デジタル庁における
サイバーセキュリティの推進

2022年5月

デジタル庁

金田　圭史　（かなだ　けいし）

- 戦略・組織グループ　セキュリティ危機管理チーム
- デジタル庁　セキュリティスペシャリスト

略歴

- 2008年からNTTD、SecureWorksにてセキュリテイ関連の業務に従事（R＆D→調査→開発構築→監視→コンサル）
- 専門はシステムセキュリティ関連のコンサル、リスクアセスメント、セキュリティポリシー策定支援、セキュリティ戦略策定支援、グローバルセキュリティガバナンス、プライバシー保護等
- 2021年9月デジタル庁立ち上げと同時に入庁。セキュリティ技術関連ガイダンス作成や事務局業務を担当。デジタル庁のシステムセキュリテ関連施策諸々を担当（セキュリテイバイデザイン推進、セキュリテイ監査、コンサル等）

デジタル庁の組織体制

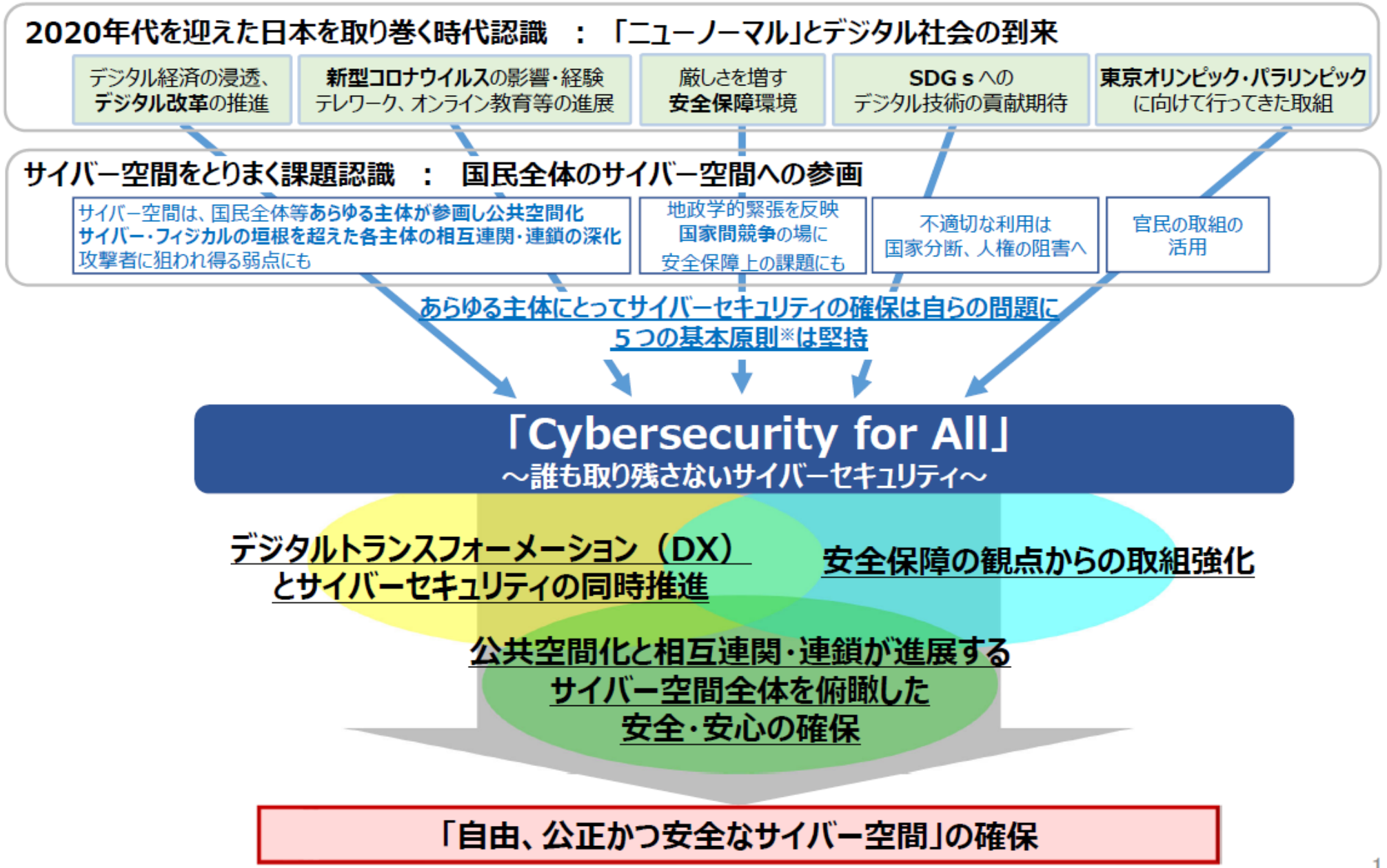
※ プロダクト（サービス）やプロジェクト毎に、必要な専門性に応じて、各人材プールから人材を配置。チームを組成して、プロジェクトベースで業務を行う。

<プロジェクト組成イメージ>

サイバーセキュリティ戦略

https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf

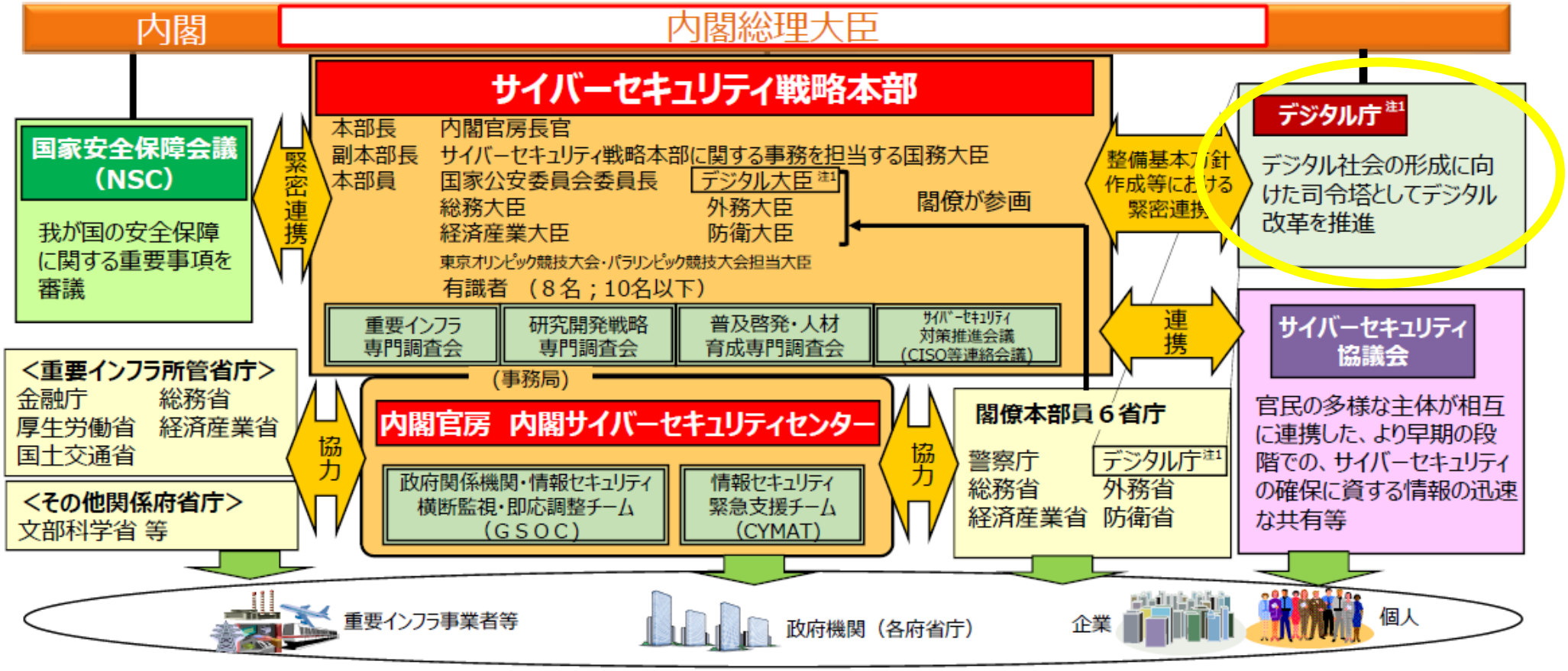
サイバーセキュリティ戦略の課題と方向性



※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

推進体制

- 我が国のサイバーセキュリティ政策により、自由、公正かつ安全なサイバー空間を確保するためには、政府一体となった推進体制が必要。デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを活用しその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。
- 各主体に期待される具体的な対策につながるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、NISCと関係府省庁が連携して、本戦略を国内外の関係者に積極的に発信。
- 本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。
- 年次報告・年次計画は、一体的に検討を行い、前年度の取組実績、評価及び次年度の取組を、戦略の事項に沿って、一連の流れを示すように整理。



（注1）デジタル社会形成基本法（令和３年法律第35号）、デジタル庁設置法（令和３年法律第36号）。（令和３年９月１日施行）

サイバーセキュリティ戦略①

４．２　国民が安全で安心して暮らせるデジタル社会の実現

・・・

これらの取組を通じて、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって、**国全体のリスクの低減とレジリエンスの向上**を図る。

４．２．２ デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

「誰一人取り残さない、人に優しいデジタル化」の実現のためには、国民目線に立った**利便性向上の徹底とサイバーセキュリティの確保の両立**が必要である。このため、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針（以下「整備方針」という。）において、サイバーセキュリティについても基本的な方針を示し、その実装を推進する。

