本資料について

- 本資料は下記の論文を基にして作成されたものです．文章の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下さい．

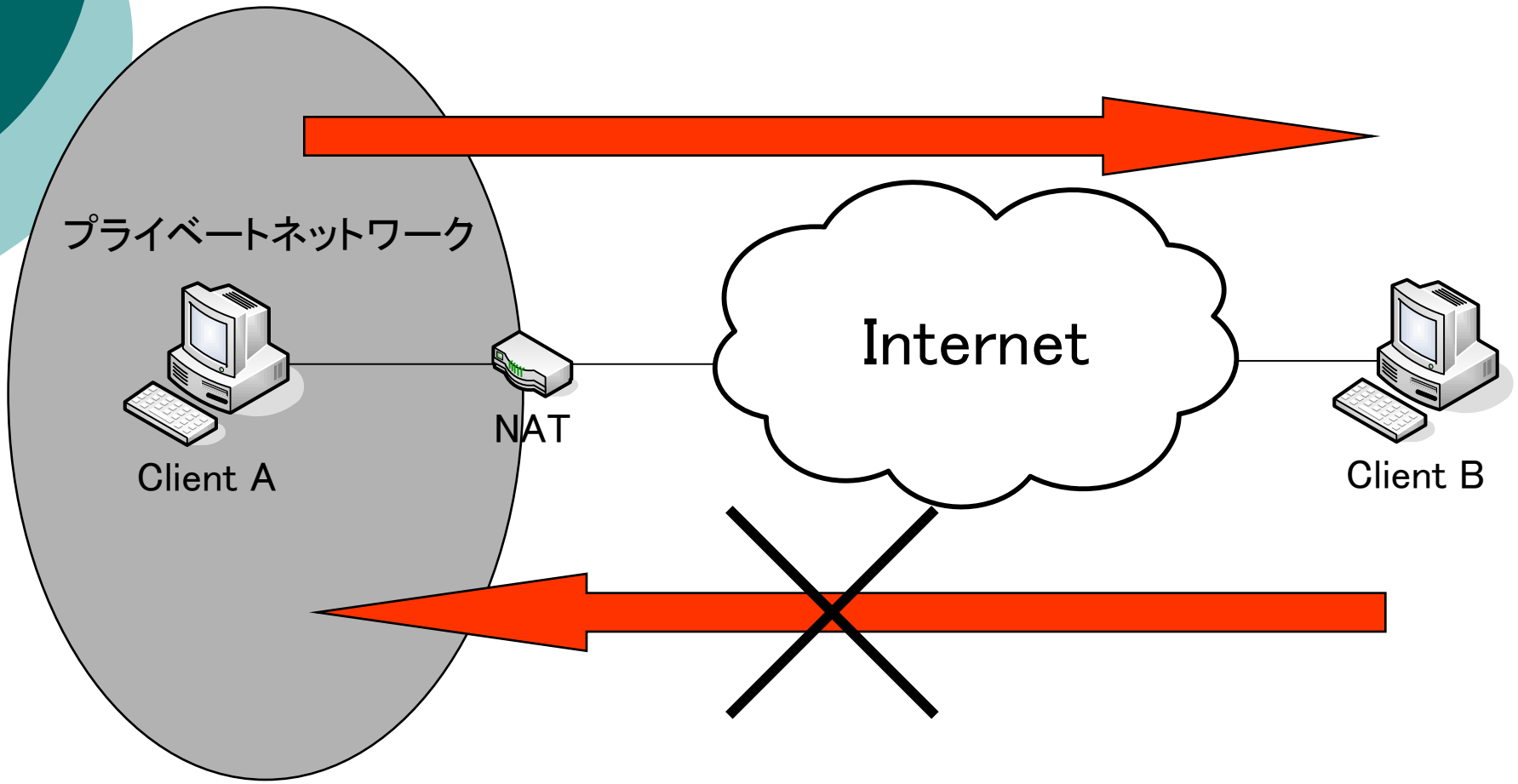
- Internet Draft :Peer-to-Peer Communication Across Network Address Translators
- Author：Bryan Ford, Pyda Srisuresh, Dan Kegel
- Document: draft-ford-midcom-p2p-03.txt
- Expires: December 12, 2004

