異なるアドレス空間を跨る DPRP の検討

02j056 後藤 裕司
渡邊研究室

1. はじめに

企業ネットワークにおける内部犯罪が増加傾向にありセキュリティ対策が重要視されている．既存のネットワークセキュリティ技術として IPsec があるがシステム構成が頻繁に変わるような環境では設定情報の変更が必要であるため，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，我々はネットワーク構成の変化に柔軟に対応できかつ運用負荷のかからない DPRP（Dynamic Process Resolution Protocol）と呼ぶ通信プロトコルを提案している．DRPP は通信に先立って通信経路上の GE（GSCIP Element）が情報を交換することにより動的に動作処理情報を生成することができる．しかし，既存の DPRP はプライベートアドレス空間とグローバルアドレス空間が混在し，通信経路上に NAT（Network Address Translation）が介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ための 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．送信側の 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のテーブル 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 を開始し PIT を生成する．DPRP は ICMP をベースとした 4 つの制御パケット DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）からなる．DDE は通信相手に最も近い GE を特定する．RGI は，通信経路上の各 GE の設定情報を収集する．この時，RGI の宛先は DDE に記載されている CID の送信元 IP アドレスに返信される．MPIT は収集した情報から決定した動作処理情報を通知する．CDN はネゴシエーションが完了を通知する．

PIT の内容は退避した通信パケットの CID から作成される．しかし，通信経路上に NAT がある場合は，通信パケットの IP アドレスが変換されるため，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．

3. ＮＡＴ越えへの対応

図 1に改良した DPRP のシーケンスを示す．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 は GNAT を通過するときに NAT としてアドレス変換が行われると共に，DDE 内に NAT を越えたという識別フラグがセットされる．DDE を受信した GES1 は，上記フラグがセットされていれば RGI の内容を GNAT 対応に変更する．RGI は GNAT でアドレス変換が行われてプライベートアドレス空間の端末に到達する．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，図 1に示すような TCP/UDP 対応の NAT 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．

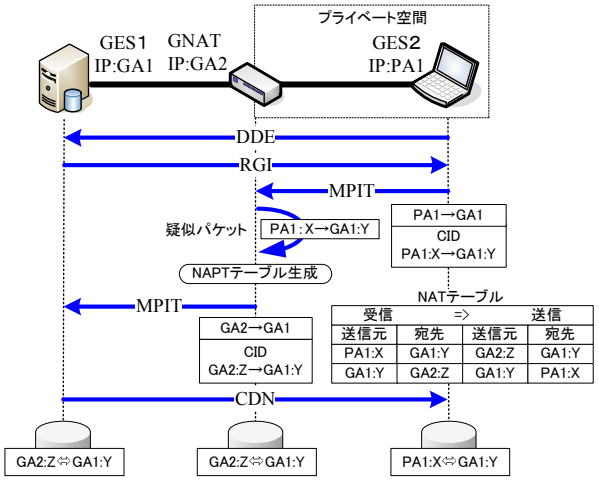


図 1 改良した DPRP のシーケンス

4. まとめ

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 DPRP を可能とするための改良方法を検討した．今後は，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 DPRP 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.

異なるアドレス空間を跨るDPRPの検討

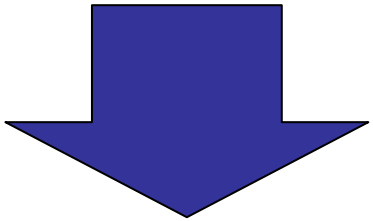
Researches on extended Dynamic Process Resolution Protocol for different types of address areas

渡邊研究室

02j056　後藤　裕司

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

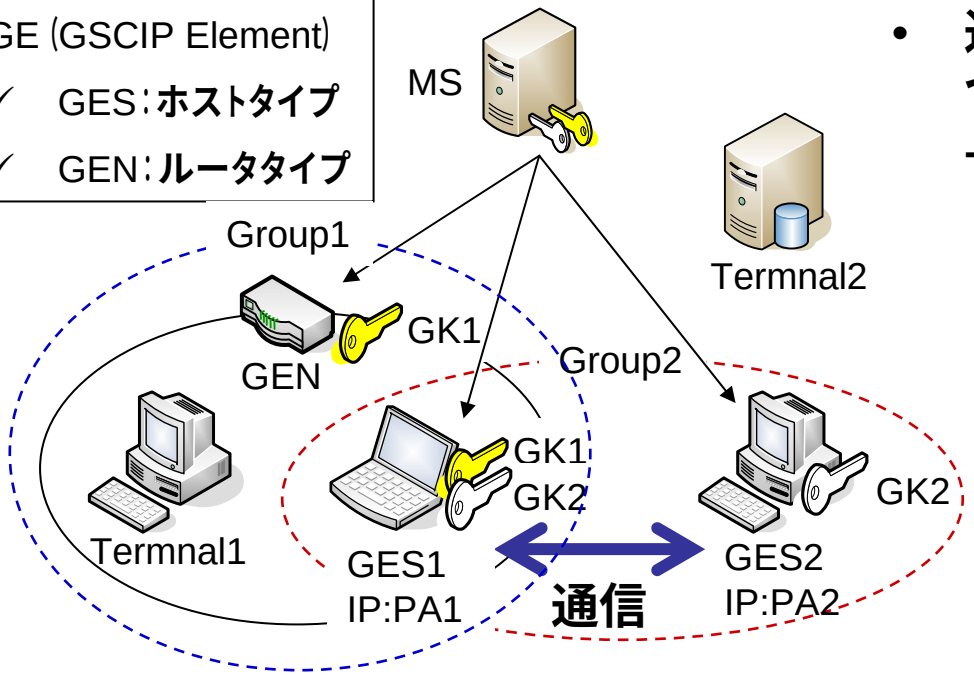


フレキシブルプライベートネットワーク
FPN（Flexible Private Network）

GSCIP (Grouping for Secure Communication for IP)

