# 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

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主に利用される方式には IPsec-VPN と SSL-VPN がある．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 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

Recently, because the spread of improving of the performance of a mobile terminal, and mobile broadband is remarkable, the demand for Remote access technology that can access to home and in-house PC from the remote place such as the movement and the business trip destinations has risen. There are IPsec-VPN and SSL-VPN in the method chiefly used by a remote access. IPsec-VPN has problems such as complex setting is necessary and compatibility with NAT is bad. Though SSL-VPN can be easily used, there is a problem that the application used is limited. In this paper, it proposes the method to achieve a remote access by adding the encryption function and the access control function, etc. to the NAT excess technology. In the proposal method, the existence of NAT doesn't worry, and a safe, remote access can be achieved.

## 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を利用することで，インターネットを通じて銀行取引を行うインターネットバンキングに代表される新たなサービスが可能になったり，在宅勤務や出張先での作業等の幅広い勤務形態が可能になる等，これまでにない多くのメリットを享受することができる．

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] 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ることが通常であり，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で安全なリモートアクセスを可能とした方式である．GSRA はすでに FreeBSD に実装が完了しているが，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した．

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．6 章で提案方式の評価を行い，最後に 7 章でまとめる．

## 2. 既存技術

現在一般的に利用されている既存の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 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，

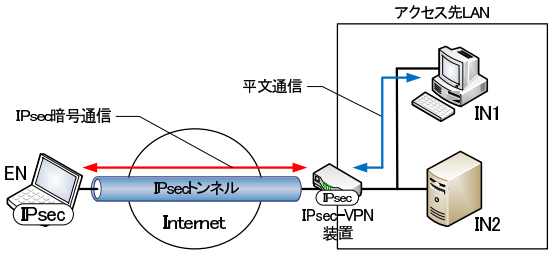


**図 1** IPsec-VPN によるリモートアクセスの構成例
Fig. 1 Example of composing by IPsec-VPN

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，管理負荷が大きい点と，エンドエンドで暗号化していない点が課題である．

### 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，ユーザによる設定は不要である．また，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を行っていない問題もある．

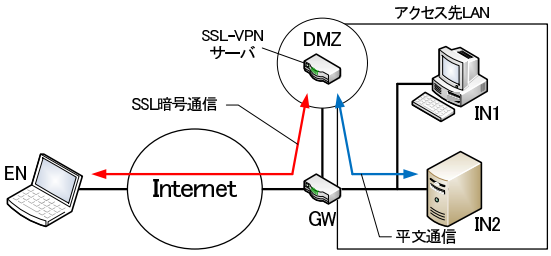


**図 2** SSL-VPN によるリモートアクセスの構成例
Fig. 2 Example of composing by SSL-VPN

## 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）[10] 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 GW 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 GW 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 GW 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 はカーネルにてパケットの中身を仮想 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 NAT 配下に位置している場合に対応していない．これらの課題はリモートアクセス方式として運用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 や PCCOM がある．

IPsec は TCP/UDP ヘッダ部が暗号化範囲に含まれているため，NAT を通過する際に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 NAT トラバーサル[9] があるが，ヘッダの

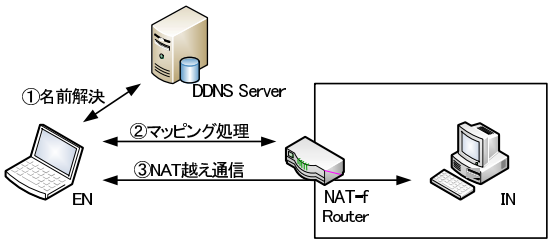


**図 3** NAT-f 通信シーケンス
Fig. 3 NAT-f sequence

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てしまう．従って，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で，本人性確認とパケットの完全性保証を実現できる．TCP/UDP ペイロード部を暗号化範囲とするため，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．

この方式によると，パケットフォーマットに変更を加えないため，追加のオーバヘッドが発生せず，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となる．

### 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．グループ毎の認証を行うことで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 に対応付けている．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，サブネットワーク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．

