政府における自動化されたセキュリティマネジメントとモダナイゼーションの取り組み

2023年11月

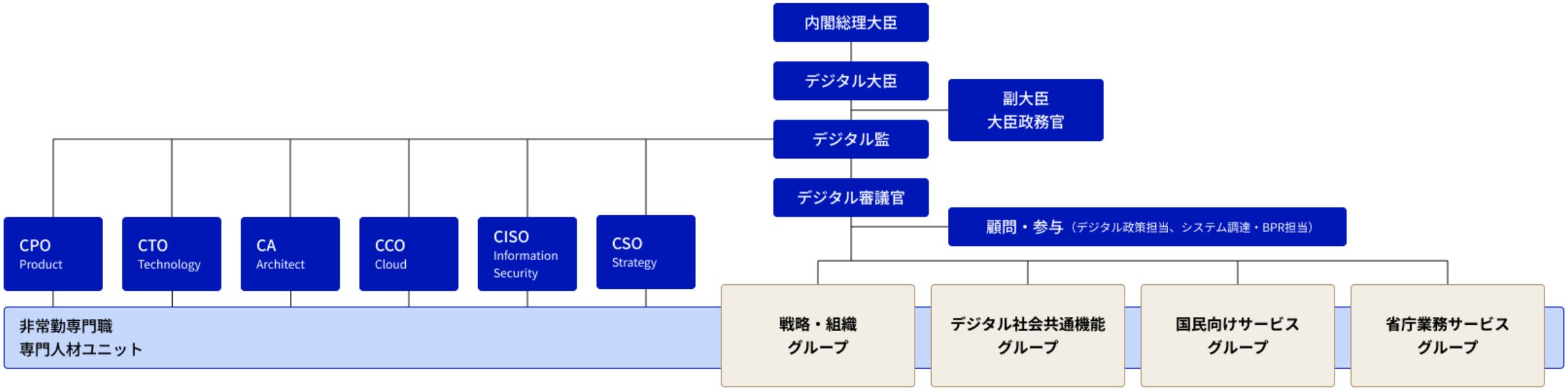
デジタル庁
Digital Agency

満塩　尚史（みつしお　ひさふみ）

戦略・組織グループ　セキュリティ危機管理チーム
セキュリティアーキテクト
公認情報システム監査人（CISA）、理学博士(物理学)

略歴
KPMGコンサルティングで、システム監査、情報セキュリティマネジメント・電子署名法対応・電子認証局等のコンサルティングを経験。
環境省CIO補佐官、経済産業省CIO補佐官、IT総合戦略室政府CIO補佐官、経済産業省最高情報セキュリティアドバイザー等を歴任。
CRYPTOREC暗号技術活用委員会、クラウドサービスの安全性評価に関する検討会、デジタルガバメント技術検討会議等のメンバー。

デジタル庁の組織体制


内閣総理大臣
デジタル大臣
副大臣
大臣政務官
デジタル監
デジタル審議官
顧問・参与（デジタル政策担当、システム調達・BPR担当）
CPO
Product
CTO
Technology
CA
Architect
CCO
Cloud
CISO
Information
Security
CSO
Strategy
非常勤専門職
専門人材ユニット
戦略・組織
グループ
デジタル社会共通機能
グループ
国民向けサービス
グループ
省庁業務サービス
グループ

デジタル庁について

組織

- デジタル社会共通機能
- 国民向けサービス
- 省庁業務サービス

主なプロジェクト

- 地方公共団体情報システム標準化
- 情報連携基盤
  公共サービスメッシュ、ベースレジストリ
- ＩＤ制度等
  番号利用法、公的個人認証法、公金口座
- 行政手続きにおけるマイナンバーカード利活用の促進
- 準公共・民間分野の手続きにおけるマイナンバーカードの活用
- マイナンバーカード普及・スマホ搭載
- 事業者の手続きシステム基盤
- 準公共（健康・医療・教育・防災、モビリティなど）
- ガバメントソリューションサービス
- ガバメントクラウド
- 政府（共通）情報システムの支援
- 運用監視・職員ＩＤ基盤
- 庁内情報システム

デジタル庁担当のシステム

大小50程度のシステムを
企画・運営

◆内訳①（成り立ち）
- 他省庁から移管されたもの
- デジタル庁で構築したもの
- クラウドサービスを利用

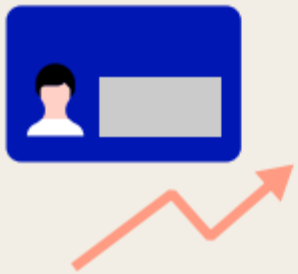
◆内訳②（種別）
- 行政サービス
- インフラ、プラットフォーム
- 内部管理、コミュニケーション

◆内訳③（開発・運用）
- 調達（外部委託）している
- 内製開発している

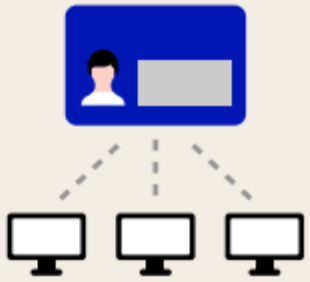
デジタル庁について

重点的な取り組み

1. マイナンバーカードとデジタル行政サービスで便利な暮らしを提供する
2. デジタル技術を活用するためのルールを整える
3. 国や地方公共団体を通じてデジタル変革を推進する
4. 官民でデータ連携の基盤を整備する
5. 準公共分野のデジタルサービスを拡充する
6. AI活用及びデータ戦略を踏まえた取組を推進する
7. データ連携とデータ移転の国際的な枠組みをつくる
8. 事業者向け行政サービスの利便性を高める
9. 公平かつ迅速な調達を実現できる仕組みをつくる
10. インターネット上の偽情報対策などを推進する



マイナンバーカードの普及と利用推進



マイナンバー制度の利用の推進

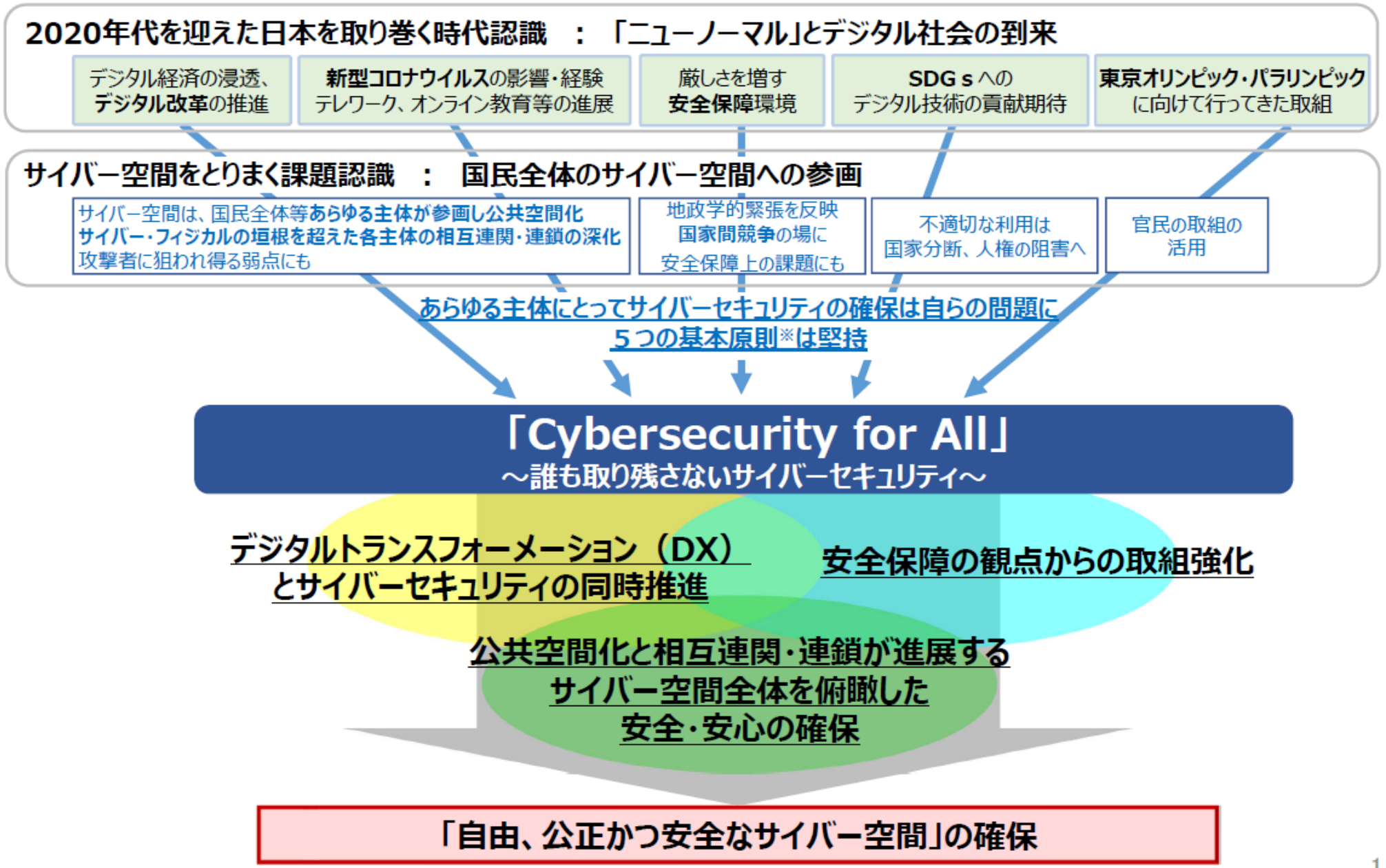
システム基盤の統一・整理

行政手続のオンライン･デジタル化

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

サイバーセキュリティ戦略

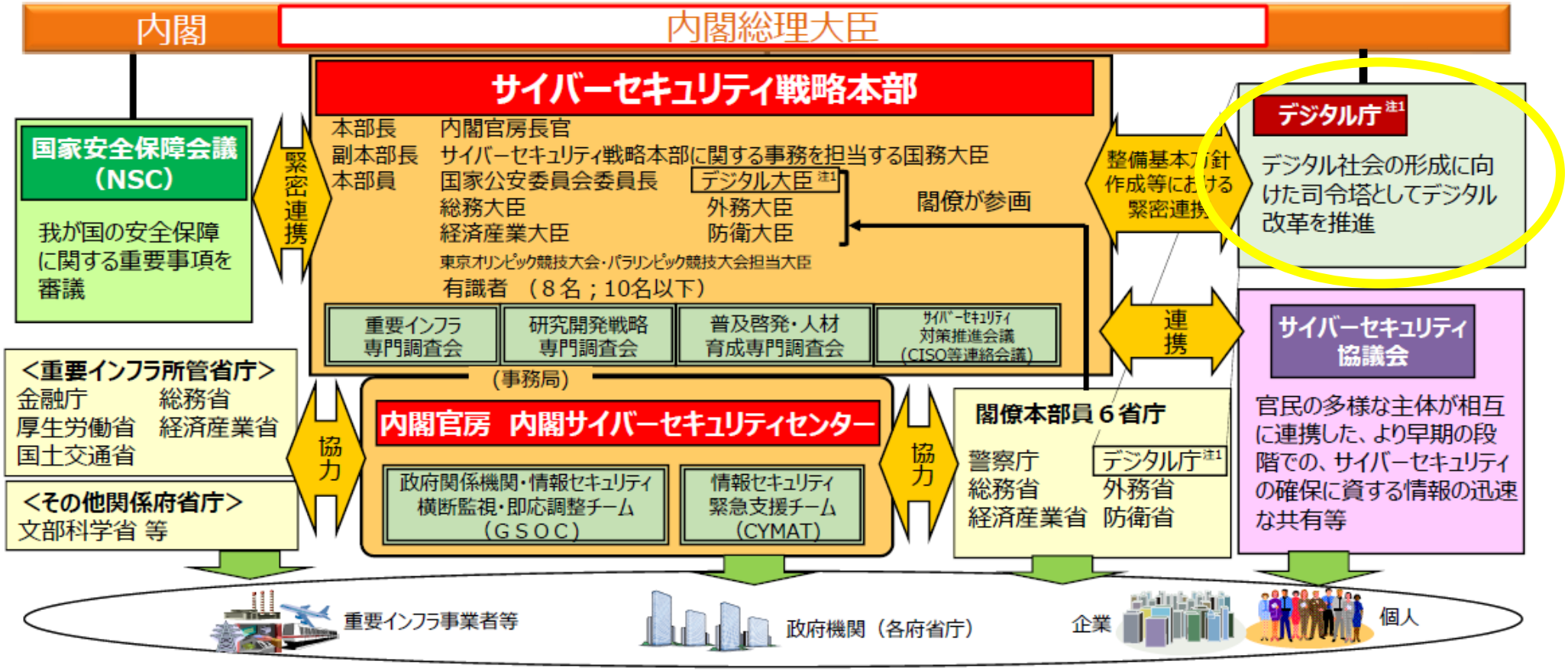
サイバーセキュリティ戦略の課題と方向性



※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）

8

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。

9

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。

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

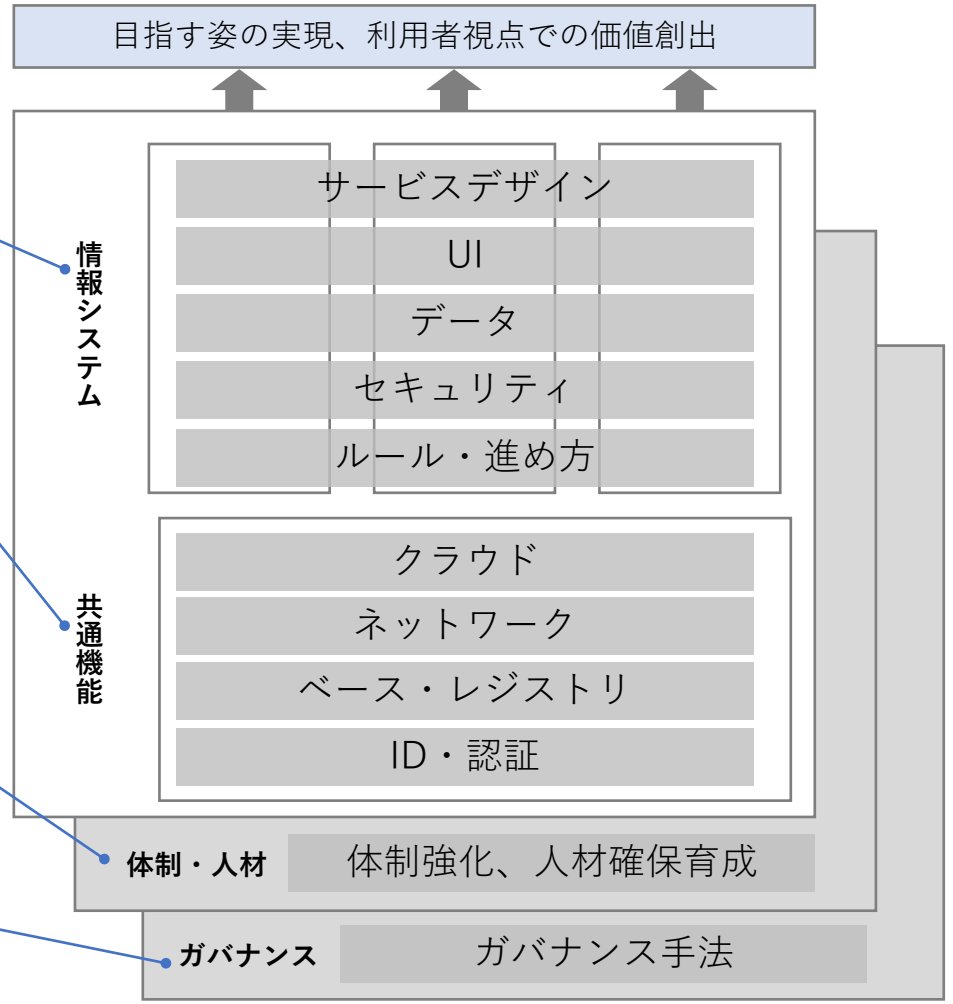
関係者が個々に努力するだけでは、目指す姿を実現できない。デジタル庁自身が特に４つの領域に注力し、旧来の課題を解消するとともに、**国・地方公共団体・独立行政法人・準公共分野等の関係者が効果的に協働**できるようにする。

