DM2-07-051

# 情報セキュリティ監査実施手順

# 策定手引書

2006 年 3 月

内閣官房情報セキュリティセンター

## 本策定手引書の目的

本策定手引書は、府省庁における情報セキュリティ監査（以下「監査」という。）の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、「政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版))」(NISD-K303-052)（以下「政府機関統一基準」という。）に準拠する省庁基準と、省庁基準を具体化する一連の実施手順群を整備することが求められている。

「情報セキュリティ監査実施手順」は、これら実施手順のひとつとして策定し、情報セキュリティ監査責任者（以下「監査責任者」という。）等が監査等を行う場合に適用するものである。すなわち、監査責任者等がこれに従うことにより、政府機関統一基準に基づく省庁基準の関係する規定を遵守することになる。

情報セキュリティの確保のためには、政府機関統一基準に準拠して省庁基準が適切に策定され、かつ、情報セキュリティ関係規程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、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、行政事務従事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。

本策定手引書は、これらの背景の下で「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、もって政府機関統一基準及び省庁基準への準拠性、対策の妥当性等において適切な実施手順の整備に資することを目的とする。

## 実施手順に記載すべき事項

「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こと。

(1) 政府機関統一基準（NISD-K303-052）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･体制の確立（３）情報セキュリティ監査責任者の設置
- 2.2.1 情報セキュリティ対策の教育（１）行政事務従事者に対する情報セキュリティ対策教育の実施
- 2.3.2 情報セキュリティ対策の監査（１）監査計画の策定
- 2.3.2 情報セキュリティ対策の監査（２）情報セキュリティ監査の実施に関する指示
- 2.3.2 情報セキュリティ対策の監査（３）個別の監査業務における監査実施計画の策定
- 2.3.2 情報セキュリティ対策の監査（４）情報セキュリティ監査を実施する者の要件
- 2.3.2 情報セキュリティ対策の監査（５）情報セキュリティ監査の実施
- 2.3.2 情報セキュリティ対策の監査（６）情報セキュリティ監査結果に対する対応

(2) 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、情報の取扱いに係る留意事項として、以下の項目を考慮すべきである。

- 監査の省内での位置付けの明確化（省内規定の作成等）
- 監査の実効性の確保（監査チームの編成等）
- 監査実施の効率化（自己点検票の活用等）

## 本策定手引書の利用方法

### 本策定手引書構成

本策定手引書では、斜体文字以外の部分が「情報セキュリティ監査実施手順」の雛形であり、斜体文字の部分が解説である。

解説のうち【手順利用者への補足説明】という見出しを付けた部分は、この雛形を利用する行政事務従事者に対する解説であり、各府省庁で当該手順を整備する際にその中に追加してもよい箇所である。

解説のうち【手順策定者への補足説明】という見出しを付けた部分は、当該手順を整備する者に対する解説であり、手順を整備した後には削除するのが適当な箇所である。

### 雛形の手直しポイント

政府機関統一基準に基づき策定された省庁基準に準拠した「情報セキュリティ監査実施手順」を作成する手順には、大別して、新規で作成するものと既存の文書を修正するものがあるが、そのどちらの場合でも以下の事項を踏まえて作業を行う必要がある。

① 雛形中に、*【・・・】*形式で明記される設定値（責任者名、期間、期日等）については、各府省庁内の定めに合わせる。
② 雛形中に、【・・・の場合】形式で明記される記述については、想定される複数の案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

### 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、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制度（実施基準ガイドライン等)」
URL: http://www.meti.go.jp/policy/netsecurity/audit.htm

(2) 特定非営利活動法人　日本セキュリティ監査協会
「2004 年度　情報セキュリティ監査制度普及啓発活動報告」
URL: http://www.jasa.jp/about/seika.html

(3) 情報システムコントロール協会「ISACA 東京支部の活動 ～基準～」
URL:http://www.isaca.gr.jp/standard/

## 改訂履歴

| 改訂日 | 改訂理由 |
|---|---|
| 2006/03/31 | 初版 |
| | |
| | |

## 商標について

本資料に記載されている会社名、製品名は、それぞれの会社の登録商標又は商標です。

# 目次

# 1　本書の目的

情報セキュリティの確保のためには、本統一基準に準拠して省庁基準が適切に策定され、かつ、情報セキュリティ関係規程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、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、行政事務従事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必要である。

本書は、*【当省】*における監査の適切な実施のための手順を策定することを目的とする。

# 2　本書の対象者

本書は、監査責任者及び情報セキュリティ監査を実施する者（以下「監査実施者」という。）を含む*【当省】*内における監査に携わる者（以下「省内監査関係者」という。）を対象とする。

# 3　監査の概要

## 3.1　監査とは

*【当省】*における監査とは、省庁基準等の客観的基準に従い、被監査部門とは独立性を有した組織又は者が行う情報セキュリティに関する確認行為（独立的評価）をいい、*【当省】*における自己点検結果等をサンプリングし、その確認・評価を行い、確認・評価の結果を最高情報セキュリティ責任者に報告することにより省内のセキュリティレベルの向上に資するものである。

