推薦論文

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

鈴木秀和[†] 渡邊晃[†]

企業ネットワークにおいてセキュアな通信を実現するために，業務に応じた通信グループを構築することは有効な手段である．しかしこれまでの通信グループ構築方法では部門単位の通信グループと個人単位の通信グループを混在させたり，ネットワーク構成の変化に動的に対応させようとしたりすると管理負荷が増大し実現が難しかった．そこで我々は柔軟性とセキュリティを兼ね備えたネットワークの概念としてFPN（Flexible Private Network）と呼ぶシステムを最終目標とし，FPNを段階的に実現するための一連の通信アーキテクチャとしてGSCIP（Grouping for Secure Communication for IP）を検討している．動的処理解決プロトコルDPRP（Dynamic Process Resolution Protocol）はGSCIPの一部を構成するもので，FPNの実現に必須となる位置透過性，すなわちネットワーク構成の変化に動的に対応する機能を実現するためのものである．DPRPは通信に先立ち通信経路上に存在するGSCIP構成装置（GE）が互いに情報を交換し，端末間の通信に必要な動作処理情報テーブルPIT（Process Information Table）を動的に生成する役割を持つ．DPRPをFreeBSDに実装し，通信開始時に発生するオーバヘッドがTCP/UDP通信にほとんど影響を与えないことを確認した．また，ネットワーク構成が変化した際に発生するコストを評価し，管理負荷を大幅に軽減できることを示した．

Implementation and its Evaluation of Dynamic Process Resolution Protocol in Flexible Private Network

Hidekazu Suzuki[†] and Akira Watanabe[†]

In order to realize secure communications in an enterprise network, an effective way is to form communication groups corresponding to different types of tasks. However, based on conventional forming methods, it has been difficult to realize an effective system due to increased management load in the environment where unit-based and individual-based communication groups coexist or when dynamic adjustment to changes in the network configuration is sought. Thus, we have been studying GSCIP (Grouping for Secure Communication for IP) as communication architecture to realize FPN (Flexible Private Network) that provides both flexibility and security. DPRP (Dynamic Process Resolution Protocol) is a protocol constituting a part of GSCIP to actualize location transparency. In DPRP, all devices existing in the communication path mutually exchange information in advance of communication, and create in each device a PIT (Process Information Table) which is needed for communication between terminals. We have implemented DPRP on FreeBSD and confirmed that the overhead of DPRP does not affect on TCP/UDP communications. We have also proved that management load can be reduced drastically.

1. はじめに

企業ネットワークでは，不正侵入，データの盗聴や漏洩・改竄などに対する様々なセキュリティ対策が重要な課題となっている．外部からの侵入防止に対しては，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を駆使したり，ファイアウォールやIDS（Intrusion Detection System）などと併用したりするなど，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の脅威は組織内部にも存在し，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[1)]．企業ネットワーク内部のセキュリティ対策と

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

本論文の内容は2005年3月のコンピュータセキュリティ研究会にて報告され，CSEC研究会前主査により情報処理学会論文誌への掲載が推薦された論文である．

しては，ユーザ名とパスワードによる簡単な相手認証，アクセス制御程度しか行わ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る．このような状況に対応するため，通信グループの構築は有効な方法である．これはネットワークのインフラ環境をそのまま利用しながら，同一グループのメンバ間の通信の安全を確保する方法であり，以下のように様々な研究が行われている[2)~17)]．

通信グループの構築は個人単位に実現する方法[2)~6)]，ドメイン単位に実現する方法[7)~10)]，および両者を混在させた方法[15)~17)]に分類できる．個人単位に実現する方法はエンド端末にセキュリティ機能を実装する方法で，代表技術として IPsec[18)] トランスポートモードがある．この方法ではきめ細かい通信グループの定義が可能であるが，すべての端末に機能を実装する必要があり，規模が大きくなると管理負荷が大きくなる．ドメイン単位に実現する方法はセキュリティゲートウェイ（以下 SGW）間に安全な通信経路を構築することにより，各 SGW 配下のサブネットを通信グループの単位として定義する方法で，代表技術として VPN（Virtual Private Network）で一般的に使用されている IPsec トンネルモードがある．この方法では SGW だけにセキュリティ機能を実装すればよいが，個人単位の場合のようなきめ細かい通信グループを定義することが難しい．両者の利点をともに生かすためには，個人単位の通信グループとドメイン単位の通信グループを混在できる方式が望ましい．これはたとえば特定のドメインの中に，別のグループに重複帰属する個人が存在するような場合にも対応できる方式である．企業では部門単位の業務グループと部門横断の個人単位の業務グループが混在することがあり，混在型は通信グループを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．また特定の個人がセキュリティドメインの内部と外部の間を移動することによりネットワーク構成が変化するような場合に対しても柔軟に対応できることが望まれる．

IPsec はトランスポートモードおよびトンネルモードの互換性がなく，上記のような混在環境への適用には向いていない．IPsec では通信経路上に同一モードの IPsec 機能を持つ装置が対で存在することが前提となっており，混在環境を実現するにはエンド端末にトランスポートモードとトンネルモードの両方を設定しなければならないなど管理負荷が大きくなるという課題がある．文献 15)，16) は SOCKS[19)] や SSL[20)] を拡張して階層的に構築されたセキュリティドメインにも対応可能とした VPN 構築手法である．セキュリティドメインの最も外側の SGW から内側に向かって 1 ホップずつ SGW を認証していくことにより混在環境に近いシステムを実現している．しかし SGW は次ホップの SGW を特定するために必要な経路情報を管理しなければならず，管理負荷の軽減にはつながっていない．

なお，通信グループを構築する手法としてマルチキャストグループを通信グループとして構成する方法があるが[11)~14)]，これらはグループメンバに一括して安全に情報を配送することが目的であり，本論文で扱う業務に対応した双方向の通信とは用途が異なる．

このような状況に鑑み，我々は柔軟性とセキュリティを兼ね備えた通信グループの構築を可能とする FPN（Flexible Private Network）と呼ぶシステムを最終目標として設定している．FPN とは以下に述べるようなネットワークのあるべき姿を示した概念である．個人単位とドメイン単位の通信グループが混在していることを前提とし，以下のような 3 つの透過性の実現を目指す．すなわち，ネットワークの物理構成が変化してもシステムが動的にその変化を学習して通信グループの関係を維持する位置透過性，通信中に端末が移動して IP アドレスが変化しても，これをアプリケーションから隠蔽して通信を継続する移動透過性，IPv4 における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違いを意識することなく自由に通信ができるアドレス空間透過性である．

一般にセキュリティの向上を図ることによって，ネットワークシステムの運用や管理が難しくなる傾向がある．我々はセキュリティ対策と運用管理負荷の軽減を両立しつつ，FPN を実現する手段として GSCIP（Grouping for Secure Communication for IP；ジースキップ）と呼ぶ一連のセキュア通信アーキテクチャを検討している[21)]．本論文の主題となる動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）[22)~24)] は GSCIP の一機能を構成するものであり，FPN で実現すべき透過性のうち，位置透過性を実現するものである．DPRP はエンド端末間の通信に先立って通信経路上に存在する複数の GSCIP 構成装置（GE）が相互に情報交換し，通信パケットの処理に必要となる動作処理情報テーブル PIT（Process Information Table）を各 GE に自動生成する．ネットワークの物理的構成に変化があっても，GE の保持する動作処理情報が DPRP により動的に再生成されるため，管理者の管理負荷を大幅に軽減できる．

我々は文献 24) において DPRP の原案を提案している．ただし，この時点では FPN，GSCIP の概念が定

義されておらず，DPRP の位置づけが不明確であった．また，通信経路上の中間装置では決定された動作処理情報を無条件に登録していたため，動作処理情報テーブルが偽造される恐れがあった．本論文では，FPN，GSCIP を新たな概念として定義し，DPRP の位置づけを明確にしている．これにともない，通信経路上の GE の情報交換に認証機能を追加し，厳密にシーケンスを定義した．またこのようにして確立した DPRP 仕様を FreeBSD に実装した．GE が送受信する通信パケットを IP 層から抜き出して処理を行い，差し戻すことで既存の処理に影響を与えない方式を実現した．この方式は今後の GSCIP の展開に応用が利く方式であり，シンプルな構造で必要な機能を実現できる．性能評価の結果，DPRP は TCP/UDP 通信にほとんど影響を与えることなく，動作処理情報を生成できることを確認した．また GSCIP/DPRP，IPsec/IKE [25] の導入時やネットワーク構成変化時に発生するコストを比較し，DPRP では大幅に管理負荷を軽減できることを示した．

