# 端末の改造が不要な NAT 越え方式の提案

宮﨑　悠*，鈴木　秀和，渡邊　晃(名城大学)

A proposal of NAT-Traversal that does not force terminals to modify

Yutaka Miyazaki, Hidekazu Suzuki, Akira Watanabe (Meijo University)

## １．はじめに

いつでもどこからでもネットワークにアクセスすることができるユビキタス社会の需要が広まっている．そこでは外出先からでも家庭内や企業内の端末に自由にアクセスしたいというニーズが考えられる．しかし，家庭内や企業内のネットワークはプライベートアドレスで構築される場合が多く、このような環境ではインターネット側の端末からプライベートアドレスの端末に対して通信を開始することができないという制約がある．そこで本稿では，DNS サーバと NAT ルータを改造し，両者が協調することにより上記制約を解決する通信方式を提案する．

## ２．既存技術

NAT の制約を解決するいわゆる NAT 越えの既存技術として，STUN(1)，NAT-f(2)などがある．

STUN はインターネット上の専用サーバを利用することにより NAT 越えを実現しているが，専用のアプリケーションや UDP 通信でしか利用できないという制約がある．

NAT-f はグローバルアドレスの端末と NAT-f ルータが連携し，グローバルアドレスの端末とプライベートアドレスの端末が通信に必要な NAT テーブルを動的且つ強制的に生成することにより NAT 越えを実現する．しかし，外部の端末と NAT ルータを改造しなければならないという課題がある．

## ３．提案方式

本提案方式は DNS サーバと NAT ルータを改造することにより NAT 越えを実現する．通信を行う各端末には手を加える必要がないという特徴がある．また，アプリケーションに依存せず P2P 通信を実現することができる．

図 1 に提案方式の動作概要を示す．改造した DNS サーバ RDNS（Remodeled DNS）には，予めプライベートアドレス空間内の端末 PN の名前と NAT ルータのアドレスを登録しておく．グローバルアドレス空間の端末 GN はプライマリ DNS として RDNS を設定する．

GN から PN（bob）へ通信を開始する場合の動作手順を以下に示す．

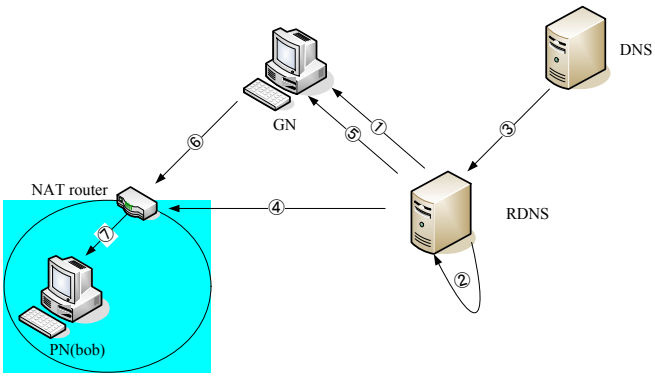



Fig.1 A schema of the proposed method

①GN は RDNS に bob の名前解決を依頼する

②RDNS はリソースレコードから bob を検索する

→存在しないなら③

→存在するなら④

③RDNS は GN の代わりに上位 DNS に名前解決を依頼する

④RDNS は GN から bob への接続依頼があることを NAT ルータに通知する

⑤RDNS は GN に bob のアドレスを応答する(実際は NAT ルータのアドレス)

⑥GN は取得したアドレスに対して通信を開始する

⑦NAT ルータは NAT テーブルを強制的に生成し，GN からの通信パケットを bob に転送する

⑦において NAT ルータは GN からの通信パケットと RDNS からの④で通知された情報を元に NAT テーブルを生成できる．これにより GN から PN への通信を開始することができる．

## ４．むすび

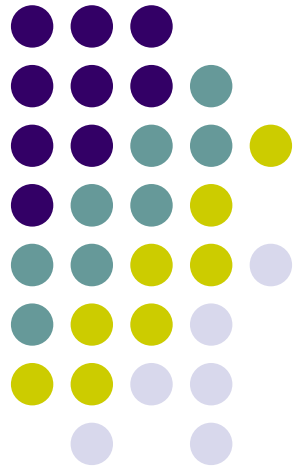
端末の改造が不要な NAT 越え方式を提案した．今後は RDNS と NAT ルータを実装し，動作検証を行う．

### 参　考　文　献

(1) J. Rosenberg, J. et al: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC3489, 2003

(2) 加藤尚樹，柳沢信成，鈴木秀和，渡邊 晃 "アドレス空間の違いを意識しない通信を可能とする NATF(NAT Free protocol) の検討と実装"DICOMO2005 シンポジウム論文集, Vol.2005, No.6, pp.373-376，Jul.2005.

