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

鈴木健太[†1]　鈴木秀和[†2]　渡邊晃[†2]

モバイル端末の高性能化やモバイルブロードバンドの普及が著しい昨今，移動中や出張先等の遠隔地から自宅や社内の PC にアクセスできるリモートアクセス技術の需要が高まってきている．リモートアクセスでよく利用される IPsec-VPN は複雑な設定が必要であり，NAT との相性が悪いなどの課題がある．SSL-VPN は手軽に利用できるが，使用す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-f と呼ぶ NAT 越え技術に暗号化機能やアクセス制御機能等を追加することによりリモートアクセスを実現する方式を提案する．提案方式では，NAT の存在を気にすること無く，安全なリモートアクセスを実現できる．

Proposal and Design of Remote Access Method using NAT Traversal Technology

Kenta SUZUKI ,[†1] Hidekazu SUZUKI[†2] and Akira WATANABE[†2]

Recently, the demand for the remote access technology increases because the improved mobile terminal performance and the spread of mobile broadband. By a remote access technology, we can accessing to home and in-house PC from the remote place such as the movement and the business trip destinations. Commonly used in IPsec-VPN remote access requires a complex configuration, and Incompatible with NAT. SSL-VPN is readily available but there is a problem that is limited to use application. In this paper, we propose to achieve a remote access by adding access control and encryption technologies, to NAT-f. In this method, secure remote access can be achieved without considering NAT.

1. はじめに

近年，モバイル端末の小型化・高性能化や，モバイルブロードバンドの普及に伴って，リモートアクセスのニーズが高まっている．リモートアクセスとは，遠隔地から社内や家庭のネットワークに接続し，そのネットワーク上の資源を利用する技術である．リモートアクセス技術は，在宅勤務やモバイルワーキング等幅広く利用可能である．更には近年の新型インフルエンザ等の流行を受け，今後のパンデミック対策としても期待されている．

リモートアクセスを実現する手法としては，インターネット上に VPN（Virtual Private Network）を構築するインターネット VPN が一般的である．インターネット VPN はインターネットを介する手法であるため，盗聴や改ざん，なりすましといったインターネット上の脅威に対抗する手段は必要不可欠である．そこで現在はセキュリティ技術に基づき VPN を構築する方式が主流となっている．

インターネット VPN を構築する方式には，PPTP（Point-to-Point Tunnering Protocol）[1]，L2F（Layer 2 Forwarding）[2]，L2TP（Layer 2 Tunnering Protocol）[3]，IPsec（Security Architecture for Internet Protocol）[4]，SSL（Secure Socket Layer）[5] などがある．

PPTP は暗号化の強度が弱く，セキュリティ強度に問題があるため利用されていない．L2F はトンネリングのためのプロトコルであり，暗号化機能を備えていないため，そのまま使用されることはない．L2TP は PPTP と L2F の仕様を統合したもので，マルチプロコトルに対応している．しかし，暗号化機能が無いため通信の暗号化には他の技術を併用する必要があり，ヘッダの追加に伴ないオーバヘッドが増加する欠点がある．そのため，近年はセキュリティ技術の IPsec や SSL を利用したインターネット VPN がよく利用される．しかし，IPsec は導入に複雑な設定が必要であり，運用するには相応の知識が必要となる．SSL はユーザ側で設定を必要とせず，誰でも簡単に使用することができるが，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．また，両方式ともインターネット上のセキュリティは強固であるが，イントラネット内でのセキュリティは考慮されていない．盗聴，改ざんといった脅威はイントラネット内にも存在し，エンドエンドで暗号化するのが望ましい．

近年のホームネットワーク・企業ネットワークは，プライベート IP アドレスで構築され

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 名城大学理工学部
Faculty of Science and Technology, Meijo University

ることが一般的であり，インターネットとの境界には NAT[6] が設置される．NAT の存在により NAT の外側から内側へ向けて通信が開始できない，いわゆる NAT 越え問題が表面化してきている．リモートアクセスを行う場合には，NAT 越え問題を解決する必要がある．これに着目すると，NAT 越えの技術に基づいてリモートアクセスを行う手法が考えられる．しかし，NAT 越え技術はあくまで NAT をまたがった通信を実現するものであり，そのままリモートアクセスに適用することはセキュリティ上問題がある．

そこで本稿では，NAT 越え技術に基づいたリモートアクセス方式として GSRA（Group-based Secure Remote Access）を提案する．GSRA は，NAT 越え技術である NAT-f（NAT-free protocol）[7] の仕組みを基盤とし，更に暗号化機能やアクセス制御機能を追加することにより安全なリモートアクセスを可能とした方式である．GSRA は FreeBSD への実装を終えている．しかし GSRA の今後の普及のためにはより一般的な OS への実装が不可決である．そこで，Windows クライアントへの実装方法を検討中である．

以降，2 章で既存技術である IPsec-VPN と SSL-VPN について述べる．3 章で提案方式の要素技術について述べ，4 章で提案方式の概要を説明する．5 章では実装方法を述べる．最後に 6 章でまとめる．

2. 既 存 技 術

現在一般的に利用されているリモートアクセス技術として，IPsec-VPN と SSL-VPN を示す．

2.1 IPsec-VPN

図 1 に IPsec-VPN を利用したリモートアクセスの構成例を示す．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．IPsec-VPN は IPsec の仕組みを利用することで VPN を構築する．アクセス先に設置した IPsec-VPN 装置と EN 間で IKE（Internet Key Exchange）[8] による認証と暗号鍵の共有をし，IPsec ESP トンネルモードによる暗号通信を行う．IPsec は IP 層においてデータの改ざん防止や秘匿機能を提供するプロトコルであるため，アプリケーションを限定することなく，通信経路上で通信内容の盗聴や改ざんを防止することができる．しかし，セキュリティポリシの設定やネゴシエーションの設定等，端末毎に行わなければならない設定項目が多いため，管理負荷が大きい．また，エンドエンドで暗号化していない点で課題が残る．

2.2 SSL-VPN

図 2 に SSL-VPN を利用したリモートアクセスの構成例を示す．SSL-VPN は SSL の仕組みを利用することで VPN を構築し，リモートアクセスを実現する．SSL-VPN を利用する場合，DMZ（DeMilitarized Zone）上に設置した SSL-VPN サーバがプロキシサーバの役割を果たすことでリモートアクセスが実現される．SSL は一般的なブラウザには標準で搭載されているため，ユーザ側の設定は不要である．携帯電話や PDA，ゲーム機等でも，ブラウザが SSL に対応していれば使用できる．しかし，SSL-VPN は利用できるアプリケーションが Web 閲覧やメール送信などに限定されるという課題がある．また，IPsec-VPN と同様に，エンドエンドでの暗号化は行われない．

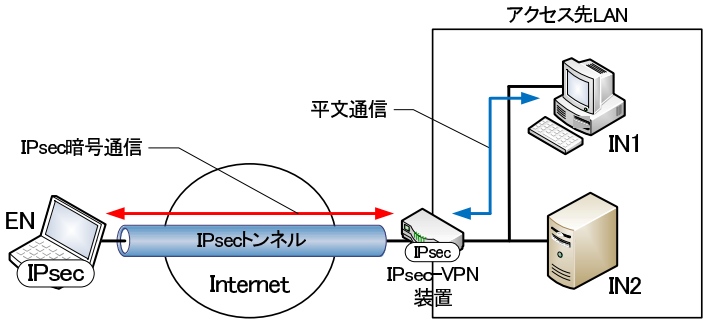


図 1 IPsec-VPN によるリモートアクセスの構成例
Fig. 1 An example of a remote access configuration with IPsec-VPN.

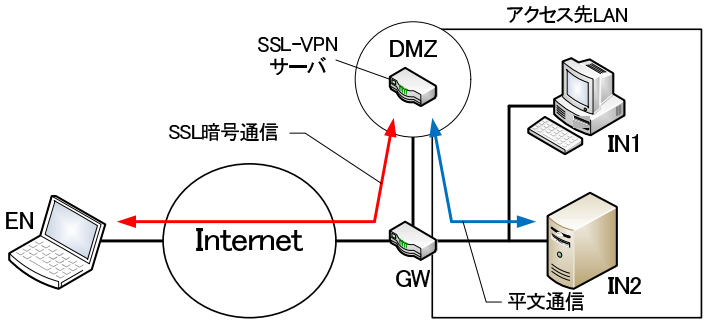


図 2 SSL-VPN によるリモートアクセスの構成例
Fig. 2 An example of a remote access configuration with SSL-VPN.

3. 要素技術

提案方式はNAT-fの仕組みを基盤に，通信の暗号化にPCCOM（Practical Cipher Communication Protocol）[9] を利用し，さらに通信グループを定義することで安全なリモートアクセスを実現する．本章では要素技術であるNAT-f，PCCOM，通信グループの定義について示す．

3.1 NAT-f

NAT-fは，ENとNATルータ間のネゴシエーションにより，NAT配下のノードに対して通信を開始することができるNAT越え技術である．**図3**にNAT-fの通信シーケンスを示す．ENとNATにはNAT-fの機能が実装されている．NAT-fの機能を実装したNATをNAT-fルータと呼ぶ．ENは通信を開始するにあたり，DDNSサーバに問い合わせてINの名前解決を行う．その結果，ENはNAT-fルータのグローバルIPアドレスを取得する．ENはカーネルにて取得したIPアドレスを仮想IPアドレスに書き換え，上位アプリケーションに対して通知する．仮想IPアドレスはNAT配下のINを識別するためのものであり，INのFQDNを元に生成される．上位アプリケーションは通知された仮想IPアドレスに対して通信を開始する．この時ENは最初のパケットをカーネル内に待避し，NAT-fルータに対してマッピング処理を要求する．この処理により，NAT-fルータはENとINが通信するために必要なマッピングテーブルを生成する．ENは仮想IPアドレスと上記マッピングアドレスの対応関係を示す仮想アドレス変換（VAT : Virtual Address Translation）テーブルを，カーネル内に生成する．ENはカーネル領域においてVATテーブルを参照し，対応するエントリに基づいて宛先アドレスをマッピングアドレスに書き換えてパケットを送信する．NAT-fルータには既にマッピングテーブルが生成されているため，通常のNATによるアドレス変換を行い，ENからのパケットをINへと転送する．

以上の処理により，NATの外側からNAT-fルータ配下の端末へ通信を開始することができる．しかし，このままではマッピング処理に認証機能が無いため，誰でもINにアクセスできるというセキュリティ上の課題がある．また，ENがグローバルIPアドレスを保持していることが前提であり，ホームネットワークのNAT配下に位置している場合が考慮されていない．これらの課題はリモートアクセス方式を実現するにあたって解決する必要がある．

3.2 PCCOM

ネットワークレベルの暗号化通信を実現する技術として，IPsec・ESPやPCCOMがある．ESPはTCP/UDPヘッダ部が暗号化範囲に含まれているため，NATでアドレスが変換

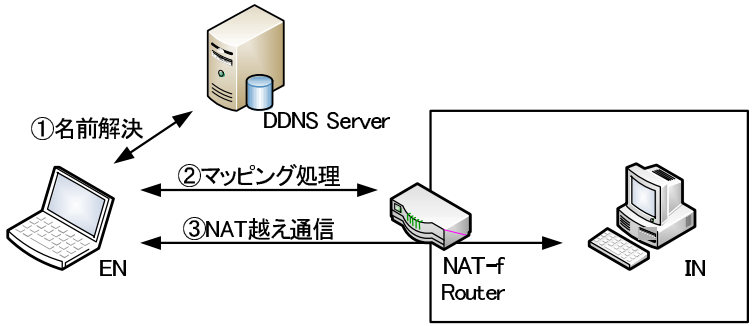


図3 NAT-f通信シーケンス
Fig. 3 NAT-f sequence.

