DM2-06-071

自己点検の考え方と実務への準備

解説書

2007 年 11 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2006/3/31	初版
2007/11/9	政府機関統一基準(第２版)の策定に伴う修正等

商標について

- Microsoft は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

目次

1. 本解説書の目的 4
2. 自己点検の概要 4
2.1 自己点検の趣旨 4
2.2 自己点検の基本的な考え方 4
2.3 自己点検に係る作業の全体像 6
3. 自己点検に関する年度計画の策定 （ 2.3.1 (1) ） 10
3.1 「年度自己点検計画」の位置付けと策定目的 10
3.2 「年度自己点検計画」を策定する際の考慮事項と制約事項 10
4. 自己点検の実施に関する準備 （ 2.3.1 (2) ） 12
4.1 情報セキュリティ関係規程の整備 (Step A) 14
4.2 自己点検項目の整備 (Step B) 15
4.3 自己点検票の集約ルートの検討 (Step C) 25
4.4 自己点検結果の確認・評価に関する委任の検討 (Step D) 27
4.5 自己点検票への展開 (Step E) 28
4.6 行政事務従事者ごとに再構成 (Step F) 29
4.7 自己点検の実施環境の整備 (Step G) 30
5. 自己点検の実施 （ 2.3.1 (3) ） 32
5.1 情報セキュリティ責任者による実施の指示 32
5.2 行政事務従事者（実施主体）による実施 33
5.3 情報セキュリティ責任者による実施状況の確認 33
6. 自己点検結果の評価 （ 2.3.1 (4) ） 34
6.1 情報セキュリティ責任者による確認・評価 34
6.2 統括情報セキュリティ責任者による確認・評価 35
6.3 最高情報セキュリティ責任者への報告 35
7. 自己点検に基づく改善 （ 2.3.1 (5) ） 36
7.1 行政事務従事者自身による自己改善 36
7.2 最高情報セキュリティ責任者による改善指示 37
付録編 39
付録１：年度自己点検計画の雛形 40
付録２：自己点検実施指示書の雛形 41

1. 本解説書の目的

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（第２版）」（NISD-K303-071、以下「政府機関統一基準」という。）に基づき、自己点検を実施することが求められている。しかしながら、自己点検については、これまで各府省庁に取り入れられていないものであることから、その計画策定及び準備は入念に行う必要がある。

本解説書は、自己点検の考え方と実務への準備を中心に、関係する遵守事項を詳細に解説するとともに、年度計画や実施手順書等の雛形を示したものであり、もって自己点検の適切な実施に資することを目的とする。

2. 自己点検の概要

2.1 自己点検の趣旨

情報セキュリティ対策は、それに係るすべての行政事務従事者が、各自の役割を確実に行うことで実効性が担保されるものであることから、すべての行政事務従事者自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要である。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

[政府機関統一基準「2.3.1 情報セキュリティ対策の自己点検」より引用]

2.2 自己点検の基本的な考え方

自己点検は、各遵守事項の実施主体となる本人が行うべき情報セキュリティ対策を適切に実施しているかを点検するものである。このため、「実施主体による自己点検」が自己点検の中心として位置付けられるが、その進捗状況の管理や集計をする体制を構築することも重要となる。したがって、政府機関統一基準 2.3.1 項に示す自己点検における実施及び確認・評価は、本人による点検及び情報セキュリティ責任者等による進捗管理・集計、そして最高情報セキュリティ責任者によるとりまとめの３つの過程により行う。（図１参照）

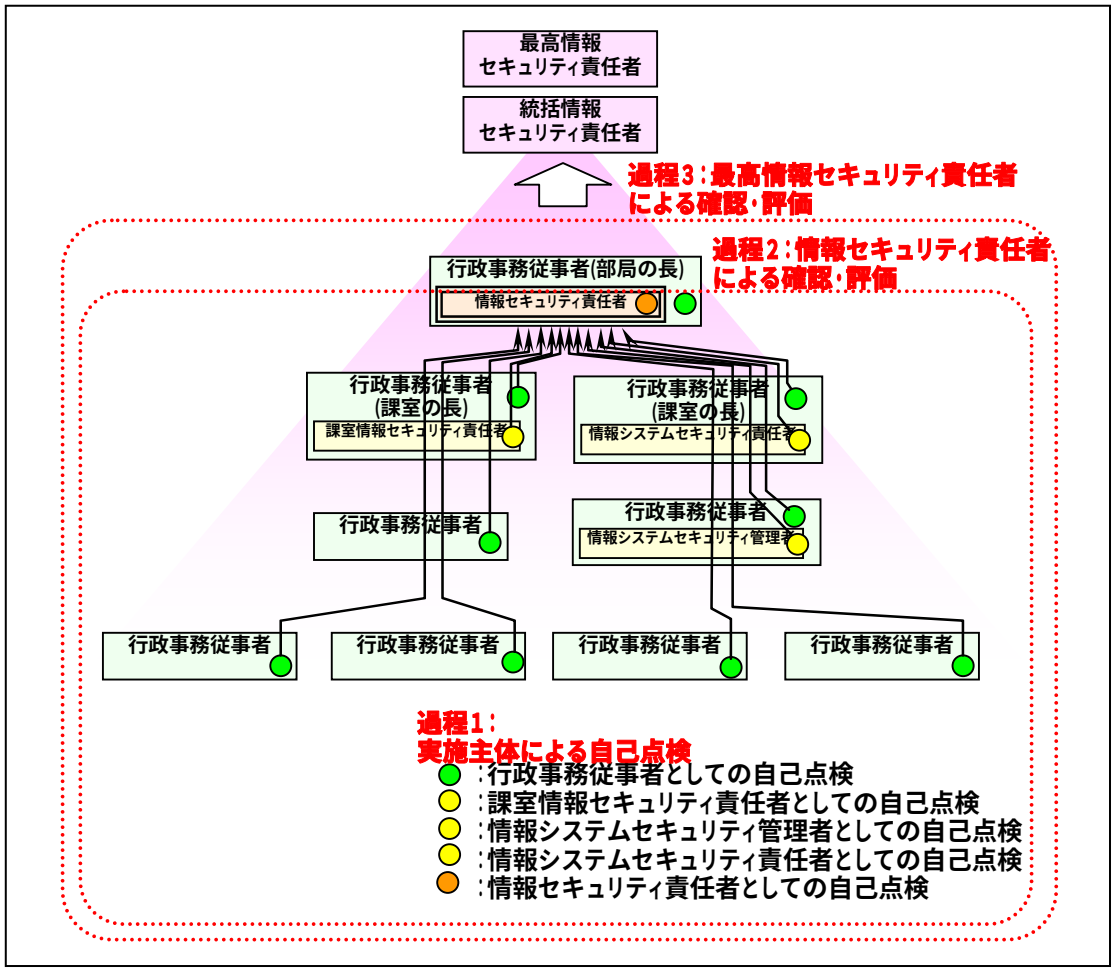


図 1. 自己点検の実施及び確認・評価における３つの過程

(1) 過程１：実施主体による自己点検

「実施主体による自己点検」とは、情報セキュリティ関係規程に定められた遵守事項における主語、すなわちその対策の実施主体本人による自己点検である。例えば、情報セキュリティ関係規程において「すべての行政事務従事者は、・・・すること」と記載がある場合の実施主体は、「すべての行政事務従事者」となり、「課室情報セキュリティ責任者は、・・・すること」と記載がある場合のそれは、「課室情報セキュリティ責任者」となる。

そのため、情報セキュリティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者その他情報セキュリティ管理の職務にある者は、当該職務者としての自己点検に加えて、行政事務従事者（利用者）としての自己点検の両方が求められることになる。また、複数の情報システムを取り扱う場合には、それぞれの情報セキュリティの管理単位に応じて、自己点検が実施されることとなる。すなわち、一人の行政事務従事者に注目した場合、取り扱う情報システムごと、及びその役割（利用者、責任者）ごとに自己点検が実施されることとなる。

なお、実施主体による回答結果は、情報セキュリティ責任者があらかじめ指定する者を経由して集約する。

(2) 過程２：情報セキュリティ責任者による確認・評価

「情報セキュリティ責任者による確認・評価」とは、所管する単位における情報セキュリティ対策全体を通して、実施主体による自己点検について進捗状況を確認し、本人による自己点検結果の記載内容に不備がないかを評価することである。すなわち、実施主体から提出された回答を閲覧し、記入ミスや記入漏れの有無の確認をした上で、全実施主体が計画した期限内に自己点検を完了するために、進捗状況（自己点検実施率）を管理する。必要に応じて、実施主体に対して進捗状況を確認したり、予定より遅れていれば実施の催促をする。実施主体による自己点検が終了したら、結果を集計し実施率等について数値評価を行う。また、必要に応じて、以前実施された自己点検方法における指摘事項が適切に改善されていること等を評価する。その上で、所管する単位における確認・評価の結果を報告書として統括情報セキュリティ責任者へ提出する。

なお、作業の効率性や自己点検結果の正確性を向上させることを目的として、確認・評価に係る作業の一部を、行政事務の管理責任を有する者や、情報セキュリティ対策の管理責任を有する者（課室情報セキュリティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者等）に委任してもよい。

(3) 過程３：最高情報セキュリティ責任者による確認・評価

「最高情報セキュリティ責任者による確認・評価」とは、情報セキュリティ責任者からの自己点検結果の報告書の提出状況などを踏まえ、最高情報セキュリティ責任者が府省庁全体での自己点検が適切に行われていることを確認・評価することである。

2.3 自己点検に係る作業の全体像

自己点検に係る作業は、前節で示した 3 つの過程（実施及び確認・評価）を核とし、「導入」、「実施指示」及び「改善」を含めた以下の作業から構成される。

(1) 実施及び確認・評価の前段階である「導入」においては、最高情報セキュリティ責任者が承認した年度自己点検計画を踏まえ、各情報セキュリティ責任者は、自らの所管する範囲の情報システム又は課室に係る自己点検を実施するために行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備する。

(2) 「実施指示」においては、上記の導入準備が完了した後、情報セキュリティ責任者が自己点検票及び自己点検の実施手順（提出先、提出期限などを含む。）を提示し、自己点検の実施を指示する。

(3) 「実施及び確認・評価」においては、前述のとおり、まず実施主体による自己点検が行われ、その結果を情報セキュリティ責任者が確認・評価し、その結果を統括情報セキュリティ責任者が確認・評価し、さらにその結果を最高情報セキュリティ責任者が評価する。

(4) 「改善」においては、行政事務従事者自身による自己改善と、最高情報セキュ

リティ責任者による改善指示に大別される。前者は、ボトムアップ的なものであり、自己点検の結果に基づいて自己の権限の範囲で改善できると判断した事項へ対処するものである（政府機関統一基準 2.3.1 (5)(a)）。その際、自己点検で気付いた問題点ですぐに改善できることがあれば、自己点検結果の集計や監査結果を必ずしも待たなくとも、適宜改善することが望ましい。後者は、トップダウン的なものであり、最高情報セキュリティ責任者が情報システムの自己点検結果を評価し、必要があると判断した場合には情報セキュリティ責任者に改善を指示するものである（政府機関統一基準 2.3.1 (5)(b)）。

実施及び確認・評価を含め、自己点検に係る作業の全体像を図２に示す。

		導入		実施指示	実施及び確認・評価				改善	
					過程 1	過程 2	過程 3			
		計画	準備		実施主体による自己点検	情報セキュリティ責任者による確認・評価	統括情報セキュリティ責任者による確認・評価	最高情報セキュリティ責任者による確認・評価	自己改善	改善指示
職位・役割	最高情報セキュリティ責任者	年度計画の承認						自己点検の評価の受領		改善指示
	統括情報セキュリティ責任者	年度計画の策定					自己点検の確認・評価			
	情報セキュリティ責任者(※1)		自己点検票及び実施手順の整備	実施の指示		自己点検の確認・評価			自己の権限の範囲で改善	
	行政事務従事者（実施主体）(※２)				自己点検の実施				自己の権限の範囲で改善	
政府機関統一基準における項番		2.3.1 (1)(a)	2.3.1 (2)(a)	2.3.1 (3)(a)	2.3.1 (3)(b)	2.3.1 (4)(a)	2.3.1 (4)(b)	2.3.1 (4)(c)	2.3.1 (5)(a)	2.3.1 (5)(b)
本手引書における解説		3 章	4 章	5 章		6 章			7 章	

