政府機関等のサイバーセキュリティ対策のための
統一基準群に基づく情報セキュリティ監査の実施手引書

令和５年 11 月

内閣官房 内閣サイバーセキュリティセンター

はじめに

情報セキュリティ対策が有効に機能しているか否かを評価・点検するためには、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対策の監査を実施することが必要である。また、監査の結果で明らかになった課題を踏まえ、必要な対策を講じることが重要である。

このため、「政府機関のサイバーセキュリティ対策のための統一規範（平成 28 年８月 31 日付けサイバーセキュリティ戦略本部決定（令和５年７月４日改定)）」（以下「統一規範」という。）に、国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）は、「対策基準が本規範及び統一基準に準拠し、かつ実際の運用が対策基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない」と規定している。また、これをより具体化する形で、「政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度版)」（以下「統一基準」という。）は、情報セキュリティ監査の実施について規定しており、「政府機関等の対策基準策定のためのガイドライン（令和５年度版)」（以下「ガイドライン」という。）に、情報セキュリティ監査に関する対策基準の策定及び実施に際しての考え方が記載されている。

各機関等は、これら規程、統一基準及びガイドラインを踏まえ各機関等が自ら定めた情報セキュリティポリシーに基づき情報セキュリティ監査を行うこととなる。内閣サイバーセキュリティセンターでは、各機関等において、情報セキュリティ監査の計画策定から、監査の実施、監査報告、改善までの各過程においてより詳細な参考となる資料として、「政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書」を策定していた。今般、統一基準群の改定に伴い、その変更内容を反映した「政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書」（令和５年 11 月）（以下「本書」という。）として改定した。

各機関等におかれては、本書も参考に、実効性のある情報セキュリティ監査を実施することが望まれる。

改版履歴

版数	年月日	変更内容
1	2006 年３月 31 日 （平成 18 年３月）	初版
2	2011 年３月 21 日 （平成 23 年３月）	平成 23 年度の政府機関統一管理基準及び政府機関統一技術基準の改定に伴う修正
3	2017 年４月 （平成 29 年４月）	平成 28 年度の統一基準群の改定に伴う改定
4	2022 年 10 月 （令和４年 10 月）	平成 30 年度及び令和３年度の統一基準群の改定等に伴い、「政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書」として全面改定
5	2023 年 11 月 （令和５年 11 月）	令和５年度の統一基準群の改定等に伴う改定

目　　次

第１部　本書の概要

1. 本書の目的

本書は、統一基準の遵守事項 2.3.2 に規定され、機関等が統一基準に基づいて実施する、情報セキュリティ関係規程（機関等の対策基準、運用規程及び実施手順の総称をいう。以下同じ。）の整備・運用に関する情報セキュリティ監査を対象としたものである。

情報セキュリティの確保のためには、機関等の基本方針及び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る。

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、監査対象からの独立性を有する者による情報セキュリティ監査を実施し、情報セキュリティ関係規程の統一基準への準拠性及び情報セキュリティ関係規程が機関等において確実に実施され、情報セキュリティ対策が有効であることを確認することが必要である。

本書は、

・監査実施計画の策定における考え方や計画に含めるべき内容

・情報セキュリティ監査を実施するにあたり、機関等が実施すべき事項、実施手順等を具体的に示すことにより、情報セキュリティ関係規程の整備・運用に関する情報セキュリティ監査の適切な実施に資することを目的とする。

2. 本書の利用方法等

(1) 本書の想定対象者

本書を利用する主な対象者は、機関等の情報セキュリティ監査の業務を担う、機関等の最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ監査責任者及び情報セキュリティ監査を実施する監査実施者である。

これらの者が、統一基準に基づく機関等の情報セキュリティ監査を実施する際に、本書を利用することを想定している。

(2) 本書の構成と利用方法

本書は、第１部「本書の概要」、第２部「情報セキュリティ監査の基礎知識及び統一基準における位置づけ」、第３部「情報セキュリティ監査の具体的な実施手順及び実施内容」から構成されている。

第２部は機関等が情報セキュリティ監査を実施するに先立ち重要と考えられる基礎知識を体系的にまとめたものである。

第３部は、記載例や付録と併せて、機関等が情報セキュリティ監査の実施手順を策定する際のひな形として利用できるように作成されている。これを用いることで効率的に監査が実施できると考えられる。

なお、機関等の特性に合わせて、情報セキュリティ監査の実施手順を修正することや、本書を利用せず独自のひな形を利用することを妨げない。

3. 統一基準群における本書の位置づけ

ガイドラインの遵守事項 2.3.2(1)(a)の解説において、「内閣官房内閣サイバーセキュリティセンターが公表している「政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書」は、監査実施計画の策定における考え方や計画に含めるべき内容等を具体的に示しており、これを参考に計画を策定するとよい。」と記載されている。

統一基準群と本書との関係を図 1.3-1 に示す。

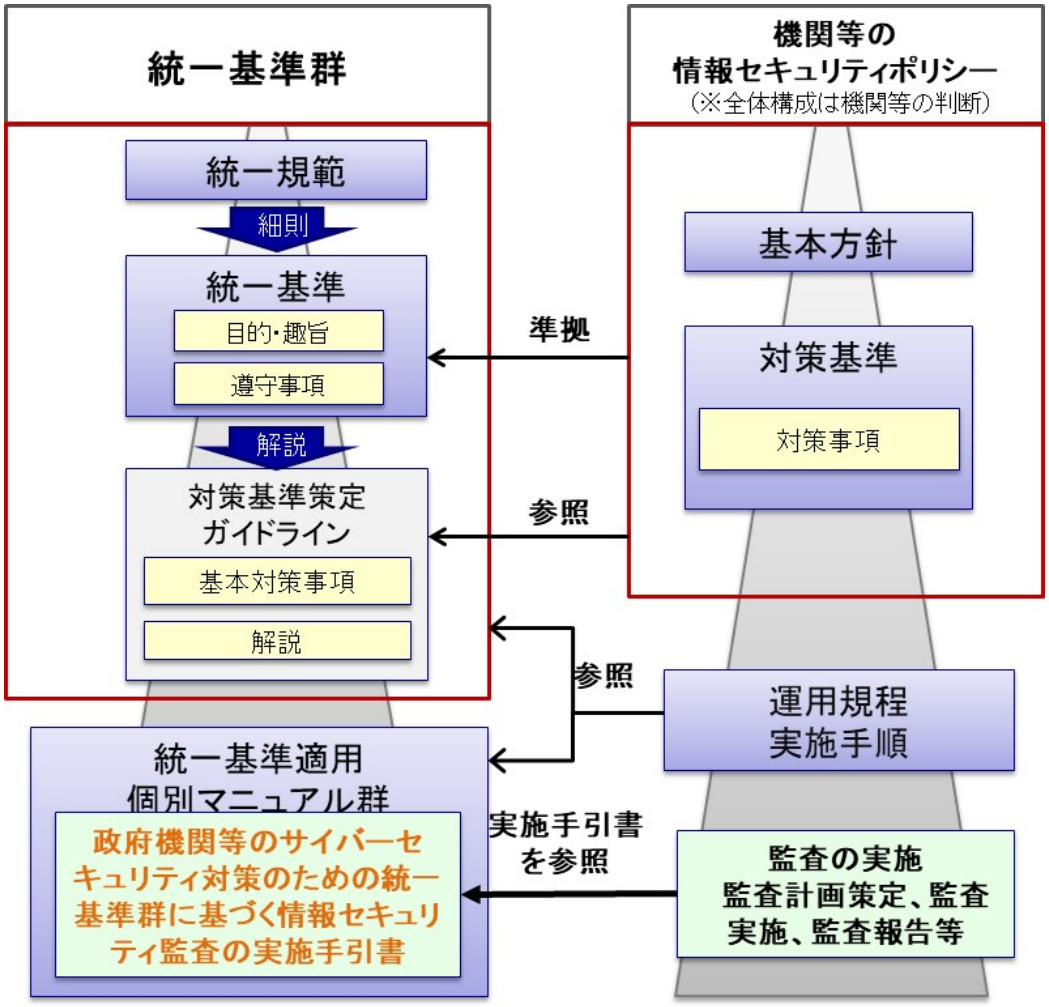

図1.3-1　統一基準群と本書との関係

4. 用語の定義

本書において使用する用語の定義は、以下に定めるところによる。

【あ】

- 「運用規程」とは、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運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。

【か】

- 「監査項目」とは、（情報セキュリティ）監査を通して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の評価をいう。
- 「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した者をいう。
- 「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、監査実施計画に則って監査を実施したという証拠、その他関連資料等をいう。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、監査対象の組織側から提出された資料のほか、場合によっては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取りまとめたファイルをいう。
- 「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、監査対象の情報システムの詳細情報を有する組織又は機関等の内部の情報システム部門等の専門家をいう。

【さ】

- 「実施手順」とは、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や手続をいう。
- 「指摘事項」とは、統一基準の遵守事項が守られておらず「改善が必要である」事項をいう。
- 「指摘事項等」とは、監査報告書に記載する「指摘事項」と「推奨事項」をいう。
- 「情報セキュリティ関係規程」とは、対策基準、運用規程及び実施手順を総称したものをいう。
- 「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。
- 「推奨事項」とは、統一基準の遵守事項は守られているが、対策として改善の余地があり、「改善が望まれる」事項をいう。

【た】

- 「対策基準」とは、機関等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。
- 「統制」とは、リスクを抑制、低減、修正するための対策をいう。コントロールということもある。

【は】

- 「発見事項」とは、監査の過程において発見された事実をいう。なお、この事実は、最終的に監査報告書に記載する指摘事項又は推奨事項になる可能性があるもの、指摘事項又は推奨事項に含まれないものの、監査で気になる点、等の幅広いものが含まれる。
- 「PDCA サイクル」とは、管理業務や品質管理の効率化を目指す手法であり、計画から改善までを１つのサイクルとして、このサイクルを回し続けて、その精度を高めることをいう。PDCA は、Plan（計画）、Do（実行）、Check（点検）、Act（改善）の頭文字を取ったものである。
- 「本部監査」とは、サイバーセキュリティ基本法第 26 条第１項第２号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いう。

第 2 部 情報セキュリティ監査の基礎知識及び統一基準における位置づけ

1. 監査に関する基礎知識

機関等では、機関等で策定した情報セキュリティ関係規程を基に、情報セキュリティの対策を実施し、PDCA サイクルを回している。この PDCA サイクルの一角を占めるのが、情報セキュリティ監査である。情報セキュリティ監査は、情報セキュリティ対策の実施状況の不備等を発見するとともに、その課題を明らかにし、情報セキュリティ対策の改善を促すことにより、機関等の情報セキュリティレベルを維持、向上させていく役割を担う。

情報セキュリティ監査に関連する監査形態、監査の種類、監査人の要件、監査技法は以下のとおりである。

(1) 情報セキュリティ監査とシステム監査[1]

情報セキュリティ監査に関して、経済産業省が作成している情報セキュリティ監査基準[2]には、「情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。」と記載されている。

他方、情報システムの監査としては、情報セキュリティ監査のほかに、システム監査がある。システム監査に関して、経済産業省が作成しているシステム監査基準3には、「システム監査は、情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。」と記載されている。

どちらも、独立、かつ専門的な立場の監査人が、リスクに対して適切に実施していることを評価する点では同じであるが、異なる点がいくつかある。

例えば、情報セキュリティ監査の場合には、リスク評価の対象が情報セキュリティ（つまり、情報資産の機密性、完全性、可用性）であり、システム監査ではリスク評価の対象は、情報システムである。

---

[1] 日本システム監査人協会：「システム監査と情報セキュリティ監査の違いと関連　１０のＱ＆Ａ」　を参考に執筆

[2] 経済産業省：情報セキュリティ監査基準　Ver1.0

[3] 経済産業省：システム監査基準　（平成 30 年 4 月 20 日）

また、情報セキュリティ監査の役割は、組織が管理、活用する情報資産に対して機密性、完全性、可用性が確保されていることを評価することにある。これに対して、システム監査の役割は、情報システムが組織の目的に合致した形で構築、運用され、情報システムに対する投資と効果が適切であり、情報システムの信頼性、安全性、効率性が確保されていることを評価することにある。

情報セキュリティ監査とシステム監査について図 2.1-1 のように整理できる。

	情報セキュリティ監査	システム監査
リスクと統制の対象	情報資産を対象にリスクと統制をとらえる	情報システムを対象にリスクと統制をとらえる
目的	組織体が情報資産を決めごとに従って目的通りに管理・活用しているかを評価	経営資源を投下して構築・運用する情報システムが組織体のためになっているかを評価 （ITガバナンスの実現に寄与しているか）
観点	情報資産に対する機密性、完全性、可用性が確保されているか	情報システムが組織体の目的に合致した形で構築・運用されているか、情報システムに対する投資効率が適切か、組織体が活動を行ううえで情報システムの信頼性・安全性・効率性が確保されているか