されるとエンド端末で偽装パケットと見なされ，破棄されてしまう問題がある．これを解決するため，パケットをUDPによりカプセル化してNAT越えをする方法[10] があるが，ヘッダの追加に伴なうオーバヘッドの増加や，ヘッダ部のセキュリティが低下する等の課題が生じる．このようにIPsecはNATとの相性が悪く，NATをまたがった通信の暗号化には向いていない．

PCCOMは上記のようなIPsecの課題を解決できる暗号化技術である．PCCOMは暗号鍵とパケットの内容から生成した値を用いて独自のTCP/UDPチェックサム計算を行うことにより，本人性確認とパケットの完全性保証を実現できる．TCP/UDPヘッダは暗号化範囲から除くため，NATを通過でき，ファイアウォールによるトラフィック制御も可能である．ヘッダ部分の完全性は，暗号鍵を検索する過程で保証される．

PCCOMによると，パケットフォーマットに変更を加えないため，オーバヘッドが少なく，高速な暗号化通信を実現できる．また，NATを通過できるため，NATをまたがったエンドエンドで暗号化通信が可能である．

3.3 通信グループの定義

特定の属性に基づいて通信グループを構築する手法は，通信の安全性を確保し，アクセス制御を行うのに有用である．グループのメンバ間の通信を暗号化することで，第三者による通信の盗聴やパケットの改ざんから保護される．またグループ毎の認証を行うことによりアクセス制御を実現できる．

通信グループを構築する方法として，GSCIP（Grouping for Secure Communication for IP）[11] が採用しているエリア定義方式[12] がある．この方式では，通信グループとグループ

鍵と呼ぶ暗号鍵をを 1 対 1 に対応付ける．ユーザが複数のグループ鍵を持つことで，複数の通信グループに多重帰属することができる．これにより，IP アドレスに依存しない柔軟なグループの定義が可能となる．通信グループを構築する場合，通信に先立って通信相手とグループ情報を交換して同一グループに属している事の確認を行い，暗号化通信に必要な動作処理情報を生成する．これを実現するためのプロトコルは DPRP（Dynamic Process Resolution Protocol）として既に定義されている[11]．

4. 提 案 方 式

4.1 概　　要

本稿では、NAT-f にセキュリティの機能を追加することで安全なリモートアクセスを実現する GSRA を提案する．具体的には，通信グループを定義することによりアクセス制御とサービス制御を行い，PCCOM により通信を暗号化する．さらに，システム構成として EN がホームルータなどの NAT 配下に存在し，プレイベートアドレスを持つ場合も想定する．この時，EN 側のホームルータには一切改造を加えない．リモートアクセスを自宅から行う場合には，EN が NAT 配下に存在することになるため，このようなシステム構成を想定することは必須である．

GSRA のネットワーク構成例を**図 4** に示す．EN は NAT 機能をもつホームルータ配下に位置する場合を想定する．GSRA の機能を実装したルータを GSRA ルータと呼び， アクセス先のネットワークの DMZ 上に設置する．EN は同一グループに所属している IN1 と

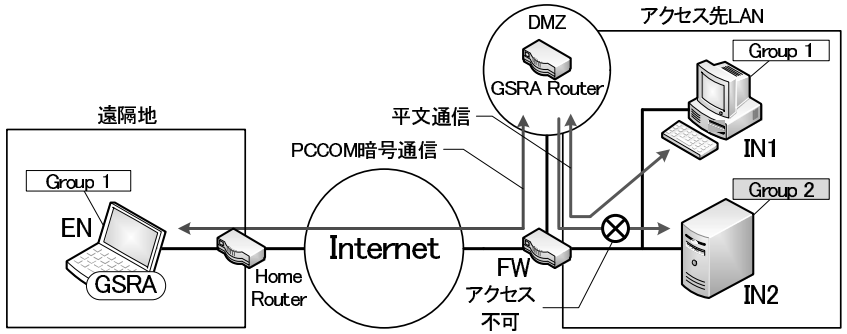


図 4　GSRA によるリモートアクセスの構成例
Fig. 4　An example of a remote access configuration with GSRA.

通信可能であるが，異なるグループの IN2 との通信は許可されない．IN のグループ情報は GSRA ルータに登録されており，この情報を基にアクセス制御とサービス制御を行う．図 4 中では GSRA ルータ-IN1 間が平文通信となっているが，IN1 が PCCOM をサポートする場合，EN-IN1 のエンドエンド間で暗号化通信が可能である．

4.2 通信シーケンス

図 5 に EN が GSRA を用いて IN1 にリモートアクセスを行うまでの GSRA シーケンスを示す．ネットワーク構成及び通信グループの定義は図 4 の通りとする．以下に本稿で使用する記号を定義する．

- G_i (i = NodeID)：グローバル IP アドレス
- P_i：プライベート IP アドレス
- V_i：仮想 IP アドレス
- s, d, t, m：ポート番号

前提として EN と GSRA ルータは共通の暗号鍵 CK と，各通信グループに対応したグループ鍵 GK を予め保持しているものとする．DDNS サーバには，IN のホスト名と GSRA

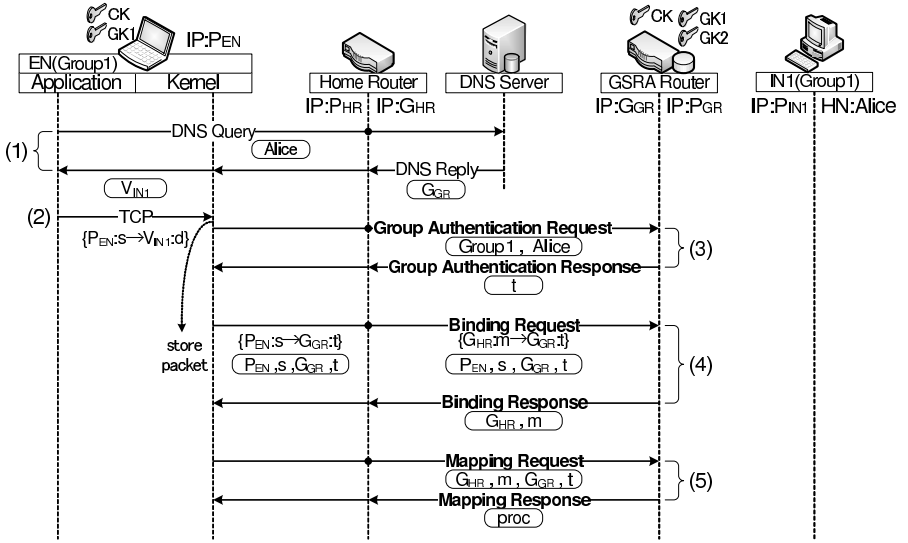


図 5　GSRA シーケンス
Fig. 5　GSRA sequence.

ルータのグローバル IP アドレス G_{GR} との関係が登録されているものとする．以下に EN が IN1 と通信を開始するまでの手順を示す．

(1) 名前解決

EN は IN1（ホスト名 : Alice）の名前解決を行い，G_{GR} を取得する． ここで EN はカーネル領域において，DNS 応答メッセージに記載されているアドレス G_{GR} を仮想 IP アドレス V_{IN1} に書き換える．これにより EN のアプリケーションは IN1 の IP アドレスを V_{IN1} と認識する．この時，IN のホスト名 Alice と GSRA ルータのグローバル IP アドレス G_{GR}，および仮想 IP アドレス V_{IN1} の関係を NRT（Name Relation Table）に登録しておく．これにより GSRA ルータ配下の端末を仮想 IP アドレスで識別する．今回の場合，IN1 宛のパケットは宛先 IP アドレスが V_{IN1} となる．

(2) 通信開始

EN から宛先が V_{IN1} のパケットを送信する時，EN はカーネルにて VAT テーブルを検索する．初回は対応する VAT のエントリが存在しないため，このパケットをカーネル内に待避してから，(3) 以降の処理へと移る．(3) 以降の処理では，VAT テーブルおよびパケットの処理内容を記載した動作処理情報テーブル（PIT : Process Information Table）を生成する．

(3) グループ認証処理

EN は通信したい IN のホスト名 “ Alice ” と自身のグループ情報 “ Group1 ” を記載したグループ認証要求を GSRA ルータへ送信する．GSRA ルータはこれを受信すると，EN と IN1 が同一グループに属しているか認証を行う．認証が成功した場合，EN と IN1 間の通信に使用するエフェメラルポート番号 t を予約し，EN へグループ認証応答を送信する．EN はグループ認証応答メッセージから t を取得して，VAT テーブルと PIT を仮生成する．エフェメラルポートとは，リモートアクセスのために一時的に使用するポートであり，その番号は GSRA ルータの空いているポートの中から選ばれる．

EN がホームルータ配下に位置する場合，更に (4) の処理を実行する．(4) の処理が必要かどうかについては，(3) の GSRA ユーザ認証時に，メッセージの送信とペイロードに記載された送信元情報（図 5 の例では $G_{\mathrm{HR}} : m$ と $P_{\mathrm{EN}} : s$）を比較することで判定する．この二つの内容が一致していれば EN との間に NAT が存在しないと判定され，(4) の処理をスキップして (5) の処理へと移る．

(4) バインディング処理

バインディング処理は，EN がホームルータ配下に存在する場合に行う処理である．EN は自身の $P_{\mathrm{EN}} : s$ と宛先となる $G_{\mathrm{GR}} : t$ を記載したバインディング要求を GSRA ルータに送信する．GSRA ルータがバインディング要求を受信すると，受信メッセージの送信元である $G_{\mathrm{HR}} : m$ を取得し，この取得した情報をバインディング応答に載せ EN へ送信する．バインディング処理の結果，GSRA ルータと EN はホームルータの情報を取得し，EN 側に NAT が存在する場合に対応したマッピング処理を実行させることが可能となる．

(5) マッピング処理

EN は (4) で通知されたホームルータのマッピングアドレス $G_{\mathrm{HR}} : m$ を送信元情報として，(2) で待避したパケットのセッション情報と，宛先情報 $G_{\mathrm{GR}} : t$ を記載したマッピング要求を GSRA ルータへ送信する．GSRA ルータはマッピング要求メッセージから取得した情報を用いて GSRA マッピングテーブルと PIT を生成し，マッピング応答を EN へ送信する．EN は受信したマッピング応答メッセージから動作処理情報を取得し，VAT テーブルと PIT を確定する．ここで確定した GSRA マッピングテーブルと VAT テーブルのエントリを**表 1** に示す．記述内容の意味は以下の通りである．

- $G_1 : s \leftrightarrow G_2 : d$; $G_1 : s$ と $G_2 : d$ の通信
- $G_1 : s \Leftrightarrow G_2 : d$; $G_1 : s$ と $G_2 : d$ の変換

表 1 GSRA マッピングテーブルと VAT テーブル
Table 1 GSRA mapping Table and VAT Table.

GSRA マッピングテーブル	:	$\{ G_{\mathrm{HR}} : m \leftrightarrow G_{\mathrm{GR}} : t \} \Leftrightarrow \{ P_{\mathrm{GR}} : t \leftrightarrow P_{\mathrm{IN1}} : d \}$
VAT テーブル	:	$\{ P_{\mathrm{EN}} : s \leftrightarrow V_{\mathrm{IN1}} : d \} \Leftrightarrow \{ P_{\mathrm{EN}} : s \leftrightarrow G_{\mathrm{GR}} : t \}$

以上で GSRA ネゴシエーションが完了し，(2) で待避させたパケットを復帰させて通信を開始する．

(6) アドレス変換処理

以後の通信の様子を**図 6** に示す．EN から IN1 宛ての通信は，まず EN のカーネル内で VAT テーブルに従い宛先 IP アドレス/ポート番号が変換される．さらに PIT に従って暗号化されてから GSRA ルータへ送信される．途中のホームルータでは通常の NAT による変換が行われる．GSRA ルータではパケットを復号後，GSRA マッピングテーブルに基づいて宛先/送信元の IP アドレス/ポート番号を変換し，IN1 へと転送される．IN1 から EN への応答は上記と逆の順序でアドレス変換および暗号化処理が行われる．以上の手順により，EN から IN1 へのリモートアクセスが実現される．

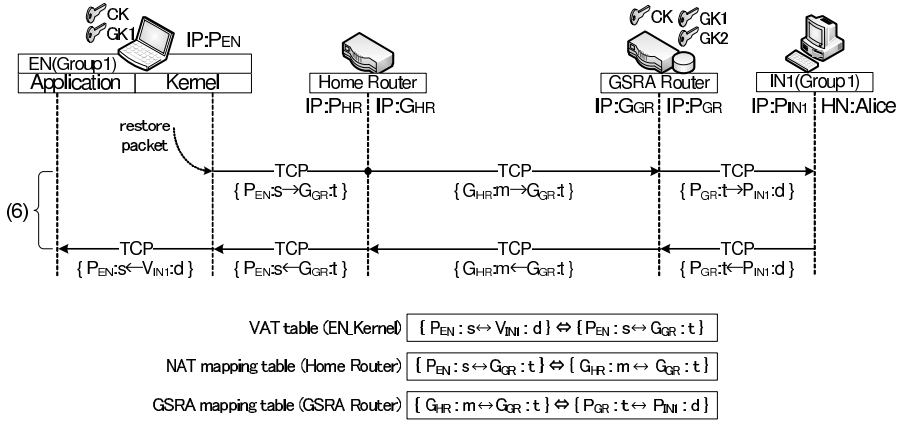


図 6 アドレス変換処理
Fig. 6 Address translation process.

