情報処理学会論文誌 Vol.54 No.6 1751–1760 (June 2013)

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,a)] 鈴木 秀和[1,b)] 旭 健作[1,c)] 渡邊 晃[1,d)]

受付日 2012年9月21日, 採録日 2013年3月1日

概要：遠隔地から組織のネットワークにアクセスできるリモートアクセスの需要が増加している．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 などがあるが，どれも一長一短をかかえている．特に，ユーザ端末が家庭内のプライベートアドレス空間に存在すると，利用方法に制約が出てくることがある．我々は既存技術の課題を解決するリモートアクセス技術として，GSRA（Group-based Secure Remote Access）と呼ぶ方式を提案してきたが，ユーザが NAT 配下から使用することは想定していないという課題があった．そこで本論文では，GSRA の特長を活かしたまま，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拡張した GSRAv2 を提案する．GSRAv2 を試作しその有用性を確認した．

キーワード：リモートアクセス，NAT 越え，VPN，アクセス制御

Proposal and Evaluation of GSRAv2 that Enables Remote Access from Home

Kenta Suzuki[1,a)] Hidekazu Suzuki[1,b)] Kensaku Asahi[1,c)] Akira Watanabe[1,d)]

Received: September 21, 2012, Accepted: March 1, 2013

Abstract: The demand for remote access technologies is increasing these days. Widely used technologies, such as IPsec-VPN, SSL-VPN, and PacketiX VPN have both merits and demerits. In particular, there appear some constraints if the terminal is in the private address areas. We have proposed GSRA (Group-based Secure Remote Access) that solves demerits of the above technologies in the past. However, it assumes that the terminal has a global address. In this paper, we propose GSRAv2, by which the terminal can have a private address while maintaining the GSRA features. The trial system shows that GSRA has superior performance compared to other technologies.

Keywords: remote access, NAT traversal, VPN, access control

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ともなって，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，ユーザが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 を構築する方式として，IPsec-VPN [1], [2]，SSL-VPN [3]，OpenVPN [4]，PacketiX VPN [5]，GSRA（Group-based Secure Remote Access）[6], [7] などがある．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

[1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 468–8502, Japan
[a)] kenta.suzuki@wata-lab.meijo-u.ac.jp
[b)] hsuzuki@meijo-u.ac.jp
[c)] asahi@meijo-u.ac.jp
[d)] wtnbakr@meijo-u.ac.jp

ケーションが制限される．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，特殊な検知装置を導入しない限り，ネットワーク管理者が社員の VPN 接続を認知できず，社員による情報漏えいを防止できないという課題がある．

GSRA は，これら既存の技術の課題を解決するために提案された技術である．GSRA は，NAT 越え技術 NAT-f（NAT-free protocol）[8] のしくみを利用し，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により安全なリモートアクセスを実現している．NAT-f はアクセスする側のユーザ端末と NAT を改造する必要がある．GSRA では，NAT-f に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，アドレス変換のみによりリモートアクセスを実現するため，高スループットが得られるという利点がある．しかし，ユーザ端末がグローバルアドレスを持つことが前提で，家庭内のプライベートアドレス空間からは利用できないという課題があった．

ここで，近年のリモートアクセスの利用シーンとして，学生が自宅から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，在宅勤務を行ったりすることなどが考えられる．このようなケースでは，ユーザ端末は NAT 配下のホームネットワーク内に存在し，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．このような利用シーンを想定して既存技術を比較し直すと，IPsec-VPN は NAT との相性が悪く，使用する NAT によっては利用できないケースがある．IPsec-VPN，OpenVPN，PacketiX VPN は，ホームネットワーク側のプライベート IP アドレスと，組織内ネットワークで使用されているプライベート IP アドレスが重複しないような管理が必要である．また，GSRA においては，ユーザ端末がホームネットワーク内にある場合は利用できなかった．

そこで本論文では，GSRA に改造を施し，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 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．FreeBSD で GSRAv2 の実装を行い，動作検証を行った．また，既存技術との性能比較を行い，その優位性を確認したので報告する．

