２．社会全体のサイバーセキュリティ及びレジリエンスの向上　関係

政府機関等のサイバーセキュリティに係る施策の基準（政府統一基準）

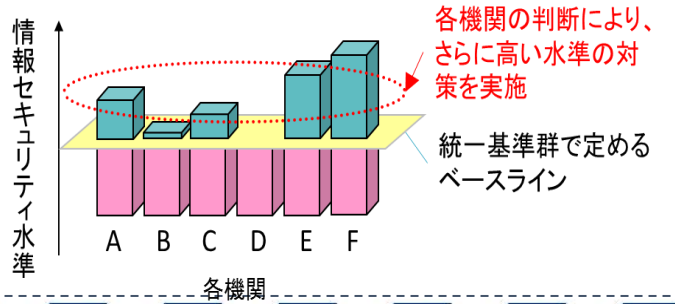
- 政府統一基準は、**サイバーセキュリティ基本法に基づく、政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み**。
- 統一基準では、**政府機関等が講ずるべき情報セキュリティ対策のベースライン**を定めている。
- 政府機関および独立行政法人等は、**政府統一基準に準拠**しつつ、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシーを策定**。これにより、政府機関等のどの組織においても、一定以上のセキュリティ対策の水準が確保されるよう図るもの。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）

第二十六条　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。

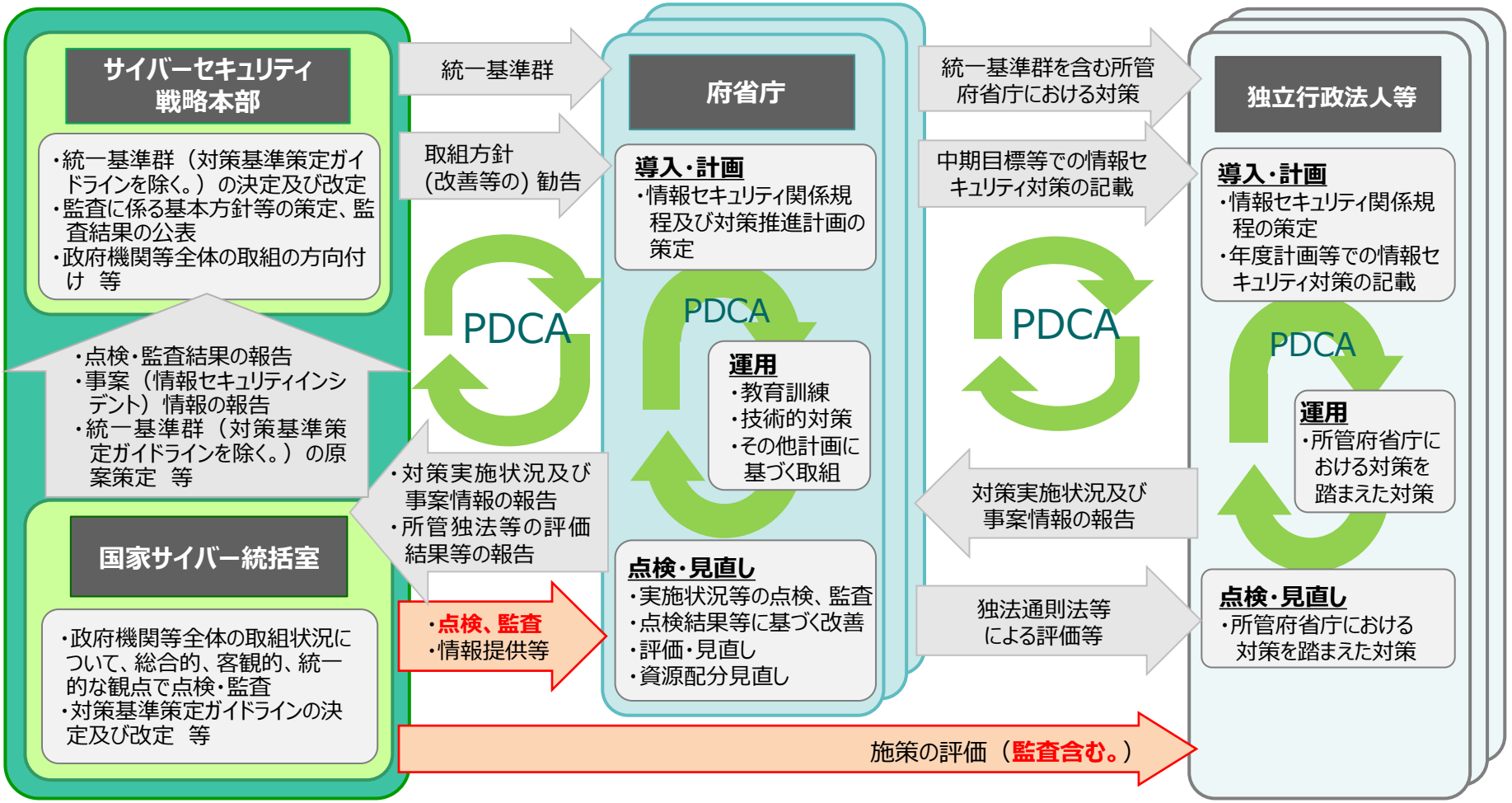
政府機関等のサイバーセキュリティ対策のための統一規範（令和７年６月27日サイバーセキュリティ戦略本部改定）（抜粋）

