AWS Builders Online Series

# 「ネットワークエンジニア向け」まずは押さえておきたいオンプレミス拠点からAWSクラウドへの接続方式パターン

藤井 拓

技術統括本部 ソリューションアーキテクト ネットワークスペシャリスト
アマゾン ウェブ サービス ジャパン合同会社

# 自己紹介

名前： 藤井 拓（ふじい たく）

所属： アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 ネットワークソリューション部
ソリューションアーキテクト ネットワークスペシャリスト

経歴： 前職は外資系通信機器メーカにてネットワーク機器に関わる
プリセールスSEを長年担当

好きなAWSサービス：
AWS Direct Connect, AWS Transit Gateway, AWS Gateway Load Balancer, AWS Marketplace

# アジェンダ

本セッションの狙い

はじめに

オンプレミスとVPCの接続パターン

1. 拠点からインターネット経由でVPCに接続
2. 複数拠点から安全にVPCに接続
3. 拠点からシステム毎に異なるVPCに接続
4. 多数のVPCやオンプレミス拠点を相互接続しルーティングを一元管理したい

まとめ

# オンプレミス拠点とAWSクラウドへの接続パターン

1. 拠点からインターネット経由でVPCに接続
   →最も容易だが、通信要件に合わせて暗号化を利用
2. 複数拠点から安全にVPCに接続
   →専用線とVPNを併用してメリハリのある構成
3. 拠点からシステム毎に異なるVPCに接続
   →Direct Connect Gatewayでシステム毎のVPCへの接続
4. 多数のVPCやオンプレミス拠点を相互接続しルーティングを一元管理したい
   →Transit Gatewayで経路を集中管理、柔軟な経路設計

# 本セッションの狙い

- 本セッションは、AWS利用を検討されている方や、すでにAWSのご利用を開始している方で、オンプレミスからAWSクラウドへの接続を最適化したい要件をお持ちの方などを対象にしています。

- すでに専用線を利用してAWSクラウドへ接続している方で、利用拡張に備えて新サービスへの移行を検討されている方にも、参考となる情報をお伝えします。

# このセッションでお話しないこと

- 本セッションではオンプレミスとAWSクラウドを接続する上で、全体的なネットワーク構成を主題にしています。各サービスについての詳細説明は対象外となります。
- 本セッションで登場するサービスについて、より詳細内容を知りたい方は、AWS Black Beltオンラインセミナーにおけるネットワークサービスの解説をご確認ください。
- AWS Direct Connect サービスデリバリーパートナーの様の情報は下記のURLをご参照ください。

# 概要

# このセッションの概要

オンプレミス拠点とAWSクラウドを接続する事により、AWSクラウドをオンプレミスの一部として利用できるようになります。

しかし実際に接続を検討する際は、要件によって様々な検討事項があります。

例えば、VPN接続を使用したい、専用線接続が必須、冗長化はどうする、など検討事項は多岐に渡ります。

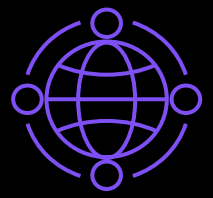
このセッションでは、オンプレミス拠点とAWSクラウド接続する方式についてユースケースを用いて説明します。

