FUJITSU
shaping tomorrow with you

# AGW: Access Gateway for Slice of vNode System

2014/04/11 第9回NV研究会

○雨宮 宏一郎, 加藤 順一, 高橋 広, 上野 仁, 阿比留 健一, 大吉 章次
富士通株式会社

本研究成果は情報通信研究機構 (NICT) 委託研究 "「新世代ネットワークを支えるネットワーク仮想化基盤技術の研究開発」課題ア 統合管理型ネットワーク仮想化基盤技術の研究開発"により得られたものです

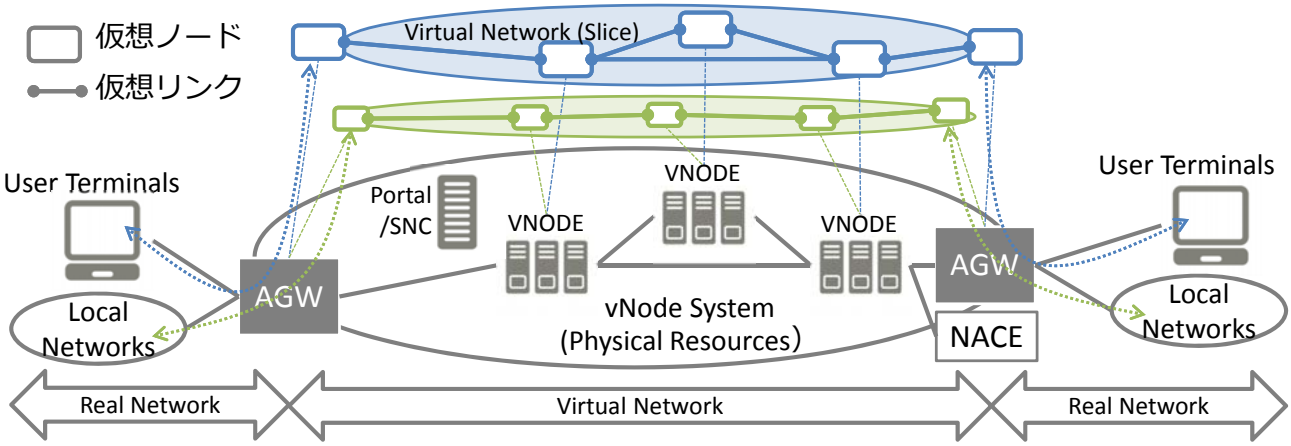


## vNode SystemとAGWの位置付け

FUJITSU

- ネットワーク仮想化基盤: vNode system
  - 仮想的なネットワーク資源 (Link), 計算・ストレージ資源 (Node) で構成される仮想ネットワーク (Slice)を、物理資源から切り出して提供するプラットフォーム

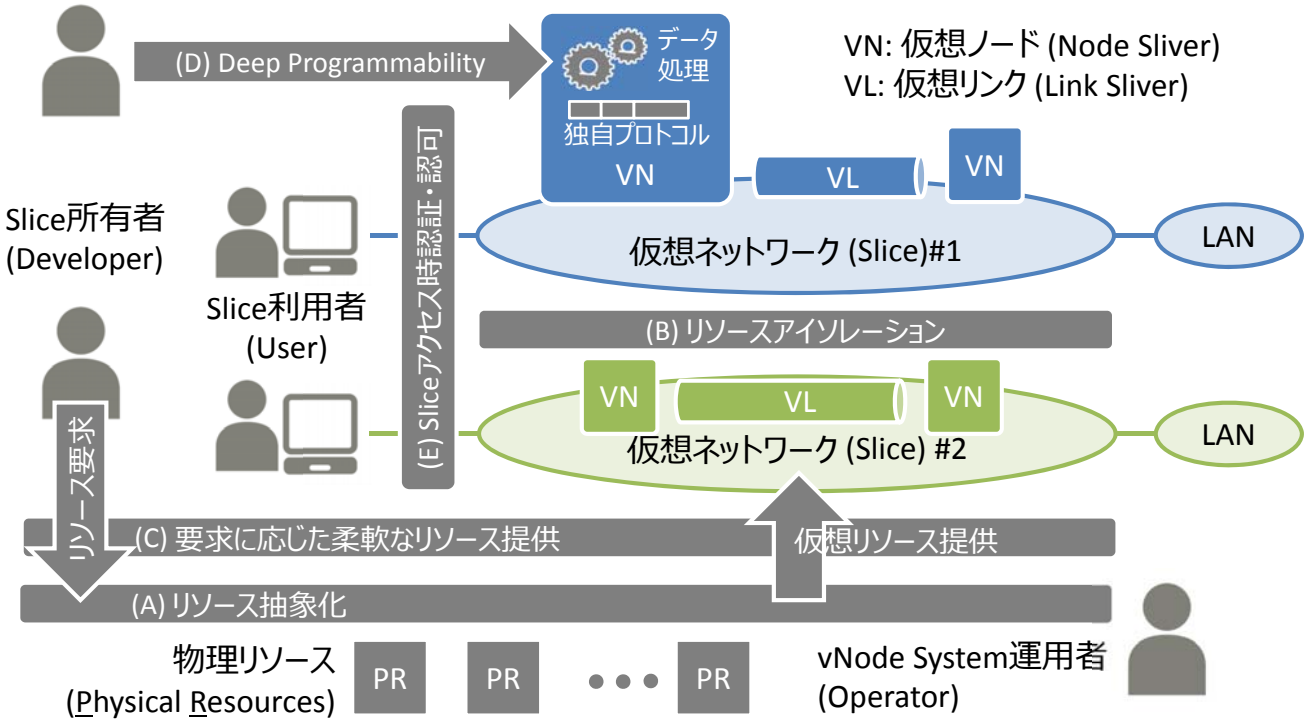
Portal: vNode Systemの利用者向けインタフェース
SNC: vNode system全体の管理・制御
VNODE: 仮想的なリンクおよびノード資源を提供
NACE: 実ネットワーク(VLAN)と仮想ネットワーク(Slice)を接続する装置
**AGW: 実ネットワークおよび同ネットワーク上端末と仮想ネットワーク (Slice)を接続する装置**



# vNode Systemが特長とする提供技術

FUJITSU

- (A) Resource Abstraction, (B) Resource Isolation, (C) Resource Elasticity, (D) Deep Programmability, (E) Authentication and Authorization



