平成20年度　修 士 論 文

邦文題目

NAT越えが可能な拡張DPRPの検討

英文題目

A Study on Extended Dynamic Process Resolution Protocol that Can Traverse NAT

情報科学専攻

(学籍番号: 073432016)

後藤　裕司

名城大学大学院理工学研究科

内容要旨

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グループを構築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，管理負荷が大きいためこのような目的に適していない．そこで，我々はシステム構成が変化しても通信グループを構築する装置がその変化を学習し，通信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）を提案している．しかし，既存の 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かった．そこで本論文では，NAT を越えて DPRP を実行できる拡張 DPRP について検討した．

拡張 DPRP は FreeBSD 上に実装し，通信経路上に NAT が介在しても通信グループ内のセキュア通信ができることを確認した．評価の結果，100BASE 環境においてはスループットの低下はほとんど見られなかった．また，多段 NAT の環境や異なるプライベートネットワークに存在する端末同士のセキュア通信も可能であることを確認した．

目 次

第1章　はじめに

企業ネットワークでは不正侵入，データの盗聴, 改竄などの脅威に対するセキュリティ対策が課題となっている．組織外部からの脅威に対しては通信の暗号化やディジタル署名など，セキュリティ強度の高い技術が利用されており，ファイアウォール（以下 FW）や IDS（Intrusion Detection System）などと協調するなど，様々な工夫がなされている．しかし，企業ネットワークのセキュリティ脅威はイントラネット内部にも存在しており社員や内部関係者による不正による犯罪が多く報告されている [1]．イントラネット内のセキュリティ対策は，ユーザ名とパスワードによる簡単な相手認証，アクセス制御しかされていないのが現状であり，有効な対策が今後必要になると考えられている．このような状況に対応するために通信グループの構築は有効手段である．

企業では企業統合によるアドレス重複を防ぐためや外部から内部のネットワークを見せないようにしてセキュリティを向上させるなどの理由から，プライベートネットワーク同士の接続においても NAT が導入されている．そのため，企業内ネットワークでも通信経路上に NAT が介在するような環境が増加している．しかし，NAT が介在する場合は外部から内部へ通信開始ができないという問題がある．そこで同一グループ間であれば NAT が介在しても通信が可能な通信グループを構築することは意義のあることだと考える．

通信グループを構築する代表的なネットワークセキュリティ技術として IPsec（Security Architecture for Internet Protocol）[2] がある．IPsec は，IP 層でパケットの暗号化などを行うことによりネットワーク自体のセキュリティを確保することができる．しかし，IPsec を利用するには事前設定項目が多く，端末が増加すると管理負担がかかる．また，IPsec はホスト間の通信を利用されるトランスポートモードと，ネットワーク間通信で利用されるトンネルモードでの互換性がないため，セキュリティドメインが階層的に構築されたり，個人単位の通信グループが混在するような環境では利用することが難しい．

そこで，我々はイントラネット内のセキュリティ対策と管理負荷を低減することができる動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）[3] を提案している．DPRP では，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て動的に動作処理情報を生成する．DPRP は，通信に先立って通信経路上の装置がネゴシエーションを行い，動作処理情報を動的に生成するのでシステム構成が変化しても通信グループの定義を維持することができる．しかし，DPRP は通信経路上に NAT（Network Address Translation）が介在すると利用することができないという課題があった．NAT は企業でも近年使われるようになっており NAT との親和性は今後重要になると考えられる．

NAT 越え問題を解決する技術は様々な方法が提案されている．例えば，インターネット上に外部サーバを設置して NAT 配下の内部ノードとサーバが連携して NAT テーブルを生成する STUN（SimpleTraversal of UDP Through Network Address Translators）[4]，すべてのパケットを外部サーバを中継することで NAT 越え通信を実現する TURN（Traversal Using Relay NAT）[5]，STUN と TURN を組み合わせた ICE（Interactive Connectivity Establishment）[6]，内部ノードと NAT が連携して動的に NAT マッピングを生成する UPnP（Universal Plug and Play）[7]，外部ノードと NAT が連携する NAT-f [8] などがある．

本論文では通信経路上に NAT が介在してもセキュアなグループ通信を行うことができる拡張 DPRP を提案する．拡張 DPRP は DPRP と NAT-f を融合させた技術である．NAT-f は特殊なサーバを利用することなくエンドツーエンドで NAT 越えを実現することができるため，この技術を DPRP に取り入れることにより NAT がある環境においても通信グループの構築を行う．NAT-f は DPRP と同様に IP 層のカーネルに実装されているため容易に組み込みやすいという利点がある．

拡張 DPRP は FreeBSD 上に実装し，通信経路上に NAT が介在しても通信ができることを確認した．評価の結果，100BASE 環境においてはスループットの低下はほとんど見られなかった．また，多段 NAT や異なるプライベートネットワーク環境においても通信ができることを確認した．

以下に 2 章に DPRP と NAT-f について述べ， 3 章で NAT 越えが可能な拡張 DPRP， 4 章で拡張 DPRP の実装， 5 章で性能測定の結果,， 6 章でまとめを述べる．

第2章　DPRPとNAT-f

2.1　DPRP

DPRPでは，サブネット単位とホスト単位の通信グループが混在する環境において柔軟性と安全性を両立することができる．DPRPにおける通信グループに属する端末からのアクセスを拒否することができる．DPRPではDPRPに対応した装置をGEと呼ぶ．ルータタイプのGEN（GE for Network），各端末にインストールされるソフトウェアタイプのGES（GE realized by Software），重要なサーバの直前に設置してGESと同じ役割を果たすブリッジタイプのGEA（GE for Adapter）がある．GENの配下に存在する一般端末Terminal（以下Term）はGENによって一括して保護される．図 2.1にDPRPにおける通信グループの構築方法について示す．DPRPでは同一の暗号鍵を所持するGEの集合を同一グループとして定義する．この暗号鍵をグループ鍵GK（Group Key）と呼ぶ．同一の通信グループのGE間の通信はGKを用いて暗号化される．GEに必要な情報は管理装置GMS（GSCIP Management Server）で定義される．この情報をGE情報と呼び，通信グループ番号と動作モードから構成される．通信グループとグループ鍵GKを1対1に対応づけることによってIPアドレスに依存することなく通信グループを定義することができ，個人単位/ドメイン単位が混在したり1ユーザに対して重複したりする複数の通信グループを定義することができる．また，サブネット内に存在する個々の端末に対して，そのサブネットとは別の通信グループを定義することができる．GMSでは通信グループ

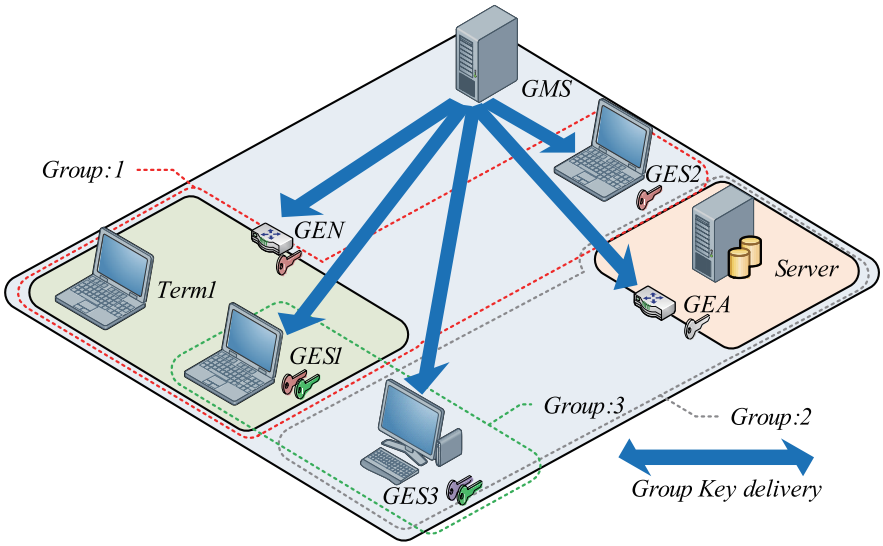

図 2.1　通信グループの定義方法

の定義の他に，グループ鍵 GK の生成，更新処理などを行う．グループ鍵 GK は定義された通信グループに対して生成され，定期的に更新される．この際，GMS と GE 間は公開鍵を用いた確実な認証と暗号化が実行される．GE は自身が保持する動作処理情報テーブル PIT（Process Information Table）に従ってパケットの処理を行う．PIT には送信元/宛先の IP アドレス，ポート番号，プロトコル番号と，パケットの処理内容を示した動作処理情報（暗号化/復号，透過中継，廃棄），およびグループ鍵の番号とバージョンが記述されている．GE は通信開始時にコネクション識別子 CID（Connection Identification：送信元/宛先の IP アドレス，ポート番号，プロトコル番号の組）を用いて PIT の検索を行う．該当する PIT が無い場合は以下に述べる DPRP を実行し PIT の生成を行う．

DPRP は端末間の通信に先立ち，通信経路上の GE に設定されている情報を相互に交換して，各 GE に対応する動作処理情報テーブル PIT を生成する．図 2.2 に DPRP の動作を示す．GES1 は TCP/UPD パケットの送信時に PIT の検索を行い，該当する PIT がない場合は上記の送信パケットを一時的にカーネルに待避し，DPRP を実行して PIT の生成を行う．DPRP は 4 つの ICMP ベースの制御パケット DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）を用いて 2 往復のネゴシエーションを行う．DDE は通信相手に最も近い GE を特定する．DDE には，DPRP のトリガーとなった TCP/UDP パケットの CID（P1:s→ P3:d）がセットされ，通信パケットの宛先へ送信する．DDE を受信した GES2 が始点 GE となり，RGI を生成する．RGI には，GE のユーザ ID，動作モード，グループ鍵情報などの設定情報，および GE を認証するために用いる識別子（以下 aID）がセットされる．RGI は宛先を CID に記載されている送信元 IP アドレス “P1” として送信される．中間 GE が RGI を転送する際，始点 GE と同様に自身の設定情報などを追記する．RGI を受信した GES1 が始点 GE となり，収集した GE 設定情報から動作処理情報を決定する．GES1 は決定した自身に関する動作処理情報から PIT を生成し，その他の動作処理情報を MPIT にセットして始点 GE, すなわち GES2 へ送信する．MPIT を受信した GEN，GES2 は動作処理情報から自身に関する動作処理情報を取り出し，“aID” を用いた認証処理後に PIT を生成する．GES2 は PIT 生成後，DPRP ネゴシエーション完了を通知するために CDN を生成し，始点 GE，すなわち GES1 へ送信する．CDN を受信した GES1 は待避していた通信パケットを元に戻し，生成された PIT に基づいて通信が開始される．

DPRP ネゴシエーション後の通信パケットの暗号化には PCCOM（Practical Cipher COMmunication）[9] と呼ぶ暗号方式を利用している．PCCOM では，暗号化による機密性確保，本人性確認とパケットの完全保証を提供することができる．また，暗号化範囲をユーザデータ部分からにすることにより NAT やファイアウォールとの共存ができ，パケットフォーマットを変えない方式のため高スループットを実現することができる．IP アドレスはとポート番号は NAT で変換されてしまうため完全性保証の範囲には含まれないが，この部分の保証に関しては動作処理情報テーブル PIT の検索過程でその内容を保証することができる．各端末には同様のコネクション情報 CID で PIT が生成される．動作処理

