報道資料

平成 25 年 9 月 26 日
内閣官房情報セキュリティセンター（NISC）
内閣官房情報通信技術(IT)総合戦略室

情報セキュリティ対策推進会議第１３回会合の開催について

本日、「情報セキュリティ対策推進会議」（議長：杉田内閣官房副長官）の第13回会合を開催しました。
その概要は以下のとおり。

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（試行版）」について（決定）

標的型攻撃等の高度サイバー攻撃による脅威が深刻化していることから、重要な情報を守るため、各府省庁が、業務システムに防護策を計画的、重点的に講じていくためのガイドラインを定めました。（別添1参照）

２「政府機関の情報セキュリティ対策のための統一基準群」の見直しの方向性について（報告）

政府機関の情報セキュリティ対策のための統一基準群について、今後の見直しの方向性を報告しました。

※　資料は、情報セキュリティ政策会議（10 月初開催予定）へ報告後、公表致します。

３ 各省庁で共用できるセキュアなグループウェアサービスについて（報告）

7 月 30 日に開催された情報セキュリティ対策推進会議において決定された「グループメールサービスの利用に関する事案の再発防止策」のうち、各省庁が共用できるグループメールサービスの提供について報告しました。（別添2参照）

【本件に関する問い合わせ先】
1及び2について
内閣官房情報セキュリティセンター（NISC）
企画官　　奥山　剛
電話　03－3581－3959
3について
内閣官房情報通信技術(IT)総合戦略室
内閣参事官　濱島　秀夫
電話　03－3581－0412

※　本会合の会議資料等は、内閣官房情報セキュリティセンターのホームページに公表致します。
http://www.nisc.go.jp/conference/suishin/index.html

別添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 試行版（概要）

平成25年9月

内閣官房情報セキュリティセンター

情報の機密性の要求度等に応じたセキュリティ対策の重点強化について

第32回 情報セキュリティ政策会議資料、
第 9回 情報セキュリティ対策推進会議資料

脅威の変化

内部規律違反（ファイル共有ソフトの使用、USBメモリの紛失等）による情報漏えい

外部からの攻撃（標的型攻撃等）による情報窃取等

社会経済環境の変化

IT依存度の一層の高まり

厳しい財政状況（限られた人員・予算）

従来の統一基準の役割

情報セキュリティ水準の全体的な底上げ

統一基準の見直し
リスク評価手法の策定

今後の対策強化に向けた取組

○ 実施すべき対策のベースラインを明確化し、全体的な底上げ対策を着実に実施

○ 各府省庁が業務で扱う情報の機密性の要求度等に応じた対策を重点強化

- 機微な取扱いが必要な情報等を扱う業務領域については、リスク評価を行い、外部の脅威（標的型攻撃等）から重要な情報を守るために必要な対策を検討
- 各府省庁のCISO（最高情報セキュリティ責任者）が残存リスクを把握し、限られた人員、予算の中で講ずるべきセキュリティ対策（投資）を計画的・重点的に実施

本取組のコンセプト

情報セキュリティガバナンスの確立

- CISOの指揮の下に、計画的・重点的な情報セキュリティ対策（投資）を実施
- 情報セキュリティ対策導入計画やその進捗状況を可視化したダッシュボードの活用

高度サイバー攻撃(※)対処のためのリスク評価の実施

- 業務・情報に係る機密度等に応じたリスク評価の実施
- リスク評価の実施にあたり、省内システム担当部署（ITサービスを供給する情報システム部署）に加えて、情報保全関係部署（業務の実施にあたり、ITサービスを利活用している部署）が参画

高度サイバー攻撃(※)対処のための対策実施

- 対策導入・実施のための複数年にわたる計画の策定と当該計画に基づく対策の着実な実施
- 高度サイバー攻撃手法を分析し、その攻撃手法に対応する対策セットを提示
  （対策セットは、産学官の有識者による検討会において、有効性、コスト妥当性、運用可能性を検証し、評価した具体的なシステム設計対策、実装・監視方法等から成る）