1 良いサービスを作るための **標準** の策定・推進

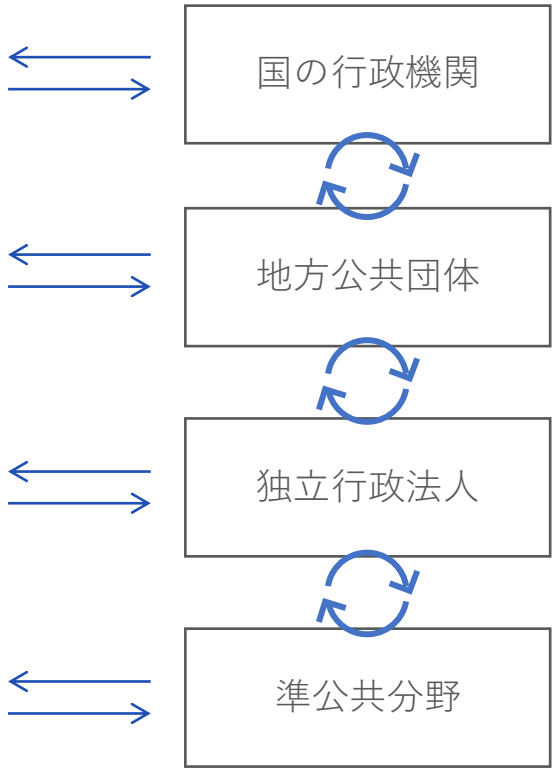
2 良いサービスを支える **共通機能** の整備・展開

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



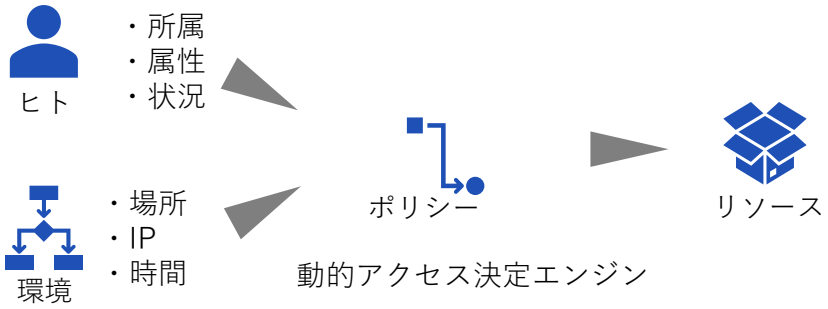
デジタル庁は、各関係者にとって利便性の高い標準、共通機能等となるように、利用状況を踏まえて**継続的に改善**を行う



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

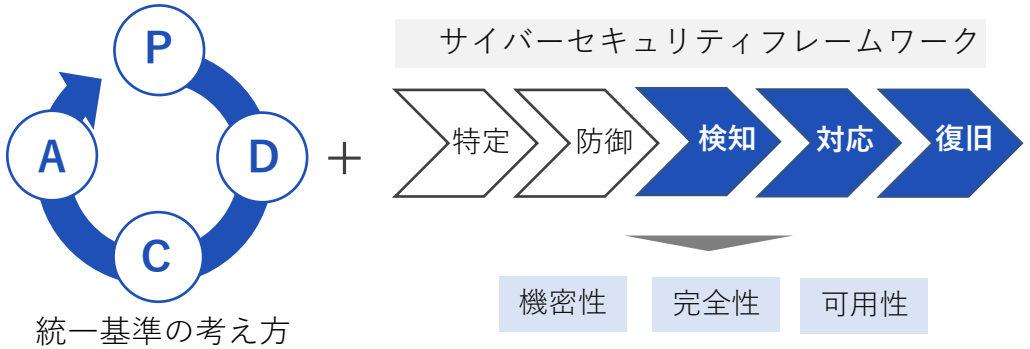
共通機能を前提とした常時診断・対応型のセキュリティアーキテクチャ実装推進

- 「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。



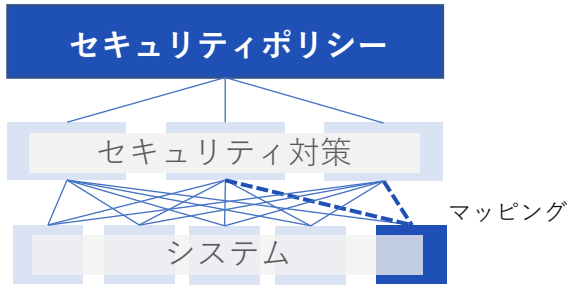
サイバーレジリエンスの強化

- 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**を導入し、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。



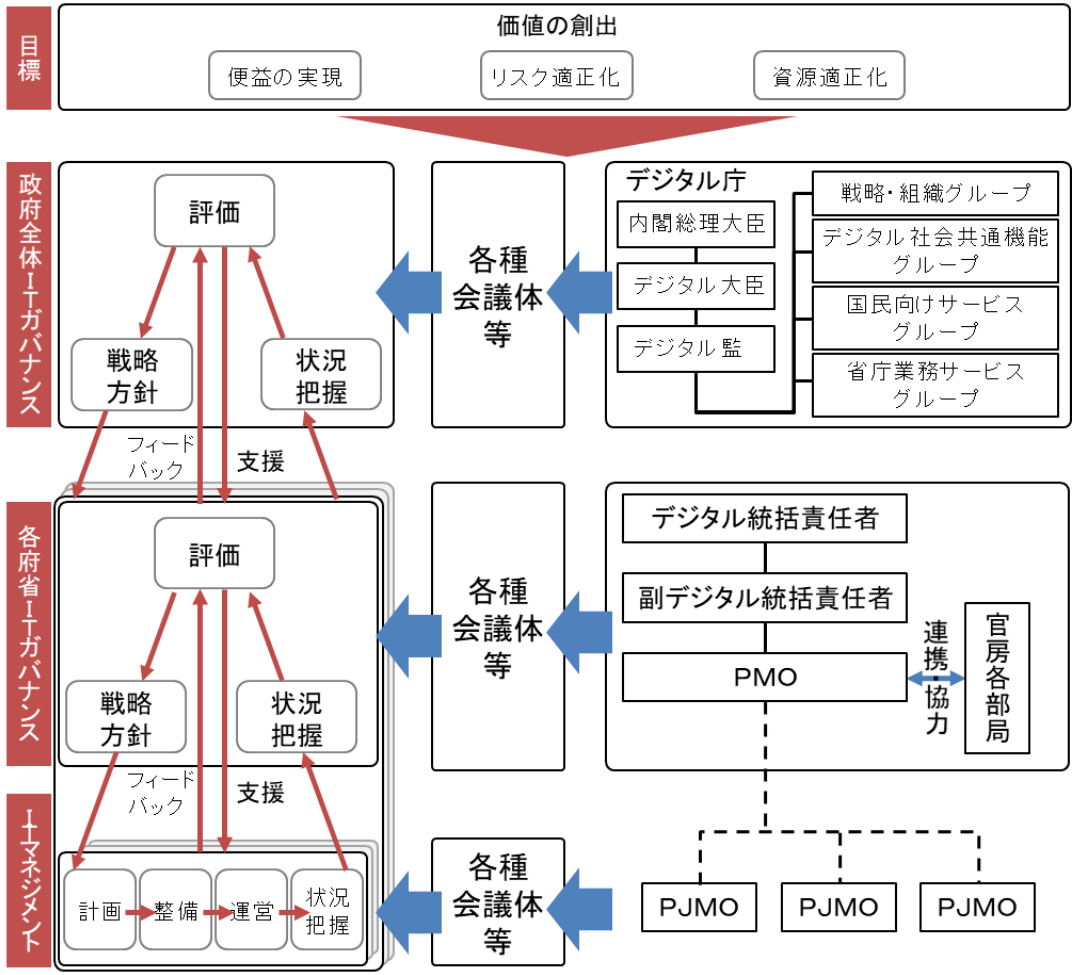
サイバーセキュリティについての基本的な方針の整備とガイドライン等の作成

デジタル社会推進標準ガイドライン

- **政府情報システム全般に関するドキュメント**
  - DS-100 デジタル・ガバメント推進標準ガイドライン
  - DS-110 デジタル・ガバメント推進標準ガイドライン解説書
  - DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック
  - DS-121 アジャイル開発実践ガイドブック
  - DS-130 標準ガイドライン群用語集
- **セキュリティに関するドキュメント**
  - DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
  - DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～
  - DS-210 ゼロトラストアーキテクチャ適用方針
  - DS-211 常時リスク診断・対処（CRSA）アーキテクチャ
  - DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート
  - DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート
  - DS-221 政府情報システムにおける脆弱性診断導入ガイドライン
  - DS-231 セキュリティ統制のカタログ化に関する技術レポート
- **クラウドに関するドキュメント**
  - DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針
- **データ連携に関するドキュメント**
  - DS-400 政府相互運用性フレームワーク（GIF）
- **トラストに関するドキュメント**
  - DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン
  - DS-531 処分通知等のデジタル化に係る基本的な考え方
- **その他ドキュメント**
  - DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い

https://www.digital.go.jp/resources/standard_guidelines/

（参考）標準ガイドラインにおけるITガバナンス



デジタル庁の役割

(1) 社会のニーズを捉え、概念検証（ＰｏＣ）等を用いて機動的に新たな政府情報システムの企画及び立案を行い、体制を確立すること。
(2) 政府情報システムについて、整備・管理の基本的な方針の策定及び改定に関すること。
(3) 標準ガイドライン群の策定及び改定に関すること。
(4) 各府省の中長期計画の策定又は改定並びにフォローアップの総合調整及び取りまとめに関すること。
(5) デジタル庁システム及びデジタル庁・各府省共同プロジェクト型システムの指定に関すること。
(6) デジタル庁システムの整備及び運用、デジタル庁・各府省共同プロジェクト型システムの整備に関すること。
(7) デジタル人材の確保・育成方針の策定、デジタル庁民間人材の一元的な採用・管理及び業務環境整備に関すること。
(8) 情報システム統一研修に関すること。
(9) 予算の要求に関すること。
(10) 予算の執行に関すること。
(11) 工程レビュー実施状況の把握に関すること。
(12) デジタル庁によるレビューに関すること。
(13) プロジェクト検証委員会の設置に関すること。

セキュリティに関する
デジタル社会推進標準ガイドライン

セキュリティ関連技術ガイドライン群の作成と各ドキュメントにおける概要①

統一基準群

政府情報システムのセキュリティ・バイ・デザインガイドライン

概要

情報システムに対し効率的にセキュリティを確保するため、**企画から運用まで一貫したセキュリティ対策**を実施する「**セキュリティ・バイ・デザイン**」の必要性が高まっている。本書では**システムライフサイクルにおけるセキュリティ対策**を俯瞰的に捉えるため、**各工程での実施内容**を記載すると共に**関係者の役割**についても定義する。

政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～

概要

情報システムのセキュリティを確保するためには、**リスクを認識して確実に管理することが不可欠**である。本文書では、**ベースラインと事業被害を組み合わせたリスク分析の手順を紹介**し、作業効率と分析精度とをバランスをとって向上させることを目的としている。

本文書は、DS-200「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」における**セキュリティリスク分析の手順を具体的に示したもの**である。

政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート

概要

過激化、複雑化の一途をたどるサイバー攻撃に対して、攻撃の発生を速やかに検知し、対応することで被害を極小化し、正常状態に迅速に復旧するための**サイバーレジリエンスの必要性**が高まっており、包括的なサイバーセキュリティ態勢を構築するためのツールとしてNISTサイバーセキュリティフレームワークが各国で活用されている。本文書では**サイバーセキュリティフレームワークの概要と導入プロセス**について説明する。

政府情報システムにおける脆弱性診断ガイドライン

概要

政府機関では従来においても情報セキュリティリスクの低減を目的として**脆弱性診断を活用してきたが、導入方法に係る明確な基準や指針は十分整備されていない。**本書は、政府情報システムの関係者が**最適な脆弱性診断を選定、調達**できるようにするための基準及び指針を提供する。

セキュリティ関連技術ガイドライン群の作成と各ドキュメントにおける概要②

統一基準群

ゼロトラストアーキテクチャ適用方針

概要
政府機関では業務環境の変化に伴い、**イントラネットの外側で情報システムを利用するケースが増大**している。このような**従来の境界型のセキュリティモデルとは前提が異なる環境**で、情報セキュリティを確保するためには、境界型のセキュリティから大幅に拡張した考え方が求められる。本書は拡張の実態となる「ゼロトラストアーキテクチャ」の適用方針を説明する。

常時リスク診断・対処（CRSA）システムアーキテクチャ

概要
ゼロトラストの環境下において安定かつ安全なサービス提供を実現するためには、政府全体の**サイバーセキュリティリスクを早期に検知し、これを低減する**ことが必要となる。本書は、この活動を**継続的に実施するための、情報収集・分析**を目的としたプラットフォームのアーキテクチャについて説明する。

ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート

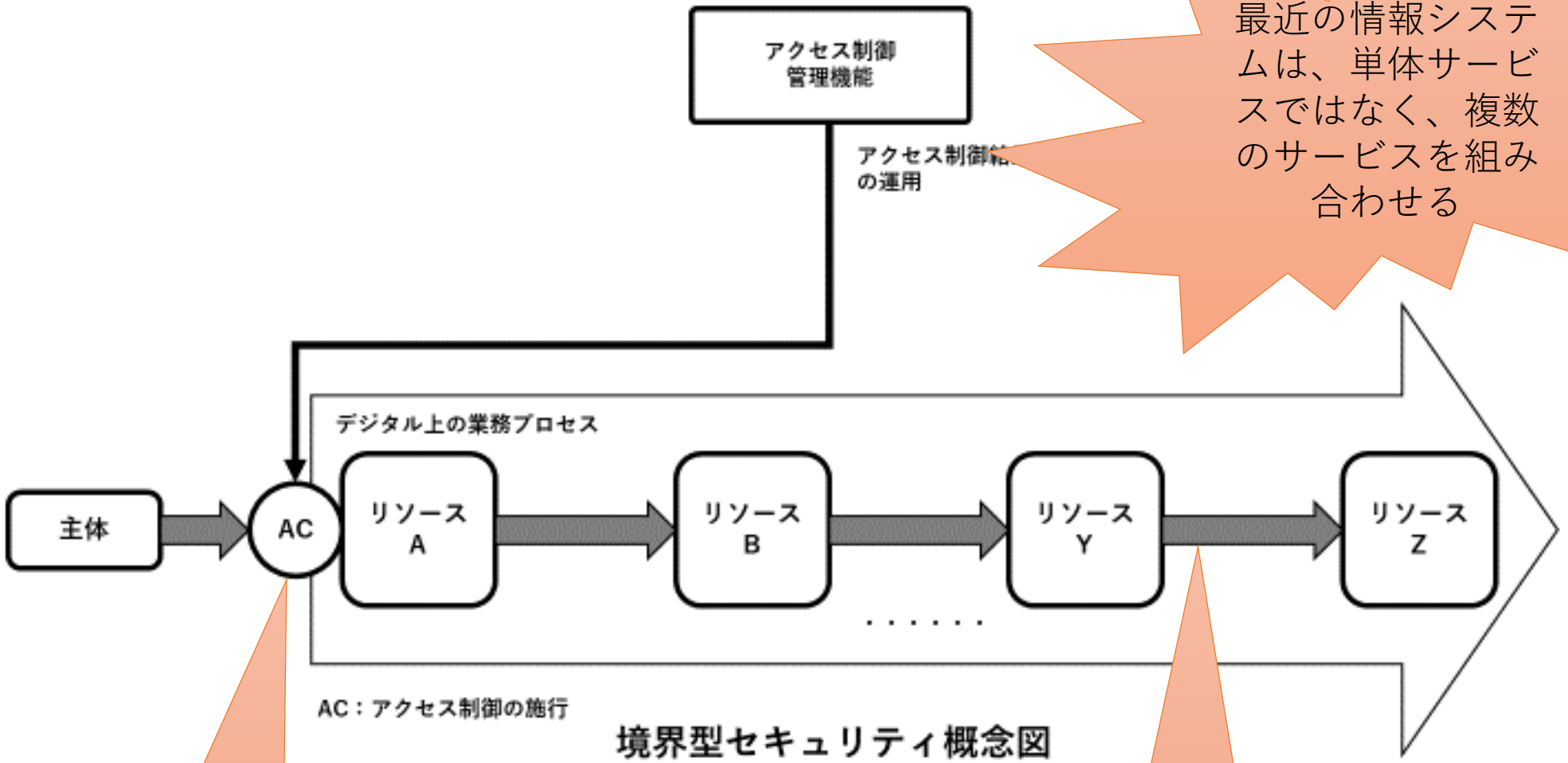
概要
変化する業務環境やリスクに対して、**アクセス制御は最小権限の原則を継続的に実現しなければならない**。不正アクセスから業務環境から保護するには、識別子（ID）や役割（ロール）といった単一の情報だけでは、アクセス制御においては十分な情報ではない。基本的な多層防御のためには、**複数で多面的な情報を組みあわせるABAC（属性ベースアクセス制御）が効果的**である。本文書ではABACの概要を説明する。

セキュリティ統制のカタログ化に関する技術レポート

概要
セキュリティ統制のカタログ化とは、セキュリティ統制に対し一意な識別子を付与し、機械可読形式で分類することを指す。これにより、統制要素間でのトレーサビリティを確保したり、システム設定自動化などを促進することができ、**システムセキュリティ評価の効率、適時性、正確性、および一貫性を向上**させることが可能となる。本文書では**セキュリティ統制のカタログ化に関する概要**について説明する。

ゼロトラストアーキテクチャ
ーデータによるセキュリティ管理ー

境界型セキュリティ概念図



最近の情報システムは、単体サービスではなく、複数のサービスを組み合わせる

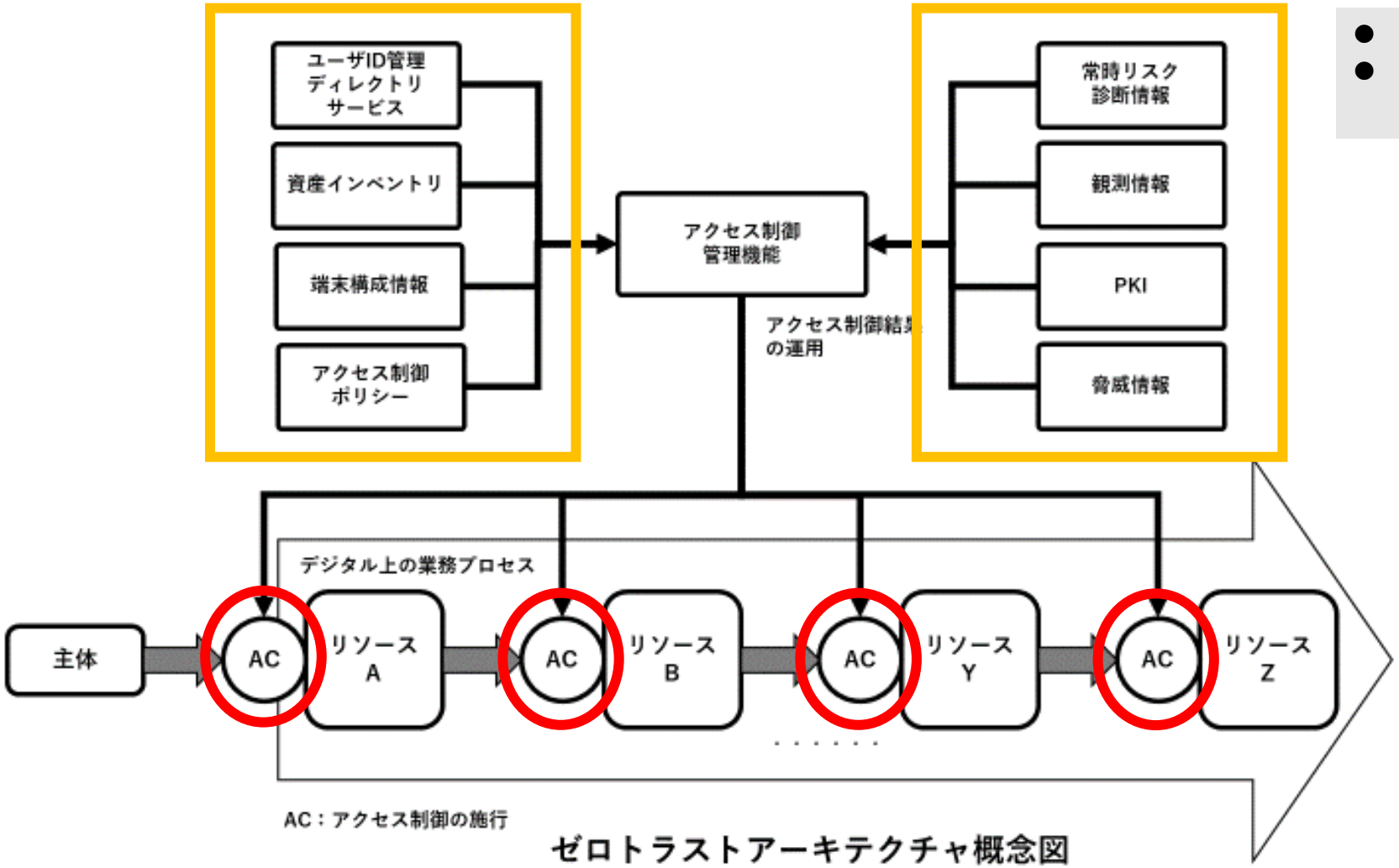
境界を越えるときにアクセス権限を確認

境界を超えた後は、特段の制限なし

ゼロトラストアーキテクチャ適用方針の概要

https://www.digital.go.jp/resources/standard_guidelines/#ds210

ゼロトラストアーキテクチャとは、
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



ゼロトラストアーキテクチャ概念図

- 従来のセキュリティモデルから考え方を拡張
- 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**

ゼロトラスト・アーキテクチャを適用する際の基本方針
①**リソースを識別し、特定**できる状態にする
②**主体の身元確認・当人認証**を実施する
③**ネットワークを保護**する
④リソースの**状態を確認**する
⑤**アクセス制御ポリシーで評価**し、アクセス管理をする
⑥リソースとアクセスを**観測**する

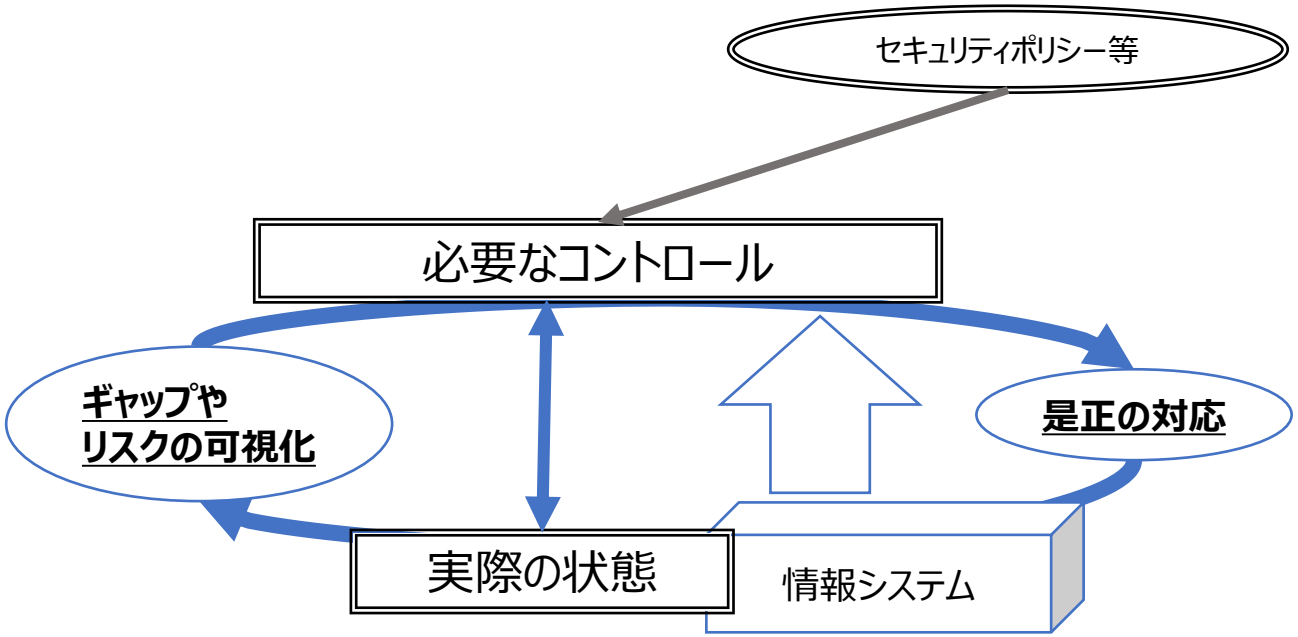
適用における留意事項

常時リスク診断・対処
CRSA：Continues Risk Scoring & Action

常時リスク診断・対処（CRSA：Continues Risk Scoring & Action）の概要

●常時リスク診断・対処

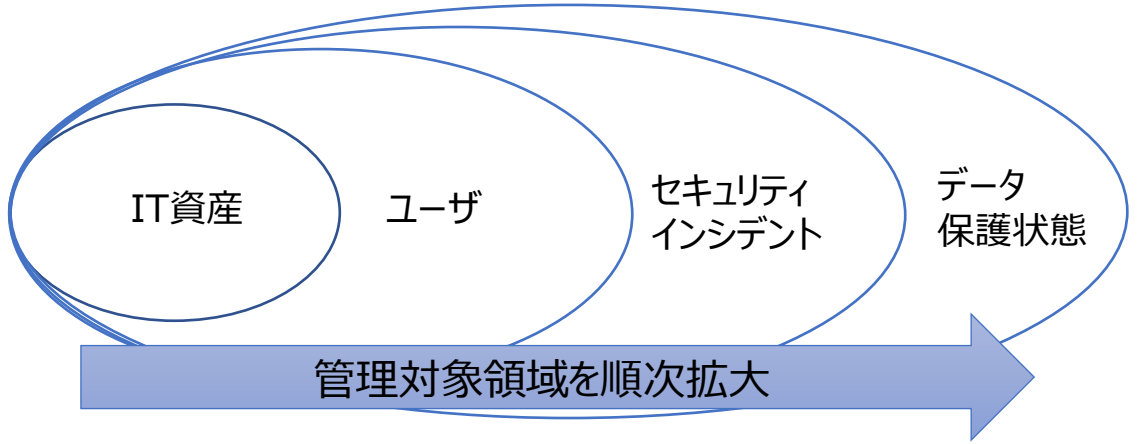
- **リスク診断**
  必要なコントロールと実際の状態の
  ギャップやリスクを可視化
- **対処**
  可視化されたギャップやリスクへ
  是正の対応
- **常時**
  ギャップやリスクを可視化し、
  是正の対応を継続的に実施



