情報処理学会論文誌 Vol. 52 No. 9 1234–1243 (Sep. 2011)

NATを跨る閉域通信グループの提案と評価

後藤 裕司[†1,*1] 鈴木 秀和[†1] 渡邊 晃[†1]

不正アクセスなどの脅威に対するセキュリティ対策として通信の安全が確保されたメンバを閉域通信グループとして定義する方法は有用である．IPsec は，端末が移動するなどしてシステム構成が頻繁に変わるような環境では，管理負荷が大きくなりこのような目的に適していない．そこで，閉域通信グループを構築する装置がシステム構成の変化を学習し，システム構成が変わってもグループの維持を可能とする動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）が提案されている．しかし，DPRP は，通信経路上に NAT（Network Address Translation）が介在するような環境には対応できない．そこで本論文では，NAT-f（NAT-free protocol）の NAT 越え技術を DPRP に流用し，NAT 越えができる拡張 DPRP を実現した．このとき，NAT が多段になることも考慮した．これにより，グローバルアドレスとプライベートアドレスを跨る閉域通信グループを定義することが可能となった．提案方式を FreeBSD 上に実装した結果，従来の DPRP が果たした役割をそのまま継承し，DPRP のオーバヘッドも 12% 程度の増加で済むことを確認した．

Proposal of Closed Communication Groups over NATs and its Evaluation

Yuji Goto,[†1,*1] Hidekazu Suzuki[†1] and Akira Watanabe[†1]

For the security measures against threats such as illegal access, etc. it is useful to define and form closed communication groups in order to make communication secure. IPsec is not appropriate in the case where system configurations frequently change like intranets, because the management loads of the network manager are quite large. To solve this problem, we have been proposing Dynamic Process Resolution Protocol (DPRP), by which devices in the network learn changes of system configurations automatically, and maintain the closed communication groups. However, the conventional DPRP was not applicable when a Network Address Translation (NAT) device exists on the way of the communication path. In this paper, we propose Extended DPRP that can traverse NATs, merging DPRP with NAT-f, one of NAT traversal technologies, considering multiple NATs. By this method, it is ready to make closed communication groups stretching over global address and private address areas. We have implemented Extended DPRP, and confirmed its effectiveness.

1. はじめに

ネットワークのインフラ環境を利用しつつ安全な通信を行うことは企業ネットワークにおいて重要な課題である．しかし，ネットワークインフラは多くの人が共有するため，悪意のあるユーザが存在していることを想定する必要がある．そこで閉域通信グループを定義し，通信開始時に認証処理を実行したり，暗号化通信を行う必要がある．ここで言う閉域通信グループとは，通信の安全が確保されたメンバの集合を示し，以下 CCG（Closed Communication Group）と記述する．

CCG の構築単位は，個人単位，ドメイン単位，両者の混在が考えられる．本論文が目指す CCG は，両者の混在環境である．企業ではドメイン単位の業務グループと個人単位の業務グループが混在することがあり，混在環境での CCG はこのような業務グループと対応づけて定義するのに適している．ドメイン単位の業務グループとは，例えば人事部，経理部のような単位である．個人単位の業務グループとは，例えば新規開発プロジェクトに係るメンバから構成され，複数部門を跨るメンバより構成されるグループである．これらの CCG 構成メンバは，共有サーバなどにより自由に情報を共有できるが，他のメンバは社員であっても当該サーバをアクセスできない．企業ネットワークでは，引っ越しや出張などにより，たびたびネットワーク構成が変化するが，CCG の定義は変わらない場合が多い．このようなときに管理負荷が少ないことが望ましい．

ここで CCG を構築するに当たり，通信経路上に NAT（Network Address Translation）が存在すると，その実現に大きな制約が出る．近年の IPv4 グローバスアドレスの枯渇により，組織のネットワークはプライベートアドレスで構築することが一般である．そのため，インターネットと組織のネットワークの間には必ず NAT が必要となる．プライベートアドレスの導入により，IPv4 は延命を果たしたが，その代償として，NAT の外側の端末から内側の端末に向けて通信が開始できないという制約が生じることとなった．これは NAT 越え

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
*1 現在，株式会社日立情報システムズ
Presently with Hitachi Information Systems, Ltd.

問題と呼ばれており，IPv4 の汎用性を損なう大きな要因となっている．IPv6 に移行した場合には NAT 越え問題は存在しないが，IPv4 との互換性がないことから，現時点では IPv6 の普及は遅々として進んでいない．IPv6 は必要に応じて徐々に導入されるが，IPv4 は今後も引き続き最も重要なネットワークであり続けるものと判断できる．従って，NAT 越え問題は，今後も重要な課題として認識する必要がある．

NAT が介在するネットワークにおいてもセキュアでかつ自由な通信が可能な CCG を構築できると有用である．例えば，企業ネットワークの中に NAT を設置するような場合においても CCG を構築することができる．また，今後のネットワークでは，家庭のネットワークをプライベートアドレスで構築することが必須である．このとき，自宅のサーバに，グローバルアドレス上の外出先からセキュアにアクセスしたいという要求を満たすことができる．

CCG を実現するためには VPN 技術が利用可能で，既存技術の代表として IPsec[1] がある．IPsec のトランスポートモードにより個人単位の CCG，トンネルモードによりドメイン単位の CCG を構築できる．しかし，CCG 定義に係る鍵情報交換プロトコル IPsec/IKE は，基本的に 1 対 1 の定義しかできないため，メンバ数 n による CCG の定義を行うには，n^2 分の設定が必要となり大きな管理負荷がかかる．また，IPsec はトランスポートモードとトンネルモードの間に互換性がなく，個人単位とドメイン単位の混在した CCG を定義する場合は，端末が両モードの設定を保持する必要がある．メンバが場所を移動して IP アドレスが変わると，IKE の再定義が必要となる．さらに，暗号化通信プロトコル IPsec/ESP は，パケットの完全性を厳密に保証するため，パケットのアドレスやポート番号を書き換える NAT との相性が極めて悪い．

