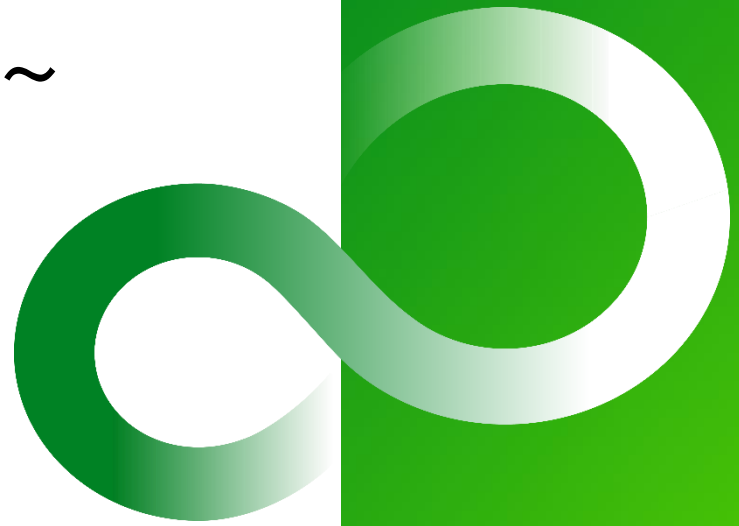
FUJITSU Hybrid IT Service FJcloud-O 設計構築ガイド

～構成サンプルから理解するIaaSと システム設計時のポイント～



V1.2.4版(2022年2月1日)

富士通株式会社

改版履歴

版	日付	内容	備考
1.0	2016.4.27	初版(2016年4月)	
1.1	2017.1.23	2017年1月時点のサービス/機能提供状況と制限事項・注意事項の情報を反映	
1.2	2018.3.30	スナップショットによるバックアップについて記載を見直し	
1.2.1	2019.11.20	サービス名称変更	
1.2.2	2020.6.11	サービス名称変更	
1.2.3	2021.8.6	“2-1-2 耐障害性” バックアップ方法 のストレージ内のデータをファイル単位でバックアップを取得する場合の説明を変更	
1.2.4	2022.2.1	“2-3. 運用・保守性で検討する項目 (5/7)” API操作時のエンドポイントからTLS/1.1を削除	

はじめに

- 本資料の目的、対象読者、前提知識
- 商標登録について／免責事項
- 本資料の構成

本資料の目的、対象読者、前提知識

FUJITSU

- 本資料は、以下のサービスを対象としています。

  FUJITSU Hybrid IT Service FJcloud-O IaaS（旧名称　FUJITSU Cloud Service for OSS IaaS）（以下本サービスまたはFJcloud-O IaaS、またはIaaSと略称）
  対象となるリージョンは東日本１、東日本２、西日本１、西日本２です。

- 本資料の目的

  FUJITSU Hybrid IT Service FJcloud-O IaaS　設計構築ガイド～構成サンプルから理解するIaaSとシステム設計時のポイント～ (以下、本資料) は、 富士通株式会社 (以下、当社) が提供するFJcloud-O IaaS　を利用したシステム設計を行う上で必要な、各サービスの特徴、留意事項について、構成サンプルの実装を通じて概要を説明し、非機能要件の単位でシステム設計時のポイントを解説することに　より、IaaSをご利用いただく方がシステム設計を円滑に行えるようになることを目的としています。

- 対象読者

  本資料は、下記のようなシステム設計を担当する方を対象としています。
  - インフラ/ネットワーク設計・構築者
  - Web/業務システム管理者/運用者
  - システムインテグレータ

- 前提知識

  前提として、以下の知識が必要です。
  - 仮想化技術（ハイパーバイザ、仮想サーバ、仮想ストレージ、仮想ネットワーク）に関する基本的な知識
  - OpenStackに関する基本的な知識
  - 使用するOSに関する基本的な知識
  - インターネット、イントラネットに関する基本的な知識
  - セキュリティに関する基本的な知識
  - バックアップ、監視、冗長化などシステム運用に関する基本的な知識

商標登録について／免責事項

FUJITSU

○ 商標登録について

- ○ 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
- ○ その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

○ 著作権・商標権・その他の知的財産権について

- ○ 本資料は、著作権・商標権・その他の知的財産権で保護されています。本資料を形式、手段(電子的又は機械的)、目的に関係なく、当社の書面による事前の承諾なく、複製、内容の改変、又は転載することを禁止します。
- ○ 本資料内の分類体系は、「IPAシステム基盤の非機能要求に関する項目一覧」 を使用しています。

○ 本資料のご利用について

- ○ 利用契約を条件に、本資料のシステム設計/構築に関する記載内容を、ご自由に利用いただけるものとします。ただし、お客様の利用については、お客様ご自身の判断と責任でなされるものとし、すべての資料、プログラム等は現状のまま提供され、当社は一切保証いたしません。また、その場合も、上記のとおり、著作権・商標権・その他知的財産権は保護されています。
- ○ ご契約いただくと、IaaSで提供する個々の機能の操作について、ヘルプデスクにお問い合わせが可能になります。その他 ヘルプデスクでは、個々の機能についてはお問い合わせ可能ですが、本資料の記載内容をそのまま又は変更するに関係なく、本資料の記載内容と同等または記載内容に類するシステム設計/構築に関する具体的なお問い合わせにはご回答できません。

○ 免責事項

- ○ 本資料は、2017年1月1日時点の情報をもとに記載しています。
- ○ 本資料は、単に情報として提供され、内容は予告なしに変更・廃止されることがあります。
- ○ 本資料について、当社は、その正確性、商品性、利用目的への適合性を保証しません。明示的又は黙示的な保証や条件は、一切無いものとします。
- ○ 本資料について、当社は、いかなる責任も負いません。本資料により、直接又は間接にいかなる契約上の義務も負うものではありません。
- ○ 本資料に記載された記載内容の使用に起因する 第三者の特許権 および その他の権利の侵害については、当社はその責を負いません。

○ 輸出管理規制について

- ○ 本資料を輸出又は第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

サービス名称の省略名について

本書では以下のオプションサービス名称を省略名で記述しています。

- FUJITSU Hybrid IT Service FJcloud-O Digital enhanced Exchange
  （旧サービス名称　FUJITSU Cloud Service for OSS プライベート接続　）
  省略名：FJcloud-O DEX
- FUJITSU Hybrid IT Service FJcloud Trend Micro Cloud One - Workload Security オプション
  （旧サービス名称 FUJITSU Cloud Service Trend Micro Deep Security as a Service オプション
  FUJITSU Cloud Service Trend Micro Cloud One - Workload Security オプション
  省略名： FJcloud C1WS オプション

本資料の構成① 第1章の構成

FUJITSU

■第1章の構成

■第1章では、構成サンプルの実装作業を通じて、IaaS の機能を説明していきます。
まったく知らない場合や、かいつまんで把握したい場合、構築時の段取りを把握したい場合は、第1章をご覧ください。

- **1-1 Web/DBシングルAZ構成**
  WebサーバとDBサーバだけを配備するシンプルな構成の実装を通じて、 IaaS の機能を記載します。

- **1-2 Web/DBマルチAZ構成**
  信頼性や性能向上の考え方を盛り込んだ構成の実装を通じて、マルチAZ構成やロードバランサー、データベース冗長構成等を記載します。

■第1章の各内容については、以下のハイパーリンクからも参照可能です。

1-1	1-2	作業項目	作業内容
p.14	p.35	実装作業	内部ネットワークを作成し、サブネットを設定
p.16	p.36	実装作業	仮想サーバに割り当てる グローバルIPアドレス を確保
p.17	p.37	実装作業	セキュリティグループを設定
p.23	p.40	実装作業	仮想ルータを作成し、仮想ルータにファイアーウォールを設定
p.25	p.43	実装作業	仮想ルータをネットワークに接続
	p.44	実装作業	ネットワークコネクター、コネクターエンドポイントを配備
	p.45	実装作業	サブネットにルーティング情報を設定
p.26	p.47	実装作業	仮想サーバを作成
p.28	p.48	実装作業	仮想サーバにグローバルIPアドレスを設定
	p.49	実装作業	ロードバランサーを配備
p.29	p.51	実装作業	データベースサービスを配備
p.30	p.52	実装作業	すべての作業が終わったら、ファイアーウォール/セキュリティグループのアクセス制御を変更してインターネットに公開

本資料の構成②　第2章の構成

FUJITSU

■ 第2章の構成

■ 第2章は、IPAの「システム基盤の非機能要求に関する項目一覧」の大項目、中項目の単位で、利用する際に検討が必要な事項について記載します。

- **2-1 可用性**
  IaaSで提供される仮想サーバ、ストレージ、ネットワークの可用性について記載します。
  - 2-1-1　継続性
  - 2-1-2　耐障害性
  - 2-1-3　災害対策
  - 2-1-4　回復性
- **2-2 性能・拡張性**
  IaaSで提供される仮想サーバ、ストレージ、ネットワークの性能・拡張性について記載します。
  - 2-2-1　性能目標値
  - 2-2-2　リリース拡張性
  - 2-2-3　性能品質保証
- **2-3 運用・保守性**
  IaaSで提供される運用監視、サポートメニューについて記載します。
  - 2-3-1　通常運用
  - 2-3-2　保守運用
  - 2-3-3　障害時運用
  - 2-3-4　運用環境
  - 2-3-5　サポート体制
- **2-4 セキュリティ**
  IaaSで提供される仮想サーバ、ストレージ、ネットワークのセキュリティについて記載します。
  - 2-4-1　アクセス・利用制限
  - 2-4-2　データの秘匿
  - 2-4-3　不正追跡・監視
  - 2-4-4　ネットワーク対策
  - 2-4-5　マルウェア対策
- **2-5 移行**
  IaaSで提供される移行サポートについて記載します。
  - 2-5-1　移行

第1章 構成サンプルから理解するIaaSのサービス／機能

第1章 記載内容について

FUJITSU

第1章では、基本的な構成を記載し、その構成を実装する際に必要な知識を説明していきます。

1-1.Web/DBシングルAZ構成

まず、Webサーバ と DBサーバだけを配備する、シンプルな構成を記載します。
この構成を実装するにあたって、必要となる IaaS の以下の機能について、説明します。

- アベイラビリティーゾーン (AZ)
- 外部ネットワーク
- 内部ネットワーク
- 仮想ルータ、ファイアーウォール (FW)
- セキュリティグループ (SG)
- 仮想サーバ
- データベースサービス

1-2.Web/DBマルチAZ構成

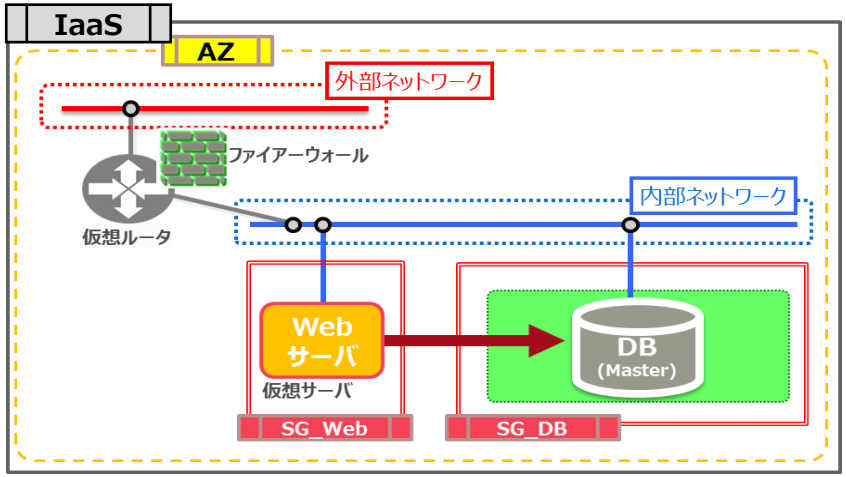
Web/DBの構成について、IaaSでとりうる可用性や性能向上の考え方を盛り込んだ構成です。
この構成を実装するにあたって、必要となる (IaaS) の以下の機能について、説明します。

- ネットワーク階層構成
- マルチAZ構成　※ネットワークコネクター (NWC) 、コネクターエンドポイント (CEP)
- ロードバランサー (LB)
- データベースサービス ※冗長化構成(Master/Standbyの運用待機構成)、リードレプリカ

第1章 記載内容について

第1章では、基本的な構成を記載し、その構成を実装する際に必要な知識を説明していきます。

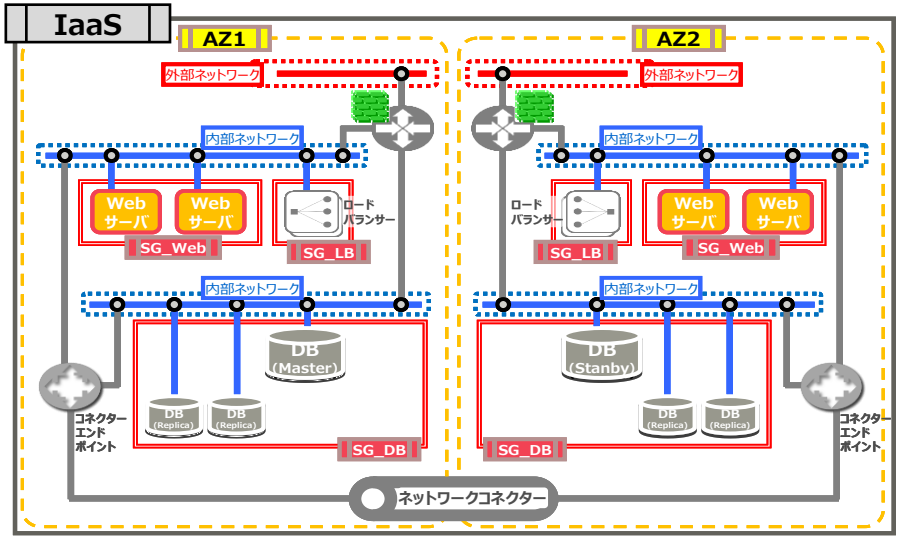
1-1.Web/DBシングルAZ構成



■1-1 構成の概要

- ✓ インターネットと内部のシステムの間に、仮想ルータを作成
- ✓ 仮想ルータにファイアーウォールを設定
- ✓ Webサーバ と DBサーバのアクセス制御用に、セキュリティグループを設定
- ✓ Webサーバ1台、DB サーバ1台を配備
- ✓ Webサーバには、グローバルIPアドレスを付与 DB サーバには、グローバルIPアドレスは付与しない

1-2.Web/DBマルチAZ構成



■1-2 構成の概要 ※1-1に対して、以下の構成を追加

- ✓ 異なるAZを2つ使用 (片方のAZで障害発生時には、もう片方のAZで業務継続)
- ✓ AZ間を内部で接続
- ✓ WebサーバとDBサーバを配備するネットワークを分離
- ✓ Webサーバ用に、ロードバランサーを配備
- ✓ Webサーバを AZごとに 2台配備
- ✓ DBサーバを運用待機構成(Master/Standby)で構成
- ✓ DBサーバに参照時の負荷を分散するリードレプリカを設定

1-1. Web/DBシングルAZ構成

① 内部ネットワークを作成し、サブネットを設定
② 仮想サーバに割り当てる グローバルIPアドレス を確保
③ セキュリティグループを設定
④ 仮想ルータを作成し、仮想ルータにファイアーウォールを設定
⑤ 仮想ルータをネットワークに接続
⑥ 仮想サーバを作成
⑦ 仮想サーバにグローバルIPアドレスを設定
⑧ データベースサービスを配備
⑨ すべての作業が終わったら、ファイアーウォール/セキュリティグループのアクセス制御を変更してインターネットに公開

本章で例示するシステムの構成と説明する機能

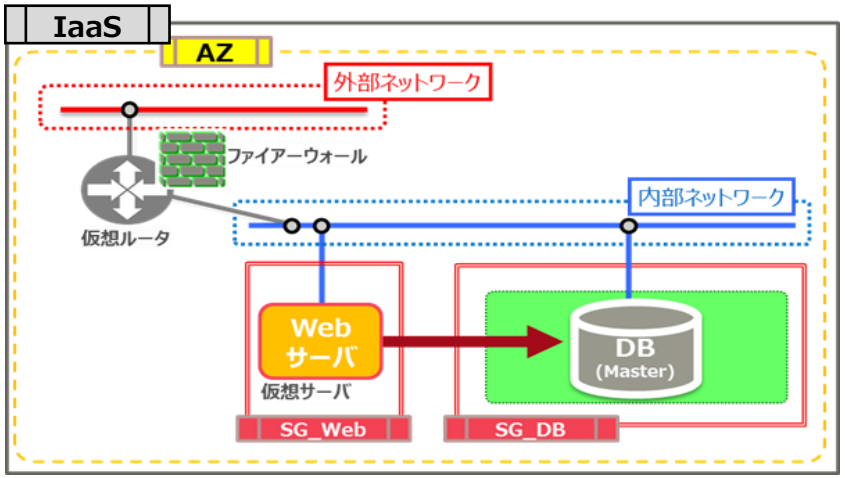
本章では、Webサーバ と DBサーバだけを配備するシンプルな構成の実装を記載しながら、
以下の IaaSの機能を説明していきます。

(1) 本章で例示するシステム構成の概要

- インターネットと内部のシステムの間に、仮想ルータを作成
- 仮想ルータにファイアーウォールを設定
- Webサーバ と DBサーバのアクセス制御用に、セキュリティグループを設定
- Webサーバ1台 (リモートログイン用のsshサーバを兼務します)、DB サーバ1台を配備
- Webサーバには、グローバルIPアドレスを付与する　　(インターネットに公開する)
- DB サーバには、グローバルIPアドレスは付与しない　　(インターネットに公開しない)

(2) 本章で説明する機能

- アベイラビリティーゾーン (AZ)
- 外部ネットワーク
- 内部ネットワーク
- 仮想ルータ、ファイアーウォール (FW)
- セキュリティグループ (SG)
- 仮想サーバ
- データベースサービス



本章で記載する実装作業の段取り

本章で記載する実装作業の段取りは以下のとおりです。

(3) 実装作業の段取り

作業内容	
①	内部ネットワークを作成し、サブネットを設定
②	仮想サーバに割り当てる グローバルIPアドレス を確保
③	セキュリティグループを設定
④	仮想ルータを作成し、仮想ルータにファイアーウォールを設定
⑤	仮想ルータをネットワークに接続
⑥	仮想サーバを作成
⑦	仮想サーバにグローバルIPアドレスを設定
⑧	データベースサービスを配備
⑨	すべての作業が終わったら、ファイアーウォール/セキュリティグループのアクセス制御を変更してインターネットに公開

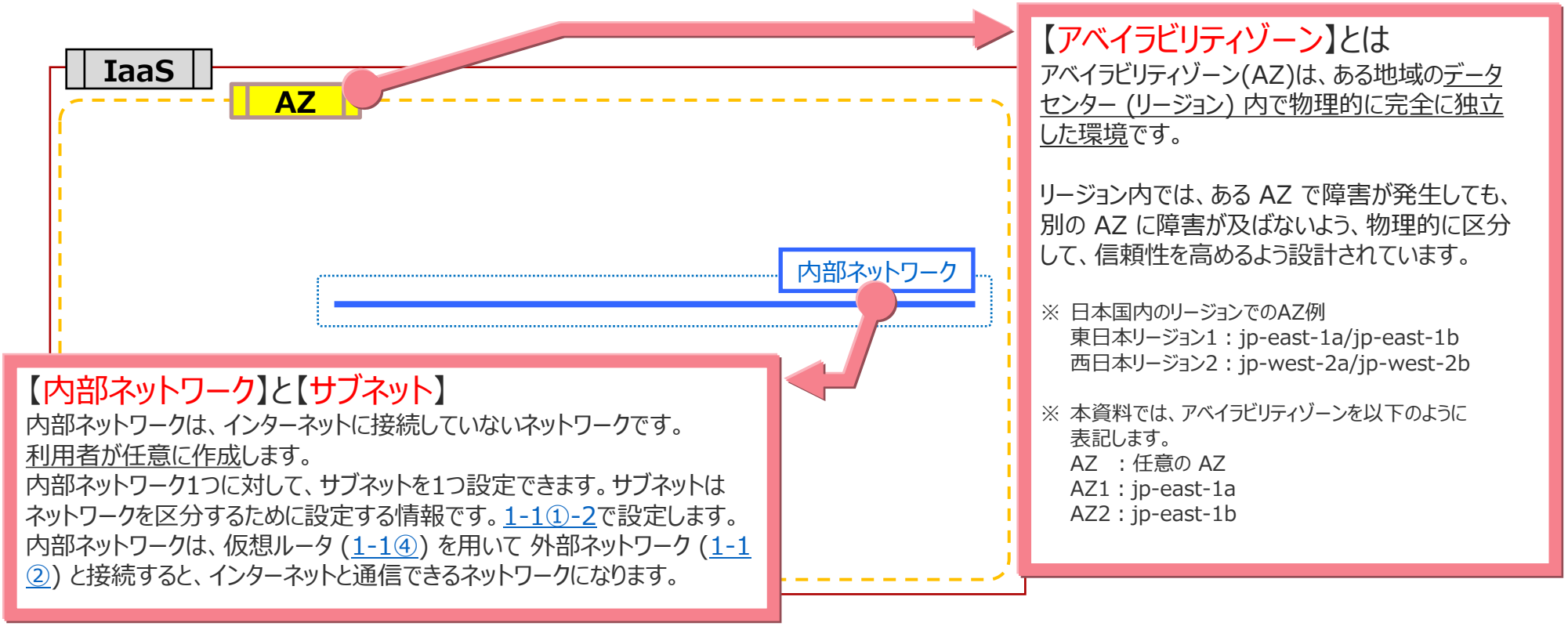
実装作業① 内部ネットワーク、サブネット (1/2)

①-1 内部ネットワークを配備するアベイラビリティゾーン (AZ) を選択

まず始めに、仮想サーバ等を配備する『内部ネットワーク』を作成します。
内部ネットワークは、IaaSの利用者が任意に作成できるネットワークです。
内部ネットワークは、アベイラビリティゾーン (以下AZ) を選択 (本ページ) して、サブネットの情報を設定 (1-1①-2) して作成します。

本ページでは、内部ネットワークを作成する際に指定する AZ を選択します。
AZは、IaaSの物理環境の区分です。

1-1の構成では、提供されているどのAZを選択してもかまいません。



【アベイラビリティゾーン】とは
アベイラビリティゾーン(AZ)は、ある地域のデータセンター (リージョン) 内で物理的に完全に独立した環境です。

リージョン内では、ある AZ で障害が発生しても、別の AZ に障害が及ばないよう、物理的に区分して、信頼性を高めるよう設計されています。

※ 日本国内のリージョンでのAZ例
東日本リージョン1：jp-east-1a/jp-east-1b
西日本リージョン2：jp-west-2a/jp-west-2b

※ 本資料では、アベイラビリティゾーンを以下のように表記します。
AZ ：任意の AZ
AZ1：jp-east-1a
AZ2：jp-east-1b

【内部ネットワーク】と【サブネット】
内部ネットワークは、インターネットに接続していないネットワークです。
利用者が任意に作成します。
内部ネットワーク1つに対して、サブネットを1つ設定できます。サブネットはネットワークを区分するために設定する情報です。1-1①-2で設定します。
内部ネットワークは、仮想ルータ (1-1④) を用いて 外部ネットワーク (1-1②) と接続すると、インターネットと通信できるネットワークになります。

実装作業① 内部ネットワーク、サブネ2/2)

①-2 サブネットの情報を設定して内部ネットワークを作成

続いて、サブネットを設定します。

サブネットの設定の中で、使用するIPアドレスの範囲や デフォルトゲートウェイ 等の一般的なネットワークの設定と、そのサブネット上に配備する仮想サーバ等のリソースに対して、①DHCP (必ず有効に設定)、②DNSサーバ、③ルーティング情報等を、あわせて設定します。

項目	必須	内容
仮想ネットワークアドレス ※変更不可	必須	CIDR形式でネットワークアドレスを設定します。　(例：192.168.0.0/24) ※IaaSで利用可能なIPアドレスの範囲は以下の通りです。 10.0.0.0　～　10.255.255.255 172.16.0.0　～　172.31.255.255 192.168.0.0　～　192.168.255.255 ※この項目は初期設定のみ可能です。後から変更できません。
ゲートウェイIP		デフォルトゲートウェイのIPアドレスを設定します。　(例：192.168.0.1)
DHCP		サブネット設定時の必須項目ではありませんが、**必ず有効にしてください**。 ※仮想サーバへのIPアドレスの配布等を DHCP 経由で行います。 DHCP が無効になっていると、そのサブネットに配備する仮想サーバ等がIPアドレスを取得できなくなります。 仮想サーバに固定のIPアドレスを設定する際も、固定のIPアドレスが DHCP 経由で仮想サーバ起動時に割り当てられます。 ※DHCP の 無効 は、DHCP で設定されたIPアドレスを振りなおす等、特別な事情がある際に使用します。 その際は、DHCPの状態を、有効→無効→有効と設定します。
IPアドレス割当プール ※変更不可		DHCP で設定するIPアドレスの範囲を設定することができます。 ※IaaSが自動的に割り当てるIPアドレスは、IPアドレス割当プールの範囲内から払い出されます。 IPアドレス割当プールを指定しない場合、ルータのゲートウェイIPアドレスを除く全てのIPアドレスが、 IPアドレス割当プールとして設定されます。 ※この項目は初期設定のみ可能です。後から変更できません。
DNSサーバ		DNSサーバを設定します。 ※DNSサーバは以下の通りです。DNSサーバの情報も、DHCP経由で仮想サーバ等に伝達されます。 AZ1：133.162.193.10、133.162.193.9 AZ2：133.162.201.10、133.162.201.9
追加のルート設定		ルーティング情報を設定します。宛先のネットワークに対して、どのIPアドレスを経由するかを設定します。 (例：192.168.10.0/24,192,168.0.254) ルーティング情報も、DHCP経由で仮想サーバ等に伝達されます。 ※1-1の構成では使用しません。1-2⑦でルーティング情報を設定しています。

memo：ポータルとAPIでのサブネット設定
IaaSポータルでは、内部ネットワーク作成の際にサブネット情報を合わせて設定します。
API の場合は、内部ネットワークを作成した後にサブネットを作成します。

