



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

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

人力検索 はてな (2001年～)

The screenshot shows the Hatena Q&A website interface. At the top, there is a search bar with the text "人力検索はてな" and a search icon. To the right of the search bar are links for "ユーザー登録", "ログイン", and "ヘルプ". Below the search bar is a navigation menu with "トップ", "カテゴリ", "質問一覧", and "注目の質問". On the right side of the navigation menu are buttons for "アンケートする", "匿名で質問する", and "質問する".

The main content area is divided into several sections:

- 疑問や悩みを解決**: A section for asking questions and getting answers. It includes a text input field for "質問・相談内容を入力してください" and buttons for "匿名で質問する" and "質問する". Below the input field, it says "質問総数 396,301 件".
- 人気の質問**: A list of popular questions. The first question is about "プリキュア5 第3話で、のぞみが、学校の女子生徒達が多くいる場所で、「でもなんかかっこいいよね、はじけるプリキュアって。」と言っ...".
- 回答募集中の質問**: A list of questions where answers are being sought. The first question is "どうすれば高卒の学力になるのですか。".
- 匿名の質問**: A list of anonymous questions. The first question is "悪口ばかり言う人ほど友達が多いのはなぜ？ 一般論として「悪口を言う人は信用されない」「悪口を言うと人が離れていく」という話を聞...".

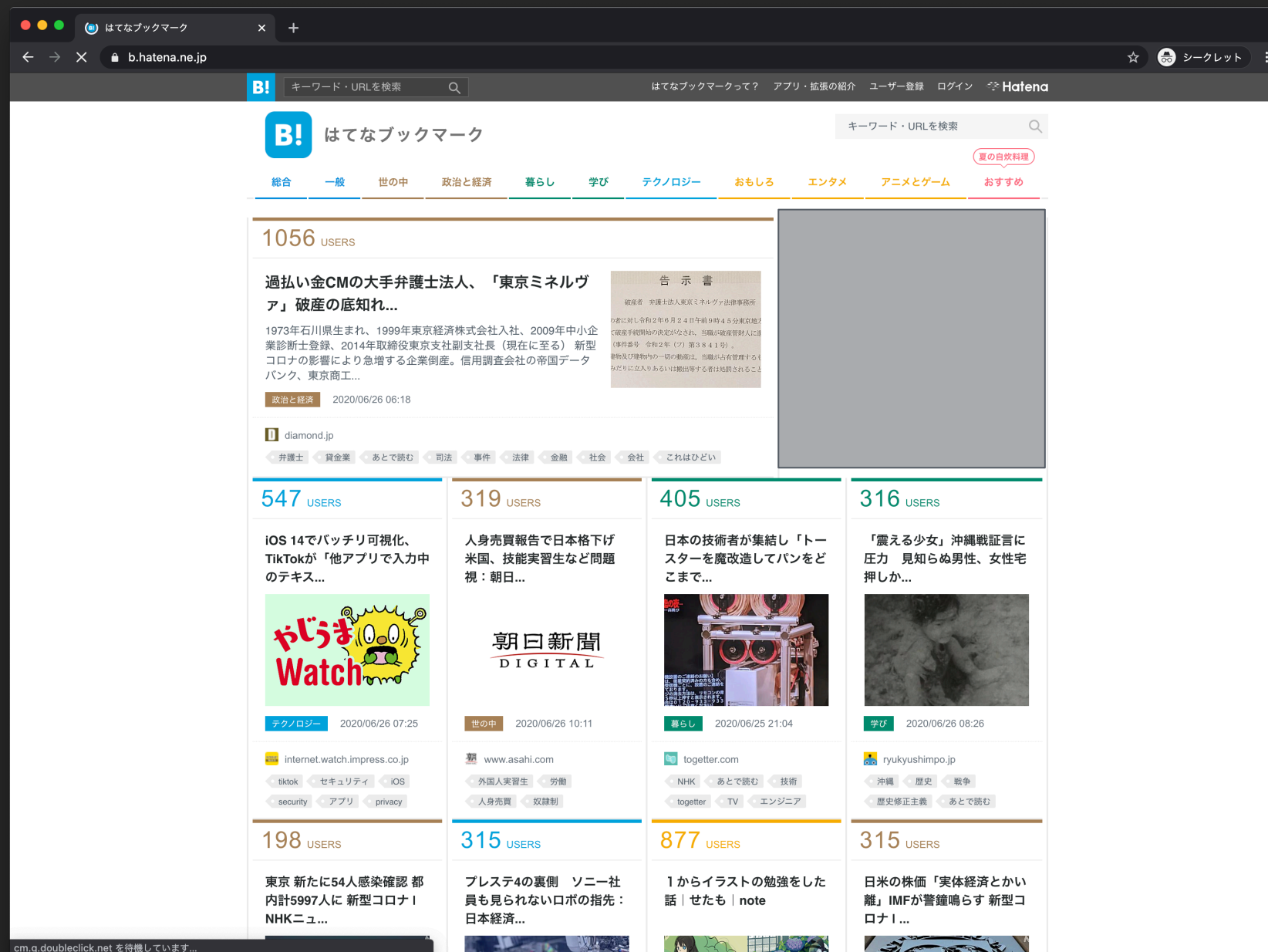
On the right side of the page, there are several promotional banners and sections:

- ユーザー登録して使いはじめる!**: A banner encouraging users to register and use the site for free.
- アンケート**: A section for surveys. It includes a "終了後公開" button and a "このアンケートに答える" button.
- 過去の人気質問**: A list of past popular questions. The first question is "征夷大将軍になれば幕府を開けると習いました。...".

At the bottom of the page, there is a "フォローする" button with "1,891人のフォロワー" and a "人力検索はてな" logo.

<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～)

はてなブログ

hatenablog.com

Hatena Blog

ブログ開設 (無料) ログイン ヘルプ Hatena

思いは言葉に。

はてなブログとは はてなブログPro 使い方講座

おすすめ記事

【日本語訳】NCTテヨンの炎上騒動について (ディスパッチ)

JUST FANCY
2時間前

[Dispatch=キム・スジ、オ・ミョンジュ記者] NCTテヨンの過去の言動による炎上騒動 (2009年5月2日) の登場人物は3人...



星野源『折れ合い』がめちゃくちゃ怖い

kansou
36分前



第12回 まともさに準拠して、性善説にふんばりながら、続ける (SHARPさん編・後編)

SNS医療のカタチTVウラ話
10時間前



金の給付率

市区町村	給付率 (%)
練馬区	79.6
足立区	53.2
葛飾区	61.6
江戸川区	15.6
23区計	30.3
札幌市	84.9
仙台市	22.9
横浜市	12.1
名古屋市	4.7
大阪市	3.1

支出処理を完了した世帯数

河村たかし名古屋市長は名古屋市の特別定額給付金支給率

クラウドワークスを退職します。

CDIが構築/運用するセキュアなりモートワーク環境 - 折れ



<https://hatenablog.com/>

はてなブログ Media (2014年～)

The screenshot shows the Hatena Blog Media website. The header includes the Hatena logo and a navigation bar. The main content area features a large blue background with white text and a central image of a woman working on a laptop. A yellow button with the text 'まずは相談してみる' is prominent. Below the main content, there is a row of logos for various companies including RECRUIT, Rakuten, mercari, DMM.com, アイアイテム, アルク, and エンジャパン. The bottom section is titled 'Owned Media Management' and lists eight common challenges.

