cloudpack専用線接続ホワイトペーパー

Site to site connection service with AWS Direct Connect

リリース 2.0
アイレット株式会社

付録

第2章　はじめに

2.1 cloudpackとは

cloudpackは、アマゾンウェブサービス（AWS）の導入設計、環境構築、運用までをトータルでサポートするマネージドホスティングサービスです。

AWSを知り尽くし、その可能性を最大限に引き出せるcloudpackのスタッフが、Amazon Elastic Compute Cloud（Amazon EC2）やAmazon Simple Storage Service（Amazon S3）をはじめとするAWSのプロダクトを、構築はもちろんのこと、24時間サポートや、サービス監視、バックアップなどの作業代行や技術サポートをスピーディかつ丁寧に行い、お客様のさまざまな運用負荷を可能な限り軽減します。

お客様が、これまで悩みの種だったサーバー周りに関するさまざまな課題から解放され、本来取り組むべきビジネスの課題に専念できるためのサービス、それがcloudpackです。

2.2 「cloudpack　専用接続プラン」とは

AWSを本格的に活用する上で、多くのお客様は以下のようなご要望をお持ちになります。

1. AWSクラウドサービスとプライベートなネットワークを確立したい
2. AWSクラウドサービスと安定した高速なデータ転送を行いたい
3. AWSクラウドサービスとのデータ転送コストを削減したい

このようなご要望にお応えするために、cloudpackはお客様のデータセンターやオフィスからAWSへのプライベートなネットワーク接続を実現する「cloudpack専用接続プラン」をご提供しています。

「cloudpack専用接続プラン」とは、AWS　が提供するプライベートネットワーク接続サービス「AWS Direct　Connect」と、その利用に必要な設備および構築・運用作業の一部もしくはすべてをcloudpackが一括でご提供するプランです。

「cloudpack専用接続プラン」のご利用により、お客様はインターネットを経由せず、プライベートネットワーク接続経由でAWSクラウドサービスのご利用やデータの配信などが可能となります。これにより、お客様環境とAWSクラウドサービスとの間に、以下のようなネットワーク接続環境を実現いたします。

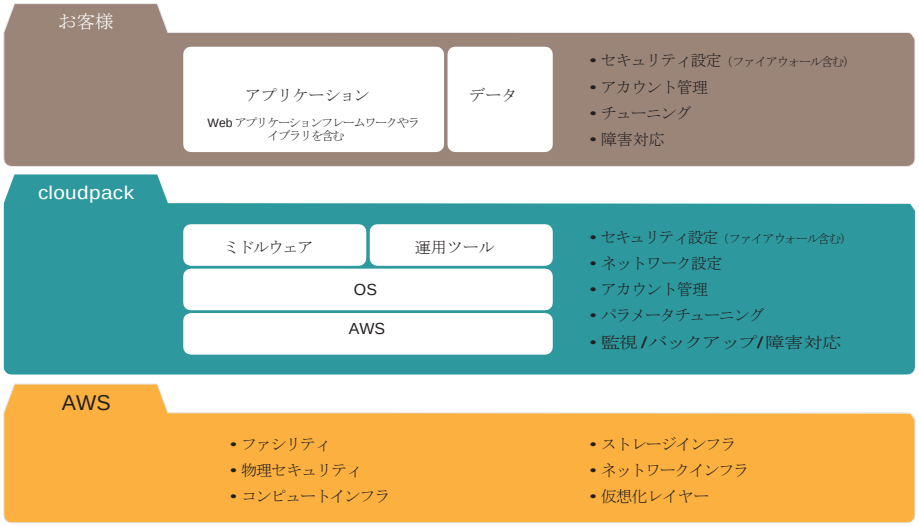
1. プライベートな通信
2. 安定した高速なデータ転送
3. 低コストなデータ転送

2.3 クラウド時代のシステム開発とシステム運用

セキュリティにおける「責任共有モデル」

AWSやcloudpackが提示する「責任共有モデル」(Shared Responsibility Model)は、クラウド運用の発展から生まれてきた考え方の一つです。

cloudpackはAWSクラウドインフラストラクチャを基盤にシステムを構築し、お客様はcloudpackが構築したシステム上で業務アプリケーションを運用することになりますので、セキュリティ上の責任はお客様とcloudpackとAWSの三者による分担となります。



ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティにおけるさまざまなコンポーネントの操作、管理、コントロールは、AWS によって行われ、AWS インフラストラクチャ上にcloudpack が構築したシステムにおけるセキュリティは cloudpack が保護いたします。cloudpack が構築したシステム上で運用される業務アプリケーションおよびデータのセキュリティについては、お客様ご自身で保護していただく必要があります。

従来のオンプレミス（構内設置）環境では、すべてについてセキュリティを確保する必要があったことと比較すると、cloudpack ご利用のお客様については、ご自分でセキュリティを確保していただく範囲が限定されることを意味いたします。

「cloudpack 専用接続プラン」における責任共有モデルの詳細は、4.5「cloudpack 専用接続プラン」における責任共有モデル をご参照ください。

ベストプラクティスによるシステム開発とシステム運用

AWS と cloudpack はクラウドシステム運用の長い経験から、それぞれに数多くのベストプラクティスを蓄積しています。

cloudpack は AWS が提供するベストプラクティスに従ったシステムを構築し、cloudpack の持つベストプラクティスに従って、お客様の環境を運用しています。

従来は、インフラストラクチャから業務アプリケーションまですべてにおいてお客様ご自身による運用ノウハウの蓄積が必要でしたが、cloudpack ご利用のお客様は、お客様が利用される業務アプリケーションの範囲に集中してノウハウの蓄積をしていただければ良いことを意味いたします。

このように、システム構築、運用、セキュリティについて、お客様、cloudpack、AWS がそれぞれに役割と責任を分担することで、より少ない労力で、より早く、求めるものが得られる時代になったと言えます。

AWS のベストプラクティスの詳細については、「付録 3：AWS が提供するシステム構築・運用上のベストプラクティス」をご参照ください。

2.4 本ホワイトペーパーについて

本ホワイトペーパーは、cloudpack がご提供する「cloudpack 専用接続プラン」の詳細をご紹介し、お客様とcloudpack との間で円滑な業務遂行を実現することを目的にご提供するものです。

対象読者：
「cloudpack 専用接続プラン」をご利用中のお客様
「cloudpack 専用接続プラン」の導入をご検討中の方

第3章　AWS Direct Connectとは

3.1 AWS Direct Connect とは

AWS Direct Connect（以下「Direct Connect」）とは、専用線を利用して、お客様のオフィスやデータセンターと AWS の間にプライベートな接続環境を提供するサービスです。

図 3.1 Direct Connect の概要

お客様環境からAWS へのアクセスには、以下の3通りがあります。

1. インターネット経由
通常のインターネットを経由してアクセスします。お客様環境と AWS 間の通信は、HTTPS によって保護されます。

2. インターネットVPN 経由
お客様側に設置したVPN 装置と、AWS Virtual Private Cloud（以下「VPC」）内の仮想プライベートゲートウェイの間でIPSec VPN で接続します。

