



AWS Cloud WAN概要

AWS Black Belt Online Seminar

藤井 拓

Solutions Architect Network Specialist
2022/11

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBIqY>

内容についての注意点

- 本資料では2022年11月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます

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ー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 Transit Gateway, AWS Gateway
Load Balancer, AWS Cloud WAN

本日持ち帰って頂きたい事

- Cloud WANの概要を理解する
- Cloud WANのユースケースを理解する
- Cloud WANの用語やコンポーネントを理解する

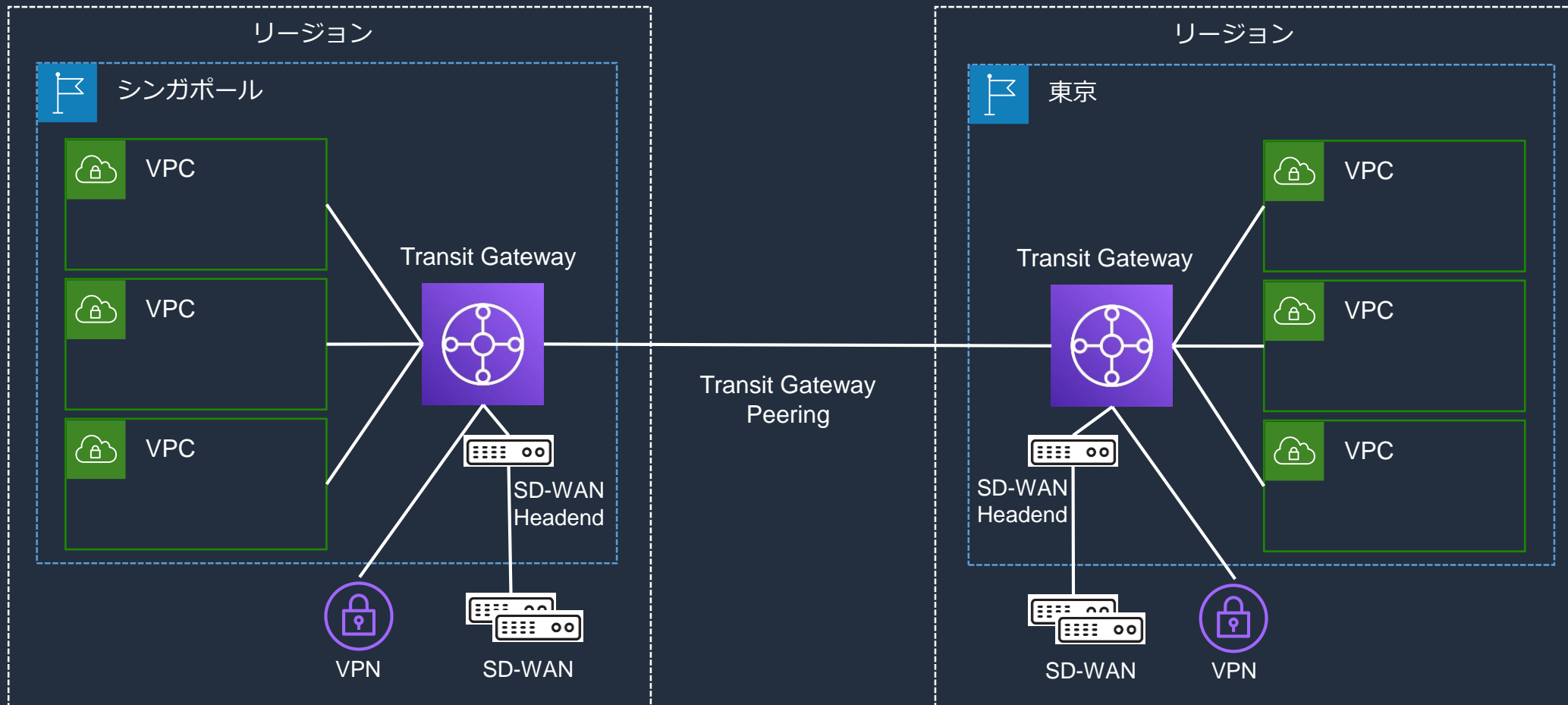
アジェンダ

- Cloud WAN概要
- Cloud WANユースケース
- AWS Transit Gateway連携
- Cloud WANコンポーネント

AWS Cloud WAN概要

Transit Gateway Inter Region Peering

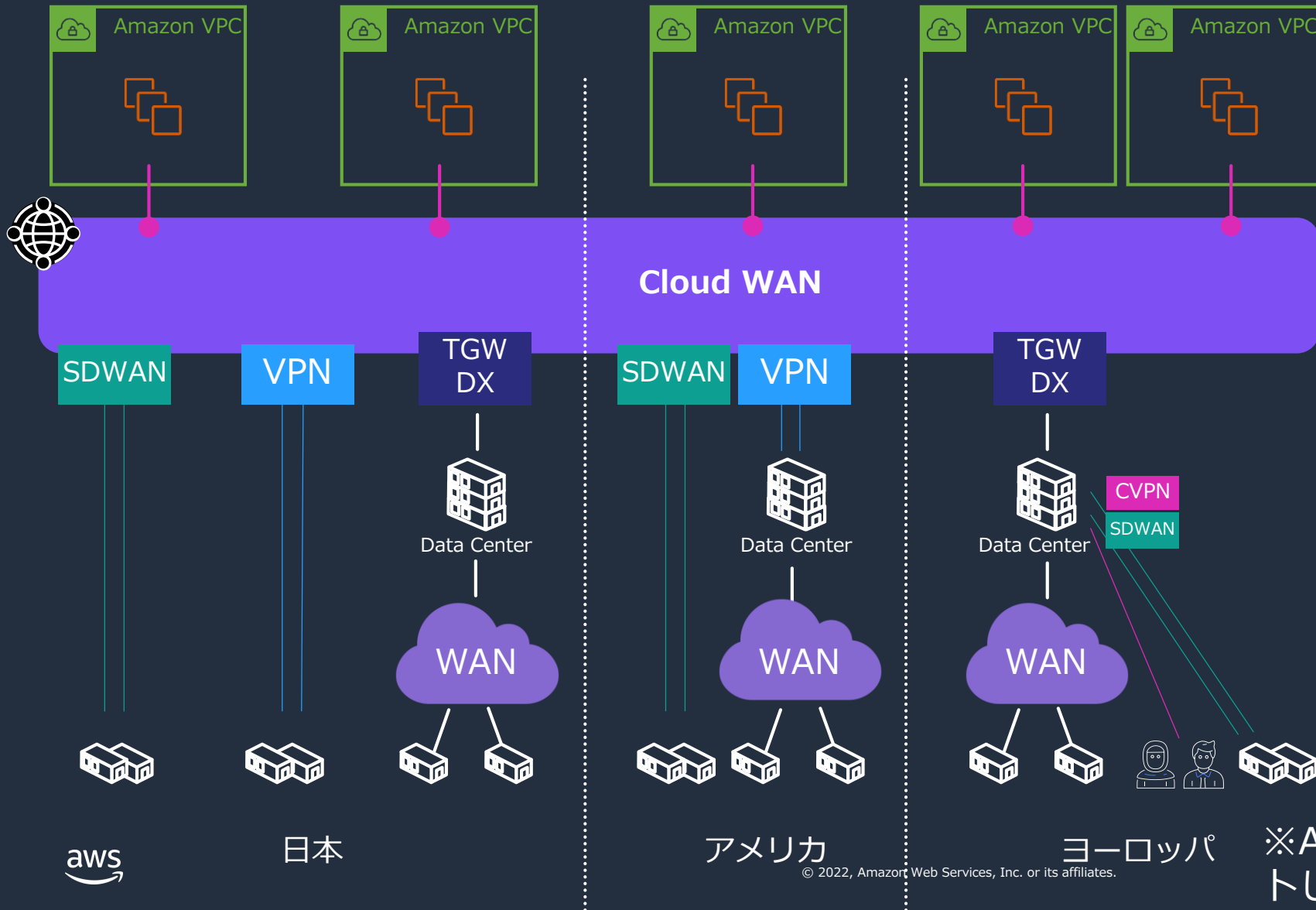
- グローバルネットワークを構築する際は個々のリージョン単位でネットワークポリシーの適用、管理が必要であった。