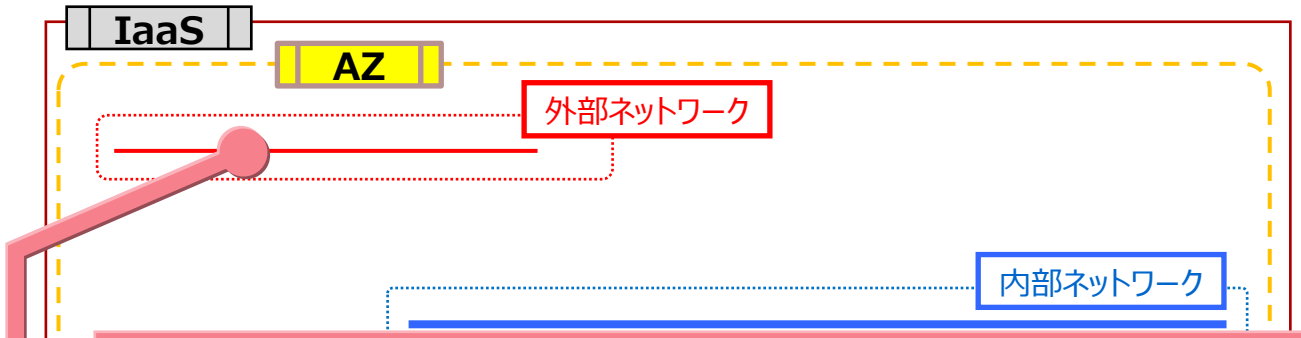
実装作業② グローバルIPアドレス

② 仮想サーバに割り当てる グローバルIPアドレス を確保

仮想サーバをインターネットに公開するために、インターネットに公開されている外部ネットワーク上のIPアドレスが必要です。
インターネットに公開されているIPアドレスを、グローバルIPアドレスといいます。

グローバルIPアドレスは、使用している AZの外部ネットワーク から取得します。
外部ネットワークは、AZごとに IaaSで複数用意されています。外部ネットワークは任意に選択してください。
※後工程で、選択した外部ネットワークと、内部ネットワークを、仮想ルータで接続します。(→1-1⑤)

グローバルIPアドレスの取得の際、IPアドレスの指定はできません。
外部ネットワーク上で使用されていないグローバルIPアドレスが、自動的に割り振られます。
取得したグローバルIPアドレスは、仮想サーバを作成した後に、仮想サーバに設定することが可能です。



【外部ネットワーク】とは
外部ネットワークは、インターネットに接続されたネットワークです。利用者が作成することはできません。
アベイラビリティゾーン (AZ) ごとに あらかじめ複数用意されていますので、任意に選択してください。
※後工程で、選択した外部ネットワークと、内部ネットワークを、仮想ルータで接続します。

【グローバルIPアドレス】とは
インターネットに公開されているネットワーク上のIPアドレスです。仮想サーバをインターネットに公開する場合は、グローバルIPアドレスが必要になります。なお、配備した仮想サーバから、インターネットに対して通信するだけの場合（インターネットから内部の仮想サーバへの通信が不要な場合）は、グローバルIPアドレスは不要です。

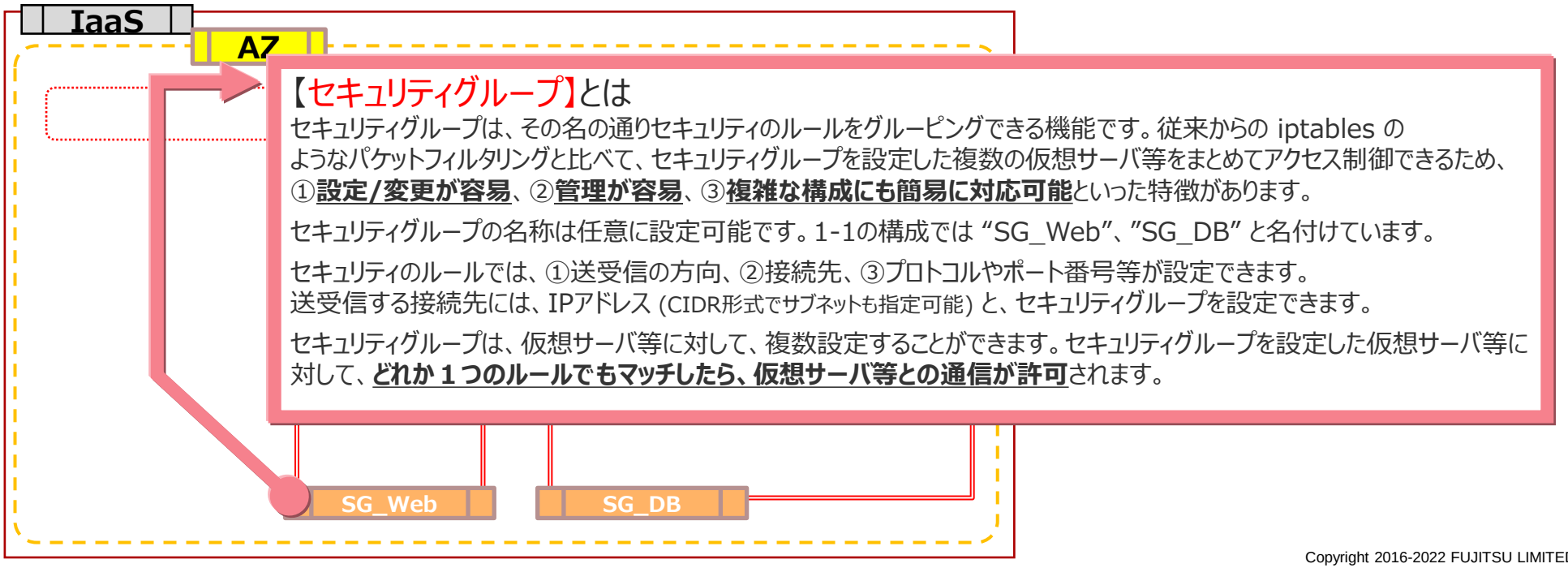
実装作業③ セキュリティグループ (1/3)

③-1 セキュリティグループを設定

仮想サーバを含むシステムをインターネットに公開するには、セキュリティの設定が必要です。IaaSのセキュリティの機能では、
セキュリティグループ という機能と、従来からの一般的なファイアーウォール機能の 2 つの機能があります。
ここではまず、セキュリティグループの設定を行います。セキュリティグループは、IaaSのセキュリティの基本となります。
以下のように、Webサーバ用に “SG_Web” 、DB用に “SG_DB” という名称でセキュリティグループを作成します。

●SG_Web	特定のアクセス元から、sshサーバ(22/tcp) へのリモートログインを許可する 不特定のアクセス元 (構築時は特定のアクセス元) に対して、Webサーバ(80/tcp) への接続を許可する セキュリティグループ “SG_DB” に対して、DBサーバ(5432/tcp) への接続を許可する
●SG_DB	セキュリティグループ “SG_Web” が設定された仮想サーバから、DB(5432/tcp) への接続を許可する

※主要分のみ/詳細は次頁



【セキュリティグループ】とは

セキュリティグループは、その名の通りセキュリティのルールをグルーピングできる機能です。従来からの iptables のようなパケットフィルタリングと比べて、セキュリティグループを設定した複数の仮想サーバ等をまとめてアクセス制御できるため、①**設定/変更が容易**、②**管理が容易**、③**複雑な構成にも簡易に対応可能**といった特徴があります。

セキュリティグループの名称は任意に設定可能です。1-1の構成では “SG_Web”、”SG_DB” と名付けています。

セキュリティのルールでは、①送受信の方向、②接続先、③プロトコルやポート番号等が設定できます。
送受信する接続先には、IPアドレス (CIDR形式でサブネットも指定可能) と、セキュリティグループを設定できます。

セキュリティグループは、仮想サーバ等に対して、複数設定することができます。セキュリティグループを設定した仮想サーバ等に対して、**どれか１つのルールでもマッチしたら、仮想サーバ等との通信が許可**されます。

実装作業③ セキュリティグループ (2/3)

③-2 セキュリティグループ “SG_Web” 設定例

※SG_Webの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	22	CIDR	x.x.x.x/32	-
カスタムTCPルール	受信	ポート	80	CIDR	(**構築時**) x.x.x.x/32 (**完了時**) 0.0.0.0/0	-
カスタムTCPルール	送信	ポート	5432	セキュリティグループ	SG_DB	IPv4
カスタムTCPルール	送信	ポート	80	CIDR	169.254.169.254/32	-
カスタムTCPルール	送信	ポート	53	CIDR	0.0.0.0/0	-
カスタムTCPルール	送信	ポート	53	CIDR	0.0.0.0/0	-
カスタムTCPルール	送信	ポート	123	CIDR	0.0.0.0/0	-
カスタムTCPルール	送信	ポート	123	CIDR	0.0.0.0/0	-

※ 表の項目は IaaS サービスポータル の セキュリティグループのルール追加画面における項目名に合わせています。
IaaS用語では、"受信" は インバウンド または ingress、"送信" はアウトバウンド または egress とも表現されます。

●IPアドレスを設定する際は、CIDR形式で設定します。
●システムの構築時は、不特定のアクセス元からWebサーバにアクセスされないよう、特定のアクセス元としておきます。
特定のアクセス元は、x.x.x.x/32 という形式だと、IPアドレス x.x.x.x をもつ特定のサーバからアクセス可能となります。
●システム構築の完了時に、不特定のアクセス元 (0.0.0.0/0) からWebサーバにアクセスできるよう、ルールを設定します。
●セキュリティグループの “SG_DB” を設定するデータベースへ、5432/tcp へのアクセスを許可します。
●169.254.169.254/32 は、キーペア等の仮想サーバが必要な情報を仮想サーバに提供する特別なIPアドレスです。
仮想サーバから169.254.169.254/32は、内部ネットワークからアクセスします。外部ネットワークが接続されていなくても問題ありません。セキュリティを厳しくする場合にも、必ず169.254.169.254/32への送信を許可する設定は入れてください。
●ポート番号53は名前解決の DNS、ポート番号 123 は時刻同期の NTP の追加例です。必要に応じて設定してください。
●パッチを取得するサーバ等も、必要に応じて追加してください。
●その他、セキュリティの考え方については『**参考：セキュリティグループとファイアーウォールの概略**』等を参照してください。

実装作業③ セキュリティグループ (3/3)

③-3 セキュリティグループ “SG_DB” 設定例

※SG_DBの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	5432	セキュリティグループ	SG_Web	-
カスタムTCPルール	受信	ポート	5432	セキュリティグループ	SG_DB	-
カスタムTCPルール	受信	ポート	5432	セキュリティグループ	SG_DB	-

●セキュリティグループの “SG_Web” が設定された仮想サーバ (Webサーバ) からの受信を許可します。
●セキュリティグループの “SG_DB” を設定するデータベースサービスで、データベースのポート番号に対して送受信を許可します。

参考：セキュリティグループとファイアーウォールの概略

FUJITSU

○セキュリティグループ

- IaaSのセキュリティの基本となる機能で、設定が必須です。
  (※セキュリティグループを指定しなかった場合、defaultという名前のセキュリティグループが自動的に指定されます。)
- セキュリティグループでは、セキュリティのルールをグルーピングできるため、
  ①設定/変更が容易、②管理が容易、③複雑な構成にも簡易に対応できます。
- セキュリティグループは、仮想サーバ等に対して、複数のセキュリティグループを設定できます。
- セキュリティグループのルールには、IPアドレスのほか、セキュリティグループも設定できます。
- セキュリティグループのルールは、ルールの順序に関わりなく、どれか 1 つのルールがマッチすれば許可されます。
- セキュリティグループは、AZで共通に使えます。

○ファイアーウォール

- デフォルトルールは全て拒否されます。(DENY ALL)
- 従来からの機能で、仮想ルータに設定します。
- ファイアーウォールでは、①送信元/送信先IPアドレス、②送信元/送信先プロトコル、③アクセス制御内容を設定します。
- セキュリティグループとちがい、③アクセス制御内容では、許可する通信だけではなく、拒否する通信を設定できます。
  →特定のアクセス元からの通信を拒否する等で利用できます。

○セキュリティグループとファイアーウォールの使い方

- ①セキュリティグループのみ という使い方と、②セキュリティグループ＋ファイアーウォール という使い方ができます。
  →セキュリティは多層防御が推奨されるため、②セキュリティグループ＋ファイアーウォールという使い方を推奨します。

○注意事項

- 仮想サーバ等を配備する前に、必ず、セキュリティグループ、ファイアーウォールでアクセス制御を設定してください。
  適切なアクセス制御を設定をしないで仮想サーバを配備した場合、不正なアクセスを受ける可能性があります。
  本ガイドでは、セキュリティグループ、ファイアーウォールを設定した後、仮想サーバ等を配備するようにしています。

参考：セキュリティグループとファイアーウォールの違い

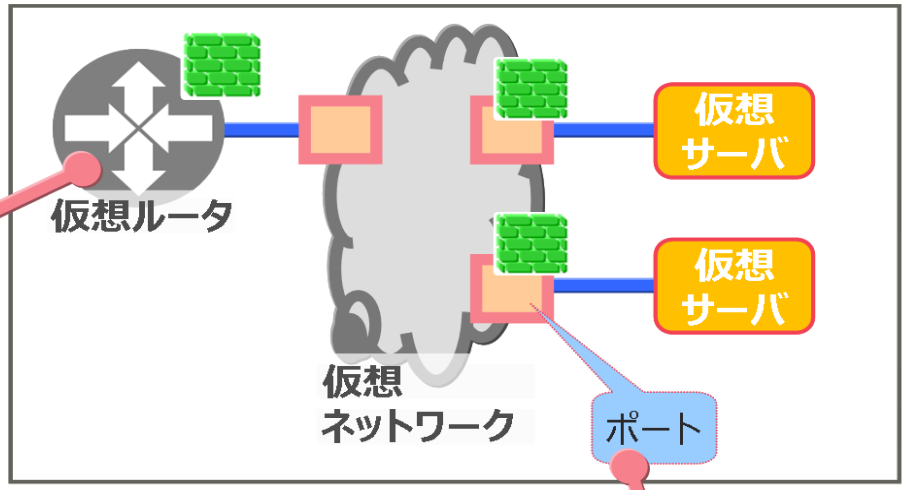
項目	セキュリティグループ（※1）	ファイアーウォール
設定する対象	仮想サーバに付けられたポート (※2) ロードバランサー、データベースサービス	仮想ルータ
通信方向の指定	セキュリティグループを適用する 仮想サーバ等に対する 受信 (ingress)、送信 (egress)	通信方向の指定はできません。
通信相手の指定	通信相手のIPアドレス (CIDR形式)、 通信相手のセキュリティグループ名	送信元IPアドレス (CIDR形式) 、 送信先IPアドレス (CIDR形式)
プロトコル、ポート番号	セキュリティグループを適用する 仮想サーバ等が通信に利用する ポート番号	送信元ポート番号、 送信先ポート番号
アクション	許可のみ	許可、拒否
判定	どれか1つでもルールにマッチした 通信は許可	優先順位にしたがってルールを判定し、 最初にマッチしたルールで許可、拒否

※1　セキュリティグループは、IaaSのベースである OpenStack で導入された考え方です。
セキュリティグループと、従来からのファイアーウォールのそれぞれの機能配置について、
物理環境と比較したイメージ図を次頁に記載しています。あわせてご参照ください。

※2　仮想サーバに付けられたポートといった文脈の場合は、ポートは、OpenStack用語の
ポートを指します。ポートの位置づけも、次頁に記載しています。

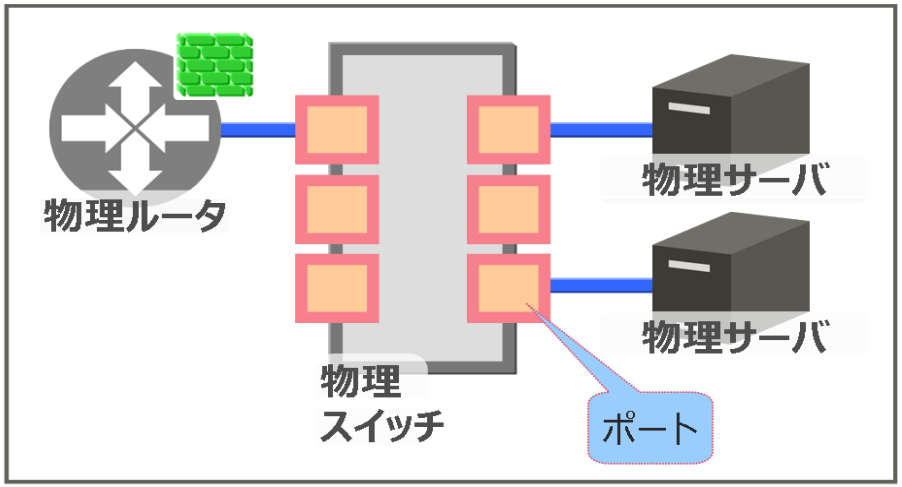
参考：セキュリティグループとファイアーウォールの機能配置

仮想環境(IaaS)



OpenStack の **仮想ルータ** では、サブネット間の**ルーティング機能**や、インターネットとの通信時に送信/受信の双方向で 使用可能な**NAT 機能**、パケット許可/遮断を設定する**ファイアウォール機能**等が提供されます。

物理環境



OpenStack の **ポート** は、物理スイッチのポートよりも高機能です。
物理スイッチのポートにはない機能として、**セキュリティグループ機能**でパケットのフィルタリングが可能です。
セキュリティグループでは、**通信相手に対する送受信の許可を設定**します。
設定で許可されないパケットは、ネットワーク上で遮断されます。そのため、**仮想サーバには、許可されないパケットが到達することがありません**。また、**仮想サーバから許可されないパケットを送信した場合**も、**ネットワーク上で遮断されます**。

実装作業④ 仮想ルータ (1/2)

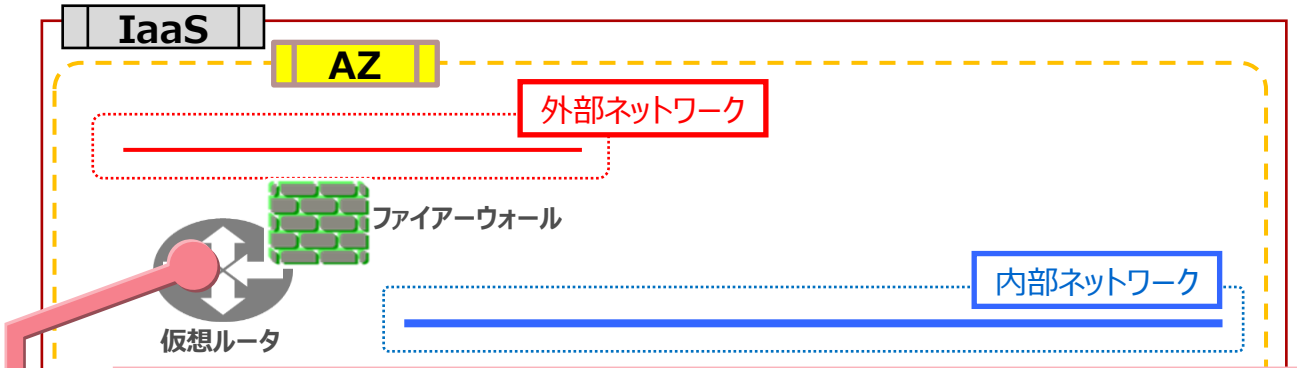
④-1 仮想ルータを作成し、ファイアーウォール機能を設定

内部ネットワークと外部ネットワークを接続し、内部ネットワークに配備する仮想サーバ等をインターネットと通信できるようにするために、内部ネットワークを配備した AZに仮想ルータを作成します。

仮想ルータには、従来からの一般的なセキュリティの機能であるファイアーウォール機能が含まれます。
セキュリティは多層防御が推奨されますので、セキュリティグループとあわせてファイアーウォールも設定します。

●設定内容	特定のアクセス元から、sshサーバ(22/tcp) へのリモートログインを許可する 不特定のアクセス元に対して、Webサーバ(80/tcp) への接続を許可する 上記以外のアクセスを遮断する

※主要分のみ/詳細は次頁



【仮想ルータ】の役割
IaaSの仮想ルータは、外部ネットワークと内部ネットワーク、内部ネットワーク同士を接続し、ネットワーク間で通信できるようにするルーティングや、不適切なアクセスを防ぐファイアーウォール等の役割を受け持っています。

【ファイアーウォール】と【セキュリティグループ】の違い
仮想ルータのファイアーウォールでは、①送信元/送信先IPアドレス、②送信元/送信先プロトコル、③アクセス制御内容(許可/拒否)を設定できます。セキュリティグループは、許可する通信を設定するのに対して、ファイアーウォールでは拒否する通信も設定可能です。

実装作業④ 仮想ルータ (2/2)

④-2 ファイアーウォールの設定例

※ファイアーウォールの設定例

ルール名称	アクション	接続元IPアドレス	接続元ポート番号	接続先IPアドレス	接続先ポート番号	AZ
ssh_ok	許可	x.x.x.x/32	–	(**構築時**) y.y.y.0/24 (**完了時**) y.y.y.Y/32	22	jp-east-1a
http_ok	許可	(**構築時**) x.x.x.x/32 (**完了時**) 0.0.0.0/0	–	(**構築時**) y.y.y.0/24 (**完了時**) y.y.y.Y/32	80	jp-east-1a
dns_ok	許可	–	–	0.0.0.0/0	53	jp-east-1a
ntp_ok	許可	–	–	0.0.0.0/0	123	jp-east-1a
all_ng	拒否	–	–	–	–	jp-east-1a

●仮想サーバのIPアドレスは、デフォルトでは配備するまで不定です。そのため、構築時は、サブネットのIPアドレスを設定してください。
●完了時に、仮想サーバのIPアドレスを設定してください。

● 東日本リージョンのAZを示します。
AZ1: jp-east-1a
AZ2: jp-east-1b

●ファイアーウォールのルールを設定すると、ルール以外のパケットはすべて拒否になります。
●そのため、上記の “all_ng” は、設定しなくても、機能的にはファイアーウォールで自動的に設定されます。
●ただし、設定項目の管理上で、上記のように “all_ng” を明示的に入れておくことは問題ありません。

●IPアドレスを設定する際は、CIDR形式で設定します。
●システムの構築時は、不特定のアクセス元からWebサーバにアクセスされないよう、特定のアクセス元のみ「許可」としておきます。
●システム構築の完了時に、不特定のアクセス元 (0.0.0.0/0) からWebサーバにアクセスできるよう、ルールを設定します。
●その他、セキュリティの考え方については『**参考：セキュリティグループとファイアーウォールの概略**』等を参照してください。

実装作業⑤ ネットワーク接続

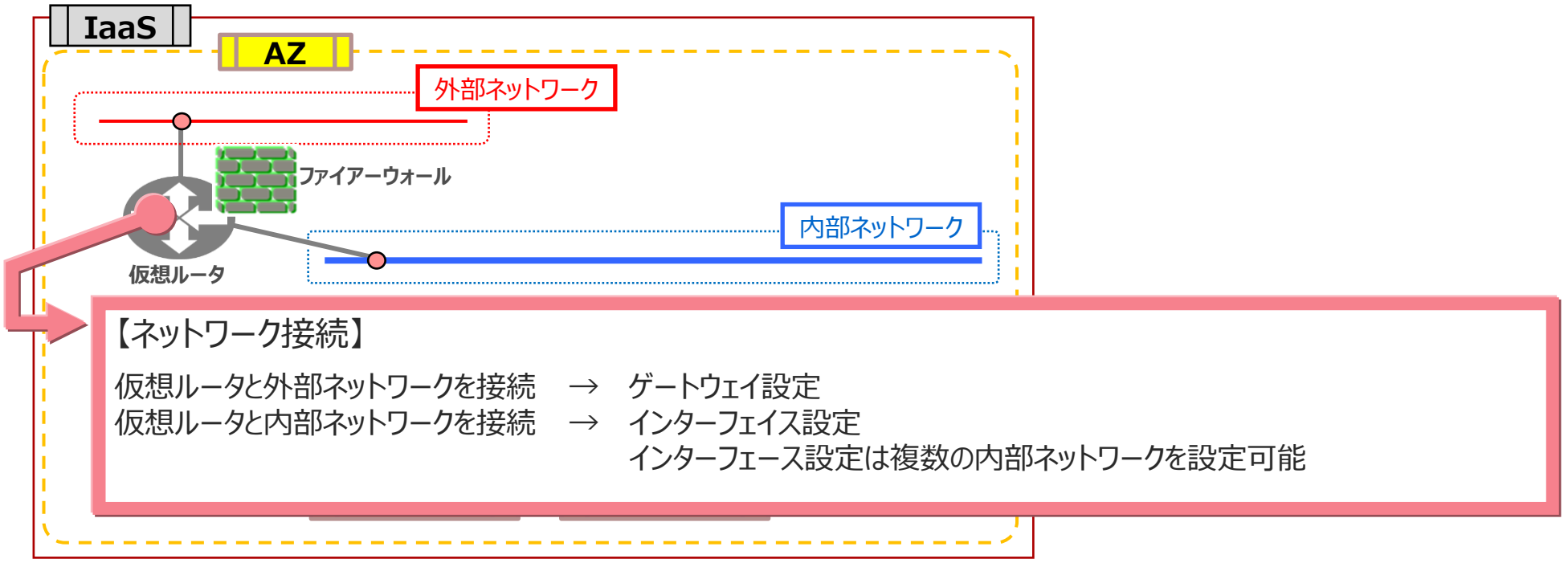
⑤　仮想ルータをネットワークに接続

作成した仮想ルータを、外部ネットワークと内部ネットワークに接続します。

外部ネットワークに接続するには、仮想ルータの ゲートウェイ設定 で外部ネットワークを接続します。

内部ネットワークに接続するには、仮想ルータの インターフェース設定 で内部ネットワークを接続します。
インターフェース設定では、複数の内部ネットワークを接続可能です。(複数接続の例は 1-2⑤を参照)

