次世代の
情報セキュリティ監査を問う

2023年10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(物理学)

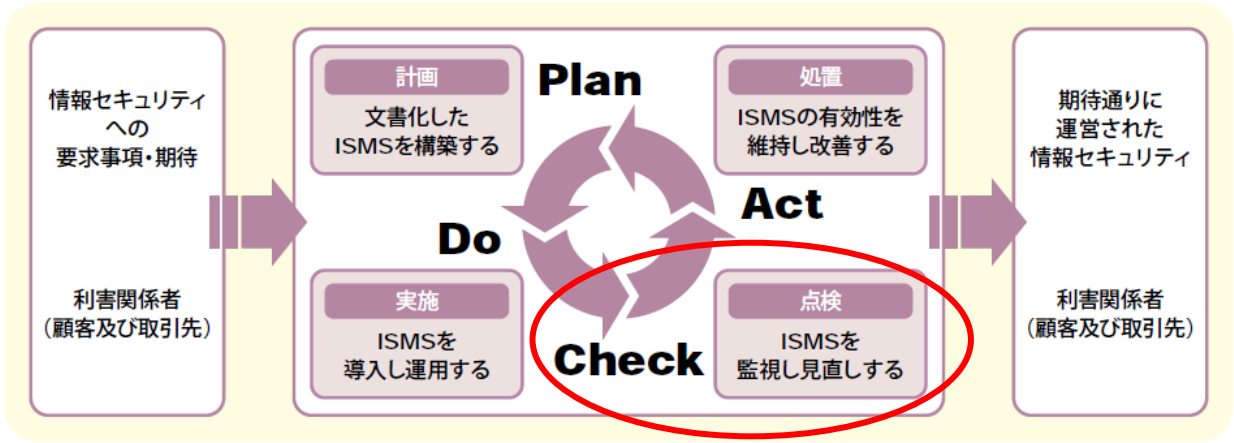
略歴

- 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。

従来の情報セキュリティマネジメント

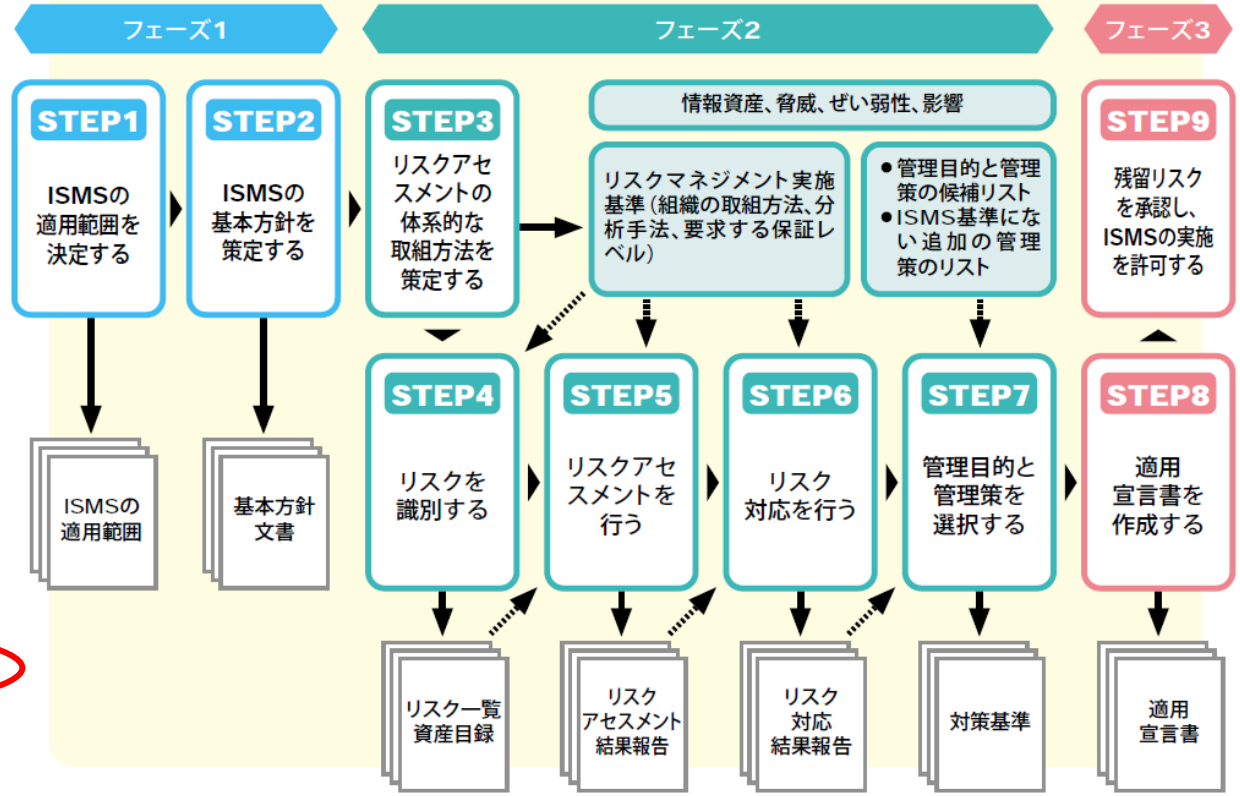
２００１年頃

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、**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