一般的に、監査には「保証型監査」と「助言型監査」があり、これらは監査対象により使い分けられることになる。*【当省】*における監査では、省庁基準及び実施手順については準拠性に対する保証型監査を行い、情報セキュリティ対策の運用については準拠性及び妥当性に対する助言型監査を行う。

*【手順策定者への補足説明：保証型監査と助言型監査の比較】*

*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利用促進等事業　実施報告書」より抜粋*

| | *保証型監査* | *助言型監査* | *コンサルティング（参考）* |
|---|---|---|---|
| *保証* | *与える* | *与えない* | |
| *意見* | *述べる* | | |
| *提言* | *しない* | *する* | |
| *客観的基準* | *存在することが前提* | | *ない* |
| *実施者の独立性* | *必須* | | *必須ではない* |
| *提言のフォローアップ* | *なし* | *あり* | *なし* |

## 3.2　基本的考え方

(1) 監査の実施は、*【当省】*省庁基準に根拠を置く。

(2) 監査の実施に係る省内規定等を作成し、監査業務及び手続に関する省内での位置付けを明確化する。

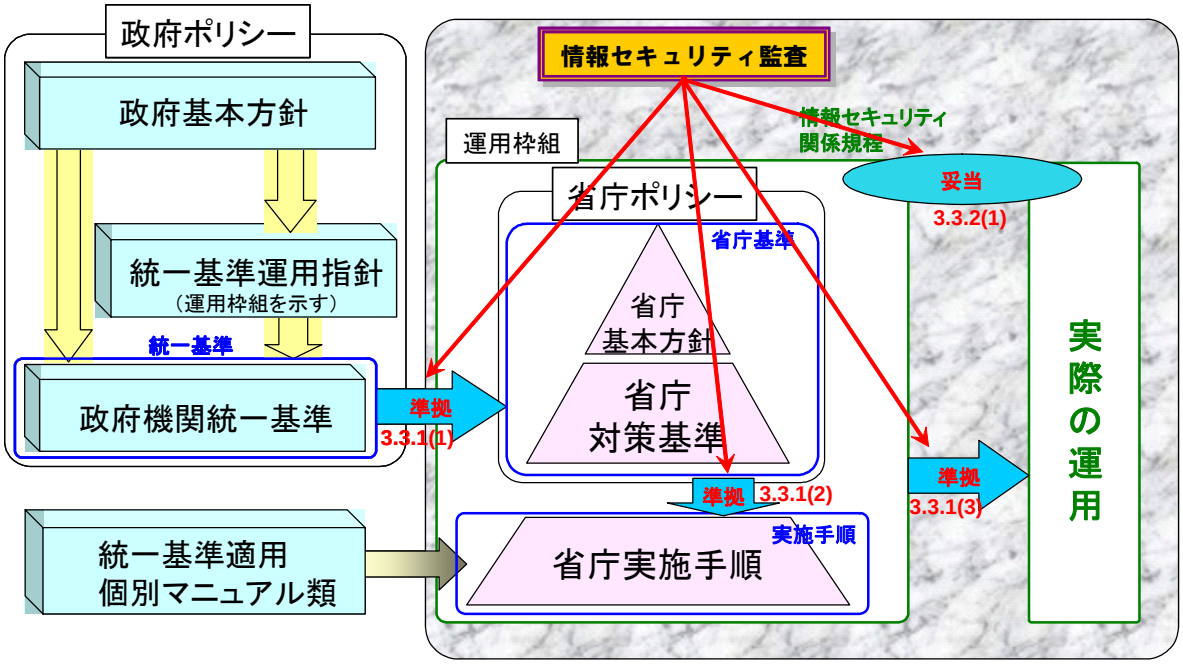
(3) 監査は、年度情報セキュリティ監査計画に基づき、最高情報セキュリティ責任者の指示により実施する。

(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。

- 専任の監査実施者の確保が困難であることを考慮し、監査業務を通常業務とは独立した業務として行うよう、監査実施者に指示する。
- 監査実施者の任命に当たっては、所属する課室長等と協議をした上で、省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。
- 監査責任者及び監査実施者で、*【当省】*内における監査チーム等の組織を編成することを検討する。
- 監査実施者には、自らが直接担当している業務やシステムの監査を実施させない。
- 監査実施者に対して、監査で知りえたことをその業務以外では利用しないよう、周知徹底する。
- 適宜必要性に応じて、外部監査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、省内の文書規定及び監査の重要性等をかんがみて、情報の格付けの実施等適切な取扱いを行うとともに、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。

### 3.3　監査の目的及び位置付け




#### 3.3.1　準拠性監査（保証意見及び助言意見）

(1)　【*当省*】の省庁基準が政府機関統一基準に準拠しているかを確認・評価する。

> **政府機関の情報セキュリティ対策における政府機関統一基準の策定と運用等に関する指針　　1-2 本指針で使用する主要な用語の説明**
> (6)「省庁基準」とは、各府省庁がそれぞれ策定する情報セキュリティポリシーであり、省庁基本方針と省庁対策基準からなる。

(2)　【*当省*】の実施手順が省庁基準に準拠しているかを確認・評価する。

> **政府機関の情報セキュリティ対策における政府機関統一基準の策定と運用等に関する指針　　1-2 本指針で使用する主要な用語の説明**
> (7)「実施手順」とは、省庁基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた文書をいう。