※１：ここで、情報セキュリティ責任者とは、自己点検の確認・評価を実施する者としての情報セキュリティ責任者を指す。

※２：ここで、行政事務従事者（実施主体）とは、実施主体としての情報セキュリティ責任者（統括情報セキュリティ責任者を含む）、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者等を含む。

図２．自己点検に係る作業の全体像

自己点検と監査の違いとは？

自己点検は、行政事務従事者自らがその情報セキュリティ対策を実施しているかを点検するものである。一方、監査は、情報セキュリティ対策の実施者とは独立性を有した者が客観性、専門性を持って監査を行うものである。

また、自己点検は、原則としてすべての情報セキュリティ対策を対象とするものである。一方、監査は、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か否かを監査するに当たっては、すべての情報セキュリティ対策を直接監査することが困難なこともある。そのため、自己点検の結果等を踏まえて、自己点検が適切に実施されているかをサンプリング調査によって確認することが可能な場合もある。

以下に、自己点検と監査との主な相違点を示す。

	自己点検	監査
実施者	情報セキュリティ対策の実施主体自ら実施する。	情報セキュリティ対策の実施者とは独立性を有した者が実施する。
報告先	自己点検の実施者は、回答を情報セキュリティ責任者へ提出する。情報セキュリティ責任者は、その確認・評価の結果を統括情報セキュリティ責任者に提出する。統括情報セキュリティ責任者は、その確認・評価の結果を最高情報セキュリティ責任者へ提出する。	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へ提出する。
実施頻度	遵守事項に応じて、日常的に実施されるべきものから、年一度程度の実施でよいものまで様々である。	主たる監査は年度末に実施されるが、自己点検に応じて随時するという実施計画を策定しても構わない。
対象の選定	原則として、すべての実施主体がすべての対策項目について実施する。	監査対象をサンプリングにより選出し、母集団の統計的性質を推定することができる場合もある。
評価の観点	実際の運用が情報セキュリティ関係規程に遵守しているかを点検する。（遵守性の観点）	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かという観点のほか、省庁対策基準が統一基準に準拠しているか、作成された実施手順等の関係規程が省庁対策基準に準拠しているかについても監査を行う。（準拠性と遵守性の観点）
評価の手法	情報セキュリティ対策の実施主体によって自己申告された回答を原票として、それを評価する。	規定文書等の確認を行って準拠性を評価し、また、被監査部門への質問・査閲・観察・点検により遵守性を評価する。
改善プロセス	最高情報セキュリティ責任者から改善指示があった場合の対処のほか、行政事務従事者が自己の権限の範囲で改善できると判断した事項は自ら対処を行う。	最高情報セキュリティ責任者から改善指示があった場合には、情報セキュリティ責任者は対応計画を作成し、報告する。

図 3. 自己点検と監査

自己点検結果の取扱い

最高情報セキュリティ責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には情報セキュリティ責任者に改善の指示を出すことが義務付けられている[政府機関統一基準の 2.3.1 (5)(b)]。なお、自己点検の結果は、監査を実施するに当たって、すべての行政事務従事者における情報セキュリティ対策の実態を把握するための重要な資料となるだけでなく、監査の方向性や重点領域を定める際の参考ともなる。

3. 自己点検に関する年度計画の策定　（ 2.3.1 (1) ）

自己点検は、各情報セキュリティ責任者の責任において、所管する単位で実施されるものである。統括情報セキュリティ責任者は、それぞれの情報システム及び課室における自己点検を効率的かつ整合的に実施するため、府省庁全体としての年度自己点検計画を定める必要がある。

> **政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検**
> (1) (a) 統括情報セキュリティ責任者は、年度自己点検計画を策定すること。
> 【基本遵守事項】

上記の遵守事項は、自己点検を実施するに当たり、その実施頻度、実施時期、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である[解説書より抜粋]。

3.1 「年度自己点検計画」の位置付けと策定目的

(1) 「年度自己点検計画」は、各府省庁における自己点検を適切に実施するため、中長期的な視点から当該年度のテーマを定めた上で、様々な考慮事項、制約事項を勘案し、実施スケジュール（実施頻度及び実施時期）、確認及び評価の方法（委任する場合の責任範囲含む。）、実施項目の選択等を定めたものである。なお、自己点検はすべての実施主体が行うものであることから、「年度自己点検計画」については、行政事務従事者がこれを共有する必要がある。

(2) 「年度自己点検計画」は、統括情報セキュリティ責任者によって策定される。この「年度自己点検計画」に基づき、情報セキュリティ責任者は、自身の管理する情報セキュリティ対策の単位における自己点検について詳細スケジュールを策定し、自己点検票及び自己点検の実施手順を整備する。

3.2 「年度自己点検計画」を策定する際の考慮事項と制約事項

(1) 府省庁における情報セキュリティ関係規程の整備状況及びその遵守状況を踏まえること。特に、新たなセキュリティ対策を施す場合には、その施行に至るまでの準備期間や移行期間を考慮して計画することが求められる。

(2) 自己点検の実施に関与する特定の組織、特定の役職、特定の行政事務従事者に負荷が集中しないように負荷を平滑化すること。例えば、対象システムをいくつかの機能に分割した上で順次実施する、実施対象者をいくつかのグループに分割した上で順次実施する、自己点検一度当たりの質問数を分割する等の配慮が必要である。

(3) 実施時期の検討に当たっては、他の事務処理へ配慮すること。例えば、年度末や予算編成期などの繁忙期を避ける等の配慮が必要である。

(4) 実施時期の検討に当たっては、「自己点検の随時実施」を検討することが重要である。

一般的には、実施者が一定期間に行った遵守事項の実施状況を確認するため、年度末などの特定の時期に、自己点検の対象期間に係る実施状況について自己点検を行うことになる。例えば、政府機関統一基準の第３部にある「情報の格付けの実施」などのように必要の都度、実施者が判断するものが該当する。

しかしながら、政府機関統一基準の第４部及び第５部の遵守事項並びに第６部の一部の遵守事項については、情報システムのライフサイクルに沿って構成してあることから、それら遵守事項の中には、情報システムのライフサイクルの各段階において、１度しか実施しないものもある。例えば、政府機関統一基準の第４部にある「アクセス制御の必要性の有無の検討の実施」などのように情報システムの設計時に実施する事項が該当する。

このような事項については、その実施後、一定期間を経過してから自己点検をするよりも、実施後、速やかに自己点検を済ませてしまう方が、実施者にとっての負担が少ないばかりではなく、自己点検結果の精度も高いものとなる。例えば、情報システムの設計時に注意すべき遵守事項について、設計作業をする傍らに自己点検票を用意して作業チェックリストのように用いることにより、作業とともに自己点検を完了することができる。この結果、事後に時間が経過してから自己点検をするよりも、事実関係に係る誤記入が防げることに加え、失念により遵守事項の実施を怠るということも防ぐことができる。

このため、情報システム対策に関係する遵守事項のうち、その都度済ませる対策については、それを実施する際に自己点検票を作業チェックリストのように用いることで、作業時に自己点検を随時済ませていくことが効果的である。また、期間を通じての対策も、それが特定期間であれば、その期間終了後に速やかに自己点検をすることが効果的である。各府省庁における情報セキュリティ対策基準に基づく自己点検作業のうち、上記の趣旨に該当するものについては、随時実施することにより、効率及び精度を向上させることができる。

(5) 自己点検結果に基づく改善活動についても考慮した実施スケジュールとすること。

年度自己点検計画の雛形を付録１に示す。

4. 自己点検の実施に関する準備　（ 2.3.1 (2) ）

自己点検は、情報セキュリティの管理単位ごとに、それに係るすべての行政事務従事者が実施するものであること、行政事務従事者の役割によって実施内容に追加があること、実施主体による回答を情報セキュリティ責任者へ提出するに当たっては複数の関係者を経由する可能性があること、情報セキュリティ責任者による確認・評価が別の者に委任される可能性があること等をかんがみ、自己点検票及び自己点検の実施手順を整備することが求められる。

> **政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検**
> (2) (a) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。
> 【基本遵守事項】

各行政事務従事者が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、情報セキュリティ責任者は、行政事務従事者ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することを求める事項である [解説書より抜粋]。

自己点検票及び自己点検の実施手順を整備するには、以下に示す手順(Step A から Step G)に従って実施すると効率的である。

- Step A : 情報セキュリティ関係規程の整備　(4.1)
- Step B : 自己点検項目の整備　(4.2)
- Step C : 集約ルートの検討　(4.3)
- Step D : 確認・評価の委任　(4.4)
- Step E : 自己点検票への展開　(4.5)
- Step F : 行政事務従事者ごとに再構成　(4.6)
- Step G :　実施環境の整備　(4.7)

また、これらの準備は、情報セキュリティ責任者が、自身の所管する単位について行うものであるが、府省庁において共通的に準備することが効率的と思われる事務については、最高情報セキュリティ責任者や他の情報セキュリティ責任者と相談の上で準備するとよい。

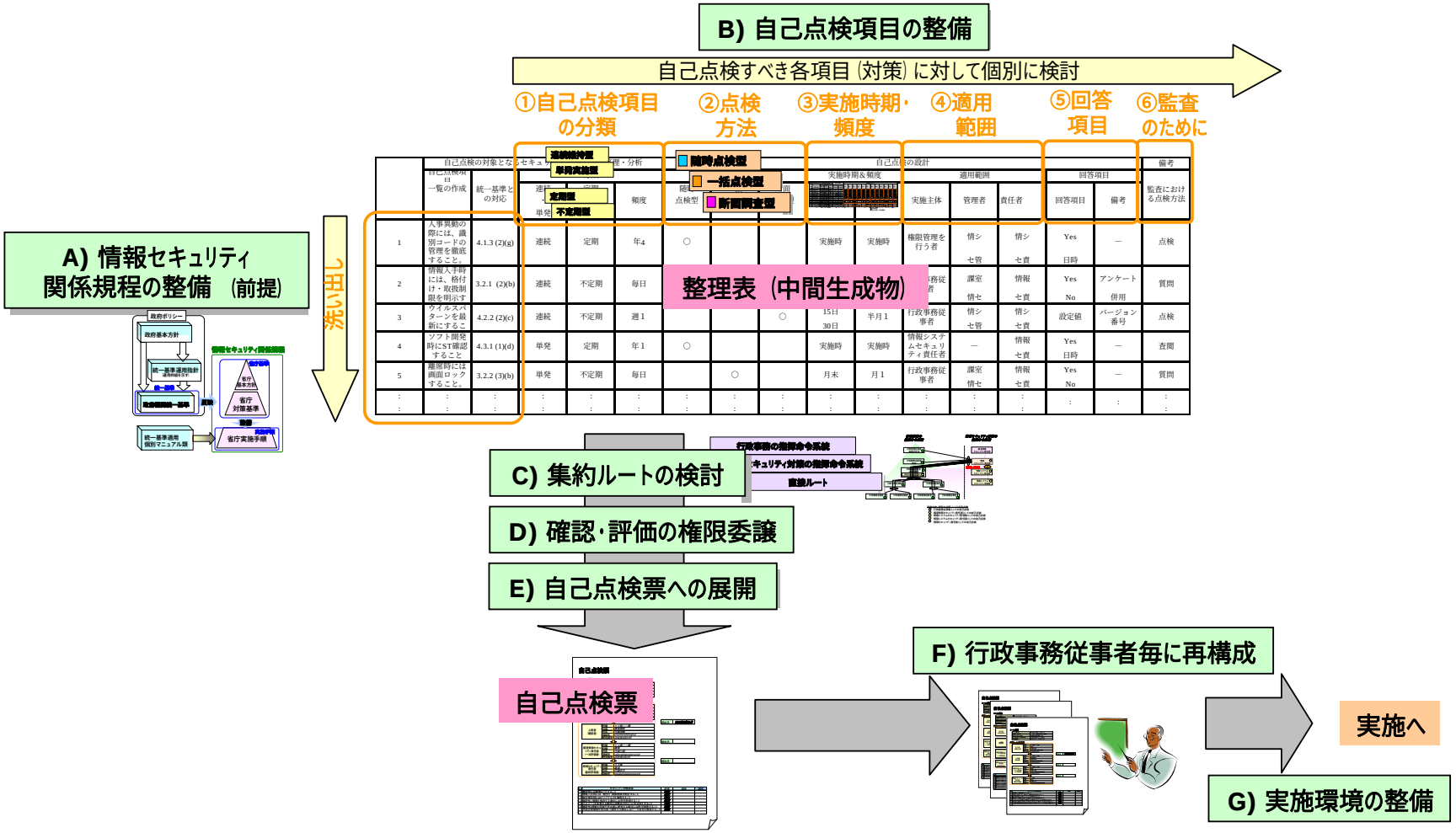


図 4. 自己点検実施の準備の全体像

4.1 情報セキュリティ関係規程の整備 (Step A)

