IIJ Technical WEEK 2017
インターネットの最新技術に触れる3日間

11/9（Thu）13：45～14：30

IIJ Omnibusサービス 運用の裏側

株式会社インターネットイニシアティブ
ネットワーク本部 ネットワークサービス部 ネットワークサービス課長
和佐 好智

本日お話しする内容

1. IIJ Omnibusサービス概要
2. サービスの裏側の仕組み
3. 運用中の出来事や事件

IIJ Omnibusサービス 運用の裏側

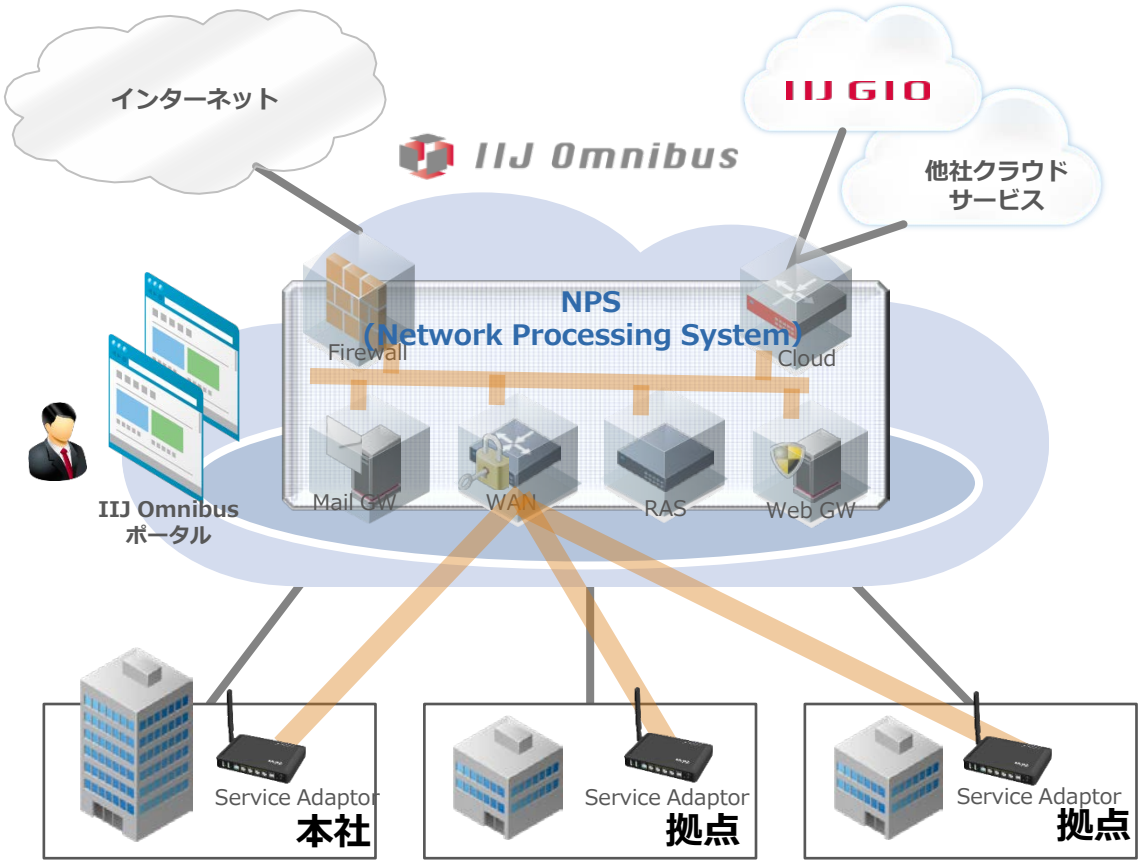
1．IIJ Omnibusサービス概要

企業ネットワークに必要な機能、
例えば**インターネット接続**、**セキュリティ**、**WAN**などを**すべて仮想化**し、
オンデマンドで提供するクラウド型のネットワークサービス(SD-WAN)
です。

最新のSDN/NFV技術を駆使し、必要な機能をオンデマンドで提供するクラウド型ネットワークサービス

ルータ、VPN装置、ファイアウォールなどの専用機器を自社で所有することなく、必要な時に必要な機能を必要な分だけ利用することが可能

- 各サービス機能は「IIJ Omnibusポータル」で一元的に契約・設定・管理が可能



クラウド上から機能を提供

クラウド上に構成されるNPSをゲートウェイとして、インターネット接続、セキュリティ、WAN接続など、お客様の**ネットワークに必要な機能をNFV技術を用いて仮想化**し、サービスモジュールとして提供します。

SDN機能で自在にネットワークを構成

お客様拠点にはサービスアダプタを設置。 **SDN技術を用いてNPSとVPNを構成**します。

サービスアダプタを繋ぐだけ

サービスアダプタは自動接続し、必要な設定を取得します。**設定情報は電源OFFで消去**。起動の度に設定を取得するため、セキュアである他、拠点の移転による回線変更や機器の故障が発生した場合にも、現地の作業はつなぐだけでネットワークの変更や復旧が完了します。

すべてをオンラインポータルで

各種ネットワーク設定、クラウドサービスとの連携や状態監視にいたるまで、**ネットワーク全体の一元的な運用管理が可能**です。

「機能モジュール」として必要な機能をご提供

企業に求められるネットワーク機能を「機能モジュール」として、必要な時に、必要な機能を、必要な分だけ自在に選択して利用可能。

① インターネットアクセスモジュール
・高品質なIIJバックボーンへ直結

② エンハンストファイアウォールモジュール
・未知のマルウェア検出・防御も可能な次世代Firewall

③ IIJセキュアMX連携モジュール
・SMXと接続しメールセキュリティ機能を提供

④ IIJセキュアWebゲートウェイ連携モジュール
・SWGと接続しWebセキュリティ機能を提供

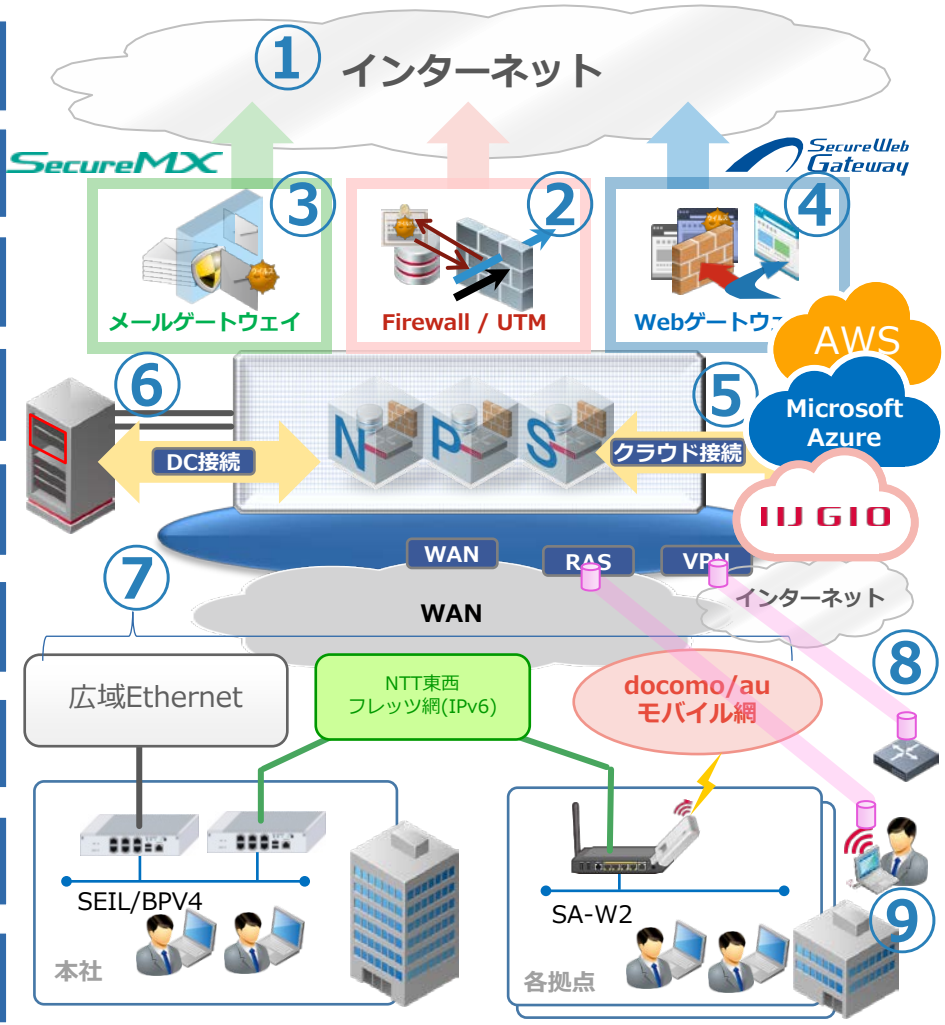
⑤ クラウドエクスチェンジモジュール
・各種クラウドサービスとの閉域接続環境を提供

