



デジタル改革推進課
Digital Innovation Promotion Division

名古屋市ガバメントクラウド利用方針 (第1.3版)

名古屋市総務局デジタル改革推進課
2025/05/21



目次①

1. はじめに

1.1 はじめに	5
1.2 他文書との関係	6

2. ガバメントクラウドの概要

2.1 ガバメントクラウド導入の経緯	8
2.2 クラウドの特徴とメリット	9
2.3 ガバメントクラウドの特徴	10
2.4 ガバメントクラウド上に構築可能なシステム	11
2.5 ガバメントクラウドの利用方式	12
2.6 ガバメントクラウドにかかる契約と手続き	13
2.7 ガバメントクラウドにかかる経費	14
2.8 ガバメントクラウドのCSP	15
2.9 ガバメントクラウド接続回線	16
2.10 ガバメントクラウド環境	17
2.11 ガバメントクラウド個別領域利用権限	18
2.12 ガバメントクラウドにおける責任分界	19
2.13 ガバメントクラウドテンプレート	20
2.14 ガバメントクラウドのサービスレベル	21
2.15 個人情報取り扱いの考え方 (PIA)	22

3. アカウントと共通機能

3.1 ガバメントクラウド利用全体構成	24
3.2 アカウント	25
3.3 ユーザー	26
3.4 ユーザー権限	27
3.5 システム環境	28
3.6 命名規則	29
3.7 時刻同期	30
3.8 名前解決	31
3.9 ログ管理	32

4. ネットワーク

4.1 ネットワーク概要	34
4.2 ネットワーク基本方針	35
4.3 ネットワークセグメント	36
4.4 インターネット接続	37
4.5 次期分離モデル	38

5. ガバナンス

5.1 統制内容	40
5.2 テンプレート	41
5.3 サポート	42
5.4 リソース集約	43



目次②

6. セキュリティ	
6.1 認証認可	45
6.2 暗号化	46
6.3 ファイアウォール	47
6.4 不正侵入対策（IDS）	48
6.5 モニタリング	49
6.6 ウイルス・マルウェア対策	50
6.7 脆弱性対策	51
6.8 セキュリティ分析	52
7. 監視	
7.1 監視設定	54
7.2 監視通知	55
8. 可用性	
8.1 冗長構成方針	57
9. バックアップとリストア	
9.1 バックアップ	59
9.2 リストア	60
10. 運用保守	
10.1 運用体制	62
10.2 役割分担	63
10.3 遠隔保守	64
10.4 予算・コスト管理	65
10.5 AWSのメンテナンス	66
10.6 マネージドサービスの変更・廃止	67
11. 移行	
11.1 モダン化の推進	69
11.2 Replatform/Rebuild	70
11.3 インフラのIaC化	71
11.4 データ移行と切替	72
改訂履歴	73



デジタル改革推進課
Digital Innovation Promotion Division

1. はじめに



1.1 はじめに



• 本文書の目的

- 国から示されているガバメントクラウド関係文書の概要を解説するとともに、名古屋市(以下「本市」という。)のガバメントクラウド利用にかかる基本的な方針を示すものです。

• 本文書の利用想定

- ガバメントクラウドの利用または利用を検討している所属において、システムの企画、予算要求、調達、運用の各段階で、関係職員および委託事業者が閲覧することを想定しています。
- ガバメントクラウドを利用するシステムの関係職員および委託事業者は、必ず本文書の内容を確認し、方針内容に準拠するよう留意してください。

• 本文書で記載する用語 サービス等

- 解釈違い防止のため、クラウドの用語やサービス名等については、本市の主たるCSPであるAWSのものを採用します(他CSPの場合については、用語やサービス名を同等のものに置き換える必要があります)。
- また契約や手続等においては単独利用方式の内容で記述します。
- デジタル改革推進課(または統合運用管理補助者)関係部分は 、業務システム所管課(またはASP事業者)関係部分は  のアイコンで表現します。

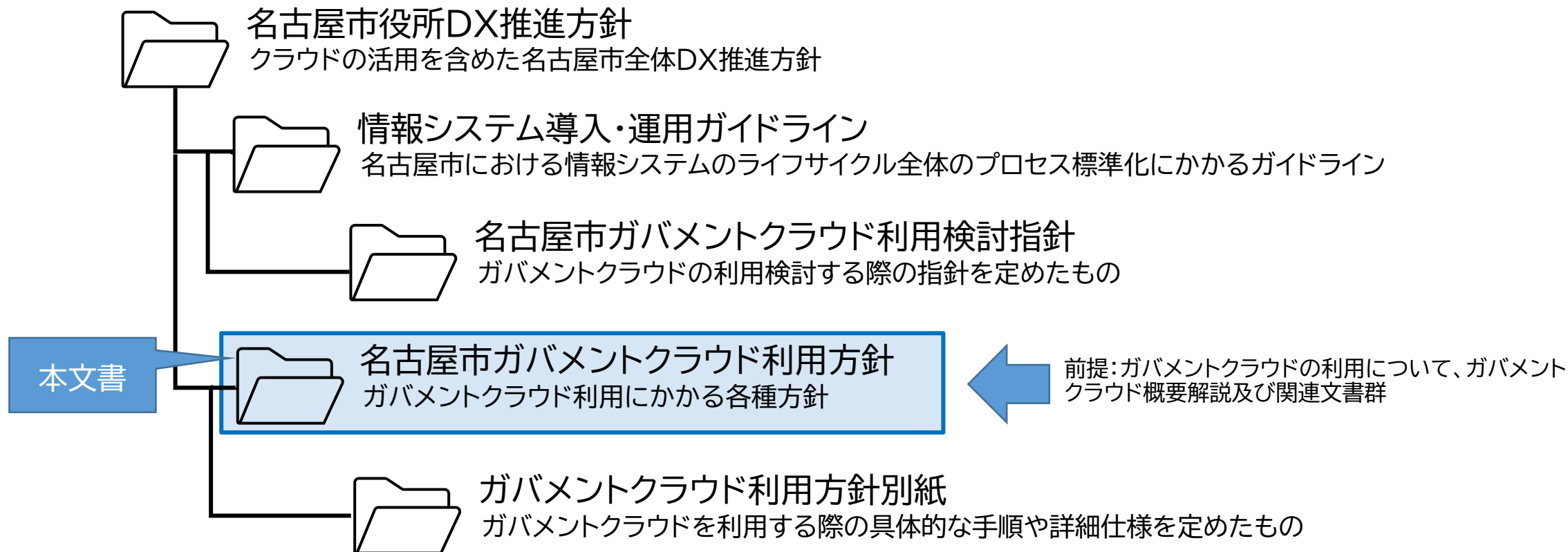
• 本文書の改定方針

- 本文書は2025年3月時点において作成しています。今後、国が提示する基準や文書等の改訂等に伴い、本資料の内容を修正・更新する事があり得ます。



1.2 他文書との関係

本文書の位置づけは以下の通り。





デジタル改革推進課
Digital Innovation Promotion Division

2. ガバメントクラウドの概要



2.1 ガバメントクラウド導入の経緯

公共領域でのクラウド利活用について、政府において段階的に検討が進められ、最終的に自治体や政府共通のクラウドサービスの利用環境としてガバメントクラウドが整備された。

- **2013年 第一期政府共通プラットフォーム(政府が調達するプライベートクラウド)**
 - 2009年の霞が関クラウド構想を元に政府情報システムの統合・集約化を目指した
- **2020年 第二期政府共通プラットフォーム(パブリッククラウド:AWS)**
 - 2018年の政府情報システムにおけるクラウドサービスの利用に係る基本方針(以下「政府クラウド基本方針」)において、クラウド利用を第一候補とするクラウド・バイ・ディフォルト原則(クラウドファースト)が定められ、その受け皿として整備された
- **2021年 ガバメントクラウド(複数のパブリッククラウド環境)**
 - 2021年のデジタル社会の実現に向けた重点計画(以下「重点計画」)において政府情報システムのクラウドは原則ガバメントクラウドを利用することとされた
 - 2022年に政府クラウド基本方針が改正され、単なるIaaSとしての利用のみならず、スマートなクラウド利用を行うこととされた(クラウドスマート)
 - 2022年の地方公共団体情報システム標準化基本方針(以下「標準化基本方針」)にて標準準拠システムの利用はガバメントクラウドの利用を第一に検討すべきとされた
 - 2024年のデジタル行政推進法改正により、全ての公共情報システムはガバメントクラウドの利用検討努力が課せられることになった



2.2 クラウドの特徴とメリット

- **サーバー機器の調達や保守管理の事務が不要になる。**
 - 機器更新の際の長期間にわたる調達事務や、機器保守にかかる委託費用が負担となっていました。クラウド移行後はこの作業が不要になります。
 - 機器調達の準備期間が不要であるため、システムの開発導入や構成変更が迅速に行えます。
- **スケーリングにより繁忙期対応が容易になる。**
 - 一時的に仮想サーバーを高性能なものに置き換えたり、自動的に仮想サーバー台数を増やす機能の活用により、繁忙期や年次処理の対応が容易になります。
 - ピークにあわせた機器を調達する必要がなくなるため、CPUやメモリ使用率等の定期レポート作成が不要となり、運用経費が低減できます。
- **閑散期や時間外は不要なサービスを停止することにより費用を低減できる。**
 - クラウド利用料は従量課金であり、運用上の工夫により費用を低減できます。
- **災害対策が容易になる。**
 - バックアップサイトの活用により、従来の災害対策手段である物理テープの遠隔地保管に比べ、RTO(目標復旧時間)やRPO(目標復旧時点)を短縮することが可能です。



2.3 ガバメントクラウドの特徴

- 国がセキュアかつクラウドネイティブ(クラウドのメリットを最大限活かしたシステムであること)なシステム導入に適したCSPを選定し、複数利用できるようにする
 - ISMAP(政府情報システムのためのセキュリティ評価制度)に登録されているCSPから選定されます。
 - かつクラウドスマートを実現するための技術仕様等を満たしているCSPが選定されます。
- 国が独自のガバナンスを適用して各省庁や地方公共団体に提供する
 - 国が最低限のセキュリティガードレールを設定します。
 - 情報セキュリティ対策上の手続きが簡略化されます(基準への適合確認やデータ消去時の確認作業等)。
- 国が直接CSPと契約することによりデータ主権の課題を解決
 - データセンターは国内に限定され、データポータビリティが確保されています。
 - 国際法上の主権免除通知要請等、有事の際のCSPとの折衝は国が行います。
 - 契約の解釈は日本法に基づき一切の紛争は日本の裁判所が管轄となります。
- 費用や稼働状況を可視化
 - 国とCSPとの直接契約により中間マージンを排除するとともに利用料がインターネット上に公開されており、透明性が確保されています。またスケールメリットによるディスカウントを享受できます。
 - 稼働状況や利用状況が可視化できるダッシュボードが提供される予定であり、継続的な改善や最適化に利用できます。



2.4 ガバメントクラウド上に構築可能なシステム

国の各種方針と「名古屋市役所DX推進方針」を踏まえ、本市においては以下の取り扱いとします。

1. 標準準拠システム

- 標準準拠システムは、原則ガバメントクラウドを利用するものとします。
- ガバメントクラウドに対応する事業者が無い場合等、やむを得ない場合は他のクラウド環境も可能としますが、当該環境(接続回線含む)はデジタル改革推進課(以下「デジ課」という。)の責任範囲外となり、所管課は「当該環境が性能面や経済合理性等を比較衡量してガバメントクラウドより総合的に優れている」旨の説明責任を負います。

2. 標準準拠システム以外の公共情報システム

- 標準化対象20業務を取り扱うシステムにおいて、標準仕様に含まれないため標準準拠システムと分離されるシステム(標準化対象外事務、標準化対象外機能及び独自機能)についても原則ガバメントクラウドを利用するものとします。
- それ以外のシステムについてはガバメントクラウドの利用検討独力義務が課せられます。利用検討の内容については名古屋市ガバメントクラウド利用検討指針を参照ください。

以下、ガバメントクラウド上に構築するシステムを総称して「業務システム」といいます。



2.5 ガバメントクラウドの利用方式

本市はマルチベンダ環境であり、既存庁内環境と同等のセキュリティとガバナンスを確保するため、単独利用方式を採用します。

1. 単独利用方式

- 地方公共団体がクラウドの運用管理を主体的に行う。
- 複数の業務システムに対し、地方公共団体として統一的なルール適用や運用が可能な反面、事業者は個別運用を強いられる。
- 統一的なルールや運用方法の内容を決める必要がある。

