NISC
National center of
Incident readiness and
Strategy for
Cybersecurity

「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」の改定（案）について

平成28年6月

内閣官房

内閣サイバーセキュリティセンター

統一基準群（平成26年度版）策定後の主な経緯

26年8月　民間企業の大量個人情報流出事案を踏まえた対策強化の指示

☛ 機微度の高い情報を始めとする情報管理の徹底を推進

27年1月　サイバーセキュリティ基本法の完全施行

☛ 独法の対策強化、戦略本部による監査の実施、NISCの機能強化等を推進

27年5月　日本年金機構における不正アクセスによる情報流出事案の発生

☛ 事案対処体制の強化、標的型攻撃を前提とした対策強化等を政府機関全体で推進

27年9月　新たなサイバーセキュリティ戦略の決定

☛ 新たに直面した脅威・課題への対応、IT製品・サービスの普及に伴う対策強化を推進

28年3月　サイバーセキュリティ人材育成総合強化方針の決定

☛ 政府機関における専門人材の確保・育成や一般職員の素養向上への取組方針

28年4月　サイバーセキュリティ基本法の改正法案の成立

☛ 指定法人への適用範囲の拡大等（公布の日から6月以内に施行）

統一基準群の位置づけの見直し及び独立行政法人等への適用範囲の拡大

統一基準群を、基本法に基づく政府機関及び独立行政法人等におけるサイバーセキュリティに関する対策の基準と位置づける。
独立行政法人等において、所管府省庁の助言等の下、情報セキュリティ対策が適切に講じられるよう、対策基準等の策定、体制の構築、対策実施状況の評価等に関する規定を追加する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋※）　※平成28年4月成立の改正法施行後の条文
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

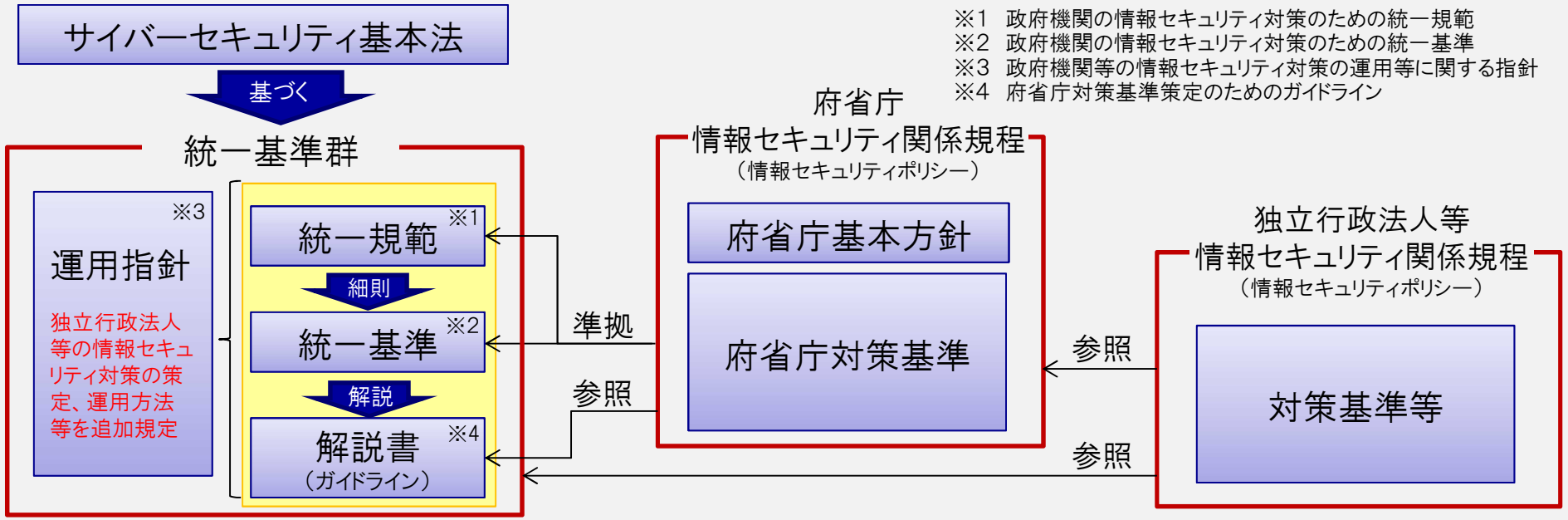
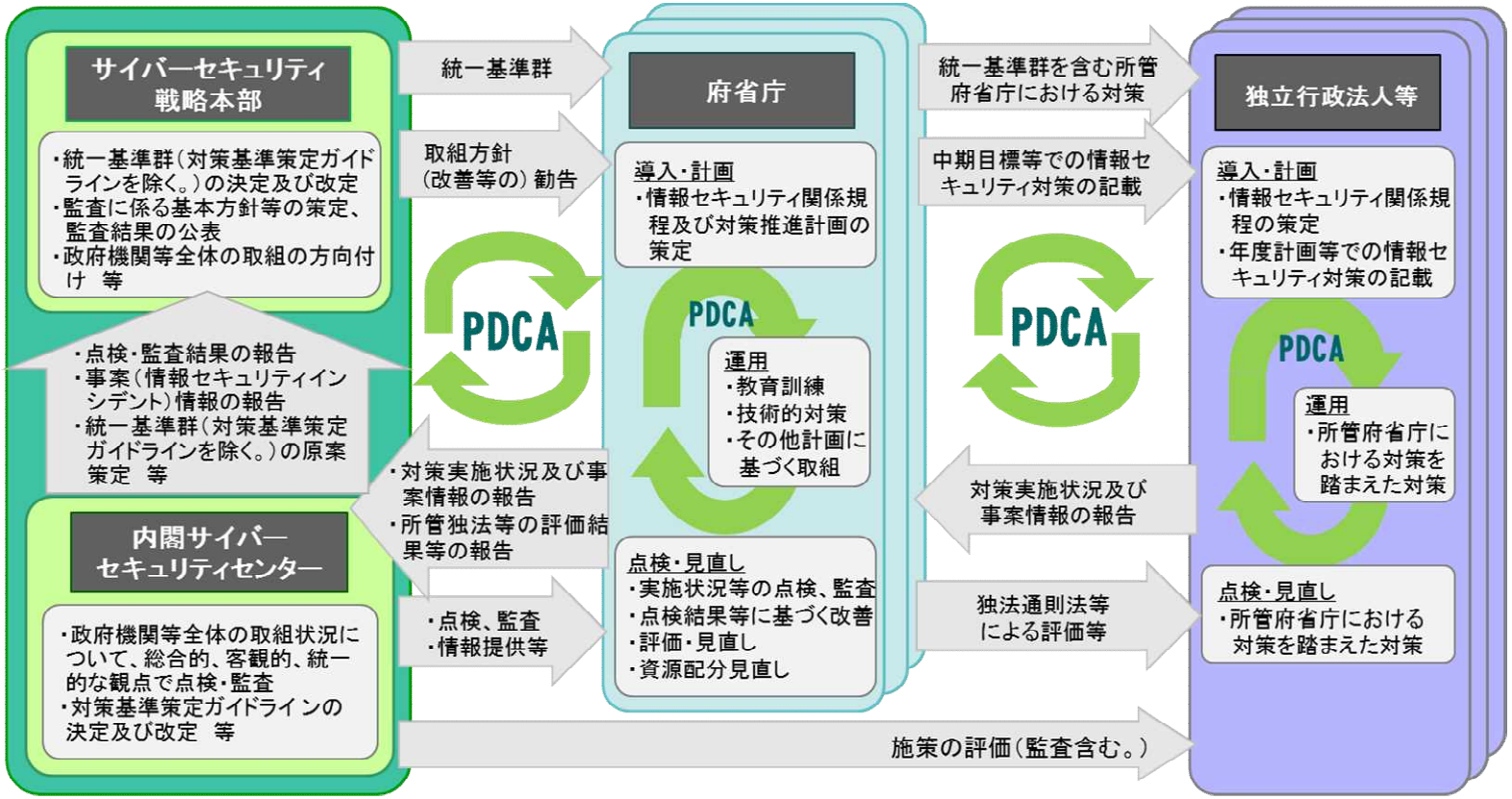


