



## 本資料について

本資料は下記の文献をもとに作成されました。  
文章内容の正確さは保障できないため、正確な知識を  
求める方は原文を参照してください。

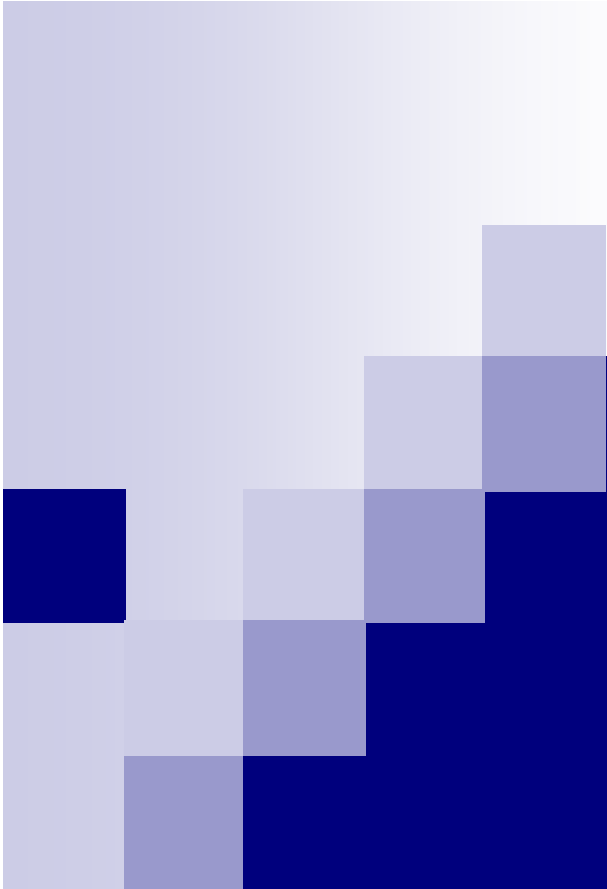
著者： J.Rosenberg, J.Weinberger, C.Huitema, R.Mahy

文献名： STUN —

Simple Traversal of User Datagram Protocol (UDP)  
Through Network Address Translators (NATs)

種類： Request for Comments (RFC) : 3489

発表日： March 2003

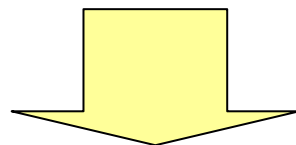


# NAT越え技術 「STUN」について

名城大学理工学部 渡邊研究室  
榎本 万人

## はじめに

クライアント同士が直接通信するP2Pタイプのアプリケーションにとって重要な問題



**「NAT越え」**

とくに両側でNATが存在する場合、既存技術でP2P通信を行うことは困難



# NAT越え技術「STUN」

- UDPによるNAT越え技術の一つ

## STUN

— Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) —



# NAT越え技術「STUN」

## ■ 基本機能

- 端末とインターネットの間にあるNATの存在, その種類を判別
- NATに割り当てられた外部アドレスを調べる

## ■ STUNを利用することで

異なるNAT内部の端末同士で  
UDPパケットを送受信することが出来る。

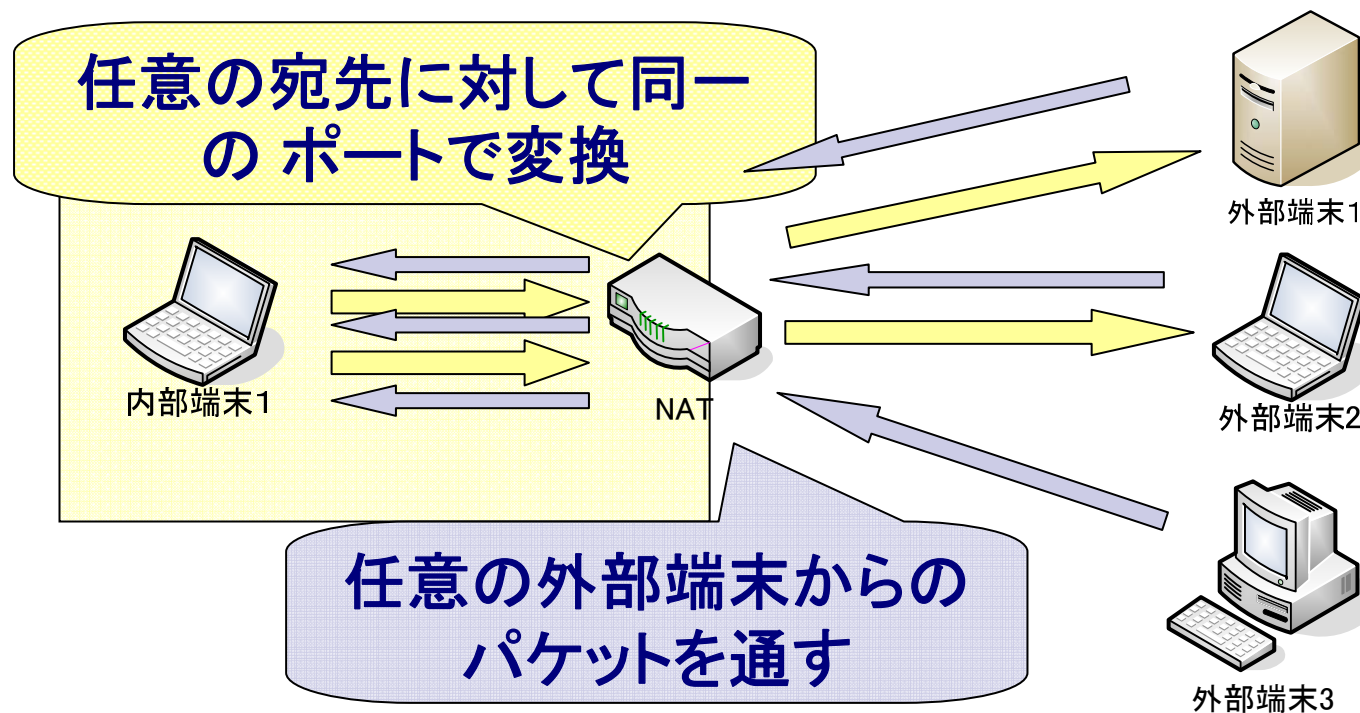


## NATのタイプ

- STUNで定義されるNATには処理に応じて次の4つのタイプがある
  - **Full Cone**
  - **Restricted Cone**
  - **Port Restricted Cone**
  - **Symmetric**

