NAT 越え技術を応用したリモートアクセス方式の提案と設計

060427330 鈴木 健太
渡邊研究室

1. はじめに

近年のモバイルブロードバンドの普及や，モバイル端末の高性能化に伴い，リモートアクセスのニーズが増加している．リモートアクセスを実現するための既存の方式として，IPsec-VPN と SSL-VPN がある．しかし，IPsec-VPN は設定項目が複雑であり，利用するためには相応の知識が必要となる．SSL-VPN は専門的な知識は必要ないものの，使用できるアプリケーションが限定されるという課題がある．

本稿では，NAT 越え技術に基づいたリモートアクセス方式 GSRA（Group-based Secure Remote Access）を提案し，Windows クライアントへの実装方法を検討する．

2. 提案方式の概要

GSRA は，我々が提案した NAT 越え技術 NAT-f（NAT-free Protocol）[1] を利用し，通信グループを設定することにより，アクセス制御とサービス制御を行う．インターネット上のトラフィックは PCCOM[2] により暗号化する．

GSRA 使用時のネットワーク構成例を図 1 に示す．GSRA の機能を実装したルータを GSRA ルータと呼び，リモート先のネットワークに GSRA 専用のゲートウェイとして設置する．リモートアクセスを行う端末を EN（External Node），アクセス先の端末を IN（Internal Node）と表記する．EN は同一グループに所属している IN1 と通信可能であるが，異なるグループの IN2 とは通信できない．IN のグループ情報は GSRA ルータに登録されている．

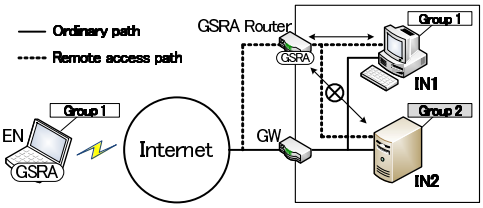


図 1: ネットワーク構成例

3. 提案方式の実装

GSRA は NAT-f と PCCOM を利用するが，これらは FreeBSD に実装されている．そのため，これらを用いて GSRA も FreeBSD での実装を完了させたが，FreeBSD はクライアント OS として一般的ではなく，今後の GSRA の普及のためには Windows への実装が不可決である．

現在の FreeBSD における GSRA の実装は，IP 層を直接改造することで実現されている．しかし，Windows OS はブラックボックスであり，直接改造することはできない．その代わりに，機能を拡張するためのインタフェースがいくつか公開されている．本稿では TCP/IP スタックに干渉できる API として WFP（Windows Filtering Platform）に着目し，Windows へ GSRA を実装する方法を検討する．

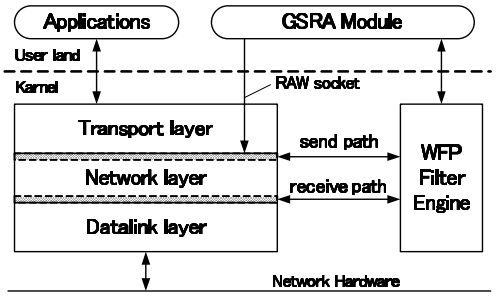


図 2: Windows における GSRA システム設計

3.1 WFP の概要

WFP では，ネットワークスタック中の特定のポイントに，パケットをフィルタリングエンジンへ渡すためのフィルタリングレイヤが定義されている．このレイヤ ID を指定して任意のフィルタやコールアウトを登録することで，トラフィックの監視やパケットの書き換え等を行うことができる．

3.2 WFP を利用した実装

図 2 に設計概要を示す．パケット送信時は，ネットワーク層最上部に登録したフィルタによってパケットをフックし，GSRA モジュールへ渡す．GSRA モジュールでは，アドレス変換等，必要な処理を行った上で，フィルタリングエンジンを通してパケットを元の流れへと返す．GSRA 制御用パケットは，RAW ソケットを使用して送信する．

パケット受信時は，ネットワーク層最下部に登録したフィルタによりパケットをフックする．これは PCCOM が独自の TCP/UDP チェックサム計算を行っており，TCP/IP スタックにおけるチェックサム検証時にパケットが破棄されることを防ぐためである．

以上の設定により，Windows に GSRA を実装することができると考えられる．

4. まとめ

NAT 越え技術に基づいたリモートアクセス方式 GSRA を提案し，Windows クライアントへの実装方法を検討した．今後は検討した設計に従い実装を行い，性能を評価する．

参考文献

[1] 鈴木秀和, 宇佐見庄五, 渡邊晃. 外部動的マッピングにより NAT 越えを実現する NAT-f の提案と実装. 情報処理学会論文誌, Vol. 48, No. 12, pp. 3949–3961, Dec. 2007.

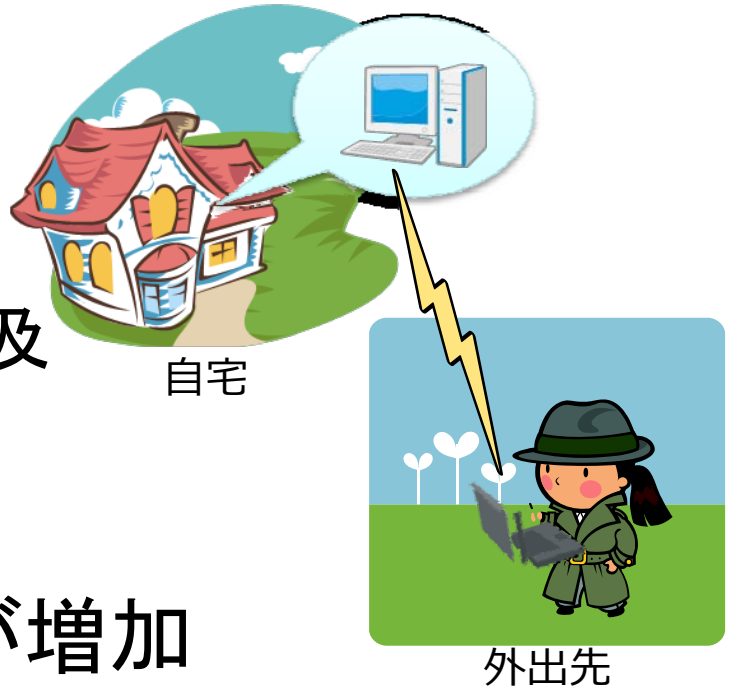
[2] 増田真也, 鈴木秀和, 岡崎直宣, 渡邊晃. NAT やファイアウォールと共存できる暗号通信方式 PCCOM の提案と実装. 情報処理学会論文誌, Vol. 47, No. 7, pp. 2258–2266, July. 2006.