3. Direct Connect 経由
専用線を経由してアクセスします。専用線はお客様環境と、AWS 側の接続拠点との間に敷設します。

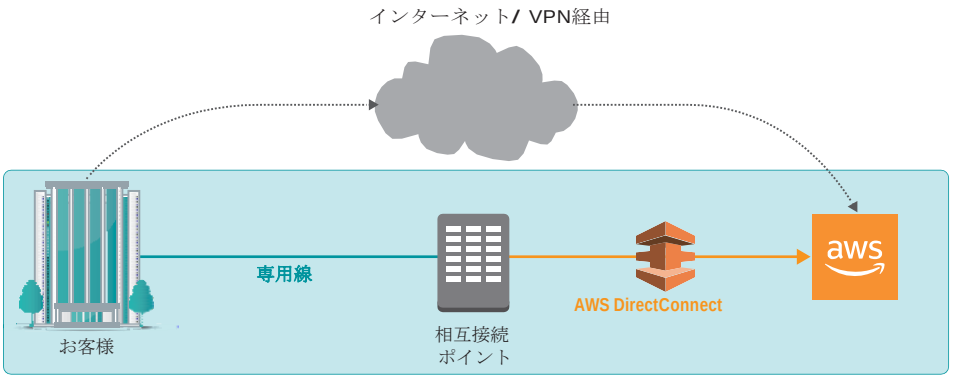


図 3.2 AWS へのアクセス経路

パフォーマンスや通信の保護の観点での特長は、以下の通りです。

接続方法	パフォーマンス	通信の保護
インターネット	△（輻輳の影響を受ける場合がある）	○ （HTTPS による保護）
インターネットVPN	△（輻輳の影響を受ける場合がある）	○ （IPSecによる保護）
Direct Connect	◎（安定したパフォーマンス）	◎（物理的な閉域網）

3.2 Direct Connect のメリット

メリット1 : ネットワーク分離によるAWS 利用パフォーマンスの向上とコストの削減

Direct Connect を利用することで、パブリックリソース（例えば S3 に格納されたオブジェクト）にはパブリック IP アドレススペースを使用してアクセスし、プライベートリソース（例えば VPC 内で実行されている EC2 インスタンス）にはプライベート IP スペースを使用してアクセスすることができるので、パブリック環境とプライベート環境の間でネットワークを分離できます。

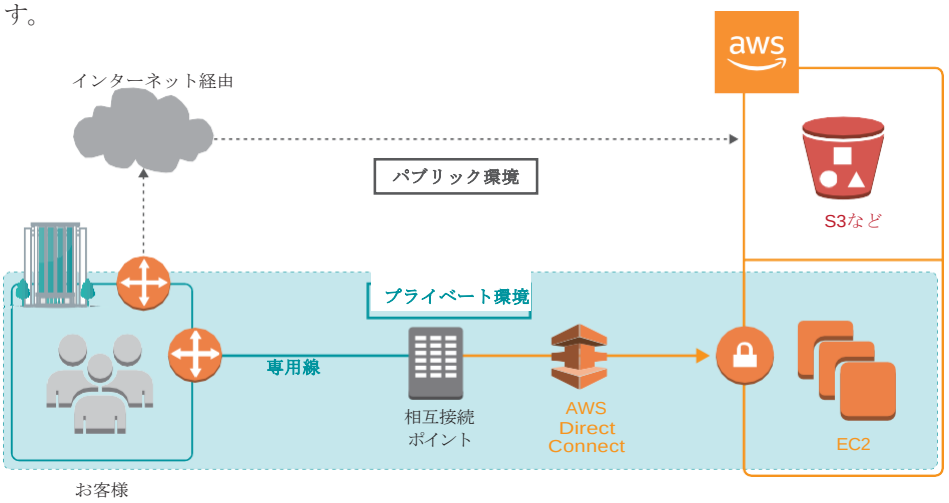


図 3.3 パブリック環境とプライベート環境の分離

パブリックリソースへのアクセスは、従来通りインターネット経由での接続になりますが、プライベートリソースへのアクセスは、プライベートネットワーク経由となり、帯域幅のスループットが向上するとともに、インターネットベースの接続よりも一貫性のあるネットワークパフォーマンスを得ることが可能となります。

メリット2: お客様環境への追加が容易

多拠点をネットワークで接続しているお客様にとっては、Direct Connect を利用することで、あたかも1 拠点が増えたかのように、AWSのクラウドサービスを自社のインフラストラクチャ環境に追加することができます。

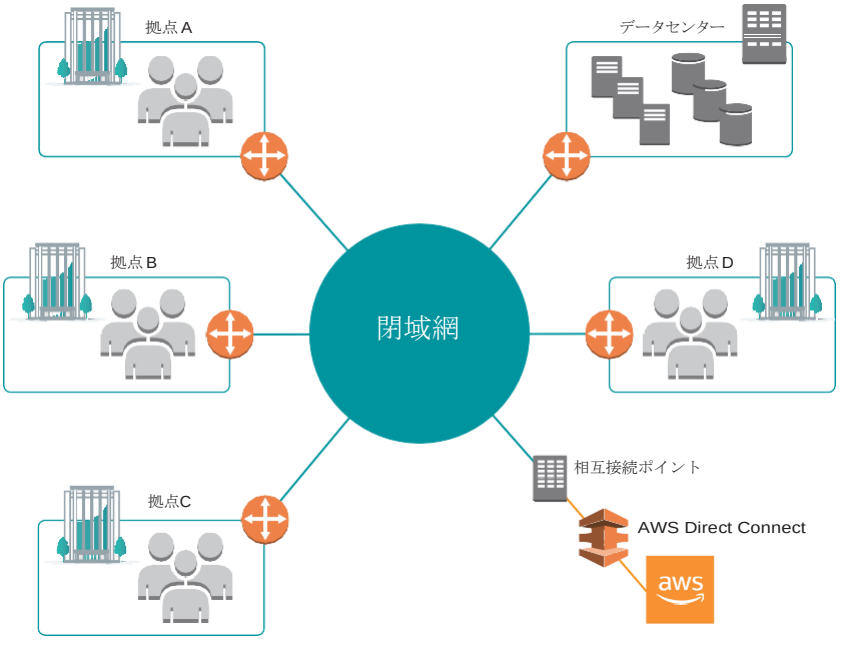


図3.4 仮想拠点としてのAWS の追加

3.3 Direct Connect の利用例

Direct Connect の典型的な利用例としては、以下のような拠点クライアント環境と AWS 上のサーバー環境によるクライアントサーバー構成が挙げられます。

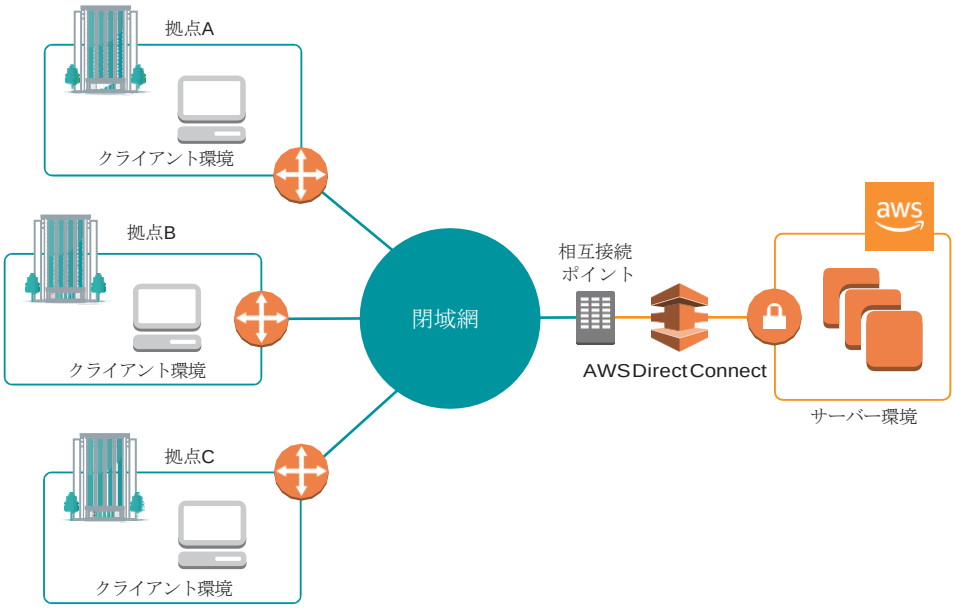


図3.5 拠点クライアントとAWS 上のサーバーによるクライアントサーバー構成

AWSが提供するスケーラブルなサーバー環境を、安定した高品質の閉域ネットワークで社内と接続することにより、「柔軟性のあるオンプレミスなデータセンター」として利用することができるようになります。

