異なるアドレス空間を跨る DPRP の検討

後藤　裕司

近年，イントラネット内における情報漏洩などの脅威に対するセキュリティ対策が重要視されている．既存のネットワークセキュリティ技術である 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，その変化に応じて設定情報を変更する必要がある．そのため管理者の管理負荷が大きく IPsec はイントラネット内でほとんど利用されていない．そこで，我々はシステム構成が変化しても動的に動作処理情報を生成することができる，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 は同一アドレス空間でしか動作せず，通信経路上に NAT（Network Address Translation）が介在し，プライベートアドレス空間とグローバルアドレス空間が混在するような環境には対応できない．

そこで本論文では，プライベートアドレス空間とグローバルアドレス空間が混在するような環境において，NAT を越えて DPRP を行うことができる拡張 DPRP について検討する．

Researches on extended Dynamic Process Resolution Protocol for different types of address areas

Yuji Goto

In late years an anti-security measure for menaces such as information leaks in intranet is regarded as important. It is necessary a terminal moves, and IPsec that is existing network security technology does it, and system constitution accepts the change in environment changing frequently, and to change setting information. Therefore management load of a manager is big, and IPsec is not almost used in intranet. Therefore I am dynamic and suggest dynamic processing solution protocol DPRP (Dynamic Process Resolution Protocol) which can generate movement processing information even if system constitution changes as for us. However, existing DPRP works only in the same address area, and NAT (Network Address Translation) exists among it on a communication course and cannot cope with the environment where private address area and global address area coexist.

Therefore, in this article, I examine expansion DPRP which I surpass NAT, and can perform DPRP in the environment where private address area and global address area coexist.

第１章　　研究背景

今日の企業ネットワークでは，不正進入，データの盗聴や漏洩，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．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）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，個人情報の漏洩など社員や内部関係者の不正による犯罪が多く報告されている．しかしながら，イントラネット内部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．ネットワークセキュリティの代表的な既存技術として IPsec があり，現在 VPN を構築する手段として広く利用されている．IPsec は通信に先立ち暗号・認証に必要なパラメータを動的に生成して安全に情報の交換を行う．しかし，IPsec は多くの設定が必要であり，システム構成が頻繁に変わるような環境では管理者による負荷が大きいという課題がある．また，ホスト間で暗号化通信を行うトランスポートモードと，ネットワーク間で利用されるトンネルモードに互換性がない．そのため，イントラネットのよ

うに，セキュリティドメインが階層的に構築されていたり，個人単位のセキュリティと混在するような環境に対応することが難しい．そこで我々はイントラネット内のセキュリティ対策と運用管理負荷の軽減を両立し，かつホストがあらゆる空間を自由に移動することが可能なネットワークの概念として，FPN（Flexible Private Network）の構築を目指している[1], [2]．また，FPN を実現するために，新たな通信アーキテクチャ GSCIP（Grouping for secure Communication for IP）を検討している．GSCIP は，システム構成が変化しても動的に動作処理情報を生成する動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）[3]，移動して IP アドレス変化しても P2P で通信の継続が可能な Mobile PPC（Mobile Peer-to-Peer Communication）[4]，グローバルアドレス空間からプライベートアドレス空間への通信開始を可能とする NATF（NAT Free protocol）[5]などのプロトコル群によって構成される．

以下，第 2 章で FPN と既存 DPRP，第 3 章で NAT 越えに対応した拡張 DPRP，第 4 章で拡張 DPRP の実装，第五章で今後の検討課題，第 6 章でまとめについて述べる．

第２章　　FPN と既存 DPRP

２-１　　FPN の概要

FPN はサブネット単位とホスト単位に安全性の確保された通信グループを構築する．グルーピングの関係はホストがサブネットの内外を自由に移動しても維持される．また，暗号化などに必要な情報は通信開始時に自動的に生成されるため，移動後もセキュアな通信を行うことが可能である図 1 に FPN の通信について示す．FPN はサブネット単位とホスト単位での混在環境においてもグループ通信を行うことが可能であり，同一通信グループのメンバ間の通信は暗号化され，異なる通信グループの端末からのアクセスを拒否することができる．

