デジタル庁におけるゼロトラストアーキテクチャへの取組

2023年8月

デジタル庁

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

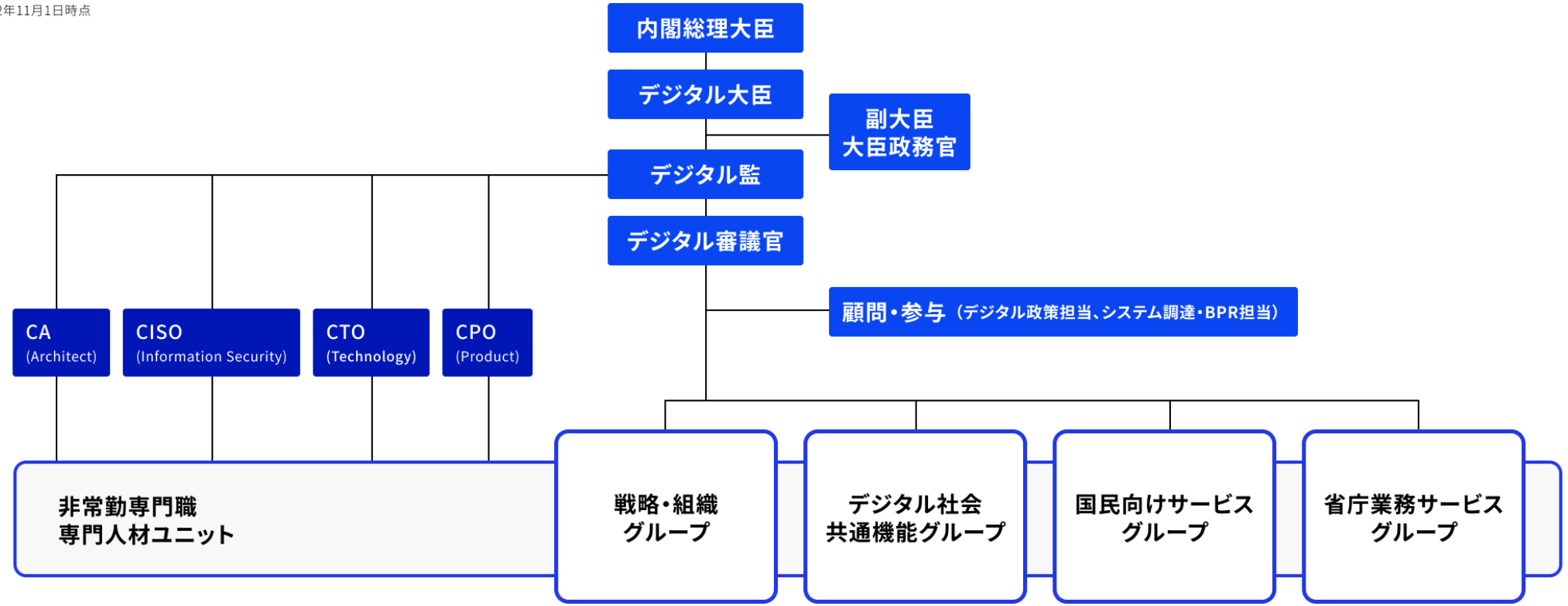
略歴

- 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

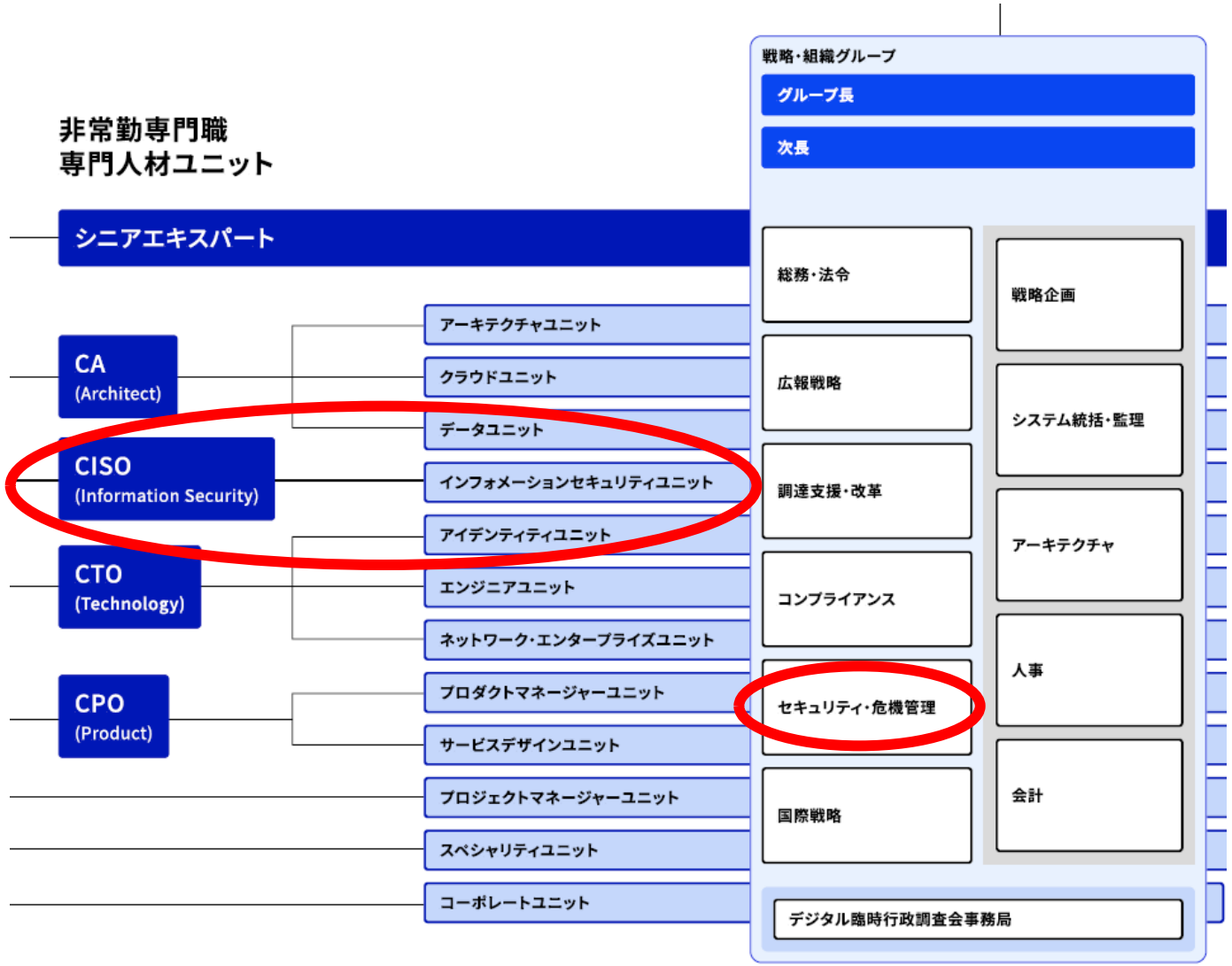
デジタル庁の組織体制

2022年11月1日時点



デジタル庁
Digital Agency

セキュリティ危機管理チーム



デジタル庁で整備・運用する主な政府情報システム

- 情報提供等記録開示システム
- 電子政府の総合窓口システム
- 補助金申請システム
- 法人共通認証基盤
- 政府共通ウェブサイト
- ＶｉｓｉｔＪａｐａｎＷｅｂ

