ORACLE
Cloud Infrastructure

接続冗長性ガイド

ORACLE WHITE PAPER | 2020年1月

免責事項

下記事項は、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コミットメント（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。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

改訂履歴

本ホワイトペーパーは、初版の公開後、次の改訂がありました。

日付	改訂内容
2020年1月24日	FastConnectに関する記述を修正
2019年9月5日	図11を更新
2019年5月30日	初版発行

目次

概要

エンタープライズ顧客は、クラウド・デプロイメントで成長を実現しており、クラウドにデプロイされるクリティカル・アプリケーションは増え続けています。こうした成長にあわせて、クラウド・インフラストラクチャが使用可能であること、オンプレミス・ネットワークに冗長な形で接続されていることを確認し、計画済のメンテナンス停止と計画外の停止時間に対応できるようにしなければなりません。

このホワイトペーパーの目的は、現在のデプロイメントで冗長性を確認し、Oracle Cloud Infrastructureへの単一接続を冗長接続にアップグレードできるよう備えることです。FastConnectを通じ、またインターネット上のVPN Connect（IPSec VPN）を通じて、接続のユース・ケースとオプションをいくつか検討します。ルーティングのプロトコルと概念、IPSec VPNの技術と構成、Oracle Cloud Infrastructureの概念とコンポーネントについて読者が熟知しているものと想定しています。

設計上の考慮事項

Oracle Cloud Infrastructureにリソースをデプロイする際には、オンプレミス・ネットワークへの単一接続から小さく始めるといいでしょう。その単一接続には、FastConnectとVPN Connectのどちらを使用することもできます。VPN Connectを使用するのが、Oracle Cloud Infrastructureへの接続をデプロイするには最速です。

冗長性を計画するためには、オンプレミス・ネットワークとOracle Cloud Infrastructureとの間でコンポーネント（ハードウェア、施設、回線、電力）をすべて考慮する必要があります。また、施設がパス間で共有されないように、多様性も考慮します。

冗長性ソリューションのために考慮する必要があるコンポーネントは、表1のとおりです。

表1. 設計上の考慮事項

コンポーネント	備考
インターネット・サービス・プロバイダ（ISP）	ISPはすべて同じではありません。ISPから関係をピア接続すると、トラフィックのルーティングが効率化し、インターネット上で異なるレイテンシを削減できます。
ハードウェア	冗長ハードウェアでサービスを有効化し、パスのどこにもシングル・ポイント障害が発生しないようにします。インフラストラクチャのメンテナンスはどのように扱いますか（オラクルと自社IT部門のどちらが担当するか）。停止時間は許容できますか。どのくらいの停止時間なら許容できますか。
施設の多様性	冗長電源はありますか。建物には、複数の電気通信エントリ・ポイントがありますか。設備が異なるラックまたはデータ・センターにありますか。

コンポーネント	備考
Oracle FastConnectのPOP多様性	両方のFastConnect回線を同じポイント・オブ・プレゼンス（POP）で終端させますか。それとも異なる場所で終端させますか。POP多様性が使用できるのは、フェニックス、アッシュバーン、フランクフルト、ロンドンの各リージョンだけです。
回線プロバイダの多様性	多様なキャリアを利用する予定がありますか。WANまたはインターネット回線は十分に多様ですか。それともPOPを共有しますか。キャリアが違っても、回線が完全に多様だとは言えないことに注意してください。

冗長性のユース・ケース

この項では、Oracle Cloudへの冗長接続の作成方法を、まず単一のFastConnectまたはVPN Connect接続から説明し、以下のユース・ケースまで進んでいくことにします。

- 冗長カスタマ・エッジ・デバイスによるVPN Connect
- VPN ConnectプラスFastConnect
- 冗長FastConnect

このユース・ケースでは、同じリージョン内のみで、プライマリとバックアップの接続を設定する方法を説明します。

Oracle VPN Connect

Oracle VPN Connectは、インターネットをトランスポートおよび暗号化に使用してインターネットからのトラフィックを保護することによって、オンプレミスのネットワークをOracle Cloudにプライベート接続する最も簡単な方法です。VPN Connect接続を作成すると、冗長性のために同じリージョンの2つのトンネル・エンドポイント（ヘッドエンド）にオラクルからパブリックIPアドレスが提供されます。本書では、トンネルのコンセプトとエンドポイントを理解しやすいように、VPNヘッドエンドを独立したコンポーネントとして表しています。しかし一般的には、これは動的ルーティング・ゲートウェイ（DRG）への接続です。

このソリューションは、オンプレミス・ネットワーク上の1つのエッジ・デバイスと、単一のOracle Cloudリージョンの2つのVPNヘッドエンド（デフォルト）で構成されています。エッジ・デバイスは、本社、データ・センター、コロケーション施設、他のクラウドなど、どこにあってもかまいません。