2. 共同利用方式

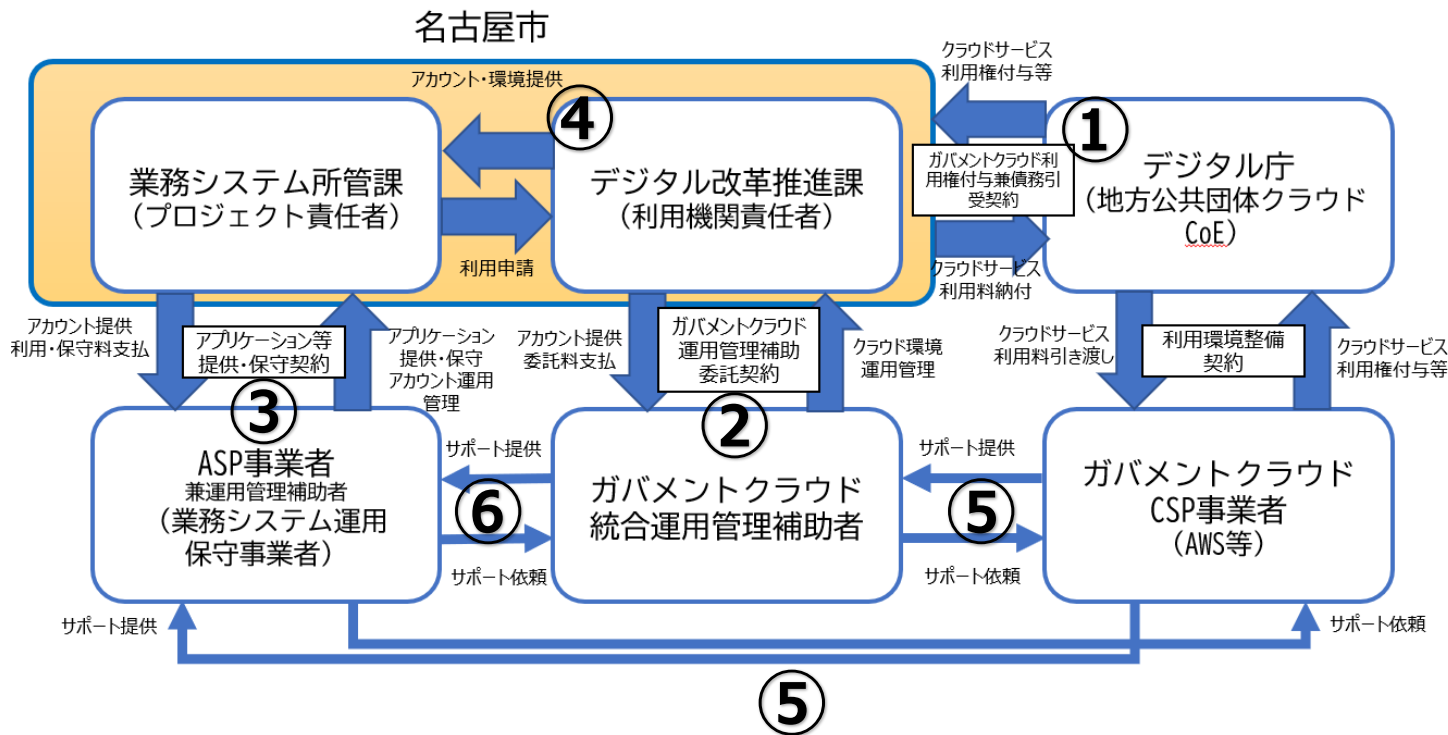
- クラウドインフラ等の共同利用を受託する事業者(運用管理補助者)がクラウドの運用管理を主体的に行い、地方公共団体はその提案を受ける。
- アカウント分離、ネットワーク分離、アプリケーション分離の3つの方式がある。
- 運用管理負担は低減できるが、自団体の望むルール適用や運用が出来ない場合がある。



2.6 ガバメントクラウドにかかる契約と手続き

本市のガバメントクラウドに関する契約等は以下のとおりです。なお利用申請の詳細については別紙2「ガバメントクラウド利用申請手順」を参照ください。

- ① デジ課がデジタル庁とガバメントクラウド利用権付と兼債務引受契約を締結します。
- ② デジ課がガバメントクラウド全体の運用管理を行う事業者(以下「統合運用管理補助者」という。)を選定し、ガバメントクラウド運用管理補助委託契約を締結します。
- ③ 各業務システム所管課は業務システムの提供を行うASP事業者兼運用管理補助者(以下「ASP事業者」という。)とアプリケーション等提供・保守契約を締結します。
- ④ 各業務システム所管課がデジタル改革推進課を通じてガバメントクラウドの利用申請を行い、それに基づいてデジタル庁からアプリケーションの構築に必要なアカウントと環境が提供されます。
- ⑤ 技術的サポートが必要になった場合はASP事業から直接CSP事業者(AWS等)にサポート依頼を行います。
- ⑥ 本市のガバメントクラウド環境にかかる問い合わせについては、ASP事業者から統合運用管理補助者に行います。



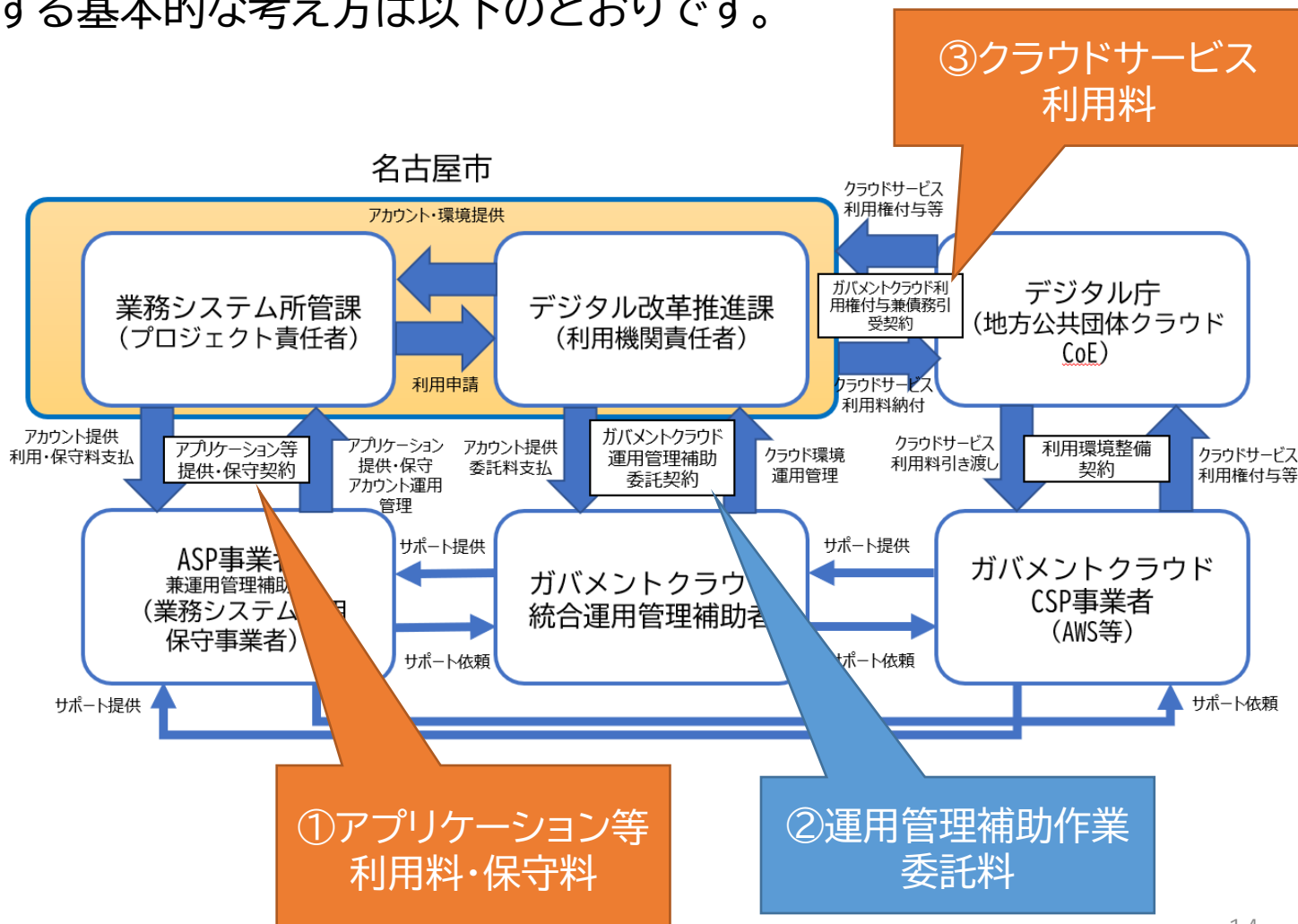


2.7 ガバメントクラウドにかかる経費

ガバメントクラウドの経費負担に関する基本的な考え方は以下のとおりです。

- ① アプリケーション等利用料・保守料については業務システム所管課がASP事業者との契約を元に料金を支払います。予算確保も業務システム所管課で行います。
- ② ガバメントクラウド全体の運用管理にかかる作業(運用管理補助作業)の委託料や接続回線の費用はデジ課が負担します。
- ③ クラウドサービス利用料については、支払いはデジ課が一本で行いますが、業務システムの各環境にかかる費用については業務システム所管課が予算を確保し、配当替で対応します。(従来のサーバーリース費用等に相当します)

※ クラウドサービス利用料の積算及び予算要求については、別紙1「クラウドサービス利用料積算」を参照ください。





2.8 ガバメントクラウドのCSP

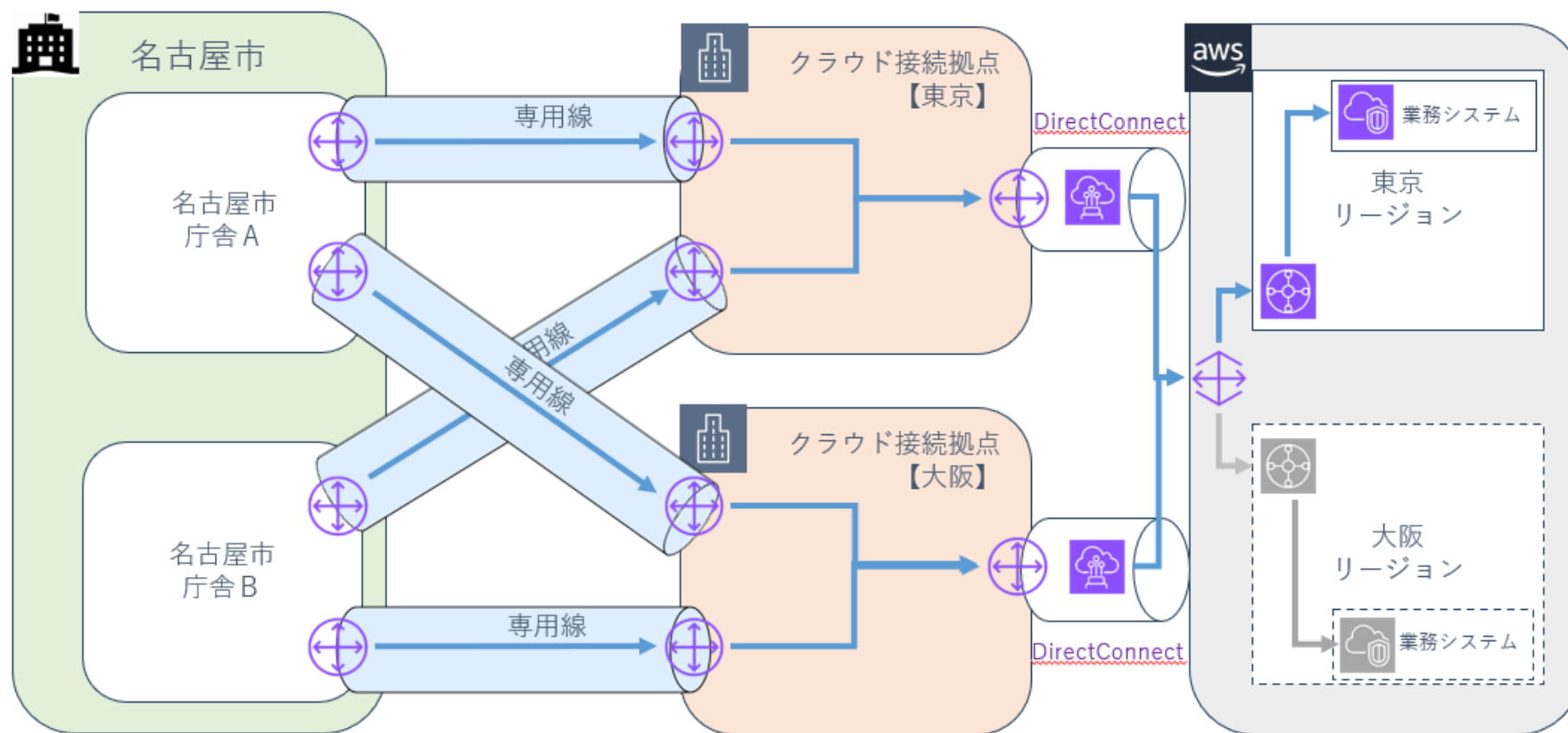
本市の主たるCSPとしてAWSを選定します。ただしSaaS等を中心に特定機能に特化する場合は他のCSPも容認するものとします。

