セキュリティに関連する標準ガイドラインの策定について

令和5年3月24日
セキュリティ危機管理チーム

デジタル庁

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

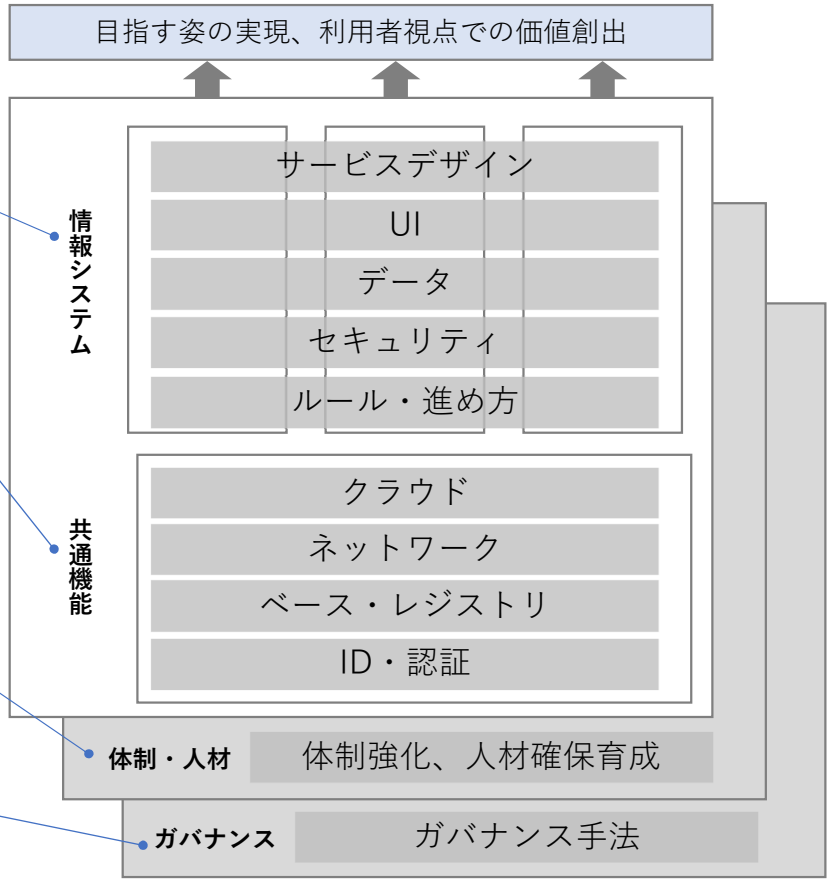
関係者が個々に努力するだけでは、目指す姿を実現できない。デジタル庁自身が特に４つの領域に注力し、旧来の課題を解消するとともに、**国・地方公共団体・独立行政法人・準公共分野等の関係者が効果的に協働**できるようにする。

1 良いサービスを作るための **標準** の策定・推進

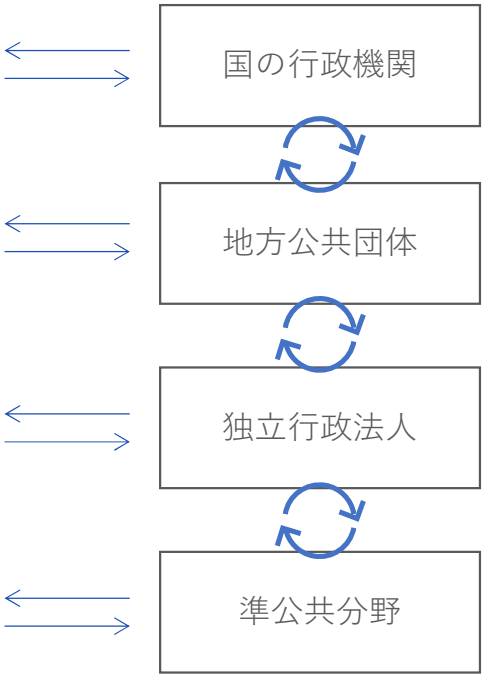
2 良いサービスを支える **共通機能** の整備・展開

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

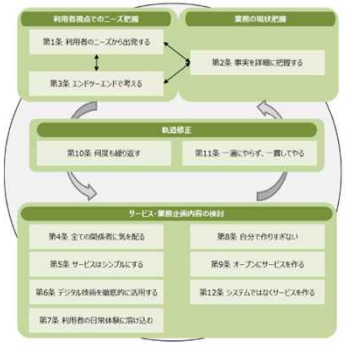
利用者視点で良いサービスを作るために、各情報システムを横断して統一すべき技術標準や進め方等について、デジタル庁自身が各プロジェクトで実践を行いながら、技術検討会議を中心に成果をまとめ、継続的改善を行う。

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

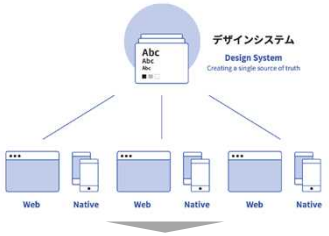


今までも標準ガイドライン等で周知展開を図っていた。デジタル庁自身が各プロジェクトで率先して**推進を徹底**する。

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。

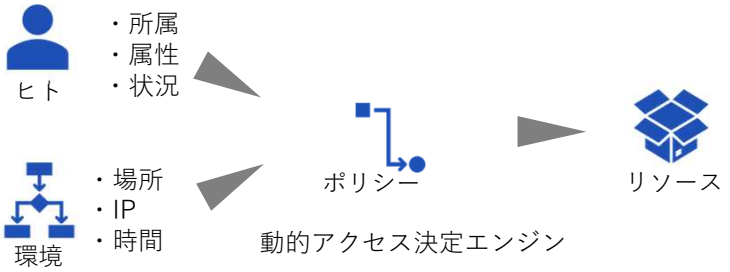
情報システムの企画、予算、調達、設計開発、運用等の実務について規定する**標準ガイドライン等**について、現場のプロジェクトを円滑に推進する観点から継続的改定を行う。

