グローバルアドレスとプライベートアドレス空間を跨る DPRP の検討

後 藤 裕 司† 鈴 木 秀 和‡ 渡 邊 晃†

名城大学理工学部† 名城大学大学院理工学研究科‡

1. はじめに

企業ネットワークにおける情報漏洩などの犯罪を防止するための既存のセキュリティ技術として IPsec がある．しかし，端末が移動するなどしてシステム構成が頻繁に変わるような環境では，それに応じて IKE の設定情報を変更する必要がある．そのため管理者の負担が大きく，IPsec はイントラネット内ではほとんど利用されていない．そこで，我々はシステム構成が変化しても端末や中継装置自身がその変化に動的に対応することができる DPRP（Dynamic Process Resolution Protocol）と呼ぶ動作処理情報生成プロトコルを提案している[1]．DPRP は端末間の通信に先立って通信経路上に存在する装置が情報を交換することにより，パケットの暗号処理や破棄など通信の処理に必要な動作処理情報を動的に生成する．しかし，既存の DPRP はグローバルアドレス空間か，プライベートアドレス空間のどちらかでしか動作せず，通信経路上に NAT（Network Address Translation）が介在し，両アドレス空間が混在するような環境に対応できない．

本稿では，この課題を解決する 1 ステップとして，プライベートアドレス空間からグローバルアドレス空間に通信が開始される場合における NAT 越えを可能とする DPRP について検討した．

2. 既存の DPRP とその課題

DPRP を実装した装置を GE と呼び，ホスト型 GE を GES，ルータ型 GE を GEN という．GEN はサブネットを構成し，配下の一般端末を保護する．

送信側 GE は，通信パケットの送信時に自身が保持する動作処理情報テーブル PIT（Process Information Table）を検索する．PIT にはコネクション識別子 CID（Connection Identification）送信元／宛先 IP アドレス，ポート番号，プロトコルタイプ，動作処理情報（暗号化/復号，透過中継，廃棄）などの情報が含まれている．検索にはコネクション情報 CID が用いられる検索の結果，該当する PIT があれば CID の内容を確認した後，動作処理情報に従ってパケットを処理する．該当する PIT がなければ，送信パケットを一時的に待避して DPRP を開始する．DPRP は図 1に示す ICMP をベースとした 2 往復の制御パケットからなる．各制御パケットには待避したパケットの CID が記載されている．DDE（Detect Destination End GE）は通信相手に最も近い GE を特定する．RGI（Report GE Information）は，通信経路上の各 GE の情報を収集する．この時，RGI の宛先は CID に記載されている送信元 IP アドレスに返信される．収集した情報から動作処理情報を決定し，MPIT（Make Process Information Table）により各 GE に対して動作処理情報の通知と PIT の登録を行う．CDN（Complete DPRP Negotiation）によりネゴシエーション完了の通知を行う．

各 GE に登録される PIT は制御パケットに記載されている CID から作成される．しかし，通信経路上に NAT がある場合は，通信パケットがアドレス変換されるため，グローバルアドレス空間側の GE が生成する PIT と通信パケットの CID が一致しないという課題が発生する．この理由は，NAT の働きによりグローバルアドレス空間側の端末は NAT と通信しているように見えるため DPRP 制御情報が運ぶ情報が一致しないためである．

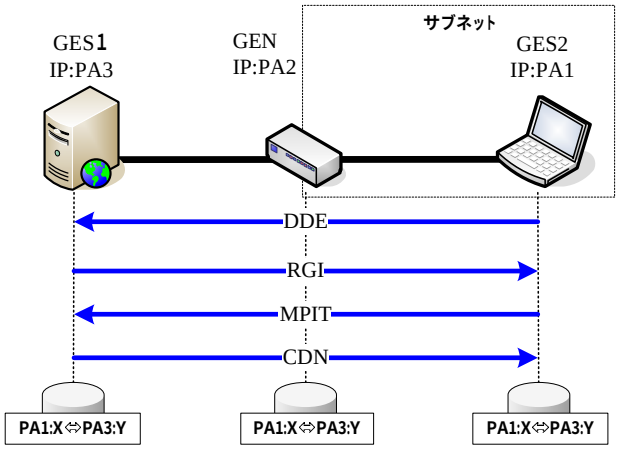


図1 既存の DPRP シーケンス

3. NAT 越えの対応

図 2に改良した DPRP シーケンスを示す．GNAT は NAT 機能を追加した GENである．GES1 側をグローバルアドレス空間，GES2 側をプライベートアドレス空間とする．

まず，DDE が GNAT を通過するときに NAT を越えたという識別フラグをセットする．DDE を受信した GES1 は，フラグをチェックして，フラグがセットされていれば RGI の宛先を GNAT 宛に変更する． RGI は GNAT でアドレス変換されてプライベートアドレス空間の端末に到達することができる．GES2 は PIT を生成して GES1 宛に MPIT を送信する．

GNAT は MPIT を受信するとパケットに記載されている CID を元に，TCP または UDP パケットを作成し，擬

"Researches on extended Dynamic Process Resolution Protocol between global and private address area"

† Yuji Goto and Akira Watanabe
Faculty of Science and Technology, Meijo University

‡ Hidekazu Suzuki
Graduate School of Science and Technology, Meijo University

似的に自分宛に送信する．このパケットを疑似パケットと呼ぶ．疑似パケットの送信元／宛先 IP アドレスとポート番号は待避した通信パケットと同一にする．この処理を行うことによって，表 1に示すような TCP/UDP 対応の NAPT テーブルが作成され，疑似パケットはアドレス変換される．GNAT はアドレス変換後の疑似パケットの CID を用いて MPIT の内容を書き換える．以後は既存の DPRP と同様の処理を行い PIT の作成を行う．このようにして，プライベートアドレス空間側の GE にはアドレス変換前の CID と一致した PIT が作成され，GNAT およびグローバルアドレス空間側の GE にはアドレス変換後の CID と一致した PIT が生成される．

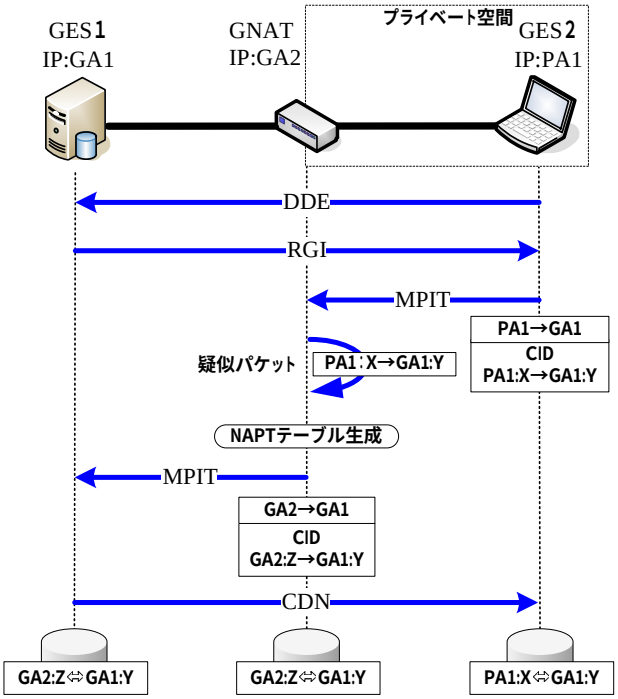


図2　改良した DPRP シーケンス

表 1　NAPT テーブル

受信		=> 送信	
送信元	宛先	送信元	宛先
PA- X	GA- Y	GA2 Z	GA- Y
GA- Y	GA2 Z	GA- Y	PA- X

XYZポート番号

4.　実装

DPRP は IP 層に実装されている．OS には IP 層の情報が豊富な FreeBSD を選択している．IP 層の入出力関数 ip_input(), ip_output()から DPRP モジュールを呼び出して処理を行う．それ以外の部分については DPRP の影響を一切受けない．

