リモートアクセス方式 GSRA の性能評価

鈴 木 健 太[†1]　鈴 木 秀 和[†1]　渡 邊　晃[†1]

遠隔地のネットワークにアクセスできる既存のリモートアクセス技術は，端末側がインターネット上にあることを想定しているもの多い．しかし，実際には端末が家庭内にあることを想定するのが現実的である．現在広く利用されているリモートアクセス技術のうち，IPsec-VPN は NAT との相性問題があり，利用できない場合がある．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，これらの課題を解決するため，我々が提案しているリモートアクセス技術 GSRA をプライベート空間からでも利用できるように改良した方式を提案する．また，一般的に想定される利用シーンに沿った形での性能評価を行い，提案方式の有用性を確認した．

Performance Evaluation of Group-based Secure Remote Access

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

Existing remote access technology to access the network remotely, as often assumed that the terminal on the Internet. Of remote access technologies that are now widely available, IPsec-VPN, NAT and by the compatibility may not be available. SSL-VPN is readily available, but applications available are limited. In this paper, Remote access technology that we have proposed a scheme to improve GSRA be available from any private network to solve these issues. In addition, we evaluate the performance of common usage scenarios to show the usefulness of the proposed method.

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

1. はじめに

モバイル端末の小型・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内のネットワークに接続し，そのネットワーク内の資源を利用する技術である．

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 を構築する方式には，PPTP（Point-to-Point Tunneling Protocol）[1]，L2TP（Layer 2 Tunnneling Protocol）[2]，IPsec（Security Architecture for Internet Protocol）[3]，SSL（Secure Socket Layer）[4] などがある．

中でも IPsec のトンネリング機能により VPN を構築する方法を IPsec-VPN，暗号化に SSL を利用するものを総称して SSL-VPN と呼び，最近ではこれら 2 つの手法が主に利用されている．IPsec-VPN はきめ細かな設定が可能である分，設定が煩雑となり，相応の専門知識が要求される．SSL-VPN はユーザが手軽に利用できるものの，使用できるアプリケーションが制限される．そこで，我々はこれらの課題を解決した方式として，GSRA (Group-based Secure Remote Access)[5),6)] を提案している．

既存のリモートアクセス技術は，アクセスを行う端末がグローバルアドレスを持つことを前提としている場合が多い．しかし，現実的なリモートアクセスの利用シーンとしては，自宅から学生が大学の学内ネットワークへアクセスしたり，社員が社内ネットワークに接続し，在宅勤務を行う事などが考えられる．このようなケースでは，リモートアクセスを行う端末は NAT[7] の配下に存在し，プライベートアドレスしか保持しないのが一般的である．このような想定のもとで，既存技術を比較すると，IPsec-VPN は NAT との相性が悪く，利用できないケースがある．SSL-VPN は使用できるアプリケーションが限定される．端末にソフトウェアをインストールするタイプの SSL-VPN であれば，アプリケーションの制限はなくなるものの，プライベートアドレスの重複により通信が行えなくなる可能性がある．GSRA においても，グローバル空間からの利用を想定していたため，NAT によっては利用できない場合がある．

そこで本稿では，GSRA を改良して，NAT 配下からの利用を可能とした方式を提案する．提案方式では，ホームネットワーク側でいかなる NAT を使用していても，その配下からリモートアクセスを行うことが可能である．また，提案方式を実装し，IPsec-VPN，SSL-VPN と比較して，高スループットを実現できることを確認した．

以降，2 章で既存技術について述べる．3 章でこ要素技術となる GSRA について述べ，4 章で GSRA の改造に係る提案を行う．5 章では実装方法を，6 章で比較評価を行い，7 章でまとめる．

2. 既 存 技 術

既存のリモートアクセス技術の代表として，IPsec-VPN，SSL-VPN の概要を示す．なお，本論文では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．

2.1 IPsec-VPN

IPsec-VPN は IPsec の仕組みを利用することで VPN を構築する．アクセス先ネットワークに設置された IPsec-VPN 装置と EN 間で IKE（Internet Key Exchange）[8)9)] による認証と暗号鍵の共有を行い，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．また，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を端末毎に設定でき，柔軟なアクセス管理ができる．しかしその分，専門的知識が要求され，管理負荷が大きいという課題がある．また，ホームネットワークから IPsec-VPN によるリモートアクセスを行う場合，NAT が IPsec パススルーに対応している必要がある．IPsec パススルーは，メーカごとに使用できる条件が設けられている場合があり，その条件を満たさなければ使用することができない．

