Internet Week 2012 IPv6実践講座
～トラシュー、セキュリティ、アプリ構築まで～

IPv6セキュリティ
エンタープライズ/ISPネットワーク編

さくらインターネット（株）
研究所　大久保 修一
ohkubo@sakura.ad.jp

はじめに

- IPv6によるセキュリティインシデントが増えている
- 弊社（さくらインターネット）での例
  - IPv6によるDoSアタック
  - IPv6によるSPAMメール
  - IPv6によるルータへの攻撃
- 本格的にIPv6が使われるようになったことの表れ
- セキュリティ対策が必須となっている

ところで・・セキュリティの目的は？

- セキュリティのCIA
  - Confidentiality(機密性)
  - Integrity(完全性)
  - Availability(可用性)

- ネットワークをちゃんと動かす
  - 落ちないように。通信不良が発生しないように。
  - トラブル発生時に原因究明、解決しやすいように。
  - 情報が漏洩しないように。乗っ取られないように。
  - 外部ネットワークに迷惑をかけないように。

そのためには‥

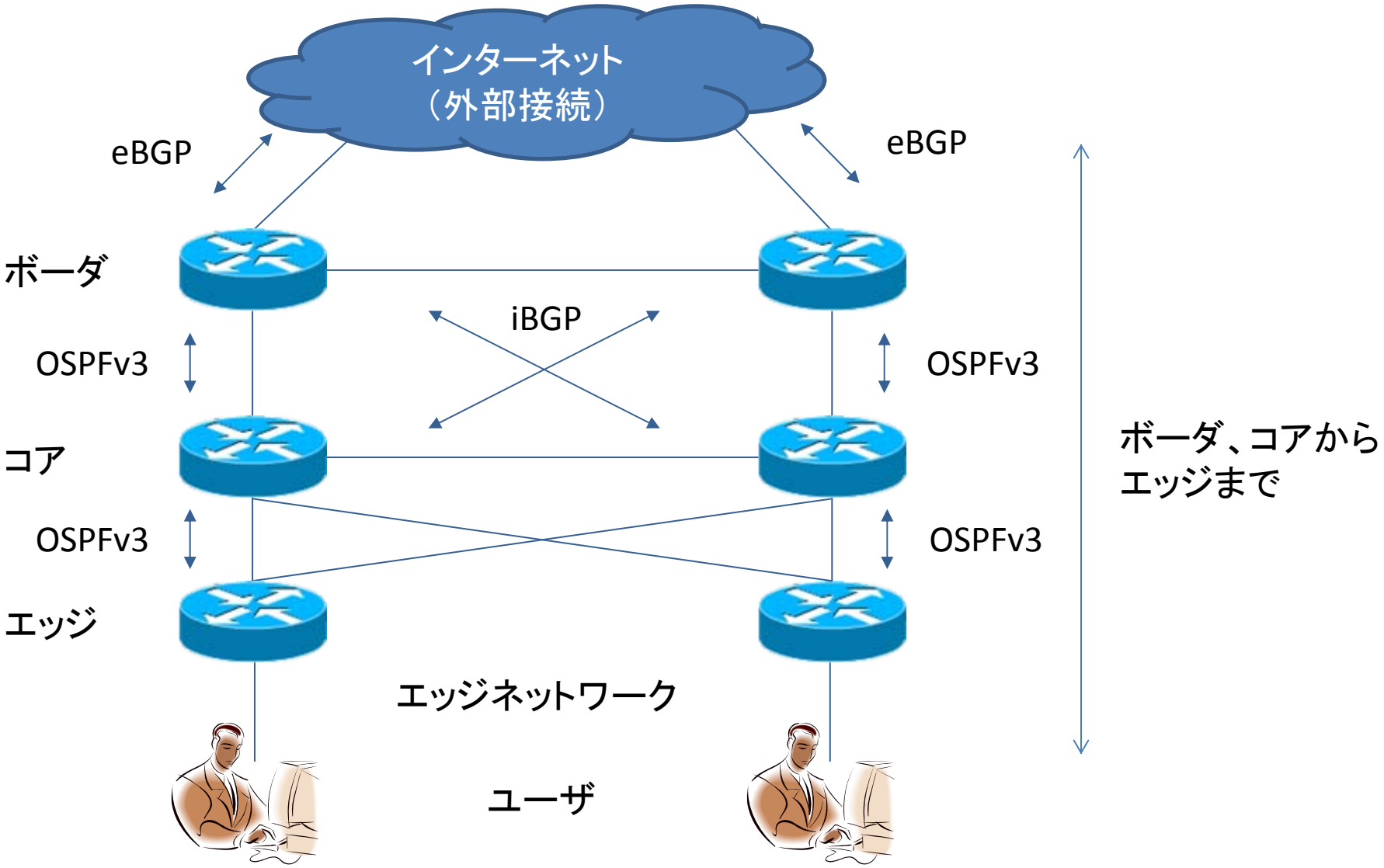
- 適切な管理
- 不正なアクセス、攻撃からの防御
- 脆弱性の対策
- ネットワークの状態把握
- 適切な収容設計
- その他

