異なるアドレス空間をまたがるDPRPの検討

後藤　裕司*,　鈴木　秀和,　渡邊　晃(名城大学)

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

Yuji Goto,　Hidekazu Suzuki,　Akira Watanabe (Meijo University)

１．はじめに

近年増加傾向にあるイントラネット内部の犯罪に対するセキュリティ対策が重視されている．既存技術の一つとしてIPsecが考えられるが,頻繁にシステム構成が変わるような環境では設定情報の変更作業が大きく，イントラネット内ではほとんど利用されていない．そこで我々は柔軟なネットワーク構成に対応できシステム構成の変化を動的に管理するためにDPRP(Dynamic Process Resolution Protocol)[1]を提案してきた.DPRPは通信に先立って通信経路上に存在するGE（Grouping Element）の情報を交換することで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NAT（Network Address Translation）に対応していないため異なるアドレス空間をまたがる通信環境では利用することができない．本稿では、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における NAT 越えDPRPについて検討した.

２．既存の DPRP とその課題

図 1 を用いてシステム構成ついて説明する．GES とはDPRP に対応した装置で，GES1 はグローバルアドレス，GES2はプライベートアドレスを持つ装置である.また経路上には必ず NAT が存在する．DPRP では DDE（Detect Destination End GE)，RGI（Report GE Information)，MPIT（Make Process Information Table)，CDN（Complete DPRP Negotiation)と呼ぶ4つの制御パケットを用いて動作処理情報の決定をしてPIT(Process Information Table)を生成する.端末は通信パケットを送受信時に PIT の内容に従ってパケットの処理を行う．該当する PIT が存在しない場合はパケットを一時的に待避してDPRPによりPITを生成する.DDEにはコネクション識別情報 CID（Connection Identification）が含まれており,NATが介在しない場合にはDDEを受信したGEはCIDに含まれる送信元IPアドレスをRGIの宛先として返信する．以降，この CID をもとにして MPIT によりPITが生成される.上記のような動作原理から図1のようにNATが介在する構成では，RGIの宛先がプライベートアドレスになってしまい，送信することができない．またグローバルアドレス空間側の端末ではCIDにより伝えられたプライベートアドレスを用いて PIT を生成してしまうため，NATでアドレス変換されたパケットに関するPITが存在しないという問題が発生する.

３．NAT 越え DPRP の検討

図1に改良後のDPRPのシーケンスを示す．RGIの宛先がプライベートアドレスになる問題を解決するためにNATはDDEが通過するときにNATを通過したという情報をパケット内に記述する．DDEを受信したGES1はその情報を読み取るとRGIの宛先をDDEの送信元であるNATに変更する．これにより，RGIはNATを通過してプライベート空間のGES2に到達することができる．次にNATはMPITを受信後に通信用のNAPTテーブルを強制的に生成し，MPITの内容を変換後のアドレスとポート番号に書き換える．これにより，GES1はNATとの間でPITを生成する．以上の改良によりNATを超えたDPRPを行うことが実行することが可能になる.

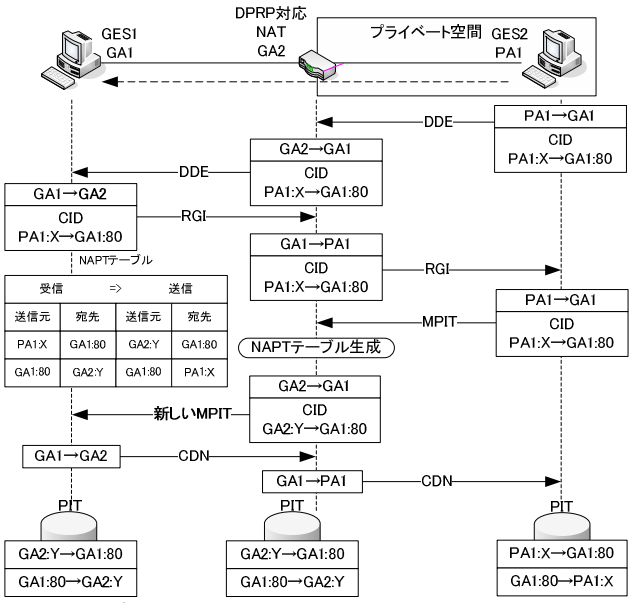


図１　プライベート空間からグローバル空間へのDPRP

4. むすび

本稿ではDPRPがNATを超えるために必要な改良点について検討した．今後は改良版 DPRP の動作確認を行う．また逆方向の通信となる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 について検討を行い，双方向の NAT 越えが可能な DPRP の実現を目指す.