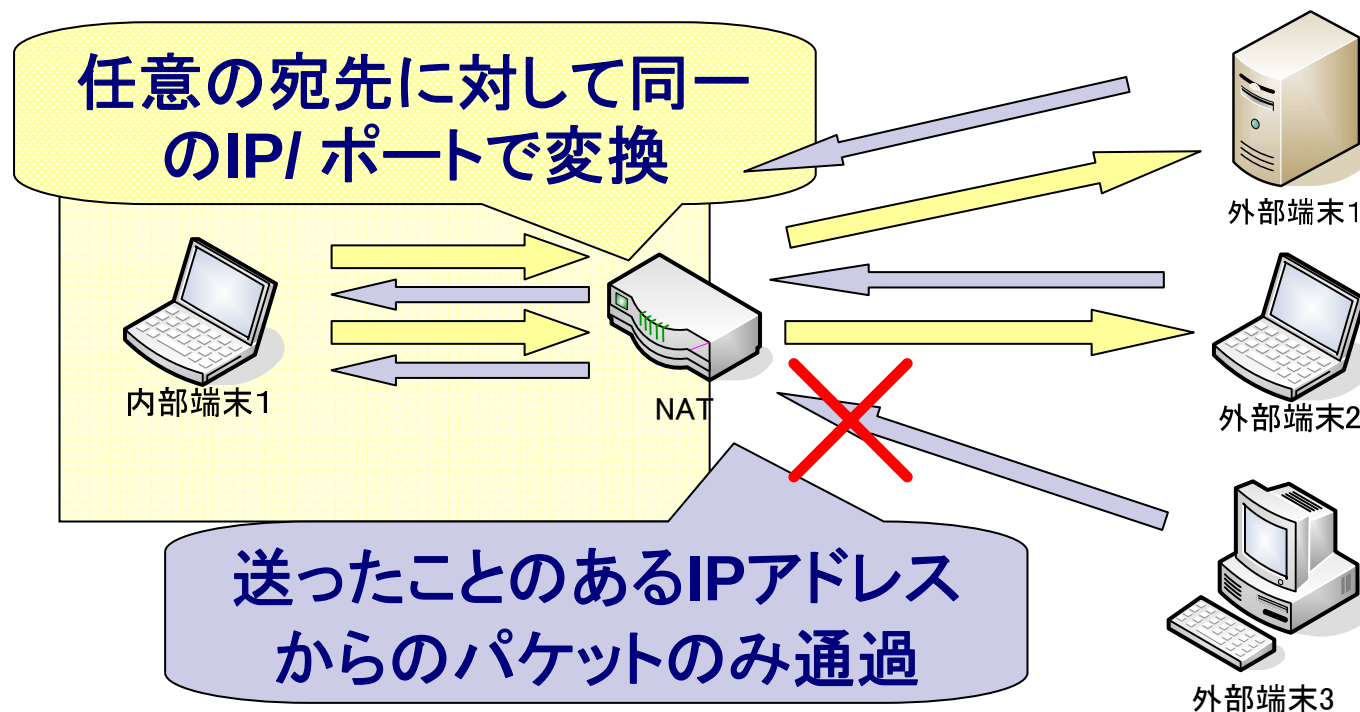
# Full Cone

- NAT内部にある同一の端末から送信されるパケットは宛先に関係なく同じポート番号が割り当てられる.
- NATでマップされたIPアドレス／ポートを宛先とすれば、任意の外部からNAT内部へ送信可能.



# Restricted Cone

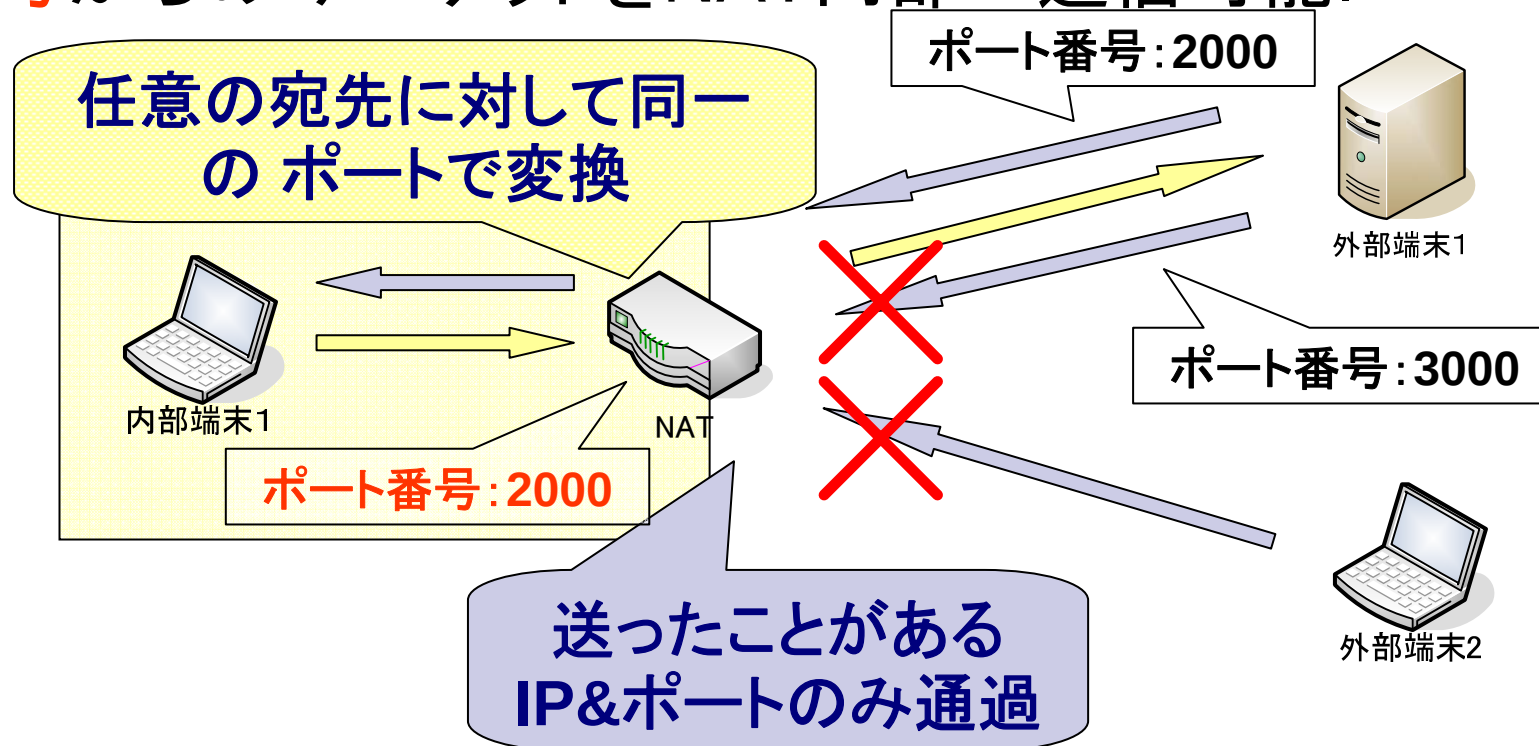
- NAT内部にある同一の端末から送信されるパケットは宛先に関係なく同じポート番号が割り当てられる.
- NAT内部から送信したことがあるIPアドレスからのみパケットをNAT内部へ送信可能.