NAT越え技術を応用したリモートアクセス方式の提案と設計

渡邊研究室
060427330　鈴木　健太

リモートアクセスとは

- 研究背景
  - モバイル端末の高性能化
  - モバイルブロードバンドの普及



リモートアクセス のニーズが増加

- 遠隔地から社内や家庭のネットワークに接続し，資源を利用する技術
  - 用途：ファイルの参照，アプリケーションの実行など
  - 利用例：FirePass

既存のリモートアクセス

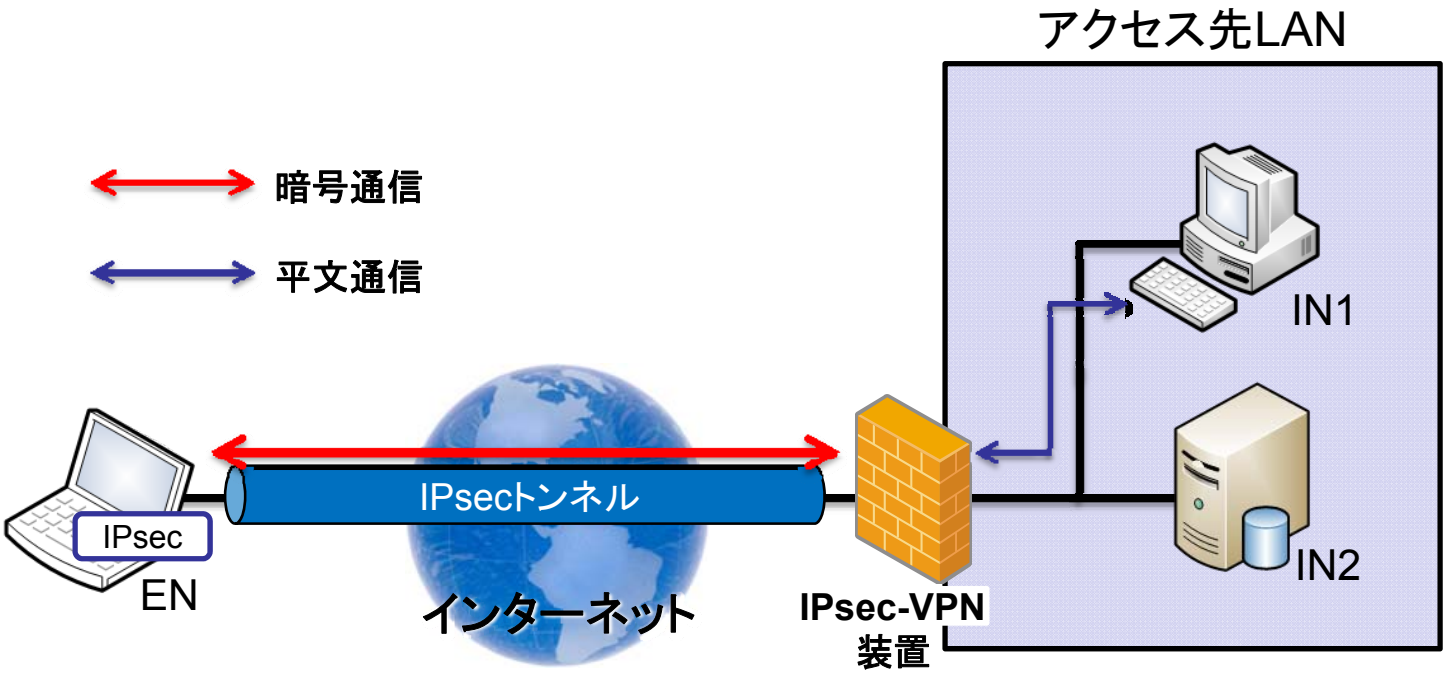
- インターネットVPNを利用したリモートアクセス
  - インターネットVPN
    - インターネット上にVPNを構築する
    - 複数箇所の拠点を低コストで接続できる
  - インターネット上の脅威
    - 盗聴，改ざん，なりすまし．．．

暗号化技術に基づいたVPN
既存方式：IPsec-VPN，SSL-VPN

VPN(Virtual Private Network)：仮想プライベートネットワーク

既存方式：IPsec-VPN

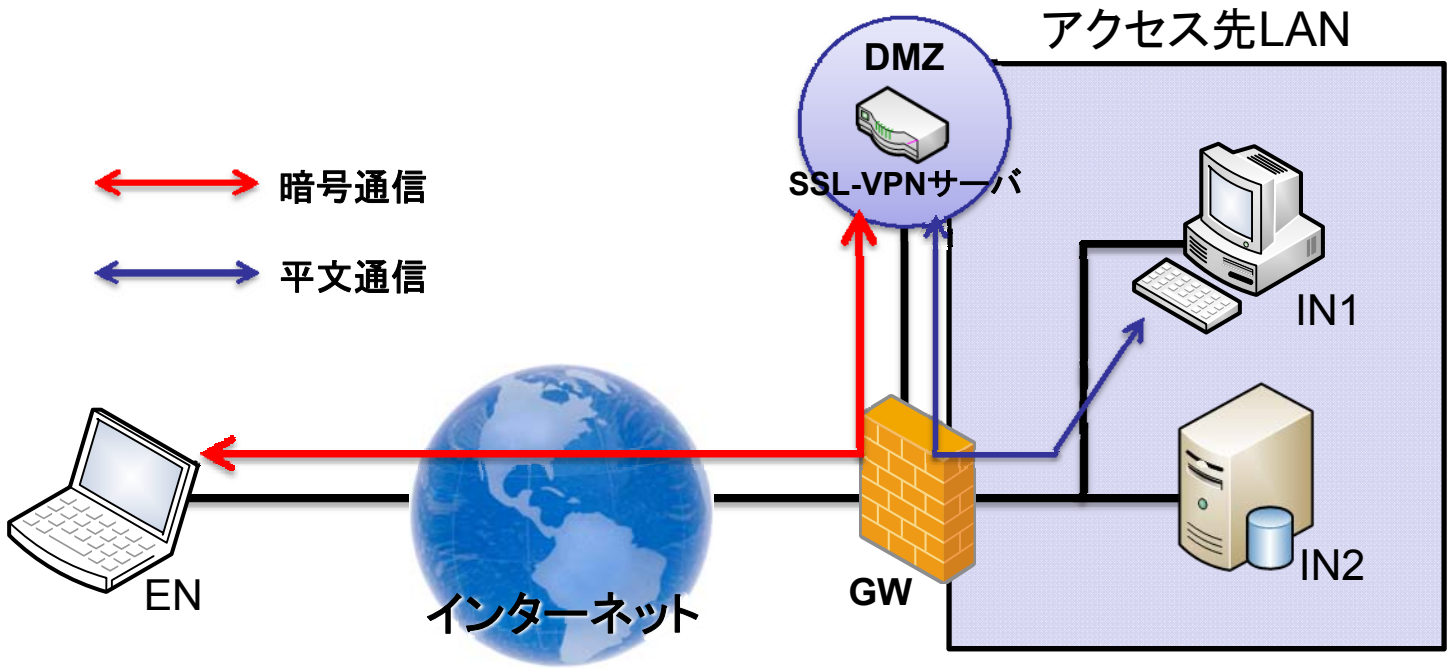
- IPsecトンネルを利用してVPNを構築する
- IPレベルで暗号化：アプリケーションに依存しない
- 運用に専門知識が必要で管理負荷が大きい