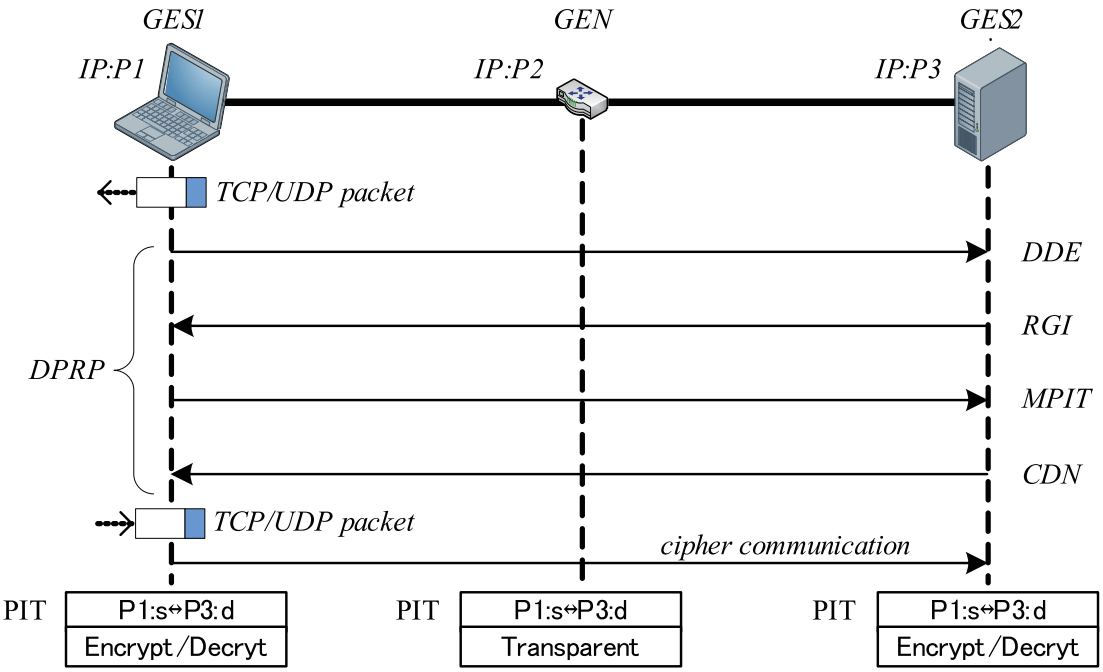

図 2.2　DPRP ネゴシエーション

情報は，GES1，GES2 では暗号化/復号，GEN では透過中継となる．その後，GES1 は待避していたパケットを復帰させ生成した PIT の動作処理情報に従ってパケットを処理し送信する．DPRP はホストやサブネットが移動して IP アドレスが変化した場合にも実行されるため，管理者やユーザは暗号化に必要な設定を更新する必要がない．

現状の DPRP は，通信経路上に NAT が介在するような環境では NAT で IP アドレスが変換されてしまうため利用することができなかった．この課題を解決するためには，NAT の内側から通信が始まる場合，及び NAT の外側から通信が始まる場合の両者について検討する必要がある．いずれの場合においても NAT によりパケットの IP アドレスとポート番号が変換されるため変換後の内容と生成した PIT の内容が一致しないという課題がある．また，NAT の外側から DPRP を開始する場合は，NAT 越え問題を解決する必要がある．DPRP は今後はイントラネット内だけではなく，インターネットとホームネットワークを組み合わせたシステムにも応用範囲を広げていくことを想定している．本稿では，NAT の内側はプライベートアドレス（以下 PA），外側はグローバルアドレス（以下 GA）であるものとして記述する．

2.2　NAT-f

NAT-f はインターネット上の外部ノードと NAT に機能を実装して NAT 越え通信を実現するプロトコルである．通信ノードはグローバルアドレス（以下 GA）とプライベートアドレス（以下 PA）のアドレス空間の違いを意識することなく通信することができ，双方向からの通信を実現することができる．本論文における NAT とは，ポート番号の変換

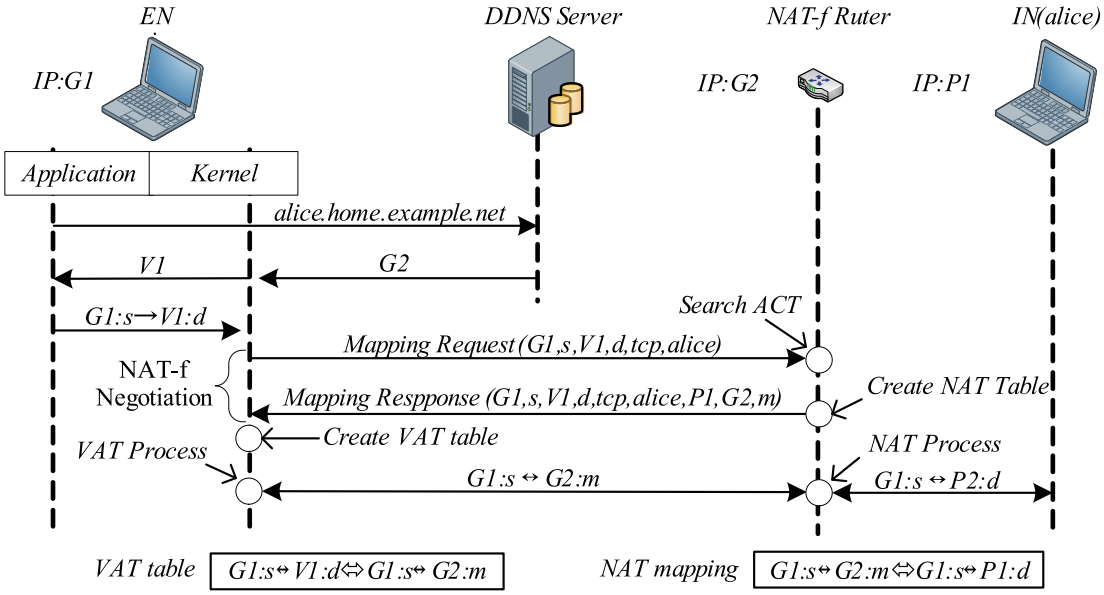

図 2.3　NAT-f の基本動作

も行う NAPT（Network Address Port Translator）[10] を含むものとする．図 2.3 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ノードをそれぞれ EN（External Node），IN（Internal Node）と表記する．DDNS（Dynamic DNS）サーバ [11] には IN の FQDN（Full Qualified Domain Name）と NAT-f ルータのグローバル IP アドレス G2 を関連づけて登録しておく．また，NAT-f ルータには IN との通信を許可するかどうかを示すアクセス制御テーブル ACT（Access Control Table）に IN のホスト名 “alice” と IP アドレス “P1” を関連づけて登録しておく．

EN は IN を通信を行うために DDNS サーバに名前解決を依頼する．DDNS サーバは NAT-f ルータのグローバル IP アドレス “G2” を応答する．EN はこれを受信すると IP 層のカーネルにおいて G2 を仮想アドレス “V1” に書き換えて上位層に渡す．仮想アドレスは NAT-f ルータの配下の IN を区別するために用いる仮想的な IP アドレスである．次に，上位のアプリケーションから仮想アドレス “V1” 宛にパケットが送信される．EN は IP 層でこれを受信すると，受信したパケットを一時的にカーネルに待避して NAT-f ルータにマッピング要求を行う NAT-f ネゴシエーションを開始する．マッピング要求パケットには NAT-f ネゴシエーションのトリガとなったパケットのコネクション識別子（送信元/宛先 IP アドレス・ポート番号，プロトコルタイプの組）と仮想アドレス V1 に対応するホスト名 “alice” が記載されている．NAT-f ルータはこれを受信すると “alice” を検索キーにして ACT の検索を行う．検索を行った結果，該当するホスト名があった場合は，ACT に記載されている “alice” のプライベート IP アドレス “P1” を用いて強制的に NAT テーブルを生成する．

ここで，“m” は NAT-f ルータが動的に割り当てた外側ポート番号である．NAT-f ルータはこの外部ポート “m” を応答パケットに記載し EN に送信する．EN はこれを受信すると，

仮想アドレスと上記ポート番号の対応関係を記録した仮想アドレス変換（VAT：Virtual Address Translation）テーブルを IP 層に生成する．EN から IN への通信パケットは EN の VAT テーブルと NAT-f ルータの NAT テーブルによりパケットの IP アドレスとポート番号を変換することにより IN と通信開始が可能となる．以後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る．

第3章　拡張DPRP

3.1　実現すべき機能

ここでは，通信経路上にNATが介在してもセキュアで自由なアクセスが可能なグループ通信を行うための拡張DPRPに必要となる実現するべき機能を述べる．

NATを介して通信を行う場合，内部から外部への通信は行うことができるが，外部から内部への通信は行うことができない．しかし，グループ通信においてはこの制約をなくし許可した同一グループのメンバであれば外部からの通信を行うことを可能にする．これにより，メンバはアドレス空間の違いを意識することなく同一グループであれば自由にアクセスすることができる．また，企業などではセキュリティ向上などの目的などからNATが多段に構築されている場合なども考えられるため，多段NATや異なるNAT配下のメンバ同士が通信ができるよう拡張を行う．さらに，NAT配下の端末はDPRPの機能を実装せずとも外部の端末とグループ通信をできるようにする．既存のDPRPはDPRPネゴシエーションのトリガとなったTCP/UDPパケットのコネクション情報を用いて各GEに同一のコネクション情報でPITを生成されるため，通信経路上にNATが介在する場合はNATによりIPアドレスとポート番号が変換されてしまう．そのため，生成したPITのコネクション情報と変換後のTCP/UDPパケットのコネクション情報が一致しない．そこで，拡張DPRPではNATで変換後のコネクション情報に一致するようにPITを生成する必要がある．変換後のコネクション情報でPITを生成するためには通信パケットのIPアドレスとポート番号がNATでどのように変換されるかあらかじめ知っておく必要がある．そこで，DPRPネゴシエーション中に実際の通信に必要なNATテーブルを生成し，そのときNATにマッピングされたIPアドレスとポート番を用いてPITを生成を行う．これらのNAT越えの機能を実現するにあたり，通常の通信に比べスループットが落ちない実装を行う．

3.2　システム構成と初期設定

図3.1に拡張DPRPのシステム構成と初期情報について示す．拡張DPRPでは新たにGNATと呼ぶ装置を導入する．GNATはGENにNAT機能を追加した装置である．各GEには拡張DPRPがインストールされており，GES1はGA空間，GES2はPA空間に存在する．GA空間とPA空間との境界にはGNATを配置する．GMSは各GEがアクセスできるようGA空間に設置しておく．ダイナミックDNS（以下DDNS）サーバには，GES2