HATENA BLOG *Media* Power by Hatena

まずは相談してみる

一部上場企業を含む
50社以上が導入

はてなブログMediaなら
オウンドメディア運営に必要な全てが揃う

まずは相談してみる

RECRUIT Rakuten mercari DMM.com アイアイテム アルク エンジャパン

オウンドメディア運営によくある8つの課題

- 管理画面の操作が **難しくて使いづらい**...
- 保守・運用に **時間や費用がかかる**...
- **セキュリティ対策**を継続してやっていたり不安...
- **SEOが出来なくて**、検索上位に表示されづらい...
- 記事作成で手一杯で **トレンドについていけない**...
- **始めるのにデザインを依頼**しないとけない...
- せっかく記事を公開しても **見てもらえない**...
- **コンテンツの内容に悩んで**更新が遅れがち...

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

mackerel (2014年～)

<https://mackerel.io/>

カクヨム (2016年～)

The screenshot shows the Kakuyomu website interface. At the top, there's a navigation bar with 'カクヨム' and links for 'マイページ', '小説を探す', '公式連載', and '書籍化作品'. A search bar and a '新規登録(無料)' button are also present. Below the navigation, there are several promotional banners for books like '優しい死神は、君のための嘘をつく', 'Spread', '燃え尽きたExcel職人の魂', and 'ダイヤモンド・プリンセス 乗船手記'. A central banner promotes a 'COVID-19 era reading list' with a deadline of 6/30. Below this, there are sections for '小説を探す' (Browse by genre like 'ライトノベル', '学園'), '注目の作品' (Featured works), and '累計ランキング' (Cumulative rankings). The featured works section contains a grid of book covers and titles such as '【書籍発売中】のんびり暮らしたいおっさんがはじめたい異世界スローライフ', 'AI美女と博士の尊い愛', '自由に作るう大事な我が家!', and '「次の転生先に、乙女ゲームの世界なんてどうですか?」'.

<https://kakuyomu.jp/>

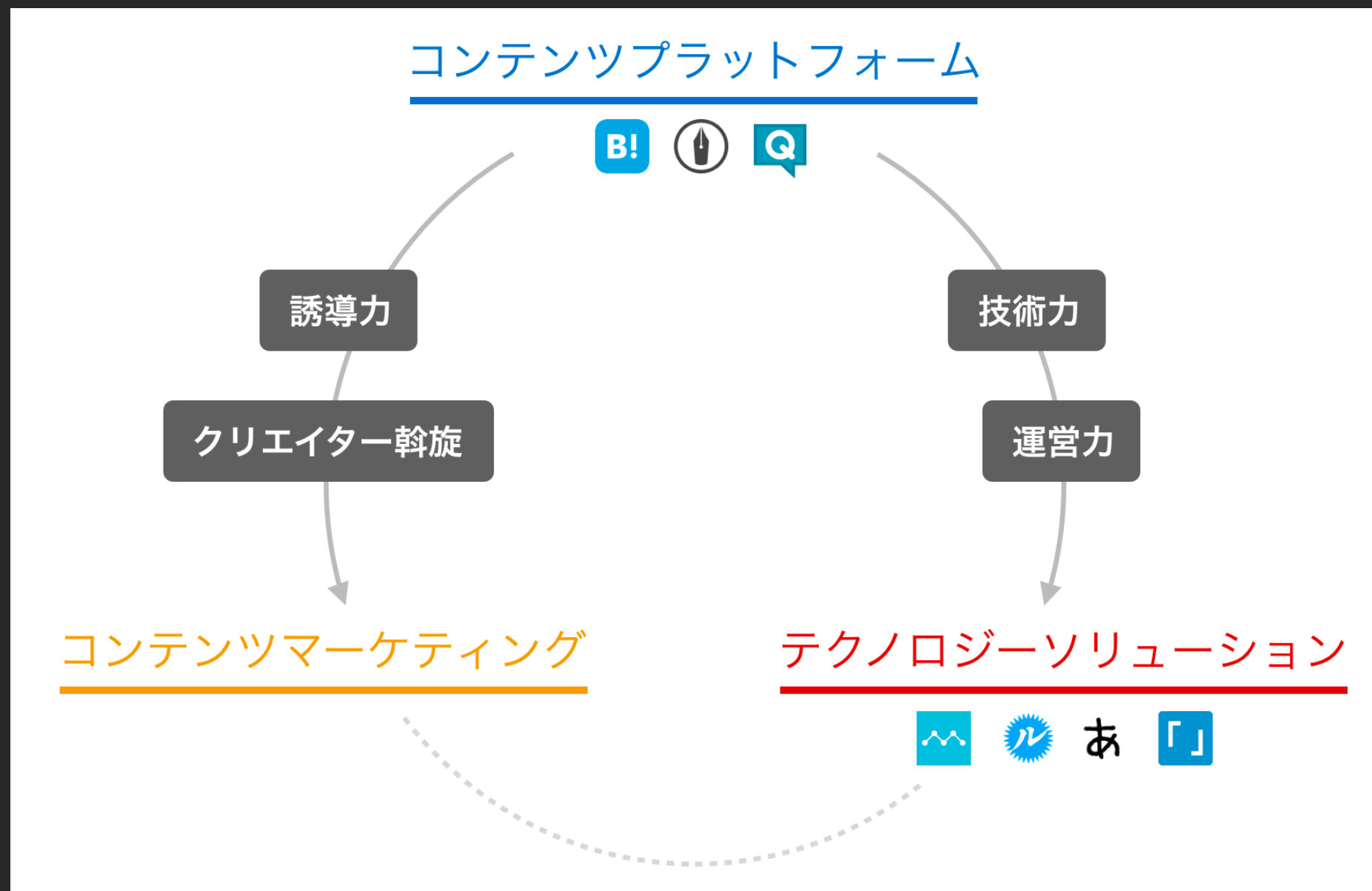
コミックDAYS (2018年～)

The screenshot shows the homepage of the comic-days.com website. At the top, there is a navigation bar with the site name, a search bar, and a 'プレミアム体験' (Premium Experience) button. Below the navigation bar, there are several promotional banners for different manga series, including 'MANGA Day to Day', 'お仕事漫画が最大3巻無料!!', and '20話無料&連続子ケツ化!!'. The main content area features a 'DAYSオリジナル' (DAYS Original) section with a '毎日更新' (Daily Update) badge. Below this, there is a date indicator '金 6月26日' (Friday, June 26th) and a notification '未熟なふたりでございませうが 他 12作品更新!' (We are immature but 12 other works are updated!). The main content area displays a grid of manga covers with their titles and brief descriptions:

- 未熟なふたりでございませうが**: 今夜どう勝つ? 身悶え新婚コメディ
- タマロワ**: ~100%金目当て 資産35億のイケメンは私のモノだ!
- あらくれお嬢様はもんもんしている**: 色欲から学ぶ恋愛事始めラブコメ!
- 淫らな青ちゃんは勉強ができない**: 青ちゃんのエロ妄想が暴走する!
- ギルティ**: ~鳴かぬ笛が身を焦がす~ 裏切者だらけのラブサスペンス
- LITTLE Bull**: リトル・ブル 高校野球界に160キロ女子現る!

