

ORACLE

OCIにおけるガバメントクラウドへの接続

日本オラクル株式会社

2024年5月24日

Safe harbor statement

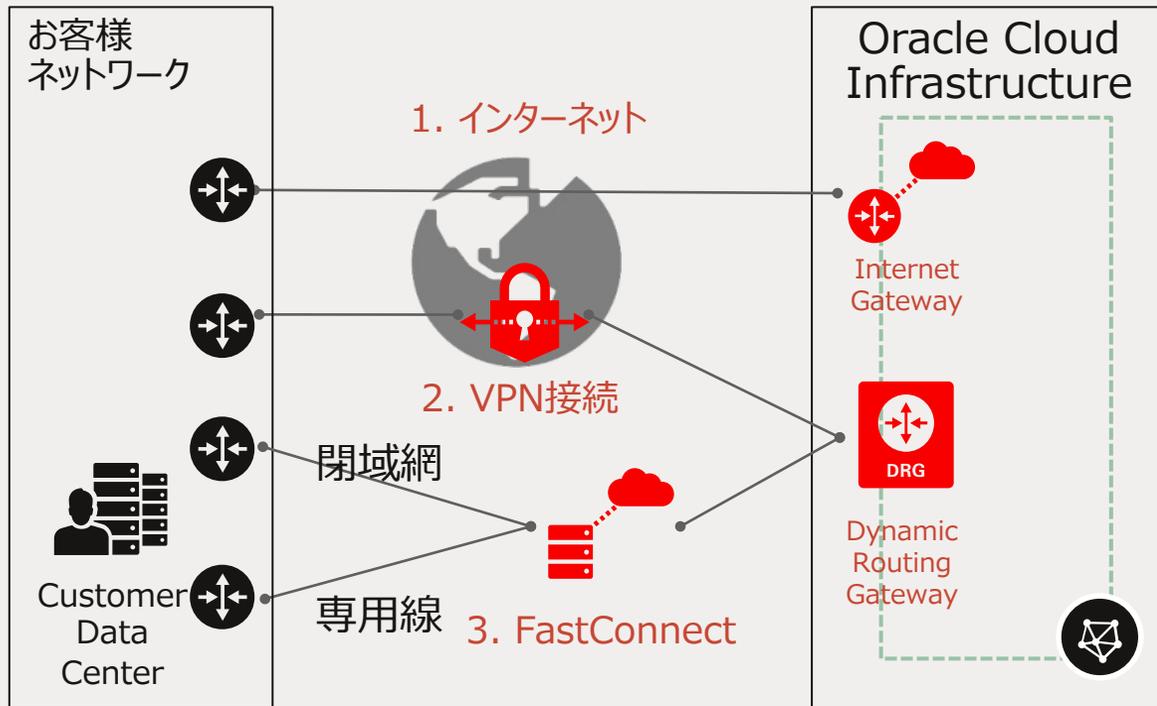
以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することを確約するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリース、時期及び価格については、弊社の裁量により決定され、変更される可能性があります。



Agenda

- パブリッククラウドとしてのOracle Cloud Infrastructure(OCI)への3つの接続方式
- ガバメントクラウドへの接続
 - 自治体とガバメントクラウドの通信
 - ガバメントクラウド内のシステムの連携
- ネットワーク運用管理補助者