第六条　機関等は、自組織の特性を踏まえ、
基本方針及び**対策基準**を定めなければならない。
（略）
３　対策基準は、**統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように**定めなければならない。



政府機関等に係わる監査

- 監査業務は、サイバーセキュリティ基本法（平成26 年法律第104 号）第26 条第１項第２号においてサイバーセキュリティ戦略本部が行う事務に規定されている。



サイバーセキュリティ対策を強化するための監査に係る基本方針（最終改定 令和7年7月1日）

1 監査の目的

サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、対策強化のための自律的かつ継続的な改善機構であるPDCAサイクルが継続的かつ有効に機能するよう助言し、対策の効果的な強化を図る。

2 監査の対象

国の行政機関、独立行政法人及び指定法人※

※サイバーセキュリティ基本法第13条に基づき、サイバーセキュリティ戦略本部が指定する法人

3 監査の基本的な方向性

(1) 助言型監査

- 有益な助言を行う。
- グッドプラクティスを共有。

(2) 第三者的視点からの監査

- 内部監査とは独立した監査を実施。

(3) 各機関の状況を踏まえた監査

- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定

- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

4 監査の実施内容

(1)マネジメント監査

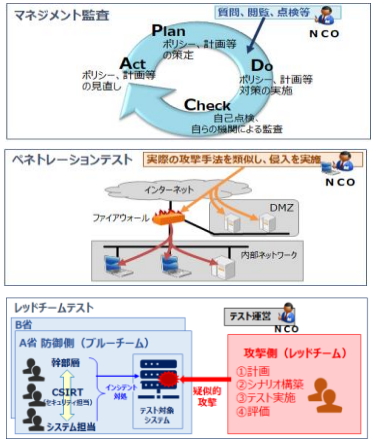
- 国際規格において基本的な考え方である組織全体としてのPDCAサイクルが有効に機能しているかとの観点から、検証する。
- 対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。

