

# 東京都クラウドインフラ 標準仕様書

1.5 版 令和 7 年 10 月 27 日  
東京都デジタルサービス局デジタル基盤部

## 目次

|     |                                   |    |
|-----|-----------------------------------|----|
| 第 1 | はじめに .....                        | 3  |
| 1   | 本文書の位置づけ.....                     | 3  |
| 2   | 改訂方針 .....                        | 3  |
| 3   | 本文書での用語の定義.....                   | 3  |
| 第 2 | 東京都クラウドインフラの概要.....               | 3  |
| 1   | 基本方針 .....                        | 3  |
| 2   | 概要 .....                          | 4  |
| (1) | 全体構成 .....                        | 4  |
| (2) | スケジュール.....                       | 4  |
| (3) | 利用可能なリージョン.....                   | 4  |
| (4) | 提供環境 .....                        | 5  |
| (5) | ネットワーク分離.....                     | 5  |
| (6) | 使用可能な CSP .....                   | 7  |
| (7) | 東京都クラウドインフラ利用開始までの流れ.....         | 7  |
| 3   | 役割分担 .....                        | 7  |
| (1) | 機能の実装分担.....                      | 7  |
| (2) | 作業の役割分担.....                      | 10 |
| 第 3 | 東京都クラウドインフラの機能一覧.....             | 12 |
| 1   | 東京都クラウドインフラ提供機能の全体像.....          | 12 |
| 2   | リソース提供機能.....                     | 12 |
| (1) | CSP 環境の提供 .....                   | 12 |
| (2) | OS テンプレート .....                   | 13 |
| (3) | ネットワーク接続.....                     | 13 |
| (4) | インターネット接続（IPS/IDS 及び WAF 付） ..... | 13 |
| (5) | 踏み台サーバー.....                      | 14 |
| 3   | リソース管理.....                       | 15 |
| (1) | CSP 利用料管理 .....                   | 15 |
| (2) | OS リポジトリ管理 .....                  | 16 |
| (3) | ネットワーク設定変更.....                   | 16 |
| (4) | SSL/TLS 証明書の更新 .....              | 16 |
| (5) | 名前解決 .....                        | 16 |
| (6) | プライベート証明書.....                    | 17 |
| 4   | セキュリティ管理.....                     | 17 |
| (1) | クラウドセキュリティ管理.....                 | 17 |

|                                                     |    |
|-----------------------------------------------------|----|
| (2) 仮想マシンセキュリティ保護.....                              | 17 |
| (3) ネットワークセキュリティ保護.....                             | 18 |
| (4) 環境及びネットワーク系統を跨いだ通信.....                         | 18 |
| 5    セキュリティ診断支援.....                                | 18 |
| 6    東京都クラウドインフラポータルサイト.....                        | 18 |
| (1) リソース提供機能.....                                   | 20 |
| (2) リソース管理.....                                     | 20 |
| (3) セキュリティ管理.....                                   | 21 |
| (4) 東京都クラウドインフラポータルサイト.....                         | 21 |
| 第4    料金体系 .....                                    | 22 |
| 1    東京都クラウドインフラの料金構造.....                          | 22 |
| 2    「業務システム分に係る経費（従量課金分）」の見積り留意事項.....             | 22 |
| (1) AWS .....                                       | 22 |
| 3    サービスレベルの考え方.....                               | 22 |
| (別紙1) 改訂履歴.....                                     | 23 |
| (別紙2) 用語の定義.....                                    | 27 |
| (別紙3) 利用可能なサービス一覧.....                              | 30 |
| 1    東京都クラウドインフラで利用可能な AWS サービス.....                | 30 |
| 2    東京都クラウドインフラの領域ごとの制約.....                       | 30 |
| 3    東京都クラウドインフラのリージョンごとに利用できない AWS サービス.....       | 39 |
| 4    留意事項 .....                                     | 39 |
| (別紙4) 利用者ネットワークの接続.....                             | 40 |
| 1    概要 .....                                       | 40 |
| 2    利用者ネットワーク接続時の作業概要.....                         | 40 |
| 3    利用者ネットワーク接続時の手続と役割分担.....                      | 42 |
| (1) 事前確認・調整からデータセンターの現地調査までの流れ.....                 | 42 |
| (2) データセンターの現地調査後から利用開始までの流れ.....                   | 43 |
| 4    利用者ネットワーク接続に係る概算金額算出の際の制限事項.....               | 44 |
| (別紙5) エンドポイント接続設定の作業分担.....                         | 46 |
| (別紙6) 環境構築作業分担.....                                 | 47 |
| (別紙7) 設計・構築・運用・保守に関する考慮事項リスト.....                   | 48 |
| (別紙8) 利用者環境にデフォルト設置されるリソース及びサービスの利用で発生する費用の積算 ..... | 52 |

第1 はじめに

1 本文書の位置づけ

本文書は、東京都クラウドインフラの仕様を記した文書であり、東京都クラウドインフラに業務システムを移行又は新規構築するに当たって必要な情報を提供するものである。

| 想定読者<br>／<br>記載粒度 | 東京都クラウドインフラ<br>利用者                                                                               | 東京都クラウドインフラ<br>利用者及び受託者                                                                                      | 受託者                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
|                   | <br>クラウド転換の基本方針 | <br>東京都クラウドインフラ<br>概要説明書    | <br>東京都クラウドインフラ<br>標準仕様書(本文書) |
|                   |                                                                                                  | <br>東京都クラウドインフラ<br>利用手続ガイド |                                                                                                                  |

図 1-1 本文書と関連文書の関係

2 改訂方針

クラウドサービスプロバイダー（以下「CSP」という。）が提供するクラウドサービスの更改、仕様変更があった場合には、変更内容に応じて本文書を改訂する。

3 本文書での用語の定義

本文書で用いる用語は、「(別紙2) 用語の定義」を参照すること。

第2 東京都クラウドインフラの概要

1 基本方針

東京都クラウドインフラは、東京都（以下「都」という。）が必要とするセキュリティやシステム要件等の各種要件に準拠し、都を対象に提供するクラウドインフラである。東京都クラウドインフラは、都が別途定める「クラウド転換の基本方針」の考え方に則って運営される。

受託者は、東京都サイバーセキュリティポリシーを遵守し、必要なサイバーセキュリティ対策を講じた上で、業務システムの設計・開発・運用を行うこと。

また、上記の方針に基づき、東京都クラウドインフラを利用すること。

## 2 概要

### (1) 全体構成

東京都クラウドインフラは、「クラウドインフラサービス」と「クラウドネットワークサービス」で構成される。東京都クラウドインフラの全体像は、図 2-1「東京都クラウドインフラの全体像」のとおり。クラウドインフラサービスでは、CSP が提供するクラウドサービスに、都として必要な統制機能やセキュリティ設定を適用した機能を提供する。クラウドネットワークサービスでは、CSP までの専用接続回線を提供する。「クラウドインフラサービス」の詳細は、「第 3-1 東京都クラウドインフラ提供機能の全体像」に、「クラウドネットワークサービス」の詳細は、「第 1-1-(5) ネットワーク分離」に記載する。

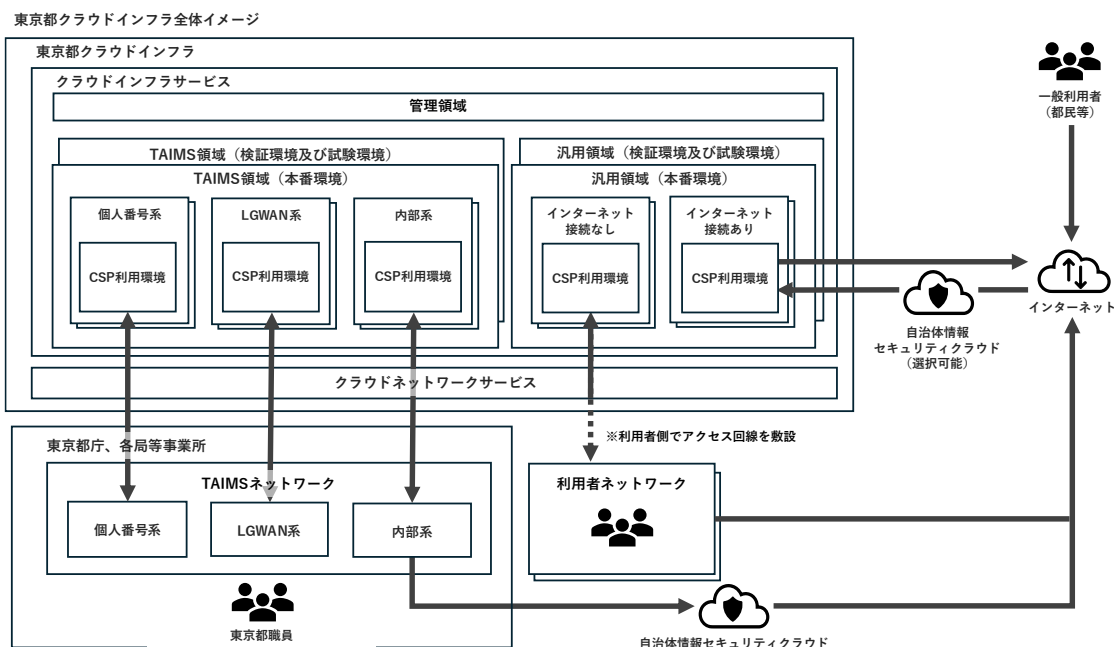


図 2-1 東京都クラウドインフラの全体像

### (2) スケジュール

東京都クラウドインフラは、令和 7 年 11 月 4 日にスモールスタート（シングルクラウド構成）としてサービスを開始する。

### (3) 利用可能なリージョン

利用可能な CSP 環境は、国内のみである。東日本リージョン（以下「プライマリーリージョン」という。）と西日本リージョン（以下「セカンダリーリージョン」とい

う。)の両方を提供する。

なお、リージョンによっては利用不可能なサービスが存在する。詳細については「(別紙3) 利用可能なサービス一覧」の記載事項を確認すること。

#### (4) 提供環境

東京都クラウドインフラの提供環境の定義を表 2-1「提供環境の定義」に示す。受託者は、業務システムの要件に応じて必要な環境を選択して利用すること。

なお、受託者は、業務システムの要件に応じて、災害対策環境をセカンダリーリージョンに構築するなど、業務継続性を確保するために必要な災害対策を講じること。

表 2-1 提供環境の定義

| # | 環境         | 定義                                                                            |
|---|------------|-------------------------------------------------------------------------------|
| 1 | 本番環境       | 業務システムの本番システムが稼働する環境                                                          |
| 2 | 検証環境及び試験環境 | 業務システムの開発・検証システムが稼働する環境であり、本番環境とはネットワークを分離した環境。東京都クラウドインフラが提供する機能については本番環境と同等 |
| 3 | 災害対策環境     | 大規模災害が発生した際にも業務を継続させるために、本番環境とは別に構築する環境                                       |

#### (5) ネットワーク分離

東京都クラウドインフラでは、東京都高度情報化推進システム（以下「TAIMS」という。）から利用可能な「TAIMS 領域」と、TAIMS ネットワークに接続できない各局等独自ネットワーク（以下「利用者ネットワーク」という。）やインターネットから利用可能な「汎用領域」を提供する。TAIMS 領域は「個人番号系」、「LGWAN 系」及び「内部系」の3つのネットワーク系統に分けられる。汎用領域は、「汎用領域（インターネット接続なし）」及び「汎用領域（インターネット接続あり）」の2つのネットワーク系統に分けられる。

また、東京都クラウドインフラのネットワークの一覧を表 2-2「クラウドネットワーク一覧」に示す。業務システムで複数の異なる環境及びネットワーク系統を利用する場合は、業務システムで必要とする各環境及びネットワーク系統単位でアカウントを申請すること。ネットワーク系統ごとの業務システムへのアクセス方法の詳細については、「第3-2-(5)踏み台サーバー」を参照すること。

表 2-2 クラウドネットワーク一覧

| # | 領域       | ネットワーク系統          | 想定利用者 | 概要                                                                                                                                                                                                                                                      |
|---|----------|-------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | TAIMS 領域 | 個人番号系             | 各局等   | <ul style="list-style-type: none"> <li>・TAIMS 領域の個人番号系の閉域網と接続するネットワーク</li> <li>・インターネットとの通信は、不可</li> </ul>                                                                                                                                              |
| 2 | TAIMS 領域 | LGWAN 系           | 各局等   | <ul style="list-style-type: none"> <li>・TAIMS 領域の LGWAN 系の閉域網と接続するネットワーク</li> <li>・インターネットとの通信は、不可</li> </ul>                                                                                                                                           |
| 3 | TAIMS 領域 | 内部系               | 各局等   | <ul style="list-style-type: none"> <li>・TAIMS 領域の内部系の閉域網と接続するネットワーク</li> <li>・インターネットからのインバウンド通信は、不可。アウトバウンドへの通信は、TAIMS ネットワーク経由で通信可能</li> <li>・汎用領域（インターネット接続あり）向けの一方向通信は申請により可能（「第3-4-(4)環境及びネットワーク系統を跨いだ通信」及び「(別紙5) エンドポイント接続設定の作業分担」を参照)</li> </ul> |
| 4 | 汎用領域     | 汎用領域（インターネット接続なし） | 各局等   | <ul style="list-style-type: none"> <li>・利用者ネットワークとのアクセスが必要な業務システム向けのネットワーク</li> <li>・受託者は、利用者拠点からクラウドネットワークサービスまでアクセス回線の敷設が必要</li> </ul>                                                                                                                |
| 5 | 汎用領域     | 汎用領域（インターネット接続あり） | 各局等   | <ul style="list-style-type: none"> <li>・インターネットとのアクセス（HTTPS）が必要な業務システム向けのネットワーク</li> </ul>                                                                                                                                                              |

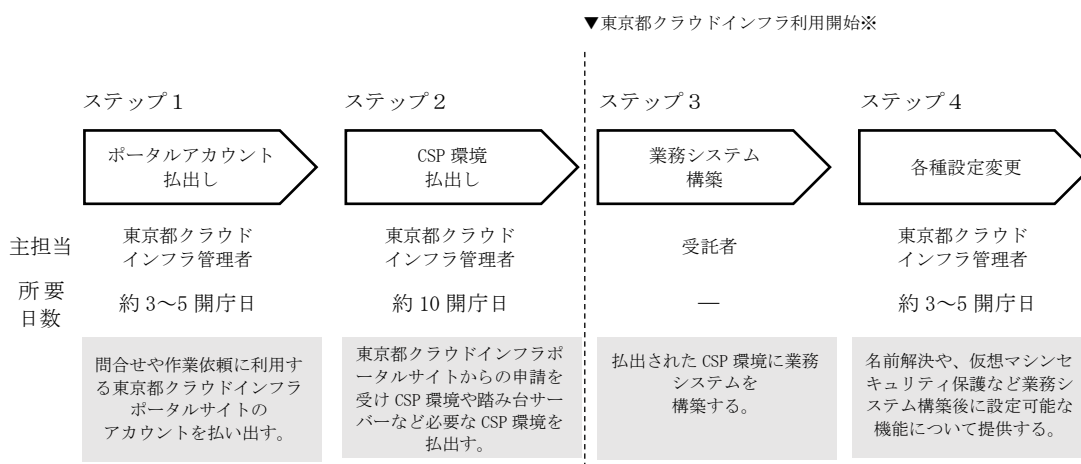
## (6) 使用可能な CSP

使用可能な CSP は、Amazon Web Services（以下「AWS」という。）である。

## (7) 東京都クラウドインフラ利用開始までの流れ

契約締結後、東京都クラウドインフラ利用者及び受託者からの申請に基づき、東京都クラウドインフラ管理者から、利用者ポータルサイトのアカウント及び CSP 環境を払い出す。東京都クラウドインフラ利用者及び受託者が東京都クラウドインフラの利用を開始するまでの流れは図 2-2「東京都クラウドインフラ利用開始までの流れ」のとおり。東京都クラウドインフラ利用者及び受託者は所要日数を考慮し、利用開始の申請を行うこと。

なお、汎用領域（インターネット接続なし）のネットワークシステムを利用する場合には、東京都クラウドインフラ利用者はクラウドネットワークサービスまでのアクセス回線の敷設が必要であるため、別途アクセス回線敷設の期間を要する。詳細は、「(別紙 4) 利用者ネットワークの接続」を参照すること。



※利用開始日に関わらず、利用開始月の 1 日から東京都クラウドインフラの利用料の請求が発生する。

図 2-2 東京都クラウドインフラ利用開始までの流れ

## 3 役割分担

### (1) 機能の実装分担

東京都クラウドインフラにおける受託者、東京都クラウドインフラ管理者及び CSP の機能の実装分担を図 2-3「機能の実装分担」に示す。

受託者は、業務システムが必要とするセキュリティ水準の確保に向けて、必要なリスク分析やセキュリティ対策を設計及び実装すること。

東京都クラウドインフラ管理者は、ネットワーク系統の分離やインターネットアクセスの制限等、サービス全体で共通して必要となるセキュリティ設定を適用し、業務システムのセキュリティ対策を支援する。

監視及びセキュリティの実装は、受託者と東京都クラウドインフラ管理者で実装範囲が分かれる。東京都クラウドインフラ管理者は、共通して提供するネットワーク接続、セキュリティ機能等を 24 時間 365 日の体制で監視し、必要に応じて受託者に通知を行う等、東京都クラウドインフラ全体に係る監視及びセキュリティ対策を実施する。

受託者は、業務システムにおけるセキュリティインシデントのアラート監視やその対応を行うこと。東京都クラウドインフラ管理者が実装する監視及びセキュリティ機能を表 2-3 「東京都クラウドインフラ管理者が提供する監視機能」及び表 2-4 「東京都クラウドインフラ管理者が提供するセキュリティ機能」に示す。

