大規模環境をAWS Transit Gatewayで設計/移行する前に考える3つのポイントと移行への挑戦

宮崎幸恵
プロダクト統括本部プロダクト開発統括室
開発ディレクション室インフラソリューションユニット

株式会社リクルート

aws SUMMIT ONLINE

Agenda

1. AWS共通基盤について
2. AWS Transit Gateway検討の背景
3. 既存の仕組みからの移行に向けての検討
4. 移行時の検討ポイント
5. まとめ

AWS共通基盤について

aws SUMMIT ONLINE

発表者紹介

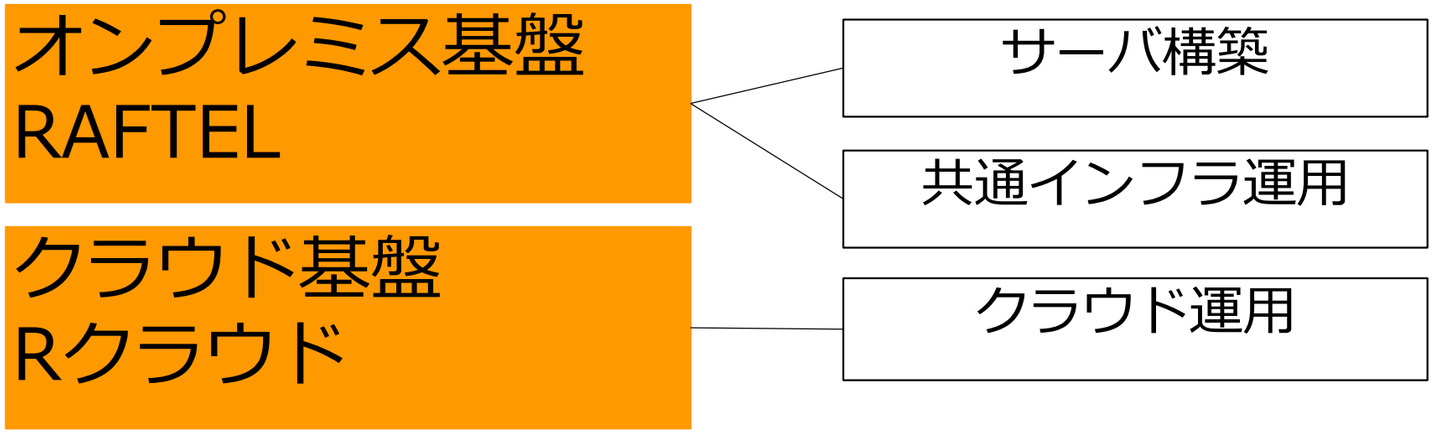
宮崎 幸恵

株式会社リクルート
プロダクト統括本部プロダクト開発統括室
開発ディレクション室インフラソリューションユニット
サイトリライアビリティエンジニアリング部　クラウドグループ