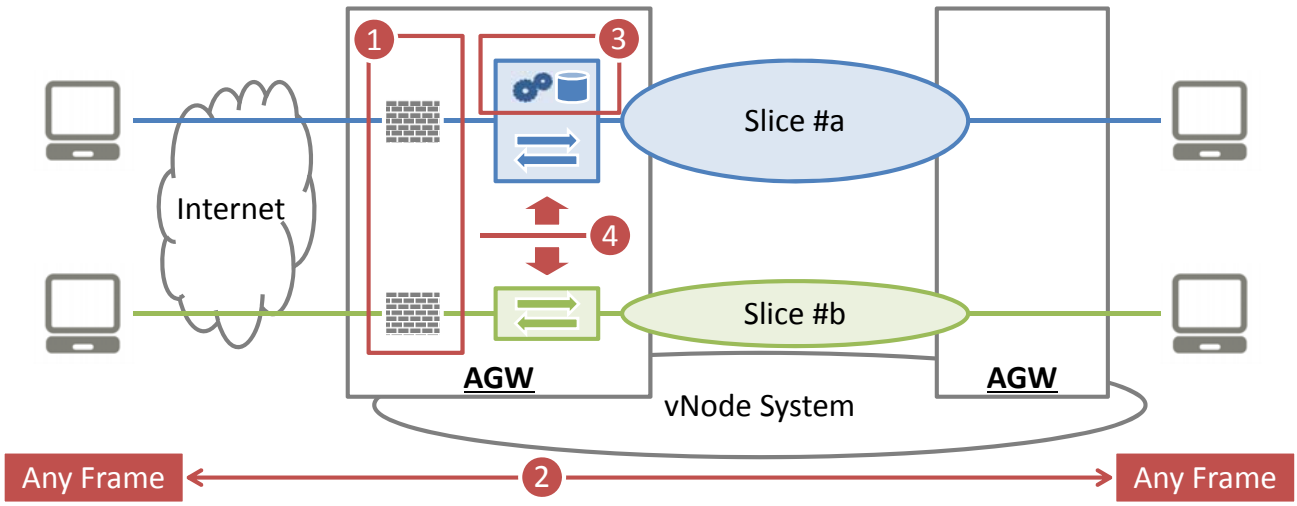




# AGW要件

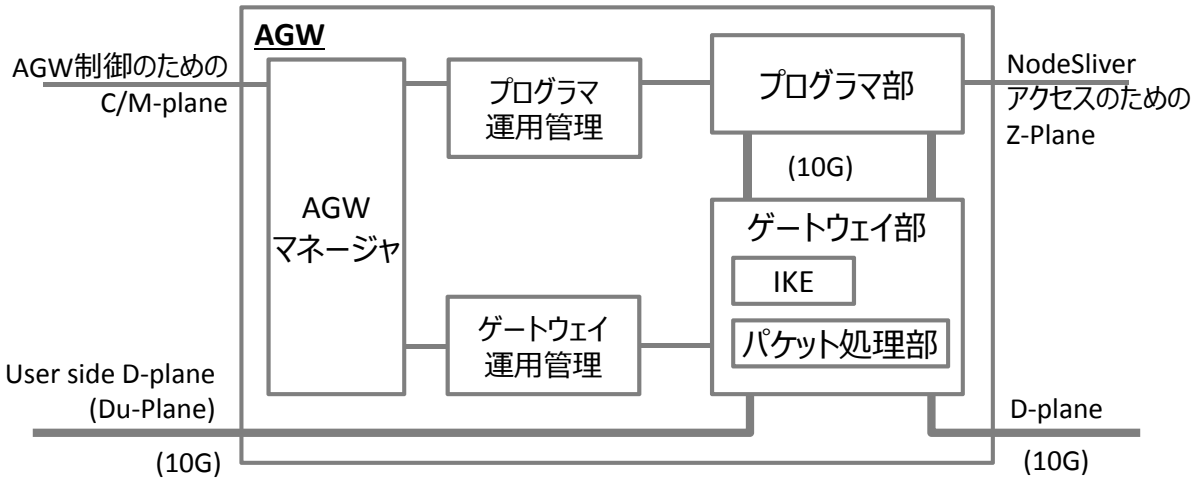
FUJITSU

- ①スライスへのアクセス認証機能の提供 →(E) AuthN/AuthZ
- ②End to EndでのAny L2 Frame疎通 →(D) Deep Programmability
- ③計算、ストレージリソースの提供 →(D) Deep Programmability
- ④リソースアイソレーション →(B) Resource Isolation



# AGW基本アーキテクチャ

- ゲートウェイ部
  - 実⇔仮想間のFrame振分
  - 仮想リンク (Link Sliver)提供
  - アクセス制御
    - IKE Daemon, IPSec処理機能
- プログラマ部
  - 仮想ノード (Node Sliver)提供
- AGWマネージャ部
  - 装置制御

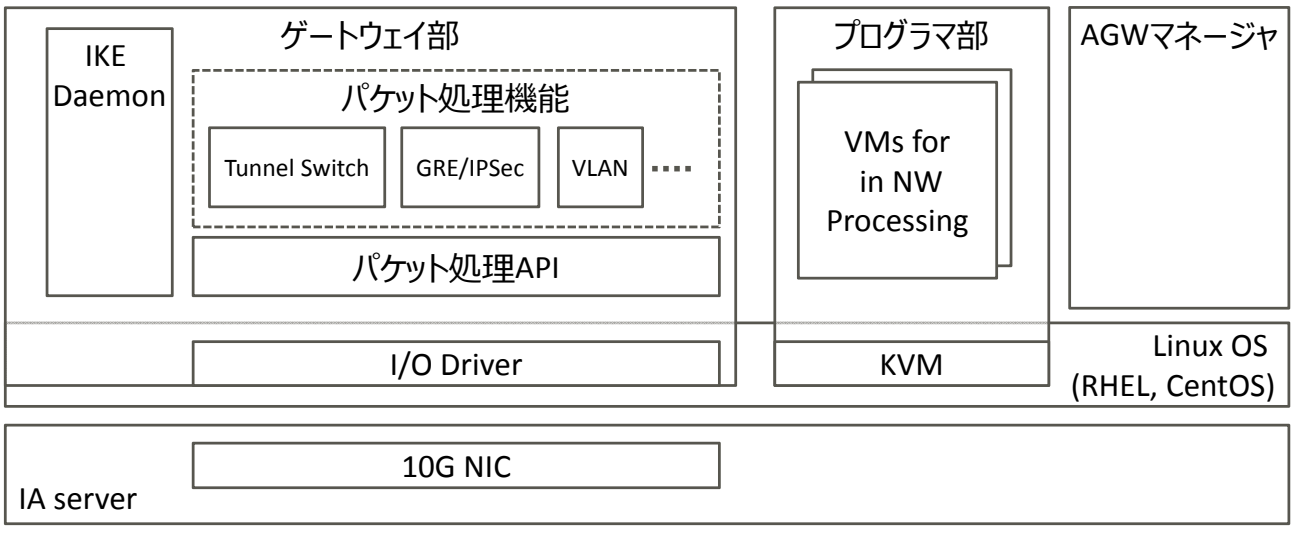






# AGWソフトウェアアーキテクチャ

- 汎用IAサーバ上ソフトウェア実装中継装置
  - ゲートウェイ部: Linux ユーザ空間上にパケット処理機能を実装し、オリジナルプロトコルスタックおよびパケット処理機能の実装を容易に
  - プログラマ部: Linux KVMベース
  - AGWマネージャ