・・・・

更に、国は**クラウド・バイ・デフォルトの実現を支える ISMAP 制度**を運用し、運用状況 等を踏まえて制度の継続的な見直しを行うとともに、民間における利用も推奨する。

7

サイバーセキュリティ戦略②

４．２．３ 経済社会基盤を支える各主体における取組①（政府機関等）

・・・・・

特に、各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は各 府省と共同で整備・運用し、**セキュリティも含めて安定的・継続的な稼働を確保**する。

・・・・・

また、国は第4期 GSOC（2021 年度～2024 年度）を着実に運用するとともに、**従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討**と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく。併せて、GSOC 等の在り方も検討する。 国は行政分野における**サプライチェーン・リスクや IoT 機器・サービス**（制御システムの IoT 化も含む）への対応を強化する。

国は**情報システムの設計・開発段階から講じておくべきセキュリティ対策**（認証機能、 クラウドサービス等における初期設定、脆弱性対応等）を実施する。 国は**セキュリティ監査や CSIRT訓練・研修等を通じて政府機関等におけるサイバーセキュリティ対応水準を維持・向上**する。

8

デジタル社会の実現に向けた重点計画

https://www.digital.go.jp/policies/priority-policy-program

デジタル社会の実現に向けた重点計画の概要

■ **デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策等**を定めるもの。（デジタル社会形成基本法37②等）

■ **デジタル社会の実現の司令塔であるデジタル庁のみならず各省庁の取組も含め工程表などスケジュール**とあわせて明らかにするもの。

我が国が目指すデジタル社会「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」

実現のための6つの方針

① デジタル化による成長戦略

② 医療・教育・防災・こども等の準公共分野のデジタル化

③ デジタル化による地域の活性化

④ 誰一人取り残されないデジタル社会

⑤ デジタル人材の育成・確保

⑥ DFFTの推進を始めとする国際戦略
※Data Free Flow with Trust

実現に向けての理念・原則

誰一人取り残されないデジタル社会の実現
→誰もが、いつでも、どこでもデジタルの恩恵を享受

デジタル社会形成のための基本原則
→10原則（デジタル改革基本方針）
①オープン・透明 ②公平・倫理 ③安全・安心 ④継続・安定・強靱 ⑤社会課題の解決 ⑥迅速・柔軟 ⑦包摂・多様性 ⑧浸透 ⑨新たな価値の創造 ⑩飛躍・国際貢献
→デジタル3原則（国の行政手続オンライン化原則）
デジタルファースト/ワンスオンリー/コネクテッド・ワンストップ

BPRと規制改革の必要性
※Business Process Reengineering

クラウド・バイ・デフォルト原則

デジタル化の基本戦略

デジタル臨時行政調査会
デジタル・規制・行政改革に通底する構造改革のためのデジタル原則を定め、全ての法令の適合性を確認

デジタル田園都市国家構想実現会議
デジタル原則の遵守やデータ基盤の活用等を前提に、各地域の社会的課題の解決などに向けた取組を支援

国際戦略の推進
DFFT/諸外国デジタル政策関連機関との連携強化

包括的データ戦略の推進
トラスト/ベース・レジストリ/オープンデータ

安全・安心の確保
サイバーセキュリティ/個人情報保護/サイバー犯罪

デジタル産業の育成
ベンチャー・中小企業等の育成

デジタル社会の実現に向けた基本的な施策

国民に対する行政サービスのデジタル化

- **国・地方公共団体・民間を通じたトータルデザイン**（アーキテクチャの将来像整理）
- **新型コロナウイルス感染症対策など緊急時の行政サービスのデジタル化**
（ワクチン接種証明書のスマホ搭載の推進/公金受取口座登録開始及び行政機関による利用）
- **マイナンバー制度の利活用の推進**
（情報連携の拡大/各種免許等のデジタル化）
- **マイナンバーカードの普及及び利用の推進**
（健康保険証利用のための環境整備/R6年度末に運転免許証との一体化/ユースケース拡充）
- **公共フロントサービスの提供等**
（ワンストップサービスの推進）

暮らしのデジタル化

- **準公共分野のデジタル化の推進等**
（健康・医療・介護（PHR/オンライン診療）/教育（校務のデジタル化/教育データ利活用）/防災/こども/モビリティ/取引）

産業のデジタル化

- **事業者向け行政サービスの質の向上に向けた取組**
（電子署名/電子委任状/商業登記電子証明書/GビズID/e-Gov）
- **中小企業のデジタル化の支援**（IT専門家派遣/IT導入補助金/サイバーセキュリティ対策支援）
- **産業全体のデジタルトランスフォーメーション**
（DX認定制度/DX銘柄選定/DX投資促進税制/サイバーセキュリティ強化）

デジタル社会を支えるシステム・技術

- **国の情報システムの刷新**
（重要システム開発体制整備/ガバメントクラウドの整備/ネットワークの整備）
- **地方の情報システムの刷新**
（標準化基本方針の策定等）
- **デジタル化を支えるインフラの整備**
（5G/光ファイバ/データセンター/海底ケーブル/半導体）
- **デジタル社会に必要な技術の研究開発・実証の推進**（情報通信・コンピューティング・セキュリティ技術高度化/スーパーコンピュータ整備）

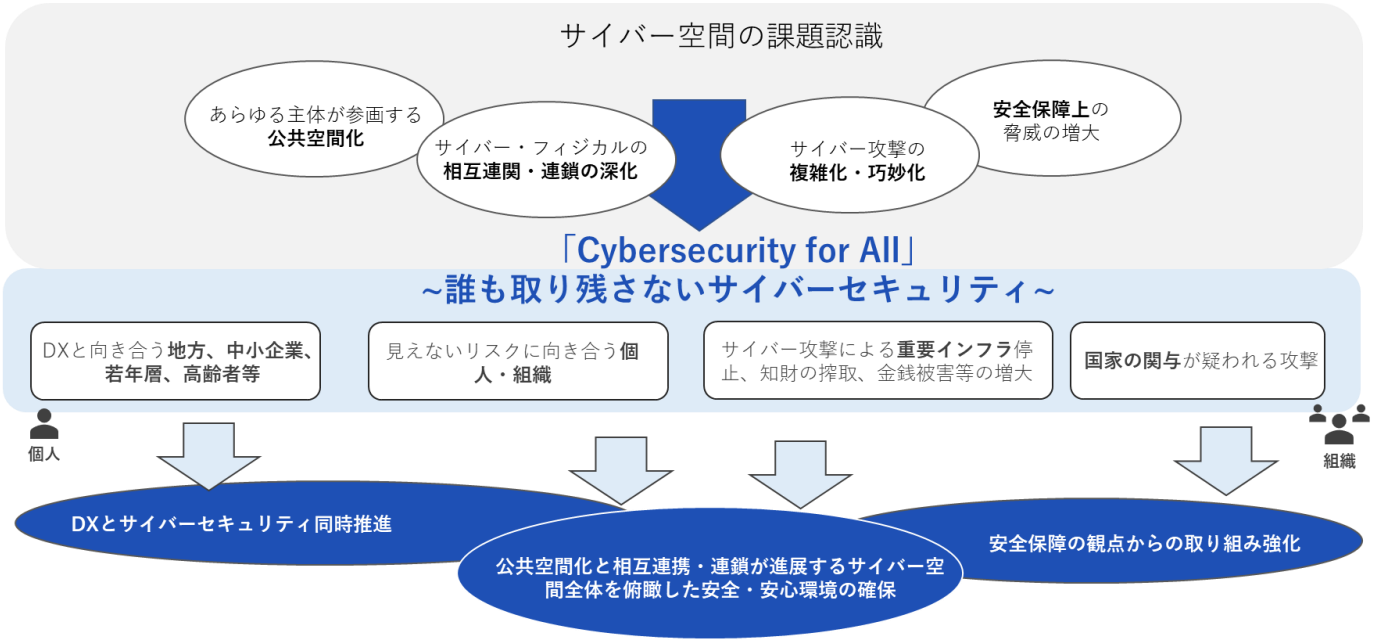
デジタル社会のライフスタイル・人材

- **ポストコロナも見据えた新たなライフスタイルへの転換**
（テレワーク/シェアリングエコノミー）
- **デジタル人材の育成・確保**
（プログラミング必修化/リカレント教育）

デジタル社会の実現に向けたサイバーセキュリティの重点計画

「**利便性とサイバーセキュリティの確保**」を目指す姿とする。

目指す姿の実現向けて基本方針を示し、この方針に基づいたサイバーセキュリティ対策の評価を図る。



- **基本方針の提示**
  - 政府情報システムの整備・運用
- **セキュリティ・バイ・デザイン、DevSecOps**を含めたセキュリティ対策の実施
- 安定的・継続的な稼働の確保等の観点から**検証・監査の実施体制の構築**
  - デジタル庁システム
  - デジタル庁・各府省共同のシステム
- **レジリエンスの向上**を目的としたリアルタイムな監視と順守状況の確認
  - インシデントの早期発見
  - 被害の最小化
  - 回復の迅速化