自己点検は、各府省庁で定めた情報セキュリティ関係規程に従った運用が行われていることを確認するものである。そのため、情報セキュリティ責任者は、自己点検票及び自己点検の実施手順を整備するに先立ち、まずは実施主体（行政事務従事者、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者、情報セキュリティ責任者等）が実施すべき情報セキュリティ対策を明確にした情報セキュリティ関係規程の整備が求められる。

(1) まず、政府機関統一基準を省庁対策基準へ反映させる(Step A-1)ことが必要である。省庁対策基準への反映については、策定時に実施されているところであるが、今後の政府機関統一基準の改訂や、情報セキュリティを取り巻く環境の変化、対策の改善などに応じて、今後も継続的に省庁対策基準を見直す必要がある。なお、府省庁全体のセキュリティポリシーである省庁対策基準の見直しに当たって、情報セキュリティ責任者がその責務を負っていない場合には、最高情報セキュリティ責任者又は統括情報セキュリティ責任者と相談の上、適宜対応すること。

(2) 次に、必要に応じて実施手順を整備する(Step A-2)ことが必要である。情報セキュリティ責任者は、省庁対策基準の導入に当たって実施手順が必要であると判断した場合には、これを整備することが求められる。当該情報システムにセキュリティ対策を講ずるための実施手順は、誰が（実施主体）何をすべきか、自己点検において評価可能な程度まで具体的に記述されている必要がある。

(3) つづいて、自己点検項目一覧を作成する(Step A-3)ことが必要である。情報セキュリティ関係規程を元に、当該情報システム又は課室について自己点検を行う項目を選別し、一覧を作成する。

(4) さらに、政府機関統一基準との対応関係を明確化する(Step A-4)ことが必要である。自己点検項目一覧に記載されたそれぞれの項目に対して、それが政府機関統一基準のどの遵守事項に対応するものであるかを明らかにするため、対応関係を明確化する。これは、自己点検の実施に直接必要となるものではないが、後に自己点検結果を分析・評価した場合に有用であるとともに、政府機関統一基準に対する運用状況等の報告を NISC から求められた場合に有用となる情報である。

4.2 **自己点検項目の整備** (Step B)

行政事務従事者等が業務において遵守すべき情報セキュリティ関係規程の項目が記載された自己点検票を作成することが必要となる。その手順を Step B から Step E において説明する。

効果的かつ効率的な自己点検を実施するためには、情報セキュリティ関係規程に定められている情報セキュリティ対策の特質を反映した自己点検票の作成が必要となる。Step B では情報セキュリティ対策の特質を検討・分類し、自己点検票を作成するための整理表を作成するところまでを説明する。

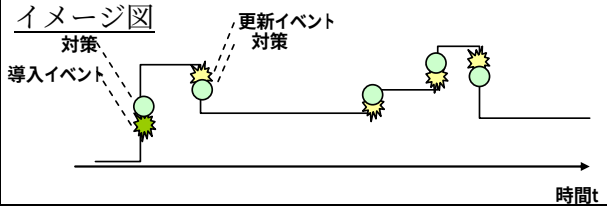
情報セキュリティ対策の特質を検討する際には、次の５つの観点から行うとよい。

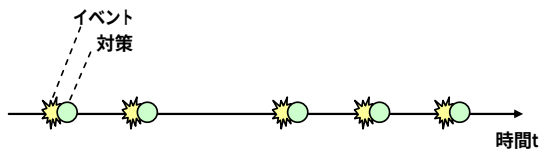
(1) 自己点検項目の分類	セキュリティ対策を実施するタイミングで自己点検をするか定期的に自己点検を実施するかを決定するために、情報セキュリティ対策の点検項目の特性を、「連続維持型」か「単発実施型」か、対策実施時期を「定期型」か「不定期型」かに分類する。
(2) 点検方法	情報セキュリティ対策の特性及び実施時期に応じた点検方法として、点検方法を「随時点検型」、「一括点検型」又は「断面調査型」に分類する。
(3) 実施時期・頻度	セキュリティ対策の重要性や点検方法に応じて実施時期及び頻度を決める。
(4) 適用範囲	セキュリティ対策の点検実施者を決める。
(5) 回答項目	実施有無の選択肢等、想定する回答を決める。

(1) 自己点検項目の分類 (Step B-1)

自己点検における点検方法を検討するに当たり、情報セキュリティ対策の特質を以下の観点から分類するとよい。

- 対策された状態の維持性による分類

タイプ	概説
連続維持型	実施されたセキュリティ対策について、それ以降もその対策状態が連続的に維持されるもの。すなわち、初期導入した後、その対策状態が保持され、セキュリティ対策の更新が必要と思われる事象の発生に応じて、対策状況の更新が行われる対策。 例えば、以下の対策が挙げられる。 ・責任者、管理者の設置及び担当変更 ・ウイルスパターン定義ファイルの更新 ・情報入手時の格付け/取扱制限の明示 イメージ図 

単発実施型	実施されたセキュリティ対策について、それ以降もその対策状態が必ずしも継続されないもの。すなわち、対策の初期導入を伴わず、セキュリティ対策が必要と思われる事象の発生に応じて、その都度実施される対策。 例えば、以下の対策が挙げられる。 ・各種の報告や申請処理 ・各種の確認処理 （例：公開時の機密度チェック） ・離席時の画面ロック イメージ図 

- 対策時期の定期・予測可能 / 不定期・予測困難　による分類

タイプ	概説
定期型 （時期予測可能型を含む）	セキュリティ対策が必要と思われる事象が定期的に発生する、又はその発生時期が予測可能なもの。 例えば、以下の対策が挙げられる。 ・識別コードの管理（人事異動反映） ・定期報告、年度計画策定 ・毎日帰宅時に書類の施錠保管 ・ソフトウェア開発における ST 確認
不定期型 （時期予測困難型を含む）	セキュリティ対策が必要と思われる事象が不定期的に発生する、又はその発生時期が予測困難なもの。 例えば、以下の対策が挙げられる。 ・ウイルスパターン定義ファイルの更新 ・情報入手時の格付け/取扱制限の明示 ・障害報告、例外申請処理

なお、定期型/不定期型ともに、対策実施の頻度は、自己点検の実施時期及び実施頻度を検討する上で重要な要素である。以下に「頻度」及び「該当する遵守事項」の分類例を示す。

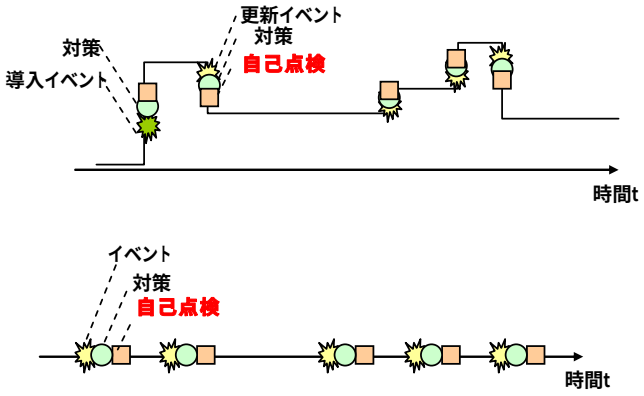
頻度	該当する遵守事項
年に一回 程度	・年度計画の策定 ・責任者、管理者の設置及び担当変更 ・ソフトウェア開発における ST 確認
6 ヶ月に一回 程度	・定期報告（上期・下期）
3 ヶ月に一回 程度	・識別コードの管理（人事異動反映） ・パスワードの変更
月に一回 程度	・Microsoft® Update
半月に一回 程度	・機密性 3 情報を移送する場合の許可申請
週に一回 程度	・ウイルスパターン定義ファイルの更新
一日に一回 程度	・毎日帰宅時に書類の施錠保管
一日に数回　程度	・離席時の画面ロック
頻度不明	・障害報告、例外申請処理

上記表内の「頻度」や「該当する遵守事項」はすべて例示であり、各府省庁におけるセキュリティ対策の対象や、各府省庁における対策状況を踏まえ、適宜定める。

(2) 点検方法の検討 (Step B-2)

自己点検項目一覧に記載されたそれぞれの項目に対して、点検方法を検討する。自己点検については、原則として実施主体における自己申告形式となるので、自己点検を実施するタイミングとその内容によって、主に以下の３つの点検方法が考えられる。

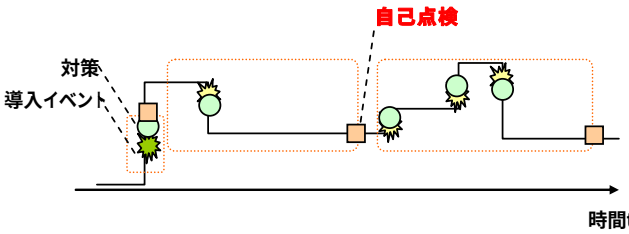
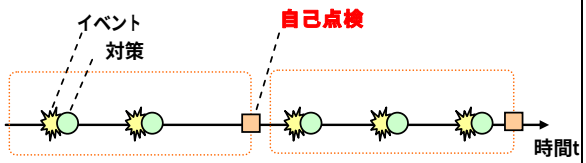
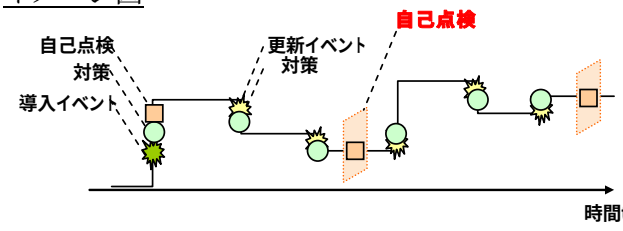
<table>
<tr><th colspan="2">点検方法</th><th>概説</th></tr>
<tr><td rowspan="2">Yes/No
回答型</td><td>随時点検型</td><td>セキュリティ対策が必要と思われる事象が発生した際に、その対策を実施した旨(Yes)を、随時、自己点検して報告する。

イメージ図
 

長所
・対策が実施された事実を情報セキュリティ責任者が即座に把握することができる。

短所
・事象ごとに自己点検が発生するため、頻度が高い場合には、実施主体側、集約する側ともに負荷が大きい。
・対策を忘れた場合には、回答もされない可能性が高いため、対策実態を把握しにくい。
・提出期限を設定することが難しく、実施主体の自発的な申告となるため、申告忘れが懸念される。

この点検方法が適している遵守事項
・発生頻度が低い事象に対する対策</td></tr>
<tr><td>一括点検型</td><td>あらかじめ設定された期間内において、セキュリティ対策が必要と思われる事象に対する対応状況(実施した(Yes)/実施しなかった(No)等)を自己点検して報告する。</td></tr>
</table>