図1に、単一VPN Connect接続のデフォルト設定を示します。

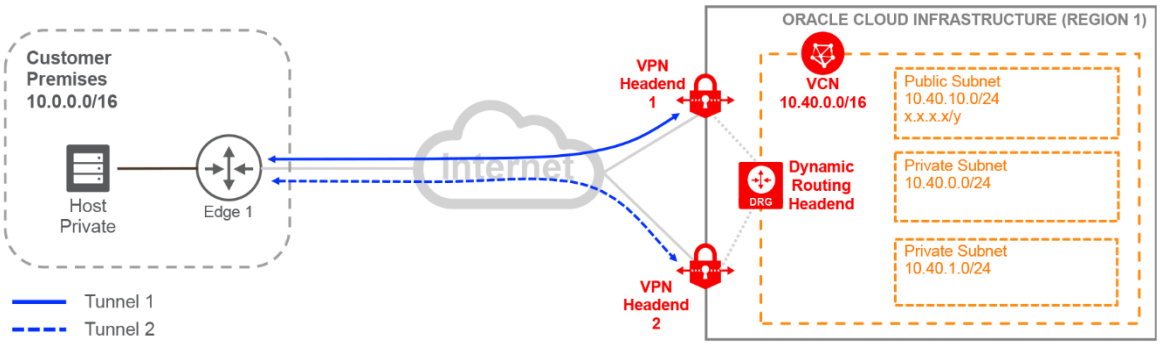

図1. 1つのカスタマ・エッジ・デバイスを使用する単一リージョン用のVPN Connect

図2に、このソリューションの動作に必要なルーティングの概略を示します。トラフィックを許可するには、セキュリティ・リストも適宜更新する必要があります。本書では、セキュリティ・リストについては扱いません。リストの内容はこの接続で許可するアプリケーションの種類とトラフィックによって異なるからです。

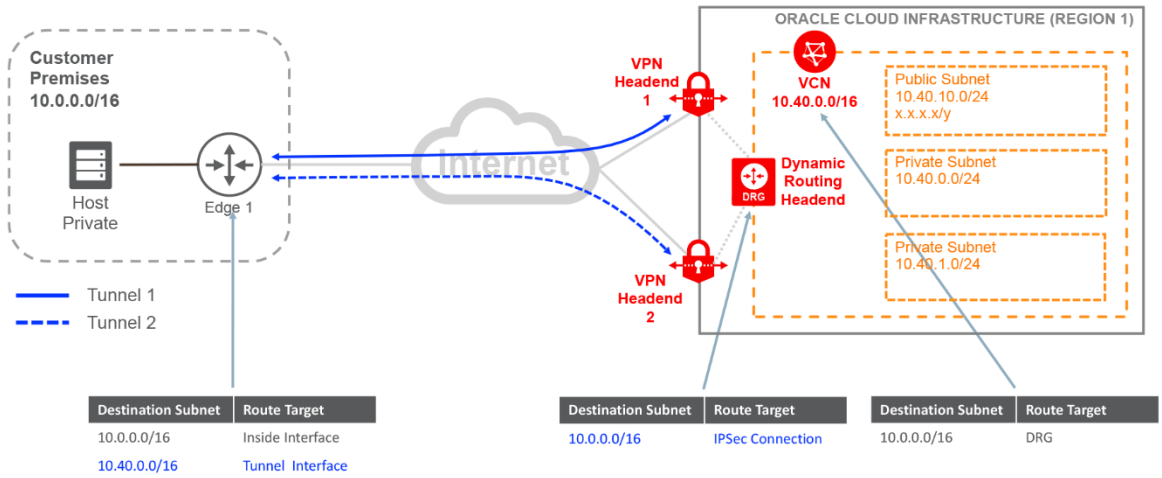

図2. 単一のカスタマ・エッジ・デバイスを使用する単一リージョン用のVPN Connectのルーティング

図2で示したように、冗長性はオラクル側でのみ提供されます。このソリューションでは、カスタマ・エッジ・デバイスがシングル・ポイント障害になります。この問題を解消するには、次の2つのユース・ケースで示すように、2つの方法があります。

冗長カスタマ・エッジ・デバイスによるVPN Connect

図1と図2で示したVPN Connectのソリューションにはシングル・ポイント障害があります。カスタマ・エッジ・デバイスです。この問題を解消するには、異なるデータ・センターまたは別のクラウドで、プライマリ・デバイスと同じ場所に2番目のエッジ・デバイスをデプロイします。2番目のデバイスがプライマリと同じ場所にある場合は、異なるインターネット・プロバイダ、LANスイッチ、電源ユニットに接続していることを確認します。エッジ・デバイスが一般的な障害点を共有していないことも確認してください。

