A-gate利用ガイドライン

（AWS編）

株式会社ＮＴＴデータ

改訂履歴

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 項番 | 版数 | 作成日/  修正日 | 作成者/  修正者 | 変更箇所 | 変更内容 | 変更理由 | 区分 |
| 1 | 1.00 | - | - | 新規 |  |  |  |
| 2 | 1.01 | 2020/1/6 | 山本 | 5章 | 申込書一覧を追加 | A-gateの利便性向上のため | 追加 |
| 3 | 1.02 | 2020/2/12 | 近藤 | 3.2.2権限分掌 | A-gateが定義する役割を追加 | A-gateの利便性向上のため | 追加 |
| 4 | 1.03 | 2020/4/1 | 伊藤 |  | DNS連携を削除 | ニーズがなく廃止したため | 削除 |
| 5 | 1.04 | 2021/5/4 | 山本 | 3.2.6 | Hinemosオプションにおいて、セルフサービスで設定・操作が可能な項目を記載した。 | Hinemosオプションセルフサービス化のため。 | 追加 |
| 6 | 1.04 | 2021/5/4 | 山本 | 3.2.6 | Hinemosカスタマーポータルに関する記載を追加 | Hinemosの仕様や不具合に関するお問い合わせ用にHinemosカスタマーポータルを開設したため。 | 追加 |
| 7 | 1.05 | 2021/8/23 | 佐藤 | 3.2.4 | AWS Configの取得ログの内容を修正。 | 記載に誤りがあったため。 | 修正 |
| 8 | 1.06 | 2021/11/22 | 山本 | 3.2.6 | Hinemos用AWSアカウントの操作について、セルフサービスで可能な操作を追記 | Hinemosオプションセルフサービス化において、Hinemos用のAWSアカウントで可能とする操作を改定したため。 | 追加 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

本書に記載されている会社名、製品名などは、一般に各社の商標、または登録商標である。

また、本書では、®および™は明記していない。

目　次

[1. はじめに 5](#_Toc90454927)

[1.1. 本書について 5](#_Toc90454928)

[1.1.1. 本書の目的 5](#_Toc90454929)

[1.1.2. 本書の位置づけ 5](#_Toc90454930)

[1.1.3. 対象読者 5](#_Toc90454931)

[2. A-gateとは 6](#_Toc90454932)

[2.1. A-gateとは 6](#_Toc90454933)

[2.2. A-gateにおける責任共有モデル 7](#_Toc90454934)

[2.2.1. 責任共有モデルについて 7](#_Toc90454935)

[2.2.2. A-gateを利用した場合の責任共有モデル 9](#_Toc90454936)

[3. A-gateが提供する共通基盤 10](#_Toc90454937)

[3.1. 共通基盤機能一覧 10](#_Toc90454938)

[3.2. 共通基盤機能詳細 10](#_Toc90454939)

[3.2.1. A-gateにおけるAWSアカウント構成 10](#_Toc90454940)

[3.2.2. 権限分掌 11](#_Toc90454941)

[3.2.3. ポリシー違反検知・自動修復 13](#_Toc90454942)

[3.2.4. 監査ログ収集 14](#_Toc90454943)

[3.2.5. 環境初期設定 14](#_Toc90454944)

[3.2.6. Hinemosオプション 14](#_Toc90454945)

[4. パブリッククラウド活用ガイドライン 18](#_Toc90454946)

[4.1. 導入編 18](#_Toc90454947)

[4.1.1. プラットフォーム選定指針 18](#_Toc90454948)

[4.1.2. アカウント分割指針 18](#_Toc90454949)

[4.1.3. 環境分離指針 20](#_Toc90454950)

[4.1.4. 多要素認証ルール 20](#_Toc90454951)

[4.1.5. マネジメントコンソール接続ルール 21](#_Toc90454952)

[4.1.6. 外部ベンダ向け環境接続ルール 25](#_Toc90454953)

[4.1.7. データ暗号化指針 29](#_Toc90454954)

[4.2. 設計・開発編 30](#_Toc90454955)

[4.2.1. ネットワークアクセス制御方針 30](#_Toc90454956)

[4.2.2. バックアップ取得方法 34](#_Toc90454957)

[4.2.3. インスタンス利用料支払い方法の選択 36](#_Toc90454958)

[5. 問い合わせについて 38](#_Toc90454959)

[5.1. A-gateに関する問い合わせ 38](#_Toc90454960)

[5.2. Hinemosオプションに関する問い合わせ 38](#_Toc90454961)

[6. 作業依頼について 38](#_Toc90454962)

# はじめに

## 本書について

### 本書の目的

本書では主に以下を説明する。

* A-gateの利用開始にあたり理解しておくべきA-gateの基礎知識・機能仕様
* A-gate上でテナントシステムの構築を始めるにあたって社内で定めるべきルール・指針
* 個別のテナントシステムの設計・構築にあたるノウハウ

### 本書の位置づけ

他のドキュメントとの位置づけを「図 1‑1 A-gateのドキュメント体系」に示す。

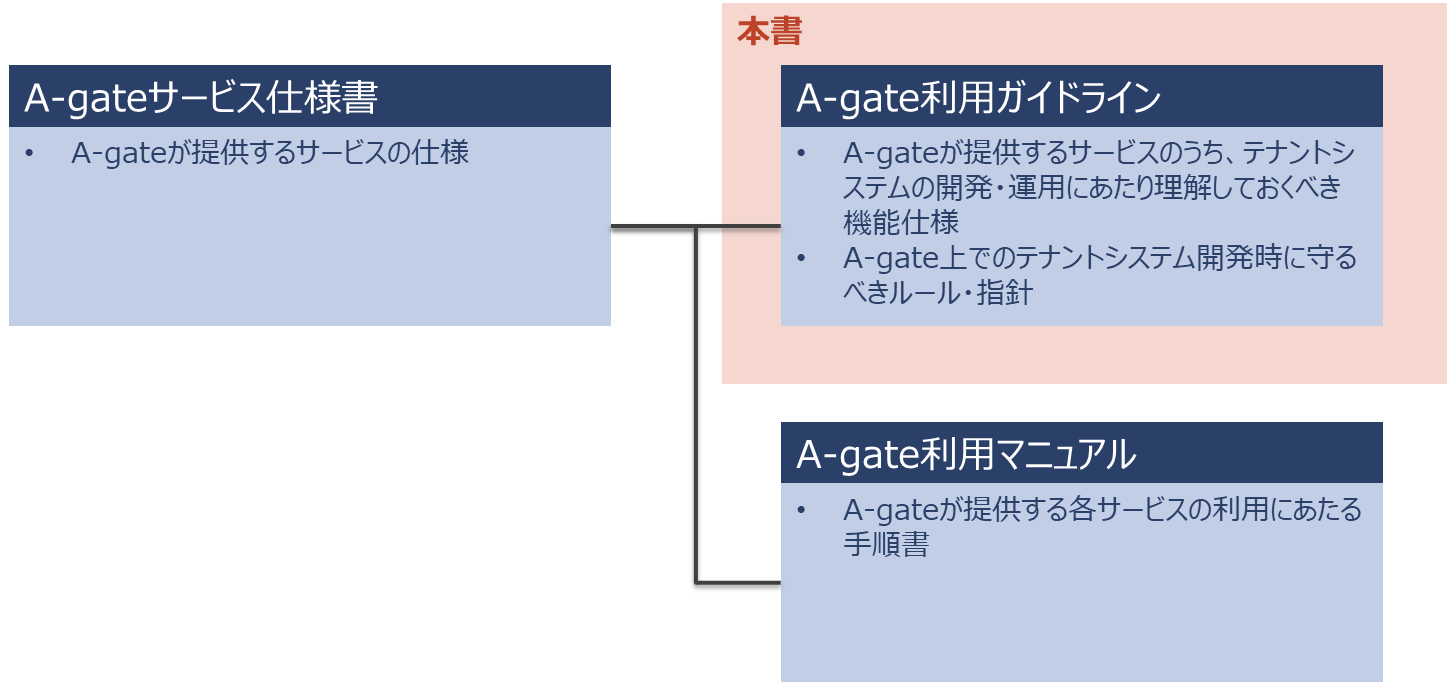


図 1‑1 A-gateのドキュメント体系

### 対象読者

* A-gateのスタートアップコンサルの内容を受け、利用者の社内やPJ内の各種ルールの整備を行う担当者
* テナントシステムの設計・構築を行う担当者

# A-gateとは

## A-gateとは

概要

A-gateは、パブリッククラウド（AWS/Azure/GCP/OCI）の導入から運用までを一元的に支援するサービスである。

A-gateを利用することで、専門的な知識を持った組織やセキュアに利用するための仕組みを自前で確立・維持することなく、パブリッククラウドが有する自由度や利便性を享受することができる。

A-gateでは、大きく分けて「スタートアップコンサル」、「仮想データセンタ構築・運用」、「マネージドCCoE」の3つのサービスを提供する。（「図 2‑1 A-gateが提供する3つのサービス」参照）

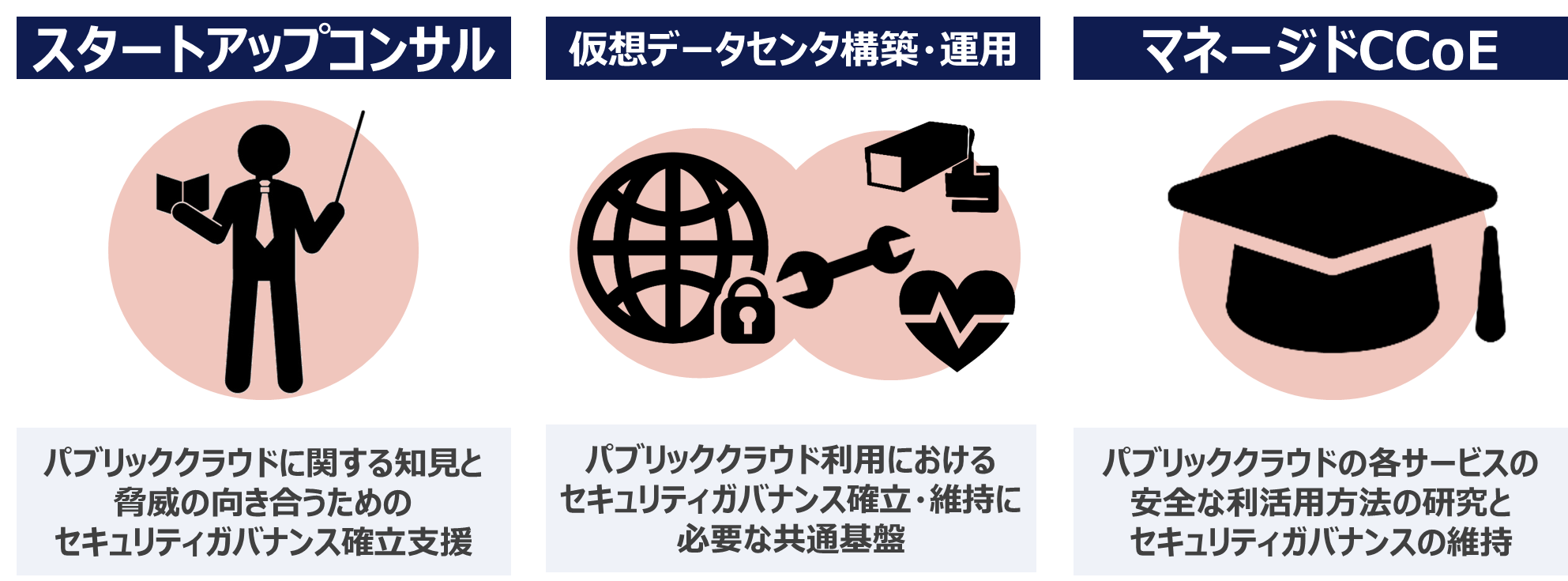


図 2‑1 A-gateが提供する3つのサービス

#### A-gateとクラウドジャーニー

一般に、組織がパブリッククラウドを活用していくためには、パブリッククラウドの導入・活用にあたる中長期的なロードマップである「クラウドジャーニー」を描き、それに沿って段階を踏むことが肝要とされている。

A-gateは「クラウドジャーニー」のうち、パブリッククラウドに関する高度なノウハウ・知見を要する工程・作業において、各種支援・サービスを提供する。（「図 2‑2 クラウドジャーニーとA-gateの支援範囲」参照）

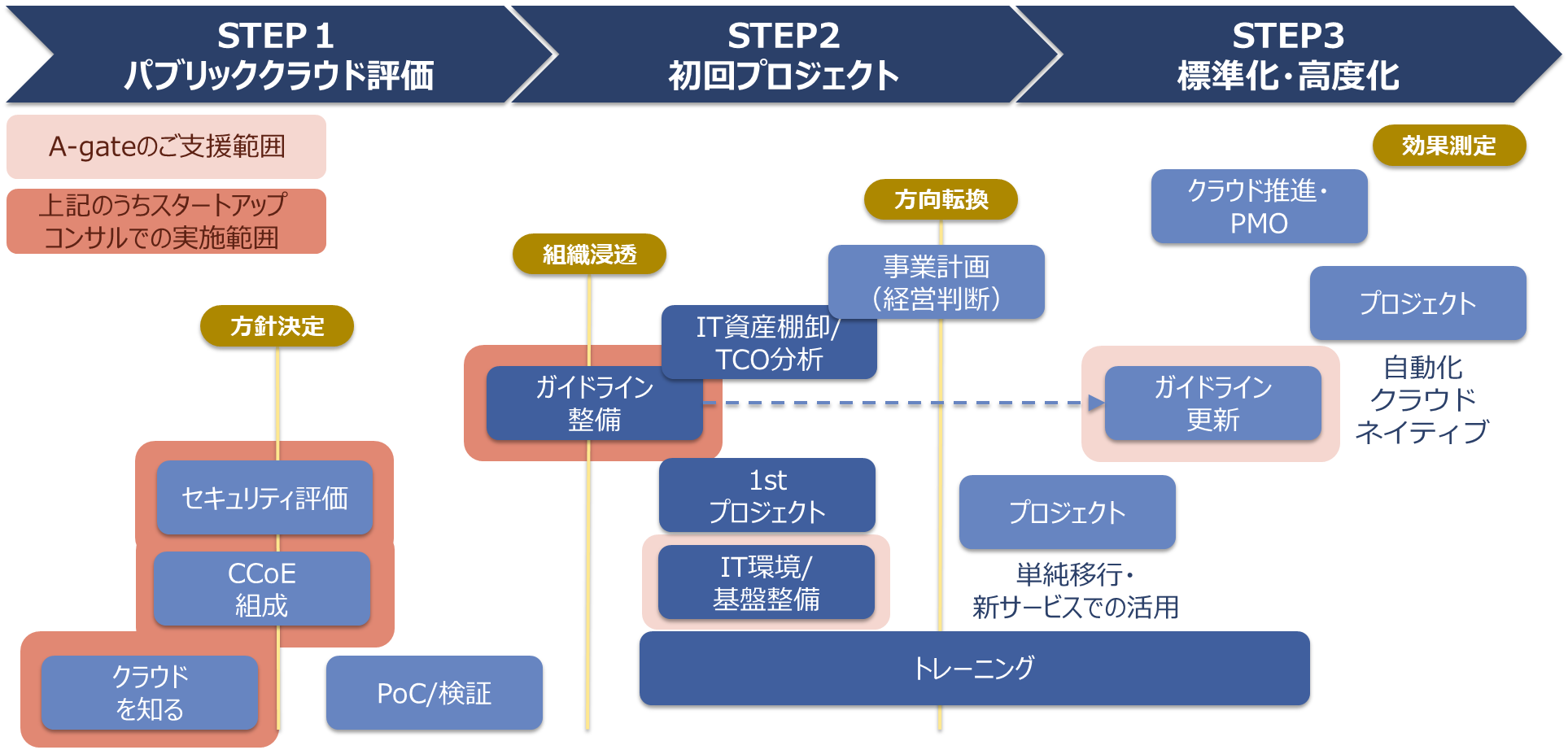


図 2‑2 クラウドジャーニーとA-gateの支援範囲

## A-gateにおける責任共有モデル

### 責任共有モデルについて

パブリッククラウド上に構築するシステムのセキュリティの担保にあたり、クラウドベンダは一般に「責任共有モデル」を採用している。「責任共有モデル」とは、クラウド事業者と利用者で責任を負う範囲を分担し、システム全体のセキュリティを担保する考え方である。

AWS、Azureにおける責任共有モデルの考え方を「図 2‑3 AWSが提唱する責任共有モデル」、「図 2‑4 Microsoftが提唱する責任共有モデル」に示す。

