作成日：○○年○○月○○日

（情報セキュリティ監査責任者）
氏　　名

○○年度　府省庁対策基準及び実施手順に関する個別監査実施計画書

１．監査目的

府省庁の府省庁対策基準で定めた情報セキュリティ管理体制の構築状況に関し、政府機関の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠して、整備・運用されていることを確かめる。
また、実施されている情報セキュリティ対策が有効に機能していることを確かめ、改善提案を行う。

２．背景

平成26年5月に統一基準群が改定され、府省庁でも従来の情報セキュリティポリシーを改定し、新たに府省庁対策基準を策定したところ、昨今政府機関からの情報漏えい事案も頻発しており、府省庁における情報管理体制の再確認が必要である。

３．監査対象：府省庁対策基準及び実施手順

４．被監査部門及び責任者：大臣官房○○課ＸＸＸＸ

５．監査実施体制

(1)監査実施責任者：△△△△
(2)監査実施者　　：△△△△

６．監査の実施時期：7月1日～9月30日の各月末の週（計15日間）

７．監査の実施場所：当府省庁内執務室

８．監査項目及び監査手続：別紙のとおり

９．監査の進捗管理手段：別紙のとおり

別紙

●監査項目及び監査手続

（ア）府省庁対策基準に統一基準を満たすための適切な事項が定められていること

監査目標	監査手続	実施時期	実施担当者
府省庁対策基準の統一基準群への準拠性※	情報セキュリティポリシーを閲覧等することにより、統一基準の遵守事項に準拠していることを確かめる。	・・・	・・・

※必要に応じて細分化してもよい。

（イ）実施手順が府省庁対策基準に準拠していること

監査目標	監査手続	実施時期	実施担当者
実施手順の府省庁対策基準への準拠性※	実施手順を閲覧等することにより、府省庁対策基準に準拠していることを確かめる。		

※必要に応じて細分化してもよい。

（ウ）実際の運用が府省庁対策基準及び実施手順に準拠していること並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当であること

監査目標	監査手続	実施時期	実施担当者
課室情報セキュリティ責任者の設置	体制図等を閲覧等することにより、課室情報セキュリティ責任者が選任されていることを確かめる。	・・・	・・・
CSIRT の体制	CSIRT の体制図や規程等を閲覧等することにより、CSIRT の体制が適切に構築されていることを確かめる。		

●監査の進捗管理手段

１．定期報告の実施

２．・・・

4.3. 個別監査実施計画の通知

監査責任者は、監査を円滑に実施するために、個別監査実施計画のうち、監査項目に対する評価手続に関連する次の内容について、被監査部門に事前に通知することが望ましい。

(1) 監査対象
(2) 監査の実施時期
(3) 当該被監査部門を担当する監査実施者の氏名

通知に際しては、監査の有効性を損なわないよう配慮する。例えば、詳細な監査項目や監査手続を通知した場合、当該監査項目や監査手続に対する対策を講じられるなどによって、監査の有効性を阻害してしまうことがある。

4.4. 監査実施計画と個別監査実施計画の統合について

年度監査実施計画を策定した後、個別監査実施計画を策定することが望ましいが、年度監査実施計画と個別監査実施計画とは相互に密接に関係しているため、両者を同時に作成する場合には、一つの監査実施計画としてまとめてもよい。

5. 監査の実施

5.1. 監査の実施の指示

最高情報セキュリティ責任者は、年度監査実施計画に従って、監査責任者に対して、監査の実施を指示する。

5.2. 年度監査実施計画及び個別監査実施計画の修正

最高情報セキュリティ責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、監査責任者に対して、年度監査実施計画で計画された事案以外の監査の実施を指示する。監査責任者は年度監査実施計画及び個別監査実施計画を修正し、実施する。

（解説）

- **5.2.「情報セキュリティの状況の変化」について**

  情報セキュリティの状況の変化の例として、次のような場合がある。

  - 新しい情報システムが運用開始されたとき
  - 新たに他の情報システム又はネットワーク等と接続したとき
  - 府省庁内における大きな人事異動や組織改編があったとき
  - 府省庁内外を問わず重大なセキュリティ侵害又はインシデントの発生があったとき
  - 我が国がサイバー攻撃の標的となる蓋然性の高いイベントの発生又は決定があったとき
  - 府省庁対策基準等が改定又は追加されたとき
  - 府省庁に影響が及ぶ情報セキュリティに関連する法令の制定又は重要な改定があったとき
  - 監査項目に対する評価手続の過程で入手した監査証拠に基づくリスクの暫定的な評価の重要な変更があったとき

5.3. 監査の実施における留意事項

(1) 監査実施者は、監査手続に基づいて、十分かつ適切な監査証拠を入手し評価する。

(2) 監査実施者は、監査手続を実施した際に十分かつ適切な監査証拠が入手できないと判断した場合には、監査手続を変更又は追加して、被監査部門への質問、別途文書の閲覧、実際に行っている作業の観察、自らが行う点検等により、必要な監査証拠を入手する。

