資料 4-2 | 参考

NISC National Information Security Center

「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

平成25年10月

内閣官房情報セキュリティセンター

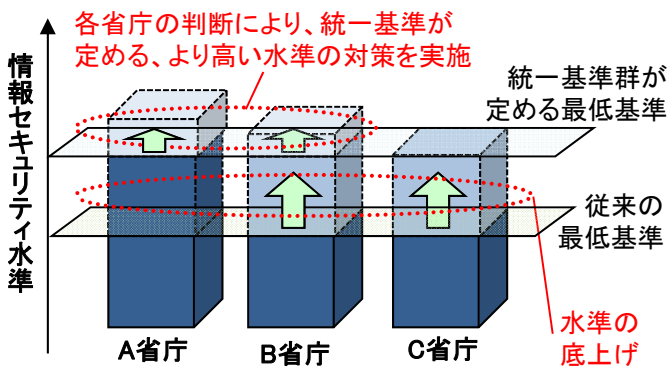
政府機関の情報セキュリティ対策のための統一基準群の見直し

「政府機関の情報セキュリティ対策のための統一基準群」とは

◆ 各府省庁が情報セキュリティ確保のために採るべき対策の最低水準や、より高い水準の対策実施を目的として、情報セキュリティ政策会議で定めた基準群。初版は平成17年に策定され、以来毎年改定を行っている。

◆ これまで各府省庁でバラつきのあったセキュリティ対策の統一化を行ったほか、水準の底上げに貢献。

＜統一基準群の効果（イメージ）＞



現行の統一基準群の主な課題と見直しの方向性

◆ 一方、現行基準の課題、最近の状況の変化を踏まえ、より実践的な基準への見直しが必要（※）。

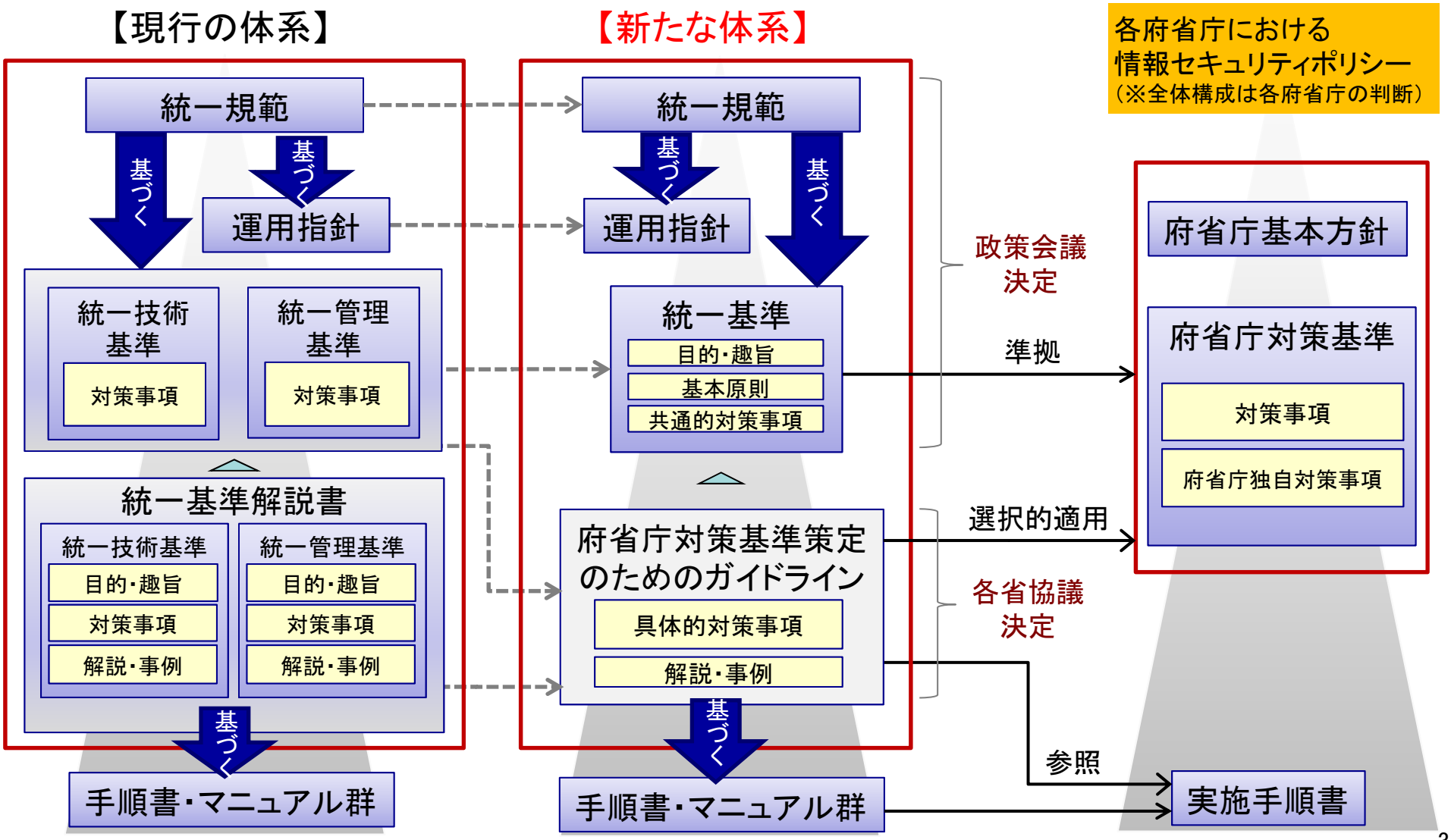
（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）においては、「標的型攻撃等への対処に関するリスク評価手法の確立等を通じて、政府機関における統一的な仕組みを強化する」こととされている。）