図 2.1-1　情報セキュリティ監査とシステム監査

(2) 監査の種類[4]

一般に、監査には、保証型監査と助言型監査がある。

保証型監査とは、監査対象となる基準のマネジメント又は統制が、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査をいう。保証型監査の例として、公認会計士による会計監査がある。保証型の監査の結論として表明される監査意見は、監査人が監査における監査基準に従って監査手続を行い全ての重要な点において適正に表示しているかどうかについて、監査人が自ら入手した監査証拠に基づいて判断した結果を意見として表明していることを留意する必要がある。

また、助言型監査とは、監査対象となる組織のマネジメント又は統制の改善を目的とし、監査の基準に対する欠陥及び懸念事項等の問題点を発見し、必要に応じて発見事項に対応した改善提言を監査意見として表明する形態の監査をいう。多くの監査は、組織のマネジメント又は統制の改善に結び付ける助言型監査を実施している。助言型の監査

[4] 日本セキュリティ監査協会：「情報セキュリティ監査用語集 Ver2.0」を参考に執筆

の結論として表明される助言意見は、改善を要すると判断した事項を監査人の意見として表明するものである。

どちらの監査を選択するかは、その費用対効果、及び通常業務への負荷等を考慮し、実際に基準に対する成熟度を考慮して決定する。

また、監査の観点として、典型的な評価方法として「準拠性評価」と「妥当性評価」がある。

準拠性評価は、事前に定めた監査の基準（本書では、統一基準及び対策基準等が該当する。）を基にして整備した規程類がその基準に準拠しているか、又はセキュリティ対策の運用状況が監査の基準に準拠しているかを評価する。

他方、妥当性評価は、組織が実施しているセキュリティ対策が監査の基準に準拠した上で、有効なものであるかを監査人の専門家の視点から評価する。

妥当性評価は、監査対象の組織、業務、情報システム等について、最新の脅威動向、サイバーセキュリティ技術動向、情報セキュリティインシデント動向、その他様々な最新動向を考慮し、監査人が監査対象の組織の情報セキュリティ対策を更に高める取り組みが適切に運用されているかを判断した上で、情報セキュリティ対策に寄与する取り組みを助言するものである。

妥当性評価は、準拠性評価を満たした上で、更なる情報セキュリティ対策を講じるよう助言するものであり、監査対象の組織と丁寧なコミュニケーションが必要となり、監査に必要な作業工数の増加や情報セキュリティ対策の必要性を説明する根拠の明確化等、監査人の負担も大きいため、情報セキュリティのリスクの高い対策に限定して実施することも考えられる。

(3) 監査人の要件

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。[5]

① 独立性、客観性と職業倫理

(a) 外観上の独立性

情報セキュリティ監査人は、情報セキュリティ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。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

(b) 精神上の独立性

情報セキュリティ監査人は、情報セキュリティ監査の実施にあたり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

[5] 経済産業省：情報セキュリティ監査基準　Ver.1.0

(c) 職業倫理と誠実性

情報セキュリティ監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

② 専門能力

情報セキュリティ監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

③ 業務上の義務

(a) 注意義務

情報セキュリティ監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

(b) 守秘義務

情報セキュリティ監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

④ 品質管理

情報セキュリティ監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

(4) 監査技法

情報セキュリティ監査の監査手続で利用できる監査技法を表 2.1-1 にまとめる。

表 2.1-1　監査技法[6]

監査技法	監査技法の概要	技法の説明、注意点
質問 （ヒアリング）	監査における判断基準について整備状況又は運用状況の準拠性を評価するために、関係者に対して口頭で問い合わせ、説明や回答を求める監査技法	・文書による問い合わせを含む。 ・必要に応じて監査対象の組織から外部委託先への問い合わせも含む ・質問結果の食い違い、虚偽の説明に注意する。 － 複数の担当者又は管理者へのヒアリングで信憑性を高める。 － 他の監査技法と組み合わせて食い違いの原因を明確にする。
チェックリスト	監査における判断基準についての整備状況又は運用状況の準拠性を評価するために、特定の事項について、直接特定者に問い合わせ、回答を入手する監査技法	・あらかじめ特定の事項について質問項目を定め、回答を選択式又は記述式により記載させる。 ・効率良く必要十分な監査証拠を入手するためには、あらかじめ、質問内容を吟味し、適切な担当者の選択が必要である。 ・虚偽の回答に注意が必要である。
査閲 （レビュー）	監査における判断基準についての整備状況又は運用状況の準拠性を評価するために、規程、手順書、記録（電磁的な記録も含む）等を確かめる監査技法	・情報セキュリティ関係規程、運用手順書、各種申請書類（ID の付与、アクセス権の付与等）、情報システム上の設定値、ログ等 － 客観性は高いが、改ざんに注意する。 － 複数の文書類の突き合せや、質問との併用が必要である。
観察 （視察）	監査における判断基準についての整備状況又は運用状況の準拠性を評価するために、監査人自ら赴き、目視によってプロセスや手続を確かめる監査技法	・運用担当者が運用手順書に従った操作を実際に行っていることを、監査人自ら直接に把握し、その妥当性や適否を判断する。 ・監査人が目視によって確かめるため、証拠力は強い。 ・厳密には観察(視察)した時点のみについての証拠能力しかもたないことに注意が必要である。 － 都合の悪い部分は見せていない可能性がある。 － 運用の全てを観察(視察)することは困難である。
再実施	監査における判断基準の準拠性についての運用状況を評価するために、監査人自らが組織体の統制を運用し、統制の妥当性や適否を確かめる監査技法	・例えば、カードによる入室管理が行われている場合、アクセス権が付与されていないカードを利用し、監査人自らがエラーとなることを確かめる。 ・監査人が自ら運用してみるため、証拠力は強い。 ・厳密には再実施を行った時点のみの証拠能力しかもたないことに注意が必要である。 － たまたまそこだけ問題なかったのかもしれない。 － 全ての統制を運用してみることは困難である。
サンプリング	監査対象となった入手資料から一部をサンプルとして抽出して監査手続を実施し、その結果から監査対象項目全体の特性を推定するという試査の技法	・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、サンプリング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。 ・評価では、評価対象期間中の母数(サンプル数)に応じてサンプリングを行う。

[6] 経済産業省：「情報セキュリティ監査手続ガイドラインを利用した監査手続策定の手引」（平成 21 年 7 月）を参考に執筆

情報システムに対する脆弱性を調査する手法として、脆弱性診断とペネトレーションテストを実施することがある。その概要を表 2.1-2 にまとめる。

表 2.1-2　脆弱性調査手法

手法	手法の概要	手法の説明、注意点
脆弱性診断	情報システムに存在する脆弱性や情報セキュリティ機能の不備を網羅的に検査する手法	・網羅的に脆弱性を洗い出すため、定型的なテストケースに基づいた作業を中心に行う。 ・脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、テスト対象の種類によって利用する脆弱性診断を使い分ける必要がある。
ペネトレーションテスト	実際に脆弱性を悪用した疑似攻撃を実施し、侵入やデータ窃取、改ざん等の目的を達成することが可能であるかどうかを検証する手法	・目的の達成可否の検証が中心で、網羅的な脆弱性調査は行わない。 ・実際の攻撃手法を用いた手動テストが中心である。 ・外部からの侵入自体を試行する例や、侵入されたことを前提として内部からテストを実施する例がある。 ・脆弱性診断と比較して、高コストで期間も長くなる傾向がある。

2. 情報セキュリティ監査の位置づけ及び全般的な留意点

2.1. 統一基準における情報セキュリティ監査の位置付け

統一基準の「第２部　情報セキュリティ対策の基本的な枠組み」は、PDCA サイクルの「2.1　導入・計画」(P)、「2.2 運用」(D)、「2.3 点検」(C)、「2.4 見直し」(A) で構成されており、情報セキュリティ監査は、C(点検)の一部として実施される。

遵守事項 2.3.2(2)(a)の基本対策事項 2.3.2(2)-2 では、統一基準の情報セキュリティ監査として以下の 3 つの項目を含む準拠性の評価の観点からの監査が求められている。

① 機関等の対策基準について、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

② 機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していること

③ 監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していること

なお、これらの監査では、①は統一基準、②は機関等の対策基準、③は機関等のセキュリティ関係規程を監査の基準とする。

本書では、これらの情報セキュリティ監査の実施手順について記載する。

なお、準拠性の評価の実施が定着した後は、監査対象の情報セキュリティが妥当であるかの観点での評価（妥当性評価）の実施を検討することも考えられる。

統一基準と本書が対象とする情報セキュリティ監査の関係を図 2.2-1 に示す。

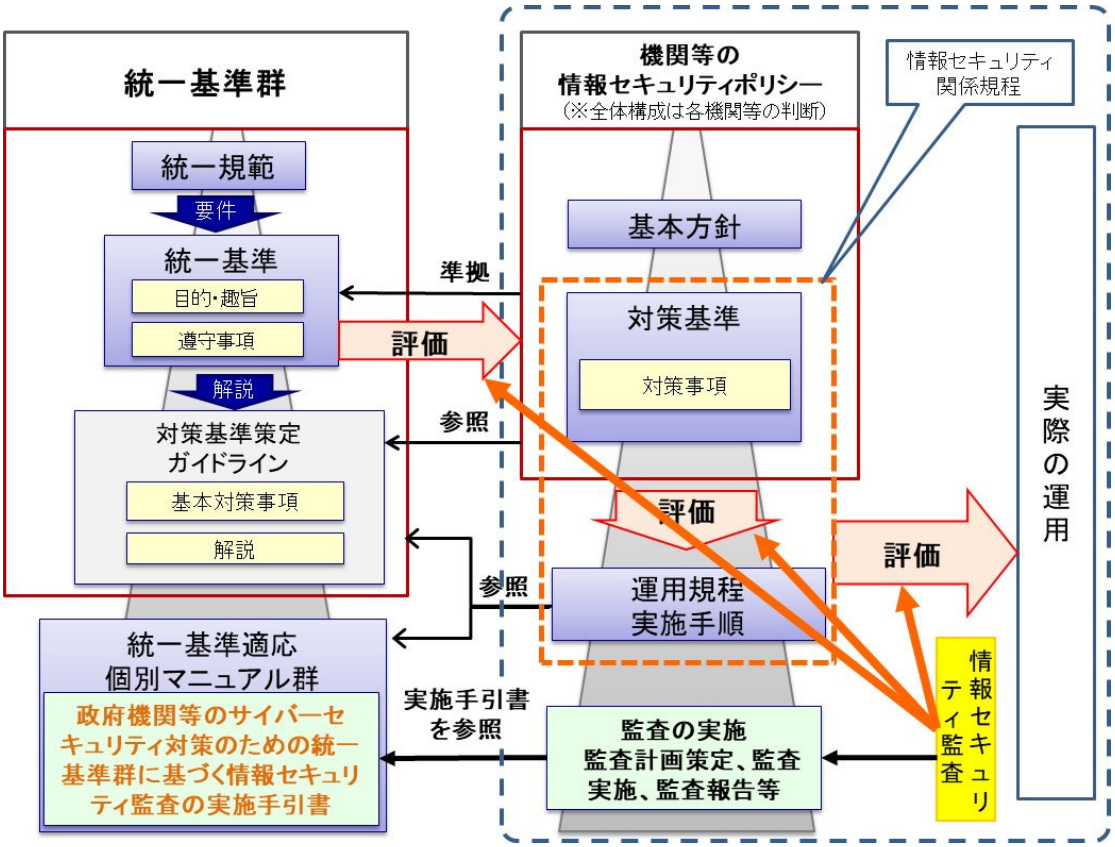

図 2.2-1　統一基準と対象とする監査の関係

統一基準 2.3「点検」には自己点検と情報セキュリティ監査の記載がある。自己点検と情報セキュリティ監査の違いを表 2.2-1 に示す。情報セキュリティ監査が自己点検と異なる点は、情報セキュリティ監査は独立性を有する者が実施するが、自己点検は職員等が自ら実施する点である。

