aws SUMMIT

TOKYO | APRIL 20-21, 2023

CUS-16

国でもできたスマートなクラウド利用
～高速試行錯誤しながら進歩を続けるクラウド CoE～

西嶋 岳大
デジタル庁／農林水産省
デジタル庁 ITストラテジスト 兼 農林水産省 ITテクニカルアドバイザー

Agenda

1. はじめに
2. 府省クラウドCoE役務
3. デジタル庁直轄システム
4. おわりに

はじめに

■個人の意見

- Digital Transformationを成功させるには、IT戦略と組織戦略の相互作用を引き出すことが、ダイジです。

IT戦略

DX成功の定義

コストパフォーマンス
と
タイムパフォーマンス
の両立

Digital Transformation

組織戦略

競争優位が得られる
戦略

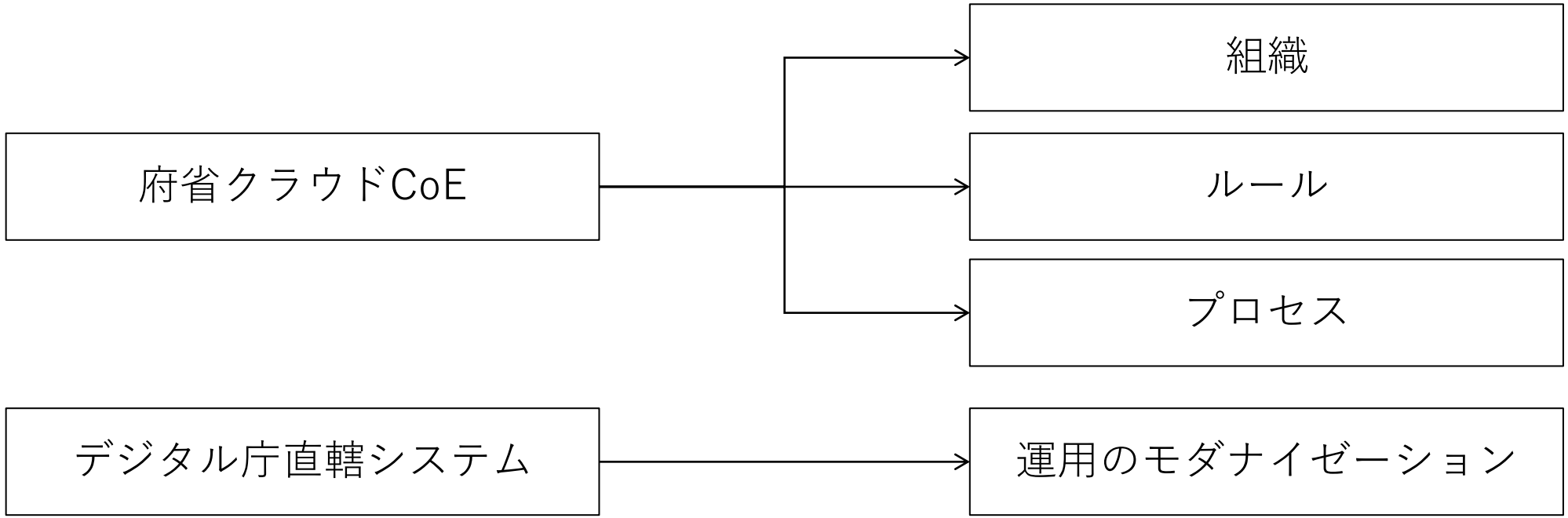
実行できないIT戦略は、
絵にかいた餅

戦略実行のための
俊敏な組織能力の変更

はじめに

■目的

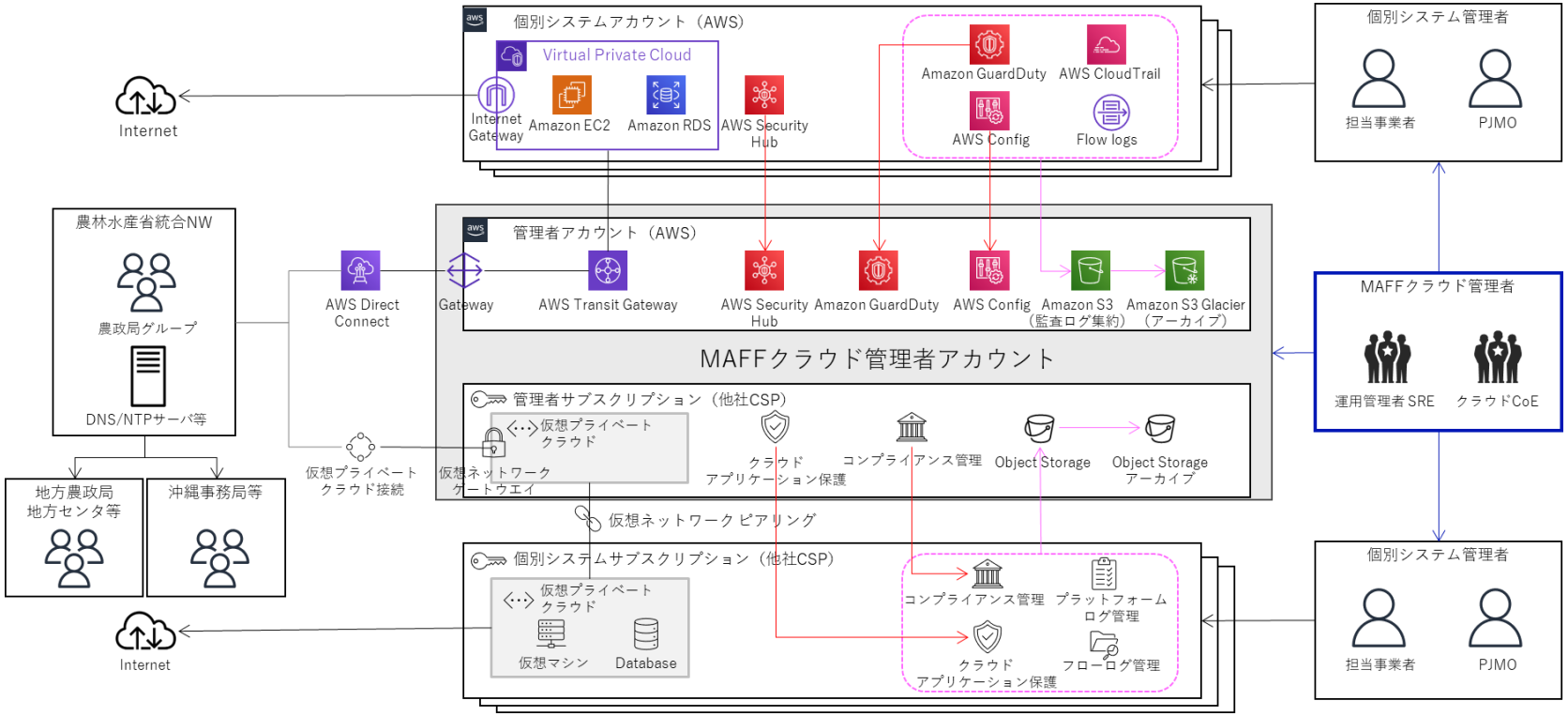
- 府省クラウドCoEの取り組みとデジタル庁直轄システムの運用のモダナイゼーションの取り組みについて、ご説明いたします。