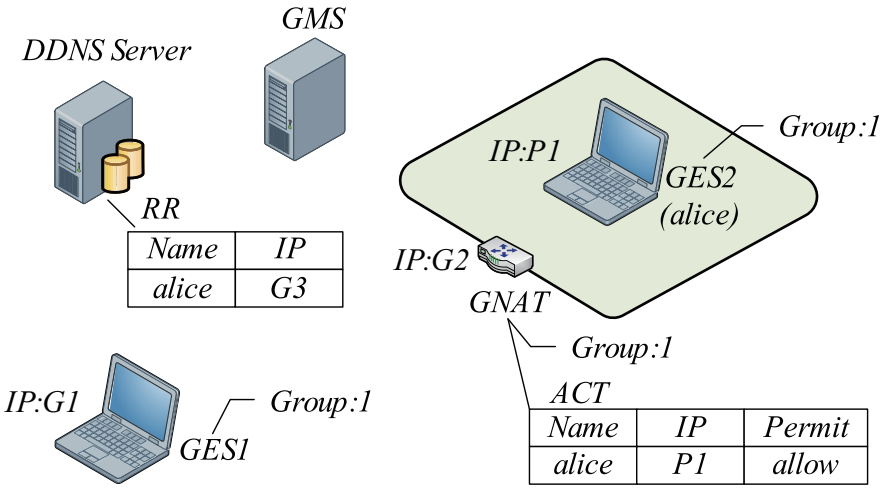

図 3.1　システム構成

の名前解決を行うために必要である．GNAT には配下の GES2 のホスト名 “alice” と IP アドレス “P1” およびアクセスの可否をアクセス制御テーブル ACT に関連づけて登録しておく．GES1 と GNAT の IP アドレスはそれぞれ “G1”，“G2” である．各 GE は同じグループに所属しているものとする．

3.3　PA 空間から GA 空間への通信

GES2 から GES1 へ通信する場合の拡張 DPRP の動作を図 3.2 に示す．GES2 は通常の DPRP と同様に DDE を GES1 に送信する．GNAT はこれを受信すると，DDE に含まれるコネクション識別子 CID（P1:s→G1:d）を用いて NAT テーブル

（P1:s↔G1:d⇔G3:m↔ G1:d）

を生成する．GNAT はこの時 GNAT にマッピングされた IP アドレス “G2” とポート番号 “m” を DDE に追加し，さらに NAT を通過したことを示すフラグをセットして GES1 に送信する．GES1 はこれを受信し，フラグがセットされている場合は RGI の宛先を CID の送信元 IP アドレスではなく DDE の IP ヘッダの送信元 IP アドレス “G2” にして送信する．RGI は GNAT の NAT により IP アドレス変換され GES2 に中継される．GES2 は RGI 受信後，動作処理情報を決定して MPIT を GES1 に送信する．MPIT，CDN の処理は 2 章で述べた内容と同様である．ただし，MPIT で各 GE に生成する PIT の内容は以下に述べるようになる．

3.4　NAT に対応した PIT

通信経路上に NAT が介在する場合は，NAT により通信パケットの IP アドレスとポート番号が変換される．このような場合の PIT は，通信相手の見え方によって GE ごとに異なる内容となる．これを APIT（Adapted PIT）と呼ぶことにする．GES2 は GES1 が通信相

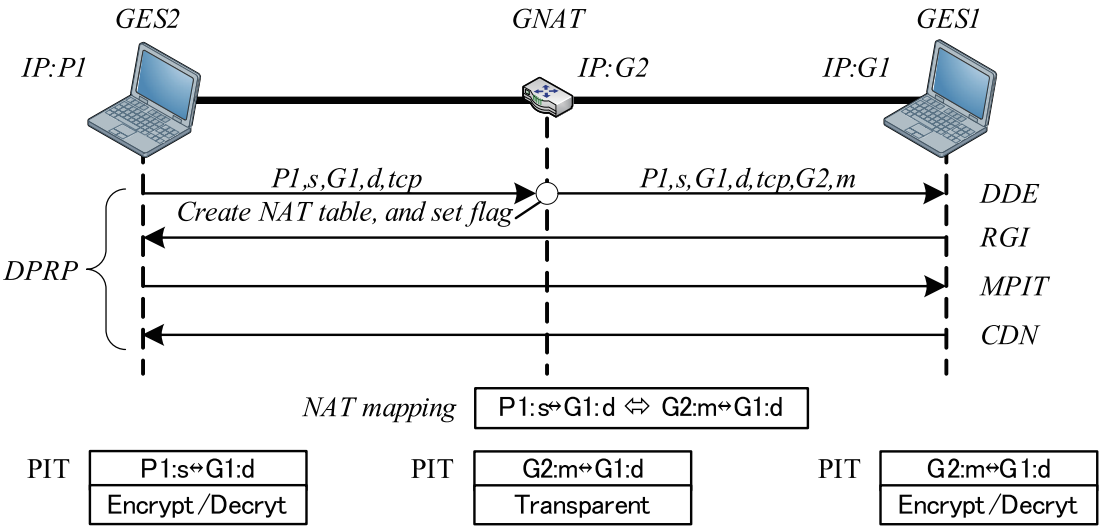

図 3.2　拡張 DPRP の動作（PA から GA）

手に見えるため GES2 と GES1 に対応した PIT となる．GES1 は通信相手が GNAT に見えるため，GES1 と GNAT に対応した PIT となる．GNAT については PIT をグローバルアドレス側で作る方法とプライベートアドレス側で作る方法がある．NAT 処理はアプリケーションに近い部分で実行されるため，グローバルアドレス側，すなわち GES1 と GNAT に対応した PIT を生成することとした．これにより，通信パケットは GNAT の NAT により図 3.2 中の NAT テーブルに従って変換されるが，PIT には変換後のコネクション情報となっているため通信パケットのコネクション情報と一致する．同様に GES1 でも，変換後のコネクション情報で PIT が生成されているため正常な通信を行うことが可能である．

3.5　GA 空間から PA 空間への通信

GES1 は GES2 と通信を開始する際に GES2 の FQDN（alice.home.net.com）を用いて DDNS サーバに名前解決を依頼する．DDNS サーバは該当するレコードとして “G2” を応答する．GES1 はこの応答を受信するとカーネルにおいて GNAT の IP アドレス “G2” と GES2 のホスト名 “alice” を取得する．さらに GNAT の IP アドレス “G2” を仮想 IP アドレス “V1” に書き換え，これらの関係を名前関連テーブル NRT（Name Relation Table）へ保存する．上位ソフトウェアには仮想アドレス “V1” が通知される．そのため，上位ソフトウェアは通信相手を仮想 IP アドレス “V1” と認識する．その後，上位ソフトウェアから GNAT 宛に最初の TCP/UDP 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 ネゴシエーションを開始する．

図 3.3 に拡張 DPRP の動作を示す．まず初めに，DDE パケット生成時に仮想 IP アドレス “V1” を用いて NRT を検索する．ここで，“V1” に該当するホスト名 “alice” と GNAT の IP アドレス “G2” を取得し，DDE パケットを生成する．DDE は既存 DPRP の情報の他にホスト名 “alice” を追加する．その後，DDE パケットの宛先 IP アドレスを “G2” にし

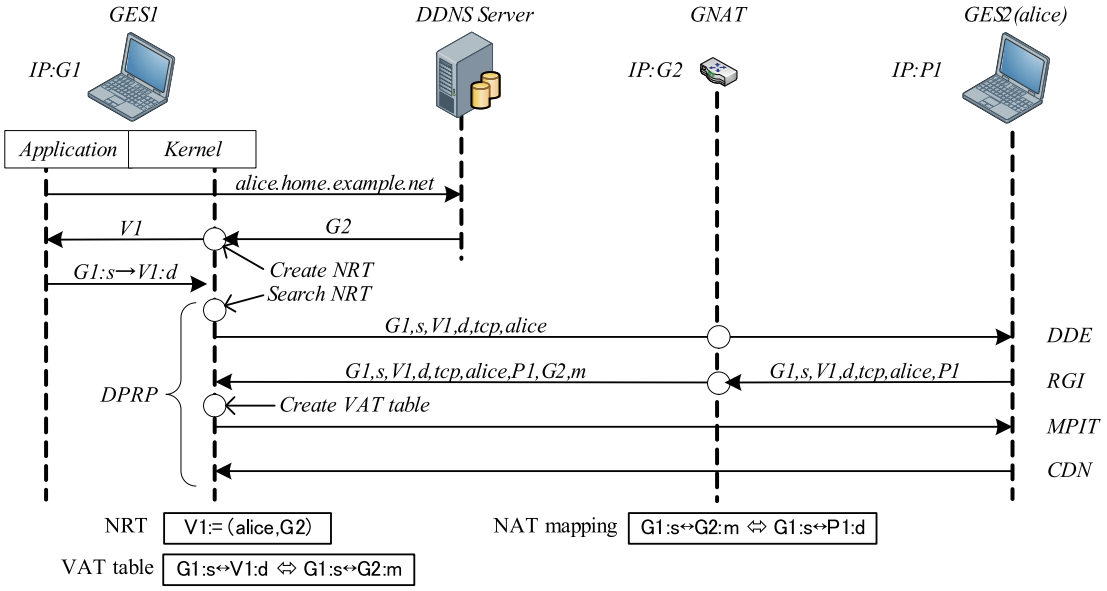

図 3.3　NAT 越え DPRP の動作（GA から PA）

て送信する．GNAT は DDE パケットを受信すると “alice” を検索キーにして ACT の検索を行い通信が許可されているかどうかのチェックを行う．通信が許可されていた場合は，“alice” のプライベート IP アドレス “P1” を取得し，DDE パケットの宛先を “P1” に変更して GES2 に転送する．GES2 は DDE パケットを受信すると RGI パケットに GES2 のプライベート IP アドレス “P1” を追加して GES1 宛に送信する．GNAT は RGI パケットを受信すると，RGI パケットに含まれている CID の情報と GES2 のプライベート IP アドレス “P1” の情報を基に NAT テーブルを動的に生成する．GNAT はこの時 NAT にマッピングされたポート番号 “m” を RGI パケットに追加して GES1 宛に送信する．GES1 はこれを受信すると，RGI パケットに含まれている情報から GES2 に対応づけられた仮想 IP アドレス “V1”，ポート番号 “d” と GNAT の IP アドレス “G2”，ポート番号 “m” の相互変換関係が記されたテーブル VAT（Virtual Address Translation table）を生成する．

MPIT，CDN の処理は 2 章で述べた内容と同様である．GES1 は TCP/UDP 通信パケットを復帰させ，VAT テーブルと NAT テーブルに基づいて宛先 IP アドレスとポート番号を変換する．さらに PIT に基づいてパケットの処理を行う．以後のパケットは全て同様の処理である．

3.6　アドレス変換処理

図 3.4 に通信パケットが VAT と NAT によりアドレス変換されていく様子を示す．GES1 の PIT は VAT で変換後に参照される．GNAT ではパケット受信後まず PIT が参照される．その後，NAT テーブルに従って宛先の IP アドレスとポート番号 “G2:m” を “P1:d” に変換して GES2 に送信する．GES2 ではアドレスの変換処理はなく PIT の参照とその処理だけが実行される．逆方向のパケットは上記と逆の変換を行う．