文献

[1]　鈴木 秀和: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 の仕組み、第 26 回 CSEC 研究発表会，July 2004

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

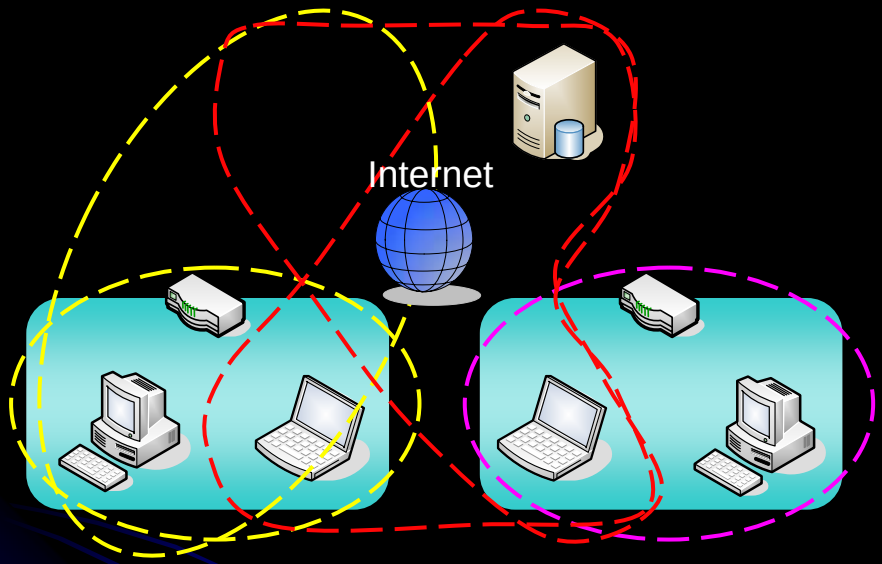
研究背景

- 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*)

柔軟かつセキュアなグループ通信を可能とするネットワーク



同一グループのメンバ間の通信は暗号化

位置透過性

システム構成が変化してもシステム情報が維持される

移動透過性

通信中に移動しても通信が継続される

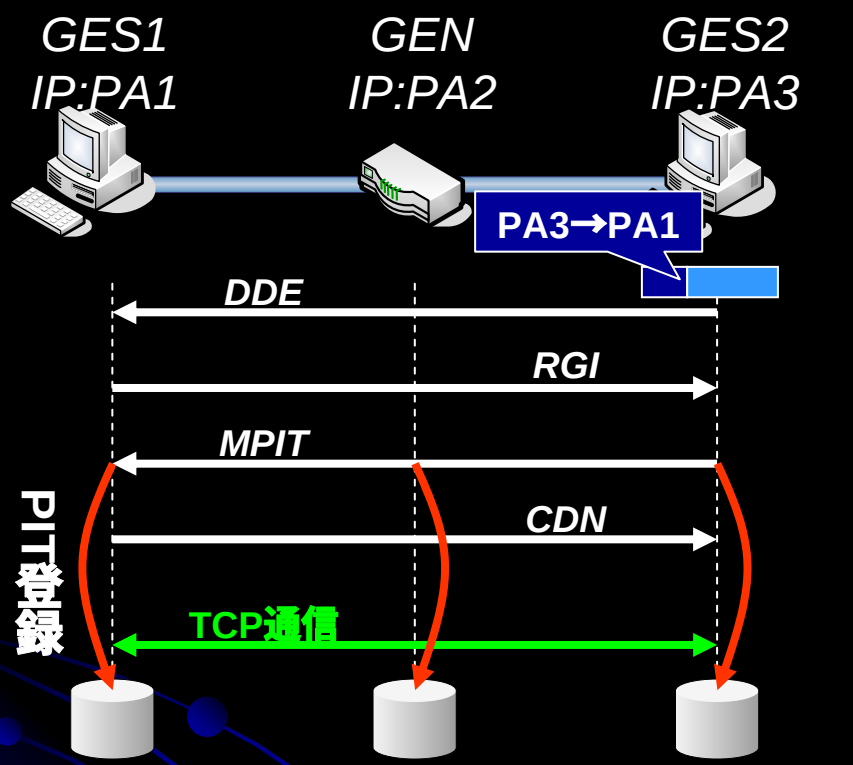
アドレス空間透過性

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

- PA空間→GA空間
- GA空間→PA空間

今回は位置透過性とアドレス空間透過性の実現方法について発表

DPRP (Dynamic Process Resolution Protocol)