そこで，CCG の構築を目的とし，IPsec の課題を解決した DPRP（Dynamic Process Resolution Protocol）が提案されている[2]．DPRP を用いたシステムでは，CCG と共通鍵暗号方式の暗号鍵を 1 対 1 に対応づけ，IP アドレスに依存しない CCG の定義を行う．DPRP は，通信開始時に CCG 構成装置が各自のグループ番号を相互に交換し，そのときのネットワーク構成に合わせて動作処理情報を動的に生成する．個人単位とドメイン単位の CCG が混在することも想定しており，このような環境であっても動作可能である．引っ越しや出張などでメンバのアドレスが変化しても，CCG の定義が同じであれば管理負荷は一切発生しない．

しかし，DPRP では通信経路上に NAT が存在することが想定されていない．そのため，通信パケットの IP アドレスおよびポート番号が NAT に より変換されると，動作処理情報が正しく生成できない．さらには，NAT 越え問題のために通信開始の方向に制約が生じることには対処できない．

NAT を跨る CCG を実現するためには，まず NAT 越え問題をどのように解決するかを検討する必要がある．NAT 越え問題に係る既存技術を大きく分類すると以下のようになる．すなわち，現存する NAT をそのまま使えることを目的としたアプリケーションレベル改造方式（STUN[3]，TURN[4]，UPnP[5]），既存のアプリケーションをそのまま使用できることを目的としたネットワークレイヤ改造方式（4+4[6]，NAT-f[7]，MIPNAT[8]），端末の改造を不要とすることを目的とした端末非依存方式（AVES[9]，NTSS[10]）がある．アプリケーションレベル改造方式は，アプリケーションが限定され，第三の装置が必要になるという課題がある．ネットワークレイヤ改造方式は，端末のカーネルを改造するため，OS ごとに異なる対応が必要となる．端末非依存方式は，NAT と連携した第三の装置が必要になるという課題がある．

本論文では，NAT が介在する環境でも CCG を構築する方法として，DPRP に NAT-f で実現している NAT 越え機能を流用した拡張 DPRP を提案する．NAT-f は，第三の装置が不要であり，かつ NAT 配下の IP アドレスを隠蔽したまま NAT 越え問題を解決できるという特長を持つ．拡張 DPRP は NAT-f の特長を継承し，かつ DPRP が果たした CCG を構築するという役割をそのまま実現できる．アプリケーションの種類に関わらず，NAT の外側または内側のどちらの端末からでも自由に通信の開始が可能である．さらに，NAT が多段構成である場合も動作可能である．

拡張 DPRP をエンド端末と NAT ルータに実装し，動作検証を行った．その結果，NAT が存在しても通信の制約がなく，かつ CCG の定義が可能であることを確認した．性能測定の結果，通信開始時のオーバヘッドは既存の DPRP と比べ，12% 程度の増加で収まった．

以下，2 章で提案方式の要素技術である DPRP と NAT-f について述べ，3 章で拡張 DPRP について詳述する．4 章で実装と評価結果を示し，5 章でまとめる．

2. 要素技術

2.1 DPRP

DPRP（Dynamic Process Resolution Protocol）は，通信開始に先立ち安全な通信経路を確立する役割を持つ IP 層のプロトコルである．**図 1** に DPRP を用いる場合の CCG の

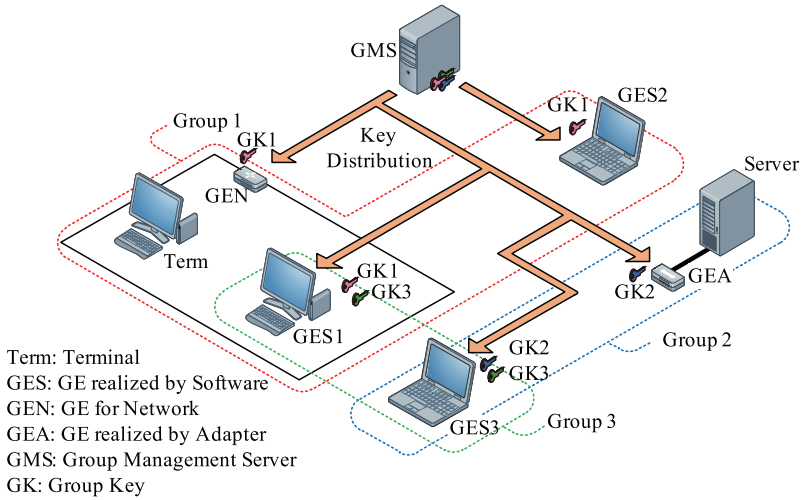

図 1　CCG の構築方法
Fig. 1　Construction method of closed communication groups.

構築方法を示す．DPRP の機能を実装した装置を GE（GSCIP ⋆1Element）と呼び，ルータタイプの GEN（GE for Network），各端末に実装するソフトウェアタイプの GES（GE realized by Software），サーバや一般ルータの直前に設置するブリッジタイプの GEA（GE realized by Adapter）がある．GEN の配下に存在する一般端末（以下 Term）は GEN によって一括して保護される．GSCIP では同一のグループ鍵 GK（Group Key）を所持する GE の集合を同一 CCG として定義する．GK を用いて通信に先立つ相手認証を実現する．サブネット内に存在する個々の端末が，そのサブネットとは別の CCG に帰属することもできる．

CCG はグループ管理装置 GMS（Group Management Server）で定義する．GMS から各 GE へは，既存技術による確実な認証と暗号化により，CCG 番号とそれに対応する GK をあらかじめ配送しておく．GK は例えば 1 日に 1 回など，トラヒックの少ない時間帯などを見計らって定期的に更新する．GK が途中で更新されても，通信中のセッションには影響を与えない．DPRP 実行中にたまたま新しい GK が配送された場合は，同一 CCG でも GK が一致しない場合がある．この場合は，GK のバージョン番号を比較し，バージョンの古い GE が GK を取得後，DPRP を再開する．