(2)ペネトレーションテスト

- 擬似的な攻撃を実施することによって、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。

(3)レッドチームテスト

- インシデントの検知能力や対応プロセスについて、組織・システム・人的側面を含めて多面的に評価し、改善のために必要な助言等を行う。



5 監査の進め方

(1) 監査方針の策定

- 年度ごとの監査の基本的な考え方を含む年度監査方針を、年次計画の一部として策定。

(2) 監査の実施

- 必要に応じて外部専門家が協力。
- 過年度の監査実施結果のうち重要な事項については、改善状況を継続的にフォローアップ。

(3) 個別の監査実施結果の通知

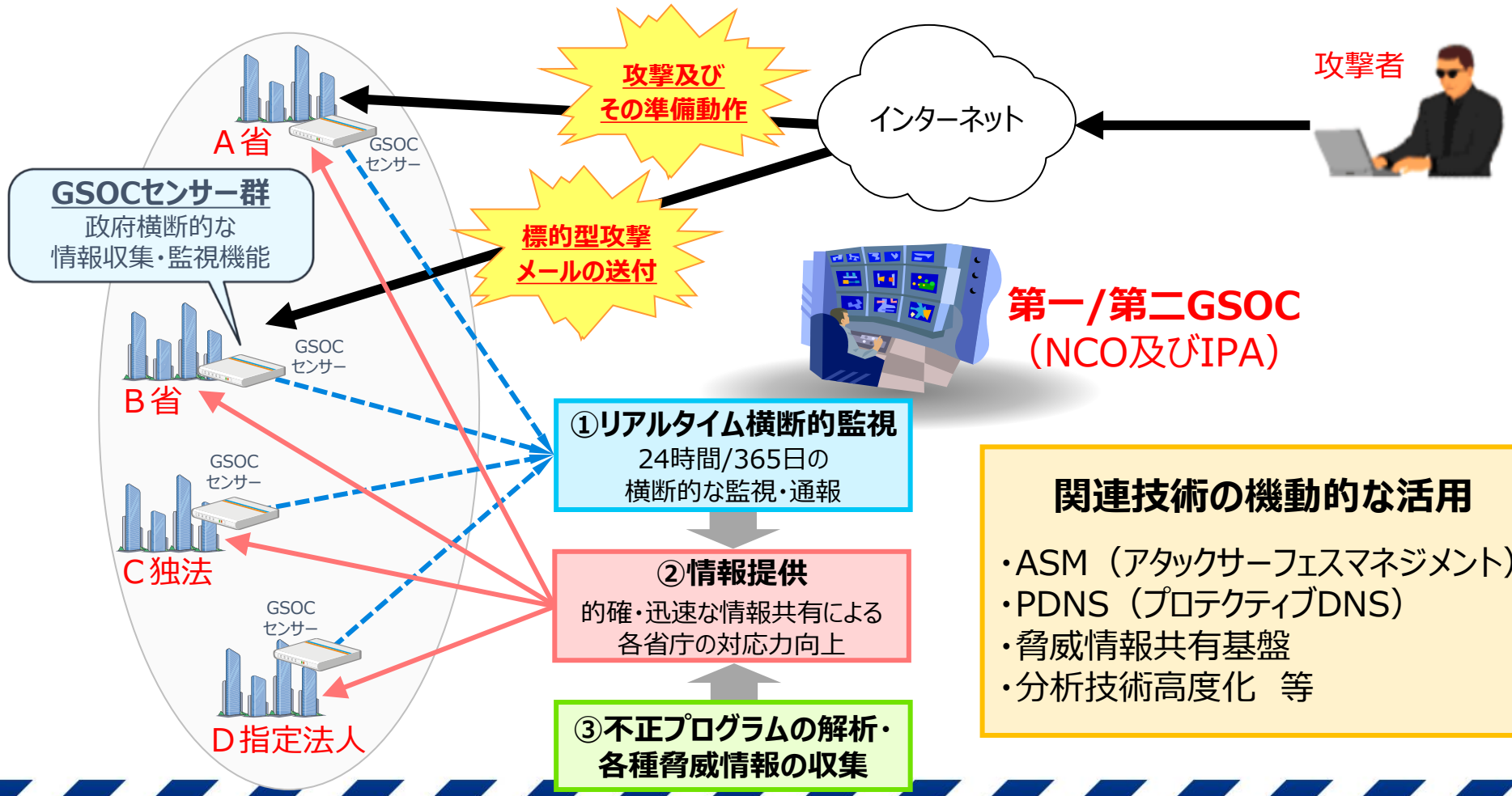
- 監査実施結果を、各機関の最高情報セキュリティ責任者（CISO）へ通知。
- 各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は計画を報告。

(4) 監査実施結果の取りまとめ・報告

- サイバーセキュリティの特性を踏まえ、攻撃者を利することのないよう配慮しつつ、当該年度に実施した監査の結果を取りまとめ。
- サイバーセキュリティ戦略本部に報告。

政府関係機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用

GSOC (Government Security Operation Coordination team)
目的：外部からのサイバー攻撃などに対して、政府関係機関の緊急対応能力強化を図る
【**第一GSOC**：政府機関が対象　**第二GSOC**：独法等が対象】