5. 実　　装

GSRA は，既に FreeBSD において EN と GSRA ルータの実装を終えている．EN については，Windows への実装を検討中である．

5.1 FreeBSD への実装

提案システムの実装方法を**図 7** に示す．FreeBSD はカーネルがソースとして公開されており，カーネルを直接改造して再構築することができる．これを利用し，IP 層の入出力関数 $ip_input()$，$ip_output()$ から GSRA モジュールを呼び出し，アドレス変換等の処理を行ったうえで元の位置に差し戻すようにカーネルを改造することにより実装している．この方式では，IP 層の処理は GSRA モジュールの影響を受けることが無い．GSRA モジュールでの処理はすべてカーネル内で閉じており，暗号鍵が処理途中で漏洩する可能性は極めて低い．

5.2 Windows への実装

Windows OS のカーネル部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）[13] に着目し，Windows へ GSRA を実装する方法を検討した．

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エンジンへ

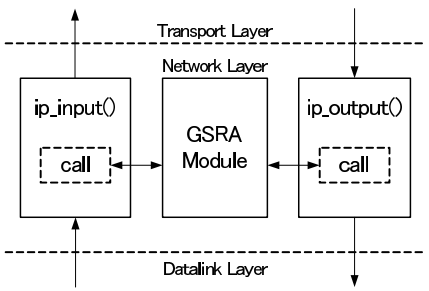


図 7 FreeBSD への実装
Fig. 7 Implementation in FreeBSD.

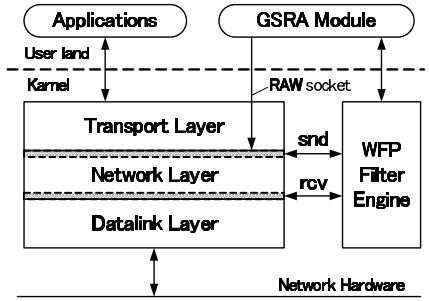


図 8 Windows への実装
Fig. 8 Implementation in Windows.

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，コールアウトを登録することにより，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．**図 8** に Windows における設計の概要を示す．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，ユーザランドで動作する 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．4.2 章で示した GSRA 制御パケットは，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．最下層でフックする理由は，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．

6. ま と め

本稿では，NAT 越え技術である NAT-f に基づきリモートアクセスを実現する方式として GSRA を提案した．NAT-f は単なる NAT 越え技術であり，アクセス制御を行えなかった．また，EN がプライベート IP アドレスを持つ場合を考慮していなかった．提案方式では，通信グループを定義することによりアクセス制御を可能とし，1 往復のバインディング処理を追加することにより EN がホームルータ配下に存在する場合にも対応した．また，FreeBSD と Windows の両 OS について実装方法を示した．今後は，FreeBSD における実装の性能測定，Windows への実装と性能測定を行い実用性を確認する．

参 考 文 献

1) Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and Zorn, G.: Point-to-Point Tunneling Protocol (PPTP), RFC 2637, IETF (1999).
2) Valencia, A., Littlewood, M. and Kolar, T.: Cisco Layer Two Forwarding (Protocol) “L2F”, RFC 2341, IETF (1998).
3) Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B.: Layer Two Tunneling Protocol “L2TP”, RFC 2661, IETF (1999).
4) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
5) Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol, RFC 5246, IETF (2008).
6) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
7) 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 (2007).
8) Hoffman, P.: Algorithms for Internet Key Exchange version 1 (IKEv1), RFC 4109, IETF (2005).
9) 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 (2006).
10) Huttunen, A., Swander, B., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).
11) 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 の実装と評価，情報処理学会論文誌， Vol.47, No.11, pp.2976–2991 (2006).
12) 渡邊　晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌， Vol.38, No.4, pp.904–914 (1997).
13) MSDN ライブラリ：http://msdn.microsoft.com/en-us/library/default.aspx

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

名城大学大学院 理工学研究科
鈴木 健太，鈴木 秀和，渡邊 晃

Watanabe Lab.

研究背景

- ブロードバンドの普及
- 新型インフルエンザの流行

↓

リモートアクセスのニーズが増加

- 遠隔地のネットワークに接続し，資源を利用する技術

Watanabe Lab.

利用シーン

- 在宅勤務（企業）
  - 自宅に居ながら社内サーバへアクセス
- 学内サービス（大学）
  - 学内からのみアクセス可能なサービスへアクセス

- ✓ 部署ごと，学科ごと等の単位でアクセス制御
- ✓ 自宅からのアクセス
  - GWにNAT※が存在する
  - リモートアクセスを利用できないケースがある

※NAT：Network Address Translation

既存方式の特徴

	長所	短所
PPTP	アプリケーションが制限されない Windows標準の機能	NATにVPNパススルー機能が必要 セキュリティが弱い
IPsec-VPN	アプリケーションが制限されない	NATにVPNパススルー機能が必要 クライアントソフトの導入が必要 設定項目が多い
SSL-VPN	Webブラウザがクライアント	アプリケーションが制限される
OpenVPN	アプリケーションが制限されない	クライアントソフトの導入が必要 通信速度が遅い

共通の問題：エンドエンドで暗号化できない

PPTP：Point-to-Point Tunneling Protocol
VPN：Virtual Private Network

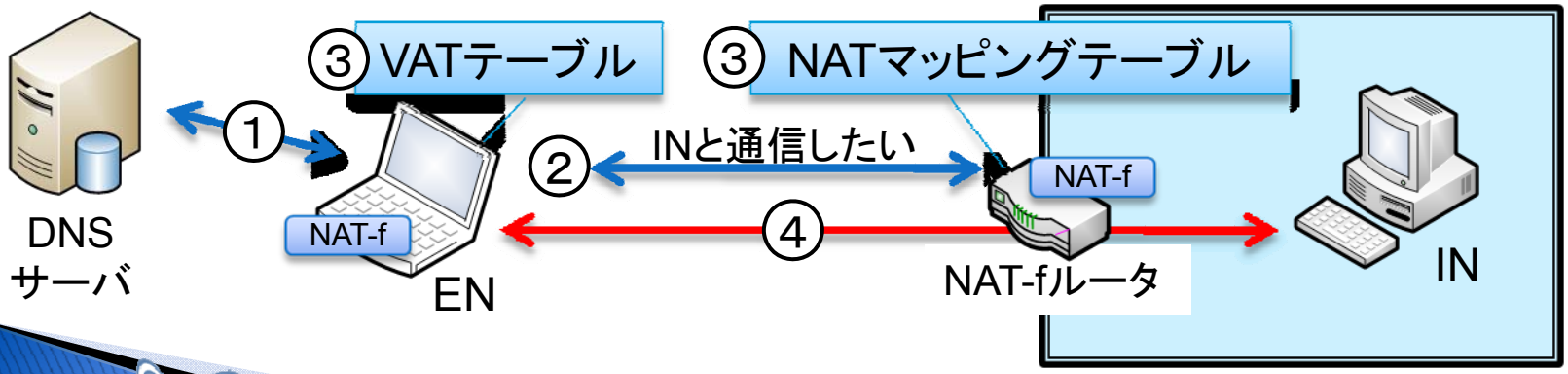
提案方式

- GSRA(Group-based Secure Remote Access)
  - NAT越え※技術を基盤とする
  - ✓NAT-f（NAT-free protocol）
    - NATの外側からNATにマッピングを実行させる
    - ENとNATにアドレス変換テーブルを生成
    - アドレス変換を行いながら通信

※NAT越え問題
NATの外側から通信を開始できない

リモートアクセスに足りない機能を追加

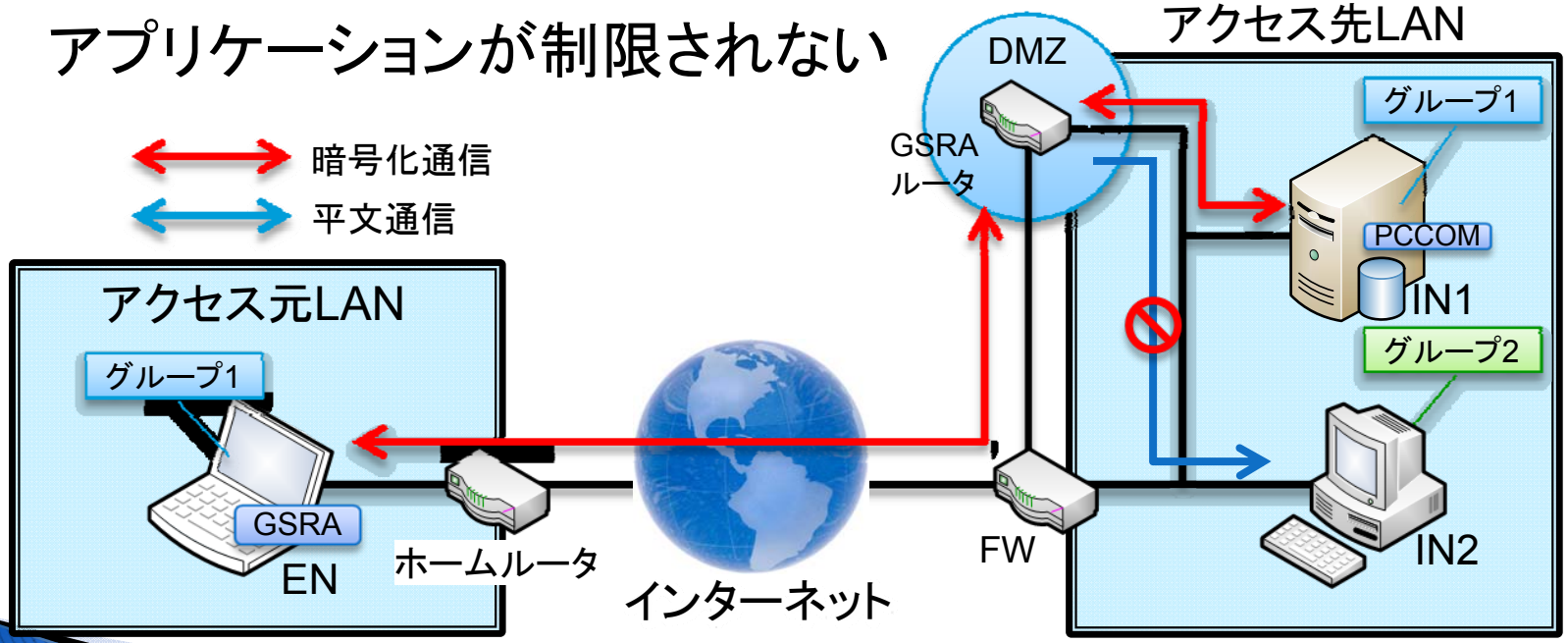
→アクセス制御，暗号化，ENがNAT配下の場合に対応



EN(External Node)：外部ノード
IN(Internal Node)：内部ノード
VAT（Virtual Address Translation）：仮想アドレス変換

提案方式の特徴

- 通信グループを定義してアクセス制御
- EN側にNATが存在する場合に対応
- PCCOM[1]によりNATを跨った暗号化通信が可能
- ネットワークアドレスが重複しても良い
- アプリケーションが制限されない



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

[1]増田. 他, 情処学論, Vol.47, No.7, pp.2258–2266(2006).