単純化するために、図3では2つのカスタマ・エッジ・デバイスが同じ場所にデプロイされており、2つのキャリアでインターネットに接続していることにします。前述したように、VPN Connectは1つの接続ごとに2つの終端VPNを自動的に提供します。オラクルのヘッドエンドはインターネットに多様に接続しており、同じリージョン内の多様なデータ・センターに配置されています。図3に示すとおり、各エッジ・デバイスには2つのトンネルがあり、それぞれ青い線（トンネル）、赤い線（バックアップ・トンネル）で表されています。

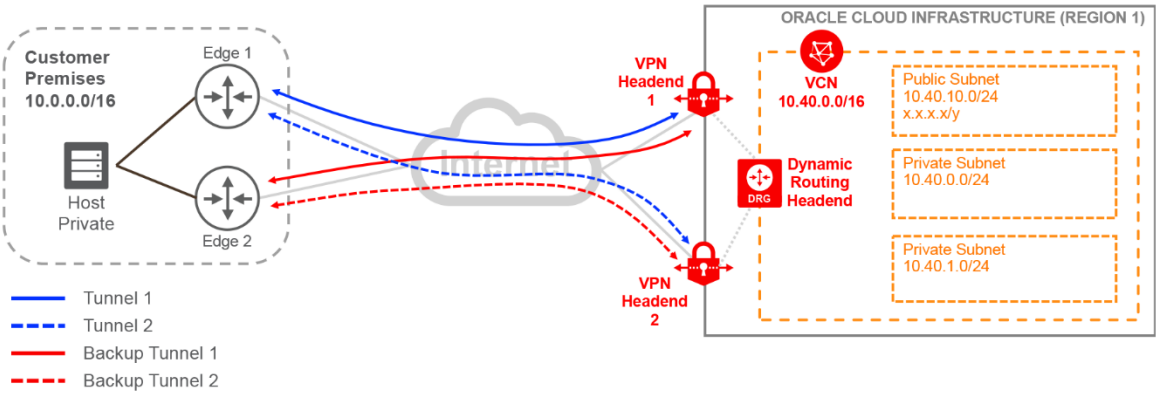

図3. 冗長カスタマ・エッジ・デバイスを使用する単一リージョン用のVPN Connect

4つのトンネルで冗長性が実現されていますが、ルーティングのデプロイメントが複雑になりそうです。ここで、4つのトンネル上のルーティングを構成し、各トンネルの優先順位を決める必要があります。図3では、顧客の側では、エッジ1でエラーが発生するか、そのインターネット回線が停止した場合にのみ、エッジ1からエッジ2に戻るトラフィックがエラーになります。

注意：オラクルには、リージョンごとに複数の多様・冗長なヘッドエンドがあります。図3では、そのうち2つしか示していません。

冗長性が維持される場合は、接続ごとに2つ目のトンネルを作成しない選択もできます。トンネルの数を4つから2つに減らすと、このソリューションを単純化できます。その場合でも、将来的に個性が必要になったときのために、オラクルは2つ目のヘッドエンドに接続情報を引き続き提供します。この設計にもまだ冗長性と多様性があります。図4に示すとおり、各エッジ・デバイスは異なるOracle VPNヘッドエンドに対して1つのトンネルを確立しているからです。単純化したこのバージョンでは、ルーティングを通じてさらに効率的に制御できるように、アクティブ/パッシブ・ソリューションを提供します。

