ISPのNATには何が求められるか？

NTTコミュニケーションズ株式会社
西谷　智広

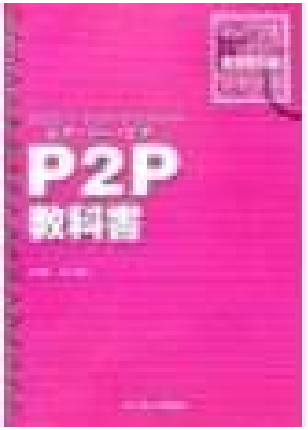
目次

1. 自己紹介
2. ISPのNATが満たすべき要件は？
    1. 透過性
    2. 接続確立性
    3. 公平性
3. サービス影響
4. まとめ

1. 自己紹介

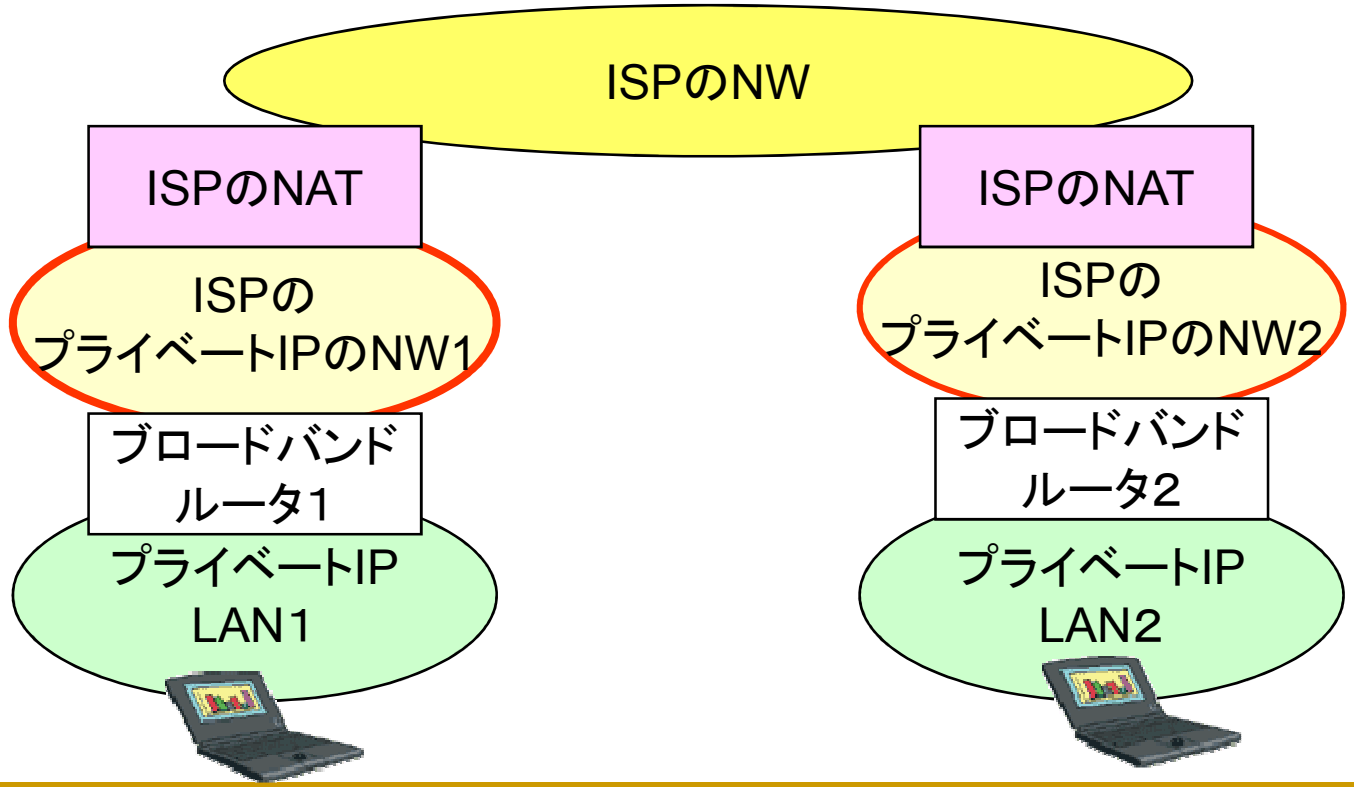
- NTTコミュニケーションズ株式会社
  先端IPアーキテクチャセンタにて
  - VoIPに関わるNAT越え研究（シームレスコネクション）
  - P2PのNW効率化に対する支援（総務省案件）
  - クリックダイヤル（VoIP-WEB連携ソフトウェア）開発