FPNを実現するためのセキュア通信アーキテクチャ

MS：管理装置
GE (GSCIP Element)
✓ GES：ホストタイプ
✓ GEN：ルータタイプ



- 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

PITの内容

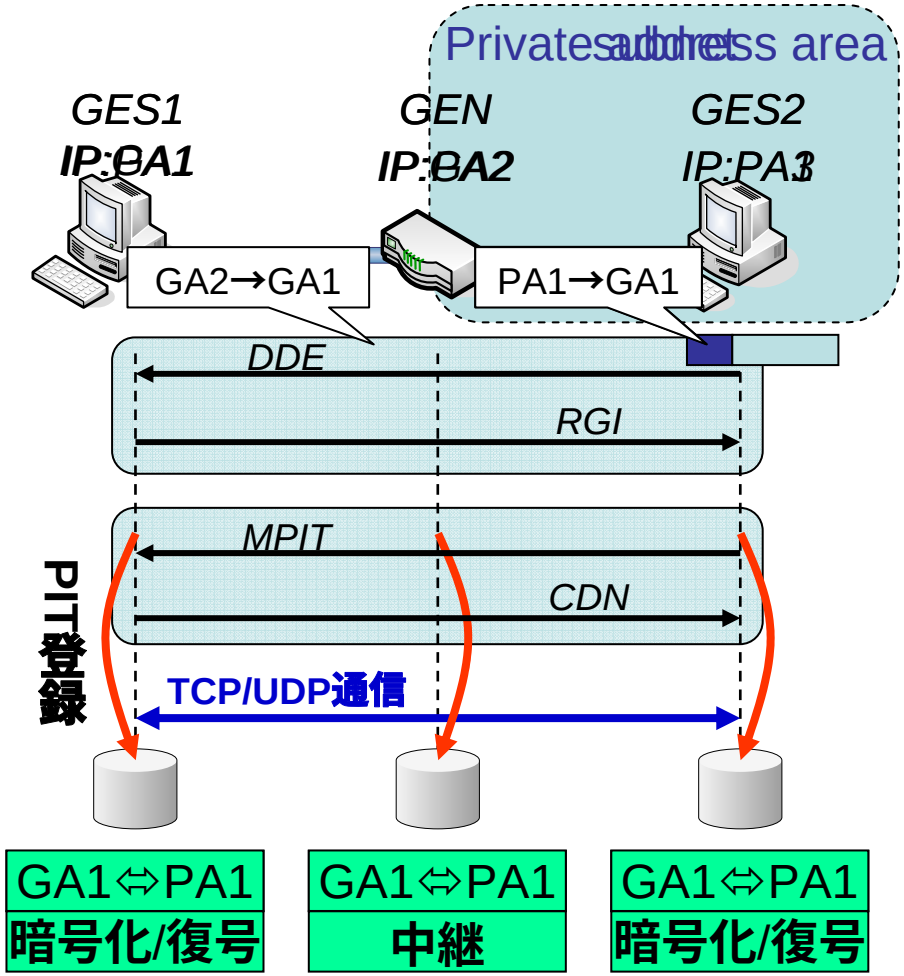
送信元・宛先：IPアドレス/ポート番号
プロトコルタイプ (TCP/UDP)
グループ鍵の番号
動作処理情報 (暗号化/復号/透過中継/破棄)

PA2⇔PA1
暗号化/復号

- GE間の通信は動作処理情報のテーブルPIT (Process Information Table) に従ってパケットを処理する
- PITがない場合→DPRPの実行

DPRP (*Dynamic Process Resolution Protocol*)

通信に先立ちDPRPネゴシエーション
を行うことでPITを生成



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**)

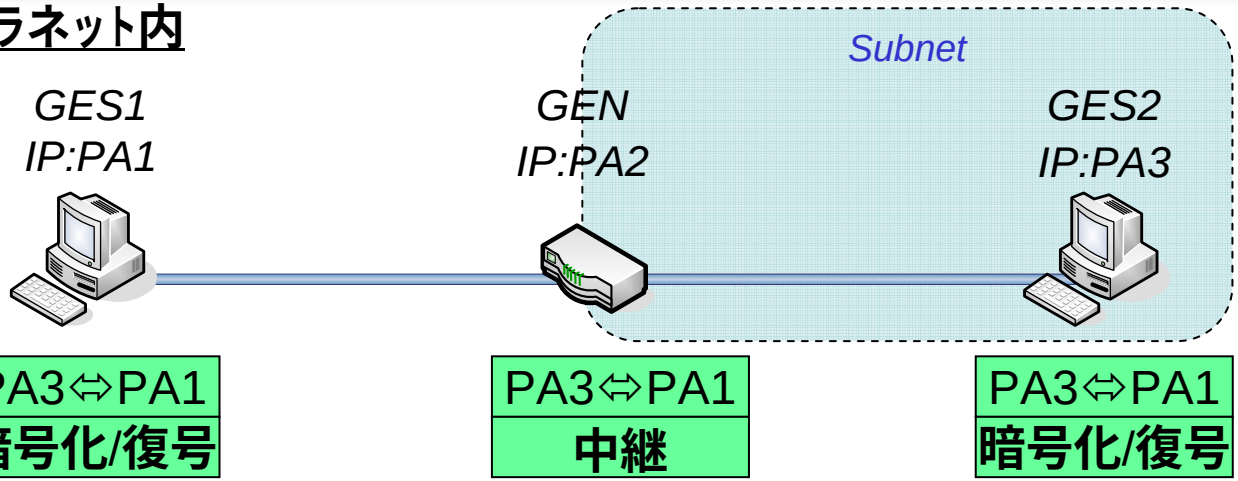
1. **通信経路上の各**GE**の設定情報を取得し動作処理情報を決定**
2. **動作処理情報を通知と**PIT**の生成**

