Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

自宅からのリモートアクセスを可能にするGSRAv2の提案と評価

鈴木健太[†1]　旭　健作[†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方式は，端末がグローバルアドレスを持つことを想定しているものが多い．しかし，実際には端末が家庭内のプライベートアドレス空間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方式に，IPsec-VPN，SSL-VPN，OpenVPN，PacketiX VPN があるが，どれも一長一短を抱えている．これらの方式の課題を解決した方式として我々は GSRA（Group-based Secure Remote Access）を提案してきたが，NAT 配下からの使用は想定されていない．そこで本稿では，GSRA を NAT 配下のプライベートアドレス空間からでも利用できるように改良した GSRAv2 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．

Proposal and Evaluation of GSRAv2 that Enables Remote Access from Home

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

Existing methods of remote access , there are many things that are supposed to have a global address by the terminal. However, it is actually realistic to assume that the private address network within the home terminal. The remote access methods that are currently widely used, IPsec-VPN, SSL-VPN, OpenVPN, there is a PacketiX VPN, are having none of the advantages and disadvantages. GSRA (Group-based Secure Remote Access) as a method of problem was resolved by these methods together but have used from behind the NAT is not expected. In this paper, we propose the GSRAv2 also be available from private address network behind a NAT. In addition, an evaluation of performance in line with expected usage scenarios generally confirmed the usefulness of the proposed method.

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，遠隔地から組織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-VPN（Security Architecture for Internet Protocol）[3]，SSL-VPN（Secure Socket Layer）[4]，OpenVPN[5]，PacketiX VPN 3.0[6]（以下 PacketiX VPN）などがある．PPTP は, 認証に MS-CHAPv2（Microsoft version of the Challenge-handshake authentication protocol version 2）[7] を使用する．MS-CHAPv2 が採用しているハッシュ関数 MD4[8] は脆弱性が報告されており，暗号化アルゴリズムとして採用している DES[9] は解析可能であることが知られている．L2TP はトンネリングプロトコルであり，単体ではセキュリティ機能を備えていない．そこで最近は，IPsec-VPN，SSL-VPN，OpenVPN，PacketiX VPN の 4 手法に注目が集まっている．

しかし，これらの手法にも，以下に示すような課題がある．IPsec-VPN は，きめ細かな設定が可能であるが，設定が煩雑となり，高い専門知識が要求される．SSL-VPN は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．また，確実なクライアント認証を行う場合は，端末に証明書を持たせる手間が生まれ，利点である手軽さが失われる．OpenVPN は，高セキュリティと手軽さを兼ね備えた方式として注目されているが，パケットのカプセル化による追加の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という課題がある．PacketiX VPN は，多様な機能を備えており，フレキシブルに利用できるという特長があるが，通信を SSL に見せかけるという性質上，ネットワーク管理者が社員の VPN 接続を認知できず，その結果ウィルスの侵入や情報の漏洩など，組織単位で危険をもたらす場合がある．また，イーサネットフレームを TCP でカプセル化するため，TCP over TCP[10] の問題が発生し，パケットロスが発生する環境では通信性能が著しく低

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

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

下する可能性がある．

そこで，我々はこれらの課題を解決する方式として，GSRA（Group-based Secure Remote Access）[11),12)] を提案してきた．GSRA は，NAT 越え技術 NAT-f[13)] の仕組みを利用し，そこにアクセス制御や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した方式である．GSRA では，通信グループの概念を取り入れることにより，簡単かつ柔軟にアクセス制御を行うことができ，アプリケーションが制限されないという利点がある．また，パケットをカプセル化せず，アドレス変換により転送するため，余計なオーバヘッドや，TCP over TCP の問題が発生しない．アドレス変換はカーネル内で行うため，高スループットが得られる．

一方，既存のリモートアクセス技術には，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ものが多い．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，学生が自宅から大学の学内ネットワークへアクセスしたり，社員が勤務先の社内ネットワークに接続し，在宅勤務を行うことなどが考えられる．このようなケースでは，リモートアクセスに使用する端末はホームネットワーク側の NAT 配下に存在し，プライベートアドレスを保持しているのが一般的である．この点に着眼し，既存技術を比較し直すと，IPsec-VPN は NAT との相性が悪く，利用できないケースが出てくる．SSL-VPN は，NAT が存在しても利用できる．IPsec-VPN と OpenVPN，PacketiX VPN は，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出てくる．GSRA は，グローバル空間からの利用を想定していたため，端末が NAT 配下にある場合は利用できない．