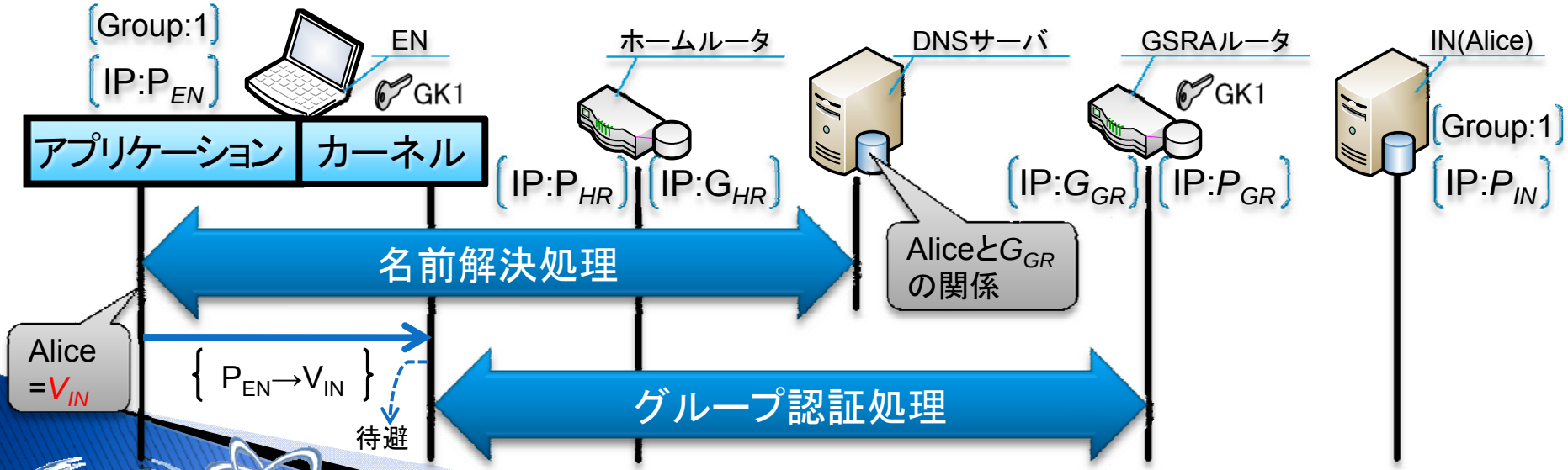
GSRA通信シーケンス1

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する

② グループ認証処理

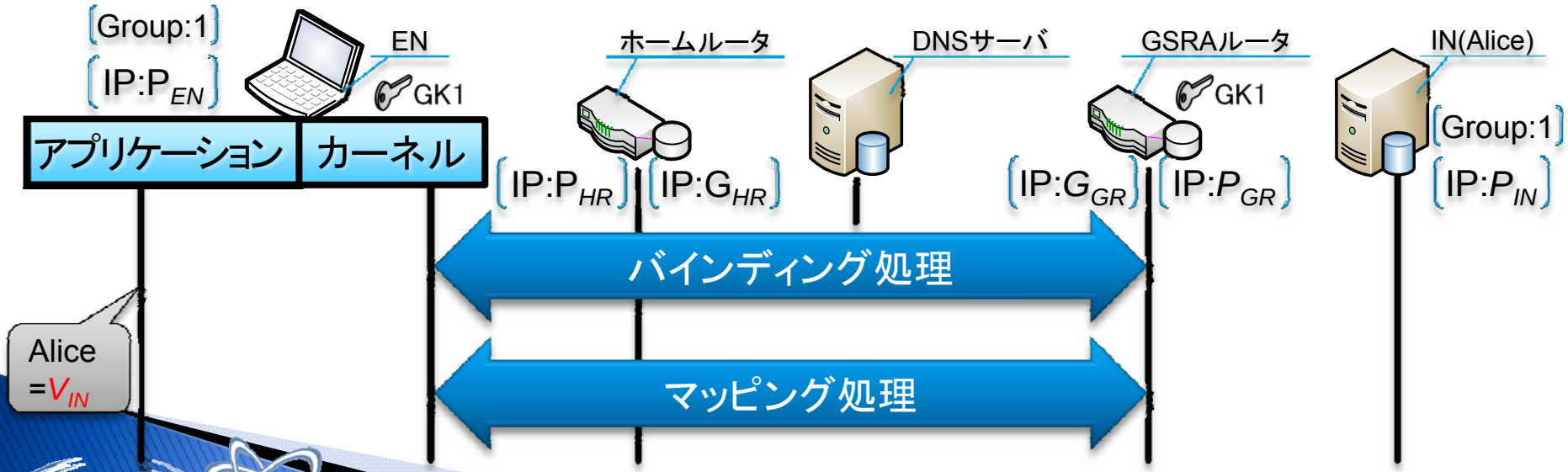
- ✓ ENとINが同一グループかどうか認証
  - 同グループ⇒アクセス許可
  - 異グループ⇒アクセス拒否



GSRA通信シーケンス2

③ バインディング処理
- ✓ EN側にNATが存在する場合に行う
- ✓ ホームルータのマッピングアドレスG_{HR}をENに通知する

④ マッピング処理
- ✓ GSRAルータにGSRAマッピングテーブルを生成
- ✓ ENにVAT※テーブルを生成　※VAT(Virtual Address Translation):仮想アドレス変換

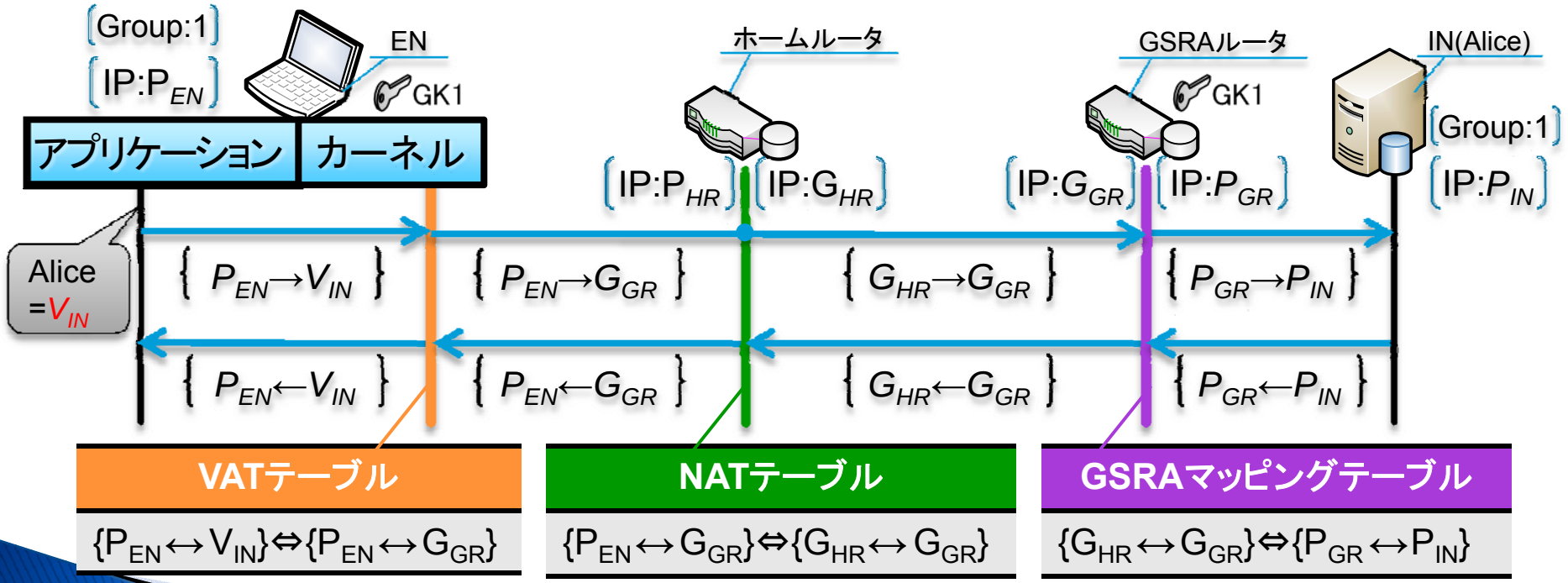


以後の通信

⑤ 生成したテーブルに従ってアドレスを変換しながら通信

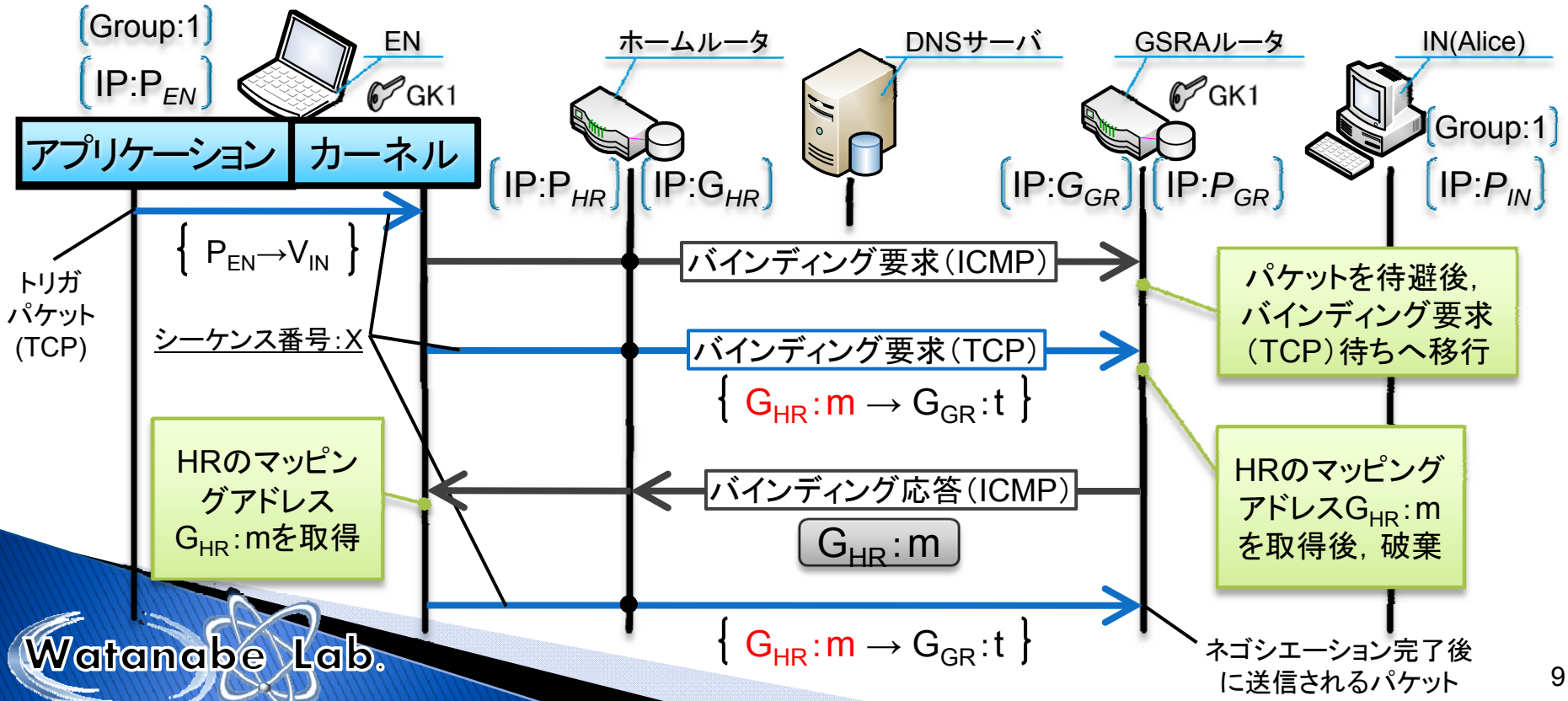
- ✓ EN（カーネル）：VATテーブル
- ✓ NAT　　：NATテーブル
- ✓ GSRAルータ　：GSRAマッピングテーブル

↔：通信
⇔：変換



バインディング処理

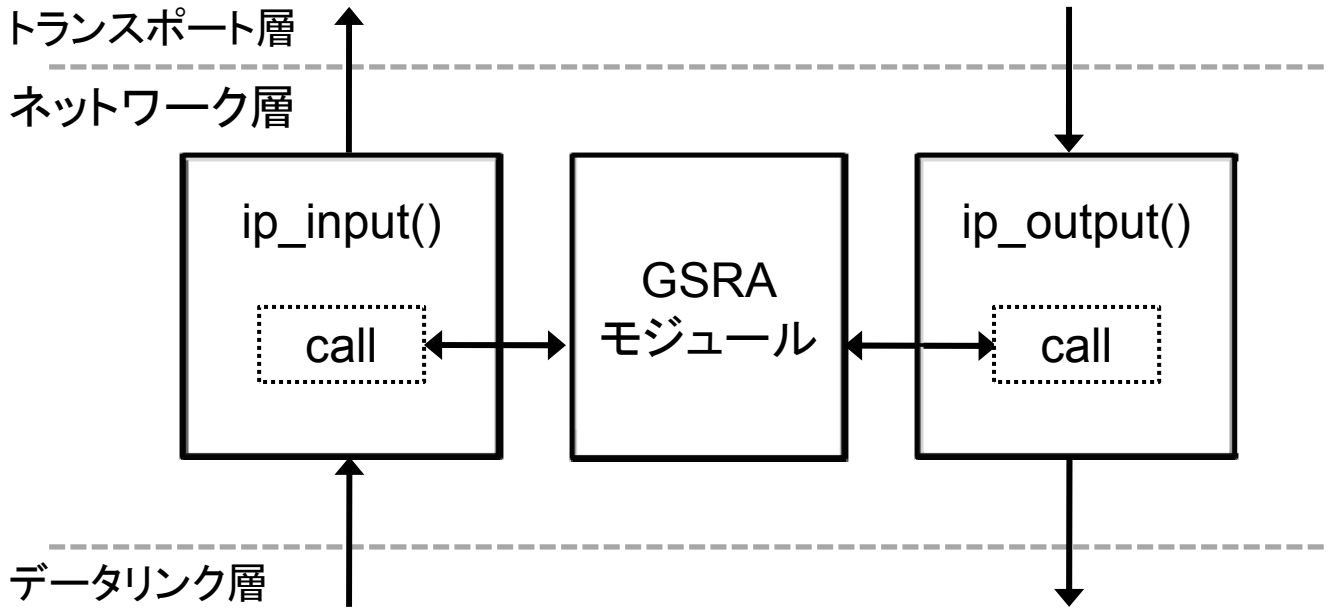
- ホームルータのマッピング内容を前もって確認
- シーケンス番号の整合性を確保
  - 受け取ったTCPのバインディング要求を破棄
    ⇒ネゴシエーション完了後に送信されるパケット→再送パケット