		イメージ図   長所 ・設定期間内における対策状況をまとめて申告することができる。 ・提出期限を設定することにより、情報セキュリティ責任者が統制することができる。 短所 ・設定期間内における対策状況について、実施主体が記憶しておく必要がある。 ・対策実施とその自己点検に時間差が発生するため、即時把握が難しい。 ・設定期間内に、セキュリティ対策を実施すべき事象が発生しない場合であっても申告する必要が発生する。 この点検方法が適している遵守事項 ・発生頻度が高い事象に対する対策 ・不定期に発生する事象に対する対策
実態 回答型	断面調査型	連続維持型の対策に対して、ある時点でのセキュリティ対策状態をスナップショット的に調査して報告する。「対策を実施した事実」の確認ではなく、調査時点での対策実態を自己申告するものであり、設定値等を合せて提出する。 イメージ図 

		長所 ・対策実態を把握することが可能 ・提出期限を設定することにより、情報セキュリティ責任者が統制することができる。 短所 ・調査時点での対策状況のみが申告対象であるため、過去の対策経緯や履歴は不明。 この点検方法が適している遵守事項 ・連続維持型の対策であって、常に最新の状態であることが期待されるセキュリティ対策

自己点検項目一覧に記載された対策項目に対して自己点検方法を決定するに当たっては、自己点検項目の分類(Step B-1)や、それぞれの点検方法の長所及び短所を踏まえ、上記３つの点検方法を基本として適宜検討することが望ましい。上記３つの点検方法のいずれかを選択するほか、例えば、対策実施の都度、その記録を取得した上で、定期的に一括点検し、併せて過去の実施状況を再確認する等、点検方法を複合的に使うことも可能であれば検討すべきである。

なお、連続維持型、単発実施型のそれぞれについて、[定期型/不定期型]及び[対策実施の頻度]を考慮して自己点検項目を比較検討した場合における適切と思われる自己点検方法は、概ね以下の図５に示すような領域となる。

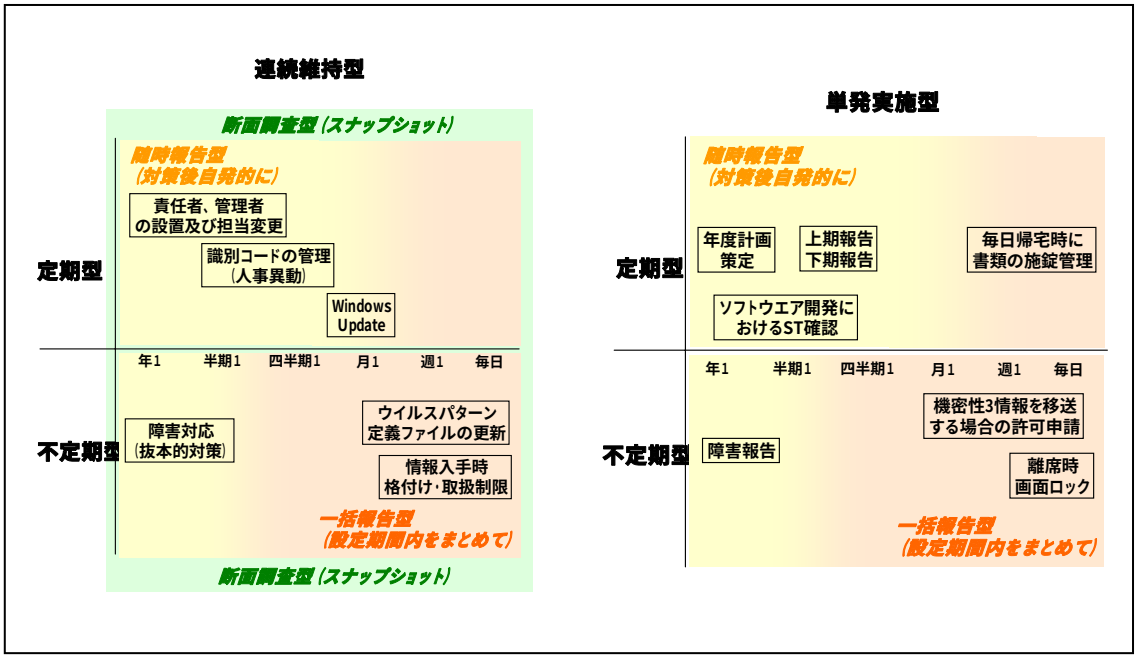


図 5. 点検方法の検討（例）

(3) 実施時期及び実施頻度の検討 (Step B-3)

自己点検項目一覧に記載されたそれぞれの項目に対して、一括点検型又は断面調査型による自己点検方法を選択した場合には、実施時期及び実施頻度に関する検討が必要である。自己点検の実施時期及び実施頻度を検討するに当たっては、統括情報セキュリティ責任者が定める年度自己点検計画を踏まえる必要がある。また、自己点検は、原則としてすべての遵守事項についてすべての実施主体が行うものであることから、当該セキュリティ対策自体の発生頻度のほか、実施主体（回答者）の作業負荷、統括情報セキュリティ責任者を含む情報セキュリティ責任者による確認・評価に係る作業負荷、最高情報セキュリティ責任者による評価に係る作業負荷なども考慮する必要がある。

負荷軽減・効率化のために例えば以下のような工夫をするとよい。

- 自己点検の実施時期及び実施頻度は、当該項目の発生時期や発生頻度に応じて適切に決定すべきであるが、発生時期や発生頻度に従い過剰に設定すると、実施する者に過大な負荷を強いるおそれがある。そのため、実施時期及び実施頻度の近い項目をグループ化し、同一グループに属する項目は同時に自己点検を実施することが効率的である。以下の図6に示す例は、毎月末に１ヶ月分、毎半期末に半期分、毎年度末に一年分の3つの異なるサイクルで自己点検を実施するモデルである。

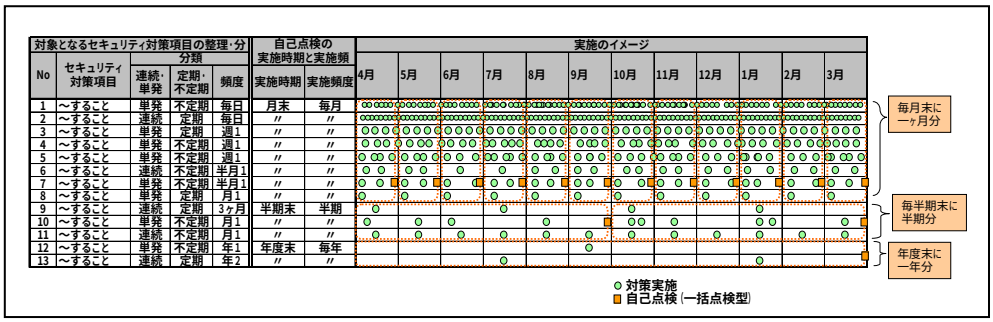


図6．自己点検の実施時期及び実施頻度の検討

- ある特定の時期（例：月末）に負荷が集中するおそれがある場合には、実施時期をずらすなどの工夫が必要である。

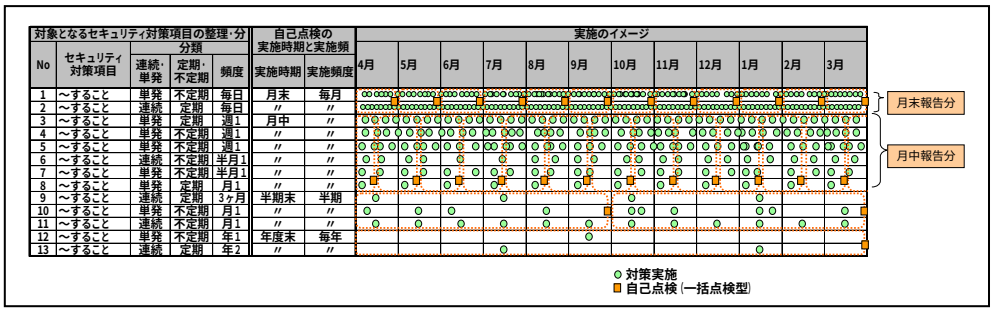


図7．自己点検の実施時期及び実施頻度の検討

- 負荷の軽減と平準化を図るためには、実施頻度と実施時期を考慮すべきである。そのためには、以下に示すように、一部の項目について実施頻度を下げるとともに、実施時期を順次ずらすなどの方法が有効である。

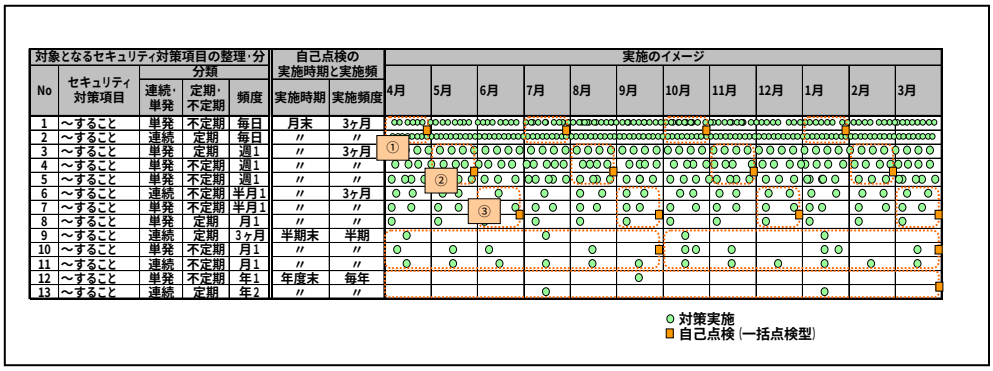


図8．自己点検の実施時期及び実施頻度の検討

(4) 適用範囲の整理 (Step B-4)

自己点検項目一覧に記載されたそれぞれの項目に対して、その実施主体（情報セキュリティ関係規程の「主語」）、管理者、責任者などを明確にする。なお、この情報は、自己点検結果の集約ルートを決定する際に必須となる。

また、後に自己点検結果を分析・評価した場合に有用と思われる属性を追加しておくことが望ましい。例えば、対象となるシステム（例：全システムが対象、モバイルＰＣが対象、メールシステムが対象等）や、ライフサイクル（例：システム開発時に適用、情報の保存時に適用等）などが挙げられる。

(5) 自己点検の回答項目の作成 (StepB-5)

実施主体における自己点検は、原則として当該実施主体による自己申告形式であるが、その回答項目は、Step B-2 において検討を行った自己点検方法（随時点検型/一括点検型/断面調査型）の区別により異なったものとなる。

(I)随時点検型の場合には、その回答は対策実施した事実とその日時を回答することが基本となる。

(II)一括点検型の場合には、その回答は実施状況、すなわち実施した(Yes)又は実施しなかった(No)による回答が基本となる。ただし、実施状況や遵守できていない場合の理由等をより詳細に把握し、今後の改善に結び付けていくため、あるいは、実施すべき対策についての認識が不十分である等の理由により自己点検の実施によって教育的な効果も期待する場合には、以下のようなアンケート形式の選択肢も有効である。

- 適切に実施している（Yes）
- 通常実施しているが、今回は実施していない（No）
  - ○ 今回実施できなかった合理的な理由があるため（自由記入）
  - ○ たまたま実施することを忘却してしまったため
  - ○ 毎回実施することは現実的には困難であるため（自由記入）

- その他（自由記入）

- 恒常的に実施していない（No）
  - 恒常的に実施していない合理的な理由があるため（自由記入）
  - 遵守事項を守ることは現実的には困難であるため（自由記入）
  - 遵守事項が抽象的であり、どう実施してよいか判断が難しいため
  - 遵守事項の存在を認識していなかったため
  - その他（自由記入）

- 該当しない(NA)
  - 既に例外承認済みであるため
  - 現在、例外申請中であるため
  - そもそも対象外であるため
  - 当該セキュリティ対策を必要とする事象が発生しなかったため
  - その他（自由記入）

(III)断面調査型の場合には、その回答は調査時点でのセキュリティ対策状態を回答することが基本となる。例えば、ウイルスパターン定義ファイルの最新化を求める対策の場合には、ウイルスパターン定義ファイルのバージョン番号を、適切なアクセス制御を求める対策の場合には、その Access Control List （アクセス制御に関する設定ファイル）の提出を求めるものである。