現行基準の主な課題	見直しの方向性
毎年の改定により基準が複雑化・肥大化	① 共通的に実施すべき基礎（ベースライン）となる対策を明確化
技術の進展、環境変化等による形骸化	② 実践的に対策を導入できるよう、実施メカニズムを見直し等
サイバー攻撃の手法が多様化・巧妙化	③ 高度サイバー攻撃のためのリスク評価等の手法の整備

（※詳細については資料1-1）

統一基準群の見直しの方向性①：基礎となる対策の明確化

◆ 細分化・肥大化している統一基準の規定を統合・集約化するとともに、個別具体的な対策事項は別の文書（ガイドライン）に規定することで、基準を明確化する。



統一基準群の見直しの方向性②：対策の実施メカニズムの見直し

各府省庁内PDCAサイクルの構築

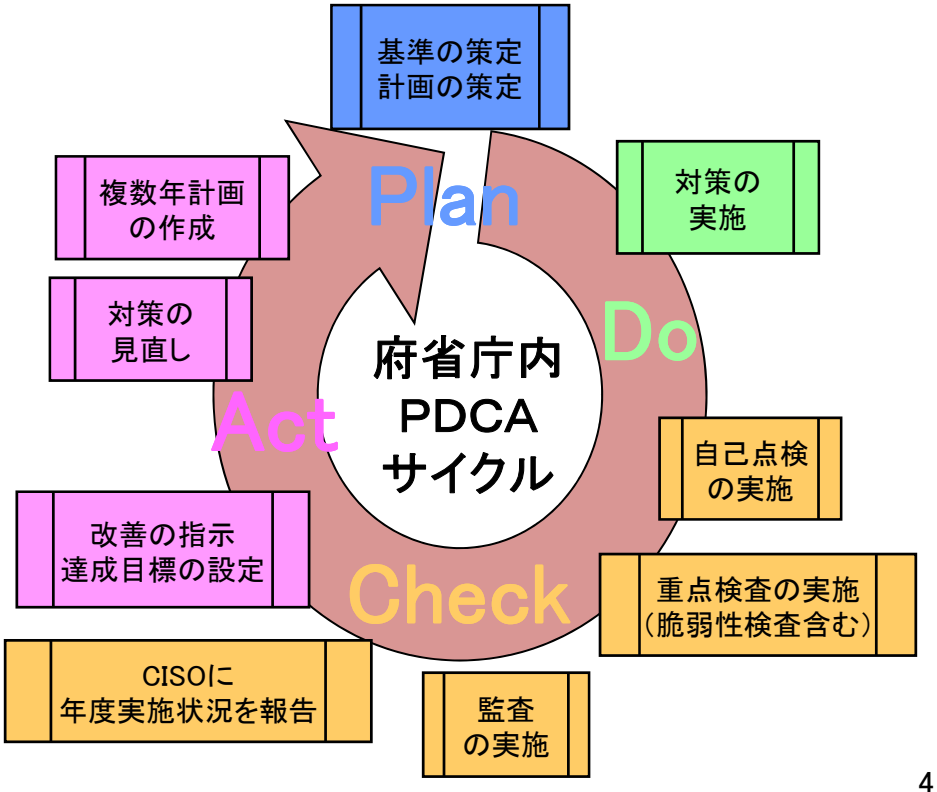
◆ 各府省庁毎に目標を設定し、その達成に向けた複数年計画を策定し、対策を計画的かつ着実に実施するためのメカニズム（PDCAサイクル）を構築する。

◆ 各年度における対策の実施状況等を踏まえ、CISOが示す取組方針に従って、達成目標や複数年計画の見直しを行い、次年度の実施計画に反映する。

NISCによる確認・評価

◆ NISCにおいて、PDCAが適切に運営されていることや、標的型攻撃等の高度サイバー攻撃のためのリスク評価等に係る、CISOによる一連の指示・資源配分が適切になされたこと（プロセス有効性）を確認・評価し、その結果をCISO会議に報告する。

CISOが責任を持って、
方針・目標・資源配分を決定・指示。



統一基準群の見直しの方向性 :その他　主な見直し事項

基準の複雑化・肥大化の解消

- ◆ 冗長な表現を排除し、全体構成をシンプル化
- ◆ “Need to Knowの原則”、“情報のオーナーシップの原則”に基づき、情報の取扱に係る規定を明確化

技術の進展、環境の変化への対応

- ◆ 省内体制の確立、各省及びNISCとの連携等、障害・事故等への対処に係る規定を追加
- ◆ 府省庁提供のアプリ・コンテンツにおいて、不用意に利用者情報の収集等を行わないよう規定を追加
- ◆ 約款による外部の情報処理サービス（SNS,クラウドサービス等）の利用に係る規定を追加
- ◆ 私物スマートフォン等を業務で使う場合、各省庁の厳格な管理下に置くよう規定を追加
- ◆ IT機器・ソフトウェアの調達に当たり、国際規格の活用に係る規定を変更

統一基準群の改定スケジュール