等

- 電子決裁システム（ＥＡＳＹ）
- 旅費等内部管理業務共通システム
- ガバメントクラウド

等

デジタル庁システム：
40＋α

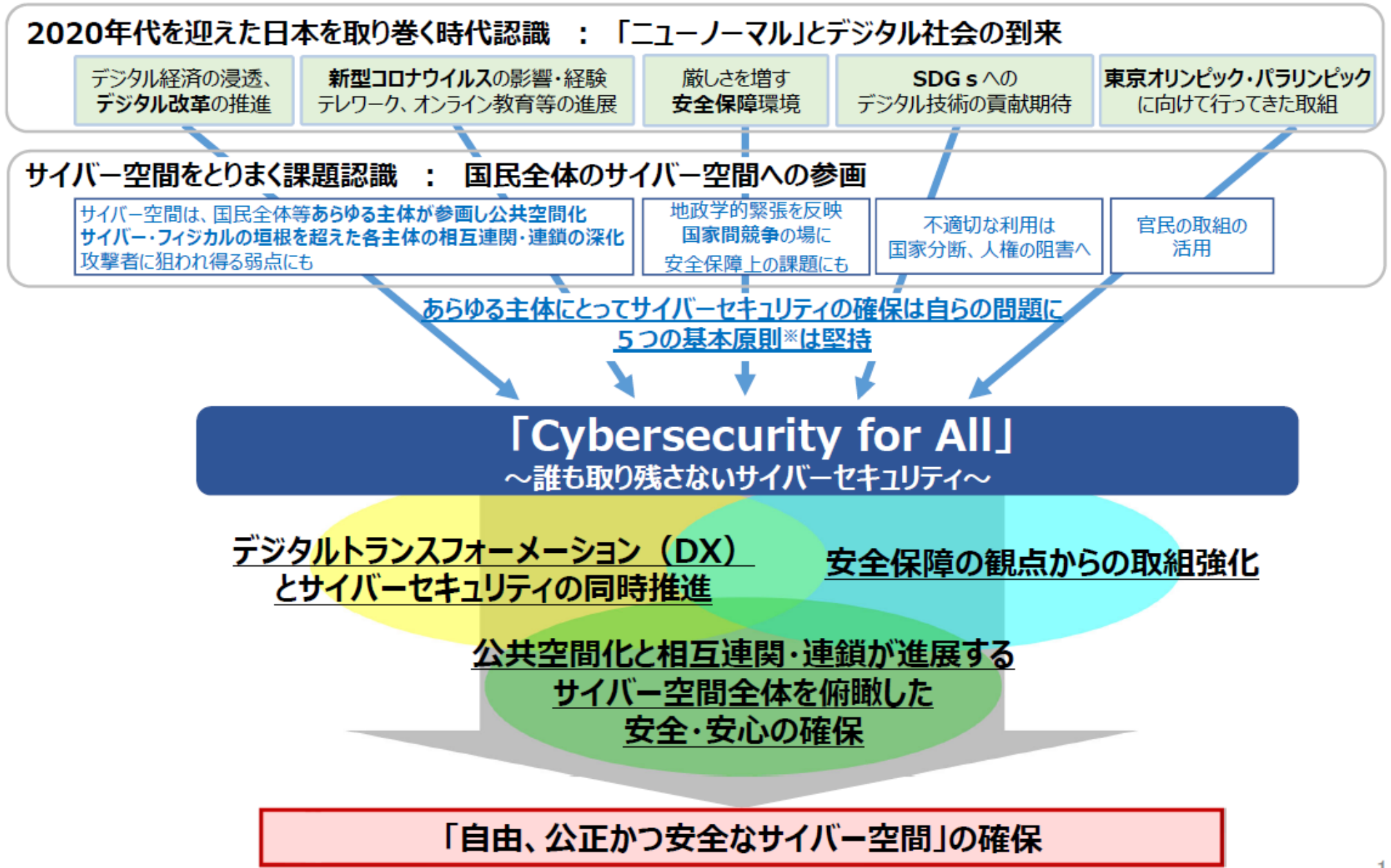
デジタル庁・各府省
共同プロジェクト型システム：
60程度

各府省システム：
1000以上

「情報システムに関する中長期計画」令和4年10月４日 デジタル庁　より
https://www.digital.go.jp/policies/development_management/

サイバーセキュリティ戦略

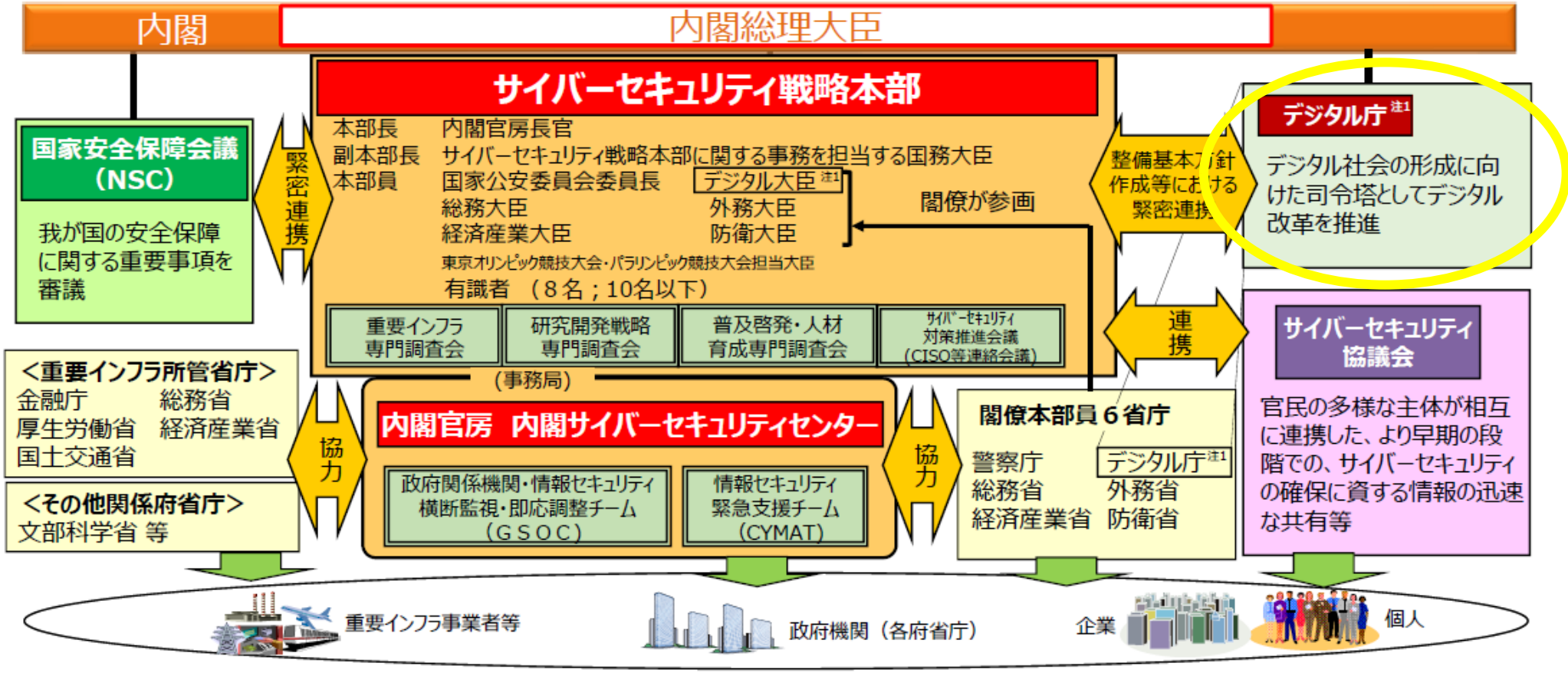
サイバーセキュリティ戦略の課題と方向性



※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

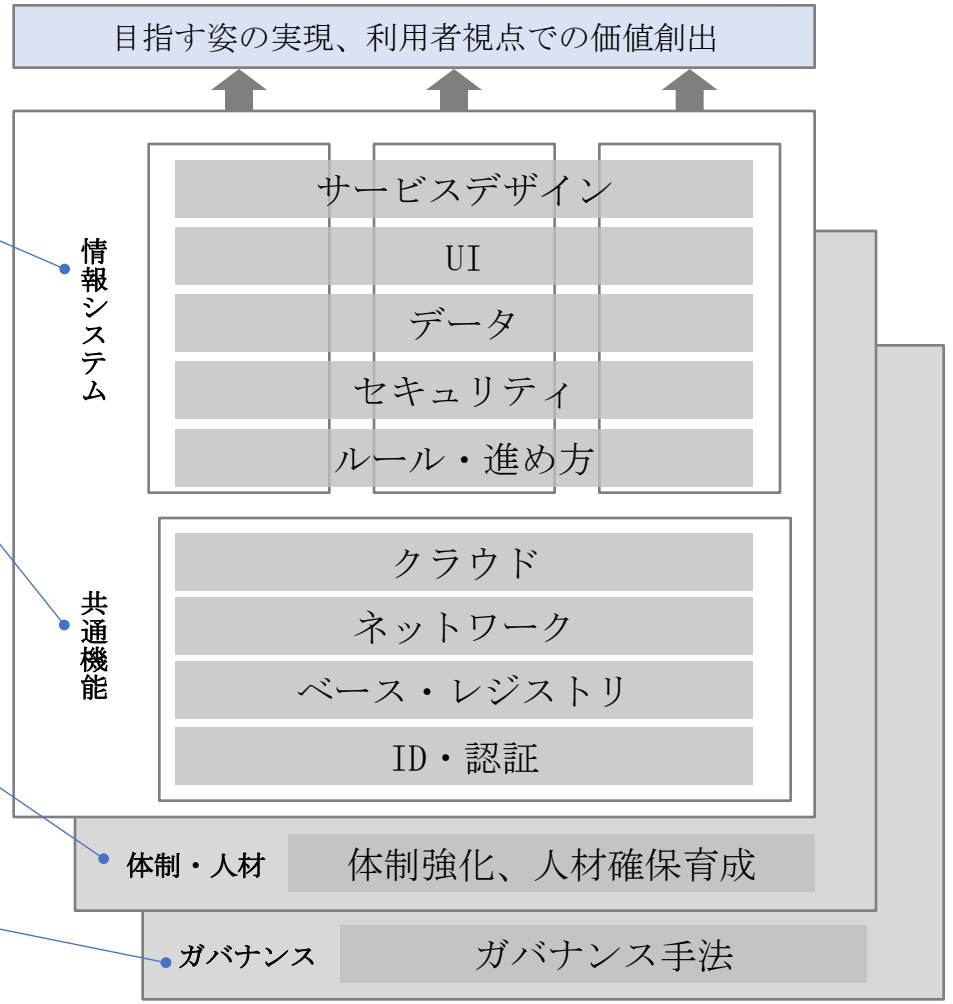
関係者が個々に努力するだけでは、目指す姿を実現できない。デジタル庁自身が特に４つの領域に注力し、旧来の課題を解消するとともに、国・地方公共団体・独立行政法人・準公共分野等の関係者が効果的に協働できるようにする。

