

# 第3回 九州NGN研究会 技術セミナー ホームゲートウェイの役割と日立の取組み

## ネットワークを含めた日立の取組み編

2008/07/04

株式会社 日立コミュニケーションテクノロジー

## *Contents*

1. IPv4からIPv6へ
2. IPv6ネットワーク構築に向けて
3. デモ

# 1

## IPv4からIPv6へ

## 現状のネットワーク

企業やキャリア網、アクセス網など、多くのネットワークがIPv4によって構築されている。しかし、急速に普及が進み、IPv4 ネットワークは限界に近づいている。

## IPv4が抱える課題

IPv4アドレス枯渇問題  
NATの課題

} 内容は次ページに説明



このような問題を解決するため

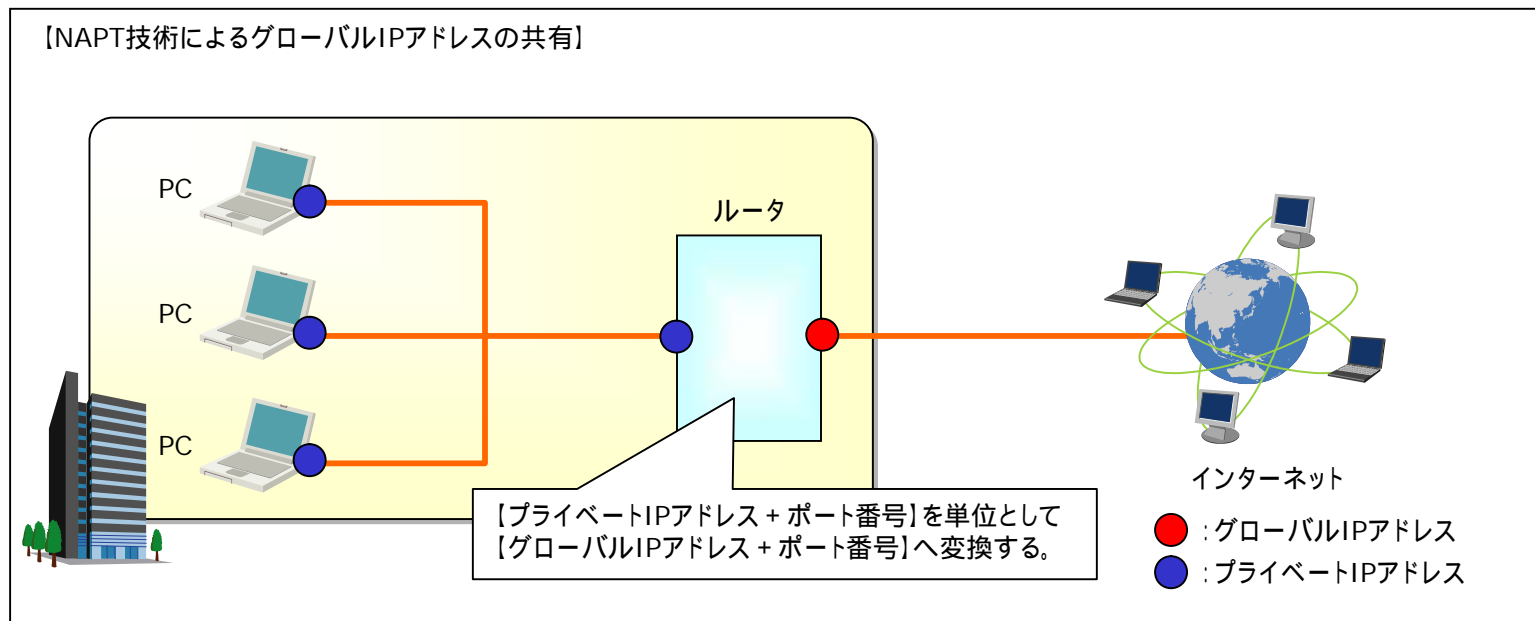
## IPv6の誕生

IPv4 の基本的な概念を踏襲

