
aws
SUMMIT
ONLINE

はてなにおける AWS Transit Gateway の導入と活用

渡辺 道和

SRE (Site Reliability Engineer) / シニアエンジニア

株式会社 はてな サービス・システム開発本部 システムプラットフォーム部

aws SUMMIT ONLINE

Who am I ?

- 渡辺 道和 / id:nabeop
  - 2018年3月に中途入社
- システムプラットフォーム部
  - はてなにおける基盤管理運用の横断部署
- 最近の趣味
  - AWS CDK を使ってインフラを Typescript で表現
- よく見ているサイト
  - https://github.com/aws/aws-cdk/projects/2

アジェンダ

- はてなにおけるサービス構成とネットワーク再構成の課題
- AWS Transit Gateway のおさらい
- ネットワーク再構成における AWS Transit Gateway の導入状況
- AWS Transit Gateway に AWS Direct Connect の接続する場合の課題と解決策

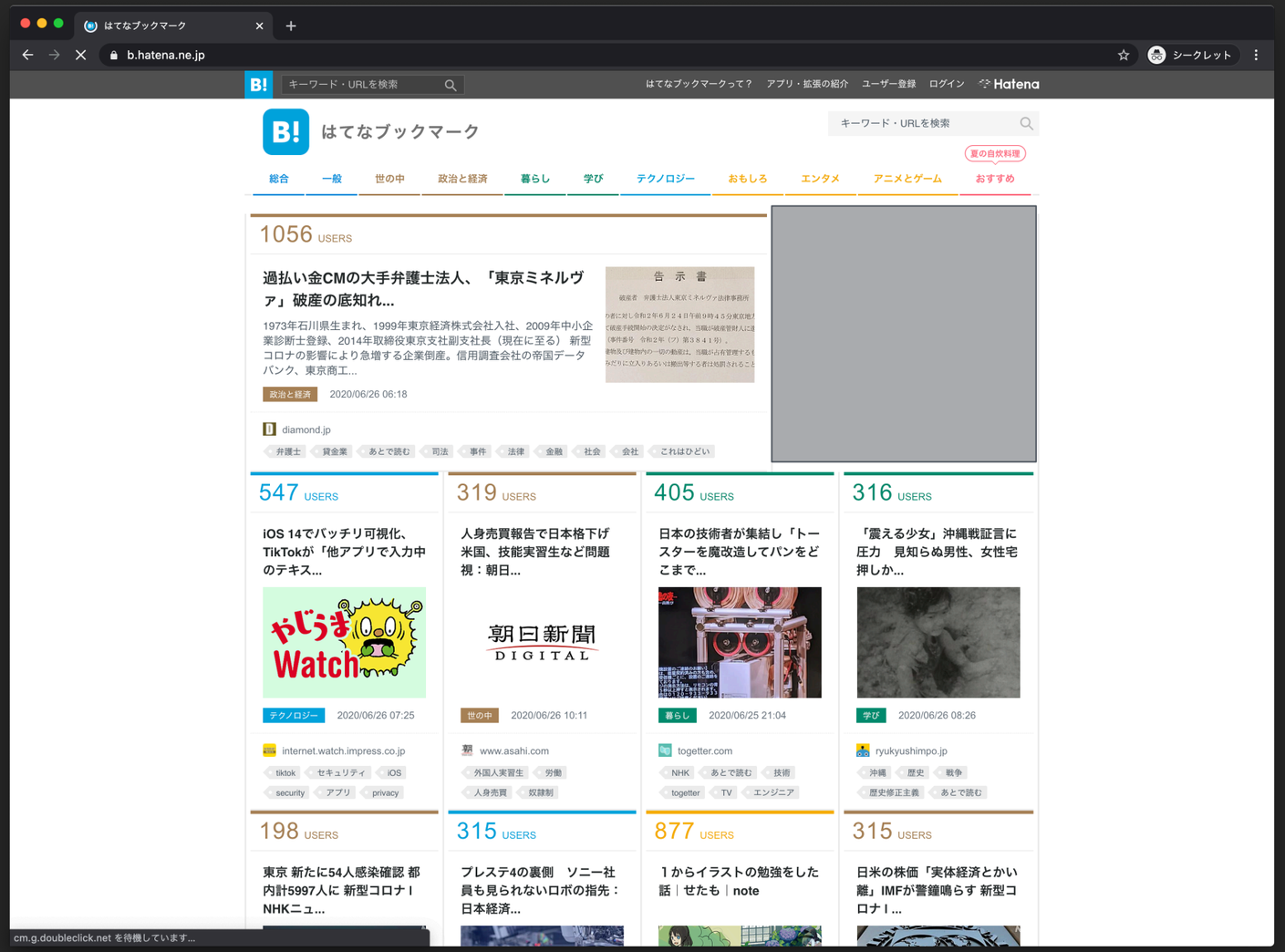
はてなにおけるサービス構成とネットワーク再構成の課題

aws SUMMIT ONLINE

人力検索 はてな (2001年 〜)

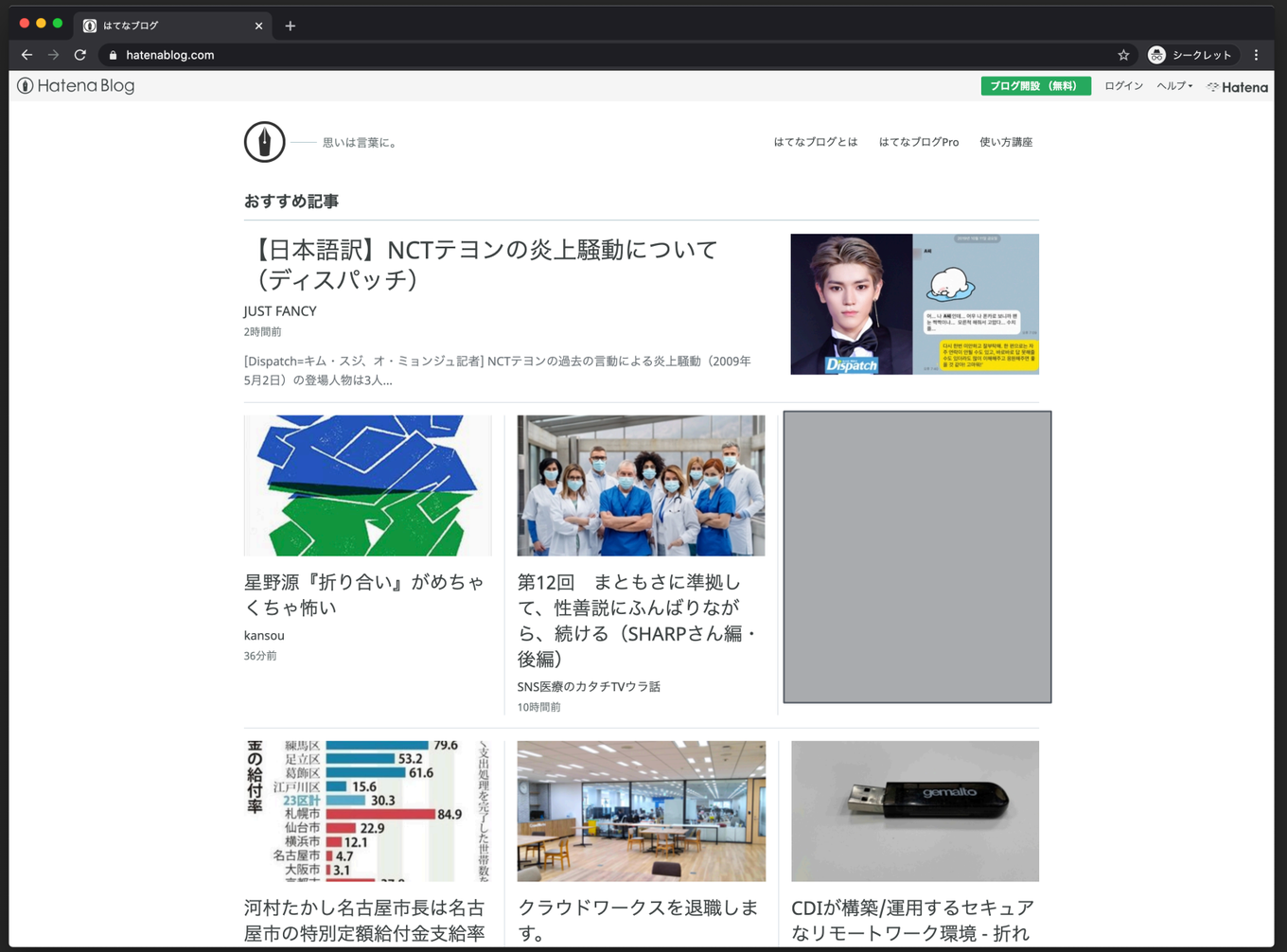
https://q.hatena.ne.jp/

はてなブックマーク (2005年〜)