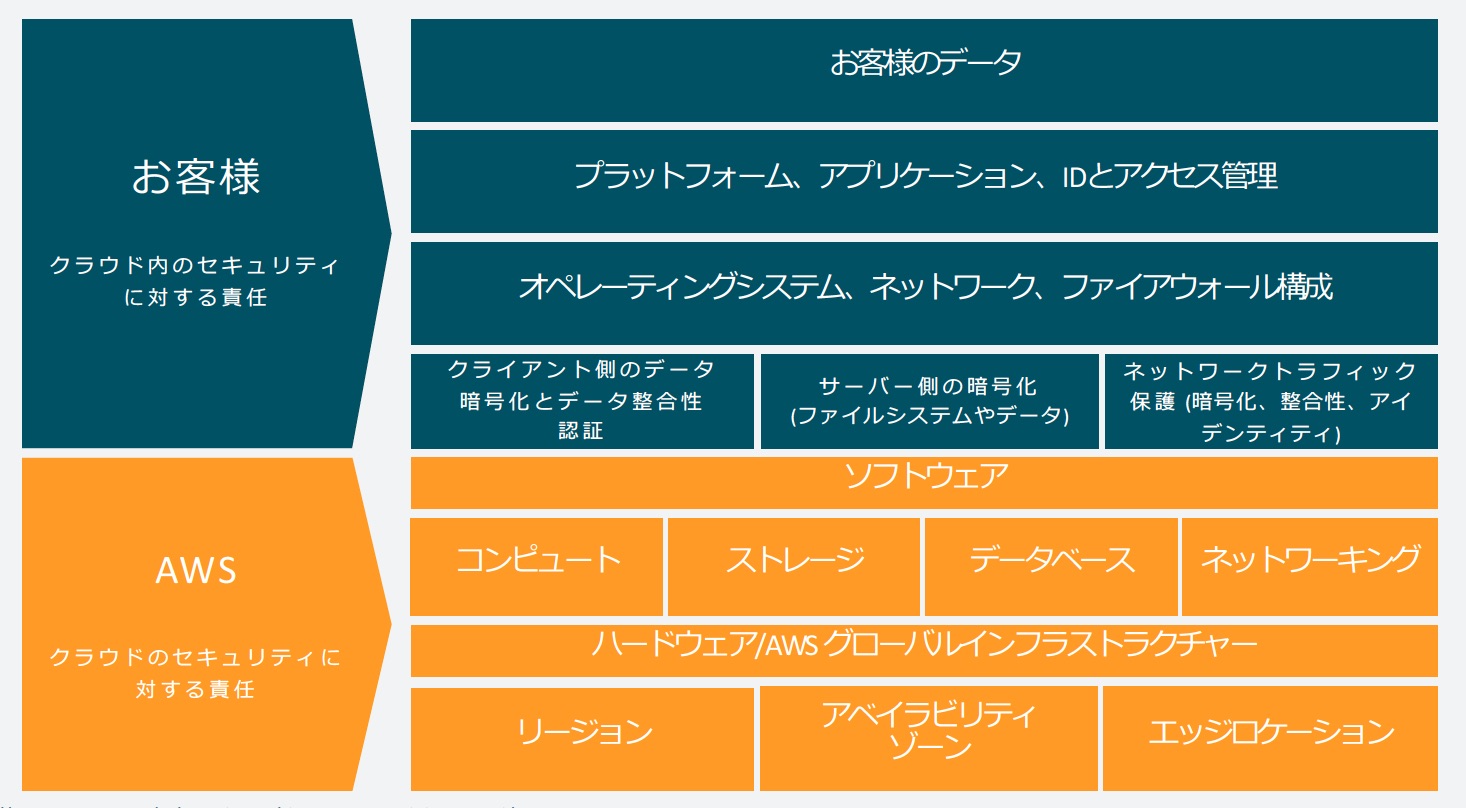


図 2‑3 AWSが提唱する責任共有モデル

（出展：https://aws.amazon.com/jp/compliance/shared-responsibility-model/）

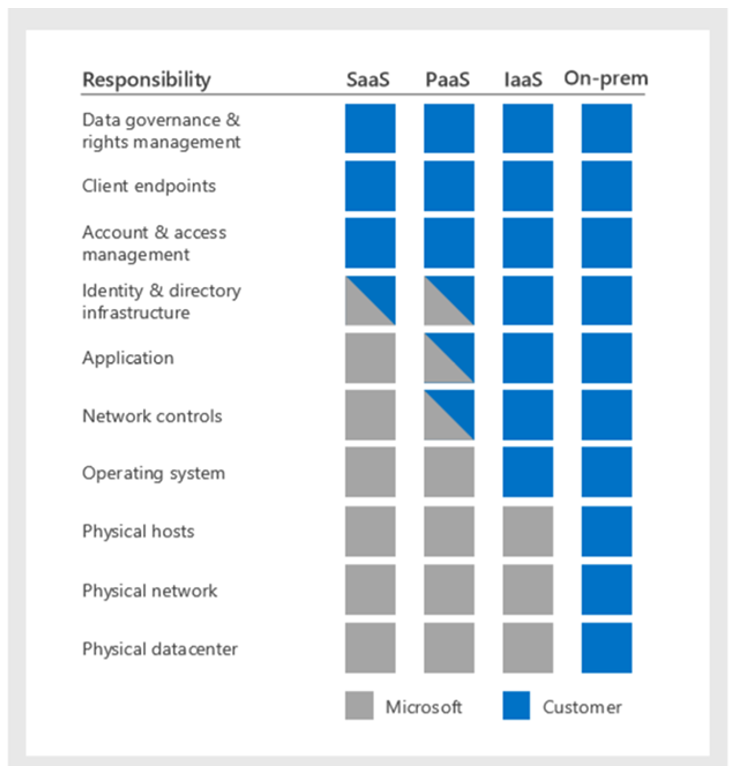


図 2‑4 Microsoftが提唱する責任共有モデル

（出展：https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview）

### A-gateを利用した場合の責任共有モデル

A-gateを利用した場合も、利用者が果たすべき責任範囲は変わらない。ただし、A-gateは利用者が責任を果たす上で有用なサポートを行う。サポートの内容を「図 2‑5 利用者の責任範囲に対する」に示す。

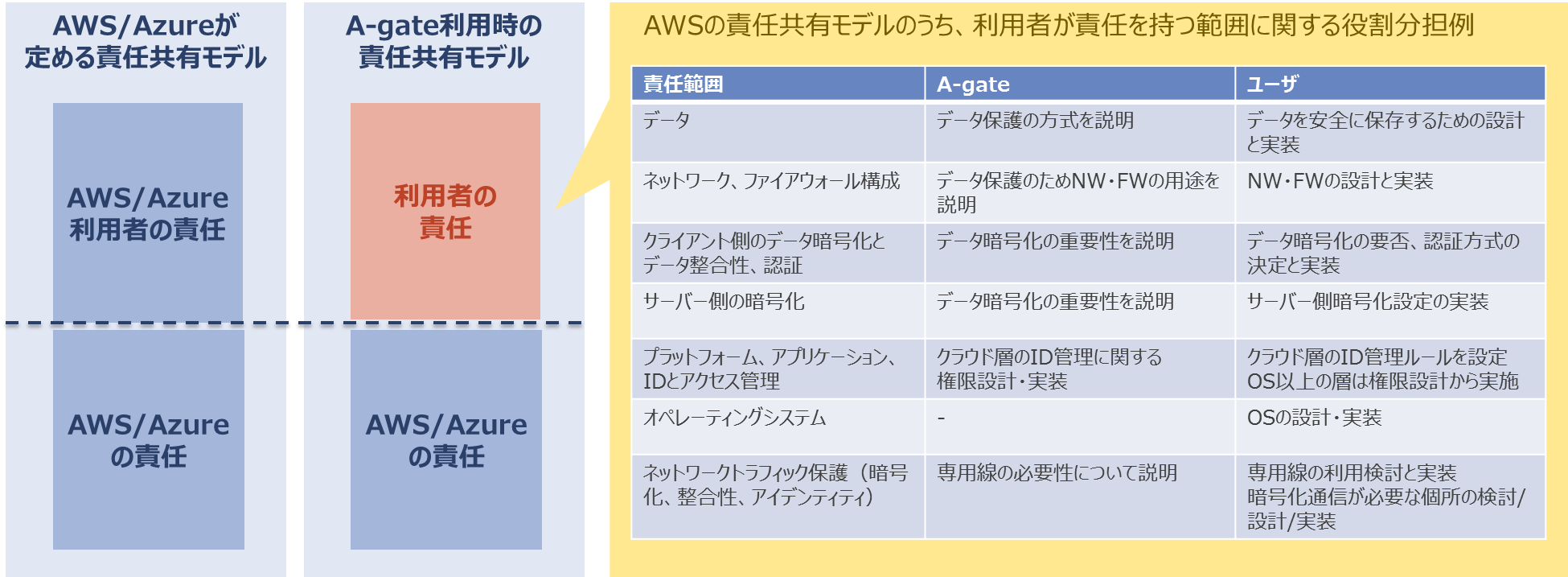


図 2‑5 利用者の責任範囲に対するA-gateのサポート内容

# A-gateが提供する共通基盤

A-gateでは、パブリッククラウドをセキュアに利用すること、およびパブリッククラウド利用時の利便性を高めることを目的とした共通基盤機能を提供する。

## 共通基盤機能一覧

A-gateが提供する基盤機能の一覧を「表 3‑1 A-gateが提供する共通基盤機能一覧」に示す。

表 3‑1 A-gateが提供する共通基盤機能一覧

|  |  |
| --- | --- |
| 機能名 | 機能概要 |
| 権限分掌 | A-gateが定義したパブリッククラウドを安全に利用するために必要な役割分担の考え方に準じ、各役割のパブリッククラウドに対する操作を適切に制限する機能 |
| ポリシー違反検知・自動修復 | 予め定めたセキュリティポリシーに違反する設定変更が行われた場合にそれを検知し、自動修復する機能 |
| 監査ログ収集 | 監査に必要なパブリッククラウドのログを収集し、保管する機能 |
| 環境初期設定 | 利用者が記入する申請書の内容に基づき、クラウド環境の設定を行う機能 |
| Hinemosオプション | クラウド上のテナントシステムの監視、およびテナントシステムにおけるジョブ管理の機能をサービスとして提供する機能 |

## 共通基盤機能詳細

### A-gateにおけるAWSアカウント構成

共通基盤機能を理解する上での前提知識となる、A-gate上のAWSアカウントの構成を「図 3‑1 A-gateにおけるAWSアカウント構成」、「表 3‑2 各アカウントの用途」に示す。

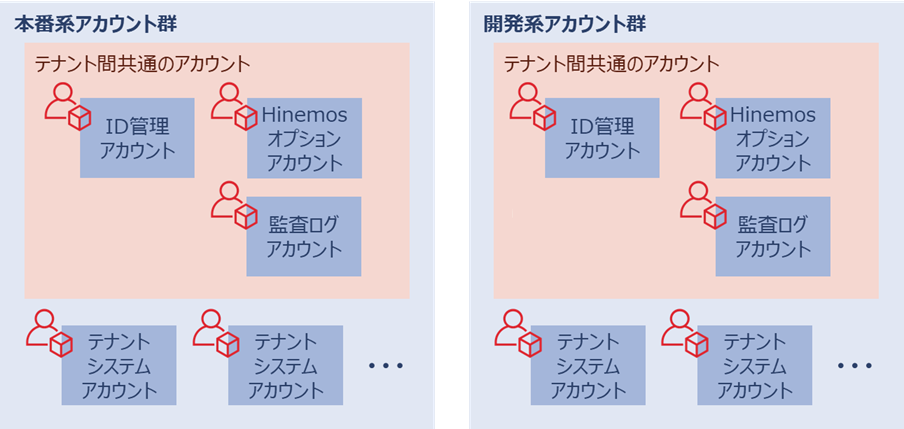


図 3‑1 A-gateにおけるAWSアカウント構成

表 3‑2 各アカウントの用途

|  |  |
| --- | --- |
| AWSアカウント | 説明 |
| ID管理アカウント | 権限分掌機能に関連する下記リソースを配備するアカウント   * 権限分掌機能で定義する役割に紐づくIAMグループ * 利用者に紐づくIAMユーザ |
| 監査ログアカウント | 監査ログ収集機能により各テナントシステムから収集した監査用ログの保管に利用するアカウント |
| Hinemosアカウント  （オプション） | Hinemosオプション機能に関連するリソースを配備するアカウント |
| テナントシステムアカウント | 個別のテナントシステムを構築するアカウント |

### 権限分掌

権限分掌は、組織がクラウドをセキュアに利用するにあたって必要となる「役割」と、各クラウドサービスのセキュリティ上のリスクの大きさを示す「リスク種別」を定めたうえで、「各役割が」「どのリスク種別のサービスに対して」「どの操作が行えるか」を定義し、クラウド上に実装した機能である。

#### 定義しているリスク種別

A-gateが定義するリスク種別を「表 3‑3 A-gateが定義するリスク種別」に示す。リスク種別は各リスクをコントロールすべき主体（管理レイヤ）に応じて分類している。

表 3‑3 A-gateが定義するリスク種別

|  |  |  |
| --- | --- | --- |
| 管理レイヤ | セキュリティリスクの説明 | リスクを管理できる・管理すべき担当 |
| SIer | * 権限制御を行うサービスに対する変更権限を必要とするサービス（権限分掌のルールを変更できる権限） | * NTTデータ |
| NW部門 | * インターネットや他アカウントと包括的に通信するためのサービス | * 社内のNW担当 |
| 開発責任者 | * 他アカウントとのデータ共有が可能なサービス * 自アカウントに閉じるNW設定（ルーティング、FW） * コーディング等によりインターネットへの情報公開が可能なサービス | * 社内横断の基盤担当の責任者 * 開発PJの責任者 |
| 開発担当者 | * 設置先がVPC内に限られるサービス * その他の事由により情報漏洩の危険性が無いサービス | * 社内横断の基盤担当の担当者 * 運用担当の担当者 * 開発PJの担当者 |

#### 定義している役割

A-gateが定義する役割を「表 3‑4 A-gateが定義する役割」に示す。各役割には役割の遂行のために最低限必要となるIAMの権限が割り当てられている。

表 3‑4 A-gateが定義する役割

|  |  |  |  |
| --- | --- | --- | --- |
| 単位 | 役割 | 説明 | 担当組織例 |
| A-gate | 特権 | 一部を除いたあらゆる権限を保有し、“管理レイヤ：SIer”のサービスの設置や操作を行う | NTTデータ |
| 利用者 | サービス/NW  管理 | クラウド上でのNW設定やインターネットとの接続・公開などの設定が可能な“管理レイヤ：NW部門”のサービス操作を担う | CCoE  自社横断のNW担当 |
| 利用者 | 全テナント管理 | 全アカウントについて、高額な購買（リザーブドインスタンス）またはリスク有り購買（マーケットプレイス）の利用と他アカウントとのデータ共有などの設定が可能な“管理レイヤ：開発責任者”のサービス操作を担う | 社内横断の基盤担当  (責任者) |
| 利用者 | テナント管理 | ※　単一アカウントに対してのみ、「全テナント管理」と同等の権限を保有する | 開発PJ  (責任者) |
| 利用者 | 全テナント担当 | 全アカウントについて、情報漏洩リスクのない設定が可能な  “管理レイヤ：開発担当者”のサービス操作を担う | 社内横断の基盤担当  (担当者)  運用部門 |
| 利用者 | テナント担当 | ※　単一アカウントに対してのみ、「全テナント担当」と同等の権限を保有する | 開発PJ  (担当者) |
| 利用者 | ID管理 | ユーザの作成・削除、ユーザのグループへの参加・除外を行う | 社内横断のユーザ管理部門 |
| 利用者 | 監査 | システム監査のため、あらゆるサービスの利用状況やログ情報の参照を行う | 社内横断のかくｋ部門 |
| 利用者 | 全インスタンス起動停止 | 全アカウントに対してサーバなどのインスタンスの起動、停止のみを行う | 社内横断の運用部門 |
| 利用者 | インスタンス起動停止 | 単一アカウントに対してのみ、「全インスタンス起動停止」と同等の権限を保有する | 運用部門 |
| 利用者 | 全クラウド自動構築 | 全アカウントに対してクラウドリソースの自動構築を行う | 社内横断の基盤担当  (責任者) |
| 利用者 | クラウド自動構築 | 単一アカウントに対してのみ、「全クラウド自動構築」と同等の権限を保有する | 開発PJ  (責任者) |

#### 現在解放されているサービス

現在利用者に解放されているサービス、および、各役割が各サービスに対して実施できる操作については、「AWS\_ガイド\_】利用可能サービス・実施可能操作一覧」参照。

