SUMMIT

TOKYO | APRIL 20-21, 2023

AWS-51

自治体がガバメントクラウド利用に向けておさえておきたい 10 のこと

豊原 啓治
アマゾン ウェブ サービス ジャパン合同会社
パブリックセクター 技術統括本部 ガバメントクラウド技術本部 本部長

自己紹介

豊原　啓治

- 2017年からアマゾン ウェブサービス ジャパンで公共部門のソリューションアーキテクトを担当
- デジタル庁のガバメントクラウド及び自治体のお客様の技術支援を担当
- AWSの好きなサービス：Amazon S3

本セッションの目的

- 対象
  - ガバメントクラウド利用を検討している自治体、企業の方
  - 標準化準拠システムの企画や開発に関係する方
- 前提
  - 本資料の内容は2023年3月31日時点の情報を基礎に作成しています
  - 各AWSサービスの具体的な説明は含まれません

- ゴール
  - ガバメントクラウド（AWS)の概要の理解
  - 自治体や開発ベンダーとして必要な業務を理解
  - 計画、意思決定を促進

押さえておきたいポイントを示す

自治体をとりまく状況

- 2025年までに基幹業務システムの標準化準拠が必須
  - 機能要件、非機能要件の仕様の統一
  - ノンカスタマイズで、更新、移行を容易に
- ガバメントクラウド利用が努力義務

地方公共団体情報システム標準化基本方針の概要

○「地方公共団体情報システムの標準化に関する法律」（令和3年法律第40号）第５条に基づき、標準化の推進に関する基本的な事項について、地方公共団体情報システム標準化基本方針（以下「基本方針」という。）を定めるもの。

○ 内閣総理大臣、総務大臣及び所管大臣が、関係行政機関の長に協議、地方３団体から意見聴取の上、作成（閣議決定）。

統一・標準化の意義及び目標

移行期間：「**2025年度までに、ガバメントクラウドを活用した標準準拠システムへの移行**を目指す」

情報システムの運用経費等：「**平成30年度（2018年度）比で少なくとも３割の削減**を目指す」

地方公共団体における**デジタル基盤の整備、競争環境の確保、システムの所有から利用へ、迅速で柔軟なシステムの構築**

→ 国又は地方公共団体は、従来、時間と費用の両面から大きなコストが生じていた基幹業務システムからのデータの取り込みを円滑に行うことが可能となり、迅速な国民向けサービスの開始に寄与する。

→ デジタル庁は総務省とともに、全地方公共団体の移行スケジュール及び移行に当たっての課題を把握し、その解決に地方公共団体と協力して取り組むこととする。

施策に関する基本的な方針

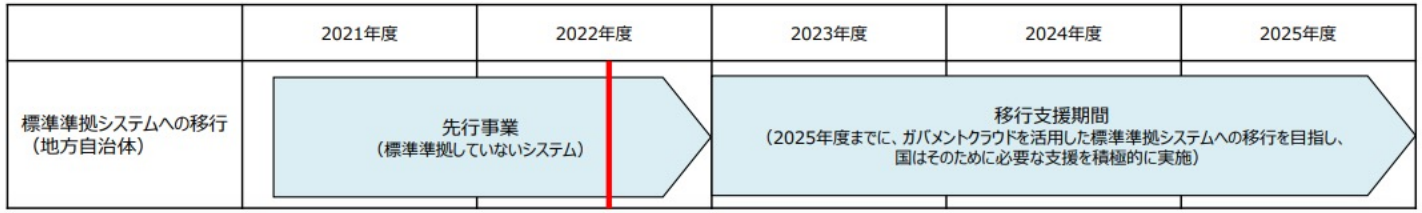
・標準化対象事務の範囲
・標準準拠システムの機能等に係る必要な最小限度の改変又は追加
・推進体制
（制度所管府省の役割、関係府省会議）
・意見聴取等

標準化基準に関する基本的な事項

・共通標準化基準に関する基本的な事項
（データ要件・連携要件、セキュリティ、ガバメントクラウドの利用、共通機能）
・標準化基準の策定に関する基本的な事項
（標準化基準の策定・変更方針、適合性の確認、検討体制）

その他推進に必要な事項

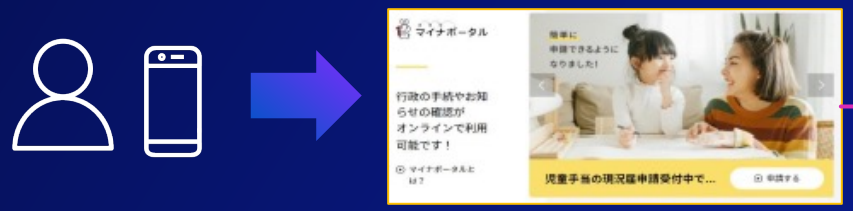
・地方公共団体への財政支援
（財政支援に関する基本的考え方、デジタル基盤改革支援補助金）
・地方公共団体へのその他の支援
（情報提供、市区町村の進捗管理、デジタル人材、都道府県の役割等）



出展　https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/dac15f8f/20221007_policies_local_governments_outline_01.pdf

TOBE 住民のユーザ体験向上

住民がスマホで手続き（Prefill）



マイナポータル

自治体庁舎

自治体窓口DXSaaS

書かない窓口

閉域網

ガバメントクラウド内で処理

公共サービスメッシュ

申請管理機能

API連携
ファイル連携

標準化準拠システム

データ参照・取込

窓口DXSaaS

Other CSPs

出展
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/72b46e0b-fbce-43a6-bd27-f0420b5064a2/18ff60e4/20220825_meeting_mynumber_outline_01.pdf
https://www.digital.go.jp/policies/cs-dx/dxsaas/

ガバメントクラウドとは

定義

「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、「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」を踏まえて構築する利用システムに、デジタル庁が提供する複数のクラウドサービスの利用環境のこと

目的

- 政府、自治体が、単にクラウドに移行するだけでなくクラウドの利用メリットを十分得れるよう、スマートなクラウド利用を得られるようにすること
- マネージドサービス、IaC、CI/CDを通して、開発スピード向上、セキュリティ品質向上、インフラ管理構築工数削減、継続的改善の効果を得る。政府や自治体のアプリケーション開発を現代的なものに促進する

出展　https://cloud-gov.note.jp/
https://www.digital.go.jp/policies/gov_cloud/

ガバメントクラウドにおける役割定義

出展：AWS Summit 2022
「ガバメントクラウドで考える技術的統制と効率性 ～ AWSでの実現策 ～」

単独利用方式と共同利用方式の違い

単独利用方式（自治体管理）

自治体（委託先）がAWS環境を管理する

A市領域

住民記録	A社製
税	B社製
福祉	C社製

共同利用方式（SaaS）

自治体はAWS環境を管理しない

X社領域（住民記録・税・福祉）

A市	B市	C市
D市	E市	F市
G町	H町	I町
J村	K村	L村

高	コスト	低？
高	自治体管理負担	低
高	自治体自由度	低

20業務のアプリケーションがシングルベンダーかマルチベンダーか調査する

出展　https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/3013abc6/20221007_policies_local_governments_outline_04.pdf