Agenda

- ISPネットワークにおけるセキュリティ
- エンタープライズ環境におけるセキュリティ

ISPネットワークにおけるセキュリティ

ISPネットワークモデル



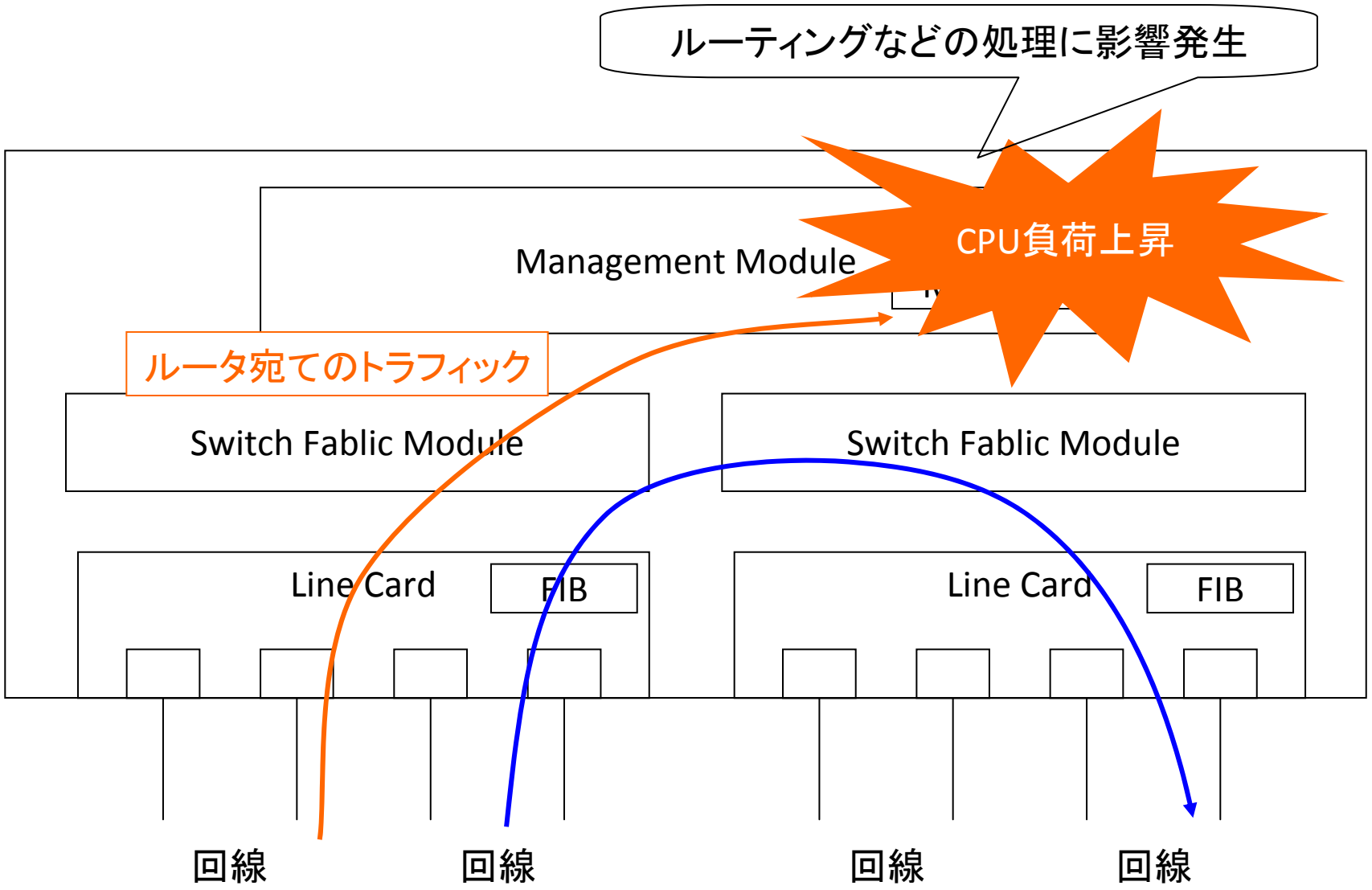
ISPにおけるセキュリティ概要

- 基本的にはIPv4で行っていた対策をIPv6でも同様に実施する。
- ただし、IPv6に同等の機能が実装されていない機器もあるため注意は必要。
- 今回は以下を中心にお話しします。
  - ルータの保護
  - eBGPの保護、OSPFの保護
  - フローサンプリング
  - DoSアタックへの対処
  - エッジネットワークの対策

ルータを守る

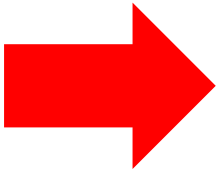
- ルータに設定しているIPアドレスは、Tracerouteすると外部からわかる。
- ルータへの攻撃
  - 不正ログイン、大量のパケット(UDPフラッドなど)
  - Telnet, SSH, BGPへのSYNアタック
  - Hop Limitが0になるパケット
  - ND未解決な宛先へのパケット
- ルータはパケットを転送するのは速いが、自身へ向かってくるトラフィック(DoSアタックなど)には弱い。

参考：一般的なアーキテクチャ



攻撃を受けた時の症状

- CPU負荷上昇
- Telnetログインできない
- BGPピアダウン
- VRRPの状態がフラップ(Master←→Backup)
- LACPが切断される
- OSPFのneighborダウン、LSAの不伝播



通信の継続に重大な影響

対策

- マネジメント系(Telnet,SSH,SNMP)の保護
  - アクセス可能なIPアドレスを制限する
- ルータ宛てアタックの防御
  - インターフェイスにそれぞれACLを設定
  - 自身宛てのパケットをフィルタ
  - Infrastructure ACLを使うと便利
  - 外部から到達性のないアドレスを使用

IPv6 ACLの設定例

シスコ社の例

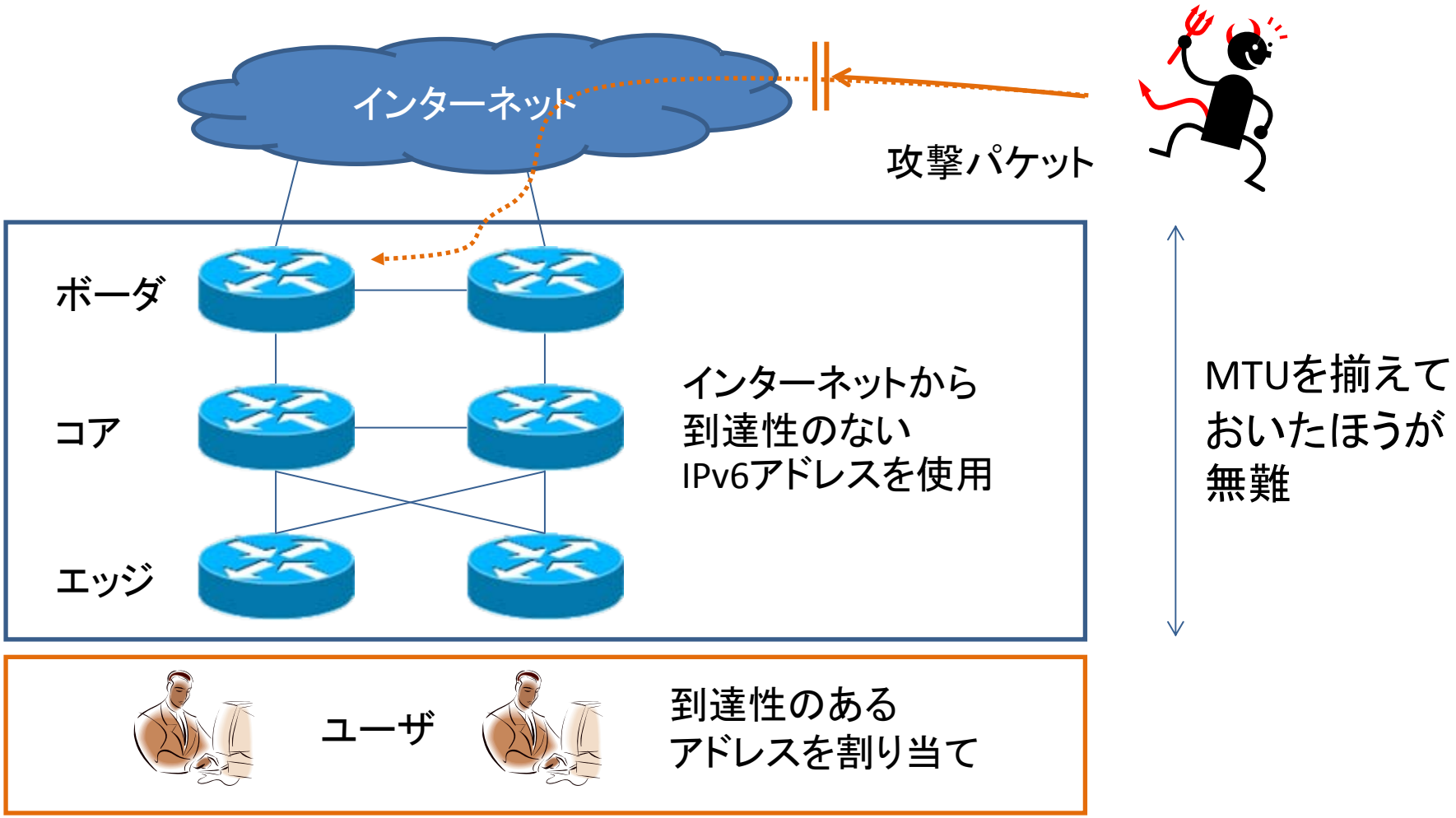
```
ipv6 access-list telnet-ipv6
 permit ipv6 2001:e40:xxx:xxx::/56 any

ipv6 access-list remote-snmp-ipv6
 permit ipv6 2001:e40:yyy:yyy::/56 any

line vty 0 4
 ipv6 access-class telnet-ipv6 in

snmp-server community xxxx RO ipv6 remote-snmp-ipv6
```

