NAT-f を応用したリモートアクセス方式 GSRA の提案

鈴木　健太*，鈴木　秀和，渡邊　晃（名城大学）

Proposal of Remote Access Method “GSRA” applying NAT-f

Kenta Suzuki, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

近年，プライベート/ビジネスを問わず幅広いシーンでリモートアクセス技術の需要が高まっている．リモートアクセスにおける代表的な方式に IPsec-VPN と SSL-VPN がある．しかし IPsec-VPN は設定項目が複雑であり，NAT を通過できない等の問題がある．SSL-VPN では，使用するアプリケーションが限定される問題がある．

本稿では，前述の問題点を解決し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．

２．提案方式

GSRA は，我々が提案している NAT-f（NAT-free protocol）[1][2]を応用することで実現される．

図 1 に GSRA の通信シーケンスを示す．リモートアクセスを行う外部ノードを EN，内部ノードを IN，GSRA の機能が実装されたルータを GSRA ルータと表記する．ユーザは事前に利用者登録を行い，ユーザ ID とグループ設定が GSRA ルータ内の GSRA 用データベースに登録されているものとする．

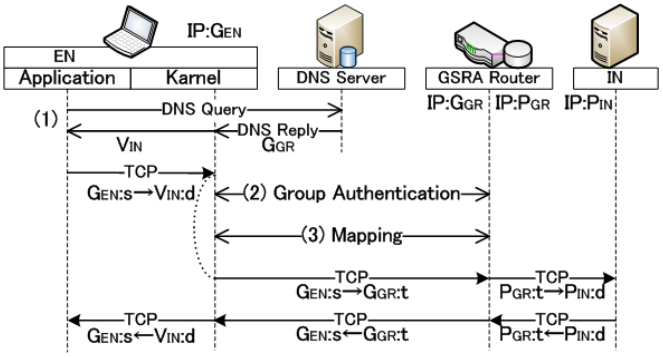


fig.1.GSRA sequence

(1)DNS 名前解決

EN は IN へ通信を開始する際，名前解決を行うため，DNS サーバに DNS クエリを送信する．DNS 応答により取得した IP アドレス G_{GR} を EN のカーネル領域でフックし，仮想 IP アドレス V_{IN} に書き換える．これにより EN のアプリケーションは IN の IP アドレスを V_{IN} と認識する．

その後，EN から宛先が仮想 IP アドレスとなっているパケットが送信される場合，仮想アドレス変換（VAT : Virtual Address Translation）テーブルを検索する．該当エントリが存在しない場合は VAT テーブルを仮生成し，トリガとなったパケットを待避する．その後グループ認証要求を GSRA ルータに送信し(2)の処理へ移る．既に該当エントリが存在する場合，そのエントリに基づき宛先を変換する．さらに動作処理情報テーブル（PIT : Process Information Table）を検索し，該当の動作処理情報に従いパケットを暗号化する．

(2)グループ認証

GSRA ルータがグループ認証要求を受信すると，GSRA 用データベースを参照して EN と IN 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，アクセスが承認された場合，通信に使用するポート番号 t を予約して EN へ応答を返す．応答を受信した EN はポート番号 t を取得し，VAT テーブルを更新する．続いてマッピング要求を GSRA ルータへ送信する．

(3)マッピング処理

GSRA ルータは，マッピング要求で取得したセッション情報からアドレス変換テーブルと PIT を生成し，応答を返す．

以後，待避していたパケットを復帰させ，GSRA ルータのアドレス変換テーブル及び EN の VAT テーブルに基づいて宛先/送信元の IP アドレス/ポート番号が変換され，リモートアクセスが実現される．

３．比較評価

提案方式と既存方式の比較評価を行った結果を表 1 に示す．

Table 1　Comparison of remote access methods

	管理負荷	アドレス管理	NAT 通過	アプリケーション
IPsec-VPN	×	×	×	○
SSL-VPN	○	○	○	×
GSRA	△	○	○	○

GSRA を利用するユーザは，ソフトウェアを PC にインストールするだけであるため，管理負荷はユーザ数に比例する．IPsec のトンネルモードでは，VPN を構築した LAN 間が同一のネットワークとなるため，アドレス管理が必要となる．GSRA ではアドレス管理は不要であり，前述のように NAT を通過できる．また，アプリケーションは限定されない．従って，既存技術と比べても優れていると評価できる．