  ・リソース確保
  ・ルール・体制の構築

高度セキュリティ技術の研究開発	情報管理手法やシステムの挙動・ソフトウェアの状況を**リアルタイムに監視**するための常時診断・対応型のアーキテクチャ

情報システムの整備及び管理の基本的な方針

https://www.digital.go.jp/policies/posts/development_management

４つの重点注力分野

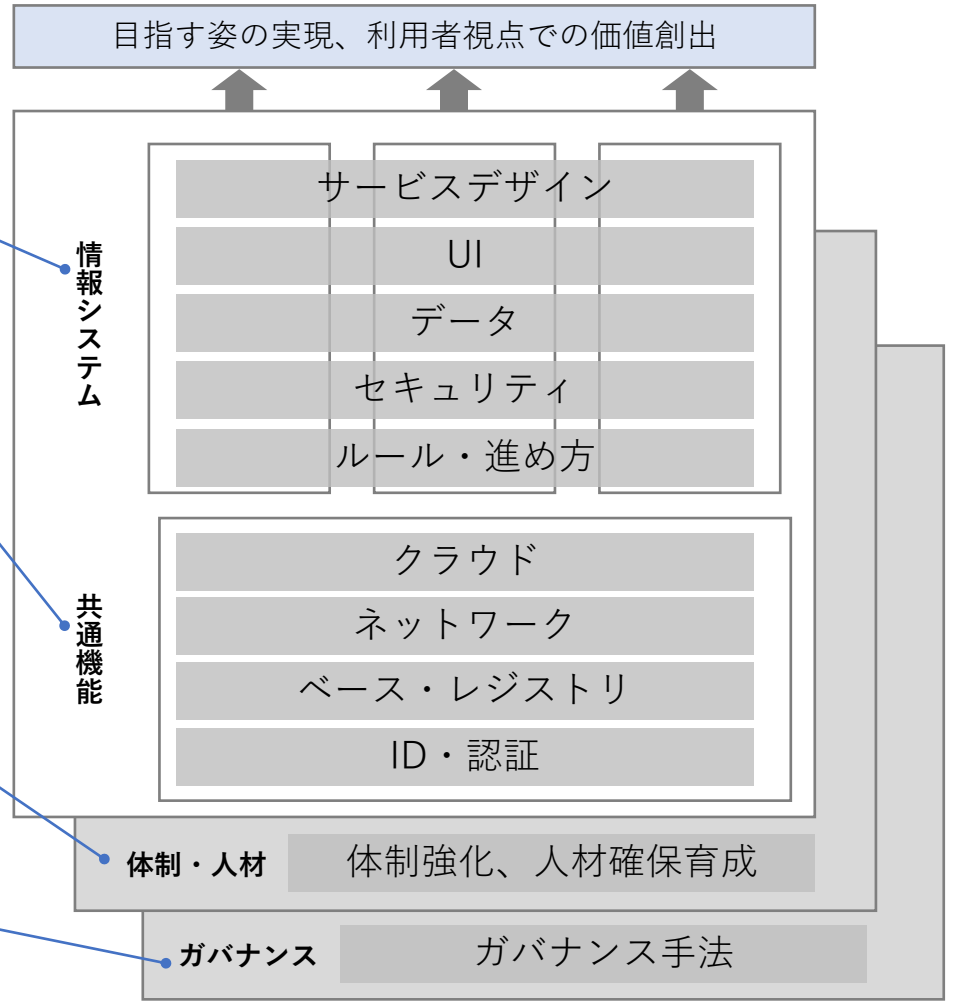
関係者が個々に努力するだけでは、目指す姿を実現できない。デジタル庁自身が特に４つの領域に注力し、旧来の課題を解消するとともに、**国・地方公共団体・独立行政法人・準公共分野等の関係者が効果的に協働**できるようにする。

1 良いサービスを作るための **標準** の策定・推進

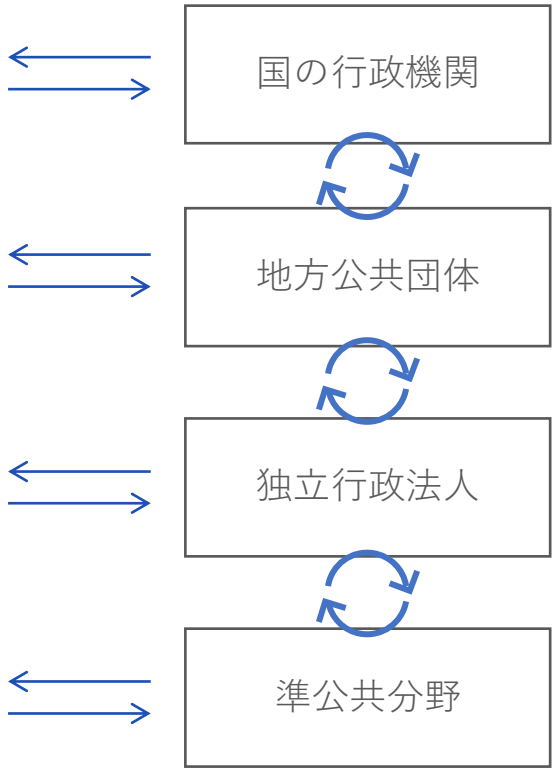
2 良いサービスを支える **共通機能** の整備・展開

3 緻密な改善を実現する **体制** 強化

4 推進力を強化するための **ガバナンス** 手法の見直し



デジタル庁は、各関係者にとって利便性の高い標準、共通機能等となるように、利用状況を踏まえて**継続的に改善**を行う



1　良いサービスを作るための「標準」の策定・推進

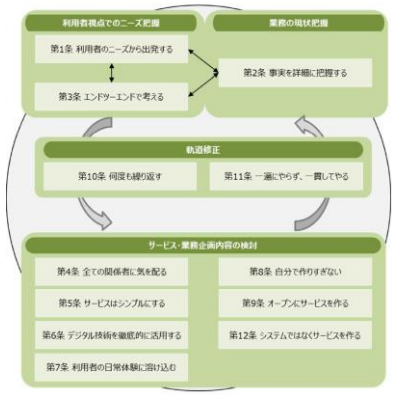
利用者視点で良いサービスを作るために、各情報システムを横断して統一すべき技術標準や進め方等について、デジタル庁自身が各プロジェクトで実践を行いながら、技術検討会議を中心に成果をまとめ、継続的改善を行う。

技術検討会議を中心とする検討

サービスデザイン

利用者が実感できる効果を創出するためには、利用者の立場で実際に発生している事実を正しく把握し、利用者と協働で改善を行う**サービスデザイン思考**が重要。

サービス設計12箇条の導入促進

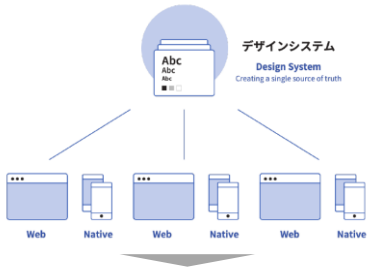


今までも標準ガイドライン等で周知展開を図っていた。デジタル庁自身が各プロジェクトで率先して**推進を徹底**する。

UIの改善

「誰一人取り残されない」デジタル化を進めるため、**ユニバーサルデザインを考慮したUI**の設計等、利用者目線で、利用者に優しい行政サービスを実現。

デザインシステムの整備
（ツールだけでなく、ガイド等を含む仕組み）



統一ウェブの推進

デジタル庁ウェブサイトで先行実証し、各省ウェブサイト等へ段階展開

データ整備

「包括的データ戦略」に基づき、データ活用、データ連携を推進する。

データの利活用や管理が効率的に行われるようにするために、**データ品質管理**フレームワークと評価モデルを整備する。

データの相互運用性を確保するために、データの記述形式、共通に解釈できる語彙、使用する文字の統一といった標準化を図る。

セキュリティ

複雑化・巧妙化したサイバー攻撃のリスクを踏まえ、サイバーセキュリティについての基本方針を定める。

常時診断・対応型セキュリティアーキテクチャの推進
従来の「境界型セキュリティ」の考え方ではなく、ゼロトラストアーキテクチャに基づいてセキュリティを確保する考え方へ。

サイバーレジリエンスの向上
セキュリティフレームワークとして識別、防御、検知、対応、復旧を認識し対応することにより、セキュリティ対策による機密性の確保に加え、情報システムの完全性、可用性の強化も目指す。

ポリシーと対策の関係性構造化及び追跡性確保
リアルタイムでのデータによるモニタリングを推進し、セキュリティポリシー及びセキュリティ対策の関係性等を構造化して追跡可能とする。

ルール・進め方

業務改革（BPR）を徹底し、利用者から見たエンドツーエンドで事実を詳細に把握した上で、行政サービスの利用者と行政機関間のフロント部分だけでなく、行政機関内のバックオフィスも含めたプロセスの再設計を行う。また、投資対効果を精査を十分に行う。

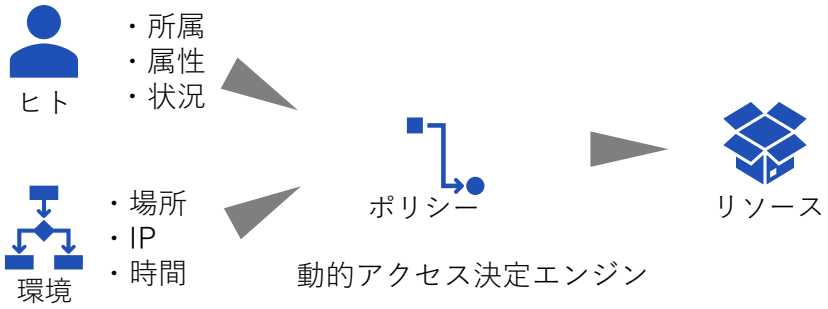
情報システムの企画、予算、調達、設計開発、運用等の実務について規定する**標準ガイドライン等**について、現場のプロジェクトを円滑に推進する観点から継続的改定を行う。