パブリッククラウドとしての Oracle Cloud Infrastructure(OCI)への3つの接続方式



- これらの方式は、OCI上のシステムにアクセスするための方式であり、OCI管理コンソールへのアクセスのために必ずインターネット接続が必要となります。

1. インターネット

- グローバルIP通信
- セキュリティはFWとSSL通信等で確保
- 通信速度・帯域はベストエフォート
- 月10TBを超える外部へのデータ転送が課金対象

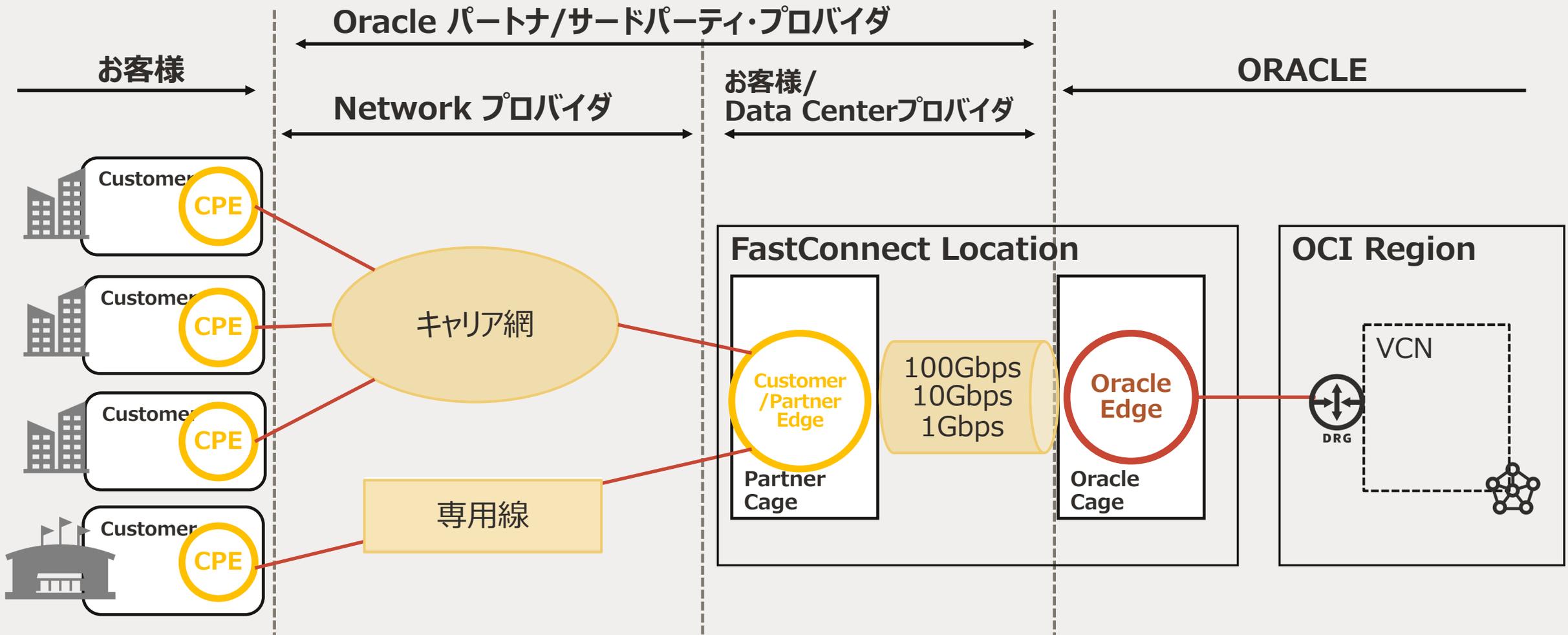
2. VPN接続 (IPsec)

- プライベートIP通信
- IPsecによりセキュリティを確保(認証,暗号化)
- 通信速度・帯域はベストエフォート
- VPN接続は無料、インターネット通信料金の対象
- OCIのVPN接続サービス、もしくはソフトウェアVPN