1 良いサービスを作るための **標準** の策定・推進

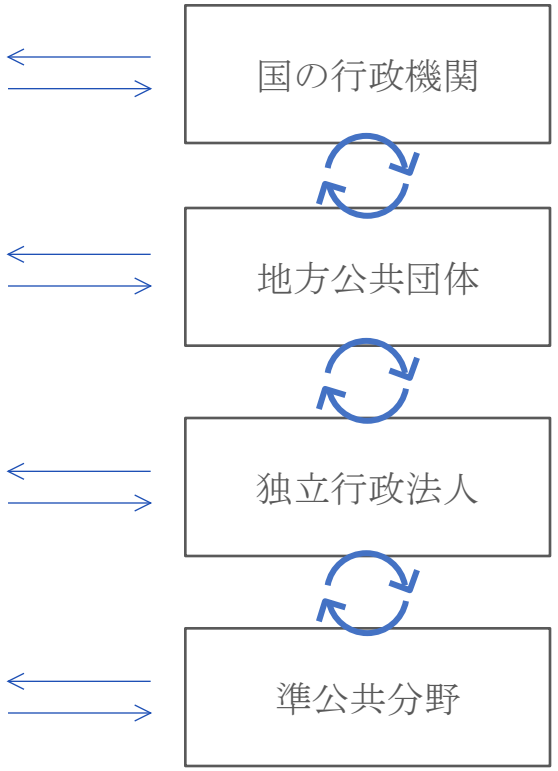
2 良いサービスを支える **共通機能** の整備・展開

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



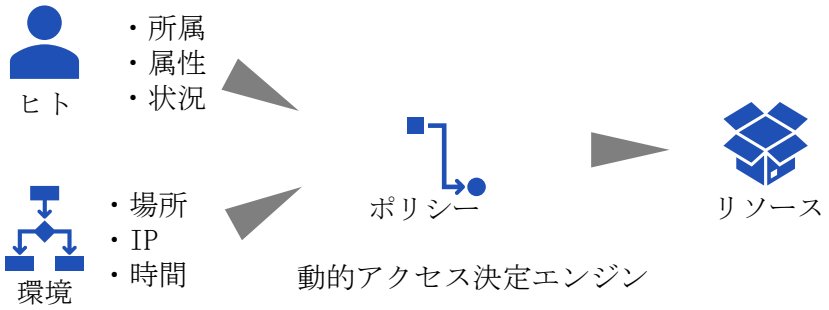
デジタル庁は、各関係者にとって利便性の高い標準、共通機能等となるように、利用状況を踏まえて継続的に改善を行う



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

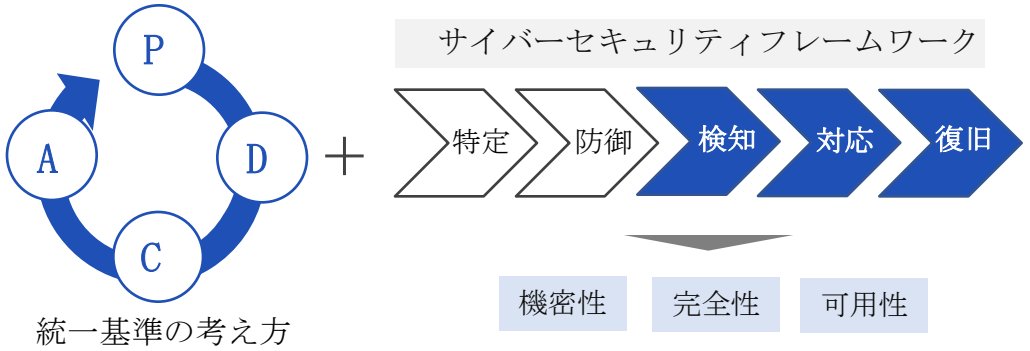
共通機能を前提とした常時診断・対応型のセキュリティーアーキテクチャ実装推進

- 「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。



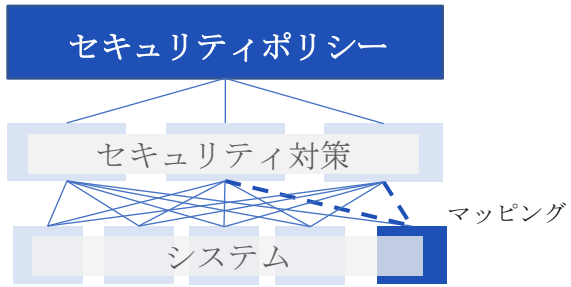
サイバーレジリエンスの強化

- 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。



デジタル社会推進標準ガイドライン（セキュリティに関するドキュメント）

セキュリティ関連標準ガイドライン群

- 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

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

高度標的型攻擊

（事例）日本年金機構の情報窃取事案

2015年5月～9月

5/8　標的型メール①

5/18-19　標的型メール②／③

5/19 警察所に相談

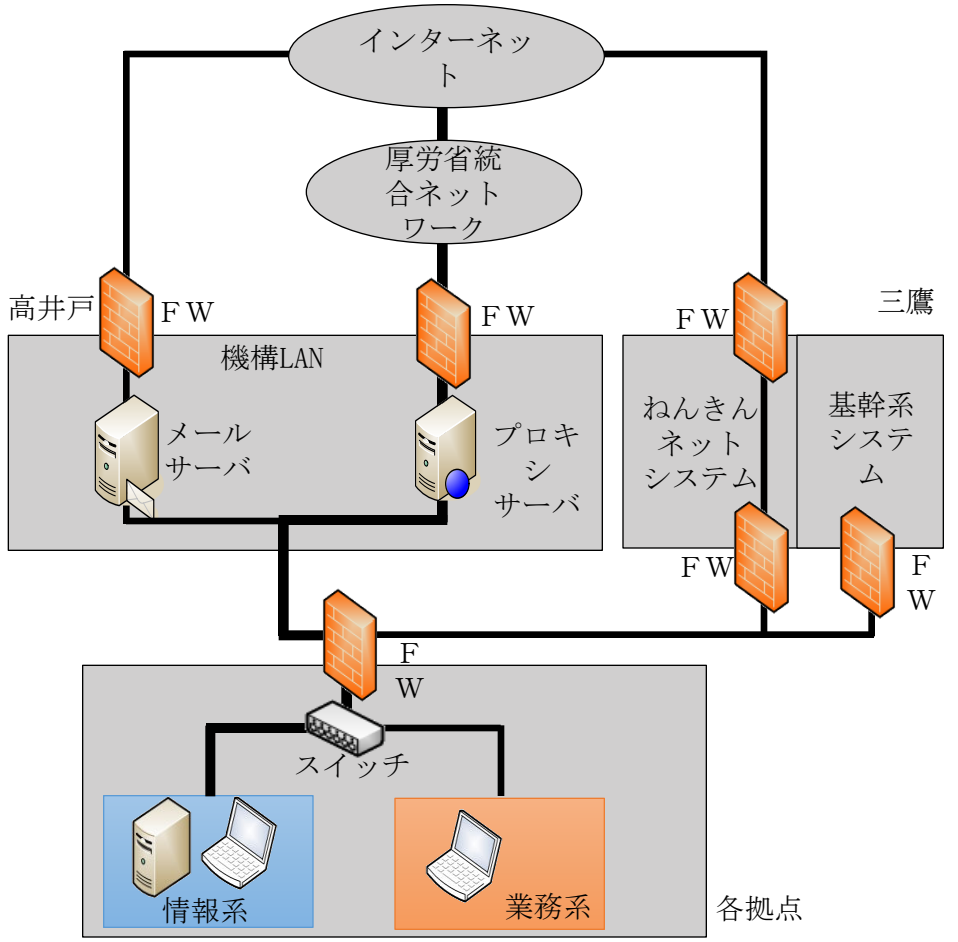
5/21　標的型メール④
5/21-23 侵入拡大・遮断

5/28 警察から情報流出事案の連絡

6/1 事案公表

8/20 原因究明調査報告書

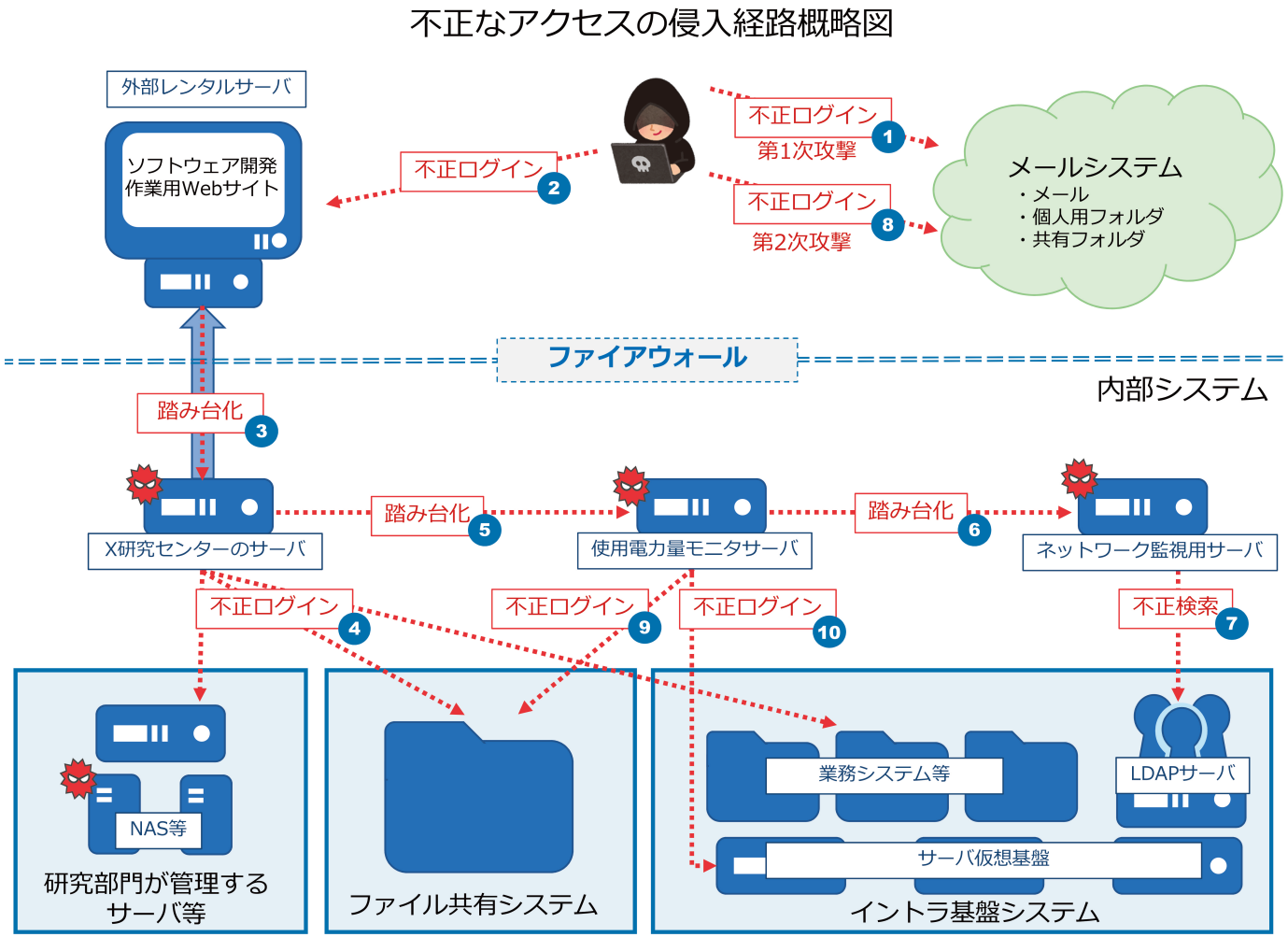
インシデント対処：サイバー攻撃を想定した具体的な対応が明確化されていない。
CSIRT体制：未整備
システム整備：業務系から情報系に個人情報を複製して取り扱っていた。