第4章「cloudpack 専用接続プラン」とは

「cloudpack 専用接続プラン」とは、お客様のデータセンターやオフィスと、AWS を直結するサービスです。

「cloudpack 専用接続プラン」では、AWS Direct Connect の接続拠点（東京および大阪）内に専用ラックおよび自社機材を設置し、お客様に共有することで低価格を実現しました。

4.1 「cloudpack 専用接続プラン」を活用するメリット

コスト削減

Direct Connect を利用するには、エクイニクス・ジャパンのラックを契約する必要があるため、お客様ご自身でご契約するとコストがかかります。

「cloudpack 専用接続プラン」では、エクイニクス・ジャパンのデータセンター内に cloudpack がご用意しているラックをお客様にご提供し、初期費用をはじめ、月額の使用料金などのコストを削減します。

構築期間の短縮

Direct Connect を自前で初めて構築されるお客様にはまだノウハウがなく、回線事業者との調整やAWS の設定で多くの工数や時間を取られることになります。「cloudpack 専用接続プラン」では、Direct Connect に精通したcloudpack スタッフにより、最短の期間と最小の工数で Direct Connect 環境を構築することが可能となり、お客様のビジネス速度を加速いたします。

cloudpack の安心サポート

cloudpack では、お客様に対してサポートサービスをご提供する窓口として、cloudpack サポートデスクを設置しています。お客様からのご依頼やご相談を承るだけでなく、万が一、お客様のシステムについて障害が発生した場合のご連絡窓口となります。

cloudpack では、お客様とcloudpack スタッフの間のコミュニケーションを円滑に行うため、システムの構築フェーズ、運用フェーズそれぞれにおいて、プロジェクト管理ツール「Backlog」をご提供しております。

cloudpack は、cloudpack サポートデスクを通じて、お客様のシステムの効率的で安定した運用を実現いたします。

4.2 「cloudpack 専用接続プラン」における選択肢

「cloudpack 専用接続プラン」では、お客様のデータセンターやオフィスと、AWS VPC を接続いたします。

お客様のご利用シーンにあわせて、以下の3 点をご選択いただくことで、「cloudpack 専用接続プラン」におけるご利用プランが決定いたします。

1. ご利用回線
2. 相互接続ポイント（Direct Connect ロケーション）
3. Direct Connect コネクションのご利用形態（専有）

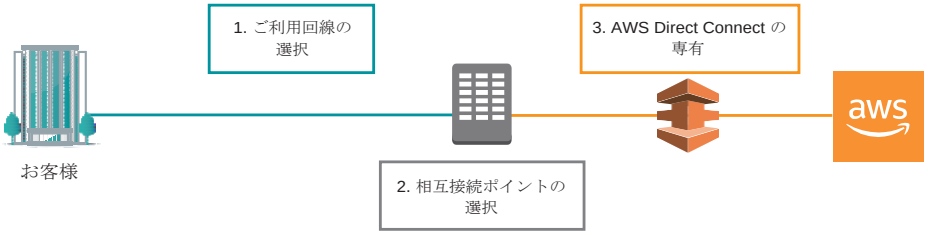


図 4.1「cloudpack 専用接続プラン」の構成

1. ご利用回線

「cloudpack 専用接続プラン」では、お客様のデータセンターやオフィスと、Direct Connect ロケーションとの間を接続する回線にお客様回線のお持ち込みが可能です。

お客様回線持ち込みの利用

お客さまが普段からご利用いただいる専用線（IP-VPN、広域イーサネット）を利用して、お客様のデータセンターやオフィスと AWS の Direct Connect ロケーションを直結するプランです。

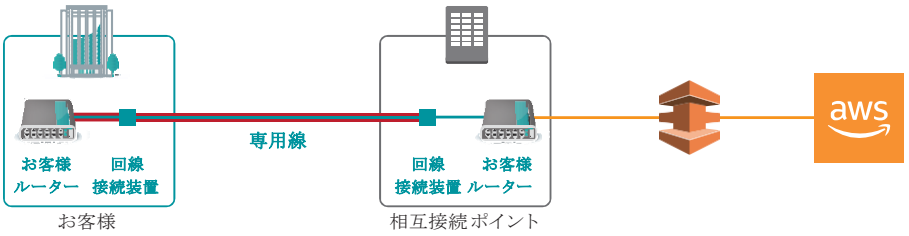


図 4.2 お客様回線持ち込み利用

お客様拠点とDirect Connect ロケーションの間を接続する専用線キャリアについては、特段の制約はありません。

接続回線の詳細については、「付録1 ご参考 : 回線サービスのご案内」をご参照ください。

お客様持ち込み回線の冗長化

お客様回線持ち込みの場合は、2回線ご用意いただくことで、BGP/OSPF などの動的ルーティングによる回線冗長化を実現することができます。

社内情報システムやサービスのバックエンド環境など、高い可用性が求められるお客様にお勧めします。

AWSでは高い回復性を実現する手段として、ロケーションを分ける事をベストプラクティスとしています。

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

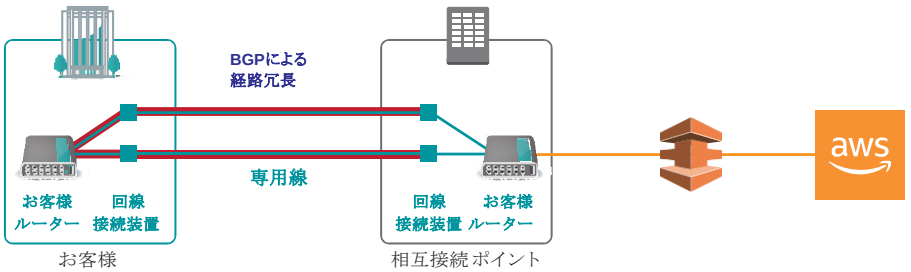


図 4.3 専用線冗長構成の例

2. 相互接続ポイント（Direct Connect ロケーション）

Direct Connect ロケーションとは、AWS リージョンへの入口となる物理的な接続拠点のことで、お客様と AWS との相互接続ポイントとなる場所のことを言います。

「cloudpack専用接続プラン」では、エクイニクス・ジャパンの東京（TY2）、大阪（OS1）で接続ポイントを提供しています。（https://www.equinix.co.jp/partners/AWS/）

ご利用回線が「フレッツ光ネクスト」の場合は、ご契約事業者が NTT 東日本の場合は東京（TY2）、NTT 西日本の場合は大阪（OS1）をご利用いただくことになります。ご利用回線がお客様回線持ち込みの場合は、Direct Connect ロケーションとして、東京（TY2）と大阪（OS1）をご選択いただくことができます。