府省クラウドCoE役務

■前提：農林水産省クラウド（以降、MAFFクラウドという）のご紹介

- ガバメントクラウドの先行事例として、令和２年から稼働しております。
  - マルチクラウド・マルチアカウントのデザインです。
  - 共通機能をMAFFクラウド管理者アカウントに集約しています。



府省クラウドCoE役務

■前提：MAFFクラウドの共通機能のご紹介

- クラウドの豊富な機能を安心・安全に活用するために、セキュリティ面で共通化すべき4つの機能を共通機能として提供しています。

閉域網接続機能

MAFFネットワークとCSPを閉域網接

AWS Direct Connect

続機能を提供する。

マネージド型脅威検出機能

各CSP上の脅威を検出し、検出時に利

Amazon GuardDuty

下管理者へ通知を行う。

監査ログ収集機能

利用システムの監査ログを収集・アー

AWS Configなど

し・確認を可能とする。

不適切設定検知機能

順守すべきポリシーと異なる利用シス

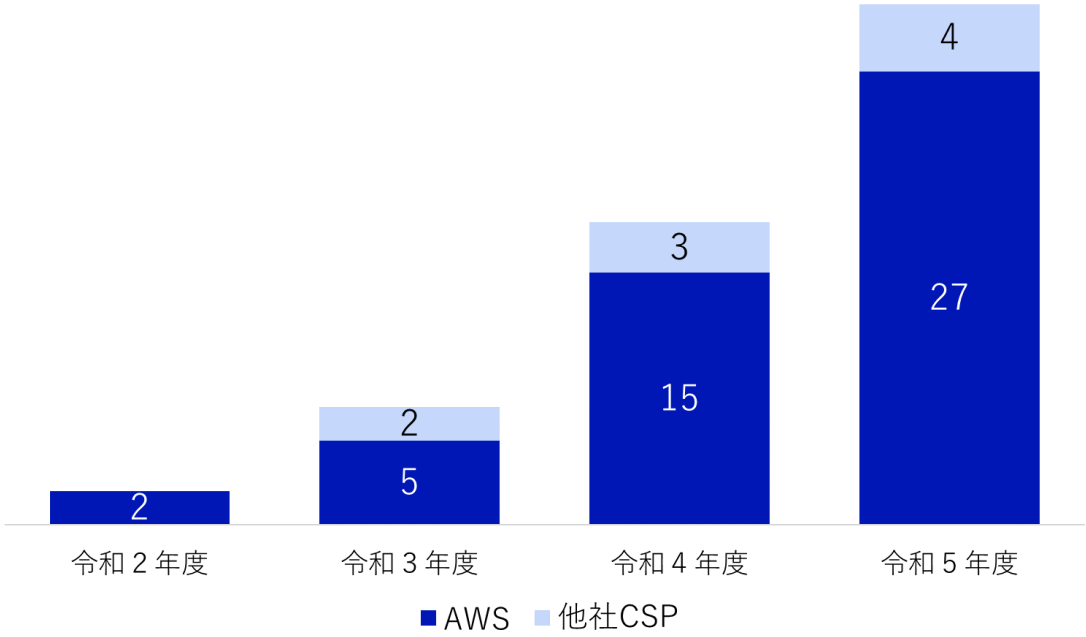
AWS Security Hub

管理者へ通知を行う。

府省クラウドCoE役務

■前提：MAFFクラウドの実績

- 令和4年度末時点で、MAFFクラウド上で18システムが稼働しています。



令和5年度は、新たに13システムが移行予定であり、計３１システムが稼働する予定です。なお、MAFFクラウド移行後にリファクタリングに取り組み、ガバメントクラウドに移行するシステムもあります。
また、農林水産省の１つのシステムが、ガバメントクラウドに移行し令和５年４月１日から稼働しています。