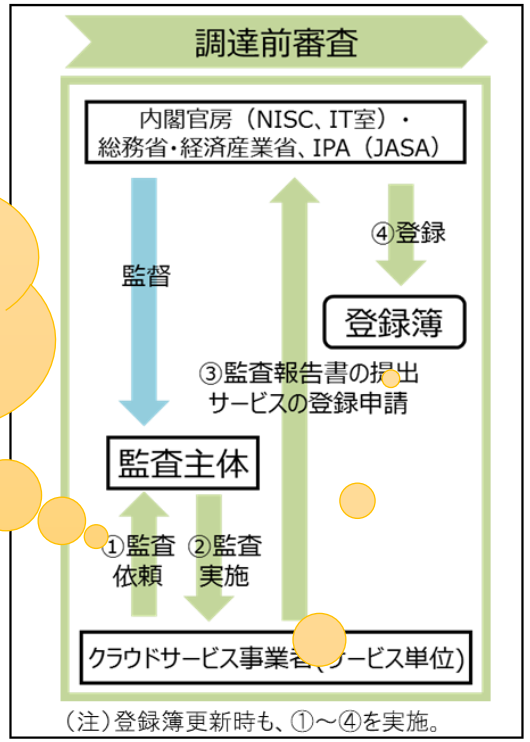
少し**複雑な管理**になると、評価、見直し等の**工数が莫大**になる。

- 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。

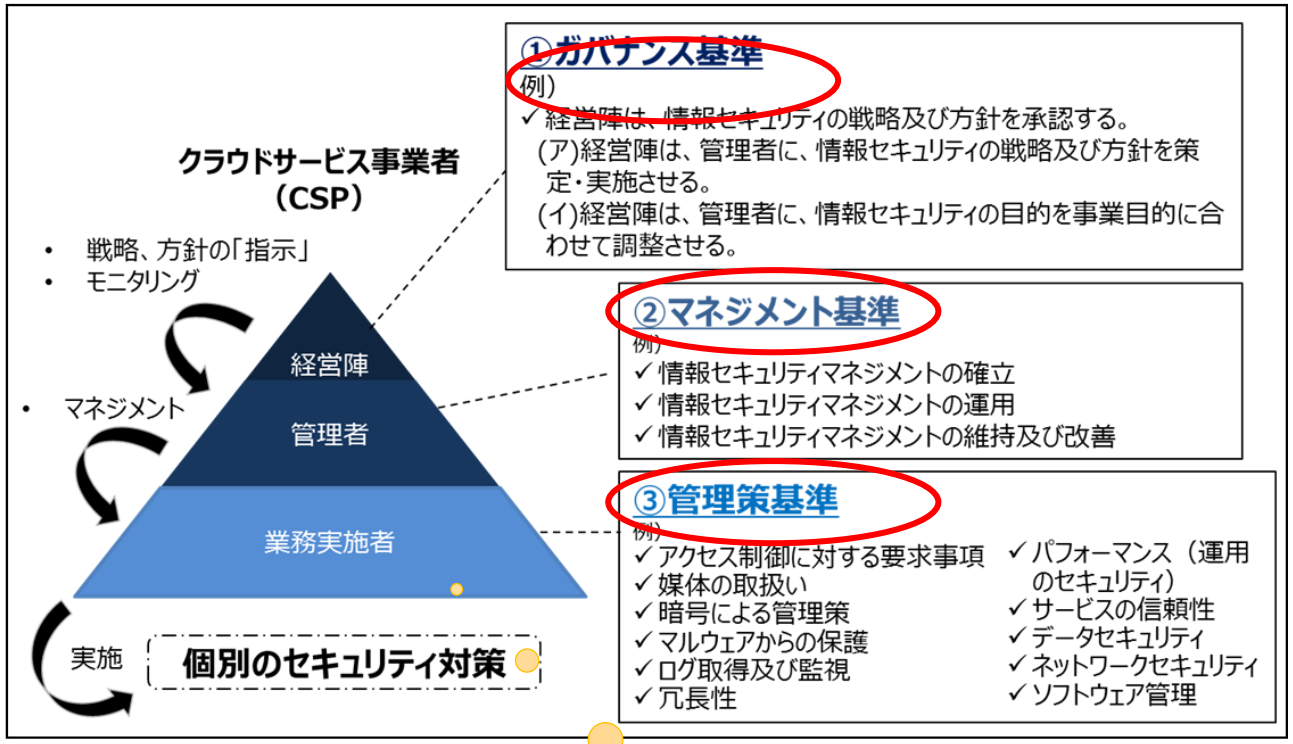
ISMAPにおける管理基準と登録の流れ

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

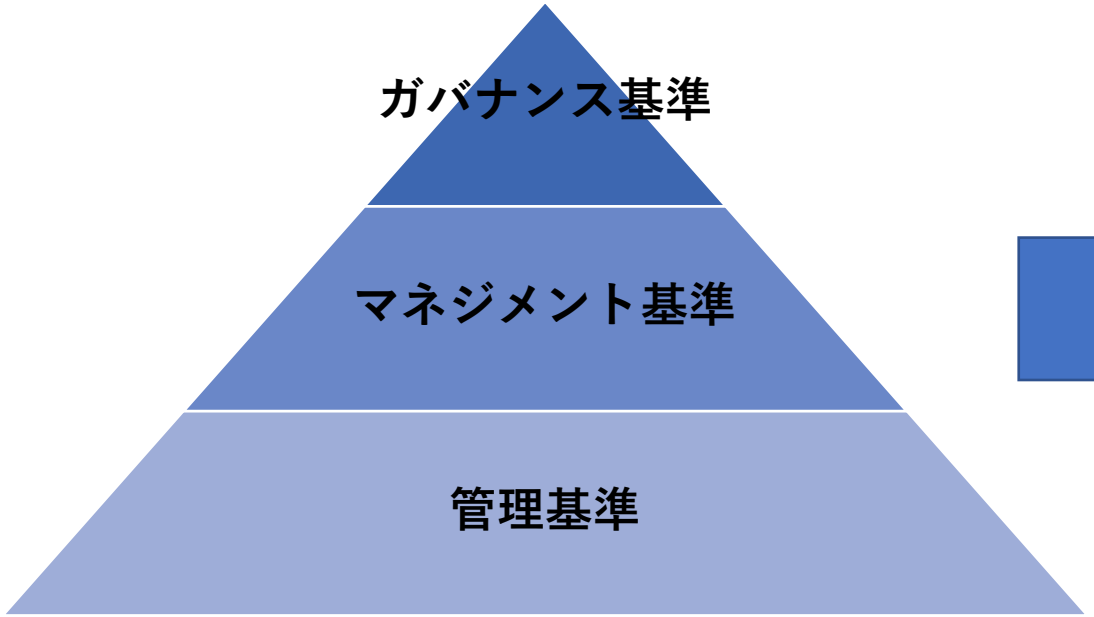


登録簿の公開による
情報開示

過去の実施状況
の確認

次世代の情報セキュリティ監査

監査手法の変革



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

監査タイミングの変革

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。