### ポリシー違反検知・自動修復

#### ポリシー違反検知・自動修復の仕組み

ポリシー違反検知・自動修復機能では、「ポリシー違反と見なし修復の対象とすべき状態（ルール）」を複数規定している。CloudWatchを用いて利用者が行ったクラウド操作がポリシー違反であるかをチェックし、修復の必要があると判断した場合はLambda Functionによりセキュリティリスクのない状態に修復する。

#### 例外登録

* 例外登録の必要性

ポリシー違反のルールに該当する設定であっても、テナントシステムとして必要な設定である、といったケースがありうる。

その場合、「例外登録」を行うことで、当該設定を例外的にポリシー違反検知・自動修復の対象外とすることができる。

* 例外登録の運用にあたる注意事項

例外登録を行った場合、当該設定に対してポリシー違反検知・自動修復が機能しなくなるため、当該アカウントはセキュリティリスクにさらされた状態となる。そのため、例外登録の運用は予め「表 3‑5 例外登録にあたり制定すべきルール」に示したルールを制定した上で開始すること。

表 3‑5 例外登録にあたり制定すべきルール

|  |  |
| --- | --- |
| 項番 | 制定すべきルール |
| 1 | 例外登録を実施できる組織を限定し、当該組織への申請制とすること |
| 2 | 例外登録が行われるまでのプロセスを制定し、然るべき設計・承認のプロセスを経たうえで例外登録が行われるようにすること |

#### 現在のポリシー違反項目と自動修復の内容

ポリシー違反と見なされる操作、および、当該操作を実施した場合に自動で行われる修復作業の内容については、「AWS\_ガイド\_ポリシー違反検知・自動修復ルール一覧」参照。

### 監査ログ収集

#### 収集対象のログ

本機能で収集するログ、およびログの収集先を「表 3‑6 収集対象のログと収集先」に示す。

表 3‑6 収集対象のログと収集先

|  |  |  |  |
| --- | --- | --- | --- |
| 収集対象 | 内容 | 収集先 | |
| テナントアカウントのS3バケット | 監査ログアカウントのS3バケット |
| CloudTrail | アカウント内のAWSリソースに対して実行された操作に関するログ | 〇 | 〇 |
| VPC  フローログ | VPC内のネットワークインターフェイスとの間で行き来するIPトラフィックのログ  A-gateで作成したVPCに限ります。  利用者様でVPCを作成された場合には、利用者様自身で設定の要否を判断していただき、必要な場合はセルフサービスで設定をお願いいたします。 | 〇 | 〇 |
| AWS  Config | AWS Configのデフォルト設定で取得される、リソースの操作ログ | × | 〇 |

### 環境初期設定

「A-gate利用者向け運用マニュアル」に記載の各種運用において、各種リソースの作成および他の共通基盤機能のセットアップを行う機能。（A-gateの利用者が直接本機能を操作することは無い。）

### Hinemosオプション

#### Hinemosオプション機能の概要・ユースケース

Hinemosオプション機能は運用管理ソフトウェア「Hinemos」の機能を月額課金形式で利用できるサービスである。

Hinemosを利用する場合の構成要素である「Hinemosマネージャ」、「Hinemosクライアント」、「Hinemosエージェント」のうち、「Hinemosマネージャ」をA-gateが提供する。（「図 3‑2 Hinemos利用時の構成要素」、「図 3‑3 Hinemosオプション機能の利用イメージ」参照）

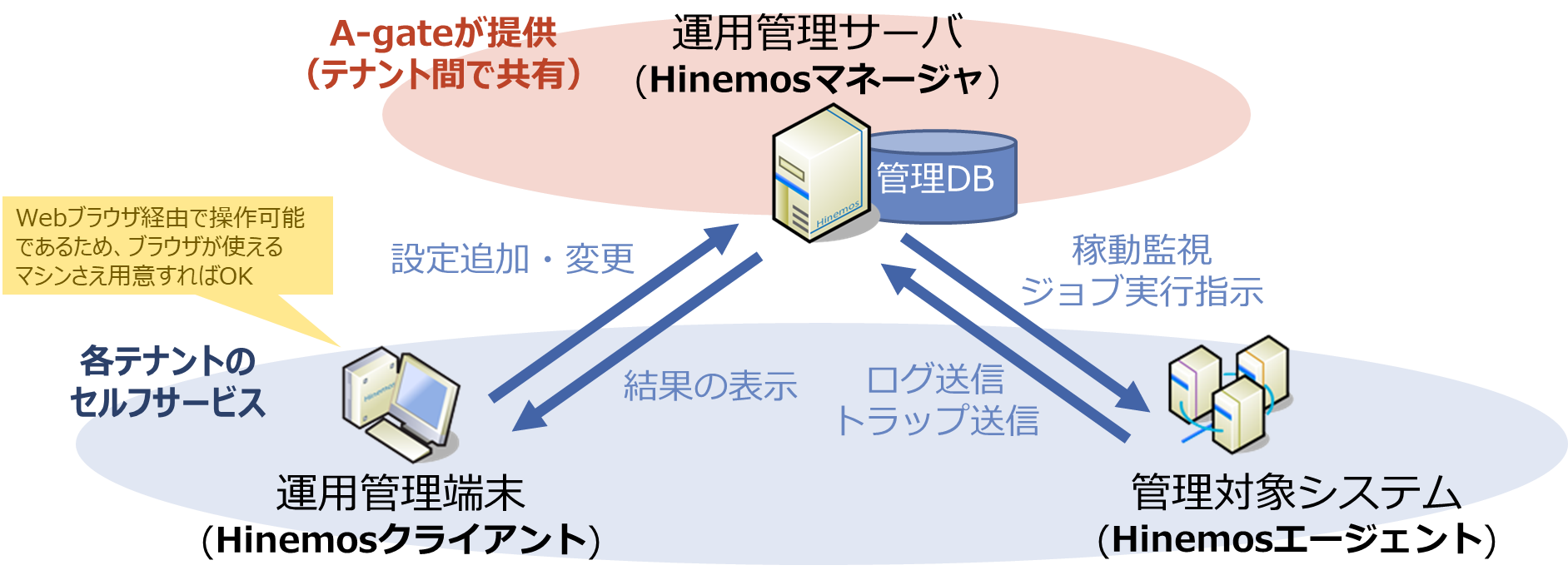


図 3‑2 Hinemos利用時の構成要素

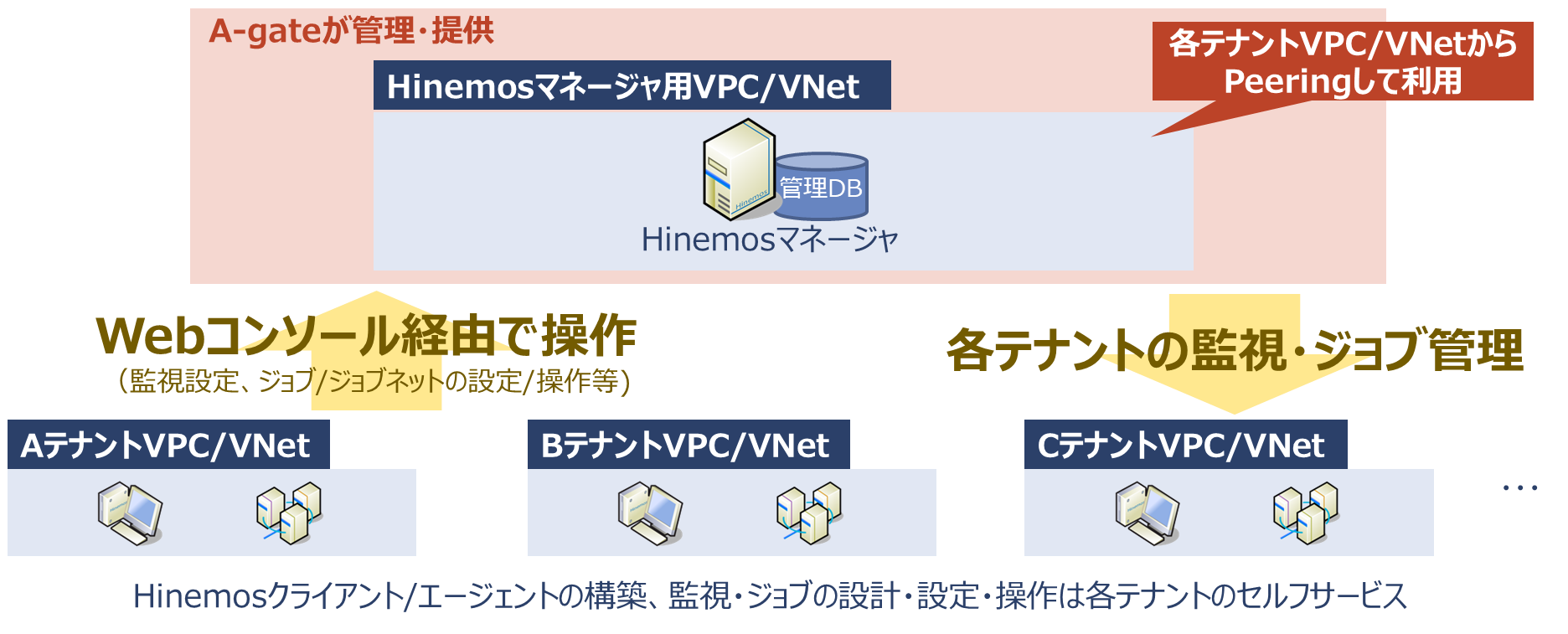


図 3‑3 Hinemosオプション機能の利用イメージ　その１

また、Hinemosオプションの利用にあたり、Hinemosマネージャの設定やメンテナンスを、利用者にてセルフサービスで実施可能とする。セルフサービスの利用イメージを「図 3‑4 Hinemosオプション機能の利用イメージ　その2」に示す。

①Hinemosマネージャのメンテナンスプロパティ設定や権限設定

・履歴情報削除期間変更

・マスタ情報の更新

・各種Hinemosメンテナンスプロパティ設定の変更

・ロールの作成

②HinemosマネージャのOS設定・操作

・Hinemosマネージャ上にスクリプトの配置（利用者独自要件による監視の設定）

・クラウドサービス監視

-監視対象サービス追加・変更（設定ファイルの編集及び再起動）

-クラウドサービスの監視メトリクス追加（SQLの実行）

・Hinemosマネージャの復旧（HA再構成）

・Hinemosマネージャ・エージェントのパッチ適用（パッチ配置・SQL実行・Hinemosマネージャ再起動）

※エージェントはHinemosマネージャにパッチを配置し、エージェントの適用作業は、HinemosWEBコンソールより実施

③Hinemosマネージャの障害時の対応をセルフサービス化

・Hinemosマネージャの状態通知（メール通知）

・Hinemosマネージャの復旧（HA再構成）

④Hinemos用のAWSアカウント上の操作

・Hinemosマネージャ搭載のEC2インスタンスの起動/停止

・Hinemosマネージャからの送信元メールアドレス変更のためのSES設定

※Hinemos用のAWSアカウント上の設定のうち、以下についてはA-gate問い合わせ窓口まで依頼をお願いいたします。

・管理対象VPCの追加

-ピアリング設定(VPC、TGW)

-ルーティング(ルートテーブル)設定

-SG設定

・監視プロトコル追加

-SG設定

・Hinemosマネージャ搭載EC2のスケールアップ、ダウン

※スケールアウトする場合には、A-gate問い合わせ窓口まで、お問い合わせください。

・バックアップ周期の変更

現状：週次(月曜日3:30頃)、3世代

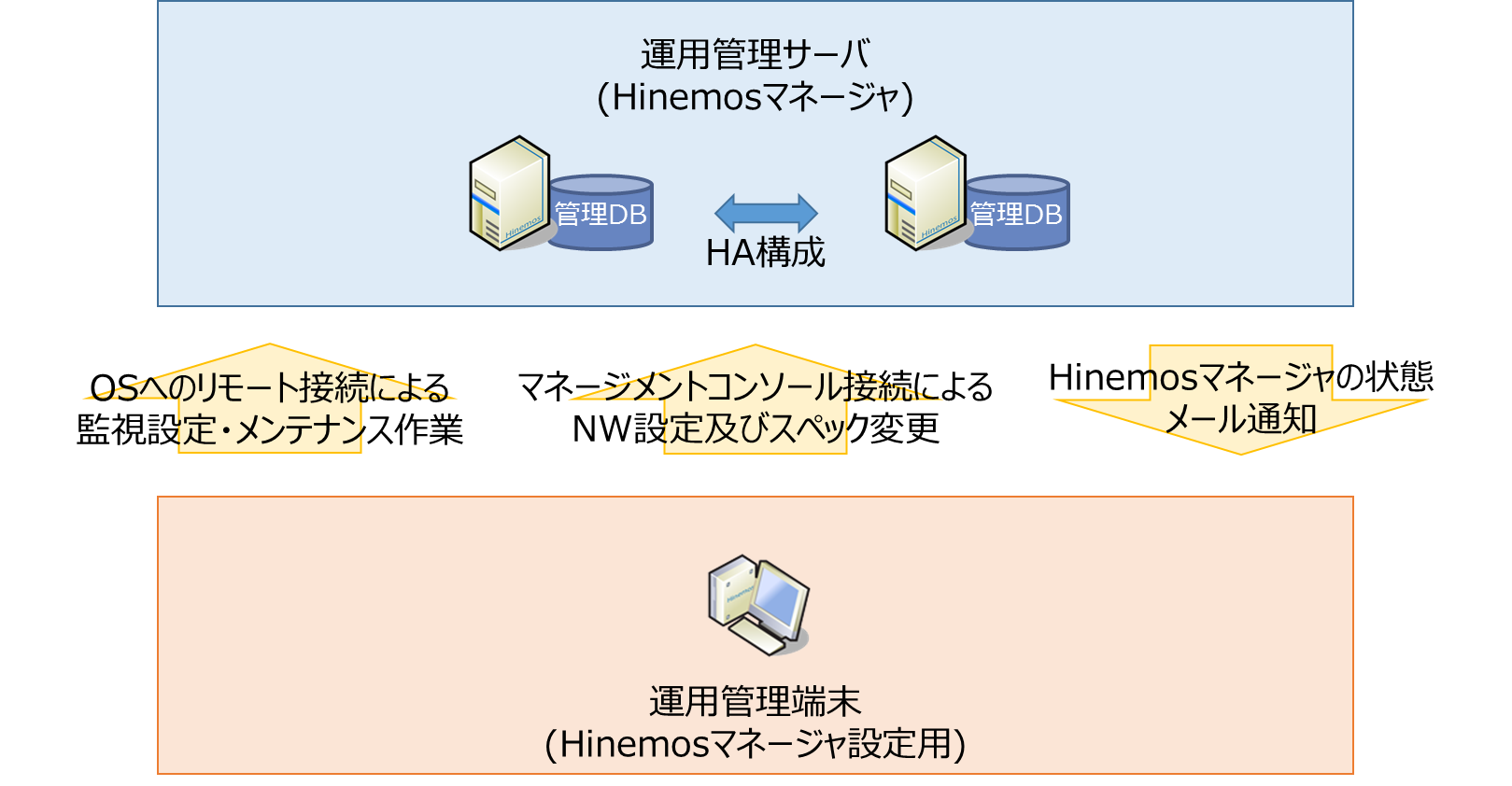


図 3‑4 Hinemosオプション機能の利用イメージ　その2

* + - 1. **Hinemosに関するお問い合わせ**

Hinemosオプションのご利用にあたり、以下のお問合せや情報取得は、Hinemosカスタマーポータル(以降、HinemosCP)より可能です。HinemosCPのご利用手続きは、Hinemosオプションのご利用開始準備において、申込書をご提示ください。

・Hinemosのマニュアル

・Hinemosの仕様に関する問合せ

・Hinemosに関する不具合の問合せ

・Hinesmoの累積パッチの入手

# パブリッククラウド活用ガイドライン

本章では主に、「2.2 A-gateにおける責任共有モデル」の責任共有モデルの中で示した利用者が担保すべき責任事項について、責任を遂行するための方策に関して具体的な指針を示す。

## 導入編

本節では、主にパブリッククラウドおよびA-gateの利用を開始する際に策定すべきルールについて述べる。

### プラットフォーム選定指針

パブリッククラウドを利用することで享受できるメリットは多岐にわたる。しかし、個別システムの特性や、自社で既に利用しているファシリティ（オンプレミス環境、プライベートクラウド、コミュニティクラウド）の有効活用の観点から、どのようなシステムでもパブリッククラウドの利用が最適な選択肢であるとは限らない。

自社で保有する情報資産の全体最適を図るためには、個別システムのプラットフォームの選定基準について指針を設けることが肝要であり、下記「図 4‑1 A-gateが推奨するプラットフォーム選定指針」に示すA-gateが推奨するプラットフォーム選定の指針を参考に、自社の指針を設けることが望ましい。