https://b.hatena.ne.jp/

はてなブログ (2013年〜)



https://hatenablog.com/

はてなブログ Media (2014年〜)

https://www.hatena.ne.jp/contentmarketing/hatena-blogmedia

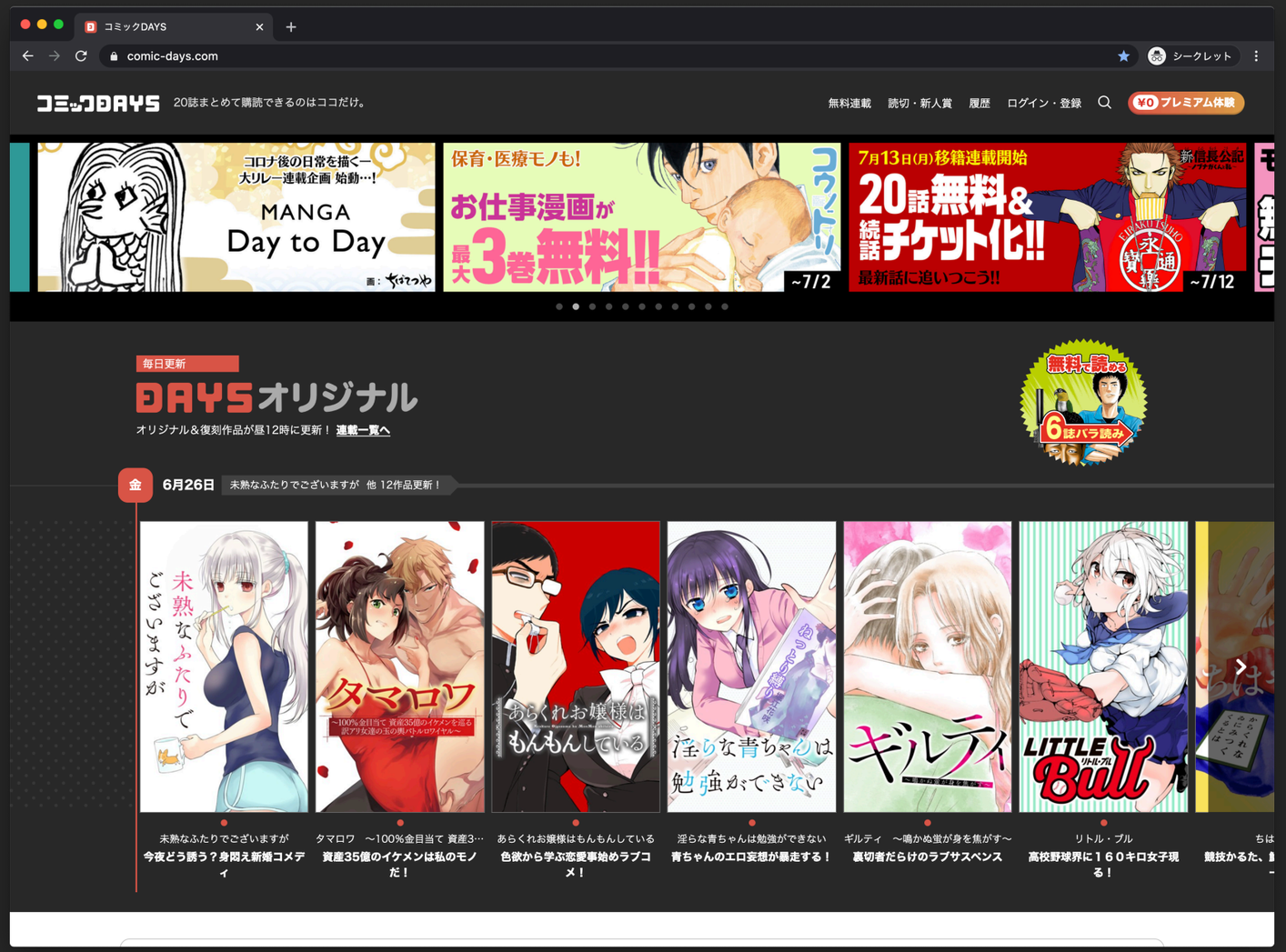
mackerel (2014年〜)

https://mackerel.io/

カクヨム (2016年〜)

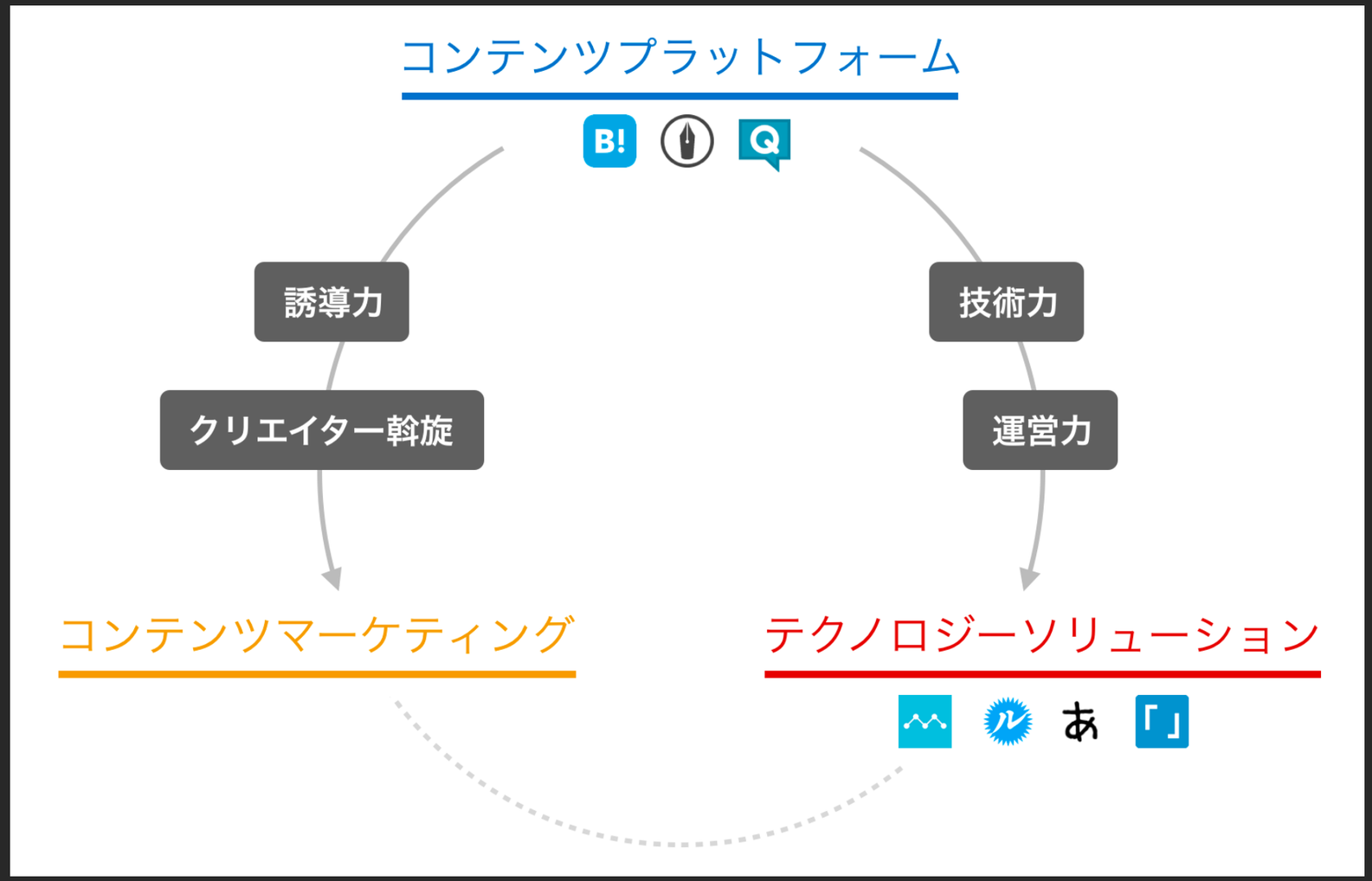
https://kakuyomu.jp/

コミックDAYS (2018年〜)