そこで本稿では，GSRA に，ホームネットワーク側の NAT のマッピング情報を GSRA ルータに通知する処理を追加し，NAT 配下からの利用を可能とした GSRAv2 を提案する．提案方式では，GSRA の利点がそのまま活かせるとともに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．GSRAv2 の実装を行い IPsec-VPN，OpenVPN，PacketiX 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 章で提案方式の要素技術となる GSRA について述べ，4 章で GSRAv2 の提案を行う．5 章では提案方式の実装方法を述べ，6 章で既存技術との比較評価を行い，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，OpenVPN，PacketiX VPN の概要を示す．なお，本稿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により 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）[14)] 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ことでリモートアクセスを実現する．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改ざんや盗聴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 によるアドレス変換を，アドレス偽装と認識されてしまい，IPsec-VPN 装置でパケットが破棄されてしまう．そのような場合，IPsec パススルーに対応した NAT を使用するなどの対策が必要となる．

2.2 SSL-VPN

SSL-VPN は，SSL を用いて VPN を構築する方式である．アクセス先ネットワークの DMZ（DeMilitarized Zone）などに SSL-VPN 機能を持った装置を設置し，それがプロキシサーバの役割を果たすことによりリモートアクセスを実現する．SSL は一般的な Web ブラウザに標準で搭載されているため，ユーザ側で特別な設定やソフトのインストールをせずとも，サーバを認証しアクセスすることができる．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は，アクセス側端末にも証明書を持たせる必要があり，手軽さという利点が損なわれる．また，ブラウザベースであるため，Web ブラウザを利用した 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．

2.3 OpenVPN

OpenVPN は，仮想ネットワークデバイス TUN/TAP[15)] 間でパケットをトンネリングすることによりリモートアクセスを実現する．OpenVPN は，暗号化に OpenSSL を用いるが，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，通信が行えなくなるという課題がある．

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

2.4 PacketiX VPN

PacketiX VPN は，コンピュータ上に独自の仮想 NIC を作成し，その仮想 NIC 間でパケットをトンネリングすることによりリモートアクセスを実現する．PacketiX VPN による VPN の構築は，パケットを SSL に偽装して行われるため，NAT やファイアウォールを透過して行うことができる．しかし，この性質上，一般社員がネットワーク管理者に無断で PacketiX VPN を利用して自宅との間で VPN を構築することが可能となる．ネットワーク管理者からは，VPN が利用されていることを認知できず，社内情報の流出や，ウィルスの侵入を許してしまう可能性がある．

3. GSRA

提案方式の要素技術となる GSRA について説明する．なお，本稿で使用する記号の定義は以下の通りである．

- 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
- $G_i : s$：トランスポートアドレス（IP アドレス G_i とポート番号 s の組）
- Group i：通信グループ番号
- GK i：Group i に対応するグループ鍵
- $G_i : s \leftrightarrow G_j : d$ ･･･ $G_i : s$ と $G_j : d$ の通信
- $G_i : s \Leftrightarrow G_j : d$ ･･･ $G_i : s$ と $G_j : d$ の変換

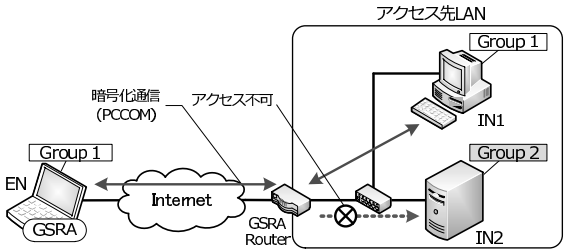

図 1 GSRA によるリモートアクセスの構成例
Fig. 1 An example of a remote access configuration with GSRA.