広いアドレス空間に基づく新しいネットワーク・プロトコル開発の必要性

## IPv4アドレス枯渇問題

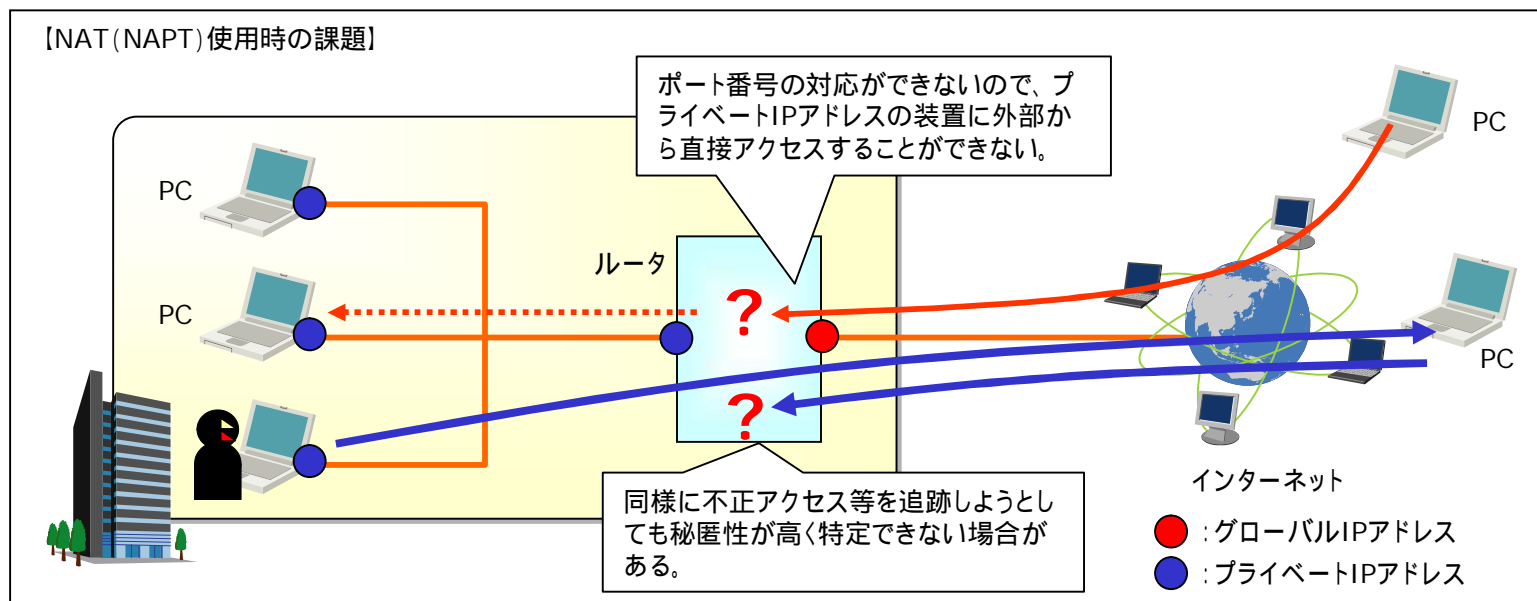
急激にインターネットの利用機器が増加した中国、インドなどをはじめ、日本などでもIP アドレス枯渇が現実のものとなりつつある。2010年頃にはIPv4アドレスが枯渇すると予測されている。



## NATの課題

ピア・ツー・ピアでの接続に対する障害  
プライベートIPアドレスを付与されたホストには、外部から直接アクセスできないことが多い。

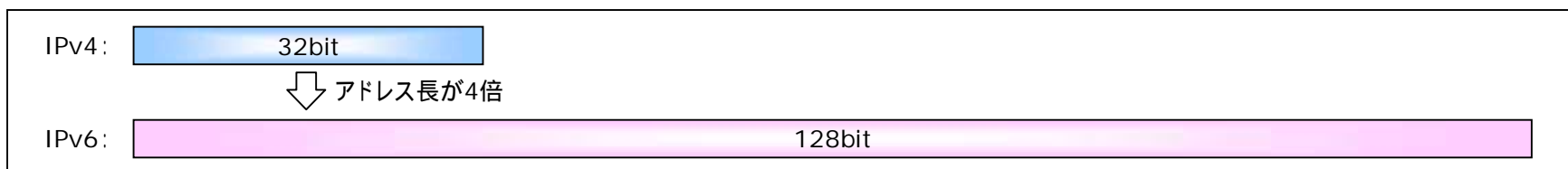
悪意のある利用がなされた場合の匿名性が高い  
複数のプライベートIPアドレスからのアクセスを1つのグローバルIPアドレスで共有するため、外部からはどのホストからのアクセスか特定が困難。