以降，2 章で既存技術について，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，本論文ではユーザ端末を EN（External Node），アクセスされる側のサーバを IN（Internal Node）と表記する．

2.1 IPsec-VPN

IPsec-VPN は IPsec のしく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）[1] による認証と暗号鍵の共有，IPsec ESP（Encapsulating Security Payload）[2] トンネルモードによる暗号通信を行うことにより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がない．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などを端末ごとに設定でき，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．ここで，ユーザがホームネットワーク内から IPsec-VPN によるリモートアクセスを行うと，ホームネットワーク側の NAT によるアドレス変換が，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る．そのため，ホームネットワーク側の NAT として，IPsec をパススルーする機能を有したもの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．組織ネットワークの DMZ（DeMilitarized Zone）上などに 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，EN 側で特別な設定やソフトのインストールをしなくても，リモートアクセスを実現できる．また，EN が NAT 配下であっても問題なく使用することができる．ただし，EN 側の認証はパスワードに頼るものとなり，企業など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，EN にも証明書を持たせる必要がある．この場合は SSL-VPN の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 [9] を用いて，EN とサーバ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，

Ethernet フレームを TCP/UDP でカプセル化して通信を行うため，任意のプロトコルを使用できるという利点がある．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．

2.4 PacketiX VPN

PacketiX VPN は，EN と IN 上に独自の仮想 NIC を作成し，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，SSL でカプセル化して行われるため，通信経路上に NAT やファイアウォールがあっても通信を行うことができる．しかし，このような特性上，一般社員がネットワーク管理者に無断で PacketiX VPN を構築できることが問題になっている．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，社内ネットワークが危険にさらされる可能性がある（ただし，SSL でカプセル化された PacketiX VPN を検知できるファイアウォールを導入すれば防止可能である）．また，TCP でカプセル化を行うため，パケットロスが発生する環境では，TCP over TCP [*1] [10] の問題が発生し，スループットが大きく減少する．

3. GSRA

本章では，提案方式の要素技術となる GSRA について説明する．GSRA は，NAT-f にセキュリティ機能を追加した技術である．NAT-f は EN のカーネルとアクセス先ネットワーク内の NAT ルータを改造し，EN のアプリケーションに依存しない NAT 越えを実現する．グループ単位の認証を行うため，管理負荷が低い．カプセル化技術は使用せず，アドレス変換により機能を実現するため，スループットが高いなどの特長がある．本論文で使用する記号の定義は以下のとおりである．

- G_x（x = NodeID）：グローバル IP アドレス
- P_x：プライベート IP アドレス
- V_x：仮想 IP アドレス
- s，d，t，m：ポート番号
- $G_x : s$：トランスポートアドレス（IP アドレス G_x 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
- $G_x : s \leftrightarrow G_y : d$：$G_x : s$ と $G_y : d$ の通信
- $G_x : s \Leftrightarrow G_y : d$：$G_x : s$ と $G_y : d$ の変換

[*1] TCP を TCP でカプセル化すると再送制御が二重に発生し通信効率が落ちる現象．

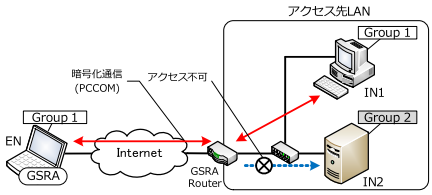


図 1 GSRA によるリモートアクセスの構成例
Fig. 1 An example of a remote access configuration with GSRA.

表 1 ACT の例
Table 1 An example of Access Control Table.