3.1 GSRA の構成

GSRA は，NAT 越え技術 NAT-f（NAT-free Protocol）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，簡単かつ柔軟なアクセス制御を行うことができる．また，独自の暗号化プロトコル PCCOM（Practical Cipher Communication Protocol）[16] を採用し，NAT をまたがるエンドエンドの通信を暗号化することができる．

GSRA によるリモートアクセスの構成例を**図 1** に示す．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 ルータと呼ぶ．GSRA では，管理を容易にするため，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 端末との通信を，IN2 は Group2 端末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の GSRA ネゴシエーションのシーケンスを示す．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．グループ鍵は，グループ毎に固有の暗号鍵であり，EN が当該グループに所属していることを証明するものである．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）が登録されている．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とサービスが決まる．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，Group1 にのみ属する端末は，Alice が公開している TCP

表 1 ACT の例
Table 1 An 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

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

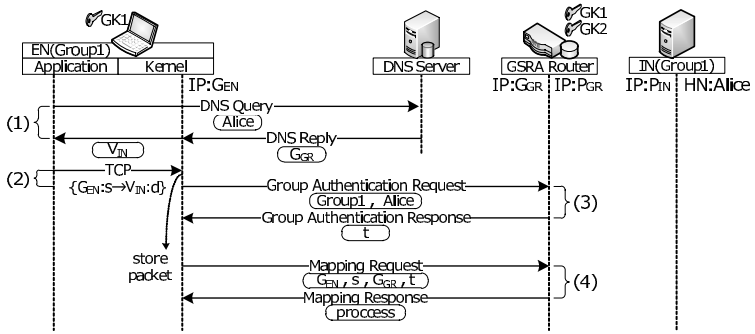

図 2 GSRA ネゴシエーションの流れ
Fig. 2 Negotiation of GSRA.

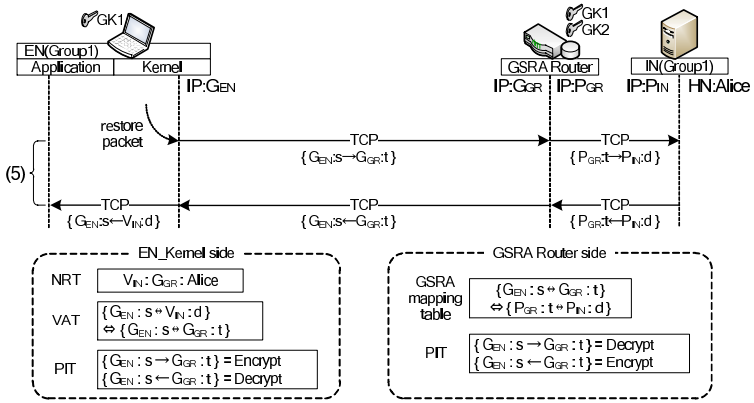

図 3 アドレス変換処理による IN へのアクセス
Fig. 3 Remote access by Address translation process.

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，GSRA ルータのグローバル IP アドレス G_{GR} を取得する．ここで EN はカーネル領域において，DNS Reply 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．IN はプライベート IP アドレスしか保持していないため，本来 EN 側から通信を開始することはできない．しかし，仮想 IP アドレスとして通知することにより，EN 側から IN を指定して通信を開始することが可能になる．この時，Alice と G_{GR}，および 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 ルータ配下の複数の端末を仮想 IP アドレスで区別することができる．

(2) 通信開始

EN のアプリケーションから宛先が V_{IN} のパケットが送信されると，EN はカーネルにて VAT（Virtual Address Translation table）を検索する．VAT 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 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，(3)，(4) の処理を行う．

(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 Group Authentication Request 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，GSRA ルータは EN と IN 間の当該セッションに使用するエフェメラルポート番号 t を予約し，t を記載した Group Authentication Response を EN へ送信する．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 Group Authentication Response メッセージから t を取得して，VAT 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．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 Mapping Request を GSRA ルータへ送信する．GSRA ルータは Mapping Request 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

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

Information Table）を生成し，EN における動作処理情報を記載した Mapping Response を EN へ送信する．GSRA マッピングテーブルは，(3) で割り当てたポート番号宛の通信を，IN 宛へと書き換えるために使用するテーブルである．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（Process Information）が記載される．EN は受信した Mapping Response 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．

(5) IN へのアクセス

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．EN から IN 宛の通信は，まず EN のカーネル内で VAT 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．ここでは，通常の NAT の動作とは違い，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．送信元情報を書き換えることで，GSRA ルータをデフォルトゲートウェイと別の入り口として設置するような場合に，応答パケットがデフォルトゲートウェイへと送信されてしまうのを防いでいる．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

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，GSRA のシーケンスを見直した．以後，ホームネットワーク側の NAT を HR（Home Router）と呼ぶ．