⋆1 GSCIP（Grouping for Secure Communication for IP，ジースキップ）は，セキュアな CCG を構築するアーキテクチャであり，DPRP は GSCIP を構成する主要なプロトコルである．

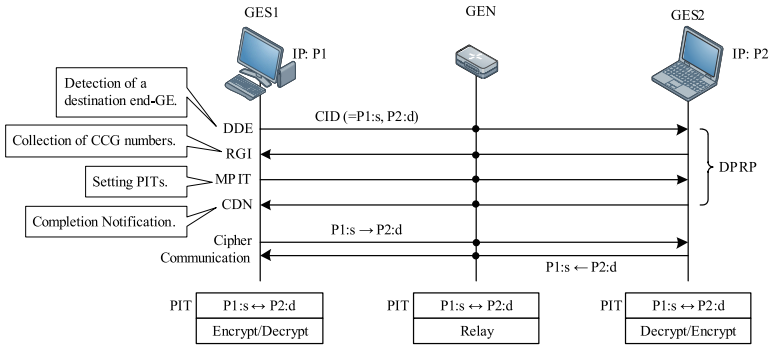

図 2　DPRP ネゴシエーション
Fig. 2　DPRP Negotiation.

DPRP は端末間の通信に先立ち，通信経路上の GE がそれぞれに設定された情報を相互に交換して，各 GE に対応した動作処理情報テーブル PIT（Process Information Table）を IP 層内に動的に生成する．PIT には通信識別子 CID（Connection ID）⋆2に応じたパケットの処理内容（暗号化/復号，透過中継，廃棄）が記述される．

図 2 に DPRP の動作を示す．GES1 と GES2 の間には GEN が存在するものとする．GES1 と GES2 のプライベート IP アドレスはそれぞれ $P1$，$P2$ とする．GES1 はカーネルにおいて，TCP 及び UDP の全ての通信パケットの送信時に，IP 層内に生成した PIT を検索し，その内容に従ってパケットの暗号化などの処理を行う．該当する PIT が存在しない場合は，上記送信パケットを一時的にカーネル（IP 層）内に待避し，DPRP を開始する．DPRP は ICMP 上で定義された以下の制御パケットからなる．

DDE（Detect Destination End-GE）　これから通信を開始する通信パケットの CID を通知し，通信経路上の終端 GE を探索する．

RGI（Report GE Information）　GEN を含む通信経路上の各 GE に設定されている

⋆2 送信元および宛先 IP アドレス/ポート番号のペアとプロトコル番号の組．本論文ではプロトコル番号（TCP/UDP の区別）の表記は省略する．

CCG 番号を収集する．また RGI には DDE と同じ CID が記載されており，各 GE は RGI を送信/転送する際に PIT を仮生成しておく．

MPIT（Make Process Information Table） GES1 は，収集した情報から各 GE の動作処理情報を決定し，MPIT に格納して GES2 へ送信する．MPIT を受信した GEN，GES2 は自身に関する動作処理情報を取り出し，PIT に仮登録する．

CDN（Complete DPRP Negotiation） GES2 は PIT 確定後 CDN を生成し，DPRP の終了を GES1 へ通知する．GEN と GES1 は CDN を受信すると，PIT を確定する．

生成された各 GE の PIT の内容は図 2 に示すとおりである．PIT の検索キーは通信パケットの CID である．ここで，IP アドレスとポート番号のペアがそれぞれ $P1:s$ と $P2:d$ であるとき，これを “$P1:s \leftrightarrow P2:d$” のように表記する．ここで “$s$” と “$d$” はアプリケーションが使用するポート番号であり，“↔” は通信を意味している．図 2 では GES1 と GES2 が同一の CCG であることがグループ鍵 GK により確認できた場合を示しており，処理内容は GES1，GES2 が暗号化/復号，GEN が透過中継となっている．暗号化範囲は，適用するプロトコルに従う．本論文では，ここに PCCOM（Practical Cipher COMmunication）[11] を使用することを想定する．GES1 は PIT を生成後，待避していた通信パケットを元に戻して通信を開始する．以後の通信パケットは全てここで生成された PIT に従って処理される．なお，PIT は無通信状態が続くと消去される．

CCG の定義は IP アドレスと独立しているため，ホストが移動して IP アドレスが変化した場合でも，DPRP により動的に PIT が生成される．管理者は CCG を再定義する必要がなく，管理負荷が大幅に軽減される[2]．DPRP は通信経路上に一般のルータがあったり，エンド端末が一般端末であってもかまわない．エンド端末が一般端末の場合は，その上流に位置する GE が当該端末に代行して DPRP を実行することができる．

このように DPRP はパケットの CID がエンドエンドで変わらないことを前提にすれば，正しく PIT を生成することができる．しかし，通信経路上に NAT が介在すると通信パケットの CID が変更されるため，このままでは正しい PIT を生成できない．

なお，本論文で想定する暗号化通信プロトコル PCCOM は，NAT と共存できるという特長を持っており，本論文が目的とする NAT を介した CCG の構築に適している．

2.2　NAT-f

NAT-f（NAT-free protocol）は，外部端末と NAT ルータに，NAT-f 機能を実装して NAT 越え通信を実現するプロトコルである．位置付けとしては，DPRP と同様に IP 層に対応する．以下の説明では一般的なケースとして NAT ルータの外側をグローバルアドレス

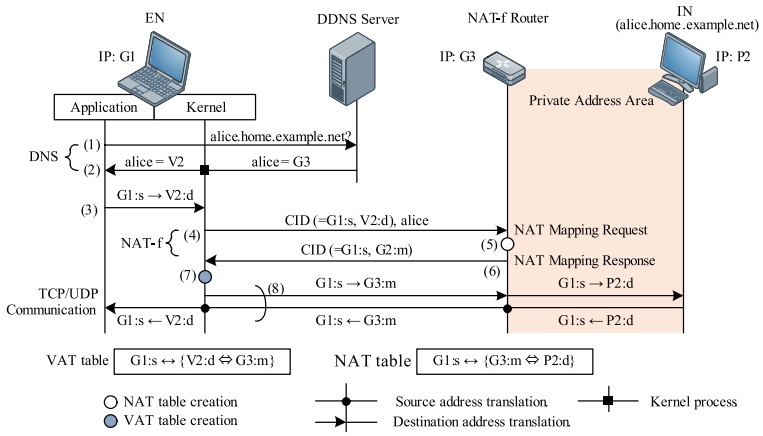

図 3　NAT-f の動作
Fig. 3　Behavior of NAT-f.