# 本日ご紹介するサービス

AWS Site-to-Site VPN

AWS Direct Connect

AWS Transit Gateway

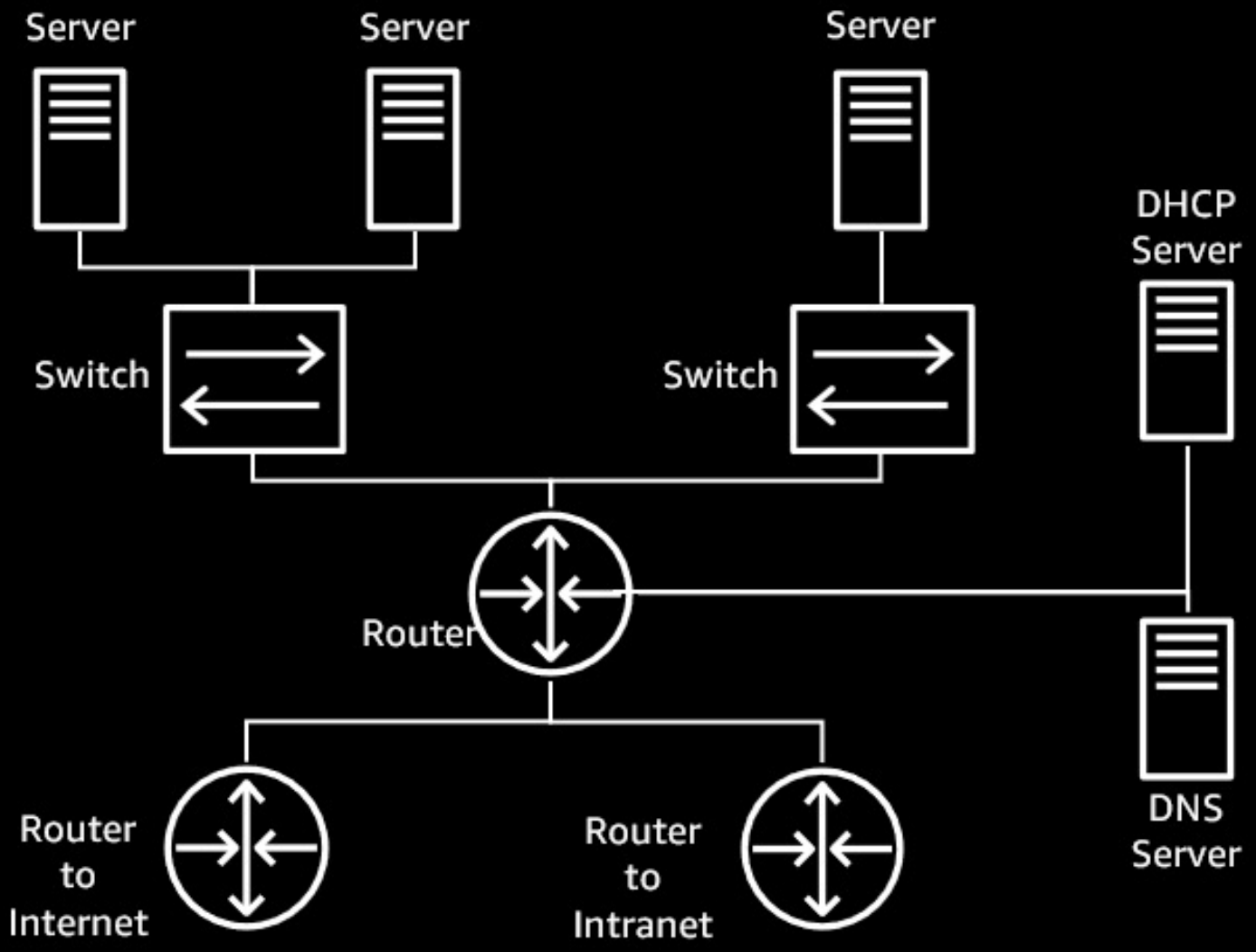


AWS Cloud WAN

**NEW!**

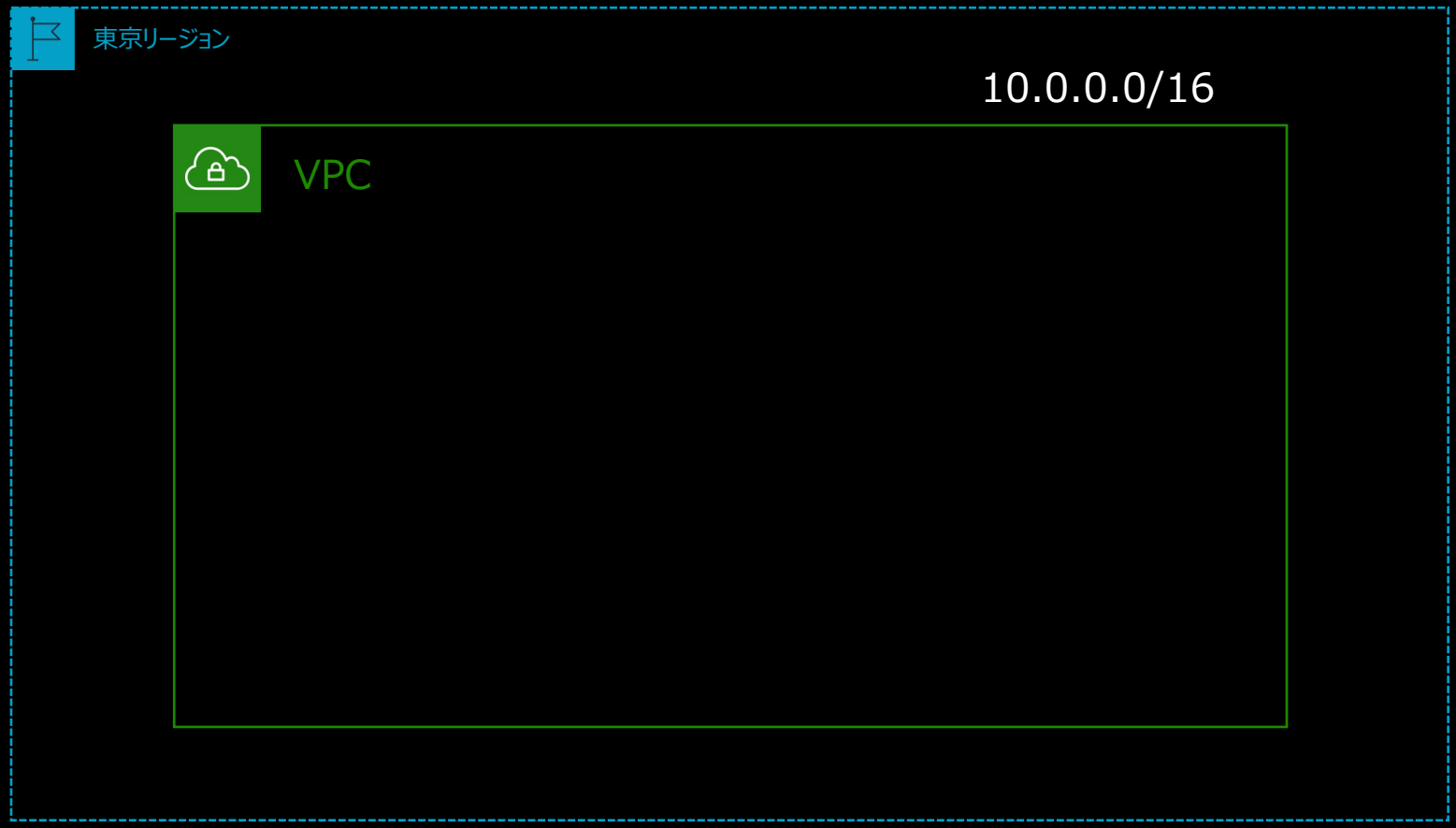
# Virtual Private Cloud (VPC)とは

# オンプレミスのネットワーク



# Virtual Private Cloud(VPC)とは

まずは全体のネットワーク空間をVPCとして定義

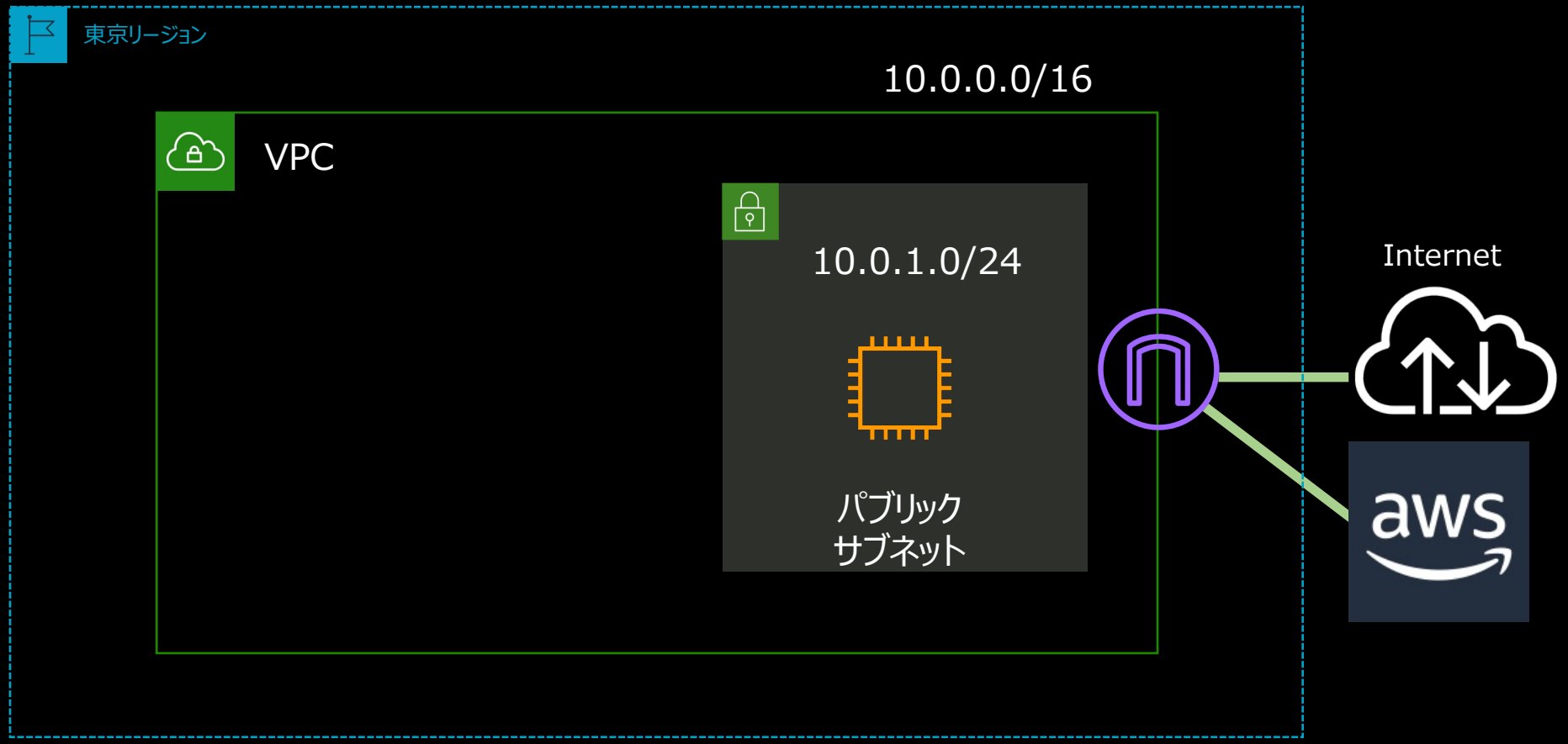


# Virtual Private Cloud(VPC)とは

## 利用するサブネットを定義

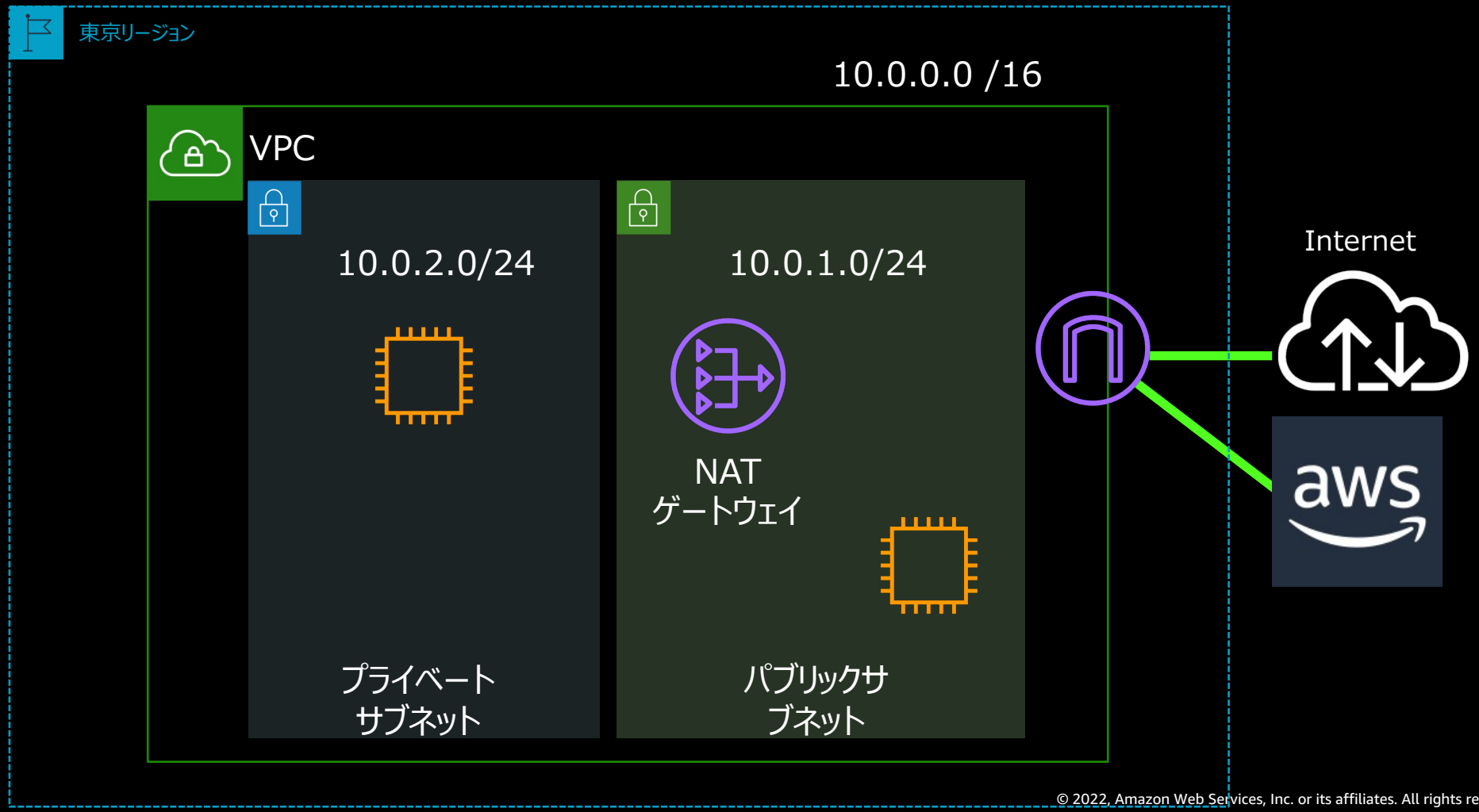
# Virtual Private Cloud(VPC)とは

## インターネットへの接続を設定



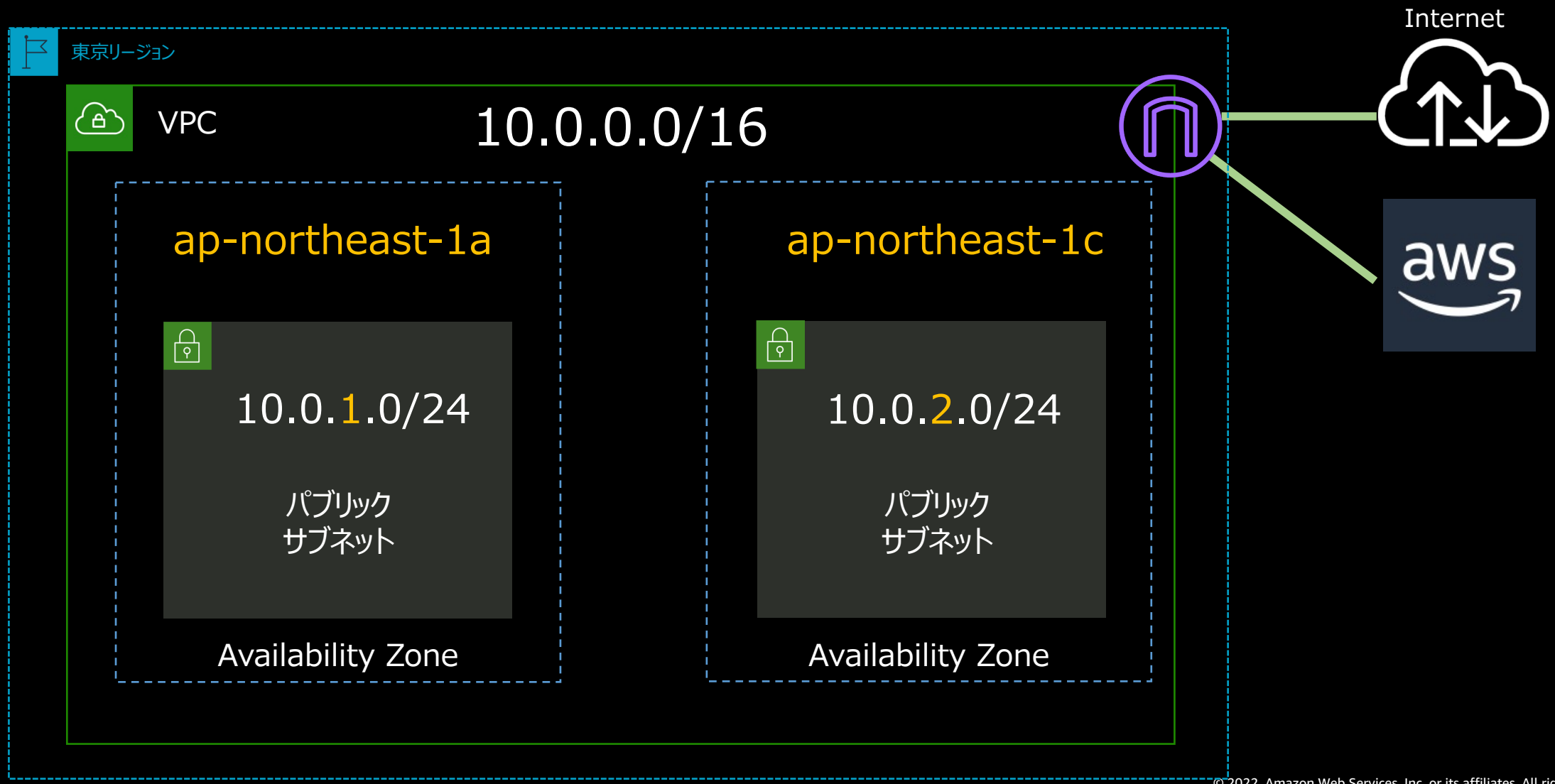
# Virtual Private Cloud(VPC)とは

## プライベートサブネットを追加



# Virtual Private Cloud(VPC)とは

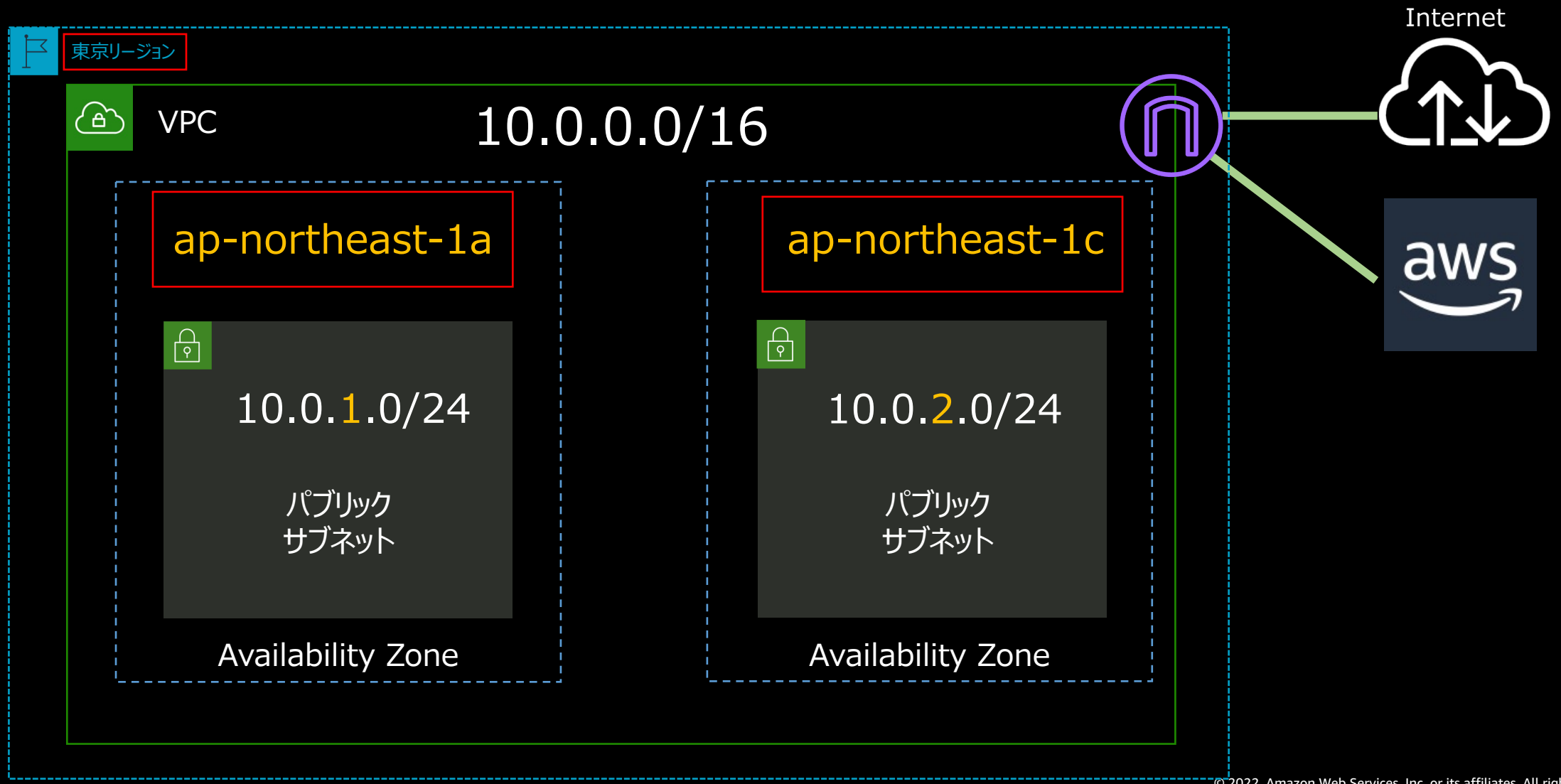
## AZを分けて可用性を担保する際はサブネットを分ける



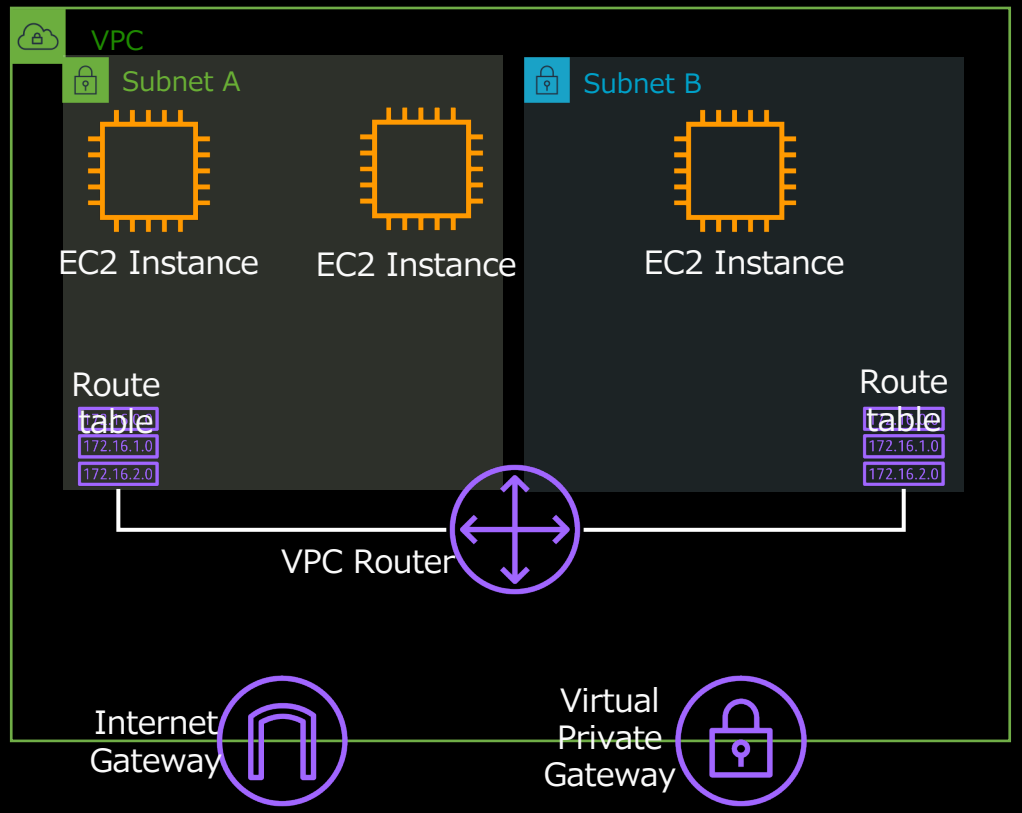

aws

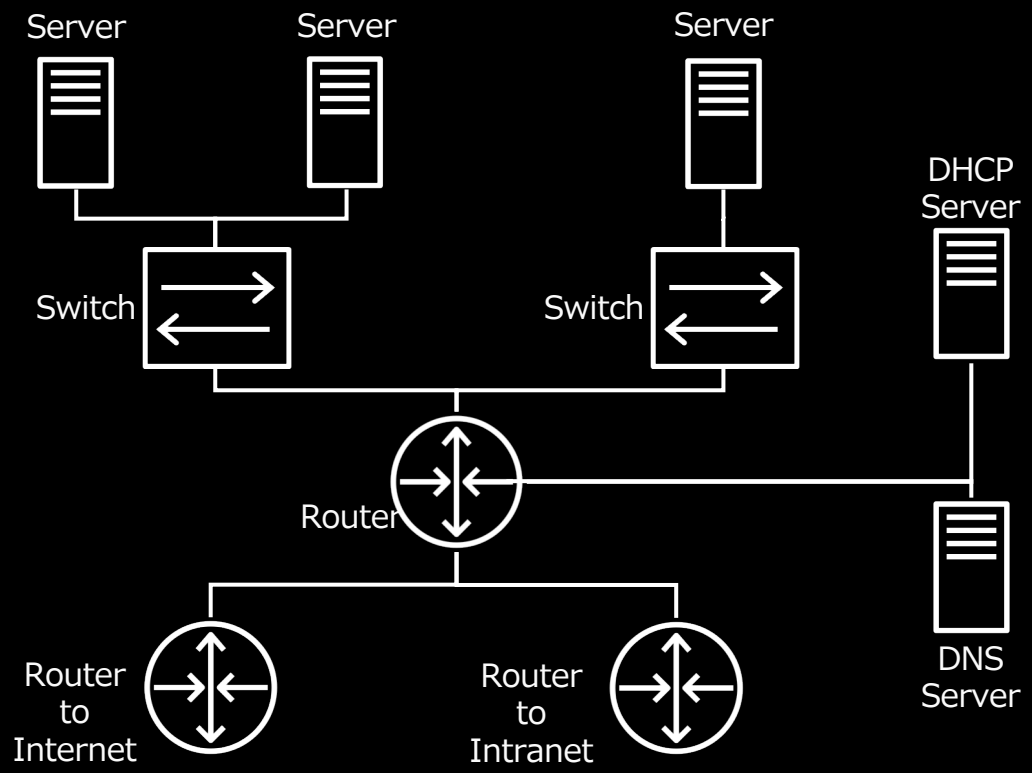