## 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，EN が 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，ホームルータには一切改造を加えない．

GSRA のネットワーク構成例を**図 4** に示す．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に GSRA 専用のゲートウェイとして設置する．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 のエンド間で暗号化通信が可能である．

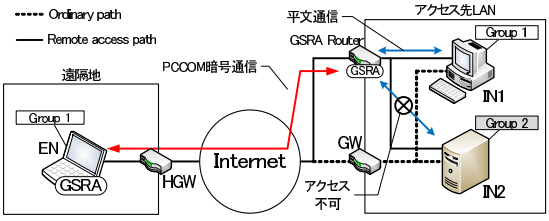


**図 4**　GSRA によるリモートアクセスの構成例
Fig. 4　Example of composing by GSRA

### 4.2 通信シーケンス

**図 5** に EN が GSRA システムを用いて IN1 にリモートアクセスを行うまでの通信シーケンスを示す．ネットワーク構成・グループ構成は図 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

ここで 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 ルータのグローバル IP アドレス $G_{\mathrm{GR}}$ 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 の名前解決を行い，$G_{\mathrm{GR}}$ 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 $G_{\mathrm{GR}}$ を仮想 IP アドレス $V_{\mathrm{IN1}}$ 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 $V_{\mathrm{IN1}}$ と認識する．この時，IN のホスト名と GSRA ルータのグローバル IP アドレス，および仮想 IP アドレスの関係を NRT（Name Relation Table）に登録しておく．これにより IN 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 $V_{\mathrm{IN1}}$ となる．

**(2) 通信開始**

その後，EN から宛先が $V_{\mathrm{IN1}}$ となっているパケットが送信される場合，VAT テーブルを検索する．

初回は対応するエントリが存在しないため，処理中のパケットを待避してから，(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 と要求された 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．

EN が NAT 配下に位置する場合，(4) の処理を実行する．(4) の処理を実行するか否かの判定は，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 $P_{\mathrm{EN}}$ : $s$）を比較することで決定される．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**

(5) に示すマッピング処理では，EN が自身の $P_{\mathrm{EN}} : s$ と，グループ認証で割り当てられた $G_{\mathrm{GR}} : t$ を指定することで，GSRA ルータがマッピングテーブルを生成する．ここで，EN が NAT 配下に存在する場合，EN から GSRA ルータに送信されるパケットの送信元情報はホームルータの $G_{\mathrm{HR}} : m$ となる．よってメッセージに記載した送信元情報と実際に送信されるメッセージの送信元情報は異なるため，正しいマッピングが行