既存方式との比較

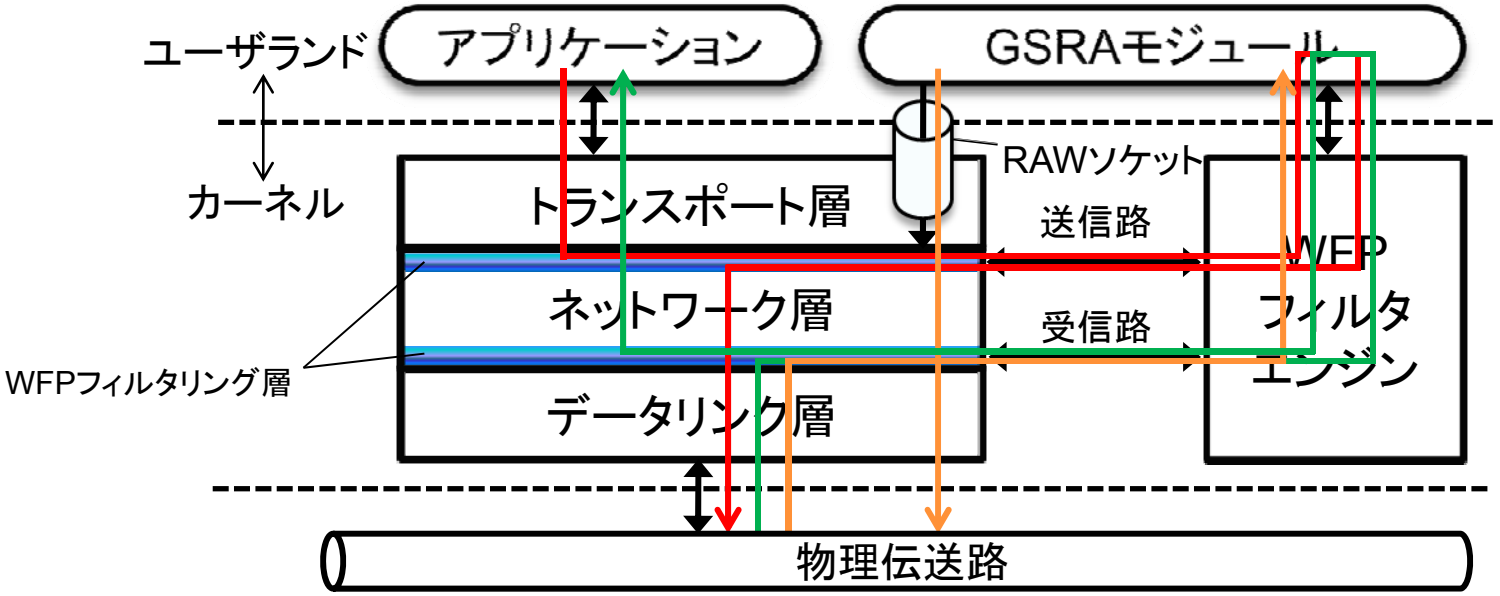
	ソフト導入(EN)	アプリ制限	NAT	アドレス重複	エンドエンド暗号化
PPTP	○	○	△	△	×
IPsec-VPN	×	○	△	△	×
SSL-VPN	○	△	○	○	×
OpenVPN	×	○	○	△	×
GSRA	×	○	○	○	○

実装：FreeBSD



- ネットワーク層の入出力関数でパケットをGSRAモジュールへ渡す
- アドレス変換等の処理を行った後，元の位置に差し戻し

実装：Windows



- WFP（Windows Filtering Platform）を利用する
  - 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制御パケット：送信にはRAWソケットを使用

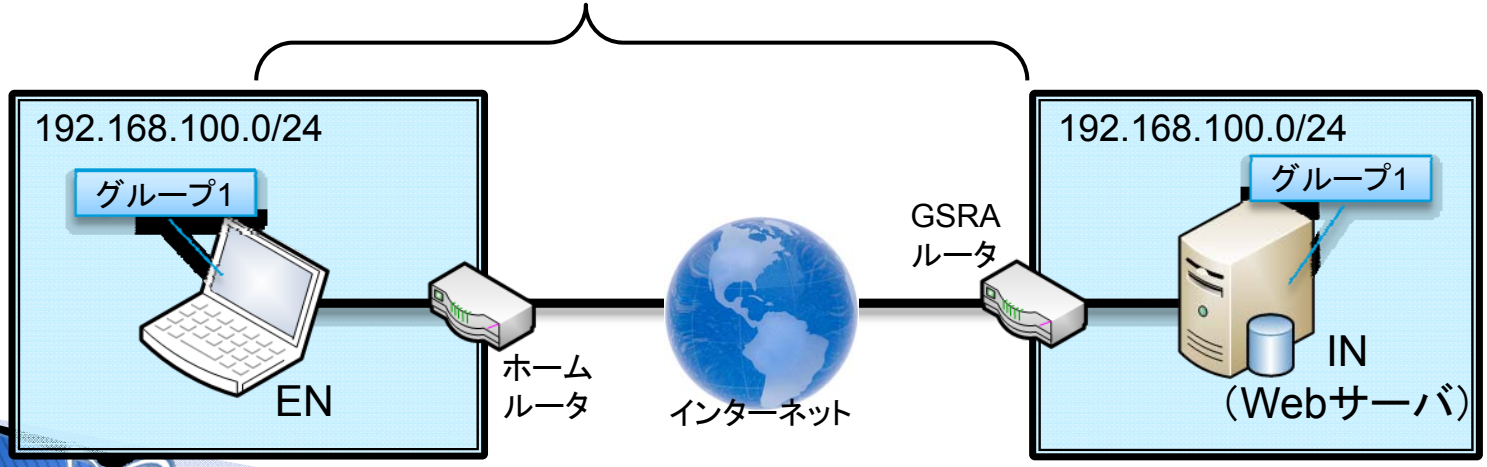
GSRAモジュールで処理後差し戻し

アドレス変換，暗号化／復号

性能評価：オーバヘッド

- 提案方式独自のネゴシエーションにより発生するオーバヘッド
  - グループ認証開始～TCPパケット送信までの時間をWiresharkで測定

	EN	GSRAルータ
OS	FreeBSD7.2	
CPU	Atom N270 (1.60GHz)	Geode LX800 (500MHz)
メモリ	1GB	128MB
NIC	100BASE-TX	



RTT(Round Trip Time)：往復遅延時間

測定結果:オーバヘッド

- 発生するオーバヘッド
  - グループ認証開始～TCPパケット送信　:66.56[ms]
  - EN-GSRAルータ間のRTT　:22.10[ms]

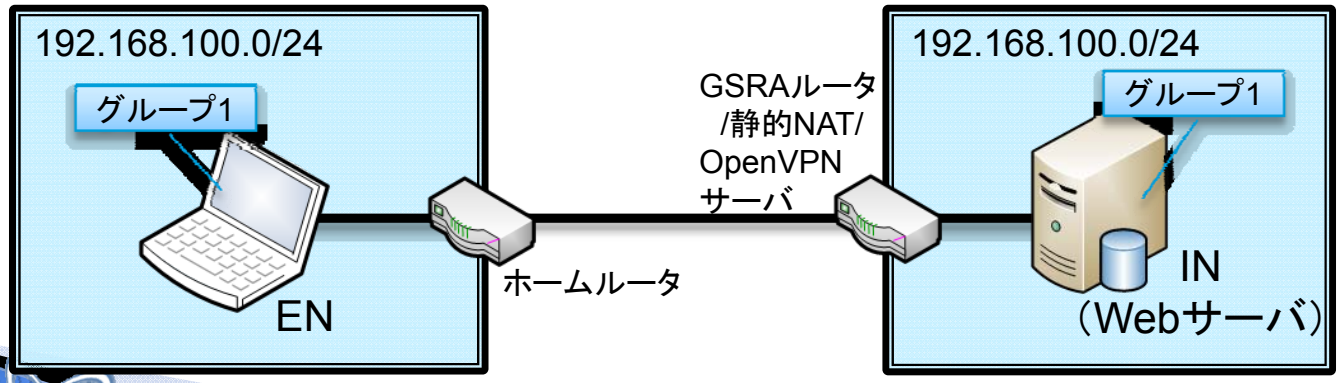
※測定結果は10回試行した平均値

- GSRAネゴシエーション≒3RTT
- EN，GSRAルータにおける処理時間は十分小さい

性能評価：スループット

- 接続確立後のスループット
  - Webサーバからファイルをダウンロード
  - 暗号化無/暗号化有（EN-GR間）の場合
- 比較対象
  - 暗号化無し：静的NAT（natd※）
  - 暗号化有り：OpenVPN

	EN	GSRAルータ/静的NAT/OpenVPNサーバ
OS	FreeBSD7.2	
CPU	Atom N270 (1.60GHz)	Geode LX800 (500MHz)
メモリ	1GB	128MB
NIC	100BASE-TX	



※natd：FreeBSDマシンをNAT化するデーモン

測定結果：スループット

- スループット［Mbps］

	GSRA	OpenVPN	静的NAT
暗号化無し	77.68		43.12
暗号化有り	25.68	9.76	

※測定結果はそれぞれ10回試行した平均値

- 暗号化有り/無し共にGSRAのスループットが優れている

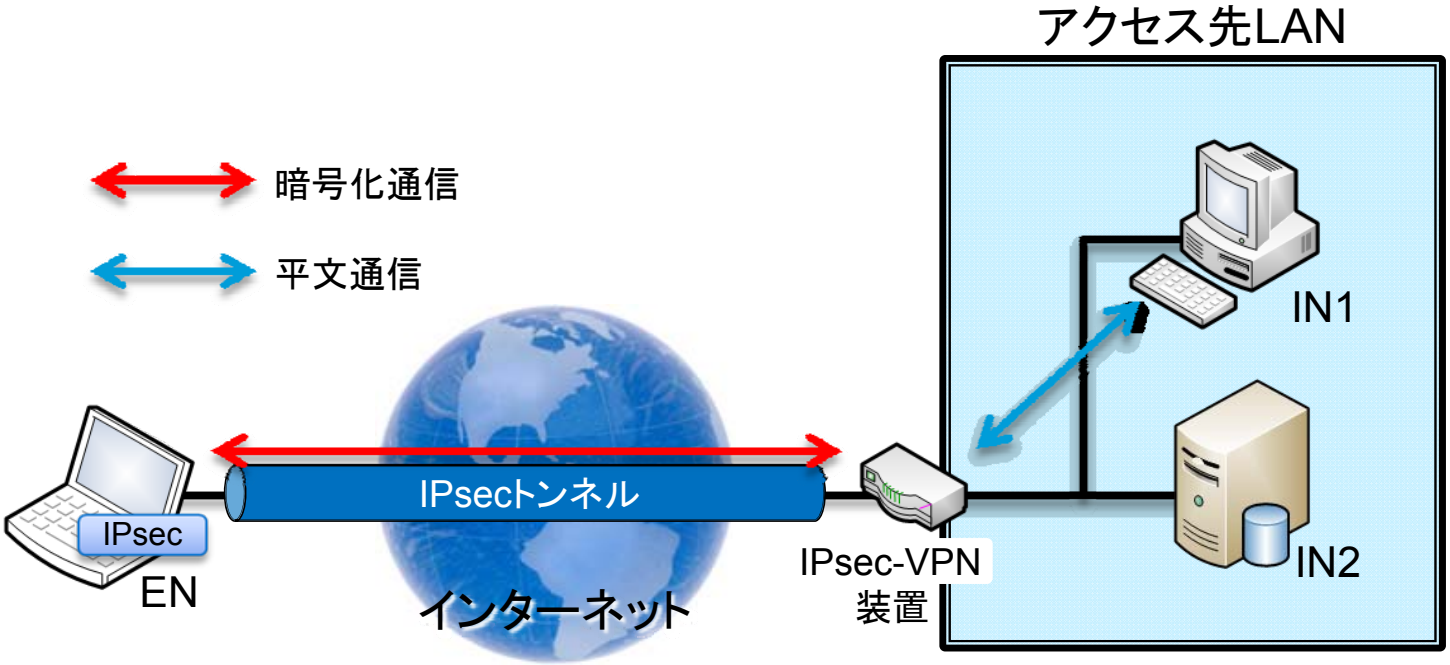
まとめ

- リモートアクセス方式GSRAを提案した
  - NAT越え技術を基盤とした方式
  - ENがNAT配下に居ても利用できる
  - グルーピングによるアクセス制御を行う
- 提案方式Windowsへの実装方法を検討した
  - ネットワーク機能を拡張できるWFPを利用する
- 提案方式をFreeBSDに実装し性能を評価した
  - 発生するオーバヘッドは小さく，高スループットを実現
- 今後はWindowsへの実装と性能評価を行う

