目次

概要

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，システム構成の変化に動的に対応させようとすると管理負荷が増大し，実現が難しかった．そこで本研究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．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）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，即ちシステム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（GSCIP Element）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，および通信中に行う PIT 検索が一般の 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作業コストを評価し，管理負荷を大幅に軽減できることを示した．

第1章　はじめに

企業ネットワークでは，不正進入，データの盗聴や漏洩，改竄等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，同一通信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，以下のような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[11]～[13]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，全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，代表技術として組織間接続型 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．これは例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無く, 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[11]，[12]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対応した VPN 構築方法である. 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繋がっていない.

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[14]～[17], 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.

このような状況を鑑み，本研究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．即ち，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．本研究で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．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）[21]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（GSCIP Element）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．システム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テーブルが DPRP により動的に再生成されるため，管理者やユーザの作業負担を大幅に軽減できる．

文献[21]において DPRP の原案が提案されている．ただし，この時点では FPN，GSCIP の概念が定義されておらず，DPRP の位置付けが不明確であった．また通信経路上の終端装置間だけで情報交換を行っており，中間装置では通知された動作処理情報を認証することなくテーブルに登録していたため，動作処理情報を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 の位置付けを明確にしている．また中間装置も情報交換するように DPRP シーケンスの見直しを行い，認証処理の機能を追加した．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 は一般の 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，および PIT の検索が行えることを確認した．また同一ネットワークを，GSCIP/DPRP を実装した装置で構築する場合と，IPsec/IKE[22]を実装した装置で構築する場合に発生する作業コストを比較し，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 の動作概要とプロトコルの定義について述べる．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．

第2章　FPN とその実現方法

第2.1節　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

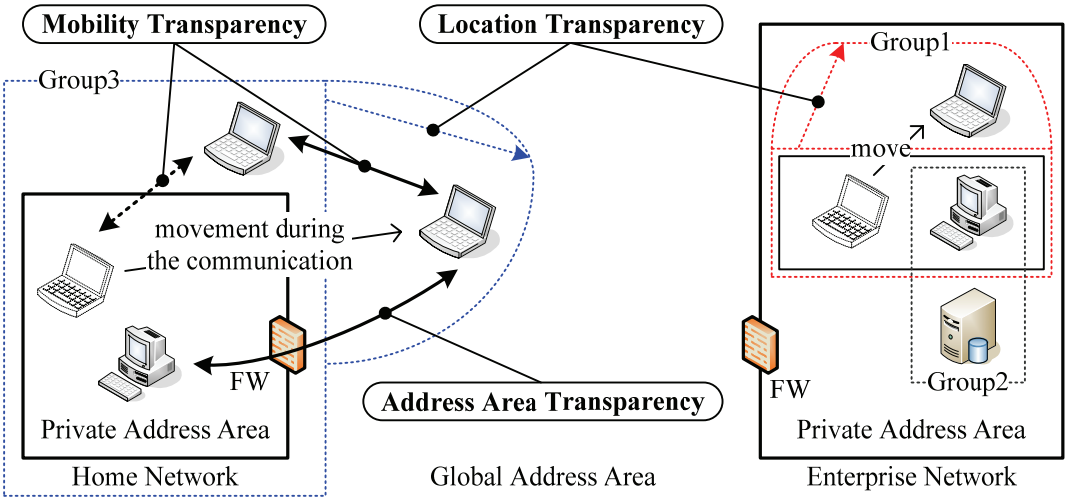


図 1　FPN の概念

Figure 1　A concept of Flexible Private Network

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った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通信グループに属する端末が存在するような環境であってもかまわない．本論文ではこのような環境を多段構成ネットワークと呼ぶ．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 3 つの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，予め定義されている通信グループの関係は維持される．このときユーザや管理者が設定情報を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．この機能を位置透過性と呼ぶ．ここで述べる移動とは端末が通信していない状態（オフライン）の場合で，人事異動に伴う引っ越しや出張先から通常の業務を行うようなことを想定している．

(2) 移動透過性（Mobility Transparency）

上記で述べた移動の他に，端末が通信中の状態（オンライン）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．

(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双方向通信ができない．これはアドレス変換 NAT（Network Address Translation）の機能を持つ装置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．このような NAT の弊害を除去して，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になる．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．本論文で扱う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等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ーにより自由な通信が禁止されているため，両者を跨る FPN の構築は想定しない．

第2.2節 GSCIP（Grouping for Secure Communication for IP）

FPN の概念を実現するには様々な方式があり得る. GSCIP とは FPN を実現するために検討した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（GSCIP Element）と呼ぶ．GE には端末にソフトウェアをインストールして実現するホストタイプの GES（GE for Software），サブネットを構成するルータに実装したルータタイプの GEN（GE for Network），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）の 3 種類がある．GEN の配下に存在する一

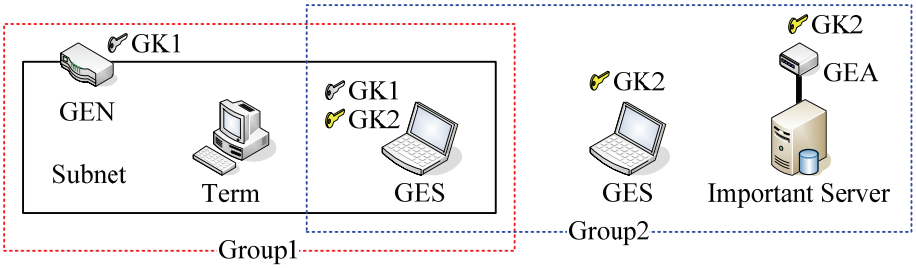


図 2　通信グループの定義方法

Figure 2　A definition method of communication group

般端末 Terminal（以下 Term）は，GEN により一括して保護される．GSCIP では同一の共通暗号鍵を所持する GE の集合を同一の通信グループとして定義する．この共通暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．同一通信グループの GE 間の通信は GK を用いて暗号化される．GE には動作モード OM（Operation Mode）が定義されており，同一通信グループに帰属しない端末との通信を一切禁止する閉域モード CL（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）がある．一般に GEN，GEA やサーバとして使用する GES には閉域モードが，ユーザが使用する GES に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）で設定される．図 3 に MS における作業内容と GE への配送情報を示す．管理者は MS において GE／ユーザ，および通信グループの設定を行う．GE の設定では常にオンラインで固定して設置されている GEN と GEA の動作モードと，帰属する通信グループの設定が行われる．ユーザの設定では GES を利用するユーザの追加／削除や，帰属する通信グループとユーザが利用する GES の動作モードの設定が行われる．グループの設定では通信グループの追加／削除と，通信グループ番号の設定が行われる．通信グループ番号とは定義された通信グループとグループ鍵 GK を 1 対 1 に対応づけるための番号であり，IP アドレスに依存することなく論理的に通信グループを定義することができる．さらに 1 ユーザに対して個人単位／ドメイン単位が混在したり，複数の通信グループを定義することもできる．管理者は組織変更や人事異動が発生した場合に，GE およびユーザが帰属する通信グループを変更する．このため，GE 自身が主導的に通信グループへ参加したり，離脱することはできない．MS ではこれらの設定の他に，グループ鍵 GK の生成，更新処理を行う．グループ鍵 GK は通信グループに対応して生成され，定期的に，または GE の参加や離脱により通信グループ内のメンバ構成が変化したときに更新される．

MS で設定された情報と生成された GK は GE へ配送される．配送される情

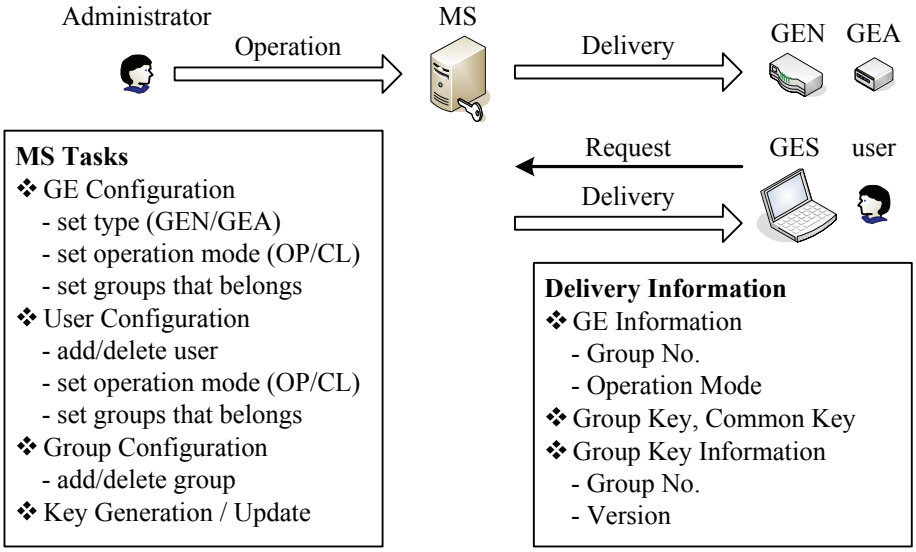


図 3　MS の機能と配送情報

Figure 3　MS tasks and Delivery Information

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．また配送される 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．MS にて鍵が更新されると,オンラインの GE に対して即座に新しい鍵が配送される．この場合，同一通信グループ内の GE 間で新旧の鍵が混在する可能性が考えられるが，バージョン番号により鍵の更新時に誤った鍵で通信しないように考慮されている．

MS の管理範囲を図 4 に示す．MS は 1 つの管理ドメインに対して 1 台設置される．MS を複数設置する場合は，DNS のようにツリー構造で管理することによって MS 間の情報の一貫性を保つ．本社や支社など複数のネットワークがある場合，各イントラネットに 1 台ずつ設置し，イントラネット間の通信グループ情報を上位 MS にて管理する．上位 MS は下位 MS に FPN 番号を定義する．末端 MS は配下で管理する通信グループ番号に上位 MS より定義された FPN 番号を付加する．このように MS で定義される通信グループ番号を階層化することで実現する．

GSCIP において位置透過性を実現するには，以下のような構成要素が必要である．即ち，(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決定，(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

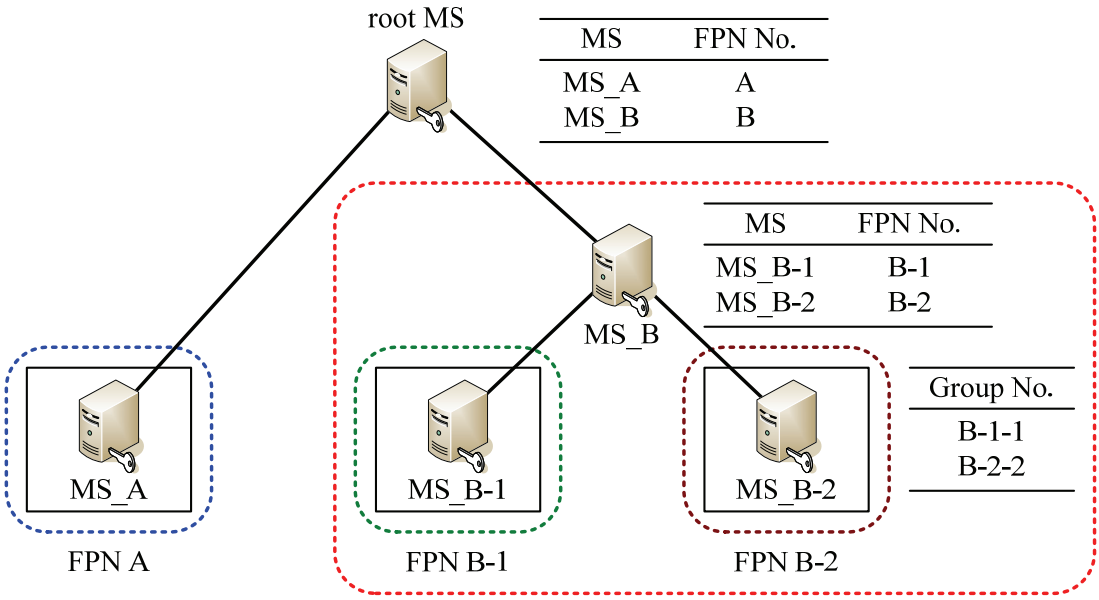


図 4　MS の管理範囲

Figure 4　Management area of MS

義が必要である．これらの実現手段については第 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 から各 GE に定義されている情報を取得，設定する．この情報には GE 情報，グループ鍵 GK，およびシステム全体で用いるシステム共通鍵 CK（Common Key）が含まれる．これにより各 GE は必要な情報を予め保持することができる．そのため 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とが必要条件となる．

(2) GE 間の認証と動作処理情報の決定

端末間の通信に先立ち，通信相手が同一の通信グループに帰属しているか，またどの動作モードが定義されているか知る必要がある．そこで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動的に決定する．GE に定義された通信グループ番号や動作モードなど，相互に交換した情報の組み合わせにより，通信パケットに対する処理内容が決定する．

DPRP は通信に先立ち実施されるので，システムの物理構成が変化して

も GE にはシステム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，パケットは暗号化／復号処理されず透過中継される．“Discard”の場合，パケットは破棄される．

第3章　DPRP（Dynamic Process Resolution Protocol）

第3.1節　概要

DPRP は端末間の通信に先立ち，通信経路上の全ての GE 間で設定されている情報を相互に交換して，通信パケットの動作処理情報を決定し，その情報を格納する動作処理情報テーブル PIT（Process Information Table）を生成する．PIT は送信元／宛先 IP アドレスとポート番号，プロトコルタイプ，処理内容，グループ鍵情報から構成されている．このうち送信元／宛先 IP アドレスとポート番号，およびプロトコルタイプのセットを通信識別子 CID（Connection Identification），処理内容およびグループ鍵情報のことを動作処理情報と呼ぶ．

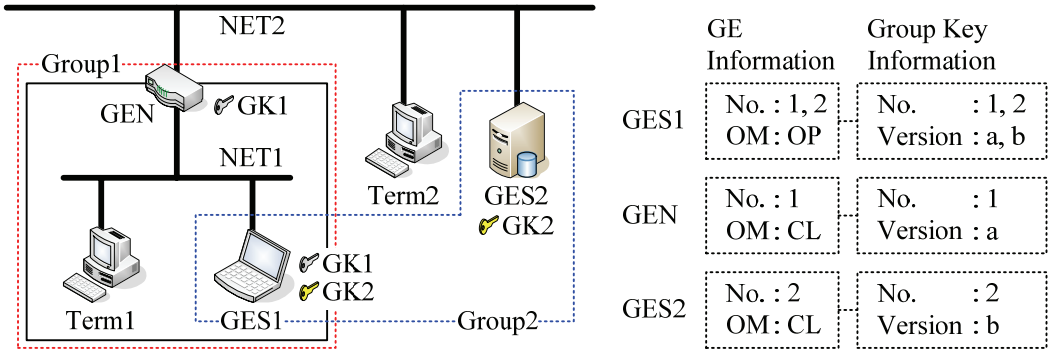


図 5　ネットワーク構成と GE 定義情報

Figure 5　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		通信可否	動作処理情報		
			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

図 5 にネットワーク構成例と GE 情報を示す．図 5 は GES1 が GEN により構成された部門サブネット 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）に帰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 も予め保持している．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が，GES1 は同一部門の一般端末とも通信するため開放モードが，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 には既に MS から GE 情報，GK，および CK が配送されているとする．端末間の通信経路上には複数の GE が存在しうるが，通信ペアに最も近い GE（送信元端末または宛先端末が GE の場合も含む）のうち，送信側を始点 GE，宛先側を終点 GE，両者をまとめて終端 GE と呼ぶ．また始点 GE と終点 GE の間に存在する GE を中間 GE と呼ぶ．ここで図 5 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／復号し，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報を自動的に決定する役割を持つ．

第3.2節　DPRP シーケンス

本論文で用いる記号を以下のように定義する．

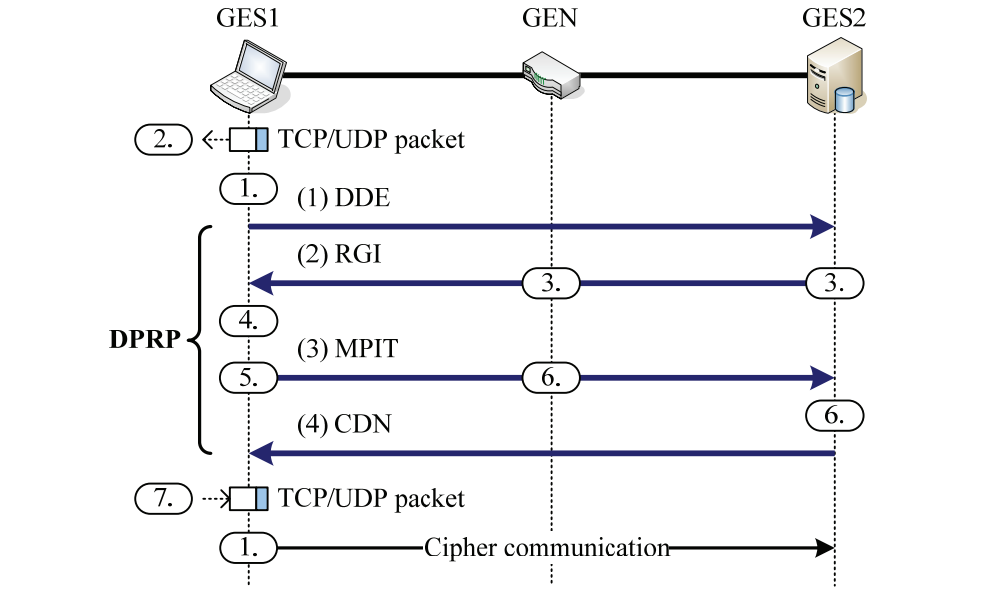
- n：通信経路上に存在する GE の数

- GE_i：通信経路上における i 番目の GE（$1 \leqq i \leqq n$）
- GE_{START}：DPRP を開始する GE
- GE_{SRC}／GE_{DST}：始点 GE（$i=n$）／終点 GE（$i=1$）
- $NODE_a$：IP アドレス a の端末
- HDR：DPRP ヘッダ
- N_i：GE_i が RGI に記載する通知情報
- D_i：GE_i に関する決定情報
- P_i：GE_i に関する動作処理情報
- UID_i：GE_i のユーザ ID
- $OM_i \in \{OP, CL\}$：GE_i の動作モード
- GKI_i：GE_i が保持するグループ鍵情報
- GNO／VER：通信グループ番号／バージョン番号
- aID_i：GE_i が生成した認証情報
- DIRECT∈{*edge*, *inbound*, *outbound*}：ネゴシエーションの方向情報
- $PROC_i \in \{Encrypt, Decrypt, Transparent, Discard\}$：$GE_i$ が行う処理内容
- CNT_i：GE_i が帰属している通信グループの数
- CK(M)：M をシステム共通鍵で暗号化
- $GK_D(M)$：M をグループ鍵 GK_D で暗号化
- A→B: M：A から B へ M を送信

図 6 に DPRP ネゴシエーションと処理内容を示す．GES1 はデータを送信する際，自身が保持する PIT の内容を検索する．検索の結果，GES1-GES2 間の動作処理情報がない場合，送信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．DPRP ネゴシエーションが完了すると，先ほど待避していた TCP/UDP パケットを復帰させて動作処理情報に基づいて処理する．以降，待避した TCP/UDP パケット，すなわち DPRP ネゴシエーションを開始するきっかけとなった通信パケットをトリガーパケットと呼ぶ．

DPRP は ICMP ECHO パケットをベースに独自に定義した制御パケットを用いてネゴシエーションを終端 GE 間で行う．図 7 に DPRP プロトコルのフォーマットを示す． DPRP ヘッダは ICMP ヘッダの次に定義され，4 つのフィールドから構成される．

$$HDR = DPRP\_ID, Code, OPT, NID$$



Operation Flow
1. Search PIT : Hit → process the TCP/UDP packet according to its Process Information
   : None → start DPRP (go to 2.)
2. Evacuate the TCP/UDP packet to kernel memory
3. Generate aID and Add GE Information and Group Key Information
4. Decide upon Process Information
5. Register Process Information in PIT
6. Authenticate MPIT and Register Process Information in PIT
7. Return the evacuated packet from kernel memory and go to 1.