何を検討すればよいかわからない

- クラウド環境
- ネットワーク
- ID管理
- セキュリティ
-
-

出展　某自治体とのAWSワークショップ結果から

3つにカテゴライズ

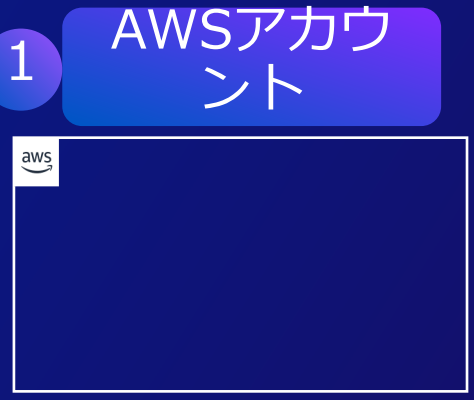
1. クラウド環境の管理

2. ネットワーク

3. アプリケーション

1、クラウド環境の管理

AWSアカウント（環境）とは

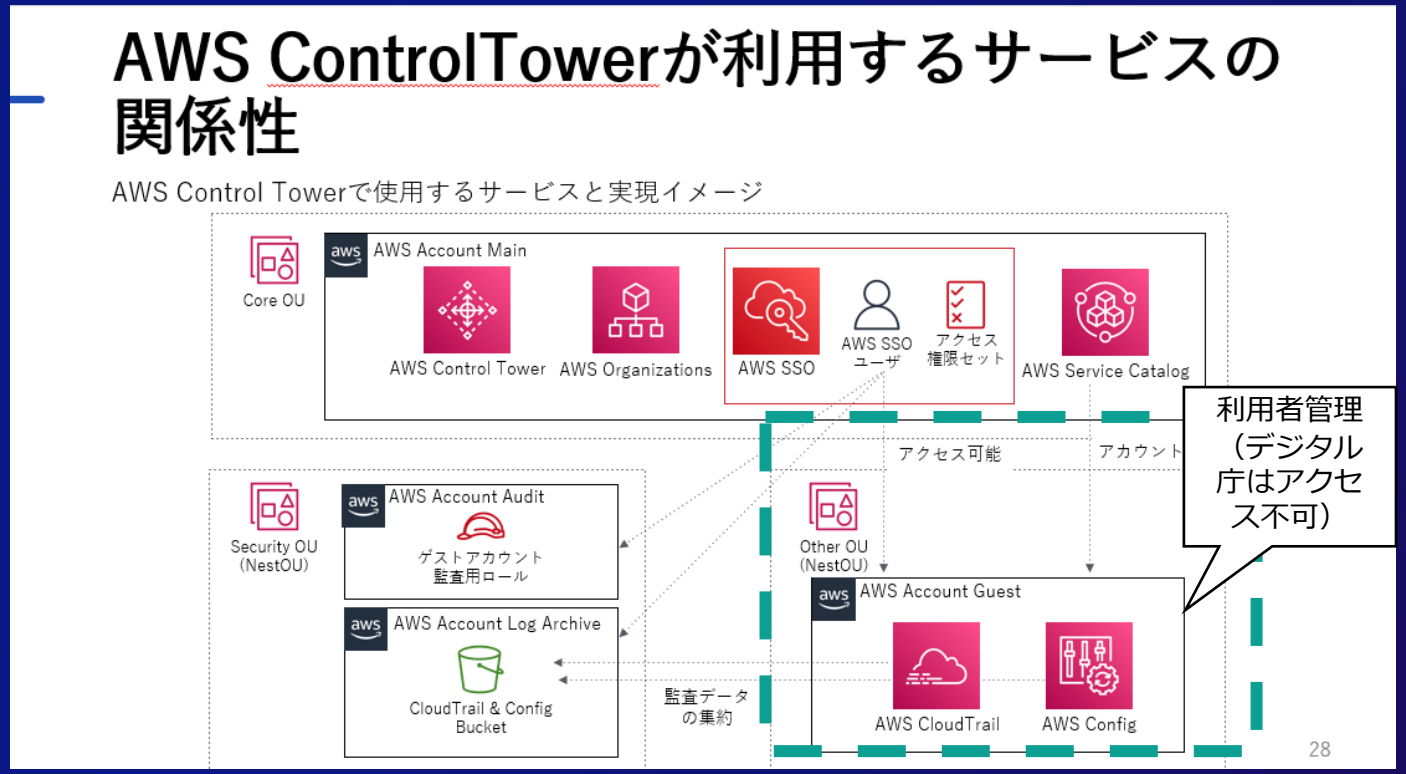


- AWSアカウント
  - セキュリティの境界であり、論理的分離されたお客様専用の環境
  - リージョン、AWSサービスが追加契約なく自由に利用可能
  - AWSの請求書発行の単位、AWSサポート契約の単位
  - 一般的な利用開始方法
    - AWSのWEBサイトからアカウント作成、クレジットカードで支払い
    - AWSのWEBサイトからアカウント作成、請求書で支払い（条件あり）
    - AWSパートナーの支払い代行を利用する

ガバメントクラウドは、デジタル庁がAWSと直接契約済み。
自治体はデジタル庁へ申請するだけなので、事務手続きがシンプルに。

AWSアカウントは誰が準備するのか？

- ガバメントクラウド方針
  - デジタル庁が、ガバメントクラウドの統制に必要な共通環境を管理
  - AWS ControlTowerとテンプレートを活用してアカウントを払い出し
  - デジタル庁が利用者に払い出すAWSアカウントは利用者が管理
  - 監査に必要なログは自動集約する。ガバメントクラウドの管理者は利用者のAWSアカウントにアクセスしないよう制御（違反の自動検出を実装）



出展:2022年AWSサミット「ガバメントクラウドで考える技術的統制と効率性～AWSでの実現策～」デジタル庁様ご講演資料

どういった仕組みなのか？

1 AWSアカウント

デジタル庁がAWS Control Towerで
AWSアカウントを自治体へ払い出す。
自治体利用に必要な機能が事前設定

デジタル庁が設定

テンプレート

- AWSアカウント作成
- SSO User作成
- 操作ログ改竄防止
- 予防的統制（SCP）
- 発見的統制（Config Rule）
- 不正アクセス脅威検出
- セキュリティ自動チェック

利用開始時からセキュリティ基準が高い

設定されているサービス

自治体

通知への対応

予防的統制の内容は？

1 AWSアカウント

- 安全に使うためリスクのある操作を禁止
  - 東京、大阪リージョン以外は制限
  - 現状デジタル庁が統制が難しいと判断した一部サービス禁止
    - AWS CloudShell、AWS Outposts、AWS Marketplace（個別相談）
  - MFAが必須
  - 自治体20業務システムを稼働するAWSアカウントはインターネットゲートウェイのアタッチが不可

アプリケーションの現代化のため、開発に必要なサービスがほぼ利用可能

発見的統制の内容は？

1 AWSアカウント

- リスクのある操作を発見して通知すること
- セキュリティにリスクのある設定を自動チェックして管理者へSlackやメールで通知する

（例）下記を含めて多数項目を自動チェック

MFAが設定されているか

S3バケットが外部アクセスがブロックされているか

ストレージが暗号化されているか

Security Groupが適切に設定されているか

発見的統制の通知を適宜改善する運用を業務に含めること

AWSアカウントは複数利用できるのか？

1 AWSアカウント

AWS アカウントで分離

システム（ベンダー）、環境に応じて AWS アカウントを分離することが推奨。テスト、本番、CI/CD環境を提供

自治体 管理者の業務

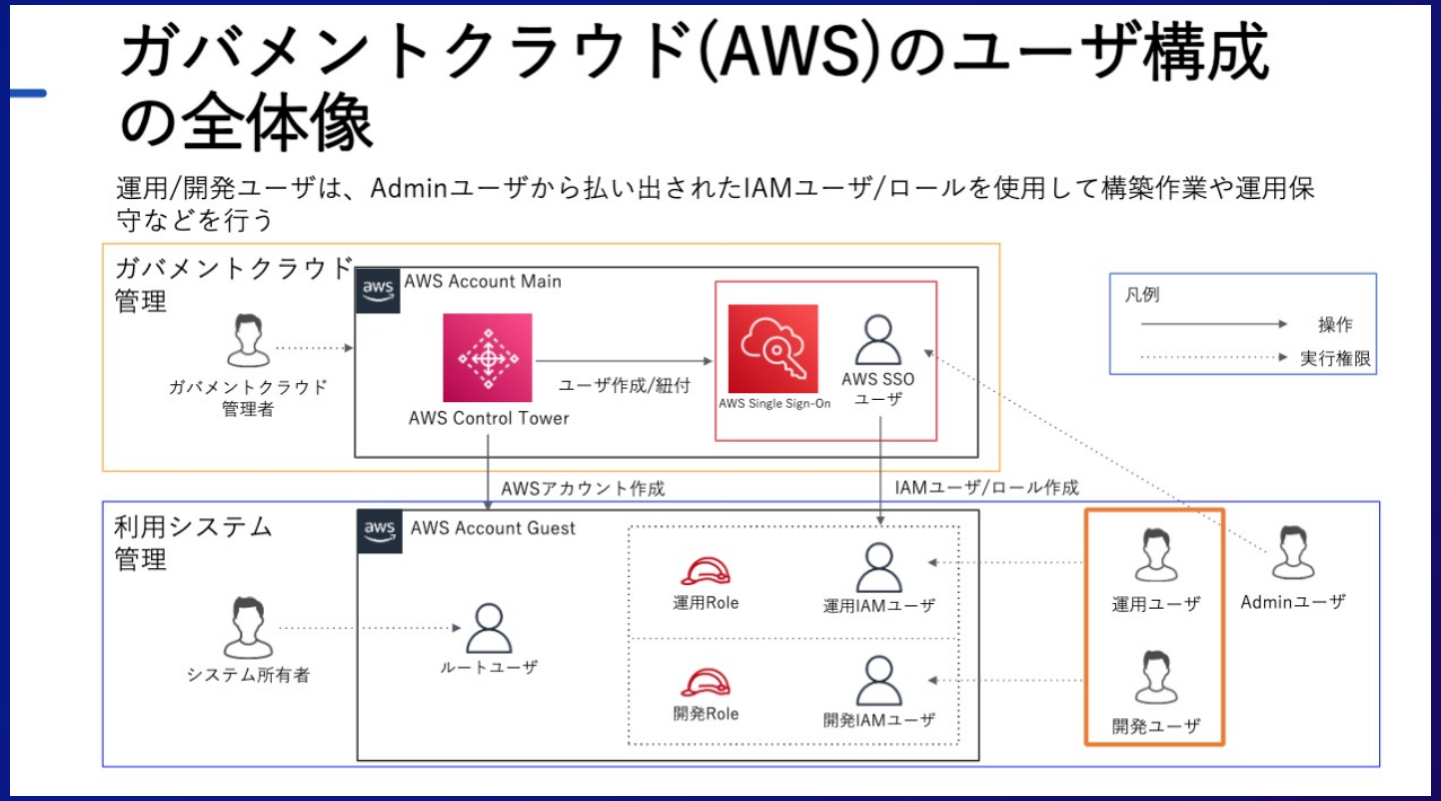
- デジタル庁へAWSアカウント及びID申請
- MFAの管理
- アクセス権限管理