以降，2 章で FPN と GSCIP について，3 章で DPRP の動作概要について述べる．4 章で実装方式について述べ，5 章で性能評価実験の結果と，管理負荷の評価について述べる．6 章で DPRP の今後の展開について述べ，7 章でまとめる．

2. FPN とその実現方法

2.1 FPN（Flexible Private Network）

FPN とはユビキタス社会に向けて，柔軟性とセキュリティを両立させたネットワークの概念であり，ネットワークのあるべき姿を示したものである．**図 1** に FPN の概念を示す．FPN では個人単位とドメイン単位の要素が混在する環境に対して通信グループの定義ができる．同一通信グループに属する端末間通信はその安全性が保証され，異な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．端末およびドメインは複数の通信グループに重複帰属することが可能で，個人単位やドメイン単位というグループ単位の違いを意識する必要はない．またセキュリティドメインが階層的に構築されていたり，セキュリティドメイン内に異なるグループに属する端末が存在したりするような環境（多段構成ネットワーク）であってもかまわない．FPN はこのようなネットワーク環境を前提とし，さらに以下に示す位置透過性，移動透過性，アドレス空間透過性を実現したものである．

(1) **位置透過性（Location Transparency）**
端末やドメインは移動可能であり，かつ端末が特定のドメインの内外を往復するなどしてネットワーク構成が変わっても，あらかじめ定義されている通信グループの関係は維持される．このとき設定情報をネットワーク管理者が更新する必要はなく，システムが自動的にネットワーク構成の変化を学習する．位置透過性は，端末が通信していない状態（オフライン）での移動を想定したもので，人事異動にともなう引越しや出張先から通常の業務を行えるようにするための機能である．

(2) **移動透過性（Mobility Transparency）**
端末が通信中（オンライン）の状態において移動することもありうる．通信中に移動すると，端末の IP アドレスが変化するため，そのままでは通信が継続できない．これは TCP コネクションや UDP ストリームを管理する情報に通信ペアの IP アドレスが含まれているためである．上位アプリケーションに対しては IP アドレスが変化したことを隠蔽して通信を継続できるようにすることが望ましい．この機能を移動透過性と呼ぶ．

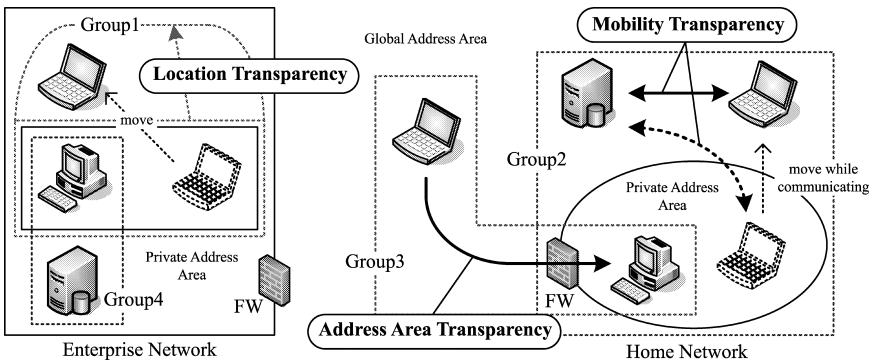

図 1 FPN の概念
Fig. 1 A concept of Flexible Private Network.

(3) **アドレス空間透過性（Address Area Transparency）**

IPv4 の通信環境においては，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存在し，現状では両者の間で自由な通信ができない．これはアドレス変換装置 NAT によりプライベートアドレス空間がグローバルアドレス空間から隠蔽されるためである．NAT と端末が連携してアドレス空間の違いを意識することなく通信できることが望ましい．この機能をアドレス空間透過性と呼ぶ．

このような最終目的を設定することにより，個々の研究テーマの方向性を統一することが可能となる．以下に述べる GSCIP や DPRP は FPN を実現するための手段であり，統一性が保たれている．FPN の適用範囲としては，イントラネット内部，および家庭ネットワークを含むインターネット上が想定され，様々なシステム構成に応じて管理負荷の増加を抑えながらセキュリティの向上を図ることができる．イントラネットでは多段構成ネットワークになることが多く，組織変更，人事異動や出張による場所の移動などが頻繁に行われるため，FPN の概念の適用は有効である．なお，企業ネットワークとインターネットとの間には強固なファイアウォールが設置され，セキュリティポリシにより自由な通信が禁止されているため，両者をまたがる FPN の構築は想定しない．

2.2 GSCIP

FPN の概念を実現するには様々な方式がありうる．GSCIP とは FPN を実現するために検討されているアーキテクチャの名称であり，一連の通信プロトコルの総称である．これらのプロトコルには以下に述べる共通した条件がある．DPRP も GSCIP の一部を構成するプロトコルであり，この条件に従う．**図 2** に GSCIP の基本となる通信グループの定義方法を示す．GSCIP における通信グループの構成要素を GE と呼ぶ．サブネットを構成するルータタイプの 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 for 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 により一括して保護される．GSCIP では同一の暗号鍵を所持する GE の集合を同一通信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 には同一通信グループに所属しない端末との通信をいっさい禁止する閉域モード CL

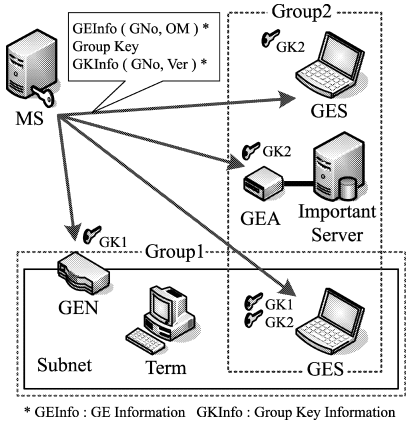

図 2 通信グループの定義方法
Fig. 2 A definition method of communication group.

（Closed Mode）と，異なる通信グループの端末とは平文での通信が可能な開放モード OP（Open Mode）という 2 つの動作モード OM（Operation Mode）がある．一般に GEN や重要サーバの直前に設置される GEA は閉域モード，クライアントとして利用される GES は開放モードが定義される．

GE に必要な情報は管理装置 MS（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．通信グループは IP アドレスに依存することなく論理的に定義し，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もできる．MS では通信グループの定義のほかに，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応して生成され，定期的に更新される．このときグループ鍵 GK には鍵を識別する情報が付与される．この付与される情報をグループ鍵情報と呼び，通信グループ番号とバージョン番号から構成される．GE 情報とグループ鍵情報に含まれている通信グループ番号により，通信グループとグループ鍵 GK を 1 対 1 に対応づけることができる．

GSCIP において位置透過性を実現するには以下のような機能要素が必要である．すなわち，(1) MS から GE への定義情報の配送，(2) GE 間の認証と動作処理情報の生成，(3) 動作処理情報に基づく通信パケットの処理である．これらの機能はそれぞれ独立して定義されており，DPRP は (2) の機能を満たすためのプロトコルである．

なお移動透過性とアドレス空間透過性を実現するに

は別途プロトコルの定義が必要である．これらの実現手段については 6 章で示すように別途議論がなされており，いずれも DPRP の実現方式をベースとして実現できる．

(1) **MS から GE への定義情報の配送**

GE は電源投入時などの初期状態において，MS から GE ごとに定義されている情報を取得する．この情報には GE 情報，グループ鍵 GK とグループ鍵情報，およびシステム全体で共通に用いる共通鍵 CK（Common Key）が含まれる．MS と GE の間は公開鍵を用いた確実な認証と暗号化が実行される．これにより各 GE は必要な情報をあらかじめ保持することができる．グループ鍵 GK および共通鍵 CK は MS から定期的に配送され更新される．