表 2.2-1 自己点検と情報セキュリティ監査の違い

	自己点検 （統一基準 遵守事項 2.3.1）	情報セキュリティ監査 （統一基準 遵守事項 2.3.2）
目的・趣旨	・職員等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否かを確認 ・組織全体の情報セキュリティ水準を確認	・監査対象から独立性を有する者による情報セキュリティ対策の監査を実施して、情報セキュリティ対策の実効性を担保
実施主体	・情報セキュリティ対策の体制ごとの責任者を含む職員等	・監査責任者及び監査実施者
特徴	・職員等が、自己の役割の応じた点検票の質問事項に回答	・組織（例：部局、課室等）、情報システムを対象に実施 ・監査対象から独立性を有する者による監査基準に基づく客観的な確認

なお、機関等を対象とした情報セキュリティ監査には、機関等が自ら実施する情報セキュリティ監査のほか、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（本部監査）がある。これらの違いを表 2.2-2 に示す。

表 2.2-2　機関等が自ら実施する情報セキュリティ監査と
サイバーセキュリティ戦略本部による監査との違い

	機関等が自ら実施する情報セキュリティ監査	サイバーセキュリティ戦略本部が実施する監査(※)
監査の位置付け	内部監査（機関等の情報セキュリティポリシー等に基づく監査）	外部監査（サイバーセキュリティ基本法に基づく監査）
特徴	・機関等の特有の課題やリスク等に応じて、監査テーマの設定や監査対象を限定した監査の実施が可能 ・組織全体を網羅的に実施することが可能 ・遵守事項 2.3.2(2)(a)、基本対策事項 2.3.2(2)-2 で実施が必須となっている監査項目以外も含めて実施することは妨げていない（例：脆弱性診断やペネトレーションテスト等）	・サイバーセキュリティに関する情勢等を踏まえ監査テーマ選定 ・助言型監査を志向 ・第三者的視点からの監査を実施 ・統一基準群等に基づく施策の取組状況等の検証、各政府機関のポリシー等において定めたサイバーセキュリティ対策の検証等をする「マネジメント監査」と、機関等の情報システムに対して疑似的な攻撃を実施することによって、サイバーセキュリティ対策の状況を検証する「ペネトレーションテスト」を実施

※　サイバーセキュリティ対策を強化するための監査に係る基本方針(平成 27 年 5 月 25 日 サイバーセキュリティ戦略本部決定)において、サイバーセキュリティ戦略本部の監査事務は内閣サイバーセキュリティセンター（NISC）が実施することとされている。独立行政法人及び指定法人における監査事務の一部については独立行政法人情報処理推進機構に委託して実施させることとされている。

統一基準に沿った情報セキュリティ監査の全体像を、図 2.2-2「監査業務の全体像」に示す。全体像では、監査を進めるフェーズと監査に係る者を明示し、体制の整備から対策の見直しのぞれぞれのフェーズにおける監査の実施項目を記載している。なお、この図には、統一基準に記載がある項目を記載しているが、情報セキュリティ監査において実施が必要な項目については、「第 3 部　情報セキュリティ監査の具体的な実施手順及び実施内容」に項目を追加して説明している。

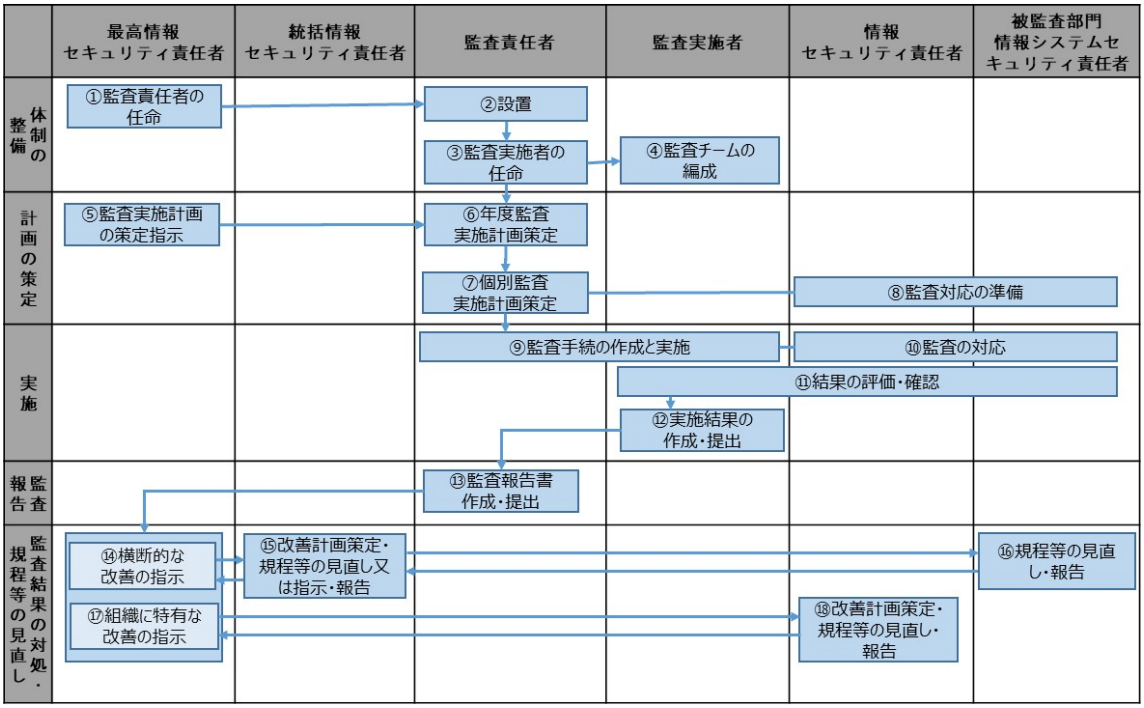

図 2.2-2　監査業務の全体像

2.2. 情報セキュリティ監査の全般的な留意点

統一基準に基づき、機関等が実施する情報セキュリティ監査の主な留意点を示す。

(1) 監査の実施にあたり、監査の実施内容毎に監査における判断基準を定める。(第 2 部「2.1. 統一基準における情報セキュリティ監査の位置付け」を参照)

(2) 対策推進計画に基づき監査実施計画を作成し、監査方針、監査対象、監査内容等を機関等内で合意する。

(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考慮する。

① 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、機関等内から広く選定することとし、任期を決める。(任期は、機関等で決める)

② 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、独立性を配慮する。

③ 監査責任者及び監査実施者は、機関等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。

④ 監査実施者には、独立性の観点から自らが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。

⑤ 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。

⑥　必要に応じて、監査業務の外部委託の活用を併せて検討する。

(5) 監査を実施する上で、監査実施者は以下の事項に留意する。

①　資料入手

(a) 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ことについて、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。

(b) 監査対象の組織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、相互に矛盾の有無、また、異常性を示す兆候がないことを評価する。

(c) 監査実施者は、サーバ又は機器等の設定状況の確認や監査証拠を入手することによる通常業務への影響を考慮する。また、監査実施者が、サーバや機器等を直接操作はしないように注意する。

②　監査証拠

(a) 監査における判断基準に対する適合、不適合の判断では、監査証拠が重要である。そのために、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。

(b) 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、監査対象の組織への質問、別途文書の査閲、実際に行っている作業の観察(視察)、自らが行う再実施等により必要な監査証拠を入手する。

(c) 現地視察、実機での設定確認、記録等の資料確認等の客観的に判断できる証拠が望ましいが、ヒアリングのみで判断が必要となる場合が多々ある。そのような場合、過年度の監査結果、他の機関等での指摘事項の事例、一般的な情報セキュリティインシデント事例等を踏まえ、リスクが高いと考える監査項目における詳細なヒアリングを行うことが考えられる。

③　監査過程

(a) 監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を監査実施において実施してはならない。

(b) 原因によって改善に向けた助言も全く違うものとなるため、監査では原因が何であるか丁寧にヒアリングをして把握する。

④　評価の判断

(a) 監査における判断基準を基に不適合と判断する監査項目があった場合、機関等の固有の事情で対策を講じる必要がないと判断する場合もあり、その妥当性を確認する。

(b) 該当する運用が存在しないため、手続を整備していない（例：例外措置や機関等支給外端末）等を理由として適合と判断する際、機関等の体制や運用変更によっ

て運用が行われる可能性も否定できないため、規程・手順や手続の整備が本当に不要であることを確認する。

(c) 情報セキュリティ関係規程を基に不適合と判断した理由が、

・情報セキュリティ関係規程の周知が不十分であった

・情報セキュリティ関係規程を無視していた

・ルールが実態に合わないものであった

・単純なミス

・情報セキュリティ関係規程が実は存在していない又は曖昧であった

等、原因によって対策が異なる。不適合を発見した際、深掘りして真の原因を明らかにする必要がある。

⑤　リスクの把握

(a) 情報セキュリティ関係規程を基に不適合と判断したことによって、どのようなリスクがあるかを把握することも重要である。情報セキュリティ関係規程に従うことでリスクを軽減できるという説明が合理的なものでなくてはならない。

(b) 情報セキュリティ関係規程を基に不適合と判断した場合でも、リスクが存在しないのであれば、その情報セキュリティ関係規程自体が適切なものであるか検討する必要がある。ただし、統一基準の遵守事項や基本対策事項に示す内容は、遵守しないとリスクがあるから遵守を求めているものであることに留意する。

(6) 監査調書又は監査報告書を含む監査関連文書は、機関等内の文書管理規程及び監査の重要性等に十分考慮し、情報の格付を実施する等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。

第 3 部 情報セキュリティ監査の具体的な実施手順及び実施内容

第 2 部 図 2.2-2「監査業務の全体像」に示した情報セキュリティ監査の各実施項目に関して、情報セキュリティ監査の具体的な実施手順（以下「監査実施手順」という。）に展開し、監査実施手順に関する実施内容を記載する。本書で例示する監査計画書、監査報告書及び調書等のひな形を付録に示す。

なお、監査実施手順ごとに、以下の事項を記載している。

【実施すべき事項】は、監査責任者、監査実施者が各監査実施手順で実施する概要を記載している。

【統一基準との関係】は、監査実施手順に関連する統一基準又はガイドラインの番号を記載している。

【監査業務の全体像（第 2 部 図 2.2-2）との関係】は、第 2 部 図 2.2-2 に記載した監査業務の全体像で該当する実施項目との関連を示す。

【実施内容】は、各監査実施手順における実施内容及び様式等の実施サンプル等を示している。なお、実施の参考となる例については、実際の情報セキュリティ監査の際の参考のものであり、機関等で適宜、修正することを想定している。

1. 準備及び体制の構築

1.1. 監査責任者の任命と役割の確定

【実施すべき事項】

監査責任者の設置、監査責任者の役割を明確にする。

【統一基準との関係】

統一基準　　遵守事項　　2.1.1(3)

ガイドライン基本対策事項　2.1.1(3)-1

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

① 監査責任者の任命

② 設置

【実施内容】

(1) 最高情報セキュリティ責任者は、情報セキュリティ監査に関する事務を統括する監査責任者を置く。監査に関する事務の統括に当たっては、独立性を確保するため、偏向を排し、常に公正かつ客観的な判断に努めることに留意して、情報セキュリティ監査責任者を置く必要がある。

(2) 監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。機関等で対象の情報システムが多い場合には、必要に応じて年度監査実施計画を策定することもある。

(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査閲(ドキュメントのレビュー)等のプロセスを通じて、監査の進捗状況、監査手続の実施状況、監査調書の作成状況等の監査業務を管理し、信頼性及び有効性に問題がないことを確認する。

1.2. 監査実施体制の確立及び監査実施者の選任

【実施すべき事項】

監査責任者は、情報セキュリティ監査の実施体制を確立し、監査実施者の負荷、監査遂行能力、独立性を考慮して監査実施者を選任し、必要に応じて外部事業者の利用を検討する。

【統一基準との関係】

統一基準	遵守事項	2.3.2(1)(a)
	遵守事項	2.3.2(2)(a)
ガイドライン	基本対策事項	2.3.2(1)-1
	基本対策事項	2.3.2(1)-2
	基本対策事項	2.3.2(2)-1

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

③監査実施者の任命

④監査チームの編成

【実施内容】

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を機関等内から選任し、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機関等内の各部局からメンバーを選任する。監査責任者は、必要に応じて監査実施者に対する兼務発令や業務指示を行う。

(3) 監査責任者は、必要に応じて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。監査チームの編成に当たって、監査実施者の負荷、役割分担等を考慮するとともに、監査実施者の独立性にも注意する。

(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の情報システムの詳細情報を有する組織、機関等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、機関等内に監査実施者が不足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。

(7) 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、機関等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。