ID管理やMFAの管理を適切に行うこと

AWSアカウントにアクセスするID管理

2 ID管理

- 管理者が、AWSアカウントにアクセスするSSO User は、Administrator Access権限が付与され、IAM権限の管理を行える
- 開発や運用に必要な権限のみを付与したIAM Roleを作成し、開発・運用を行うSSOユーザーまたはIAMユーザーは適切なIAM Roleへスイッチして作業を行う



IAM権限の最適化やIDの定期的な棚卸しを行うこと

出展:2022年AWSサミット「ガバメントクラウドで考える技術的統制と効率性～AWSでの実現策～」デジタル庁様ご講演資料

AWS Security Hubでセキュリティ管理

3 セキュリティ対応

- **AWS 基礎セキュリティのベストプラクティス**
  - AWSアカウントとリソースが、AWSセキュリティベストプラクティスと一致していないものを検出する自動セキュリティチェックを実施
- **CIS AWS Foundations Benchmark（v1.2）**
  - Center for Internet Security (CIS)が定義した、AWSのセキュリティ設定のベストプラクティス
- NIST SP 800-53 Rev.5

運用開始後も継続的にセキュリティ基準との不一致を対応・抑制していくこと

コスト最適化　Trusted Advisorの利用

4 コスト管理

- 利用状況と環境を分析し、推奨ベストプラクティスを以下5カテゴリで提示
  ①コスト最適化、②パフォーマンス、③セキュリティ、④耐障害性、⑤サービスの制限
- AWS Cost Explorerで、月次のコスト変化を把握、次期予算の正確な予測

- 赤: アクションを推奨
- 黄: 調査を推奨
- 緑: 問題の検出なし

AWS Trusted Advisor、AWS Cost Explorerを使い継続的にコスト最適化していくこと

AWSサポート

- ガバメントクラウドは、AWSの最上位サポートを利用可能
  - ケースの重要度と応答時間に「ビジネス/ミッションクリティカルなシステムのダウン：15分以内」が利用可能
  - 自治体ないしは委託先の企業から直接AWSにCaseオープンが可能
- AWSの利用者のリソースに問題がある場合は、AWS Personal Health Dashboardに通知があるので対応

AWS Personal Health Dashboard の通知へ対応すること

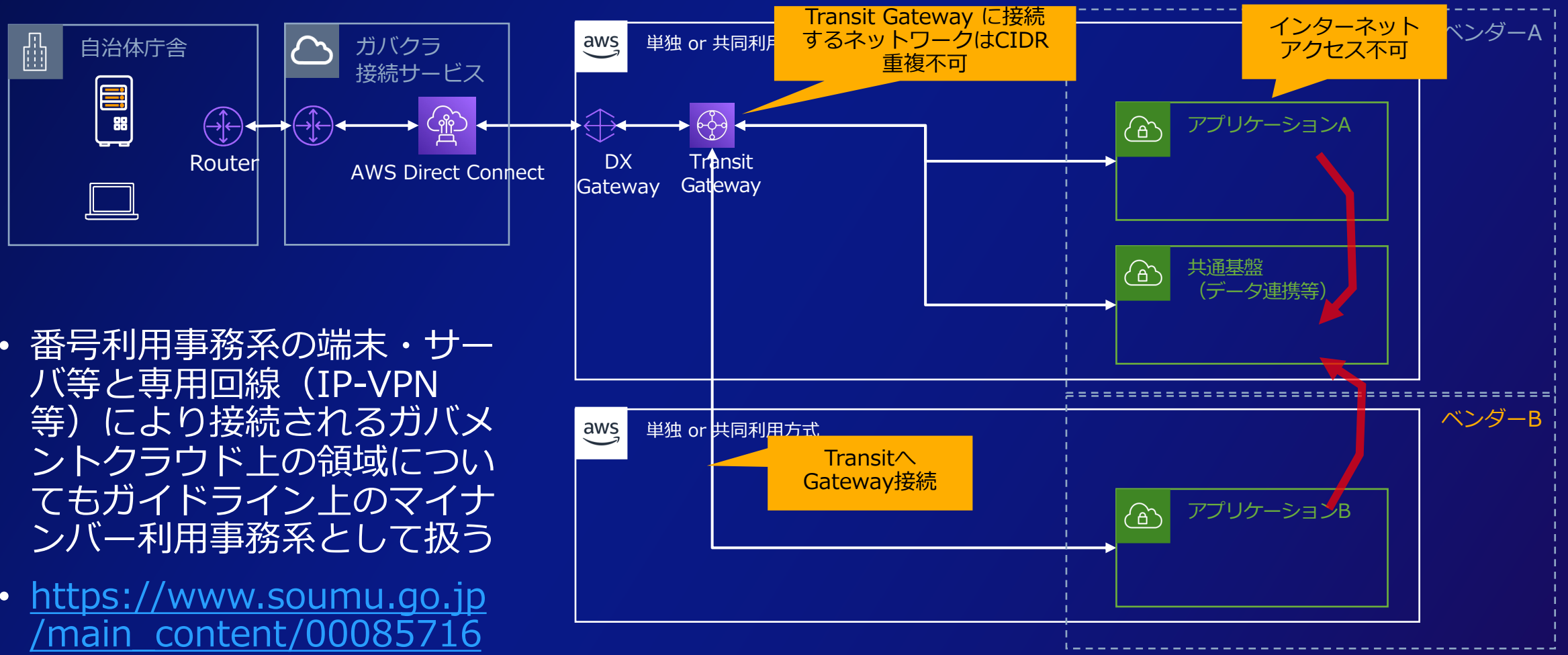
2、ネットワーク構成

ネットワーク

- Amazon VPCは自由に構成できる
  - CIDR（IPアドレスブロック）の指定はない
  - CIDRが庁内ネットワーク、VPC間で重複しないよう設計する
- インターネット接続
  - 自治体番号事務系システムが稼働するAWSアカウントは、Internet Gatewayのアタッチが禁止されている（予防的統制）
- 庁内ネットワークとの接続
  - デジタル庁から、自治体にガバメントクラウド接続サービスが提供される
  - 個別にIP-VPN等の専用線を手配してもよい(Transit VIF対応していることを要確認、冗長構成が必須)