図 3に natd（NAT 機能を実現するデーモン）を実装した GNAT の処理の流れを示す． GNAT では DPRP の呼び出す位置に注意が必要である．プライベート側のインタフェースで受信した場合はアドレス変換を行ってから DPRP を呼び出し，グローバル側のインタフェースで受信した場合は，DPRP の呼び出しを行ってからアドレス変換を行う．ここで，NAT を処理する前に DPRP の処理を実行すると，natd 通過後に ip_input()に処理が渡された時に，受信時と natd 通過後でパケットの内容が変化しているためにチェックサムが一致しないという問題が起こる．そのため natd の改造を行い，チェックサムを差分だけ再計算を行うようにした．

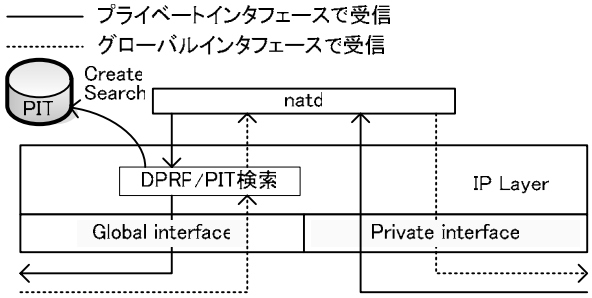


図 3　GNAT の処理の流れ

図 2に示したシステム構成において，プライベートアドレス空間側の GES2 からグローバルアドレス空間側の GES 1 に対して，FTP 接続や telnet を行った．その結果，GNAT において NAT テーブルが正しく生成できることを確認した．また GNAT および GES1 では，アドレス変換後の CID で PIT を作成できることも確認した．さらに FTP 接続，telnet のパケットがアドレス変換されても，PIT 検索を行い，動作処理情報に基づいて通信できることを確認した．

5.　まとめ

本稿ではグローバルアドレス空間とプライベートアドレス空間を跨る DPRP の検討を行った．DPRP により作成された PIT と NAT でアドレス変換されたパケットの CID が一致するように DPRP の改良を検討した．その検討に基づいて実装を行い，プライベートアドレス空間からグローバルアドレス空間への通信できることを確認した．今後は別途検討中の NATF（NAT Free protocol）[2]と統合することにより，グローバルアドレス空間からプライベートアドレス空間への通信開始とそれに伴う DPRP の実現について検討を行う．

参考文献

[1]　鈴木秀和，渡邊晃：フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装，情報処理学会研究報告，2005-CSEC-28，pp.199-204，March. 2005.

[2]　加藤尚樹，柳沢信成，鈴木秀和，宇佐見庄五，渡邊晃:インターネットから家庭ネットワークへの接続を可能とする NATF プロトコルの検討と実装，2005-情報ワークショップ 2005(WiNF2005)，pp.142-146，September.2005.

[3]　Paul Francis，Ramakrishna Gummadi，IPNL:A NAT-Extended Internet Architecture ， 2001-SIGCOMM 2001,pp.69-80,August.2001

[4]　Zoltan Turanyi ， Andras Valko ， IPv4+4 ， 2002-ICNP2002，pp.290-301，November.2002

異なるアドレス空間を跨るDPRPの検討

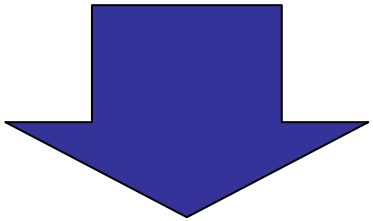
Researches on extended Dynamic Process Resolution Protocol for different types of address areas

名城大学　理工学部

後藤　裕司　鈴木　秀和　渡邊　晃

はじめに

- ユビキタスネットワークでは
  - 安全な通信
  - 自由に移動しながら通信
  - どんな環境からでもアクセス

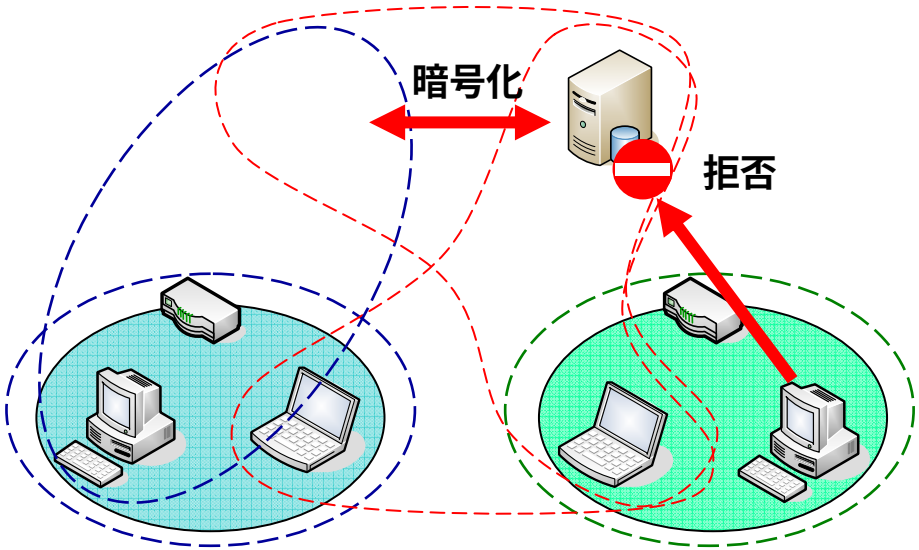


フレキシブルプライベートネットワーク

FPN（Flexible Private Network）

FPN (*Flexible Private Network*)