※ 技術検討会議 ： 整備方針の策定や各省が遵守すべき標準ガイドライン群の策定・改訂等を行うためにデジタル庁が設置した会議

政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針

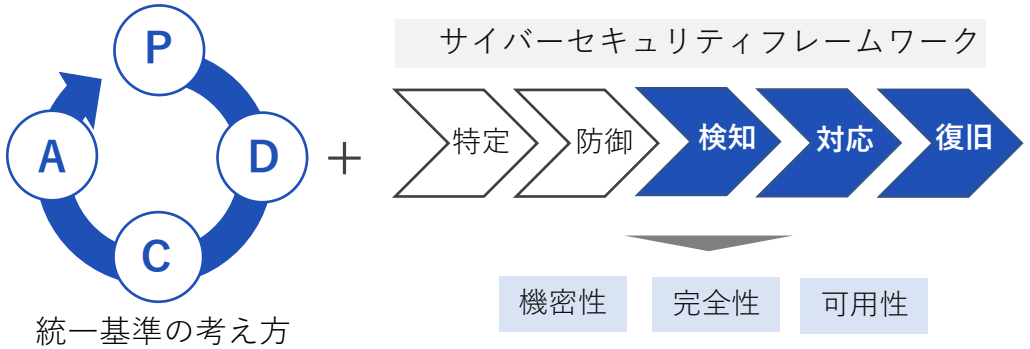
共通機能を前提とした常時診断・対応型のセキュリティーアーキテクチャ実装推進

- 「境界型のセキュリティ対策」に加え、**ゼロトラストアーキテクチャ**の考え方に基づきセキュリティ確保。これにより**属性情報ベースのアクセス制御**を実現する。
- その上で**業務のリスク分析**に基づく**企画・設計と運用を通した継続的なセキュリティ対策**を実施する。



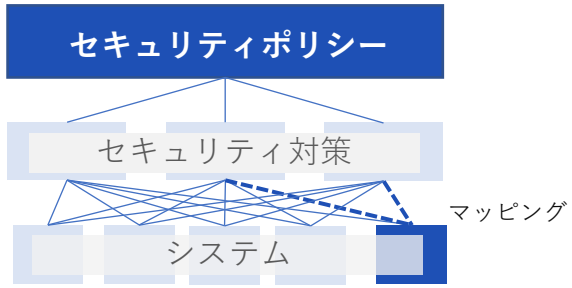
サイバーレジリエンスの強化

- 脅威の侵入を前提とし、検知・対応・復旧を行うレジリエンスを実現するため、統一基準に加え、**サイバーセキュリティフレームワーク**の導入し、被害の最小化及び回復の迅速化を図る。
- **脆弱性診断、安定的・継続的な稼働確保等**の観点の検証、**バックドアの有無**の検証等を実施する。



セキュリティのポリシーと対策の構造化及び追跡性の確保

- セキュリティポリシーとセキュリティ対策の**構成要素化とその関係性の構造化**を行うことで、**追跡可能性を確保し**、必要なセキュリティ対策の実施状況を**リアルタイムかつ容易に把握**する。

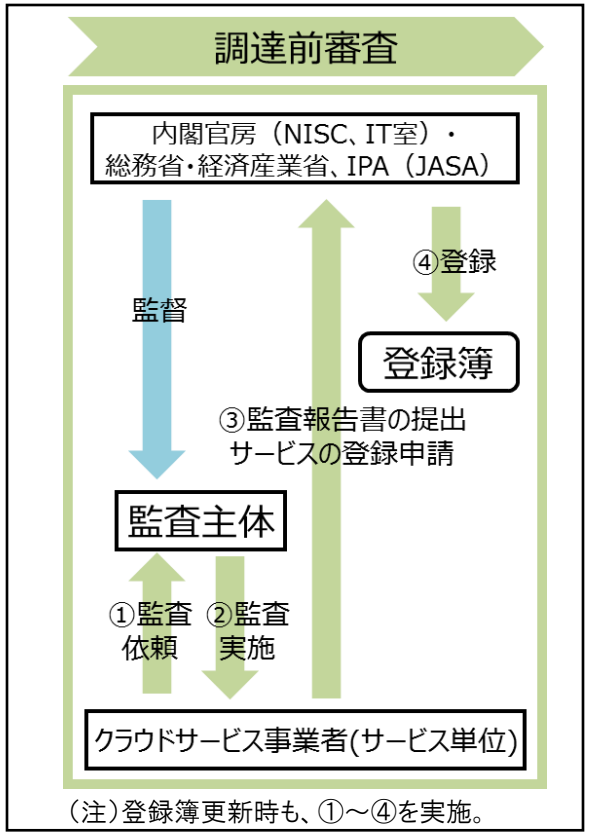


政府情報システムのためのセキュリティ評価制度（ISMAP）

【参考】ISMAPのセキュリティ確保の仕組み

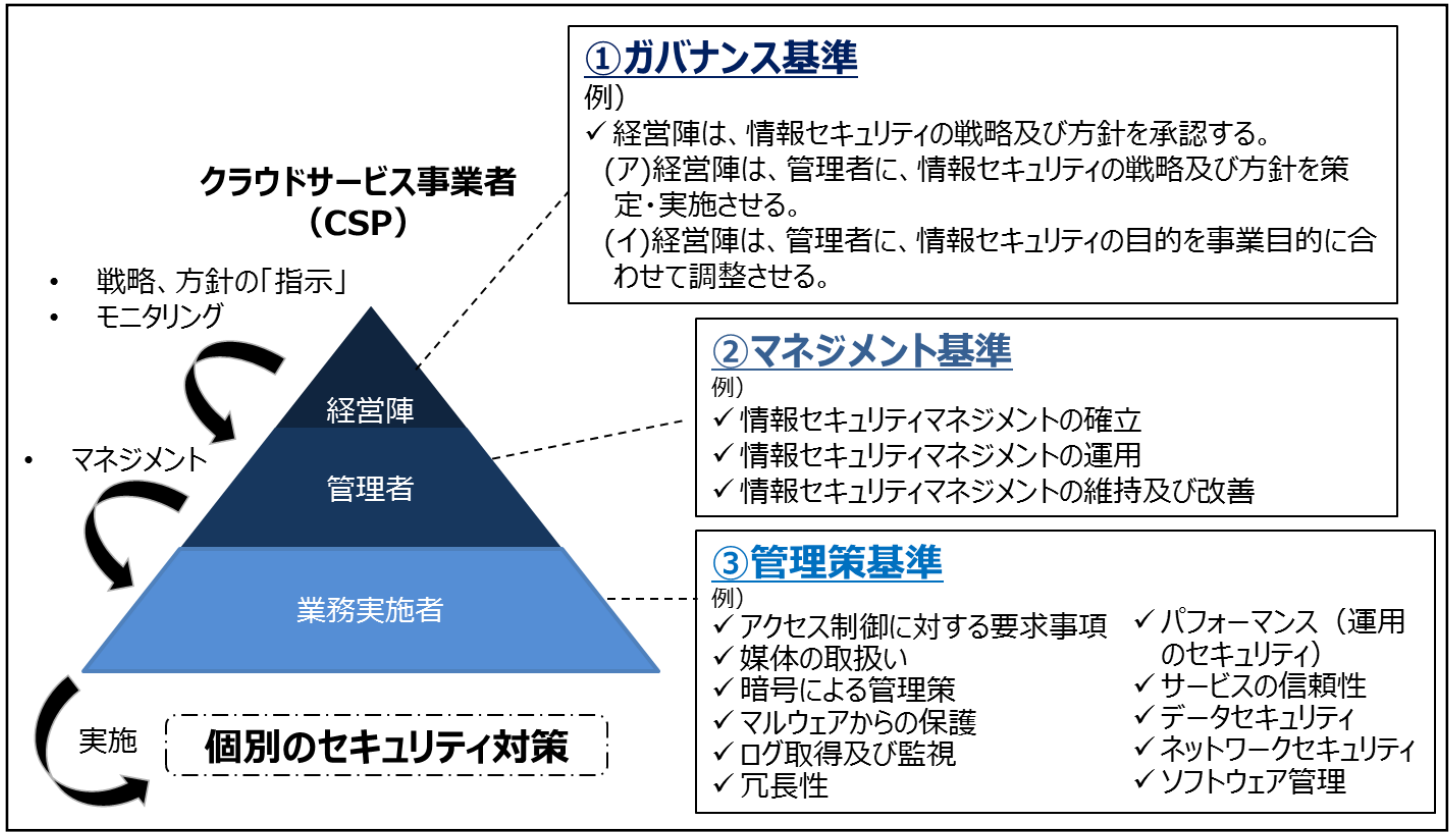
- 本制度は、クラウドサービスの情報セキュリティに関する**JIS Q(ISO/IEC) 27017等を基礎**としてクラウドサービスに係る**統一的なセキュリティ基準（管理基準）**を策定・公表。基準の策定の際には、システム監査にかかる知見者を集めたＷＧにおいて膝詰めで議論。
- 本制度が選定する**監査主体による監査プロセスを経て、クラウドサービス事業者（CSP）において、管理基準が適切に実施されているかを確認**。**毎年、登録簿更新審査を行い、継続的な確認**を実施。
- 管理基準では、情報セキュリティマネジメントに加えて、クラウドサービスのパフォーマンス、信頼性、データ、ネットワーク、ソフトウェア等に係る**セキュリティ対策の実装を要求**しており、**監査においてもこれらの実装状況まで確認**を行うこととしている。