※ 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

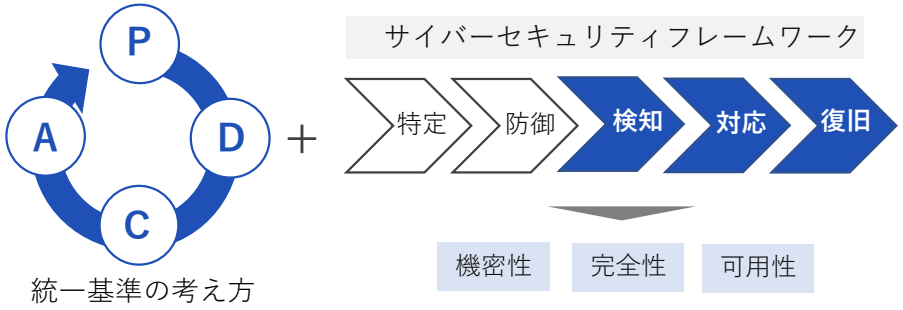
共通機能を前提とした 常時診断・対応型のセキュリティアーキテクチャ実装推進

- 「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。



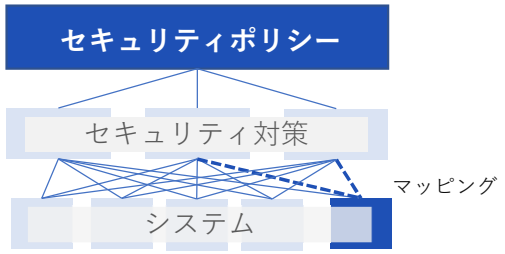
サイバーレジリエンスの強化

- 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。



策定予定のガイドライン/技術レポート（セキュリティ）

【参考：前回分】セキュリティ関連技術ガイドライン群と各ドキュメントにおける概要

統一基準で示されるセキュリティ対策に係る基本的な考え方と実践のポイントをふまえ、下記の4テーマについて統一基準群を具体化した技術ガイダンスを作成。まずはデジタル庁を適用範囲とする。6月末に策定。なお、将来的には各府省庁への適用する方向で改訂することを視野にいれている。

統一基準群

informative

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**クラウドサービスの利用**や**業務環境の変化**が進んでいる。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、サイバーセキュリティ要件を満たすには、パラダイムシフトが求められる。本文書は**ゼロトラスト・アーキテクチャというパラダイムシフトの適用方針**に関する原則を説明する。

informative

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。本文書は、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している。

informative

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て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。本文書では**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。併せてセキュリティバイデザインの実用性確保するための**関係者の役割**を定義する。

informa

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、これまでにも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ているが、導入方法に明確な基準や指針があるとは言えない。**本取り組みでは、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ガイダンスを提供する。

セキュリティ関連技術ガイドライン群と各ドキュメントにおける概要

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に則り、４つの文書に加え、下記4つの文書を追加策定。

統一基準群

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～

informative

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の事例**として具体的に示したものである。

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

informative

概要

クラウド・バイ・デフォルト原則に従い、今後多くの業務がクラウドサービスを通じて処理される中、従来の業務処理環境においても**堅牢性を維持・向上するには、「ゼロトラストアーキテクチャ」の考え方を組み込むことが重要**になる。本文書ではアクセス制御モデルの１つであり、リソースに付与された属性や環境の情報等を活用した**属性ベースアクセス制御に関する俯瞰的な技術的内容**を記載する。