府省クラウドCoE役務

■MAFFクラウドCoEを引き受けるにあたり、考えたこと。

課題	原因
クラウドの進化を取り込みMAFFクラウドの陳腐化を抑止したい。	クラウドが、進化するから
MAFFクラウド利用システムの可用性を高めたい。	セキュリティリスクが、逓増するから
MAFFクラウドCoEでは、解決できない課題を解決したい。	個別システム担当者への指導力が、不足するから

- 課題解決のための組織、ルール、プロセスについて、ご説明いたします。

府省クラウドCoE役務

■組織

- 毎週３つの委員会を開催しました。

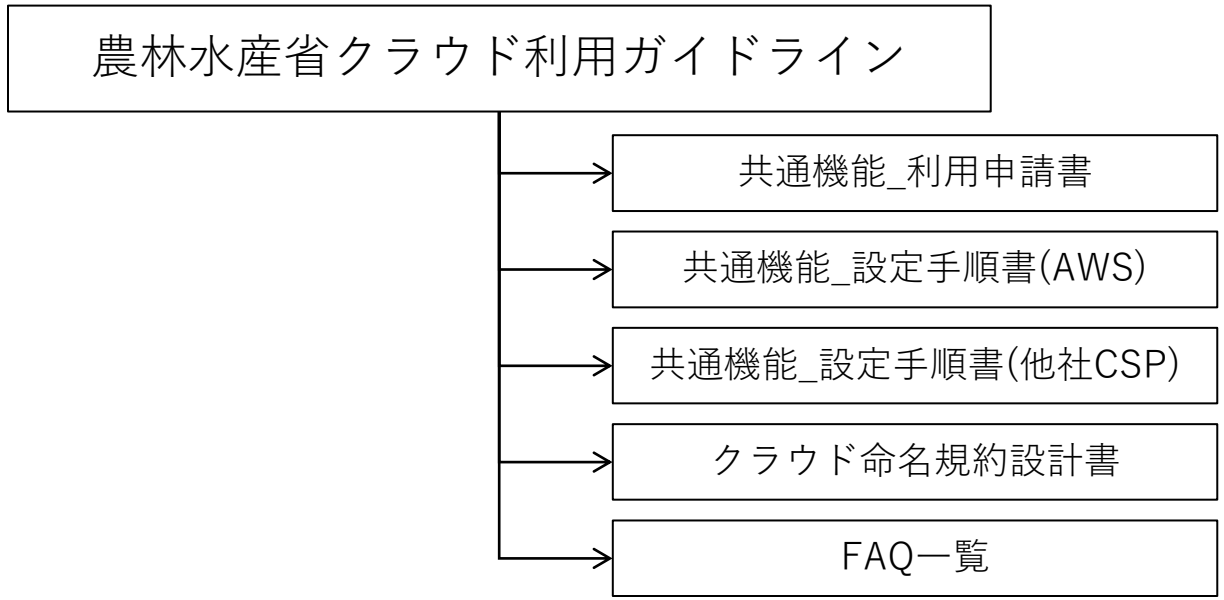
技術検討会	運用管理委員会	進捗管理委員会
クラウドの進化を取り込みMAFFクラウドの陳腐化を抑止する。	運用管理からMAFFクラウド利用システムの可用性を高める。	MAFFクラウドCoEでは解決できない課題を解決する。
新サービスの導入検討 各システムのアーキテクチャーの評価 MAFFクラウドのガイドラインの更新 FAQの更新 命名規約の更新 手順書の更新	専用線の管理 不適切設定の検知状況 セキュリティリスクの検知状況 問い合わせ対応の状況 狭義のSRE役務	各クラウド移行プロジェクトの進捗管理 新サービス導入の承認・審査 ガイドラインなどの更新の承認・審査 外部環境の変化の把握と対応の相談
クラウドアーキテクト コンサルタント 運用担当（SRE）	クラウドアーキテクト コンサルタント 運用担当者（SRE）	クラウドアーキテクト コンサルタント ITテクニカルアドバイザー（旧：政府CIO補佐官） 農林水産省のPMO