CSP登録の流れ

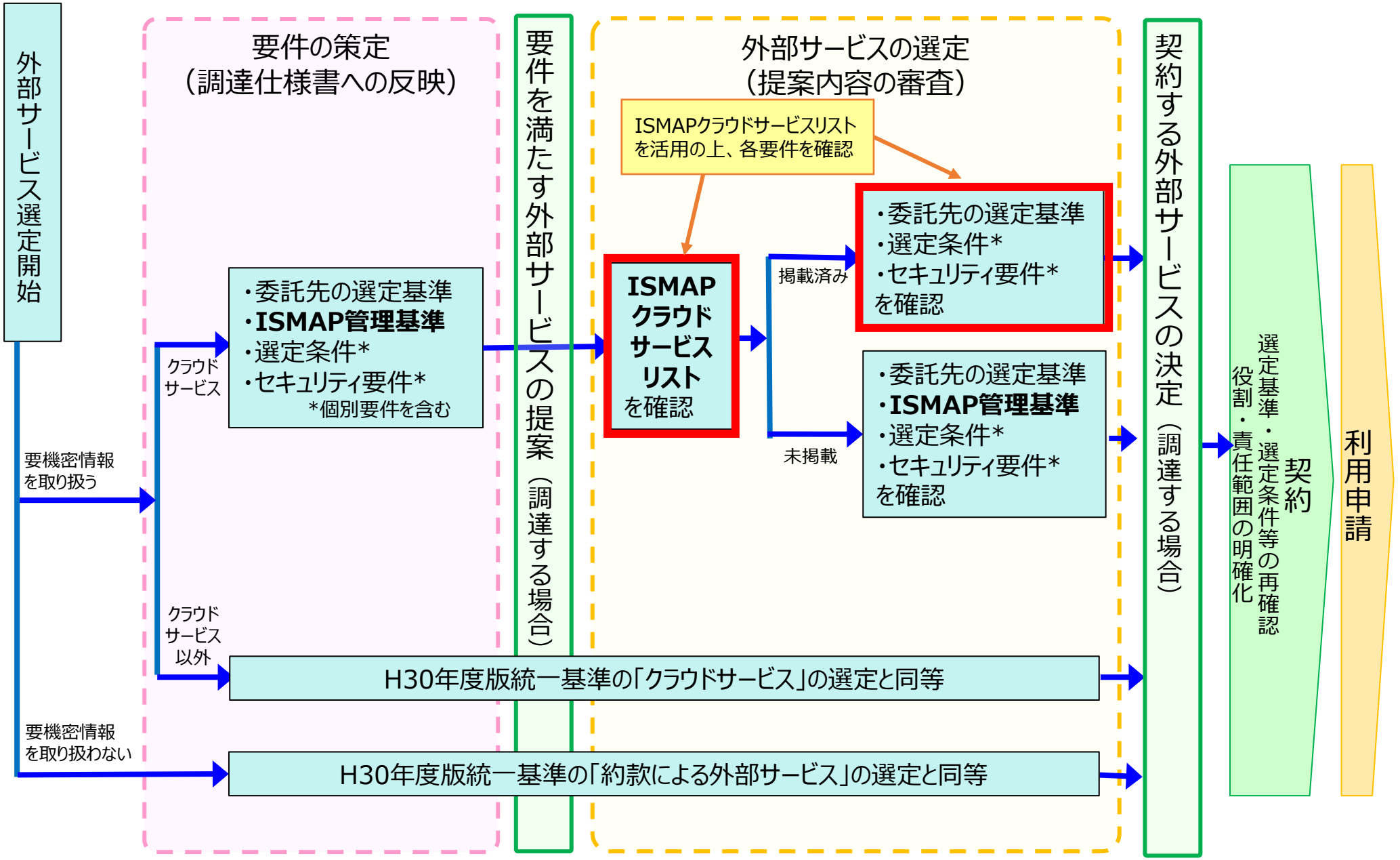


（注）登録簿更新時も、①～④を実施。

管理基準の構成



令和３年度版統一基準群に基づくクラウドサービス等の選定の流れ



https://www.ismap.go.jp　ホーム>コンテンツ>制度案内 (コンテンツグループ)>ISMAP概要

ISMAP管理基準のイメージ

- 管理基準は、**統制目標とされる3桁管理策（A.x.x.x）**と、それを達成するための手段となる**詳細管理策である4桁管理策（A.x.x.x.x）**で構成される。
- 原則として**３桁管理策を必須**、**4ケタ管理策は選択性**とし、一部の重要な管理策を必須とする。

３桁管理策：統制目標　※全て必須

管理策番号	管理策
8.1.2	目録の中で維持される資産は、管理する。
8.1.2.1	資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。
8.1.2.2	資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。
8.1.2.3	資産の管理責任者は、資産の目録を作成する仕組みを整備する。
8.1.2.4	資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。
8.1.2.5	資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。
8.1.2.6	資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。

４桁管理策：手段　※原則選択性。全て必須に規定してしまうと、動的な変化への対応が困難。

③詳細情報の添付文書（統制目標の管理策） （例　Open Canvas）

OpenCanvas (IaaS)　基本言明要件のうち実施している統制目標の管理策

統制目標番号	統制目標番号	統制目標番号	統制目標番号	統制目標番号	統制目標番号	統制目標番号
3.1.2	3.1.3	3.1.4	3.1.5	3.1.6		
4.4.1	4.4.2	4.4.3	4.4.4	4.4.5	4.4.6	4.4.7
4.4.8	4.5.1	4.5.2	4.5.3	4.5.4	4.5.5	4.6.1
4.6.2	4.6.3	4.7.1	4.8.1	4.8.2	4.9.1	4.9.2
5.1.1	5.1.2					
6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.2.1	6.2.2
6.3.1.P						
7.1.1	7.1.2	7.2.1	7.2.2	7.2.3	7.3.1	
8.1.1	8.1.2	8.1.3	8.1.4	8.1.5.P	8.2.1	8.2.2
8.2.3	8.3.1	8.3.2	8.3.3			
9.1.1	9.1.2	9.2.1	9.2.2	9.2.3	9.2.4	9.2.5
9.2.6	9.3.1	9.4.1	9.4.2	9.4.3	9.4.4	9.4.5
9.5.1.P	9.5.2.P					
10.1.1	10.1.2					
11.1.1	11.1.2	11.1.3	11.1.4	11.1.5	11.1.6	11.2.1
11.2.2	11.2.3	11.2.4	11.2.5	11.2.6	11.2.7	11.2.8
11.2.9						
12.1.1	12.1.2	12.1.3	12.1.4	12.1.5.P	12.2.1	12.3.1
12.4.1	12.4.2	12.4.3	12.4.4	12.4.5.P	12.5.1	12.6.1
12.6.2	12.7.1					
13.1.1	13.1.2	13.1.3	13.1.4.P	13.2.1	13.2.2	13.2.3
13.2.4						
14.1.1	~~14.1.2~~	~~14.1.3~~	14.2.1	14.2.2	14.2.3	14.2.4
14.2.5	~~14.2.6~~	~~14.2.7~~	14.2.8	14.2.9	14.3.1	
15.1.1	15.1.2	15.1.3	15.2.1	15.2.2		
16.1.1	16.1.2	16.1.3	16.1.4	16.1.5	16.1.6	16.1.7
17.1.1	17.1.2	17.1.3	17.2.1			
18.1.1	18.1.2	18.1.3	18.1.4	18.1.5	18.2.1	18.2.2
18.2.3						

●実施している統制目標の管理策

ISMAPが国際規格や統一基準等を踏まえ策定したISMAP管理基準には、統制目標（３桁管理策）と、それを達成するための手段（４桁管理策）があり、本欄においては、統制目標の言明状況を記載している。

●対象外としている統制目標の管理策

斜線については、対象外としている管理策である。

ISMAPは、クラウド事業者に対し、調達府省庁等の求めに応じて言明書の詳細を提出することを求めており、詳細について必要な場合はクラウド事業者に対して問い合わせを行うこと。

ゼロトラストアーキテクチャへの取組

2．ゼロトラストアーキテクチャについて

ネットワーク上には、外部/内部を問わず脅威が存在するといった前提に立ち、ユーザー、デバイスなど個々のID（Digital Identity）に焦点を当て、**「都度必要なアクションに対して必要なレベルの認証を行い、問題なければ適切なアクセス権を認可する」**といった検証を厳密に行うことで、セキュリティを担保し、且つ柔軟なUser Experienceを実現するといった概念

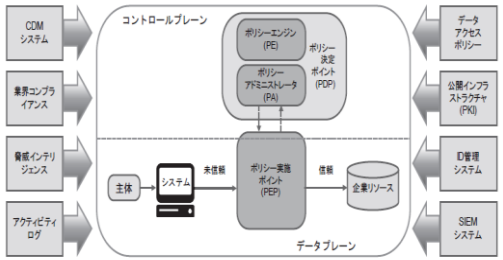


図 2:ゼロトラストの中核となる論理コンポーネント

出所;
米国National Institute of Standards and Technology
Zero Trust Architecture （nist.gov）