- **ガバメントクラウドで選択可能なCSPは以下の5つ**
 - Amazon Web Services(AWS)
 - Google Cloud(GC)
 - Microsoft Azure(Azure)
 - Oracle Cloud Infrastructure(OCI)
 - さくらのクラウド ※2025年度までに所要の条件を満たすことを前提とする
- **単独利用方式は地方公共団体が、共同利用方式はベンダがCSPを選定(FAQNo.250)**
- **政府ガイドラインでCSPを複数用いるマルチクラウドは忌避されている**
 - マルチクラウドはコストが増大することが多いため、真に必要性がある場合を除いては避けること。
 - 技術的な合理性と経済的な合理性を持たないマルチクラウドは厳に避ける必要がある。
- **AWSの選定理由**
 - シェア・第三者評価・技術者数・マネージドサービス数で優位性があり、先行事業での実績がある。
 - RFIの結果から全業務で対応可能なCSPはAWSのみ。



2.9 ガバメントクラウド接続回線

ガバメントクラウドへのネットワーク接続回線については、デジ課が専用回線を独自調達し、利用します。
これにかかる契約や予算確保はデジ課で行います。

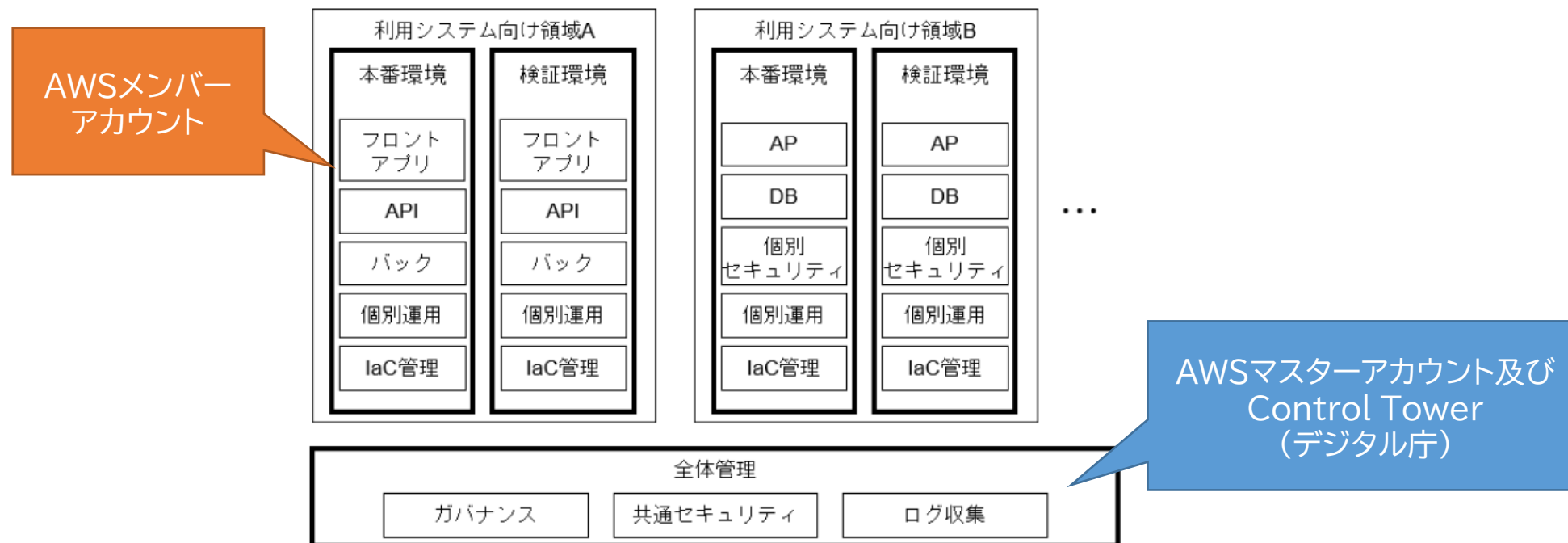




2.10 ガバメントクラウド環境

ガバメントクラウドの利用システム向け領域は、デジタル庁をマスターとするAWS Organizationsのメンバーアカウントの集合体であり、各業務システムに必要なとする環境用のアカウントが付与されます。

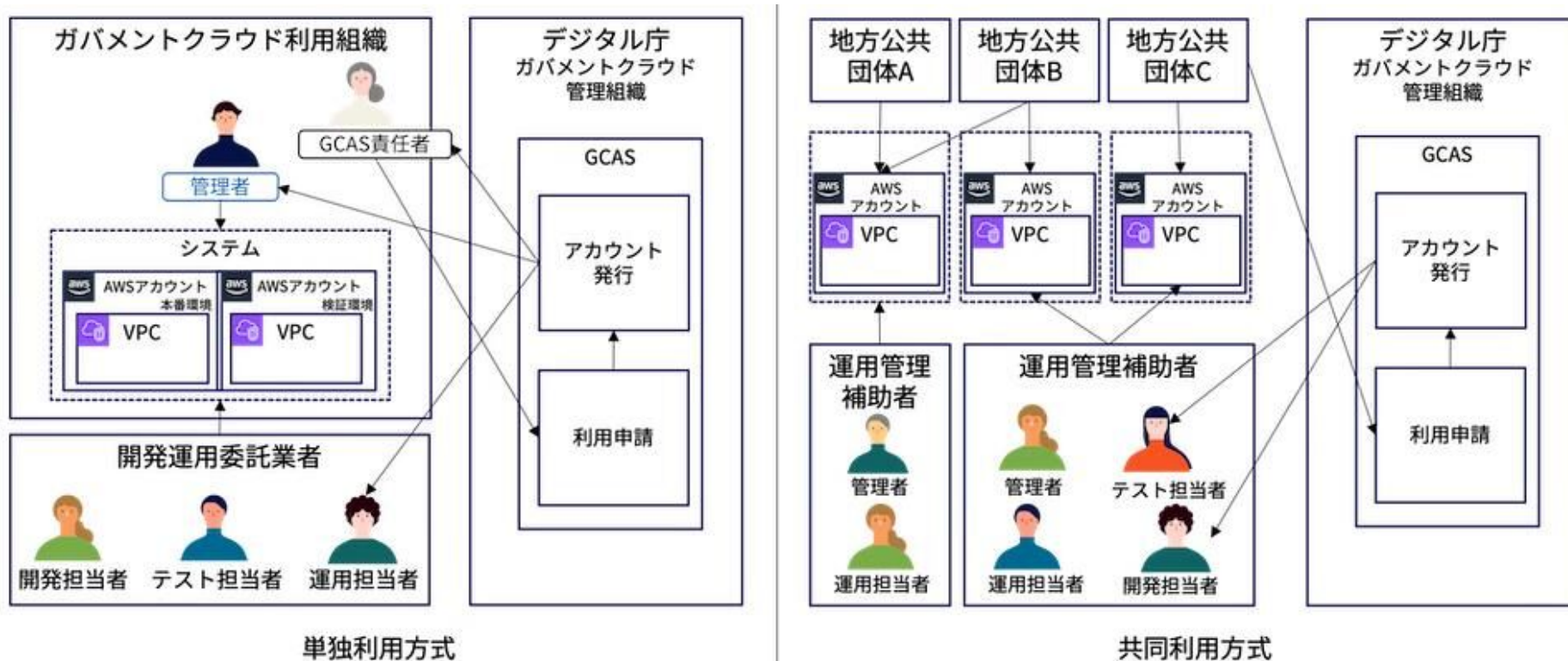
なお、開発用途でアカウントを利用する事はできませんが、例外的にCI/CD(継続的インテグレーション/継続的デリバリー)手法を用いる場合に限り、ガバメントクラウドで指定するツールやテンプレートを用いてCI/CD用のアカウントを利用する事ができます。





2.11 ガバメントクラウド環境利用権限

ガバメントクラウド環境とその利用権限は、GCASというデジタル庁のオンボーディングサイトを通じてデジタル庁に利用申請を行い、発行を受けます。またASP事業者作業員やサービスに必要となるロールはASP事業者が適宜作成可能です。



- The diagram illustrates the division of responsibility for cloud services across three levels:

 - City's Responsibility (本市の責任範囲):**
 - Development/Operation System (開発運用体制)
 - Security Management (セキュリティ管理) (Certification, ID, PaaS/IaaS/Others)
 - Data (データ)
 - Application (アプリケーション)
 - Managed Service Composition (マネージドサービス構成)
 - Middleware/OS (ミドルウェア/OS)
 - Network Composition (ネットワーク構成) (In-system/Internet connection)
 - Individual Domain Responsibility (個別領域の責任範囲):**
 - Guardrail (全体利用ポリシー) (ガードレール)
 - Template (リファレンス構成) (テンプレート)
 - Environment (払い出し) (環境)
 - Application Recommendation Composition Guide (アプリ推奨構成ガイド)
 - Consultation (コンサルテーション)
 - Training (トレーニング)
 - Gateway Cloud Window (ガバメントクラウド窓口)
 - Gateway Cloud Operation System (ガバメントクラウド運用体制)
 - CSP Responsibility (CSPの責任範囲):**
 - Managed Service (マネージドサービス)
 - Cloud Base (クラウド基盤) (Compute, Storage, Network, Region, etc.)
 - Cloud Base Security Management (クラウド基盤セキュリティ管理)
 - CSP Support (24/365) (CSPサポート)

* 平日9:00-17:00



2.13 ガバメントクラウドテンプレート

- ガバメントクラウドテンプレートには自動適用テンプレート、必須適用テンプレート、サンプルテンプレートの3種類があります。
- 自動適用テンプレートは、デジタル庁が情報セキュリティ上最低限必要となる機能について予め共通的に適用するものです。(セキュリティガードレール)
- 必須適用テンプレートは自動適用テンプレートと同様ですが、自治体側でパラメータ設定を行った上で適用を行う必要があるものです。
- サンプルテンプレートは各種リソースやアーキテクチャのIaC(Infrastructure as Code、環境構築をコードで行うこと)サンプルで、統合運用管理補助者やASP事業者が環境構築時に活用できます。
- これ以外に本市独自の統制テンプレート(以下「本市テンプレート」という。)も作成します。