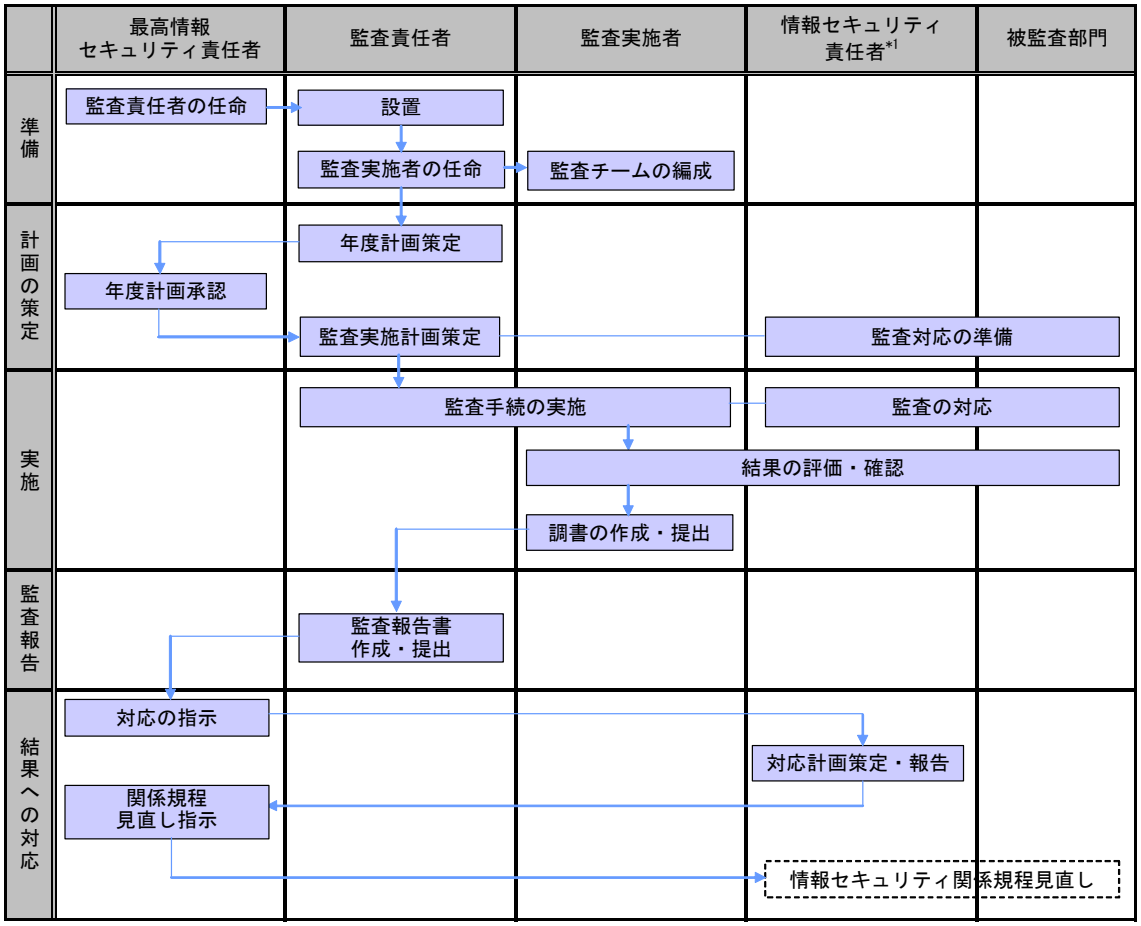
(3)　【*当省*】における情報セキュリティ対策の運用が情報セキュリティ関係規程に準拠しているかについて、自己点検結果等をもとに確認・評価する。

> **政府機関統一基準　　1.1.3 用語定義**
> 「情報セキュリティ関係規程」とは、省庁基準及び省庁基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。

### 3.3.2　妥当性監査（助言意見）

(1)　*【当省】*の情報セキュリティ関係規程が実効性のあるものになっているか（政府機関統一基準における強化遵守事項について、特に重要なシステムへの適用の採否が妥当であるかを含む）、情報セキュリティ対策が妥当であるか又は有効に機能しているかについて、自己点検結果等をもとに確認し、改善提案等の助言を行う。

## 3.4　監査業務の全体像




＊1：被監査部門以外の情報セキュリティ責任者を含む場合がある。

# 4　監査実施に当たっての前提及び準備

## 4.1　監査責任者の役割及び権限

(2)　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。

(3)　監査責任者は、年度情報セキュリティ監査計画及び監査実施計画（以下「監査計画」という。）を策定し、監査を実施する。

(4)　監査責任者は、監査実施者を任命*【し、監査チームを編成】*する。

(5) 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。

- 監査責任者は、準拠性監査の結果を保証する。
- 監査責任者は、妥当性監査の結果に基づき、改善提案等の助言を行う。

(6) 監査責任者は、監査計画の立案、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。

***【手順策定者への補足説明：監査業務の品質とは】***

*実施された監査が、省庁基準や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かという監査業務の信頼性及び有効性のこと。*

