資料５

サイバーセキュリティ対策を強化するための施策の評価（監査）の方針について

1　サイバーセキュリティ戦略本部による評価（監査）

サイバーセキュリティ基本法第25条第１項第２号において、新たにサイバーセキュリティに関する対策基準に基づく、施策の評価（監査を含む。）に関する事務が、サイバーセキュリティ戦略本部の所掌事務として規定されたことに伴い、当該事務に係る方針を定める必要がある。

（1）国の行政機関の情報セキュリティ対策

国の行政機関における情報セキュリティ対策は、「政府機関における情報セキュリティ対策のための統一基準群」（以下「統一基準群」という。）に準拠した各機関の情報セキュリティポリシーに基づき取組を推進。

（2）サイバーセキュリティ戦略本部による評価（監査）

これまでは、NISCが、国の行政機関の対策の実施状況について、自己点検結果及び各機関自らが実施した監査等について報告を受け、国の行政機関全体の課題を把握し、全体として必要な取組を実施。

サイバーセキュリティ基本法の施行

サイバーセキュリティ戦略本部が、国の行政機関におけるサイバーセキュリティに関する対策の基準に基づく施策の評価（**監査**を含む。）を実施。

各機関における取組に加えて、第三者の視点から、行政機関に対し改善策の助言を実施。

2 評価(監査)の目指すべき方向

(1)評価(監査)の対象

国の行政機関(統一基準群が適用される機関※)

※ 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、国家行政組織法第3条第2項に規定する機関、これらに置かれる機関

(2)評価(監査)の内容

目的:国の行政機関におけるサイバーセキュリティ対策の強化を図ること

サイバーセキュリティ戦略本部

事務委任

報告等

NISC

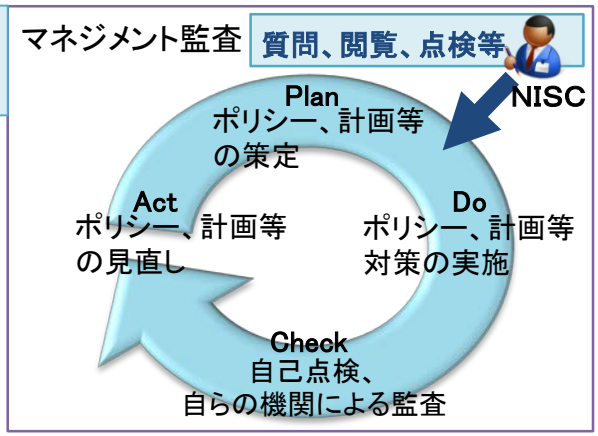
①②の二本立てで監査を実施

①セキュリティ対策強化のための体制・制度が機能しているかの検証による評価(監査)(以下「マネジメント監査」という。)

統一基準群に基づく施策の取組状況について、主に組織全体としての**対策強化を続ける仕組みが有効に機能しているかどうかの観点**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、**改善のための必要な助言等を行う**。

マネジメント監査の着眼点

P(計画立案)、D(実行)、C(点検)、A(見直し)の実施状況を確認するとともに、セキュリティ対策のための体制等についても確認



②情報システムに対する疑似的攻撃による評価(監査)

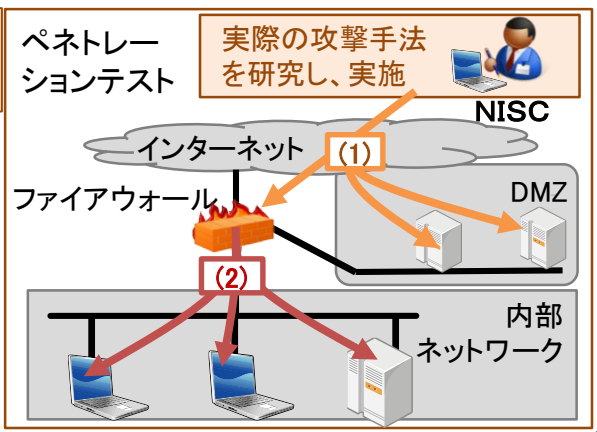
(以下「ペネトレーションテスト」という。)