(3)　自己点検結果の活用

監査実施者は、対策の実施状況を効率的に確認するために、必要に応じて自己点検結果を活用する。

また、府省庁において、自己点検結果の監査票等を利用して、自己点検結果に基づく担当者への質問、記録文書の閲覧及び機器の設定状況の点検等の方法により、運用の準拠性を確認している場合には、その結果を活用する。

【例】自己点検結果の監査票の活用例

平成27年度

情報セキュリティ責任者　監査票

記入年月日		所属		氏名	

監査実施年月日		監査実施者	

1　管理体制　　↓該当する箇所に○を記載　　確認方法の凡例: ◎は実施が必須、○は◎の実施が難しい場合代替手段として実施、△は実施が望ましい

平成27年度自己点検票の参考雛形（①-D　自己点検票（情報セキュリティ責任者）の参考雛形）より					監査票(監査手順)											確認結果		
項目ID	府省庁対策基準	点検事項	回答	回答例	①確認方法				確認対象		④確認ポイント					○×	コメント	入手資料No.
					質問	閲覧	観察	点検	②対象者	③対象物								
情セ1.1	2.1.1(4)d	所管する情報システムごとに情報セキュリティ対策に関する事務の責任者として、情報システムセキュリティ責任者を置いていますか。		① 置いている	○	◎			情報セキュリティ責任者	・体制図等	・回答が①又は②の場合、体制図等の文書を入手して確認する。文書がない場合は、組織・体制等について質問し、実際に整備しているかを確認する。 ・回答が②又は③の場合、情報システムセキュリティ責任者を置いていない理由を質問する。							
				② 一部置いていない														
				③ 置いていない														
				④ 所管する情報システムがないため置く必要がなかった														
情セ1.2	2.1.1(4)b	所管する組織が管理する区域それぞれにおいて、施設及び環境に係る対策を推進する責任者として、区域情報セキュリティ責任者を置いていますか。 ※ 区域情報セキュリティ責任者はその役割の性質上、施設の管理者が兼任することが想定される。定める単位としては、例えば以下が考えられる。 （ア）単一の課室が利用する執務室及び会議室を管理する場合は、課室情報セキュリティ責任者。 （イ）情報システムが設置された部屋（サーバ室等）を管理する場合は、情報システムセキュリティ責任者。 （ウ）ロビー、廊下等を管理する場合は、庁舎等の管理に関する部門の責任者。		① 置いている	○	◎			情報セキュリティ責任者	・体制図等	・回答が①又は②の場合、要管理対策区域の対策の基準や体制図等の文書を閲覧し、施設及び環境に係る対策を行う単位ごとに区域を定めているか、取り扱う情報や設置される情報システムの特性から外部からの侵入があった場合の被害の大きさなどを考慮して区域を定めているかなどを確認する。また、施設及び環境に係る対策を行う単位ごとの区域に情報セキュリティ責任者を置いているか全体制図等を閲覧し確認する（文書がない場合は、組織・体制等について質問し、実際に整備しているかを質問する）。 ・回答が②又は③の場合、施設及び環境に係る対策を行う単位ごとの区域に区域情報セキュリティ責任者を置いていない理由を質問する。							
				② 一部置いていない														
				③ 置いていない														
				④ 所管する区域がないため置く必要がなかった														

2　例外措置　　↓該当する箇所に○を記載

平成27年度自己点検票の参考雛形（①-D　自己点検票（情報セキュリティ責任者）の参考雛形）より					監査票(監査手順)											確認結果		
項目ID	府省庁対策基準	点検事項	回答	回答例	①確認方法				確認対象		④確認ポイント					○×	コメント	入手資料No.
					質問	閲覧	観察	点検	②対象者	③対象物								
情セ2.1	2.2.2(2)b	例外措置の申請を受けた場合には、定められた手続きに従って審査を行い、許可の可否を決定していますか。		① 手続きに従い決定している	◎	◎			情報セキュリティ責任者	・例外措置申請に関する規程、手順書 ・適用審査記録等	・予め例外措置申請手続きに関する規程や手順書を確認し、あれば把握しておく。 ・回答が①又は②の場合、申請・審査の記録（メールを含む）を閲覧し、規程や手順書どおりに審査・決定・エスカレーション（最高情報セキュリティ責任者への報告）等を行っているか確認する。また、例外措置によって生じる リスクに対する受容又は対策実施の判断、例外措置の設定期間等の申請内容が適切なものであるか確認する。 ・回答が②又は③の場合、手続きに従っていない理由を質問し、申請手順に不備がないかなどを確認する。							
				② 手続きに従っていない場合がある														
				③ 手続きに従っていない														
				④ 例外措置の申請を受けることがなかった														
情セ2.2	2.2.2(2)c	例外措置の申請を受けた場合には、その申請状況を台帳に記録していますか。		① 記録している	◎	◎			情報セキュリティ責任者	・例外措置申請に関する規程、手順 ・記録台帳等	・予め例外措置申請手続きに関する規程や手順書を確認し、あれば把握しておく。 ・回答が①又は②の場合、申請・審査の記録（メールを含む）を閲覧により確認する。また、申請に対する承認者の承認の可否、日付等を確認し、合わせて承認の理由が適切か確認する。 ・回答が②又は③の場合、記録していない理由を質問する。							
				② 一部の情報について記録していない														
				③ 記録していない														
				④ 例外措置の申請を受けることがなかった														