2.2 SSL-VPN

SSL-VPN は通信の暗号化に SSL の仕組みを利用したリモートアクセス手法の総称である．SSL-VPN はクライアントに一般の Web ブラウザを使用してアクセスを行う場合と，専用ソフトウェアを使用する場合に大別できる．

(1) Web ブラウザを使用する場合

一般的に SSL-VPN と呼ぶのはこの方法である．SSL-VPN を利用する場合，DMZ（De-Militarized 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，ユーザ側で特別な設定をせずとも，サーバを認証しアクセスすることができる．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．ただし，企業等の高セキュリティなネットワークへアクセスを行う場合で，サーバがアクセス側端末を認証したい場合にはアクセス側端末に証明書が必要となる．また，ブラウザベースであるため，Web ブラウザを経由した Web 閲覧やメール送信などに用途が限定されるという課題がある．

(2) 専用ソフトウェアを使用する場合

クライアントに専用ソフトウェアを使用する方法として，OpenVPN[10)] がある．OpenVPN は，Ethernet フレームをカプセル化して通信を行うため，任意のアプリケーションを使用できる利点がある．しかし，カプセル化によるヘッダオーバヘッドやフラグメントの発生により，スループットが低下する．また，サーバからクライアントに対して IP アドレスや DNS サーバなどの設定情報を配布する必要があり，配布された設定情報と，クライアント側の LAN 内の端末の設定情報が重複した場合は通信が行えなくなる．

3. GSRA

提案方式の要素技術となる GSRA について説明する．

3.1 概　　要

GSRA は，我々が提案する NAT 越え技術 NAT-f（NAT-free Protocol）[11)] にセキュリティの機能を追加することにより安全なリモートアクセスを実現した技術である．通信グループを定義することによりアクセス制御を行うことができる．また，暗号化プロトコル PCCOM（Practical Cipher Communication Protocol）[12)] を用いて NAT をまたがるエンドエンドの通信を暗号化することが可能である．

GSRA によるリモートアクセスの構成例を**図 1** に示す．前提として EN はグローバルアドレスが割り当てられているものとする．GSRA の機能を実装したルータを GSRA ルータ

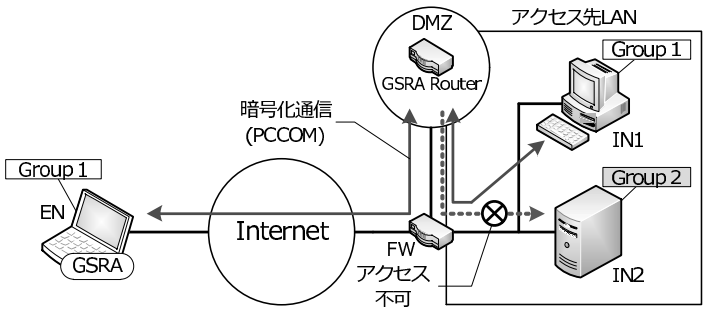

図 1 GSRA によるリモートアクセスの構成例
Fig. 1 An example of a remote access configuration with GSRA.

と呼び，アクセス先のネットワークの DMZ 上に設置する．GSRA では，内部端末へのアクセスをグループ単位で制御する．図 1 の例では，EN は Group1 に所属しており，IN1 は Group1 との通信を，IN2 は Group2 との通信を許可している．この場合，EN は IN1 へアクセス可能であるが，IN2 へのアクセスは拒否される．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 GSRA ルータがアクセス制御とサービス制御を行う．