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

informative

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。

DS-231

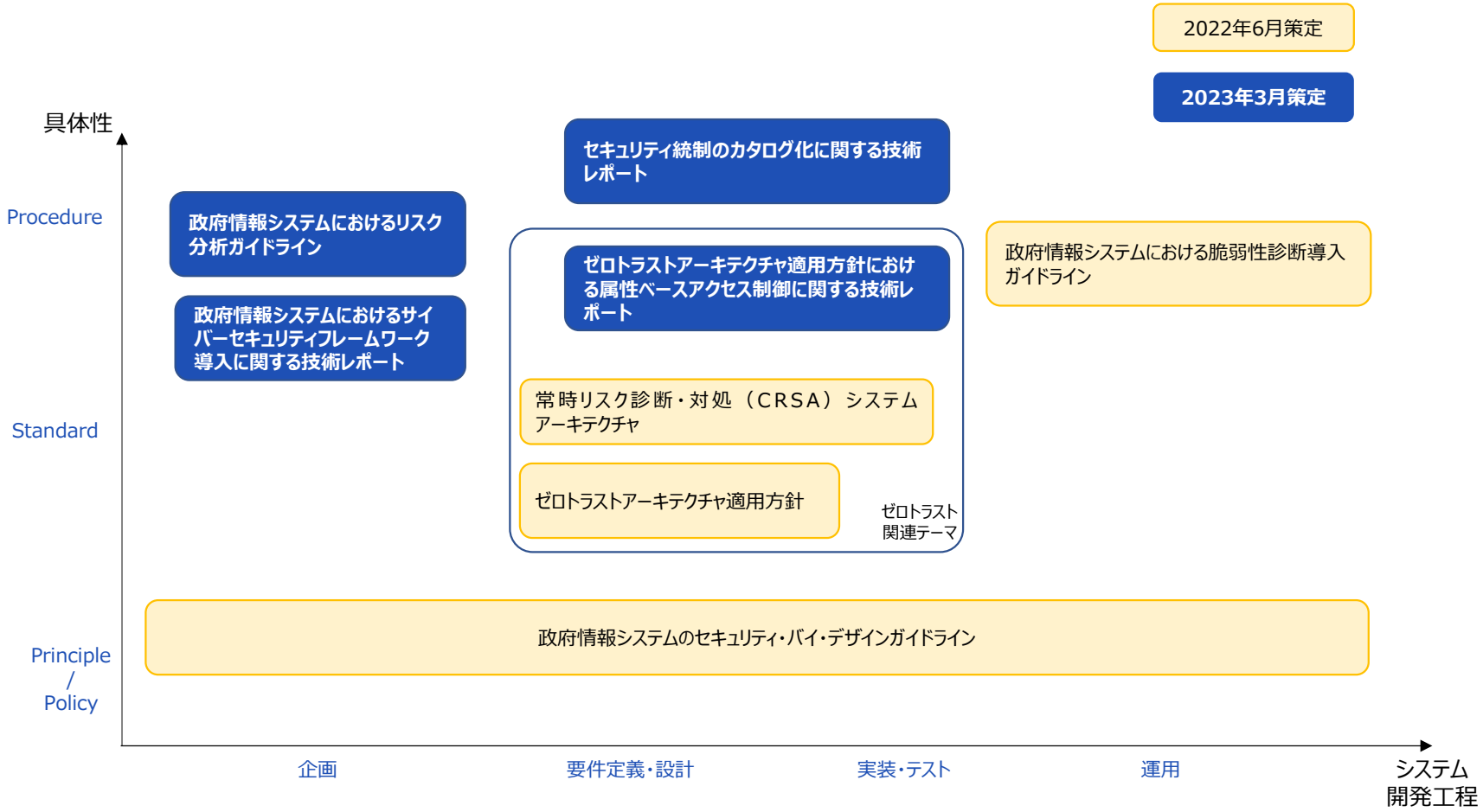
セキュリティ統制のカタログ化に関する技術レポート

informa

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。

セキュリティ技術ガイドライン全体の構造整理



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　～

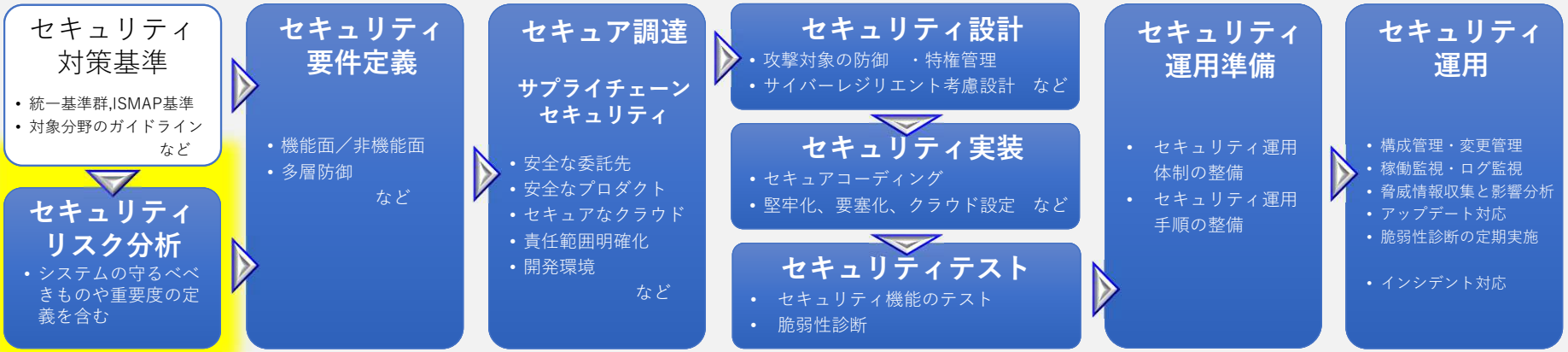
デジタル庁

なぜ、必要か。

- 「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(2022年6月デジタル庁発行）」より

政府情報システムにおいて、セキュリティ対策を確実かつ効率的に実装するためには システム開発の上流工程から取り組むことが重要

セキュリティ・バイ・デザインの最初のプロセスは、セキュリティリスク分析となる。



本レポートの目的

- セキュリティ・バイ・デザインでのセキュリティリスク分析について　具体的な手順の事例を示す。

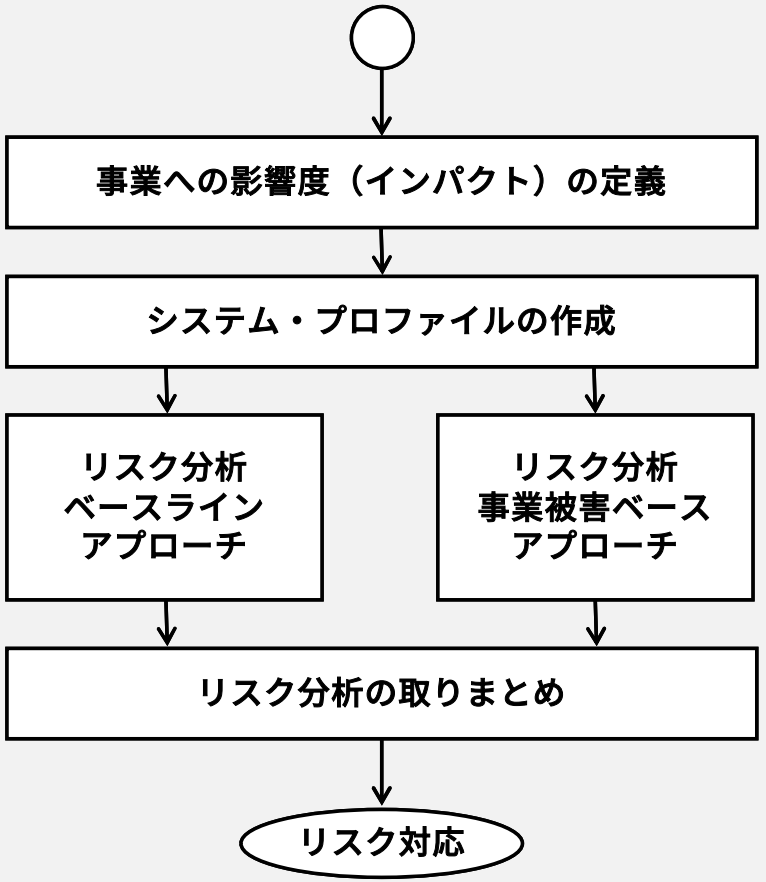
本ガイドラインで採用するリスク分析

◆ セキュリティリスク分析の根拠に十分な
- **事業への影響度**
- **システム・プロファイル**

を作成

◆ セキュリティリスク分析は、
- **ベースラインからのアプローチ**
- **事業被害ベースからのアプローチ**

の組み合わせ方式を採用



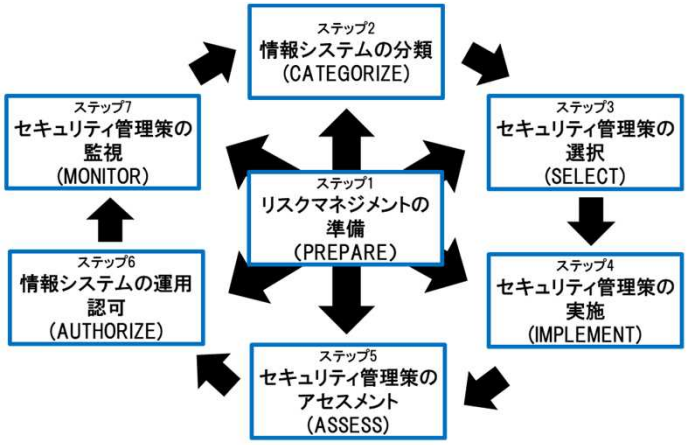
ベースラインからのアプローチ