(7) 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ヒヤリング等により、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。

### 4.2 監査実施体制の確立及び監査実施者の任命

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を省内から広く選定し、監査実施体制を確立する。

***【手順策定者への補足説明：監査実施者に求められる一般的な要件】***

- *高い倫理観*
- *監査対象業務についての知識・理解*
- *情報セキュリティについての知識・技術*
- *情報システムについての知識・技術*
- *監査についての知識・技術*

(2) 監査責任者は監査実施者を任命する際に、監査責任者自らの所管する部署又は省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。

***【手順策定者への補足説明：監査チーム編成における配慮事項】***

- *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*

(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、当該情報システム等の監査を実施させないものとする。

(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、省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。

***【手順策定者への補足説明：監査に必要な人的リソースの目安】***

*監査対象とする項目やシステム、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は異なるが、10～20 名程度／省、人年換算をすると 5 ～10 名程度の体制が目安と考えられる。*

*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。*

(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。

***【手順策定者への補足説明：監査遂行能力とは】***

*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。*

(8) 監査責任者は、外部委託をする場合、委託先の選定に当り、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。

***【手順策定者への補足説明：監査業務の委託先の選定に関する配慮事項】***

*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人資格者の参画を考慮することが望ましい。*

### 4.3 情報収集及び状況の理解

(1) 監査責任者は、監査計画の策定及び監査の実施に当たり、事前に情報セキュリティ責任者等へのヒヤリングや省内の組織及び所管業務に関する情報収集を行い、省内のセキュリティ関連状況に関する理解に努める。

***【手順策定者への補足説明：収集する情報の例】***

- *省内の組織図及び情報セキュリティ関係の体制図*
- *省内の情報セキュリティ関係規程（省庁基本方針、省庁対策基準、実施手順等）*
- *各組織及び各情報セキュリティ関係の責任者の一覧*
- *各組織の業務内容*
- *各業務で取り扱う情報の種別*
- *保有している情報システムの一覧*
- *ネットワーク図等の情報システムに関する情報*
- *以前に実施した監査に関する計画及び報告書等の監査結果*

## 5 年度情報セキュリティ監査計画の策定

### 5.1 目的及び位置付け

(1) 監査責任者は、省内監査関係者と情報を共有することにより、省内における監査業務を円滑に実施することを目的とし、継続的かつ定期的に行うべく当該年度における監査の年度計画を策定する。

(2) 【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。

## 5.2　概要

(1) 監査責任者は、*【毎年２月末日】*までに翌年度の「年度情報セキュリティ監査計画」を策定する。

(2) 策定した「年度情報セキュリティ監査計画」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。

(3) 監査責任者は、監査実施計画の修正で適応しきれないほどのリスクの変動があった場合には、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。

(4) 監査責任者は、当該年度に実施する監査の位置付けや目的、目標を明確化する。

(5) 【中・長期計画を策定する場合】
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監査計画を策定する。

*【例】*

- *初年度　：省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実施の定着化及び省内セキュリティレベルの底上げ*

(6) 監査責任者は、当該年度計画の監査対象を明確化し、省内監査関係者に周知する。

***【手順策定者への補足説明：監査対象選定のための観点の例】***

- *自己点検が適切に行われているかを確認するための観点*
- *遵守できていない（と思われる）ところを重点的に監査する観点*
- *毎年同様の監査を実施し、対策状況の進捗や成熟度を経年で確認・評価する観点（定点観測的に経年で確認・評価する観点）*
- *環境の変化や監査時点での情報セキュリティ事案の動向・トピックス、体制・規定の変更等をかんがみ、年度別の重点監査対象の項目や重点システムを評価する観点（当該年度重点監査対象の選定）*
- *導入段階、定常的運用段階等業務のライフサイクルに応じて確認する観点*
- *以前実施した監査結果で明らかになった課題及び問題点の改善状況を確認する観点*

(7) 監査責任者は、実施時期の調整や内容の重複の回避などを配慮し、会計検査や特定業務の監査等、恒常的に行われている通常の監査業務との連携を視野に入れて年度計画を策定する。

(8) 監査責任者は、年度情報セキュリティ監査計画に次の事項を記載する。

- 監査方針
- 監査の目的
- 監査対象（業務、システム、段階等）及び監査対象に係る監査目標（例えば、機密性、情報漏えい防止、不正アクセス防止等）
- 監査の想定カバー率

- 監査スケジュール
- 監査業務の管理体制
- 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
- リソース管理（監査予算、人材育成計画等）

### (9) 【例】年度情報セキュリティ監査計画の雛形

作成日：○○年４月１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計画書**

１．監査方針

本年度は、当省内における情報セキュリティ関係の体制構築及び対策の実施状況を網羅的に把握・評価する。来年度以降の対策レベル向上に向けた基盤整備を行う。

２．監査の目的

当省内における情報セキュリティ関係の状況を網羅的に把握することにより、現在の情報セキュリティ関係規程の妥当性を評価し、来年度以降の対策レベル向上に向けた情報収集・分析を行う。