- MAFFクラウドCoEの支援事業者は、株式会社ビッグツリーテクノロジー&コンサルティングです。

府省クラウドCoE役務

■ルール

- MAFFクラウド利用者が、必要なルールをわかりやすくシンプルに記載し、持続的に更新しました。



コンセプト
標準化・共有化・シンプル化
により
ムリ・ムダ・ムラを無くす

農林水産省クラウド利用ガイドラインを２年で１８回改訂しました。
FAQ一覧を２年で４６項目を追記しました。

府省クラウドCoE役務

■プロセス

- システムライフサイクルの全フェイズに関与しています。

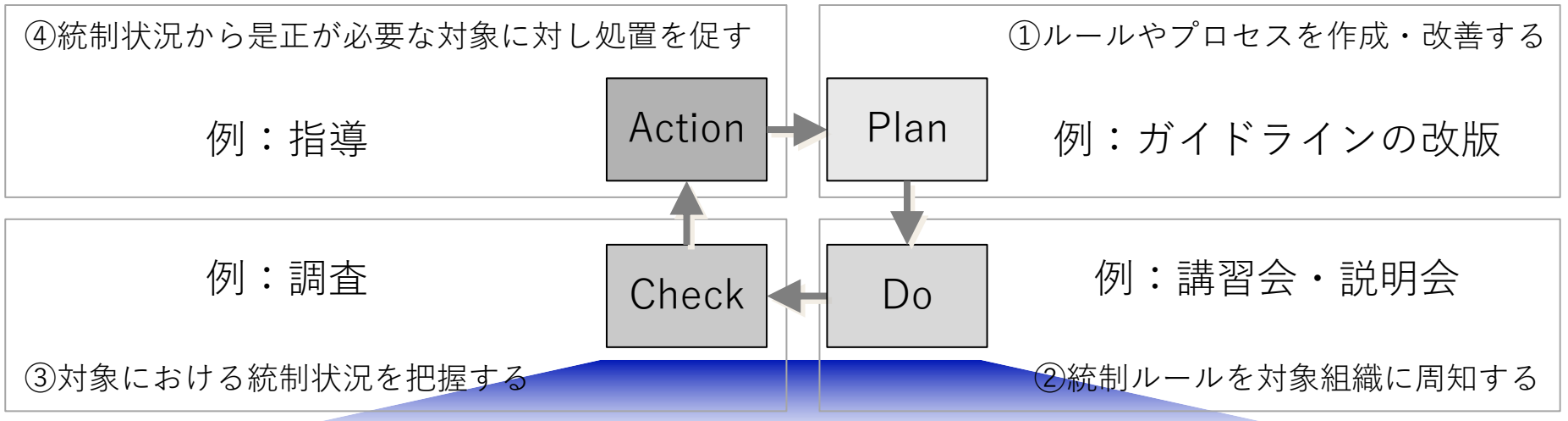
	政府情報システム担当（PJMO）	MAFFクラウドCoE
企画・予算要求	• PJMOが事業者に概算見積を要求し、内容を精査 • システム要件の整理 • 予算要求 • PoC実施	• 複数社の見積を取得するよう指導 • AWS Pricing Calculatorを用いた見積もりの精査 • 構成概要図のレビュー • PoC実施支援
要件定義	• 要件定義、機能要件、非機能要件の策定	• AWS Well-Architected Framework に基づく非機能要件観点のレビュー • 要件定義書、運用計画書作成支援及びレビュー
調達	• 調達仕様書の作成 • 調達手続き • ベンダー選定	• 調達仕様書レビュー • 複数社から提案頂いて、一社応札とならないように指導
システム設計・開発	• 進捗管理 • 意思決定、会議体の開催 • 成果物の検収	• 設計書などの成果物レビュー • MAFFクラウド接続支援
運用・保守	• システム状況監視 • 保守業務 • 機能拡張の検討 • 障害対応	• 運用保守報告の妥当性チェック • 運用改善支援 • セキュリティアラート対応サポート

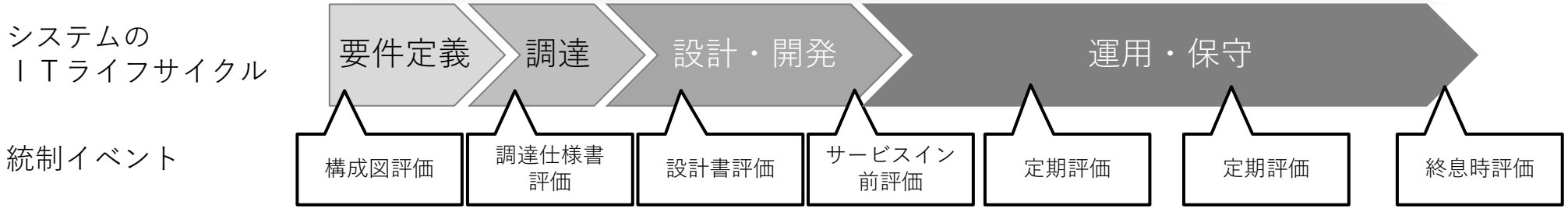
府省クラウドCoE役務

■プロセス

- ２つのプロセスを高速回転させています。

統制を改善し続けるプロセス





統制を掛け続けるプロセス

府省クラウドCoE役務

■MAFFクラウドCoEの変遷

開始時

EC2だらけの構成図のレビューをして、EC2 on OracleをRDSに変えるように促すことくらいしかできませんでした。

組織を使って、ルールを作り、プロセスを高速回転させて、MAFFクラウド稼働システムを増やし、実績を積み重ねることで、MAFFクラウドCoEに信頼の貯金を貯めました。

現在

MAFFクラウドCoEは、必要な時にその貯金を切り崩して、統制を強めることが、できるようになりました。

横展開

MAFFクラウドCoEは、デジタル庁が考える府省CoEのモデルケースとなり、他府省にも府省CoEが置かれることになりました。

府省クラウドCoE役務

■MAFFクラウドCoEが取り組んだ改善の一部

提案書に構成図が記載されて無い	AWSアイコンを用いた構成図とAWS Pricing Calculatorを提示依頼
Amazon EC2だらけで、国費の無駄遣い	Fargate、Lambda、RDSを活用し、Amazon EC2インスタンス数を逓減
マネジメントコンソールを用いて手作業で構築	システムは、AWS CloudFormationで構築
サーバにログインして運用、パッチ適応	Amazon EC2の運用には、SSMを導入し活用
システム毎に踏み台サーバを構築	踏み台サーバを構築せずにFleet managerやSession managerを利用
独自の監視ツールを導入している	監視にAmazon CloudWatchを用い、独自の監視ツールを持ち込ませない
データやベストプラクティスに基づいた改善提案が無い	改善のためにAWS Trusted Advisorや運用報告書などの内容提示を義務化