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

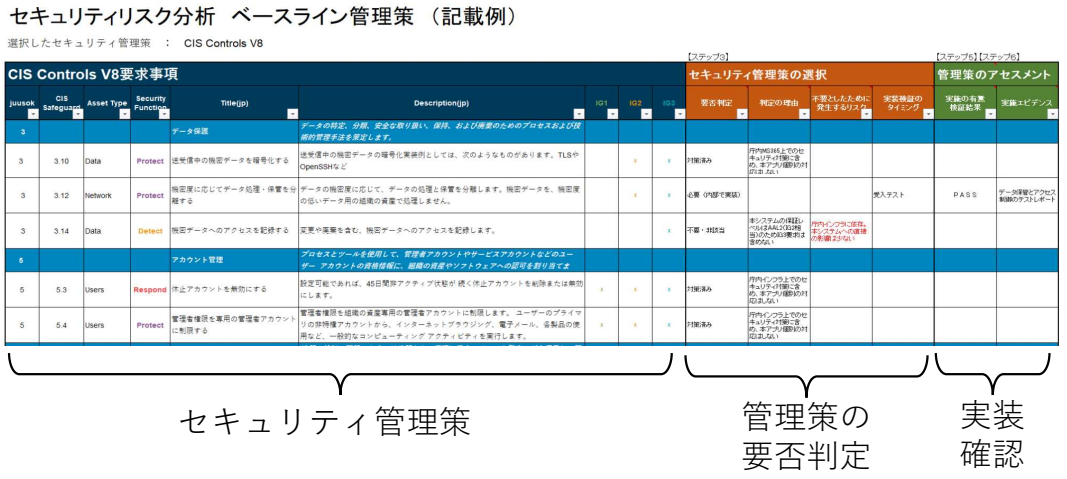
「Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy」
（情報システムおよび組織のためのリスクマネジメントフレームワーク　－セキュリティとプライバシーのためのシステムライフサイクルアプローチ）

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

事業被害ベースからのアプローチ

事業への影響度を分析したときの
最も大きな事業被害（最悪シナリオ）についてリスク分析する。

【ステップ１】事業被害の洗い出し
【ステップ２】脅威の特定
【ステップ３】攻撃シナリオの分析
【ステップ４】リスク値の算定
【ステップ５】リスクへの対策

【判定】分析結果の対策がベースラインの
管理策に含まれているかを確認する。
管理策に含まれていない場合は、
セキュリティ要件に追加する。

事業被害ベースのリスク分析のイメージ

目次

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

デジタル庁

なぜ、必要か。

- **2022/06に公開された「ゼロトラストアーキテクチャ適用方針」（以降、適用方針）は、業務プロセスにおける各リソース間のアクセス制御をセキュリティの核としているが、クラウド・バイ・デフォルト環境における業務を前提としたアクセス制御に関する技術文書・ガイド・レポートが少ない**
- **新しい業務環境を整備していくことでこれらの知見不足は、要件整理やその後の実装が困難になりうる**

本レポートの目的

- 時代と働き方や脅威など、様々な変化を踏まえ、多角的なデータをもとにアクセス制御をおこなうABACに関する一般的な構成や考え方を示す
- 実装例を別添とすることで、具体的な実装方法や運用方法のイメージを想起させる