4.1 解決すべき課題

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（HR のマッピングアドレス）へと変換される．従って 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． これを実現する一般的な方法として，一往復の TCP/UDP シーケンスを追加することにより，その応答パケットのヘッダ情報から HR のマッピングアドレスを得る方法が考えられる．しかし，近年の NAT ルータには SPI（Stateful Packet Inspection）機能が搭載されていることが多い．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．そのため，単純に TCP のシーケンスを追加すると，その通信ログが HR の SPI に記憶されてしまい，アプリケーションから送信される TCP/UDP パケットとの整合性が保たれず，HR で破棄されてしまう．よって，SPI 機能を搭載した HR であっても通信を開始できる手段が新たに必要となる．

4.2 解 決 策

上記課題を解決するため，GSRA のマッピング処理の手前に，ICMP による Binding Request（以下 $BReq_i$），TCP による Binding Request（以下 $BReq_t$），ICMP による Binding Response（以下 $BRes_i$）を追加する．$BReq_t$ は，GSRA ネゴシエーションのトリガとなった最初の通信パケットの内容をコピーし，宛先を GSRA ルータに書き換えたものである．GSRA ルータでは，$BReq_t$ を受信したら，応答を返さず，これを破棄する．これにより，ネゴシエーション完了後に改めて送信されるトリガパケット（最初の通信パケット）は，HR には “$BReq_t$ の再送パケット” とみなされる．HR は，再送パケットに対して再送前と同じ変換を行うという特徴がある．また，$BReq_t$ は，トリガパケットの内容をコピーしているため，シーケンス番号などの情報が同値となる．再送パケットであれば，再送前とシーケンス番号が変わらないのは自然であるため，SPI による破棄を回避することができる．

$BReq_i$，$BRes_i$ の往復パケットは，HR によるマッピングアドレスを EN に通知する役割を持つ．$BRes_i$ のメッセージには，$BReq_t$ のヘッダ情報から得た，HR によるマッピングアドレスを記載する．これにより，EN は HR のマッピングアドレスを得て，HR に対応したマッピング処理につなぐことが可能となる．

4.3 GSRAv2 のシーケンス

GSRAv2 のネゴシエーションシーケンスを**図 4** に示す．GSRAv2 では，HR に対応するためのバインディング処理を新たに追加する．バインディング処理では，まず EN が $BReq_i$ 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 $BReq_t$ を GSRA ルータへ送信する．$BReq_t$ 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，グループ認証処理で得たエフェメラル・ポート番号である．GSRAv2 ネゴシエーション後に送信されるトリガパケットは，$BReq_t$ の再送パケットとして HR に扱われる．GSRA ルータは $BReq_i$ を受信すると，受信したパケットを待避する．続いて $BReq_t$ 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とポート番号 $G_{HR} : m$ を取得する．その後，待

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

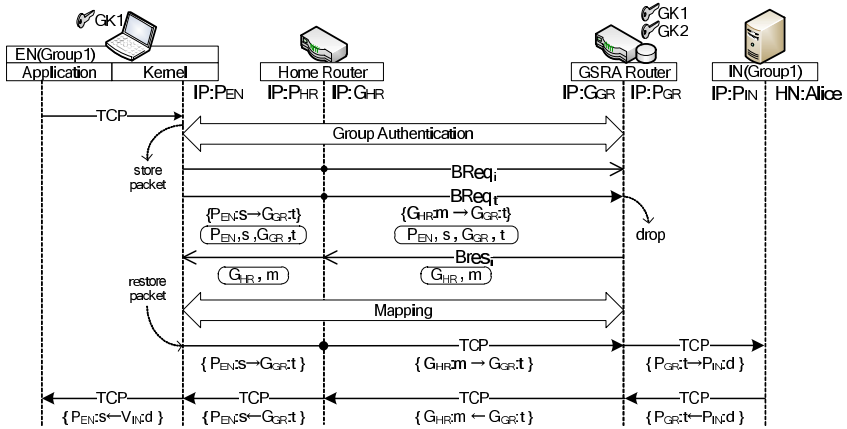

図 4 GSRAv2 ネゴシエーションの流れ
Fig. 4 Negotiation of GSRAv2.