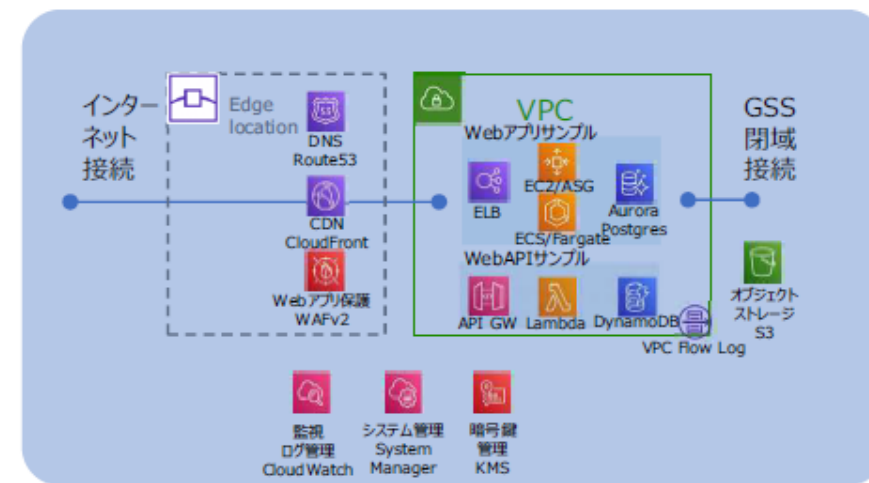
サンプル
テンプレート

必須適用
テンプレート

自動適用
テンプレート

テンプレートの全体像

ガバメントクラウド利用組織環境



アカウント
アクティビティ
モニタリング
Cloud Trail

構成管理
Config

セキュリティ
パフォーマンス
評価
Trusted Advisor

マネージド
ルール
の有効化
Config Rule

アカウント
権限管理
IAM

コスト
管理
Budgets

メッセージング
プッシュ通知
SNS



2.14 ガバメントクラウドのサービスレベル



ガバメントクラウドのサービスレベルはCSPのサービスレベルに準じます。具体的な数値はCSPの公表値を参照します。(https://aws.amazon.com/jp/legal/service-level-agreements/)

以下の各構成要素の積から業務システムが非機能要件の稼働率を満たすかどうかを判別します。

- **ガバメントクラウド接続回線**

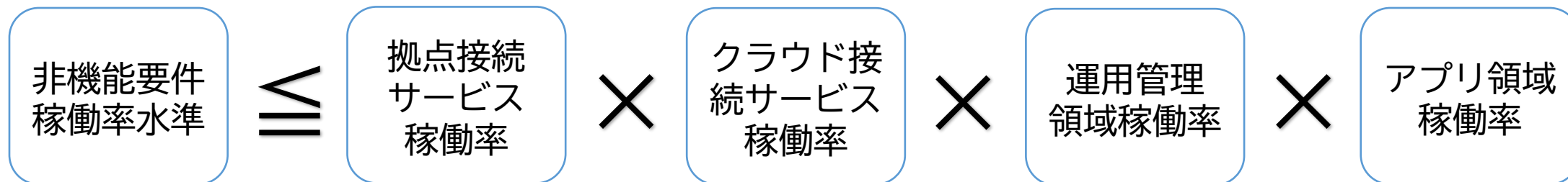
- 拠点接続サービスの稼働率は99.99%です。
- クラウド接続サービスの稼働率は99.99%です。

- **各標準準拠システムアプリ領域**

- ASP事業者がシステム構成と用いるCSPの各サービスの稼働率等から算出を行います。

- **運用管理領域**

- 運用管理領域のTransit Gatewayの稼働率は99.99%です。Route53の稼働率は100%とします。



関係資料: 利用について 3.1.5、4.2、ガバメントクラウド利用権付与兼債務引受契約 第12条、等



2.15 個人情報取り扱いの考え方(PIA)



- ガバメントクラウドへの移行について、対象業務が個人番号利用事務の場合については特定個人情報の保管場所やリスク対策内容に変更が生じますので、特定個人情報の取り扱いに関する重大な変更として、PIAの再実施が必要となります。
- デジタル庁及びCSPは個人情報が含まれる本市の個別領域にアクセスする事は出来ません。このため本市とデジタル庁が締結するガバメントクラウド利用権付与兼債務引受契約は番号法に規定する特定個人情報ファイルの取扱いの委託に該当しないこととなります。
- 一方で業務システム所管課がASP事業者と締結するアプリケーション等提供・保守契約については、特定個人情報ファイルの取扱いの委託に該当します。
- PIAの進め方については「システム標準化に伴う特定個人情報保護評価について」を参照してください。

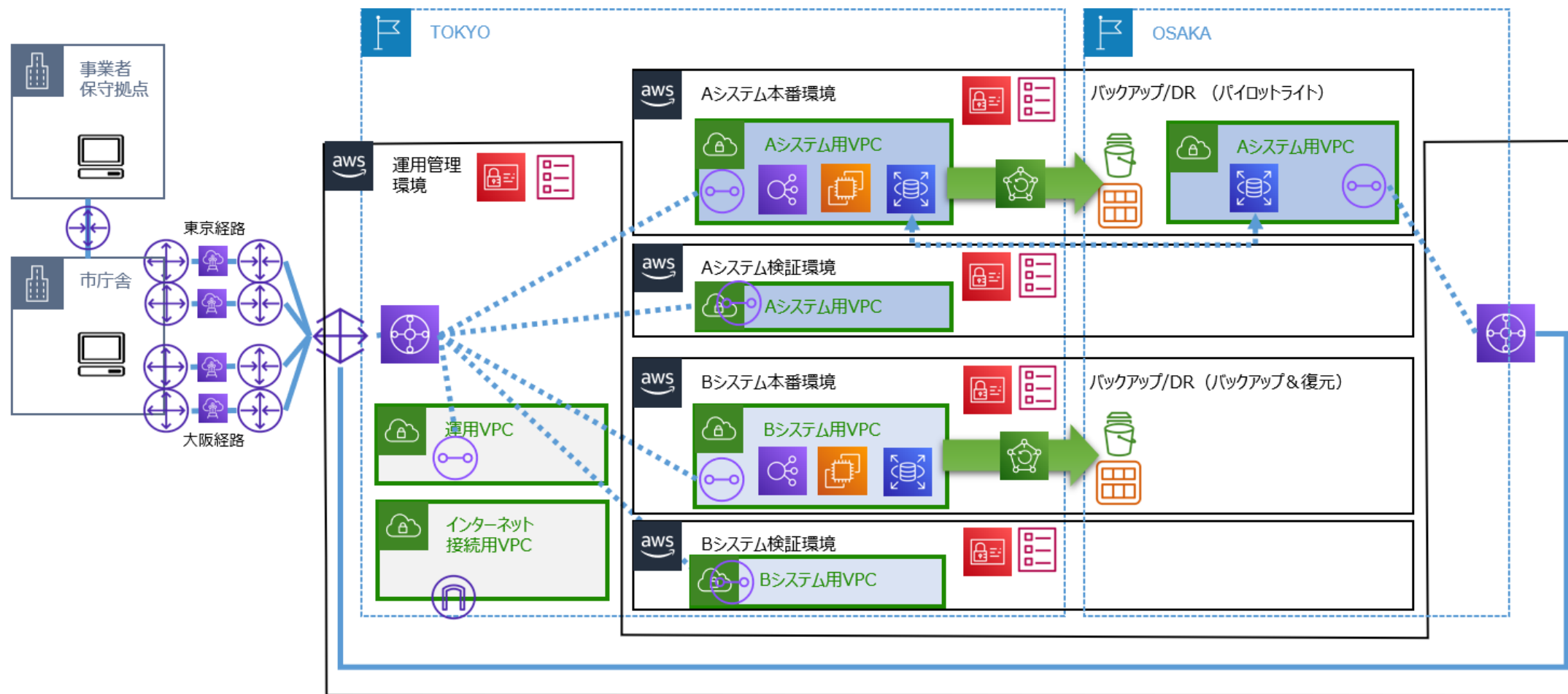


デジタル改革推進課
Digital Innovation Promotion Division

3. アカウントと共通機能



3.1 ガバメントクラウド利用全体構成





3.2 アカウント



- **基本方針**

- 運用管理環境、本番環境、検証環境の3つのランドスケープをアカウント単位で分離します。
- 業務システムごとに本番環境と検証環境のアカウントを割り当てます。必要に応じサブシステム単位で割り当てすることも可能とします。

- **運用管理アカウント**

- デジ課が管理し、統合運用管理補助者が運用します。
- 各業務システムのVPCと庁内ネットワークとを接続します。
- インターネット接続環境(基盤系、マイナンバー利用事務系、LGWAN接続系)を設け、各業務システムが更新プログラムやウイルスパターンファイルを取得できるようにします。

- **本番環境アカウント**

- 業務システム所管課が管理し、ASP事業者が運用します。
- 本番環境用VPCを有し、その中に業務システムの本番環境用リソースを構築します。
- マネジメントコンソール経由で本番業務データを参照することは禁止されます。

- **検証環境アカウント**

- 業務システム所管課が管理し、ASP事業者が運用します。
- 検証環境用VPCを有し、その中に業務システムの検証環境用リソースを構築します。
- 本番業務データを扱う事は禁止されます。

- **CI/CDアカウント**

- CI/CDパイプライン構築を行う場合のみ導入可能です。業務システム所管課が管理し、ASP事業者が運用します。

関係資料: ガバメントクラウド概要解説 3.3.1、ガバメントクラウド手続き概要 5.2.2



3.3 ユーザー



- ガバメントクラウドにおいてはRootユーザーやIAMユーザーは利用せず、GCASアカウントを用いたIdC※ユーザーを利用します。
 - IAMユーザーの利用は原則禁止されていますが業務所管課においてサードパーティ製品利用等の理由でIAMユーザーやアクセスキーが必要になる場合、デジ課に相談ください。
 - 本来Rootユーザーの権限を必要とする操作(誤って設定したS3バケットポリシー削除等)はデジタル庁に依頼します。
- IdCユーザー
 - 利用者はGCASアカウントと同期されたフェデレーションユーザー(IdCユーザー)を利用して認証およびアクセスが制御されます。
 - GCASアカウントのメールアドレスをIdCのユーザー名として利用しています。
 - IdCユーザーは管理者とそれ以外の2つの権限種別があり、GCASアカウント申請に基づき割り当てられます。
 - 管理者権限を持つGCASアカウントは、運用管理アカウントの場合は統合運用管理補助者が管理し、業務システムの本番環境と検証環境の場合はASP事業者が管理します。
 - 作業は、必要に応じてポリシーが設定されたロールを引き受けて行います。
 - 詳細は別紙2「ガバメントクラウド利用申請手順」を参照ください。

※IdC

AWS IAM Identity Centerの略称であり、一組織で複数のAWSアカウントを運用する際の認証及びアクセス制御を一元化するためにリリースされたサービスです。ガバメントクラウドでは、デジタル庁が管理するAWSアカウント内に構成されています。

ガバメントクラウドではGCASで利用しているアプリケーション、SaaS、各CSP環境とCloud IdentityをSAML規格に基づいてシングルサインオン連携を実装しています。AWS環境では認証・アクセス権管理サービスのAWS IAM Identity CenterとSAML連携し、ユーザー情報を同期します。



3.4 ユーザー権限



• IAMロール

- 統合運用管理補助者およびASP事業者が管理者権限をもつIdCユーザーを用いて、システムに必要となるIAMポリシー、IAMロールを設定します。
- IAMポリシー、IAMロールの方針の詳細については各システムで決定します。
- 本市テンプレートにて適用されたIAMポリシーやIAMロールを削除する事は禁止します。
- GCASにおいてマイナンバー利用事務系本番環境用のポリシーを記述したjsonファイル(GovCloudLgDataRegidencyアクセス許可セット)が提供されていますので、必要に応じて利用します。



3.5 システム環境

各システムの環境については、以下の方針とします。また、本市テンプレートの適用により、VPCを含む最小限のシステム環境が構築でき、ASP事業者はそれを活用して業務システムを構築します。

- ロケーション(リージョン)

- ガバメントクラウドの制限により国外リージョンは利用できません。
- 東京リージョンをメインサイトとし、大阪リージョンをバックアップ/DRサイトとします。

- VPC

- 業務システムの本番環境、検証環境ごとに作成します。
- 運用管理アカウントにはネットワークセグメントごとに運用管理VPCとインターネット接続用VPCを作成します。

- AZ

- ap-northeast-1a, ap-northeast-1c の2つAZを用いたマルチAZ構成を基本とします。
- 必要な場合には、ap-northeast-1d も利用します。

- サブネット

- 原則は外部へのルートを持たないプライベートサブネットであり、インターネット接続系ネットワークの業務システムと運用管理アカウントのインターネット接続用VPCのみパブリックサブネットを構築します。