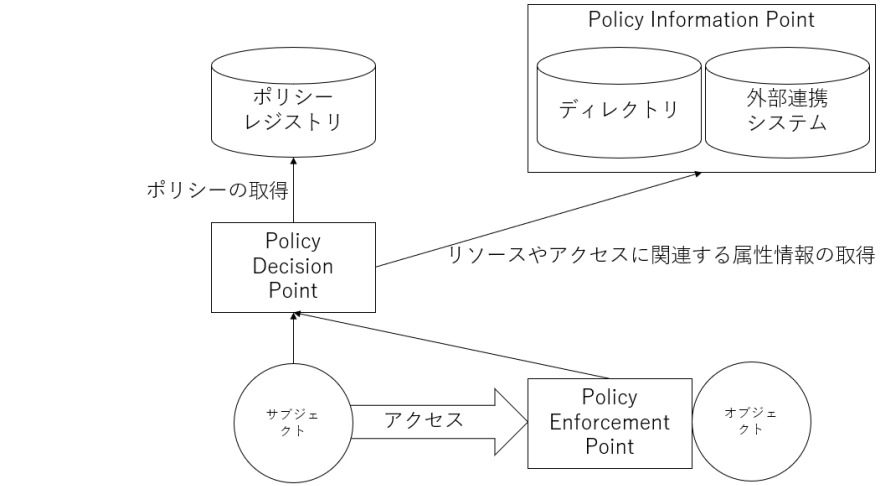
目次

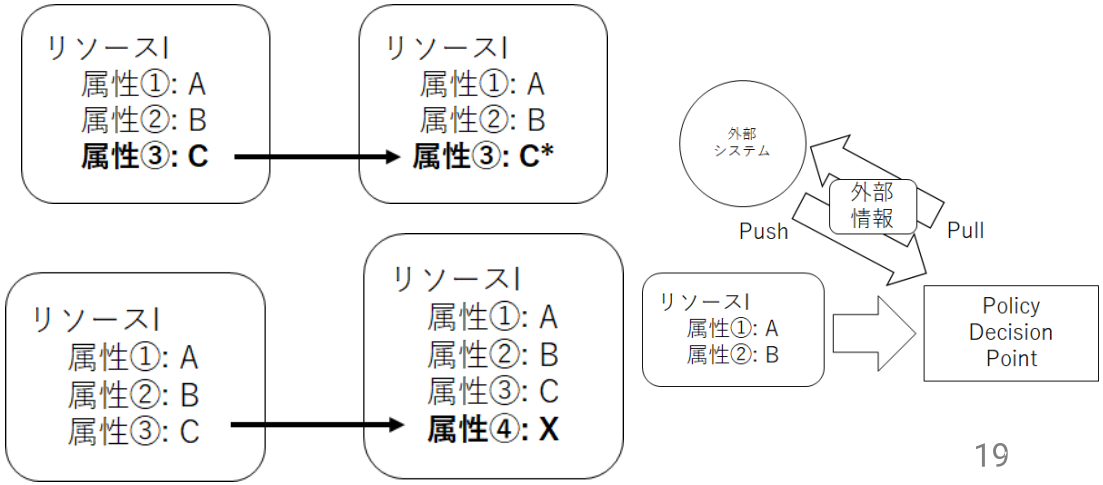
アクセス制御とAttribute Based Access Control（ABAC）の概要