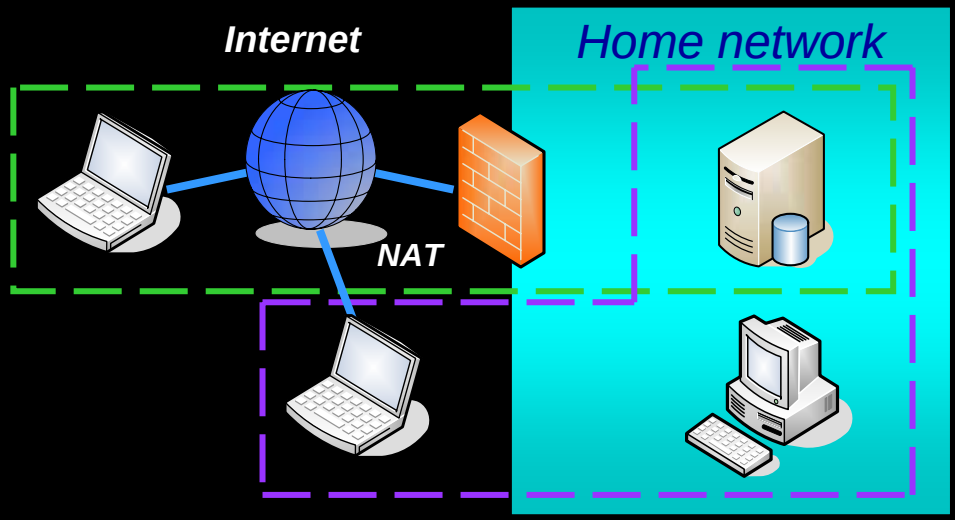
- 通信に先立ってDPRP Negotiationを開始
- 4つのDPRP制御パケットで動作処理情報テーブルPIT (Process information Table) を作成

- DDEでCID (Connection ID) を報告
- CIDの送信元IPに対してRGIを応答
- MPIT通過時に PITを生成
- CDNでDPRP Negotiationの完了を通知