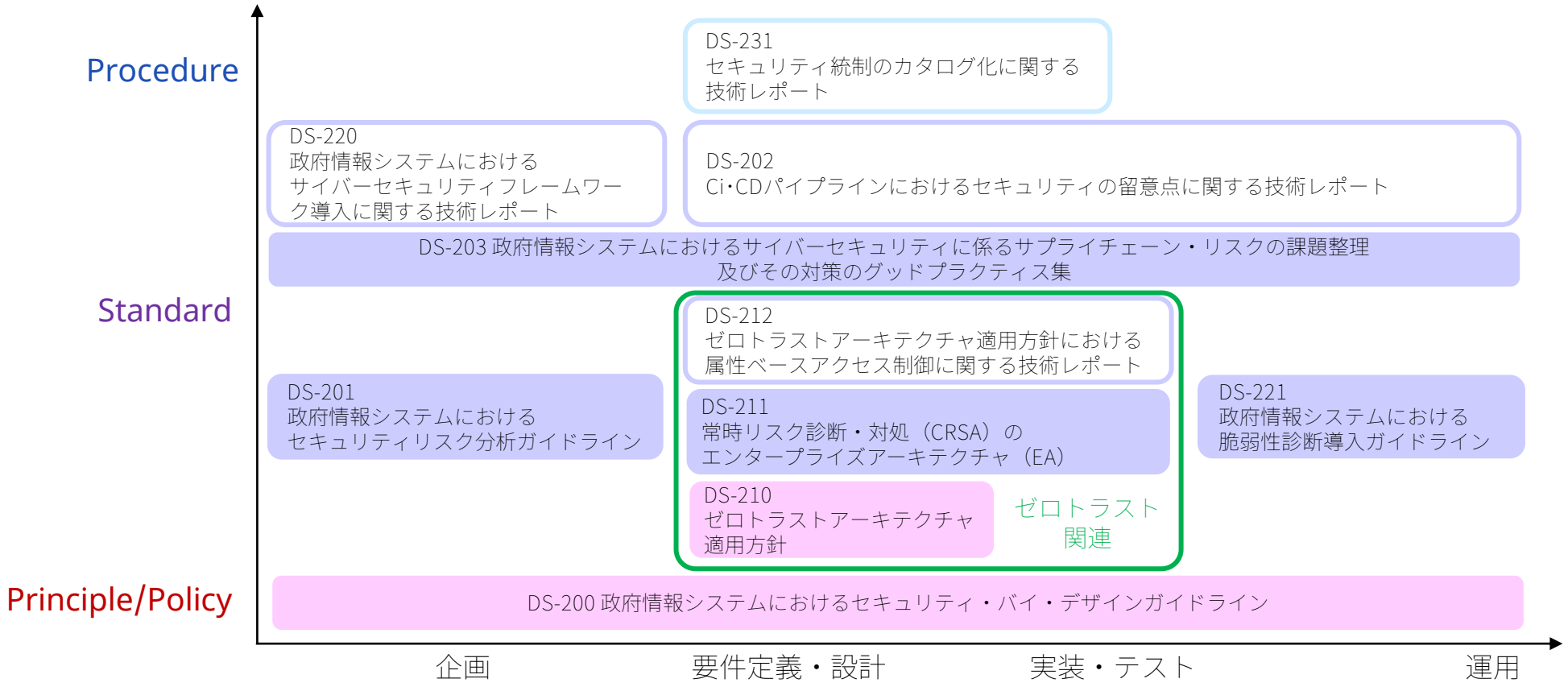


関連技術の機動的な活用

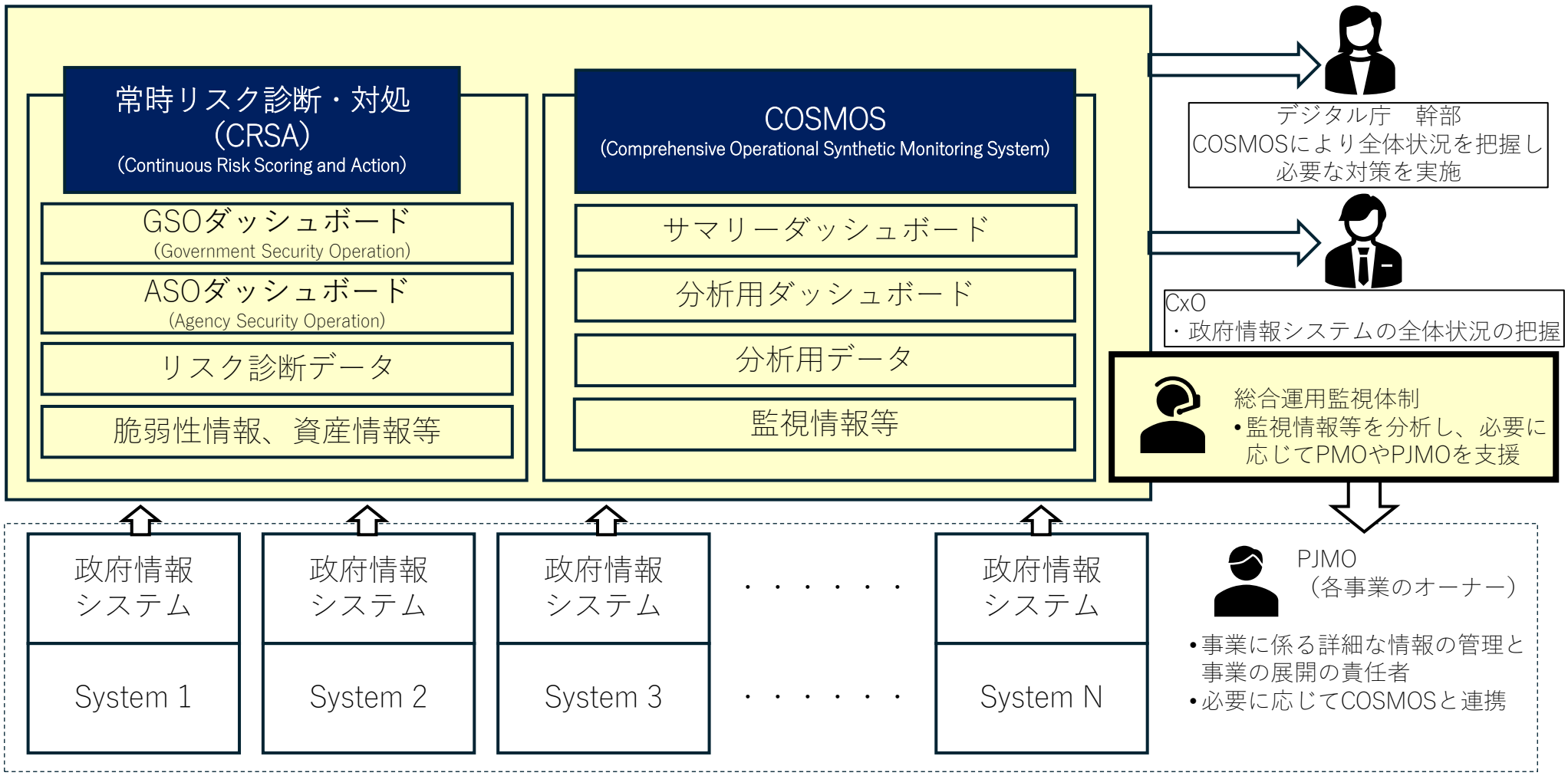
- ASM（アタックサーフェスマネジメント）
- PDNS（プロテクティブDNS）
- 脅威情報共有基盤
- 分析技術高度化　等

デジタル社会推進標準ガイドラインの策定

デジタル庁が、「サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続・手順や、各種技術標準等に関する共通ルール」をまとめた参考ドキュメント群
※セキュリティに関するドキュメントはDS-2XXで附番