EN(External Node)：外部ノード　IN(Internal Node)：内部ノード

既存方式：SSL-VPN

- DMZ上のSSL-VPNサーバがプロキシの役割
- EN側にはWebブラウザさえあれば使用できる
- アプリケーションが限定される



DMZ(DeMilitarized Zone)：非武装地帯

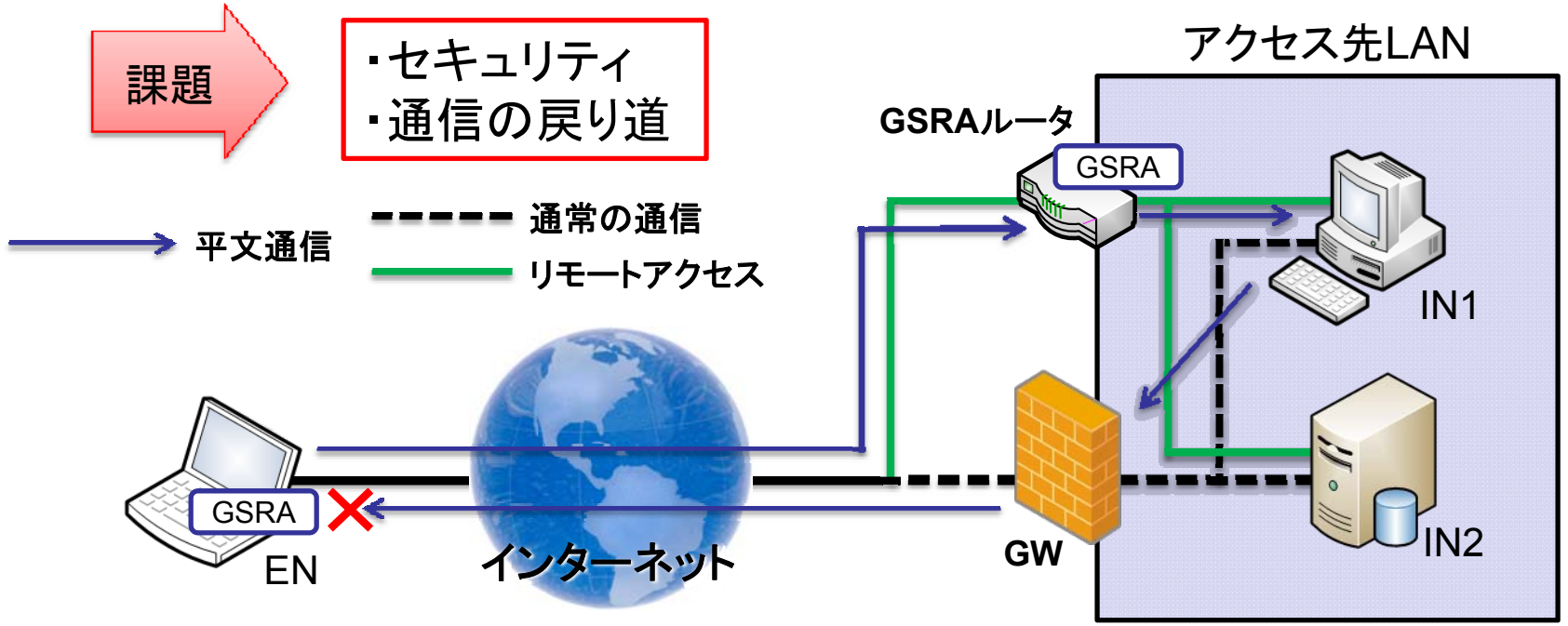
提案方式

- GSRA(Group-based Secure Remote Access)
  - NAT越え※技術を基盤とする
    - NAT-f(NAT-free protocol)
  - 既存のGWには改造を加えない
    - GSRAルータ：専用のGW

※NAT越え問題
NAT(Network Address Translation)の外側から通信を開始できない

課題

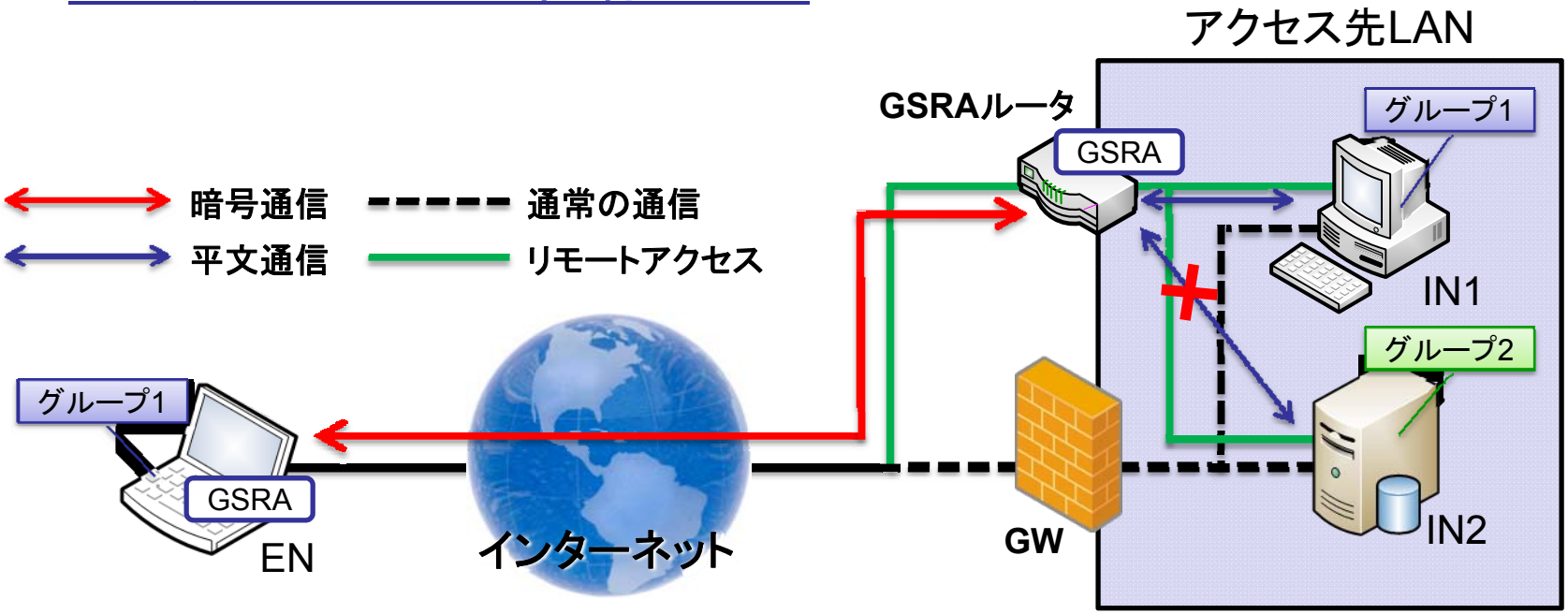
・セキュリティ
・通信の戻り道



GSRA：概要

PCCOM（Practical Cipher Communication Protocol）

- INからはGSRAルータが通信相手に見える
- パケットはPCCOMにより暗号化
- 通信グループを定義してアクセス制御
  - 端末ごとの制御に比べ管理負荷を軽減
- アプリケーションに依存しない