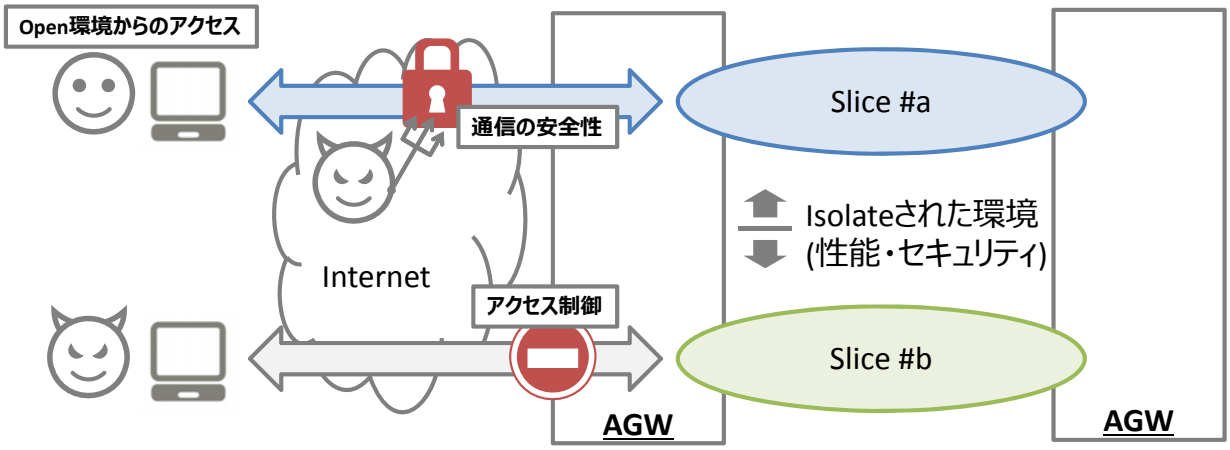


# Sliceアクセス時認証・認可要件

①認証・認可

FUJITSU

- 要件: Isolation担保されたSlice環境にOpenな環境からセキュアにアクセス
  - Slice内はIsolationが担保されている
  - ユーザによるSliceへのアクセスに関して
    - ユーザ利便性のために、ユーザはInternet等Openな環境からアクセス可能とする
    - Openな環境において、通信の安全性が担保されていること
    - Sliceへのアクセス権を有するユーザのみアクセスできるようにする





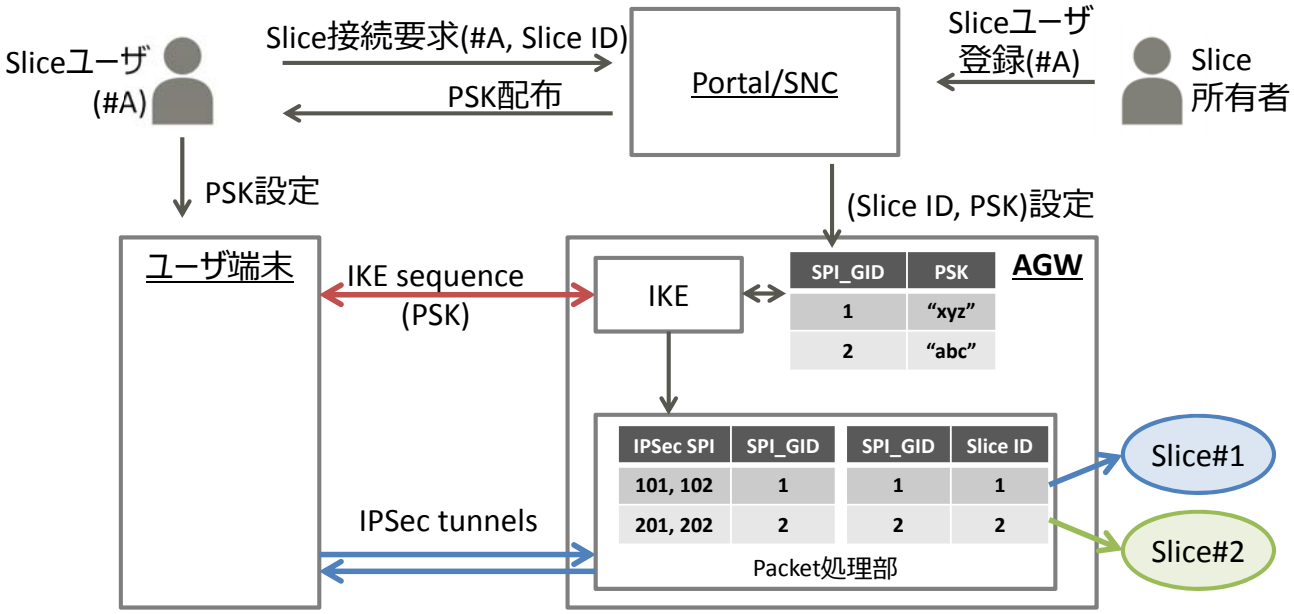



# Sliceアクセス時認証・認可

①認証・認可

FUJITSU

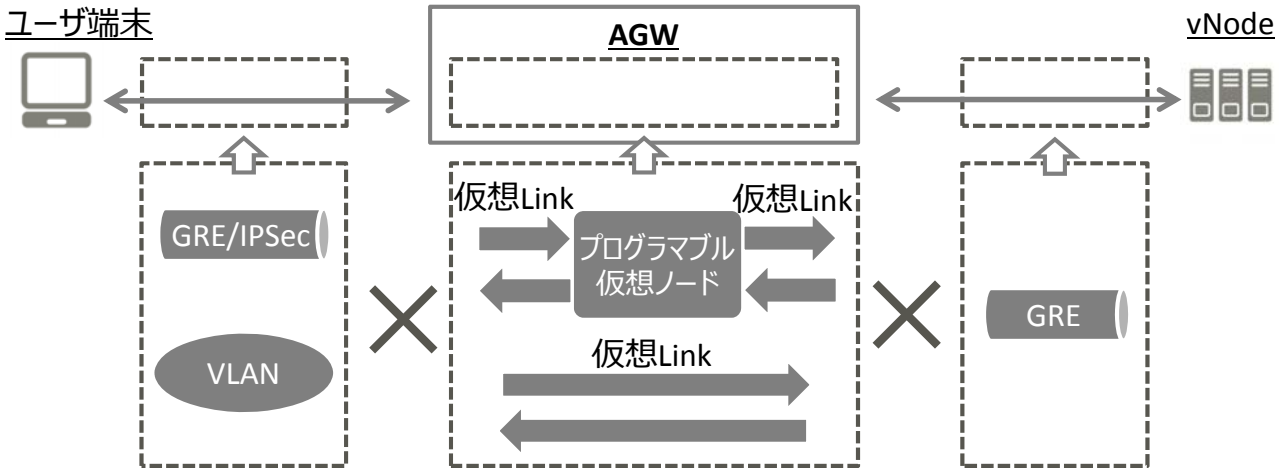
- IPSecを用いた認証・認可によるセキュリティ担保
  - Sliceの所有者が登録したユーザのみSliceへのアクセスを可能にする
  - Slice所有者が登録したユーザに対してPre-Shared Key (PSK) を払い出す
  - 払いだされたPSKを用いてユーザ端末から、AGWまでのIPSec tunnelを確立する



