



ガバメントクラウドへの接続

日本オラクル株式会社
2025年

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。

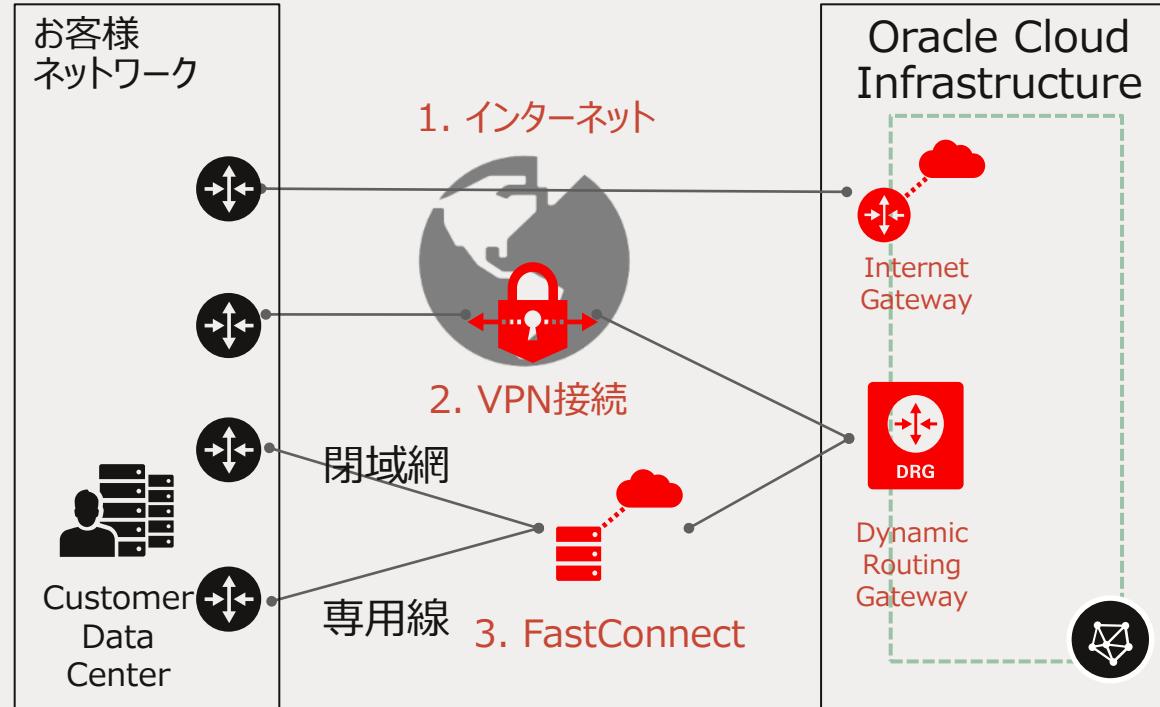
オラクル製品に関して記載されている機能の開発、リリース、時期及び価格については、弊社の裁量により決定され、変更される可能性があります。



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



- これらの方程式は、OCI上のシステムにアクセスするための方程式であり、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)

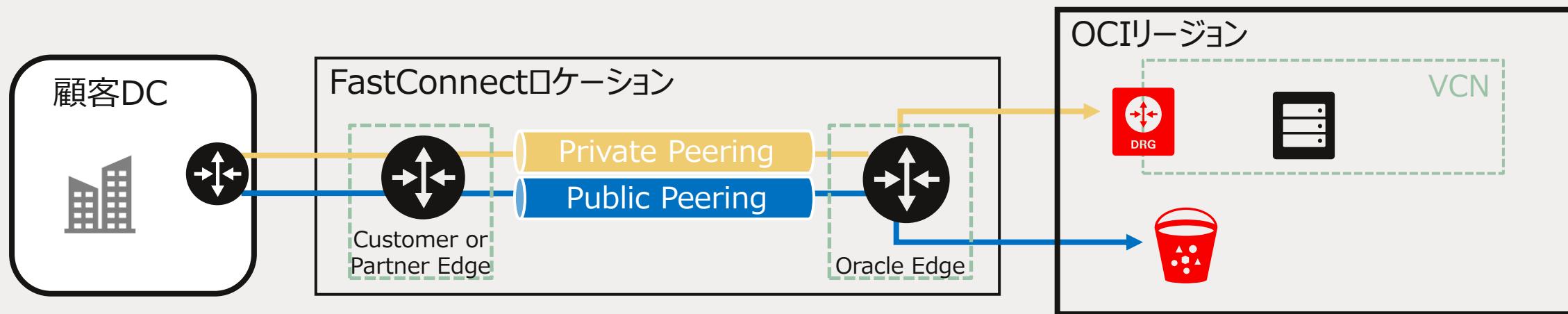
- プライベートIP通信
- IPsecによりセキュリティを確保(認証,暗号化)
- 通信速度・帯域はベストエフォート
- VPN接続は無料、インターネット通信料金の対象
- OCIのVPN接続サービス、もしくはソフトウェアVPN

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

自治体向けのガバメントクラウドへの接続には閉域接続必須

FastConnectの2つのユースケース



プライベート・ピアリング

- VCNの中のリソースに閉域接続したい場合
- パブリックIPを持つOCIサービス* と、VCN内のリソースの両方に閉域接続したい場合

パブリック・ピアリング

- パブリックIPを持つOCIのサービス* に閉域接続したい場合

OCI上に構築したシステムを利用する際にはプライベート・ピアリングを利用

* パブリックIPを持つOCIサービスの例：オブジェクト・ストレージ / Analytics Cloud などの パブリックIPを持つPaaSサービス / APIエンドポイント
(注意) OCIのコンソール画面については、現時点では完全な閉域接続はできません(CDNなどを利用するため)