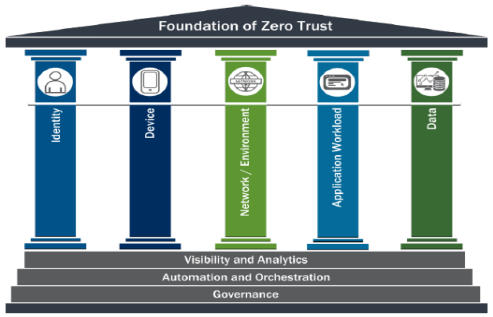
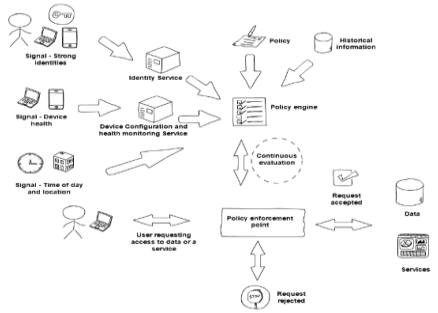


Figure 1: Foundation of Zero Trust[7]

出所；
米国CyberSecurity & Infrastructure Security Agency
CISA Zero Trust Maturity Model



出所;
英国National Cyber Security Centre
Zero trust architecture design principles - NCSC.GOV.UK

- ゼロトラストアーキテクチャはセキュリティの概念モデルであり、ソリューションではない
- 上記概念モデルを実現するためには様々なコンポーネントを構成する必要がある
- これまでのネットワークセグメンテーションを単一の信頼源とせず、デジタルアイデンティティを基にした信頼付与へのシフト

米国CDMについて

米国CDMプログラムの概要

●CDM（Continuous Diagnostics and Mitigation）

- **Diagnostics**
  理想状態と現状状態のギャップやリスクを可視化
- **Mitigation**
  可視化されたギャップやリスクへ対応
- **Continuous**
  ギャップやリスクを可視化し、対応を継続的に実施

●米国におけるCDMプログラムの位置づけ

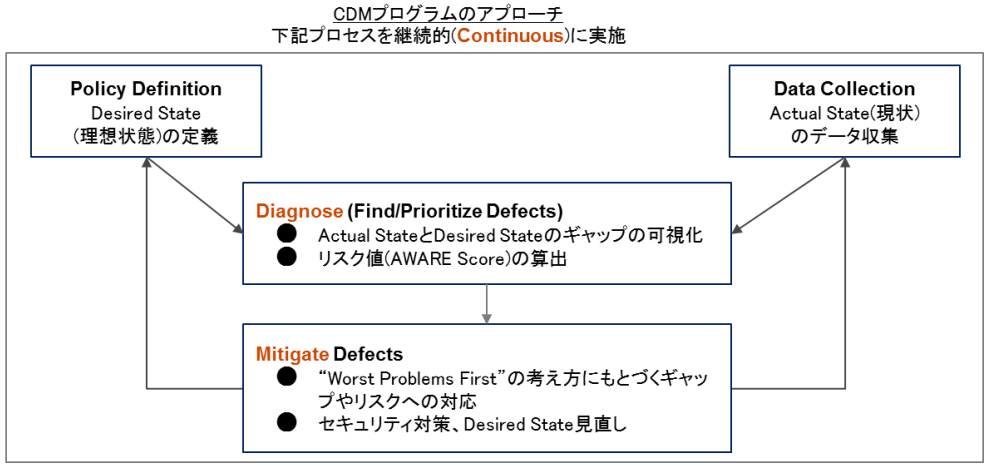
- 連邦政府機関の情報システムに関する管理状況をほぼリアルタイムに報告する仕組み
- 従来から各機関は、FISMA（連邦情報セキュリティ管理法）に基づき定期的に報告書を提出している
- DHS（Department of Homeland Security）及びOMB（Office of Management and Budget）がプログラムを推進。なお、小規模組織向けのCDMのシェアサービスは、GSA（General Services Administration）で提供
- ゼロトラストの導入を促進するプロジェクトと位置付けられており、2022年1月26日にOMBから発出された覚書においても、各機関に対してCDMプログラムに参加するための計画を立てることが指示されている

●CDMの管理対象

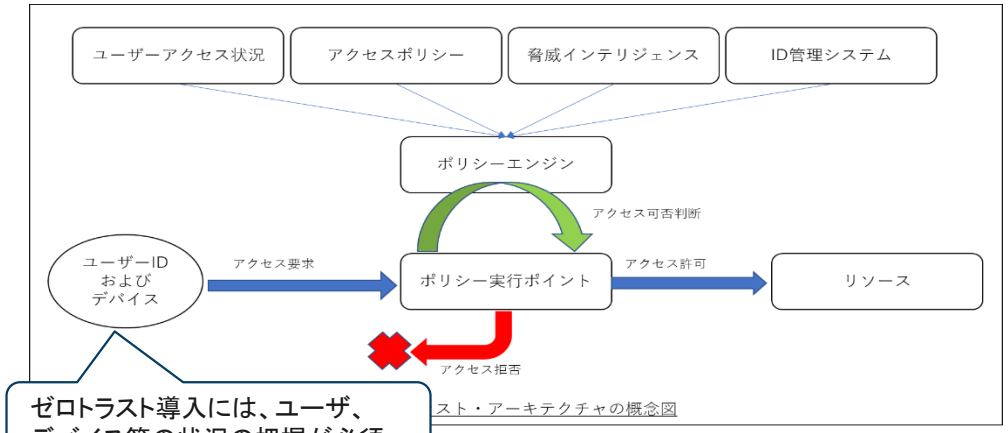
- IT資産（デバイス、ソフトウェア等）、ユーザ、ネットワークセキュリティ、データ保護を管理対象としている

※2020年時点では、主に資産管理、ユーザ管理が行われている。ネットワークセキュリティ、データ保護管理は順次構築中

CDMの基本概念



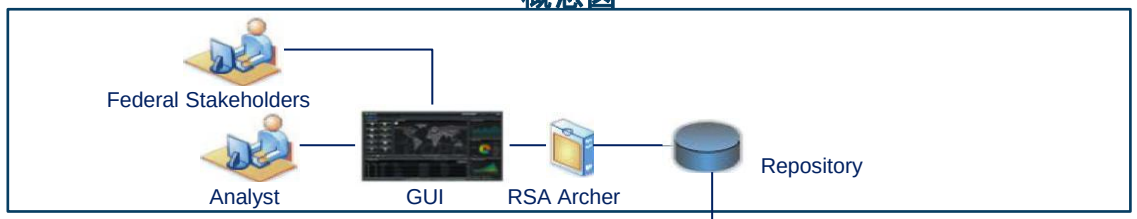
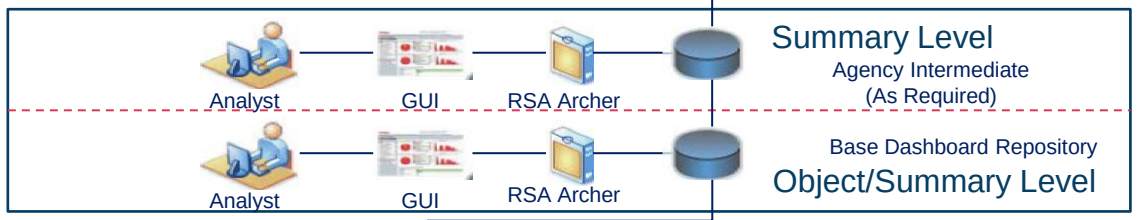
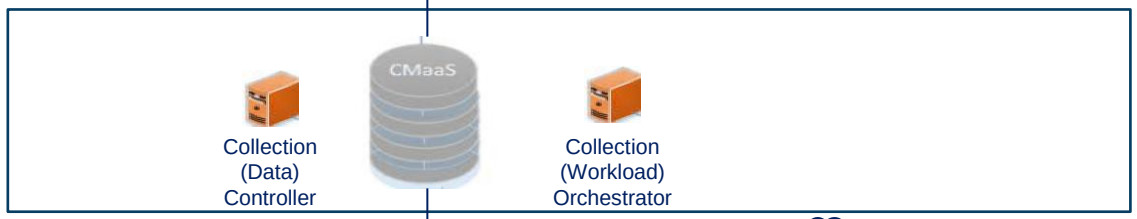
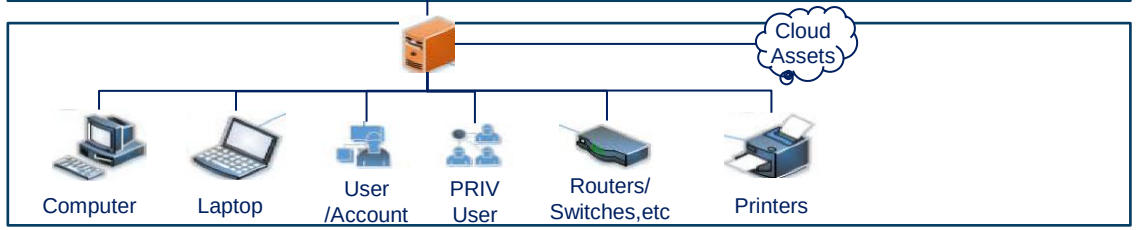
（参考）ゼロトラスト・アーキテクチャーの概念図