⑥ コネクタモジュール
・IIJ DCに設置した物理アプライアンスと接続

⑦ WANモジュール
・閉域網やフレッツ、モバイルなど多彩な接続に対応

⑧ VPNモジュール
・お客様用意のルータ等からのIPsec VPN接続に対応

⑨ リモートアクセスモジュール
・ノートPCやスマートデバイスからセキュアに接続



「機能モジュール」として必要な機能をご提供

企業に求められるネットワーク機能を「機能モジュール」として、必要な時に、必要な機能を、必要な分だけ自在に選択して利用可能。

① インターネットアクセスモジュール
・高品質なIIJバックボーンへ直結

② エンハンストファイアウォールモジュール
・未知のマルウェア検出・防御も可能な次世代Firewall

③ IIJセキュアMX連携モジュール
・SMXと接続しメールセキュリティ機能を提供

④ IIJセキュアWebゲートウェイ連携モジュール
・SWGと接続しWebセキュリティ機能を提供

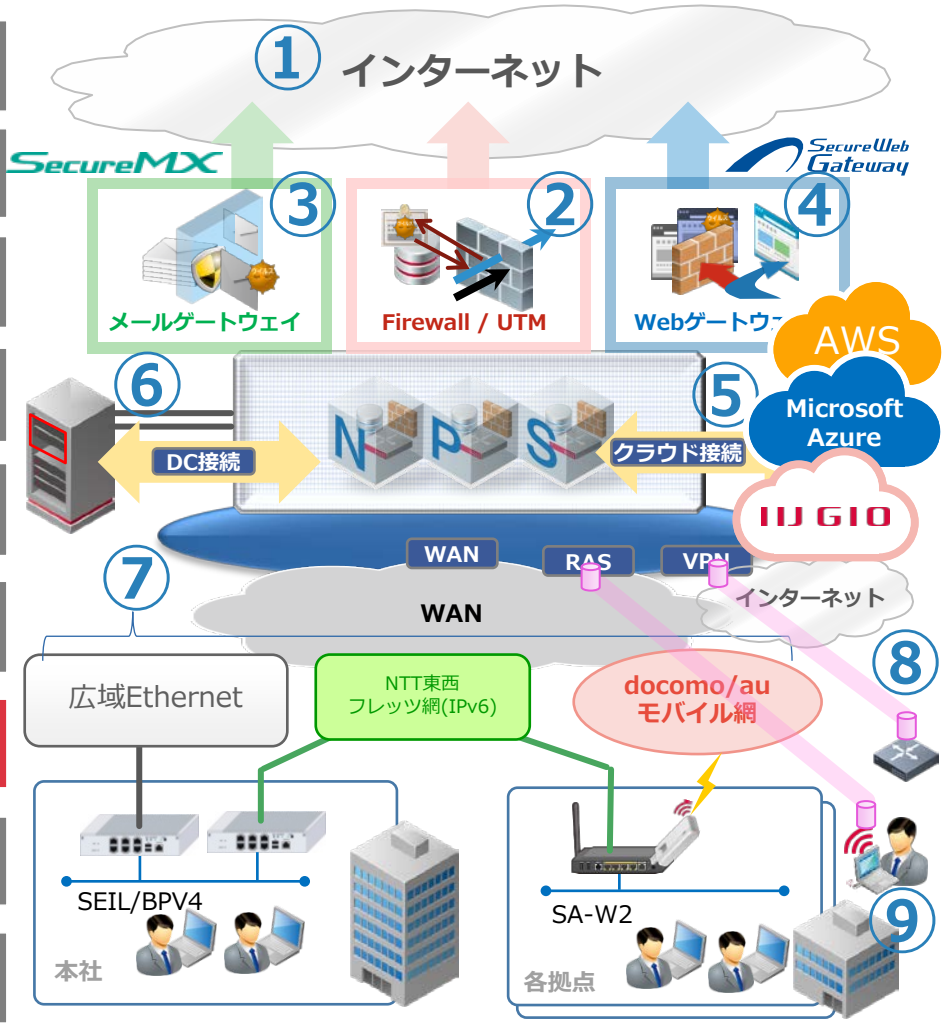
⑤ クラウドエクスチェンジモジュール
・各種クラウドサービスとの閉域接続環境を提供

⑥ コネクタモジュール
・IIJ DCに設置した物理アプライアンスと接続

⑦ WANモジュール
・閉域網やフレッツ、モバイルなど多彩な接続に対応

⑧ VPNモジュール
・お客様用意のルータ等からのIPsec VPN接続に対応

⑨ リモートアクセスモジュール
・ノートPCやスマートデバイスからセキュアに接続



WAN環境を簡易的に構築するための機能を提供

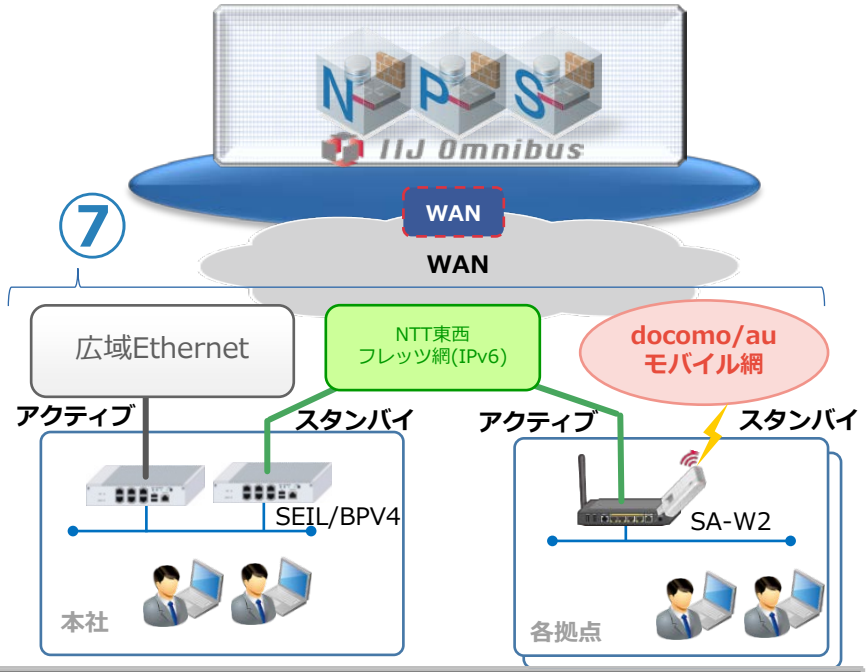
⑦ WANモジュール
・閉域網やフレッツ、モバイルなど多彩な接続に対応

アクセス回線はマルチキャリア対応

NTT東西のフレッツ 光ネクストやIIJモバイル等のベストエフォート回線からギャランティ型の専用線まで、マルチキャリア対応で多彩な回線ラインナップから選択可能です。
回線種別によっては、**お客様用意の回線をそのまま利用していただくことも可能**です。

モバイルキャリアによる接続

IIJはモバイルサービスもマルチキャリア対応。お客様側に設置するサービスアダプタ（SA）にマルチキャリアのUSBドングルを接続するだけで、簡単にマルチキャリアモバイル冗長WAN環境を構築することが可能です。



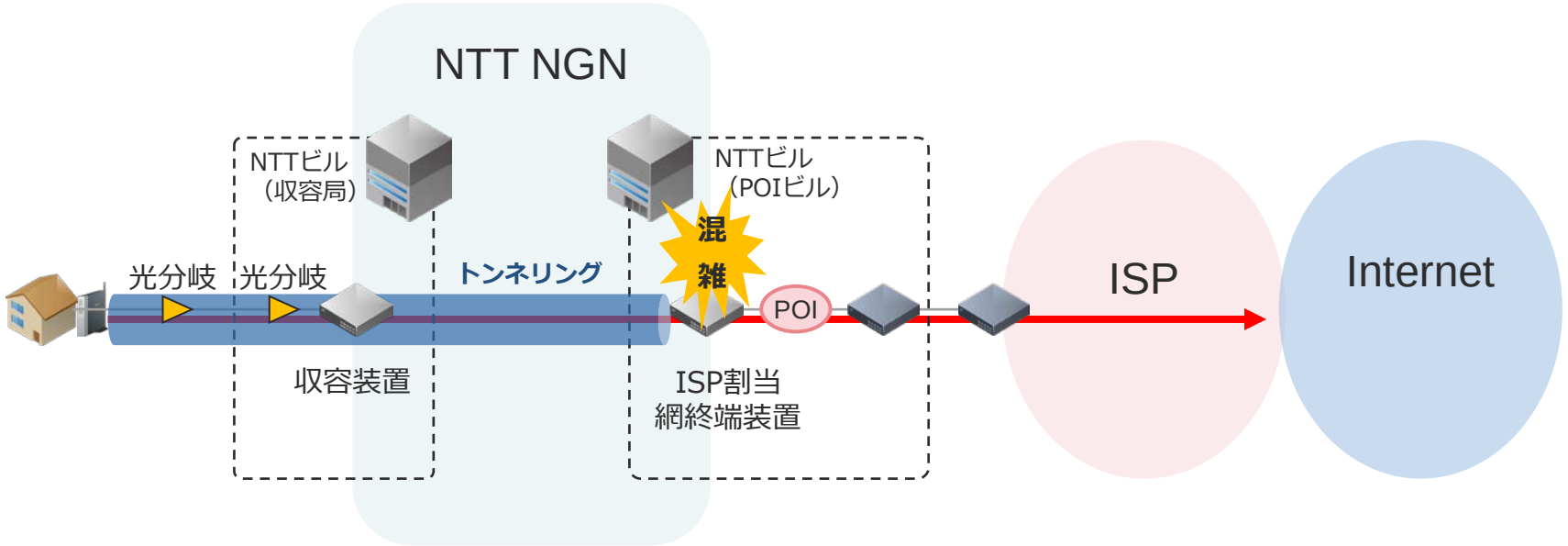
IIJから提供されるサービスアダプタ

サービスアダプタ		主要スペック	
SA-W2 小～中規模向け 【モバイル・無線LAN対応】		●200mm（W）× 145mm（D）× 35mm（H） ●重量　約420g （ACアダプタ含まず）	●Gigabit Ethernet×1Port（WAN） ●Gigabit Ethernet×4Port（LAN） ●無線LAN2.4GHz（IEEE802.11b / 11g/ 11n） ●無線LAN 5 GHz(IEEE802.11a / 11ac / 11n) ●USB×2Port
SEIL/BPV4 中～大規模向け 【広帯域対応】		●194mm（W）× 283mm（D）× 44mm（H） ●重量　1.9kg （装置全体）	●Gigabit Ethernet×1Port（WAN） ●Gigabit Ethernet×6Port（LAN） ●USB×2Port

フレッツ光の輻輳問題

NTT NGNとISP網間の相互接続部分（網終端装置）において混雑が発生し、通信速度が低下してしまう現象

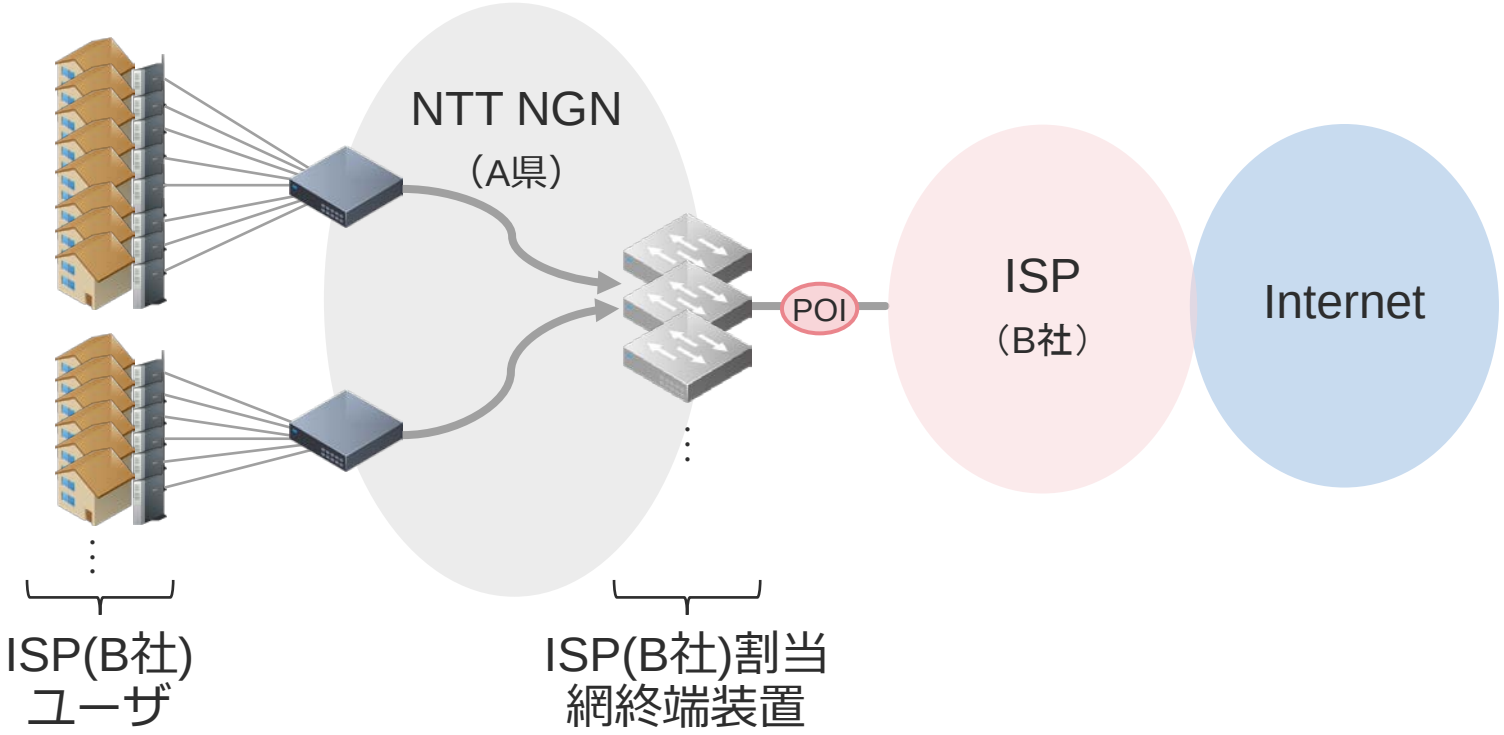
- 昨今ではPPPoE方式での接続時に問題が発生
- エリアや事業者によって通信速度が上下する原因の一つ
- フレッツ光や各事業者が提供する光コラボ※等で発生