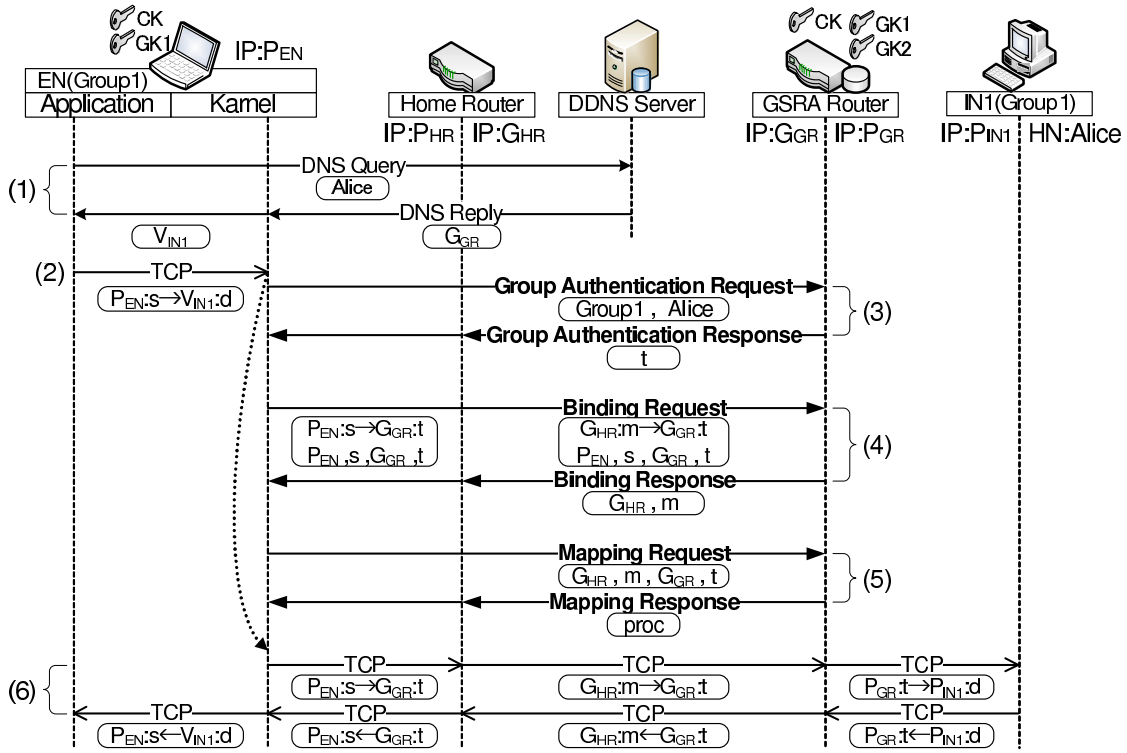


**図 5** GSRA 通信シーケンス
Fig. 5 GSRA sequence

**表 1** アドレス変換テーブルと VAT テーブル
Table 1 Address Transration Table and VAT Table

| | | |
|---|---|---|
| アドレス変換テーブル | : | $\{ G_{\mathrm{HR}} : m \leftrightarrow G_{\mathrm{GR}} : t \} \Leftrightarrow \{ P_{\mathrm{GR}} : t \leftrightarrow P_{\mathrm{IN1}} : d \}$ |
| VAT テーブル | : | $\{ P_{\mathrm{EN}} : s \leftrightarrow V_{\mathrm{IN1}} : d \} \Leftrightarrow \{ P_{\mathrm{EN}} : s \leftrightarrow G_{\mathrm{GR}} : t \}$ |

えない．そのため，EN にホームルータのマッピングアドレスを通知しておく必要がある．このための処理をバインディング処理と呼ぶ．

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，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．このバインディング処理によって GSRA ルータはホームルータの情報を取得し，NAT によるアドレス変換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アドレス変換テーブルと 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（proc）を取得し，VAT テーブルと PIT を確定する．ここで確定したアドレス変換テーブルと VAT テーブルのエントリを**表 1** に示す．以下にエントリの定義を示す．

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

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再開する．

**(6) アドレス変換通信**

以後，EN から IN1 宛ての通信は，EN の VAT テーブルに従って宛先 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

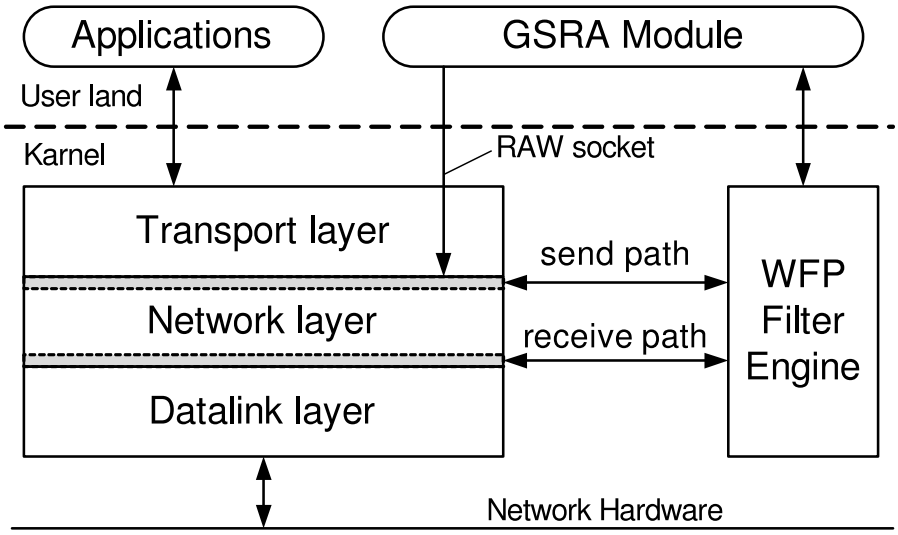


**図 6** Windows における GSRA システム設計
Fig. 6 GSRA system design in Windows

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，アドレス変換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．