FPN の適応範囲はイントラネット内とインターネット上の 2 種類が考えられる．前者は企業ネットワーク，後者はホームネットワークを想定している．企業にイントラネット内に適応することにより多段構成にも対応でき，かつセキュリティも確保することができる．企業にはインターネットとイントラネットの間には強固な FW があるためインターネット上までに適応することは想定していない．一方，ホームネットワークの FW（以下 HFW）は企業のほど強固ではなくインターネットの延長に近い．そこで，図 3 に示すようなインターネットとホームネットワークのグルーピングの実現させる．しかし，従来の DPRP は通信経路上に NAT が介在する環境には対応していないため，インターネット上の FPN を実現できなかった．また，イントラネット内にも部門単位で NAT が存在することも考えられる．これらの環境に対応するために DPRP の NAT 越えを提案する．本論文では，その第一ステップとしてプライベートアドレス空間からグローバルアドレス空間への DPRP について述べる．

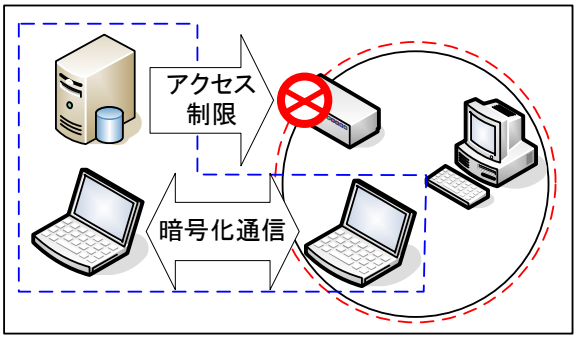

図 1　FPN の通信

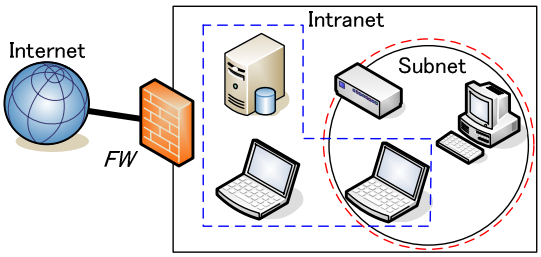

図 2　イントラネット内の FPN

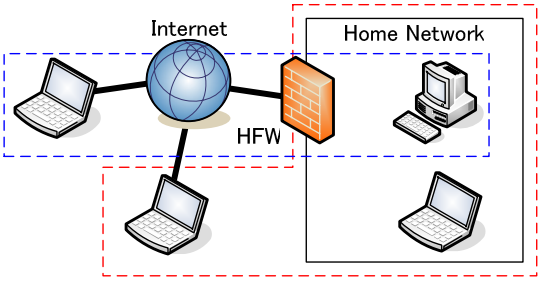

図 3　インターネット上の FPN

２-２　　GSCIP の概要

GSCIP とは FPN を実現するための通信アーキテクチャである．図 4 に GSCIP のグルーピングの定義方法を示す．GSCIP の通信グループを構成する機器を GE（GSCIP Element）と呼び, ホストタイプの GES, ルータタイプの GEN などがある．GEN はサブネットを構成し，配下の一般ホスト Term を保護する．GSCIP では各ホストが所持する共通鍵を用いて GE 間の通信を暗号化することでグループ通信を可能にする．GSCIP ではこの共通鍵のことをグループ鍵 GK（Group Key）と呼び，通信グループとグループ鍵を１対１に対応づけることで，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る．グループ鍵は各 GE が起動時に管理装置 MS（Management Server）から通信グループ情報と共に配送される．この際, 公開鍵を用いた確実な認証が行われている．グループ鍵 GK は定期的に, または通信グループ内のシステム構成が変更された時に更新される．