# E2E Any Frameの実現



- 要件: IPSecでセキュリティを担保しつつ、Any Frameを搭載可能にする
- **→Any Frame/GRE/IPSecを基本とする**
  - ユーザ端末側通信プロトコル
    - Any Frame / GRE / IPSec
    - IP / VLAN / Ethernet (既存ネットワーク収容向け)
  - AGW内仮想リソース
    - 仮想リンク
    - プログラマブル仮想ノード+仮想リンク
  - vNode側通信プロトコル
    - Any Frame / GRE



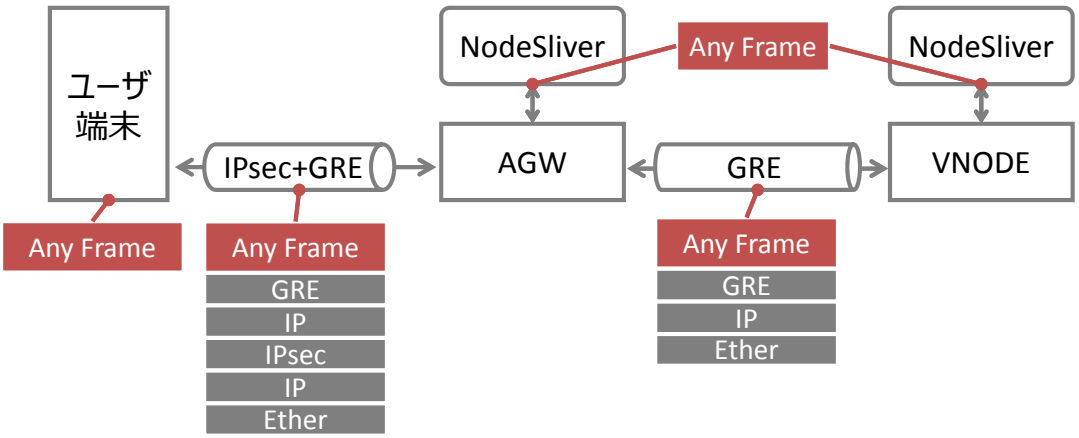





# Frame Format (GRE/IPSec接続)



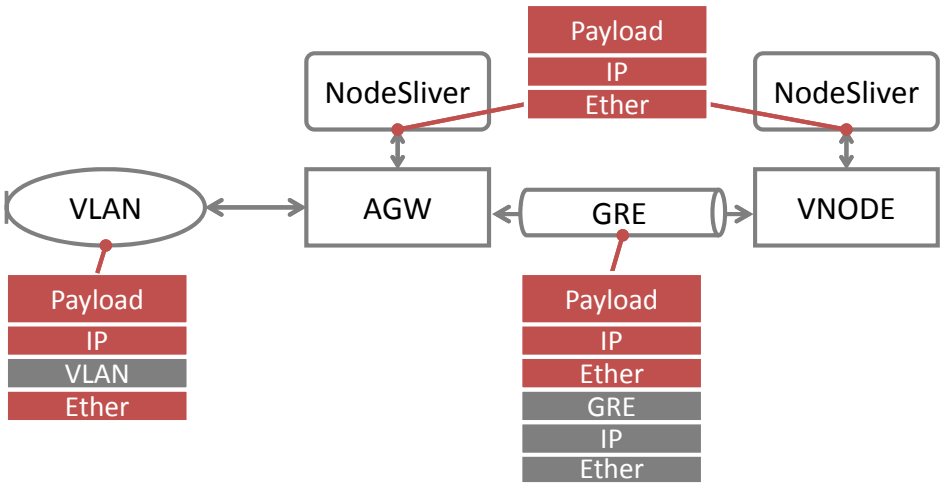
- Any FrameをSlice内へ収容可能
- Internet等のネットワーク経由での接続が可能
- 端末ごとにSliceへ収容



# Frame Format (VLAN接続)



- 既存ネットワークを容易にSliceへ収容可能
- VLANごとにSliceへ収容
- NACE (Network Accommodation CE)も同様の機能を有する