CID (Connection ID)
送信元IP：ポート → 宛先IP：ポート
プロトコル

動作処理情報テーブル (PIT)
CID, **動作処理情報など**

FPNの適用範囲

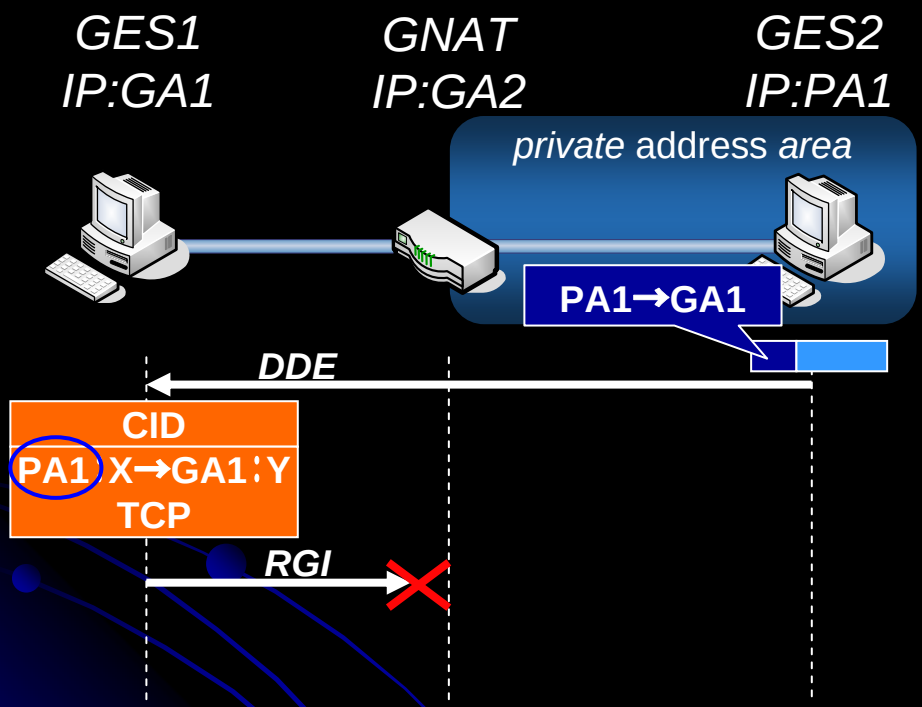


- 既存のDPRPは位置透過性にのみ対応
  - アドレス空間透過性に対応していない
- インターネットとホームネットワークでグルーピングしたい
- アドレス空間が異なっている

DPRPをアドレス空間透過性に対応させる必要がある

DDEに対するRGIの応答

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***

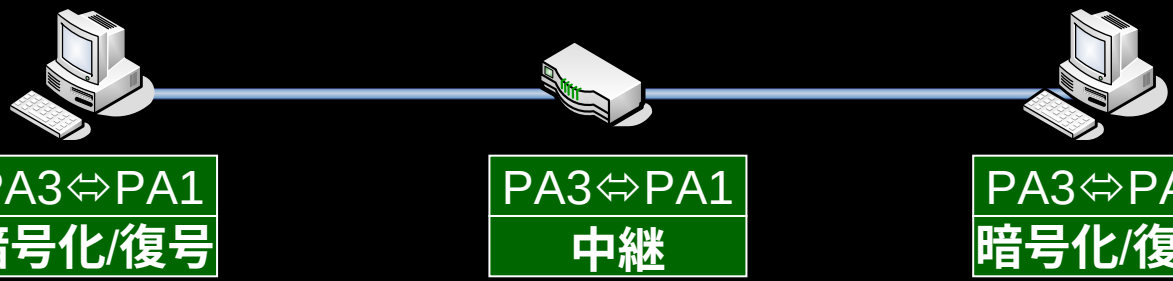
GENにNAT機能を追加：***GNAT***

1. トリガーとなるパケットからCID取得
2. DDEをGES2からGES1に送信
3. GES1がDDEを受信
4. DDEに含まれるCIDの送信元IPをRGIの宛先IPとする