Cloud WAN概要

- 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

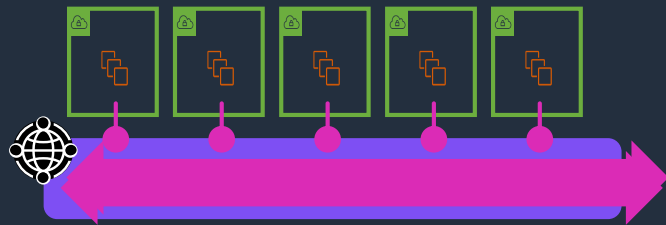
アタッチメント

VPCs
VPNs
SD-WAN(TGW Connect)
Transit Gateway RTBs

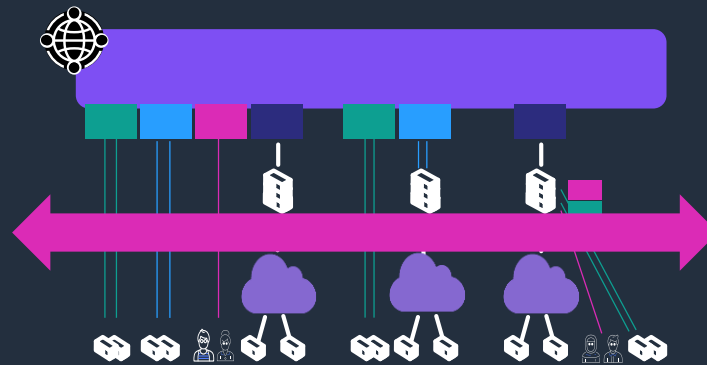
※AWS Direct Connectは現在サポ
ートしていません。

Cloud WANユースケース

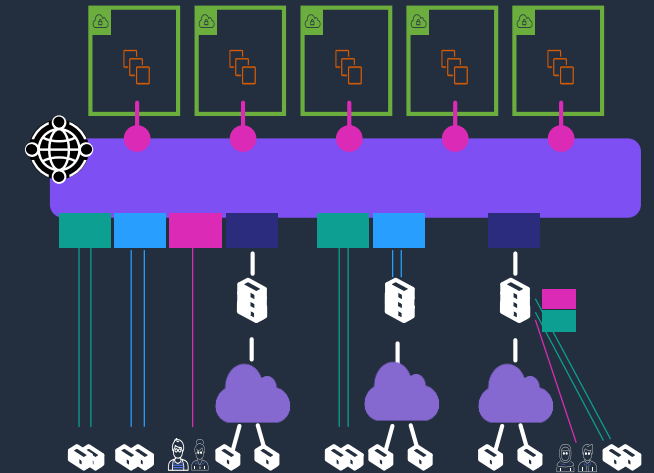
Cloud WANユースケース



VPC間通信

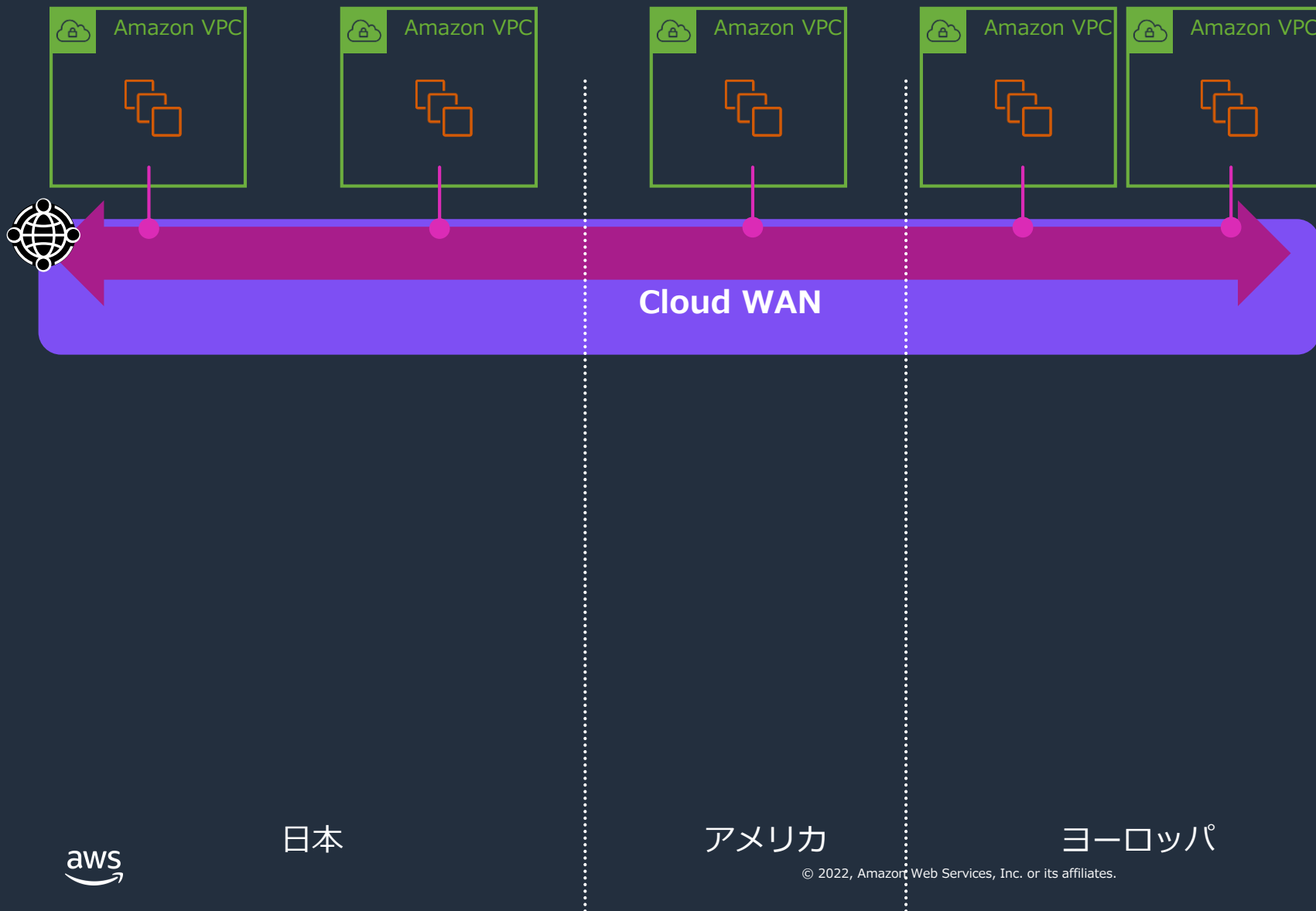


WAN接続



ハイブリッド構成

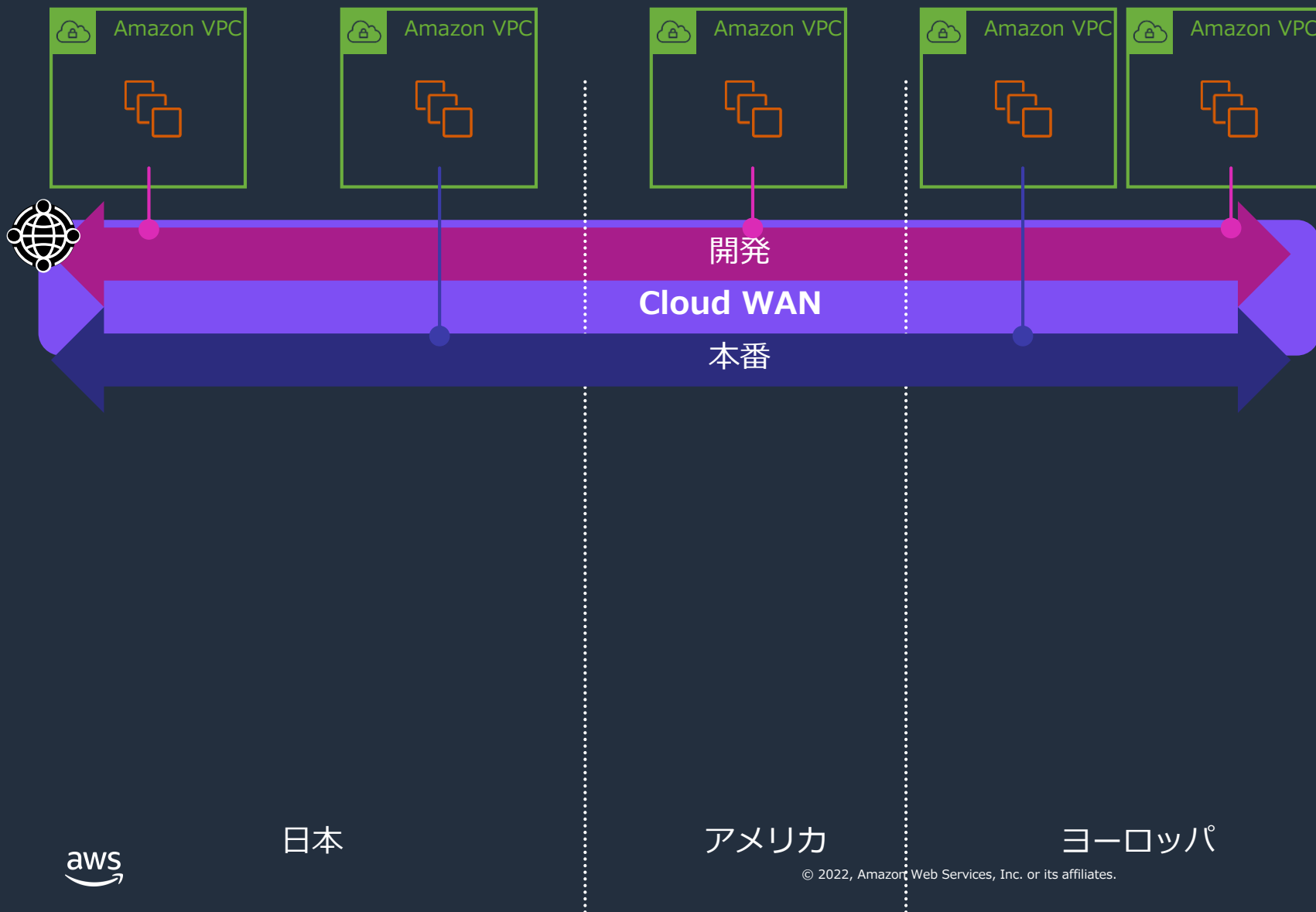
VPC間接続例



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。

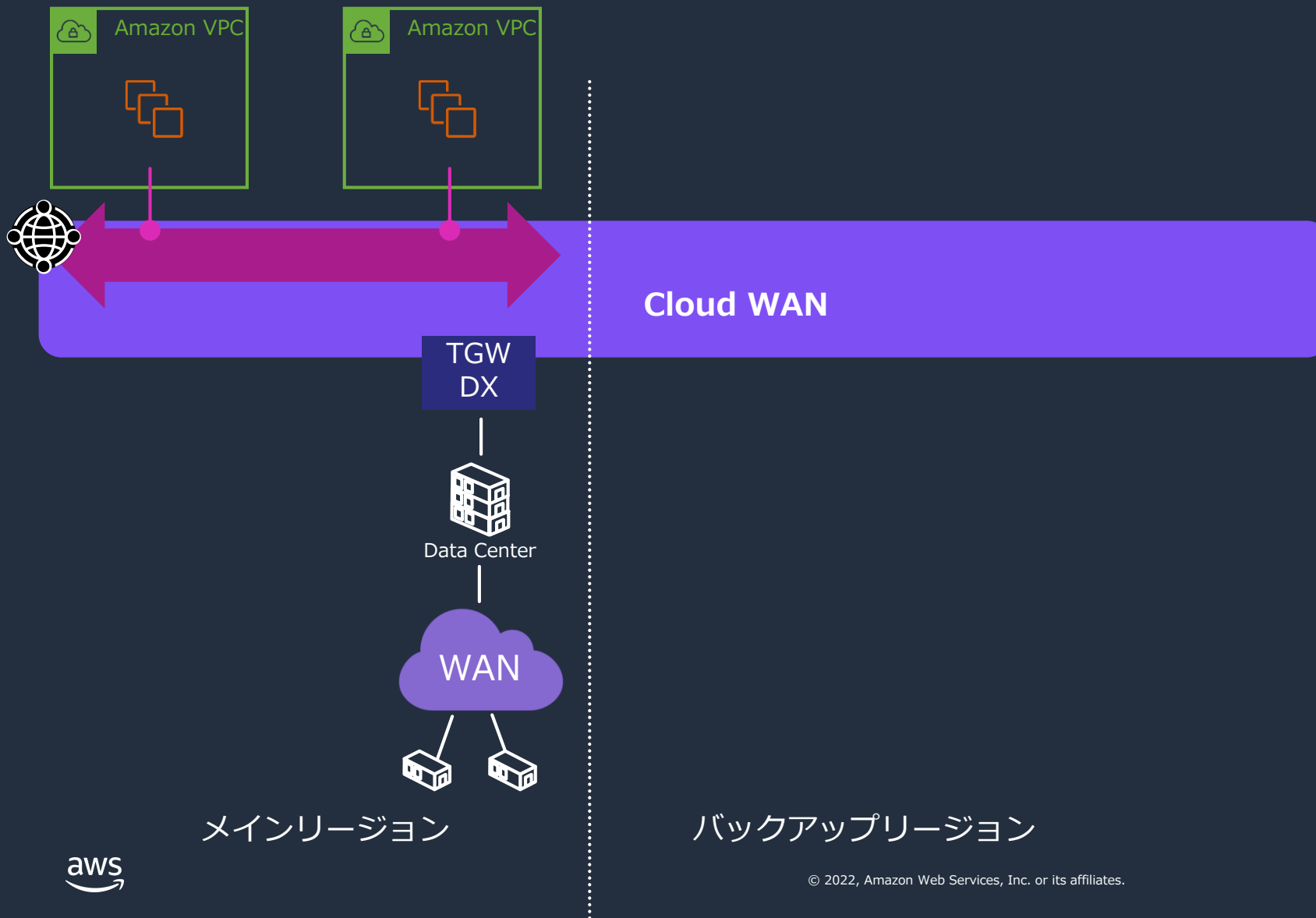
VPC間接続例



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。

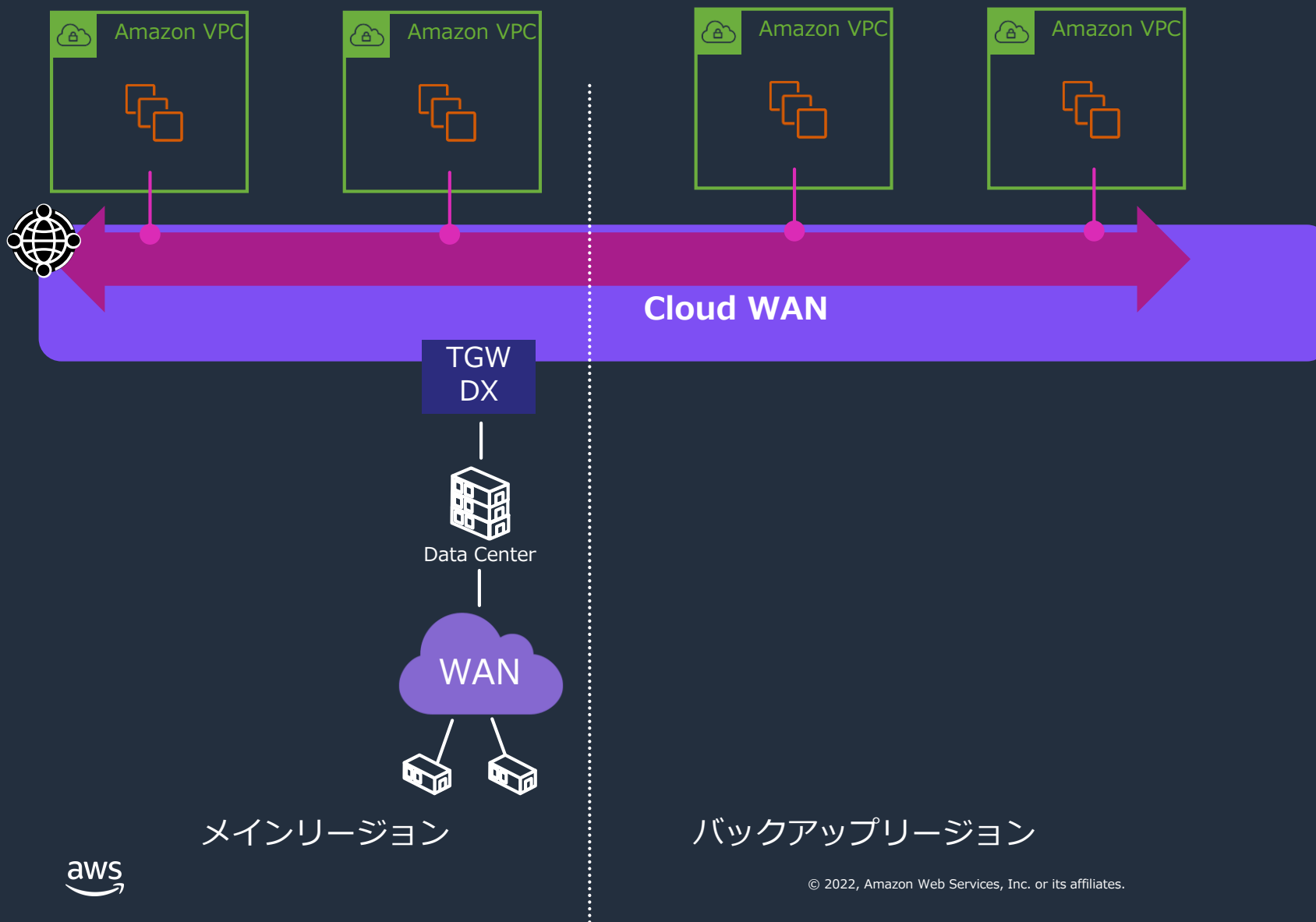
リージョンの追加例 (DR対策)



ユースケース

DR対策

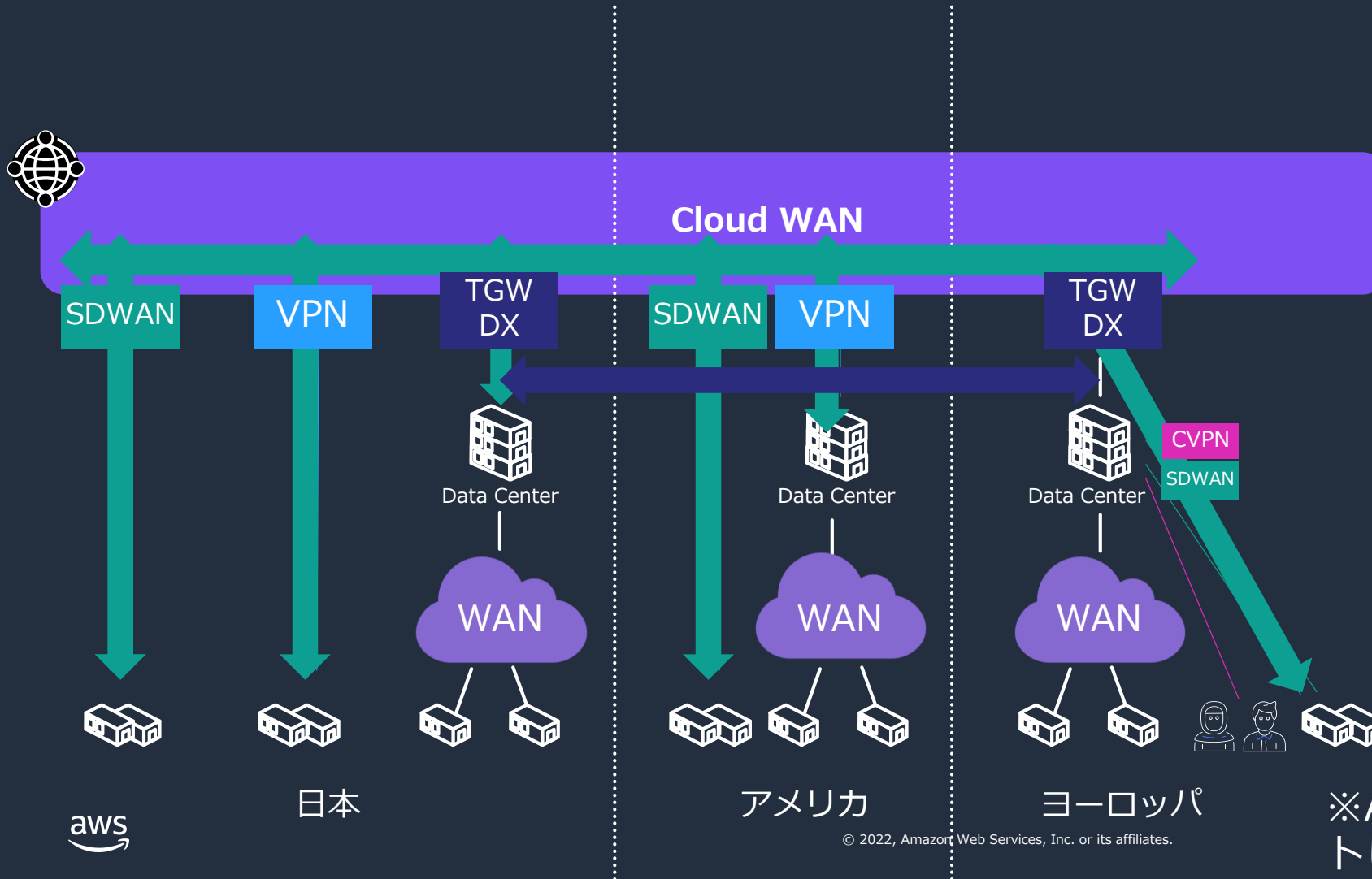
リージョンの追加例 (DR対策)