Host Name	IP Address	Service	Group
Alice	P_{IN}	d（tcp）	Group1
		e（udp）	Group2

3.1 GSRA の構成

GSRA は，NAT 越え技術 NAT-f 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．GSRA によるリモートアクセスの構成例を**図 1** に示す．ここで，EN に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．GSRA ルータには ACT（Access Control 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），グループ番号が登録されている．ACT の設定により，サービスごと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，Group2 に属する端末は，UDP の e 番ポートに該当するサービスを利用できる．

3.2 通信シーケンス

図 2 に 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 をあらかじめ所持している．グループ鍵は，グループごと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．

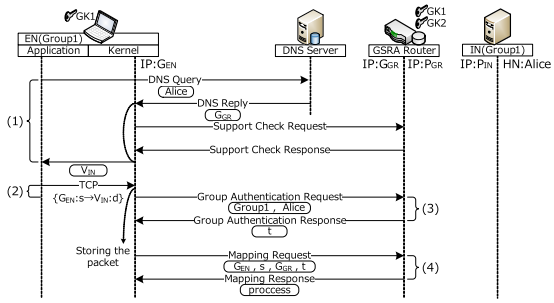


図 2 GSRA ネゴシエーションの流れ
Fig. 2 Negotiation of GSRA.

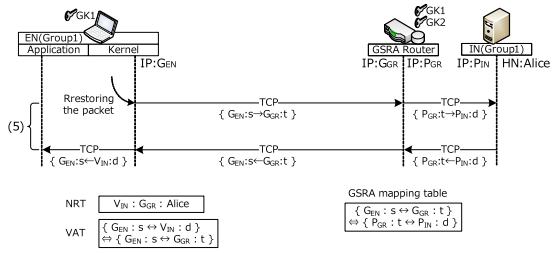


図 3 アドレス変換処理によるリモートアクセス
Fig. 3 Remote access with address translation process.

EN が IN と通信を開始するまでの手順は以下のとおりである．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 GSRA ルータ配下ホストを識別できない．しかし，仮想 IP アドレスとして通知することにより，EN 側から特定の IN を指定することが可能になる．このとき，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 はカーネルで 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，あらかじめ共有していたグループ鍵を用いて，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 が提供するサービスへのアクセス可否の確認を行う．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，GSRA ルータの未使用ポートの中から選ばれる番号で，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る．EN は Group Authentication Response メッセージから t を取得して，VAT を生成する．

(4)マッピング処理

GSRA では，EN のカーネルおよび 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．

(5)IN へのアクセス

図 3 に，生成されたテーブルを用いて，通信パケットのアドレス情報が変換されていく様子を示す．暗号化処理に関しては，本論文の本質ではないため記述を省略する．EN は (2) でカーネル内に待避していたパケットを送信バッファに戻し，通信を開始する．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．GSRA ルータでは，受け取ったパケットを GSRA マッピングテーブルに従って，宛先と送信元のアドレス/ポート番号を GSRA ルータのものに書き換え IN へ転送する．IN から EN への応答は上記と逆の順序でアドレス変換を行い 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

GSRA は EN がグローバルアドレスを持つことを想定していた．そこで，プライベートアドレス空間からのリモートアクセスを可能とするため，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

GSRA ルータでは，Mapping Request のメッセージ部分に記載してある EN のアドレス/ポート番号をもとに GSRA マッピングテーブルを生成する．しかし，HR が存在すると，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 のマッピング情報）へと変換される．そこで，HR が存在する場合は，Mapping Request の中に記述する情報を HR のマッピング情報とする必要がある．これを可能とするには，EN があらかじめ HR のマッピング情報を知っておく必要がある．

一方，近年の NAT ルータには SPI（Stateful Packet Inspection）と呼ぶ強力なフィルタリング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，到着したパケットの整合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．特に TCP のコネクション確立シーケンスが正しくないと，不正パケットとして破棄される．HR が生成するマッピング情報は，TCP の SYN パケットによって初めて生成されるため，あらかじめ HR のマッピング情報を EN が知っておかなくてはならない．また，この方法は HR に SPI 機能が搭載されていることを前提として実現する必要がある．