# 端末の改造が不要なNAT越え方式の提案



名城大学　理工学部

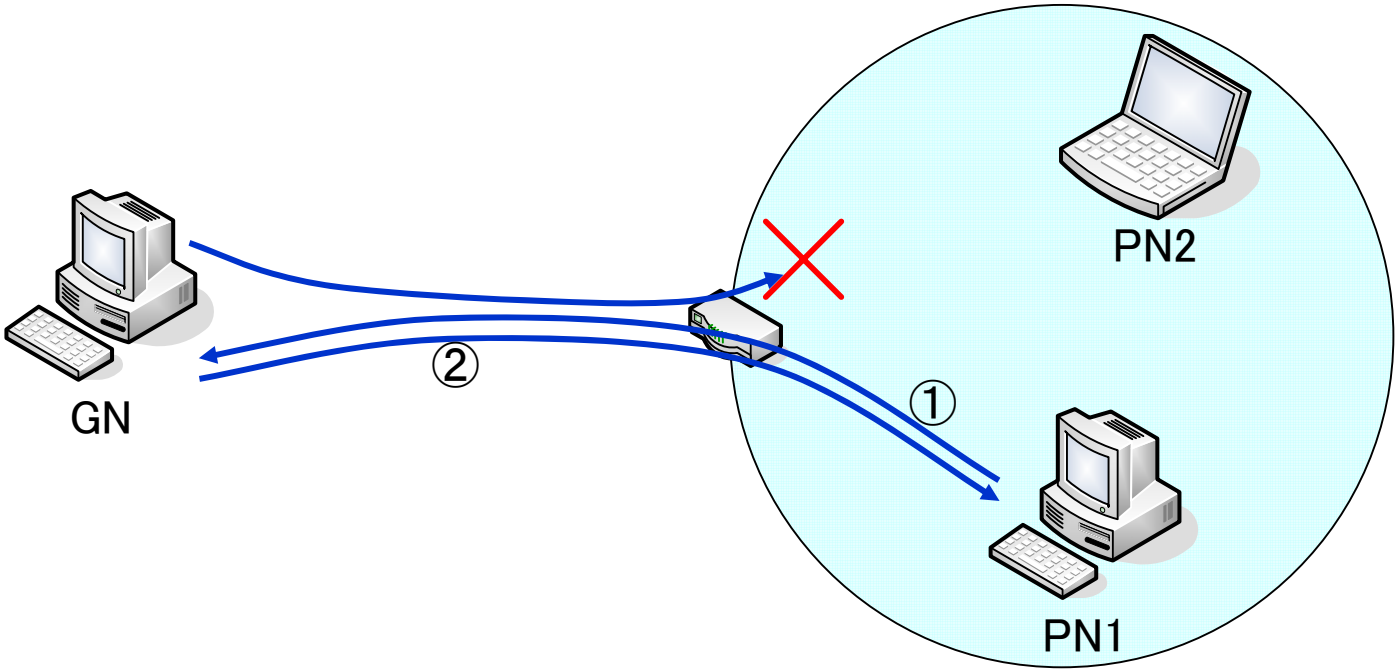
宮﨑　悠　　鈴木　秀和　　渡邊　晃

# 研究背景

- インターネットの普及に伴ない、ユビキタス社会の需要が広まっている
  →いつでもどこからでも情報を得たい

- 家庭内や企業内のネットワークはプライベートアドレスで構築される場合が多い
  →NAT越えの課題がある

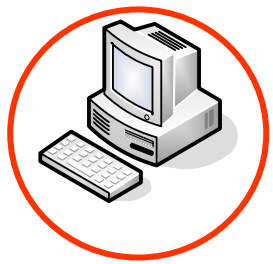
# NAT越え問題

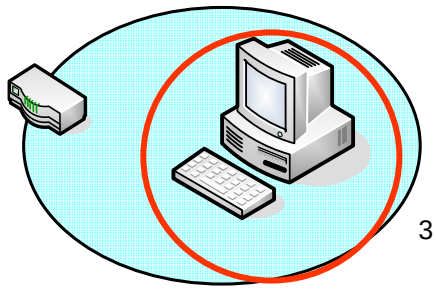



NATの原理(GNにはプライベートネットワーク内の環境が見えない)により外側から内側にアクセスすることができない

# NAT越え既存技術例1

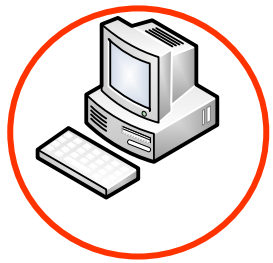
- 各端末と第三装置に実装
  - 利点
    - 端末はNAT越え技術に対応したソフトをインストールさせるだけ
  - 欠点
    - 第三装置を設置する必要がある
  - 技術例
    - STUN
    - TURN