(2) **GE 間の認証と動作処理情報の生成**

端末間の通信開始に先立ち，通信経路上に存在する GE は DPRP により相互に情報交換を行い，通信相手の認証や，通信パケットの処理に必要となる動作処理情報を生成する．GE に定義された通信グループ番号や動作モードの組合せにより，通信パケットに対する処理内容が決まる．

DPRP は通信開始に先立ち実施されるので，ネットワークの物理構成が変化しても GE にはネットワーク構成に応じた動作処理情報が自動生成され，位置透過性が実現される．

(3) **動作処理情報に基づく通信パケットの処理**

TCP/UDP パケットは (2) で決定した動作処理情報に基づいて処理される．処理内容が “Encrypt”，“Decrypt” の場合，グループ鍵 GK で暗号化/復号される．“Transparent” の場合，パケットは透過中継される．“Discard” の場合，パケットは破棄される．

本システムでは管理者が MS で GE 情報の変更を行うことにより，通信グループのメンバ構成を管理する．すなわち，ユーザが自発的に通信グループへ参加したり，離脱したりすることはできない．通信グループの変更処理は組織変更や人事異動が発生した際に行われ，これらは一般に 4 月 1 日付けなどのように日単位であるため，鍵の定期更新と同期させて実行することが可能である．鍵の更新間隔は管理者が定めることができるが，一般に 24 時間間隔で夜間に実施するなどと決めておく．これにより GE は電源投入時に確実に最新の鍵を取得することができる．また GE が保持する鍵の更新は通信中に行うことも可能である．この場合，すべての GE の鍵更新が完了するまでに，新旧の鍵が混在する時間帯が発生してしまうが，鍵のバージョン番号により誤った鍵で通信しないように考慮されている．通信中に鍵が更新された場合，GE は動作処理情報を初期化する．これにより次の通信開始時には必ず GE 間で DPRP ネゴシエーションが実行され，グループ鍵情報の交換を行う．古い鍵を持つ GE はネゴシエーションを中止して，MS に対して新しい鍵を要求する．この方法によれば通信中においても鍵の更新が可能で，かつ通信中の GE に一時的な遅延が発生するだけで済むため，通信グループのメンバ数に十分スケールできる．出張などによりユーザの場所が変化した場合は，ユーザの所属自体が変更されるわけではないため，鍵の更新は必要ない．

MS は通常，イントラネット内に 1 台設置される．ただし通信グループの規模が大きくなる場合は，MS の処理負荷が増大するため，MS を分散して設置することが望ましい．この場合は，MS を DNS のようにツリー構造で管理し，通信グループ番号を階層化するなどにより，管理情報の一貫性を確保する必要がある．

3. 動的処理解決プロトコル DPRP

3.1 プロトコル定義と動作概要

DPRP は端末間の通信開始に先立ち，通信経路上のすべての GE 間で設定されている情報を相互に交換して，通信パケットの処理内容を決定し，動作処理情報テーブル PIT を生成する．PIT は送信元/宛先 IP アドレスとポート番号，プロトコル番号，処理内容，グループ鍵情報などの情報から構成されている．このうち動作処理情報は処理内容およびグループ鍵情報のことを示す．

図 3 にネットワーク構成例と GE 定義情報を示す．図 3 は GES1 が GEN により構成された部門サブネットワーク NET1（Group1）の内部に存在し，かつ GES2 へのアクセスが許可されているグループ（Group2）に所属している状況を想定している．GES1 は NET1 の外部 NET2 へ移動した場合，部門内の一般端末 Term1 との通信が可能なように GK1 もあらかじめ保持している．GES2 は他のグループからの通信を拒否するために閉域モード，GES1 は同一部門の一般端末とも通信するため開放モード，GEN は部門内の一般端末を保護するために閉域モードがそれぞれ定義されている．各 GE が所属する通信グループ番号とそれに対応するグループ鍵 GK は，すでに MS から配送されている．ここで図 3 の状態において端末間に生成されるべき動作処理情報を**表 1** に示す．GES1 と GES2 間の通信に着目すると，GES1，GES2 は通信パケットを GK2 で暗号化/復号，GEN は通信パケットを透過中継する．DPRP はこのような動作処理情

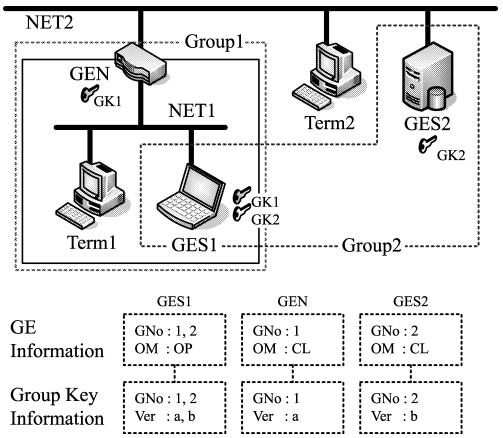

図 3 ネットワーク構成図と GE 定義情報
Fig. 3 Network model and GE definition information.

表 1 端末間の通信可否と各 GE が保持する動作処理情報
Table 1 The propriety between terminals and Process Information which each GE holds.

通信ペア		通信	動作処理情報		
		可否	GES1	GEN	GES2
GES1	GES2	○	E2	T	E2
GES1	Term1	○	T	—	—
GES1	Term2	×	D	D	—
GES2	Term1	×	—	D	D
GES2	Term2	×	—	—	D
Term1	Term2	×	—	D	—

Ex: Encrypt/Decrypt by GKx T: Transparent
D: Discard —: No Record

報を自動的に生成する役割を持つ．

以下に本論文で用いる記号を定義する．

- n：通信経路上に存在する GE の数
- i：通信経路上における GE の順番（$1 \leq i \leq n$, $i = n$：始点 GE, $i = 1$：終点 GE）
- HDR：DPRP ヘッダ
- C：通信識別子
- N_i：i 番目の GE が RGI に記載する通知情報
- P_i：i 番目の GE に関する動作処理情報
- $DPRP_{ID}$：DPRP 制御パケットであることを示す識別子（固定値）
- NID：セッションごとに異なるネゴシエーション識別子（乱数値）
- $ICMP_{ID}$：ICMP の識別子
- $ICMP_{SEQ}$：ICMP のシーケンス番号
- IP_{SRC}/IP_{DST}：トリガパケットの送信元/宛先 IP アドレス
- PRT_{SRC}/PRT_{DST}：トリガパケットの送信元/宛先ポート番号
- PROTO：トリガパケットのプロトコル番号
- UID：GE を使用しているユーザのユーザ ID
- aID：動作処理情報の認証に用いる認証情報（乱数値）
- OM：GE に定義された動作モード（OP/CL）
- CNT：GE が保持するグループ鍵の数
- PROC：決定した処理内容（Encrypt/Decrypt/Transparent/Discard）
- STS：CDN においてネゴシエーションの成功，失敗を示す確認情報（OK/NG）
- CKI：共通鍵 CK の鍵情報
- GKI：グループ鍵 GK の鍵情報
- DGK/DGKI：決定したグループ鍵/鍵情報
- h(M)：メッセージ M の MD5 ハッシュ値
- $M1 \parallel M2$：メッセージ $M1$ とメッセージ $M2$ の結合
- $K(IV, M)$：初期ベクトル値を IV としてメッセージ M を鍵 K で暗号化した値

図 4 に DPRP ネゴシエーションと処理内容を示す．GES1 は TCP/UDP パケットを送受信する際，自身が保持する PIT の内容を検索する．検索の結果，GES1 と GES2 間の動作処理情報がない場合，TCP/UDP パケットを一時的に待避させてから DPRP ネゴシエーションを開始し，PIT を生成する．以後，DPRP を開始するきっかけとなったパケットをトリガパケットと呼ぶ．

DPRP は ICMP ECHO パケットをベースとした制御パケットを用いてネゴシエーションを行う．両端末間の通信経路上には複数の GE が存在しうるが，両通信端末に最も近い GE をそれぞれ始点 GE，終点 GE と呼び，それ以外を中間 GE と呼ぶ．制御パケットは共通鍵 CK を使って暗号化され，安全に情報の交換を行う．制御パケットには以下に示す 4 種類のパケットがある．