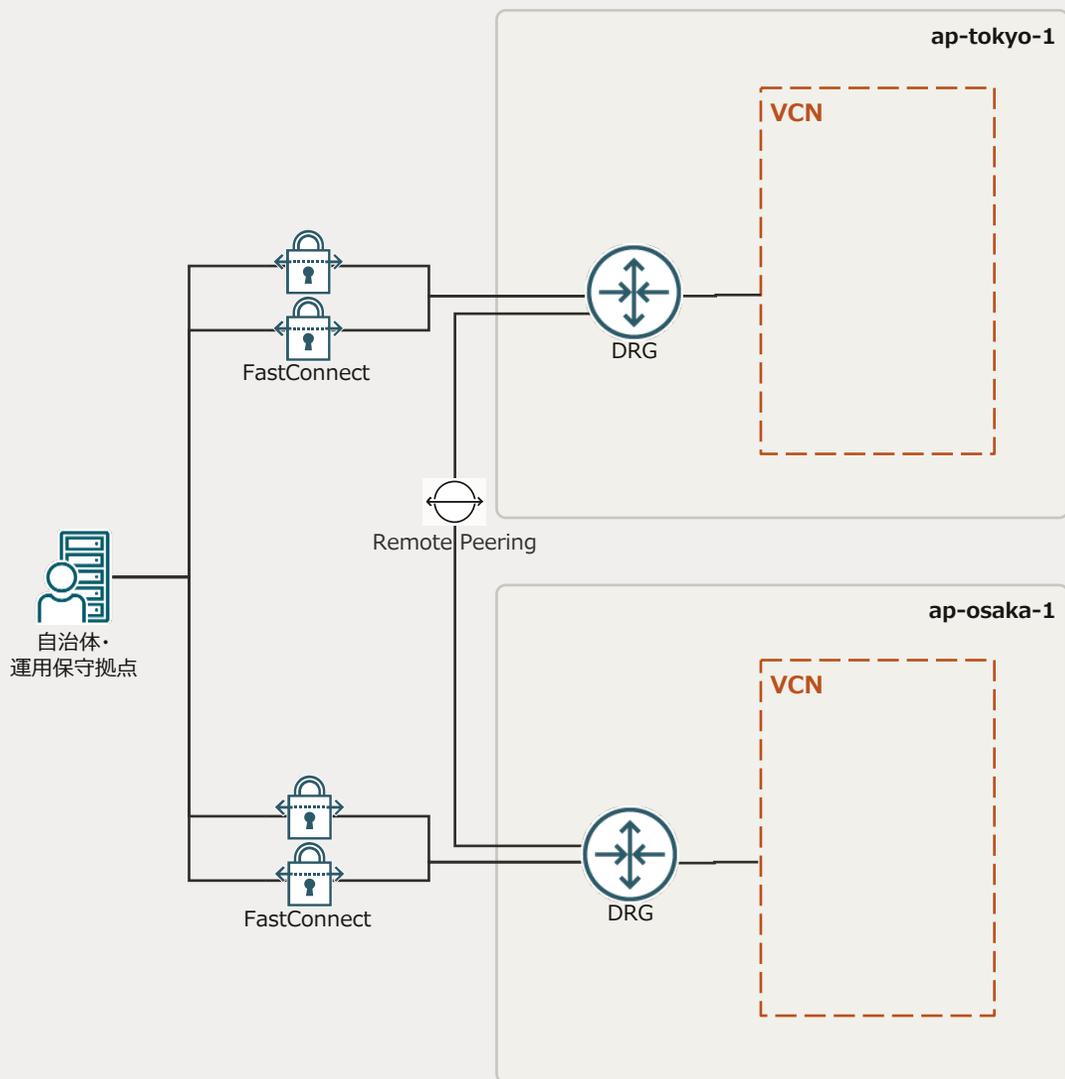
3. FastConnect

- プライベートIP/グローバルIP通信
- プライベート回線による高いセキュリティ
- 通信キャリアによる速度・帯域・品質の保証 *
- 固定額のポート料金のみ課金、データ転送に伴う従量課金なし、回線費用が別途必要

お客様環境との接続と役割分担



OCIへの接続の冗長化に関して



FastConnect冗長性のベスト・プラクティス

<https://docs.oracle.com/ja-jp/iaas/Content/Network/Concepts/fastconnectresiliency.htm>

にあるように、一つのリージョンに対して2つのFastConnectを利用することで冗長性を担保します。FastConnectのSLAは同じリージョンで冗長化されていることが前提となります。

そのためクラウド接続サービス提供者は、OCIの各リージョンに2つのFastConnectを利用できるように準備する必要があります。

その上で利用者は、バックアップ保存のためのリージョンにはFastConnect不要/専用線の冗長性不要などといったシステムごと要件を考慮し、システムごとに最適な構成を選択ください。

東京リージョンに1つ、大阪リージョンに1つのFastConnectの構成時にDRGで、障害やメンテナンスなどの通信不通時にFastConnectではなく、別リージョンのDRGにルーティングすることは可能です。ただし、自治体・運用保守拠点側環境設定にも依存するため、障害時に自動的に正しく切り変わり、復旧後に切り戻せることがOCIだけでは保証できず、切り替わった際のレイテンシも考慮する必要があるため、冗長構成としては推奨されません。