# Virtual Private Cloud(VPC)とは

## AZを分けて可用性を担保する際はサブネットを分ける



# Virtual Private Cloud(VPC)とは




環境を作る≒ VPC を作る ≒ ルーターと DNS を設定する

可用性を高める≒サブネットを複数使う ≒データセンター冗長

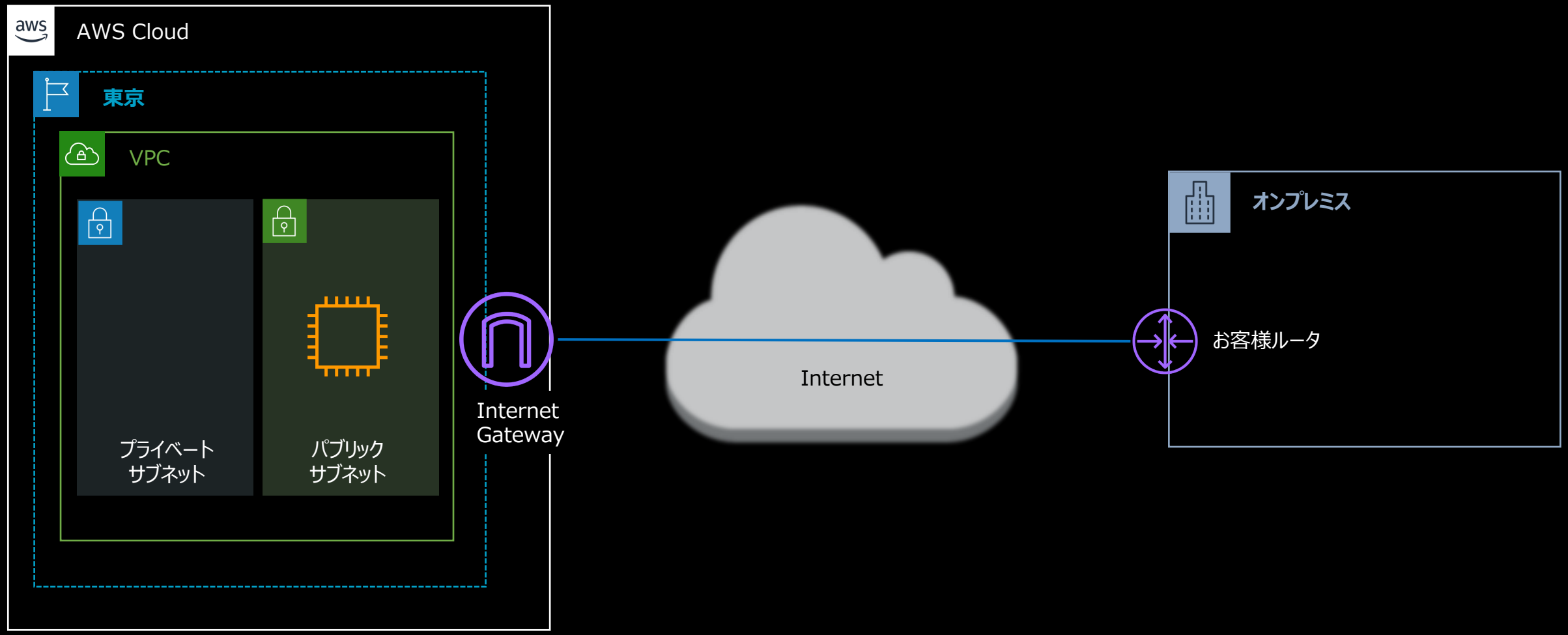
# 要件別オンプレミスとの接続方式

# オンプレミス拠点とAWSクラウドへの接続パターン

1. 拠点からインターネット経由でVPCに接続
   →最も容易だが、通信要件に合わせて暗号化を利用
2. 複数拠点から安全にVPCに接続
   →専用線とVPNを併用してメリハリのある構成
3. 拠点からシステム毎に異なるVPCに接続
   →Direct Connect Gatewayでシステム毎のVPCへの接続
4. 多数のVPCやオンプレミス拠点を相互接続しルーティングを一元管理したい
   →Transit Gatewayで経路を集中管理、柔軟な経路設計

# 拠点からインターネット経由でVPCに接続

# オンプレミス拠点よりInternet経由でVPCに接続




インターネットが接続できる環境であれば、どこからでもアクセス可能。アクセス制限や通信の暗号化は考慮する必要がある。

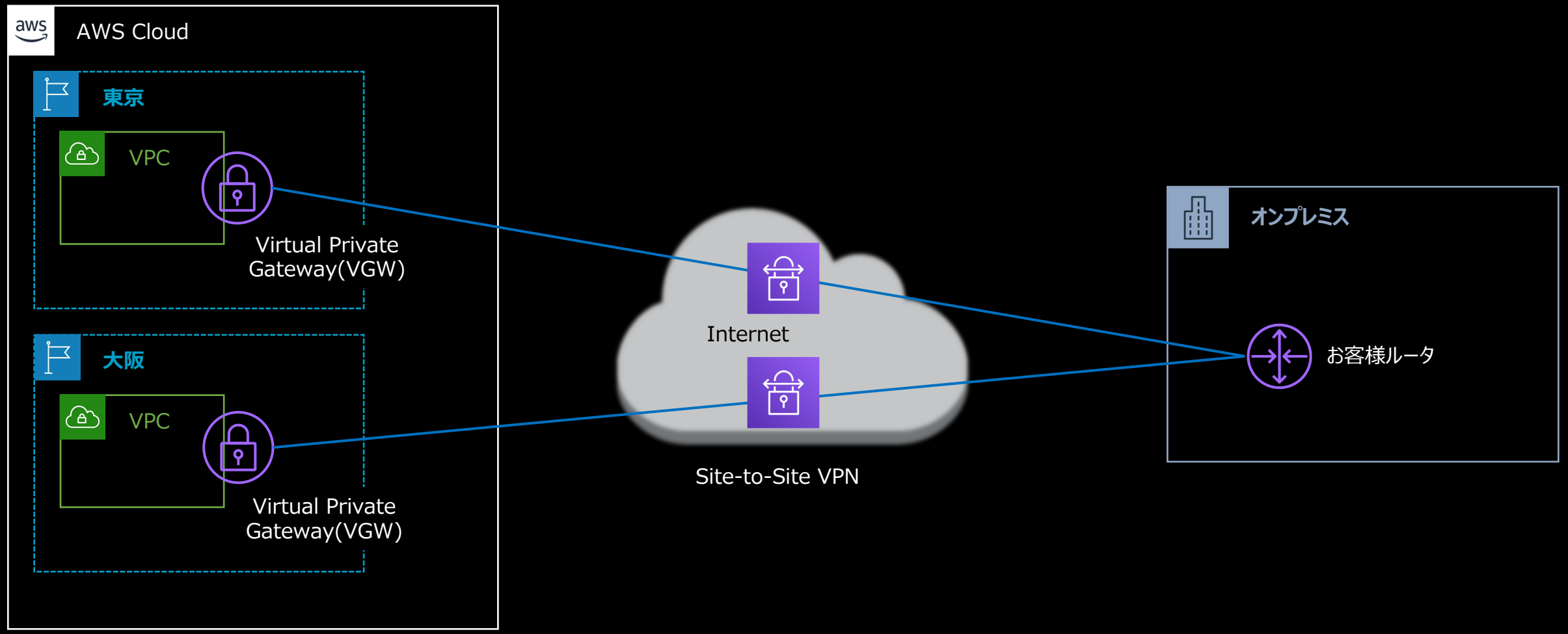
# 複数拠点から安全にVPCに接続

# Site-to-Site VPNとは

- お客様のデータセンターやオフィスのハードウェアルータからVPNを介してAWSへプライベートに接続するサービス

- 種類
  - Virtual Private Gatewayと接続
  - Transit Gatewayと接続
- ユースケース
  - 拠点とAWSを簡単に早く接続したい
  - 少量のトラフィック
  - 価格重視/スモールスタート
  - バックアップ回線