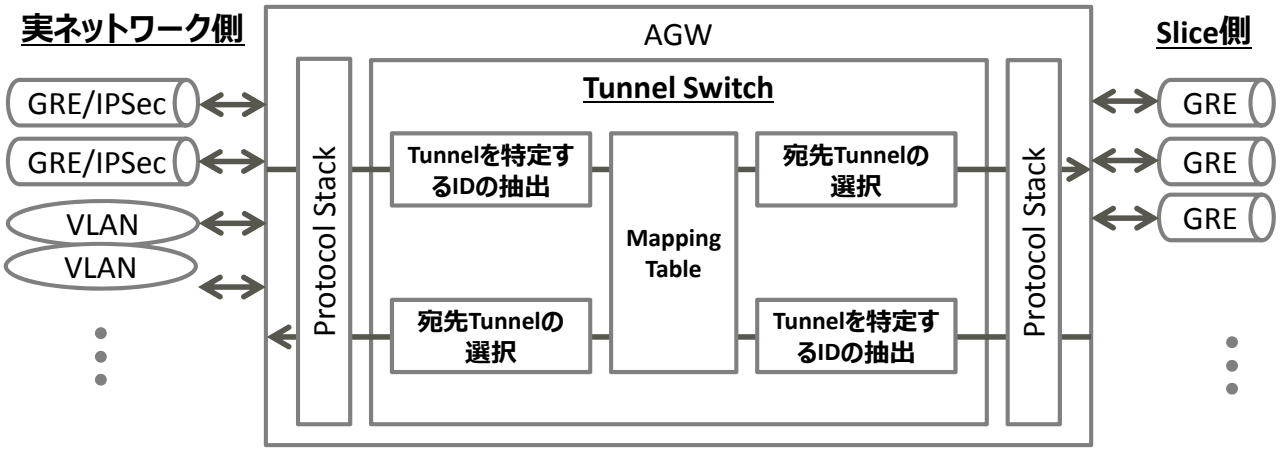




# 実ネットワークとSliceとの接続 (基本構造)



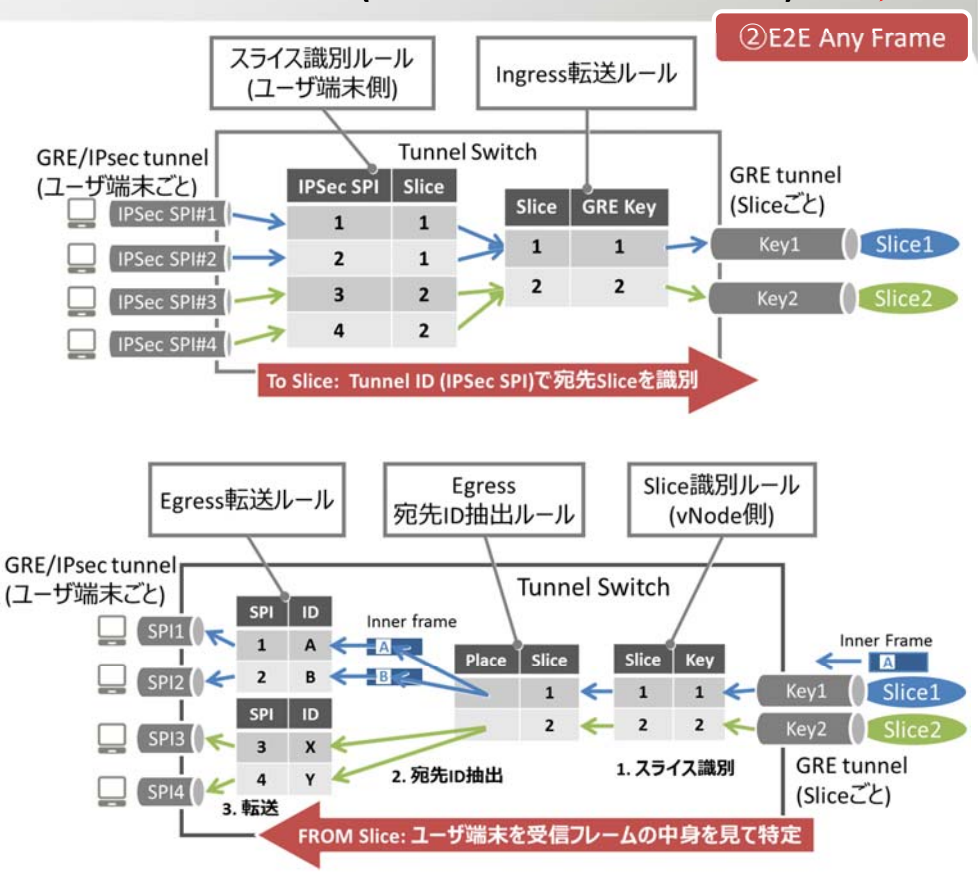
- Tunnel Switch: 基本的にはSlice内のパケットは参照せずに、外側のトンネルを識別するIDのみを参照してパケットの送り先を決定することで、Any Frameの導通を可能にする
  - トンネル(GRE, IPSec, VLANなど)を一意に特定するIDを、受信パケットから抽出
  - Slice作成時に作られるMapping Tableに従って、宛先トンネルを決定し、同トンネルIFにパケットを送信する



# 実ネットワークとSliceとの接続 (IPSec端末の場合)

FUJITSU

- 事前処理/設定
  - Inner Frameの宛先IDの場所を登録
  - 宛先IDとIPSec SPIとの関係を登録
  - IPSec tunnel確立時にIPSec SPIとSliceとの関係を学習
- Sliceへの振分
  - IPSec SPIに基づいて宛先Sliceを決定
- ユーザ端末への振分
  - GRE KeyからSliceを特定
  - Frame内宛先Idから宛先IPSec (SPI)を特定



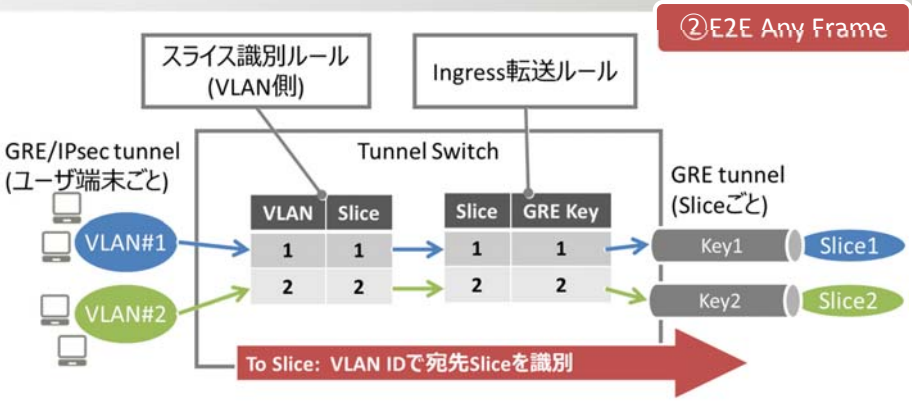




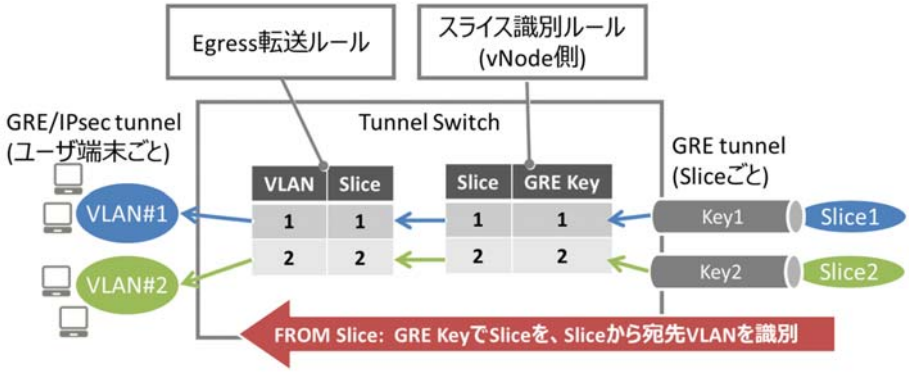
# 実ネットワークとSliceとの接続 (VLANの場合)

