# NATによる
# 準マルチホーム化技法

梶田将司　　結縁祥治

名古屋大学
情報メディア教育センター

# マルチホームの一般化

- マルチホーム化
  ホスト/ネットワークを複数の接続点によって
  インターネット接続すること
  - 目的
    - 信頼性の向上
    - 負荷分散
- 最近のインターネット接続の多様化により
  マルチホーム化の要求は高まりつつある

# 様々なマルチホーム化手法［1999，JANOG5山口］

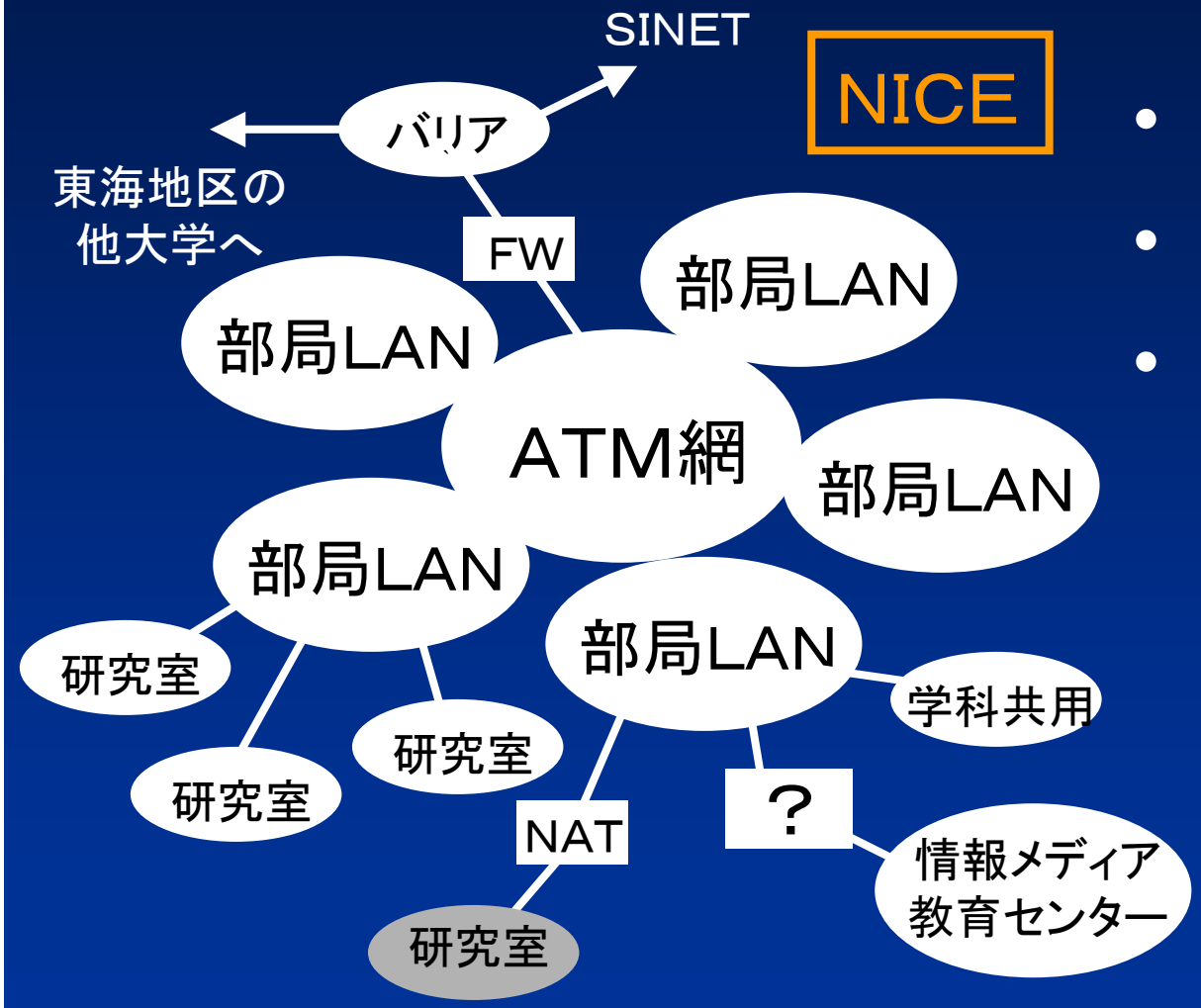
- アドレス空間（Provider Aggrigatable or Provider Independent），技術力，運用コスト，運用ポリシーにより様々
- IPレベル
  - 経路制御：BGP，Private BGP，IGP
  - Cisco Balance，Firewall，NAT…
- アプリケーションレベル
  - Mail，Web，FTP…
  - Proxy（delegatedなど）