３．監査対象及び監査対象に係る監査目標

(1) 重点監査対象

① 省庁基準及び実施手順の準拠性監査（監査目標：○○○）
② 情報セキュリティ管理体制の構築の監査（監査目標：○○○）
③ 情報の格付け業務の監査（監査目標：○○○）
④ 省内 LAN の運用状況の監査（監査目標：○○○）

(2) その他の監査対象

① 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．監査の想定カバー率

(1) 対象となる行政事務従事者（対象となる行政事務従事者/全行政事務従事者）
(2) 対象となるシステム（対象システム数/全システム数）
(3) 対象となる端末（対象端末数/全端末数）

５．監査スケジュール：別紙のとおり

６．監査業務の管理体制：別紙のとおり

７．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

８．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
目標：監査スキルの向上と要員の確保

① 監査業務基礎講座：４月１日～４月 30 日の２週間程度

② 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）

## ●監査スケジュール

| 監査対象 | 作業フェーズ | 2月 | 3月 | 4月 | 5月 | 6月 | 7月 | ・・・ | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 年度計画策定 | | | | | | | | ・・・ | | | | | | |
| 省庁基準及び実施手順の準拠性監査 | 実施計画策定 | | | | | | | ・・・ | | | | | | |
| | 被監査部門への周知 | | | | | | | ・・・ | | | | | | |
| | 監査の実施 | | | | | | | ・・・ | | | | | | |
| 体制の構築の監査 | 実施計画策定 | | | | | | | ・・・ | | | | | | |
| | 被監査部門への周知 | | | | | | | ・・・ | | | | | | |
| | 監査の実施 | | | | | | | ・・・ | | | | | | |
| 情報の格付けの監査 | 実施計画策定 | | | | | | | ・・・ | | | | | | |
| | 被監査部門への周知 | | | | | | | ・・・ | | | | | | |
| | 監査の実施 | | | | | | | ・・・ | | | | | | |
| 省内ＬＡＮの運用の監査 | 実施計画策定 | | | | | | | ・・・ | | | | | | |
| | 被監査部門への周知 | | | | | | | ・・・ | | | | | | |
| | 監査の実施 | | | | | | | ・・・ | | | | | | |
| ・<br>・<br>・ | | | | | | | | ・・・ | | | | | | |
| | | | | | | | | ・・・ | | | | | | |
| | | | | | | | | ・・・ | | | | | | |

## ●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 | △△△△ |
| ・・・ | | | | |
| ・・・ | | | | |
| ・・・ | | | | |
| | | | | |

# 6　監査実施計画の策定

## 6.1　目的及び位置付け

(1) 監査責任者は、年度情報セキュリティ監査計画で対象とした個別業務、システム等に応じて、具体的な監査方法及び監査時期等を計画する。

(2) 監査責任者は、省内における監査を円滑に実施することを目的とし、監査実施計画の内容を被監査部門及び当該部門の所属職員に対し事前に通知する。

## 6.2　概要

(1) 監査責任者は、年度情報セキュリティ監査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実施指示に基づき、個別の監査対象ごとの監査実施計画を策定する。

(2) 監査責任者は、過年度の監査の実施状況その他過去の経験、事前の質問、世の中の状況等を勘案し、監査対象ごとの監査実施計画を策定する。

***【手順策定者への補足説明：監査実施計画策定上の配慮事項】***

- *府省庁のシステム、業務、組織等の特性を分析した上で、影響度や脆弱性から判別し、リスクが高いと思われる領域を抽出する。*
  - *事故の発生可能性が高いと思われる領域（対策を実施していなければ事故の発生可能性が高い領域、対策が不十分と思われる領域、対策が十分に行われているか不明な領域等）*
  - *事故が発生した場合の影響が大きいと思われる領域（機密性の高い情報を取り扱っている領域、完全性の確保が必要となる情報・システムを取り扱っている領域、可用性の確保が必要となる情報・システムを取り扱っている領域等）*
- *自己点検が終了している等、監査の受入れが十分と考えられる領域を選定する。*
- *監査が円滑に実施できるように考慮する。*
  - *人的リソースや予算の状況*
  - *監査対象部門の負荷状況*
  - *システムの運用状況（負荷の多い日、時間帯を避ける等）*
- *システムをカテゴリー分けし、監査頻度を決定する。*

*【例】*

*カテゴリーA：2回／年で監査を実施*

*カテゴリーB：1回／年で監査を実施*

*カテゴリーC：1回／3年で監査を実施*

(3) 監査責任者は、監査実施計画に次の事項を記載する。

- 監査目的
- 背景（直前の情報セキュリティの状況認識）
- 監査対象
- 被監査部門及びその責任者

- 監査実施責任者及び実施担当者
- 監査の実施時期
- 監査の実施場所
- 監査の想定カバー率
- 実施する監査手続の概要（監査要点、評価方法の種類等）
- 監査の進捗管理手段
- 外部委託先との役割分担（外部委託を行う場合）