FUJITSU

- Sliceへの振分
  - VLAN IDに基づいて宛先Sliceを特定




- VLANへの振分
  - GRE keyに基づいて宛先VLANを決定

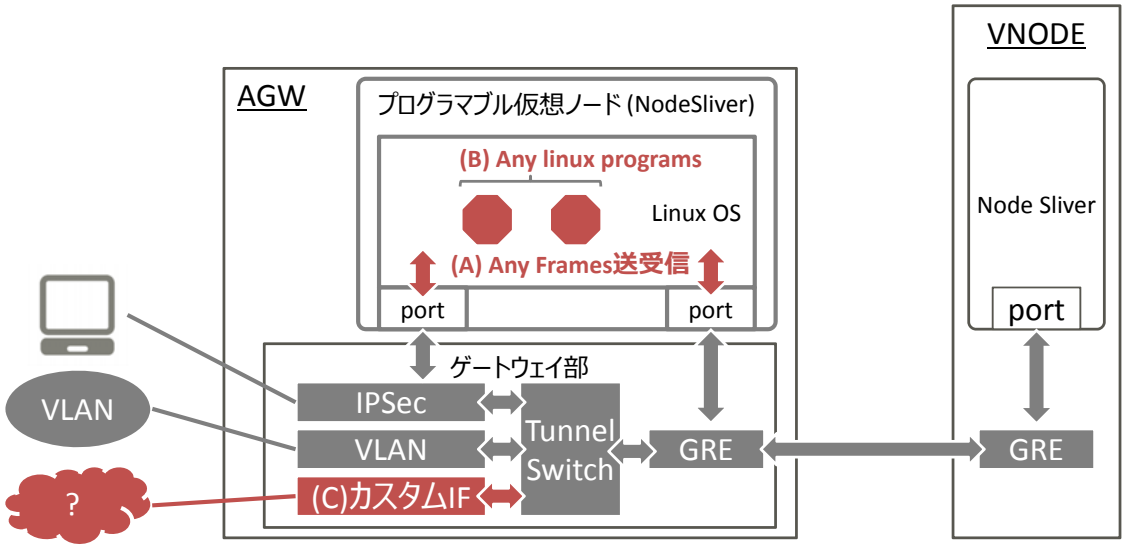


# AGWの提供するプログラマビリティ

③Deep Programmability

FUJITSU

- プログラマブル仮想ノード (NodeSliver)の提供 (vNode SlowPathと同等)
  - 仮想ネットワーク(Slice)エッジでの情報処理・蓄積を可能とする
    - (A) Any FormatのL2 Frameを送受信可能
    - (B) 任意のLinuxプログラムを搭載可能
- ソフトウェア実装の特性を活かしたインフラプログラマビリティ
  - (C) 収容する実ネットワーク／端末に応じたプロトコルスタックへの対応



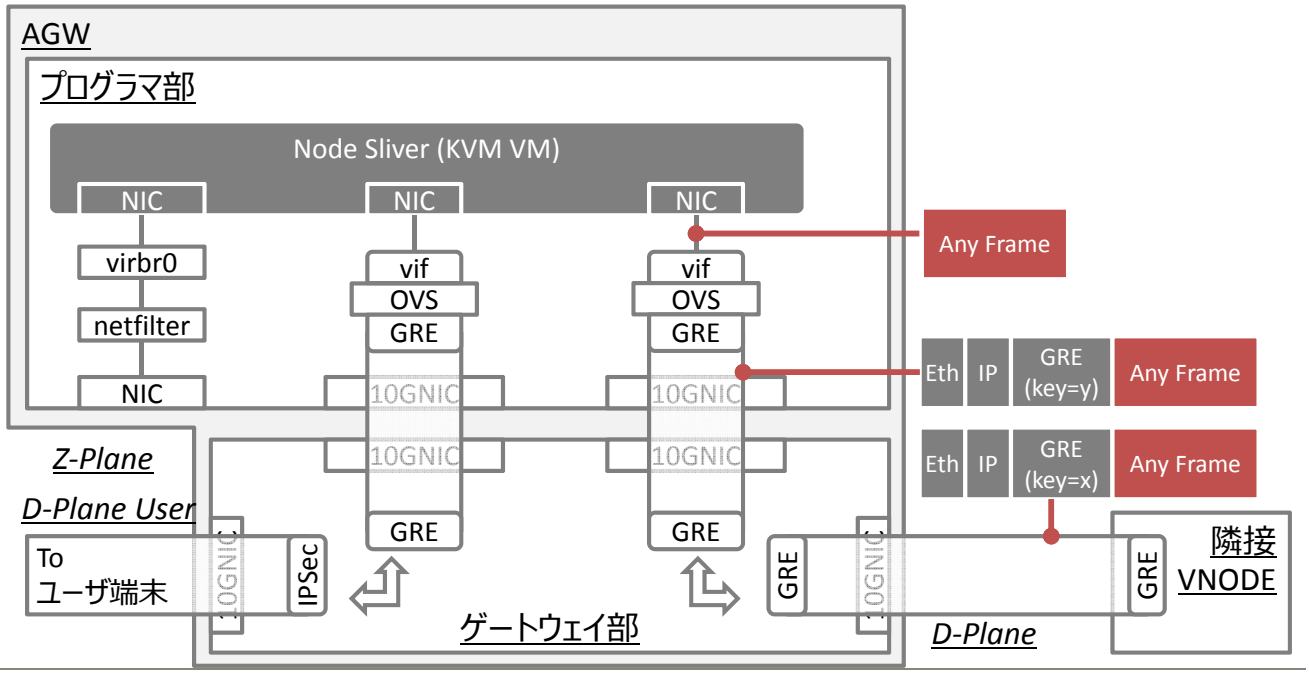





# プログラマブル仮想ノード (NodeSliver)

③Deep Programmability

- NodeSliverはKVM hypervisor上のVM (Linux OS)として提供
- GRE tunnelとOpen vSwitch (OVS)の組合せにより、NodeSliverによるAny Frameの送受信を実現