なお、東京都クラウドインフラ利用者及び受託者は、表に記載のない機能については業務要件に応じて実装すること。

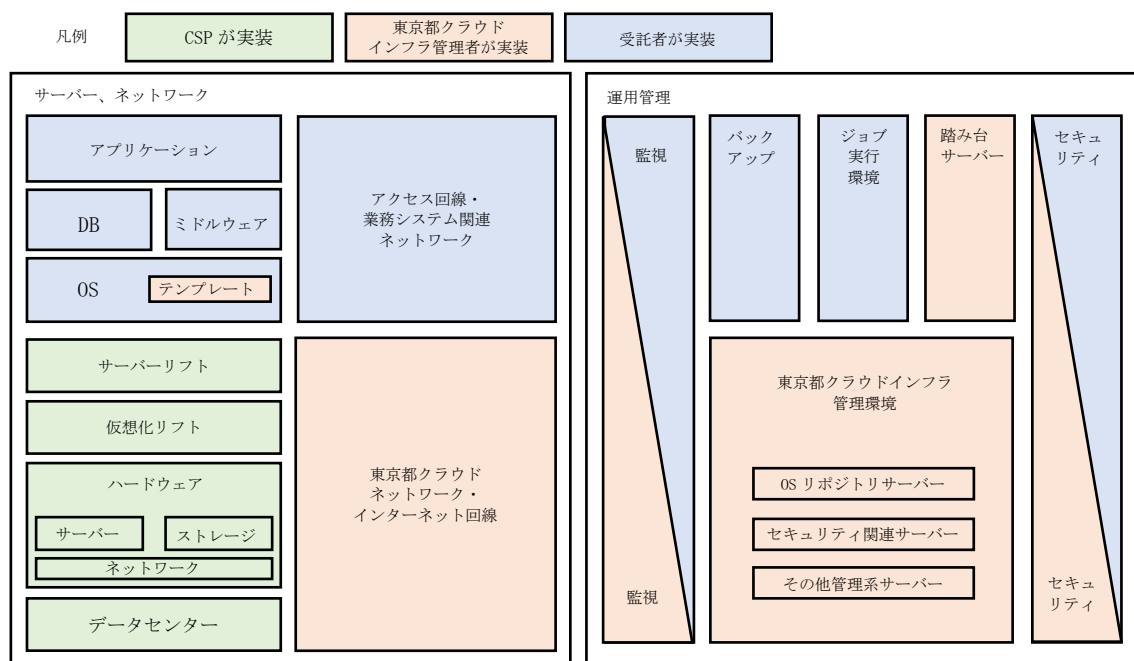


図 2-3 機能の実装分担

表 2-3 東京都クラウドインフラ管理者が提供する監視機能

| # | 区分     | 項目           | 実装範囲 | 備考                                    |
|---|--------|--------------|------|---------------------------------------|
| 1 | 業務システム | エンドツーエンド監視   | —    |                                       |
| 2 | 業務システム | 仮想マシンログ監視    | —    |                                       |
| 3 | 業務システム | 仮想マシンプロセス監視  | —    |                                       |
| 4 | 業務システム | 仮想マシン死活監視    | —    |                                       |
| 5 | クラウド   | クラウドサービス死活監視 | ○    | 受託者は、業務システムの要件に応じて追加で監視機能の設計・構築を行うこと。 |
| 6 | クラウド   | リージョン死活監視    | ○    | 受託者は、業務システムの要件に応じて追加で監視機能の設計・構築を行うこと。 |

表 2-4 東京都クラウドインフラ管理者が提供するセキュリティ機能

| # | 区分     | 項目             | 実装範囲 | 備考                                                                         |
|---|--------|----------------|------|----------------------------------------------------------------------------|
| 1 | 業務システム | EPP/EDR        | —    | 個人番号系、LGWAN 系、汎用領域（インターネット接続なし）が対象                                         |
| 2 | 業務システム | EPP/EDR        | ○    | 内部系、汎用領域（インターネット接続あり）が対象                                                   |
| 3 | 業務システム | セキュリティパッチ適用    | —    | アップデート用サーバーは、東京都クラウドインフラから提供する。<br>マスターOS イメージのパッチ適用は、東京都クラウドインフラ管理者が実施する。 |
| 4 | 業務システム | データ暗号化         | —    | 受託者は、CSP のサービスやミドルウェアの機能を用いて暗号化すること。                                       |
| 5 | ネットワーク | 通信制御（ファイアウォール） | ○    | 業務システムへの通信を対象にしたファイアウォール機能                                                 |
| 6 | ネットワーク | 通信制御（IPS/IDS）  | ○    | インターネット通信を対象に                                                              |

| # | 区分     | 項目                 | 実装範囲 | 備考                                                    |
|---|--------|--------------------|------|-------------------------------------------------------|
|   | ク      |                    |      | した IPS/IDS 機能                                         |
| 7 | ネットワーク | 通信暗号化（証明書管理）       | －    | 東京都クラウドインフラが管理するネットワークの証明書の更新作業は、東京都クラウドインフラ管理者が実施する。 |
| 8 | クラウド   | クラウドセキュリティ管理（CSPM） | ○    | CSP サービスの潜在的な脆弱性を検知する機能                               |

## (2) 作業の役割分担

東京都クラウドインフラの利用に係る作業の役割分担を、表 2-5「作業の役割分担」に示す。

表 2-5 作業の役割分担

| # | 項目               | 内容                                                                                   | 役割分担                |                |
|---|------------------|--------------------------------------------------------------------------------------|---------------------|----------------|
|   |                  |                                                                                      | 東京都クラウドインフラ利用者及び受託者 | 東京都クラウドインフラ管理者 |
| 1 | 申請               | 東京都クラウドインフラの利用開始、変更及び終了の申請をすること。                                                     | ○                   | —              |
| 2 | 利用開始・変更・終了手続     | ポータルアカウント・CSP 環境の払い出し、変更又は削除をする。                                                     | —                   | ○              |
| 3 | CSP 環境の構築        | 業務システムに必要な CSP リソース（「(別紙6) 環境構築作業分担」を参照）の構築及び削除をすること。                                | ○                   | —              |
| 4 | 業務システムの構築・削除     | 業務システムの OS、ミドルウェア、アプリケーションの構築及びデータ削除をすること。                                           | ○                   | —              |
| 5 | 業務システムの移行        | 業務システム及びデータ移行をすること。                                                                  | ○                   | —              |
| 6 | 東京都クラウドインフラの運用保守 | CSP 全体及び東京都クラウドインフラの運用保守をする。                                                         | —                   | ○              |
| 7 | CSP 環境の運用保守      | 業務システムに必要な CSP リソースの運用保守（利用状況のモニタリング、構成管理等）をすること。                                    | ○                   | —              |
| 8 | 業務システムの運用保守      | 業務システムの OS、ミドルウェア、アプリケーションの運用保守（業務システムの監視、バックアップ、ジョブ運用、セキュリティパッチ適用、サーバー証明書更新等）をすること。 | ○                   | —              |
| 9 | セキュリティインシデント対応   | 業務システムにおいてセキュリティインシデントが発生した場合、東京都サイバーセキュリティポリシーに準じ、対処すること。                           | ○                   | —              |

### 第3 東京都クラウドインフラの機能一覧

#### 1 東京都クラウドインフラ提供機能の全体像

東京都クラウドインフラの提供機能の全体像は、図 3-1「東京都クラウドインフラの提供機能の全体像」のとおり。受託者は、東京都クラウドインフラから払い出されたアカウントを使用し、アカウントに紐づいた環境に業務システムを構築すること。

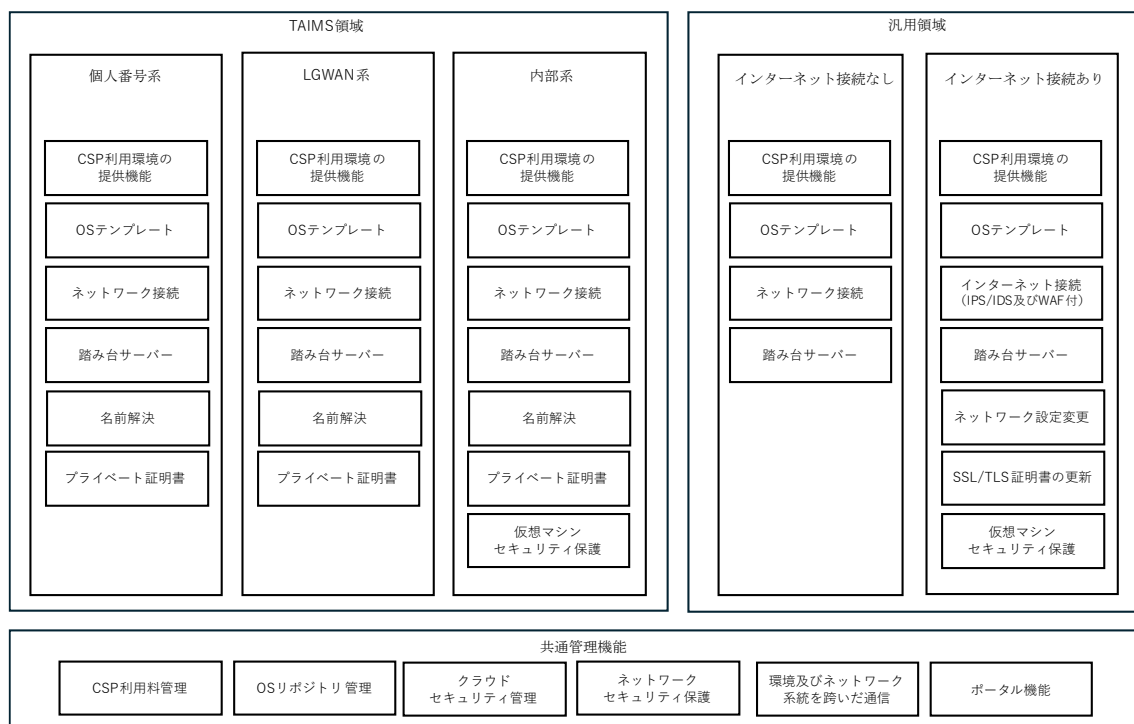


図 3-1 東京都クラウドインフラの提供機能の全体像

#### 2 リソース提供機能

##### (1) CSP 環境の提供

東京都クラウドインフラでは、東京都クラウドインフラ利用者からの申請に基づき、アカウント及びその環境を管理するための CSP の特権ユーザーを提供する。本機能の制限事項は、以下のとおりである。

- ・受託者が利用可能な CSP のサービスは、「(別紙3) 利用可能なサービス一覧」を参照すること。
- ・CSP の特権ユーザーには、払い出された環境を管理するために必要な権限を付与する。
- ・受託者は、CSP の特権ユーザーを適切に管理すること。
- ・CSP の特権ユーザーを用いた CSP アカウントへのログインは、利用者が申請したグローバル IP アドレスからのみ接続可能とする。

- ・受託者は、CSP の特権ユーザーを用いて、業務システムの構築に必要な最低限の権限を付与したユーザーを作成及び管理すること。
- ・作成した IAM ユーザーには CSP の特権ユーザーと同様にグローバル IP での接続制限をかけること。
- ・受託者は、アカウントに多要素認証を導入し、認証の強化を実施すること。
- ・VPC ピアリングや PrivateLink を使用して、他のネットワークとの接続をしてはならない。

## (2) OS テンプレート

業務システムを構築するための OS テンプレートを提供する。受託者は、この OS テンプレートを用いて、業務システムを構築すること。OS テンプレートの仮想マシン OS は、表 3-1 「OS テンプレート」 のとおり。受託者は、システムの要件に合わせて、適切な OS を選択して利用すること。本機能の制限事項は、以下のとおりである。

- ・受託者は、東京都クラウドインフラ管理者によってあらかじめ設定された OS テンプレートの各 OS パラメータの設定や、事前にインストールされた各種管理用のエージェントの変更・削除等を行うことができない。

表 3-1 OS テンプレート

| # | 仮想マシン OS                          | バージョン                 |
|---|-----------------------------------|-----------------------|
| 1 | Windows Server Datacenter Edition | 2019 / 2022           |
| 2 | RedHat Enterprise Linux           | 8 / 9                 |
| 3 | Ubuntu Server                     | 22.04 LTS / 24.04 LTS |

## (3) ネットワーク接続

クラウドインフラサービスとクラウドネットワークサービスを接続する機能を提供する。本機能により、東京都クラウドインフラ利用者及び受託者は、TAIMS ネットワークや利用者ネットワークの利用者拠点からクラウドインフラサービスの TAIMS 領域、汎用領域（インターネット接続なし）に構築した業務システムへのアクセスが可能となる。

## (4) インターネット接続（IPS/IDS 及び WAF 付）

汎用領域（インターネット接続あり）ネットワーク向けに、サイバー攻撃を検知及び防御するために共通のセキュリティポリシーが適用された IPS/IDS 及び WAF 機能を提供する。本機能の制限事項は、以下のとおりである。

- ・受託者は、IPS/IDS 及び WAF のセキュリティポリシーを変更できない。

- ・受託者は、インターネットゲートウェイを作成できない。
- ・ネットワークの暗号化通信に使用する証明書については、東京都クラウドインフラ利用者及び受託者は、原則として東京都デジタルサービス局が定める証明書機関からの取得を推奨する。ただし、必要に応じて、独自に取得した証明書を利用することも可能とする。

#### (5) 踏み台サーバー

業務システムにアクセスするための踏み台サーバーを提供する。受託者は、踏み台サーバーを経由して仮想マシンへのアクセスや操作を実施すること。

各領域への業務システムへのアクセス方法は、図 3-2「各領域へのアクセス方法」のとおり。踏み台サーバーでは、東京都クラウドインフラ管理者によりログイン制限とともに証跡情報が記録される。

なお、踏み台サーバーには Windows 標準のソフトウェアに加えて、表 3-2「踏み台サーバーにインストール済みのソフトウェア」に示すソフトウェアをインストールする。本機能の制限事項は、以下のとおりである。

- ・接続元の端末は、東京都クラウドインフラの提供範囲外となるため、東京都クラウドインフラ利用者及び受託者が業務システムの要件に応じて準備すること。
- ・受託者は、TAIMS 領域又は汎用領域（インターネット接続なし）に構築した業務システムにアクセスする場合、踏み台サーバーに RDP で接続し、踏み台サーバー経由で業務システムにアクセスすること。
- ・受託者は、汎用領域（インターネット接続あり）に構築した業務システムにアクセスする場合、CSP の管理画面から CSP が提供するサーバーの管理機能使用し、踏み台サーバー経由で業務システムにアクセスすること。
- ・受託者は、踏み台サーバーに導入済のソフトウェアを変更・削除してはならない。
- ・踏み台サーバーのストレージ容量は 130GB である。このうち、東京都クラウドインフラの利用者及び受託者が使用できる容量は、OS 領域を除いた約 100GB 弱となる。なお、OS 領域はアップデートなどによって増減する可能性があるため、利用可能な容量も変動する場合がある。
- ・受託者は、業務システムの構築や運用保守に当たって、踏み台サーバーに事前にインストールされたソフトウェア以外のソフトウェアが必要な場合には、当該ソフトウェアをインストールした運用サーバーを別途構築すること。  
また、踏み台サーバーから運用サーバーを経由し、業務システムにアクセスする構成とすること。
- ・踏み台サーバーが接続元から受け付ける同時接続数は最大 2 である。東京都クラウドインフラ利用者は受託者の構築上の必要に応じて、東京都クラウドインフラ

管理者に対して増設する申請を行うこと。

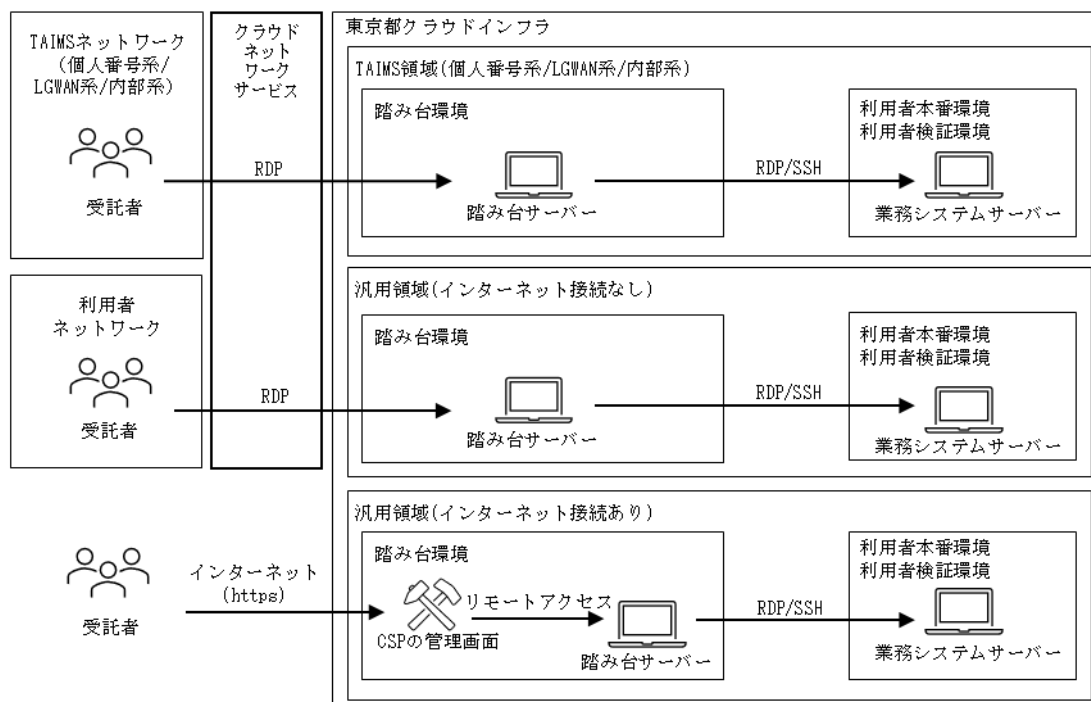


図 3-2 各領域へのアクセス方法

表 3-2 踏み台サーバーにインストール済みのソフトウェア

| # | ソフトウェア名        | 機能                                              |
|---|----------------|-------------------------------------------------|
| 1 | Tera Term      | 踏み台サーバーから業務システムの Linux OS にアクセス (SSH) する際に利用する。 |
| 2 | WinSCP         | 踏み台サーバーから業務システムにファイル転送する際に利用する。                 |
| 3 | Google Chrome  | 踏み台サーバーから業務システムにブラウザアクセスする際に利用する。               |
| 4 | Microsoft Edge | 踏み台サーバーから業務システムにブラウザアクセスする際に利用する。               |