# Site-to-Site VPNとは



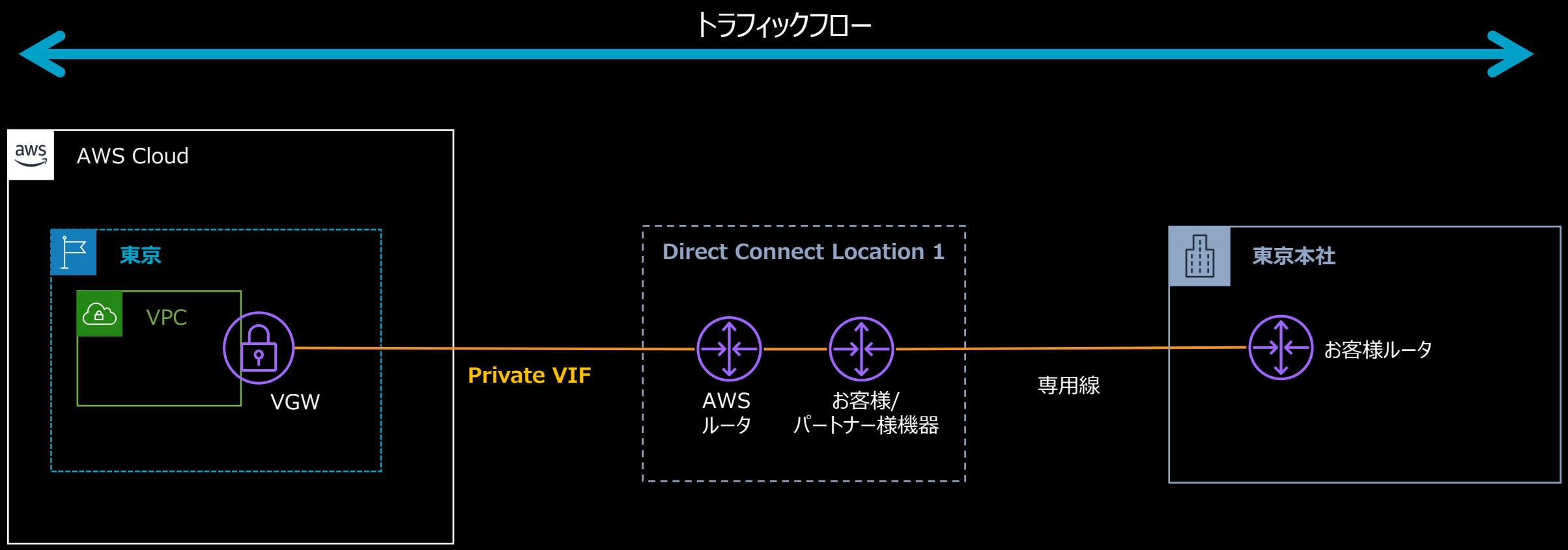

Site-to-Site VPNは、お客様の拠点とAWS CloudをVPNを使用して接続するサービスです。

# Direct Connectとは

- お客様のデータセンターやオフィスをハードウェアルータから専用線を介してAWSへプライベートに接続するサービス

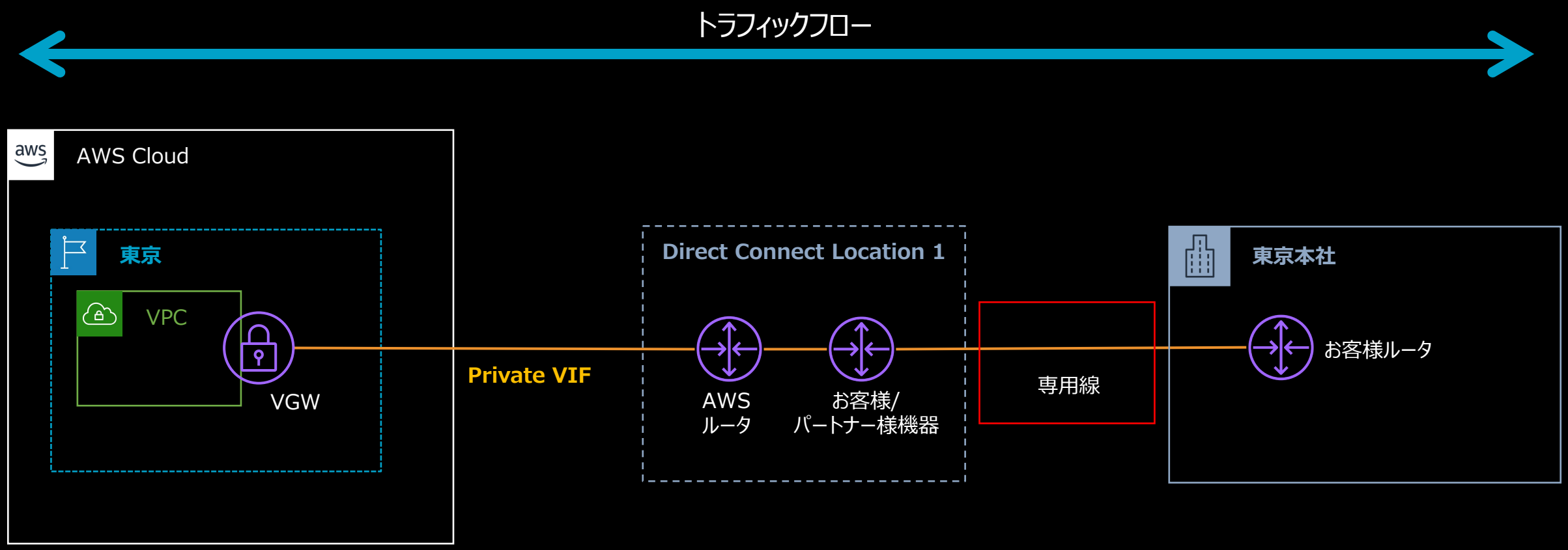
- **ユースケース**
  - 安定したパフォーマンスが必要
  - 専用線での接続が必要
  - 大量のトラフィック
  - 主回線
  - 一貫性のある管理を実現したい