到達性のないアドレスを設定



参考：バックボーンアドレス分離とセキュリティの考察
http://irs.ietf.to/past/docs_20090521/

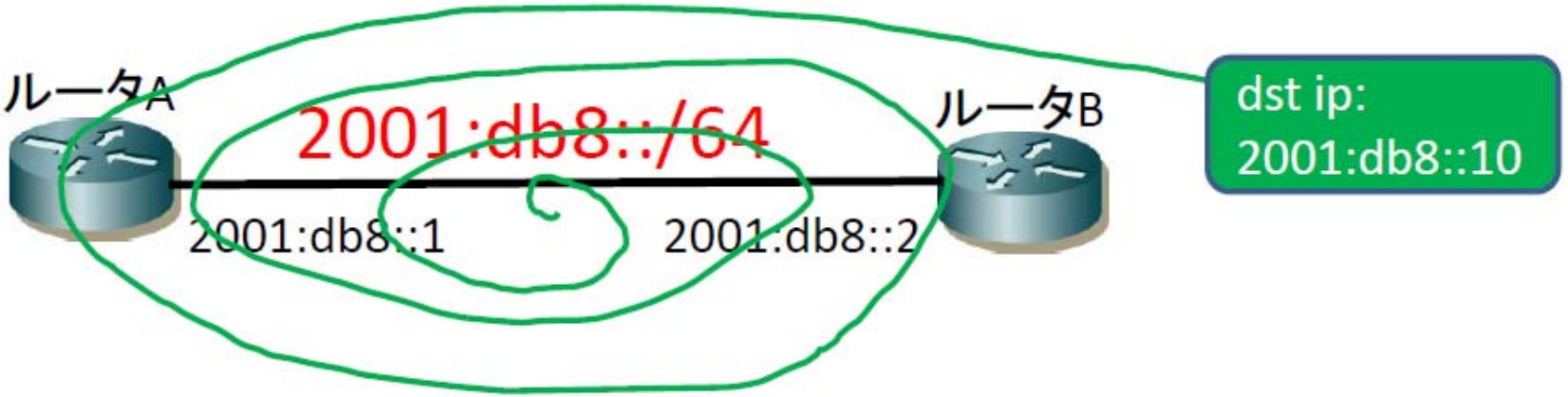
ルータによるパケット生成の抑制

- ルータの負荷上昇につながる
- ICMPv6 redirectの抑制
  - 出さない、受け取らない、経路障害にもつながる
- ICMPv6エラーの抑制、レートリミット
  - Destination Unreachableは可能なら抑制
    フォールバックに影響するので慎重に
  - Time Exceededはレートリミット
  - Packet Too Bigは必ず生成するように
    ただし、必要に応じてレートリミット

その他

- SLAACを無効化
  - RAは出さない、受け取らない
- 開いているポートがないか確認
  - あらかじめポートスキャンを掛けて不要なサービスが動いていないか確認
- point to pointリンクのピンポン抑制
  - あるメーカさんのルータで発生。
  - point to pointリンクで使用していない宛先のパケットがピンポンする。
  - /127のアドレッシングを使用するのも手(RFC6164)

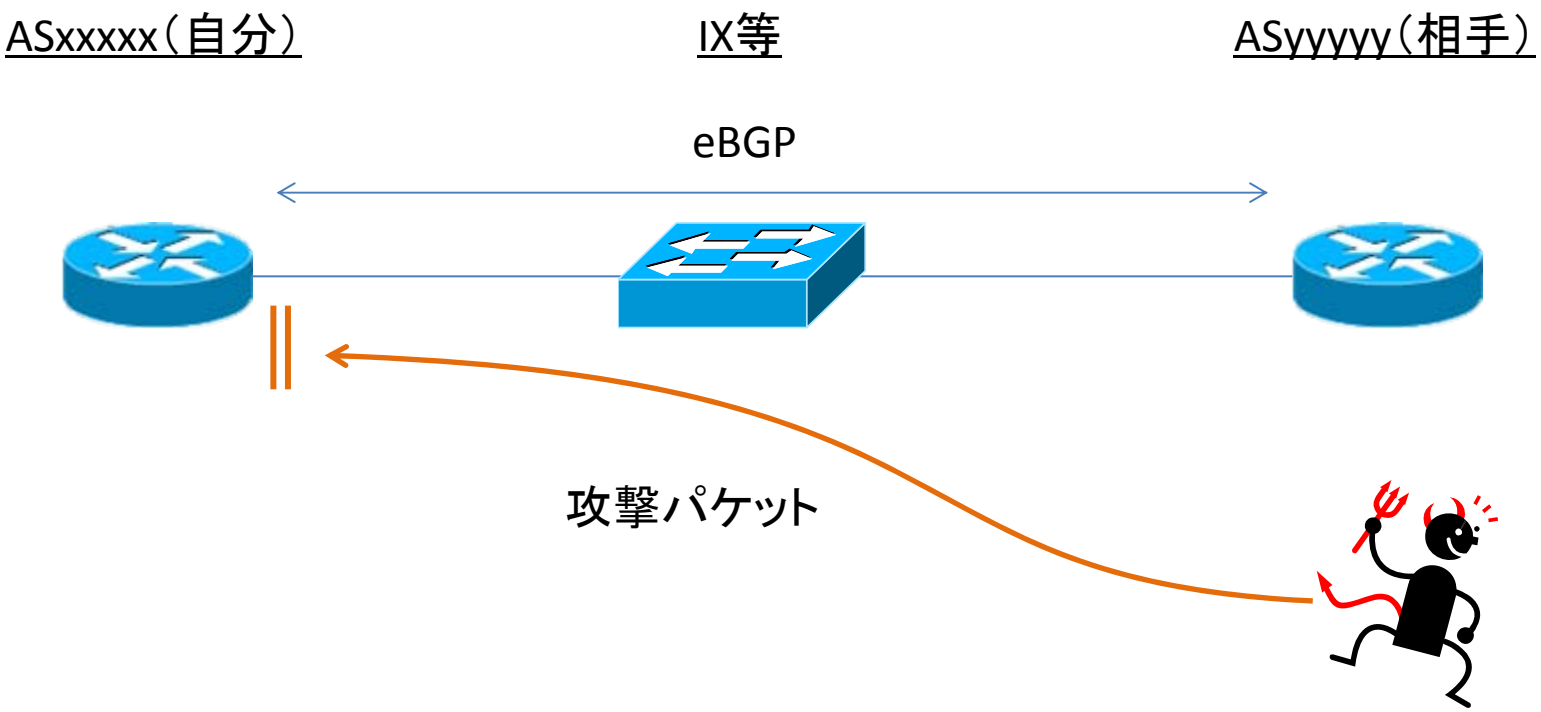
参考：point to pointリンクのピンポン



出典：Internet Week 2010 松崎さんの資料より
http://www.nic.ad.jp/ja/materials/iw/2010/proceedings/s9/

BGPセッションの保護

- IPv6でもTCP MD5オプションを有効に
- eBGPではneighborのアドレスのみACLで許可



eBGP受信経路のフィルタ

- JANOGが発行しているドキュメント(JC1006)が参考になる
  http://www.janog.gr.jp/doc/janog-comment/jc1006.txt
- ポリシーの例:

経路受信元	受信ポリシー
トランジット	Special-Use Prefix、自ASのPrefixを拒否、その他は許可
フリーピア	トランジットと同様 もしくは、AS-PATHフィルタ（＋Prefixフィルタ）
カスタマ	Prefixフィルタ + AS-PATHフィルタ

OSPFv3の保護

- 信頼するインターフェイスのみ有効化しておけば、それほど問題はない
- それでもなお信頼性を向上したい場合
  - IPsecを用いる
  - IPv6(OSPFv3)では認証オプションが削除された