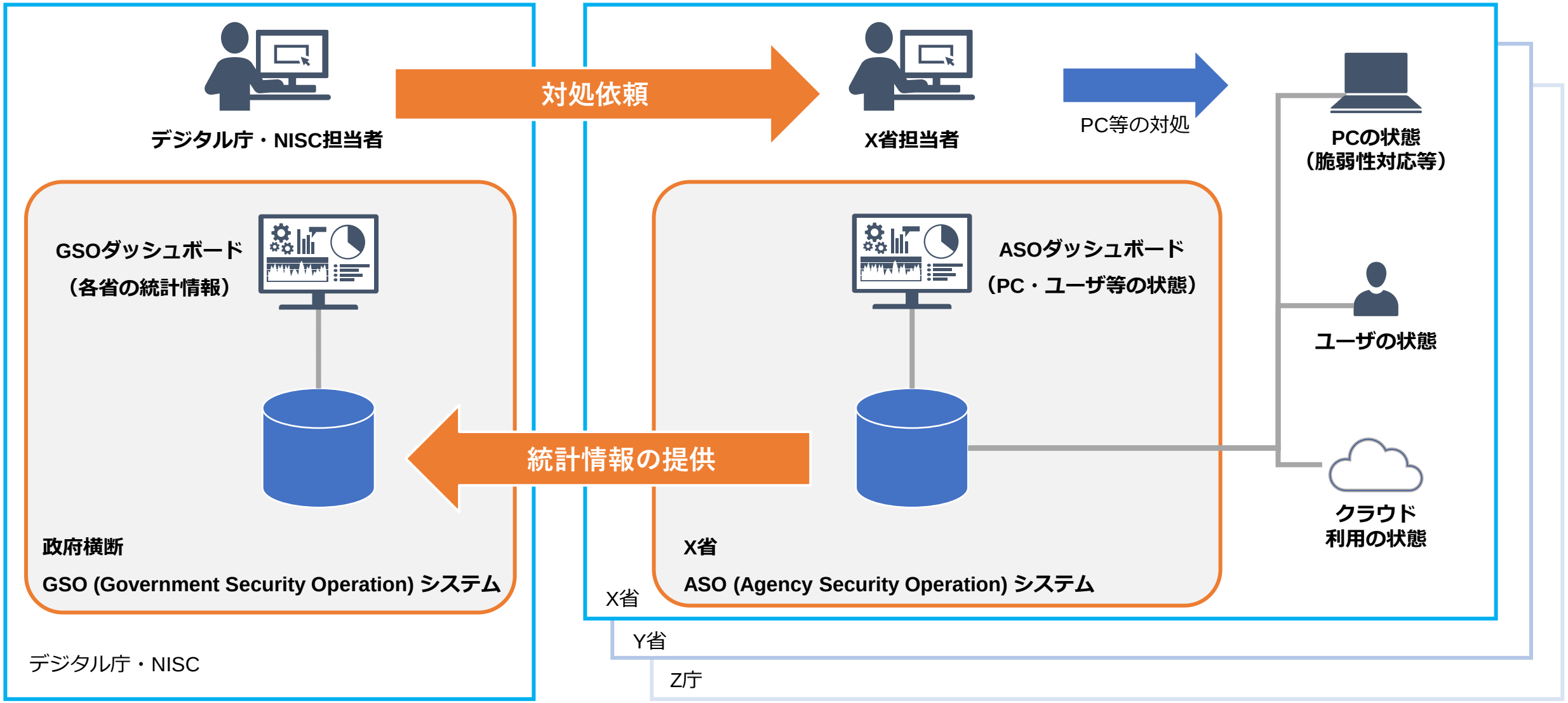
継続的に実施

●管理対象

- **IT資産（デバイス、ソフトウェア、サービス等）、ユーザ、セキュリティインシデント、データ保護状態**を管理対象と想定。
- 実装される管理対象は、順次追加している。



常時リスク診断・対処（CRSA）のシステム構成概要



常時リスク診断・対処（CRSA）の目的と効果

① 政府機関統一基準等に準拠したコントロール（管理策）からの逸脱の迅速な把握と是正対応

CRSAシステムは、サイバーセキュリティ対策に必要なコントロールの実施状況を継続的にモニタリングすることができるため、どこが不適切な状態になっているかを迅速に把握し、是正対応を実施することができる。

② インシデント発生時のトリアージ等の効果的な対応

CRSAシステムは、リアルタイムに自組織の資産状況、脆弱性対応状況等を把握できるため、インシデント発生時の資産等への影響規模や対応の優先度について迅速に判断することができる。

③ リアルタイムデータによるセキュリティ対策実施状況の効率的な報告

CRSAシステムの導入によって、各組織としては、リアルタイムに自組織の資産の状態、アカウントの利用状況、インシデントの発生状況等を把握できるため、サイバーセキュリティ対策の状況を客観的および効率的に報告および説明することができる。政府全体としては、各組織のセキュリティ対策状況を各組織に負担をかけることなく効率的に把握することができる。

④ 脅威やインシデントに対する政府横断的な脆弱箇所の迅速な発見と是正対応

CRSAシステムは、特定の脅威情報やインシデントに関する情報をもとに、影響のある箇所やインシデントの発生する可能性のある箇所を政府横断的に特定できるため、迅速かつ効果的に対処することができる。

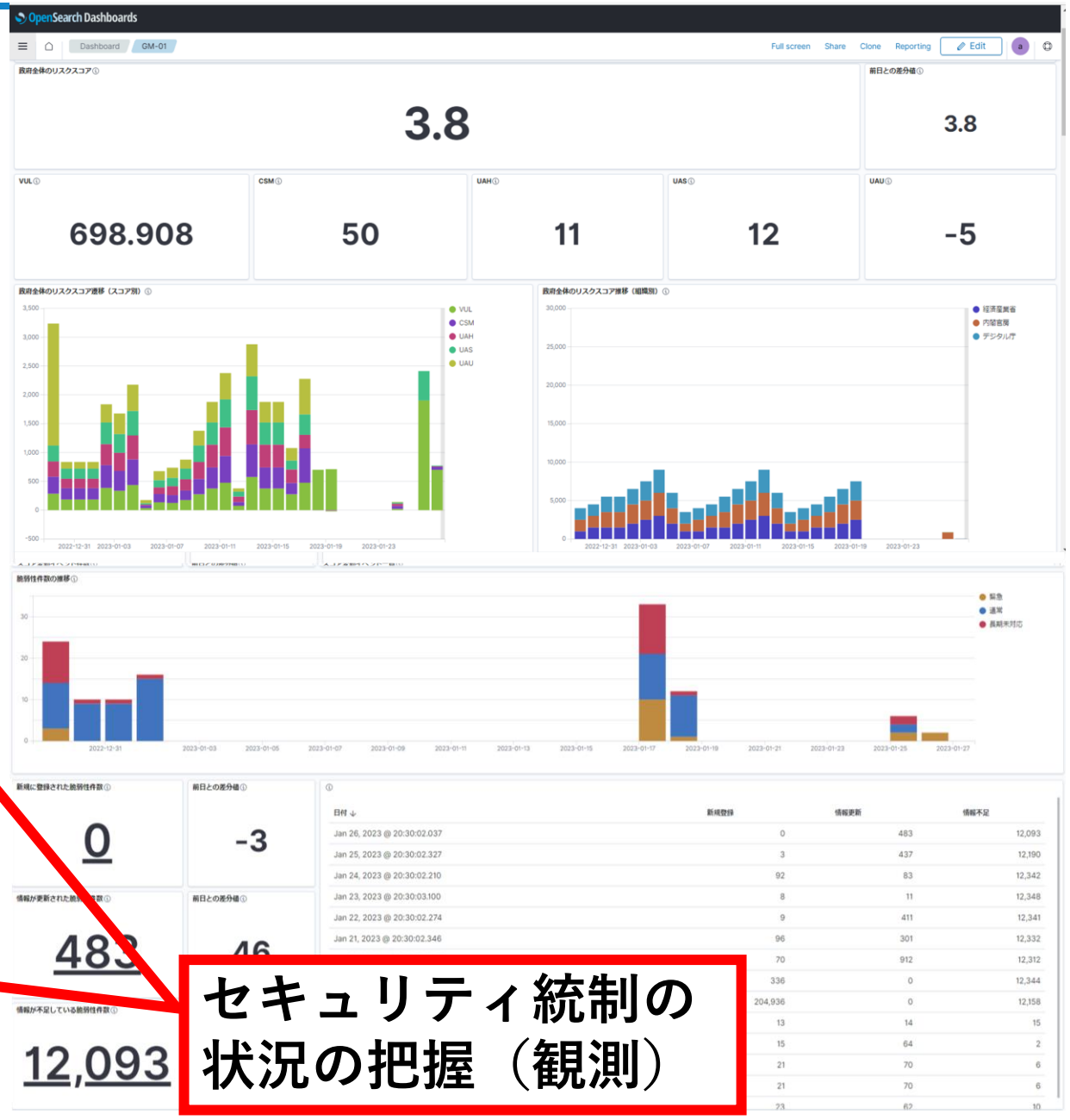
⑤ ゼロトラストアーキテクチャの運用環境を適切に維持

ゼロトラストアーキテクチャの具体的な実装・運用においては、ネットワーク上の各デバイスでの脆弱性対応状況等を把握することにより、システム全体の健全性を把握し、維持していく必要がある。CRSAシステムにおける診断結果は、ゼロトラストアーキテクチャにおけるポリシーエンジンのインプット情報としても活用していく。

リスクスコア候補とGSOダッシュボード（検討中）

- リスクスコアについても候補を整理し、適用の検討中。
- ダッシュボードについても検討中

CDM	対象領域 CRSA	基本スコア名称	評価項目	スコア概要
Area 1	端末とサーバ装置等の管理	VUL	ソフトウェア脆弱性の対応状況	デバイスにおける未対応の脆弱性をスコア化
		CSM	構成の規定準拠状況	ソフトウェアにおける構成誤りについてスコア化
		UAH	デバイスの管理状況	未承認（非管理）デバイスの存在をスコア化
		UAS	ソフトウェアの管理状況	未承認ソフトウェアの存在をスコア化
		USS	ソフトウェアの署名状況	未署名ソフトウェアの存在をスコア化
Area 2	認証・認可・特権の管理	UAU	ユーザの管理状況	未承認（非管理）ユーザの存在をスコア化
		PPS	パスワードの管理状況	パスワード強度が低いアカウントの存在をスコア化
Area 3	情報システムのライフサイクル管理	*LSS*	ログ管理の状況	不適切なログの保管状況をスコア化
		EVT	不正アクセス等の発生状況	セキュリティアラートの発生状況をスコア化
Area 4	データの保全管理	*NPF*	情報の保護状況	要保護情報が適切に保護されていない状況をスコア化
		ETS	データ暗号化の状況	暗号化されていないデータの存在をスコア化



セキュリティ統制の状況の把握（観測）

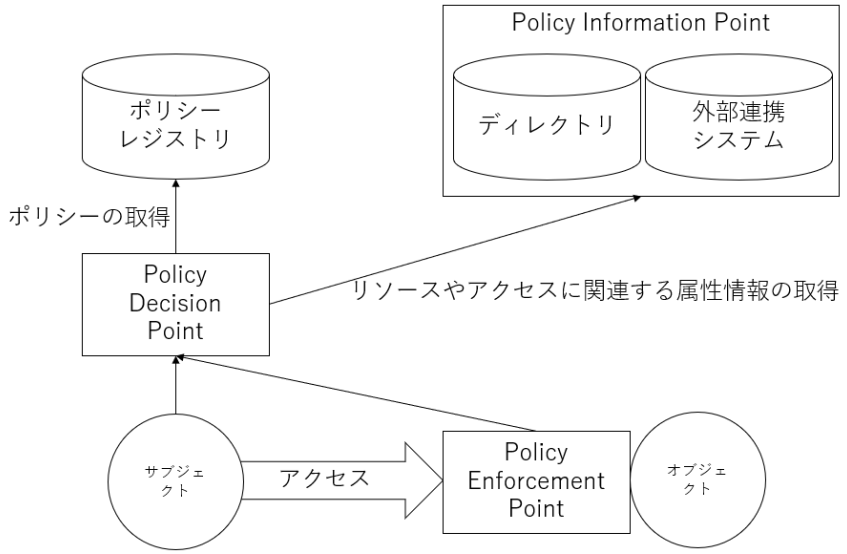
アクセス制御とAttribute Based Access Control（ABAC）の概要

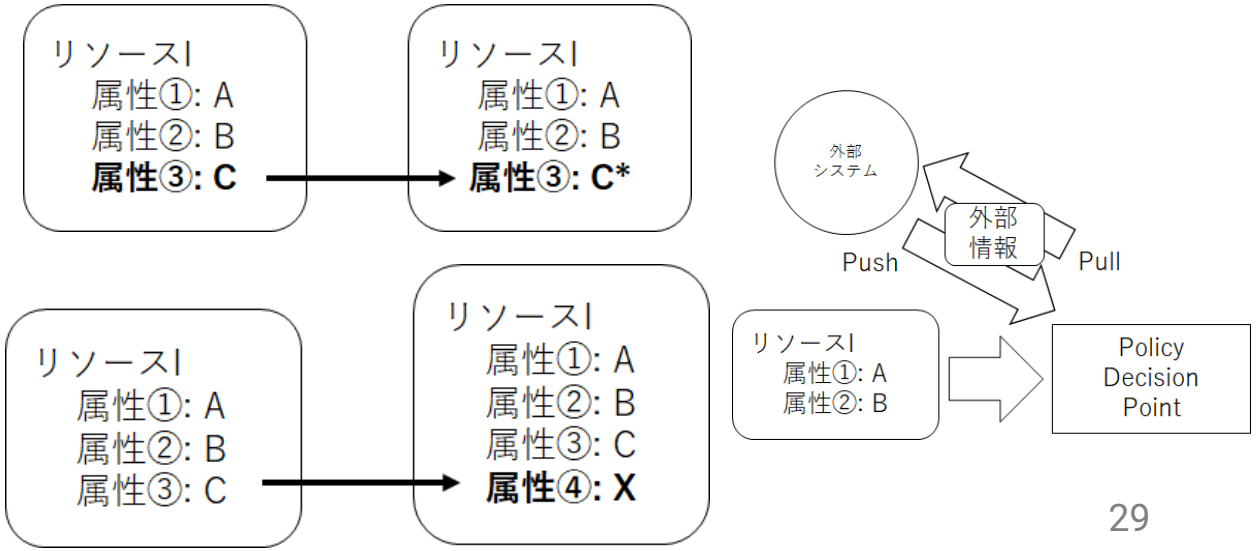
アクセス制御とAttribute Based Access Control（ABAC）の概要

アクセス制御に関するコンポーネントやアクセス制御モデルのバリエーションを ISO29146およびNIST SP800-162ベースで紹介し、ABACの特性を解説する。

ISO/IEC 29146:2016 A framework for access management
SP 800-162, ABAC Definition and Considerations

具体的にはABACの特徴である複数のデータを組み合わせたアクセス制御においては、**属性の加工・変換**や**外部情報**の活用により、インターネット空間など必ずしも信頼できない環境での処理に対し、柔軟なアクセス制御ルールを適用できるようになる。