# 1-4 . IPv4課題の解決 -IPv6ネットワークの特徴

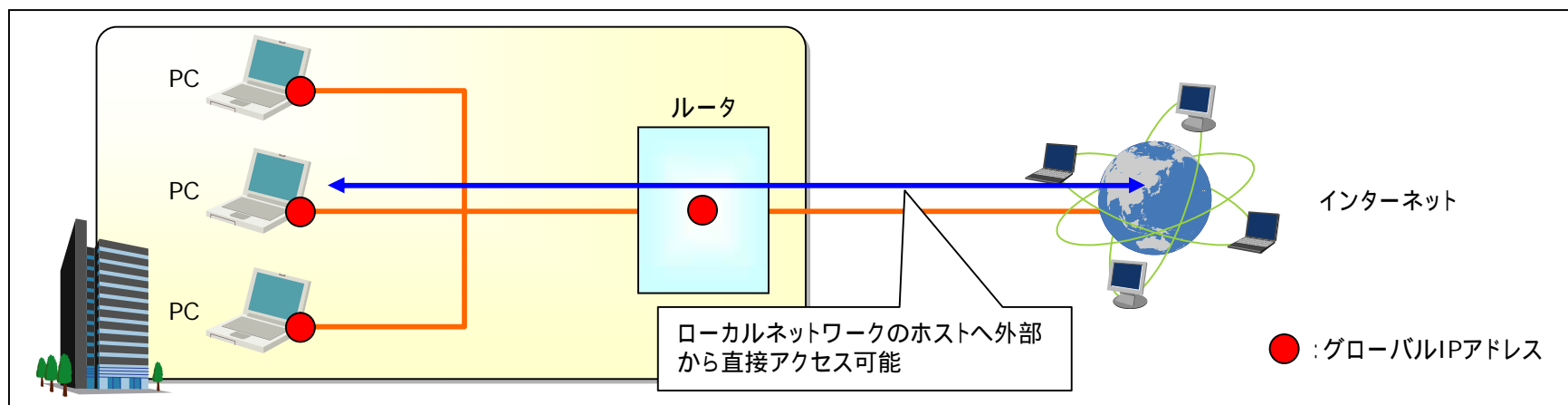
## IPv4アドレス枯渇問題 豊富なIPアドレス

32bit 128bitへ拡張(約43億 約43億個の4乗個)。ほぼ無尽蔵。



## NATの課題 ピア・ツー・ピアでの接続

全ての端末にIPv6アドレスの割当、従来のNATによる変換が不要。  
ピア・ツー・ピアでの接続が可能になり、匿名性はなくなる。  
全ての端末が特定可能となる。



# 1-5 . IPv4 / IPv6の比較

項目	IPv4	IPv6
アドレス数	×少ない 既に枯渇問題が発生している状況。	<b>ほぼ無限</b> 全端末にアドレスを付与しても問題無い。
ヘッダ長	×可変長 オプションによって長さが変化する。さらにチェックサムもあるため、バックボーンルータでは処理負荷が大きくなってしまふ。	<b>固定長</b> オプションはヘッダを追加する方式のため、基本的なヘッダは固定長。チェックサムもないため、バックボーンルータの処理負荷が少ない。
IPsec	上位層で対応する必要あり。 さらに、NAT/NAPTとの併用で使用する際に様々な注意が必要。	<b>標準オプション</b> より手軽にセキュアな通信が可能。
アドレス設定	DHCP/固定 DHCPサーバによって配布、または固定で設定。	<b>自動生成</b> ホストが自動的に自分のアドレスを生成するため、手間がかからない。
遠隔アクセス	×プライベートアドレスへのアクセスは難しい ローカルネットワーク上のアドレスを特定するのは難しい。UPnP等が必要となる。	<b>全グローバルアドレスなので容易に可能</b> ローカルネットワーク内でもグローバルアドレスを持つため、外部からのアクセスが容易に可能。
セキュリティ	<b>ローカルアドレスを隠蔽可能</b> NAT/NAPTによってローカルアドレスを外部から保護できる。	外部からアクセスが容易に可能 遠隔アクセスが容易であるため、その反面外部からの攻撃にさらされる場合があるため、より高いセキュリティが必要。
対応OS	<b>ほぼ全てが対応</b> 現在のネットワークはIPv4がほとんどであるため、どのOSでも問題なく動作する。	一部のOSでは対応不可 Linuxをはじめ、最近ではサポートしているOSが多くなってきたが、まだ不安定なものも多い。
導入しやすさ	<b>技術者が多数</b> 成熟した技術が多く、対応製品も多数あるため導入が容易。	認識度、技術者の数も少ない まだ発展途中の技術であり、導入の際の検証に手間がかかる。既存製品が使えない場合が多く、追加投資がかかるのも大きな壁。