４．まとめ

リモートアクセス方式 GSRA を提案し，IPsec-VPN 及び SSL-VPN との比較評価を行った．今後は実装を行う．

文　献

[1] 鈴木．他：情処学論, Vol47, No.11, pp.2976-2991, 2006
[2] 鈴木．他：情処学論, Vol48, No.12, pp.3949-3961, 2007

NAT-fを応用したリモートアクセス方式GSRAの提案

名城大学　理工学部
鈴木　健太，鈴木　秀和，渡邊　晃

はじめに

- リモートアクセス
  - モバイルブロードバンドの普及によりニーズが高まっている
  - インターネットを通じてネットワークやコンピュータに外部から接続すること
  - メールの閲覧，ファイルの参照，アプリケーションの実行等の用途に用いられる

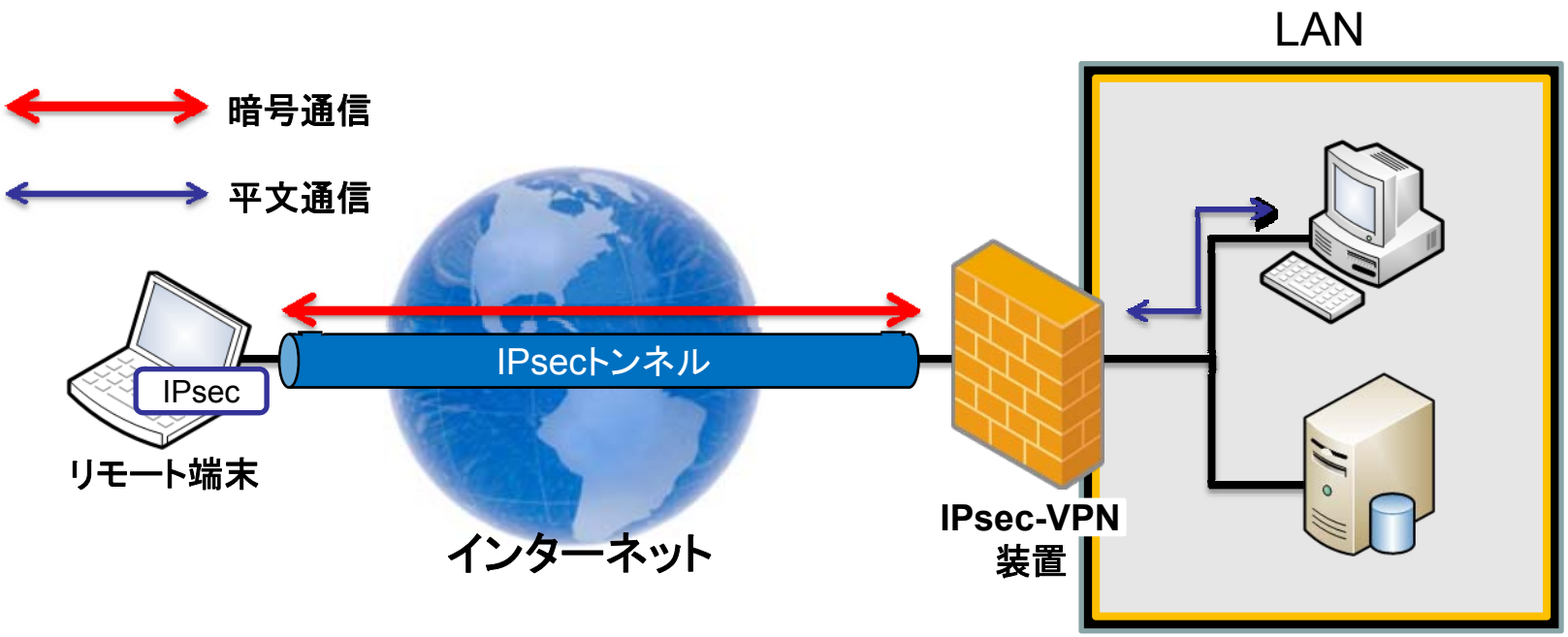
安全なリモートアクセスのために

- インターネット空間における脅威
  - 盗聴，改ざん，なりすまし

- VPNを利用したリモートアクセス
  - 暗号化，認証技術によりセキュリティを確保
  - 既存方式：IPsec-VPN，SSL-VPN

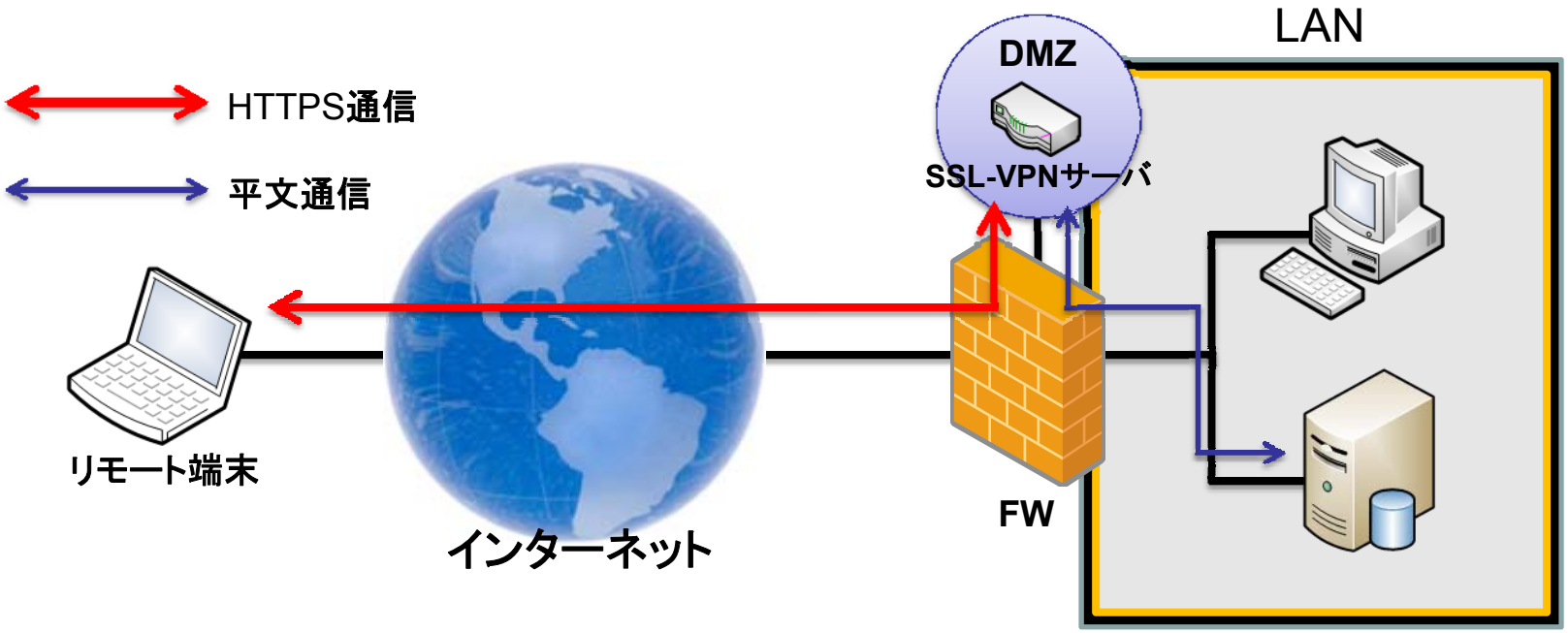
※VPN:Virtual Private Network

既存方式：IPsec-VPN



- ネットワーク層に実装→アプリケーションに依存しない
- 管理負荷が大きい
  -端末の追加等に伴い管理負荷が増大する