図 6　DPRP ネゴシエーションと処理内容

Figure 6　DPRP negotiation and operations

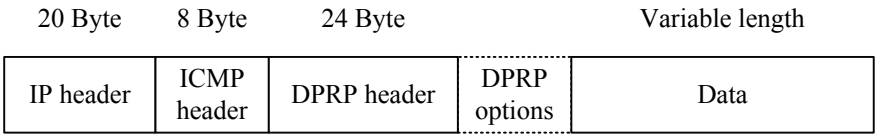


図 7　DPRP プロトコルのフォーマット

Figure 7　The format of DPRP protocol

DPRP_ID は DPRP 制御パケットであることを識別するための値が，Code は DPRP 制御パケットの種類を示す値が設定される．OPT はオプションの有無を示す情報が設定される．NID はネゴシエーションを識別し，リプレイ攻撃から防御するために使用される乱数値が設定される．Code で示されるパケットのデータが DPRP ヘッダの次に記載される．また OPT が有効な場合，オプション領域が DPRP ヘッダとデータ領域の間に挿入される．DPRP 制御パケットは全ての GE が保持するシステム共通鍵 CK を使ってデータ領域が暗号

化され，安全に情報の交換を行う．DPRP 制御パケットは以下に示す 4 種類がある．

(1) DDE（Detect Destination End GE）

DPRP ネゴシエーションを開始する GE は終点 GE を決定するために，DDE（Detect Destination End GE）をトリガーパケットの宛先（GES2）に送信する．DDE にはトリガーパケットの通信識別子 CID，すなわち送信元／宛先 IP アドレス（saddr/daddr）とポート番号（sport/dport），およびプロトコルタイプ（proto）が記載される．

$$\mathrm{GE_{START}} \rightarrow \mathrm{NODE_{daddr}}: \quad \mathrm{DDE} = \mathrm{HDR}, \mathrm{CK}(\mathrm{CID})$$
$$\mathrm{CID} = \mathrm{saddr}, \mathrm{daddr}, \mathrm{sport}, \mathrm{dport}, \mathrm{proto}$$

$\mathrm{NODE_{daddr}}$ が GE の場合は，DDE を受信した $\mathrm{NODE_{daddr}}$ が終点 GE に決定する．$\mathrm{NODE_{daddr}}$ が一般端末であった場合，一般端末は DDE を ICMP ECHO パケットとして認識するため, ICMP ECHO REPLY を $\mathrm{GE_{START}}$ に対して応答する. この ICMP ECHO REPLY を最初に受信した GE が終点 GE に決定する．

(2) RGI（Report GE Information）

DDE によって決定した終点 GE（GES2）は，DDE に記載されている CID の送信元，即ちトリガーパケットの送信元（GES1）に RGI（Report GE Information）を送信する．RGI には DDE から取得した CID と通知情報 N が記載される．

$$\mathrm{GE_{DST}} \rightarrow \mathrm{NODE_{saddr}}: \quad \mathrm{RGI} = \mathrm{HDR}, \mathrm{CK}(\mathrm{CID}, \mathrm{N_1})$$
$$\mathrm{N_1} = \mathrm{UID_1}, \mathrm{OM_1}, \mathrm{aID_1}, \mathrm{DIRECT_1}, \mathrm{CNT_1}, \mathrm{GKI_1}$$
$$\mathrm{GKI_1} = \{(\mathrm{GNO}_c, \mathrm{VER}_c) \mid c = 1, \cdots, \mathrm{CNT_1}\}$$

通知情報 N は自 GE に設定されている UID, OM, CNT_i 個の GKI に加え，生成された認証情報 aID（Authentication Identification）とネゴシエーションの方向情報 DIRECT から構成される．ここで aID は 2 バイトの乱数値で，PIT に一時的に記憶しておき，RGI 以降の DPRP 制御パケットを認証するために利用される．ネゴシエーションの方向情報とは RGI が GEN の配下から出る方向（outbound）なのか，配下へ入る方向（inbound）なのかを示す情報である．GES においては終点（edge）を示す情報が記載される．また DPRP ヘッダに記載されている NID も PIT に記憶してお

く．中間 GE（GEN）が RGI を受信すると，終点 GE が記載したものと同種の情報を RGI に追加して転送する．すなわち，i 番目の GE が転送する RGI は

$$\mathrm{RGI} = \mathrm{HDR}, \mathrm{CK}\left(\mathrm{CID}, \mathrm{N}_1, \cdots, \mathrm{N}_i\right)$$

となる．$\mathrm{NODE}_{\mathrm{saddr}}$ が GE の場合は，RGI を受信した $\mathrm{NODE}_{\mathrm{saddr}}$ が始点 GE に決定する．$\mathrm{NODE}_{\mathrm{saddr}}$ が一般端末であった場合，一般端末は RGI を ICMP ECHO パケットとして認識するため，ICMP ECHO REPLY を $\mathrm{NODE}_{\mathrm{daddr}}$ に対して応答する．この ICMP ECHO REPLY を最初に受信した GE が始点 GE に決定する．

始点 GE は RGI から通信経路上の全 GE の通知情報 $\mathrm{N}_1, \cdots, \mathrm{N}_n$ を取得する．始点 GE はこの情報を元に，通信経路上の全 GE の動作処理情報を決定する．動作処理情報の決定方法は第 3.3 節にて述べる．

(3) MPIT（Make Process Information Table）

始点 GE（GES1）は通信経路上の各 GE に決定した情報を伝えるため，自らの動作処理情報を PIT に登録してから MPIT（Make Process Information Table）を終点 GE（GES2）宛に送信する．MPIT には RGI から取得した CID と決定情報 $\mathrm{D}_{n-1}, \cdots, \mathrm{D}_1$ が記載される．

$$\mathrm{GE}_{\mathrm{SRC}} \rightarrow \mathrm{GE}_{\mathrm{DST}}: \quad \mathrm{MPIT} = \mathrm{HDR}, \mathrm{CK}\left(\mathrm{CID}, \mathrm{D}_{n-1}, \cdots \mathrm{D}_1\right)$$

$$\mathrm{D}_i = \begin{cases} \mathrm{UID}_i, \mathrm{GK}_{\mathrm{D}}\left(\mathrm{aID}_i\right), \mathrm{P}_i & \textit{if} \ \ \mathrm{PROC}_i = \textit{Decrypt} \\ \mathrm{UID}_i, \mathrm{aID}_i, \mathrm{P}_i & \textit{if} \ \ \mathrm{PROC}_i \neq \textit{Decrypt} \end{cases}$$

$$\mathrm{P}_i = \left(\mathrm{PROC}_i, \mathrm{GKI}_{\mathrm{D}}\right) \quad \left(1 \leq i < n\right)$$

決定情報 D は RGI で受信した各 GE の UID と aID，および動作処理情報 P から構成される．PIT に登録する際，処理内容が“Encrypt”であれば，処理内容が“Decrypt”である決定情報 D に含まれている aID を決定したグループ鍵 GK_{D} で暗号化する．GK_{D} は決定したグループ鍵情報 $\mathrm{GKI}_{\mathrm{D}}$ から一意的に選択することができる．各 GE が MPIT を受信すると，UID を元に自 GE に該当する決定情報 D を取得する．取得した処理内容が“Decrypt”であれば，aID を GK_{D} で復号する．次に取得した NID，aID を PIT に記憶していた NID，aID と比較して認証を行う．認証の結果，正しければ RGI で通知された情報を元に作成された動作処理情報であり，

かつ暗号化通信を行う GE 間で決定したグループ鍵を保持していることが証明される．その後，動作処理情報 P を PIT に登録して転送する．認証の結果，正しくなければ MPIT は破棄される．

(4) CDN（Complete DPRP Negotiation）

終点 GE（GES2）は各 GE に PIT が生成されたことを通知するために，CDN（Complete DPRP Negotiation）を始点 GE（GES1）宛に送信する．CDN には MPIT から取得した CID が記載される．

$$GE_{DST} \rightarrow GE_{SRC}: \quad CDN = HDR, CK(CID)$$

始点 GE（状況によっては DDE を送信した中間 GE）が CDN を受信すると，待避していた通信パケットを復帰させることにより通信が再開される．以後の通信は PIT の内容に基づいて処理される．

図 8 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（宛先ポート番号 21）接続した場合に生成される PIT の一例である．

GES1

saddr	daddr	sport	dport	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

saddr	daddr	sport	dport	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

saddr	daddr	sport	dport	proto	PROC	GNO	VER
192.168.1.10	192.168.2.20	49230	21	tcp	Dencypt	2	b
192.168.2.20	192.168.1.10	21	49230	tcp	Encrypt	2	b

図 8　GES1-GES2 間に生成される PIT の一例

Figure 8　The example of PITs which are created between GES1 and GES2

第3.3節　動作処理情報の決定

図 9 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 $N_1,\cdots,N_n$ は分割関数により，始点 GE 側と終点 GE 側の情報に分割される．通知情報の分割後，導出関数により動作処理情報を決定する．

分割関数は N_i と N_{i+1} の方向情報 DIRECT を比較する．$i=s$ $(1 \leqq s < n)$のとき，図 10 に示す分割条件のいずれかに合致した場合，$N_1,\cdots,N_s$ を終点 GE 側の情報に，$N_{s+1},\cdots,N_n$ を始点 GE 側の情報に分割する．例えば図 10 の条件 3 において，GE_{s+1} が GE_s の配下に存在する GE_{s-1} と通信する場合，GE_{s+1} と GE_s，および GE_{s+1} と GE_{s-1} の通信グループ関係だけを確認すればよく，GE_s と GE_{s-1}

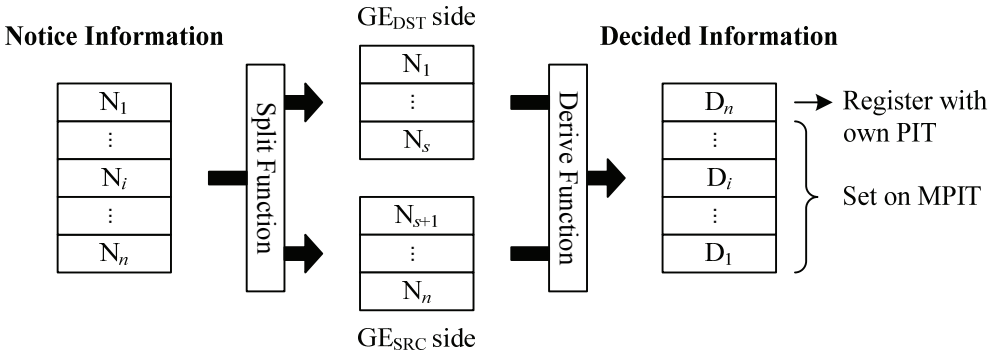


図 9　動作処理情報の決定プロセス

Figure 9　A decision process of Process Information

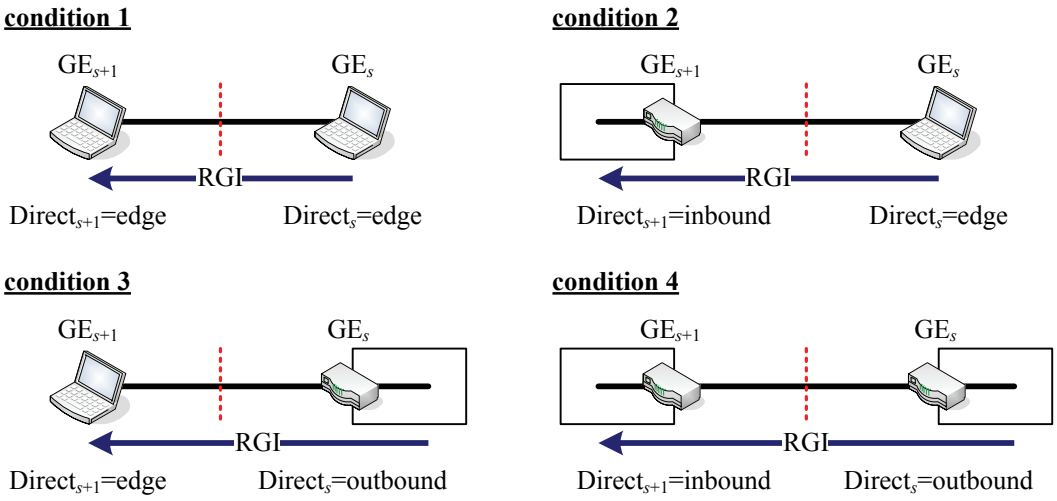


図 10　通知情報の分割条件

Figure 10　Split conditions of notice information

が同一通信グループであるか否かに影響されない．すなわち，始点 GE 側と終点 GE 側だけを比較するために通知情報を分割する．図 10 に示す分割条件のいずれにも合致しない場合は分割しない．

導出関数は分割関数により出力された $N_{s+1},\cdots,N_n$ に含まれている GKI と OM を比較する．分割関数の出力結果が分割されていない場合，N_1 から N_n の動作モード OM を確認する．1 つも閉域モードが含まれていなければ処理内容が“Transparent”，1 つでも閉域モードが含まれていれば処理内容が“Discard”の動作処理情報 $P_1,\cdots,P_n$ が生成される．これらの処理内容の場合，グループ鍵情報は設定されない．

$$P_i = \begin{cases} (Transparent,0) & if\ \ CL \notin \{OM_j \mid j=1,\cdots,n\} \\ (Discard,0) & if\ \ CL \in \{OM_j \mid j=1,\cdots,n\} \end{cases} \quad (i=1,\cdots,n)$$

分割関数の出力結果が分割されている場合，以下の手順に従って処理される．

Step1

始点 GE 側の通知情報 N_p (p=n,⋯,s+1)と終点 GE 側の通知情報 N_q (q=1,⋯,s)に含まれている GKI を比較する．同一の GKI があればそれを決定したグループ鍵情報 GKI_D として，以下の動作処理情報 $P_1,\cdots,P_n$ が生成される．

$$P_i = \begin{cases} (Decrypt, GKI_D) & if\ \ i=q \\ (Transparent,0) & if\ \ i \neq p,q \\ (Encrypt, GKI_D) & if\ \ i=p \end{cases} \quad (i=1,\cdots,n)$$

同一の GKI がなれば Step2 へ移る．

Step2

始点 GE 側の通知情報 N_p と終点 GE 側の通知情報 N_q に含まれている OM を比較する．

- 終点 GE 側，始点 GE 側が共に閉域モードであれば，処理内容が“Discard”の動作処理情報 $P_1,\cdots,P_n$ が生成される．
- 終点 GE 側が開放モードであれば，終点 GE 側の比較先を N_q から N_{q+1} へシフトして，Step1 を再度実行する．N_q= N_s まで繰り返しても同じ結果であった場合，終点 GE 側の比較先を N_1 に戻し，始点 GE 側の比較元を N_p から N_{p-1} へシフトして，Step1 を再度実行する．N_p= N_{s+1} まで繰り返しても同じ結果であった場合，処理内容が“Discard”の動作処理情報 $P_1,\cdots,P_n$ が生成される．
- 終点 GE 側が閉域モード，かつ始点 GE 側が開放モードであれば，終点

GE 側の比較先を N_1 に戻し，始点 GE 側の比較元を N_p から N_{p-1} へシフトして，Step1 を再度実行する．$N_p = N_{s+1}$ まで繰り返しても同じ結果であった場合，処理内容が“Discard”の動作処理情報 $P_1,\cdots,P_n$ が生成される．

第4章　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 11 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，通信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 の影響を一切受けることがない．DPRP のトリガーとなった TCP/UDP パケットを一時待避するが，待避パケットは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．これは ARP（Address Resolution Protocol）要求をブロードキャストする際に，IP データグラムを保持する方式と同じである．DPRP により生成される PIT や，MS から配送された GK および CK 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

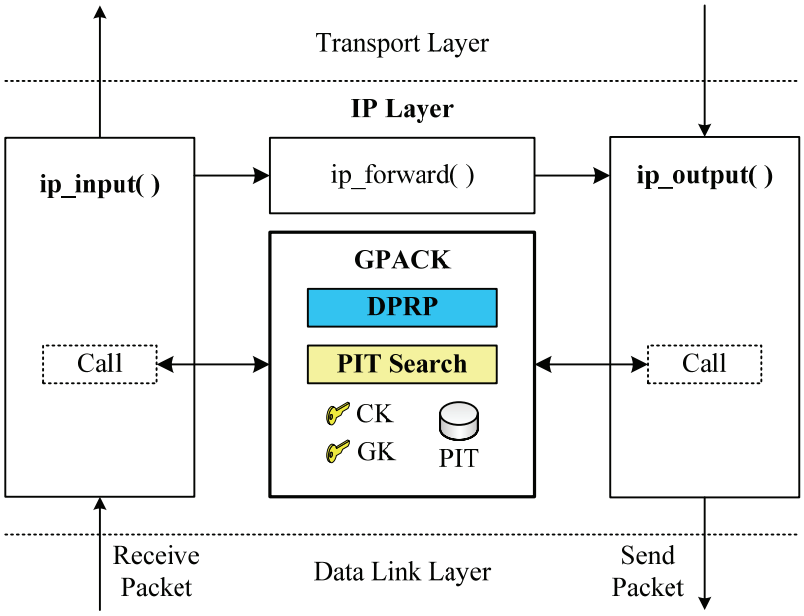


図 11　GSCIP の実装

Figure 11　Implementation of GSCIP

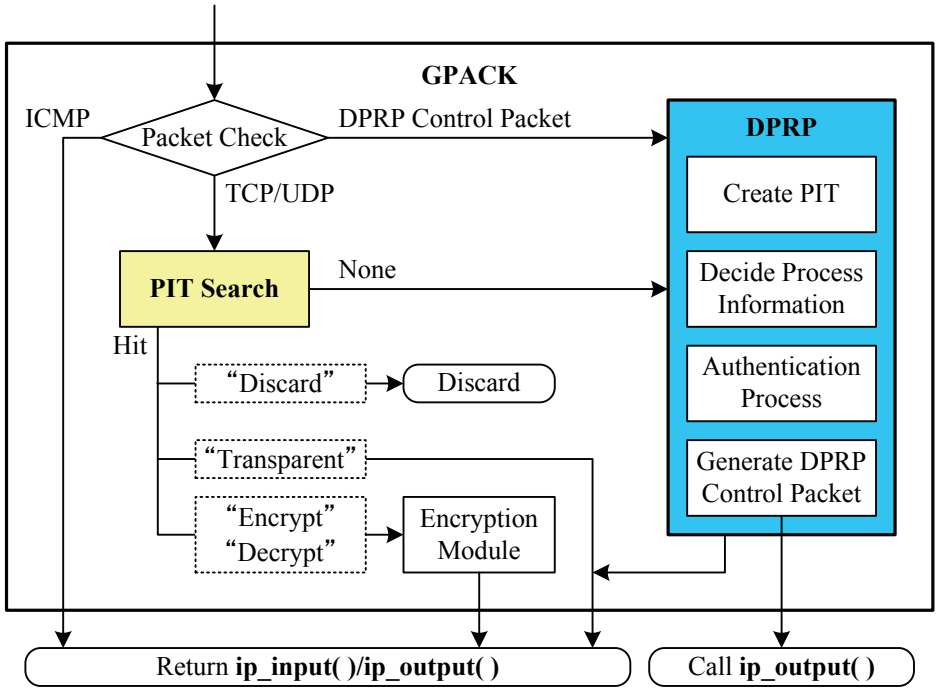


図 12　GSCIP モジュールの処理フロー

Figure 12　Process flow of GSCIP module

は全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極めて低い. 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，CID，即ち送信元／宛先 IP アドレスとポート番号，プロトコルタイプのセットである．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度，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，その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.