3　情報セキュリティインシデントへの対処　　↓該当する箇所に○を記載

※情セ3.1については、情報セキュリティ責任者に対する規定がポリシー等に設けられている場合は本点検事項を使用するとよい。（統一基準の遵守事項の名宛人は情報システムセキュリティ責任者）

平成27年度自己点検票の参考雛形（①-D　自己点検票（情報セキュリティ責任者）の参考雛形）より					監査票(監査手順)											確認結果		
項目ID	府省庁対策基準	点検事項	回答	回答例	①確認方法				確認対象		④確認ポイント					○×	コメント	入手資料No.
					質問	閲覧	観察	点検	②対象者	③対象物								
情セ3.1	2.2.4(2)d	所管する部局において情報セキュリティインシデント（※）を認知した場合（行政事務従事者によって認知され、報告・連絡を受けたものを含む。）には、府省庁で定められた対処手順又はCSIRTの指示若しくは勧告に従って対処することを認識していますか。 ※「情報セキュリティインシデント」とは、例えば、要機密情報（機密性2情報、機密性3情報）が含まれるメールの誤送信、要機密情報が格納されたUSBメモリの紛失、コンピュータウイルス等の不正プログラムへの感染等（おそれがある場合を含む。）が挙げられる。		① 対処することを認識している	◎	○			情報セキュリティ責任者	・体制図 ・情報セキュリティインシデントの対処手順	・予め情報セキュリティインシデントに備えた体制及び情報セキュリティインシデント発生時の対処手順について確認し、あれば把握しておく。 ・回答が①の場合には、以下について質問し、定められた対処手順に合っていることを確認する。 －情報セキュリティインシデントを認知した際の対処手順 －CSIRTからの指示若しくは勧告への対処手順 ・回答が③の場合には、予め把握した体制や対処手順の適用の要否について、質問により確認する。							
				② 対処することを認識していない														
				③ 対処手順又はCSIRTが整備されていない														
情セ3.2	2.2.4(3)a	情報セキュリティインシデントが発生し、CSIRTの指示を受けた場合には、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として、最高情報セキュリティ責任者に報告していますか。		① 報告書として報告している	◎	◎			本人	・再発防止策等の報告書 ・情報セキュリティインシデント一覧 ・CISOへの報告に関する記録等	・予め情報セキュリティインシデント発生時の対処手順の有無について確認し、あれば把握しておく。 ・回答が①の場合、再発防止策等を含む報告書と情報セキュリティインシデントの記録を突合して確認する。 ・回答が①又は②の場合、再発防止策等を含む報告書を閲覧し、以下について確認する。 －原因の究明がなされていること －再発防止策を策定していること －CISOへの報告履歴が分かる記録類の確認 ・回答が②又は③の場合、報告していない理由を質問する。							
				② 報告書として報告していない場合がある														
				③ 報告書として報告していない														
				④ CSIRTの指示を受けなかった（情報セキュリティインシデントが発生しなかった場合も含む）														

(4)　監査証拠の証拠力の評価

入手した資料は、その入手元及び入手時の状況等を勘案して、監査証拠として採用するかについて、それらが有する信用性及び証明力の程度を慎重に判断する。

(5)　被監査部門から提出された資料、監査実施者自らが入手した資料、自らが行ったテスト結果等を総合的に勘案して、相互に矛盾があるかないか、また、異常性を示す兆候があるかを評価する。

（解説）

- **5.3. (3)「自己点検結果を活用する」について**

統一基準群では、行政事務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するため、自己点検を実施することとしている。自己点検は、本質的には監査とその目的を一にしている。そのため、自己点検を監査において利用することも考えられるが、両者の実施形態や個別具体的な目的の違いから、監査項目に対する十分性と適合性を評価することなく、その結果を監査証拠として直ちに採用することはできない。例えば、自己点検の結果は行政事務従事者が各々回答したものであるため、監査証拠としての証明力は一般的に極めて弱い。

このようなことから、監査人は、自己点検の結果を監査証拠に採用する場合、次の手続を含む評価を実施する。

・ 自己点検票に含まれる点検項目が監査項目の範囲を満たしていること
・ 自己点検票に含まれる点検項目が監査項目で確かめたい事項の証拠となること
・ 自己点検の回答が適切であることを試査によって確かめること