<https://comic-days.com/>

はてなのサービス



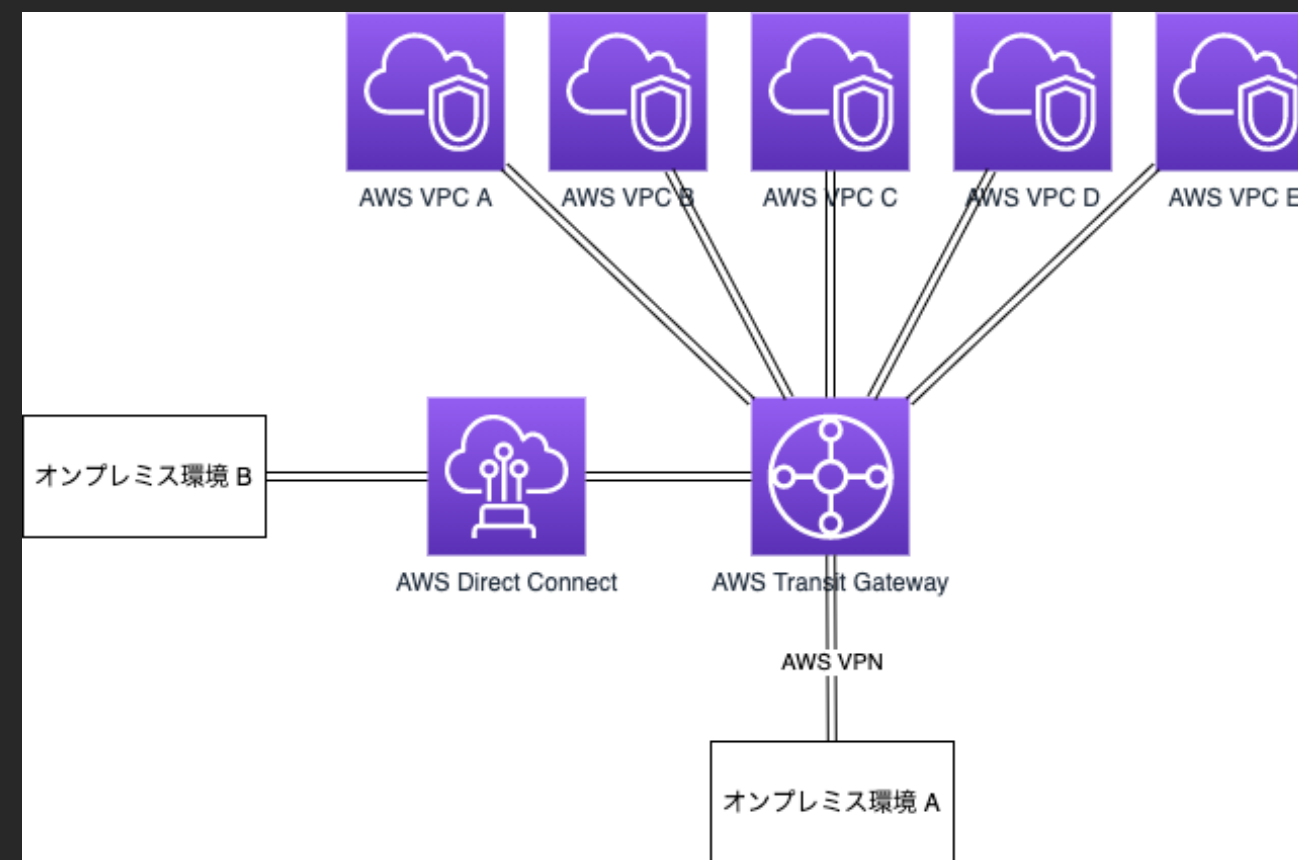
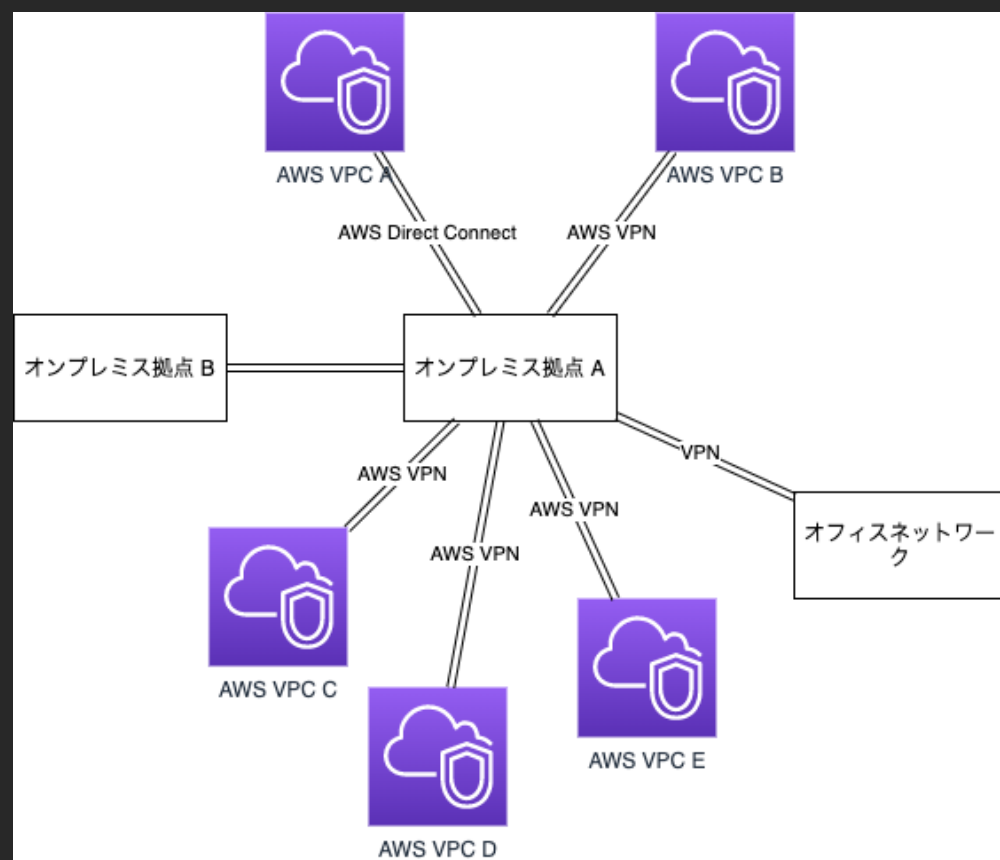
はてなのサービスと基盤部分の課題

- 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ワー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