(1) **DDE（Detect Destination End-GE）**

HDR, CK(IV1, C)
HDR=$DPRP_{ID}$, NID
C=IP_{SRC}, IP_{DST}, PRT_{SRC}, PRT_{DST}, PROTO
IV1=h(CKI ‖ NID ‖ $ICMP_{ID}$ ‖ $ICMP_{SEQ}$)

ネゴシエーションを開始する GE（GES1）は終点 GE を決定するために DDE を通信相手（GES2）に向けて送信する．DPRP ヘッダに記載する NID は DDE 生成時にランダムに生成される．DDE にはトリガパケットの送信元/宛先 IP アドレスとポート番号，プロトコル番号の情報が記載される．DDE の宛先が GE

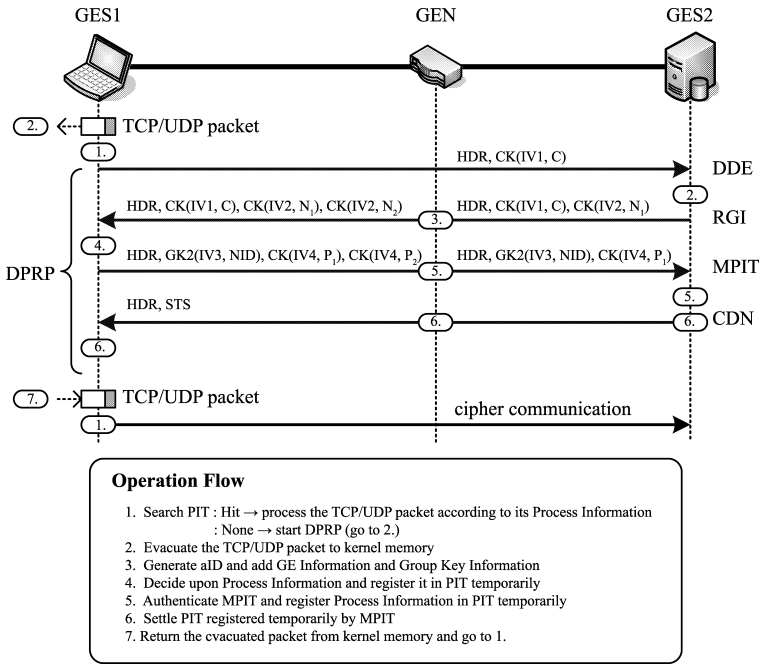

図 4 DPRP ネゴシエーションと処理内容
Fig. 4 DPRP Negotiation and operations.

の場合は，DDE を受信した GE が終点 GE となる．もし DDE の宛先が一般端末であった場合，一般端末からの応答パケット ICMP ECHO REPLY を最初に受信した GE が終点 GE となる．

(2) **RGI（Report GE Information）**

HDR, CK(IV1, C), {CK(IV2, N_i) | $i = 1, \cdots, n-1$}
N_i=UID_i, aID_i, OM_i, CNT_i, {GKI_c | $c = 1, \cdots, CNT_i$}
IV2=h(CKI ‖ NID ‖ $ICMP_{ID}$ ‖ $ICMP_{SEQ}$ ‖ IP_{DST})

DDE によって決定した終点 GE（GES2）は始点 GE を決定するため，また通信経路上の GE に定義されている情報を通知するために，RGI をトリガパケットの送信元（GES1）に送信する．RGI には自 GE に定義されている GE 情報，グループ鍵情報，認証情報 aID などの情報が記載される．ここで aID は乱数で，ユーザ ID や NID とともに PIT に一時的に登録しておき，RGI 以降の DPRP 制御パケットを認証するために利用される．中間 GE（GEN）が RGI を受信すると，自 GE に対して定義されている情報を RGI に追加する．始点 GE は終点 GE と同様の原理で決定される．始点 GE が RGI を受信すると，通信経路上の全 GE の定義情報を取得できる．始点 GE はこれらの情報をもとに，すべての GE の動作処理情報を決定することができる．

(3) **MPIT（Make Process Information Table）**

HDR, DGK(IV3, NID), {CK($IV4_i$, P_i) | $i = 1, \cdots, n-1$}
P_i=UID_i, aID_i, $PROC_i$, DGKI
IV3=h(DGKI ‖ NID ‖ $ICMP_{ID}$ ‖ $ICMP_{SEQ}$)
$IV4_i$=h(CKI ‖ NID ‖ $ICMP_{ID}$ ‖ $ICMP_{SEQ}$ ‖ N_i)

始点 GE（GES1）は通信経路上の各 GE に決定した動作処理情報を伝えるため，自らの動作処理情報を PIT に仮登録してから MPIT を終点 GE（GES2）に送信する．MPIT には決定した動作処理情報と，決定したグループ鍵で暗号化された NID が記載される．各 GE が MPIT を受信すると，自 GE に該当する動作処理情報を取得する．ここで取得した NID，ユーザ ID，aID と PIT に登録しておいた情報を比較して認証を行い，正常なら動作処理情報を PIT に仮登録する．

(4) **CDN（Complete DPRP Negotiation）**

HDR, STS

終点 GE（GES2）は各 GE に PIT が生成され，DPRP ネゴシエーションが完了したことを通知し，MPIT で

GES1

IP_{SRC}	IP_{DST}	PRT_{SRC}	PRT_{DST}	PROTO	PROC	GNO	VER
192.168.1.10	192.168.2.20	49230	21	tcp	Encrypt	2	b
192.168.2.20	192.168.1.10	21	49230	tcp	Decrypt	2	b

GEN

IP_{SRC}	IP_{DST}	PRT_{SRC}	PRT_{DST}	PROTO	PROC	GNO	VER
192.168.1.10	192.168.2.20	49230	21	tcp	Transparent	−	−
192.168.2.20	192.168.1.10	21	49230	tcp	Transparent	−	−

GES2

IP_{SRC}	IP_{DST}	PRT_{SRC}	PRT_{DST}	PROTO	PROC	GNO	VER
192.168.1.10	192.168.2.20	49230	21	tcp	Decrypt	2	b
192.168.2.20	192.168.1.10	21	49230	tcp	Encrypt	2	b

図 5 GES1-GES2 間に生成される PIT の一例
Fig. 5 The example of PITs which are created between GES1 and GES2.

仮登録された PIT を確定するために，確認情報 STS を OK として CDN を始点 GE（GES1）に送信する．DDE を送信した GE が CDN を受信すると，待避していた TCP/UDP パケットを復帰させることにより TCP/UDP 通信が開始される．以後の通信は PIT の内容に基づいて処理される．

図 5 に GES1-GES2 間に生成される PIT を示す．これは GES1，GES2 の IP アドレスを 192.168.1.10, 192.168.2.20 として，GES1 が GES2 へ FTP 接続した場合に生成される PIT の一例である．

3.2 安 全 性

DPRP ヘッダに記載される NID はセッションごとに異なる乱数値で，PIT の生成過程から削除されるまで PIT に登録される．DPRP 制御パケットを受信した際，ICMP ヘッダに記載されているシーケンス番号と NID をチェックし，リプレイ攻撃に対処する．DPRP 制御パケットを CK で暗号化する際に必要となる初期ベクトル値 IV には ICMP のシーケンス番号や NID などの情報を含む．したがって，DPRP 制御パケットを改竄しても復号時に異常を検出することが可能である．また MPIT を受信した GE は該当する動作処理情報を復号する際，IV を求めるために PIT に一時的に登録していた aID や NID の情報，すなわち RGI で通知した情報 N_i を用いる．したがって第三者が不正な MPIT により，意図的に GE 間の動作処理情報を生成したり，セッションをハイジャックしたりすることはきわめて困難である．さらに DPRP ネゴシエーションの過程において不正が検出された場合，CDN により NG を報告し，仮登録中であった PIT をクリアすることができる．以上の処理により，PIT は安全に GE 内に生成することができる．