RGIの宛先IPがPAのためRGIを送信することができない

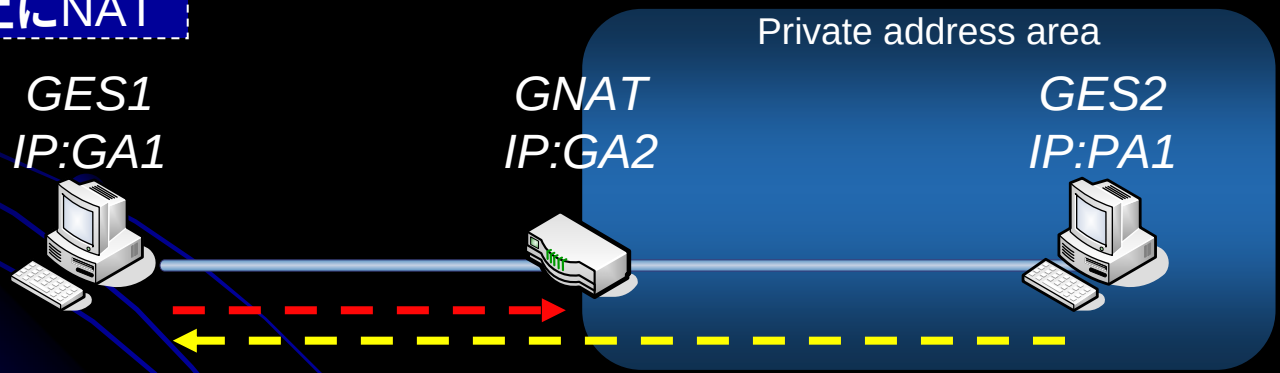
PITの考え方

イントラネット内



PIT
IPアドレス/ポート番号のペアに対する動作を規定したもの

経路上にNAT



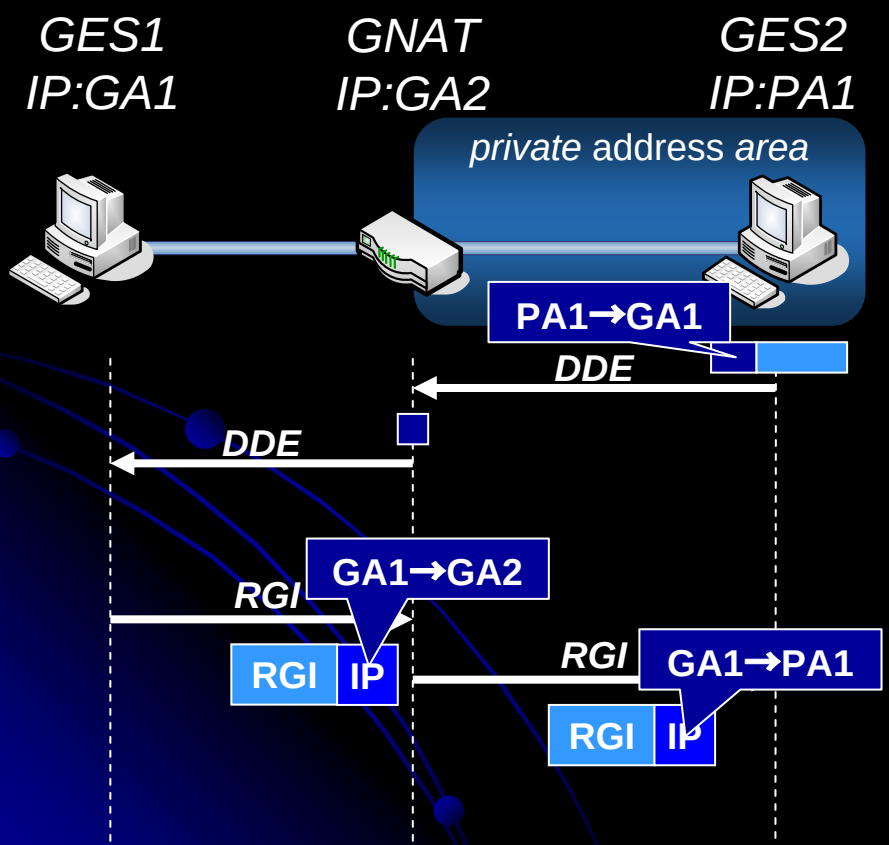
GES1はGNATが通信相手に見える

→GES1はGES2が見えない

GES2はGES1が通信相手に見える