（以下 GA）空間，NAT の内側をプライベートアドレス（以下 PA）空間であるものとして説明する．本論文における NAT とは，ポート番号の変換も行う NAPT（Network Address Port Translation）を含むものとする．

図 3 に NAT-f の動作を示す．NAT-f 機能を実装したルータを NAT-f ルータと呼び，NAT-f ルータの外部および内部ネットワークに存在する端末をそれぞれ EN（External Node），IN（Internal Node）と呼ぶ．EN と NAT-f ルータはグローバル IP アドレス $G1$，$G3$ が，IN はプライベート IP アドレス $P2$ が割り当てられているものとする．DDNS（Dynamic DNS）サーバには，IN の FQDN（Fully Qualified Domain Name）“*alice.home.example.net*” と，NAT-f ルータの IP アドレス $G3$ を関連づけて登録しておく．また，NAT-f ルータには，IN のホスト名 “*alice*” と IP アドレス $P2$ を関連づけて登録しておく．

(1) EN は IN と通信を開始するために，IN の名前解決を行い，DDNS サーバから NAT-f ルータのグローバル IP アドレス $G3$ を取得する．一般には，EN のプライマリ DNS サーバが反復的問い合わせにより $G3$ を取得するが，図 3 ではこの部分を省略して記述している．

(2) EN は $G3$ を取得すると，カーネル（IP 層）において DNS 応答メッセージ内に記載されている IP アドレス $G3$ を仮想 IP アドレス $V2$ に書き換えて上位層に渡す．仮想 IP アドレスは NAT-f ルータの内側に存在する IN が複数ある場合，これらを区別

するために用いる仮想的な IP アドレスである．

(3) EN の上位アプリケーションから仮想 IP アドレス $V2$ 宛にパケットが送信されると，EN は上記パケットをカーネル内に一時的に待避する．

(4) EN のカーネルは，NAT-f ルータとの間で NAT-f ネゴシエーションを開始する．NAT マッピング生成要求パケットには，NAT-f ネゴシエーションのトリガとなったパケットの CID とホスト名が記載される．

(5) NAT-f ルータは上記パケットを受信すると，通知されたホスト名 “*alice*” を検索キーとしてプライベート IP アドレス $P2$ を取得し，受信した CID と合わせて下記のような NAT テーブルを生成する．

$$G1 : s \leftrightarrow \{G3 : m \Leftrightarrow P2 : d\} \quad (1)$$

ここで，“↔” は通信を，“⇔” はアドレス/ポート番号変換を示しており，*alice* のポート番号 d に対して NAT-f ルータのポート番号 m がマッピングされたことを意味している．

(6) NAT-f ルータはマッピングされた情報 “$G2 : m$” を受信した CID に反映させ，これを NAT マッピング応答パケットに記載して EN に返信する．

(7) EN は応答パケットを受信すると，仮想 IP アドレスと NAT-f ルータでマッピングされた IP アドレス及びポート番号の対応関係を記録した，以下のような仮想アドレス変換テーブル（VAT: Virtual Address Translation table）を IP 層に生成する．

$$G1 : s \leftrightarrow \{V2 : d \Leftrightarrow G3 : m\} \quad (2)$$

(8) VAT 生成後は，EN と IN 間のすべての通信パケットに対して VAT と NAT によるアドレス/ポート変換が行われ，EN からの通信開始が可能となる．

NAT-f は，パケットの CID が変化していくことに対応したアドレス/ポート変換テーブルを生成するプロトコルである．通信開始時のネゴシエーションは EN と NAT-f ルータの間で実行し，IN はこのネゴシエーションに関与しない．NAT-f は，NAT 配下のネットワーク構成が外部から隠蔽されるという NAT の特性を活かしたまま，NAT 越えを実現している．

3. 提 案 方 式

本章では提案方式の動作について述べる．提案方式では，PA 空間側から通信を開始する場合と，GA 空間側から通信を開始する場合で生成されるテーブルが異なる．これは，後者においては NAT 越え問題の解決に係る処理が必要なためである．

3.1 要求仕様と課題

DPRP は CCG を構築するために考え出されたプロトコルであり，CCG メンバ間の確実な認証と自由な通信を実現することができる．IP 層に実装するため，既存のアプリケーションには一切影響を与えない．CCG の定義は IP アドレスと独立しているため，ネットワーク構成が変化しても CCG の再定義が不要である．また，プロトコルをカーネルにて実現しているため，認証に係るネゴシエーション時間が極めて短いという特長がある．

NAT を跨る CCG を構築するために，新たに以下のような要求仕様と，これを可能とするための課題が発生する．

課題 1　NAT によるアドレス変換に対応した PIT を生成できなければならない．DPRP の制御メッセージの中には，CID など PIT を生成するための情報が含まれている．NAT により通信パケットの CID が変更されるため，そのままでは PIT の内容と実際のパケットの CID が食い違うことになる．そのため，正しい PIT が生成できるように制御メッセージの内容を見直す必要がある．

課題 2　CCG メンバ間では NAT 越え問題のような通信の制約があってはならない．NAT が存在すると，外部端末から内部端末に向けた通信の開始ができない．従ってこのままでは DPRP 自体の開始もできない．まず DPRP の NAT 越えを実現し，かつ DPRP シーケンスの流れの中で，通信パケットに対応したアドレス/ポート変換テーブルを生成する必要がある．