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**

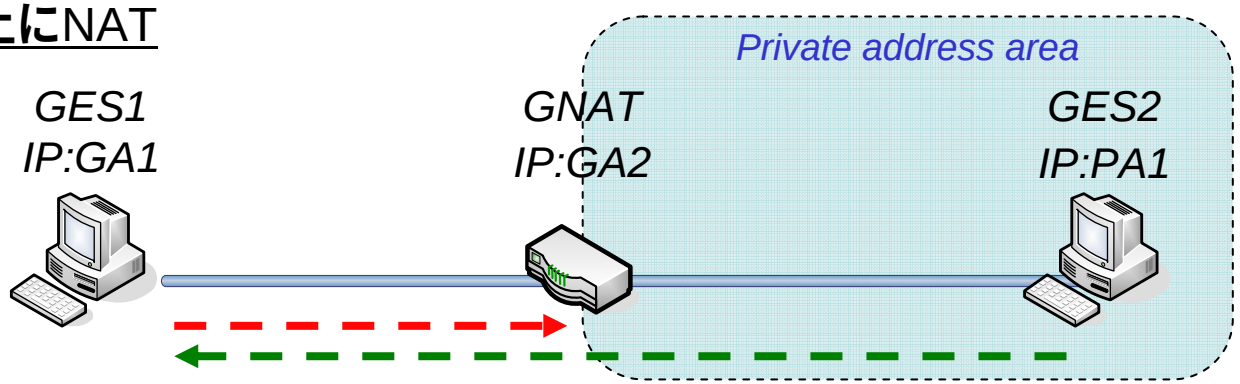
CID
送信元IP：ポート→宛先IP：ポート **プロトコルタイプ**

PITの考え方

イントラネット内

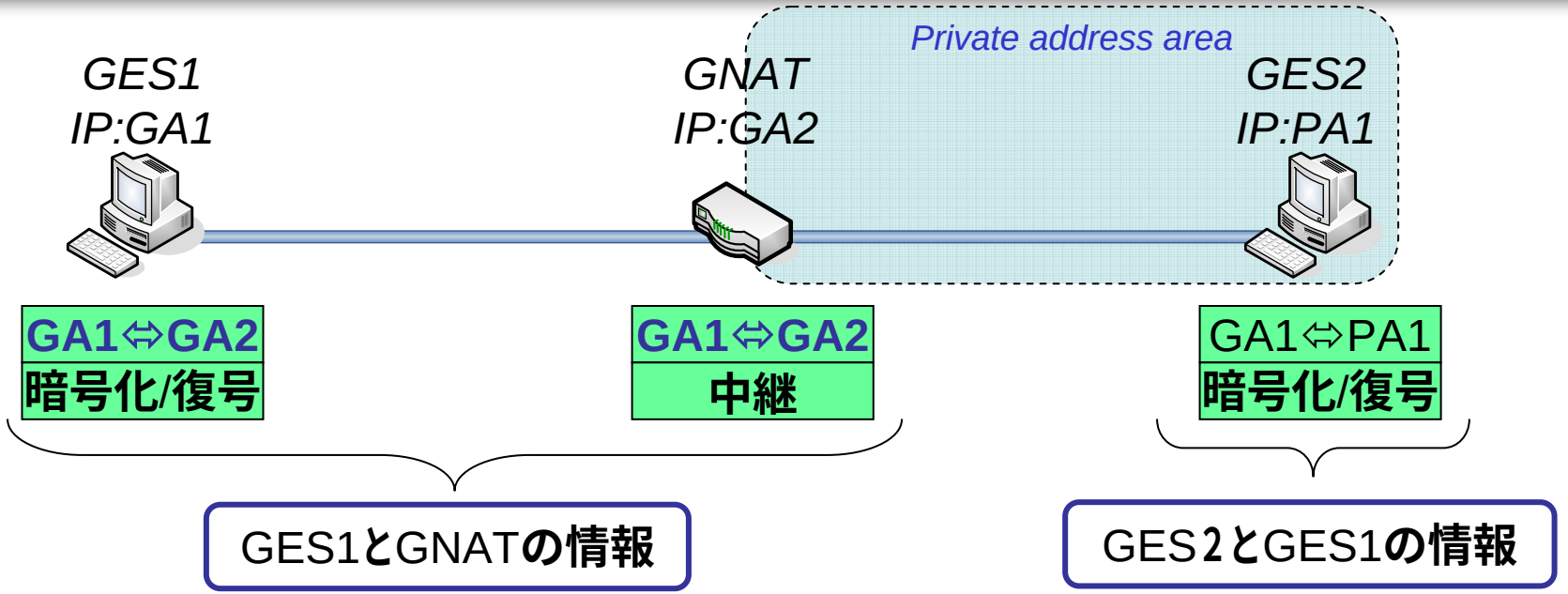


経路上にNAT



- GES2はGES1が通信相手に見える
- GES1はGNATが通信相手に見える
  - →GES1はGES2が見えない

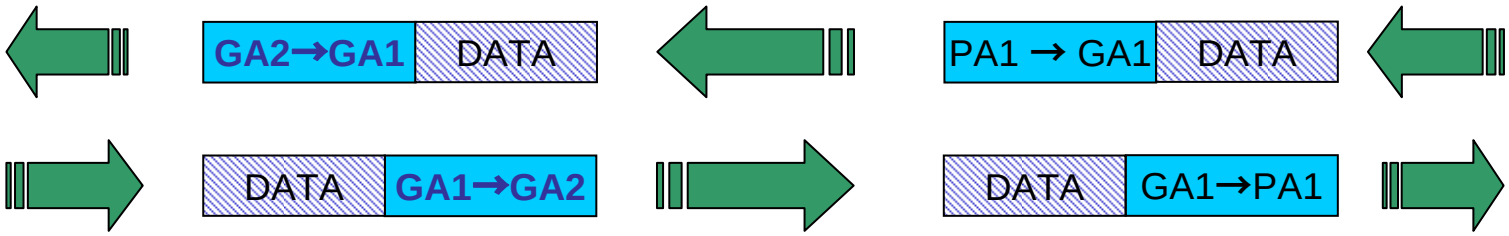