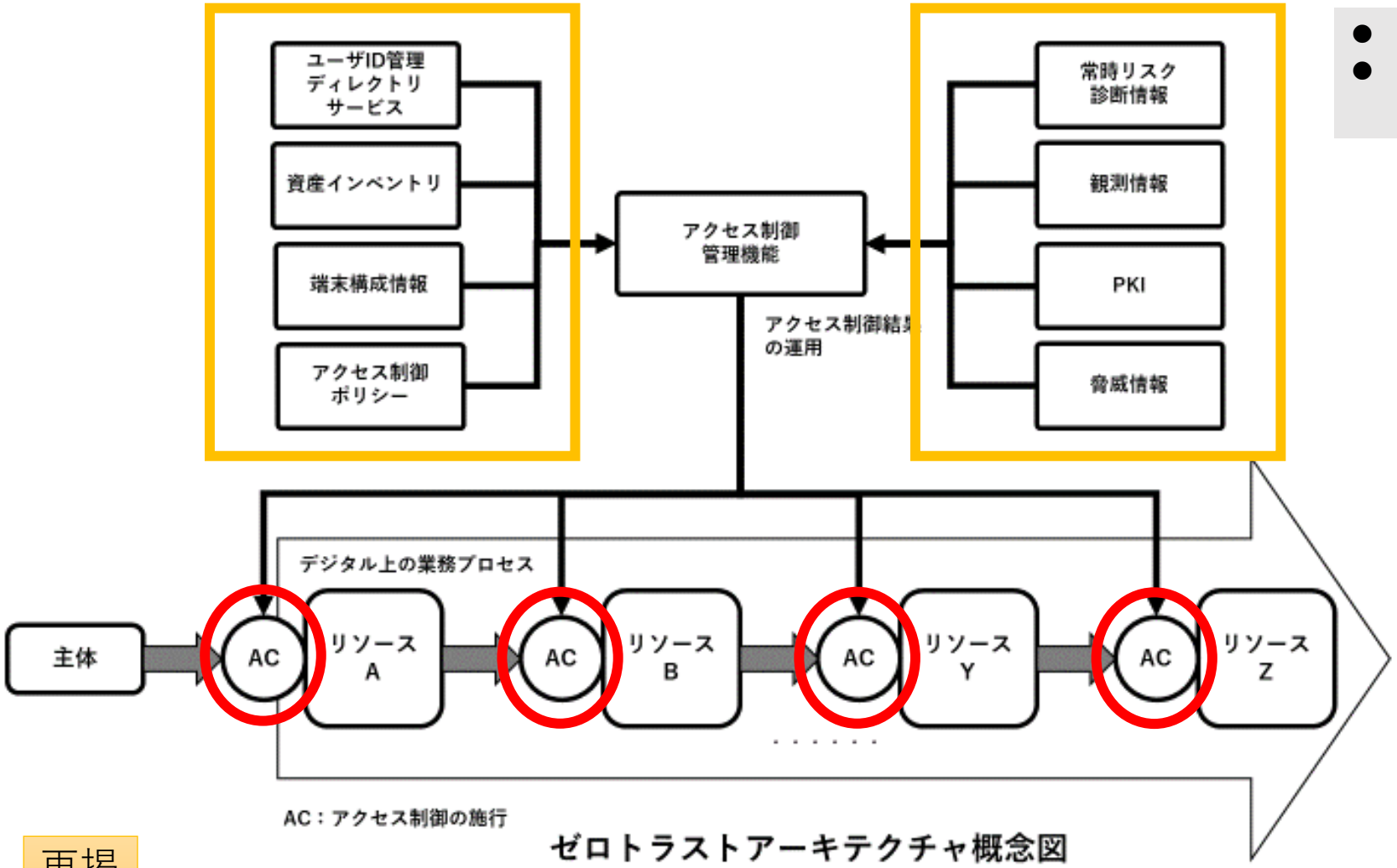




ゼロトラストアーキテクチャ適用方針の概要

https://www.digital.go.jp/resources/standard_guidelines/#ds210

ゼロトラストアーキテクチャとは、
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



ゼロトラストアーキテクチャ概念図

再掲

- 従来のセキュリティモデルから考え方を拡張
- 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**

ゼロトラスト・アーキテクチャを適用する際の基本方針
①**リソースを識別し、特定**できる状態にする
②**主体の身元確認・当人認証**を実施する
③**ネットワークを保護**する
④リソースの**状態を確認**する
⑤**アクセス制御ポリシーで評価**し、アクセス管理をする
⑥リソースとアクセスを**観測**する

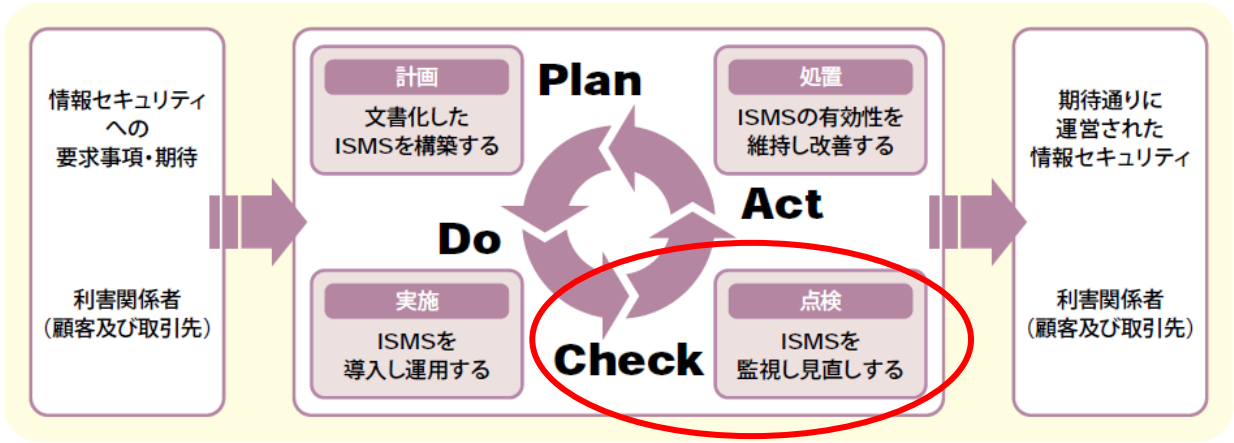
適用における留意事項

セキュリティマネジメントの自動化

従来の情報セキュリティマネジメント

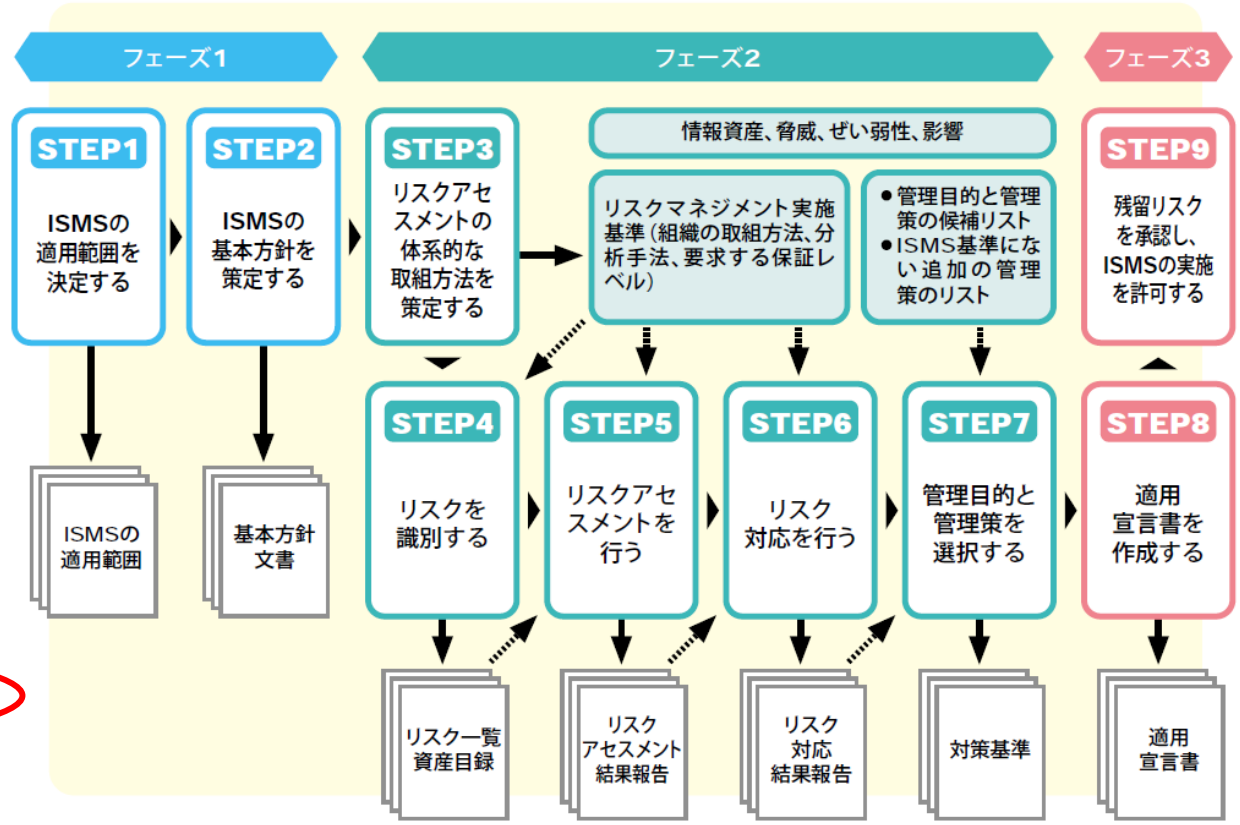
２００１年頃

PDCAモデル



Plan－計画（ISMSの確立）	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。
Do－実施（ISMSの導入及び運用）	その情報セキュリティ基本方針、管理策、プロセス及び手順を導入し運用する。
Check－点検（ISMSの監視及び見直し）	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act－処置（ISMSの維持及び改善）	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

ISMSの確立



「一般財団法人日本情報経済社会推進協会　ISMS適合性評価制度の概要」より

近年におけるセキュリティマネジメントの課題

２０２３年頃

リスクアセスメント、文書作成、見直しが**人間によって行われる**

- 作業が難しい。冗長である。俗人化。（客観的な評価が困難）

PDCAのサイクルは、**年に１回程度**を想定している。

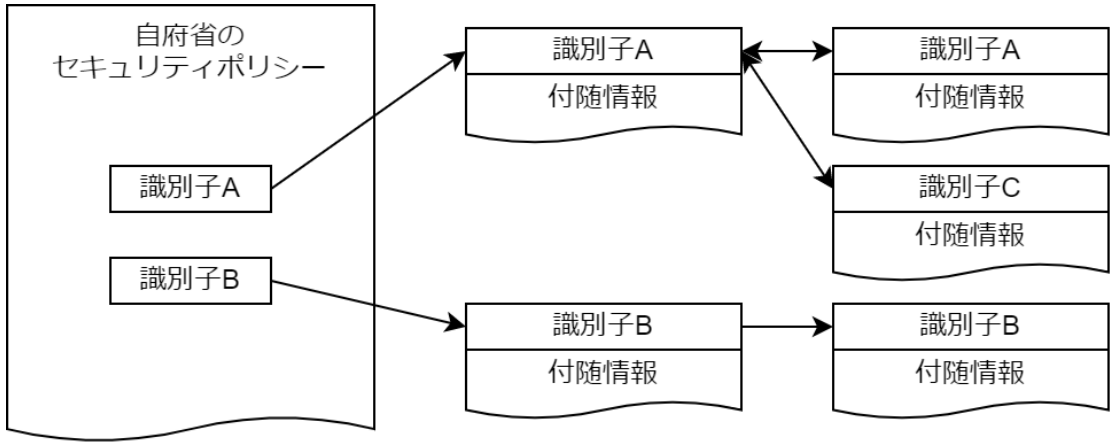
- システム開発やサービス開発は、短期間になってきている。また、システム開発もサービス開発も**アジャイル的な発想**になっており、**DevOPS**（継続的インテグレーション/継続的デリバリー）になっている

少し**複雑な管理**になると、評価、見直し等の**工数が莫大**になる。

- 対応が**複雑化**し始めている。例えば、「政府機関等のサイバーセキュリティ対策のための統一基準群」「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の複数のポリシー準拠が必要。サービスによっては、「PCIDSS」等の**業界標準にも対応**することが必要になる。これらを評価し、見直すためには、人員でおこなう場合、かなりの工数が必要。

セキュリティ統制のカタログ化の概要

- カタログ化とは、以下に示すセキュリティ対策において、**統制を有効にするために設定する目標「セキュリティ統制」**に対して**一意な識別子を付与**し、**機械可読な形式で分類**することを指すものである
  - **情報セキュリティポリシー運用業務**
  - **システム実装業務および運用業務**
  - **セキュリティ監査業務を検討および実施**



- セキュリティ統制を識別子によって一意に識別し、マークアップ言語などで表現し機械可読化することにより、例として以下を実現することが可能となる。
  - **ポリシーの柔軟な変更（統制の追加、変更）**、**システム実装および変更の自動化**
  - **IaC、テンプレート活用など、クラウドネイティブ技術にてセキュアな実装を促進**
  - **オートスケール環境や短命なシステムにおいても、セキュアな状態を維持**
  - **監査および是正の自動化まで実施することで、24時間/365日セキュアな状態を実現**

セキュリティ統制のカタログ化の例

- NIST SP800-53およびOSCALについて
  - NIST SP800-53 は、米国連邦政府の内部セキュリティ基準を示すガイドラインの一つであり、**管理策番号としてAC-1のような番号で表現**している。
  - OSCAL（Open Security Controls Assessment Language）は、情報セキュリティ責任者、ベンダー、および監査人などのセキュリティ統制業務に携わる関係者の事務処理を減らすため、正確で**機械可読な形式を使用して、セキュリティ制御カタログ、規制フレームワーク、およびシステム情報の表現を正規化**し、組織間での制御実装情報の共有を可能にしている。

```
groups:
    - id: ia
      class: family
      title: Identification and Authentication
      controls:
（中略）
        - id: ia-3
          class: SP800-53
          title: Device Identification and Authentication
          params:
            - id: ia-03_odp.01
              label: devices and/or types of devices
              guidelines:
                - prose: devices and/or types of devices to be uniquely identified
                    and authenticated before establishing a connection are defined;
…略
```