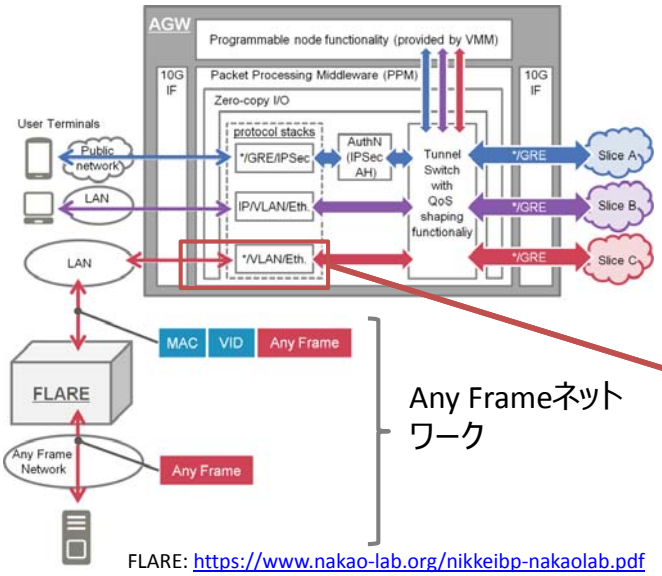


# 実ネットワーク／端末に応じたプロトコルスタックへの対応

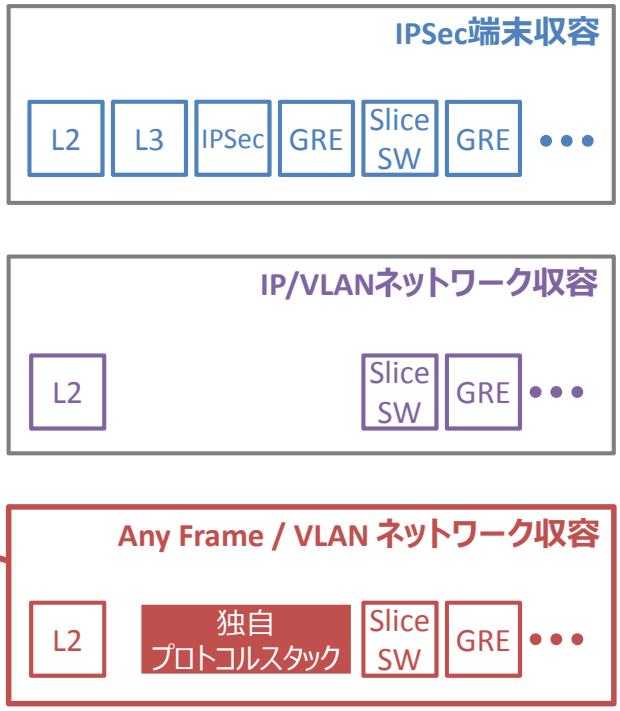
FUJITSU

③Deep Programmability

- パケット処理のユーザ空間ソフトウェア実装の特長を活かして、独自プロトコルスタックの追加が可能
  - 他装置と連携したAny Frame網の収容を実現




**様々なプロトコルスタックに対応可能**




FLARE: https://www.nakao-lab.org/nikkeibp-nakaolab.pdf

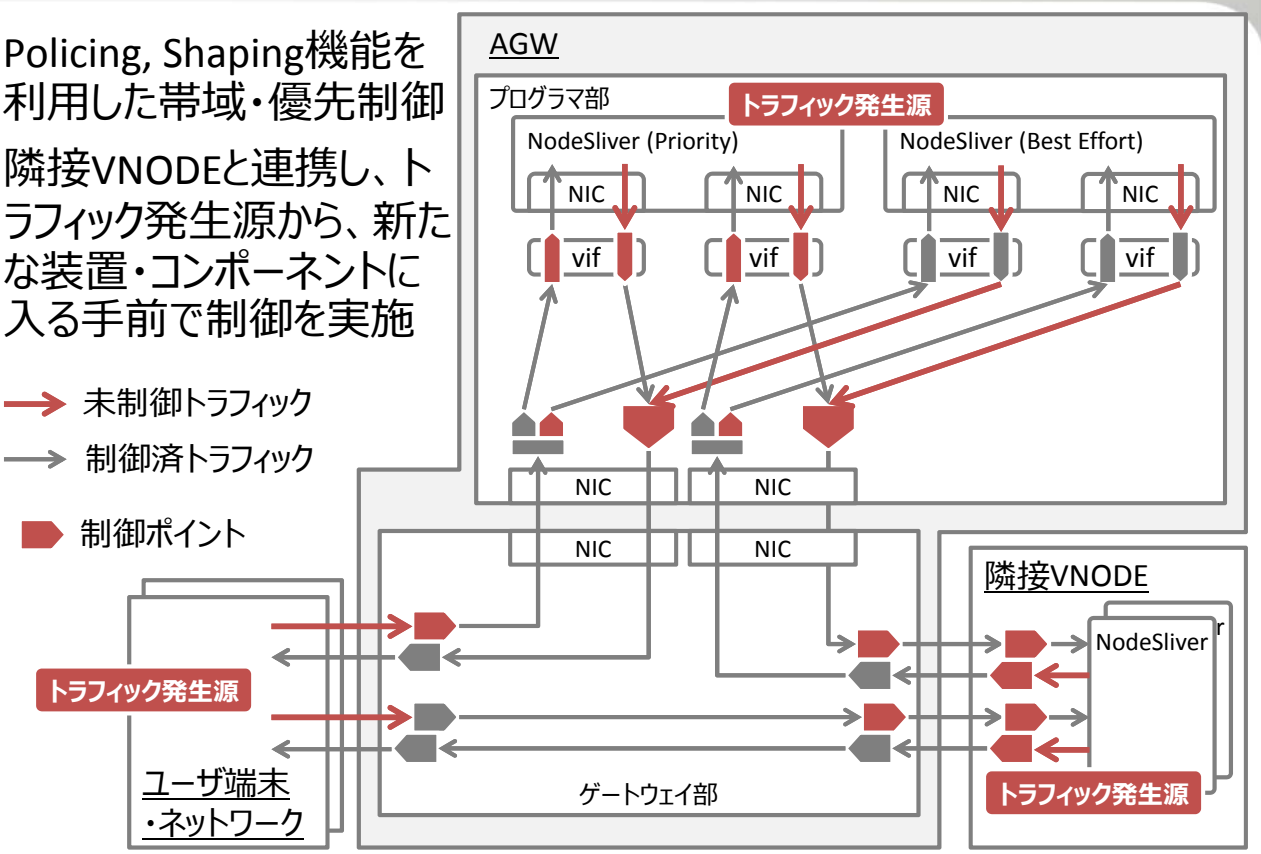



# Resource Isolation

④リソース分離

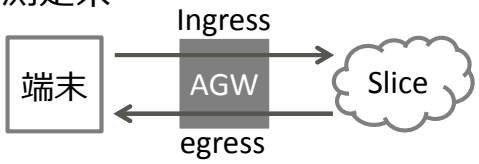
FUJITSU

- Policing, Shaping機能を利用した帯域・優先制御
- 隣接VNODEと連携し、トラフィック発生源から、新たな装置・コンポーネントに入る手前で制御を実施

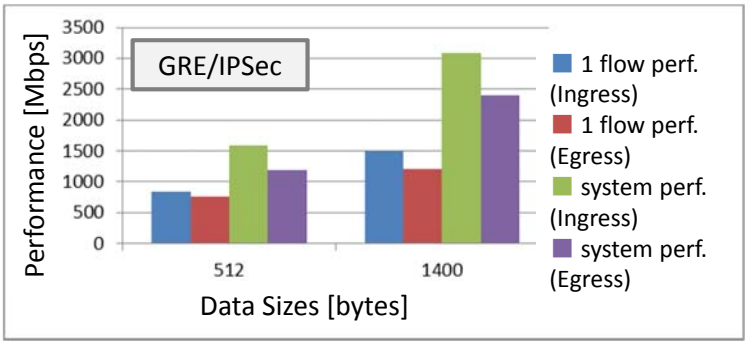


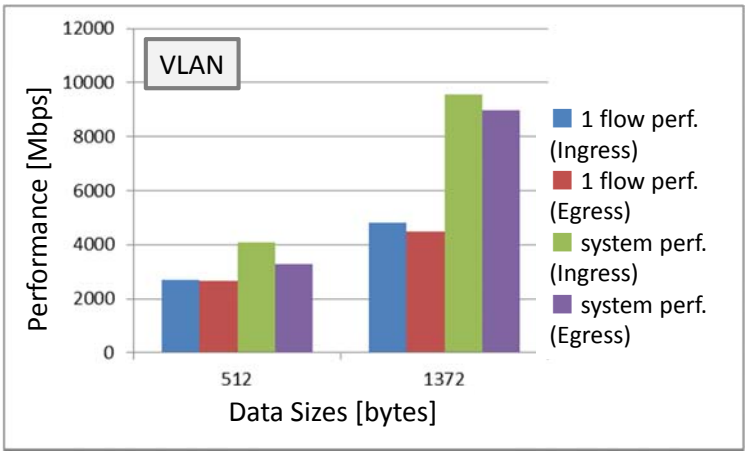
# 性能評価 – ゲートウェイ処理性能

- 測定系




- AGWハードウェア仕様
  - CPU: Intel Xeon X5690 (3.46GHz x 6 cores x 2 CPU)
  - Memory: 12GB
- 性能
  - GRE/IPSec@1400bytes Frame
    - 約1200Mbps for 1flow
    - 約2500Mbps for multiple flows
  - VLAN@1372bytes Frame
    - 約4Gbps for 1flow
    - 約9Gbps for multiple flows