# 2

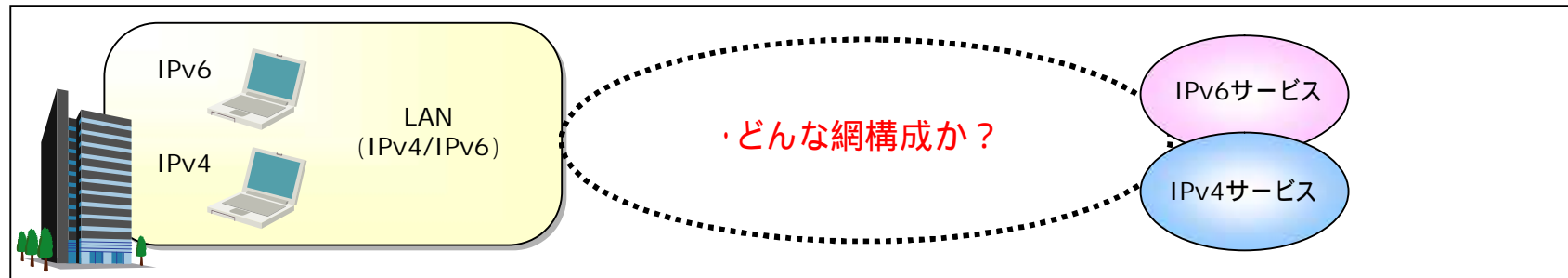
## IPv6ネットワーク構築に向けて

## 2-1. IPv6導入時の検討事項

### IPv4 / IPv6ネットワーク共存のための技術

相互接続という点においては互換性はない。

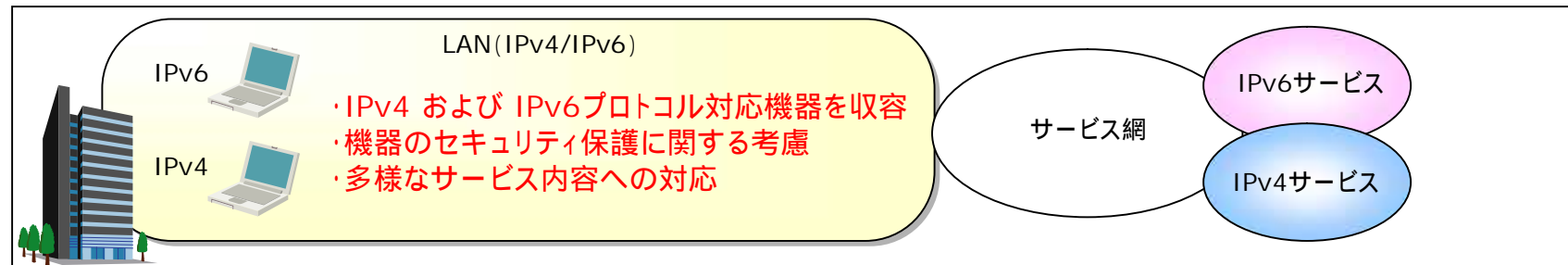
ネットワーク製品のIPv6対応は未完了で、緩やかなIPv6化が現実的。



### 複数装置収容とサービス提供のための技術

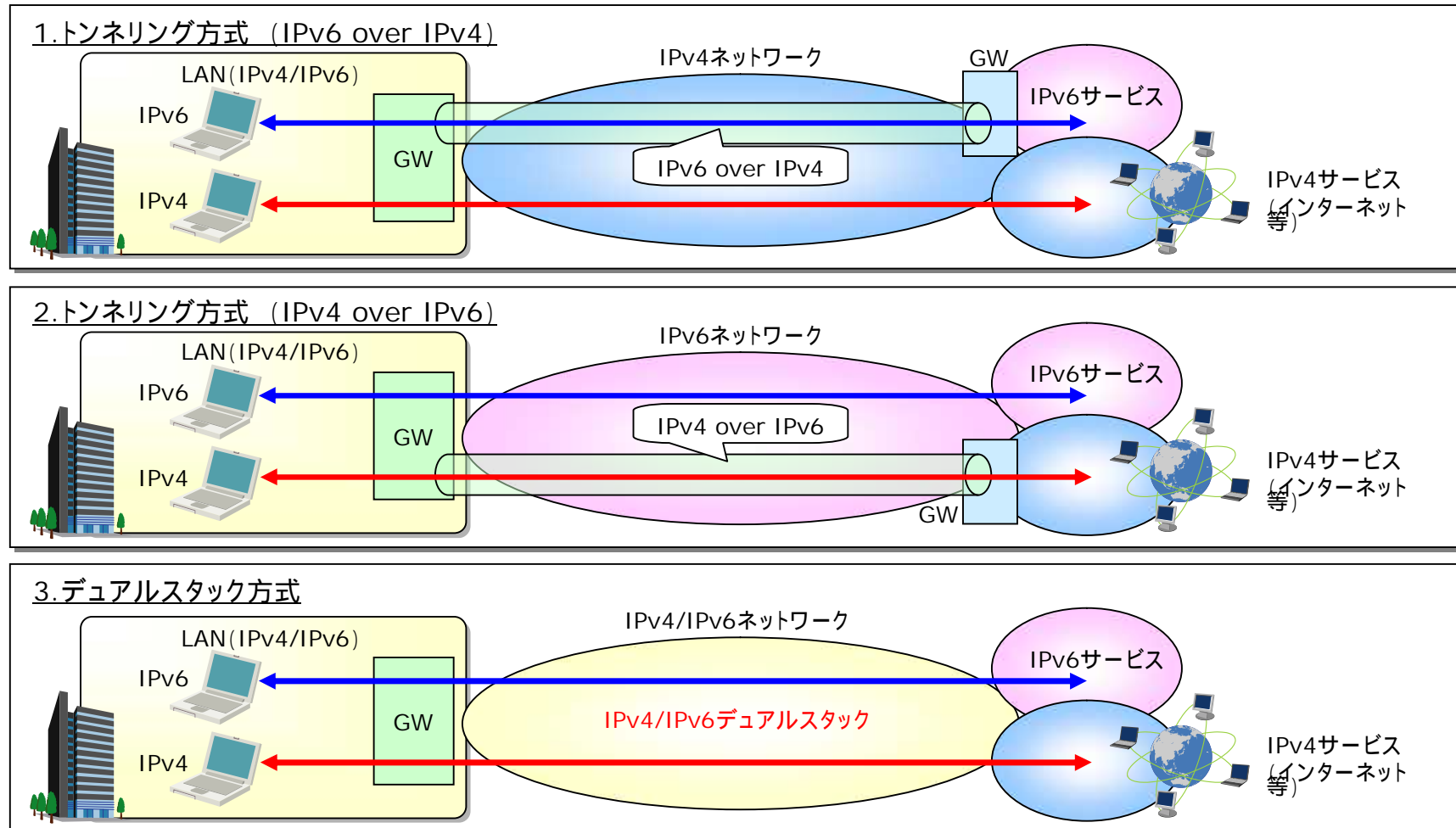
IPv4からIPv6への移行中は、IPv4とIPv6の複数の機器が共存。

IPv4/6の特徴の違いからサービス内容やセキュリティの考慮も異なる。



## 2-2 . IPv6導入時の検討事項 IPv4/IPv6ネットワーク共存のための技術

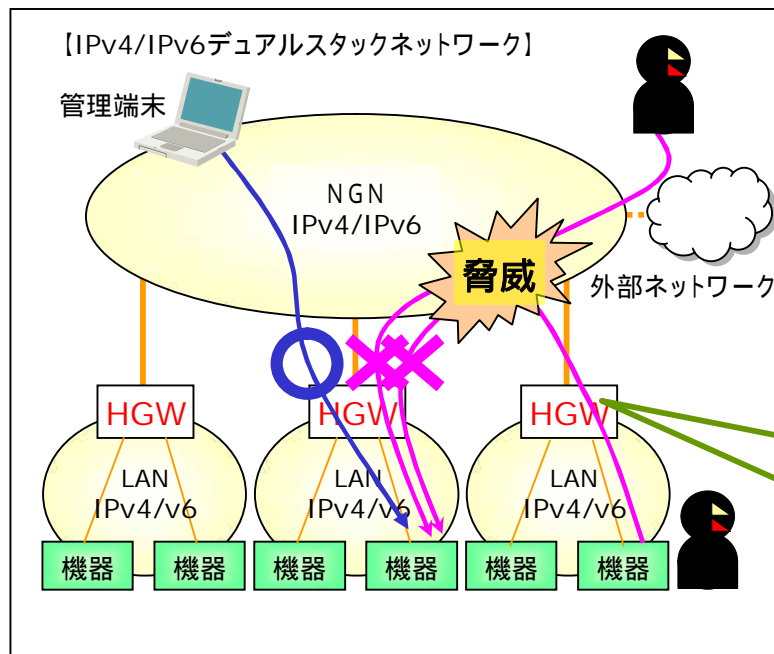