# 発表内容

名古屋大学情報メディア教育センターでの
NATによる複数接続手法（IPレベル）

- 背景
- 問題点
- 解決策
- 運用状況
- まとめ

# 名古屋大学のネットワーク事情

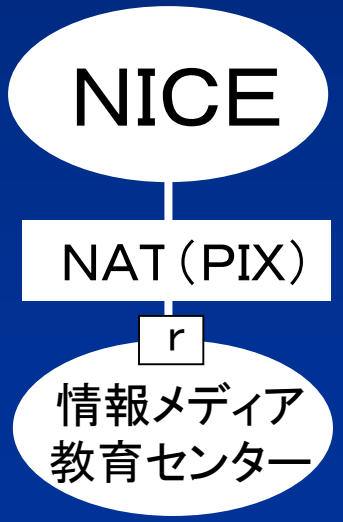



- シングルホーム
- 研究用ネットワーク
- Firewall
  （フィルタリングのみ）

約800台からなる
センターネットワー
クをどうつなぐか？

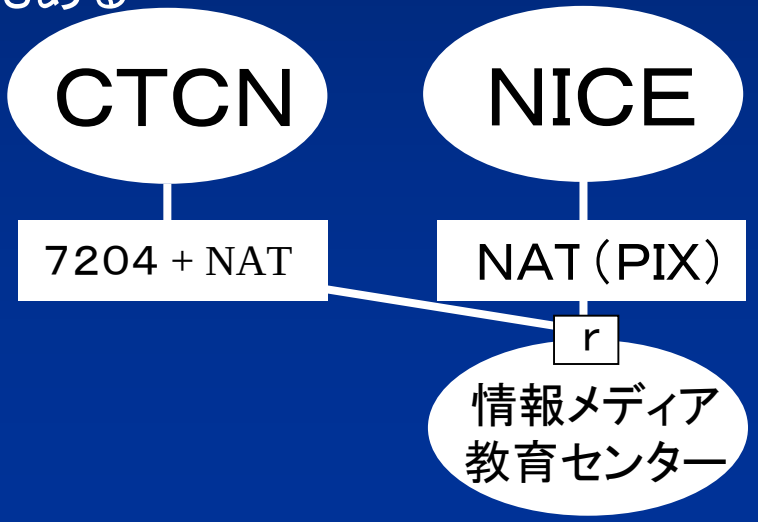
# 当初の接続ポリシー

- 教育用システム
  → 内部から外部はできるだけ透過にしたい
- 約800台の端末群（UNIX，WindowsNT）
  → Firewall により外部からの不要な通信は遮断し，限られたホストへのみ外部からのアクセスを許可
- 割り当てられたIPが約500
  → プライベートアドレス
- 学内からのアクセスが多い
  → 高速なアドレス変換



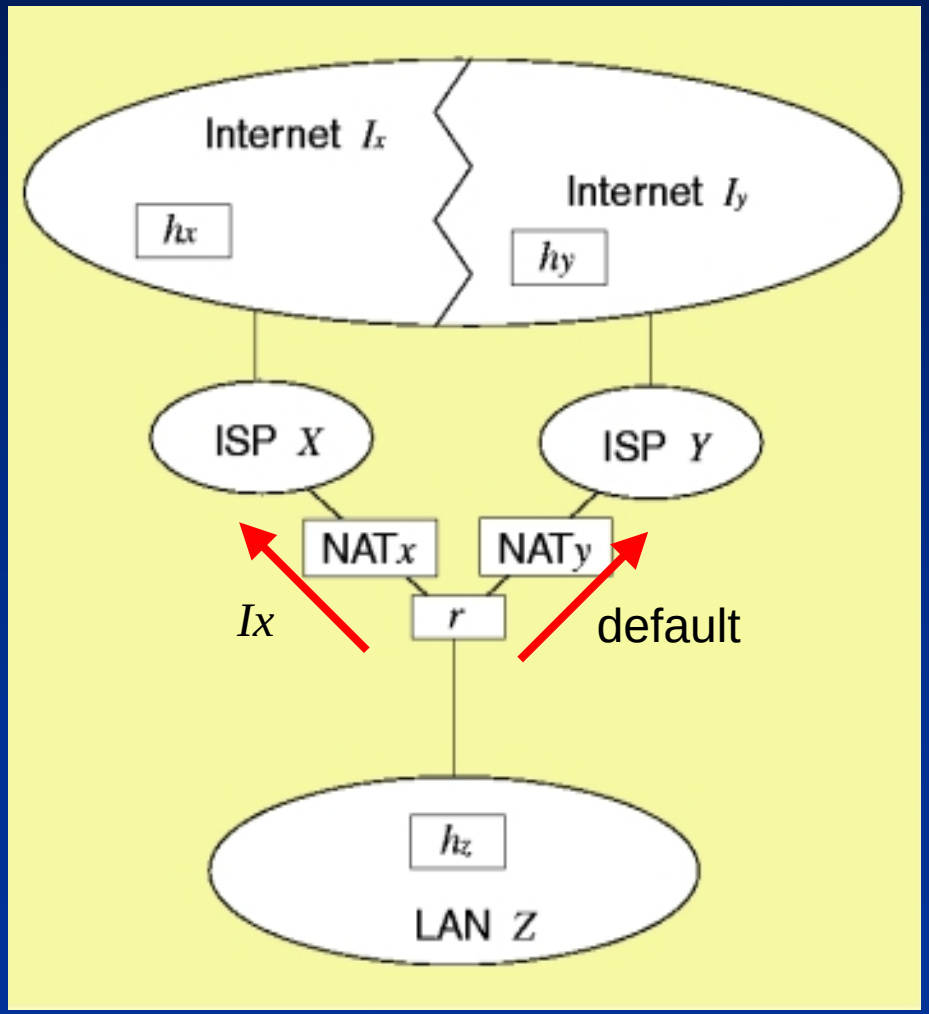
# 突然の複数接続化

- 年度末の特別予算により具体化
- 目的：講義における対外接続の信頼性・帯域確保
  - つながらないのは許されない
  - 集中したアクセスが発生
    →研究用ネットワークへの負荷大
  - あらかじめ接続先が既知の場合もある
    →独自のルーティングポリシー
- AS取得は不可能
  ← AS申請は大学レベルの話