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。

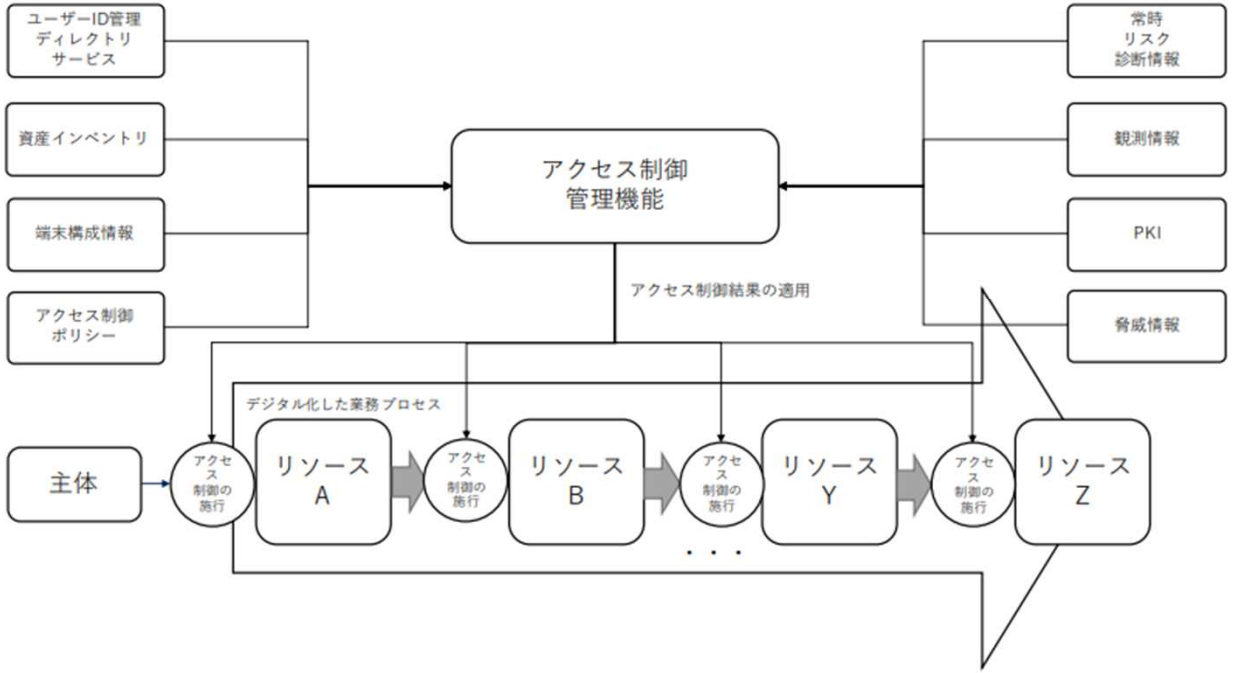




ABACとゼロトラストアーキテクチャ適用方針

アクセス制御モデルとしてABACが採用された際のメリットを、適用方針にあげた観点から提示する。

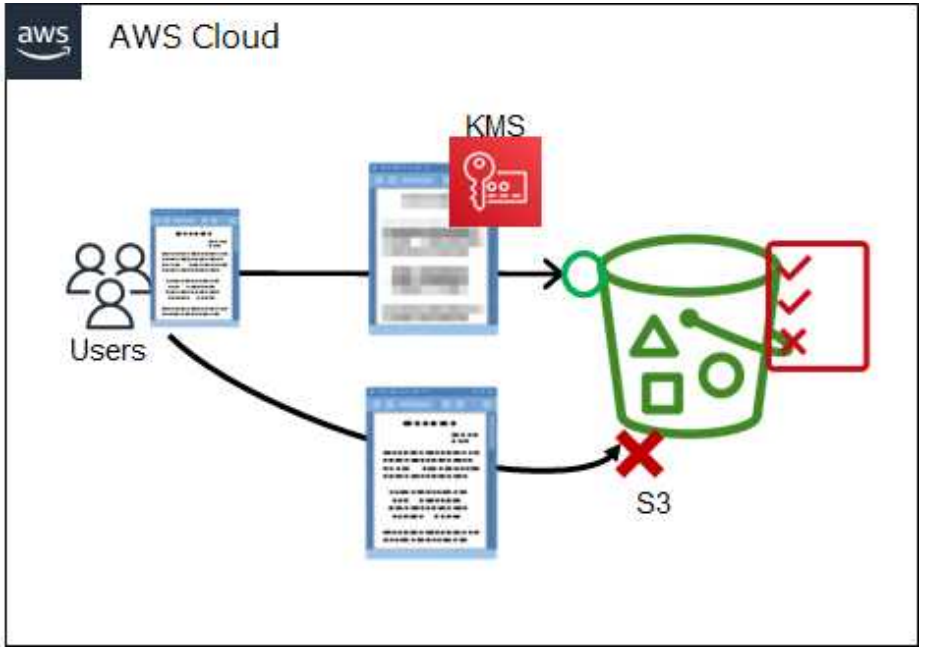
具体的には、「**リソースを識別し、特定できる状態にする**」「**主体の身元確認・当人認証を実施する**」「**ネットワークを保護する**」「**リソースの状態を確認する**」といった観点において、ABACの特性がどのように実現性・効率化・堅牢化に貢献するかについて記述する。

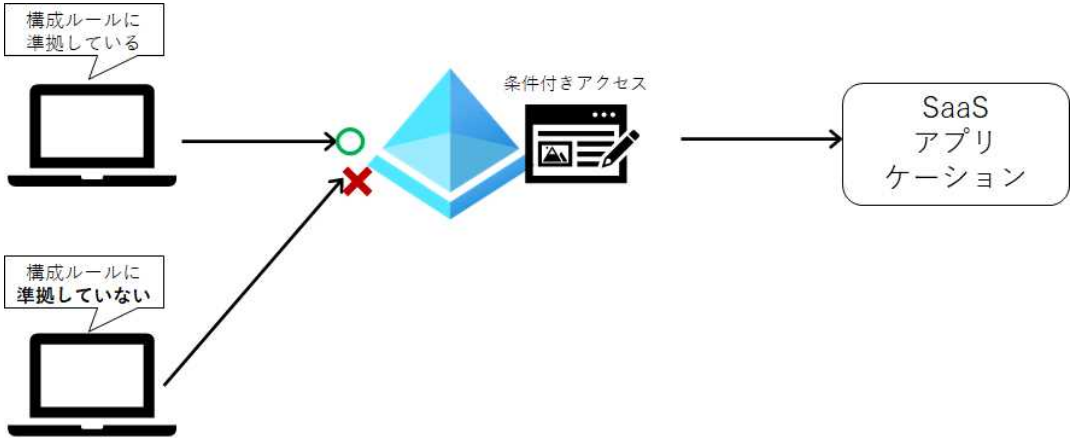


別添

ABACについて簡易な実装の紹介。
ガイドラインはToBeで最終形の話が多く、PDCAライフサイクルなどの継続的な改善を前提に参照する際には実現可能性が難しいのもある。別添では、**簡易的な実装を例示**することで、想定読者である各システム管理者・担当者は理解を深めやすくなる。

具体的には、サービス提供環境としてのIaaS（AWS）および、社内アクセス管理のためのIDaaS（AzureAD）に関する例を提示する。





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

デジタル庁

なぜ、必要か。

- サイバーレジリエンスの強化が求められており、脅威の侵入を前提とし、識別・防御に加え、検知・対応・復旧を認識し、対応していくことが重要
- 統一基準においても、サイバーレジリエンスを含め、セキュリティに係る要求事項は定められているが、サイバーセキュリティフレームワークを導入することで、セキュリティの各プロセス（特定・防御・検知・対応・復旧）の対策実施状況を評価し、可視化することが可能となる

本レポートの目的

- 組織がサイバーセキュリティフレームワークを導入・活用することでセキュリティ対策の強化や改善に資するよう、サイバーセキュリティフレームワークの概要およびそのプロセスや導入時の留意点を示す。