(8) 監査責任者は、外部委託をする場合、委託先の選定にあたり、監査対象の組織との独立性を考慮する。また、経済産業省が定める「情報セキュリティサービス審査登録制度」の「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）に登録されている事業者等を参考に、監査遂行能力を有している外部事業者を選択することも考えられる。また、ペネトレーションテストや脆弱性診断については、「情報セキュリティサービス基準適合サービスリスト」（うち脆弱性診断サービスに係る部分）登録されている事業者等を参考に、監査遂行能力を有している外部事業者を選択することも考えられる。

2. 監査実施計画の策定

遵守事項 2.3.2(1)(a)に示すとおり、監査責任者が、対策推進計画に基づき監査実施計画を策定する。

ガイドラインの解説『遵守事項 2.3.2(1)(a)「対策推進計画に基づき監査実施計画を定める」について』では、対策推進計画には、監査の基本的な方針として、

・重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にする）
・監査の実施時期
・監査業務の管理体制

等の簡潔な記載を想定するとともに、対策推進計画に基づき、個別の監査実施計画を策定することが示されている。

機関等における情報セキュリティ監査では、それぞれの機関等が保有する情報システム数、情報セキュリティ監査の実施体制等を踏まえて、中長期監査実施計画、年度監査実施計画、個別監査実施計画を定めることが考えられる。

中長期監査実施計画は、機関等が運用・管理する情報システム数が多数ある場合等には、同一の重視する監査テーマ等に基づき、複数年の計画により横断的に情報セキュリティ監査を実施することで、機関等全体の評価を目的として策定することが考えられる。また、年度監査実施計画は、複数の業務、部署、情報システムを監査対象とした全体の計画を策定し、個別監査実施計画には、それぞれの監査対象ごとに策定することが考えられる。

なお、現状では、複数の業務、部署、情報システムを一つの個別監査実施計画にまとめた上で監査を実施している傾向が多い。

2.1. 中長期監査実施計画 （実施が望まれる事項）

2.1.1. 中長期監査実施計画の策定

【実施すべき事項】

監査責任者は、中長期監査実施計画を策定する場合は、機関等の情報システムの状況や情報セキュリティを取り巻く状況、監査リソース等を勘案して、中長期監査実施計画を策定する。

【統一基準との関係】

特になし

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

特になし

【実施内容】

一般的に、機関等には複数の情報システムがある。また、それら情報システムの抱えるリスクや、システムの更改のタイミング等もシステムごとに様々であるほか、監査実施のための要員や予算等といった制約もある。情報セキュリティ対策の運用状況の監査を実施する際には、このような機関等の情報システムの状況や情報セキュリティを取り巻く状況、監査リソース等を踏まえて、中長期的な視野に立って、同一の重視する監査テーマ等に基づき、監査のサイクルや順序、優先度付け等を検討する必要が出てくる場合がある。

統一基準には、中長期監査実施計画の策定に関する規程はないが、必要に応じて、対策推進計画に基づき、機関等で複数年を見据えた中長期監査計画を策定し、その下で年度ごとに年度監査実施計画を策定することが考えられる。中長期監査実施計画を策定する場合、監査責任者は、以下の項目を記載した中長期監査実施計画を策定することが望ましい。

・中長期監査方針
・実施目標
・監査対象
・監査実施内容
・監査スケジュール
・監査リソース　（監査人の確保、予算の確保）

2.2. 年度監査実施計画

2.2.1. 年度監査実施計画の策定

【実施すべき事項】

最高情報セキュリティ責任者の指示により、監査責任者は、対策推進計画に基づき監査の目的、監査の対象、監査の方法、監査の実施体制、監査の実施時期等を記載した年度監査実施計画を作成する。

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、監査対象、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もできる。

【統一基準との関係】

統一基準	遵守事項	2.1.1(3)(a)
		2.3.2(1)(a)
ガイドライン	基本対策事項	2.1.1(3)-1
		2.3.2(1)-1
		2.3.2(1)-2

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑤ 監査実施計画の策定指示

⑥ 年度監査実施計画策定

【実施内容】

(1) 監査責任者は、年度末までに、翌年度の年度監査実施計画を策定する。（策定期日については、機関等で決定する）

(2) 監査責任者は、年度監査実施計画の策定にあたり、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、機関等を取り巻く環境を概括的に把握し、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。

(3) 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。

(4) 中長期監査実施計画を策定している場合は、当該中長期監査実施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。

(5) 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。

(6) 監査責任者は、年度監査実施計画に以下の事項等を記載する。

- 監査方針
- 機関等の概要
- 情報セキュリティに関連する動向（情報セキュリティに関する法令等の施行、機関等がサイバー攻撃を受けるようなイベント情報、サイバー攻撃の動向、サイバーセキュリティのインシデント状況等）
- 過去の監査の内容と指摘事項
- 監査対象（対象となる組織、業務、情報システム等）、監査項目及び監査目標（例えば、機密性、情外部事業者による監査及び外部専門家の活用の必要性及び範囲
- 報漏えい防止、不正アクセス防止等）
- 監査スケジュール

・監査業務の管理体制
・外部事業者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）

様式例１に年度監査実施計画の例を示す。

様式例１　年度監査実施計画の例

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、「政府機関等のサイバー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について監査する。

機関等の対策基準の統一基準群への準拠性、運用規程及び実施手順の機関等の対策基準への準拠性及び実際の運用の運用規程及び実施手順への準拠性を評価し、当該評価結果に基づく指摘事項に関して発見事項への助言を行う。

２．機関等の概要

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
機関等の対策基準、運用規程及び実施手順	（ア）機関等の対策基準に統一基準を満たすための事項が定められていること （イ）運用規程及び実施手順が機関等の対策基準に準拠していること （ウ）実際の運用が機関等の対策基準、運用規程及び実施手順に準拠していること	・機関等の対策基準の統一基準群への準拠性 ・運用規程及び実施手順の機関等の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
機関等の LAN	機関等の 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情報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．外部事業者による監査の範囲及び必要性

(1) 外部事業者の範囲及び必要性

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情報セキュリティ設定の監査

② 必要性

脆弱性診断、ペネトレーション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）

●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	機関等の対策基準、運用規程及び実施手順	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												
	機関等内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	全職員等	△△△△
・・・				
・・・				
・・・				

2.3.個別監査実施計画

2.3.1.個別監査実施計画の策定

【実施すべき事項】

監査責任者は、対策推進計画に基づいて監査の方針、目的、監査の対象や監査項目、監査の実施方法、監査の実施体制、監査の実施時期を記載した個別監査実施計画を作成する。

情報システムの数が多い場合は、個別監査実施計画を情報システム単位で策定することも検討する。

【統一基準との関係】

統一基準	遵守事項	2.3.2(1)(a)
ガイドライン	基本対策事項	2.3.2(1)-1
		2.3.2(1)-2

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑦ 個別監査実施計画策定

【実施内容】

監査責任者は、対策推進計画に基づいて監査対象ごとに個別監査実施計画書を作成する。作成に当たっては、監査手続を実施できるように十分検討する。

(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て、監査対象ごとに個別監査実施計画を策定する。

(2) 監査責任者は、機関等の対策基準等の内容確認を行った上で、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、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。

(3) 監査責任者は、監査手続の作成のために、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、精査により整備状況を確かめる。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、監査証拠を入手し、試査（母集団から一部のサンプルを抽出する方法）により確かめる。

(4) 情報システムや情報セキュリティについて、知見の少ない職員が情報セキュリティ監査の担当者となる場合がある。このような場合においては、当該職員に代わり、情報セキュリティ対策推進体制や情報システムの管理を担当する職員が監査を実施することも考えられる。ただし、監査を実施する職員は、監査の独立性を確保するために、自らが担当する業務・情報システムの監査には携わらないよう留意する必要がある。

(5) 監査責任者は、個別監査実施計画に以下の事項等を記載する。

・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（対象となる組織、情報システム、業務等）
・監査対象の組織及びその責任者

・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
・監査項目及び監査手続
・監査の進捗管理手段
・外部事業者との役割分担（外部委託を行う場合）

様式例 2 に個別監査実施計画の記載例を示す。

様式例 2　個別監査施計画書例

作成日：〇〇年〇〇月〇〇日

（情報セキュリティ監査責任者）
氏　　名

〇〇年度　機関等の対策基準、運用規程及び実施手順に関する個別監査実施計画書

１．監査目的

機関等の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、「政府機関等のサイバー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、発見事項への助言を行う。

２．背景

令和●年に統一基準群が改定され、機関等でも従来の情報セキュリティポリシーを改定し、新たに機関等の対策基準を策定した。情報セキュリティポリシーの改定を踏まえ、また、昨今サイバーセキュリティに関するリスクが一層高まっていることも考慮しながら、機関等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：機関等の対策基準、運用規程及び実施手順

４．監査対象の組織及び責任者：大臣官房〇〇課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：10月1日～11月30日の各月末の週（計15日間）

７．監査の実施場所：当機関等内執務室

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）機関等の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
機関等の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査閲等することにより、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）運用規程及び実施手順が機関等の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
運用規程及び実施手順の機関等の対策基準への準拠性※	運用規程及び実施手順を査閲等することにより、機関等の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）実際の運用が機関等の対策基準、運用規程及び実施手順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
課室情報セキュリティ責任者の設置	体制図等を査閲等することにより、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査閲等することにより、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．・・・

2.3.2. 個別監査実施計画の通知

【実施すべき事項】

監査対象の組織の準備があるため、監査責任者は、個別監査実施計画を作成後、個別監査実施計画のうち監査対象、監査の実施時期、監査実施者を監査対象の組織に事前に通知する。

【統一基準との関係】

外部事業者による監査及び外部専門家の活用の必要性及び範囲

統一基準　　遵守事項　　2.3.2(1)(a)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑦ 個別監査実施計画策定

【実施内容】

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以下の内容について、監査対象の組織に事前に通知する。

・監査対象

・監査の実施時期及び監査基準日

・当該監査対象の組織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あらかじめ講じられる等によって、監査の有効性を阻害してしまうことがあるので、注意が必要である。

2.3.3. 年度監査実施計画と個別監査実施計画の統合

【実施すべき事項】

年度監査実施計画と個別監査実施計画は相互に関係するため、監査の内容、個別監査の対象数等を考慮して、統合して策定することも可能とする。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(1)(a)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑥ 年度監査実施計画策定

⑦ 個別監査実施計画策定

【実施内容】

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、監査対

象の組織が１つの場合や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。

2.3.4. 年度監査実施計画及び個別監査実施計画の修正

【実施すべき事項】

監査責任者は、情報セキュリティインシデントの発生、新しい情報システムの運用開始、情報セキュリティの状況の変化等に応じて実施計画の修正が必要と判断した場合、年度監査実施計画及び個別監査実施計画を修正する。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(1)(b)

【監査業務の全体像（第２部 図 2.2-2）との関係】

⑥ 年度監査実施計画策定

⑦ 個別監査実施計画策定

【実施内容】

監査責任者は、

(1) 情報セキュリティインシデントの発生

(2) 情報セキュリティ対策の実施内容に大きな変更

・新しい情報システムの運用開始

・機関等の大きな人事異動又は組織の改編

・機関等の対策基準の改定又は追加

等が生じた場合、必要に応じて監査の実施内容に追加することを検討し、監査計画を修正し、追加の監査を監査実施者に指示する。

3. 監査の実施

3.1. 監査の実施の指示

【実施すべき事項】

監査責任者は、監査実施者に監査の実施を指示する。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(2)(a)

【監査業務の全体像（第２部 図 2.2-2）との関係】

⑨ 監査手続の作成と実施

【実施内容】

監査責任者は、監査実施計画に基づき、監査実施者に監査の実施を指示する。

3.2. 監査手続の作成と実施

【実施すべき事項】

本書が対象とする監査を実施する監査手続を作成し、監査を実施する。

【統一基準との関係】

統一基準	遵守事項	2.3.2(2)(a)
ガイドライン	基本対策事項	2.3.2(2)-2

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑨ 監査手続の作成と監査の実施

【実施内容】

ガイドラインの基本対策事項 2.3.2(2)-2 では、以下の監査の実施を必須としている。

(1) 機関等の対策基準について、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

(2) 機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していること

(3) 監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程（対策基準、運用規程及び実施手順）に準拠していること

以下に、上記(1)～(3)の監査の監査手続の作成と実施及びその注意点を示す。

3.2.1. 機関等の対策基準について、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に関する監査

(1) 実施する監査の概要

統一基準には情報セキュリティ対策の項目ごとに機関等が遵守すべき遵守事項を規定している。また、ガイドラインにおいて、統一基準の遵守事項を満たすためにとるべき基本対策事項を例示している。

以上を踏まえ、機関等は、遵守事項を満たし、基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより対応する遵守事項を満たす必要がある（統一基準　第 1 部 1.1(5) 機関等の対策基準)。