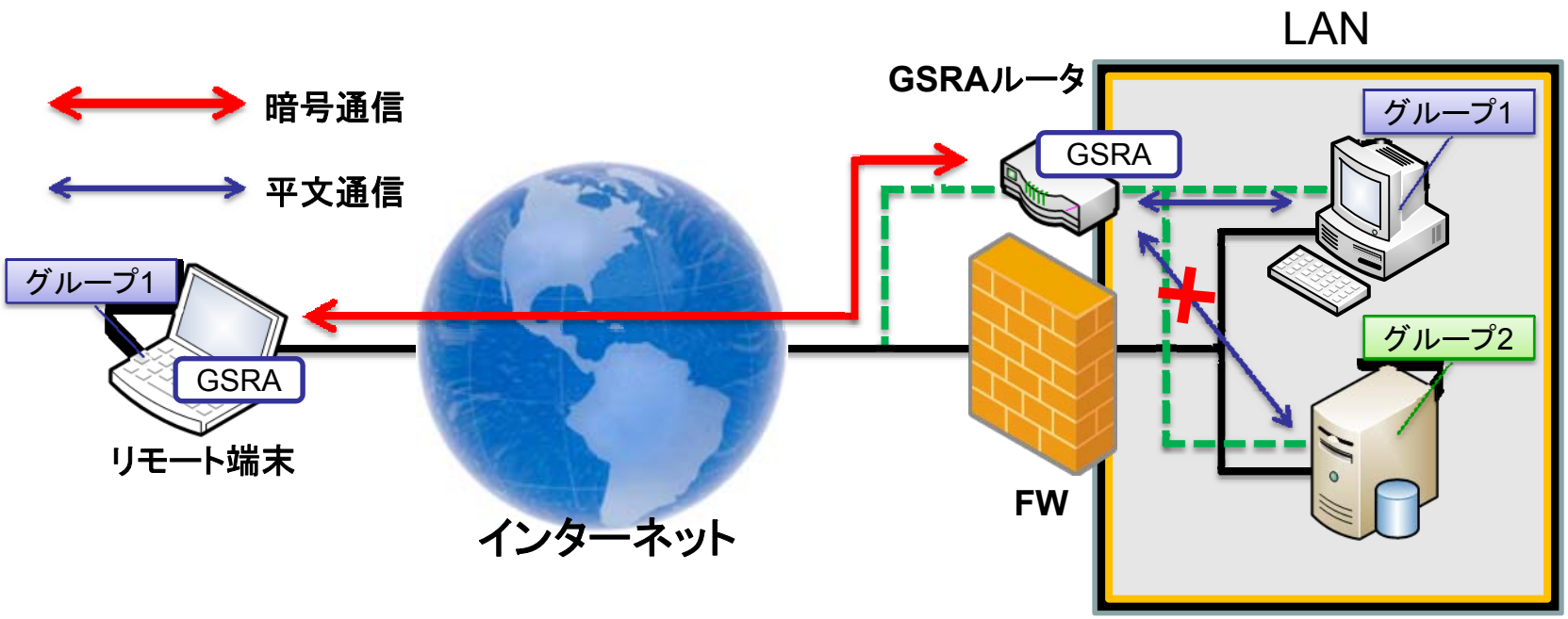
既存方式：SSL-VPN



- リモート側にはWebブラウザがあれば良い
- アプリケーションに実装→用途が限定される

DMZ(DeMilitarized Zone) : 非武装地帯

提案方式：GSRA(Group-based Secure Remote Access)



- ネットワーク層に実装
- 通信グループを設定し，グループ単位でアクセス制御を行う
- GSRAルータはGSRA専用の出入口として設置

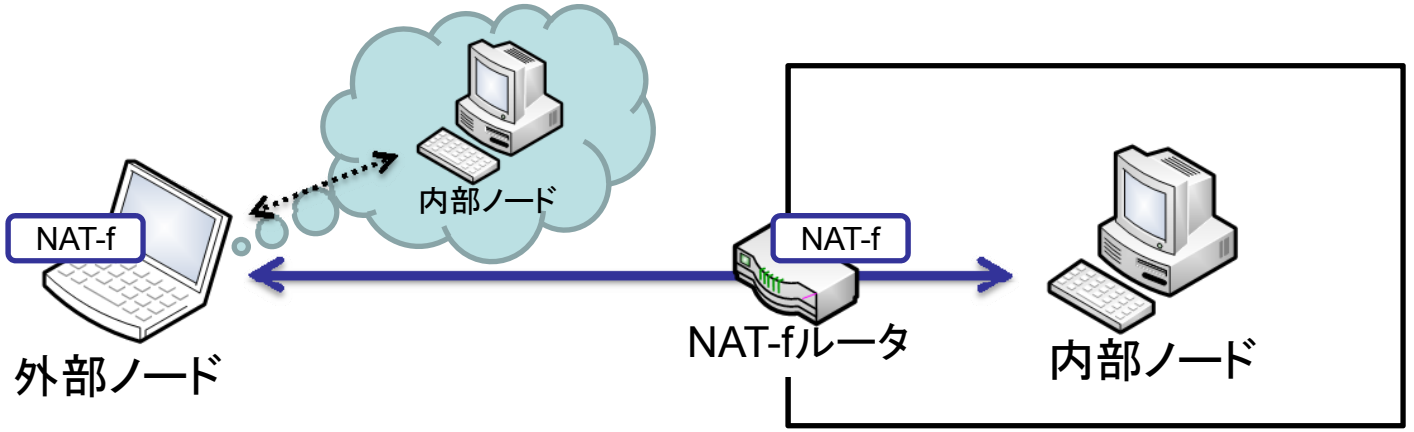
課題
- NAT越え問題 ⇒ NAT-fを利用する
- セキュリティの確保
- 通信の帰り道

