AWS-55

グローバルネットワーク展開を迅速化する AWS インフラストラクチャ活用方法

藤井 拓
技術統括本部 ネットワークスペシャリスト ソリューションアーキテクト
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
ネットワークソリューションアーキテクト

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

本日持ち帰ってもらいたい事

- AWS Direct Connect SiteLinkの概要及び、ユースケースを理解する
- AWS Cloud WANの概要及び、ユースケースを理解する
- WAN構築時におけるAWSグローバルネットワークの活用方法を理解する

本セッションでご紹介する内容

- AWSが描くNetworkingのビジョン
- AWSグローバルネットワークインフラストストラクチャ活用方法

  新サービス：AWS Direct Connect SiteLink New

  新サービス：AWS Cloud WAN(Public Preview) New

※AWS Cloud WANは現在Public Previewとしてご利用可能です。

AWSが描くNetworkingのビジョン

AWSグローバルフットプリント

26のリージョン、84のアベイラビリティゾーンで構成
冗長化された100 Gbpsリンクで接続

AWSが描くNetworkingのビジョン

エッジからデーセンターまでを繋ぐネットワーク

AWSハイブリッド接続ソリューション

On premises

Cloud

Users and customers

Branch offices

5G devices

Metro areas

幅広いハイブリットネットワーク接続を提供

AWSが描くNetworkingのビジョン

エッジからデーセンターまでを繋ぐネットワーク

多様な接続方式を提供

AWSグローバルインフラストラクチャをオンプレミスネットワークの一部として利用

AWS Direct Connect

NEW!

AWS Direct Connect SiteLink

NEW!

AWS Cloud WAN (preview)

AWS Site-to-Site VPN

AWS Client VPN

Global Regions

AWS Local Zones

AWS Outposts

AWS Wavelength

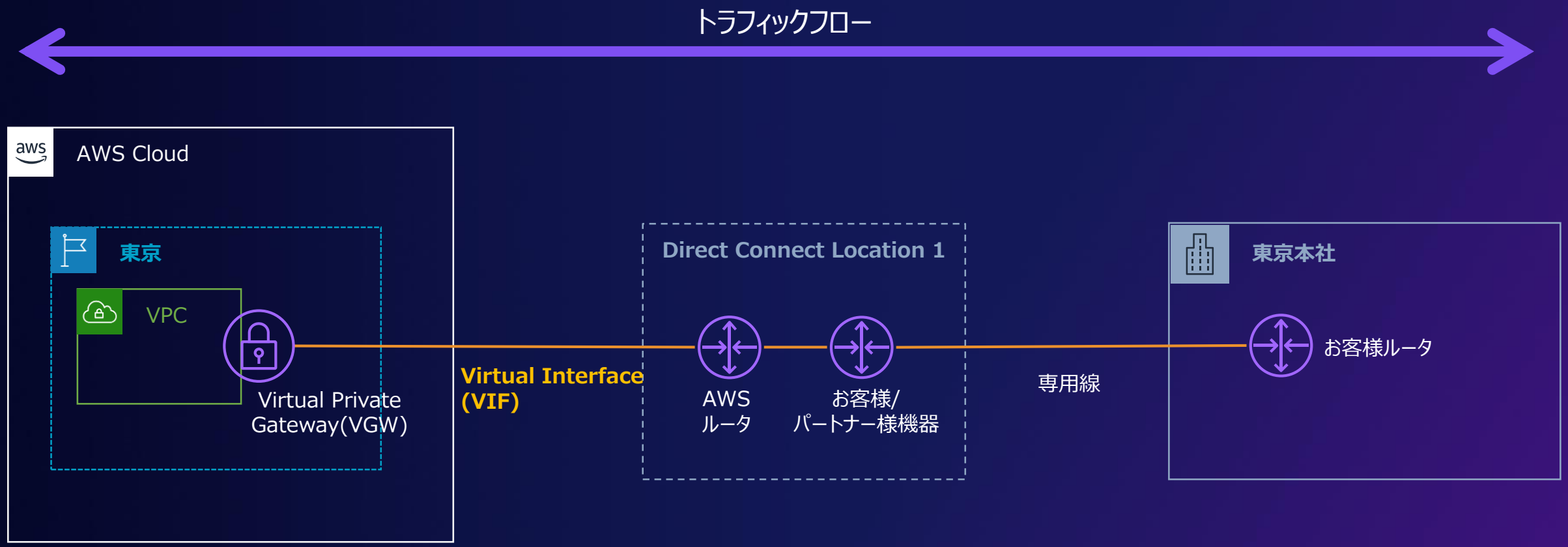
AWS Private 5G

AWSグローバルネットワーク インフラストラクチャ活用方法

AWS Direct Connect SiteLink

AWS Direct Connect

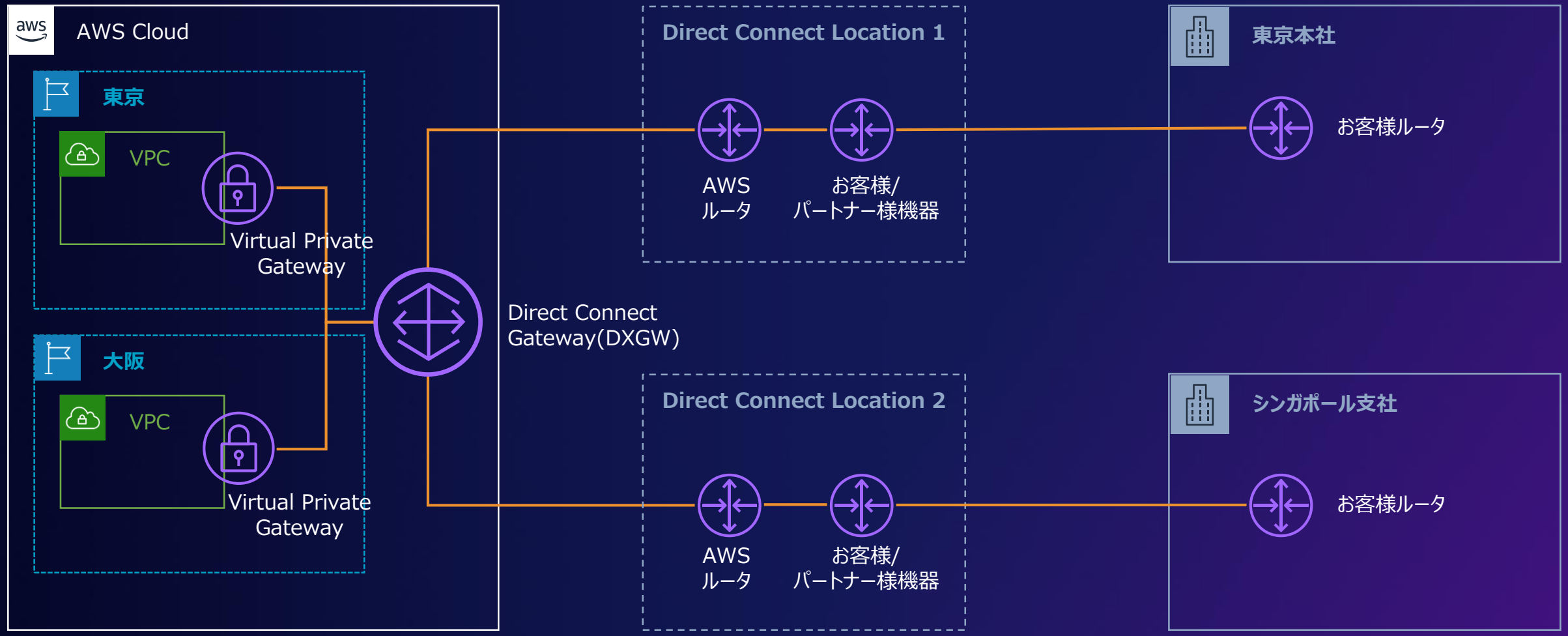
Direct Connectとは



AWS Direct Connectは、お客様の拠点と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の詳細に関しましてはこちら

Direct Connect Gateway（DXGW）



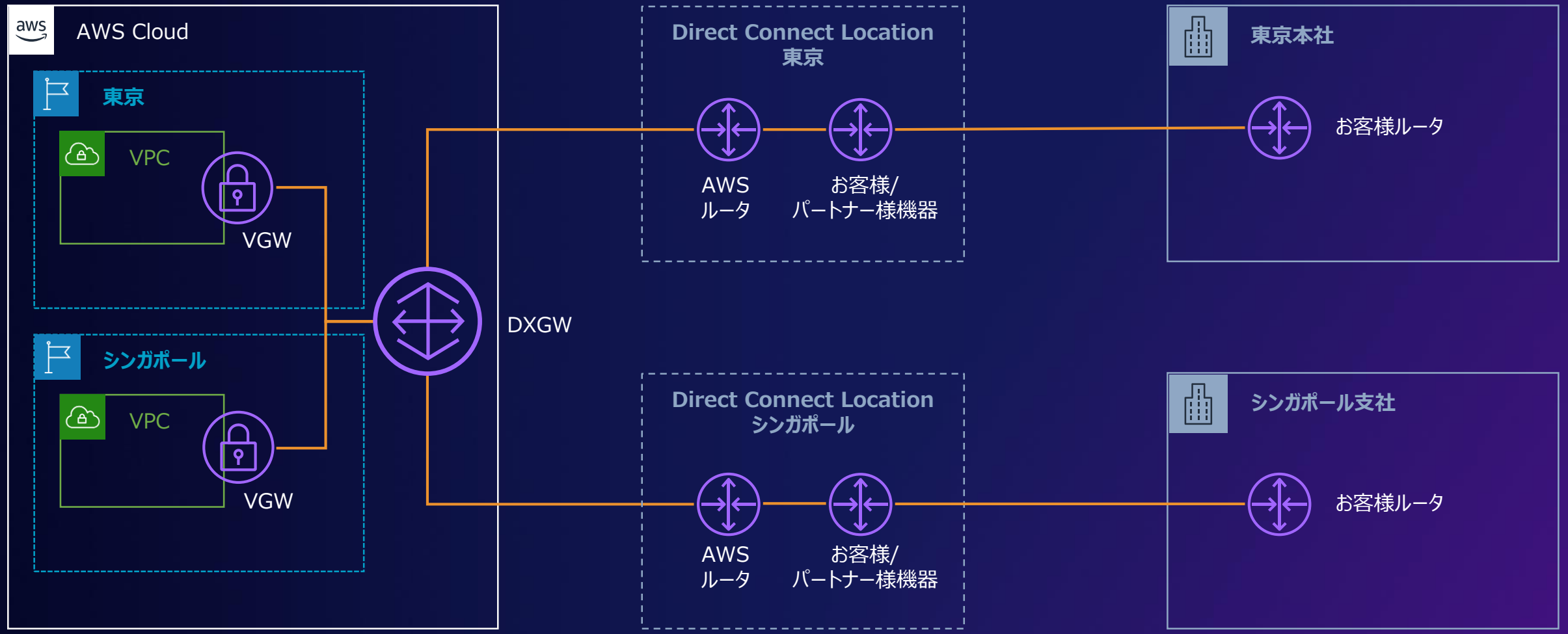
Direct Connect Gatewayを使用する事により、中国を除く全リージョンの複数VPCとAWS閉域網を使用して通信が可能です。

Direct Connect SiteLink

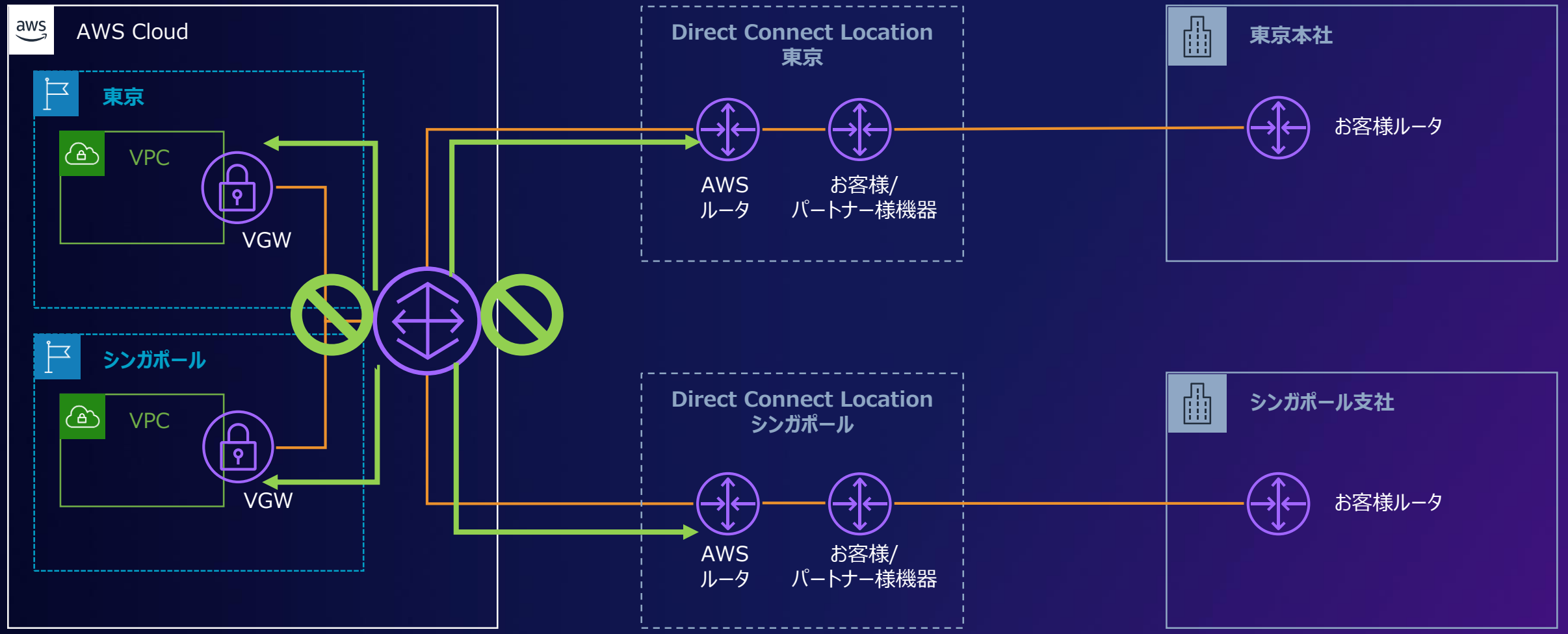
Direct Connect SiteLink概要

- 機能を利用したいVirtual Interface(Private VIF又はTransit VIF)のコンソール上で有効化するだけで利用可能
- オンプレミス拠点間のネットワークをAWSグローバルネットワークバックボーン網を介し、網内の最短パス経路で相互接続性を提供
- 全リージョンで利用可能（中国を除く）
- 柔軟な接続帯域をご用意（50 Mbps～100 Gbps）