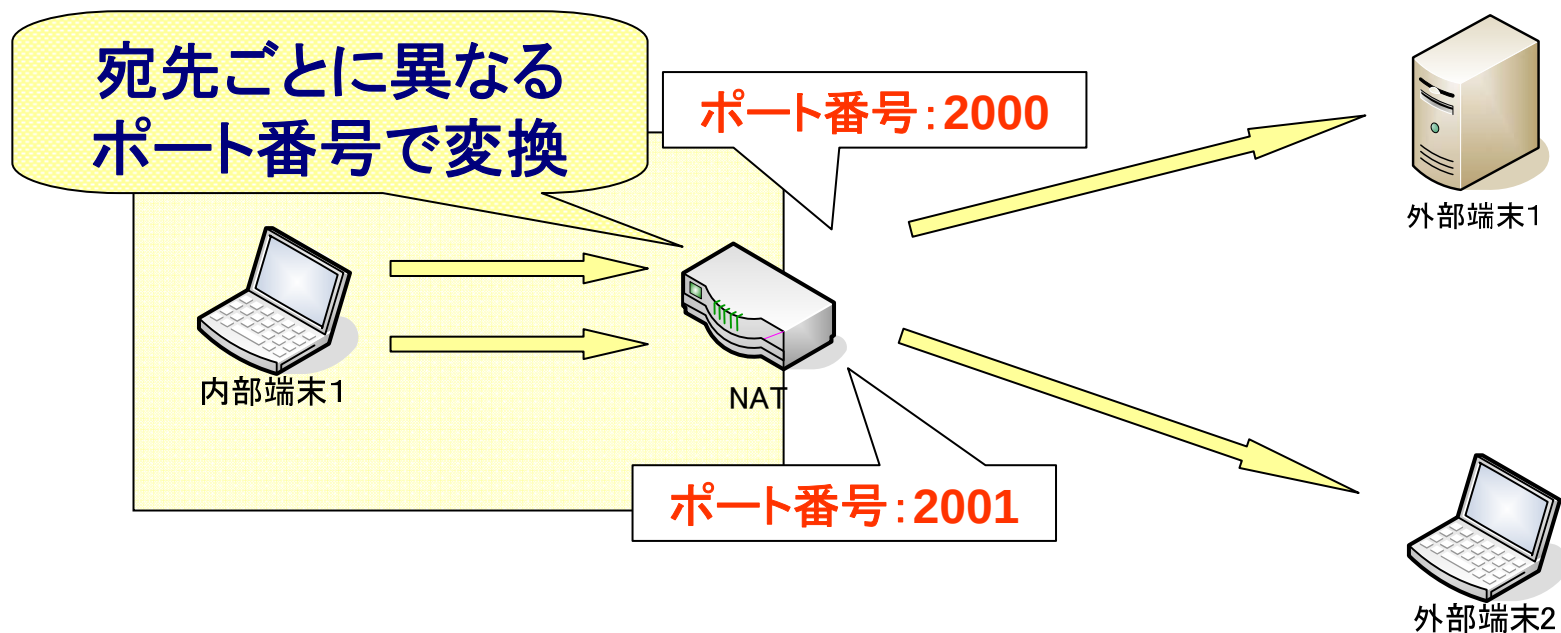
# Port Restricted Cone

- NAT内部にある同一の端末から送信されるパケットは宛先に関係なく同じポート番号が割り当てられる.
- NAT内部から送信したことがあるIPアドレス & ポート番号からのみパケットをNAT内部へ送信可能.



# Symmetric

- NAT内部にある同一の端末から送信されるパケットは宛先が異なれば、異なるポート番号が割り当てられる.
- NAT内部から送信したことのあるIPアドレス & ポート番号からのみパケットをNAT内部へ送信可能.

