政府機関等の情報セキュリティ対策のための統一基準群の見直し（案）について

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

①情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止、②IT資産管理の自動化とそれによる脆弱性への迅速な対応、③データ保護による情報漏えい対策の導入を、今後政府機関等が目指すべき3本の柱とし、これらの対策の導入を推奨。

2. 政府機関等のサービスの利用者の側に立った対策

政府機関等は、自らの情報システムのサイバーセキュリティ対策に加え、国民が安心して安全にウェブサイト等を通じて行政サービスを利用できるよう、“利用者側に立った追加的な対策”を講じる。

3. 政府機関等の自律的な能力向上への誘導（PDCA※サイクルの効果的運用）

一巡した府省庁監査の結果から得られた知見を統一基準群にフィードバック。自らの対策状況を評価し、より効果的な改善に繋げるべく、政府機関等の自律的なPDCAサイクルの更なる循環を促す。

※ PDCA：[Plan（計画）、Do（実行）、Check（評価）、Act（改善）]

4. 業務形態に対応した規定の整備

多様な業務形態が存在する独立行政法人等に目を向け、これらを踏まえたサイバーセキュリティ対策を導入。

（今後の対応）

- 本改定案についてパブリックコメントを募集。
- 夏頃に開催されるサイバーセキュリティ戦略本部において決定予定。
- 統一基準群改定後、政府機関等において速やかにポリシーの見直しが図られるよう、改定内容に係る説明会や勉強会の開催等、NISCとして必要な支援を実施予定。

情報セキュリティ対策のための統一基準群の構成

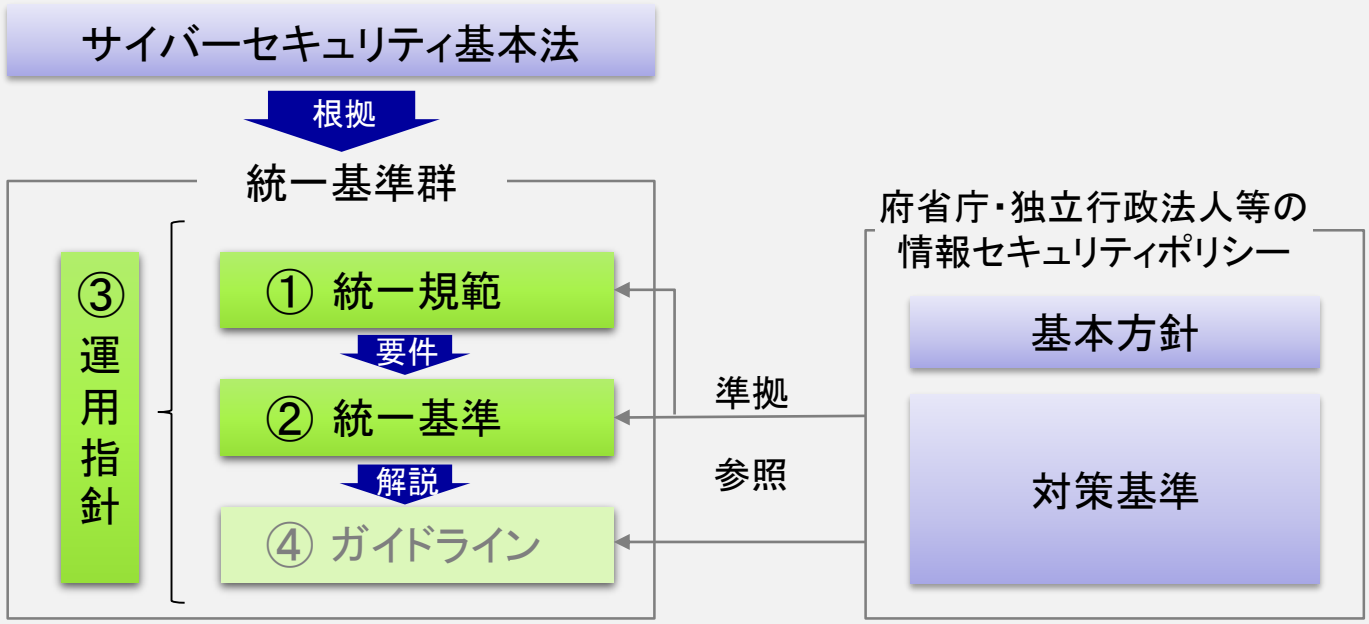
■ 統一基準群の対象

① 政府機関等の情報セキュリティ対策のための統一規範
② 政府機関等の情報セキュリティ対策のための統一基準
③ 政府機関等の情報セキュリティ対策の運用等に関する指針
　} サイバーセキュリティ戦略本部決定文書