※光コラボ：光コラボレーションの略称で、NTT東日本／西日本が提供する光回線「フレッツ光」を各事業者（プロバイダなど）が借り受け、様々な独自サービスなどを付加して各社の“ブランド”として販売するモデルのこと

PPPoE方式を利用する場合、NTTビル内の「網終端装置※」に利用者の通信が集約され、各ISP事業者網と相互接続

・フレッツ光などのブロードバンドサービスは
統計多重効果を期待して多数の通信を集約することで
コストを抑えて安価にインターネット接続を提供

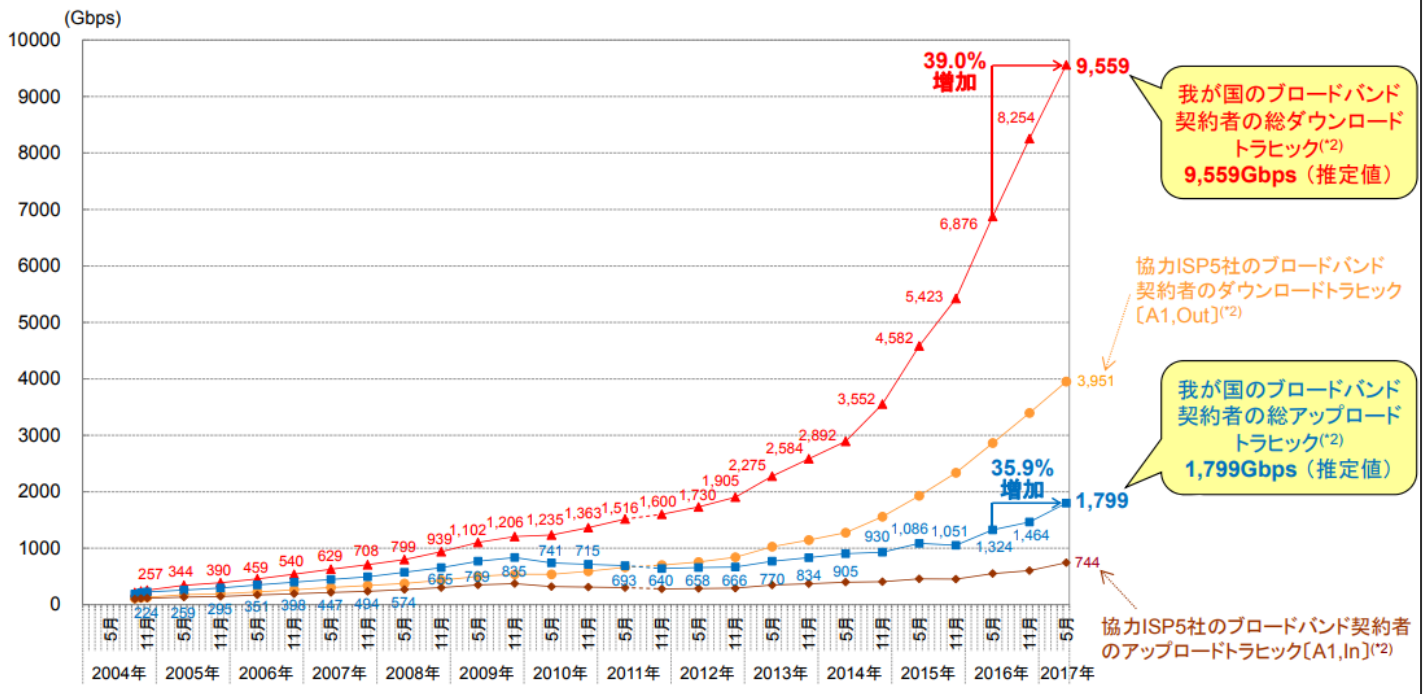


※原則として都道府県毎に網終端装置が設置されており、エリア毎の利用者数に応じて装置増設依頼が許可される

リッチコンテンツの増加に伴って、ブロードバンド契約者のトラフィックが年々増加

２．我が国のブロードバンド契約者の総トラヒック

○ 我が国のブロードバンドサービス契約者(*1)の総ダウンロードトラヒックは推定で約9.6Tbps（前年同月比39.0%増）。
○ また、総アップロードトラヒックは推定で約1.8Tbps（前年同月比35.9%増）。



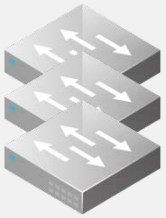
(*1) FTTH、DSL、CATV、FWA
(*2) 2011年5月以前は、一部の協力ISPとブロードバンドサービス契約者との間のトラヒックに携帯電話網との間の移動通信トラヒックの一部が含まれていたが、当該トラヒックを区別することが可能となったため、2011年11月より当該トラヒックを除く形でトラヒックの集計・試算を行うこととした。

2

（総務省 H29年8月15日 公開資料より）http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000119.html

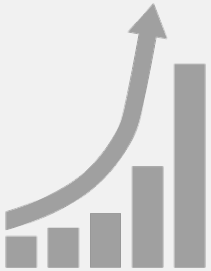
フレッツ光の輻輳問題 まとめ

大量ユーザ通信を集約する網終端装置



×

ユーザ当りのトラフィック増加



＝

フレッツ光の「輻輳」

✓ 同じISPでもエリアによって混雑状況が異なることがあります

- 網終端装置を設置するNTTビルは都道府県毎に指定されており、原則、網終端装置も別々に設置されています。
- エリア内の利用者数の変動や、装置の増設タイミングによって、エリア毎の混雑状況が異なります。

✓ 同じ県でもISPによって混雑状況は異なることがあります

- 網終端装置はISP毎に別々の設備のため、ISP毎のユーザ増加数や増設タイミングにより混雑状況は異なります。

✓ ブロードバンドルータを再起動すると通信速度がある程度改善することがあります

- ISPによってはユーザ数に応じて網終端装置が複数存在する場合があり、ルータの再起動等でPPPoE接続の再試行を行い混雑の少ない網終端装置に接続された場合、通信速度がある程度改善されることがあります。

IIJ Omnibusサービス 運用の裏側

2．サービスの裏側の仕組み

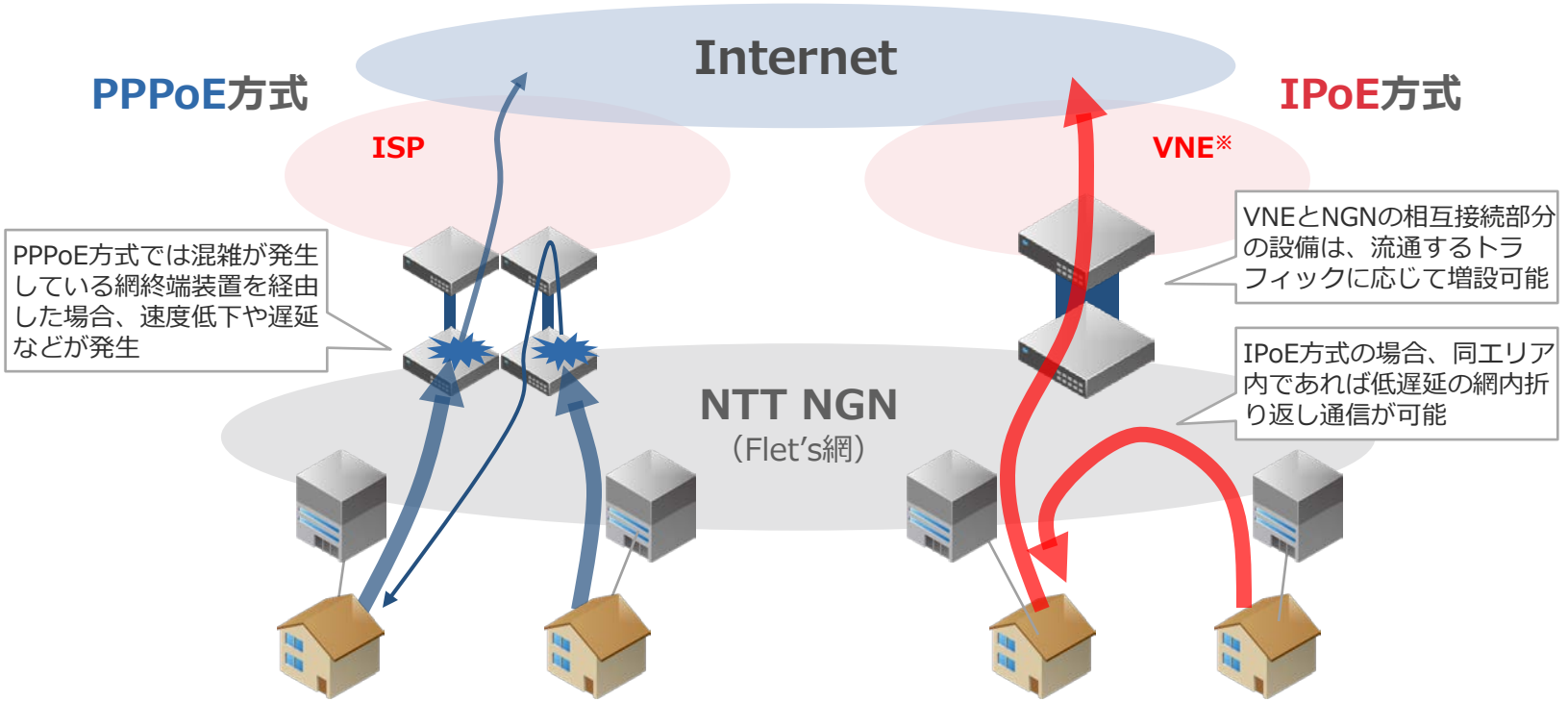
フレッツ光の輻輳問題を解消する、WANモジュールの裏側の仕組みを詳しくご紹介します。