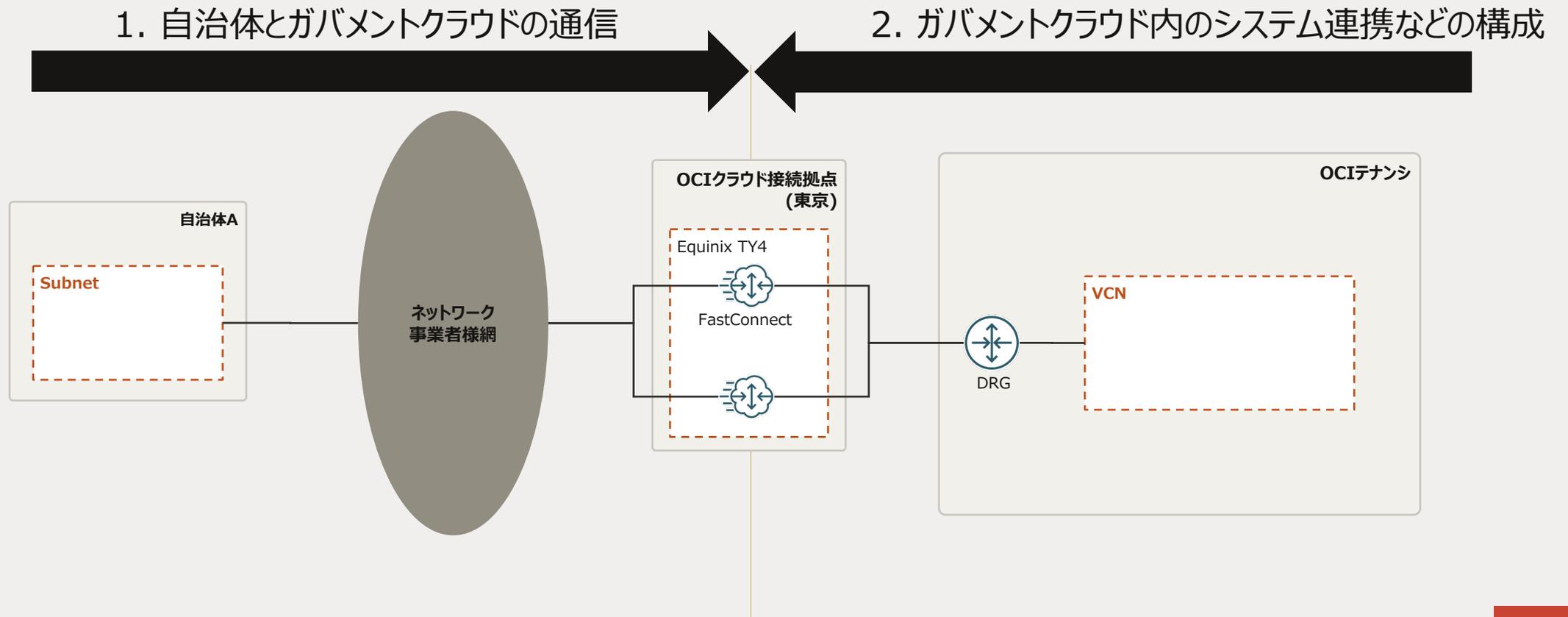




ガバメントクラウドへの接続

ガバメントクラウドへの接続

- 1. 自治体とガバメントクラウドの通信
- 2. ガバメントクラウド内のシステムの連携などの構成



自治体からガバメントクラウドへの4つの接続方式

自治体とガバメントクラウドの通信

	自治体からの個別接続	ネットワーク接続サービスプロバイダ主導による集約	アプリケーションサービスプロバイダ(ASP)主導による集約	LGWAN経由の接続
概要	自治体からガバメントクラウドに個別に接続する	ネットワーク接続サービスプロバイダが複数自治体を集約してガバメントクラウド環境への接続する	自治体から一度ASPに接続し、複数自治体を集約してガバメントクラウド環境に接続する	LGWANのガバメントクラウド接続サービス経由でガバメントクラウド環境に接続する
構成	<p>この図は、自治体Aが個別にガバメントクラウドに接続する構成を示しています。自治体Aはネットワークサービスプロバイダに接続し、Fast Connectを通じてOCIテナンシ（VCN）と他のCSP環境に接続します。</p>	<p>この図は、ネットワーク接続サービスプロバイダ主導による集約の構成を示しています。自治体Aと自治体Bはネットワークサービスプロバイダに接続し、Fast Connectを通じてOCIテナンシ（VCN）と他のCSP環境に接続します。</p>	<p>この図は、アプリケーションサービスプロバイダ主導による集約の構成を示しています。自治体Aと自治体Bはアプリケーションサービスプロバイダに接続し、Fast Connectを通じてOCIテナンシ（VCN）と他のCSP環境に接続します。</p>	<p>この図は、LGWAN経由の接続の構成を示しています。自治体AはLGWANに接続し、Fast Connectを通じてOCIテナンシ（VCN）と他のCSP環境に接続します。</p>
特徴・考慮事項	自治体が個別に利用するガバメントクラウドに接続するためのネットワークを契約する。ASPによっては直接ガバメントクラウドに接続できない可能性がある。他CSPとの連携はネットワーク接続サービスプロバイダが考慮する必要がある。	共同利用団体単位などで接続を集約することで回線費用の負担を抑えられる可能性がある。他CSPとの連携はネットワーク接続サービスプロバイダが考慮する必要がある。	ASPが自治体からの接続を集約し、ガバメントクラウドに接続する。ASPは基本的に単一CSP利用のためクラウド接続は集約され回線費用を抑えられる可能性がある。他CSPとの連携をどうするか検討が必要となる。	J-LISが提供するガバメントクラウド接続サービスを契約する。ASPによっては直接ガバメントクラウドに接続できない可能性がある。他CSPとの連携はLGWANのガバメントクラウド接続サービス経由で実施する。