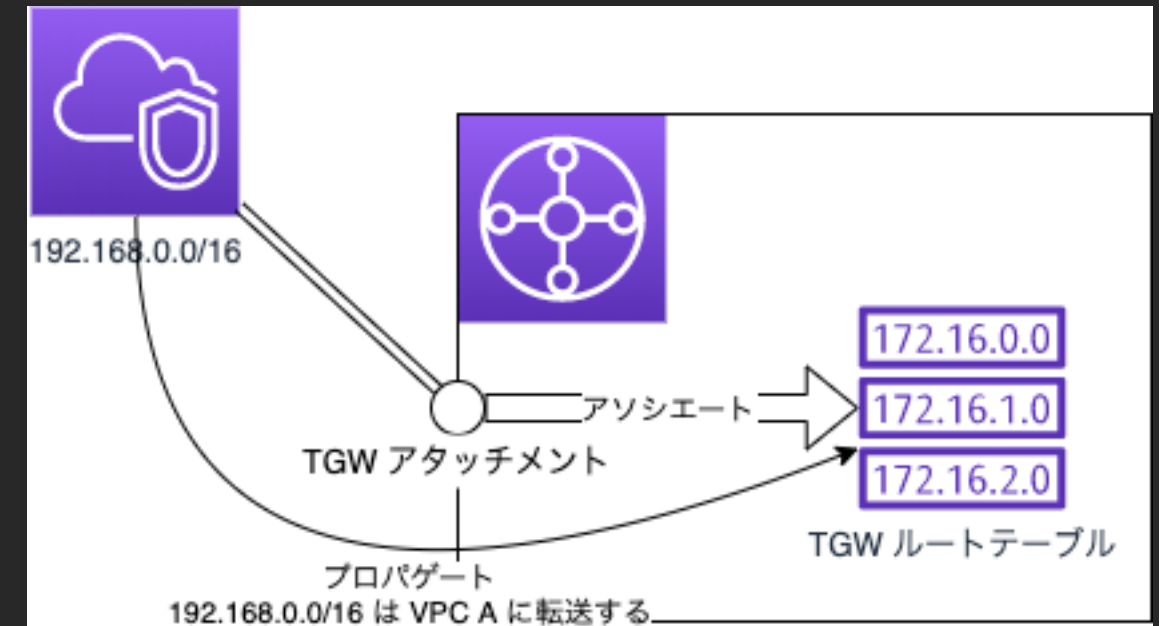
AWS Transit Gateway についておさらい

AWS 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

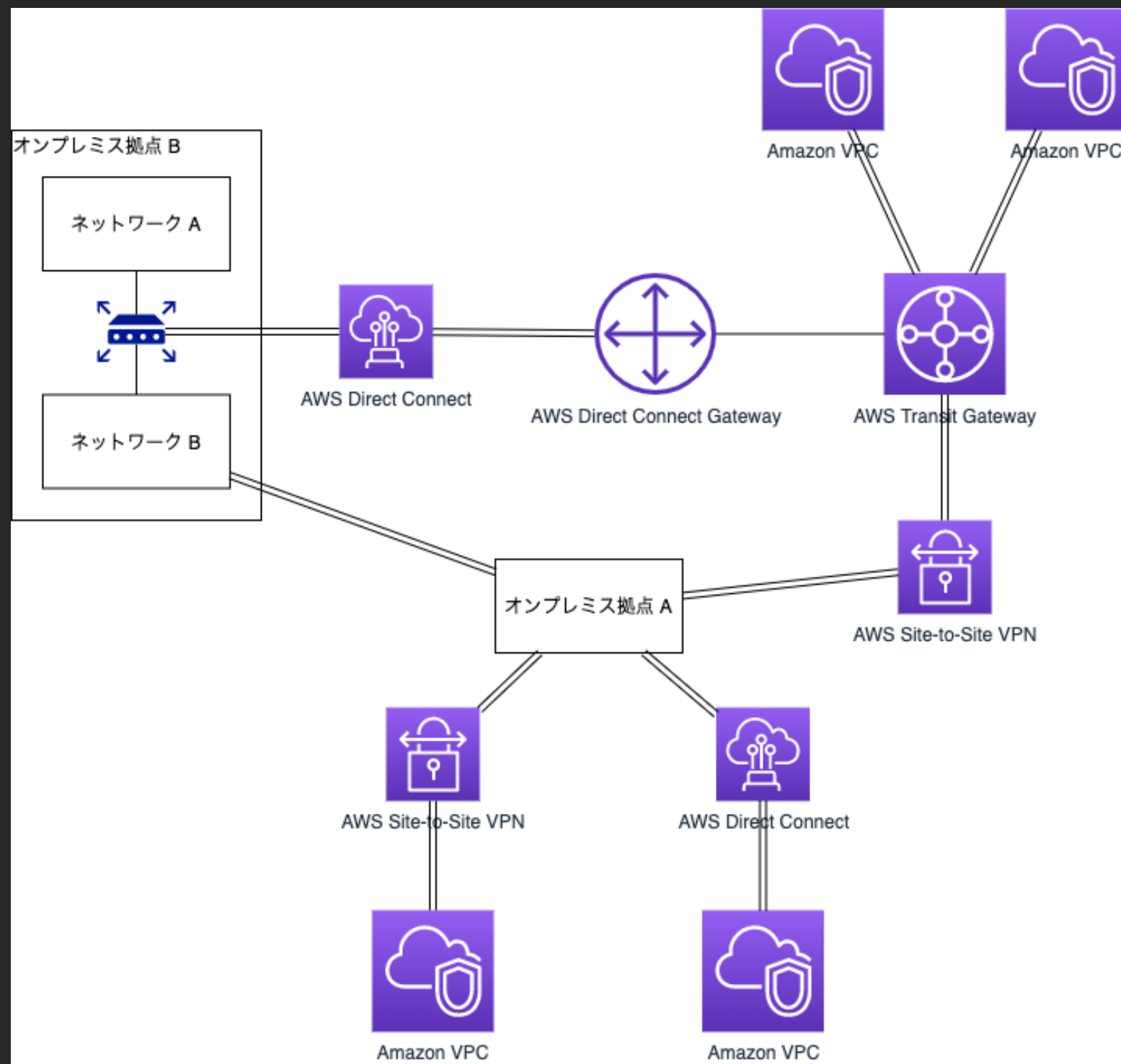


構成の概要

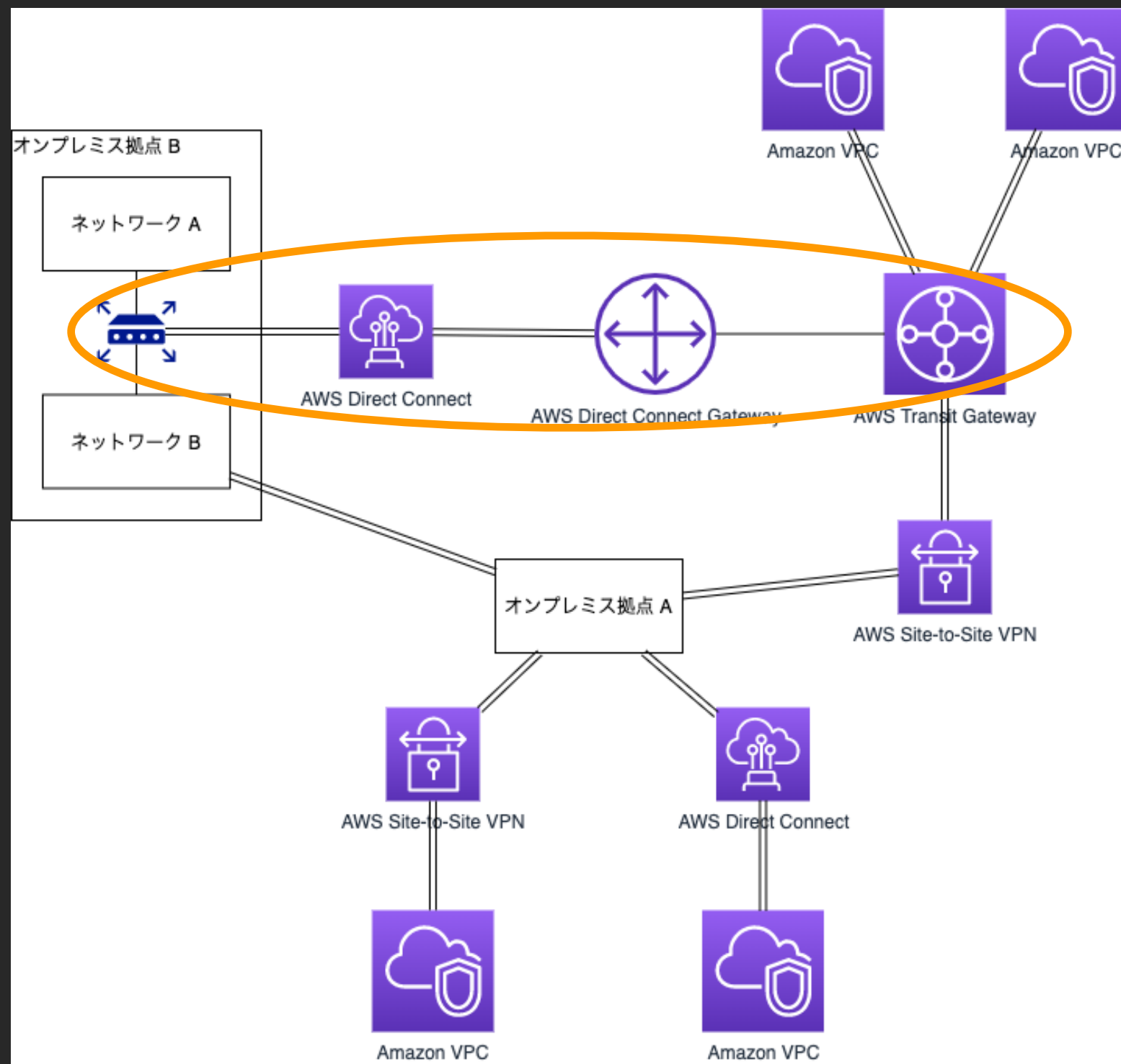
内部ネットワークの構成変更の履歴

- 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



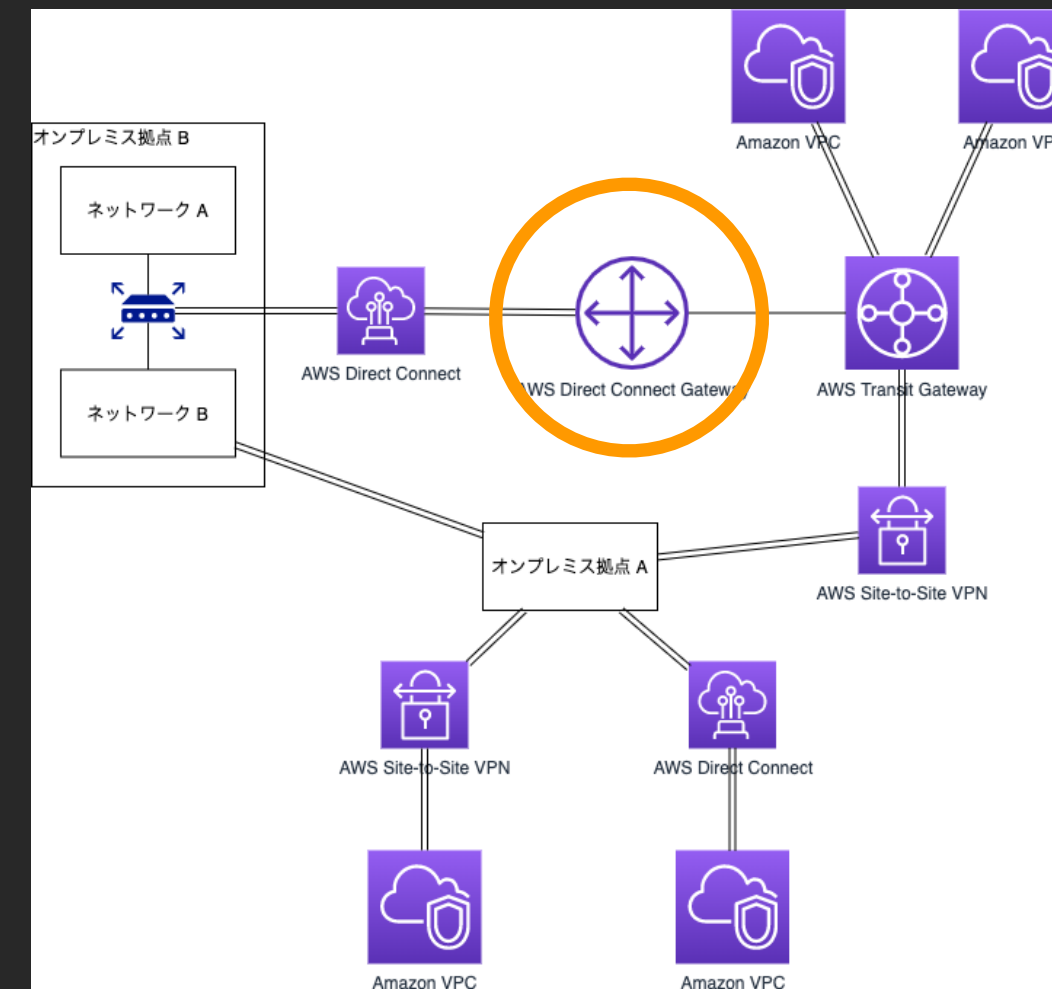
今回お話しするネットワークの全体像



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

AWS Direct Connect Gateway ?

