AWSにおける
ガバメントクラウドへの接続

小林 竜也
アマゾン ウェブ サービス ジャパン 合同会社
パブリックセクター 技術統括本部
ソリューションアーキテクト

自己紹介

小林 竜也 (こばやし たつや)

- 公共に属するお客様を担当している
  パブリックセクター　技術本部にて主に自治体のお客様の
  クラウド活用支援を担当

- 前職はシステムインテグレータに在籍、
  自治体様を中心に防災、防犯ソリューションの構築等の技術支援を担当

- 自治体のお客様のクラウド移行支援や
  新しいクラウドの活用のお手伝いをしています

- 趣味は、Crossfitという身体を動かす競技スポーツをやってます

内容についての注意点

本資料では 2024年 4月 時点でのサービス内容および価格に基づいたスライドや説明になっています。最新の情報は AWS 公式ウェブサイト (http://aws.amazon.com) にてご確認ください。

資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます。

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

アジェンダ

- AWSとガバメントクラウドの接続について
- 構成パターン例

AWSとガバメントクラウドの接続について

自治体のマイナンバー利用事務系ネットワークとの接続

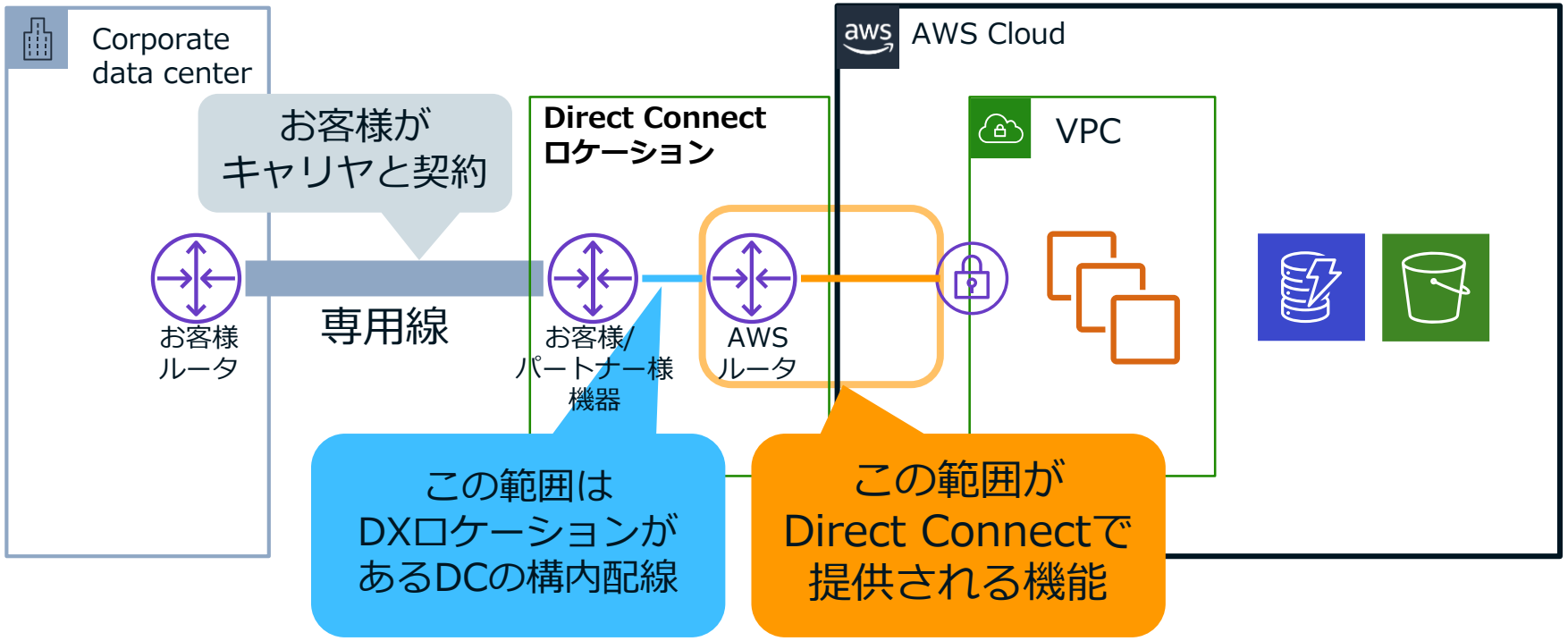
- 総務省の情報セキュリティポリシーガイドライン改定方向性
  - マイナンバー利用事務系ネットワークを専用回線（AWSでは**Direct Connect** を指す）を使って接続した領域は、マイナンバー利用事務系として扱う

3．情報システム全体の強靭性の向上	
○情報システム全体の強靭性の向上	・地方公共団体は、マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるクラウドサービス上の情報システムの領域については、マイナンバー利用事務系として扱い、当該地方公共団体の他の領域とはネットワークを分離する。 ・LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、マイナンバー利用事務系とネットワークを分離し、そのアクセスにおいては、LGWAN接続系の端末から接続する。 【ガバメントクラウド個別事項】 ガバメントクラウドでは、マイナンバー利用事務系、LGWAN接続系の情報システムが稼働する環境は、インターネット接続が出来ない設定があらかじめ行われている。

参考: https://www.soumu.go.jp/main_content/000825774.pdf

AWS Direct Connectとは

お客様がキャリヤから調達する専用線の片端とAWS Cloudを、Direct Connectロケーションで接続するサービスです。日本のDirect Connectionロケーションは、東京(Equinix TY2、アット東京 CC1）大阪（Equinix OS1)と印西（NEC印西)にあります。



仮想インターフェイス（Virtual Interface = VIF）

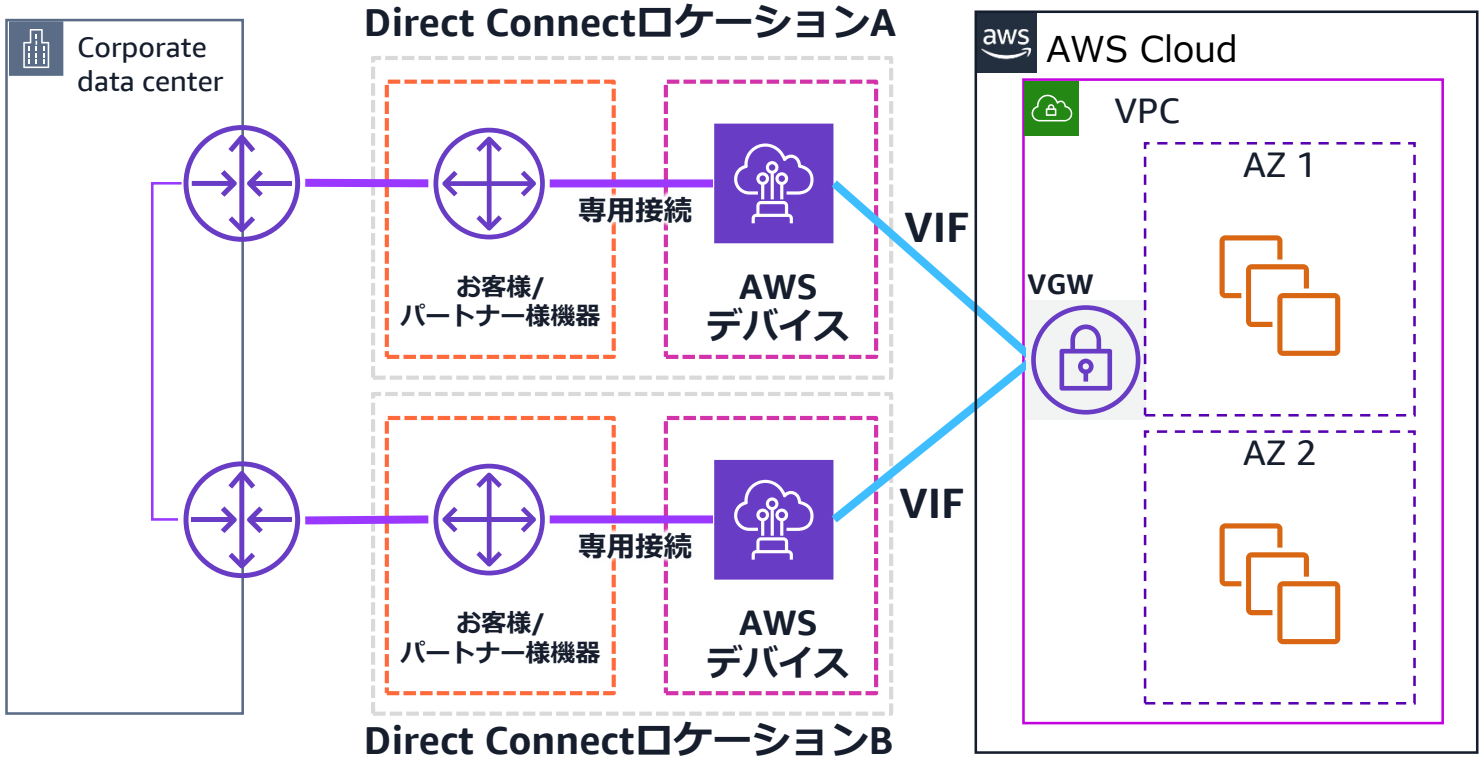
Connection(接続) = 物理接続（1/10/100G）
VIF = Connectionを通してAWSリソースにアクセスするための論理インターフェイス
- AWSとお客様ルータの間でBGPピアを確立し経路交換をするために必要
- VLAN IDをもつ

- **プライベートVIF：**VPCへプライベートIPを介した接続を提供
- **パブリックVIF：**AWSの全リージョンへパブリックIPを介した接続を提供
- **トランジットVIF：**Transit Gateway用のDirect Connectゲートウェイへ接続を提供

ベストプラクティス：クリティカルなワークロードの高い回復性

- AWS Direct Connect の回復性に関する推奨事項
  https://aws.amazon.com/jp/directconnect/resiliency-recommendation