### IPv4とIPv6ネットワークの共存のための技術 トンネル方式: 「IPv6 over IPv4」と「IPv4 over IPv6」 デュアルスタック方式



## 2-3 . IPv6本格導入時代の検討事項 複数装置収容とサービス提供のための技術

#	IPv6導入に必要な機能	課題
1	既存IPv4機器に加え 新規IPv6機器を収容する機能	HGWによるNGN Adaptation
2	IPv6遠隔管理機能	安全な宅内機器アクセス

↓ HGWにて課題を解決



課題 :HGWによる NGN Adaptation

SIP連携オンデマンドVPN(デモ)

OSGiバンドルによるALG

課題 :安全な宅内機器アクセス

OSGiバンドルによる動的FW制御(デモ)

SIPピンホール制御

## 2-4 . HGWによるNGN Adaptation

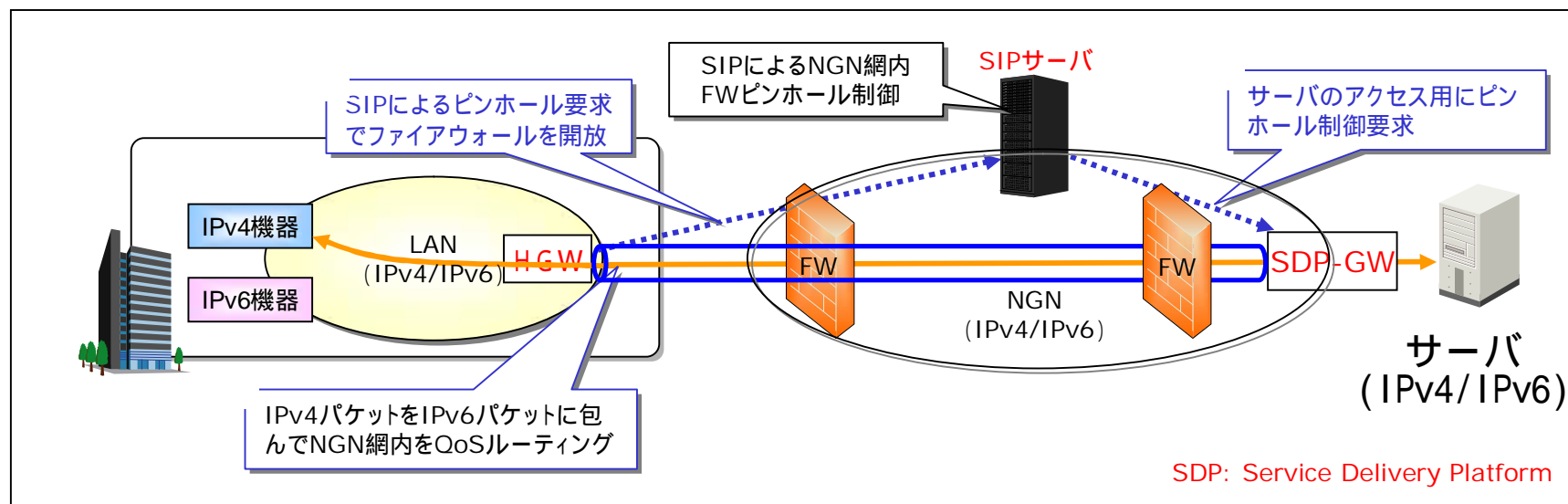
LAN内のP C (IPv4/IPv6機器) とNGN網側のサーバ (IPv4機器) をシームレスに接続する

SIP連携オンデマンドVPN (デモ)