現行踏襲を望む個別システム管理者に改善の意思決定させるには、CoEに勇気が必要です。

府省クラウドCoE役務

■まとめ：個人の見解

- 定性効果

組織	MAFFクラウドCoEの統制により、スマートなクラウドサービスの利用とクラウドの機能を用いた運用改善が実行されたことで、費用逓減することができました。
ルール	MAFFクラウドのガイドラインと関連ドキュメントを提供することで、共通機能の設定手順書作成やタグ設計などのムダな作業を無くしました。
プロセス	統制を掛けるプロセスと新技術の採用を促すプロセスのダブルループで、現行踏襲と陳腐化を抑止しながら、クラウド移行の効果を得ることができました。
共通機能	MAFFクラウドの共通機能を提供することで、重複投資を抑止しました。

府省クラウドCoE役務

■まとめ：個人の見解

- 定量効果

ROI	MAFFクラウドCoEへの投資額を上回るコスト削減効果などのリターンが得られており、ROIは、プラスです。
NPV	クラウド移行をオンプレミスからの取り換え投資として算出した差分キャッシュフローを用いたAPV法により算出したNPVは、プラスです。

根拠となる具体例

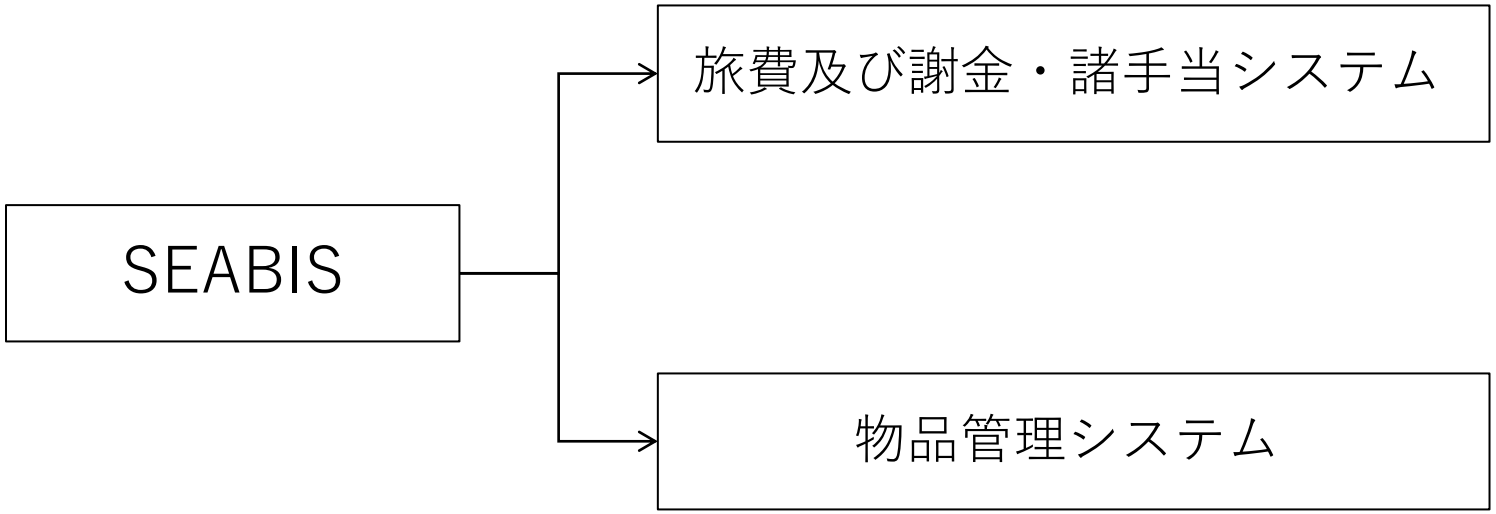
Aシステムでは、予算要求金額と契約金額の削減率が６６％

Bシステムでは、移行前のオンプレミスとクラウド移行後の運用経費の削減率が７０％

デジタル庁直轄システム

■前提：旅費等内部管理業務共通システム（以降、SEABISという）のご紹介

- 国家公務員（ユーザー約32万人）が、利用する経費精算システムです。