2011年　株式会社リクルート入社
入社当初から全社クラウド基盤の設計/運用業務に従事

リクルートのクラウド基盤について

リクルートでは、大きく2つのサービス向けインフラを運用



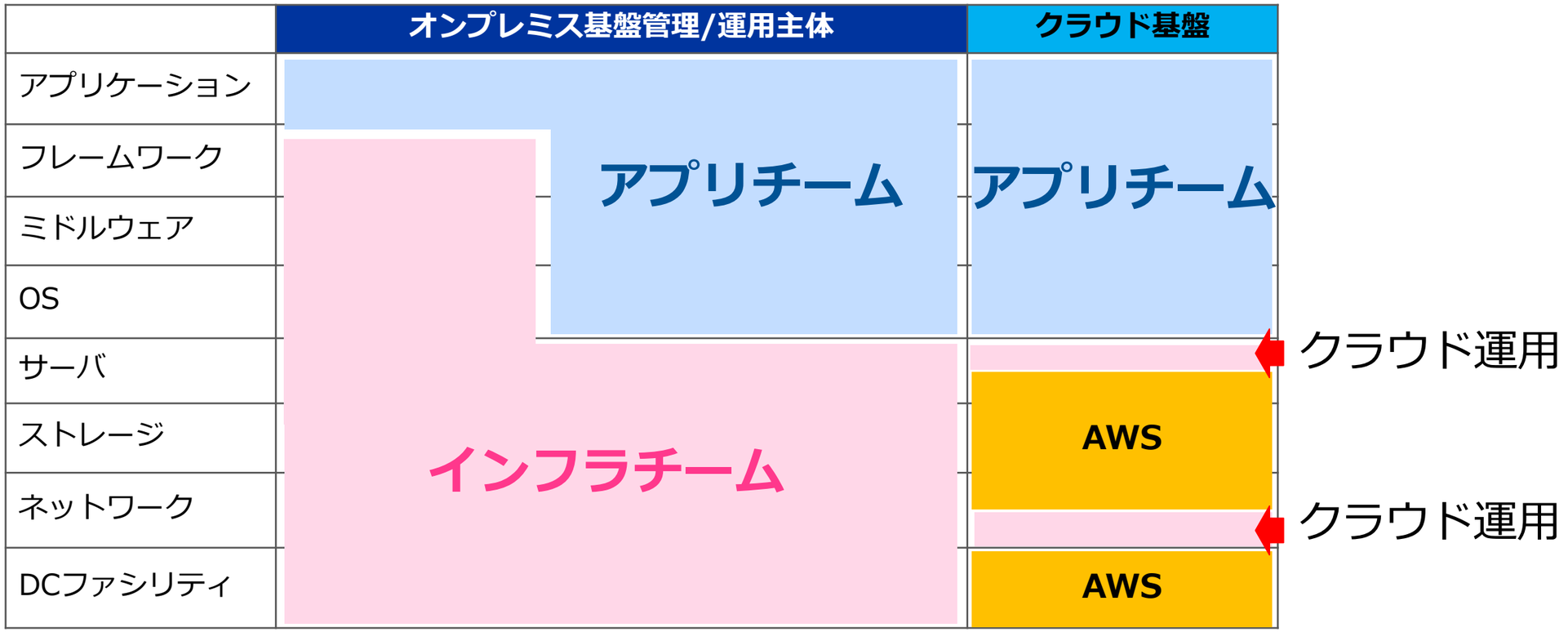
AWS基盤としての対応範囲

責任共有モデルで、ユーザー側の責任範囲となっている
一部の機能を共通提供

クラウド基盤におけるインフラチームの役割

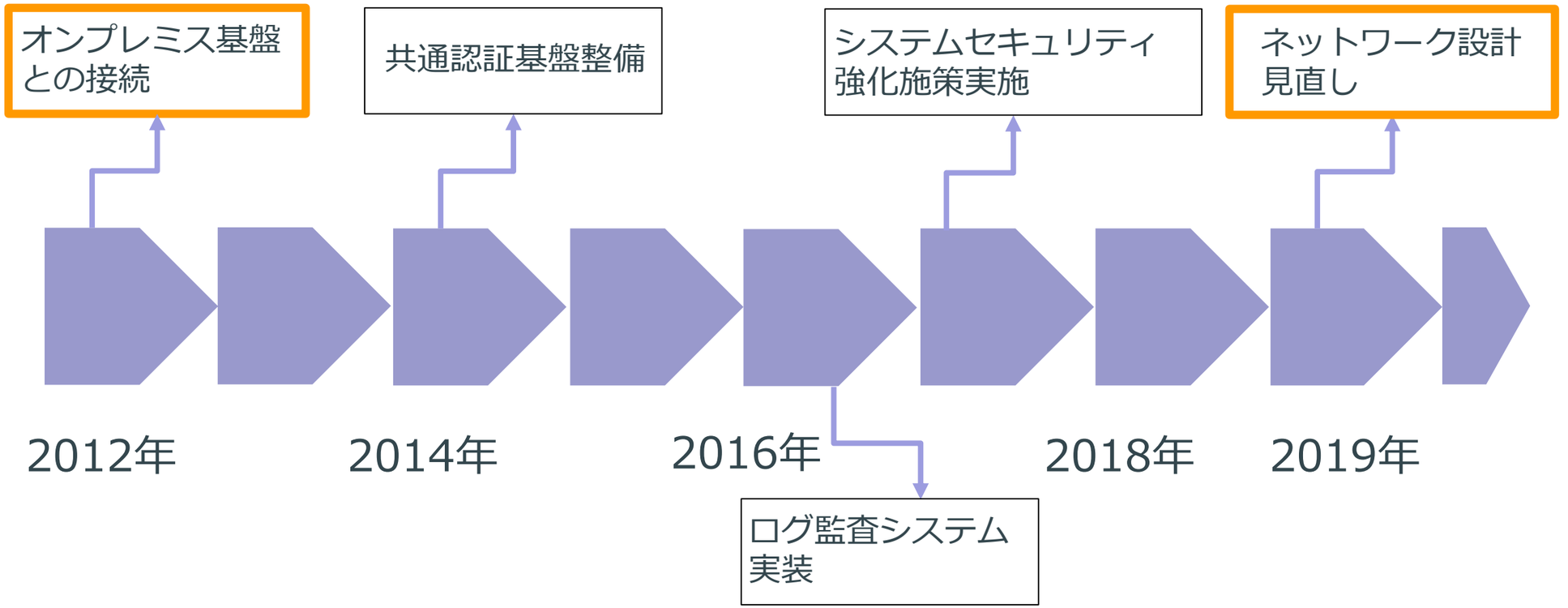
アプリサイド/サービスインフラサイド/基盤運用がはっきり分かれているのが特徴