第二回　輪講

Peer-to-Peer Communication Across Network Address Translators

030432106　渡邊研究室　　宮﨑　悠

NAT越え問題



Introduction

- 解決策

  本論文では、単純ではあるが、最も実用的なNAT横断技術として一般に知られている「***hole punching***」について分析する

Hole Punching

- NAT の内側にあるノードのポートに対してマッピングされるNAT の外側のポートが，アドレス変換ルールをNAT が保持している間は同じであるということを利用して，パケットをNAT の外側から内側へ通過させる．これを利用することで，異なるプライベートネットワーク内のノード間で直接的な通信が行える．

  しかし，適用できないタイプのNATも存在する．
- 通信プロトコルは，UDP でもTCP でも可能
  - UDP：82%
  - TCP：64%

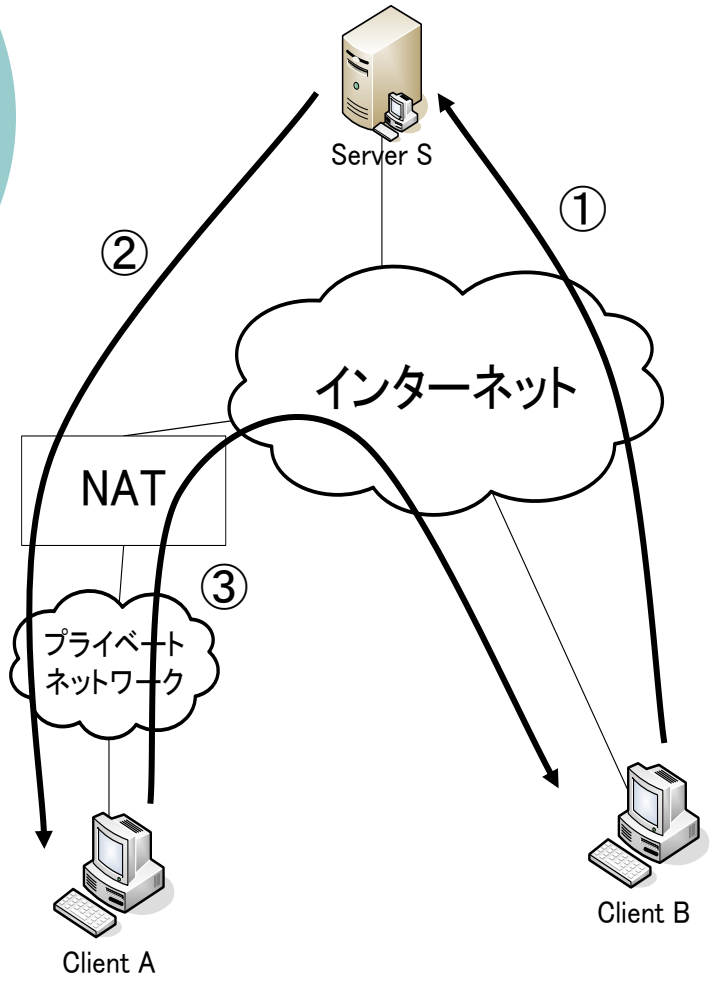
  のNATで適用可能
- UDP hole punchingはRFC3489で規定しているSTUN(Simple Traversal of UDP Through NATs)でも使われています

