

「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」の一部改正について

資料 3-1 「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」の一部改正について（概要）

資料 3-2 「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」の一部改正について

資料 3-3 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

「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」の一部改正について(案) (概要) ※レッドチームテストの実施

- 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つかさどる事務のうち、監査について、実施のための「基本方針」(注1)においては、「監査の実施内容」として、「マネジメント監査」及び「ペネトレーションテスト」が定められている。

注1：「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31年4月1日一部改定(最終改定))



- サイバー攻撃の洗練化・巧妙化が高度に進展している昨今の情勢を鑑み、「政府のサイバーセキュリティ体制の抜本的強化」が必要(注2)。

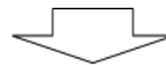
注2：「サイバーセキュリティ2024」(2024年7月10日 サイバーセキュリティ戦略本部決定)(抜粋)

【背景及び課題】

「> サイバー攻撃の侵入起点となり得るIT資産・サービスの急増や、…サイバー攻撃の手法の劇的な高度化に対応するため、政府機関全体におけるサイバーセキュリティ対策はこれまで以上に戦略的に実行していくことが強く求められる。」

【取組の概要】

「✓ …レッドチームテストといった政府機関の対策・対応について、組織・システム・人的側面を含め多面的に評価するための取組の検討といった施策を推進する。」



- 政府機関等において令和7年度から同テストの実施を開始するため、「基本方針」の「監査の実施内容」に「レッドチームテスト」を追加する。

※レッドチームテストとペネトレーションテストの違い

	レッドチームテスト	ペネトレーションテスト
評価対象	システム+対応プロセス	システム
攻撃手法	システムに対する直接的な侵入 + 標的型メール攻撃等、実際のサイバー攻撃で 用いられる手法	システムに対する直接的な侵入
被評価組織の 対応・対処	疑似攻撃の検知・確認、拡大防止、組織内の報 告・共有等のインシデント対応を行う	疑似攻撃に対する検知は行わず、インシデ ント対応も行わない
利点	システム(少数)を重点的・総合的に確認	システム(多数)を網羅的・効率的に確認

○レッドチームテストとは

テスト対象ごとの脅威分析を踏まえたシナリオに基づき、攻撃者を模した「レッドチーム」が攻撃を実施し、テスト対象側のサイバー攻撃への対応等の実効性等を検証する、実践的な侵入テストである。

○目的

システムの設定の不備や脆弱性対策だけでなく、インシデントの検知能力や対応プロセスも含めて評価し、改善のために必要な助言等を行うことで、テスト対象機関における脆弱性対策・対応能力等の向上を図る。また、得られた知見等を横展開することで政府機関全体におけるサイバーセキュリティ体制の強化を図る。

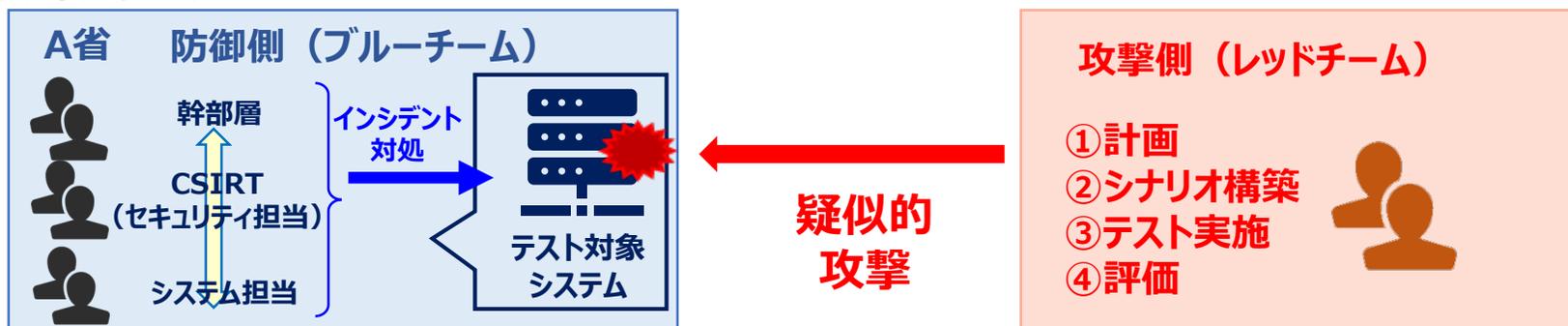
○対象システムの考え方

過年度に重大インシデントが発生したシステムや、システム障害等により国民生活等に多大な影響を及ぼすシステムを優先

○効果

- ・テスト対象機関における脆弱性対策・インシデント対応能力等の向上
- ・得られた知見等を横展開することによる政府機関全体におけるサイバーセキュリティ体制の強化

レッドチームテストスキーム



(案)

資料 3 - 2

「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」の
一部改正について

〔 令和 年 月 日
サイバーセキュリティ戦略本部決定 〕

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）の一部を次表のように改正する。

（下線部分は改定部分）

改正後	改正前
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 <u>令和 7 年 月 日一部改定</u>	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
1 (略)	1 (略)
2 (略)	2 (略)
3 (略)	3 (略)
4 監査の実施内容 (1)・(2) (略) (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・	4 監査の実施内容 (1)・(2) (略) (新設)

(案)

<p>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。</p> <p>5 (略)</p>	<p>5 (略)</p>
-----------------------------------------------------------	--------------

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 ● 月 ● 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 P D C A 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 P D C A 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

案

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、内閣サイバーセキュリティセンターに実施させる。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。