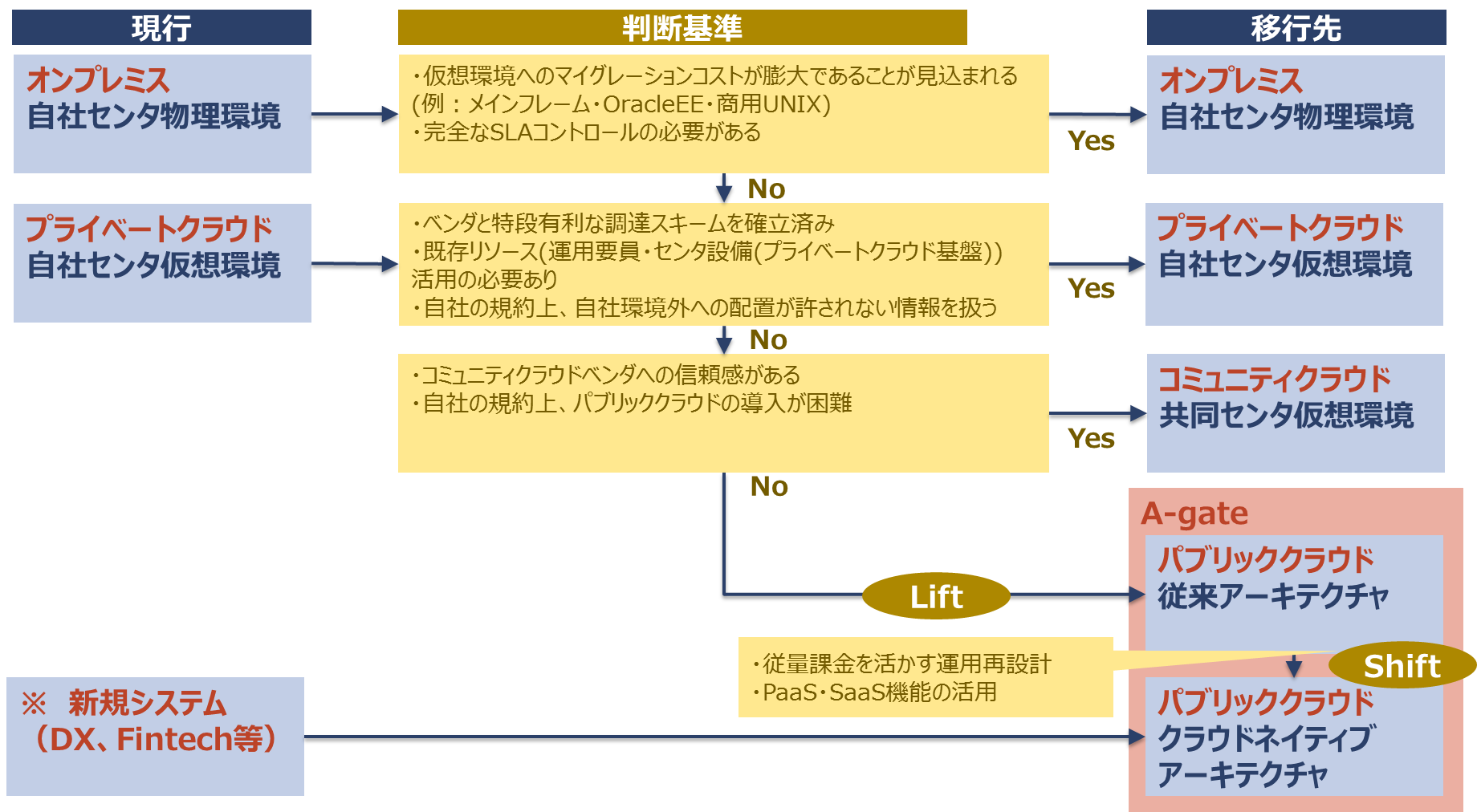


図 4‑1 A-gateが推奨するプラットフォーム選定指針

### アカウント分割指針

#### アカウントとは

AWSにおけるアカウントは、主にAWS利用料の請求単位であり、かつAWS上のリソース（例：仮想マシン、仮想ネットワーク）の管理単位である。

A-gateとして推奨するアカウントの分割単位

分割の方針は「図 4‑2 様々なアカウント分割の方法とA-gateが推奨する方法」に示すように複数の案が考えられるが、A-gateでは「1システム・1環境：1アカウント」とすることを推奨する。

推奨の理由を「表 4‑1 「1システム・1環境：1アカウント」の推奨理由」に示す。



図 4‑2 様々なアカウント分割の方法とA-gateが推奨する方法

|  |  |
| --- | --- |
| 観点 | 説明 |
| 会計の明朗化 | 1アカウントに複数システムを混在させない分割方法とすることで、単一の請求が所管部署を跨ぐことが無く、支払いの手続が簡易になる。また、利用料がシステム毎に算出されることで、コスト最適化のための分析が実施しやすくなる。 |
| 権限分離によるオペレーションミスの防止 | 各システムの環境単位に別アカウントとすることで権限が分離されるため、オペレーションミス（例：環境変更権限を持ったユーザが、開発環境サーバと間違えて本番環境サーバの環境を変更してしまった、等）を防止できる。 |
| 変更作業の影響極小化 | 新規システムの追加や既存システムの環境変更を実施する際に、稼働中の他システムや他環境に及ぼす影響を極小化することができる。 |
| 拡張性 | AWSの仕様として定められている各種リソースの上限値について、アカウント単位に設けられているものが多く存在する。（（※）参照。）  そのため、割当て単位を極力細分化することで拡張性を担保することができる。（A-gateが推奨する、運用上の利便性を損なわずに最大限細分化する場合のベストプラクティスが1システム・1環境あたり1アカウントである。）  （※）<https://docs.aws.amazon.com/ja\_jp/general/latest/gr/aws\_service\_limits.html> |

表 4‑1 「1システム・1環境：1アカウント」の推奨理由

### 環境分離指針

テナントシステムをパブリッククラウド上に構築するにあたり、用途に応じて複数の環境（例：本番環境、開発環境、等）を用意し、それぞれに適したリソース、セキュリティレベル等を定めて運用することが望ましい。

本項では、パブリッククラウドにおける環境分離の指針について述べる。

#### A-gateが推奨する環境分離の方法

A-gateが推奨する環境分離の指針を「表 4‑2 A-gateが推奨する環境分離指針」に示す。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 環境種別 | 定義 | オンプレ  接続先 | 利用データ | 想定利用者 | 接続元 |
| 本番環境  (システム部所管) | システム部所管で商用システムを稼働させる環境 | 本番環境 | 本番データ | システム関連会社  システムベンダ | システム関連会社の本番ルーム  システムベンダの本番ルーム |
| 本番環境  (ユーザ部所管) | ユーザ部所管で商用システムを稼働させる環境 | 本番環境 | 本番データ | 社内各部門 | ※既存のEUCと平仄を合わせる |
| ステージング環境 | 開発、機能改修時の結合試験工程以降を実施する環境 | 開発環境 | マスク済  データ | システム関連会社  システムベンダ | システム関連会社の開発ルーム  システムベンダの開発ルーム |
| M/UT環境 | 開発時の製造、単体試験工程を実施する環境 | なし | なし | システム関連会社  システムベンダ | システム関連会社のPoCエリア  システムベンダのPoCエリア |
| PoC環境 | 新規事業・サービスの検証を行うための環境 | なし | なし | 社内各部門  システム関連会社 | 自社本部のPoCエリア  システム関連会社のPocエリア |

表 4‑2 A-gateが推奨する環境分離指針

### 多要素認証ルール

#### 多要素認証の必要性

パブリッククラウドのユーザ（AWSのIAMユーザ、およびAzureのAzureADユーザ）は、各種のクラウドに対する操作が「誰が実施したか」がログから特定できるよう、**1人に対し１ユーザを割り当てることが望ましい**。

ただしそのようにした場合、ユーザID・パスワードの管理を個人に委任することとなるため、オンプレミス環境の運用で多くみられる中央管理の方式（例：必要なタイミングで管理者に申請しユーザID・パスワードの貸出を受ける）と比較すると、ユーザID・パスワードの漏洩のリスクは高くなる。

上記リスクへの対策として、クラウドユーザはユーザID・パスワードの認証に加え、複数の要素による認証（多要素認証）を導入することが望ましい。

#### 多要素認証に用いる代表的な認証要素

多要素認証に用いる代表的な認証要素を「図 4‑3 多要素認証に用いる代表的な認証要素」に示す。これらの認証要素を複数併用し、クラウドへのアクセスをセキュアに保つ必要がある。

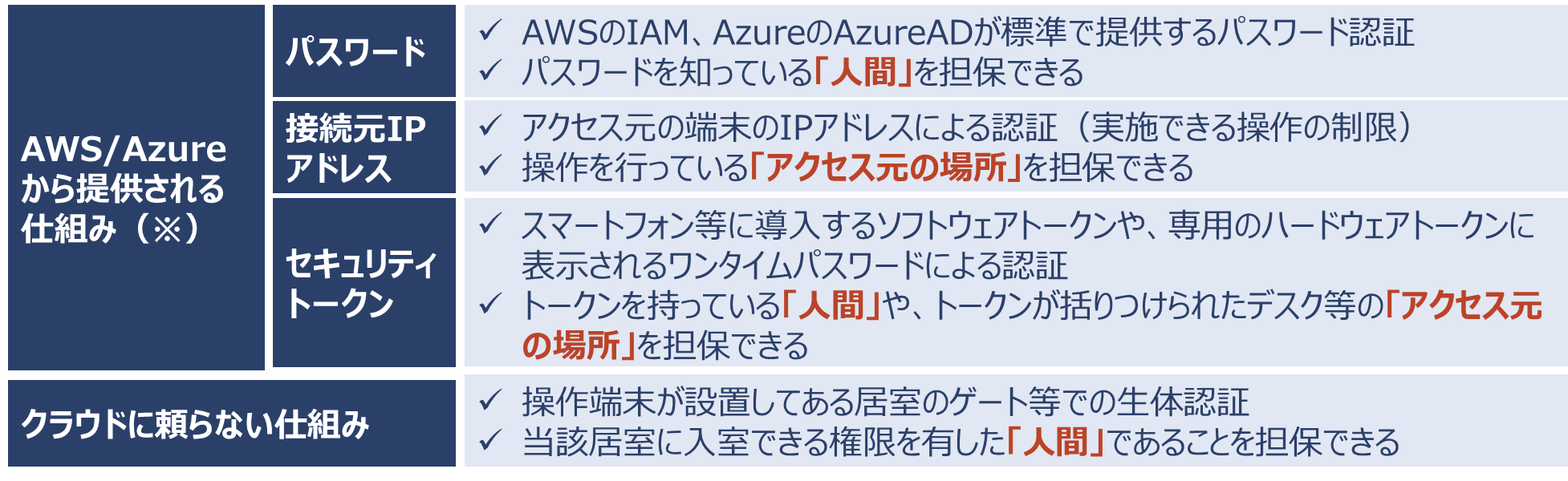


図 4‑3 多要素認証に用いる代表的な認証要素

### マネジメントコンソール接続ルール

パブリッククラウドにおけるマネジメントコンソールは、クラウド上のサービスやリソースをGUI（ブラウザ）で操作できるサービスである。

利便性が高くパブリッククラウドの利用にあたっては必要不可欠なサービスであるが、その反面大きなセキュリティリスクをはらむサービスでもあり、安全対策が不可欠である。

#### マネジメントコンソールのセキュリティリスクと対策の全体像

マネジメントコンソールをセキュアに使うには対策を施すべき課題がある。課題とそれに対する対応策の概要を「表 4‑3 マネジメントコンソールのセキュリティリスクと対策（概要）」に示す。

|  |  |  |  |
| --- | --- | --- | --- |
| 項番 | 概要 | リスクの説明 | 推奨する対策 |
| 1 | 不正な拠点からの アクセス | Internet接続可能な環境であればどこからでも利用することができ、アクセス元を制限しないと不正な拠点（例：担当者の自宅PC等）からアクセスすることが可能である | クラウドの機能により、当該アカウントのマネジメントコンソールの接続元IPアドレスを制限する |
| 2 | 不特定のNWを経由する通信経路 | Internet経由でアクセスする場合、不特定のNWを経由することになり、盗聴等のリスクがある | クラウド上の踏み台サーバからアクセスすることで、クラウドベンダのデータセンタ内に閉じた通信とする |
| 3 | 野良アカウントへの アクセス | ID/パスワードを変えればどのアカウントの環境にもログイン可能であり、自社で正式に利用しているものではない「野良アカウント」を用いた情報の不正持出が可能である | マネジメントコンソール利用時の運用ルールを厳格化し、個人の不正を牽制する |

表 4‑3 マネジメントコンソールのセキュリティリスクと対策（概要）

リスクと対策の詳細（不正な拠点からのアクセス）

* セキュリティリスク

マネジメントコンソールはInternetを介して利用するサービスであり、Internetが利用できる環境であれば場所を問わずアクセスすることができてしまう。（「図 4‑4 不正な拠点からのアクセスによるリスク」参照）

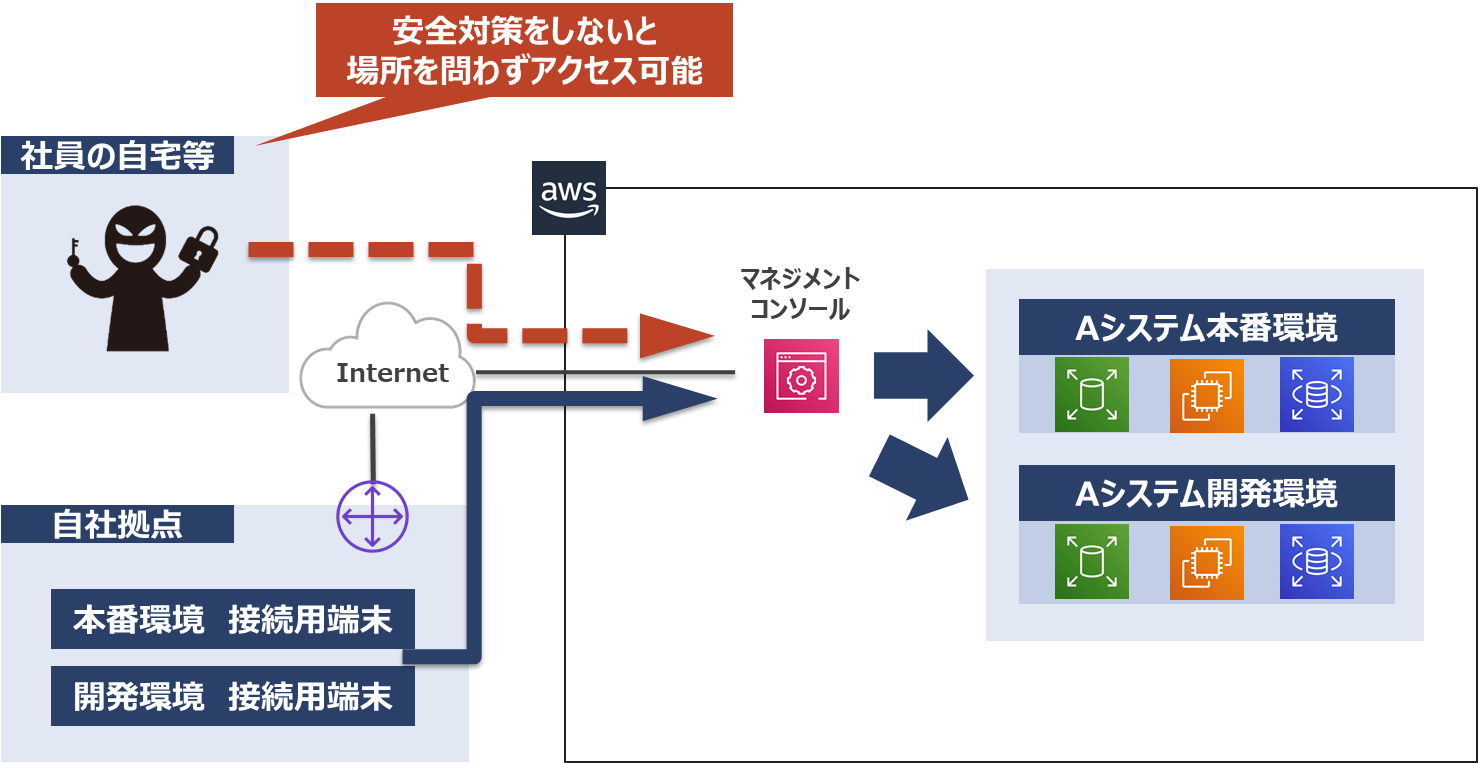


図 4‑4 不正な拠点からのアクセスによるリスク

* 推奨する対策

クラウドの機能より、マネジメントコンソールのアクセス元のIPアドレスを制限することが可能である。本番環境接続用の端末/居室、開発環境接続用の端末/居室それぞれに固有のグローバルIPアドレスを用意し、当該アドレスからのアクセスのみを許可するよう設定する。（「図 4‑5 不正な拠点からのアクセスによるリスクへの対策」参照）