避していた $BReq_i$ に対する $BRes_i$ を生成し，取得したマッピングアドレスをメッセージに記載して EN へ送信する．以上のバインディング処理により，GSRA ルータと EN は HR によるマッピングアドレスを得ることができ，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．ネゴシエーション完了後に送信される最初の通信パケットのシーケンス番号は，それ以前までの通信との整合性が保たれており，HR の SPI 機能によって破棄されることは無い．

バインディング処理の追加により，いかなる HR 配下からでも，リモートアクセスを開始することが可能となる．ただし，通信経路上に HR が存在するかどうかは定かでなく，HR が存在しないような状況では，Binding 処理にかかる時間は無駄となる．そのため，バインディング処理はグループ認証処理とマッピング処理の間に行うものとする．HR が存在するか否かは，Group Authentication Request のメッセージ内に記載された EN の送信元情報と，ヘッダ内の送信元を比較し，一致するかどうかで判定する．両者が等しい場合は，HR が存在しないと判断し，バインディング処理をスキップする．これにより，続いて行われるマッピング処理は，HR の有無に関わらず共通の処理とすることができる．

5. 実　　装

GSRAv2 を FreeBSD に実装した．GSRA では，EN および GSRA ルータに，GSRA 用

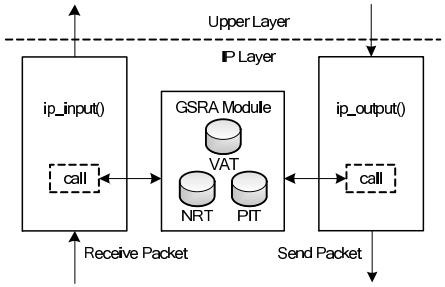

図 5 EN の実装
Fig. 5 Implementation of External Node.

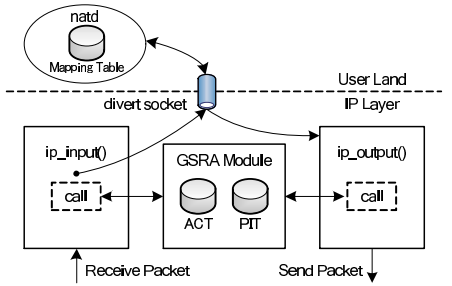

図 6 GSRA ルータの実装
Fig. 6 Implementation of GSRA router.

の処理を行う GSRA モジュールを IP 層に実装している．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．

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各制御パケットは，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．GSRAv2 では，これまでと同様に GSRA モジュールにバインディング処理の機能を追加する形で実装を行った．

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. 評　　価

既存のリモートアクセス方式と GSRAv2 を，機能面および性能測定結果から比較評価する．

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

6.1 機能面の比較

表 2 にリモートアクセス方式の比較を示す．また，各項目の詳細を以下に述べる．

- **E2E 暗号化の可否** ：GSRAv2 では，IN に PCCOM の機能を追加することでエンドエンドの暗号化通信が可能である．SSL-VPN では，VPN サーバ-IN 間も https 通信を行うことが可能である．その他の方式では，EN-VPN サーバ装置間が暗号化区間となる．社内犯等の存在を考慮すると，ローカルネットワークを通過するパケットも暗号化可能である方が望ましいといえる．
- **スループット**：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．パケットのカプセル化は，パケットを暗号化するためと，パケットをトンネリングするための 2 パターンがあり，OpenVPN と PacketiX VPN では 2 重のカプセル化オーバヘッドが発生する．PacketiX VPN はトンネリングのために Ethernet フレームを TCP でカプセル化するため，TCP over TCP の問題が起きる．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．表内の評価は，次節で述べる実測値を評価基準とした．
- **HR 対応** : IPsec-VPN は，HR が IPsec パススルー機能に対応している必要がある．その他の方式では，HR を通過することが可能である．しかし，HR が存在することで，IPsec-VPN，OpenVPN，PacketiX VPN ではアドレス管理に注意する必要が出てくる．すなわち，EN のプライベートアドレスと，VPN の通信に使用するアドレスが重複しないように管理しなければならない．
- **クライアントソフトの必要性** : SSL-VPN は Web ブラウザさえあれば使用できるが，クライアントを認証する場合は証明書を持たせる必要がある．IPsec-VPN は，多くの OS で標準でサポートしているものの，機能を有効にするためにはユーザによる設定の変更を必要とする場合がある．OpenVPN と PacketiX VPN，GSRA の 3 方式では，クライアント端末に専用ソフトウェアをインストールする必要がある．
- **アプリケーションの制約** : SSL-VPN は，使用するアプリケーションが Web ブラウザベースのものに制限される．その他の方式ではアプリケーションの制限は無い．
- **アドレス管理の必要性** : IPsec-VPN，OpenVPN，PacketiX VPN では，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注意し，管理する必要がある．各方式とも，DHCP のように 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おり，これを使用することでアクセス先 LAN で元々使用されているアドレスとの重複は防げるが，配布されたアドレスがアクセス元 LAN 内で使用されているアドレスと重複してしまう可能性がある．