### 3 リソース管理

#### (1) CSP 利用料管理

アカウントの利用料の確認や、想定利用料を超える場合にアラートを発報する機能等、アカウントの利用料に関する管理機能を提供する。

## (2) OS リポジトリ管理

仮想マシンの OS セキュリティパッチ、更新プログラム及びパッケージを提供する。受託者は、必要な修正プログラムや重要な更新に関するパッチをダウンロードし、業務システムに適用すること。

なお、OS セキュリティパッチは自動取得することが可能である。本機能の制限事項は、以下のとおりである。

- OS セキュリティパッチを配信する対象 OS は、表 3-1 「OS テンプレート」で提供する OS バージョンに限る。
- パッケージを配布する対象 OS は、Red Hat Enterprise Linux 及び Ubuntu に限る。
- 各ネットワーク系統に指定された OS リポジトリ以外に接続してはならない。
- 業務システムで個別の更新プログラム適用サーバーを実装する場合、本機能を参照サーバーとして指定することはできない。

## (3) ネットワーク設定変更

東京都クラウドインフラ管理者は、汎用領域（インターネット接続あり）ネットワーク向けに設置する IPS/IDS やファイアウォール等、必要なネットワークの設定変更を行う。

インターネットへのアウトバウンド通信は、ドメインフィルタリング（ブラックリスト形式）で制御する。

インターネットからのインバウンド通信は、5tuple（送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、プロトコル）で制御する。

## (4) SSL/TLS 証明書の更新

東京都クラウドインフラ管理者は、汎用領域（インターネット接続あり）ネットワークの暗号化通信に使用する外部の認証機関で発行された、SSL/TLS 証明書のインポート・更新を行う。

## (5) 名前解決

東京都クラウドインフラは、TAIMS ネットワークから CSP 環境に構築する業務システムのドメイン名を名前解決する機能を東京都クラウドインフラ利用者及び受託者からの申請に応じて提供する。

また、東京都クラウドインフラが提供する名前解決機能は、正引き（ドメイン名から IP アドレスへの変換）のみを行い、逆引き（IP アドレスからドメイン名への変換）は実施しない。

なお、インターネット経由の名前解決や、東京都クラウドインフラから TAIMS ネットワークへ名前解決などを希望する場合は、プロトコル試験申請書を用いて、デジ

タルサービス局デジタル基盤部デジタル基盤運用課ネットワーク基盤担当に申請すること。

#### (6) プライベート証明書

東京都クラウドインフラ管理者は、TAIMS 領域（個人番号系、LGWAN 系、内部系）において、東京都クラウドインフラが提供する内部ドメインを利用する東京都クラウドインフラ利用者及び受託者に対し、プライベート証明書を発行する。

内部ドメインを利用する場合、AWS Certificate Manager (ACM) Private CA 又は Private Hosted Zone を用いてプライベート証明書を発行する必要がある。Private CA 及び Private Hosted Zone の管理主体は東京都クラウドインフラであり、東京都クラウドインフラ利用者では証明書を直接発行できない。

このため、証明書は東京都クラウドインフラ管理者が発行し、東京都クラウドインフラ利用者及び受託者が証明書のインポート・更新を行う。

なお、東京都クラウドインフラが提供する内部ドメインを利用しない場合は、東京都クラウドインフラ利用者及び受託者が任意の手段で証明書を取得し、自らインポート・更新を行う必要がある。

また、業務システム用サブネット上の Amazon EC2 などのリソースをターゲットとする ALB に対する証明書の関連付け（アタッチ）及び更新作業についても、東京都クラウドインフラ利用者及び受託者にて行う必要がある。

### 4 セキュリティ管理

#### (1) クラウドセキュリティ管理

東京都クラウドインフラ管理者は、CSP が提供するリソースの不正な設定変更の監査、セキュリティ状況の監視及びログの保管を行う。本機能の制限事項は、以下のとおりである。

- ・東京都クラウドインフラ管理者が収集するログに対する変更や削除はできない。

#### (2) 仮想マシンセキュリティ保護

内部系及び汎用領域（インターネット接続あり）の仮想マシンに対して、侵入検知、マルウェア対策、ふるまい検知、改ざん検知等、仮想マシンのセキュリティ保護機能を提供する。本機能の制限事項は、以下のとおりである。

- ・受託者は、本機能で提供する各機能のセキュリティポリシーを変更できない。
- ・受託者は、東京都クラウドインフラ管理者によってあらかじめ設定された OS テンプレートの各 OS パラメータの設定や、事前にインストールされた各種管理用のエ

ージェントの変更・削除等を行うことができない。

- ・東京都クラウドインフラが提供する OS テンプレートから仮想マシンを作成した場合、セキュリティ機能の競合による誤動作防止のため、Microsoft Defender など他の仮想マシンセキュリティ保護を行う機能を有効化してはならない。

#### (3) ネットワークセキュリティ保護

業務システム、踏み台サーバーへの通信などを対象としたファイアウォール機能を提供する。ファイアウォールの通信設定は、東京都クラウドインフラ利用者及び受託者からの申請に応じて東京都クラウドインフラ管理者が行う。

また、東京都クラウドインフラ管理者は、汎用領域（インターネット接続あり）の本番環境ネットワーク上に設置する IPS/IDS やファイアウォール等のログ収集や監視を行い、脅威を検知する。業務システムにて対処が必要な場合には、東京都クラウドインフラ管理者から東京都クラウドインフラ利用者及び受託者に通知する。

#### (4) 環境及びネットワーク系統を跨いだ通信

東京都クラウドインフラには東京都のポリシーが適用されるため、原則としてネットワーク系統を跨いだ通信はできず、また、本番環境と検証環境及び試験環境は、開発中資産等の本番環境への誤反映防止の観点から分離されている。ただし、東京都クラウドインフラ管理者は、同一環境の TAIMS 領域（内部系）から汎用領域（インターネット接続あり）への一方向の通信のみを可能にする機能及び同一ネットワーク系統の本番環境と通信可能な検証環境及び試験環境を東京都クラウドインフラ利用者及び受託者からの申請に応じて提供する。この場合、接続先の汎用領域（インターネット接続あり）に VPC エンドポイント及び NLB を作成すること。

上記以外の環境及びネットワーク系統を跨いだ通信を希望する場合は、東京都クラウドインフラ管理者及び東京都デジタルサービス局総務部情報セキュリティ課へ相談の上、協議をすること。

### 5 セキュリティ診断支援

東京都クラウドインフラ利用者及び受託者は、東京都サイバーセキュリティポリシーに準じて脆弱性対策を行い、定期的な確認と措置を行うこと。東京都クラウドインフラ管理者は、セキュリティ診断時における受託者及び東京都クラウドインフラ利用者からの問合せに対応し、診断実施期間の監視抑止を支援する。

### 6 東京都クラウドインフラポータルサイト

東京都クラウドインフラ利用者及び受託者は、東京都クラウドインフラの提供する

東京都クラウドインフラポータルサイトから、問合せ受付やインシデント情報等を閲覧できる。

東京都クラウドインフラポータルサイトによって東京都クラウドインフラ利用者及び受託者に提供する機能は、表 3-3「東京都クラウドインフラポータルサイト」のとおり。

表 3-3 東京都クラウドインフラポータルサイト

| # | 東京都クラウドインフラポータルサイト機能一覧 | 機能内容詳細                                |
|---|------------------------|---------------------------------------|
| 1 | 問合せ窓口                  | 各種問合せ、作業依頼及び障害報告                      |
| 2 | セキュリティインシデント           | 不正なアクセスやサイバー攻撃等、発生したセキュリティインシデント情報の閲覧 |
| 3 | インシデント発生状況レポート         | セキュリティに係るもの以外を含む、インシデント発生状況レポートの閲覧    |
| 4 | お知らせ情報                 | サービスの計画停止やリリース情報等の事前閲覧                |

各ネットワーク系統に提供される機能

東京都クラウドインフラの各ネットワーク系統に提供される機能を示す。

なお、凡例は以下のとおりである。

○：提供する機能

—：提供しない機能

(1) リソース提供機能

表 3-4 リソース提供機能

| # | 機能名                         | 個人<br>番号系 | LGWAN<br>系 | 内部系 | 汎用領域（イン<br>ターネット<br>接続なし） | 汎用領域（イン<br>ターネット<br>接続あり） |
|---|-----------------------------|-----------|------------|-----|---------------------------|---------------------------|
| 1 | CSP 環境の提供機能                 | ○         | ○          | ○   | ○                         | ○                         |
| 2 | OS テンプレート                   | ○         | ○          | ○   | ○                         | ○                         |
| 3 | ネットワーク接続                    | ○         | ○          | ○   | ○                         | —                         |
| 4 | インターネット接続（IPS/IDS 及び WAF 付） | —         | —          | —   | —                         | ○                         |
| 5 | 踏み台サーバー                     | ○         | ○          | ○   | ○                         | ○                         |

(2) リソース管理

表 3-5 リソース管理

| # | 機能名                | 個人<br>番号系 | LGWAN<br>系 | 内部系 | 汎用領域（イン<br>ターネット<br>接続なし） | 汎用領域（イン<br>ターネット<br>接続あり） |
|---|--------------------|-----------|------------|-----|---------------------------|---------------------------|
| 1 | CSP 利用料管理          | ○         | ○          | ○   | ○                         | ○                         |
| 2 | OS リポジトリ管理         | ○         | ○          | ○   | ○                         | ○                         |
| 3 | ネットワーク設定<br>変更     | —         | —          | —   | —                         | ○                         |
| 4 | SSL/TLS 証明書の<br>更新 | —         | —          | —   | —                         | ○                         |
| 5 | 名前解決               | ○         | ○          | ○   | —                         | —                         |

| # | 機能名                | 個人<br>番号系 | LGWAN<br>系 | 内部系 | 汎用領域（イン<br>ターネット<br>接続なし） | 汎用領域（イン<br>ターネット<br>接続あり） |
|---|--------------------|-----------|------------|-----|---------------------------|---------------------------|
| 1 | CSP 利用料管理          | ○         | ○          | ○   | ○                         | ○                         |
| 2 | OS リポジトリ管理         | ○         | ○          | ○   | ○                         | ○                         |
| 3 | ネットワーク設定<br>変更     | —         | —          | —   | —                         | ○                         |
| 4 | SSL/TLS 証明書の<br>更新 | —         | —          | —   | —                         | ○                         |
| 6 | プライベート証明<br>書      | ○         | ○          | ○   | —                         | —                         |

### (3) セキュリティ管理

表 3-6 セキュリティ管理

| # | 機能名                | 個人<br>番号系 | LGWAN<br>系 | 内部系 | 汎用領域（イン<br>ターネット<br>接続なし） | 汎用領域（イン<br>ターネット<br>接続あり） |
|---|--------------------|-----------|------------|-----|---------------------------|---------------------------|
| 1 | クラウドセキュリ<br>ティ管理   | ○         | ○          | ○   | ○                         | ○                         |
| 2 | 仮想マシンセキュ<br>リティ保護  | —         | —          | ○   | —                         | ○                         |
| 3 | ネットワークセキ<br>ュリティ保護 | ○         | ○          | ○   | ○                         | ○                         |

### (4) 東京都クラウドインフラポータルサイト

表 3-7 東京都クラウドインフラポータルサイト

| # | 機能名    | 個人<br>番号系 | LGWAN<br>系 | 内部系 | 汎用領域（イン<br>ターネット<br>接続なし） | 汎用領域（イン<br>ターネット<br>接続あり） |
|---|--------|-----------|------------|-----|---------------------------|---------------------------|
| 1 | ポータル機能 | ○         | ○          | ○   | ○                         | ○                         |

## 第4 料金体系

### 1 東京都クラウドインフラの料金構造

東京都クラウドインフラに係る経費は、東京都クラウドインフラ基本機能に係る「基本機能部分（基盤分）」、各局等の利用状況に応じた「業務システム分に係る経費（従量課金分）」及び「業務システムの開発・運用保守に係る経費」の3つの経費で構成される。

受託者は、「業務システム分に係る経費（従量課金分）」及び「業務システムの開発・運用保守に係る経費」の見積りを行うこと。

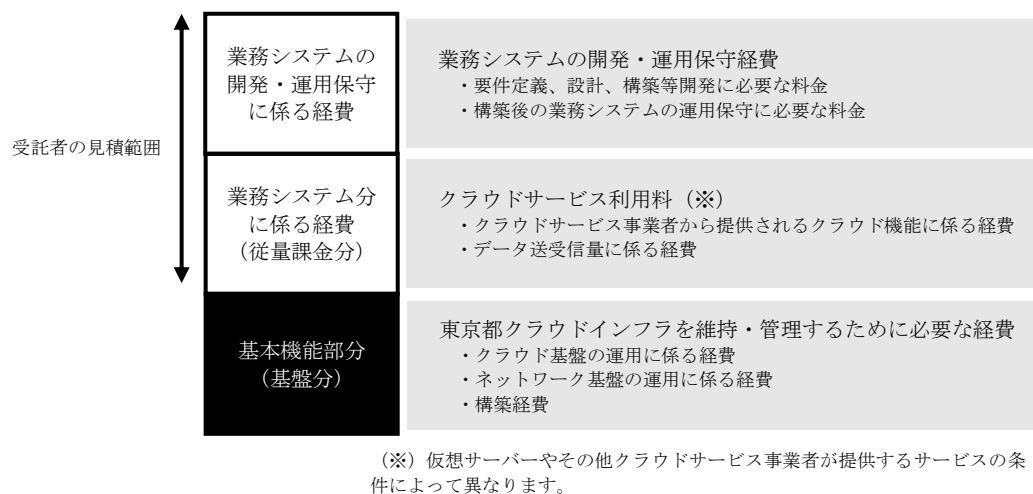


図 4-1 経費の内訳

### 2 「業務システム分に係る経費（従量課金分）」の見積り留意事項

#### (1) AWS

受託者は、AWS Pricing Calculator 等を利用し、サービスごとの利用料を算出し、AWS のサービス利用に係る利用料を見積ること。

### 3 サービスレベルの考え方

クラウドインフラサービスのサービスレベルは、各 CSP が定める SLA に準拠する。受託者は、各 CSP の SLA を参照し、業務システムの可用性や業務継続性の要件に応じて、技術的対応策を講じること。CSP が定める SLA 未達時における、CSP からの返金対応については、CSP との契約に従い、東京都クラウドインフラ管理者で必要な対応を行う。

(別紙1) 改訂履歴

| #  | 改訂年月日      | 版     | 改訂内容                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|------------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 令和5年12月22日 | 0.5   | 新規作成                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 2  | 令和6年1月15日  | 0.7   | 内容の一部加筆、修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 3  | 令和6年4月8日   | 0.8   | 内容の一部加筆、修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 4  | 令和6年5月14日  | 0.8.1 | 内容の一部加筆、修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5  | 令和6年6月21日  | 0.9   | 機密性をBからCに変更                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 6  | 令和6年11月20日 | 1.0.0 | 文書構成の修正、内容の一部加筆、修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 7  | 令和6年11月29日 | 1.0.1 | スケジュールの追加、内容の一部修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 8  | 令和7年2月6日   | 1.1.0 | 内容の一部加筆、修正                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 9  | 令和7年4月11日  | 1.2.0 | <ul style="list-style-type: none"> <li>・改訂履歴：(別紙1)として記載し、既存の別紙の番号を修正</li> <li>・図1-1本文書と関連文書の関係：「東京都クラウドインフラ利用ガイド」から「東京都クラウドインフラ利用手続ガイド」に修正</li> <li>・第2-2-(7)東京都クラウドインフラ利用開始までの流れ：提供までの流れを具体的に追記</li> <li>・表2-4東京都クラウドインフラ管理者のセキュリティ機能の実装範囲：#2に「内部系」を追加。追加に伴い、表3-6を修正</li> <li>・図3-1：東京都クラウドインフラ提供機能の全体像：名前解決及びネットワーク系統を跨いだ通信を追加。追加に伴い、第3-3-(5)、第3-4-(4)の項を追加。第2-2-(5)を軽微な修正。</li> <li>・第3-2-(3)：ネットワーク接続：文面の修正に伴い、別紙4を追加</li> <li>・図4-1経費の内訳：業務システムのクラウド機能の利用に係る経費の記載内容を修正</li> </ul> |
| 10 | 令和7年6月10日  | 1.3.0 | <ul style="list-style-type: none"> <li>・リージョンによって利用できるサービスに違いがあることを記載</li> <li>・踏み台サーバーへの同時接続数を記載</li> <li>・別紙4の利用者ネットワークの接続についての記載を全面的に改訂</li> <li>・図2-2クラウドネットワークサービスの全</li> </ul>                                                                                                                                                                                                                                                                                                   |

|    |                 |         |                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|-----------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                 |         | <p>体像へ「検証環境及び試験環境」の図を追加</p> <ul style="list-style-type: none"> <li>・図 3-1 東京都クラウドインフラの提供機能の全体像内の画像を差し替え</li> <li>・表 2-1 提供環境の定義の#2 へ本番環境との差異についての説明を追加</li> <li>・第 2-2-(5) ネットワーク分離説明へネットワーク系統だけではなく、環境についての記載を追加</li> <li>・第 3-4-(4) ネットワーク系統を跨いだ通信の説明へネットワーク領域や系統だけではなく、環境についての記載を追加</li> <li>・表 2-2 クラウドネットワーク一覧：項番 3 の文面の修正に伴い、別紙 5 を追加</li> <li>・表 2-5 作業の役割分担：項番 3 の文面の追加に伴い、別紙 6 を追加</li> </ul> |
| 11 | 令和 7 年 7 月 11 日 | 1. 3. 1 | <ul style="list-style-type: none"> <li>・第 2-2-(1)：誤記修正</li> <li>・表 2-5 作業の役割分担：誤記修正</li> <li>・図 4-1 経費の内訳：全体的な文言の修正及び業務システムの利用状況に応じた経費について、「サポートに係る経費」及び「踏み台サーバーの使用料」を削除</li> <li>・別紙 3 の誤記修正</li> <li>・別紙 4 の「ネットワーク接続要件書」に事業者への提供条件の文言を追加。誤字の修正</li> <li>・別紙 6 の誤字修正</li> </ul>                                                                                                                      |
| 12 | 令和 7 年 7 月 28 日 | 1. 4    | <ul style="list-style-type: none"> <li>・第 1-2：誤記修正</li> <li>・第 2：誤記修正</li> <li>・第 3-5：誤字修正</li> <li>・別紙 3 の利用可能な AWS サービスの制約について追記。一部、表記修正及び誤記修正</li> <li>・別紙 4 の構内配線工事の手続を見直して修正。</li> <li>・別紙 7 の追加</li> <li>・別紙 8 の追加</li> </ul>                                                                                                                                                                    |
| 13 | 令和 7 年 8 月 8 日  | 1. 4. 1 | <ul style="list-style-type: none"> <li>・別紙 8 の内容を修正</li> </ul>                                                                                                                                                                                                                                                                                                                                         |