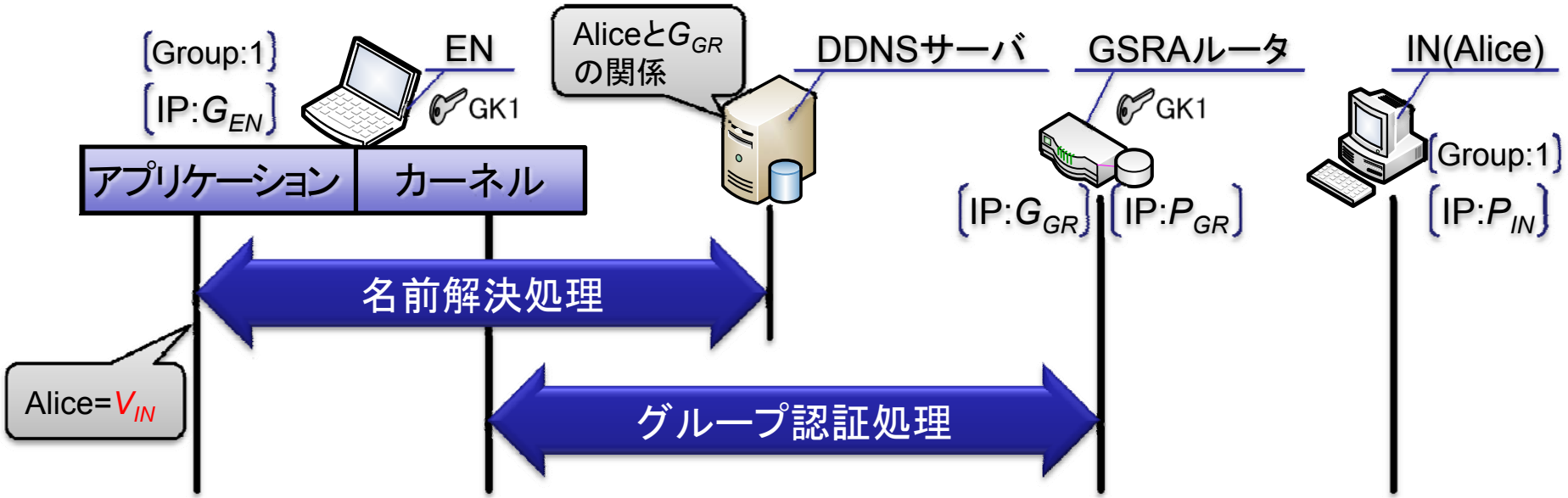
GSRA通信シーケンス1

① 名前解決処理

- ✓ 応答内容(G_{GR})を仮想IPアドレス(V_{IN})に書き換え
- ✓ 仮想IPアドレスで内部ノードを識別

② グループ認証処理

- ✓ ENとINが同一グループかどうか認証
  - 同グループ→アクセス許可
  - 異グループ→アクセス拒否



GSRA通信シーケンス2

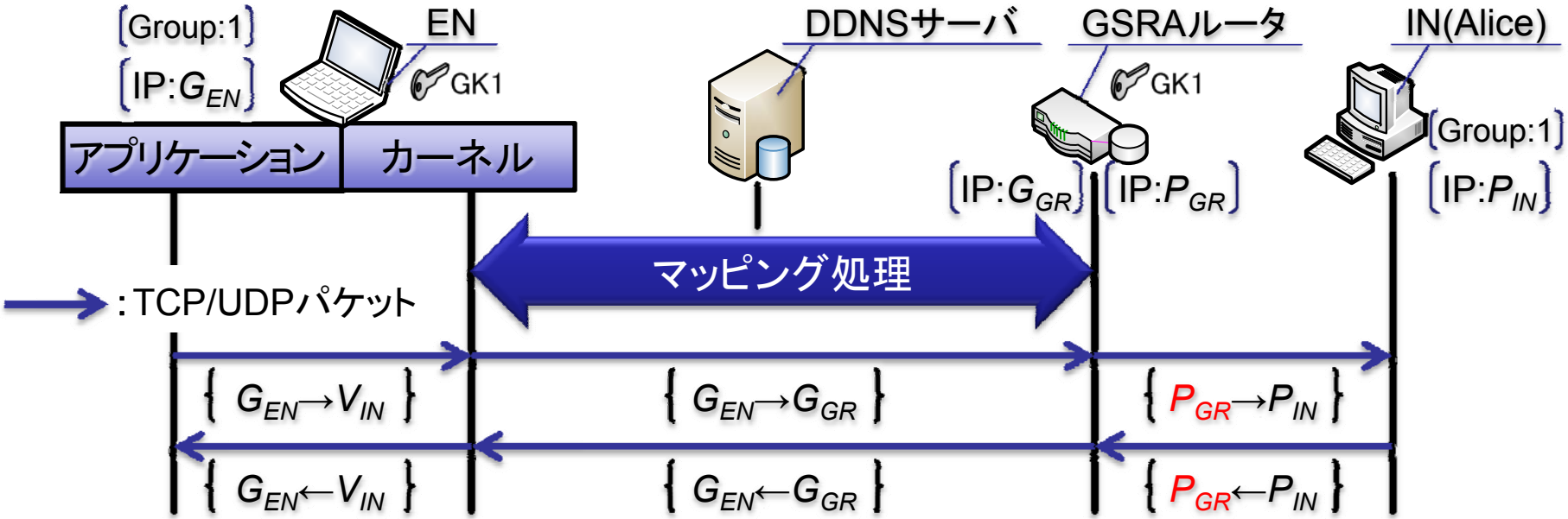
VAT(Virtual Address Translation)：仮想アドレス変換

③ マッピング処理

- ✓ GSRAルータにアドレス変換テーブルを生成
- ✓ ENにVATテーブルを生成

④ 生成したテーブルに従ってアドレス変換しながら通信

- ✓ GSRAルータは送信元を自身に書き換える
- ✓ INはGSRAルータが通信相手に見える

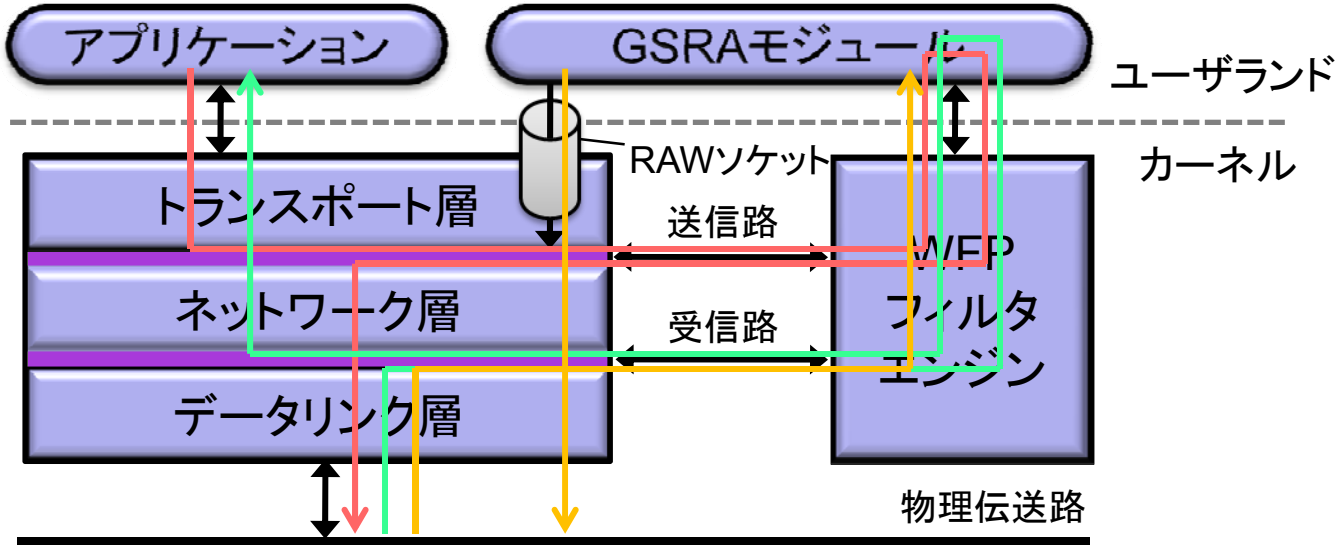


Windowsへの実装

- Windowsへ実装する
  - Windows OSはブラックボックス
  - 機能拡張のためのインターフェースが存在

- WFP（Windows Filtering Platform）
  - ネットワークスタックに干渉できるAPI
  - トラフィックの監視やパケットの書き換え等