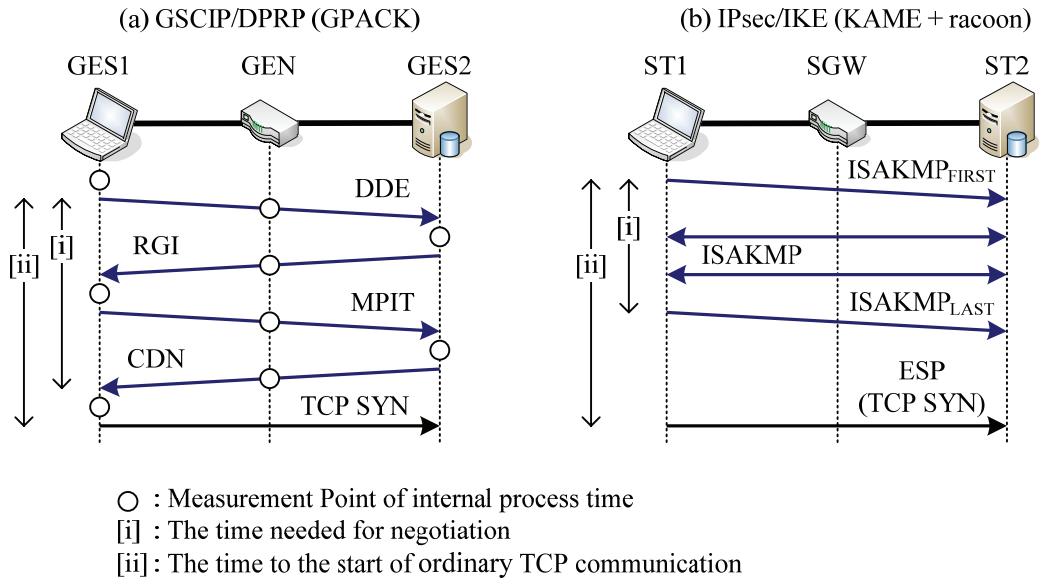
図 12 に GSCIP モジュールの処理フローを示す．GPACK は受け取った通信パケットの種類を判別してから，適切なモジュールを選択し実行する．送受信パケットが TCP/UDP の場合，まず PIT 検索を行う．該当する PIT レコードが存在した場合，PIT レコードに記された動作処理情報に従って通信パケットの処理を実行する．該当する PIT レコードが存在しない場合，DPRP モジュールに処理が渡される．DPRP モジュールは DDE を作成して `ip_output()` に渡し送信する. その後, トリガーパケットとなった TCP/UDP パケットを待避する. 送受信パケットが通常の ICMP の場合，GPACK の処理を行わずに IP 層に戻す. 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，DPRP 制御パケットの生成，動作処理情報の決定，認

証，PIT 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 CK により暗号化される．暗号アルゴリズムは AES（Advanced Encryption Standard）[23]を採用し，CK の鍵長は 128bit 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[24]（バージョン 0.9.7d）を用いた．

第5章　評価

第5.1節 DPRP の性能評価

100BASE-TX の Ethernet ネットワーク環境下において，GES1 が GES2 に FTP 接続を行う場合の DPRP の性能を測定した．測定項目は DPRP ネゴシエーションのオーバヘッド時間，DPRP モジュールの内部処理時間，および FTP のスループット値とした．表 2 に性能測定に使用した各装置のスペックを示す．各 GE は予め図 5 に示した GE 情報，GK および CK を保持しているものとし，図 12 に示す暗号モジュールの処理は行わず，PIT 検索の結果，処理内容が“Encrypt”，“Decrypt”であっても平文通信とした．



○ : Measurement Point of internal process time
[i] : The time needed for negotiation
[ii] : The time to the start of ordinary TCP communication

図 13　測定ポイント

Figure 13　Measurement points

表 2　装置スペック

Table 2　Terminal specifications

	GES1／GEN／GES2
PC Model	Dell PowerEdge 750
CPU	Pentium4 3.0GHz
RAM	512MB PC3200（400MHz）
NIC	Intel PRO/1000 MT×2（Driver version: 3.2.18）
OS	FreeBSD5.3-Release

表 3　racoon の設定パラメータ

Table 3　Configuration parameters of racoon

設定項目	設定値
交換モード	メインモード
相互認証方式	既知共有秘密鍵方式
暗号化アルゴリズム	rijindael（AES）
ハッシュアルゴリズム	SHA-1（フェーズ 1）
	HMAC-SHA-1（フェーズ 2）

(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[25]を用いた．参考のために，同一条件下における IPsec/IKEv1[22]の処理時間も測定した．FreeBSD に実装されている KAME[26]および IKE デーモン racoon[27]を使用し，表 3 に示す設定で行った．IKEv2[28]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 13 (a)に示す[i]DPRP ネゴシエーション時間（DDE～CDN 間）と，[ii]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）である．一方，IKE では図 13 (b)に示す[i]IKE ネゴシエーション時間（$ISAKMP_{FIRST}$～$ISAKMP_{LAST}$ 間）と[ii]通信開始までの時間である．図 13 (b)における ST1，ST2，SGW はそれぞれ GES1，GES2，GEN に 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 4 に示す．DPRP のネゴシエーション時間は 1.13 ミリ秒，通信開始までの時間は 1.17 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 1068.46 ミリ秒（約 1 秒），通信開始までの時間は 2994.96 ミリ秒（約 3 秒）となった．

表 4　オーバヘッドの測定結果

Table 4　Measurement results of overheads

	GSCIP/DPRP	IPsec/IKE
[i] ネゴシエーション時間	1.13	1068.46
[ii] 通信開始までの時間	1.17	2994.96

Unit: [ms]

表 5　GE における内部処理時間

Table 5　Internal process time of GEs

	GES1	GEN	GES2	Total
DPRP 処理全体	176.00	145.23	123.05	444.28
うち暗号処理部分	29.16	38.27	26.83	94.26

Unit: [μs]

表 6　FTP スループットの違い

Table 6　Differences of FTP throughput

	GSCIP 未実装時	GSCIP 実装時
100BASE-TX	82.31	82.15
1000BASE-TX	378.03	376.34

Unit: [Mbps]

(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）[29]を用いた．測定箇所は図 13 (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 5 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 444.28μ秒となった．またこのうち，約 21%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 145.23μ秒となった．

(3) GPACK 実装時における 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 100BASE-TX と 1000BASE-TX の Ethernet ネットワーク環境下において， GES2 から 500MB のファイルを null デ

バイスにダウンロードした．GPACK 実装時と未実装時における FTP スループット値を表 6 に示す．100BASE-TX の Ethernet ネットワーク環境下において，GSCIP 未実装時は 82.31Mbps，GSCIP 実装時は 82.15Mbps であった．また 1000BASE-TX の Ethernet ネットワーク環境下において，GSCIP 未実装時は 378.03Mbps，GSCIP 実装時は 376.34Mbps であった．

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，一般の 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 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ながら，予めグループ鍵 GK が配送されている．通信開始時の認証と通信パケットの暗号化は共通鍵であるグループ鍵 GK を用いるため，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の他に，公開鍵やディジタル署名などを用いた認証もあり，通信パケットを暗号化する共通鍵を DH 鍵交換[30]により別途生成しているため，GSCIP に比べて処理が遅い．

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．GSCIP/DPRP は実装がシンプルなため，全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，わずかな遅延で一般の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，トリガーパケットを破棄して IKE ネゴシエーションを開始する．即ち，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．

ネゴシエーションが完了して PIT が生成された後，全ての送受信パケットに対して PIT 検索を行うが，スループットにその影響はほとんどない．

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．例えば，VoIP アプリケーションでは一般にパケット送出間隔が 20 ミリ秒に設定されるが，イントラネットでは約 1 ミリ秒で DPRP ネゴシエーションを完了するため影響はない．

第5.2節 管理負荷

ネットワークの物理構成が変化した状況を想定し，このとき管理者およびユーザに発生する管理負荷を評価した．ここでの変化とは引っ越し，人事異動や出張などオフラインでの移動によるシステム構成の変化であり，通信中の移動は考えない．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初期管理負荷と，構成変化時に発生する管理負荷を算出する．

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 7 に示す．GSCIP ではグループ鍵情報と GE 情報の設定が必要である．各設定に必要な項目数は合計で 5 項目である．一方，IPsec では事前にエンド端末と共有する秘密鍵，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ー，および IKE の設定が必要である．鍵はどの相手と共有しているかを指定する必要があり，1 つの鍵を

表 7　設定内容と項目数の比較

Table 7　Comparison of setting parameters and its numbers

GSCIP/DPRP			
	グループ鍵情報		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			
	鍵	セキュリティポリシー	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（Transparent/Tunnel） SGW ペア識別子　など	通信相手識別子 自端末識別子 交換モード （main/aggressive） 暗号化アルゴリズム 認証方式　など
項目数	2	None / Discard　: 8 IPsec, Transport　: 14 IPsec, Tunnel　　: 16	12

表 8　初期管理負荷の違い

Table 8　Difference of initial management loads

GSCIP/DPRP			
	グループ鍵情報	GE 情報	合計
GES1	6	2	8
GEN	3	2	5
GES2	3	2	5

IPsec/IKE				
	鍵	セキュリティポリシー	IKE	合計
ST1	4	14（Transport: 14）	12	30
SGW	2	16（None: 8，Discard: 8）	0	18
ST2	2	22（Transport: 14，Discard:8）	12	36

設定するために通信相手識別子と鍵データの 2 項目が必要となる．セキュリティポリシーは双方向定義する必要があり，処理内容に応じて項目数が異なる．処理内容が IPsec を適用しない場合，または全て破棄の場合は 8 項目，トランスポートモードの場合は 14 項目，トンネルモードの場合は 16 項目の設定が必要となる．IKE は細かな設定ができるため 12 項目必要となる．IPsec における鍵，セキュリティポリシー，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．

図 5，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 8 に示す．ここで初期管理負荷とは表 7 で示した設定 1 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，グループ鍵 1 個に対して 1 つのグループ鍵情報と，GE1 台に対して 1 つの GE 情報を定義する．GES1 は 2 つの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ーと 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 18，36 となる．GSCIP は GE が所属するグループ数の増加に伴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 はセキュリティポリシーを 1 つ設定する度に，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

表 9　ネットワーク構成変化時の動作処理情報の変化

Table 9　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

SGW にそれぞれ 14，8 ずつ増加する．このことより，GSCIP は IPsec と比較すると初期設定の管理負荷が非常に小さいことがわかる．

次にネットワーク構成が変化した場合に発生する管理負荷の違いを算出する． 図 5 において GES1（IPsec では ST1）が NET1 から NET2 へ移動した場合，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 9 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 10 に示す．GSCIP ではドメインが階層構造になっていて，端末がドメインの内外を跨って移動するような場合においても，その都度 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一切発生しない．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ーと 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ーと IKE の設定を追加する必要もあり，その管理負荷はそれぞれ 16, 12 となり，ST1 の管理負荷の合計は 33 となる．また移動していない SGW に対しても管理負荷が 29 発生する．図 5 のネットワーク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 が 2 台以上存在することも十分考えられる．この場合，さらに設定追加に伴う管理負荷が増加する．IKE にはメインモードの他にアグレッシブモードがある．アグレッシブモードでは，

表 10　ネットワーク構成変化時の管理負荷の違い

Table 10　Difference of measurement loads when the network configuration changes

GSCIP/DPRP			
	グループ鍵情報	GE 情報	合計
GES1	0	0	0
GEN	0	0	0
GES2	0	0	0

IPsec/IKE				
	鍵	セキュリティポリシー	IKE	合計
ST1	0	20（変更：Transport: 4, 追加：Tunnel: 16）	13（変更：1, 追加：12）	33
SGW	1（変更：1）	16（追加：Tunnel: 16）	12（追加：12）	29
ST2	1（変更：1）	4（変更：Transport: 4）	1（変更：1）	6

通信相手識別子および自端末識別子に FQDN などのユーザ ID を利用することが可能で，変更すべき設定の数を抑制する方法があるが，メインモードと同様に IKE の応答側は必ず静的 IP アドレスでないといけないなどの制約がある．

これらのことから，GSCIP は初期導入時の管理負荷の軽減や，端末の移動に伴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．

第6章　DPRP の今後の展開

FPN の目指す機能として位置透過性の他に，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）[31]，アドレス空間透過性に対して NATF（NAT Free protocol）[32]がある．

Mobile PPC は通信中に移動して IP アドレスが変化しても，第三の機器を必要とせず P2P で通信の継続を可能とするためのプロトコルである．通信中の端末が移動後に，移動前後の IP アドレスを含む通信識別子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．これにより 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空間からプライベートアドレス空間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）はアドレス変換装置（NAT BOX）とその背後のプライベートアドレスを持つ端末（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 BOX の NAT テーブルを強制的に生成する．以後の通信は外部端末側で NAT テーブルに合わせてポート番号変換し，NAT BOX では通常のアドレス変換処理を行う．これにより外部端末から通信開始が可能となり，アドレス空間透過性を実現することができる.

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同士で情報を交換し，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.

第7章　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 を実現するための通信アーキテクチャ GSCIP, および GSCIP の中でも重要な位置づけをしめる DPRP についてそれぞれの概念と関係を述べた. 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化通信に必要な動作処理情報テーブルを動的に生成し, 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, 動作処理情報テーブル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，かつ一般の TCP/UDP 通信開始に与える影響がほとんど無いことがわか

った．また，ネットワーク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．

謝辞

本研究を遂行するにあたり，多大なるご指導，ご鞭撻を賜りました，名城大学大学院理工学研究科　渡邊晃教授に心より厚く御礼申し上げます．

本研究を遂行するにあたり，多大なるご指導，ご鞭撻を賜りました，名城大学大学院理工学研究科　小川明教授，柳田康幸教授，宇佐見庄五講師に心より厚く御礼申し上げます．

本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学部情報科学科渡邊研究室の皆様に心より感謝いたします．とりわけ，本研究テーマである GSCIP グループにて深い議論をしていただいた，加藤尚樹氏，竹内元規氏，竹尾大輔氏，保母雅敏氏，増田真也氏，柳沢信成氏，坂本順一氏，瀬下正樹氏，榎本万人氏，金本綾子氏，後藤裕司氏に心より感謝します．

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

参 考 文 献

[1] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, “2005 CSI/FBI Computer Crime and Security Survey,” Computer Security Institute publication, Jul. 2005.

[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, Dec. 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」”，コンピュータセキュリティシンポジウム（CSS2001）論文集，pp. 67-72, Oct. 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-14, pp. 205-210, Jul. 2001.

[5] Kenichi Kourai, Toshio Hirotsu, Koji Sato, Osamu Akashi and Kensuke Fukuda, “Secure and Manageable Virtual Private Networks for End-users,” LNC2003, pp. 385-394, Sep. 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，pp. 200, Mar. 2004.

[7] Ohad Rodeh, Ken Birman, Mark Hayden and Danny Dolev, “Dynamic Virtual Private Networks,” Dept. of Computer Science, Cornell University, Technical Report TR98-1695, Aug. 1998.

[8] 加島伸吾，後藤幸功，荒木啓二郎，“DVPN の提案と応用”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2003）論文集，pp. 365-368, Jun. 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, Mar. 2004.

[10] Darrell Kindred and Daniel Sterne, “Dynamic VPN Communities: Implementation and Experience,” DISCEX II’01, pp. 254-263, Jun. 2001.

[11] 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, Jun. 1999.

[12] 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, Dec. 2001.

[13] 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, Apr. 1997.

[14] Chung Kei Wong, Mohamed Gouda and Simon S. Lam, “Secure Group Communications Using Key Graphs,” SIGCOMM’98, pp. 68-79, Sep. 1998.

[15] 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, Nov. 1999.

[16] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, John Schultz, Jonathan Stanton and Gene Tsudik, “Secure Group Communication Using Robust Contributory Key Agreement,” IEEE Trans. on Parallel Distributed Systems, Vol. 15, No. 5, pp. 468-480, May 2004.

[17] H. Harney, U. Meth, A. Colegrove and G. Gross, “GSAKMP: Group Secure Association Group Management Protocol,” Internet Draft, IETF, May 2005. draft-ietf-msec-gsakmp-sec-10.txt

[18] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” Internet Draft, IETF, Mar. 2005. draft-ietf-ipsec-rfc2401bis-06.txt

[19] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones, “SOCKS Protocol Version 5,” RFC1928, IETF, Mar. 1996.

[20] T. Dierks and C. Allen, “The TLS Protocol, Version 1.0,” RFC2246, IETF, Jan. 1999.

[21] 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, Mar. 2001.

[22] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC2409, IETF, Nov. 1998.

[23] National Institute of Standards and Technology, U.S. Department of Commerce, “Specification for the Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, Nov. 2001.

[24] OpenSSL. http://www.openssl.org/

[25] Ethereal. http://www.ethereal.com/

[26] Tatsuya Jinmei, Kazu Yamamoto, Munechika Sumikawa, Yoshinou Inoue, Kazushi Sugyo and Shoichi Sakane, “An Overview of the KAME Network Software: Design and implementation of the advanced internetworking platform,” INET99, Jun.

1999. http://www.isoc.org/inet99/proceedings/4s/4s_2.htm

[27] KAME Project. http://www.kame.net/

[28] Charlie Kaufman, “Internet Key Exchange (IKEv2) Protocol,” Internet Draft, IETF, Sep. 2004. draft-ietf-ipsec-ikev2-17.txt

[29] Intel Corporation, “IA-32 Intel Architecture Software Developer’s Manual, Volume 2B: Instruction Set Reference, N-Z,” pp. 4-207-4-208, Apr. 2005. http://developer.intel.com/design/Pentium4/documentation.htm

[30] E. Rescorla, “Diffie-Hellman Key Agreement Method,” RFC2631, IETF, Jun. 1999.

[31] 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，pp. 17-24, Sep. 2004.

[32] 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”，情報学ワークショップ（WiNF2004）論文集，pp. 222-225, Sep. 2004.

研　究　業　績

1. 学術論文

❖ 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，推薦論文（条件付採録）

2. 国際会議

❖ Shinya Masuda, Hidekazu Suzuki, Naonobu Okazaki and Akira Watanabe, “Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls,” The International Conference on Information Networking (ICOIN2006), Jan. 2006.

3. 口頭発表

1) 鈴木秀和，渡邊晃，“イントラネットに柔軟な閉域通信グループを実現する動的処理解決プロトコル DPRP の検討”, 平成 15 年度電気関係学会東海支部連合大会論文集，pp. 359, Oct. 2003.
2) 鈴木秀和，渡邊晃，“GSCIP を構成する DPRP の仕組みの検討”，情報処理学会第 66 回全国大会講演論文集，pp. 3-479, Mar. 2004.
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 の仕組み”, 情報処理学会研究報告, 2005-CSEC-26, pp. 259-266, Jul. 2004.
4) 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-CSEC-28, pp. 199-204, Mar. 2005.
5) 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”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005，No. 6，pp. 441-444, Jul. 2005.
6) 鈴木秀和，渡邊晃，“動的処理解決プロトコル DPRP の性能評価”，平成 17 年度電気関係学会東海支部連合大会論文集，講演番号 O-229, Sep. 2005.
7) 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，2005-MBL-32，pp. 29-35, Mar. 2005.
8) 竹内元規, 鈴木秀和, 渡邊晃, “エンドエンドで移動透過性を実現する Mobile PPC の実装と評価” マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005，No. 6，pp. 125-128, Jul. 2005.
9) 竹内元規，鈴木秀和，瀬下正樹，渡邊晃，“移動通信プロトコル Mobile PPC の実装とその評価”，平成 17 年度電気関係学会東海支部連合大会論文集，講演番号 O-225, Sep. 2005.
10) 増田真也，鈴木秀和，渡邊晃，“IPv4/v6 混在環境における暗号通信方式の考察”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005，No. 6，pp. 693-696, Jul. 2005.
11) 坂本順一，鈴木秀和，竹内元規，渡邊晃，“Mobile P2P を利用した移動ネットワークの提案”，平成 16 年度電気関係学会東海支部連合大会論文集，講演番号 O-382, Sep. 2004.
12) 坂本順一，鈴木秀和，竹内元規，渡邊晃，“Mobile PPC を利用したネットワーク単位の移動通信の提案”，情報処理学会第 67 回全国大会講演論文集，講演番号 5U-7, Mar. 2005.
13) 坂本順一，鈴木秀和，竹内元規，渡邊晃，“Mobile PPC を利用したネットワーク単位の移動透過性の提案”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005, No. 6, pp. 133-136, Jul. 2005.
14) 坂本順一，鈴木秀和，竹内元規，渡邊晃，“ネットワーク単位の移動透過性を実現する Mobile NPC とその実装”，平成 17 年度電気関係学会東海支部連合大会論文集，講演番号 O-227, Sep. 2005.
15) 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, 講演番号 O-231, Sep. 2005.
16) 柳沢信成，加藤尚樹，鈴木秀和，渡邊晃，“グローバルアドレス環境を挟んだプライベートアドレス端末同士の通信の提案と実装”，情報処理学会研究報告，2005-DPS-122，pp. 357-362, Mar. 2005.
17) 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”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005, No. 6, pp. 369-372, Jul. 2005.
18) 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，2005-DPS-122, pp. 351-356, Mar. 2005.