課題 3　内部ネットワークのアドレスを隠蔽するという NAT の特長をそのまま活かせることが望ましい．NAT-f は内部ネットワークのアドレスを隠蔽したまま NAT 越え問題を解決できる．従って NAT-f の原理をそのまま適用することにより，この課題を解決できる．

課題 4　NAT が多段構成であっても CCG を構築したい．NAT が多段構成になる場合は，内部ネットワークが多重に隠蔽されることになる．このような場合でも，NAT-f ルータへの設定や，通信プロトコルが複雑にならないような配慮が必要である．

課題 5　NAT が介在してもネゴシエーション時間が大きく増加してはいけない．実装に当たっては，既存の DPRP の高速性を活かすことと，既存の NAT ルータの機能など動作が保証されたモジュールをできるだけ流用することを考慮した工夫が必要である．

3.2 初期設定と APIT

拡張 DPRP では，GA 空間と PA 空間との境界に GNAT（GE with NAT）を配置する．GNAT は GEN に NAT-f に係る機能を追加した装置と考えることができる．以後の図に

おいて，通信開始端末を GES1 として左側に，相手側端末を GES2 として右側に記述する．IP アドレスは，左側端末を*1，右側端末を*2，NAT のアドレスを*3，*4 として統一する．ここで，*は P または G で，P はプライベートアドレスを，G はグローバルアドレスを示す．DDNS サーバには，GES2 の FQDN“*alice.home.example.net*” と GNAT の外側アドレス $G3$ を登録し，GNAT には GES2 のホスト名 “*alice*” とプライベート IP アドレス $P2$ を関連づけて登録しておく．GES1 と GES2 は同じ CCG として定義されており，同一のグループ鍵 GK を保持しているものとする．

拡張 DPRP により生成される PIT を以後 APIT（Adapted PIT）と呼ぶ．APIT の検索キーは，通信相手の見え方によって GE ごとに異なる．プライベートアドレス端末はグローバルアドレス端末が直接通信相手に見えるため，アドレス部分に着目するとエンド端末どうしを検索キーとした APIT を生成する．一方，グローバルアドレス端末は通信相手が GNAT に見えるため，自らのアドレスと GNAT を検索キーとした APIT を生成する必要がある．GNAT については APIT を GA 空間側で作る方法と PA 空間側で作る方法がある．ここでは，既存の NAT 機能をできるだけ流用することを考え，APIT は GA 空間側で生成することとする．すなわち，GNAT はグローバルアドレス端末と同じアドレスを検索キーとした APIT を生成する．

3.3　PA 空間から GA 空間への通信開始

PA 空間から GA 空間へ通信を開始する場合の拡張 DPRP の動作を**図 4** に示す．この動作により，3.1 節課題 1 を解決することができる．GES1 は通信に先立ち，DDE を GES2 に送信する．GNAT はこれを受信すると，DDE に記述された CID（$P1:s, G2:d$）を用いて TCP/UDP 通信用の NAT テーブル

$$\{P1:s \Leftrightarrow G3:m\} \leftrightarrow G2:d \tag{3}$$

を生成する．DDE 自体は ICMP であるため，ICMP に対応した NAT テーブルも生成されるが，これは通常の NAT の原理で別途生成されるため，説明を省略する．GNAT は DDE に記載された CID に，マッピングされた情報 “$G3:m$” を反映させて GES2 に中継する．

GES2 は DDE に記述された CID を検索キーとした APIT を仮生成後，RGI を GNAT 宛に返信する．GNAT は RGI に記載された CID により APIT を生成後，RGI の宛先を $P1$ に変換して GES1 に転送する．以後に続く MPIT と CDN の処理は通常の DPRP と同様である．この結果，各 GE に生成される APIT の内容は図 4 に示したとおりとなる．

以後の通信パケットは APIT の内容に従って処理される．GNAT では，GES1 からの通信パケット受信時は，NAT テーブルによるアドレス変換後 APIT による処理を，GES2 からの通信パケット受信時は，APIT での処理を行った後 NAT テーブルによるアドレス変換を行う．

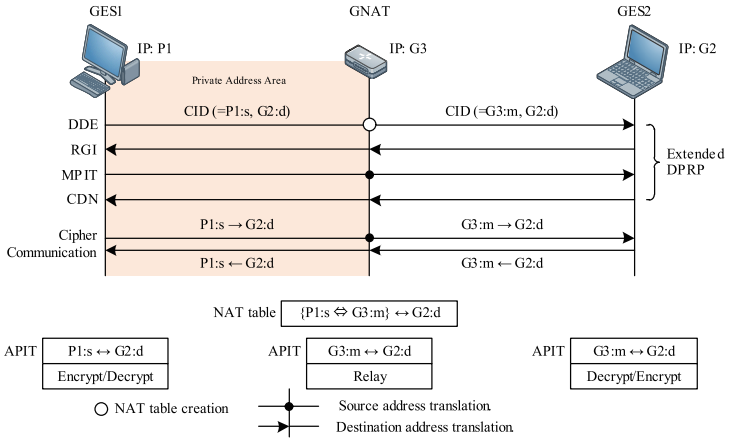

図 4　拡張 DPRP の動作（PA 空間から GA 空間）
Fig. 4　Extended DPRP negotiation (from PA area to GA area).