NGN-SIPシグナリングに同期してオンデマンドでVPNトンネルを張る。

OSGiバンドルによるALG

OSGiバンドルのALG (Application Level Gateway) でIPv4/IPv6変換。



## 2-5 . 安全な宅内機器アクセス

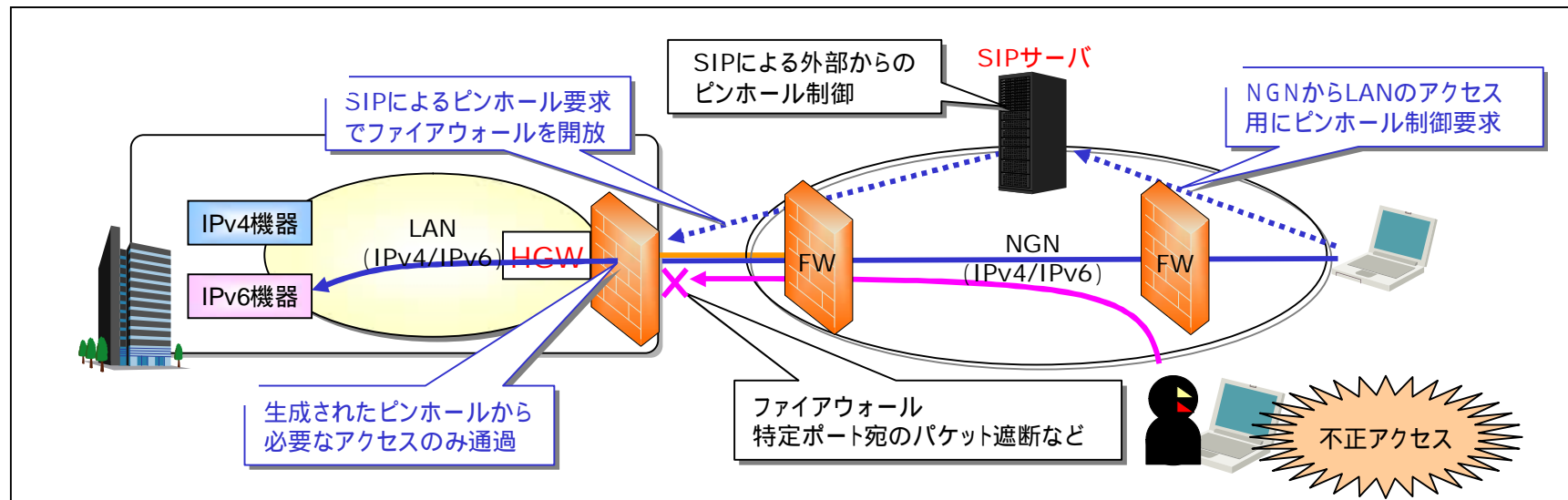
セキュアなサービスを提供するために、必要な外部からのアクセスを通過させる一方、外部からの不正侵入を阻止する