お客様の大切なワークロードを担うネットワークとして、シングルポイントを作らない事が重要。そのための推奨構成を以下に記載します。



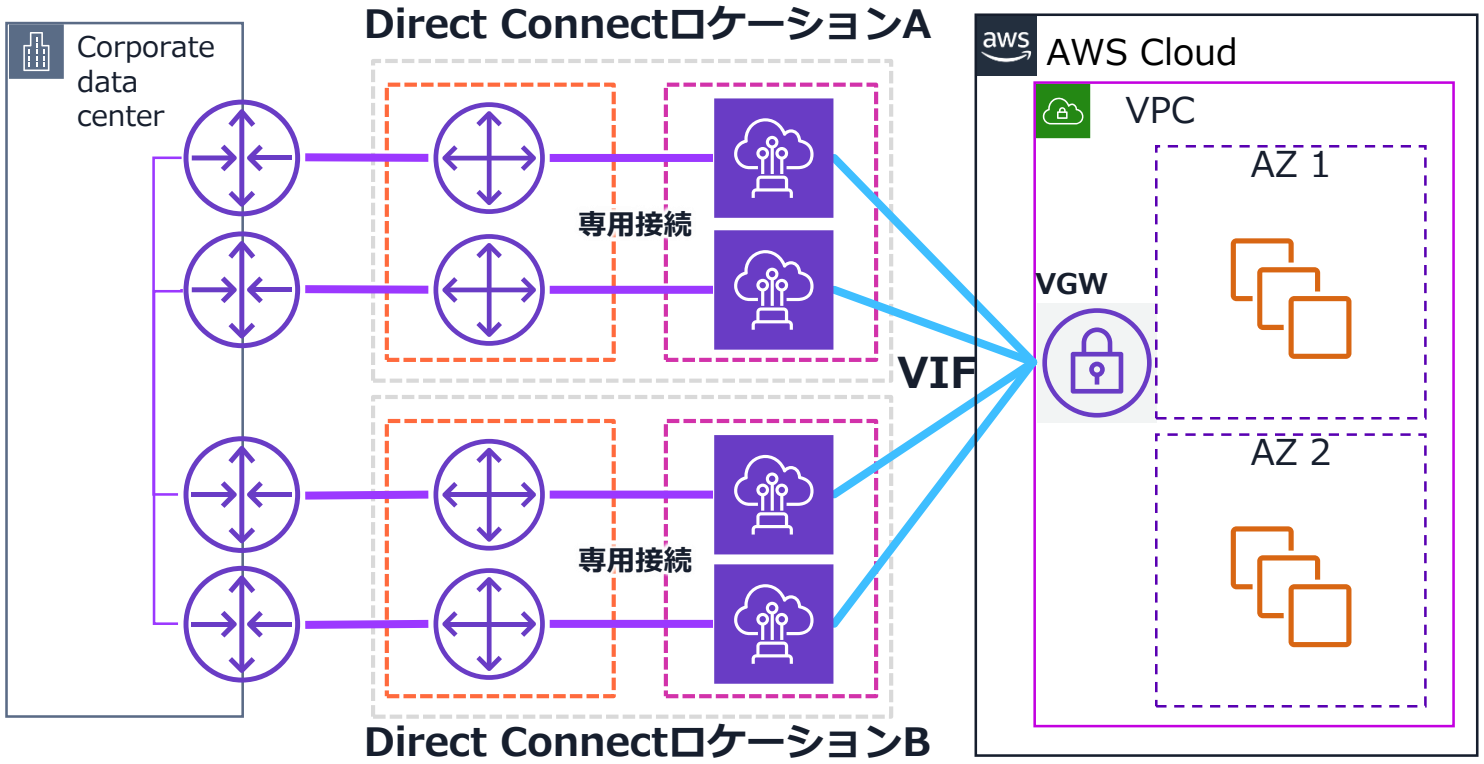
- Active-Active、Active-Standbyは問わない
- Direct Connectゲートウェイ、Transit Gatewayも利用可能

SLA 99.9%要件

- 2つのロケーションに接続を配置
- エンタープライズサポート契約に加入
- AWS上のリソースをマルチAZ化

ベストプラクティス：クリティカルなワークロードの最大回復性

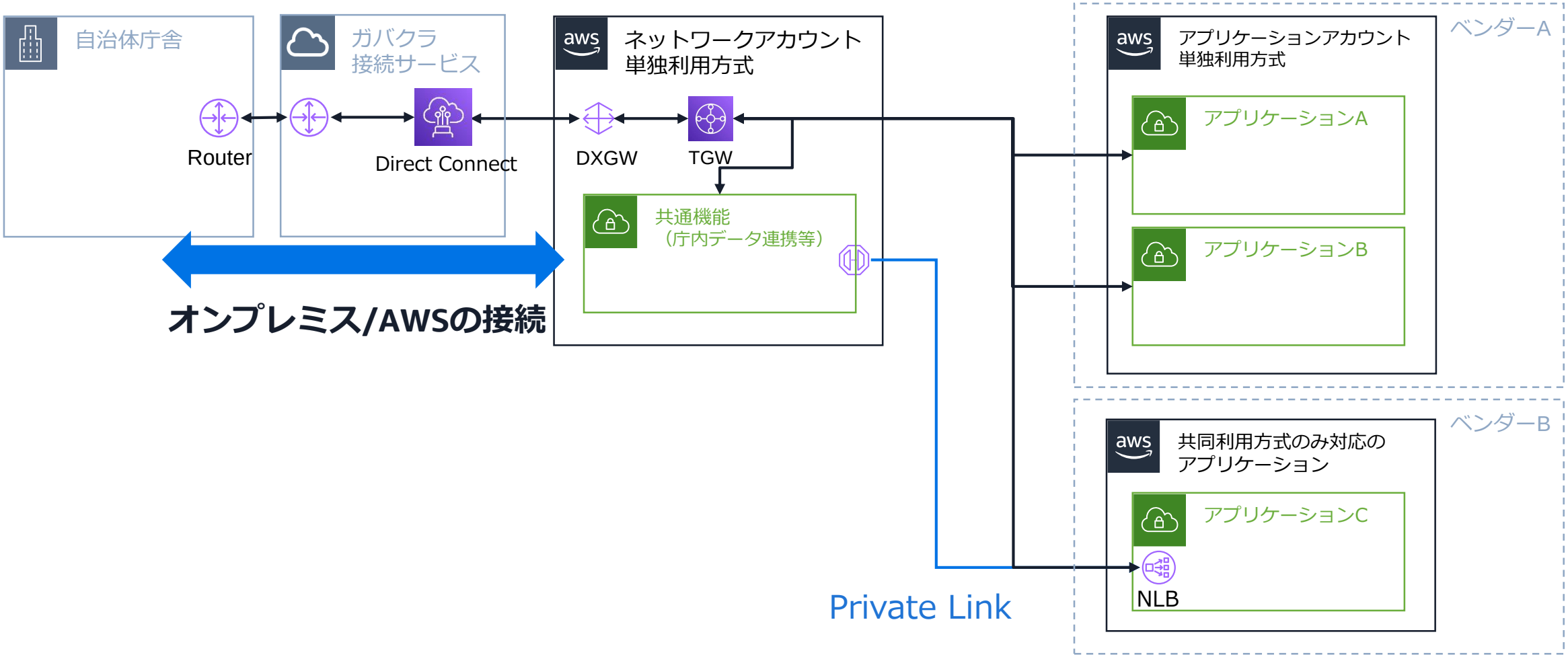
- AWS Direct Connect の回復性に関する推奨事項
  https://aws.amazon.com/jp/directconnect/resiliency-recommendation



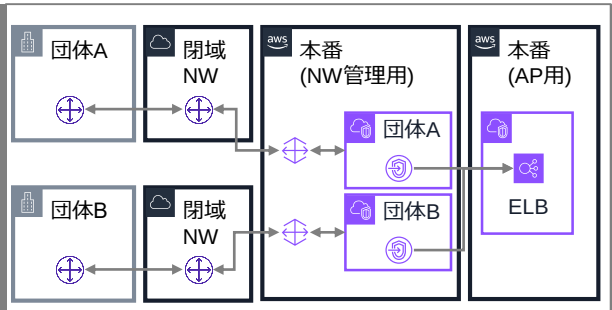
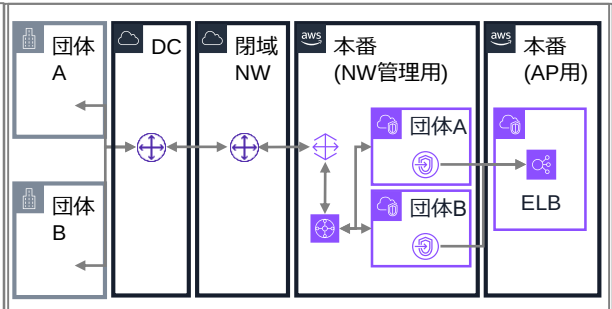
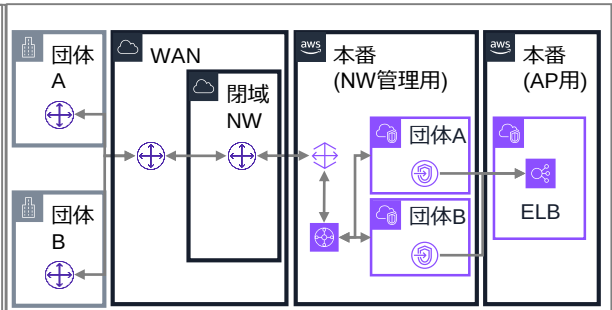
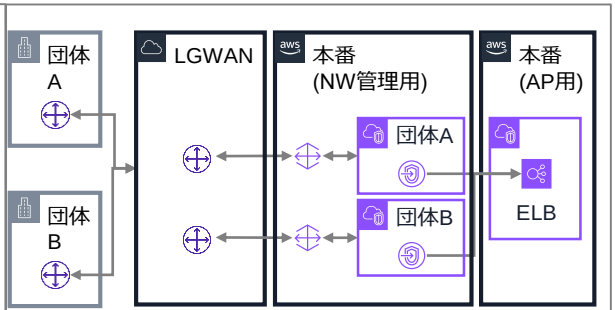
SLA 99.99%要件

- 2つのロケーションに各2つの接続、合計4つの接続を配置
- エンタープライズサポート契約に加入
- AWS上のリソースをマルチAZ化
- SAによるW-Aレビュー