3.2 通信シーケンス

図 2 に EN が IN へリモートアクセスを行うために行う GSRA ネゴシエーションのシーケンスを示す．本稿で使用する記号の定義は以下の通りとする．

- 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 ルータは各通信グループに対応したグループ鍵 GK を予め所持しているものとする．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．また，GSRA ルータには ACT（Access Contorol Table）と呼ぶテーブルに，IN のホスト名，プライベート IP アドレス，サービス情報（ポート番号，プロトコル），グループ番号，外部からのアクセス許可情報（allow または deny）を登録しておく．ACT の設定により，サービス毎にリモートアクセスを許可するグループを制御する．グループ番号として，複数のグループを指定することも可能であり，簡単かつ柔軟にアクセス制御を行うことができる．ACT の例を**表 1** に示す．表 1 の例では，グループ 1 にのみ属する端末は，Alice が公開している TCP の d 番ポートに該当するサービスは利用可能であるが，UDP の e 番ポートに該当するサービスは利用できない．また，Alice は PCCOM をサポートしているため，エンドエンドで暗号化通信が可能である．

以下に EN が IN と通信を開始するまでの手順を説明する．なお，括弧付きの数字は図 2 中の数字と対応している．

(1) 名前解決

EN は DNS サーバに IN（ホスト名 : Alice）の名前解決を依頼し，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_{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．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_{IN} の関係を NRT（Name Relation Table）に登録しておく．これにより EN は GSRA ルータ配下の端末を仮想 IP アドレスで区別することができる．

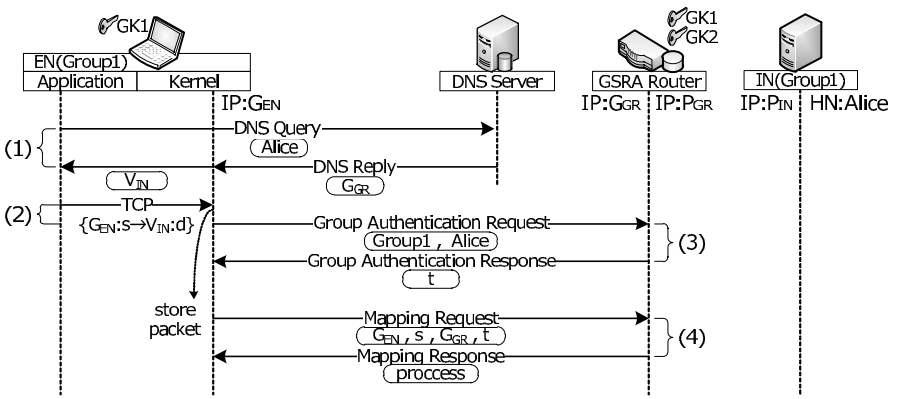

図 2 GSRA ネゴシエーション
Fig. 2 GSRA negotiation.

表 1 ACT の例
Table 1 Example of Access Contorol Table.

Host Name	IP Address	PCCOM Support	Service	Group	Permit
Alice	P_{IN}	Yes	d (tcp)	Group1	allow
			e (udp)	Group2	allow

(2) 通信開始

EN のアプリケーションから宛先が V_{IN} のパケットを送信されると，EN はカーネルにて VAT（Virtual Address Translation）テーブルを検索する．VAT テーブルは，(1) の処理で EN に通知した仮想アドレス宛のパケットを，実アドレス宛てへと書き換えるために使用するテーブルである．初回は対応する VAT テーブルのエントリが存在しないため，送信されたパケットをカーネル内に待避してから，以降に示す GSRA ネゴシエーションを行う．

(3) グループ認証処理

グループ認証処理は，EN からのアクセスを許可するかどうかの認証を行う処理である．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，ACT をチェックし，EN から IN へのアクセス可否の認証を行う．アクセスが許可されていた場合，EN と IN 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．エフェメラルポート番号とは，リモートアクセスのために一時的に使用するポート番号であり，GSRA ルータの未使用ポートの中から選ばれる．EN はグループ認証応答メッセージから t を取得して，VAT テーブルを更新する．

(4) マッピング処理

GSRA では，EN のカーネル及び GSRA ルータにアドレス変換テーブルを生成し，テーブルのエントリに従ってパケットのアドレス変換を行うことでリモートアクセスを実現している．マッピング処理は，そのためのテーブルを生成する処理である．EN は（2）で待避したパケットのセッション情報と，宛先情報 $G_{GR} : t$ を記載したマッピング要求パケットを GSRA ルータへ送信する．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 GSRA マッピングテーブルと PIT（Process Information Table）を生成し，EN における動作処理情報を記載したマッピング応答パケットを EN へ送信する．PIT には，通信の送信元/宛先の組み合わせ毎に，パケットを暗号化するか復号するかといった情報（動作処理情報）が記載される．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，EN 側の PIT を生成する．