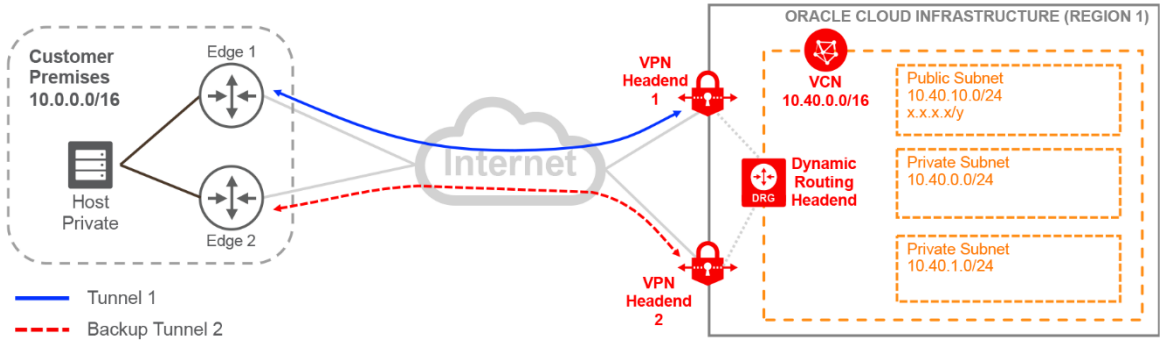

図4. 冗長カスタマ・エッジ・デバイスを使用する単一リージョン用のVPN Connect、簡略版

このソリューションではパスが完全に多様なので、次のステップでは接続の両側でルーティングが正しく設定されるよう確認して、プライマリおよびバックアップのパスを定義します。図5では、青いトンネル（トンネル1）がプライマリ・パス、赤いトンネル（バックアップ・トンネル2）がバックアップです。ルーティングに影響するように、プライマリ・パス上では固有性の高いルートに通知し、バックアップ・パス上では固有性の低いルートに通知することをお薦めします。このアプローチでは、トラフィックが双方向で対称形になります。プライマリ・パスでエラーが発生すると、バックアップ・パスを通じて固有性の低いルートが使用可能になります。プライマリ・パスが復帰すると、固有性の高いルートに通知するため、プライマリ・パスに戻るトラフィックはエラーになります。

このユース・ケースでは静的ルーティングを使用しているため、パスが使用できなくなったときにルート表からルートを削除できるようにルーティングを設定することが重要です。そうしないと、エラー時にトラフィックがバックアップ・パスに移りません。VPN Connectは、ボーダー・ゲートウェイ・プロトコル（BGP）もサポートしているので、それに応じてルートを操作することもできます。

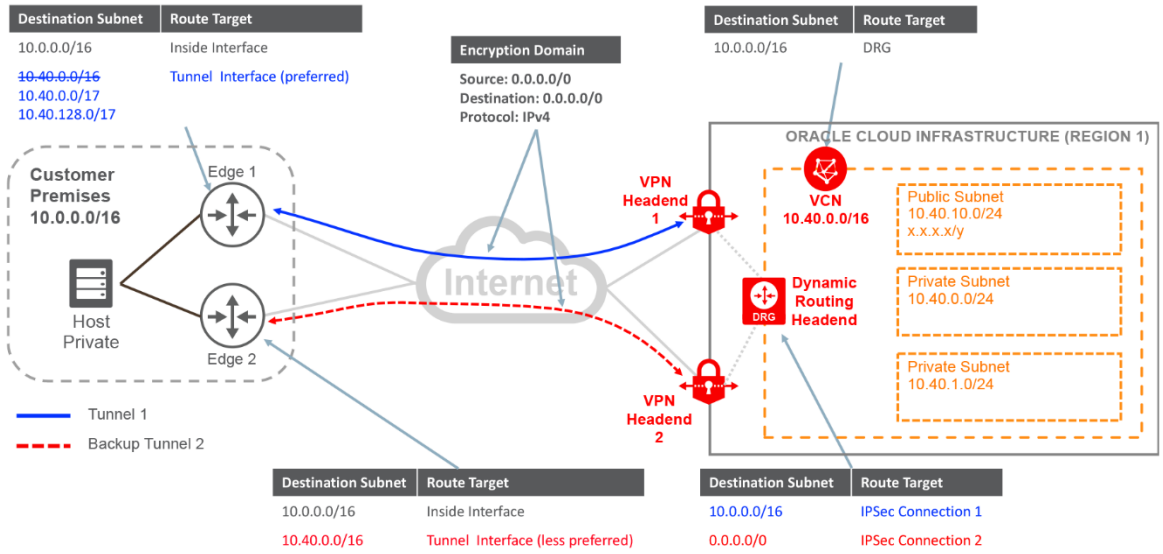

図5. 冗長カスタマ・エッジ・デバイスを使用する単一リージョン用のVPN Connectのルーティング

図5では、各コンポーネントのルーティングを示しており、ルートに割り当てた色で所属先のパスを強調しています。オンプレミス・ネットワークでは、どちらのエッジ・デバイスも同じVCNサブネットに通知するので、内部ルーティング・プロトコルに基づいてプライマリ（青色）パスを変更します。オラクル側から、プライマリ（青）パスではオンプレミス・ネットワークに通知し、バックアップ（赤）パスではデフォルト・ルートまたは固有性の低いルートに通知します。図5で、取消し線を引いた部分は既存の構成で変更が必要な箇所を示しています。図5には、プライマリ・パス上のオンプレミス・ネットワークから、固有性の高いサブネットの数値が反映されています。同じ結果は、プライマリ・パスを優先するように内部ルーティング・プロトコルのメトリックを操作して達成することもできます。