柔軟性とセキュリティを兼ね備えたグループ通信を可能にするネットワーク

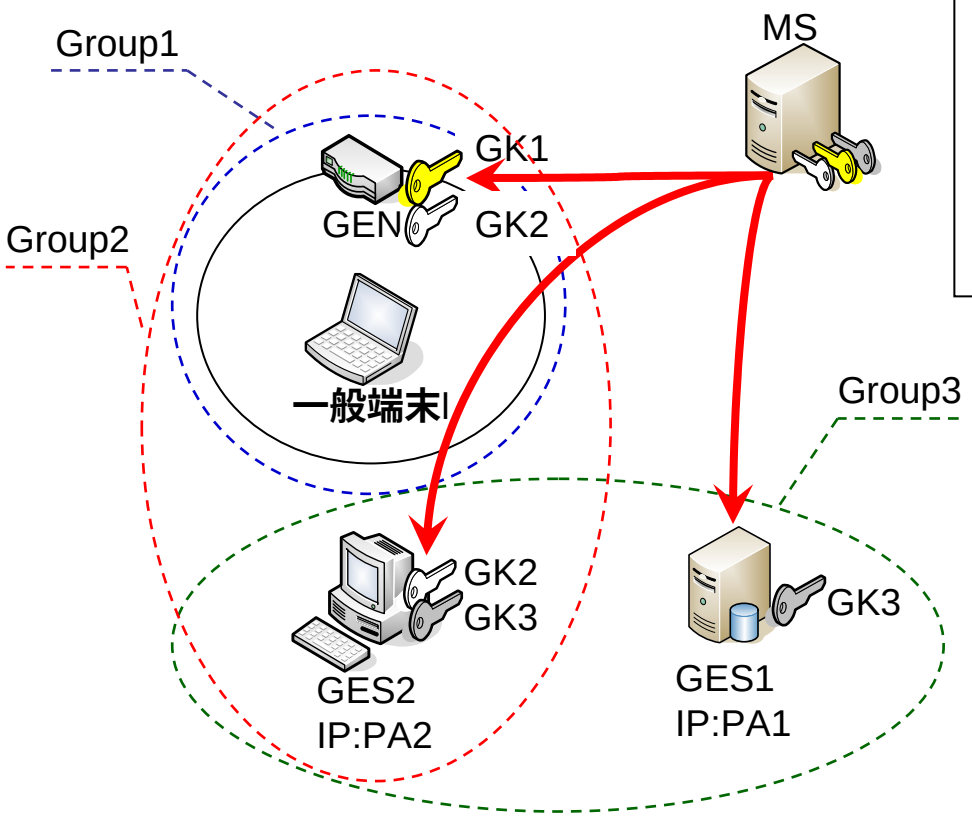


- ホスト-サブネットの混在したグルーピングが可能
- システム構成が変化しても自動的に位置情報を学習して必要な情報を生成
- 移動してもグルーピング関係は維持
- 同一グループ間の通信は暗号化
- グループ外からのアクセスは拒否が可能

- **同一アドレス空間にしか対応していない**
  - GA (グローバルアドレス) 空間とPA (プライベートアドレス) 空間を跨いでグルーピングできない.

FPNを異なるアドレス空間に対応させる

FPN：グループの定義方法



MS（Management Server）：管理装置

GE：FPNに対応した装置

GES（Software型）：ホストタイプ

GEN（Network型）：ルータタイプ

グループ鍵は定期的に更新

- **通信グループとグループ鍵を1：1に対応づける**
  - **IPアドレスに依存しないグループを定義**
- **MSは各GEにグループ番号とグループ鍵GKを配送**

DPRP *(Dynamic Process Resolution Protocol)*

- **通信に先立って通信経路上のGE間で必要な情報を交換**
- **動作処理情報テーブル**PIT (Process Information Table) **を生成**
- **パケットは動作処理情報に従って処理される**

PITの内容

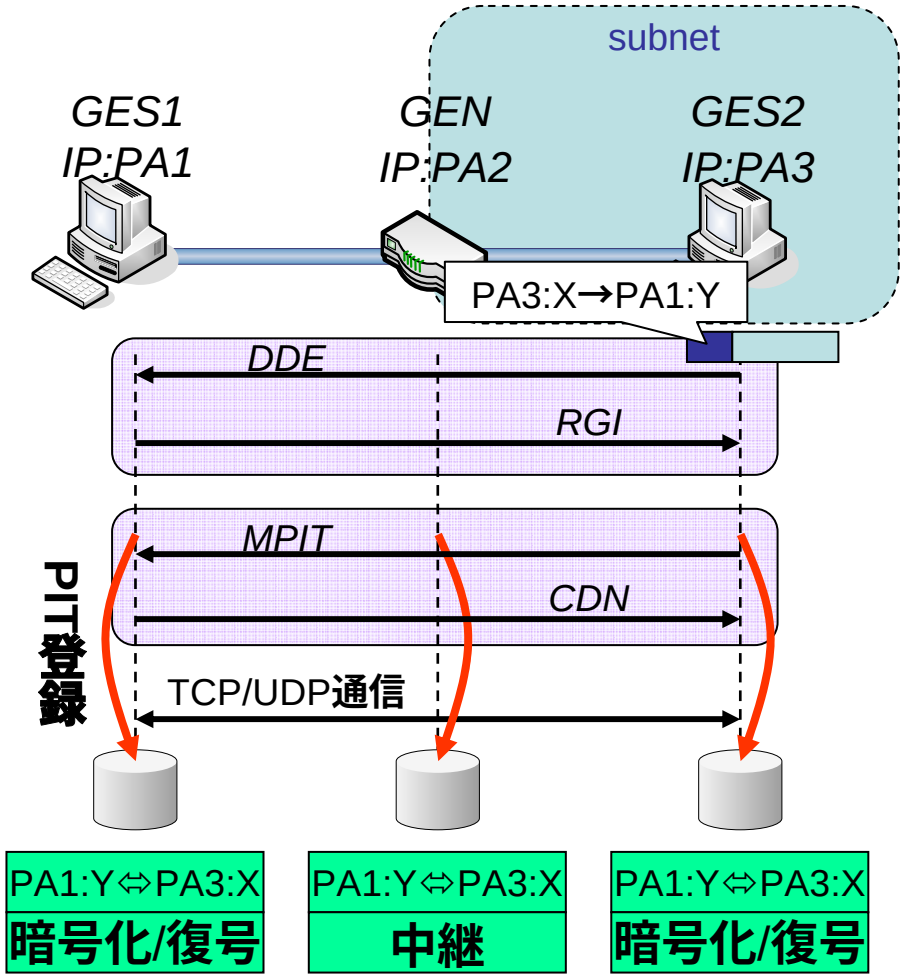
送信元/宛先：IPアドレス/ポート番号，プロトコルタイプ
グループ鍵の番号，動作処理情報 (暗号化/復号/透過中継/破棄) など

- **通信開始時，端末/サブネットが移動してIPアドレスが変化**

PITを検索 { **あり→PITに従って処理**
なし→DPRPネゴシエーションの実行

システム構成が変化しても動的にPITを生成
→FPNにおけるグループ通信を可能にする

DPRPの動作概要



4つの制御パケット（ICMPベース）

- DDE（Detect Destination End GE）
- RGI（Report GE Information）
- MPIT（Make Process Information）
- CDN（Complete DPRP Negotiation）

DPRPの動作（2往復のネゴシエーション）

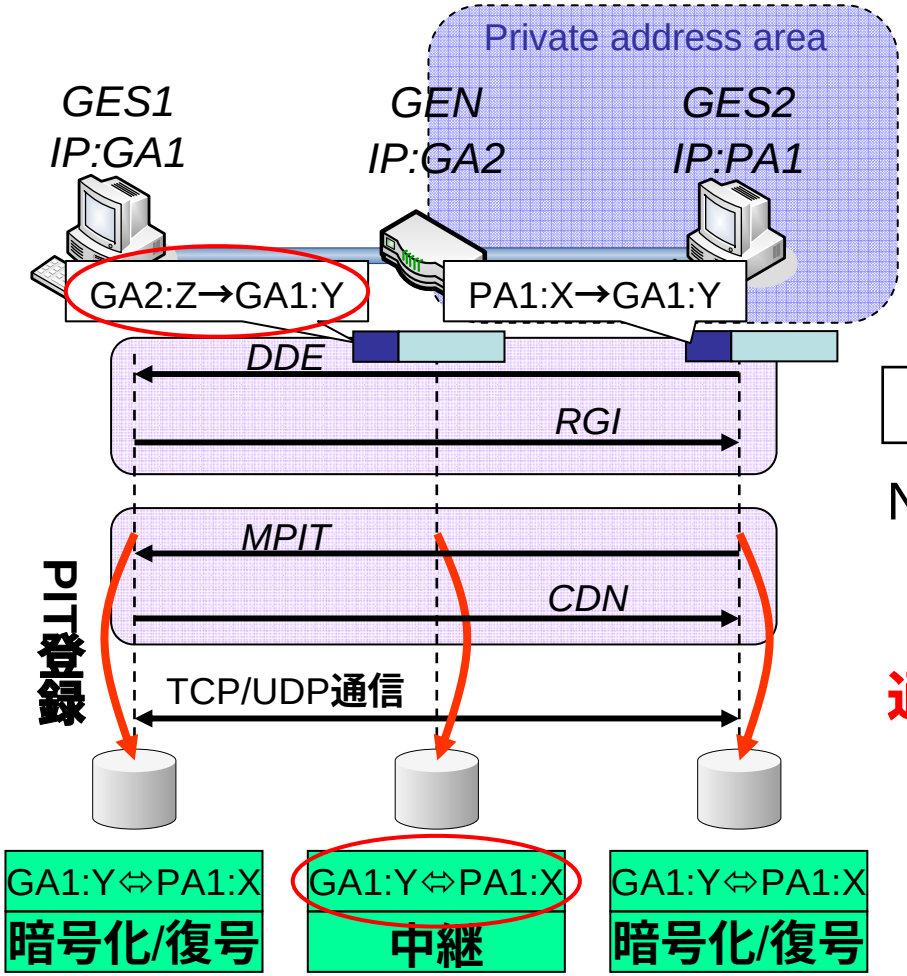
1. **終端GEの決定，通信経路上の各GEの設定情報を取得し動作処理情報を決定**
2. **動作処理情報を通知とPITの生成とDPRPネゴシエーションの完了を通知**