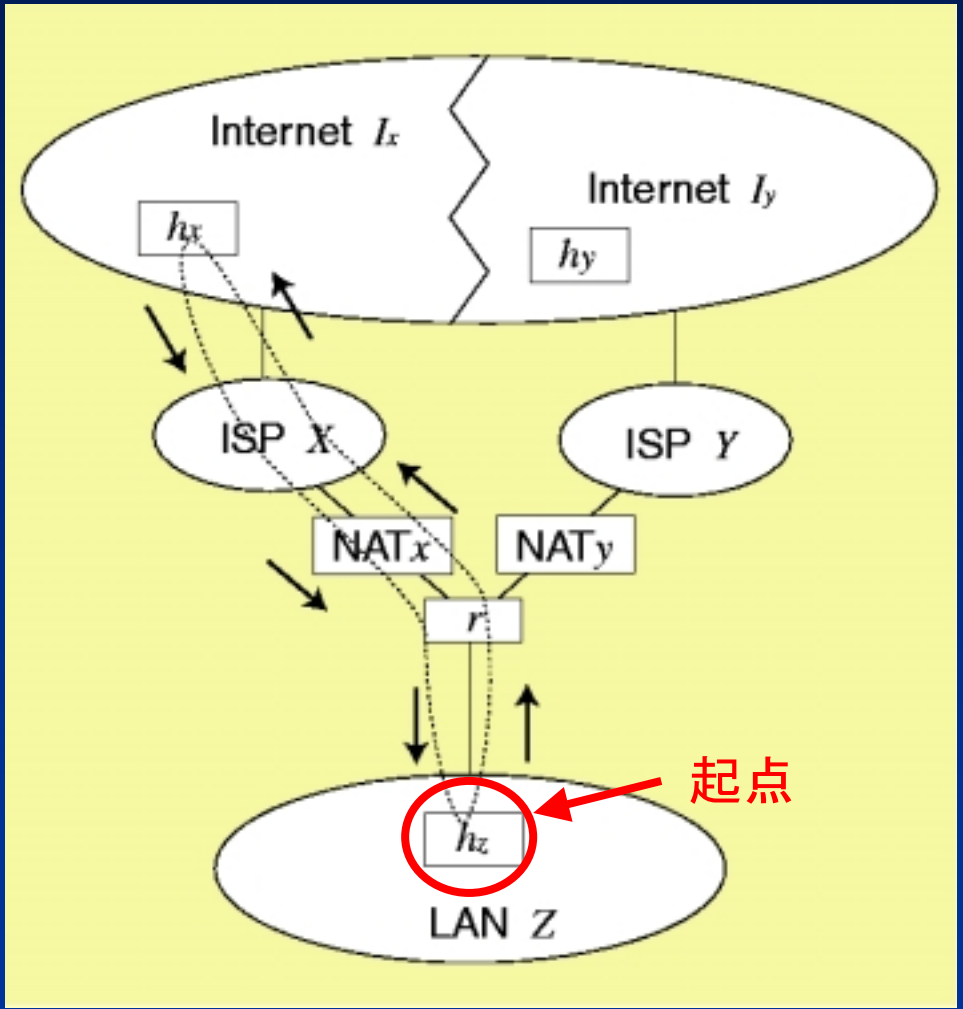

NAT機能付きCISCO7204を
用いてコスト最小で複数接続化

# NATを用いた複数接続の問題点




- ISP X，ISP Yに接続
- LAN Z：基幹に属さない任意のネットワーク
（例）研究室，部門，研究所，事業所，会社，家庭…
- ルータ $r$ はパケットの宛先に応じて適切にルーティングを行う
- NAT$x$，NAT$y$ではそれぞれISP X，ISP Yのアドレスにstaticに変換
- NAT$x$，NAT$y$では外部からの接続がないホストに対しては動的にアドレスを割り当てる