### (4) 【例】監査実施計画の雛形

作成日：○○年○○月○○日

（情報セキュリティ監査実施者）
氏　　名

**○○年度　××××省情報セキュリティ管理体制の構築に関する監査実施計画書**

1．監査目的
　政府機関統一基準及び当省省庁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、体制図・設置規定等の文書及び当該責任者への質問により確認する。
2．背景
　平成17年12月に政府機関統一基準が策定され、当省でも従来のセキュリティポリシーを改訂し、新たに省庁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、当省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：当省情報セキュリティ管理体制の監査
4．被監査部門及び責任者：大臣官房○○課××××
5．監査実施責任者：△△△△
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：当省内執務室
8．監査の想定カバー率
　対象となる行政事務従事者（対象となる推定行政事務従事者/全行政事務従事者）
　対象となるシステム（対象システム数/全システム数）
　対象となる端末（全端末数/全端末数）
9．実施する監査手続の概要：別紙のとおり
10．監査の進捗管理手段：別紙のとおり

別紙

●監査手続の概要

| 遵守事項 | 対策内容 | 評価方法 | 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 | 設置 | 体制図の確認 | ・・・ | ・・・ |
| | | 質問 | ・・・ | ・・・ |
| | 連絡網の整備 | 体制図の確認 | ・・・ | ・・・ |
| | | | | |
| | | | | |

●監査の進捗管理手段
1．定期報告の実施
2．・・・

# 7 監査の実施

## 7.1 監査の実施の指示

(1) 最高情報セキュリティ責任者は、年度情報セキュリティ監査計画に従って、監査責任者に対して、監査の実施を指示する。

(2) 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、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。監査責任者は監査実施計画を修正し、実施する。

***【手順策定者への補足説明：情報セキュリティ状況の変化の例】***

- *新しいシステムが開発又は導入されたとき*
- *新たに他のシステム又はネットワーク等と接続したとき*
- *省内における大きな人事異動や組織改編があったとき*
- *省内外を問わず重大なセキュリティ侵害があったとき*
- *省庁基準等が改訂又は追加されたとき*

(3) 監査責任者は、被監査部門から独立した監査実施者に対して、監査の実施を指示する。

- 情報システムを監査する場合、当該情報システムを構築又は開発した者はその監査を担当しない。
- 情報資産の運用状況を監査する場合、当該情報資産を運用している者はその監査を担当しない。

## 7.2 監査の実施における留意事項

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

***【手順利用者への補足説明：監査証拠の十分かつ適切な入手方法例】***

- *関連書類の査閲*
- *担当者への質問*
- *現場への視察*
- *システムテストへの立会い*
- *テストデータによる検証*
- *脆弱性スキャン、システム侵入テスト*

(2) 監査実施者は、省庁基準等の規定文書の内容確認を行った上で、被監査部門への質問を基本とする。さらに、別途文書による裏づけをとったり（査閲）、実際に行っている作業を観察したり（観察）、自らが実際に行って点検したり（点検）することにより、質問への回答を検証する。

***【手順策定者への補足説明：評価方法の解説】***

- *質問：講じた対策、行為*
- *査閲：規程類、設定文書（設計書等の設定一覧等）、記録文書、文書証拠*

- *観察：日常の行為*
- *点検：物理的状態、システム上のセキュリティ設定*

***【手順利用者への補足説明：点検による評価における配慮事項】***

*点検という手法を採用する場合には、システム運用を停止させること等がないように配慮し、実際の操作は情報システムセキュリティ管理者等に行ってもらうことが望ましい。*

(3) 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、自己点検票及び自己点検結果を活用する。

***【手順利用者への補足説明：自己点検票の利用等チェックリストによる監査実施における配慮事項】***

*事前に監査チェックリスト等を用意して監査を実施することは、監査業務の経験の浅い監査実施者が行う場合等に有効であるが、通常、監査の最終段階で監査手続が網羅的に行われたかをチェックするために使用することが効果的とされており、以下のことに留意して行うことが望ましい。*

- *効率性確保の観点*
  *リスト上のチェック項目の意味や重要性をかんがみ、上から下に順番に行ったり、同じような質問を繰り返したりしない。*
- *有効性検討の観点*
  *チェック項目の内容が現実に合っているかを考慮しながら監査を実施する。*
- *網羅性確保の観点*
  *チェックリストに記載されていない重要な項目がないか検討する。*