19) 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を可能とする NATF（NAT Free protocol）の検討と実装”，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）論文集（査読付き），Vol. 2005，No. 6，pp. 373-376, Jul. 2005.
20) 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”，情報学ワークショップ（WiNF2005）論文集，pp. 142-146, Sep. 2005.
21) 榎本万人，坂本順一，鈴木秀和，渡邊晃，“異なるアドレス空間を跨る移動通信の検討”，平成 17 年度電気関係学会東海支部連合大会論文集，講演番号 O-230, Sep. 2005.

受　賞　歴

❖ 2005 年度 IEEE 名古屋支部学生奨励賞（IEEE Nagoya Section Student Paper Award）

付録A　GPACK 仕様書

I.　概要

GPACK は GSCIP を実装するためのソフトウェアを指し，特にカーネル部分に実装されるモジュール群の名称である．GPACK は IP 層に実装されるアーキテクチャで，パケットの送受信時に IP 層からパケットを渡される．GPACK はパケットのプロトコルを判別し，GPACK のモジュール群の中から適切なモジュールを呼び出す．各モジュールでの処理が終わったパケットは，状況に応じて IP 層に戻すか，破棄する．

II.　GPACK 動作概要

(1) GPACK の呼び出し

図 A-1 に GPACK の構造を示す．GPACK は `ip_input()`，`ip_output()`および `ip_fragment()` の複数の箇所から呼び出される．呼び出す際にどの箇所から呼ばれたかを区別するために，呼び出しモードを設定する．図 A-2 に GPACK の呼び出しの概要図を示す．また表 A-1，表 A-2，表 A-3 に `ip_input()`，`ip_output()`，`ip_fragment()`における GPACK の呼び出し箇所と対応する呼び出しモードを示す

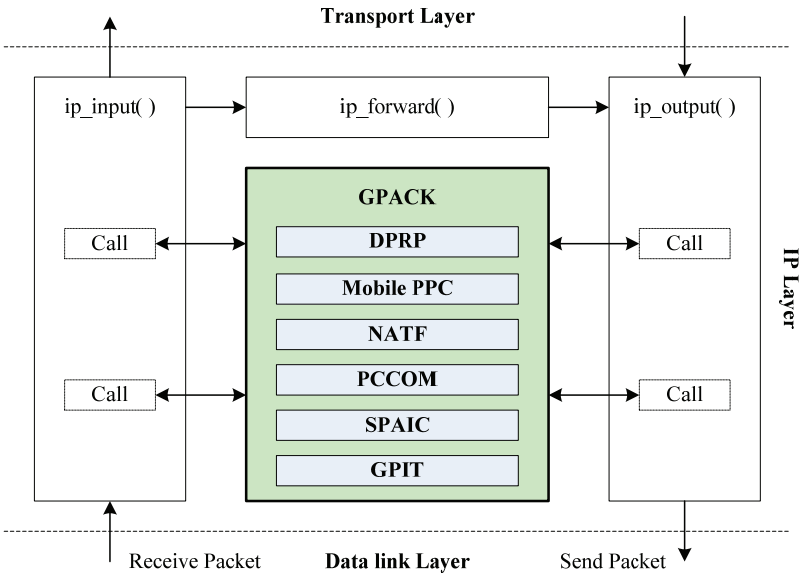


図 A-1　GPACK の構造

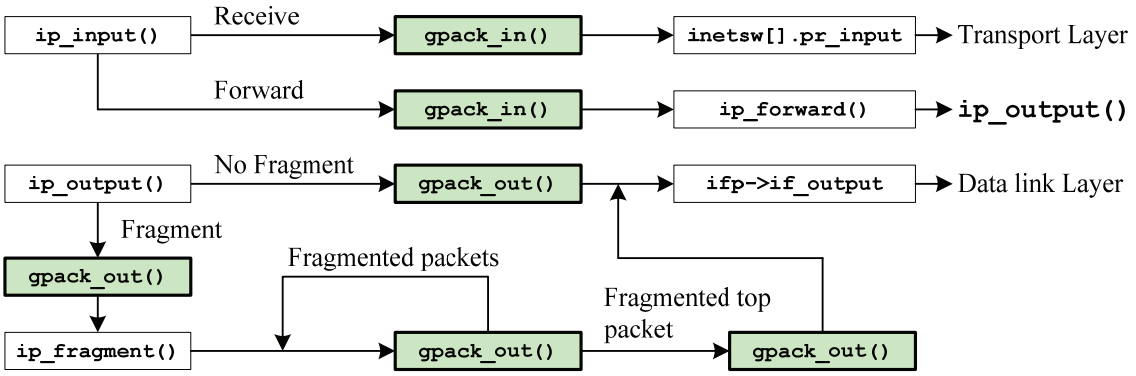


図 A-2　GPACK 呼び出しの概要

表 A-1　ip_input()における GPACK の呼び出し箇所

対象パケット	呼び出し箇所	呼び出しモード
転送パケット	ラベル passin:の ip_forward()の直前	GPACK_FWD
受信パケット	ラベル out:内	GPACK_RCV

表 A-2　ip_output()における GPACK の呼び出し箇所

対象パケット	呼び出し箇所	呼び出しモード
フラグメントなし	ラベル passout:の if_output()より前	GPACK_SND
フラグメント処理前	ラベル passout:の ip_fragment()より前	GPACK_BFRFRG

表 A-3　ip_fragment()における GPACK の呼び出し箇所

対象パケット	呼び出し箇所	呼び出しモード
フラグメント処理中	フラグメント処理を行う for 文内	GPACK_FRG
フラグメント処理後の先頭	フラグメント処理を完了した後	GPACK_FRGTOP

(2) GPACK 処理フロー

GPACK は IP 層から受け取ったパケットの種類に応じて処理を行う．図 A-3 に ip_input()から呼ばれる gpack_in()の処理を，また図 A-4 に ip_output()および ip_fragment()の複数の箇所から呼ばれる gpack_out()の処理を示す．

1. パケットのフラグメントチェック
   フラグメントされている場合 → 終了
2. パケットの長さをチェック
   異常な場合 → 終了（ip_input()でパケット破棄）
3. パケットのプロトコルタイプをチェック
   A) TCP の場合
      TCP 除外ポートかチェック
        除外ポートに一致　→ 終了
        除外ポートに不一致 → 4. PIT 検索へ
   B) UDP の場合
      UDP 除外ポートかチェック
        除外ポートに一致　→ 終了
        除外ポートに不一致 → 4. PIT 検索へ
   C) ICMP の場合
      DPRP を実行 → 終了（処理結果に応じて ip_input()でパケット破棄）
4. PIT 検索
   A) 該当情報あり
      動作処理内容をチェック
        暗号化／復号 → PCCOM を実行して終了
        透過中継　　→ 終了
        破棄　　→ 終了（ip_input()でパケット破棄）
   B) 該当情報なし
      DPRP を実行 →終了（処理結果に応じて ip_input()でパケット破棄）

図 A-3　gpack_in()の処理概要

1. 呼び出しモードのチェック
   GPACK_BFRFRG，GPACK_FRG，GPACK_FRGTOP の場合 → 終了
2. パケットの長さをチェック
   異常な場合 → 終了（ip_output()でパケット破棄）
3. パケットのプロトコルタイプをチェック
   A) TCP の場合
      TCP 除外ポートかチェック
        除外ポートに一致　→ 終了
        除外ポートに不一致 → 4. PIT 検索へ
   B) UDP の場合
      UDP 除外ポートかチェック
        除外ポートに一致　→ 終了
        除外ポートに不一致 → 4. PIT 検索へ
   C) ICMP の場合
        終了
4. PIT 検索
   A) 該当情報あり
      動作処理内容をチェック
        暗号化／復号 → PCCOM を実行して終了
        透過中継　　→ 終了
        破棄　　→ 終了（ip_output()でパケット破棄）
   B) 該当情報なし
      DPRP を実行 →終了（処理結果に応じて ip_output()でパケット破棄）

図 A-4　gpack_out()の処理概要

(3) 動作設定

GPACK の設定はユーザランドのプログラム, デーモンにより行われる. 図 A-5 に動作設定の仕組みを示す. GPACK の設定に必要な情報は/etc 内の GE 設定ファイル gscip.conf，鍵ファイル gscip.key，除外ポート定義ファイル gscip.filter の 3 つのファイルに記述する．/etc/rc.d 内のデーモン gscip により/usr/sbin 内のプログラム setgscip が実行され，システムコール syscall_gpack_init()により GPACK カーネルの設定を行う. デーモンは GPACK の設定だけでなく，GPACK の動作のオンオフを切り替えることも同時に行う.

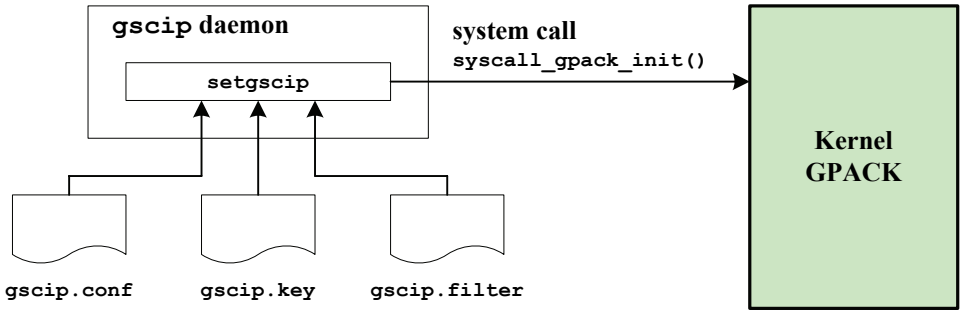


図 A-5　GPACK の動作設定の仕組み

❖ 起動スクリプト設定ファイル rc.conf

デーモン gscip を利用する場合，rc.conf の設定を行う必要がある．このファイルでは表 A-4 に示す項目の設定を行う．図 A-6，図 A-7 に GES，GEN として動作させる場合の記述例を示す．記述スタイルは rc.conf に準ずる.

表 A-4　起動スクリプト設定ファイル rc.conf の設定内容

項目	記述の型	説明
gscip_enable	“YES”|”NO”	デーモンの自動起動
gscip_file	文字列	GE 設定ファイルのパス
gscip_key	文字列	鍵ファイルのパス
gscip_filter	文字列	除外ポート定義ファイルのパス
gscip_interface	文字列	外側のインタフェース名

```
# GSCIP Configuration for GES
gscip_enable=”YES”
gscip_file=”/etc/gscip.conf”
gscip_key=”/etc/gscip.key”
gscip_filter=”/etc/gscip.filter”
```

図 A-6　GES の場合の rc.conf の記述例

```
# GSCIP Configuration for GEN
gscip_enable="YES"
gscip_file="/etc/gscip.conf"
gscip_key="/etc/gscip.key"
gscip_filter="/etc/gscip.filter"
gscip_interface="em0"    # GEN が構成するサブネットの外側インタフェース名を設定

gateway_enable="YES"
firewall_enable="YES"    # ファイアウォールを動作
firewall_type="OPEN"     # firewall_XXX の設定は各自で適切に設定すること
firewall_quiet="NO"
```

図 A-7　GEN の場合の `rc.conf` の記述例

❖ GE 設定ファイル `gscip.conf`

GE 設定は `gscip.conf` に記述する必要がある．このファイルでは表 A-5 に示す項目の設定を行う．図 A-8 に GE 設定ファイルの記述例を示す．

表 A-5　GE 設定ファイル `gscip.conf` の設定内容

項目	記述の型	説明	備考
uid	数値	ユーザ ID	0≦数値＜2^{32}
mode	`OP`|`CL`	動作モード	`OP`：開放モード，`CL`：閉域モード
group	数値	所属通信グループ番号	0≦数値＜2^{16} ※複数所属の場合は“,”区切りで続けて記述

```
# GSCIP Configuration File
uid   = 286331153
mode  = OP
group = 1,2

# コメントは行頭に"#"を記述
# 項目と"="と設定値の間は，スペースおよびタブを挿入してもよい
```

図 A-8　GE 設定ファイル `gscip.conf` の記述例

❖ 鍵ファイル `gscip.key`

鍵情報は `gscip.key` に記述する必要がある．このファイルでは表 A-6 に示す項目の設定を行う．図 A-9 に鍵ファイルの記述例を示す．

表 A-6　鍵ファイル gscip.key の設定内容

項目	記述の型	説明	備考
count	数値	鍵数	システム共通鍵とグループ鍵の合計
ck[n,v]	ck|gk	鍵の種類	ck：システム共通鍵，gk：グループ鍵
gk[n,v]	[数値,数値]	グループ鍵情報	n：通信グループ番号，v：バージョン番号 ※“,”区切りで続けて記述
	16 進数値	鍵データ	32 バイト長

```
# GSCIP Key File
count = 3
ck[0,0]   =9F34B7F7AE27DC71315C8885E7AC73826ECD5AC21357466C100DDD93BF15E4AE
gk[1,100] =31C1D5D03977674211B1C3FD79756732DC6E81B887DDC44C2CE1F4688EB51D1E
gk[2,200] =11D3DAA24667212515B2D3FF717A6A334BE9B2988DE8C52D9AA89FEA26BD498A

# コメントは行頭に“#”を記述
# 鍵設定の前に鍵数を記述
# 項目と“=”と設定値の間にスペースおよびタブを挿入してもよい
# 鍵数と鍵設定の数を一致させること．また GE 設定ファイルで定義した通信グループ番号と
# ここで設定するグループ鍵情報の通信グループ番号を一致させること
# 共通鍵の設定は 1 つに限る
```

図 A-9　鍵ファイル gscip.key の記述例

❖ 除外ポート定義ファイル gscip.filter

GPACK で処理を除外するポート番号の定義は gscip.filter に記述する必要がある．このファイルでは表 A-7 に示す項目の設定を行う．図 A-10 に除外ポート定義ファイルの記述例を示す．

表 A-7　除外ポート定義ファイル gscip.filter の設定内容

項目	記述の型	説明	備考
proto　n	tcp|udp	プロトコルタイプ	proto=tcp：TCP，proto=udp：UDP
	数値	除外ポート番号	$0 \leqq n < 2^{16}$

```
# GSCIP Except Port Filter File
tcp   80    # HTTP
tcp   10080 # Proxy

# コメントは行頭に“#”を記述
# プロトコルタイプと設定値の間にスペースまたはタブを挿入すること
```

図 A-10　除外ポート定義ファイル gscip.filter の記述例

付録B　GPIT 仕様書

I.　概要

GPIT（GSCIP Process Information Table）は，動的処理解決プロトコル DPRP により動的に生成される動作処理情報テーブルであり，通信パケットの処理内容を登録したものである．

II.　GPIT 動作概要

(1) テーブル構成

GPIT はハッシュテーブルのチェイン法として設計される．GPIT のテーブル構成を図 B-1 に示す．GPIT の配列をレコード（Record），チェインで繋がるレコードをリスト（List）と呼ぶ．

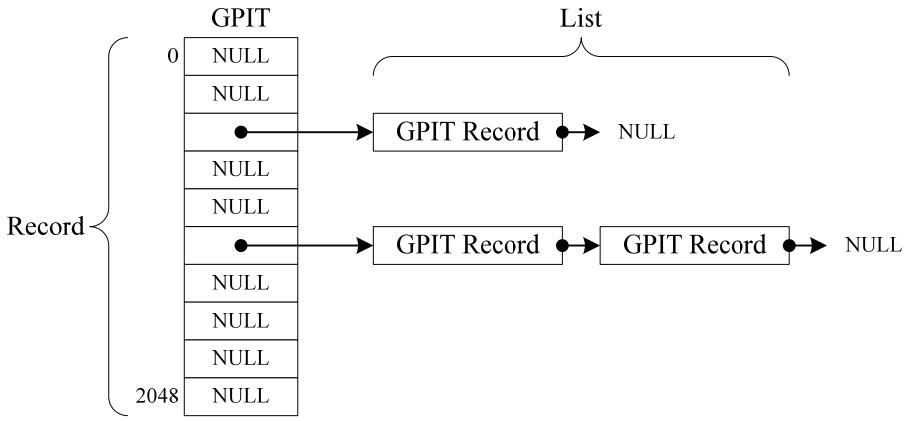


図 B-1　GPIT の構造

(2) GPIT Record フォーマット

GPIT Record は図 B-2 に示すフォーマットで定義される．各項目の内容を表 B-1 に示す．

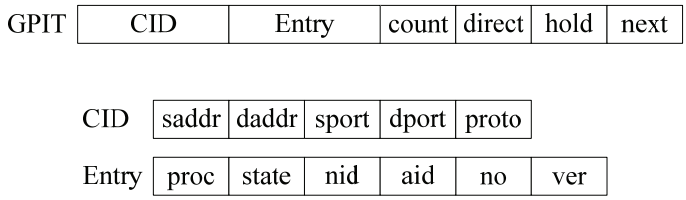


図 B-2　GPIT Record フォーマット

表 B-1　GPIT Record の項目

項目	説明
CID	通信識別子
saddr	送信元 IP アドレス
daddr	宛先 IP アドレス
sport	送信元ポート番号
dport	宛先ポート番号
proto	プロトコルタイプ
Entry	GPIT Record のエントリ情報
proc	処理内容
state	GPIT Record の状態
nid	NID を一時的に記憶する領域
aid	aID を一時的に記憶する領域
no	通信グループ番号
ver	バージョン番号
count	GPIT Record を削除するためのカウント値
direct	待避パケットの送受信方向
hold	待避パケットとなる mbuf のアドレスを格納
next	次 GPIT Record のアドレスを格納

(3) テーブルの初期化

デーモン gscip により GPACK が有効になるときにテーブルの初期化が行われる．初期化は全レコードに NULL を設定した後，カーネルタイマ（スケジューラ，callout）の初期化と設定を行う．

(4) タイマによる GPIT Record の管理

タイマにより指定時間毎に GPIT Record のカウント値を 1 ずつ減らす．PIT 検索が行われると，該当する GPIT Record のカウント値は初期値にリセットされる．カウント値が 0 になると，その GPIT Record の通信識別子で特定される通

信が行われていないと判断して，GPIT Record を削除し，リストの付け替え処理を行う．

(5) GPIT Record の検索

通信パケットの通信識別子 CID のハッシュ値を用いて GPIT を検索する．通信パケットから GPIT を検索する過程を図 B-3 に示す．検索の結果，通信パケットの通信識別子と GPIT Record の CID が一致したら，その GPIT Record のエントリ情報を返す. CID が一致しなかったり, GPIT Record が存在しない場合は，該当情報なしということで NULL を返す.