- **5.3. (4)「入手した資料は、その入手元及び入手時の状況等を勘案して」について**

入手資料については、例えば以下の情報がある。

・ 監査対象である部局が作成した情報

監査人は、当該情報が監査項目に照らして、十分に信頼性を有しているかどうかを評価する。

・ 自己点検の結果

監査人は、自己点検の結果が監査項目に対して十分性と適合性を有していることを確かめる手続を実施する。

・ 外部委託先の業務により作成された情報

監査人は、監査証拠として利用する情報が府省庁の利用する外部委託先の業務により作成されている場合には、監査項目に照らして、当該外部委託先の業務の重要性を考慮し、必要な範囲で次の手続を実施する。

（次頁に続く）

✓　外部委託先の適性、能力及び客観性を評価すること
✓　外部委託先の業務を理解すること
✓　外部委託先の業務について、監査証拠としての適切性を評価すること

・インターネット上で取得できる公開情報
　監査人は、当該情報の信憑性を確かめる手続を実施する。
・内閣サイバーセキュリティセンターから提供される情報
　監査人は、当該情報の内容を吟味する手続を実施する。
・過年度の監査において入手した監査証拠
　監査人は、当該監査証拠が依然として監査項目に適合することを確かめる監査手続を実施する。

5.4.　実施結果の評価

(1)　準拠性に関する評価

(a)　府省庁対策基準等の整備状況の準拠性に関する評価

監査実施者は、統一基準、府省庁対策基準及び実施手順の間に矛盾、相違点、不足があれば、発見事項とその原因・問題点・重要性を検討し、指摘事項とする。

(b)　府省庁対策基準等の運用状況の準拠性に関する評価

監査実施者は、府省庁対策基準及び実施手順に基づいた運用について遵守事項違反があれば、発見事項とその原因・問題点・重要性を検討し、指摘事項とする。

(c) 監査実施者は、準拠性に関する違反について、重大な違反と軽微な違反に区分する。

(2)　情報セキュリティ対策の内容の妥当性に関する評価

(a) 監査実施者は、想定するリスクと現状の対策後のリスクを比較して、その対策後のリスクが小さければ対策が妥当であるものと判断する。ただし、対策後のリスクが組織の許容範囲を超えていれば、発見事項とその原因・問題点・重要性を検討し、指摘事項とする。

(b) 監査実施者は、府省庁対策基準等の整備状況及び運用状況の準拠性が適切であっても、府省庁対策基準等の改定が望まれる事象があれば、発見事項とその原因・問題点・重要性を検討し、指摘事項とする。

(3)　監査実施者の改善提案の位置づけ

(a) 監査実施者は、指摘事項を報告するに当たり、対策についての改善提案を行うことを役割とし、実現可能性についての検討は被監査部門の情報セキュリティ責任者が行う。

(b) 被監査部門の情報セキュリティ責任者は、改善提案による対策の実現可能性について監査報告書に基づく最高情報セキュリティ責任者からの指示により検討する。

(4)　指摘事項の取扱い

指摘事項とは、監査の過程で発見したマネジメントシステム又は情報セキュリティ対策の不備をいう。監査人は、指摘事項を監査報告に含める前に、次の手続を実施する。

(a)　当該発見事項に関する事実関係について、事実誤認等がないかを含め、監査対象の担当者と合意する。

(b)　事実関係が確かめられた発見事項は、監査報告書を通じてその重要性を伝達するため、原因と問題点を検討し、重要性を評価する。

（解説）

- **5.4. (1) (b)「運用について遵守事項違反があれば」について**

  監査実施者は、運用状況を確かめるために、母集団からサンプリングした監査証拠により判断する。

- **5.4. (4) (a)「当該発見事項に関する事実関係について、事実誤認等がないかを含め、監査対象の担当者と合意する」について**

  監査人は、発見事項について事実誤認を避けるために、事実確認の手続を書面又は対面にて実施することが望ましい。監査人は、書面にて実施した場合は当該書面を監査調書化することにより、対面にて実施した場合はその記録を作成することにより、事実確認の過程を監査調書に記録する。

- **5.4. (4) (b)「重要性を評価する」について**

  監査人は、発見事項の重要性の評価基準をあらかじめ設定し、当該基準に基づいて発見事項を評価する。評価基準には、次のようなものが考えられる。

区分	内容
重大な指摘事項	単独で又は他の発見事項と組み合わさることにより、重大なリスクの発生を引き起こす可能性がある指摘事項
軽微な指摘事項	上記以外の指摘事項

5.5.　監査手続の実施結果等の文書化

監査実施者は、監査対象等ごとに、個別監査実施計画に基づいて実施した監査手続の結果、入手した監査証拠等を監査調書として整理し、個別監査実施計画に基づいて実施した監査業務により発見された指摘事項及び改善提案を実施結果としてまとめ、監査責任者に報告する。