- AWS Direct Connect を AWS Transit Gateway に接続する場合に必要なになる
- 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

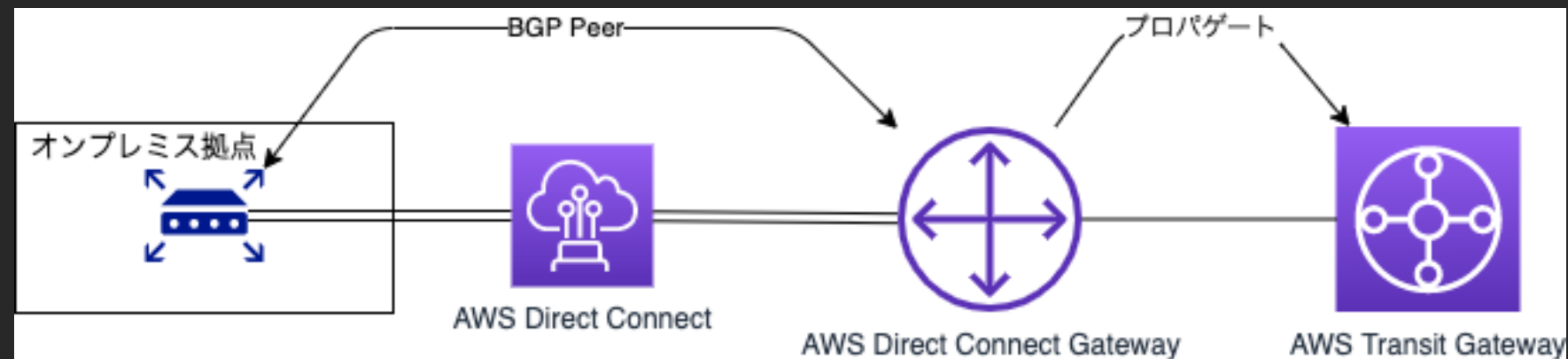


AWS Direct Connect Gateway の注意点

- 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

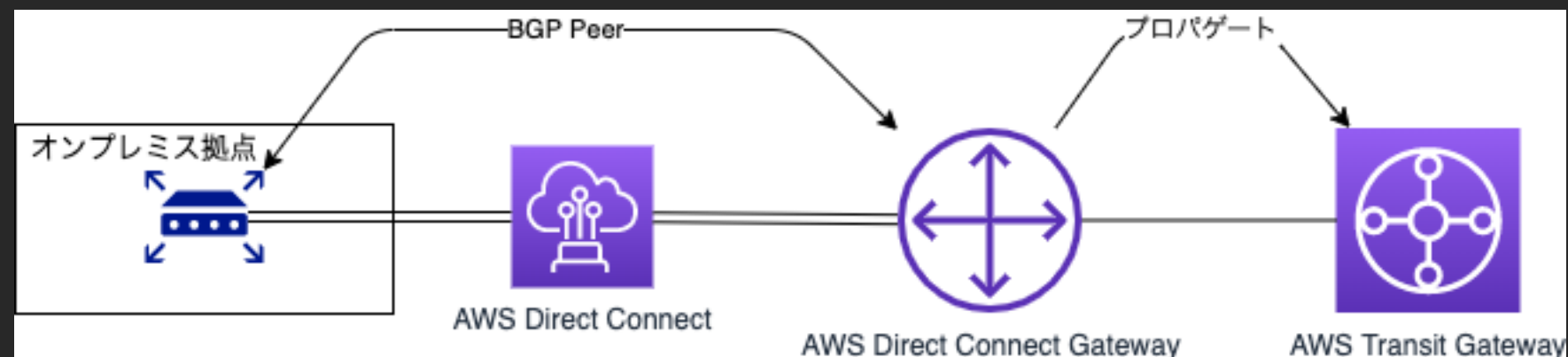
- オンプレミス環境に設置している AWS Direct Connect の終端装置と AWS Direct Connect Gateway が BGP で経路交換している
- AWS Direct Connect Gateway がプロパゲートしている AWS Transit Gateway のルートテーブルに経路が伝播する