PITは**通信パケットのコネクション識別子**CID（Connection ID）**を元に生成される**

CID
送信元IP：ポート→宛先IP：ポート プロトコルタイプ

DPRPの課題

通信経路上にNAT



GA空間側の端末：*GES1*

PA空間側の端末：*GES2*

課題

NATでアドレスとポート番号が変換される

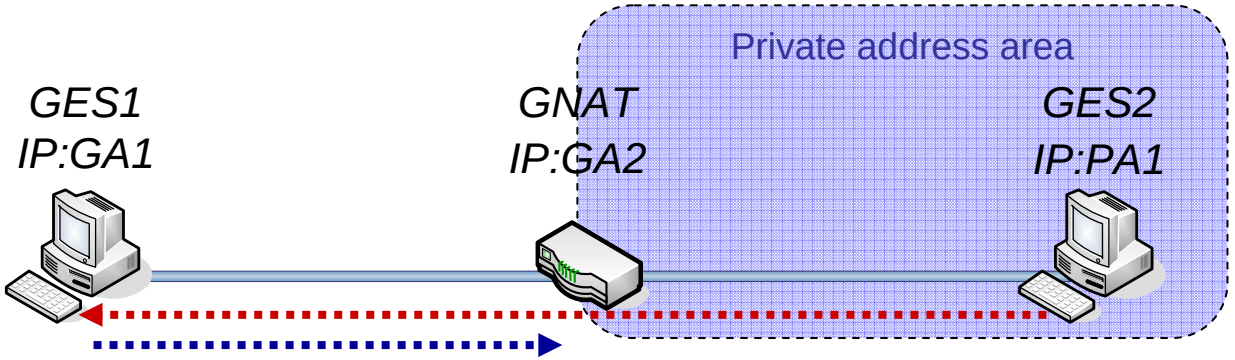
通信パケットとPITの内容が一致しない

DPRPの改良を行いNATに対応したPITを生成する

NATに対応したPIT

通信経路上にNAT

GNAT：GENにNAT機能を追加



GA1:Y⇔GA2:Z	GA1:Y⇔GA2:Z	GA1:Y⇔PA1:X
暗号化/復号	中継	暗号化/復号

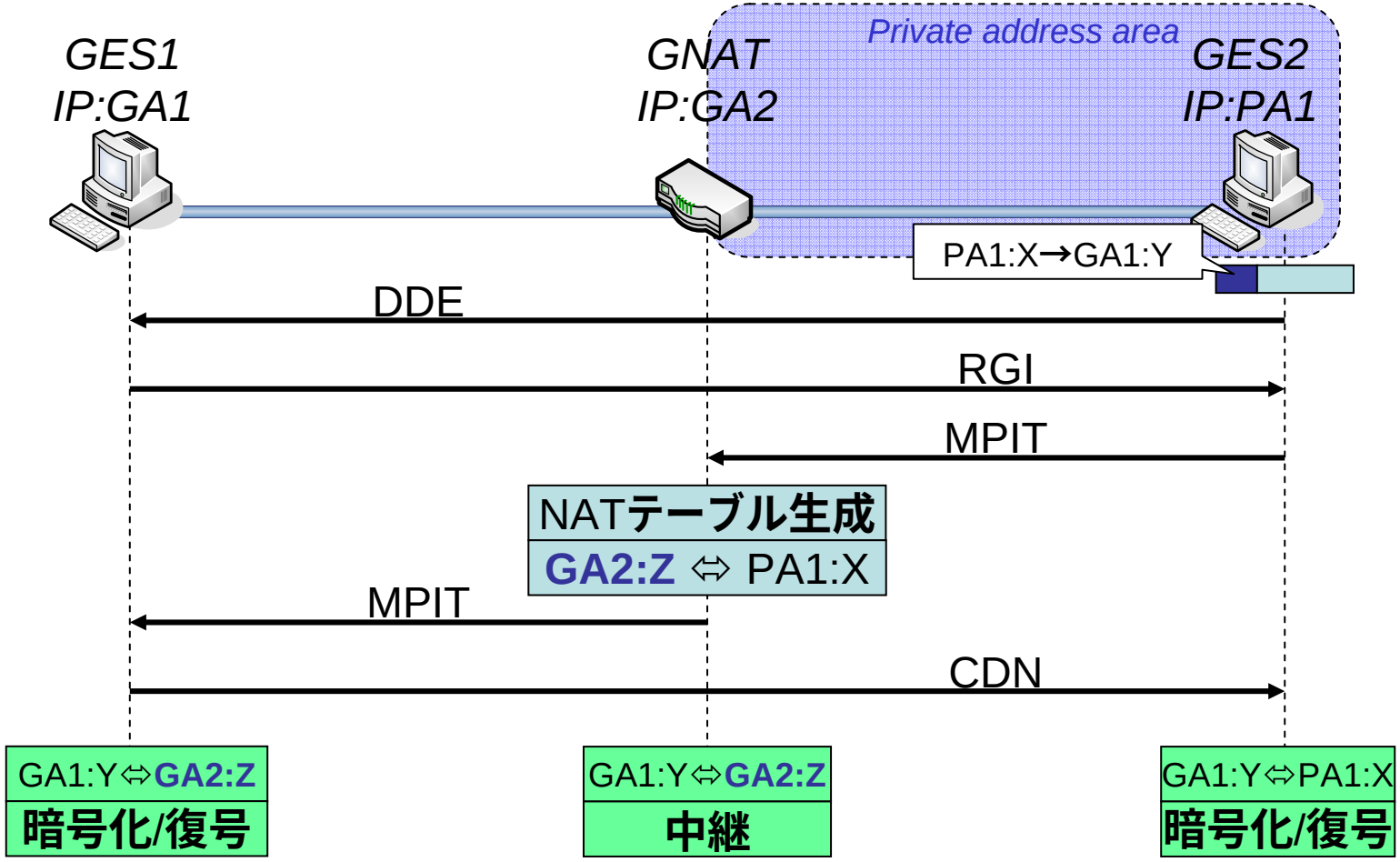
NATテーブル

GA2:Z⇔PA1:X