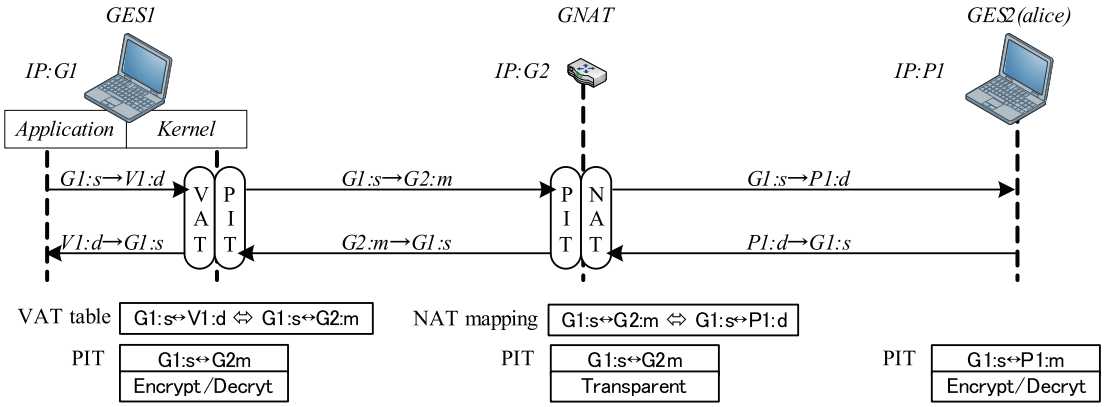

図 3.4　VAT と NAT によるアドレス変換処理

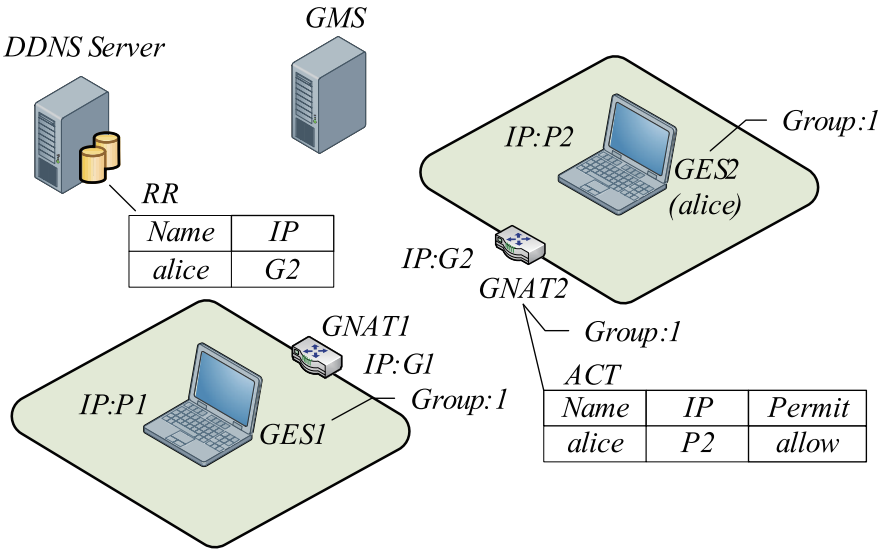

図 3.5　異なる PA 空間:システム構成と初期情報

3.7　異なる PA 空間の端末の通信

DPRP を更に拡張することにより，図 3.5 に示すような異なる PA 空間同士においても DPRP を利用することが可能である．図 3.6 に異なる PA 空間同士の通信を行う場合の動作を示す．GNAT1 の配下に GES1，GNAT2 の配下に GES2 が存在し，それぞれ異なる PA 空間に存在する．

GES1 は GES2 の “alice” と通信を行うために GNAT1 を経由して DDNS サーバに名前解決依頼を行う．DDNS サーバは該当する GNAT2 のアドレス “G2” を GNAT1 に応答する．GNAT1 は，DNS 応答パケットを受信すると，GNAT1 のカーネルにおいて GNAT2 の IP アドレス “G2” を仮想アドレス “V1” に変換する．GES1 が GA 空間に存在する場合は，アドレス変換処理を GES1 が行っていたが，GES1 が PA 空間に存在し，端末が所属している PA 空間を構成する装置が GNAT の場合は，GNAT が VAT アドレス変換処理を行う．GNAT1 は，アドレス変換処理を行った後，NRT テーブルにホスト名と IP アドレスの関係を保存後，GES2 にパケットを送信する．GES2 には DNS 応答として仮想アドレ

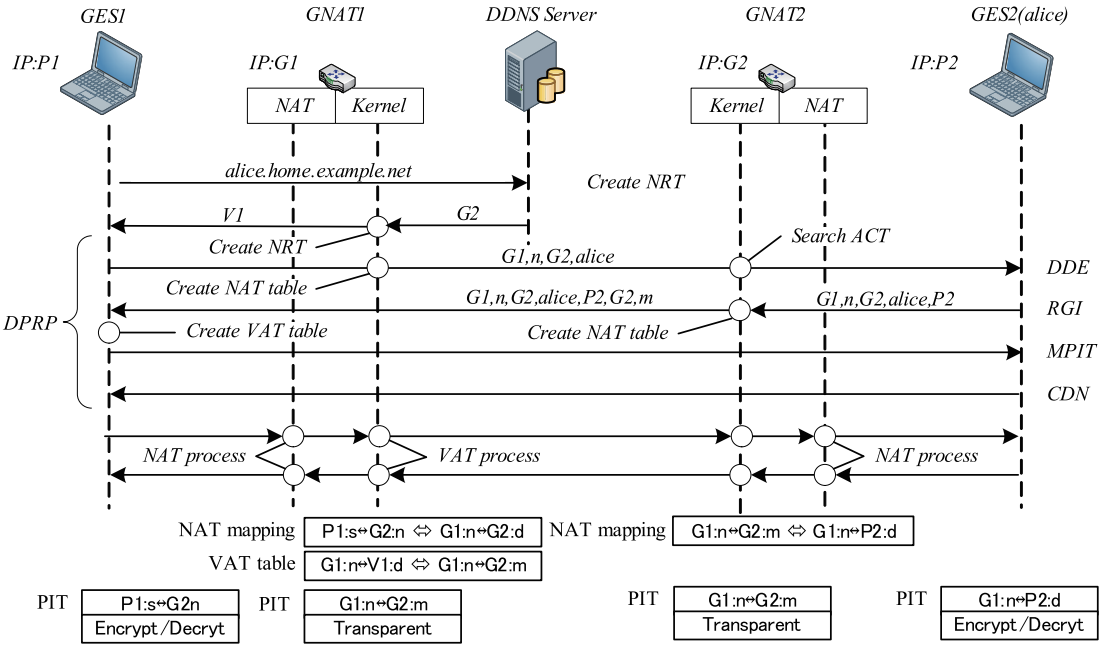

図 3.6　異なる PA 空間同士の通信

ス “V1” が報告されることになる．GES2 の上位ソフトウェアは通信パケットを仮想アドレス “V1” 宛に送信する．GES2 のカーネルはこれを受信すると，通信パケットを待避して DPRP ネゴシエーションを開始する．GES2 は DDE を仮想アドレス宛 “V1” に送信する．GNAT1 はこれを受信すると，仮想アドレス “V1” で NRT テーブルの検索を行い，該当するホスト名 “alice” と GNAT2 の IP アドレス “G2” を取得する．そして，その情報と DDE に含まれている CID の情報から GES2 と GNAT2 に対応する NAT テーブルを作成する．GNAT2 では DDE を受信すると ACT の検索を行い “alice” のプライベート IP アドレス “P2” を取得し GES2 に転送する．GES2 は DDE を受信後，DDE に記載されている CID と取得した “P2” で新たに CID を作り，RGI に追加して送信する．GNAT2 はこれを受信すると，追加された CID の情報を元に NAT テーブルを動的に作成する．GNAT2 は NAT にマッピングされたポート番号 “y” を RGI に追加して GNAT1 に送信する．GNAT1 は RGI を受信したら，ポート番号 “y” と RGI に含まれている仮想アドレスなどの情報から VAT を生成する．MPIT では，各アドレス空間に対応した PIT を各端末に生成する．DPRP ネゴシエーション終了後，GES2 は待避していた通信パケットを仮想アドレス “V1” 宛に送信する．GNAT1 はこれを受信すると，NAT によりアドレス変換を行った後に VAT 処理を行うことにより通信パケットを GNAT2 に送信することが出来る．以後の通信は 3 と同様である．

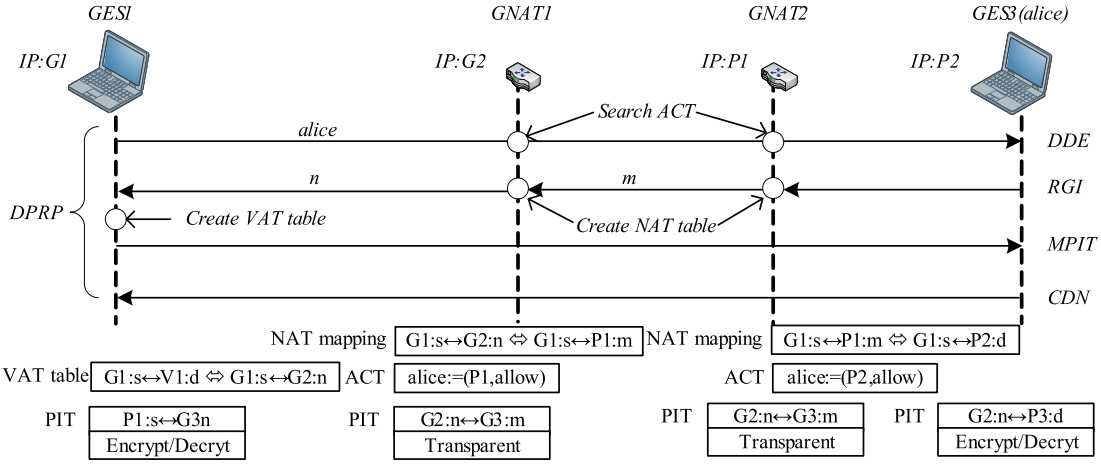

図 3.7　多段 NAT：GA 空間から PA 空間の場合

3.8　多段 NAT

3.8.1　多段 NAT の動作

拡張 DPRP は次の条件の場合に，多段 NAT 環境下においても利用可能である．多段 NAT の内側から外側へ通信を行う場合は一番外側にある NAT また，通信経路上のすべての NAT がが DPRP に対応していれば，3.3 節で説明した拡張 DPRP の動作で利用可能である．多段 NAT の外側から内部に通信を行う場合，通信相手までの経路上の全ての NAT 装置が DPRP 対応（GNAT）でなくてはならない．拡張 DPRP では外部からの通信に対して ACT を用いてアクセス制御を行っているため，一般 NAT 装置が通信経路上にある場合は外部からの通信を内部に通すことができない．

図 3.7 に多段 NAT 環境で GA 空間から PA 空間へ通信を開始する場合の動作を示す．GNAT1 の ACT には GNAT2 の外側の IP アドレス “P2” を登録する必要がある．GES1 は名前解決後，DDE を GNAT1 宛に送信する．GNAT1 では，“alice” で検索を行い GNAT2 の IP アドレス “P1” を取得し，GNAT2 宛に DDE を転送する．GNAT2 では，同様に検索を行い “alice” のプライベート IP アドレス “P2” を取得し，DDE を GES2 に転送する．RGI では GNAT2 で NAT にマッピングを行い，マッピングされたポート番号 “m” を RGI に追加して GNAT1 に送信する．GNAT1 では，ポート番号 “m” を用いて NAT にマッピングを行い，マッピングされたポート番号 “n” を RGI に追加して GES1 に送信する．以後の処理は 3.3 節に示す動作と同様である．

第4章　拡張DPRPの実装

4.1　拡張DPRPのモジュール構成

拡張 DPRP は既存の DPRP モジュールと NAT-f モジュールを追加し FreeBSD7.0 上の IP 層に実装した．

図 4.1 に GES のモジュール構成を示す．DPRP と NAT-f はいずれも IP 層の入出力関数 $ip\_input()$，$ip\_output()$ から呼び出される構造となっている．GES には DPRP のモジュールに NAT-f のモジュールである VAT と NRT モジュールを追加した．制御パケットモジュールは新たに追加するホスト名やコネクション情報 CID に対応できるよう処理の追加を行った．また，アドレス空間ごとに異なる PIT を生成するために制御パケットに記載する CID をアドレス空間ごとに区別できる仕組みの追加を行った．制御パケットモジュールは各制御パケットの処理を行い，PIT，VAT の生成を行う．NRT モジュールは仮想 IP アドレスと実アドレスを関連づけるテーブルを生成し，DDE 送信時には NRT を検索することにより仮想 IP アドレスに対応するホスト名を取得することができる．VAT モジュールは DPRP ネゴシエーションで取得した NAT のマッピング情報から仮想 IP アドレスを NAT にマッピングされた IP アドレスとポート番号に変換するテーブルを作成する．また，データパケットの送受信時に呼び出され検索とアドレス変換の処理を行う．各制御パケットの暗号化とデータパケットの暗号化には PCCOM の暗号化モジュールを使用する．PIT，NRT，VAT のテーブルはカーネル空間に作成して，不要となったら削除する．