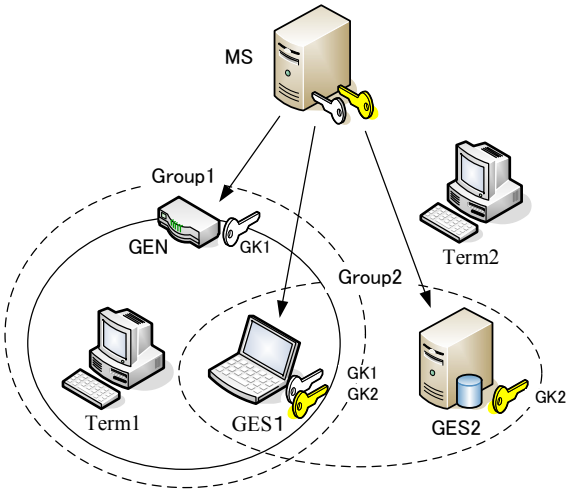

図 4　グルーピングの定義方法

GSCIP では通信に先立ち，GE は自身が保持する動作処理情報テーブル PIT（Process Information Table）に従い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，プロトコルタイプと，これらに一致するパケットの処理内容を規定した動作処理情報（暗号化/復号/透過中継/破棄），およびグループ鍵の識別情報が記述されている．PIT の検索には通信パケットの送信元/宛先 IP アドレス, ポート番号, およびプロトコルタイプの組を用いる．これらの情報の組をコネクション識別子 CID（Connection Identification）と呼ぶ．該当する PIT が無い場合は GSCIP の一部である動的処理解決プロトコル DPRP を用いて PIT の生成を行う．

２-３　　動的処理解決プロトコル DPRP

図 5 に既存の DPRP の動作を示す．GEN のサブネット配下にいる GES2 が GES1 と通信を行う場合の動作について説明する．GES2 は GES1 と通信を開始するときに PIT 検索を行う．該当する PIT が無い場合は, 通信パケットを一時的に待避させ，DPRP ネゴシエーションを行う． DPRP ネゴシエーションには，ICMP をベースとした DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）という 4 つの制御パケットを用いる．DDE には，DPRP のトリガーとなった通信パケットの CID 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 が終点 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「PA1」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 にセットして終点 GE，即ち 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 ネゴシエーションの完了を通知するために CDN を生成し, 始点 GE, 即ち 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 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. そのため, 管理者やユーザは暗号化通信に必要な設定を更新する必要がない．

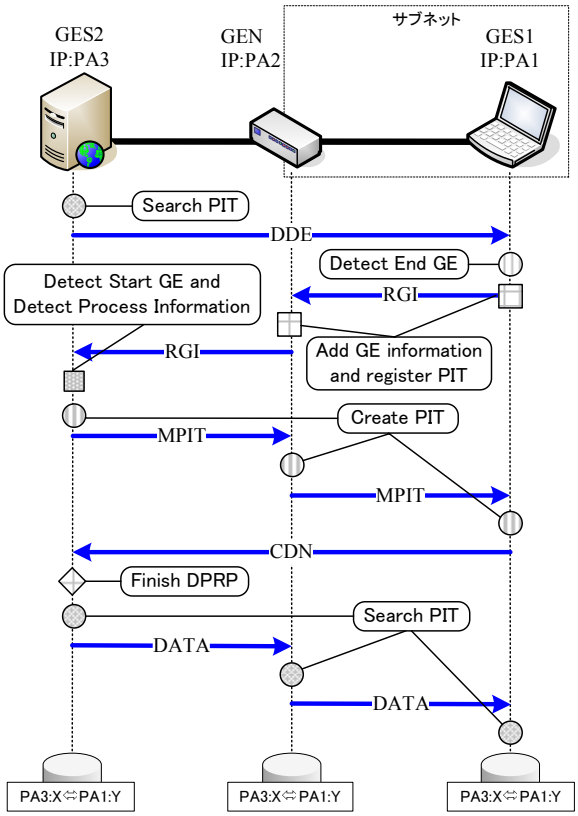

図 5　既存の DPRP シーケンス

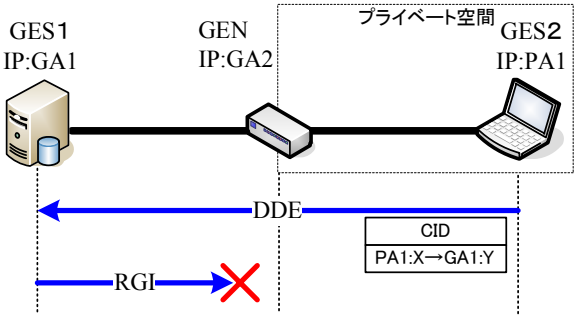

図 6　RGI の宛先問題

2-4　　DPRP の課題

各 GE が保持する PIT は制御パケットに記載されている CID の情報を元に生成される．そのため，通信経路上に NAT が介在すると CID と PIT の内容が一致しないという問題が起こる．その理由は，IP アドレスが NAT により変換されてしまうため，グローバルアドレス空間側の GE は NAT が通信相手に見え，プライベートアドレス空間側の GE はグローバルアドレス空間の GE が通信相手に見えるためである．