https://comic-days.com/

はてなのサービス



https://hatenacorp.jp/infomation/

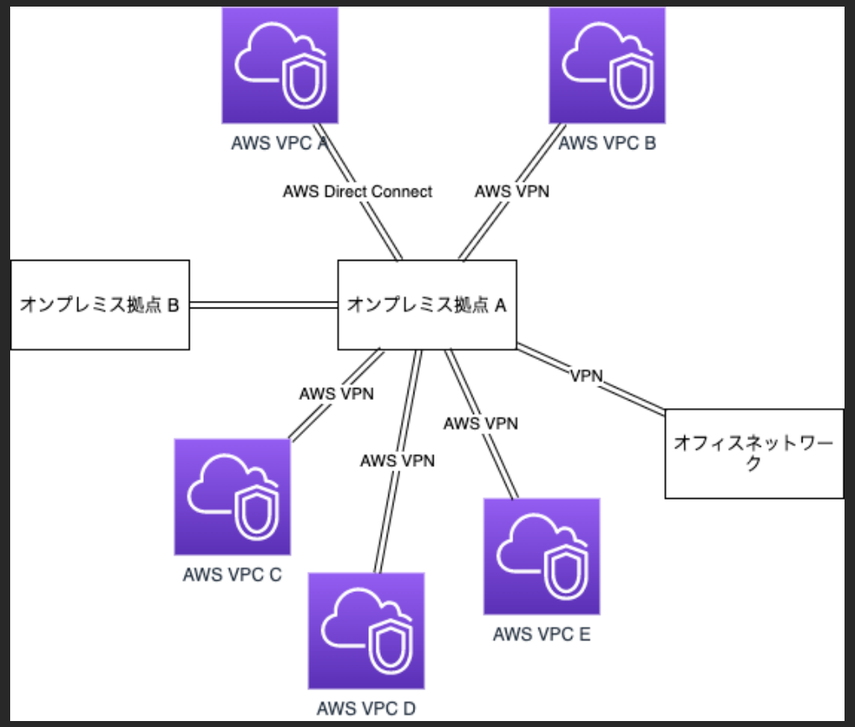
はてなのサービスと基盤部分の課題

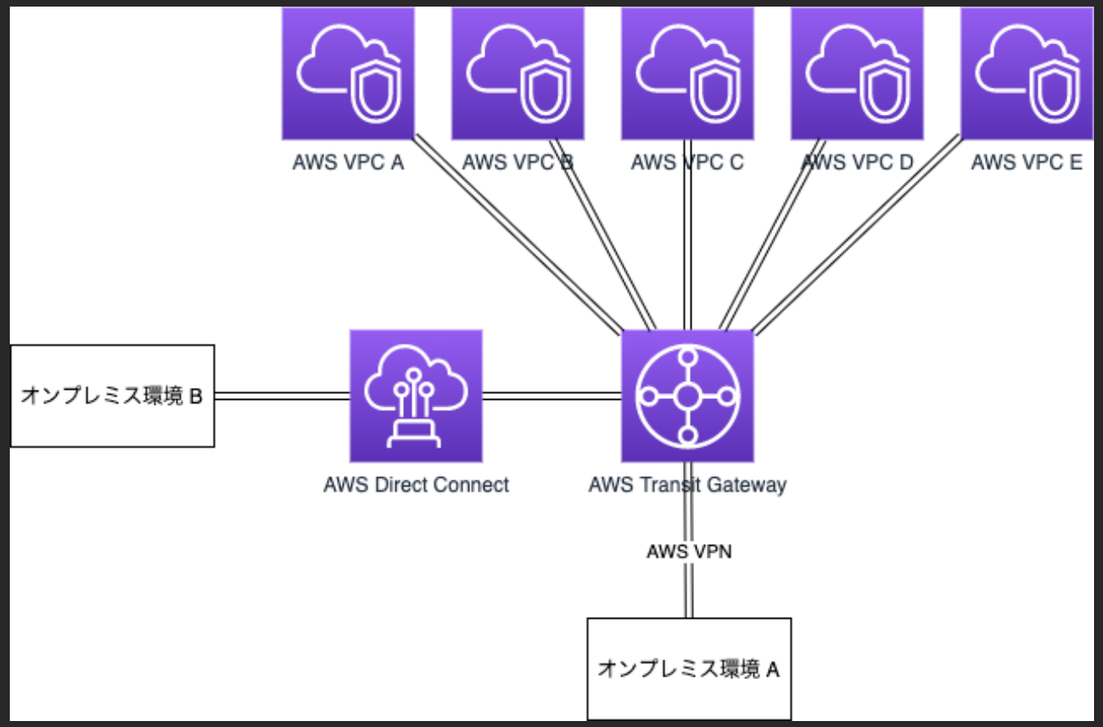
- サービスの性質
  - 異なる性質 (toC / toBtoC / toB 向け SaaS) のサービス
  - リリースから10年以上経っているサービスからリリースしたばかりのサービスまで構成に差異がある状態
- 基盤側の事情
  - AWS とオンプレミス環境のハイブリッドクラウド構成
  - 1つの Amazon VPC に複数の性質が異なるサービスを収容

内部ネットワークの整備

- AWS アカウントを分離してサービスごとの Amazon VPC を構築
  - Amazon VPC 同士は内部通信ができるようにネットワーク的な到達性を確保
  - 相互接続の管理コストを極力抑えたい
- サービス提供に影響しないネットワークの構成変更
  - 内部ネットワークのコア部分の構成変更なので作業影響がネットーワク全体に波及する可能性が高い

AWS Transit Gateway を中心にしたスター型ネットワークへの構成変更





AWS Transit Gateway についておさらい

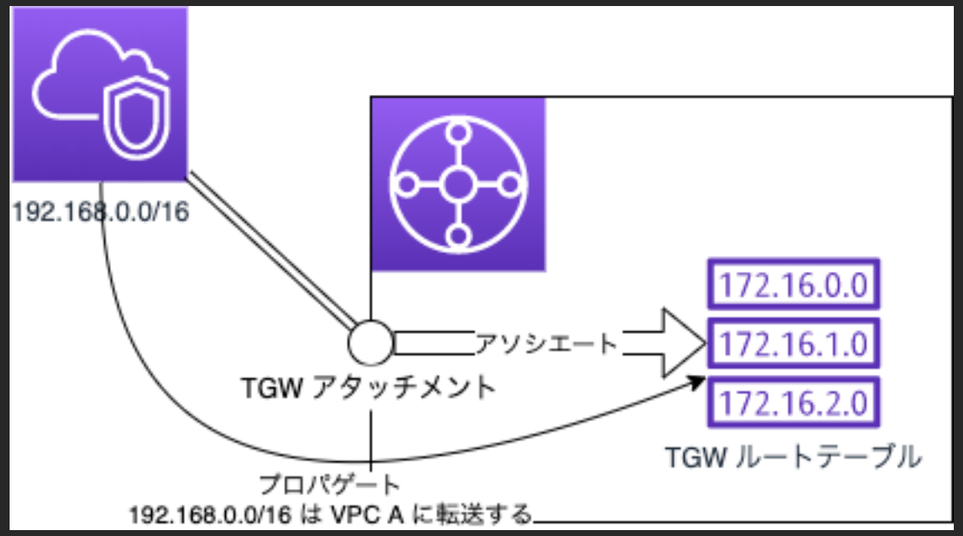
aws SUMMIT ONLINE

AWS Transit Gateway とは (話者の理解)