ルーティングは、このソリューションが動作するために重要であり、トンネルでの*暗号化ドメイン*の構成からは独立しています。ルーティングを使用すると、どのトラフィックをトンネル・インタフェースに送信するかを決めることができますが、どのトラフィックを暗号化するかは暗号化ドメインによって決定されます。図5で、暗号化ドメイン（図の中央）は、どちら側のどのトンネルに対しても同じですが、ルーティングはプライマリ・パスと、冗長性のためのバックアップ・パスへの接続の両端で処理されます。このソリューションでは、ルーティングで特定のサブネットを使用しますが、トンネルごとの暗号化ドメインは1つのままです。

注意：暗号化ドメインは、トンネル内で暗号化される「注目のトラフィック」を定義します。Oracle Cloud Infrastructure仮想クラウド・ネットワーク（VCN）またはオンプレミス・ネットワークで複数のサブネットに対応しようとして複数の暗号化ドメインを作成しないでください。かわりに、サブネットを1つのスーパーネット（複数のサブネットを1つのCIDR接頭辞で1つのネットワークに一体化、つまり集約したもの）に集約します。たとえば、VCNネットワークが 10.40.0.0/17と10.40.128.0/17で、オンプレミス・ネットワークが10.0.0.0/18、10.0.64.0/18、10.0.128.0/18、10.0.192.0/18の場合、任意対任意、または10.0.0/16対10.40.0.0/16を使用して1つの暗号化ドメインを作成できます。

VPN ConnectプラスFastConnect

接続をアップグレードし、Oracle CloudにFastConnectソリューションをデプロイする必要がある場合があります。FastConnectは、プライベート接続を通じてOracle Cloudに接続できるソリューションです。FastConnectのほうが、VPN Connectよりパフォーマンスが向上し、帯域幅も大きくなります。オラクルは、FastConnectを通じて次の種類の接続を提供します。

表2. FastConnectのオプション

FastConnect	説明
Oracleプロバイダ	この接続オプションは、任意のOracle FastConnectパートナからのネットワーク接続サービスを使用する予定である、またはすでに使用している場合に適しています。パートナによっては、Oracle FastConnectパートナから冗長クラウド接続サービスを注文する必要があります。 データ・センターの所在のリストは、「Oracle FastConnectパートナ」を参照してください。

FastConnect	説明
サードパーティ・プロバイダ	この接続オプションは、特定のネットワーク・キャリアとすでに関係がある場合、あるいはオンプレミスまたはリモートのデータ・センターがオラクルのFastConnectパートナによるサービスを受けていない場合に適しています。
コロケーション	この接続オプションは、Oracle FastConnectロケーションにすでにプレゼンスがある、またはいずれかにコロケーション・プレゼンスを確立したい場合に適しています。この接続を1つのデータ・センターに2つ注文して冗長性を確保することができます。

以上のオプションの詳細は、FastConnectのドキュメントを参照してください。

図6では、FastConnectロケーションにコロケートされている場合に、プライベート・クラウドがプロバイダまたはクロス・コネクトに当たります。このソリューションでも引き続きVPN Connectを使用しますが、ここではプライマリ・パスではなくバックアップ・パスとして使用します。FastConnect上で、エッジ2へのDRGからBGPを使用してルートを交換します。

FastConnectとVPN Connectを、オンプレミス・ネットワークの同じエッジ・デバイスからはデプロイしないでください（シングル・ポイント障害が発生します）。図6に示すように、別々のエッジ・デバイスを使用してサービスをデプロイしてください。