※ 現時点においては、政府機関において極めて大きな脅威となっている組織的・持続的な意図をもって行われる標的型攻撃を対象としている。

情報セキュリティガバナンスの確立・リスク評価の実施

CISOによる情報セキュリティガバナンスプロセス

CISOの指揮の下に、計画的・重点的な情報セキュリティ対策（投資）を実施

リスク評価に基づき、対策導入計画をCISOへ提案

CISOが実態を把握し、対策導入計画の評価、承認

CISOによるコミットメント（方針指示）

NISC

CISOによる情報セキュリティガバナンス等が適正に実施されていることを把握し、当該事項を政府機関を代表して表明。

実際に行われたリスク評価プロセスが基準等に照らして、適正に実施されているかどうかを確認

リスク評価手法に基づく
・重点的に守るべき業務・情報の特定
・リスク評価の実施
・対策導入計画の策定

情報セキュリティ対策に関する組織としての取組の実行方針を決定
必要な資源を重点配分

実務レベルの情報セキュリティマネジメント

対策導入計画の進捗状況等の報告

C A D P

リスク評価を踏まえた情報セキュリティ対策の見直し

ダッシュボードに基づきCISOが承認・決定する事項

ダッシュボードに基づき CISOが承認・決定する事項

自府省庁において**重点的に守るべき業務・情報**が妥当かどうか

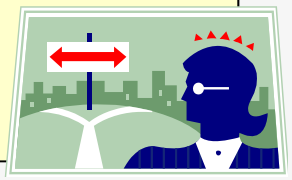
現状の情報システムの**対策状況等**

計画内容（優先順位付け、進捗状況、資源配分等）

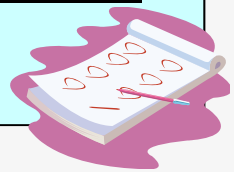
ダッシュボードの記載内容

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。

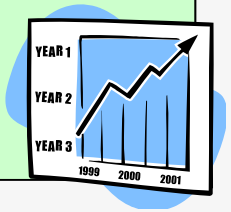
①重点的に守るべき業務・情報
- 重点的に守るべき業務・情報を評価
- 脅威事象発生時の影響　等



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



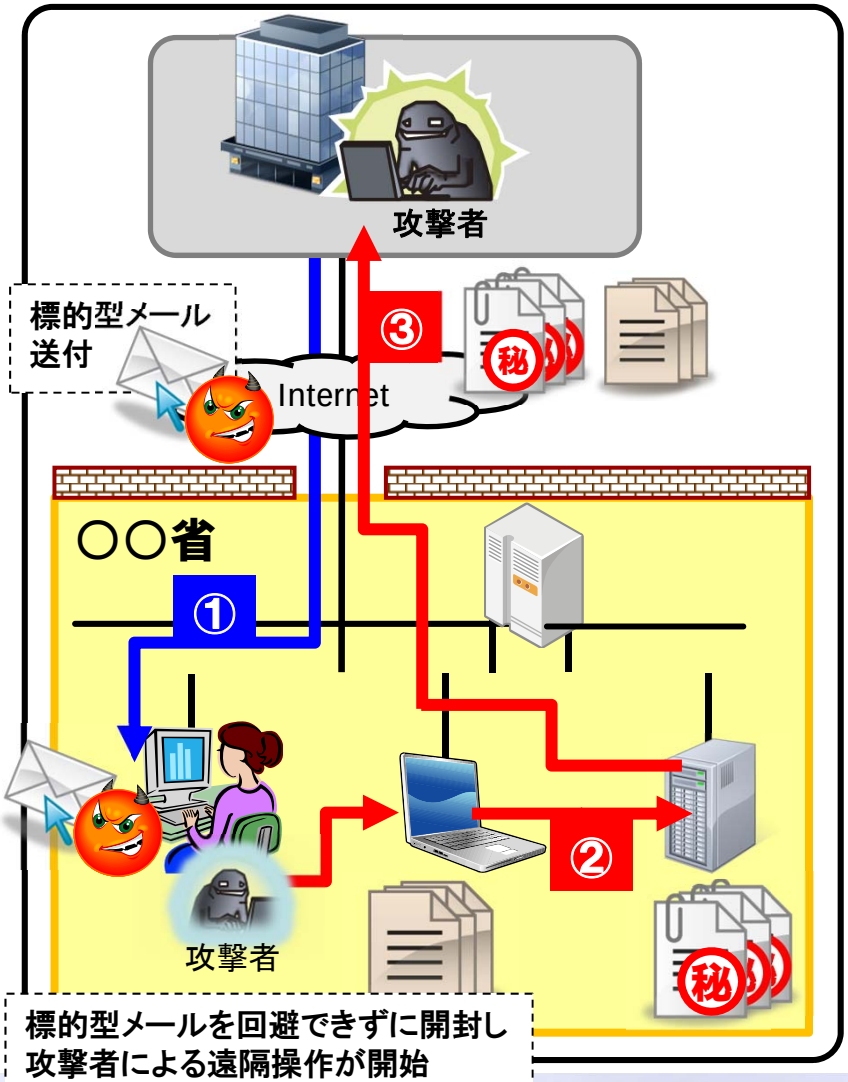
③次年度以降の対策導入計画
- 次年度の対策導入計画の概要（投資計画含む）
- 次年度以降の対策実施の推移（グラフ）
- 対策実施までの間の応急策　等