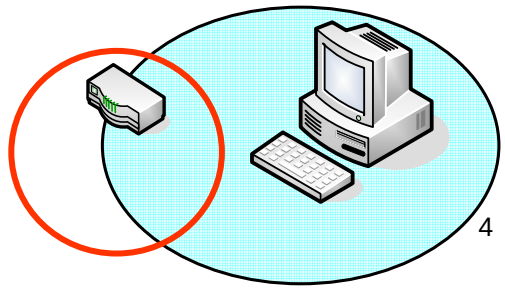




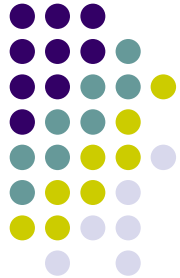
# NAT越え既存技術例2

- GNとNATルータ（DNS）を改良・設置
  - 利点
    - 場合によってはDNSを改良するが、特別な第三装置は必要ない
  - 欠点
    - GNは送信先のネットワークが
      この技術を使っていることを知っていて、
      対応している必要がある
  - 技術例
    - NATS
    - IPv4+4





# 端末の改造が不要なNAT越え方式の提案

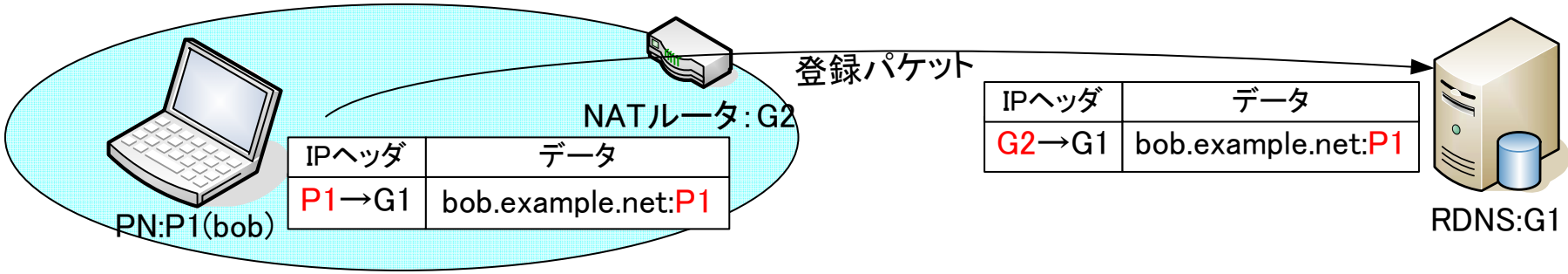


- 端末には手を加えずに問題を解決したい

- 本方式ではNATルータとDDNSサーバを改造し、そのNATルータとDDNSサーバ(RDNS：Remodeled DNS)が連携をとることにより問題を解決する

# 提案方式(事前設定)

- 予めプライベートアドレス空間内の端末PNの名前とNATルータのアドレスがRDNSへ登録される

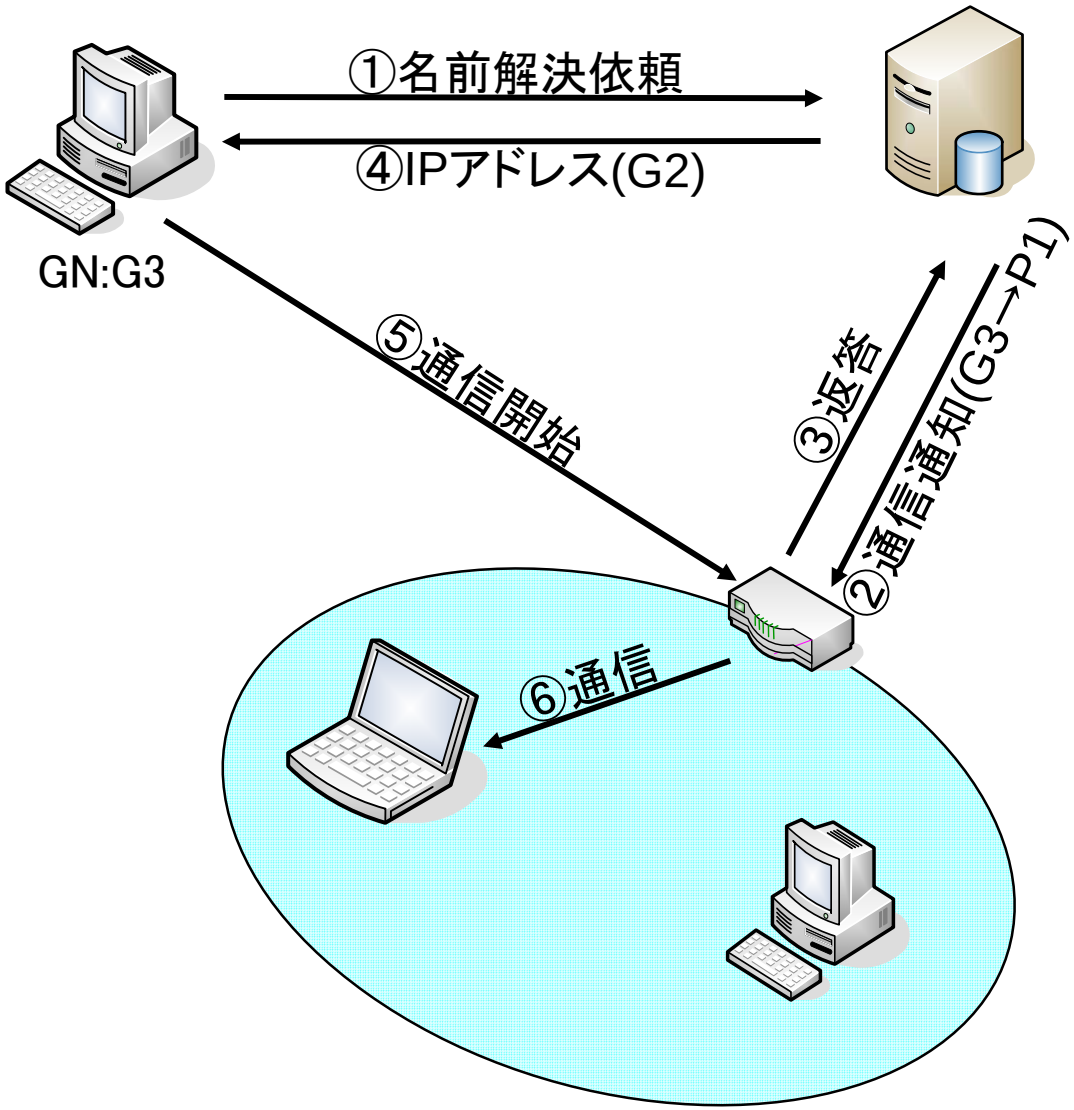



- 上の登録時にNATルータでAccess Control Table (ACT)を作成する

| ACT | |
|---|---|
| *Host Name* | *Private address* |
| bob | P1 |

- グローバルアドレス空間の端末GNはプライマリDNSとしてRDNSを設定する

# 提案方式(動作手順)




| RDNSレコード | | |
|---|---|---|
| *FQDN* | *Private address* | *NAT router* |
| bob.example.net | P1 | G2 |