ユースケース

DR対策

WAN接続例

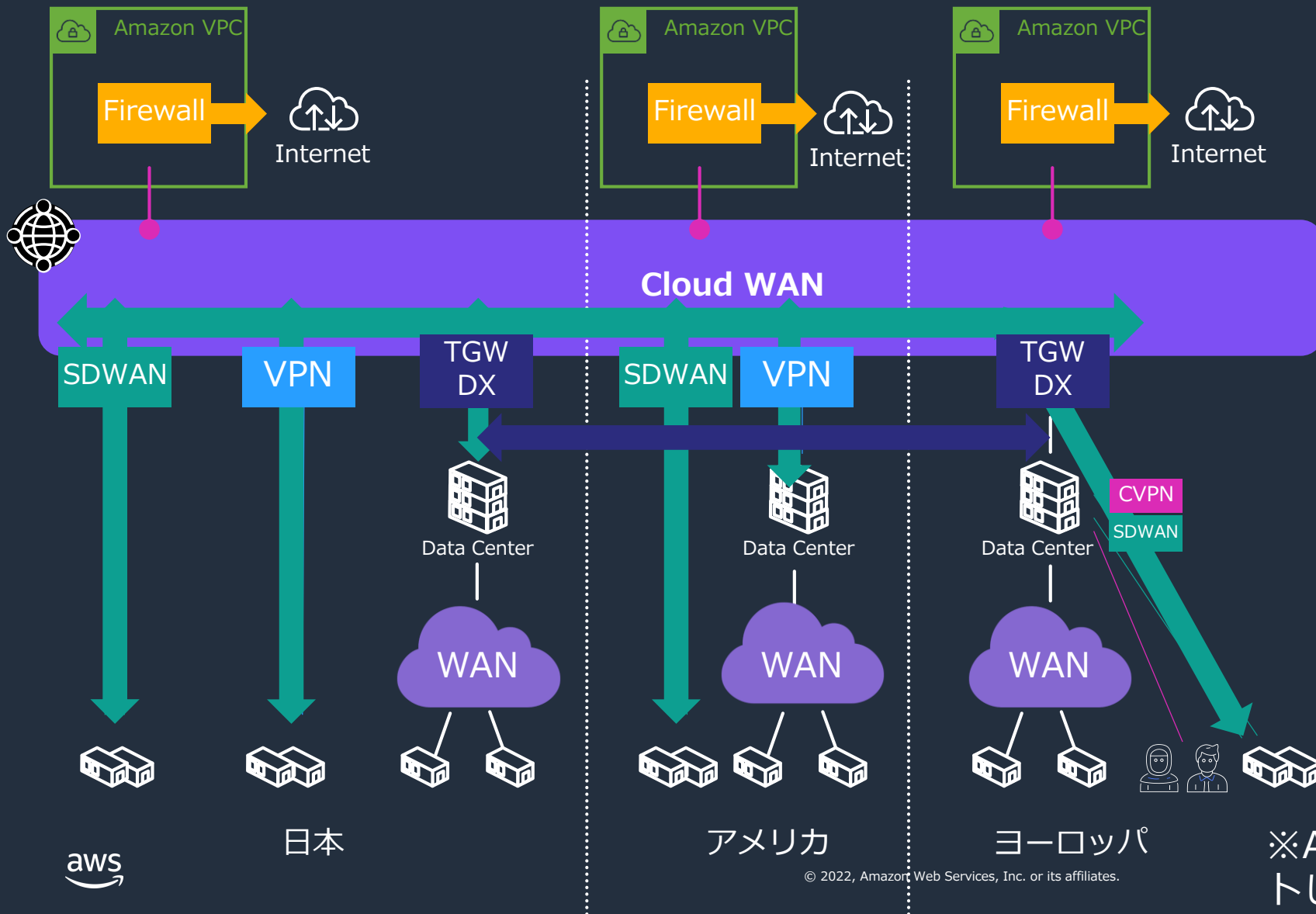


ユースケース

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いません。

WAN接続例



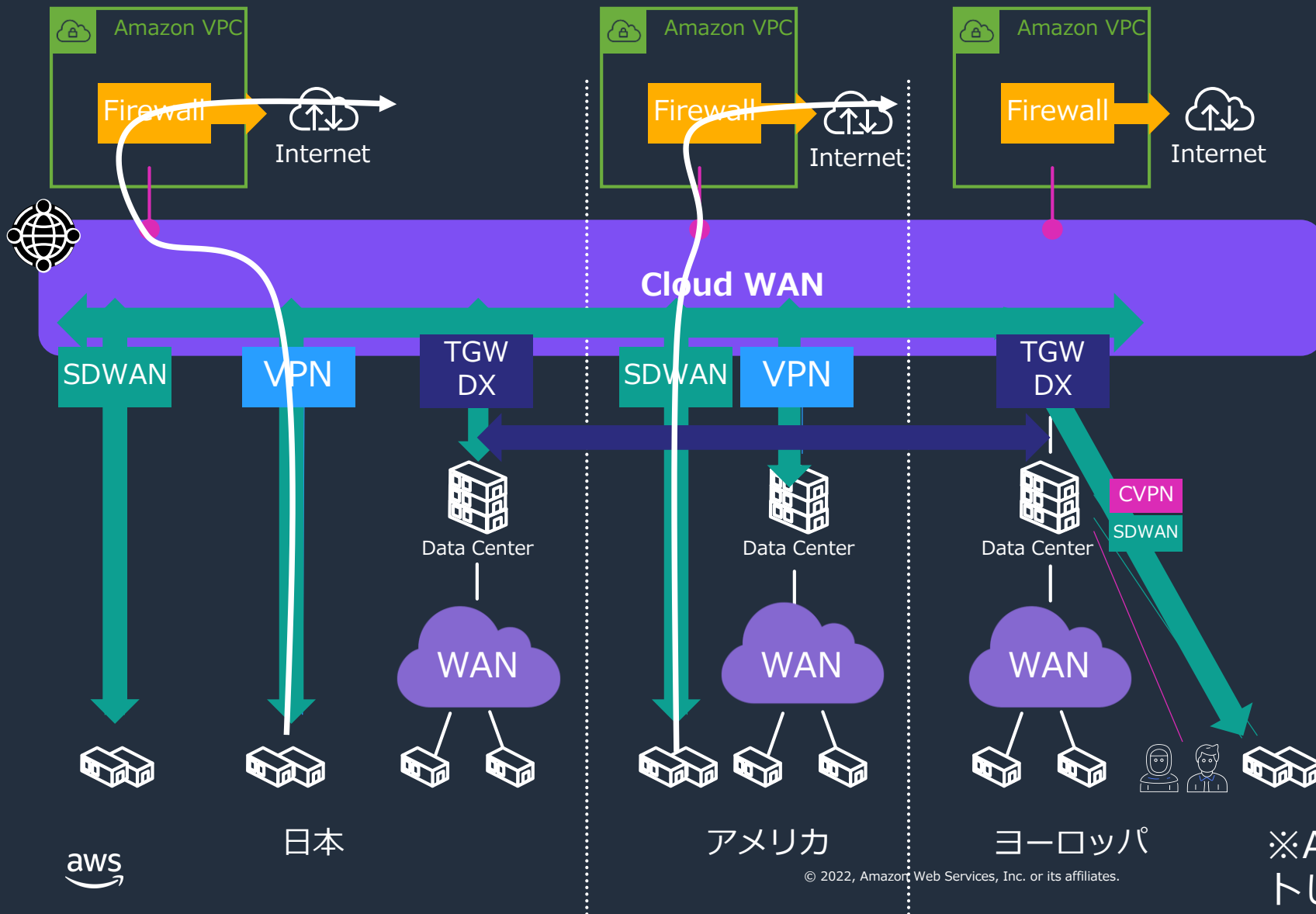
ユースケース

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



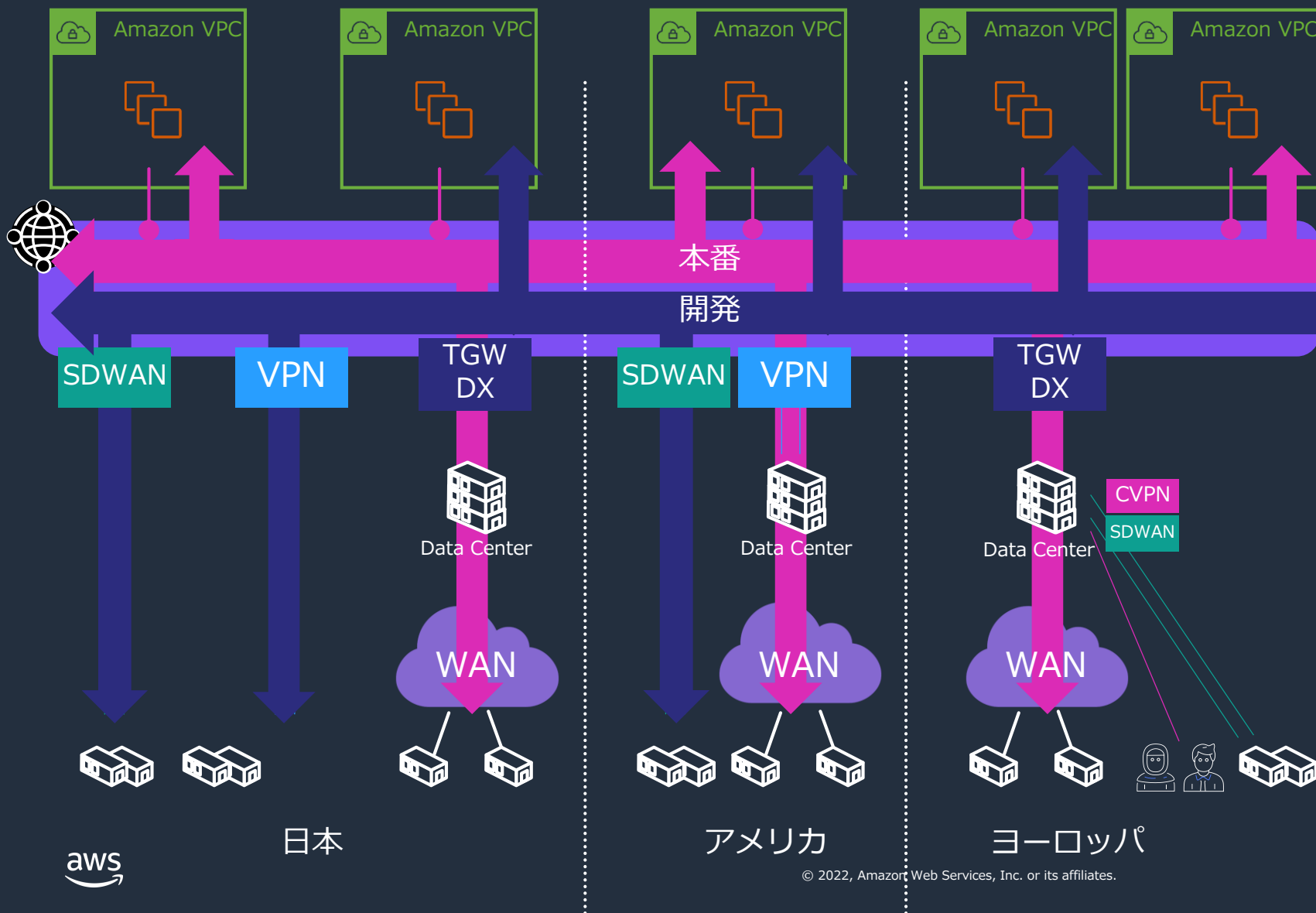
ユースケース

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



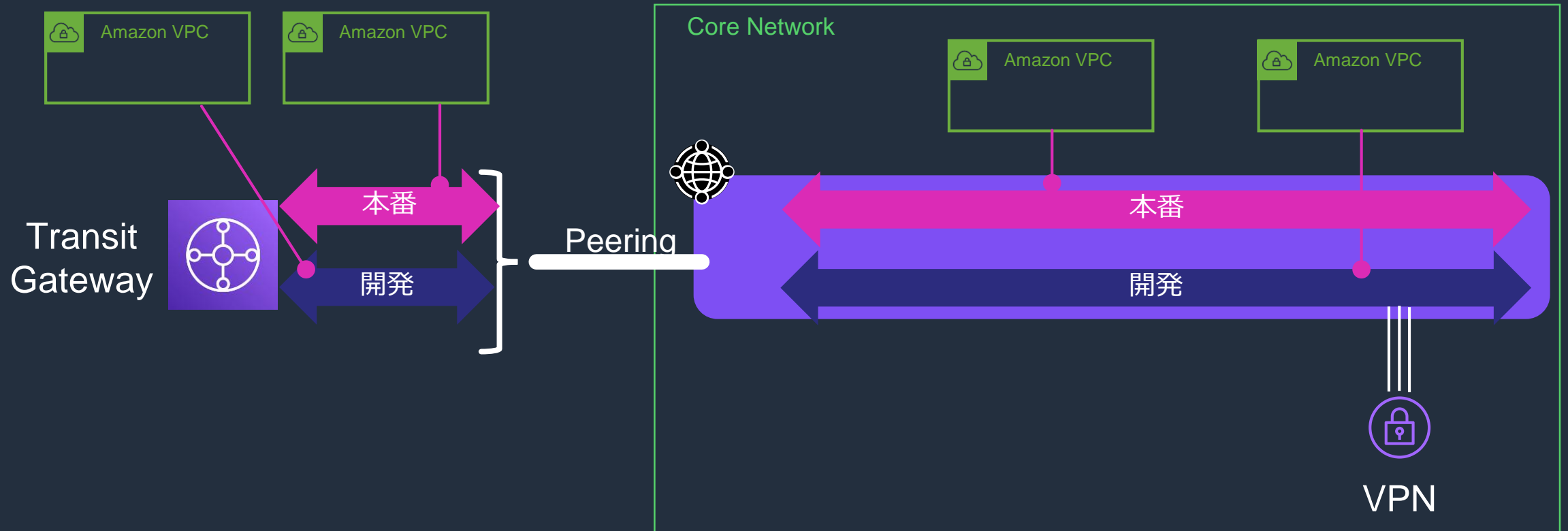
ユースケース