ガバメントクラウド内のシステムの連携 OCI上に複数のシステムがあるケース

	ひとつのテナントに複数のシステムがある場合	複数のテナントにシステムが分散している場合		
概要	複数ASPのシステムをひとつのテナントでコンパートメントやVCNで分割	テナントごとにFastConnect接続	特定テナントのFastConnect接続とDRGを共有して接続	特定テナントのFastConnect接続を共有し、DRG間のRPC通信で接続
構成	<p>The diagram shows a single OCI tenant. On the left, '団体A' (Group A) is connected to a '接続サービスプロバイダ' (Connection Service Provider) via a 'Fast Connect' link. This provider is connected to a shared '共通運用基盤 VCN' (Common Operation Base VCN) within the tenant. From this base VCN, two separate VCNs branch out: 'システム1 VCN' (System 1 VCN) and 'システム2 VCN' (System 2 VCN). Each system VCN is connected to its own 'OCIテナンシ' (OCI Tenant) icon.</p>	<p>The diagram shows three OCI tenants. Each tenant has its own 'OCIテナンシ' icon and a '共通運用基盤 VCN'. Each tenant is connected to a '接続サービスプロバイダ' (Connection Service Provider) via a separate 'Fast Connect' link. All three providers are connected to a single shared '共通運用基盤 VCN' (Common Operation Base VCN) that spans across the tenants. From this shared VCN, three separate VCNs branch out: 'システム1 VCN', 'システム2 VCN', and '共通運用基盤 VCN'. Each system VCN is connected to its respective 'OCIテナンシ'.</p>	<p>The diagram shows three OCI tenants. Only one tenant is connected to a '接続サービスプロバイダ' (Connection Service Provider) via a 'Fast Connect' link. This provider is connected to a shared '共通運用基盤 VCN' (Common Operation Base VCN) that spans across all three tenants. From this shared VCN, three separate VCNs branch out: 'システム1 VCN', 'システム2 VCN', and '共通運用基盤 VCN'. Each system VCN is connected to its respective 'OCIテナンシ'.</p>	<p>The diagram shows three OCI tenants. Only one tenant is connected to a '接続サービスプロバイダ' (Connection Service Provider) via a 'Fast Connect' link. This provider is connected to a shared '共通運用基盤 VCN' (Common Operation Base VCN) that spans across all three tenants. From this shared VCN, three separate VCNs branch out: 'システム1 VCN', 'システム2 VCN', and '共通運用基盤 VCN'. Each system VCN is connected to its respective 'OCIテナンシ'. Additionally, there are bidirectional arrows between the OCI tenants, indicating RPC communication between them.</p>
特徴・考慮事項	構成が非常にシンプル。システム連携はテナント内に閉じている。ASPにこの構成が取れるか要確認。	必要な回線が増えるため価格に影響する。システム連携はネットワーク接続サービスプロバイダ側のルータで実施。ASP間の調整が簡単だが、ASPにこの構成が取れるか要確認。	FastConnectを接続するテナントをどのテナントにするか決める必要がある。システム連携のための通信はDRGのあるテナントで設定する必要がある。ASPにこの構成が取れるか要確認。	FastConnectを接続するテナントをどのテナントにするか決める必要がある。システム連携のための通信は連携するシステムのあるテナントで設定する。ASPにこの構成が取れるか要確認。



ガバメントクラウド内のシステムの連携 他CSPやデータセンターとの接続

	ネットワーク接続サービスプロバイダ 経由での他CSPとの連携	OCIとAzureのインターコネクトを 利用した連携	ASPへの確認が必要なケース	データセンターとの連携
概要	CSP間で閉域接続が必要なため、 接続サービスプロバイダで折り返す	OCIとAzureで無償で提供されてい る閉域接続回線を利用する	ASPのデータセンター経由で複数の CSPと接続している場合	OCIとデータセンター間での連携を 行う場合は接続サービスプロバイ ダーで折り返す
構成				
特徴・ 考慮 事項	団体まで通信を戻す必要はなく、最短経 路での折り返しとなる。 ネットワーク接続サービスプロバイダがこの構 成を実現できるかを確認する。	OCIの内部でAzureへの接続環境が準備 されているため、ネットワーク接続サービスプ ロバイダにAzureへの回線を依頼する必要 がない。	ASPのデータセンター経由で接続している場合、 他CSPとどのように連携が取れるかはASPの 接続方法により変わる可能性があるため ASPへ確認が必要。	データセンターとの接続はネットワーク接続 サービスプロバイダで折り返すことが基本だ が、そもそもネットワーク接続サービスプロバ イダ拠点がデータセンターのこともある。また、 ネットワーク接続サービスプロバイダがクラウ ドデータセンターで異なる場合には自治 体で折り返す必要があることもある。



OCIへの接続の設定

ルーティング

- Inbound (接続サービスプロバイダのルータの設定)
 - OCIのVCNに設定しているCIDRと、Object Storageなどサービスネットワーク上のサービスに閉域網で接続するためサービスネットワークに割り当てられているパブリックIPアドレスのCIDRをFastConnectにルーティング

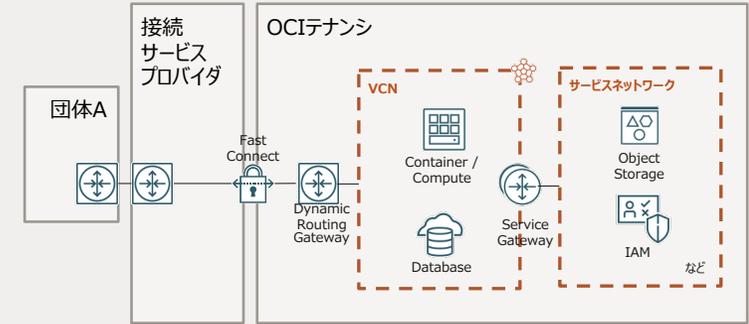
参考 : <https://docs.oracle.com/ja-jp/iaas/Content/General/Concepts/addressranges.htm>