cloudpack は、東京と大阪のいずれにもサポート拠点を設置し、迅速に対応できる体制をご用意しています。

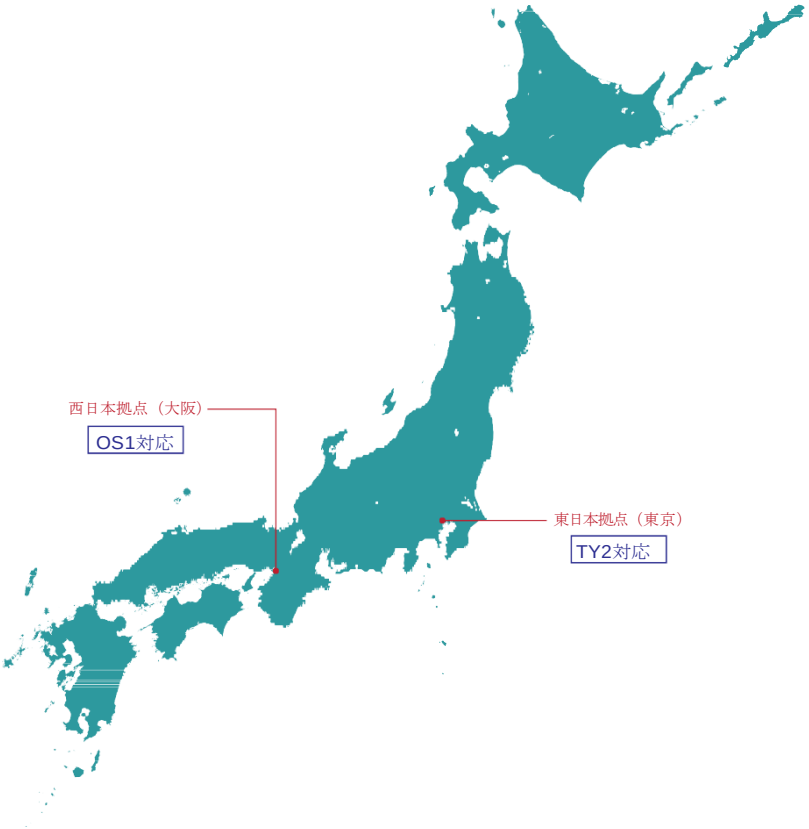


図 4.4 Direct Connect ロケーションとcloudpack サポート拠点

3. Direct Connect コネクションのご利用形態

「cloudpack 専用接続プラン」では、Direct Connect コネクションのご利用形態に専有利用を提供します。

Direct Connect コネクション 専有

Direct Connect コネクションをお客様が専有する利用形態です。Direct Connect のパフォーマンスを最大限活用することが可能となります。

Transit Virtual Interfaceの作成が可能でTransit Gatewayの機能をフルにご活用頂けます。

cloudpack 契約の Direct Connect コネクションを専有してご利用いただきます。
Direct Connect コネクション内の帯域は 1Gbps or 10Gbps（専有）になります。
ルーター（L3 スイッチ）はお客様にご用意いただきます。

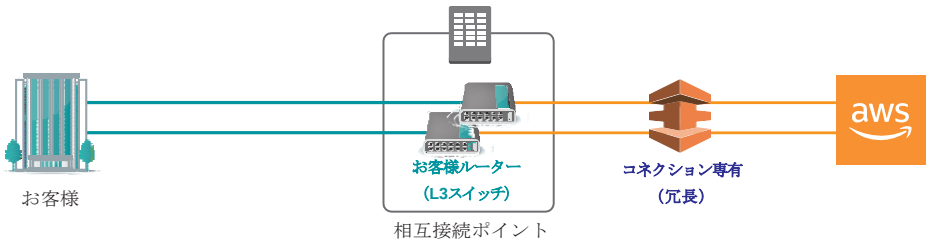


図 4.5 Direct Connect コネクション 専有

Direct Connect の計画メンテナンスなどにより、一定の頻度で数分から1 時間程度の接続断が発生します。本メンテナンスは、実施の数営業日前にアナウンスがあります。ただし、日程調整はできません。AWS機器側で緊急を要す場合は緊急でメンテナンスを実施する事があります。

4.3 必要となる機材の調達と設置

必要となる機材

ご選択いただいたプランの構成に従い、下記の機器をお客様にご用意いただく必要があります。

1. お客様側 ルーター
お客さま環境と専用線を繋ぐために、お客様環境内に設置するルーター機器をご用意いただく必要があります。

回線冗長の場合：2 台

2. Direct Connect ロケーション側 ルーター
お客様回線とcloudpack が Direct Connect ロケーションに設置している機器を繋ぐために、cloudpack が提供するラック内に設置するルーター機器をご用意いただく必要があります。

回線冗長の場合：2 台

お客様側ルーター、Direct Connect ロケーション側ルーターは同一機器で構成する事も可能です。

（回線持ち込みの場合）ONU
お客様回線持ち込みの場合、回線の両端に ONU が必要となります。

回線冗長の場合：2 台

ONUは、一般的に回線提供事業者から提供されます。

コールドスタンバイ機の用意

高い可用性が求められるお客様には、回線冗長の上でさらにコールドスタンバイ機のご用意をお勧めします。

稼動機器のハードウェア障害時には、コールドスタンバイ機への切り替えにより、迅速な機器交換が可能となります。

利用できるルーター

「cloudpack 専用接続プラン」では、以下の仕様を満たしたルーターをご利用いただくことができます。

• BGP（Border Gateway Protocol）に対応し、MD5 認証が利用できること
• 100V で動作すること

お客様環境から、Direct Connect 経由で複数のVPC に接続する場合は、以下の機能が必要になります。

• 802.1q VLAN

回線によっては、PPPoE（Point-to-Point Protocol over Ethernet）に対応している必要があります。詳細については、ご利用の回線事業者にご確認ください。

ご利用いただけるルーターについては「、付録2 ご参考: Direct Connect に対応するルーター製品」をご確認ください。

cloudpack では、ご利用回線の両端（お客様環境と Direct Connect ロケーション）で、同一メーカーのルーター製品のご利用を推奨しています。

機器の設置（Direct Connect ロケーション内ラック）

「cloudpack 専用接続プラン」ご利用のお客様に、ご利用機器を設置するために Direct Connect ロケーション内にcloudpack が設置したラック（以下、「cloudpack ラック」） をご提供しています。ラックには、以下の機器を設置します。

回線に接続する機器

お客様回線持ち込み利用の場合

機器	回線冗長の場合
ルーター	2 台
ONU	2 台

Direct Connect に接続する機器

Direct Connect コネクション専有の場合は、シングルモードファイバー上の 1000Base-LX（10Gbpsの場合は10GBASE-LR）に対応しているネットワーク機器が必要となります。

4.4 お申し込みと導入の流れ

「cloudpack 専用接続プラン」のお申し込みと導入の流れは、下記の図のようになります。

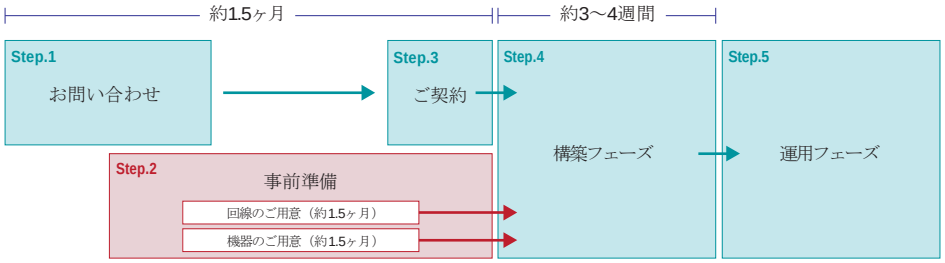


図 4.6 お申し込みと導入の流れ

事前準備から導入まで、概ね 2ヶ月の期間が必要となります。

Step1. お問い合わせ

まず、「AWS 導入相談、お見積りについてのお問い合わせ」（https://cloudpack.jp/contact/form/ ）より、以下の内容でお問い合わせください。

お問い合わせ種別 : AWS 導入相談

> お問い合わせ内容: 以下の内容をご記載ください。
>
> サービス名：
> cloudpack 専用接続プラン
>
> ご利用回線種別：
> フレッツ光 / お客様回線
>
> Direct Connect の利用形態：
> 専有（1Gbps or 10Gbps）
>
> 場所：
> 東京 / 大阪
>
> ご利用開始希望日：
> 会社名:
> お名前:
> ご連絡先電話番号：
> ご連絡先メールアドレス：

1営業日以内に、cloudpack 営業担当よりご連絡いたします。

Step2. 事前準備（約 1.5 ヶ月）

ご契約前に以下のご用意をお願いいたします。事前準備には、概ね 1.5ヶ月程度の期間が必要となります。

回線のご用意（ご利用開始約1.5ヶ月前）
Direct Connect をご利用いただくためには、お客様のデータセンターやオフィスと、Direct Connect ロケーションとの間で回線接続をしていただく必要があります。