図　サイバーセキュリティ基本法と統一基準群及び情報セキュリティ関係規程の関係

監査に係る規定整備及び政府機関等の情報セキュリティ対策の強化

基本法第25条第1項第2号に基づく監査の実施に係る規定を整備し、以下のとおり独立行政法人等を含む政府機関等のセキュリティ強化に向けたPDCA※サイクルを明確化する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋：平成28年4月成立の改正法施行後の条文）
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。



※ PDCA：（Plan〔計画〕、Do〔実行〕、Check〔評価〕、Act〔改善〕）

日本年金機構事案等の外部動向を踏まえた規定の見直し・強化

日本年金機構における不正アクセスによる情報流出事案を始めとする事案（情報セキュリティインシデント）の発生状況やサイバー攻撃の動向、IT利活用環境の変化等を踏まえ、以下の規定の追加及び強化を図る。

事案発生に備えた対処体制（CSIRT※）、対処・連絡手順等の整備に係る規定の強化

- ◆ 事案対処に必要な知識・能力を有する対処体制（CSIRT）の構築、外部専門家による支援
- ◆ 発生した事案の対処に係る意思決定手法や判断基準、対処方法等の事前準備

※ CSIRT（Computer Security Incident Response Teamの略称）

標的型攻撃等による不正プログラム感染の発生を前提とする情報システムの防御策の強化

- ◆ 情報システムの重要な情報を扱う部分のインターネットからの分離
- ◆ セキュリティ監視の集中・強化等を目的とした、インターネット接続口の集約
- ◆ 実行プログラム形式ファイルが添付された電子メール受信時のシステム措置
- ◆ サイバー攻撃を受けた際の影響範囲の特定、原因究明等を適切に実施するための通信記録の管理

情報及び情報システムへの不正アクセスの防止等を目的とする対策の見直し・強化

- ◆ 個人情報や機微な情報を始めとした機密性・完全性の高い情報を大規模かつ体系的に管理するデータベースに対する対策

新たなIT製品・サービスの普及等に伴う対策事項の明確化

- ◆ 情報の取扱いを外部事業者に委ねる際のリスク評価に基づくクラウドサービス※利用可否の判断
- ◆ 必要に応じて委託事業の実施場所（クラウド構成機器の所在地等）、準拠法・裁判管轄の指定
- ◆ クラウドサービス及び提供事業者の信頼性の確認

※ 外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

今後の対応について

パブリックコメントの募集

改定原案についてパブリックコメントを募集し、提出のあった意見等を検討し、必要に応じて見直しを行い、サイバーセキュリティ戦略本部において夏頃に決定する。

府省庁・独法等の関係規程類の見直し

統一基準群改定後、府省庁や独立行政法人等において速やかに関係規程類の見直しが図られるよう、改定内容に係る説明会の開催、見直し状況の把握等、NISCとして必要な支援を行う。

指定法人の取扱い

サイバーセキュリティ基本法に基づき、指定法人に位置づけられた法人は、統一基準群に基づく情報セキュリティ対策を講ずるとともに、戦略本部による監査の対象となる。