図 4.2 に GNAT のモジュール構成を示す．GNAT には，DPRP モジュールに NAT-f モジュールである VAT，NRT，ACT モジュールと擬似パケットモジュールを追加した．ACT モジュールは，DDE 受信時に呼び出されホスト名から対応する IP アドレスを取得することができる．さらに FreeBSD 標準の NAT デーモン natd を動作させる．擬似パケットモジュールは，DDE または RGI パケットを受信時に NAT テーブル作成のため呼び出され擬似パケットの作成を行う．NAT テーブルの作成方法については 4.2 節で述べる．GES と同様にカーネル空間内に PIT と ACT を生成する．GNAT が受信したパケットは divert ソケットを通じて natd で NAT のアドレス変換処理が行われる．natd は改造を必要とせず，そのまま利用することができる．GNAT では DPRP モジュールはグローバル側のインタフェースから呼び出される．よって，プライベート側のインターフェイスで受信した場合は，NAT 処理後に DPRP モジュールが呼び出されることになる．

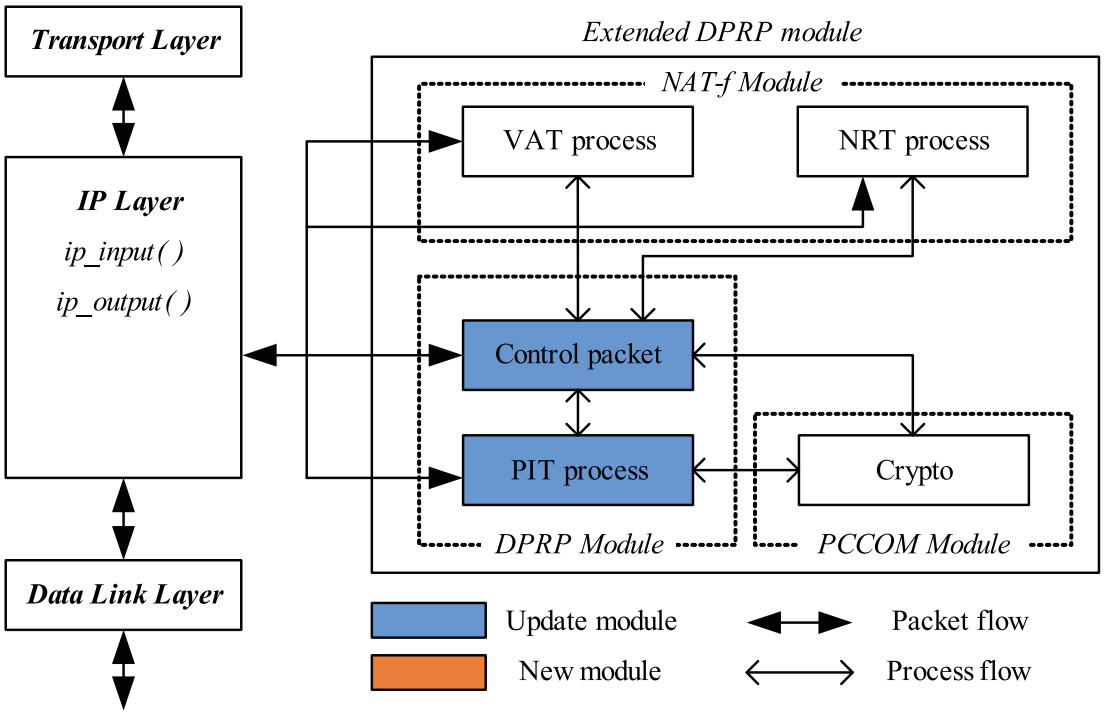

図 4.1　GES のモジュール構成

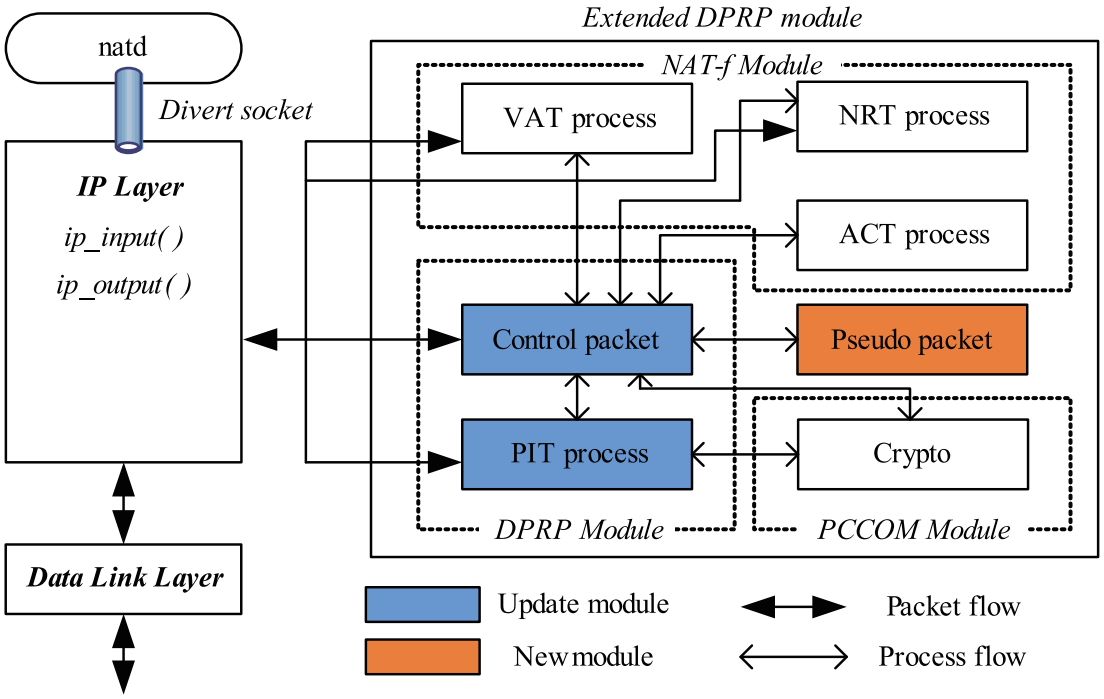

図 4.2　GNAT のモジュール構成

4.2　NAT テーブルの作成方法

図 4.3 に DPRP ネゴシエーションで生成される NAT テーブルの生成方法を示す．GNAT は DPRP ネゴシエーションのパケットを受信すると，制御パケットに含まれている CID や ACT で得られた IP アドレスの情報から TCP/UDP データパケットを生成する．このパ

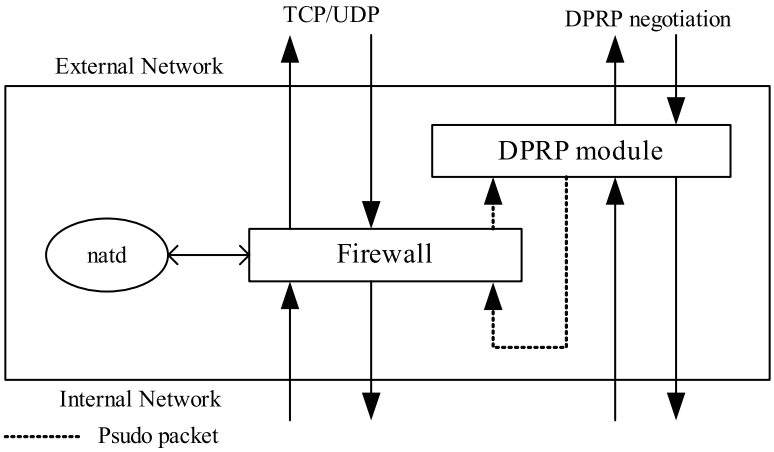

図 4.3　NAT テーブルの生成方法

ケットを擬似パケットと呼ぶ．擬似パケットは IN から EN へパケットが送信されたと見せかけた物でありこのパケットを *ip_input*() に渡すと，natd は IN から EN へ送信されるパケットを受信したと判断して，NAT にマッピングを行う．この時 NAT にマッピングされた内容は，実際の通信を行った時に必要となるものである．GNAT は DPRP モジュールで擬似パケットを受け取ると擬似パケットのコネクション情報から NAT にマッピングされたポート番号を新たに生成した制御パケットに追加してパケットを送信することにより VAT テーブルに必要なポート番号を通知することができる．

第5章　性能測定

5.1　動作検証

3 章で説明したシステム構成において NAT を越えて FTP によるファイル転送が可能であることを確認した．また，本稿では説明を行っていないが，GNAT 配下の端末が一般端末の場合においても通信が可能であることを確認した．その結果，NAT がある環境下でもグループ通信が可能であることが実証できた．

5.2　性能評価

図 3.1 のシステム構成において，GES1 から GES3 へ FTP 接続を行った場合の性能測定を行った．性能測定に使用した装置の仕様は，CPU が Pentium4 3.0GHz，メモリが 512MB である．またネットワーク環境は 100BASE-TX，1000BASE-TX の Ethernet であり，GES1，GNAT2，DDNS サーバをスイッチで接続した．

5.2.1　通信性能の測定

通信性能の測定は PCCOM の論文において行われているが，NAT を介したスループットの測定は行われていないため，今回の測定では NAT を介した環境において測定を行った．

以下に IP パケット長とスループットの関係を 100BASE，1000BASE の通信ごとに暗号化しない場合（以下，Normal と呼ぶ），PCCOM で暗号化する場合，PCCOM で暗号化しない場合のそれぞれについて示したものである．PCCOM ない場合とは通信相手が一般端末の場合であり，PIT の検索だけを行う場合である．スループットの測定にはネットワークベンチマークソフト Netperf を用いてメッセージサイズ変えて 10 秒間の TCP 通信

表 5.1　実験端末の仕様

項目	内容
CPU	Pentium4 3.0GHz
Memory	512MB(800Hz,L2:1MB)
NIC	100BASE-TX,1000BASE-TX
OS	FreeBSD（7.0 Release）

表 5.2　スループット測定結果（100BASE 環境）

	スループット（Mbps）
Normal	94.1
暗号化あり	94.1
暗号化なし	94.1

を 10 回行い，その平均値をとった．Netperf はパケットサイズ以外はデフォルトの値を使用した．この測定に用いた GNAT の NAT には natd を用いている．natd は divert ソケットを用いてユーザランドにパケットをコピーしたあと natd デーモンによりアドレス変換することで NAT 機能を実現している．PCCOM の暗号化には，128bit のグループ鍵，暗号化処理には AES（128bit）を使用した．