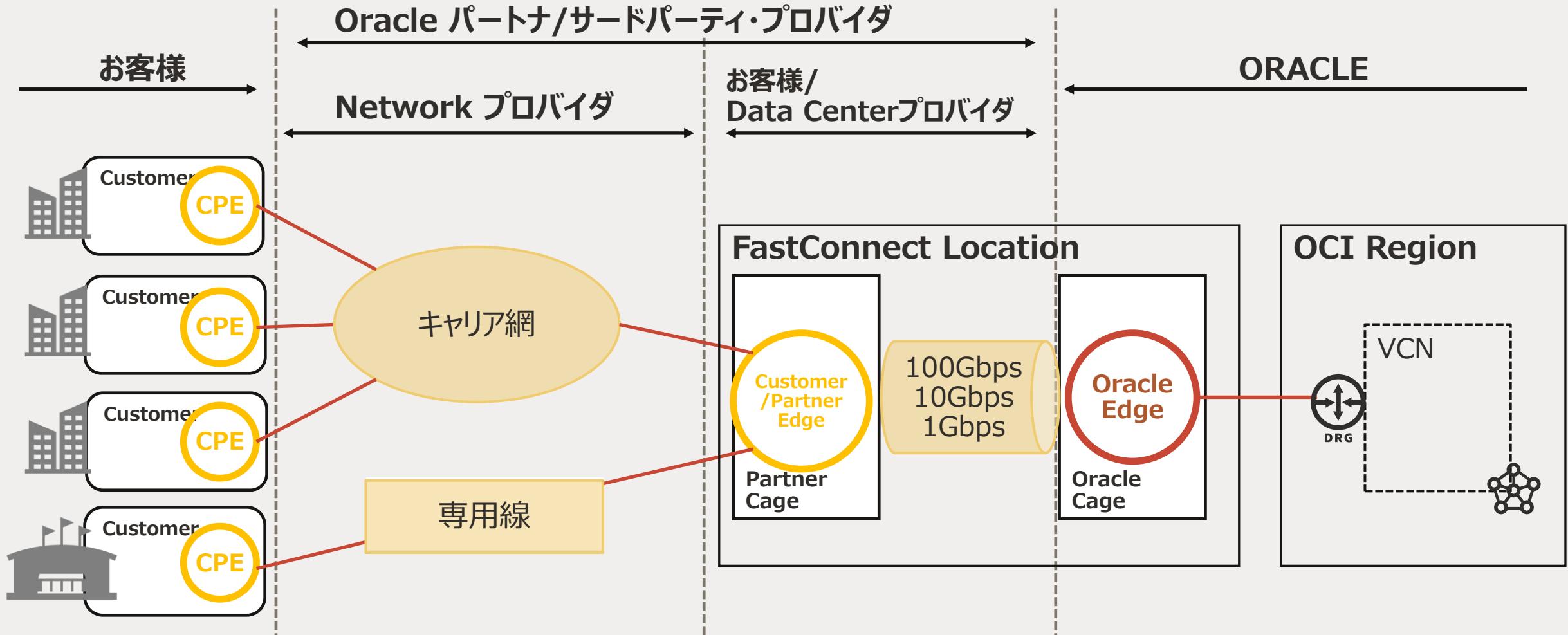
FastConnect 3つの接続モデル

接続モデル	概要	課金単位
FastConnect パートナ	Oracleパートナ Oracle接続サービスを提供している通信事業者 https://www.oracle.com/jp/cloud/networking/fastconnect/providers ※	仮想回線 (Virtual Circuit) 論理ポート: 1Gbps, 10 Gbps, 100Gbps プロバイダ帯域 : 10M~ ※利用可能な帯域は通信事業者によって異なります
FastConnect ダイレクト	サードパーティ・ プロバイダ 「Oracleパートナ」以外の通信事業者に専用回線を注文して接続 例：アルテリア	クロスコネクト (Cross-Connect) 物理ポート: 1Gbps, 10Gbps, 100Gbps単位
	コロケーション FastConnect ロケーションに設置されたお客様の機器を直接OCIへ接続 例：Equinix TY4, NTTデータ 堂島 ※	クロスコネクト (Cross-Connect) 物理ポート: 1Gbps, 10Gbps, 100Gbps単位

※東京・大阪リージョンの FastConnect パートナ、およびFastConnectロケーション については、以下の URL より確認可能

- <https://www.oracle.com/jp/cloud/networking/fastconnect/providers/#apac>

お客様環境との接続と役割分担



OCI 東京、大阪リージョンの FastConnect 接続プロバイダー(2025年2月現在)