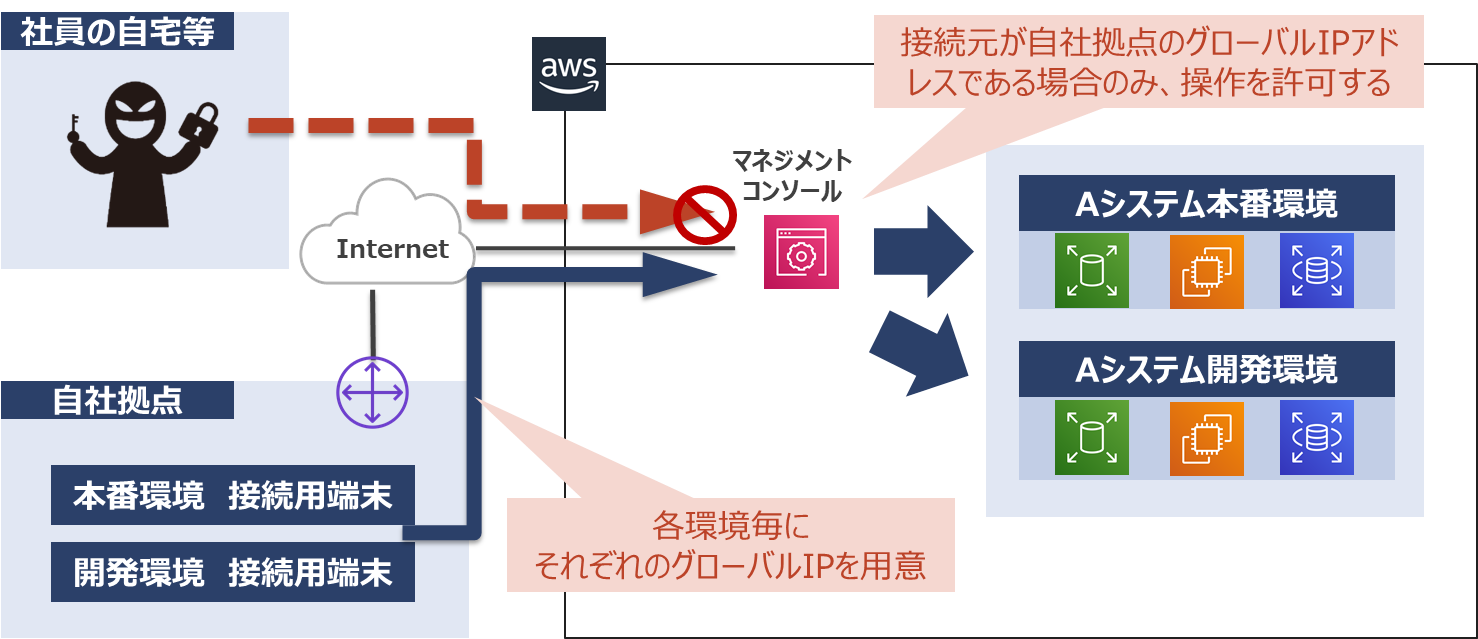


図 4‑5 不正な拠点からのアクセスによるリスクへの対策

リスクと対策の詳細（不特定のNWを経由する通信経路）

* セキュリティリスク

Internet経由でマネジメントコンソールにアクセスする場合、不特定のNWを経由することとなり、通信の盗聴等のリスクがある。HTTPSにより暗号化されているため情報漏洩につながるリスクは低いが、「不特定のNWを経由する」という事実を社内ルールとして許容していない場合は対策が必要となる。（「図 4‑6 不特定のNWを経由する通信経路に伴うリスク」参照）

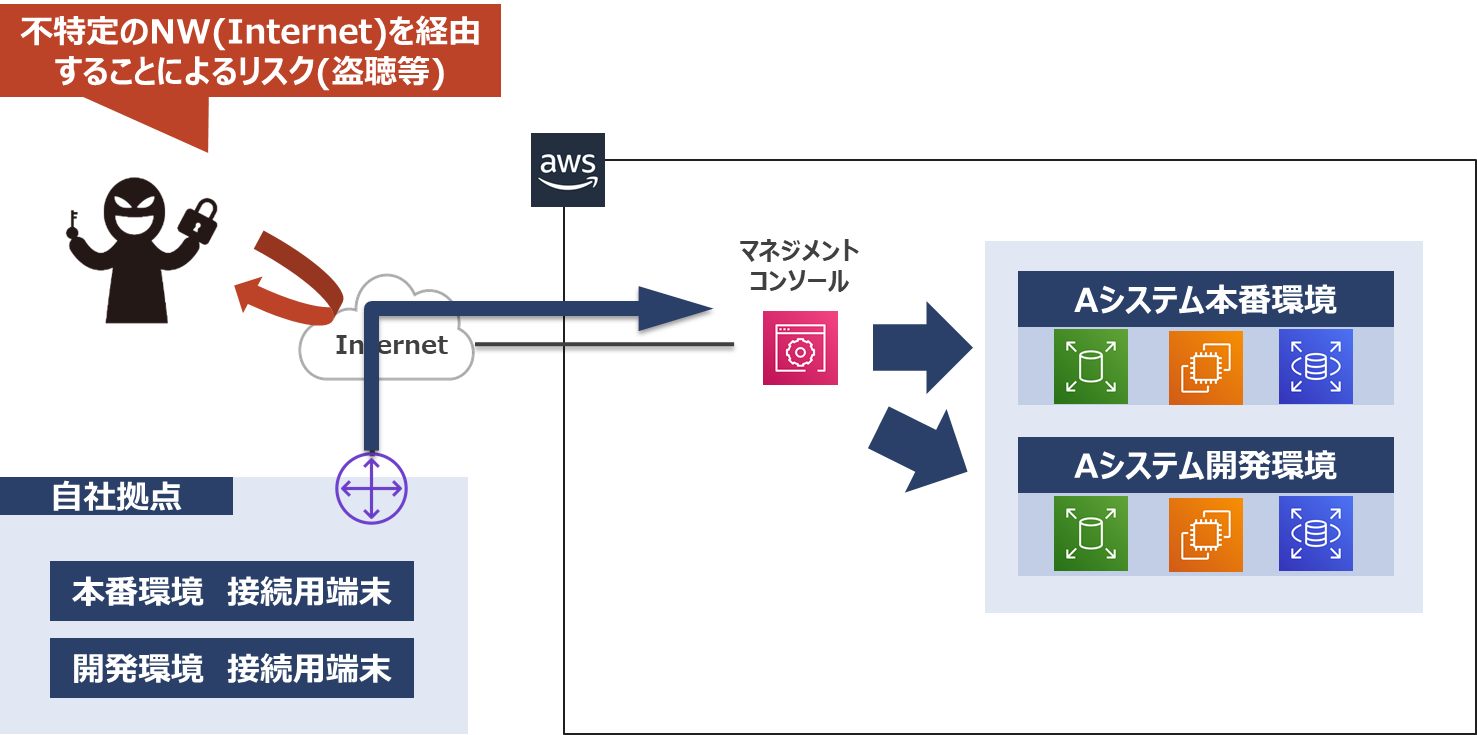


図 4‑6 不特定のNWを経由する通信経路に伴うリスク

* 推奨する対策

オンプレミスの拠点ではなく、クラウド上の環境（クラウド上に構築した踏み台サーバ）からアクセスすることで、クラウドベンダのデータセンタ内に閉じた通信経路でアクセスすることが可能となる。

また、アクセス元を踏み台環境上のProxyサーバのグローバルIPアドレスのみに制限することで、「(2)リスクと対策の詳細（不正な拠点からのアクセス）」と併せて対策することが可能である。（「図 4‑7 不特定のNWを経由する通信経路に伴うリスクへの対策」参照）

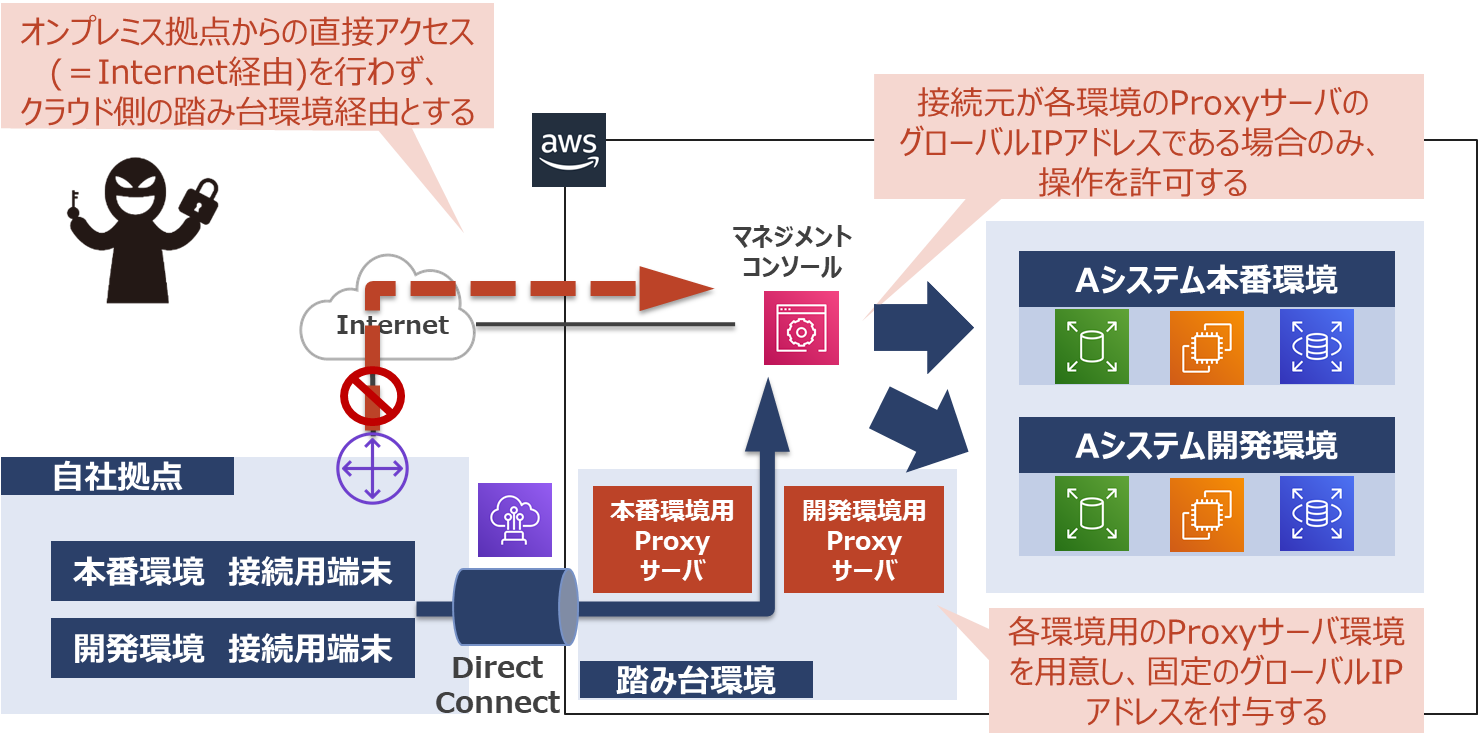


図 4‑7 不特定のNWを経由する通信経路に伴うリスクへの対策

リスクと対策の詳細（野良アカウントへのアクセス）

* セキュリティリスク

マネジメントコンソールはID/パスワードを変えればどのアカウントの環境にもログイン可能である。そのため、本番環境の作業拠点から、自社で正式に利用しているものではない所謂「野良アカウント」にアクセスし、情報を不正に持出すことが可能である。（「図 4‑8 野良アカウントの利用による情報漏洩リスク」参照）

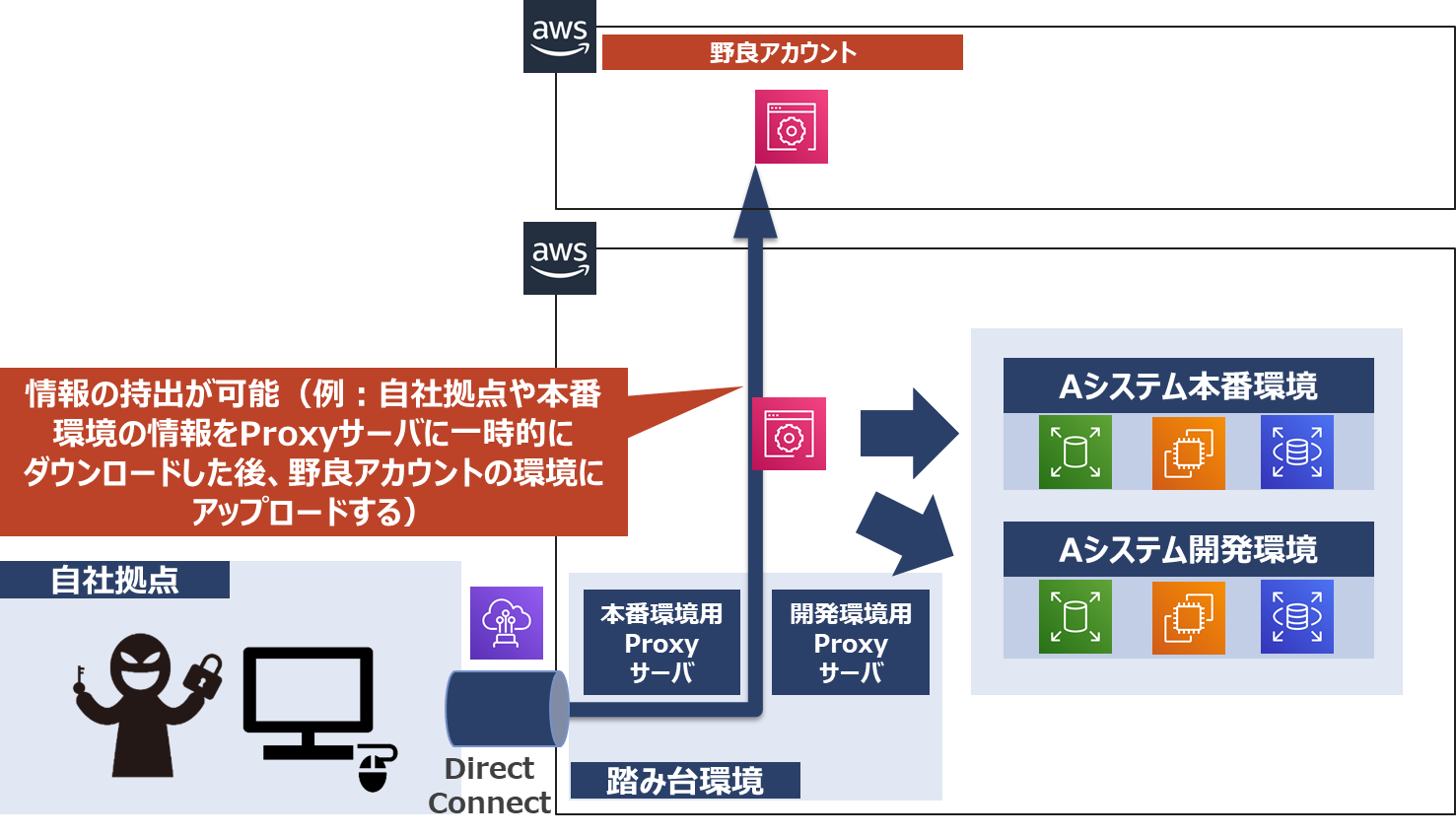


図 4‑8 野良アカウントの利用による情報漏洩リスク

* 推奨する対策

マネジメントコンソールを利用する際の運用ルールを厳格化することで、不正を牽制する。牽制のための運用ルールとして、マネジメントコンソールを操作する作業は必ず二名体制での実施の義務付ける、マネジメントコンソールの操作元端末を画面録画する等の対策が有用である。（「図 4‑9 野良アカウントの利用による情報漏洩リスクへの対策」参照）