3.6 命名規則



本市統一ルールとして、クラウドリソースに以下の通り7種のタグを付与し、管理を行います。
これ以外に業務システムにおいて必要に応じてタグを追加する事も可能です。

これらの詳細な命名規則は別紙4「命名規則」を参照ください。

・ タグ一覧

1. 名称:サーバーやサービスの名称。「TPJRAP01」など。
2. 業務システムID:原則従来のコードを踏襲。住民記録システム「CA」など。
3. 概要:和名のサーバ名称。「APサーバー01」など。
4. ランドスケープ:運用管理、本番、検証
5. OS/データベースエンジン
6. セキュリティ:AWS Inspector用
7. バックアップ:AWS Backup用

・ サーバー名称

- ロケーション、ランドスケープ、業務システムID、サーバー種別、連番の組み合わせで表記します。

・ サービス名称

- サービス識別子、ランドスケープ、業務システムID、用途、連番の組み合わせで表記します。



3.7 時刻同期



全システムにおいて、AWSが提供する時刻同期サービス(Amazon Time Sync Service)を利用します。



3.8 名前解決



AWSが提供するDNSサービス(AWS Route53)を利用します。各業務システムでDNSサーバーを設けて併用する事も可能です。

基本方針

- 庁内→ガバクラは、Route53 ResolverにてHosted Zoneに問い合わせ転送します。
- ガバクラ→庁内は、Route53 Resolverにて庁内DNSサーバーに問い合わせ転送します。各業務システムにてDNSサーバーを設ける場合も同様です。
- AWSの名前解決を必要とする各リソースについて、Hosted Zone(プライベート)にレコードを登録します。

• ドメイン

- 用途、ランドスケープ、業務システムID、ネットワーク種別を組み合わせたドメイン名とします。詳細は別紙4「命名規則」を参照ください。各業務システムにてDNSサーバーを設ける場合もこのドメイン名とする必要があります。
- Hosted ZoneにAレコードとして、IPアドレスまたはエンドポイント名を登録します。

• Hosted Zone

- 運用管理アカウントの運用管理VPCに作成し、ホストゾーンの関連付けで業務システムアカウントと連携し、全体を管理します。
- インバウンド用/アウトバウンド用のエンドポイントを運用管理VPCのRoute53用サブネットにマルチAZで作成します。
- 大阪リージョンへのエンドポイント配置は必要に応じて実施します。



3.9 ログ管理



システム障害やインシデント対応に備え、必要なログを収集します。全てのログについてはS3にて1年間保存した後、アーカイブ化して必要な期間保存します(Glacier等を利用)。アーカイブされた各ログの保存期間は別途定めます。

また、本市テンプレートの適用により、運用管理アカウントにてこれらのログの集約 閲覧ができるようにします。

- **AWSサービスのログ**

- ネットワークフローログ(VPCフローログ)
- 監査ログ(CloudTrail、Config)
- セキュリティログ(CloudWatch)

- **各サーバーのログ**

- OSのイベントログ(CloudWatch)

なお上記以外の、業務システムにて管理が必要となるアプリケーションログや個人情報ログ等については、各業務システムにて管理方法を定めます。



デジタル改革推進課
Digital Innovation Promotion Division

4. ネットワーク



4.1 ネットワーク概要

- 集中管理

- 運用管理アカウントにおいて、東京リージョンと大阪リージョンにTransitGateway(TGW)を設置し、全てのネットワーク通信を集約します。
- 運用管理環境および各業務システムのVPCはTGWを経由し、他のVPCや庁内ネットワークと通信します。

- 三層分離

- マイナンバー利用事務系とLGWAN接続系のネットワークのセグメントを分離します。
- 接続回線においてもVLANでセグメントを論理的に分離します。このため、デジタル庁の示す推奨構成とは異なる構成となります。
- 標準準拠システム及び標準準拠システムと密接に連携する関係システムについては、実際に個人番号を扱うシステムかどうかに関わらず、マイナンバー利用事務系ネットワークに所属するものとして扱います。

- 本市テンプレートによる構築

- 業務システムのアカウントに本市テンプレートを適用することで、VPC、TGWアタッチメント、アタッチメント用サブネットとそのネットワークACLが構築され、自動的に庁内との疎通と三層分離環境が確保できます。
- その後、ASP事業者はこの環境に業務システムを構築します。なお、許可なくテンプレート由来のリソースを修正したり、VPCピアリングを構築したりすることは禁止です。



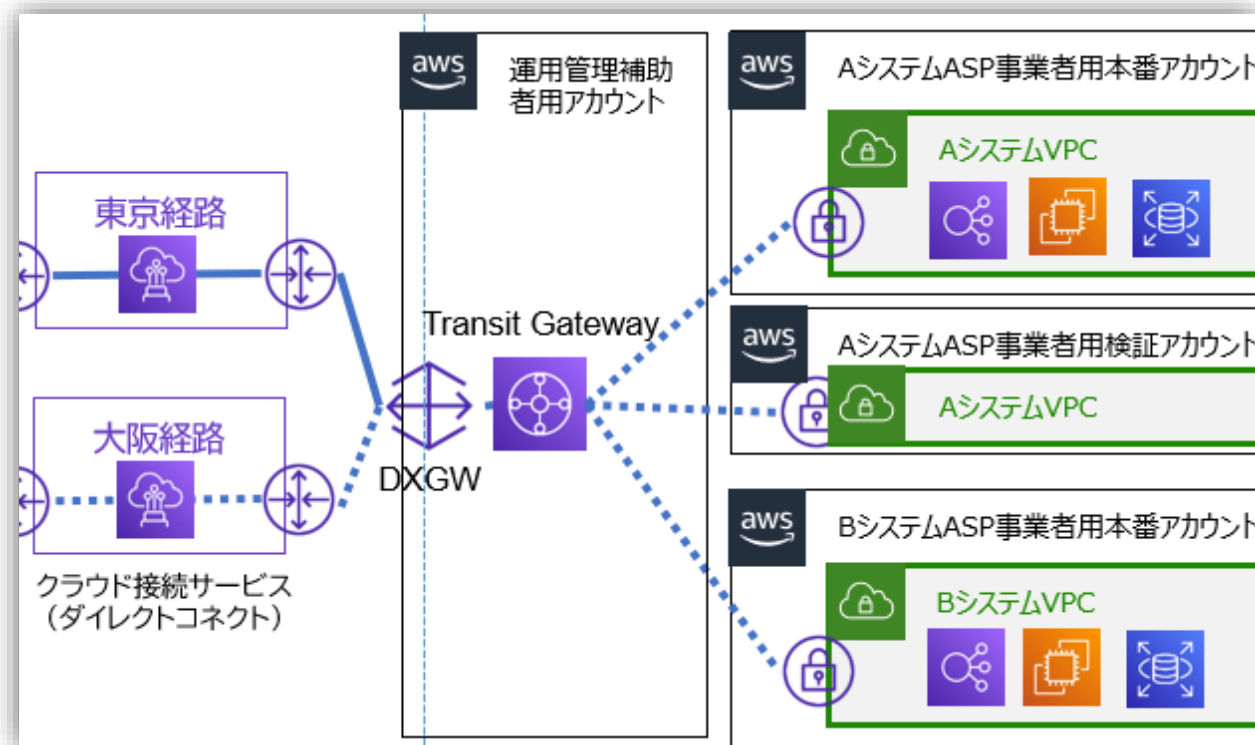
4.2 ネットワーク基本方針

• AWS内の通信

- TGWを仲介してVPC間の通信を行い、VPCピアリングは原則禁止とします。
- 本市テンプレートにより、VPCに加えてTGWアタッチメントとアタッチメント用サブネットがマルチAZで構成され、TGWと接続されます。

• 庁内とAWS間の通信

- DirectConnect(DX)による閉域網接続で行います。
- DXからはTransitVIFを利用して、Direct Connect Gateway(DXGW)に接続し、その後TGWに接続します。
- 接続回線における三層分離方式については、VLANで各層を分離し、別々のVIFとして引き込みを行い、分離します。
- ただし認証サーバ等、マイナンバー利用事務系からもLGWAN接続系からもアクセスする必要があるものについては、別途仕組みを構築します。





4.3 ネットワークセグメント

ガバメントクラウドは本市庁内ネットワークの延伸であり、同じプライベートネットワーク空間として扱います。このため、本市ネットワーク管理者が各CSPのガバメントクラウド用セグメントのIPアドレス範囲(CIDR表記)を割り当てます。

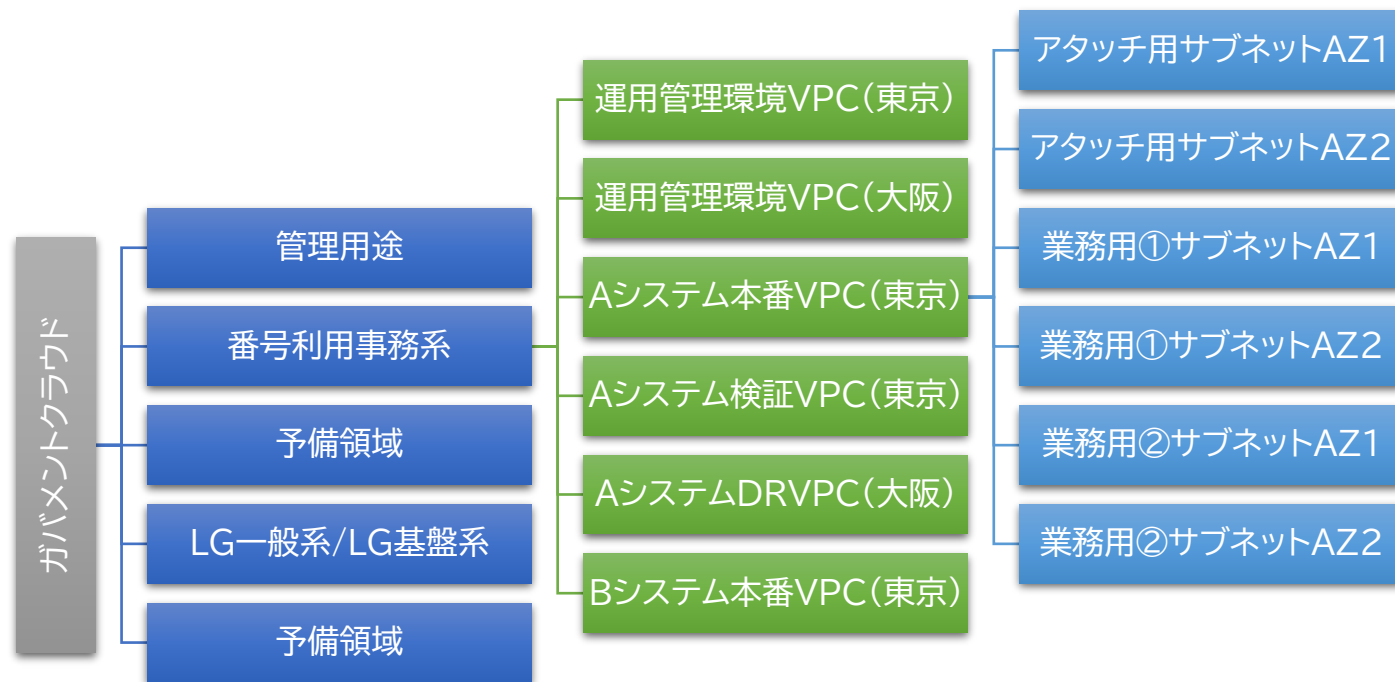
IPアドレス割り当て方針の詳細については別紙3「CIDR割当方針」を参照ください。

• VPC

- 本市ネットワーク管理者が、ガバメントクラウド用セグメントのIPアドレス範囲から、各システムのランドスケープのVPCに割り当てるIPアドレス範囲を決定し、統合運用管理補助者を通じてASP事業者に通知します。
- 基本は23bitセグメント単位とします。

• サブネット

- TGWアタッチメント用サブネット(2つまたは4つ)については、統合運用管理補助者がIPアドレス範囲を決定します。
- それ以外のサブネットについては、ASP事業者がVPCのIPアドレス範囲の中から任意に(重複しないように)IPアドレス範囲を割り当てます。





4.4 インターネット接続

・インターネット接続の方法

- 業務システムの本番環境および検証環境からのインターネット接続は禁止し、運用管理環境のインターネット接続VPCを経由して行うものとします。
- 各業務システムではインターネットゲートウェイおよびNATゲートウェイの設置は禁止します。(インターネット接続系を除く)
- 各業務システムから運用管理環境を経由したインターネット接続を実施する場合は、別紙6「ガバメントクラウドでのウイルス対策・脆弱性対策(WSUS)等について」を参照ください。