Flow情報の収集

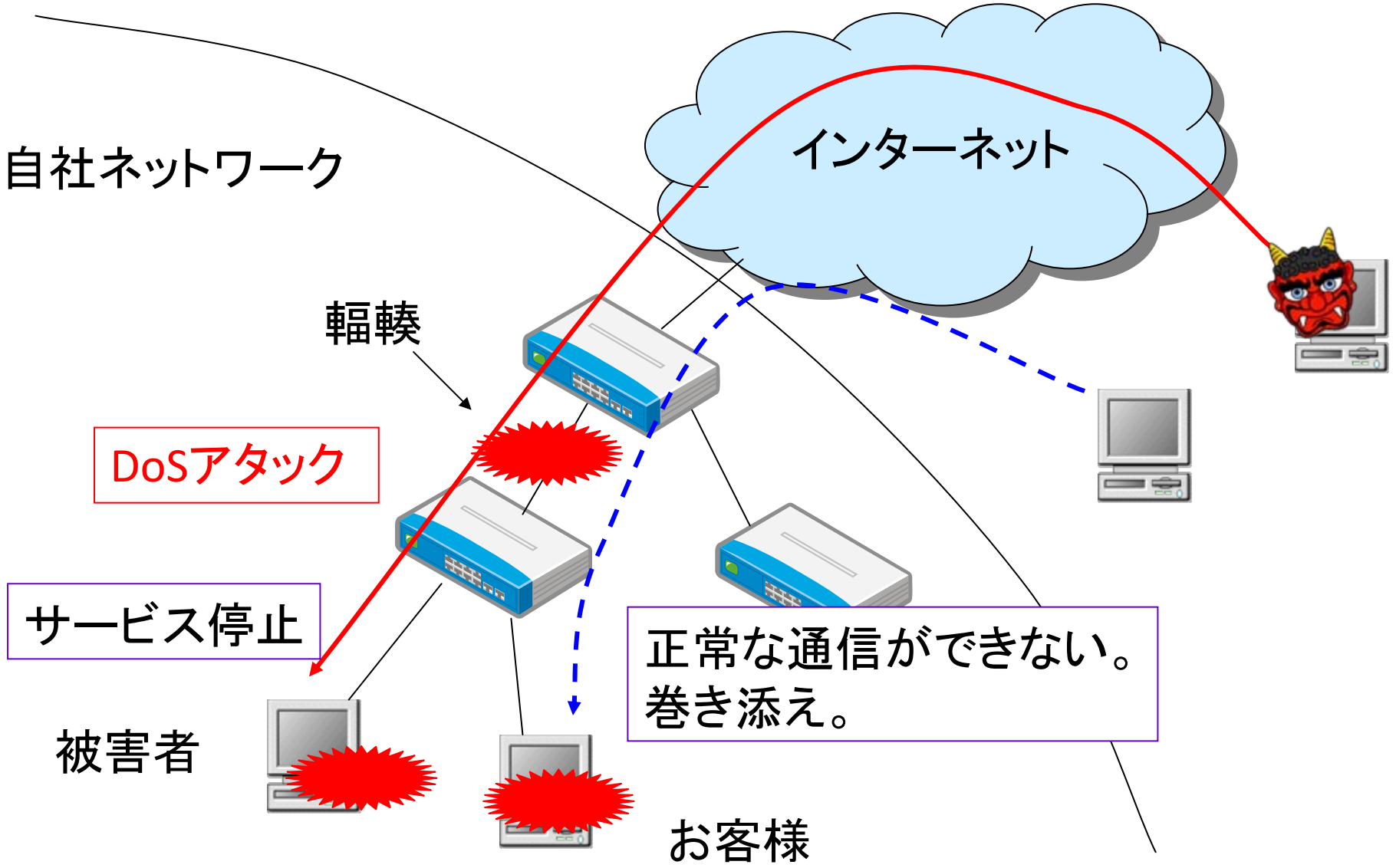
- トラフィックエンジニアリング以外にも、セキュリティインシデント発生時のトレースにも使用
- IPv6に対応しているプロトコル
  - NetFlow Version9
  - sFlow
  - IPFIX
- エクスポータ、コレクタの両方のIPv6対応が必要
- IPv6トラフィックが少ない場合は、ACL based sFlowを使う手もある
- ※ 通信の秘密を侵害しないよう、目的、手段に問題ないか確認の上で実施してください。

参考：sFlowでのサンプリング例

```
dstMAC 003048956801
srcMAC 0030489565ff
decodedVLAN 2
decodedPriority 0
IPSize 78
IPTOS 0
IP6_label 0x0
IPV6_payloadLen 38
IPTTL 64
srcIP6 2001:0e40:ffff:ffff:0000:0000:0000:0008
dstIP6 2001:0e40:ffff:ffff:0000:0000:0000:0007
IP6HeaderExtension: 44
IPProtocol 17
UDPSrcPort 10865
UDPDstPort 12337
UDPBytes 12851
```