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。

AWS Transit Gateway 連携

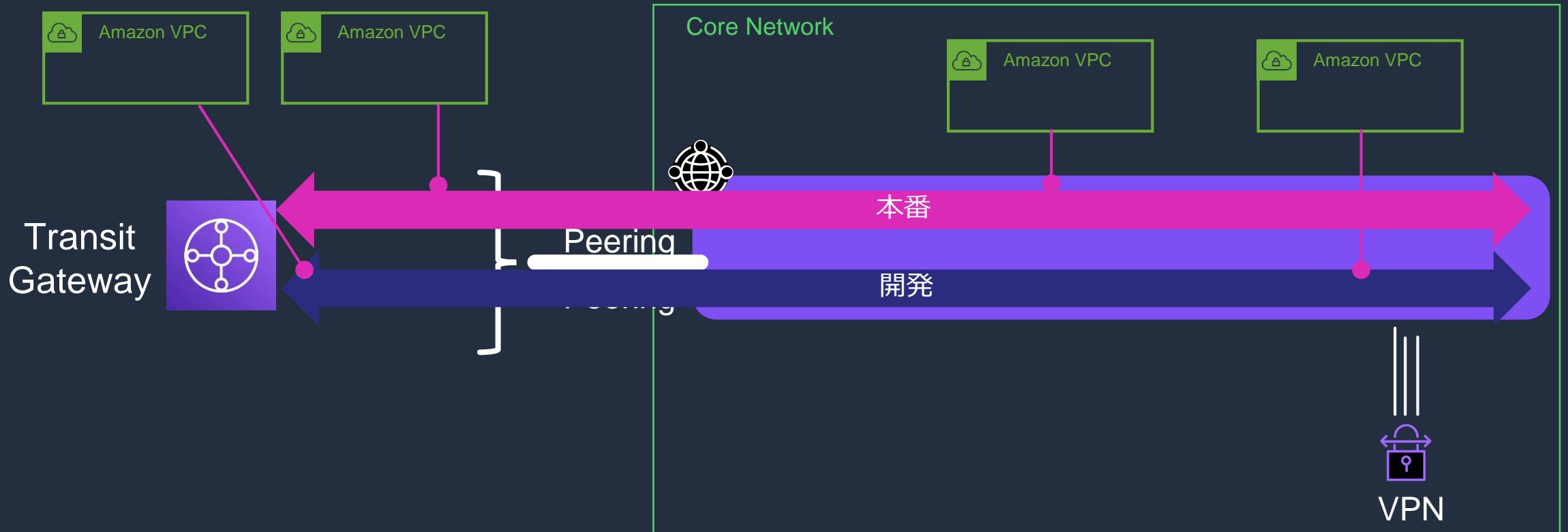
TGWとCloud WAN間接続



接続方法

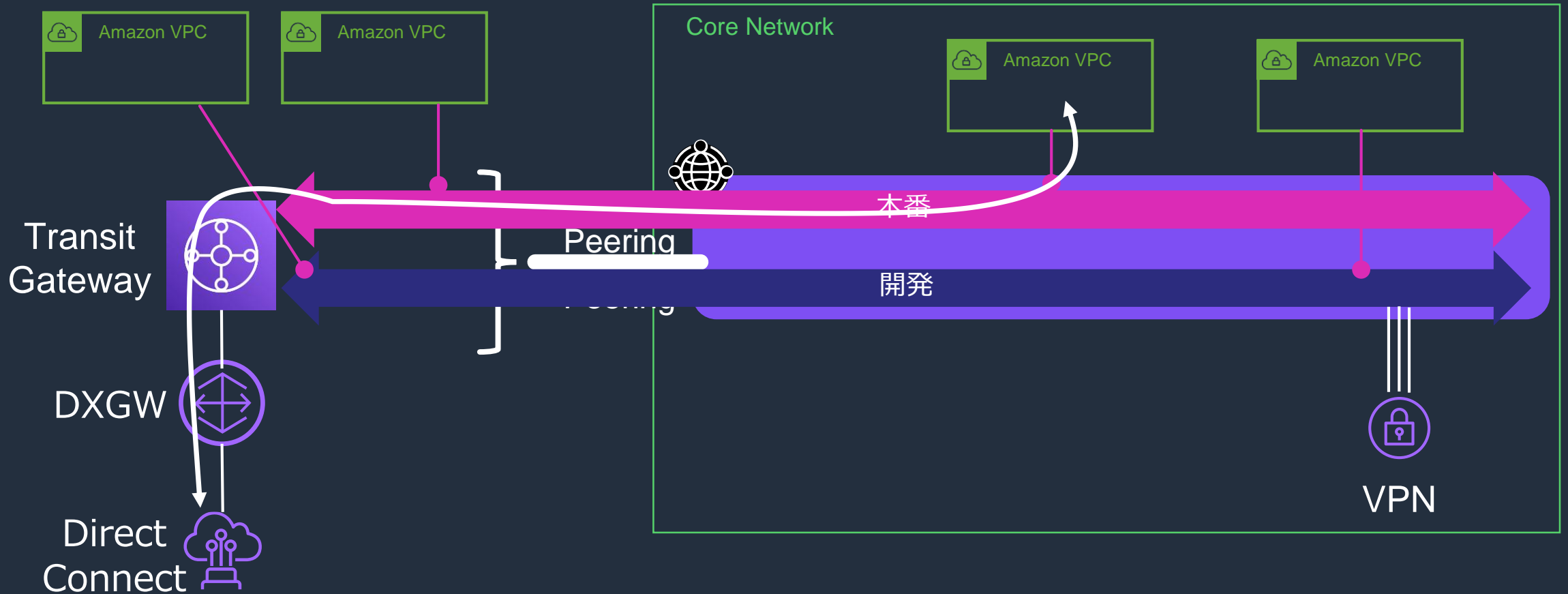
1. TGWとCloud WAN間をPeering
2. ルートテーブル単位でアタッチメント

TGWとCloud WAN間接続



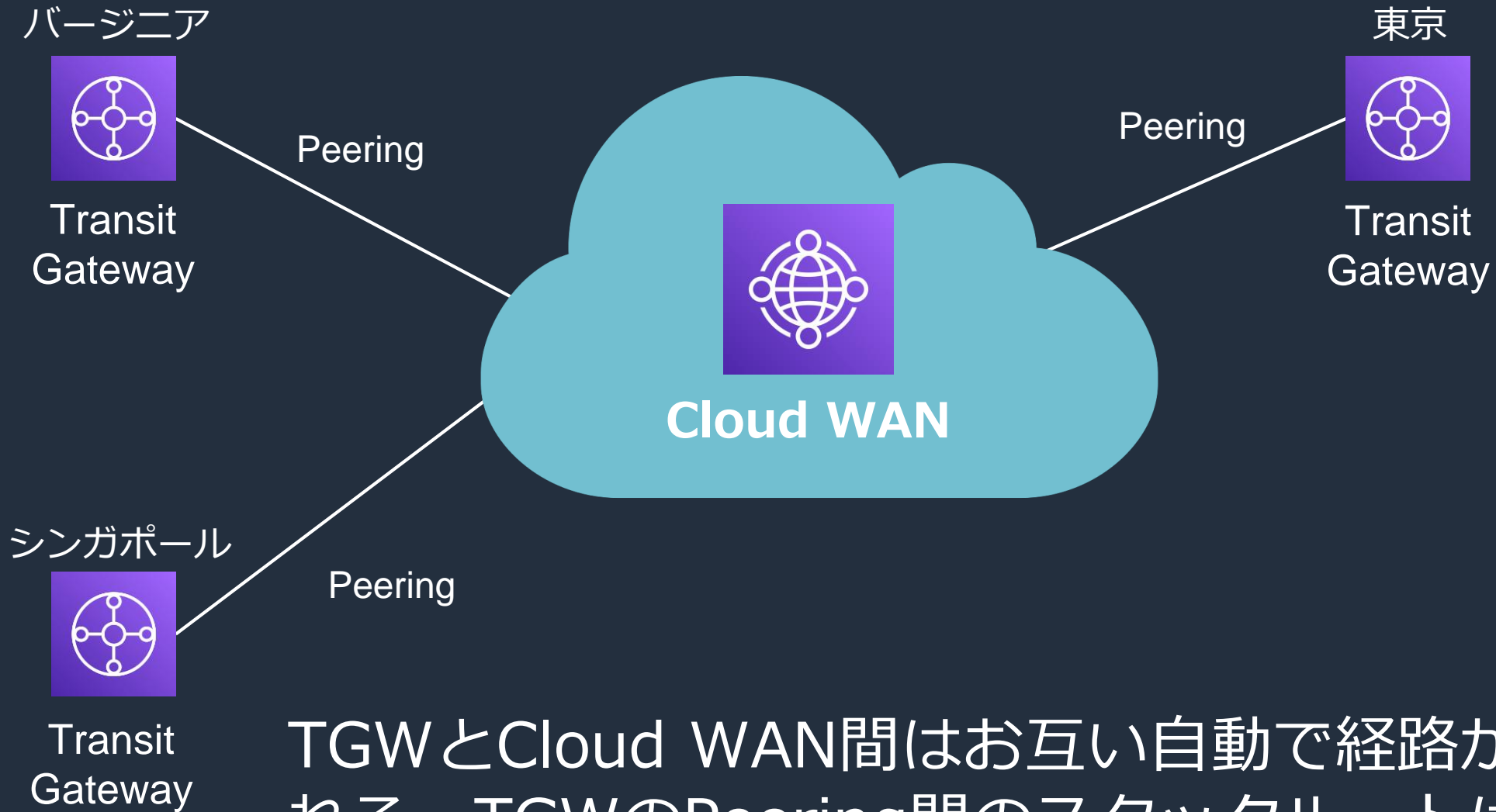
TGWとCloud WAN間はお互い自動で経路が伝搬される

TGW + DXとCloud WAN間接続



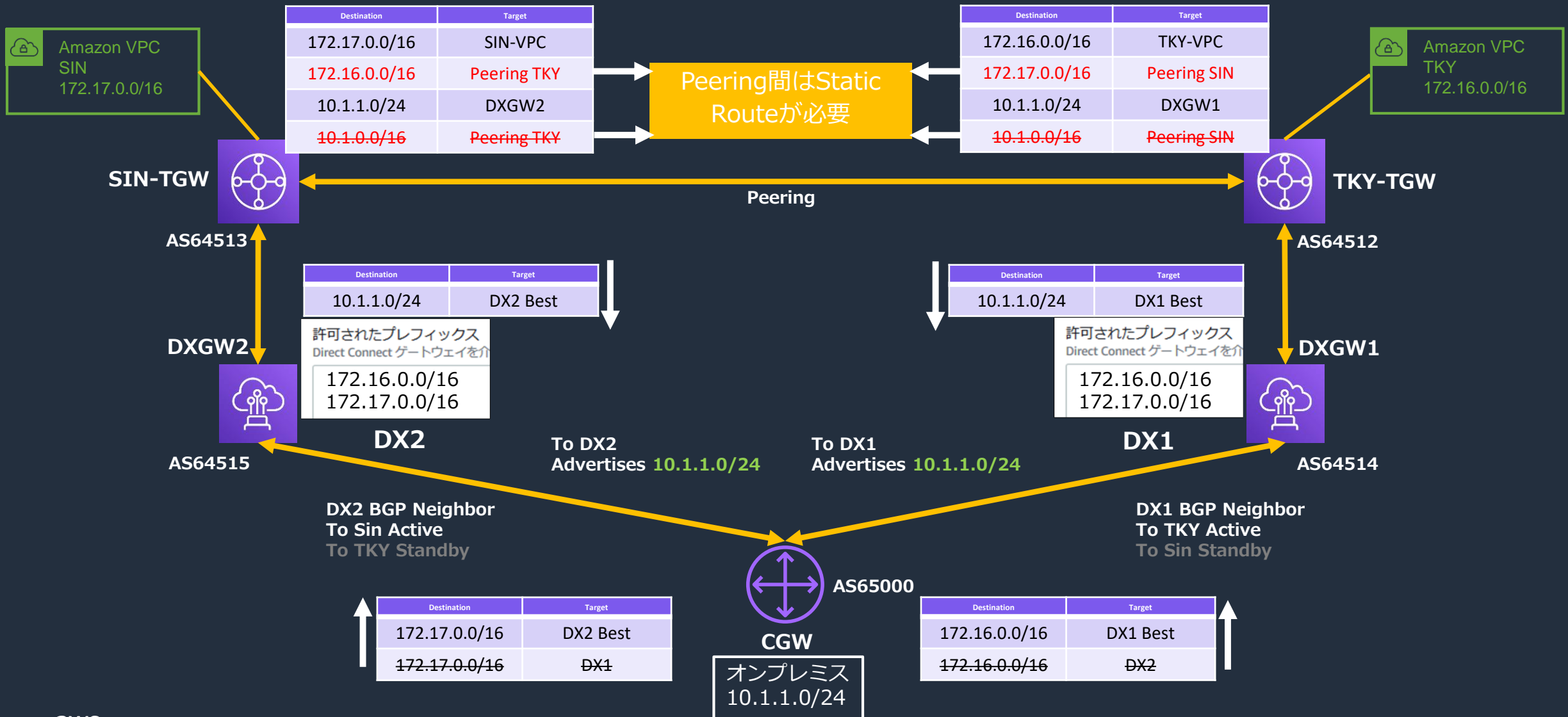
DXGWがアタッチメントされたTGWをCloud WANにアタッチメントする事も可能。