- GES2はGES1が通信相手に見える
- GES1はGNATが通信相手に見える

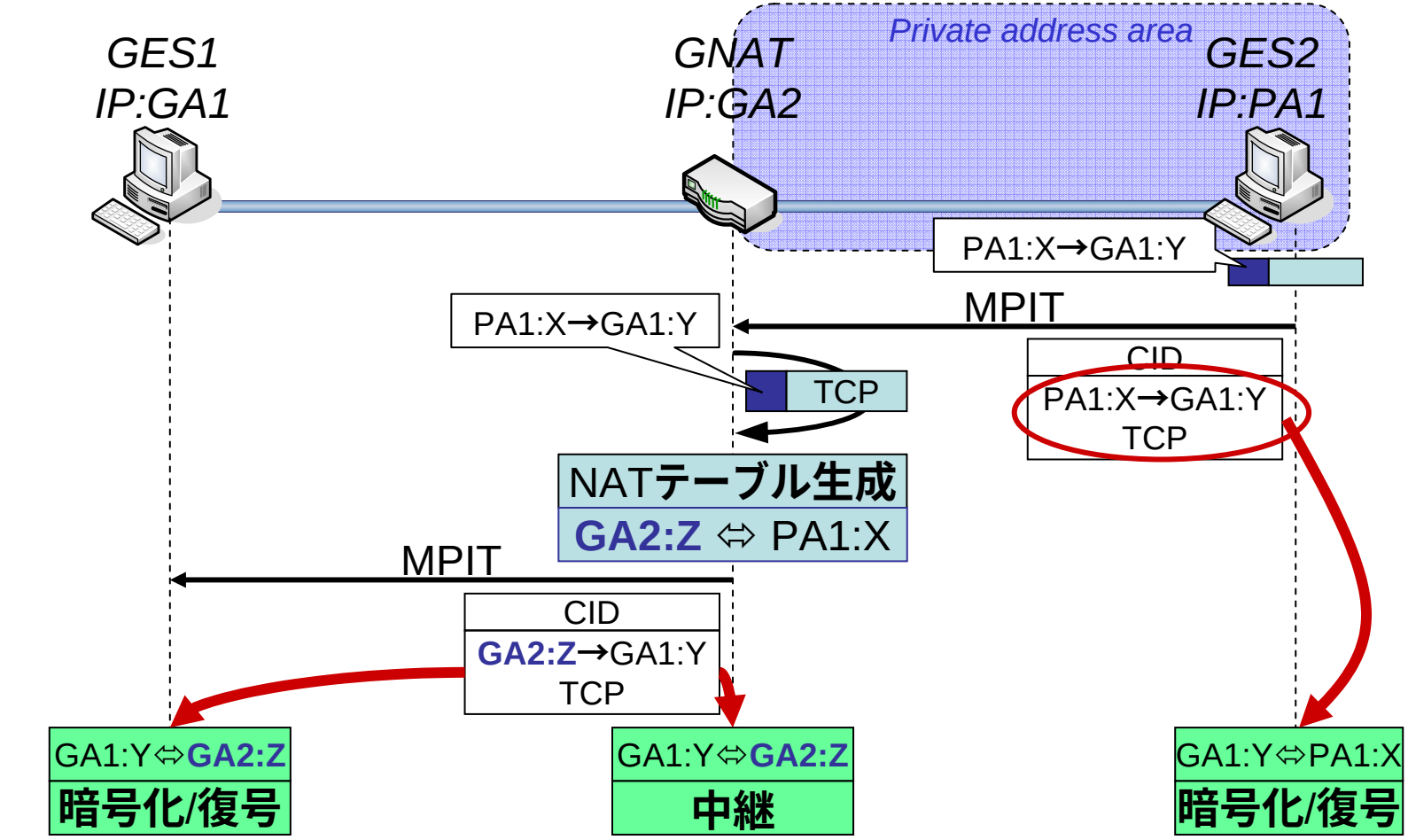
通信相手の見え方によって異なるPITを生成する

PITの生成方法1



強制的にNATテーブルを生成
NATテーブルの変換後の情報でPITを生成

PITの生成方法2

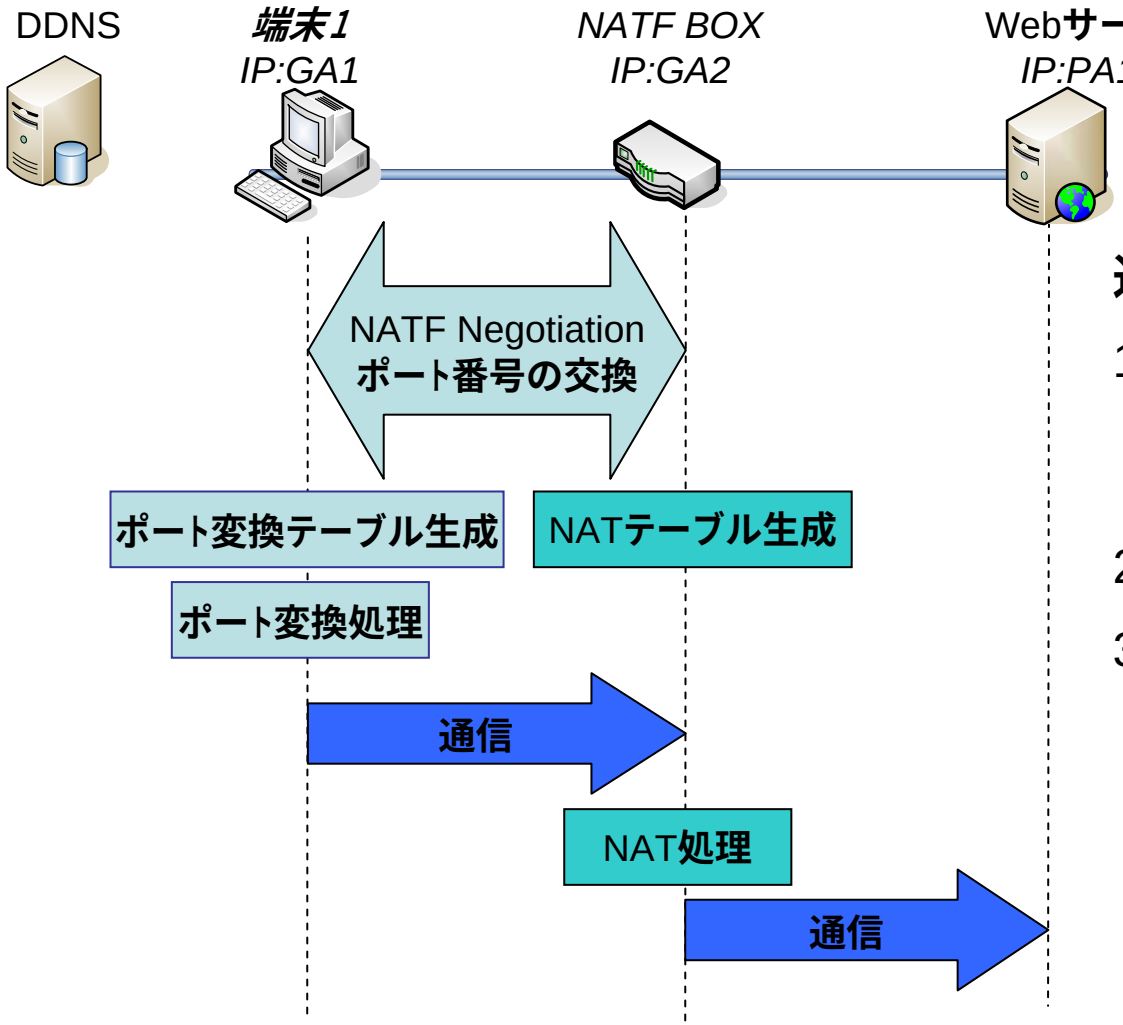


PA空間からGA空間へのDPRPが可能
→PA空間とGA空間を跨いでグルーピングすることが可能

まとめ

- 異なるアドレス空間を跨るDPRPについて提案
  - NATに対応したPITの考え方
  - PITの生成方法
  - PA空間とGA空間の混在環境でのグルーピング
  - 実装済み，動作確認済み
- 今後の予定
  - 改良したDPRPの性能測定
  - GA空間からPA空間へのDPRPの検討