|    |                  |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14 | 令和 7 年 10 月 27 日 | 1.5 | <ul style="list-style-type: none"> <li>・第 1-1：図 1-1 について修正</li> <li>・第 2-1：区市町村及び政策連携団体の記載を削除</li> <li>・第 2-2-(1)：図 2-1 の修正</li> <li>・第 2-2-(2)：記載を修正</li> <li>・第 2-2-(5)：記載を修正。図 2-2 を削除。表 2-2 の#5 について一部追記。</li> <li>・第 2-2-(7)：誤記の修正。図 2-3 における用語について記載を修正</li> <li>・第 2-3-(1)：図 2-4 の修正。表 2-4 の#5, #6 の修正及び#8 の追加</li> <li>・第 2-3-(2)：表 2-5 の#2 を修正</li> <li>・第 3-1：図 3-1 について修正</li> <li>・第 3-2-(1)：用語の修正及び制限事項について記載を追加</li> <li>・第 3-2-(3)：誤記を修正</li> <li>・第 3-2-(4)：WAF 及び証明書に関する記載を追加</li> <li>・第 3-2-(5)：制限事項について追記。表 3-2 の#4 について記載を追加。図 3-2 を修正</li> <li>・第 3-3-(2)：更新プログラム及びパッケージ、制限事項について記載を追加</li> <li>・第 3-3-(3)：ファイアウォール及び通信制御について記載を追加</li> <li>・第 3-3-(5)：名前解決機能について記載を追加</li> <li>・第 3-3-(6)：プライベート証明書について記載を追加</li> <li>・第 3-4-(1)：制限事項について記載を追加</li> <li>・第 3-4-(2)：制限事項について記載を追加</li> <li>・第 3-4-(3)：ファイアウォールに関する記載を追加</li> <li>・第 3-4-(4)：本番環境と検証環境及び試験環境の通信について記載を修正</li> <li>・第 3-6-(1)：表 3-4 の#1 及び#4 について記</li> </ul> |
|----|------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  | <p>載を修正</p> <ul style="list-style-type: none"> <li>・第 3-6-(2) : 表 3-5 の#2 について修正及び#6 について記載を追加</li> <li>・第 3-6-(3) : 表 3-6 の#3 について記載を修正</li> <li>・第 4-1 : 本文及び図 4-1 の記載を修正</li> <li>・第 4-2 : 題目の記載を修正</li> <li>・別紙 2 : (旧) #5、18、20、21 を削除及び (新) #35-41 を追加</li> <li>・別紙 3-2 : 記載の修正及びサービスの統制に関する記載を追加</li> <li>・別紙 4-1 : 図 1 の修正</li> <li>・別紙 7 : (旧) No. 1、2 の修正及び No. 3 ファイアウォールの記載について削除。(新) #3 の内容を修正及び#11 IPS/IDS、WAF について記載を追加</li> <li>・別紙 8 : 表 1 の注釈を追記。表 2 の内容を修正</li> </ul> |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

(別紙2) 用語の定義

本文書で用いる用語の定義を記載する。

| #  | 用語                | 内容                                                                                                     |
|----|-------------------|--------------------------------------------------------------------------------------------------------|
| 1  | 東京都クラウドインフラ       | 東京都が各局等に対して提供するクラウドサービスの利用環境及びクラウドサービスまでの専用接続回線                                                        |
| 2  | 業務システム            | 各局等が管理運用する情報システム                                                                                       |
| 3  | クラウド転換の基本方針       | 東京都が定めた、業務システムのクラウドベースへの転換に当たり、基本方針を定めたドキュメント                                                          |
| 4  | CSP               | Cloud Service Provider の略称。クラウドサービスを提供する事業者                                                            |
| 5  | 東京都サイバーセキュリティ基本方針 | 東京都が実施するサイバーセキュリティ対策に関する基本的な事項を定め、情報資産の機密性、完全性及び可用性を維持することを目的にした基本方針                                   |
| 6  | 東京都サイバーセキュリティポリシー | 東京都サイバーセキュリティ基本方針及びサイバーセキュリティ対策基準<br>なお、東京都サイバーセキュリティ対策基準は、契約締結後、都から受託者に提供する。                          |
| 7  | TAIMS             | Tokyo Advanced Information Management System の略称。東京都高度情報化推進システム                                        |
| 8  | ネットワーク系統          | 東京都クラウドインフラにおける、TAIMS 領域の「個人番号系」、「LGWAN 系」、「内部系」、「汎用領域（インターネット接続あり）」、及び「汎用領域（インターネット接続なし）」のそれぞれのネットワーク |
| 9  | LGWAN             | Local Government Wide Area Network の略称。地方公共団体を結ぶ行政専用のネットワーク                                            |
| 10 | 汎用領域              | 東京都クラウドインフラ内において、全ての東京都クラウドインフラ利用者が利用可能な領域                                                             |
| 11 | 汎用領域（インターネット接続なし） | 汎用領域において、各局等の独自閉域向けのネットワーク                                                                             |
| 12 | 汎用領域（インターネット接続あり） | 汎用領域において、インターネットからのアクセスが必要な業務システム向けの系統で、TAIMS 領域の内部系から接続するネットワーク                                       |
| 13 | 東京都クラウドインフラ管理者    | 東京都クラウドインフラ全体を維持・管理する者                                                                                 |

|    |                           |                                                                                                                                                                    |
|----|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14 | 東京都クラウドインフラ利用者            | 東京都クラウドインフラを利用する各局等の業務システム管理者及び担当者                                                                                                                                 |
| 15 | 受託者                       | 各局等から業務システムの構築運用に必要な業務を受託した事業者                                                                                                                                     |
| 16 | Amazon Web Services (AWS) | Amazon Web Services, Inc. が提供するクラウドコンピューティングサービス                                                                                                                   |
| 17 | 各局等                       | 東京都組織規程（昭和27年東京都規則第164号）第8条第1項に規定する本庁の局、室及び住宅政策本部、中央卸売市場、東京都公営企業組織条例（昭和27年東京都条例第81号）第1条の規定により設置された局、教育庁、選挙管理委員会事務局、人事委員会事務局、監査事務局、労働委員会事務局、収用委員会事務局、警視庁、東京消防庁及び議会局 |
| 18 | CSP アカウント                 | CSPが発行する、東京都クラウドインフラ内の機能を利用するための権限                                                                                                                                 |
| 19 | EPP                       | Endpoint Protection Platform の略称。PC や仮想マシン等の端末（エンドポイント）をマルウェア感染から守るセキュリティ対策の1つ                                                                                     |
| 20 | EDR                       | Endpoint Detection and Response の略称。マルウェアを検知し、デバイスを隔離する等の対処を行うための仕組み                                                                                               |
| 21 | 多要素認証                     | 複数の認証情報を用いる認証方法                                                                                                                                                    |
| 22 | 踏み台サーバー                   | 外部から東京都クラウドインフラ内の目的の仮想マシンにアクセスするために設置するサーバー                                                                                                                        |
| 23 | IPS                       | Intrusion Prevention System の略称。外部とクラウド内の通信の監視を行い、不正アクセスを検知し遮断する機能                                                                                                 |
| 24 | IDS                       | Intrusion Detection System の略称。外部とクラウド内の通信の監視を行い、不正アクセスを検知し管理者に通知する機能                                                                                              |
| 25 | ジャンボフレーム                  | イーサネット標準の最大フレームサイズ（1,518 バイト）を超えるフレームサイズ                                                                                                                           |
| 26 | VPC                       | Virtual Private Cloud の略称。クラウド上に構築するプライベートなネットワーク領域で、IP アドレス設計やルーティング制御が可能な仮想ネットワーク                                                                                |

|    |                      |                                                                                     |
|----|----------------------|-------------------------------------------------------------------------------------|
| 27 | サブネット                | 仮想ネットワーク内の IP アドレス空間を分割し、用途やアクセス制御に応じて論理的に区切るための単位                                  |
| 28 | NLB                  | Network Load Balancer の略称。TCP/UDP など L4 レイヤーの通信を対象に、宛先ポートや IP アドレスに応じてトラフィックを分散する機能 |
| 29 | TGW                  | Transit Gateway の略称。複数の VPC やオンプレミス環境をハブ&スポーク型で接続し、ルーティングを集約・管理する機能                 |
| 30 | TGW アタッチメント          | Transit Gateway に接続するための論理的なリンク。経路制御の単位としても機能する                                     |
| 31 | VPC Endpoint         | クラウド内のサービスや他の仮想ネットワークに対し、インターネットを経由せずプライベートな接続を行うための機能                              |
| 32 | VPC Endpoint Service | 自 VPC 内のサービスを、別の VPC からセキュアに接続できるようにする公開機能                                          |
| 33 | Availability Zone    | クラウド事業者が提供する物理的に独立したデータセンター群。障害の影響を局所化し、高可用性を実現するために用いられる                           |
| 34 | 共通アクセスネットワーク         | 複数のネットワークやシステムが集約的に接続される中継基盤                                                        |
| 35 | WAF                  | Web Application Firewall の略称。Web アプリケーションを狙った攻撃から保護するための機能                          |
| 36 | RDP                  | Remote Desktop の略称。手元の端末から PC やサーバーに接続できる仕組み                                        |
| 37 | OS リポジトリ             | OS に関連するソフトウェアやパッケージや更新プログラムなどを一元管理するサーバー                                           |
| 38 | CSP の特権ユーザー          | システムの設定変更などあらゆる操作が可能な権限を持つユーザー                                                      |
| 39 | ALB                  | Application Load Balancer の略称。共通アクセスネットワーク内に配置され、アプリケーションレベルで負荷分散を行う機能              |
| 40 | CSPM                 | Cloud Security Posture Management の略称。CSP サービスの設定を監視し、潜在的な脆弱性を検知する機能                |
| 41 | CSP 環境               | CSP アカウントと他のリソース及びサービスを含んだ環境                                                        |

### (別紙3) 利用可能なサービス一覧

#### 1 東京都クラウドインフラで利用可能な AWS サービス

東京都クラウドインフラ管理者は、AWS Solution Provider Program を使用し、受託者に AWS 環境を提供する。利用可能な AWS サービスについては、下記 URL を参照すること。

【AWS Solution Provider Program 認定済み AWS サービス一覧】

<https://s3-us-west-2.amazonaws.com/solution-provider-program-legal-documents/Solution+Provider+Program+List+of+Services.pdf>

なお、サービス名の後ろに「\*」が記載されたサービスは、利用条件があるため、事前に東京都クラウドインフラ管理者に利用可否等を確認すること。

また、【AWS Solution Provider Program 認定済み AWS サービス一覧】に記載されたサービスのうち、東京都クラウドインフラの領域ごとに一部利用できないサービスがある。詳細は、「2 東京都クラウドインフラの領域ごとの制約」を参照すること。

#### 2 東京都クラウドインフラの領域ごとの制約

「1 東京都クラウドインフラで利用可能な AWS サービス」で示したサービスのうち、東京都クラウドインフラの領域ごとの制約を示す。

| # | 領域       | 制約                                                                                                                                                                                                                                                                                                                                                                                  |
|---|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 全ての領域    | 管理者機能のため利用できない AWS サービスを以下に示す。 <ul style="list-style-type: none"><li>• AWS Control Tower</li><li>• AWS Direct Connect</li><li>• AWS Direct Connect Gateway</li><li>• AWS Marketplace</li><li>• AWS Organizations</li><li>• AWS VPN</li></ul> また、以下の購入オプションは会計上の理由により、現在利用できない。 <ul style="list-style-type: none"><li>• AWS Savings Plans</li><li>• AWS Reserved Instances</li></ul> |
| 2 | TAIMS 領域 | 「東京都サイバーセキュリティ対策基準」に基づき、インターネットと直接通信するサービス (Amazon Simple Email Service (Amazon SES) など) の利用を制限する。<br>利用可能なサービスについても、設計及び設定によりインターネットと直接通信が可能な場合があるため、個人番号                                                                                                                                                                                                                          |

|   |      |                                                                                                     |
|---|------|-----------------------------------------------------------------------------------------------------|
|   |      | 系、LGWAN 系及び内部系の分離を順守し、通信については利用者責任にて管理・判断をすること。                                                     |
| 3 | 汎用領域 | 原則として制約はない。ただし、東京都クラウドインフラが提供する共通アクセスネットワークを経由せずにインターネットに接続するサービスを利用する場合は、受託者の責任でセキュリティ対策などを実施すること。 |

また TAIMS 領域（個人番号系、LGWAN 系、内部系）、汎用領域（インターネット接続あり）、汎用領域（インターネット接続なし）における AWS サービスの統制について、AWS サービスの使用可否・機能制限の可否を示す。

| #  | サービス名                                   | 提供有無 |     | 分類<br>(※) | 使用可否          |               |               |                 |                 | 個別の統制方針など                                                               |
|----|-----------------------------------------|------|-----|-----------|---------------|---------------|---------------|-----------------|-----------------|-------------------------------------------------------------------------|
|    |                                         | 東日本  | 西日本 |           | TAIMS 領域      |               |               | 汎用領域            |                 |                                                                         |
|    |                                         |      |     |           | 個人番号系         | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                         |
| 1  | AWS Amplify                             | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 2  | AWS App Mesh                            | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 3  | AWS App Runner                          | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 4  | AWS AppFabric                           | ○    | ×   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                         |
| 5  | AWS AppSync                             | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 6  | AWS Application Discovery Service       | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 7  | AWS Application Migration Service (MGN) | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 8  | AWS Artifact                            | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             | 新規承諾については、AWS アカウントの統制上、管理環境のみで使用し、<br>利用者環境では使用不可                      |
| 9  | AWS Audit Manager                       | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 10 | AWS Auto Scaling                        | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 11 | AWS Backup                              | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 12 | AWS Batch                               | ○    | ○   | ⑥         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 13 | AWS Billing and Cost Management         | ○    | ○   | ⑤         | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | 発注書、請求設定、一括請求設定、Cost Categories、コスト配分タグ<br>は使用不可。Savings Plans の購入も利用不可 |
| 14 | AWS Budgets                             | ○    | ×   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 15 | AWS Certificate Manager                 | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 16 | AWS Chatbot                             | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 17 | AWS Clean Rooms                         | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 18 | AWS Cloud Control API                   | ○    | ○   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                         |
| 19 | AWS Cloud Map                           | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 20 | AWS Cloud9                              | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2024/7)                                                        |
| 21 | AWS CloudFormation                      | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 22 | AWS CloudHSM                            | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 23 | AWS CloudShell                          | ○    | ○   | ⑦         | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | VPC 内で起動させた場合、AWS マネジメントコンソールから仮想サーバ<br>ーへ接続可能となるため使用不可。踏み台経由でアクセスすること。 |
| 24 | AWS CloudTrail                          | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 25 | AWS CodeArtifact                        | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 26 | AWS CodeBuild                           | ○    | ○   | ⑦         | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | TAIMS 領域では VPC 内での起動に制限                                                 |
| 27 | AWS CodeCommit                          | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2024/7)                                                        |
| 28 | AWS CodeDeploy                          | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 29 | AWS CodePipeline                        | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 30 | AWS Compute Optimizer                   | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 31 | AWS Config                              | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                         |
| 32 | AWS Control Tower                       | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | AWS アカウントの統制に利用するサービスのため、管理環境のみで使用<br>し、利用者環境では使用不可                     |
| 33 | AWS Data Exchange                       | ○    | ×   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                         |
| 34 | AWS Data Pipeline                       | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                         |
| 35 | AWS DataSync                            | ○    | ○   | ⑦         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS<br>領域では使用不可                          |

| #  | サービス名                                    | 提供有無 |     | 分類<br>(※) | 使用可否<br>TAIMS 領域 |               |               | 汎用領域            |                 | 個別の統制方針など                                                             |
|----|------------------------------------------|------|-----|-----------|------------------|---------------|---------------|-----------------|-----------------|-----------------------------------------------------------------------|
|    |                                          | 東日本  | 西日本 |           | 個人番号系            | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                       |
| 36 | AWS Database Migration Service           | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 37 | AWS Deadline Cloud                       | ○    | ×   | ②         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                       |
| 38 | AWS Direct Connect                       | ○    | ○   | ①         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            | 閉域接続は共通アクセスネットワークアカウントでの接続に限定するため、利用者環境では使用不可                         |
| 39 | AWS Directory Service                    | ○    | ○   | ⑥         | 使用可<br>(制限付き)    | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | ディレクトリ情報を別の AWS アカウントと共有可能。<br>共有先アカウントの制限は不可のため、TAIMS 領域では共有機能のみ使用不可 |
| 40 | AWS Elastic Beanstalk                    | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 41 | AWS Elastic Disaster Recovery (DRS)      | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 42 | AWS Elemental MediaConnect               | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 43 | AWS Elemental MediaConvert               | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 44 | AWS Elemental MediaLive                  | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 45 | AWS Elemental MediaPackage               | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 46 | AWS Elemental MediaStore                 | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 47 | AWS Elemental MediaTailor                | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 48 | AWS Entity Resolution                    | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 49 | AWS Fargate                              | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 50 | AWS Fault Injection Service              | ○    | ×   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 51 | AWS Firewall Manager                     | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 52 | AWS Global Accelerator                   | ○    | ○   | ④         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 53 | AWS Glue                                 | ○    | ○   | ⑦         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可                           |
| 54 | AWS Health Dashboard                     | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 55 | AWS IAM Identity Center                  | ○    | ○   | ⑤         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            | 利用者環境では IAM ユーザーを使用するため本サービスは使用不可                                     |
| 56 | AWS IQ                                   | ○    | ○   | ②         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                       |
| 57 | AWS Identity and Access Management (IAM) | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 58 | AWS IoT Analytics                        | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 59 | AWS IoT Core                             | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 60 | AWS IoT Device Defender                  | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 61 | AWS IoT Device Management                | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 62 | AWS IoT Events                           | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 63 | AWS IoT Greengrass                       | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 64 | AWS IoT SiteWise                         | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 65 | AWS IoT TwinMaker                        | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 66 | AWS Key Management Service               | ○    | ○   | ⑦         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 67 | AWS Lake Formation                       | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 68 | AWS Lambda                               | ○    | ○   | ⑦         | 使用可<br>(制限付き)    | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | TAIMS 領域では VPC 内での起動に制限                                               |
| 69 | AWS Launch Wizard                        | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                       |
| 70 | AWS License Manager                      | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                       |
| 71 | AWS Mainframe Modernization              | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラ管理者まで問合せすること。                                     |
| 72 | AWS Managed Services                     | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラ管理者まで問合せすること。                                     |