庁内ネットワークとガバメントクラウド上のシステムが通信できるようクラウド環境のネットワーク設計・設定を行うこと

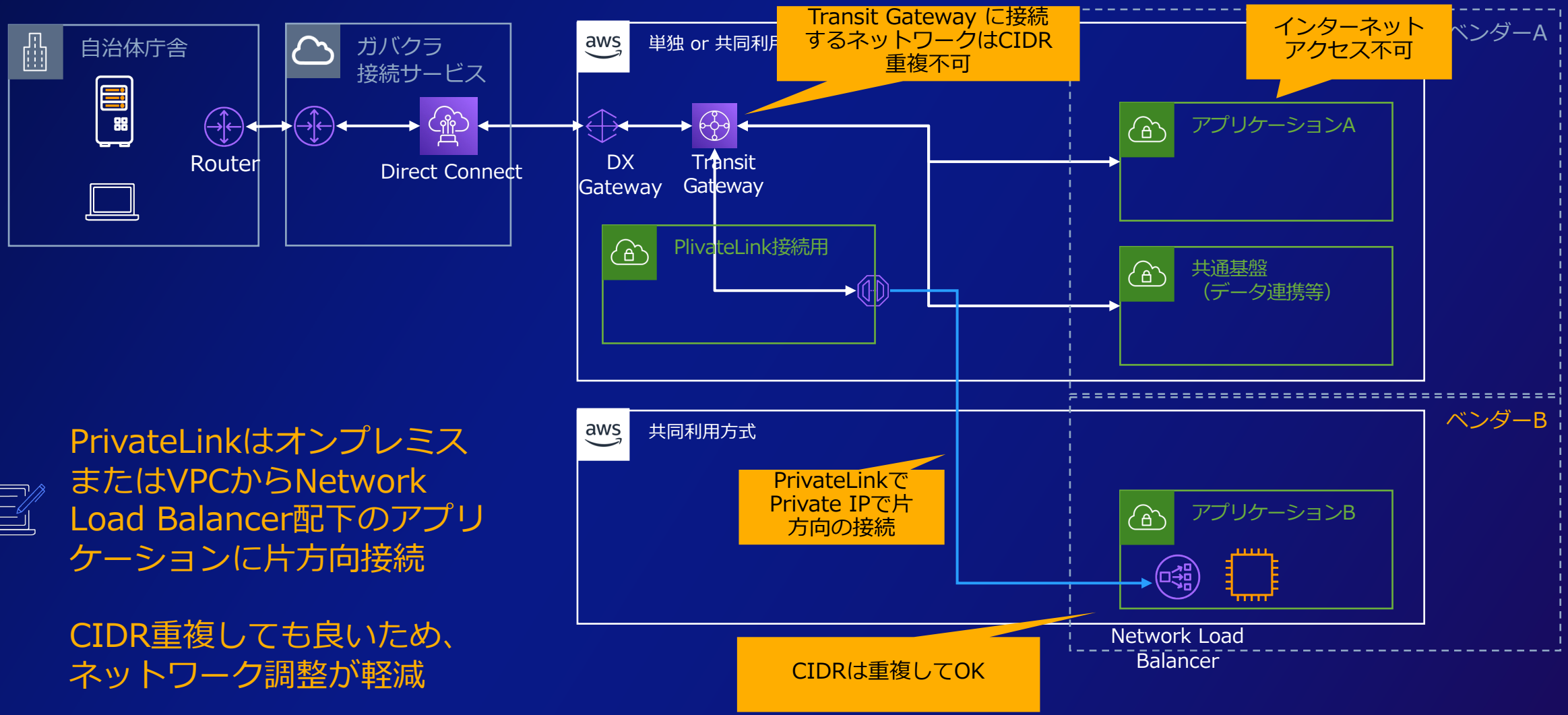
自治体とAWS間のネットワーク 1/3



- 番号利用事務系の端末・サーバ等と専用回線（IP-VPN等）により接続されるガバメントクラウド上の領域についてもガイドライン上のマイナンバー利用事務系として扱う
- https://www.soumu.go.jp/main_content/000857162.pdf

AWS Transit Gatewayはオンプレミス、VPC間の相互ルーティング可能

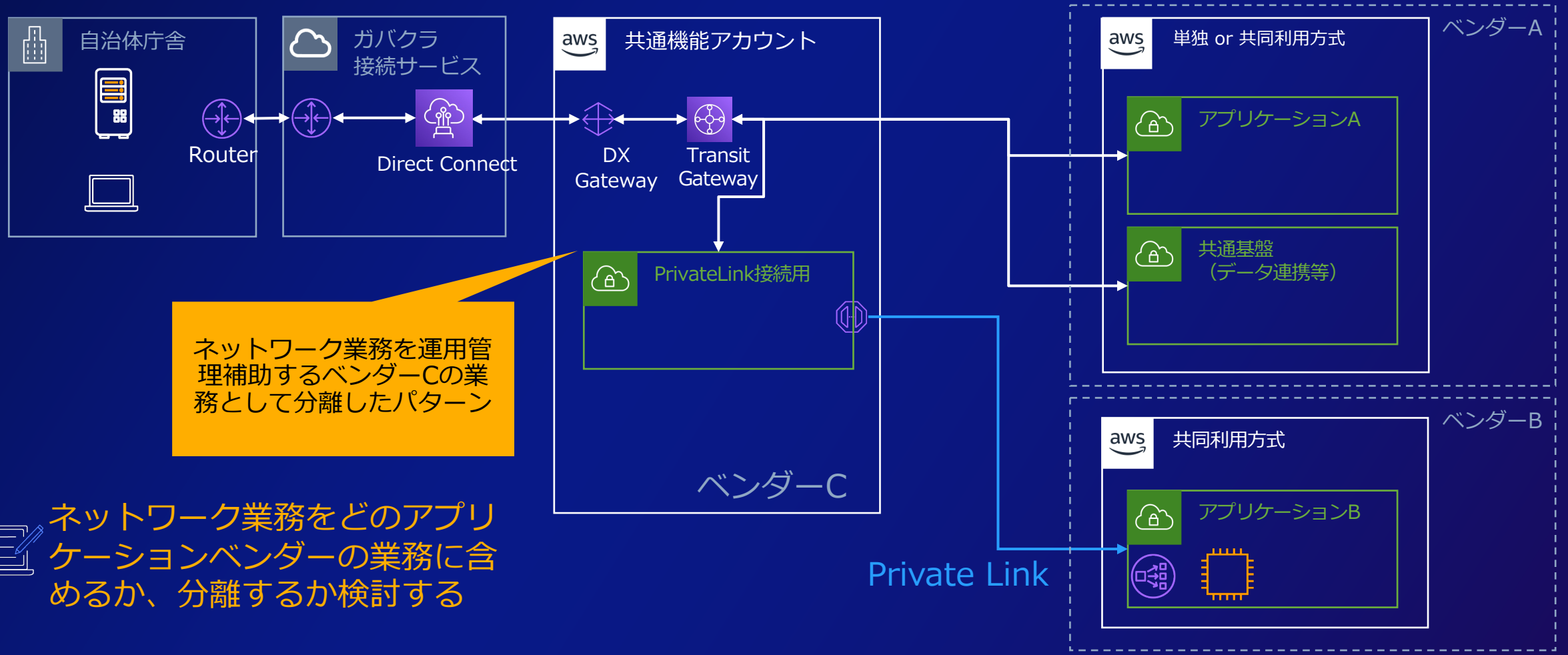
自治体とAWS間のネットワーク 2/3



PrivateLinkはオンプレミスまたはVPCからNetwork Load Balancer配下のアプリケーションに片方向接続

CIDR重複しても良いため、ネットワーク調整が軽減

自治体とAWS間のネットワーク 3/3



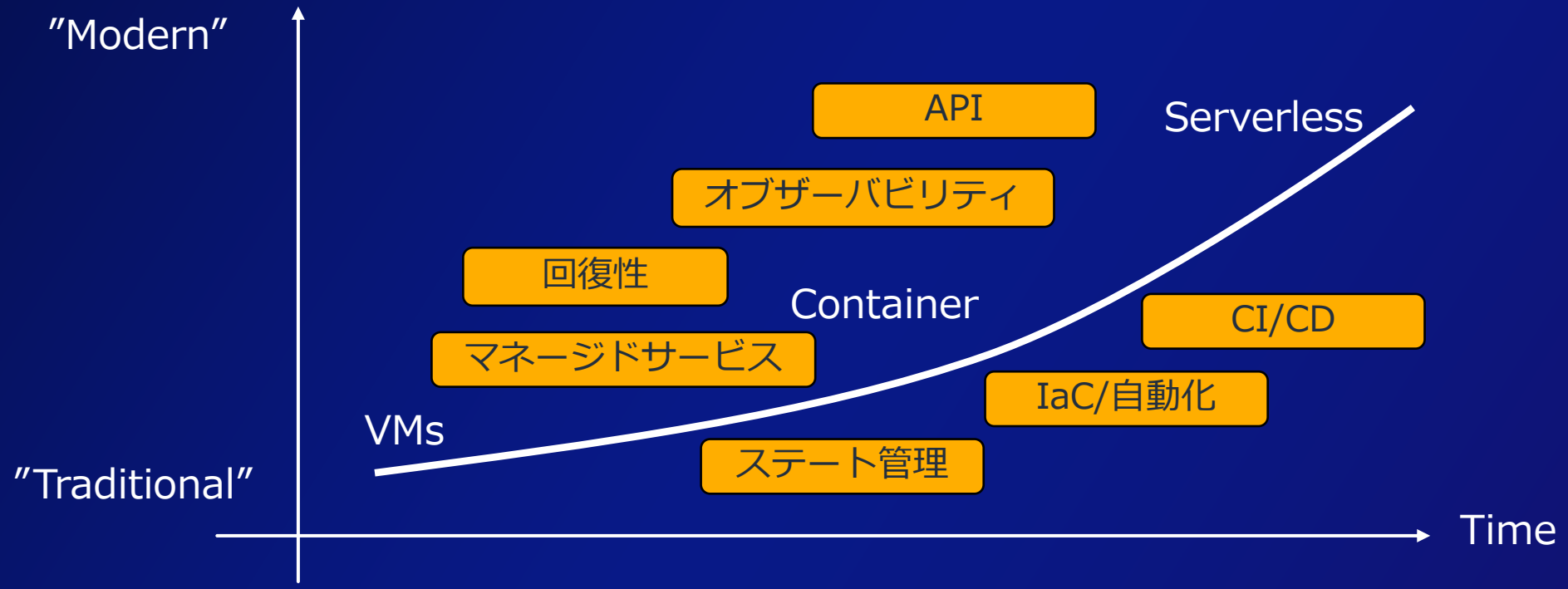
ネットワーク業務をどのアプリケーションベンダーの業務に含めるか、分離するか検討する