目次

サイバーセキュリティフレームワークの概要

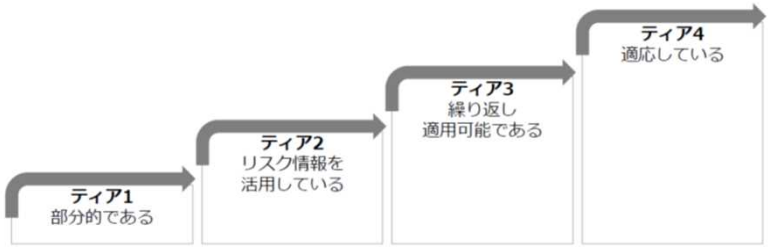
サイバーセキュリティフレームワークはレジリエンスを含む包括的なサイバーセキュリティ態勢を構築するための代表的なツールであり、サイバーセキュリティ態勢の構築に必要な機能を定義したリスクベースアプローチのフレームワーク

フレームワークコア

- 業種業態、企業規模に問わず考慮すべきサイバーセキュリティ対策を定義
- サイバーセキュリティ対策は識別、防御、検出、対応、復旧の5つの機能に分類
- 各機能の下には複数のカテゴリがあり、各カテゴリの下には複数のサブカテゴリが存在

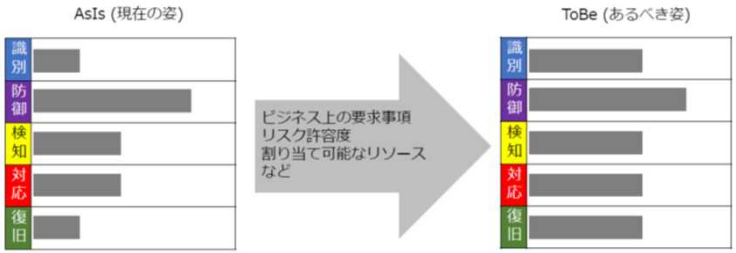
フレームワークインプリメンテーションティア

- サイバーセキュリティ対策の実施状況を評価する際の指標を定義
  - ティア1「部分的」
  - ティア2「リスク情報を活用している」
  - ティア3「繰り返し適用可能である」
  - ティア4「適用している」

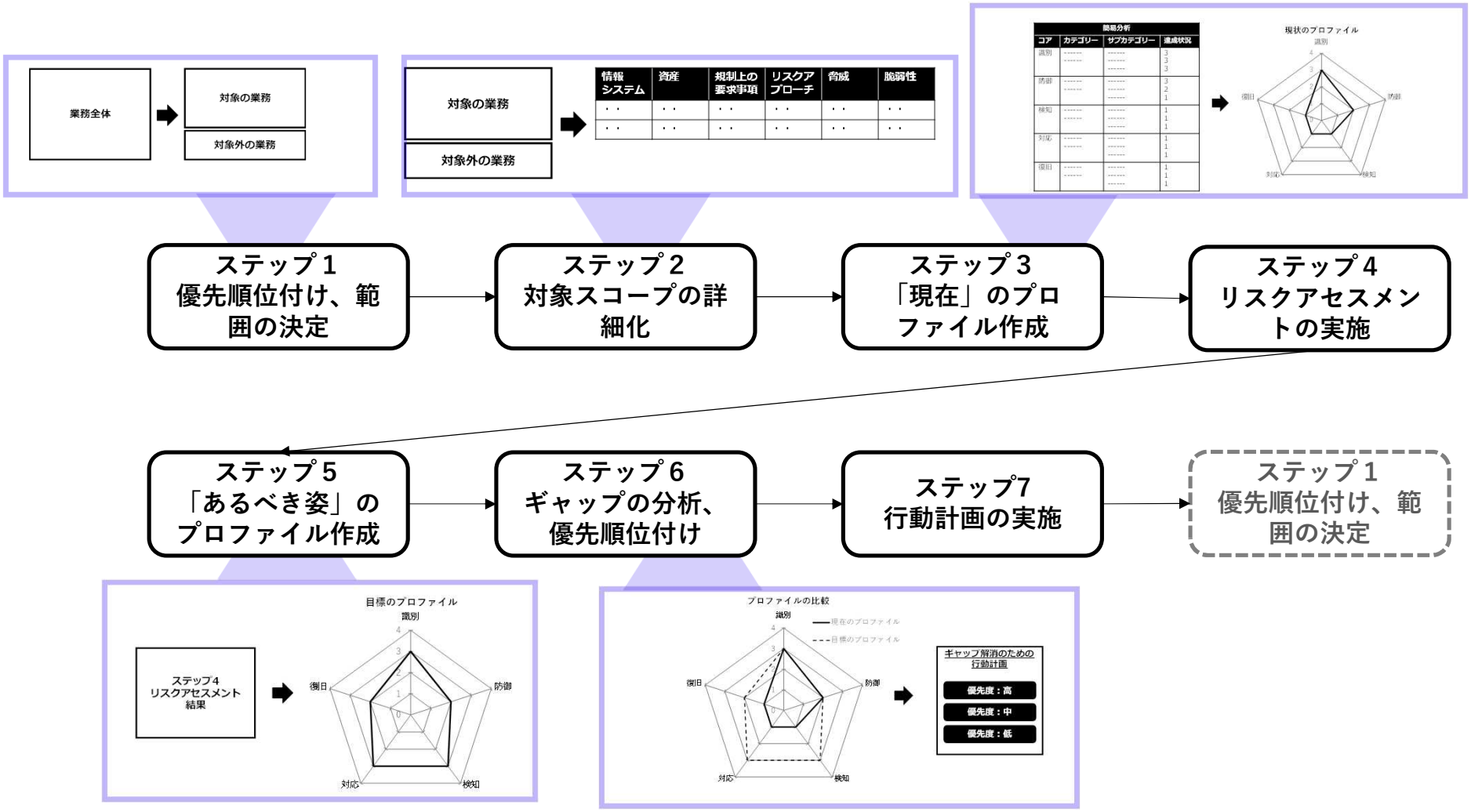


フレームワークプロファイル

- 機能・カテゴリ・サブカテゴリについて、組織毎に調整、整理されたもの
- フレームワークプロファイルを用いて「現在の姿」と「あるべき姿」を、明らかにすることで、ギャップを導き出すことが可能