<https://www.oracle.com/jp/cloud/networking/fastconnect-providers.html>

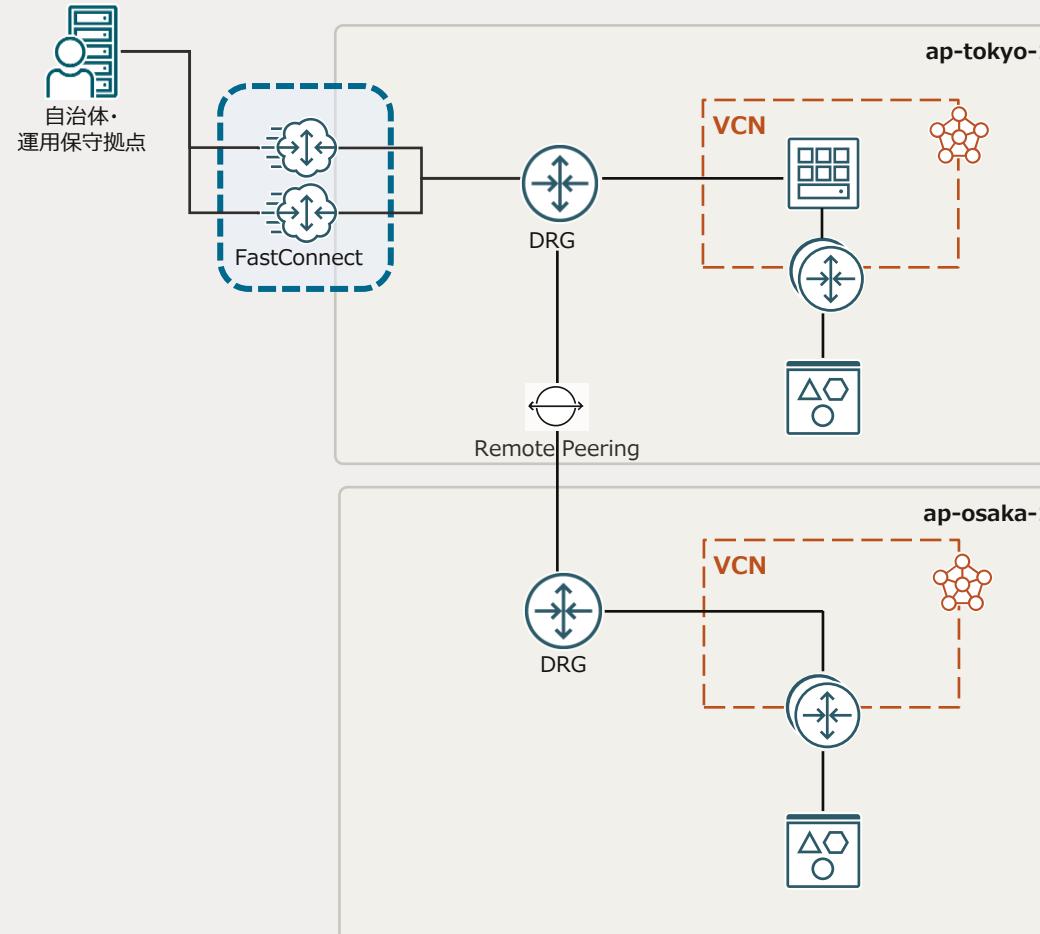
最新情報はURLを確認してください。

東京リージョン(ap-tokyo-1) Equinix TY4	東京リージョン(ap-tokyo-1) NEC 印西データセンター	大阪リージョン(ap-osaka-1) NTT DATA堂島第4ビル
<ul style="list-style-type: none">•アット東京•BBIX•Chief Telecom•Console Connect PCCWG•Colt Dedicated Cloud Access•CTC Cloud Connect•Equinix Fabric•Google Cloud: OCI Interconnect•IIJ•KDDI•Lumen•Megaport•Microsoft Azure Express Route•三菱電機インフォメーションネットワーク株式会社•NRI•NTT Communications - Flexible InterConnect•NTTデータ•NTT東日本•SINET•ソフトバンク•TOKAIコミュニケーションズ	<ul style="list-style-type: none">•NEC•SCSK	<ul style="list-style-type: none">•アット東京•BBIX•Colt Dedicated Cloud Access•Equinix Fabric•IIJ•KDDI•Megaport•三菱電機インフォメーションネットワーク株式会社•NTT Communications - Flexible InterConnect•SINET•ソフトバンク•TOKAIコミュニケーションズ



