NAT-f を応用したリモートアクセス方式 GSRA の提案と実装

鈴木　健太† 鈴木　秀和‡ 渡邊　晃†
名城大学理工学部† 名城大学大学院理工学研究科‡

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]により暗号化される．

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，アクセス先の端末を IN 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．

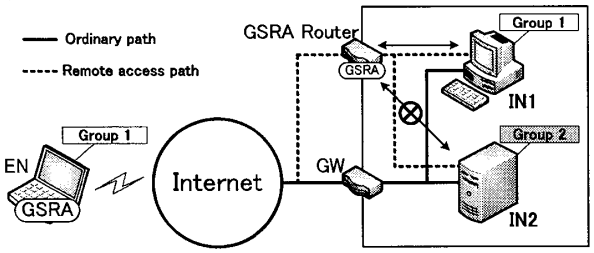

図 1　ネットワーク構成例

Proposal and Design of Remote Access Method "GSRA" applying NAT-f
†Kenta Suzuki and Akira Watanabe
Faculty of Science and Technology, Meijo University
‡Hidekazu Suzuki
Graduate School of Science and Technology, Meijo University

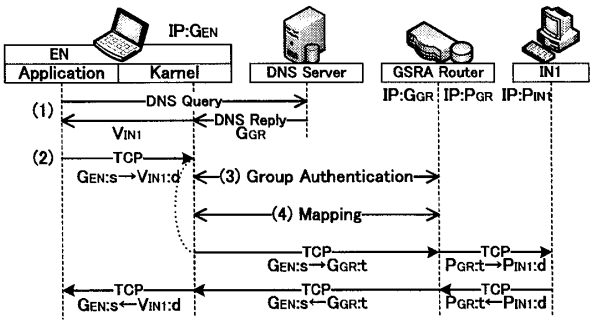

図 2　通信シーケンス

図 2 に GSRA の通信シーケンスを示す．DNS 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_{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_{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．

(2)通信開始

その後，EN から宛先が V_{IN1} 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．VAT テーブルは，EN が認識した仮想 IP アドレス/ポート番号と実際にパケットを送信する宛先 IP アドレス/ポート番号の対応関係が登録されるテーブルである．

宛先の仮想 IP アドレスに対応するエントリが存在する場合は，そのエントリに従い宛先 IP アドレス/ポート番号を変換する．更に暗号化通信に必要となる動作処理情報テーブル（PIT：Process Information Table）に従いパケットを暗号化する．

対応するエントリが存在しない場合，処理中のパケットを待避してから，VAT テーブルおよび PIT を生成するために，(3)の処理へと移る．

(3)グループ認証処理

EN は通信したい IN と自身のグループ情報を提示するために，グループ認証要求を GSRA ル

ータへ送信する．GSRA ルータがこれを受信すると，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，今後 EN と IN1 間の通信に使用するポート番号 t を予約し，EN へグループ認証応答を送信する．

EN は応答パケットからポート番号 t を取得して，VAT テーブルと PIT を仮生成する．続いて EN は(2)で待避したパケットのセッション情報と取得したポート番号 t を記載したマッピング要求を GSRA ルータへ送信する．

(4)マッピング処理

GSRA ルータはマッピング要求パケットから取得した情報を用いてアドレス変換テーブルと PIT を生成する．その後，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から動作処理情報を取得し，VAT テーブルと PIT を確定する．

以上で GSRA ネゴシエーションが完了し，待避していたパケットを復帰させて通信を再開する．以後の通信は，EN の VAT テーブル及び GSRA ルータのアドレス変換テーブルに従い IP アドレス/ポート番号が変換されることにより，リモートアクセスが実現される．

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，提案方式を検証するために FreeBSD での実装を完了させた．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．

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している．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．

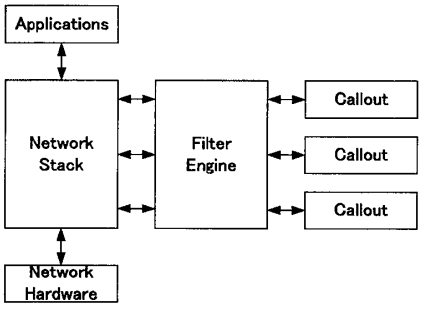

図 3　WFP の概観

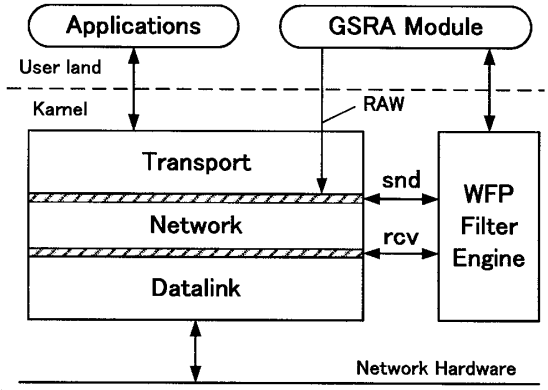

図 4　Windows における GSRA システム設計

3.1.WFP の概要

図 3 に WFP の概観を示す．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，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 4 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．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．

4. まとめ

NAT-f を利用し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，Vol48，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，Vol47，No.7，pp.2258-2266，July.2006