Direct Connect SiteLink使用前

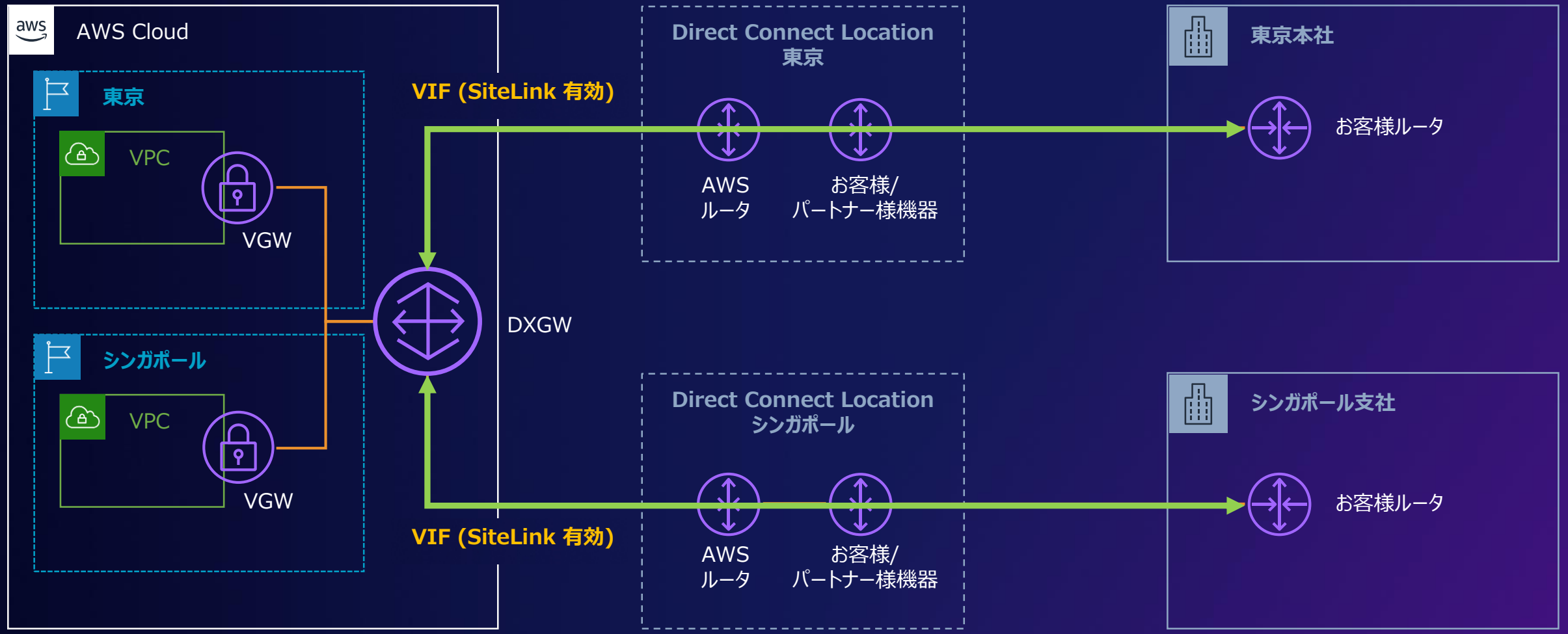


Direct Connect SiteLink使用前



Direct Connect Gatewayはオンプレミス拠点間、VPC間の折返し通信は未サポート。

Direct Connect SiteLink使用後



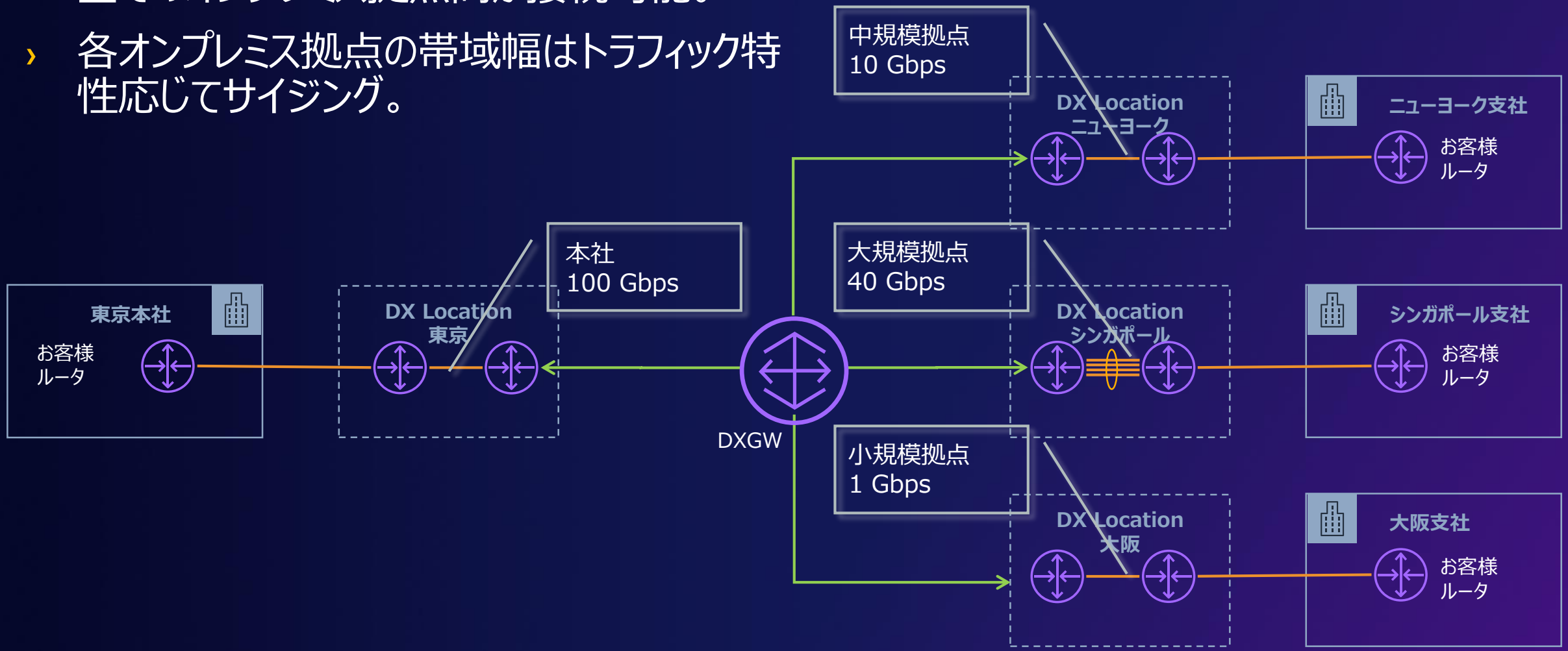
Site Linkは同じDirect Connect Gatewayに収容されたVIF間で折返し通信をサポート。

Direct Connect SiteLink の有効化

- 機能を利用したい VIF のコンソール上で有効化するだけで利用可能
- VIF 作成時および作成後のいつでも編集可能
  ※デフォルトは“無効”

Direct Connect SiteLink ユースケース

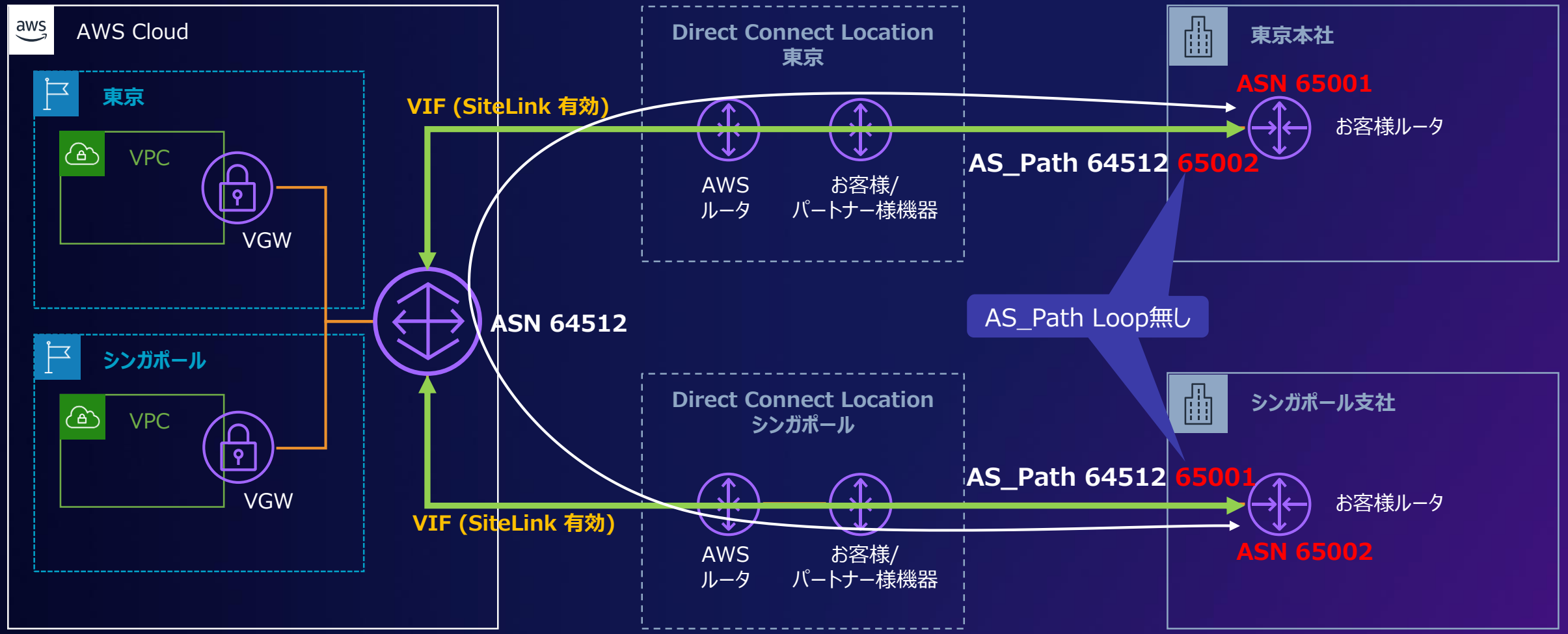
- 全てのオンプレミス拠点間が接続可能。
- 各オンプレミス拠点の帯域幅はトラフィック特性応じてサイジング。



Direct Connect SiteLink 補足

ASN設計の注意点

オンプレミス拠点間通信が可能なASN設計

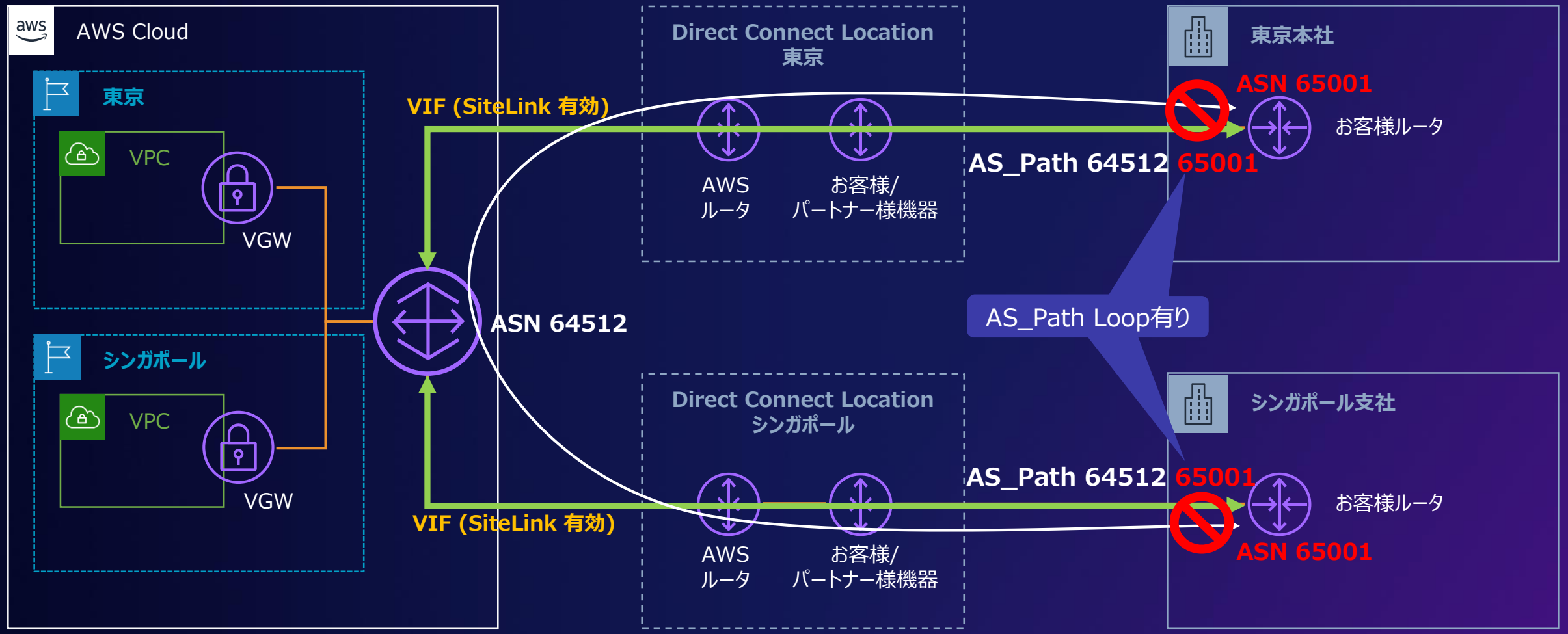


ASN設計の注意点

オンプレミス拠点間通信が不可能なASN設計

※Customer RouterのBGP設定により、自身のAS_Pathが含まれている経路でも、受信する事も可能です。

例：BGP Neighborに対してAllowas-in(Ciscoの場合)を適用する。



BGPは自身のAS_PATHが含まれている経路はループと判断し、その経路を破棄します。結果拠点間の通信ができません。

Direct Connectロケーションマップ

世界中の100以上のロケーションに展開

United States

Ashburn
Atlanta
Boston
Chicago (x2)
Columbus
Dallas
Denver
El Segundo
Hillsboro
Houston
Kansas City
Las Vegas
Los Angeles (x2)
Miami
Milpitas
Minneapolis
New York, NY
Newark
Philadelphia
Phoenix
Portland (x2)
Reston
San Jose (x2)
Santa Clara
Seattle (x2)
Secaucus

Canada

Montreal (x2)
Toronto
Vancouver

South America

Rio de Janeiro
Sao Paulo (x2)

Europe and Africa

Amsterdam (x2)
Berlin
Cape Town
Copenhagen
Dublin (x2)
Frankfurt (x2)
Helsinki
Johannesburg
London (x3)
Madrid (x2)
Manchester
Marseille
Milano (x2)*
Munich
Oslo
Paris (x3)
Prague
Slough
Stockholm
Vienna
Warsaw
Zurich

Middle East

Dubai UAE
Fujairah
Israel Haifa
Manama (x2)

China

Shanghai
Shenzhen
Ningxia (x2)
Beijing (x2)

Asia Pacific

Bangalore
Canberra
Chennai
Delhi
Hong Kong (x2)
Hyderabad*
Kuala Lumpur
Melbourne
Mumbai (x2)
Osaka
Perth
Seoul (x2)
Singapore (x2)
Sydney (x2)
Taipei (x2)
Tokyo (x2)

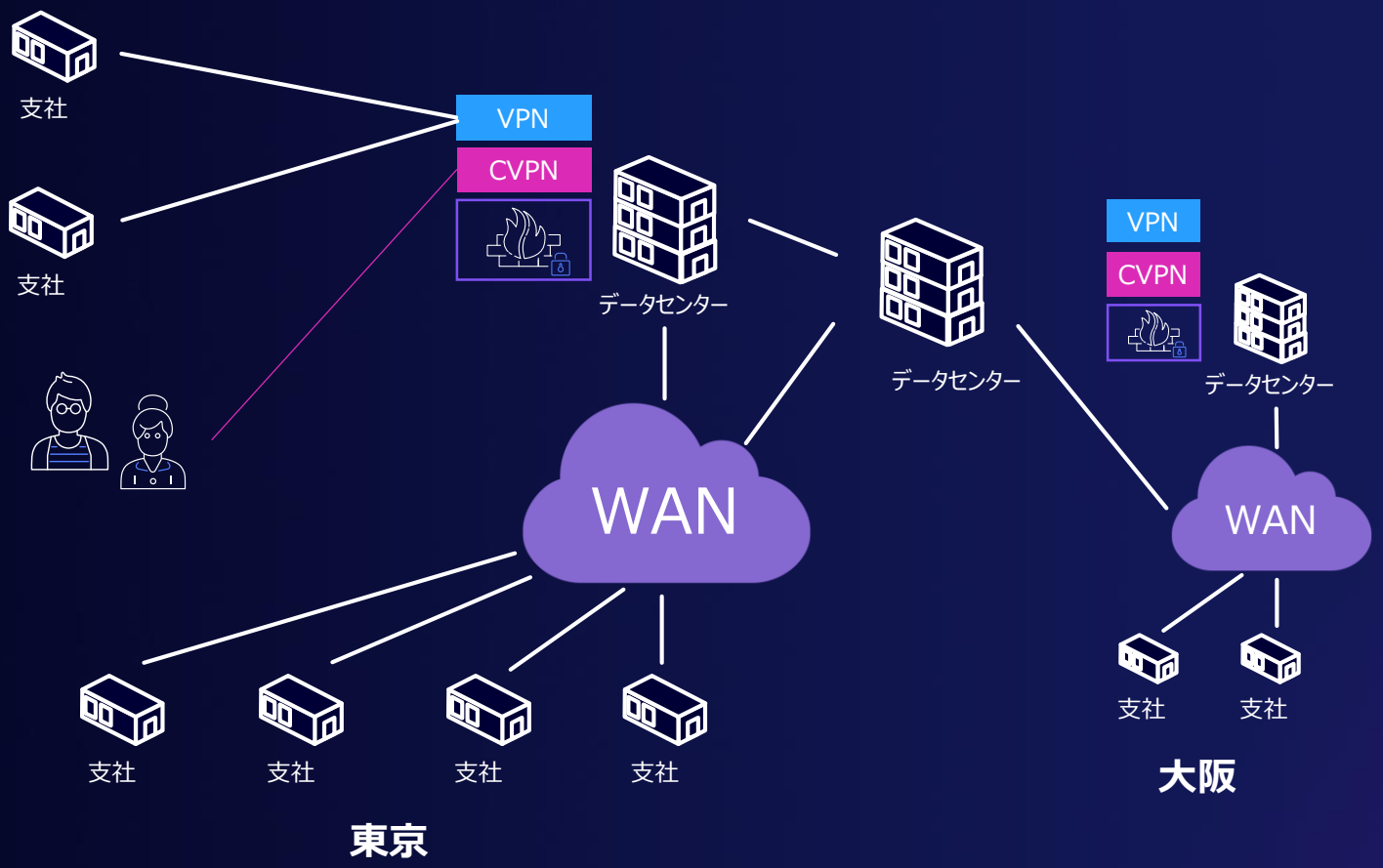
*New in 2021

詳細は AWS Direct Connect locations page （英語）をご参照ください。

AWS Cloud WAN(Public Preview)

Wide Area Network(WAN)