4. 実 装 方 式

DPRP は IP 層に実装される．GSCIP を実現するモジュール群のことを GPACK（Gscip PACKage）と呼び，DPRP はその一部を構成する．OS には IP 層の情報が豊富な FreeBSD を選択した．**図 6** に GPACK の実装概要を示す．GPACK は IP 層の入出力関数 `ip_input()`，`ip_output()` から呼び出され，DPRP 対応の処理などを行い，パケットを元の場所に差し戻す．この方式では既存の IP 層の処理は GPACK の影響をいっさい受けることがない．DPRP ではトリガとなった TCP/UDP パケットを一時待避するが，待避パケットをそのままカーネルに残しておき，一連の DPRP 処理が終了した時点でカーネル内から直接送信する．DPRP により生成される PIT や，MS から配送された共通鍵 CK およびグループ鍵 GK の保存領域はカーネルメモリ空間に作成し，不要になったら削除する．これらの処理はすべてカーネル処理で閉じており，暗号鍵が処理過程で漏洩する可能性はきわめて低い．PIT はハッシュテーブルとして実装する．ハッシュの検索キーは，通信識別子，すなわち送受信パケットの送信元/宛先 IP アドレスとポート番号，プロトコル番号である．PIT レコードにはカウンタ値が定義されており，カーネルタイマ処理により減少していく．PIT レコードが参照されるたびに，カウンタ値は初期値に戻される．一定時間参照されていない PIT レコードはカウンタ値が 0 になり端末間の通信が行われていないと判断されて削除される．削除までの時間は ARP キャッシュと同等の約 5 分とした．

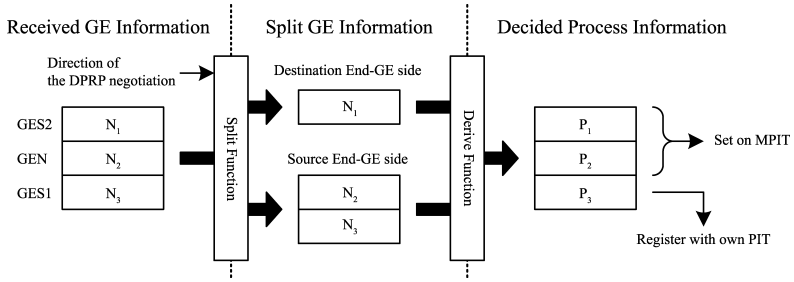

図 8 動作処理情報の決定プロセス
Fig. 8 A decision process of Process Information.

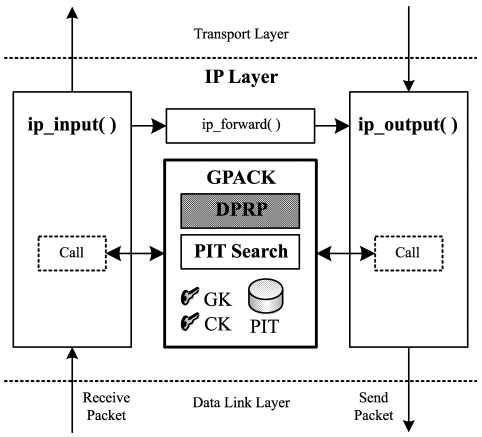

図 6 GSCIP の実装
Fig. 6 Implementation of GSCIP.

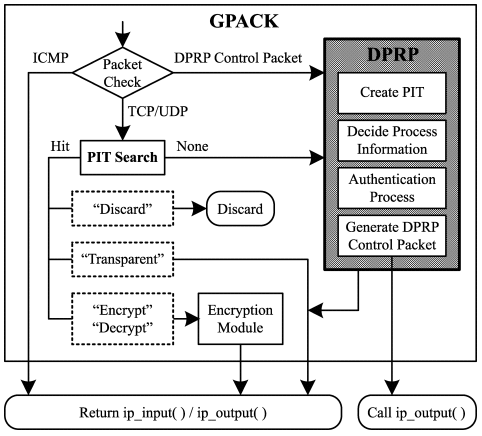

図 7 GSCIP モジュールの処理フロー
Fig. 7 Process flow of GSCIP module.

図 7 に GSCIP モジュールの処理フローを示す．GPACK は受け取った通信パケットの種類を判別してから，適切なモジュールを選択し実行する．送受信パケットが TCP/UDP の場合，PIT の検索を行う．該当する PIT レコードが存在した場合，PIT の内容に従ってパケットの処理を実行する．該当する PIT レコードが存在しない場合，DPRP モジュールに処理が渡され，DPRP モジュールは DDE を作成して `ip_output()` に渡し送信する．その後，ネゴシエーションのトリガとなった TCP/UDP パケットを待避させる．送受信パケットが ICMP の場合，GPACK で処理を行わずに IP 層へ戻す．送受信パケットが DPRP 制御パケットの場合，DPRP モジュールに渡され，PIT の生成，動作処理情報の決定，認証，DPRP 制御パケットの生成などのプロセスを実行する．DPRP 制御パケットは生成後に共通鍵 CK により暗号化される．暗号アルゴリズムは AES（Advanced Encryption Standard）[26] CBC（Cipher Block Chaining）モード，鍵長は 128 bit とした．暗号ライブラリには FreeBSD 5.3-Release に実装されている OpenSSL [27]（Version 0.9.7d）を用いた．**図 8** に動作処理情報の決定プロセスを示す．RGI により取得した通知情報 N_i は，RGI 転送中に設定されたネゴシエーションの方向情報により，始点 GE 側と終点 GE 側の情報に分割される．方向情報とは DDE が GEN の配下から出る方向なのか，配下へ入る方向なのかを示す情報である．GE 情報の分割後，始点 GE 側の情報と終点 GE 側の情報を比較して動作処理情報を決定する．

5. 評　　価

5.1 DPRP の性能

100BASE-TX の Ethernet において，GES1 が GES2 に FTP 接続を行う場合の DPRP の性能を測定した．性能測定に使用した各装置仕様は CPU が Pentium4 2.4 GHz，メモリが 512 MB である．DPRP ネゴシエーションのオーバヘッド時間および DPRP モジュールの内部処理時間を測定した．また，GSCIP では TCP/UDP パケットを送受信する際，必ず PIT 検索を行うため通信性能に影響が出る可能性がある．そのため PIT 検索のオーバヘッドを調査するため，

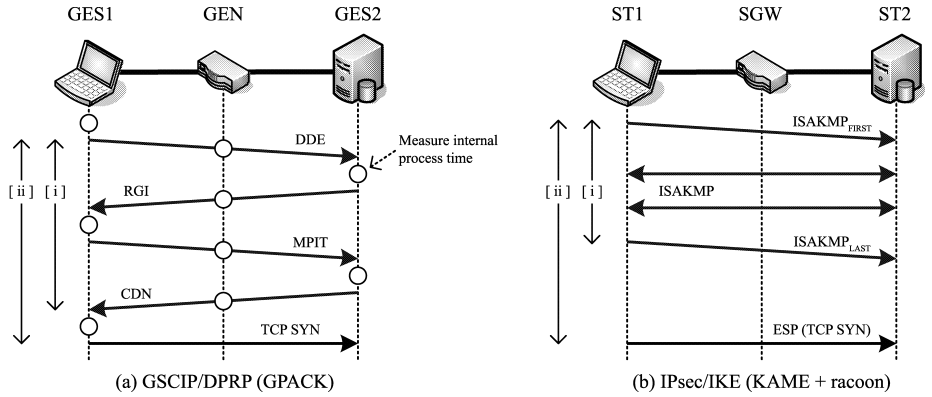

図 9 測定ポイント
Fig. 9 Measurement points.