4.2 解決策

上記の課題を解決するために採用した提案方式の原理を図 4 に示す．ここで示す処理を以後バインディング処理と呼ぶ．バインディング処理は，EN のアプリケーションが宛先 V_{IN} のパケットを最初に送信する際に実行される．この処理では，まず最初に送信される宛先 V_{IN} のパケットをカーネルにおいて待避しておく．TCP の場合，最初のパケットは TCP SYN である．次に，EN は ICMP による制御パケットを送付し，HR に ICMP のマッピングを行わせる．このマッピングは，後で GSRA ルータから EN に対して HR のマッピング情報を伝えるために利用される．EN は待避した TCP SYN パケットとまったく同一のパケットを GSRA ルータに送信し，HR に TCP のマッピングを行わせる．GSRA ルータは，このパケットを受信すると，IP ヘッダの内容から，HR で生成された TCP マッピング情報を取得する．上記 TCP SYN パケットは GSRA ルータで廃棄する．GSRA ルータは，取得したマッピング情報を ICMP のメッセージの中に記載して EN に返送する．このパケットは，HR にすでに ICMP のマッピングができているため，EN に到着することができる．EN は取得したマッピング情報をもとに，VAT を生成し，さらにこの情報を使って以後の GSRA マッピング処理を実行する．GSRA マッピング処理の方法は，従来の GSRA とまったく同様である．

上記の方法により，EN の VAT と GSRA ルータの GSRA マッピングテーブルが正しく生成される．EN は待避していた TCP SYN を送信バッファに戻し，通信を開始する．EN が TCP SYN を送信すると，HR には 2 回目の TCP SYN パケットが通過することになるが，これは再送パケットと見なされ，HR で廃棄されることはない．この方法によると，HR が SPI のフィルタリング機能を備えていても，その制約を回避できる．

4.3 GSRAv2 のシーケンス

図 5 に GSRAv2 ネゴシエーションの流れを示す．GSRAv2 では，基本的な GSRA の処理内容をそのままに，図 4 で述べたバインディング処理を実行する．バインディング処理において，上位アプリケーションが TCP の場合に使用する TCP パケット名を $BReq_t$，上位アプリケーションが UDP の場合に使用する UDP パケット名を $BReq_u$，ICMP パケット名を $BReq_i$，$BRes_i$ とする．$BReq_t$ は，GSRA ネゴシエーションのトリガとなる最初の TCP SYN パケットをコピーし，宛先を GSRA ルータに書き換えたもの，$BReq_u$ は，トリガとなった最初の UDP パケットをコピーし，宛先を GSRA ルータに書き換えたものである．図 5 は TCP 通信の場合を示しており，UDP 通信の場合は $BReq_t$ のパケットが $BReq_u$ に置き換わったものになる．

通信経路上に HR が存在しないような状況では，バインディング処理を行う必要がないため，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挿入する．

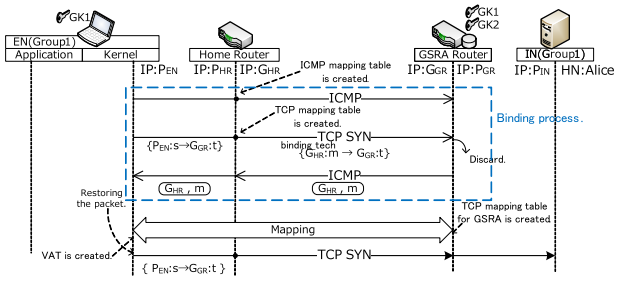


図 4 提案方式の原理
Fig. 4 The principle of the proposed method.

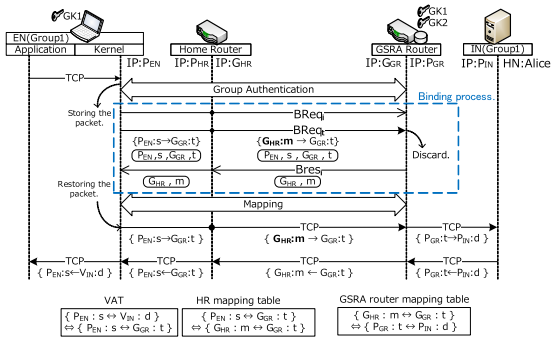


図 5 GSRAv2 ネゴシエーションの流れ
Fig. 5 Negotiation of GSRAv2.