回線の詳細については、4.2「cloudpack　専用接続プラン」における選択肢の「ご利用回線」をご確認ください。

回線のご用意には、概ね1.5ヶ月程度の期間が必要となります。

回線の開通には、事前に回線事業者による Direct Connect ロケーションにおける現地調査が必要となります。お客様と回線事業者との間で現地調査日程をご調整の上、cloudpack 担当スタッフまで入館のご依頼をお願いいたします。

機材のご用意（ご利用開始約 1.5ヶ月前）
ご選択いただいたプランの構成に従い、ルーターなどの機材をご用意いただく必要があります。

必要な機材の詳細については「4.3 必要となる機材の調達と設置」の「必要となる機材」をご確認ください。

機材のご用意には、概ね1.5ヶ月程度の期間が必要となります。

Step3. ご契約

お申し込み後、所定の手続きを経て、正式にご契約いただきます。ご契約時点で、以下の日程が確定している必要があります。

- ご利用予定の回線の開通予定日
- ご利用予定の機材の納品日

Step4. 構築フェーズ（約3〜4週間）

ご契約後、お客様側の担当者様と cloudpack スタッフとの間での進捗管理ツールとして、「構築プロジェクト用 Backlog」のご提供を開始いたします。構築フェーズでは、この「構築プロジェクト用 Backlog」で情報共有を行いながら、以下の作業を進めていきます。

作業	担当者	作業の詳細
1. ネットワーク設計	お客様側ご担当者様 および cloudpack スタッフ	お客様のネットワーク構成に従い、Direct Connect 利用におけるネットワーク設計を決定いたします。
2. 配線作業	cloudpack スタッフ	お客様回線の開通日程に合わせて、Direct Connect ロケーション内での配線について、申請および作業を行います。
3. Direct Connect 構築作業	お客様側ご担当者様 および cloudpack スタッフ	お客様の AWS 環境と、cloudpack の Direct Connect 環境の双方で構築作業を行います。構築作業の詳細は、第 5 章「cloudpack 専用接続プラン」の導入（構築フェーズ）をご参照ください。

作業	担当者	作業の詳細
4. Direct Connect ロケーション作業	お客様側ご担当者様 および cloudpack スタッフ	Direct Connect ロケーションに入館し、お客様のルーターの設置作業をしていただきます。入館に際しては、cloudpack スタッフが同行いたします。ルーターの設置作業完了後、「cloudpack 専用接続プラン」の課金が開始いたします。
5. お客様環境側のルーティング設定変更	お客様側ご担当者様	お客様環境側のルーティング設定を変更することで、お客様環境と AWS 環境の間で通信できる状態にします。
6. 疎通確認	お客様側ご担当者様	お客様環境と AWS 環境内に構築いただいた VPC 間で通信できることを確認します。正常に通信できることが確認できれば、Direct Connect の導入は完了となります。

構築フェーズでは、概ね 3〜4 週間程度のお時間をいただきます。

Step5. 運用フェーズ

疎通確認後、実際にDirect Connect をご利用いただくことができます。

疎通確認後、お客様側の担当者様とcloudpack サポートデスクとの間での依頼管理ツールとして、「運用プロジェクト用 Backlog」のご提供を開始いたします。

運用フェーズでは、「運用プロジェクト用Backlog」から、各種ご依頼やお問い合わせを行うことができます。

4.5 「cloudpack 専用接続プラン」における責任共有モデル

「cloudpack 専用接続プラン」のご利用においては、ご契約のプランの接続構成に応じて、お客様とcloudpack で責任を共有いたします。

2つの責任共有モデル

お客様持ち込み回線をご利用の場合は、Direct Connect の利用に必要な下記の構築および運用をcloudpack が行います。

- cloudpack ラックからお客様 AWS 環境への Direct Connect の接続

お客様には、下記の構築および運用をお願いいたします。

- 専用線
- 回線両端のお客様ルーター
- AWS 環境（VGW / VPC）

cloudpack はお客様の構築および運用に必要なご支援をいたします。

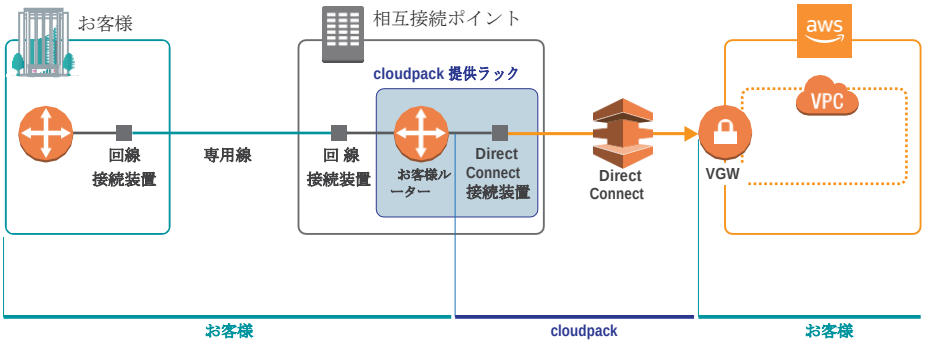


図 4.7「cloudpack 専用接続プラン」責任共有モデル（お客様持ち込み回線）

構築における分担

「cloudpack 専用接続プラン」の構築においては、「cloudpack 専用接続プラン責任共有モデル」に基づき、お客様とcloudpack で以下の通り構築を分担いたします。

Direct Connect 構築の分担（概要）

構築作業	お客様持ち込み回線
ルーターの構築（お客様側）	お客様
ご利用回線の構築	お客様（Direct Connect ロケーション設備はcloudpack が立ち合いいたします）
ルーターの構築（Direct Connect ロケーション側）	お客様（cloudpack が設定サンプルをご用意いたします）
Direct Connect の構築	cloudpack
VGW の構築	お客様
VPC の構築	お客様
DXGW,TGWの構築	お客様

運用における分担

「cloudpack 専用接続プラン」構築後のご利用においては、「cloudpack 専用接続プラン責任共有モデル」に基づき、お客様と cloudpack で以下の通り、運用を分担いたします。

Direct Connect 運用の分担（概要）

構築作業	お客様持ち込み回線
ルーターの監視 / 設定変更（お客様側）	お客様
ご利用回線の監視 / 設定変更	お客様
ルーターの監視 / 設定変更（Direct Connect ロケーション側）	お客様
Direct Connectの監 視 / 設定変更	cloudpack
VGW の監視 / 設定変更	お客様
VPC の監視 / 設定変更	お客様

第5章「cloudpack 専用接続プラン」構築フェーズ

5.1 Direct Connect 導入への基礎知識

Direct Connect を利用する場合、以下の構成要素について理解しておくことをお勧めします。

VPC

Virtual Private Cloud（VPC）は、AWS の他の仮想ネットワークから論理的に切り離された、お客様専用の仮想ネットワーク環境です。VPC は、EC2 やRDS などのコンピューティングリソースを起動するための環境として利用することができます。

VPC では、利用するIP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイ、セキュリティの設定などが可能となっています。