なお、自己点検は、その情報セキュリティ対策実施状況を忠実に自己申告することが大前提であり、回答者が虚偽の申告（No であることを隠して Yes と回答する等）を行ったり、不適切な申告（自己点検項目の中身を理解せず全部 Yes と回答する等）を行ったりすることのないようにする必要がある。すなわち、忠実に自己申告することを実施手順書において改めて確認するとともに、No と回答した場合の対応手順を明確にするほか、システム化によって回答者の負荷を軽減したり、明確な質問として回答しやすくする等の配慮が求められる。

(6) 情報セキュリティ監査における調査方法 (Step B-6)

なお、本解説書の範囲外ではあるが、自己点検結果を踏まえて実施される情報セキュリティ監査における調査方法も合わせて検討しておくと効率的である。情報セキュリティ監査における調査方法としては、主に以下のものがある。詳細は、セキュリティ監査に関するマニュアル類を参照のこと。

- 質問
- 査閲
- 観察
- 点検

以上、自己点検項目の整備(Step B)を行うに当たっては、以下の図 9 に示すような整理表を用いて作業を行うとよい。

	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	政府機関統一基準との対応	分類			点検方法			実施時期＆頻度		適用範囲			回答項目		監査における調査方法
			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・取扱制限を明示すること。	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と。	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	6.1.3 (3)(e)	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 A-3	StepA-4	Step B-1			Step B-2			Step B-3		Step B-4			Step B-5		Step B-6

注：本検討例では、自己点検の対象となるセキュリティ対策項目の例として典型的な５つの対策を列記したが、実際には、これらを所管する情報セキュリティ責任者が必ずしも一致するものではない。

図 9. 自己点検項目の整備(Step B)における整理表の例

4.3　自己点検票の集約ルートの検討 (Step C)

実施主体によって記入された自己点検票は、情報セキュリティ責任者へ集約し、最終的に自己点検の結果を最高情報セキュリティ責任者に集約することが必要となる。

自己点検票を集約するに当たっては、概ね以下の３つの集約ルートが想定されるところ、情報セキュリティ責任者は、自己点検の規模、指揮命令系統の構造、確認・評価の実施方法などをかんがみ、適切な集約ルートを選択する必要がある。

(1) 行政事務の指揮命令系統を軸とした集約ルート（図 10 参照）

実施主体は、行政事務遂行上の指揮命令系統における上司に当たる者へ自己点検票を提出し、順次、この指揮命令系統に沿って回収し、最終的に情報セキュリティ責任者へ集約するルートである。この集約ルートでは、行政事務遂行上の指揮命令系統における上司を経由させることによって、統制機能が作用し、対策の実態をより適切に反映した回答を得ることが期待できる。また上司による改善指導も期待できる。そのため、実施主体（回答者）が行うべきセキュリティ対策について、上司が十分認識している場合には有効な方法である。

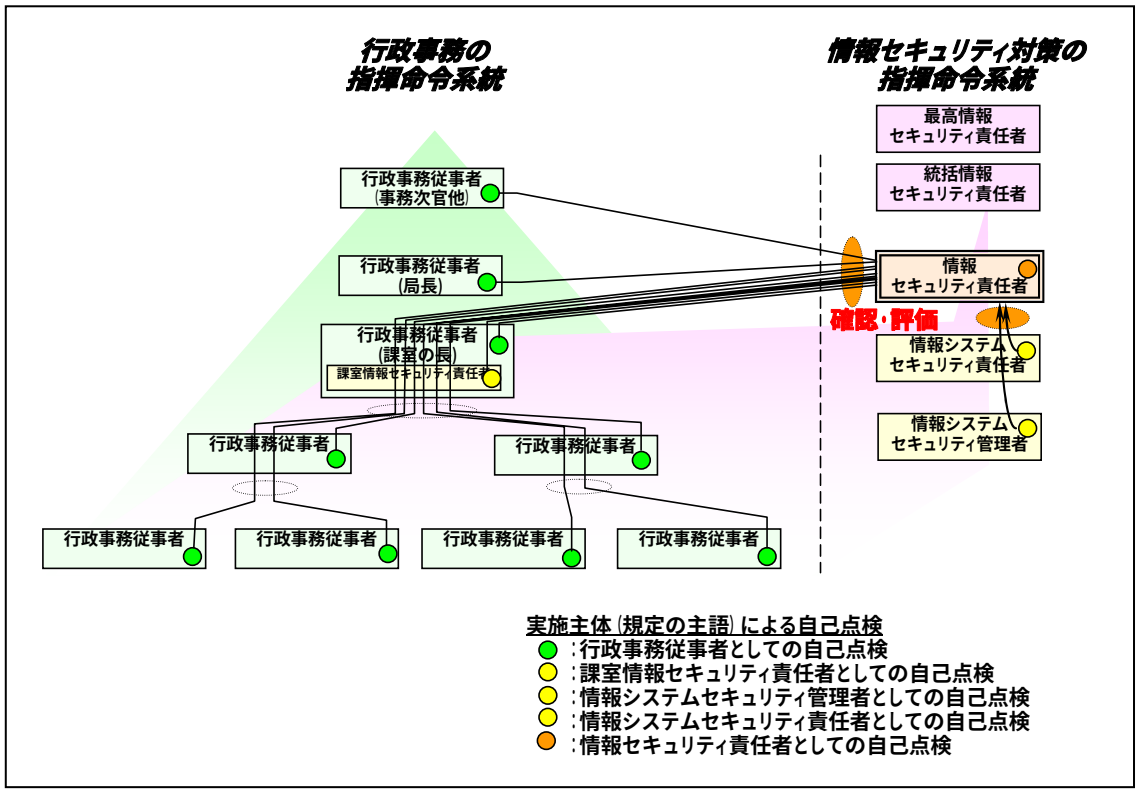


図 10. 行政事務の指揮命令系統を軸とした集約ルート

(2) 情報セキュリティ対策の指揮命令系統を軸とした集約ルート（図 11 参照）

実施主体は、情報セキュリティマネジメント上の本来の集約ルートである情報システムセキュリティ管理者に自己点検票を提出し、情報システムセキュリティ責任者を経由して情報セキュリティ責任者へ集約するルートである。この集約ルートでは、情報セキュリティ対策の責任分担が明確化されているため、情報システムセキュリティ責任者や情報システムセキュリティ管理者が、各実施主体（回答者）との

面識がある場合など、適切な意思疎通が可能な場合には有効な方法である。

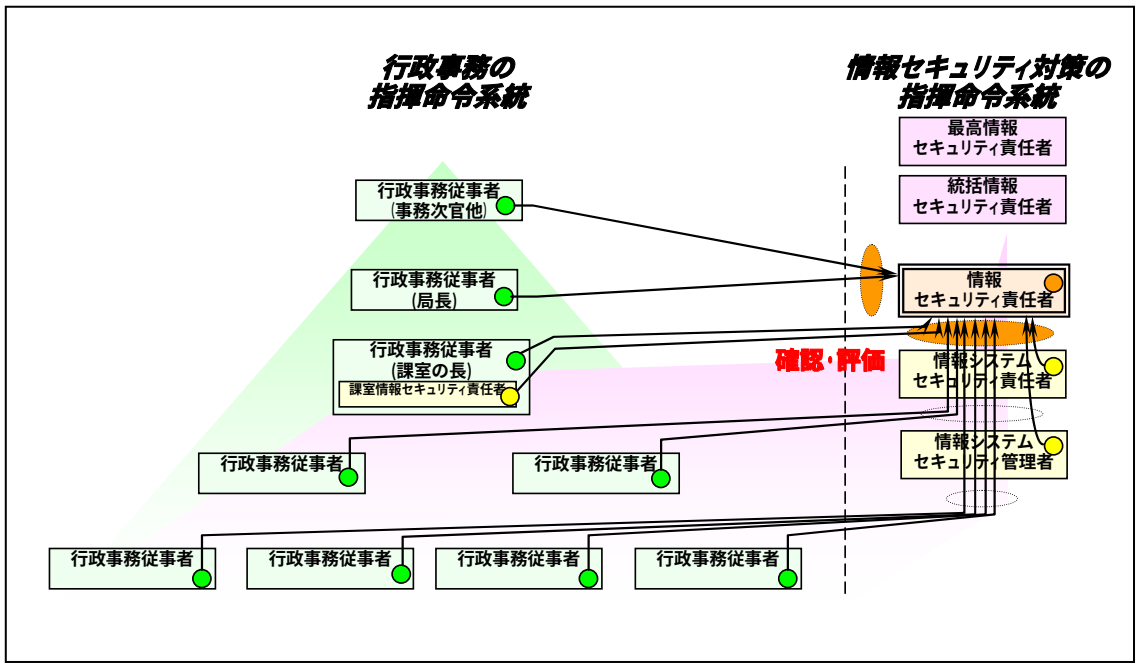


図 11. 情報セキュリティ対策の指揮命令系統を軸とした集約ルート

(3) 情報セキュリティ責任者へ直接提出する集約ルート（図 12 参照）

最も簡素な（オーバーヘッドの少ない）集約ルートであり、自己点検を実施する範囲が小規模な場合には有効な方法である。

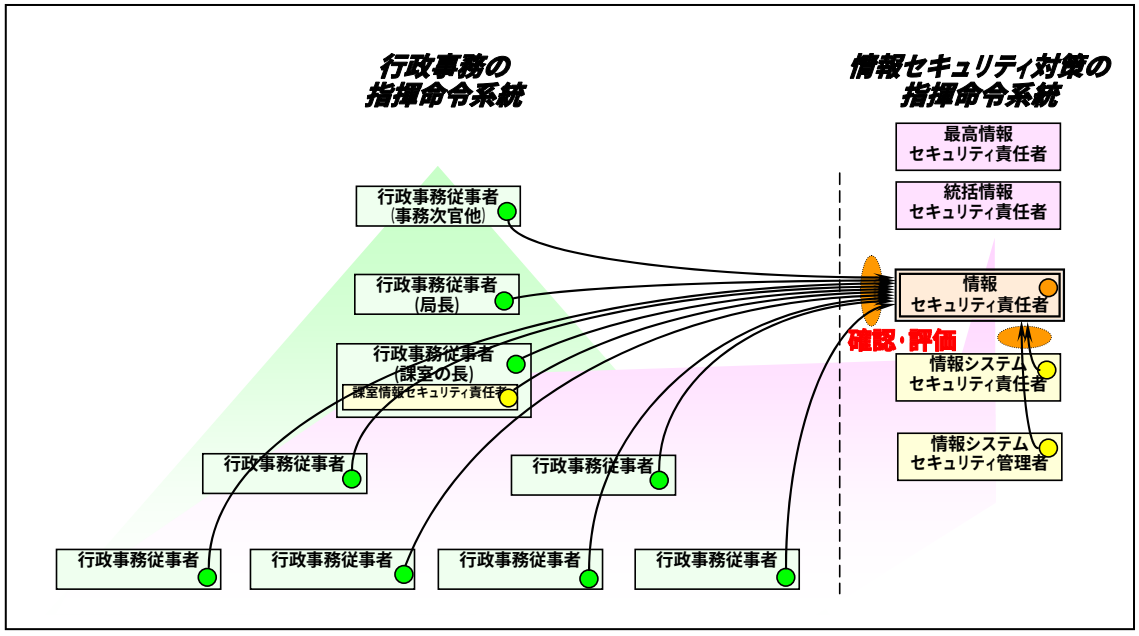


図 12. 情報セキュリティ責任者へ直接提出する集約ルート

4.4　自己点検結果の確認・評価に関する委任の検討 (Step D)

自己点検の回答については、本来、情報セキュリティ責任者がそれを確認・評価するものであるが、大規模な自己点検を実施する場合には、情報セキュリティ責任者にその負荷が集中する可能性がある。そのため、作業の効率性や自己点検結果の正確性を向上させることを目的として、確認・評価に係る作業の一部を、行政事務の管理責任を有する者や、情報セキュリティ対策の管理責任を有する者（課室情報セキュリティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者等）に委任することができる。