以後は（2）で待避したパケットを復帰させて通信を開始する．

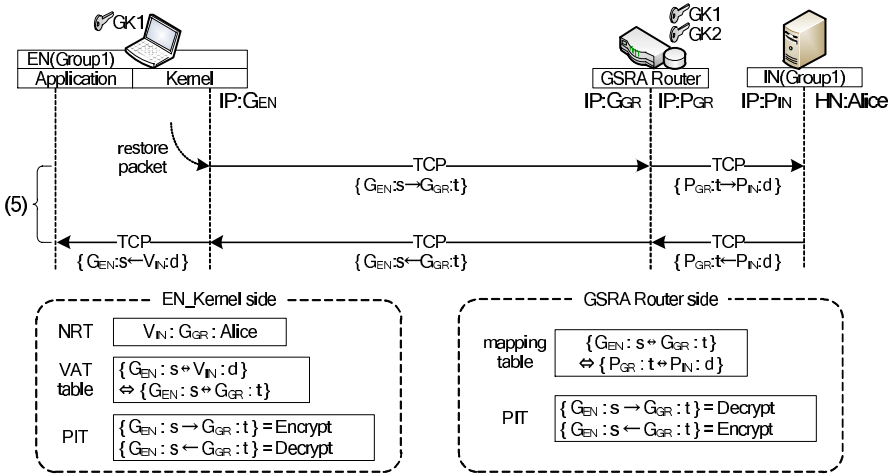

図 3 アドレス変換処理
Fig. 3 Address translation process.

(5) アドレス変換処理

以後の通信の様子と，生成されたテーブルの内容を**図 3** に示す．テーブル内の矢印は以下の意味を示している．

- $G_i : s \leftrightarrow G_j : d$ … $G_i : s$ と $G_j : d$ の通信
- $G_i : s \Leftrightarrow G_j : d$ … $G_i : s$ と $G_j : d$ の変換

EN から IN 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/ポート番号を変換する．さらに PIT に従ってパケットを PCCOM で暗号化してから GSRA ルータへ送信する．GSRA ルータでは，受け取ったパケットを復号後，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，IN へと転送する．ここで送信元アドレス/ポート番号も GSRA ルータのものに書き換えることによって，応答パケットを必ず GSRA ルータへ戻すことができる．IN 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を行い，EN まで届ける．以上の手順により，EN から IN へのリモートアクセスが実現される．

4. 提 案 方 式

既存の GSRA は，EN がグローバル空間にいることを前提としている．そこで，EN がホームネットワークの NAT 配下に位置する場合に対応するため，以下のようにシーケンスを見直した．

4.1 解決すべき要件

ホームネットワーク側の NAT を HR（Home Router）と呼ぶ．HR が存在する場合，EN から送信されるパケットの送信元は HR によってマッピングされた IP アドレス/ポート番号へ変換される．GSRA ルータでは，HR によってマッピングされた情報に対応したマッピングテーブルを生成する必要がある．そこで，HR のマッピングアドレスを GSRA ルータに通知する手段が必要である．

次に，近年の NAT ルータは，SPI（Stateful Packet Inspection）機能が搭載されている場合が多い．SPI とは，ルータを通過するパケットの状態をログに記録しておき，記録されたログの内容と到着したパケットの内容を照合することで正当性を確認する動的なパケットフィルタリング機能である．照合する内容は，TCP の接続状態やシーケンス番号などであり，これらが矛盾している場合，パケットが破棄されてしまう．SPI 機能を搭載した HR で

あっても通信を開始できるようにしなければならない．

一般に NAT に穴を開けるためには GSRA ルータに対して TCP/UDP パケットを送信し，その応答に記載された情報により穴の情報を得る．これを行うために 1 往復のシーケンスの追加が必要である．しかし，HR で SPI 機能が働いている場合，単に追加しただけでは，そのパケットが NAT の SPI に記憶されるため，マッピング処理完了後にあらためてアプリケーションから送信される TCP/UDP パケットはシーケンスの整合性が保たれず，HR で破棄されてしまう．