FastConnect接続の冗長性について

ガバメントクラウドへの接続の基本的なパターン

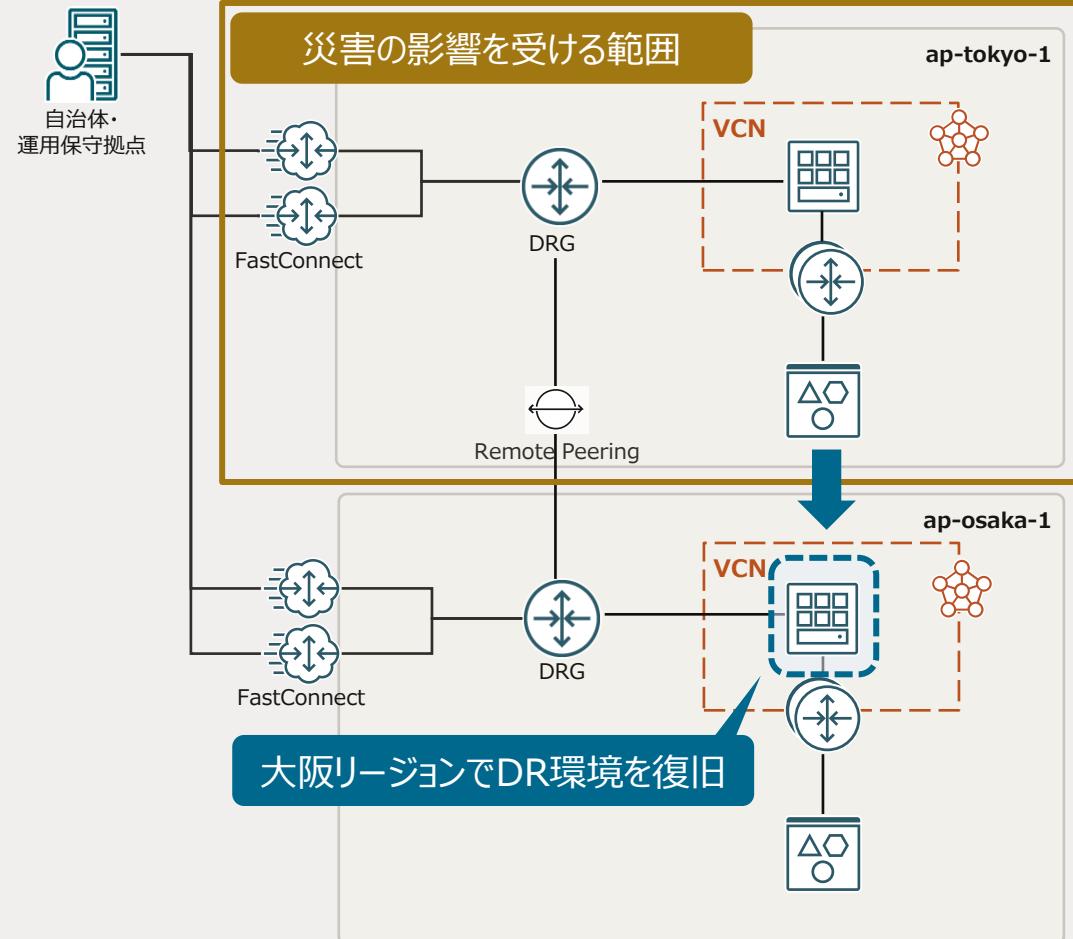


- 一つのリージョンに対して**2つのFastConnectを利用することで冗長性を担保**します。FastConnectのSLAは同じリージョンで冗長化されていることが前提となります。
- 図のような構成の場合、メインサイトのリージョンで災害が発生した際にはリージョンの復旧を待ってDRサイトのバックアップからメインの環境を復旧する想定です。リモートリージョンのバックアップに対しても、バックボーン回線を利用した通信でアクセス可能です。
- 2つのリージョンに1つずつのFastConnect構成では、障害やメンテナンスなどの通信不通時にはDRGをFastConnectではなく、別リージョンのDRGヘ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替わり、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。

(参考) 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>

FastConnect接続の災害対策について

東京と大阪の双方に専用線を接続するパターン



- メインサイトのリージョンで2本の冗長化した専用線を利用するほか、DRサイトのリージョンにも専用線を接続する構成も可能です。
- その場合、メインサイトのリージョンで災害が発生した際には、DRサイトの最小限のDR環境を大阪リージョンのバックアップから復旧することになります。
- なお、大阪リージョンへの専用線は基本的に災害時のみに必要なものため、
 - コスト削減のために多重化せずに1本のみ接続する
 - 常時接続するのではなく災害発生時に専用線を迅速に接続できるような契約を接続サービスプロバイダとしておく

などの方法も考慮ください。

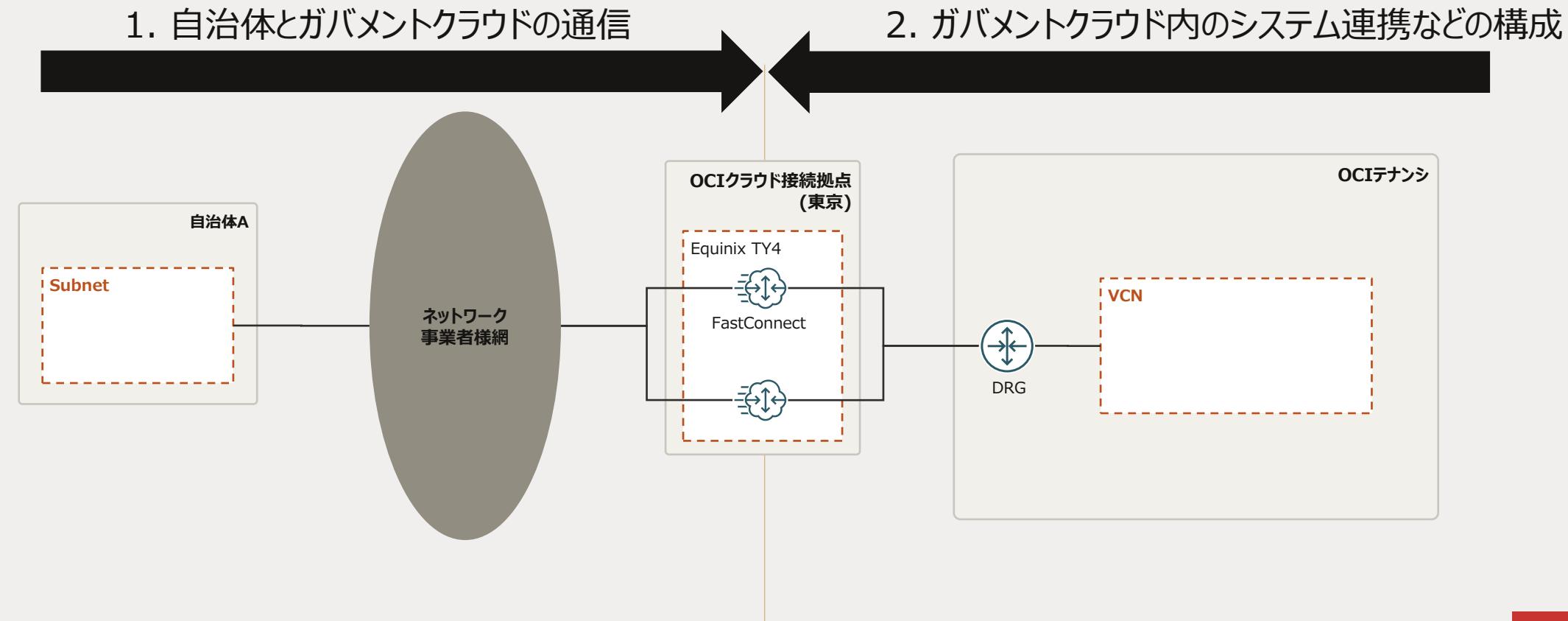
本資料では、東京リージョンに本番環境を構築していますが、OCIでは東京リージョンと大阪リージョンで主要提供サービスの差がないため、大阪リージョンに本番環境を構築することもできます。