エンタープライズWAN（クラウド接続前）



接続形態

- キャリア網、VPN、Client VPN

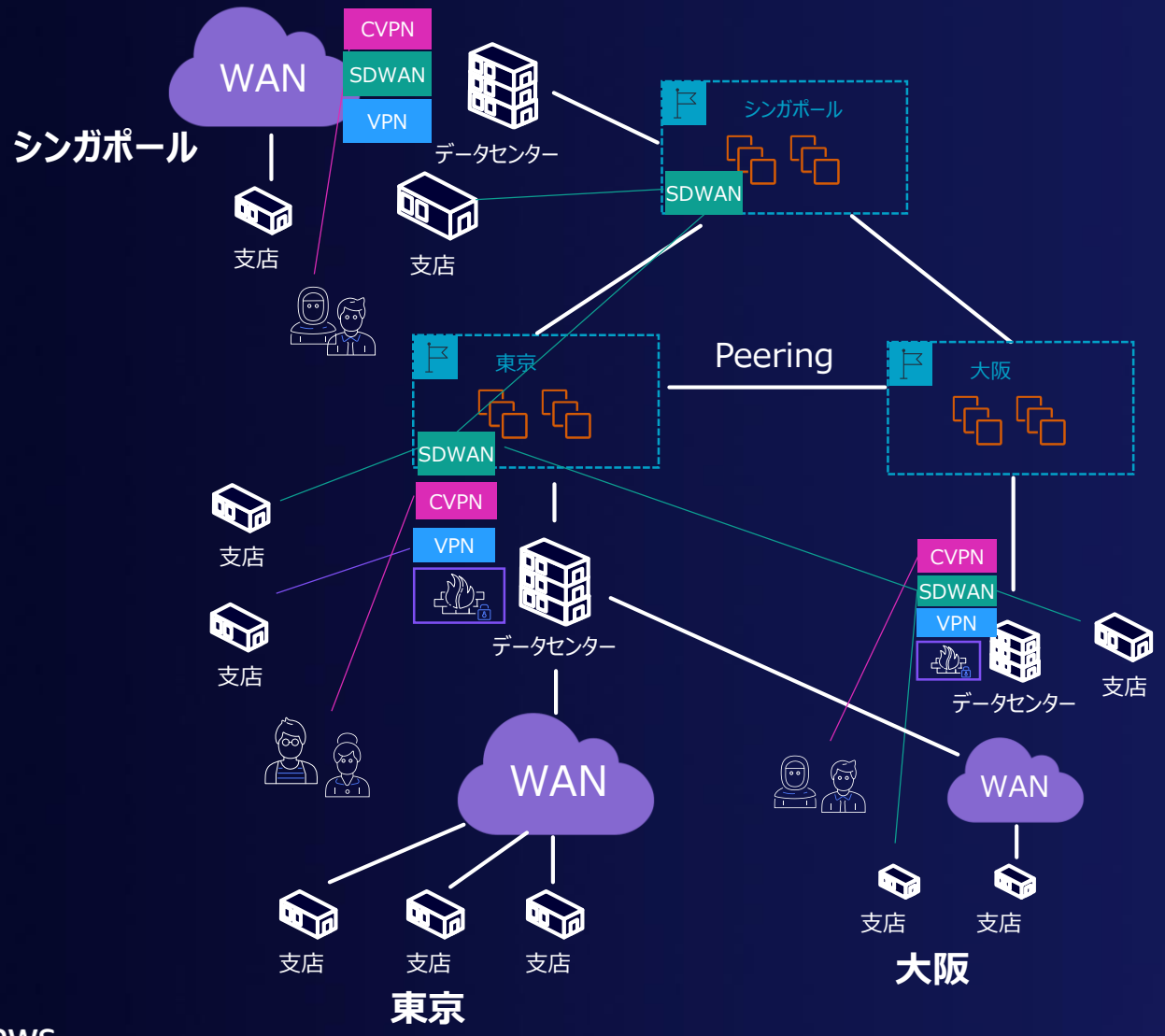
トラフィックフロー

- オフィス拠点間
- オフィス拠点⇔データセンター間
- リモートユーザ⇔データセンター間

課題

- ネットワーク肥大化によるポリシー管理
- 拠点追加時のリードタイム
- 新たに海外拠点追加する際のリードタイムはさらに伸びる

エンタープライズWAN（クラウド接続追加）



追加される接続形態

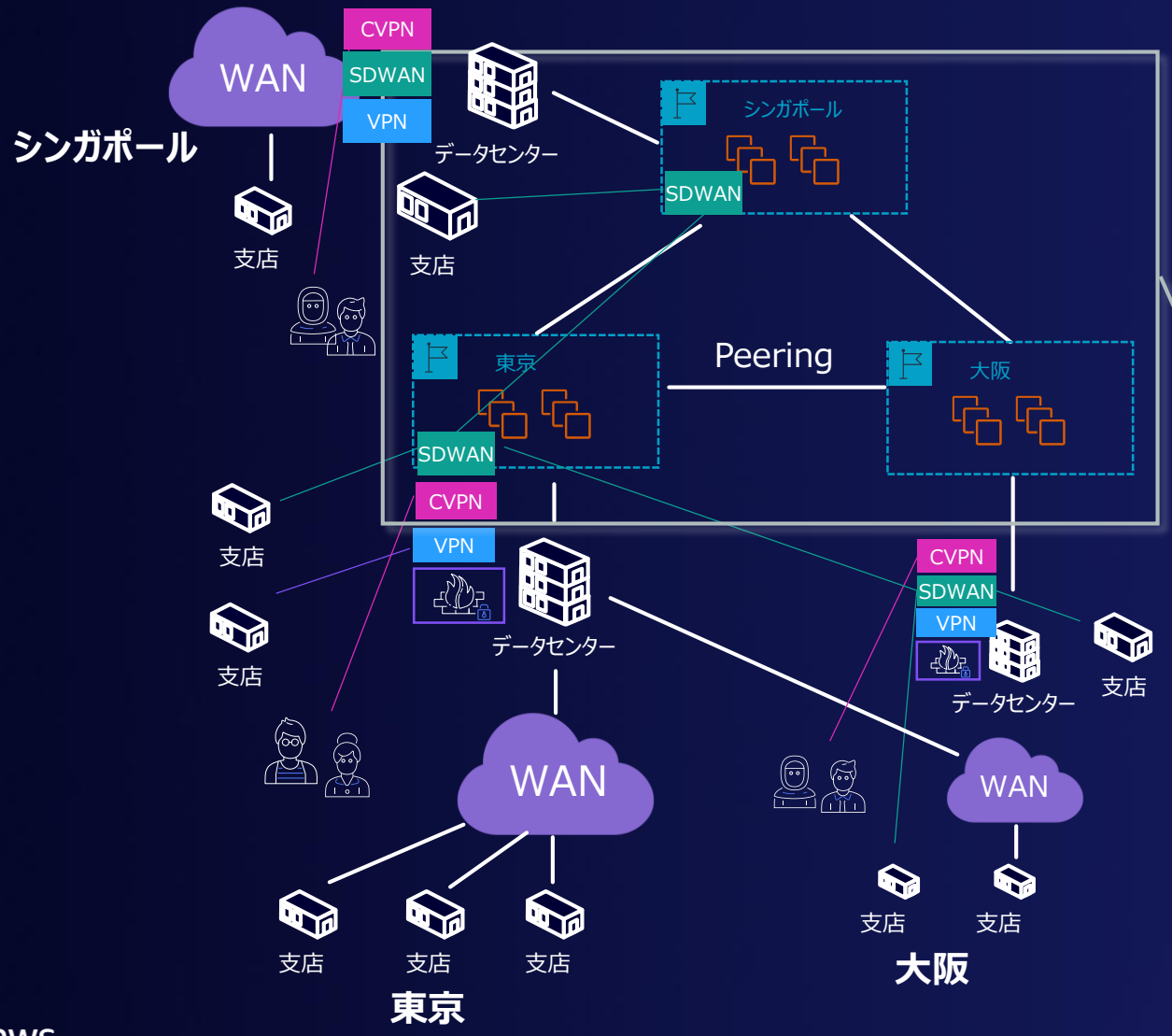
- クラウド接続
  (Direct Connect, VPN SD-WANなど)

追加されるトラフィックフロー

- オンプレミス拠点⇔クラウド
- リモートユーザ⇔クラウド
- クラウドリージョン間の通信
  ⇒SD-WANなどの拠点間通信はクラウド内のバックボーンを通過する場合もある。

Transit Gatewayの詳細に関しましてはこちら

エンタープライズWAN（クラウド接続追加）



追加される接続形態

- クラウド接続、SD-WAN

追加されるトラフィックフロー

- オンプレミス拠点⇔クラウド
- リモートユーザ⇔クラウド
- クラウドリージョン間の通信
  ⇒SD-WANなどの拠点間通信もクラウド内のバックボーンを通過する場合もある。

課題（将来）

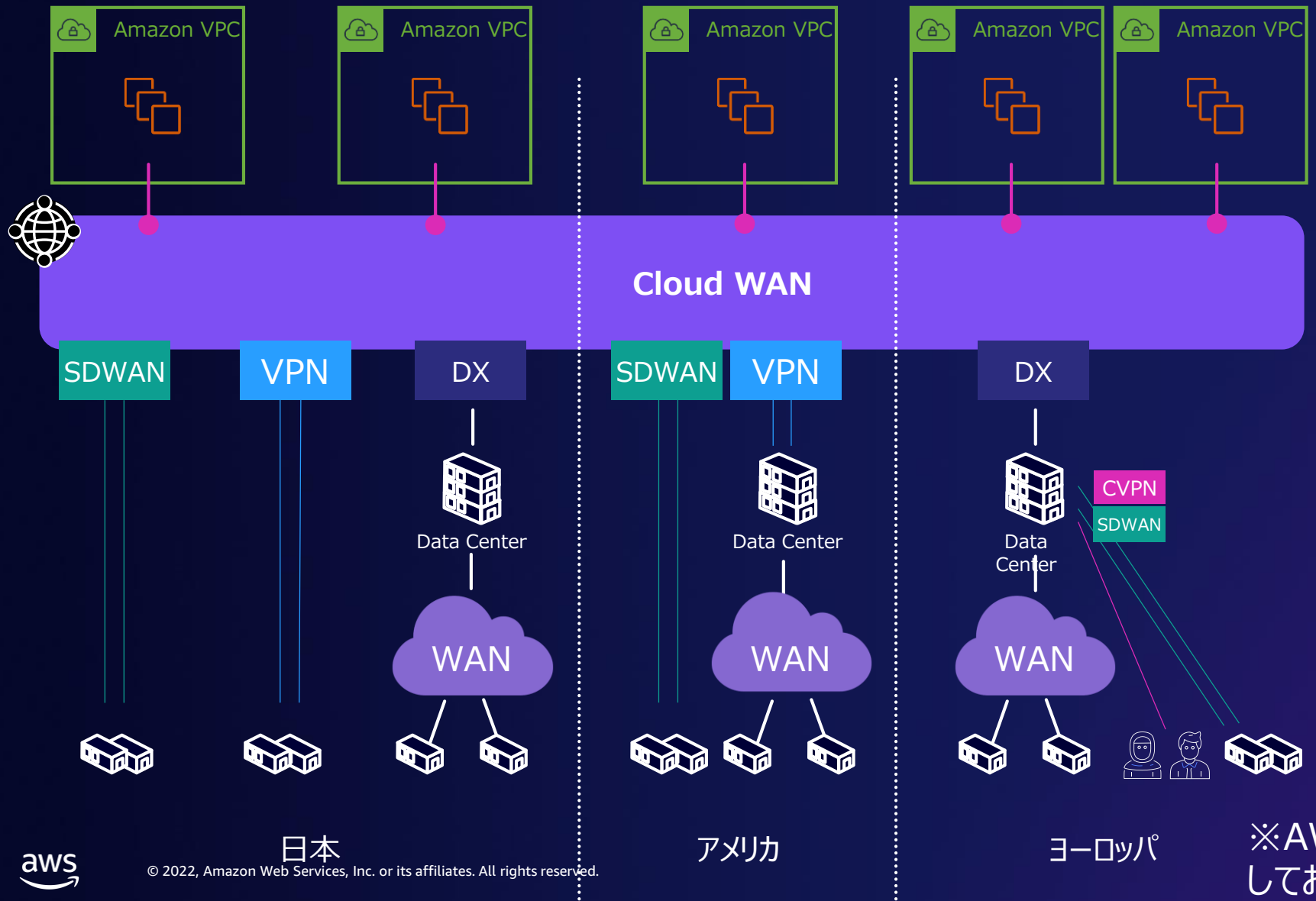
- グローバルネットワークの要件変更対応の迅速化及びポリシー管理
- 新たに国内外の拠点追加する際のリードタイムをより迅速化

Cloud WAN(Public Preview)

Cloud WAN概要

- AWS Cloud WANはグローバルに展開されているオンプレミス拠点間や、AWSクラウドへのネットワーク接続性を迅速に提供し、その間をグローバルにルーティングさせる事が可能です。
- グローバルネットワークの全体のポリシーを事前に作成しておく事により、新たな拠点やVPCの追加など、日常的なネットワーク管理タスクを自動化できます。
- グローバルネットワーク全体を簡単にセグメント化する事が可能です。例えば、機密性の高いアプリケーションのネットワークと一般的なネットワークトラフィックを分離する事ができます。
- Cloud WANを使用する事により、グローバルネットワーク全体を一つのダッシュボードで表示、メトリック監視が可能です。またアクセスポリシーやルーティング制御も中央より一元管理できます。グローバルネットワークの運用、管理の負担を軽減します。

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

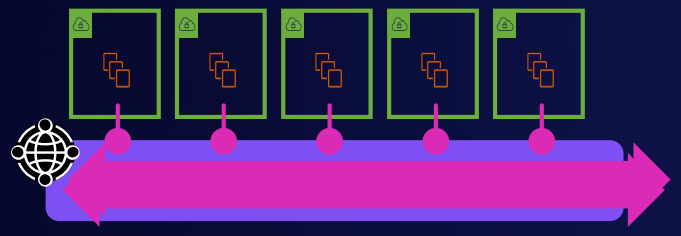
ルーティング情報
ネットワークポリシー
日常業務の自動化

アタッチメント

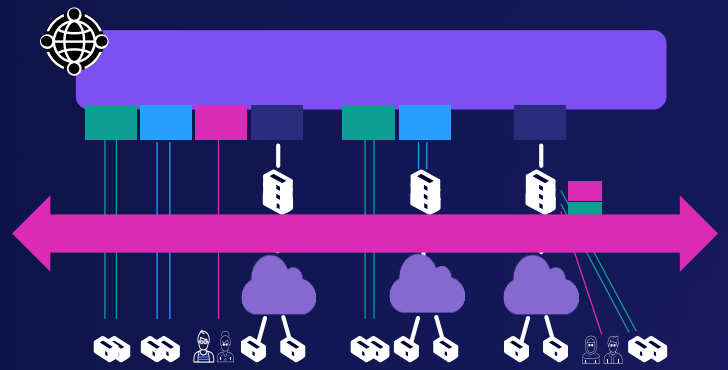
VPCs
VPNs
SD-WAN(TGW Connect)