ここでは、Direct Connect を利用する上で設定が必要な以下のリソースについて解説します。

- ネットワークゲートウェイ
- サブネット
- ルートテーブル
- セキュリティグループ

VPC で設定するIP アドレスについては、「5.2 アドレス設計ガイドライン」をご参照ください。

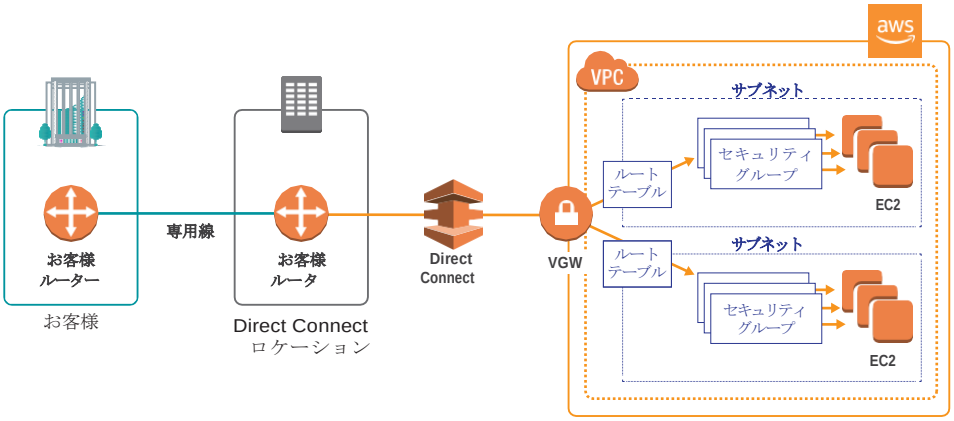


図 5.1 Direct Connect の構成要素

ネットワークゲートウェイ

VPC から外部のネットワークに接続するためには、ネットワークゲートウェイの作成が必要となります。VPC では、以下の2 種類を構築することができます。

- IGW（Internet GateWay）：インターネットへの接続
- VGW（Virtual private GateWay）：ユーザ独自のネットワークへの接続

Direct Connect の利用には、VGW の作成が必要となります。

サブネット

AWS では、1つのリージョンが複数の物理的なデータセンター（「アベイラビリティゾーン」）で構成されており、VPC は複数のアベイラビリティゾーンにまたがって作成することができます。サブネットは、インスタンスを起動するための空間で、アベイラビリティゾーン単位で作成する必要があります。

ルートテーブル

ルートテーブルは、ネットワークトラフィックの経路を決定するルールである「ルート」が登録された一覧です。インスタンスがサブネットの外部と通信するためには、各サブネットとルートテーブルを関連付ける必要があります。ルートテーブルの設定がされていない場合は、デフォルトで設定されている「メインルートテーブル」が利用されます。

セキュリティグループ

セキュリティグループは、ステートフルな仮想ファイアウォールとして機能し、インスタンスへのインバウンドトラフィックとアウトバウンドトラフィックをコントロールします。セキュリティグループは、インスタンス単位で適用されます。

BGP

BGP（Border Gateway Protocol）とは、動的ルーティングプロトコルの一つで、インターネット上の組織（AS）間の相互接続（インターコネクション）において、お互いの経路情報を交換するために使われます。

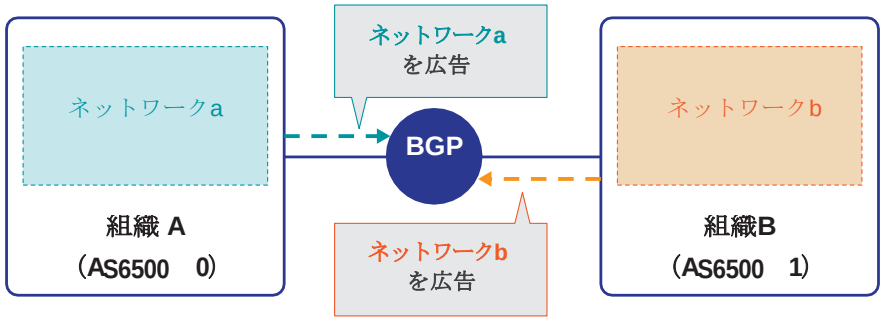


図 5.2 BGP の仕組み

Direct Connect では、主に BGP を利用してお客様環境とVPC 間をルーティングします。

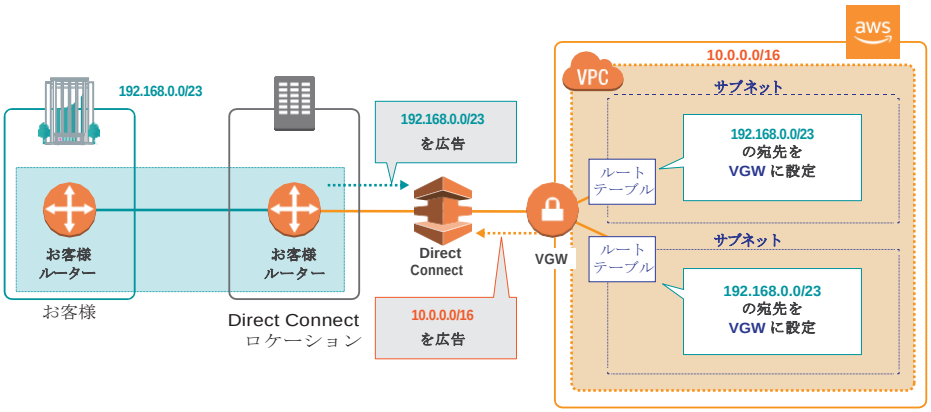


図 5.3 BGP によるルーティング

Direct Connect コネクションと仮想インターフェイス

Direct Connect における物理インターフェイスを「Direct Connect コネクション」と言います。

1つの Direct Connect コネクションは、複数の「仮想インターフェイス」を持ち、各仮想インターフェイスは VLAN ID という識別子を持ちます。

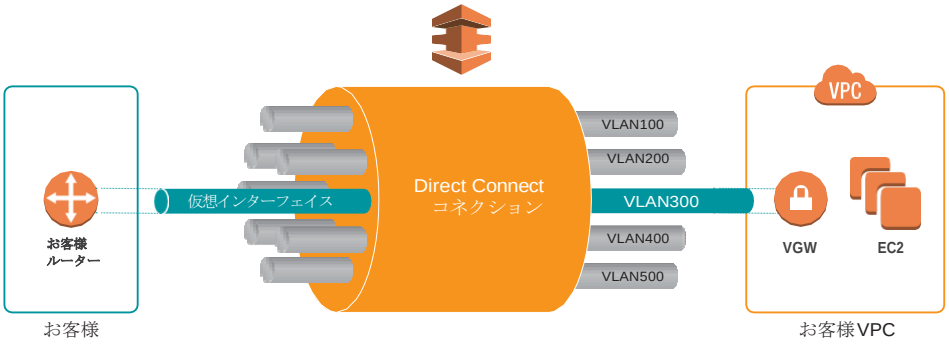


図 5.4 Direct Connect コネクションと仮想インターフェイス

注意事項

1. お客様環境側ルーターから広告できるネットワーク数は 100 個が上限となります。

2. Direct Connect に接続した VPC（VPC1）と「VPC Peering」で接続されている VPC（VPC2）がある場合、お客様環境と VPC2は通信できません。

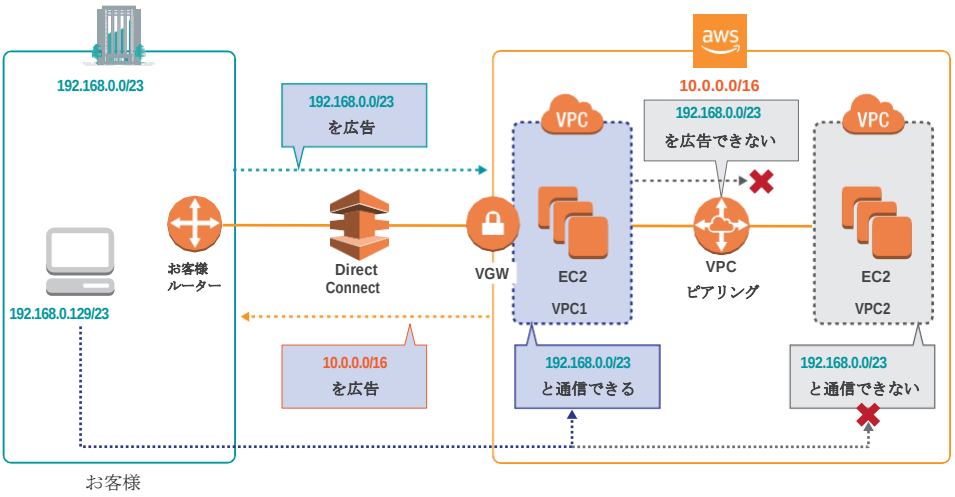


図 5.5 Direct Connect とVPC Peering

5.2 アドレス設計ガイドライン

VPC 利用におけるIP アドレスの制約

1. サブネットの CIDR ブロックサイズ
サブネットで指定できる CIDR ブロックサイズ（ネットマスク）は /16 から /28 までの間となります。

VPC に複数のサブネットを作成する場合は、サブネットの CIDR ブロックサイズの合計よりも VPC の CIDR ブロックサイズを大きく設定することをお勧めします。特に、マルチ AZ 構成では一つの機能を複数のサブネットで実装するため、VPC の CIDR ブロックサイズを大きめに確保することをご検討ください。