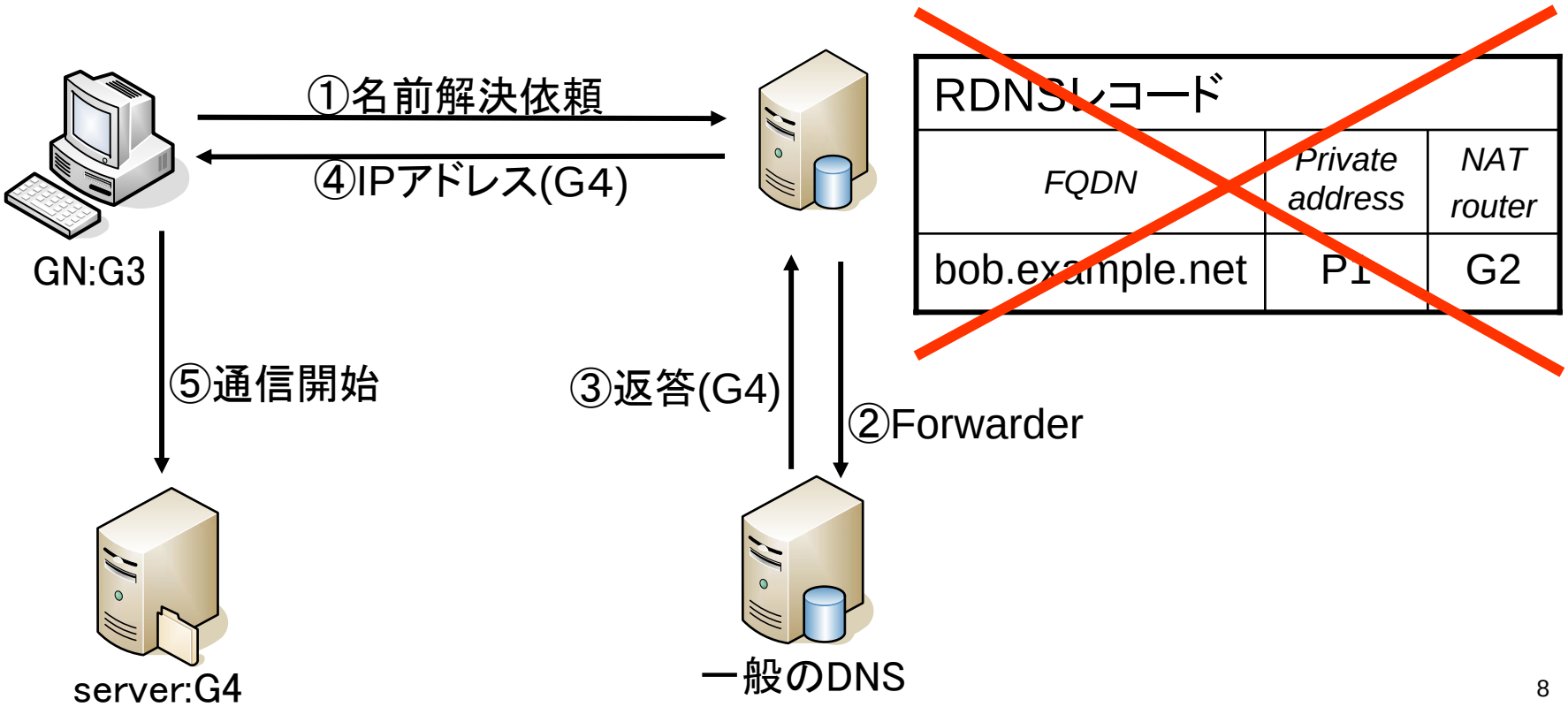
②の後ACTをチェックしてから③を返信

| ACT | |
|---|---|
| *Host Name* | *Private address* |
| bob | P1 |

NATルータは⑤を受信後，②とACTを元にNATテーブルを生成し，通信を転送