# Direct Connectとは




Direct Connectは、お客様のオンプレミス拠点とAWS Cloud
をDirect Connectロケーション経由して接続するサービスです。

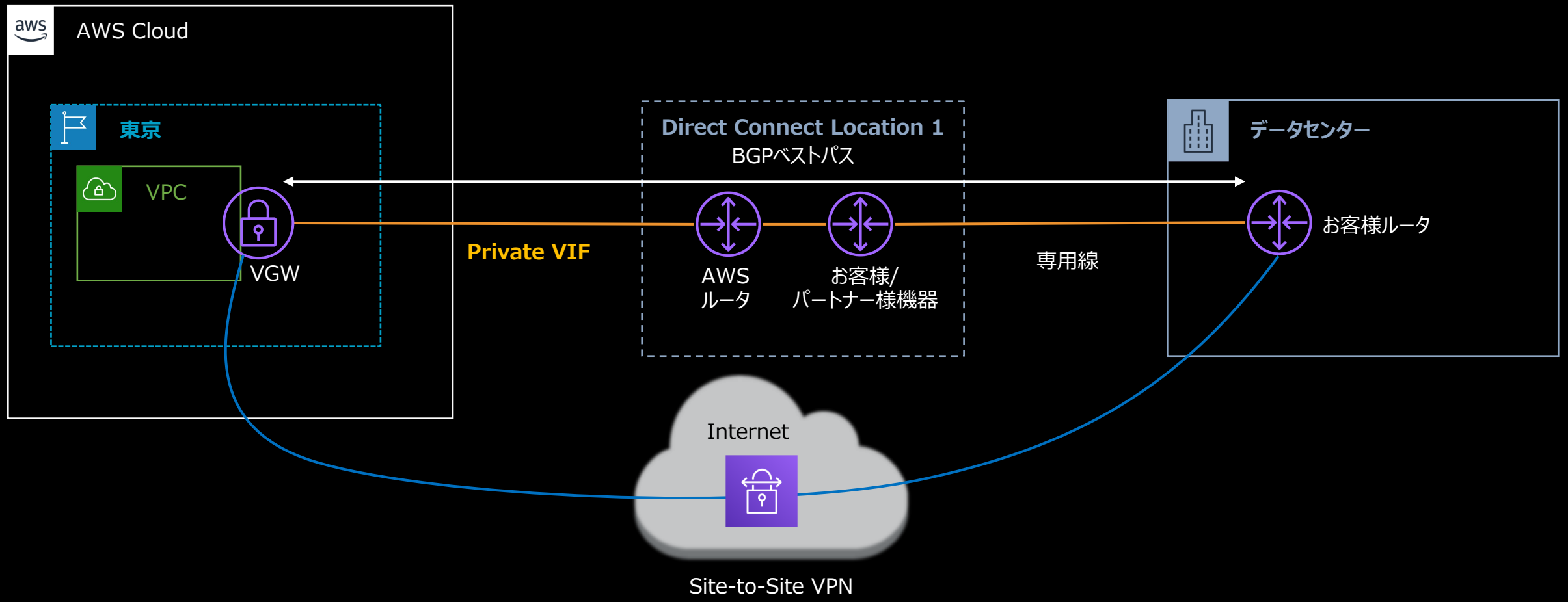
# Direct Connectとは




Direct Connectは、お客様のオンプレミス拠点とAWS Cloud
をDirect Connectロケーション経由して接続するサービスです。

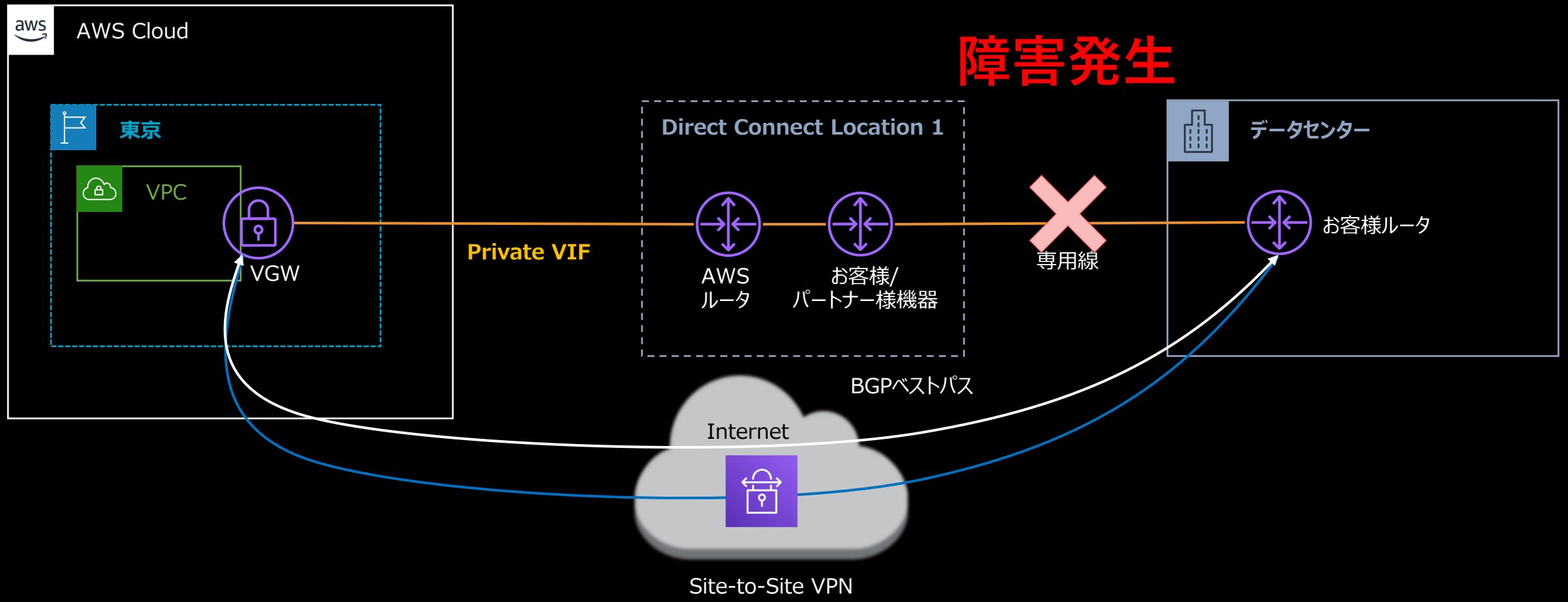
# Direct Connect + Site-to-Site VPN

## Direct Connectのバックアップ回線としてSite-to-Site VPNを使用



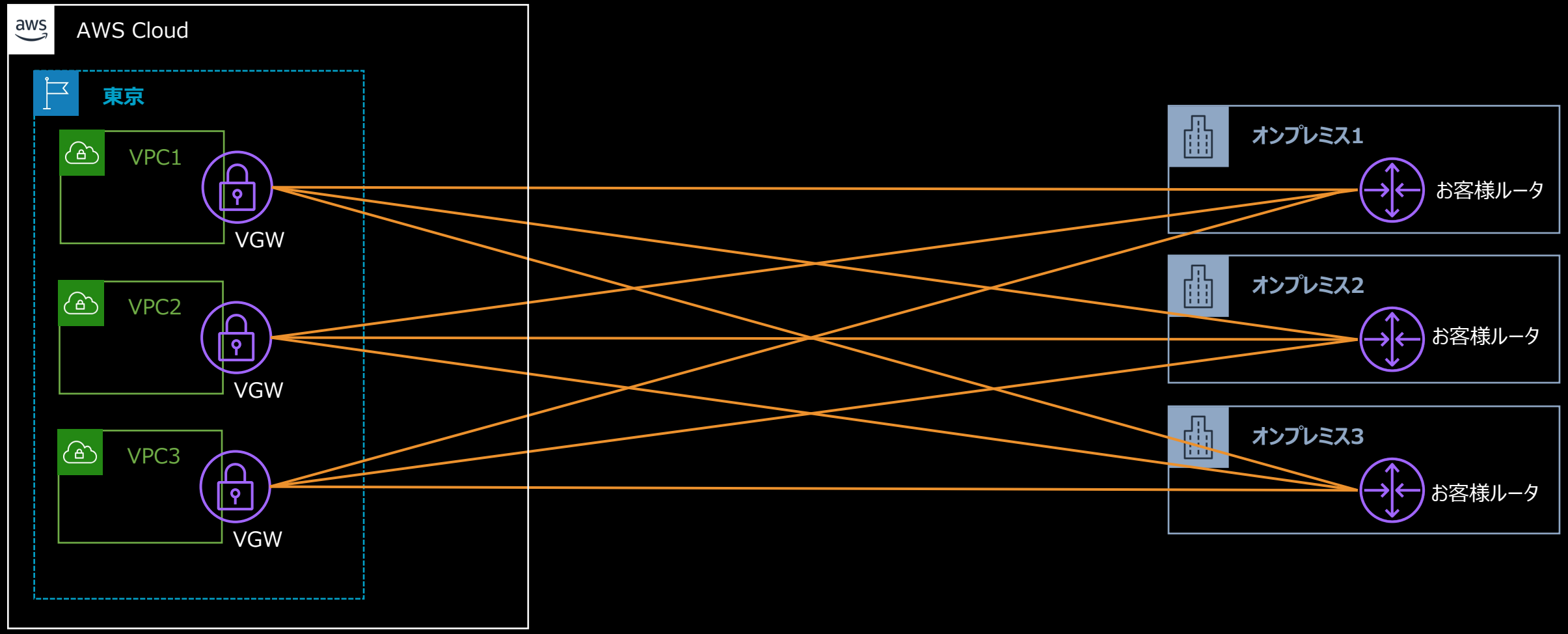
# Direct Connect + Site-to-Site VPN

## Direct Connectのバックアップ回線としてSite-to-Site VPNを使用



# オンプレミス拠点からシステム毎に異なるVPCに接続

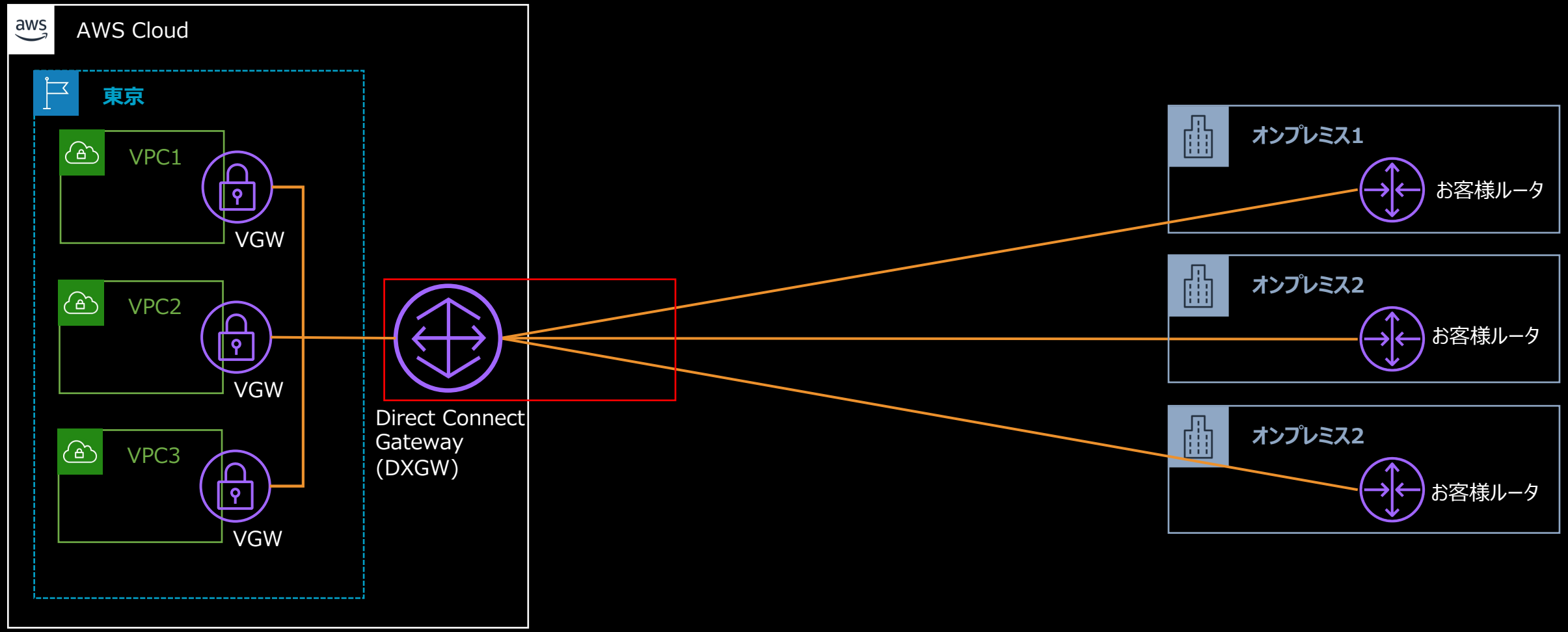
# オンプレミス拠点からシステム毎に異なるVPCに接続




複数のオンプレミス拠点、VPCがある場合ダイレクトコネクトはメッシュ構成になってしまう。

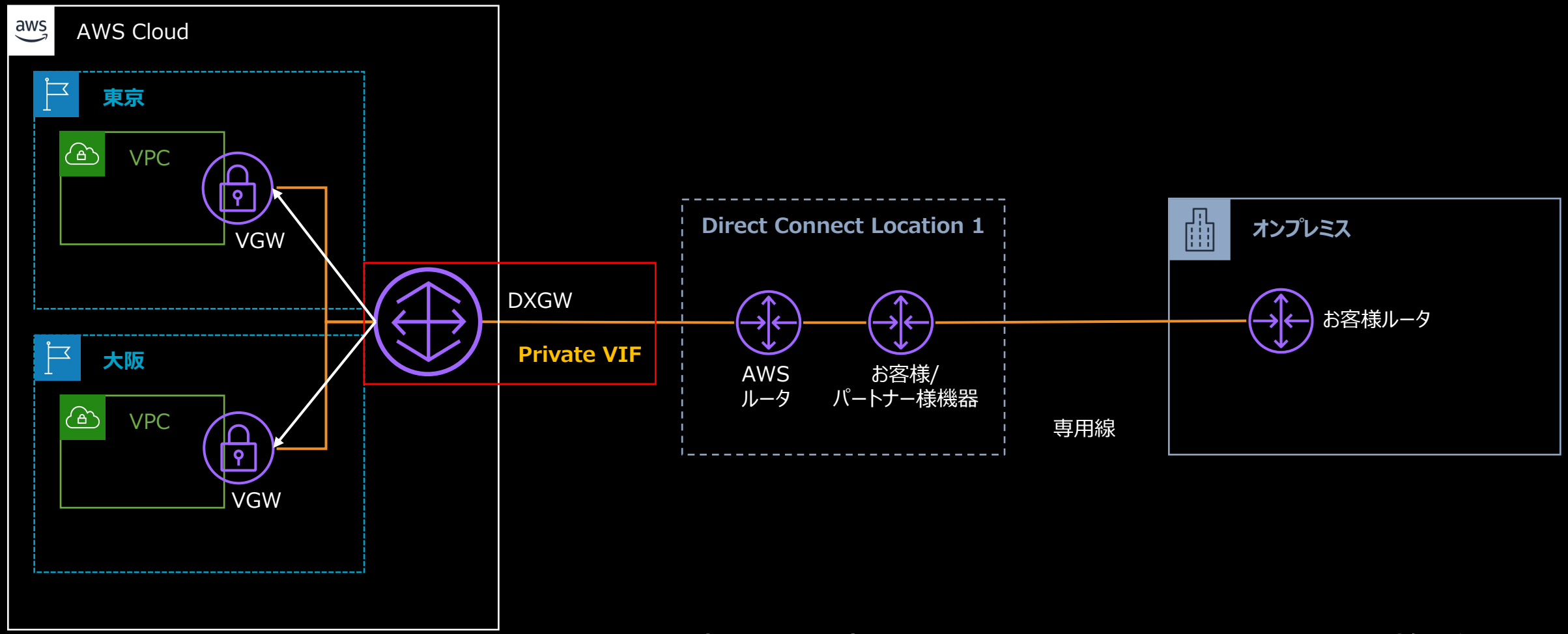
# AWS Direct Connect Gateway

# オンプレミス拠点からシステム毎に異なるVPCに接続



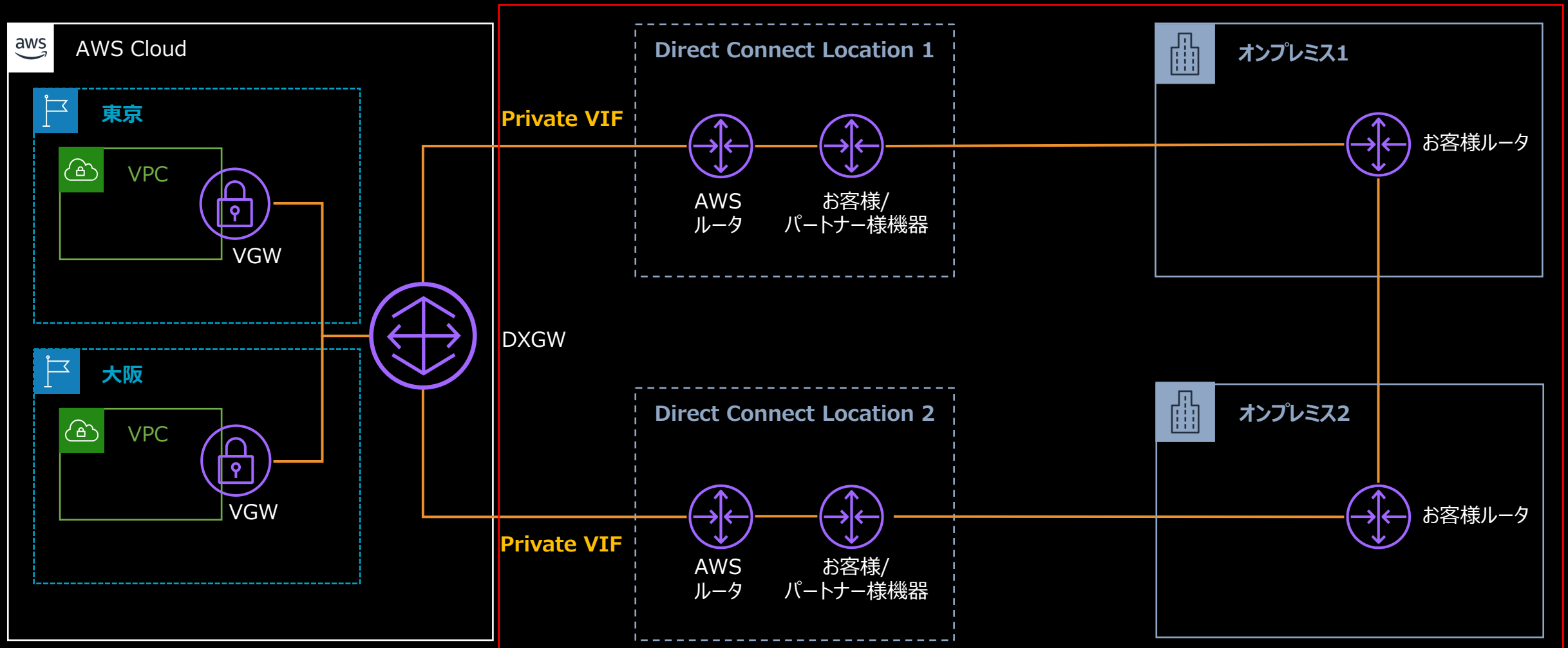

ダイレクトコネクトの本数は3拠点分のみ。複数のVPCがあっても、DXGWを使用する事により
効率的にダイレクトコネクトを使用する事ができます。 ※最大10VPCまで接続可能

# オンプレミス拠点からシステム毎に異なるVPCに接続




DXGWを使用する事により、中国を除く全リージョンの複数VPCと
AWS専用線を使用して通信が可能です。

# Direct Connect冗長化

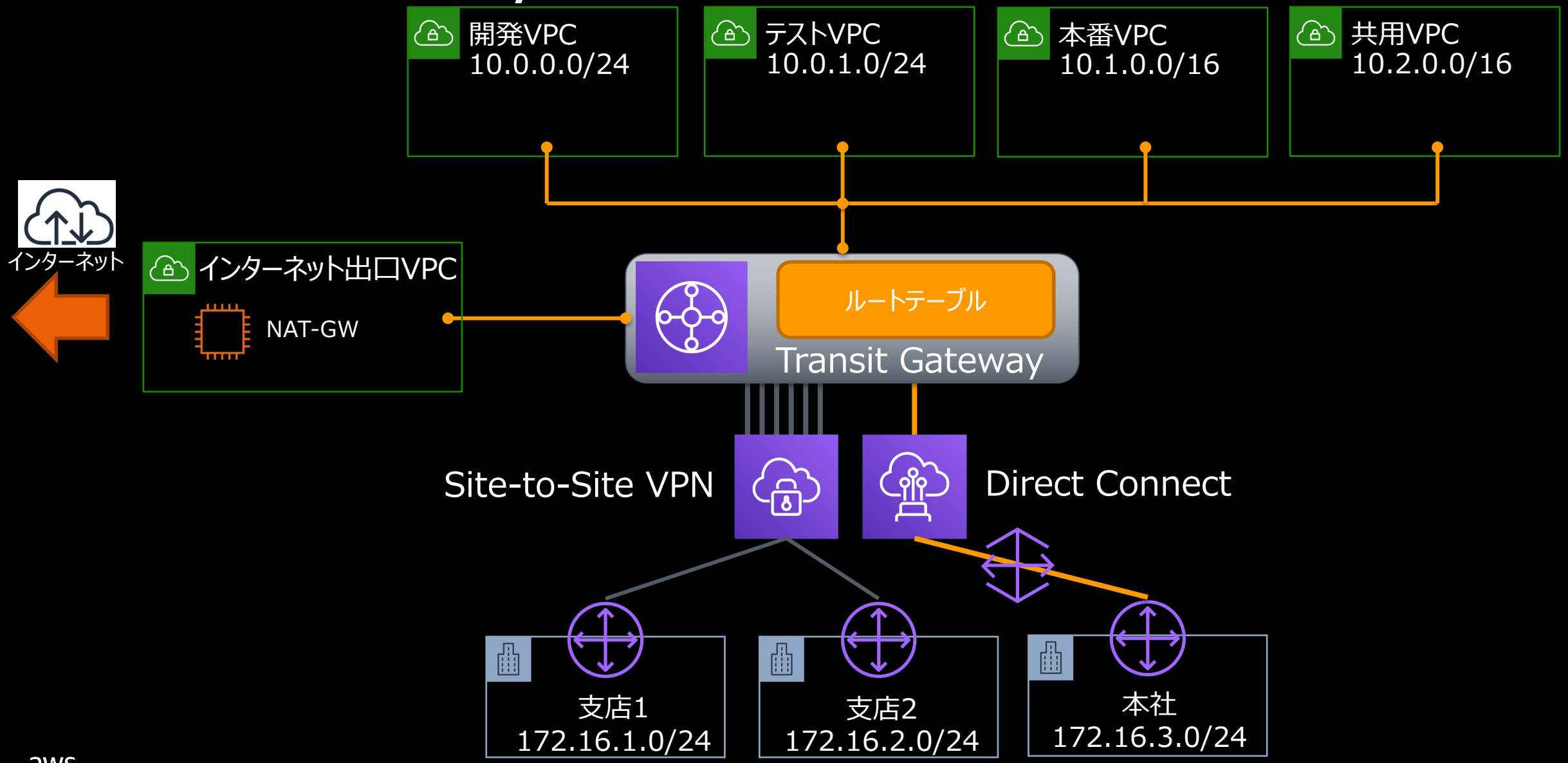



回線のみを冗長するのではなく、Direct Connect Locationやお客様のオンプレミス拠点設備を冗長する事で、より物理的な耐障害性を高める事が可能です。

