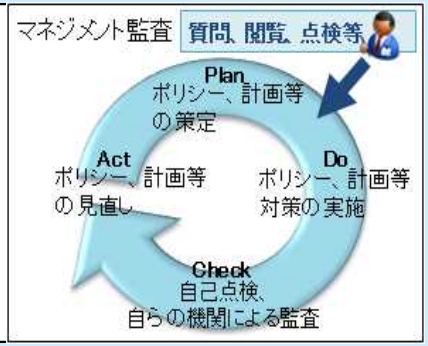
資料5

サイバーセキュリティ基本法第25条第１項第２号に基づく監査の報告について

- サイバーセキュリティ基本法第25 条第１項第２号の規定に基づき、平成28年度、サイバーセキュリティ戦略本部の事務である監査を府省庁、独立行政法人及び指定法人※1に対して実施。監査は、マネジメント監査及び侵入テスト（ペネトレーションテスト）からなる。全体として、監査項目について統一基準が求める必要な水準を満たすようサイバーセキュリティに係る取組が実施されていることを確認した。
- この枠組みにおいて、厚生労働省情報セキュリティ推進部局及び年金局並びに日本年金機構本部及び地方拠点（全国９地域）に対して、所要の体制整備、技術的対策及び教育・訓練を主な監査項目として監査を実施。必要なサイバーセキュリティ対策が実施されていることを確認した。

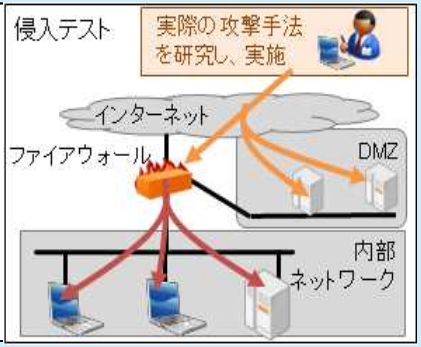
マネジメント監査

- 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。



侵入テスト

- 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。



平成28年度の監査においては、以下に示す主な監査項目について、改善のために必要な助言等を行った。

【主な監査項目】
- ・情報セキュリティ対策の基本的枠組みの整備及び運用状況
- ・情報の取扱いに係る規程の整備及び運用状況
- ・外部委託に係る規程の整備及び運用状況
- ・CSIRT※2に係る規程の整備及び運用状況
- ・情報システムのセキュリティ要件に係る規程の整備及び運用状況
- ・情報システムのライフサイクルに係る規程の整備及び運用状況
- ・情報システムの構成要素に係る規程の整備及び運用状況
- ・情報システムの利用に係る規程の整備及び運用状況

平成28年度の侵入テストにおいては、以下に示す項目についてテストを行い、必要な助言等を行った。

【主なテスト項目】
- ・インターネット（外部）からの侵入テスト
- ・情報システム内部の端末がウイルスに感染した場合を想定した、当該端末（内部）から調査対象サーバ等への侵入テスト

※1　マネジメント監査は、12府省庁（内閣官房、内閣法制局、内閣府、消費者庁、復興庁、総務省、外務省、財務省、厚生労働省、経済産業省、国土交通省、防衛省）及び7独立行政法人・指定法人（日本年金機構を含む。）に対して実施。また、侵入テストは、22府省庁及び7独立行政法人・指定法人（日本年金機構を含む。）に対して実施。

※2　CSIRTとはComputer Security Incident Response Teamの略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。