9/11 勧告

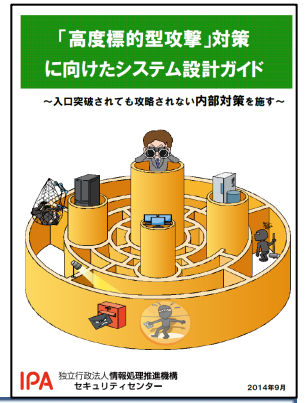
（事例）産総研の情報システムへの不正アクセス

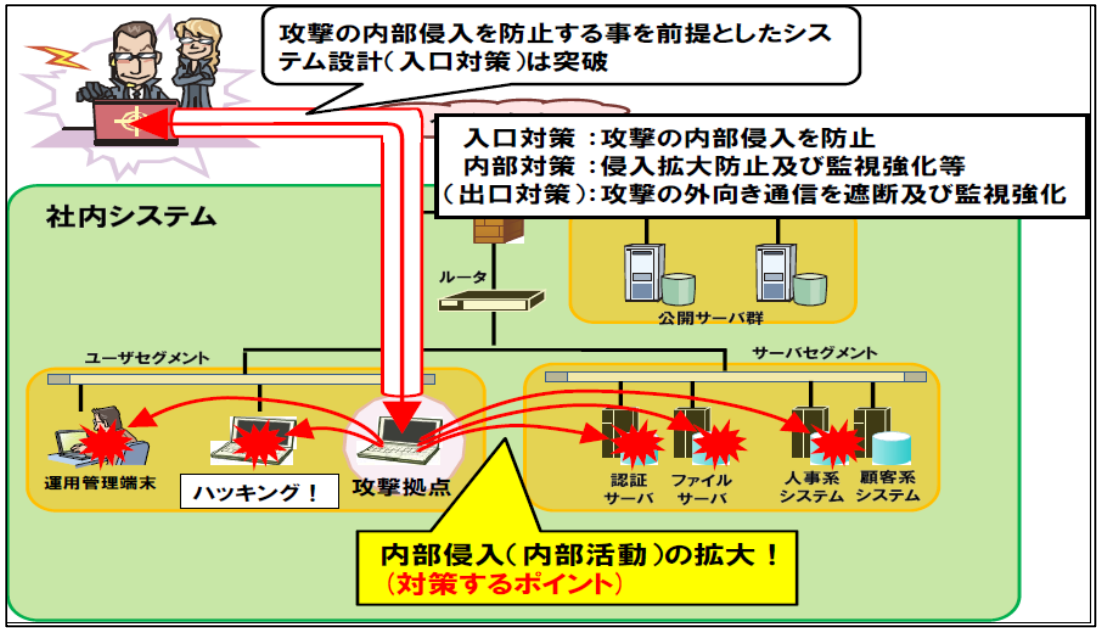
- 2017年10月、2018年1月のメールシステムへの不正なアクセスから始まり、研究情報、個人情報が外部へ漏洩又は閲覧された。

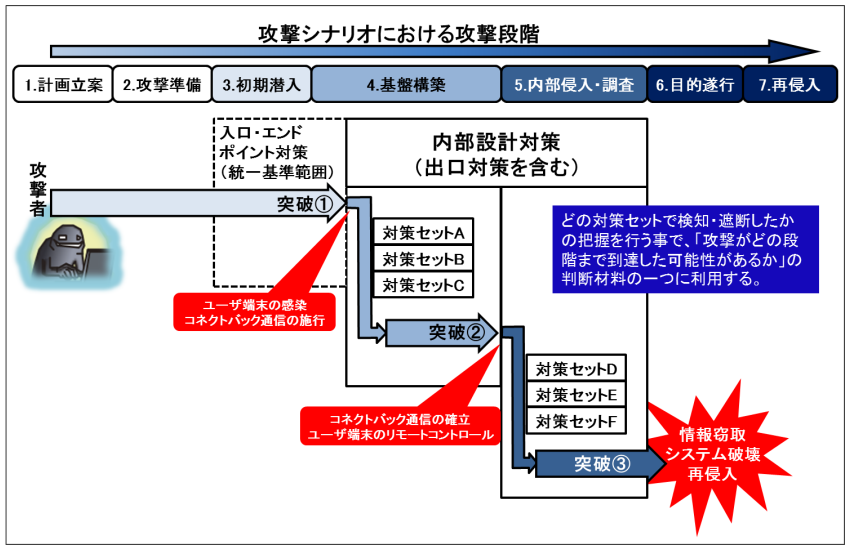


「産総研の情報システムに対する不正なアクセスに関する報告」（2018 年7 月20 日）
https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf

『高度標的型攻撃』対策に向けたシステム設計ガイド（2014年9月30日）
https://www.ipa.go.jp/security/vuln/newattack.html