WFPを用いた実装



- パケット送信時
  - ネットワーク層最上部でパケットをフック
- パケット受信時
  - ネットワーク層最下部でパケットをフック

GSRAモジュールで処理後差し戻し

アドレス変換，暗号化/復号

- GSRA制御パケット
  - 送信時にはRAWソケットを使用

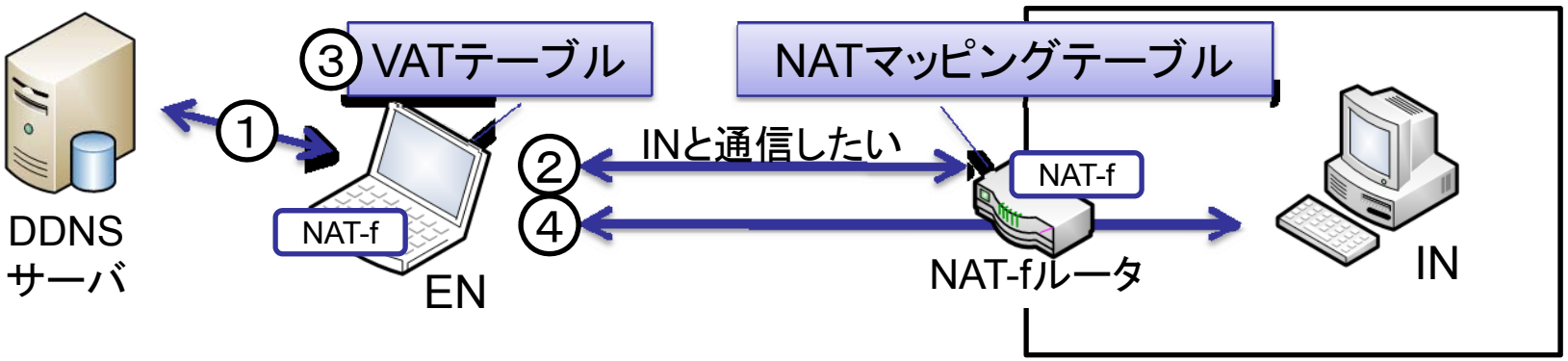
まとめ

- リモートアクセス方式GSRAの提案を行った
  - NAT越え技術に基づいたリモートアクセス方式
  - 既存方式の課題を解決
- 提案方式のWindowsへの実装方法を検討した
  - OSがブラックボックスであり直接改造できない
  - ネットワーク機能を拡張できるWFPを利用する
- 今後は実装と性能評価を行う

補足資料

要素技術：NAT-f

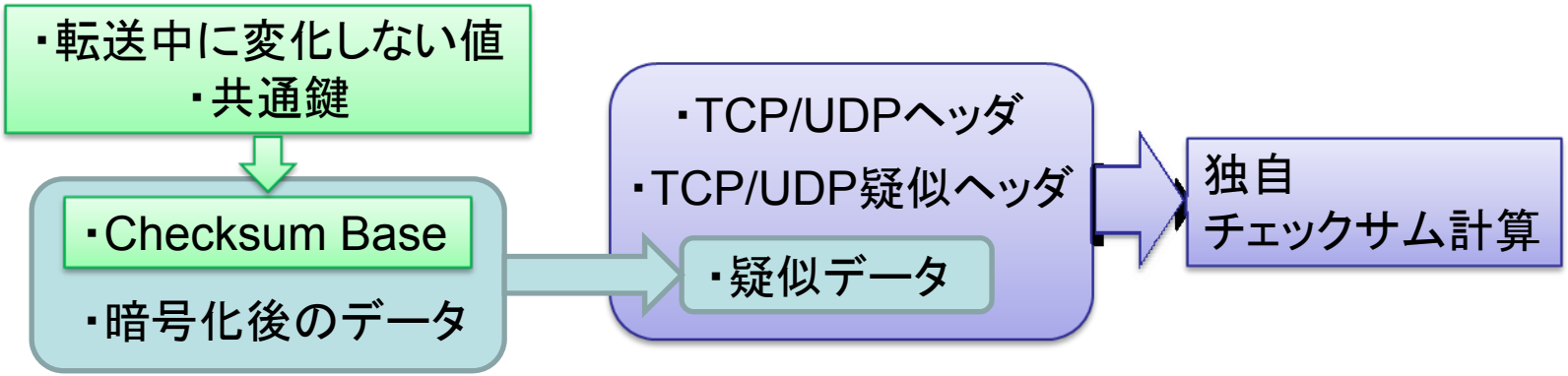
- NAT-f (NAT-free protocol)
  - ① ENはINを仮想IPアドレスで認識する
  - ② ENからNATにマッピングテーブルを生成させる
  - ③ NATのマッピング内容に対応するVATテーブルをENに生成する
  - ④ 生成したテーブルに従いアドレスを変換しながら通信を行う



VAT（Virtual Address Translation）：仮想アドレス変換

要素技術：PCCOM

- 独自のTCP/UDPチェックサム計算
  - 本人性確認とパケットの完全性保証
- 暗号化範囲＝TCPペイロード部
  - NATをまたがった暗号通信が可能
- パケットフォーマットに変更を加えない
  - 高スループットを実現