(1) 監査実施者は、参照符号等を整備して、監査の結論に至った経過が秩序整然と分かるように監査調書を作成する。
(2) 監査実施者は、被監査部門から提出された資料や組織の外部の第三者から入手した資料を監査調書に含める。
(3) 監査責任者は、監査実施期間中の監査調書の保管場所や保管責任者を決定し、情報漏えいや紛失等を防止する。
(4) 監査実施者は、個別監査実施計画に基づく実施結果として、次の事項を記載する。
    (a) 表題（監査対象又は監査業務等を示す名称）
    (b) 監査実施者の氏名・署名
    (c) 実施期間
    (d) 被監査部門及び責任者
    (e) 発見事項、原因・問題点・重要性、改善提案
    (f) 確認した遵守項目（必要な場合）
    (g) 確認した対策の内容
    (h) サンプルの件数及び抽出方法（必要な場合）
    (i) 評価方法及び評価結果
    (j) 監査証拠としての形態（文書か口頭か）
    (k) 監査証拠の入手元（被監査部門から提出された資料か、監査実施者が直接入手した資料か、第三者から入手した資料か）
    (l) 関連資料番号（チェックした項目をマーキングし、資料として添付する。）

【例】個別監査実施計画に基づく実施結果のひな形

（監査実施者）
氏　名

府省庁対策基準及び実施手順の監査の実施結果

１．監査対象：府省庁対策基準及び実施手順

２．実施期間：××年××月××日から○○年○○月○○日まで

３．被監査部門及び責任者：・・・・・・

４．発見事項、原因・問題点・重要性、改善提案

(1) 重大な指摘事項

	指摘事項		改善提案
	発見事項	原因・問題点・重要性	
①○○に関する違反			
②○○に関する違反			

(2) 軽微な指摘事項

	指摘事項		改善提案
	発見事項	原因・問題点・重要性	
③○○に関する違反			
④○○に関する違反			

５．実施内容：別紙（実施結果の詳細）のとおり

別紙

【実施結果の詳細】

監査目標	監査手続	対策内容	評価方法	評価結果	監査証拠		関連資料番号
					形態	入手元	
課室情報セキュリティ責任者の設置	体制図等を閲覧等することにより、課室情報セキュリティ責任者が選任されていることを確かめる。		対策基準に明記されていることの確認	適切に選任されていた。	文書	○○課	001
CSIRT の体制	CSIRT の体制図や規程等を閲覧等することにより、CSIRT の体制が適切に構築されていることを確かめる。		対策基準に明記されていることの確認	以下の発見事項があった。 「○○に関する事項が○○規程に含まれていなかった。」	文書	○○課	002

6.　監査報告

6.1.監査報告書の作成と提出

監査責任者は、監査業務の実施結果に基づき、監査報告書を作成し、最高情報セキュリティ責任者に報告する。監査責任者は、監査報告書において、改善提案を行い、情報セキュリティ対策の改善につなげる。

(1) 監査責任者は、監査報告書の読み手が最高情報セキュリティ責任者であることを意識し、最高情報セキュリティ責任者が指摘事項や改善提案の重要性や緊急性等を理解し、情報セキュリティ責任者等への指示すべき内容が明瞭になるように記述する。
(2) 監査責任者は、改善提案を述べるに際して、府省庁対策基準やその他の基準及び当該契約書等の監査の基準に照らして発見された課題及び問題点について指摘し、改善提案を行う。また、保証を付与するかのような誤解を与える表現を用いないようにする。
(3) 監査責任者は、監査報告書の正本を最高情報セキュリティ責任者に提出、写を自らが保管する。

（解説）

- **6.1 (1)「監査報告書を作成」について**

  監査報告とは、監査責任者が、監査を通じて識別された情報セキュリティ対策の状況等について、最高情報セキュリティ責任者に伝達することをいう。監査報告に当たっては、監査報告書を作成する。監査報告書は、監査の結果に関する内容が必要十分で正確なだけではなく、監査人が必要と判断するその他の事項についても明瞭かつ簡潔に記載されている必要がある。

  【監査報告書記載上の配慮事項】

  ・ 要約と詳細を分ける
  ・ 指摘事項等の対象となる部門や責任者をわかりやすく記述
  ・ 準拠性の違反等の事実と妥当性の改善提案については、分けて記述
  ・ 違反の事実については、重要性により区分けをして記述

6.2. 監査報告書の記載事項

監査報告書は、当該報告書に記載された指摘事項に対して適切な改善提案を行うことにより、情報セキュリティ対策の水準を向上させることを目的としている。この目的を達成するため、監査報告書には、以下の項目を記載する。

(1) 報告書の名称

監査報告書には、他の監査報告書との区別を容易にするため、実施年度、府省庁名を含め、監査に係る報告書であることを示す表題を付す。

(2) 報告書の日付

報告書に付す日付は、個別監査実施計画において設定された全ての監査項目に対して十分かつ適切な監査証拠を入手した日以降にする。十分かつ適切な監査証拠には、監査対象の事実確認に対する回答を含むことに留意する。

(3) 報告書の宛名

監査報告は最高情報セキュリティ責任者に向けて実施され、最高情報セキュリティ責任者はその内容に基づいて必要な措置を講じる。したがって、監査報告書の宛名は、当該府省庁の最高情報セキュリティ責任者とすることが望ましい。

