資料3

サイバーセキュリティ基本法第25条第１項第２号に基づく監査の状況について

2016年10月12日

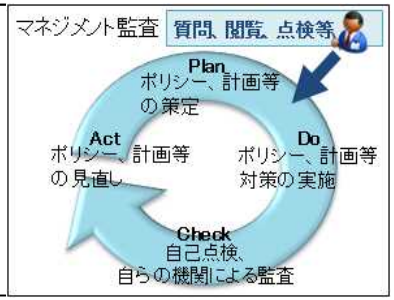
平成28年10月12日

サイバーセキュリティ基本法第25条第1項第2号に基づく監査の状況について

- 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、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に対して平成27年度から実施。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。
- この枠組みにおいて、厚生労働省及び厚生労働省と一体となって公的業務を行っている日本年金機構への監査を実施中。

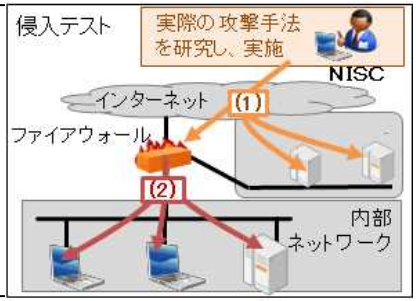
マネジメント監査

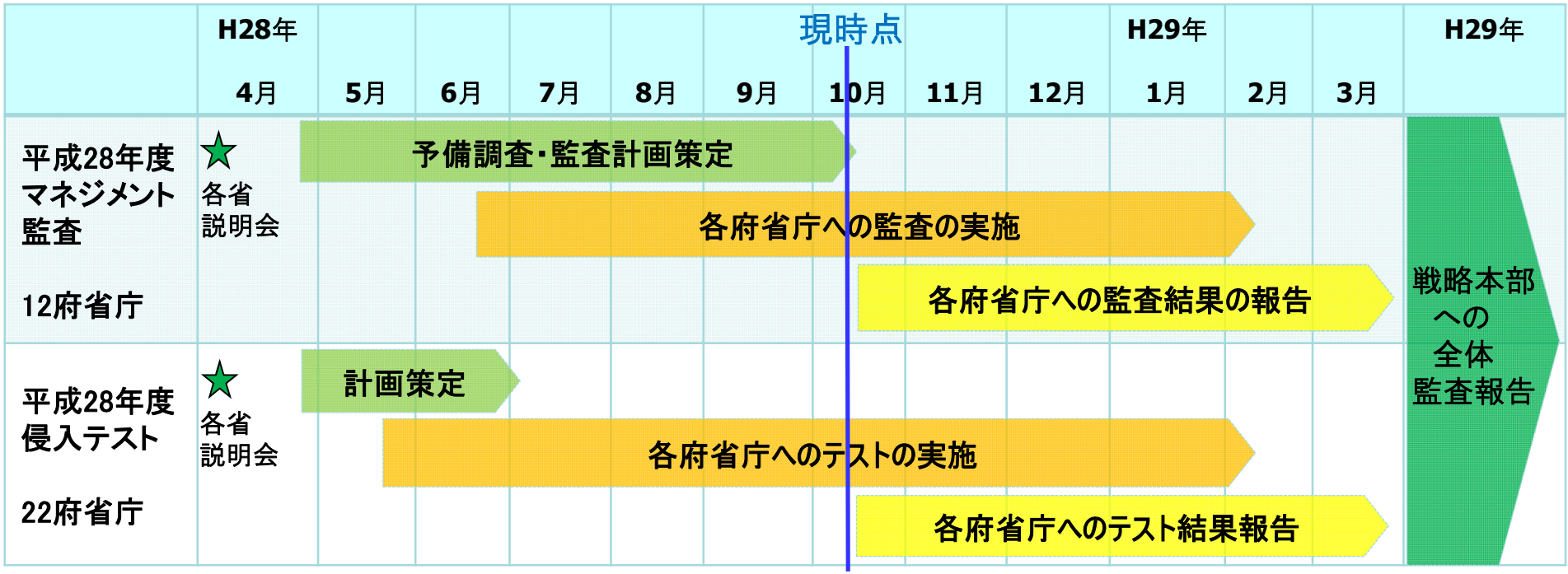
- 国際規格において基本的な考え方である組織全体としてのPDCAサイクルが有効に機能しているかとの観点から検証する。
- 対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。



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。





（参考） 平成27年度のマネジメント監査は、10府省庁（人事院、宮内庁、公正取引委員会、警察庁、個人情報保護委員会、金融庁、法務省、文部科学省、農林水産省、環境省）に対して実施。平成28年度の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）に対して実施中。

平成28年10月12日

厚生労働省及び日本年金機構に対する監査の中間報告

中間報告　〔監査期間〕平成28年５月～平成29年３月

１　体制整備

○厚労省：情報セキュリティに係る新たな役職や部署の設置による省内体制の見直し、外部人材や実務要員を含んだ実効あるCSIRT※体制の構築等を実施した。

○機　構：理事長をトップとした対策本部やその実行部隊の設置による組織内体制の見直し、ポリシーの改定による役割・責任・権限の明確化、CSIRT体制の新設等を実施した。

２　技術的対策

○厚労省：大量の個人情報や機微な情報を取り扱う業務に対してインターネット経由の攻撃が及ばないよう、情報システムの分離を実施した。

○機　構：（以下のとおり）

３　教育・訓練

○厚労省：幹部も含めた階層別の情報セキュリティ研修、機構との合同訓練、重要情報の適正管理に係る全職員への周知等を実施した。

○機　構：全役職員に対する計画的な教育・研修の立案・実施、厚労省との合同訓練、機構外での訓練や研修への参加等を実施した。

機構における主な技術的対策

＜機構における情報流出事案の原因となった情報システムに係る技術的対策の状況＞

○大量の個人情報や機微な情報を取り扱う業務においては、当該業務を処理する情報システムをインターネットへの接続ができないよう分離策が講じられた。

○分離策を講じたシステムにおいて記録媒体に書き出す場合には、全て暗号化措置が講じられている。

○インターネットへの接続を要する特定の情報システムについては、インターネット経由の攻撃に対する多重防御策が講じられている。また、NISCが実施した侵入テスト（ペネトレーションテスト）においても、現時点において想定される侵入に係る脆弱性は発見されなかった。

※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。