UDP Hole Punching

以下の二つの状況について考える

- AはNATによって区切られたプライベートネットワーク内、Bはグローバルネットワーク内にある場合
- AとBは異なるプライベートネットワーク内にある場合

UDP Hole Punching　パターン1



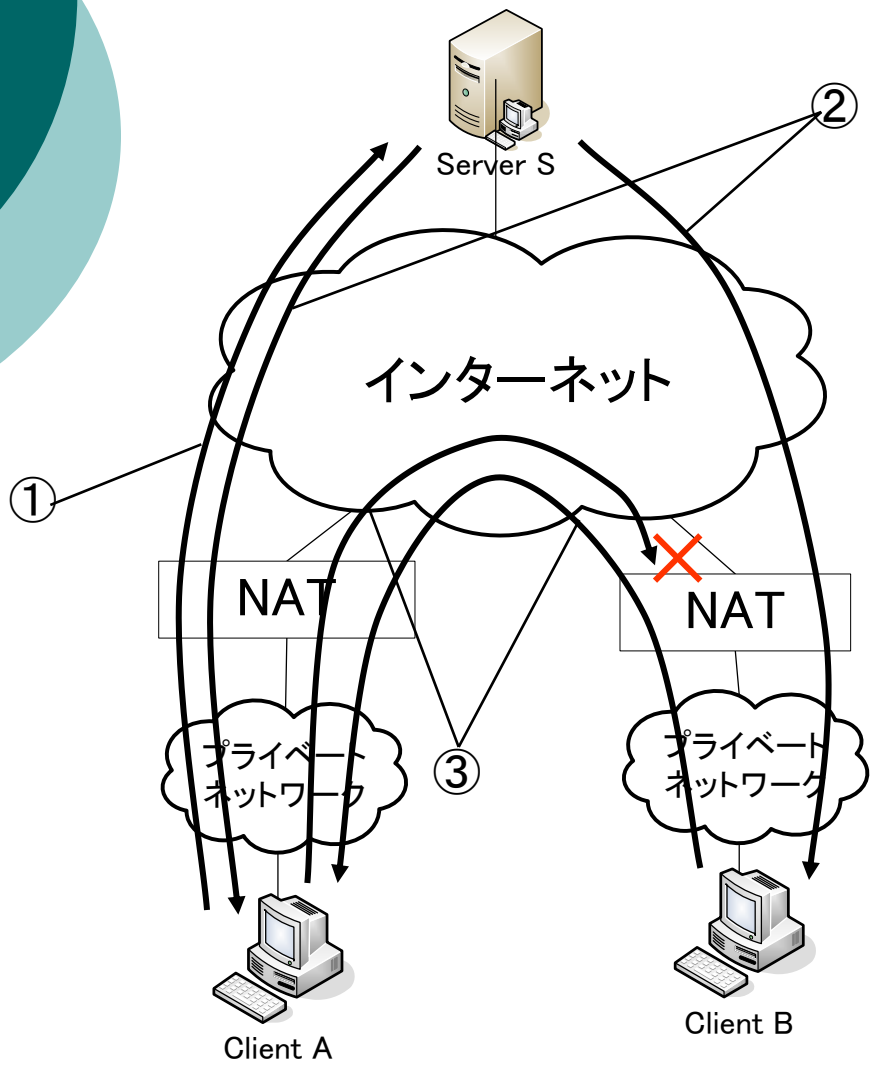
① AはSにBへの接続援助要求

② SはBのグローバル(IPアドレス・ポート番号)をAに教える

③ AはSからの情報を元に、BへUDP通信を開始し、Bはそれに応じることでAへのUDP通信を確立する

以後はNATは一度AからBへのパケットを通しているため、NATがアドレス情報を保持している間、相互に通信が可能

UDP Hole Punching　パターン2



※A、Bは予めSに情報を記録している

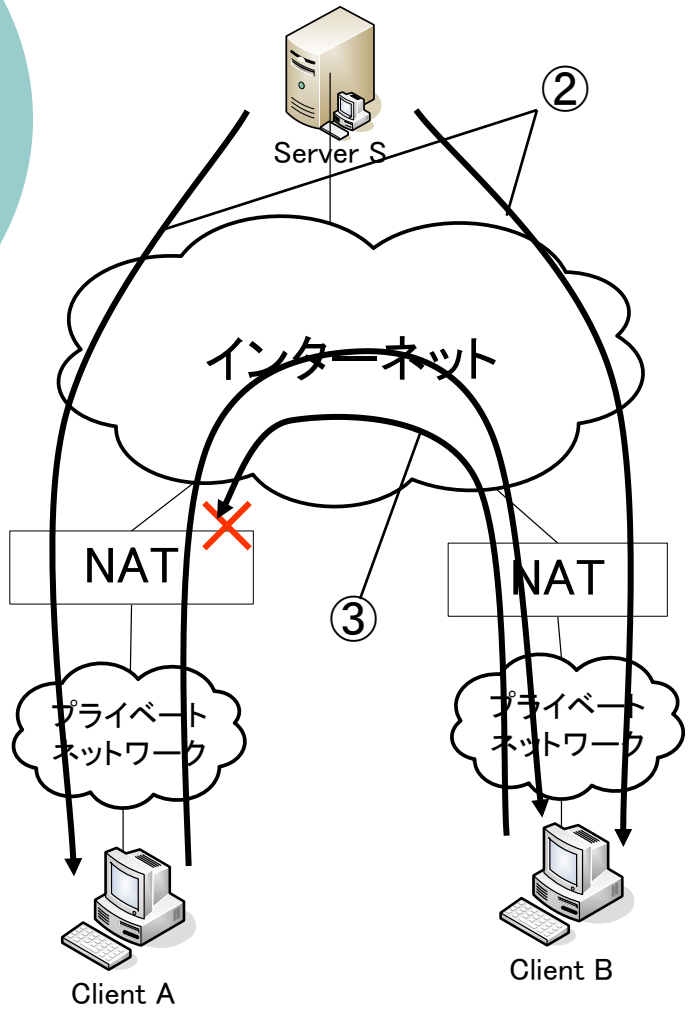
① AはSにBへの接続援助を要求

② SはAにBの情報をBにAの情報を送信する

③ AはBへ通信を開始し、BはAへの通信を開始する