} NAT-fを拡張する

NAT : Network Address Translation　NAT-f : NAT free protocol

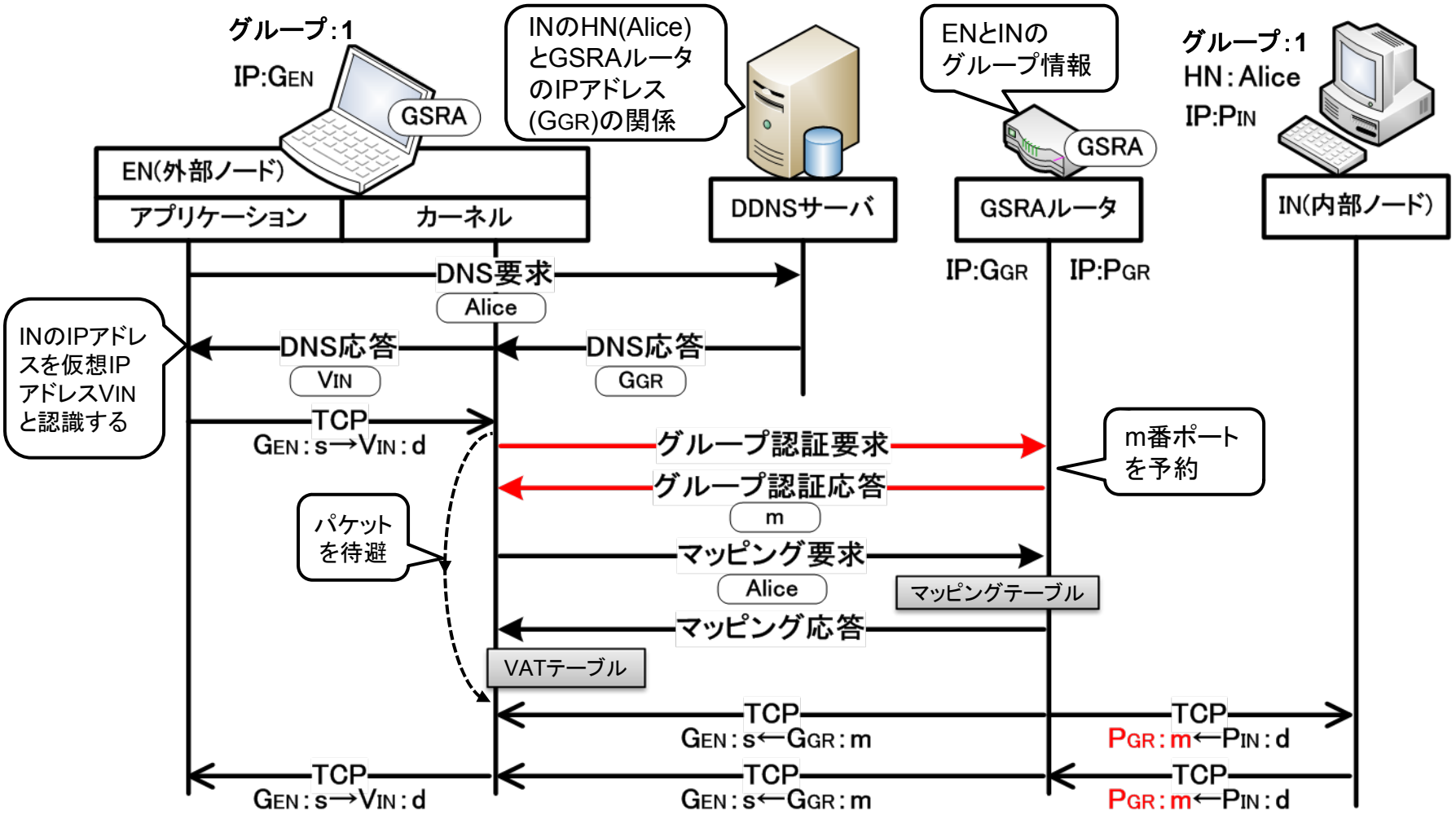
NAT-fの概要

- NAT-f (NAT-free protocol)
  - NATの外側からのネゴシエーションによってNATにマッピングを実行させるプロトコル
  - 外部ノードは内部ノードを仮想的に認識する
  - NATのマッピング内容に対応するVATテーブルを外部ノードに生成する