補足資料

既存方式：IPsec-VPN

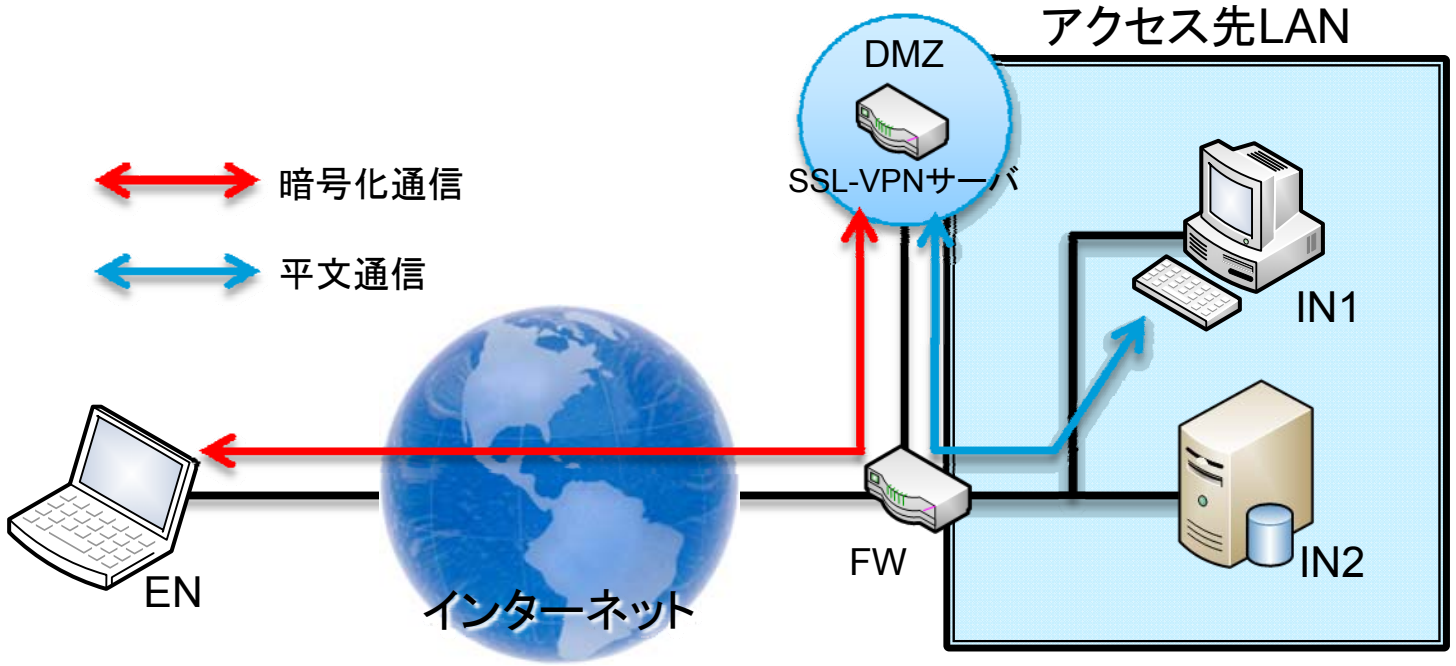
- IPsecトンネルを利用してVPNを構築する
- IPレベルで暗号化：アプリケーションに依存しない
- 端末ごとに設定が必要：管理負荷が大きい



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

既存方式：SSL-VPN

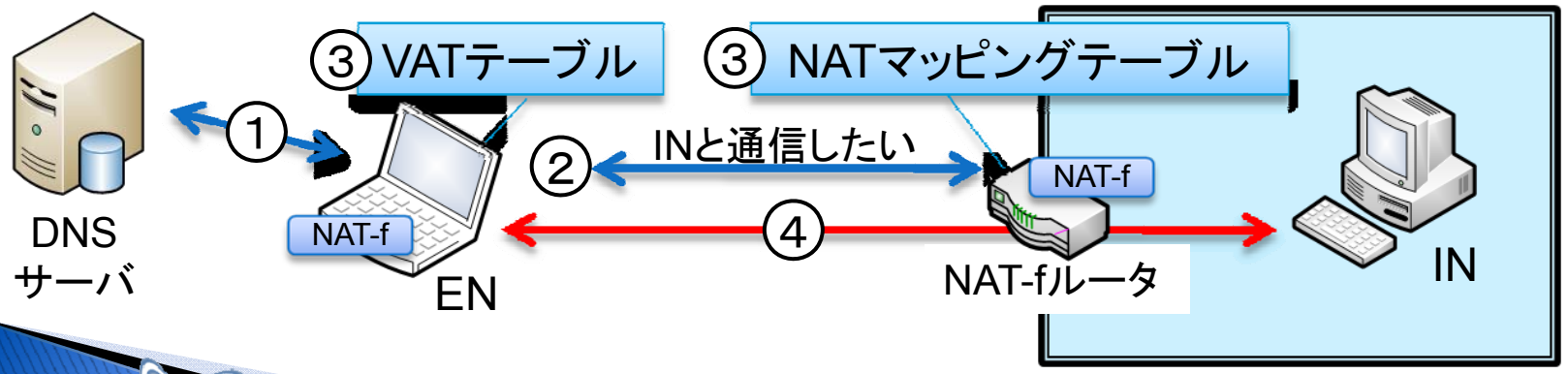
- SSL-VPNサーバがプロキシの役割
- EN側にはWebブラウザさえあれば良い
- アプリケーションが限定される



DMZ(DeMilitarized Zone)：非武装地帯

要素技術：NAT-f

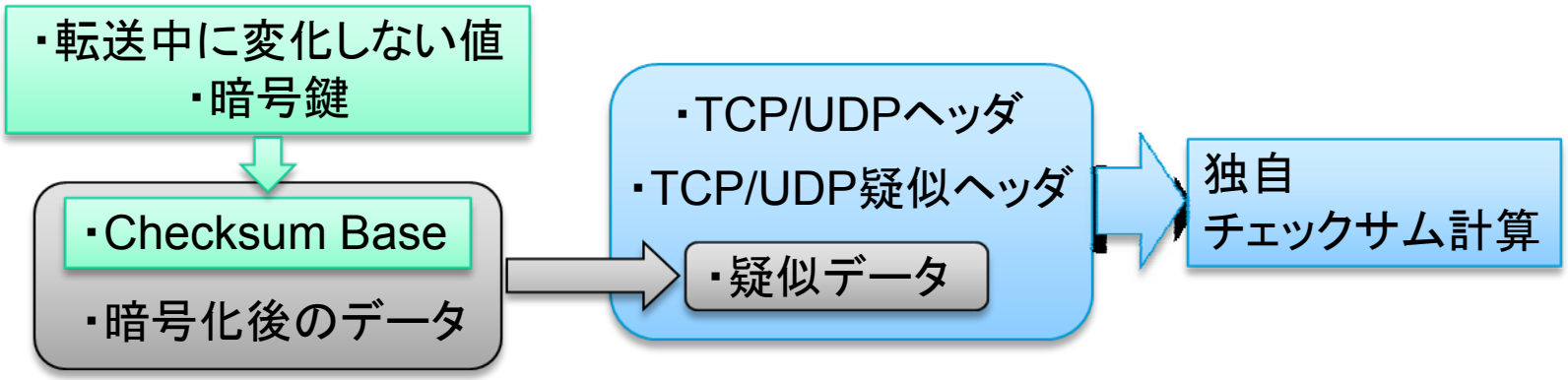
- NAT-f (NAT-free protocol)
  - ① ENはINを仮想IPアドレスで認識する
  - ② ENからNATにマッピングテーブルを生成させる
  - ③ NATのマッピング内容に対応するVATテーブルをENに生成する
  - ④ 生成したテーブルに従いアドレスを変換しながら通信を行う



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



仮想アドレスの生成方法

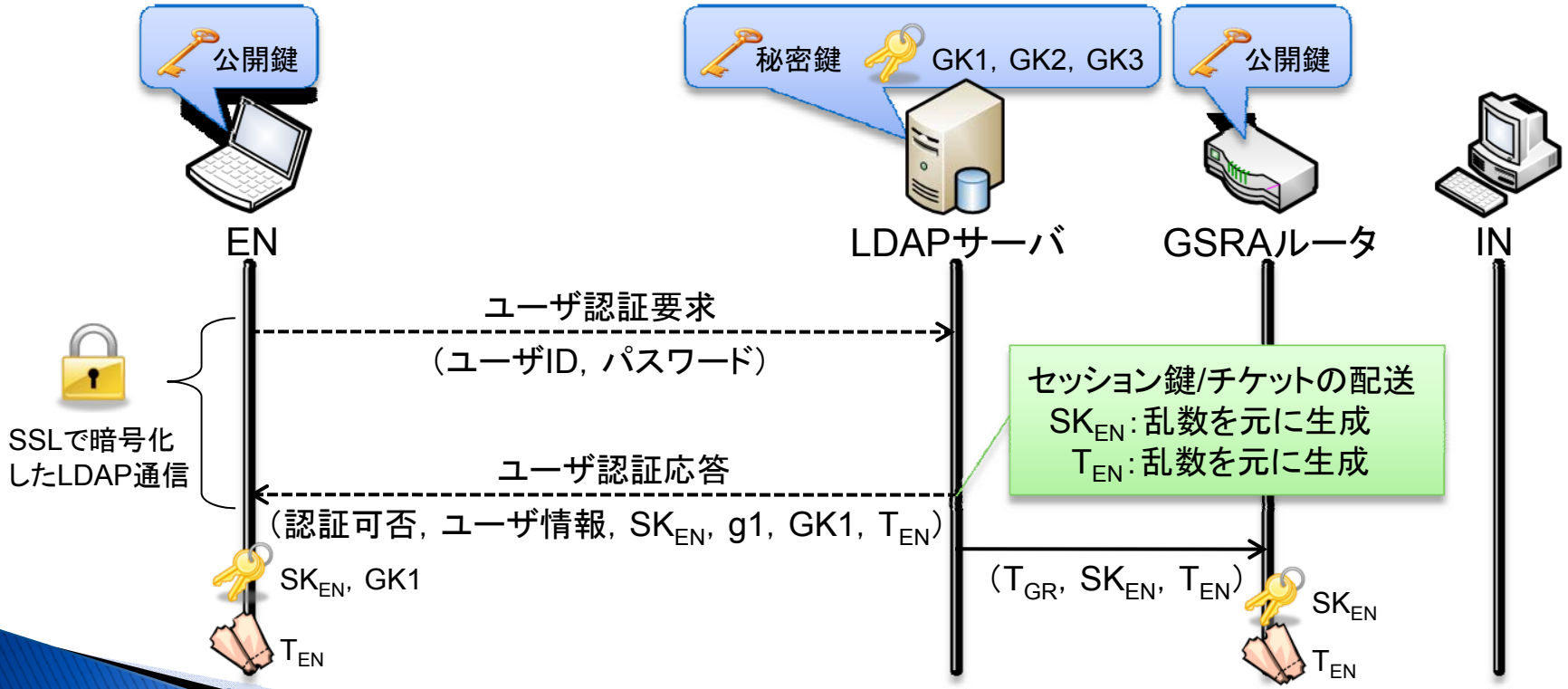
- INのFQDNから生成する
- V_{IN}＝A.B.C.D
  - A：仮想アドレスと認識するための値
    - ENから到達性がない値
  - B：初期値=0
    - 仮想アドレスが重複した場合に変化させる
  - C：ドメイン名(example.net)のハッシュ値
  - D：ホスト名(alice)のハッシュ値