※AWS Direct Connectは現在サポートしておりません。

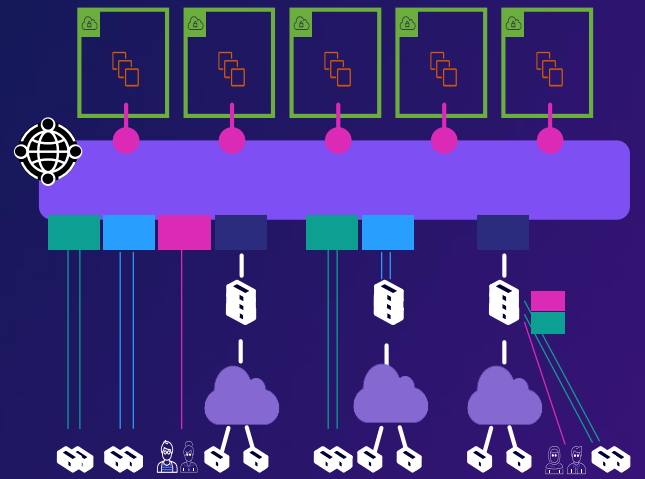
Cloud WAN ユースケース



VPC間通信

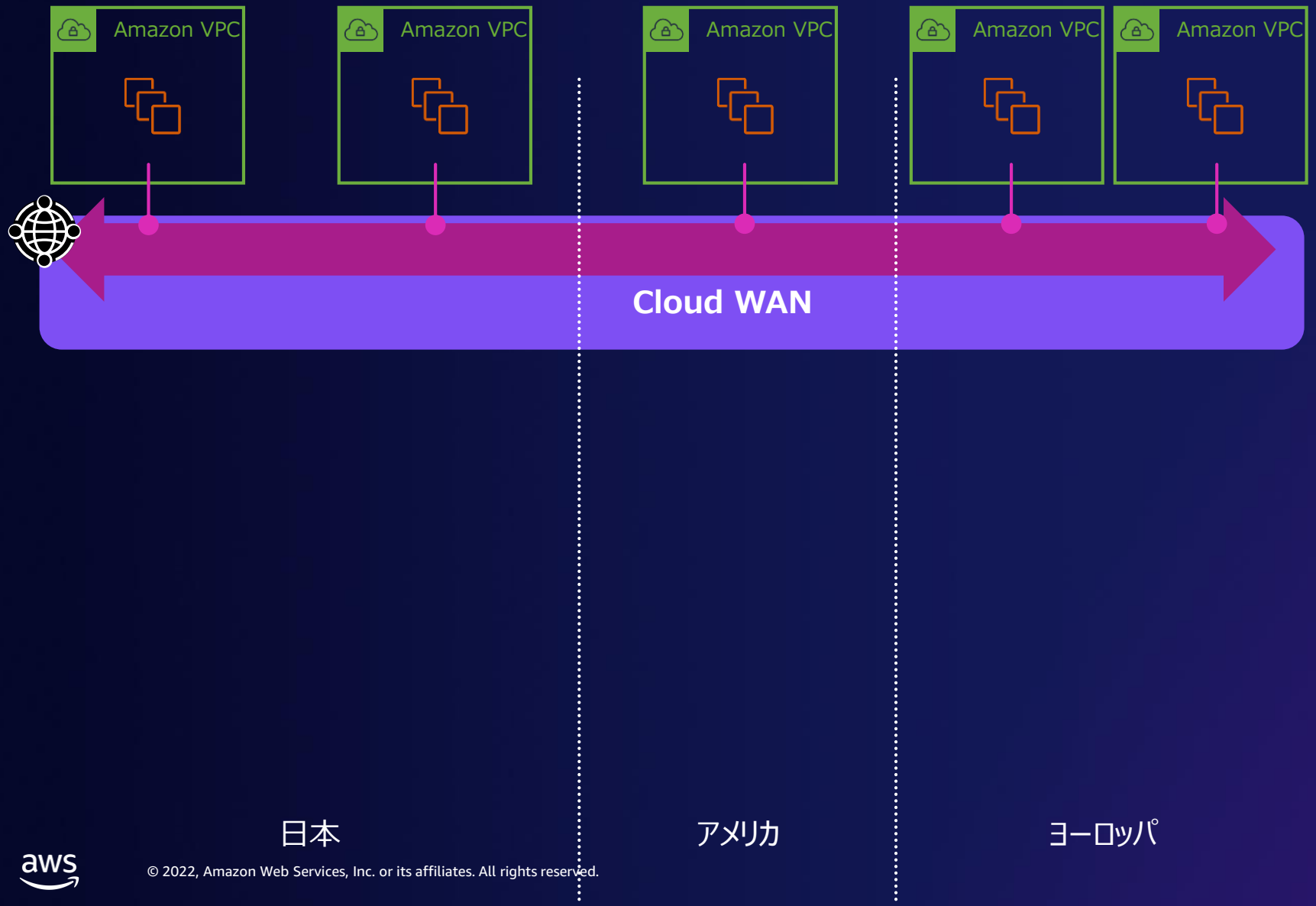


WAN接続



ハイブリッド構成

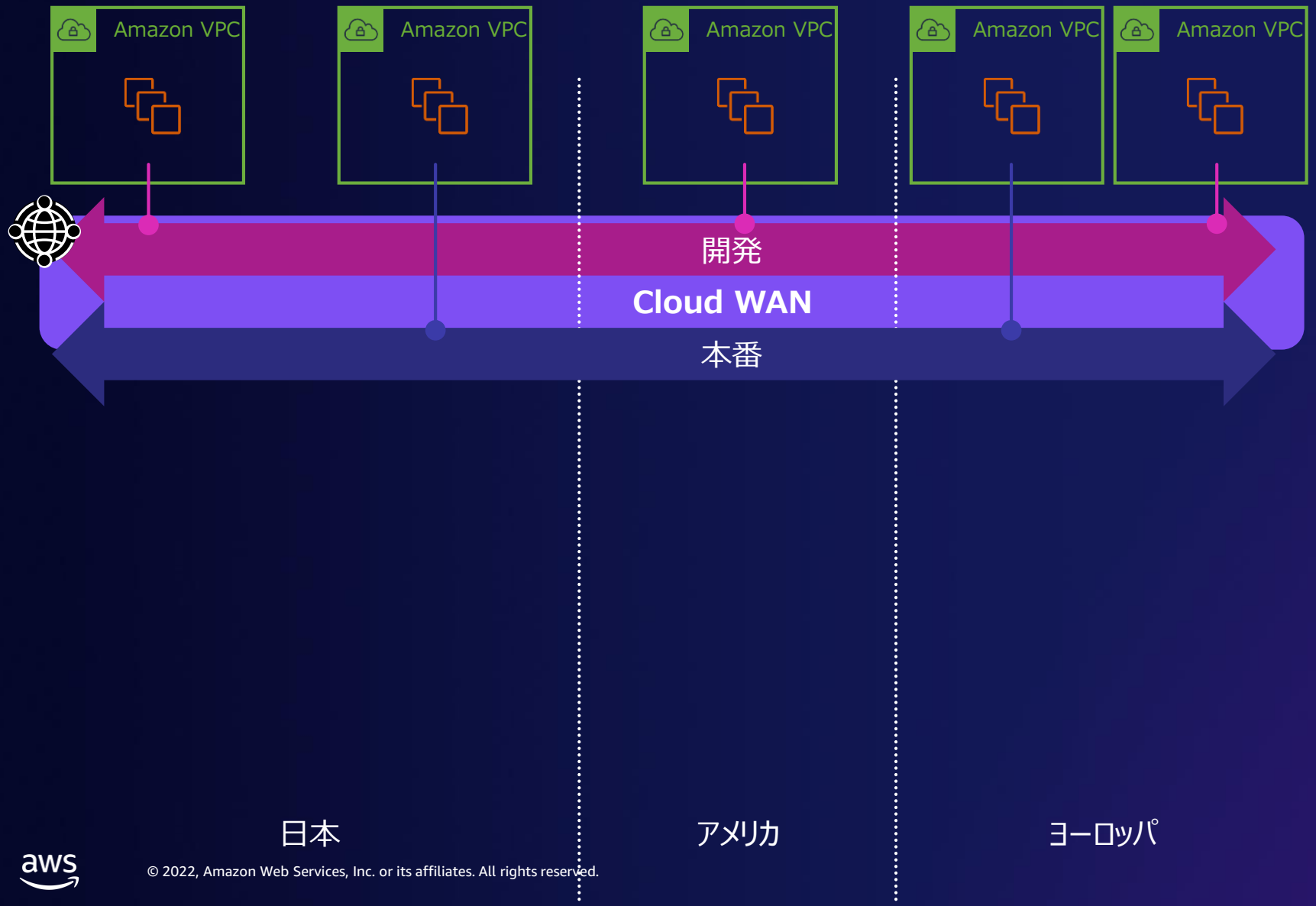
VPC間接続例



ユースケース

VPC間をグローバルなフラットネットワークで接続しルーティングを行う。リージョンを後から追加する事も可能。

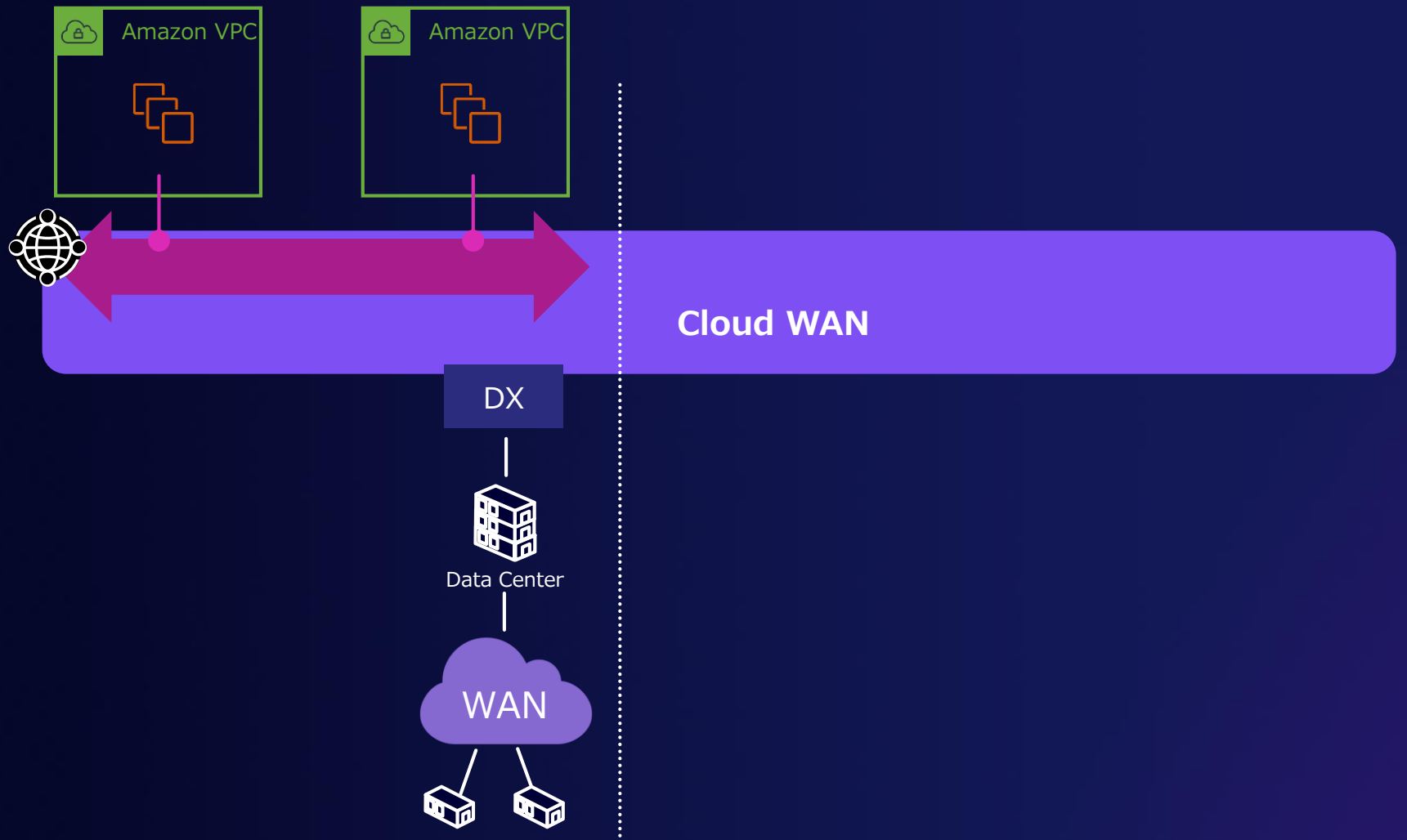
VPC間接続例



ユースケース

VPC間をグローバルなフラットネットワークで接続し、かつネットワークをセグメンテーションしルーティングを分ける。

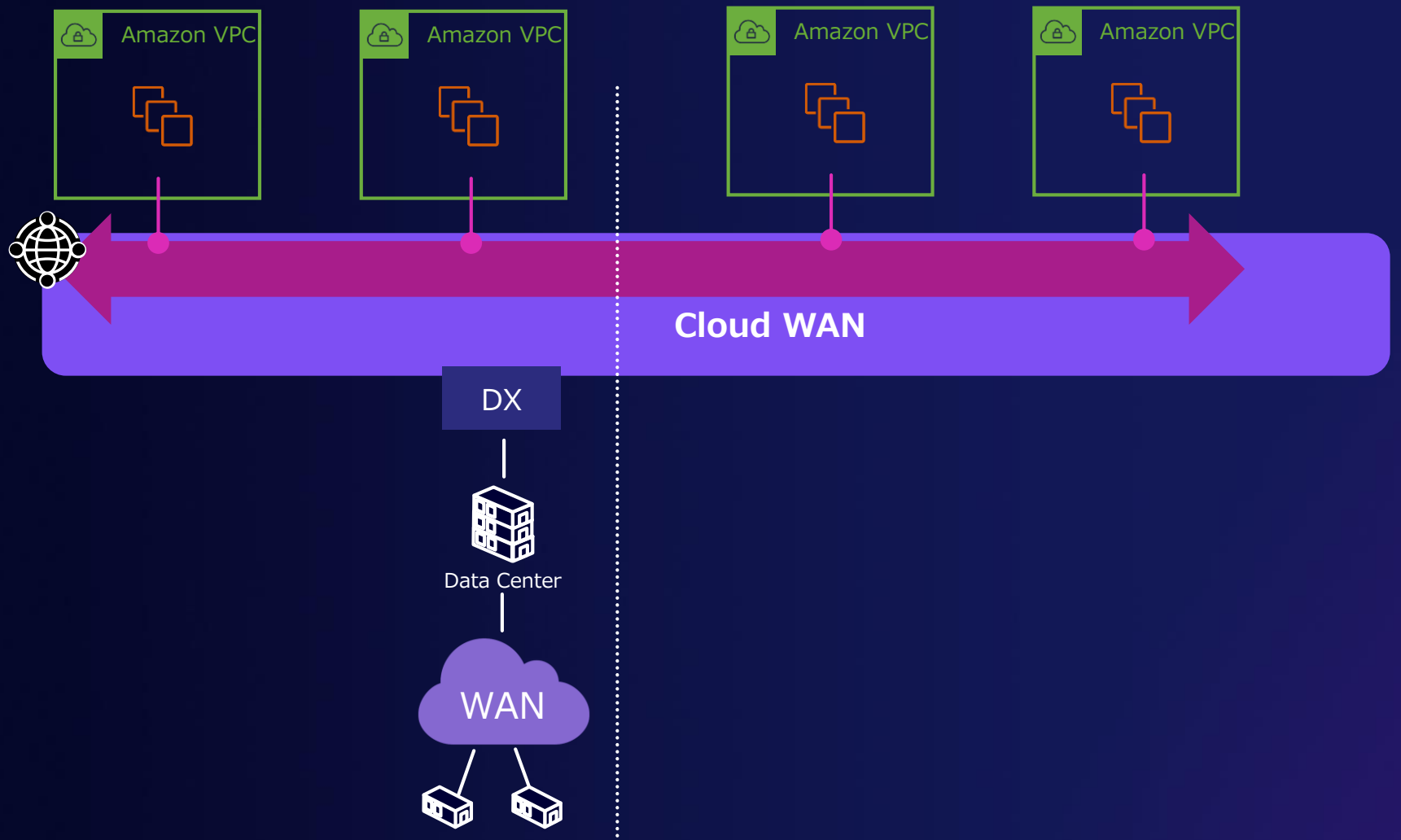
リージョンの追加例（DR対策）



Use Cases

DR対策

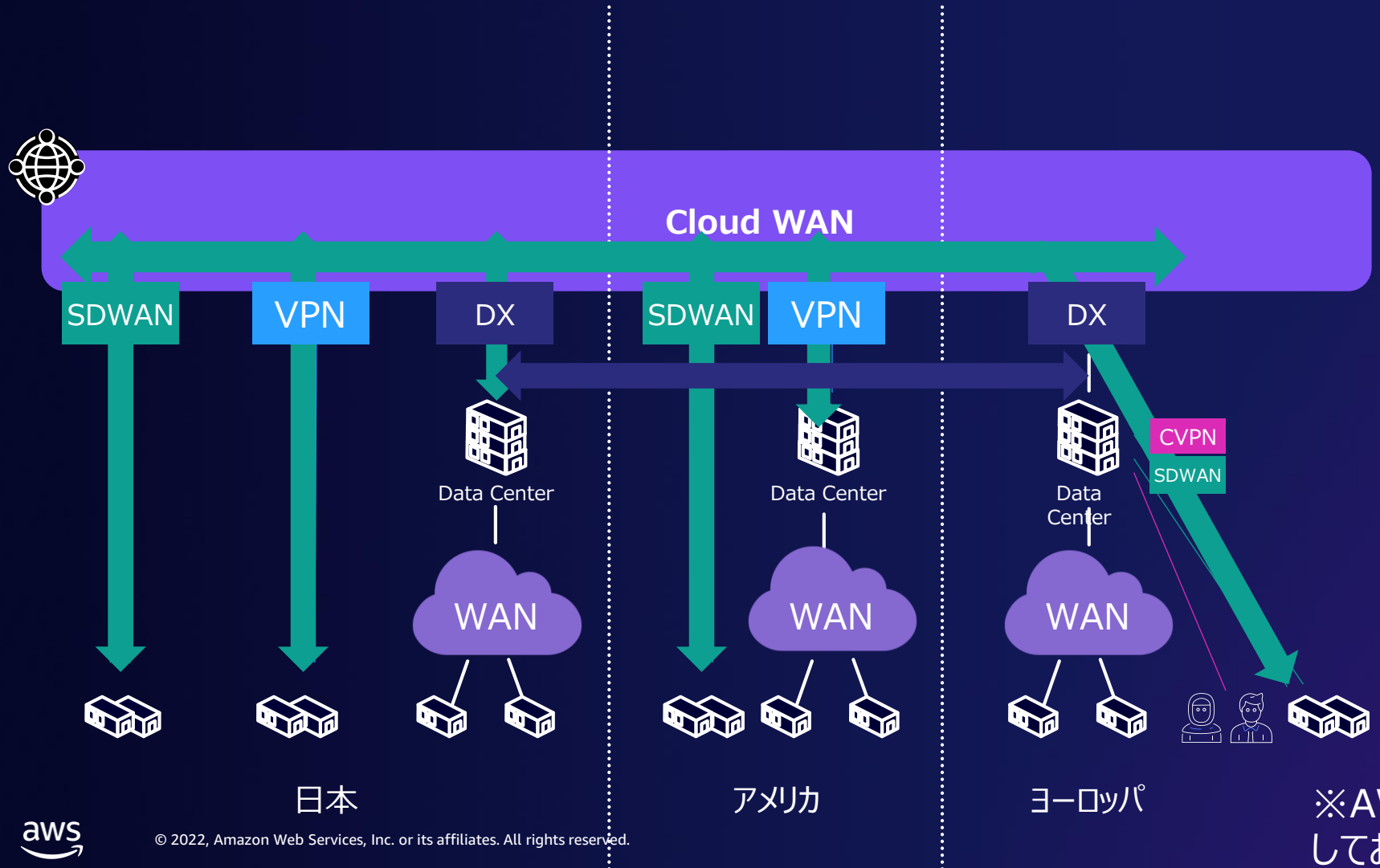
リージョンの追加例（DR対策）



Use Cases

DR対策