- AWS Site-to-Site VPN / AWS Direct Connect / Amazon VPC を相互接続できるゲートウェイ
- 中身は複数のルートテーブル
  - Amazon VPC におけるルートテーブルと極めて似ている
  - 単一のルートテーブルのみという運用も可能
- BGP による経路交換でオンプレミス環境の経路を AWS Transit Gateway のルートテーブルに経路伝播させる
- コスト的には VPC Peering のほうが安い

AWS Transit Gateway に AWS リソースを接続するときの各種用語

- アタッチ
  - Amazon VPC などの AWS リソースを AWS Transit Gateway に関連付ける
- アソシエート
  - AWS リソースのアタッチメントを AWS Transit Gateway のルートテーブルに接続する
- プロパゲート
  - AWS Transit Gateway のルートテーブルにアタッチメントから経路情報を伝播させる

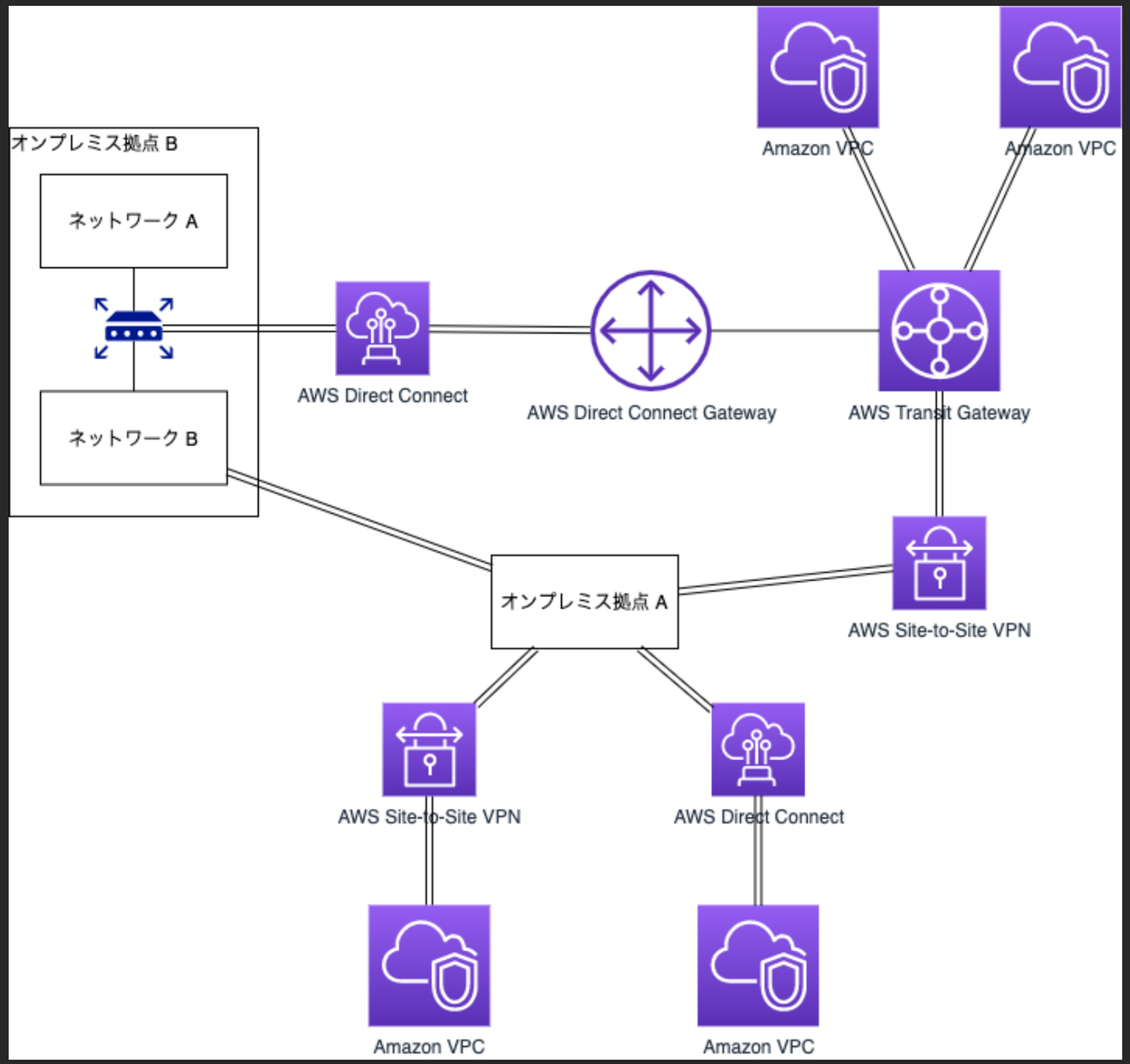


構成の概要

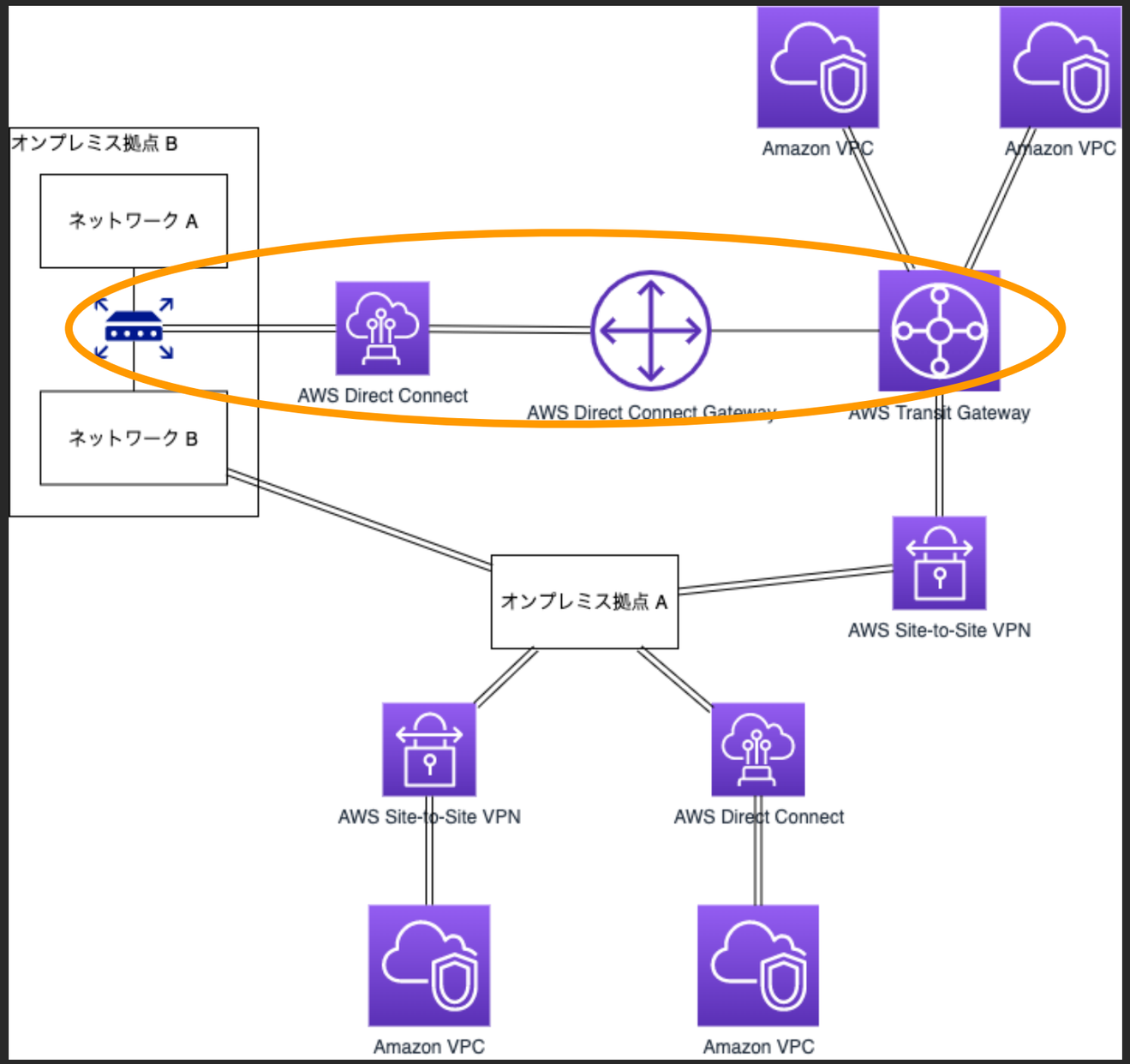
内部ネットワークの構成変更の履歴

- 2019/09
  - AWS Classic VPN のリプレースのため AWS Transit Gateway を導入
- 2019/12
  - オンプレミス環境の1つと AWS Transit Gateway を AWS Direct Connect で接続 ← 今日お話しする内容
- 2020/XX
  - オンプレミス環境と AWS Site-to-Site VPN で接続している AWS VPC を AWS Transit Gateway に収容変え