高度サイバー攻撃（標的型攻撃）対処のための対策実施

標的型メールを開封し、省内システムが不正プログラムに感染したとしても、攻撃者が最終目的（重要な情報の窃取やシステム破壊）を達成する前までに、攻撃の兆候を監視・検知又は攻撃を防御し、対処する。

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管理・技術基準で対策を規定

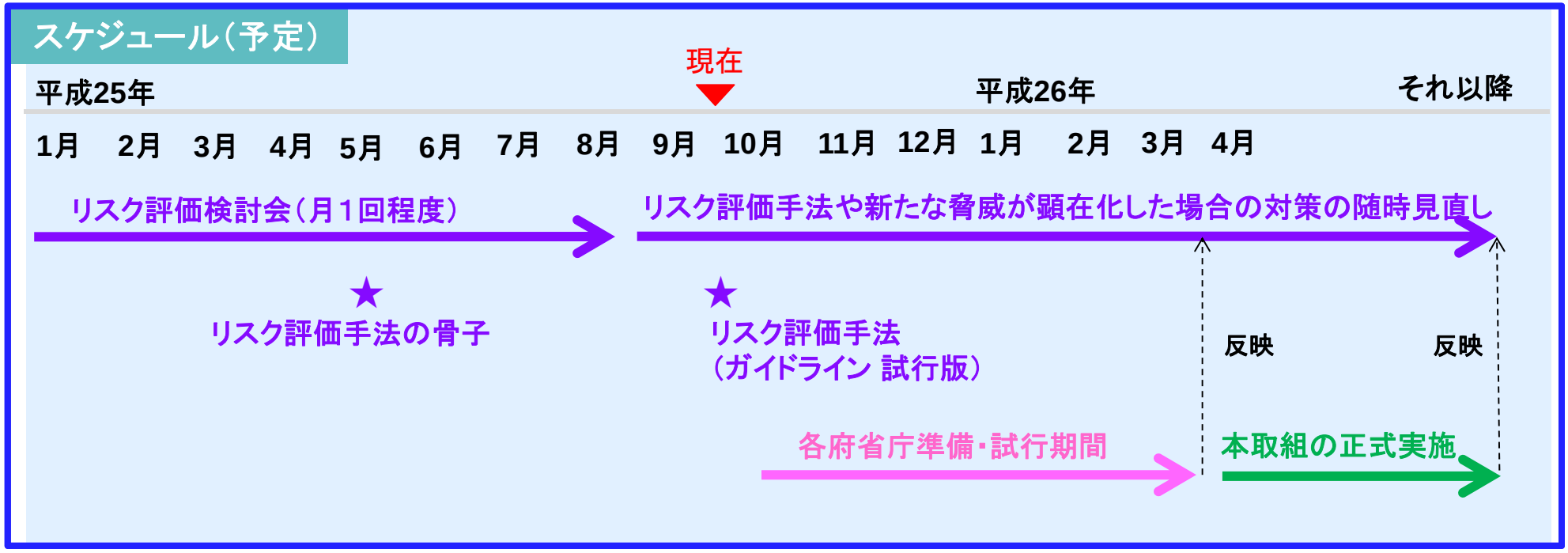
情報システム内部の設計対策

統一管理・技術基準の上乗せ対策

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	• 攻撃者にとってハッキング技術を用いた内部探索をしづらいシステム設計 • 機器乗っ取りをし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）の痕跡を残す • 攻撃者の侵入を発見・検知するためのトラップ（罠）を設置 • 上記の継続的な監視