表 5.2 は EN と IN の双方向から 100BASE の環境で測定した結果である．3 パターンとも NIC の上限性能を発揮しておりスループットほぼ 94.1Mbps となり低下が見られなかった．これは，単位時間あたりの処理すべきパケットが少ないため PCCOM の処理オーバヘッドとなっていない．次に 1000BASE 環境での比較のために図 5.2 に直接通信を行った場合と図 5.3 にルータ（GEN）を挟んだ場合を示す．直接通信を行った場合は，PCCOM を用いた場合は短・長パケットとも 200Mpbs 程度となっており暗号化によるオーバヘッドが大きいことがわかる．PCCOM なしの場合は，PIT 検索のみのためそれほどスループットが低下していない．ルータを挟んだ場合では，短パケットの 64bytes，128bytes では直接通信を行った場合とほぼ同等の値であった．256bytes から 1460bytes までの Normal と PCCOM なしの場合，730Mbps 前後で同じになっている．これらの結果から中継によるオーバヘッドは約 110Mbps（27 %）であり，256bytes から 1460bytes の間では中継によるオーバヘッドで送信するパケット数が減少したため PIT 検索によるオーバヘッドが発生しなかったということがわかる．

図 5.4 に 1000BASE 環境で IN から EN へ通信を行った場合のスループットの結果を示す．Normal では 300Mpbs 程度のスループットが得られた．ルータを挟んだ場合と比べて約 430Mbps（59 %）低下しており，NAT によるオーバヘッドがかなり大きいといえる．これは natd がユーザランドで実行されており，カーネルから divert ソケットを用いてユーザランドへパケットをコピーを行った後，natd によりアドレス変換処理を行ってからパ

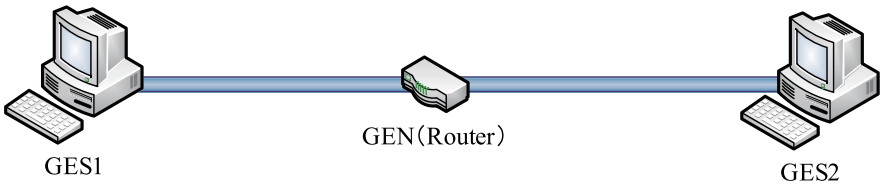

図 5.1　測定環境:ルータを経由した場合

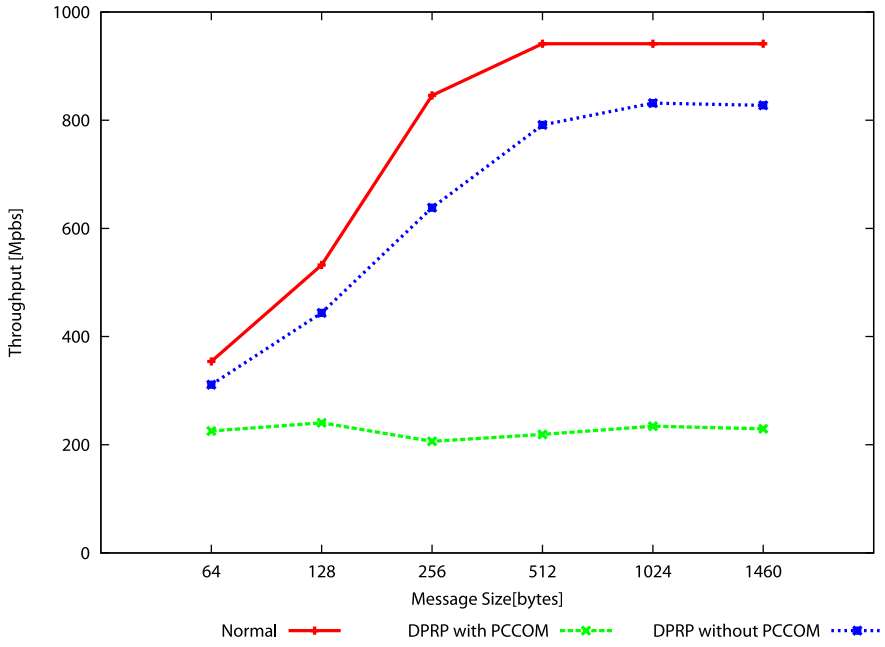

図 5.2　直接通信の場合のスループット測定結果（1000BASE-TX）

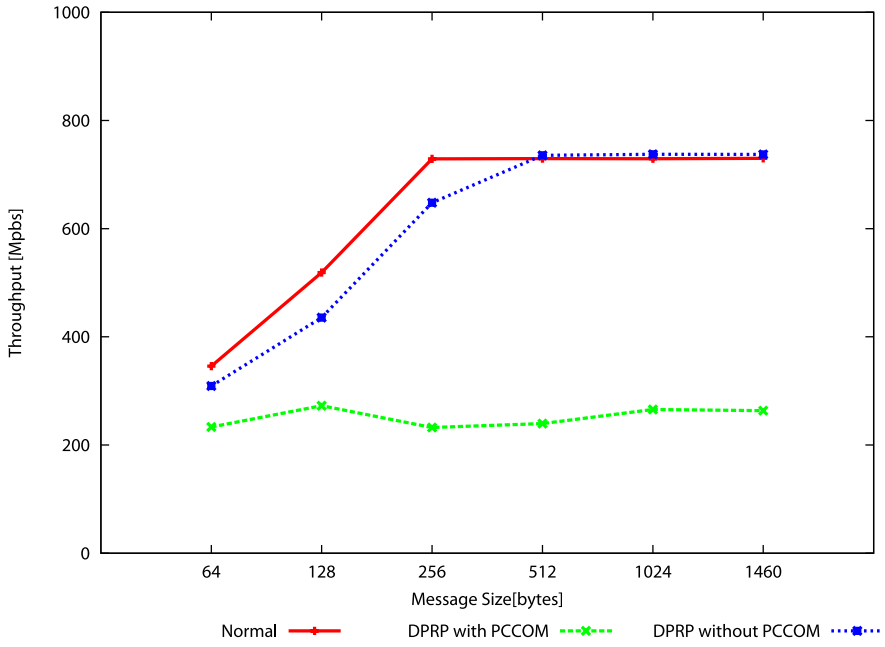

図 5.3　ルータを経由した場合のスループット測定結果（1000BASE-TX）

ケットを送信しているためである．natd により送受信で 2 回のメモリコピーが発生するため大きなオーバヘッドとなっいる．

図 5.5 に EN から IN へ通信を行った場合のスループットの結果を示す．EN からの通信の場合は VAT 処理が入るため IN からの通信に比べて若干スループットの低下が見られたが，VAT 処理によるオーバヘッドはほぼないといえる．これらの結果から 1000BASE 環境での PCCOM ありの場合は，暗号化によるオーバヘッドが大きいため 200 数十 Mbps 程度しかスループットがでないということがわかる．

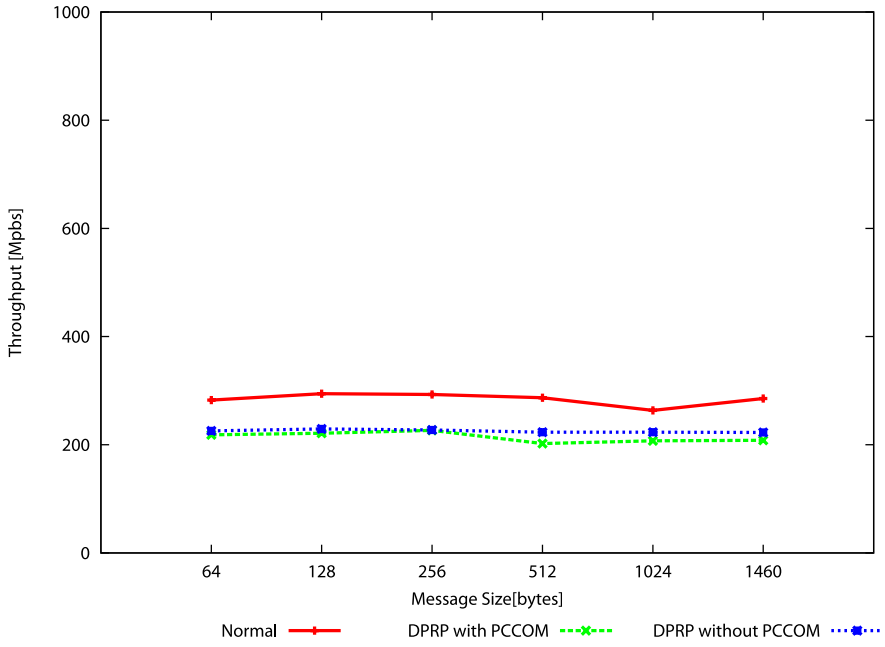

図 5.4　スループット測定結果:PA to GA（1000BASE-TX）

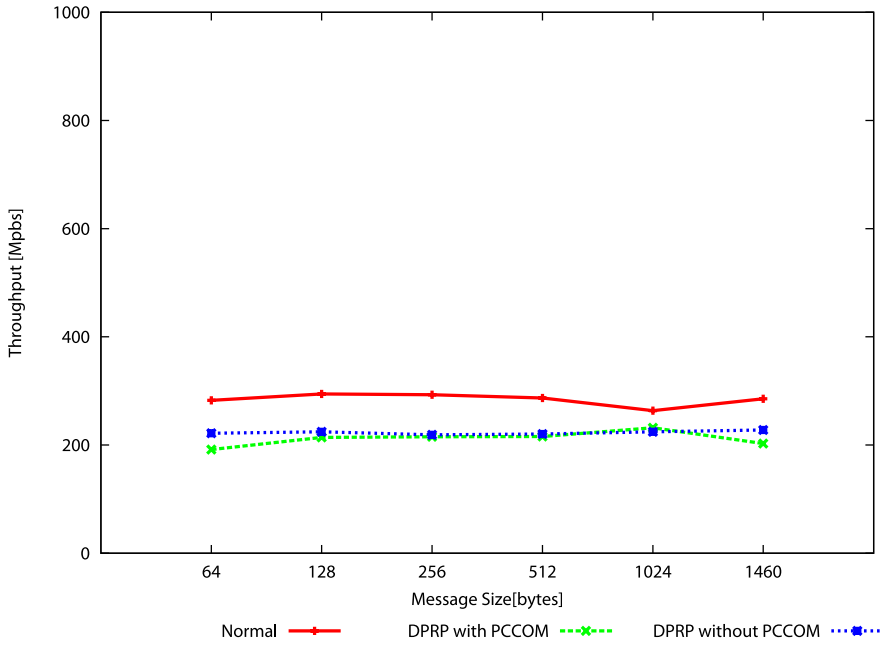

図 5.5　スループット測定結果:GA to PA（1000BASE-TX）

5.2.2　DPRP のオーバヘッド

提案方式のオーバーヘッドを明らかにするために，実際の通信が開始されるまでの時間にはネットワークアナライザ Ethereal を，また実装した拡張 DPRP モジュールの内部処理時間には RDTSC（Read Time Stamp Counter）を用いて測定した．RDTSC は CPU のカウンタから周波数クロックを取得する命令で，モジュール処理に費やした時間を正確に算出することができる．

表 5.3 に GEN と GNAT を通信経路上に設置した場合の DPRP ネゴシエーションの時間

表 5.3　DPRP のオーバヘッド時間

	ネゴシエーション時間 (μs)	通信開始までの時間 (μs)
GEN	1010	1025
GNAT	1144	1162

と通信開始までの時間を示す．ネゴシエーション時間は GEN の場合は 1010(μs)，GNAT では 1144(μs) となり拡張したことによるオーバヘッドは，約 130(μs) しかないことを確認した．通信開始までの時間では，VAT 処理による違いがあるがこちらもほとんどオーバヘッドがないことを確認した．