庁舎 – クラウド接続



ガバメントクラウドへの接続方法

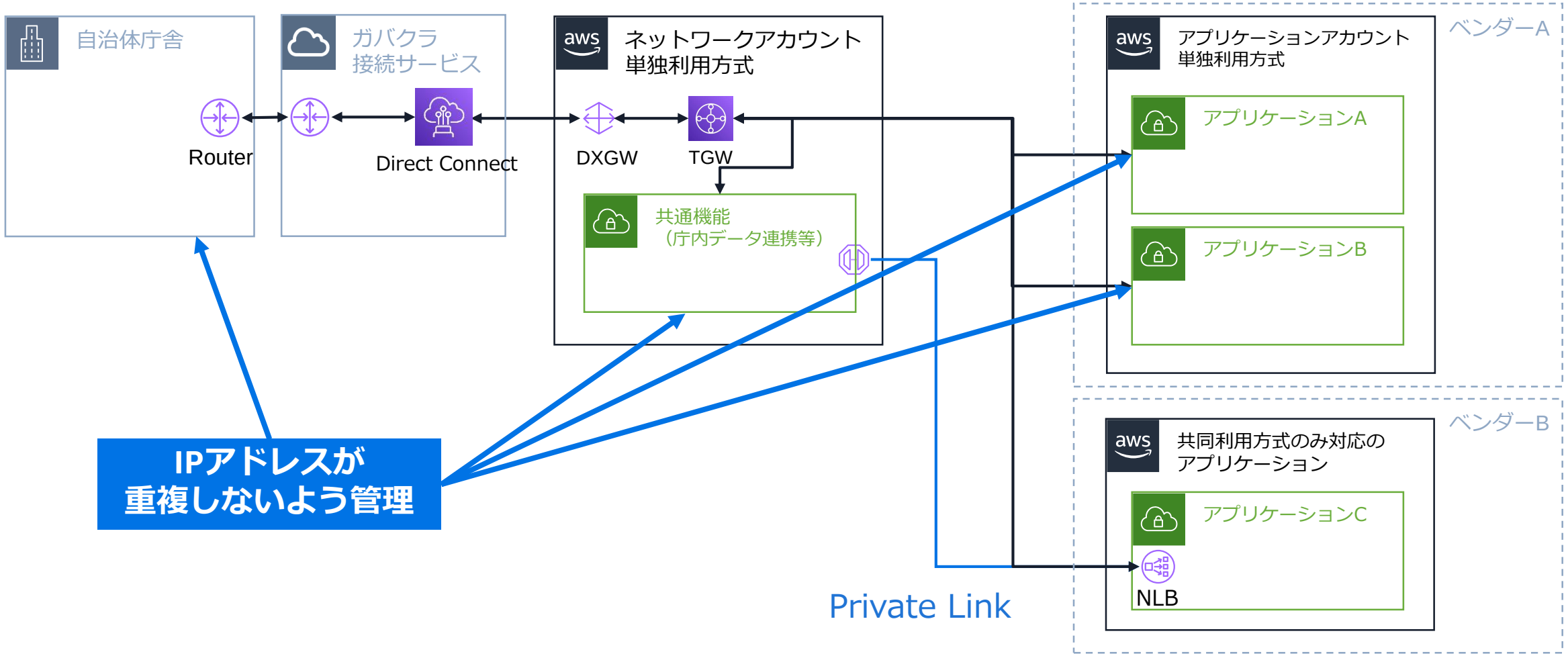
	1．地方公共団体から専用線で接続する方法	2．ASPのデータセンターから専用線で接続する方法	3．都道府県WANを経由して接続する方法	4．LGWANを経由して接続する方法
概要	• 各地方公共団体から個別に専用線・Direct Connectを敷設し、ガバメントクラウドへ接続する	• 既存の地域回線等を利用し、各地方公共団体からDCへ専用線接続を集約する • 既存DCを管理する事業者とガバメントクラウド運用管理補助者が同一の場合を想定	• 地方公共団体において都道府県WAN運用事業者の回線を利用する	• 各地方公共団体からLGWANを利用し、ガバメントクラウドへ接続する
特徴	• アドレス設計や契約を団体ごとに調整可能であるため、個別の事情に応じた柔軟な対応が可能となる	• 個別に接続する場合と比較して、回線費用の負担を抑えられる可能性がある • 新規に敷設する回線はDCとガバメントクラウド間のみであるためイニシャルコストを抑えられる	• 個別に接続する場合と比較して、回線費用の負担を抑えられる可能性がある • 新規に敷設する回線は都道府県WANとガバメントクラウド間のみであるためイニシャルコストを抑えられる	• ガバメントクラウドに接続するためのクラウド接続サービスはLGWANで構築予定のため、クラウド接続サービスに係る新規調達等が不要になりイシャルコストを抑えられる可能性がある
考慮事項	• 回線を共同利用する場合と比較して、回線費用の負担が大きくなる可能性がある	• 団体間でIPアドレス帯が重複する場合はトンネリングやアドレス変換等の対応が必要となる • 各団体の接続を集約する部分では、十分な可用性・性能を確保する必要がある	• 団体間でIPアドレス帯が重複する場合はトンネリングやアドレス変換等の対応が必要となる • 各団体の接続を集約する部分では、十分な可用性・性能を確保する必要がある	• アクセス回線区間の帯域について、ガバメントクラウドにおけるネットワークの通信量等を考慮し再検討する必要がある
構成				

ガバメントクラウドのネットワーク設計の注意点

- ガバメントクラウドで AWS を利用する場合、AWS 上で使用する IP アドレス範囲はお客様側で自由に決定が可能です。
- 一部の共同利用方式では ASP と連携しながら IP アドレスを決める必要があります。
- 一方で、AWS とオンプレミス (庁舎など) は L3 レベルで接続されるため、AWS に割り当てる IP アドレスは**オンプレミスで使用していない IP アドレス**である必要があります。
- そこで、ガバメントクラウドを利用するにあたってはオンプレミスで使用していない IP アドレス範囲を確認し、各利用領域に割り当てる必要があります。
- またVPC の CIDR ブロックは**1度作成すると変更することが困難**のため、CIDR 設計は、十分な検討が必要不可欠です。

https://aws.amazon.com/jp/blogs/news/govcloud-hint-for-network-cidr/

IPアドレスが重複しないように管理

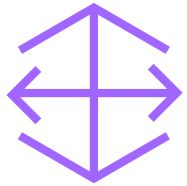


構成パターン例
(弊社考え)

考慮事項

- 単独利用方式/共同利用方式
- 共同利用方式の場合の環境分離方式
  - アプリケーションレベル、VPCレベル、AWSアカウントレベル
- 各自治体 – AWSアカウントのネットワーク経路

AWS用語の簡単な解説

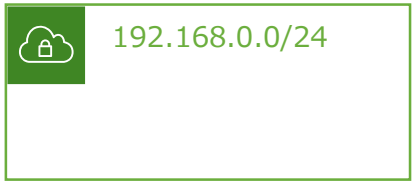


Direct Connect Gateway
(DXGW)

- Direct Connectからの接続（VIF）を束ねることができる
- Transit VIFという種類の回線を利用した場合、Transit Gatewayに紐づけが可能

AWS Transit Gateway
(TGW)

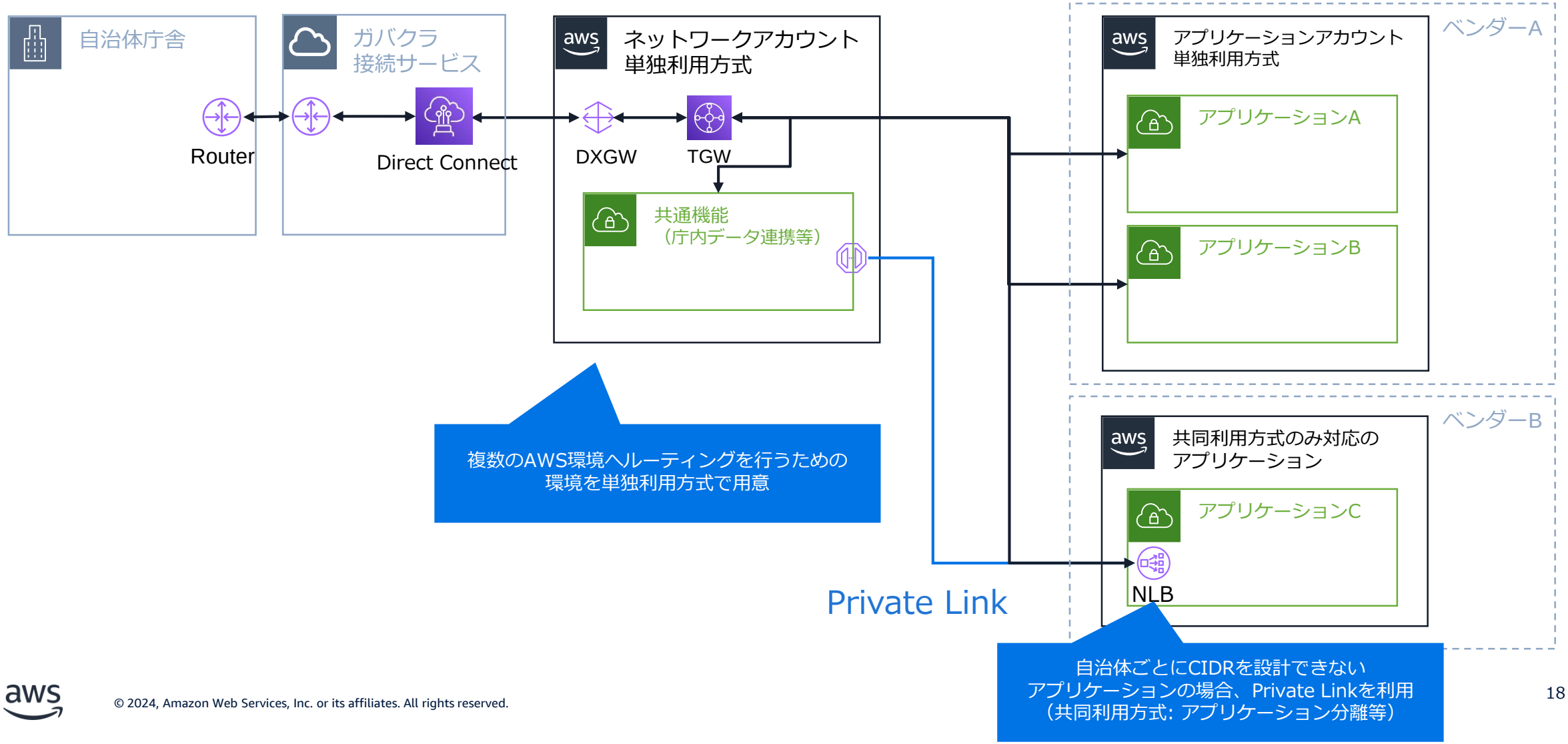
- AWS内のルーターのようなサービス
- VPCやオンプレミスへのルーティングが可能



Amazon VPC

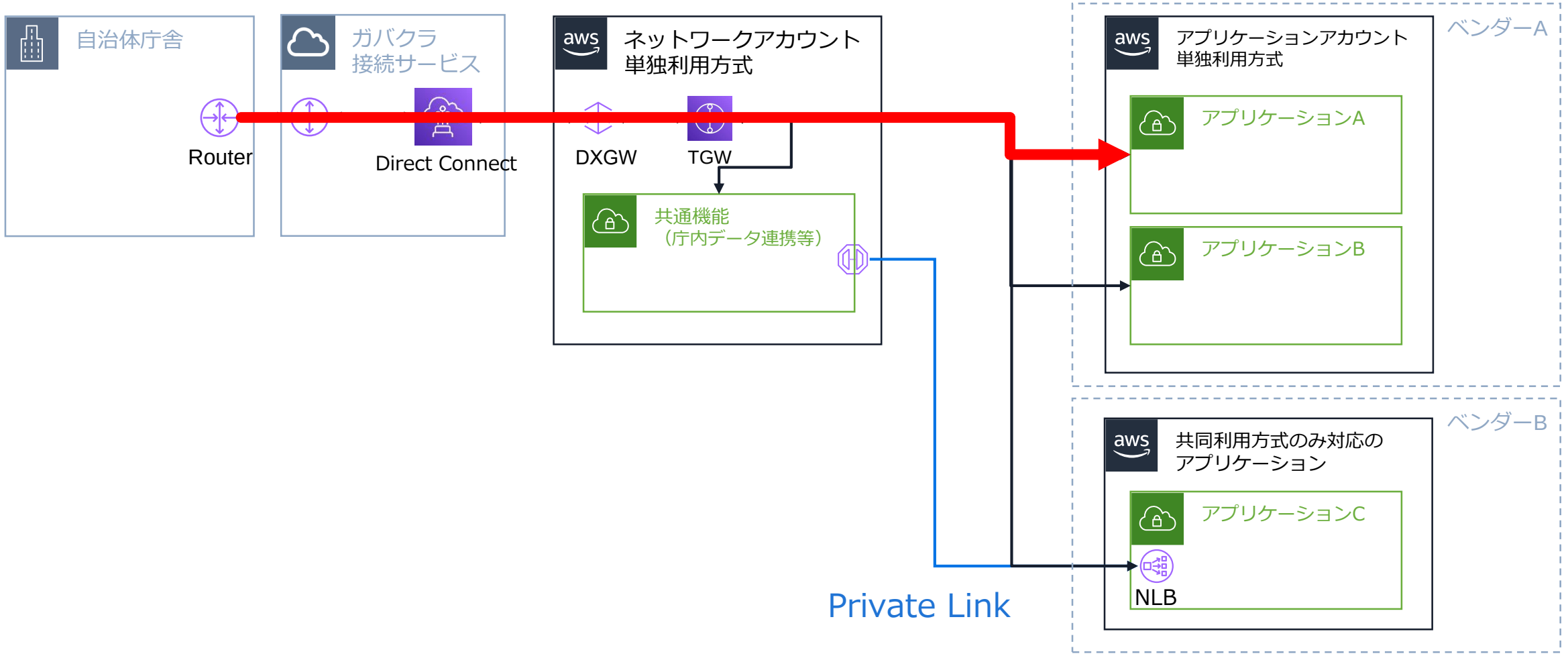
- AWS内の仮想ネットワーク領域
- CIDRを設定し、お客様専用のネットワーク領域として扱うことができる