「機関等の対策基準について、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に関する監査」では、機関等の対策基準が統一基準を満たすための適切な事項が定められているか否かを判断することが監査の評価となり、機関等における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性等を踏まえ、必要な事項が対策基準に盛り込まれていることを確認する必要がある。

特に、上記に示した「基本対策事項に例示される対策又はこれと同等以上の対策を講じること」については、対策基準を策定する際に以下の対応を機関等で行われることが考えられるため、監査実施時に考慮する必要がある。

・対策基準に基本対策事項で定められている内容を規定（一部のみ規定を含む）
・運用規程及び実施手順に基本対策事項で定められている内容を規定（一部のみ規定を含む）
・対策基準、運用規程及び実施手順に基本対策事項で定められている内容を規定（上記の２パターンの混合）
・対策基準において、ガイドラインに準拠するためガイドラインを参照と規定

このため、基本対策事項の取扱いについては、対策基準改定時や監査の作業効率化の観点等による改定の際には、対策基準の策定に当たって、対策基準に各事項を取り入れた理由やガイドラインの基本対策事項との関係等について記録がある場合はその記録を確認し、記録がない場合には監査実施時に確認する必要がある。

なお、統一基準の構成と全く異なる体系の対策基準が策定されている場合には、対策基準、遵守事項及び基本対策事項との関係性に関する記録が重要となるため留意する必要がある。

更に、基本対策事項を対策基準で規定する場合には、例示される対策事項について、表 3.3-1 の表現を使用している。

基本対策事項を対策基準に含めた際には、下記の解釈を正しく理解した上で策定ことも重要であり、解釈が間違っている場合、統一基準を満たすための適切な事項が対策基準に定められていない可能があるため、当該監査では下記の記載へ注意することが必要である。

表3.3-1　基本対策事項の記載における検証のポイント

No.	基本対策事項の 個別対策事項の記載	分類	検証する際のポイント
①	「～以下を例とする･･･」	例示	・基本対策事項にて示されている例示のうち、いずれかの対策を実施しているか。 ・例示以外の対策を実施している場合、その対策は例示している対策と同等以上であると判断できるか。
②	「～以下を全て含む･･･」	包含	・基本対策事項にて示されている項目が全て実施されているか（含まれているか）。 ・含まれていない場合、その対策は示されている対策と同等以上であると判断できるか。
③	上記①②に該当し「･･･すること」	遵守	・基本対策事項にて示されている対策を実施しているか。 ・記載以外の対策を実施している場合、その対策は記載している対策と同等以上であると判断できるか。
④	「～の場合に、･･･」 「～のとき」	条件	・基本対策事項にて示されている条件に該当するか。 ・該当する場合、記載内容が上記①～③の該当する分類にて検証する。
⑤	「～に努めること」	努力目標	・基本的には個別対策事項の記載が、上記①～③の該当する分類にて検証する。 ・対策が実施されていない場合、または同等の対策と判断できない場合は、一律に不十分とは判断せず、個別の事情を考慮する。

(2) 監査手続の実施

機関等の対策基準について、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を確認する。監査手続としては、遵守事項を監査における判断基準として、以下の事項が満たされていることを確認する。

① 統一基準の遵守事項に基づいて対策基準で定める対策事項が網羅的に規定されていること

② 各項目で規定された対策について、機関等における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性等を踏まえ、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

③ 各項目の達成レベルが十分であること

②を確認する際は、ガイドラインの基本対策事項及び解説の記載を参照し、表 3.3-1 に示す基本対策事項の対応方法に応じて確認する必要がある。

監査の評価方法は、統一基準の遵守事項と対策基準、運用規程又は実施手順の各ドキュメントを対象に、査閲(ドキュメントのレビュー)により確認する。また、ガイドラインの基本対策事項及び解説を確認し、対策基準が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を確認する。

(3) 注意点

遵守事項又は基本対策事項において、「以下を全て含む」（全ての項目の実施を求めるもの）として列挙されている事項に対して、「以下を例とする」（いずれか１項目以上の実施を求めるもの）と規定した場合、同等以上の対策を定めていると評価できないので、評価の際に注意が必要である。

また、基本対策事項の「以下を例に」として列挙されている事項に対して、「以下を全て含む」と規定した場合、実際の運用に対して、統一基準が求めている以上の対策が求められることになり、達成できない対策が求められる可能性があるため、評価の際に注意が必要である。

3.2.2. 機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していることに関する監査

(1) 実施する監査の概要

整備する運用規程及び実施手順等をガイドラインの「付録（3）統一基準群で整備を求めている運用規程及び実施手順等」で整理している。「機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していることに関する監査」では、機関等で整備している運用規程及び実施手順又は機関等で追加して整備した運用規程及び実施手順等が、対策基準に準拠していることを確認する。

(2) 監査手続の実施

運用規程及び実施手順には、必要な事項、手順、手続等が記載され、対策基準から逸脱がないことを確認する。監査手続としては、運用規程及び実施手順の各項目を監査における判断基準として、対策基準から必要な事項、手順、手続の逸脱がなく、準拠していることを確認する。また、基本対策事項において、運用規程及び実施手順で規定すべき内容が定められているものがあるため、ガイドラインの基本対策事項を参考に、運用規程及び実施手順の項目を確認する必要がある。

監査の評価方法としては、対策基準、運用規程及び実施手順の各ドキュメントを対象に、査閲(ドキュメントのレビュー)により確認する。

(3) 注意点

表 3.3-1 に示すように、基本対策事項において「以下を全て含む」（全ての項目の実施を求めるもの）として列挙されている事項に対して、「以下を例とする」（いずれか１項目以上の実施を求めるもの）と規定した場合、同等以上の対策を定めていると評価できないので、評価の際に注意が必要である。

また、基本対策事項において「以下を例に」として列挙されている事項に対して、「以下を全て含む」と規定した場合、実際の運用に対して、統一基準が求めている以上の対策が求められることになり、達成できない対策が求められる可能性があるため、評価の際に注意が必要である。

この他、許可権限者等が異なる等、対策基準の規程と相違する内容や矛盾が無いように、運用規程及び実施手順が定められていることを確認する必要がある。

3.2.3. 監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していることに関する監査

(1) 実施する監査の概要

機関等では、策定された情報セキュリティ関係規程に則って情報セキュリティの対策が実施されている。そのため、監査対象の部門における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していることを対象に監査を実施する必要がある。

当該監査では、情報セキュリティ関係規程を基に、情報セキュリティ対策の基本的枠組み、情報の取扱い、外部委託、情報システムのライフサイクル、情報システムの情報セキュリティ要件、情報システムの構成要素、情報システムの利用に関する整備や運用状況を確認する。

また、当該監査の監査対象は、機関等の組織体制、業務、取り扱っている情報や保有する情報システムに対して、監査テーマに応じて検討することとし、監査を実施する人員、日数、予算等を考慮して効果的な監査を実施することが求められる。

(2) 監査手続の作成と実施

監査対象の部門に対して、情報セキュリティ関係規程の項目を監査における判断基準として、情報セキュリティ対策に関する運用を確認する監査手続を作成する。

本監査を実施するに当たっての監査技法の例を以下に示す。監査対象や監査テーマに応じて効果的な技法を実施することで監査品質を向上できるが、監査の作業負荷に留意することが必要である。

・監査対象の組織の職員等への質問(ヒアリング)
・記録文書等の査閲(ドキュメントレビュー)
・執務室、サーバ室等の観察(視察)
・監査人自らが監査対象の組織で実施される運用を試行することによる情報セキュリティ対策の運用状況の評価（再実施）
・情報システムの脆弱性の脆弱性診断又はペネトレーションテスト

更に、必要に応じて、サーバ、端末、通信回線装置等の機器、クラウド環境を含む情報システムの情報セキュリティに関する設定情報の確認、ログ出力状況の確認等考えられる。

監査手続の様式に記載する項目の例を以下に示す。

・「対策基準」には、監査の評価に使用した情報セキュリティ関係規程の項番を記載する。
・「監査項目」には、情報セキュリティ関係規程の項番に対応する監査項目を記載する。
・「監査手続」には、実際の運用の準拠性を確認するための監査手続を記載する。
・「発見事項（所見)」　（監査調書作成の際に記載する。）
・「監査証拠」　（監査調書作成の際に記載する。）

監査手続の様式の例と記載例を、表 3.3-2 に示す。

表3.3-2　監査対象の部門における実際の運用が情報セキュリティ関係規程に準拠していることに関する監査手続の記載例

対策基準	監査項目	監査手続	発見事項（所見）	監査証拠
○○省情報セキュリティポリシー 2.3.1(2)(b)	職員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。	• 自己点検実施計画書及び自己点検票、実施手順書等の閲覧、職員へのヒアリングにより、自己点検が実施されていることを確認する。		
○○省情報セキュリティポリシー 2.3.2(3)(a)	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統括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指示すること。	• 情報セキュリティ対策推進体制へのヒアリング及び関係書類の閲覧により、最高情報セキュリティ責任者からの、監査報告書における指摘事項に対する改善計画の策定等の指示の有無を確認する。		

(3) 注意点

・対策基準が遵守事項を満たすためにとるべき基本的な対策事項を定めていない場合、当該遵守事項に対応する基本対策事項を参照し、「以下を全て含む」、「以下を例とする」の記載に注意して、実際の運用が例示される対策又はこれと同等以上であることを確認する。

・監査における心証の強度を高めるためには、監査証拠は文書や資料等客観的に判断できるものが望ましい。ヒアリングのみの確認となる場合はヒアリング観点を明確にする。

・遵守事項 2.3.2(2) 「監査の実施」の項目に関して、平成 30 年度の統一基準から、自己点検は客観性が求められる監査とは別の取り組みであることから削除されたことに留意する。

・監査対象、監査範囲は、機関等の実情に応じて検討する必要があるが、以下に例を示す。

■ 情報セキュリティ対策推進体制を監査対象とした場合

➢ 最高情報セキュリティ責任者や統括情報セキュリティ責任者等が担う役割を対象に、情報セキュリティ関係規程の運用が適切に行われていることを確認する。

■ 特定の業務を監査対象とした場合

➢ 業務に関与する部門、取り扱う情報、使用する情報システムについて、業務手順の観点から情報セキュリティ関係規程の運用が適切に行われていることを確認する。

■ 特定の部門を監査対象とした場合

- 部門で取り扱う情報、利用する情報システムについて、職員等が情報セキュリティ関係規程の運用が適切に行われていることを確認する。

■ 特定の情報システムを監査対象とした場合

- 情報システムの情報セキュリティ対策について、情報セキュリティ関係規程で規定されている情報セキュリティ対策が講じられていること、及び実際に運用されていることを確認する。

■ 特定の情報セキュリティ対策を監査範囲とした場合

- 最新のサイバーセキュリティに関する脅威動向、インシデント事例、様々な情報セキュリティ技術の普及等を踏まえ、以下に示す例のように、セキュリティリスクの高い範囲に監査を限定し、複数の情報システムへ監査を同時に実施する。
  - ✧ 情報システム関連文書の整備状況
  - ✧ インターネットに接続する認証機能での多要素認証の導入
  - ✧ アクセス制御機能の適切な運用
  - ✧ 管理者権限を持つ主体の識別コード及び主体認証情報に関する管理
  - ✧ ソフトウェアに関する脆弱性対策の実施
  - ✧ 情報システムの情報セキュリティに影響する各種設定情報
  - ✧ 不正アクセスへの対策状況

3.3. 監査調書の作成

【実施すべき事項】

監査を実施した事実を監査調書としてまとめる。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(2)(a)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑨ 監査手続の作成と監査の実施

【実施内容】

監査実施者が、監査調書を作成方法、記載事項、調書作成上の注意点を以下に示す。

(1) 監査実施者は、実施した監査手続の結果と、監査手続に関連して入手した資料、監査の結論に至った経過を監査調書として作成し、情報漏えいや紛失等を考慮し、適切に保管しなければならない。

(2) 監査調書は、監査実施者が行っ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べき監査証拠、その他関連資料等を綴り込んだものである。監査実施者自身が直

接、入手した資料や監査した結果だけでなく、監査対象の組織から提出された資料等を含み、監査対象の組織以外の第三者から入手した資料等を含むことがある。

(3) 監査実施者は、監査手続を変更又は追加した場合には、変更又は追加した監査手続、入手した監査証拠、監査結果についても、監査調書に記載又は追記する必要がある。

(4) 監査調書の作成に当たっては、正確かつ漏れなく必要な事項を綴り込まなければならない。また、監査実施者が監査の結論に至った経過が理路整然と分かるように記載しなければならない。