またここには記載のない非機能要件（ID/認証等）の対応もしている



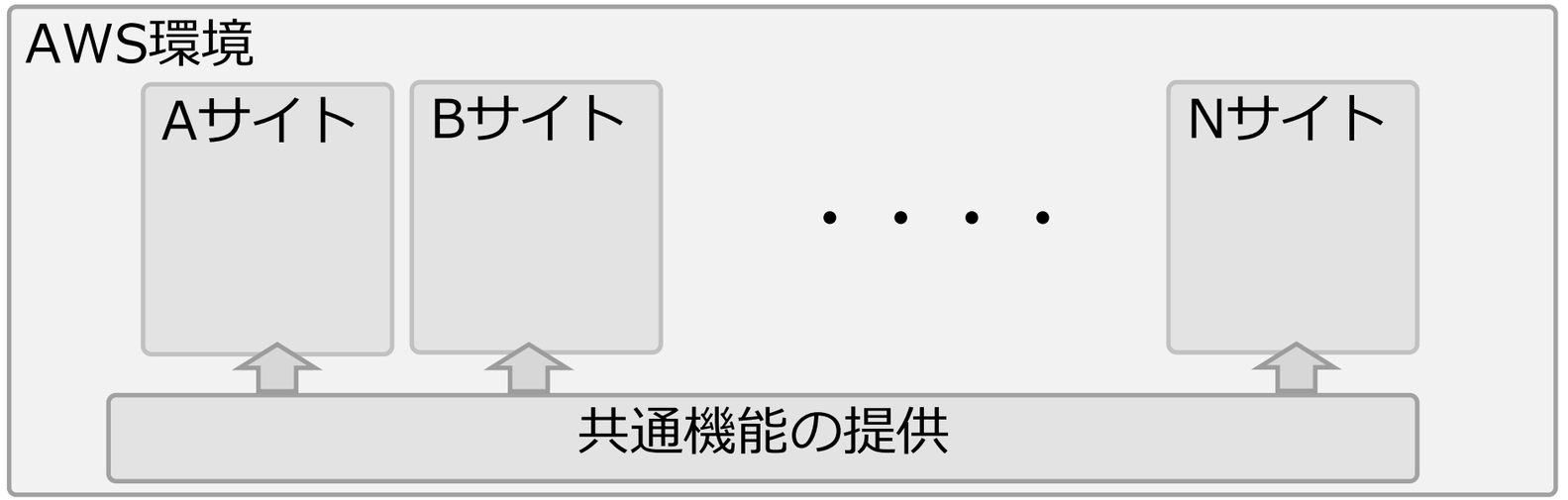
AWS基盤のこれまで

AWS基盤自体は2011年から提供開始



提供している共通機能について

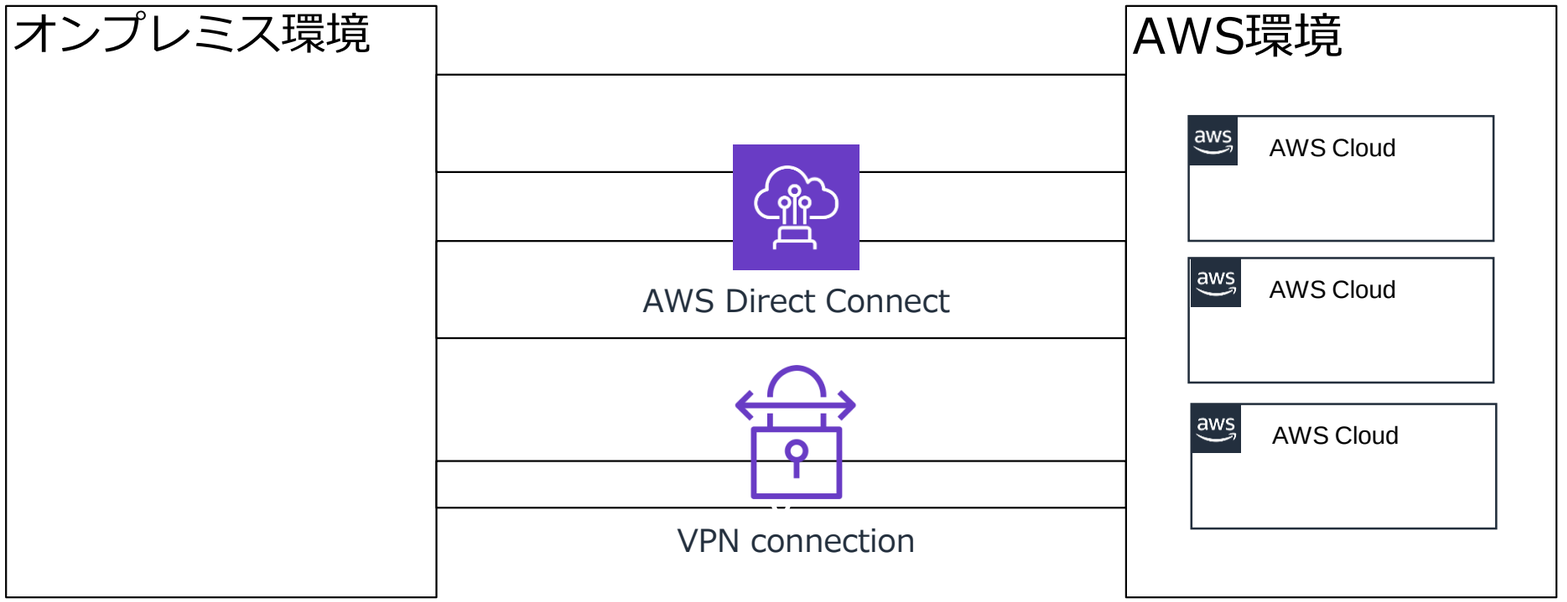
主に3つの共通機能を全環境に対して提供



分類	機能
ネットワーク	他インフラとの接続 AWS基盤内仮想NW設計
ID/認証/共通ログ保管	ID・認証/ログ保管
契約・コスト管理	全体契約・各アカウントごとのコスト管理