（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 AppFl		
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。

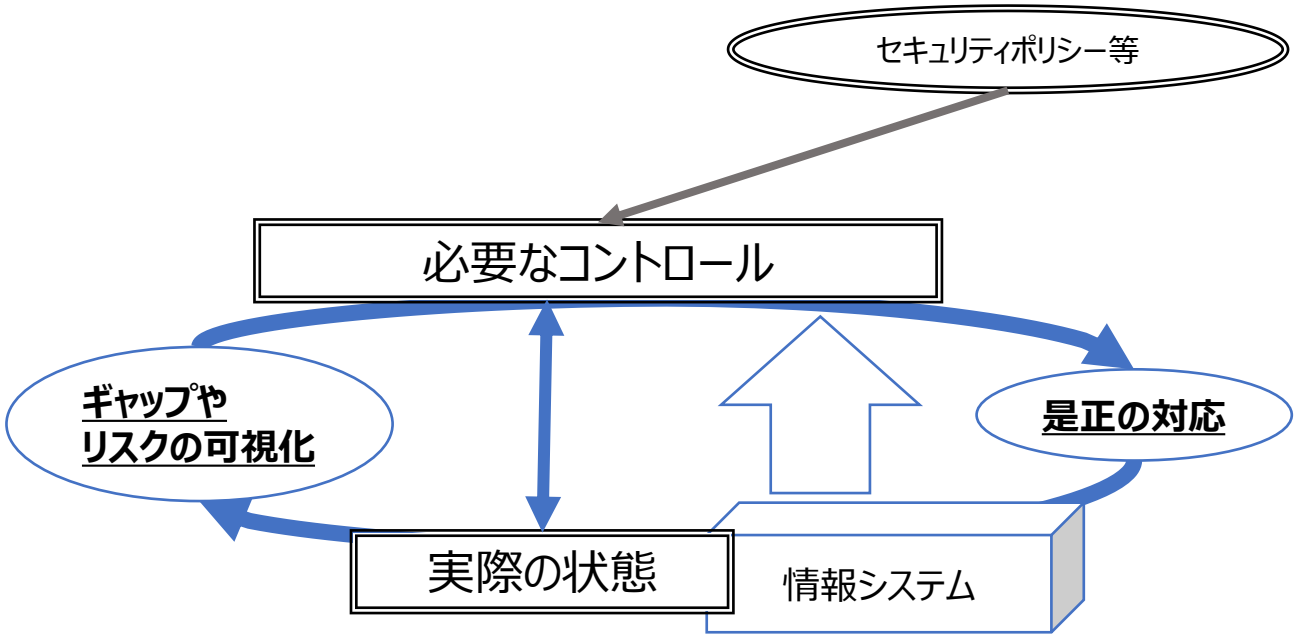
お客様がプライバシーとデータセキュリティについて懸念されるのは当然のことです。このため、AWS ではコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツをどこに保存するかをお客様に決定していただき、転送中のコンテンツと保管中のコンテンツを保護し、お客様のユーザーの AWS のサービスとリソースに対するアクセスを管理できるようにしています。また、お客様のコンテンツに対する不正アクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。