1つの仮想ルータで、ゲートウェイ設定、インターフェース設定で接続したネットワーク同士は、特に追加の設定をしないで、
それぞれのネットワーク同士と通信可能です。



実装作業⑥ 仮想サーバ (1/2)

⑥-1　仮想サーバへのログイン用のキーペアを作成

ネットワークの設定後、仮想サーバを作成します。

まず、仮想サーバ作成の準備として、仮想サーバへログインする際に使用する キーペア を作成します。
キーペアは、*.pem という名称になります。

作成したキーペアの利用

作成したキーペアは、1-1⑦で仮想サーバにログインする際に利用します。

仮想サーバが Linux系OS の場合は、Tera Term　等の sshクライアントを用いて、
作成したキーペアの鍵ファイル *.pem を利用する設定をして仮想サーバに sshでログインします。

Windowsの場合は 作成したキーペアの鍵ファイル *.pem を利用して、IaaSが発行したランダムな
管理者ユーザーパスワードを取得し、そのパスワードで仮想サーバにリモートデスクトップでログインします。

キーペアの管理

作成したキーペアは、厳重に保管/管理してください。

- キーペアを紛失した場合

  キーペアを紛失すると、そのキーペアを割り当てた仮想サーバにログインできなくなります。
  また、キーペアは再発行できません。そのため、新たにキーペアを作成して、仮想サーバを再度作成することとなります。

- キーペアが漏えいした場合

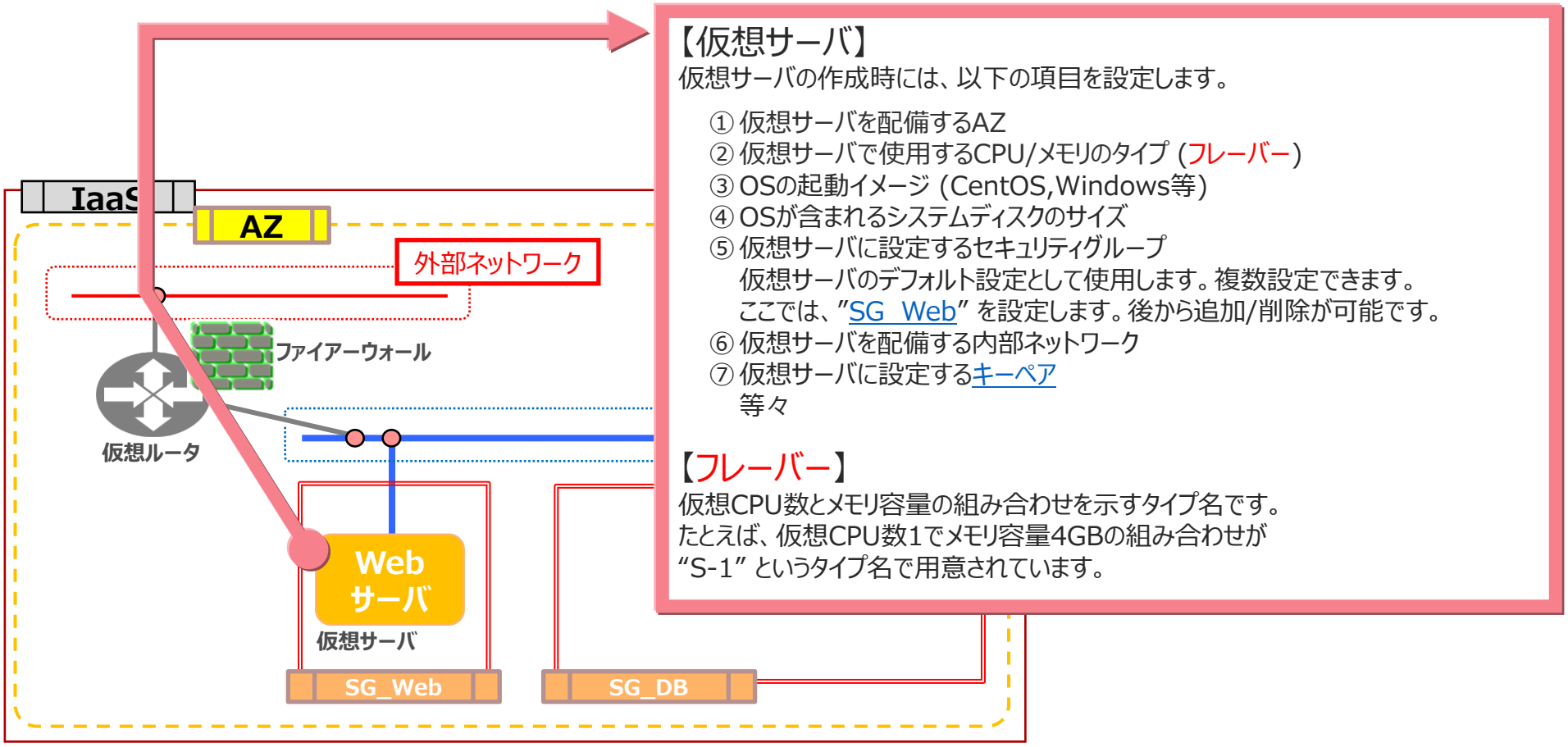
  キーペアが漏えいすると、そのキーペアで仮想サーバに不正にアクセスされる可能性があります。

実装作業⑥ 仮想サーバ (2/2)

⑥-2 仮想サーバを作成

仮想サーバを作成します。

この構成では、Linux系OS で作成します。(1-1③、1-1④で、sshでログインする設定にしています。)



【仮想サーバ】
仮想サーバの作成時には、以下の項目を設定します。

① 仮想サーバを配備するAZ
② 仮想サーバで使用するCPU/メモリのタイプ (フレーバー)
③ OSの起動イメージ (CentOS,Windows等)
④ OSが含まれるシステムディスクのサイズ
⑤ 仮想サーバに設定するセキュリティグループ
仮想サーバのデフォルト設定として使用します。複数設定できます。
ここでは、"SG_Web" を設定します。後から追加/削除が可能です。
⑥ 仮想サーバを配備する内部ネットワーク
⑦ 仮想サーバに設定するキーペア
等々

【フレーバー】
仮想CPU数とメモリ容量の組み合わせを示すタイプ名です。
たとえば、仮想CPU数1でメモリ容量4GBの組み合わせが
"S-1" というタイプ名で用意されています。

実装作業⑦ 仮想サーバにグローバルIPアドレスを設定

⑦　仮想サーバにグローバルIPアドレスを設定

仮想サーバが作成できたら、仮想サーバにグローバルIPアドレスを割り当てます。

仮想サーバにグローバルIPアドレスを割り当てた後、数分すると、
その仮想サーバにインターネットからログインできるようになります。

【ログイン】
仮想サーバにログインできることを確認します。

※　仮想サーバが Linux系の場合には、sshクライアント側で、
キーペア (*.pem) を利用する設定をして仮想サーバにログインしてください。

※　仮想サーバが Windowsの場合は、設定したキーペアの鍵ファイルを
利用して、管理者パスワードを入手してログインしてください。

仮想サーバの作成時に、キーペアを設定しなかった、あるいはキーペアの
ファイルを紛失した場合は、その仮想サーバにはログインできません。
仮想サーバを再作成してください。

【グローバルIPアドレスを割当】
作成した仮想サーバに、1-1②で確保したグローバルIPアドレスを割り当てます。

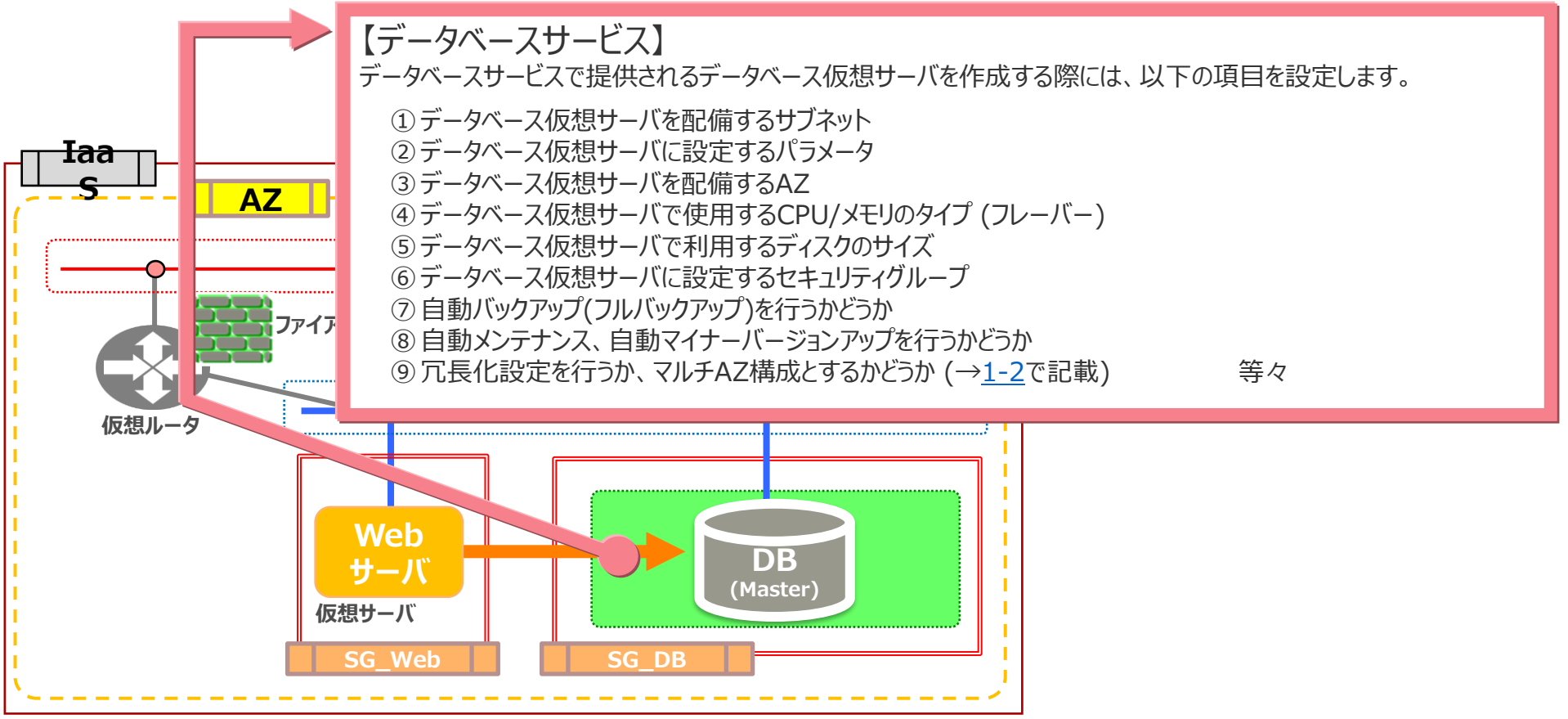
※ 正確には、グローバルIPアドレスは、仮想ルータ上で NAT機能によって、
仮想サーバのプライベートIPアドレスに割り当てられます。

実装作業⑧ データベースサービス

⑧　データベースサービスを配備

データベースを自前で構築しないで利用可能なデータベースサービスが用意されています。
データベースサービスを利用すると、手間のかかる構築/運用を IaaSサービス側に任せることができます。
利用者は、業務アプリケーションの開発に注力できるようになります。

この構成のデータベースサービスは、PostgreSQL ver9.2.4互換です。

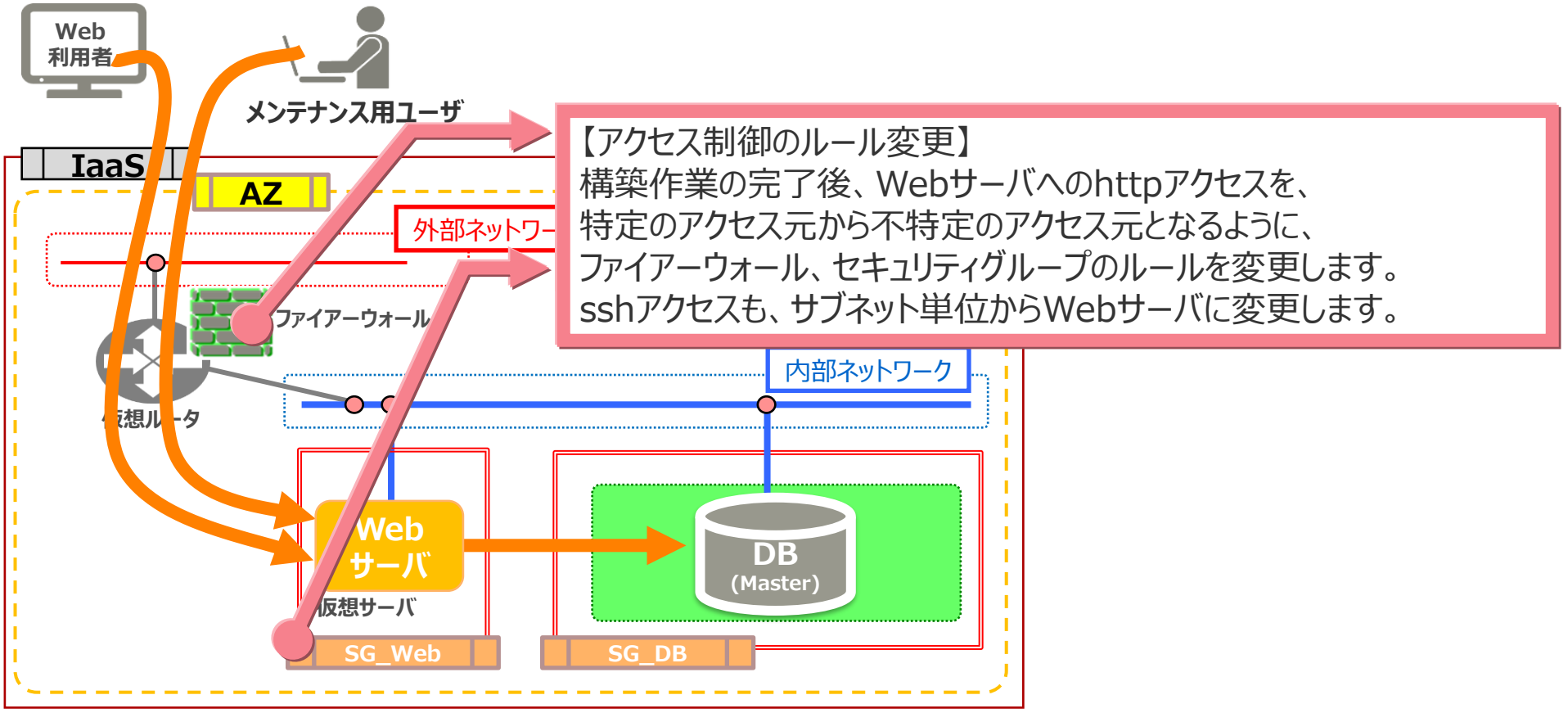


実装作業⑨ アクセス制御

⑨　すべての作業が終わったら、FW/SGのアクセス制御を変更してインターネットに公開

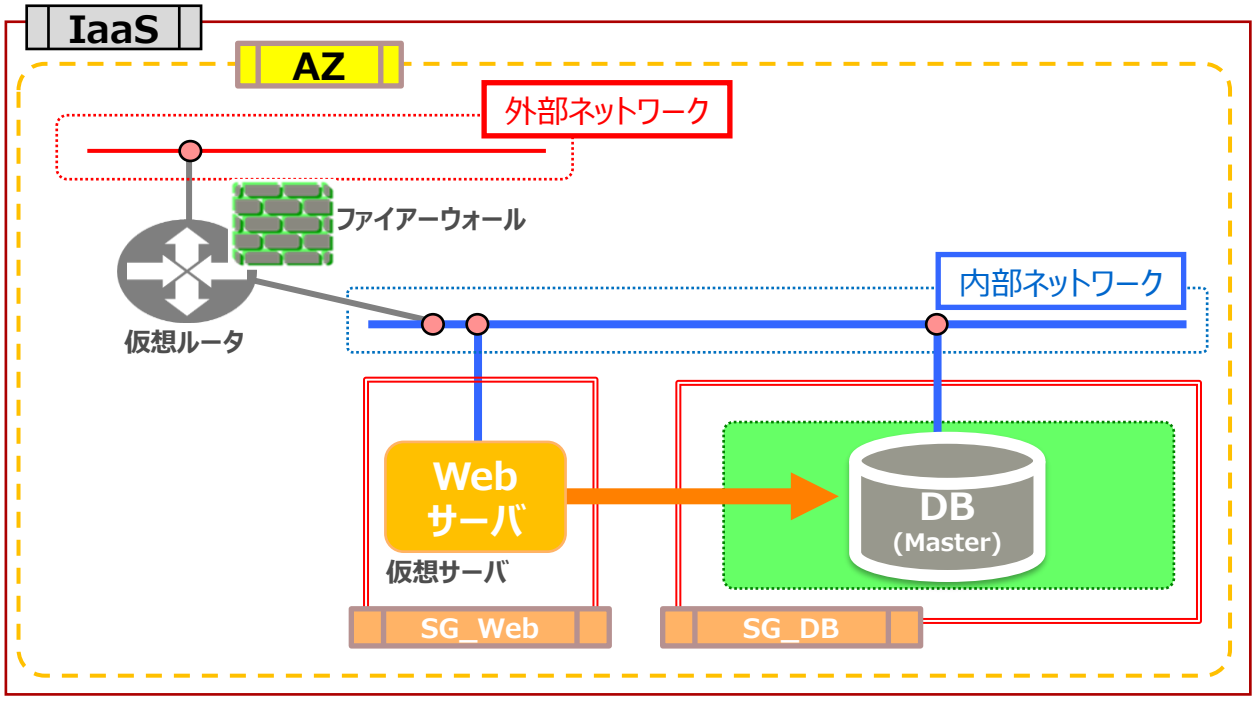
仮想サーバの構築作業、データベース仮想サーバの設定作業などが終わりましたら、FW/SGのアクセス制御を変更します。

Webサーバ(80/tcp)へのアクセスを、不特定のアクセス元から接続可能になるよう変更します。



実装作業まとめ

- 以上の実装手順で、Web/DBのシンプルな構成をIaaS上に配備できます。
- 1-1の構成では、1つの AZ に仮想サーバとデータベースを 1台ずつ配備していますので、トラブルを考慮した構成や性能を考慮した構成ではありません。どこかが停止すれば、業務もその時点で停止する恐れがあります。
- 1-2では、仮想サーバを複数作成し、さらに複数のAZを使い、トラブルがあっても業務を継続できるマルチAZ構成の実装方法を記載します。



1-2. Web/DBマルチAZ構成

① 内部ネットワークを作成し、サブネットを設定
② 仮想サーバに割り当てる グローバルIPアドレス を確保
③ セキュリティグループを設定
④ 仮想ルータを作成し、仮想ルータにファイアーウォールを設定
⑤ 仮想ルータをネットワークに接続
⑥ ネットワークコネクター、コネクターエンドポイントを配備
⑦ サブネットにルーティング情報を設定
⑧ 仮想サーバを作成
⑨ 仮想サーバにグローバルIPアドレスを設定
⑩ ロードバランサーを配備
⑪ データベースサービスを配備
⑫ すべての作業が終わったら、ファイアーウォール/セキュリティグループのアクセス制御を変更してインターネットに公開

本章で例示するシステムの構成と、本章で説明する機能

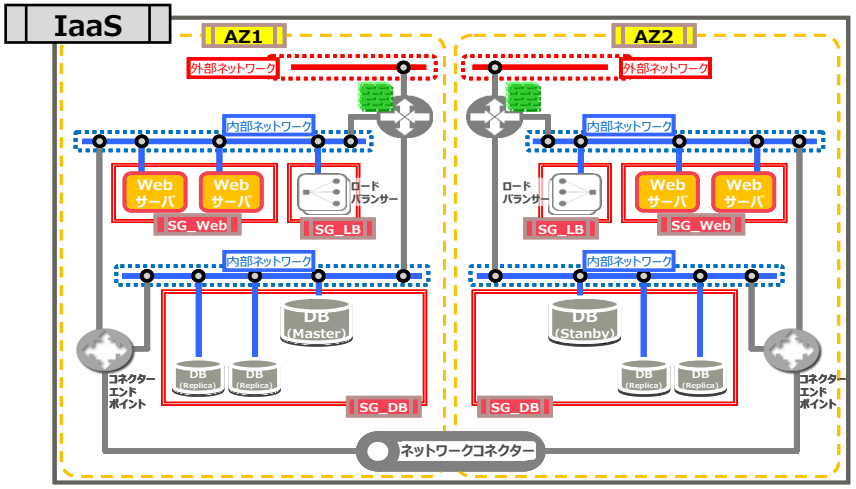
本章では、IaaSでとりうる可用性や性能向上の考え方を盛り込んだ構成の実装を記載しながら、
以下の IaaSの機能を説明していきます。

(1) 本章で例示するシステム構成の概要　※1-1の構成からの変更点

- 物理環境が異なるAZを2つ使用し、AZ間を内部で接続
- WebサーバとDBサーバを配備するネットワークを分離
- Webサーバ用に、ロードバランサーを配備 (ロードバランサーは80/tcpで待ち受け、Webサーバは81/tcpで待ち受けとする)
- Webサーバを AZごとに 2台配備
- DBサーバを運用待機構成 (Master/Standby) で構成
- DBサーバに参照時の負荷を分散するリードレプリカを設定

(2) 本章で説明する IaaSの機能

- マルチAZ構成
- ネットワークコネクター (NWC)
- コネクターエンドポイント (CEP)
- ロードバランサー (LB)
- データベースサービス
  運用待機構成/リードレプリカ



本章で記載する実装作業の段取り

本章で記載する実装作業の段取りは以下のとおりです。

(3) 実装作業の段取り

作業内容	
①	内部ネットワークを作成し、サブネットを設定
②	仮想サーバに割り当てる グローバルIPアドレス を確保
③	セキュリティグループを設定
④	仮想ルータを作成し、仮想ルータにファイアーウォールを設定
⑤	仮想ルータをネットワークに接続
⑥	ネットワークコネクター、コネクターエンドポイントを配備
⑦	サブネットにルーティング情報を設定
⑧	仮想サーバを作成
⑨	仮想サーバにグローバルIPアドレスを設定
⑩	ロードバランサーを配備
⑪	データベースサービスを配備
⑫	すべての作業が終わったら、ファイアーウォール/セキュリティグループのアクセス制御を変更してインターネットに公開

実装作業① 内部ネットワーク、サブネット

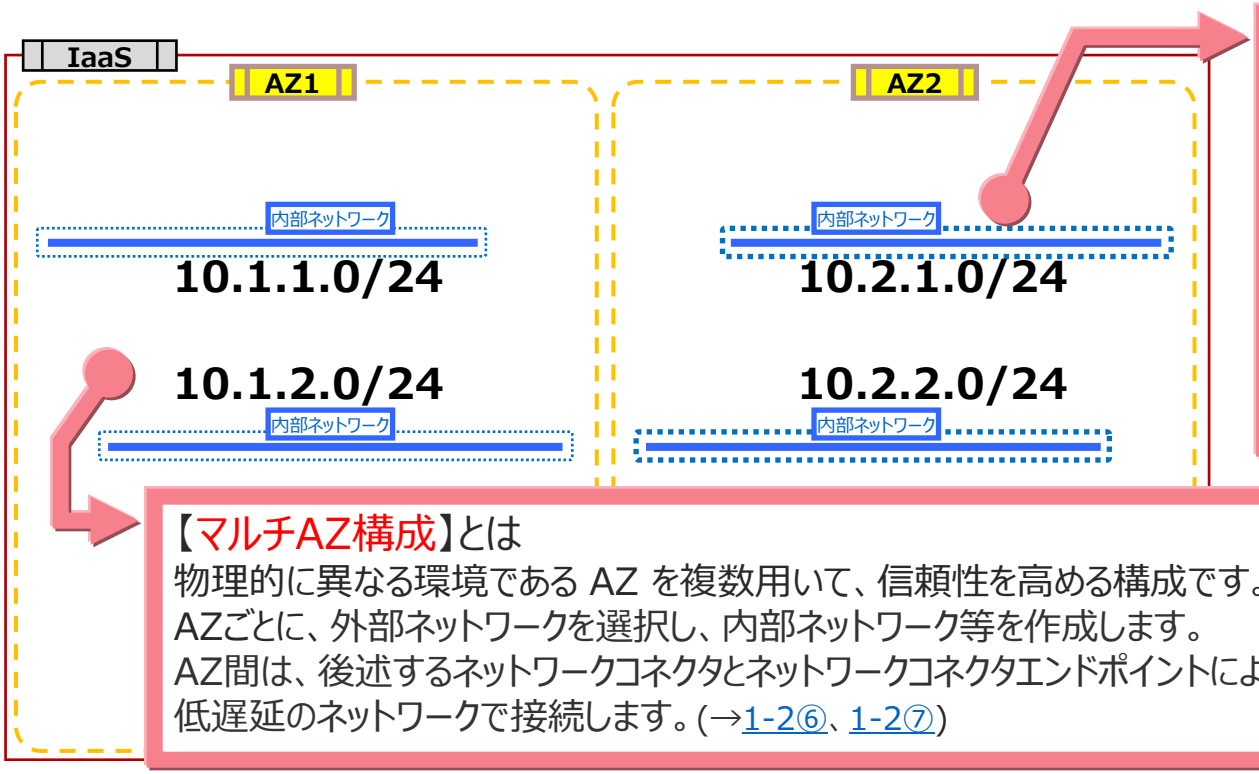
① 内部ネットワークを作成し、サブネットを設定

まず始めに、仮想サーバ等を配備する『内部ネットワーク』を 異なる アベイラビリティゾーン (以下AZ) ごとに作成します。

1-2構成では、ロードバランサー、Webサーバ用の内部ネットワークと、DBサーバ用の内部ネットワークを別々に作成し、
それぞれのサブネットを設定します。この例では、サブネットはそれぞれ図中の値で設定します。

