資料６

NISC

National center of
Incident readiness and
Strategy for
Cybersecurity

「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（平成27年度）について

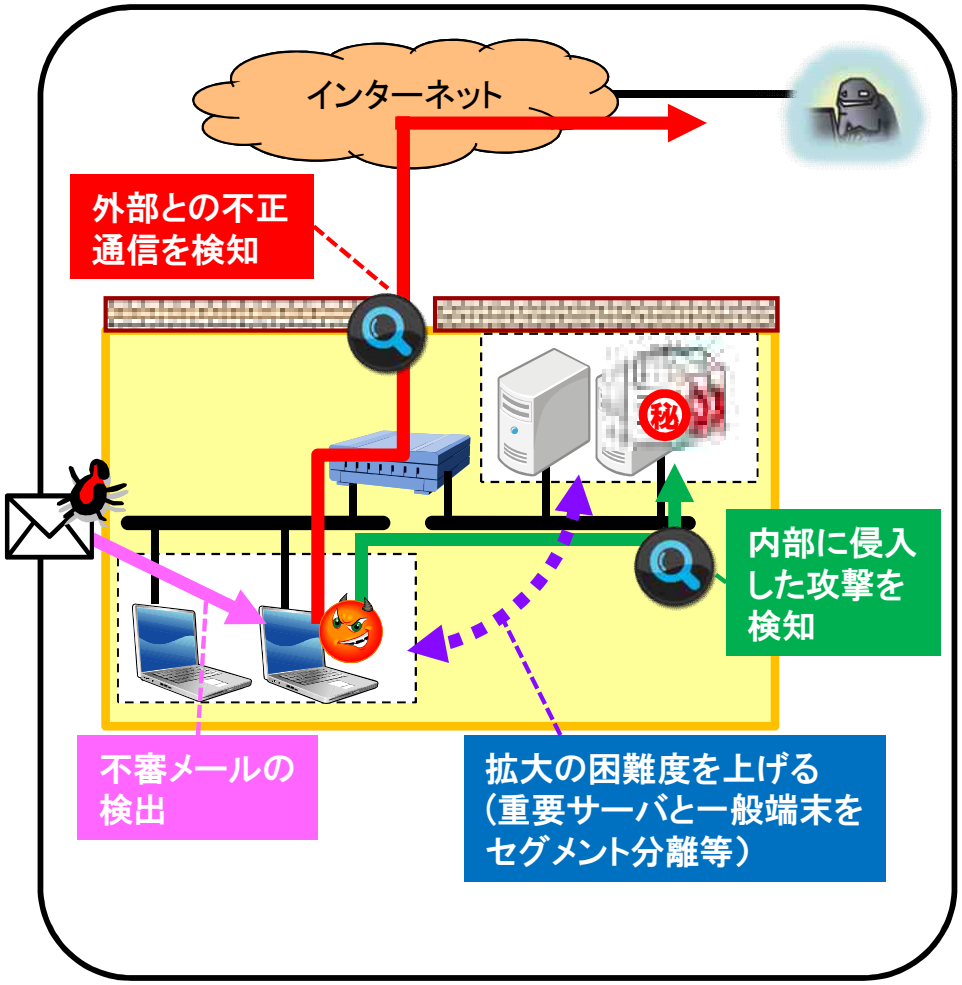
平成28年６月

内閣官房内閣サイバーセキュリティセンター

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)



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

政府機関全体としての状況

- 平成27年度における政府機関全体(22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、計画的・重点的に対策を導入する対象として、約100の業務領域に使用されている約40の情報システムを特定し、CISOによる方針決定の下で計画を策定した。
  - 府省庁が対象とした情報システムについて、特に重点的に取組が実施された結果、平成27年度末の時点で、ガイドラインに記載されているほぼ全ての標的型攻撃手法に対応する対策又は府省庁独自の対策が講じられた。
    特に、防御の優先度が高いシステムについては、全て、いずれかの対策が既に講じられている。
  - 計画に基づく強化後（平成30年度末）には、ガイドラインに掲載されている対策が、全てのシステム・標的型攻撃手法に対して完了する計画となっている。
  - 今後も、計画に基づき着実に対象システムの標的型攻撃対策を強化していくとともに、平成27年６月に明らかとなった日本年金機構における情報流出事案の教訓等を踏まえ、重要なシステムのインターネットからの分離等を推進することで、高度サイバー攻撃への更なる対処を推進していく。