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

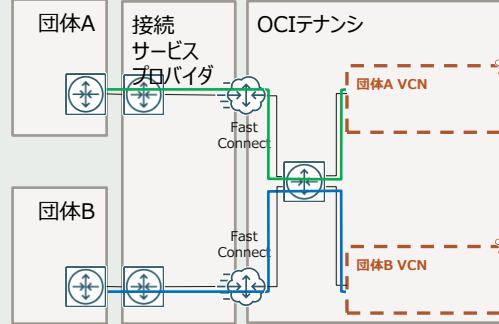
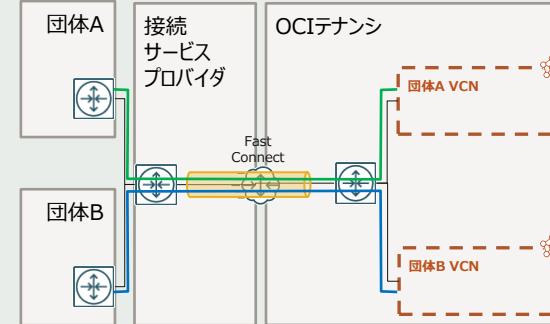
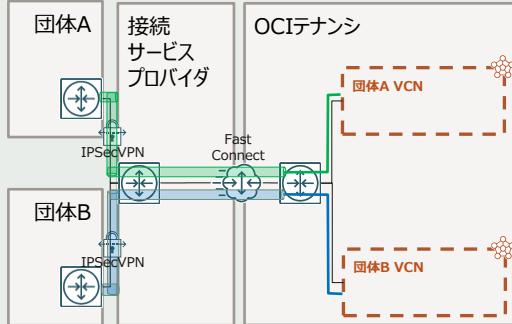
自治体とガバメントクラウドの通信

	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				
特徴・考慮事項	<p>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。</p> <p>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。</p>	<p>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。</p> <p>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。</p>	<p>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。</p> <p>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。</p> <p>他CSPとの連携をどうするか検討が必要となる。</p>	<p>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。</p> <p>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。</p> <p>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。</p>

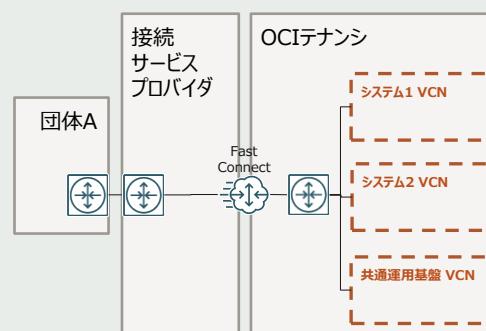
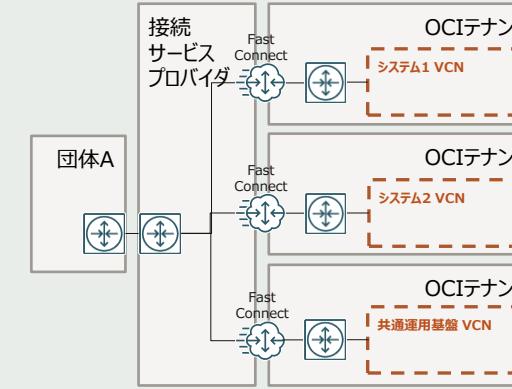
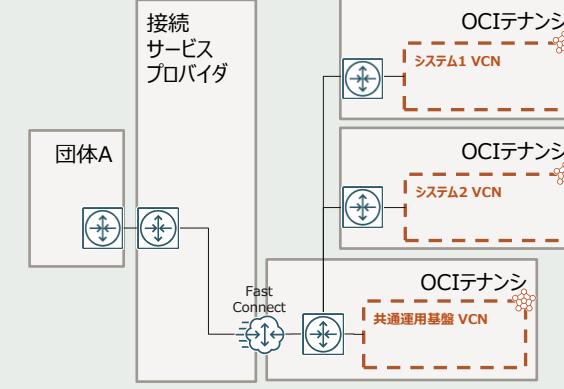