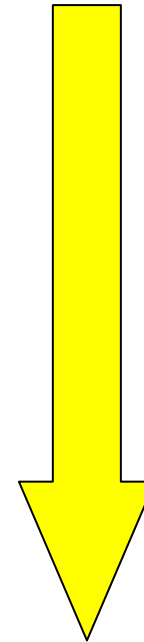


# 4種類のNATの比較

- Full Cone
- Restricted Cone
- Port Restricted Cone
- Symmetric

異なる宛先でも同じポート番号が割り当てられる

NAT越えが容易



NAT越えが困難

異なる宛先には異なるポート番号が割り当てられる



# STUNの動作

## ■ クライアント・サーバプロトコル

- STUNクライアント
- STUNサーバ      ーグローバル空間に存在

## ■ 2種類のリクエスト

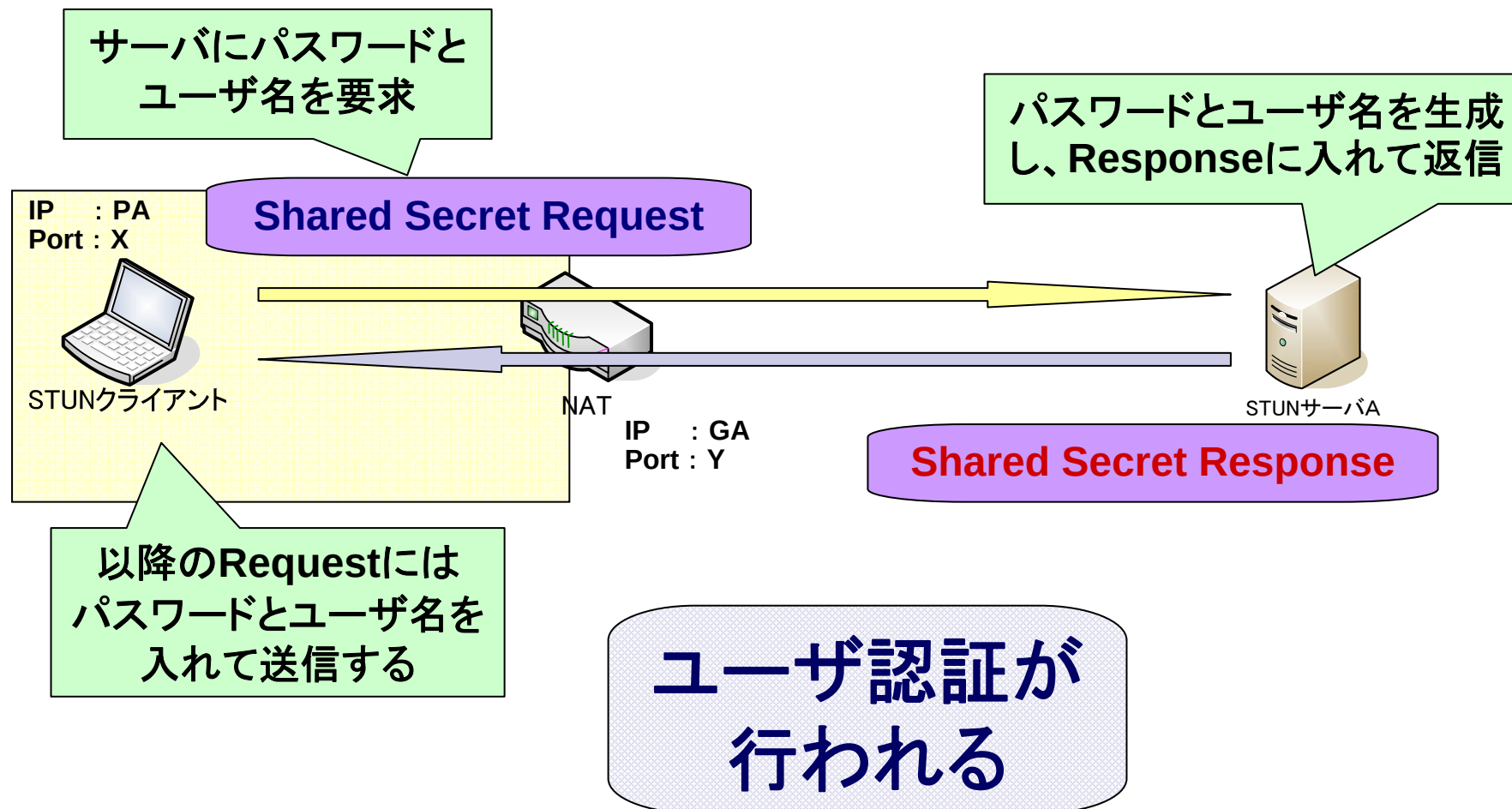
- Shared Secret Request

⇒ 一時的なパスワードとユーザ名を要求

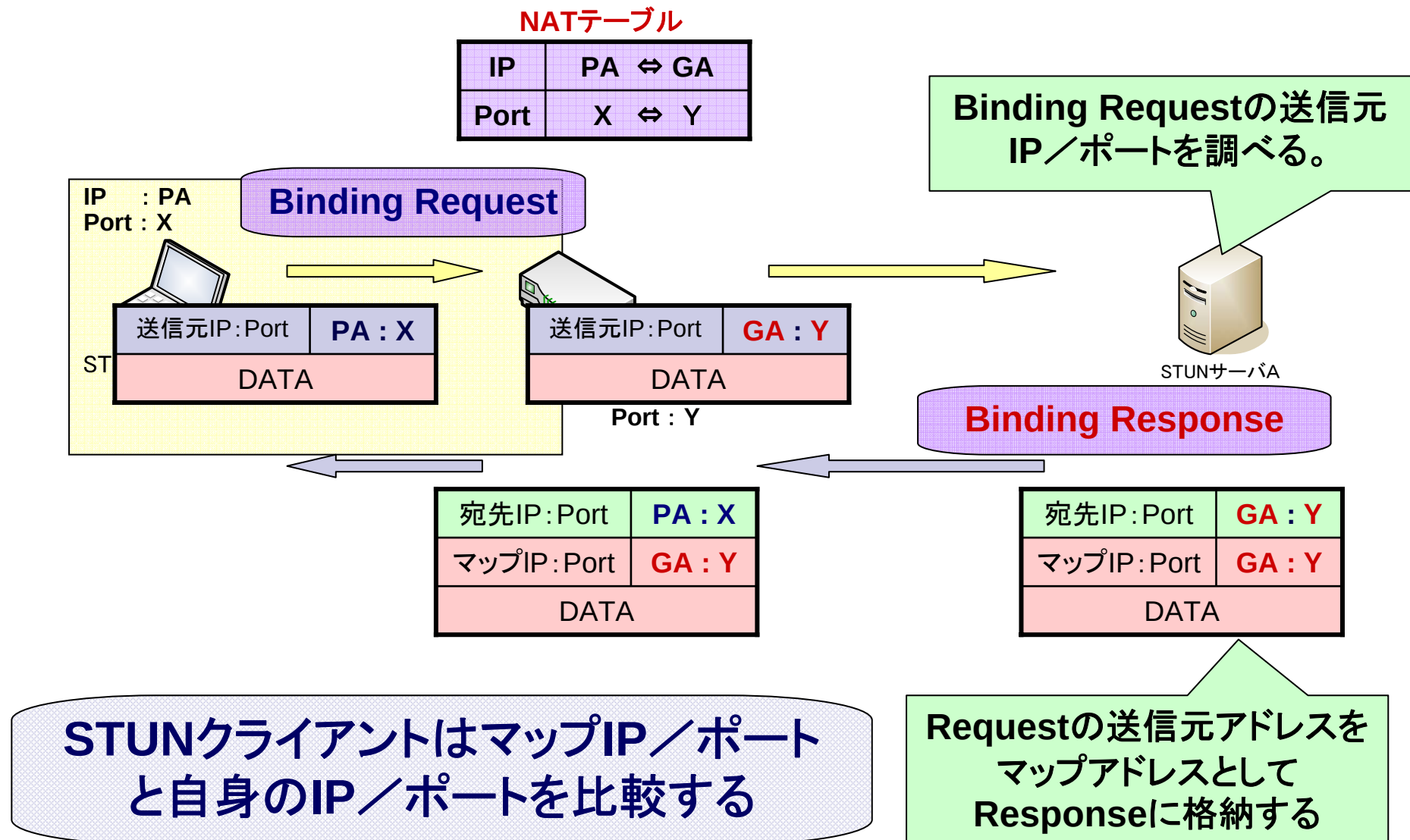
- Binding Request

⇒ NATの存在と種類、  
NATで割り当てられるIPアドレス／ポート  
番号を調べるのに使用

# STUNの動作－Shared Secret Request－

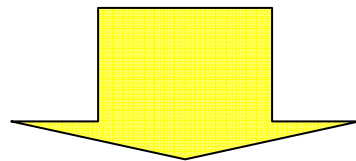


# STUNの動作－Binding Request－



# STUNの動作－NATの存在を判断－

IPアドレス／ポート番号  
が一致しない場合



クライアントは一つ以上の  
NATの配下にあると判断



STUNクライアント

IP : PA  
Port : X

Binding Response

|            |        |
|------------|--------|
| 宛先IP:Port  | PA : X |
| マップIP:Port | GA : Y |
| DATA       |        |