また RGI が宛先へ到達しないという問題も発生する．図 4 の GEN に NAT 機能を持たせ，サブネットをプライベートアドレス空間として見立てると，RGI の宛先は CID の送信元 IP アドレスに送信するため，プライベートアドレスとなる．プライベートアドレスはインターネット上では無効なアドレスであるため RGI を送信することができない（**図 6**）．

第３章　　NAT 越えに対応した拡張 DPRP

３-１　　拡張 DPRP

前章で述べた問題を解決するために NAT 越えに対応した拡張 DPRP について述べる. 拡張 DPRP ではアドレス変換に対応させた GEN を GNAT と呼ぶことにする.

図 10 に DPRP のパケットフォーマットを示す．DPRP は ICMP ベースとした制御パケットであり，ICMP ペイロード部に DPRP ヘッダ，各 DPRP 制御パケットヘッダ，オプション部，データ部が定義されている. オプション部は可変長であり，DPRP を拡張するために必要な情報を記載する．DPRP ヘッダには，通信パケットの CID のハッシュ値, DPRP パケットであることを示す識別子 DPRP ID や，フラグなどが記載される. CID のハッシュ値は PIT を検索するときに使われる．フラグフィールドには GNAT を通過する際に情報が設定される. 即ち, DPRP パケットがグローバルアドレス空間を流れているのか, プライベートアドレス空間を流れているのかを判断することができる．各 GE はこのフラグフィールドの値をチェックすることで，パケットの処理内容を変化する.

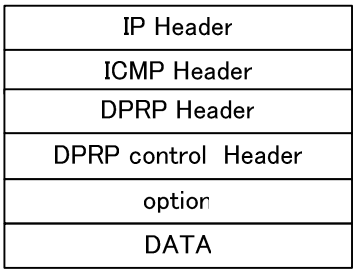

図 7　DPRP のパケットフォーマット

３-２　　拡張 DPRP の動作

図 8 にプライベートアドレス空間からグローバルアドレス空間への通信を行う場合の拡張 DPRP の動作を示す. システム構成はプライベートアドレス空間を構成する GNAT, その配下に GES1 を，グローバルアドレス空間に GES2 を配置する. IP アドレスはそれぞれ GA1, PA1，GA2 とする.

GES1 が GES2 に対して通信を行う場合を想定し, このときの送信元および宛先ポート番号を X 番, Y 番とする．X 番ポートは GES1 がランダムに選択するポート番である. まず, GES1 が DDE を GES2 宛に送信する．GNAT は DDE が通過する際に NAT によるアドレス変換を行うと共に，DPRP ヘッダのフラグフィールドに NAT を越えたという識別フラグをセットする. DDE を受信した GES2 は上記のフラグがセットされていれば，RGI の宛先を CID の送信元 IP アドレス PA1 ではなく，DDE の送信元 IP アドレス GA1 に変更する. RGI は GNAT で NAT によりアドレス変換され, プライベートアドレス空間の GES1 へ転送される．GES1 は動作処理情報を決定し，PIT を生成する．ここで生成される PIT は通信パケットの CID の情報が設定されている．その後，MPIT を生成する際，オプション部に DPRP のトリガーになった通信パケットの CID を記載して GES2 宛に送信する. GNAT は MPIT を受信すると CID に記載されている情報から同一のコネクション情報を持つ TCP または UDP パケットを生成する. このパケットを疑似パケットと呼ぶ. 疑似パケットのデータ部には MPIT に記載されている動作処理情報などをコピーする. GNAT は疑似パケットを受信したかのように見せかけることで， 表 1 に示すような NAT テーブルを強制的に作成する. NAT により送信元ポートが X 番から Z 番へ変換される．NAT テーブル生成後，アドレス変換後の疑似パケットの CID 情報を元に PIT の生成を行い，この CID を記載した MPIT を新たに作成する. 疑似パケットは MPIT を GES2 へ送信した後に破棄される. GES2 は MPIT 受信後, PIT の生成を行い, CDN を送信して DPRP ネゴシエーションの完了を通知する．このように処理を行うことで, プライベートアドレス空間側の GES1 にはアドレス変換前の CID と一致した PIT が作成され, GNAT および GES2 にはアドレス変換後の CID と一致した PIT が作成される．GES1 は待避していたパケットに対し PIT 検索を行い，GES2 宛にパケットを送信する. GNAT はプライベートアドレス空間側からパケットを受信すると, 表 1 の NAT テーブルに従って通常のアドレス変換を行い, PIT に基づいた処理を行う. また, グローバルアドレス空間側からパケットを受信した場合は，PIT に基づいた処理を行った後にアドレス変換を行う.