TGW Peering構成の簡素化

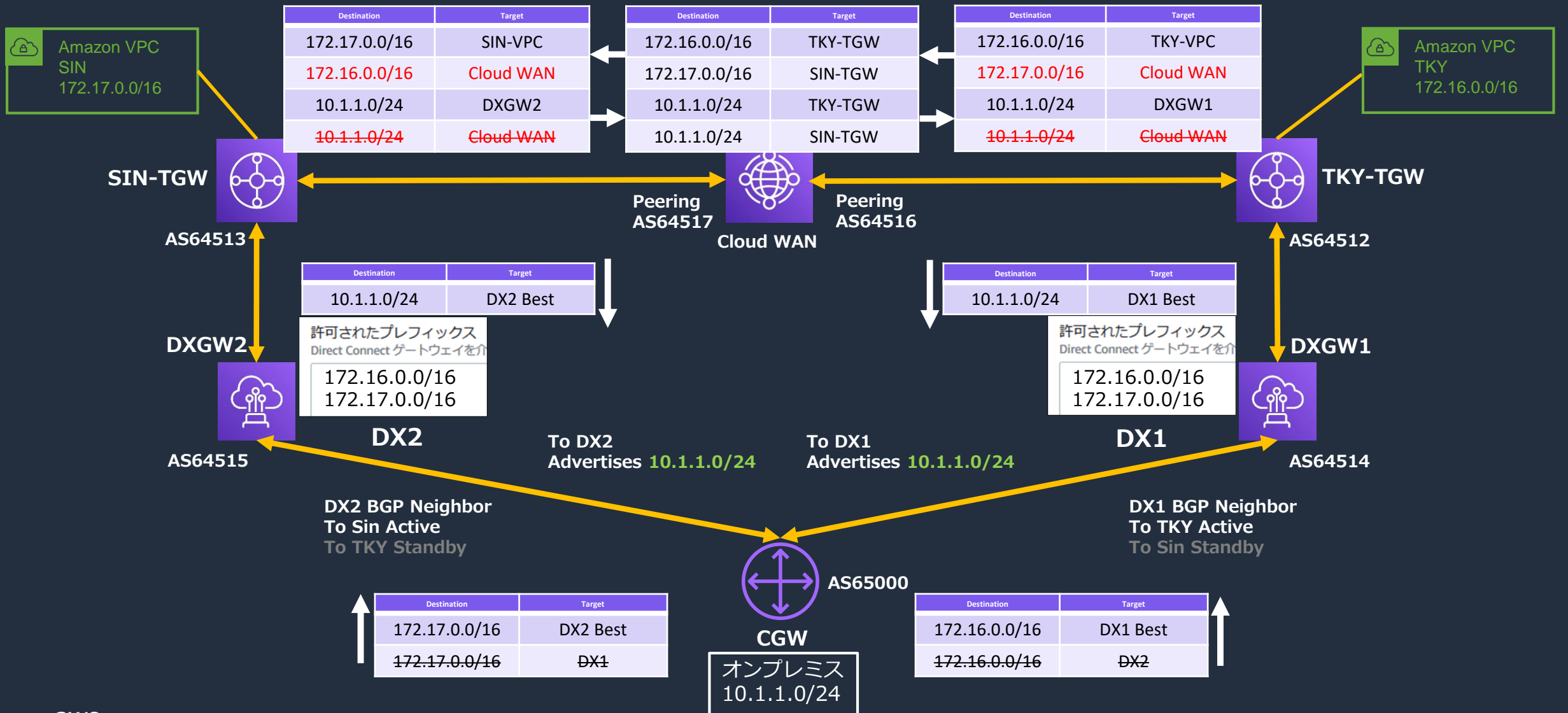


TGWとCloud WAN間はお互い自動で経路が伝搬される。TGWのPeering間のスタックルートは不要。

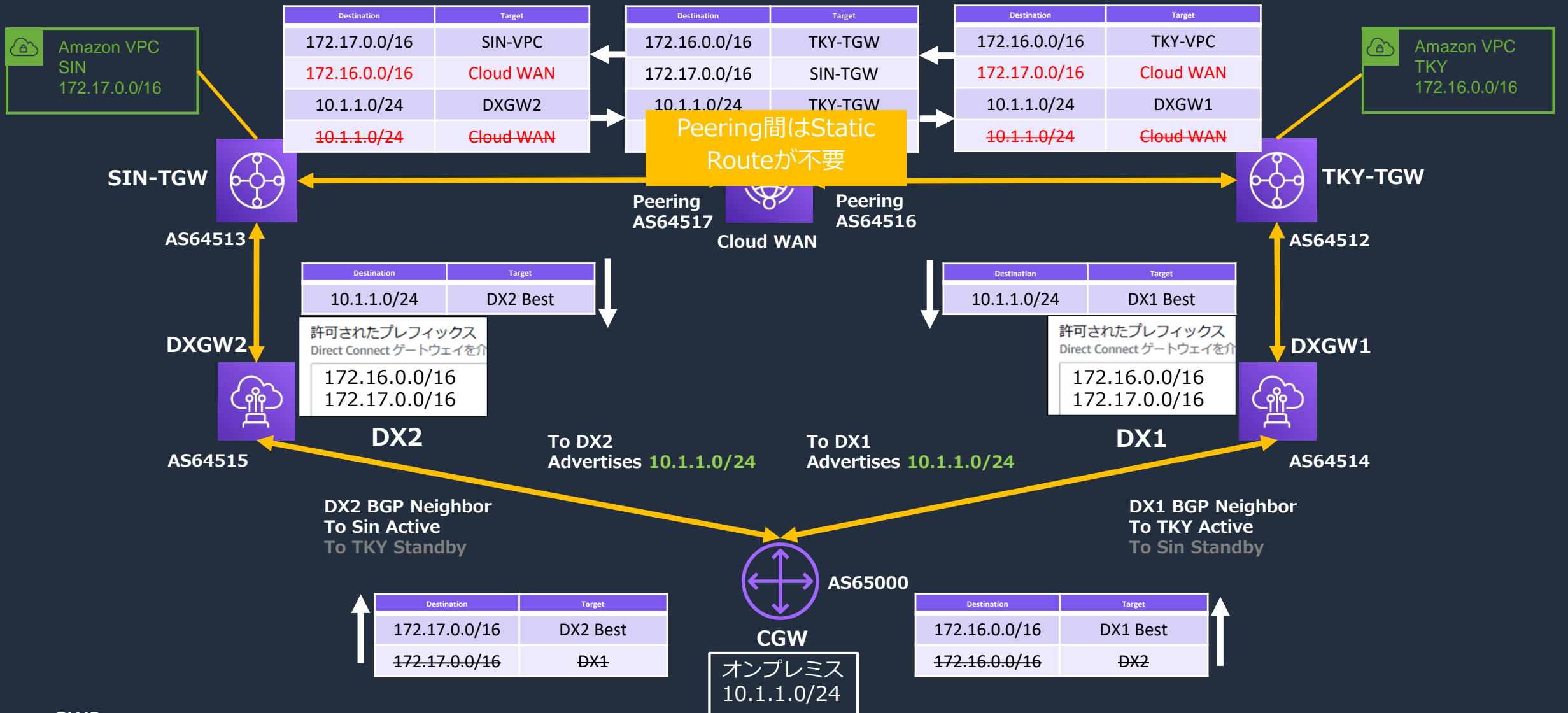
TGW Peering構成の簡素化(Cloud WAN未使用)



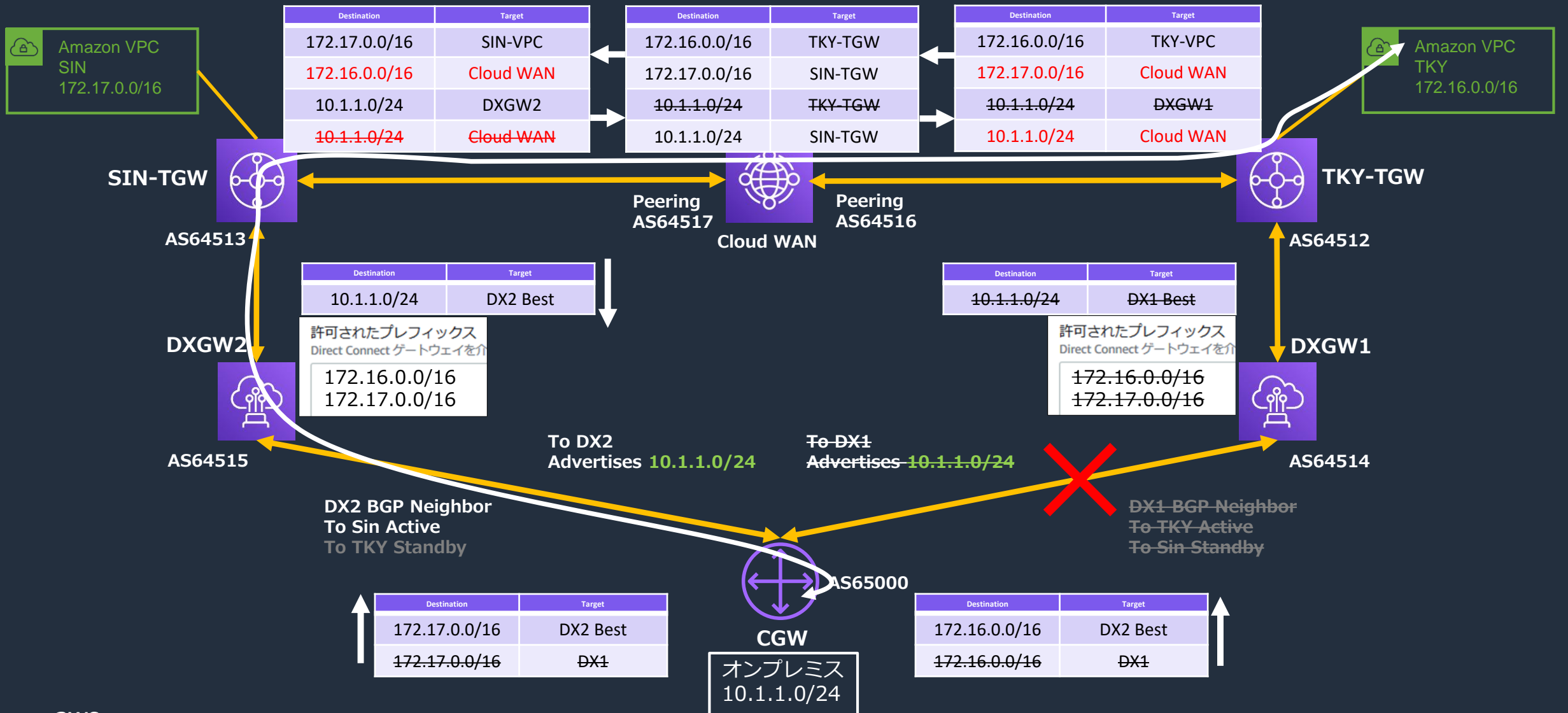
TGW Peering構成の簡素化(Cloud WAN使用)



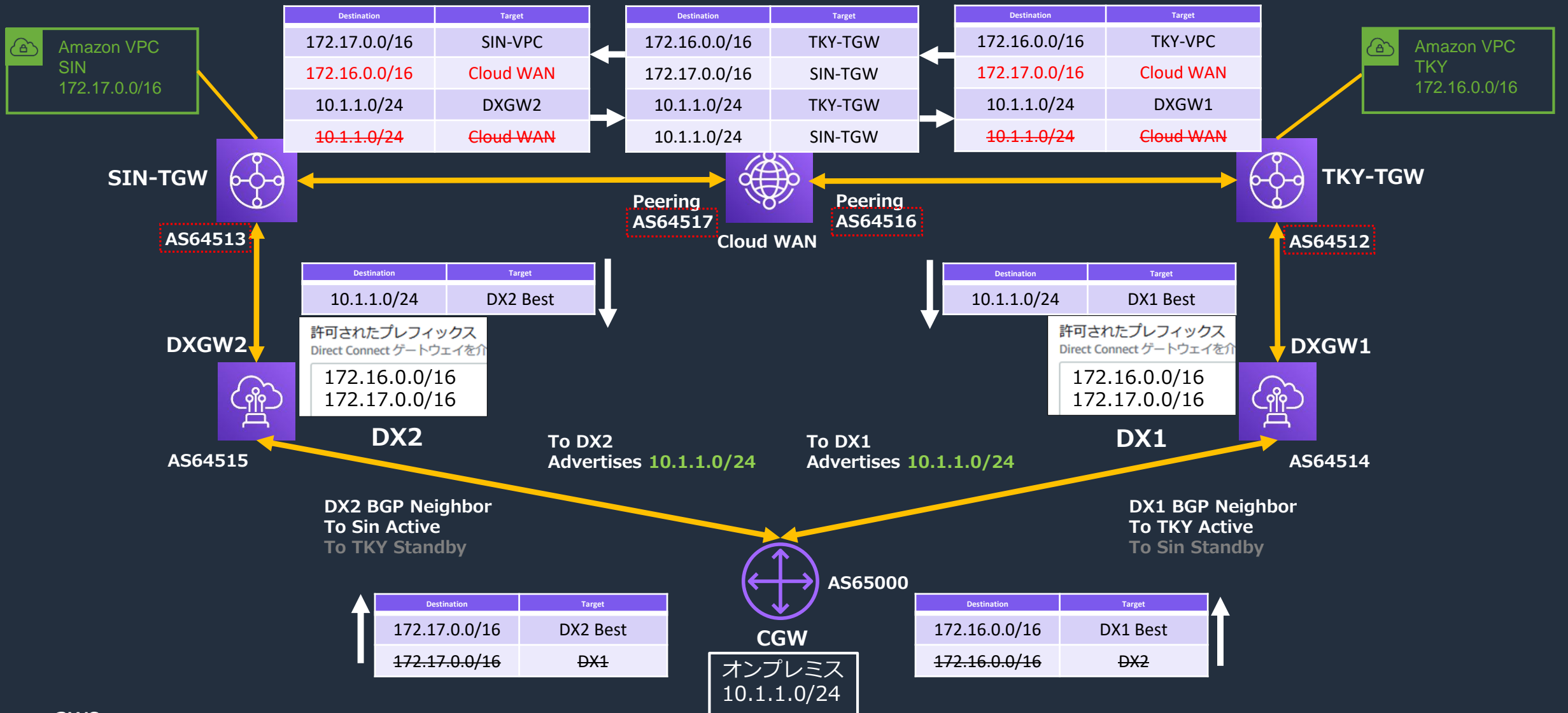
TGW Peering構成の簡素化(Cloud WAN使用)



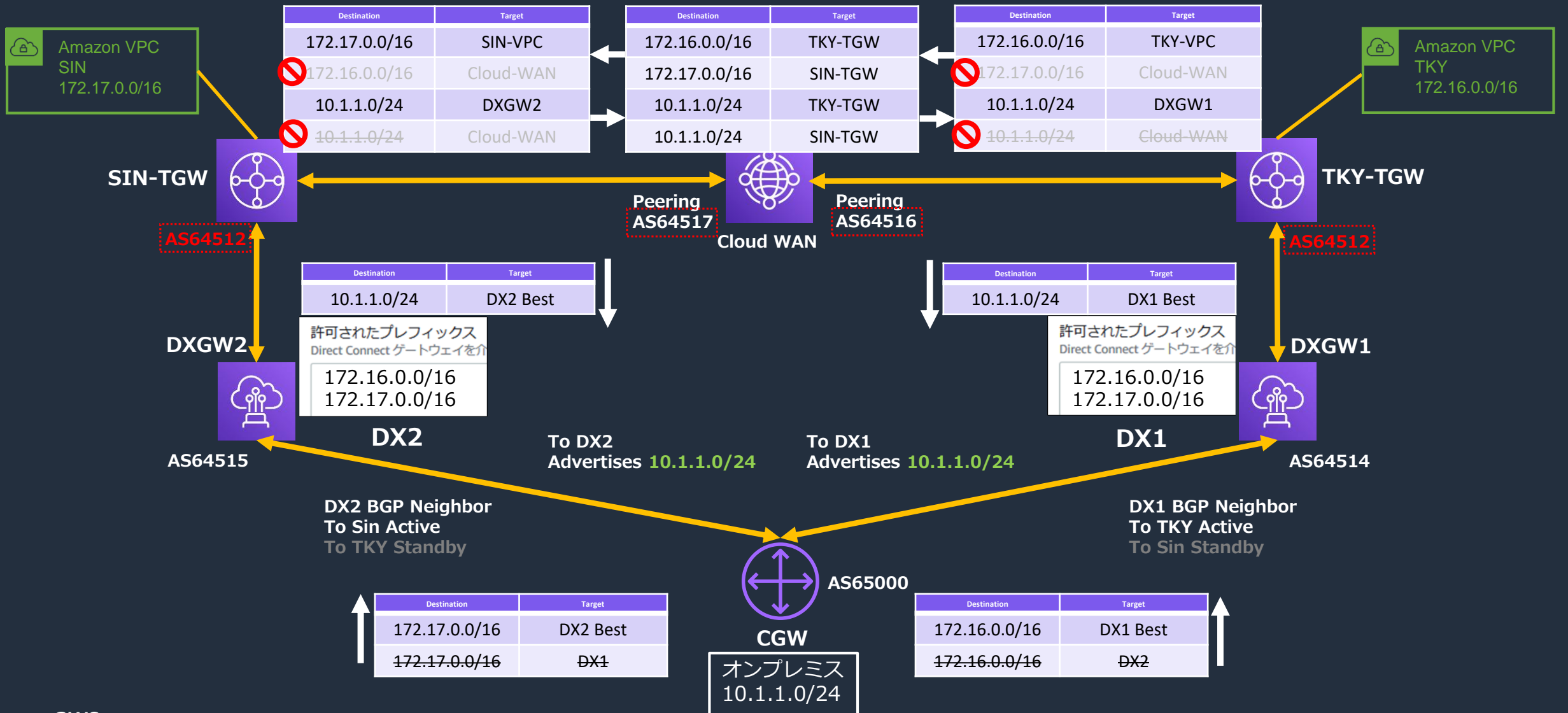
TGW Peering構成の簡素化(Cloud WAN使用)