  等を担当
- 主な執筆書
  - インプレスR&D　P2P教科書（2007年12月）
  - UNIX　Magazine P2P特集号（2006年10月



2. ISPのNATが満たすべき要件

ISPのNATは、家庭用BBルータのNATや、企業用FWのNATとは異なったある一定の要件を満たすべきと考える



2. ISPのNATが満たすべき要件

満たすべき要件
「できる限り、通信を阻害しない」

- 高い透過性
- 高い接続確立性
- 公平性の確保

- 高スループット
- 高可用性

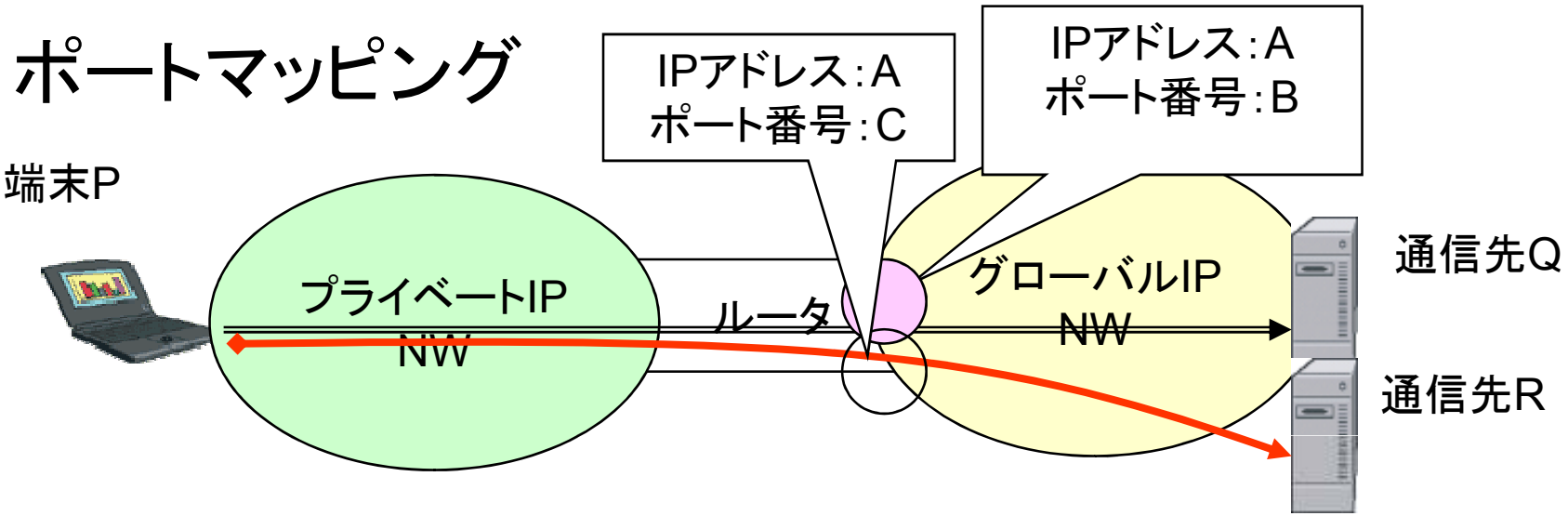
これらを満たすものがキャリアグレードNATであると考える

2-1. 透過性

- NATの分類方法
  - RFC4787
    - Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
      - ポートマッピング
      - ポートフィルタリング
      - ヘアピニング