3.4　GA 空間から PA 空間への通信開始

図 5 に GA 空間から PA 空間へ通信を開始する場合の拡張 DPRP の動作を示す．この動作により，3.1 節課題 1〜3 を解決することができる．GA 空間からの通信開始は NAT 越えを実現する必要がある．GES1 はまず GES2 の FQDN（*alice.home.example.net*）を用いて DDNS サーバに名前解決を依頼する．DDNS サーバは該当する IP アドレスとして GNAT のグローバル IP アドレス $G3$ を応答する．GES1 はこの応答を受信すると，カーネルにて DNS 応答メッセージ内に記載されている IP アドレス $G3$ を仮想 IP アドレス $V2$ に書き換え，上位アプリケーションに通知する．その後，上位アプリケーションから $V2$ 宛に最初の通信パケットが送信されると，カーネルにおいて上記パケットを待避して，拡張 DPRP を開始する．ここまでの処理は NAT-f の動作をそのまま踏襲している．

以後のシーケンスは DPRP が基本であるが，パケット内に拡張 DPRP を実現するための情報が追加される．DDE の宛先は，GNAT の IP アドレス $G3$ とする．DDE の内容にはトリガとなった通信パケットの CID の他に，宛先ホスト名 “*alice*” を追加する．GNAT は DDE を受信すると，宛先 $G1$ と CID に記載されている $V2$ を，*alice* の IP アドレス $P2$ に変換して中継する．GES2 は DDE を受信すると，APIT を生成してから RGI を GES2

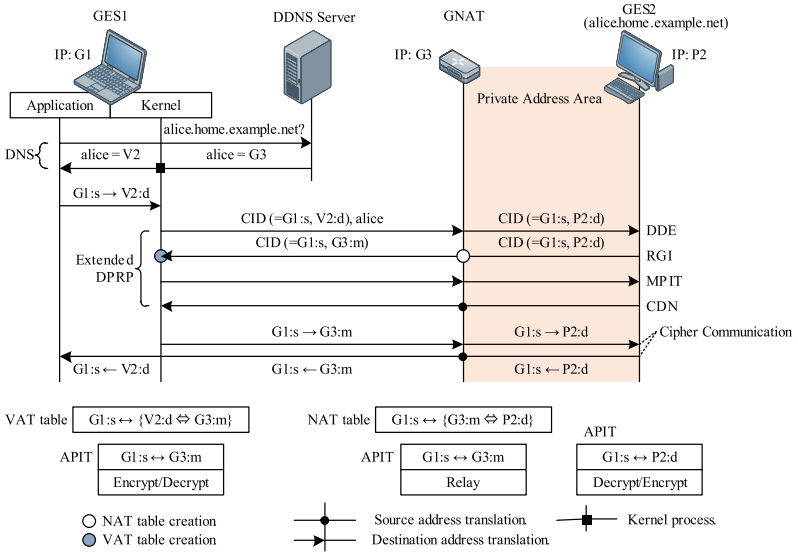

図 5　拡張 DPRP の動作（GA 空間から PA 空間）
Fig. 5　Extended DPRP negotiation (from GA area to PA area).

宛に返信する．

GNAT は RGI を受信すると，記載されている CID から TCP/UDP 通信用の NAT テーブルを以下のように生成する．

$$G1 : s \leftrightarrow \{G3 : m \Leftrightarrow P2 : d\} \tag{4}$$

GNAT は RGI に記載されている CID をマッピングされた情報 “$G3 : m$” に変更してから GES1 へ転送する．

GES1 はこれを受信すると，GES2 に対応づけられた仮想 IP アドレス/ポート番号 $V2 : d$ と，GNAT でマッピングされた IP アドレス/ポート番号 $G3 : m$ の関係が記された VAT テーブルを生成する．

$$G1 : s \leftrightarrow \{V2 : d \Leftrightarrow G3 : m\} \tag{5}$$

MPIT，CDN の処理は CID の扱いを除き，従来の DPRP と同様である．

以後の通信パケットは APIT の内容に従って処理される．GES1 では，通信パケット送信時は，VAT テーブルによるアドレス変換後 APIT による処理を，通信パケット受信時は，APIT による処理後 VAT テーブルによるアドレス変換を行う．

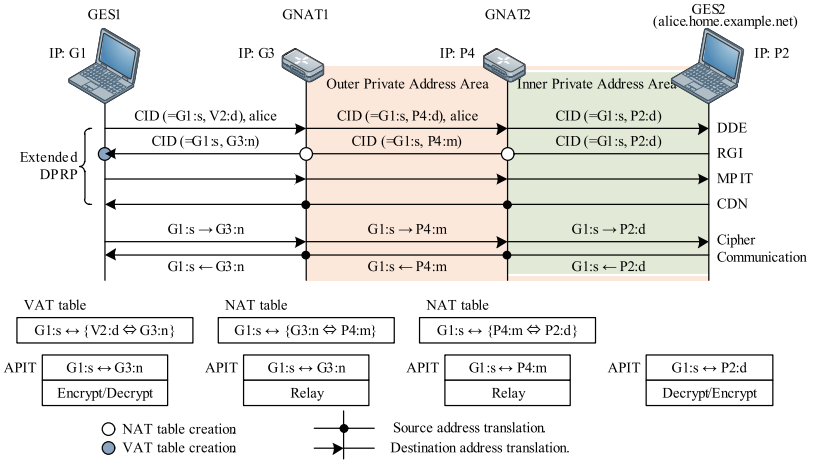

図 6　多段 NAT における拡張 DPRP の動作
Fig. 6　Multistage NAT (from GA area to PA area).