ASN設計の注意点

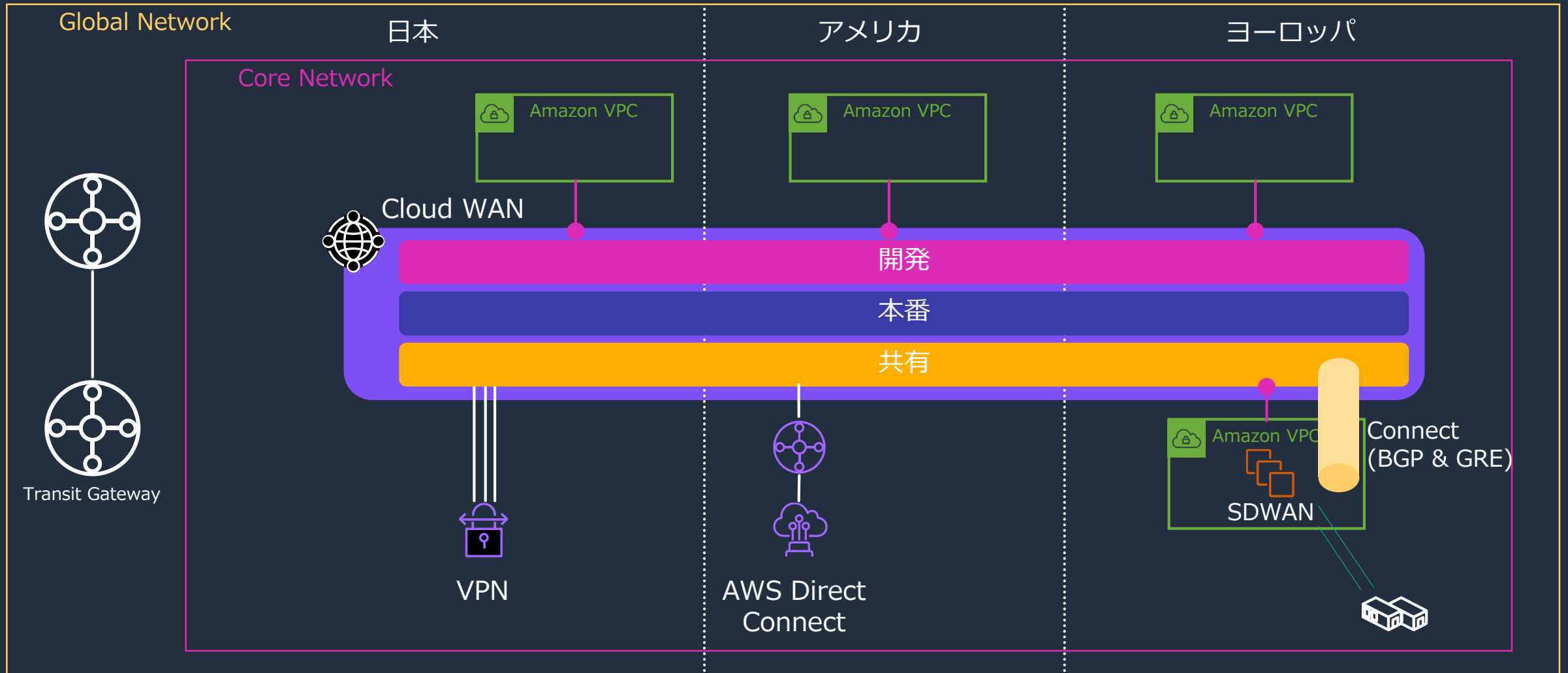


ASN設計の注意点

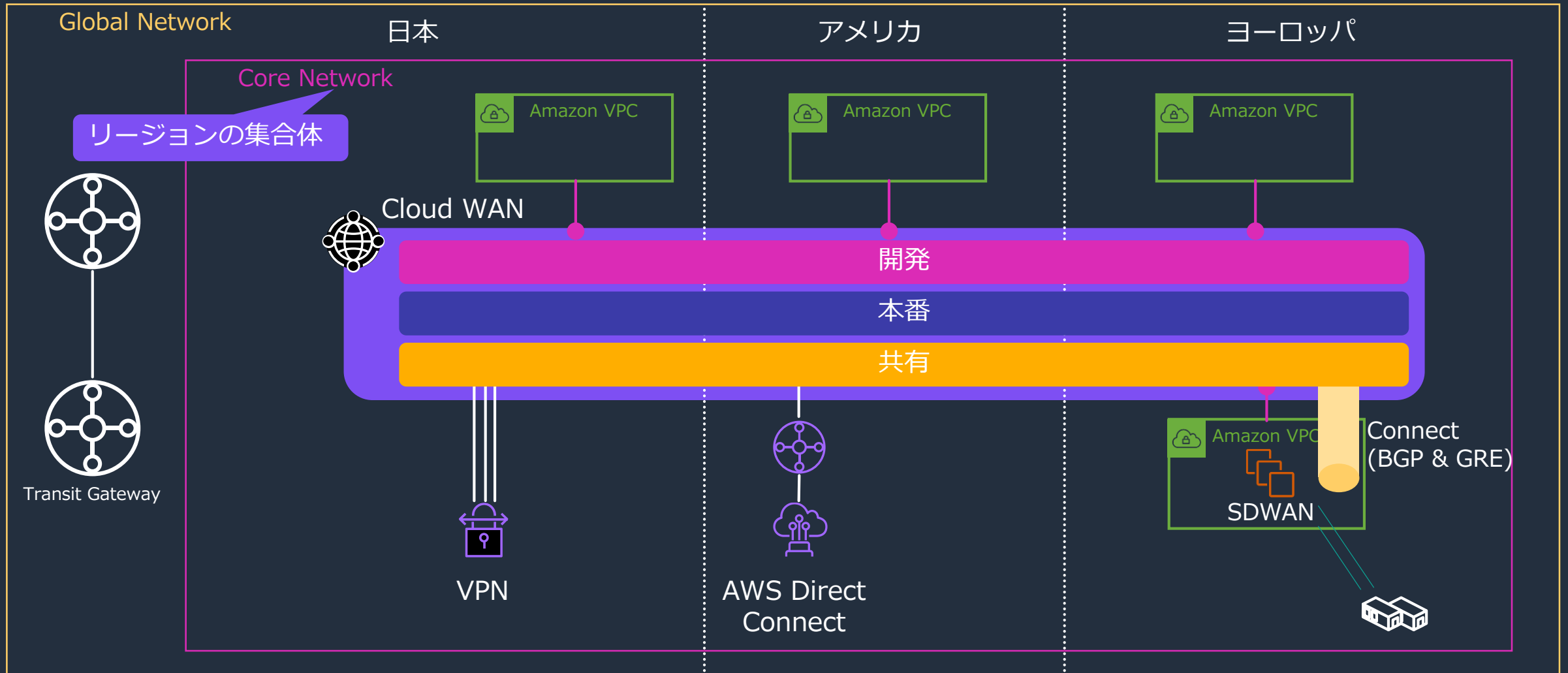


Cloud WANコンポーネント

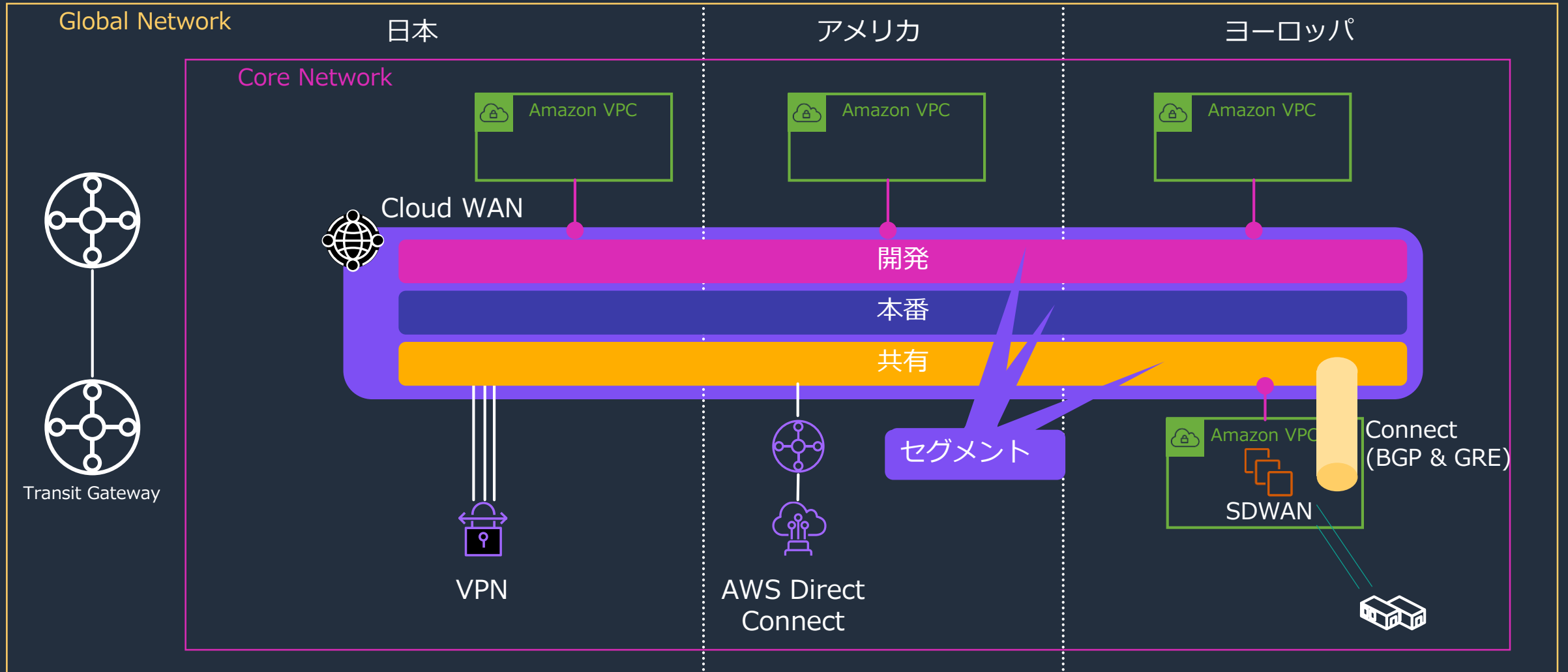
Cloud WANコンポーネント



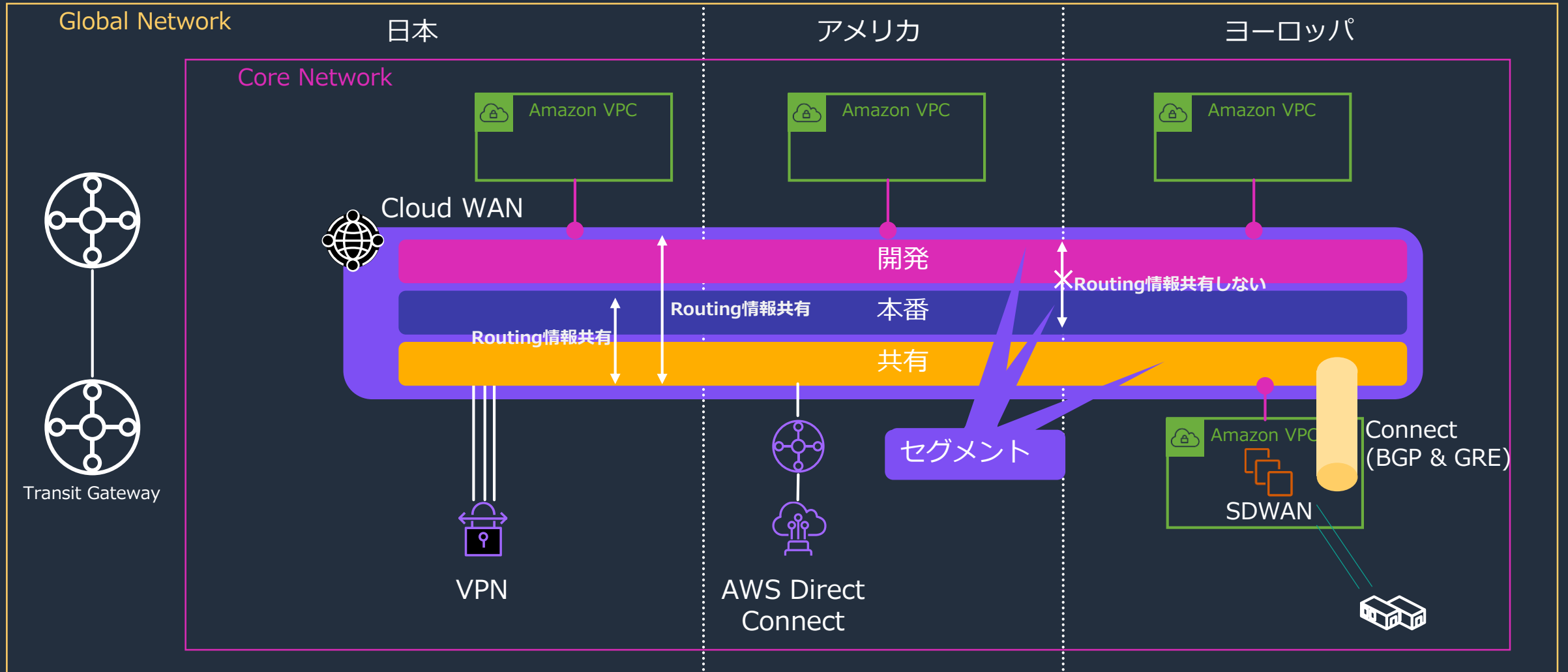
Cloud WANコンポーネント



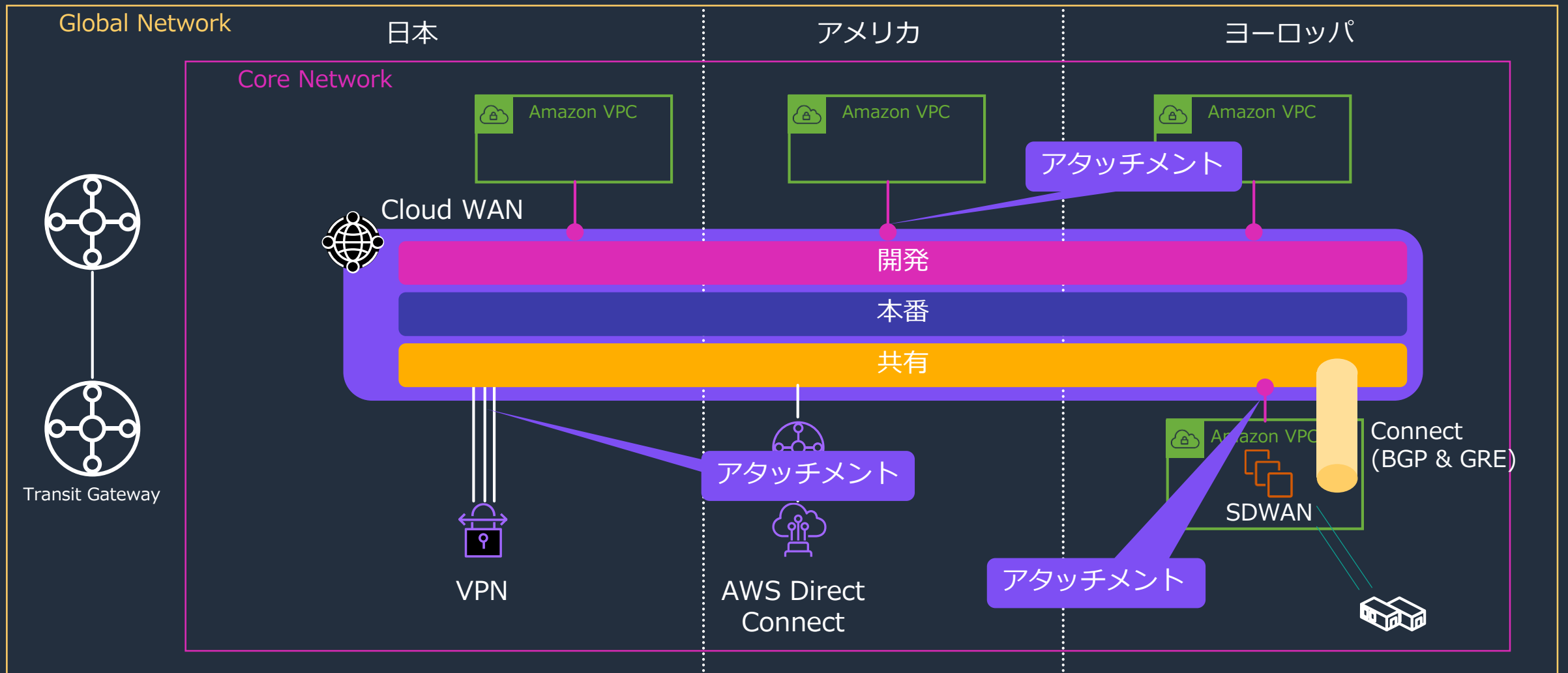
Cloud WANコンポーネント：セグメント



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

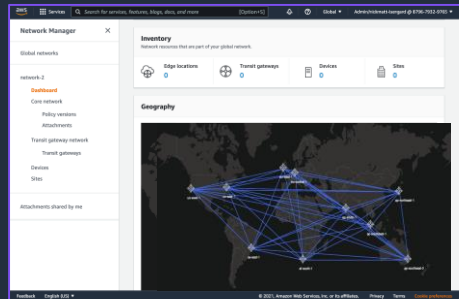


Cloud WANコンポーネント : Core Network Policy

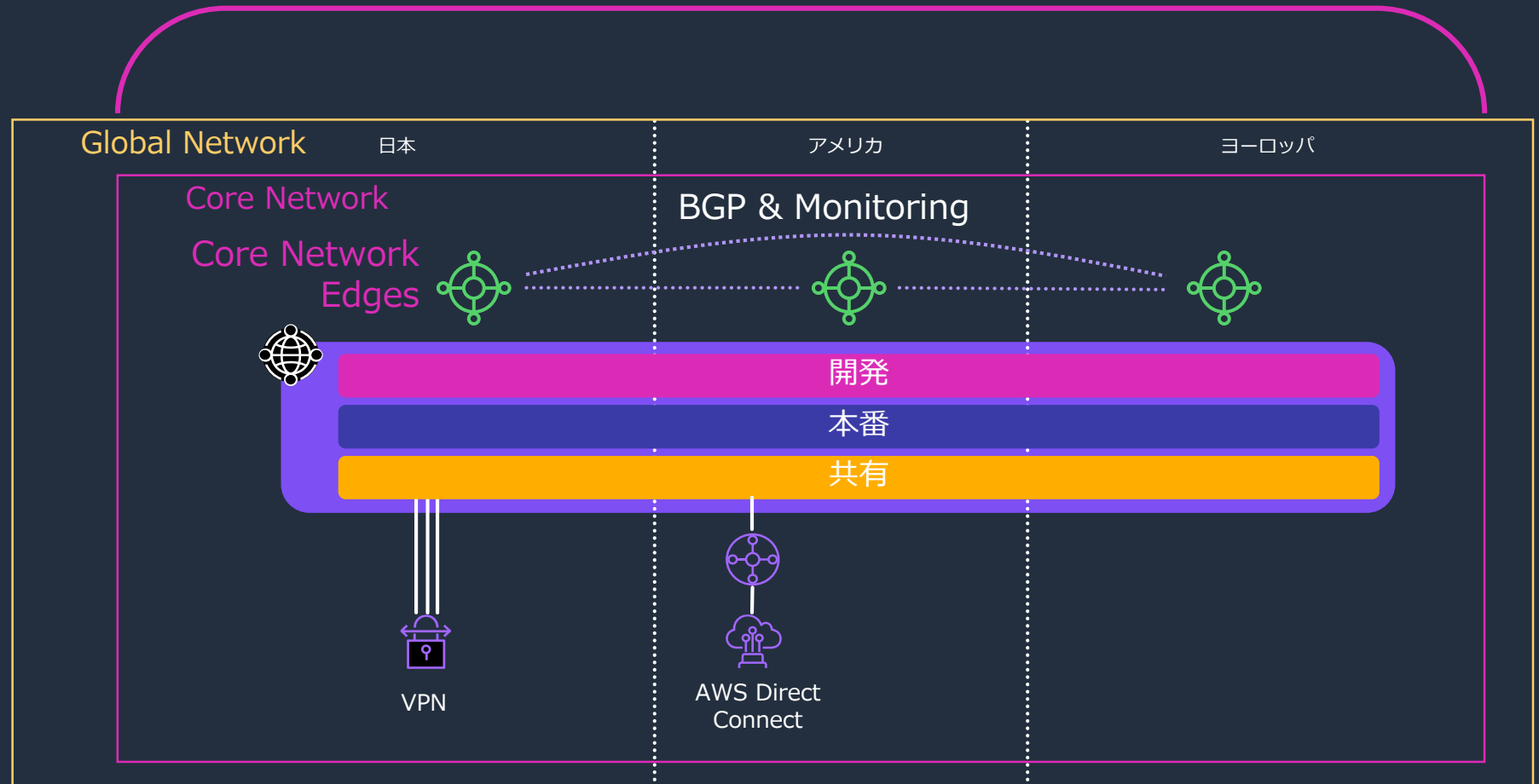
Core Networkのネットワーク構成を定義するポリシー



Core Network Policy(CNP)