今回お話しするネットワークの全体像



今回お話しするネットワークの全体像

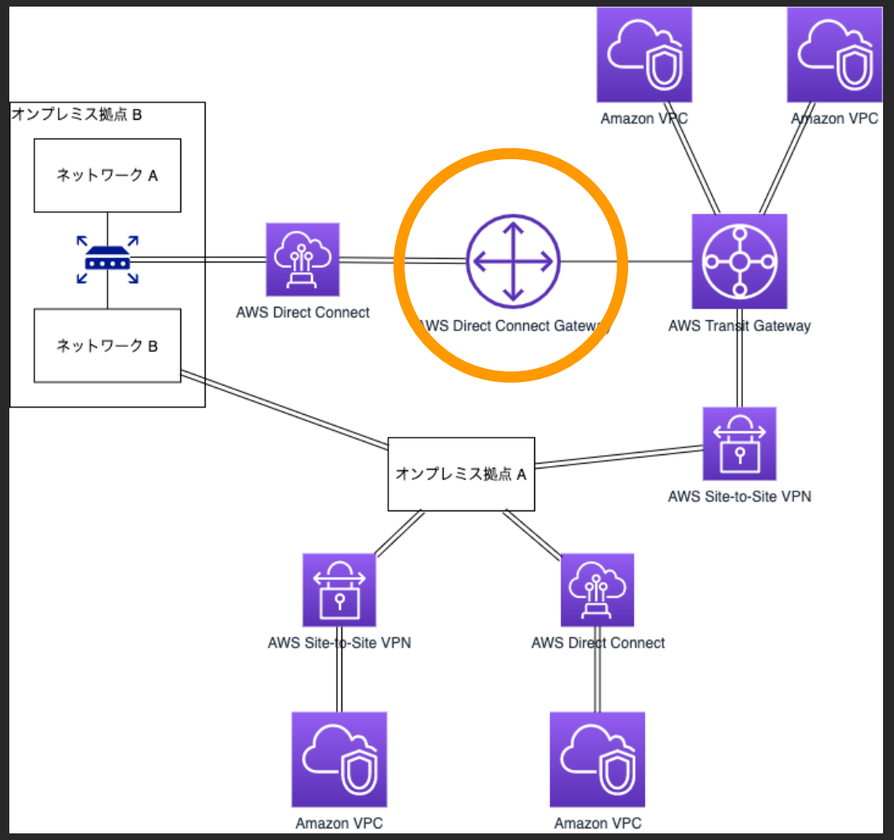


AWS Transit Gateway に AWS Direct Connect を接続する場合の課題と解決方法

aws SUMMIT ONLINE

AWS Direct Connect Gateway ?

- AWS Direct Connect を AWS Transit Gateway に接続する場合に必要になる
  - AWS Direct Connect の仮想インターフェースを AWS Direct Connect Gateway に収容して、AWS Direct Connect Gateway を AWS Transit Gateway にアタッチする
- AWS Direct Connect のオンプレ側終端と BGP による経路交換を担当している

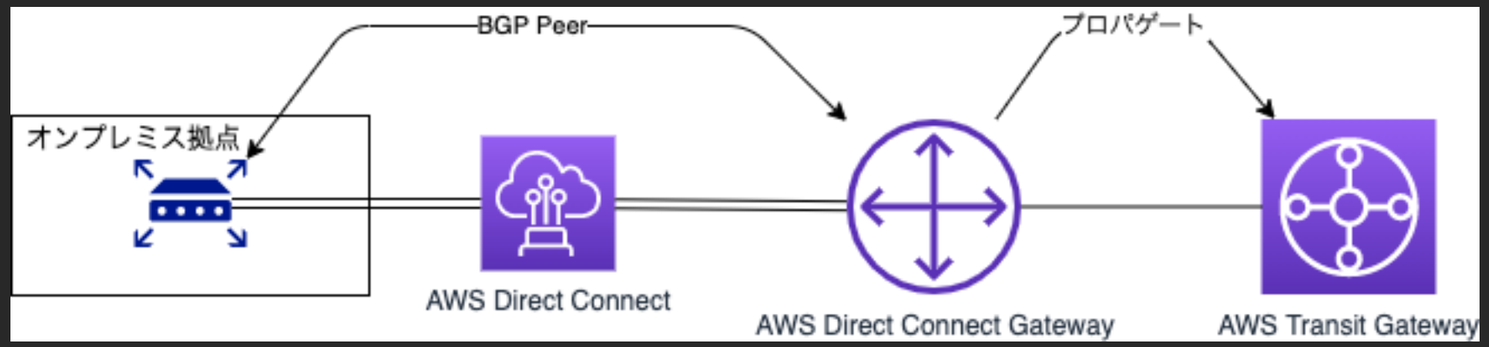


AWS Direct Connect Gateway の注意点

- AWS Direct Connect Gateway にアタッチした AWS Direct Connect の仮想インターフェースはデタッチできない
  - AWS Direct Connect Gateway の作り直しは AWS Direct Connect の仮想インターフェースの作り直しを意味する

オンプレミス環境から AWS Transit Gateway への経路伝播

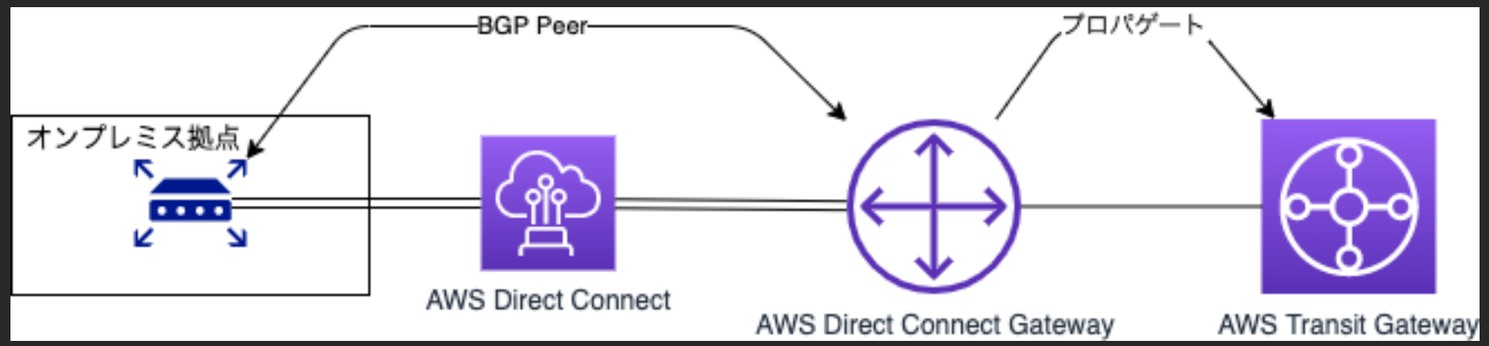
- オンプレミス環境に設置している AWS Direct Connect の終端装置と AWS Direct Connect Gateway が BGP で経路交換している
- AWS Direct Connect Gateway がプロパゲートしている AWS Transit Gateway のルートテーブルに経路が伝播する



AWS Transit Gateway からオンプレミス環境への経路伝播

- AWS Transit Gateway で持っている経路情報は伝播されない
  - AWS VPC と AWS Transit Gateway を接続した場合も AWS VPC のルートテーブルに AWS Transit Gateway 経由の静的経路を追加する
- オンプレミス環境との BGP セッションを終端している AWS Direct Connect Gateway に静的に書かれた経路情報が経路交換の対象