3.5　多段 NAT の動作

NAT が多段構成になっていても拡張 DPRP は有効である．ただし，NAT はすべて拡張 DPRP に対応した GNAT である必要がある．GNAT の動作は，登録内容の違いを除きこれまでの説明と同様である．

図 6 に，多段 NAT 環境において GA 空間から PA 空間へ通信を開始する場合の動作を示す．この動作により，3.1 節課題 4 を解決することができる．DDNS サーバへの問い合わせ部分については，図 5 と同様であるため記述を省略している．GNAT2 には 3.4 節と同様に，配下の PA 空間に存在する GES2 の名前 “*alice*” とそのプライベート IP アドレス $P2$ の対応関係が登録されている．一方，GNAT2 の上流に当たる GNAT1 には，GES2 の名前 “*alice*” と GNAT2 の外側プライベート IP アドレス $P4$ の関係が登録されている必要がある．

GES1 は名前解決後，DDE を GNAT1 宛に送信する．GNAT1 では通知されたホスト名 “*alice*” から GNAT2 の IP アドレス $P4$ を取得し，GNAT2 宛に DDE を転送する．GNAT2 では同様にホスト名から該当する IP アドレス $P2$ を取得し，GES2 に転送する．GES2 は DDE に記載されている CID をもとに APIT を生成し，RGI を返信する．RGI を受信した GNAT2 は NAT テーブルを生成し，マッピングされた情報 “$P4 : m$” を RGI の CID

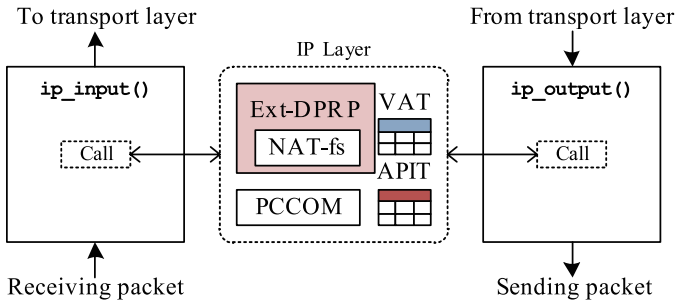

図 7　GES のモジュール構成
Fig. 7　Implementation of GES.

に反映して転送する．GNAT1 でも同様に NAT テーブルを生成し，マッピングされた情報 “$G3 : n$” を RGI の CID に反映して GES1 に中継する．

以後の処理は 3.3 節に示す動作と同様である．生成される APIT は図 6 のとおりである．以上のようにして，多段の NAT 越えを実現するとともに，多段 NAT を跨る CCG の構築が実現できる．

4. 実装と評価

拡張 DPRP を FreeBSD 7.0-RELEASE の IP 層に実装したので，その内容を示す．機能的には，NAT-f と融合しても従来の DPRP が果たした役割をそのまま継承できる．

4.1 拡張 DPRP のモジュール構成

図 7 に GES のモジュール構成を示す．既存の DPRP と NAT-f はそれぞれ独立したモジュールであるが，いずれも IP 層の入出力関数 `ip_input()`，`ip_output()` から呼び出される構造である点が共通している．DPRP の機能拡張が目的であるため，DPRP モジュールを基本とし，NAT-f の機能を NAT-fs モジュールとして追加実装することとした．NAT-fs モジュールは拡張 DPRP で取得した NAT のマッピング情報から VAT テーブルを生成し，通信パケットのアドレス/ポート番号変換を行う．このとき，暗号化が必要であれば，PCCOM モジュールを呼び出す．

図 8 に GNAT のモジュール構成を示す．基本的な構成は GES と同様であるが，通信パケットは上位アプリケーションに渡されるのでなく，中継される点が異なる．GNAT には VAT テーブルが存在せず，代わりに NAT テーブルがある．NAT-fn モジュールは，拡張 DPRP で取得した情報をもとに，`natd` と共同で NAT テーブルを生成する．`natd` とは，ユーザランドで動作する FreeBSD に標準搭載されている NAT デーモンである．GNAT が受信したパケットは divert ソケットを通じて `natd` に渡され，アドレス変換処理を行った後カーネルへ戻される．NAT テーブルの生成は以下に述べる疑似パケットと呼ぶ仮想のパケットを用いて実装した．

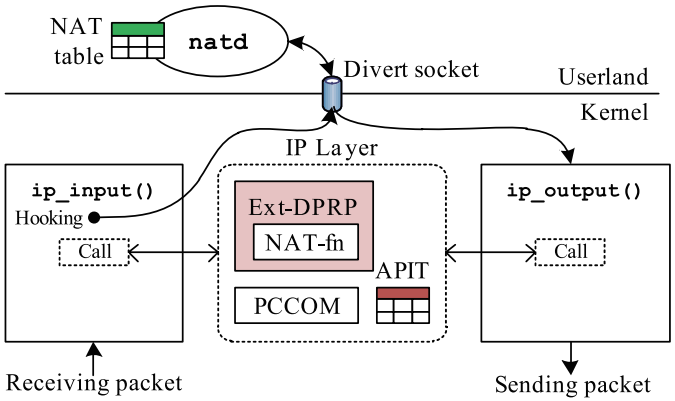

図 8　GNAT のモジュール構成
Fig. 8　Implementation of GNAT.

図 9 に疑似パケットによる NAT テーブルの生成方法を示す．GNAT は内部 GE からの制御パケット（図 4 における DDE，または図 5 における RGI）を受信すると，メッセージ内の CID から疑似パケットを作成する．疑似パケットとは，内部 GE から外部の通信相手へ通信パケットが送信されたように見せかけたものであり，図 4 では送信元が $P1 : s$ で宛先が $G2 : d$ となる．このパケットを `ip_input()` へ渡すと，ファイアウォール `ipfw` によりフッキングされ，divert ソケット経由で `natd` に渡される．`natd` は通常の手段により送信元を $P1 : s$ から $G3 : m$ にマッピングし，NAT テーブル生成処理を行う．疑似パケットは実際のネットワークには送信されず，カーネルの NAT-fn モジュールにおいてマッピングされた情報から DDE または RGI が生成された後に破棄される．この手法により，`natd` にすべての NAT 処理を任せることができる．

4.2 性能評価

NAT 越え処理が必要となる図 5 のシステム構成を想定し，GES1 から GES2 へ FTP 接続を行った場合における提案システムの性能測定を行った．性能測定に使用した GES1,

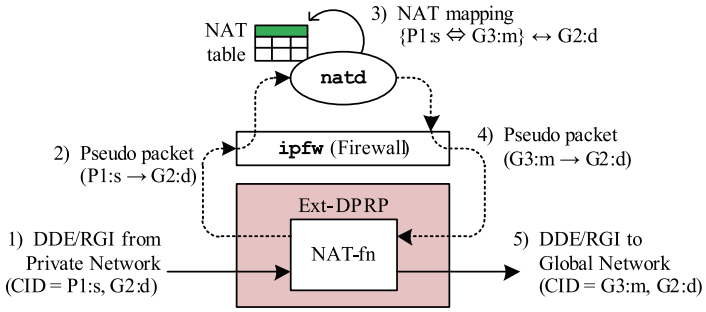

図 9　疑似パケットによる NAT テーブルの生成方法
Fig. 9　NAT mapping method with pseudo packet.