考慮事項：ネットワーク共同利用における自治体IPアドレス重複の対応

自治体のIPアドレス重複時の接続に関して

	FastConnectパートナ	FastConnectダイレクト	IPsec over FastConnect
概要	利用自治体ごとに仮想回線(VC)を準備してネットワーク経路を分離する方式	専用の物理回線を新たに準備し、物理回線上に複数の仮想回線(VC)を作成してネットワーク経路を分離する方式	FastConnectの仮想回線上でIPSecVPNを張り、ネットワーク経路を論理的に分離する方式
構成	 <pre> graph LR subgraph CommunityA [Community A] A1[OCIテナント] --- A2[接続サービスプロバイダ] A2 --- A3[Fast Connect] A3 --- A4[OCIテナント] A4 --- A5[団体A VCN] end subgraph CommunityB [Community B] B1[OCIテナント] --- B2[接続サービスプロバイダ] B2 --- B3[Fast Connect] B3 --- B4[OCIテナント] B4 --- B5[団体B VCN] end </pre>	 <pre> graph LR subgraph CommunityA [Community A] A1[OCIテナント] --- A2[接続サービスプロバイダ] A2 --- A3[Fast Connect] A3 --- A4[OCIテナント] A4 --- A5[団体A VCN] end subgraph CommunityB [Community B] B1[OCIテナント] --- B2[接続サービスプロバイダ] B2 --- B3[Fast Connect] B3 --- B4[OCIテナント] B4 --- B5[団体B VCN] end </pre>	 <pre> graph LR subgraph CommunityA [Community A] A1[OCIテナント] --- A2[接続サービスプロバイダ] A2 --- A3[IPsecVPN] A3 --- A4[OCIテナント] A4 --- A5[団体A VCN] end subgraph CommunityB [Community B] B1[OCIテナント] --- B2[接続サービスプロバイダ] B2 --- B3[IPsecVPN] B3 --- B4[OCIテナント] B4 --- B5[団体B VCN] end </pre>
特徴・考慮事項	<p>FastConnectパートナーを利用し、自治体ごとに仮想回線(VC)を準備する。</p> <p>各団体はそれぞれの仮想回線を経由して論理的に分離されたネットワーク経路でVCNにアクセスする。</p> <p>物理回線は敷設済を利用するため、発生する費用は仮想回線単位のFastConnectポート料金のみ。</p>	<p>専用の物理回線を準備し、その中に複数の仮想回線(VC)を作成する。</p> <p>各団体は専用の物理回線上に作成された仮想回線を経由して論理的に分離されたネットワーク経路でVCNにアクセスする。</p> <p>新たに専用物理回線を敷設するため、物理回線の敷設費用とFastConnectの物理ポート利用料が発生する。</p> <p>集約する仮想回線の帯域によっては性能問題が発生し得るため、どこまで集約するか等をよく検討する必要がある。</p>	<p>1本のFastConnect仮想回線の中で複数のIPSecVPNを張ることで、論理的に分離された経路を確立することができる。</p> <p>集約する仮想回線の帯域によっては性能問題が発生し得るため、どこまで集約するか等をよく検討する必要がある。</p>

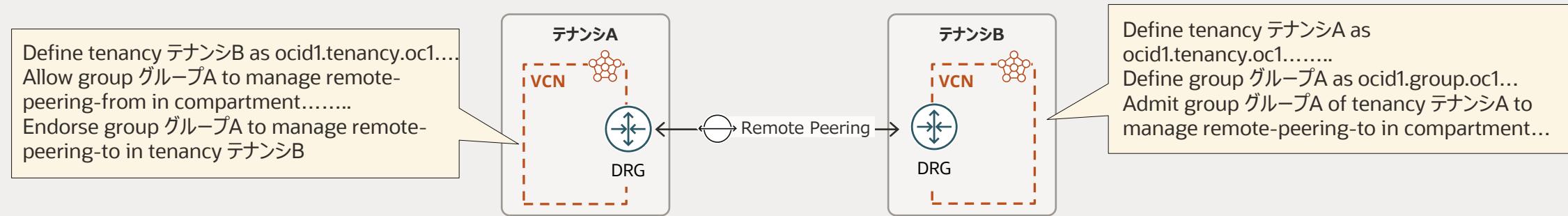
ガバメントクラウド内のシステムの連携 OCI上に複数のシステムがあるケース

	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接続を共有し、DRG間のRPC通信で接続
構成			
特徴・考慮事項	<p>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。</p>	<p>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。</p>	<p>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。</p>



参考：テナント間の接続に必要なポリシー設定 クロステナント・ポリシーの設定

異なるテナントのリソースにアクセスするためには、双方のテナントで**クロステナント・ポリシー**を設定する必要があります。例えば以下のように異なるテナントのVCNをDRG経由でピアリング接続する際など、テナントを跨いだリソースの利用時に必要になるのがクロステナント・ポリシーです。



クロステナント・ポリシーはルート・コンパートメントに対して適用するため、rootユーザー相当の権限が求められます。一方で、現在ガバメントクラウド環境では各利用者に払い出されているAdminユーザーでは、ユーザー・コンパートメントまでの設定は可能ですが、ルート・コンパートメントに対しての操作は許可されていません。そのため、クロステナント・ポリシーの設定が必要な場合には、別途デジタル庁様へご相談願います。

<参考> [Oracle Cloud Infrastructureドキュメント]-[クロステナント・ポリシー]
<https://docs.oracle.com/ja-jp/iaas/database-tools/doc/cross-tenancy-policies.html>

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と他CSP間の直接接続サービ スを利用した連携	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、もしくはOCIとGoogle Cloud間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	<p>団体A</p> <p>接続サービスプロバイダ Fast Connect</p> <p>OCIテナント</p> <p>他CSP環境</p> <p>VCN</p>	<p>団体A</p> <p>接続サービスプロバイダ Fast Connect</p> <p>OCIテナント</p> <p>Azure or Google Cloud</p> <p>VCN</p>	<p>団体A</p> <p>アプリケーションサービスプロバイダ</p> <p>OCIテナント</p> <p>接続サービスプロバイダ</p> <p>他CSP環境</p> <p>?</p> <p>団体A VCN</p> <p>Fast Connect</p>	<p>団体A</p> <p>接続サービスプロバイダ Fast Connect</p> <p>OCIテナント</p> <p>データセンタ</p> <p>VCN</p>
特徴・考慮事項	<p>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。</p> <p>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。</p>	<p>OCIとAzureとの接続環境、もしくはOCIとGoogle Cloud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回線敷設作業を依頼する必要がない。</p>	<p>ASPのデータセンタ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。</p>	<p>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と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。</p>