一致しない

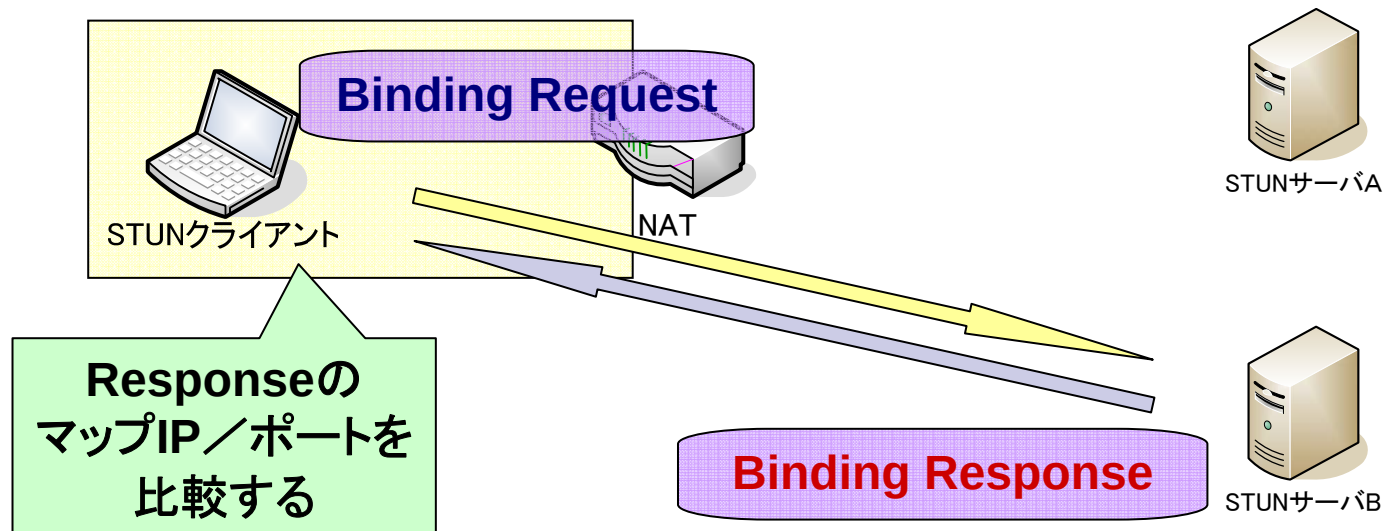
マップアドレスよりNATの外部アドレス  
が「GA : Y」であると分かる

どの種類のNATの配下にあるか判別するた  
めに、さらにBinding Requestを使用する。

# STUNの動作－NATタイプの判別－

## ■ Symmetricかどうか

- Binding Requestを異なるIP／ポートへ送信する
- Binding ResponseのマップIP／ポートを最初のマップアドレスと比較する





# STUNの動作－NATタイプの判別－

## ■ Symmetricかどうか

マップIP／ポートを比較

- ポート番号が一致しない

⇒ Symmetric であると判別

宛先ごとにNATの外部  
ポート番号が異なる

- ポート番号が一致する

⇒ 残り3タイプのいずれかである

# STUNの動作－NATタイプの判別－

## ■ 残り3タイプのどれか

次の要求をするフラグを持つBinding Requestを送信する