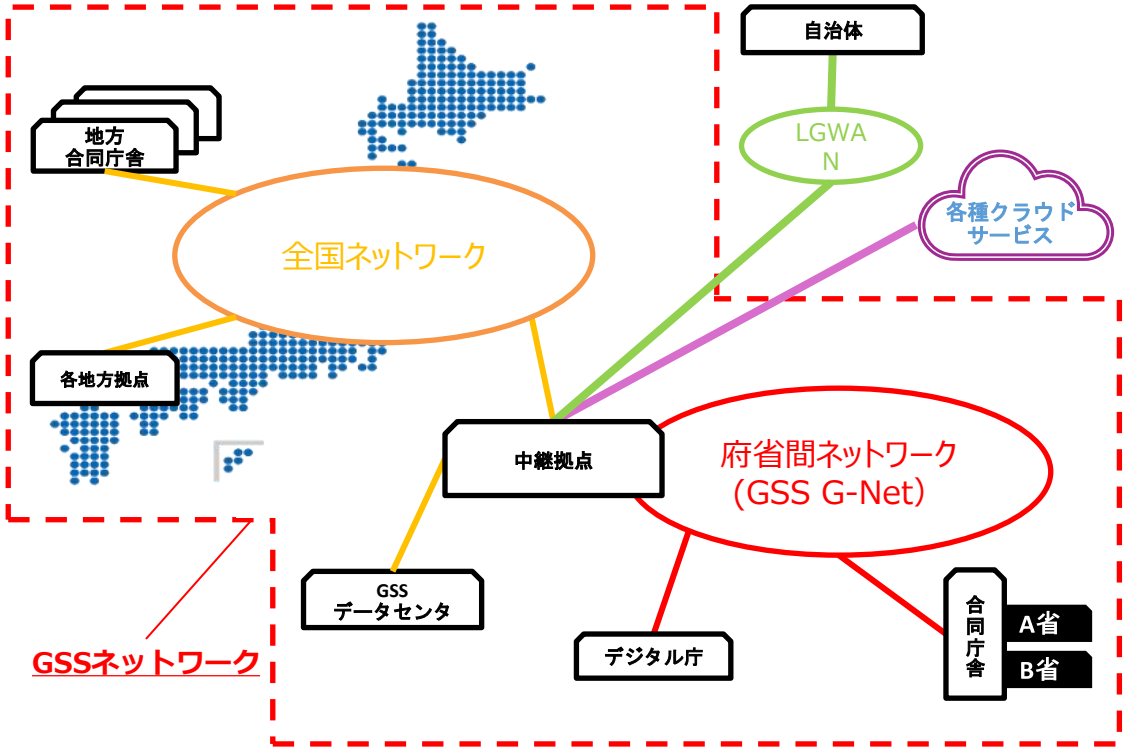
総合運用監視に係るシステム全体概要図



ガバメントソリューションサービス（GSS）

デジタル社会の実現に向け、**行政機関の利用するデジタル基盤の高度化**が必要となっている。

ガバメントソリューションサービス（GSS）では、その中の重要な要素である、**政府の共通基盤となる、柔軟で合理的なネットワークの構築と運用**を行う。



「デジタル社会の実現に向けた重点計画（重点政策一覧）」（R7.6.13閣議決定）の記載事項の概要

[ネットワーク面]

- ✓ 各府省庁は、引き続き、ネットワーク更改等を契機に、原則、GSSへの移行を進める
- ✓ 規模拡大や高度化するセキュリティ脅威に対応するため、各府省庁の人的協力を得て、機能強化及び保守・運用体制強化を進める

[業務実施環境面]

- ✓ 政府共通の標準的な業務実施環境（業務用PCやネットワーク環境）を提供
- ✓ GSS AMS（アカウント管理サービス）等利用者向けのサービスの利便性向上に取り組む