| #   | サービス名                                 | 提供有無 |     | 分類<br>(※) | 使用可否              |               |               |                 |                 | 個別の統制方針など                                                                                      |
|-----|---------------------------------------|------|-----|-----------|-------------------|---------------|---------------|-----------------|-----------------|------------------------------------------------------------------------------------------------|
|     |                                       | 東日本  | 西日本 |           | TAIMS 領域<br>個人番号系 | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                                                |
|     |                                       |      |     |           |                   |               |               |                 |                 | と。                                                                                             |
| 73  | AWS Marketplace                       | ○    | ○   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サードパーティ製品、サードパーティーOS テンプレートの使用を禁止するために、利用者環境では使用不可                                             |
| 74  | AWS Migration Hub                     | ○    | ×   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 75  | AWS Network Firewall                  | ○    | ○   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 76  | AWS OpsWorks for Chef Automate        | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 77  | AWS OpsWorks for Puppet Enterprise    | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 78  | AWS Organizations                     | ○    | ○   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                |
| 79  | AWS Outposts                          | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラ管理者まで問合せすること。                                                              |
| 80  | AWS Parallel Computing Service (PCS)  | ○    | ×   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                |
| 81  | AWS Payment Cryptography              | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 82  | AWS Private Certificate Authority     | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 83  | AWS PrivateLink                       | ○    | ○   | ⑧         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | NW 層跨ぎの通信での PrivateLink は利用者環境では作成不可                                                           |
| 84  | AWS Proton                            | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 85  | AWS Resilience Hub                    | ○    | ×   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 86  | AWS Resource Access Manager (RAM)     | ○    | ○   | ⑧         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | 東京都クラウドインフラ管理領域からのリソース共有のみを許可                                                                  |
| 87  | AWS Resource Explorer                 | ○    | ○   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                |
| 88  | AWS Resource Groups                   | ○    | ○   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                |
| 89  | AWS RoboMaker                         | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 90  | AWS Secrets Manager                   | ○    | ○   | ⑦         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 91  | AWS Security Hub                      | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 92  | AWS Security Incident Response        | ○    | ×   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                |
| 93  | AWS Security Token Service (STS)      | ○    | ○   | ⑧         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | TAIMS 領域で許可されるスイッチロール：<br>同じ環境・同じネットワーク層に属するアカウント間でのロール切替<br>同じ環境・同じネットワーク層にある踏み台用アカウントへのロール切替 |
| 94  | AWS Serverless Application Repository | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 95  | AWS Service Catalog                   | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 96  | AWS Shield                            | ○    | ○   | ⑤         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 管理領域(汎用領域(インターネット接続あり))の共通アクセスネットワーク)のみで使用とし、TAIMS 領域の利用者環境では使用不可                              |
| 97  | AWS Signer                            | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                |
| 98  | AWS Snowball                          | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラ管理者まで問合せすること。                                                              |
| 99  | AWS Snowcone                          | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラ管理者まで問合せすること。                                                              |
| 100 | AWS Step Functions                    | ○    | ○   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 101 | AWS Storage Gateway                   | ○    | ○   | ⑦         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可                                                    |
| 102 | AWS Support                           | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                |
| 103 | AWS Systems Manager                   | ○    | ○   | ⑧         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             | AWS マネジメントコンソールから EC2 ヘリモート接続する機能(Session                                                      |

| #   | サービス名                                  | 提供有無 |     | 分類<br>(※) | 使用可否              |               |               |                 |                 | 個別の統制方針など                                                                                                                                         |
|-----|----------------------------------------|------|-----|-----------|-------------------|---------------|---------------|-----------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                        | 東日本  | 西日本 |           | TAIMS 領域<br>個人番号系 | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                                                                                                   |
|     |                                        |      |     |           | (制限付き)            | (制限付き)        | (制限付き)        | (制限付き)          | (制限付き)          | Manager、Fleet Manager) は使用不可                                                                                                                      |
| 104 | AWS Transfer Family                    | ○    | ○   | ⑦         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可                                                                                                       |
| 105 | AWS Transit Gateway                    | ○    | ○   | ⑧         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | 利用者環境では TGW の作成は不可                                                                                                                                |
| 106 | AWS Trusted Advisor                    | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 107 | AWS User Notifications                 | ○    | ○   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                                   |
| 108 | AWS VPN                                | ○    | ○   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            | オンプレミスとの接続は、Direct Connect のみで提供するため使用不可                                                                                                          |
| 109 | AWS Verified Access                    | ○    | ×   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                                   |
| 110 | AWS WAF                                | ○    | ○   | ⑤         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 管理領域(汎用領域(インターネット接続あり)の共通アクセスネットワーク)のみで使用とし、TAIMS 領域の利用者環境では使用不可                                                                                  |
| 111 | AWS Well-Architected Tool              | ○    | ×   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 112 | AWS Wickr                              | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 113 | AWS X-Ray                              | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 114 | Amazon API Gateway                     | ○    | ○   | ⑧         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用者の設定ミスによって情報が他アカウントから接続できてしまうリスクがあるため、TAIMS 領域では使用不可                                                                                            |
| 115 | Amazon AppFlow                         | ○    | ×   | ④         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 116 | Amazon AppStream 2.0                   | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 117 | Amazon Application Recovery Controller | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 118 | Amazon Athena                          | ○    | ○   | ⑦         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可。                                                                                                      |
| 119 | Amazon Augmented AI (A2I)              | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 120 | Amazon Aurora                          | ○    | ○   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 121 | Amazon Bedrock                         | ○    | ○   | ②         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                                   |
| 122 | Amazon Chime                           | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 利用検討の場合は、東京都クラウドインフラまで問合せすること。                                                                                                                    |
| 123 | Amazon Chime SDK                       | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 124 | Amazon CloudFront                      | ○    | ○   | ④         | 使用不可              | 使用不可          | 使用不可          | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | 利用者環境では Internet Gateway の作成を禁止しているため、Internet Gateway への接続した利用ができない。                                                                             |
| 125 | Amazon CloudSearch                     | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 126 | Amazon CloudWatch                      | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 127 | Amazon CloudWatch Logs                 | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                   |
| 128 | Amazon CodeGuru                        | ○    | ×   | ⑧         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | 外部コードのみ接続不可とすることはできず、また対象のコードは S3 へ保管され持込みが可能となるため、TAIMS 領域では使用不可                                                                                 |
| 129 | Amazon Cognito                         | ○    | ○   | ④         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 130 | Amazon Comprehend                      | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 131 | Amazon Connect                         | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                   |
| 132 | Amazon Data Firehose                   | ○    | ○   | ⑦         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | VPC 外からの操作可能。<br>ただし、アカウント間通信の制限についてはスイッチロール可能な範囲を制限。<br>制限は、スイッチロールを提供する Security Token Service により実施。<br>(#93 の AWS Security Token Service を参照) |

| #   | サービス名                                             | 提供有無 |     | 分類<br>(※) | 使用可否<br>TAIMS 領域 |               |               | 汎用領域            |                 | 個別の統制方針など                                                                                                                                    |
|-----|---------------------------------------------------|------|-----|-----------|------------------|---------------|---------------|-----------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                   | 東日本  | 西日本 |           | 個人番号系            | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                                                                                              |
| 133 | Amazon DataZone                                   | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 134 | Amazon Detective                                  | ○    | ×   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 135 | Amazon DevOps Guru                                | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 136 | Amazon DocumentDB<br>(with MongoDB compatibility) | ○    | ×   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 137 | Amazon DynamoDB                                   | ○    | ○   | ⑦         | 使用可<br>(制限付き)    | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | TAIMS 領域では以下の統制を実施。<br>・ テーブルのデータ操作は、AWS マネジメントコンソールなどインターネットからの操作を禁止し、VPC 内からの操作のみ許可 (VPC Endpoint からのみアクセス可能)                              |
| 138 | Amazon DynamoDB Accelerator                       | ○    | ×   | ②         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                              |
| 139 | Amazon EC2 Auto Scaling                           | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 140 | Amazon ElastiCache                                | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 141 | Amazon Elastic Block Store (EBS)                  | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 142 | Amazon Elastic Compute Cloud (EC2)                | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 143 | Amazon Elastic Container Registry (ECR)           | ○    | ○   | ⑧         | 使用可<br>(制限付き)    | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可             | 使用可             | TAIMS 領域では以下の統制を実施。<br>・ パブリックリポジトリの使用は禁止<br>・ リポジトリのイメージファイルの操作は、AWS マネジメントコンソールなどインターネットからの操作を禁止し、VPC 内からの操作のみ許可 (VPC Endpoint からのみアクセス可能) |
| 144 | Amazon Elastic Container Service (ECS)            | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 145 | Amazon Elastic File System (EFS)                  | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 146 | Amazon Elastic Kubernetes Service (EKS)           | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 147 | Amazon Elastic MapReduce (EMR)                    | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 148 | Amazon Elastic Transcoder                         | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 149 | Amazon EventBridge                                | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 150 | Amazon FSx                                        | ○    | ○   | ⑥         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 151 | Amazon File Cache                                 | ○    | ×   | ②         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                              |
| 152 | Amazon FinSpace                                   | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 153 | Amazon Forecast                                   | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 154 | Amazon GameLift Servers                           | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 155 | Amazon GameLift Streams                           | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 156 | Amazon GuardDuty                                  | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 157 | Amazon IVS                                        | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 158 | Amazon Inspector                                  | ○    | ○   | ⑤         | 使用可              | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                              |
| 159 | Amazon Inspector Classic                          | ○    | ×   | ②         | 使用不可             | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                              |
| 160 | Amazon Kendra                                     | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 161 | Amazon Keyspaces (for Apache Cassandra)           | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 162 | Amazon Kinesis Data Streams                       | ○    | ○   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 163 | Amazon Kinesis Video Streams                      | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 164 | Amazon Lex                                        | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 165 | Amazon Lightsail                                  | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 166 | Amazon Location Service                           | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |
| 167 | Amazon Lookout for Metrics                        | ○    | ×   | ③         | 使用不可             | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                              |

| #   | サービス名                                       | 提供有無 |     | 分類<br>(※) | 使用可否              |               |               |                 |                 | 個別の統制方針など                                                                                                                                                                                   |
|-----|---------------------------------------------|------|-----|-----------|-------------------|---------------|---------------|-----------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                             | 東日本  | 西日本 |           | TAIMS 領域<br>個人番号系 | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                                                                                                                                             |
| 168 | Amazon Lookout for Vision                   | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 169 | Amazon Lumberyard                           | ○    | ×   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了                                                                                                                                                                                    |
| 170 | Amazon MQ                                   | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 171 | Amazon Macie                                | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 172 | Amazon Managed Blockchain                   | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 173 | Amazon Managed Grafana                      | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 174 | Amazon Managed Service for Apache Flink     | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 175 | Amazon Managed Service for Prometheus       | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 176 | Amazon Managed Streaming for Apache Kafka   | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 177 | Amazon Managed Workflows for Apache Airflow | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 178 | Amazon MemoryDB                             | ○    | ×   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 179 | Amazon Neptune                              | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 180 | Amazon OpenSearch Service                   | ○    | ○   | ⑦         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可                                                                                                                                                 |
| 181 | Amazon Personalize                          | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 182 | Amazon Pinpoint and End User Messaging      | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 183 | Amazon Polly                                | ○    | ○   | ⑤         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 184 | Amazon Quantum Ledger Database (QLDB)       | ○    | ×   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2025/7)                                                                                                                                                                            |
| 185 | Amazon QuickSight                           | ○    | ×   | ⑦         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | インターネット経由のみの接続を制限することはできないため、TAIMS 領域では使用不可                                                                                                                                                 |
| 186 | Amazon Redshift                             | ○    | ○   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 187 | Amazon Rekognition                          | ○    | ×   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 188 | Amazon Relational Database Service (RDS)    | ○    | ○   | ⑥         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 189 | Amazon Route 53                             | ○    | ○   | ⑧         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 190 | Amazon SageMaker AI                         | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 191 | Amazon Security Lake                        | ○    | ○   | ③         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                                                                             |
| 192 | Amazon Simple Email Service (SES)           | ○    | ○   | ①         | 使用不可              | 使用不可          | 使用不可          | 使用可             | 使用可             | メールの送受信が可能なサービス。<br>インターネットへのメール送受信が可能なため、TAIMS 領域では使用不可とする。<br>SES でメール送信を行う場合、SMTP 認証で IAM ユーザーが必要となるがこのユーザーは個人に紐づかないため MFA 登録はできない。そのため、MFA に関する制限において、SES でのメール送信操作は MFA 登録なしでも実行可能とする。 |
| 193 | Amazon Simple Notification Service (SNS)    | ○    | ○   | ⑦         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             | システム間またはシステムと端末間でメッセージを受信、配信するサービス。<br>SNS は VPC に紐付ける必要がないサービスなので、通信経路については留意すること。<br>システム間の通知手段として利用することを前提とし、個人情報ははじめとした機密情報の送信には利用しないこと。                                                |
| 194 | Amazon Simple Queue Service (SQS)           | ○    | ○   | ⑦         | 使用可               | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                                                                             |
| 195 | Amazon Simple Storage Service (S3)          | ○    | ○   | ⑦         | 使用可<br>(制限付き)     | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | TAIMS 領域・汎用領域において、S3 バケットのパブリックアクセスを禁止する。<br>別ネットワーク層のアカウントからの制限は利用者側で行うこと。                                                                                                                 |

| #   | サービス名                                   | 提供有無 |     | 分類<br>(※) | 使用可否          |               |               |                 |                 | 個別の統制方針など                                                                                                                          |
|-----|-----------------------------------------|------|-----|-----------|---------------|---------------|---------------|-----------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
|     |                                         | 東日本  | 西日本 |           | TAIMS 領域      | LGWAN 系       | 内部系           | インターネット接続<br>なし | インターネット接続<br>あり |                                                                                                                                    |
| 196 | Amazon Simple Workflow Service (SWF)    | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 197 | Amazon SimpleDB                         | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 198 | Amazon Timestream                       | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 199 | Amazon Transcribe                       | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 200 | Amazon Translate                        | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 201 | Amazon VPC Lattice                      | ○    | ○   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                    |
| 202 | Amazon Verified Permissions             | ○    | ○   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 203 | Amazon Virtual Private Cloud (VPC)      | ○    | ○   | ⑧         | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き) | 使用可<br>(制限付き)   | 使用可<br>(制限付き)   | 以下の作成を制限。<br>・ Internet Gateway<br>・ VPC Lattice<br>・ VPN<br>・ Verified Access<br>・ キャリアゲートウェイ<br>・ Transit Gateway<br>・ VPC ピアリング |
| 204 | Amazon WorkDocs                         | ○    | ×   | ④         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 205 | Amazon WorkSpaces                       | ○    | ×   | ④         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 206 | Amazon WorkSpaces Secure Browser        | ○    | ×   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                    |
| 207 | CloudEndure Disaster Recovery           | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2024/3)                                                                                                                   |
| 208 | CloudEndure Migration                   | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2022/9)                                                                                                                   |
| 209 | EC2 Image Builder                       | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                    |
| 210 | Elastic Load Balancing                  | ○    | ○   | ⑤         | 使用可           | 使用可           | 使用可           | 使用可             | 使用可             |                                                                                                                                    |
| 211 | FreeRTOS                                | ○    | ×   | ③         | 使用不可          | 使用不可          | 使用不可          | 使用可             | 使用可             |                                                                                                                                    |
| 212 | Red Hat OpenShift Service on AWS (ROSA) | ○    | ○   | ②         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            |                                                                                                                                    |
| 213 | VMware Cloud on AWS                     | ○    | ○   | ①         | 使用不可          | 使用不可          | 使用不可          | 使用不可            | 使用不可            | サービス提供終了(2024/4)                                                                                                                   |

※分類については以下の表に示す。

| 分類                           | 説明                                                                            | サービス使用可否                       |
|------------------------------|-------------------------------------------------------------------------------|--------------------------------|
| ① 提供不可のサービス                  | 提供終了したサービス、提供終了が発表されているサービス                                                   | 使用不可                           |
| ② 再販できないサービス                 | AWS の制約により再販できないサービス                                                          | 使用不可                           |
| ③ 要望に応じて詳細検討するサービス           | 一律で右記の使用可否を適用                                                                 | TAIMS 領域では使用不可、汎用領域では使用可       |
| ④ インターネットとの接続が必須のサービス        | CloudFront などインターネットからの接続を前提としたサービス                                           | TAIMS 領域では使用不可、汎用領域では使用可       |
| ⑤ AWS 内でのみ稼働するサービス           | 運用管理 (CloudWatch, CloudTrail 等) やセキュリティ (GuardDuty, Security Hub 等) に関連するサービス | 使用可 ※個別機能は必要に応じて制限             |
| ⑥ VPC 内でのみ稼働するサービス           | EC2 や RDS のように VPC 内でのみ稼働し、インターネットとの通信は Transit Gateway などネットワーク機能で統制可能なサービス  | 使用可 ※個別機能は必要に応じて制限             |
| ⑦ インターネットと VPC の両方と通信可能なサービス | VPC 外で稼働し、インターネットとの通信や VPC 内との通信が可能なサービス。インターネットとの通信の制限可否などにより使用可否を決定する。      | サービスの仕様・特性により使用可否・個別機能の制限要否を決定 |
| ⑧ その他                        | 上記の分類に属さないサービス。個々のサービスの特性により使用可否を決定する。                                        | サービスの仕様・特性により使用可否・個別機能の制限要否を決定 |