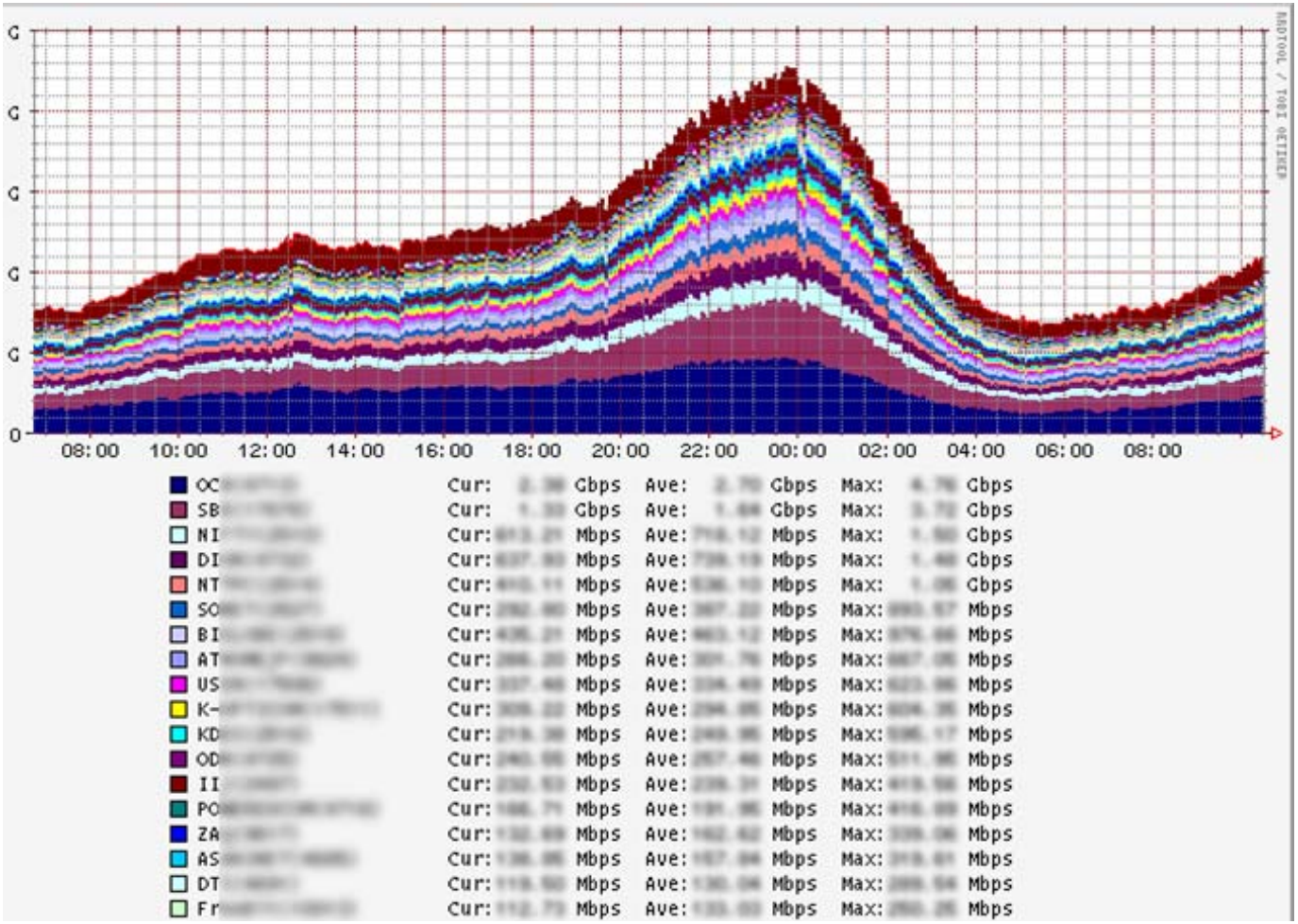
IPv6のフィールドが見えるか？

応用例：DoSアタックの検知



応用例:トラフィックエンジニアリング

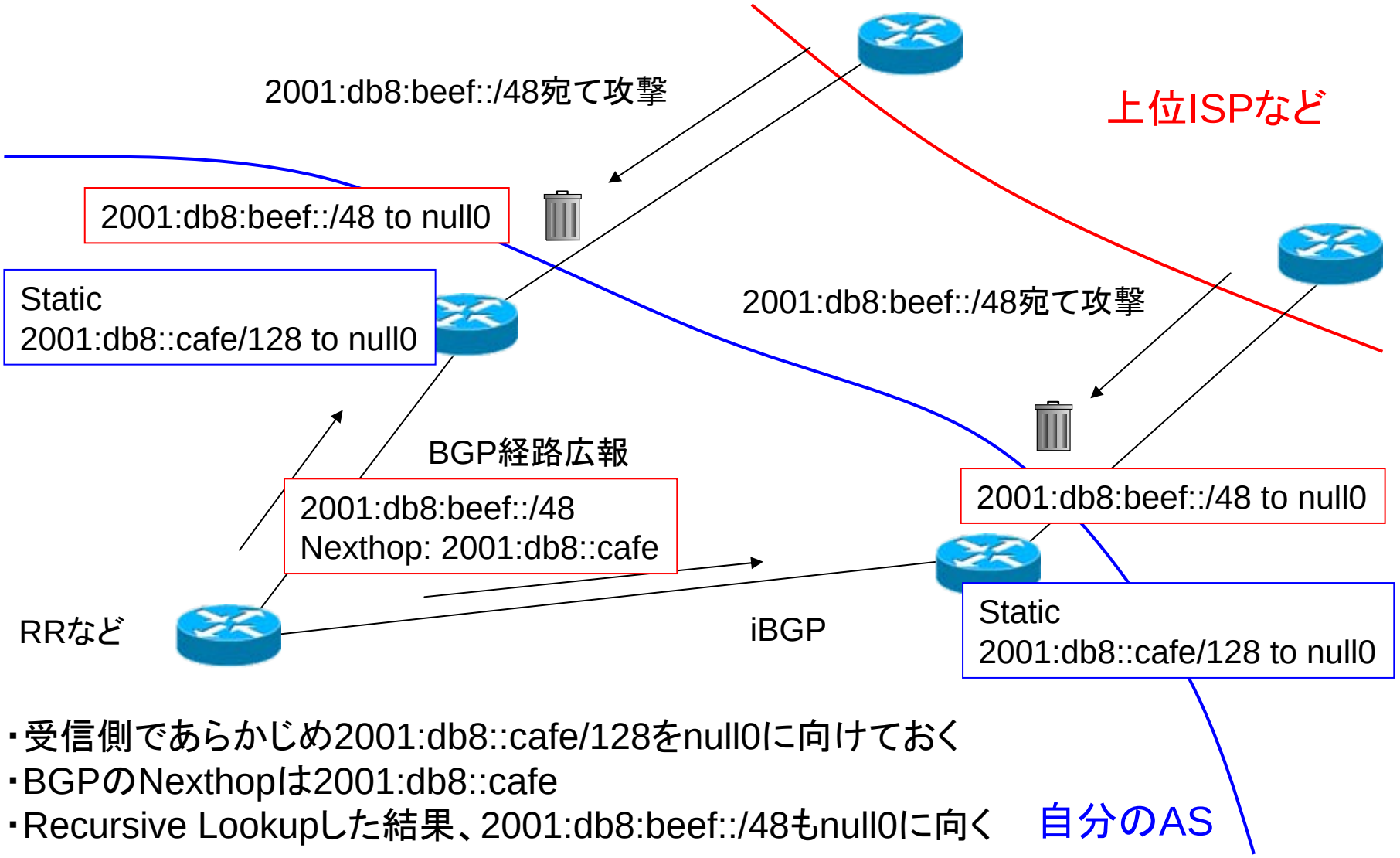
宛先AS別のトラフィック量測定



DoSアタックのフィルタリング

- インターネットから特定ユーザ向けに大量の攻撃トラフィックが発生した場合
- 攻撃トラフィックをフィルタする
- （１）ボーダルータでACLを書く
- （２）RTBHを使う
  - 参考：IRS14 RTBH実装例の紹介（AS9370編）
  - http://irs.ietf.to/past/docs_20071011/