# 提案方式(対GN)

- 本方式を採用した端末GNがグローバルアドレス空間にあるサーバー等にアクセスしたい場合



# むすび

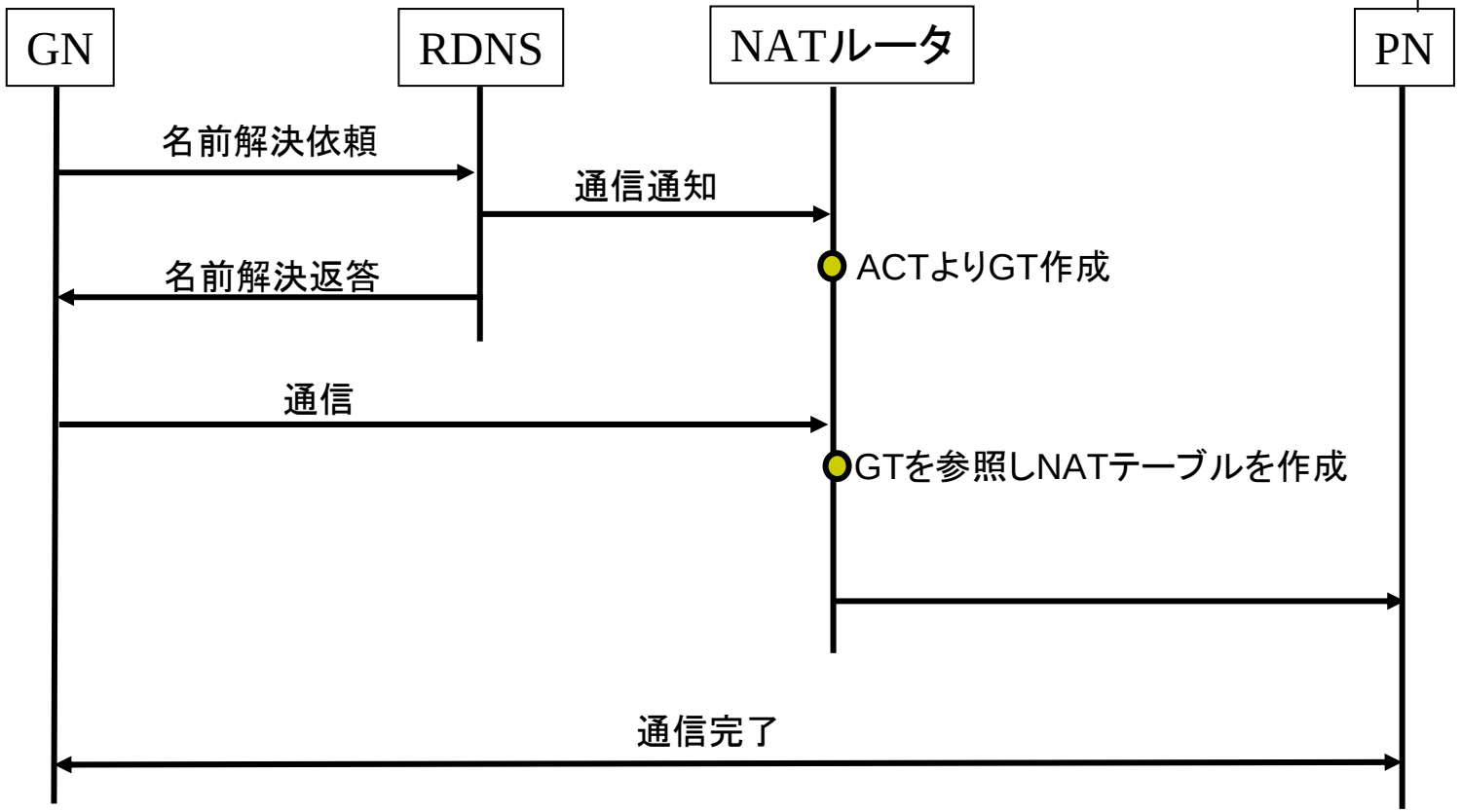
- 提案技術
  - 改良したNATルータとRDNSにより、端末に手を加えることなくNAT越え問題を解決する方法を提案
  - 第三の特殊な装置は必要なく、経路やパケットなどの冗長はない
- 今後の展開
  - 提案方法の実現