- 【同じサーバから、異なるポート番号で返信する】

⇒ RestrictedかPort Restrictedのどちらか判別

- 【Responseを異なるサーバから返信する】

⇒ Full Coneかどうか判別

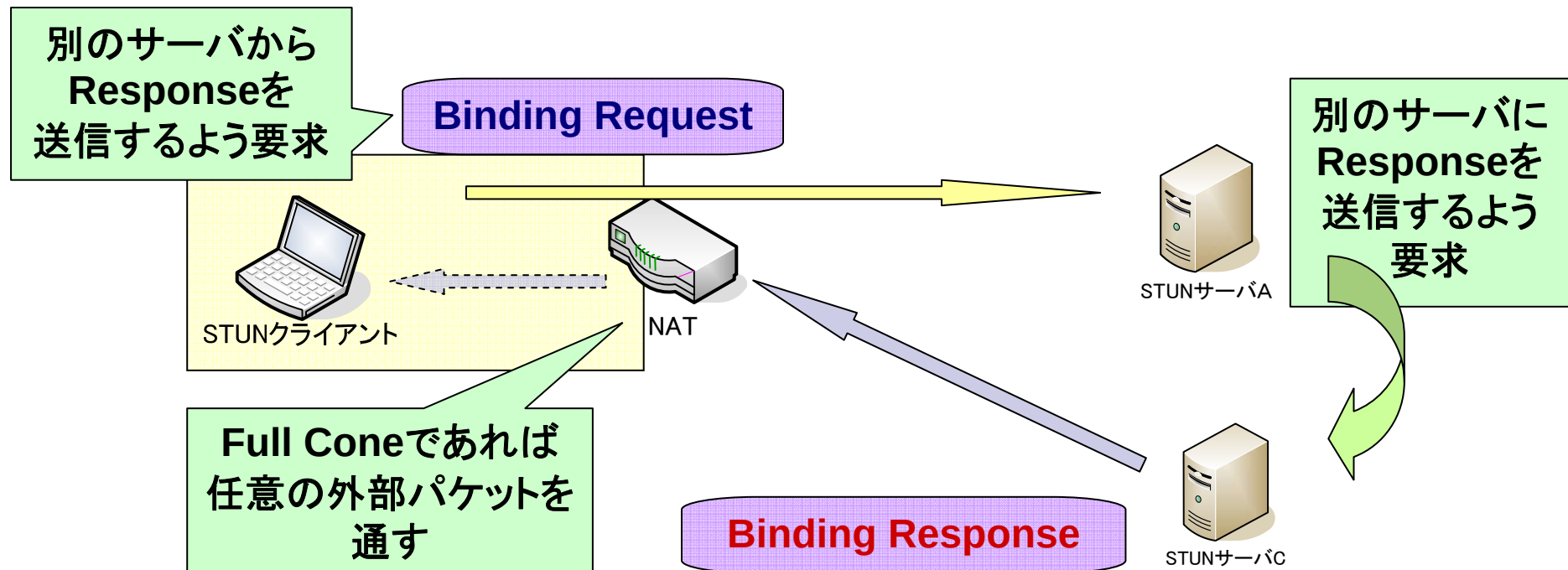
# STUNの動作－NATタイプの判別－

## ■ Full Coneかどうか

異なるサーバからのResponseを受信する



**Full Coneであると判別**



# STUNの動作－NATタイプの判別－

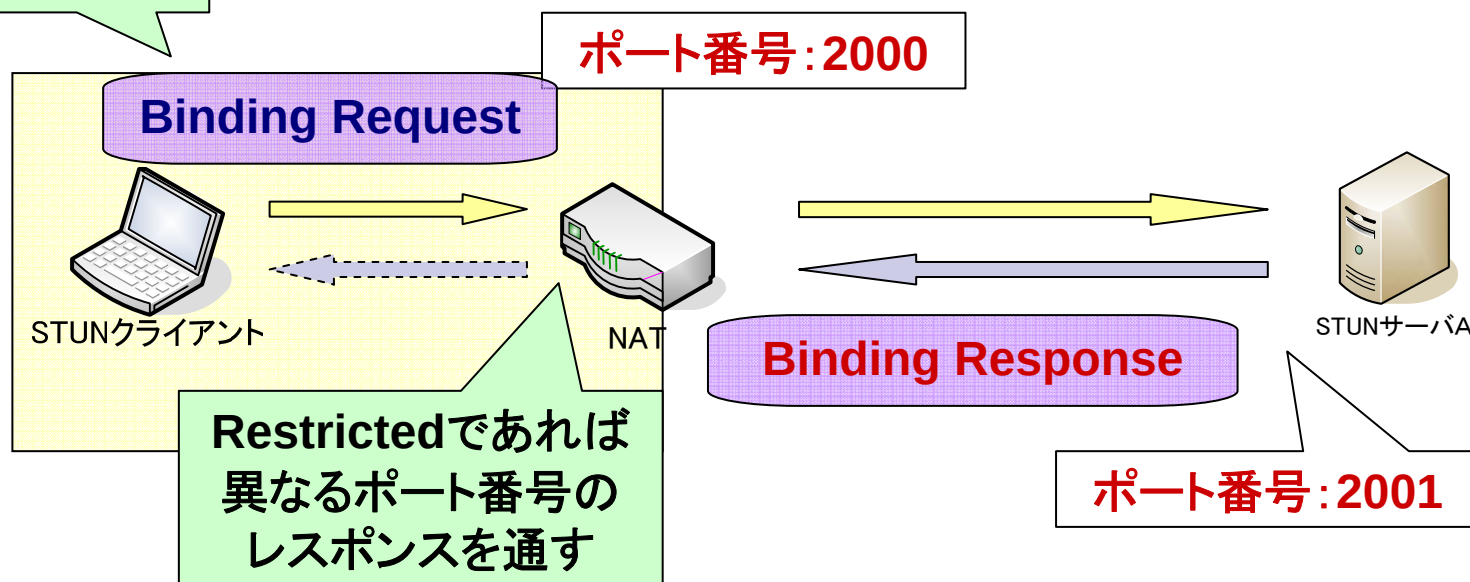
## ■ RestrictedかPort Restrictedか

同じサーバからの異なるポート番号のResponse

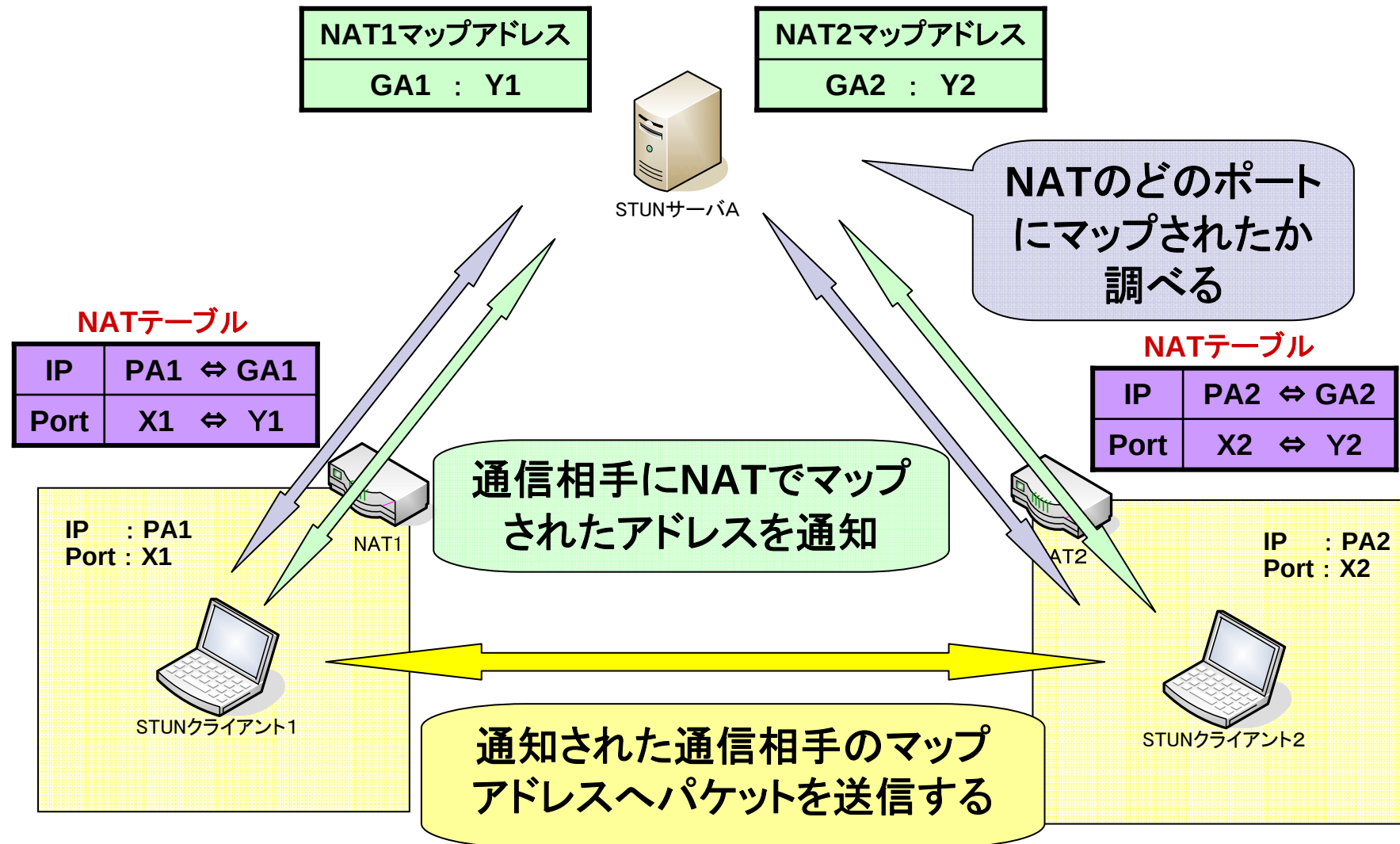
受信する ➡ Restricted Cone

受信しない ➡ Port Restricted Cone

異なるポート  
番号で返信  