(5) 監査調書は、主に監査意見の根拠とするために作成されるが、次回以降の監査を合理的、効率的に実施するための資料として役立つ。更に、監査実施者が正当な注意を払って監査業務を遂行したことの証跡となることがある。

実際に、監査調書は監査を実施した根拠となる調書を作成することになる。本書が対象とする監査には、以下の 3 つの監査があり、それぞれの監査について、監査調書を作成する。

① 機関等の対策基準について、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

② 機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していること

③ 監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していること

監査調書に記載する項目と様式の例を、以下に示す。

(a)「機関等の対策基準について、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」に関する監査の場合

・「統一基準」には、監査の基準となる統一基準の項番と監査項目を記載する。

・「対策基準」には、統一基準の監査項目に対応する対策基準の該当する項番と項目を記載する。

・「発見事項(所見)」には、監査の基準と監査対象の該当項目の準拠性を監査した監査結果として、その発見事項又は所見を記載する。

監査調書の様式の例と記載例を表 3.3-3 に示す。

表3.3-3　機関等の対策基準について、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に関する監査調書の例

統一基準	対策基準	発見事項（所見）
2.1.1 組織・体制の整備 (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置 (a) 機関等は、機関等における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者１人を置くこと。	○○省情報セキュリティポリシー 2.1.1 組織・体制の整備 (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置 (a) △△を、○○省における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者とする。	• 特になし
(b) 機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置くこと。	（該当する記載無し）	• 統一基準に該当する事項が○○省情報セキュリティポリシーに記載されていないが、情報セキュリティ対策推進体制へのヒアリングにより、○○省では最高情報セキュリティ副責任者は組織として不要と判断し、設置していないことを確認した。

(b)「機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していること」に関する監査の場合

・「対策基準」には、監査の基準となる対策基準の項番と監査項目を記載する。

・「運用規程・実施手順」には、対策基準の監査項目に対応する機関等で策定した手順書、実施要領、マニュアル等の該当項目を記載する。

・「発見事項(所見)」には、対策基準と運用規程及び実施手順の準拠性を監査した監査結果として、その発見事項又は所見を記載する。

監査調書の様式の例と記載例を表 3.3-4 に示す。

表 3.3-4　機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していることに関する監査調書の例

対策基準	運用規程・実施手順	発見事項（所見）
○○省情報セキュリティポリシー 2.2.2 (1)　例外措置手続の整備 2.2.2(1)-1 最高情報セキュリティ責任者は、例外措置について以下を含む手順を定めること。 a) 例外措置の許可権限者 b) 事前申請の原則その他の申請方法 c) 審査項目その他の審査方法 ・ 申請者の情報（氏名、所属、連絡先） ・ 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等） ・ 例外措置の適用を申請する期間 ・ 例外措置の適用を申請する措置内容（講ずる代替手段等） ・ 例外措置により生じる情報セキュリティ上の影響と対処方法 ・ 例外措置の適用を終了した旨の報告方法 ・ 例外措置の適用を申請する理由	○○省情報セキュリティポリシー例外措置手続き要領	・ ○○省情報セキュリティポリシー例外措置手続き要領書の閲覧により、対策基準基本対策事項で策定することが求められている実施事項及び実施手順が定められていることを確認した。

(c)「監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していること」に関する監査の場合

監査手続に記載する項目の例を以下に示す。

・「対策基準」には、監査の基準となる対策基準の項番を記載する。
・「監査項目」には、対策基準の項番に対応する監査項目を記載する。
・「監査手続」には、実際の運用の準拠性を関するための監査手続を記載する。
・「発見事項（所見)」には、監査手続を実施し、監査結果としてその発見事項又は所見を記載する。
・「監査証拠」には、監査手続を実施する際に使用した対策基準に関連し、かつ、検証できる記録、事実の記述又はその他の情報を記載する。

監査調書の様式の例と記載例を表3.3-5に示す。

表3.3-5　監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していることに関する監査調書の例

対策基準	監査項目	監査手続	発見事項（所見）	監査証拠
○○省情報セキュリティポリシー 6.1.1(1)(a)	情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。	• 当該情報システムの設計書、運用手順書等の閲覧により、ユーザの識別方式及びユーザ認証方式が実装されていることを確認する。	• 運用手順書の閲覧により、 ➢ 利用者毎に固有のユーザIDを発行している。 ➢ システムへのログイン時に、パスワードの入力を求めている。 ことを確認した。	• ○○システム運用手順書
○○省情報セキュリティポリシー 6.1.1(2)-6	情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	• 当該情報システムの設計書、運用手順書等の閲覧および被監査の情報システム担当へのヒアリングにより、 ➢ 共用識別コードの有無 共用識別コードがある場合、 ➢ 利用者を特定できる仕組みの有無 ➢ 共用識別コードの取り扱いに関する規程の整備状況 について確認する。	• 設計書及び運用手順書の閲覧、被監査の情報システム担当へのヒアリングにより、 ➢ 当該情報システムの運用・保守用に、共用識別コードを使用している。 しかしながら、 ➢ **利用者を特定できる仕組みが講じられていない。** ➢ **共用識別コードの取り扱いに関する規程が整備されていない。** ことを確認した。**→NG**	• ○○システム設計書 • ○○システム運用手順書

3.4. 監査の実施結果の評価

【実施すべき事項】

監査を実施した結果をともに評価し、発見事項及び優れた取組（以下、「グッドプラクティス」という。）をまとめる。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(2)(a)

【監査業務の全体像（第2部 図2.2-2）との関係】

⑪ 結果の評価・確認

【実施内容】

(1) 監査の評価結果

① 「機関等の対策基準について、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」に関する評価

監査実施者は、遵守事項及び基本対策事項と対策基準の間に、矛盾、相違点、不足がある場合は、発見事項としてまとめる。その原因、問題点、重要性を検討し、評価する。また、対策基準が、遵守事項及び基本対策事項の基準を上回ると評価できた場合は、グッドプラクティスとしてまとめる。

② 「機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していること」に関する評価

監査実施者は、運用規程及び実施手順と対策基準の間に、矛盾、相違点、不足がある場合は、発見事項としてまとめる。その原因、問題点、重要性を検討し、評価する。また、運用規程及び実施手順が、遵守事項及び基本対策事項の基準を上回ると評価できた場合は、グッドプラクティスとしてまとめる。

③ 「監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していること」に関する評価

監査実施者は、監査対象の組織で実施されている情報セキュリティの対策の実施状況、運用状況が、対策基準、運用規程及び実施手順との間に矛盾、相違点、不足がある場合は、発見事項としてまとめる。その原因、問題点、重要性を検討し、評価する。また、情報セキュリティの対策の実施状況、運用状況が、対策基準、運用規程及び実施手順の基準を上回ると評価できた場合は、グッドプラクティスとしてまとめる。

(2) 発見事項の評価

監査の所見の例として、統一基準の遵守事項が守られために改善が必要な「指摘事項」、統一基準の遵守事項は守られているが改善の余地がある「推奨事項」のように、発見事項に対する重要度において監査所見の重要度を評価する。

指摘事項としては、

・対策基準に、統一基準の遵守事項を満たす事項が定められていない
・運用規程及び実施手順に、対策基準の項目を満たす事項が定められていない
・監査対象の組織での運用状況が情報セキュリティ関係規程に準拠していない

等の理由がある。

また、推奨事項に挙げられる項目としては、

・監査対象の組織の運用状況において、情報セキュリティ関係規程に違反していると即時に評価できるものではないが、改善が必要と判断する

等の理由がある。

(3) 発見事項への助言

① 監査責任者は、発見事項への助言の記載に際して、機関等の対策基準やその他の基準等の監査の基準に基に発見された課題及び問題点について指摘し、発見事項への助言を行う。また、助言型監査の場合、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。

② 監査対象の組織の状況を考慮した上で、情報セキュリティに関するリスクが存在し、リスクを軽減するための改善指示が監査対象の組織で受け入れられるもの（改善内容が明確で、実現可能性のあるもの）である必要がある。

③ 監査対象の組織に対する改善の助言を明確なものにするため、発生した原因を徹底的に調べ上げることが必要である。特に、情報セキュリティ関係規程に起因するもの、整備した体制や仕組みが不完全であるもの等、監査対象の組織以外に起因する原因がないことを確認する点に注意する。

④ ガイドラインに示されている内容を参考に、監査対象の組織や機関等に特有のリスクがないことを確認する注意する。

(4) 発見事項の取扱い及び事実確認手続の実施

事実確認手続としては、当該発見事項に関する事実関係について、事実誤認等がないことを含め、監査対象の担当者と合意する。

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。

なお、事実確認の結果、事実誤認により発見事項の修正、取り下げが発生する場合があるが、監査手続を適切に行うため、修正、取り下げの理由及び履歴は、事実確認の記録に記載することが必要である。

3.5. 監査の実施結果等の文書化

【実施すべき事項】

監査対象等ごとに、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、監査により発見された発見事項、発見事項の評価及び発見事項のリスク、発見事項への助言を発見事項一覧としてまとめる。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(2)(a)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑫ 実施結果の作成・提出

【実施内容】

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又は推奨事項、発見事項の評価及び発見事項のリスク、発見事項への助言を発見事項一覧としてまとめ、監査責任者に報告する。

発見事項一覧の記載する項目の例を、以下に示す。

- 「発見事項区分種別」には、「指摘事項」又は「推奨事項」を記載する。併せて、発見した事項の該当する対策基準の番号を記載すると良い。
- 「監査項目」には、該当する基準の監査項目を記載する。
- 「発見事項（所見）」には、監査調書の「発見事項(所見)」の指摘事項又は推奨事項の内容を記載する。
- 「発見事項のリスク」には、指摘事項又は推奨事項となる根拠となるリスクを記載する。
- 「発見事項への助言」には、指摘事項又は推奨事項に関する改善に向けた助言を記載する。

発見事項一覧の様式の例と記載例を表 3.3-6 に示す。

表 3.3-6　発見事項一覧の記載例

発見事項					発見事項への助言
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク	
1	**指摘事項** ○○省情報セキュリティポリシー 2.3.2(3)(a)	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統括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指示すること。	• 監査結果については、情報セキュリティ監査報告書の閲覧により、最高情報セキュリティ責任者宛て報告がされていることを確認したが、最高情報セキュリティ責任者から統括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対して、指摘事項に対する改善計画の策定等を指示したことは確認できなかった。	監査結果に対して最高情報セキュリティ責任者の改善指示が欠落した場合、当該機関の改善実施の機会が失われ、情報セキュリティ対策の実効性が担保できなくなるおそれがある。	「○○省情報セキュリティ監査実施手順」X.X.X(X)項を改定して、監査報告時に必ず最高情報セキュリティ責任者からの改善指示を得ることを定めるとともに、措置結果及び改善計画の報告についても必ず実施する規定を設け、規定に従った運用を行うことが必要です。
2	**推奨事項** ○○省情報セキュリティポリシー 6.1.1(2)-6	情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	• 設計書及び運用手順書の閲覧、被監査の情報システム担当者へのヒアリングにより、 ➢当該情報システムの運用・保守用に、共用識別コードを使用している。 しかしながら、 ➢利用者を特定できる仕組みが講じられていない。 ➢共用識別コードの取り扱いに関する規程が整備されていない。 ことを確認した。	運用・保守時に利用する特権を伴う識別コードを用いたアクセス主体を特定できない場合、正規の主体へのなりすましや脆弱性を悪用した攻撃等の不正アクセス行為を特定できなくなるおそれがある。	「□□システム運用手順書」に、共用識別コードを用いる際に採るべき情報セキュリティ対策を規定し、不正アクセス行為の防止策を講じることが推奨されます。

4. 監査報告

4.1. 監査報告書の作成、提出

【実施すべき事項】

監査責任者が監査報告書を作成し、最高情報セキュリティ責任者に提出する。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(2)(a)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑬ 監査報告書作成・提出

【実施内容】

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、発見事項への助言を行い、監査対象の組織の情報セキュリティ対策の改善につなげる。監査責任者は、監査報告書を最高情報セキュリティ責任者に提出する。

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、機関等の名称を含め、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。従って、監査報告書の宛名は、当該機関等の最高情報セキュリティ責任者とする。

④ 監査責任者の記載

監査結果の報告に係る事務は、監査責任者が統括する。従って、監査報告書には、監査責任者の氏名を記載する。

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 情報セキュリティ監査の基準とした基準名等

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がある場合には、そのグッドプラクティスを含めることが望ましい。

⑨ 指摘事項等及び発見事項への助言の総括

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発見事項への助言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・重要性及び発見事項への助言を一覧表にすると理解されやすいことを考慮する。