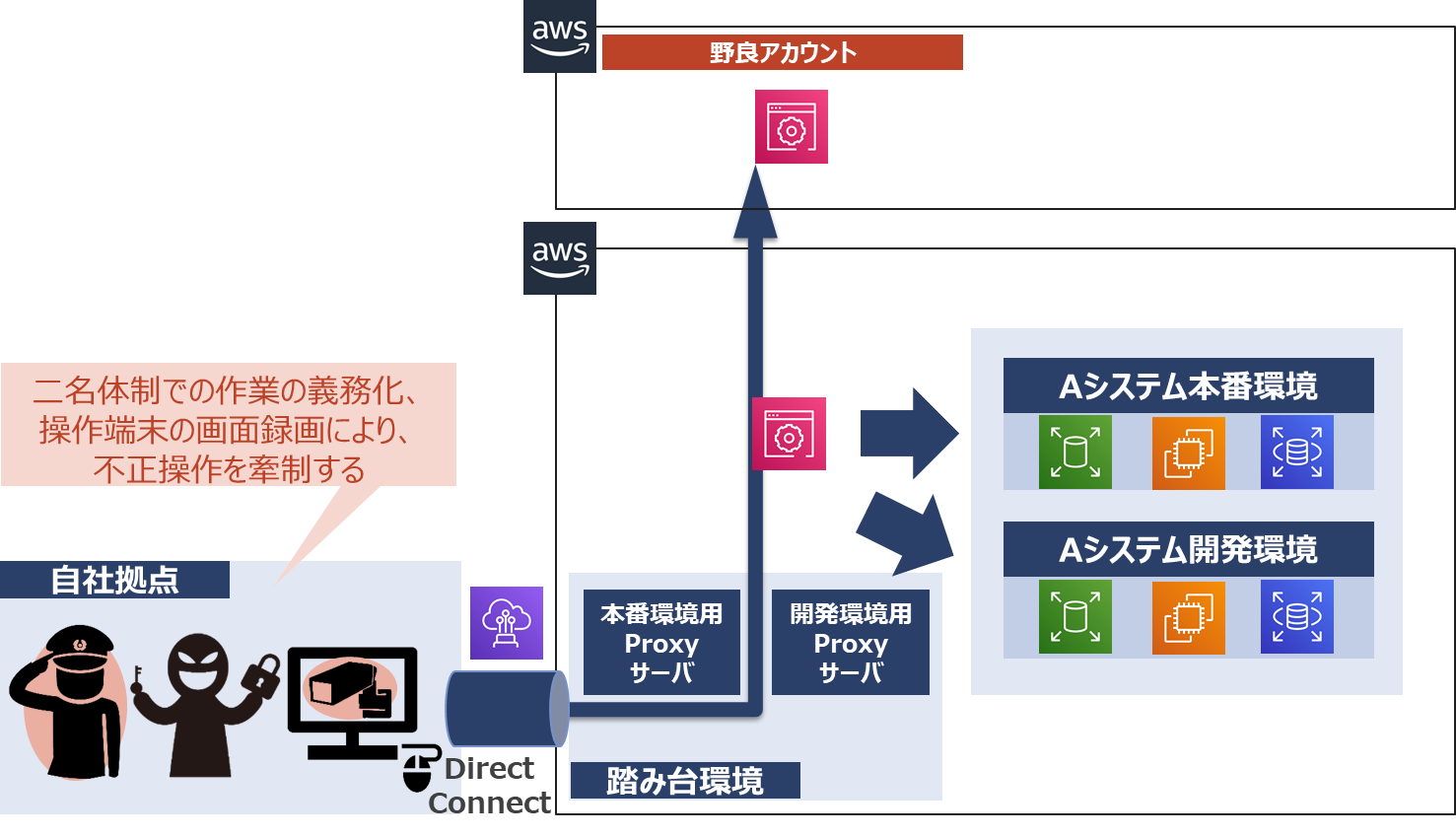


図 4‑9 野良アカウントの利用による情報漏洩リスクへの対策

### 外部ベンダ向け環境接続ルール

自社要員のパブリッククラウド利用にあたっては、自社拠点からの専用線による接続経路の確立や、自社拠点における多要素認証の義務化等により、セキュリティの担保が可能である。

しかし、システムの開発・保守を外部ベンダに委託する場合、外部ベンダ要員が自社のパブリッククラウド環境をセキュアに利用するためのルールを別途定め、施行する必要がある。

#### 外部ベンダから自社パブリッククラウド環境への接続形式

外部ベンダの要員が自社のパブリッククラウド環境に接続する方法は、自社拠点利用型とベンダ拠点利用型の2パターンが考えられる。それぞれの詳細を「図 4‑10 自社拠点利用型とベンダ拠点利用型」に示す。

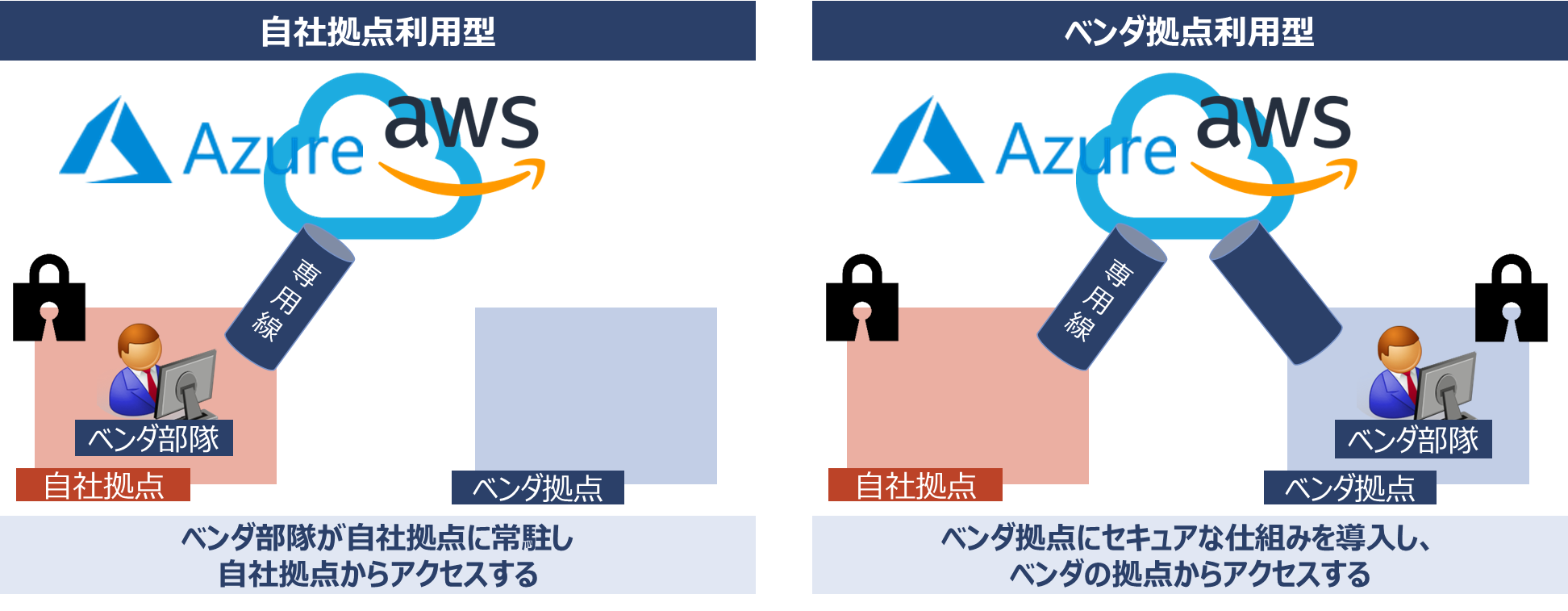


図 4‑10 自社拠点利用型とベンダ拠点利用型

#### 採用する接続形式の選定方針

採用する接続形式は、自社の外部委託に関する社内ルールや外部ベンダ側のファシリティの保有状況等、複数の要素を勘案し、最適な形式を判断する必要がある。

ただし、本番稼働中のトラブルのように、ベンダ要員による迅速な対応を要するケースが発生しうることを鑑み、特別な自由が無い限りベンダ拠点利用型を採用することを強く推奨する。

（現状の社内ルールでベンダ拠点での開発・運用を認めていない場合は、当該ルールの見直しを行うことが望ましい。）

#### 【参考】　ベンダ拠点利用型の構成例

ベンダ拠点利用型とする場合の具体的な構成例を示す。

* ベンダ拠点利用型の構成例と考慮すべきポイント

ベンダ拠点利用型を採用する場合の構成例とポイントを「図 4‑11 ベンダ拠点利用型の構成例とポイント」に示す。

本構成では、テナントシステムとは別のアカウント（ベンダ拠点接続用アカウント）に、踏み台サーバとマネジメントコンソールアクセス用のプロキシサーバを配置し、テナントシステムへのアクセスをそれらのサーバからのみ許可する。

そのうえで、テナントシステム側とベンダ拠点接続用アカウント側の双方で「図 4‑11 ベンダ拠点利用型の構成例とポイント」の1～10に示したポイントを遵守するようルール化する。

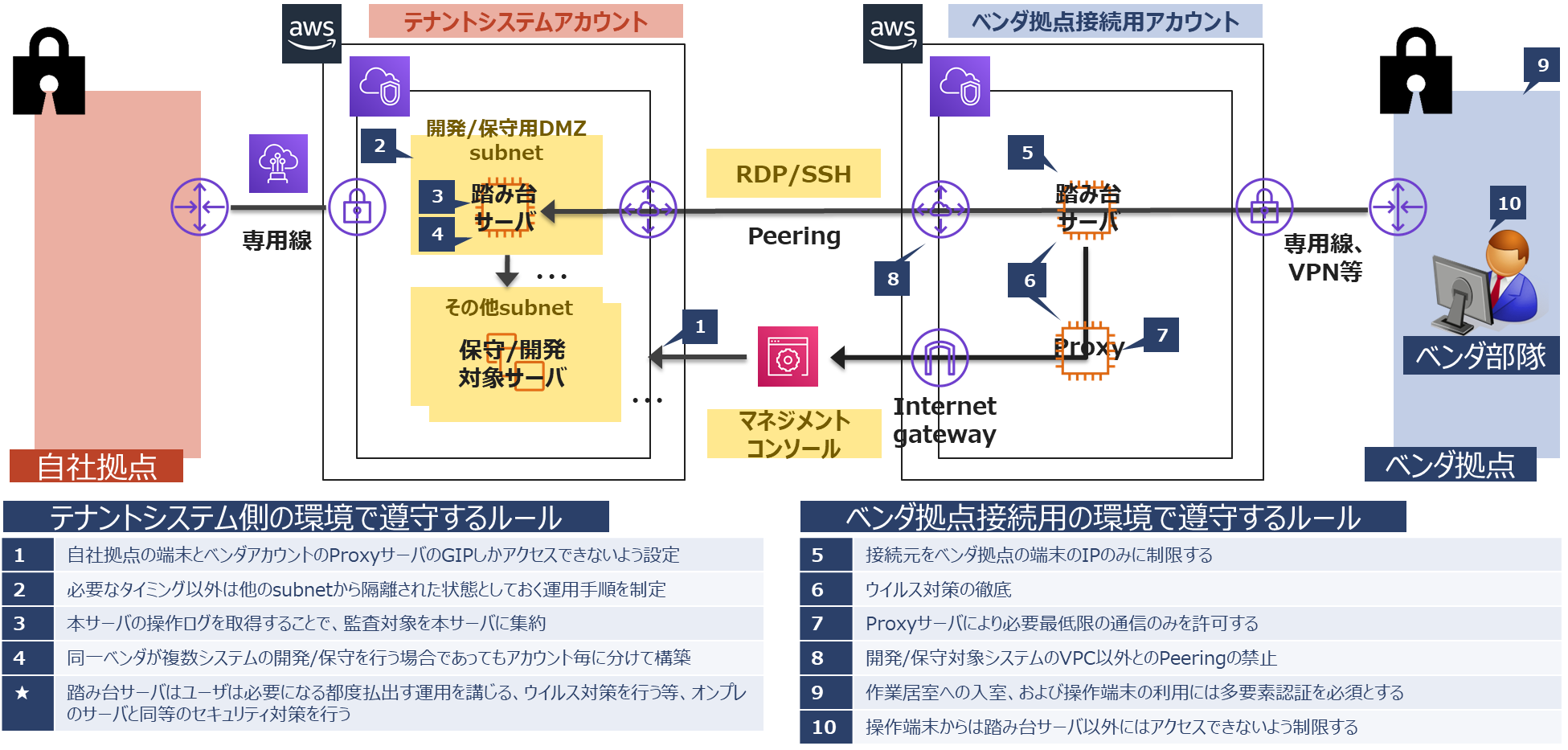


図 4‑11 ベンダ拠点利用型の構成例とポイント

* ベンダ拠点接続用アカウントの払出しパターン

ベンダ拠点接続用アカウントは、自社でA-gateのアカウントとして払出すケース（パターンA）とベンダ側で用意するケース（パターンB）の2パターンがある。（「図 4‑12 ベンダ拠点接続用アカウントの払出パターン」参照）

どちらのパターンを採用するかは観点（「図 4‑13 パターンの比較観点」に観点の例を示す）を設けて比較し、自社に適したものを採用することが望ましい。

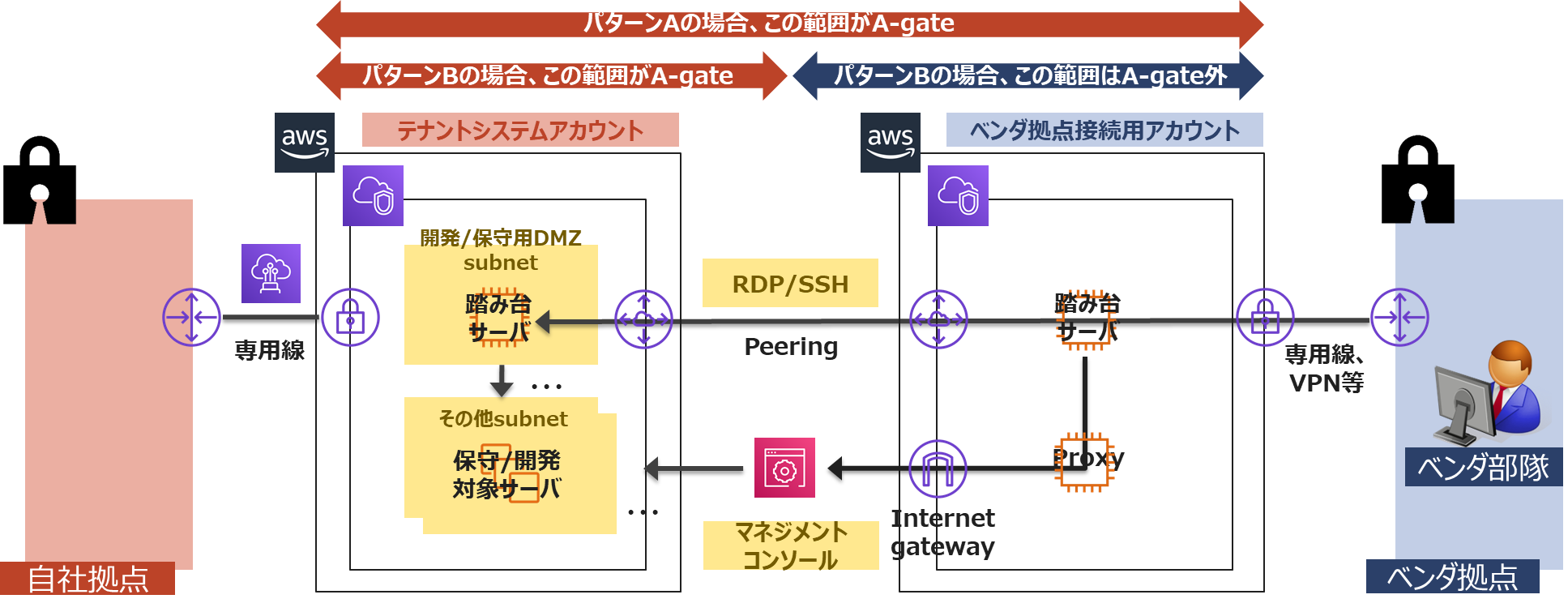


図 4‑12 ベンダ拠点接続用アカウントの払出パターン

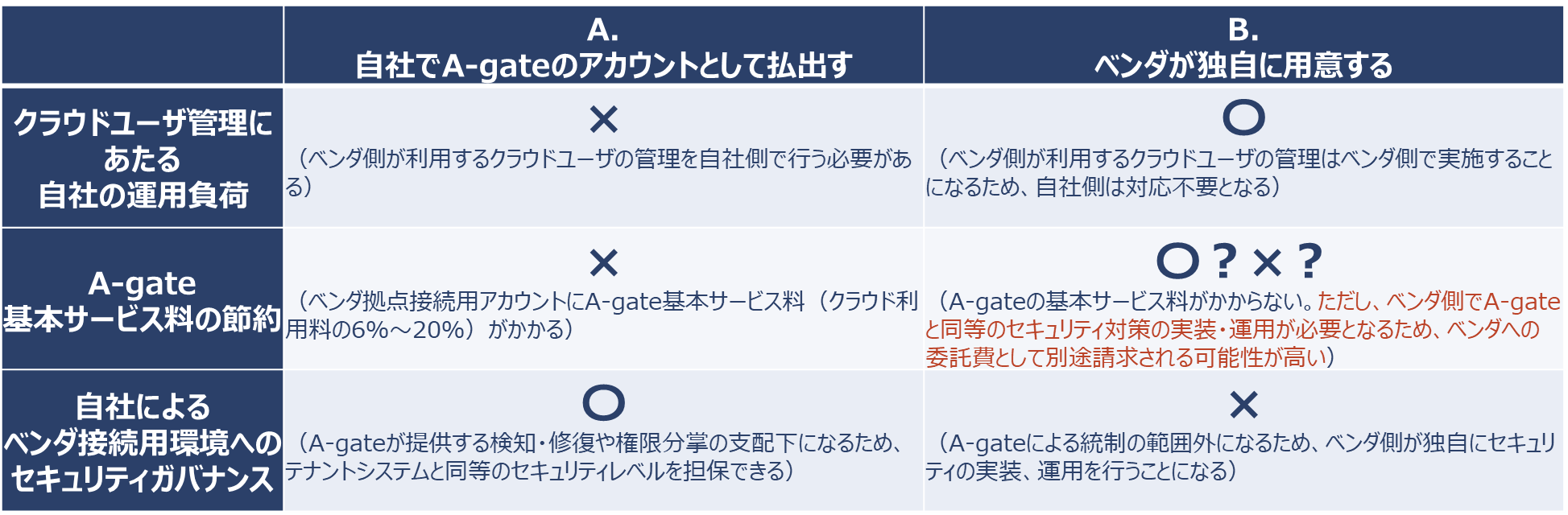


図 4‑13 パターンの比較観点

### データ暗号化指針

パブリッククラウド上に配置したデータの流出による情報漏洩を防ぐため、データが不正に持出されても情報漏洩に直結しないよう、パブリッククラウド上に配備するデータは暗号化を義務付けることが望ましい。