NATを意識したPIT



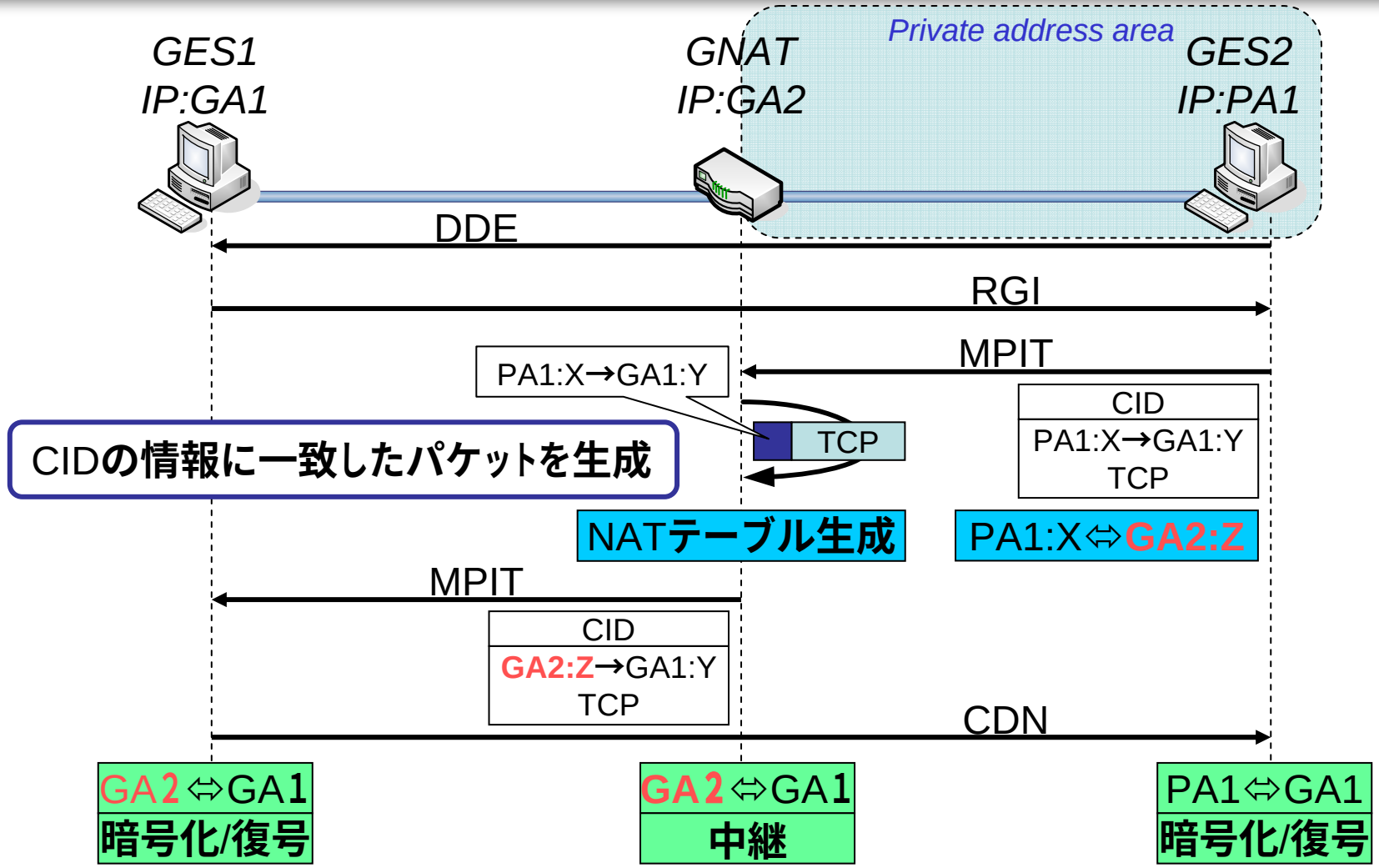
パケットの流れ

NATテーブル

GA2 ⇔ PA1



PITの生成方法

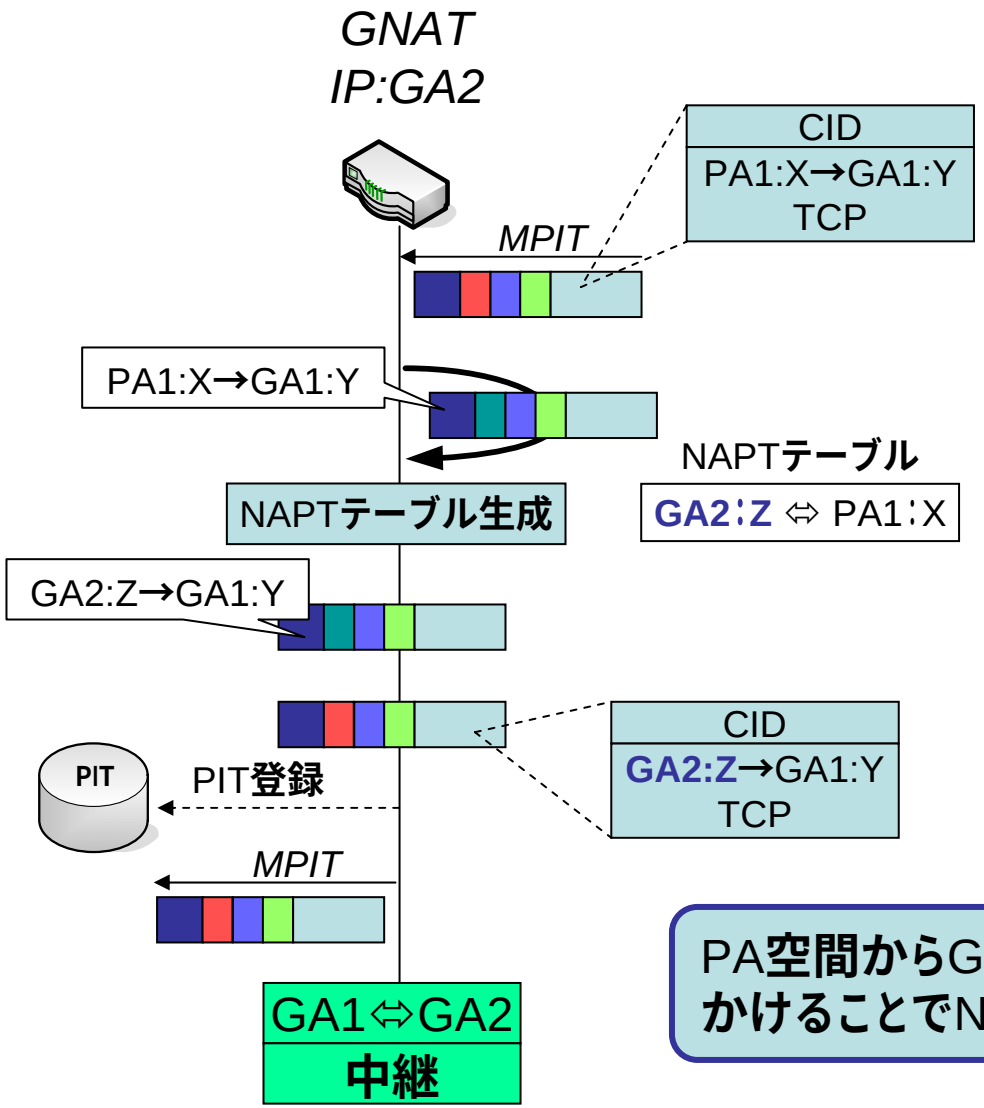


PA空間からGA空間へのDPRPが可能

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空間からGA空間へのDPRPを可能にした
  - 実装済み，動作を確認
- 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