(4) 監査責任者の署名又は記名押印

監査結果の報告に係る事務は、監査責任者が統括することとされている。したがって、監査報告書には、監査責任者の署名又は記名押印を付すことが望ましい。

(5) 監査実施期間

監査項目に対する評価手続を実施した期間を記載する。

(6) 監査対象範囲

監査報告書が報告する対象を明らかにするため、監査対象を記載する。監査対象には、部局名や情報システム、行政事務の名称等を含めることが考えられる。

(7) 情報セキュリティに関する管理基準等

(8) 監査の結果

監査の結果には、監査対象ごとに指摘事項等を要約する。なお、監査の結果には、指摘事項等だけでなく、組織として推奨すべき優れた取組等がある場合には、その優れた取組等について含めることが望ましい。

(9) 指摘事項及び改善提案の総括

監査項目に対する評価手続における発見事項のうち、事実確認が完了しているものについて、当該発見事項の原因・問題点・重要性及び当該発見事項に係る改善提案とあわせて記載する。記載に当たっては、発見事項、原因・問題点・重要性及び改善提案を一覧表にするといった方法が考えられる。

(10) 監査人の独立性に関する事項

全ての監査担当者が監査対象範囲の組織等から独立していることを記載する。例えば、情報システムを監査する場合には監査担当者が当該情報システムの構築や運用に関与していなかったこと、情報の取り扱われ方に関する監査を行う場合には監査担当者が当該情報の取扱いに関与していなかったことを示すことが望ましい。

ただし、独立性についての詳細な記述までは必要なく、「本職及び監査実施者は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有している。」という記載でもよい。

(11) 監査報告書の取扱い（利用及び利用者の制限事項等）

(12) 添付資料（監査対象ごとの監査報告書）

【例】監査報告書のひな形

○○年○○月○○日

最高情報セキュリティ責任者　殿

（情報セキュリティ監査責任者）
署　　名

○○年度　××××省情報セキュリティ監査報告書

平成○○年度情報セキュリティ監査実施計画に基づき、情報セキュリティの状況について監査を実施したところ、以下のとおり報告する。

１．監査の目的

府省庁対策基準の統一基準群への準拠性、実施手順の府省庁対策基準への準拠性、実際の運用の実施手順への準拠性並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当性を評価し、指摘事項に関して改善提案を行うこと。

２．監査実施期間：××年××月××日から○○年○○月○○日まで

（次頁に続く）

３．監査対象範囲

(1)重点監査対象

監査対象	監査項目	監査目標
府省庁対策基準及び実施手順	（ア）府省庁対策基準に統一基準を満たすための適切な事項が定められていること （イ）実施手順が府省庁対策基準に準拠していること （ウ）実際の運用が府省庁対策基準及び実施手順に準拠していること並びに府省庁の特性に照らした府省庁対策基準及び実施手順の妥当であること	・府省庁対策基準の統一基準群への準拠性 ・実施手順の府省庁対策基準への準拠性 ・課室情報セキュリティ責任者の設置 ・CSIRT の体制　等
情報セキュリティ管理体制	情報システム対策の導入・計画、運用、点検見直しの整備・運用状況	情報セキュリティ管理体制が整備され、有効に機能していること等
○○局の情報格付業務	情報の取扱いに係る整備・運用状況	○○局の情報の機密性が確保されていること等
府省庁内 LAN	府省庁内 LAN の運用状況	不正アクセスの防止対策が有効に機能していること等

(2)その他の監査対象

インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

４．情報セキュリティに関する管理基準等：府省庁対策基準

５．監査の結果

６．指摘事項及び改善提案の総括

７．添付資料

(1) 府省庁対策基準及び実施手順の監査に係る情報セキュリティ監査の報告

(2) 情報セキュリティ管理体制の構築の監査の報告

・・・・・

なお、本職及び監査実施者は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり報告するものである。

また、本報告書の利用は、府省庁における最高情報セキュリティ責任者及び情報セキュリティ責任者に限る。

添付資料１

○○年○○月○○日

府省庁対策基準及び実施手順の監査の実施結果報告

平成○○年度情報セキュリティ管理体制の構築に関する個別監査実施計画に基づき、情報セキュリティ管理体制の構築状況を対象として監査を実施したので、以下のとおり報告する。

１．実施期間：××年××月××日から○○年○○月○○日まで

２．被監査部門及び責任者：・・・・・・

３．指摘事項及び改善提案の総括

(1) 重大な指摘事項

	指摘事項		改善提案
	発見事項	原因・問題点・重要性	
①○○に関する違反			
②○○に関する違反			

(2) 軽微な指摘事項

	指摘事項		改善提案
	発見事項	原因・問題点・重要性	
③○○に関する違反			
④○○に関する違反			

7. 監査結果に対する対処

7.1. 情報セキュリティ責任者への改善指示

(1) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を情報セキュリティ責任者に指示する。（遵守事項 2.3.2 (3) (a)）