ネットワークの共通機能

ネットワークの共通機能として、オンプレミス環境との専用線/VPN接続を提供

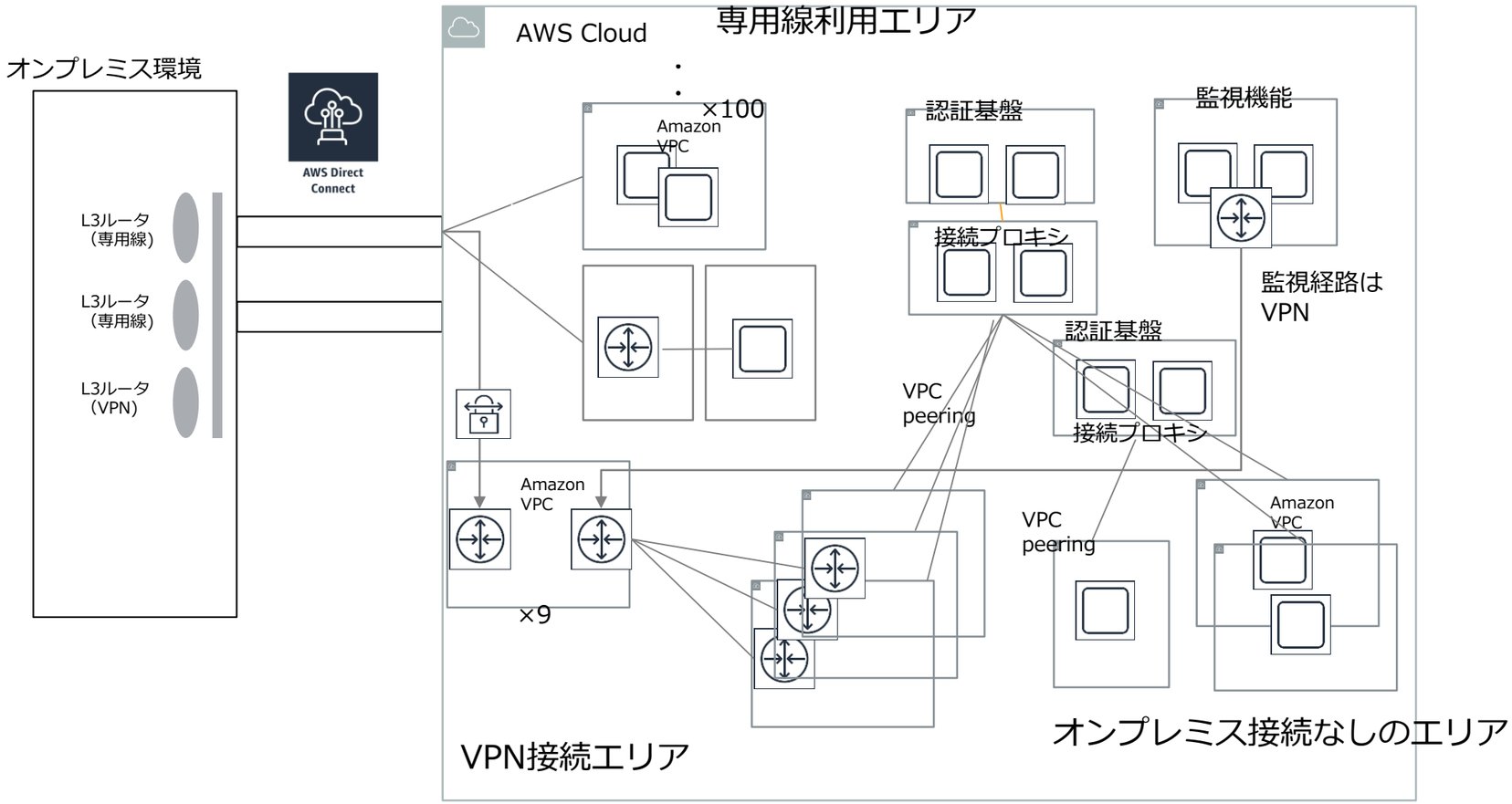


AWS Transit Gateway検討の背景

aws SUMMIT ONLINE

ネットワーク構成の課題

オンプレミス環境との接続は、当初からのつぎはぎ構成となっており、複雑化していた



複雑化の理由

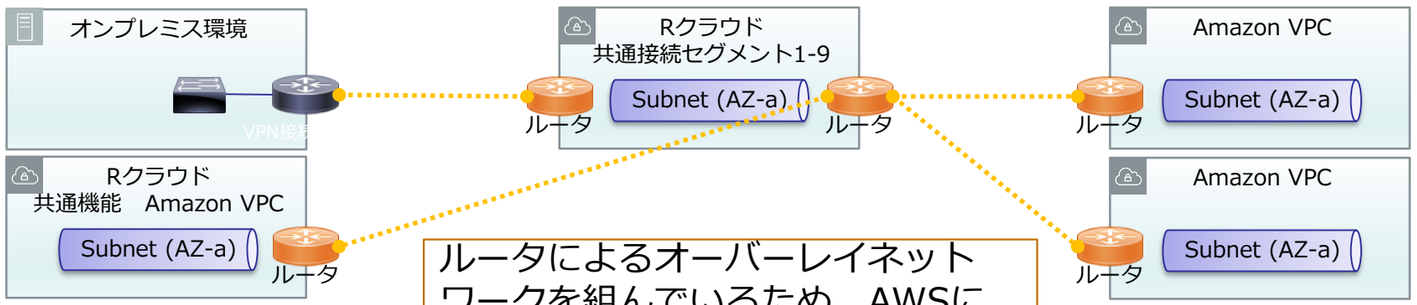
用途に応じてVPN/専用線を使い分け
AWSの機能で実現できない箇所は独自実装

主な用途	構成	接続VPC数
オンプレミス環境とのデータ連携/バッチ連携	専用線（AWS Direct Connect利用）	100
オンプレミス環境の一部共通機能の利用	VPN接続（独自ルータで実装）	300
AWS基盤内の共通機能との接続	VPC Peeringが主だが、一部VPN接続（独自ルータで実装）	600