解決方法1：NAT通過フラグの定義

- DDEに通過フラグを定義
- RGIの宛先をGNATに変更する



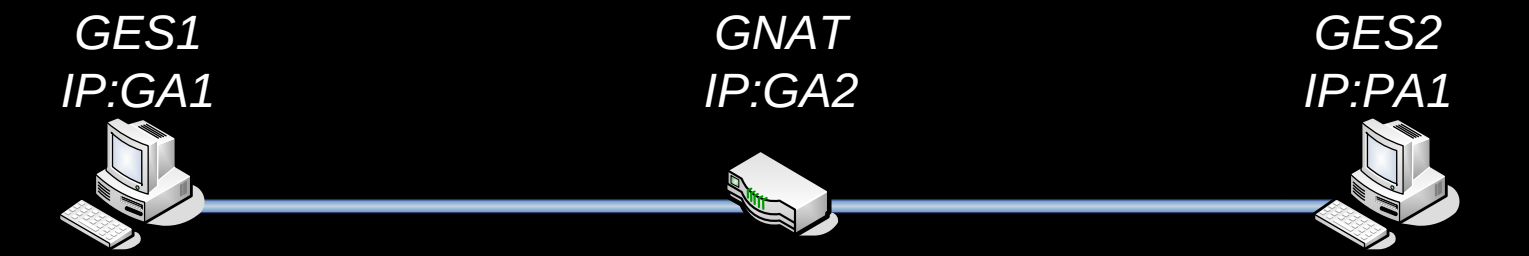
GNATの変更点

NAT通過フラグをオンにする

GES1の処理

NAT通過フラグがオンであった場合
RGIの宛先をPA1ではなくパケットの送信元のGA2に変更

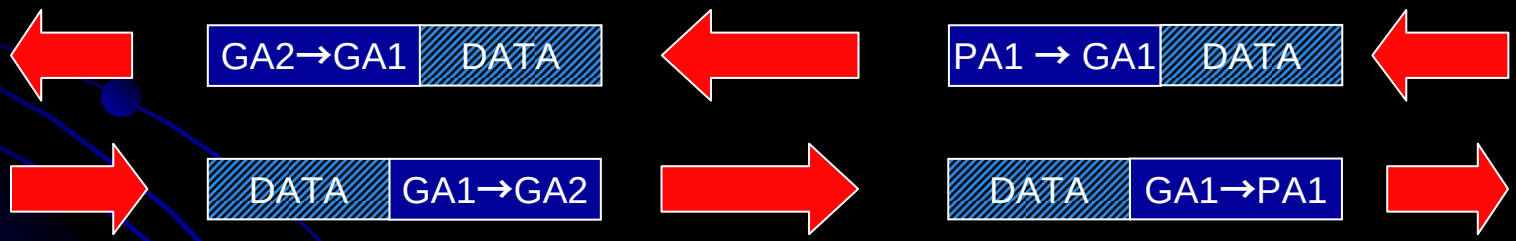
解決方法2：NATを意識したPITの生成



NATテーブル

