「政府機関の情報セキュリティ対策のための統一基準群」パブリックコメント版（案）について

資料 4-1

現行の統一基準群の課題

◆毎年の改定により基準が複雑化・肥大化・形骸化

◆脅威の高度化・多様化や技術進展などの環境変化

改定の方向性（※）

◆統一基準群の実効性の向上

- 各府省庁が直面する情報セキュリティリスクを踏まえてCISO自らの判断で目標や実施計画を策定し、これに基づく対策の実施・評価・点検や、計画の見直しを行うよう求めることで、府省庁独自のPDCAサイクルによる自律的対策強化を図る。
- 定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人毎の遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく、守られやすい基準作りを目指す。

◆新たな脅威・技術への対応

- 標的型攻撃から守るべき重点業務・情報を特定し、攻撃の早期検知や、侵入後の活動を困難化するため、内部対策をリスクに応じて計画的に講ずる。
- 情報システムの構築等の外部委託の際、委託先における不正機能の混入などを防止するための管理体制を求める。
- 私物スマートフォン等の業務使用について、責任者の設置及び安全管理措置の規定により、厳格な管理を求める。
- ＳＮＳ、グループメールサービス等の利用に際して責任者の設置、なりすまし防止対策の実施、機密情報の取り扱いの禁止等を求める。
- ＵＳＢメモリ等について、ウイルス混入や紛失等の脅威に対抗するための利用手順を定めるよう求める。
- 複合機等のネット接続機器について、国際規格への適合や適切な設定等、必要な対策を講ずるよう求める。

（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）において決定された事項を踏まえ検討。）

スケジュール（予定）