GSCIP 実装時と未実装時の FTP スループットを暗号化しない状態で比較した．各 GE はあらかじめ通信グループ番号，共通鍵 CK およびグループ鍵 GK を保持しているものとした．

(1) **ネゴシエーションのオーバヘッド**

オーバヘッドの測定には，ネットワークアナライザ Ethereal[28] を用いた．参考のために，同一条件下における IPsec/IKEv1[25] の処理時間も測定した．FreeBSD に実装されている KAME[29] および IKE デーモン racoon[30] を使用し，事前共有鍵方式のメインモードで行った．IKEv2[31] は現時点では安定して動作するソフトウェアが存在しないため今回は測定を見送った．測定対象は DPRP では**図 9** (a) に示す DPRP ネゴシエーション時間（DDE〜CDN 間）`[i]` と，TCP の最初の SYN パケットが GES1 から送信されるまでの時間（通信開始までの時間）`[ii]` である．一方，IKE では図 9 (b) に示す IKE ネゴシエーション時間（$\text{ISAKMP}_{\text{FIRST}}$〜$\text{ISAKMP}_{\text{LAST}}$ 間）`[i]` と，通信開始までの時間 `[ii]` である．図 9 (b) における ST1，ST2，SGW はそれぞれ GES1，GES2，GEN の位置に該当し，IPsec 機能を実装した装置である．それぞれのオーバヘッド測定結果を**表 2** に示す．DPRP のネゴシエーション時間は 1.01 ミリ秒，通信開始までの時間は 1.04 ミリ秒となった．それに対し，IKE のネゴシエーション時間は 1105.95 ミリ秒（約 1 秒），通信開始までの時間は 2994.03 ミリ秒（約 3 秒）となった．

(2) **DPRP モジュールの内部処理時間**

内部処理時間の測定には RDTSC (Read Time-Stamp Counter)[32] を用いた．測定箇所は図 9 (a) に示す ○ 印の部分である．GPACK モジュールの処理時間と DPRP 制御パケットの暗号処理時間を**表 3** に示す．GES1-GES2 間のネゴシエーション全体の内部処理時間は 203.34 マイクロ秒となった．またこのうち，約 30%が DPRP 制御パケットの暗号化/復号，ならびに認証処理に要する時間であった．中間 GE に該当する GEN の処理時間は 44.32 マイクロ秒となった．

表 2 オーバヘッドの測定結果
Table 2 Measurement results of overheads.

	GSCIP/DPRP	IPsec/IKE
`[i]` ネゴシエーション時間	1.01	1105.95
`[ii]` 通信開始までの時間	1.04	2994.03

Unit:[ms]

表 3 GE における内部処理時間
Table 3 Internal process time of GEs.

	GES1	GEN	GES2	合計
DPRP 処理全体	96.59	44.32	62.43	203.34
うち暗号処理部分	23.57	18.86	19.20	61.63

Unit:[μs]

表 4 FTP スループットの違い
Table 4 Difference of FTP throughput.

	GSCIP 実装時	GSCIP 未実装時
スループット	82.15	82.31

Unit:[Mbps]

(3) **FTP のスループット値**

FTP のスループット値は FreeBSD の FTP クライアントソフトに表示される値を採用した．測定方法は GES2 から 500 MB のファイルをダウンロードした．GPACK 実装時と未実装時における FTP スループット値を**表 4** に示す．GSCIP 実装時では 82.15 Mbps，GSCIP 未実装時では 82.31 Mbps となった．

これらの測定結果より，DPRP は通信開始に先立つネゴシエーションであることを考えると，TCP 通信にはほとんど影響を与えることがないといえる．これに対し IKE では，DPRP の測定結果と比べて 3 桁以上遅い結果となっている．これは GSCIP と IPsec

表 5 設定内容と項目数の比較
Table 5 Comparison of setting parameters and its numbers.

GSCIP/DPRP			
	グループ鍵		GE 情報
設定内容	通信グループ番号 バージョン番号 鍵データ		動作モード（OP/CL） 通信グループ番号
項目数	3		2
IPsec/IKE			
	共有秘密鍵	セキュリティポリシ	IKE
設定内容	通信相手識別子 鍵データ	通信ペア識別子（送信元，宛先） 処理内容（IPsec/Discard/None） プロトコル（ESP/AH） モード（Transport/Tunnel） SGW ペア識別子　など	通信相手識別子 交換モード（main/aggressive） 暗号化アルゴリズム ハッシュアルゴリズム 認証方式　など
項目数	2	Discard/None　:8 IPsec,Transport:14 IPsec,Tunnel　:16	12

の通信開始時における認証の考え方の違いに起因している．GSCIP では GE の起動時に MS との間で公開鍵を用いた認証を行い，あらかじめグループ鍵 GK を取得しておく．これは認証機能の一部を前処理していることに相当する．通信開始時は DPRP による共有秘密鍵 GK を用いたエンド端末間認証が行われるため，処理時間が短くてすむ．一方，IPsec は通信開始時にエンド端末間で事前共有秘密鍵や公開鍵，ディジタル署名などで認証し，かつ通信パケットを暗号化する共有鍵を DH 鍵交換[33] により別途生成している．このため，GSCIP と比べて通信開始時の認証に関わるオーバヘッドが大きい．

また通信開始までの時間については上記以上の大きな差が生じている．これは GSCIP/DPRP と IPsec/IKE の実装モデルの違いに起因している．DPRP は実装がシンプルなためすべての処理をカーネルで実行でき，カーネル内でのパケットの待避や復帰などの処理が可能である．そのため TCP の再送処理が発生することがなく，わずかな遅延で TCP 通信を開始することができる．一方，IKE は汎用的な利用を想定しているため，アプリケーションレベルで動作させており，カーネルに実装されている KAME とリアルタイムに連携することが難しい．その結果，パケットを破棄して IKE ネゴシエーションを開始する．すなわち，最初のパケットは TCP の再送処理に頼ることで通信を実現している．そのため TCP の再送タイムアウト RTO の初期値である約 3 秒後に暗号通信が始まっている．

FTP スループットでは，GSCIP 実装時と未実装時の差は 0.2%程度であった．すなわち，GSCIP による PIT 検索のオーバヘッドは十分許容できる範囲である．DPRP は IP 層で動作するプロトコルであるため，UDP 通信の場合においても上記結果と同等の性能を得ることができる．

5.2 管理負荷

FPN で目指す位置透過性を GSCIP と IPsec で実現する場合に発生する管理負荷を評価する．評価項目は（1）初期管理負荷,（2）ネットワークの構成変化時に発生する管理負荷，および（3）通信グループのメンバ構成変化時に発生する管理負荷とし，各管理負荷を算出する．ここでの構成変化とは引越し，人事異動や出張などオフラインでの移動による変化であり，通信中の移動は考えない．

GSCIP の場合と IPsec の場合における設定内容と，各設定 1 つあたりに必要な項目数の比較を**表 5** に示す．GSCIP ではグループ鍵と GE 情報の設定が必要で，各設定に必要な項目数はそれぞれ 3，5 である．一方，IPsec では事前にエンド端末で共有する秘密鍵，どの通信パケットに対してどのような処理を行うかを定めたセキュリティポリシ，および IKE の設定が必要である．セキュリティポリシは双方向定義する必要があり，処理内容やモードに応じて項目数が異なる．各設定に必要な項目数はそれぞれ 2，8〜16，12 である．IPsec における共有秘密鍵，セキュリティポリシ，IKE の各設定には通信相手識別子，通信ペア識別子，および自端末識別子の項目が含まれており，管理者およびユーザはこれらの項目に IP アドレスまたは FQDN などのユーザ ID を設定する必要がある．

(1) 初期管理負荷

図 3，表 1 で表される通信環境を GSCIP および IPsec で実現するために，各装置に必要な初期管理負荷を**表 6** に示す．ここで初期管理負荷とは表 5 で示した設定 1

表 6 初期管理負荷
Table 6 Initial management loads.