NATF (NAT Free protocol)の概要



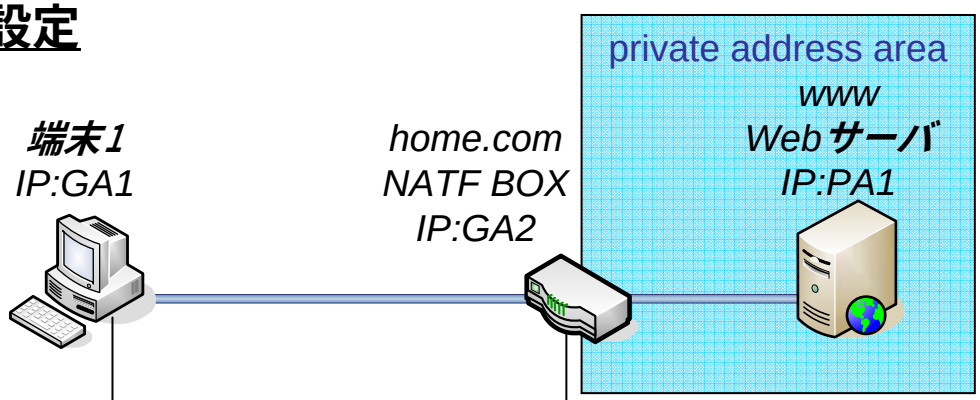
通信開始時に

1. NATF Negotiation **を行いNAT テーブルの生成とポート番号交換テーブルの生成**
2. **ポート変換処理を行い送信**
3. NATF BOX**でアドレス変換して** GES2**にパケット送信**

NATF BOX**と端末1に初期設定が必要**

NATF (NAT Free protocol)の動作1

初期設定



NRDB (Name Resolution Data Base)

APDB (Access Permission Data Base)