IN：alice.example.net

FQDN： Fully Qualified Domain Name

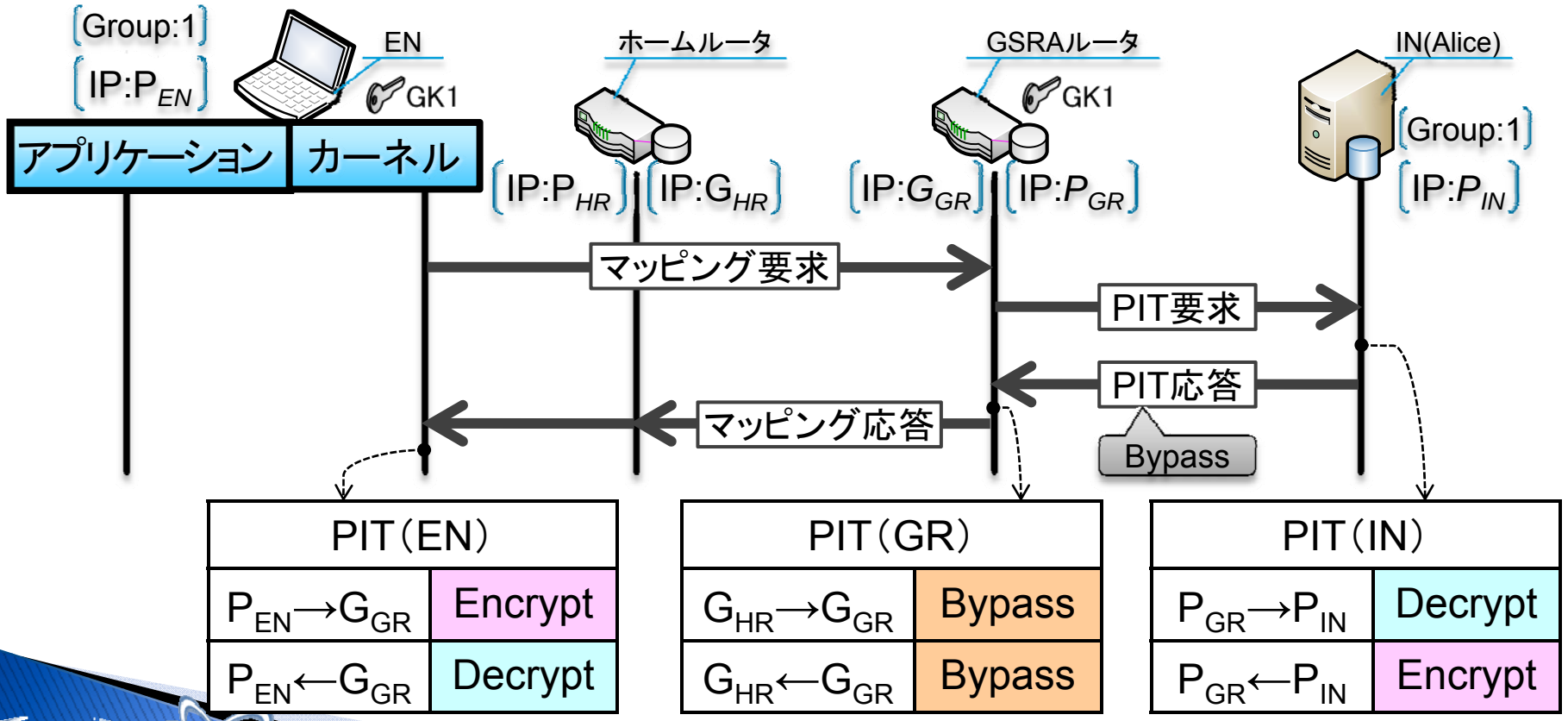
暗号鍵の配送について

- LDAP（Lightweight Directory Access Protocol）
  - ディレクトリサービスへとアクセスするためのプロトコル
  - ユーザ名などのキー値から情報を検索することが可能

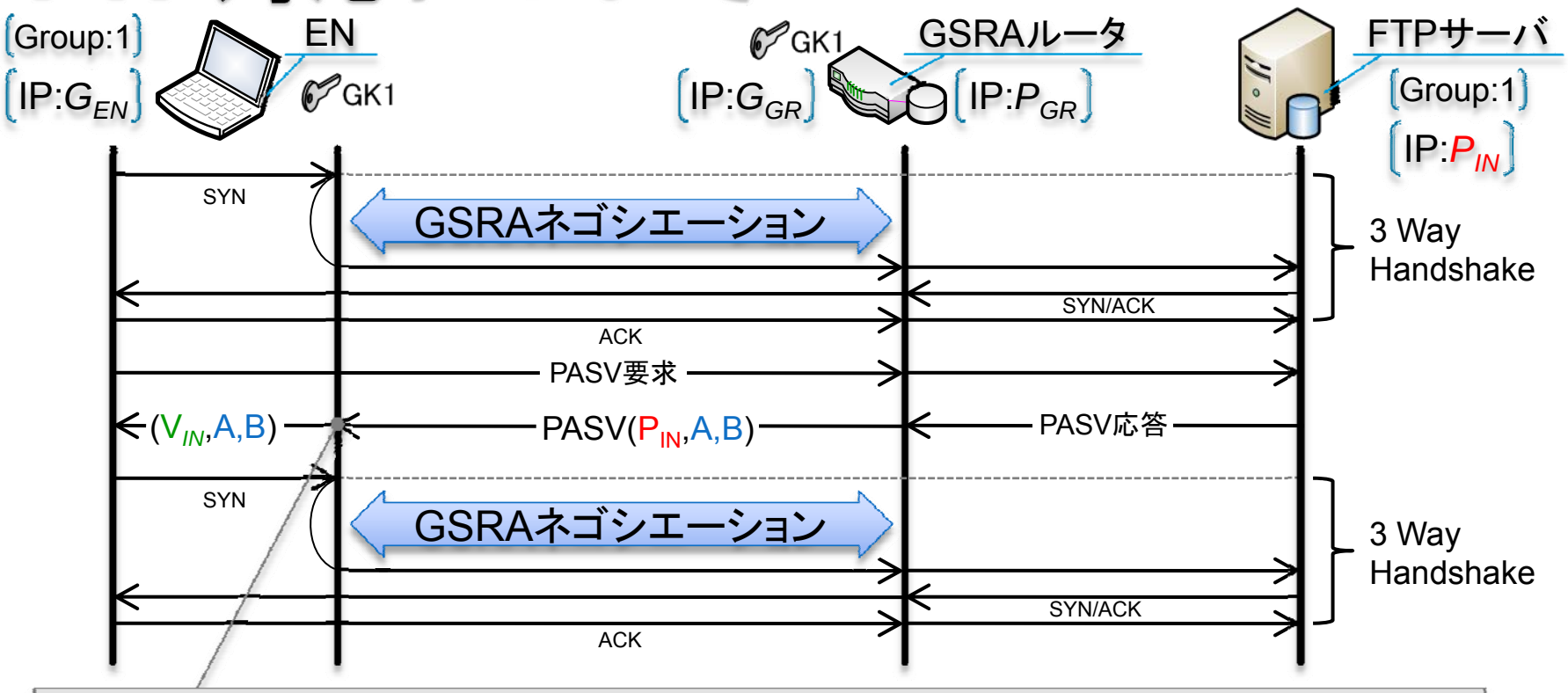


INがPCCOMをサポートする場合

- INにPIT（Process Information Table）を生成
- GSRAルータはアドレス変換のみ行う



FTP対応について



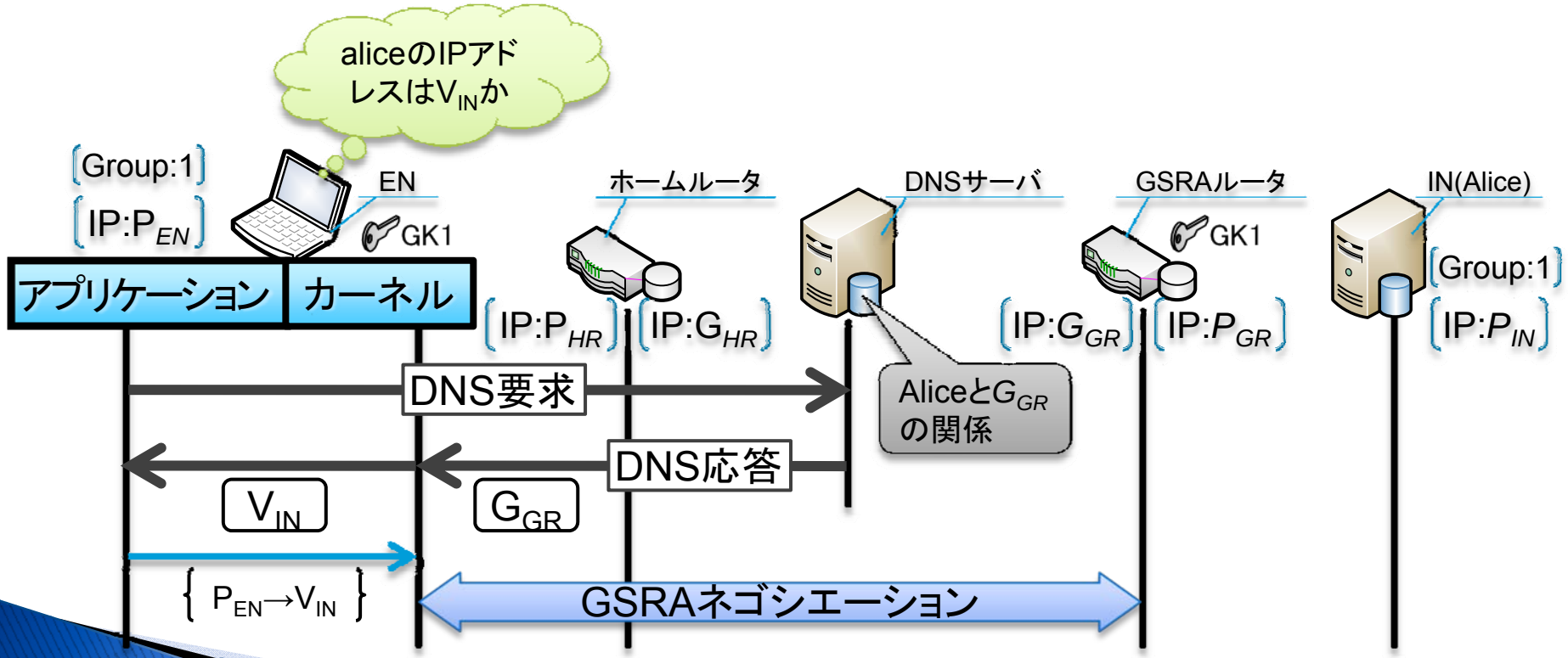
PASV応答メッセージ内のサーバIPアドレスを仮想IPアドレスに書き換え
＆ポート番号をGSRAルータへ通知→エイリアスリストを生成