WAN接続例

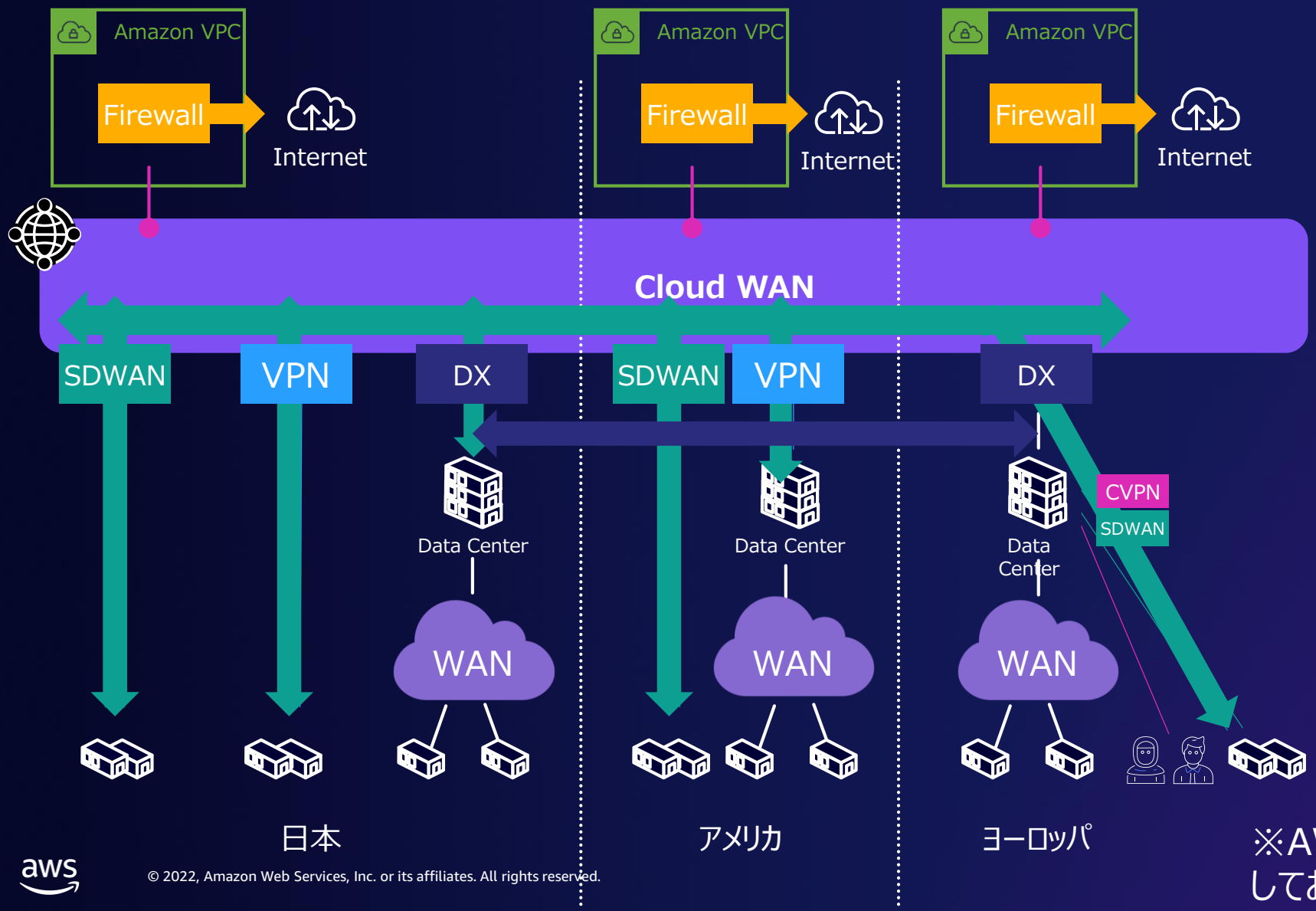


ユースケース

各オンプレミス拠点間をグローバルなフラットネットワークで接続しルーティング行う。
SiteLinkとの併用も可能。

※AWS Direct Connectは現在サポートしておりません。

WAN接続例



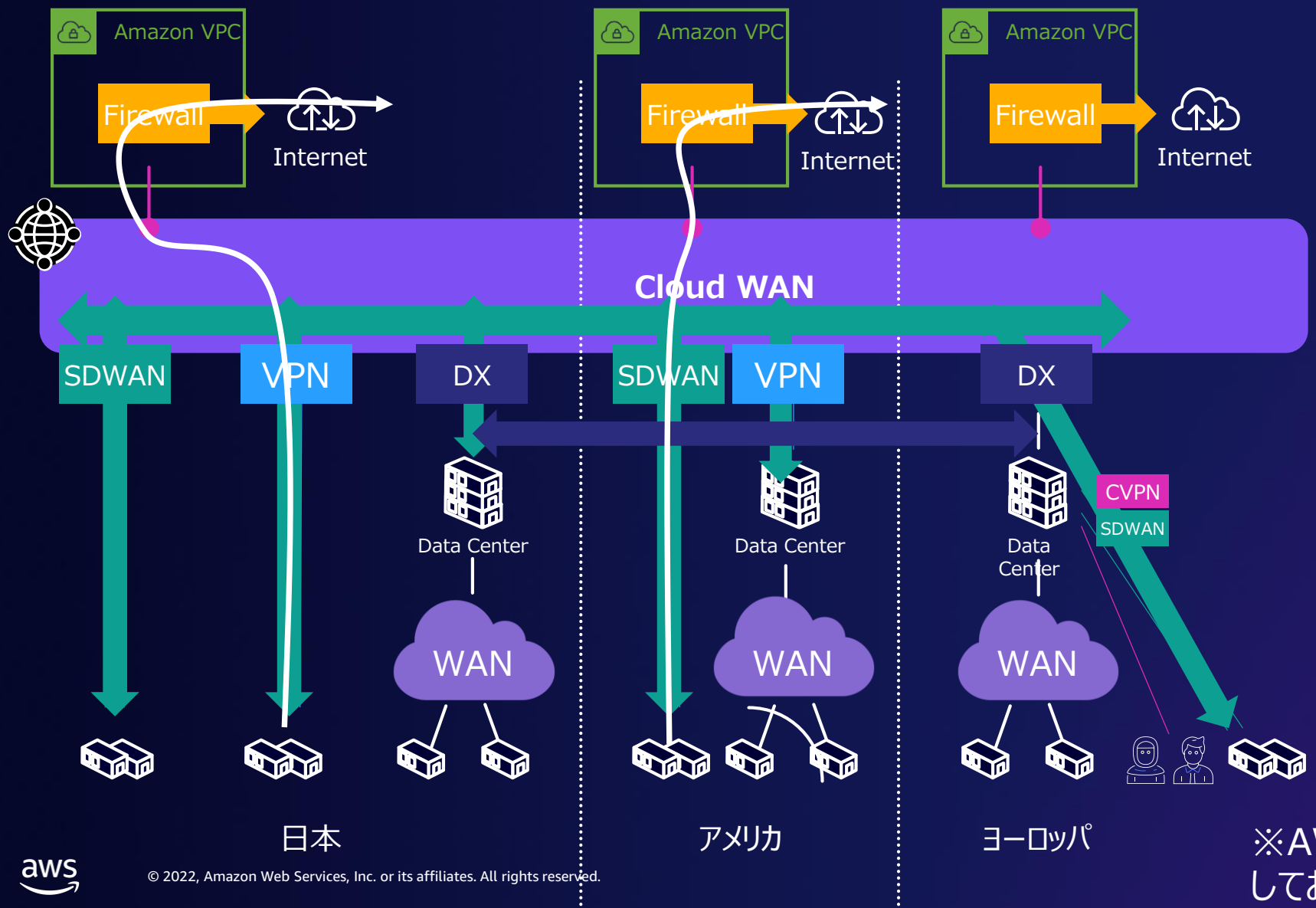
ユースケース

各オンプレミス拠点間をグローバルなフラットネットワークで接続しルーティング行う。
SiteLinkとの併用も可能。

インターネットの出口は、AWSの各リージョンごとに個別設定する事も可能。

※AWS Direct Connectは現在サポートしておりません。

WAN接続例



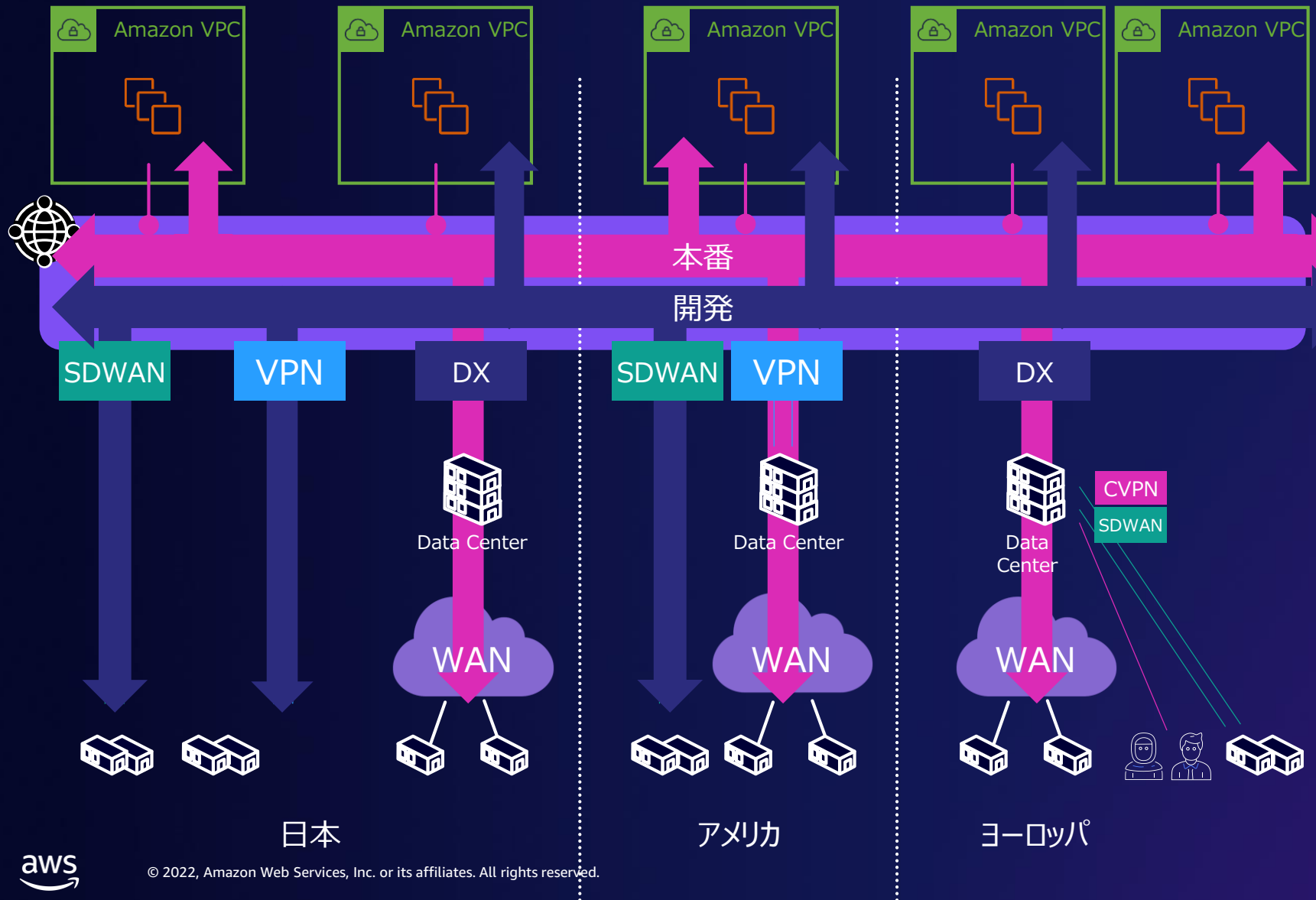
ユースケース

各オンプレミス拠点間をグローバルなフラットネットワークで接続しルーティング行う。
SiteLinkとの併用も可能。

インターネットの出口は、AWSの各リージョンごとに個別設定する事も可能。

※AWS Direct Connectは現在サポートしておりません。

ハイブリッド構成例