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

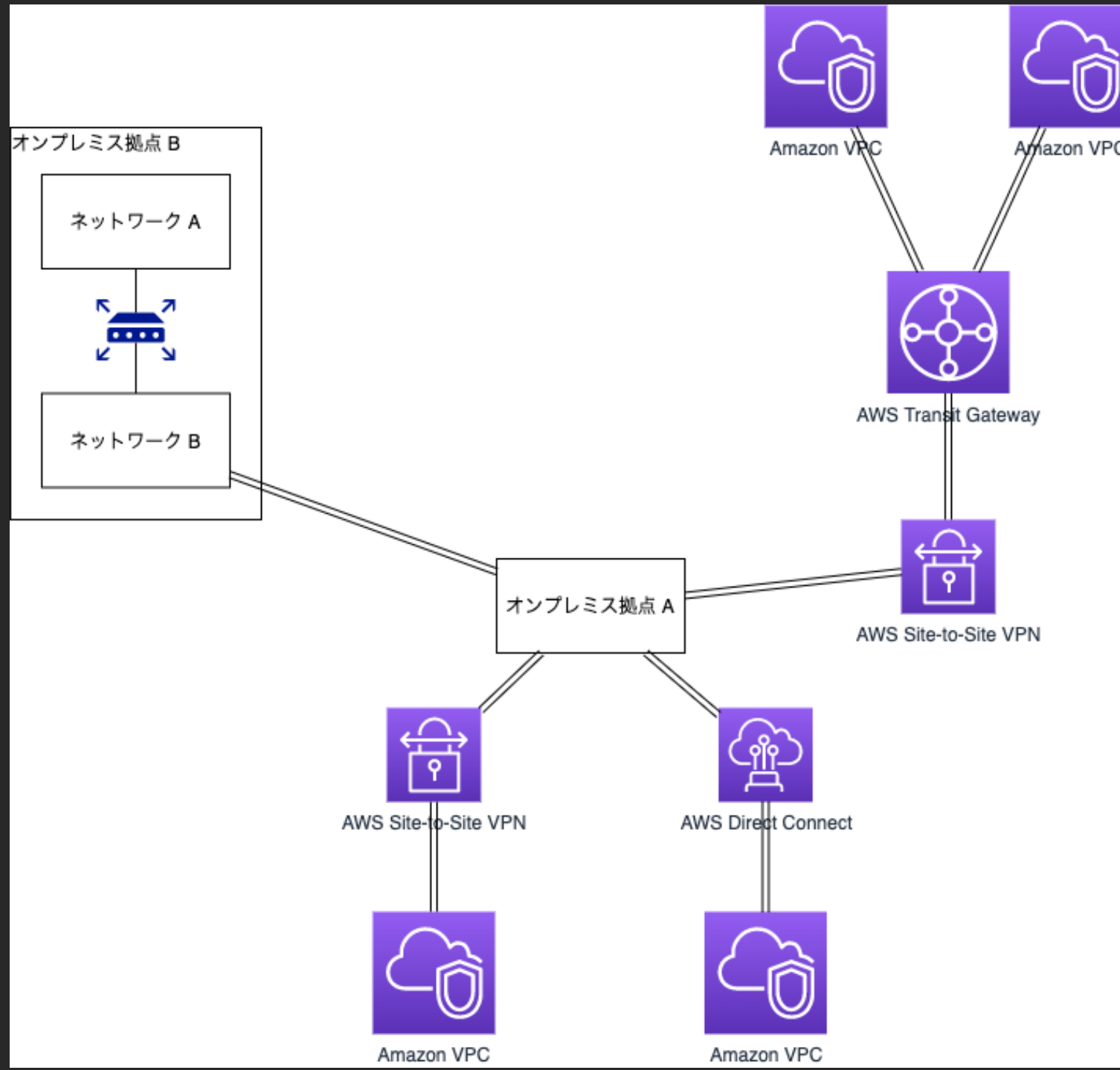
AWS Direct Connect の仮想インターフェース

- 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

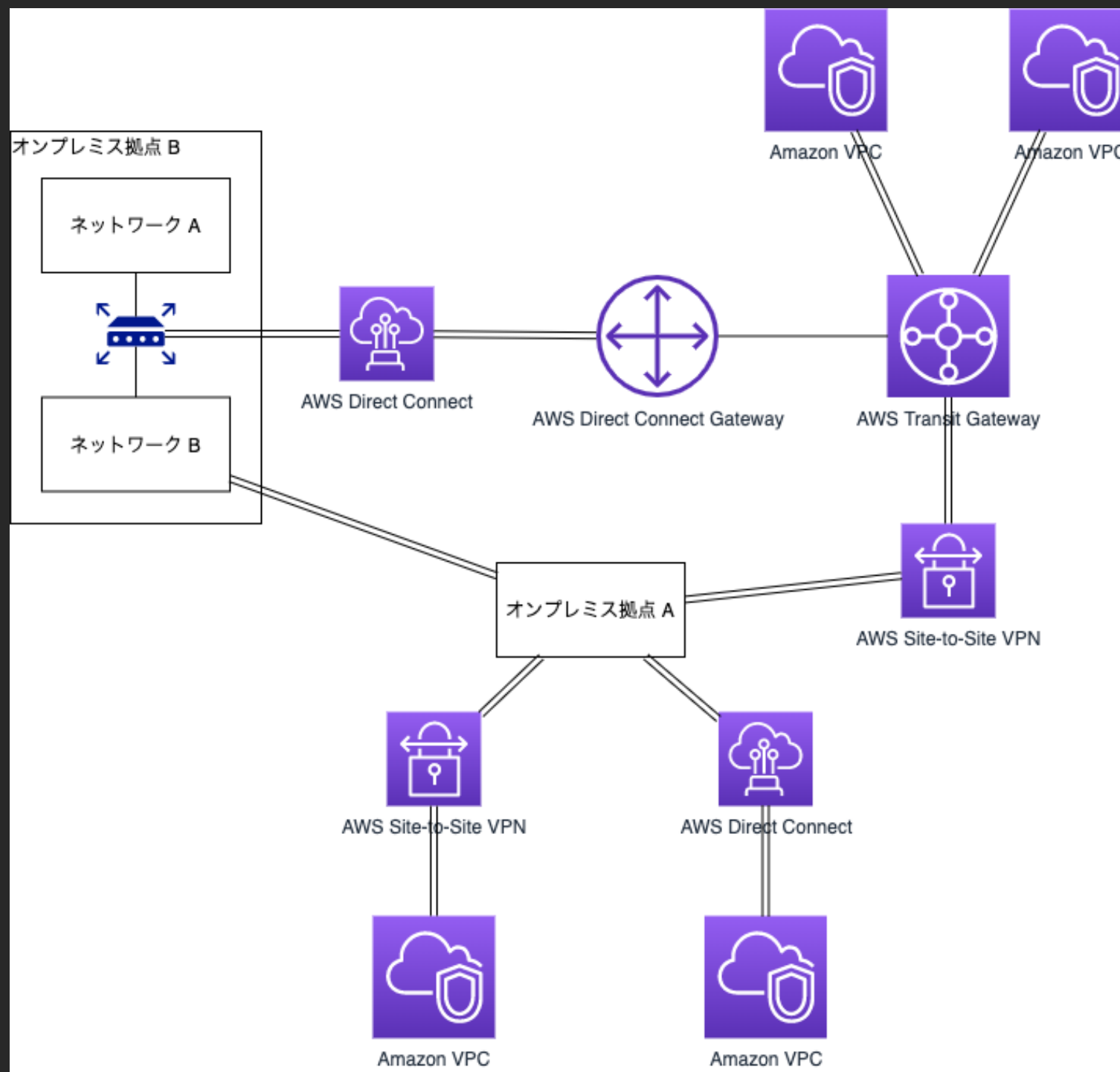
AWS Transit Gateway と AWS Direct Connect の接続作業時の課題と解決方法