するよう要求

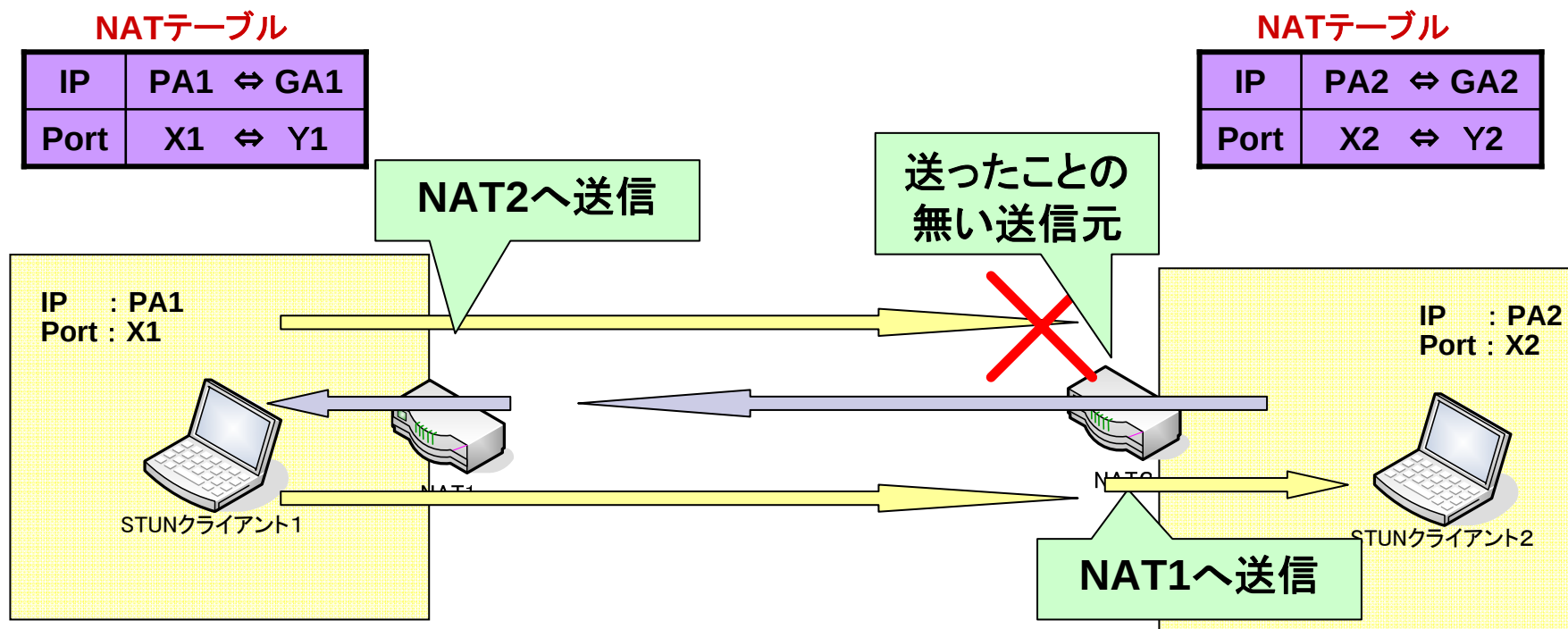


# STUNを利用したNAT越え



# Port Restricted Coneの場合

通信相手にNATでのマップアドレスを通知した後



異なるNAT内部の端末間で双方向にUDPパケットを投げ合う

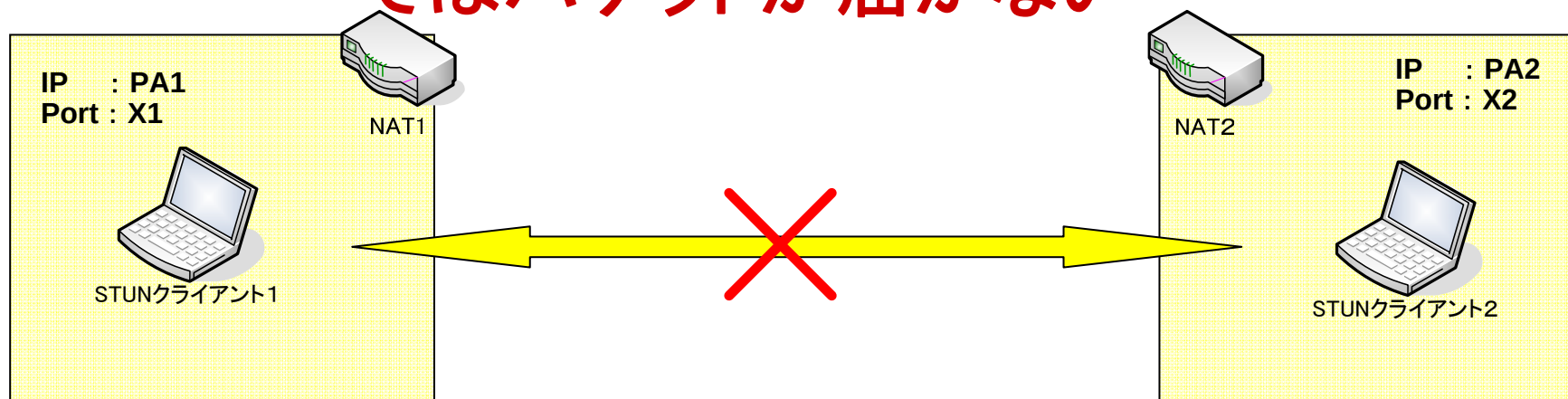
## UDP hole punching

# STUNの問題点

## ■ Symmetric NATに対するNAT越え

Symmetric NATが構成されている場合、宛先ごとにNATで割り当てられるポート番号が異なる

⇒ サーバから通知されたアドレスではパケットが届かない





## Symmetricを超える技術の検討

- 「Symmetric NAT Traversal using STUN」

<draft-takeda-symmetric-nat-traversal-00>

- 「TURN —Traversal Using Relay NAT—」