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

GSRAの動作



VATテーブル

{GEN:s↔VIN:d}⇔{GEN:s↔GGR:m}

マッピングテーブル

{GEN:s↔GGR:m}⇔{PGR:m↔PIN:d}

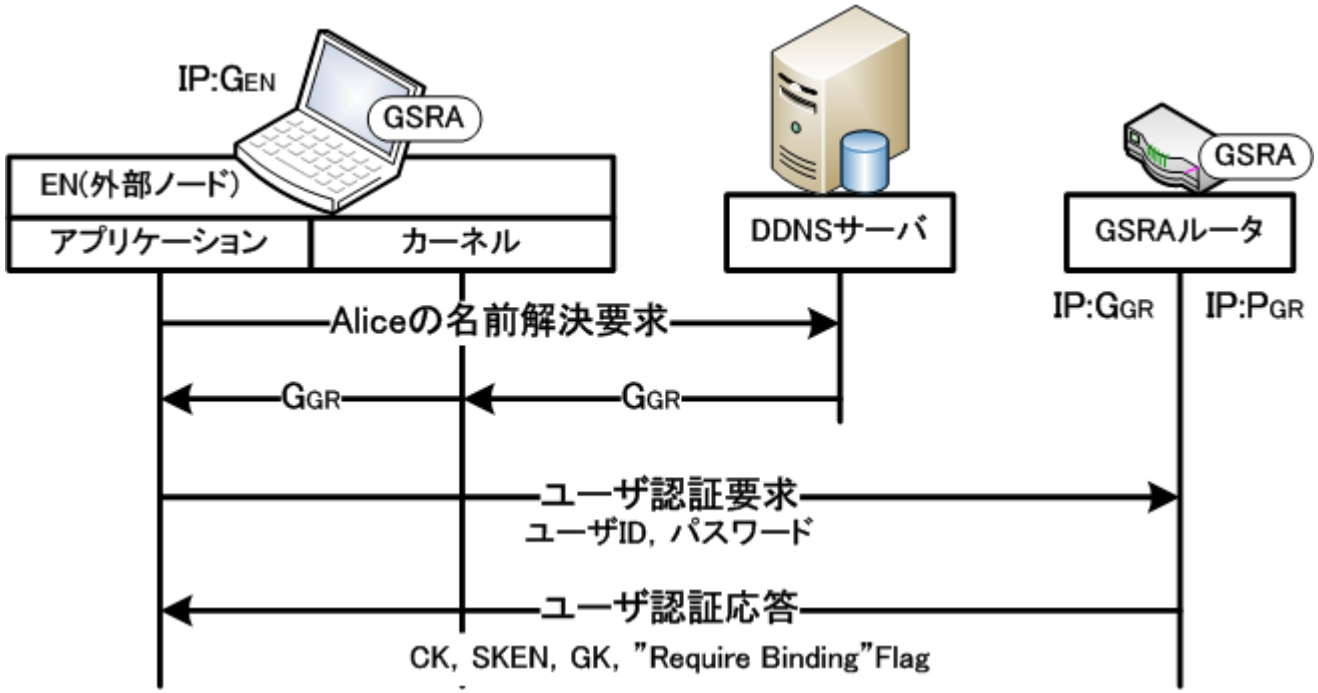
VAT（Virtual Address Translation）:仮想アドレス変換