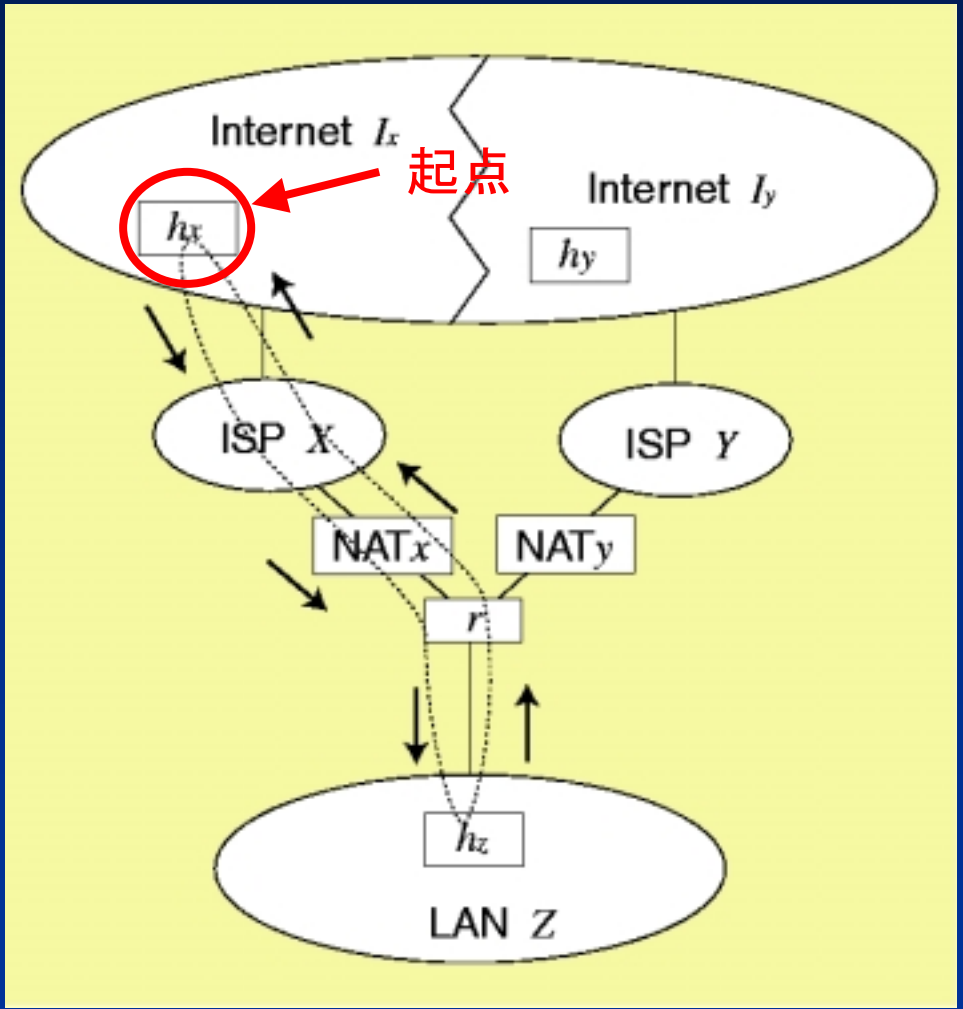
# 内部ホストからの通信




$h_z$ が起点となる場合

問題なし

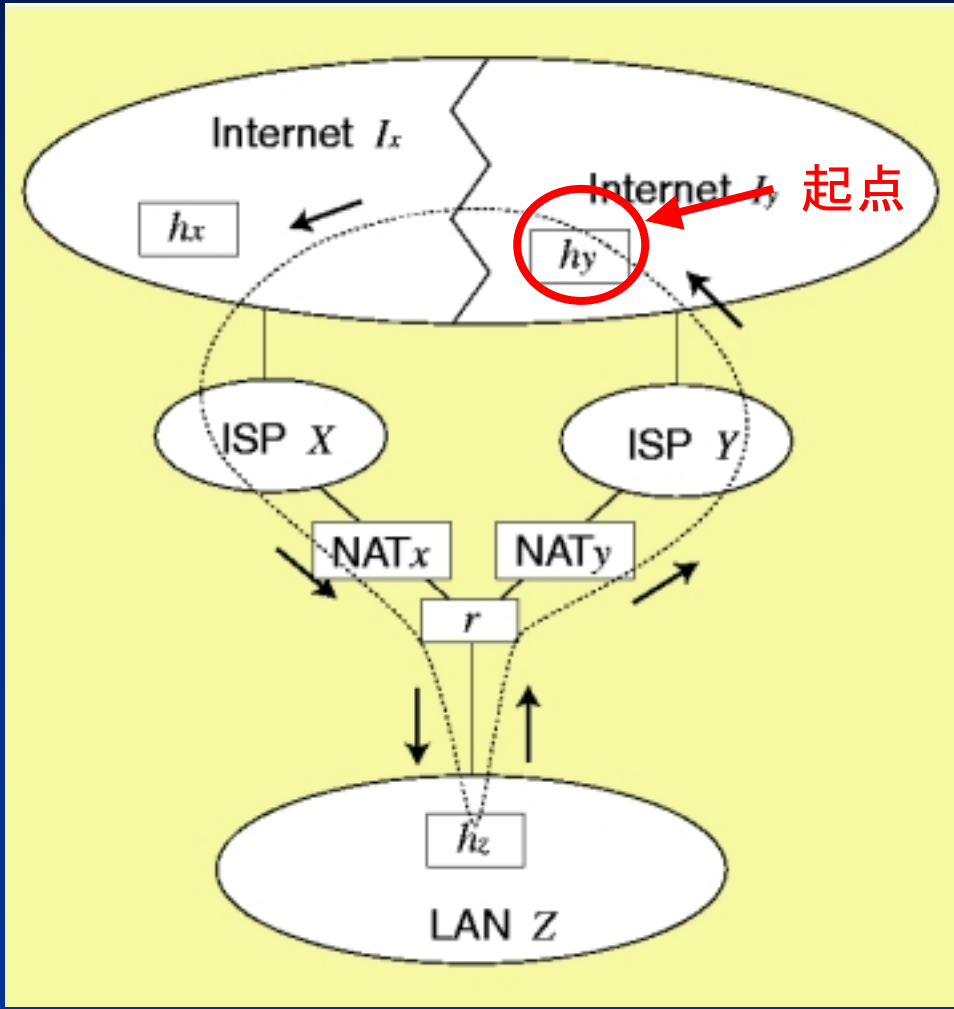
# 外部ホストからの通信（1）




$h_x$ が起点となる場合

問題なし

# 外部ホストからの通信（2）




$h_y$ が起点となる場合