→ AWS Direct Connect Gateway に登録するネットワーク情報が重要になってくる



AWS Direct Connect Gateway に登録できるネットワーク情報

- 登録できる経路は 20 prefix まで
  - ハードリミット
- 多数のネットワークを AWS Transit Gateway で収容した場合
  - 20 prefix のハードリミットがネックになることが予想できる

→ あらかじめ経路集約可能なネットワーク構成にしておく

AWS Direct Connect の仮想インターフェース

- AWS Direct Connect が AWS Transit Gateway に対応したときに仮想インターフェースのタイプとして transit が追加された
- AWS Direct Connect を AWS Transit Gateway に収容する場合は仮想インターフェースを transit で作成する必要がある
  - 既存の AWS Direct Connect では仮想インターフェースを private か public で作成しているはずなので注意が必要
  - 利用しようとするパートナーの AWS Direct Connect の提供形態によっては transit に対応していない場合があるので注意が必要

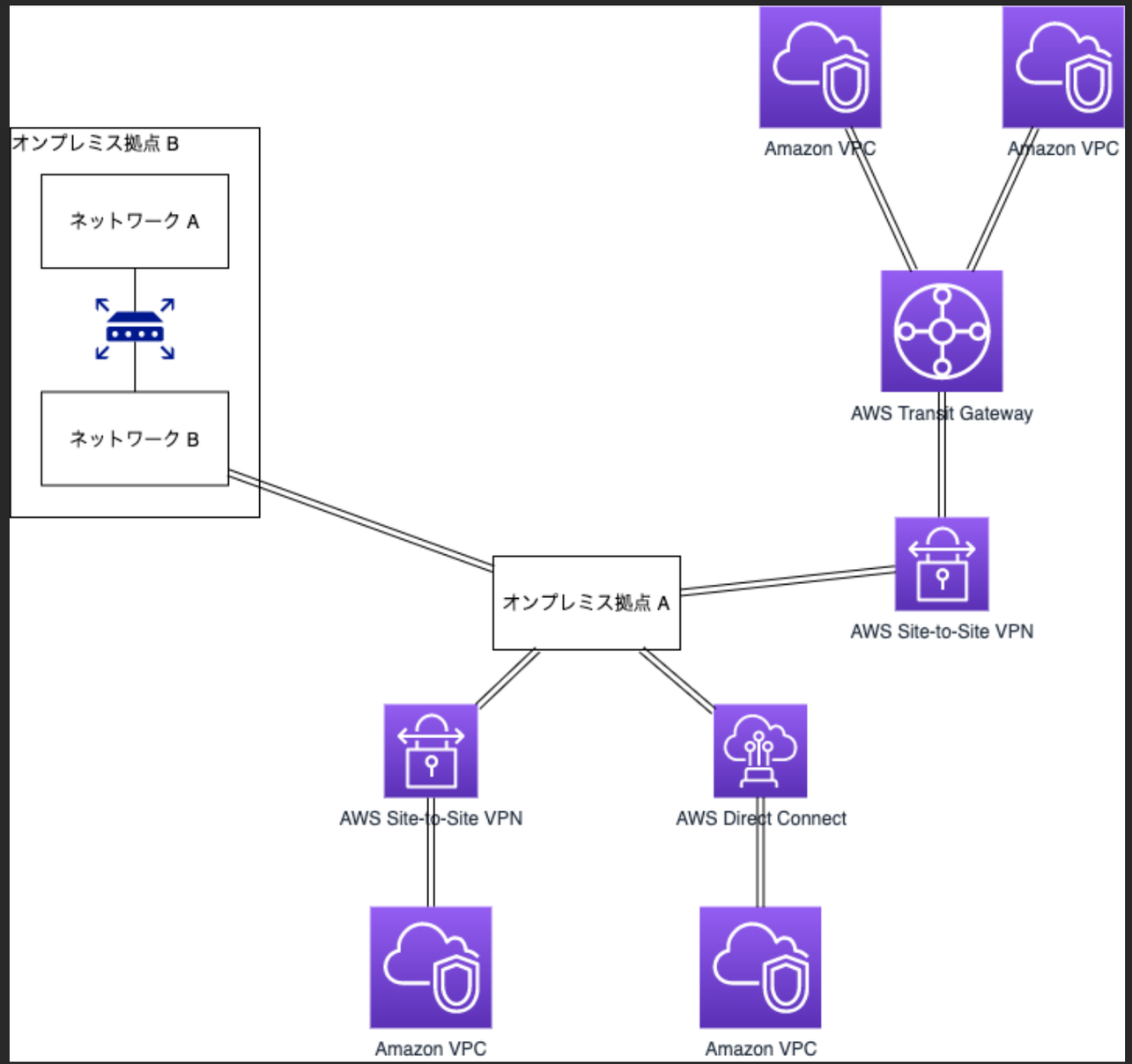
AWS Transit Gateway と AWS Direct Connect の接続作業時の課題と解決方法