IPoE方式によるIPv6接続

IIJ Omnibus

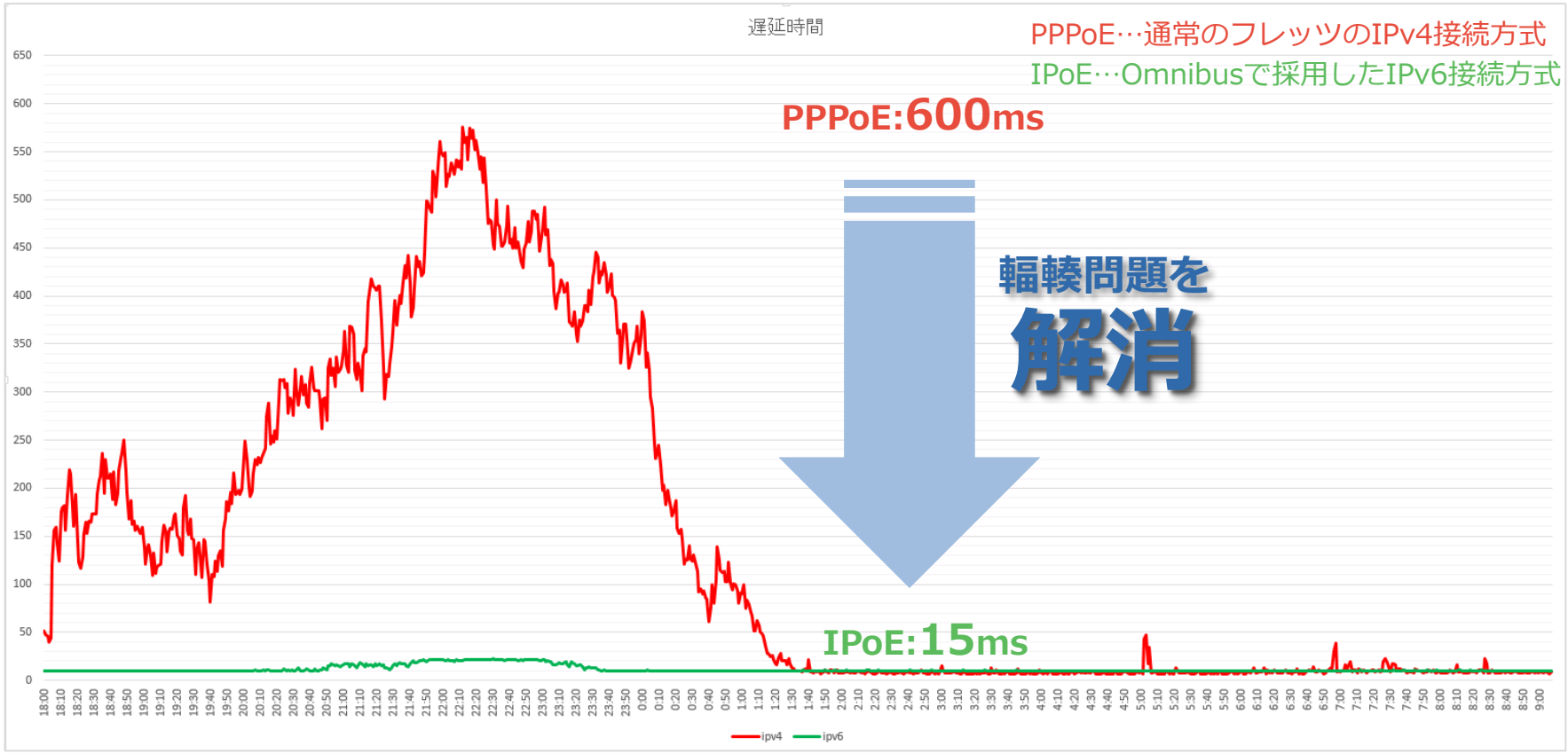
「IPoE方式」は、現在PPPoE方式でボトルネックとなっている網終端装置をバイパスする通信方式

- インターネット通信時に網終端装置を経由しないため、現在フレッツ光や光コラボで発生している網終端装置に起因する混雑は発生しない



※VNE：NGNのIPv6 IPoEサービスにおいて、IPv6インターネット接続サービスを提供する事業者

通常フレッツ光回線で行うPPPoE IPv4接続では、地域によっては大幅な遅延が見られるが、OmnibusでIPoE IPv6接続を利用することで輻輳問題が解消、遅延問題も大きく改善

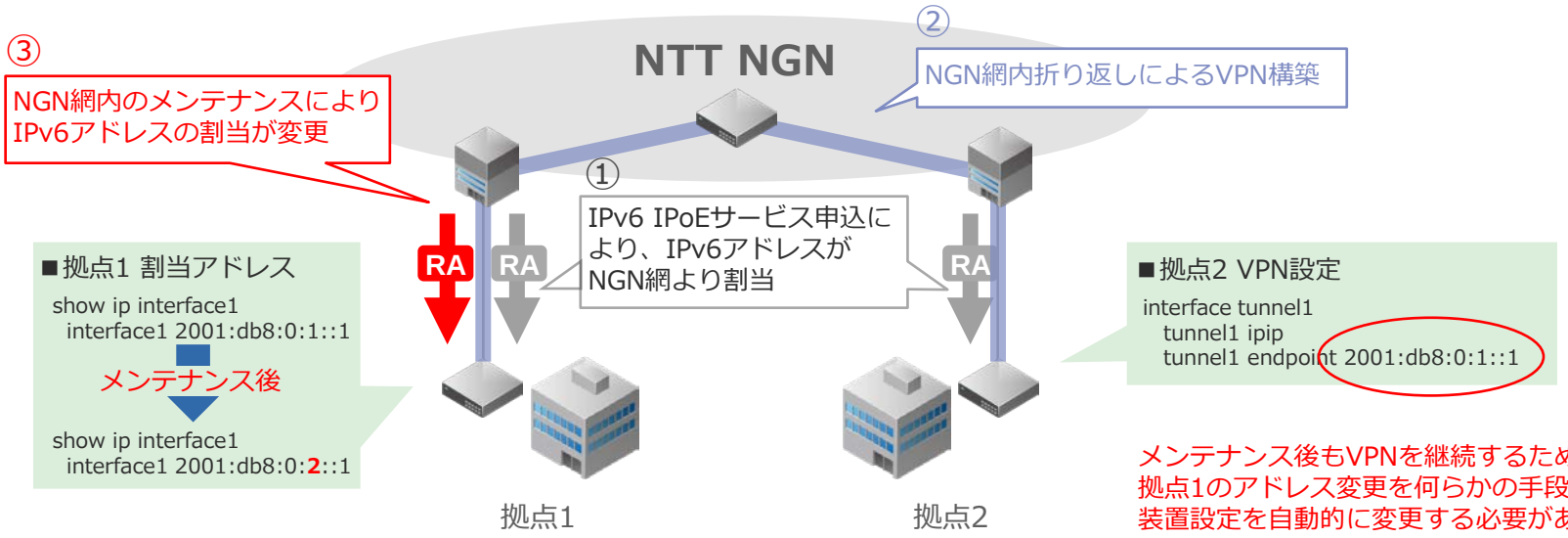


NTT NGNのIPv6 IPoEサービスにおける注意点

- **現在主流のIPv4は利用できない**
  ⇒「DS-Lite※」等のIPv4 over IPv6 技術を用いることで、IPv4での通信も可能
  ⇒ IPv4のreachabilityが存在する拠点に対し、IPsecでトンネリングで対応する等
  ※DS-Lite：次項参照

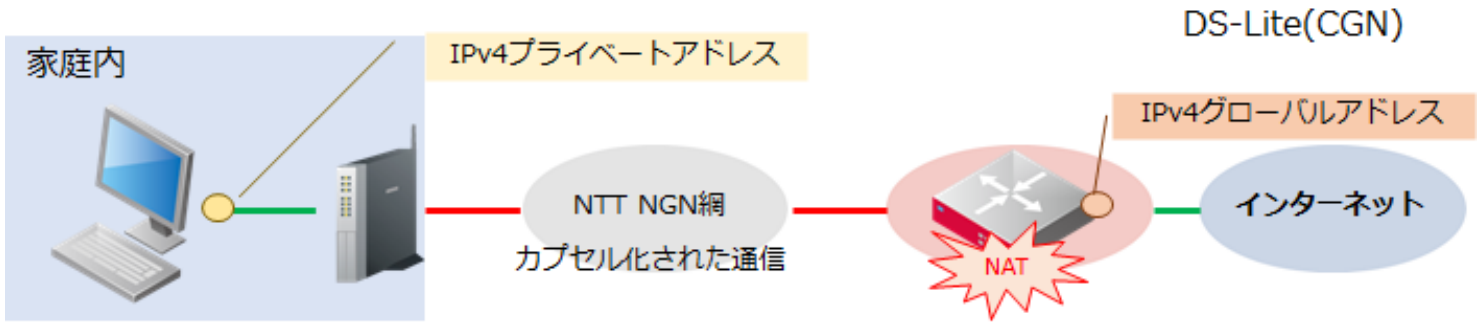
- **NTTにより払い出されるIPv6アドレスは半固定**
  NTT側の設備メンテナンスによって変更される場合あり
  移転、場変、品目変更などで変更となる場合あり

  ⇒VPNを構築する場合、対向拠点の不定期なアドレス変更への追従が課題に



IPv4をIPv6で運ぶ DS-Lite（RFC6333 Dual-Stack Lite）

- IPv6ネットワーク上でIPv4インターネットへの接続環境を実現する標準技術
- IPv6をメインとして、IPv4のサービスを維持するための仕組み



DS-LiteによるシンプルなCGN(Carrier Grade NAT)