- Outbound (Dynamic Routing Gatewayなどの設定)
 - OCI以外への接続をFastConnectにルーティング

名前解決

- OCI内部で利用されている下記のゾーンに対する名前解決はプライベートDNS機能で名前解決可能
 - VCNで利用しているドメイン名のゾーン
 - xxxx.oraclevcn.com
 - ユーザーがプライベートDNSに設定したドメイン名のゾーン
 - サービスネットワークで利用しているドメイン名のゾーン (グローバルDNSでも名前解決可能)
 - xxxx.oraclecloud.com

参考 : <https://speakerdeck.com/ocise/ociji-shu-zi-liao-jia-xiang-kuraudonetutowaku-vcn-xiang-xi>
<https://docs.oracle.com/ja/learn/resolve-onprem-dns-from-oci/>

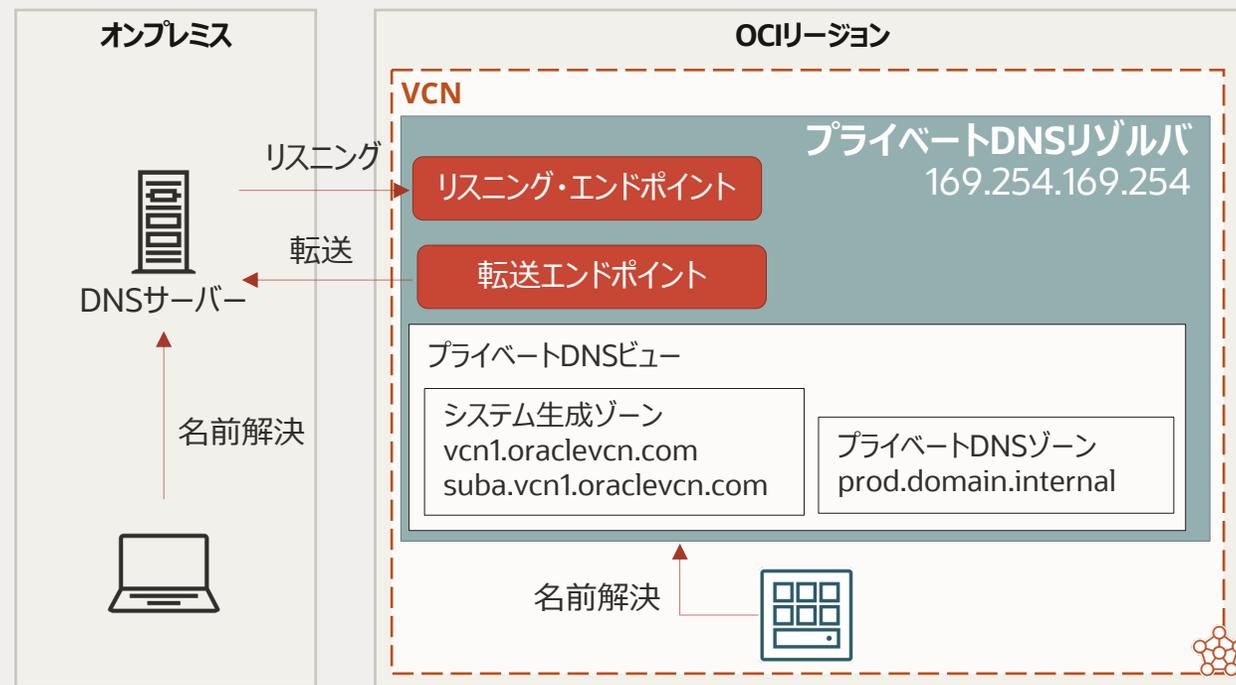


プライベートDNS

プライベートDNSを利用することで、プライベート・ネットワークの名前解決を行うためのゾーンとレコード管理が可能
また、プライベートDNSリゾルバで、VCN間、オンプレミスや他のネットワークとの間でのフォワーディングが可能

- プライベートDNSゾーン
 - プライベートネットワーク内で利用可能なDNSデータ。
- プライベートDNSビュー
 - プライベート・ゾーンの論理的な集まり。リゾルバからビューを関連付ける。
- プライベートDNSリゾルバ
 - VCN内でDNSクエリに回答するリゾルバ
 - VCN内でデフォルトで169.254.169.254でリッスン
 - エンドポイントを利用しフォワーディング設定も可能

プライベートDNSは無償。プライベートDNSゾーンや、エンドポイント、DNSクエリーなどに対する費用は不要。





ネットワーク運用管理補助者

ネットワーク運用管理補助者とは

デジタル庁の「地方公共団体情報システムのガバメントクラウドの利用に関する基準」では、ガバメントクラウド個別領域のクラウドサービス等の運用管理の補助を委託する事業者を「ガバメントクラウド運用管理補助者」として定義している。