GSCIP/DPRP				
	グループ鍵		GE 情報	合計
GES1	6		2	8
GEN	3		2	5
GES2	3		2	5
IPsec/IKE				
	共有秘密鍵	セキュリティポリシ	IKE	合計
ST1	4	14（Transport:14）	12	30
SGW	2	16（None:8, Discard:8）	12	30
ST2	2	22（Transport:14, Discard:8）	12	36

つあたりに必要な項目数に，実際に設定する数を掛けた値である．GSCIP の場合，GES1 は 2 つの通信グループに所属するため，初期管理負荷の合計は 8 となる．同様に GEN，GES2 の初期管理負荷はそれぞれ 5 となる．一方，IPsec の場合，ST1 は 2 個の共有秘密鍵を保持し，ST2 に対するトランスポートモードのセキュリティポリシと IKE の設定が必要である．そのため初期管理負荷はそれぞれ 4，14，12 となり，ST1 の初期管理負荷の合計は 30 となる．同様に SGW，ST2 の初期管理負荷は 30，36 となる．GSCIP は GE が所属するグループ数の増加にともない初期管理負荷も増加するが，その増分はわずかである．これに対して IPsec はトランスポートモードのセキュリティポリシを 1 つ設定するたびに，初期管理負荷が両エンド端末および通信経路上に存在する SGW にそれぞれ 14，8 ずつ増加する．

(2) **ネットワーク構成変化時に発生する管理負荷**

図 3 において GES1（IPsec では ST1）が NET1 から NET2 へ移動した際，端末間で生成されるべき動作処理情報が表 1 に対してどのように変化するかを**表 7** に示す．またこのような変化に対して発生する管理負荷を**表 8** に示す．GSCIP では端末が移動しても，そのつど DPRP により動作処理情報を新しく生成するため，ユーザや管理者が行う作業はいっさい発生しない．一方，IPsec で同様の構成を実現しようとすると，ST1 は移動により IP アドレスが変化するため，通信を識別するための識別子を変更する必要がある．ST1 は ST2 に対するトランスポートモードのセキュリティポリシと IKE の設定を変更する必要があり，その管理負荷はそれぞれ 4，1 となる．さらに同一部門の Term1 と通信するために，SGW に対するトンネルモードのセキュリティポリシの設定を追加する必要がある．その管理負荷は 16 となり，ST1 の管理負荷の合計は 21 となる．

図 3 のネットワーク環境はシンプルな構成であるため，移動後の ST1 と Term1 間の通信経路上に SGW が 1 台しか存在しないが，実際の環境を想定した場合，SGW の台数が 2 台以上存在することも十分考えられる．この場合，さらに設定追加にともなう管理負荷が増加する．

表 7 ネットワーク構成変化時の動作処理情報の変化
Table 7 The change of Process Information when the network configuration changes.

通信ペア		通信可否	動作処理情報 GES1	GEN	GES2
GES1	GES2	○	E2	T→—	E2
GES1	Term1	○	T→E1	—→E1	—
GES1	Term2	○	D→T	D→—	—
GES2	Term1	×	—	D	D
GES2	Term2	×	—	—	D
Term1	Term2	×	—	D	—

Ex：Encrypt/Decrypt by GKx　T：Transparent
D：Discard　—：No Record

(3) **通信グループのメンバ構成変化時に発生する管理負荷**

図 3 において Group1 に所属し，開放モードに定義された GES3（IPsec では ST3）を新たに NET1 に配置する場合に発生する管理負荷を**表 9** に示す．GSCIP では管理者が MS において GES3 の GE 情報を追加定義する．GES3 は電源投入時に定義された GE 情報とグループ鍵を MS から取得し，自動的に設定される（合計 5）．後は DPRP により動作処理情報を自律的に生成するため管理負荷はほとんど発生しない．一方，IPsec では ST3 に共有秘密鍵，セキュリティポリシ，および IKE の設定を行う必要がある（合計 30）．さらにメンバ構成の変化が発生する通信グループのメンバ全員（ST1，SGW）に共有秘密鍵，セキュリティポリシの設定を追加する必要があり，大きな管理負荷（ST1 の合計 16，SGW の合計 2）発生する．実際の環境では 1 つの通信グループに大勢のメンバがいることが想定されるため，さらに設定追加にともなう管理負荷が増加する．

表 8 ネットワーク構成変化時の管理負荷
Table 8 Management loads when the network configuration changes.

GSCIP/DPRP				
	グループ鍵		GE 情報	合計
GES1	0		0	0
GEN	0		0	0
GES2	0		0	0
IPsec/IKE				
	共有秘密鍵	セキュリティポリシ	IKE	合計
ST1	0	20（変更 Transport:4，追加 Tunnel:16）	1（変更：1）	21
SGW	1（変更：1）	16（追加 Tunnel:16）	0	17
ST2	1（変更：1）	4（変更 Transport:4）	0	5

表 9 メンバ構成変化時の管理負荷
Table 9 Management loads when member composition changes.

GSCIP/DPRP				
	グループ鍵		GE 情報	合計
GES1	0		0	0
GEN	0		0	0
GES2	0		0	0
GES3	3		2	5
IPsec/IKE				
	共有秘密鍵	セキュリティポリシ	IKE	合計
ST1	2	14 (Transport:14)	0	16
SGW	2	0	0	2
ST2	0	0	0	0
ST3	4	14 (Transport:14)	12	30

これらのことから，GSCIP は初期導入時や，端末の移動にともなう管理負荷が発生しないため，位置透過性の実現と FPN の重要な目的である運用管理負荷の軽減を両立しているといえる．

6. DPRP の今後の展開

FPN の目指す機能として位置透過性のほかに，移動透過性とアドレス空間透過性がある．GSCIP にはこれらに対応するプロトコルとして，移動透過性に対して Mobile PPC（Mobile Peer-to-Peer Communication protocol）[34),35)]，アドレス空間透過性に対して NATF（NAT Free protocol）[36)~38),☆]がある．

Mobile PPC は通信中の端末が移動後に移動前後の IP アドレスなどの情報を相手端末と交換し，以後の通信を IP 層でアドレス変換する．IP 層より下位層では移動後の IP アドレスで正しくルーティングされ，IP 層より上位層に対しては IP アドレスの変化が隠蔽されるため，移動透過性を実現することができる．

NATF はグローバルアドレス環境からプライベートアドレス環境に対して通信の開始を可能とするためのプロトコルである．グローバルアドレス空間側の端末（外部端末）は NAT に対して，プライベートアドレス空間の端末（内部端末）に関する情報を含んだネゴシエーションを行い，NAT テーブルを強制的に生成する．外部端末側では NAT テーブルに合わせてポート番号変換テーブルを生成し，送受信するパケットに対して IP 層でポート番号変換する．これにより外部端末から内部端末への通信開始が可能となり，アドレス空間透過性を実現できる．

Mobile PPC，NATF とも DPRP と同じ IP 層で動作するため，プロトコル間の連携をとることが容易である．また Mobile PPC，NATF のネゴシエーションには端末どうしで情報を交換，共有するという DPRP と共通動作を含んでおり，DPRP の実装方式をそのまま利用することが可能である．今後は DPRP の実装技術を応用して GSCIP に Mobile PPC と NATF の機能を統合していくことにより，位置透過性に加えて移動透過性とアドレス空間透過性を同時に実現できると考えられる．アドレス空間透過性については，家庭のプライベートアドレス空間とインターネット上の端末との間で通信グループを定義できることを意味しており，FPN の適用範囲を大きく広げることが可能になると考えられる．

検討課題としては以下のようなものがあげられる．GSCIP では定期的にグループ鍵を更新することを想定しているため，通信グループのメンバ数 n が増加

☆ 現在は NAT-f（NAT-free protocol）として検討中である．

すると鍵配送におけるオーバヘッドの増加が懸念される．これについてはメンバ数 n に対して $\log n$ の通信でよい方式や，n に依存しない方式がすでに知られている[39),40)]．また鍵更新が頻繁でかつ時間がかかるため，DoS 攻撃の対象にされる危険性があり，今後検討が必要と考えられる．

7. むすび

ユビキタス社会におけるネットワークのあるべき姿を示す FPN の概念，FPN を実現するためのアーキテクチャGSCIP，および GSCIP の中でも重要な位置づけを占める DPRP についてそれぞれの概要と関係を述べた．DPRP は FPN の前提となる個人単位とドメイン単位の通信グループが混在する環境において，端末間の認証と暗号通信に必要な動作処理情報を動的に生成し，位置透過性を実現することができる．FreeBSD の IP 層を改造し，DPRP モジュールを組み込んだ．GE が送受信する通信パケットを IP 層から抜き出して処理を行い，差し戻すことで既存の処理に影響を与えない方式を実現した．DPRP の性能を測定した結果，高速かつ安全に通信相手を認証することが可能で，暗号通信に必要な動作処理情報を動的に生成できることを確認した．IPsec/IKE と性能を比較した結果，十分に短い時間でネゴシエーションを完了し，かつ TCP/UDP 通信に与える影響がほとんどないことが分かった．また，ネットワークの物理構成の変更時における管理者やユーザの管理負荷について評価した結果，IPsec で FPN を構築した場合と比較して大幅な負荷軽減を実現できることを示した．