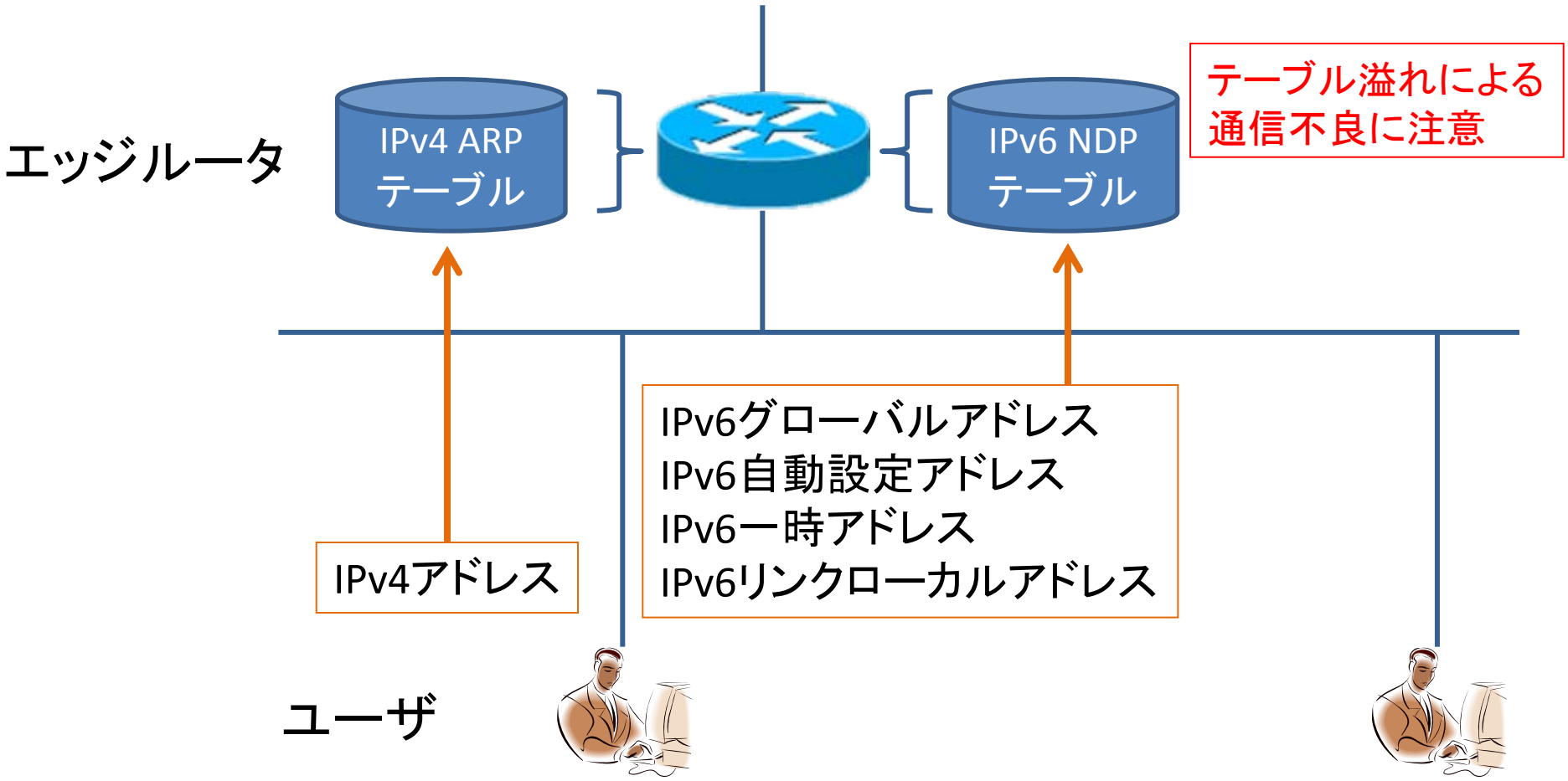
RTBHの動作原理



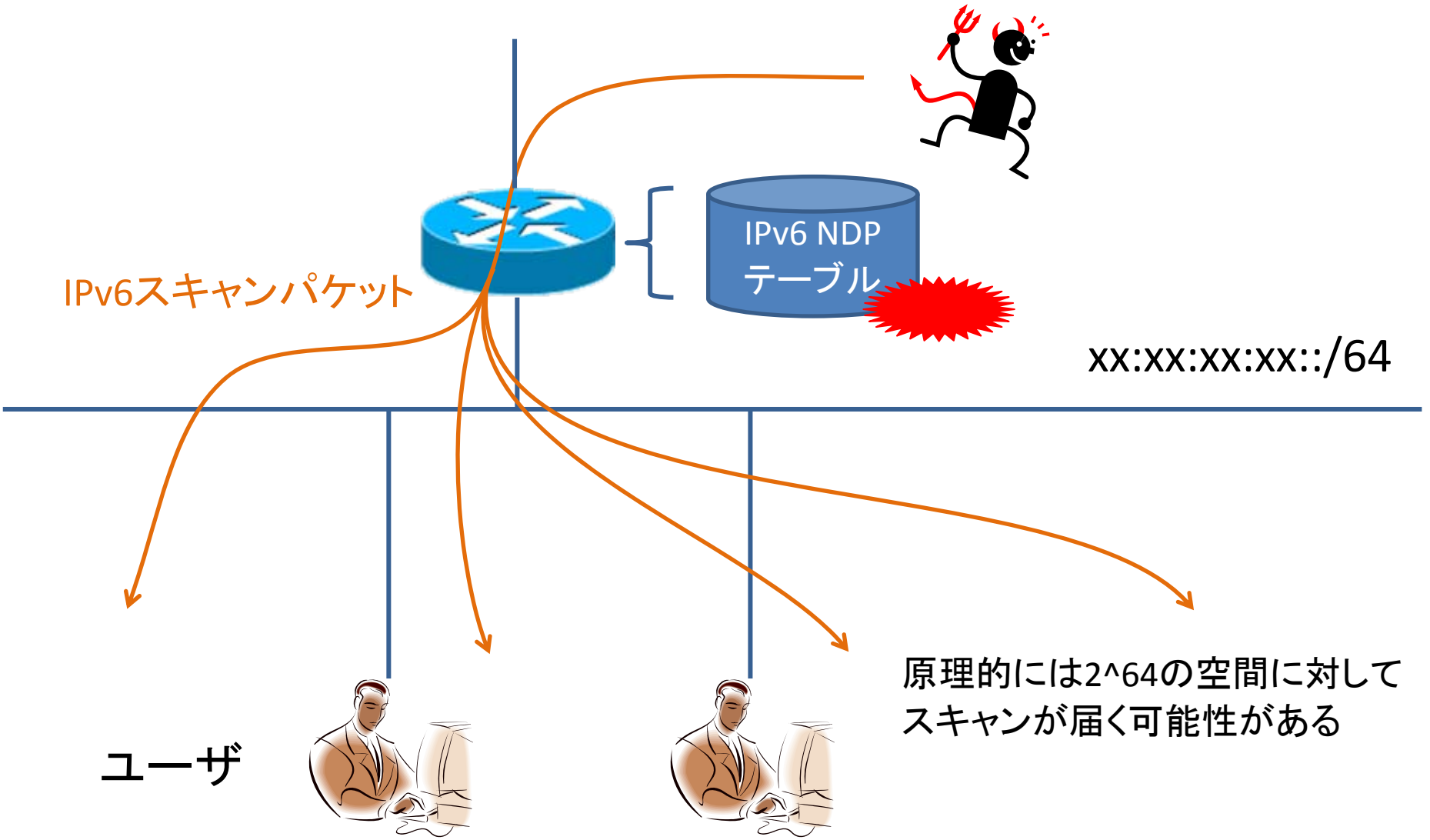
・受信側であらかじめ2001:db8::cafe/128をnull0に向けておく
・BGPのNexthopは2001:db8::cafe
・Recursive Lookupした結果、2001:db8:beef::/48もnull0に向く

エッジルータのリソース管理

デュアルスタックの場合、エッジルータのリソースが厳しくなる



IPv6によるスキャン



ユーザからの不正パケット防止

uRPFを使う方法もあり
（粒度が荒くてもよければ）

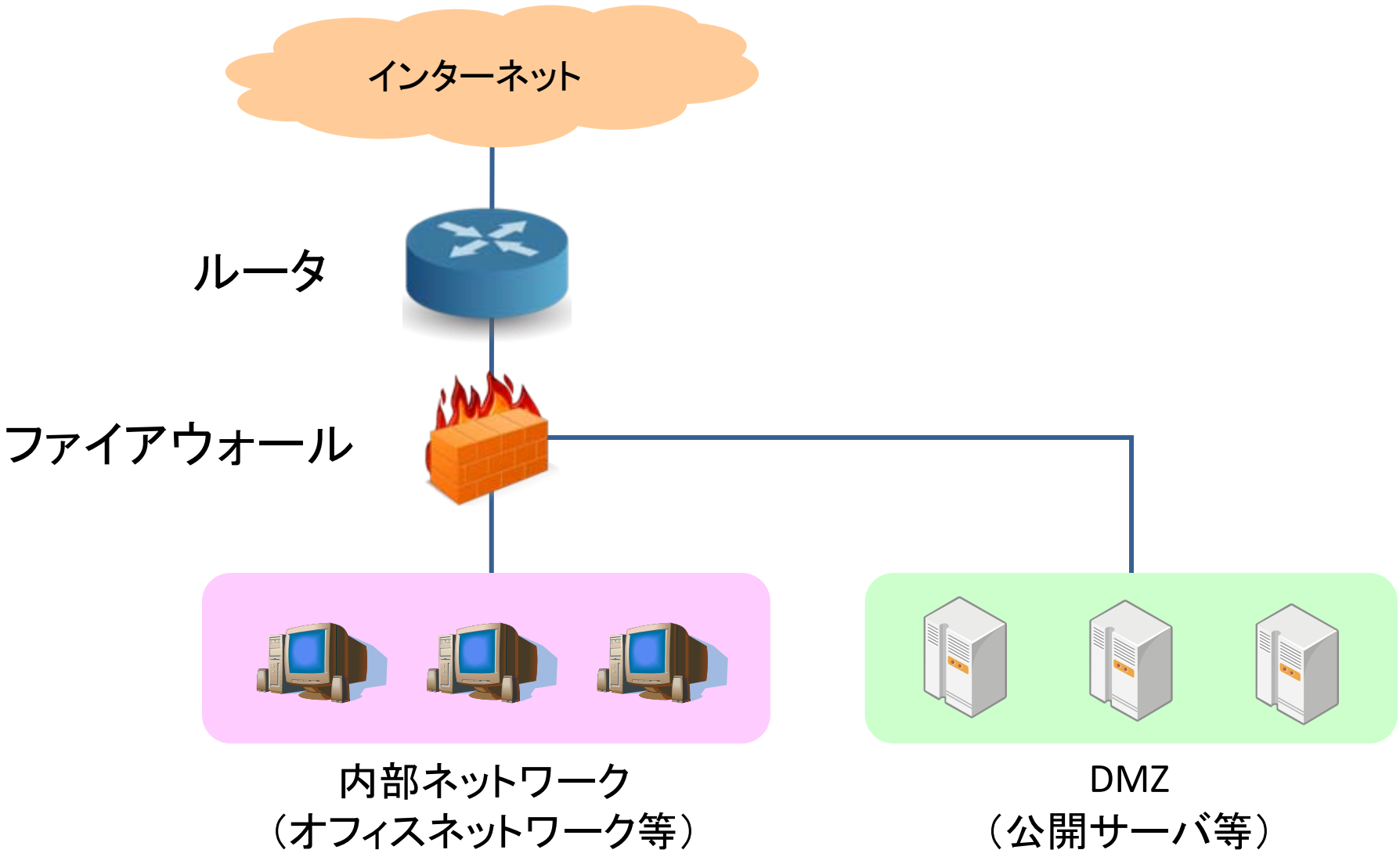
他ユーザのアドレス乗っ取りを防止
- ソースMACアドレス詐称防止フィルタ
- NA詐称防止フィルタ
- ソースIPv6アドレス詐称フィルタ
- Port Isolate機能の使用も有効