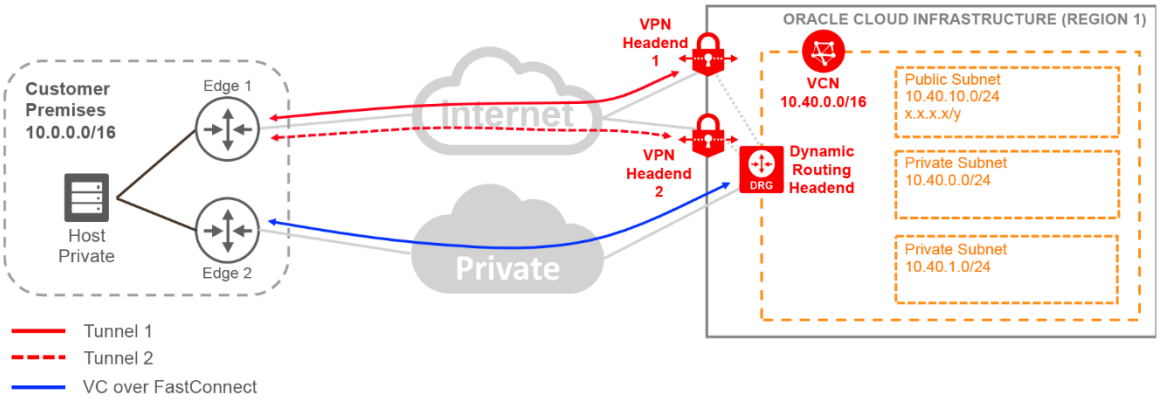

図6. FastConnectプラス単一VPN Connect接続

ルーティングのために、前のソリューションと同じアプローチに従います。ここで、固有性の高いルートにはプライマリ・パス（FastConnect上のVC）を通じて通知し、固有性の低いルートにはバックアップ・パス（VPN Connect）を通じて通知します。DRGは、FastConnect上のBGPを通じてオンプレミス・ネットワークを学習し、VPN Connect上で静的ルーティングまたはBGPを使用できます。ネットワーク内でルーティングを操作し、VPN Connectを通じて学習されたルート上のFastConnectを通じて学習されたルートを優先します。たとえば、AS prependまたはローカル・プリファレンスを使用します。

図7は、接続の両側におけるルーティング構成を示したものです。

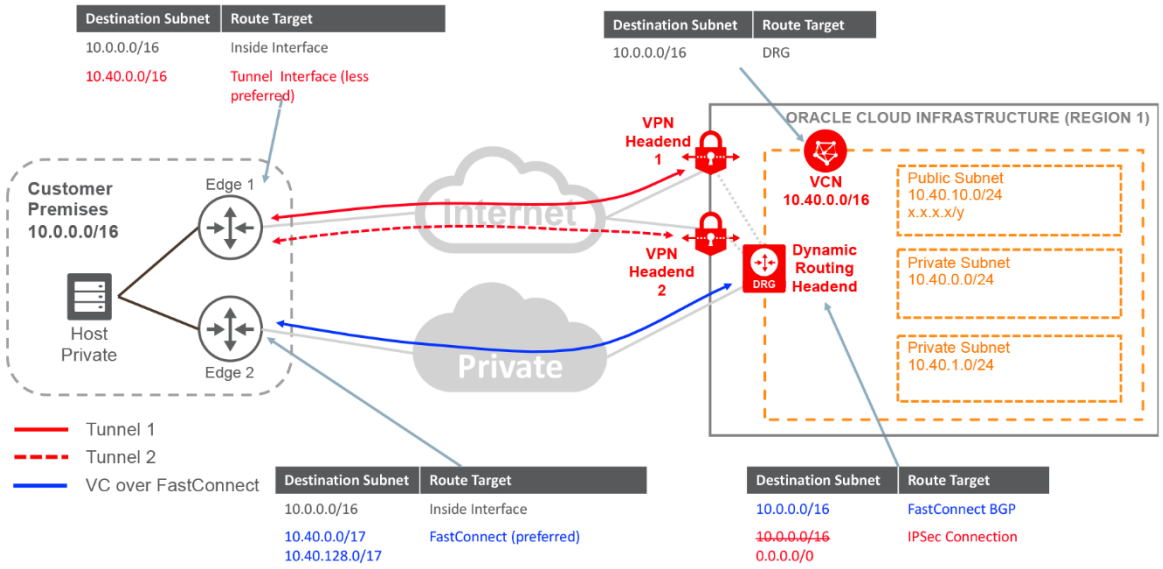

図7. FastConnectプラス単一VPN Connect接続のルーティング

冗長FastConnect

前の項で説明したようにオラクルは、Oracleプロバイダ、サードパーティ・プロバイダ、オラクルとのコロケーションという3種類のFastConnectを提供しています。単純化するために、図8に示すプライベート・クラウドは、FastConnectの任意のオプションを表しています。FastConnectのいずれかのタイプが特に必要な場合は、別途指定しています。