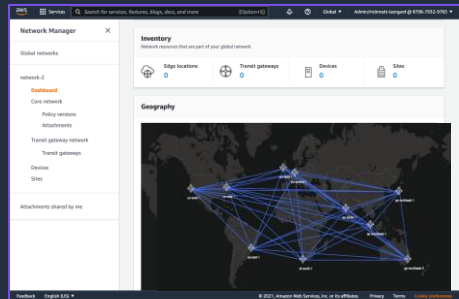
AWS Network Manager



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

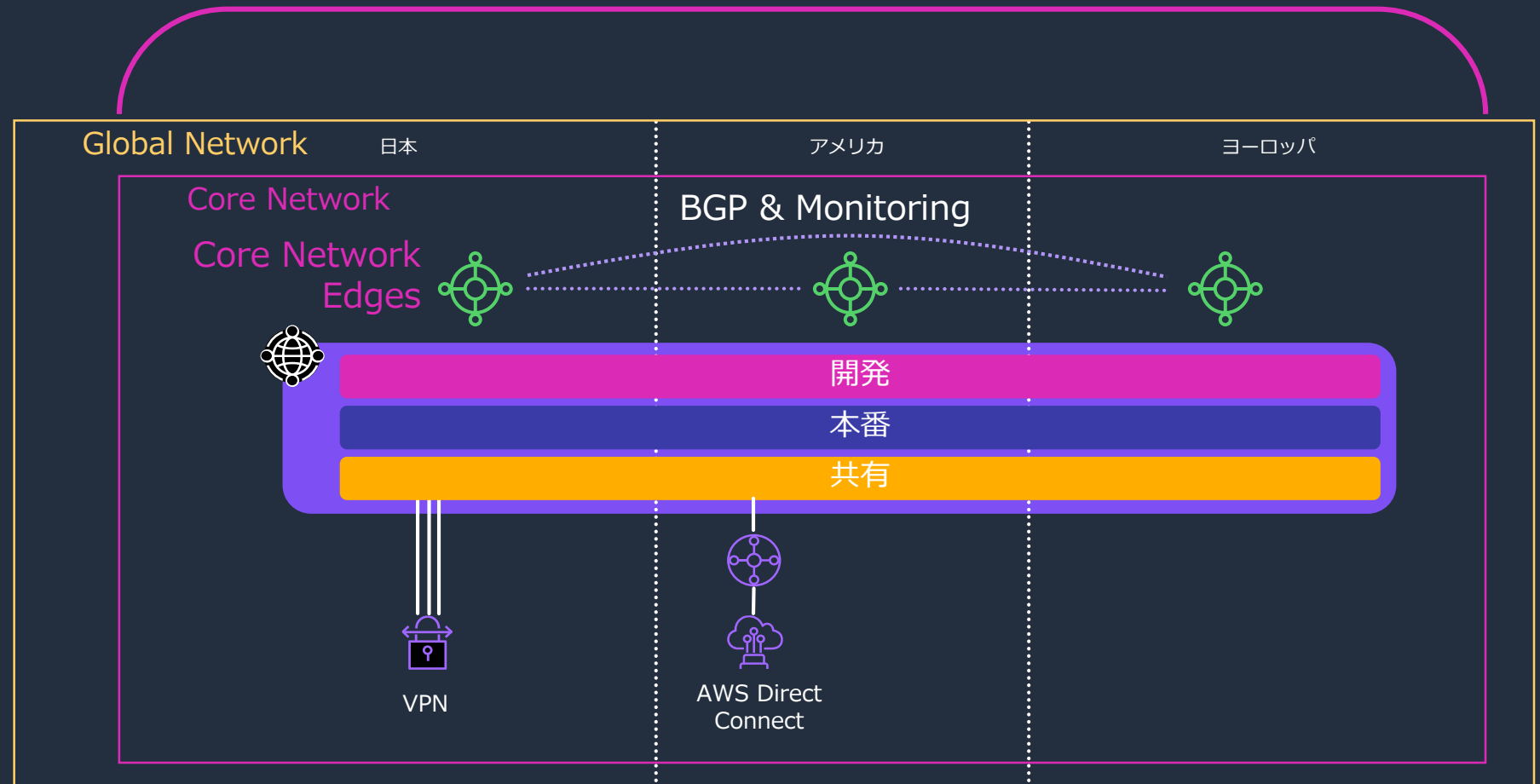
ダッシュボード
ポリシーの設定
トポロジー情報
ルーティング情報
イベント一覧



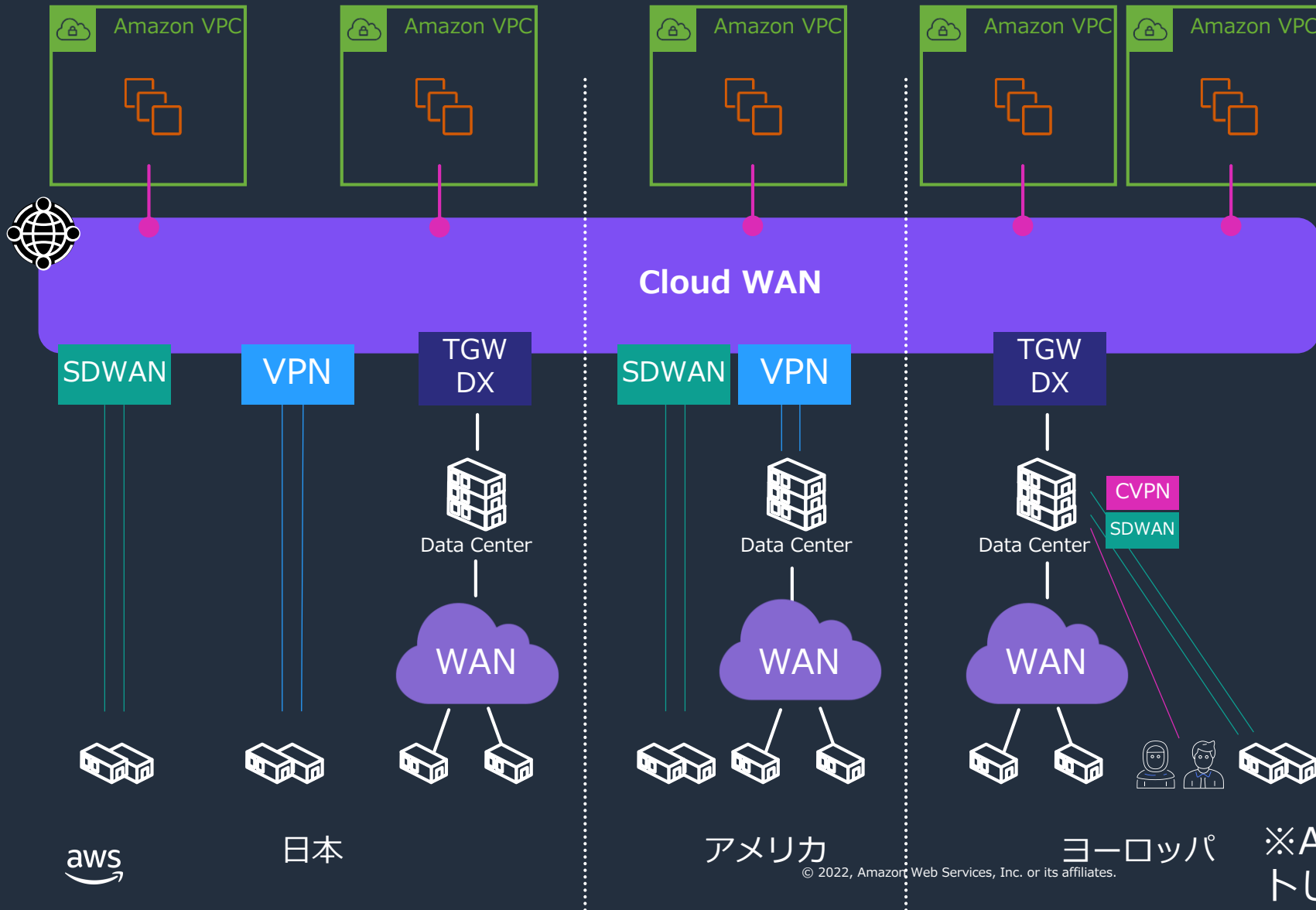
AWS Network Manager



Core Network Policy(CNP)



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)
Transit Gateway RTBs

※AWS Direct Connectは現在サポ
ートしておりません。

まとめ

まとめ

- AWS Cloud WANはグローバルに展開されているVPCやオンプレミス拠点に対し、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。

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!