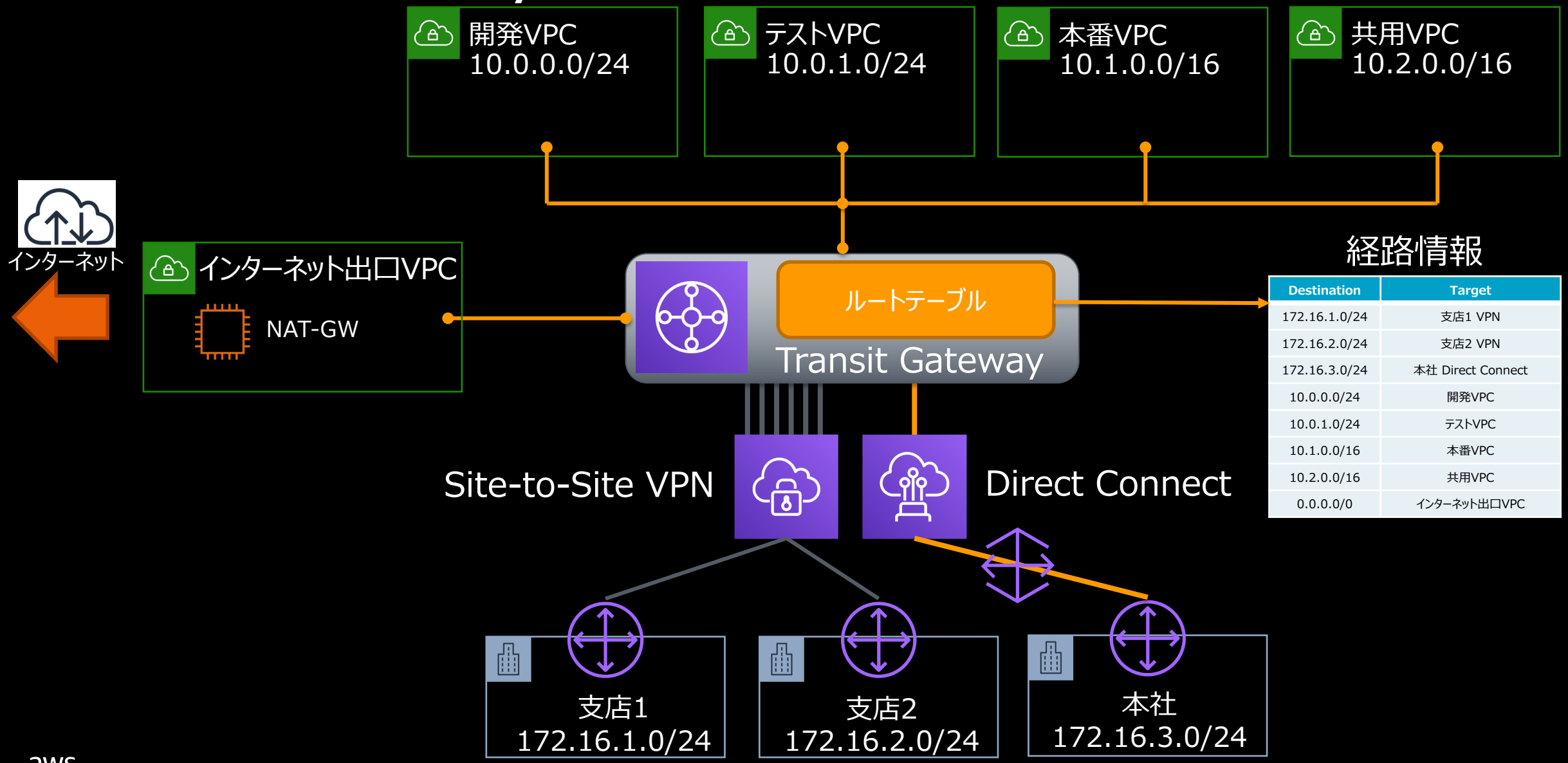
# 多数のVPCやオンプレミス拠点を相互接続しルーティングを一元管理したい

# AWS Transit Gateway

# Transit Gatewayとは



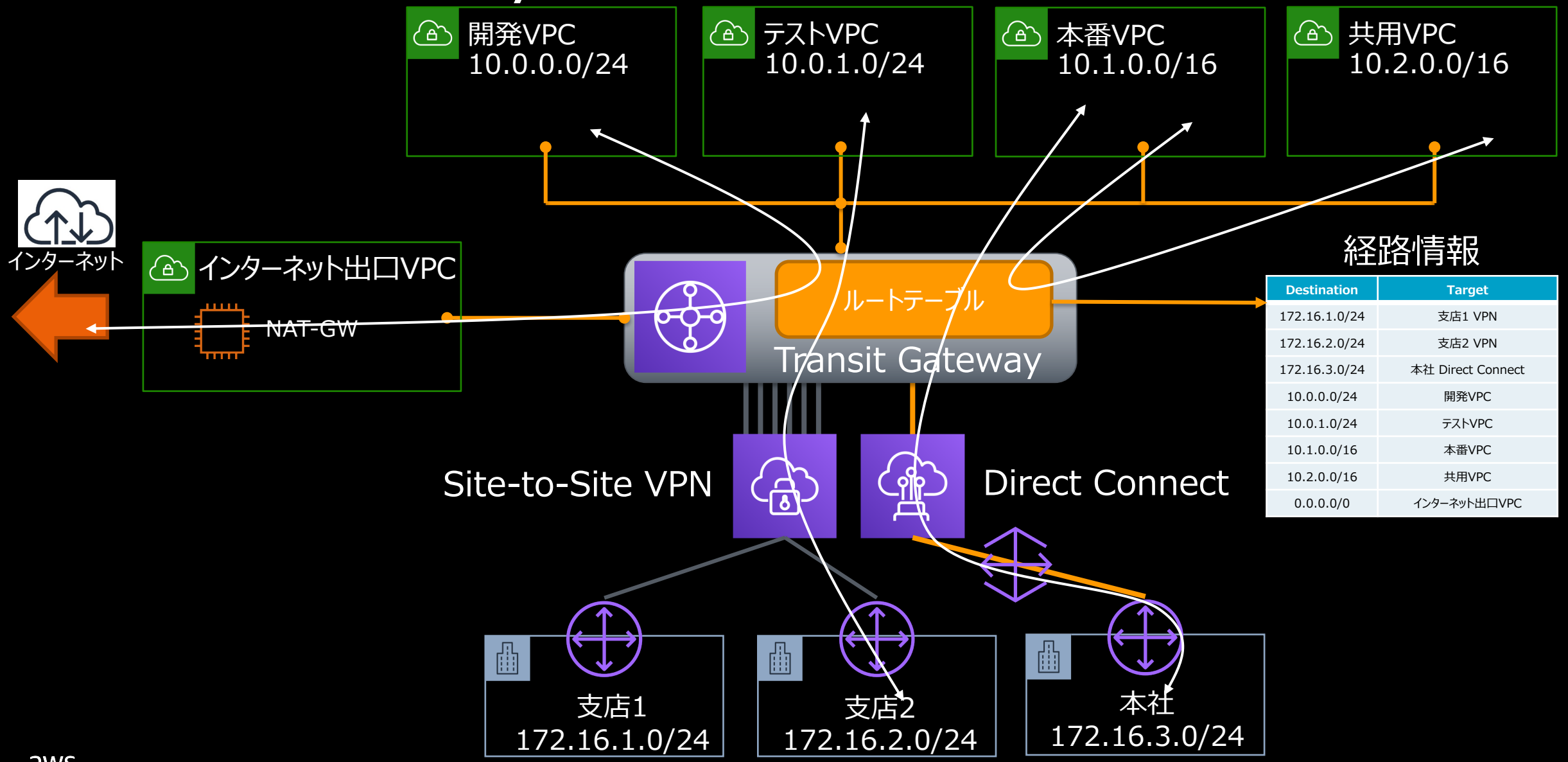
# Transit Gatewayとは




経路情報

| Destination | Target |
|---|---|
| 172.16.1.0/24 | 支店1 VPN |
| 172.16.2.0/24 | 支店2 VPN |
| 172.16.3.0/24 | 本社 Direct Connect |
| 10.0.0.0/24 | 開発VPC |
| 10.0.1.0/24 | テストVPC |
| 10.1.0.0/16 | 本番VPC |
| 10.2.0.0/16 | 共用VPC |
| 0.0.0.0/0 | インターネット出口VPC |

# Transit Gatewayとは



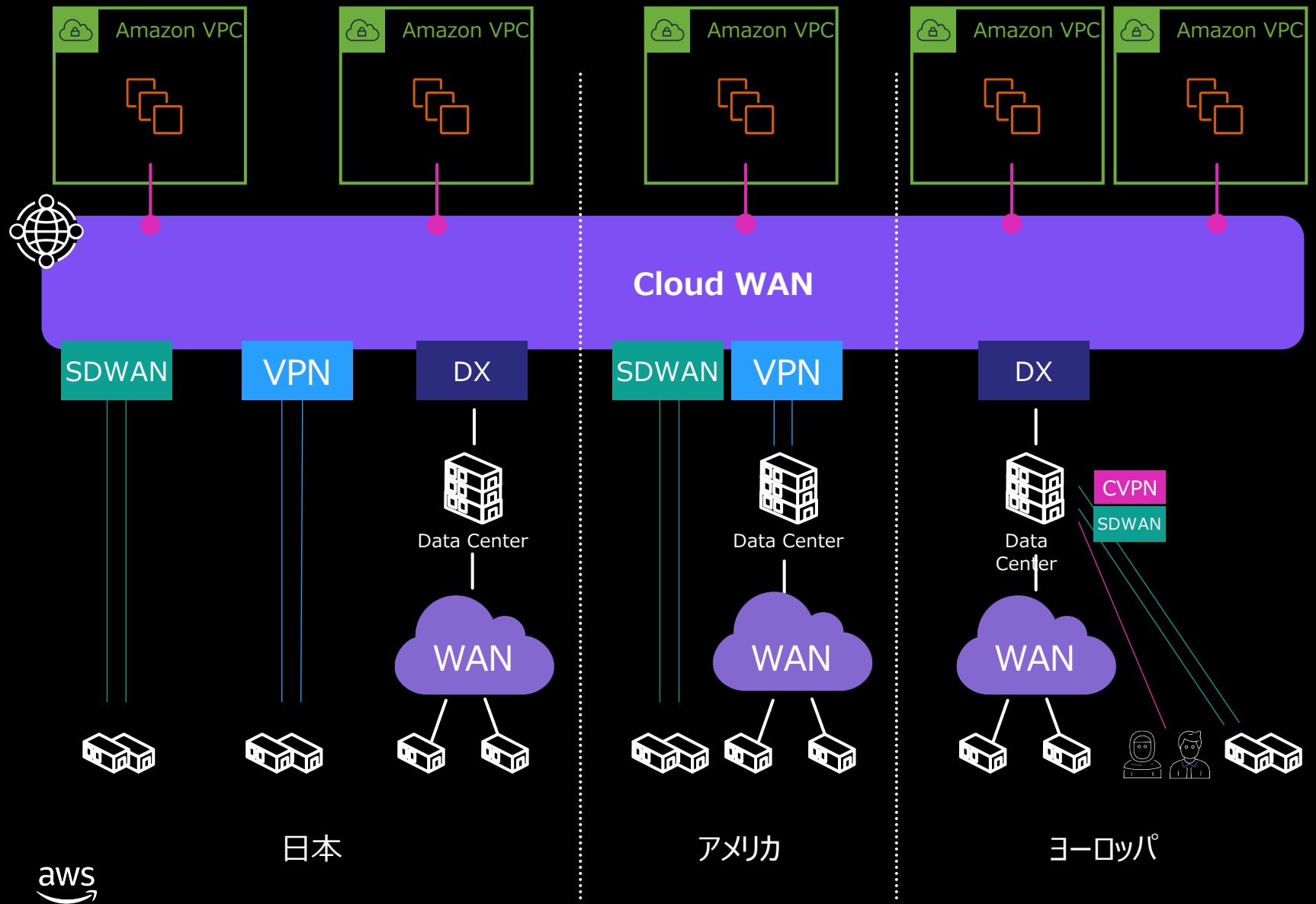

経路情報

| Destination | Target |
|---|---|
| 172.16.1.0/24 | 支店1 VPN |
| 172.16.2.0/24 | 支店2 VPN |
| 172.16.3.0/24 | 本社 Direct Connect |
| 10.0.0.0/24 | 開発VPC |
| 10.0.1.0/24 | テストVPC |
| 10.1.0.0/16 | 本番VPC |
| 10.2.0.0/16 | 共用VPC |
| 0.0.0.0/0 | インターネット出口VPC |

# 新サービス紹介

# AWS Cloud WAN

# Cloud WAN




## グローバルネットワーク

リージョンを跨いだネットワーク
接続性を提供

## 一元管理

ルーティング情報
ネットワークポリシー
日常業務の自動化

## アタッチメント

VPCs
VPNs
SD-WAN(TGW Connect)