PA1⇔GA2

パケットの変化



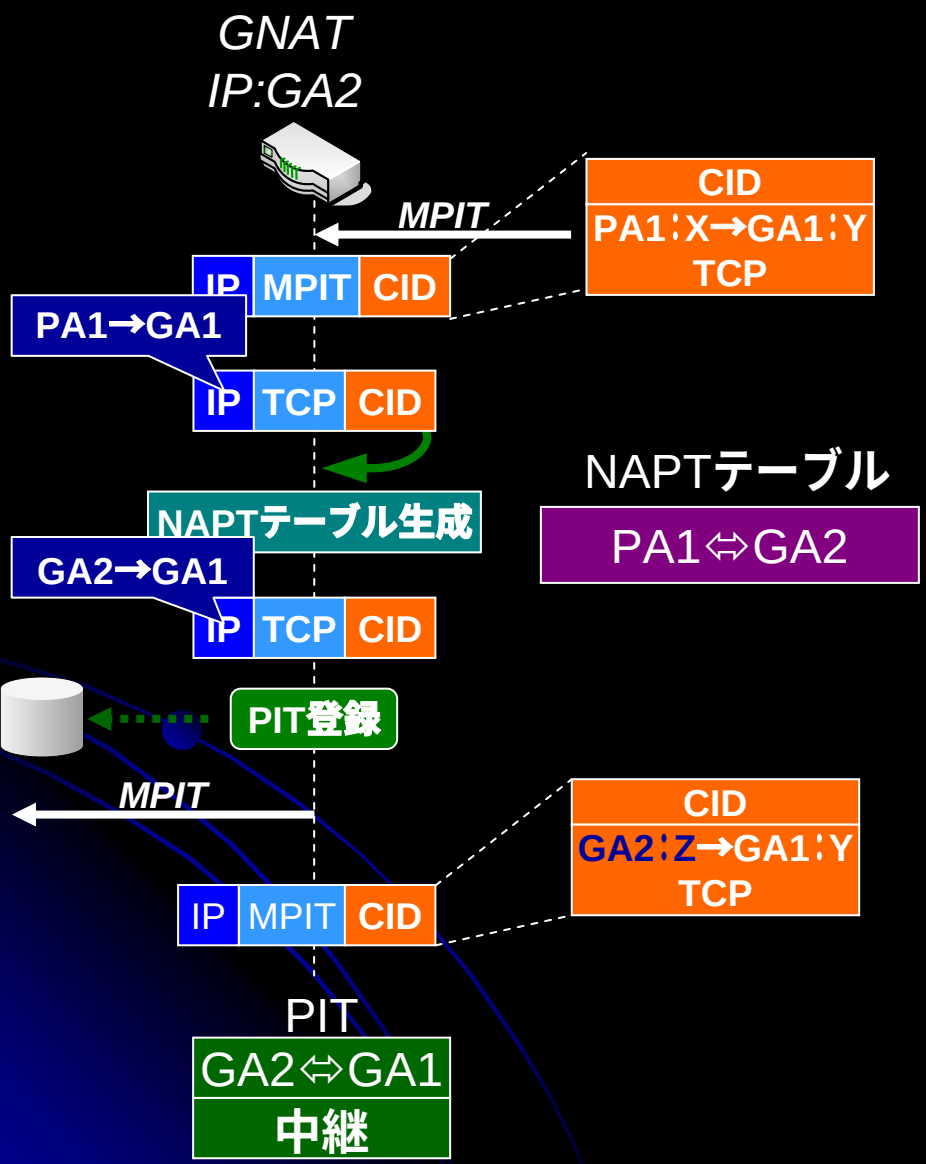
暗号化

PA空間からGA空間へのDPRPが可能

まとめ

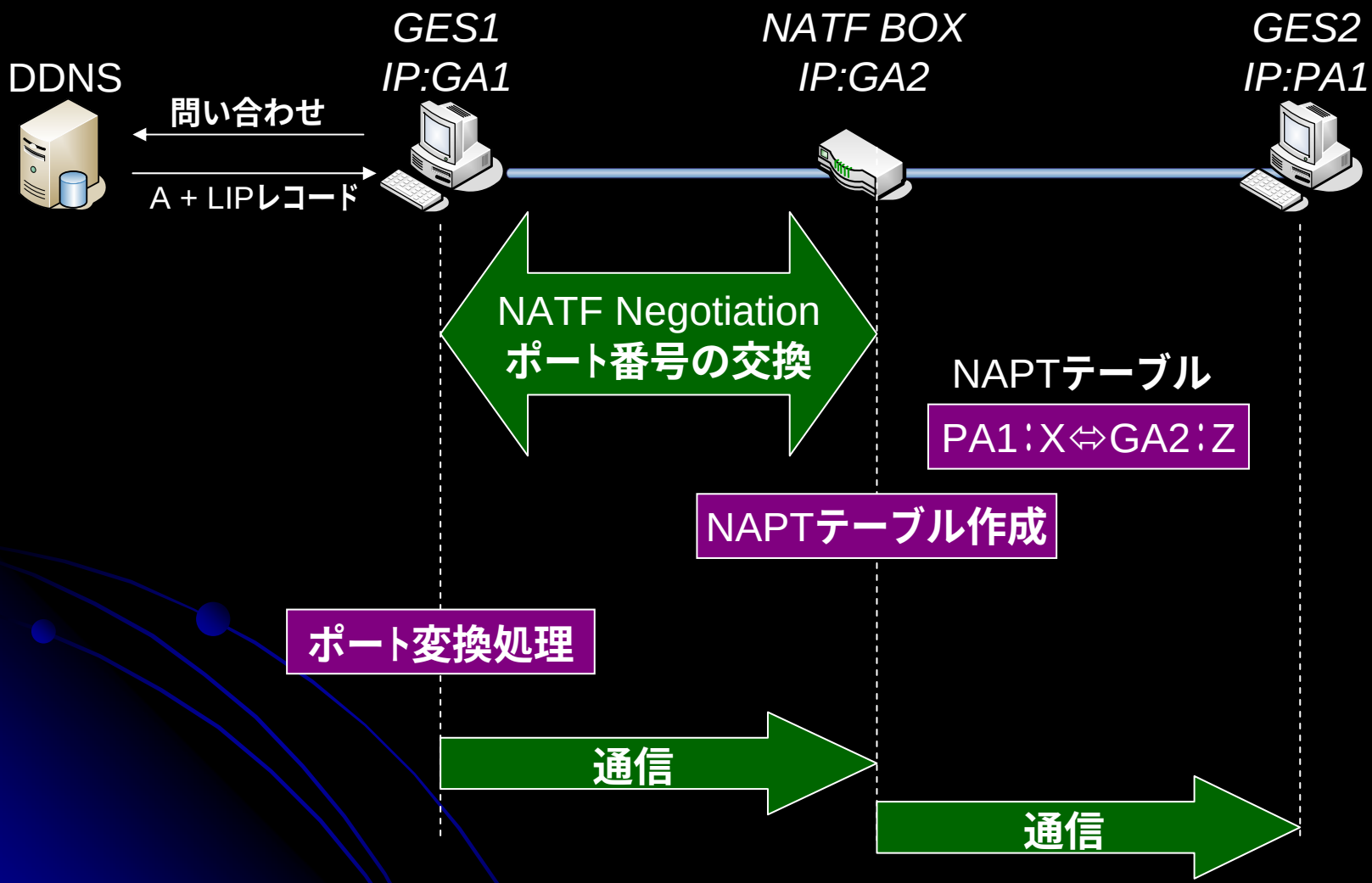
- 異なるアドレス空間をまたがるDPRPの提案
  - 既存DPRPの課題とその解決方法
  - PA空間からGA空間へのDPRPが可能
- 今後の課題
  - 実装
  - GA空間からPA空間へのDPRPの検討