(2) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の情報セキュリティ責任者に対しても、同種の課題又は問題点の有無を確認するように指示する。（基本対策事項 2.3.2 (3)-1）

(3) 最高情報セキュリティ責任者は、(1)(2)に掲げるもののほか必要な事項について、該当する情報セキュリティ責任者に対処を指示する。

7.2. 改善計画の作成及び報告

(1) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、必要な措置を行った上で改善計画を策定し、措置結果及び改善結果を最高情報セキュリティ責任者に報告する。（遵守事項 2.3.2 (3) (b)）

(2) 情報セキュリティ責任者は、監査報告書において指摘された課題又は問題点の改善が困難であることについて正当な理由がある場合には、その影響を低減させるための補完的な措置を示した上で、達成することが可能な改善計画を最高情報セキュリティ責任者へ報告する。（遵守事項 2.3.2 (3) (b)の解説）

(3) 情報セキュリティ責任者は、監査報告書において指摘された課題又は問題点の改善が教育・訓練により解決すべき課題であると判断した場合には、統括情報セキュリティ責任者と相談の上、教育計画及び資料に反映する。

7.3. 情報セキュリティ関係規程の見直しの指示

(1) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、府省庁対策基準について必要な見直しを行う。（遵守事項 2.4.1 (1) (a)）

(2) 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。（遵守事項 2.4.1 (1) (b)）

8. 監査調書の管理と保存

8.1. 監査調書の管理と保存

監査の全ての過程が終了した後の監査調書は、監査人が適切な監査を実施したことに関する説明責任を果たさなければならない場合において、その根拠となるものである。また、監査調書には、府省庁における情報セキュリティに係る対策の実施状況や監査項目に対する評価の結果等、府省庁の情報セキュリティ対策に関する重要な情報を含んでいる。そのため、監査調書は最終的に紙媒体又は電子媒体等に記録された監査ファイルとしてとりまとめ、適切に管理し保存する。

(1) 監査調書に係る情報の取扱い

(a) 機密性に係る取扱い

監査調書に含まれる情報には、その漏えいによってサイバー攻撃者に利するものが含まれる可能性が高いことを考慮して取り扱う。

(b) 完全性に係る取扱い

監査調書は、その改ざんや誤びゅう、破損によって、監査人が適切な監査を実施したことの根拠となる証拠能力を失うことを考慮して取り扱う。

(c) 可用性に係る取扱い

監査調書は、その滅失、紛失又は必要な状況において閲覧できないことにより、監査人が適切な監査を実施したことの説明責任を果たすことができないことを考慮して取り扱う。

(2) 監査ファイルの整理

監査人は、監査項目に対する評価の結果を導出した過程が理路整然となるように監査ファイルを整理する。これには、監査調書に適当な参照番号を付して監査手続と監査証拠を紐付けるなど、監査調書間の関係性を明らかにすること、監査調書の順序を揃えること、監査調書の分類をすること、差し替えられた修正前の監査調書を破棄すること等が含まれる。

(3) 監査ファイルの最終的な整理

監査人は、当該監査が実施された年度が終了するまでに、監査業務に関連する全ての監査調書を監査ファイルとしてとりまとめ、監査ファイルにおける監査調書を整理する。

(4) 監査ファイルの最終的な整理が完了した後の監査調書の追加又は修正

監査ファイルの最終的な整理が完了した後に、既存の監査調書の修正又は新たな監査調書の追加が必要になった場合には、その修正や追加の内容に関わらず、監査人は次の項目を監査調書に記録する。

(a)　修正又は追加が必要となった具体的理由
(b)　修正又は追加を実施した者及び実施日
　　修正又は追加された監査調書を閲覧した者及び実施日

(5) 監査ファイルの保存

監査責任者は、監査ファイルの保存場所や保存責任者、保存期間を決定し、その情報の取扱いに従って適切に保存する。

（解説）

- **8.1. (1)「監査調書に係る情報の取扱い」について**

監査ファイルとして集約された監査調書に含まれる情報は、相互に関連しあうとともに、監査人の評価や判断が付加されることにより、単体で取り扱われた場合に比べて機密性が高まると考えられる。このため、最終的な整理が完了した監査ファイルについては、監査ファイルに含まれる個別の監査証拠の機密性区分の如何によらず、監査ファイル総体としての機密性を定めなければならないことに留意する。

一方、最終的な整理が完了する前の監査調書については、監査業務の利便性に考慮して、例えば次の例のように上記と異なる取扱いとすることも考えられる。

・ 監査人が作成した監査調書は、機密性２として取り扱う。
・ 部局から提供された監査証拠を監査調書とした場合は、当該部局によって付された機密性区分に従って取り扱う。

- **8.1. (2)「監査項目に対する評価の結果を導出した過程が理路整然となる」について**

監査調書に記載される内容はその監査調書の性質に依るが、次の項目は基礎的な情報として、基本的に記載すべきものである。

・ 参照番号

調書番号とも呼ばれ、調書を一意に識別するため、原則として全ての監査調書に対して記載する。ただし、監査調書が複数ページから構成される場合において、2 ページ目以降への記載は必要な場合のみでも構わない。