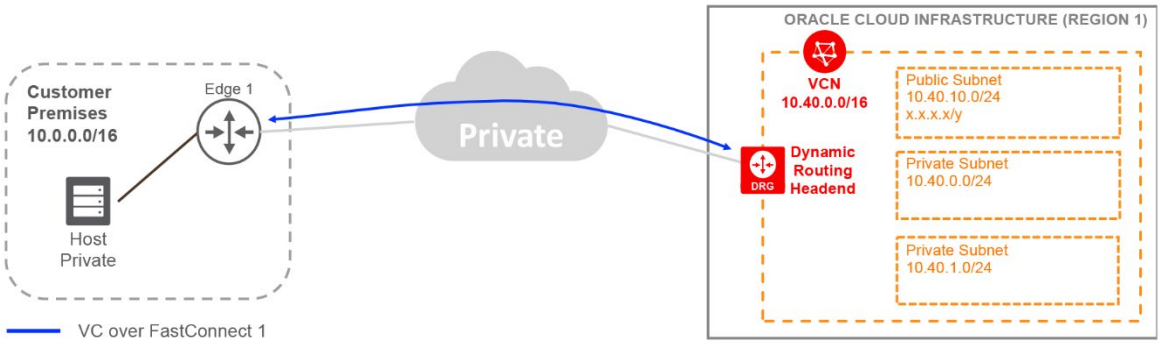

図8. 単一FastConnect

図8に示すように、クラウドへのデプロイメントは、単一FastConnect接続とプライベート仮想回線（VC）を使用して始めてもかまいません。OracleプロバイダでFastConnectをデプロイした場合は、POP（ポイント・オブ・プレゼンス）でプロバイダ・ネットワークに接続しているか、プロバイダがすでにバックボーン・プロバイダでした。サードパーティ・プロバイダでFastConnectをデプロイした場合は、プロバイダのネットワークからオンプレミスのネットワークに回線をリクエストしました。

オラクルとのコロケーションを使用する場合は、施設プロバイダからのクロス・コネクトをリクエストしてオラクルに接続しています。

FastConnectで冗長性を確立する場合は、冗長性と多様性を確保できるように、物理的な接続性に注意してください。パートナおよびキャリアと協力する際は、必要な多様性が提供されるように、既存の接続の物理的な接続性が十分理解されていることを確認してください。

FastConnectの場所（フェニックス、アッシュバーン、フランクフルト、ロンドン）によっては、オラクルはパートナがオラクルに接続できる物理的なロケーションを2つ用意しています。図9に示すように、各ロケーションでオラクルは冗長エッジ・デバイスを提供しています。

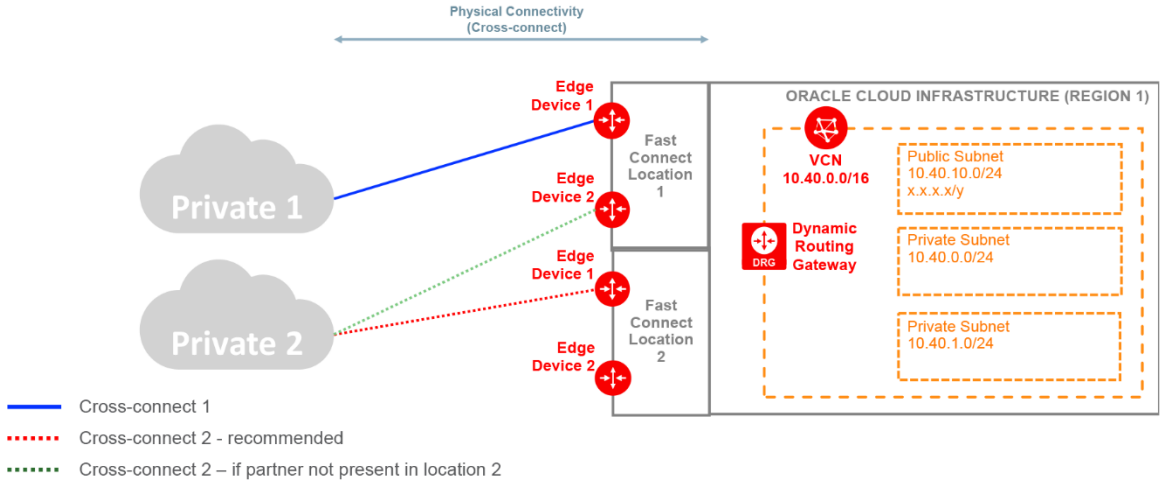

図9. Oracle FastConnectリージョンの物理的な概要

この例に沿って、すでにクロス・コネクト1（青色）は設定されており、そこでロケーション1、エッジ・デバイス1は終端されます。2番目のFastConnect接続をデプロイする場合は、赤い線で示したようにロケーション2で終端することをお薦めします。これは、Oracleプロバイダ、サードパーティ・プロバイダ、ロケーション1のみでのコロケーションのいずれかです。その場合、ロケーションの多様性はなくなりますが、ハードウェアの多様性は確保されます。2番目のFastConnect接続がエッジ・デバイス2をロケーション1で終端するからです（図9の緑色の線）。

注意：オラクルとの冗長性の判定については、Oracleパートナにお問い合せください。

Oracleプロバイダ、サードパーティ・プロバイダ、またはコロケーション・プロバイダとの間で物理的な冗長性を確認できると、図10に示すようにOracle CloudへのFastConnect接続が2つ成立します。

そこで、どの接続をプライマリに、どの接続をバックアップにするかを決める必要があります。これは、接続のパフォーマンスまたは容量によって選択できます。本書では、プライベート1をプライマリに、プライベート2をバックアップに指定することにします。2番目のFastConnect接続上で、仮想回線（VC）を作成し、2番目のエッジ・デバイスにBGPを確立することも必要です。