単一自治体/複数ベンダー – AWS



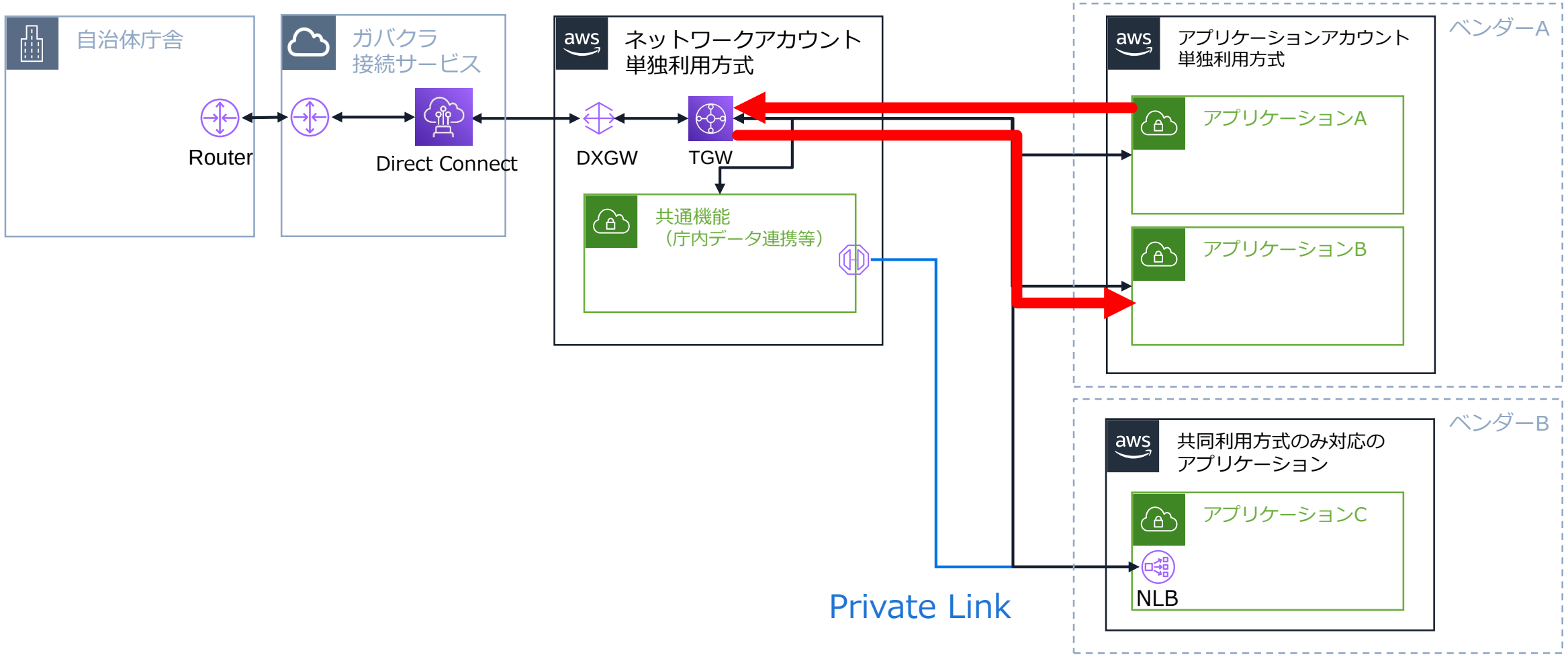
単一自治体/複数ベンダー – AWS

オンプレミス – AWSの通信



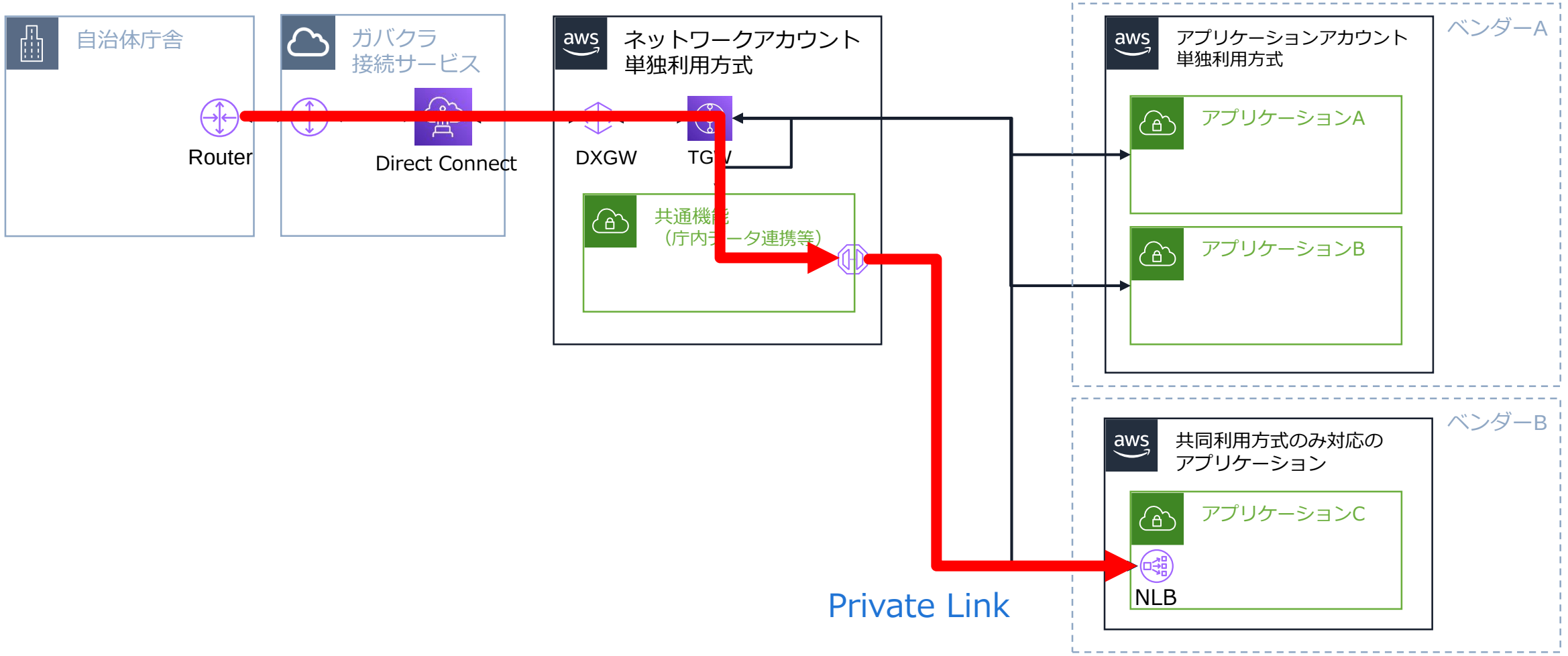
単一自治体/複数ベンダー – AWS

VPC間の通信

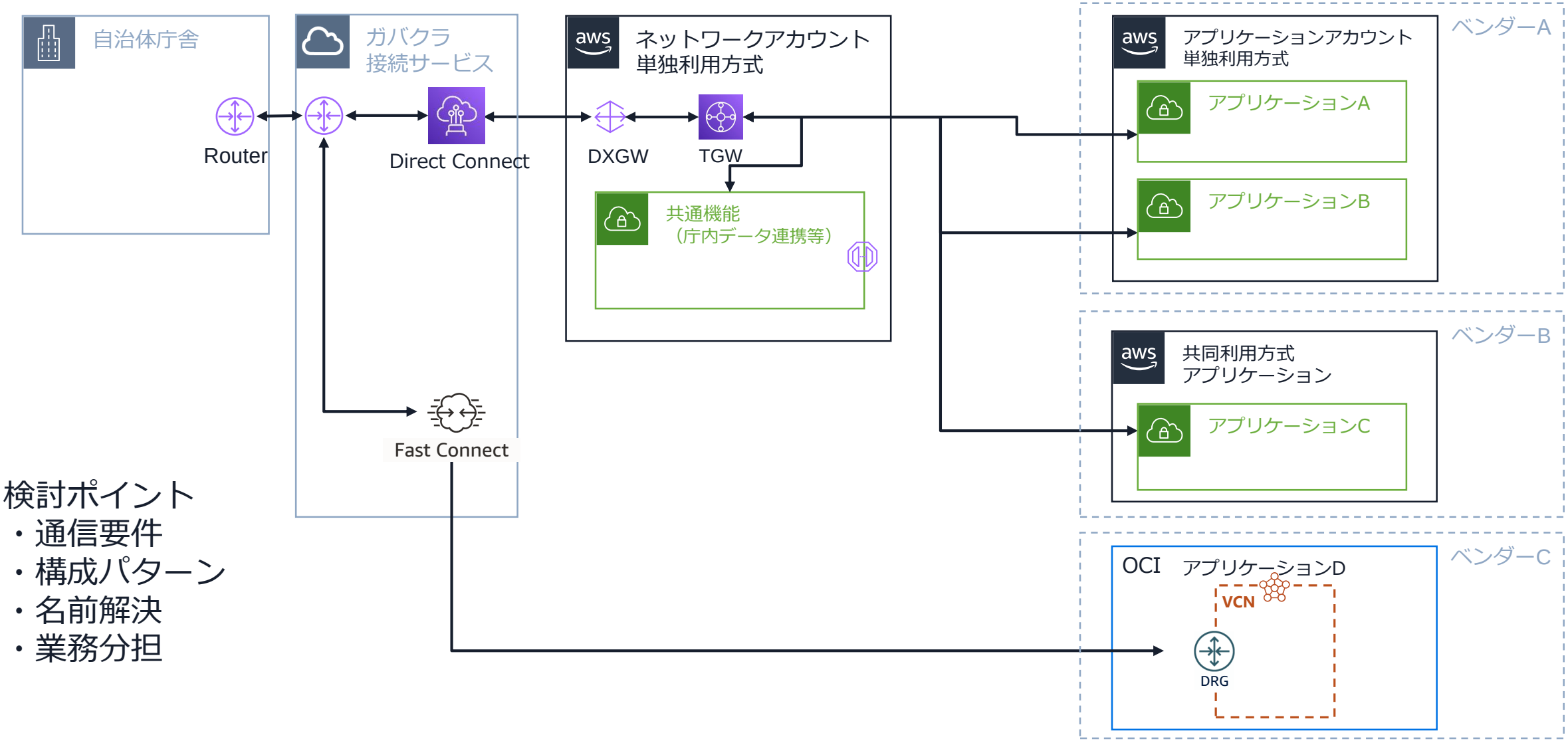


単一自治体/複数ベンダー – AWS

Private Link を利用した共同利用アプリケーションへの通信

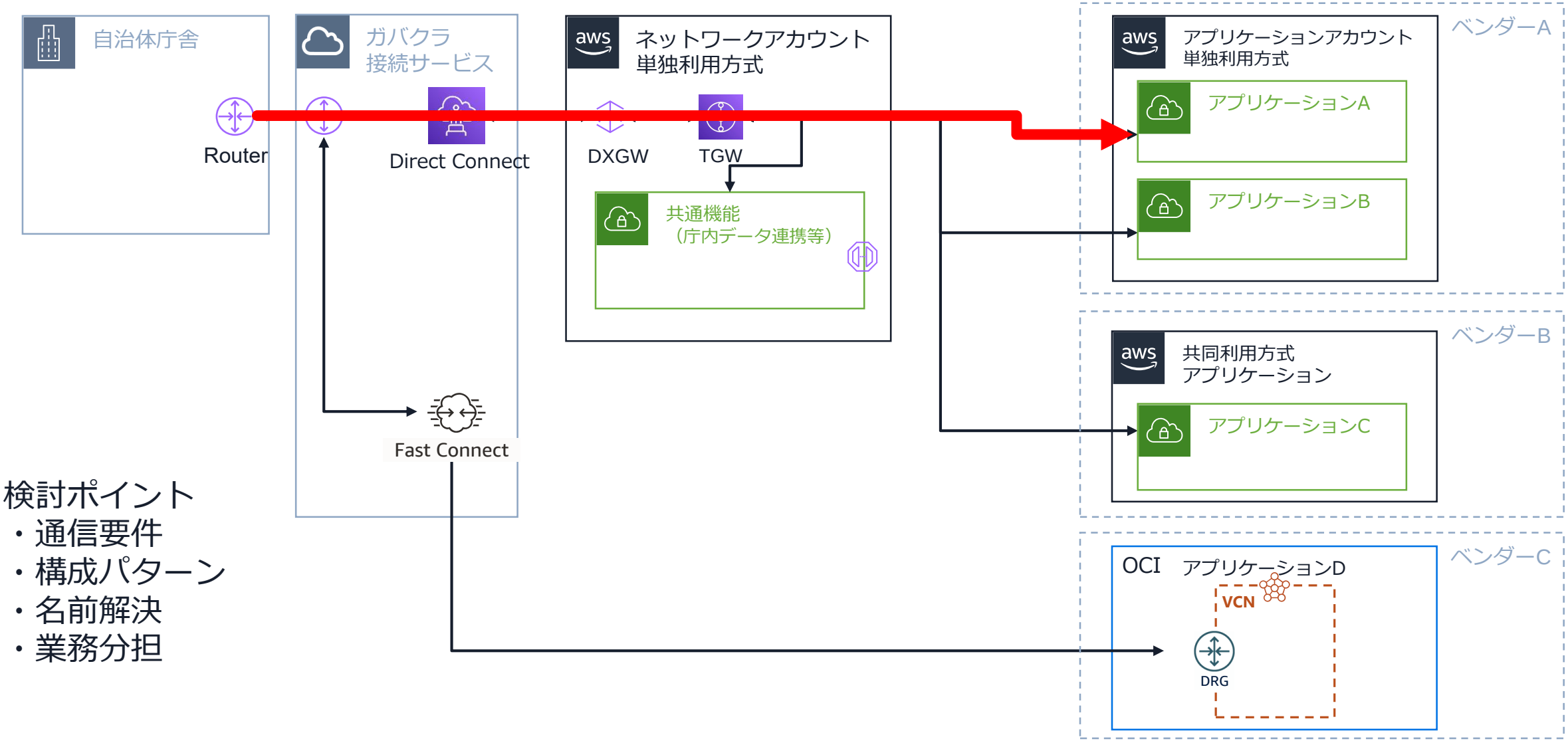


単一自治体/複数ベンダー – マルチCSP



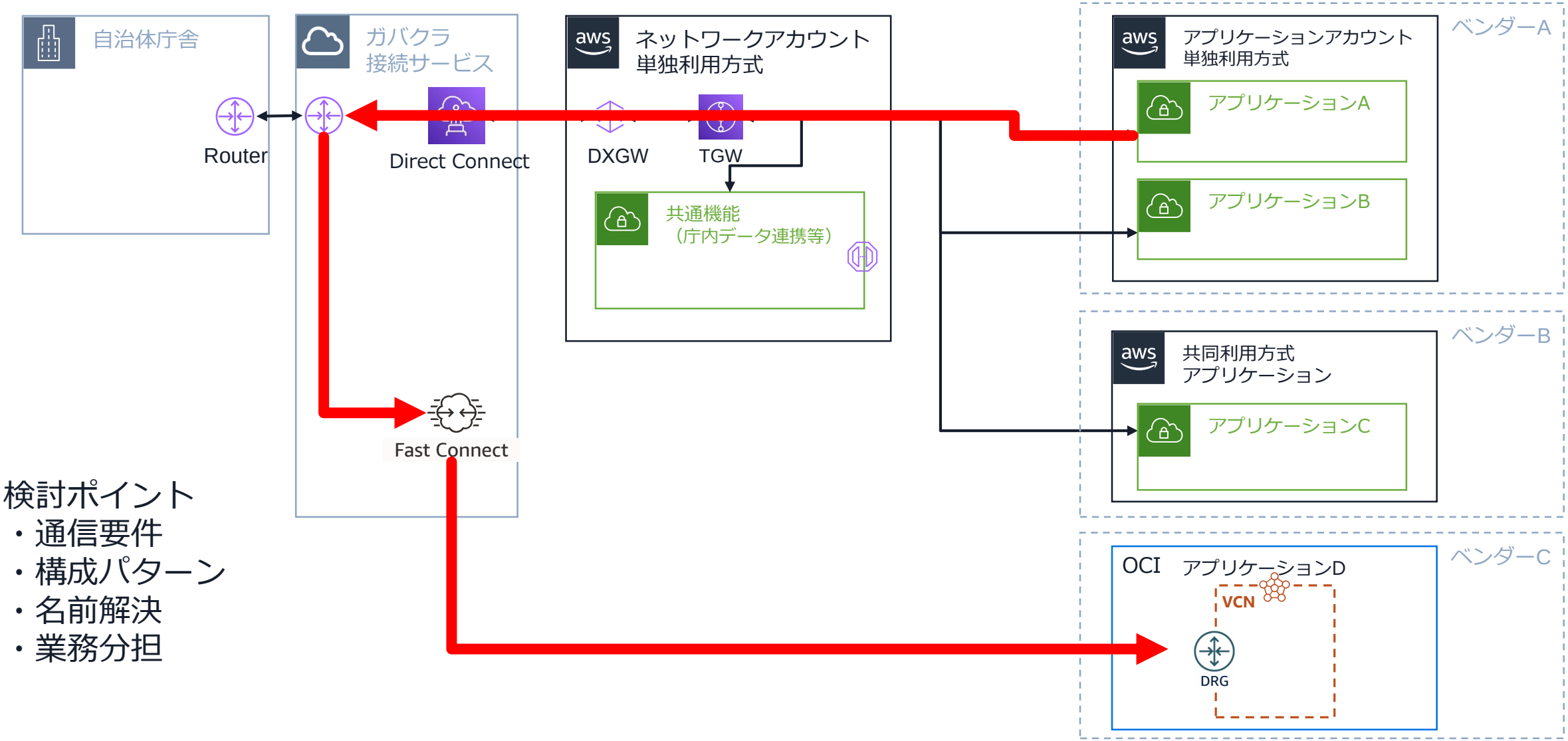
検討ポイント
- 通信要件
- 構成パターン
- 名前解決
- 業務分担

単一自治体/複数ベンダー – マルチCSP



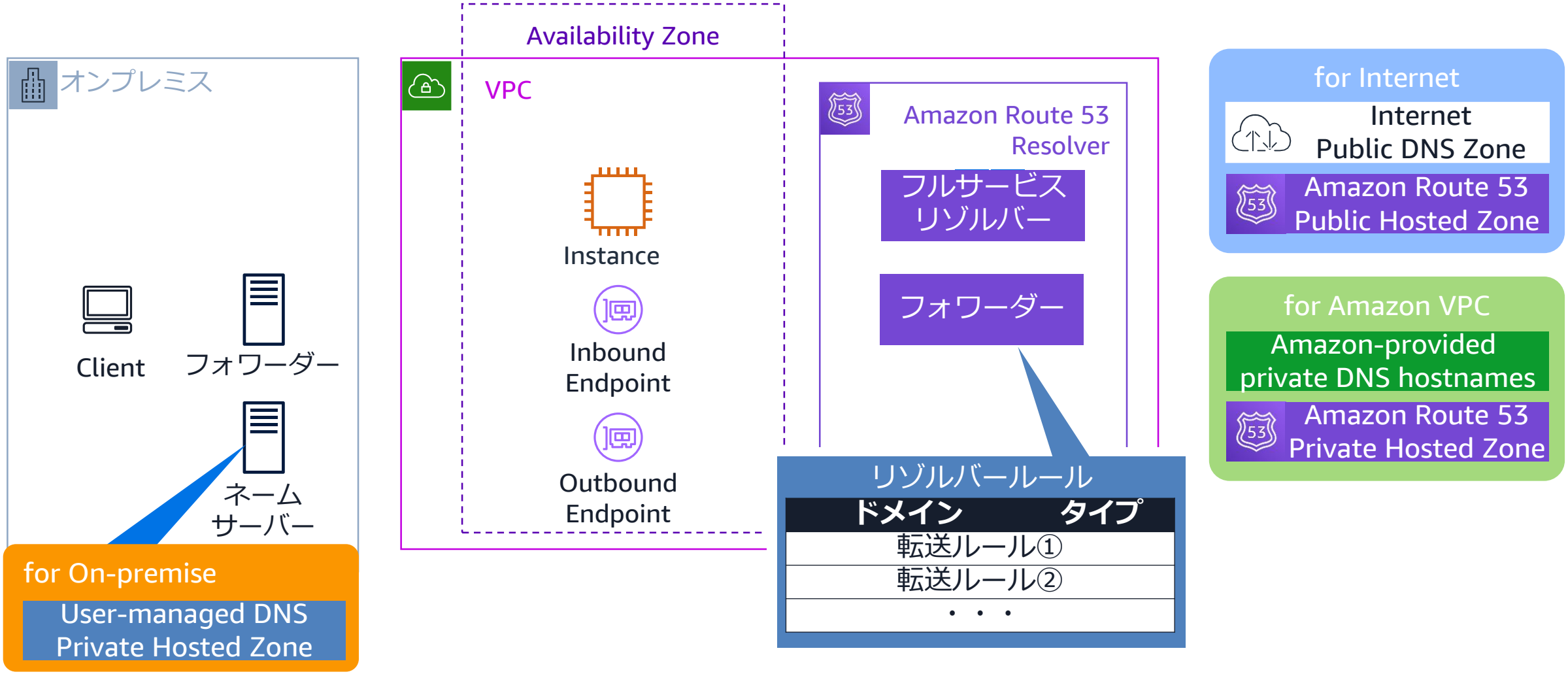
検討ポイント
- 通信要件
- 構成パターン
- 名前解決
- 業務分担

単一自治体/複数ベンダー – マルチCSP

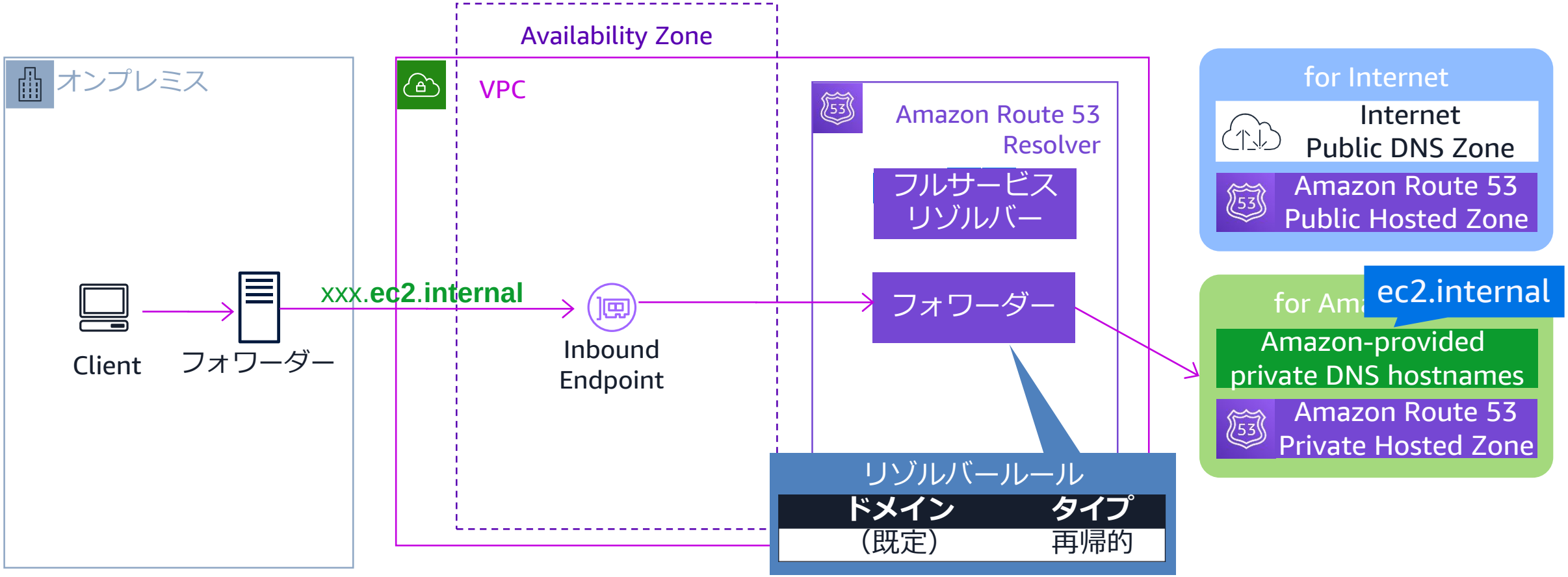


検討ポイント
- 通信要件
- 構成パターン
- 名前解決
- 業務分担

名前解決について：Route 53 Resolver

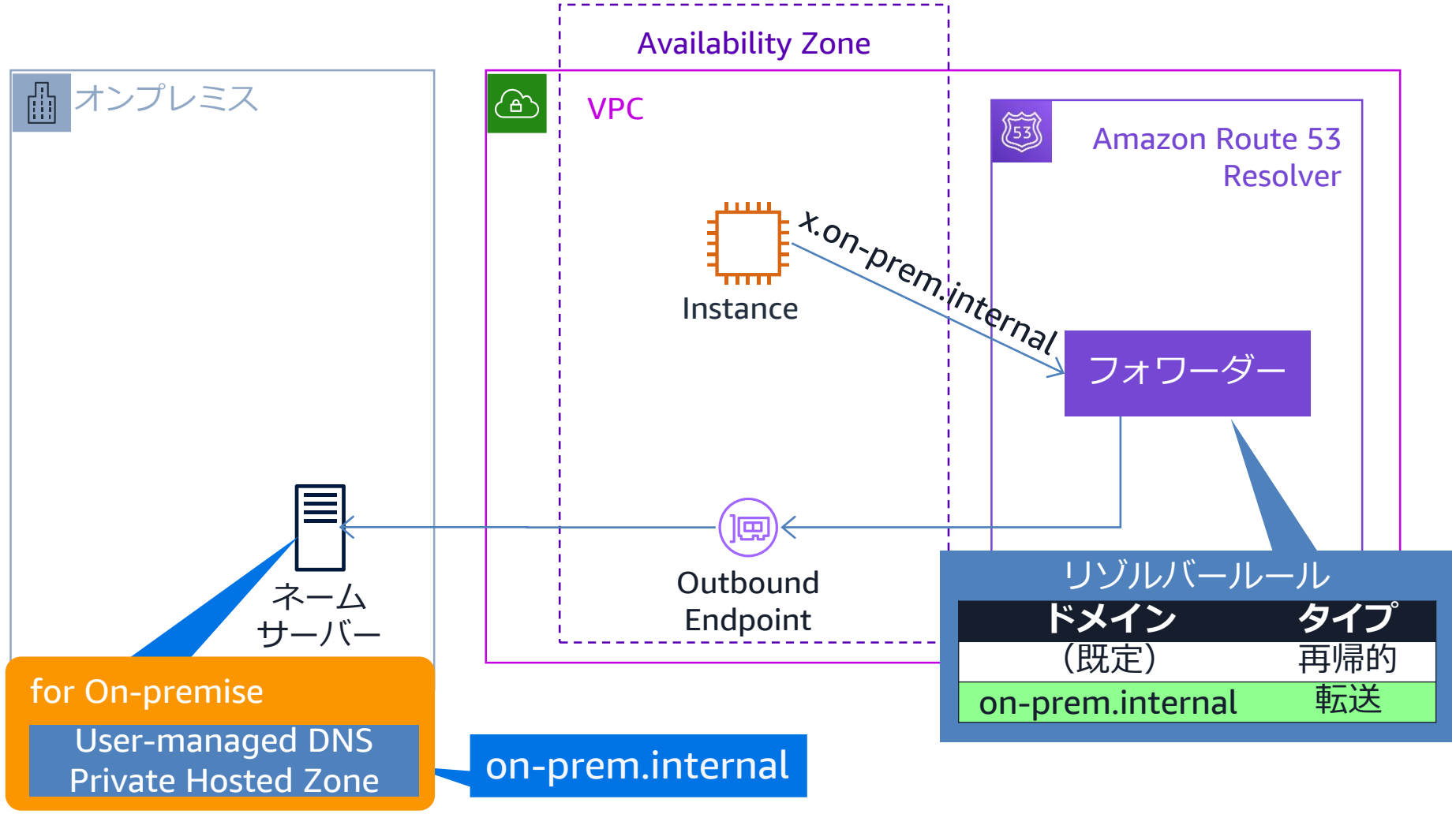


オンプレミスからVPC向けゾーンへの名前解決



https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2023_Amazon-Route53-Resolver_0530_v1.pdf

VPCからオンプレミス向け (他CSP) の名前解決