# 補足説明

# 補足：提案方式動作

①GNはRDNSにbobの名前解決を依頼する
　RDNSはソースレコードからbobを検索する
　→ない場合は本方式対応ではないと判断して，一般のDNSにフォワーダする
②RDNSはNATルータにG3からP1へ通信要求があったことを通知する
③②に対しての返答
④RDNSはGNにbobのアドレスを応答する
　（実際はNATルータのアドレスG2）
⑤GNは取得したアドレス(G2)に対して通信を開始する
⑥NATルータは得ている情報からNATテーブルを生成し，GNからの通信パケットをbob(P1)に転送する

# 補足:提案方式時間的流れ



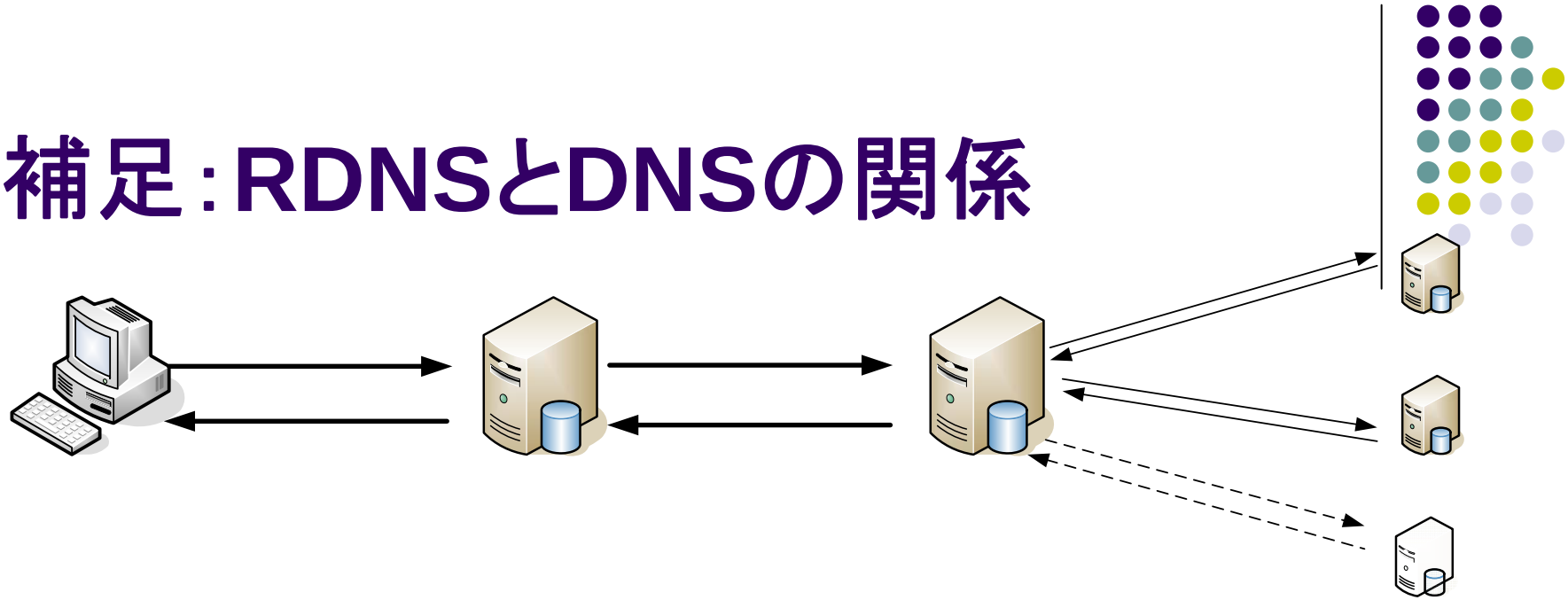
# 補足:考えられる問題点

- 通信の乗っ取り

他のGNからIPアドレスを装ってNATルータ宛に通信が開始された時，NATルータは誤ってPNに通信を通してしまう可能性がある

→RDNSとNATルータに事前に鍵を持たせておけば，盗聴される可能性があるのは④か⑤の為，危険性は軽減できる

# 補足:RDNSとDNSの関係



- GNは予めプライマリDNSにRDNSを登録しておく必要がある
  →RDNSは直接GNと通信を行うことでGNのIPアドレスを得る
- 異なるアドレス空間のPNが増大するとRDNSの対応が悪くなる可能性がある。
- この方式が普及し、一般のDNSにRDNSの様なルータをやり取りする機能が(ブリッジ等で)実装されれば、GNはプライマリDNSを変換することなく実現できる