IaaSのサブネットの設定項目とその考え方については、1-1①-2 を参照してください。

マルチAZ構成では、それぞれのサブネットに、通信したい別AZのサブネットへのルーティング情報を設定します。(1-2⑦に記載)



【サブネット】
1-2構成では、以下のように設定します。

- ロードバランサー、Webサーバ用
  AZ1　10.1.1.0/24
  AZ2　10.2.1.0/24
- データベースサービス用
  AZ1　10.1.2.0/24
  AZ2　10.2.2.0/24

【マルチAZ構成】とは
物理的に異なる環境である AZ を複数用いて、信頼性を高める構成です。
AZごとに、外部ネットワークを選択し、内部ネットワーク等を作成します。
AZ間は、後述するネットワークコネクタとネットワークコネクタエンドポイントにより、
低遅延のネットワークで接続します。(→1-2⑥、1-2⑦)

実装作業② グローバルIPアドレス

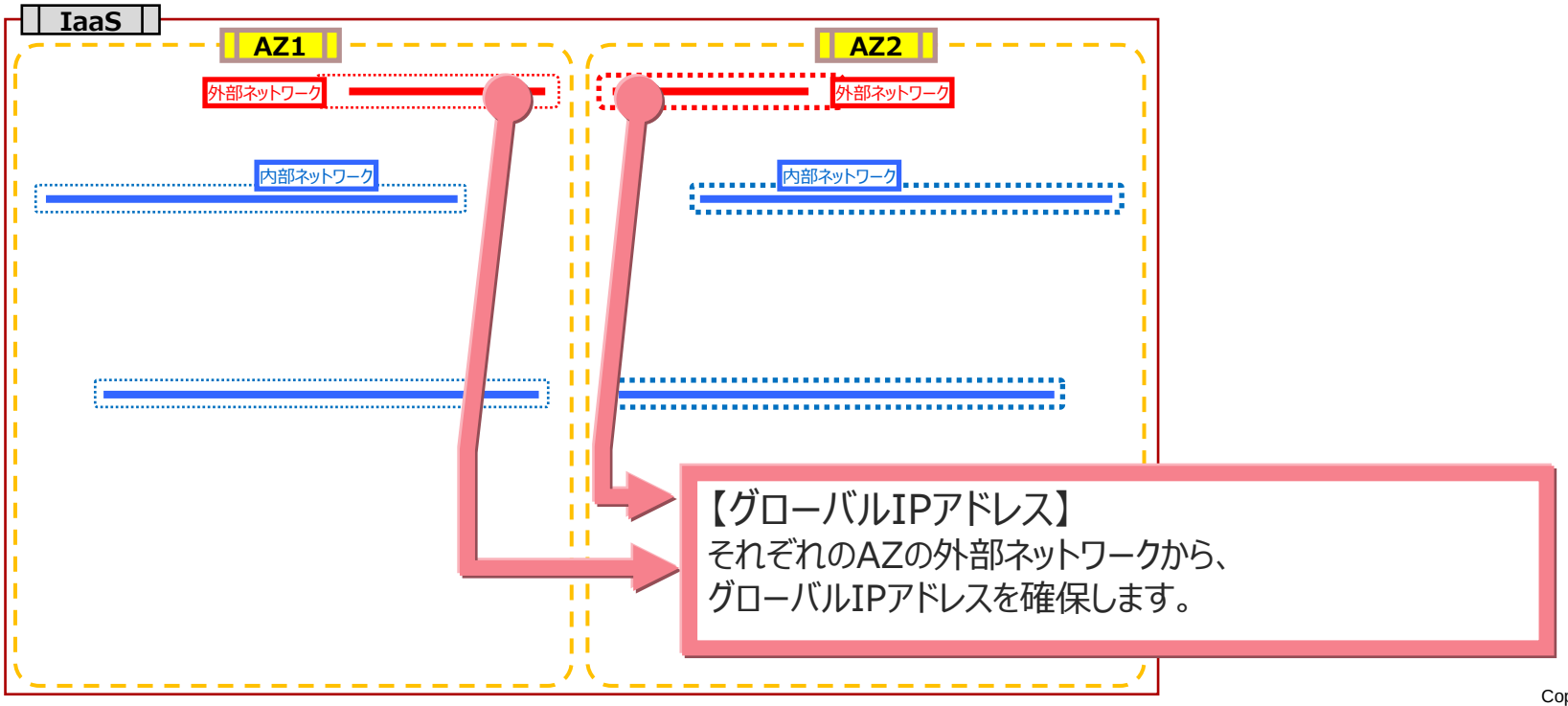
②　仮想サーバに割り当てる グローバルIPアドレス を確保

1-1の構成と同じように、仮想サーバにログインするためにグローバルIPアドレスを確保します。
1-1の構成では、仮想サーバは 1台でしたが、1-2の構成では AZごとに 2台ずつで計4台の仮想サーバを配備します。

ここでは、AZごとに 仮想サーバ1台を sshログイン用のサーバと兼務することとします。

なお、各AZごとのsshログイン用の仮想サーバからその他の各仮想サーバにログインできるため、すべての仮想サーバにsshログイン用のグローバルIPアドレスを割り当てる必要はありません。AZの障害を考慮して、各AZで1台をssh用のログインサーバとします。

それぞれの外部ネットワークから、グローバルIPアドレスを 1つずつ確保します。

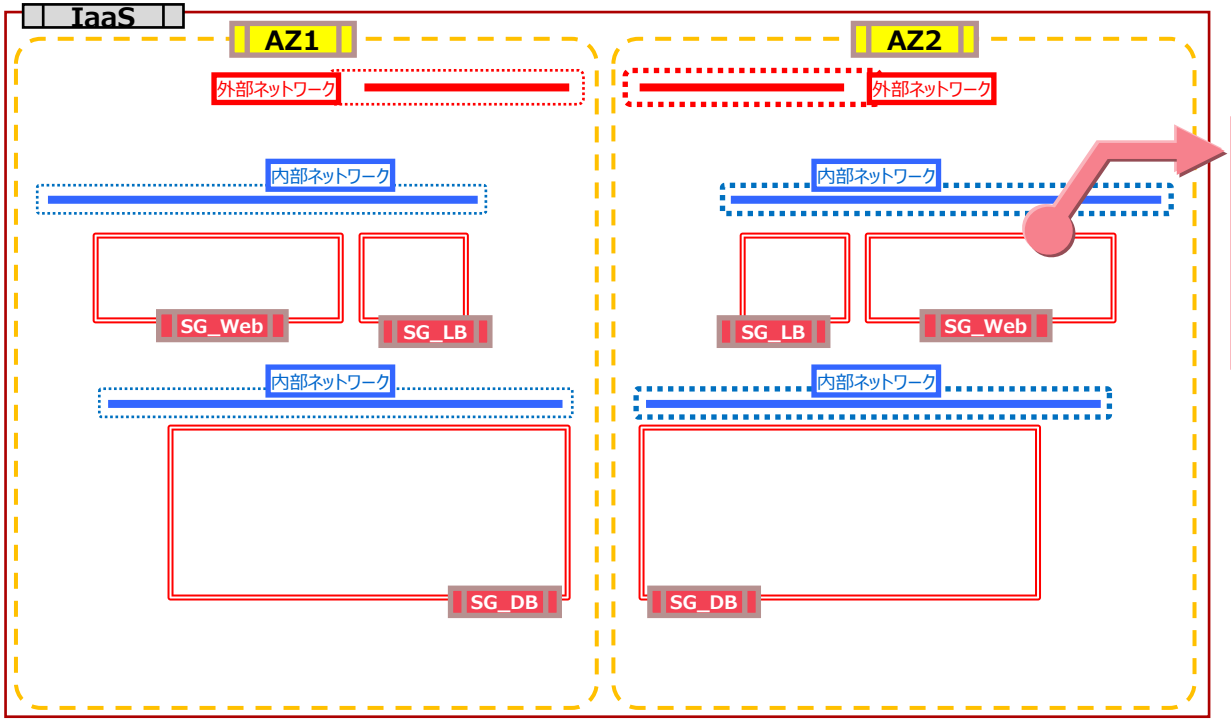


実装作業③ セキュリティグループ (1/3)

③-1 セキュリティグループを設定

マルチAZ構成のセキュリティグループでは、1-1の構成のセキュリティグループを変更し、1-2⑩ロードバランサー用のセキュリティグループ “**SG_LB**” と、1-2⑨で仮想サーバへログインを許可する “**SG_Gate**” を作成します。

●SG_LB	不特定のアクセス元 (構築時は特定のアクセス元) に対して、ロードバランサー(80/tcp) への接続を許可する セキュリティグループ “SG_Web” に対して、81/tcp への接続を許可する。
●SG_Web	セキュリティグループ “SG_LB” が設定されたロードバランサーから、 Webサーバ(81/tcp) への接続を許可する セキュリティグループ “SG_DB” に対して、DBサーバ(5432/tcp) への接続を許可する ※主要分のみ／詳細は次頁
●SG_DB	セキュリティグループ “SG_Web” が設定された仮想サーバから、DBサーバ(5432/tcp) への接続を許可する
●SG_Gate	特定のアクセス元から、sshサーバ(22/tcp) へのリモートログインを許可する



【セキュリティグループ】
セキュリティグループを設定してください。
セキュリティグループは、AZ間で共通で使用可能です。

実装作業③ セキュリティグループ (2/3)

③-2 セキュリティグループ 設定例

※SG_LBの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	80	CIDR	(構築時) x.x.x.x/32 (完了時) 0.0.0.0/0	-
カスタムTCPルール	送信	ポート	81	セキュリティグループ	SG_Web	-

●システムの構築時は、不特定のアクセス元からWebサーバにアクセスされないよう、特定のアクセス元としておきます。
●システム構築の完了時に、不特定のアクセス元 (0.0.0.0/0) からロードバランサーにアクセスできるよう、ルールを設定します。

※SG_Webの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	22	セキュリティグループ	SG_Gate	IPv4
カスタムTCPルール	受信	ポート	81	セキュリティグループ	SG_LB	IPv4
カスタムTCPルール	送信	ポート	5432	セキュリティグループ	SG_DB	IPv4
カスタムTCPルール	送信	ポート	80	CIDR	169.254.169.254/32	-
カスタムTCPルール	送信	ポート	53	CIDR	0.0.0.0/0	-
カスタムUDPルール	送信	ポート	53	CIDR	0.0.0.0/0	-
カスタムTCPルール	送信	ポート	123	CIDR	0.0.0.0/0	-
カスタムUDPルール	送信	ポート	123	CIDR	0.0.0.0/0	-

●セキュリティグループの “SG_Gate“ を設定する仮想サーバから、sshログインできるよう、22/tcp への受信を許可します。
●セキュリティグループの “SG_LB“ を設定するロードバランサーから、81/tcp へのアクセスを許可します。
●セキュリティグループの “SG_DB“ を設定するデータベースへ、5432/tcp へのアクセスを許可します。
●169.254.169.254/32 は、キーペア等の仮想サーバが必要な情報を仮想サーバに提供する特別なIPアドレスです。
セキュリティを厳しくする場合にも、必ず169.254.169.254/32への送信を許可する設定は入れてください。
●その他、セキュリティの考え方については『**参考：セキュリティグループとファイアーウォールの概略**』等を参照してください。

実装作業③ セキュリティグループ (3/3)

③-3 セキュリティグループ “SG_DB” 設定例

※SG_DBの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	5432	セキュリティグループ	SG_Web	-
カスタムTCPルール	送信	ポート	5432	セキュリティグループ	SG_DB	-
カスタムTCPルール	受信	ポート	5432	セキュリティグループ	SG_DB	-

●セキュリティグループの “SG_Web” が設定された仮想サーバ (Webサーバ) からの受信を許可します。
●セキュリティグループの “SG_DB” を設定するデータベースサービスで、データベースのポート番号に対して送受信を許可します。

※SG_Gateの設定例

ルール	方向	オープンポート	ポート	接続先	セキュリティグループ/CIDR	Ethernetタイプ
カスタムTCPルール	受信	ポート	22	CIDR	x.x.x.x/32	-
カスタムTCPルール	送信	ポート	22	セキュリティグループ	SG_Web	IPv4

●特定のアクセス元から ssh ログインできるよう、22/tcp への受信を許可します。
●セキュリティグループの “SG_Web” が設定された仮想サーバ (Webサーバ) への ssh接続を許可します。
●仮想サーバのうち、各AZごとに 1台ずつ、このセキュリティグループを設定します。

実装作業④ 仮想ルータ (1/3)

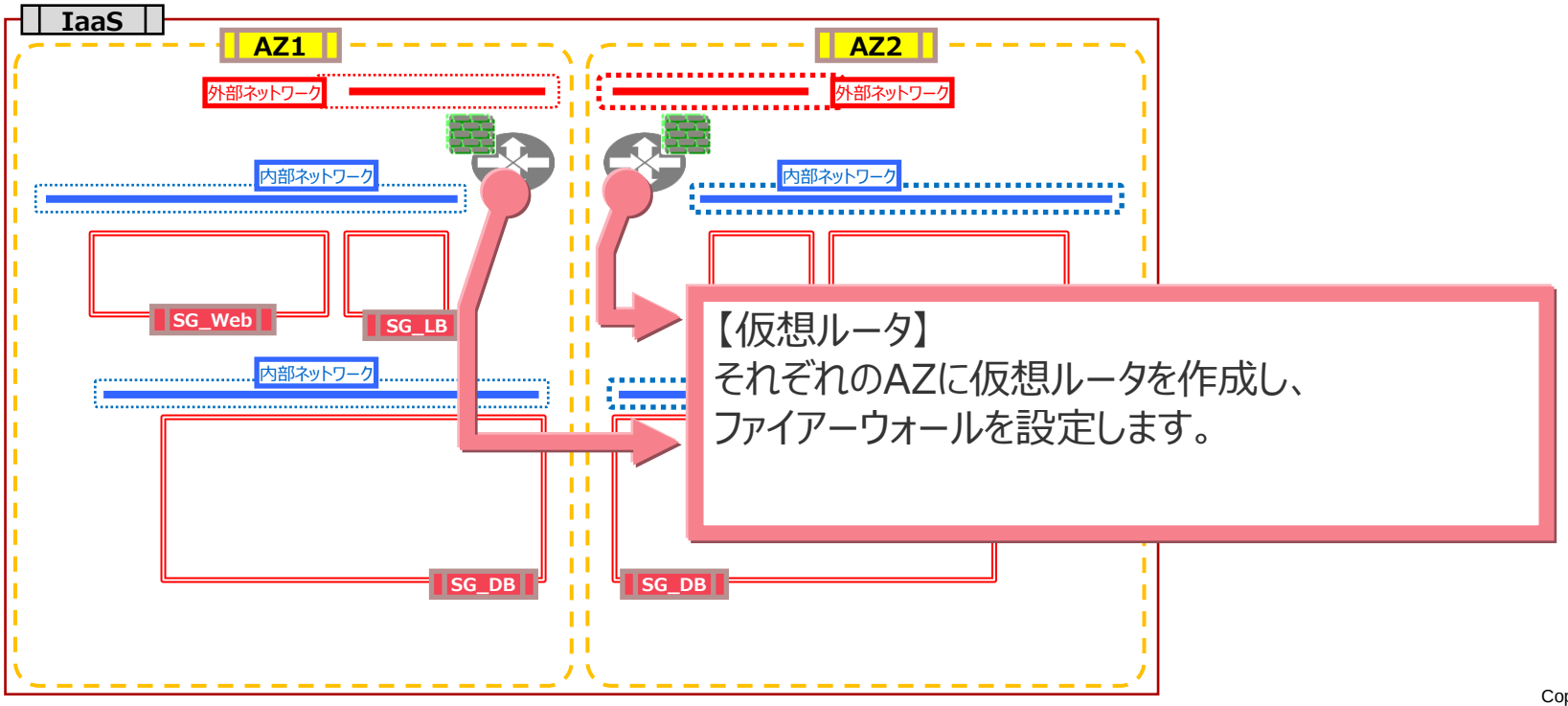
④-1　仮想ルータを作成し、ファイアーウォール機能を設定

内部ネットワークと外部ネットワークを接続し、内部ネットワークに配備する仮想サーバ等をインターネットと通信できるようにするために、内部ネットワークを配備した それぞれの AZに仮想ルータを作成します。

仮想ルータには、従来からの一般的なセキュリティの機能であるファイアーウォール機能が含まれます。
セキュリティは多層防御が推奨されますので、セキュリティグループとあわせてファイアーウォールも設定します。

●設定内容	特定のアクセス元から、sshサーバ(22/tcp) へのリモートログインを許可する 不特定のアクセス元に対して、ロードバランサー(80/tcp) への接続を許可する 上記以外のアクセスを遮断する

※主要分のみ/詳細は次頁



実装作業④ 仮想ルータ (2/3)

④-2 AZ1側ファイアーウォールの設定例

●仮想サーバのIPアドレスは、デフォルトでは配備するまで不定です。そのため、構築時は、サブネットのIPアドレスを設定してください。
●完了時に、仮想サーバのIPアドレスを設定してください。

ルール名称	アクション	接続元IPアドレス	接続元ポート番号	接続先IPアドレス	接続先ポート番号	AZ
ssh_ok	許可	x.x.x.x/32	–	(構築時) 10.1.1.0/24 (完了時) 10.1.1.y/32	22	jp-east-1a
http_ok	許可	(構築時) x.x.x.x/32 (完了時) 0.0.0.0/0	–	10.1.1.0/24	80	jp-east-1a
db_ok	許可	10.1.1.0/24	–	10.1.2.0/24	5432	jp-east-1a
dns_ok	許可	–		0.0.0.0/0	53	jp-east-1a
ntp_ok	許可	–	–	0.0.0.0/0	123	jp-east-1a
all_ng	拒否	–	–	–	–	jp-east-1a

●1-2①で設定した、AZ1側でロードバランサーを配備するサブネットです。

●1-2①で設定した、AZ1側でデータベースを配備するサブネットです。

●ロードバランサーとデータベースは、割り当てられるIPアドレスが不定です。(サブネット内で空きのIPアドレスが割り当てられます)
また、メンテナンス時に、ロードバランサーやデータベースに割り当てられていたIPアドレスが変更される可能性があります。
そのため、ロードバランサー用とデータベース用のFWルールでは、それぞれを配備するサブネットを指定してください。
●ロードバランサーのグローバルIPアドレスは、ファイアーウォールのルールでは設定不要です。
ロードバランサーに割り当てられたグローバルIPアドレスは、同じくロードバランサーに割り当てられた内部のサブネットのIPアドレスと、仮想ルータのNAT機能により自動的に対応づけられます。

実装作業④ 仮想ルータ (3/3)

FUJITSU

④-3 AZ2側ファイアーウォールの設定例

●仮想サーバのIPアドレスは、デフォルトでは配備するまで不定です。そのため、構築時は、サブネットのIPアドレスを設定してください。
●完了時に、仮想サーバのIPアドレスを設定してください。

ルール名称	アクション	接続元IPアドレス	接続元ポート番号	接続先IPアドレス	接続先ポート番号	AZ
ssh_ok	許可	x.x.x.x/32	–	(構築時) 10.2.1.0/24 (完了時) 10.2.1.z/32	22	jp-east-1b
http_ok	許可	(構築時) x.x.x.x/32 (完了時) 0.0.0.0/0	–	10.2.1.0/24	80	jp-east-1b
db_ok	許可	10.2.1.0/24	–	10.2.2.0/24	5432	jp-east-1b
dns_ok	許可	–		0.0.0.0/0	53	jp-east-1b
ntp_ok	許可	–	–	0.0.0.0/0	123	jp-east-1b
all_ng	拒否	–	–	–	–	jp-east-1b

●1-2①で設定した、AZ2側でロードバランサーを配備するサブネットです。

●1-2①で設定した、AZ2側でデータベースを配備するサブネットです。

●ロードバランサーとデータベースは、割り当てられるIPアドレスが不定です。(サブネット内で空きのIPアドレスが割り当てられます)
また、メンテナンス時に、ロードバランサーやデータベースに割り当てられていたIPアドレスが変更される可能性があります。
そのため、ロードバランサー用とデータベース用のFWルールでは、それぞれを配備するサブネットを指定してください。
●ロードバランサーのグローバルIPアドレスは、ファイアーウォールのルールでは設定不要です。
ロードバランサーに割り当てられたグローバルIPアドレスは、同じくロードバランサーに割り当てられた内部のサブネットのIPアドレスと、仮想ルータのNAT機能により自動的に対応づけられます。

実装作業⑤ ネットワーク接続

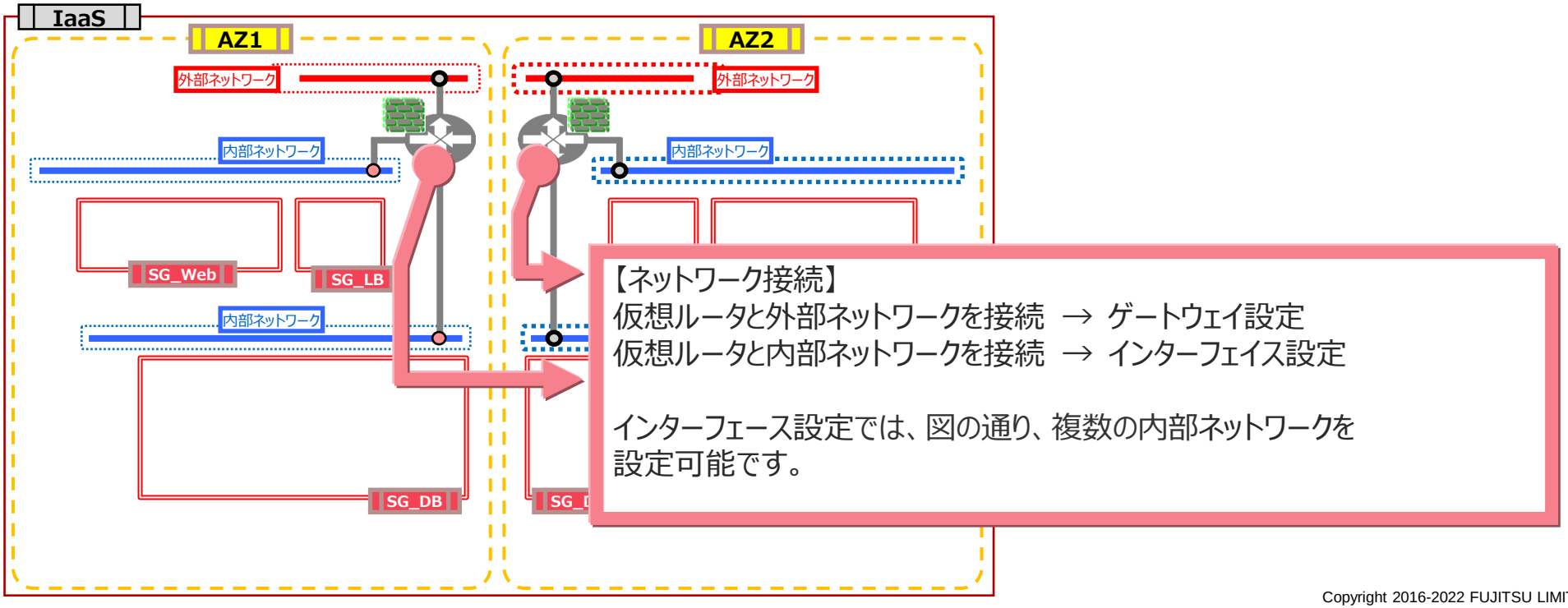
⑤　仮想ルータをネットワークに接続

作成した仮想ルータを、外部ネットワークと内部ネットワークに接続します。

外部ネットワークに接続するには、仮想ルータの ゲートウェイ設定 で外部ネットワークを接続します。

内部ネットワークに接続するには、仮想ルータの インターフェース設定 で内部ネットワークを接続します。
インターフェース設定では、複数の内部ネットワークを接続可能です。