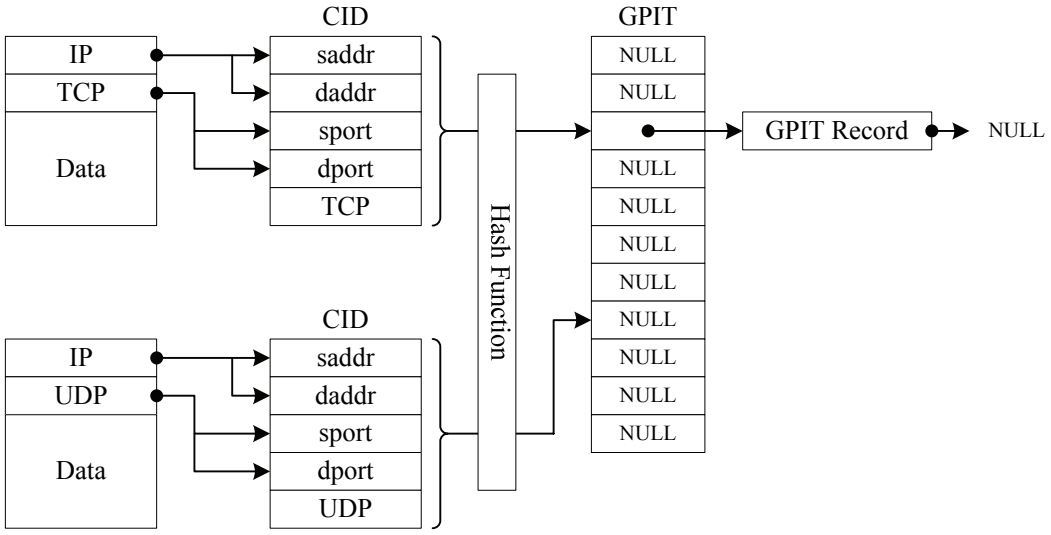


図 B-3　通信パケットから GPIT を検索する過程

(6) GPIT Record の登録

CID 情報とエントリ情報を用いて GPIT Record の登録を行う．図 B-4 に GPIT Record の登録過程を示す. まずテーブルを検索して該当する GPIT Record が存在する場合，エントリ情報を上書きする．該当する GPIT Record が存在しない場合, 新規に GPIT Record の領域を確保してエントリ情報を登録する. その後，作成した GPIT Record をレコードまたはリストに連結する．以上の処理が完了すると，次に逆方向の GPIT Record の登録作業を行う．CID 情報，エントリ情報の反転処理を行い, 逆方向の情報にして同様の処理を行う. また GPIT Record を登録する際に通信パケットを待避する場合，そのパケットの mbuf のアドレスと通信パケットの送受信方向を GPIT Record にセットする.

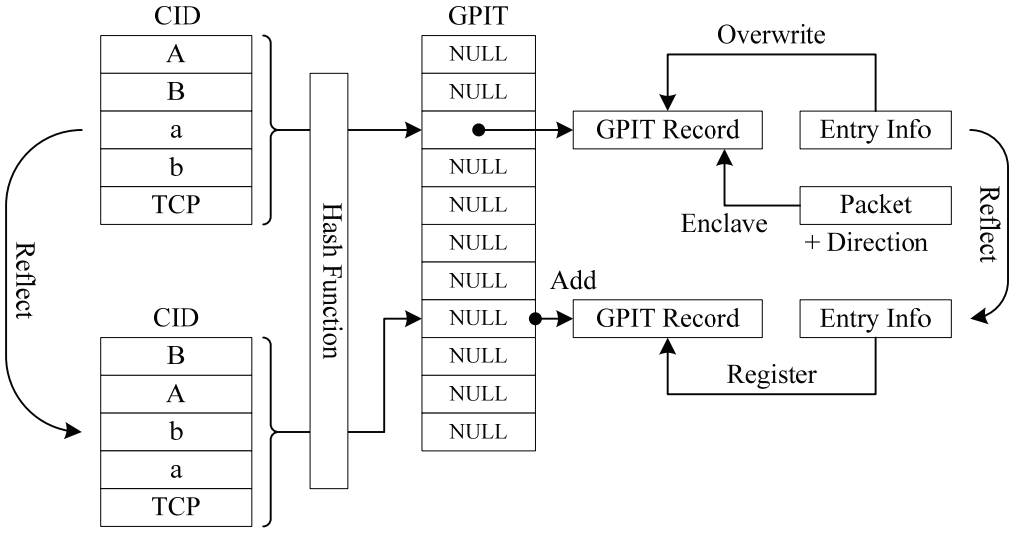


図 B-4　GPIT Record の登録過程

(7) GPIT Record の確定

CID 情報を用いて，作成中の GPIT Record の確定処理を行う．まずテーブルを検索して該当する GPIT Record が存在する場合，GPIT Record の状態を作成中から確定する. 該当する GPIT Record が存在しない場合, 何も処理を行わない. 以上の処理が完了すると，次に登録時と同様に，逆方向の GPIT Record の確定作業を行う．

(8) GPIT Record の削除

CID 情報を用いて，GPIT Record の削除を行う．まずテーブルを検索して該当する GPIT Record が存在する場合，その GPIT Record を削除する．該当する GPIT Record が存在しない場合，何も処理を行わない．その後，削除した GPIT Record の前後を連結する．以上の処理が完了すると，次に登録時と同様に，逆方向の GPIT Record の削除作業を行う．また GPIT Record を削除する際に通信パケットを待避していた場合，そのパケットも同時に削除する．

(9) 待避パケットの復帰処理

CID 情報を用いて，待避していた通信パケットの復帰処理を行う．まずテーブルを検索して該当する GPIT Record が存在し，かつ通信パケットを待避していた場合, GPIT Record にセットしている送受信方向を元に IP 層の入出力関数に通信パケットを渡す．送受信方向が「受信（RCV)」の場合，待避パケットを `ip_input()` に渡す．送受信方向が「送信（SND)」の場合，待避パケットをそのまま，`ip_output()` に渡す．通信パケットを待避していない場合や，該当する GPIT Record が存在しない場合，何も処理を行わない．

付録C　DPRP 仕様書

I.　概要

動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）は，FPN（Flexible Private Network）を実現するためのセキュア通信アーキテクチャ GSCIP（Grouping for Secure Communication for Internet Protocol；ジースキップ）を構成するプロトコルである．GSCIP を実現するモジュール群のことを GPACK（GSCIP PACKage）と呼び，GPACK を実装した装置を GE（GSCIP Element）という．

DPRP は通信に先立ち，通信相手が同一グループに帰属しているかを確認し，通信パケットをどのように処理するかを示す動作処理情報を動的に生成する．

II.　DPRP 動作概要

(1) ネットワーク構成

本仕様書は図 C-1 に示すネットワーク構成に基づいて説明する．表 C-1 に各 GE の通信グループ番号および動作モードの一覧を示す．端末は○が付いている通信グループに所属していることを示している．●は GEN または GEA によって保護されていることを示している．

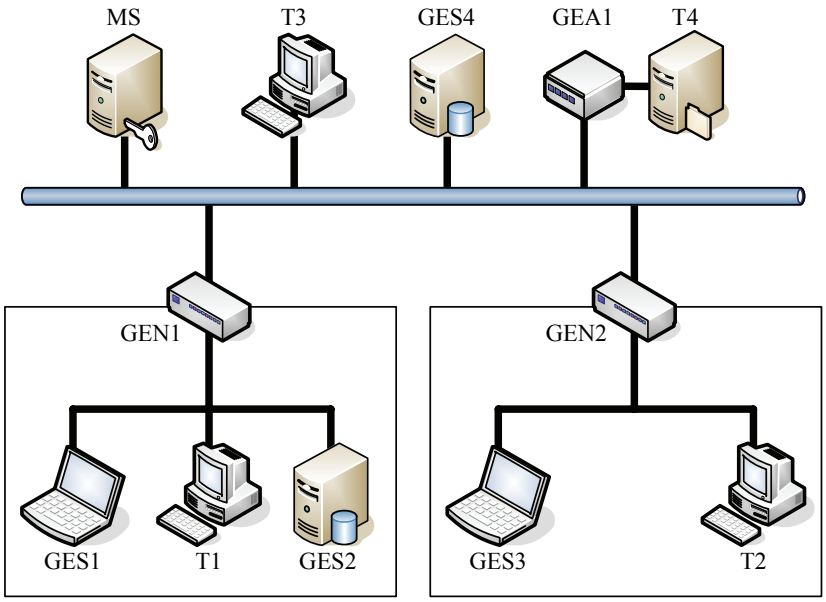


図 C-1　ネットワーク構成

表 C-1　GE の所属する通信グループと動作モードの一覧

端末	Group1 部署 1	Group2 部署 2	Group 3 役職 A	動作モード
GES1	○		○	OP
GES2	○			OP
GES3		○	○	OP
GES4	○			CL
GEN1	○			CL
GEN2		○		CL
GEA1			○	CL
T1	●（GEN1）			－
T2		●（GEN2）		－
T3				－
T4			●（GEA1）	－

(2) DPRP シーケンス

DPRP は DDE，RGI，MPIT，CDN の 4 種類の制御パケットを基本として，ネゴシエーションを行う．通信経路上の GE と T の組み合わせにより，7 種類のネゴシエーションのパターンがある．図 C-2 から図 C-8 に DPRP シーケンスのパターンを示す． DDE および RGI の宛先が T の場合，受信したその T は通常の ICMP 処理を行い，ICMP ECHO REPLY を応答する．この応答をそれぞれ DDE REPLY，RGI REPLY という．

❖ **通信ペアが共に GE の場合**

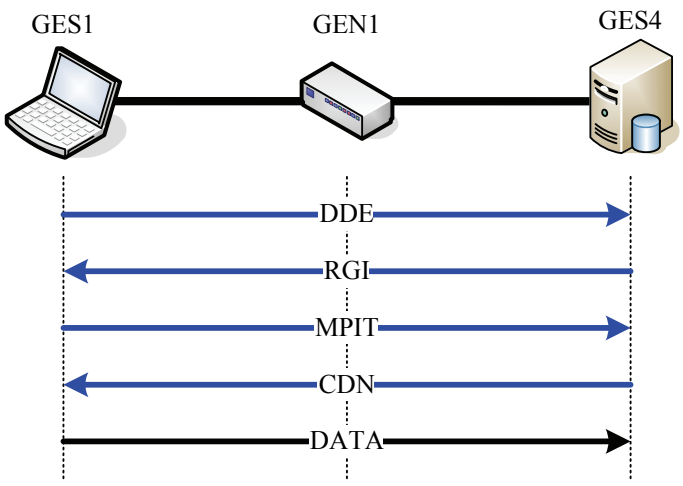


図 C-2　DPRP シーケンス（パターン 1）

❖ **送信元が T，宛先が GE で，通信経路上に中間 GE がある場合**

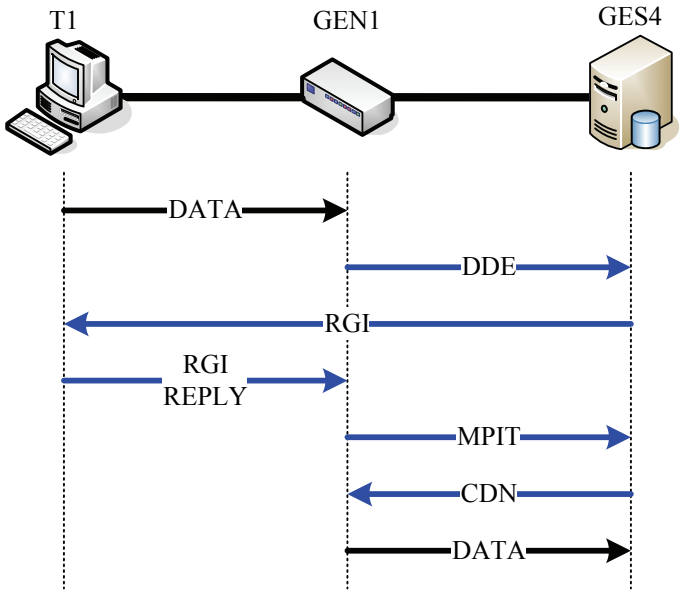


図 C-3　DPRP シーケンス（パターン 2）

❖ **送信元が GE，宛先が T で，通信経路上に中間 GE がある場合**

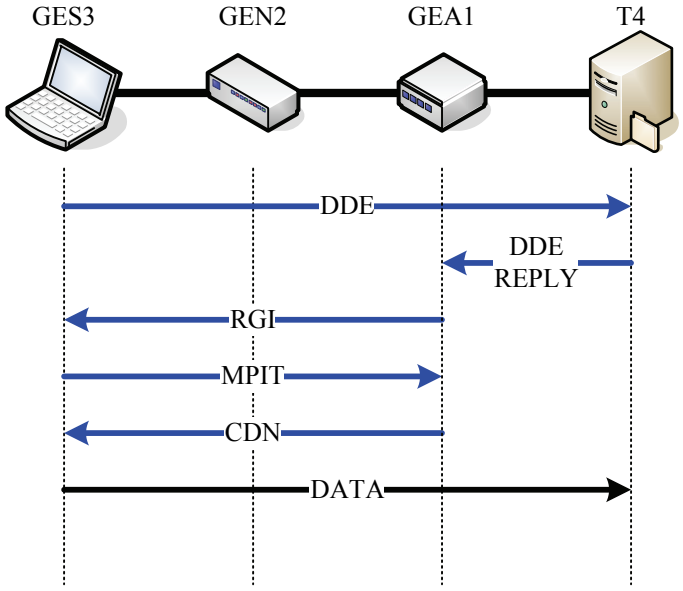


図 C-4　DPRP シーケンス（パターン 3）

❖ 通信ペアが共に T で，通信経路上に中間 GE が 2 台以上ある場合

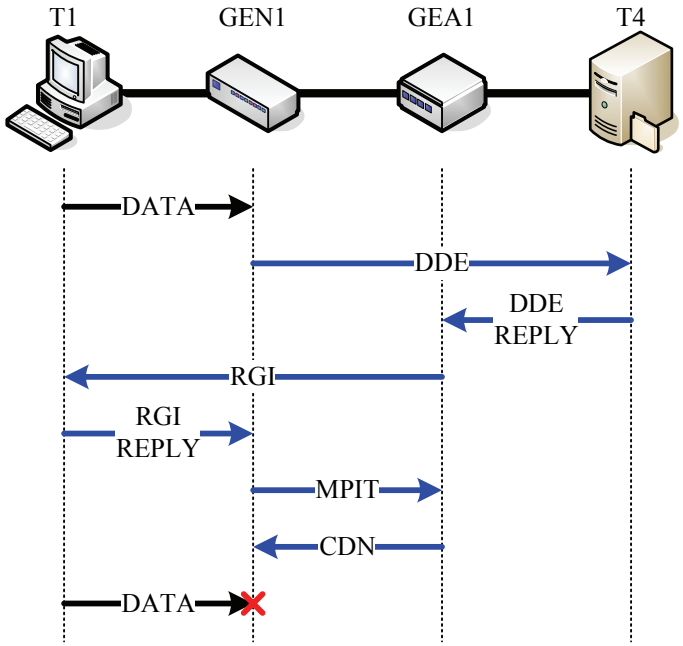


図 C-5　DPRP シーケンス（パターン 4）

❖ 通信ペアが共に T で，通信経路上に中間 GE が 1 台ある場合

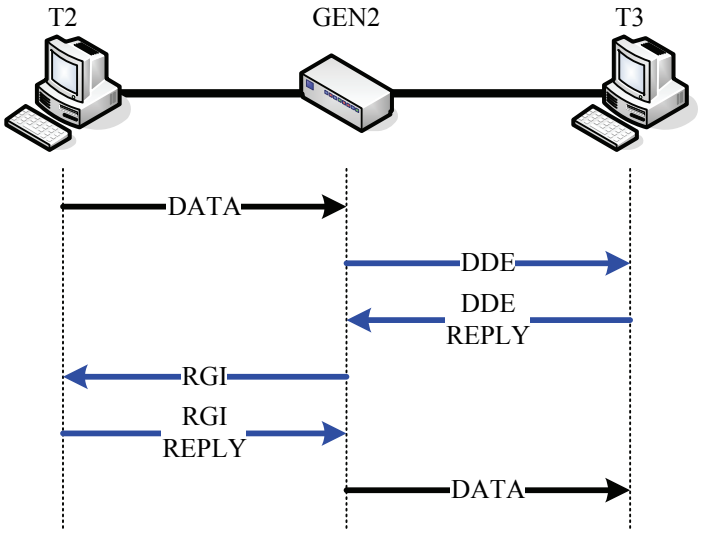


図 C-6　DPRP シーケンス（パターン 5）

❖ **送信元が T，宛先が GE で，通信経路上に中間 GE がない場合**

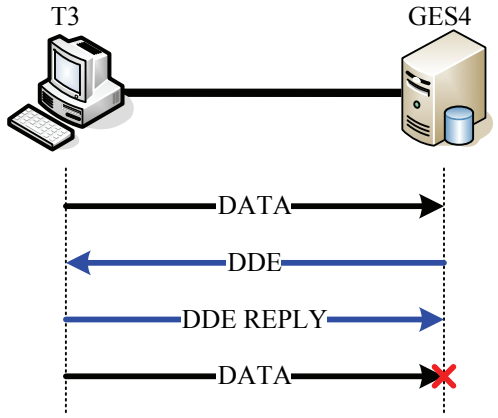


図 C-7　DPRP シーケンス（パターン 6）

❖ **送信元が GE，宛先が T で，通信経路上に中間 GE がない場合**

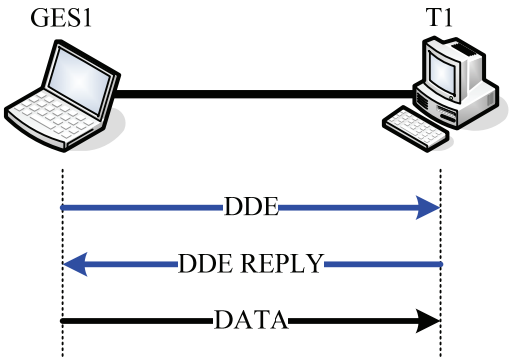


図 C-8　DPRP シーケンス（パターン 7）

(3) ネゴシエーションの開始

GE が通信パケットを受信すると，PIT を検索する．図 C-9 に送信パケットがネゴシエーションのトリガーとなる場合の，図 C-10 に受信パケットがネゴシエーションのトリガーとなる場合の PIT 検索から DDE 送信までの処理過程を示す．該当する PIT レコードが無い場合，DDE を生成する．DDE にはトリガーとなった通信パケットの通信識別子 CID（送信元/宛先 IP アドレス，送信元/宛先ポート番号，プロトコルタイプ）の情報がセットされる．DDE の宛先はトリガーとなった通信パケットの宛先とする．DDE が生成されたらシステム共通鍵 CK で暗号化する．その後，PIT を作成中としてから DDE を送信する．送信後，トリガーとなった通信パケットを待避して，そのパケットが送信パケットなのか，受信パケットなのかを PIT に記録しておく．