NA(P)Tテーブルの生成

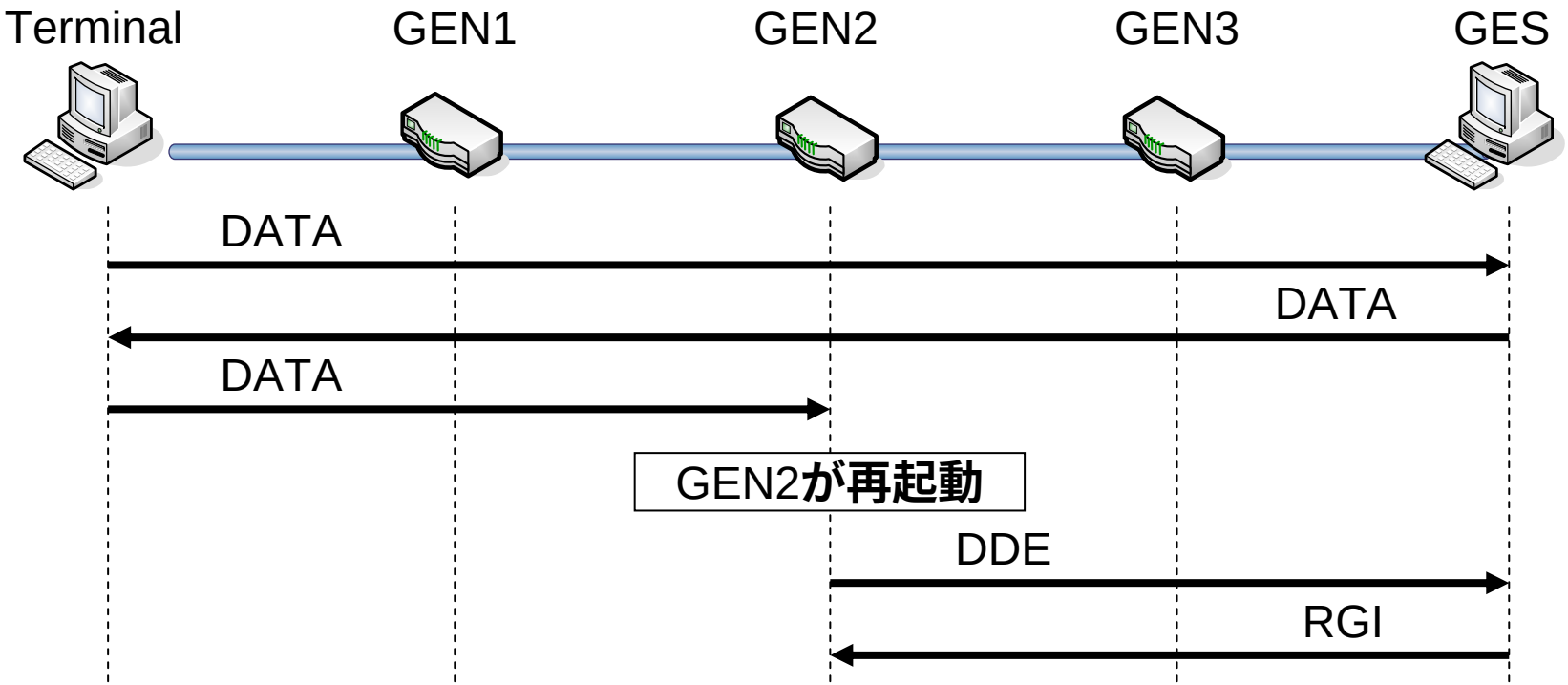


IPヘッダ　TCPヘッダ
ICMPヘッダ　DPRPヘッダ
MPITヘッダ　DATA

I. CIDを追加したMPITを受信
II. CIDの情報と一致したTCPまたはUDPパケットを生成（疑似パケット）
III. 疑似パケットの送受信
IV. NAPTテーブルを生成
V. 疑似パケットから新たにMPITを生成
VI. アドレス変換後の情報（CID）でPIT登録
VII. CIDを追加したMPITを送信

PA空間からGA空間へパケットを送るように見せかけることでNAPTテーブルを生成する

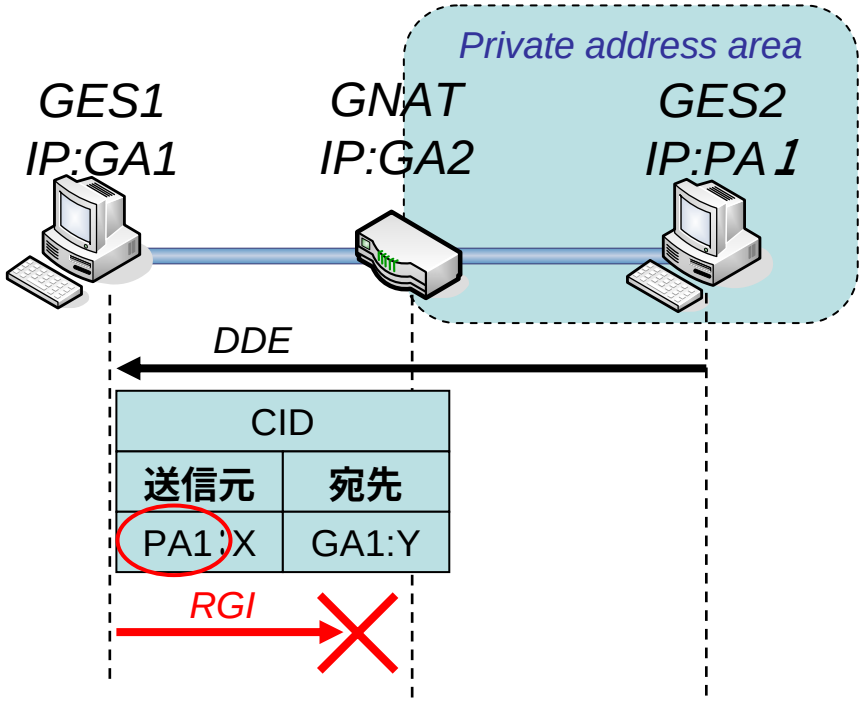
既存DPRP：RGIの宛先



- 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***

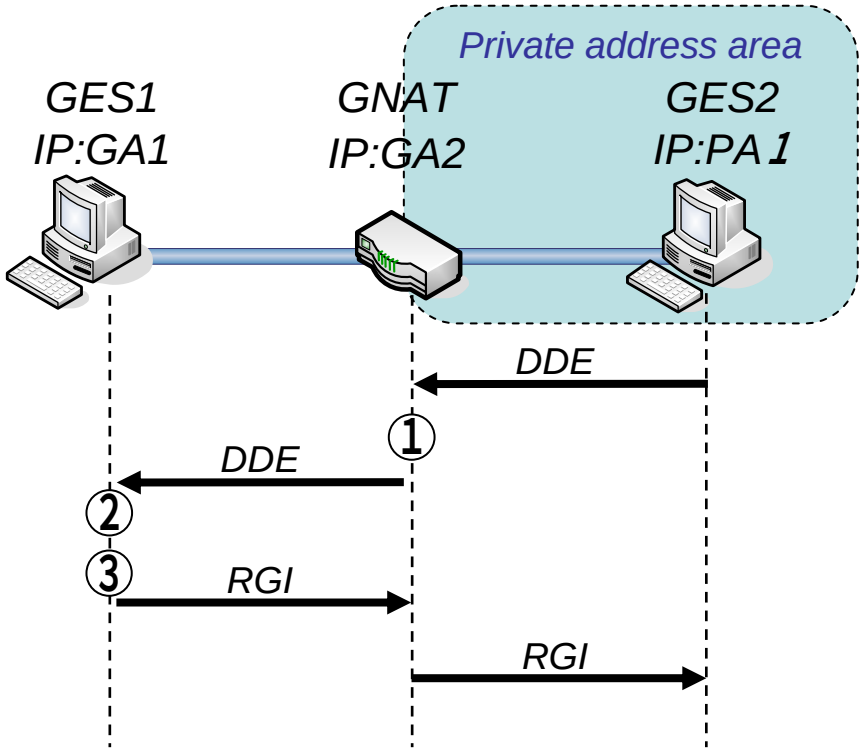
1. 通信パケットのCIDを取得
2. GES2からGES1にDDEを送信
3. GES1がDDEを受信
4. CIDの送信元IPアドレスにRGIを送信