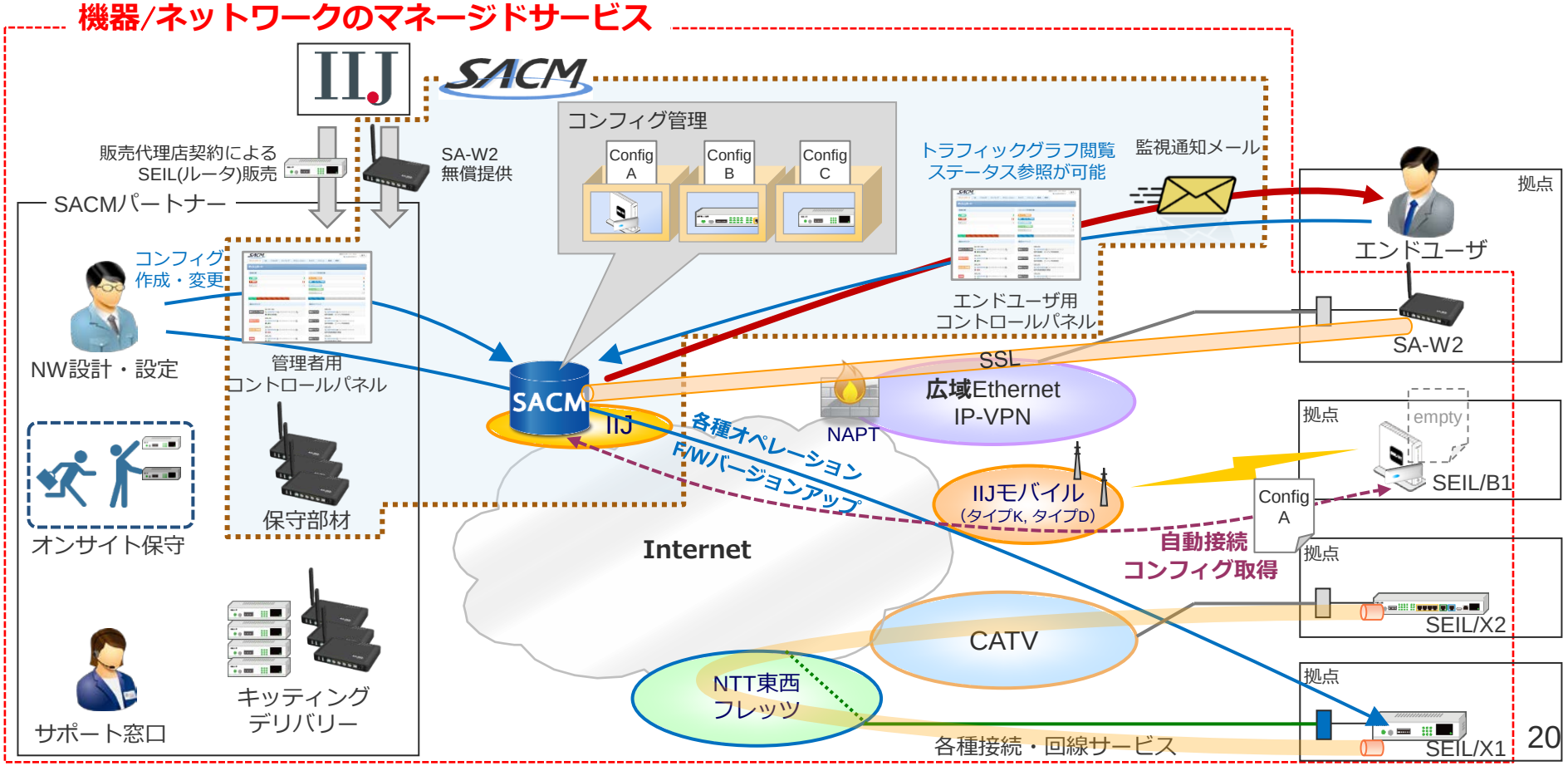
＜注意点＞

DS-Liteはフレッツ光ネクストで**IPoE方式のIPv6が利用できることが前提**となります。DS-Lite 対応ルータのみではご利用いただけません。

SACMは、機器の自動接続・一元管理を実現する特許技術「SMF(※)」を基に開発された、マネジメントシステムをご提供するOEM専用サービス

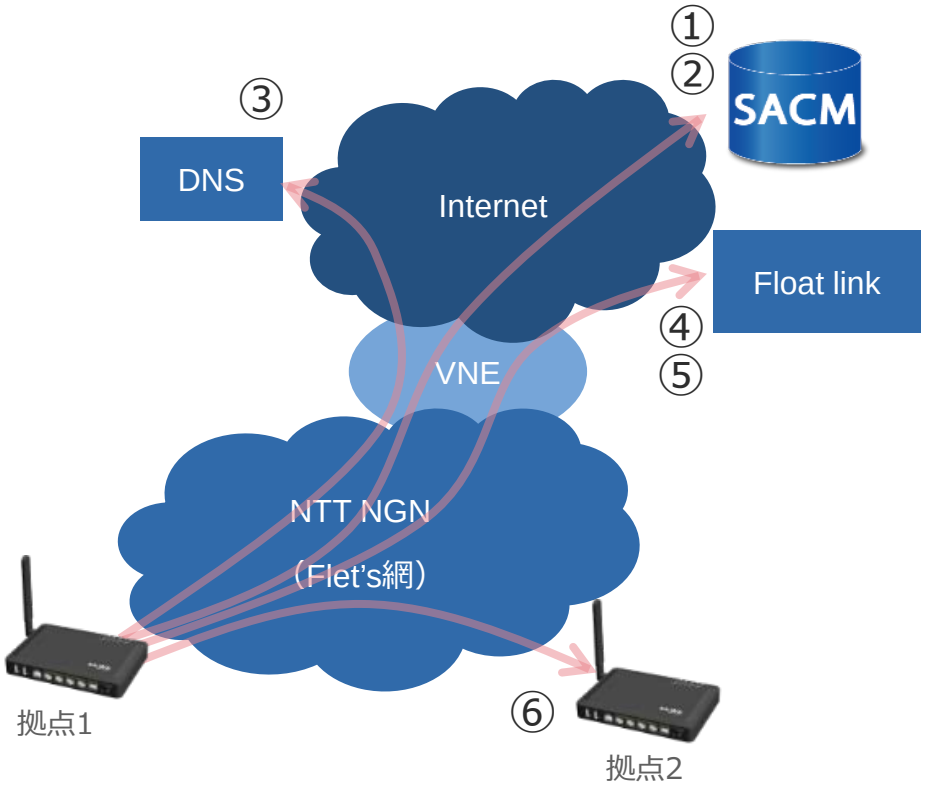
※SEIL Management Frameworkの略

本サービスを活用することで、機器/ネットワークの各種マネージドサービスを低コストかつスピーディーに開始出来ます。



SACMにおけるVPN自動設定機能の一つ

- サービスアダプタのFloat link機能を使用すると、ネームサーバとの連携によってVPN接続を行う対向ノード（サービスアダプタ）のIPアドレスを自動的に設定し、IPアドレスが変更された際に自動追従することができる



① 事前設定

- SACM に Config や ID を登録

② Configの取得

- ノード起動時にSACMへアクセスし、Configを取得

③ DNS での名前解決

- Float linkサーバのアドレス解決

④ Float link へ登録

- Float link サーバへIDやアドレスを登録

⑤ 対向アドレスの取得

- VPN の対向アドレスを取得

⑥ VPN 接続

- 対向ルータとのVPN接続

WAN環境を簡易的に構築するための機能を提供

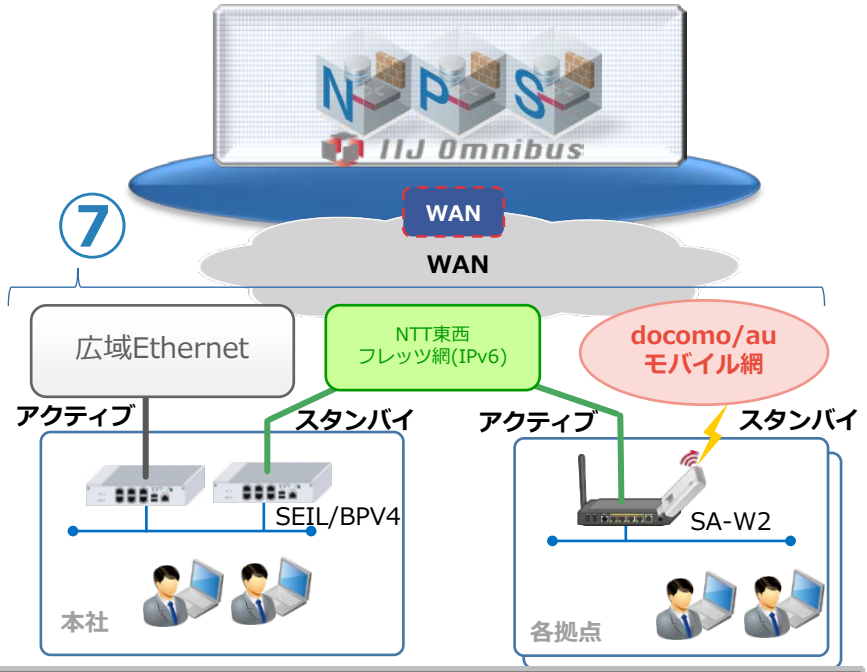
⑦ WANモジュール
・閉域網やフレッツ、モバイルなど多彩な接続に対応

アクセス回線はマルチキャリア対応

NTT東西のフレッツ 光ネクストやIIJモバイル等のベストエフォート回線からギャランティ型の専用線まで、マルチキャリア対応で多彩な回線ラインナップから選択可能です。
回線種別によっては、**お客様用意の回線をそのまま利用していただくことも可能**です。

モバイルキャリアによる接続

IIJはモバイルサービスもマルチキャリア対応。お客様側に設置するサービスアダプタ（SA）にマルチキャリアのUSBドングルを接続するだけで、簡単にマルチキャリアモバイル冗長WAN環境を構築することが可能です。



IIJから提供されるサービスアダプタ

サービスアダプタ		主要スペック	
SA-W2 小～中規模向け 【モバイル・無線LAN対応】		●200mm（W）× 145mm（D）× 35mm（H） ●重量　約420g （ACアダプタ含まず）	●Gigabit Ethernet×1Port（WAN） ●Gigabit Ethernet×4Port（LAN） ●無線LAN2.4GHz（IEEE802.11b / 11g/ 11n） ●無線LAN 5 GHz(IEEE802.11a / 11ac / 11n) ●USB×2Port
SEIL/BPV4 中～大規模向け 【広帯域対応】		●194mm（W）× 283mm（D）× 44mm（H） ●重量　1.9kg （装置全体）	●Gigabit Ethernet×1Port（WAN） ●Gigabit Ethernet×6Port（LAN） ●USB×2Port