旅費業務及び謝金・諸手当業務のうち、旅行計画、旅費精算等の書類作成、支払金額の決定、決裁処理、支出処理等の共通的な処理について支援するシステム

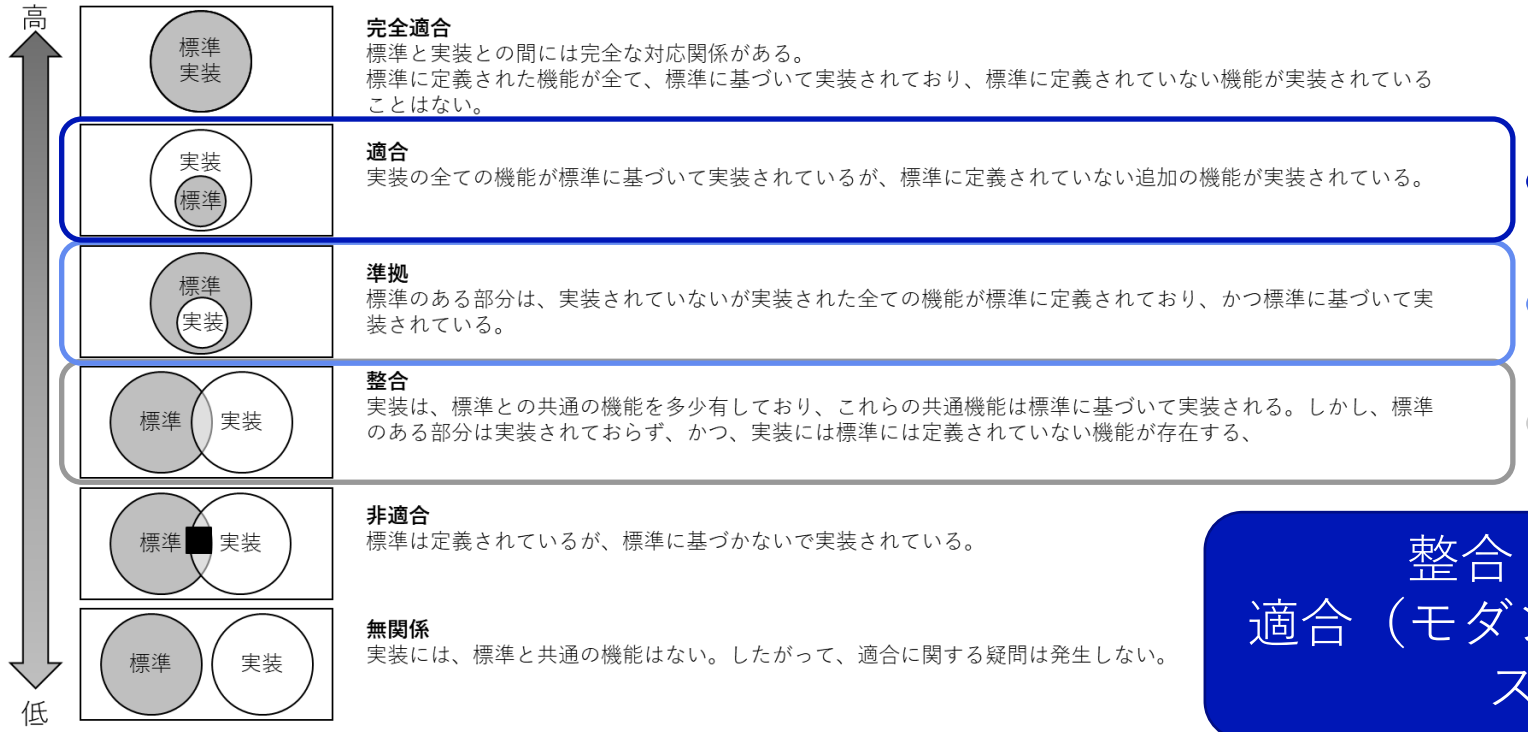
物品管理業務に係る書類作成等の処理について支援するシステム

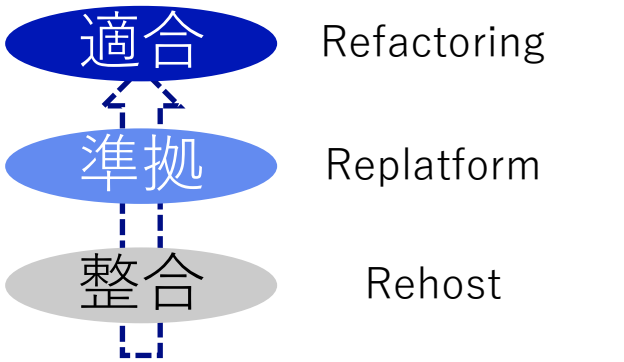
SEABISが、第一期政府共通プラットフォーム（オンプレミス）の終息に伴い、第二期政府共通プラットフォーム（AWS）に移行することになり、その支援を行いました。

デジタル庁直轄システム

■ＩＴストラテジストとして、俯瞰し統制を掛け続ける。

- 統制を高め過ぎた場合、業務の効率性や柔軟性が失われます。
- 統制を弱め過ぎた場合、投資やリスク低減の効果が望めなくなります。





整合（単純移行）から
適合（モダンなクラウド運用）まで
ステップアップ

図.統制の６段階

出典：TOGAF9 アーキテクチャ・コンプライアンス

デジタル庁直轄システム

■必要に応じて標準を変える：適合

- 構想として、AWS ChatbotとSlackを組み合わせて、ChatOpsを実現したい。
  - 具体的には、Amazon CloudWatchやSSMのIncident ManagerをAmazon EventBridgeとAWS Chatbotを用いて、デジタル庁のSlackと連携させたい。

ルール	AWS Chatbotは、グローバルサービスであり、海外リージョンにデータを持つため、第二期政府共通プラットフォームの標準（SCP）を変えないと使えない。