2-1. 透過性

- ポートマッピング



グローバル側IFのポート番号（ポート番号C）の規則

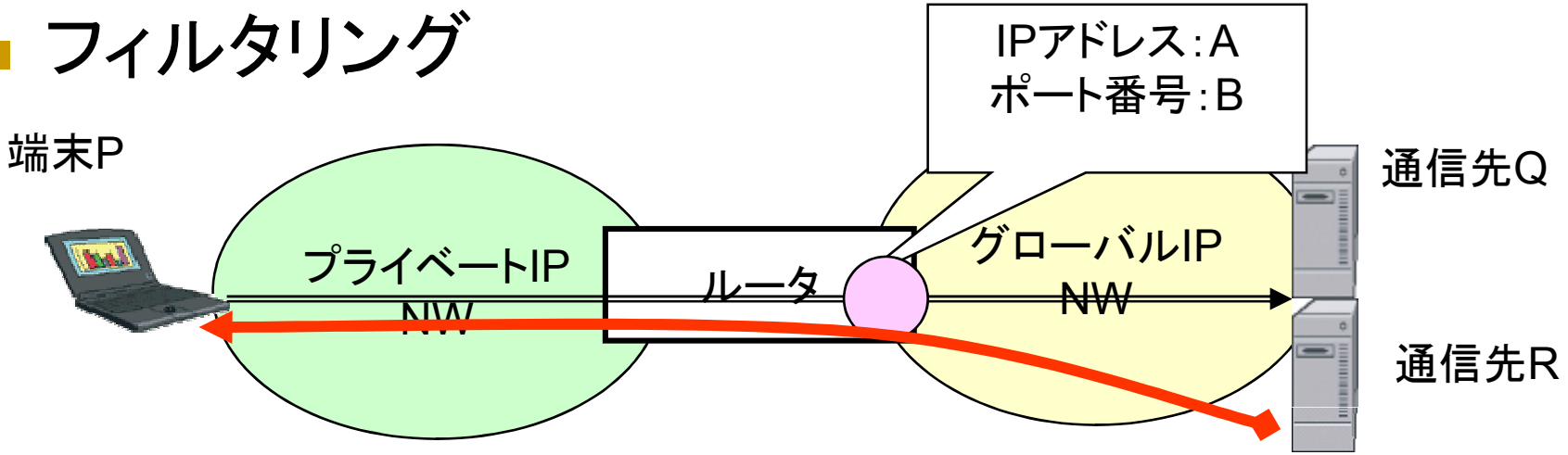
◆相手によらず同一

◆IPアドレス依存

◆IPアドレス＆ポート番号依存

2-1. 透過性

- フィルタリング



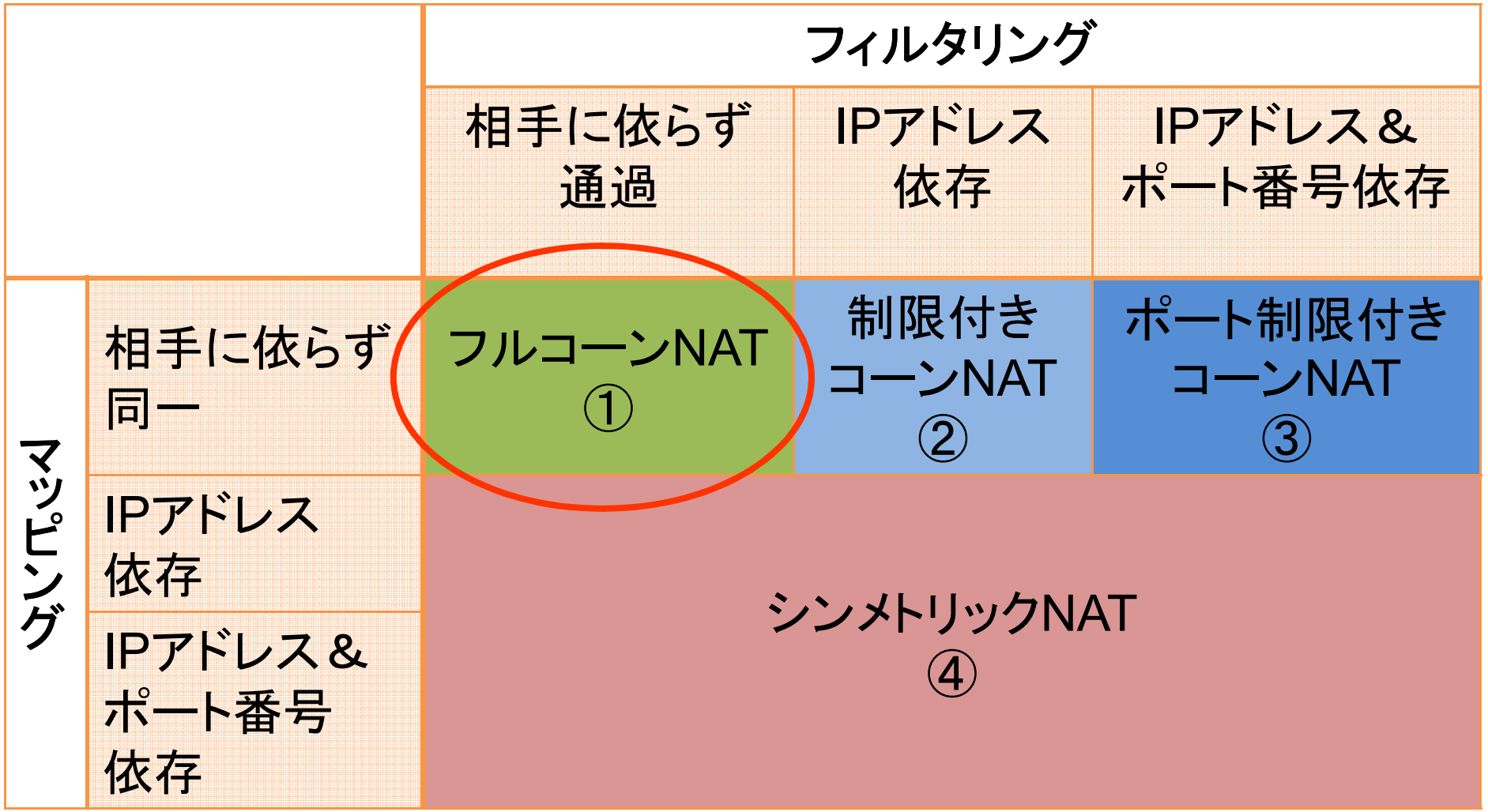
NAT外部からの通信透過の規則

◆相手によらず通過

◆IPアドレス依存

◆IPアドレス＆ポート番号依存