自己点検結果の確認・評価に係る作業の一部を委任する場合には、自己点検の実施準備の段階で十分な検討を行い、委任される者に対して作業内容を具体的に説明する指示書を作成した上で事前に説明する必要がある。

図 10 に示した「行政事務の指揮命令系統を軸とした集約ルートの場合」について、情報セキュリティ責任者が行うべき確認・評価の一部を行政事務における管理責任者へ委任した例を図 13 に示す。この例は、行政事務従事者の記入内容をその上席者が「一次確認」し、その結果について課室情報セキュリティ責任者が「二次確認及び評価」を実施するモデルである。

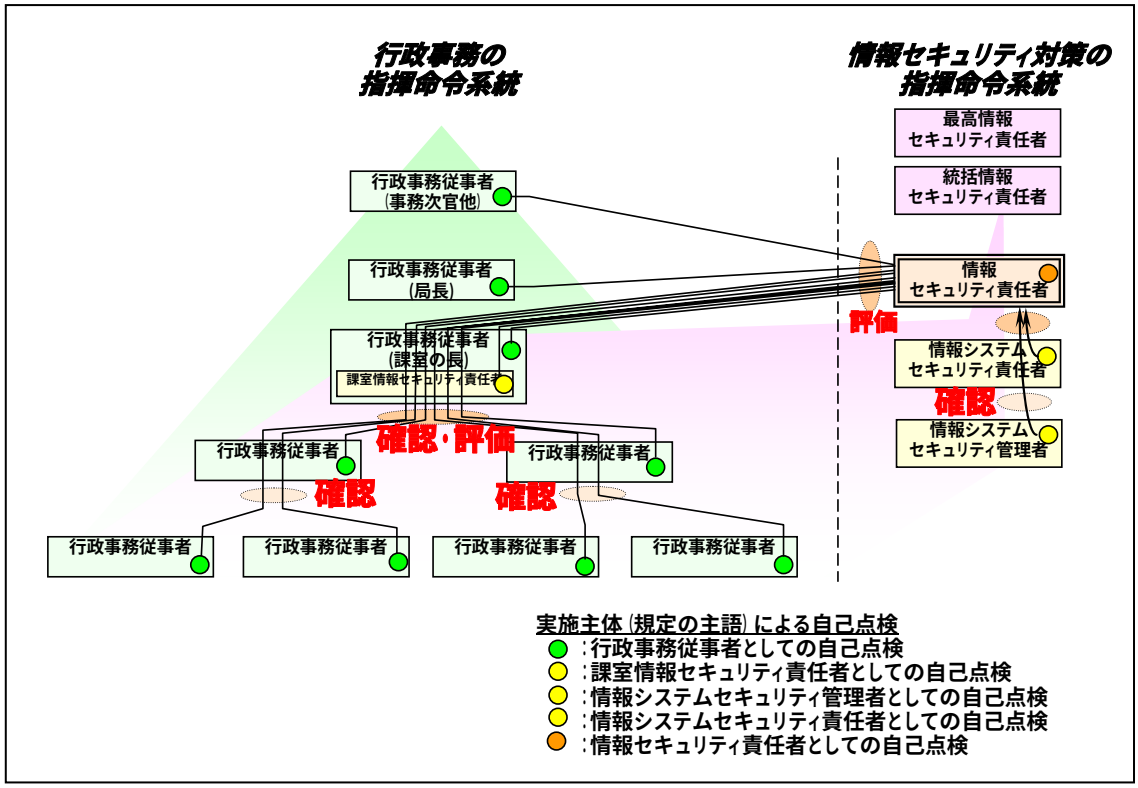


図 13. 確認・評価を委任した例

確認・評価の委任に係る留意事項は以下のとおりである。

- 実施主体から提出された自己点検票は必ずしも情報セキュリティ責任者に送付し、同人において保管する必要はないが、参照が求められた際に迅

速に提示できるよう適切に管理するとともに、あらかじめ定められた期間、適切に保管する必要がある。例えば、物理的な保管場所の確保の観点から、すべての自己点検票を情報セキュリティ責任者へ集めることが困難であると予想される場合には、その確認・評価を行った者が分散してこれらを保管することが望ましい。

- 確認・評価に係る作業の一部を委任した場合であっても、確認・評価の最終的な責任は情報セキュリティ責任者が有することに注意すること。

4.5 自己点検票への展開 (Step E)

Step B で作成された整理表をもとに、職位・職階・役割ごとに自己点検票への展開を行う。

(1) 実施主体の職位・職階・役割を考慮して自己点検票への展開(Step E-1)

実施主体となる職位・職階・役割ごと（すべての行政事務従事者、情報セキュリティ責任者、課室情報セキュリティ責任者、情報システムセキュリティ管理者等）に、それぞれ実施すべき自己点検項目を抽出して自己点検票の原票を作成する。なお、一括点検型の自己点検については、その実施時期及び実施頻度に応じて、複数種類の自己点検票を準備する必要がある。（図 14 参照）

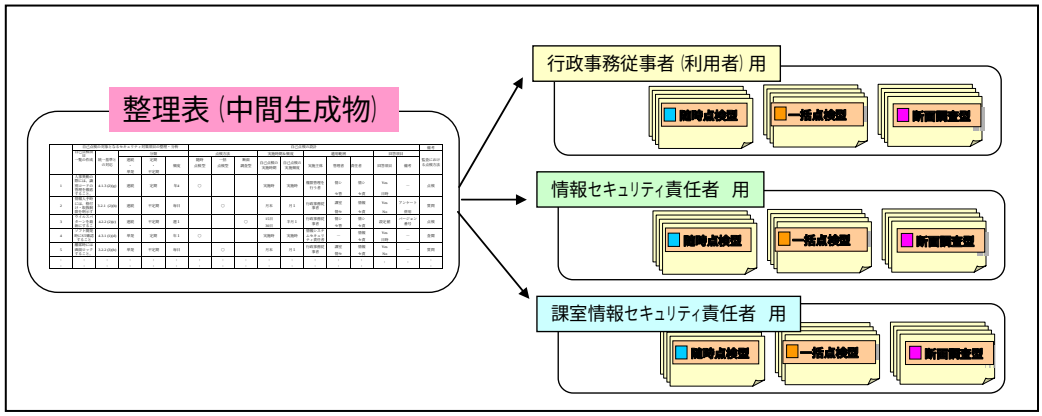


図 14. 自己点検票への展開

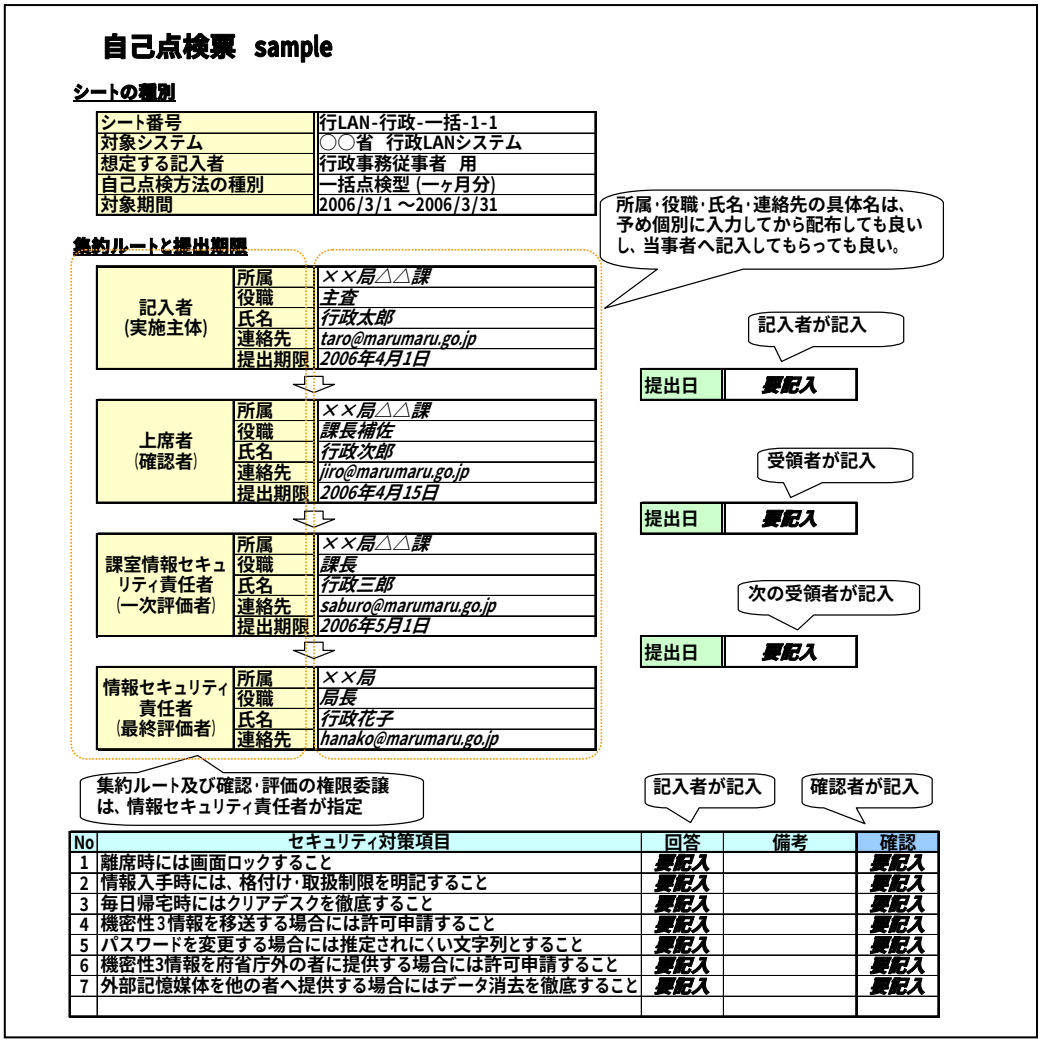
(2) 関連する情報の付加(Step E-2)

上記で作成された自己点検票の原票に対して、以下の関連情報を付加する。（図 15 参照）

- シートの種別（シート番号）
- 対象システム
- 想定する記入者
- 自己点検方法の種別
  - ○ 一括調査型
  - ○ 随時点検型

○ 断面調査型

- 集約ルートと提出期限
- 記入者の所属、役職、氏名、連絡先
- 提出日



自己点検票　sample

シートの種別

シート番号	行LAN-行政-一括-1-1
対象システム	○○省　行政LANシステム
想定する記入者	行政事務従事者　用
自己点検方法の種別	一括点検型 (一ヶ月分)
対象期間	2006/3/1 ～2006/3/31

所属・役職・氏名・連絡先の具体名は、予め個別に入力してから配布しても良いし、当事者へ記入してもらっても良い。

集約ルートと提出期限

記入者（実施主体）	所属	××局△△課
	役職	主査
	氏名	行政太郎
	連絡先	taro@marumaru.go.jp
	提出期限	2006年4月1日
上席者（確認者）	所属	××局△△課
	役職	課長補佐
	氏名	行政次郎
	連絡先	jiro@marumaru.go.jp
	提出期限	2006年4月15日
課室情報セキュリティ責任者（一次評価者）	所属	××局△△課
	役職	課長
	氏名	行政三郎
	連絡先	saburo@marumaru.go.jp
	提出期限	2006年5月1日
情報セキュリティ責任者（最終評価者）	所属	××局
	役職	局長
	氏名	行政花子
	連絡先	hanako@marumaru.go.jp

記入者が記入　提出日　要記入

受領者が記入　提出日　要記入

次の受領者が記入　提出日　要記入

集約ルート及び確認・評価の権限委譲は、情報セキュリティ責任者が指定

No	セキュリティ対策項目	回答（記入者が記入）	備考	確認（確認者が記入）
1	離席時には画面ロックすること	要記入		要記入
2	情報入手時には、格付け・取扱制限を明記すること	要記入		要記入
3	毎日帰宅時にはクリアデスクを徹底すること	要記入		要記入
4	機密性3情報を移送する場合には許可申請すること	要記入		要記入
5	パスワードを変更する場合には推定されにくい文字列とすること	要記入		要記入
6	機密性3情報を府省庁外の者に提供する場合には許可申請すること	要記入		要記入
7	外部記憶媒体を他の者へ提供する場合にはデータ消去を徹底すること	要記入		要記入