VPN接続でトランジットしていた理由

接続VPCが初期段階から100近くあり、頻繁に追加/削除があったことから、AWSの機能は使わずVPNルータを利用し、独自実装していた

■VPN接続構成



ルータによるオーバーレイネットワークを組んでいるため、AWSによる制限を受けず、自由にNWを構成できる

ルータの独自管理は非常に負荷が高く、品質低下にも苦しんでいた

AWS Transit Gateway

2018年のre:InventでAWS Transit Gateway発表
その後東京リージョンには、2018/12に対応

AWS News Blog

New – Use an AWS Transit Gateway to Simplify Your Network Architecture

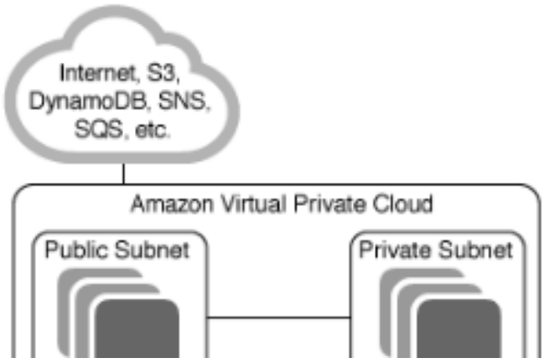
by Jeff Barr | on 26 NOV 2018 | in Amazon VPC, AWS Re:Invent, Launch, News | Permalink | Share

▶ 0:00 / 0:00

Voiced by Amazon Polly

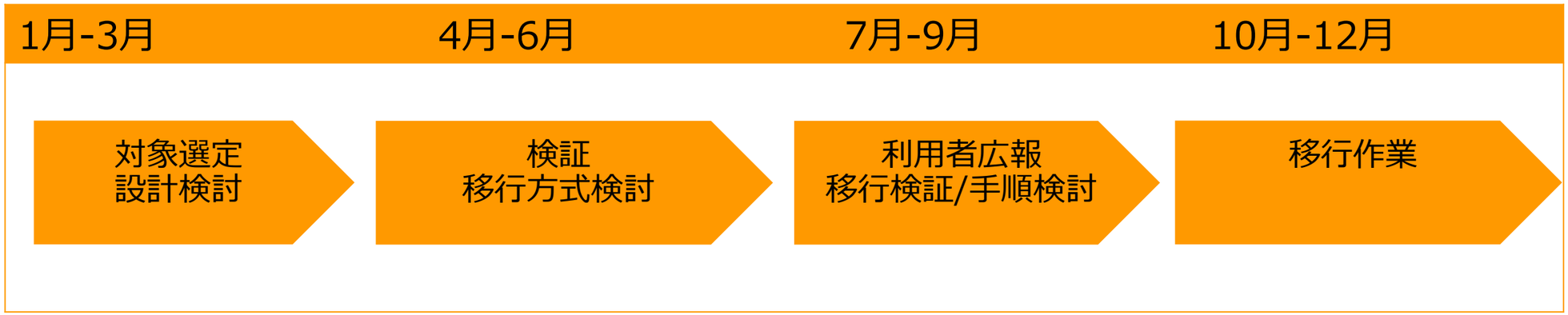
It is safe to say that Amazon Virtual Private Cloud is one of the most useful and central features of AWS. Our customers configure their VPCs in a wide variety of ways, and take advantage of numerous connectivity options and gateways including AWS Direct Connect (via Direct Connect Gateways), NAT Gateways, Internet Gateways, Egress-Only Internet Gateways, VPC Peering, AWS Managed VPN Connections, and PrivateLink.

Because our customers benefit from the isolation and access control that they can achieve using VPCs, subnets, route tables, security groups, and



AWS Transit Gatewayへの移行検討

2019年初からAWS Transit Gatewayへの移行検討開始
最終的には12月までの約1年をかけて移行完了



既存の仕組みからの移行に向けての検討

aws SUMMIT ONLINE

移行対象について

全てAWS Transit Gatewayにするのではなく一部のみ移行検討

主な用途	構成	接続VPC数	移行対象
データ連携/バッチ連携	専用線	100	×
オンプレミス側の一部共通機能の利用	VPN接続	300	○
AWS基盤内の共通機能との接続	VPC Peeringが主だが、一部VPN接続	600	一部のみ○