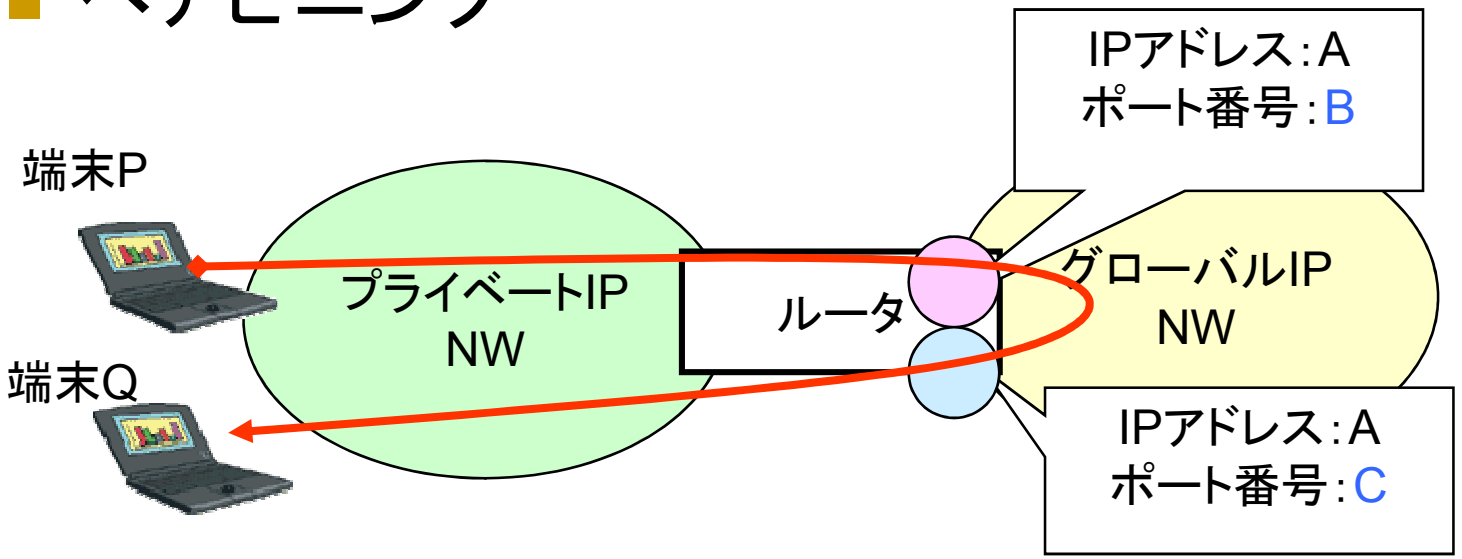
2-1. 透過性



*コナミDE　佐藤氏資料から引用

2-2. 接続確立性

- ヘアピニング

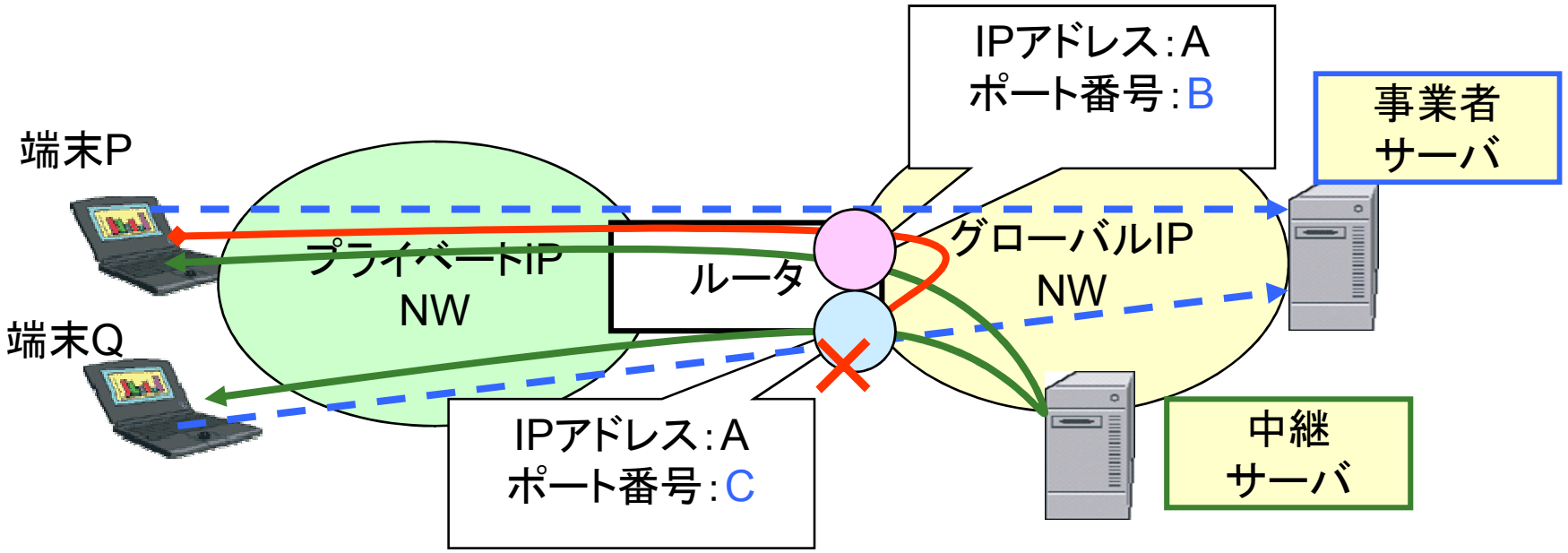


ヘアピニング有り

同一NAT配下の端末の「グローバル側IFのIPアドレスとポート番号」を指定して通信すると、NATルータが通信を折り返ししてくれる機能

2-2. 接続確立性

- ヘアピニング機能がルータにないと！