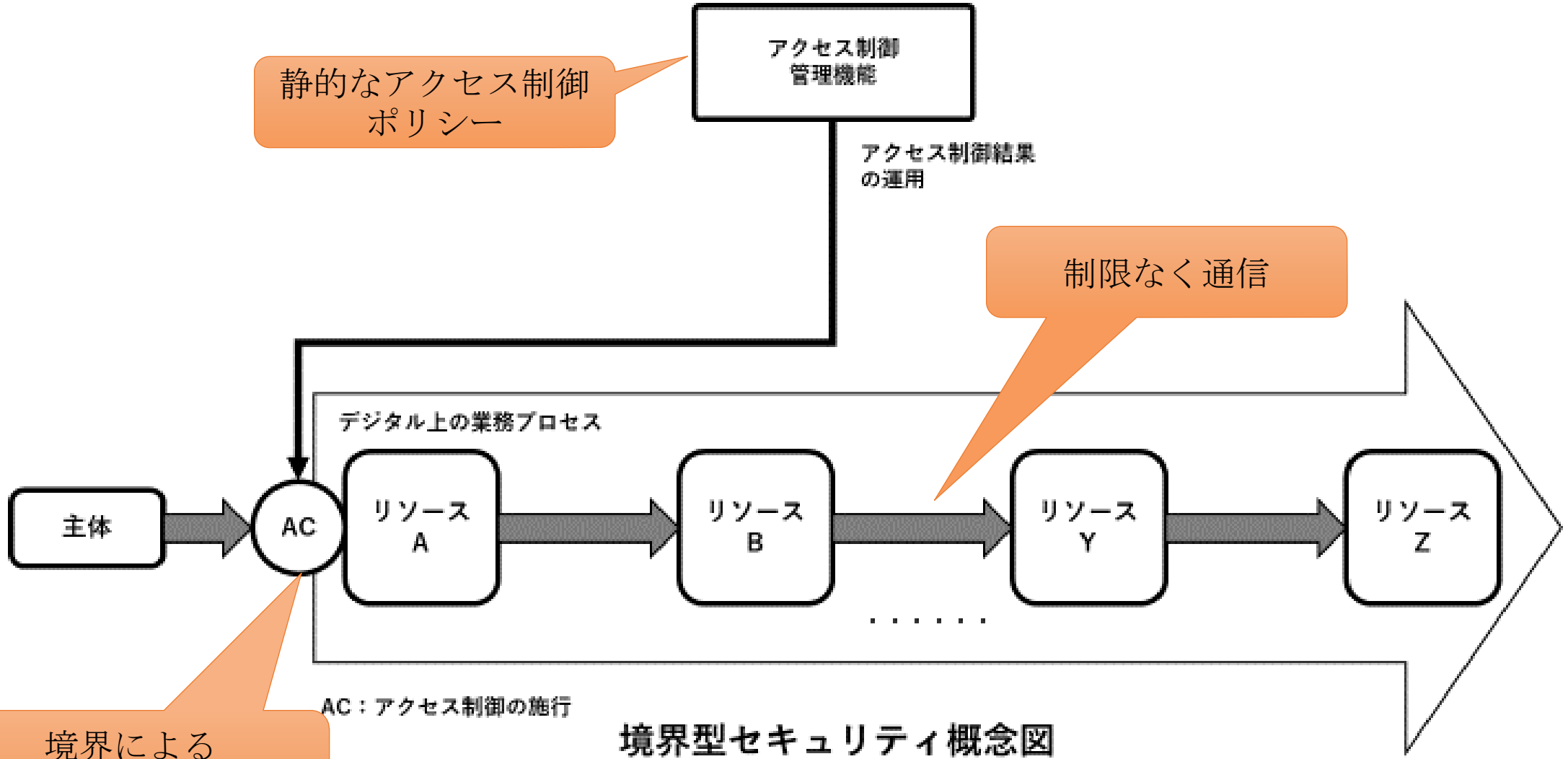






ゼロトラストアーキテクチャへの取組

従来の境界型セキュリティの概念



境界型セキュリティ概念図

ゼロトラストアーキテクチャ

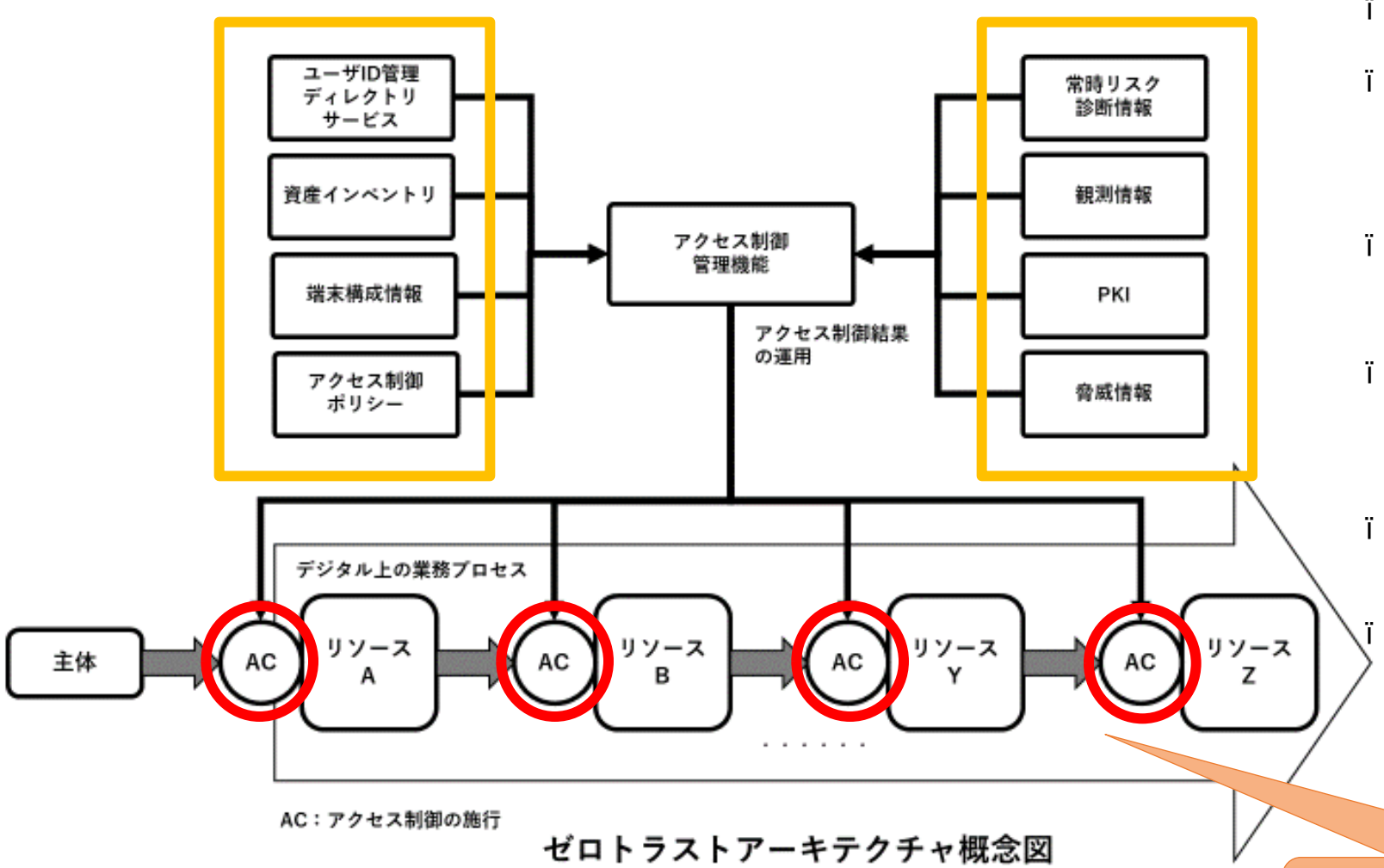
- ネットワーク上には、外部/内部を問わず脅威が存在するといった前提に立ち、ユーザー、デバイスなど個々のID（Digital Identity）に焦点を当て、「都度必要なアクションに対して必要なレベルの認証を行い、問題なければ適切なアクセス権を認可する」といった検証を厳密に行うことで、セキュリティを担保し、且つ柔軟なUser Experienceを実現するといった概念
- ゼロトラストアーキテクチャはセキュリティの概念モデルであり、ソリューションではない

（参考）政府機関等の対策基準策定のためのガイドライン（令和３年度版）

- 常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等と呼称される。）

ゼロトラストアーキテクチャ適用方針

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



ゼロトラストアーキテクチャ概念図

- 1) リソースを識別し、特定できる状態にする
  - アカウント、デバイス、サービス、データ
- 2) 主体の身元確認・当人認証を実施する
  - 「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」
  - ア　身元確認
  - イ　当人認証
- 3) ネットワークを保護する
  - 「電子政府推奨暗号リスト」や「TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～」
- 4) リソースの状態を確認する
  - ユーザの属性情報、当人認証に利用した認証要素、デバイスの OS やミドルウェアのバージョン、デバイスの構成情報、サービスへの入力値、アクセス時の位置情報
- 5) アクセス制御ポリシーで評価し、アクセス管理をする
  - 属性情報アクセスコントロール
- 6) リソースとアクセスを観測する
  - リソースとアクセスのログの取得、アラートの通知などの観測

常時アクセス判断をしているので、自由な構成が可能

境界型セキュリティからゼロトラストアーキテクチャへの変容により変わる点

- 多様な業務環境への適用
  - クラウド・バイ・デフォルト原則を前提にした環境であっても、既存のオンプレミスな境界型セキュリティな環境であっても、適用できる考え方になる。
- 複数の異なる情報を使ったアクセス制御
  - リソース間同士のアクセス制御に細分化したことにより、ディレクトリサービスなどのネットワークパケット以外の情報を使ったアクセス制御が可能になる。
  - ネットワークベースの境界型セキュリティを追加のアクセス制御として扱える。
- 観測情報の入手の拡大
  - 業務フローをリソースごとに区切り、それぞれにアクセス制御を施行するため、詳細かつ広範囲な観測データが入手できるようになる。
- 連携する外部システムの拡大
  - 脅威情報やPKIなど外部システムの属性情報と、アクセス制御管理機能が連携し情報の交換を想定している。
- アクセス制御機能における評価と施行を分離
  - アクセス制御におけるポリシーとの評価とアクセスへの施行を分離することで、柔軟な設計が可能となる。

適用における留意事項

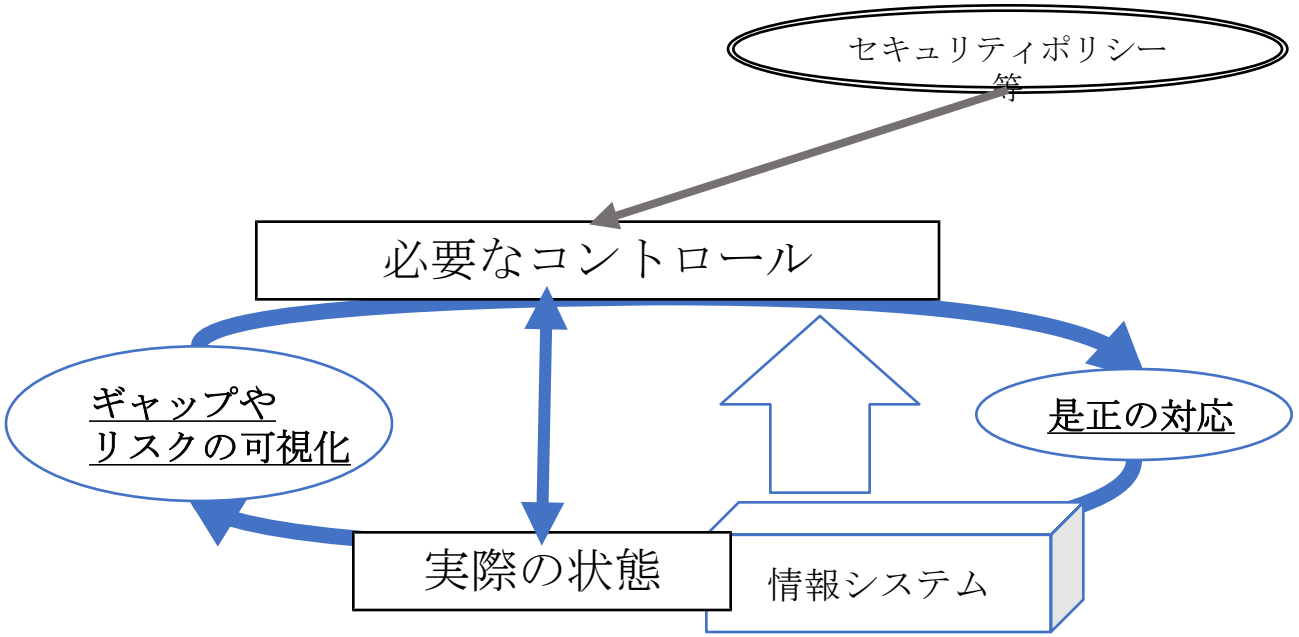
- 1) 運用・保守体制を確保する
- 2) 運用の設計と実装を初期段階から想定した適用プロセスを進める
- 3) アクセス制御の評価タイミングをアクセス要求時に限定しない
- 4) 技術標準による相互互換性を確保する
- 5) 利用者の問い合わせ対応を強化する