1つの仮想ルータで、ゲートウェイ設定、インターフェース設定で接続したネットワーク同士は、特に追加の設定をしないで、
それぞれのネットワーク同士と通信可能です。

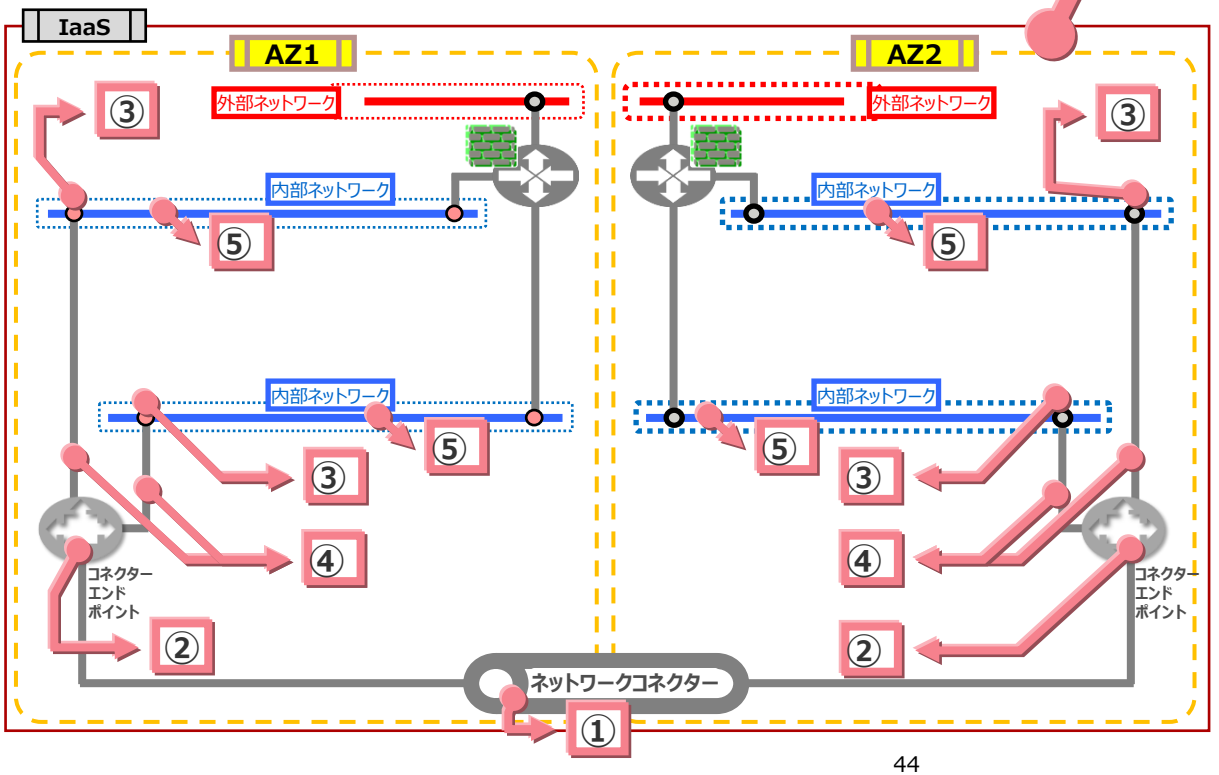


実装作業⑥ ネットワークコネクター、コネクターエンドポイント

⑥　ネットワークコネクター、コネクターエンドポイントを配備

それぞれのAZのネットワークの設定の完了後、AZ間を接続するためのネットワークコネクターとコネクターエンドポイントを作成して配備します。AZ間の接続は、以下の作業を行います。

①AZ間に、ネットワークコネクター を作成
②それぞれのAZ内に、コネクターエンドポイント を作成
③それぞれのAZ内で、コネクターエンドポイントをサブネットと接続する (コネクターエンドポイントにIPアドレスを付与する) ための
　　ポート を作成 (この場合の “ポート” は、1-1③の参考資料の機能配置図に記載のポートを指します)
④それぞれのAZ内で、コネクターエンドポイントにポートを割り当て
⑤それぞれのサブネットにルーティング情報を追加　(→1-2⑦)



【ネットワークコネクター】と
【コネクターエンドポイント】
AZ内のネットワークを接続する仮想ルータに対して、ネットワークコネクターとコネクターエンドポイントは、AZを超えたネットワーク同士を接続するための機能を提供します。

ネットワークコネクターは、AZ間に作成します。
コネクターエンドポイントは、AZ内に作成します。

仮想ルータのようにネットワークを接続しますが、以下のように差異があります。

- ネットワークコネクターには、ファイアーウォール機能はありません。
- ネットワークコネクター経由で通信をする場合は、ルーティング情報を手動でサブネットに設定します。（→設定内容は⑦-1、⑦-2に例示）
  ルーティング情報を設定しないと、サブネットに定義されたデフォルトゲートウェイ宛てにすべての通信が向かってしまい、AZ間の通信ができません。

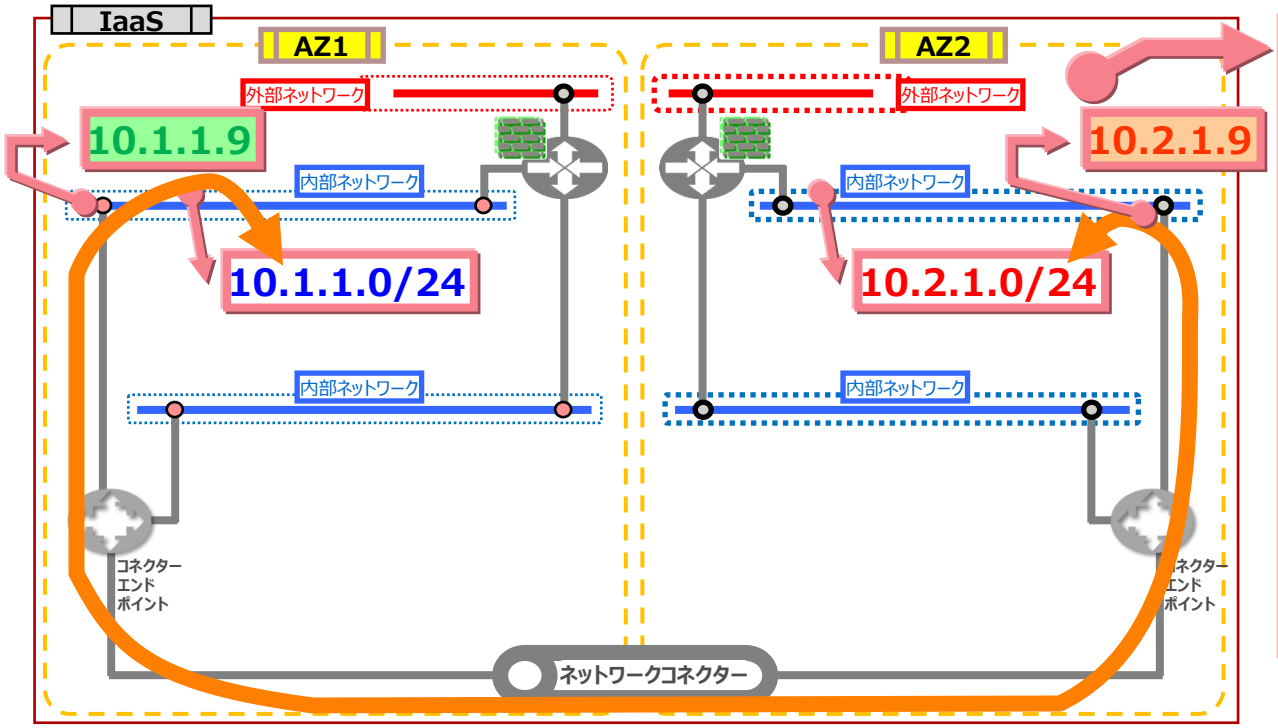
実装作業⑦ ルーティング情報 (1/2)

⑦-1 サブネットにルーティング情報を設定

ネットワークコネクターとコネクターエンドポイントで接続されたサブネットに対して、各々のサブネットと通信できるよう、
ルーティング情報をサブネットに設定します。

ルーティング情報の設定内容は、たとえば、
『AZ1 の **10.1.1.0/24** の サブネットから AZ2 の **10.2.1.0/24** のサブネットに通信する際の経路は、**10.1.1.9** とする 』

というように、AZ間をまたぐ通信を設定します。また、以下のように、行きと帰りの経路が同一になるように設定します。
『AZ1 の **10.2.1.0/24** の サブネットから AZ2 の **10.1.1.0/24** のサブネットに通信する際の経路は、**10.2.1.9** とする 』



【サブネットにルーティングを設定】
サブネットにルーティングを設定するというのは、OpenStack由来の概念です。

サブネットにルーティングを設定しておくことで、仮想サーバが起動する際に、仮想サーバは、自分が属するサブネットからルーティング情報を取得します。

オンプレミスでは、複数ネットワークに接続されたサーバのルーティングはサーバに個別に設定する手間がありましたが、OpenStackはそういった手間を無くし、サブネット単位でルーティングを一括設定できるよう効率化されています。
※仮想サーバの再起動が必要

実装作業⑦ ルーティング情報 (1/2)

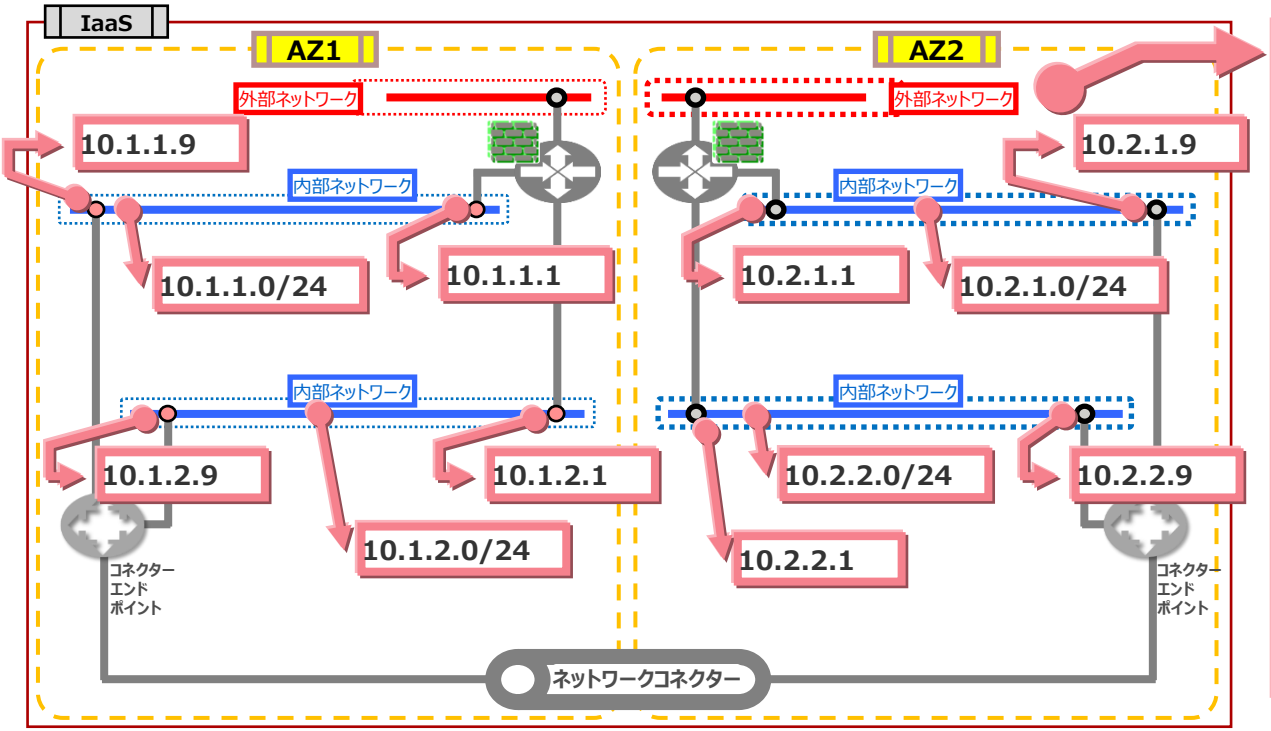
⑦-2　1-2の構成でのルーティングの設定内容

- **10.1.1.0/24に設定する内容（※１）**
  サブネット10.2.1.0/24との通信は　10.1.1.9を経由する
  サブネット10.2.2.0/24との通信は　10.1.1.9を経由する
  その他全て(0.0.0.0/0)との通信は 10.1.1.1を経由する

- **10.2.1.0/24に設定する内容（※２）**
  サブネット10.1.1.0/24との通信は　10.2.1.9を経由する
  サブネット10.1.2.0/24との通信は　10.2.1.9を経由する
  その他全て(0.0.0.0/0)との通信は 10.2.1.1を経由する

- **10.1.2.0/24に設定する内容**
  サブネット10.2.1.0/24との通信は　10.1.2.9を経由する
  サブネット10.2.2.0/24との通信は　10.1.2.9を経由する
  その他全て(0.0.0.0/0)との通信は 10.1.2.1を経由する

- **10.2.2.0/24に設定する内容**
  サブネット10.1.1.0/24との通信は　10.2.2.9を経由する
  サブネット10.1.2.0/24との通信は　10.2.2.9を経由する
  その他全て(0.0.0.0/0)との通信は 10.2.2.1を経由する



【サブネットにルーティングを設定】

AZ1のWeb用のサブネットから、
AZ2のWeb用のサブネットや、
AZ2のDB用のサブネットへ経路を
設定したり(※1)、同じように
AZ2のWeb用のサブネットから、
AZ1のWeb用のサブネットや、
AZ1のDB用のサブネットへ経路を
設定します(※2)。

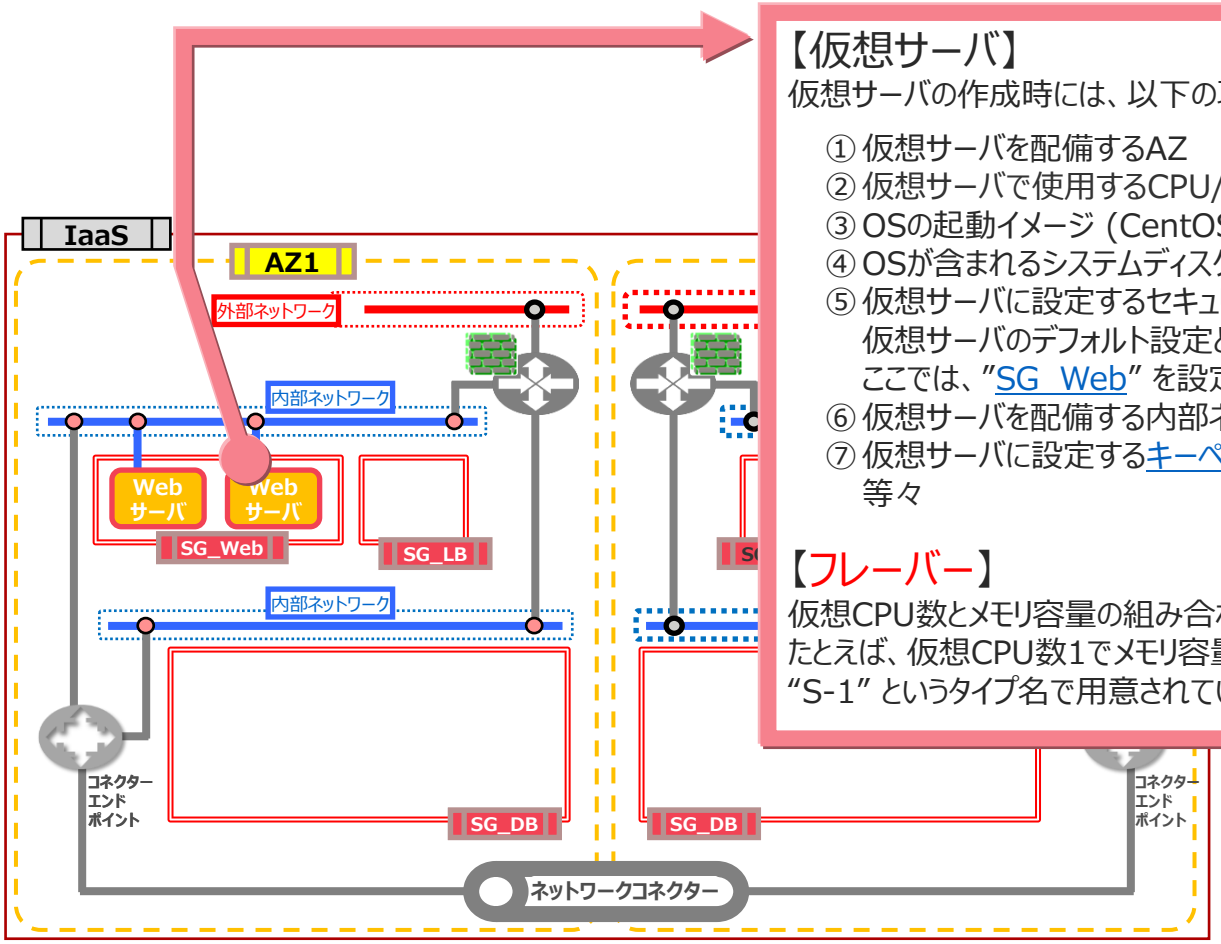
また、AZ間をまたぐ通信に対して、
行きと帰りの経路が同じになるように、
ルーティング情報を設定します。

実装作業⑧ 仮想サーバ

⑧　仮想サーバを作成

ネットワークの設定後、1-1⑥-1で記載したキーペアを各AZで作成し、同じく各AZで仮想サーバを作成します。

この構成では、Linux系OS で作成します。(1-2③、1-2④で、sshでログインする設定にしています。)



【仮想サーバ】

仮想サーバの作成時には、以下の項目を設定します。

① 仮想サーバを配備するAZ
② 仮想サーバで使用するCPU/メモリのタイプ (フレーバー)
③ OSの起動イメージ (CentOS,Windows等)
④ OSが含まれるシステムディスクのサイズ
⑤ 仮想サーバに設定するセキュリティグループ
　仮想サーバのデフォルト設定として使用します。複数設定できます。
　ここでは、"SG_Web" を設定します。後から追加/削除が可能です。
⑥ 仮想サーバを配備する内部ネットワーク
⑦ 仮想サーバに設定するキーペア (キーペアは各AZで作成)
　等々

【フレーバー】

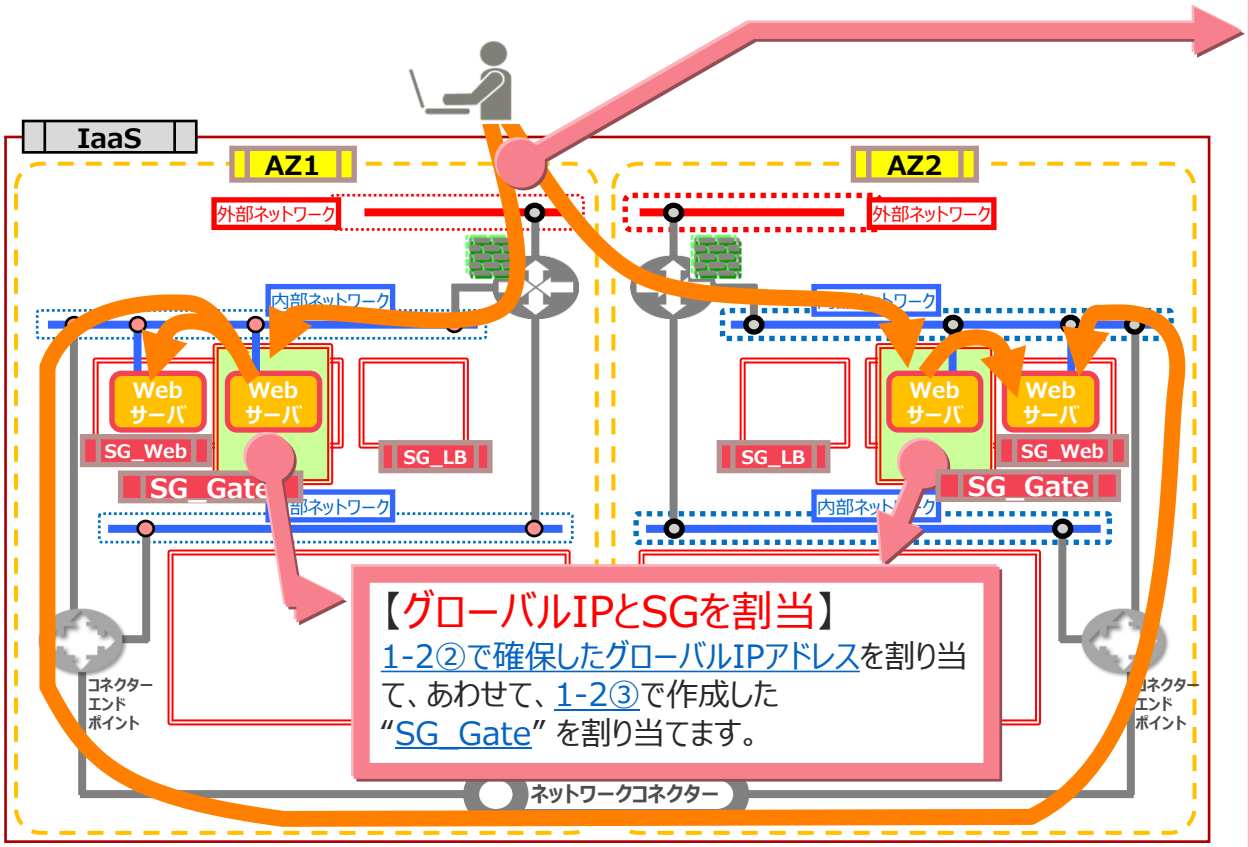
仮想CPU数とメモリ容量の組み合わせを示すタイプ名です。
たとえば、仮想CPU数1でメモリ容量4GBの組み合わせが
"S-1" というタイプ名で用意されています。

実装作業⑨ 仮想サーバにグローバルIPアドレスを設定

⑨SSH接続対象の仮想サーバにグローバルIPアドレスを設定

仮想サーバが作成できたら、各AZの仮想サーバ （SSH接続対象サーバ）1台ずつに、1-2②で確保したグローバルIPアドレスを割り当てます。あわせて、1-2③で作成したセキュリティグループ “SG_Gate” も割り当てます。

仮想サーバにグローバルIPアドレスとセキュリティグループを割り当てた後、数分すると、その仮想サーバにインターネットからログインできるようになります。 仮想サーバにログインしたら、その仮想サーバから 別のすべての仮想サーバにログインできることも確認してください。



【ログイン】
仮想サーバにログインできることを確認します。

※ 仮想サーバが Linux系OSの場合には、sshクライアント側で、キーペア (*.pem) を利用する設定をして仮想サーバにログインしてください。

※ 仮想サーバが Windowsの場合は、設定したキーペアの鍵ファイルを利用して、管理者パスワードを入手してログインしてください。

各AZで、SG_Gate を割り当てた仮想サーバから、別のすべての仮想サーバにログインできることを確認してください。

※ グローバルIPアドレスとセキュリティグループの割り当ては、ssh でログインして作業をする時だけでかまいません。
ログインしない時に、グローバルIPアドレスとセキュリティグループの設定を外すと、インターネットを含む外部から ログイン できない状態になりますので、セキュリティが向上します。

実装作業⑩ ロードバランサー (1/2)

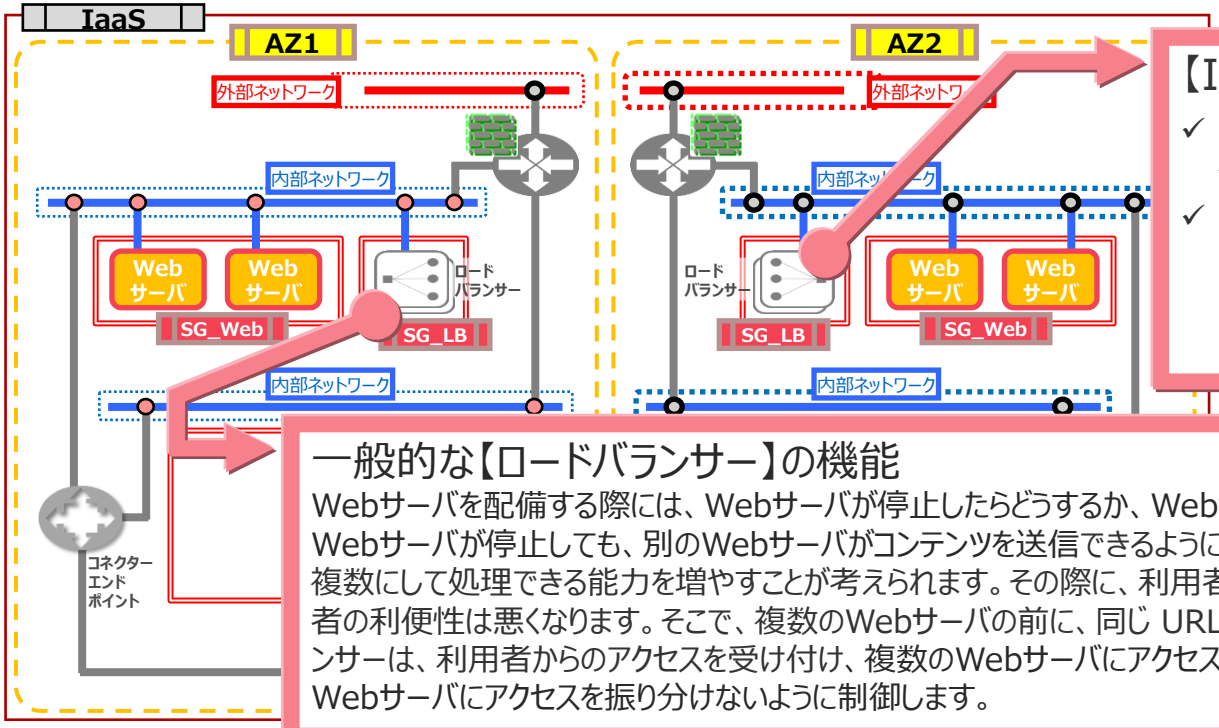
⑩-1 ロードバランサーを配備

可用性向上と性能向上のための負荷分散機能として、ロードバランサーサービスを提供しています。

ロードバランサーの作成時は、①インターネットに公開するか内部ネットワークで利用かを示すロードバランサータイプ、
②同時に処理可能な性能を指定するグレード、③ロードバランサーが待ち受けるプロトコル/ポート番号、
④仮想サーバにアクセスする際のプロトコル/ポート番号、⑤SSL証明書ID、⑥負荷分散対象のサブネットリスト、
⑦ロードバランサーに適用するセキュリティグループリスト (この構成では “SG_LB”) 等を設定します。