セキュリティ統制のカタログ化の効果

情報セキュリティポリシーのメンテナンス性向上への対応

- 組織における情報セキュリティポリシーのメンテナンス性を高めたい。

セキュリティ統制の業務間におけるトレーサビリティ確保への対応

- 様々な基準、ガイドライン等に整合性のある対応を着実に効率よく実施したい。

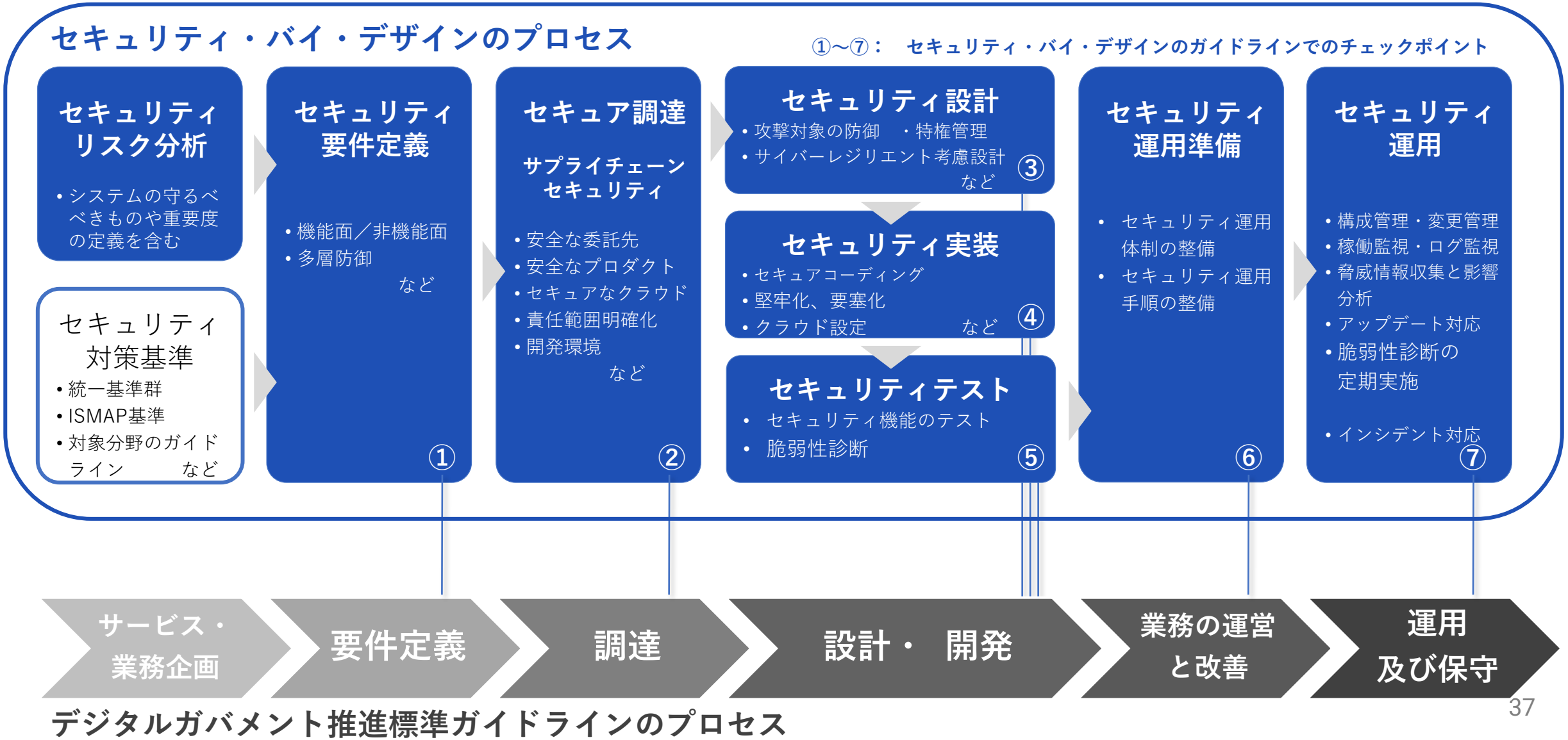
政府情報システム環境の多様化への対応

- 多様化するシステム環境それぞれにおいて、一貫したポリシーに基づくセキュリティ統制を行いたい。

セキュリティ監査の高度化

- 自動化や機械化による監査の高度化および効率化を目指したい。

（参考）セキュリティ・バイ・デザインの概要



デジタルガバメント推進標準ガイドラインのプロセス

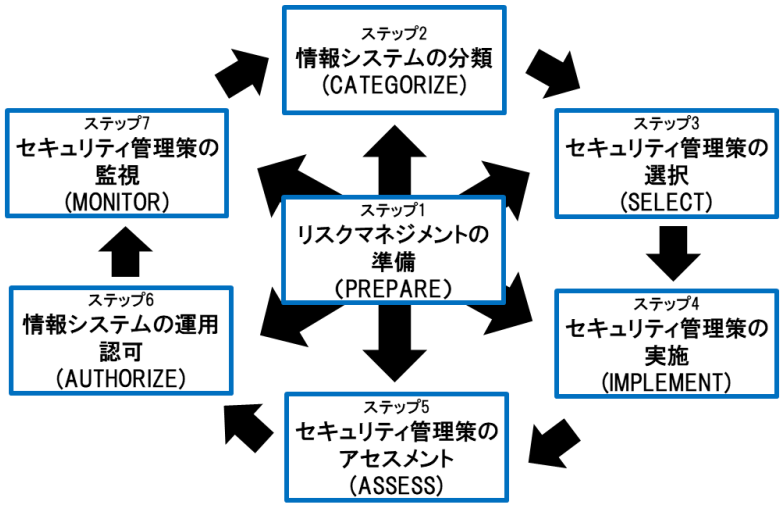
（参考）ベースラインからのリスク分析のアプローチ

米国標準技術研究所(NIST)　SP800-37Rev2　を参考にリスク分析の手順を作成

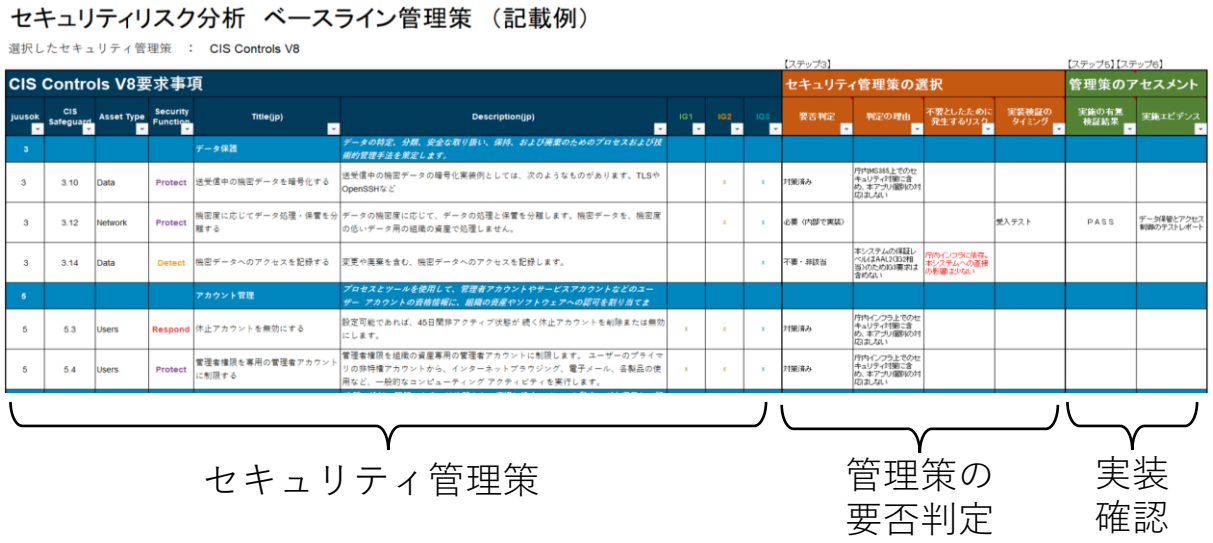
「Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy 」
（情報システムおよび組織のためのリスクマネジメントフレームワーク　－セキュリティとプライバシーのためのシステムライフサイクルアプローチ）

脅威分析をするのでなく、セキュリティ管理策をマネージメントする方式

システムには、このセキュリティ管理策が必要か？ ……→ 管理策を要否判定（テーラリング）
その管理策を実施しないとしたらどんなリスクがあるか？ ……→ 分析してレビュー確認



SP800-37のプロセス



ベースラインリスク分析のイメージ

（参考）ベースラインリスク分析のイメージ

セキュリティリスク分析　ベースライン管理策　（記載例）

選択したセキュリティ管理策　：　CIS Controls V8

CIS Controls V8要求事項									セキュリティ管理策の選択【ステップ3】				管理策のアセスメント【ステップ5】【ステップ6】	
juusok	CIS Safeguard	Asset Type	Security Function	Title(jp)	Description(jp)	IG1	IG2	IG3	要否判定	判定の理由	不要としたために発生するリスク	実装検証のタイミング	実施の有無 検証結果	実施エビデンス
3				データ保護	*データの特定、分類、安全な取り扱い、保持、および廃棄のためのプロセスおよび技術的管理手法を策定します。*									
3	3.10	Data	Protect	送受信中の機密データを暗号化する	送受信中の機密データの暗号化実装例としては、次のようなものがあります。TLSやOpenSSHなど		x	x	対策済み	庁内MS365上でのセキュリティ対策に含め、本アプリ個別の対応はしない				
3	3.12	Network	Protect	機密度に応じてデータ処理・保管を分離する	データの機密度に応じて、データの処理と保管を分離します。機密データを、機密度の低いデータ用の組織の資産で処理しません。		x	x	必要（内部で実装）			受入テスト	PASS	データ保管とアクセス制御のテストレポート
3	3.14	Data	Detect	機密データへのアクセスを記録する	変更や廃棄を含む、機密データへのアクセスを記録します。			x	不要・非該当	本システムの保証レベルはAAL2(IG2相当)のためIG3要求は含めない	庁内インフラに依存。本システムへの直接の影響は少ない			
5				アカウント管理	*プロセスとツールを使用して、管理者アカウントやサービスアカウントなどのユーザー アカウントの資格情報に、組織の資産やソフトウェアへの認可を割り当てま*									
5	5.3	Users	Respond	休止アカウントを無効にする	設定可能であれば、45日間非アクティブ状態が 続く休止アカウントを削除または無効にします。	x	x	x	対策済み	庁内インフラ上でのセキュリティ対策に含め、本アプリ個別の対応はしない				
5	5.4	Users	Protect	管理者権限を専用の管理者アカウントに制限する	管理者権限を組織の資産専用の管理者アカウントに制限します。 ユーザーのプライマリの非特権アカウントから、インターネットブラウジング、電子メール、各製品の使用など、一般的なコンピューティング アクティビティを実行します。	x	x	x	対策済み	庁内インフラ上でのセキュリティ対策に含め、本アプリ個別の対応はしない				

セキュリティ管理策　　管理策の要否判定　　実装確認

セキュリティ統制のカタログ化の例

ISMAPの概要

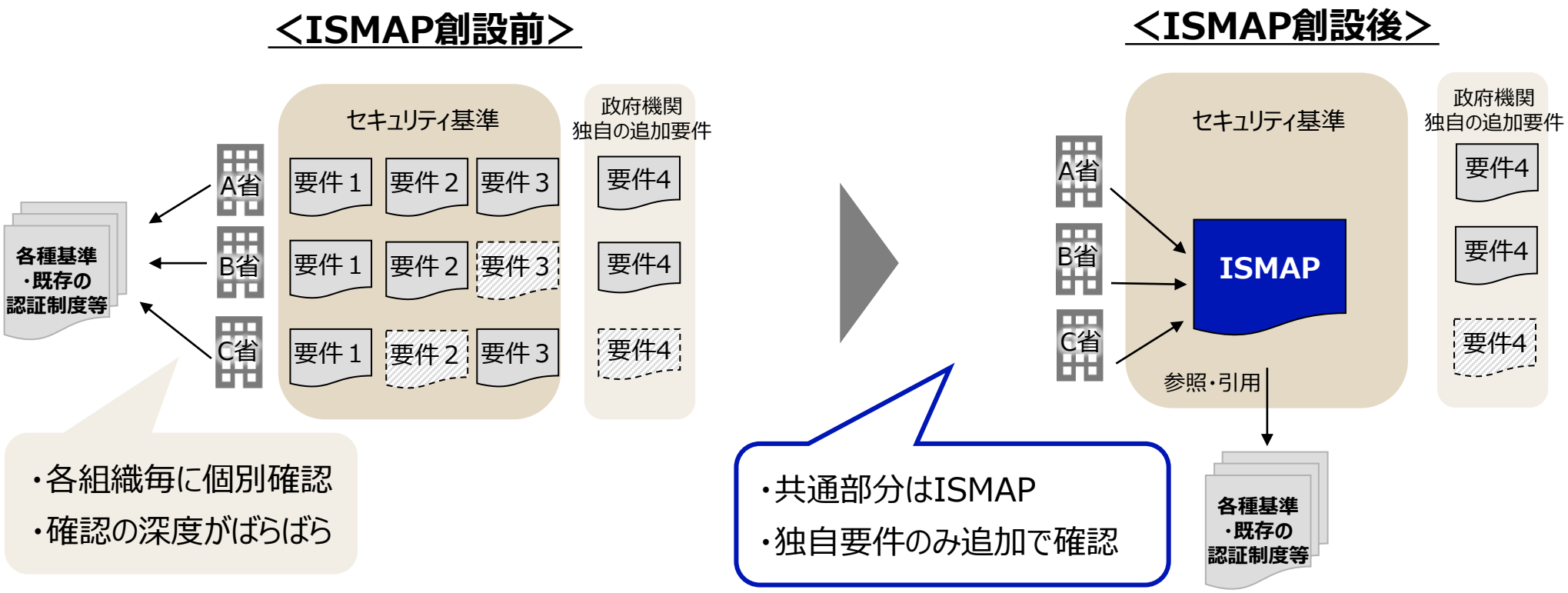
ISMAPについて

政府情報システムのためのセキュリティ評価制度
ISMAP：Information system Security Management and Assessment Program