常時リスク診断・対処（CRSA）

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

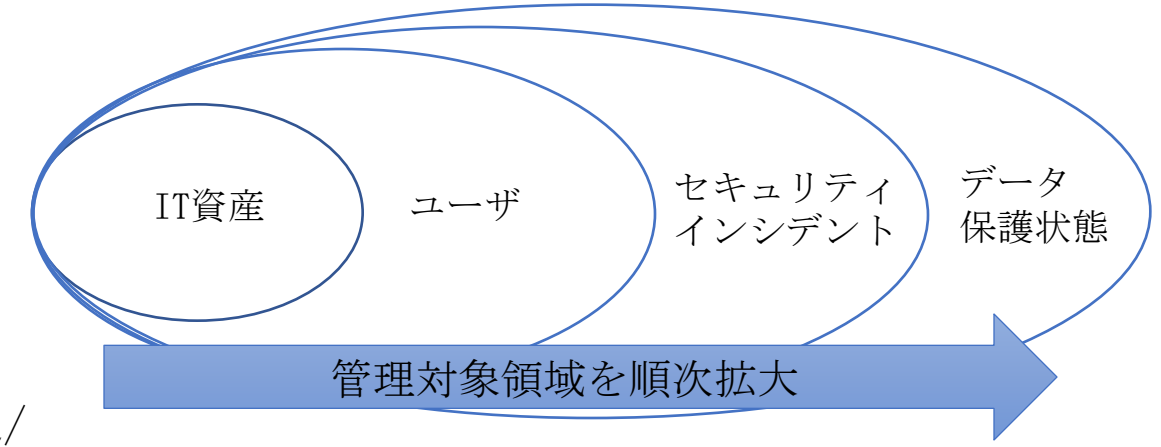
1常時リスク診断・対処

- 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



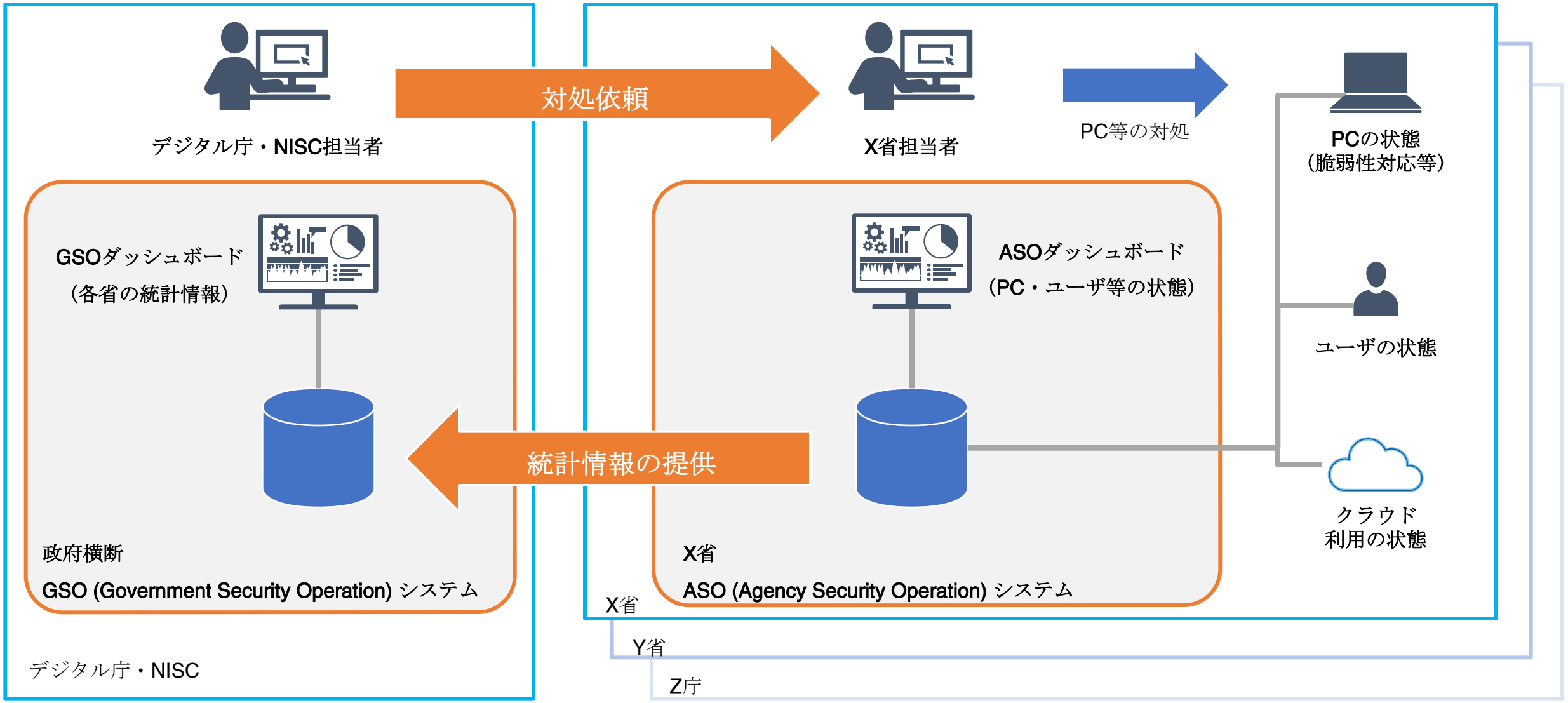
1管理対象

- 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。



https://www.digital.go.jp/policies/security/crsa/

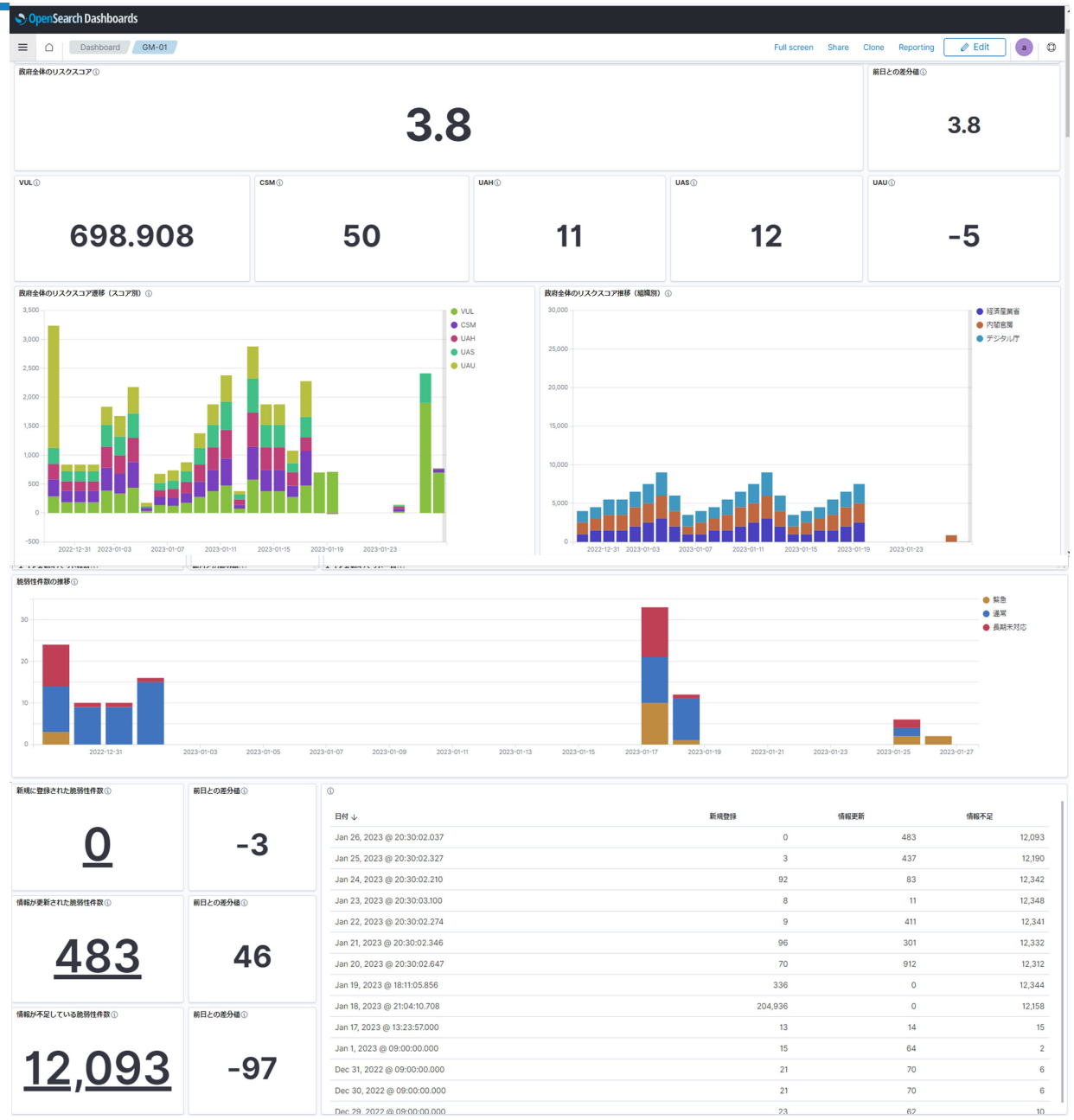
常時リスク診断・対処（CRSA）のシステム構成概要



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

対象領域 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

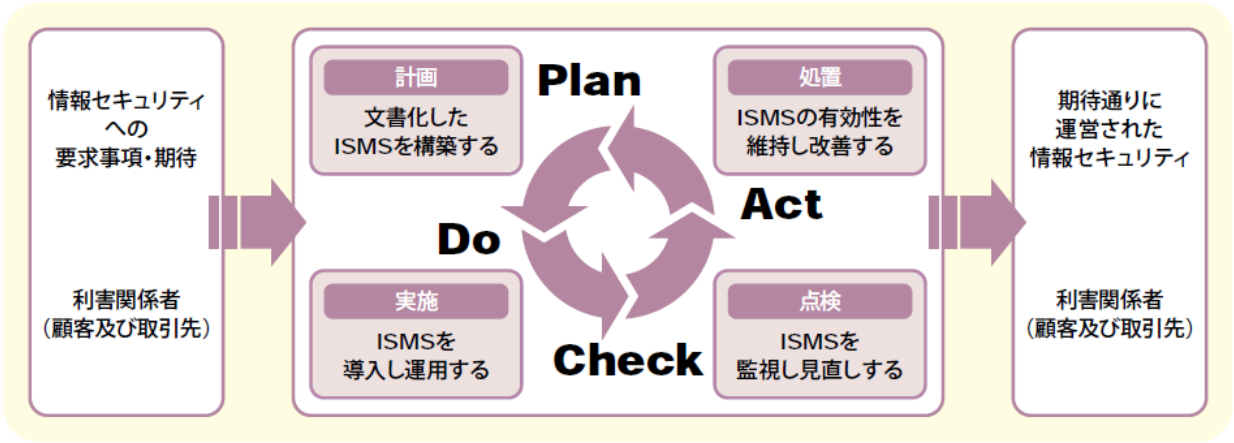


セキュリティ統制のカタログ化

従来の情報セキュリティマネジメント

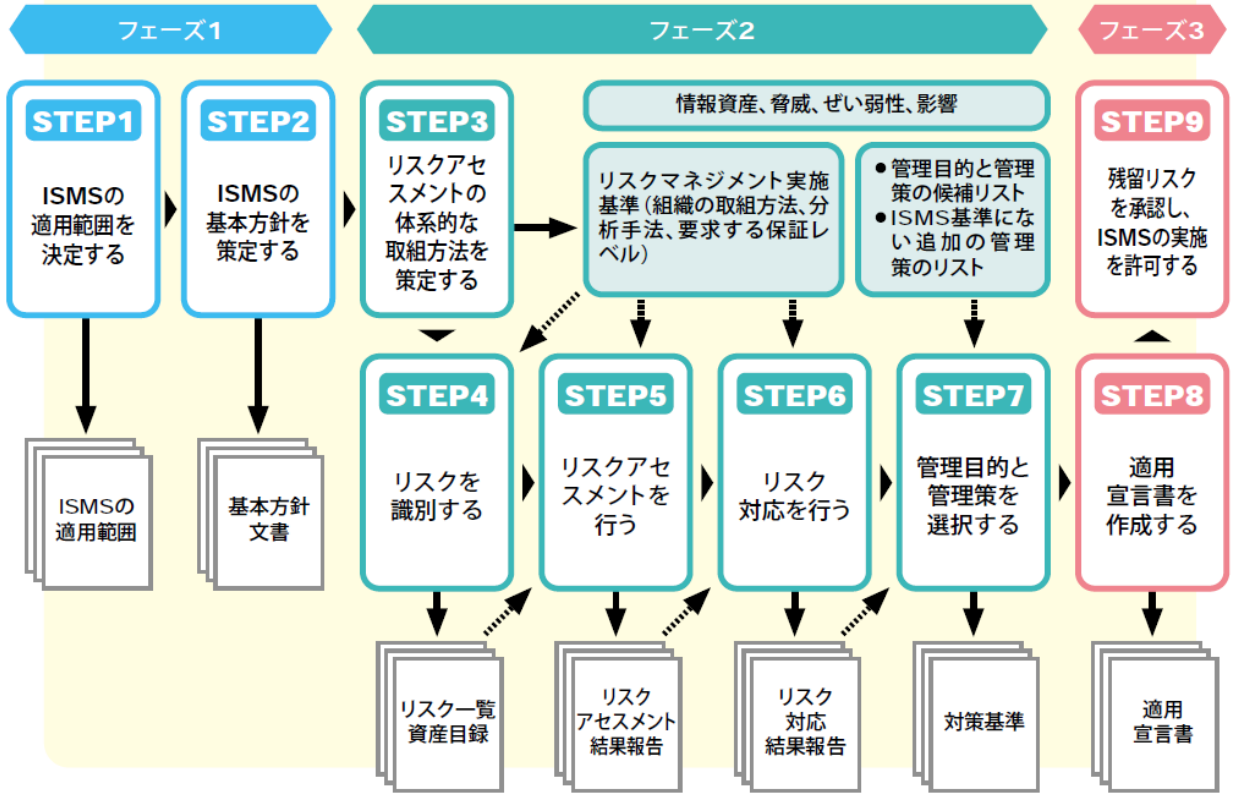
２００１年頃

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

２０２２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。