情報システムに対して、攻撃者が用いる手法で**実際に侵入できるかどうかの観点**から防御策の状況を**検証**し、**改善のための必要な助言等を行う**。

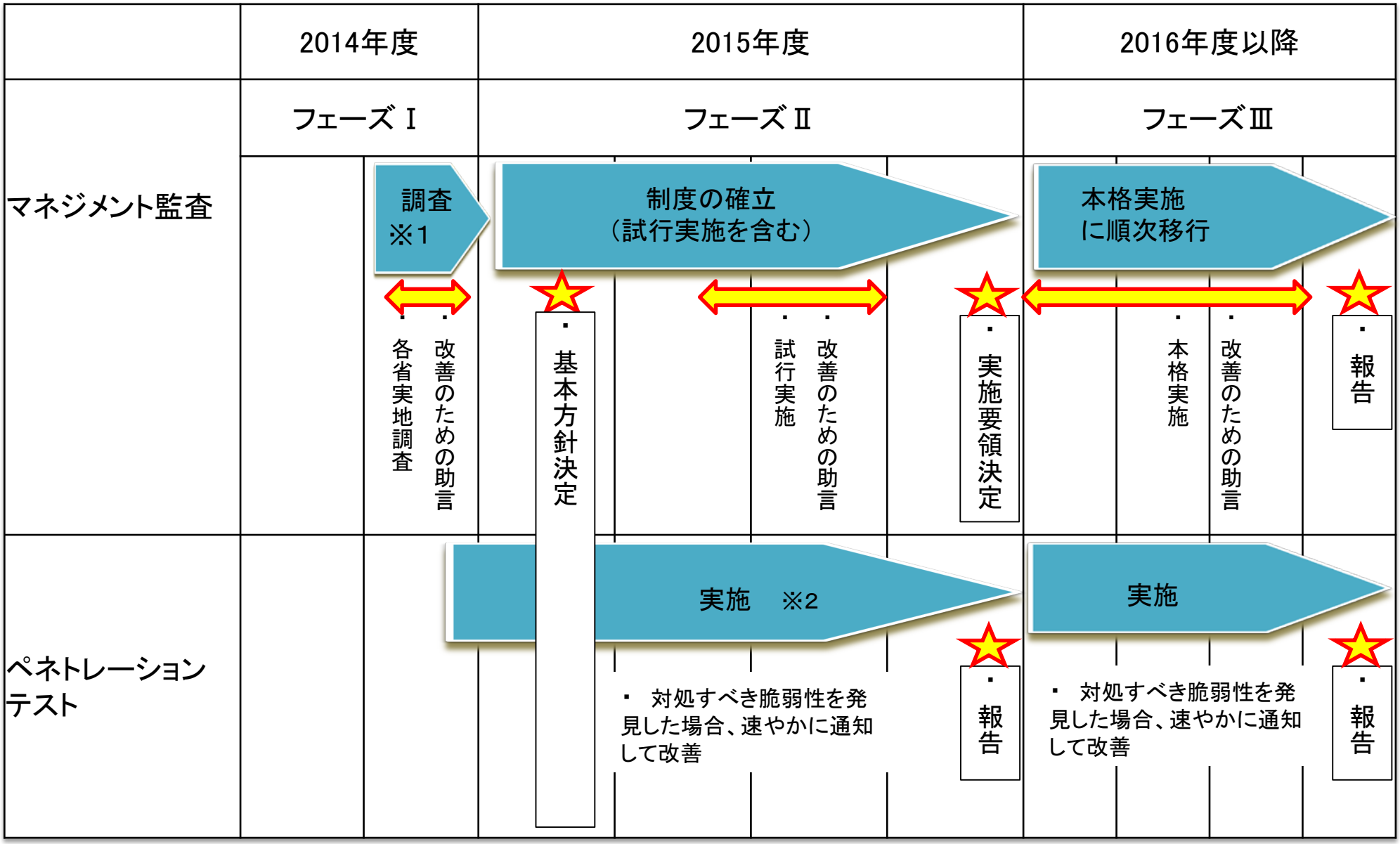
ペネトレーションテストの着眼点

(1)インターネット経由での不正アクセスを想定し、問題点の有無を検証

(2)インターネットとの境界を突破できた場合、内部ネットワークについても、問題点の有無を検証



3　今後のスケジュール（案）



※1　サイバーセキュリティ基本法の施行により、基本方針決定に向け各機関の施策の取組状況についてヒアリング等の実地調査等を実施。

※2　平成26年度補正予算及び平成27年度予算（予定）により実施。