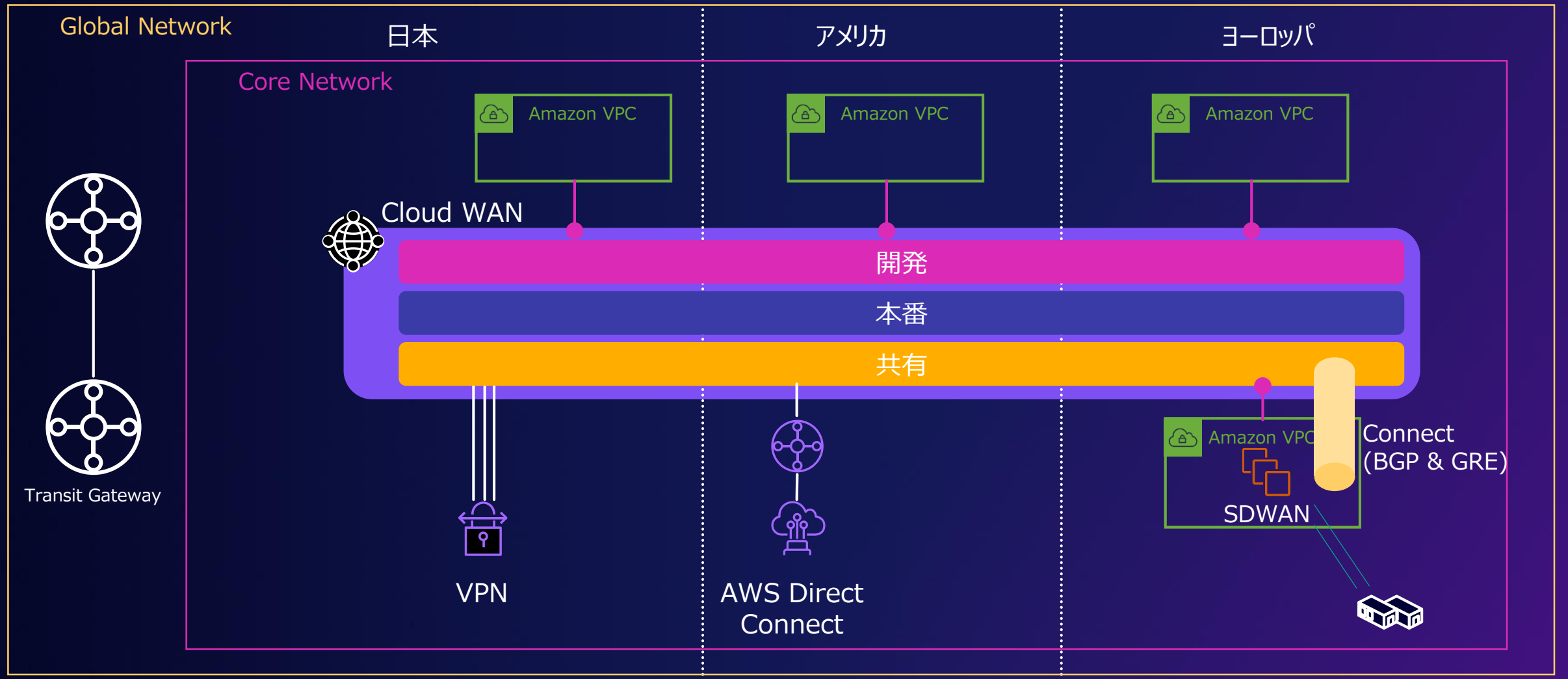
ユースケース

グローバル展開。

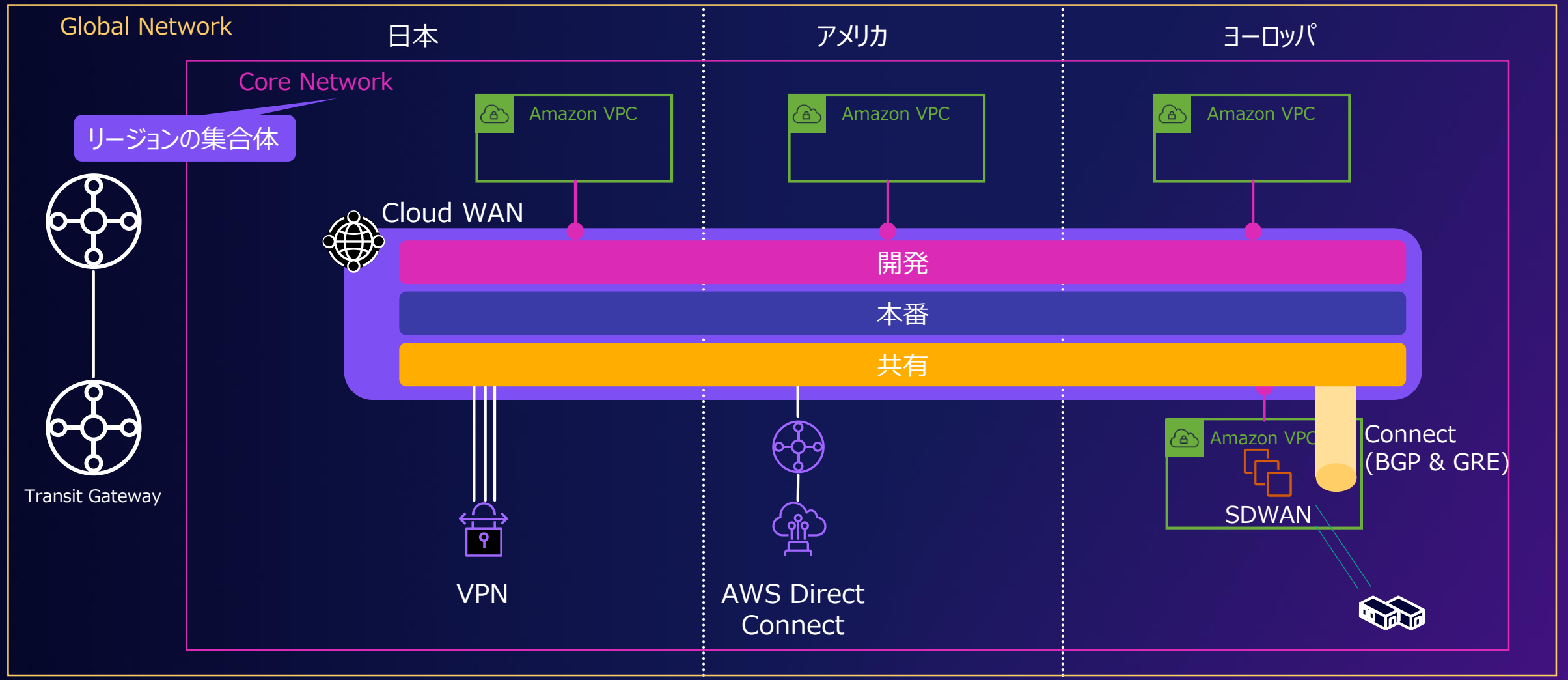
グローバルネットワークをEnd-to-Endでセグメント化する事が可能。

Cloud WAN コンポーネント

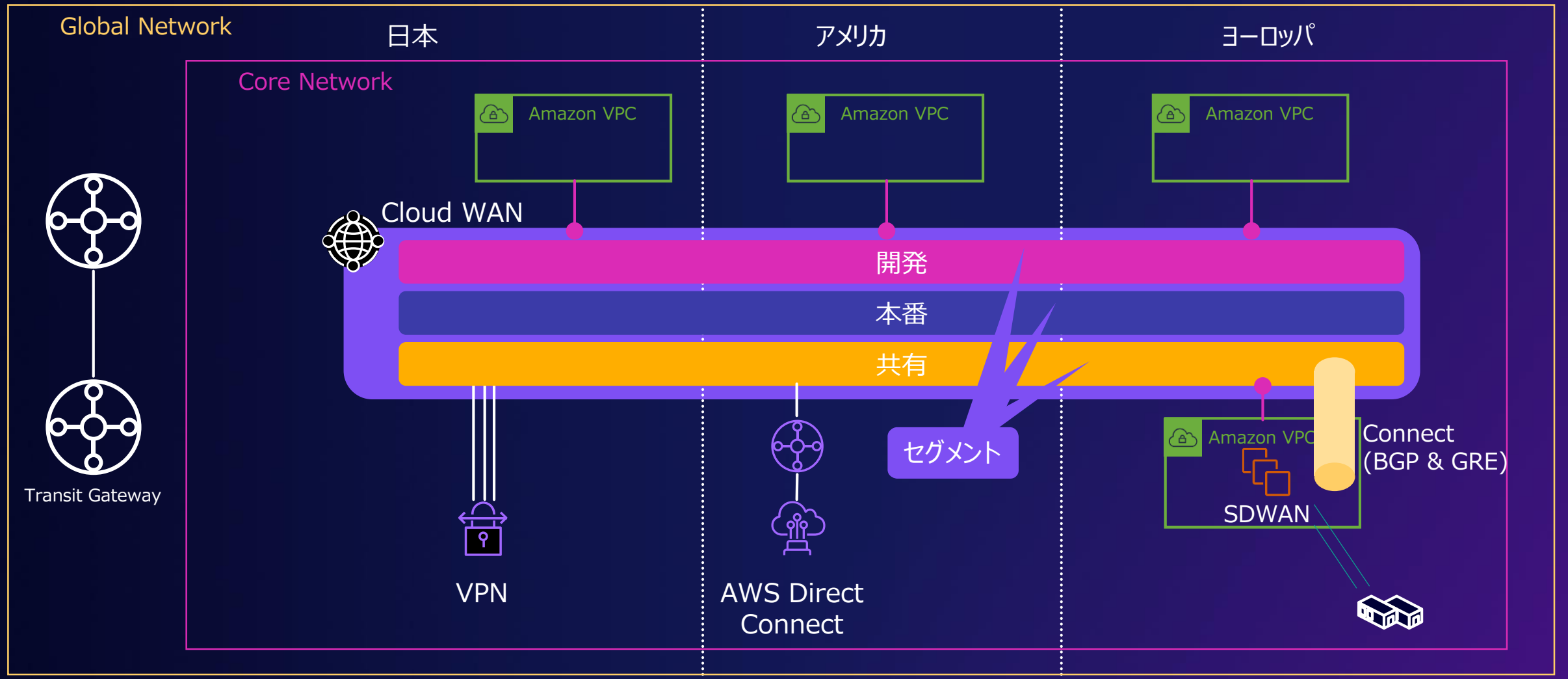
Cloud WANコンポーネント



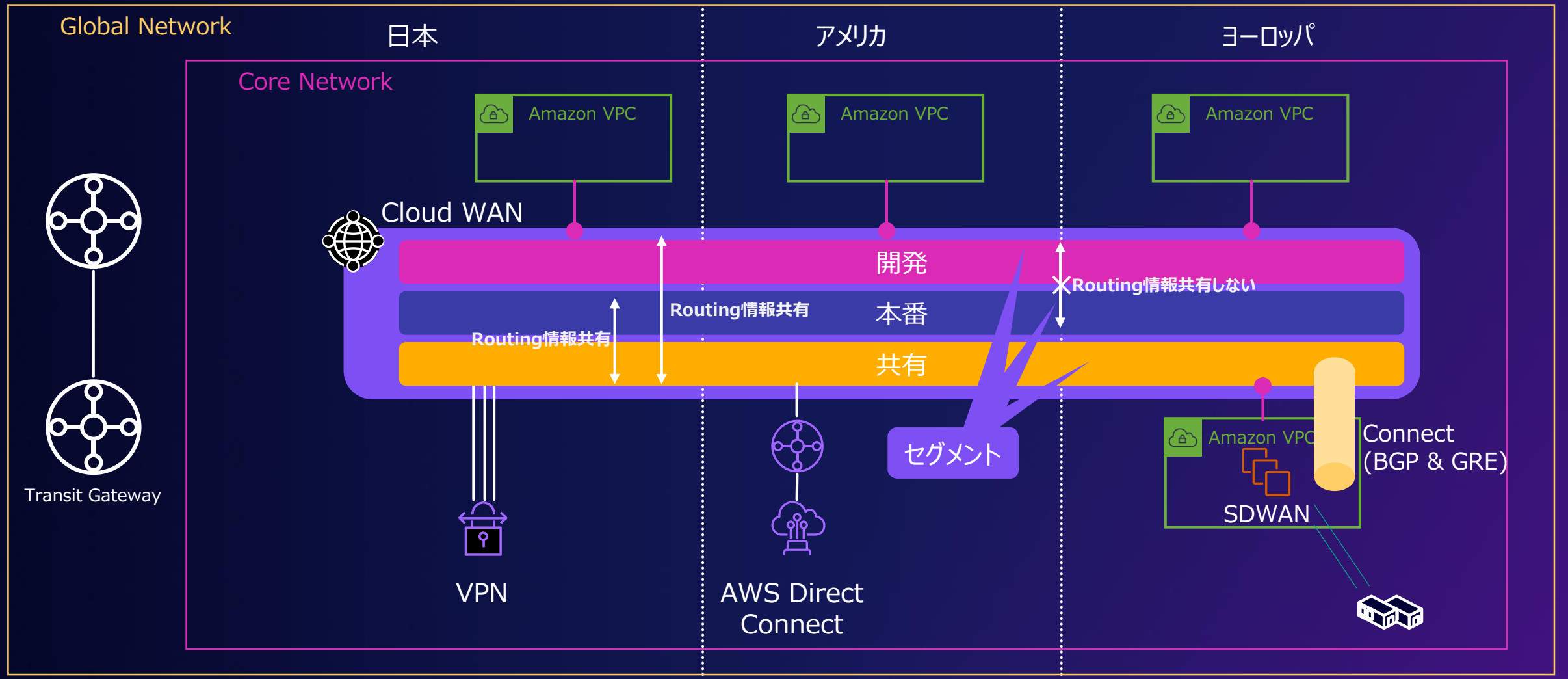
Cloud WANコンポーネント：Core Network



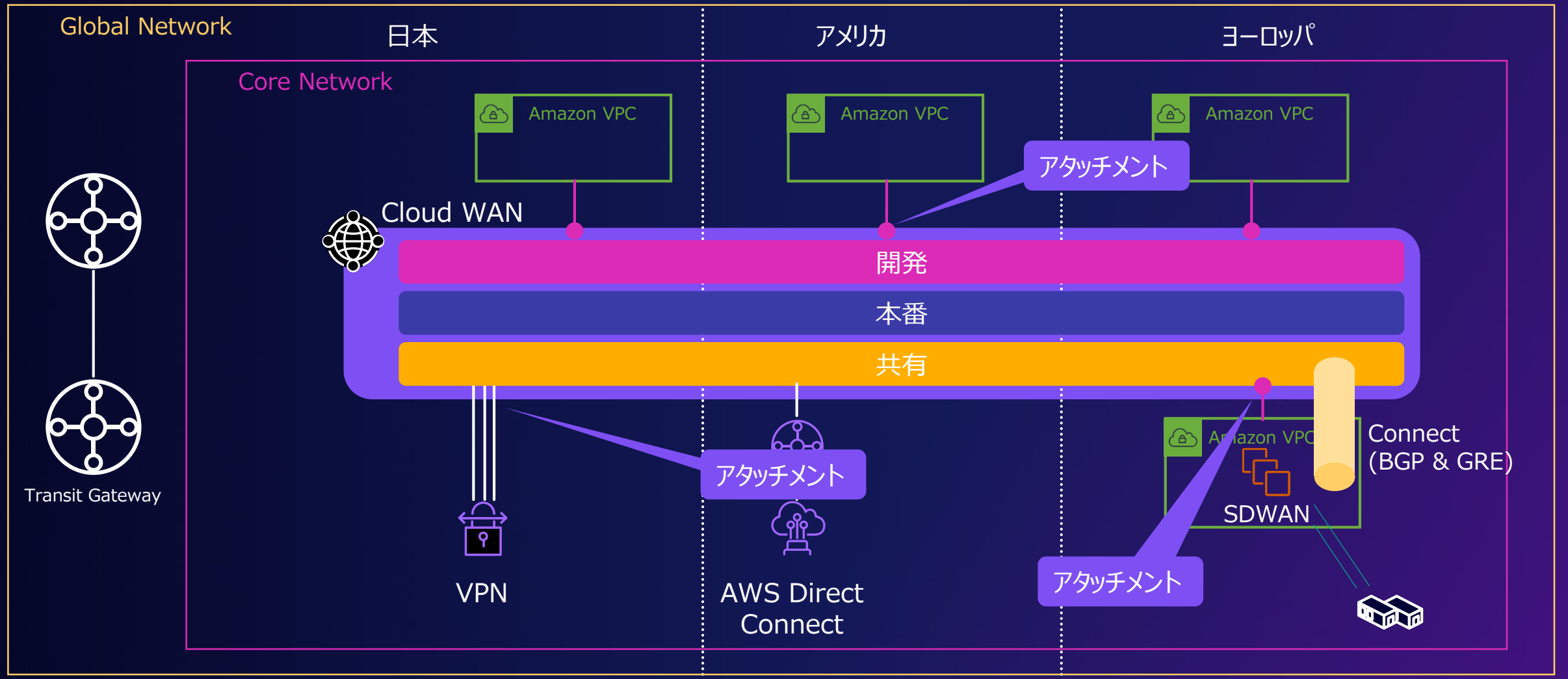
Cloud WANコンポーネント：セグメント



Cloud WANコンポーネント：セグメント



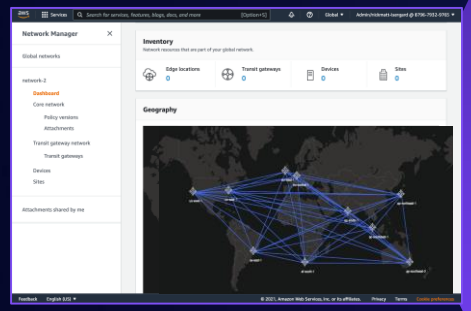
Cloud WANコンポーネント：アタッチメント



Cloud WANコンポーネント：Core Network Policy

Core Networkのネットワーク構成を定義するポリシー

Core Network Policy(CNP)