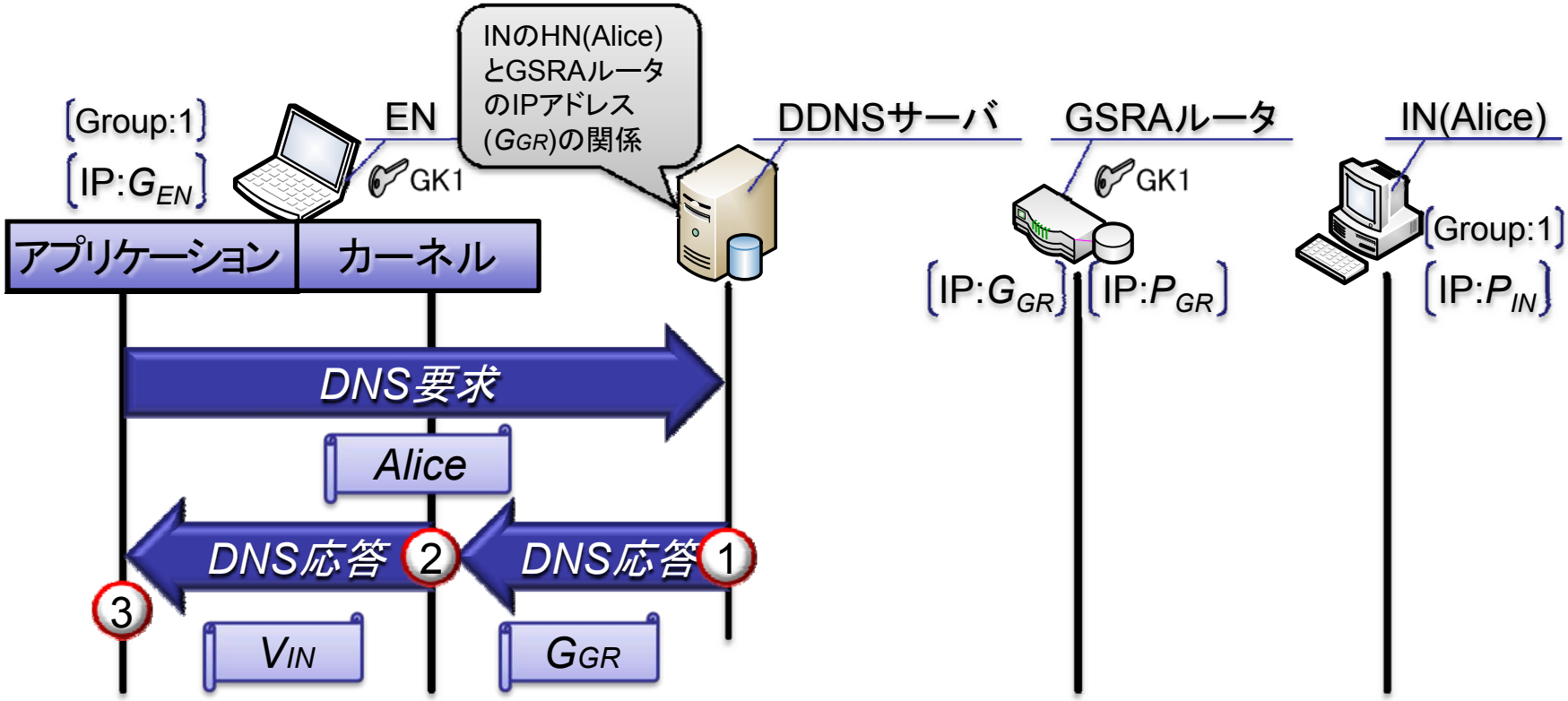
GSRA通信シーケンス1：名前解決

INの名前解決処理

① GSRAルータのIPアドレスG_{GR}を応答

② G_{GR}をIPアドレスV_{IN}書き換え

③ ENはINを仮想的に認識⇒仮想IPアドレスでINを識別



GSRA通信シーケンス2：グループ認証

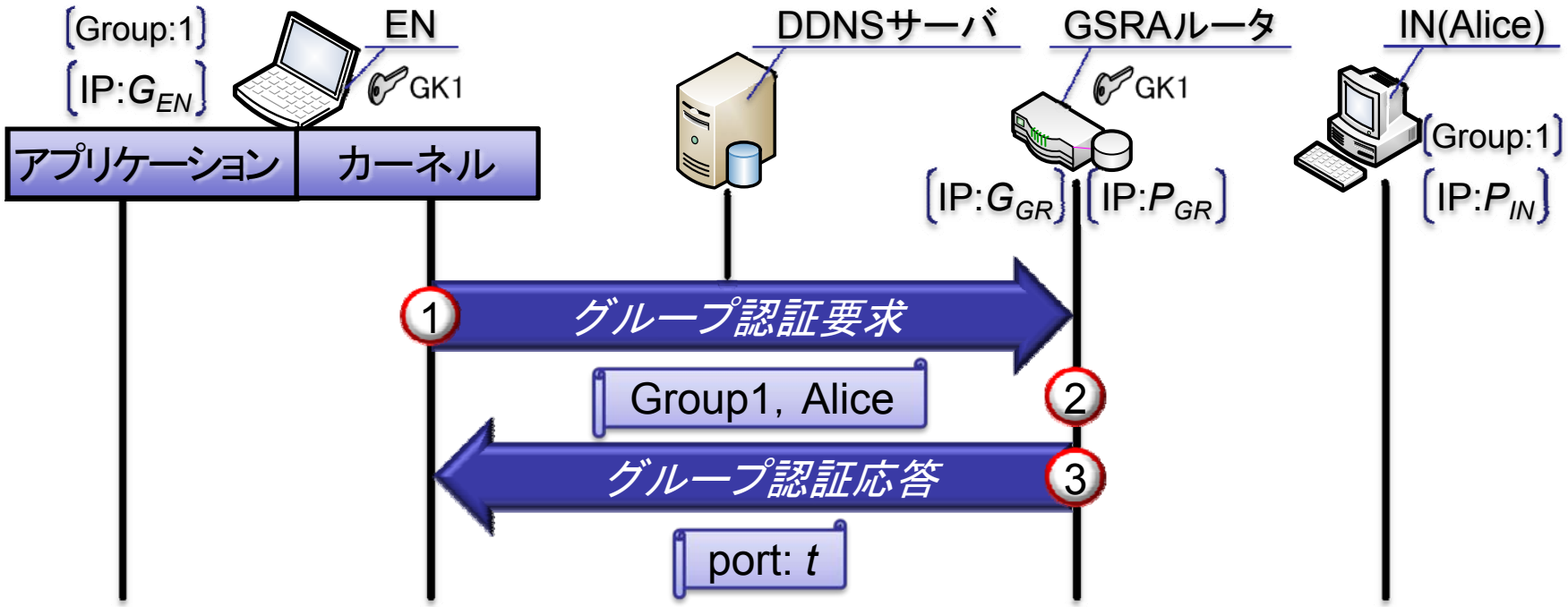
アクセス制御のためのグループ認証処理

① 自身のグループ情報と通信したいINを提示

② ENとINが同一の通信グループかどうか照合

③ ○：ENとINの通信に使用するポート番号を予約して応答

　×：アクセス拒否



GSRA通信シーケンス3：バインディング

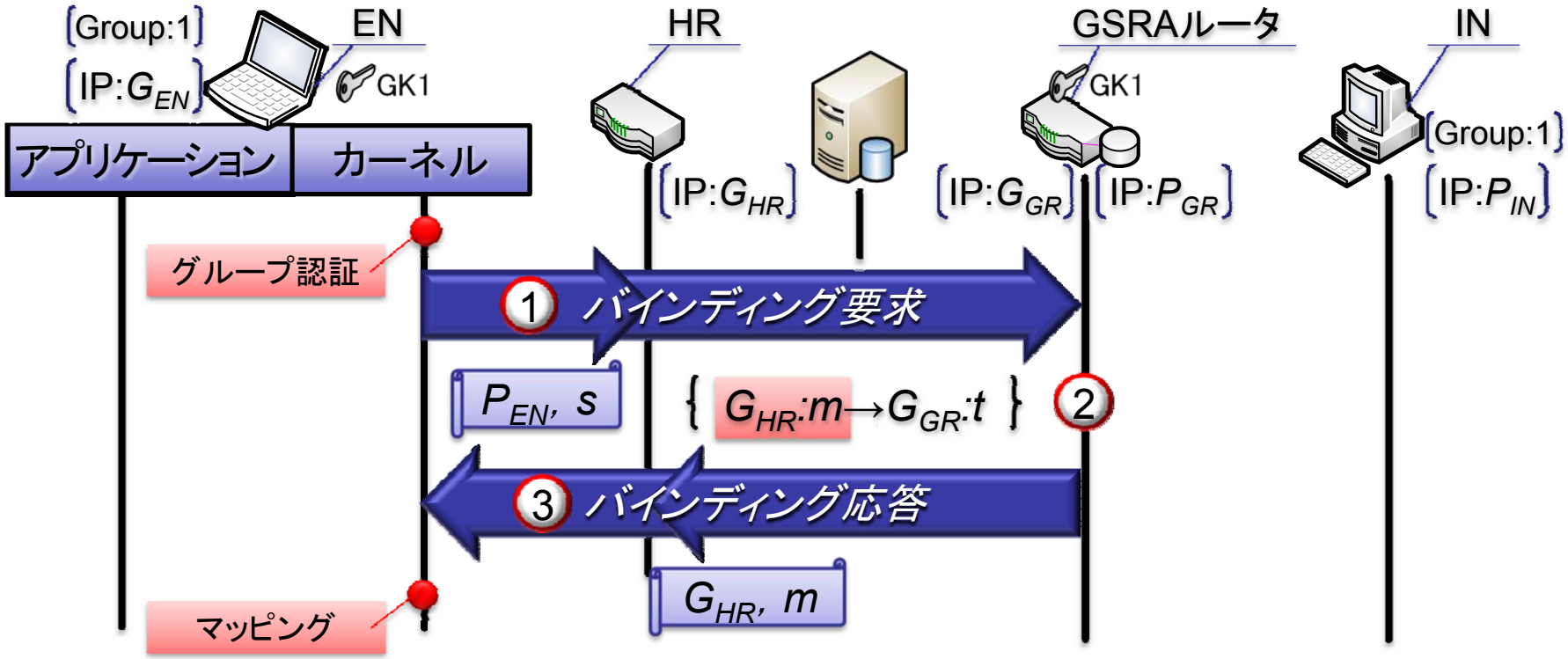