3、　アプリケーション

モダンアプリケーションへの移行

6 マネージドサービス

7 IaC

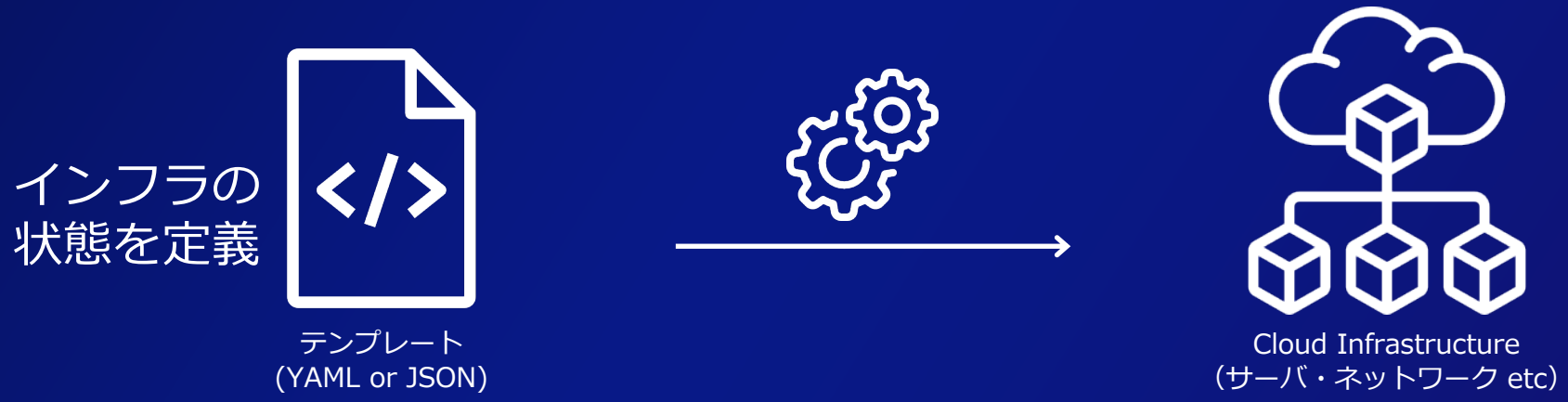


モダンアプリケーションは、ランタイムだけではなく、データベース、オブザーバビリティ、IaC、CI/CD・・マネージドサービスや自動化を取り入れ、迅速性、柔軟性、拡張性を高めている状態

OSを管理する必要のないマネージドサービスの利用、アプリケーションやインフラの更新の自動化を取り入れること

IaC Infrastructure as Code とは

サーバやネットワーク等の**インフラ構成をコードで記述する**ことにより、
環境の構築や管理を自動化すること。



IaCのメリット

- **コスト削減**
- **信頼性の向上**
- ガバナンスを効かせた
  継続的な開発・改善

先行事業：盛岡市の事例

7 IaC

○ ガバメントクラウドへリフトした場合、イニシャルコスト・ランニングコスト共に経費の削減効果があり、全体で8%の削減
○ シングルベンダー、既存環境の一括リフトによりコスト効果が出やすい条件がそろったと推測

【団体概要】20万人以上、データセンタ(単独)環境、オールインワン（アイシーエス）
【先行事業採択 評価点】費用対効果の検証について、現状における比較、5年後での比較、KPIを定めて検証を実施。ハウジング、自庁サーバで運用しており、クラウド利用の実績がない団体のモデルケースとしても有用と考えられる。

経費区分			A:現行システムを利用	B:ガバメントクラウドへリフト	コスト差異（ガバメントクラウド-現行）	現行継続と比較したときのガバメントクラウドリフトの削減率
イニシャルコスト	作業費	カスタマイズ費	¥0	¥0	¥0	0%
		環境構築費	¥10,491,000	¥2,601,000	¥-7,890,000	-75%
		データ移行費	¥0	¥2,167,500	¥2,167,500	純増
		他システム連携機能構築作業費	¥0	¥0	¥0	0%
		操作マニュアル作成・職員研修費	¥2,310,000	¥2,167,500	¥-142,500	-6%
		プロジェクト管理費	¥867,000	¥3,901,500	¥3,034,500	350%
イニシャルコスト計			¥13,668,000	¥10,837,500	¥-2,830,500	-21%
ランニングコスト	作業費	システム運用作業	¥57,741,600	¥57,741,600	¥0	0%
		ハードウェア保守作業	¥20,966,400	¥20,966,400	¥0	0%
		その他外部委託費	¥0	¥0	¥0	0%
	作業費計		¥78,708,000	¥78,708,000	¥0	0%
	物品費	ハードウェア借料	¥137,790,000	¥0	¥-137,790,000	-100%
		ハードウェア保守費	¥17,820,000	¥0	¥-17,820,000	-100%
		ソフトウェア借料	¥623,190,000	¥623,190,000	¥0	0%
		ソフトウェア保守費	¥129,612,000	¥129,612,000	¥0	0%
		データセンター利用費	¥15,600,000	¥0	¥-15,600,000	-100%
		通信回線費	¥3,416,880	¥15,798,000	¥12,381,120	362%
		クラウド利用経費	¥0	¥77,954,803	¥77,954,803	純増
	物品費計		¥927,428,880	¥846,554,803	¥-80,874,077	-9%
ランニングコスト計			¥1,006,136,880	¥925,262,803	¥-80,874,077	-8%
合計			¥1,019,804,880	¥936,100,303	¥-83,704,577	-8%

イニシャルコスト
- ✓ Bは、テンプレートの利用等により作業工数を抑えることができ費用削減されたのではないかと考えられる
- ✓ ガバメントクラウド移行に際し、AWSとの調整や移行作業における管理費が増加している

経費区分の中でも金額割合の大きい「環境構築費」を約75%削減できていることが、全体としてのイニシャルコストを約21%抑える要因となっている。

ランニングコスト
- ✓ ガバメントクラウドを利用することでハードウェアおよびデータセンタ利用費が全て削減となった
- ✓ ソフトウェア関連費は庁内設置システムの環境費であり、現行・ガバメントクラウド共に計上
- ✓ 庁舎とガバメントクラウド間で新たなデータ連携経路が発生するため、通信回線費が増加となっている

クラウド化によりインフラ関連の費用が大幅削減、クラウド利用料で発生する額を吸収できている

- クラウド利用及びIaCテンプレートによる自動化が作業工数を抑えていると考えられる
- 環境構築費を約75%削減された

出展　https://www.digital.go.jp/news/ZYzU5DYY/

自治体パッケージ向けテンプレートの公開

マネージドサービスやIaCを実践した経験がない

Amazon Web Services ブログ

閉域網での利用を前提としたCDKのサンプルテンプレートを公開しました

by Yozo Suzuki | on 10 3月 2023 | in General, Government, Public Sector, State Or Local Government, Technical How-To | Permalink | Share

こんにちは、公共部門でプロトタイプSAをしている鈴木です。
デジタル庁が整備するガバメントクラウドではAWSが採択されており、中央省庁や地方自治体等でAWSをご利用いただくお客さまが増えてきました。
このブログではこれからAWSを利用し始めるお客さまやアプリケーションのモダナイズをご検討されているお客さま向けに開発した、閉域網での利用を前提としたサンプルテンプレートについてご紹介します。

サンプルテンプレート開発背景

公共部門に限った特性ではありませんが、「閉域網の中にシステムを構築する」や「オンプレとの通信が発生する」という特性は、公共部門のお客さまからもよくお聞きします。
しかし、AWSのサンプルには、閉域網を前提としたサンプルが多くなく、インターネット接続を前提にしたものが多いです。

そのため、これからAWSをご利用したい、といった場合に、閉域網ではどういった構成、サービスを利用すればいいんだろう？と悩むことが多いのではないでしょうか。

特に、クラウドのメリットを最大限得るために、Amazon Elastic Compute Cloud (Amazon EC2)の利用ではなく、「マネージドサービスの活用」、「アプリケーションのコンテナ/サーバーレス化」、「Infrastructure as Code(IaC)やCI/CDパイプラインによる開発効率化」などの要素を、どのように自分たちのシステムに適用していこうかと、検討されているのではないでしょうか。

サンプルテンプレートのご紹介

出展　https://github.com/aws-samples/template-for-closed-network-system-workloads-on-aws