2. AWS の予約アドレス
各サブネット CIDR ブロックのうち下記の IP アドレスは、AWS の予約アドレスとされているため、インスタンスに割り当てることはできません。

- 最初の4 つの IP アドレス（ネットワークアドレス及びその直後の3つの IP アドレス）
- 最後の IPアドレス（ネットワークブロードキャストアドレス）

3. ELB 利用時の制約
ELB（Elastic Load Balancing）をご利用の場合は、さらに下記の制約があります。

- ロードバランサーの各サブネットの CIDR ブロックサイズは /27以上必要となります
- 少なくとも 8 個の空き IP アドレスを用意する必要があります。

IP アドレス設計における留意点

1. 割り当て可能な IP アドレス

プライベート IP アドレス
RFC1918（Address Allocation for Private Internets）に定められているプライベート IP アドレス空間のうち、以下の IP アドレスについては、VPC に割り当てが可能です。

- 10/8（10.0.0.0 - 10.255.255.255）
- 172.16/12（172.16.0.0 - 172.31.255.255）
- 192.168/16（192.168.0.0 - 192.168.255.255）

以下のプライベートIP アドレスについてもVPC への割り当ては可能ですが、Windows インスタンスが正しく起動できません。

- 224/4（224.0.0.0 - 239.255.255.255）
- 240/4（240.0.0.0 - 255.255.255.255）

2. 社内ネットワークとの整合性
VPC に割り当てるIP アドレスは、お客様環境ですでにご利用の IP アドレスと重複することはできません。未使用の IP アドレス空間が必要となります。

また、VPC に接続する予定のお客様環境から、VPC に割り当てるIP アドレスに対してネットワーク的に到達できる必要があります。必要なルーティングの設定が可能かどうか予めご確認ください。

3. 適切な CIDR ブロックサイズ
Direct Connect でご利用中のVPC の CIDR ブロックサイズを変更するためには、VPC の再作成および Direct Connect の再設定が必要となります。VPC に割り当てるCIDR ブロックについては、かなり余裕を持って設計されることをお勧めします。

目安として、最低でも /22、複数のシステム環境を配置する場合は /16 をご検討ください。

5.3 事前にご確認いただきたいこと

構築フェーズで作業を行うために、以下の情報が必要となります。事前にご確認ください。

項目	内容
お客様側ネットワークアドレス	VPC に接続するお客様側ネットワークアドレス
VPC 側ネットワークアドレス	VPC 側で利用するプライベートネットワークアドレス
AWS アカウントID	AWS アカウントに割り当てられる12桁の ID
Direct Connect 接続予定 VPC 数	Direct Connect に接続する予定があるVPC の数

5.4 構築作業の詳細

1. ネットワーク設計

上記のご確認項目に従い、お客様ご担当者様と cloudpack スタッフで、Direct Connect 利用に必要なネットワーク構成を決定いたします。

担当者 : お客様側ご担当者様および cloudpack スタッフ

2. 配線作業

お客様回線の開通日程に合わせて、Direct Connect ロケーション内での配線について、申請および作業を行います。

担当者 : cloudpack スタッフ

作業	作業者
1. 事前現地調査（設備確認）	お客様がご利用する回線事業者
2. 構内配線依頼	cloudpack スタッフ
3. 構内配線	エクイニクス
4. ONU の設置（上流との接続）	お客様がご利用する回線事業者

3. Direct Connect 構築作業

お客様の AWS 環境と、cloudpack の Direct Connect 環境の双方で構築作業を行います。

担当者：お客様側ご担当者様および cloudpack スタッフ

作業	担当者
1. VGW 作成	お客様側ご担当者様
2. 仮想インターフェイス作成	cloudpack スタッフ
3. 仮想インターフェイス承認	お客様側ご担当者様
4. 仮想インターフェイスの VGW への割り当て	お客様側ご担当者様
5. サンプル設定ファイル作成 / VGW 確認	cloudpack スタッフ
6. サンプル設定ファイル渡し	cloudpack スタッフ
7. 機器設定	お客様側ご担当者様

4. Direct Connect ロケーション作業

Direct Connect ロケーションに入館し、お客様のルーターの設置作業をしていただきます。
入館に際しては、cloudpack スタッフが同行いたします。

担当者：お客様側ご担当者様および cloudpack スタッフ

作業	担当者
入館申請	cloudpack スタッフ
入館作業（ルーター設置、接続）	お客様側ご担当者様

本作業完了とともに「cloudpack 専用接続プラン」の課金が開始いたします。

5. お客様環境側の設定変更

担当者：お客様側ご担当者様

作業	内容
1. VPC の設定	お客様環境との通信に必要に応じてセキュリティグループの設定をしていただきます。
2. ルーティング設定変更	お客様環境側のルーティング設定を変更することで、お客様環境と AWS 環境の 間で通信できる状態にします。
3. 疎通確認（リリース）	お客様環境と AWS 環境内に構築いただいた VPC 間で通信できることを確認します 。正常に通信できることが確認できれば、Direct Connect の導入は完了となります。

第6章「cloudpack 専用接続プラン」運用フェーズ

6.1 cloudpack サポートデスク

cloudpack のお客様窓口である「cloudpack サポートデスク」では、ご提供するサポートサービスに対する信頼性および透明性を高めるために、サービスレベル合意（SLA）およびサービスレベル目標（SLO）を定義し、公開しています。

サービスレベルの定義および cloudpack サポートデスクの詳細については、「cloudpack サポートデスク ホワイトペーパー」（https://cloudpack.jp/whitepaper/supportdesk.html ）をご参照ください。

6.2 作業のご依頼

cloudpack サービスデスクでは、お客様ご利用の「cloudpack 専用接続プラン」に関する構成変更のご依頼を受け付けています。

ご依頼は、プロジェクト管理ツール「Backlog」上で、以下の項目を記載したチケットの起票をお願いいたします。チケットに記載されたご依頼内容を確認後、原則として 5営業日以内に対応いたします。(cloudpack スタッフが特段の事情があると判断した場合を除きます)

cloudpack では、システムの構築フェーズ、運用フェーズそれぞれにおいて、プロジェクト管理ツール「Backlog」によりお客様とスタッフの間のコミュニケーションを行います。

接続先VPC の追加、変更

cloudpack サービスデスクでは、お客様ご利用の「cloudpack 専用接続プラン」に接続するVPC の追加および変更に関するご依頼を受け付けています。

標準日数（サービスレベル目標）: 5 営業日

Backlog によるご依頼方法 :

種別	接続先 VPC の追加 / 変更
作業に必要な詳細情報	作業の種類（追加 / 変更）対象となる VPC のネットワークアドレス

ルーティングの追加、変更

cloudpack サービスデスクでは、お客様ご利用の「cloudpack 専用接続プラン」におけるルーティングの追加および変更に関するご依頼を受け付けています。

標準日数（サービスレベル目標）: 5 営業日

Backlog によるご依頼方法 :