https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2023_Amazon-Route53-Resolver_0530_v1.pdf

主要情報について

ガバメントクラウド(AWS 環境) ナレッジデータベース

参考: 地方自治体のためのガバメントクラウド情報サイト(AWS 環境)
https://aws.amazon.com/jp/government-education/worldwide/japan/LG-Industry-Site/govcloud-lg/knowledge/

タスクリストについて

AWS Blog「自治体のお客様向け「ガバメントクラウド利用タスクリスト」を公開します」

Amazon Web Services ブログ

自治体のお客様向け「ガバメントクラウド利用タスクリスト」を公開します

by Masahiro Tabuki | on 14 6月 2023 | in Public Sector | Permalink | Share

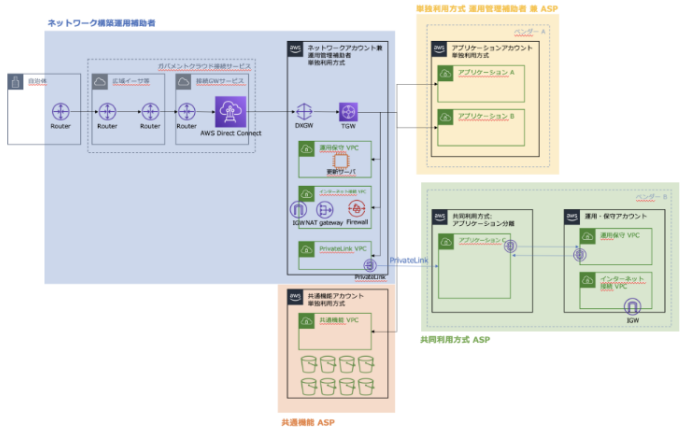
自治体のお客様において、現在ガバメントクラウドの利用検討が進んでいますが、「運用補助事業者」「ASP」など、それぞれの事業者においてどのような作業が必要かを洗い出す作業は、クラウドにこれから触れていく方の多い自治体様においては難しい作業となるかと思います。

そこで、自治体を担当しているソリューションアーキテクトがガバメントクラウドを利用する際に必要となる作業内容一覧（タスクリスト）をまとめました。

各事業者における作業内容の確認や、RFP / RFI の非機能要件の作成にお役立ていただけると嬉しいです。

本記事では、タスクリストの対象範囲についてご紹介します。
（本記事の後半にタスクリストのダウンロードリンクを掲載しています。）

対象とする環境



今回対象としている環境は上図において四角で囲ってある4つの部分