参照番号は、監査ファイルにおける監査調書の閲覧性を確保するため、原則として監査調書の右上に記載する。

・ 監査調書の作成目的

監査調書の内容を端的に表す情報を記載する。例えば、監査項目に対する評価手続に対する監査調書であれば当該監査項目、入手した証跡に手続を加えて監査調書とする場合であれば当該証跡の内容等を記載する。

（次頁に続く）

・ 監査手続を実施した者及び完了日

特に監査手続においてなんらかの結果を記載した調書には必ず記載する。

・ 査閲者、査閲日及び査閲対象の手続

査閲の範囲が明示的又は暗黙に把握できる場合には、必ずしも全ての監査調書に記録する必要はない。

・ 情報の入手源

監査人が作成した監査調書と監査対象となる部局から入手した証憑を区別するために、後者には入手源を朱記する。ただし、府省庁ポリシーのように、入手源が自明な場合又は明記することが明らかに不要な場合は、その限りではない。

・ チェックマークの凡例

当該監査調書で実施した監査手続においてチェックマークを使用した場合には、監査手続の内容を明確化するために、当該チェックマークの定義を簡潔に記載する。

- **8.1. (2) 「監査ファイルを整理する」について**

監査における監査調書には、情報セキュリティリスクの動向や府省庁ポリシー等の基礎となる監査証跡、個別監査実施計画、監査項目に対する評価手続の内容及びその結果並びに関連する証跡、発見事項、監査報告等、多岐にわたるものが含まれる。また、複数の監査手続の結果を集約して監査項目に対する評価の結果を導出するなど、監査調書間の参照が発生する。このため、監査人は、監査調書を体系的に整理するとともに、個々の監査調書には参照番号と呼ばれる識別子を付与し、一意に識別できるようにする。

監査調書は、個別監査実施計画の策定から監査報告書の提出に至る一連の監査業務ごとに監査ファイルとして取りまとめるものとする。監査ファイルは、少なくとも以下の区分を設けて整理する。それぞれの区分に含まれる監査調書に付す参照番号は、監査ファイルの構成に調和するよう体系化するため、予め区分ごとに接頭詞を定めて統一することが望ましい。

参照番号	文書名
1	府省庁ポリシー等、監査ファイル全体から参照する可能性のある基礎的な証跡
2	個別監査実施計画
3	監査項目に対する評価手続の内容及び結果
4	指摘事項の検討と管理
5	監査報告

（次頁に続く）

- **8.1. (2)「適当な参照番号を付して監査手続と監査証拠を紐付ける」について**

  参照番号の記法は、監査ファイルを構成する区分を示す接頭詞の後に数桁の数字を連結する方法等が考えられる。参照番号の体系は、数字の桁ごとに一定の意味を持たせるなど、査閲者等の利便性に資するため、当該体系をもって監査ファイル全体が体系化されるよう定めることが望ましい。

- **8.1. (2)「監査調書間の関係性」について**

  監査調書の多くは、他の監査調書に記載された情報を参照、集約し、別の監査手続を実施することで、全体として新たな結果を導くものである。したがって、ある監査調書から監査手続の結果や途中経過、発見事項等、監査人が手続の過程で導出した何らかの事項を参照する場合には、明らかに不要な場合を除き、監査調書間で参照されていることを明記する。参照されていることの記載方法は、次の要件を充足するように予め定めることが望ましい。

  ・ 参照元調書にあっては、参照先調書の調書番号を記載し、当該監査調書を参照していることが判別できること
  ・ 参照先調書にあっては、参照元調書の調書番号を記載し、当該監査調書から参照されていることが判別できること

- **8.1. (4)「監査ファイルの最終的な整理が完了した後の監査調書の追加又は修正」について**

  監査調書は監査報告の根拠となるものであるから、通常は、監査報告書の確定後に新たな監査手続を実施したり、新たな結果を導いたりすることは想定されない。このため、監査報告書の確定後に行う監査ファイルの最終的な整理には、次のような事務的な作業が中心となる。

  ・ 差し替えられた修正前の証憑等、不要な監査調書を破棄する作業
  ・ 監査調書の順序を揃え、適当な参照番号を付すこと
  ・ 監査調書間の参照関係を適切に記載すること
  ・ 証憑に対してすでに実施した監査手続の内容と結果を記入すること

  しかし、監査ファイルの最終的な整理の過程において、指摘事項となりうる不備が存在する可能性を識別した時は、監査人は、その状況に応じて次の対応を検討する。

  ・ 関連する部局に対する翌年度の監査の実施が間近に予定されている場合は、当該不備が存在する可能性に係る監査調書を作成し、翌年度の個別監査実施計画に反映する。
  ・ 上記以外の場合は、関連する部局の担当者と合意の上、個別監査実施計画の修正、追加の監査手続の実施及び必要に応じて監査報告書の修正を実施する。

以上