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できる．マッピング処理は，HR の有無にかかわらず既存の GSRA と同一である．上記の方法により，GSRA の特長を活かしつつ，HR 配下からも利用することが可能となり，追加の処理時間も最小限に抑えることができる．

5. 実装

GSRAv2 を FreeBSD に実装した．既存の GSRA は，EN および GSRA ルータの IP 層に GSRA モジュールを実装し，動作検証を終えている．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 層の処理はいっさい変更しない構造となっている．

5.1 EN のモジュール構成

EN のモジュール構成を**図 6** に示す．パケットを送受信する際，IP 層で入出力関数 `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 の情報を保持する．その後の通信パケットは，すべて GSRA モジュールへ渡され，テーブルのエントリに従ってアドレス変換などの処理を行う．GSRAv2 では，GSRA モジュールのネゴシエーション処理にバインディング処理の機能を追加する形で改造を行った．

5.2 GSRA ルータのモジュール構成

GSRA ルータのモジュール構成を**図 7** 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 のユーザランドで NAT 機能を実行するデーモンである．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，アドレス/ポート変換を行う．GSRA モジュールには ACT の情報を保持し，アクセス制御および暗号化などの処理を行う．

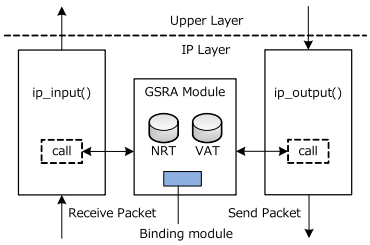


図 6 EN のモジュール構成
Fig. 6 Module configuration of EN.

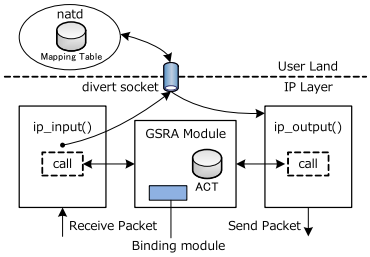


図 7 GSRA ルータのモジュール構成
Fig. 7 Module configuration of GSRA router.

6. 評価

本章では，既存のリモートアクセス方式と GSRAv2 を機能面で定性的に比較する．また，既存方式と GSRAv2 を実際に構築し，通信開始時のオーバヘッド時間とスループットを測定し，結果について考察を行った．

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．機能面の比較項目として，HR への対応の有無，クライアントへの導入のしやすさ，アプリケーションの制約，ユーザ管理の容易さ，スループットを取り上げた．

- **HR への対応：**
  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 が存在することにより，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に管理する必要がある．各方式とも，VPN サーバ側から DHCP でアドレスを配布するしくみが用意されており，これを使用することで IN 側ネットワーク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 EN 側ネットワークで使用されているアドレスと重複しないよう管理する必要がある．SSL-VPN と GSRAv2 は，HR の存在をまったく意識する必要がない．
- **クライアントへの導入のしやすさ：**
  OpenVPN と PacketiX VPN，GSRAv2 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ため×とした．IPsec-VPN は，多くの OS で標準でサポートしているものの，ユーザ

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	Open VPN	PacketiX VPN	GSRA v2
HR への対応	△	○	△	△	○
導入のしやすさ	△	△	×	×	×
アプリケーションの制約	○	×	○	○	○
管理の容易さ	×	○	△	×	○
スループット	×	△	△	×	○

による複雑な設定の変更が必要な場合があるため△とした．SSL-VPN は Web ブラウザさえあれば使用できるため導入が容易とされているが，クライアント端末を確実に認証する場合はクライアントにも証明書を持たせる必要があるため△とした．

- **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ない．
- **ユーザ管理の容易さ：**
  IPsec は汎用性を重視するあまり設定項目数が多く，サーバ側とクライアント側で 1 対 1 での設定が必要となるため×とした．SSL-VPN は 1 対 1 の設定が必要であるが，設定項目数がユーザ名とパスワードのみであり設定項目が少ないことから○とした．OpenVPN は設定項目数は多いものの，クライアント間で共通化できる部分が多いため△とした．PacketiX VPN は設定項目数としては OpenVPN と同程度であるが，ネットワーク管理者としては，ユーザが勝手に PacketiX VPN を使うことを防止するための管理が別途必要になることを考慮し×とした．GSRA は設定項目数が少ないうえ，グループ単位の管理が可能であり○とした．
- **スループット：**
  GSRAv2 はパケット長が変化せず，アドレス変換のみで実現する．また，すべての処理をカーネルで実現するためスループットが高い．他の方式は，カプセル化が基本であり，一般に通信性能が劣化する．パケットのカプセル化は，暗号化するためと，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 TCP によりカプセル化するため，アプリケーションが TCP の場合は，TCP over TCP の問題が発生し，性能劣化の要因となる．スループットについては，次節であらためて比較する．