### 3 東京都クラウドインフラのリージョンごとに利用できない AWS サービス

「1 東京都クラウドインフラで利用可能な AWS サービス」で示したサービスにおいても、プライマリーリージョン、セカンダリーリージョンそれぞれにおいてサービスの提供が行われていない場合、受託者は、当該サービスを利用できない。

受託者は下記 URL で当該リージョンでのサービス提供の有無を確認すること。

【リージョン別に利用可能な AWS サービスのリスト】

<https://aws.amazon.com/jp/about-aws/global-infrastructure/regional-product-services/>

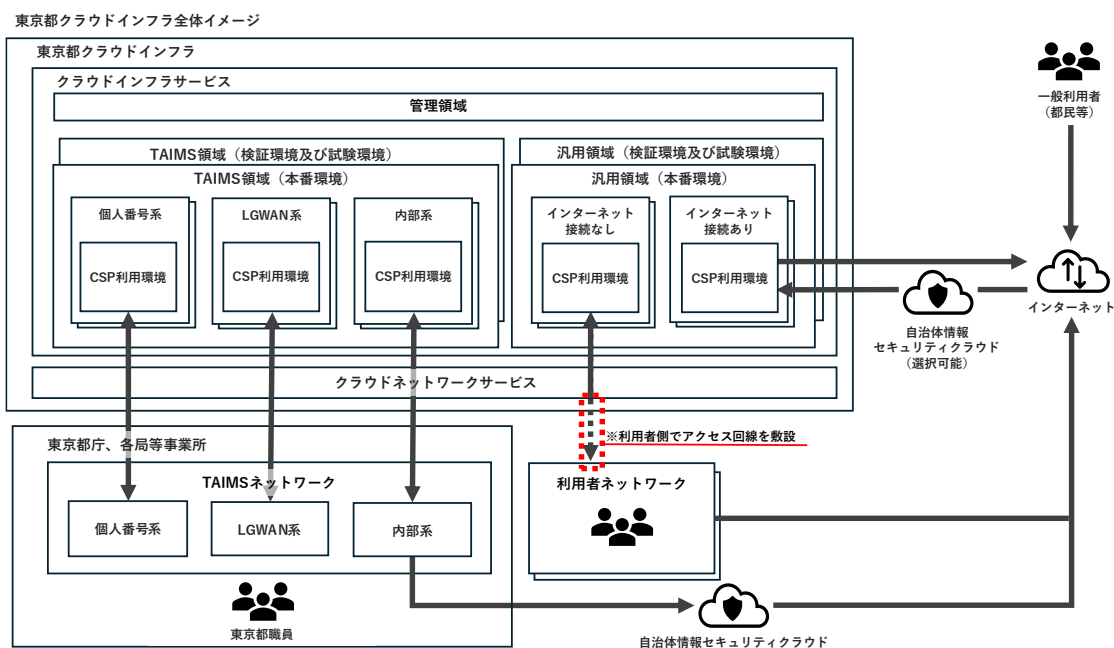
### 4 留意事項

別紙3に記載の内容は、令和7年3月31日時点の情報である。そのため、当該日以降にリリースされた AWS サービスの利用に関しては、事前に東京都クラウドインフラ管理者に利用可否等を確認すること。

## (別紙4) 利用者ネットワークの接続

### 1 概要

東京都クラウドインフラの汎用領域（インターネット接続なし）に構築した業務システムに、利用者ネットワークから接続するためには、クラウドネットワークサービスまでのアクセス回線の敷設が必要である。対象範囲については、別紙4図 1「アクセス回線の対象範囲」に赤点線で示す。



別紙4図 1 アクセス回線の対象範囲

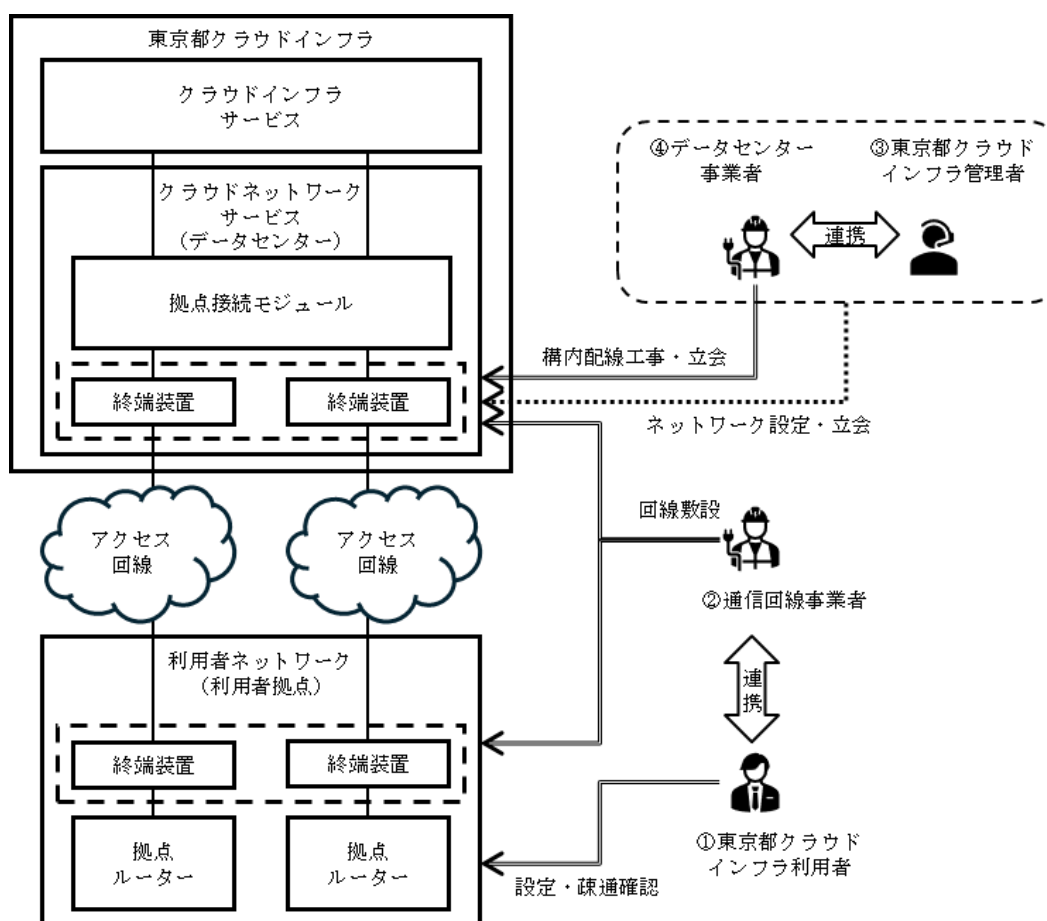
### 2 利用者ネットワーク接続時の作業概要

東京都クラウドインフラ利用者は、通信回線事業者と連携してアクセス回線の敷設を実施する。回線契約については、東京都クラウドインフラ利用者と通信回線事業者間で行うこと。

また、東京都クラウドインフラ管理者は、クラウドネットワークサービス側のネットワーク設定を実施する。

なお、クラウドネットワークサービス側の拠点（以下「データセンター」という。）では、アクセス回線の敷設以外に、クラウドネットワークサービスに接続するための構内配線工事を、データセンターを管理する事業者（以下「データセンター事業者」という。）に依頼する必要がある。データセンター事業者への構内配線工事の依頼は東京都クラウドインフラ管理者が行う。

利用者ネットワーク接続時の各担当者の作業イメージを、別紙4図 2「利用者ネットワーク接続作業の全体像」に示す。



別紙4 図 2 利用者ネットワーク接続作業の全体像

利用者ネットワーク接続時の各担当者の作業詳細を別紙4表 1「各担当者の作業詳細」に示す。

別紙4表 1 各担当者の作業詳細

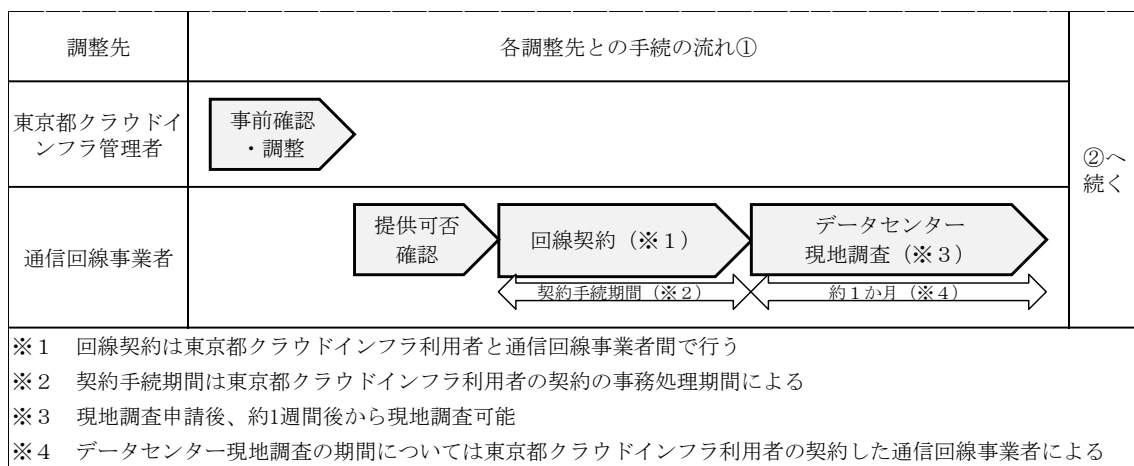
| # | 担当者            | 作業詳細                                                                               |
|---|----------------|------------------------------------------------------------------------------------|
| 1 | 東京都クラウドインフラ利用者 | 通信回線事業者と連携してアクセス回線の敷設を実施する。<br>また、利用者拠点のルーター（以下「拠点ルーター」という。）への設定及び回線敷設後の疎通確認を実施する。 |
| 2 | 通信回線事業者        | データセンター及び利用者拠点の各終端装置設置までのアクセス回線敷設を実施する。                                            |
| 3 | 東京都クラウドインフラ管理者 | クラウドネットワークサービスのネットワーク設定及びデータセンターでの立会等を実施する。                                        |
| 4 | データセンター事業者     | クラウドネットワークサービスのデータセンターで現場立会及び構内配線工事を実施する。                                          |

### 3 利用者ネットワーク接続時の手続と役割分担

#### (1) 事前確認・調整からデータセンターの現地調査までの流れ

東京都クラウドインフラ利用者は、利用者ネットワークからクラウドネットワークサービスへ接続したい場合、接続方法及びデータセンターの場所等について、事前に「クラウドネットワーク接続マニュアル」及び利用者と機密保持契約等を締結した事業者のみに提供される「ネットワーク接続要件書」を確認し、東京都クラウドインフラ管理者と調整を実施すること。その後、通信回線事業者にアクセス回線の提供可否を確認し、東京都クラウドインフラ利用者と通信回線事業者間で回線契約を行い、データセンターの現地調査を実施すること。

データセンターの現地調査を行うまでの各調整先との手続の流れ及び実施期間の目安について、別紙4図 3「利用者ネットワーク接続時の手続の流れ①」に示す。



別紙4図 3 利用者ネットワーク接続時の手続の流れ①

利用者ネットワーク接続時の各手続の内容及び役割分担を、別紙4表 2「各手続の役割分担①」に示す。

別紙4表 2 各手続の役割分担①

| # | 手続      | 内容                                                 | 役割分担                 |                |         |
|---|---------|----------------------------------------------------|----------------------|----------------|---------|
|   |         |                                                    | 凡例<br>○：担当者<br>—：対応無 |                |         |
|   |         |                                                    | 東京都クラウドインフラ利用者       | 東京都クラウドインフラ管理者 | 通信回線事業者 |
| 1 | 事前確認・調整 | クラウドネットワークサービスへの接続方法及びデータセンターの場所等について、事前確認及び調整を行う。 | ○                    | ○              | —       |

|   |                 |                                              |   |   |   |
|---|-----------------|----------------------------------------------|---|---|---|
| 2 | 提供可否確認          | 利用者拠点とクラウドネットワークサービスのデータセンターに回線が敷設できるか確認を行う。 | ○ | — | ○ |
|   | 回線契約            | アクセス回線の契約を行う。                                | ○ | — | ○ |
|   | データセンター<br>現地調査 | クラウドネットワークサービスのデータセンターの現地調査を行う。              | ○ | — | ○ |

## (2) データセンターの現地調査後から利用開始までの流れ

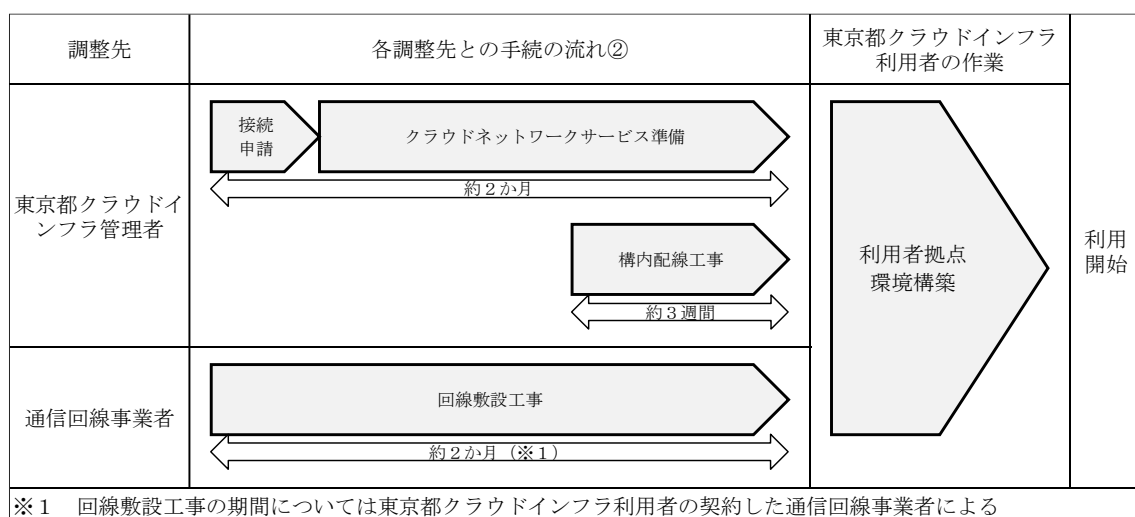
データセンターの現地調査後、東京都クラウドインフラ利用者は、各調整先にそれぞれの作業の実施を依頼すること。

東京都クラウドインフラ管理者へは、クラウドネットワークサービスの接続申請を提出し、クラウドネットワークサービスのネットワーク設定等を依頼すること。同時に、東京都クラウドインフラ管理者よりデータセンター事業者へ構内配線工事を依頼する。

通信回線事業者へは、クラウドネットワークサービスのデータセンター及び利用者拠点の各終端装置設置までの回線敷設工事を依頼すること。

各調整先の作業完了後、東京都クラウドインフラ利用者は、拠点ルーターへの設定及び回線敷設後の疎通確認等を行い、利用者拠点の環境構築を実施すること。

データセンターの現地調査後から利用開始までの各調整先との手続の流れ及び実施期間の目安について、別紙4図 4「利用者ネットワーク接続時の手続の流れ②」に示す。



別紙4図 4 利用者ネットワーク接続時の手続の流れ②

利用者ネットワーク接続時の各手続の内容及び役割分担を、別紙4表 3「各手続の役割分担②」に示す。

別紙4表 3 各手続の役割分担②

| # | 手続               | 内容                                                         | 役割分担           |                |         |            |
|---|------------------|------------------------------------------------------------|----------------|----------------|---------|------------|
|   |                  |                                                            | 東京都クラウドインフラ利用者 | 東京都クラウドインフラ管理者 | 通信回線事業者 | データセンター事業者 |
| 1 | 接続申請             | データセンター現地調査の結果に基づき、東京都クラウドインフラ管理者へ、クラウドネットワークサービスの接続申請を行う。 | ○              | —              | —       | —          |
|   | クラウドネットワークサービス準備 | 接続申請に基づき、クラウドネットワークサービスのネットワーク設定等を行う。                      | —              | ○              | —       | —          |
|   | 構内配線工事           | クラウドネットワークサービスのデータセンターの構内配線工事を行う。                          | —              | ○              | —       | ○          |
| 2 | 回線敷設工事           | クラウドネットワークサービスのデータセンター及び利用者拠点の各終端装置設置までの回線敷設を行う。           | —              | —              | ○       | —          |
| 3 | 利用者拠点環境構築        | 拠点ルーターへの設定及び回線敷設後の疎通確認等を行う。                                | ○              | —              | —       | —          |

#### 4 利用者ネットワーク接続に係る概算金額算出の際の制限事項

- ・クラウドネットワークサービスの拠点接続モジュールのインターフェース規格は、1000BASE-LX又は10GBASE-LRを採用している。このため、アクセス回線の帯域は1Gbps又は10Gbpsから選定すること。
- ・拠点ルーターをシングル構成で実装する場合は、Static ルート又は BGP (Border Gateway Protocol) を利用可能である。拠点ルーターを冗長構成で実装する場合は、BGP のみの利用となる。
- ・拠点ルーターに設定するクラウドネットワークサービス側の VLAN 番号は、東京都クラウドインフラ利用で採番することとし、採番した VLAN 番号を東京都クラウドインフラ管理者に連絡すること。
- ・ジャンボフレームを使用しないこと。
- ・その他、利用者ネットワークからクラウドネットワークサービスへの接続要件等の詳細は、「クラウドネットワーク接続マニュアル」及び利用者と機密保持契約等を締結した事業者のみに提供される「ネットワーク接続要件書」を参照すること。
- ・利用者ネットワークからクラウドネットワークサービスまでのアクセス回線は L2 専