ドメイン名	IPアドレス
home.com	GA2

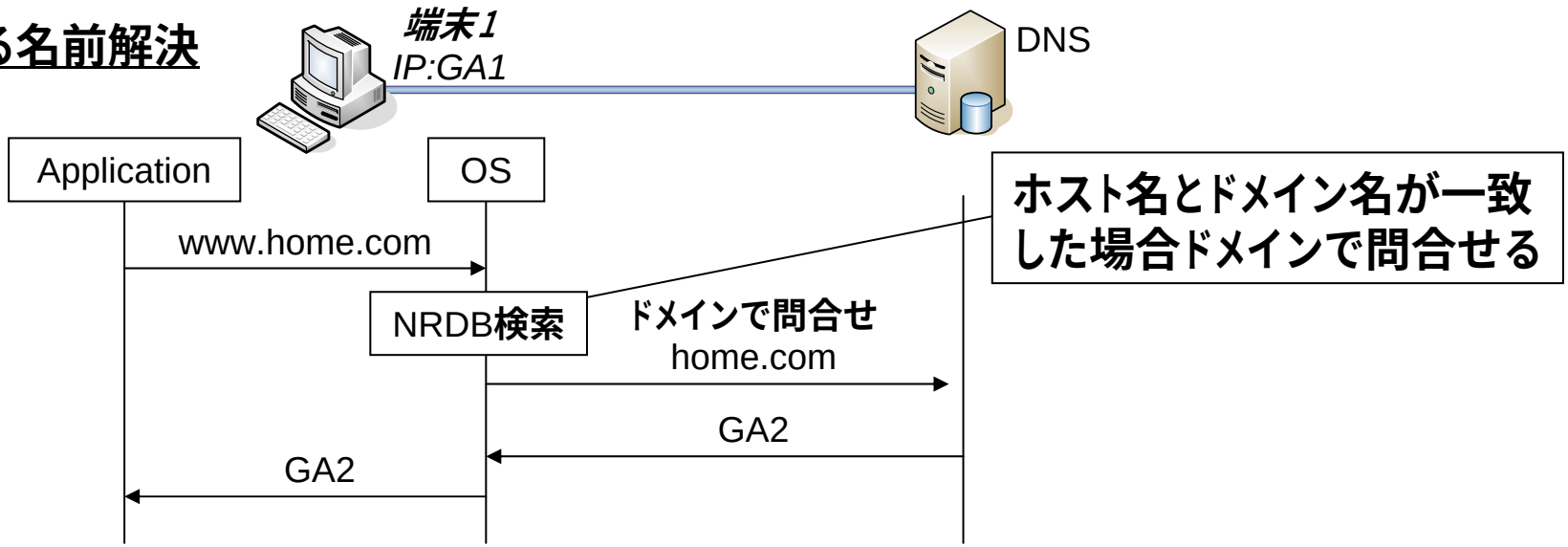
NRDB

ホスト名	ドメイン名
www	home.com

APDB

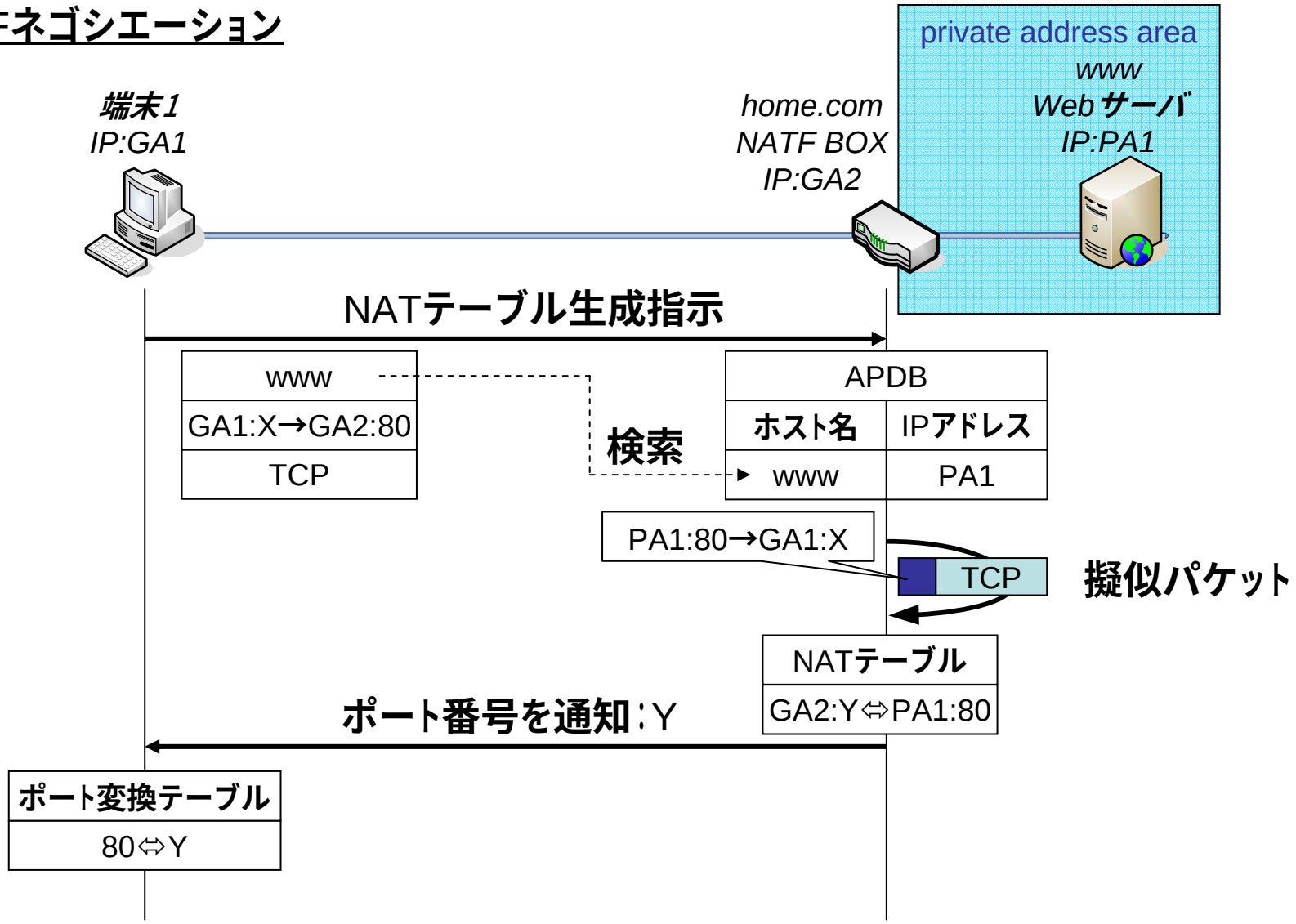
ホスト名	IPアドレス
www	PA1

DNSによる名前解決

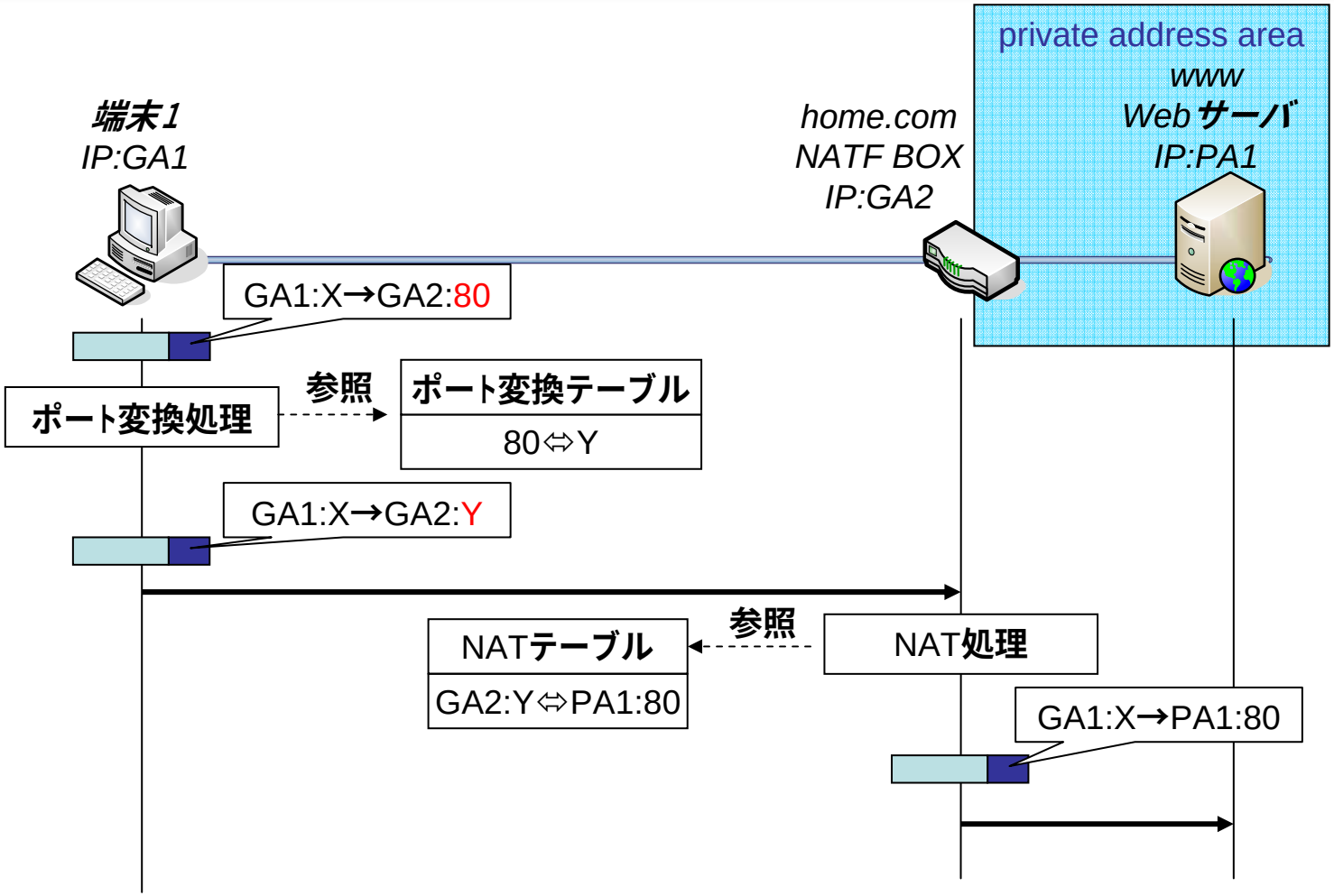


NATFの動作2

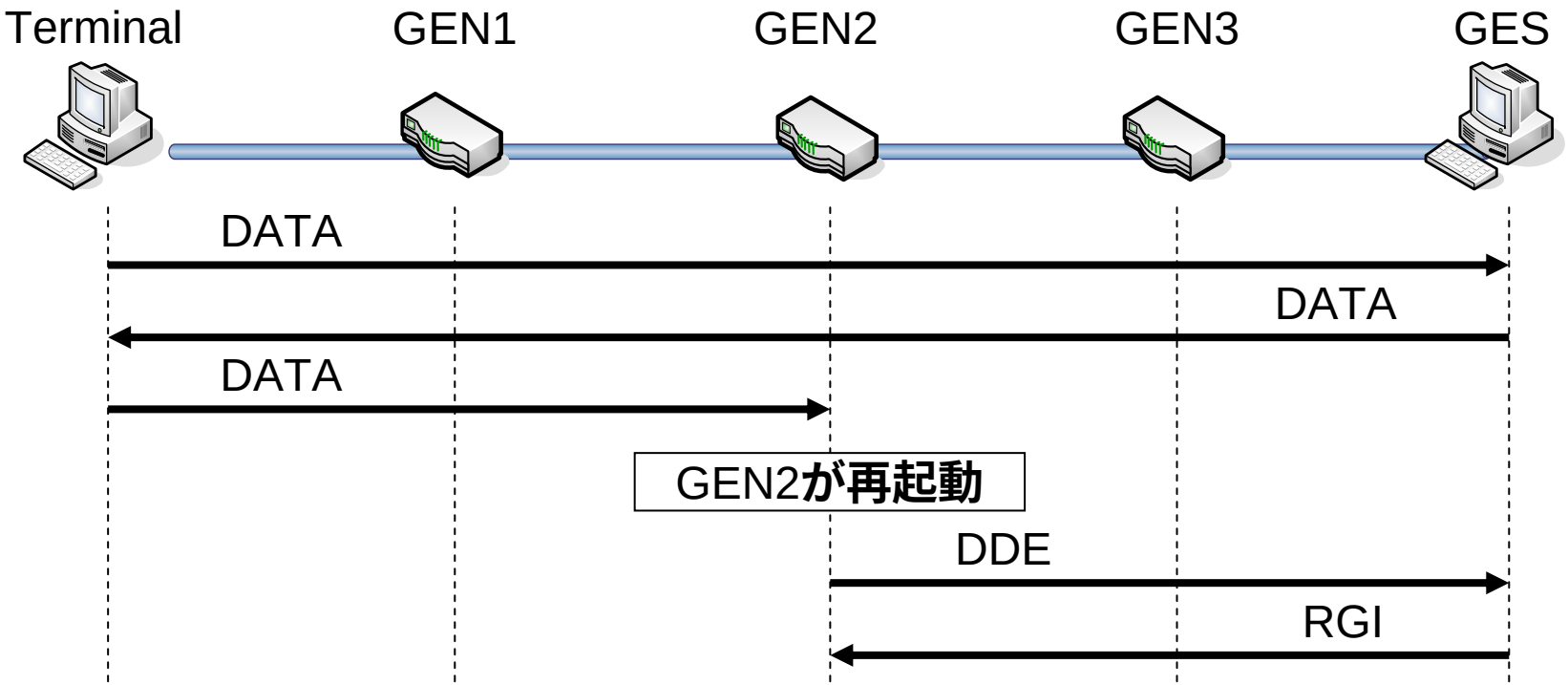
NATFネゴシエーション



NATFの動作3


private address area
www
Webサーバ
IP:PA1
端末1
IP:GA1
home.com
NATF BOX
IP:GA2
GA1:X→GA2:80
参照
ポート変換テーブル
80⇔Y
ポート変換処理
GA1:X→GA2:Y
参照
NATテーブル
GA2:Y⇔PA1:80
NAT処理
GA1:X→PA1:80

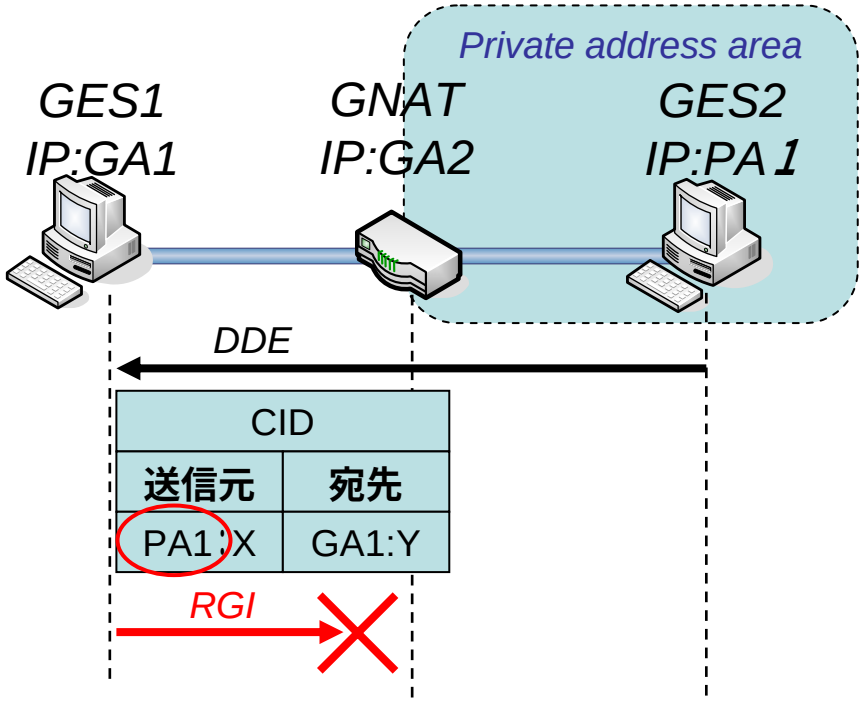
既存DPRP：RGIの宛先