ガバメントクラウド

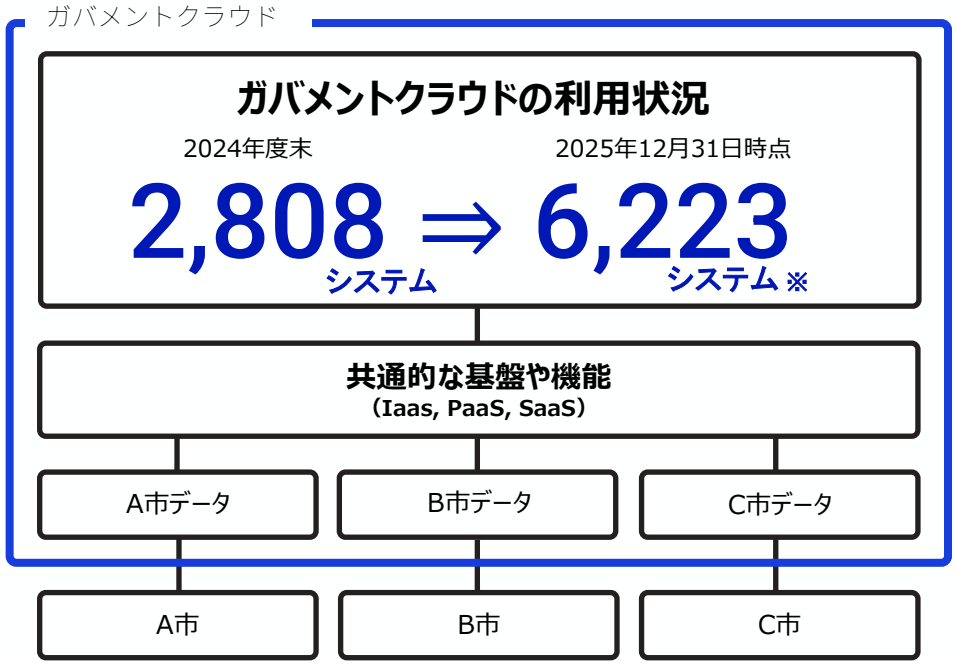
○ 従来は、行政機関はそれぞれ独自に業務システムの開発や保守運用を実施。利便性の高いサービスをスピーディに提供、改善するため、国や地方公共団体、準公共分野等で共通のクラウドサービス利用環境をガバメントクラウドとして提供。

○ 5つのサービスを提供し、6,223システムで利用（25年12月末現在）。

選定したクラウドサービス（2021年度～）

Amazon Web Services （アマゾン ウェブサービス）
Google Cloud （グーグル クラウド）
Microsoft Azure （マイクロソフト アジュール）
Oracle Cloud Infrastructure （オラクル クラウド インフラストラクチャー）
さくらのクラウド （※2025年度末までに全ての要件を満たす条件付き） （さくらインターネット株式会社）

ガバメントクラウドの利用状況



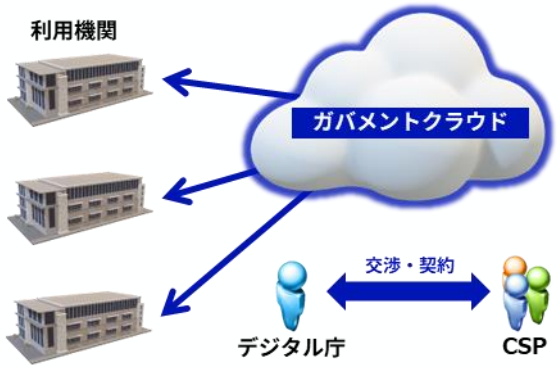
※内訳：国 159システム、地方公共団体 6,064システム

ガバメントクラウドへの移行の意義

- 従来少子高齢化社会が進み、急速な人口減少社会に突入する中で、質の高い公共サービスを維持し、国民のニーズの多様化に柔軟に対応していくためには、**国・地方公共団体・独立行政法人等の公共情報システムが共同で利用するガバメントクラウドの推進が重要。**
- ガバメントクラウドへの移行は、**事務の効率化、公共情報システム全体のセキュリティレベルの高度化、大規模災害対策の実現等にも資する。**

事務の効率化

◆ クラウドサービス事業者との交渉等は全てデジタル庁が行うため利用機関の負担が軽減



セキュリティレベルの高度化

◆ 海外のデータセンターの利用禁止や各種セキュリティ設定の制御など最高水準のセキュリティ対策をデジタル庁が一括して行うため、公共情報システム全体のセキュリティレベルの向上を実現

◆ 各機関ごとに行っていたセキュリティツール、データ分析ツールなどの調達や制御が不要

大規模災害対策の実現

◆ 日本国内に分散して設置されているクラウドサービス提供事業者の複数のデータセンターにシステムとデータを保管しているため、大規模災害発生時のシステム障害・停止やデータ紛失の可能性が低減し、業務継続性が大幅に向上