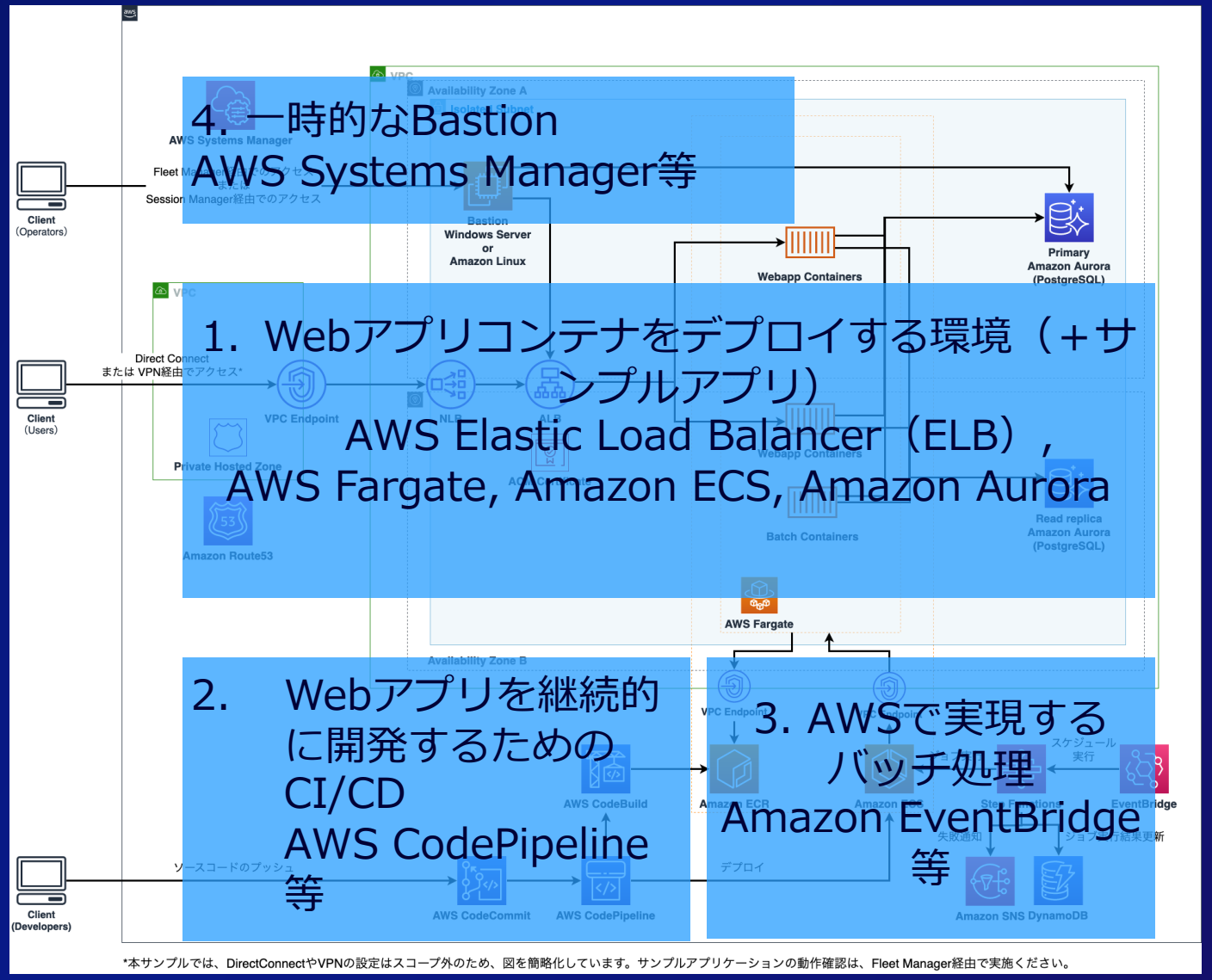
サンプルテンプレートの構成

6 マネージドサービス

7 IaC

・地方公共団体情報システム非機能要件の標準に、配慮した構成を組み込み

・通信暗号化
・DB暗号化
・ログの取得
・マルチAZ
・ECRイメージスキャン
・世代管理

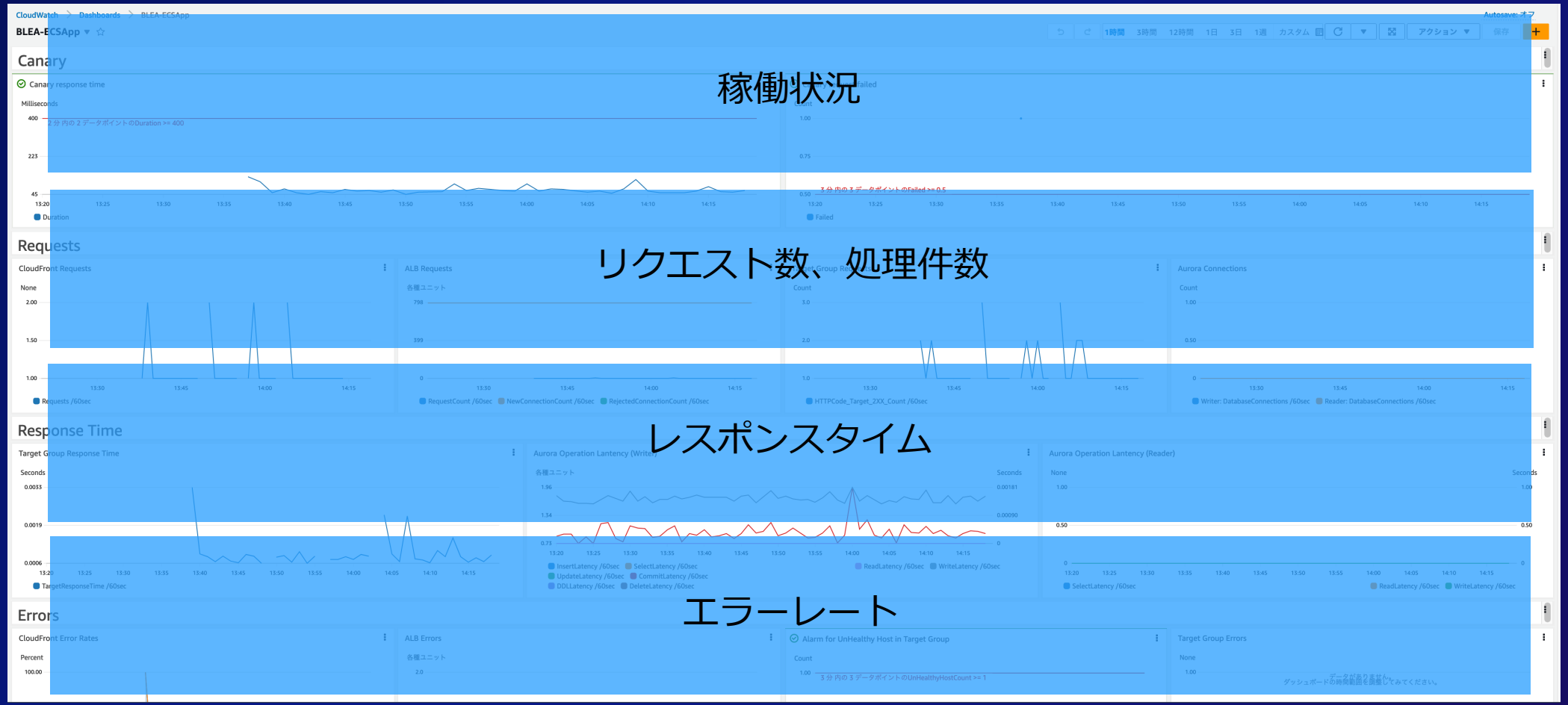


CloudWatchダッシュボードの利用

6 マネージドサービス

7 IaC

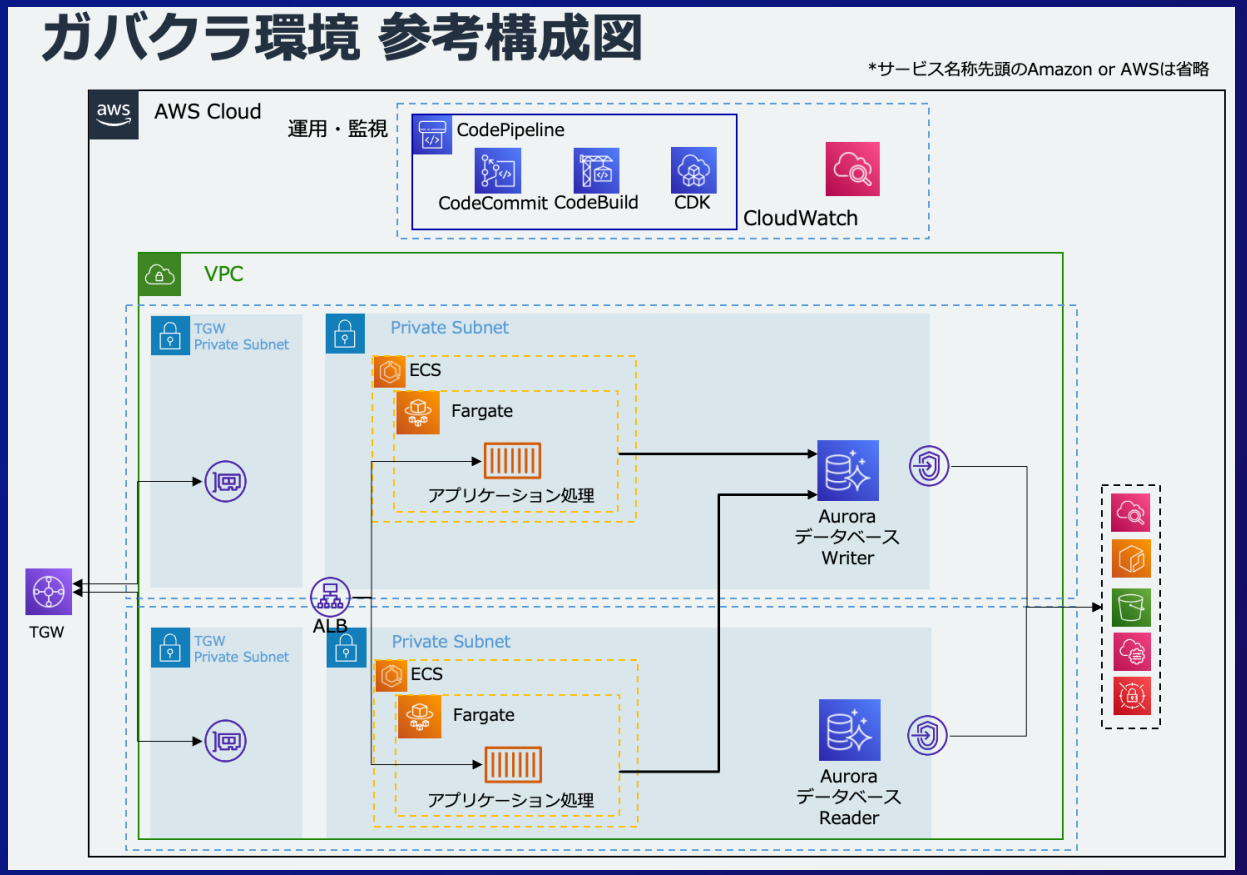
システムの可観測性を高めるための
サンプルテンプレートを提供（Baseline Environment on AWS)



出展　https://aws.amazon.com/jp/blogs/news/announcing-baseline-environment-on-aws/

浜松市様　書かない窓口サービス

- 課題
  - 開発チームは、コンテナの本番利用、AWSの利用、IaCの利用がはじめての状態であり、短期間でDeployする必要があった
  - AWS上の構成がベストプラクティクスに合致しているか知見がない
- 解決方法
  - テンプレートを要件に合わせて修正するだけで迅速に環境のDeployが完了した。