※もし、AからBへの通信が、BからAへの通信がBのNATを通過する前に到着すると、AからBへの通信は破棄される。一度お互いに通信を通していれば、NATは以後、相互の通信を通す

TCP Hole Punching　接続方法概要



Client AとBはServer Sとすでに TCP接続があるとする

① AはBとの接続のためにSとのTCPセッションを使う

② SはAにBのグローバル・プライベート(IPアドレス・TCPポート)をBにAのグローバル・プライベート(IPアドレス・TCPポート)を送る

③ BはAに接続を試みる

※実際は失敗する

④ BはSとの接続を閉じて、そのローカルポートで接続要求を待つ

⑤ Sはそれを合図にAとの接続を絶ち、AにBへの接続をさせる

その後、AとBはUDPと同様に相互に通信できるようになる

Hole Punchingの必要条件

NATは一般的にアドレス・ポートペアのマッピングの作成と管理の方法の違いにより以下の4種類に分類される

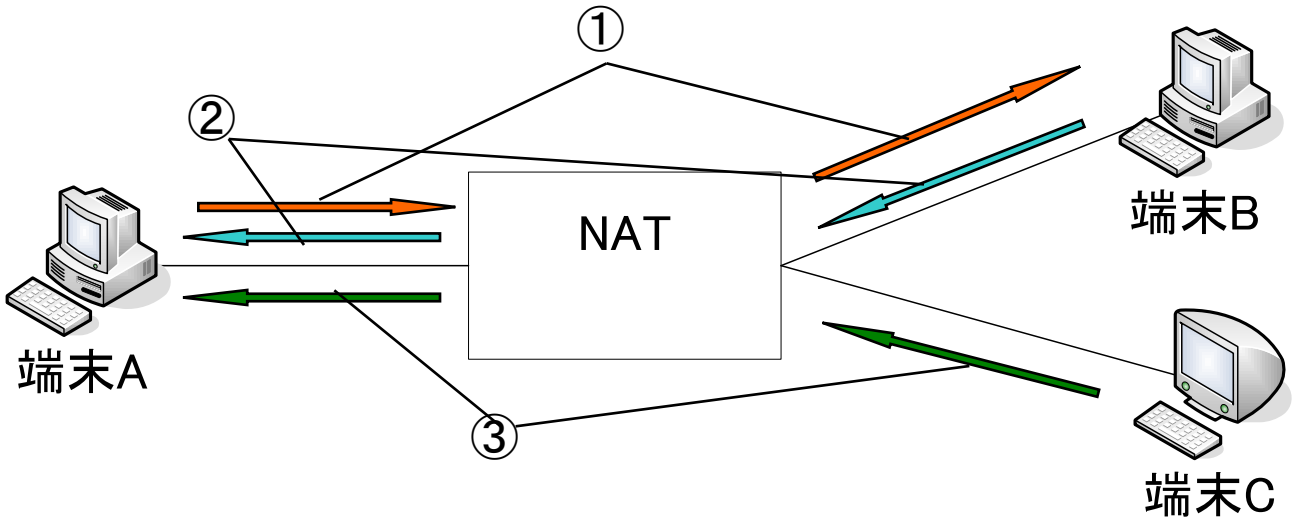
- Cone NAT
- Restricted cone NAT
- Port-restricted cone NAT
- Symmetric NAT