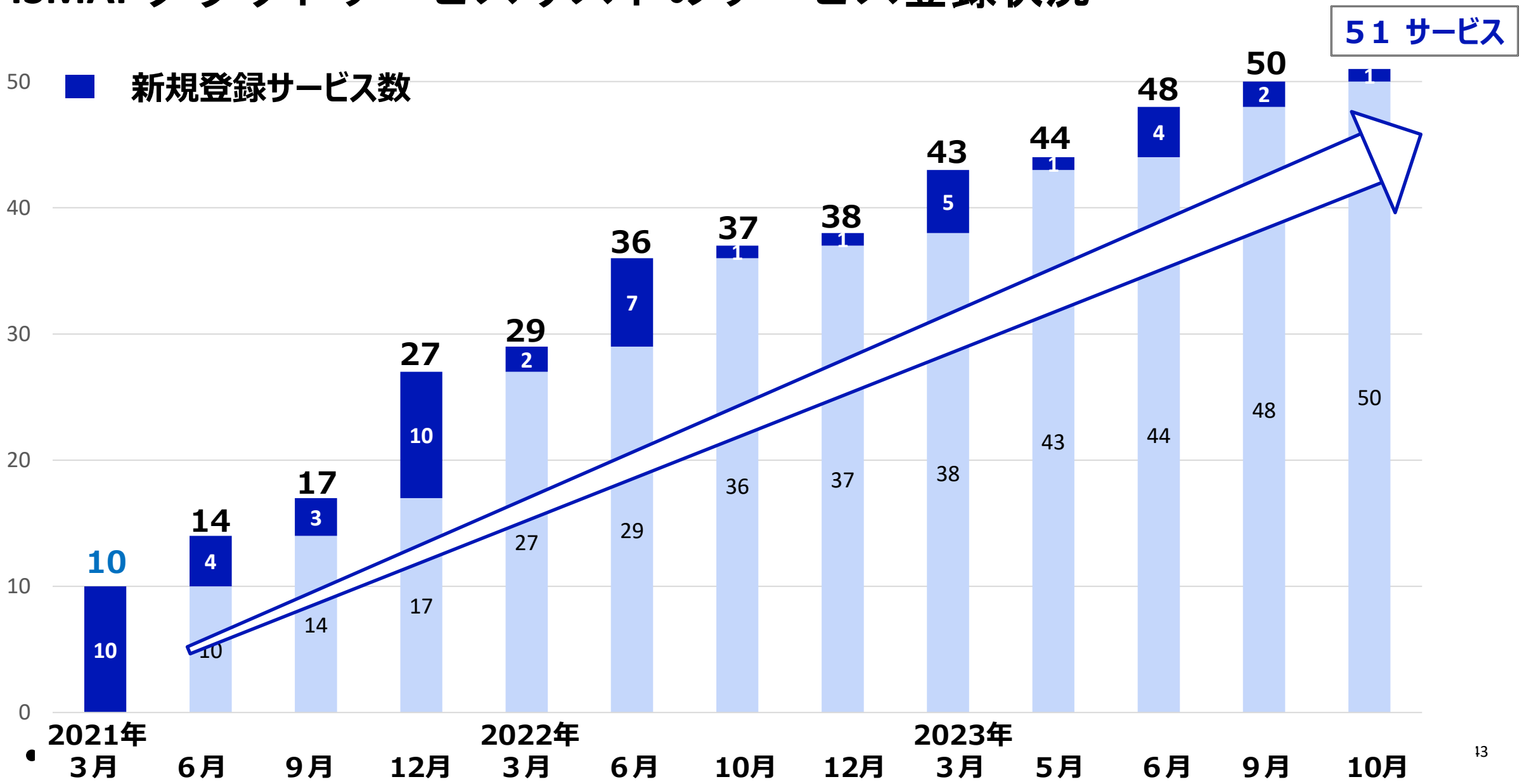
- 「**クラウド・バイ・デフォルト原則**」が提唱され、安全性評価を通して適切なセキュリティ水準が確保された信頼できるクラウドサービスを利用する必要性が顕著に。
- 国際的なセキュリティの標準をふまえ、ISMAP管理基準（セキュリティの基準）を策定し、各基準について**第三者が監査するプロセスを経て、クラウドサービスを登録する制度**として、2020年6月にISMAPを創設した。
- 政府機関のクラウドサービスの調達にあたっては、**原則、「ISMAPクラウドサービスリスト」から調達する**こととされている。

ISMAP創設の狙い

- 政府機関がクラウドサービスを利用する際の**統一的なセキュリティの基準**を明確化し、定められた手続きに基づいて**安全性が評価されたクラウドサービス**を、効率的に利用すること。



ISMAPクラウドサービスリストのサービス登録状況



ISMAP登録までの流れ

準備

- ISMAP管理基準に基づいた**統制の整備・運用を実施**する
- 「言明書」「経営者確認書」を作成し、**自身のセキュリティ対策について言明**を行い、監査機関に提出する

監査

- **監査機関による外部監査**が実施される
- 監査実施後、監査機関により「実施結果報告書」が作成される

申請

- 言明書・実施結果報告書等の申請に係る文書を添えてISMAPポータルサイトから申請する

審査

- ISMAP運用支援機関（IPA）による申請の受理後、申請文書に基づき**技術的審査が実施される**
- 技術的な審査を踏まえ、**「ISMAP運営委員会」により登録の意思決定が行われる**

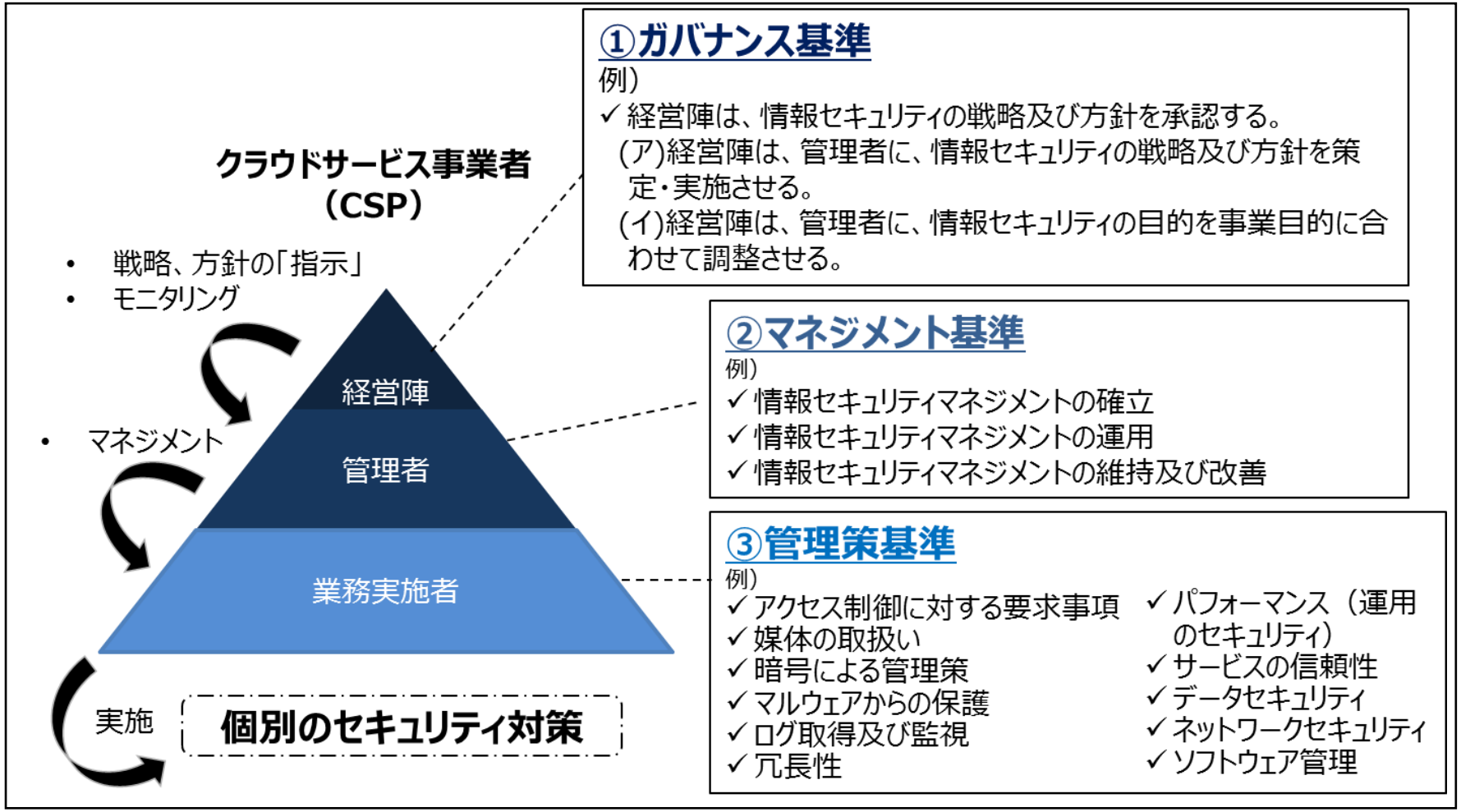
登録

- クラウドサービスリストへ登録され、**ISMAPポータルサイトにおいて公表**される

ISMAPの管理基準

- 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。

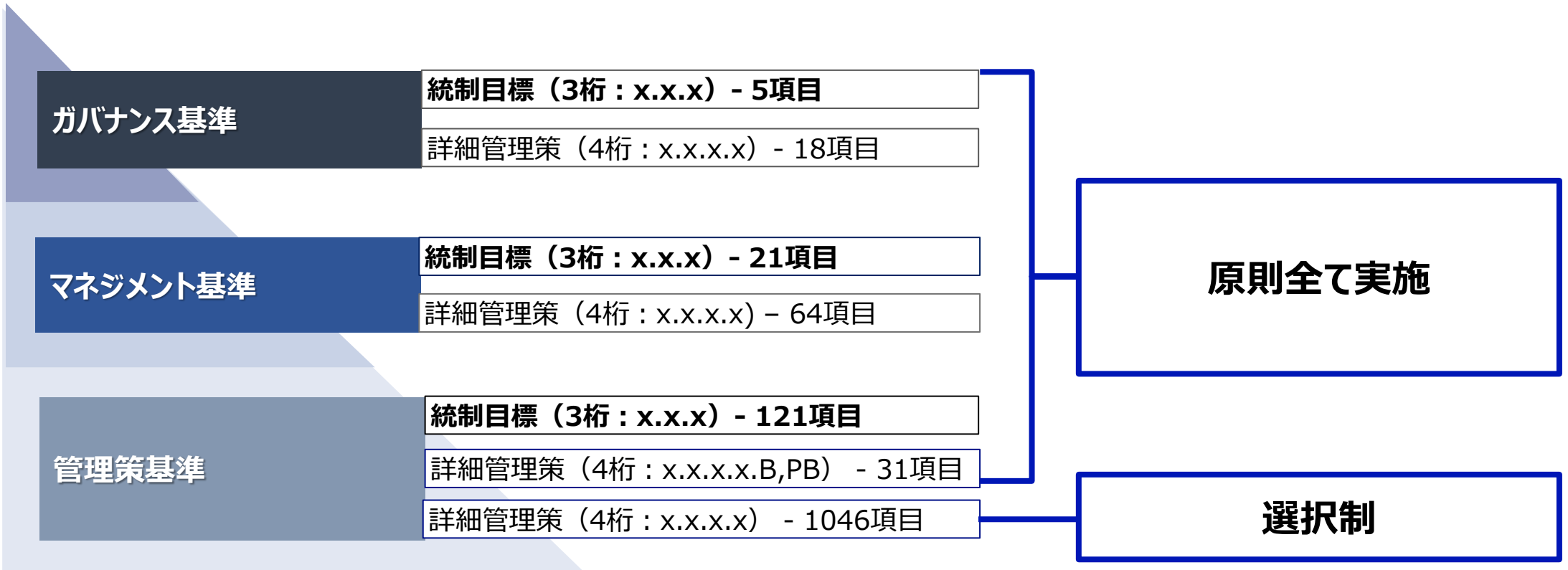
管理基準の構成



ISMAP管理基準について

〔ISMAP管理基準の言明〕

統制目標：CSPがリスクに対応するために達成するべき統制の目標とする項目
詳細管理策：CSPが統制目標を実現するために選択して満たすべき事項



クラウドサービスリスト

C21-0001-2	OpenCanvas(IaaS)	株式会社エヌ・ティ・ティ・データ	9010601021385	東京都江東区豊洲３丁目３番３号	2021/03/12	2022/11/30	2021/12/20　登録の更新期限、監査対象期間、言明の対象範囲、情報等を変更
C21-0002-2	FUJITSU Hybrid IT Service FJcloud	富士通株式会社	1020001071491	神奈川県川崎市中原区上小田中四丁目１番１号	2021/03/12	2023/02/28	2022/3/29　登録の更新期限、監査対象期間、情報等を変更
C21-0003-2	Apigee Edge	Google LLC	3700150072195	1600 Amphitheatre Parkway Mountain View, California 94043, USA	2021/03/12	2022/04/09	2022/04/08　更新申請が行われているため有効期限以降も登録は有効
C21-0004-2	Google Cloud Platform	Google LLC	3700150072195	1600 Amphitheatre Parkway Mountain View, California 94043, USA	2021/03/12	2022/04/09	2021/9/13　言明対象範囲（サービス）を変更 2022/04/08　更新申請が行われているため有効期限以降も登録は有効
C21-0005-2	Google Workspace	Google LLC	3700150072195	1600 Amphitheatre Parkway Mountain View, California 94043, USA	2021/03/12	2022/04/09	2022/04/08　更新申請が行われているため有効期限以降も登録は有効
C21-0006-2	Salesforce Services	株式会社セールスフォース・ジャパン	4010401076766	東京都千代田区丸の内1-1-3　日本生命丸の内ガーデンタワー(Salesforce Tower)	2021/03/12	2022/04/14	2022/3/4　事業者の名称・所在地を変更 2022/04/14　更新申請が行われているため有効期限以降も登録は有効
C21-0007-2	Heroku Services	株式会社セールスフォース・ジャパン	4010401076766	東京都千代田区丸の内1-1-3　日本生命丸の内ガーデンタワー(Salesforce Tower)	2021/03/12	2022/04/14	2021/6/22　言明対象範囲（リージョン及びサービス）を変更 2022/3/4　事業者の名称・所在地を変更 2022/04/14　更新申請が行われているため有効期限以降も登録は有効
C21-0008-2	Amazon Web Services	Amazon Web Services,Inc.		410 Terry Avenue North Seattle, WA 98109-5210	2021/03/12	2022/03/31	2021/6/22　言明対象範囲（リージョン及びエッジロケーション）を変更 2022/03/31　更新申請が行われているため有効期限以降も登録は有効
C21-0009-2	NEC Cloud IaaS	日本電気株式会社	7010401022916	東京都港区芝５丁目７番１号	2021/03/12	2022/04/01	2022/04/01　更新申請が行われているため有効期限以降も登録は有効
C21-0010-2	KDDIクラウドプラットフォームサービス	KDDI株式会社	9011101031552	東京都新宿区西新宿 2-3-2	2021/03/12	2022/04/18	2022/04/18　更新申請が行われているため有効期限以降も登録は有効
C21-0011-2	Oracle Cloud Infrastructure	Oracle Corporation		2300 Oracle Way, Austin, TX 78741, United States	2021/06/22	2022/04/30	2022/04/28　更新申請が行われているため有効期限以降も登録は有効

https://www.ismap.go.jp/csm?id=cloud_service_list

（C21-0008-2 Amazon Web Servicesの場合）

登録簿の公開

Amazon Web Services　言明対象範囲

本システムは以下の対象範囲で構成されています。

AWS のサービス	名前空間*	概要
Amazon API Gateway	apigateway	数回クリックするだけで、簡単に API の作成、配布、保守、監
Amazon AppF		
Amazon AppSt		

アメリカ	Arizona	California	Colorado	Florida	Georgia
	Illinois	Massachusetts	Minnesota	Missouri	Nevada
	New Jersey	New Y			
	Texas	Virgini			
ベトナム	Hanoi	Ho Chi			

Wavelength ロケーション（AWS イン
トワークに拡張することにより、超低レ
供できるように設計されています。）

国名	Wavelength ロケーション	Wavel ロケー
日本	Osaka	Tokyo

1　契約に定める準拠法・裁判管轄に関する情報：

準拠法：　日本国法
管轄裁判所：　東京地裁

記

1　資本関係及び役員等の情報：
Amazon Web Services, Inc.の株主 - AWSHC, Inc.の発行済株式数は1株のみです。
Amazon.com, Inc.は、Amazon Web Services, Inc.の直接の親会社ではありません。
Amazon Web Services, Inc.とAmazon.com, Inc.の関係は、Amazon.com, Inc.が間接的にAmazon Web Services, Inc.を所有していることになります。