スケジュール

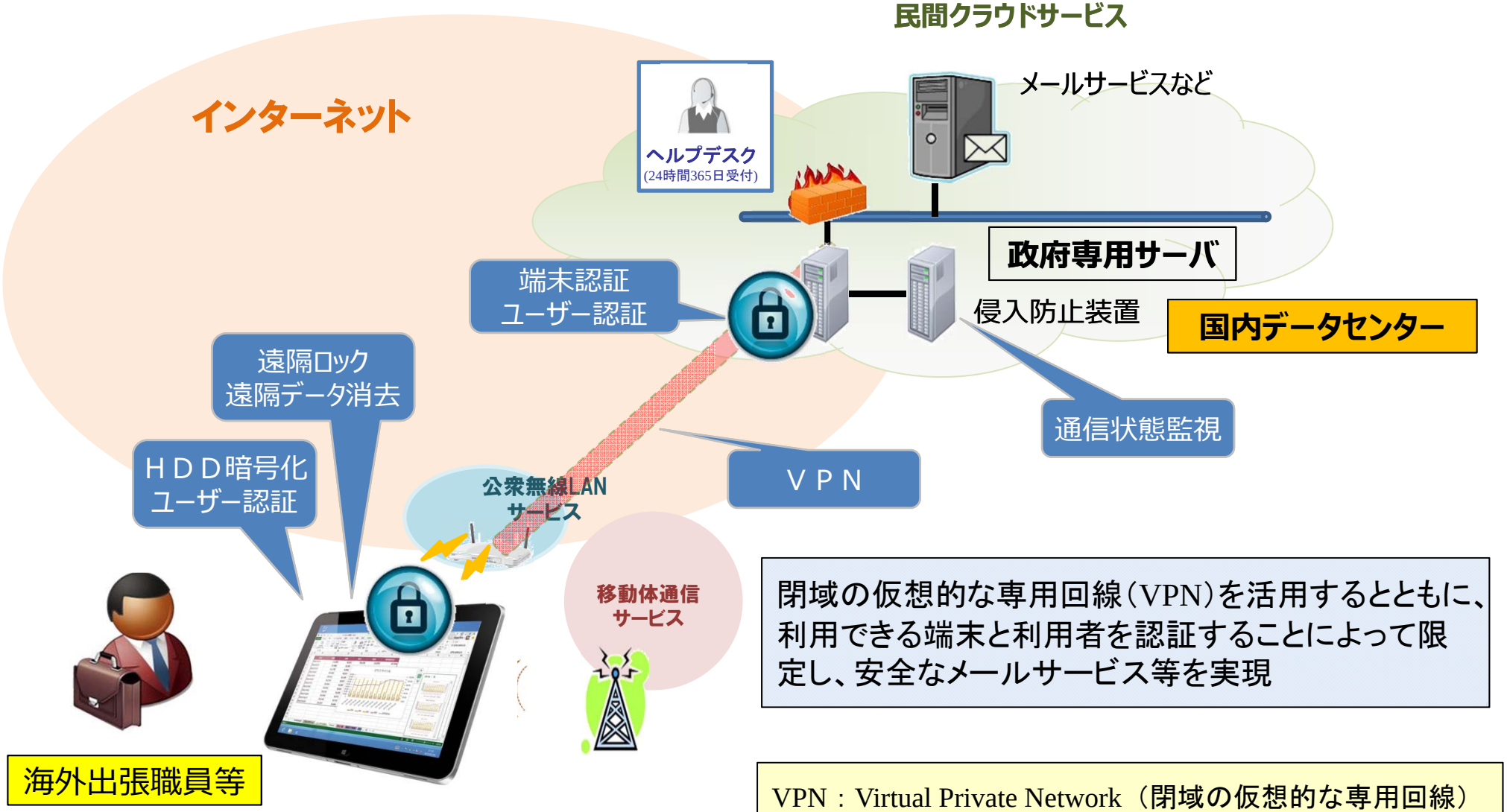
- 平成25年1月より産官学の専門家によるリスク評価手法等に関する検討会を定期的に開催。
- 平成25年度上期にリスク評価手法に係るガイドラインを策定し、同年度下期に試行。
  平成26年度より正式に本取組を実施予定。



各省庁で共用できるセキュアなグループウェアサービス

別添２

グループウェアサービス利用に伴う情報漏出事案を踏まえ、主にTPP交渉に対応する政府職員が安全に利用できるグループウェアサービス（タブレット端末台数：６０台）を導入。
－１０月初旬よりＴＰＰ交渉において活用予定



閉域の仮想的な専用回線（VPN）を活用するとともに、利用できる端末と利用者を認証することによって限定し、安全なメールサービス等を実現

VPN：Virtual Private Network（閉域の仮想的な専用回線）