4.2 解 決 策

上記の問題を解決するため，TCP の再送制御を特性を利用する．再送される TCP パケットには以下のような特徴がある．

- シーケンス番号は再送前と同値
- NAT でマッピングされるポート番号は再送前と同値

この特徴を利用するため，新たに追加するバインディング処理時においてトリガパケットをコピーした TCP/SYN パケットを送信し，GSRA ルータでは，この応答を返さないようにしておく．こうすることで，ネゴシエーション完了後に送信されるトリガパケットは，バインディング処理時に送信したパケットの再送であると HR をに認識させることができる．再送であれば，SPI により破棄されることは無いため，通信を開始できる．

ただし，HR が存在するかどうかは定かでなく，HR が無い場合にはバインディング処理は余分な処理となってしまう．そのため，バインディング処理はグループ認証後，マッピング処理の前に独立して行うこととする．HR が存在するか否かは，グループ認証要求パケットのメッセージに記載された送信元情報と，ヘッダの送信元を比較し，一致するかどうかで判定する．両者が等しい場合は，HR が存在しないことが分かるため，バインディング処理をスキップする．

また，後のマッピング処理時に送信元情報として使用するため，HR によるマッピングアドレスを EN にも通知しておく必要がある．そのためには，ICMP の 1 往復パケットを使用し，取得したマッピングアドレスを応答パケットに記載して EN に通知する．

4.3 新たな GSRA シーケンス

バインディング処理を追加した新たな GSRA シーケンスを**図 4** に示す．バインディング以外の処理は従来のままである．

バインディング処理では，まず EN が ICMP をベースとしたバインディング要求パケットを GSRA ルータへ送信する．EN はこのパケットの応答を待たず，続けて TCP ベースのバインディング要求パケットを GSRA ルータへ送信する．この TCP のバインディング要求パケットは，GSRA ネゴシエーションのトリガとなった TCP パケットをコピーし，宛先を $G_{GR} : t$ に書き換えたものである．ポート番号 t は前段階のグループ認証処理で得た，リモートアクセス用のエフェメラル・ポート番号である．

GSRA ルータは ICMP のバインディング要求パケットを受信すると，受信したパケットを待避する．続いて TCP のバインディング要求パケットを受信すると，そのヘッダ情報から，HR にてマッピングされたアドレスである $G_{HR} : m$ を取得する．その後，待避していた ICMP のバインディング要求パケットに対するバインディング応答パケットを生成し，取得したマッピングアドレスを記載して EN へ送信する

以上の処理により，GSRA ルータと EN は HR によるマッピングアドレスを取得し，HR によるアドレス変換に対応したマッピングテーブルを生成することが可能となる．この処理は HR がどのようなルータであっても成立する．

5. 実　　装

新たな GSRA ネゴシエーションを FreeBSD に実装した．EN および GSRA ルータに，GSRA のための処理を行う GSRA モジュールを IP 層に実装した．カーネルは GSRA モジュールの呼び出し部のみを変更しており，その他の IP 層の処理は一切変更しない．GSRA

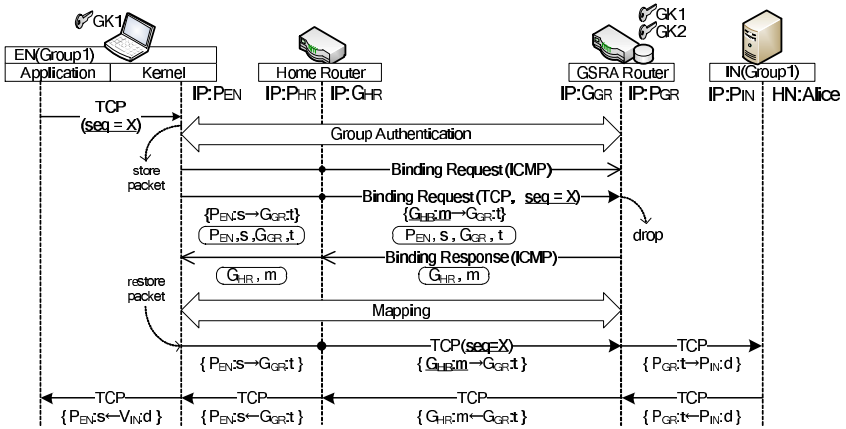

図 4　新たな GSRA シーケンス
Fig. 4　New GSRA sequence.