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

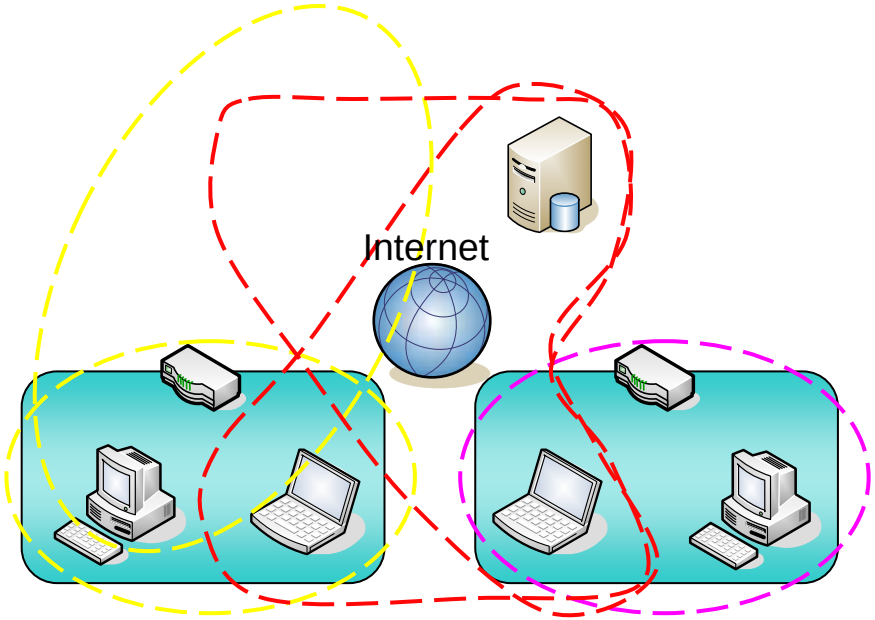
2. GES1がDDEを受信後

   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

FPN (Flexible Private Network)