NATのMPIT受信時の処理



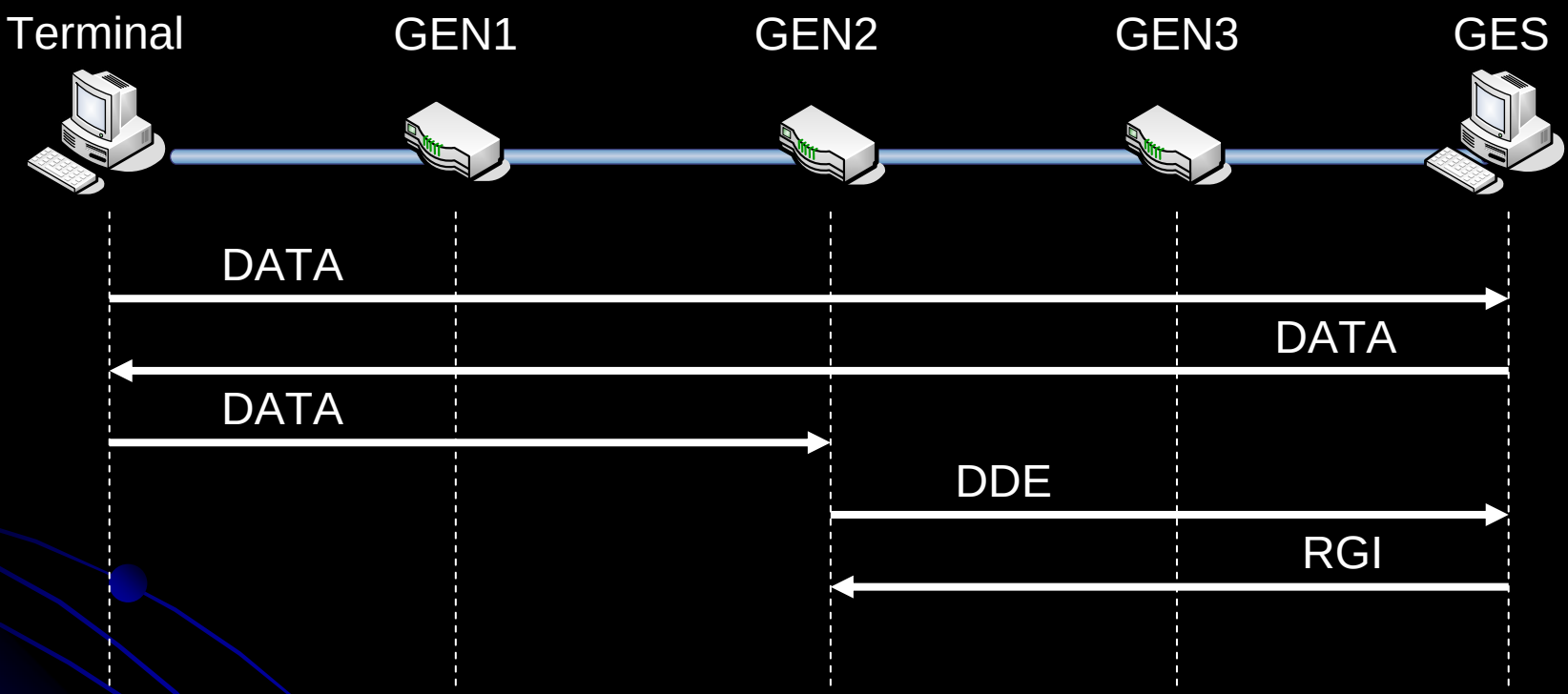
I. CIDを追加したMPITを受信
II. CIDを元に疑似パケットを作る
III. NAPTテーブルを生成
IV. 変換後のアドレスとポート番号でCIDを作成
V. 変換後のCIDを追加したMPITを新たに作成して送信

NATF（NAT Free protocol）の概要



RGIの宛先

RGIの宛先がパケットの送信元であった場合



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が作成できない