AWS Network Manager

Global Network

日本

アメリカ

ヨーロッパ

Core Network

BGP & Monitoring

Core Network Edges

開発

本番

共有

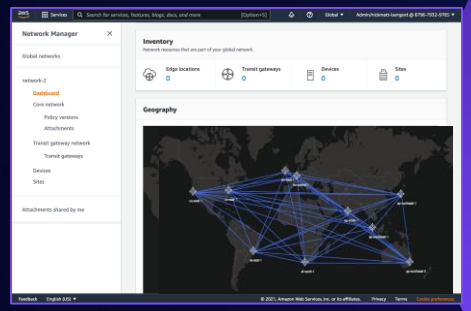
VPN

AWS Direct Connect

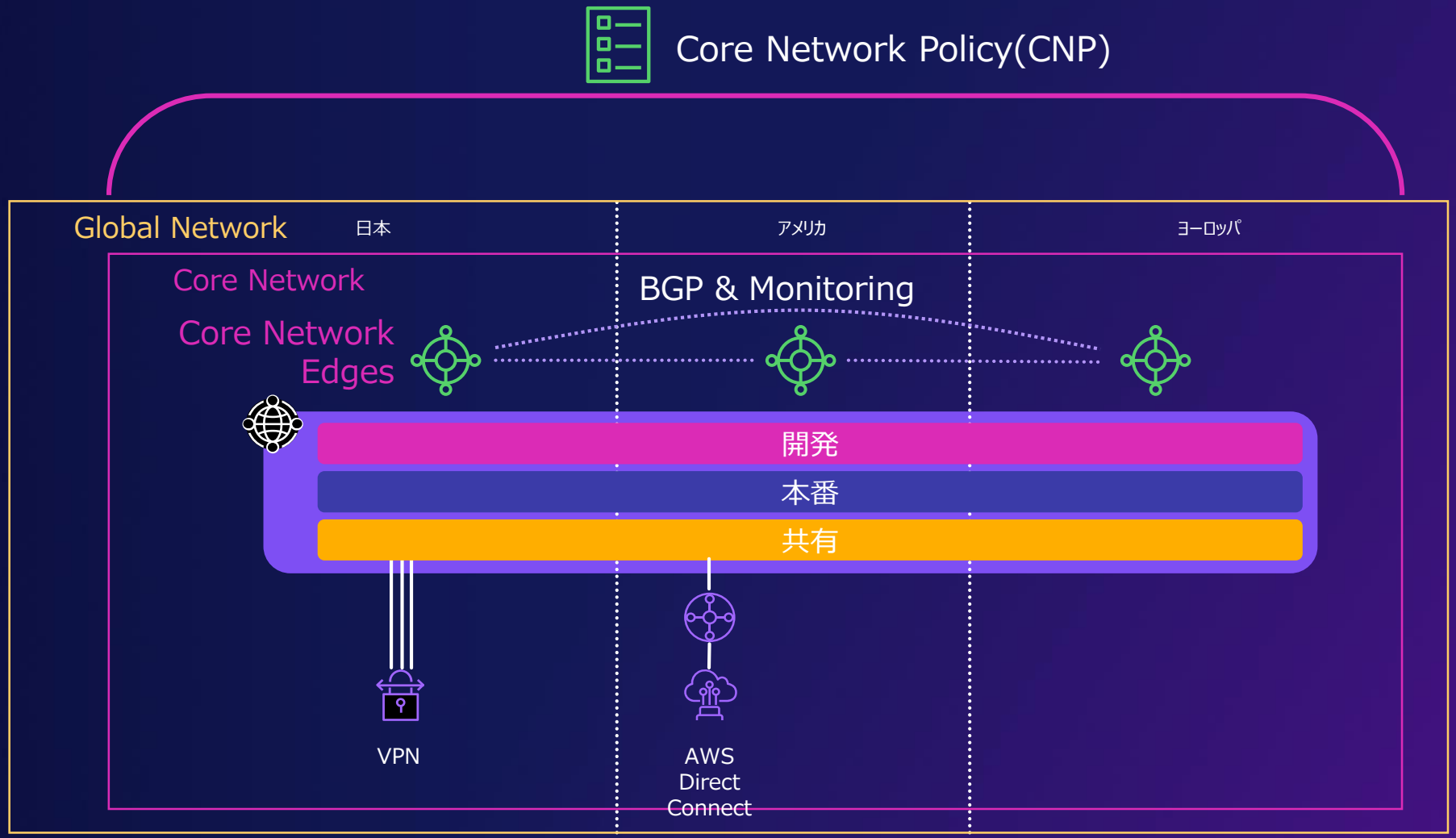
Cloud WANコンポーネント：ダッシュボード

Core Network全体を一元管理するダッシュボード

ダッシュボード
- ポリシーの設定
- トポロジー情報
- ルーティング情報
- イベント一覧

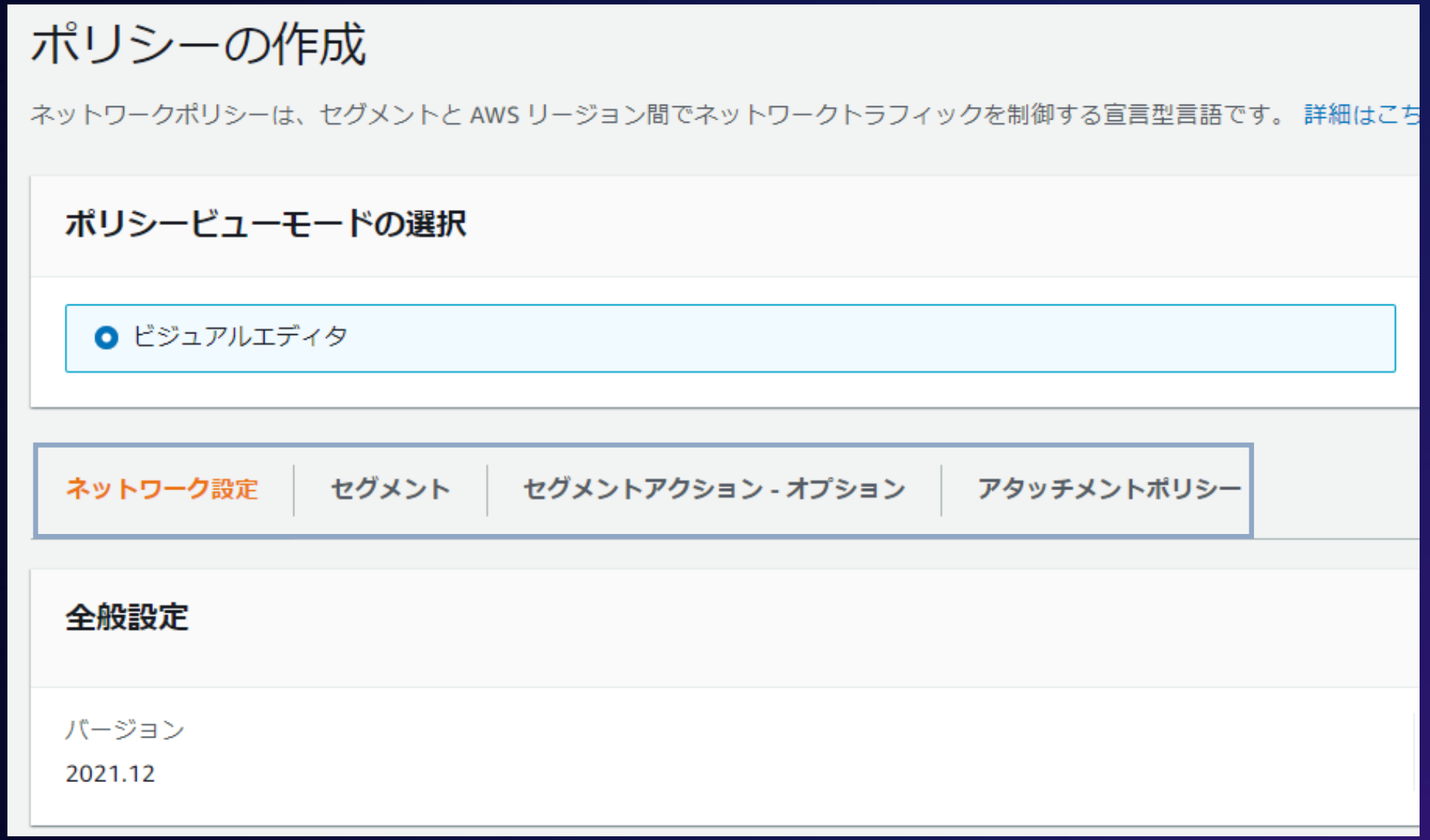


AWS Network Manager



Cloud WAN サンプル画面

Core Network Policy



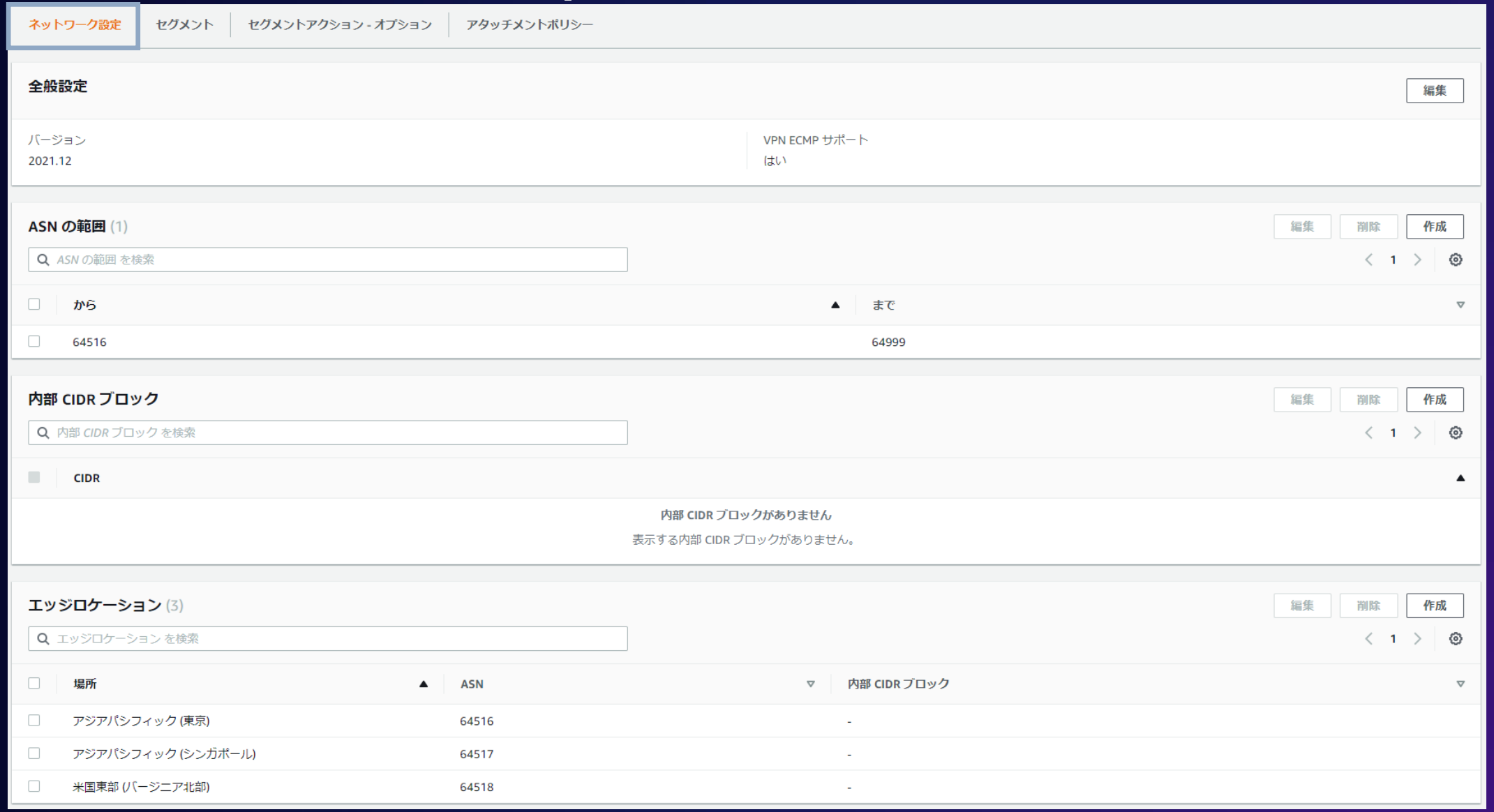
ネットワーク設定
リージョン, AS番号

セグメント
セグメント作成
セグメント内のポリシー

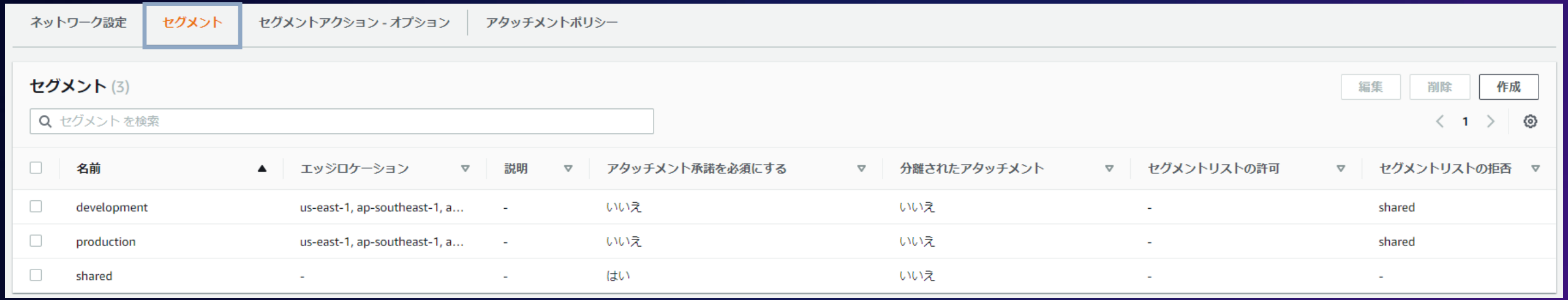
セグメントアクション・オプション
セグメント間のポリシー
スタティックルート

アタッチメントポリシー
アタッチメンとセグメントの紐づけ

Core Network Policy：ネットワーク設定



Core Network Policy：セグメント



Core Network Policy：セグメントアクション・オプション

ネットワーク設定 | セグメント | セグメントアクション - オプション | アタッチメントポリシー

共有 (2)

編集 | 削除 | 作成

共有 を検索

1

セグメント	セグメントと共有済み	セグメントを除いて共有済み
development	shared	-
production	shared	-

ルート (5)

編集 | 削除 | 作成

ルート を検索

1

セグメント	送信先 CIDR ブロック	送信先
development	0.0.0.0/0	attachment-029cd7a8cd92742e0, attachment-02dc7a51660a5b8...
development	172.16.1.0/24, 172.17.1.0/24, 172.18.1.0/24	ブラックホール
production	0.0.0.0/0	attachment-029cd7a8cd92742e0, attachment-02dc7a51660a5b8...
production	172.16.2.0/24, 172.17.2.0/24, 172.18.2.0/24	ブラックホール
shared	0.0.0.0/0	attachment-029cd7a8cd92742e0, attachment-02dc7a51660a5b8...

Core Network Policy：アタッチメントポリシー

Network Manager：ジオグラフィー

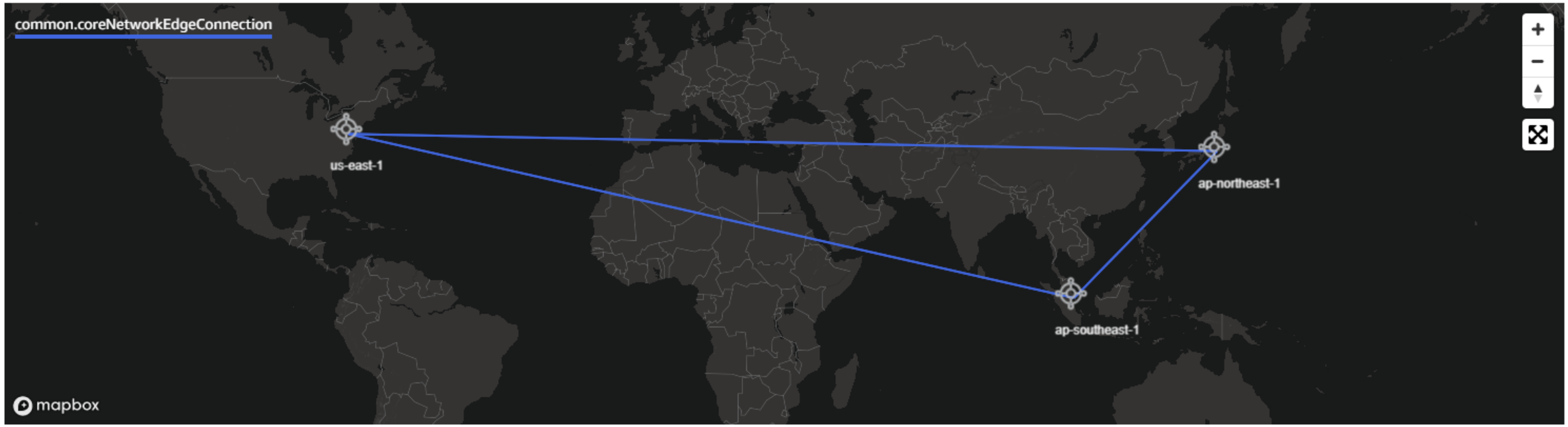
概要 | 詳細 | 共有 | トポロジグラフ | トポロジツリー | セグメント | ルート | イベント | モニタリング