DPRP 内部処理時間を表 5.4 に示す．各制御パケットにおいて処理時間がかかっているが，これは大部分がパケットを暗号化/復号をしている時間である．制御パケットによって処理時間が異なるが暗号化/復号にはそれぞれ約 8(μs) かかっている．PIT 検索と VAT 検索・処理時間は合計でも約 1.28(μs) となっておりオーバヘッドは問題とならない．

表 5.4　モジュールの内部処理時間

測定対象	処理時間 (μs)
DNS の応答処理	5.553
VAT 検索処理	0.477
データパケット受信から DDE 送信まで	20.12
DDE 中継処理	18.84
DDE 受信から RGI 送信まで	28.839
RGI 受信から擬似パケット送信まで	17.634
擬似パケット受信から RGI 送信まで	15.76
RGI 受信から MPIT 送信まで	31.139
MPIT 中継処理	15.346
MPIT 受信から CDN 送信まで	18.77
CDN 中継処理	11.351
CDN 受信から待避パケット送信まで	28.975
VAT 処理	0.548
PIT 検索	0.257
暗号化/復号処理	49.03

第6章　まとめ

本稿ではDPRPを拡張しNAT越えを可能とする拡張DPRPを提案した．応用として多段NAT環境下における実現について検討した．拡張DPRPにより，外部から動的にNATテーブルを生成し，そのNATテーブルに対応したPITを生成を行う．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の混在する環境においてもGSCIPによるグループ定義が可能となった．プロトタイプシステムの実装を行い．NAT環境における双方向の通信ができることを実証した．提案方式の評価を行った結果，100BASEの環境においては実装しない場合と比べ，同等であることを確認した．今後はブロードキャストやマルチキャストパケットへの対応や，GMSを必要とせずエンドツーエンドでグループ定義を行い認証するような方法を検討していく予定である．

謝辞

本研究に関して，研究の方向や進め方など終始にわたり御指導，御助言を賜りました指導教官の渡邊晃教授に心より熱くお礼申し上げます.

論文作成にあたり，副査の柳田康幸教授，宇佐見庄五准教授には貴重なコメントや至らないところを指導していただき深く感謝いたします.

また，本研究を行うにあたり，本研究室の皆様にも多くの方々から多大な助言と協力を承り，深く感謝しております．とりわけ GSCIP グループに配属されて以来，深い議論をして頂いた鈴木秀和氏に心より感謝いたします.

最後に，研究を進めていく中，いつも暖かく支えて頂いた両親に心より感謝いたします.

参考文献

[1] Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R.: 2006 CSI/FBI Computer Crime and Security Survey, Technical report, Computer Security Institute (2006).

[2] Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998).

[3] 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).

[4] 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).

[5] Rosenberg, J., Mahy, R. and Huitema, C.: Traversal Using Relay NAT (TURN), Internet-draft, IETF (2005). draft-rosenberg-midcom-turn-08.

[6] Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, Internet-draft, IETF (2006). draft-ietf-mmusic-ice-12.txt.

[7] UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardized dcps/igd.asp.

[8] 鈴木秀和，渡邊　晃：.

[9] 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 (2006).

[10] Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, IETF (1999).

[11] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).

[12] Kivinen, T., Swander, B., Huttunen, A. and Volpe, V.: TNegotiation of NAT-Traversal in the IKE, RFC 3947, IETF (2005).

[13] Swander, B., Huttunen, A., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).

[14] OpenVPN: OpenVPN, http://openvpn.net/.

[15] Takeda, Y.: Symmetric NAT Traversal using STUN, Internet-draft, IETF (2003). draft-takeda-symmetric-nat-traversal-00.txt.

[16] Guha, S. and Francis, P.: Characterization and Measurement of TCP Traversal through NATs and Firewalls, *Proc. ACM International Measurement Conference (IMC)*, pp. 199–211 (2005).

[17] Guha, S. and Francis, P.: Simple Traversal of UDP Through NATs and TCP too (STUNT), Internet-draft, IETF (2004). draft-guha-STUNT-00.txt.

研究業績

学術論文

なし

国際会議

1. Yuji Goto, Hidekazu Suzuki, Akira Watanabe, ”Researches on Extended Dynamic Process Resolution Protocol that Can Traverse NAT”, Proceedings of the IEEE International Region 10 Conference 2007 (TENCON2007), Oct.2007.

研究会・大会等

1. 後藤裕司, 鈴木秀和，渡邊晃, “異なるアドレス空間をまたがる DPRP の検討,” 平成 17 年度電気関係学会東海支部連合大会論文集, Jan. 2005.

2. 後藤裕司, 鈴木秀和，渡邊晃, “グローバルアドレスとプライベートアドレス空間を跨る DPRP の検討,” 情報処理学会第 68 回全国大会講演論文集, Jan. 2006.

3. 後藤裕司, 鈴木秀和，渡邊晃, “NAT 越えが可能な DPRP の検討,” 電子情報通信学会 2007 年総合大会講演論文集, p.1373-1377, Jan. 2007.

4. 後藤裕司, 鈴木秀和，渡邊晃, “NAT 越えを可能にする DPRP の検討,” マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム論文, p.1373-1377, Jan. 2007.

5. 後藤裕司, 鈴木秀和，渡邊晃, “NAT を越えてグループ通信が可能な拡張 DPRP の提案,” マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム論文, p.593-600, Jan. 2008.

付 録A　既存技術

本章では図 A.1 に示す環境下において，既存の VPN 技術，NAT 越え技術を分類し，それらの特徴を整理する．以後，外部ノードを EN（External Node），内部ノードを IN（Internal Node），両ノードが共にアクセス可能な専用サーバを RS（Rendezvous Server）と略する．

A.1　VPN 技術

A.1.1　IPsec

IPsec は，IP 層でパケットの暗号化などを行うことによりネットワーク自体のセキュリティを確保することができる代表的なセキュリティ技術である．IPsec は IP 層のカーネルに実装されておりアプリケーションとは独立しており，汎用的に利用できる．IPsec を利用するには SA（Security Association）双方で共有する必要がある．SA を共有するプロトコルとして IKE（Internet Key Exchange）がある．IKE では，暗号化アルゴリズムや認証方式などの SA の各パラメータの決定と通信相手と認証を行い IPsec で使う鍵の交換を行う．IKE を実行するには，動作モード，鍵交換アルゴリズム，暗号化アルゴリズム，認証アルゴリズムなどの事前設定項目が多く，端末が増加すると設定に負担がかかる．IPsec では AH（Authentication Header）で認証，改竄防止機能を提供し，ESP（Encapsulated Security Payload）はペイロード部を暗号化する．動作モードには，ホスト間の通信で利用されるトランスポートモードとネットワーク通信で利用されるトンネルモードがある．しかし，これらが暗号化に利用する ESP は通信経路上に NAT/NAPT [10]（以後 NAT と総称する）がある場合，NAT でアドレス変換後ににチェックサムを更新できないなどの問題があり利

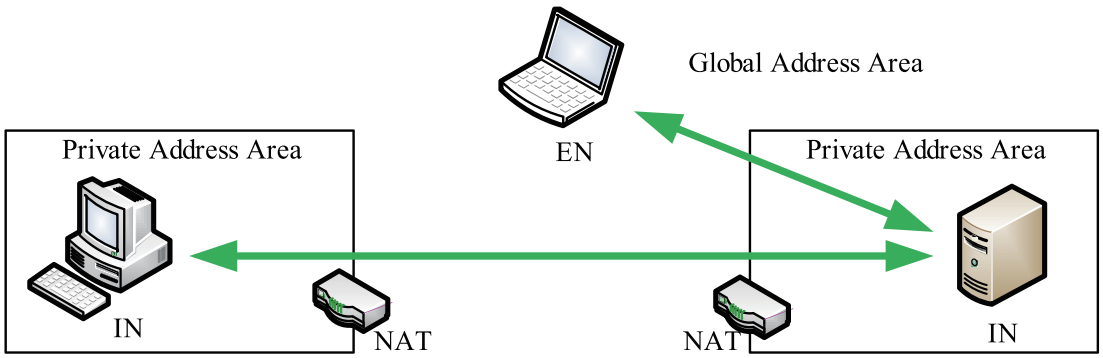

図 A.1　比較モデル

用することができない．そこで，この問題を解決するためにUDPによるカプセル化をすることによってNATを通過するを方法がRFC [12] [13] で提案されている．しかし，UDPでカプセル化することによりカプセル部分は完全保証の範囲に含むことができず，ヘッダの追加によるオーバヘッドの増加やフラグメントの発生などの課題が発生する．NAT環境下でトランスポートモードを利用する場合は，IKE，データ通信に必要なポートを開放しておく必要がある．さらに，IPsecを利用するには設定項目など多く，利用することが難しい．また，端末のIPアドレスが変更された場合，再設定が必要となり端末は柔軟に移動することができないないなどの問題がある．

A.1.2 OpenVPN

OpenVPN [14] はユーザランドで実装されているVPNソフトウェアである．OpenVPNに用いる二重認証SSL/TLS鍵共有/鍵交換はIPsecのIKEとほぼ同等かつ，IPsecのESPと類似のトンネル・システムを実装している．OpenVPNはTUN/TAP仮想ネットワークドライバを利用することでルーティングとブリッジの2つのモードを実現している．ルーティングはOpenVPNサーバとクライアントはそれぞれ別のセグメントのネットワークが割り当てられる．そのため，ブロードキャストのような無駄なパケット転送がされたいためアクセス制御が実施しやすい．ブリッジはOpenVPNサーバとクライアントが同一セグメントに仮想的に接続するため，ブロードキャストパケットや，非TCP/IPパケットもクライアントに転送することができる．秘密鍵，公開鍵証明書，パスワードを利用して相互の認証を行うのため，IPアドレスの変化に柔軟に対応することができる．しかし，UDPまたはTCPによるカプセル化をソフトウェアで行うため，スループットはIPsecよりも低い．ENがINと通信を行う場合は，トンネリングに必要なポートの設定を行っておくことで通信可能である．

A.2 NAT越え技術

A.2.1 STUN

STUN（SimpleTraversal of UDP Through Network Address Translators）[4] はENがRSからINに対応するマッピングアドレスを取得し，そこに向けて通信することによりNAT越え通信を実現する方式である．INは定期的にRSと通信を行い，NATではINに対するマッピングアドレスが割り当てられる．RSはINから送信されたパケットの送信元IPアドレスおよびポート番号から，マッピングアドレスを取得することができる．ENはRSよりINのマッピングアドレスを取得し，マッピングアドレス宛へ通信することにより，INへの通信を実現している．この方式は最も普及しているCone NATに対応できることから，すでに実用化されてている．しかし，UDP通信アプリケーションに限定されていたり，Symmetric NATに対応できなかったりするなどの課題がある．近年は，STUNを

拡張することにより TCP や Symmetric NAT に対応できる手法 [15] [16] [17] が検討されている．

A.2.2 TURN

TURN（Traversal Using Relay NAT）[5] は EN と IN 間の通信を RS が仲介することで NAT 越え通信を実現する．この方式は Cone NAT と Symmetric NAT の両方に対応することができる．しかし，すべての通信が RS を経由するため，RS にネットワーク負荷や処理負荷が集中したり，RS の設置や二重化などにコストがかかったりするという課題がある．また経路が冗長になることなどから，今後さらに普及する P2P 通信の特徴である柔軟性やリアルタイム性が失われる懸念がある．