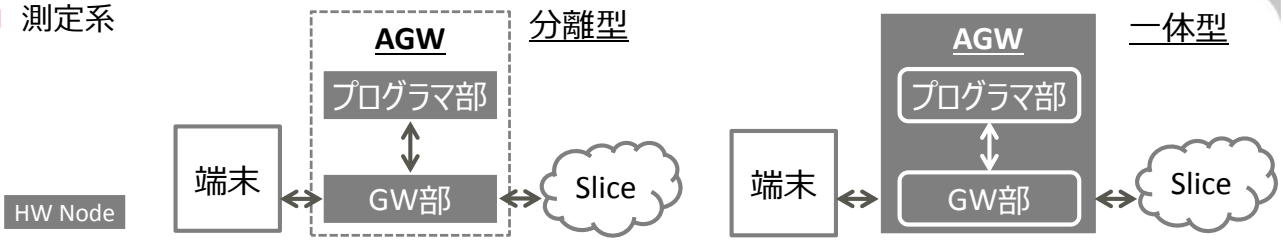





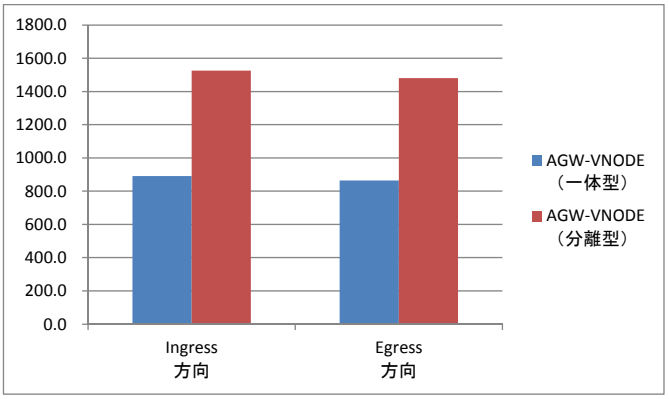


# 性能評価 – 仮想ノード込性能

- 測定系




- ハードウェア仕様
  - 一体型
    - CPU: Intel Xeon E5-2670 (2.60GHz/8コア) ×2個
      - GW部: 8コア
      - プログラマ部(VM+Vhostnet): 8コア
    - Memory: 128GB
  - 分離型-プログラマ部
    - CPU: Intel Xeon X5690 (3.46GHz/6コア) ×2
    - Memory: 96GB
  - 分離型-GW部
    - CPU: Intel Xeon X5690 (3.46GHz/6コア) ×2
    - Memory: 48GB
- 性能
  - VLAN@1372bytes Frame
    - 約1500Mbps for 1flow@分離型
    - 約900Mbps for 1flow@一体型



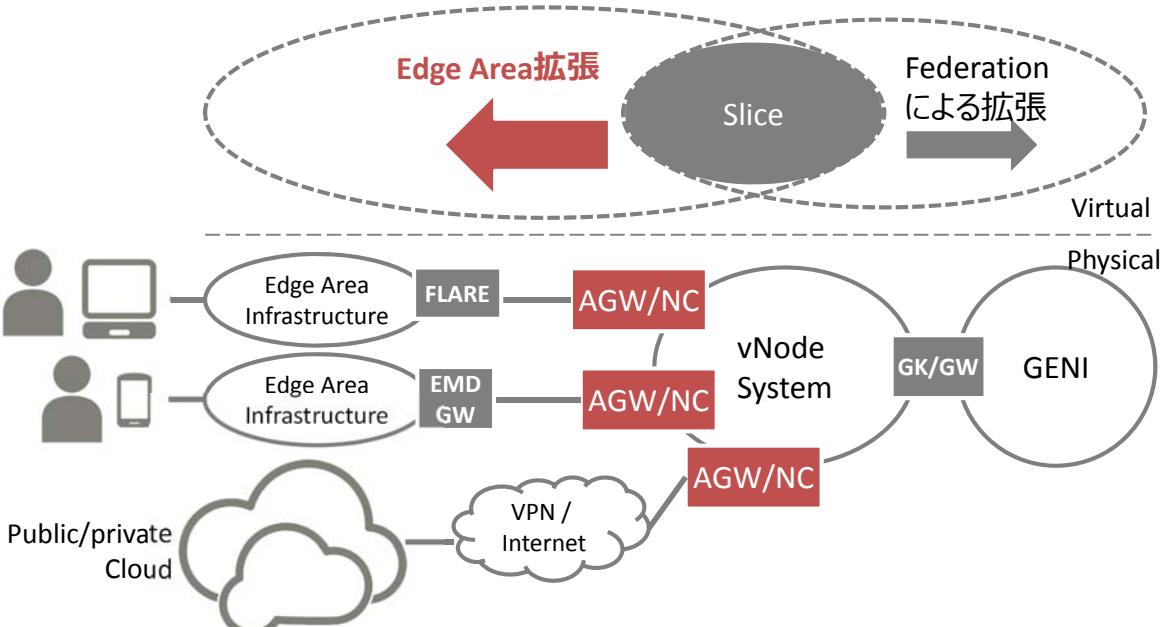
# まとめ

- 仮想ネットワーク向けゲートウェイ装置 AGW
  - 実⇔仮想ネットワーク間でFrameの識別・振分を行い、End to Endで任意のプロトコルフレームを疎通可能な仮想ネットワークの構築を可能に
  - 仮想ネットワークへのアクセス制御機能を提供
  - リソース分離された仮想リンク、プログラマブルな仮想ノードを提供

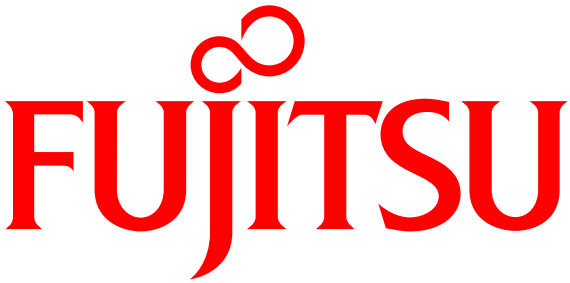



# 今後

- AGWのEdge Area拡張GWとしての活用　→　他リソース活用によるリソース拡充、エンドユーザへのReachability拡大




- エッジリソースと合わせて、ユーザ近傍にプログラム・データを配備可能なエッジ装置として、各種ネットワーク分散アプリケーションの評価・検証に活用




shaping tomorrow with you