柔軟でセキュアなグループ通信を可能にするネットワーク



✓同一グループ間の通信は暗号化

✓グループ外の通信は拒否

位置透過性

システム構成が変化しても自動的に学習して動作処理情報を生成

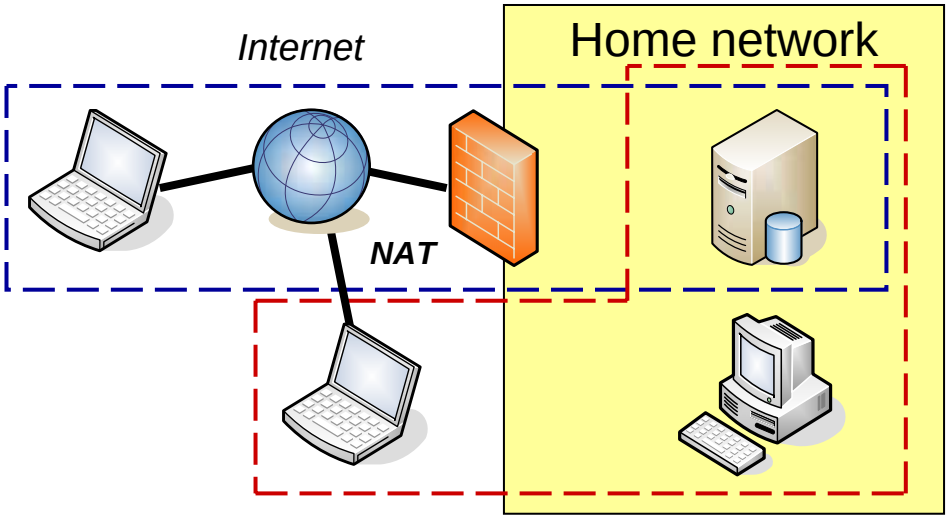
アドレス空間透過性

GA (グローバルアドレス) 空間とPA (プライベートアドレス) 空間を意識せずに通信

- PA空間→GA空間
- GA空間→PA空間

位置透過性とアドレス空間透過性の実現方法について

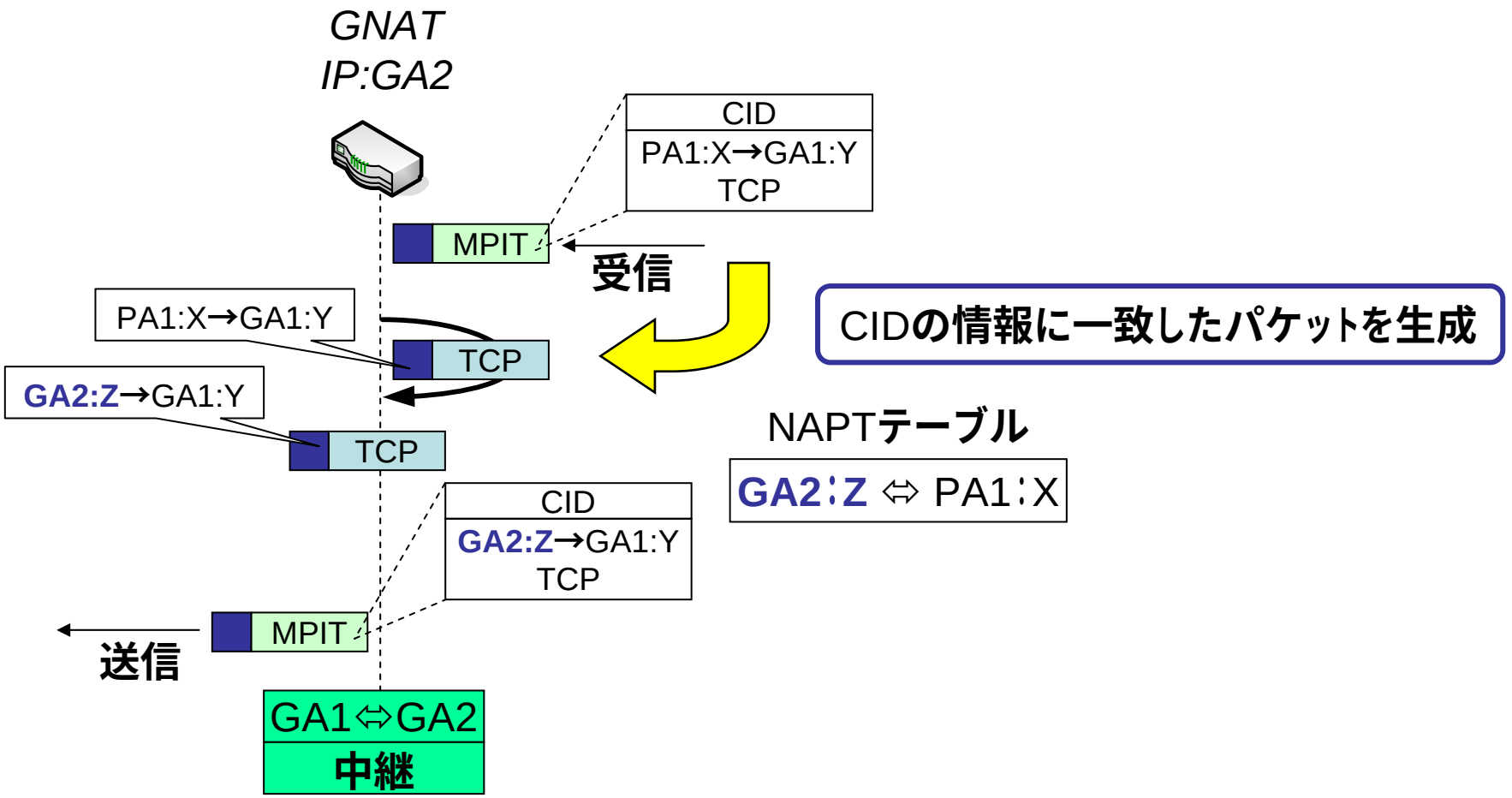
FPNの適応範囲