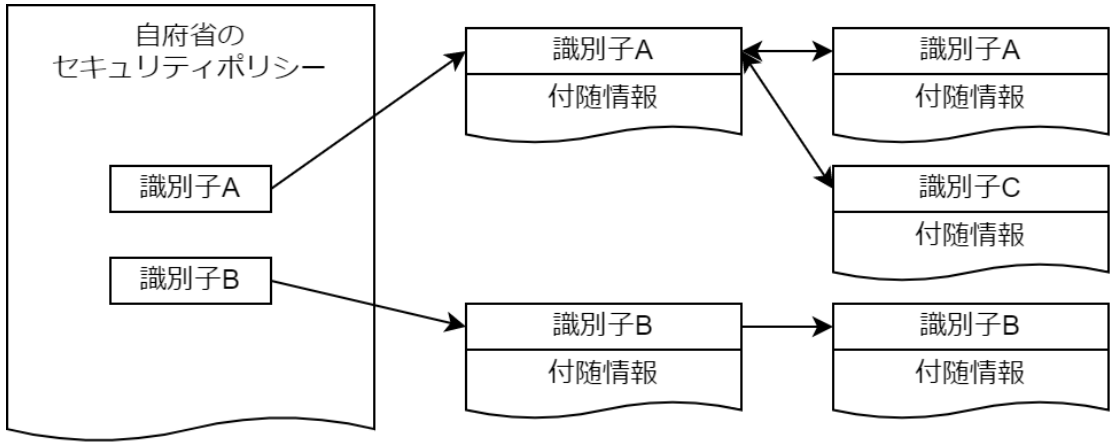
- システム開発やサービス開発は、短期間になってきている。また、システム開発もサービス開発もアジャイル的な発想になっており、プロセスは、CI/CD（継続的インテグレーション/継続的デリバリー）になっている

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について

- 例１：ISMAP管理基準
  - ISMAP管理基準において、クラウドサービス事業者が、リスクに対応するために達成するべき統制目標を、管理基準のうち（X.X.X）という３桁の番号で表現している。

8.1.1	情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。
8.1.2	目録の中で維持される資産は、管理する。
8.1.3	情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。
8.1.4	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。
8.1.5 P	クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。

- 例２：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

複雑なセキュリティを管理

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。

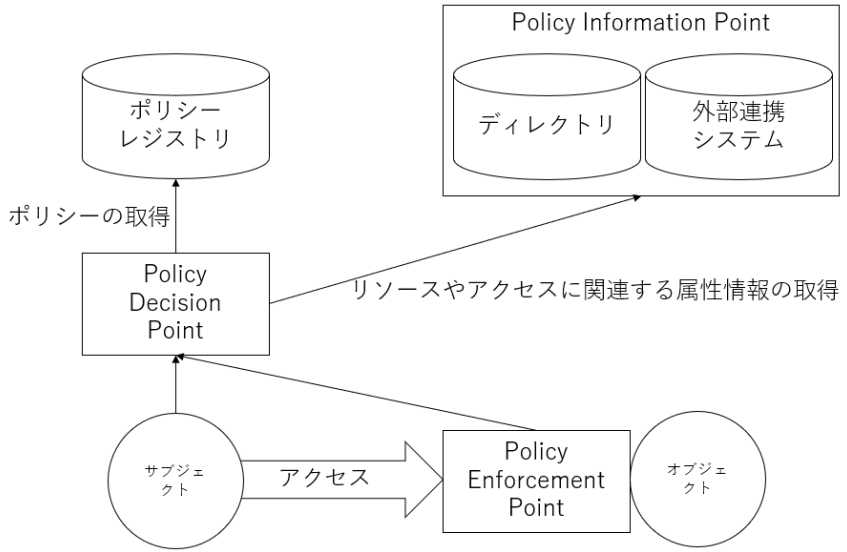
Attribute Based Access Control (ABAC)