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(テナント)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。



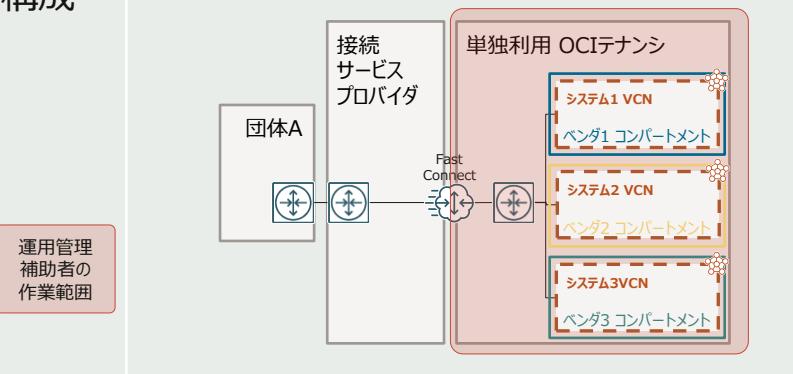
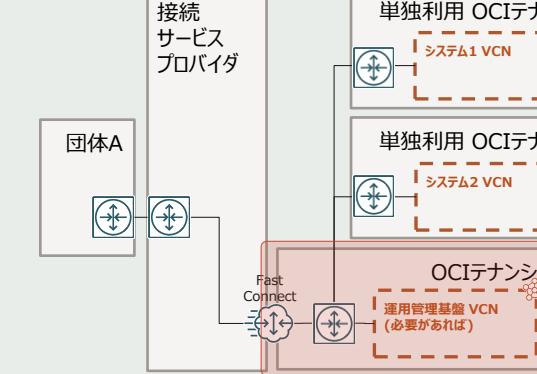
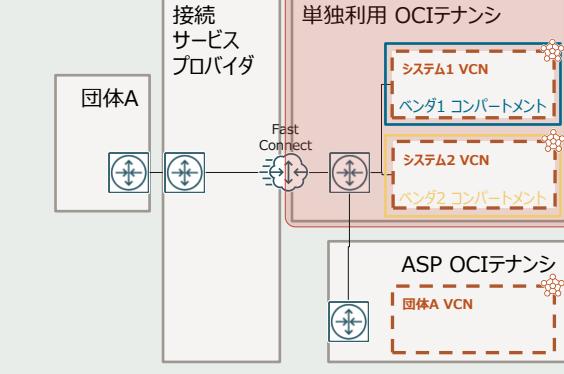
専任のネットワーク運用管理補助者が不要なケース(他者が兼任するケース)

ガバメントクラウドとして払い出されたOCIのテナントには自治体からのネットワーク接続専用の環境がないため、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トはひとつで、このひとつのテナント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ト、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

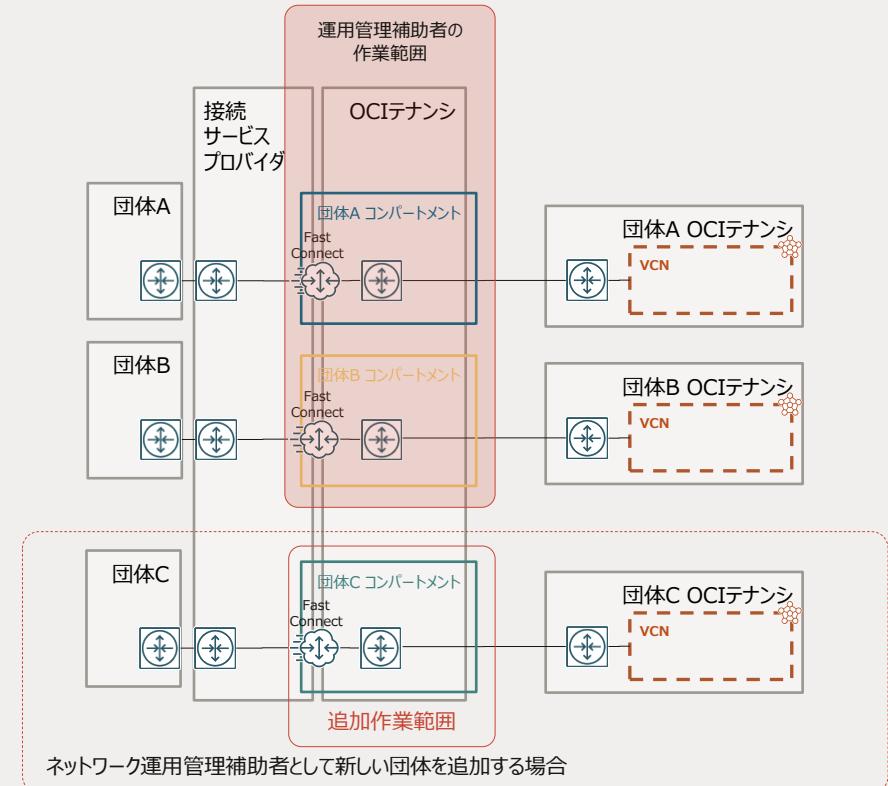
単独利用方式でも、複数ベンダが払い出されたひとつのテナント上にシステムを構築する場合や、複数の払い出された環境(テナント)に分散する場合には、ネットワーク運用管理補助者が必要です。