ここで，表 2 の比較は GSRAv2 の導入環境が整備されたことを仮定したものである．GSRAv2 は現在のところ OS が FreeBSD に限定される．また，EN のカーネルに実装する必要があるため，専門知識がなくても導入できるようにするには，GUI のサポートなどが必須となる．

6.2 性能測定

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および，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．IPsec は FreeBSD7.2 のパッケージ racoon2-20090327c，OpenVPN は同じく FreeBSD7.2 のパッケージ openvpn-2.0.6_9 を使用した．Packetix VPN クライアントは FreeBSD に対応していないため，PacketiX VPN の性能測定時のみ，EN には Windows7 を使用し，PacketiX Ver.3.0 を使用した．

本論文で使用した測定環境を**図 8** に示す．各装置の諸元は**表 3** に示すとおりである．各装置の NIC としては，すべて 1000Base-T を使用した．EN が存在するネットワークと IN が存在するネットワーク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 [11] を挿入した．Dummynet の設定値は，**表 4** に示す 2 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 がないものと等価である．この設定では，各方式の最大性能を測定できる．設定 B は，伝送遅延時間 10 ms，パケットロス率 0.05%とした場合である．この設定は，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．ここで，パケットロス率の値は，筆者の自宅と大学研究室のサーバ間で連続して `ping` を実行し，4 週間分の実測値の平均から設定したものである．

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 128 bit）を使用し，暗号化範囲は EN と VPN サーバ間とした．IPsec-VPN の鍵交換プロトコルは IKEv2 [1] を使用した．OpenVPN 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．暗号化プロトコルは，IPsec-VPN は ESP，OpenVPN と PacketiX VPN は SSL，GSRAv2 は PCCOM [12] である．

OpenVPN と PacketiX VPN は一般に第 3 のサーバ装置

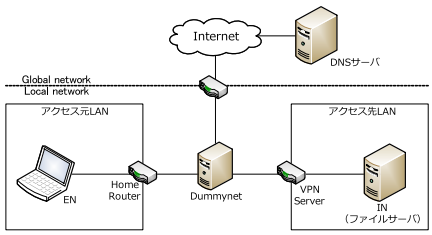


図 8 測定環境
Fig. 8 Measurement environment.

表 3 諸元
Table 3 Device specification.

	OS	CPU	Memory
EN	FreeBSD7.2	Pentium4 3.40 GHz	1 GB
Home Router	FreeBSD7.2	Pentium4 3.00 GHz	512 MB
Dummynet	FreeBSD8.0	Pentium4 2.80 GHz	512 MB
VPN Server	FreeBSD7.2	Pentium4 3.40 GHz	2 GB
IN	FreeBSD7.2	Pentium4 2.80 GHz	1 GB

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 ms	0%
設定 B	10 ms	0.05%

を経由した通信であり，経路が冗長となる可能性があるが，今回の測定ではこの機能を VPN サーバに内蔵させ，冗長経路のない形で測定した．通信開始時のオーバヘッド時間，スループットの測定はすべての条件において 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 [*2]を用いた．EN で Wireshark によるパケットキャプチャを行い，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，EN の立ち上げ時にネゴシエーションが単独で実行されるためこの時間を測定した．一方，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ため，`wget` コマンド[*3]を使用して IN 上のファイルにアクセスすることによりネゴシエーションを開始させた．測定する区間は，ネゴシエーションの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実際の通信が開始されるまでの時間（通信開始時間）の 2 通りとした．実際に利用する際には後者の数値が重要となる．