### OSGiバンドルによる動的FW制御(デモ)

設定された規則に従いパケットの遮断/通過を設定。

### SIPピンホール制御

外部からファイアウォールを制御し、**外部からの必要な通信のみを通過。**



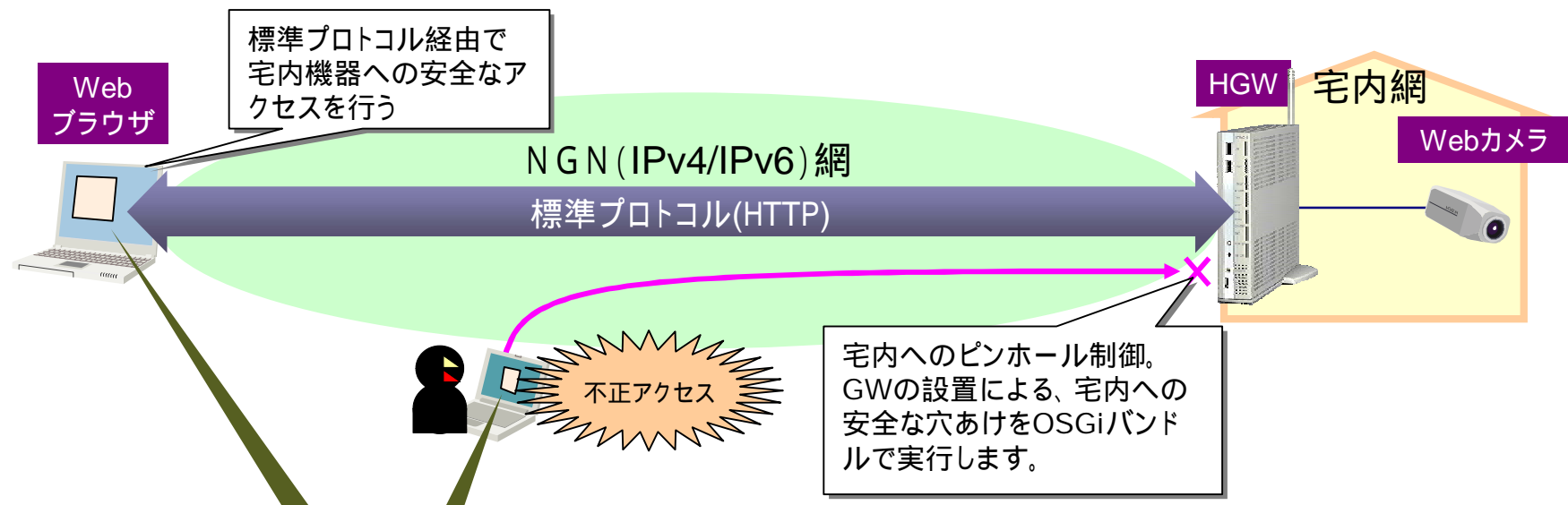
# 3

## デモ

- ・OSGiバンドルによる動的FW制御
- ・SIP連携オンデマンドVPN

# 3-1 . OSGiバンドルによる動的FW制御デモ構成

外部PCのWebブラウザから、標準プロトコルであるHTTPを用い、HGWを経由して、宅内のWebカメラへ遠隔アクセスするデモ

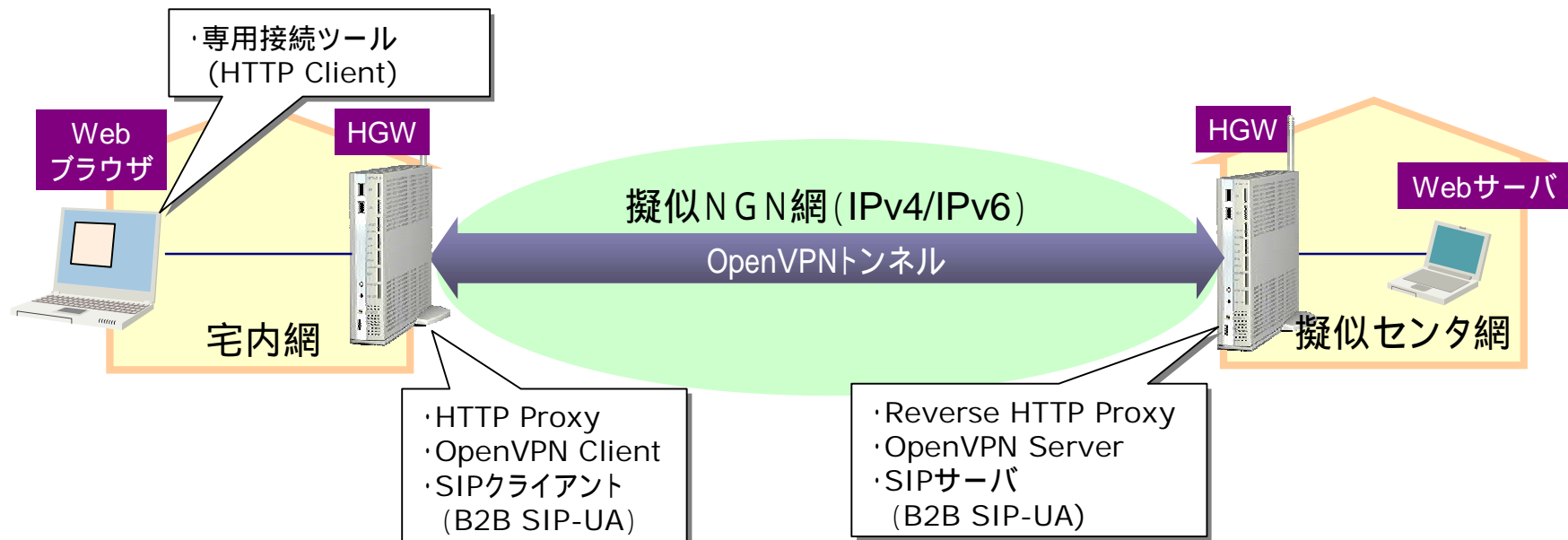


OSGiバンドルによる動的FW制御デモ(動画)を行います。



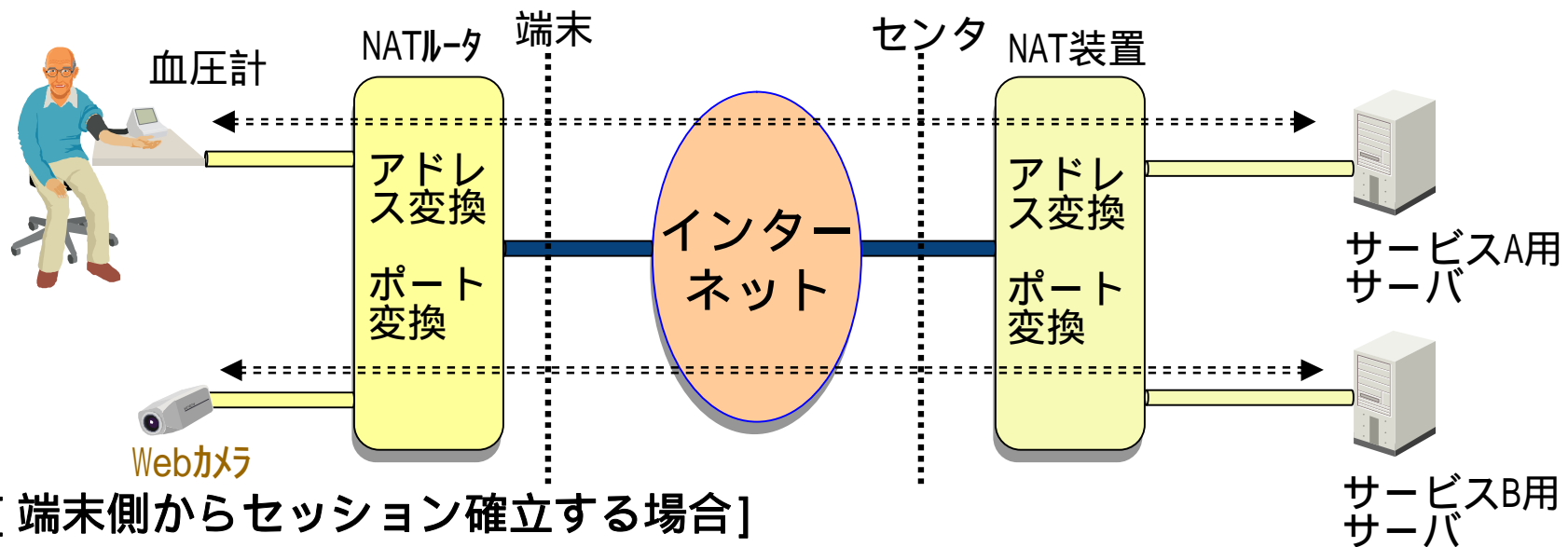
## 3-2 . SIP連携オンデマンドVPNデモ構成

宅内PCの専用接続ツールを使って、HGWのSIP-UAを叩くことにより  