米国CDMについて

米国CDMの全体アーキテクチャ

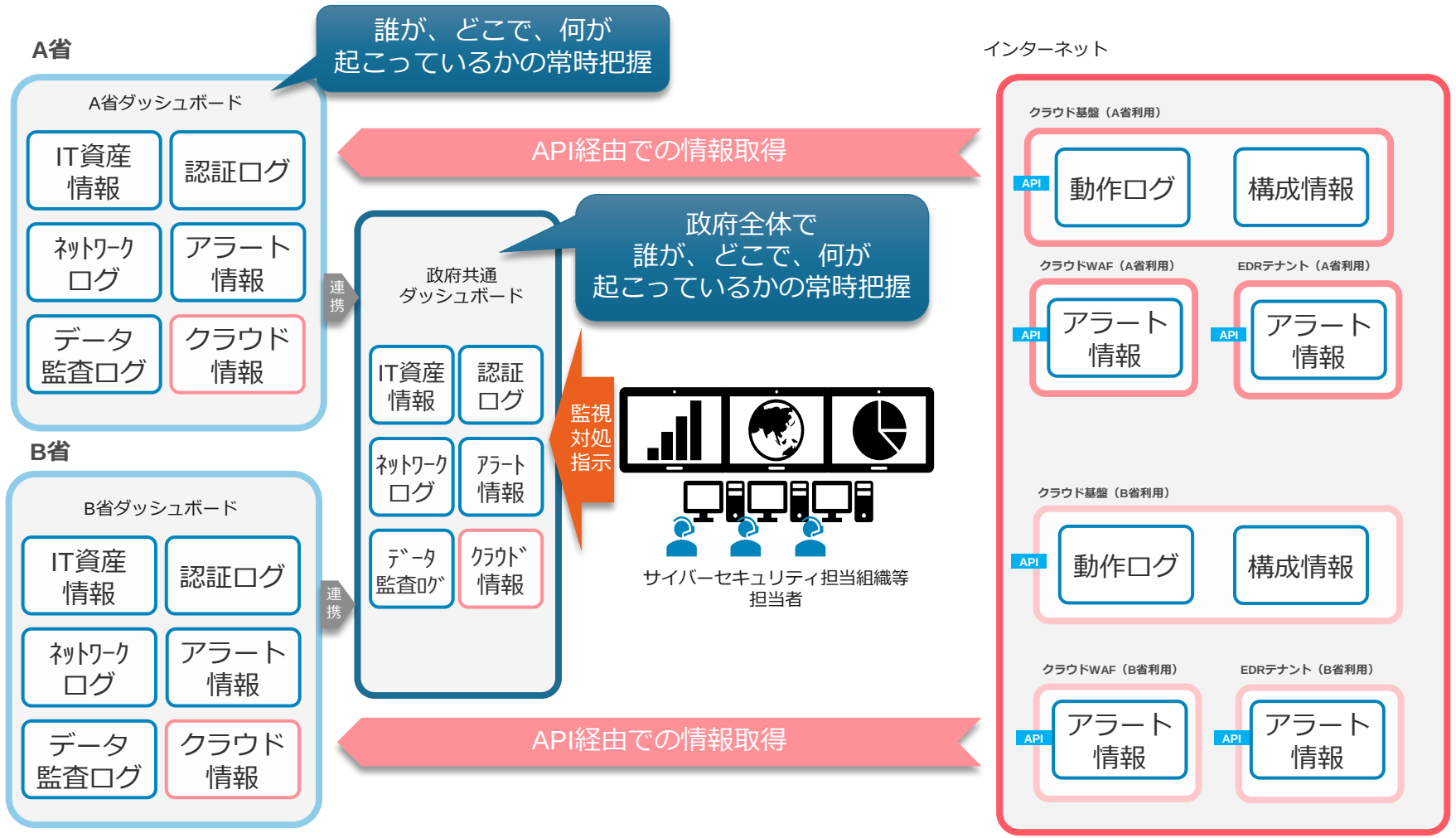
米国CDMのアーキテクチャは、下図のLayer A-Dの4つのレイヤーから構成される。

レイヤー	概念図	説明
Layer D Federal Dashboard		Agencyダッシュボードからサマリ情報を取得し表示する。 新たな脅威を特定した場合など、必要な場合はAgencyダッシュボードにリスクスコア算出のためのパラメータを送信する。
Layer C Agency Dashboard		レイヤーBを介して、各Agencyのオブジェクトレベルのデータを取得し表示する。”Desired State”と”Actual State”の比較を表示し、リスクの特定と改善アクションの優先順位付けを行う。各AgencyにおけるFederal ダッシュボードとの唯一の接点となる。
Layer B CMaaS Integration		レイヤーAから収集したデータの集約、統合、正規化を行い、CMaaSソリューションの自動化・運用上の制御ポイントとなる。拡張や地政学的なニーズに応じた水平・垂直統合への対応が 必要となる。また、レイヤーBの各インスタンスはレイヤーCに 採用されているトポロジーに合わせる必要がある。
Layer A Tools & Sensors		最下位で最も多様なレイヤーであり、各Agencyのハードウェアおよびソフトウェアと相互作用するツールとセンサーによりデータ収集を行う。レイヤーAは多岐にわたるツールで構成され 高度に分散されており、基本的に一元化されることはない。

