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）
平成28年10月12日
一部改定
平成31年4月1日
一部改定
令和7年5月29日
一部改定
令和7年7月1日
一部改定

サイバーセキュリティ基本法（平成26年法律第104号。以下「法」という。）第26条第1項第2号の規定に基づきサイバーセキュリティ戦略本部（以下「戦略本部」という。）がつかさどる事務のうち、監査について、その実施のための基本方針を以下のとおり定める。

1　監査の目的

本監査は、戦略本部がサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、国の行政機関、独立行政法人及び指定法人のサイバーセキュリティ対策に関する現状を適切に把握した上で、これらの組織において対策強化のための自律的かつ継続的な改善機構であるＰＤＣＡサイクルの構築、及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該ＰＤＣＡサイクルが継続的かつ有効に機能するよう助言することによって、これらの組織におけるサイバーセキュリティ対策の効果的な強化を図ることを目的とする。

2　監査の対象

国の行政機関、独立行政法人及び指定法人（以下「行政機関等」という。）を監査の対象とする。

なお、本基本方針において「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関、内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成11年法律第89号）第49条第1項及び第2項に規定する機関、国家行政組織法（昭和23年法律第120号）第3条第2項に規定する機関並びにこれらに置かれる機関をいう。また、本基本方針において「指定法人」とは、法第13条

に規定する指定法人をいう。

3　監査の基本的な方向性

(1) 助言型監査

サイバーセキュリティ対策は、技術や環境の変化に応じて、段階的に実施内容の向上を図ることが重要であるため、監査をそのためのモニタリング機能として位置づけることが有効である。このことを踏まえて、本監査は、被監査主体である行政機関等がサイバーセキュリティ対策を強化する上で有益な助言を行うことを目的とする「助言型監査」を志向する。

また、行政機関等のサイバーセキュリティ対策を全体的に強化するため、それぞれの行政機関等（以下「各機関」という。）が実施している優れた取組（グッドプラクティス）については、他の各機関におけるサイバーセキュリティ対策の強化に資するよう、それらの取組を適切に共有するとともに、サイバーセキュリティ対策を強化する観点からの監査の必要性、有効性について、各機関がより深い理解を得られるよう、丁寧な説明を行う。

(2) 第三者的視点からの監査

監査の客観性、専門性等を確保することを目的として、各機関で実施している内部監査とは独立した、第三者的視点から監査を実施する。

(3) 各機関の状況を踏まえた監査

各機関のサイバーセキュリティ対策の実施状況、体制の整備状況等を踏まえ、各機関におけるサイバーセキュリティ対策に係る課題等について対話し、相互認識と信頼関係を深めるよう努めるとともに、各機関における監査の実施方法を双方協議の上、決定する。

また、各機関におけるサイバーセキュリティ対策の推進体制の発展段階に応じて、監査の内容も段階的に発展させていくよう配慮する。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定

我が国を取り巻くサイバーセキュリティに関する情勢を踏まえて、行政機関等のサイバーセキュリティ対策において、より重要性・緊急性・リスクの高いものから監査テーマを適切に選定する。

4　監査の実施内容

(1) マネジメント監査

「政府機関等の情報セキュリティ対策のための統一基準群」等に基づく施策の取組状況について、国際規格において基本的な考え方である組織全体としてのＰＤＣＡサイクルが有効に機能しているかとの観点から、関係者への質問、資料の閲覧、情報システムの点検等により検証し、改善のために必要な助言等を行う。

また、サイバーセキュリティ対策を強化するための体制等の整備状況についても検証し、改善のために必要な助言等を行う。

なお、上記の検証の一環として、各機関がサイバーセキュリティに係るポリシー等において定めたサイバーセキュリティ対策を適切に実施しているか検証する。

(2) ペネトレーションテスト

インターネットに接続されている情報システムについて、疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。

なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。

(3) レッドチームテスト

政府機関等が整備した情報システムに対し疑似的な攻撃（実際の攻撃者の戦術・技術・手順を模倣した攻撃）を実施し、インシデントの検知能力や対応プロセスまでを組織・システム・人的側面を含めて多面的に評価し、改善のために必要な助言等を行う。

5　監査の進め方

(1) 監査方針の策定

本基本方針を踏まえ、年度ごとの監査の基本的な考え方、前述の監査テーマを含む年度監査方針を、サイバーセキュリティ戦略を実施するために戦略本部が決定する年次計画の一部として策定する。

(2) 監査の実施

(1)の年度ごとに策定する監査方針に基づいて、監査を実施する。監査の実施に当たっては、必要に応じて外部の専門家の協力を得る。

また、過年度の監査実施結果のうち重要な事項については、その改善状況を継続的にフォローアップする。

(3) 個別の監査実施結果の通知

個別の監査実施結果については、改善のために必要な助言等を含めて、各機関の最高情報セキュリティ責任者（ＣＩＳＯ）へ通知する。

なお、重要な事項については、改善策の提案を含めて通知する。また、独立行政法人及び指定法人における監査実施結果については、所管府省庁を通じて通知する。

通知を受けた各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は改善計画を戦略本部に報告するものとする。なお、独立

行政法人及び指定法人は所管府省庁を通じて報告を行うものとする。

(4) 監査実施結果の取りまとめ・報告

サイバーセキュリティの特性を踏まえ、攻撃者を利することにならないよう配慮した形で、当該年度に実施した監査の結果を取りまとめる。戦略本部は、当該結果について、報告を受ける。

(5) 監査事務の処理

以上の監査事務については、内閣官房国家サイバー統括室に実施させる。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、法第 31 条第 1 項第 1 号の規定に基づき独立行政法人情報処理推進機構に委託し、同機構に実施させる。