まとめ

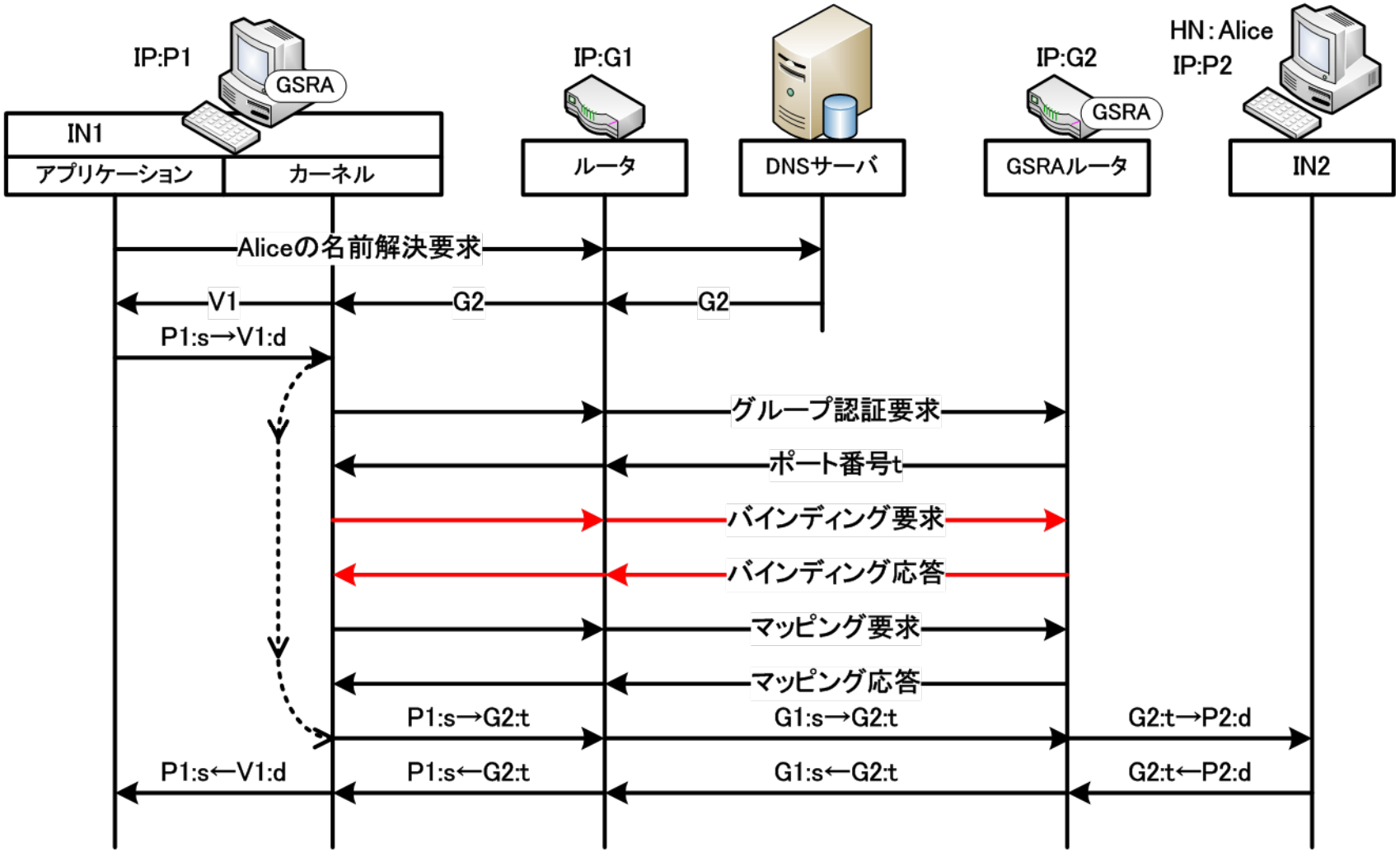
- リモートアクセス方式GSRAの提案を行った
  - ネットワークレベルの解決
  - グルーピングを用い管理負荷を軽減
- 今後は実装を行う

補足資料

ユーザ認証


IP:GEN
GSRA
EN(外部ノード)
アプリケーション
カーネル
DDNSサーバ
GSRA
GSRAルータ
IP:GGR
IP:PGR
Aliceの名前解決要求
GGR
GGR
ユーザ認証要求
ユーザID，パスワード
ユーザ認証応答
CK，SKEN，GK，"Require Binding"Flag

GSRAの動作（プライベート↔プライベート）



比較評価

	管理負荷	アプリケーション	専用ソフト （リモート側）
IPsec-VPN	×	○	必要
SSL-VPN	○	△	不要
GSRA	△	○	必要