A.2.3 ICE

ICE（Interactive Connectivity Establishment）[6] はマッピングアドレス取得に STUN や TURN を用いる方式である．NAT の種類によって STUN と TURN を使い分けることによって Symmetric NAT であっても NAT 越え通信を行うことができる．しかし，場合によっては中継しなければならないため，TURN の欠点であるスループットの低下や遅延が発生してしまう．

A.2.4 UPnP

UPnP（Universal Plug and Play）[7] は NAT に機能を実装し，IN から指示により動的にマッピングを行う方式である．IN は NAT から設定されたマッピングアドレスを取得して利用することができる．EN がマッピングアドレスを取得するために，IN はアプリケーションサーバとして用意された RS へマッピングアドレスを通知する必要がある．UpNP 対応ルータ（NAT）は動的にマッピングを行うためにブロードキャストを利用するため，クライアントに一番近い NAT にしかマッピングを行うことができない．そのため，多段 NAT 環境の場合，外側からの通信は一番外側の NAT で対応するマッピングがないためパケットを内部に転送することができない．

A.2.5 NAT-f

NAT-f（NAT-free protocol）[8] は RS を必要とせずエンドツーエンドで NAT 越えを実現できる方式である．NAT-f は EN と NAT の IP 層のカーネルに実装されておりアプリケーションと独立しているため，汎用性がある．NAT-f は通信開始前に NAT-f ネゴシエーションを行い NAT に実際の通信に必要な NAT テーブルを生成する．そして，そのときに NAT にマッピングされたポート番号を EN に通知することで EN はそのマッピングされたポー

表 A.1　既存技術とその実装箇所

	実装方法	実装箇所			RS
		EN	IN	NAT	
IPsec transport	Kernel	✓	✓	—	なし
IPsec tunnel	Kernel	✓	—	✓	なし
OpenVPN	Userland	✓	✓[3]	—	OpenVPN サーバ
STUN	Userland	✓	✓	—	STUN サーバ
UPnP	Userland	✓	✓	✓	Application サーバ
TURN	Userland	✓	✓	—	TURN サーバ
ICE	Userland	✓	✓	—	STUN/TURN サーバ
NAT-f	Kernel	✓	—	✓	なし

[3] 実装する必要がないが，実装した場合は暗号化範囲に含まれる

ト番号宛にポートを変換して送信する．NAT では NAT テーブルに従って IP アドレスとポート番号を変換することにより IN と通信が可能となる．NAT-f ネゴシエーションではトリガとなったパケットのプロトコルタイプに応じた NAT マッピングが行われるため，TCP/UDP の双方に対応することができる．NAT では EN と IN 間で確立するコネクションごとにマッピングが行われるため，Cone NAT と Symmetric NAT の双方に対応することができる．また，カプセル化をする必要がなくエンドツーエンドで通信することが可能なため，遅延は発生せず NAT-f を実装しない場合と比べて同等のスループットを得ることができる．

表 A.1 に既存技術の実装箇所と必要な装置についてまとめる．OpenVPN は IPsec と同等の機能を持っているが TUN/TAP を利用することでユーザランドに実装することを可能としている．OpenVPN では，IN と通信をする場合は NAT の内側に OpenVPN サーバを設置しトンネルで利用するポート番号を設定するだけでよく NAT に機能を実装する必要はない．NAT-f 以外の NAT 越え技術はユーザランドで実行されるアプリケーションごとに機能を実装する必要があるため，汎用的に利用することができない．UPnP は NAT に機能を実装する必要があるが最近のブロードバンドルータには機能が実装されているため，導入は容易である．

表 A.2 に VPN 技術の要求条件を表 A.3 に NAT 越え技術の要求条件と，既存技術の満足度を示す．表中の “○”，“△”，“×” は各要求条件を満たしているかどうかを示す．“△” は場合によっては満足しない．又は一部満足していないことをします．端末の IP アドレスが変化した場合，OpenVPN は証明書により認証を行うため “○”，IPsec は IP アドレスの再設定を行わなければならないため “×” とする．NAT との相性は，“△” はポートフォワーディングの設定が必要があるが NAT を介しての通信はできる．IPsec のトンネルモードは，ポートフォワーディングの設定がいらないため “○” とした．OpeVPN は TUN/TAP を使用しカーネルからユーザランドにパケットを取り出し処理を行ってからパケットを送信するためオーバヘッドが大きいためスループットは IPsec よりも低いため “×” とした．OpenVPN の設定項目数は，OpenVPN サーバの設定項目数は多いが，クライ

表 A.2　VPN 技術との比較

	OpenVPN	IPsec transport	IPsec tunnel
IP アドレスの変化	○	×	×
NAT との相性	△	△	○
スループット	×	△	△
設定項目数	△/×[1]	×	×
暗号化方式	SSL/TLS	ESP	ESP
暗号化範囲	G-G/C-G/C-C	C-C	G-G/C-G

C：Client, G：Gateway(NAT, OpenVPN Server)

[1] クライアントの設定は少ないが，OpenVPN サーバの設定が多い

表 A.3　NAT 越え技術との比較

	STUN	UPnP	TURN	ICE	NAT-f
多段 NAT	○	×	○	○	○
TCP 通信への対応	×	○	○	○	○
Symmetric NAT	×	×	○	○	○
スループット	○	○	×	△	○
遅延	○	○	×	△	○

アントの設定はそれほど多くないため “△” と “×” とした．暗号化範囲とは実際の通信を行う場合のどこからどこまでの装置の通信経路が暗号化されているかを示す．“C” はクライアント “G” はゲートウェイを表しており “C-C” はクライアント間が暗号化されるということを表している．OpeVPN は，OpenVPN のソフトウェアがインストールされている端末まで暗号化することが可能であるため，“G-G/C-G/C-C” とした．今後 IPv4 アドレスの枯渇により多段 NAT 環境が多くなってくると考えられる．STUN，TURN,ICE はインターネット上にサーバがあるため多段 NAT 環境でも利用できる．しかし，UPnP は UpNP 対応ルータ（NAT）は動的にマッピングを行うためにブロードキャストを利用するため，クライアントに一番近い NAT にしかマッピングを行うことができない．そのため，多段 NAT 環境の場合，外側からの通信は一番外側の NAT で対応するマッピングがないためパケットを内部に転送することができないため “×” とした．UDP と TCP にも対応することが望まれるが STUN は TCP 通信ができない．さらに，Cone NAT だけでなく Symmetric NAT に対応することが望まれるが STUN と UPnP は原理上対応することができない．TRUN はすべてのパケットが RS を中継するため遅延が大きくスループットが大きく低下するため “×”，ICE は “△” とした．NAT-f はすべての項目において条件を満たしており優れているのが分かる．

付 録B　既存技術との比較

B.1　VPN 技術との比較

提案方式は IPsec と同様にカーネルの IP 層で実装されており，アプリケーションに依存しない．OpenVPN はカーネルに実装されていないが，TUN/TAP 仮想ネットワークドライバを利用することでアプリケーションがカーネルに渡したパケットに対して処理を行うことができるため，Ipsec と同様のことが可能である．OpenVPN はブリッジ方式を利用することでマルチキャストパケットやブロードキャストパケットに対応することができるが，IPsec と提案方式は IKE と DPRP ネゴシエーションがユニキャストのみしか対応していないため DLNA などには対応していない．IPsec は通信相手の IP アドレスを設定する必要があり端末が移動などして IP アドレスが変更された場合再設定が必要となる．OpenVPN は証明書で通信相手を認証しているため IP アドレスが変更されても再設定は必要がない．DPRP は，IP アドレスが変更された場合は DPRP ネゴシエーションにより暗号化などに必要なグループ鍵などの情報を収集し PIT を作成するため再設定は必要としない．また，通信経路上に NAT がある場合は OpenVPN と IPsec のトランスポートモードはトンネル通信に必要なポート番号をあけておく必要がある．提案方式は NAT 装置を GNAT にする必要があるが通信時に DPRP ネゴシエーションによって NAT に通信に必要なマッピングができるためポートの設定をする必要がない．OpenVPN と IPsec はカプセル化する必要があるためオーバヘッドが大きいためスループットは大きく低下するが，提案方式はカプセル化する必要がなくパケットフォーマットを変える必要がない暗号化方式 PCCOM を利用しているため 100BASE 環境においてはスループットはほとんど低下しない．また，提案方式は IPsec のトランスポートモード/トンネルモードと同様の機能かつ両モード混在するような環境においても可能であるため，トランスポートモードのように NAT 装置が GNAT でない場合は EN と IN が GE であれば暗号化通信を行うことができる．さらに，EN と NAT が GE であれば IN が一般端末であっても NAT の内外のどちらからでも通信開始をすることが可能である．

B.2　NAT 越え技術との比較

提案方式と NAT-f 以外の既存技術はアプリケーションに実装されているため，アプリケーションごとにその機能を追加する必要があるが，提案方式は上記で述べたように IP 層のカーネルの実装されているためアプリケーションに依存しない．DPRP ネゴシエー

ションではトリガとなったパケットのプロトコルタイプに応じたNATマッピングが行われるため，TCP/UDPの双方に対応することができる．DPRPネゴシエーションにより生成されるVATテーブルのエントリにはENのIPアドレスと共にポート番号を含んでいるため，NATではENとIN間で確立するコネクションごとにマッピング処理が行われる．そのため，Cone NATとSymmetric NATの双方に対応することができる．提案方式ではDPRPネゴシエーション後の通信はエンドツーエンドで実現できるため，TURNのような冗長経路による通信遅延は発生しない．提案方式は多段NAT環境でENからINの通信を開始する場合は，UPnP以外の他の方式と異なり通信経路上のNAT装置に実装が必要があるため“△”とする．提案方式ではグループ鍵などを配送する管理サーバGMSが必要であるが，一般家庭などに導入するには難しいと考えられる．現在の実装ではグループ鍵など必要な情報をファイルから読み込む方式にも対応しているため必ずGMSは導入する必要がない．しかし，その場合はグループ鍵などの情報は確実に安全な方法で共有する必要がある．

表 B.1　提案方式の評価

項目	評価
端末の移動	○
ブロードキャスト/マルチキャスト	×
NAT/FWとの相性	○
スループット	○
多段NATへの対応	△
symmetric NATへの対応	○
遅延	○
TCP通信への対応	○
RS	GMS

この章ではOpenVPNと拡張DPRPを比較することで評価を行う．表B.1に拡張DPRPの評価を示す．拡張DPRPは，システム構成が変化してIPアドレスが変化しても端末自身が動的にDPRPネゴシエーションを行うこと暗号化に必要な情報を再設定を行うため管理負荷は発生しない．OpenVPNでは，証明書により通信相手の認証を行っているためIPアドレスが変化しても再設定を行う必要がない．OpenVPNは，NAT配下の端末と通信を行う場合，NATやFWにトンネル通信に必要なポート番号の設定を行っておく必要があるが，拡張DPRPでは通信開始時に，外側の端末とNATが連携してコネクションごとにNATにマッピングを行うためあらかじめ設定を行う必要がなく，symmetric NATにも対応することができる．拡張DPRPはカプセル化や第3の装置などの中継せずエンドツーエ

ンドで行う方式のため遅延が発生せず高スループット実現することができる．OpenVPN は，ユーザランドで暗号化やカプセル化の処理を行っており，かなりのオーバヘッドが発生するためスループットは低い．また，NAT 配下の端末と通信する場合は OpenVPN サーバを経由する必要があるため遅延が発生してしまう．多段 NAT への対応では，OpenVPN はポートの設定を行うことで可能であり，拡張 DPRP も通信経路上の NAT 装置を GNAT に置き換えることによって対応が可能である．