以上の比較から，GSRAv2 は既存方式に比べ，機能的に優れているといえる．

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

	IPsec-VPN	SSL-VPN	OpenVPN	PacketiX	GSRAv2
E2E 暗号化の可否	×	○	×	×	○
スループット	×	△	△	×	○
HR 対応	△	○	△	△	○
クライアントソフトの必要性	△	△	×	×	×
アプリケーションの制約	○	×	○	○	○
アドレス管理の必要性	×	○	×	×	○

6.2 性能測定結果

性能を比較するため，通信開始時に発生するオーバヘッド時間及び，スループットを測定した．比較対象は，アプリケーションに制約のない IPsec-VPN と OpenVPN，PacketiX VPN の 3 方式とした．

本稿で使用した測定環境を**図 7** に示す．各装置の諸元は**表 3** 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[17] を使用した．Dummynet の設定値は，**表 4** に示す 3 パターンを用意した．

設定 A は，伝送遅延，パケットロス率ともに 0 で，Dummynet が無いものと等価である．この設定では，各方式の最大の性能を測定できる．これは，同一オフィス内の他部署との限

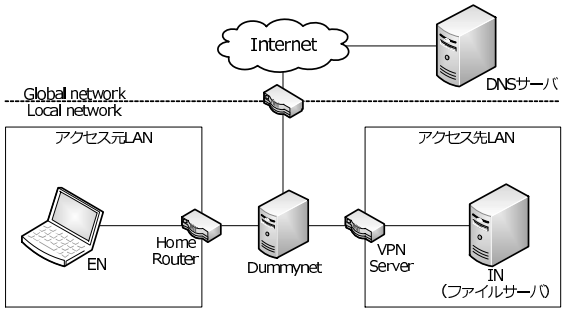

図 7 測定環境
Fig. 7 Measurement environment.

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

表 3 諸元
Table 3 Device specification.

	OS	CPU	Memory	NIC
EN	FreeBSD 7.2	Pentium4 3.40 GHz	1 GB	1000Base-TX
Home Router	FreeBSD 7.2	Pentium4 3.00 GHz	512 MB	1000Base-TX
Dummynet	FreeBSD 8.0	Pentium4 2.80 GHz	512 MB	1000Base-TX
VPN Server	FreeBSD 7.2	Pentium4 3.40 GHz	2 GB	1000Base-TX
IN	FreeBSD 7.2	Pentium4 2.80 GHz	1 GB	1000Base-TX

表 4 Dummynet の設定値
Table 4 Parameter of Dummynet.

	伝送遅延	パケットロス率
設定 A	0	0
設定 B	10 ms	0
設定 C	10 ms	0.05 %

定的なネットワーク接続などに使用する場合のスループット目安となる．

設定 B は，伝送遅延のみ発生し，パケットロスがない設定である．距離は離れているが，回線が高品質であるなどの理由からパケットロスが発生しない場合のスループットの目安となる．

設定 C は，伝送遅延とパケットロスの両方が発生する設定である．最も多い利用シーンとして想定される，インターネットを経由したリモートアクセス時の目安となる．パケットロス率の設定値は，自宅 LAN と大学の研究室 LAN 間の 4 週間分の実測値に基づいて決定した．

公平な比較を行うため，各方式とも，暗号化アルゴリズムには AES（鍵長 128bit）を使用し，暗号化範囲は EN-VPN サーバ間とした．IPsec-VPN の鍵交換プロトコルは IKEv2 を使用した．OpenVPN のパケットのカプセル化は，TCP，UDP 両方に対応しているが，TCP over TCP の問題を避けるため，UDP を選択した．オーバヘッド時間，スループットの測定は全ての条件において 10 回ずつ行い，その平均値を測定結果とした．