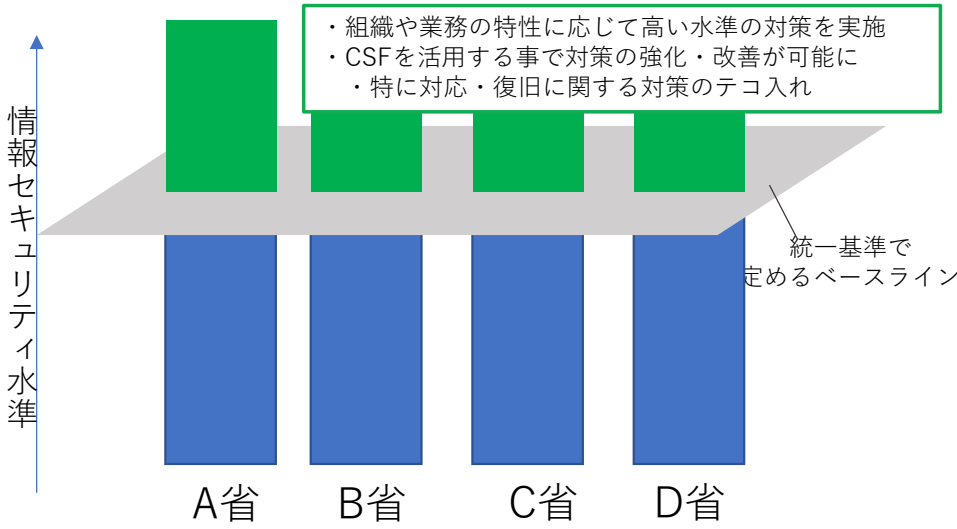
サイバーセキュリティフレームワークの導入プロセス



統一基準とサイバーセキュリティフレームワークの関係

サイバーセキュリティフレームワークは統一基準を踏まえ活用する

- 政府統一基準は政府機関等が準拠すべきセキュリティ対策の基準が規定
  - 各府省は統一基準群で定めるベースラインとして各組織の情報セキュリティ水準を確保することが可能
- 他方、政府機関が組織の特性や扱う情報に応じて、**更に高い水準のセキュリティ対策**を実施することも可能である。
- サイバーセキュリティフレームワークの利用は、リスクアセスメントに基づいたセキュリティ対策の強化・改善を可能とする
  - 「あるべき姿」と「現在の姿」の明確化とギャップ分析を行う事で、組織が実施すべき具体的なセキュリティ対策について、行動計画の策定を支援する



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

デジタル庁

なぜ、必要か。

- **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。

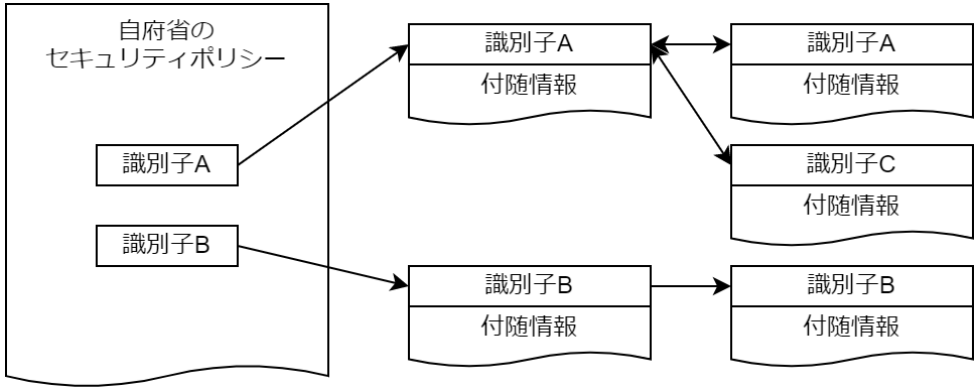
本レポートの目的

本技術レポートで示すセキュリティ統制のカタログ化を行うことで、セキュリティ統制業務の自動化促進が必要となるのではないかと考える。本技術レポートではセキュリティ統制のカタログ化に関する見通しを掲載し、今後のセキュリティ対策自動化の一助とすることを目的とする。

目次

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**

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。
8.1.5P	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
```

カタログ化、参考情報

- デジタル庁 - デジタル社会の実現に向けた重点計画（令和４年６月７日）
  https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/d130556b/20220607_policies_priority_outline_05.pdf
- 内閣サイバーセキュリティセンター - 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
  https://www.nisc.go.jp/policy/group/general/kijun.html
- ISMAP運営委員会 - 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準
  https://www.ismap.go.jp/csm
- NIST(National Institute of Standards and Technology）- SP800-53　（組織と情報システムのためのセキュリティおよびプライバシー管理策）
  https://www.ipa.go.jp/files/000092657.pdf
  https://www.ipa.go.jp/files/000092658.pdf
- NIST（National Institute of Standards and Technology） – the Open Security Controls Assessment Language (OSCAL)
  https://pages.nist.gov/OSCAL/
- NIST（National Institute of Standards and Technology） –　OSCALに関するgithubページ
  https://github.com/usnistgov/OSCAL
- ASCS (Australian Cyber Security Centre) – ISM (Information Security Manual) OSCAL
  https://www.cyber.gov.au/ism/oscal