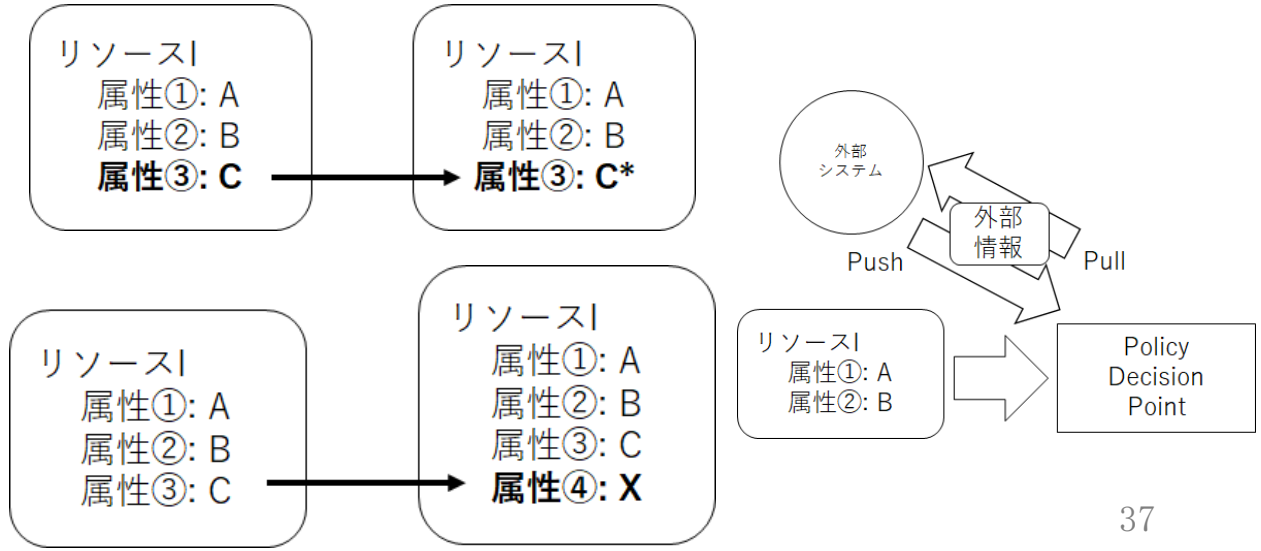
アクセス制御とAttribute Based Access Control（ABAC）の概要

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。

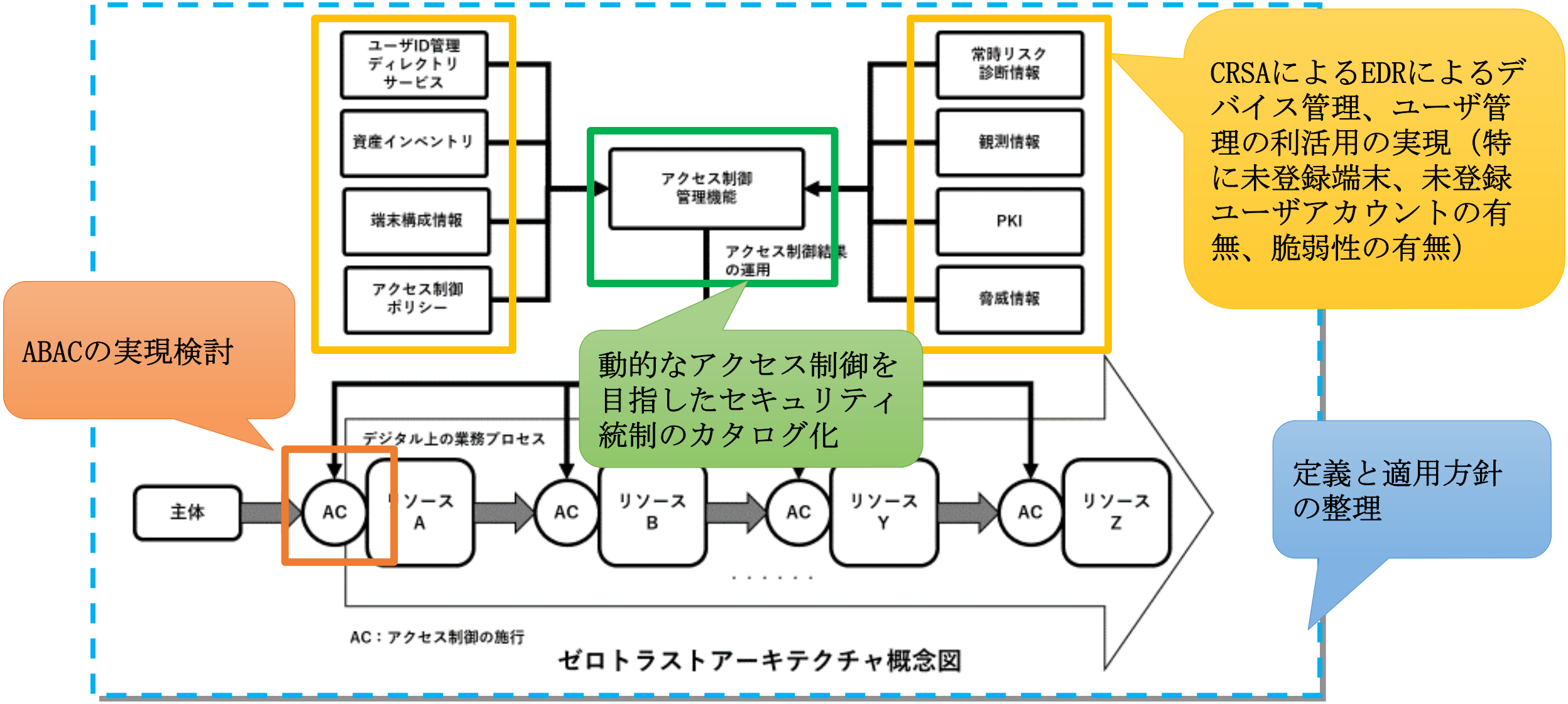
ISO/IEC 29146:2016 A framework for access management
SP 800-162, ABAC Definition and Considerations

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。



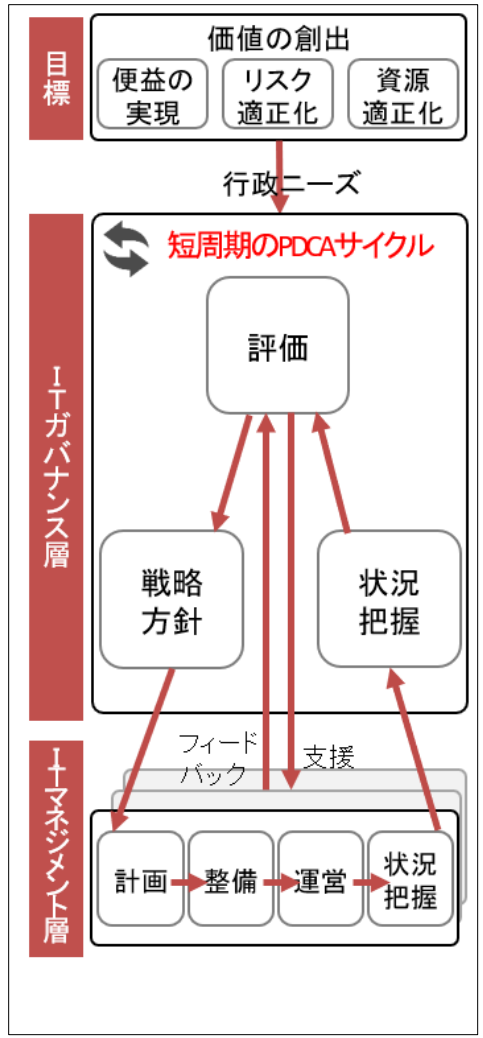


ゼロトラストアーキテクチャと施策の関係性


ユーザID管理
ディレクトリ
サービス
資産インベントリ
端末構成情報
アクセス制御
ポリシー
アクセス制御
管理機能
アクセス制御結果
の運用
常時リスク
診断情報
観測情報
PKI
脅威情報
CRSAによるEDRによるデバイス管理、ユーザ管理の利活用の実現（特に未登録端末、未登録ユーザアカウントの有無、脆弱性の有無）
ABACの実現検討
動的なアクセス制御を目指したセキュリティ統制のカタログ化
定義と適用方針の整理
デジタル上の業務プロセス
主体
AC
リソース
A
AC
リソース
B
AC
リソース
Y
AC
リソース
Z
AC：アクセス制御の施行
ゼロトラストアーキテクチャ概念図

（改めて）ゼロトラストアーキテクチャとは何か

- 高度標的型攻撃を想定したアーキテクチャ
- アーキテクチャの変革
  - 境界型セキュリティ概念からの拡張
    - ゼロトラストアーキテクチャは、境界型セキュリティ概念を包含
    - 境界型セキュリティに戻ることはない。
- System of System
  - セキュリティ管理策のライフサイクルの自動管理
    - セキュリティ統制のカタログ化、ABAC
    - cf.オーケストレーションシステム
- ITガバナンスの実装
  - ITマネジメントのコントロール



デジタル庁