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

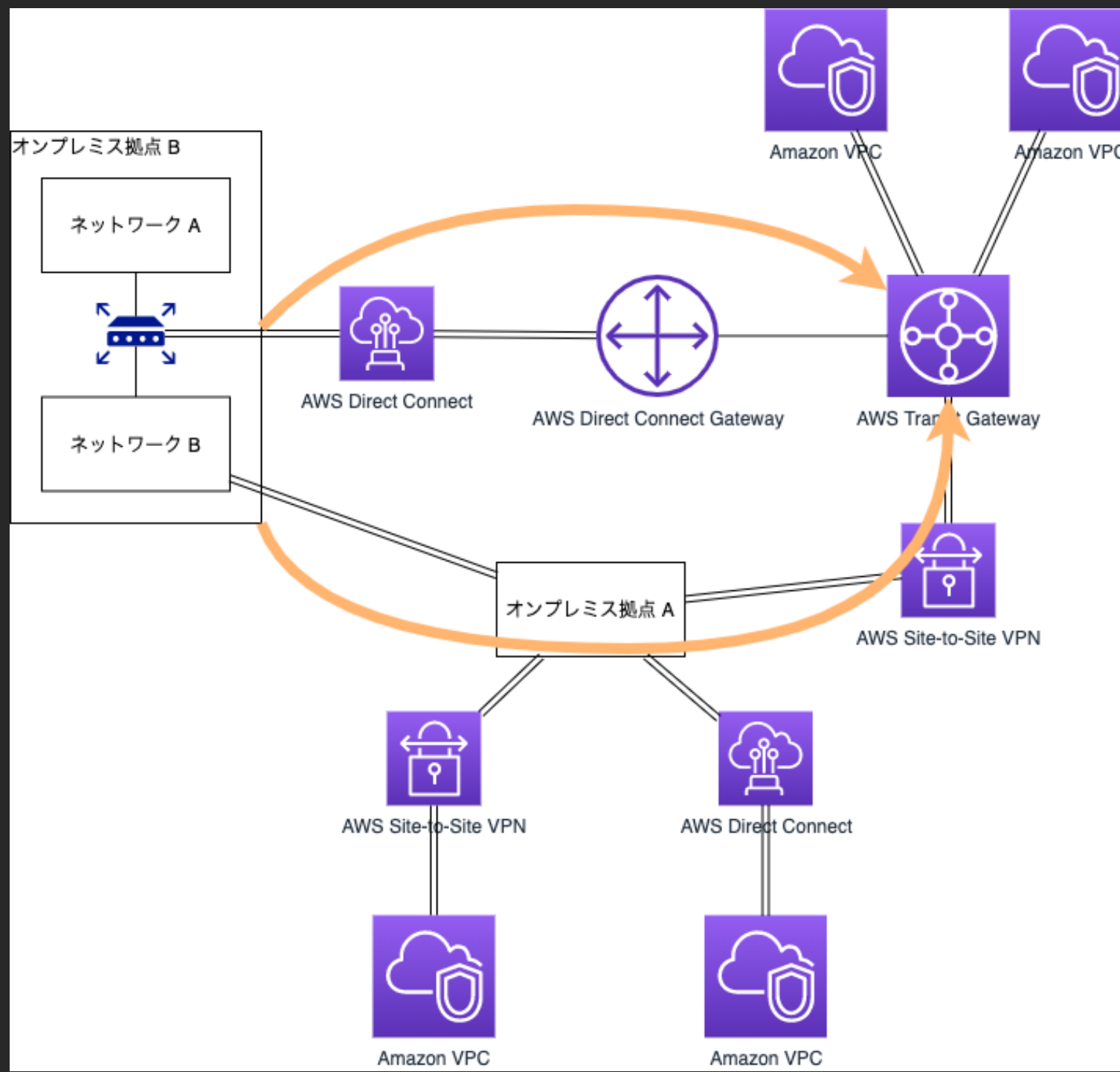
AWS Direct Connect 接続前の構成



AWS Direct Connect 接続後の構成 (再掲)