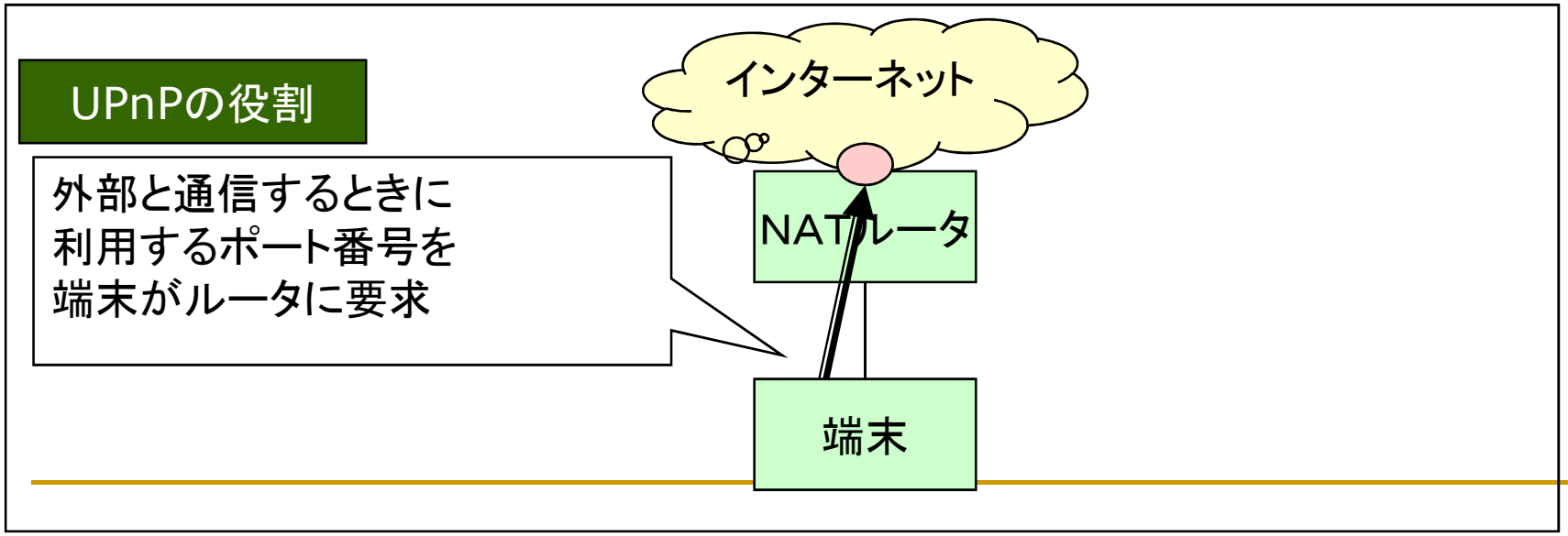


•事業者サーバが端末として意識できるNW情報はルータのグローバルIF側のIPアドレスとポート番号のみ！

•NATにヘアピン機能がないと、端末間で通信できるようにする中継サーバを設置する必要がある。

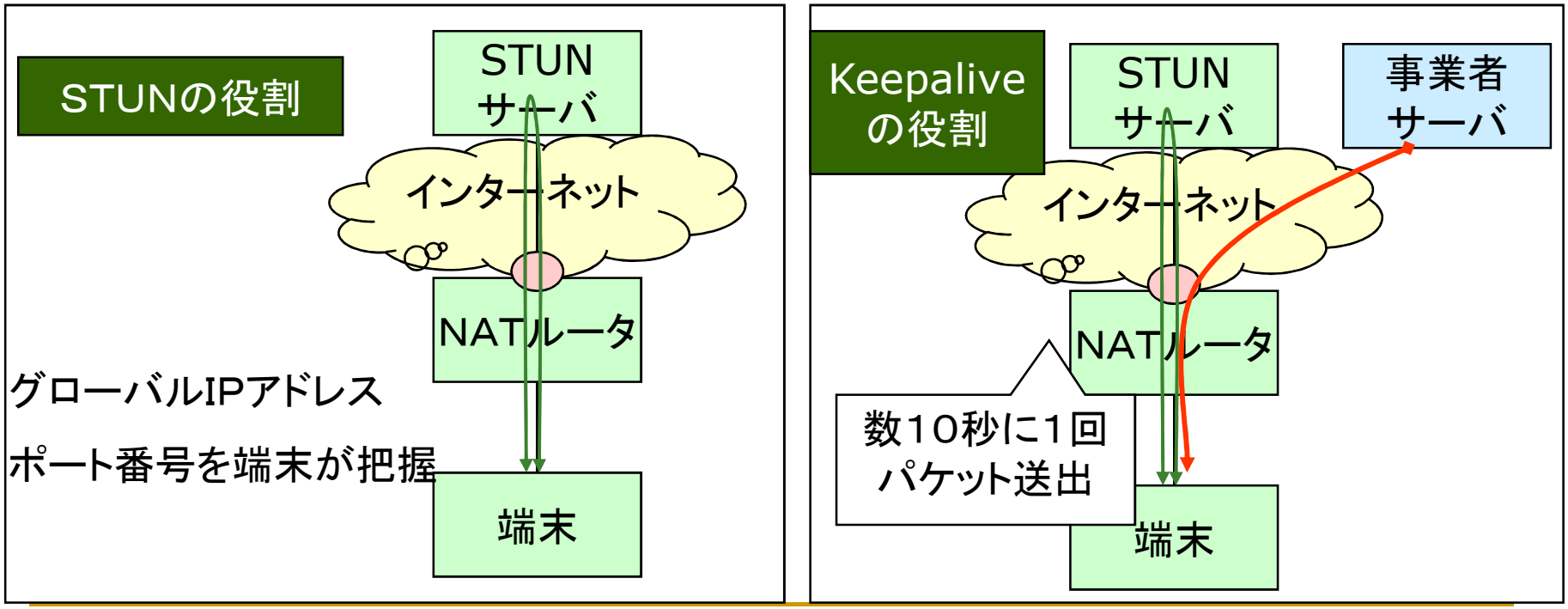
2-2. 接続確立性

- UPnP (Universal Plug and Play)
  - サーバレスでNAT越えが可能
  - コンシューマ向けは対応しているルータが多い
  - マルチキャストでUPnPルータを探索
  - 2重NAT越えは（UPnPだけでは）困難
  - 認証機能もなく、ISPのNATへの導入は簡単ではない



2-2. 接続確立性

- STUN（Session Traversal Utilities for (NAT)）
  - NATルータのグローバル側IFのIPアドレス、ポートを取得する
  - Keepalive（NATルータのグローバル側IFのポート番号の維持）