ロードバランサーの作成時に、AZ1、AZ2それぞれのサブネットを負荷分散対象のサブネットと設定すると、
複数のAZに配備された仮想マシンに対して負荷分散することが可能になります。

(この構成では、1-2①で設定した AZ1の “10.1.1.0/24” と AZ2の “10.2.1.0/24” を設定します。)



【IaaSのロードバランサーサービスの特徴】

- ✓ 1つのロードバランサーで、AZ1/AZ2に配備された仮想サーバに負荷分散可能です。
- ✓ ロードバランサーは、ロードバランサーが作成された時に生成される 1つの FQDN でのみアクセス可能です。
  (ロードバランサーに割り当てられたIPアドレスは、変更される可能性があります)

一般的な【ロードバランサー】の機能

Webサーバを配備する際には、Webサーバが停止したらどうするか、Webサーバへのアクセスが増大したらどうするか等を検討します。Webサーバが停止しても、別のWebサーバがコンテンツを送信できるようにしたり、Webサーバのアクセスが増大したらWebサーバを複数にして処理できる能力を増やすことが考えられます。その際に、利用者がWebサーバのアクセス先を都度指定するのでは、利用者の利便性は悪くなります。そこで、複数のWebサーバの前に、同じ URL でアクセスできるロードバランサーを配備します。ロードバランサーは、利用者からのアクセスを受け付け、複数のWebサーバにアクセスを分散します。Webサーバが停止した際は、停止したWebサーバにアクセスを振り分けないように制御します。

実装作業⑩ ロードバランサー (2/2)

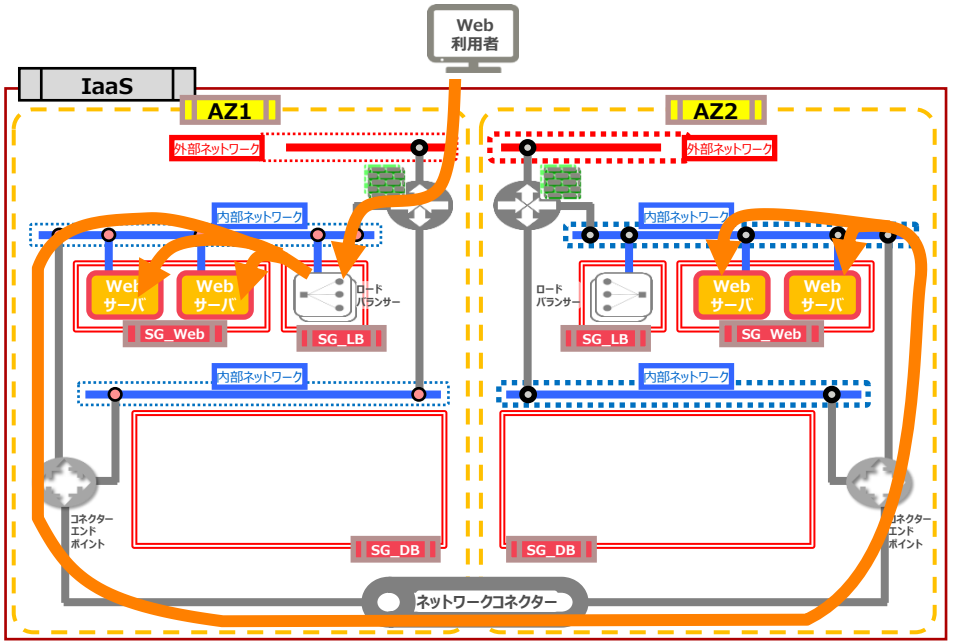
⑩-2 ロードバランサーによる仮想サーバへの接続経路

ロードバランサーを作成すると、ロードバランサーに対して FQDN が割り当てられます。
ロードバランサーの作成時に、各AZのサブネットを設定したマルチAZ構成では、各AZにロードバランサーが接続されます。

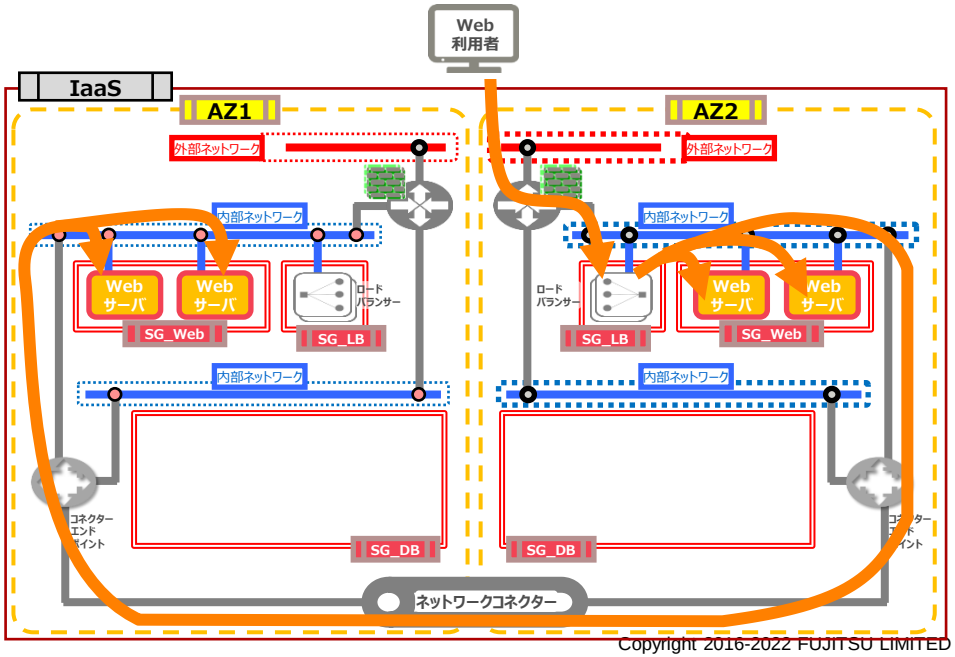
マルチAZ構成では、ロードバランサーの FQDN に対して、DNSにはAZ1内に接続されたロードバランサーのIPアドレスと、AZ2内に接続されたロードバランサーのIPアドレスが設定されます。どちらの AZのロードバランサーにアクセスされるかは、DNSサーバが回答するIPアドレスの順番と、それを処理するアプリケーション次第となります。

AZ1のロードバランサーからAZ2の仮想サーバへのアクセスは、ネットワークコネクター経由でのアクセスとなります。同様に、AZ2のロードバランサーからAZ1の仮想サーバへのアクセスは、ネットワークコネクター経由でのアクセスとなります。

- ロードバランサーのFQDNに対するDNSサーバからの回答がAZ1側のIPアドレスだった場合の負荷分散の経路



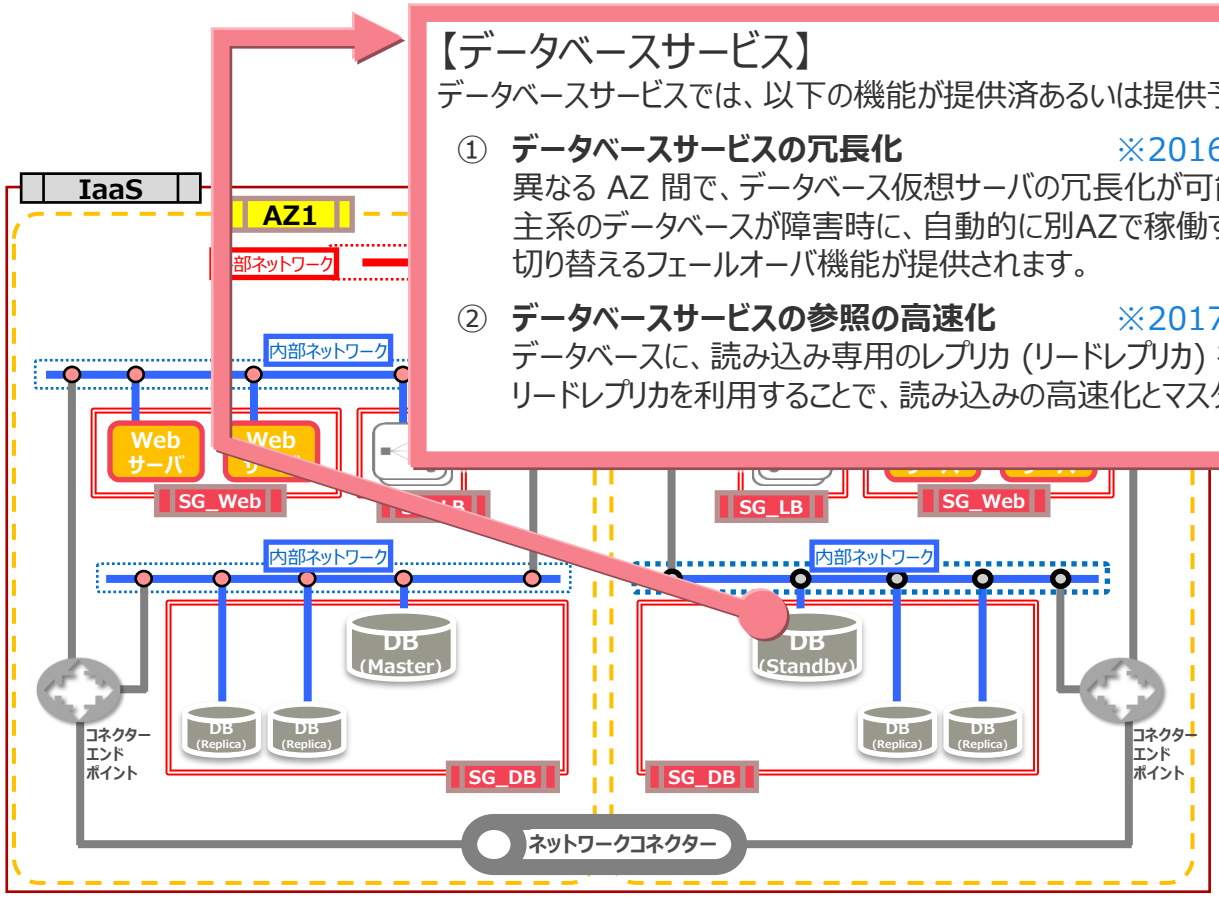
- ロードバランサーのFQDNに対するDNSサーバからの回答がAZ2側のIPアドレスだった場合の負荷分散の経路



実装作業⑪ データベースサービス

⑪　データベースサービスを配備

データベースを自前で構築しないで利用可能なデータベースサービスが用意されています。
データベースサービスを利用すると、手間のかかる構築/運用を IaaSサービス側に任せることができます。
異なるAZ間でデータベース仮想サーバの冗長化も可能です。主系のデータベースが障害時に、自動的に別AZで稼働する従系を主系として切り替えるフェールオーバ機能が提供されています。



【データベースサービス】
データベースサービスでは、以下の機能が提供済あるいは提供予定です。

① **データベースサービスの冗長化**　※2016年7月提供済
異なる AZ 間で、データベース仮想サーバの冗長化が可能になります。
主系のデータベースが障害時に、自動的に別AZで稼働する従系を主系として切り替えるフェールオーバ機能が提供されます。

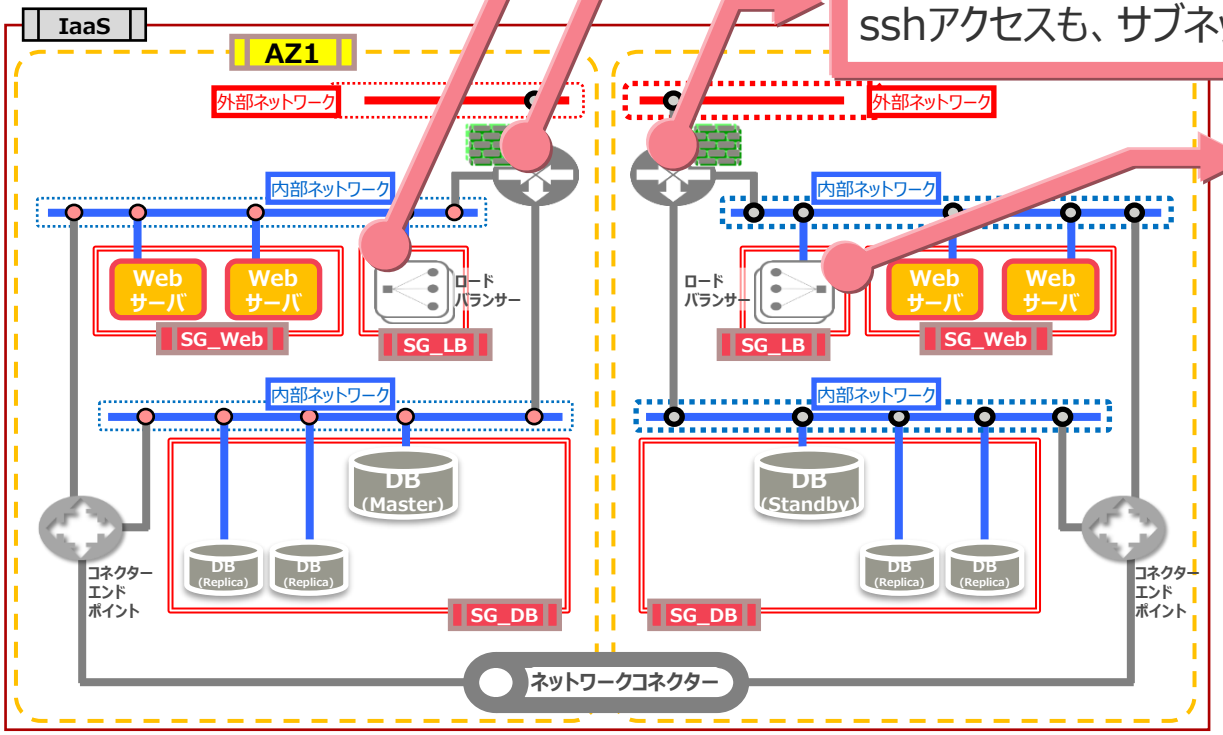
② **データベースサービスの参照の高速化**　※2017年1月時点では未提供
データベースに、読み込み専用のレプリカ (リードレプリカ) を配備できるようになります。
リードレプリカを利用することで、読み込みの高速化とマスターDBの負荷の軽減が図れます。

実装作業⑫ アクセス制御

⑫　すべての作業が終わったら、FW/SGのアクセス制御を変更してインターネットに公開

仮想サーバの構築作業、ロードバランサーやデータベース仮想サーバの設定作業などが終わりましたら、
FW/SGのアクセス制御を変更します。

ロードバランサー(80/tcp)へのアクセスを、不特定のアクセス元から接続可能になるよう変更します。



【アクセス制御のルール変更】
構築作業の完了後、Webサーバへのhttpアクセスを、
特定のアクセス元から不特定のアクセス元になるように、
ファイアーウォール、セキュリティグループのルールを変更します。
sshアクセスも、サブネット単位からWebサーバに変更します。

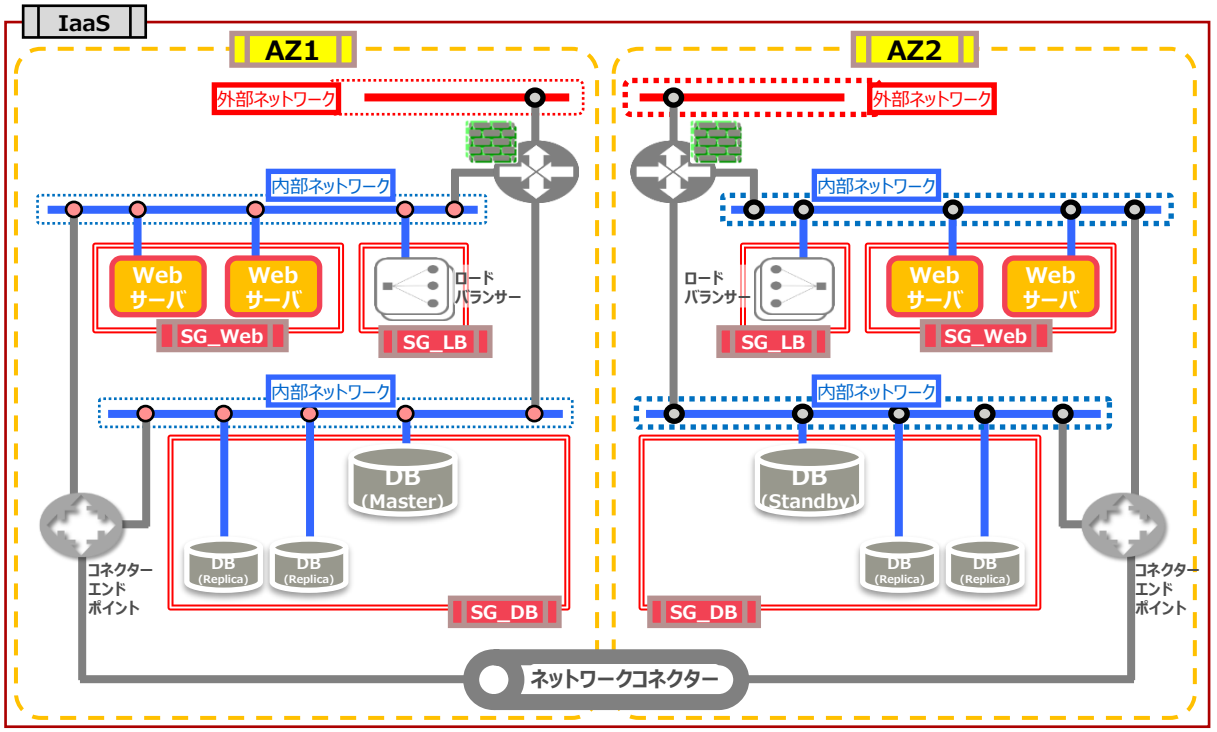
【参考】ロードバランサーのFQDN
1-2の構成例では、IaaSのロードバランサーのFQDN をそのまま使用する例となっています。

実際にサービスで利用される際は、利用者のドメイン名 でアクセスすることができるように、IaaSのロードバランサーのFQDNをIaaSのDNS
サービスもしくは利用者のDNSサーバで別名をCNAME で定義して、利用者管理のドメイン名でロードバランサーにアクセスできるよう設定してください。

実装作業まとめ

- 以上の実装手順で、マルチAZ構成を配備できます。
- 1-2の構成では、仮想サーバやデータベースを複数稼働させることで、同時に処理できる処理量を向上し、あわせてサーバ障害時にも業務を継続できるようにしています。
  さらに、複数のAZを利用しているため、片方のAZで不具合が発生した場合でも、もう片方のAZで業務を継続できるようにしています。

※ なお1-2の構成では、Webサーバに sshでログインする設定にしていますが、ssh でログインするサーバを別の仮想サーバにする (別にログイン専用サーバを用意する) と、サービス提供用のサーバとメンテナンス用のサーバとを分離できるため、セキュリティが向上します。



第2章　システム設計時のポイント

2-1.　可用性で検討する項目

IaaSで提供される仮想サーバ、ストレージ、ネットワークの可用性について記載します。

2-1. 可用性で検討する項目 (1/4)

FUJITSU

項目	要件	対応
2-1-1 継続性	稼動率 ※補足資料も参照してください。	[仮想サーバのサービスレベル] •IaaSの月間稼働率は仮想サーバを対象として99.99%です。 ※ 契約者が、同一契約内において、同一リージョン内の複数の アベイラビリティゾーンに仮想サーバを作成した場合が適用範囲です。 詳細については「サービスレベル仕様書」を参照してください。
2-1-2 耐障害性	仮想サーバの冗長構成	[Webサーバ/APサーバ等の冗長化] •WebサーバやAPサーバ等の仮想サーバは、IaaSで提供されている ロードバランサーによる冗長構成を検討してください。 •1つのロードバランサーにつき、仮想サーバ側は1つのポートのみ設定ができます。 仮想サーバ側を複数ポートで冗長構成を行う場合は、ロードバランサーを複数 配備してください。 [データベースサービスの冗長化] •データベースサービスでは、冗長化構成が可能です。 今後、リードレプリカへの非同期レプリケーションを提供予定です。 •データベースサービスの冗長化構成では同期で複製が行われるため、 スタンドアロン構成に比べて、書き込み性能に影響が生じる可能性があります。 •データベースサービスのリードレプリカ(今後提供予定)は非同期で複製されるため、 データ参照時に古いデータが参照される可能性があります。 ※2017年1月時点では未提供 •データベースサービスを利用したアプリケーション設計ができない場合は、 仮想サーバにデータベース用ソフトウェアを個別に導入するなどして、 データベースの冗長構成を実現してください。

2-1. 可用性で検討する項目 (2/4)

FUJITSU

項目	要件	対応
2-1-2 耐障害性(つづき)	物理サーバの冗長構成	[物理サーバの冗長化] ●仮想サーバ作成時にフェイルオーバを有効にすることで、物理ホストマシンが故障などにより停止した場合、自動的に別のホストマシンに移動して稼働させることができます。ただし、オートスケールと併用はできませんので注意してください。
	ストレージデータ保全	[ブロックストレージ] ●IaaSのブロックストレージの物理ディスクは、冗長構成によりデータが保持されます。 [オブジェクトストレージ] ●IaaSのオブジェクトストレージに格納されたデータは、自動的に複数のアベイラビリティゾーンに保存されます。 ●1オブジェクトの最大容量は5GBです。 5GBを超過するオブジェクトは、分割アップロード後に結合してください。
	バックアップ方法 ※バックアップ方式については 2-3-1項も参照してください。	[スナップショットによるバックアップ] ●スナップショット機能は、システムストレージ/増設ストレージ の どちらに対しても利用可能です。 ●オンラインで取得したスナップショットは動作保証されないため、オンラインでのバックアップが必要な場合は、サードパーティー製のバックアップソフトウェアの導入が必要です。 アプリケーション部分の復旧は、別途設計してください。 [バックアップソリューションを提供するソフトウェアによるバックアップ] ●ストレージ内のデータをファイル単位でバックアップを取得する場合は、バックアップ用ソフトウェアによるバックアップソリューションの適用を検討してください。 ※利用には別途ソフトのセットアップ(BYOL)が必要です。

2-1. 可用性で検討する項目 (3/4)

FUJITSU

項目	要件	対応
2-1-2 耐障害性(つづき)	バックアップ方法 ※バックアップ方式については 2-3-1項も参照してください。 ※補足資料も参照してください。	[オブジェクトストレージへのバックアップ] ●オブジェクトストレージは容量無制限です。 大容量のデータなどを格納する必要がある場合に検討してください。 [データベースサービスのバックアップ] ●データベースサービスは、自動バックアップ設定をすることにより、 日次で最大10日間分のデータと設定ファイルを保持します。 [仮想サーバイメージの保管] ●作成済の仮想サーバより仮想サーバイメージを作成しておくことで、 同じ環境の仮想サーバを複製することが可能です。 [バックアップ装置の持ち込み] ●テープ装置など、物理的なバックアップ機器の持ち込みは行えません。
2-1-3 災害対策	リージョン(地域) 災害 ※補足資料も参照してください。	[リージョン] ●地理的に独立した地域、独立したデータセンターを リージョンと呼びます。 ●各リージョン(データセンター)内の設備は、サービス提供用設備などの 物理的な施設を共有する単位の “アベイラビリティゾーン(AZ)“ にて 運営されています。通常、各リージョンは複数のAZで構成されます。 ●2017年1月時点で、東日本第1リージョン(2AZ)、西日本第2リージョン(2AZ)、 UK(2AZ)、フィンランド(2AZ)でサービス提供しています。 最新のリージョンは機能説明書をご確認ください。 [DNSを利用した複数リージョンのシステムの冗長化] ●複数のリージョンに構築したシステムの FQDN を同一にすることにより、 複数のリージョンを跨いだ冗長構成を構築することが可能です。

2-1. 可用性で検討する項目 (4/4)

FUJITSU

項目	要件	対応
2-1-3 災害対策(つづき)	リージョン(データセンター) 災害 ※補足資料も参照してください。	[アベイラビリティゾーン(AZ)] ●異なるAZに仮想サーバやデータベースサービス等を分散して業務システムを冗長構成で配置することにより、物理的な施設レベルの障害に対しても、高い可用性を実現できます。 ●同一リージョン内の AZ同士は、低遅延ネットワークで接続されています。 [DNSを利用した複数AZのシステムの冗長化] ●複数のAZに構築したシステムの FQDN を同一にすることにより、複数のAZを跨いだ冗長構成を構築することが可能です。
2-1-4 回復性	データベースの復旧 ※補足資料も参照してください。	[データベースサービスのデータの復旧方法] ●データベースサービスの復旧方法には、以下の2通りの方法があります。 ①自動バックアップデータからの ポイントインタイムリカバリ ②スナップショットのデータからの 新規データベース仮想サーバ作成 [仮想サーバに個別構築したデータベースの復旧方法] ●要件に応じたバックアップ手法にて定期的にデータを保存し、障害発生時にリストアしてください。

補足)2-1-2.稼働率(SLA適用構成について)