} **UDP Hole Punchingに対応**

Cone NAT

- 内部アドレスおよびUDPポートと外部アドレスおよびUDPポートのマッピングを作成し、ポートがアクティブである限り、マッピングを有効に保持する。
- マッピングが有効の間は、NATのWAN側アドレスの該当UDPポートにて受信されたUDPパケットはNAT内部の対応するホストへと転送される。

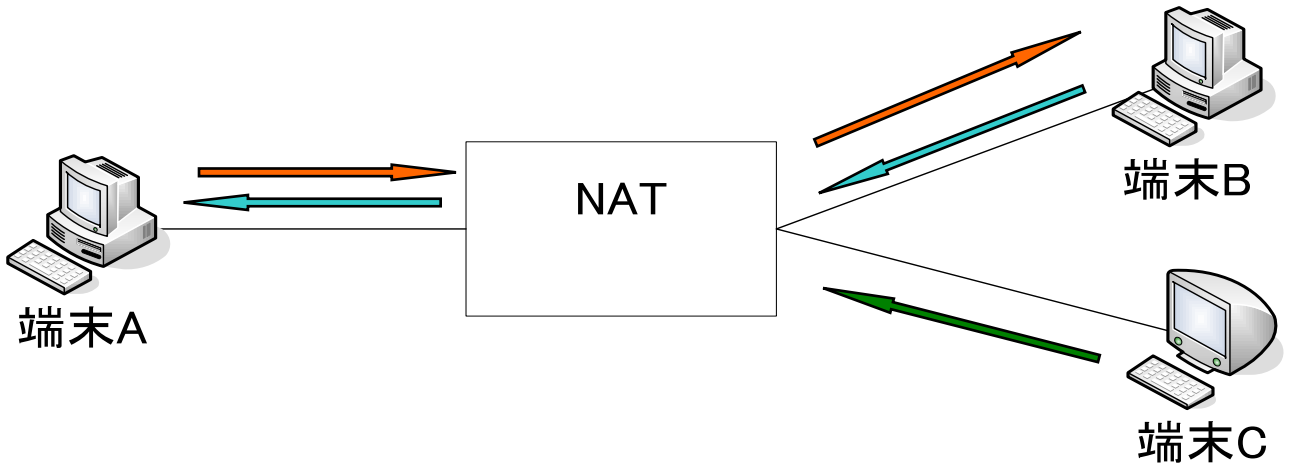
Cone NAT の動作



- 内部ホストAから送信された①のパケットによりマッピングテーブル中にエントリが作成される。
- Cone NATでは対象となる外部ホストの管理は行われないため、同一外部の端末Bからのパケット②だけでなく、異なる端末Cのパケット③もNATデバイスにより内部ホストAに転送される。