役員等の情報
Chair of the Board　Adam Selipsky
Director and Secretar
Director
Director
Director

記

1　ISMAPクラウドサービス登録規則3.4(4)に定める情報：
AWS Securityでは、厳選された業界の専門家や独立したセキュリティ会社により定期的にペネトレーションテストを実施していますが、その結果をお客様と直接共有することはありません。その代わりに、結果は弊社の監査人によってレビューされ、検証されます。
お客様は、お客様のインスタンスに限定され、AWSの利用規定に違反しない限り、下記のサービスに関しAWSリソースを対象とした、またはAWSリソースを起点としたペネトレーションテストを実施する許可を要求することができます。

許諾なしに検査可能なサービス
Amazon EC2 インスタンス、NAT ゲートウェイ、Elastic Load Balancer
Amazon RDS
Amazon CloudFront
Amazon Aurora
Amazon API Gateway
AWS Lambda 関数およ
Amazon Lightsail リ
Amazon Elastic Beans

Amazon Web Services　基本言明要件のうち実施している統制目標の

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			

記

1　ISMAPクラウドサービス登録規則3.4(2)に定める情報：
AWSのお客様は、適用されるコンプライアンスに関する法律および規制に準拠する責任があります。場合によっては、お客様のコンプライアンスをサポートするために、AWSから機能（セキュリティ機能など）、支援ドキュメント、法的な契約書（AWS データ処理契約や事業提携契約など）が提供されます。

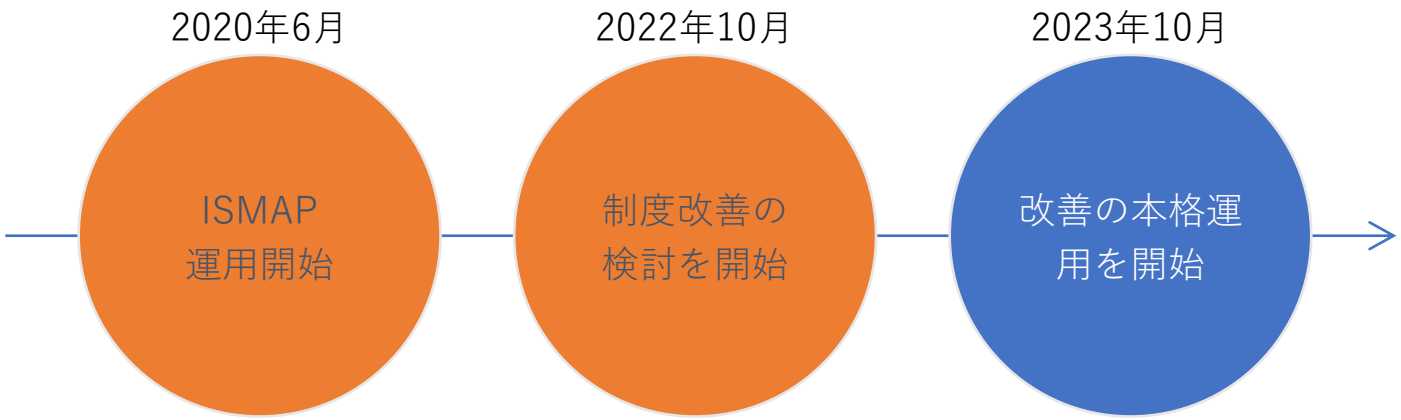
お客様がプライバシーとデータセキュリティについて懸念されるのは当然のことです。このため、AWS ではコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツをどこに保存するかをお客様に決定していただき、転送中のコンテンツと保管中のコンテンツを保護し、お客様のユーザーの AWS のサービスとリソースに対するアクセスを管理できるようにしています。また、お客様のコンテンツに対する不正アクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。

ISMAPの制度改善について

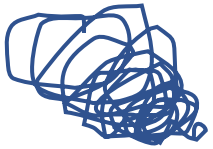
49

ISMAPにおける制度改善の歩み

- ISMAP運用開始以降、クラウドサービスに対するセキュリティ評価制度として定着。
- 一方で、運用開始から3年を通じた**課題が浮き彫り**となっており、セキュリティ評価制度としての信頼性・安全性は確保しつつ、**制度運用を合理化・明確化**する必要性が増している。
- **2022年10月から制度改善の検討**に着手し、**本年10月以降、順次、改善の本格運用を開始**。



ISMAP制度の課題と改善の概要（1/3）



外部監査の負担が重い

- **監査費用・工数**が大きな負担
- 更新時に係る外部監査の範囲と頻度について、登録申請時と同等の負担が毎年発生している

外部監査の負担を軽減

- **複数年を軸とした外部監査サイクル**を導入する
  - 管理策の重要度に応じてメリハリをつけて監査をすることで、監査対象の管理策数を削減する

ISMAP制度の課題と改善の概要（2/3）

審査の期間が長い

- 登録/更新申請から、審査が完了し登録/更新されるまでに**時間がかかっている**
- 新サービスがISMAPに登録されるまでの未登録期間が長く、新サービスをタイムリーに使うことが難しい

審査の迅速化・明確化

- **審査プロセスを改善**し、審査期間の短縮とプロセスの明確化する
  - 「モデル審査期間」を設定し、一般的な対応プロセスと期間を明確化することで、最短2ヶ月での審査完了*を可能とする
  - 審査遅延の主要因である「発見事項」への対応を充実させる

*更新申請のうち審査上問題の無いサービスが最短2ヶ月となり、新規登録申請についても概ね5ヶ月以内の審査を目指す

ISMAP制度の課題と改善の概要（3/3）

関係主体間のコミュニケーション不足

- 定期的なコミュニケーションの場が益々重要になっている
- 透明性のある制度のため、制度改善をはじめとする検討状況について情報公開が求められている
- 地方公共団体や重要インフラ含め、国全体のセキュリティレベルの底上げを推進する役割が期待されている

コミュニケーションの深化、透明性の確保、利用層の拡大

- 関係主体との継続的なコミュニケーションの場を設定
- ISMAP運営委員会の議事概要を公開
- ISMAPで安全性を評価したクラウドサービスの更なる利活用を目指す
  - 地方公共団体へのISMAPの利活用推奨、および基幹インフラ分野での活用策検討
  - ISMAP-LIUの登録促進に向けた取組

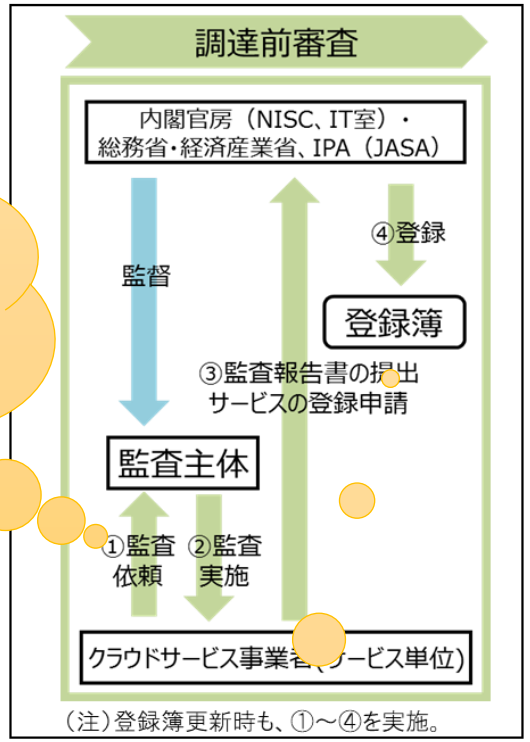
次世代セキュリティマネジメント

54

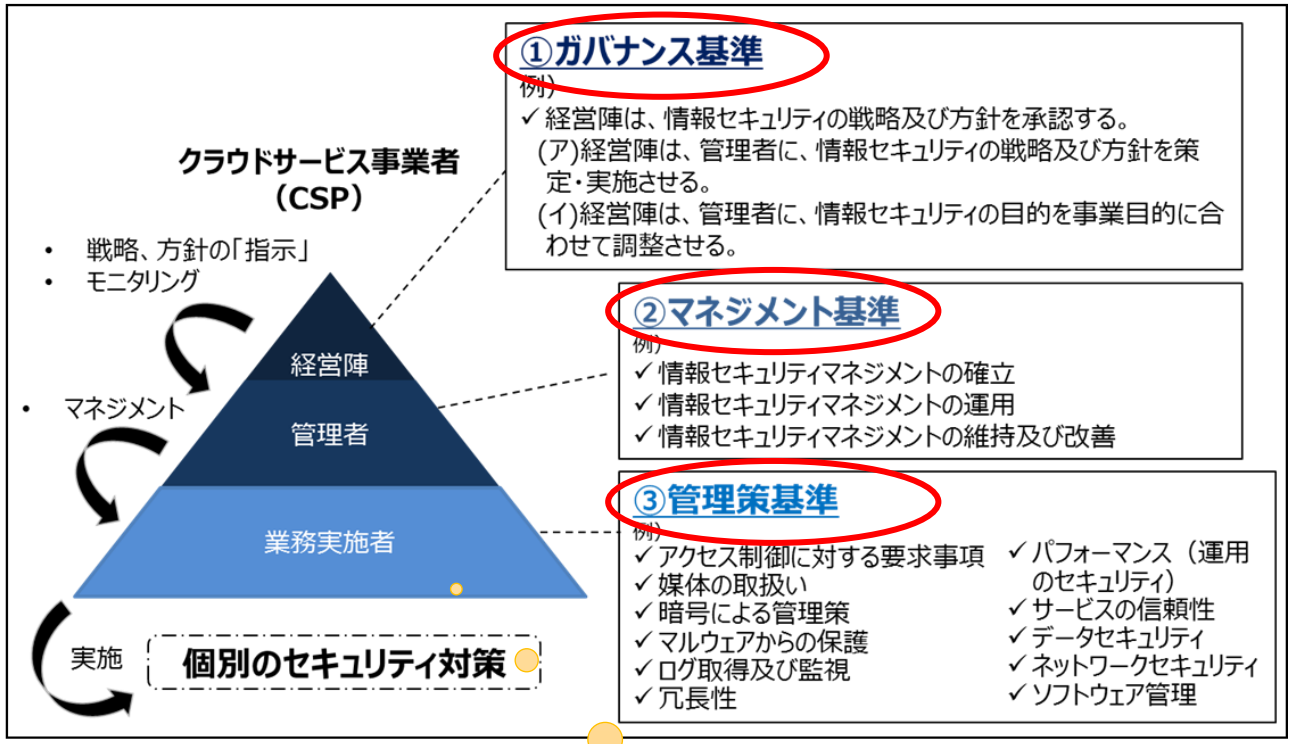
ISMAPにおける管理基準と登録の流れ

人がヒアリング・実査・
検証レポートの確認

CSP登録の流れ



管理基準の構成

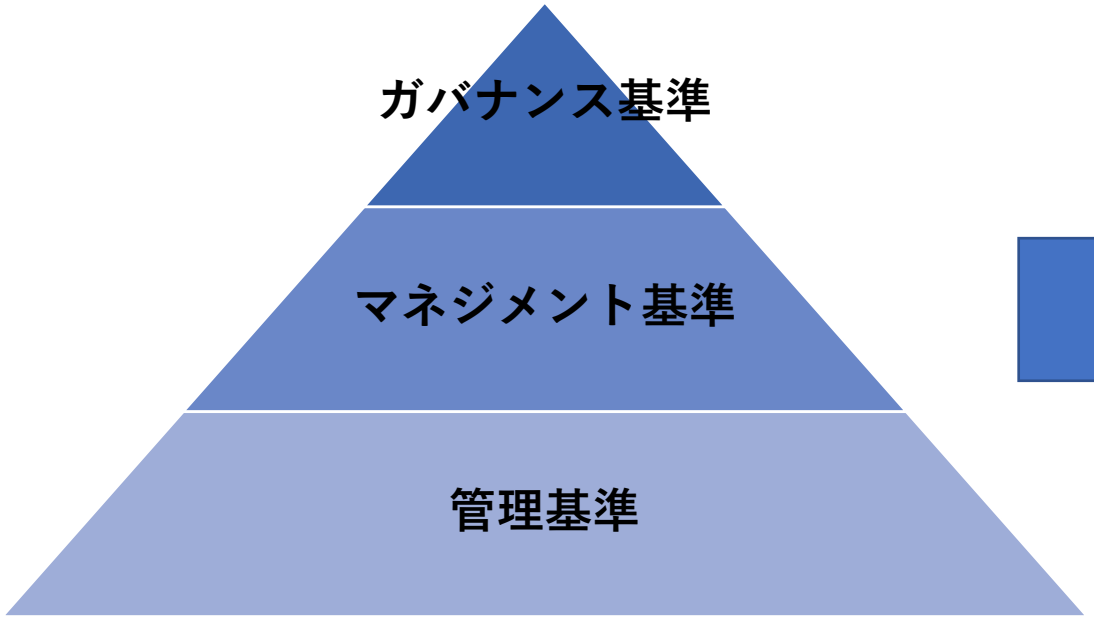


登録簿の公開による
情報開示

過去の実施状況
の確認

次世代の情報セキュリティマネジメント

マネジメント手法の変革



モニタリング手法

人によるヒアリング、実査等

システムのパラメーターを
直接モニタリング

システムを管理
するシステム

PDCAサイクルのタイミングの変革

半年or1年の監査対象期間を
半年後に監査報告

- 毎日、毎時間等の状況を数分後、数時間後には確認できる。
- ほぼリアルタイムにシステムの状況を把握

過去の状況であるが、未来予測につなげたい。

まとめ

- **ゼロトラストアーキテクチャー**は、サービスを最小化し、連携することを前提としたシステム構成における**セキュリティマネジメントの自動化**と言えるのではないか。
  - ✓ **アクセス制御のためのデータ（CRSA等）**を収集する。
  - ✓ **動的アクセス制御（ABAC等）でアクセス制御の最適化**を行う。

- **PDCAサイクルをデータで管理**し、セキュリティマネジメントをモダナイゼーションする。
  - ✓ **セキュリティコントロールのカタログ化**し、**セキュリティマネジメント（セキュリティ・バイ・デザイン、リスク分析、セキュリティ監査）をデジタル化**する。
  - ✓ PDCAサイクルのモニタリング手法の中で、**システムに関連する管理基準への対応は直接データをモニタリング**し、可視化する。
  - ✓ PDCAサイクルをデジタル化することにより、一回のサイクルを年単位から、月単位、日単位へ変えていく。できるだけ、**リアルタイムの状況把握**が可能にしたい。更には、**未来予測**につなげたい。

デジタル庁