IIJ Omnibusサービス 運用の裏側

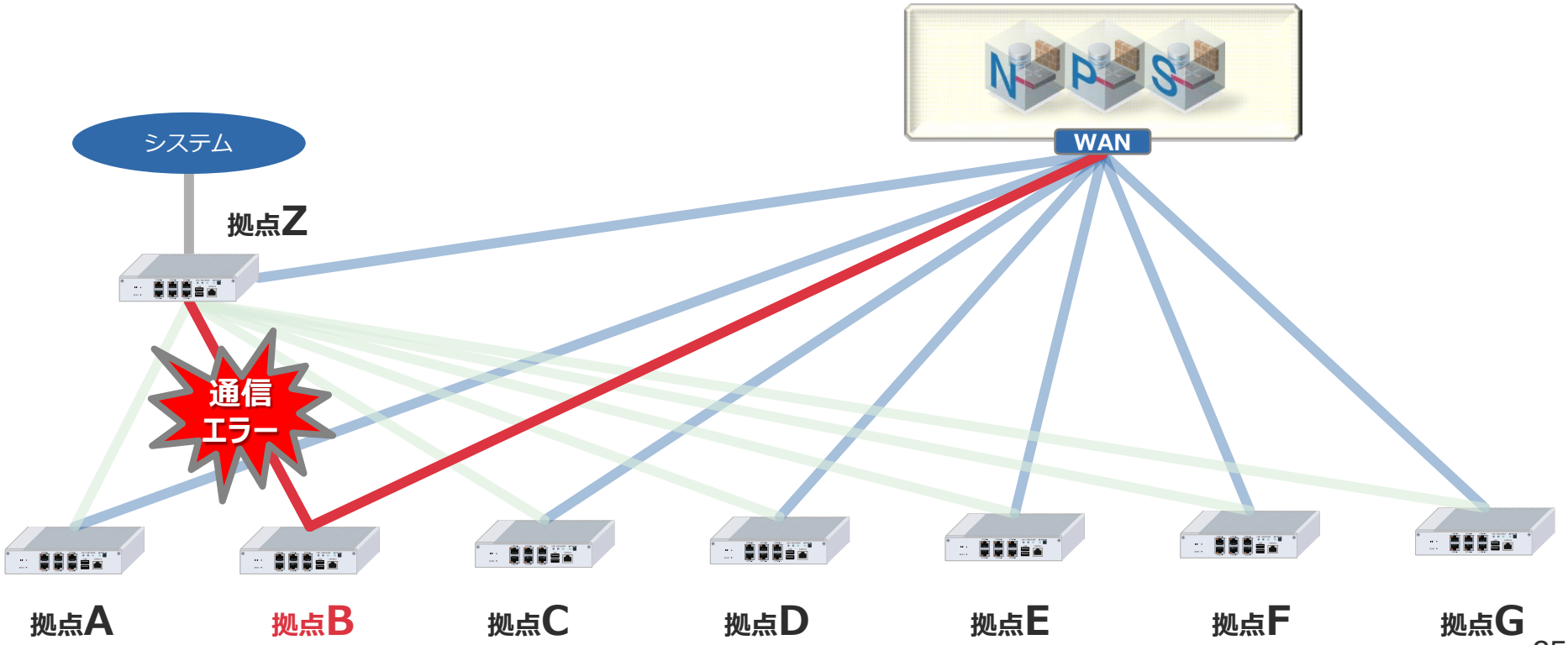
3．運用中の出来事や事件

IIJ Omnibusサービスを運用してきた約2年間に起きた様々な出来事や
事件の中で、今回はWANモジュールに関連したトピックをご紹介します。

無効化したはずのESXiの
FWモジュールが誤動作
（しかもIPv6だけ）

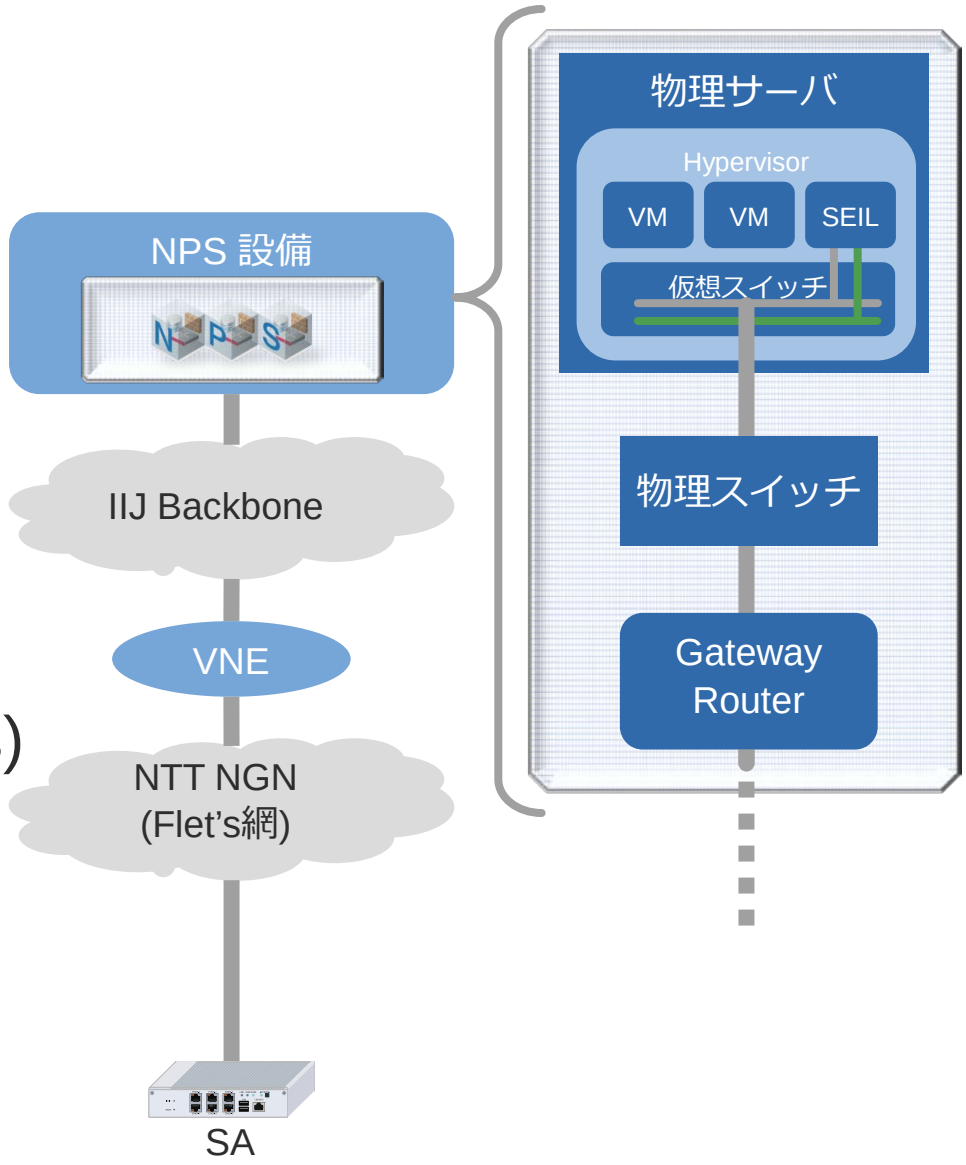
発生事象

- Omnibus への移行後、特定拠点からアプリケーション通信でエラーが増加
- 拠点Bからの通信のみ1日に数回数秒から数十秒の ping ロスが発生
- VPN の切断は発生していない



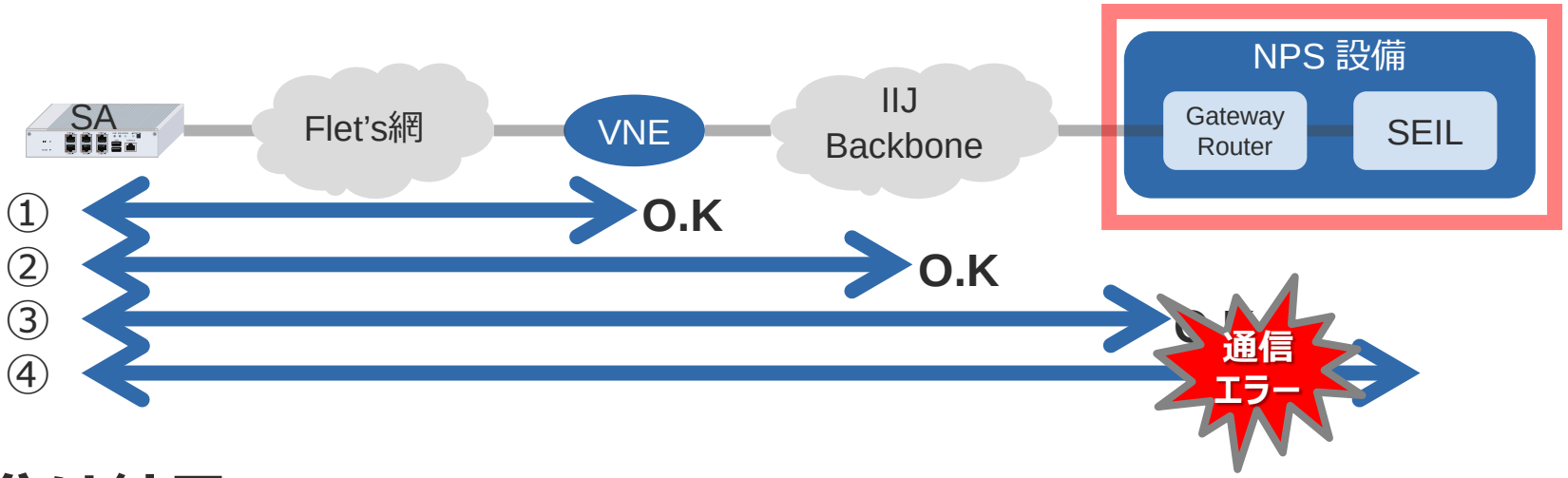
調査対象

- ✓ NPS 設備
  - Gateway Router
  - 物理 スイッチ
  - 物理サーバ(NIC)
  - Hypervisor
  - 仮想スイッチ
  - 仮想ルータ(SEILx86)
- ✓ IIJ バックボーン
- ✓ Flet's網との接続点
- ✓ 足回り回線(NTT Flet's)
- ✓ サービスアダプタ



切り分け作業＃１

- （大まかに）どこでロスが発生しているかあたりをつける
- 下記区間でそれぞれ観測を行い、どの区間でパケットロスが発生しているか切り分け



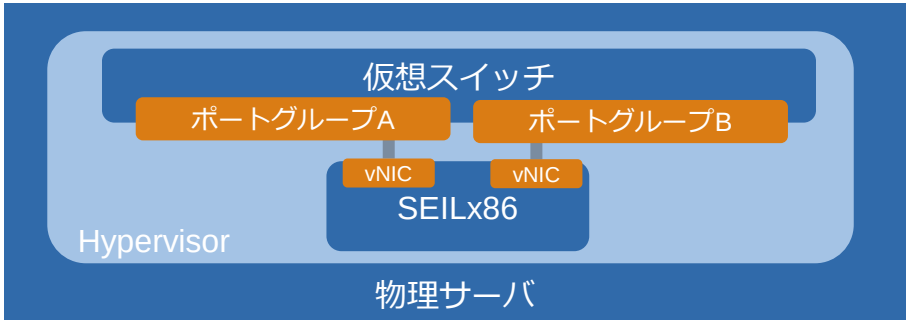
切り分け結果

- ①,②,③は問題無し
- ④のグローバルとVPN内のプライベートでそれぞれ断が発生
- IPv6通信のみ断続的に切れている
- Ping 疎通断が発生した際、Destination unreachable: Address unreachable が発生

  ⇒原因は**NPS 設備内**にあると絞り込み

切り分け作業＃２

- （前項の切り分け結果を踏まえ）NPS 設備内の仮想スイッチとVMの仮想NICでパケットダンプを取得



原因

- 仮想スイッチが IPv6 NDP※ を落としていた！

  ⇒vNICでは観測されていた IPv6 NDP が仮想スイッチでは見つからない！

  ⇒ NDP がルータまで届かないため、ルータでは Destination unreachable になってしまう
- VMware NSX の分散FW モジュールが有効なホストで発生する、**稀に IPv6 NDP を落としてしまう分散FWのバグ**
- 分散FWの機能自体は元々無効にしていたが、**サーバ機器の入れ替え時に有効になってしまうバグ**があった