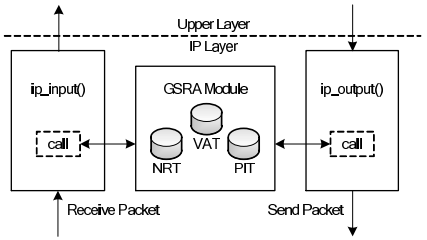

図 5 EN の実装
Fig. 5 Implementation of External Node.

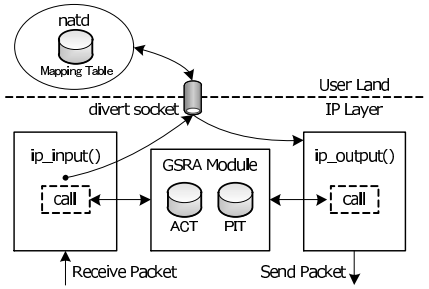

図 6 GSRA ルータの実装
Fig. 6 Implementation of GSRA router.

モジュール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．

5.1 EN への実装

EN における実装を**図 5** に示す．パケットを送受信する際，IP 層にて入出力関数 `ip_input()`，`ip_output()` から GSRA モジュールを呼び出す．GSRA ネゴシエーションに使用する制御パケットは，GSRA モジュール内で生成する．ネゴシエーション完了後は，GSRA モジュールが NRT，VAT，PIT の情報を保持することとなり，GSRA モジュールへ渡されたパケットは，これらのテーブルのエントリに従って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．

5.2 GSRA ルータへの実装

GSRA ルータにおける実装方法を**図 6** に示す．GSRA ルータでは，GSRA モジュールに加えて，NAT の機能を有する `natd` を動作させる．`natd` は，FreeBSD で利用できる，ユーザランドで動作するアプリケーションである．GSRA ルータが受信したパケットは，divert ソケットを通じて，natd へと渡され，そこでアドレス変換を行う．また，GSRA モジュールには ACT と PIT の情報が保持され，アクセス制御及び暗号化などの処理を行う．

6. 性 能 評 価

既存の VPN 方式と新 GSRA を，定性的・定量的観点から比較評価する．

表 2 リモートアクセス方式の比較
Table 2 Compare of remote access method.

	IPsec-VPN	SSL-VPN		L2TP	新 GSRA
		Web base	OpenVPN		
暗号化	IPsec-ESP	SSL	SSL	IPsec-ESP	PCCOM
P2P 暗号化	×	×	×	×	○
カプセル化オーバヘッド	×	○	×	×	○
HR 対応	△	○	○	△	○
クライアントソフト	△	○	×	△	×
アプリケーション制限	○	×	○	○	○
アドレス管理	×	○	×	×	○
スプリットトンネル	○	○	○	×	○

6.1 既存方式との比較

表 2 にリモートアクセス方式の比較を示す．

- 暗号化プロコトル：各方式とも，インターネット上を流れるパケットは暗号化される．
- P2P 暗号化：比較した方式の中で，GSRA は唯一エンドエンドでの暗号化が可能である．
- カプセル化オーバヘッド：パケットのカプセル化を行う方式では，ヘッダオーバヘッドが増加し，通信の性能が劣化するため×としたが，GSRA ではパケットに変更を加えないため，カプセル化による性能の劣化は起こらない．
- HR 通過：どの方式も HR を通過すること自体は可能であるが，IPsec-VPN，L2TP は NAT がそれぞれの VPN パススルーに対応している必要があるため△とした．その他の方式はどのような HR を使用していても良い．
- クライアントソフト：Web ベースの SSL-VPN は Web ブラウザさえあれば良い．IPsec-VPN，L2TP は，標準でサポートしている OS もあるが，そうでない場合もある．OpenVPN と GSRA はクライアントソフトをインストールする必要がある．
- アプリケーション制限：Web ベースの SSL-VPN は，アプリケーションが制限される．その他の方式ではアプリケーションの制限は無い．
- アドレス管理：IPsec-VPN，OpenVPN，L2TP はトンネリングを行うため，リモートアクセスに使用するアドレスと実環境のアドレスが重複しないよう管理する必要がある．それぞれ VPN サーバ側からアドレスを配布する仕組みが用意されているが，配布されたアドレスが実環境と重複しない保証があるわけではない．
- スプリットトンネル：L2TP はスプリットトンネルに対応しておらず，リモートアクセスによる通信を行っている間はインターネット接続等，本来の経路から通信を行えな

い. その他の方式では本来のネットワークを通じた通信と両立可能である.