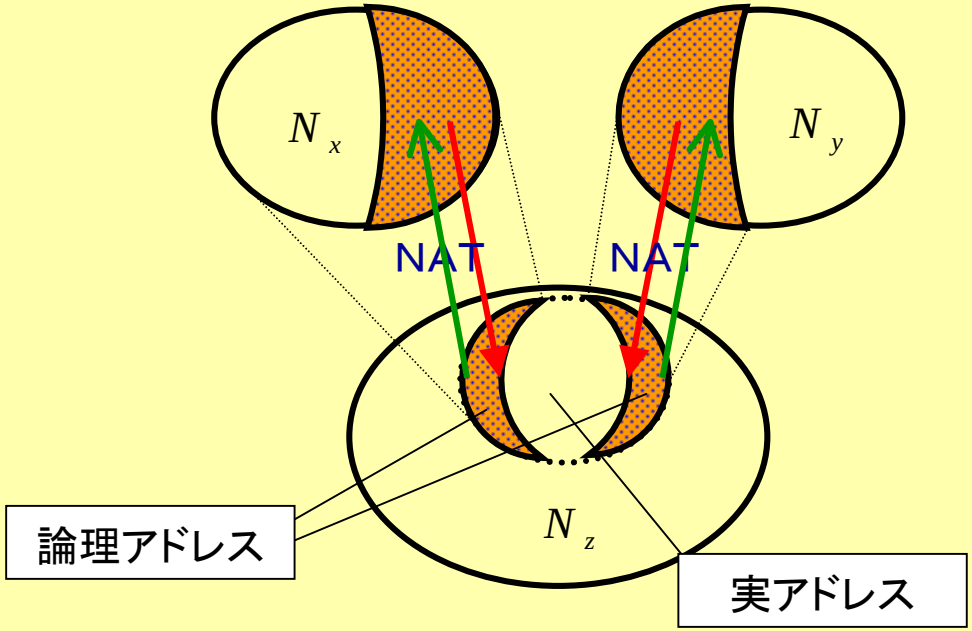
- 非対称経路
- 送信先とは異なるアドレスから，戻ってくる

どちらでNATされたか分からなくなってしまう

IPパケットにどちらから入ってきたかが分かる情報を付加してやればよい

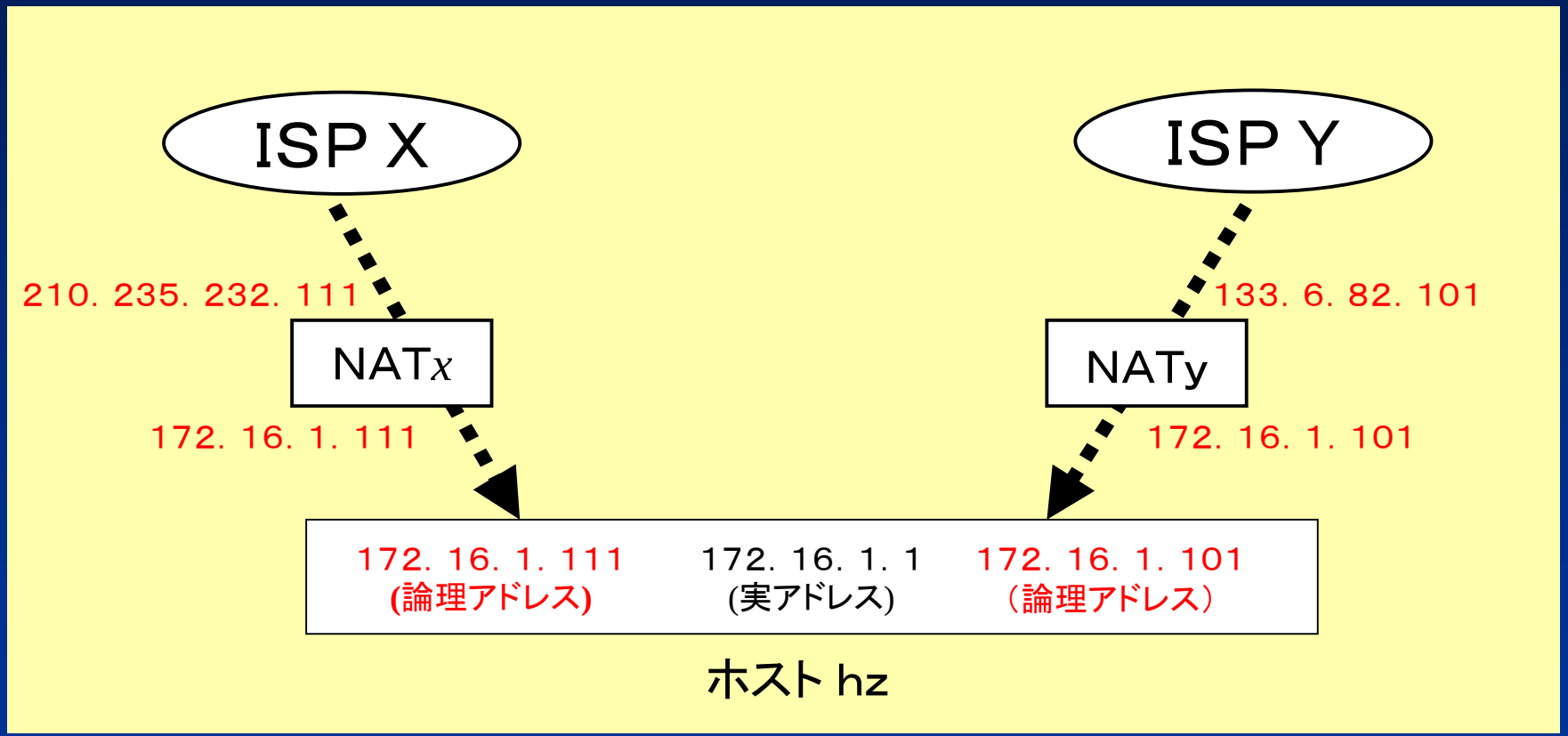
# 論理IPアドレス＆ポリシールーティング

- 外部が起点の場合の参照アドレスを経路ごとに変える