選定の理由について

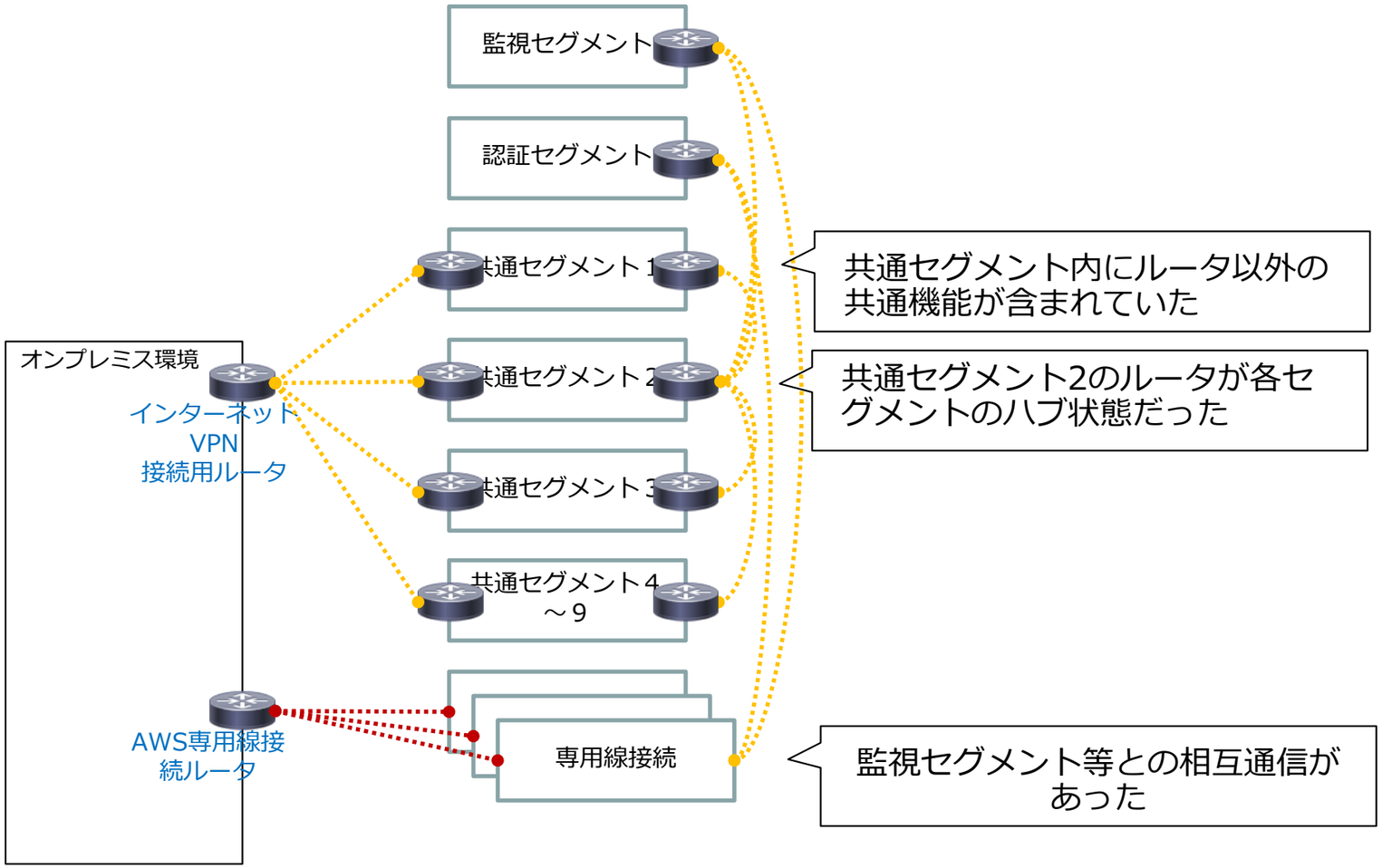
認証機能については、アクセス制御要件があり、それをVPC Peering前提で実装していたため移行対象外とした

主な用途	構成	接続VPC数	移行対象
AWS基盤内の共通機能との接続	VPC Peeringが主だが、一部VPN接続	600	一部のみ〇

主な用途	移行対象	理由
認証機能との接続	×	VPC Peering前提で接続先のアクセス制御を独自実装していたため
監視/モニタリング機能との接続	〇	独自実装要件がない
ログ収集との接続	〇	独自実装要件がない