<draft-rosenberg-midcom-turn-03 >

- 「拡張STUN」

フラクタリストの開発キット「NAT Traversal SDK」に含まれるNAT越え技術





## まとめ –STUN–

### ■ UDPによるNAT越え技術

- Symmetric NATは超えられない
- 既存NAT以外では、超えることが困難な場合がある。

### ■ NATの存在と種類を判別

### ■ NATの外側のアドレスを知ることが出来る



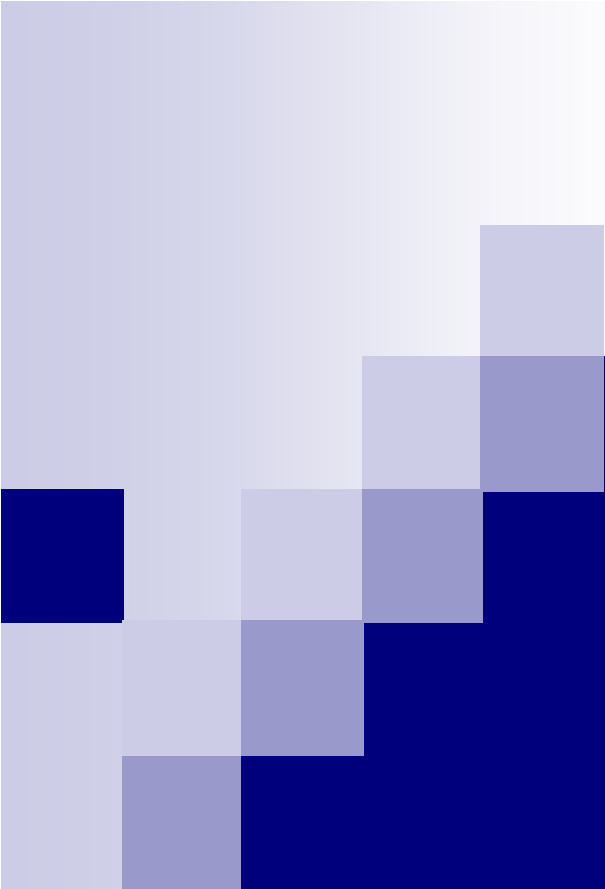
## 終わりに

STUNの問題はNATの処理の標準化と、規制の不足に関係がある.

この標準化の不足は、処理が想定できない、変更された、制御出来ない装置の激増をもたらした.

一番の解決方法は、このような対立する環境を減らすことである. そして、NAT処理の標準化や規制を導入することである.

しかし、それが実現されるまでSTUNはその対立する環境で最善を尽くし、短い時間でよい解決方法を与える.



# 終わり