その他
- RAパケットのフィルタ
  RA Guard等
  （回避手段に注意）
- DHCPv6

L2スイッチ

エンタープライズ環境における
セキュリティ

エンタープライズネットワークモデル

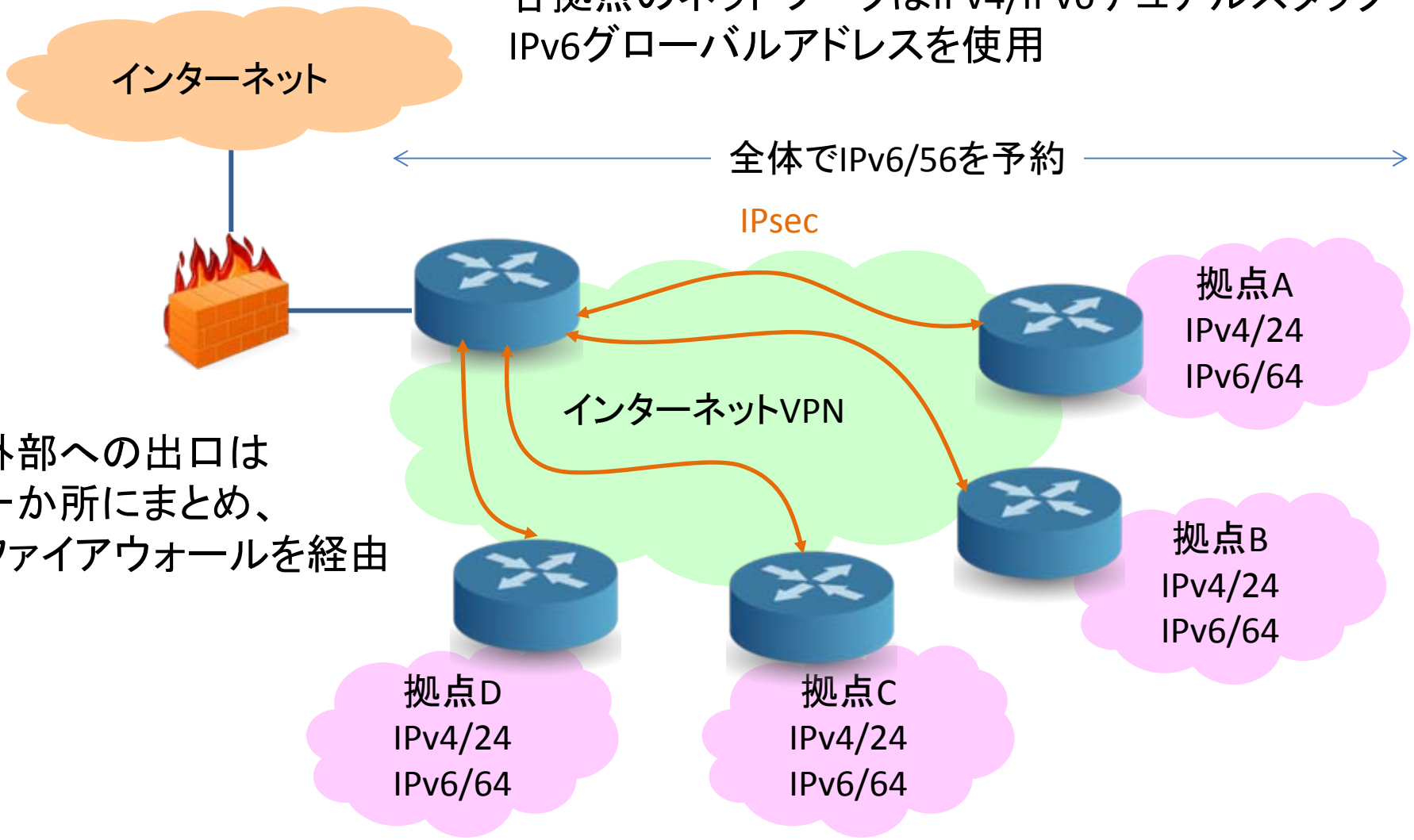


内部ネットワークの構成

- アドレス構成の選択肢
  - グローバルアドレス（GUA）
  - ユニークローカルアドレス（ULA）
- グローバルアドレスの場合
  - 構成がシンプル
  - ステートフルファイアウォールと組み合わせ
- ユニークローカルアドレスの場合
  - 実績が少ない
  - マルチホームが可能（なはず）
  - NAT66(NPTv6)機能が必要

弊社での構成例（GUAを使用）

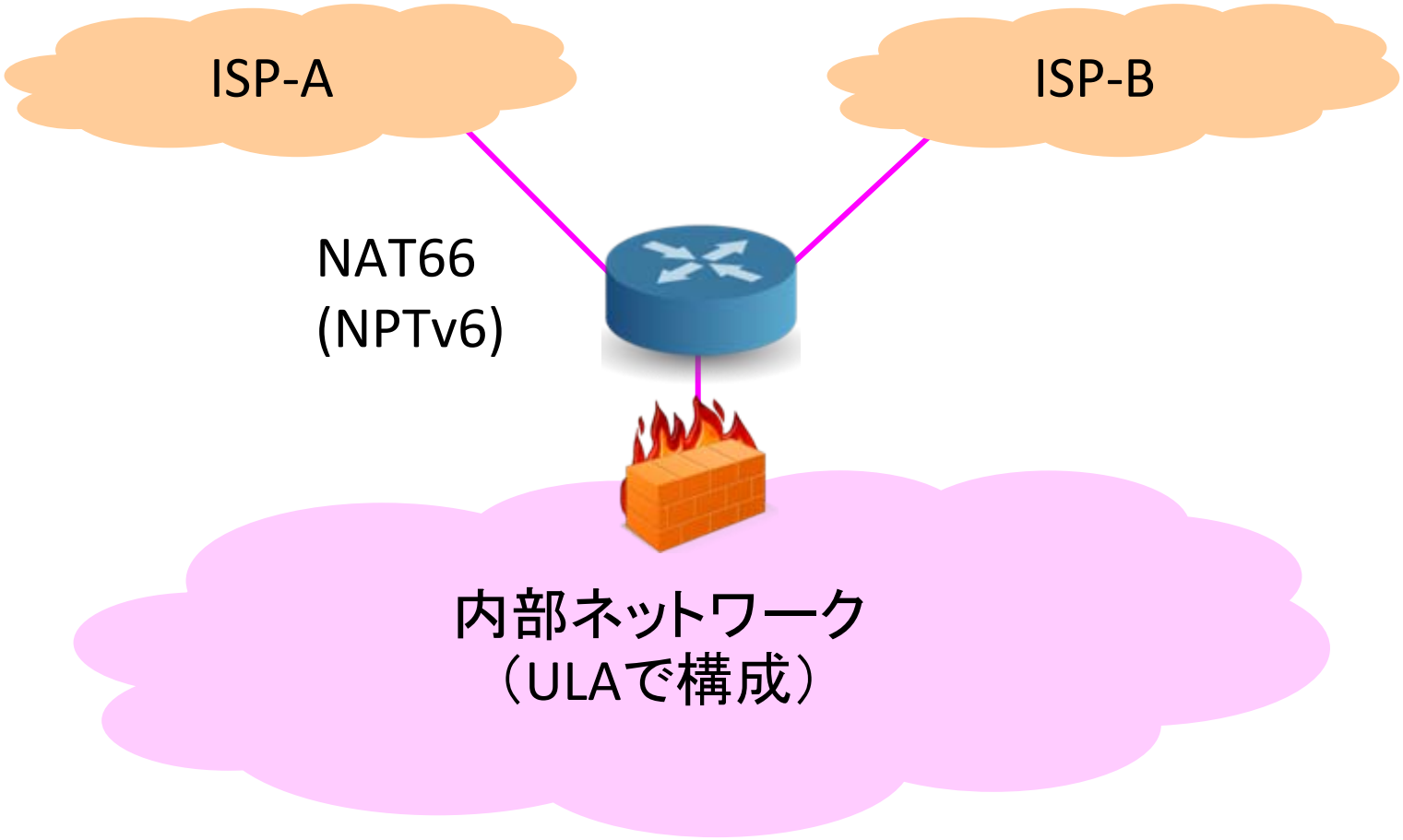
各拠点のネットワークはIPv4/IPv6デュアルスタック
IPv6グローバルアドレスを使用