図 15. 自己点検票の例

4.6　行政事務従事者ごとに再構成 (Step F)

実施主体となる職位・職階・役割ごとに作成された自己点検票をもとに、それを実際の行政事務従事者ごとに再構成する。

(1) 行政事務従事者ごとの再構成 (Step F-1)

実際の運用においては、一人の行政事務従事者が、システムの利用者としての立場のほかに、管理者あるいは責任者等の複数の立場で情報セキュリティ対策を実施する場合がある。そのため、自己点検の実施対象となるすべての行政事務従事者の

それぞれに対して、その情報セキュリティ対策上の立場を個別に考慮して、必要とされる自己点検項目を、統合・再構成する必要がある。以下の図 16 に、行政事務従事者のAさんが課室情報セキュリティ責任者としての自己点検及び行政事務従事者（利用者）としての自己点検を実施する場合の例を示す。

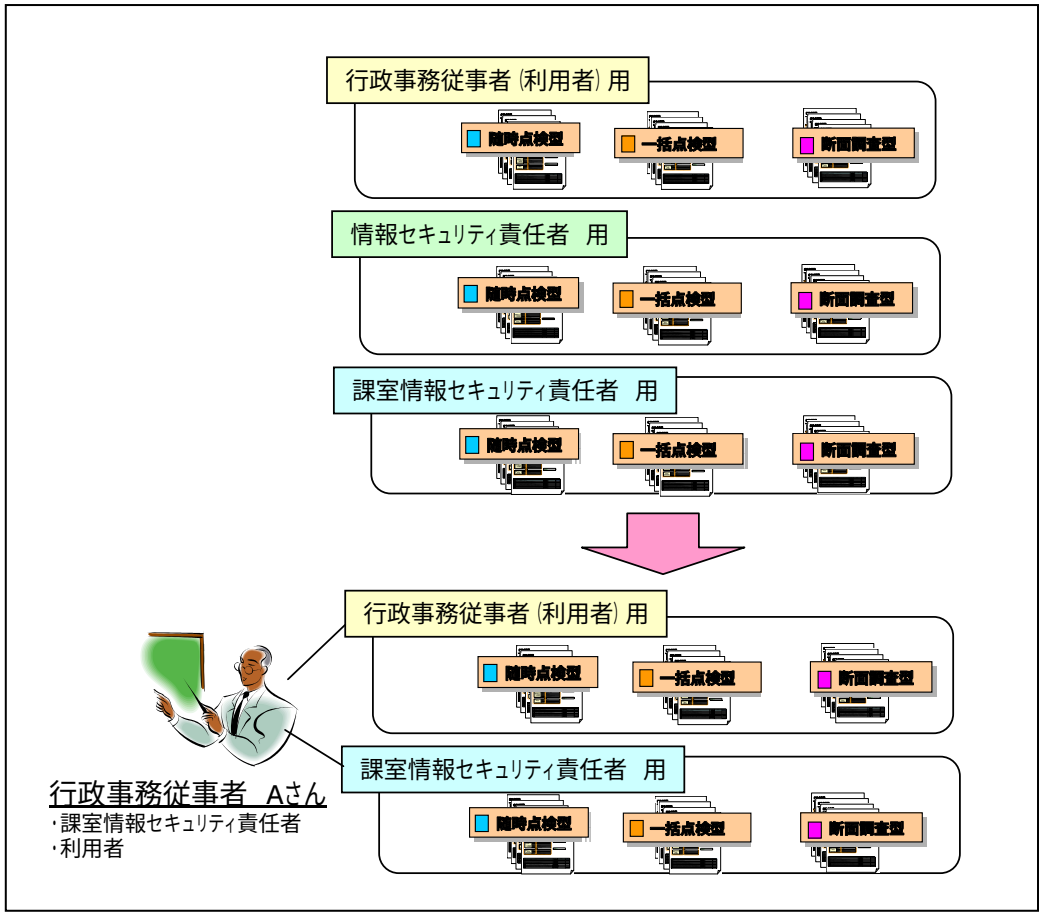


図 16. 自己点検実施の例

なお、複数の情報システムを取り扱う場合には、それぞれの情報システムに、それぞれの情報セキュリティ対策上の立場から要請される自己点検を行うことが求められる。

4.7 自己点検の実施環境の整備 (Step G)

自己点検は、情報セキュリティの管理単位ごとに、それに係るすべての行政事務従事者が実施するものであること、行政事務従事者ごとに実施内容が異なるものであること、実施主体による回答結果を情報セキュリティ責任者へ提出するに当たっては複数の関係者を経由する可能性があること、情報セキュリティ責任者による確認・評価が別の者に委任される可能性があること等をかんがみ、その実施環境を整備しておくことが望ましい。

情報セキュリティ責任者の所管する単位が小規模であれば、紙媒体による回答用紙の配布、記入、回覧、分析が可能であるが、より効率的に自己点検を実施する必要がある場合や当該単位が大きい場合には、電子メールの添付ファイルによる回答用紙の送付のほか、ワークフロー環境（電子決裁システム等）の利用、Web フォームによる回答・集約、自動集計、自動分析などの環境を整備することが望ましい。

5. 自己点検の実施　（ 2.3.1 (3) ）

5.1 情報セキュリティ責任者による実施の指示

政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検

(3) (a)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が定める年度自己点検計画に基づき、行政事務従事者に対して、自己点検の実施を指示すること。

【基本遵守事項】

統括情報セキュリティ責任者が定める年度自己点検計画は、府省庁全体の自己点検計画であり、情報セキュリティ対策の運用に係る単位、すなわち情報セキュリティ責任者の所管する単位ごとに実施される自己点検の集合体として整合的に構成される。そのため、各情報セキュリティ責任者は、年度自己点検計画に基づき、自らの所管する情報セキュリティの運用単位について自己点検を実施することが求められる。また、自己点検の実施に当たって、情報セキュリティ責任者は、当該運用単位に関与するすべての実施主体（行政事務従事者のほか、情報システムセキュリティ責任者、情報システムセキュリティ管理者及び課室情報セキュリティ責任者を含む。）に対して自己点検の実施を指示する必要がある。

自己点検実施の指示においては、以下の事項を明示する。

- 自己点検を実施する対象（システム名称等）と自己点検項目
- 自己点検の記入方法や留意事項
- 自己点検結果の提出先及び提出方法
  提出方法の例：
  - 情報セキュリティ責任者に直接提出
  - 行政事務の指揮命令系統に沿って提出
  - 情報セキュリティ対策の指揮命令系統に沿って提出
  - 統一窓口へ提出
  - 紙面による提出
  - ワークフローの活用
  - Webフォーム入力
- 自己点検結果の提出期限

自己点検実施指示書の雛形を付録２に示す。

5.2 行政事務従事者（実施主体）による実施

政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検

(3) (b) 行政事務従事者は、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実施手順を用いて自己点検を実施すること。
【基本遵守事項】

情報セキュリティ関係規程に定められた遵守事項の実施主体本人による自己点検を実施する。その回答結果は、情報セキュリティ対策を把握する際の基本的な資料となる。このため、その実施においては、情報セキュリティ責任者の指示に行政事務従事者が従って自己点検することが重要である。

5.3 情報セキュリティ責任者による実施状況の確認

各行政事務従事者に対して、自己点検結果の提出期限を示してその実施を指示したのであるから、期限に従って提出することは、行政事務従事者の責任である。

しかし、情報セキュリティ責任者が所管する運用単位における、すべての自己点検が遅滞なく完了することについては、情報セキュリティ責任者も責任を担う。

そのためには、多くの行政事務従事者が関わることから、情報セキュリティ責任者は、彼らの実施状況の進捗度合いを管理することが重要である。最終的な期限になる前に、途中の進捗などを随時確認し、予定よりも遅れている者がいれば期限の再周知や実施の催促をするなどして、実施状況を確認し、必要な対応を取る。

6. 自己点検結果の評価　（ 2.3.1 (4) ）

実施主体によって実施された自己点検の結果について、情報セキュリティ責任者による確認・評価が行われる。さらに、情報セキュリティ責任者による自己点検が適切に行われているかを統括情報セキュリティ責任者が確認・評価し、その結果を最高情報セキュリティ責任者が評価する。

6.1 情報セキュリティ責任者による確認・評価

> **政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検**
> (4) (a) 情報セキュリティ責任者は、行政事務従事者による自己点検が行われていることを確認し、その結果を評価すること。
> 【基本遵守事項】

情報セキュリティ責任者は、所管する情報セキュリティ対策運用の単位全体について、自己点検が適切に行われていることを確認し、その結果を評価する必要がある。

(1) 情報セキュリティ責任者による確認・評価においては、主に以下の観点からの確認・評価を行う。

- 行政事務従事者による自己点検が実施されたかを確認する。すなわち、全員が自己点検を実施したかを確認する。
- 回答の不備（記入ミス（期待する回答形式と異なる回答をしている）や記入漏れ（回答すべきところに回答がされていない））の有無を確認する。回答の不備を発見した場合には、実施主体に対して回答の再提出を指示すること。なお、回答の不備の検出については、システム的な仕組みを構築するなどして、作業負荷を軽減することも検討すべきである。
- 必要に応じて、行政事務従事者へ内容を確認する。実施主体の回答結果に矛盾があると思われる場合には、実施主体又はその管理責任者に対して、その内容を確認する。たとえば、情報システムの対策において、求められた機能の導入がされていないのに当該機能の運用がされているという場合には、あるはずのない機能が運用されていることになる。そのような場合には、回答内容について確認をして適切な回答にする必要がある。
- 回答を集計し、所管単位における数値評価を行う。自己点検項目ごとに、実施数 / 回答数　により実施率を把握したり、実施主体ごとの実施率を把握したりすることが考えられる。

(2) 個々の回答を受領した段階で随時点検するのか、回答をすべて受領した段階で一括して点検するのか等は任意であり、実施主体による自己点検の実施時期及び実施頻度と必ずしも一致させる必要はない。しかしながら、統括情報セキュリティ責任者が定める年度自己点検計画のスケジュールに整合するよう、確認・評価を実施しなければならない。

(3) 情報セキュリティ責任者は、自己点検結果に関する報告書を作成し、統括情報

セキュリティ責任者へ提出する。

なお、情報セキュリティ責任者による確認・評価の一部を委任するに当たっては、事務作業のみの委任、事務作業及び判断作業の委任など様々な選択肢があるが、状況に応じて適切に判断すること。ただし、確認・評価の最終的な責任は情報セキュリティ責任者が有することに注意すること。

6.2 統括情報セキュリティ責任者による確認・評価

政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検

(4) (b) 統括情報セキュリティ責任者は、情報セキュリティ責任者による自己点検が行われていることを確認し、その結果を評価すること。
【基本遵守事項】

統括情報セキュリティ責任者に、情報セキュリティ責任者による自己点検が適切に行われていることを確認し、現状の情報セキュリティ対策状況を評価することが求められる。

(1) 統括情報セキュリティ責任者による確認・評価においては、主に以下の観点から確認・評価を行う。

- 情報セキュリティ責任者による自己点検が実施されたかを確認する。すなわち、全員が自己点検を実施したかを確認する。
- 提出内容の不備の有無を確認する。提出内容の不備を発見した場合には、情報セキュリティ責任者に対して提出内容の再提出を指示すること。
- 必要に応じて、情報セキュリティ責任者へ内容を確認する。情報セキュリティ責任者の提出内容に矛盾があると思われる場合には、情報セキュリティ責任者に対して、その内容を確認する。
- 回答を集計し、数値評価を行う。自己点検項目ごとに、実施数 / 回答数により実施率を把握したり、実施主体ごとの実施率を把握したりすることが考えられる