⑩　監査人の独立性に関する事項

全ての監査実施者が監査対象範囲の業務や監査項目等から独立していることを記載する。例えば、情報システムの調達又は構築段階が監査対象の場合、監査実施者が当該調達又は構築に関与していなかったことを、また、情報システムの運用状況が監査対象の場合、監査実施者が監査対象となる時期の当該情報システムの運用に携わってなかったことを示すことが望ましい。

⑪　監査報告書の取扱い（利用及び利用者の制限事項等）

監査報告書の公開・非公開、開示範囲等の制約がある場合には記載する

様式例 3 に監査報告書の例を示す。

様式例 3 監査報告書の例

○○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）
氏　　名

○○年度　××××省情報セキュリティ監査報告書

令和○○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

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に関する準拠性の評価、運用規程及び実施手順が対策基準に準拠していることに関する準拠性の評価、監査対象の部門における実際の運用が情報セキュリティ関係規程に準拠していることに関する準拠性の評価を実施し、指摘事項に関して発見事項への助言を行うこと。

２．監査実施期間：××年××月××日から○○年○○月○○日まで

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
機関等の対策基準、運用規程及び実施手順	（ア）機関等の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）運用規程及び実施手順が機関等の対策基準に準拠していること （ウ）実際の運用が機関等の対策基準、運用規程及び実施手順に準拠していること	・機関等の対策基準の統一基準群への準拠性 ・運用規程及び実施手順の機関等の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
機関等内 LAN	機関等内 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情報セキュリティ設定の監査

４． 情報セキュリティ監査の基準とした基準名等：機関等の対策基準

５． 監査の結果

６． 指摘事項及び発見事項への助言の総括

７． 添付資料

(1) 機関等の対策基準、運用規程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、機関等における最高情報セキュリティ責任者、統括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。

添付資料の例

発見事項					発見事項への助言	改善結果/改善計画	フォローアップ結果
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1	**指摘事項** ○○省情報セキュリティポリシー 2.3.2(3)(a)	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統括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指示すること。	• 監査結果については、情報セキュリティ監査報告書の閲覧により、最高情報セキュリティ責任者宛て報告がされていることを確認したが、最高情報セキュリティ責任者から統括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対して、指摘事項に対する改善計画の策定等を指示したことは確認できなかった。	監査結果に対して最高情報セキュリティ責任者の改善指示が欠落した場合、当該機関の改善実施の機会が失われ、情報セキュリティ対策の実効性が担保できなくなるおそれがある。	「○○省情報セキュリティ監査実施手順」X.X.X(X)項を改定して、監査報告時に必ず最高情報セキュリティ責任者からの改善指示を得ることを定めるとともに、措置結果及び改善計画の報告についても必ず実施する規定を設け、規定に従った運用を行うことが必要です。	報告書の作成時点では、本項目は必要としないが、監査中に改善が完了し、監査で改善結果を確認している場合、本項目に記載する必要がある。	
2	**推奨事項** ○○省情報セキュリティポリシー 6.1.1(2)-6	情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	• 設計書及び運用手順書の閲覧、被監査の情報システム担当者へのヒアリングにより、 ➢当該情報システムの運用・保守用に、共用識別コードを使用している。 しかしながら、 ➢利用者を特定できる仕組みが講じられていない。 ➢共用識別コードの取り扱いに関する規程が整備されていない。 ことを確認した。	運用・保守時に利用する特権を伴う識別コードを用いたアクセス主体を特定できない場合、正規の主体へのなりすましや脆弱性を悪用した攻撃等の不正アクセス行為を特定できなくなるおそれがある。	「□□システム運用手順書」に、共用識別コードを用いる際に採るべき情報セキュリティ対策を規定し、不正アクセス行為の防止策を講じることが推奨されます。		

なお、監査報告書の添付資料は、発見事項一覧を基に作成する。報告会後に改善計画の検討、フォローアップを実施するために、あらかじめ添付資料のように、改善計画/改善結果、フォローアップ結果の列を用意しておくと良い。

監査報告書の作成において、注意すべき項目を以下に示す。

(1) 監査報告書の目的

① 監査報告書は、最高情報セキュリティ責任者に提出する報告書であり、最高情報セキュリティ責任者が指摘事項等や発見事項への助言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 監査を通じて情報セキュリティに関する課題を把握し、監査の結果で明らかになった課題を踏まえて、最高情報セキュリティ責任者は、統括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必要な対策を講じさせる。

(2) 監査の実施期間中から監査報告書の作成までに改善された指摘事項等

① 監査で確認した指摘事項等については、監査報告書の作成以前に対処を行った場合でも、必ず監査報告書に記載する。

② 監査を始める監査基準日（監査の実施開始日等）について、監査対象の組織とあらかじめ合意する。観察（視察）した違反事実を事後に修正すると、情報セキュリティに関する実態把握を妨げ、機関等全体（他の組織や情報システム）の改善の機会を失うおそれが生じる。

(3) 監査対象の組織との合意

① 監査責任者は、監査対象の組織と事実確認を行うが、必要に応じて、監査報告書の内容に齟齬がないことを監査対象の組織に確認する。齟齬があった場合は、監査証拠を確認し、修正を検討する。なお、監査人としての独立性を保つために、監査証拠で確認できた内容のみを修正する。

② 指摘事項等に対する助言は最高情報セキュリティ責任者の改善指示に影響するため、その内容については監査対象の組織とあらかじめ協議して、実行困難な改善指示が出ることを防ぐ。

4.2. 監査報告会の実施

【実施すべき事項】

監査責任者は、監査対象の組織に対する報告会を実施する。

【統一基準との関係】

特になし

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

特になし

【実施内容】

監査責任者は、監査対象の組織に対する報告会を実施し、指摘事項等の説明、発見への助言等を行う。報告会の説明内容を基に意見交換を実施することは、監査対象の組織の改善活動に有意義である。報告会には、監査対象の組織の責任者、担当者、監査対象のシステムの責任者、担当者の参加が望まれる。

5. 監査結果に応じた対処

5.1. 改善指示

監査結果に応じた対処では、監査報告書の内容を踏まえ、最高情報セキュリティ責任者は改善を指示する。

5.1.1. 横断的な改善事項の対応

【実施すべき事項】

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、指摘事項等（指摘事項、推奨事項）に対する機関等内で横断的に改善が必要な事項の改善計画の策定等を統括情報セキュリティ責任者に指示する。

【統一基準との関係】

統一基準	遵守事項	2.3.2(3)(a)
		2.3.2(3)(b)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑭ 横断的な改善の指示

【実施内容】

(1) 監査報告書に記載されている指摘事項等は、監査対象組織やシステム以外においても同じ課題や問題が存在する可能性がある。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、指摘事項等の分析・評価を行い、監査対象組織以外の機関等内の組織又はシステムにおいても指摘事項等が検出される可能性がある場合には、横断的な対応を検討する。横断的な対応の必要性が高いと考えられる場合としては、例えば、

① 今回の監査結果において、複数の監査対象組織やシステムで同様の問題が発見されている場合や、以前の監査結果で発見された事項と同様の問題が繰り返して発見されている場合（機関等内において何らかの構造的な問題や組織的な体質等が要因となって、問題が多発している可能性がある場合）

② 今回の監査結果の内容やその原因を検討した結果、今回の監査対象以外の組織やシステムにも同様の指摘内容の問題が内在する可能性があると考えられる場合

③ 監査対象のシステムや機器等と同種のシステムや機器等が機関等内の他の部局にも存在することが把握されていたり、存在する可能性が高い場合

④ 発見された問題が、機関等か否か問わず、他の機関等においてもよく発生しているものとして注意喚起されている場合

⑤ 機関等に同様の問題が残っていると非常にリスクが高い問題であり、前広に横断的対応を実施して、もし他組織等で問題があれば至急の改善を促す必要がある場合等が考えられる。最高情報セキュリティ責任者は、横断的な改善の必要性を検討した上で、横断的な改善計画を策定することを統括情報セキュリティ責任者に指示する。

(2) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者の指示を踏まえ、横断的な改善の必要性を検討するとともに、必要な場合には横断的な対応を検討する。また、横断的な対応を指示されていない事項であっても、監査において得られた教訓等を機関等内に展開することで組織全体の情報セキュリティの強化につながる取組を考慮する。

なお、横断的な対応としては様々な方法が考えられるが、単に周知や注意喚起を行うだけでは、十分な効果をもたらさない可能性もある。

改善すべき事項の性質に応じて、例えば、周知や注意喚起だけでなく、機関内の他の組織・システムの責任者に対して、同種の問題が発生していないか確認や報告を求めたり、各機関の定期的な情報セキュリティ教育や自己点検において監査で発見された問題点の盛り込むこと等が考えられるほか、次期情報セキュリティ監査において、周知や注意喚起、問題有無の報告を求めた事項と同様の問題の有無を監査事項として、フォローアップする等の方法も想定される。

(3) 改善計画の策定等の指示に当たっては、以下に示す機関等内で横断的に改善が必要な事項の検討も含めて指示する。

① 監査を受けた部門以外の部門においても同種の課題や問題が存在している可能性ある場合

② 機関等内で共通的に使用している情報システムに対する改善が必要な場合

③ 情報セキュリティ関係規程の改善が必要な場合

5.1.2.組織に特有な改善事項の対応

【実施すべき事項】

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、指摘事項等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。

なお、改善計画の策定等の指示に当たっては、組織に特有な指摘事項等として改善が必要であるか検討することも含める必要がある。

【統一基準との関係】

統一基準	遵守事項	2.3.2(3)(a)
		2.3.2(3)(c)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑰ 組織に特有な改善の指示

【実施内容】

(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、組織に特有な指摘事項等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。

(2) 情報セキュリティ責任者は、最高情報セキュリティ責任者の指示に基づき、最高情報セキュリティ責任者の指示を踏まえ、改善計画の策定に向けた改善内容を検討する。また、組織に特有な指摘事項等があるか検討した上で、組織に特有な指摘事項等がある場合には対応を検討する。

5.2. 改善計画の作成、改善の実施及び報告

5.2.1. 横断的な改善事項の改善計画の策定、改善の実施及び報告

【実施すべき事項】

統括情報セキュリティ責任者は、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、最高情報セキュリティ責任者に報告する。また、改善に必要な措置を実施し、措置結果を最高情報セキュリティ責任者に報告する。措置が完了していない改善計画については、定期的に最高情報セキュリティ責任者に報告する。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(3)(b)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑮ 改善計画策定・規程等の見直し又は指示・報告

⑯ 規程等の見直し・報告

【実施内容】

(1) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定する。

(2) 統括情報セキュリティ責任者は、監査報告書に記載される改善が必要な事項の内容が、例えば以下のような場合は、統括情報セキュリティ責任者がその対策に係る事務を統括することが求められる。

・監査対象の組織以外の組織においても同種の課題や問題が存在している。
・機関等内で共通的に使用している情報システムについては、監査を受けた組織のみで対処することが困難である。
・情報システムの利用部門全体に係る改善が必要な事項となる。

(3) 機関等全体での運用状況が把握できていない場合は、緊急の実態調査、自己点検内容への反映等により、問題の有無を調査した上で対処する。

(4) 改善計画は、その改善を実施することにより、指摘があった監査項目の基準を満たす計画を策定する必要がある。

(5) 統括情報セキュリティ責任者は、改善計画を踏まえ、機関等内で横断的に改善が必要となる運用規程、実施手順の見直しを行う。改善が必要となる事項のうち機関等の対策基準の見直しが必要な場合は、対策基準を見直す。また、改善が必要となる事項のうち各システムの情報セキュリティ責任者が策定している実施手順については、情報セキュリティ責任者に改善の指示を行う。

(6) 統括情報セキュリティ責任者は、措置の実施又は指示の結果をとりまとめて最高情報セキュリティ責任者へ報告する。また、改善計画の対応状況について、最高情報セキュリティ責任者に定期的に報告する。

5.2.2.組織に特有な改善事項の改善計画の策定、改善の実施及び報告

【実施すべき事項】

情報セキュリティ責任者は、自らが担当する組織に特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、最高情報セキュリティ責任者に報告する。また、必要な措置を実施、措置結果を最高情報セキュリティ責任者に報告する。措置が完了していない改善計画については、定期的に最高情報セキュリティ責任者に報告する。

【統一基準との関係】

統一基準　　遵守事項　　2.3.2(3)(c)

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

⑱ 改善計画策定・規程等の見直し・報告

【実施内容】

(1) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織に特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、最高情報セキュリティ責任者に報告する。