本項ではパブリッククラウド上でデータを暗号化する場合の実施方法の選択肢、および選定にあたる評価軸を示す。各選択肢の特徴を理解したうえで、自社に最適な方法をルールとして制定すること。

#### 鍵の作成・管理方法の選択肢と評価軸

暗号化に用いる鍵の生成・管理方法の選択肢、および評価軸について「表 4‑4 鍵の生成・管理方法の評価軸」、「表 4‑5 鍵の生成管理方法の選択肢と評価」に示す。

|  |  |
| --- | --- |
| 評価軸 | 説明 |
| クラウドへの  依存度 | 暗号化に用いる鍵の作成と保管について、どれだけ自社側のガバナンスを効かせることができるか、という観点  他者（クラウド）に任せることが不安であり、自社で確立したセキュアな運用ルールやHSM等の仕組みに則りたい場合は、クラウドへの依存度が低い方式を選択する |
| 運用負荷 | 暗号化に用いる鍵の作成と保管にあたり、どれだけ自社側に運用負荷がかかるか、という観点  他者（クラウド）に任せる範囲を広くすればその分運用負荷は低くなるため、「クラウドへの依存度」の観点とはトレードオフの関係にある |

表 4‑4 鍵の生成・管理方法の評価軸

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No, | 選択肢 | | 評価軸 | | 特徴 |
| 鍵の作成 | 鍵の保管 | クラウドへの依存度 | 運用負荷 |
| 1 | 利用者 | 利用者 | 弱 | 大 | 鍵の作成・保管を利用者の設備で実施する。クラウドに一切依存せず、最も利用者のガバナンスが効かせられる反面、運用の負荷が大きい |
| 2 | 利用者 | クラウド |  |  | 鍵の作成のみを利用者の設備で実施することで、鍵の複雑さのみ利用者のガバナンスを効かせることが可能である |
| 3 | クラウド  (手動) | クラウド |  |  | 鍵の作成・保管共にクラウドのサービスを利用する。鍵の作成のオペレーションは、利用者がクラウドサービスを使って手動実施する |
| 4 | クラウド  (自動) | クラウド | 強 | 小 | 鍵の作成・保管共にクラウドのサービスを利用する。鍵の作成のオペレーションもクラウド側で自動実施する |

表 4‑5 鍵の生成管理方法の選択肢と評価

## 設計・開発編

本節では主に、個別テナントシステムの設計・構築にあたり守るべきルール、指針について述べる。

### ネットワークアクセス制御方針

テナントシステムの設計にあたり、データの流出による情報漏洩を防ぐため、データの不正持出を狙う脅威の主体（オンプレミスNW側から侵入する内部犯、およびInternetから侵入する外部犯）が容易にデータにアクセスできないようにする対策が必要である。

上記対策の実現方法として、**データと脅威の主体の間に、ネットワーク的なアクセス制御ルールで分離した「ゾーン」を設けることが有効**である。

本項では、ゾーンの設置パターン、およびゾーン間に設けるべきネットワークアクセス制御ルールの指針について述べる。

#### ゾーン分離の基本的な考え方

脅威の主体に対し、データおよびデータを操作するロジックを隠蔽することを目的とし、ゾーンは「表 4‑6 推奨するゾーン構成」に示す3層構成とすることを推奨する。

|  |  |  |
| --- | --- | --- |
| 層 | 説明 | 配置する機能の役割 |
| Interface層 | 脅威（オンプレミスNW、およびInternet）と  直接接する層 | * アクセスの受付・攻撃緩衝 * 負荷分散 * データアクセスロジックの隠蔽 |
| Function層 | 脅威とデータの中間に位置する層 | * データアクセスロジックの実装 * 柔軟性（拡張性）の確保 * データの隠蔽 |
| Data層 | データを格納する層 | * データの永続化 * データの機密性・完全性・可用性の確保 |

表 4‑6 推奨するゾーン構成

ゾーン間のアクセス制御指針

セキュリティを担保するために設けるべきゾーン間のアクセス制御ルールについて述べる。

* インバウンドアクセスルール

テナントシステムへのインバウンド通信は、原則、隣接するゾーンに対してのみアクセスを許可する。

許可する通信プロトコルは業務上必要最小限のものに限定する。(「図 4‑14 インバウンドアクセスルールの推奨構成」参照)

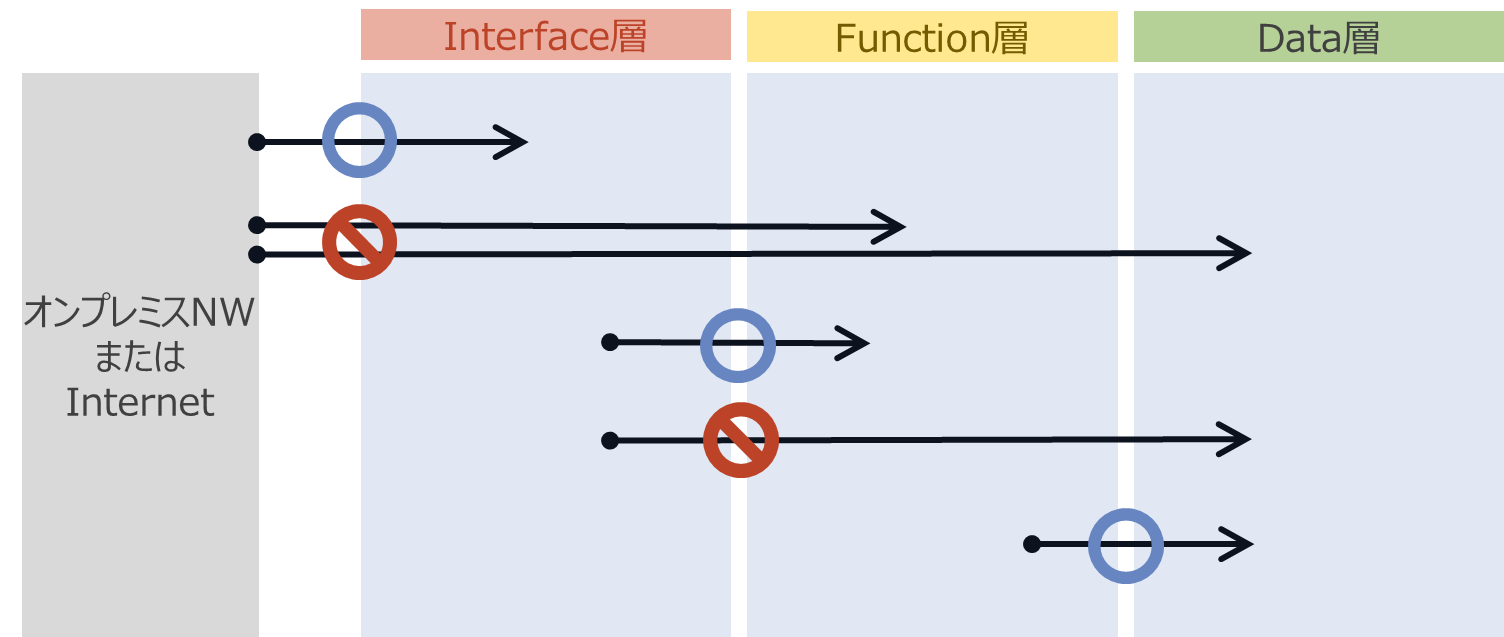


図 4‑14 インバウンドアクセスルールの推奨構成

* アウトバウンドアクセスルール

テナントシステムからのアウトバウンド通信は、隣接するゾーン、およびInterface層のゾーンへのアクセスのみを許可する。また、オンプレミスNWおよびインターネットへのアクセスはInterface層からのみに制限する。

（Interface層のゾーンへの直接アクセスを許可する理由は、運用上の利便性が高くなるケースがあるためである。例えば、Data層のDBサーバがInterface層のProxyサーバを経由し、システム外にウイルスパターンファイルやOSパッチを取得しに行くことが可能になる等。）

許可する通信プロトコルは、業務上必要最小限のものに限定する。（「図 4‑15 アウトバウンドアクセスルールの推奨構成」参照）

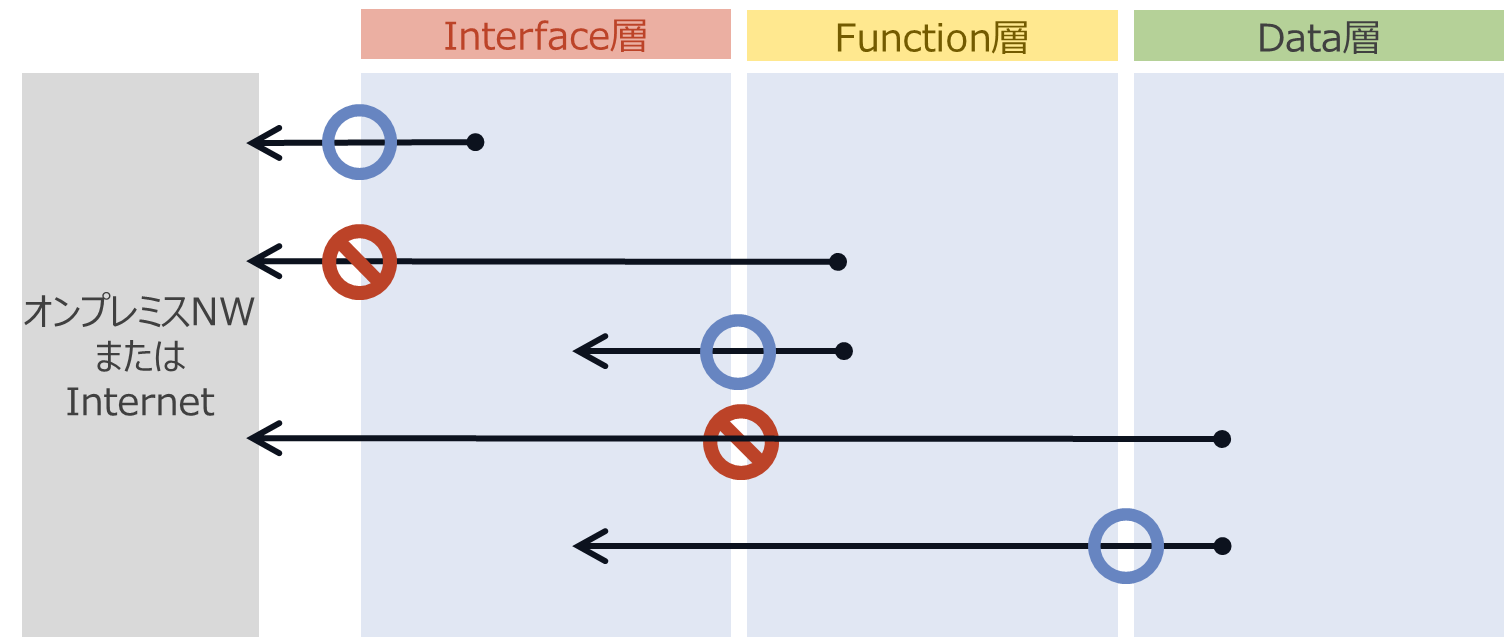


図 4‑15 アウトバウンドアクセスルールの推奨構成

* 運用系アクセスルール

監視・保守用の通信で利用する経路は、通信元・通信先・通信プロトコルを必要最低限に絞ったうえで直接アクセスを許可する。（「図 4‑16 運用系アクセスルールの推奨構成」参照）

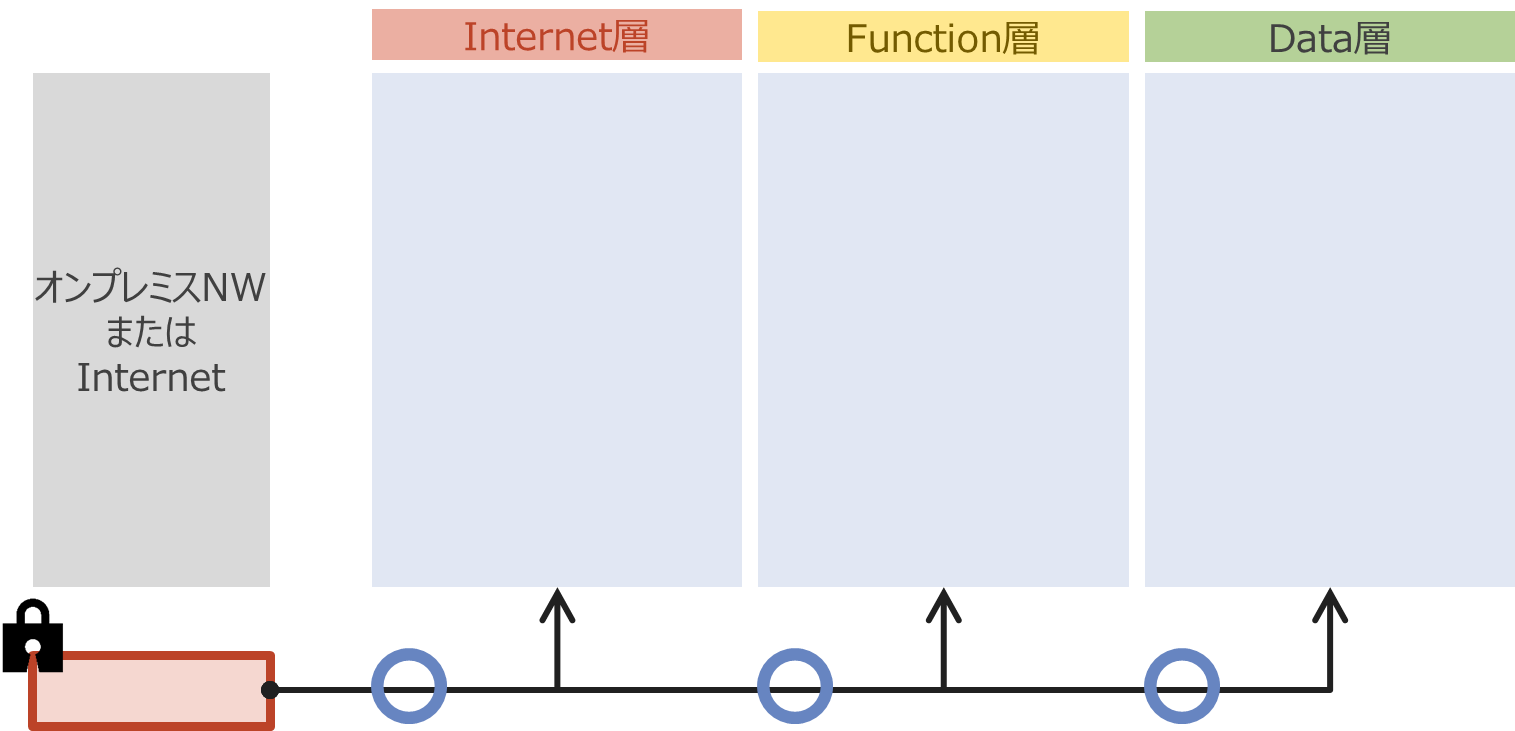


図 4‑16 運用系アクセスルールの推奨構成

#### A-gateにおけるゾーン（Subnet・SG）の払出パターン

A-gateにおけるゾーンの払出パターンについて述べる。各テナントシステムの設計者はA-gateから払出されたSubnet・SGに対し、「(1)ゾーン分離の基本的な考え方」、「(2)ゾーン間のアクセス制御指針」の考え方を参考に適切なアクセス制御ルールを設計すること。