このガバメントクラウド運用管理補助者のうち、ネットワーク領域の運用管理補助をおこなう業者を「ネットワーク運用補助者」とこの資料では呼ぶ。

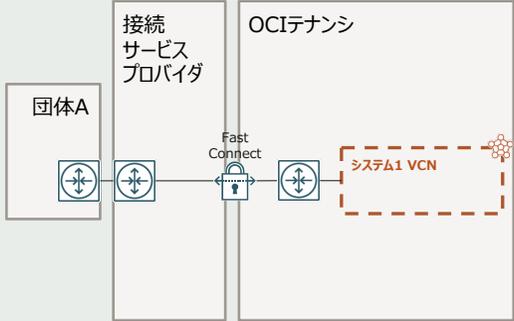
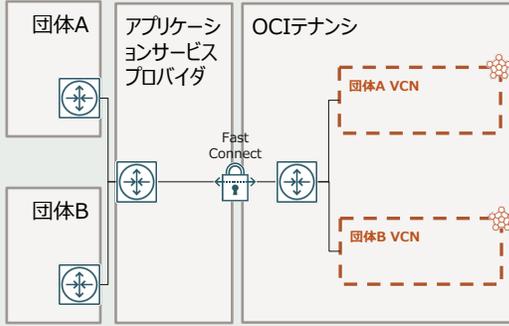
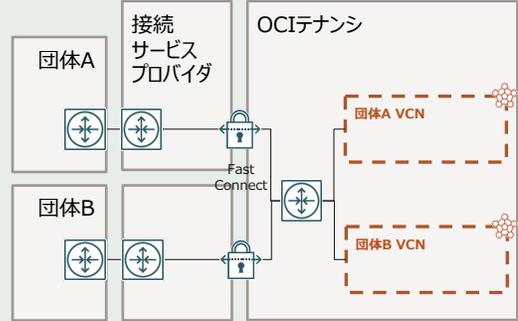
ただし、OCIのガバメントクラウドではネットワーク運用管理のためだけに環境(テナンシ)を払い出すことは必須ではないため、ネットワーク運用管理だけを専門におこなうネットワーク運用管理補助者が必要ないケースもある。その場合、自治体に個別に払い出されたクラウド基盤全体を管理するガバメントクラウド運用管理補助者やシステム提供ベンダ、ASPなどがネットワーク運用管理補助者を兼ねることになる。

ここではOCIのガバメントクラウドのさまざまな利用形態において、誰がネットワークを管理すべきかの例を示す。



専任のネットワーク運用管理補助者が不要なケース (他者が兼任するケース)

ガバメントクラウドとして払い出されたOCIのテナンシには自治体からのネットワーク接続専用の環境がないケースもあるため、そもそも専任のネットワーク運用管理補助者が不要なケースがある。

	単一ベンダによる単独利用方式のケース	アプリケーションサービスプロバイダ(ASP)経由で接続するケース	アプリケーションサービスプロバイダ(ASP)に個別に直接接続するケース
概要	単独利用の場合、自治体に払い出されるテナンシはひとつで、このひとつのテナンシに複数のコンパートメントやVCNを作成して利用する。払い出された環境にひとつのベンダのシステムしか載らない場合、払い出されたテナンシ、ネットワーク、システムすべての運用管理を同じベンダがおこなう。	自治体から一度ASPに接続し、複数自治体を集約してガバメントクラウド環境に接続するケースでは、ASPがガバメントクラウドのネットワークの管理をおこなうため、ネットワーク運用管理補助者は不要となる。	ASPが自治体からの直接個別接続を許可している場合、接続サービスプロバイダとの契約だけで、ASPがガバメントクラウドのネットワークの管理をおこなうため、ネットワーク運用管理補助者は不要となる。
構成			
ネットワーク管理主体	システム提供ベンダ	ASP	ASP



ネットワーク運用管理補助者が必要なケース

単独利用方式でも、複数ベンダが払い出されたひとつのテナンシ上にシステムを構築する場合や、複数の払い出された環境(テナンシ)に分散する場合には、ネットワーク運用管理補助者が必要です。

	複数ベンダによる単独利用方式のケース	複数の単独利用環境への接続を集約するケース	アプリケーションサービスプロバイダ(ASP)に単独利用環境経由で接続するケース
概要	単独利用で自治体に払い出されるテナンシはひとつでも、このひとつのテナンシに複数のベンダがコンパートメントやVCNを区切ってシステムを構築する場合には、ネットワーク、コンパートメント、ユーザ権限管理などをおこなうネットワークを含むクラウド基盤全体の運用管理補助者が必要となる	単独利用方式でも自治体に払い出されるテナンシが複数ある場合で自治体からガバメントクラウドへの接続を集約したい場合、自治体からの接続を受けるテナンシの運用管理補助者が他のテナンシへのネットワーク設定をおこなう必要がある	ASPサービスに対して自治体からの接続するのではなく、ガバメントクラウド内のネットワーク通信を経由して接続したい場合、自治体からの接続を受けるテナンシの運用管理補助者がASPテナンシへのネットワーク設定をおこなう必要がある
構成			