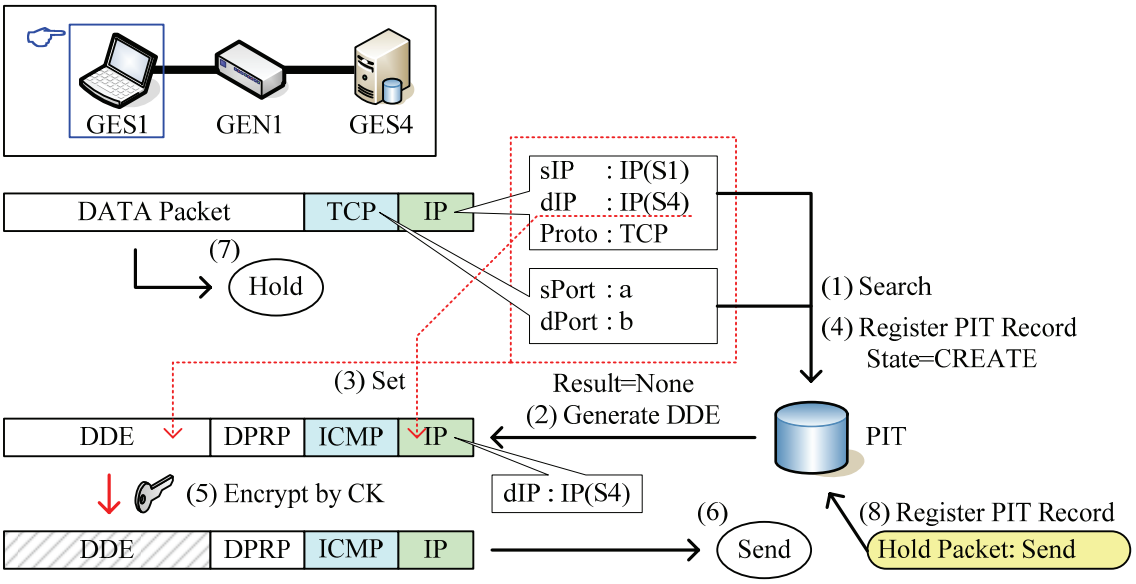


図 C-9　PIT 検索から DDE 送信までの処理過程（パターン 1）

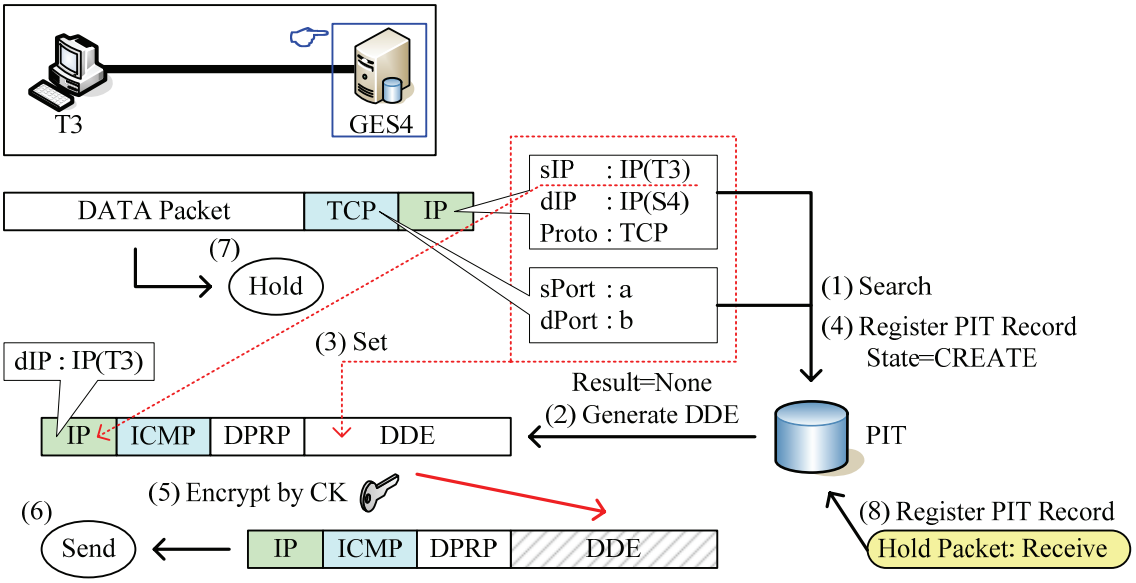


図 C-10　PIT 検索から DDE 送信までの処理過程（パターン 2）

(4) 終点 GE の決定方法

DDE を受信した GE は, DDE を受信するのか, 転送するのかをチェックする. 図 C-11 に DDE の宛先が GE の場合の，図 C-12 に DDE の宛先が T の場合の終点 GE の決定方法を示す．転送する場合は何も処理を行わずに転送する．受信するホストが GE の場合，受信した GE が終点 GE となる．受信するホストが T の場合，DDE REPLY を応答し，このパケットを最初に受信した GE が終点 GE となる.

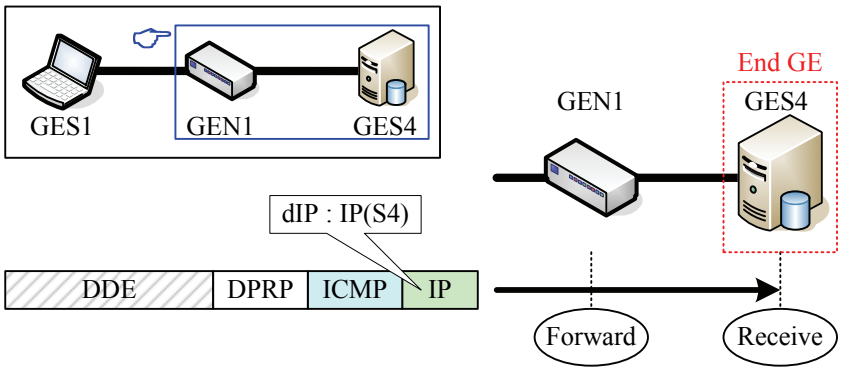


図 C-11　終点 GE の決定方法（パターン 1）

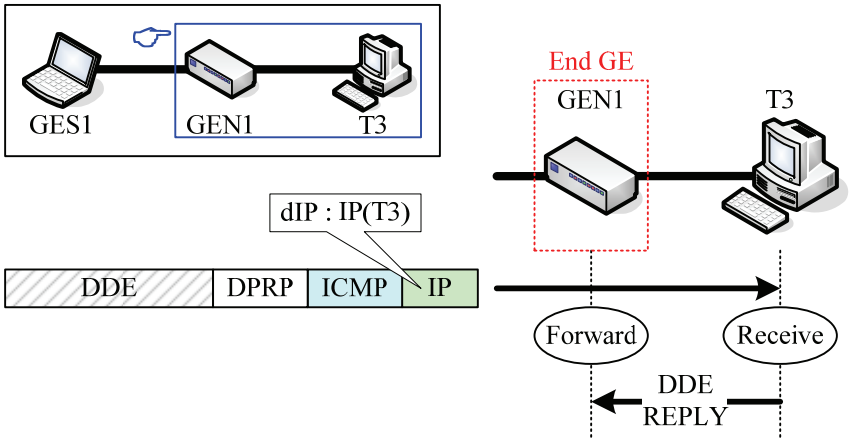


図 C-12　終点 GE の決定方法（パターン 2）

(5) GE 設定情報の追加

終点 GE は通信経路上の GE 設定情報を収集するため RGI を生成する．図 C-13 に DDE 受信から RGI 送信までの処理過程を示す．GE は乱数発生により aID を生成する．RGI には自端末の GE 設定情報と，生成した aID およびネゴシエーションの方向情報（Direct）がセットされる．表 C-2 にネゴシエーションの方向情報を示す．RGI の宛先は DDE のトリガーとなった通信パケットの送信元となる．よって DDE 内の CID にある sIP となる．RGI が生成されたらシステム共通鍵 CK で暗号化する．その後，PIT を作成中としてから RGI を送信する．

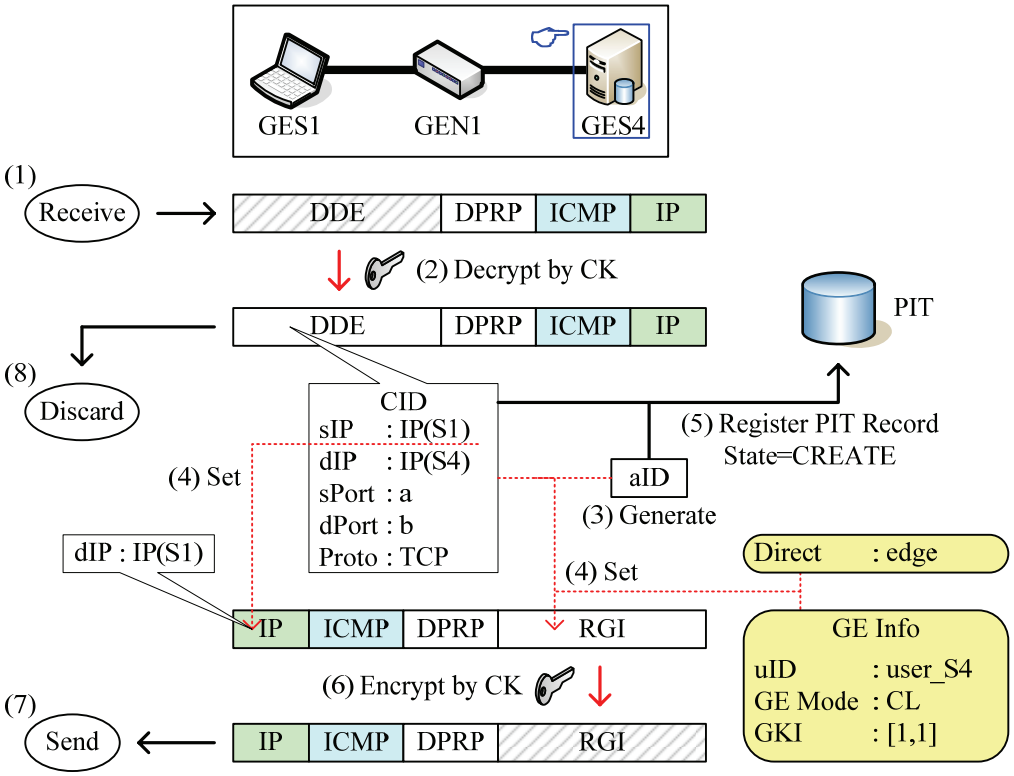


図 C-13　DDE 受信から RGI 送信までの処理過程

表 C-2　ネゴシエーションの方向情報

設定値	内容
edge	終端 GE の場合
inbound	RGI の送信方向が GEN および GEA の外側から内側の場合
outbound	RGI の送信方向が GEN および GEA の内側から外側の場合

RGI を受信した GE は CK で復号後，終点 GE と同様に aID を生成して GE 設定情報と一緒に RGI に追加する．追加後，PIT を作成中として RGI の宛先を

チェックする．図 C-14 のように転送する場合は CK で暗号化して送信する．図 C-15 のように転送しない場合は，その GE が始点 GE に決定する．

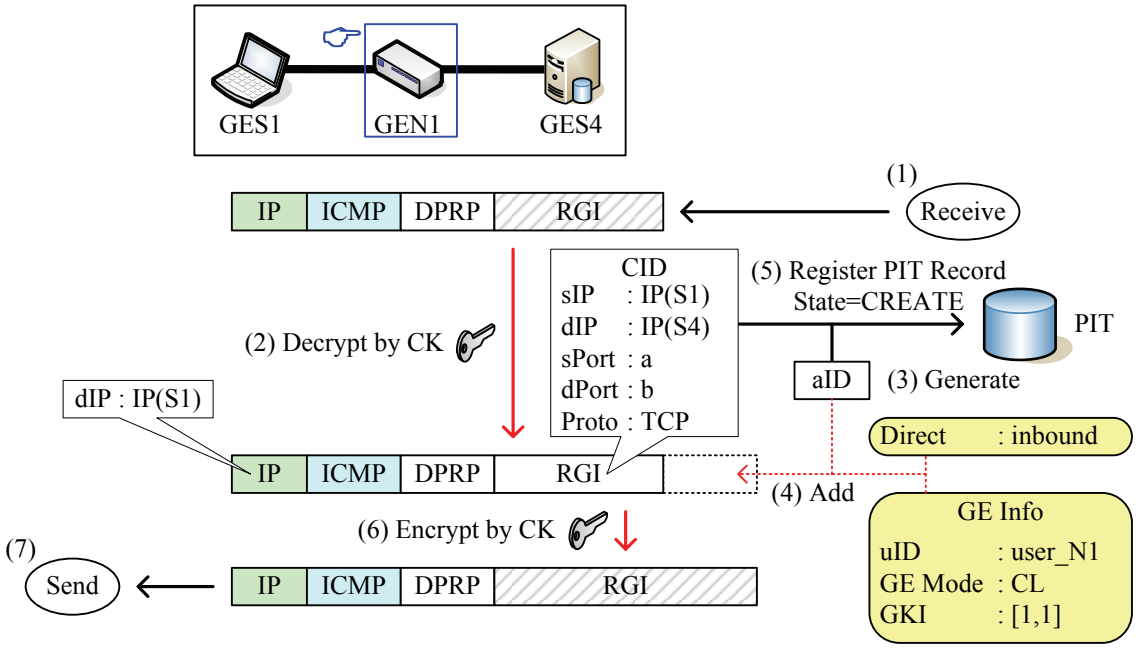


図 C-14　RGI 受信から転送までの処理過程

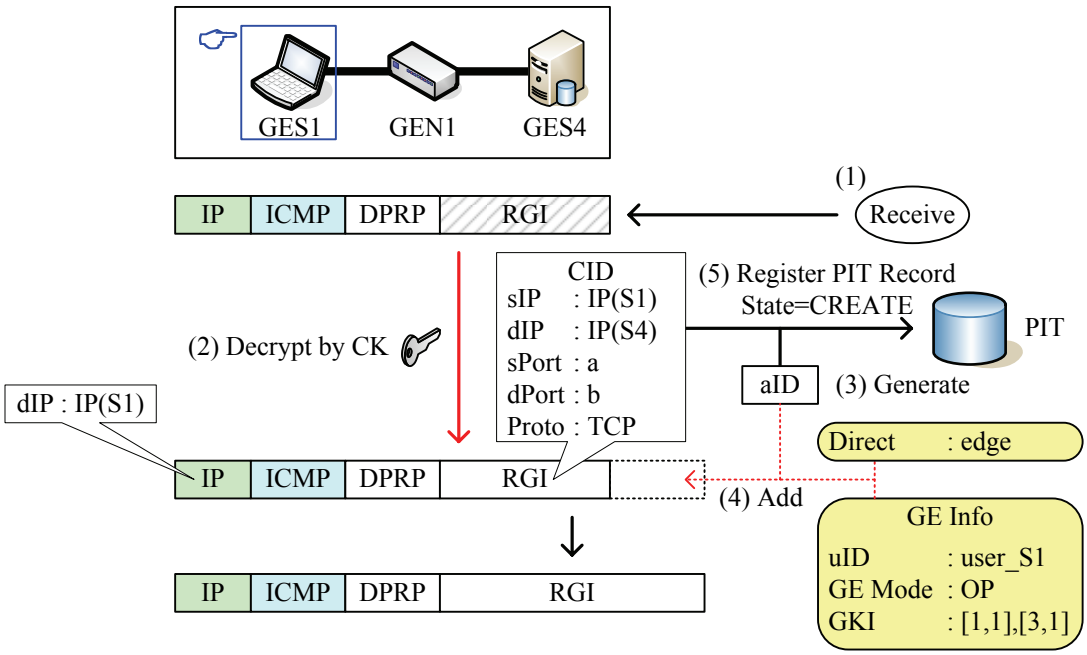


図 C-15　RGI 受信から始点 GE 決定までの処理過程

(6) 始点 GE の決定方法

RGI を受信した GE は，RGI を受信するのか，転送するのかをチェックする．図 C-16 に RGI の宛先が GE の場合の，図 C-17 に RGI の宛先が T の場合の終点 GE の決定方法を示す．受信するホストが GE の場合，受信した GE が始点 GE となる．受信するホストが T の場合，RGI REPLY を応答し，このパケットを最初に受信した GE が始点 GE となる．

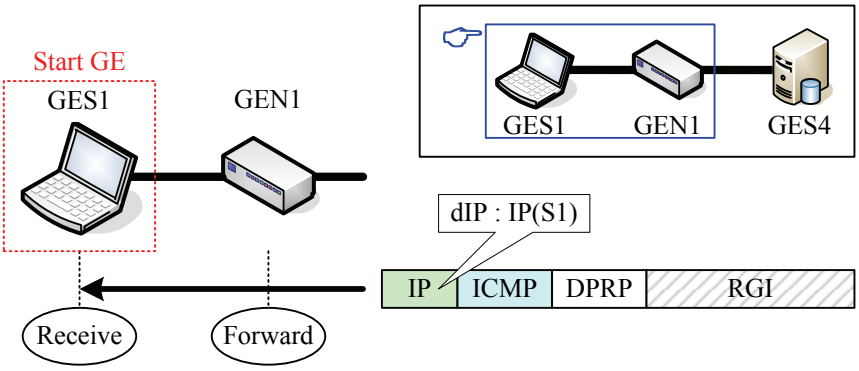


図 C-16　始点 GE の決定方法（パターン 1）

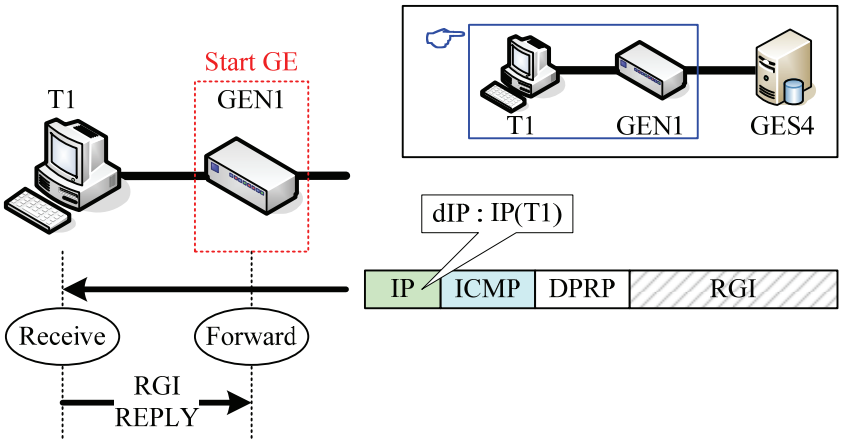


図 C-17　始点 GE の決定方法（パターン 2）

(7) 動作処理情報の決定プロセス

始点 GE は受信した RGI から通信経路上の図部手の GE 設定情報，aID とネゴシエーションの方向情報を取得することができる．取得した情報の数により以下の処理を行う．

❖ 取得した情報が 1 つの場合

図 C-18 に取得情報が 1 つの場合の動作処理情報決定プロセスを示す．動作モードを確認して，開放モードなら処理内容“Transparent”，閉域モードなら処理内容“Discard”の動作処理情報を生成する．

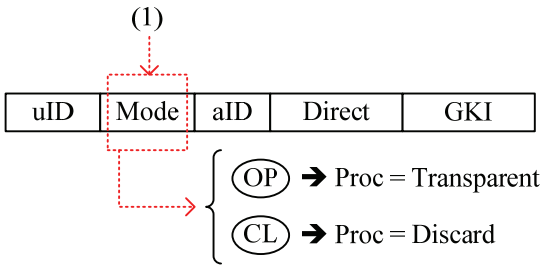


図 C-18　取得情報が 1 つの場合の動作処理情報決定プロセス

❖ 取得した情報が 2 つ以上の場合

図 C-19 のように取得した情報を分割関数により分割する．分割関数のアルゴリズムを図 C-20 に示す．

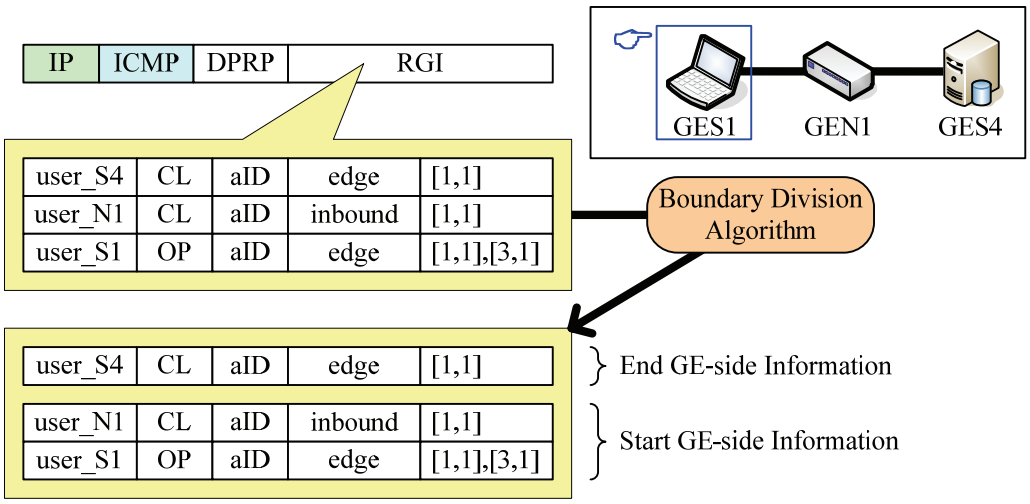


図 C-19　取得情報の分割処理

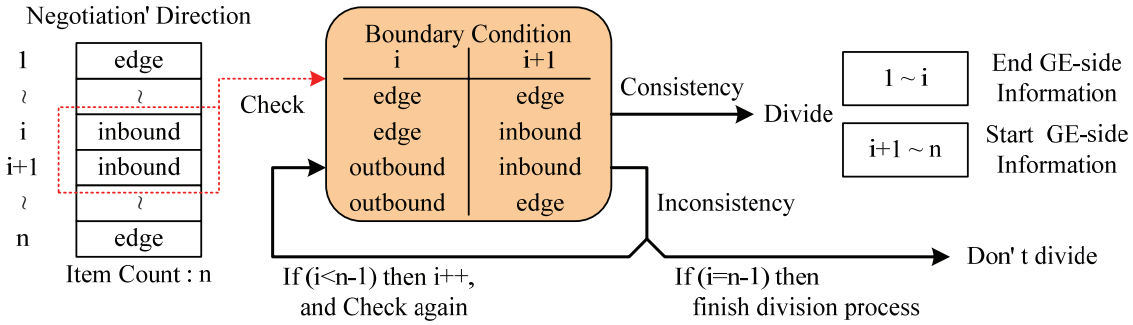


図 C-20　分割関数のアルゴリズム

分割処理の結果，分割されなかった場合は図 C-21 に示す動作処理情報決定プロセスを実行する．取得した情報の全動作モードを確認する．その結果，1 つも閉域モードがない，すなわち全て開放モードであれば処理内容 “Transparent” の動作処理情報を生成する．

