資料２－１

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(案)について

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（案）

1 監査の目的

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、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サイクルが継続的かつ有効に機能するよう助言し、対策の効果的な強化を図る。

2 監査の対象

国の行政機関　※独立行政法人については、当面、特に必要があると認める場合に監査の対象とする。

3 監査の基本的な方向性

(1) 助言型監査
- 有益な助言を行う。
- グッドプラクティスを共有。

(2) 第三者的視点からの監査
- 内部監査とは独立した監査を実施。

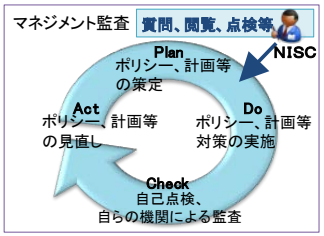
(3) 各機関の状況を踏まえた監査
- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

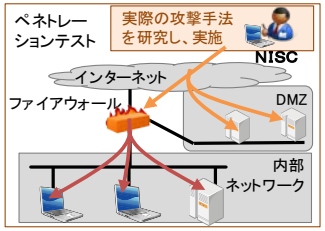
(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定
- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

4 監査の実施内容

(1) マネジメント監査
- 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検証する。
- 対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。

(2) ペネトレーションテスト
- 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し、改善のために必要な助言等を行う。





5 監査の進め方　※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が実施する。

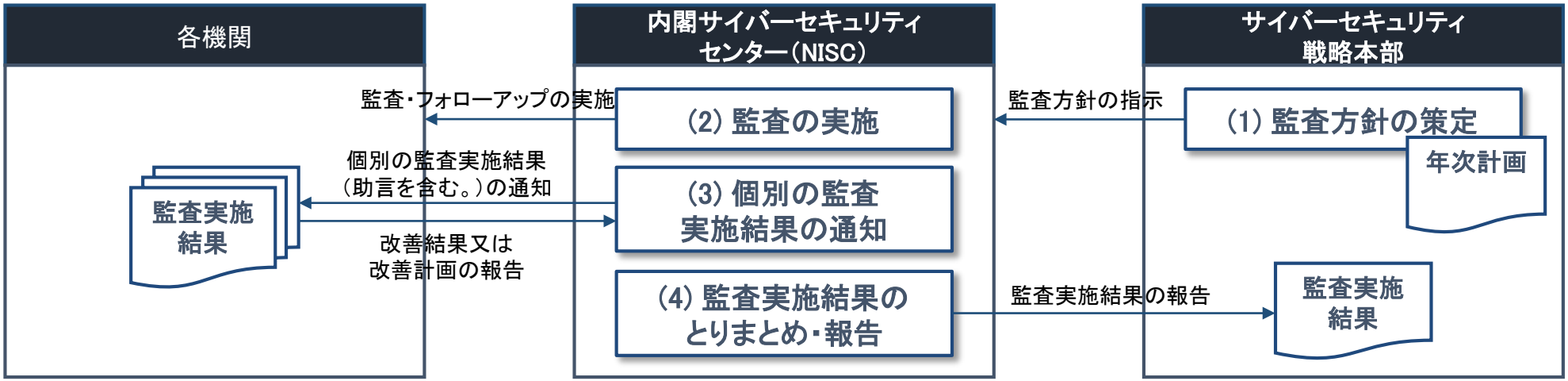
(1) 監査方針の策定
- 年度ごとの監査の基本的な考え方を含む年度監査方針を、年次計画の一部として策定。

(2) 監査の実施
- 必要に応じて外部専門家が協力。
- 過年度の監査実施結果のうち重要な事項については、改善状況を継続的にフォローアップ。

(3) 個別の監査実施結果の通知
- 監査実施結果を、各機関の最高情報セキュリティ責任者（CISO）へ通知。
- 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、改善結果又は計画を報告。

(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のないよう配慮しつつ、当該年度に実施した監査の結果を取りまとめ。
- サイバーセキュリティ戦略本部に報告。

監査の進め方



今後のスケジュール