aws SUMMIT ONLINE

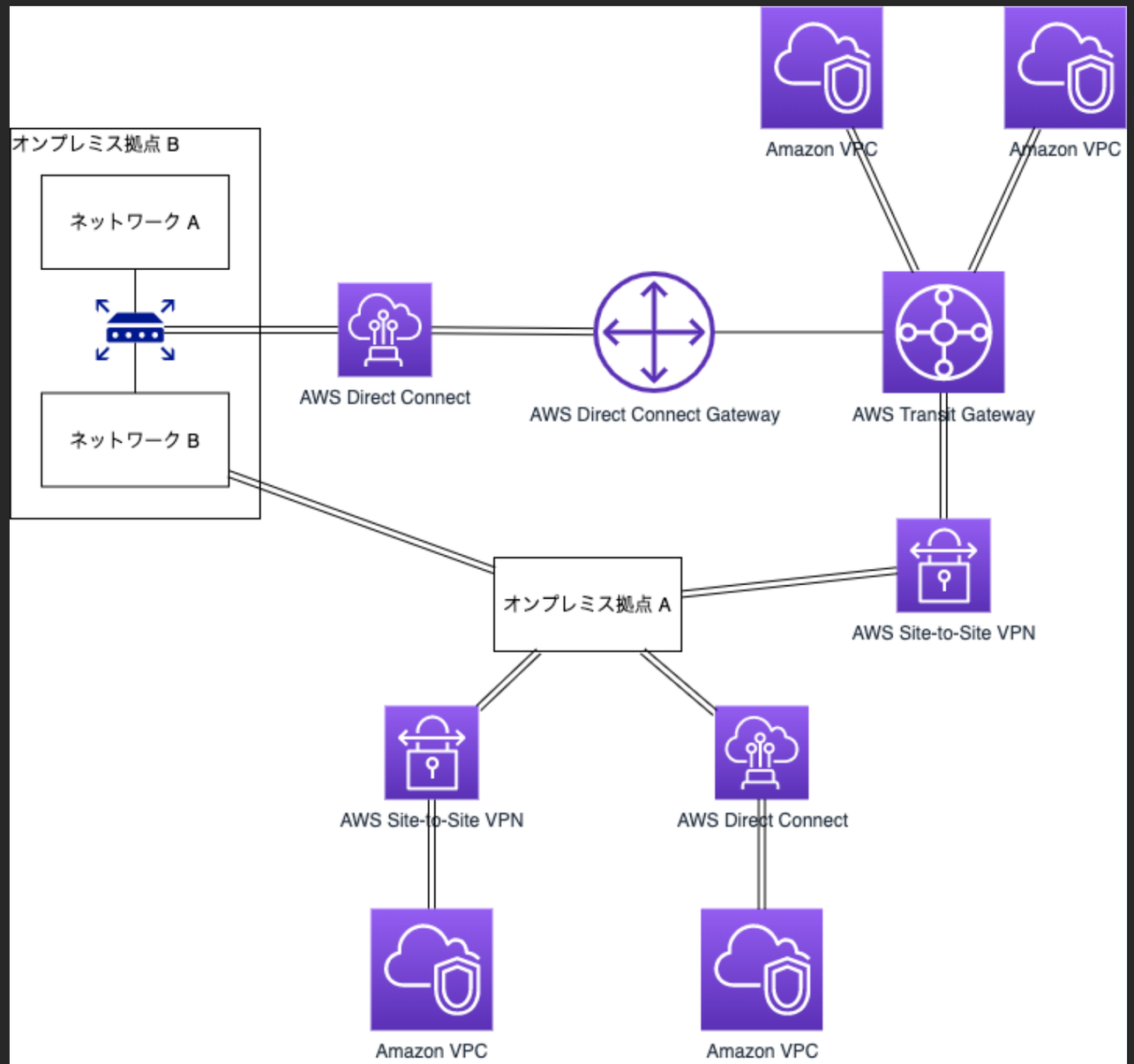
AWS Transit Gateway のルートテーブルにおける経路の優先順位

aws SUMMIT ONLINE

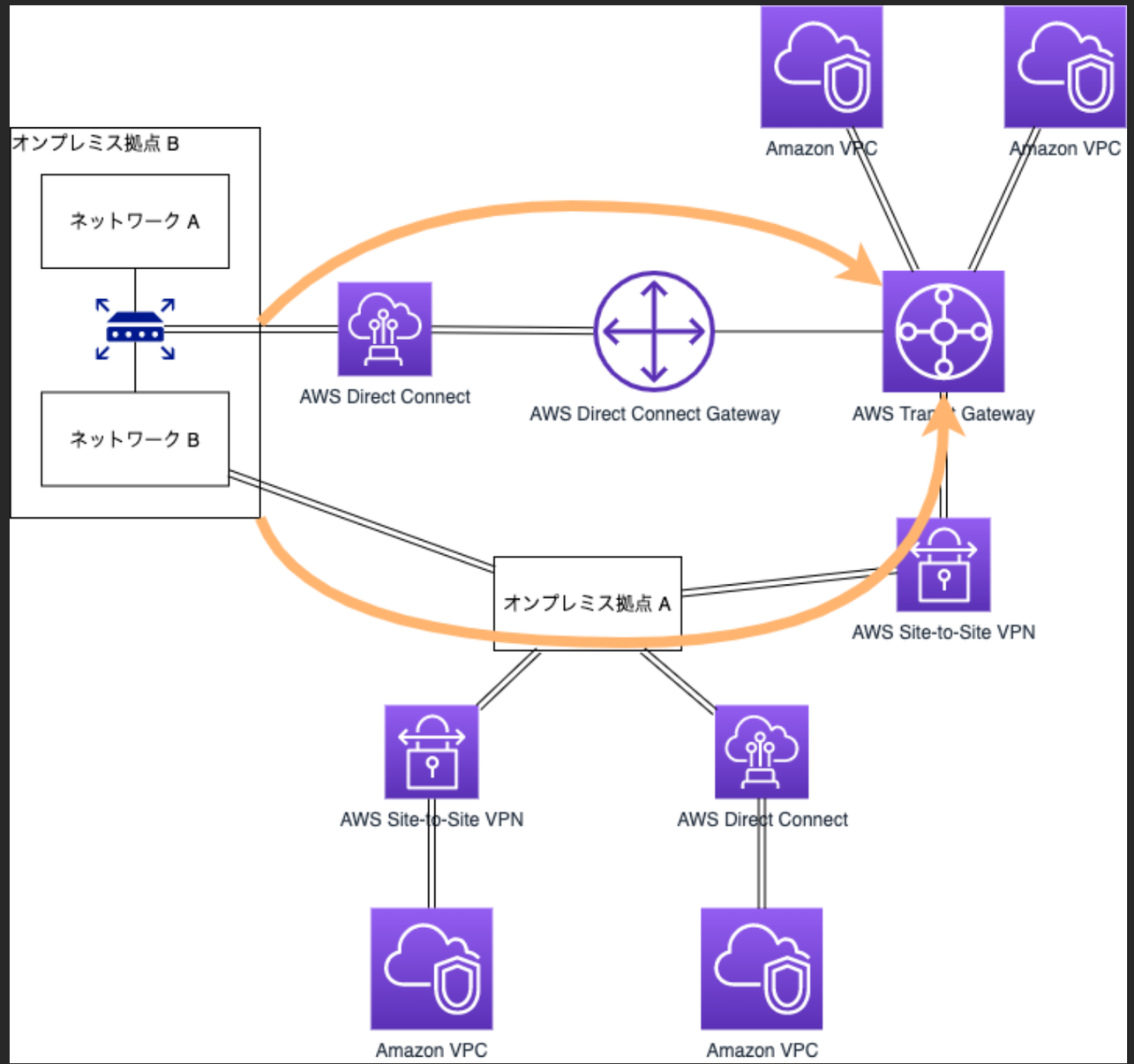
AWS Direct Connect 接続前の構成



AWS Direct Connect 接続後の構成 (再掲)

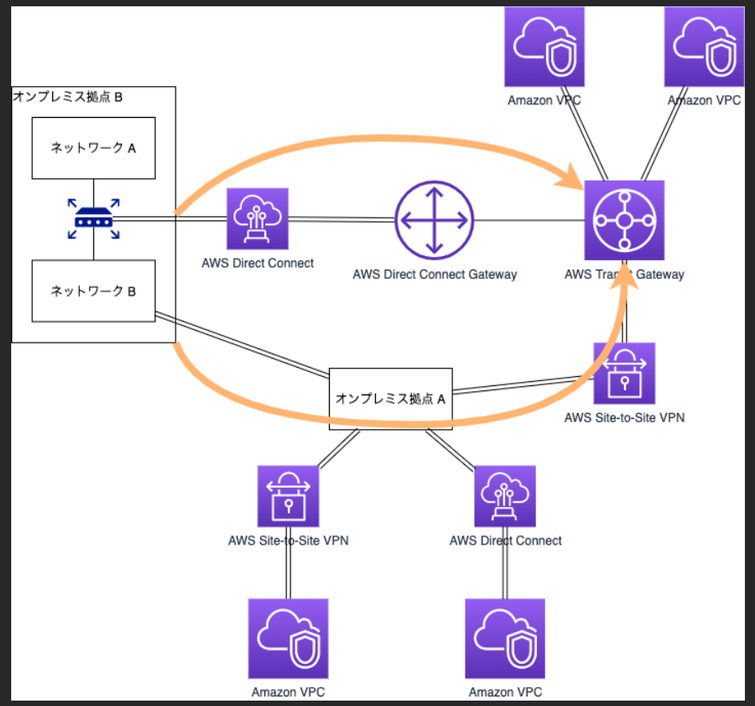


オンプレミス環境 B の経路情報が2つの経路で伝播する



AWS Transit Gateway のルートテーブルにおける経路選択の優先順位

- 同一 prefix の場合は以下の順番で選択される
  1. 静的に入れた経路情報
  2. Amazon VPC 由来の経路情報
  3. AWS Direct Connect Gateway から伝播した経路情報
  4. AWS Site-to-Site VPN から伝播した経路情報