OpenVPNトンネル経由で、Webサーバへアクセスするデモ



次ページでSIP連携オンデマンドVPNアーキテクチャを説明します。  
その後、SIP連携オンデマンドVPNデモ(動画)を行います。

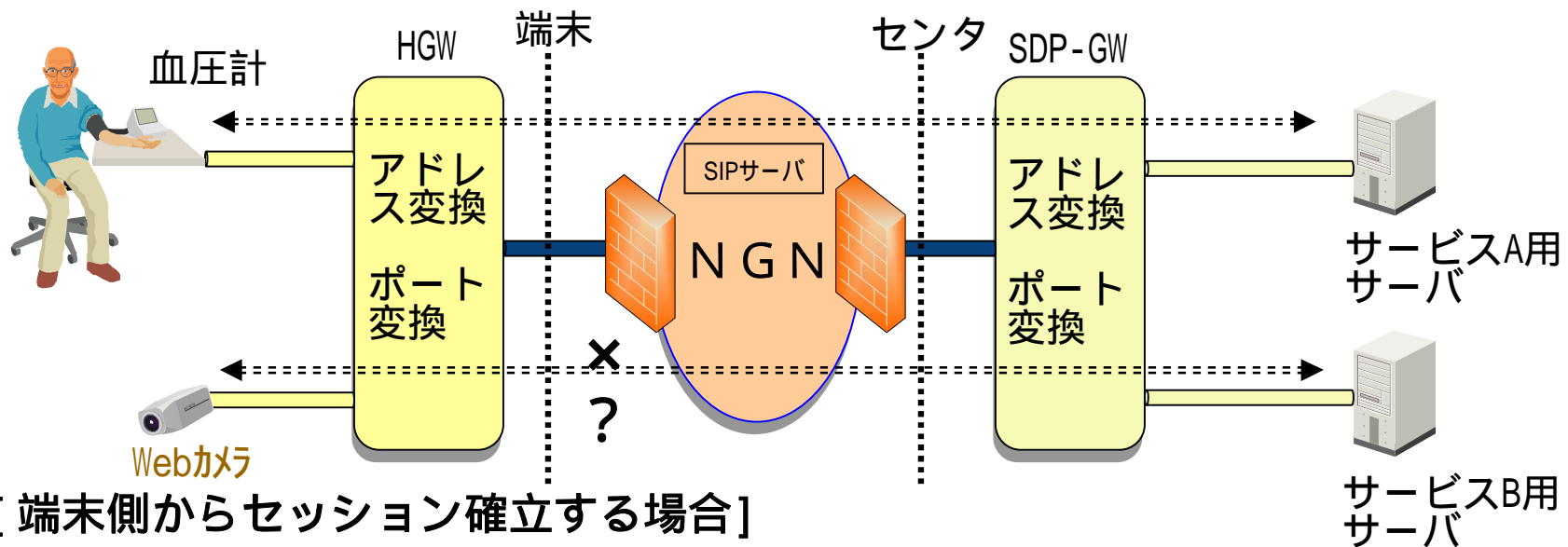
送受信IPアドレスが同じ場合でも、複数の送信元ポート番号を使って複数セッション接続が可能



- ・ データ系のセッションを確立する際のポート番号をサービス毎に区別して設定
- ・ ポート番号でサービス識別が可能

[ インターネット内では、ポート番号の透過性を保証 ]

送受信IPアドレスが同じ場合、複数セッション接続を許容するかどうかはN G Nの運用ポリシーに依存



[ 端末側からセッション確立する場合 ]

- ・ TCP/IPセッションを確立する際のポート番号をSDPで規定(RFC4145/4566)
- ・ 単一SIPセッションで一組のポート番号の割り当てしかできないのが課題

[ N G N網内では、ポート番号透過性を制限 ] 特殊VPN

**uVALUE**