・運用管理環境(基盤系)のインターネット接続用途

- インターネット経由でのパッチ適用、ウイルス対策ソフトのパターンファイル更新

・運用管理環境(マイナンバー利用事務系およびLGWAN接続系)のインターネット接続用途

- ソフトウェアのアクティベーション、インターネット経由でのマネジメントコンソール接続

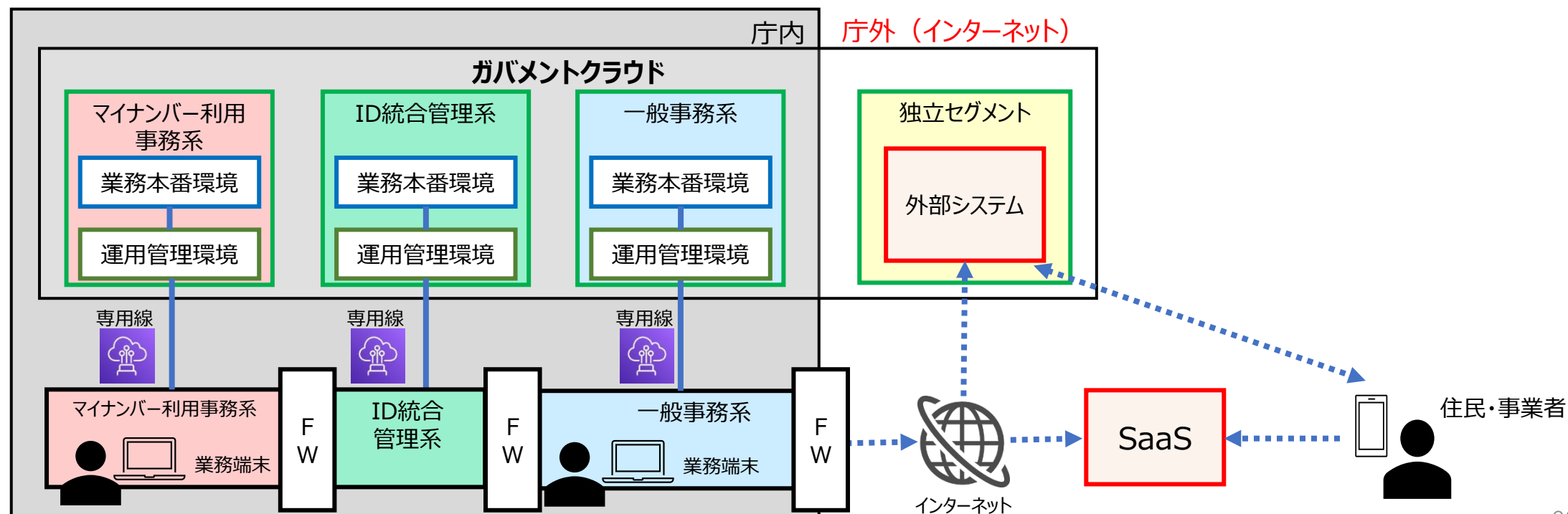




4.5 次期分離モデル

・次期分離モデル

- 2026年(令和8年)5月に次期分離モデルへ移行を予定しており、基盤系はID統合管理系に再編し、ID管理以外のサーバ機器を置かず、認証基盤を集約します。
- ガバメントクラウドの庁内領域(マイナンバー利用事務系、ID統合管理系、一般事務系)は専用線で接続し、庁外領域(独立セグメント)はインターネット回線で接続します。一般利用事務系から直接インターネットにアクセスができるようになり、庁外(インターネット)にある独立セグメントの領域も活用できます。



次期分離モデルの構成イメージ



デジタル改革推進課
Digital Innovation Promotion Division

5. ガバナンス



5.1 統制内容

- デジタル庁が行う統制

- 予防的統制は、SCPにより最低限禁止すべき内容を設定します。
- 発見的統制は、マネージドサービスとアラートの組み合わせにより、設定誤りや違反があった場合にメール等で通知を行います。デジ課と各業務システム所管課はこの内容を確認し、是正する必要があります。
- 具体的な内容は「ガバメントクラウド利用概要(AWS編)」を参照。

- 本市が行う統制

- IAMポリシーにより以下の制限や設定を行い、本市テンプレートで実装します。ただしデジタル庁の統制で足りる場合はこの限りではありません。
 1. 運用管理アカウント以外でのNATゲートウェイ作成(インターネット接続系を除く)
 2. 運用管理アカウント以外でのインターネットゲートウェイ作成(インターネット接続系を除く)
 3. IAMユーザのパスワード複雑性の設定
 4. タグの必須化
 5. 特定のAWSサービスに対する暗号化の必須化
 6. SystemsManagerによるサーバーログイン
 7. サーバー接続の際のIPアドレス範囲制限



5.2 テンプレート

・ガバメントクラウドテンプレート

- 自動適用テンプレートは、デジタル庁が設定するため本市では作業不要です。
- 必須適用テンプレートは、本市で必要なパラメータ設定を行ってから全てのアカウントに適用を行います。
- サンプルテンプレート(必須適用テンプレートに同梱)と定量的計測サンプルテンプレートは、自由にカスタマイズして利用可能ですが、利用結果は業務システム所管課の責任となるため、内容を良く理解した上で任意に活用します。

・本市テンプレート

- デジ課が本市の統制の実現およびネットワーク環境の構築のために配布するテンプレートで、業務システムのアカウントに適用します。以下の内容が含まれています。
 1. 統合運用管理補助者が業務システムアカウントに必要なアクセスを行うためのIAMロールやポリシーの設定
 2. VPCおよびTGWアタッチメントの作成(アタッチメント用のサブネットやネットワークACL含む)
 3. 本市が行う統制を実現するためのIAMポリシー設定
 4. 各種ログの集約及び外部SaaS利用のための設定

適用対象	必須適用テンプレート	本市テンプレート
運用管理アカウント	要	
本番環境/検証環境アカウント	要	要



5.3 サポート



・ガバメントクラウドに関わる事

- ガバメントクラウドに係る問い合わせや情報取得はガバメントクラウドのGCASヘルプデスクを利用してください。(問い合わせをする際、必要に応じてCCにデジ課を追加してください。)

・AWSの技術的な内容に関わる事

- CSPの技術的な内容にかかるサポートについては、CSPのサポートを直接受けてください。(全アカウントで利用可能です)
- サポート内容は下記リンク先のBusinessに加え、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」を含む内容となります。
<https://aws.amazon.com/jp/premiumsupport/plans/>
- またデジタル庁においてAWS Shield Advancedを利用するため、DDos攻撃を受けた場合にAWS Shield Response Team (SRT) のサポートを受けることが可能です。

・本市環境に関わる事

- サポート依頼を起票し、統合運用管理補助者に提出してください。詳細は別途定めます。
- 統合運用管理補助者はサポート依頼内容から、本市環境特有の事項か、ガバメントクラウド環境に関する事項かの切り分けを行い、前者の場合は統合運用管理補助者が回答・対応を行います。後者の場合はヘルプデスクツール経由でデジタル庁に問い合わせ対応を行います。



5.4 リソース集約



デジ課が本市のガバメントクラウドの統制を取りつつコスト最適化を行うため、業務システムで共通して必要になる以下のサービスを集約します。

サービスの集約を希望する場合は、本市テンプレートへの事前設定が必要となるため、デジ課へ申請してください。

- **Route 53 resolver**

- 各システムのRoute 53 Hosted Zoneを運用管理環境に関連付けを行い、各システムではリゾルバールールを作成せず、運用管理アカウントのRoute 53 Resolverを利用します。

- **Private認証局**

- 業務アプリケーションなどで利用するサーバー証明書の発行が必要な場合に個別でPrivateCAの利用は行わず、運用管理環境に共有のPrivateCAを構築し、証明書の発行を行います。
- 市内のルート証明書の管理を簡素化します。

- **一部のVPCエンドポイント**

- 各業務アカウント(各システム)にVPCエンドポイントを配置せず、運用管理環境に配置したVPCエンドポイントを経由する構成にします。
- 対象となるエンドポイントは以下を想定しています。
 - ・CloudWatch用、SystemsManager用、Backup用、SNS用



デジタル改革推進課
Digital Innovation Promotion Division

6. セキュリティ



6.1 認証認可



- マネジメントコンソール

- GCAS シングルサインオン機能を用いて認証を行います。本番相当環境(本番環境、共通運用管理環境、CI/CD環境)にアクセスする際はパスワード認証に加えてFIDO規格準拠(FIDO U2F/FIDO2)のハードウェアMFAトークンが求められます。それ以外の環境はセキュリティキー等による追加認証が求められます。

- コマンドによる操作

- AWS CLIを利用します。なおCloud Shellはデジタル庁により利用が禁止されています。
- アクセスキーの発行も禁止されているため、各システムにおいて適切なIAMポリシーを設定する必要があります。

- 統合運用管理補助者によるスイッチロール

- 統合運用管理補助者が必要があり業務システムアカウントにアクセスする場合、スイッチロールにて行います。

- その他

- 業務システムのサービスで用いる認証情報は、AWS Secrets Managerを活用し、ハードコーディングを避けてください。
- 業務システムのサーバーOSの認証にかかる運用は、業務システムにて方針を決定します。
- 業務システムを利用する際の職員の認証については別途「システム端末導入・認証方式方針」で定めます。
- GCASアカウントで必要となるMFA(ハードウェアMFAデバイス等)は、事業者用は事業者側で準備します。職員用については別途定めます。



6.2 暗号化



• データの暗号化

- 各システムにおいて、暗号化が可能なサービスは原則暗号化を実施します。
- 暗号化はAWSサービスの機能を用いて行い、暗号鍵はAWS KMSにて管理を行います。ただしKMSを利用すると不都合があるサービス(ELBアクセスログにおけるS3等)についてはこの限りではありません。
- アカウントを廃止する場合は、暗号化消去の手法によりデータの論理的削除を行います。

• 通信の暗号化

- インターネット接続系等、業務システムにおいて外部環境からのアクセスを行う場合、通信を暗号化してください。
- またマイナンバー利用事務系については、庁内との通信においても暗号化が必須です。
- 通信暗号化に必要な証明書はAWS CertificateManagerで管理し、CloudWatchやConfigによるモニタリングで有効期限切れを防止します。

• データアクセス制御

- 各システムにおいて、不正にデータにアクセスされないよう、S3バケットに適切なバケットポリシーを設定します。
- EBSについてもEC2にマウントした上でIAMポリシーにより適切なアクセス制御を行います。



6.3 ファイアウォール

- 基本方針

- ネットワークアドレス、プロトコル、ポート番号によりAWSリソースへの許可/拒否を設定します。
- ネットワーク経路の制御は、運用管理アカウントのTGWのルートテーブルで行います。
- プロトコル、ポート制御はセキュリティグループで行い、必要に応じてネットワークACLを併用します。

- TGWでのネットワーク制御

- 統合運用管理補助者が、複数のネットワークセグメント間のアクセスを制御します。
- またインターネット接続用VPCは、運用管理VPC経由でしかアクセスできないよう制御します。

- セキュリティグループでの制御

- 各システムにおいて、リソースや用途ごとに作成し、関連づけを行います。詳細は各システムにおいて方針を決定します。

- ネットワークACLでの制御

- 三層分離を目的として、本市テンプレートにて各業務システムにネットワークACLを設定します。このネットワークACLは業務システム側で変更を行わないでください。
- その他のサブネットのアクセス制御については、各システムにおいて方針を決定します。



6.4 不正侵入対策(IDS)



- 不正侵入検知

- Amazon GuardDutyにより脅威を検出します。
- GuardDutyはデジタル庁の設定により自動的に有効化されます。

- 公開用サーバーの保護

- インターネット接続系における公開用Webサーバーは、AWS WAF(Web Application Firewall)で保護を行います。
- またDDos攻撃についてはAWS Shield Advancedで保護を行います。なお、デジタル庁がAWS Organizationsとしてサブスクリプションを行っているため、無料で利用する事ができます。



6.5 モニタリング



AWSサービス群の自動的なモニタリングを行い、セキュリティインシデント発生時の検知やトレースができるようにします。

- **操作ログ**

- AWS CloudTrailにより、マネジメントコンソールやAPIを介した操作のログが取得されます。
- CloudTrailはガバメントクラウドテンプレート(自動適用テンプレート)により、自動的に有効化されます。