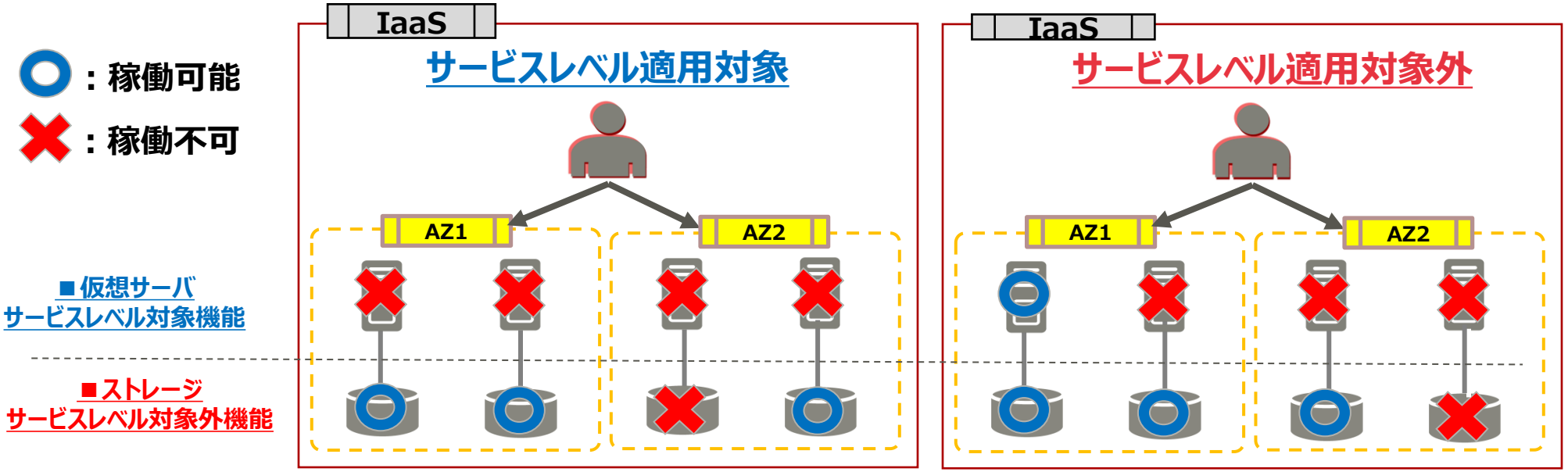
■SLAとして仮想サーバの月間稼働率99.99%が設定されています。適用条件を満たす為には、
仮想サーバを複数のアベイラビリティゾーンに配備するシステム構成を検討する必要があります。

対象機能	仮想サーバ
月間稼働率	99.99%
適用条件	同一契約、同一リージョン内で契約している全仮想サーバが動いている複数アベイラビリティゾーンが利用不可の状態
クレジット保証	仮想サーバの利用料金の10%を翌月以降利用料金から減額

■サービスレベル適用構成

○：稼働可能

×：稼働不可



・左図はAZ1、AZ2に配備してある全ての仮想サーバが稼動不可状態なのでサービスレベル適用対象となります。
・右図では、AZ2の仮想サーバが全て稼動不可の状態ですが、AZ1の仮想サーバが1台稼動可能状態なので、
サービスレベル適用対象となりません。※対象機能は「仮想サーバ」のみの為、ストレージの稼動可否は影響しません。

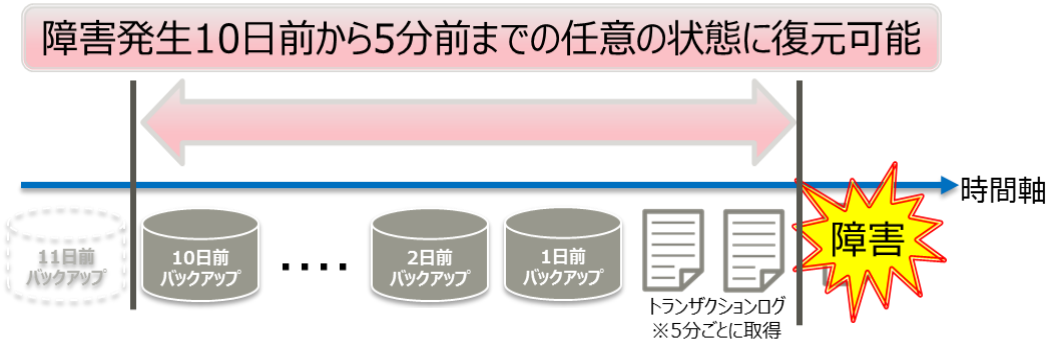
補足)2-1-4.回復性(データベースサービスの復旧)

FUJITSU

■**データベースサービスでは、以下の2種類の復旧方法が提供されています。**

①ポイントインタイムリカバリー(自動バックアップ機能)

自動バックアップのデータから、復旧したい時点の「日時」を指定して復旧。バックアップ保持期間(最長10日前)～最新のトランザクションログ保持時点(最短で5分前)までの任意の時間を指定して復旧することができます。

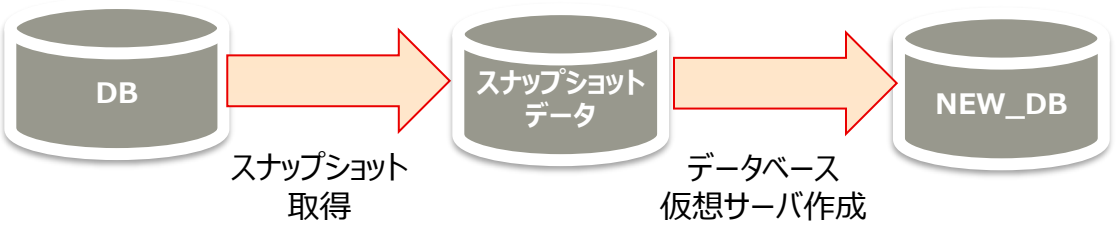


■**ポイントタイムリカバリー(自動バックアップ機能)による復旧**

- 指定した時間帯に1日1回、データ全体をバックアップします。
- 5分おきにトランザクションログを継続的にバックアップします。
- バックアップデータは、バックアップ保持期間(最長10日間)まで保持されます。
- バックアップ保持期間を過ぎたデータは自動的に削除されます。

②スナップショットデータを指定して復旧

任意の時点で取得したスナップショットデータを指定して復旧することができます。



■**スナップショット機能による復旧**

- スナップショット取得した時点でのデータ状態で復元します。
- 新規にデータベース仮想サーバの構築が必要です。
- 事前にDBサブネットグループなど構築環境の準備が必要です。
- スナップショットデータは復旧したデータに問題が無い事を確認してから削除してください。

2-2.　性能・拡張性で検討する項目

IaaSで提供される仮想サーバ、ストレージ、ネットワークの性能・拡張性について
記載します。

2-2. 性能・拡張性で検討する項目 (1/6)

項目	要件	対応
2-2-1 性能目標値	オンラインレスポンス	[レスポンスタイムの検証/確認] •IaaSの仮想CPUとメモリ以外のリソースはベストエフォート方式での提供となります。 そのため、レスポンス時間や処理終了期限は、実際の環境で検証や確認が必要となります。 •期待する性能が得られない場合は、ロードバランサーで仮想サーバをスケールアウトするなど 受付性能の向上を検討してください。
	ターンアラウンドタイム	[ターンアラウンドタイムの検証/確認] •IaaSの仮想CPUとメモリ以外のリソースはベストエフォート方式での提供となります。 そのため、レスポンス時間や処理終了期限は、実際の環境で検証や確認が必要となります。 •期待する性能が得られない場合は、仮想サーバのスケールアップにより処理性能の 向上を検討してください。
	バッチスループット	[バッチ処理時間の検証/確認] •IaaSの仮想CPUとメモリ以外のリソースはベストエフォート方式での提供となります。 そのため、レスポンス時間や処理終了期限は、実際の環境で検証や確認が必要となります。 •APサーバ上のアプリケーションによりDBサーバへネットワーク経由で大量にアクセスが発生する バッチ処理の場合、期待するスループットが得られるか、事前検証による 確認を行ってください。

2-2. 性能・拡張性で検討する項目 (2/6)

FUJITSU

項目	要件	対応
2-2-2 リソース拡張性	CPU拡張性 メモリ拡張性	[CPUとメモリのリソース] ●CPU と メモリ を セットにした仮想サーバモデルを、フレーバーとして提供しています。 ●稼動するアプリケーションが大容量のメモリを必要とする場合は、メモリ容量の観点からフレーバーを選定してください。 ●CPU 見積りについては、オンプレミスの物理機器のシステムとは異なり、クラウドではシステム係数などによる厳密な性能見積りはできません。
	ディスク拡張性	[仮想サーバにアタッチするブロックストレージの拡張性] ●仮想サーバにブロックストレージをアタッチすると、仮想サーバ上で増設ディスクとして使用できるようになります。仮想サーバにアタッチするブロックストレージの容量や本数は指定可能です。 [ストレージ容量が不足した場合の対処方法] ●仮想サーバにアタッチした増設ストレージは、スナップショット機能を利用したり、ストレージの容量拡張のAPIを実行することで、容量拡張が可能です。なお、増設ストレージの容量拡張の際には、対象の増設ストレージを仮想サーバからデタッチする必要があります。

2-2. 性能・拡張性で検討する項目 (3/6)

FUJITSU

項目	要件	対応
2-2-2 リソース拡張性(つづき)	ネットワーク拡張性 ※補足資料も参照してください。	[インターネット接続] •インターネット経由での接続をする場合は、IaaSで標準提供されるインターネット接続サービスの利用を検討してください。 •複数の仮想ルータを設置することで、インターネットから接続するポイントを拡張可能です。複数仮想ルータを設置する場合は、仮想ネットワークやサブネットもそれぞれ作成してください。 [マルチAZ間接続によるネットワーク拡張] •AZ跨ぎでの冗長構成を検討される場合は、ネットワークコネクタ および コネクターエンドポイント の設定をしてください。 [プロジェクト間接続によるネットワーク拡張] •プロジェクト間接続機能を設定することで、同一ドメインで異なるプロジェクト同士のネットワークの接続が可能です。 [IPsecVPN接続によるネットワーク拡張] •IPsecVPN接続によるネットワーク拡張により、オンプレミス環境との接続、またはリージョン間同士のシステム接続が可能です。 •IaaSの仮想ルータに接続される1つのサブネットと対向ゲートウェイに接続される1つのサブネット間の通信ができます。 •L2TP/IPsecVPNでリモートアクセス端末からの接続はできません。 •2拠点間を結ぶようなハブアンドスポーク型トポロジー構成、NATトラサーバルで接続することはできません。 •1仮想ルータあたり20拠点まで接続が可能です。

2-2. 性能・拡張性で検討する項目 (4/6)

FUJITSU

項目	要件	対応
2-2-2 リソース拡張性(つづき)	ネットワーク拡張性	[SSL-VPN接続] ●1接続あたり20クライアントまで接続が可能です。 [FJcloud-O DEX(旧称 プライベート接続オプション）によるネットワーク拡張] ●富士通データセンター内のハウジング環境やオンプレミス環境、他社クラウドと接続し、ネットワーク拡張することが可能です。 ●各リージョンで提供されるメニューが異なります。 利用されるリージョンで提供される接続形態を検討してください。 [ダイレクトポート接続によるネットワーク拡張] ●IaaS環境と直接接続できる物理ポートを提供します。他社との共有ネットワークではなく専用ネットワークで利用されたい場合に検討してください。
	仮想サーバ処理能力 増強/縮退	[仮想サーバの処理性能の増強/縮退~スケールアップ/スケールダウン] ●仮想サーバの処理性能を増強する場合は、性能検証/確認を行い、適切なフレーバーを選定してください。 ●サービスポータルでは、仮想サーバが起動状態(ACTIVE)であること、かつ全てのアプリケーションが停止していることを確認したうえで、スケールアップ/スケールダウンを行ってください。仮想サーバが再起動されフレーバーの変更が反映されます。 ●稼動後のスケールアップ/ダウンを見越してフレーバーの選定を行う場合、スケールアップ/ダウン実行時の業務影響とその対処を検討してください。

2-2. 性能・拡張性で検討する項目 (5/6)

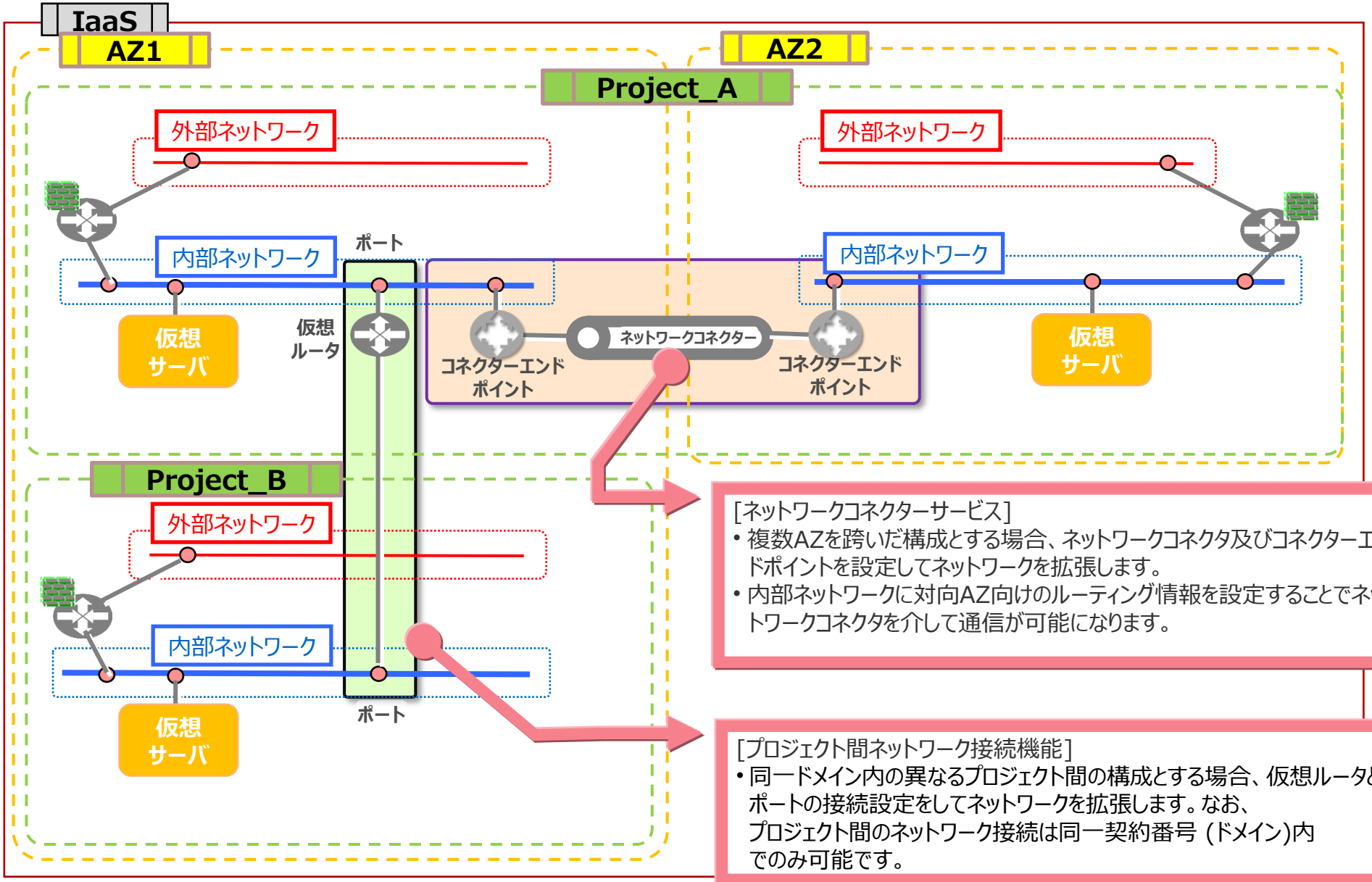
FUJITSU

項目	要件	対応
2-2-2 リソース拡張性(つづき)	仮想サーバ処理能力 増強/縮退	[システム全体の処理性能の増強~スケールアウト/スケールイン] ●仮想サーバ単体の性能に加えて、システム全体の性能が充足するよう、仮想サーバのスケールアウトを考慮してください。 ●監視サービスのCPU使用率等の閾値条件や、スケジューラーの設定時間に応じて自動的にスケールアウト/スケールインを行う オートスケール機能 の利用を検討してください。 ●オートスケールを設定すると、予め作成しておいた仮想サーバのイメージを使って、スケーリンググループで設定した最小台数の仮想サーバが配備されます。 ●オートスケールは、仮想サーバイメージを元にスケールアウトを行います。そのため、定期的に、セキュリティパッチを適用した環境で仮想サーバイメージを作成し、オートスケール用の仮想サーバイメージを置き換える運用を検討してください。 ●業務アプリの改修が出来ないなどの理由で、セッション情報維持のために業務時間中にスケールインできない場合は、業務停止のタイミングを設定し、そのタイミング（時間）になるとオートスケールを利用してスケールインするといった対応を検討してください。 ●稼動後のスケールアウト/インを見越してフレーバーの選定を行う場合、スケールアウト/イン実行時の業務影響とその対処を検討してください。 ●オートスケールが頻繁に実行される場合は、条件の見直しや、クールダウン時間の設定などを行ってください。 ●スケールアウトで起動する仮想サーバは、仮想サーバ使用料やライセンス費用がかかります。

2-2. 性能・拡張性で検討する項目 (6/6)

項目	要件	対応
2-2-3 性能品質保証	ネットワーク帯域保証	[インターネット接続] •IaaSは1Gbpsベストエフォート方式での提供となります。そのため、レスポンス時間や処理終了期限は、実際の環境で 検証を行い確認してください。 •利用するネットワーク接続の形態 (インターネット接続/IPsecVPN/閉域網/構内接続等) ごとに、必要なスループットを満たすことを確認してください。 •帯域保証が必要な場合は、FJcloud-O DEX (旧称プライベート接続オプション) の帯域確保型を検討してください。

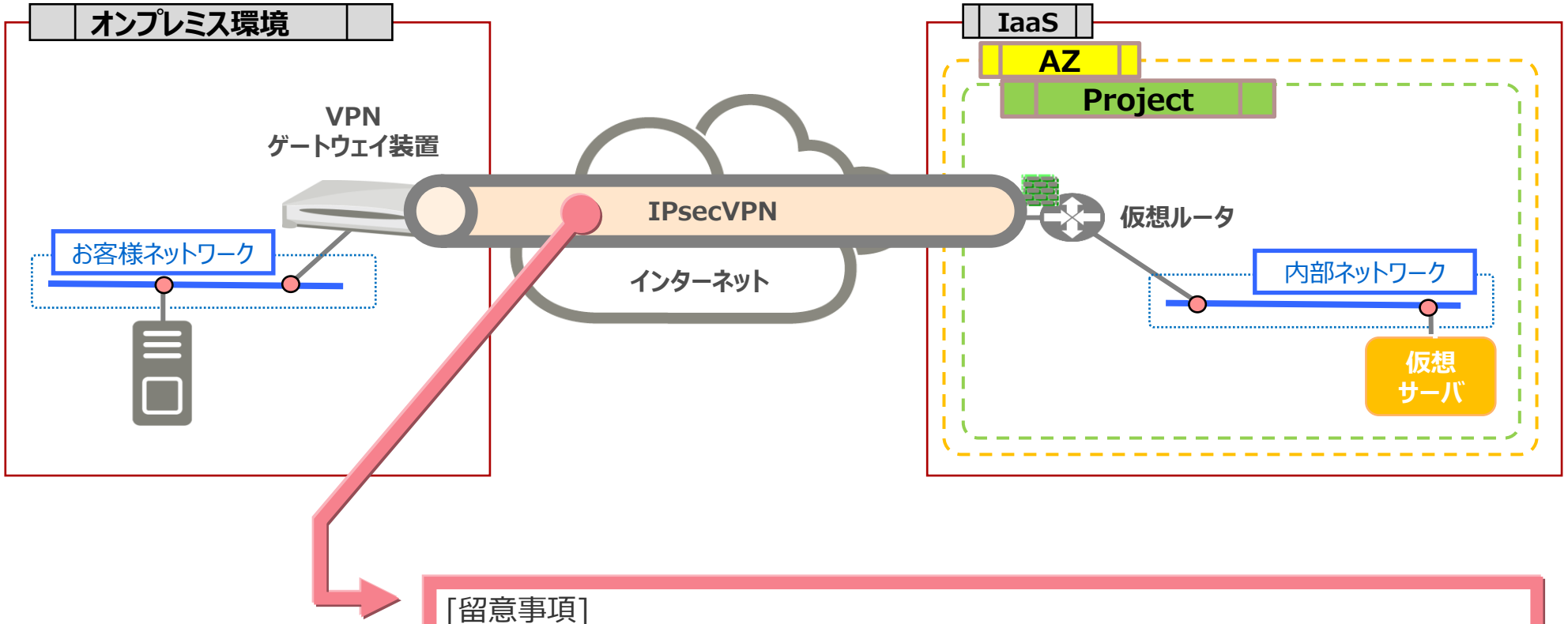
補足)2-2-2.ネットワーク拡張性(AZ間/プロジェクト間接続)



[ネットワークコネクターサービス]
- 複数AZを跨いだ構成とする場合、ネットワークコネクタ及びコネクターエンドポイントを設定してネットワークを拡張します。
- 内部ネットワークに対向AZ向けのルーティング情報を設定することでネットワークコネクタを介して通信が可能になります。

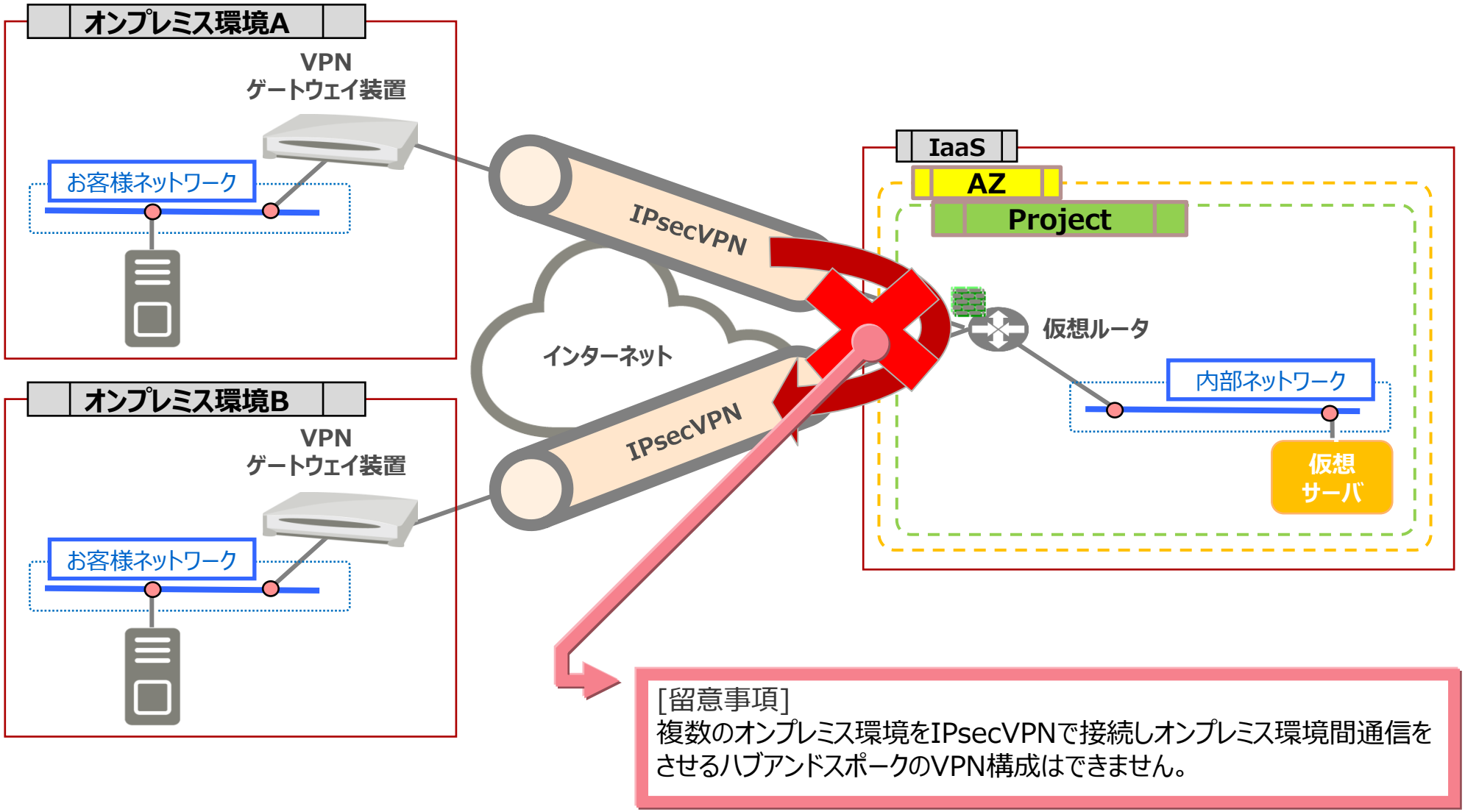
[プロジェクト間ネットワーク接続機能]
- 同一ドメイン内の異なるプロジェクト間の構成とする場合、仮想ルータとポートの接続設定をしてネットワークを拡張します。なお、プロジェクト間のネットワーク接続は同一契約番号 (ドメイン)内でのみ可能です。

補足)2-2-2.ネットワーク拡張性(IPSecVPN接続①)