インベントリ

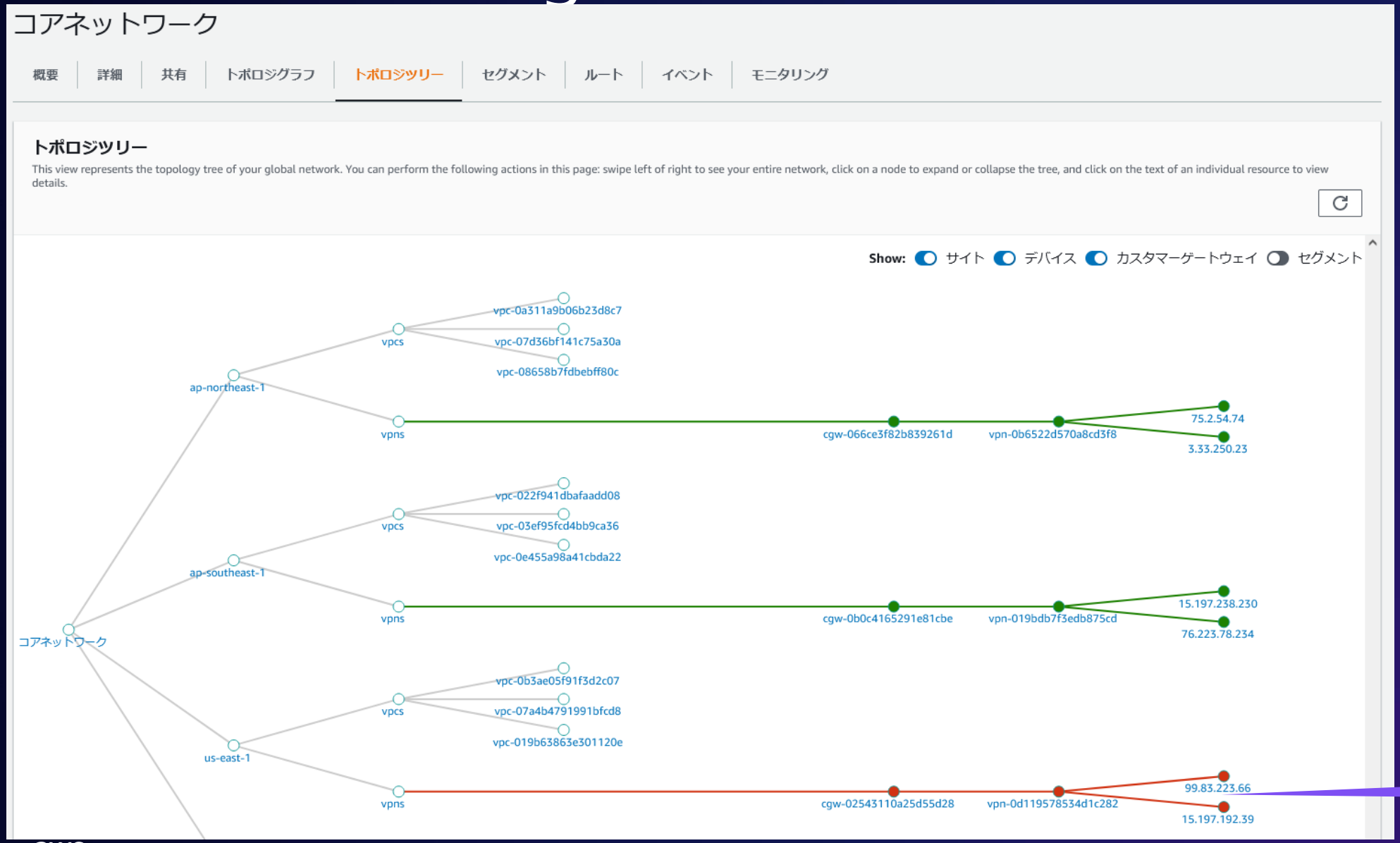
コアネットワークの一部であるネットワークリソース。

エッジロケーション	セグメント	デバイス	サイト
3	3	0	0

Geography



Network Manager：トポロジーツリー



トポロジーツリー情報

トポロジーの階層

VPNの状態

VPNダウン

Network Manager：セグメント情報

Logical

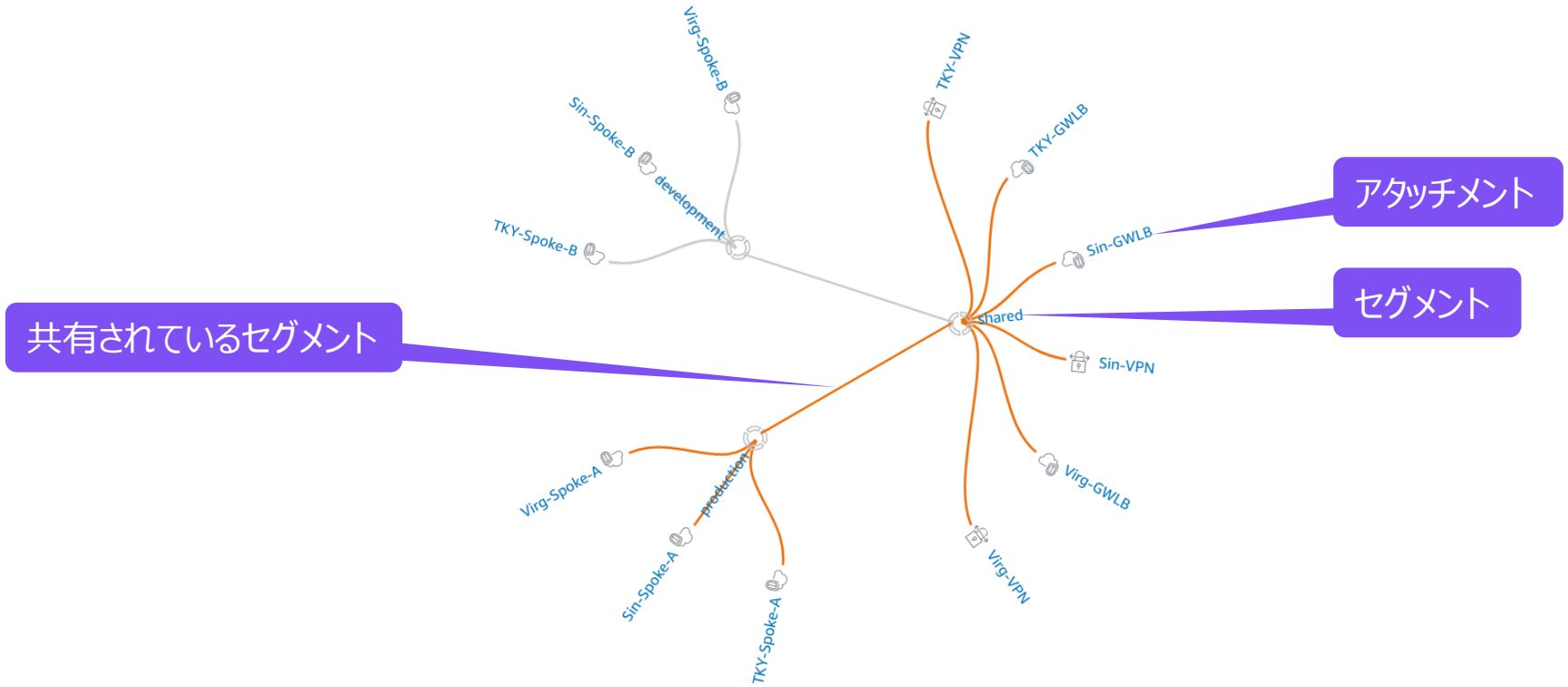
This view represents the logical association of segment to attachment mapping on your core network. You can perform the following actions in this page: click on a segment icon to expand or collapse the attachments view, and click on the text of an individual resource to view details.

Filter by:

送信元セグメント	送信元アタッチメント	送信先セグメント	送信先アタッチメント	
shared	アタッチメントの選択	production	アタッチメントの選択	クリア

VPC　接続　セグメント　VPN

表示する: アタッチメント　関連付けられていないアタッチメントを表示



Network Manager ：セグメント情報

Logical

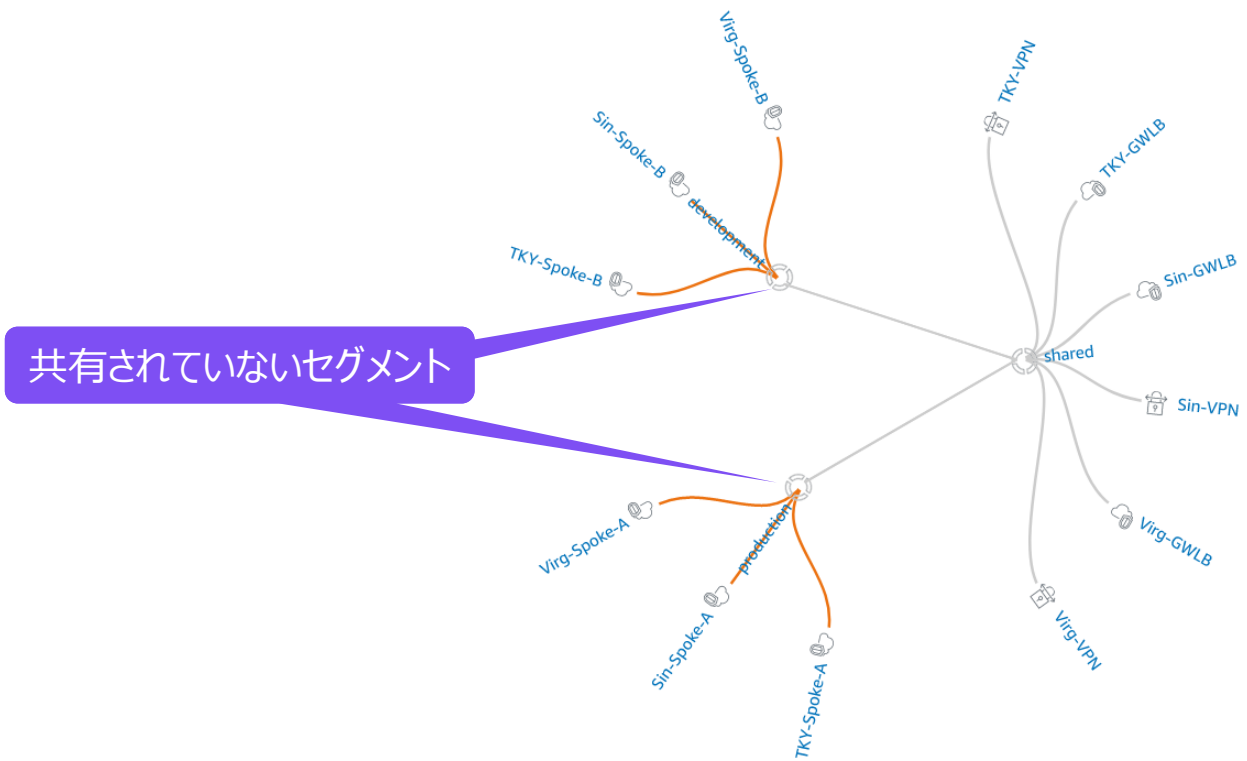
This view represents the logical association of segment to attachment mapping on your core network. You can perform the following actions in this page: click on a segment icon to expand or collapse the attachments view, and click on the text of an individual resource to view details.

Filter by:

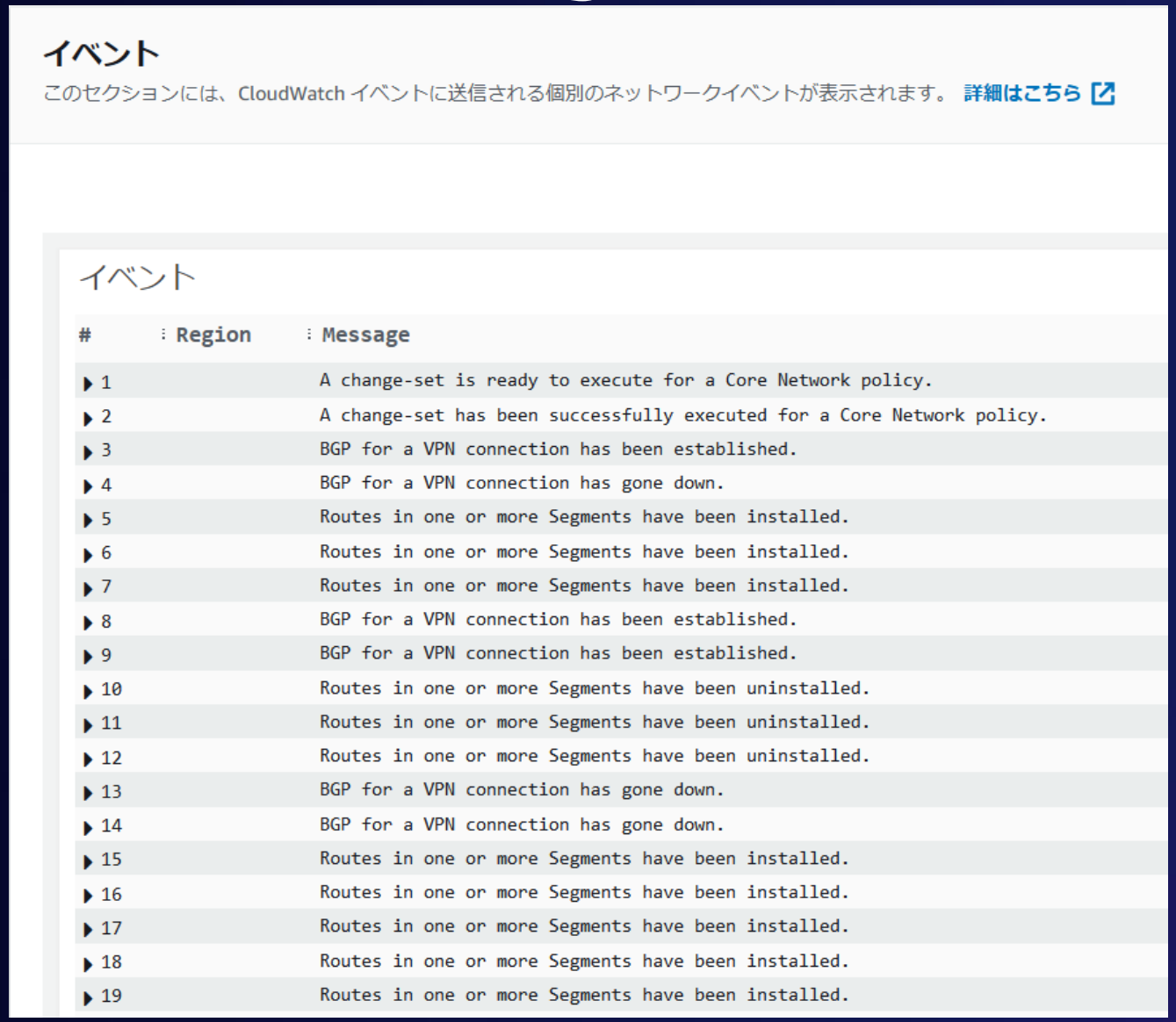
送信元セグメント	送信元アタッチメント	送信先セグメント	送信先アタッチメント	
production	アタッチメントの選択	development	アタッチメントの選択	クリア

VPC　接続　セグメント　VPN

表示する: アタッチメント　関連付けられていないアタッチメントを表示



Network Manager：イベント情報



イベント

このセクションには、CloudWatch イベントに送信される個別のネットワークイベントが表示されます。 詳細はこちら

イベント

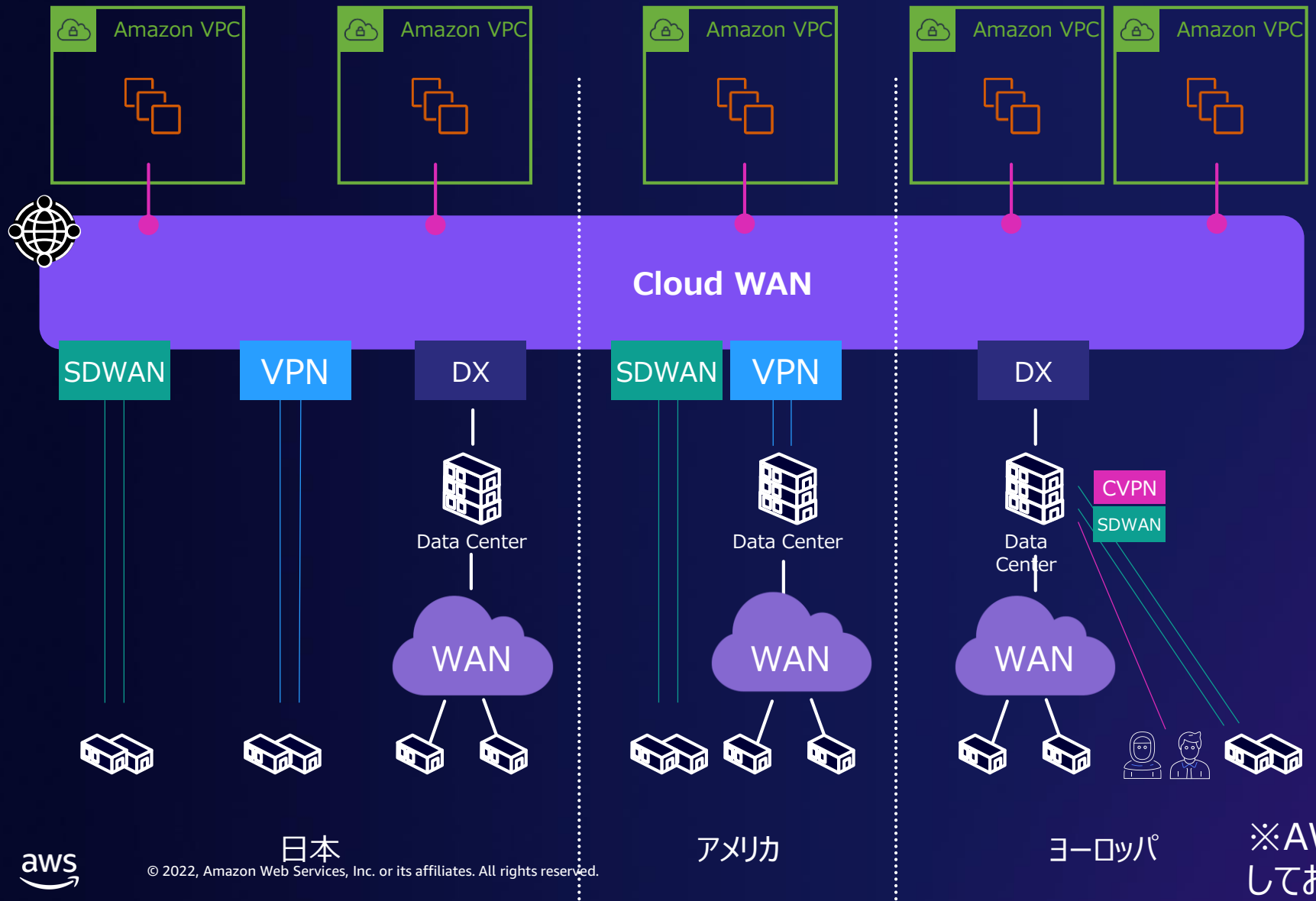
#	Region	Message
1		A change-set is ready to execute for a Core Network policy.
2		A change-set has been successfully executed for a Core Network policy.
3		BGP for a VPN connection has been established.
4		BGP for a VPN connection has gone down.
5		Routes in one or more Segments have been installed.
6		Routes in one or more Segments have been installed.
7		Routes in one or more Segments have been installed.
8		BGP for a VPN connection has been established.
9		BGP for a VPN connection has been established.
10		Routes in one or more Segments have been uninstalled.
11		Routes in one or more Segments have been uninstalled.
12		Routes in one or more Segments have been uninstalled.
13		BGP for a VPN connection has gone down.
14		BGP for a VPN connection has gone down.
15		Routes in one or more Segments have been installed.
16		Routes in one or more Segments have been installed.
17		Routes in one or more Segments have been installed.
18		Routes in one or more Segments have been installed.
19		Routes in one or more Segments have been installed.

ネットワーク変更情報

- トポロジー変更
- ポリシー変更
- アタッチメント変更
- 経路変更
- BGPアップデート

など

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。

まとめ

まとめ

- AWS Direct Connect SiteLinkはDirect Connectを使用しているオンプレミス拠点間をAWSバックボーン網を介し、グローバルネットワークの接続性を迅速に提供します。機能を使用する場合はVIF のコンソール上で有効化するだけで利用可能です。

- AWS Cloud WANはグローバルに展開されているオンプレミス拠点間や、AWSクラウドへのネットワーク接続性を迅速に提供します。様々なアタッチメントタイプをサポートしており、その間をグローバルにルーティングする事が可能です。またグローバルネットワーク全体を一つのダッシュボードからポリシーの定義や監視でき、運用の負担を軽減します。

- お客様はAWSグローバルインフラストラクチャをオンプレミスネットワークの一部として利用する事により、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

Introducing AWS Cloud WAN (Preview) (英語ブログ)
Introducing AWS Direct Connect SiteLink (英語ブログ)
Simplify SD-WAN connectivity with AWS Transit Gateway Connect (英語ブログ)
AWS On Air demo (YouTube ビデオ)
AWS Direct Connect (Black Belt 日本語資料)
AWS Transit Gateway (Black Belt 日本語資料)

以下のAWS Summit Japan Onlineのセッションもご参照ください。
AWS-54：Amazon VPC ネットワーキングの基本構成・運用管理
AWS-56：より快適、より安全なアプリケーションを実現する AWS エッジネットワークサービス

Thank you!

藤井　拓

tafuj@amazon.co.jp