外部への出口は
一か所にまとめ、
ファイアウォールを経由

ULAの使用例

NATによるマルチホームを実現したい場合など



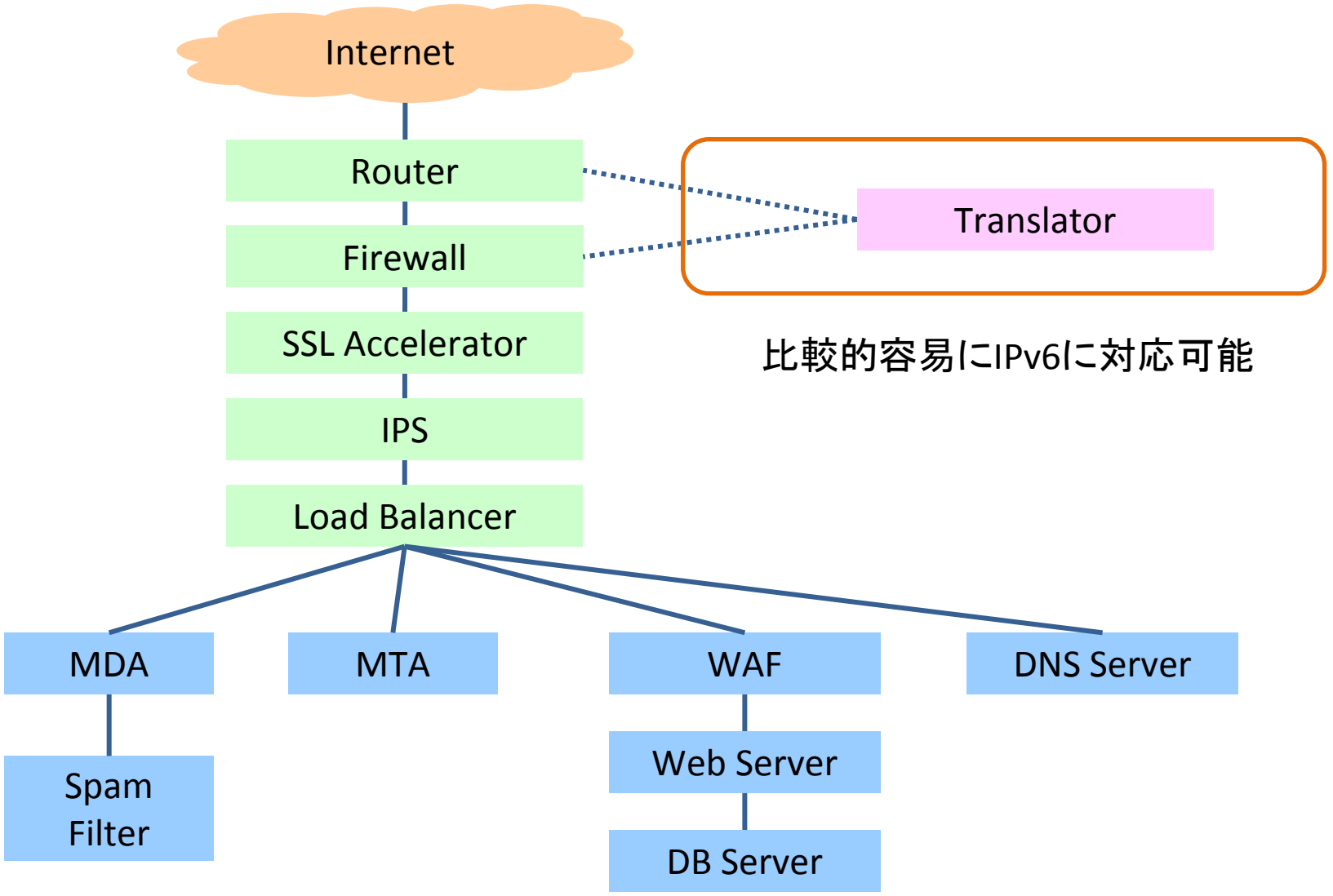
ファイアウォールの設定ポリシー例

- 外向け
  - 基本許可。ステートフルインスペクションにて、帰りのパケットを自動的に許可。
  - トンネルは原則禁止（IPinIPトンネル、Teredo、6to4などIPv4のポリシーに設定）。
  - その他、通信を不許可とする宛先を個別に拒否。
- 内向け
  - 基本拒否。
  - サーバ向けなど、開放するポートを個別に許可。
  - 外部からVPN等で接続する場合、送信元を個別に許可。
  - 不正なパケットを拒否（RH0など）。

ファイアウォール実装の確認項目

- フラグメントヘッダの扱い
  - リアセンブルしてインスペクションできるか？
- 拡張ヘッダの扱い
  - 何段までトレースできるか
  - unknownな拡張ヘッダの扱い
- シグネチャ
  - IPv6にどの程度対応しているか

DMZのモデル


Internet
Router
Firewall
SSL Accelerator
IPS
Load Balancer
Translator
比較的容易にIPv6に対応可能
MDA
MTA
WAF
DNS Server
Spam Filter
Web Server
DB Server

トランスレータを使用しているケース

- いくつかセキュリティ課題が存在
- ログ取得が必須
  - 本来のソースIPv6アドレスが見えなくなる
  - トランスレータにてアクセスログの調査が必要
- ログのIPv6アドレス表記ゆれに注意
  - トラブル発生時の調査が困難になるケースも
  - RFC5952に準拠する
- セッション溢れの懸念
  - 同時セッション数やCPS（新規コネクション/秒）の性能を確認しておく。
- サーバでのアクセス制御の注意点
  - IPv6からのアクセスが、単一（トランスレータ）のIPv4アドレスからきているように見える。

IPv6サービス監視、マネジメント

- サービス監視
  - IPv6トランスポートでも行う
  - エージェントを仕込む場合、エージェントとの通信はIPv4でもよい。
- マネジメント
  - Out-of-bandで行うのが一番良い。
  - In-bandで行う場合、IPv4でも良いが、IPv6も通っている場合は、IPv6でのアクセス制限を忘れずに。
  - 外部からのアクセスが筒抜けにならないように注意する。

まとめ

- ISPネットワーク
  - ルータの防御を中心にルーティングプロトコル、リソース管理、統計情報の採取を適切に行う
  - 顧客による不正通信にもケアが必要
- エンタープライズネットワーク
  - 内部にもIPv6グローバルアドレスを使用するケースもある
  - ステートフルファイアウォールの実装が必須
  - 拡張ヘッダ、フラグメントヘッダには要注意
  - サービス監視、マネジメントをきちんと行う