(1) 通信開始時のオーバヘッド時間

通信開始時のオーバヘッド時間の測定には，パケットキャプチャソフト Wireshark[⋆1]を用いた．EN で Wireshark によるキャプチャを行い，ネゴシエーションパケットが送受信される時間の差から測定結果を得た．OpenVPN と PacketiX VPN は，ネゴシエーションのみを単独で行うことができるが，IPsec-VPN と GSRAv2 では，特定の宛先のパケットが初めて送信されるときにネゴシエーションが開始される．そのため，`wget` コマンド[⋆2]を使用して IN 上のファイルにアクセスすることでネゴシエーションを開始させた．`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．測定する区間は，ネゴシエーション開始から完了までの時間（ネゴシエーション時間）と，ネゴシエーション開始からネゴシエーション完了後に実際の通信が開始されるまでの時間（総オーバヘッド時間）の 2 区間とした．これは方式によって，実際の通信パケットが送信されるまでにタイムラグが生じる場合があるためであり，実際に利用する際には後者の数値が重要となる．

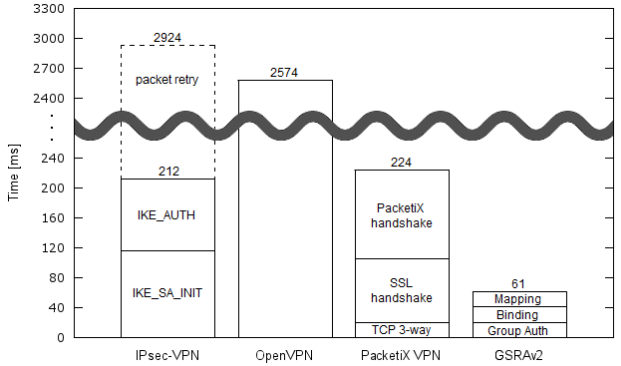

図 8 ネゴシエーション時間内訳
Fig. 8 Result of a measurement of negotiation time.

測定の結果を**図 8** に示す．IPsec-VPN によるネゴシエーションは，IKE 用の SA を確立する IKE_SA_INIT と，IPsec 通信用の SA の確立を行う IKE_AUTH の 2 往復からなり，200ms 程度のオーバヘッドが発生している．流れるパケットは 2 往復だけであるため，2RTT=40ms を除いた約 172ms が，暗号鍵の生成などの内部処理に費やされていることになる．また，総オーバヘッド時間を見ると，ネゴシエーション完了から大きなタイムラグが発生し，合計で約 3 秒となっている．この理由は，IPsec-VPN ではネゴシエーション開

⋆1 http://www.wireshark.org/

⋆2 http://www.gnu.org/software/wget/

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

始のトリガとなったパケットが失われるためである．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のを待つ必要があるため，通信開始までの時間が大きくなる．今回は`wget`（TCP）による測定であり，標準的な TCP の再送時間である 3 秒程度が上乗せされる結果になっている．図 8 では，ネゴシエーション部の時間を実線で，パケットの再送待ち時間をを破線で示している．

OpenVPN は，ネゴシエーション完了までに約 2.5 秒の時間がかかっている．処理中のパケットはすべて SSL で暗号化されるため処理時間の内訳は分からないが，VPN 用トンネルの生成や，サーバ・クライアントの SSL による認証など，計 50 往復以上のパケットのやりとりが行われる．パケットの往復数が多いため，RTT が 20ms よりも長い環境では，オーバヘッド時間が大きく延びると考えれられる．

PacketiX VPN は，SSL による認証の他に行われる処理は少なく，IPsec-VPN と同じく 200ms 程でネゴシエーションが完了している．本測定では，EN の仮想 NIC に割り当てる IP アドレスを予め固定で設定したため，アクセス先 LAN の DHCP サーバから IP アドレスを配布する場合や，PacketiX VPN の SecureNAT 機能などを使用する場合には，その分の時間が上乗せされることになる．

GSRAv2 は，通信開始まで約 60ms で完了している．GSRAv2 ネゴシエーションでは，バインディング処理が追加され，計 3 往復のパケットがやりとりされるが，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，3 往復の RTT だけで 60ms が必要となる．このことから，EN と GSRA ルータにおける内部処理時間は非常に短いと言える．また，トリガとなったパケットは，ネゴシエーション中も保持されるため，ネゴシエーション完了後すぐに通信を開始することができる．

以上から，実際にインターネットを経由した場合の RTT を想定した環境において，GSRAv2 は既存方式と比較して最も短時間で通信を開始できることが確認できた．

(2) スループット

スループットは，EN がリモートアクセスにより IN へ接続し，`wget` コマンドを用いて IN 上に保存されているファイルをダウンロードすることで測定した．測定値には `wget` による測定結果をそのまま採用した．ダウンロード対象のファイルには，1GB のダミーファイルを用意した．