Appendix

参考資料

[Introducing AWS Cloud WAN\(英語ブログ\)](#)

[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 \(Black Belt 日本語資料\)](#)

Cloud WANサンプル画面

Core Network Policy

ポリシーの作成

ネットワークポリシーは、セグメントと AWS リージョン間でネットワークトラフィックを制御する宣言型言語です。 [詳細はこちら](#)

ポリシービューモードの選択

ビジュアルエディタ

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

全般設定

バージョン

2021.12

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

アタッチメントとセグメントの紐づけ

Core Network Policy : ネットワーク設定

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

全般設定

バージョン: 2021.12 | VPN ECMP サポート: はい

編集

ASN の範囲 (1)

編集 | 削除 | 作成

Q ASN の範囲を検索

< 1 > ⚙

<input type="checkbox"/>	から	▲	▼	まで
<input type="checkbox"/>	64516			64999

内部 CIDR ブロック

編集 | 削除 | 作成

Q 内部 CIDR ブロックを検索

< 1 > ⚙

■ CIDR ▲

内部 CIDR ブロックがありません
表示する内部 CIDR ブロックがありません。

エッジロケーション (3)

編集 | 削除 | 作成

Q エッジロケーションを検索

< 1 > ⚙

<input type="checkbox"/>	場所	▲	▼	ASN	▼	内部 CIDR ブロック	▼
<input type="checkbox"/>	アジアパシフィック (東京)			64516		-	
<input type="checkbox"/>	アジアパシフィック (シンガポール)			64517		-	
<input type="checkbox"/>	米国東部 (バージニア北部)			64518		-	

Core Network Policy : セグメント

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

セグメント (3)

編集

削除

作成

🔍 セグメントを検索

< 1 > ⚙️

<input type="checkbox"/>	名前 ▲	エッジロケーション ▼	説明 ▼	アタッチメント承諾を必須にする ▼	分離されたアタッチメント ▼	セグメントリストの許可 ▼	セグメントリストの拒否 ▼
<input type="checkbox"/>	development	us-east-1, ap-southeast-1, a...	-	いいえ	いいえ	-	shared
<input type="checkbox"/>	production	us-east-1, ap-southeast-1, a...	-	いいえ	いいえ	-	shared
<input type="checkbox"/>	shared	-	-	はい	いいえ	-	-

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)

共有 を検索

編集 削除 作成

< 1 > ⚙️

<input type="checkbox"/>	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	▼
<input type="checkbox"/>	development		shared		-	
<input type="checkbox"/>	production		shared		-	

ルート (5)

ルート を検索

編集 削除 作成

< 1 > ⚙️

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

Core Network Policy : アタッチメントポリシー

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**

アタッチメントポリシー (3)

[編集](#) [削除](#) [作成](#)

🔍 アタッチメントポリシーを検索

< 1 > ⚙️





<input type="checkbox"/>	ルール番号 ▲	説明 ▼	アタッチするセグメント ▼	承諾を必須にする ▼	条件 ▼	オペレーター ▼	条件値 ▼	条件ロジック ▼
<input type="checkbox"/>	1	-	shared	-	tag-value	equals	key=segment, value=shared	and
<input type="checkbox"/>	2	-	production	-	tag-value	equals	key=segment, value=production	and
<input type="checkbox"/>	3	-	development	-	tag-value	equals	key=segment, value=development	and

Network Manager : ジオグラフィ

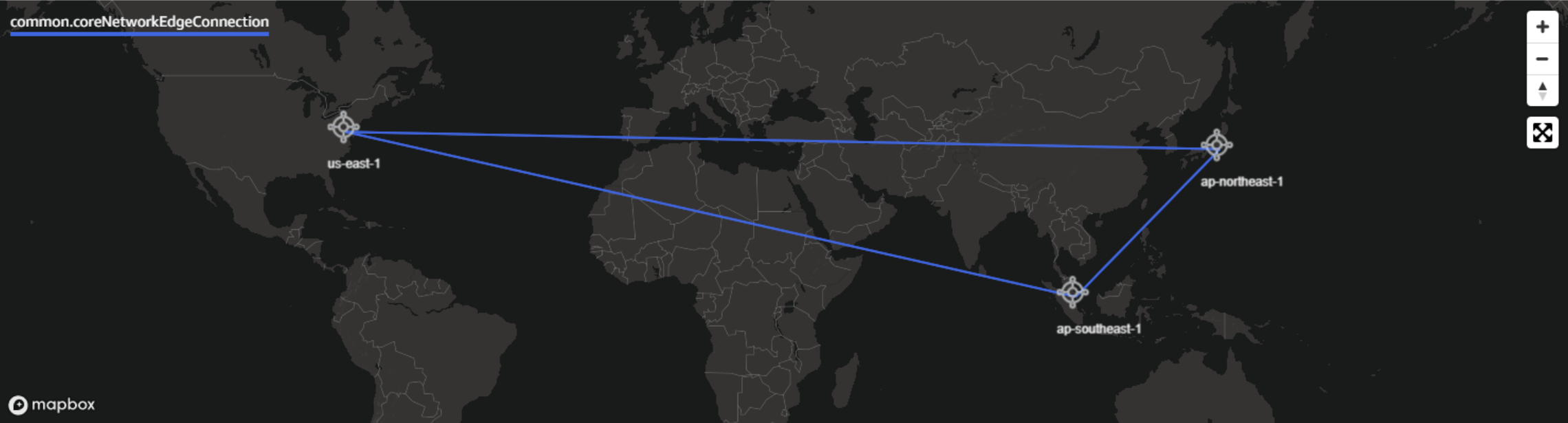
概要 | 詳細 | 共有 | トポロジグラフ | トポロジツリー | セグメント | ルート | イベント | モニタリング

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 3	 セグメント 3	 デバイス 0	 サイト 0
--	--	---	--

Geography



common.coreNetworkEdgeConnection

us-east-1

ap-northeast-1

ap-southeast-1

mapbox

Network Manager : トポロジーツリー

コアネットワーク

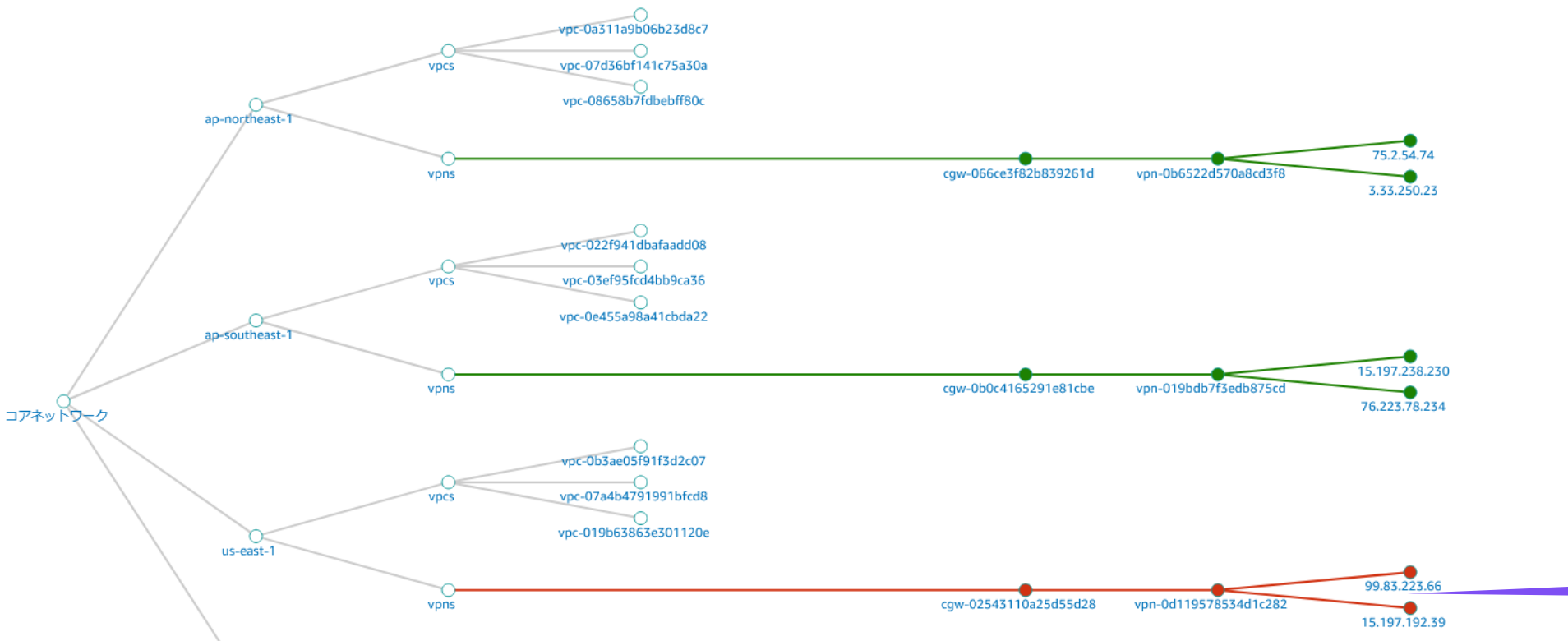
概要 | 詳細 | 共有 | トポロジグラフ | **トポロジツリー** | セグメント | ルート | イベント | モニタリング

トポロジツリー

This view represents the topology tree of your global network. You can perform the following actions in this page: swipe left of right to see your entire network, click on a node to expand or collapse the tree, and click on the text of an individual resource to view details.



Show: サイト デバイス カスタマーゲートウェイ セグメント



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

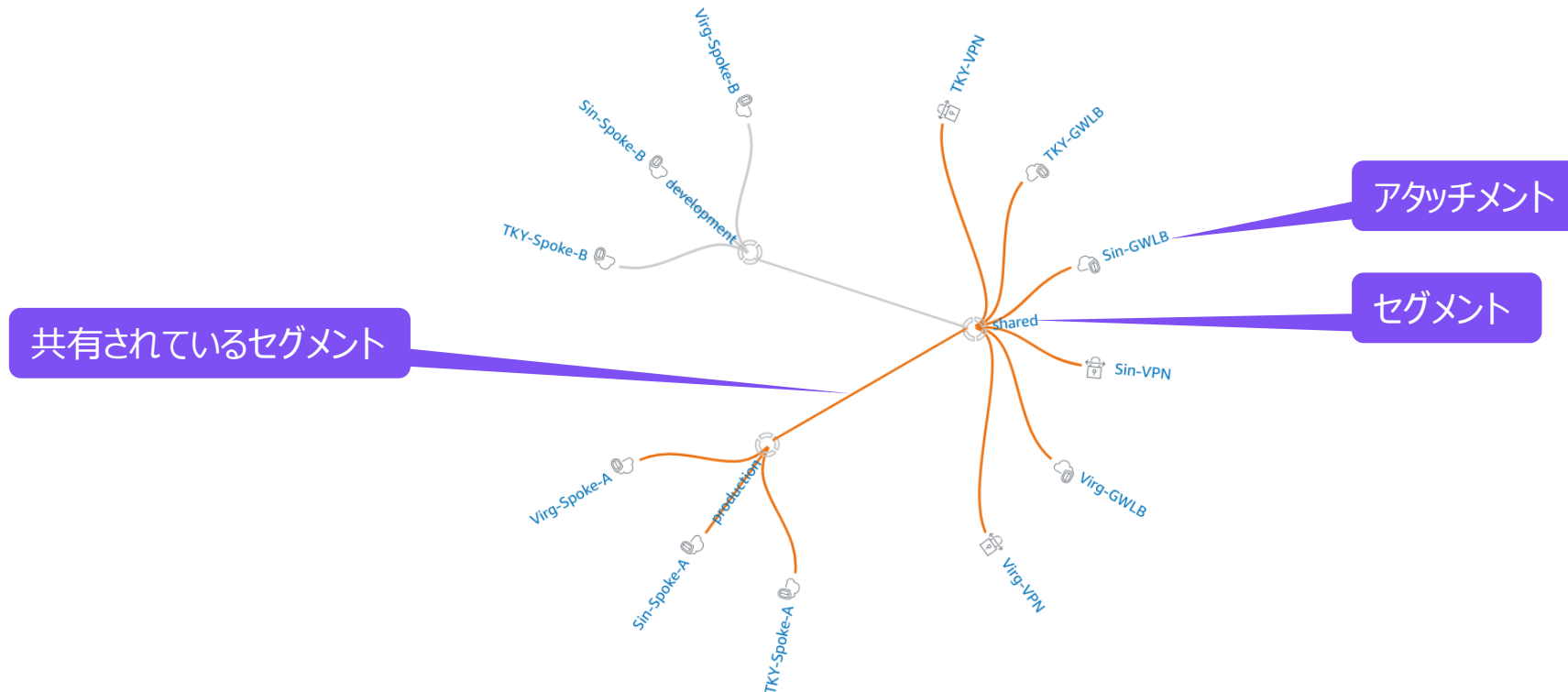
Logical

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

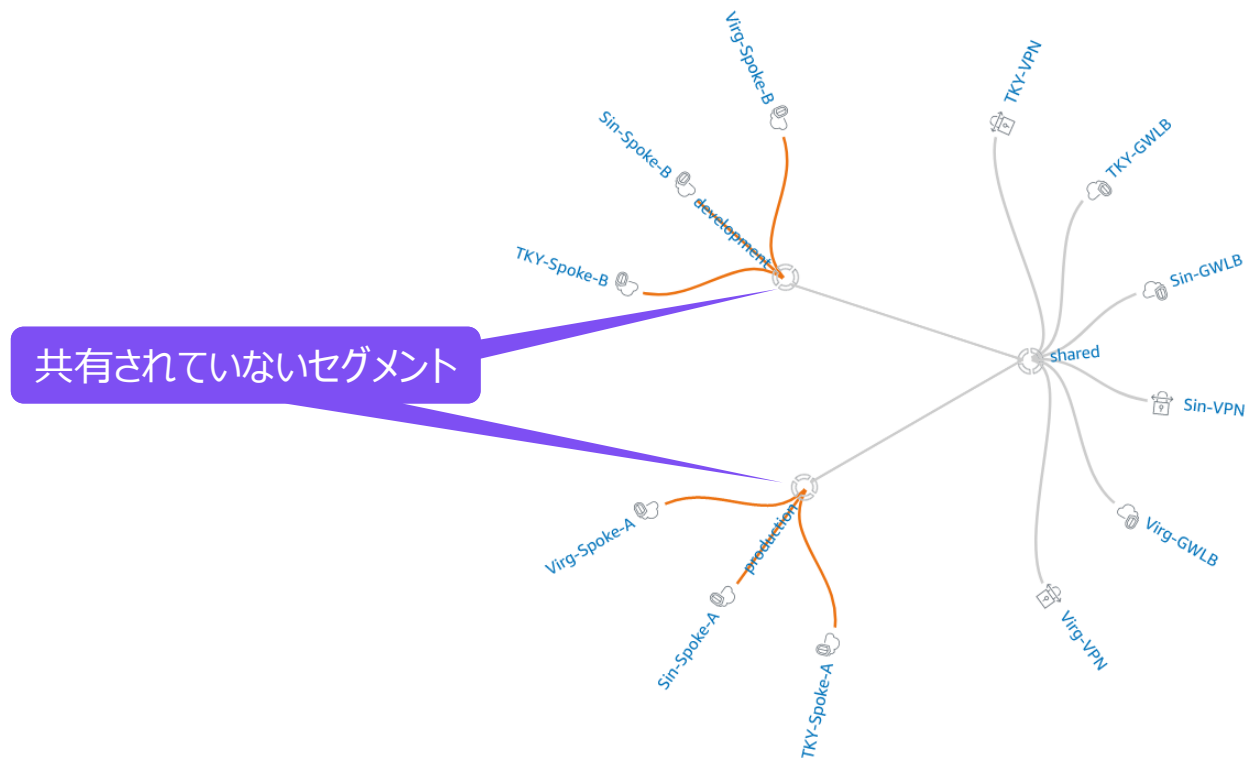
Logical

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