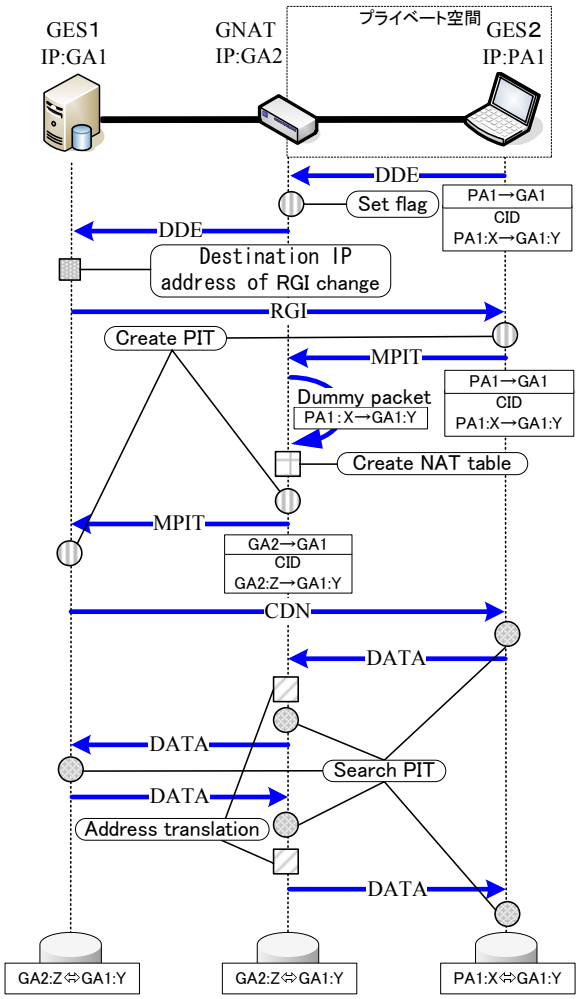

図 8　改良 DPRP のシーケンス

表 1 NAT テーブル

PA1:X⇔GA2:Z

第４章　　拡張 DPRP の実装

４-１　　実装概要

DPRP は FreeBSD の IP 層に実装される．図 12 に DPRP の実装概要を示す．DPRP は IP 層の入出力関数 ip_input()，ip_output()から DPRP モジュールを呼び出して処理を行うため，IP 層の処理部分は DPRP の影響を一切受けない．

４-２　　拡張 DPRP のモジュール構成

４－２－１　　疑似パケット生成モジュール

疑似パケット生成モジュールは GNAT が MPIT を受信したときに呼ばれ，MPIT のオプション部にある CID の情報で図に示す TCP または UDP パケットを生成する．疑似パケットのデータ部には MPIT の DPRP ヘッダ以降の内容がコピーされる．

４－２－２　　疑似パケット判別モジュール

疑似パケットは通常の TCP/UDP パケットのフォーマットであるため, 疑似パケットであるか判別することができない．そこで，疑似パケット判別モジュールを PIT 検索の直前に呼び出す. 疑似パケットの判別には DPRP ヘッダにある識別子 DPRP ID を用いた．DPRP ID は 16 バイトの固定値で DPRP 制御パケットであるかどうかを示す値である. 疑似パケットのデータ部の先頭には DPRP ID が記載されているため, この値を比較することで疑似パケットか通常の TCP/UDP パケットかを判別する．