以上の比較により，GSRA は既存方式に比べ，有用である事が確認できる.

6.2 性能測定結果

FreeBSD に実装済みの提案方式を利用し，通信開始までのネゴシエーションにかかる時間，及びスループットを測定した．測定環境は**図 7** に示す通りである．アクセス元 LAN とアクセス先 LAN の間はインターネットを想定し，擬似的に背景負荷をかけることができる Dummynet[13] を動作させた．Dummynet の設定パラメータは，帯域制限 40Mbps，往復の遅延各 10ms の計 20ms，パケットロス率は 0% とした．このパラメータは，近年の一般的な家庭において，PC を有線で接続した場合のインターネットの通信速度を想定したものである．各装置の仕様は**表 3** に示す通りである．公平な測定を行うため，各方式とも，暗号化アルゴリズムは AES-128bit を使用し，暗号化範囲は EN-VPN サーバ間としている．OpenVPN は，パケットのカプセル化に TCP と UDP のどちらかが選択できるが，TCP でカプセル化した場合，TCP over TCP の問題でスループットが大幅に低下する場合がある．そのため，UDP を選択した．ネゴシエーション時間の測定には，パケットキャプチャソフト Wireshark[*1] を用いた．スループットの測定は，EN で `wget`[*2] コマンドを使用し，IN に保存されている 50MB のファイルをダウンロードする．`wget` は UNIX のコマンドライン上で HTTP や FTP 経由のファイル取得を行えるツールであり，同時にスループットの計測も行うことができる．測定はそれぞれ 10 回ずつ行い，その平均値を測定結果とした．比較対象は，現在広く利用されている IPsec-VPN と，想定する用途の近い OpenVPN の 2 手法とした.

(1) ネゴシエーション時間

ネゴシエーション時の特徴として，IPsec-VPN と GSRA が特定のパケットの送信をトリガとしてネゴシエーションを開始するのに対し，OpenVPN では，予め認証のみを独立して行う．そのため，IPsec-VPN，GSRA に関しては，EN で wireshark によるパケットキャプチャを開始した状態で，`wget` コマンドを用いて IN から 0Byte のダミーファイルをダウンロードすることでネゴシエーションを開始させた．一方，OpenVPN は予め行うネゴシエーションの様子をキャプチャした.

ネゴシエーション時間の測定結果を**表 4** に示す．GSRA では DNS による名前解決が必須処理となるため，名前解決にかかる時間もネゴシエーション時間に含める．他方式では IP アドレスで直接指定できるため，名前解決時間はゼロとした．ネゴシエーションの最後のパケットを EN が受信した時間を，ネゴシエーション完了時間としたが，現実的には実際に行われる通信の最初のパケットが送信される時間が重要だと考えられるため，それまでの時間も測定対象に含めた.

IPsec-VPN の結果について見ると，通信開始 IPsec-VPN ではネゴシエーション自体は 200ms 程度で完了しているにも関わらず，実際の通信開始までに約 3 秒かかっている．IPsec-VPN はネゴシエーションの最中にトリガとなったパケットが失われてしまうためである．失われたパケットは，アプリケーションにより再送されるため，通信開始までの時間は使用するプロトコル次第で変動すると考えられる.

OpenVPN は，ネゴシエーションに 3 秒近くの時間がかかっている．これは，リモートアクセスに使用するトンネルの生成や，サーバ・クライアントの SSL による認証など，多くの処理が発生するためである．これに加え，ネゴシエーション完了後に，実際の通信を行う手間が必要になるため，通信を開始するまでの時間はさらに長くなる.

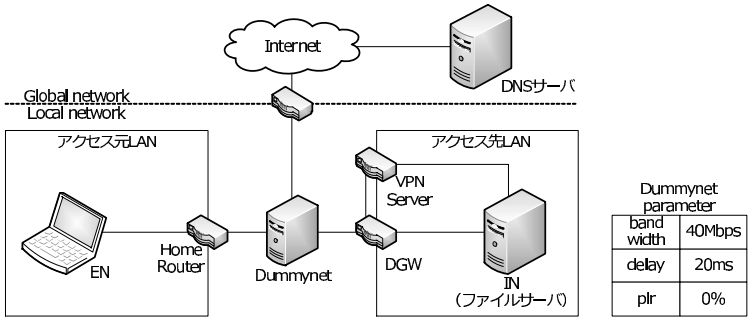

図 7 測定環境
Fig. 7 Measurement environment.