# 補足：ACT (Access Control table)

- ACTにはPNのホスト名、プライベートIPアドレス、グローバルアドレス空間からの通信の許可・拒否が書かれている。

| ACT | | |
|---|---|---|
| *Host Name* | *Private address* | *authorization* |
| bob | P1 | allow |

- 外側からの通信の許可・拒否はデフォルトでは許可にしておき、何らかの理由により通信をしたくない端末だけ別途拒否登録をする。

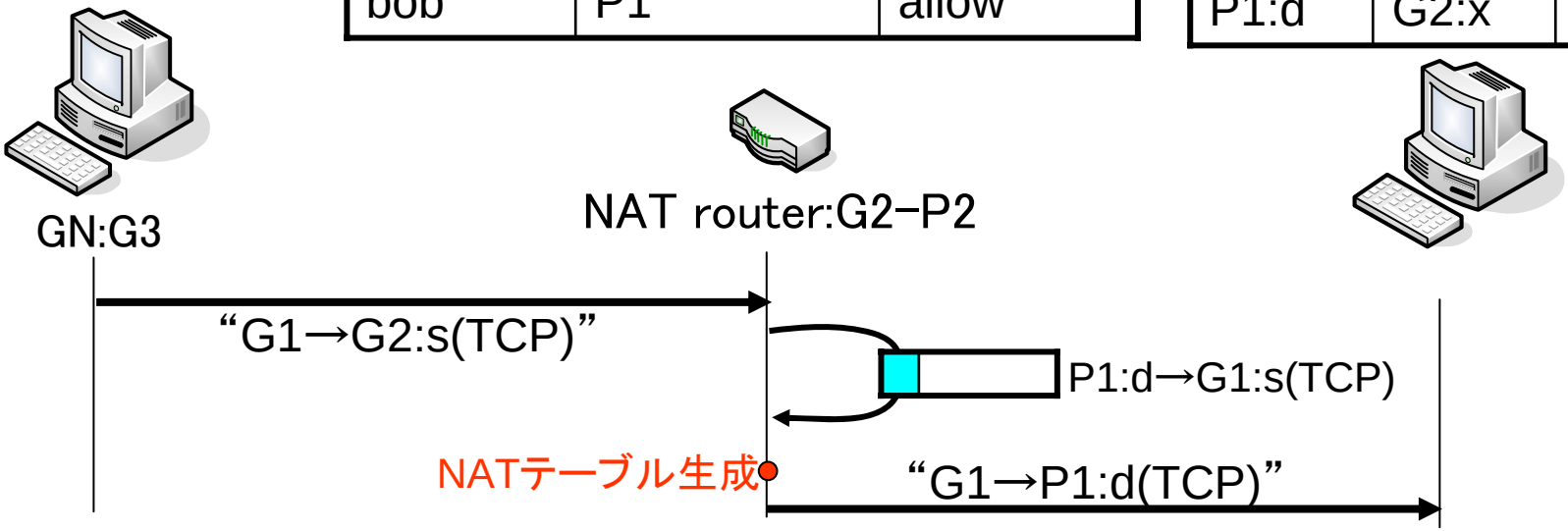
# 補足:NATテーブル生成手法

- GNからのパケットとACT情報から擬似パケットを生成
  - PNからGNへの送信パケットに見せかけもの
  - NATルータの内側インターフェースで受信した際の処理を実行