※AWS Direct Connectは現在サポートしておりません。

# 本日ご紹介するサービス

VPNを介してAWSへプライベートに接続するサービス

AWS Site-to-Site VPN

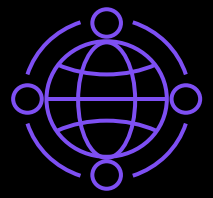
専用線を介してAWSへプライベートに接続するサービス

AWS Direct Connect

多数のVPCやオンプレミス拠点のルーティングを一元管理

AWS Transit Gateway

グローバルを跨いだVPCやオンプレミス拠点間のWANルーティングを一元管理



AWS Cloud WAN

**NEW!**

# まとめ

# まとめ

- VPCはお客様の仮想データセンターです。オンプレミスネットワークと同様な環境がつくれます。また、VPC内はデータセンターが冗長化された可用性の高いシステム構成が構築できます。
- オンプレミス拠点とAWSクラウドを接続する事により、AWSクラウドをオンプレミスの一部として利用する事が可能となります。
- オンプレミス拠点とAWSクラウドを接続する際は、お客様の要件によりAWSネットワークサービスを使い分ける事ができます。よって、各サービスの特性を理解する事が重要です。
- 新サービスである、 Cloud WANを活用する事で、お客様はAWSのグローバルインフラストラクチャをWANとして利用する事ができます。お客様のWANにおいてもクラウドならではの俊敏性を得る事ができます。

# 参考資料

- AWS リージョン別のサービス
  https://aws.amazon.com/jp/about-aws/global-infrastructure/regional-product-services/
- Black Beltオンラインセミナー：Amazon VPC
  https://aws.amazon.com/jp/blogs/news/webinar-bb-amazonvpc-2020/
- Black Beltオンラインセミナー：Amazon VPC Advanced
  https://aws.amazon.com/jp/blogs/news/webinar-bb-amazon-vpc-advanced-2019/
- Black Beltオンラインセミナー：AWS Site-to-Site VPN
  https://aws.amazon.com/jp/blogs/news/webinar-bb-amazonvpc-2020/
- Black Beltオンラインセミナー：AWS Direct Connect
  https://aws.amazon.com/jp/blogs/news/webinar-bb-awsdirectconnect-2021/
- Black Beltオンラインセミナー：AWS Transit Gateway
  https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-transit-gateway-2019/

# Thank you!

藤井 拓

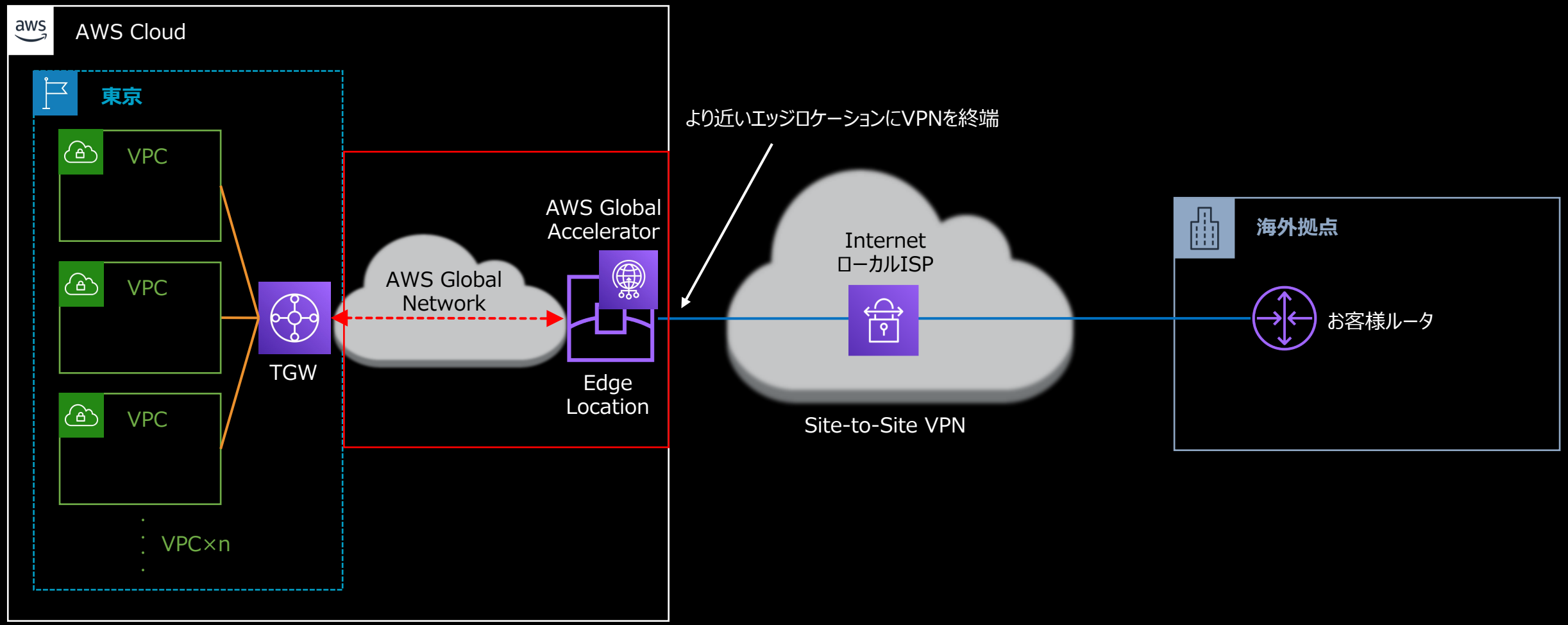
tafuj@amazon.co.jp

# Appendix

# 応用編

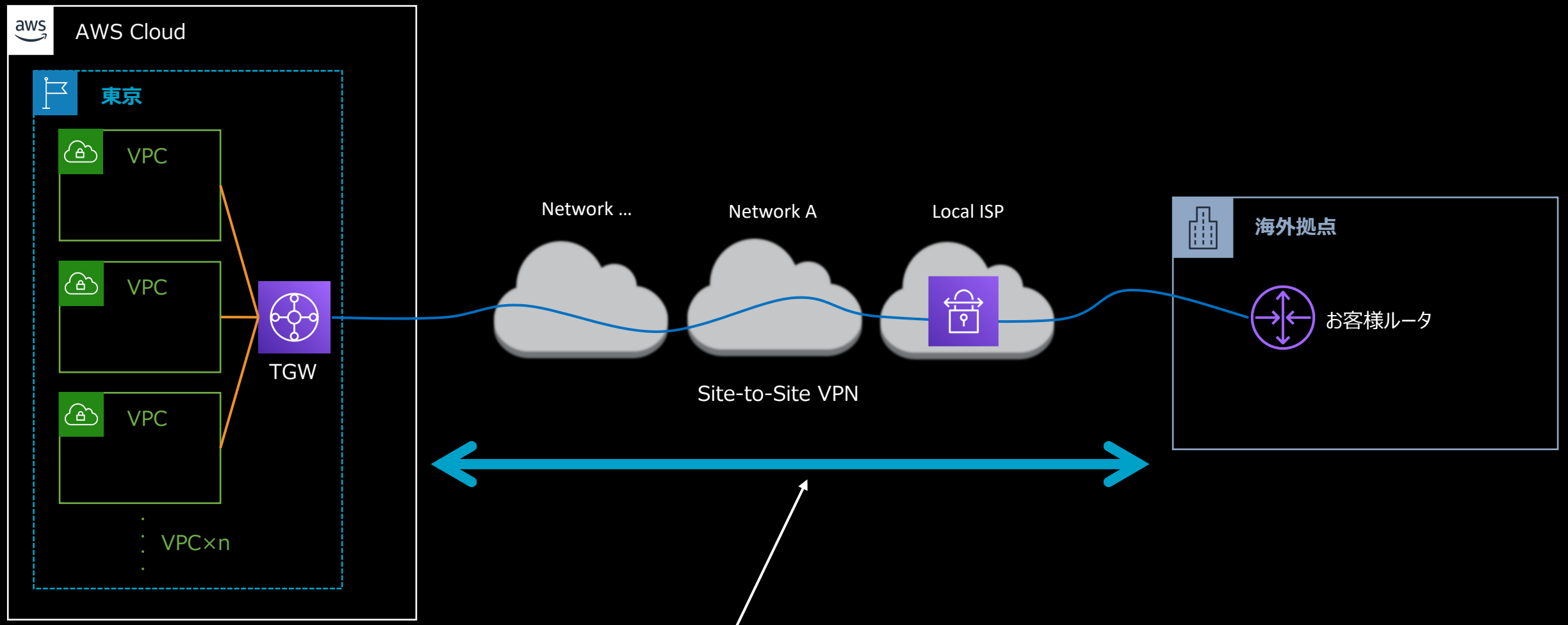
# Accelerated Site-to-Site VPN

# AWS Accelerated Site-to-Site VPN




AWSバックボーンを使いオンプレミスにより近い場所にあるエンドポイントへ接続する事が可能。
海外から東京リージョンへVPN接続している場合等に有効。

# AWS Accelerated Site-to-Site VPN（未使用）




複数の管理が違うパブリックインターネットを経由するため、トラフィックの品質が不安定になる可能性がある。

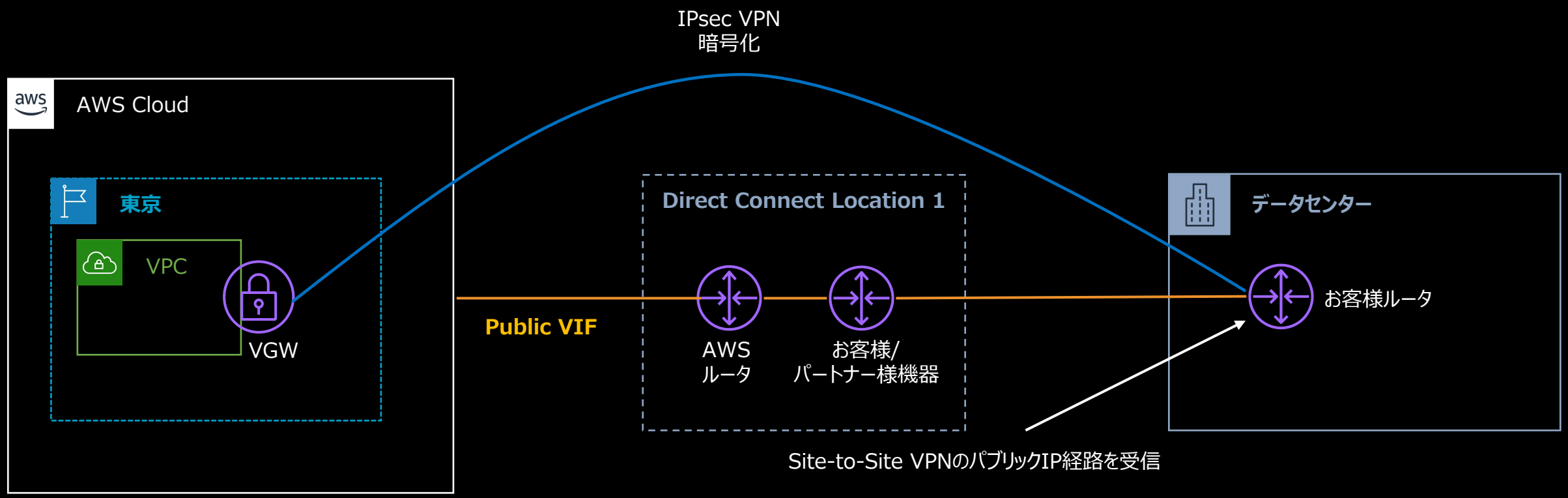
# Direct Connect区間を暗号化したい

# Direct Connectパブリック接続

# Direct Connectパブリック接続

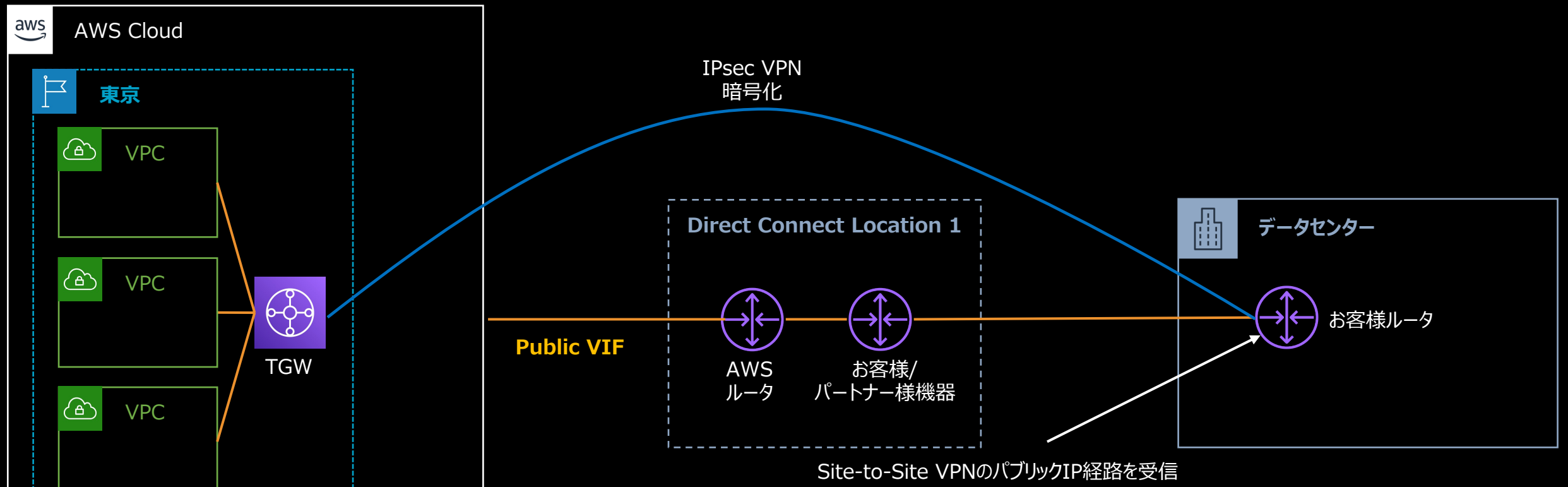

Direct Connectパブリック接続は中国リージョンを除く全リージョンのAWSサービスのパブリックIPをお客様のオンプレミスルータに広報します。よって、Internetを使用せずDirect Connectを経由し、AWSのパブリックサービスにアクセスできます。