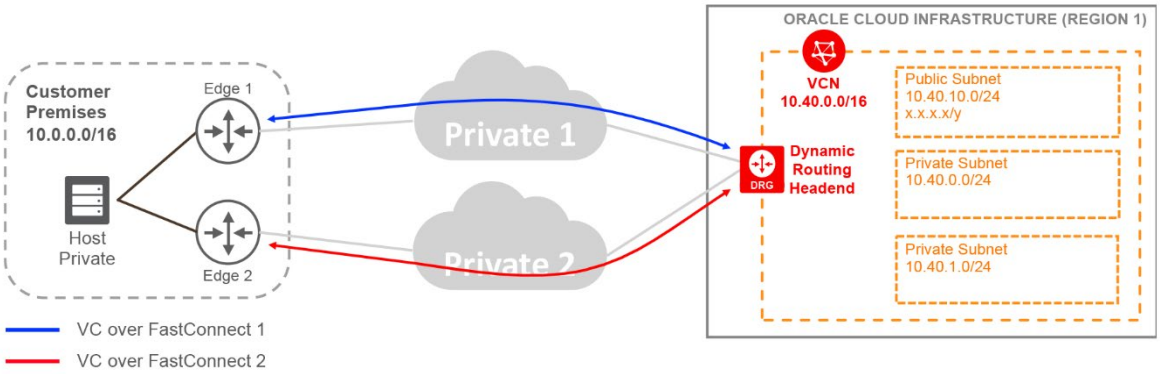

図10. 冗長FastConnect

カスタマ・エッジ・デバイスから適宜ルーティングを操作し、適切なパスを通じてトラフィックをルーティングします。これには、AS prependを実行するか、別の方法で固有性を問わずルートに通知します。

FastConnectでは、BGPを称してオンプレミス・ネットワークとオラクルの間でルートを交換します。

- レイヤー2のプロバイダを使用している場合、仮想回線のBGPセッションはエッジ・デバイスとオラクルの間になります。
- レイヤー3のプロバイダを使用している場合、仮想回線のBGPセッションはプロバイダとオラクルの間になります。

図11に示すように、固有性の高いサブネットにはプライマリ・パスを通じて、固有性の低いサブネットにはバックアップ・パスを通じて通知することをお薦めします。

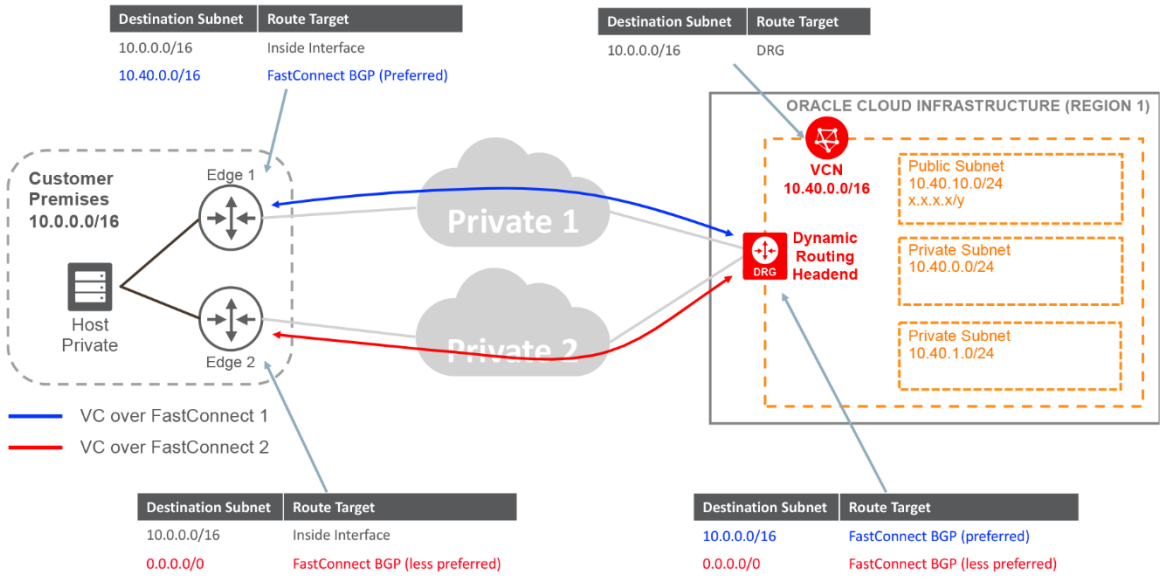

図11. 冗長FastConnectルーティング

参考資料

- VPN Connectのドキュメント
- Oracle Cloud Infrastructure Networkingのドキュメント
- FastConnectのドキュメント

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax：+1.650.506.7200

Integrated Cloud Applications & Platform Services

接続冗長性ガイド
2020年1月
著者：Javier Ramirez