※FTPサーバがPCCOM対応（エンドエンドで暗号化通信）の場合

- 応答メッセージを送信する前にポート番号をGSRAルータに通知

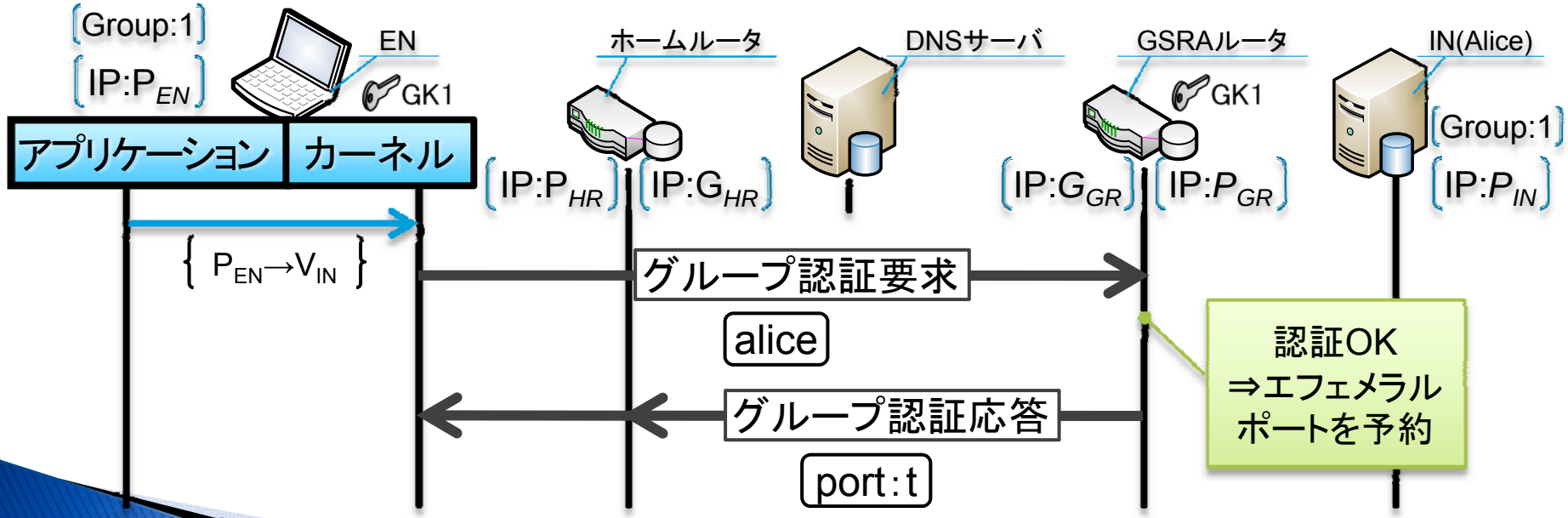
名前解決処理

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



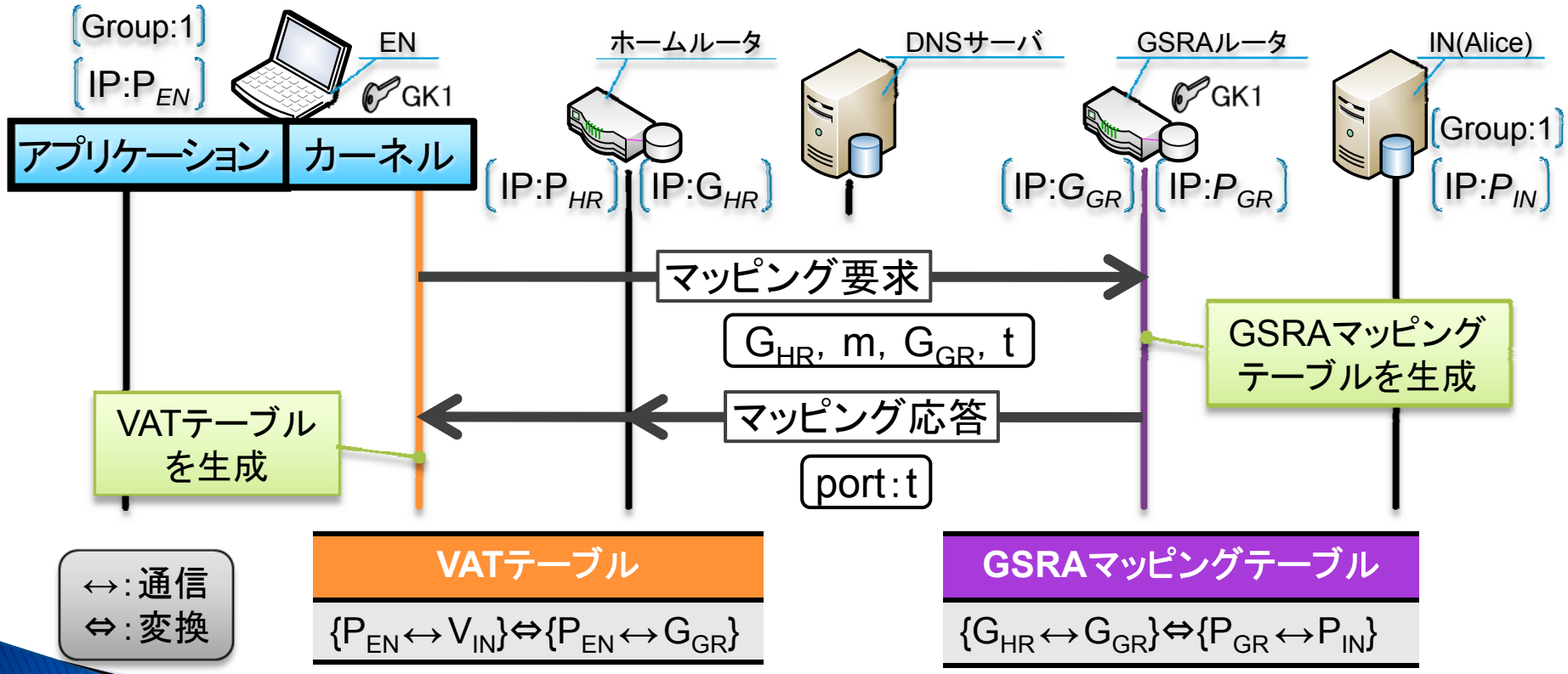
グループ認証処理

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

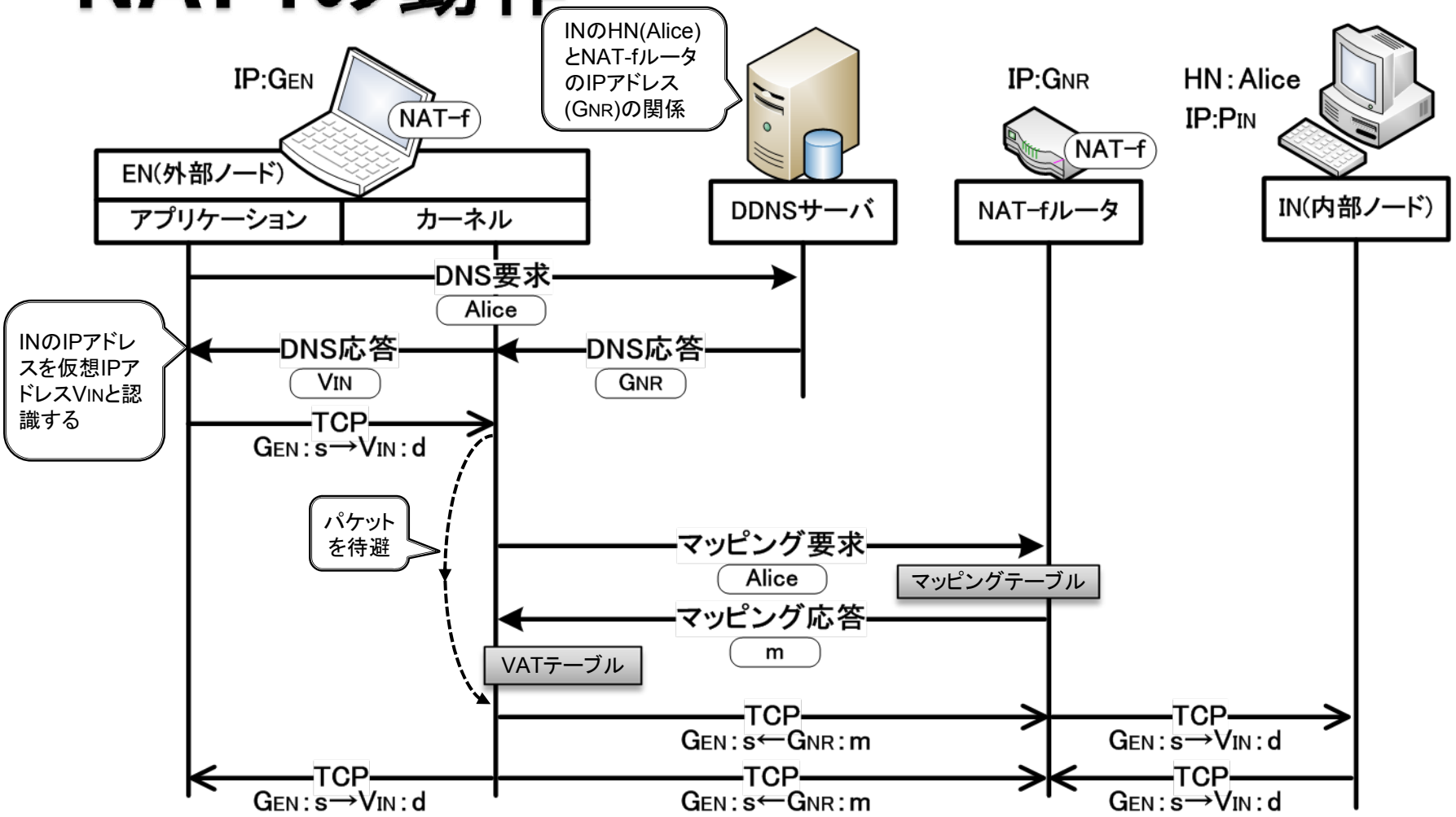


マッピング処理

① GSRAマッピングテーブル：NATマッピングとINを対応させる
② VATテーブル：仮想IPアドレスを実アドレスに変換する



NAT-fの動作



VATテーブル

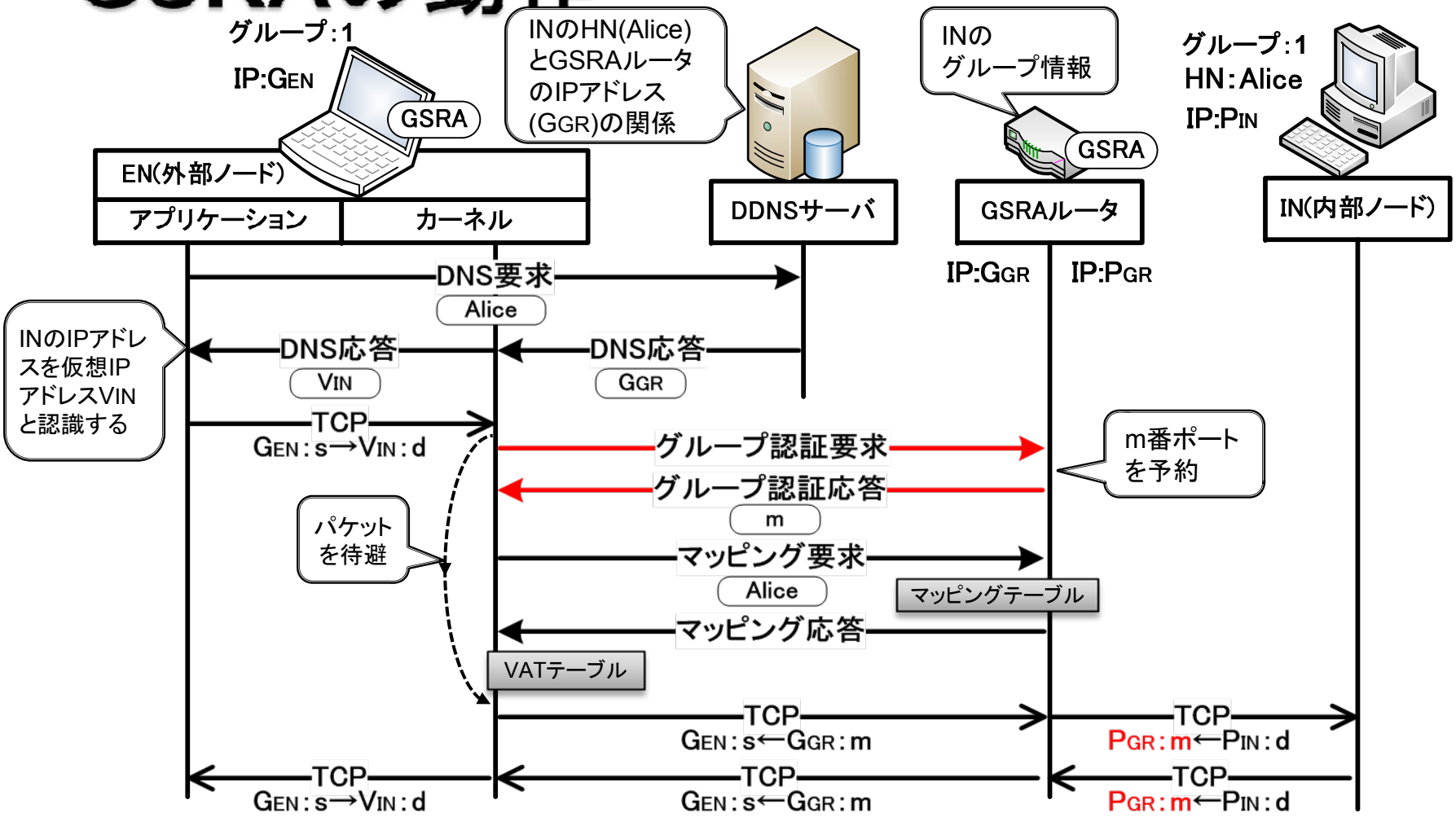
GEN:s↔VIN:d⇔GEN:s↔GNR:m

マッピングテーブル

GEN:s↔GNR:m⇔GEN:s↔PIN:d

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

GSRAの動作



VATテーブル	アドレス変換テーブル
{GEN:s↔VIN:d}⇔{GEN:s↔GGR:m}	{GEN:s↔GGR:m}⇔{PGR:m↔PIN:d}

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