*【例】自己点検票の活用例*

| | 自己点検の対象となるセキュリティ対策項目の整理・分析 | | | | | 自己点検の設計 | | | | | | | | | | 備考 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 自己点検項目一覧の作成 | 統一基準との対応 | 分類 | | | 点検方法 | | | 実施時期&頻度 | | 適用範囲 | | | 回答項目 | | 監査における評価方法 |
| | | | 連続・単発 | 定期・不定期 | 頻度 | 随時点検型 | 一括点検型 | 断面調査型 | 自己点検の実施時期 | 自己点検の実施頻度 | 実施主体 | 管理者 | 責任者 | 回答項目 | 備考 | |
| 1 | 人事異動の際には、識別コードの管理を徹底すること。 | 4.1.3 (2) (g) | 連続 | 定期 | 年4 | ○ | | | 実施時 | 実施時 | 権限管理を行う者 | 情シセ管 | 情シセ責 | Yes 日時 | — | 点検 |
| 2 | 情報入手時には、格付け・取扱制限を明示す | 3.2.1 (2) (b) | 連続 | 不定期 | 毎日 | | ○ | | 月末 | 月1 | 行政事務従事者 | 課室情セ | 情報セ責 | Yes No | アンケート併用 | 質問 |
| 3 | ウイルスパターンを最新にするこ | 4.2.2 (2) (c) | 連続 | 不定期 | 週1 | | | ○ | 15日 30日 | 半月1 | 行政事務従事者 | 情シセ管 | 情シセ責 | 設定値 | バージョン番号 | 点検 |
| 4 | ソフト開発時にST確認すること | 4.3.1 (1) (d) | 単発 | 定期 | 年1 | ○ | | | 実施時 | 実施時 | 情報システムセキュリティ責任者 | — | 情報セ責 | Yes 日時 | — | 査閲 |
| 5 | 離席時には画面ロックすること。 | 3.2.2 (3) (b) | 単発 | 不定期 | 毎日 | | ○ | | 月末 | 月1 | 行政事務従事者 | 課室情セ | 情報セ責 | Yes No | — | 質問 |
| ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： | ： |
| | Step 1-1 | Step1-2 | Step 1-3 | | | Step 1-4 | | | Step 1-5 | | Step 1-6 | | | Step 1-7 | | Step 1-8 |

(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、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、異常性を示す兆候があるかを評価する。

## 7.3　実施結果の評価

### 7.3.1　準拠性に関する保証意見

(1) 監査実施者は、政府機関統一基準及び省庁基準、省庁基準及び実施手順の間に矛盾、相違点、不足がなければ、準拠しているものと判断する。

(2) 監査実施者は、遵守事項違反がなければ、準拠しているものと判断する。

*【例】準拠性判断の基準例（最大逸脱率が9%であることを90%の信頼度で確認する場合）*

- *25件のサンプルのうち、1件も遵守事項違反がなければ、準拠しているものとする。*
- *25件のサンプルのうち、1件の遵守事項違反があっても、追加で20件のサンプルを選び、1件も遵守事項違反がなければ準拠しているものとする。*
- *それ以外は準拠していないものとする。*

### 7.3.2　妥当性に関する助言意見

(1) 助言意見は、想定するリスクと比較して、対策が妥当であるかについての意見とする。

(2) 監査実施者は、将来の遵守事項違反につながる可能性のある事象について助言を行う。

(3) 監査実施者は、助言意見を検討するに当たり、実施すべき対策の実現可能性についてまでは考慮せず、原則を指摘することを役割とし、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。

(4) 被監査部門の情報セキュリティ責任者は、実施すべき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。

### 7.3.3　監査業務において発見された問題点・違反等の取扱い

(1) 監査実施者及び被監査部門の情報セキュリティ責任者は、発見された問題点に関する事実関係について、事実誤認等がないかを含め合意をしておく。

(2) 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して報告する。

***【手順策定者への補足説明：重大な違反と軽微な違反の定義例】***

- *重大な違反とは、その違反単独で、又は他の違反と複合することにより、重大なリスクの発生を引き起こす可能性のあるものをいう。*
- *軽微な違反とは、重大な違反以外のものをいう。*

## 7.4　監査調書の作成

(1) 監査実施者は、実施した監査業務ごとに、監査実施の過程を監査報告書作成の基礎とするため記録した監査業務の実施記録であり、監査意見表明の根拠となる監査証拠集である監査調書を作成し、監査責任者に報告する。

(2) 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作成する。

(3) 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添付する。

(4) 監査責任者は、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考慮した上で、あらかじめ定められた期間保存する。

(5) 監査実施者は、監査調書に次の事項を記載する。

- 表題（何を確認したか、何を証明したいか）
- 監査実施者氏名・署名
- 実施期間
- 被監査部門及び責任者
- 発見された問題点（重大な違反、軽微な違反）
- 意見（保証意見、助言意見）
- 確認した遵守項目
- 確認した対策の内容
- サンプルの件数及び抽出方法
- 評価方法及び結果
- 監査証拠としての形態（文書か口頭か）
- 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）
- 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。）

### (6) 【例】監査調書の雛形

〇〇年〇〇月〇〇日

情報セキュリティ監査責任者　殿

（監査実施者）
署　名

**情報セキュリティ管理体制構築に係る情報セキュリティ監査の報告**

平成〇〇年度情報セキュリティ管理体制の構築に関する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××日から〇〇年〇〇月〇〇日まで
2．被監査部門及び責任者：・・・・・・
3．発見された問題点
　(1) 重大な違反
　　・・・・・・
　(2) 軽微な違反
　　・・・・・・
　(3) 課題及び問題点等
　　・・・・・・
4．意見
　(1) 準拠性に関する保証意見
　　・・・・・・
　(2) 妥当性に関する助言意見
　　・・・・・・
5．実施内容：別紙のとおり

別紙

| 遵守事項 | 対策内容 | 評価方法 | 評価結果 | サンプル | | 監査証拠 | | 関連資料番号 |
|---|---|---|---|---|---|---|---|---|
| | | | | 件数 | 抽出方法 | 形態 | 入手元 | |
| 課室情報セキュリティ責任者の設置 | ・・・ | ・・・ | ・・・ | 50/200 | 無作為 | 文書 | 第三者 | 001 |
| | ・・・ | ・・・ | ・・・ | ・・・ | ・・・ | 口頭 | 直接入手 | — |
| | | | | | | | | |
| | | | | | | | | |