- 既存のDPRPは位置透過性のみに対応
  - アドレス空間透過性に対応していない
- インターネットとホームネットワークでグルーピングしたい
  - アドレス空間が異なる

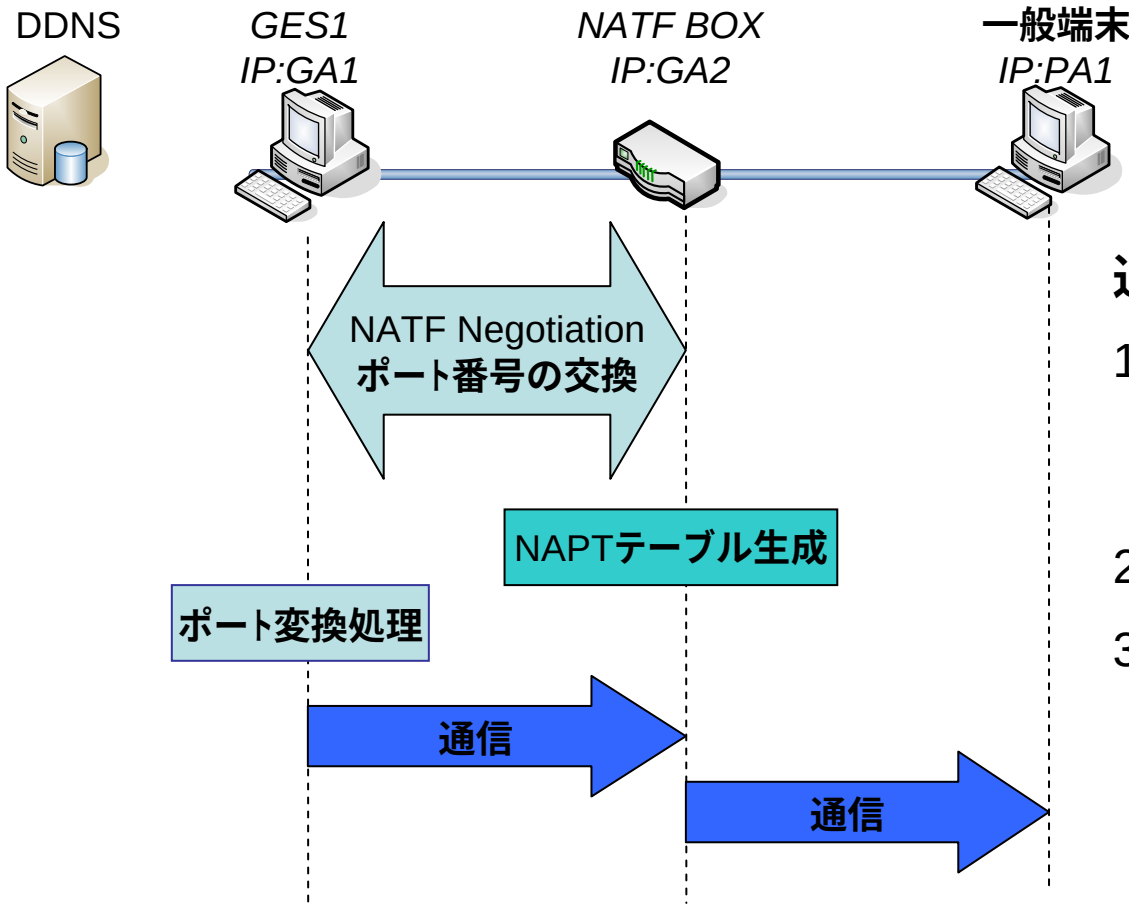
DPRPをアドレス空間透過性に対応させる

PITの生成方法



PA空間からGA空間へのDPRPが可能なる

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の交換を行う**
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**