- **リソース**

- AWS Configにより、AWSリソースの準拠状況や変更履歴が確認できるようになります。
- Configはガバメントクラウドテンプレート(自動適用テンプレート)により、自動的に有効化されます。

- **セキュリティ状況の一元管理**

- AWS Security Hubにより、セキュリティポリシーの遵守状況をチェックすると共に、違反があった場合のアラート集約 自動修復を実現します。
- 重大な違反はデジタル庁でも検知します。
- Security Hubはデジタル庁の設定により自動的に有効化されます。



6.6 ウイルス・マルウェア対策



ウイルス マルウェア感染の検知 駆除を目的として、ウイルス対策の仕組みを導入します。

- ウイルス対策クライアント

- 運用管理アカウントの運用管理VPC(基盤系)にウイルス対策サーバーを設けます。
- ウイルス対策サーバーから業務システムアカウントの各サーバーにクライアントを導入し、またパターンファイルの取得もできるようにします。
- クライアントソフトウェアはデジ課がライセンスを保有するトレンドマイクロ社の製品です。
- 詳細は別紙6「ガバメントクラウドでのウイルス対策・脆弱性対策(WSUS)等について」を参照ください。

- 保護対象

- 各システムのEC2インスタンス等、OSレイヤーを持つ全てのAWSリソースが保護対象です。



6.7 脆弱性対策



脆弱性対策として、OS セキュリティパッチが適切に適用／管理される仕組みを導入します。

- **WSUS**

- 運用管理アカウントの運用管理VPC(基盤系)にWSUS(Windows Server Update Services)サーバーを設けます。
- WSUSサーバーから業務システムアカウントの各サーバーがセキュリティパッチを取得できるようにします。
- 詳細は別紙6「ガバメントクラウドでのウイルス対策・脆弱性対策(WSUS)等について」を参照ください。

- **脆弱性の検知**

- Amazon Inspectorにより、EC2インスタンスの脆弱性診断が自動で行われます。
- ガバメントクラウドでは自動有効化されていないため、各システムのアカウントで有効化を行う必要があります。

- **保護対象**

- 各システムのEC2インスタンス等、OSレイヤーを持つ全てのAWSリソースが保護対象です。



6.8 セキュリティ分析



- セキュリティ分析

- AWS Trusted Advisorを用いて、システムのセキュリティ状況を確認します。
- Trusted Advisorはガバメントクラウドテンプレート(自動適用テンプレート)により、自動的に有効化されます。



デジタル改革推進課
Digital Innovation Promotion Division

7. 監視



7.1 監視設定



- **基本方針**

- システムの監視は、原則Amazon CloudWatchを活用し、極力自動化を行います。
- 監視は各システムにて必要なものを行います。ただし各システムの監視結果のログは、運用管理補助環境に集約します。

- **監視内容**

- 監視対象とするリソース、メトリクス、ログ、イベント、設定するアラーム、実行するアクション等の内容については、各システムにおいて方針を決定します。

- **AWSサービス自体の障害検知**

- AWSサービス自体の障害検知は、各システムにおいてPersonal Health DashBoardで行います。
- 統合運用管理補助者やデジタル庁から通知を行うことはありません。



7.2 監視通知



- **基本方針**
 - 監視結果の通知が必要なものは、AWS SNSで行います。
 - 併せて代替連絡先を登録し、AWSからの通知を受け取ります。
- **運用管理環境にかかる通知**
 - 統合運用管理補助者の指定連絡先宛て通知を行います。
- **業務システムにかかる通知**
 - 業務システムにおいて、通知先を決定します。



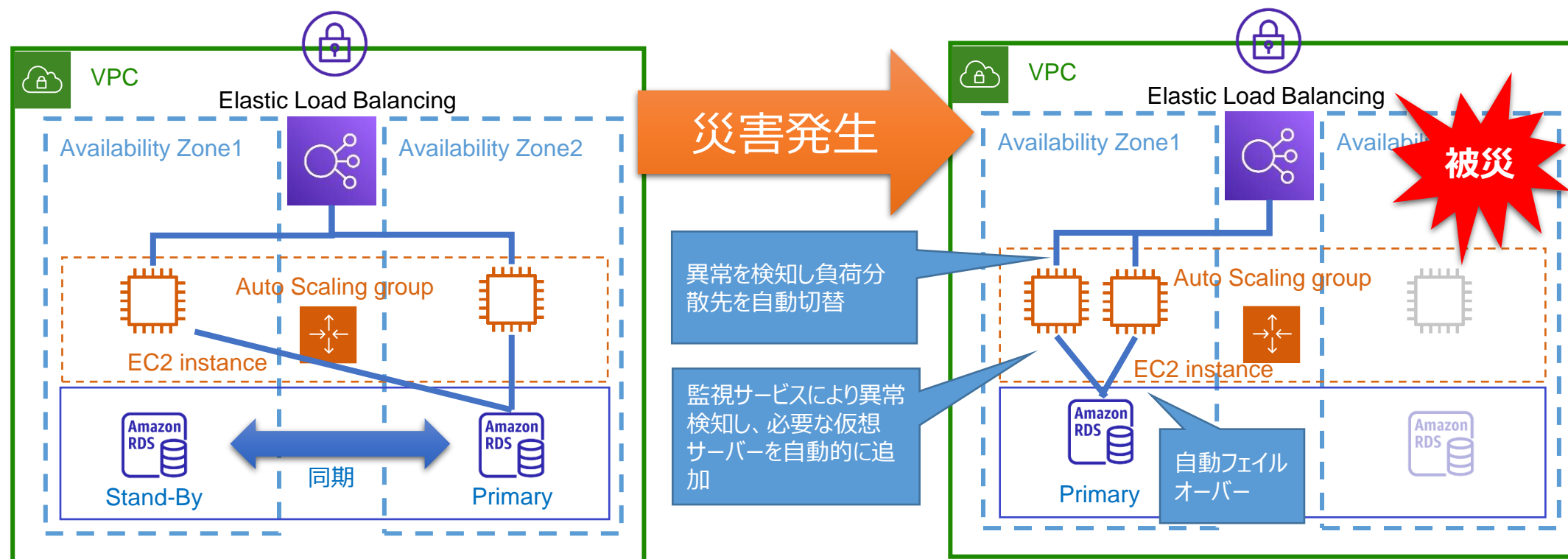
デジタル改革推進課
Digital Innovation Promotion Division

8. 可用性



8.1 冗長構成方針

業務継続に必要なサーバー及びDBについては、各システムにおいてマルチAZで冗長化を行い、片系障害発生の場合でも業務継続を行えるような構成としてください。





デジタル改革推進課
Digital Innovation Promotion Division

9. バックアップとリストア



9.1 バックアップ



- **基本方針**

- システム障害等に備え、AWS Backupを用いてバックアップを取得します。
- 大規模災害に備え、東京リージョンで取得したバックアップを大阪リージョンへコピーして保存します。
- 運用管理環境は統合運用管理補助者が、業務システム環境はASP事業者がバックアップとリストアを行います。

- **バックアップ対象**

- EC2インスタンスはAMI、ディスクボリュームはスナップショット、DBはスナップショットに加えてランザクションログを保存します。
- 具体的なバックアップの対象や方法等の方針は、各システムにおいて決定します。

- **スタンバイ構成**

- 業務システムで定める非機能要件において、より短いRTO/RPOが求める場合、スタンバイ構成を取ります。
- スタンバイ構成にはパイロットライト方式、ウォームスタンバイ方式、マルチサイト方式があり、詳細な方針は業務システムで決定します。



9.2 リストア



- **基本方針**

- 障害が発生した場合の対応方針として、障害の種類、リストアを行う条件、リストアの方法を予め各システムにおいて決めておきます。

- **障害の種類**

- インスタンス障害、AZ障害、リージョン障害、AWSのサービス障害の区分で整理します。
- インスタンス障害は更にAWS基盤障害、OS/SW停止障害、データ障害に分類します。

- **リストア/リカバリ**

- リストア/リカバリを行う条件や方法は各システムにおいて決定します。
- AutoScalingによるインスタンス復旧、AutoRecoveryによるインスタンスの復旧、AMIからのリストア、スナップショットからのリストア、トランザクションログからのDBリカバリなどがあります。
- とりわけリージョン障害で長期間復旧する見込みがない場合に大阪リージョンにリカバリすることになりますが、その判断基準を決めておく必要があります。



デジタル改革推進課
Digital Innovation Promotion Division

10. 運用保守



10.1 運用体制



- **ガバメントクラウド運用管理責任者**

- デジタル改革推進課長
- ガバメントクラウド運用にかかる統括と意思決定を行います
- GCASにおいては利用機関責任者のロールを担います

- **ガバメントクラウド統合運用管理補助者**

- デジタル改革推進課から委託を受けたクラウド運用事業者
- 「利用について」でいう「統括的な運用管理補助者」に相当します
- 運用管理環境の管理および、各業務システムへのテンプレートの配布、共通機能サービスの運用 保守を実施します。

- **業務システム管理者**

- 業務システムの所管課長
- 業務システムの運用にかかる意思決定を行います
- GCASにおいてはプロジェクトチーム責任者のロールを担います

- **ASP事業者**

- 業務システム所管課から委託を受けたアプリケーション事業者等
- 多くの場合「利用について」でいう「ガバメントクラウド運用管理補助者」を兼務します
- 業務システムの本番環境および検証環境の構築や運用 保守を実施し、各業務システムに必要なAWSサービスやOSの構築、業務アプリケーションおよびミドルウェア等を担当します。



10.2 役割分担



- 基本的な役割分担

- 運用管理アカウントは統合運用管理補助者が管理を行います。
- 業務システムの本番アカウントと検証アカウントはASP事業者が管理を行います。ただし、例外的に一部の作業は統合運用管理補助者が行います。

例外的に、統合運用管理補助者が業務システム環境で行う作業は以下の通り。(名古屋市統制テンプレートで実装)

- ネットワーク

- VPCの作成
- TransitGatewayAttachmentの設定
- Route53における共通的に利用する内部ドメインの作成

- セキュリティ

- Trusted Advisor、Security Hub、Guard Duty、Inspector、CloudTrail、Configにかかる情報の集約
- 情報の集約が困難な場合はスイッチロールで業務システムの上記情報を参照。

- 予算・コスト管理

- Budgets、Cost Explorer等にかかる情報の集約と外部SaaSの設定
- 情報の集約が困難な場合はスイッチロールで業務システムの上記情報を参照。



10.3 遠隔保守

- 基本的な考え方

- 遠隔保守はコマンドライン(AWS CLI)、AWS CDK、もしくはマネジメントコンソールから行います。
- AWS CLIとAWS CDKは専用線経由の閉域ネットワーク環境から、マネジメントコンソールはインターネットからアクセスを行います。
- 詳細は、別紙5「ガバメントクラウド遠隔保守基準」を参照ください。

- 閉域ネットワーク環境からの利用

- 以下のいずれかの方法によります。具体的には各システムにおいて決定します。
 1. 庁舎内に運用保守作業用の場所を確保し、庁内ネットワーク経由で行う。
 2. 事業者の保守拠点まで庁内ネットワークから専用線を敷設し、庁内ネットワーク経由で行う。
 3. 事業者の保守拠点から専用線で接続されるアカウントのVPC(共同利用方式の運用管理環境を想定)から業務環境にピアリングして行う。併せて必要なセキュリティ対策を行う。
- 上記3の方法を行う場合、別紙5を確認し事前にデジ課に相談を行ってください。



10.4 予算とコスト管理

• 基本方針

- AWS Budgetsで予算の管理を行い、AWS Cost Explorer等で利用コストを可視化します。
- 統合運用管理補助者は、運用環境の予算およびコスト管理を行います。また全市的な状況の把握のため、外部SaaSを用い、業務システム環境にかかる情報を集約または参照します。
- ASP事業者は、業務システム環境の予算およびコスト管理を行います。
- コスト配分タグの活用やコストアラートの設定等の運用については、各システムにおいて方針を決定します。
- クラウド利用料にかかる予算積算の詳細については、別紙1「クラウドサービス利用料積算」を参照ください。

• コスト最適化

- Cost ExplorerやTrusted Advisorを用い、コストの最適化を行います。
- デジ課から各業務システムにコスト最適化にかかる助言を行う場合があります。