- 結果
  - 設計工数短縮、テストが容易で繰り返し可能であり納期も間に合った
  - モダナイズ・自動化したことでコスト減
  - テンプレートで他自治体へSaaS展開に期待



出展：株式会社 北見コンピューター・ビジネス様

自治体システム内のデータ連携の特性

8 データ連携

- データ連携をプライベートネットワークで行う必要がある
  - 業務システム間のデータ連携
    - 基幹系２０業務の場合、標準仕様に沿った方法でデータ共有する
    - REST/FTP/オブジェクトストレージ

- 課題
  - オンプレミスとAWS
  - AWS間

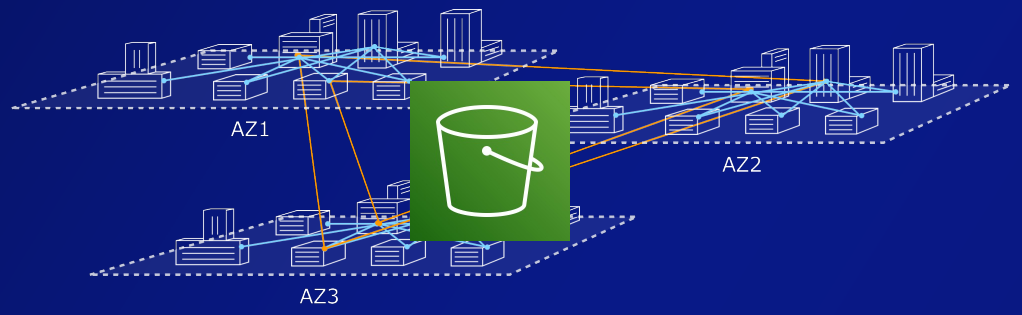
出展
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/a810f063/20230330_local_governments_16.pdf

オブジェクトストレージの利点

8 データ連携

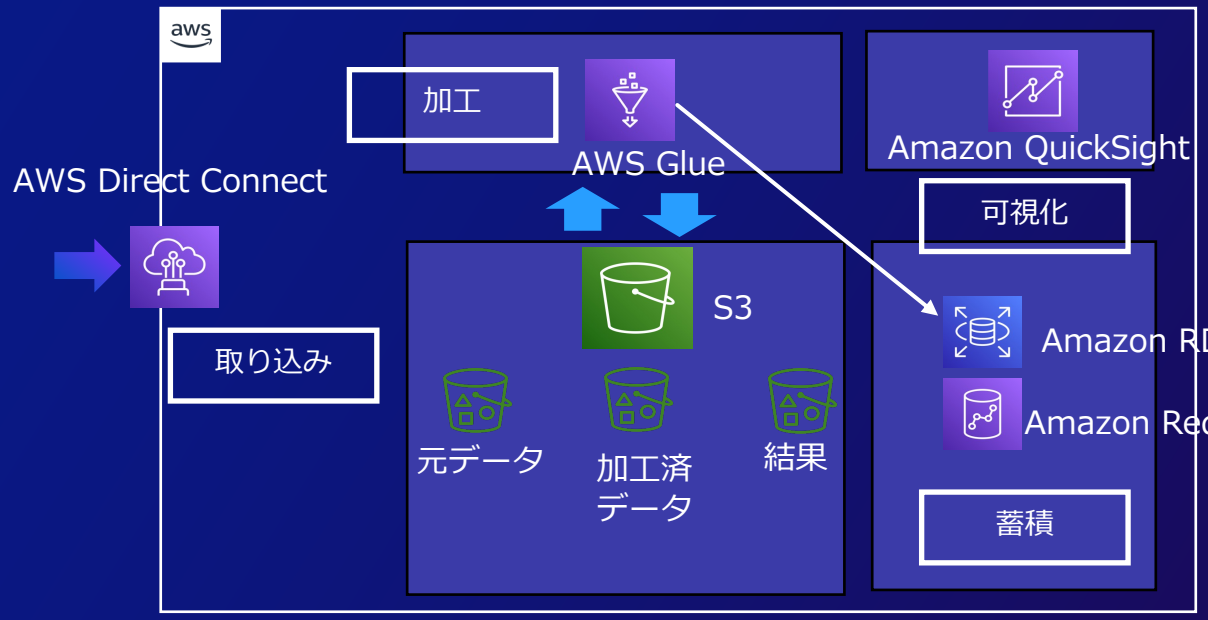
Amazon S3の特徴

- スケーラブル
- 99.999999999%の耐久性
- アクセス制御と監査ログ
- データ保護
- 様々なAWSサービスと連携
- AWS SDK、REST API、AWS CLI