用線又は広域イーサ網であること。回線種別と必要回線の本数の対応は別紙4表4「必要回線本数」に示す。

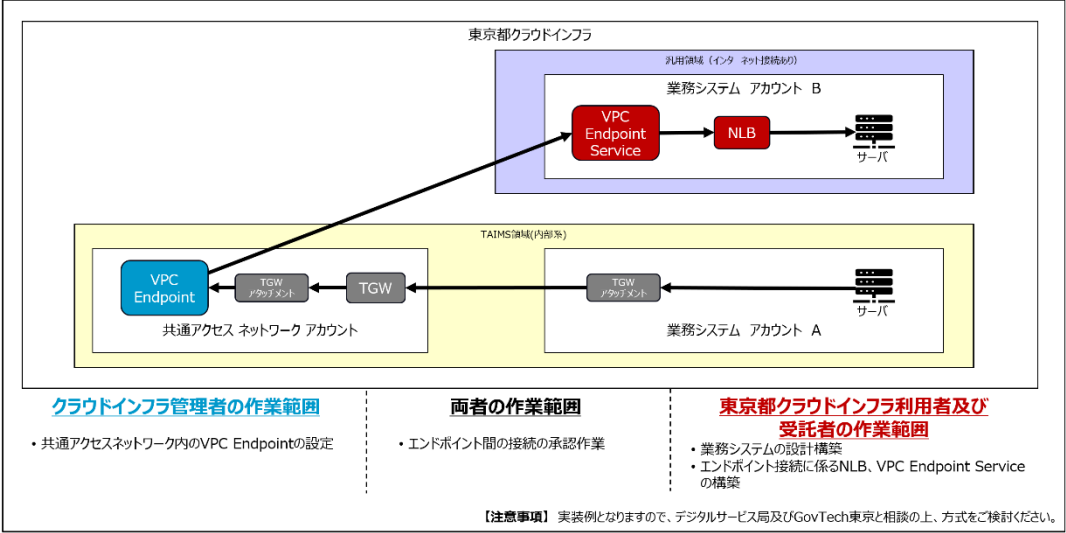
別紙4表 4 必要回線本数

| # | 回線種別   | シングル or 冗長 | 必要回線本数                               |
|---|--------|------------|--------------------------------------|
| 1 | L2 専用線 | シングル       | 起点(利用者拠点)から終点(クラウドネットワークサービス)で1回線    |
| 2 |        | 冗長         | 起点(利用者拠点)から終点(クラウドネットワークサービス)で2回線    |
| 3 | 広域イーサ網 | シングル       | 利用者拠点側で1回線、クラウドネットワークサービス側で1回線(計2回線) |
| 4 |        | 冗長         | 利用者拠点側で2回線、クラウドネットワークサービス側で2回線(計4回線) |

(別紙5) エンドポイント接続設定の作業分担

TAIMS 領域（内部系）から汎用領域（インターネット接続あり）向け一方向通信のエンドポイント接続設定の作業分担概要を以下に示す。

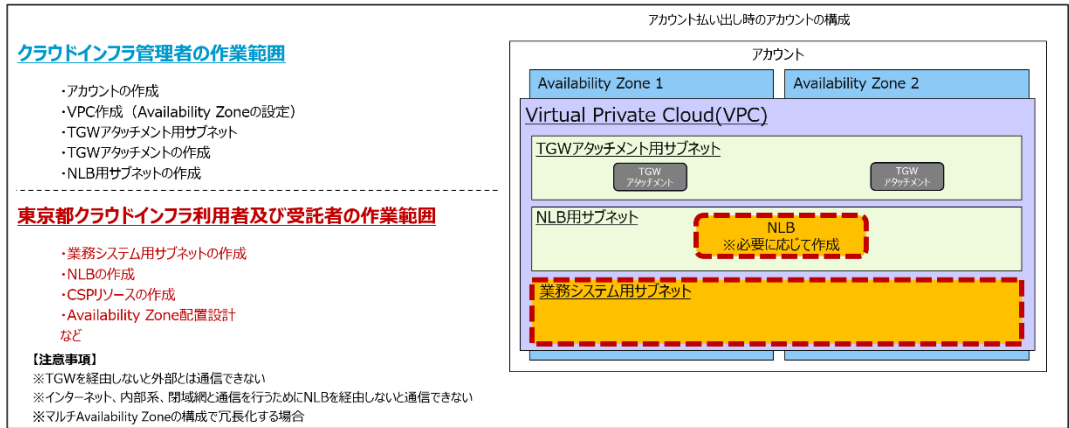
エンドポイント接続設定の作業分担



(別紙 6) 環境構築作業分担

AWS アカウント払出し後の CSP リソース作成作業分担概要を以下に示す。

環境構築作業分担



(別紙7) 設計・構築・運用・保守に関する考慮事項リスト

東京都クラウドインフラ上で業務システムを設計・構築・運用・保守するに当たり、考慮すべき事項を以下に示す。

| # | 考慮事項                          | 関係する記載箇所                        | 考慮内容                                                                                                                                                                                                    | 該当ケース(例)                              |
|---|-------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 1 | TAIMS 領域の運用保守                 | 第2-2-(5)<br>表 2-2「クラウドネットワーク一覧」 | TAIMS 領域の業務システムはインターネット経由でのアクセスが不可であるため、運用保守拠点からの遠隔保守は実施できない。<br>(TAIMS ネットワークに接続された端末がある拠点まで移動する必要がある。)<br>このため、当該対応に要する運用・保守費用を考慮する必要がある。                                                             | TAIMS 領域<br>(個人番号系、LGWAN系、内部系)の業務システム |
| 2 | 業務システムにおけるセキュリティインシデントのアラート監視 | 第2-3-(1)<br>機能の実装分担             | 受託者は、業務システムにおけるセキュリティインシデントのアラート監視及び対応を行うものとする。<br>各局等においては、これらの対応に係る設計・構築・運用・保守費用を考慮する必要がある。                                                                                                           | 全ての業務システム                             |
| 3 | BYOL の場合の運用保守費                | 第3-2-(2)<br>OS テンプレート           | 東京都クラウドインフラでは、業務システム向けに OS テンプレートを提供している。このテンプレートを利用する業務システムでは、OS 及び OS セキュリティパッチの配信が行われ、設定によっては自動アップデートも可能となる。<br>一方、OS テンプレートを利用されない場合 (BYOL: ライセンス持込みの場合)、OS、OS セキュリティパッチ、更新プログラム及びパッケージのアップデートは業務シス | TAIMS 領域、汎用領域を利用する業務システムで OS 持込みの場合   |

|   |                |                         |                                                                                                                                                                                                 |                                                            |
|---|----------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
|   |                |                         | <p>テムの利用者又は受託者が実施する必要がある。</p> <p>このため、各局等においては、これらの対応に係る設計・構築・運用・保守費用を考慮する必要がある。</p>                                                                                                            |                                                            |
| 4 | SSL/TLS 証明書の購入 | 第3-3-(4) SSL/TLS 証明書の更新 | <p>SSL/TLS 証明書を利用する場合、業務システム利用者は外部認証機関から SSL/TLS 証明書を取得する必要がある。（SSL/TLS 証明書の取得は業務システム利用者の責任、証明書のインポートと更新作業は東京都クラウドインフラ管理者の責任となる。）</p> <p>このため、各局等においては、外部認証機関から SSL/TLS 証明書の取得費用を考慮する必要がある。</p> | TAIMS 領域、汎用領域の SSL/TLS 証明書を利用する業務システム                      |
| 5 | セキュリティ診断支援     | 第3-5 セキュリティ診断支援         | <p>東京都クラウドインフラ利用者及び受託者は、東京都サイバーセキュリティポリシーに準じて脆弱性対策を行い、定期的な確認と措置を行うこと。</p> <p>このため、各局等においては、脆弱性対策を行い、定期的な確認と措置のための費用を考慮する必要がある。</p>                                                              | TAIMS 領域、汎用領域の業務システム                                       |
| 6 | Amazon RDS の利用 | 第4-1 図 4-1「経費の内訳」       | <p>Amazon RDS は、基本機能部分（基盤分）の利用料金の算出に関する考え方におけるサーバー台数のカウントに含めない。ただし、Amazon RDS には別途従量課金が発生するため、その費用は考慮する必要がある。</p>                                                                               | <p>データベースについて、AWS のマネージドサービスである Amazon RDS を利用する業務システム</p> |

|    |                                   |                         |                                                                                                                                                                                              |                                           |
|----|-----------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 7  | AWS サポート                          | 第 4-1 図<br>4-1「経費の内訳」   | AWS サポートについては、東京都クラウドインフラからエンタープライズサポートを提供するため、「業務システムのクラウド機能の利用に係る経費」における AWS サポートの料金の考慮は不要である。                                                                                             | 全ての業務システム                                 |
| 8  | Amazon EC2 の契約形態                  | 第 4-1 図<br>4-1「経費の内訳」   | Amazon EC2 の費用積算にあたっては、契約形態としてオンデマンドインスタンスを前提とする。<br>なお、リザーブドインスタンス等の割引は利用できない。                                                                                                              | Amazon EC2 を利用する業務システム                    |
| 9  | 領域、ネットワークシステムを跨ぐ通信におけるエンドポイント接続設定 | (別紙 5) エンドポイント接続設定の作業分担 | 別紙 5 に記載されているエンドポイント接続設定の作業分担において、領域やネットワークシステムを跨ぐ通信が発生する場合、東京都クラウドインフラ管理者と東京都クラウドインフラ利用者及び受託者の両者が協力してエンドポイント接続設定作業を行う必要がある。このため、領域、ネットワークシステムを跨ぐ通信が発生する場合は、各局等にてエンドポイント接続設定作業の費用を考慮する必要がある。 | 領域、ネットワークシステムを跨ぐ通信が発生する業務システム             |
| 10 | DNS (Route53)                     | -                       | 名前解決には東京都が管理する DNS を使用することが可能である。ただし、業務システム側で DNS を用意する場合は、Amazon Route 53 など CSP が提供するマネージドサービスの費用を含めて考慮する必要がある。                                                                            | 汎用領域（インターネット接続あり）において、自前で DNS を用意する業務システム |
| 11 | IPS/IDS、WAF などのサービス               | 第 3-2-(4) インターネット接続     | 東京都クラウドインフラの汎用領域（インターネット接続あり）ネットワーク向けに提供される                                                                                                                                                  | 汎用領域（インターネット接続あり）を                        |

|  |  |                    |                                                        |            |
|--|--|--------------------|--------------------------------------------------------|------------|
|  |  | (IPS/IDS 及び WAF 付) | IPS/IDS、WAF などのサービスは「基本機能部分（基盤分）」の扱いとなるため、費用の考慮は不要である。 | 利用する業務システム |
|--|--|--------------------|--------------------------------------------------------|------------|

(別紙8) 利用者環境にデフォルト設置されるリソース及びサービスの利用で発生する費用の積算

東京都クラウドインフラの利用者本番環境及び検証環境において、デフォルト設置されるリソース及びサービスの利用で発生する費用の積算方法を(別紙8) 表1「リソース及びサービスの利用で発生する費用」及び(別紙8) 表2「サーバーの管理機能通信で発生する費用」に示す。

前提条件として、東京都クラウドインフラ利用者へ提供時に管理者側で作成済みのリソースを対象とする。

また通信料については、東京都クラウドインフラの管理機能を利用するための通信のみ対象とする。

対象となるリソース及びサービスは、TGW アタッチメント、Amazon EventBridge、AWS Config、Amazon GuardDuty、AWS Security Hub、AWS Key Management Service とする。

(別紙8) 表1 リソース及びサービスの利用で発生する費用

| # | 用途                        | 費目               | 数量  |          | 備考                                                                                                                                  |
|---|---------------------------|------------------|-----|----------|-------------------------------------------------------------------------------------------------------------------------------------|
|   |                           |                  | 数量  | 課金<br>単位 |                                                                                                                                     |
| 1 | TGW アタッチメント料<br>(時間単位の課金) | TGW アタッチメントに係る費用 | 730 | /hour    | TGW アタッチメントについては、時間課金のため730h/月で費用を計算                                                                                                |
| 2 | Amazon EventBridge<br>利用料 | 固定発生分            |     |          | 利用者の利用状況に関わらず発生する費用<br>AWS 料金見積りツールにて、以下の条件で算出可能<br>・ペイロードのサイズ = 1 [KB]<br>・AWS 管理イベントの数 = 0 [100 万/月]<br>・カスタムイベントの数 = 2 [100 万/月] |
|   |                           | 利用者での利用分         | ※1  | /イベント    |                                                                                                                                     |
| 3 | AWS Config 利用料            | 固定発生分            |     |          | 利用者の利用状況に関わらず発生する費用<br>AWS 料金見積りツールにて、以下の条件で算出可能<br>・記録された継続的な設定項目の数 = 665<br>・設定ルール評価の数 = 1                                        |
|   |                           | 利用者での利用分         | ※1  | /ルール     |                                                                                                                                     |
| 4 | Amazon GuardDuty 利用料      | GuardDuty の利用料   | ※1  | /イベント    |                                                                                                                                     |

|   |                                |                  |    |       |                                                                                                                |
|---|--------------------------------|------------------|----|-------|----------------------------------------------------------------------------------------------------------------|
| 5 | AWS Security Hub 利用料           | 固定費発生分           |    |       | 利用者の利用状況に関わらず発生する費用<br>AWS 料金見積りツールにて、以下の条件で算出可能<br>・アカウント数 = 1<br>・アカウントごとのセキュリティチェックの数 = 5,000               |
|   |                                | Security Hub 利用料 | ※1 | /チェック |                                                                                                                |
| 6 | AWS Key Management Service 利用料 | 固定費発生分           |    |       | 利用者の利用状況に関わらず発生する費用<br>AWS 料金見積りツールにて、以下の条件で算出可能<br>・カスタマー管理型のカスタマーマスターキー (CMK) の数 = 1<br>・対称リクエストの数 = 333,400 |

※1 黄色網掛け部分については、利用者の利用状況に応じて変動

※2 金額については、AWS 料金見積りツールを使用して確認すること。

※3 各サービスの機能は、ガバナンス及びセキュリティの観点から必須で設置する。

(別紙 8) 表 2 サーバーの管理機能通信で発生する費用

| # | 分類                                            | 用途                                                     | 費目 ※1      | 数量 ※2 |      |
|---|-----------------------------------------------|--------------------------------------------------------|------------|-------|------|
|   |                                               |                                                        |            | 数量    | 課金単位 |
| 1 | Windows サーバーで<br>必要となるデータ通<br>信費用（1 台あた<br>り） | OS リポジトリとの通信                                           | TGW データ処理料 | 2.3   | /GB  |
|   |                                               |                                                        | 通信費用       | 2.3   | /GB  |
| 2 |                                               | EPP/EDR マネージャーとの通信<br>（汎用領域（インターネット接続<br>あり）及び内部系のみ）   | TGW データ処理料 | 1.1   | /GB  |
|   |                                               |                                                        | 通信費用       | 1.1   | /GB  |
| 3 |                                               | Endpoint Central エージェントの<br>通信                         | TGW データ処理料 | 1.5   | /GB  |
|   |                                               |                                                        | 通信費用       | 1.5   | /GB  |
| 4 | RHEL サーバーで<br>必要となるデータ通<br>信費用（1 台あた<br>り）    | OS リポジトリとの通信                                           | TGW データ処理料 | 16.5  | /GB  |
|   |                                               |                                                        | 通信費用       | 16.5  | /GB  |
| 5 |                                               | EPP/EDR マネージャーとの通信<br>（汎用領域（インターネット接続<br>あり）領域及び内部系のみ） | TGW データ処理料 | 1.1   | /GB  |
|   |                                               |                                                        | 通信費用       | 1.1   | /GB  |

|                                              |                                  |                            |            |     |     |
|----------------------------------------------|----------------------------------|----------------------------|------------|-----|-----|
| 6                                            |                                  | Endpoint Central エージェントの通信 | TGW データ処理料 | 1.5 | /GB |
|                                              |                                  |                            | 通信費用       | 1.5 | /GB |
| 7                                            | Ubuntu サーバーで必要となるデータ通信費用（1 台あたり） | OS リポジトリとの通信               | TGW データ処理料 | 1.2 | /GB |
|                                              |                                  |                            | 通信費用       | 1.2 | /GB |
| EPP/EDR マネージャーとの通信（汎用領域（インターネット接続あり）及び内部系のみ） |                                  | TGW データ処理料                 | 1.1        | /GB |     |
|                                              |                                  | 通信費用                       | 1.1        | /GB |     |
| 9                                            |                                  | Endpoint Central エージェントの通信 | TGW データ処理料 | 1.5 | /GB |
|                                              |                                  |                            | 通信費用       | 1.5 | /GB |

※1 TGW のデータ処理及び通信に係る費用は、OUT 分の通信料のみ発生する。

※2 「数量」は、1 か月間あたりの通信量となる。

※3 金額については、AWS 料金見積りツールを使用して確認すること。

東京都交通局

自動車部様

「自動車部データプラットフォーム」

全体計画

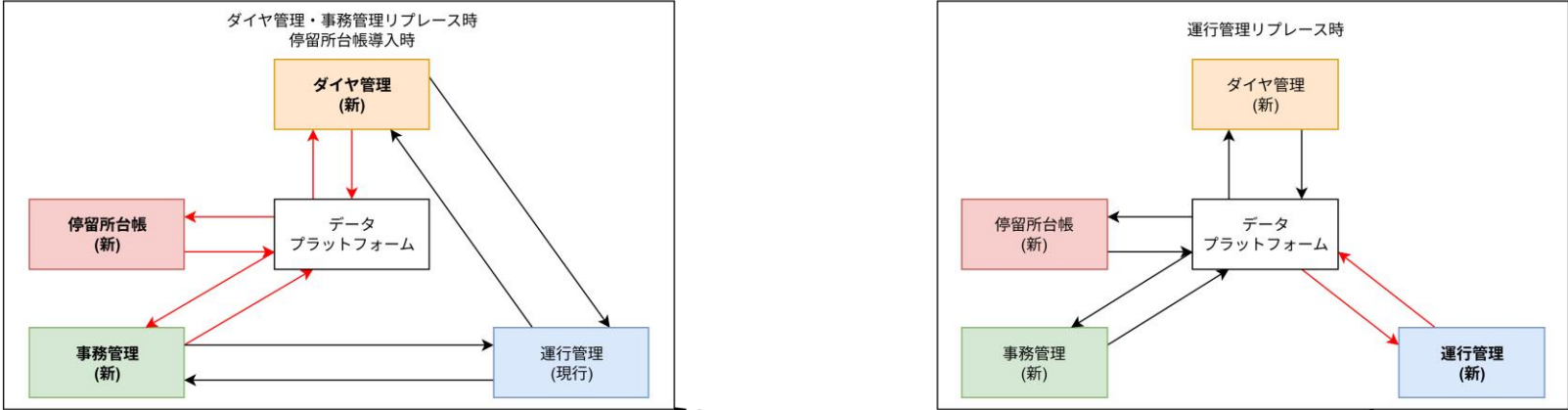
(第1.1版)