• リソースの購入オプション

- 基本はオンデマンドで利用します。
- リザーブドインスタンスやセービングプランの利用についてはガバメントクラウド特有の制約があります。詳細は別紙1別添2「長期継続割引」を参照ください。



10.5 AWSのメンテナンス



- スケジュールされたメンテナンス

- EC2およびRDSはAWS側でメンテナンスを行う場合があります。
- メンテナンスの実施は各システムにおいて、マネジメントコンソール上で把握します。必要に応じてCloudwatchEventsやEventBridgeにSNSを組み合わせ、通知化します。
- メンテナンス予定時刻になると、停止や再起動などが自動的に行われます。

- メンテナンスの回避

- 対象のリソースを事前に停止/起動することで、メンテナンス対象外の物理ホストにて起動しますので、スケジュールメンテナンスを回避する事が可能です。
- メンテナンスの回避の実施要否やスケジュール調整は、各システムにおいて行います。



10.6 マネージドサービスの変更・廃止



- **基本方針**

- AWSのマネージドサービスは頻繁に新サービスがリリースされ、それに伴い既存サービスの変更や廃止が行われます。
- そのためマネージドサービスの更新情報の把握に努め、支障なく後継サービスへの切り替えを行えるようにします。
- サービスの変更等に伴い、マネジメントコンソールのインターフェイスも頻繁に変更されるため、マネジメントコンソールを用いた手順書による運用は極力行わず、CLIやIaCによる管理を行います。

- **変更・廃止**

- 業務システムで利用しているマネージドサービスの変更・廃止情報を捕捉した場合、業務システムで対応方針を決定し、後継または代替サービスへの切り替えを行います。



デジタル改革推進課
Digital Innovation Promotion Division

11. 移行



11.1 モダン化の推進



ガバメントクラウド上に構築するアプリケーションは、一定のモダン化が必須とされています。具体的にはAWS Well-Architected Frameworkを参考に、以下のようなモダン技術の採用に努めるものとします。

- **Amazon ECSやAmazon EKS AWS Fargate等のコンテナ関連サービスを利用**
 - インスタンス管理やOSメンテナンスの省力化
 - アプリケーションの実行 スケーリング実現の容易化
 - 運用時間に応じたインスタンスの自動起動 自動停止の設定によるコスト削減
- **Auto Scalingグループの設定**
 - 需要に応じたリソースのスケールアウト/インを自動化
 - 安定したパフォーマンスの実現
- **セキュリティ・可用性・コスト及びパフォーマンス効率に優れたマネージドサービスの利用**
 - Amazon RDS、Amazon S3などの活用による管理負担やコストの削減
- **ジョブフローで繋がったバッチ処理のサーバーレス化**
 - AWS Step FunctionsやAWS Lambdaなど
- **AWS CodeCommitやAWS CodeBuildによるCI/CDの活用**
 - リリースサイクルを高速 高頻度化し、安全なデプロイを実現
 - リリースサイクルの短期間化による継続的なアプリケーション改修
 - 検証の自動化によるアプリケーション品質の向上



11.2 Replatform/Rebuild

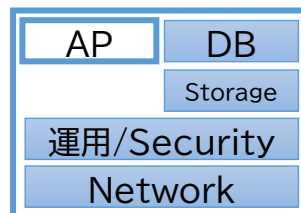
- ガバメントクラウド利用のモダン化にかかる基本的な考え方は以下の通りです。

- ガバメントクラウド上でシステムを新規構築する場合
 - 当初からモダン化が原則
- オンプレミス等他環境からのガバメントクラウド移行
 - 当初からモダン化が原則だが、困難な場合は2段階のモダン化を想定

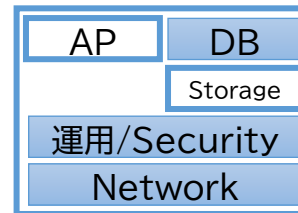
- 上記を踏まえ、本市の標準準拠システムの移行は2段階のモダン化で対応します。

- 移行1段階目(Replatform:アプリケーションの変更を最小限にマネージドサービスを活用)

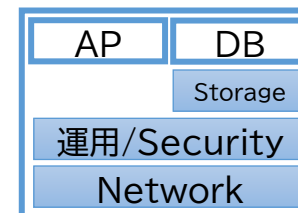
基本形:APサーバ以外のマネージド化



例外1:ストレージとAPサーバ以外をマネージド化

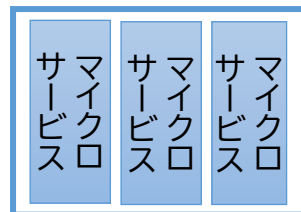


例外2:DB/APサーバ以外のマネージド化

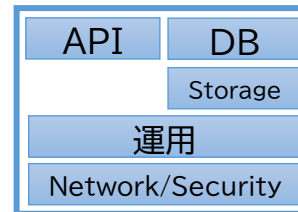


- 移行2段階目(Rebuild:アプリケーションを変更してマネージドサービスをフル活用し、モダン化を達成)

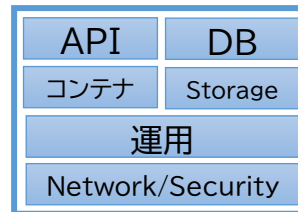
基本形1:マイクロサービス化



基本形2:APIイベントドリブン型



例外:アプリケーションのコンテナ化





11.3 インフラのIaC化



- 構成管理のIaC化とテンプレートの活用

- マネジメントコンソールの操作はヒューマンエラーのリスクがあり、またAWSの機能追加や仕様変更によりUIが頻繁に変更され、手順書の維持管理の負担が大きい傾向にあります。
- このため、インフラの構築、変更はAWS CDK(Cloud Development Kit)、AWS CloudFormation、Terraform等のIaCツールにて行うことを推奨します。
- これにより環境構築時の作業負荷の軽減やヒューマンエラーの防止が可能となり、業務や環境の変化に迅速かつ柔軟に対応できるようになるのみならず、ディザスタリカバリ時のRTO短縮も可能となります。
- ただし全ての構成をIaCで管理しようとするると運用上無理が生ずる場合もあり、運用設計の段階でIaCで管理する部分と手動で作成管理を行う部分を、冪等性により分類整理することが推奨されます。

- 作業要員の水準

- これらの理由から、統合運用管理補助者やASP事業者にはIaCに基づくシステム構築や運用管理等の経験や知識を有する要員が居る事が望ましく、仕様上該当CSPの上級認定資格(AWSの場合はSAP-C02相当)保持者を求めることを推奨します。



11.4 データ移行と切替

• データ移行

- 現行システムからガバメントクラウド上の業務システムにデータを移行する場合、以下の一連の作業が必要となります。これらの具体的な計画については各システムにおいて決定します。
 - ✓ 現行システムにおけるデータの事前調査とクレンジング
 - ✓ データの出力と変換
 - ✓ 本番環境へのデータの移送と取り込み
- データの移送は以下のいずれかの方法で行います。
 - ✓ 庁内ネットワークから接続回線(閉域網)経由で本番環境にアップロード
 - ✓ 物理媒体でASP事業者を提供し、ASP事業者の保守拠点から共同利用方式アカウント経由でアップロードし、S3経由で本番環境に取り込み
 - ✓ 上記2つの手段が利用できない場合のみ、本番環境アカウントからAWS Snowball Edgeを発注

• 切替

- システムの切替については、データ移行の完了確認、ネットワークの疎通、アプリケーションの稼働、利用者のユーザー認証、業務間のデータ連携等、各種の確認や検証作業が発生します。
- このため実際の切替の際にはタスクリストやタイムテーブルを作成し、業務システム所管課、デジ課、関係委託事業者が連携して対応する必要があります。



改訂履歴(1/5)

版数	改訂年月日	改訂箇所	改訂内容
1.0	2023年8月1日		
1.01	2023年8月4日	6.2 暗号化	マイナンバー利用事務系における通信の暗号化
1.1	2023年12月5日	2.7 ガバメントクラウドにかかる経費 2.8 ガバメントクラウドのCSP 3.3 ユーザー 4.1 ネットワーク概要 4.2 ネットワーク基本方針 4.3 ネットワークセグメント 6.3 ファイアウォール 7.2 監視通知 10.4 予算とコスト管理	クラウド利用料のデジタル庁への支払方法について追記 CSPを追加 Adminユーザー、IAMユーザーについて追記 三層分離について追記 三層分離について追記 記述の修正・詳細化 記述の修正 業務システム所管課への通知について追記 リソースの購入オプションについて追記
1.2	2024年11月1日	全般 2.3 2.5	ガバメントクラウドの利用について【2.0版】改定等に伴う関係資料等の記述変更 主権免除関連の記述修正、ディスカウント及びダッシュボードの記述を追記 経費比較にかかる記述を抹消



改訂履歴(2/5)

版数	改訂年月日	改訂箇所	改訂内容
1.2	2024年11月1日	2.6 2.7 2.9 2.10 2.11 2.12 2.14 3.1 3.3 3.4(追加) 3.6 3.8	事業者名称及び図の修正、名古屋市環境にかかる問い合わせ対応、今後の法改正について追記 事業者名称及び図の修正、その他軽微な修正 ガバメントクラウド接続サービス関連の記述及び図の修正、関係資料等の記述変更 図の修正、CI/CD事項の追記 GCAS導入に伴い全面改訂 図の修正 運用管理領域の稼働率を追記 図の修正 GCASアカウントによるSSO実施に伴いAdminユーザーの説明を削除し、IdCユーザーの説明を追記 GCASアカウントによるSSO実施に伴い、ユーザ権限として、IAMロールの説明を追加(以降の項番を更新) 命名規則に関する参照先資料を追記 大阪リージョンへのエンドポイント配置に関する記載を更新



改訂履歴(3/5)

版数	改訂年月日	改訂箇所	改訂内容
1.2	2024年11月1日	3.9 4.4 4.5(追加) 5.2 5.3 5.4(追加) 6.1 6.3 6.6 6.7 7.2 10.3	AWSサービスアップデートに伴い、アーカイブ先の対象を更新 各業務システムからインターネット接続を希望する場合の参照先を追記、図の修正 次期分離モデルに関する内容を追加 設計内容に合わせ、軽微な更新 ガバメントクラウドに関わる事の問い合わせについて追記 サービスの集約に関する内容を追加 GCAS SSOの導入に伴う更新 本市テンプレートで設定するネットワークACLについて追記 ウイルス マルウェア対策に関する参照先資料を追記 WSUSに関する参照先資料を追記 運用管理環境にかかる通知の詳細のに関する記述を抹消 遠隔保守に関する参照先資料を追記



改訂履歴(4/5)

版数	改訂年月日	改訂箇所	改訂内容
1.3	2025年5月21日	全般	法改正及び国資料の改定等に伴う用語及び関係資料の記述の修正 別紙関係の記述の整理
		1.2	法改正及びガバメントクラウド利用検討指針の策定に伴い、位置付けを整理
		2.1	法改正に伴う記載内容の修正
		2.3	選定条件の記載の一部修正
		2.4	法改正に伴う記載内容の修正
		2.6	法改正に伴う記載内容と図の修正
		2.7	法改正に伴う記載内容と図の修正
		2.10	国ドキュメントの改正に伴う記載内容の修正
		2.11	国ドキュメントの改正に伴う記載内容の修正
		3.2	セキュリティ関連記述の詳述化
		3.3	国が追加で実施するセキュリティ対策に伴う関係記載内容の修正
		3.4	国が追加で実施するセキュリティ対策に伴う関係記載内容の修正
		5.2	国ドキュメントの改正及び外部SaaS導入に伴う記載内容の修正



改訂履歴(5/5)

版数	改訂年月日	改訂箇所	改訂内容
1.3	2025年5月21日	5.3 6.1 7.2 10.1 10.2 10.4 11.3 11.4	GCASヘルプデスクにかかる記載内容の修正 MFAデバイスにかかる取り扱いの追記 国が追加で実施するセキュリティ対策に伴う関係記載内容の修正 国ドキュメントとの対応にかかる記述の追加 外部SaaS導入に伴う記載内容の修正 外部SaaS導入及び長期継続割引の取扱変更に伴う記載内容の修正 IaC利用方針にかかる記述の詳細化 全体移行方針で記述する内容の整理、Snowball Edge選定にかかる優先度の追記