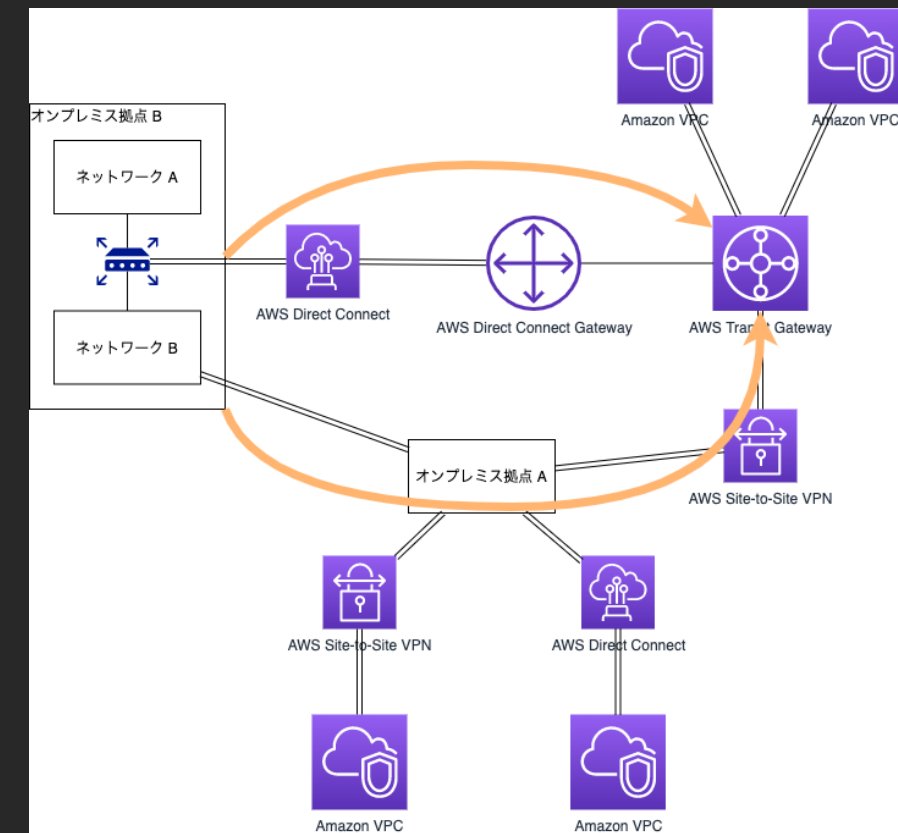


オンプレミス環境 B の経路情報が2つの経路で伝播する



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

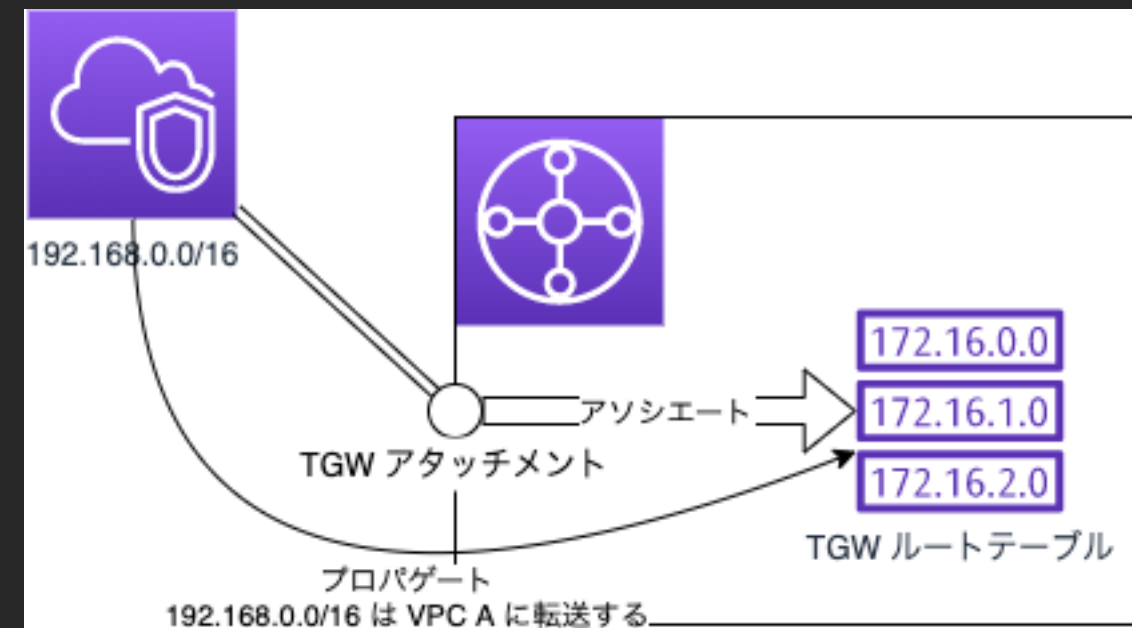
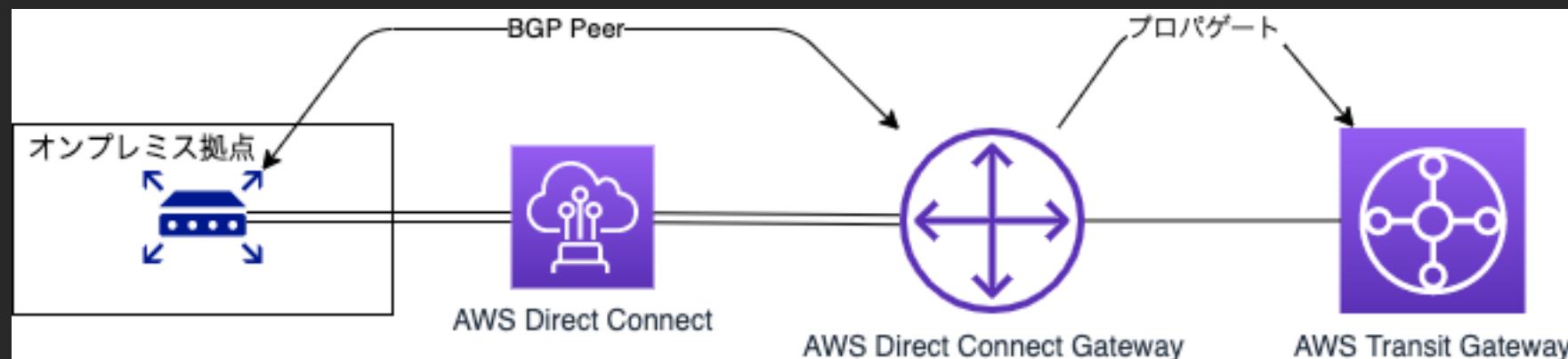
- 同一 prefix の場合は以下の順番で選択される
 1. 静的に入れた経路情報
 2. Amazon VPC 由来の経路情報
 3. AWS Direct Connect Gateway から伝播した経路情報
 4. AWS Site-to-Site VPN から伝播した経路情報



構成変更による影響を最小限に抑える

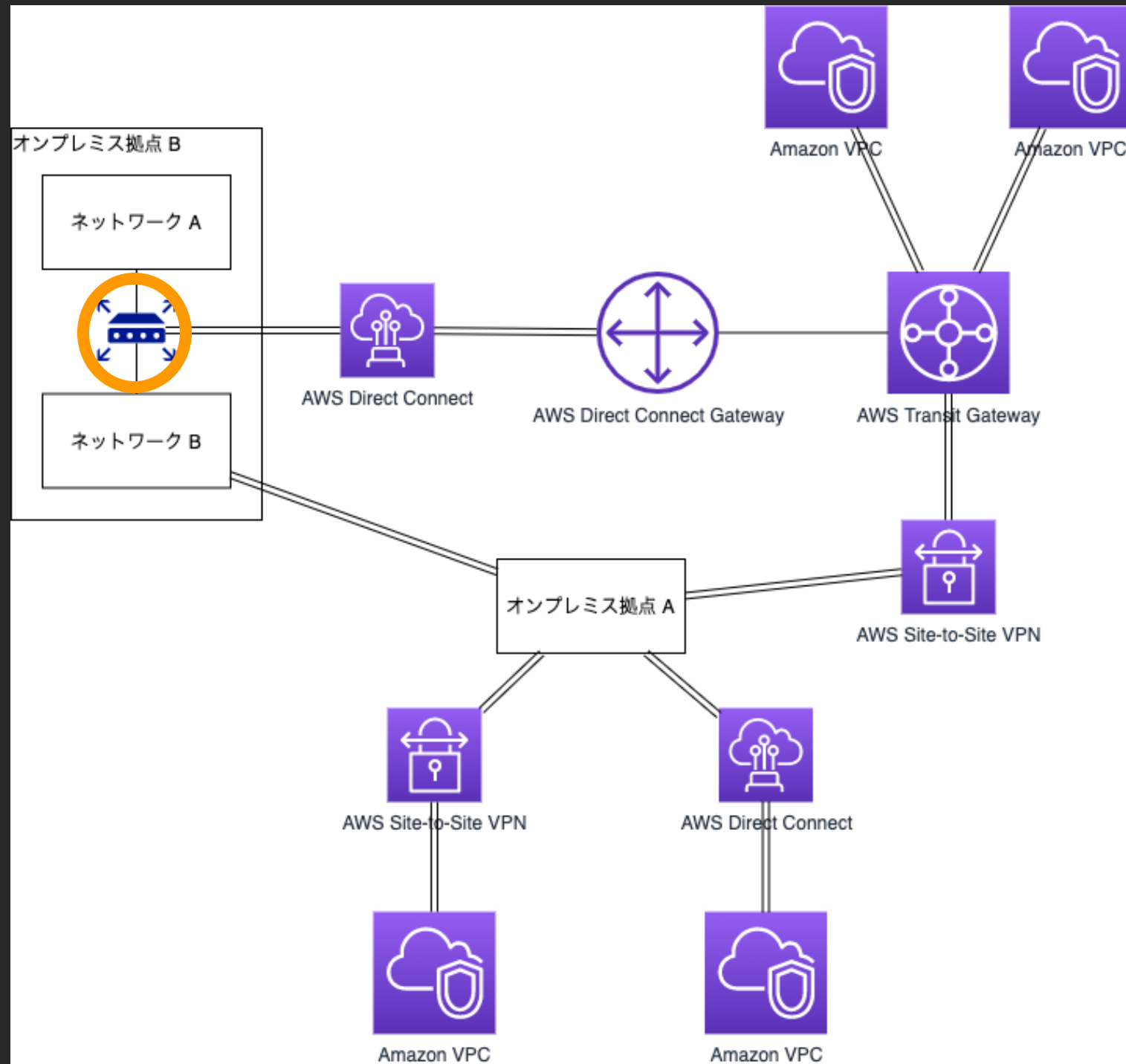
それぞれの操作によって発生するネットワーク的变化を把握する

- 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变化を把握する

- 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

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