令和7年10月16日

株式会社 日立システムズ

# 連携の切替方針

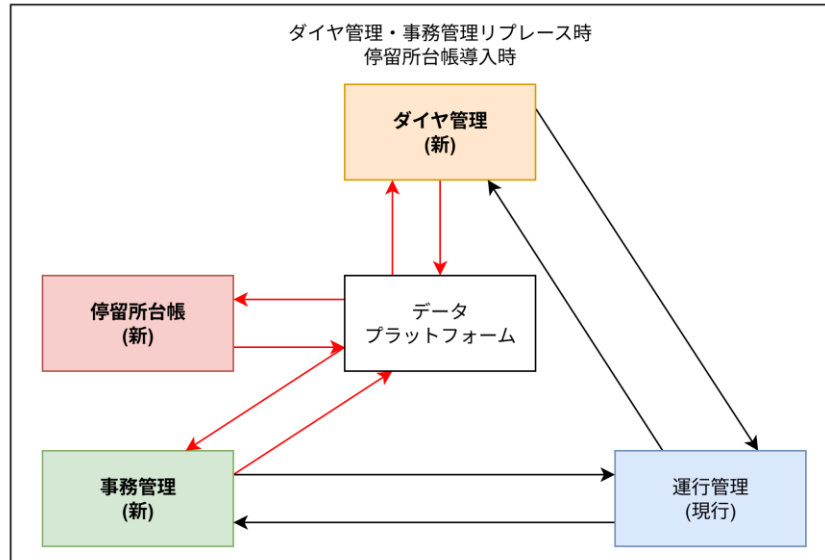
ダイヤ管理、事務管理、停留所台帳、運行管理での例



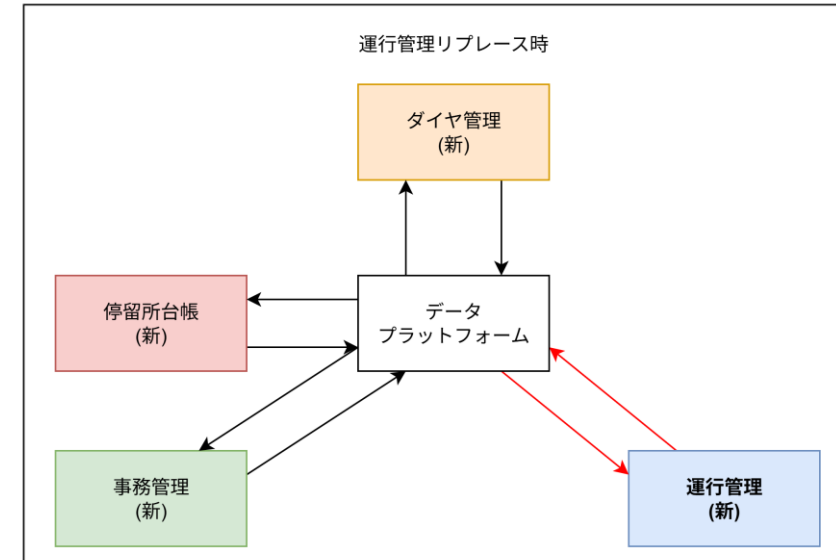
| 項番 | 大分類       | 中分類 | 2025年度（令和7年度） |    |    |    |    |    |     |     |     |    |    |    | 2026年度（令和8年度）       |    |    |    |    |    |     |     |     |    |    |    | 2027年度（令和9年度） |    |    |    |    |    |     |     |     |    |    |    |
|----|-----------|-----|---------------|----|----|----|----|----|-----|-----|-----|----|----|----|---------------------|----|----|----|----|----|-----|-----|-----|----|----|----|---------------|----|----|----|----|----|-----|-----|-----|----|----|----|
|    |           |     | 4月            | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 4月                  | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 4月            | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
| 1  | ダイヤ管理アプリ  |     | 調査            |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | 要件定義（5/30迄）         |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | 設計・製造・単体テスト         |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | CT・ST               |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
|    |           |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 2  | 事務管理アプリ   |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 3  | 勤務管理      |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 4  | 収入金管理     |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 5  | 車両管理      |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 6  | 乗務員台帳システム |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 7  | 貸切業務システム  |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 8  | 停留所台帳システム |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 9  | 出勤確認システム  |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約（最短でこの時期） |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |
| 10 | バス運行管理アプリ |     |               |    |    |    |    |    |     |     |     |    |    |    | ★ 対向システム契約          |    |    |    |    |    |     |     |     |    |    |    | ★ 連携開始        |    |    |    |    |    |     |     |     |    |    |    |

# 連携の切替方針

ダイヤ管理、事務管理、停留所台帳、運行管理での例



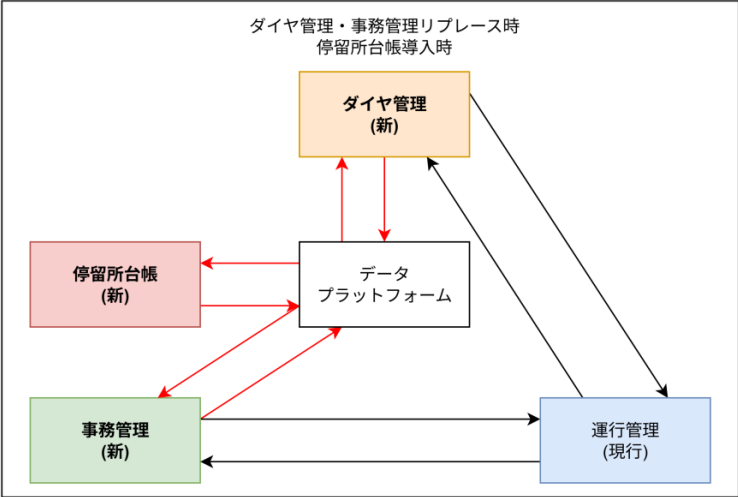
- ダイヤ管理(新)/事務管理(新)/停留所台帳(新)間の連携はデータプラットフォームを介する
- ダイヤ管理(新)と運行管理(現行)の連携は維持する
- 事務管理(新)と運行管理(現行)の連携は維持する



- ダイヤ管理(新)/事務管理(新)/停留所台帳(新)/運行管理(新)間の連携はデータプラットフォームを介する

各フェーズにおける役割分担の整理

フェーズ1 ダイヤ管理アプリ, 事務管理アプリ, 停留所台帳アプリとの連携

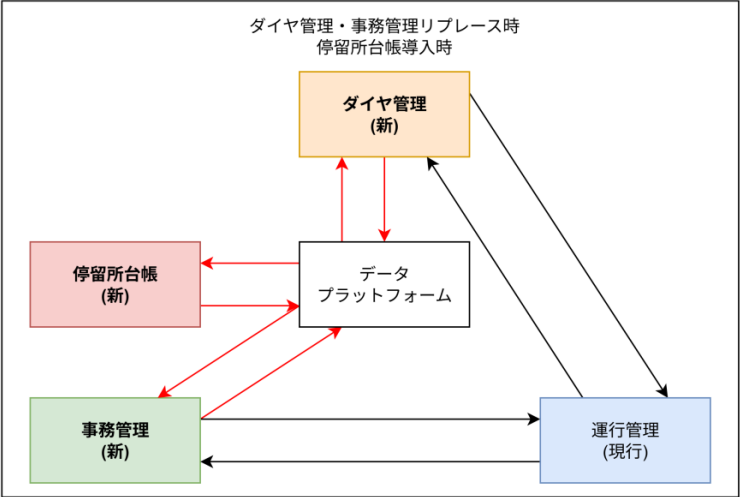


- ダイヤ管理(新)/事務管理(新)/停留所台帳(新)間の連携はデータプラットフォームを介する
- ダイヤ管理(新)と運行管理(現行)の連携は維持する
- 事務管理(新)と運行管理(現行)の連携は維持する

| No. | 区分                    | データ連携に係る検討項目/作業項目 | データPFに関する分担 |                      |       |
|-----|-----------------------|-------------------|-------------|----------------------|-------|
|     |                       |                   | 東京都様        | 業務システム事業者            | HISYS |
| 1   | ダイヤ管理(新)<br>→データPF    | 連携要件、仕様に関する検討/協議  | ○           | ダイヤ管理(新)             | ○     |
| 2   | ダイヤ管理(新)<br>→データPF    | データ出力側の設計/実装      |             | ダイヤ管理(新)             |       |
| 3   | ダイヤ管理(新)<br>→データPF    | データ受取側の設計/実装      |             |                      | ○     |
| 4   | ダイヤ管理(新)<br>→運行管理(現行) | 連携要件、仕様に関する検討/協議  | ○           | ダイヤ管理(新)<br>運行管理(現行) |       |
| 5   | ダイヤ管理(新)<br>→運行管理(現行) | データ出力側の設計/実装      |             | ダイヤ管理(新)             |       |
| 6   | ダイヤ管理(新)<br>→運行管理(現行) | (データ受取側の設計/実装)    |             | 運行管理(現行)             |       |
| 7   | 運行管理(現行)<br>→ダイヤ管理(新) | 連携要件、仕様に関する検討/協議  | ○           | ダイヤ管理(新)<br>運行管理(現行) |       |
| 8   | 運行管理(現行)<br>→ダイヤ管理(新) | データ出力側の設計/実装      |             | 運行管理(現行)             |       |
| 9   | 運行管理(現行)<br>→ダイヤ管理(新) | データ受取側の設計/実装      |             | ダイヤ管理(新)             |       |
| 10  | 事務管理(新)<br>→データPF     | 連携要件、仕様に関する検討/協議  | ○           | 事務管理(新)              | ○     |
| 11  | 事務管理(新)<br>→データPF     | データ出力側の設計/実装      |             | 事務管理(新)              |       |
| 12  | 事務管理(新)<br>→データPF     | データ受取側の設計/実装      |             |                      | ○     |
| 13  | 事務管理(新)<br>→運行管理(現行)  | 連携要件、仕様に関する検討/協議  | ○           | 事務管理(新)<br>運行管理(現行)  |       |
| 14  | 事務管理(新)<br>→運行管理(現行)  | データ出力側の設計/実装      |             | 事務管理(新)              |       |
| 15  | 事務管理(新)<br>→運行管理(現行)  | (データ受取側の設計/実装)    |             | 運行管理(現行)             |       |

各フェーズにおける役割分担の整理

フェーズ1    ダイヤ管理アプリ, 事務管理アプリ, 停留所台帳アプリとの連携

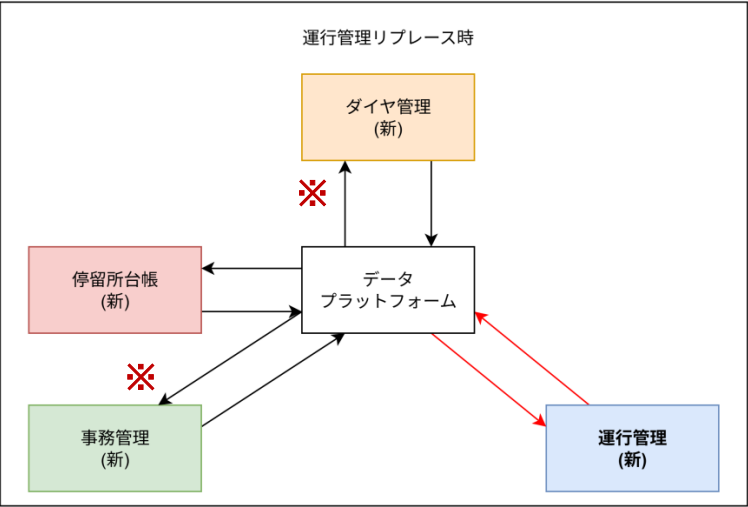


- ダイヤ管理(新)/事務管理(新)/停留所台帳(新)間の連携はデータプラットフォームを介する
- ダイヤ管理(新)と運行管理(現行)の連携は維持する
- 事務管理(新)と運行管理(現行)の連携は維持する

| No. | 区分                   | データ連携に係る検討項目/作業項目 | データPFに関する分担 |                     |       |
|-----|----------------------|-------------------|-------------|---------------------|-------|
|     |                      |                   | 東京都様        | 業務システム事業者           | HISYS |
| 16  | 運行管理(現行)<br>→事務管理(新) | 連携要件、仕様に関する検討/協議  | ○           | 事務管理(新)<br>運行管理(現行) |       |
| 17  | 運行管理(現行)<br>→事務管理(新) | データ出力側の設計/実装      |             | 運行管理(現行)            |       |
| 18  | 運行管理(現行)<br>→事務管理(新) | データ受取側の設計/実装      |             | 事務管理(新)             |       |
|     |                      |                   |             |                     |       |
| 19  | 停留所台帳(新)<br>→データPF   | 連携要件、仕様に関する検討/協議  | ○           | 停留所台帳(新)            | ○     |
| 20  | 停留所台帳(新)<br>→データPF   | データ出力側の設計/実装      |             | 停留所台帳(新)            |       |
| 21  | 停留所台帳(新)<br>→データPF   | データ受取側の設計/実装      |             |                     | ○     |
|     |                      |                   |             |                     |       |
| 22  | データPF<br>→ダイヤ管理(新)   | 連携要件、仕様に関する検討/協議  | ○           | ダイヤ管理(新)            | ○     |
| 23  | データPF<br>→ダイヤ管理(新)   | データ出力側の設計/実装      |             |                     | ○     |
| 24  | データPF<br>→ダイヤ管理(新)   | データ受取側の設計/実装      |             | ダイヤ管理(新)            |       |
|     |                      |                   |             |                     |       |
| 25  | データPF<br>→事務管理(新)    | 連携要件、仕様に関する検討/協議  | ○           | 事務管理(新)             | ○     |
| 26  | データPF<br>→事務管理(新)    | データ出力側の設計/実装      |             |                     | ○     |
| 27  | データPF<br>→事務管理(新)    | データ受取側の設計/実装      |             | 事務管理(新)             |       |
|     |                      |                   |             |                     |       |
| 28  | データPF<br>→停留所台帳(新)   | 連携要件、仕様に関する検討/協議  | ○           | 停留所台帳(新)            | ○     |
| 29  | データPF<br>→停留所台帳(新)   | データ出力側の設計/実装      |             |                     | ○     |
| 30  | データPF<br>→停留所台帳(新)   | データ受取側の設計/実装      |             | 停留所台帳(新)            |       |

各フェーズにおける役割分担の整理

フェーズ2 運行管理アプリとの連携



- ダイヤ管理(新)/事務管理(新)/停留所台帳(新)/運行管理(新)間の連携はデータプラットフォームを介する

| No. | 区分                 | データ連携に係る検討項目/作業項目                              | データPFに関する分担 |                                    |       |
|-----|--------------------|------------------------------------------------|-------------|------------------------------------|-------|
|     |                    |                                                | 東京都様        | 業務システム<br>事業者                      | HISYS |
| 1   | データPF<br>→ダイヤ管理(新) | 連携要件、仕様に関する検討/協議                               | ○           | ダイヤ管理(新)                           | ○     |
| 2   | データPF<br>→ダイヤ管理(新) | データ出力側の設計/実装                                   |             |                                    | ○     |
| 3   | データPF<br>→ダイヤ管理(新) | データ受取側の設計/実装<br>(運行管理からのデータ流入をデータPF経由に切り替える対応) |             | ダイヤ管理(新)<br>※フェーズ2においてもダイヤ管理の改修が必要 |       |
| 4   | データPF<br>→事務管理(新)  | 連携要件、仕様に関する検討/協議                               | ○           | 事務管理(新)                            | ○     |
| 5   | データPF<br>→事務管理(新)  | データ出力側の設計/実装                                   |             |                                    | ○     |
| 6   | データPF<br>→事務管理(新)  | データ受取側の設計/実装<br>(運行管理からのデータ流入をデータPF経由に切り替える対応) |             | 事務管理(新)<br>※フェーズ2においても事務管理の改修が必要   |       |
| 7   | データPF<br>→停留所台帳(新) | 連携要件、仕様に関する検討/協議                               | ○           | 停留所台帳(新)                           | ○     |
| 8   | データPF<br>→停留所台帳(新) | データ出力側の設計/実装                                   |             |                                    | ○     |
| 9   | データPF<br>→停留所台帳(新) | データ受取側の設計/実装<br>(運行管理からのデータ流入をデータPF経由に切り替える対応) |             | 停留所台帳(新)<br>※フェーズ2においても停留所台帳の改修が必要 |       |
| 7   | データPF<br>→運行管理(新)  | 連携要件、仕様に関する検討/協議                               | ○           | 運行管理(新)                            | ○     |
| 8   | データPF<br>→運行管理(新)  | データ出力側の設計/実装                                   |             |                                    | ○     |
| 9   | データPF<br>→運行管理(新)  | データ受取側の設計/実装                                   |             | 運行管理(新)                            |       |
| 10  | 運行管理(新)<br>→データPF  | 連携要件、仕様に関する検討/協議                               | ○           | 運行管理(新)                            | ○     |
| 11  | 運行管理(新)<br>→データPF  | データ出力側の設計/実装                                   |             | 運行管理(新)                            |       |
| 12  | 運行管理(新)<br>→データPF  | データ受取側の設計/実装                                   |             |                                    | ○     |