6.3 最高情報セキュリティ責任者への報告

政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検

(4) (c) 統括情報セキュリティ責任者は、自己点検の結果を最高情報セキュリティ責任者へ報告すること。
【基本遵守事項】

統括情報セキュリティ責任者に、自己点検を確認・評価した結果を最高情報セキュリティ責任者へ報告することを求める事項である。

7. 自己点検に基づく改善　（ 2.3.1 (5) ）

自己点検結果に基づく改善では、行政事務従事者自身による自己改善と、最高情報セキュリティ責任者による改善指示の２つの方法が挙げられる。

前者は、ボトムアップ的な改善であり、自己点検の結果に基づき、自己の権限の範囲で改善できると判断した事項へ対処するものである。政府機関統一基準 2.3.1 (5)(a) に記す遵守事項がこれに相当する。

後者は、トップダウン的な改善であり、最高情報セキュリティ責任者が情報システムの自己点検結果を評価し、必要があると判断した場合には情報セキュリティ責任者に改善を指示するものである。政府機関統一基準 2.3.1 (5)(b)に記す遵守事項がこれに相当する。

7.1 行政事務従事者自身による自己改善

> **政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検**
> (5) (a) 行政事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、情報セキュリティ責任者にその旨を報告すること。
> 【基本遵守事項】

行政事務従事者自身による自己改善には、実施主体の自発によるものと、情報セキュリティ責任者の指導によるものがある。本事項では、自己点検を行い気付いた問題点で自己の権限の範囲で改善できることがあれば、自己点検結果の集計や監査結果を必ずしも待たなくとも、適宜改善することを求めている。

(1) 実施主体は、自己点検によって実施していないセキュリティ対策を認識した際に、それを自己の権限の範囲で改善できると判断した場合は、それを適時改善する必要がある。以下に例を示す。

- 遵守事項について失念していただけで、直ちにそれを実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法について直ちに実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法の実施が困難で現状の方法を続けるために例外措置の手続きを取る場合。

なお、そもそも情報セキュリティ関係規程の定める遵守事項が現実的ではない等の理由により、情報セキュリティ関係規程自体を改訂すべきと思われる場合については、まず省庁対策基準により例外措置の適用を申請した上で、情報セキュリティ対策における管理責任者又は情報セキュリティ責任者へ

相談すること。

遵守事項を実施できない合理的理由がある場合は、例外措置の適用を申請することで、遵守事項が求める対策を実施せずとも遵守事項違反にはならない。しかし、例外措置の適用を申請することなく、遵守事項が求める対策を実施しないことは、違反となることに注意すること。

(2) 情報セキュリティ責任者（委任された者等を含む。）は、その所管する範囲で違反を発見した場合には、どのような理由によって実施主体が遵守事項を実施できなかったのかを十分調査した上で、管理責任者として部下への改善指導を行う。

- 違反した実施主体への直接指導
- 違反した実施主体の管理責任者への指導

(3) 行政事務従事者は自己改善を行なった場合には、以下の事項について情報セキュリティ責任者への報告を行うこと。

- 違反した情報セキュリティ関係規程
- 違反した理由・背景
- 改善事項
- その他

7.2 最高情報セキュリティ責任者による改善指示

政府機関統一基準　　2.3.1 情報セキュリティ対策の自己点検

(5) (b) 最高情報セキュリティ責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には情報セキュリティ責任者に改善を指示すること。
【基本遵守事項】

最高情報セキュリティ責任者が自己点検の結果を全体として評価し、必要に応じて情報セキュリティ責任者に改善を指示するに当たっては、以下の観点が考えられる。

(1) 情報システム又は課室に関する自己点検の結果を踏まえ、改善する必要があることが明らかになった事項について改善を指示する。

(2) ある情報システム又は課室に関する自己点検の結果を踏まえ改善する必要があることが明らかになった事項が、他の情報システム又は課室にも該当する可能性が高い場合には、併せて改善を指示する。

また、改善するに当たっては、どのような理由によって遵守事項が実施されていないのかを十分調査した上で対応方法を検討する必要がある。以下に改善指示の例を示す。

- 実施主体（行政事務従事者）による遵守の徹底
- システム的な仕組みの整備による、実施主体（行政事務従事者）の負荷の軽減

- 情報セキュリティ関係規程における記述の詳細化・具体化
- 情報セキュリティに関する教育の見直し
- 情報セキュリティ関係規程の見直し、政府機関統一基準へのフィードバック
- 例外措置の申請

付録編

雛形の利用方法

雛形において想定する前提

これらの雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 情報セキュリティ対策の運用に係る単位が定められ、その単位ごとに情報セキュリティ責任者が設置されている。
- 当該運用単位において、情報セキュリティ責任者以下、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者が設置されている。
- 政府機関統一基準が省庁対策基準へ適切に反映されており、また、必要に応じて実施手順が整備されている。すなわち、当該運用単位における情報セキュリティ関係規程が整備されており、情報セキュリティ対策を実施するに当たって行政事務従事者自らが実施すべき具体的な対策項目が明確になっている。

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対策基準に準拠した「年度自己点検計画」及び「自己点検の実施手順」を策定する手順には、以下の事項を踏まえて作業を行う必要がある。

(1) 各府省庁において所有する情報システムの数及び規模、それに係る行政事務従事者の数、各府省庁における情報セキュリティ対策状況や情報セキュリティ対策体制等を踏まえ、実効的な実施手順とすること。特に、自己点検に係る者に過度の作業負荷を強いることのないよう配慮する。

(2) 実施手順（雛形）において*[・・・]* 形式で示す設定値（システム名称、担当者名、文書名等）については、各府省庁内の定めに合わせる。

(3) 実施手順（雛形）において【・・・の場合】形式で示す記述については、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。

(4) 自己点検や情報セキュリティ監査に関してマニュアル、ガイドライン等を作成する場合には、それらとの整合性を考慮し、適切に分割、統合、相互参照する。

付録１：年度自己点検計画の雛形

作成日：*[○○年○月○日]*
統括情報セキュリティ責任者
[　氏　名　]

[○○年度]　*[×××省]*　自己点検計画

1. 本自己点検計画の位置付け

本自己点検計画は、各情報セキュリティ責任者が所管する単位で自己点検を行うに当たり、省全体として効率的かつ整合的に実施するための計画である。

2. 自己点検の実施方針

本年度の自己点検は、以下の方針で実施する。

2.1　実施頻度

(1) 自己点検は、各点検項目について、年間を通じて*最低[1]回以上* 実施する。

(2) ただし、情報システムの運用に係る点検項目については、年間を通じて*最低[2]回以上* 実施する。

2.2　実施時期

(1) 情報セキュリティ責任者は、*[10 月 31 日]* までに自己点検の確認・評価結果を統括情報セキュリティ責任者へ提出すること。

(2) 行政事務従事者（実施主体）による自己点検の実施時期は、自己点検項目それぞれの実施頻度や上記の提出期限を考慮の上、情報セキュリティ責任者が定めること。通年で日々実施する対策以外の、特定の時点や期間に実施する対策については、対策実施後遅滞なく随時自己点検を実施すること。

2.3　確認及び評価の方法

(1) 行政事務従事者による自己点検が実施されたか（全員が自己点検を実施したか）を確認する。

(2) 以下の数値評価を行う。

- 実施主体（自己点検項目の主語）ごとの実施率（＝実施数 / 回答数）
- 自己点検項目ごとの実施率

3. 自己点検の全体スケジュール

（詳細を別紙で添付する）

付録２：自己点検実施指示書の雛形

[○○○号]
[平成□年□月□日]

[○○システムの全利用者] 殿

[○○システム] 情報セキュリティ責任者
[○○局長　　行政花子]

[○○システム] に係る自己点検の実施について

1. 自己点検の実施

（自己点検を実施する趣旨を記述する。）

2. 自己点検の対象者

2.1 対象者

【利用者を対象者とする場合の記述例】

本自己点検は、*[○○システム]*を利用するすべての行政事務従事者を対象とする。

【情報システムセキュリティ責任者及び情報システムセキュリティ管理者を対象者とする場合の記述例】

本自己点検は、*[○○システム]*における情報システムセキュリティ責任者及び情報システムセキュリティ管理者を対象とする。

3. 自己点検の対象システム及び関係規程

3.1 自己点検を実施する対象システム

本自己点検は、*[○○システム]*を対象とする。

3.2 対象となる情報セキュリティ関係規程

本自己点検は、以下に示す規程に記載された事項を自己点検の項目とする。

- *[○○システム運用管理規定 ver1.3]*
- *[○○システム利用者の手引 ver2.2]*

4. 自己点検票（一式）の入手方法

【本実施指示書に添付する場合】

対象者は、本通達に添付された自己点検票を使用すること。

【自己点検に関するウェブページからダウンロードする場合】

対象者は、以下 URL より自身の自己点検票をダウンロードして使用すること。

[http://○○.go.jp/security/self-check/index.html]

5. 自己点検票（一式）の構成

シート No	シート名称	自己点検方法	対象者（実施主体）	
[○○-11]	*[○○]*	*[一括点検型]*	*[課室情報セキュリティ責任者]*	
[○○-12]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-13]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-14]	*[○○]*	*[随時報告型]*	*[課室情報セキュリティ責任者]*	
[○○-15]	*[○○]*	*[随時報告型]*	*[利用者]*	*[○]*

【利用者を対象者とする場合の記述例】

これらの自己点検票（一式）のうち、利用者を実施対象とした自己点検票（上表右列の○を付した自己点検票）を用いること。

6. 自己点検票の記入時の留意事項

(1) 対象者は、虚偽の申告（実施していない事実を隠して「実施した」と回答）をしないこと。

(2) 対象者は、不正確な申告（自己点検項目の中身を理解せず「実施した」と回答）をしないこと。

7. 自己点検結果の提出先

【本実施指示書において明示する場合】

自己点検結果の提出先は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出先
[○○-12]	*[○○]*	*[一括点検型]*	*[課室情報セキュリティ責任者]*
[○○-13]	*[○○]*	*[一括点検型]*	*[課室情報セキュリティ責任者]*
[○○-15]	*[○○]*	*[随時報告型]*	*[課室情報セキュリティ責任者]*

【自己点検票において明示する場合】

自己点検結果の提出先は、各自己点検票の記載のとおりとする。

8. 自己点検結果の提出期限

【本実施指示書において明示する場合】

自己点検結果の提出期限は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出期限
[○○-12]	*[○○]*	*[一括点検型]*	*[2006 年 4 月 30 日]*
[○○-13]	*[○○]*	*[一括点検型]*	*[2006 年 5 月 30 日]*
[○○-15]	*[○○]*	*[随時報告型]*	*[随時報告]*

【自己点検票において明示する場合】

自己点検結果の提出期限は、各自己点検票に記載のとおりとする。

9. 自己点検に基づく改善

9.1 対象者による自己改善

(1) 対象者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善すること。

- 遵守事項について失念していただけで、直ちにそれを実施することができる場合。
- 遵守事項の実施方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法により直ちに実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法の実施が困難で現状の方法を続けるために、例外措置の手続きを取る場合。

なお、そもそも情報セキュリティ関係規程の定める遵守事項が現実的ではない等の理由により、情報セキュリティ関係規程自体を改訂すべきと思われる場合については、まず省庁対策基準により例外措置の適用を申請した上で、情報セキュリティ対策における管理責任者又は情報セキュリティ責任者へ相談すること。

遵守事項を実施できない合理的理由がある場合は、例外措置の適用を申請することで、遵守事項が求める対策を実施せずとも遵守事項違反にはならない。しかし、例外措置の適用を申請することなく、遵守事項が求める対策を実施しないことは、違反となることに注意すること。

(2) 対象者は、自己改善を行なった場合には、以下の事項について情報セキュリティ責任者への報告を行うこと。

- 違反した情報セキュリティ関係規程
- 違反した理由・背景
- 改善事項
- その他

9.2 最高情報セキュリティ責任者による改善指示

最高情報セキュリティ責任者から情報セキュリティ対策の改善指示があった場合には、その趣旨を理解の上これに従うこと。

10. 参考資料

【本実施指示書に添付する場合】
自己点検の概要について、*[別紙○]* に示す。

【自己点検に関するウェブページで公開する場合】
自己点検の概要について、以下 URL を参照のこと。
[http://○○.go.jp/security/self-check/index.html]