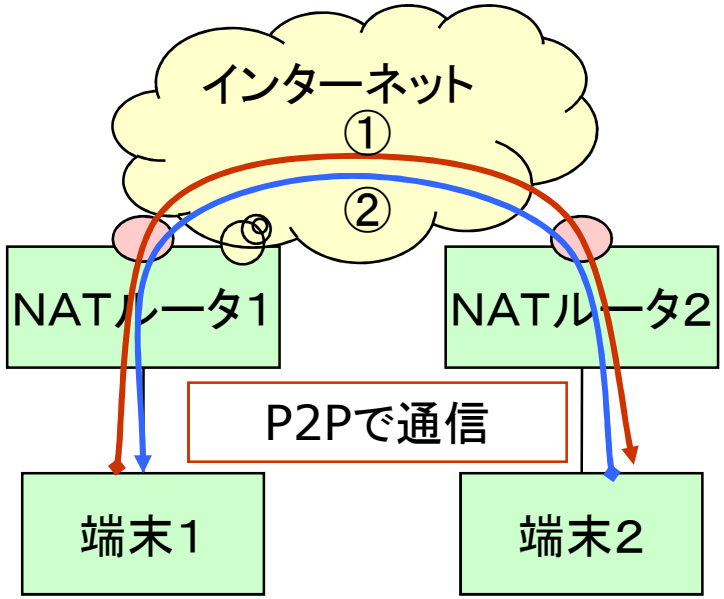


2-2. 接続確立性

UDP Hole Punching

・NATルータ間で直接UDPを送受信するテクニック

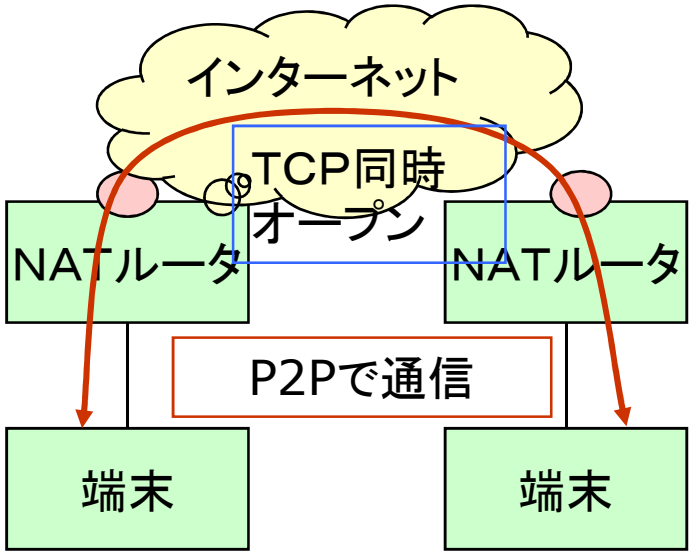
・実施可能性はルータ依存



TCP Hole Punching

・NATルータ間で直接TCPを送受信するテクニック

・実施可能性はルータ、OS依存



2-3. 公平性

- 公平性の確保
  - グローバルIPアドレスの複数ユーザでのシェア
  - ポート番号、ICMP IDは各ユーザで排他的に利用
  - ユーザ毎に、ポート番号、ICMP IDを制限する

2. ISPのNATが満たすべき要件(再掲)

満たすべき要件

「できる限り、通信を阻害しない」

- 高い透過性　　(Full Coneであること)
- 高い接続確立性(ヘアピニング、UDP/TCP Hole Punchingが利用可能であること)
- 公平性の確保　(ポート番号、ICMP IDはユーザ毎に制限可能であること)
- 高スループット
- 高可用性

これらを満たすものがキャリアグレードNATであると考える

3. サービス影響

（1）NATそもそもの仕様により影響するサービス

1-1 アプリケーション層にNW情報を格納する

- SIP

1-2 パケットの改ざんを検証する

- IPSec

1-3 ポート番号を（容易に）制御できない

- SIP,IPSec

1-4　インターネット側から端末への通信が発生する

- FTP,インスタントメッセンジャー,P2Pサービス

⇒UPnPは使えない！（キャリアグレードNATの穴あけはできない）

3. サービス影響

（2）IPアドレスによって認証、利用許諾をチェックするサービス

- 複数ユーザが同一IPアドレスを共有
- 他人が成りすまし出来る可能性
- ポート番号まで意識する必要がある
- パスワード認証等が必要

3. サービス影響

（3）ポート使用数の制限により影響のあるサービス

3-1 同時コネクション数が多いサービス

- Ajax,P2Pソフトの一部
  - Google Earth,Google Maps
- Webサイト、特にマッシュアップサイト
- 高速ダウンロード・アップロードを行うソフトウェア

3-2 通信相手が非常に多いサービス

- RSSリーダー等

4. まとめ

- ISPのNATが満たすべき要件「出来る限り通信を阻害しない」
  - 高い透過性
  - 高い接続確立性
  - 公平性

  } キャリアグレードNAT

- キャリアグレードNATでも、影響を受けるサービスはある
  - NATそもそもの仕様
  - IPアドレスによる認証、利用許諾
  - ポート使用数の制限

- IPv6へ速やかに移行する必要がある

（参考）

キャリアグレードNATの要求条件

⇒draft-nishitani-cgn-00 “Carrier Grade NAT Behavioral Requirements for Unicast UDP, TCP and ICMP”