表 1　実験装置の仕様
Table 1　Specifications of devices.

項目	内容
CPU	Pentium4 3.0GHz
Memory	512MB
NIC	100BASE-TX
OS	FreeBSD 7.0-RELEASE

GES2，GNAT，DDNS サーバの仕様は全て同一で，**表 1** の通りである．GNAT は NIC を 2 つ使用し，一方は GES1，DDNS サーバが接続された 100BASE-TX スイッチに，他方は GES2 に直接接続した．

拡張 DPRP のオーバーヘッドを明らかにするため，GES1 と GES2 においてネットワークアナライザ Wireshark によりネットワーク上を流れるパケットをキャプチャした．連続するパケットのキャプチャ時間の差から，さらにネットワーク上を流れるパケットの伝送時間を引くことにより，各装置における拡張 DPRP の処理時間を求めた．試行回数は 10 回で，その平均値を**表 2** に示す．拡張 DPRP はカーネル内に実装されていることから，いずれの処理も極めて高速に実行されていることがわかる．DPRP ネゴシエーション終了後から TCP/UDP パケットを送信するまでの時間は 49.79 μs となったが，その内訳を RDTSC（Read Time Stamp Counter）を用いてさらに詳細に解析したところ，PIT 検索と VAT 検索の合計処理時間が約 1.28 μs，残りの時間は最初のパケットを PCCOM により暗号化するための処理であった．

表 2　拡張 DPRP の処理時間
Table 2　Process time of Extended DPRP.

端末	測定範囲	処理時間
GES1	DNS 応答受信～DDE 送信	20.12 μs
	RGI 受信～MPIT 送信	31.13 μs
	CDN 受信～TCP/UDP 送信	49.79 μs
GNAT	DDE 受信～DDE 転送	18.84 μs
	RGI 受信～RGI 転送	38.39 μs
	MPIT 受信～MPIT 転送	15.34 μs
	CDN 受信～CDN 転送	11.35 μs
GES2	DDE 受信～RGI 送信	28.83 μs
	MPIT 受信～CDN 送信	18.77 μs

図 5 の構成における実際の DPRP ネゴシエーション時間（DNS 応答受信から最初の TCP パケットが送信されるまで）は，上記モジュール処理時間とネットワーク上を流れる DPRP パケット伝送時間の合計値となる．この値は 1,144 μs であった．同様の環境における既存の DPRP ネゴシエーション時間は 1,010 μs であったので[2)]，今回の提案方式により 134 μs（比率にして 12% ）の増加があったことがわかる．既存の DPRP モジュールと拡張 DPRP モジュールの処理時間を比較したところ，GES1 と GNAT のみ処理負荷が増加していた．解析したところ，追加した NAT-fs/NAT-fn モジュールの処理時間および疑似パケットによる NAT テーブルの生成処理が大部分を占めていることがわかった．

いずれにしても，この値は通信開始時のネゴシエーション時間としては極めて小さく，実用上の問題になることはない．以上の評価結果より，3.1 節課題 5 を解決したことを示すことができた．

5. ま と め

DPRP を拡張し，通信経路上に NAT が存在しても閉域通信グループ（CCG）を構築することができる拡張 DPRP を提案した．拡張 DPRP では，PIT の検索キーをネットワーク上を流れるパケットの CID と一致させるような改造を行った．また，NAT 越え問題による制約をなくし，同一 CCG のメンバであれば自由な相互通信を可能とした．これにより，グローバルアドレス空間とプライベートアドレス空間を跨る CCG を定義することが可能となった．

プロトタイプシステムの実装を行い，NAT 環境における動作検証を行った．提案方式の性能評価を行った結果，100BASE-TX のネットワーク環境においては従来の DPRP と遜

色のない性能であることを確認した．今後は異なるプライベートアドレス空間を跨る通信グループの構築も可能となるよう検討を進める予定である．

謝辞　本研究の一部は，日本学術振興会科学研究費補助金（特別研究員奨励費 20・1069）の助成を受けたものである．

参 考 文 献

1) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
2) 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).
3) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, IETF (2003).
4) Rosenberg, J., Mahy, R. and Huitema, C.: Traversal Using Relay NAT (TURN), Internet-draft, IETF (2005). draft-rosenberg-midcom-turn-08.
5) Forum, U.: Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0 (2001).
6) Turanyi, Z., Valko, A. and Campbell, A.: 4+4: An Architecture for Evolving the Internet Address Space Back Toward Transparency, *ACM SIGCOMM Computer Communication Review*, Vol.33, No.5, pp.43–54 (2003).
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 越え通信を実現する 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) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
9) Ng, T., Stoica, I. and H.Zhang: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Proc. USENIX Annual Technical Conference*, pp.319–332 (2001).
10) 宮崎　悠，鈴木秀和，渡邊　晃：端末の改造が不要な NAT 越え通信システム NTSS の提案と評価，情報処理学会論文誌， Vol.51, pp.1234–1241 (2010).
11) 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).

(平成 22 年 11 月 8 日受付)
(平成 23 年 6 月 14 日採録)

後藤　裕司

2006 年名城大学理工学部情報工学科卒業．2009 年同大学大学院理工学研究科情報科学専攻修了．同年株式会社日立情報システムズ入社．中部支社システム本部所属．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情報工学科助教．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．

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．