※NDP：Neighbor Discovery Protocolの略で、IPv6における近隣者を発見するためのプロトコル

対処

- 分散FWの無効化！
  ⇒サーバ入れ替え時に分散FWを無効化する手順を追加。。。

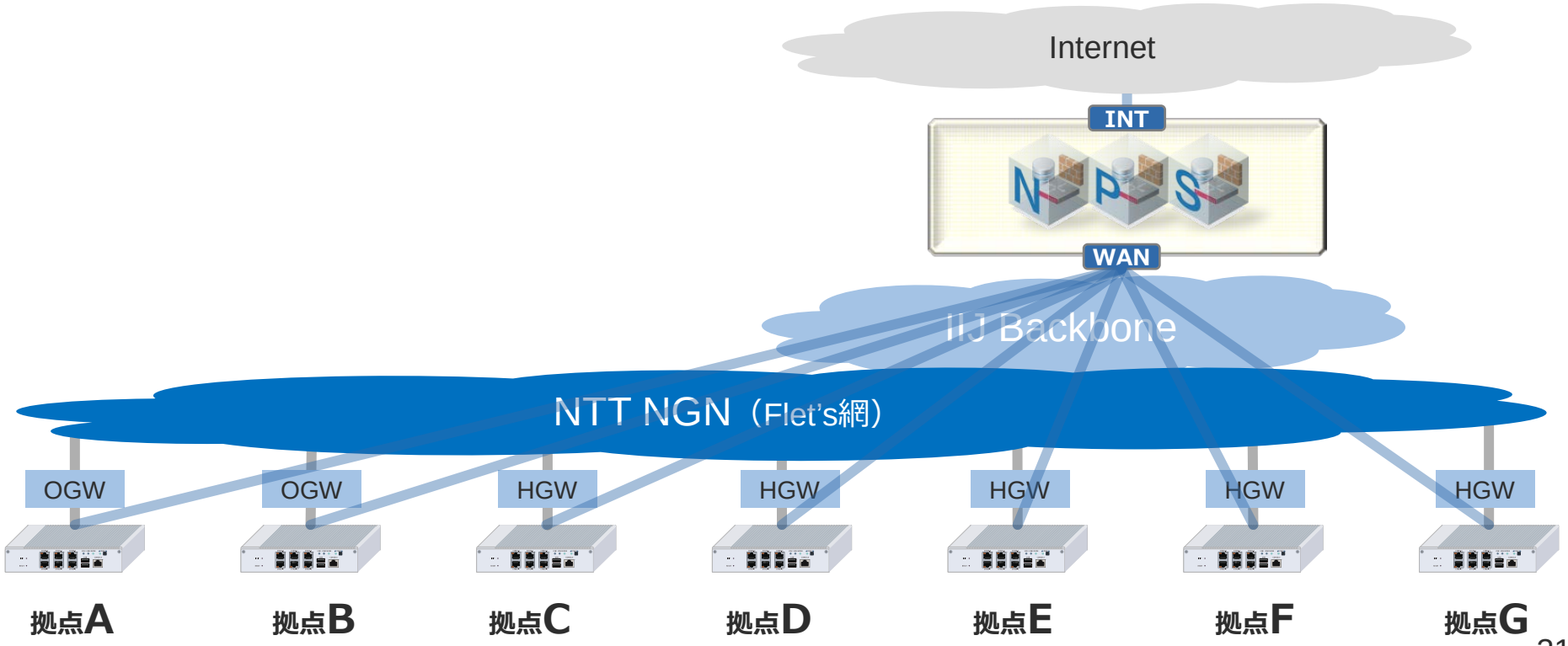
本事例のポイント

- **障害切り分けの基本的なアプローチは、物理環境でも仮想環境でも同じ**
  ⇒ただし、技術的にも幅広い知識が必要
- **（物理環境と比べ）パケットダンプの取得が簡単にできるのは仮想化のメリット**
- **仮想環境は視覚化しづらいので、想定した経路を通過していることを確認する方法（ツール）は用意しておくべき**

ホームゲートウェイで
IPsec通信だけ遅い

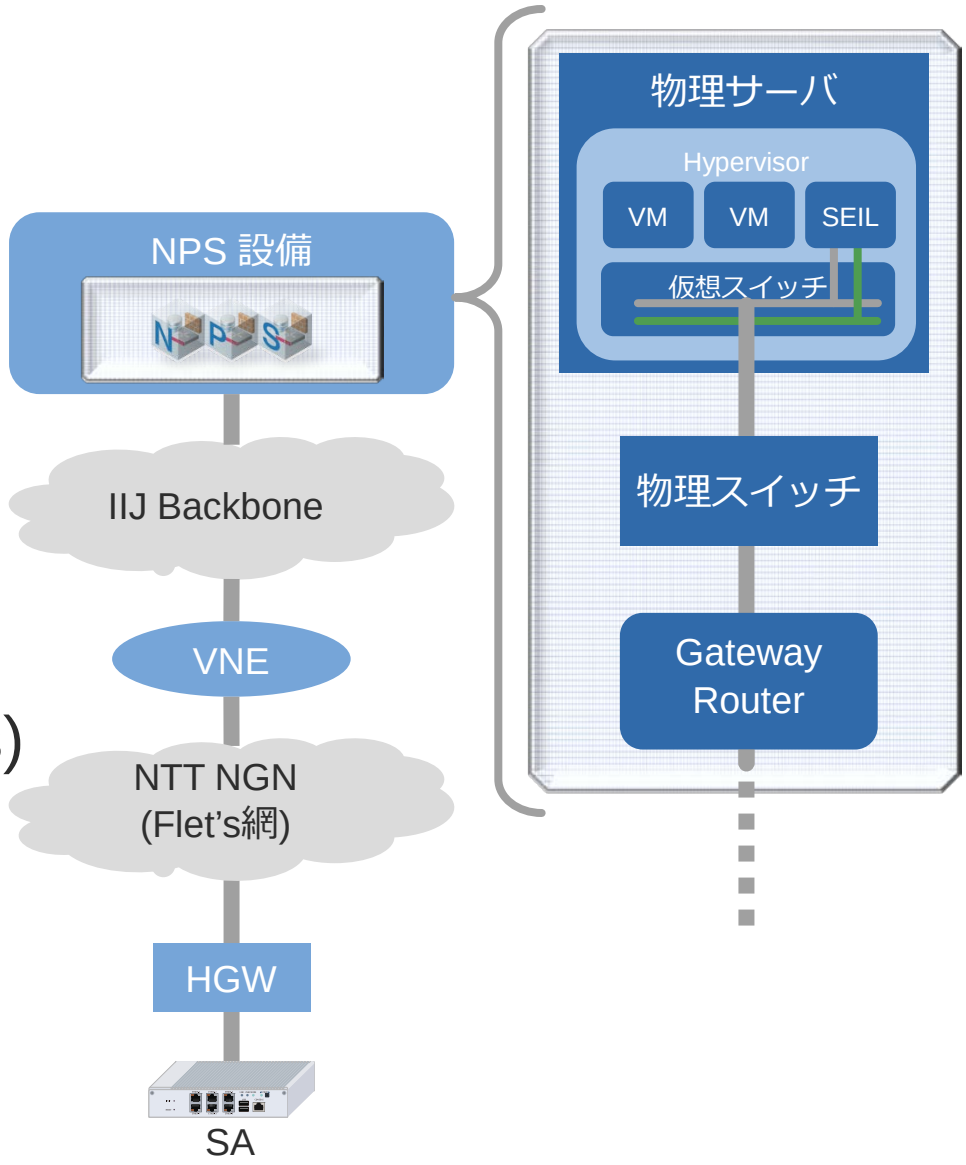
事象

- IPoE方式へ変更したが通信が遅くなった！
- ファイルダウンロードが途中で失敗する状況が連続して発生
- 同時にウェブサイトへのアクセスも出来なくなった
- インターネット通信自体もかなり遅い



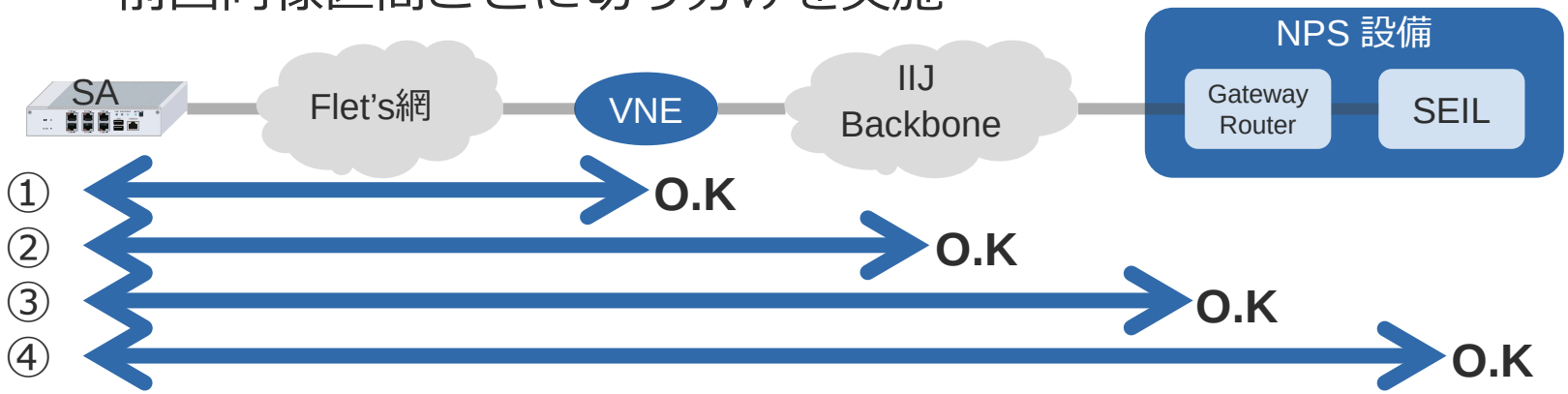
調査対象

- ✓ NPS 設備
  - Gateway Router
  - 物理 スイッチ
  - 物理サーバ(NIC)
  - Hypervisor
  - 仮想スイッチ
  - 仮想ルータ(SEILx86)
- ✓ IIJ バックボーン
- ✓ Flet’s網との接続点
- ✓ 足回り回線(NTT Flet’s)
- ✓ ホームゲートウェイ
- ✓ サービスアダプタ

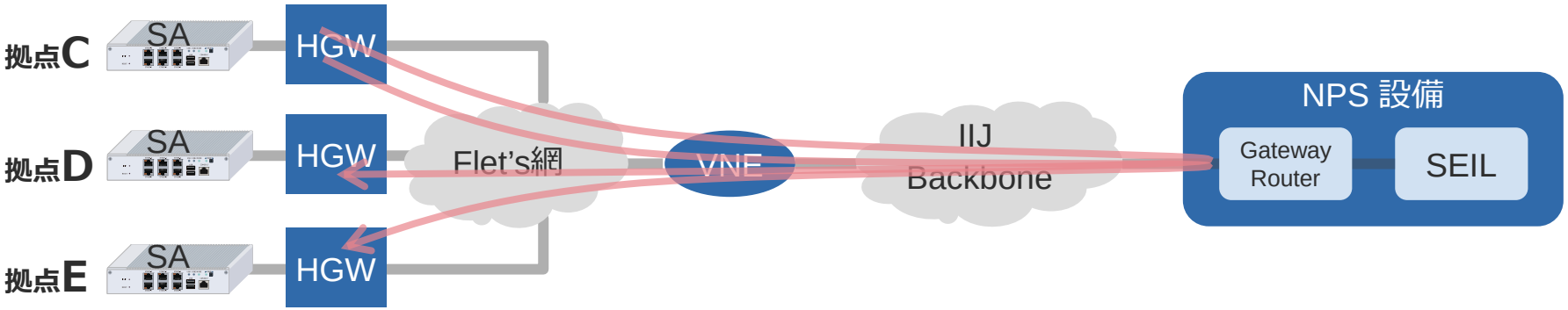


切り分け作業

- 前回同様区間ごとに切り分けを実施



- ①～④全て問題無し（ Ping では現象再現せず。。。）
- 次に拠点間の折り返しで大量のトラフィックを生成して試験を実施



切り分け結果

- Pingレベルでは発生しないが、数Mbps以上のトラフィックになるとパケットロスが発生
- 拠点毎にロスの発生し始める帯域とロスする量が異なる
- IPv4(PPPoE) 拠点では発生しないが、IPv6(IPoE) 拠点でも発生する拠点としない拠点がある
- VNE、IIJ BB、NPS設備上に異常やパケットロスの発生無し