HR：Home Router

HRで変換されたアドレスに対してマッピングするための準備

① ENの送信元情報を記載⇔メッセージの送信元はHR

② ホームルータのIPアドレス，ポート番号を取得

③ 取得したHRの情報をENへ通知



GSRA通信シーケンス4：マッピング処理

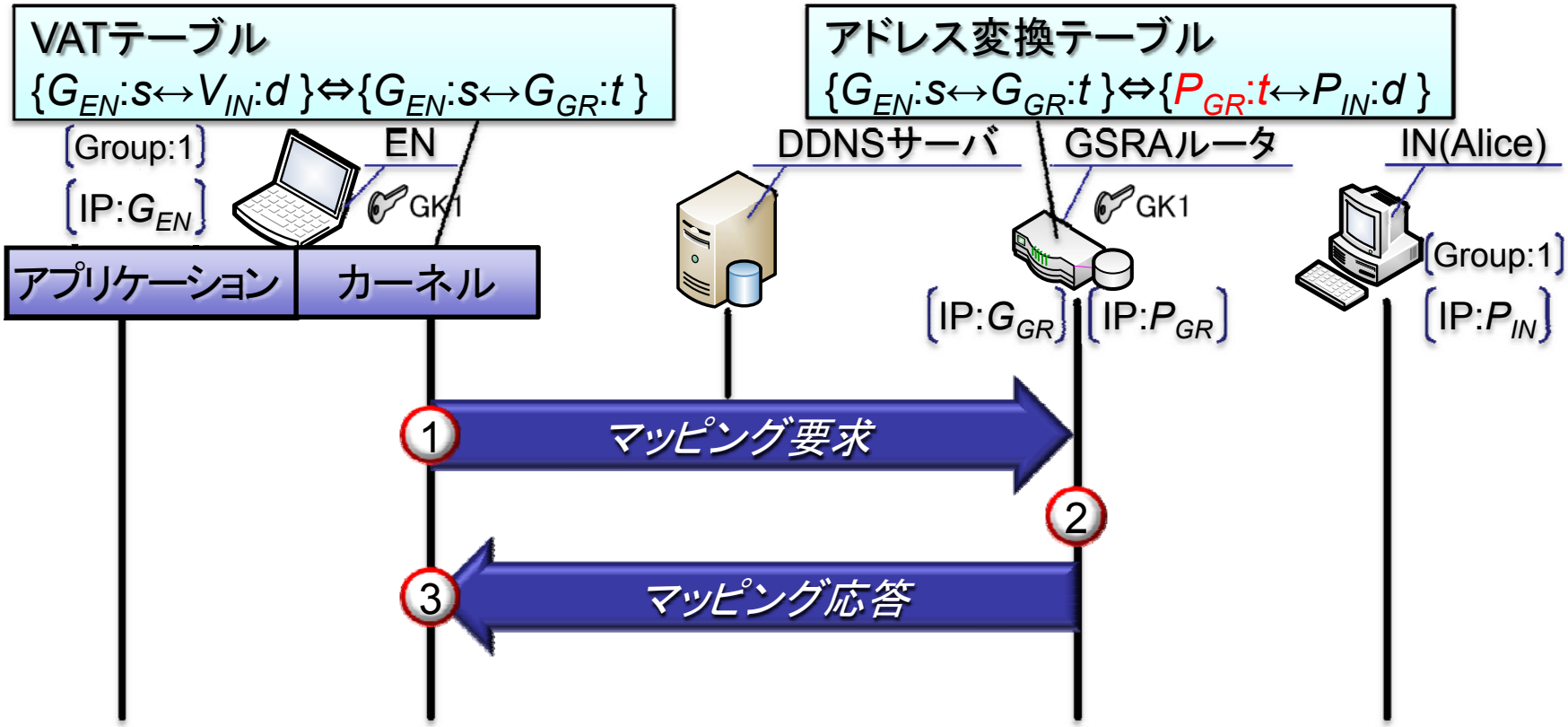
アドレス変換テーブルを生成するためのマッピング処理

① 割り当てられたポート番号に対しマッピング要求を行う

② GSRAルータ：アドレス変換テーブルを生成

③ EN：VATテーブルを生成

↔：両辺の通信
⇔：両辺の変換



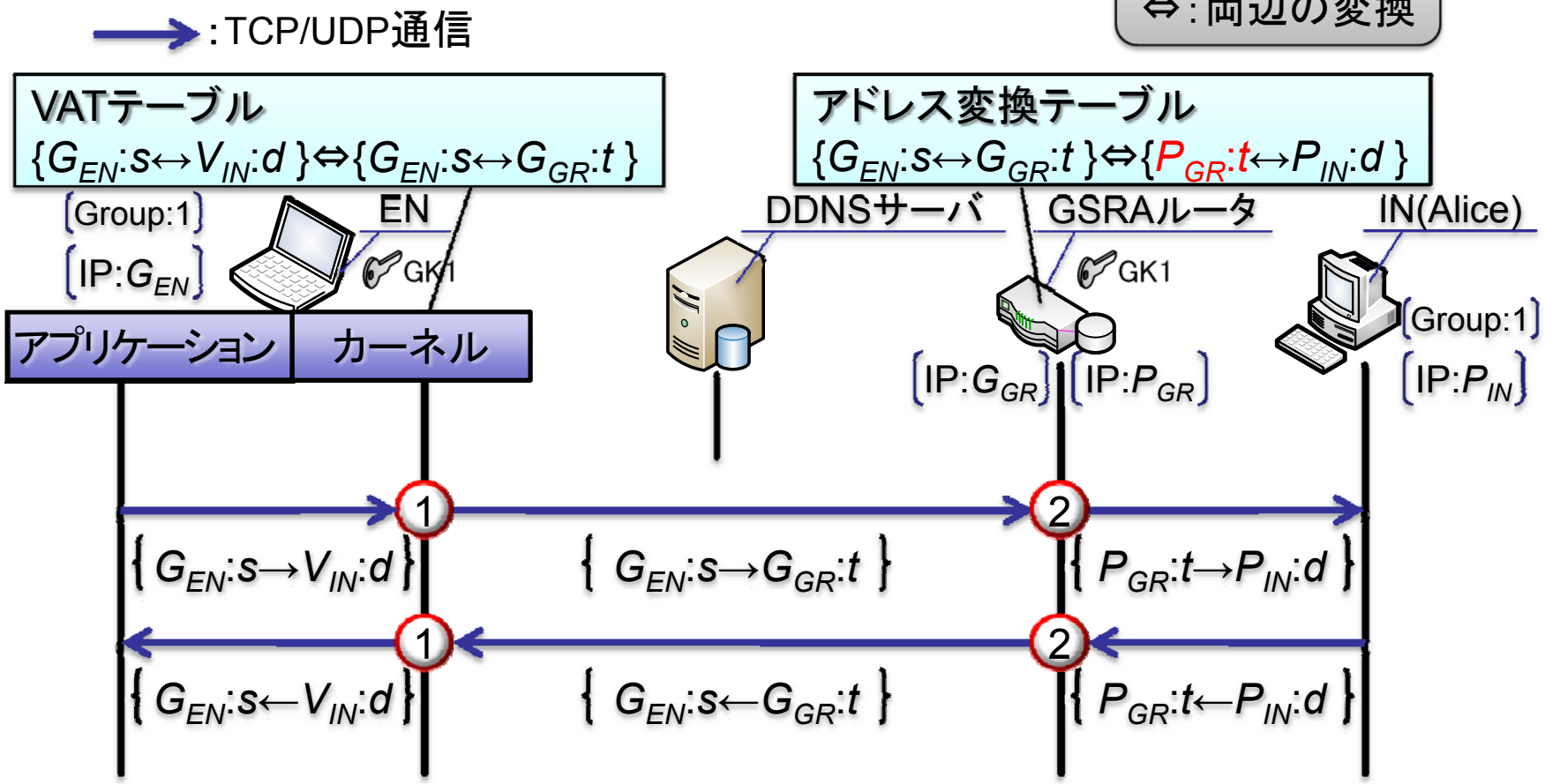
GSRA通信シーケンス5：アドレス変換

生成したテーブルに従ってアドレス変換通信