スループットの測定結果を**図 9** に示す．

設定 A では，GSRAv2 のスループットが最も高く，他方式に比べ約 1.3 倍以上の速度を記録している．処理ネックとなる部分を解析したところ，HR で動作している NAT の処理がボトルネックになっていることが分かった．IPsec-VPN，OpenVPN，PacketiX VPN 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起こりスループットが低下する．GSRA で使用している暗号化プロトコル PCCOM は，暗号化時にパケットフォーマットを変更する必要がなく，カプセル化を必要としないため，上記の要因によるスループット低下が起きない．

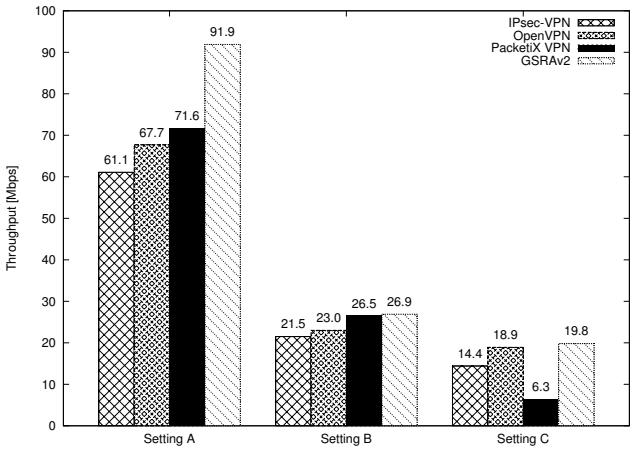

図 9 スループット測定結果
Fig. 9 Result of throughput measurement.

設定 B では，1 秒間に送受信できる回数に制限が生まれる．RTT20ms の場合であれば，50 往復が上限となる．ここで，TCP のウィンドウ制御におけるウィンドウサイズの最大値は 64KB であるため，64 × 1024 × 50 × 8=26.2Mbps が理論上の上限となる．そのため，どの方式でもそれ以下のスループットに落ち着いている．その中でも GSRAv2 が最もスループットが高く，ほぼ理論値と同等の結果を得られている．理論値を若干超えているのは，`wget` による測定の誤差と考えられる．設定 A と同じく GSRAv2 が最も早いという結果となったが，他方式との差が小さくなっている．RTT やパケットロスが発生する環境（設定 B，C）では，通信路に起因するスループット低下のウエイトが大きく，カプセル化などの影響が小さくなっていると考えられる．

設定 C では，パケットロスの発生により，どの方式でも設定 B よりスループットが低下している．中でも，PacketiX VPN は大きくスループットが低下した．PacketiX VPN は，

Vol.2012-DPS-150 No.29
Vol.2012-CSEC-56 No.29
2012/3/1

TCP/UDP パケットを TCP でカプセル化するため，パケットロスが起こる環境では TCP Over TCP 問題による影響が顕著に現れたためと考えられる．

測定結果より，GSRAv2 は全てのケースにおいて既存方式を上回るスループットを発揮することが確認できた．

7. ま と め

本稿では，リモートアクセス技術の比較評価を行い，GSRAv2 の有用性を示した．GSRAv2 は，エンドエンドでの暗号化通信が可能である点や，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) OpenVPN Technologies, Inc.: OpenVPN - Open Source VPN. http://openvpn.net/
6) Corporation., S.: PacketiX VPN 3.0 Web サイト. http://www.softether.co.jp/jp/vpn3/
7) Zorn, G.: Microsoft PPP CHAP Extensions, Version 2, RFC 2759, IETF (2000).
8) Rivest, R.: The MD4 Message-Digest Algorithm, RFC 1320, IETF (1992).
9) Brown, R.H. and Good, M.L.: DATA ENCRYPTION STANDARD (DES), FIPS 46-3, NIST (1999).
10) Olaf Titz: Why TCP Over TCP Is A Bad Idea. http://sites.inka.de/sites/bigred/devel/tcp-tcp.html
11) 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).
12) 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).
13) 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).
14) C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).
15) M.Krasnyansky: Universal TUN/TAP device driver. http://www.kernel.org/pub/linux/kernel/people/marcelo/linux-2.4/Documentation/networking/tuntap.txt
16) 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).
17) L.Rizzo: Dummynet home page. http://info.iet.unipi.it/luigi/dummynet/