	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トはひとつでも、このひとつのテナント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ト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トの運用管理補助者が他のテナント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トの運用管理補助者がASPテナントへのネットワーク設定をおこなう必要がある
構成	 <p>団体A</p> <p>接続サービスプロバイダ</p> <p>Fast Connect</p> <p>単独利用 OCIテナント</p> <ul style="list-style-type: none"> システム1 VCN ベンダ1 コンパートメント システム2 VCN ベンダ2 コンパートメント システム3 VCN ベンダ3 コンパートメント <p>運用管理補助者の作業範囲</p>	 <p>団体A</p> <p>接続サービスプロバイダ</p> <p>Fast Connect</p> <p>OCIテナント</p> <ul style="list-style-type: none"> 運用管理基盤 VCN (必要があれば) <p>単独利用 OCIテナント</p> <ul style="list-style-type: none"> システム1 VCN ベンダ1 コンパートメント システム2 VCN ベンダ2 コンパートメント 	 <p>団体A</p> <p>接続サービスプロバイダ</p> <p>Fast Connect</p> <p>OCIテナント</p> <ul style="list-style-type: none"> 運用管理基盤 VCN (必要があれば) <p>単独利用 OCIテナント</p> <ul style="list-style-type: none"> システム1 VCN ベンダ1 コンパートメント システム2 VCN ベンダ2 コンパートメント <p>ASP OCIテナント</p> <p>団体A VCN</p>

複数の自治体を取りまとめるネットワーク運用管理補助者

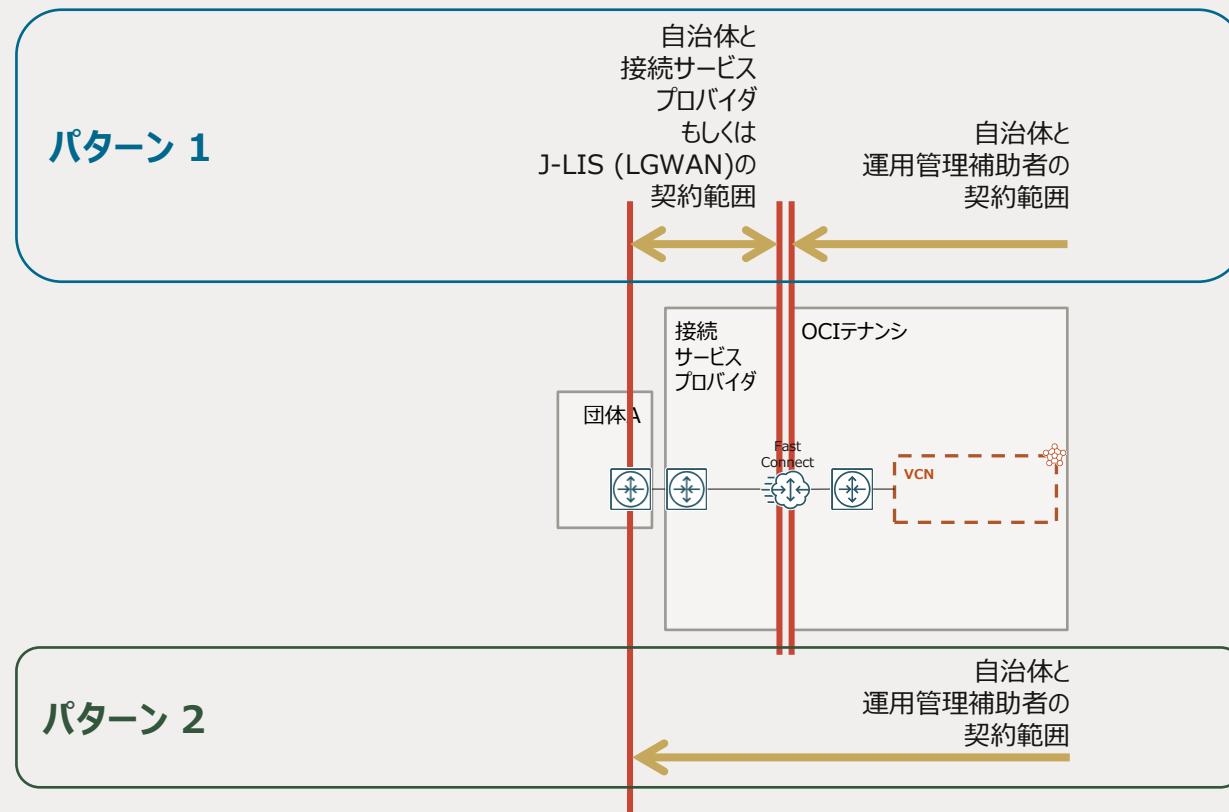
「複数の単独利用環境への接続を集約するケース」の場合、ネットワーク運用管理補助者は団体ごとに環境を分割することもできるが、複数の自治体のネットワーク運用管理をひとつのテナントに集約して構築し、共同利用方式でネットワーク運用管理サービスを提供できる。

新しい団体のネットワーク運用管理を追加する場合、同じテナントに新しい団体の環境を追加できる。



ネットワーク運用管理補助者とネットワーク接続サービスプロバイダの役割分担

ガバメントクラウドでは、払い出されたクラウド環境を運用管理する事業者を運用管理補助者として定義しているが、自治体との契約によってはネットワーク接続サービスプロバイダとの契約も自治体ではなくネットワーク運用管理補助者がおこない、クラウド環境の運用管理と合わせて自治体に費用請求するパターンも考えられる。



ORACLE