４－２－３　　新 MPIT 生成モジュール

疑似パケットと判別されたパケットは疑似パケットから MPIT を生成するため，新 MPIT 生成モジュールが呼び出される．MPIT は疑似パケットのデータ部にある DPRP ヘッダ以降の情報により作成される．MPIT のオプション部分に疑似パケットの CID と CID のハッシュ値を記載する. CID には疑似パケットのアドレス変換後の情報が記載される．

４-３　　DPRP の呼び出し位置

拡張 DPRP では DPRP の呼び出し位置を変更している. 図 13 に既存の DPRP の GEN の処理の流れ, 図 14 に NAT 機能を実現するデーモン natd を実装した GNAT の処理の流れを示す．

既存の GEN では，どちらのインタフェースで受信した場合も ip_output()で DPRP を呼び出す. GNAT では DPRP の呼び出す位置を変更している. プライベートアドレス側のインタフェースで受信した場合はアドレス変換を行ってから ip_output()で DPRP を呼び出し，グローバルアドレス側のインタフェースで受信した場合は, ip_input()で DPRP の呼び出しを行ってからアドレス変換を行う．ここで，NAT を処理する前に DPRP の処理を実行すると, natd 通過後に ip_input()に処理が渡されたときに，受信時と natd 通過後でパケットの内容が変化しているため, チェックサムが一致しないという問題が発生する. そのためチェックサムの差分だけ再計算するように natd を改造した．