参考資料

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

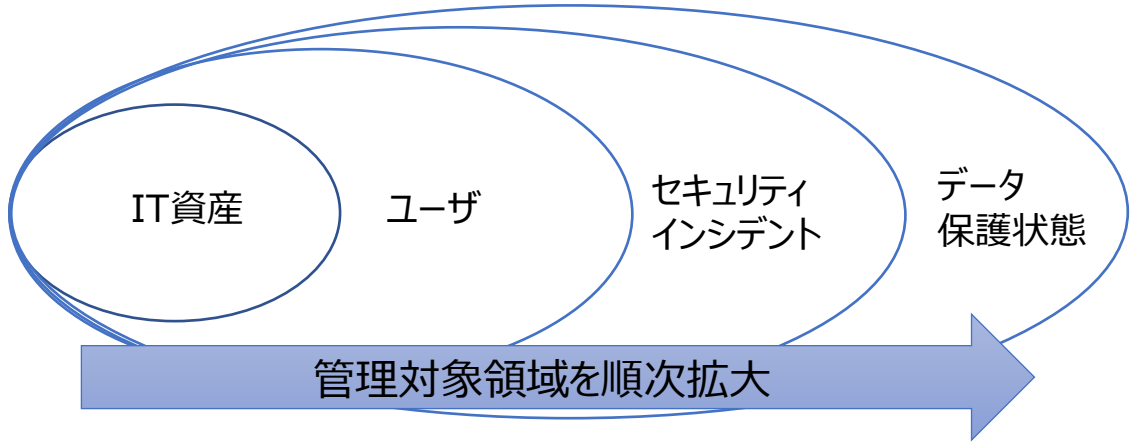
- **リスク診断**
  必要なコントロールと実際の状態の
  ギャップやリスクを可視化
- **対処**
  可視化されたギャップやリスクへ
  是正の対応
- **常時**
  ギャップやリスクを可視化し、
  是正の対応を継続的に実施



継続的に実施

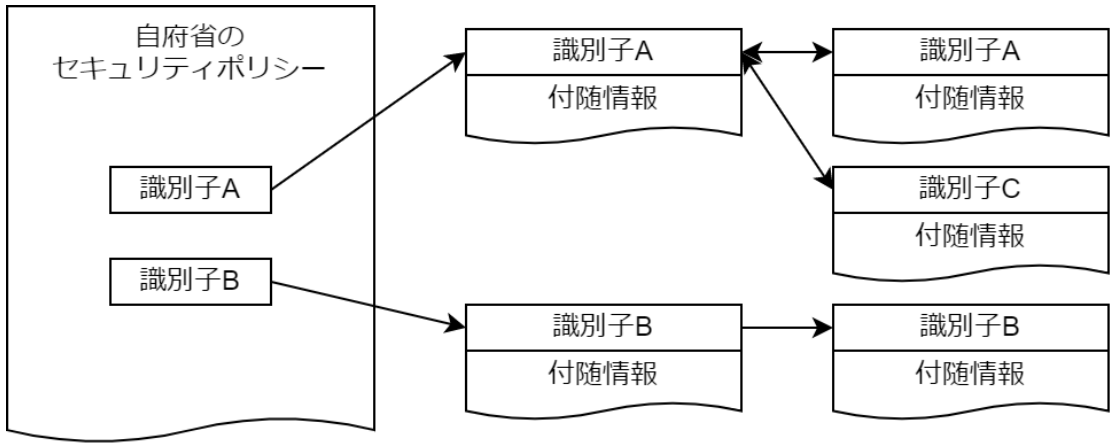
●管理対象

- **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。



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
```

デジタル庁