- ネットワーク構築運用補助者
- 単独利用方式 運用管理補助事業者 兼 ASP
- 共同利用方式 ASP
- 共通機能

各事業者における作業内容の確認や、RFP / RFI の非機能要件の作成にお役立ていただける内容となっています。

https://aws.amazon.com/jp/blogs/news/tasklist-for-lg-govcloud-jp/

ブログについて

- ガバメントクラウドの道案内『自治体職員編』
  - https://aws.amazon.com/jp/blogs/news/govcloud-guide-for-lg-staff/
- ガバメントクラウドの道案内『統合運用管理補助者編』
  - https://aws.amazon.com/jp/blogs/news/integrated-manager-for-lg-govcloud-jp/
- ガバメントクラウドの道案内『ネットワーク構築運用補助者編』
  - https://aws.amazon.com/jp/blogs/news/network-for-lg-govcloud-jp/
- ガバメントクラウドの道案内『ASP＆運用管理補助者編』
  - https://aws.amazon.com/jp/blogs/news/govcloud-guide-for-asp-and-management/
- ガバメントクラウド活用のヒント『共同利用方式におけるコスト・ セキュリティ管理について』
  - https://aws.amazon.com/jp/blogs/news/govcloud-hint-for-shared-use-cost-security/
- ガバメントクラウド活用のヒント『ガバメントクラウド上で CIDR 重複を起こさないために！』
  - https://aws.amazon.com/jp/blogs/news/govcloud-hint-for-network-cidr/

Thank you!