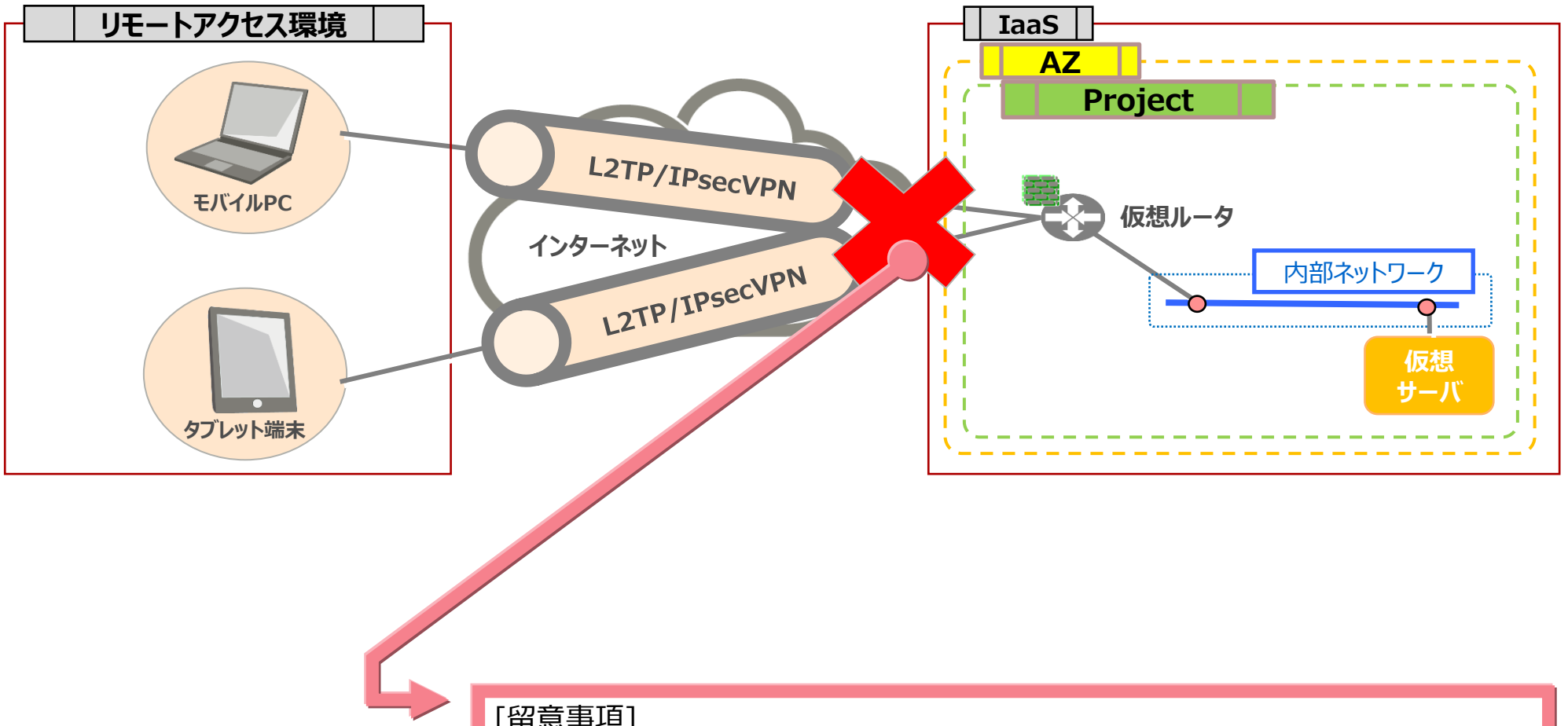


[留意事項]
- 仮想ルータ1台で最大20までIPsecVPN接続設定が可能です。
- IPsecVPNで定義されていない内部ネットワークへはお客様ネットワークからアクセスできません。
- IPsecVPN通信は仮想ルータに接続されている1つの内部ネットワークと、対向のVPNゲートウェイ装置に接続される1つのお客様ネットワークのみ通信ができます。
- オンプレミス環境のVPNゲートウェイ装置はお客様で準備する必要があります。
- 仮想ルータへのIPsecVPN設定は利用者の責任で実施してください。

補足)2-2-2.ネットワーク拡張性(IPSecVPN接続②)



補足)2-2-2.ネットワーク拡張性(IPSecVPN接続③)



[留意事項]
- IaaSのIPsecVPN機能ではL2TP/IPsecVPN接続はできません。
- リモートアクセス端末からのアクセスが必要な場合は、個別にリモートアクセス環境の構築を検討してください。

2-3.　運用・保守性で検討する項目

IaaSで提供される運用監視、サポートメニューについて記載します。

2-3. 運用・保守性で検討する項目 (1/7)

FUJITSU

項目	要件	対応
2-3-1 通常運用	運用時間	[運用時間] ●24時間365日(計画停止／定期保守/即時対応を除く)
	バックアップ ※バックアップ方式については 2-1-2項も参照してください	[システムストレージ/増設ストレージのバックアップ] ●スナップショット機能で各ストレージをバックアップすることが可能です。 ●確実なバックアップデータとしたい場合は、仮想サーバを停止したうえで スナップショットを実行してください。 [ファイル単位でのバックアップ] ●オブジェクトストレージへのファイルコピーを検討してください。 1ファイルが5GB以上になる場合はファイル分割してください。 ●バックアップツールによるバックアップを検討してください。 [システム変更/パッチ適用前後のバックアップ] ●システムへの変更やパッチ提供前にバックアップすることで、 万が一不具合が発生した場合、変更前の状態に戻すことができます。 ●システム変更後、パッチ適用後に問題がなければ、 最新のシステム状態をバックアップすることを検討してください。

2-3. 運用・保守性で検討する項目 (2/7)

FUJITSU

項目	要件	対応
2-3-1 通常運用(つづき)	バックアップ ※ バックアップ方式については 2-1-2項も参照してください	[データベースサービスのバックアップ] ●データベースサービスで標準提供される自動バックアップの利用を検討してください。 ●仮想サーバに個別構築したデータベースサーバのバックアップは、 それぞれのDBMSに応じたバックアップ手法を検討してください。 [その他] ●利用者独自の仮想サーバイメージやシステムテンプレートを保管可能です。
	運用監視	[IaaS基盤の監視] ●ハードウェア監視、ハイパーバイザー稼動監視は、富士通(IaaS)で行います。 [OS/アプリケーションの監視] ●仮想サーバ上のOS等の稼働監視は、利用者側で実施してください。 ●アクセスログなど各種ログの監視が必要な場合は、別途監視用のソフトウェア (富士通製 Systemwalker Centric Manager等) の利用を検討してください。

2-3. 運用・保守性で検討する項目 (3/7)

FUJITSU

項目	要件	対応
2-3-1 通常運用(つづき)	運用監視	[リソース監視] ●仮想サーバ、ロードバランサー、ストレージのリソースについて、リソースごとに定義されたリソース監視項目のデータを取得します。 ●監視サービスにより、データベースサービスのデータベース仮想サーバも監視することが可能です。利用者は、データベース仮想サーバサーバで発生するイベントに対して、メール通知を受け取ることが可能です。 ●監視サービスによるリソース(仮想サーバやデータベース仮想サーバ)の他、利用者が実行するアプリケーションの監視をカスタムメーターとして追加することが可能です。 ●監視項目は、APIやサービスポータルでモニタリングやアラーム通知が可能です。 ●監視サービスで対応できない項目について監視が必要な場合は、別途監視用のソフトウェア (富士通製Systemwalker Centric Manager等) の利用を検討してください。 [モニタリングしたデータの保持期間] ●モニタリングしたデータは２週間保持します。２週間を超過してモニタリングデータの保存が必要な場合は、API操作にてデータを定期的に取得し、別途ストレージに保存するなどの対策を検討してください。

2-3. 運用・保守性で検討する項目 (4/7)

FUJITSU

項目	要件	対応
2-3-2 保守運用	計画停止	[計画停止の通知と対処] ●14日前までにメールおよびサービスポータルにて実施が通知されます。 業務影響が最小限となるように対策を検討してください。 ●計画メンテナンスの他、予告無しの緊急メンテナンスが実施される場合があります。 ●計画メンテナンス時には、富士通(IaaS)側で仮想サーバを他の物理サーバに 移動させるため、仮想サーバは停止しません。
	パッチ適用	[IaaS基盤のパッチ適用] ●IaaS基盤（ハイパーバイザー等）に対するセキュリティパッチは、定期的に サービス提供元で実施します。 [仮想サーバのパッチ適用] ●仮想サーバについては、利用者側で実施する必要があります。 ●共有ネットワークサービスで以下のアップデート環境が提供されます。 利用を検討してください。 - Red Hat Update Infrastructure (RHUI) - yumリポジトリミラーサーバ - WSUSサーバ [データベース仮想サーバのマイナーバージョンアップとパッチ適用] ●自動マイナーバージョンアップオプションを設定することで、データベースエンジンの マイナーバージョンアップが提供された場合に、バージョンアップを自動で行うことが できます。 ●データベース仮想サーバに対するセキュリティパッチは、2017年1月時点では 制限事項により適用できません。

2-3. 運用・保守性で検討する項目 (5/7)

FUJITSU

項目	要件	対応
2-3-2 保守運用(つづき)	データベース運用	[データベースサービスの運用] •データベースサービスで配備されるデータベース仮想サーバの管理は、富士通(IaaS)側で行います。 •データベース仮想サーバ自体には、SSH や リモートデスクトップ を利用してアクセスすることはできません。 •データベースサービスの運用管理はAPIで行います。 •管理者権限が必要なプロシージャやテーブルへのアクセスは制限されています。
	メンテナンス	[メンテナンス環境] •インターネット経由でサービスポータル、APIからの操作が可能です。 •API操作にはcurlの実行環境が必要です。（Cygwin　など） •API操作時のエンドポイント利用時はTLS/1.2を指定可能です。 [仮想サーバの接続] •Linux：SSH接続でのリモート操作。 •Windows：RDP接続でのリモート操作。

2-3. 運用・保守性で検討する項目 (6/7)

FUJITSU

項目	要件	対応
2-3-3 障害時運用	データベース障害	[データベースサービスの耐障害性向上～フェイルオーバ] ●データベースサービスは、Mastar/Standby構成を適用することで、 同一AZまたは別AZに待機系のデータベース仮想サーバが作成されます。 ●主系のデータベース仮想サーバが利用不可になったことを検知した際には、 自動でフェイルオーバ処理を行って、待機系のサーバに切り替わります。 (切替時間は約1～5分程度) [データベースサービスのデータの復旧方法] ●データベースサービスの復旧方法には、以下の2通りの方法があります。 ①自動バックアップデータからの ポイントインタイムリカバリ ②スナップショットのデータからの 新規データベース仮想サーバ作成
	仮想サーバ障害	[スナップショットで取得したデータからのリストア] ●仮想サーバをスナップショットからリストアする際は、APIを利用することにより、 配備されている仮想サーバをスナップショットの時点に置き換えて復元可能です。 ●サービスポータルでは、配備されている仮想サーバの復元はできません。 サービスポータルでは、スナップショットから新規仮想サーバの作成のみ可能です。

2-3. 運用・保守性で検討する項目 (7/7)

FUJITSU

項目	要件	対応
2-3-4 運用環境	ハイブリッド構成	[ネットワーク性能] ●バッチ処理等をオンプレミス側のシステムとネットワーク越しに行う場合、大量のネットワーク通信により、通信がボトルネックとなり処理時間に影響を与える可能性があります。設計時には十分留意してください。
2-3-5 サポート体制	サポートメニュー	[ヘルプデスクの選定] ●利用したいサービスの内容に合わせて、ライト/スタンダード/プレミアムのヘルプデスクメニューを選択（契約）してください。 ※詳細はヘルプデスクサービス仕様書を参照してください。 ●ヘルプデスクサービス契約は必須です。 [OSサポートの選定] ●OSのサポートは、システム要件や運用要件に合ったサポートを利用者側で設定してください。 ●Windows:24時間365日、平日9時～19時、ノンサポートより選択 ●RHEL:24時間365日、平日8時30分～19時より選択 ※詳細はソフトウェアサポート仕様書を参照してください。

2-4.　セキュリティで検討する項目

IaaSで提供される仮想サーバ、ストレージ、ネットワークのセキュリティについて記載します。

2-4. セキュリティで検討する項目 (1/5)

FUJITSU

項目	要件	対応
2-4-1 アクセス・利用制限	利用権限(ロール)	[用途に応じた利用権限の設定] •契約者、全体管理者、設計・構築者、運用者、監視者、一般ユーザなどの権限を設定したロールを提供します。
	利用者アクセス	[利用者アクセスの設定] •ユーザーID/パスワードによるアクセス制御を行います。 •利用者パスワード有効期限は90日間です。 •APIトークンの有効期限は3時間です。
	サービスポータルアクセス	[サービスポータルへのアクセス] •リージョン/契約番号/ユーザーID/パスワードで認証を行います。
	APIエンドポイントアクセス	[APIエンドポイントへのアクセス] •ドメインID/ユーザーID/パスワードで認証を行い、APIエンドポイントでトークンを発行し、IaaS基盤へのアクセスを許可します。 •15分間内に連続で5回を超えるパスワードエラーが検知された場合は、15分間は認証エラーになります。

2-4. セキュリティで検討する項目 (2/5)

FUJITSU

項目	要件	対応
2-4-1 アクセス・利用制限 (つづき)	仮想サーバへのアクセス	[仮想サーバの管理者ユーザパスワード設定とログイン] •Linux 登録済みキーペアを、仮想サーバ作成時に設定します。 設定したキーペアを使用して仮想サーバにSSHでログインします。 •Windows 登録済みキーペアを、仮想サーバ作成時に設定します。 仮想サーバ作成時に設定したキーペアの鍵ファイルを利用して、 APIで、システム側で設定されたランダムパスワードを入手します。 入手したランダムパスワードを使用して、仮想サーバにRDPでログインします。 •キーペアを再ダウンロードする事はできません。

2-4. セキュリティで検討する項目 (3/5)

FUJITSU

項目	要件	対応
2-4-2 データの秘匿	通信データの暗号化	[ネットワーク経路の暗号化] ●オンプレミス環境とIaaS間とのデータ送受信等でインターネットを利用する場合は、データを暗号化する IPSecVPN機能を検討してください。 ●HTTPSプロトコルによるHTTP通信の暗号化を検討してください。ロードバランサーを使用することにより、HTTPSプロトコルの暗号化処理を、ロードバランサーに任せることができます。 ●インターネット環境よりIaaS環境の仮想サーバへセキュアな通信を行う際は、SSL-VPN機能の利用を検討してください。 ※より機密性の高いデータの送受信が必要な場合は、FJcloud-O DEX（旧プライベート接続オプション）で構内接続を検討してください。
	蓄積データの暗号化	[ストレージの機能による暗号化] ●以下のデータは、物理ディスクへの書き込み時に暗号化しています。 - システムストレージ - 増設ストレージ - スナップショットデータ - 仮想サーバイメージ - オブジェクトストレージ [データベースサービスの暗号化] ●データベースサービスにおいて、テーブル内のデータの暗号化は未対応です。 ※物理ディスクへの書き込み時に暗号化しています。 [ファイル単位の暗号化] ●仮想サーバ上のファイルの単位で暗号化が必要な場合は、個別にソフトウェアの導入を検討してください。

2-4. セキュリティで検討する項目 (4/5)

FUJITSU

項目	要件	対応
2-4-3 不正追跡・監視	不正追跡	[追跡/証跡用のログ取得] ●仮想サーバのシステムログ、アプリケーションログについては、オンプレミスのシステムと同様に、個別に検討してください。 ●サービスポータル、APIの操作ログは、利用者には提供しておりません。
	監視	[リソースのモニタリング] ●監視サービスによるモニタリングデータは2週間保持されます。 [独自監視項目のモニタリング] ●カスタムメータによる独自監視項目のモニタリングを検討してください。 [アラーム通知] ●アラーム通知機能によるしきい値条件でのメール通知などを利用した異常検知を検討してください。 [変更監視] ●IaaSの標準機能では提供していません。ファイルの変更監視は、オプションサービスの「FJcloud C1WS オプション」を利用することが可能です。

2-4. セキュリティで検討する項目 (5/5)

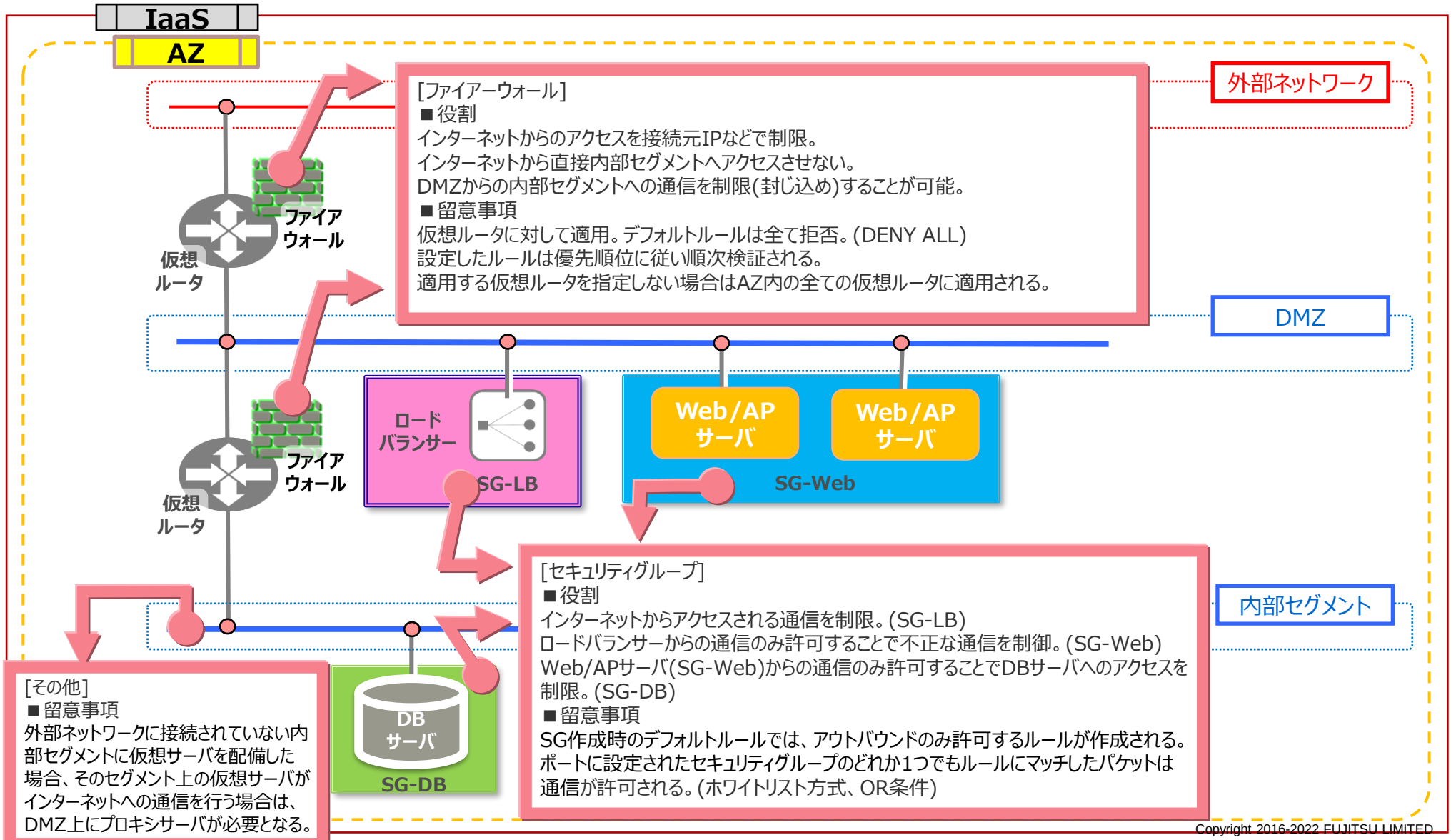
FUJITSU

項目	要件	対応
2-4-4 ネットワーク対策	ネットワーク制御 ※補足資料も参照してください。	[アクセス制御] •IaaSの標準機能のセキュリティグループとファイアーウォールを使用して、不正な通信からの防御が可能です。 •セキュリティグループとファイアーウォールは併用して設定することで、多段的なアクセス制御が可能です。 •データベースサービス で配備される データベース仮想サーバも、セキュリティグループによるアクセス制御が可能です。 •ファイアーウォール配備直後は、自動的に全てのアクセスを遮断するルールが適用されます。正しくフィルタリングルールを設定したうえで利用してください。 •セキュリティグループ作成時は、IaaSのデフォルトルールが適用されます。正しくフィルタリングルールを設定したうえで利用してください。
2-4-5 マルウェア対策	IDS/IPS	[OS/アプリケーションの脆弱性への対処] •SQLインジェクションなど、OSやアプリケーションの脆弱性を突いた攻撃に対する対策として、「FJcloud C1WS オプション」を利用することが可能です。
	ウイルス対策	[ウィルスへの対処] •トロイの木馬など、有益なプログラムを装って不正なプログラムを送りこむ攻撃への対策として、「FJcloud C1WS オプション」 を利用することが可能です。

補足)2-4-4.ネットワーク制御(FWとSG)

FUJITSU

■ファイアーウォール(FW)とセキュリティグループ(SG)を併用することで論理多層防御が可能。



2-5.　システム移行で検討する項目

IaaSで提供される移行サポートについて記載します。

2-5. システム移行で検討する項目

FUJITSU

項目	要件	対応
2-5-1 移行	移行方法	[仮想サーバインポート機能による移行] ●オンプレミス仮想環境で動作している仮想サーバのイメージファイル(VMDK形式) を採取し、IaaSにインポートすることでIaaSで利用可能なイメージファイルとして登録が可能です。
	移行可能OS	[仮想サーバインポート機能による移行対象OS例] ●主な移行可能OS • Windows Server 2012 SE 64bit (日本語版) • Windows Server 2012 SE R2 64bit (日本語版) • RHEL7 64bit • CentOS 6.5 64bit • Ubuntu 14.04 LTS 64bit 詳細な情報、最新の情報は マニュアル IaaS機能説明書 コンピュート/スタンダードサービス/仮想環境間の移行 を参照願います。 https://doc.cloud.global.fujitsu.com/lib/iaas/jp/function-manual/index.html
	移行対象	[仮想サーバインポート機能による移行対象データ] ●システムディスクのみが対象になります。

付録　A-1.参考資料

IaaSで使用されるマニュアル類について記載します。

A-1.参考資料

[マニュアル]
https://doc.cloud.global.fujitsu.com/jp/iaas/index.html

- ■IaaS機能説明書
- ■サービスポータルユーザーズガイド
- ■IaaS API ユーザーズガイド
- ■IaaS API リファレンスマニュアル
- ■IaaS HEATテンプレート解説書
- ■ Trend Micro Cloud One - Workload Securityインストールガイド（※旧称　Trend Micro Deep Security as a Service インストールガイド　）

[利用規約]
https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/document/

- ■利用規約

[サービス仕様書]
https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/document/

- ■IaaS サービス仕様書
- ■プライベート接続サービス仕様書（又はDigital enhanced Exchangeサービス仕様書）
- ■ヘルプデスクサービス仕様書
- ■ソフトウェアサポート仕様書
- ■サービスレベル仕様書

上記マニュアル類につきましては、FUJITSU Hybrid IT Service FJcloud-Oのページより、
最新バージョンを常に入手するようにしてください。

https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/

付録　B-1.用語説明

IaaSで使用される用語について記載します。

B-1.用語説明

用語	説明
アベイラビリティゾーン(AZ)	データセンター設備やサービス提供用設備などの物理的な施設を共有する単位。
イメージ	配備済の仮想サーバより、固有情報を削除した雛形を用意し容易に仮想サーバの複製が行える機能。
APIエンドポイント	クライアントが API にアクセスするための通信の接続先。
オートスケール	システム負荷などの条件に従って、仮想サーバの増減を自動的に制御する機能。
フェイルオーバ	サービス提供環境でハードウェアトラブルなどが生じた場合、自動的に他のハードウェアでサービスを再開する仕組み。
オブジェクトストレージ	オブジェクト(コンテンツとメタデータからなる)単位で分割保存するストレージ。
外部ネットワーク	インターネットに接続するためにIaaS側で用意したネットワーク。
カスタムメーター	利用者が独自の監視項目を登録しモニタリングする機能。
仮想ネットワーク	仮想サーバなどのリソースが通信するための仮想的なネットワーク。サブネットに対応して作られる。
仮想ルータ	外部ネットワークとネットワーク、またはネットワーク同士を接続する機能。
キーペア	仮想サーバへSSHでログインする場合や、Windowsのランダムパスワードを暗号化するために使われる公開鍵と秘密鍵の組み合わせ。仮想サーバには公開鍵のみが登録される。
コネクタエンドポイント(CEP)	アベイラビリティゾーン内の内部ネットワークからネットワークコネクタへ接続するための接続口。
サブネット	ネットワークの論理分割単位。配備されるリソースに対してプライベートIPアドレスの管理、DHCP機能、ルーティング管理などを提供します。
スナップショット	ブロックストレージの状態をあるタイミングで抜き出したもので、バックアップなどに利用することが可能。
セキュリティグループ	仮想サーバに接続されたポートに対してパケットフィルタリングを行うルールをグルーピングする機能。
トークン	API操作を行う場合に必要な認証情報。
ドメイン	IaaSの契約の単位を示すもの。DNSのドメイン名とは異なる単位。

B-1.用語説明(つづき)

FUJITSU

用語	説明
内部ネットワーク	インターネットに接続されていないネットワーク。
ネットワークコネクタ(NWC)	アベイラビリティゾーンを越えたネットワーク同士(アベイラビリティゾーン間やオンプレミス環境との接続など) を接続するための機能で、各ネットワーク同士はコネクタエンドポイントを通して通信が行われる。
ファイアーウォールサービス(FW)	仮想ルーターに対するパケットフィルタリングルール。
プロジェクト	ドメイン内で仮想リソースの管理を分割し、ユーザやグループ毎に異なる操作権限(ロール)を設定できる単位。
ブロックストレージ	システムストレージ、増設ストレージとして利用可能なデバイス。
ポート	仮想サーバなどリソースをネットワークに接続するため、IPアドレスとの関連付けを行うネットワークインターフェース。
リージョン	各国または国内における東西、南北など地域的に隔離された単位。
ロードバランサー(LB)	仮想サーバへのトラフィックを複数の仮想サーバへ分散処理します。

Thank you