# Direct Connect区間暗号化（VGWの場合）




Site-to-Site VPNはパブリックサービスです。Public VIFを使用する事により、Direct Connect区間でVPNを使用する事ができます。

# Direct Connect区間暗号化（TGWの場合）

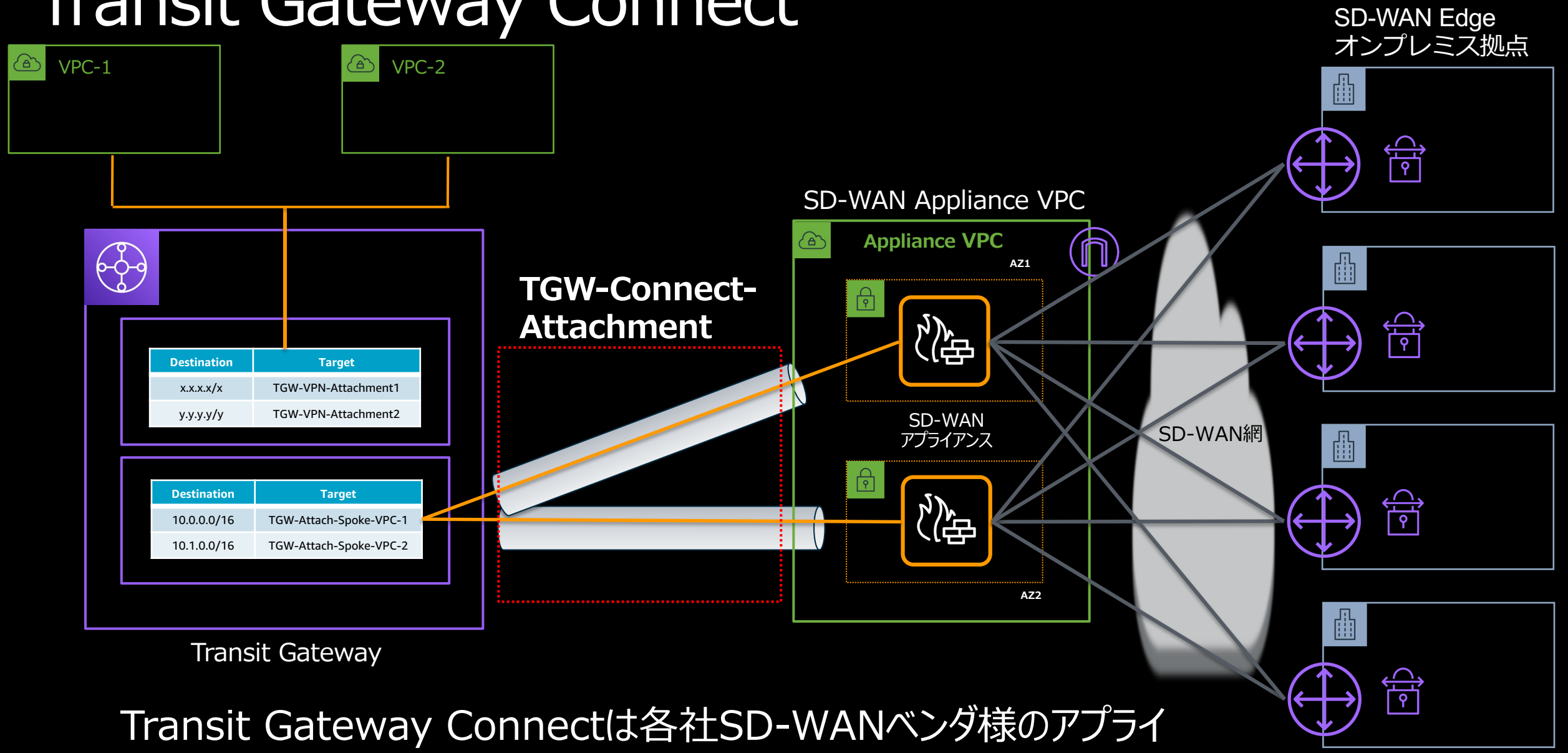



Site-to-Site VPNはパブリックサービスです。Public VIFを使用する事により、Direct Connect区間でVPNを使用する事ができます。

# SD-WAN経由でAWSクラウドにアクセスしたい

# Transit Gateway Connect

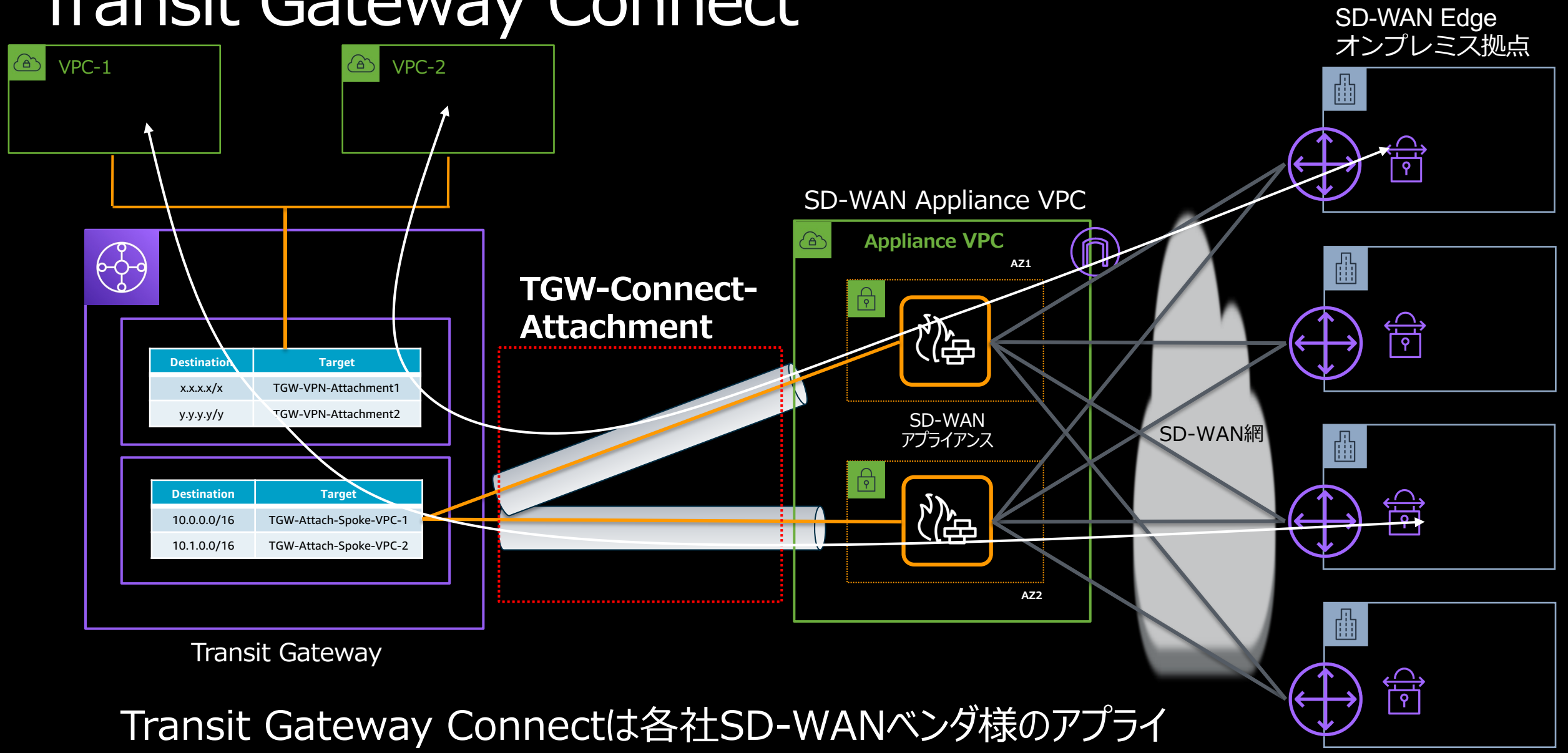
# Transit Gateway Connect




Transit Gateway Connectは各社SD-WANベンダ様のアプライアンスとTransit Gatewayの接続を簡素化します。

TGW Connectの詳細に関しましてはこちら

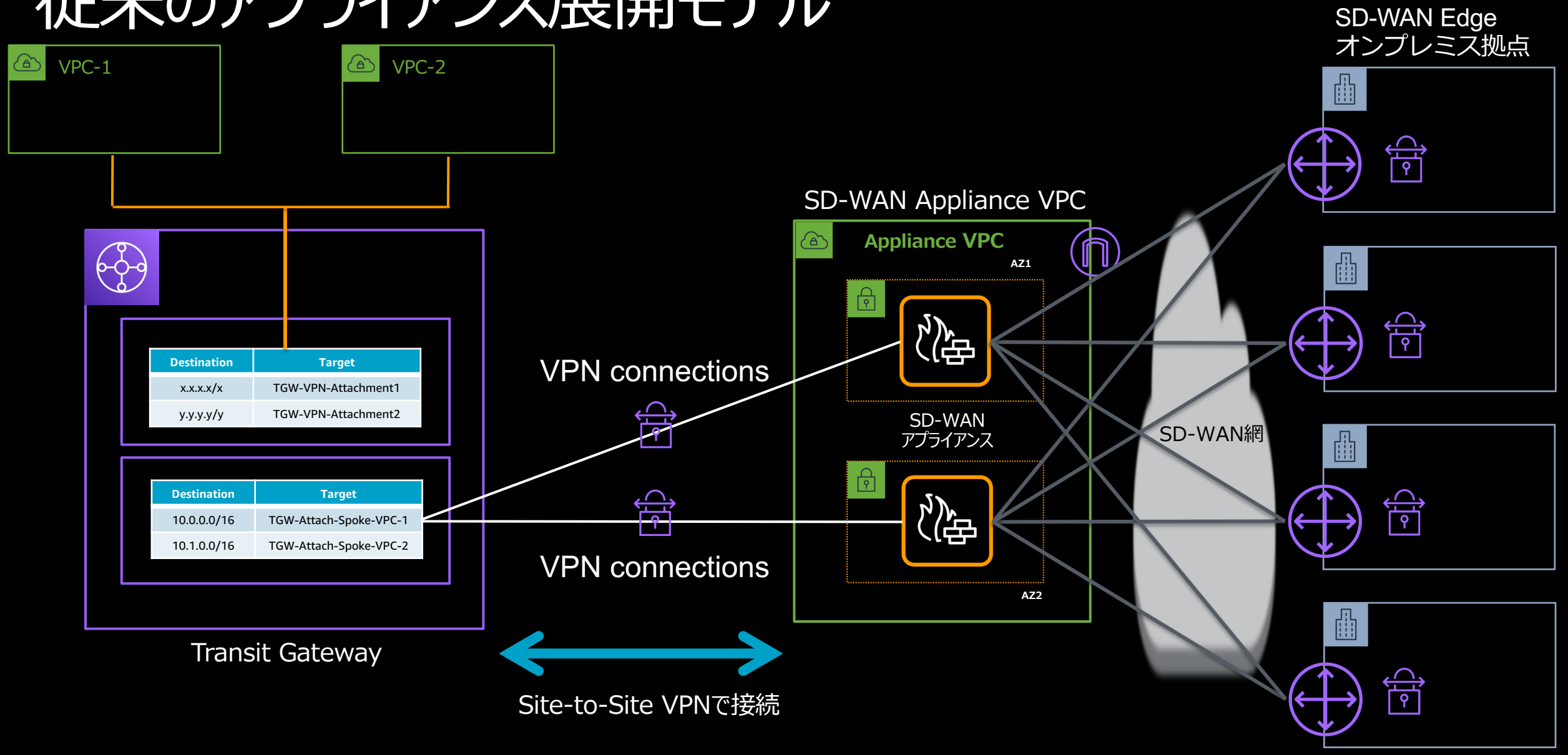
# Transit Gateway Connect




Transit Gateway Connectは各社SD-WANベンダ様のアプライアンスとTransit Gatewayの接続を簡素化します。

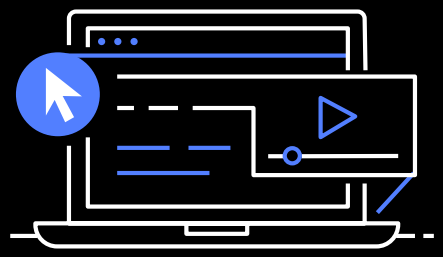
TGW Connectの詳細に関しましてはこちら

# 従来のアプライアンス展開モデル



# Transit Gateway Connect

# AWS デジタルトレーニング



実力、自信、信頼性を高め、業界で認められた資格で差をつけよう

## デジタル学習

- スキルビルダー – AWS のエキスパートが開発した数百のデジタルトレーニングを自分のスケジュールで学習できます
- Cloud Quest - AWS Cloud Quest は、実践的なクラウド経験を積み、AWSクラウドのスキルを身につけることができる、初めてで唯一のロールプレイングゲームです

## 認定試験準備ためのリソース

- Cloud Practitioner - AWS Certified Cloud Practitioner 取得に役立つリソースをご紹介します
- Developer – Associate – AWS Certified Developer – Associate 取得に役立つリソースをご紹介します

aws

aws.amazon.com/jp/training

# AWS Builders Online Series に
# ご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについての
ご希望や改善のご提案などがございましたら、ぜひお聞かせください。


aws-apj-marketing@amazon.com


twitter.com/awscloud_jp


facebook.com/600986860012140


https://www.youtube.com/user/AmazonWebServicesJP


https://www.linkedin.com/showcase/aws-careers/


twitch.tv/aws

# Thank you!