# 8　監査報告

## 8.1　監査報告書の作成と提出

(1) 監査責任者は、監査調書に基づき、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。

(2) 監査責任者は、監査報告書において、準拠性監査については、当該監査対象の準拠性に関する保証を行うとともに、違反を改善するための助言を行う。また、妥当性監査については、助言を行い、省内 PDCA サイクルの実施により改善につなげる。

(3) 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報告内容の重要性や指摘事項の緊急性等を理解し、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。

***【手順利用者への補足説明：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助言意見については、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、記述*

(4) 監査責任者は、助言意見を述べるに際して、監査人の自由裁量ではなく、省庁基準や当該契約書等の監査の基準に照らして検出された課題及び問題点の指摘と改善提言とするものとし、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。

(5) 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。

(6) 監査責任者は、監査報告書に次の事項を記載する。

- 報告書の名称
- 報告書の日付
- 報告書の宛名
- 監査人の署名、又は記名押印
- 監査実施期間
- 監査対象範囲（組織、システム、業務機能等）
- 監査の基準（判断の尺度）とした管理基準等
- 総合的所見
- 監査意見（違反の有無、課題及び問題点等）
- 監査人の独立性に関する事項

  *【独立性の例】*
  - ○ 過去一度も当該監査対象業務に従事していない
  - ○ 過去2年の間、当該監査対象業務に従事していない

- 過去1年の間、当該監査対象業務に従事していなく、それ以前に当該業務に係る規定の整備又はシステムの設定等現在に影響の及ぶ行為をしていない

- 運用状況の準拠性に関する監査を実施した旨及びその結果（準拠性監査の場合）
- 遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨及びその結果（妥当性監査の場合）
- 監査報告書の取扱い（利用及び利用者の制限事項等）
- 添付資料（個別業務ごとの監査調書等）

### (7) 【例】監査報告書の雛形

- 準拠性監査報告書の雛形

○○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**
（準拠性監査報告）

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

1. 監査実施期間：**××年××月××日から○○年○○月○○日まで**
2. 監査対象範囲
   ・・・・・・
   ・・・・・・
3. 監査の基準：省庁基準及び当該請負契約書
4. 総合的所見：・・・・・・・・
5. 監査意見
   (1) 違反の有無
      ① 重大な違反
         ・・・・・・
      ② 軽微な違反
         ・・・・・・
   (2) 課題及び問題点
      ・・・・・・
   (3) 助言意見
      ・・・・・・
6. 添付資料
   (1) 平成○○年度×××に係る情報セキュリティ監査の報告
   (2) ・・・

なお、本職**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、以上のとおり意見を表明するものである。**
また、本報告書の利用は、当省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。

- *妥当性監査報告書の雛形*

*○○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***
*（妥当性監査報告）*

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

1. *監査実施期間：**××年××月××日から○○年○○月○○日まで***
2. *監査対象範囲*
   ・・・・・・
   ・・・・・・
3. *監査の基準：省庁基準及び当該請負契約書*
4. *総合的所見：・・・・・・・・*
5. *監査意見*
   *(1) 課題及び問題点*
   ・・・・・・
   *(2) 助言意見*
   ・・・・・・
6. *添付資料*
   *(1) 平成○○年度×××に係る情報セキュリティ監査の報告*
   *(2) ・・・*

*なお、本職**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、以上のとおり意見を表明するものである。***
*また、本報告書の利用は、当省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。*

# 9　監査結果に対する対応

## 9.1　監査報告書の内容の分析及び評価

(1) 最高情報セキュリティ責任者は、報告内容を分析し、全体像の把握と課題及び問題点の整理を行う。

(2) 最高情報セキュリティ責任者は、監査報告書において、改善提案等の助言があった場合、その内容の妥当性及び実現可能性等を検討する。

(3) 最高情報セキュリティ責任者は、同種の課題及び問題点が他の部門にもあり得るかの検討及び対策の見直し等の緊急性の検討を行う。

## 9.2　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、被監査部門の情報セキュリティ責任者に対して、指摘事案に対する対応を指示する。

(2) 最高情報セキュリティ責任者は、被監査部門における課題及び問題点が他の部門にも発生する可能性があると判断した場合、他の情報セキュリティ責任者に確認する。

(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応を指示する。

## 9.3　対応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事案について、対応計画を作成し、報告する。

(2) 情報セキュリティ責任者は、指示された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、リスク軽減策を示した上で、達成可能な対応目標を提示する。

(3) 情報セキュリティ責任者は、指示された改善内容が教育・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。

## 9.4　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、監査報告書において情報セキュリティ対策の妥当性に関した改善提案を受けた場合、情報セキュリティ関係規程の妥当性を評価し、当該規定を整備した者に対して必要に応じてその見直しを指示する。

(2) 最高情報セキュリティ責任者は、改善提案を受けた場合であって、情報セキュリティ関係規程の見直しの必要がないと判断したときは、その理由を明確にする。