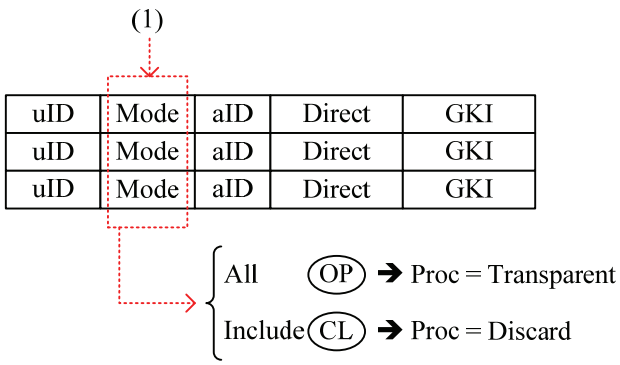


図 C-21　分割されなかった場合の動作処理情報決定プロセス

分割された場合は図 C-22 に示す動作処理情報決定プロセスを，図 C-23 に示す順番に従って繰り返し実行する．まずグループ鍵情報を比較する．その結果，一致したら処理内容 “Encrypt” の動作処理情報を生成する．一致しなかったら動作モードを比較する．始点 GE 側，終点 GE 側ともに閉域モードなら処理内容“Discard”の動作処理情報を生成する．終点 GE が開放モードなら終点 GE 側の情報の比較元を 1 つ始点 GE 側（図 C-23 の右方向）へシフトして，再度グループ鍵情報の比較を繰り返す．終点 GE 側の比較元が全て完了した場合，次は始点 GE 側の情報の比較先を 1 つ終点 GE 側（図 C-23 の上方向）へシフトして，同様に比較処理を繰り返す．始点 GE 側の比較先が全て完了した場合（図 C-23 の右上），処理内容“Discard”の動作処理情報を生成する．

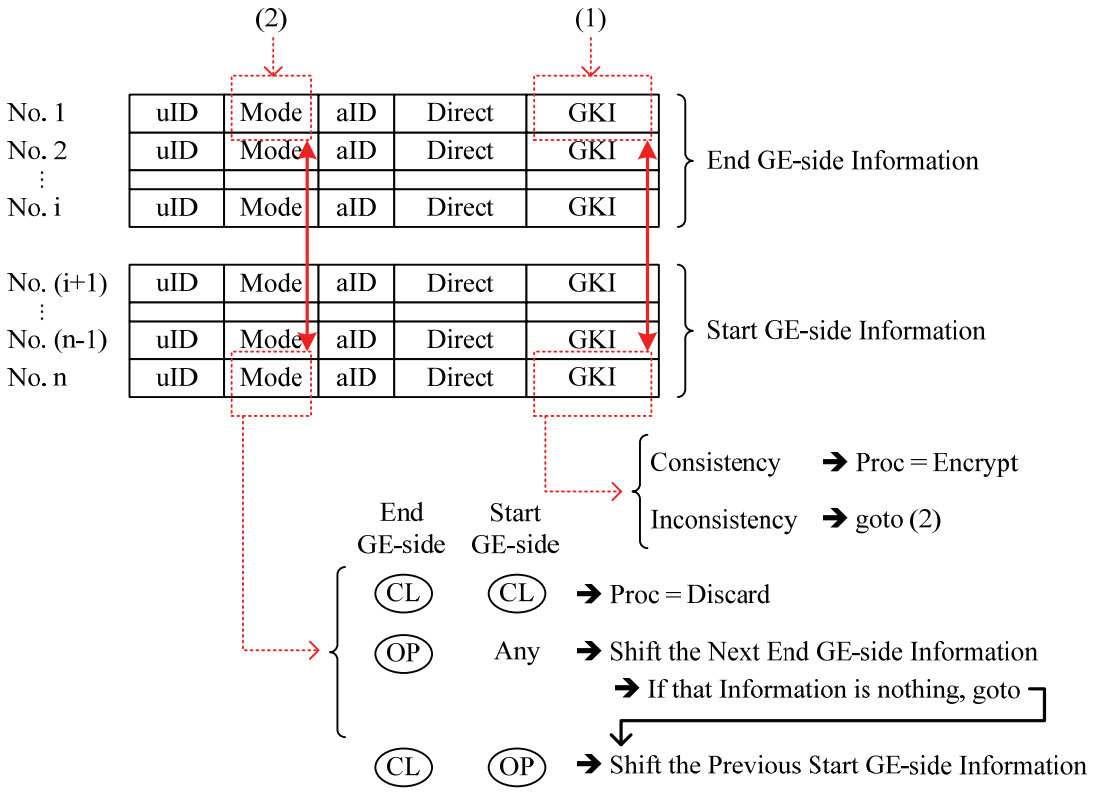


図 C-22　分割された場合の動作処理情報決定プロセス

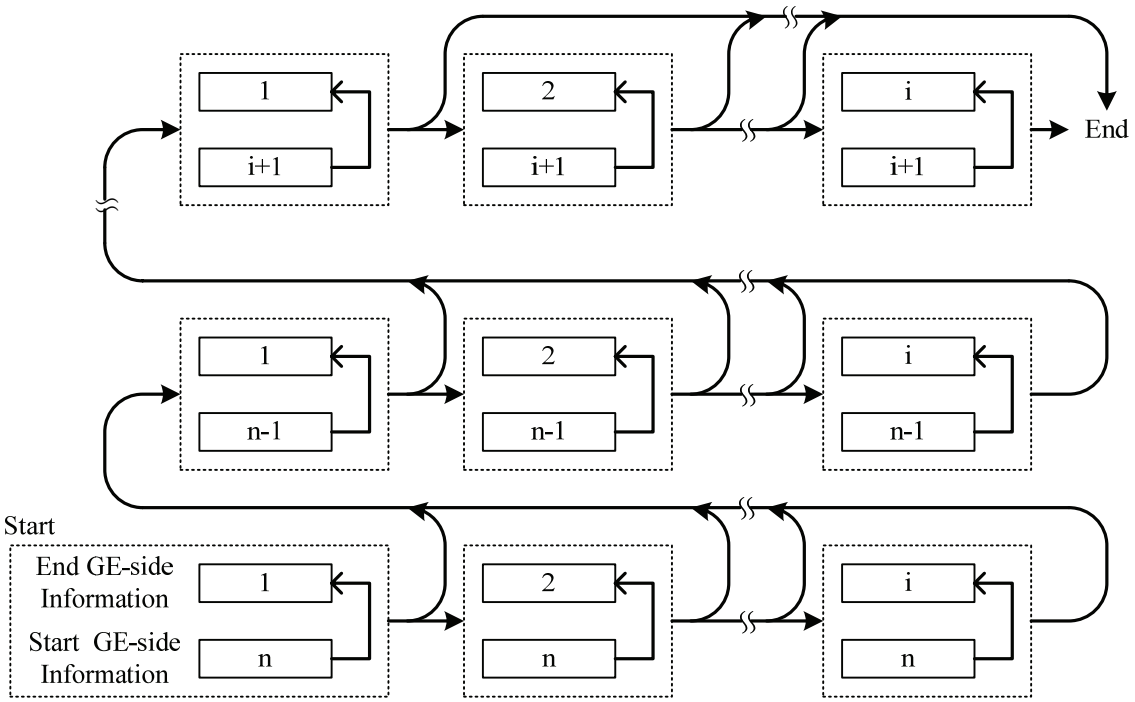


図 C-23　始点 GE 側と終点 GE 側の情報を比較する順序

(8) GE の認証処理と PIT 登録

図 C-24 に RGI 受信から MPIT 送信までの処理過程を示す．始点 GE は(7)で述べた処理に従って RGI から動作処理情報を生成する．生成された動作処理情報のうち，自端末に関する情報を PIT に登録し，ここで自端末に関する処理内容が“Encrypt”の場合，グループ鍵情報で指定されているグループ鍵 GK で，処理内容が“Decrypt”になっている動作処理情報の aID を暗号化する．その後，MPIT を生成して決定した動作処理情報と受信した aID が記載される．MPIT の宛先は受信した RGI の送信元となる．MPIT が生成されたらシステム共通鍵 CK で暗号化する．その後，MPIT を送信する

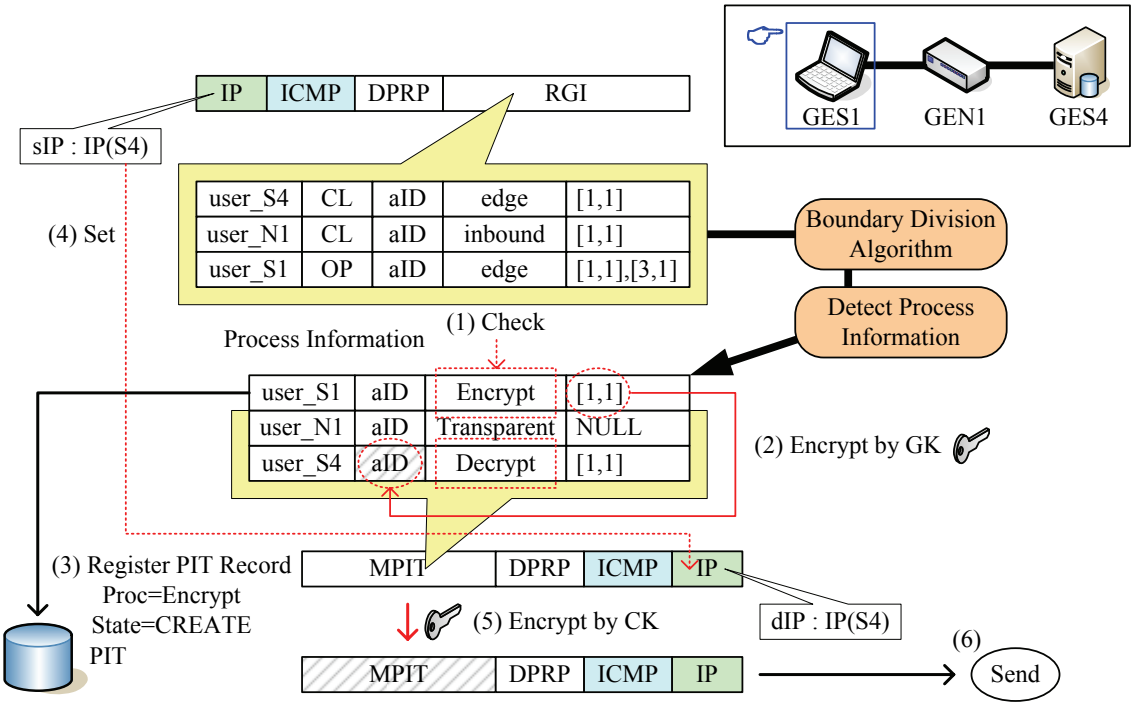


図 C-24　動作処理情報決定から MPIT 送信までの処理過程

MPIT を受信した GE は CK で復号後，MPIT 内の先頭にある動作処理情報の uID と自端末の uID 比較する．一致しなかった場合は，無効な MPIT と見なしてパケットを破棄する．一致したら表 C-3 に示す処理内容に対応した追加処理を行う．その後，動作処理情報の aID と PIT に登録しておいた aID を比較して認証を行う．認証結果が正しくない場合はパケットを破棄する．認証結果が正しい場合，PIT に動作処理情報を登録して，MPIT からこの動作処理情報を削除する．その後，図 C-25 のように転送する場合は CK で暗号化して送信する．図 C-26 のように終点 GE が受信した場合，CDN の生成を行う．

表 C-3　処理内容別の追加処理

処理内容	追加処理
Encrypt	決定したグループ鍵情報で指定されたグループ鍵 GK で，処理内容が“Decrypt”になっている動作処理情報の aID を暗号化（図 C-24）
Decrypt	決定したグループ鍵情報で指定されたグループ鍵 GK で，aID を復号（図 C-26）
Transparent	処理無し（図 C-25）
Discard	処理無し（図 C-25）

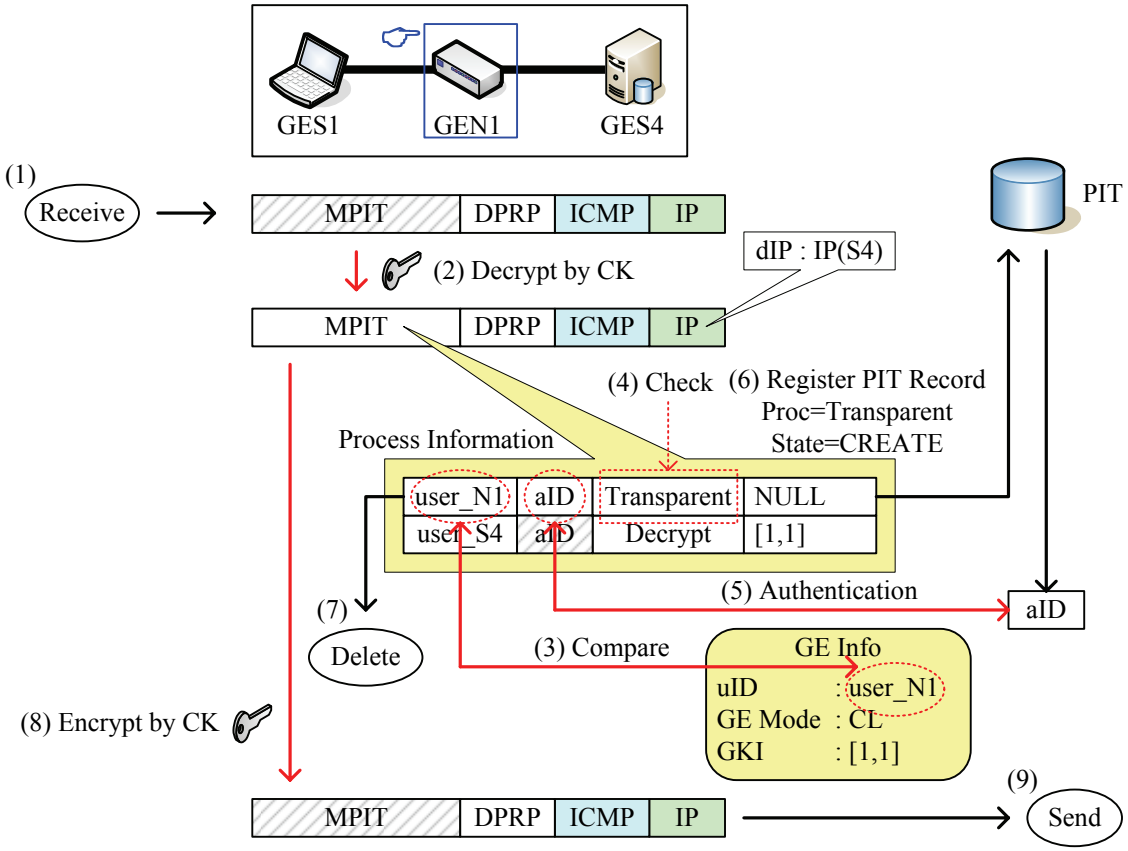


図 C-25　MPIT 受信から転送までの処理過程

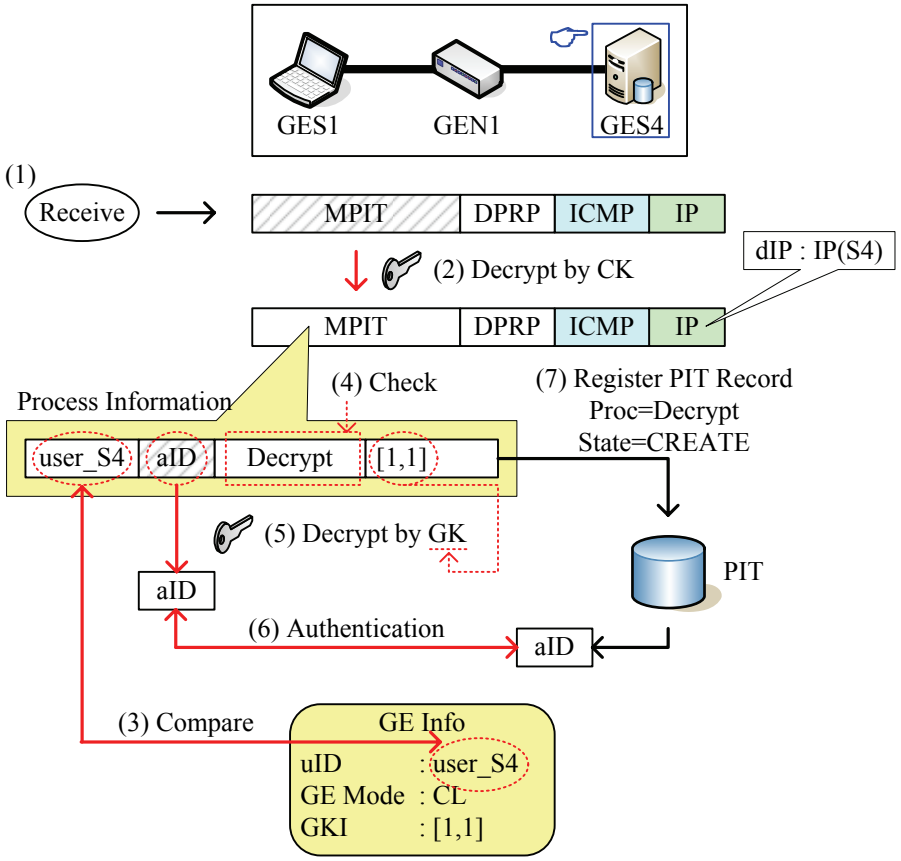


図 C-26　終点 GE における MPIT 受信から PIT 登録までの処理過程

(9) ネゴシエーションの完了通知

図 C-27 に PIT 登録から CDN 送信までの処理過程を示す．終点 GE は CDN を生成する．生成後，MPIT により登録された PIT を確定する．CDN の宛先は受信した MPIT の送信元となる．その後，CK で暗号化して送信する．