設計の検討

複数のセグメントが存在し、相互に役割が違う機能が混ざっていた



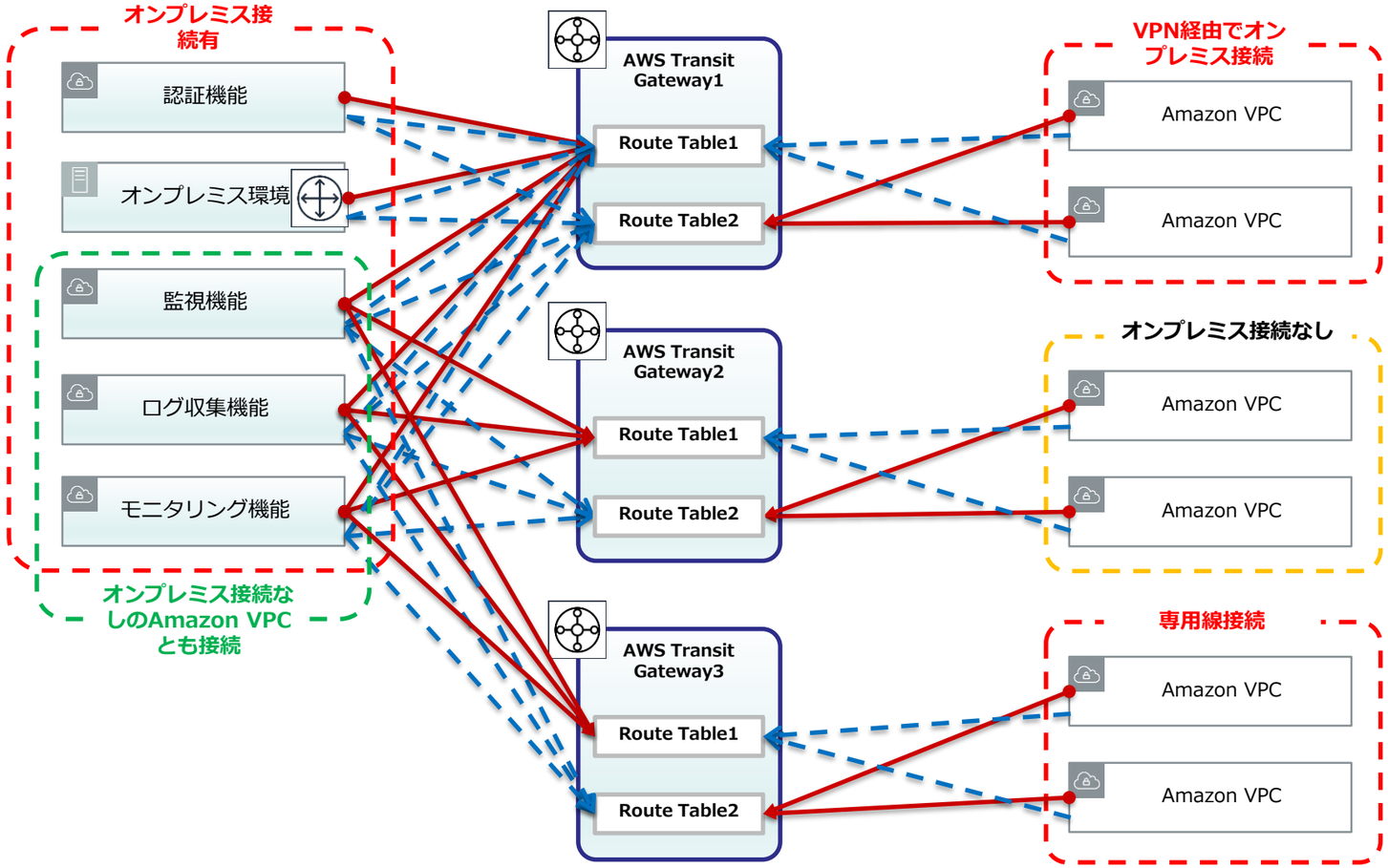
設計の検討

オンプレミスのセグメントと接続があるかどうかでAWS Transit gatewayを分けるか、用途との掛け合わせで分けるかの検討

案	Transit Gateway数		メリット/デメリット
A	2	既存のオンプレミスとのVPN接続をすべてAWS Transit gateway 1 に置き換え、それ以外の通信をAWS Transit Gateway 2 に集約する	• 今後セグメントが追加された際にも設定変更不要 • 専用線接続Amazon VPC側でのルートテーブル設定次第ではオンプレミス側へVPN経路での接続が可能（※意図しない通信ができてしまう）
B	3	案 1 の 2 つのAWS Transit Gatewayはそのまま、専用線接続VPCからのパケットがオンプレミス側に流れてこない構成とするため、専用線接続専用のAWS Transit Gateway 3 を増やす	• 今後セグメントが追加された際には設定の追加が必要 • 専用線接続Amazon VPC側でのルートテーブル設定には関係なくオンプレミス側へVPN経路での接続は不可 採用
C	3	用途別（共通機能との通信/オンプレミスとの通信)にAWS Transit Gatewayを分離する	• 今後セグメントが追加された際には設定の追加が必要 • 専用線接続Amazon VPC側でのルートテーブル設定には関係なくオンプレミス側へVPN経路での接続は不可 • 用途別のため、つなぐ先のアカウントAmazon VPCに、複数のAWS Transit Gatewayと接続するためのAttachmentが複数必要になってしまう場合があり、利用料金と構成管理の複雑さが増す