| 通知情報 |
| --- |
| G3→P1 |

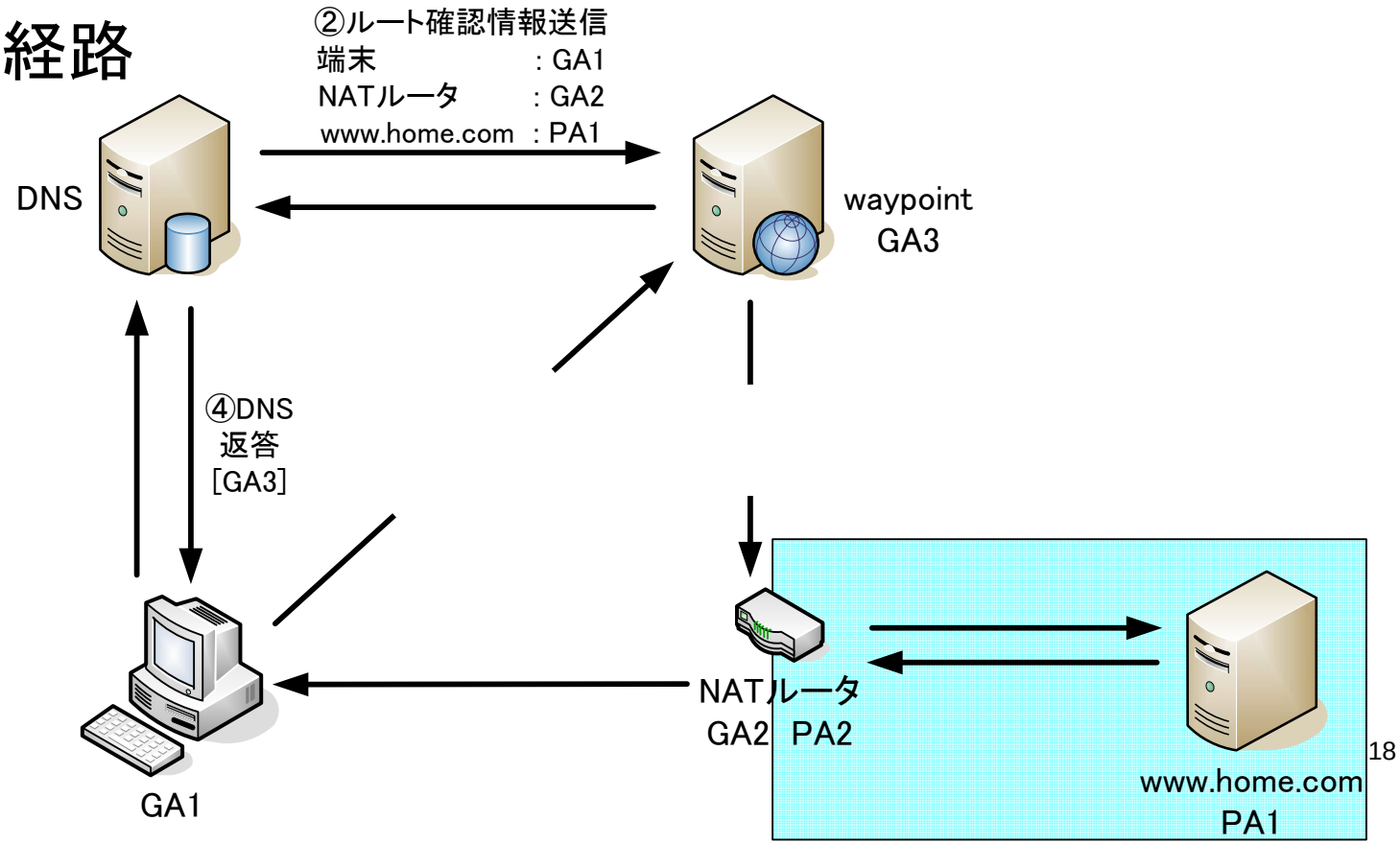
| ACT | | |
| --- | --- | --- |
| *Host Name* | *Private address* | *authorization* |
| bob | P1 | allow |

| NAT table | | |
| --- | --- | --- |
| *Inside* | *Outside* | *protocol* |
| P1:d | G2:x | TCP |



# NAT越え既存技術例

| 技術名 | 実装箇所 | 概略 |
|---|---|---|
| STUN<br>(Simple Traversal of UDP Through NATs | PN<br>STUNサーバ | UDP Hole Punchingを使ってNATを通過する方法 。<br>UDP Hole Punching：UDPを用いて予め内部より外部に通信を行うことでNATに通り道を用意しておき、そこを通して外部より内部に通信を行う方式。 |
| IPv4+4 | GN<br>NATルータ | IPv4ヘッダをカプセル化することで更に32bit追加する。<br>グローバルアドレスとプライベートアドレスを両方保持し、NAT通過時にこのヘッダを見て二つのアドレスを入れ替えることにより通信が可能となる。 |
| NATS<br>(NAT with Sub-Address) | GN<br>NATルータ<br>DNS | IPアドレスとは別に16bitsのサブ・アドレスを定義し、1つの（グローバル）IPアドレスに対して16bitsのサブ・アドレスを割り当てることで、NAT／NAPT内のホストを特定する手段を提供 |
| AVES<br>（Address Virtualization Enabling Service） | Waypoint<br>DNS<br>NATルータ | グローバル空間にwaypointと呼ばれる機器を配置し、それを経由してグローバルアドレス空間の端末はプライベートアドレス空間の端末に通信を行う。 |

# NAT越え既存技術例：AVES

- DNS,NATルータ,waypointサーバを改良・設置
- 外側の端末は内側の端末への通信に全てwaypointを中継する
  →三角経路