種別	ルーティングの追加 / 変更
作業に必要な詳細情報	作業の種類（追加 / 変更）ルーティングプロトコル（スタティック / BGP）対象となるネットワークアドレス

計画作業のための入館依頼

お客さまが Direct Connect ロケーション内の cloudpack ラックに設置するための設定や障害発生時など、ラック内での作業が必要となった場合には、お客様とご一緒に cloudpack が現地に行きお客様の作業をサポートいたします。

標準日数（サービスレベル目標）:5営業日

Backlog によるご依頼方法 :

種別	入館依頼
作業に必要な詳細情報	入館目的 入館者（所属、氏名）入館者の連絡先

6.3 監視について

cloudpack 専用接続プランでは、仮想インターフェイスを監視しています。

6.4 Direct Connect のメンテナンスについて

AWS によるシステムメンテナンスのため、不定期に Direct Connect コネクション単位でサービス停止が発生いたします。

告知 : 停止の約 1 週間前（緊急メンテナンスの場合を除く）

停止時間 : 数分から1時間程度

cloudpack サポートデスクでは、Direct Connect のメンテナンス告知があった場合は、すみやかにお客様にご連絡いたします。

なお、停止日程や停止時間については AWS が決定しており、契約上個別に調整する余地がないことにご留意ください。

付録1 ご参考: 回線サービスのご案内

「cloudpack 専用接続プラン」では、お客さまが普段からご利用いただいている、以下の専用線サービスをお持ち込みいただくことが可能です。

IP VPN（レイヤー 3VPN）

IP ネットワーク上に構築される専用線網です。インターネットサービスプロバイダ（ISP） が外部公開していない通信網を他のユーザと共用するため、一般的に帯域と経路はベストエフォートになります。（帯域保証するプランが提供されている場合もあります）

レイヤー2 の運用保守を提供事業者が行うため、自由度は低い一方でユーザ側の導入や運用保守が容易になります。

広域イーサネット（レイヤー2VPN）

LAN（ローカルエリアネットワーク）と同じイーサネット上に構築される専用線網です。一般的に通信速度が速く、遅延も小さいのが特徴です。

レイヤー2 の運用保守をユーザが自ら行うため、拠点の追加・プロトコルの変更などの構成変更を柔軟に行うことができます。

回線提供事業者

上記の回線サービスを提供している主要な通信事業者として、以下の各社があります。

- 東日本電信電話（NTT 東日本）
- 西日本電信電話（NTT 西日本）
- KDDI
- ソフトバンク
- NTT コミュニケーションズ
- TOKAI コミュニケーションズ

付録2 ご参考: Direct Connect に対応するルーター製品

「cloudpack 専用接続プラン」では、以下の仕様を満たしたルーターをご利用いただくことができます。

• BGP（Border Gateway Protocol）に対応し、MD5 認証が利用できること
• 100V で動作すること

お客様環境から、Direct Connect 経由で複数のVPC に接続する場合は、以下の機能が必要になります。

• 802.1q VLAN

回線によっては、PPPoE（Point-to-Point Protocol over Ethernet）に対応している必要があります。詳細については、ご利用の回線事業者にご確認ください。

cloudpack では、ご利用回線の両端（お客様環境と Direct Connect ロケーション）で、同一メーカーのルーター製品のご利用を推奨しています。

ルーター機器を購入する前に、機器のレンタルができる場合もございますので、相性確認を行った上でご購入されることをお奨めいたします。

cloudpackでの実績がある機器

cloudpack では、お客様の機器導入の参考情報として、動作実績のある機器を公開しています。

お持ち込み可能なルーターについて
https://cloudpack.jp/service/plan/direct-connect.html#router

機器導入の事前確認などにご活用ください。

付録3: 参考となる情報やドキュメント

AWS が提供するベストプラクティスに関するドキュメント（抜粋）

cloudpack は、AWS が提供するベストプラクティスに従ったシステムを構築し、cloudpack が持つベストプラクティスに従ってお客様の環境を運用しています。

AWS セキュリティのベストプラクティス
https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Best_Practices.pdf

Security at Scale: Governance in AWS

https://d0.awsstatic.com/whitepapers/aws-security-at-scale-governance-in-aws.pdf

Securing Data at Rest with Encryption
https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf

Security Whitepaper
https://aws.amazon.com/jp/blogs/security/tag/whitepaper/

Security at Scale: Logging in AWS
https://aws.amazon.com/jp/blogs/security/tag/logging/

Risk and Compliance WhitePaper
https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

Direct Connect 関連ドキュメント

Direct Connect を理解する上で、下記の公式ドキュメントが参考になります。

AWS Direct Connect
https://aws.amazon.com/jp/directconnect/

料金
https://aws.amazon.com/jp/directconnect/pricing/

Direct Connect ユーザガイド
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/dc-ug.pdf

VPC 関連ドキュメント

VPC を理解する上で、下記の公式ドキュメントが参考になります。

Amazon VPC
https://aws.amazon.com/jp/vpc/

料金
https://aws.amazon.com/jp/vpc/pricing/

入門ガイド
http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/GettingStartedGuide/ExerciseOverview.html

VPC ネットワーク管理者ガイド
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/VPC_VPN.html

AWS クラウドサービス活用資料集

AWSJ(アマゾン ウェブ サービス ジャパン) 社が提供している資料リンク集です。主に、ウェブセミナーでの発表資料が置かれています。

https://aws.amazon.com/jp/aws-jp-introduction/

Direct Connect 、VPCについては、「AWS Black Belt Tech シリーズ」で最新資料として公開されています。

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/

Amazon VPC VPN 接続設定 参考資料
https://aws.amazon.com/jp/vpn/

付録4: 用語集

本ホワイトペーパーで定める用語

お客様
cloudpack をご利用いただいている企業様又は企業様の部門およびご担当者様。
（JIS Q 20000-1 に定める「顧客（customer）」とほぼ同じ意味で使用します）

エクイニクス・ジャパン
日本国内において東京大阪にデータセンターを展開している企業

BGP（Border Gateway Protocol）
インターネット上の組織（AS）間の相互接続（インターコネクション）において、お互いの経路情報を交換するために使われる動的ルーティングプロトコル。

Direct Connect コネクション
Direct Connect における物理インターフェイス。

VGW（Virtual private GateWay）
ユーザ独自のネットワークへの接続するためのネットワークゲートウェイ。

VPC（Virtual Private Cloud ）
AWS の他の仮想ネットワークから論理的に切り離された、お客様専用の仮想ネットワーク環境。VPC は、EC2 や RDS などのコンピューティングリソースを起動するための環境として利用することができます。

サブネット
インスタンスを起動するための空間。

セキュリティグループ
インスタンスへのインバウンドトラフィックとアウトバウンドトラフィックをコントロールするステートフルな仮想ファイアウォール。

ルーター
コンピュータネットワークにおいて、2 つ以上の異なるネットワークに接続され、各ネットワーク間のデータ通信を中継する機器。本ホワイトペーパーでは、L3 スイッチを含みます。

ルート
ネットワークトラフィックの経路を決定するルール。

ルートテーブル
「ルート」が登録された一覧（テーブル）。

仮想インターフェイス
Direct Connect における論理インターフェイス。Direct Connect コネクションは、複数の仮想インターフェイスを持ち、各仮想インターフェイスは VLAN ID という識別子を持ちます。

付録5: エクイニクス提供サービス

エクイニクスが提供するデータセンター内及びデータセンター間で利用するサービス名を記載します。

クロスコネクト

クロスコネクトとはエクイニクスが提供するデータセンター内の構内配線サービスです。 クロスコネクトを利用することで MDF 室からラック間を接続することで回線サービス利用を可能にします。

iret

cloudpack™

https://cloudpack.jp

お問い合わせ sales@cloudpack.jp
0120-677-989

運営 アイレット株式会社

東京都港区虎ノ門 1-23-1
虎ノ門ヒルズ森タワー 7F
http://www.iret.co.jp