④ 政府機関等の対策基準策定のためのガイドライン
　} 内閣サイバーセキュリティセンター決定文書

※ ①～③と関連性が高いドキュメントのため、同時に改定する。

■ サイバーセキュリティ基本法、統一基準群、政府機関等の情報セキュリティポリシーの関係



改定の概要1

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

≪主な内容≫

- ✓ 端末、サーバにおける『未知の不正プログラムの検知／実行の防止の機能の導入』
  ⇒未知の不正プログラム対策を「侵入後の検知」から「感染の未然防止」へ、「境界監視」に加え「プログラムが動作する内部」へ進化
- ✓ ソフトウェア等の情報を自動的に収集する『IT資産管理ソフトウェアの導入』
  ⇒脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応
- ✓ 情報へのアクセス制御機能として、『デジタル著作権管理による方式』を導入
  ⇒万が一ファイルが外部に流出しても、オンプレミス※／クラウドを問わず記録された内容の漏洩を防止し、ダメージを無効化

※ オンプレミス：[情報システムのハードウェアを自ら調達し主体的に管理する運用形態]

2. 政府機関等のサービスの利用者の側に立った対策

≪主な内容≫

- ✓ 『政府機関等の全WEBサイトの常時暗号化』の義務化を新設
- ✓ 『電子メール通信の暗号化対応』の義務化を新設

利用者の通信相手（ウェブサイト、メールの送信元）が真に政府機関であることを保証するとともに、通信途中での盗聴／改ざん／なりすましの防止を可能とし、国民の安心感を醸成

改定の概要2

3. 政府機関等の自律的な能力向上への誘導（PDCA サイクルの効果的運用）

≪主な内容≫

- ✓ 『情報セキュリティ対策の運用、自己点検、教育等』の取組において発生した課題をCISO※等責任者に報告させる規定を整備 **⇒責任者への報告を通じ、自らの課題の認識と、これに対する対応方針の検討を誘発し、自律的改善スパイラル（PDCAサイクル）を効果的に機能させる**
- ✓ CISOから、組織横断的及び部門特有の改善事項を、それぞれ適切な責任者に指示する規定を整備
  ⇒改善事項について、組織横断的取組及び部門特有の取組を、それぞれ効果的に推進させる
- ✓ 従来の責任者を中心に役割を規定していたことに加え、政府機関等の実情も踏まえ、情報セキュリティ対策の推進を担う部門を「情報セキュリティ対策推進体制」と位置付け、その役割を明確化
  ⇒マネジメントの更なる円滑な推進を促進

※CISO：[最高情報セキュリティ責任者 Chief Information Security Officer]

4. 業務形態に対応した規定の整備

≪主な内容≫

- ✓ モバイル端末の利用について、一定の安全対策を講じた場合には、組織内外のいずれにおいても端末をネットワーク接続して業務を行うことを可能とする規定を新設
  ⇒府省庁とは異なる独立行政法人等の柔軟な業務形態を支援すべく、統一基準群において、モバイル端末の柔軟な使用についての道を開拓
- ✓ 政府ドメイン名（go.jp）の使用に関する規定を見直し（『教育機関である法人における高等教育機関向けドメイン名（ac.jp）の使用に係る規定』を整備）
  ⇒独立行政法人において、業務の特性等に応じたドメイン名の選択を可能に

5. その他の見直し事項

≪主な内容≫

- ✓ IoT機器が統一基準群の規定の対象であることを明確化するとともに、安全対策に係る規定を追加
  ⇒一般の情報システムに加え、IoT機器にも防御の幅を広げる