Oracle Cloud Infrastructure 主要情報

1 OCI活用資料集

<https://oracle-japan.github.io/ocidocs/>

OCIを使ってみたい! という方のための技術ドキュメント集。OCIのサービス別技術資料をはじめ、PPTスライドを中心とした公開ドキュメントや、セミナーで使用した資料をアップロードしています。

2 チュートリアル: OCI を使ってみよう

<https://oracle-japan.github.io/ocitutorials/>

OCIを使ってみよう! という人のためのチュートリアル集。各項目ごとに画面ショットなどを交えながらステップ・バイ・ステップで作業を進めて、OCIの機能についてひとつひとつ学習することができるようになっています。

3 OCIドキュメント

各サービスのマニュアル。

<https://docs.cloud.oracle.com/ja-jp/iaas/Content/home.htm>

4 オラクルエンジニア通信

<https://blogs.oracle.com/oracle4engineer/>

技術資料、コラム、マニュアルなど、OCIに関するその他の情報は、「オラクルエンジニア通信」よりお届けしています。

5 OCIサービスアップデート

<https://blogs.oracle.com/oracle4engineer/category/o4e-oci-service-update>

毎月公開するOCIのサービス・アップデート情報をスライドで分かり易く説明。各サービスの詳細な情報は、各サービスのドキュメントや下記「OCI活用資料集」をご覧ください。

6 OCIセミナー情報

https://blogs.oracle.com/oracle4engineer/column_cloud_seminar

今後開催予定のウェビナー(含むハンズオントレーニング)についてご案内します。

ほぼ毎週 2回+ハンズオンを様々なテーマで開催中!

7 OCIお客様活用事例

<https://blogs.oracle.com/oracle4engineer/oracle-cloud-platformpaasiaas>

OCIを活用したお客様の事例のご紹介。データベースはもちろんのこと、アナリティクス、セキュリティ、システム管理、コンテンツ管理、ブロックチェーン、チャットボットなど様々なサービスのお客様事例をご紹介します。

8 Oracle Code Night

<https://oracle-code-tokyo-dev.connpass.com/>

オラクルのテクノロジーだけに限定しない、Developer (開発者) のDeveloper (開発者) によるDeveloper (開発者) のための開発者向けコミュニティ Meetup セミナーのこと。様々なテーマで開催中!



OCIガバメントクラウド関連各種情報提供サイトと弊社ガバメントクラウド関連専用問い合わせ窓口

Oracle Japan > クラウド >

政府・自治体向けOracle Cloud Infrastructure (OCI)

日本の政府・自治体のお客様に対し、OCIに関する情報をワンストップで提供するサイトです。

[OCIの概要資料を読む\(PDF/日本語\)](#) [お問い合わせ](#)

<https://www.oracle.com/jp/cloud/government/>



自治体様へ各種情報をまとめております

以下直近のBlog (和歌山市様)

有識者に聞く自治体最前線の現状と課題：システム標準化とその先にあるDXの姿

国の定める標準システムへの移行期まで残っております。多くの自治体やアプリケーションベンダーが標準化の進展を待ち、どうも「標準」に期待が寄せられています。この期待が実現するまで、システム標準化の進展となった地方自治体標準化推進の推進は「2024年度に向けて前倒しする変化（課題）への対応であり、標準化推進に必要で、標準化の進展を促すための取り組みが必要となります。

こういった課題を踏まえ、和歌山デジタル推進課の和歌山、及び和歌山を拠点とするベンダーである和歌山デジタル推進課と連携し、

標準化・ガバメントクラウドに関する貴市の取組み状況や、期待・課題についてお聞かせください。



和歌山県では、2023年度から、和歌山県デジタル推進課が推進する「和歌山県標準システム」の導入を進めています。この取り組みは、和歌山県全体のデジタル化を促進し、業務効率化を図るための重要な取り組みです。和歌山県標準システムは、和歌山県内の自治体や企業向けに提供される標準的なシステムであり、和歌山県全体のデジタル化を促進し、業務効率化を図るための重要な取り組みです。

何かご不明点などございましたら、以下弊社ガバメントクラウド担当窓口までご連絡お待ちしております

oracle_governmentcloud_oci_jp_grp@oracle.com

共同利用方式と単独利用方式両方のタスクリストを公開



共同利用方式向けガバメントクラウド利用タスクリスト

2023/8/23
日本オラクル株式会社

単独利用方式向けガバメントクラウド利用タスクリスト

2024/3/15
日本オラクル株式会社

※HPでの公開はしておりません、別途お問合せ下さい



ORACLE