- 復路については経路を選択しなければならない
→ポリシールーティング

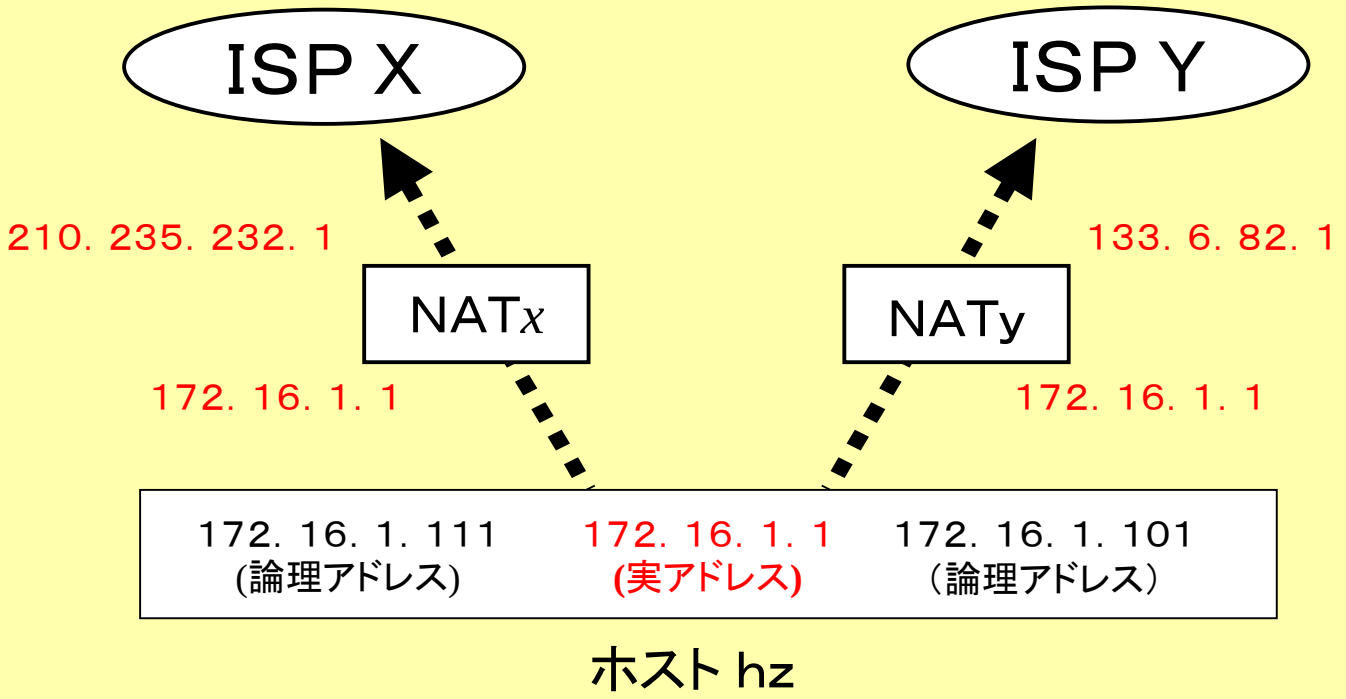



外部が起点の場合の通信

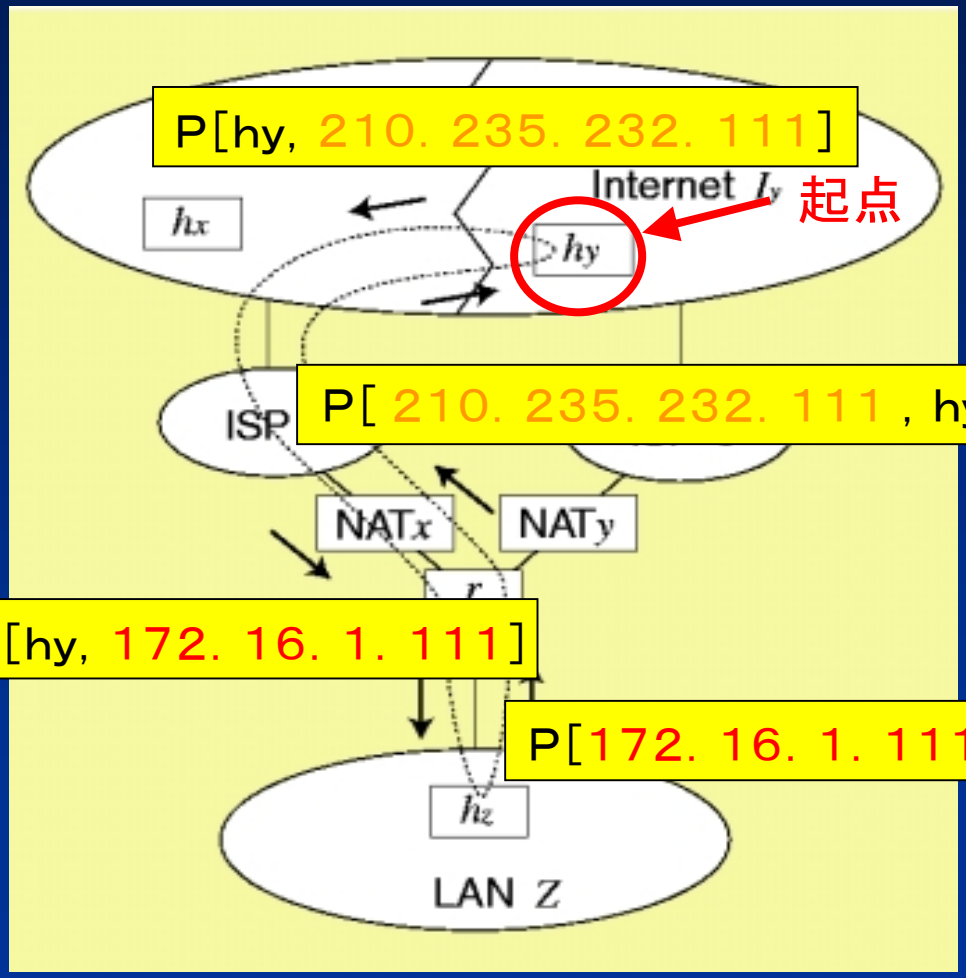
# アドレス変換の具体例（外部が起点）



# アドレス変換の具体例（内部が起点）



# 外部ホストからの通信(2)の改善結果



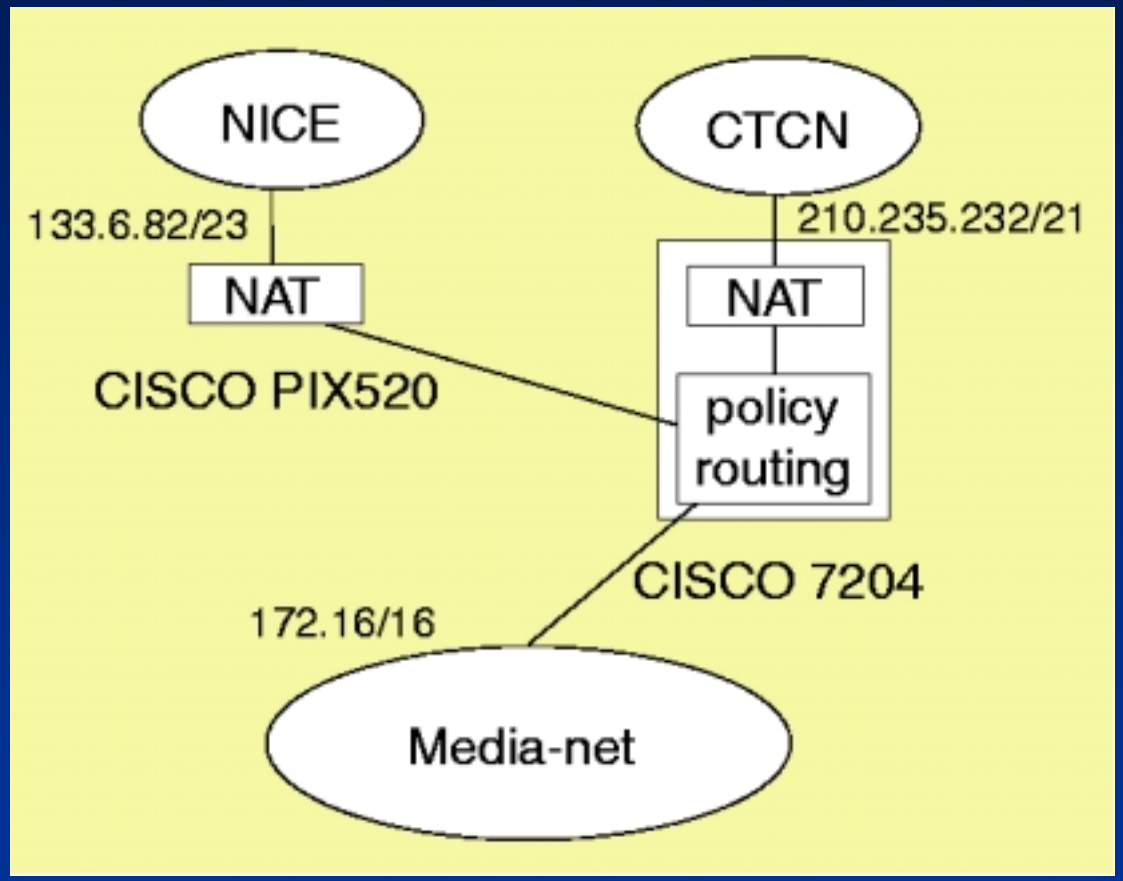

- ホストhz のアドレス
  実アドレス:
  172.16.1.1
  ISP X用論理アドレス:
  172.16.1.111
  ISP Y用論理アドレス:
  172.16.1.101
- NATx でのアドレス変換
  172.16.1.111
  ⇔ 210.235.232.111
- NAT y でのアドレス変換
  172.16.1.101⇔133.6.82.1