ネゴシエーション時間内訳の測定結果を**図 9** 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，212 ms のオーバヘッドが発生した．2 往復だけであるため，伝送遅延 × 2 往復 = 40 ms を除いた 172 ms 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，通信開始時間を見ると，約 3 秒が必要であった．この理由は，IPsec ではネゴシエーション開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り，通信開始までの時間が大きくなる．今回は TCP による測定であり，標準的な TCP の再送時間である 3 秒が必要という結果になった．

OpenVPN は，ネゴシエーション完了までに約 2.6 秒の時間が必要であった．処理中のパケットはすべて SSL で暗号化されるため内訳は解析できないが，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，伝送遅延が大きい環境では，オーバヘッド時間がさらに大きくなると考えれられる．ただし，この動作は端末の立ち上げ時のみである．

PacketiX VPN は，IPsec-VPN と同程度の 224 ms でネゴシエーションが完了した．ただし，この測定では EN の仮想 NIC に割り当てる IP アドレスをあらかじめ固定としたため，DHCP によって EN に対して IP アドレスを配布する場合には，その分の時間が別途必要である．PacketiX VPN においても，この動作は端末の立ち上げ時のみである．

GSRAv2 は，通信開始まで 61 ms で完了した．この時間はコネクションごとに必要であるが，実用上は問題のない値である．GSRAv2 ネゴシエーションでは，バインディング処理の追加で，計 3 往復のパケットがやりとりされるため伝送遅延だけで 60 ms 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 1 ms と非常に短いことが分かる．ネゴシエーションは，GSRA では 2 往復，GSRAv2 では 3 往復であることから，単純に換算すると 1 往復あたり約 20 ms となり，この時間が GSRA と GSRAv2 の差になると考えられる．

(2)スループット

スループットは，EN が `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により測定した．測定値は `wget` による測定結果をそのまま採用した．ダウンロード対象ファイルには，1 GB のダミーファイルを用意した[*4]．なお，PacketiX VPN の圧縮機能は無効とした．

スループット測定結果を**図 10** 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 倍以上の速度を達成した．1000Base-T の NIC 単体での性能値は，LAN 間直接接続で 932 Mbps という値を確認済みであり，NIC は性能ネックにはならない．また，HR が単に NAT ルータとして動作したときの限界スループット値は 98.4 Mbps であった．この値は GSRAv2 の測定値 91.9 Mbps と比較的近いため，どの程度の影響があったかはさらなる調査が必要である．

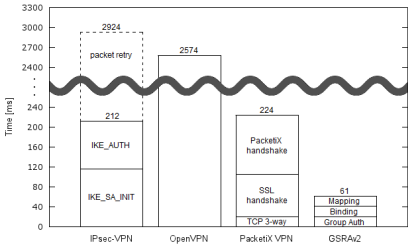


図 9 ネゴシエーション時間内訳

Fig. 9 Result of a measurement of negotiation time.

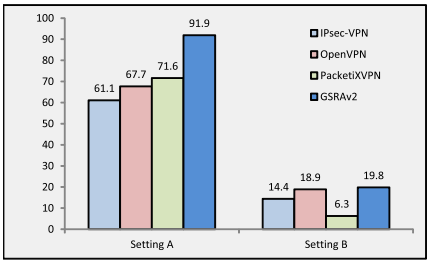


図 10 スループット測定結果

Fig. 10 Results of throughput measurement.

*2 http://www.wireshark.org/
*3 http://www.gnu.org/software/wget/
*4 ダミーファイルは下記コマンドで作成したものである．
`dd if=/dev/zero of=dummy.file bs=1M count=1000`

IPsec-VPN，OpenVPN，PacketiX VPN は，パケットのカプセル化処理とヘッダオーバヘッドによ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，スループット低下が発生しない．データ転送に係る部分の動作は GSRA と GSRAv2 ではまったく同じであるため，両者は同一のスループットである．