* AWSにおけるゾーンの考え方

AWSでは、ゾーンはSubnet、SG、Routetableにより構成する。

* A-gateにおける初期払出時のゾーンの構成

A-gateでは、各テナントシステムが「(1)ゾーン分離の基本的な考え方」、「(2)ゾーン間のアクセス制御指針」の考えに則ったネットワークアクセス制御を行うことを前提とし、アカウントの初期払出時に「図 4‑17 初期払出時のゾーン構成」に示す構成のSubnet、SG、Routetableを払出す。

なお、払出対象のSubnet・SGは、各テナントシステムの要件（例：Internet接続の有無等）に応じ、必要なもののみに限定することが可能である。

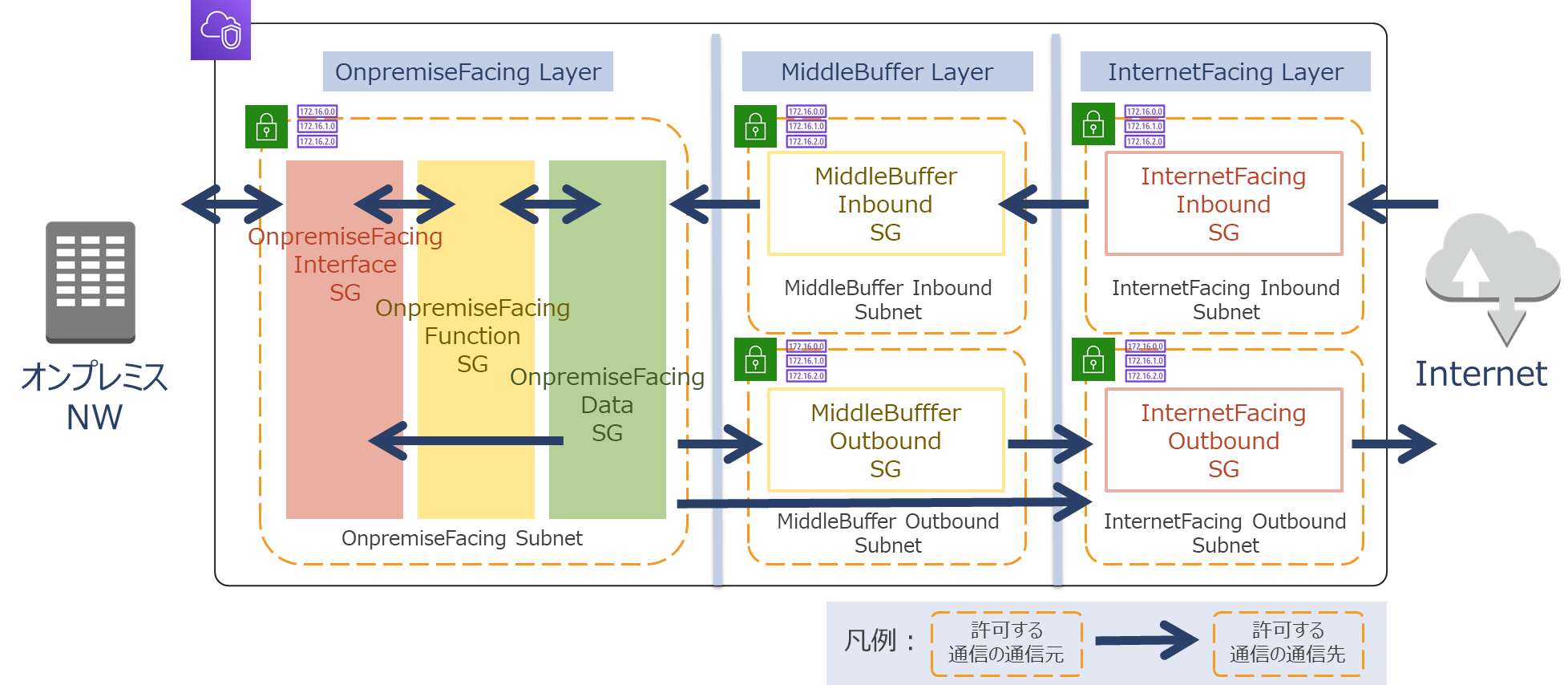


図 4‑17 初期払出時のゾーン構成

|  |  |  |  |
| --- | --- | --- | --- |
| ゾーン | | 層 | 配置する機能・サービスの例 |
| Onpremise  Facing | Interface | Interface層（オンプレミスNW側） | 社内向けロードバランサ |
| Function | Function層（オンプレミスNW側） | 社内向けWeb/APサーバ |
| Data | Data層 | DBサーバ |
| Middle  Buffer | Inbound | Function層（Internet側） | 社外向けWeb/APサーバ |
| Outbound | Function層（Internet側） | Proxyサーバ用ロードバランサ |
| Internet  Facing | Inbound | Interface層（Internet側） | 社外向けロードバランサ、WAF |
| Outbound | Interface層（Internet側） | Proxyサーバ |

表 4‑7 初期払出対象の各ゾーンの役割

* 【補足】　Internet側の各層におけるInbound通信用ゾーン・Outbound通信用ゾーンの分離

Internet側のInterface層とFunction層（InternetFacing Layer・MiddleBuffer Layer）は、オンプレミスNW側と比較すると、不特定多数の脅威にさらされるため、よりセキュリティリスクが高いゾーンである。

そのため、それぞれをInbound通信専用のゾーンとOutbound通信専用のゾーンに分割することで、よりセキュアなネットワークアクセス制御が行える構成としている。

### バックアップ取得方法

オンプレミスの場合と同様、クラウド上に構築するシステムにおいてもデータのバックアップを適切に取得し、データ損失を伴うトラブルの復旧時間を最小限に抑え、ビジネスへの影響を極小化する必要がある。

本節では、AWSにおける代表的なバックアップの取得方法について述べる。テナントシステムの設計者は、本情報を参考に、適切なバックアップ設計を行うこと。

#### AWSにおけるバックアップの取得方法

AWSの各種バックアップはストレージサービスであるAmazon S3上に取得する。

AWSにおけるバックアップの全体像を「図 4‑18 AWSのバックアップの全体像」に、また、代表的なバックアップ対象とそれぞれの特徴について「表 4‑8 バックアップの種類と主な特徴」に示す。

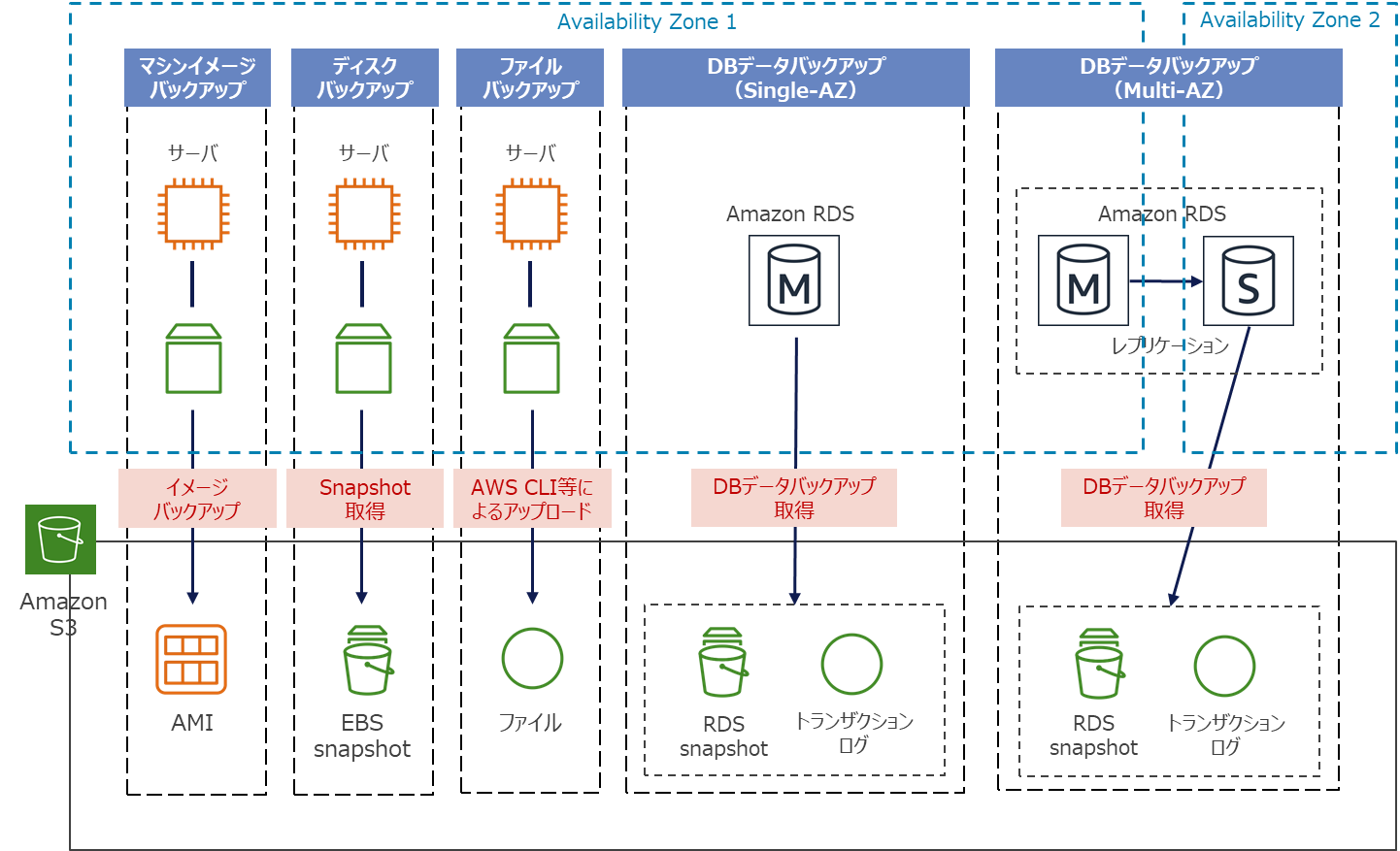


図 4‑18 AWSのバックアップの全体像

|  |  |
| --- | --- |
| バックアップ対象 | 説明・ポイント等 |
| マシンイメージ | * EC2インスタンスのマシンイメージのバックアップをAMI（Amazon Machine Image）として取得する * 一時的に存在するファイルや編集中のファイルもそのまま記録されてしまうため、インスタンスを停止した上で取得することを推奨する * リストア時は、対象のインスタンスを停止し、AMIから新規インスタンスを作成する。（その際、IPアドレス等の踏襲したい情報はリストア前と同等の値を指定する。） |
| ディスクイメージ | * EC2インスタンスにアタッチしているディスク（EBSボリューム）のスナップショット * 一時的に存在するファイルや編集中のファイルもそのまま記録されてしまうため、インスタンスを停止した上で取得することを推奨する * リストア時は、スナップショットから新規EBSボリュームを作成し、EC2インスタンスにアタッチする。（必要なファイルのみコピーした後デタッチすることで、ファイル単位の復元も実現可能。） |
| ファイル | * S3のクライアント（例：S3 APIを実行するユーザアプリケーション、CLI、マネジメントコンソール等）を用いて、バックアップ対象のファイルをアップロードする * リストア時は、バックアップと同様の手段でS3からダウンロードする |
| DBデータ  （Single-AZ  構成のRDS場合） | * RDS内のデータのバックアップ。特定時点の断面であるスナップショットと、更新情報であるトランザクションログをS3にバックアップする * スナップショットは1日1回、トランザクションログは5分間隔で自動取得される（スナップショットは、任意のタイミングで手動取得も可能） * スナップショット取得中はI/Oが短時間（数秒～数分）中断する * リストア時は、スナップショットから新たにRDSのインスタンスを起動し、セキュリティグループおよびパラメータグループ（インスタンスに適用するDBMSのパラメータのセット）等をリストア前と同じものを適用する * アプリケーション側で設定しているRDSインスタンスの接続先情報（エンドポイント）がリストアに伴い変更となる。本変更に伴うアプリケーション側の設定変更を行わずに済むよう、Route53にCNAMEレコードを登録しておくことが望ましい。詳細は（※）参照   （※）<https://docs.aws.amazon.com/ja\_jp/Route53/latest/DeveloperGuide/routing-to-rds-db.html> |
| DBデータ  （Multi-AZ  構成のRDS場合） | （※）　基本的に「DBデータ（Single-AZ構成のRDSの場合）」と同様。ただし、Multi-AZ構成の場合、スナップショットはスタンバイ側のインスタンスから取得されるため、I/O中断の影響は受けない |

表 4‑8 バックアップの種類と主な特徴

### インスタンス利用料支払い方法の選択

AWSではインスタンス利用料の支払い方法が複数提供されており、インスタンスのユースケースに適した購入オプションを選択することで、インスタンス利用料を最適化できる。

テナントシステムの設計・構築時にはインスタンスのユースケースを見定め、それに適した課金オプションを選択すること。

#### 購入オプション

AWSのEC2では「表 4‑9 インスタンスの購入オプション」に示した課金オプションが選択できる。（※　2019/4現在の情報）

各課金オプションに適するユースケースを踏まえ、SIMPLE MONTHLY CALCULATOR（※）で具体的な見積りを行い、最適な課金オプションを選択すること。

（※）<https://calculator.s3.amazonaws.com/index.html>

|  |  |  |
| --- | --- | --- |
| オプション | 説明 | 適するケース |
| オンデマンド  インスタンス | * デフォルトの従量課金方式 * EC2インスタンスが起動している時間に応じて料金が発生する * 当月中の利用料が毎月請求される | * 計画的な停止時間があるインスタンス （例：日中帯のみ稼働するオンラインAPサーバ、有事のタイミングのみ起動するデバッグ用環境のサーバ、等） * ScaleSetsでピーク時のみ起動するインスタンス |
| スポット  インスタンス | * インスタンスの利用有無を入札による決める仕組み * スポット価格（需要と供給により常時変動） * スポット価格が、利用者が指定した入札価格を上回った場合、インスタンスが停止する | * いつ削除されてもよいインスタンス （例：AutoScalingで追加起動するサーバ） |
| Dedicated  Host | * 専用の物理サーバで複数のインスタンスを起動できる * 物理サーバ単位で課金される | * インスタンス上で利用するソフトウェアの制約上、ライセンスを特定の物理サーバに紐づける必要があるケース等 |
| リザーブド  インスタンス | * 1年または3年の利用予約をすることで割引される仕組み | * 長期的な常時稼働が見込まれるインスタンス （例：基幹系システムにおける運用管理サーバ） |

表 4‑9 インスタンスの購入オプション

1. **問い合わせについて**
   1. **A-gateに関する問い合わせ**

A-gate問い合わせ窓口へ以下に関する問い合せができる。

・権限分掌の仕様

・違反検知・修復の仕様(例外登録方法)

・A-gateポータルサイトの仕様

基本的なAWSの利用方法についてはAWSサポートに問い合わせること。

* 1. **Hinemosオプションに関する問い合わせ**

A-gate問い合わせ窓口へ以下に関する問い合せができる。

・Hinemosオプションのプリセット設定

Hinemosの仕様、操作方法、不具合については、HinemosCPよりHinemosサポートに問い合わせること。

1. **作業依頼について**

A-gateに作業依頼を行う場合には、A-gateポータルサイトに掲載している申込書を使って依頼することができる。

A-gateポータルサイトに申込書が無い作業の依頼が必要な場合には、A-gate問い合わせ窓口に確認すること。

作業の受付と実施日はつぎのとおり。

・受付：金曜日〆

・作業：翌営業日

※　作業の混雑具合によっては、作業完了連絡が作業日の翌営業日となる。

※　AWSのアカウント追加が必要な場合には、A-gate営業窓口に申込むこと。

※　申込方法を別途取り決めている場合

アカウント追加にあたり申込み方法について別途取り決めている場合は、別途取り決めている方法で申込むこと。  
事前の取り決め状況が不明な場合は、A-gate営業窓口に確認すること。