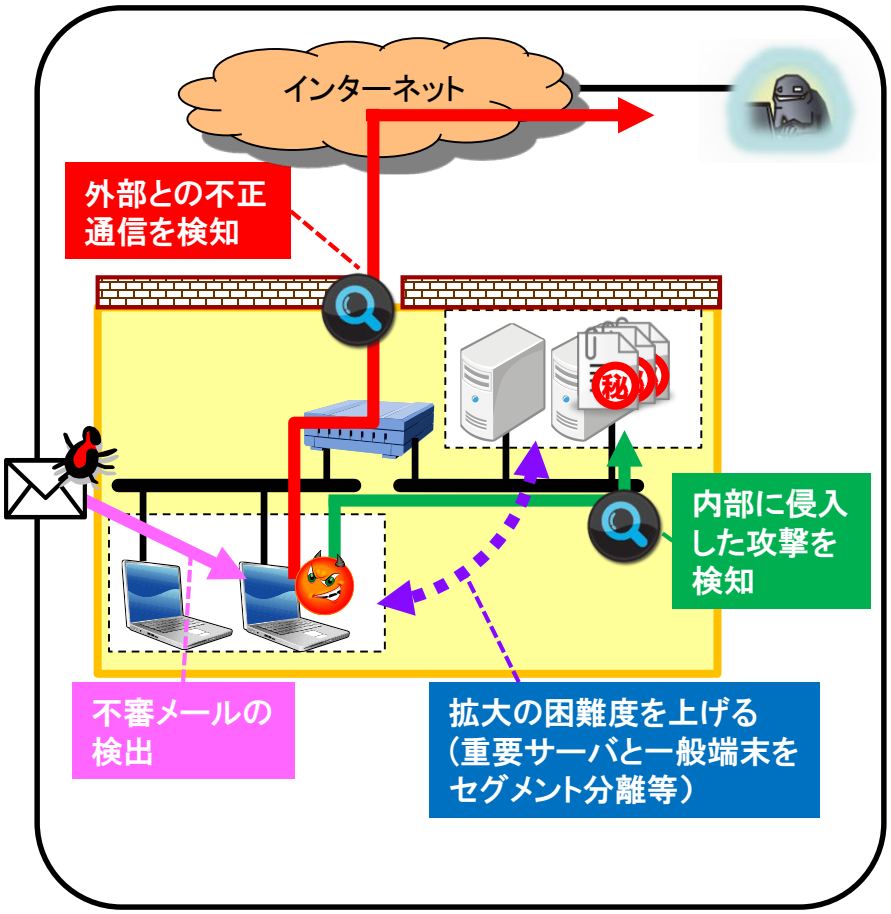
資料３－１

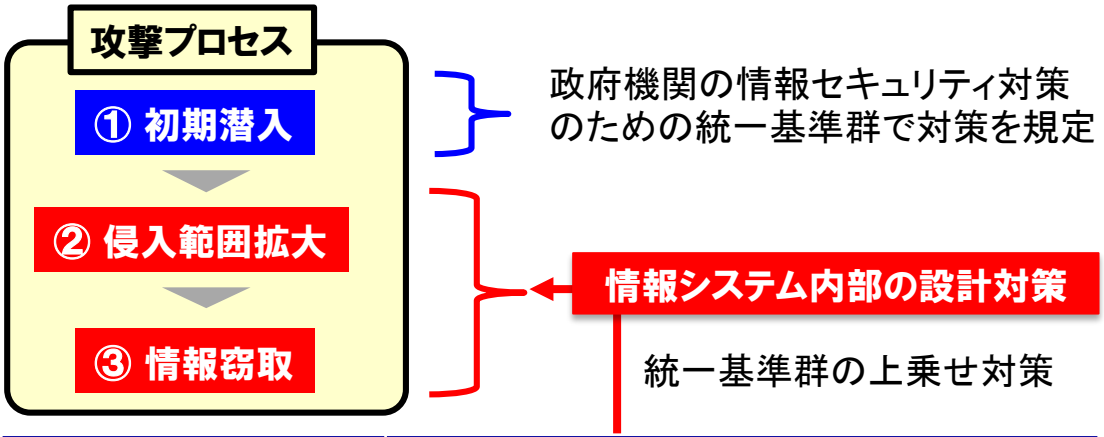
「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用状況について

本取組の概要

- 高度なサイバー攻撃から重要な業務・情報を守るため、情報システムが不正プログラムに感染したとしても、攻撃者が情報の窃取等を達成する前に攻撃を検知・遮断するための対策を計画的・重点的に導入する。

対策の概要(例)





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

政府機関全体としての状況

- 平成26年度における政府機関全体(21府省庁)としての状況は以下のとおり。
  - 本ガイドラインに基づくリスク評価等のプロセスを通じて、計画的・重点的に対策を導入する対象として、およそ40の情報システムを特定した。
  - 対策実施状況の現状点検を実施した上で、対策の更なる強化の要否を検討し、CISOによる方針決定の下、およそ５割の対象システムにおいて更なる対策強化を図る計画を策定した。
  - 対象システム全体としての対策実施状況(平均)の現状を100とすると、計画に基づく強化後は114となる見込み。また、対象システムの中でも防御の優先度が高い評価結果であるものについては、現状は106、強化後は119と全体と比較して高い水準となっている。