Restricted cone NAT

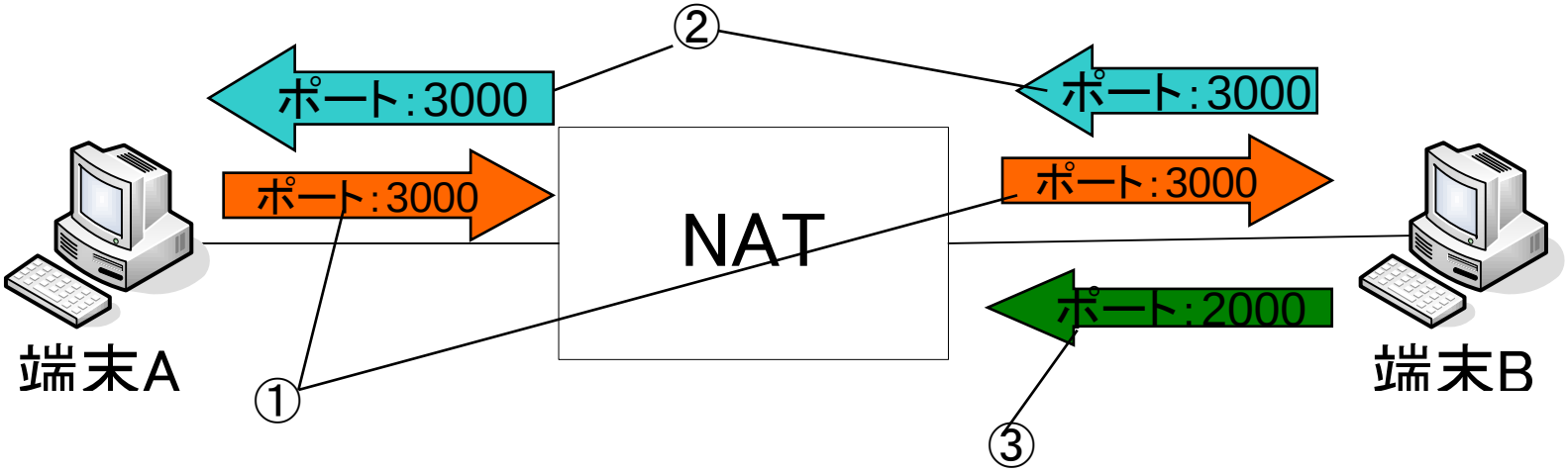
- 単にアドレスとUDPポートのマッピングを作成および維持するだけではなく、内部ホストからUDPパケットを送信した対象の外部ホストを管理している。
- これにより、内部ホストにより通信が開始された外部ホスト以外からのパケットの受信は拒否される。



Port-restricted cone NAT

- Port-restricted cone NATはRestricted cone NATによる外部からのパケットの受信の制限をさらに強化したNAT
- Restricted cone NATが承認された外部ホストだけを管理しているのに対し、Port-restricted cone NATは使用されているポートも管理対象とする。
- 外部からのパケットは内部ホストから通信が開始されたホストからであることとともに、そのときに利用されたポート宛であることが要求され、それ以外のパケットはすべて拒否される。