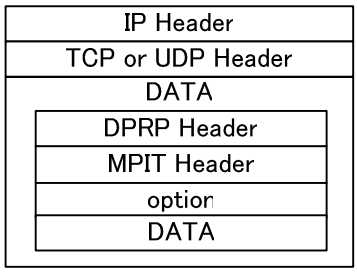

図 13　疑似パケットのフォーマット

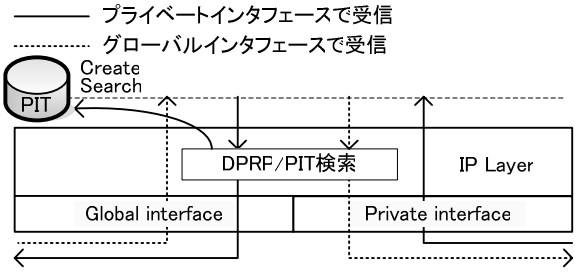

図 14　GEN の処理の流れ

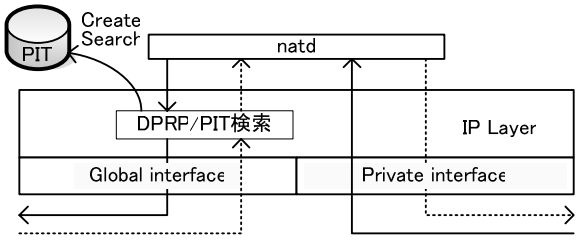

図 15　GNAT の処理の流れ

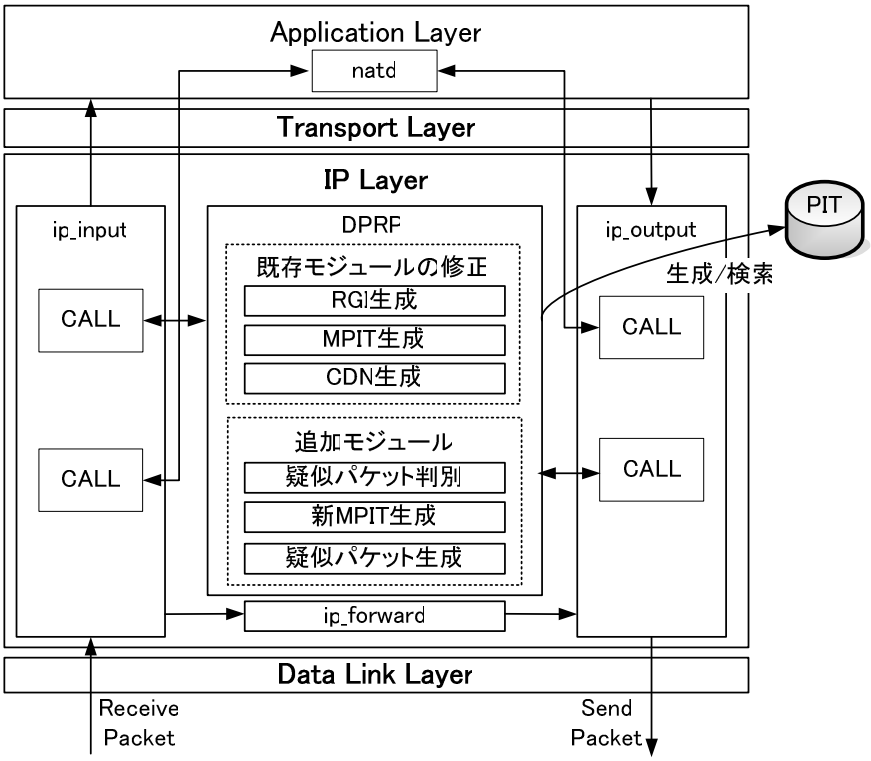

図 12　DPRP の実装概要

第５章　　今後の検討課題

５-１　　今後の検討

第 3 章，第 4 章でプライベートアドレス空間からグローバルアドレス空間へ通信を開始するときの DPRP の動作と実装について述べた．これにより FPN をインターネット上に適応することができる．しかし，今回の改良ではプライベートアドレス空間からの通信開始しか対応しておらず，グローバルアドレス空間からプライベートアドレス空間に通信を開始することはできない．そこで，グローバルアドレス空間からプライベートアドレス空間への DPRP を実現する方法として，GSCIP の一部を構成する NATF と組み合わせることを検討している．

NATF はインターネットからホームネットワークの端末にアクセスすることを想定している．通常，インターネットからホームネットワークにアクセスを行っても，HFW に実装されている NAT の変換テーブルが作成されないため通信を開始することができない．NATF においても今回実装した疑似パケットによる NAT テーブルの強制生成を実現しているため，拡張 DPRP と組み合わせることが容易である．

第６章　　まとめ

本論文では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 DPRP の検討と実装について述べた．DPRP により生成された PIT と NAT でアドレス変換されたパケットの CID が一致するように DPRP の改良を検討した．その検討に基づいて実装を行い，プライベートアドレス空間からグローバルアドレス空間への DPRP ネゴシエーションができることを確認した．今後は別途検討中の NATF と統合することにより，グローバルアドレス空間からプライベートアドレス空間への DPRP の実現について検討を行う．

参　考　文　献

[1] 鈴木秀和, 竹内元規, 加藤尚樹, 増田真也, 渡邊晃 : フレキシブルプライベートネットワークを実現するセキュア通信アーキテクチャ GSCIP の提案，2005-DICOMO2005 シンポジウム

[2] 名城大学理工学部，渡邊研究室，http://www.wata-lab.meijo-u.ac.jp/research/fpn1.html

[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, 情報処理学会研究報告，2005-CSED-28，pp.199-204，March.2005.

[4] 竹内元規，鈴木秀和，渡邊晃 : モバイル端末の移動透過性を実現する Mobile PPC の実装，2005-第 32 回 MBL 研究会発表，

[5] 加藤尚樹，柳沢信成，鈴木秀和，宇佐見庄五，渡邊晃:インターネットから家庭ネットワークへの接続を可能とする NATF プロトコルの検討と実装，2005-情報ワークショップ 2005(WiNF2005)，pp.142-146，September.2005

[6] 柳沢信成，加藤尚樹，鈴木秀和，渡邊晃：異なるプライベートアドレス空間端末の通信(CIPA)の提案

[7] Paul Francis，Ramakrishna Gummadi，IPNL:A NAT-Extend Internet Architecture, 2001-SIGCOMM2001,pp69-80,August.2001

[8] Zoltan Turanyi，Andras Valko,IPv4+4,2002-ICNP2002,pp.290-301,November.2002