表 3 諸元
Table 3 Device specification.

	OS	CPU	Memory	NIC
EN	FreeBSD 7.2	Pentium4 3.4GHz	1GB	100Base-TX
VPN Server	FreeBSD 7.2	Pentium4 2.8GHz	2GB	100Base-TX
Dummynet	FreeBSD 8.0	Pentium4 3.4GHz	512MB	100Base-TX

⋆1 http://www.wireshark.org/
⋆2 http://www.gnu.org/software/wget/

表 4 ネゴシエーション時間の測定結果
Table 4 Result of a measurement of negotiation time.

	DNS 名前解決 [ms]	ネゴシエーション完了まで [ms]	通信開始まで [ms]
IPsec-VPN	0	211.9946	2924.2503
OpenVPN	0	2720.0936	2720.0936+ α
GSRA	44.0591	104.9613	104.9754

表 5 スループットの測定結果
Table 5 Result of a measurement of throughput.

	背景負荷無し [Mbps]	背景負荷有り [Mbps]
IPsec-VPN	82.9	10.7
OpenVPN	73.0	13.8
GSRA	89.6	23.0

GSRA は，通信開始まで約 100ms で完了している．DNS の名前解決は A レコード，AAAA レコードの 2 往復で行われ，GSRA ネゴシエーションでは 3 往復のパケットがやりとりされる．通信経路上には Dummynet により 1 往復あたり 20ms の遅延が発生しており，5 往復の RTT だけで最低 100ms 必要となる．このことから，EN と GSRA ルータにおける処理時間は非常に短いことが分かる．

体感的に，既存方式のネゴシエーションにかかる 2〜3 秒という時間は長く感じられ，正常に処理が進んでいるかどうか不安に感じるが，GSRA ではそのようなことは無い．ネゴシエーション時間という観点において，GSRA は既存方式によりも優秀だといえる．

(2) スループット

スループットの測定結果を**表 5** に示す．背景負荷をかけた場合，かけない場合共に，GSRA が最も高いスループットを記録している．IPsec-VPN，OpenVPN は，パケットをカプセル化して転送するため，追加のヘッダオーバヘッドやフラグメントが発生し，スループットが低下する．一方，GSRA で使用している暗号化プロトコル PCCOM は，パケットフォーマットを変えないまま暗号化を行うため，高スループットが得られる．

このように，実機での性能において GSRA は既存方式を上回っており，有用な方式であると言える．

7. ま と め

本稿では，リモートアクセス技術の評価を行い，GSRA の有用性を示した．GSRA は，エンドエンドでの暗号化通信や，アドレス管理が不要である点など，これまでのリモートアクセスには無かった特徴を兼ね備えている．既存の GSRA に特殊なバインディング処理を追加することで，あらゆる HR にも対応できるものとした．実機での測定においては，インターネットを想定した環境でも既存方式を上回る性能を発揮できることを確認した．今後は，Windows をはじめとした他の OS のへの実装と性能測定を行い，普及を目指していく．

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) Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B.: Layer Two Tunneling Protocol “L2TP”, RFC 2661, IETF (1999).
3) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
4) Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol, RFC 5246, IETF (2008).
5) 鈴木秀和，渡邊 晃：通信グループに基づくサービスの制御が可能な NAT 越えシステムの提案，情報処理学会論文誌，Vol.51, No.9, pp.1881–1891 (2010).
6) 鈴木健太，鈴木秀和，渡邊 晃：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，マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム論文集，Vol.2010, No.1, pp.288–294 (2010).
7) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
8) Hoffman, P.: Algorithms for Internet Key Exchange version 1 (IKEv1), RFC 4109, IETF (2005).
9) C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).
10) OpenVPN Technologies, Inc.: OpenVPN - Open Source VPN. http://openvpn.net
11) 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).
12) 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).
13) L.Rizzo: Dummynet home page. http://info.iet.unipi.it/luigi/dummynet/