資料3-1

NISC National Information Security Center

高度サイバー攻撃対処のためのリスク評価等のガイドラインの試行状況等について（報告）

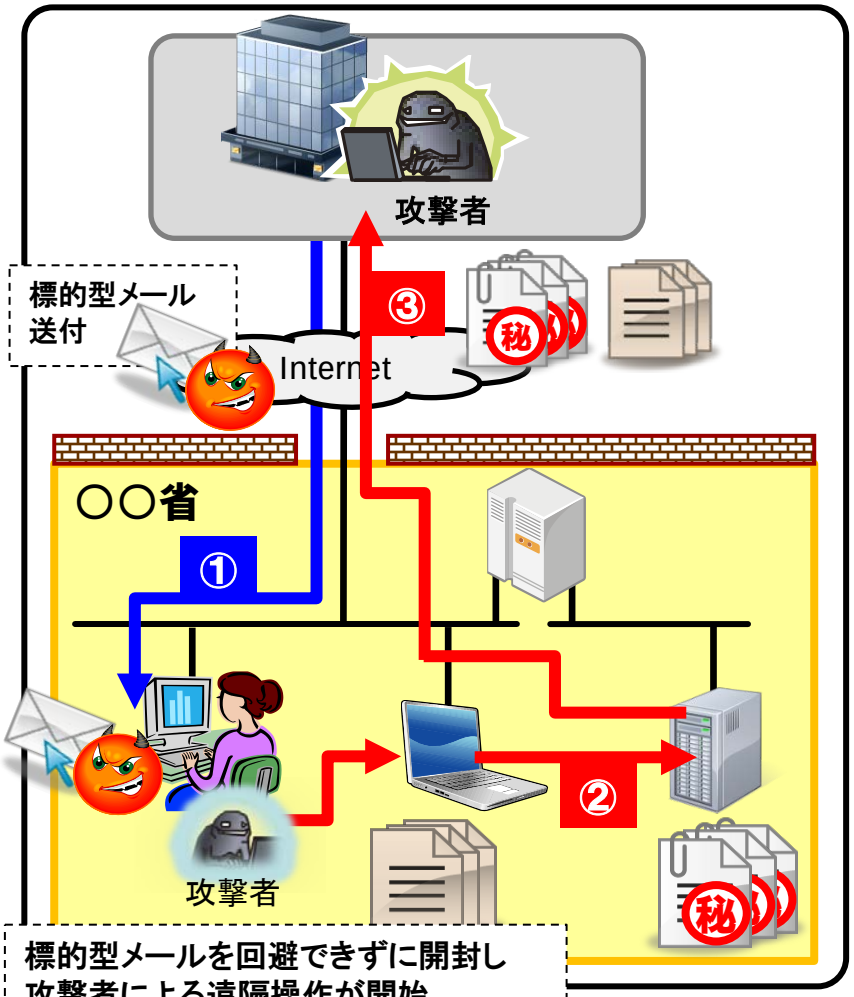
平成26年3月

内閣官房情報セキュリティセンター

本取組の概要

- 各府省庁の最高情報セキュリティ責任者（CISO）の指揮の下、機密度等に応じて保護対象とする業務を特定し、当該業務に係るリスク評価を実施するとともに、高度サイバー攻撃から保護対象を守るために必要な情報セキュリティ対策を計画的・重点的に実施するものであり、現在、各府省庁で試行中（平成25年度中）。