- GEN2**が再起動などをして**PIT**が消えたとすると，そこから**DPRP Negotiation**が始まる**
- **エンドエンドの情報で**PIT**が生成できない**
  - GEN2**と**GES**の情報で**PIT**が生成される**

課題2：RGIの宛先問題

PA空間からGA空間へのDPRP



GA空間側の端末：*GES1*

PA空間側の端末：*GES2*

GENにNAT機能を追加：***GNAT***

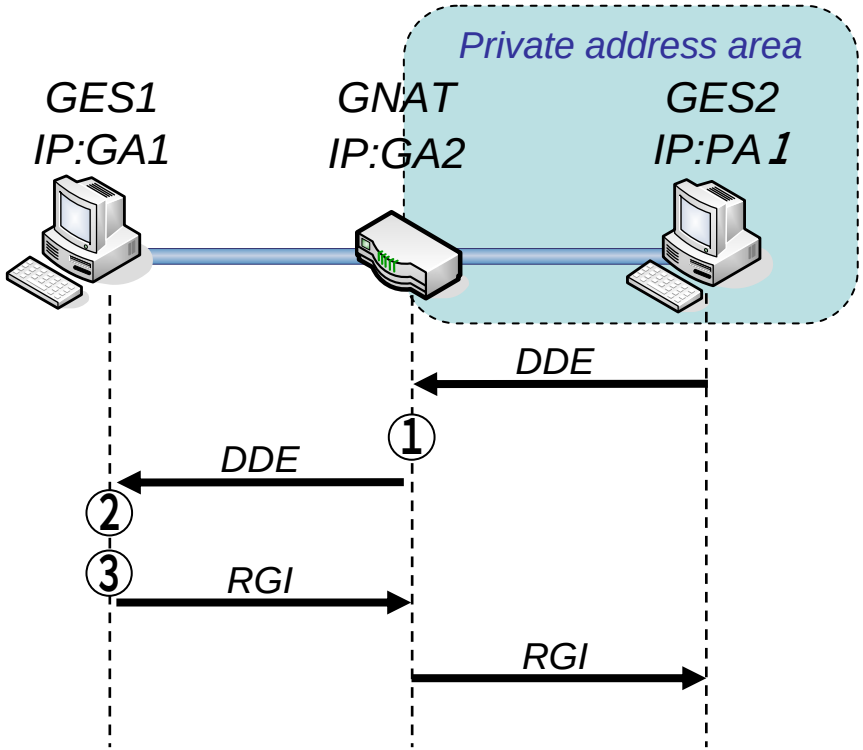
1. 通信パケットのCIDを取得
2. GES2からGES1にDDEを送信
3. GES1がDDEを受信
4. CIDの送信元IPアドレスにRGIを送信

RGIの宛先がプライベートIPアドレスため送信できない

課題2の解決方法

◆NAT通過したという識別フラグを定義

◆RGIの宛先を変更



GNATの動作

1. DDEがNAT通過後

   ① DDE内に識別フラグをセット

GES1の動作

2. GES1がDDEを受信後

   ② 識別フラグをチェック

   ③ 識別フラグがあればRGIの宛先をDDEの送信元IPアドレスに変更