質疑応答

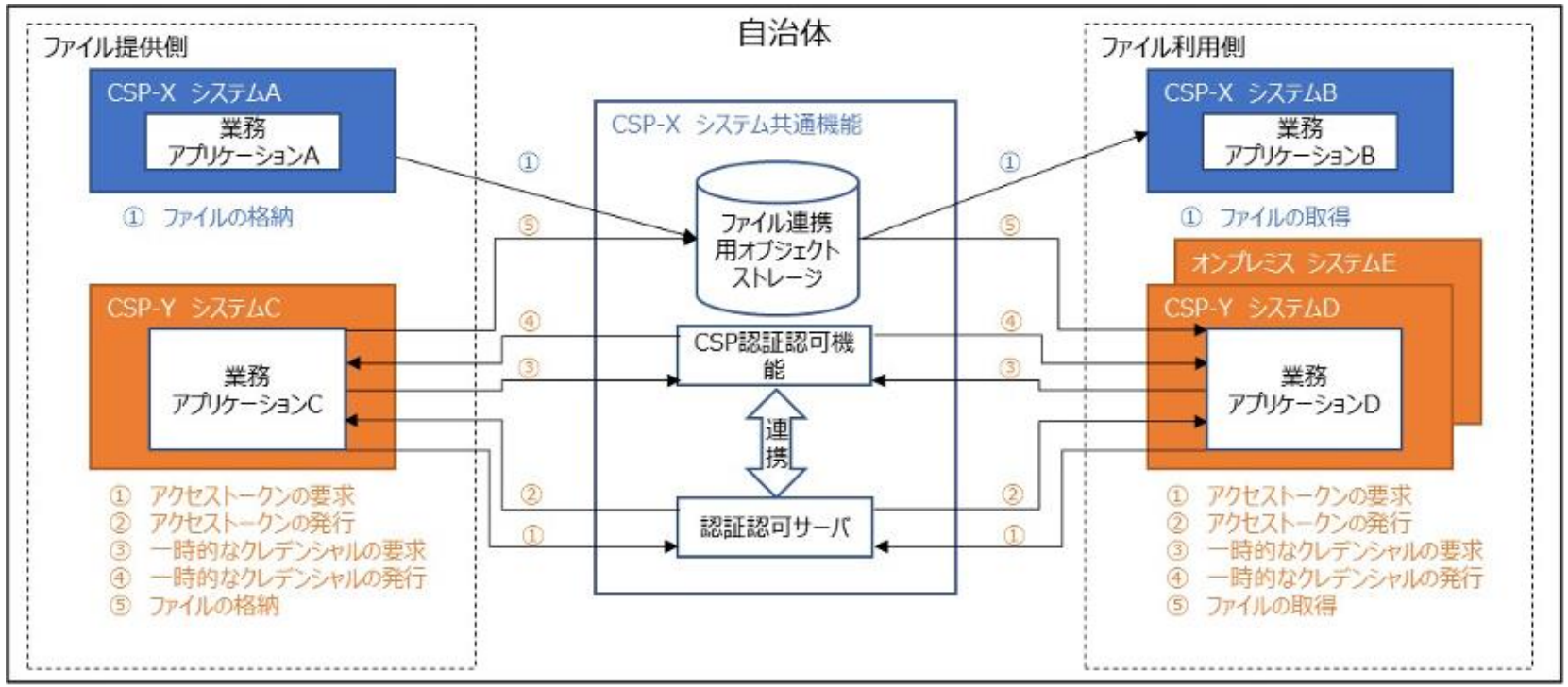
ファイル連携

ファイル連携での認証認可サーバ

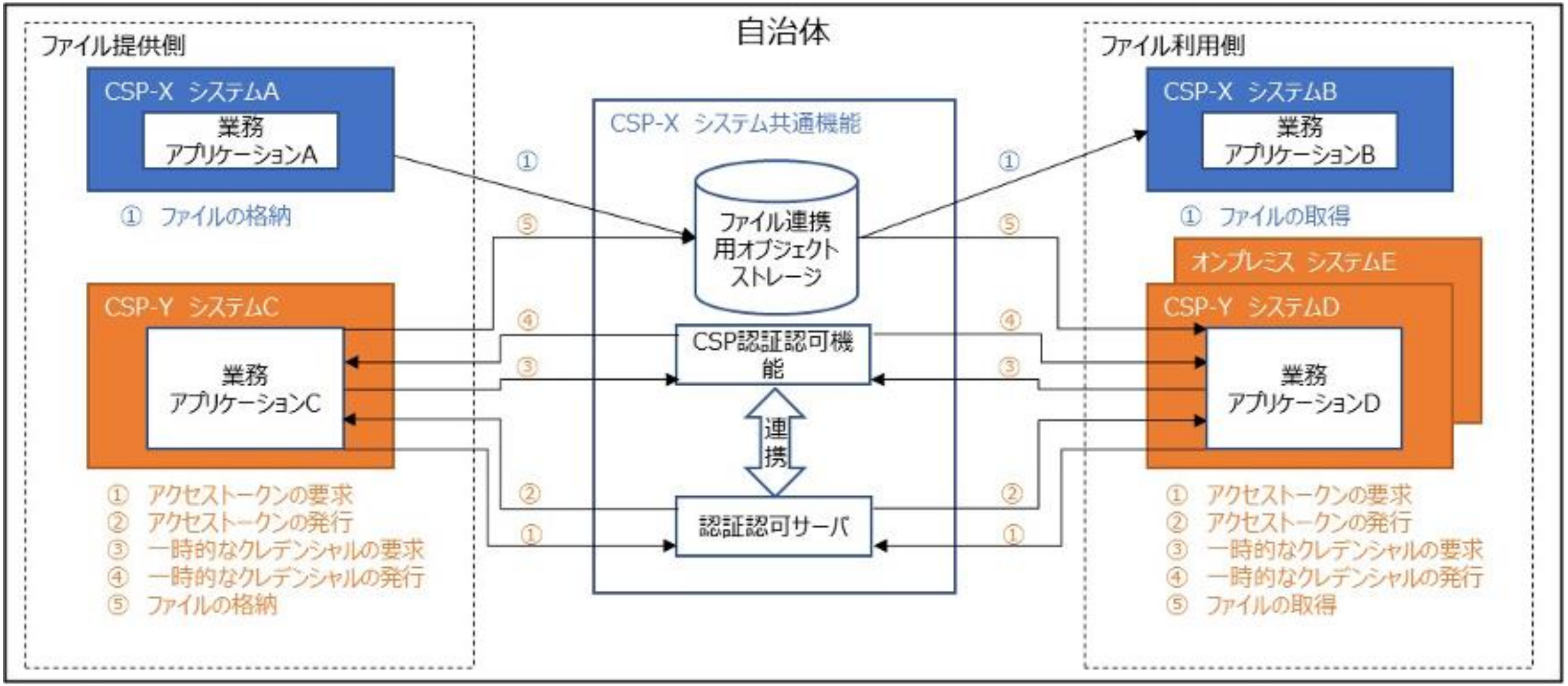
「ファイル連携に関する詳細技術仕様書」で以下の言及

異なるCSP間又はCSPとオンプレミス環境間でファイル連携を行う場合、 API 連携で利用する認証認可サーバを ID プロバイダー(以下「IdP」という。) とし、 CSP の認証認可機能と連携(フェデレーション)させ、IdP でオブジェクトストレージの認証を行うこと。