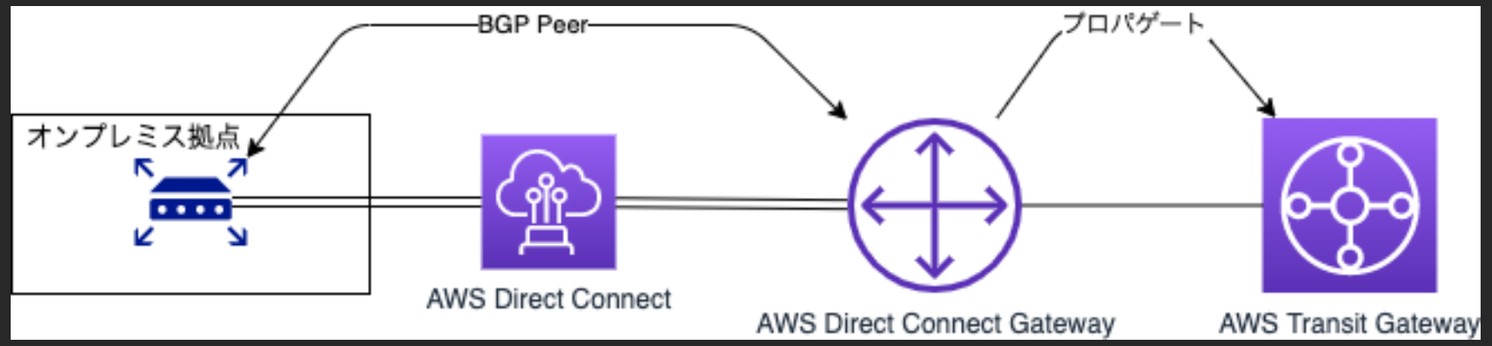


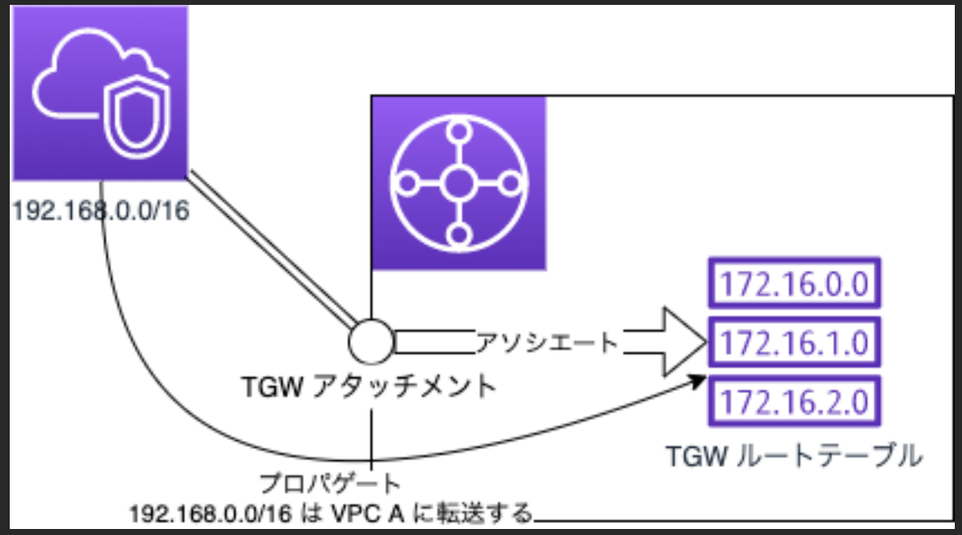
構成変更による影響を最小限に抑える

aws SUMMIT ONLINE

それぞれの操作によって発生するネットワーク的変化を把握する

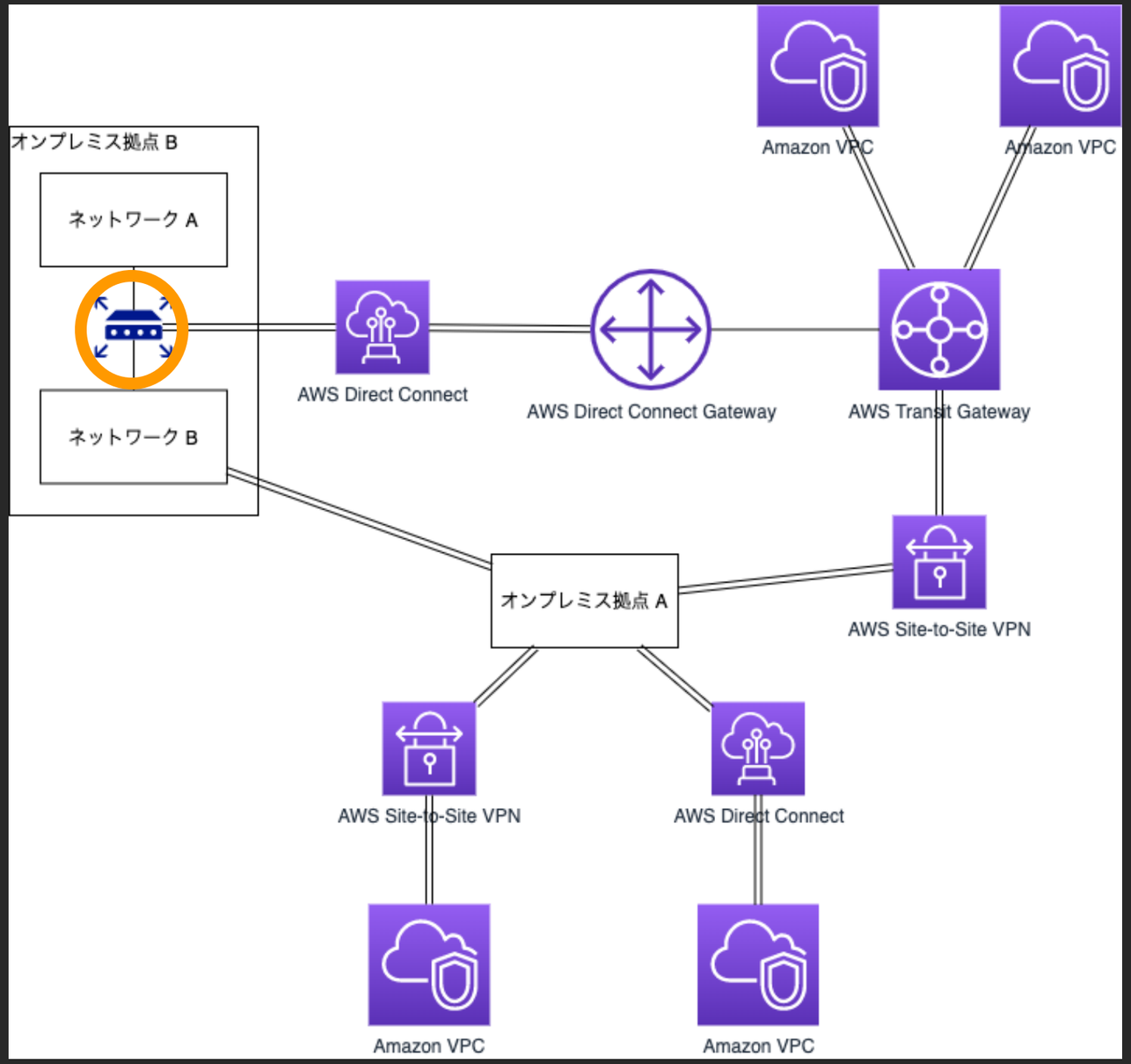
- AWS Transit Gateway のルートテーブルにアタッチメントしてアソシエートしたら、AWS Direct Connect から AWS Transit Gateway にパケットが流れるようになる
- AWS Transit Gateway のルートテーブルにプロパゲートしたら、AWS Transit Gateway から AWS Direct Connect にパケットが流れるようになる
- AWS Direct Connect Gateway に経路情報を追加するとオンプレミス環境から AWS Direct Connect Gateway までパケットが到達する





それぞれの操作によって発生するネットワーク的変化を把握する

- オンプレミス側で AWS Direct Connect を収容しているルータで BGP ピアがアップしたときの状態を想定する
  - オンプレミス側から AWS Transit Gateway に広報される経路情報
  - AWS Direct Connect Gateway からオンプレミス側のルータに広報される経路情報
  - AWS Direct Connect Gateway から広報された経路によって生じるオンプレミス側のネットワークの経路情報の変化



構成変更によって生じる影響を最小限に抑える

- 各手順で発生するネットワーク的な変化に矛盾が生じないように手順を考える
- 必要に応じてオンプレミス側のネットワーク設定を変更する
- AWS Transit Gateway のルートテーブルにプロパゲートすることが適切かを考える
  - ヒント：アソシエートして、静的経路を書くだけで AWS Transit Gateway から AWS Direct Connect にパケットを流すことは可能

まとめ

aws SUMMIT ONLINE

まとめ

- AWS Transit Gateway と AWS Direct Connect を接続するときに注意すること
  - AWS Direct Connect Gateway が必要
  - AWS Direct Connect の仮想インターフェースは transit で作成する
  - AWS Direct Connect との経路交換は AWS Site-to-Site VPN と異なる
- AWS Transit Gateway に複数のオンプレミス環境を収容した場合は経路の優先順位に気をつける
- トラブルを未然に防ぐために、ネットワーク全体を俯瞰して作業計画を立てる