(2) 情報セキュリティ責任者は、最高情報セキュリティ責任者から指示を受けた改善すべき事項のうち、「機関等内で横断的に改善が必要な事項」を除いた事項に対処する必要がある。

(3) 指摘事項等に対する改善の実施では、予算要求が必要な場合がある。改善計画について、予算取りまとめ時期を考慮した上で、改善の実施時期を検討する必要がある。

(4) 改善計画は、その改善を実施することにより、指摘があった監査項目の基準を満たす計画を策定する必要がある。

(5) 情報セキュリティ責任者は、機関等における情報セキュリティ監査の結果を踏まえ、情報セキュリティ対策に関する運用規程及び実施手順を見直す。

(6) 情報セキュリティ責任者は、措置の実施又は指示の結果をとりまとめて最高情報セキュリティ責任者へ報告する。また、改善計画の対応状況について、最高情報セキュリティ責任者に定期的に報告する。

監査報告書の添付資料を利用した改善計画及び改善結果の記載例を表 3.5-1 に示す。

表 3.5-1　改善計画及び改善結果の記載例

発見事項					発見事項への助言	改善結果/改善計画	フォローアップ結果
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1	指摘事項 ○○省情報セキュリティポリシー 2.3.2(3)(a)	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統括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指示すること。	・監査結果については、情報セキュリティ監査報告書の閲覧により、最高情報セキュリティ責任者宛て報告がされていることを確認したが、最高情報セキュリティ責任者から統括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対して、指摘事項に対する改善計画の策定等を指示したことは確認できなかった。	監査結果に対して最高情報セキュリティ責任者の改善指示が欠落した場合、当該機関の改善実施の機会が失われ、情報セキュリティ対策の実効性が担保できなくなるおそれがある。	「○○省情報セキュリティ監査実施手順」X.X.X(X)項を改定して、監査報告時に必ず最高情報セキュリティ責任者からの改善指示を得ることを定めるとともに、措置結果及び改善計画の報告についても必ず実施する規定を設け、規定に従った運用を行うことが必要です。	【必要な措置】 今年度監査報告書に関して、○月○日情報セキュリティ委員会において最高情報セキュリティ責任者から改善指示を得て、改善済みの事項に係る改善結果及び未改善の事項に係る改善計画について報告、了承を得た。 【改善計画】 統括情報セキュリティ責任者は、「情報セキュリティ監査実施手順」の改定を今年度内に実施する。	
2	推奨事項 ○○省情報セキュリティポリシー 6.1.1(2)-6	情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	・設計書及び運用手順書の閲覧、被監査の情報システム担当へのヒアリングにより、 ➢当該情報システムの運用・保守用に、共用識別コードを使用している。 しかしながら、 ➢利用者を特定できる仕組みが講じられていない。 ➢共用識別コードの取り扱いに関する規程が整備されていない。 ことを確認した。	運用・保守時に利用する特権を伴う識別コードを用いたアクセス主体を特定できない場合、正規の主体へのなりすましや脆弱性を悪用した攻撃等の不正アクセス行為を特定できなくなるおそれがある。	「□□システム運用手順書」に、共用識別コードを用いる際に採るべき情報セキュリティ対策を規定し、不正アクセス行為の防止策を講じることが推奨されます。	【必要な措置】 当該システムに関しては管理者ごとに識別コードを付与した。 【改善計画】 システム運用方針として、特権を付与する識別コードの共用を原則的に禁止し、やむを得ず共用を行う場合は例外申請手続の審査を経ることとする。当該改善については、関係者間で確認の上、情報システムセキュリティ責任者は本報告より30日以内に「システム運用手順書」に反映する。	

5.3. フォローアップの実施（実施が望まれる事項）

【実施すべき事項】

フォローアップとは、改善計画の実施状況を定期的に確認することをいう。また、改善結果を最高情報セキュリティ責任者に報告し、個別監査結果の報告と同様に、承認を得ることが望まれる。統一基準では、フォローアップについての記載はないが、監査のPDCAの観点から必要であることから追記する。

【統一基準との関係】

特になし

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

特になし

【実施内容】

(1) フォローアップの実施者は統一基準群に定めがないが、機関等の実態に応じて、監査責任者、監査実施者、情報セキュリティ推進体制等が担当することが考えられる。改善の指示と同様に、横断的な改善事項に関しては統括情報セキュリティ責任者が、また組織に特有な改善事項に関しては情報セキュリティ責任者が改善計画に対する改善の実施状況、改善結果を確認することが考えられる。

(2) 改善結果を最高情報セキュリティ責任者に報告し、承認を得ることが望まれる。
(3) 改善の取組が中長期にわたる場合には、改善計画の実施状況の進捗等につき定期的な報告を行うことが望ましい。改善の進捗により、複数の改善項目について一括したフォローアップを行うことが効率的な場合もある。

監査報告書の添付資料を利用し、改善計画及び改善結果を記載した結果を確認する。改善計画及び改善結果を基にフォローアップの結果の記載例を表 3.5-2 に示す。

表3.5-2　フォローアップの結果の記載例

発見事項					発見事項への助言	改善結果/ 改善計画	フォローアップ結果
No.	発見事項 区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1	指摘事項 ○○省情報セキュリティポリシー 2.3.2(3)(a)	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統括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指示すること。	• 監査結果については、情報セキュリティ監査報告書の閲覧により、最高情報セキュリティ責任者宛て報告がされていることを確認したが、最高情報セキュリティ責任者から統括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対して、指摘事項に対する改善計画の策定等を指示したことは確認できなかった。	監査結果に対して最高情報セキュリティ責任者の改善指示が欠落した場合、当該機関の改善実施の機会が失われ、情報セキュリティ対策の実効性が担保できなくなるおそれがある。	「○○省情報セキュリティ監査実施手順」X.X.X(X)項を改定して、監査報告時に必ず最高情報セキュリティ責任者からの改善指示を得ることを定めるとともに、措置結果及び改善計画の報告についても必ず実施する規定を設け、規定に従った運用を行うことが必要です。	【必要な措置】 今年度監査報告書に関して、○月○日情報セキュリティ委員会において最高情報セキュリティ責任者から改善指示を得て、改善済みの事項に係る改善結果及び未改善の事項に係る改善計画について報告、了承を得た。 【改善計画】 統括情報セキュリティ責任差は、「情報セキュリティ監査実施手順」の改定を今年度内に実施する。	【フォローアップ結果】 • 改定「情報セキュリティ監査実施手順」第○条において、監査報告会における改善指示の取得及び改善指示に対応する報告事項に関する規定を確認した。 【証跡】 • △月△日改定「情報セキュリティ監査実施手順」
2	推奨事項 ○○省情報セキュリティポリシー 6.1.1(2)-6	情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	• 設計書及び運用手順書の閲覧、被監査の情報システム担当へのヒアリングにより、 ➢ 当該情報システムの運用・保守用に、共用識別コードを使用している。 しかしながら、 ➢ 利用者を特定できる仕組みが講じられていない。 ➢ 共用識別コードの取り扱いに関する規程が整備されていない。 ことを確認した。	運用・保守時に利用する特権を伴う識別コードを用いたアクセス主体を特定できない場合、正規の主体へのなりすましや脆弱性を悪用した攻撃等の不正アクセス行為を特定できなくなるおそれがある。	「□□システム運用手順書」に、共用識別コードを用いる際に採るべき情報セキュリティ対策を規定し、不正アクセス行為の防止策を講じることが推奨されます。	【必要な措置】 当該システムに関しては管理者ごとに識別コードを付与した。 【改善計画】 システム運用方針として、特権を付与する識別コードの共用を原則的に禁止し、やむを得ず共用を行う場合は例外申請手続の審査を経ることとする。当該改善については、関係者間で確認の上、情報システムセキュリティ責任者は本報告より30日以内に「システム運用手順書」に反映する。	【フォローアップ結果】 • 改定「システム運用手順書」第○条において、特権ID共有の原則禁止及び例外の扱いに関する規定を確認した。 【証跡】 • △月△日改定「□□システム運用手順書」

5.4. 情報セキュリティ運用上の対応

【実施すべき事項】

情報セキュリティ監査、自己点検結果、最新のサイバーセキュリティ動向等を踏まえて、必要に応じて機関等の情報セキュリティ対策の運用を見直す。

【統一基準との関係】

特になし

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

特になし

【実施内容】

(1) 機関等の情報セキュリティ監査結果、自己点検結果、戦略本部監査におけるマネジメント監査やペネトレーションテスト、最新のサイバーセキュリティ動向、インシデント事例、様々なセキュリティ技術の普及等を踏まえて、必要に応じて機関等の情報セキュリティの運用を見直し、情報セキュリティ対策の向上に対応する。
(2) 対策の実施に際して、運用規程及び実施手順の見直し、実施の運用方法の見直し等で対応できる項目を始め、情報セキュリティ対策の製品の導入等、様々な対応が想定される。対策には、対応要員が必要な場合、調達のために費用が発生する場合等が

あるため、機関等で緊急度、対応の優先度を勘案して、情報セキュリティ対策の向上に対応する必要がある。

6. 監査関係ファイルの管理及び保存

6.1. 監査関係ファイルの管理及び保存

【実施すべき事項】

監査の全ての過程が終了した後の監査調書は、機関等の情報セキュリティ対策に関する重要な情報を含むため、適切に管理し、保存しなければならない。

【統一基準との関係】

特になし

【監査業務の全体像（第 2 部 図 2.2-2）との関係】

特になし

【実施内容】

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。監査調書には、機関等における情報セキュリティ対策の実施状況や監査項目に対する評価の結果等、機関等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取りまとめ、適切に管理し、保存しなければならない。

(1) 監査調書に係る情報の取扱い

① 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。

② 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。

③ 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査閲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。このためには、

・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

等のために、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必要がある。

(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取りまとめ、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、監査人は以下の項目を監査調書に記録する。

・修正又は追加が必要となった具体的理由
・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査閲した者及び実施日

(5) 監査ファイルの保存

監査責任者は、定められた監査ファイルの保存場所や保存責任者、保存期間に準じて、その情報の取り扱いに従って適切に保存する。

付録　監査計画・報告書・調書等のひな形

①　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
2. 機関等の概要
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
(2) その他の監査対象

6. 監査の実施体制
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. 外部事業者による監査の範囲及び必要性

(1) 外部事業者の範囲及び必要性

①　範囲
②　必要性委託契約の必要性の要否

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（別紙のとおり）

①　目標：
②　監査業務基礎講座：
③　情報セキュリティ基礎講座：

別紙

●監査業務の管理体制

●監査スケジュール

●監査予算

●人材育成計画

② 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　機関等の対策基準、運用規程及び実施手順に関する個別監査実施計画書

1. 監査目的
2. 背景
3. 監査対象：
4. 監査対象の組織及び責任者：
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. 監査の実施場所：
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）機関等の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

（イ）運用規程及び実施手順が機関等の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

（ウ）実際の運用が機関等の対策基準、運用規程及び実施手順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

●監査の進捗管理手段

1.

③　監査対象の部門における実際の運用が情報セキュリティ関係規程に準拠していることに関する監査手続のひな形

対策基準	監査項目	監査手続	発見事項（所見）	監査証拠

④　機関等の対策基準について、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に関する監査調書のひな形

統一基準	対策基準	発見事項（所見）

⑤　機関等が策定した運用規程及び実施手順について、機関等の対策基準に準拠していることに関する監査調書のひな形

対策基準	運用規程・実施手順	発見事項（所見）

⑥　監査対象の組織における実際の運用について、機関等の策定した情報セキュリティ関係規程に準拠していることに関する監査調書のひな形

対策基準	監査項目	監査手続	発見事項（所見）	監査証拠

⑦　発見事項一覧のひな形

発見事項					発見事項への助言
No.	発見事項 区分種別	監査項目	発見事項（所見）	発見事項のリスク	
1					
2					

⑧　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）
氏　　名

○○年度　××××省情報セキュリティ監査報告書

令和○○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
2.　監査実施期間：
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

(2)　その他の監査対象
4.　情報セキュリティ監査の基準とした基準名等：機関等の対策基準
5.　監査の結果
6.　指摘事項及び発見事項への助言の総括
7.　添付資料
(1)
(2)

⑨　監査報告書の添付資料のひな形

発見事項					発見事項への助言	改善結果/改善計画	フォローアップ結果
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1							
2							

⑩　改善計画及び改善結果のひな形

発見事項					発見事項への助言	改善結果/改善計画	フォローアップ結果
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1							
2							

⑪　フォローアップの結果のひな形

発見事項					発見事項への助言	改善結果/改善計画	フォローアップ結果
No.	発見事項区分種別	監査項目	発見事項（所見）	発見事項のリスク			
1							
2							