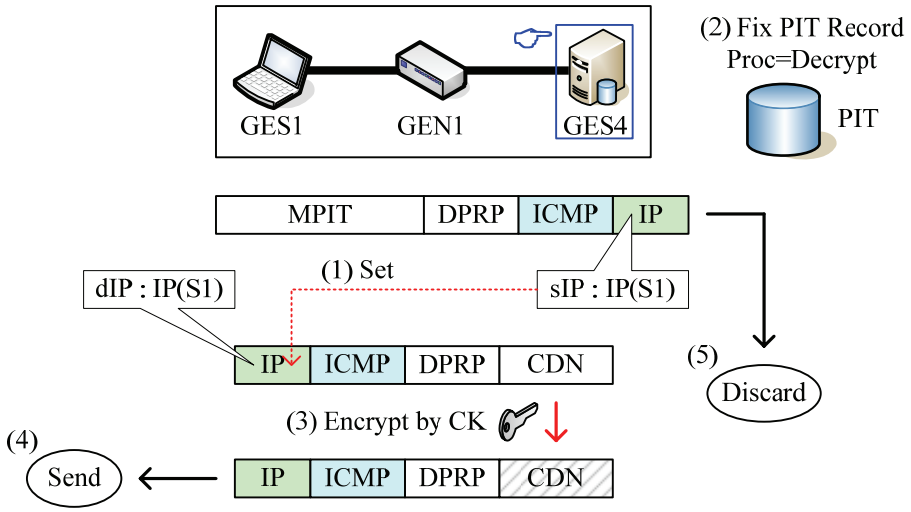


図 C-27　PIT 登録から CDN 送信までの処理過程

CDN を受信した GE は，先に作成中であった PIT を確定する．またパケットを待避していた場合は，そのパケットを送信または受信する．図 C-28 のように CDN を転送する場合は送信し，図 C-29 のように受信する場合は DPRP のネゴシエーションを完了する．

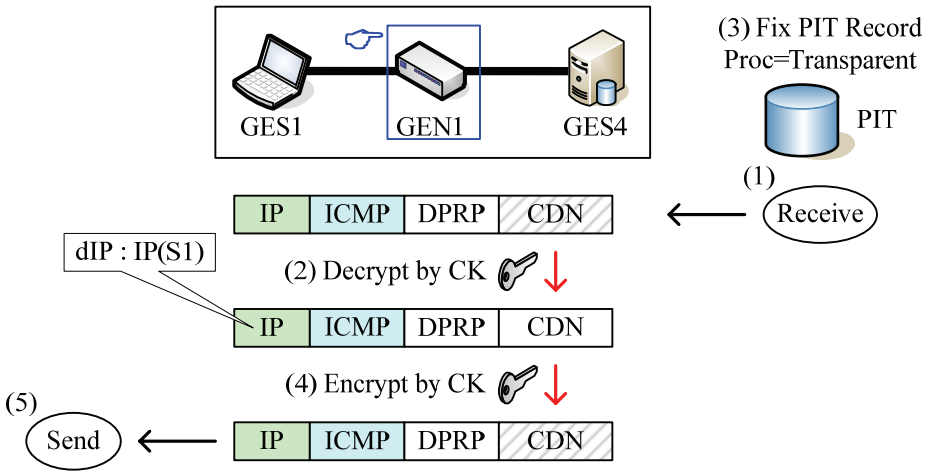


図 C-28　CDN 受信から転送までの処理過程

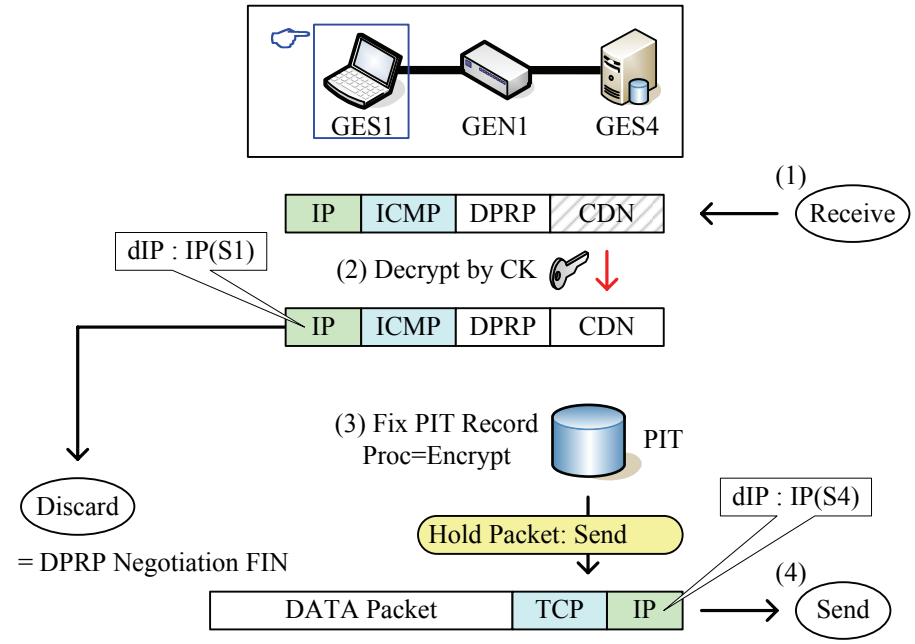


図 C-29　CDN 受信からネゴシエーション完了までの処理過程

III. DPRP 制御パケットフォーマット

(1) DPRP プロトコルフォーマット

DPRP 制御パケットは ICMP をベースに定義されている．図 C-30 に DPRP プロトコルのフォーマットを示す．ICMP ヘッダは DPRP 制御パケットの種類により異なるタイプが設定される．表 C-4 に ICMP のヘッダタイプを示す.

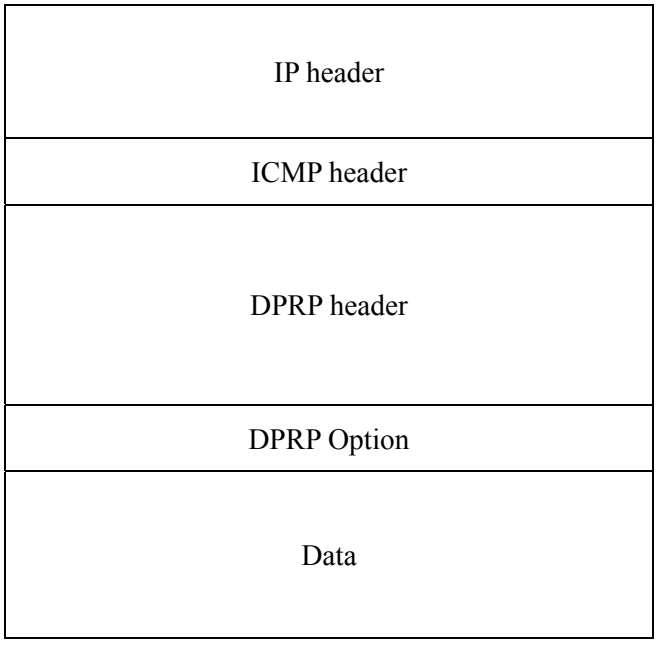


図 C-30　DPRP プロトコルフォーマット

表 C-4　ICMP ヘッダのタイプ

DPRP 制御パケット種別	ICMP タイプ
DDE	ICMP ECHO（値：8）
RGI	
MPIT	
CDN	ICMP ECHOREPLY（値：0）

DPRP 制御パケットは CK により暗号化される．暗号化範囲は各 DPRP 制御パケットヘッダより下位領域（DPRP オプションおよびデータ領域）である．暗号モジュールは PCCOM のサブモジュールを利用する. 暗号モジュールを利用する際に必要な IV は，図 C-31 に示す DPRP ヘッダのうち，Flag，Count および Option フィールドを 0 に設定した DPRP ヘッダから生成する.

(2) DPRP ヘッダ

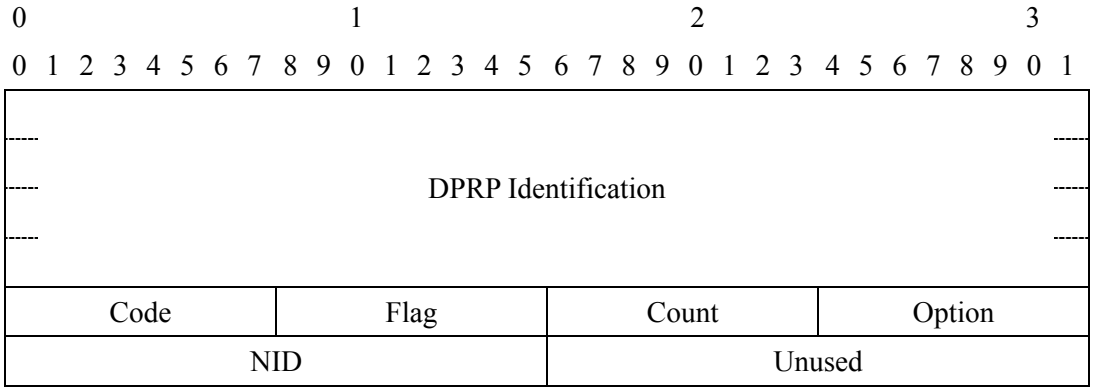


図 C-31　DPRP ヘッダフォーマット

表 C-5　DPRP ヘッダフィールド

フィールド名	サイズ	値
DPRP Identification	16	DPRP 制御パケットを識別する固定値 C734E6923B433BBFA54B2D91D44E059E
Code	1	DPRP 制御パケットの種類 1：DDE　2：RGI　3：MPIT　4：CDN 5：エラー通知
Flag	1	0（未定）
Count	1	通信経路上の GE 数
Option	1	オプション有無と種類 0：オプション無し 1：拡張 DPRP　2：Mobile PPC　3：NATF
NID	2	ネゴシエーション識別子
Unused	2	0（未使用）

✧　ヘッダ長：固定　24 オクテット

(3) DPRP オプションヘッダ，オプション領域

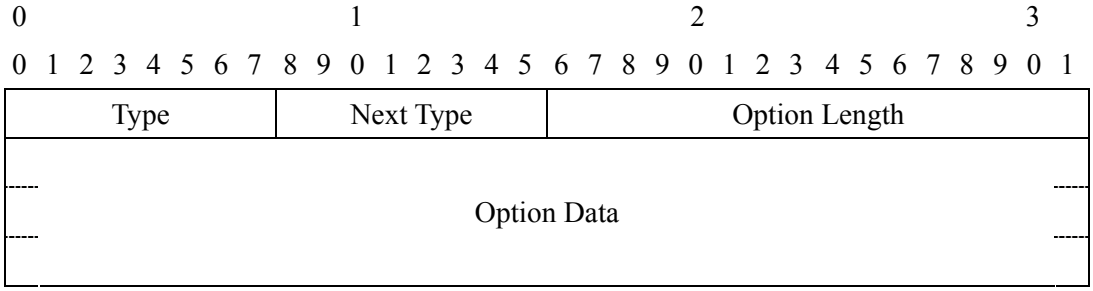


図 C-32　DPRP オプションフォーマット

表 C-6　DPRP オプションヘッダフィールド

フィールド名	サイズ	値
Type	1	オプションの種類 1：拡張 DPRP　2：Mobile PPC　3：NATF
Next Type	1	次のオプションの種類 0：オプション無し　2：Mobile PPC　3：NATF
Option Length	2	Option Data の長さ

- ✧ ヘッダ長：固定　4 オクテット
- ✧ オプションデータ長：可変長

DPRP オプションは IPv6 のように数珠繋ぎでヘッダを配置される．

(4) DDE

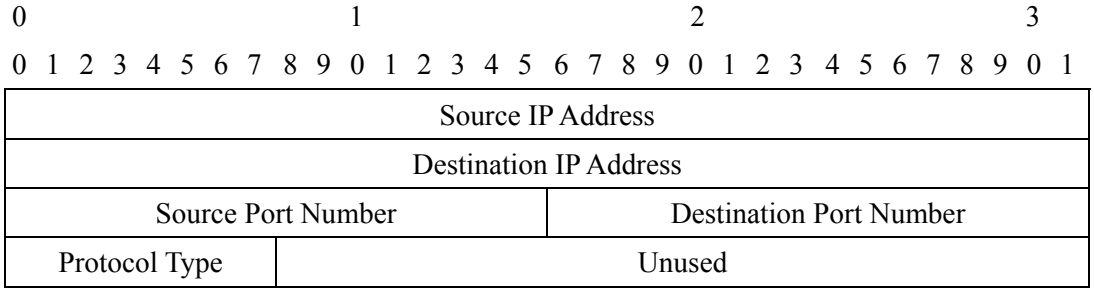


図 C-33　DDE データフォーマット

表 C-7　DDE データフィールド

フィールド名	サイズ	値
Source IP address	4	送信元 IP アドレス
Destination IP Address	4	宛先 IP アドレス
Source Port Number	2	送信元ポート番号
Destination Port Number	2	宛先ポート番号
Protocol Type	1	プロトコルタイプ
Unused	3	0（未使用）

- ✧　データ長：固定　16 オクテット
- ✧　CID：Source IP Address から Protocol Type まで

(5) RGI

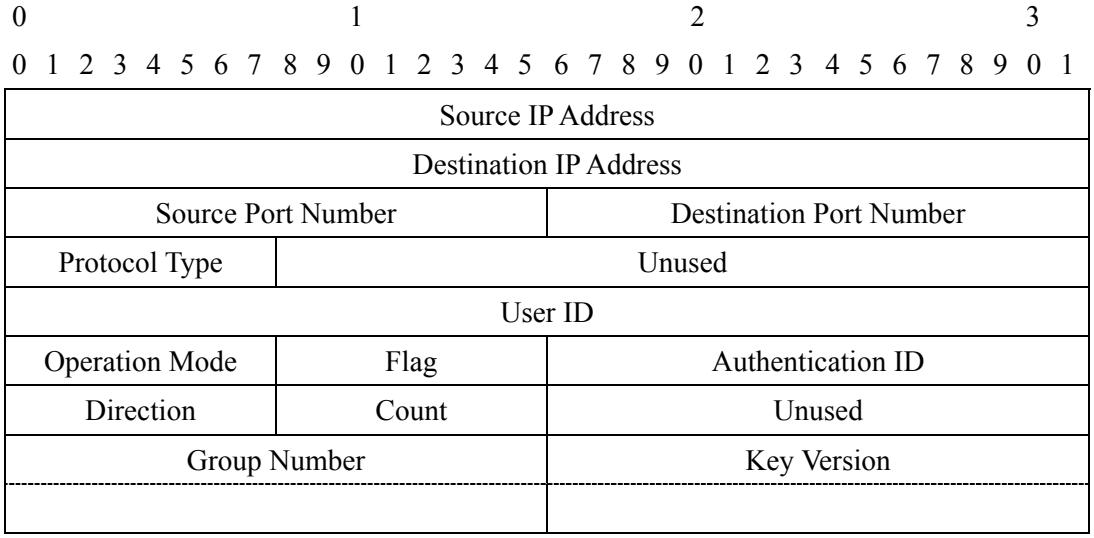


図 C-34　RGI データフォーマット

表 C-8　RGI データフィールド

フィールド名	サイズ	値
Source IP address	4	送信元 IP アドレス
Destination IP Address	4	宛先 IP アドレス
Source Port Number	2	送信元ポート番号
Destination Port Number	2	宛先ポート番号
Protocol Type	1	プロトコルタイプ
Unused	3	0（未使用）
User ID	4	ユーザ ID
Operation Mode	1	動作モード 1：OP（開放モード）　2：CL（閉域モード）
Flag	1	0（未定）
Authentication ID	2	認証識別子 aID
Direction	1	ネゴシエーションの方向情報 1：edge　2：outbound　3：inbound
Count	1	以降に続くグループ鍵情報の数
Unused	2	0（未使用）
Group Number	2	通信グループ番号
Key Version	2	バージョン番号

✧ データ長：可変

16＋（GE が追加するデータ長×通信経路上の GE 数）オクテット

✧ GE が追加するデータ：User ID から Key Version まで

✧ GE が追加するデータ長：可変長　12＋（4×Count）オクテット

✧ CID：Source IP Address から Protocol Type まで

✧ グループ鍵情報：Group Number から Key Version まで

中間 GE が情報を追加すると以下のような構造になる.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Source IP Address		
Destination IP Address		
Source Port Number		Destination Port Number
Protocol Type	Unused	
User ID		
Operation Mode	Flag	Authentication ID
Direction	Count＝2	Unused
Group Number		Key Version
Group Number		Key Version
User ID		
Operation Mode	Flag	Authentication ID
Direction	Count＝1	Unused
Group Number		Key Version

図 C-35　中間 GE における情報追加後の RGI データフォーマット

(6) MPIT

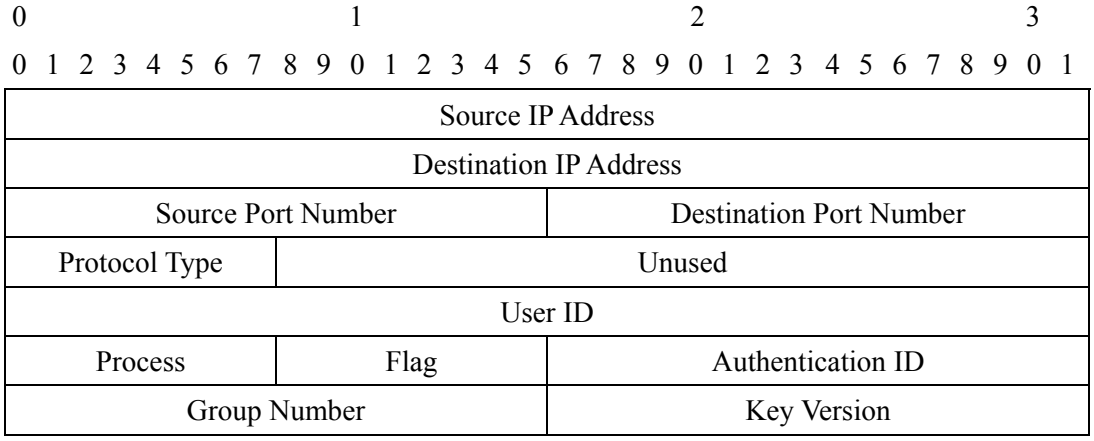


図 C-36　MPIT データフォーマット

表 C-9　MPIT データフィールド

フィールド名	サイズ	値
Source IP address	4	送信元 IP アドレス
Destination IP Address	4	宛先 IP アドレス
Source Port Number	2	送信元ポート番号
Destination Port Number	2	宛先ポート番号
Protocol Type	1	プロトコルタイプ
Unused	3	0（未使用）
User ID	4	ユーザ ID
Process	1	処理内容 1：Encrypt　2：Decrypt　3：Transparent 4：Discard
Flag	1	0（未定）
Authentication ID	2	認証識別子 aID
Group Number	2	通信グループ番号
Key Version	2	バージョン番号

- ✧ データ長：可変　16＋12×（通信経路上の GE 数－1）オクテット
- ✧ GE が登録するデータ：User ID から Key Version まで
- ✧ GE が登録するデータ長：12 オクテット
- ✧ CID：Source IP Address から Protocol Type まで
- ✧ グループ鍵情報：Group Number から Key Version まで

(7) CDN

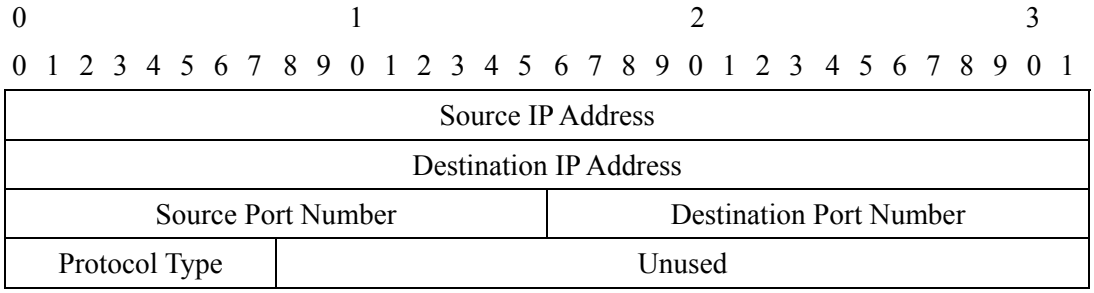


図 C-37　CDN データフォーマット

表 C-10　CDN データフィールド

フィールド名	サイズ	値
Source IP address	4	送信元 IP アドレス
Destination IP Address	4	宛先 IP アドレス
Source Port Number	2	送信元ポート番号
Destination Port Number	2	宛先ポート番号
Protocol Type	1	プロトコルタイプ
Unused	3	0（未使用）

- ✧　データ長：固定　16 オクテット
- ✧　CID：Source IP Address から Protocol Type まで