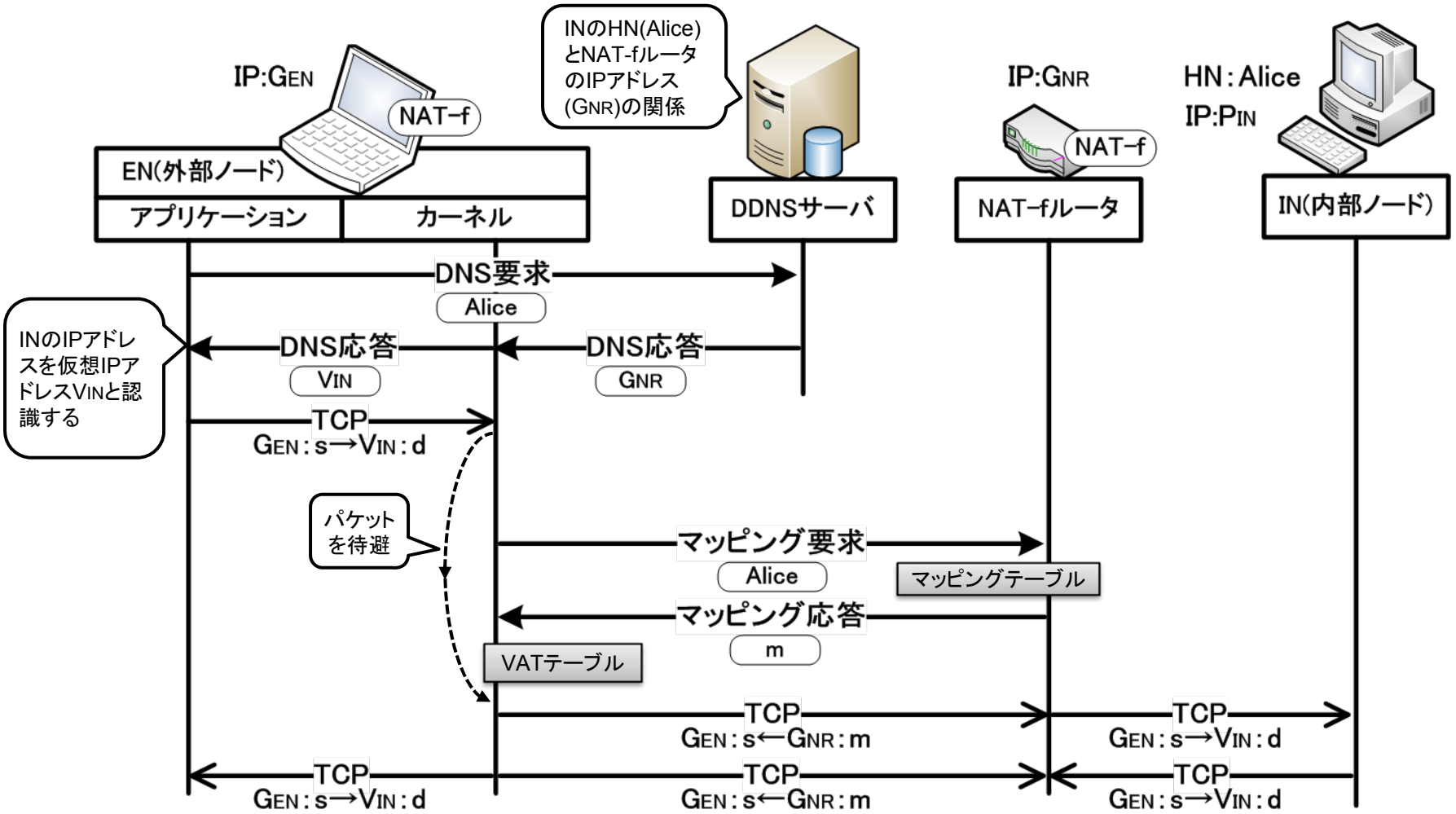
① VATテーブルに従ってアドレス変換

② アドレス変換テーブルに従ってアドレス変換

↔：両辺の通信
⇔：両辺の変換



NAT-fの動作



VATテーブル

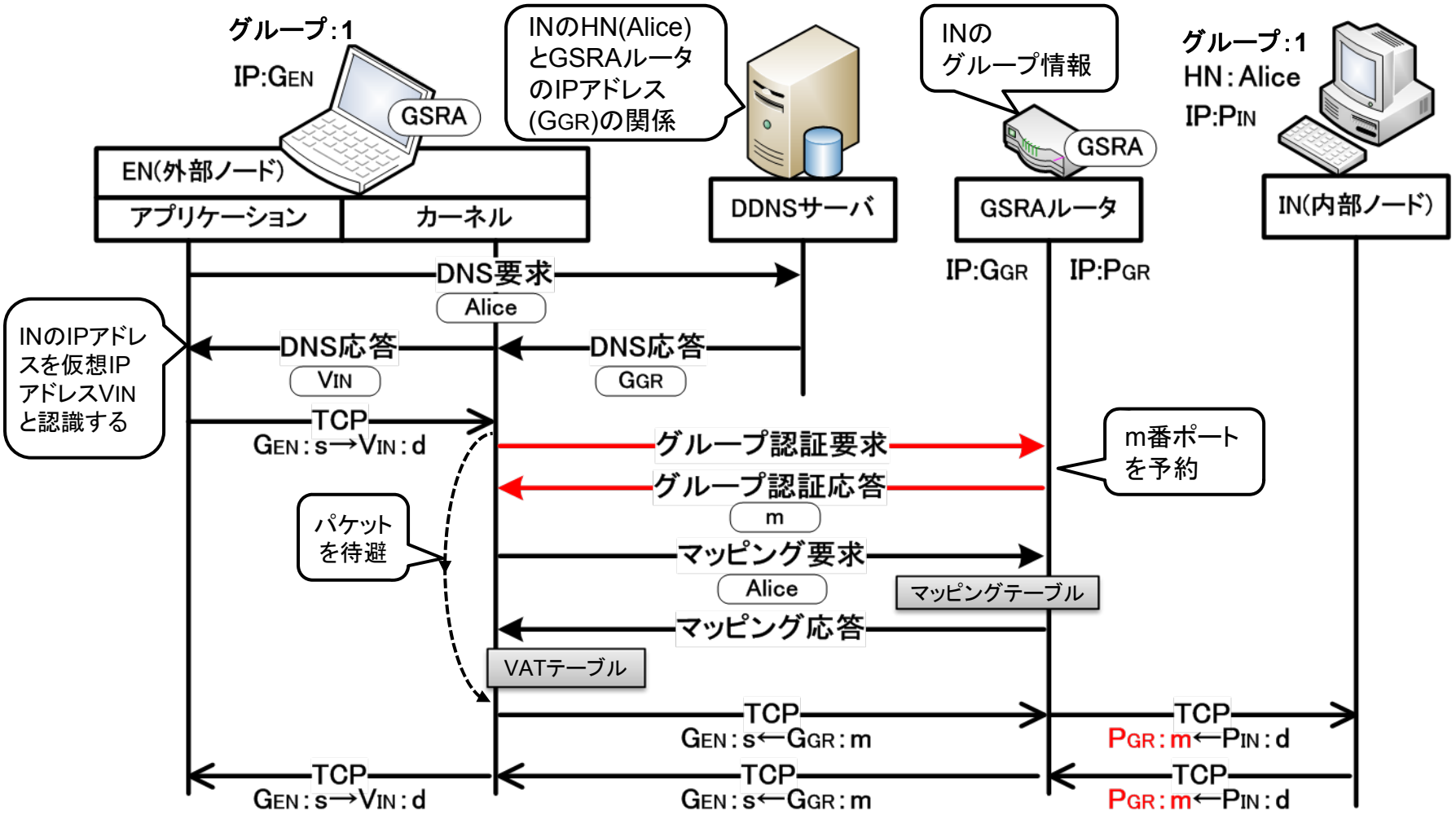
GEN:s↔VIN:d⇔GEN:s↔GNR:m

VAT(Virtual Address Translation):仮想アドレス変換

マッピングテーブル

GEN:s↔GNR:m⇔GEN:s↔PIN:d

GSRAの動作



VATテーブル

{GEN:s↔VIN:d}⇔{GEN:s↔GGR:m}

アドレス変換テーブル

{GEN:s↔GGR:m}⇔{PGR:m↔PIN:d}

VAT（Virtual Address Translation）:仮想アドレス変換