今後は FPN の実現に向けて，今回実現した DPRP の実装を Mobile PPC や NATF に拡張する予定である．また GSCIP と IPsec の連携や DPRP の IPv6 への適用などを検討していく予定である．

参考文献

1) Gordon, L., Loeb, P., Lucyshyn, W. and Richardson, R.: 2004 CSI/FBI Computer Crime and Security Survey, Technical report, Computer Security Institute (2004).
2) 荒井正人，鍛　忠志，伊藤浩道，手塚　悟，佐々木良一：企業情報向けグループ暗号システム，情報処理学会論文誌，Vol.40, No.12, pp.4378–4387 (1999).
3) 岡田浩一，冨士　仁：個人単位の VPN を実現するネットワークサービス「VPN-exchange」，CSS2001 論文集，pp.67–72 (2001).
4) 辻本孝博，唐澤　圭，藤崎智宏，三上博英：IPv6 IPSec による End-to-End VPN 構築方式に関する考察，情報処理学会研究報告，2001-CSEC-014, Vol.2001, No.75, pp.205–210 (2001).
5) Kourai, K., Hirotsu, T., Sato, K., Akashi, O., Fukuda, K., Sugawara, T. and Chiba, S.: Secure and Manageable Virtual Private Networks for End-users, *Proc. IEEE LCN2003*, pp.385–394 (2003).
6) 藤田範人，石川雄一，岩田　淳，飯島明夫：DNS を用いたスケーラブルな VPN アーキテクチャ，電子情報通信学会 2004 年総合大会講演論文集，p.200 (2004).
7) Rodeh, O., Birman, K., Hayden, M. and Dolev, D.: Dynamic Virtual Private Networks, Technical Report TR98-1695, Dept. of Computer Science, Cornell University (1998).
8) 加島伸吾，後藤幸功，荒木啓二郎：DVPN の提案と応用，DICOMO2003 シンポジウム論文集，pp.365–368 (2003).
9) 堀　賢治，吉原貴仁，堀内浩規：ピアツーピア型レイヤ 2 インターネット VPN の自動設定方式の実装と評価，情報処理学会第 67 回全国大会論文集，pp.3-485–3-486 (2004).
10) Kindred, D. and Sterne, D.: Dynamic VPN Communities: Implementation and Experience, *Proc. DISCEX II'01*, Vol.I, No.75, pp.254–263 (2001).
11) Wong, C., Gouda, M. and Lam, S.: Secure Group Communications Using Key Graphs, *Proc. ACM SIGCOM'98*, pp.68–79 (1998).
12) 鎌田　実，川瀬徹也，渡邊　晃，笹瀬　巌：部門 VPN 構成下におけるマルチキャスト通信方式の提案とその評価，電子情報通信学会論文誌 B, Vol.J82-B, No.11, pp.2061–2073 (1999).
13) Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J., Stanton, J. and Tsudik, G.: Secure Group Communication Using Robust Contributory Key Agreement, *IEEE Trans. Parallel Distrib. Syst.*, Vol.15, No.5, pp.468–480 (2004).
14) Harney, H., Meth, U., Colegrove, A. and Gross, G.: GSAKMP: Group Secure Association Key Management Protocol, RFC 4535, IETF (2006).
15) 萱島　信，寺田真敏，藤山達也，小泉　稔，加藤恵理：多重ファイアウォール環境に適した VPN 構築方式の提案，電子情報通信学会論文誌 D-I, Vol.J82-D-I, No.6, pp.772–778 (1999).
16) 岡山聖彦，山井成良，石橋勇人，安倍広多，松浦敏雄：代理ゲートウェイを用いた SOCKS ベースの階層的 VPN 構成法，情報処理学会論文誌, Vol.42, No.12, pp.2860–2868 (2001).
17) 渡邊　晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌, Vol.38, No.4, pp.904–914 (1997).

18) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
19) Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: SOCKS Protocol Version 5, RFC 1928, IETF (1996).
20) Dierks, T. and Allen, C.: The TLS Protocol Version 1.0, RFC 2246, IETF (1999).
21) 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，DICOMO2005 シンポジウム論文集，Vol.2005, No.6, pp.441–444 (2005).
22) 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 の仕組み，情報処理学会研究報告，2004-CSEC-026, Vol.2004, No.75, pp.259–266 (2004).
23) 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，2004-CSEC-028, Vol.2005, No.33, pp.199–204 (2005).
24) 渡邊 晃，井手口哲夫，笹瀬 巌：イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案，電子情報通信学会論文誌 D-I，Vol.J84-D-I, No.3, pp.269–284 (2001).
25) Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE), RFC 2409, IETF (1998).
26) National Institute of Standards and Technology: Specification for the ADVANCED ENCRYPTION STANDARD (AES), FIPS-197, U.S. Department of Commerce (2001).
27) OpenSSL: The Open Source toolkit for SSL/TLS. http://www.openssl.org/
28) Ethereal: A Network Protocol Analyzer. http://www.ethereal.com/
29) Jinmei, T., Yamamoto, K., Hagino, J., Sumikawa, M., Inoue, Y., Sugyo, K. and Sakane, S.: An overview of the KAME network software: Design and implementation of the advanced internetworking platform, *Proc. INET'99* (1999). http://www.isoc.org/isoc/conferences/inet/99/proceedings/4s/4s_2.htm
30) The KAME project: racoon. http://www.kame.net/
31) Kaufman, C.: Internet Key Exchange (IKEv2) Protocol, RFC 4306, IETF (2005).
32) Intel Corp.: Using the RDTSC Instruction for Performance Monitoring (1998). http://developer.intel.com/drg/pentiumII/appnotes/RDTSCPM1.htm
33) Rescorla, E.: Diffie-Hellman Key Agreement Method, RFC 2631, IETF (1999).
34) 竹内元規，渡邊 晃：モバイル端末の移動透過性を実現する Mobile PPC の提案，情報処理学会研究報告，2004-MBL-030, Vol.2004, No.95, pp.17–23 (2004).
35) 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，情報処理学会研究報告，2004-MBL-032, Vol.2005, No.28, pp.29–35 (2005).
36) 加藤尚樹，渡邊 晃：アドレス空間の違いを意識しない通信方式 NATF の提案，WiNF2004 論文集，pp.222–225 (2004).
37) 加藤尚樹，柳沢信成，鈴木秀和，渡邊 晃：アドレス空間の違いを意識しない通信方式 NATF の提案と実装，情報処理学会研究報告，2004-DPS-122, Vol.2005, No.33, pp.351–356 (2005).
38) 鈴木秀和，渡邊 晃：アドレス空間透過性を実現する NAT-f の実装と評価，DICOMO2006 シンポジウム論文集（I），Vol.2006, No.6, pp.453–456 (2006).
39) Boneh, D., Gentry, C. and Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *Proc. CRYPTO'05*, LNCS, Vol.3624, pp.258–275 (2005).
40) Halevy, D. and Shamir, A.: The LSD Broadcast Encryption Scheme, *Proc. CRYPTO'02*, LNCS, Vol.2442, pp.47–60 (2002).

(平成 17 年 9 月 16 日受付)
(平成 18 年 9 月 14 日採録)

推 薦 文

FPN（Flexible Private Network）を実現するために提案した GSCIP（Group for Secure Communication for IP）を実装し評価している．また，端末間の認証および暗号通信に必要な暗号動作処理情報テーブルを動的に生成する動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）も実装と評価を行っている．評価は多面的かつ厳密であり，信頼性が高い．IPsec と比べて高速に認証処理を行えることも実装評価により示している．加えて，応用例も示しており，信頼性と実用性，完成度が高いので，論文として推薦する．

（コンピュータセキュリティ研究会
前主査 村山優子）

鈴木 秀和（学生会員）

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．現在，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に在学中．ネットワークセキュリティ，モバイルネットワーク等の研究に従事．修士（工学）．2006 年 IEEE 名古屋支部学生奨励賞受賞．2006 年 DICOMO2006 松下賞（最優秀プレゼンテーション賞）受賞．電子情報通信学会所属．

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．