

「政府機関における情報セキュリティに係る年次報告(平成23年度)」: 各府省庁の情報セキュリティ報告書等を踏まえ、対策の実施状況等についてCISO等連絡会議で評価した報告書 (H24.5.30 CISO等連絡会議において決定し、公表)

国内外における情報セキュリティに関する動向

- ① 巧妙化する攻撃手法
 - * 政府機関や民間企業への**標的型攻撃の顕在化** 等
- ② 攻撃目的の多様化
 - * 愉快犯・技術力の誇示、社会・政治的主張、金銭・情報の窃取 等
- ③ 東日本大震災による情報システムへの影響
 - * 地震・津波・停電(計画停電含む)に伴う被害の発生
- ④ 海外の状況
 - * サイバー空間に対する**戦略の策定**、国際会議の開催 等
- ⑤ 技術の進歩や利用環境の変化
 - * **スマートフォン・タブレット端末の利用拡大**

政府機関の取組に対する評価

- ① 対策の実施状況(自己点検結果)に関する評価
 - * 統一基準群を踏まえた**対策の実施率: 99.0%**
 - * 情報の作成・入手等について、更なる対策の向上が必要
- ② 情報システムへの対策状況(重点検査結果)に関する評価
 - * OS・サーバアプリの**セキュリティアップデートの実施率: 100%**
 - * DoS攻撃対策等について、更なる対策の向上が必要

政府機関の取組(NISC)

* 赤字: 重点取組事項

- ① 官民連携の強化を図るための対策の策定・実施
- ② 情報セキュリティに係る年次報告書の作成・公表
- ③ 新たな脅威等を踏まえた政府機関統一基準群の見直し
- ④ **標的型不審メール訓練の実施** (12省庁 約6万名の職員)
- ⑤ 公開ウェブサーバに対する**脆弱性検査の実施** (11省庁)
- ⑥ 政府機関から発信する**電子メールに係るなりすましの防止**
- ⑦ **東日本大震災における情報システムの被害状況の調査・分析**
- ⑧ 暗号危殆化の危険度判定及び対応フローの決定 等

平成24年度に取り組むべき政府機関の課題

- ① 情報セキュリティに関する動向を踏まえた課題
 - * 巧妙化している標的型攻撃に対応するための**体制の整備**
 - * **スマートフォン等**に対する**情報セキュリティ対策の検討**
 - * 共通利用基盤システム等に係るセキュリティ水準の確保 等
- ② 平成23年度の政府機関の取組を踏まえた課題
 - * 情報システムの**運用継続に向けた具体的な対策の促進**
 - * **公開ウェブサーバの脆弱性検査**によるセキュリティ水準の底上げ
 - * **標的型不審メール対処訓練**の充実強化
 - * **なりすまし防止対策**の更なる推進 等