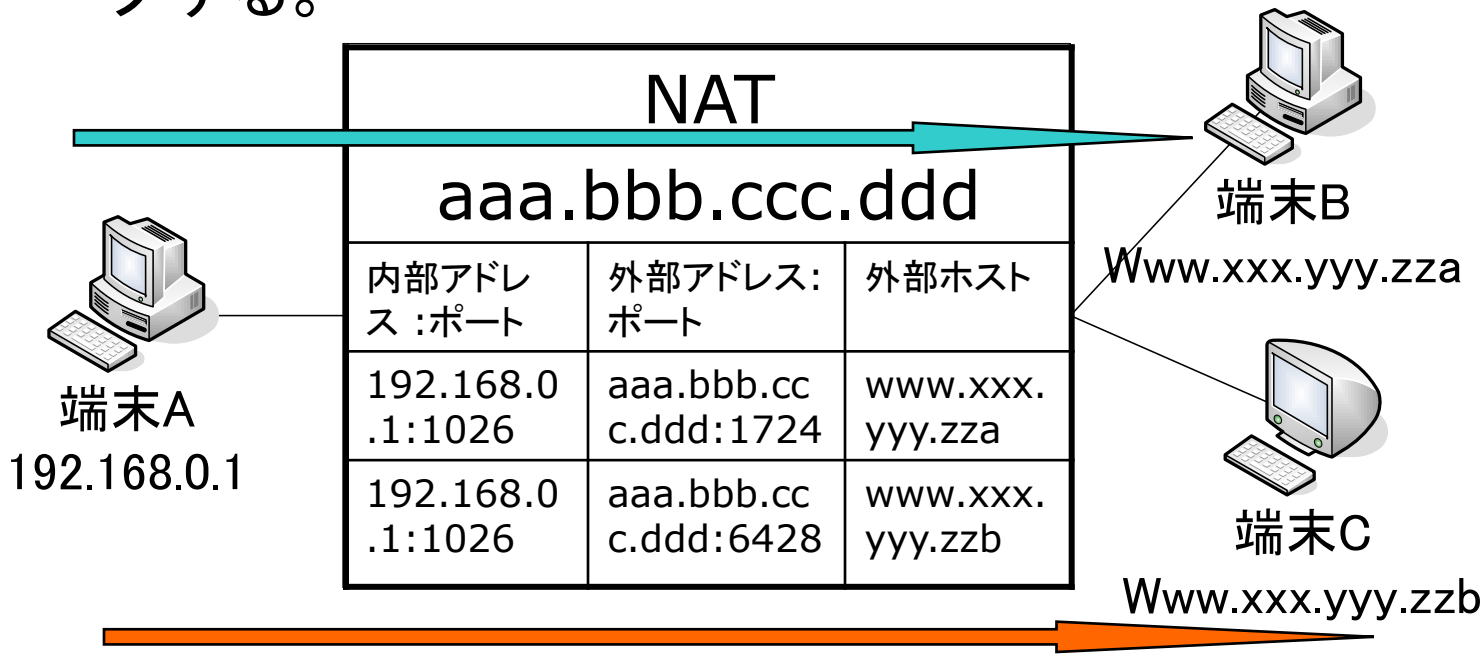
Port-restricted cone NAT の動作



パケット①と②の動作はRestricted cone NATと同様だが、たとえ同一のホストである外部ホスト端末Bあっても、異なるポートからのパケットである③はNAT内部に転送されない。

Symmetric NAT

- Symmetric NATは同一の内部アドレスとポートのペアを異なる外部アドレスとポートのペアにマッピングする。



※symmetric NATでは、内部ポートと外部ポートが違うため、hole punchingを対応させることができない。

最後に

- Hole punchingは、NATのある環境でP2P接続を確立する多目的技術である
  - STUNやICE、Teredoにも応用されている
- 関係するNATが条件を満たす限り、hole punchingはTCP通信とUDP通信に大いに役立つ
- 特定のネットワークトポロジー情報なしで、普通のアプリケーションで実行できる

END

補足：クライアントサーバシステム

クライアントの命令に対して、サーバが結果を返す

- 長所
  - クライアントの処理が小さくて済む
  - システムの中央管理及び監視，特に著作権処理やログイン処理がしやすい
  - データーの更新が比較的楽
  - サーバーに処理が集中できるため、ビジネスモデルが比較的簡単に作れ，お金を儲けやすい
- 短所
  - サーバーに非常に重い処理が必要で、時に高価なコンピューターを多数揃える必要がある
  - サーバーに処理が集中するため，サーバーに繋がるための回線帯域を圧迫する恐れがあり，より大容量の回線が必要となる。

補足：P2P通信

P2Pではすべてのコンピューターの立場が等しく，コンピューターはある時にはサーバー，ある時にはクライアントと立場を変化させることが可能

- 長所
  - 処理がお互いに分散できるために，個々のコンピューターの性能や回線の容量がそれほど要求されない。
  - 処理を比較的秘密裏でおこなえる。隠匿性が高い
- 短所
  - 処理が分散するために管理や監視がしにくい
  - お金を取るビジネスモデルをつくりにくい