## 5. 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．しかし，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 への実装は不可決である．

FreeBSD はカーネルそのもの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．現在の GSRA の実装は，この方法を用いてネットワークスタック上で GSRA モジュールを呼び出すように改造することで実現している．しかし，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．

### 5.1 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，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．

### 5.2 WFP を利用した実装

**図 6** 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．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．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．

## 6. 評　　価

提案方式の評価を行った結果を**表 2** に示す．まずユーザにかかる管理負荷を比較する．2 章で説明した通り，IPsec-VPN は管理負荷が非常に高いため“×”とした．SSL-VPN はユーザによる設定などは基本的に発生しないため“○”とした．それに対して GSRA は，ユーザが使用する PC に GSRA システムを導入す

る必要があるが，導入後はユーザ側に管理負荷を要求しないため“△”とした．次に，利用できるアプリケーションをを評価項目とした．IPsec-VPN と GSRA はネットワークレベルに実装される方式であるため，アプリケーションを限定せず使用することができるため，評価は“○”とした．SSL-VPN はアプリケーションが限定されるため“×”とした．

ネットワークレベルの解決策として，GSRA は既存方式の IPsec-VPN に比べ管理負荷を軽減しているため，既存方式よりも優れていると言える．また，IPsec-VPN では NAT との相性を考慮する必要があるが，GSRA は NAT 越え技術を根幹としているため，ユーザが NAT の存在を特別意識する必要が無い．SSL-VPN と GSRA を比較した場合，管理負荷の面では SSL-VPN が優れている．従って，SSL-VPN を使用することができるアプリケーションに用途を限定する場合，GSRA を選択するメリットは少ない．しかしながら，想定する用途次第で SSL-VPN と GSRA は棲み分けが可能であると言える．

**表 2** GSRA の評価
Table 2 Evaluation of GSRA.

| | 管理負荷 | アプリケーション |
|---|---|---|
| IPsec-VPN | × | ○ |
| SSL-VPN | ○ | × |
| GSRA | △ | ○ |

## 7. ま と め

本稿では，NAT 越え技術である NAT-f にセキュリティ機能を追加することでリモートアクセスを実現する方式として GSRA を提案した．既存方式と提案方式で比較評価を行い，有用性を示した．また，GSRA を Windows クライアントへ実装する方法について検討した．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) K.Hamzeh, G.Pall, W.Verthein, J.Taarud, W.Little and G.Zorn: Point-to-Point Tunneling Protocol (PPTP), *RFC 2637* (1999).
2) A.Valencia, M.Littlewood and T.Kolar: Cisco Layer Two Forwarding (Protocol) ”L2F”, *RFC 2341* (1998).
3) W.Townsley, A.Valencia, A.Rubens, G.Pall, G.Zorn and B.Palter: Layer Two Tunneling Protocol ”L2TP”, *RFC 2661* (1999).
4) S.Kent and K.Seo: Security Architecture for the Internet Protocol, *RFC 4301* (2005).
5) T.Dierks and E.Rescorla: The Transport Layer Security (TLS) Protocol, *RFC 5246* (2008).
6) P.Srisuresh and K.Egevang: Traditional IP Network Address Translator (Traditional NAT), *RFC 3022* (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) P.Hoffman: Algorithms for Internet Key Exchange version 1 (IKEv1), *RFC 4109* (2005).
9) A.Huttunen, B.Swander, V.Volpe, L.DiBurro and M.Stenberg: UDP Encapsulation of IPsec ESP Packets, *RFC 3948* (2005).
10) 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).
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 ライブラリー：http://msdn.microsoft.com/en-us/library/default.aspx.