標的型攻撃　（典型的なモデル）



攻撃プロセス

① 初期潜入

② 侵入範囲拡大

③ 情報窃取

政府機関の情報セキュリティ対策のための統一基準群で対策を規定

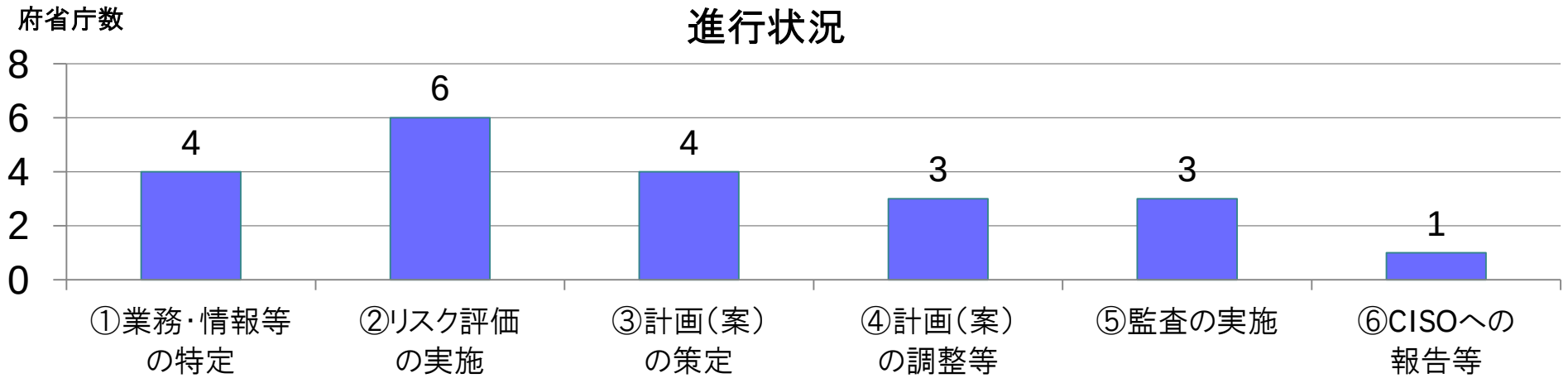
情報システム内部の設計対策

統一基準群の上乗せ対策

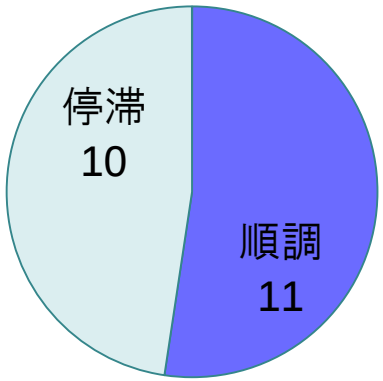
対策目的	対策方針
攻撃を遮断し、侵入範囲の拡大を防止する	• ハッキング技術を用いた内部探索がしづらいシステム設計 • 機器を乗っ取りづらいシステム設計
攻撃の兆候を監視し、早期に発見・検知する	• 攻撃（主に攻撃失敗）の痕跡が残るシステム設計 • 攻撃の兆候を発見・検知するためのトラップ（罠）の設置 • 上記の継続的な監視

試行の進捗状況

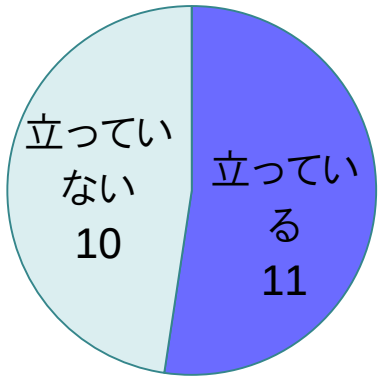
- 半年間の試行期間を通して、実施プロセスや技術的対策の運用上の問題点等、本取組の正式実施に向けた課題を洗い出した。



これまでの進行具合



今後の見通し



2014/3/14現在

正式実施に向けた対応

実施プロセスの明確化

保護対象とする業務を特定するためのプロセスを始め、本取組のプロセスをより明確なものにする。

評価方法の見直し

対策状況の評価方法（硬直的・減点方式）を見直し、対策の多様化・技術の進展といった状況の変化に対応可能なものとする。

新たな対策の導入スキームの整備

攻撃手法の変化等に迅速に対応するため、新たな技術対策を積極的に導入できるスキームを整備する。

今後の予定

試行の仕上げ

年度内にダッシュボードを用いてCISOへ報告し、決定を仰ぐ

ダッシュボードの概要

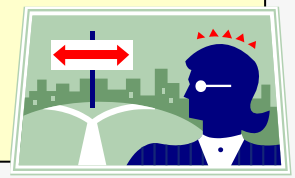
情報セキュリティ推進の目標・計画に照らして進捗状況を可視化し、CISOへのリスク評価結果等の報告及び対策導入計画の提案に用いるもの。

自府省庁において**保護対象とする業務**が妥当かどうか

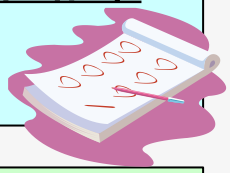
現状の情報システムの**対策状況等**

計画内容（優先順位付け、進捗状況、資源配分等）

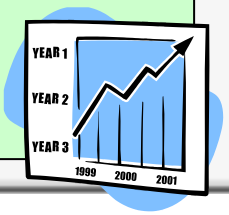
①保護対象とする業務
- 保護対象とする業務を評価
- 脅威事象発生時の影響　等



②情報システムの対策実施状況・リスク評価結果
- 情報システムの対策実施状況
- 現状についてのリスク評価結果　等



③次年度以降の対策導入計画
- 次年度の対策導入計画の概要（投資計画含む）
- 次年度以降の対策実施の推移（グラフ）
- 対策実施までの間の応急策　等



今後の予定

試行の結果を踏まえてガイドラインの見直しを行い、平成26年6月（予定）の情報セキュリティ対策推進会議においてガイドライン（正式版）を決定した上で、平成26年度から本取組を正式に実施予定。