P[x, y]:ソースアドレスがx, デスティネーションアドレスがyのIPパケット

# 本手法の特徴

- 自ネットワークの経路情報を外部に複数アナウンスすることなく複数接続化
  →外部からの到達可能性を一部犠牲（準マルチホーム化）
- PI or PAに依存しない
- IPレベルのマルチホーム化
  →NATを使用するので，アプリケーションは限定される
  （教育システムとしては特に問題なし）
- 中継は不可
  →基幹部分に属さないネットワークのみに適用可能
- 既存技術＆装置により可能

# 本センターでの実現


NICE
CTCN
133.6.82/23
210.235.232/21
NAT
NAT
CISCO PIX520
policy
routing
CISCO 7204
172.16/16
Media-net

# 運用状況
# （外部を起点とする通信）

| ホスト名 | 用途 | 内部→外部 | 外部→内部 | |
|---|---|---|---|---|
| | | | NICE 経由時 | CTCN 経由時 |
| sv001 | DNS サーバ | 172.16.1.1 | 172.16.1.101 | 172.16.1.111 |
| sv003 | ニュースサーバ | 172.16.1.3 | 172.16.1.103 | 172.16.1.113 |
| sv005 | メールサーバ | 172.16.1.5 | 172.16.1.105 | 172.16.1.115 |
| sv006 | telnet・ftp サーバ | 172.16.1.6 | 172.16.1.106 | 172.16.1.116 |
| sv007 | telnet・ftp サーバ | 172.16.1.7 | 172.16.1.107 | 172.16.1.117 |
| sv009 | WWW サーバ | 172.16.1.9 | 172.16.1.109 | 172.16.1.119 |

| 用途 | ホスト名 | 負荷分散方法 |
|---|---|---|
| DNS サーバ | sv001 | NICE 側からの経路と CTCN 側からの経路双方を NS レコードに登録. |
| メールサーバ | sv005 | NICE 側からの経路を優先度 10 で，CTCN 側からの経路を優先度 20 で MX レコードに登録. |
| telnet・ftp サーバ | sv006, sv007 | NICE 側からの経路のみ．sv006, sv007 を DNS ラウンドロビンにより選択. |
| WWW サーバ | sv009 | NICE 側からの経路のみ. |

# 運用状況
# （外部を起点とする通信）

内部から外部へのアクセスがNICE経由となるホストからのアクセス

| ホスト名 | NICE 経由 | | CTCN 経由 | |
|---|---|---|---|---|
| | セッション数 | 割合 | セッション数 | 割合 |
| sv001 | 17248 | 5.34% | 15878 | 4.92% |
| sv003 | 26489 | 8.20% | 3 | 0.00% |
| sv005 | 210988 | 65.32% | 1532 | 0.47% |
| sv006 | 11865 | 3.67% | 57 | 0.02% |
| sv007 | 14105 | 4.37% | 88 | 0.03% |
| sv009 | 24723 | 7.65% | 19 | 0.01% |
| 小計 | 305418 | 94.56% | 17577 | 5.44 % |

内部から外部へのアクセスがCTCN経由となるホストからのアクセス

| ホスト名 | NICE 経由 | | CTCN 経由 | |
|---|---|---|---|---|
| | セッション数 | 割合 | セッション数 | 割合 |
| sv001 | 41610 | 7.43% | 388938 | 69.42% |
| sv003 | 266 | 0.05% | 14987 | 2.68% |
| sv005 | 66464 | 11.86% | 1562 | 0.28% |
| sv006 | 1809 | 0.32% | 0 | 0.00% |
| sv007 | 865 | 0.15% | 0 | 0.00% |
| sv009 | 43734 | 7.81% | 0 | 0.00% |
| 小計 | 154748 | 27.62% | 405486 | 72.38% |

非対称経路問題が本技法により解決された割合

# 内部を起点とした通信の負荷分散

- デフォルトはNICE側（SINET）
  - Static に設定
- CTCNからPravate BGP により国内フルルートを取得し，学術系をフィルタアウト

国内非学術系はCTCN経由，国内学術系及び海外はSINET経由

# まとめ

- NATを用いたマルチホーム化の一手法
  論理IPアドレスとポリシールーティングの併用による
  非対称経路，応答アドレス問題の対応
- 名古屋大学情報メディア教育センターでの
  運用状況

教育用システムとしては目的は達成

# 今後の課題
## ～障害時の対応～

- CTCN側回線断
  - 内部が起点の通信
    BGPダウンによりすべてがNICE（SINET）経由
  - 外部が起点の通信
    NICE経由のみ，明示的にNICE側ルートを指定
- NICE側回線断
  - 内部が起点の通信
    デフォルトをCTCN側にマニュアルで変更
    →回線断時の自動的な切り替え
  - 外部が起点の通信
    CTCN経由のみ，明示的にCTCN側ルートを指定