設定 B 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るため，各方式の違いは少なくなった．この中で，PacketiX VPN は大きくスループットが低下した．これは，TCP によりカプセル化するため，カプセルヘッダによる TCP の再送と，オリジナルパケットによる TCP の再送が重畳する TCP over TCP の問題が顕著に現れたためと考えられる．

6.3 IPv6 への対応について

IPv4 グローバルアドレスの枯渇状況から，今後 IPv6 へ移行していくことは避けられないといわれている．しかしながら，IPv4 は今後も存在し続けることが想定でき，NAT が存在するネットワークを考慮することは必須である．GSRAv2 は，通信経路上に NAT が介在するときの課題を解決するために考案されたものであり，IPv6 への対応は現時点では考慮されていない．一方，NAT の利点として，内部ネットワークのアドレスを外部から隠蔽できるという点が注目されることがある．IPv6 に移行したとしても，NAT の役割を果たす装置は必要になるという考えも存在する [13], [14]．そのような場合には，GSRAv2 のような方式を，IPv6 にも適用できる可能性はあると考えられる．

7. まとめ

既存の GSRA は，リモートアクセスとして優れた特長を備えていたが，自宅などのプライベートアドレス空間からの利用ができないという課題があった．本論文では，既存の GSRA にバインディング処理を追加することにより，あらゆる HR 配下のプライベートアドレス空間からのリモートアクセスを可能とした．GSRAv2 は，管理負荷が少ないことや，アドレス管理が不要である点など，既存の GSRA の特長をそのまま引き継いでいる．実機での測定においては，既存方式を上回る性能を発揮できることが分かった．

参考文献

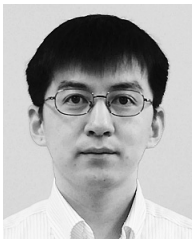
[1] Kaufman, C., Hoffman, P., Nir, Y. and Eronen, P.: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).
[2] Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).
[3] Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol, RFC 5246, IETF (2008).
[4] OpenVPN Technologies, Inc.: OpenVPN – Open Source VPN, available from ⟨http://openvpn.net/⟩.
[5] SoftEther Corporation: PacketiX VPN 3.0, available from ⟨http://www.softether.co.jp/jp/vpn3/⟩.
[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] 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).
[8] 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).
[9] Krasnyansky, M.: Universal TUN/TAP device driver, available from ⟨http://www.kernel.org/pub/linux/kernel/people/marcelo/linux-2.4/Documentation/networking/tuntap.txt⟩.
[10] Titz, O.: Why TCP Over TCP Is A Bad Idea, available from ⟨http://sites.inka.de/sites/bigred/devel/tcp-tcp.html⟩.
[11] Rizzo, L.: Dummynet home page, available from ⟨http://info.iet.unipi.it/˜luigi/dummynet/⟩.
[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] Thaler, D., Zhang, L. and Lebovitz, G.: IAB Thoughts on IPv6 Network Address Translation, RFC 5902, IETF (2010).
[14] Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prefix Translation, RFC 6296, IETF (2011).

鈴木 健太 （正会員）

2010 年名城大学理工学部情報工学科卒業．2012 年同大学大学院理工学研究科情報工学専攻修了．同年中部テレコミュニケーション株式会社入社．サービスオペレーションセンターに所属．修士（工学）．

鈴木 秀和 （正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．2009 年同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．2008 年日本学術振興会特別研究員．2010 年より名城大学理工学部助教．ネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事．博士（工学）．電子情報通信学会，IEEE 各会員．



旭 健作 （正会員）

2001 年名城大学理工学部電気電子工学科卒業．2003 年同大学大学院理工学研究科電気電子工学専攻修士課程修了．2008 年同大学院理工学研究科電気電子工学専攻博士課程修了．同年名城大学理工学部助教，現在に至る．博士（工学）．無線通信や音響に関する信号処理の研究に従事．平成 14 年度情報処理学会東海支部学生論文奨励賞受賞，平成 16 年度電気関係学会東海支部連合大会奨励賞受賞．電子情報通信学会，日本音響学会，IEEE 各会員．

渡邊 晃 （正会員）

1974 年慶應義塾大学工学部電気工学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．