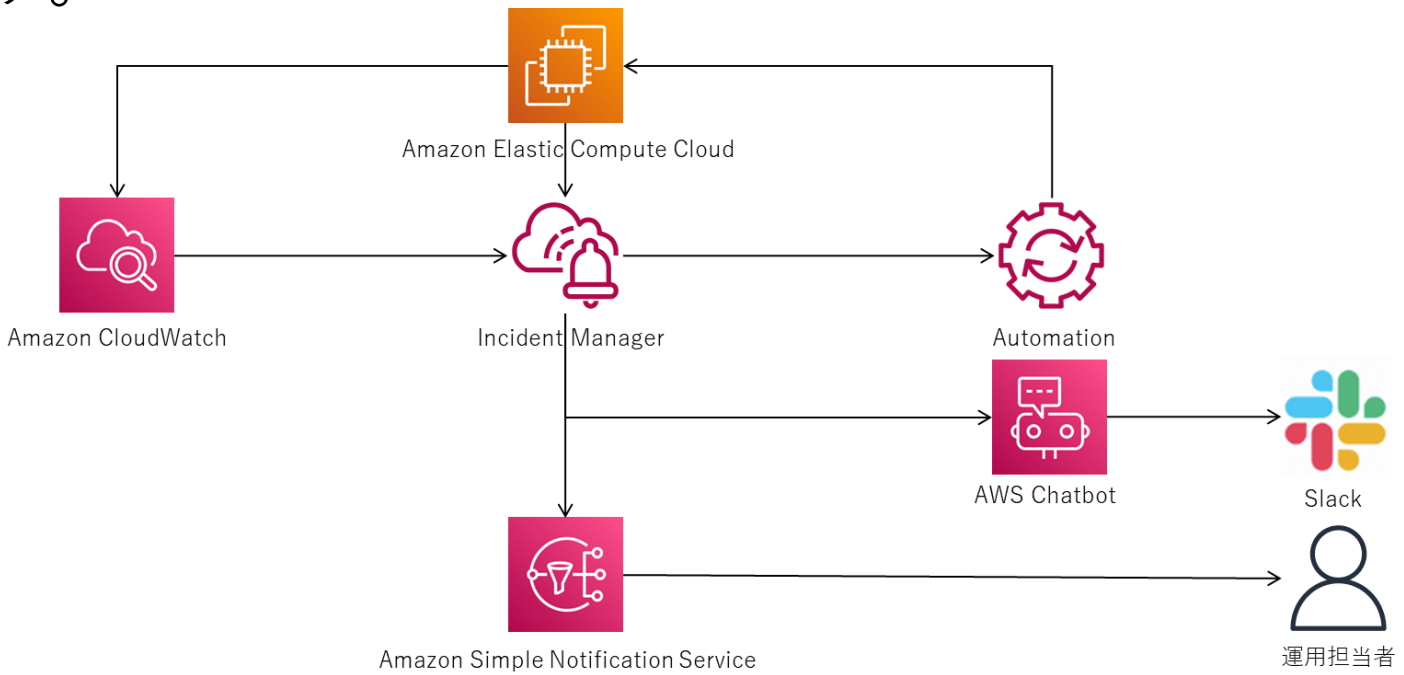
Q.AWS Chatbot は、AWS Chatbot を使用している AWS リージョン外のデータを処理しますか?
AWS Chatbot はグローバルサービスであり、当社は、Chatbot の設定と許可、Slack ワークスペースとチャンネル名、通知、ユーザー入力、AWS Chatbot が生成した応答と画像などのお客様の情報を任意の商用 AWS リージョンに保存したり、それらのリージョンで処理したりする場合があります。以下に示すようにオプトアウトしない限り、AWS Chatbot は、AWS Chatbot エクスペリエンスおよび他の Amazon 機械学習/AI テクノロジーの継続的な改善と開発に関連してお客様の情報を保存する場合もあります。
AWS Chatbot および他の Amazon 機械学習/AI テクノロジーの質を改善および開発することを目的としたお客様のデータの使用をオプトアウトすると、お客様のデータはすべての AWS リージョンから削除されます。オプトアウトする方法の詳細については、AWS Support にお問い合わせください。

デジタル庁に相談し、AWS Chatbotについての標準を変更しました。

デジタル庁直轄システム

■結果：ChatOpsの実現

- Amazon EC2で障害が発生した場合に、Amazon CloudWatchで検知し、Incident ManagerからAmazon SNSで通知し、AWS ChatbotからのSlack連携により、デジタル庁に障害情報の共有の上で、定義したAutomationを実行し復旧します。



デジタル庁直轄システム

■前提：俯瞰して運用業務を見直す上で使用した枠組み

項目	問
Eliminate：排除	無くすことができないか？
Combine：結合	１つにまとめられないか？異なる場合は、分離できないか？
Rearrange：交換	順番を入れ替えて、効率化ができないか？
Simplify：簡素化	より単純にできないか？