※CMaaS : Continuous Monitoring as a Service

日本版CDM（CRSAアーキテクチャ）の導入について

常時診断を実現する日本ToBeモデル概要（現状案）

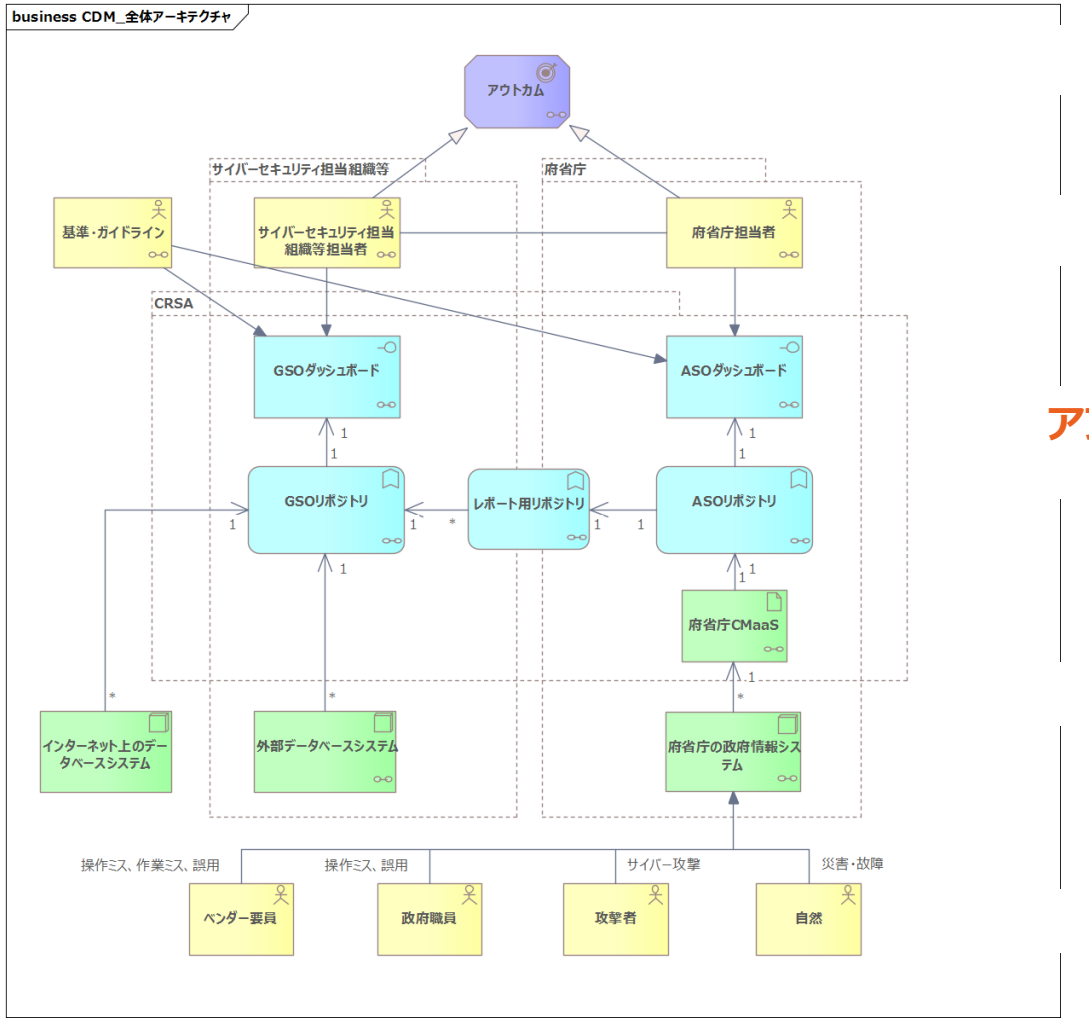


Continuous Risk Scoring and Action（CRSA）アーキテクチャ

政府全体で各種データを収集することにより
継続的にリスクを可視化し、その変化に対処する

日本版CDM（CRSAアーキテクチャ）の導入について

CRSAアーキテクチャ全体概要図



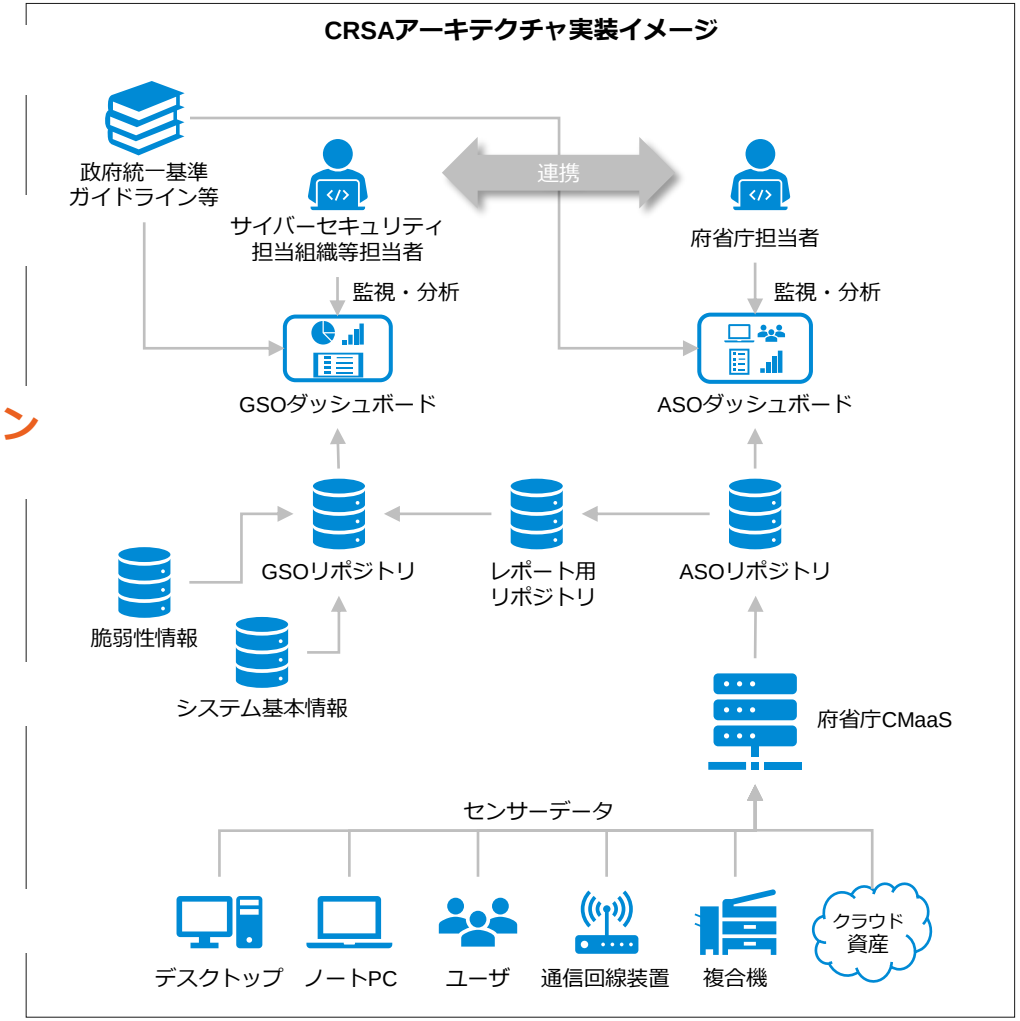
ガバナンスレイヤ

業務レイヤ

アプリケーションレイヤ

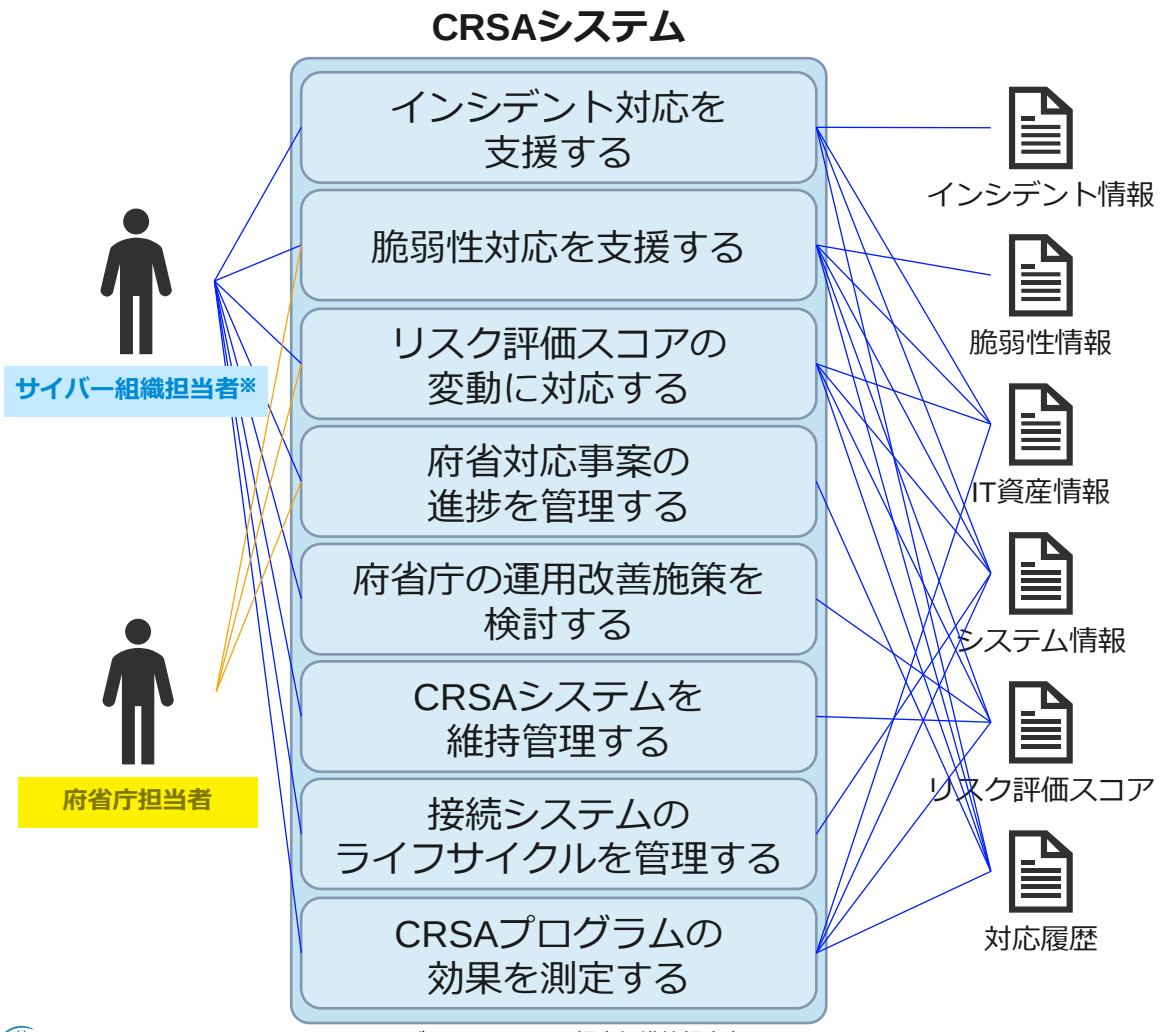
技術レイヤ

関係要素



日本版CDM（CRSAアーキテクチャ）の導入について

CRSAシステムのユースケース（案）



※サイバーセキュリティ担当組織等担当者

- **インシデント対応支援** サイバー組織担当者
  府省庁におけるインシデント発生状況を随時把握し、インシデントに係るソフトウェアやデバイスの情報をサイバーセキュリティ担当組織等に提供することにより、政府横断的なインシデント対応の支援を行う
- **脆弱性対応支援** サイバー組織担当者 府省庁担当者
  脆弱性情報の政府マスター情報（脆弱性辞書）を維持管理するとともに、新たな脆弱性情報や政府組織における脆弱性対応状況を随時把握し、府省庁担当者への情報提供等により脆弱性対応を支援する
- **リスク評価スコア変動対応** サイバー組織担当者 府省庁担当者
  リスク評価スコア変動の原因を分析し、必要に応じて各組織への状況確認や対応支援を行う
- **進捗管理** サイバー組織担当者 府省庁担当者
  サイバーセキュリティ担当組織等担当者の業務に係る府省庁担当者とのやり取りについて、進捗管理を行う
- **運用改善施策の検討**
  リスクスコア変動や対応状況の傾向から、府省庁におけるセキュリティ運用の状況、改善施策の効果等を分析・評価し、政府横断的な対応施策を検討する

- **CRSAシステムの維持管理**
- **接続システムのライフサイクル管理**
- **CRSAプログラムの効果測定**

サイバー組織担当者

日本版CDM（CRSAアーキテクチャ）の導入について

CRSAダッシュボードのトップ画面イメージ

GSOダッシュボードトップ画面の表示項目（概要）

- **脆弱性に関する情報**
  - 脆弱性件数（緊急・新規・更新）
  - 長期間未対応の脆弱性件数
- **リスク評価スコア変動に関する情報**
  - スコア変動のあった件数
  - 政府全体のリスク評価スコアの最新値
  - 政府全体のリスク評価スコアの推移
- **進捗管理（チケット）に関する情報**
  - 新規・更新チケット件数
  - チケット一覧
- **政府内の資産管理情報**
  - 政府全体の情報システム数、デバイス数
  - デバイスのOSバージョン分布
- **インシデントに関する情報**
  - 新規に発生したインシデント件数
  - 対応状況が更新されたインシデント件数
  - 政府内で発生したインシデント一覧

※表示されている情報は実際のものではありません。

まとめ

- デジタル庁のセキュリティ危機管理チーム
- サイバーセキュリティ戦略
- デジタル社会の実現に向けた重点計画
- 情報システムの整備及び管理の基本的な方針
- 政府情報システムのためのセキュリティ評価制度（ISMAP）
- ゼロトラストアーキテクチャへの取組

デジタル庁