- UDP
  - RFC4784 “NAT Behavioral Requirements for Unicast UDP “
- TCP
  - draft-ietf-behave-tcp-07 “NAT Behavioral Requirements for TCP”
- ICMP
  - draft-ietf-behave-nat-icmp-08 “NAT Behavioral Requirements for ICMP protocol “

プライベートIPアドレスの割り当て

⇒draft-shirasaki-isp-shared-addr-00

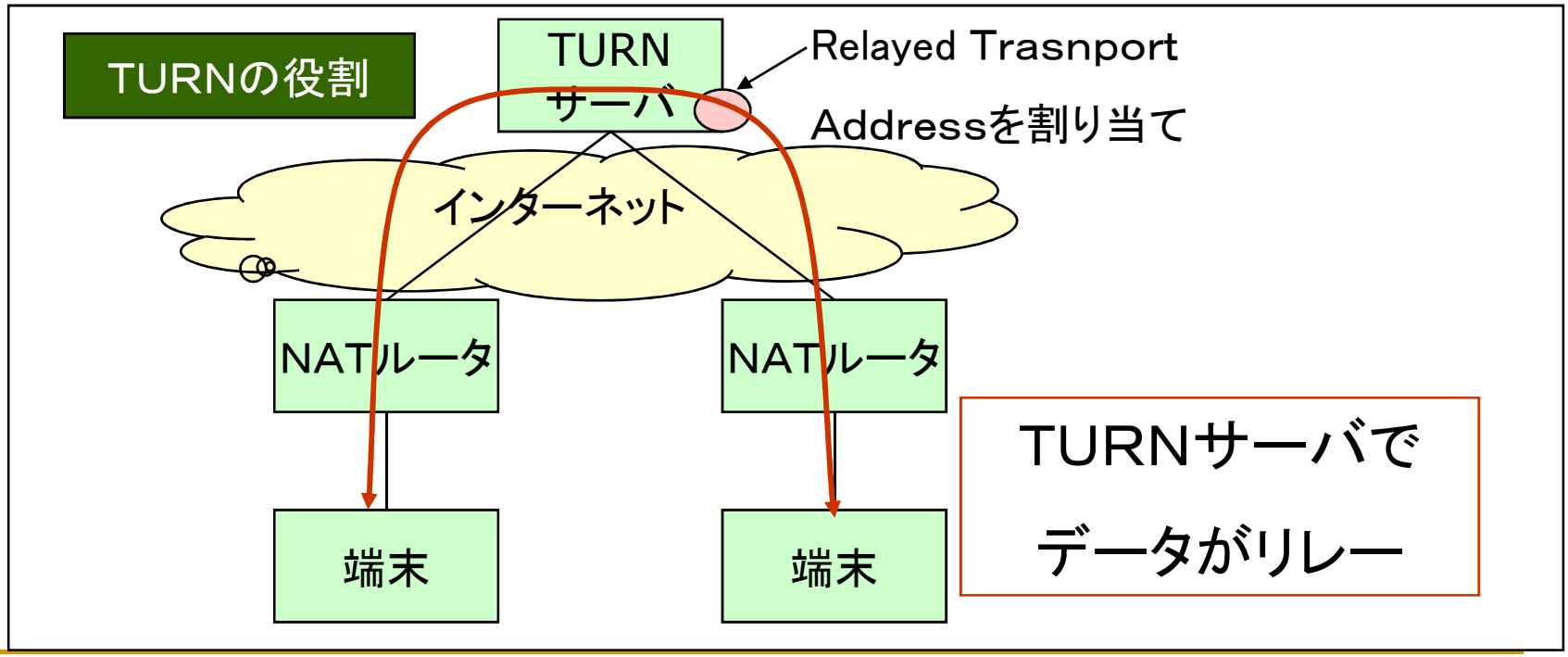
(参考) サービス影響の低減案

- ポート、セッション数制限に対する考慮
  インフラ的な重要プロトコル、例えば
  - メール（POP3,SMTP）
  - NTP

  等については、
  方式１：特別にポート番号を確保
  方式２：パススルー方式
  によってユーザはいつでも使える、という案もあるかも

NAT越え技術（参考）

- TURN（Traversal Using Relays around NAT）
  - サーバリレーにてUDP/TCP通信のNAT越えを行う



NAT越え技術（参考）

- ICE（Interactive Connectivity Establishment ）