出典：生産管理の基本としくみ（田島悟、2010）

デジタル庁直轄システム

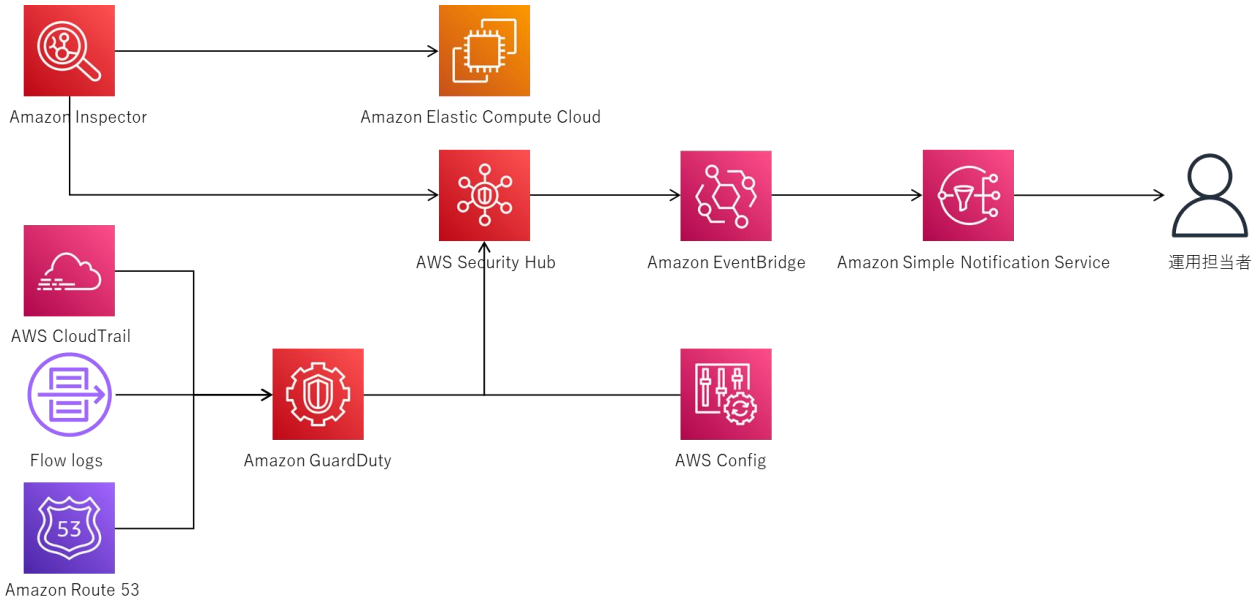
■SEABISの運用業務見直しの具体例

項目	打ち手
Eliminate：排除	障害対応時にデジタル庁職員が、AWS コンソールにログインし、Incident Managerの承認操作しなくても良いように、Slackで承認可能にしました。
Combine：結合	障害対応において、デジタル庁職員の承認回数を 3 回から 2 回に減らしました。 セキュリティサービスの検出結果をAWS Security Hubを用いて、結合しました。
Rearrange：交換	全AWSサービスをAWS CloudFormationで構築しました。 AWS Systems Manager Inventoryを用いてインベントリ管理をおこなう。 HinemosをAmazon CloudWatchなどに交換しました。
Simplify：簡素化	運用マニュアルに画面キャプチャをなるべく貼らないルールとしました。

デジタル庁直轄システム

■SEABISの運用業務見直しの具体例（Combine：結合）

- Amazon Inspector、Amazon GuardDutyを用いて、監査に必要な情報を収集し、収集した情報をAWS Security Hubで評価し、対処が必要なアラートを運用担当者へ通知します。

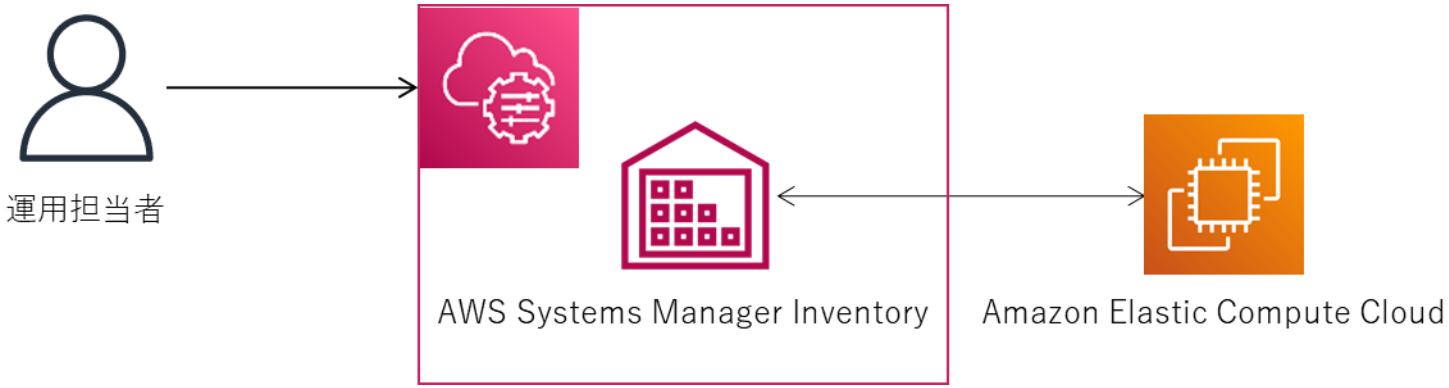


AWS Security Hubのセキュリティスコア９０％を目標に改善プロセスを実行しました。

デジタル庁直轄システム

■SEABISの運用業務見直しの具体例（Rearrange：交換）

- AWS Systems Manager Inventoryを用いてインベントリ管理をおこなう。
- 手作業で行っていたインベントリ管理をAWS移行を起点に自動化しました。



最新のソフトウェアインベントリ情報を維持することで、重要なセキュリティ情報について、迅速に影響の有無を判断できるようになりました。

デジタル庁直轄システム

■SEABISのスマートなクラウド運用のために利用している28サービス

- SEABISの構築支援業者は、富士通株式会社です。

おわりに

■クラウドCoEとＩＴストラテジストの経験から得た学びと気づき

- ダイジ、差、持続性の枠組みでご説明いたします。

ダイジ	物事の流れを知るために俯瞰することが、ダイジです。
差	段階的に統制を強めることが、実現度の差になります。
持続性	成果を持続的に出すために高速試行錯誤できる組織が、必要です。

おわりに

■自己紹介

氏名	西嶋　岳大（ニシジマ　タケヒロ）
所属	デジタル庁 ＩＴストラテジスト（デジタル庁の初期メンバー） 農林水産省 ＩＴテクニカルアドバイザー（旧官職：政府CIO補佐官）
担当領域	府省CoEとして、クラウド移行推進 デザイン思考などを用いたDXのコンサルティングサービス データマネジメントのコンサルティングサービス

デジタル庁

Digital Agency

Thank you!