  ⇒IPoE 拠点に依存していたため、各拠点側のホームゲートウェイへ調査範囲を拡大

原因

- Flet's で提供されている**ホームゲートウェイの機種によっては IPv6 IPsec のパフォーマンスが出ない**ことが判明

  ⇒光電話を1回線だけ利用するような小規模拠点では、個人向けのホームゲートウェイが利用される場合がある

  ⇒最新のホームゲートウェイ（500番台）では問題無いレベルの速度（100Mbps以上）で利用できることを確認

対処

- （お客様の既存回線だったため）お客様にて回線品目を変更（＝機種変更）してもらうことで本事象が解消

本事例のポイント

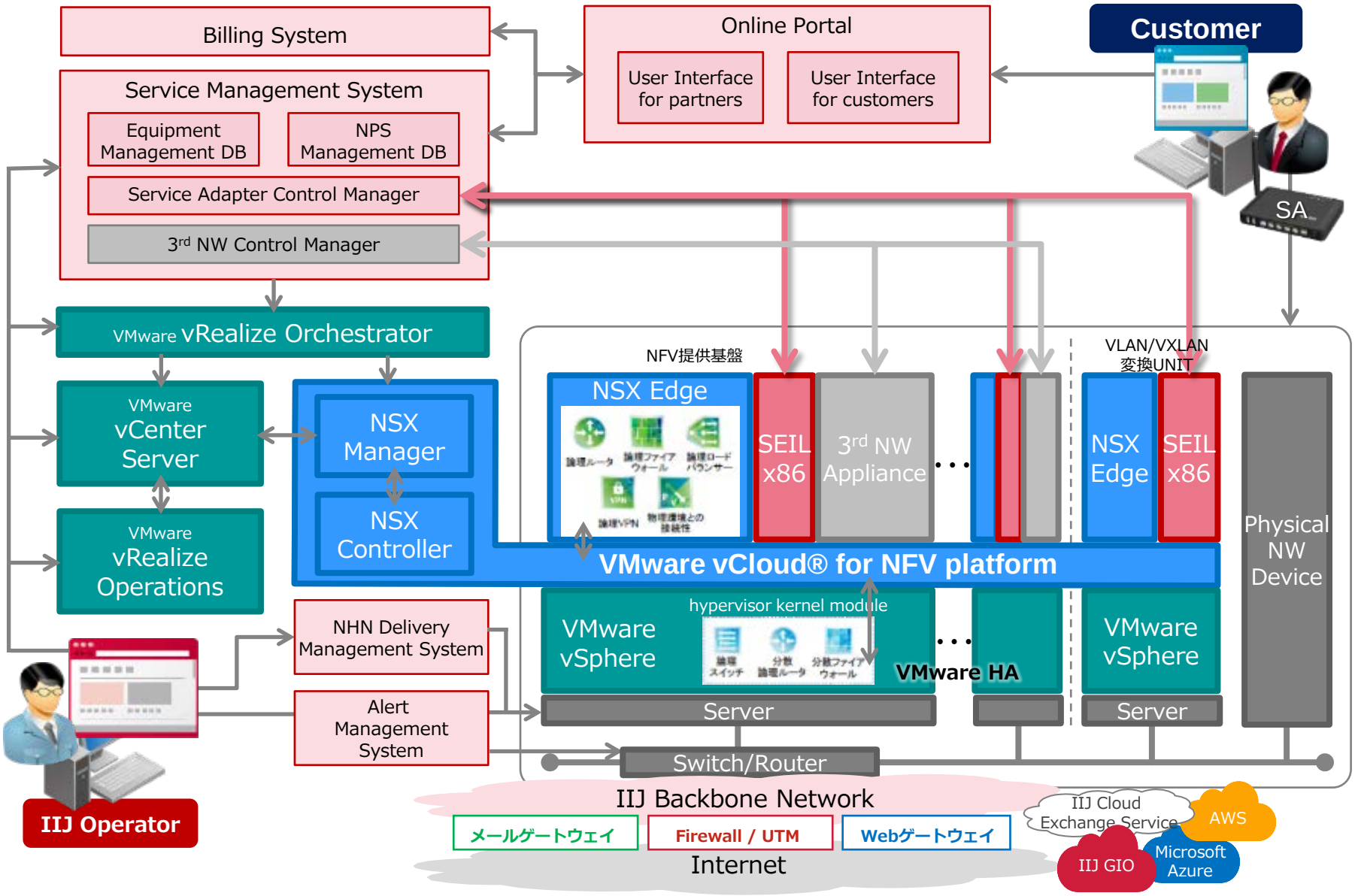
- 広域なネットワークでは様々な要素が含まれている
- 仮想化やオーバーレイの技術を使うことで論理的な部分の単純化が行えるが、様々なアンダーレイ環境への対応が必要
- お客様ネットワークの健全性をどうやって確認するかが課題

IIJ Omnibus

- IIJ Omnibusサービス -

VMware ESXiとNSXを２年間運用してきて

インフラアーキテクチャ概要図



NSXバージョンアップ

IIJ Omnibus

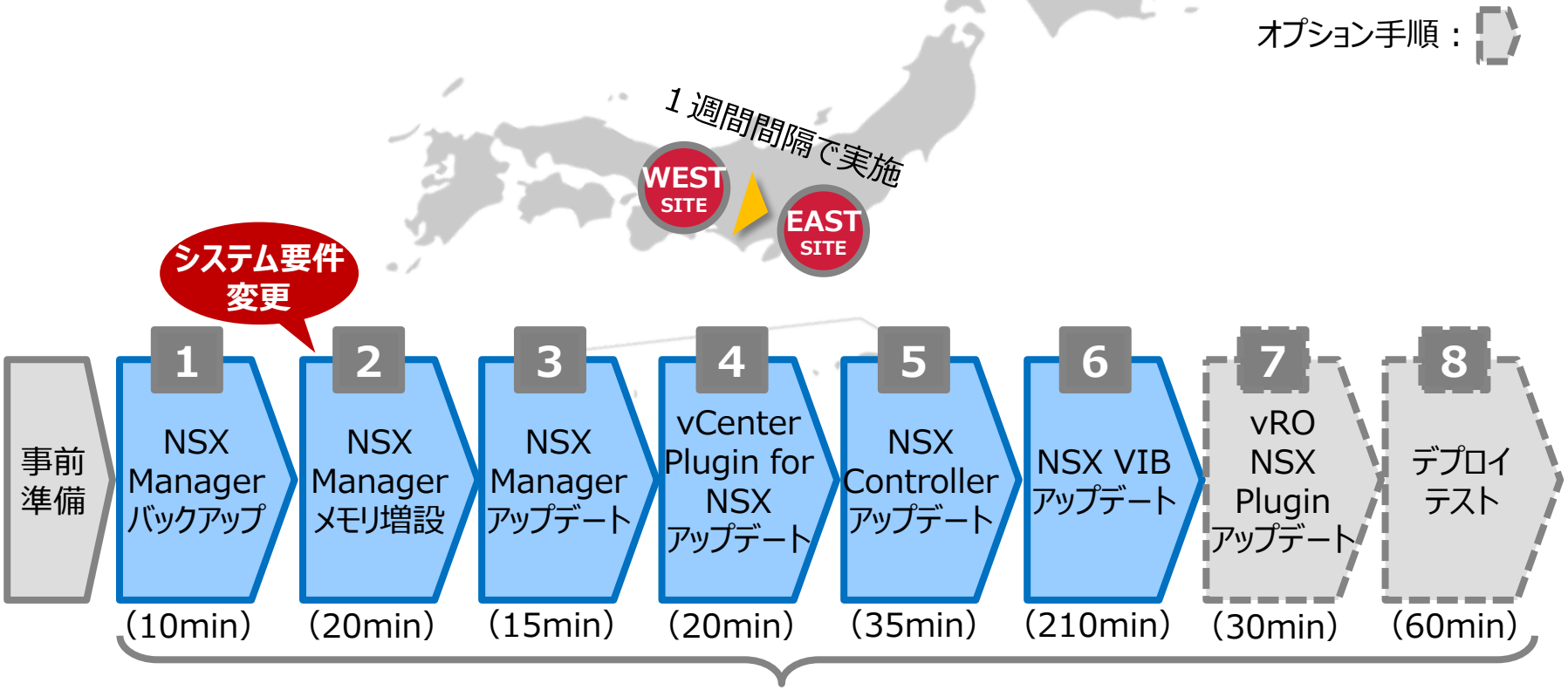
NSXコントローラのメモリリークによるダウンというリリースバージョンの抱える不具合とサービス開始１年後にはジェネラルサポート終了という課題に直面していたため、リリース早々にバージョンアップを計画

- 当時NSXのサポートライフサイクルは2年(現在は3年)と、エンタープライズ向けとしては短かった

本番稼働中のサービス設備のため、無停止でのバージョンアップが必須

- バージョンアップ対象は“**NSX**と**各種プラグイン**(vCenter,ESXi,VIB,vRO等)”
- VMware社から提示された標準アップデート手順をベースに、検証を重ねることで問題点を洗い出し、ダウンタイムが最小限になるよう再構成
- ダウンタイムが発生する自動化処理を分解し、敢えて手動で実施することで無停止手順を確立。万が一のトラブルに備え、変更した手順がサポートされることをVMware社に逐次確認

バージョンアップステップ



本事例のポイント

- **技術に追随していくためにもバージョンアップは必須だが、手順が煩雑**
  ⇒手順とツールの最適化が必要

要改善

- **導入するバージョンを見極める**
  ⇒新機能よりも不具合解消＆安定性重視

- **複数バージョンの検証環境を残しておくべき**
  ⇒バージョンアップを一度実施すると元の環境に戻すのは困難。問題の切り分け用に現行環境と新環境は常に保持しておいた方がよい

IIJ Omnibusサービス 運用の裏側

４．まとめ

1

IIJ OmnibusサービスのWANモジュール

- ✓ フレッツ光の輻輳問題に対処可能
- ✓ IPoE方式によるIPv6接続による既存の網終端装置のバイパス

2

NFV環境と物理筐体

- ✓ 仮想環境のメリット活かしていく
- ✓ 求められるサービスレベルは変わらない
- ✓ ネットワークにおける障害対応のアプローチは基本的に変わらない
  ⇒仮想環境の知見があると尚良い
  ⇒可視化のための工夫(ツール)が必要

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。

IIJ-BKLT999-0001