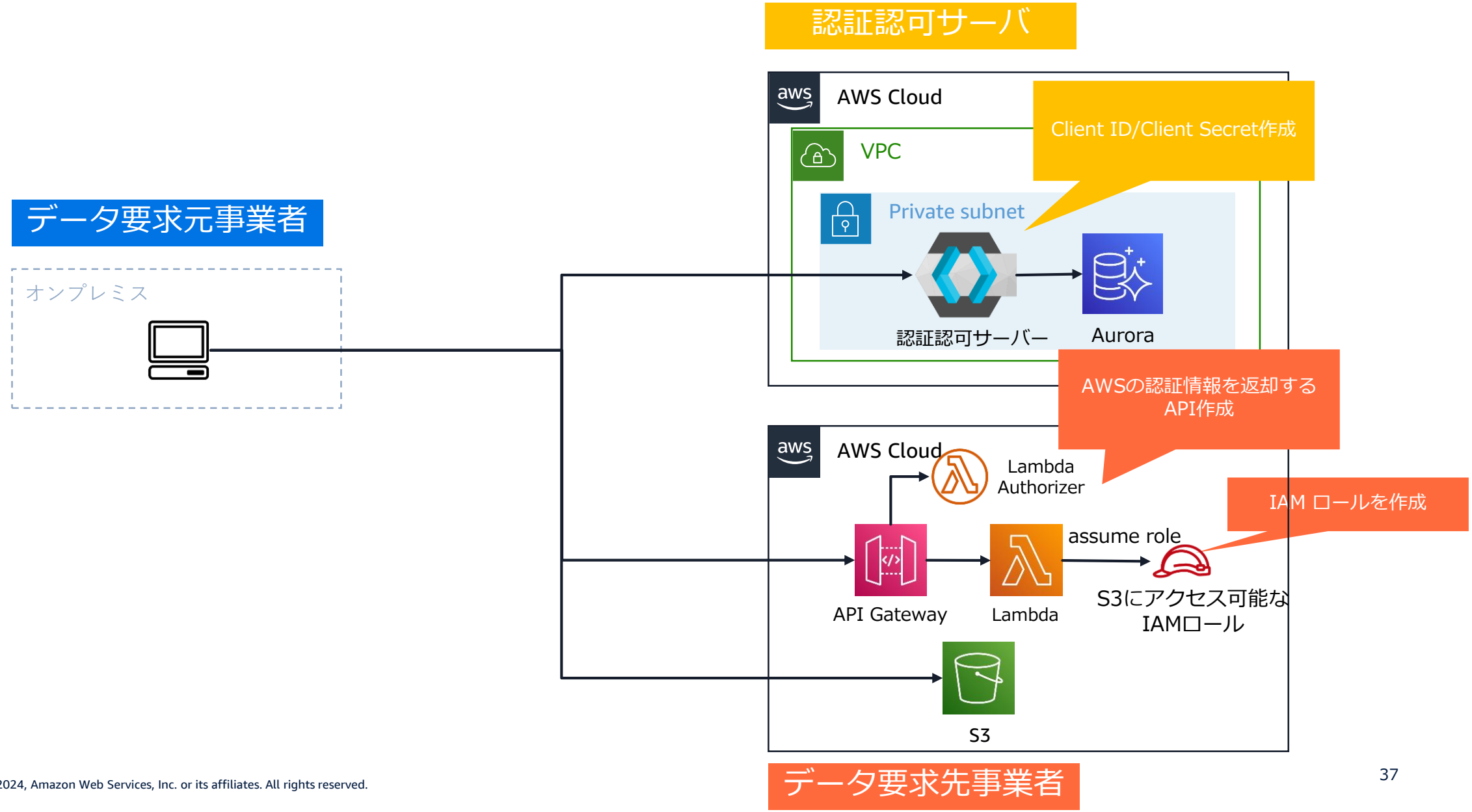
アクセストークンをAWSの一時クレデンシャルと交換する



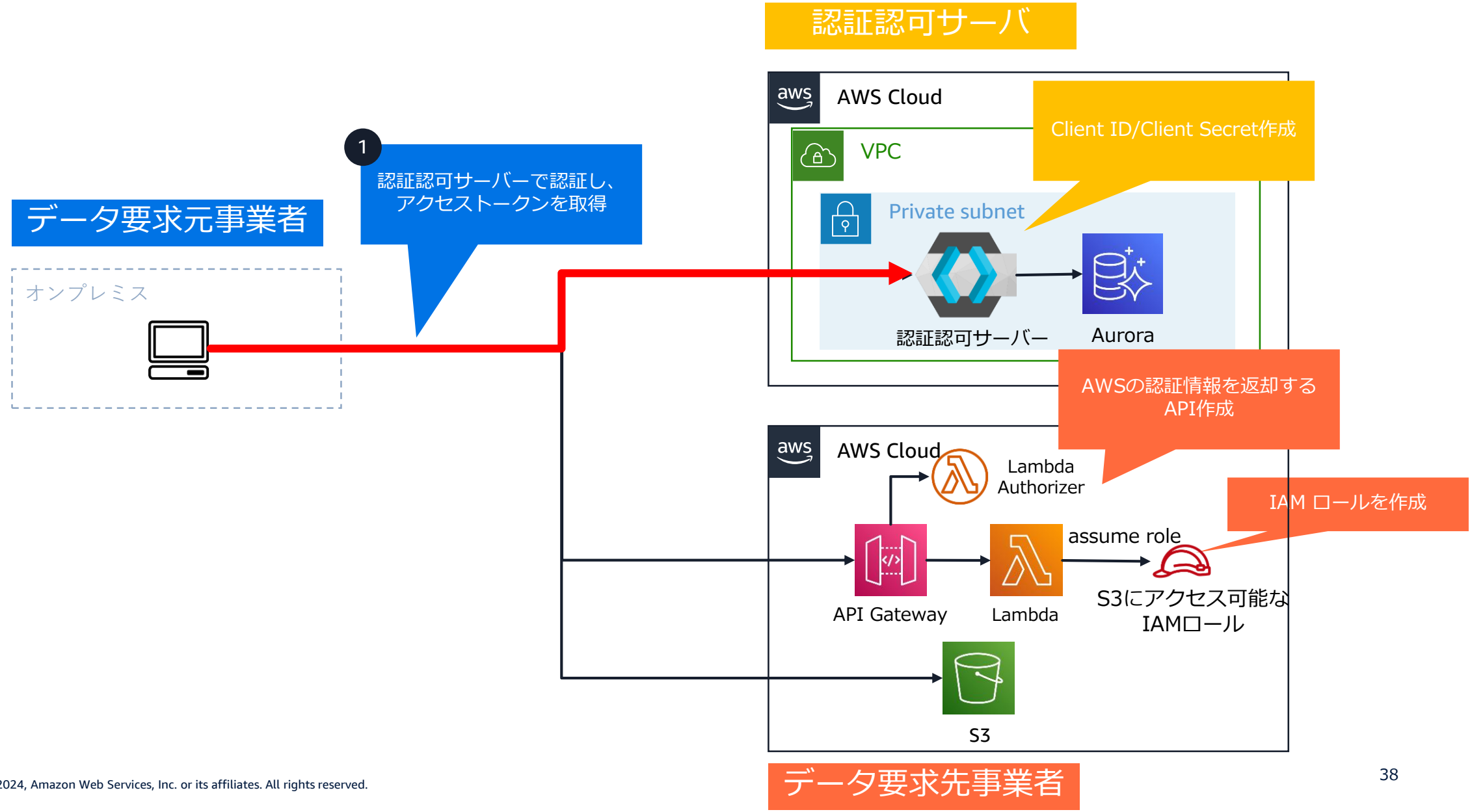
アクセスの流れ



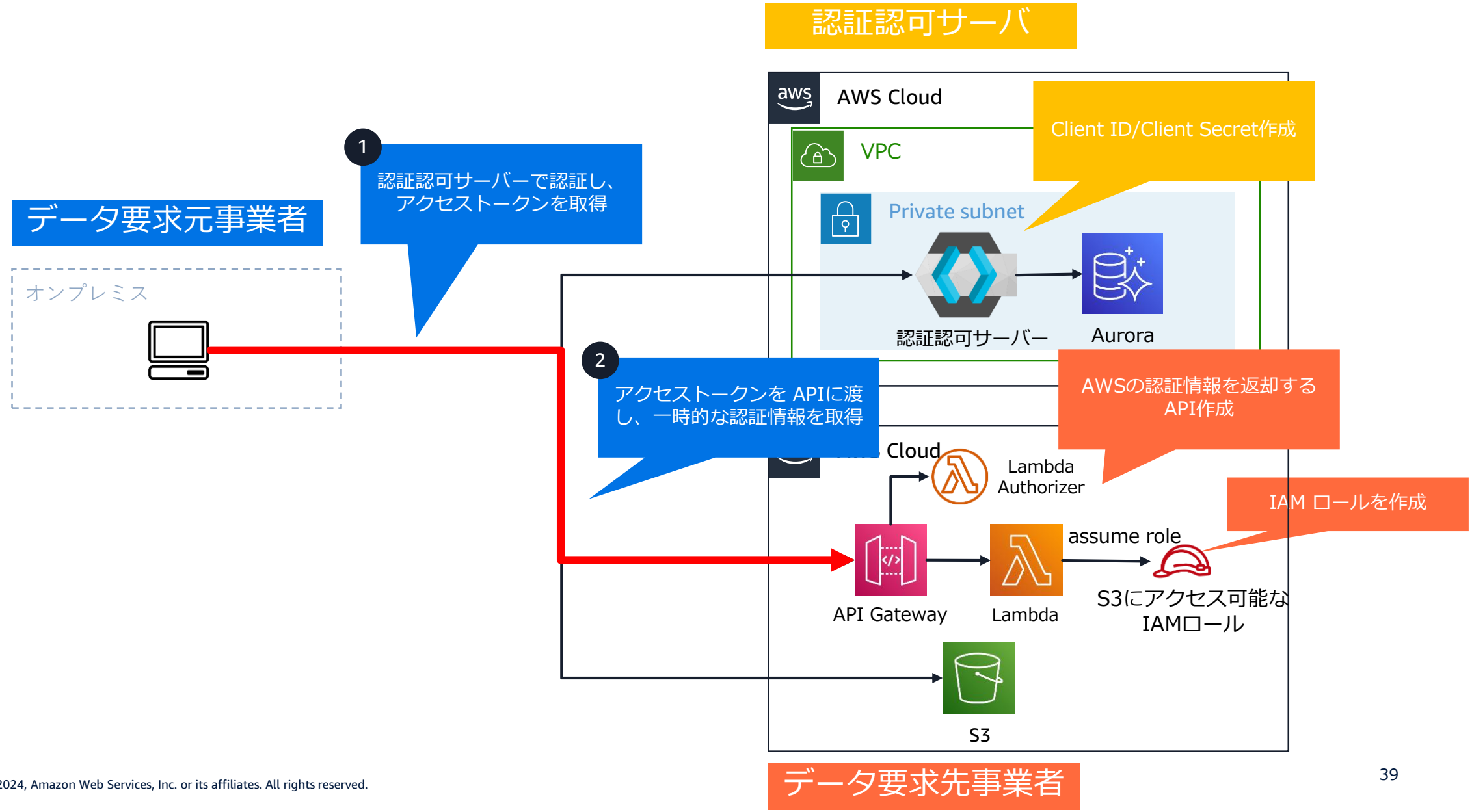
認証認可サーバを利用したS3へのアクセス



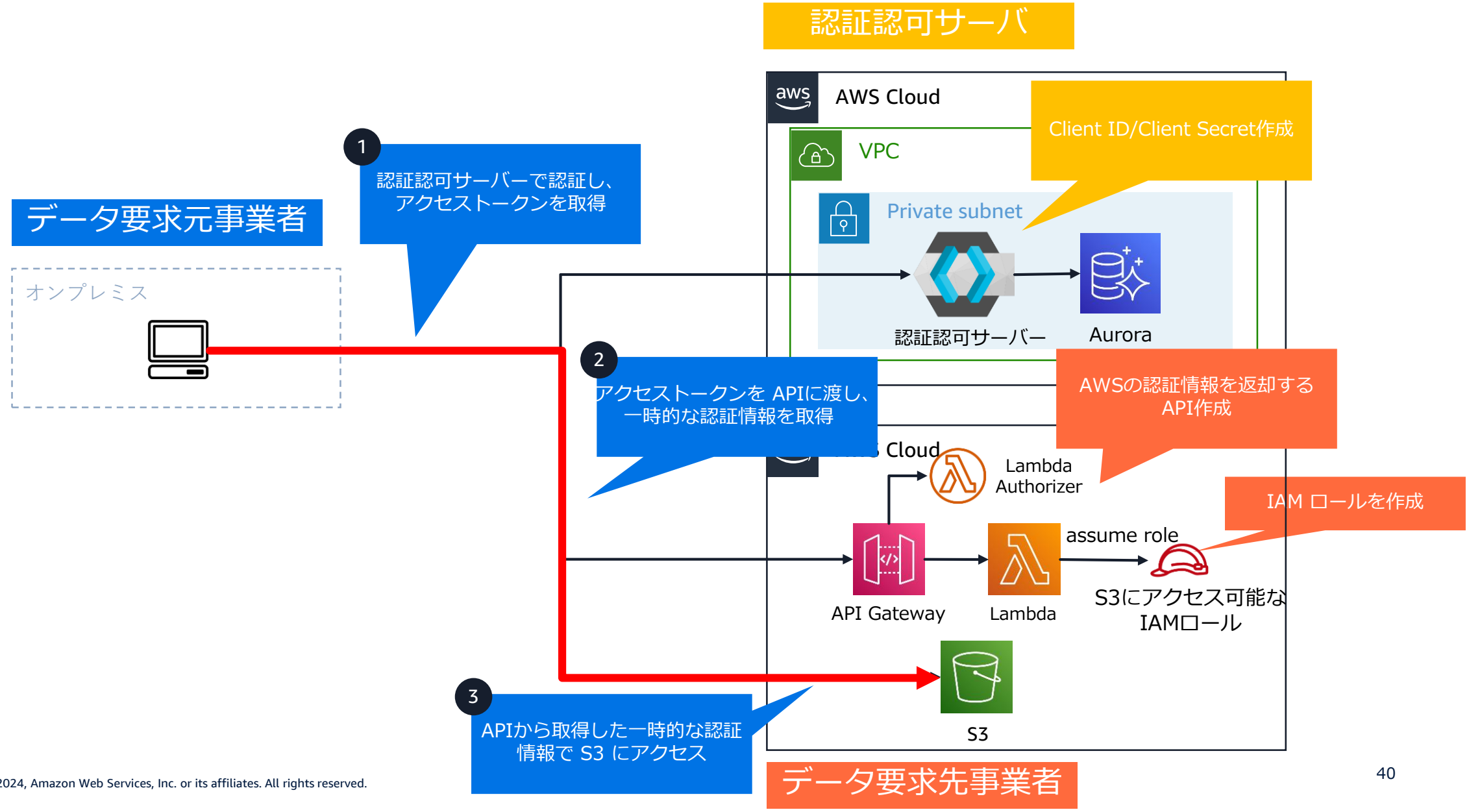
認証認可サーバを利用したS3へのアクセス



認証認可サーバを利用したS3へのアクセス



認証認可サーバを利用したS3へのアクセス



それぞれの事業者に発生する設定項目

データ要求元

OAuth 2.0のクライアント側の実装

認証認可サーバからのアクセストークンの取得

アクセストークンを利用したデータ要求先へのリクエスト発行

etc...

認証認可サーバ

- データ利用事業者・共通機能事業者にクライアントID/クライアントシークレットを発行
- クライアントスコープの作成

データ要求先

- IAM Role の作成
- OAuth 2.0のリソースサーバ側の実装
  - アクセストークン情報の取得
  - アクセストークンの検証
  - etc...