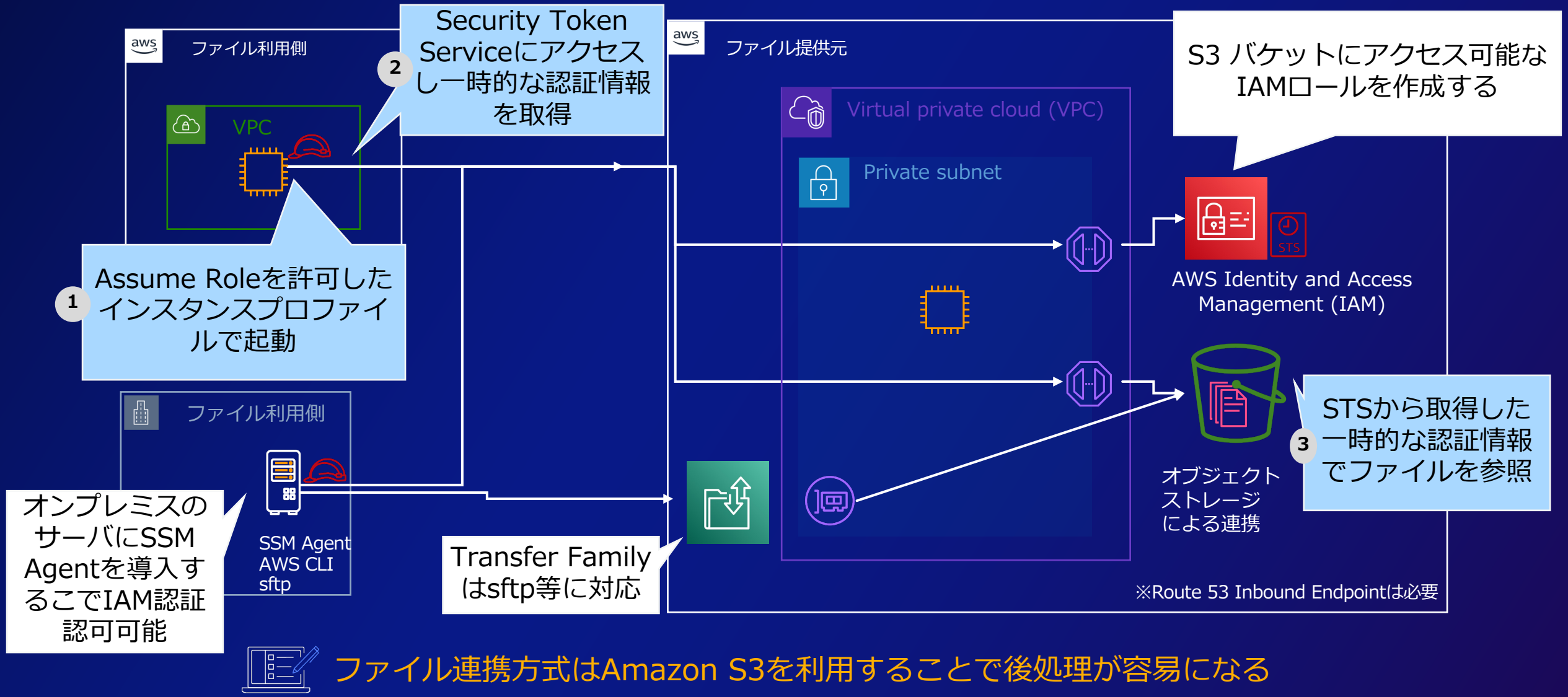
マネージドサービスで自動処理

- マネージドサービスを利用して自動化すればファイルを処理するためのEC2、コンテナが不要
- AWSサービスを使ったデータ分析が可能



オンプレミスやAWS間のファイル連携

8 データ連携

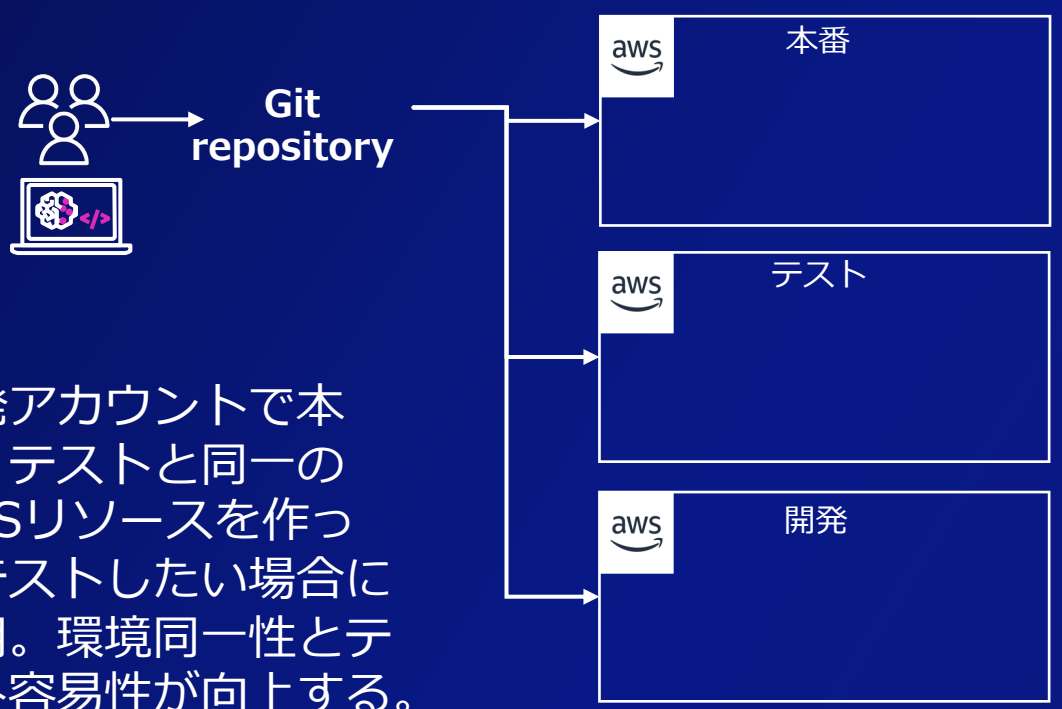


ファイル連携方式はAmazon S3を利用することで後処理が容易になる

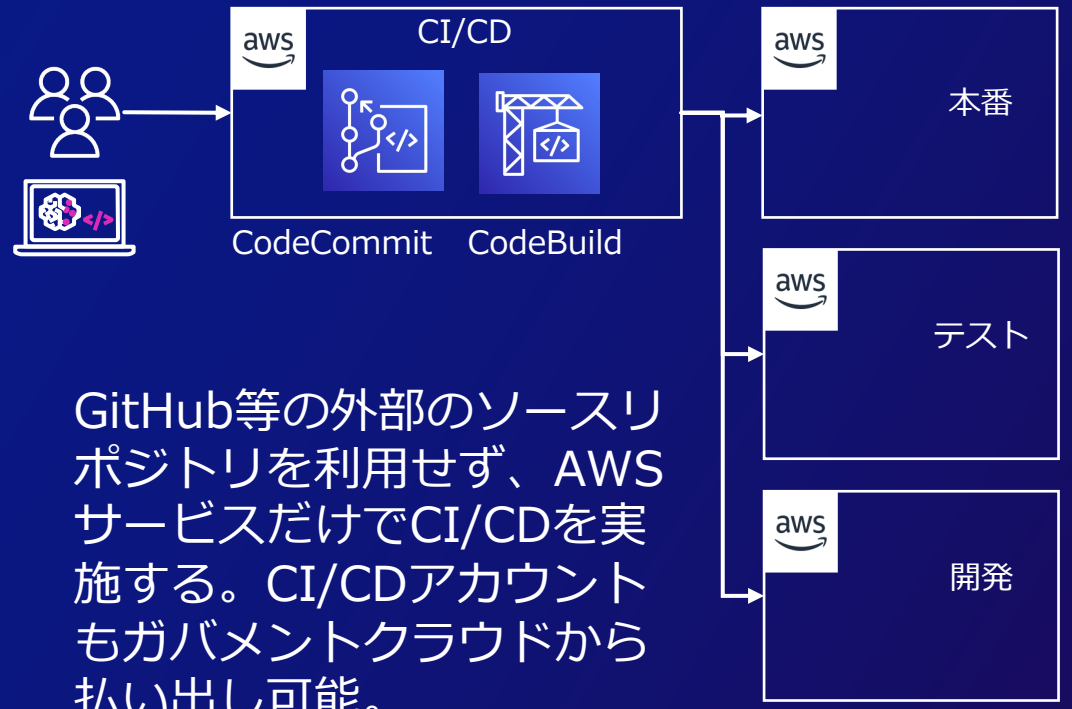
アプリケーション、インフラのCI/CD

9 保守 CI/CD

CI/CDを利用することで、開発ベンダーがリモートからアプリケーションのDeployができる開発環境を支援



開発アカウントで本番・テストと同一のAWSリソースを作ってテストしたい場合に採用。環境同一性とテスト容易性が向上する。



GitHub等の外部のソースリポジトリを利用せず、AWSサービスだけでCI/CDを実施する。CI/CDアカウントもガバメントクラウドから払い出し可能。

アプリケーション、インフラのCI/CDにマネージドサービスを取り入れること

バックアップ

- バックアップ、リストアは利用者側の役割
- システム非機能要件を踏まえて、RPO・RTO定義し最適な構成を設計する
- AWS Backup等のマネージドサービスに組み込まれたバックアップ機能を利用
- 大阪リージョンにデータ転送可能（リージョン間コピー）
- 復旧プロセスにIaCの活用

業務：RPO、RTOおよびバックアップ要件を踏まえて最適な構成を設計、設定、運用すること。
バックアップデータは耐久性の高いAmazon S3に保管する。

まとめ

- ガバメントクラウドは、標準化準拠システムの実行環境
- デジタル庁がCSPと契約済みのため事務手続きが軽減
- 予防的統制、発見的統制でセキュリティ基準を高めている
- AWSは一歩モダナイズを進めるためのテンプレートを準備済み
- AWSは先行事業の知見から短期間での検討を実現する支援が可能
- クラウド知識向上のため無償トレーニングを提供中

自治体向け
Monthly Training

Thank you!

自治体向け
Monthly Training

豊原　啓治

アマゾン ウェブ サービス ジャパン合同会社
パブリックセクター 技術統括本部 ガバメント・クラウド技術本部 本部長

ご相談はこちらまで！

lgjp-govcloud@amazon.co.jp