設計の検討

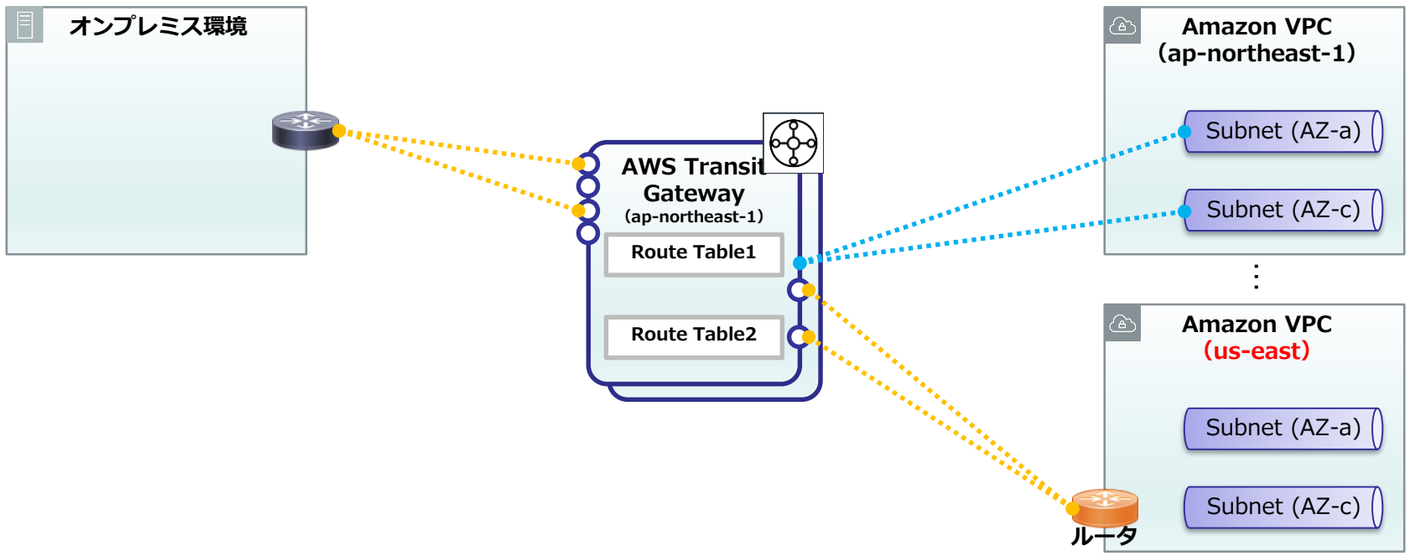
設計は以下の構成とした



設計の検討

ほぼ東京リージョンだが、一部VPN接続が必要なAmazon VPCが東京以外のリージョンに存在していた

移行時は東京リージョンのインターリージョン接続に対応していなかったので、そのままルータ-AWS Transit Gateway間のVPN接続で設定



設計の検討

アカウントならびにAmazon VPCが非常に多いので、上限値にあたらないかの検討も事前に実施

項番	項目	利用数(予定)	上限	備考
1	アカウントあたりの AWS Transit Gateway Attachmentの数	650	5,000	共通系Amazon VPCが利用するAWS Transit Gateway Attachmentは12程度のため、サイト用Amazon VPCの数が上限に達する要因になる。1Amazon VPCが1 Attachmentを利用するので、5,000サイト用Amazon VPC程度で上限に達する
2	VPN 接続ごとの帯域幅	不明	1.25 Gbps	今後増えた際は、ここがボトルネックとなる可能性があり
3	Amazon VPC 接続ごとの帯域幅 (バースト)	不明	50 Gbps	Amazon VPC間でそれほど帯域を必要とする処理は行っておらず、本項目は今後も問題とならない。
4	アカウントあたりの AWS Transit Gateway の数	3	5	今以上にAWS Transit gatewayを分けるメリットが感じられないので、本項目は今後も問題にならないと考える。申請により上限緩和可能
5	Amazon VPC あたりの AWS Transit Gateway Attachmentの数	3	5	今以上にAWS Transit gatewayを分けるメリットが感じられないので、本項目は今後も問題にならないと考える。
6	AWS Transit gatewayあたりの Route Tableの数	2	20	Route Tableを3つ以上にするケースは想定していないため本項目は今後も問題にならないと考える。申請により上限緩和が可能
7	AWS Transit Gateway Route Table当たりのルート数	660	10,000	Amazon VPCからのPropagationにより、AWS Transit Gateway Route Tableのルートが1つ増えると考えられるので、サイト用Amazon VCPの数が上限に達する要因となる。が現状ではおそらく問題ない。
8	Amazon VPCのルートテーブルエントリ数	～100	1,000 (100以内が推奨値)	宛先IPアドレスをある程度集約したルーティングを設定することで、上限に達することはないと考える。
9	セキュリティグループ当たりのインバウンドルールまたはアウトバウンドルールの数	50	60×5 =300	今後ルールが増える要因は特にない

移行の検討

用途の異なる機能が複数含まれたため影響範囲と万一の際の切り戻しのしやすさもふまえて、全部で7回に分けて移行

フェーズ	作業内容	影響範囲	実施期間
1	AWS Transit Gateway 1、2、 3の作成	影響なし	10月
	監視経路をAWS Transit Gatewayに切り替える	1 Amazon VPC	
2	監視経路をAWS Transit Gatewayに切り替える	影響なし	
	ログ収集経路をAWS Transit Gatewayに切り替える	影響なし	
	モニタリング基盤との接続準備	影響なし	
3	AWS Transit Gateway 1の用意	影響なし	
	監視、ログ収集、モニタリング経路を準備	影響なし	
	共通セグメント９のVPN経路をAWS Transit Gateway経由に切り替える	60 Amazon VPC	11月
4	共通セグメント３－８のVPN経路をAWS Transit Gateway経由に切り替える	160 Amazon VPC	
5	共通セグメント1，2と共通機能間の通信を切り替える	90 Amazon VPC	
6	Peeringを経由している監視やログ収集やモニタリングの通信をAWS Transit Gateway経由に切り替える	80 Amazon VPC	12月
7	オンプレミス側VPNルーターの構成変更実施	VPN接続をしている全Amazon VPC	

移行時の検討ポイント

aws SUMMIT ONLINE

検討ポイント

設計時は以下3点を特に判断のポイントとした

- 構成がシンプルになるか
- ある程度の拡張性があるか
- 他の接続方法が適していると考えられないか

リリースされて間もないころから検討を開始したため、
AWSのプロフェッショナルサービスも活用

検討ポイント

移行時は以下3点を特に判断のポイントとした

- できるだけ同じ作業と影響が出る作業でまとめる
- 切り替え時の断時間が最短になる方法を検討する
- 既存の構成変更と移行は一緒におこなわない

設計時/移行時の課題

実際には設計時、移行時にいくつか後から発覚した問題はあった

- 東京リージョン以外への対応
  - 当初リージョンをまたいだアタッチメント付与ができず、途中で気づいて追加で方式検討/検証を実施
- AZ単位のアタッチメント付与
  - 2つ以上AZがある場合、片方にしか付与してなかったので、片側AZでしか当初疎通ができなかった。
  - 移行時に気付きアタッチメントを追加
- AWS Transit Gatewayでの監視とモニタリング
  - CloudWatchだけでは疎通が正しくできているかの確認までとれないため、どのようにモニタリングするかは課題としていまもある

移行後の所感

- 現在のところ大きな障害もなく非常に安定している
- マネージドサービスのため運用もしやすくなった

まとめ

aws SUMMIT ONLINE

AWS Transit Gateway移行時の3つのポイント

- ネットワーク関連の構成更改には設計にも移行にも事前検討が他のサービスに比べるとより重要
- AWSの上限値を意識しつつ、今後の拡張も踏まえての設計する
- 全ての変更ではなく、より適した箇所にサービスを適用する

Thank you!

aws SUMMIT ONLINE