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

043432022　鈴木 秀和
渡邊研究室

1　はじめに

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，IPsec[1] のような従来の通信グループ構築方法では，部門単位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．そこで本研究で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）と呼ぶシステムの構築を最終目標とし，FPN を実現するため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）[2] 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．

本論文では DPRP を FreeBSD に実装し，性能評価実験を行ったので，その結果について述べる．

2　FPN とその実現方法

2.1　FPN とは

FPN（Flexible Private Network）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，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．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．FPN はこのようなネットワーク環境を前提とし，端末の移動によりネットワーク構成が変化しても，システムが自動的にその変化を学習する．これによりユーザや管理者が暗号化通信に必要な設定情報を更新する必要はない．この機能を位置透過性という．

2.2　セキュア通信アーキテクチャGSCIP

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，DPRP は GSCIP の一部を構成するプロトコルである．図 1 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 と呼び，ホストタイプの GES，ルータタイプの GEN などがある．GEN はサブネットを構成し，配下の一般端末 Term を保護する．GSCIP では同一の共通鍵を所持する GE の集合を同一の通信グループとして定義する．この共通鍵をグループ鍵 GK と呼ぶ．通信グループと GK を 1 対 1 に対応づけることで，IP アドレスに依存することなく論理的に通信グループを定義することができる．

GE に必要な情報は管理装置 MS で生成され，GE 起動時に確実な認証のもとに配送される．グループ鍵 GK は定期的に，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する．

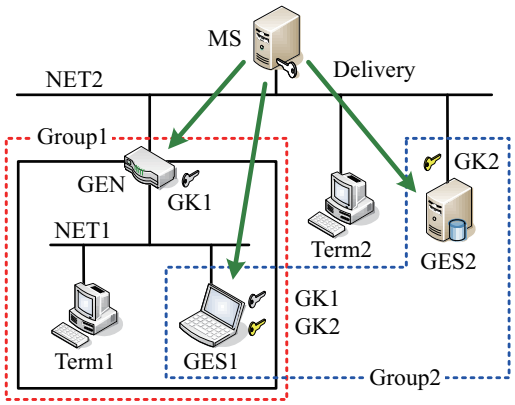


図 1: 通信グループの定義方法

3　動的処理解決プロトコル DPRP

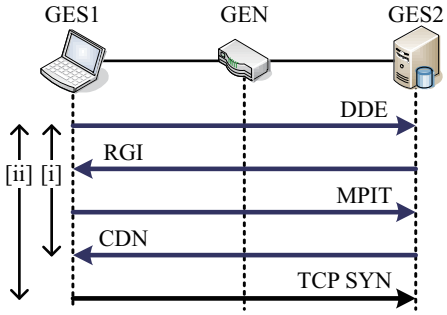
3.1　動作概要

DPRP は端末間の通信に先立って図 2 に示す 2 往復のネゴシエーションを行う．1 往復目で通信経路上の GE に予め設定されている情報を取得して，通信の処理に必要な動作処理情報を動的に決定する．2 往復目で決定した情報を通信経路上の GE に通知し，各 GE は受信した情報の認証処理を行い，動作処理情報テーブル PIT に保存する．

以後の通信はこの PIT の動作処理情報を元に，パケットの暗号化／復号，透過中継や破棄などを行う．DPRP は全 GE が共有しているシステム共通鍵 CK により暗号化され，安全に情報交換が行われる．

3.2　実装方式

図 3 に GSCIP の実装概要を示す．DPRP は GSCIP を実現するモジュール GPACK の一部を構成し，UNIX 系 OS である FreeBSD の IP 層に実装される．GPACK は IP 層の入出力関数 `ip_input()`，`ip_output()` から呼び出され，DPRP 対応の処理や PIT 検索などを行い，パケットを



[i] : The time needed for DPRP negotiation
[ii] : The time to the start of ordinary communication

図 2: DPRP シーケンスと測定ポイント

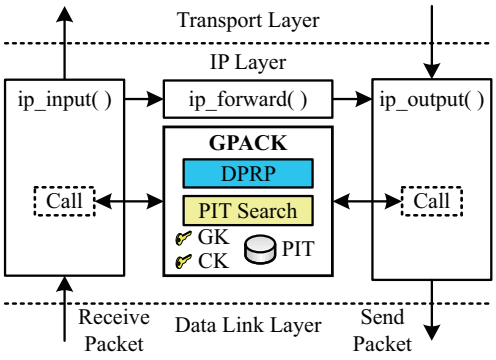


図 3: GSCIP の実装概要

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 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．PIT はハッシュテーブルとして実装する．一定時間参照されていない PIT レコードは，その端末間の通信が行われていないと判断されてカーネルタイマ処理により削除される．DPRP の暗号化には FreeBSD に実装されている OpenSSL ライブラリを使用し，暗号アルゴリズムは AES（Advanced Encryption Standard）を採用した．

4 評価

4.1 DPRP の性能評価

100BASE-TX の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．各装置のスペックは Pentium4 3GHz，メモリ 512MB である．測定対象は図 2 に示す [i] ネゴシエーション時間と，[ii] 実際の通信が開始されるまでの時間である．表 1 にオーバヘッドの測定結果を示す．DPRP のネゴシエーション時間は 1133 μ 秒，通信開始までの時間は 1169 μ 秒となった．参考のために，同一条件下における IPsec/IKE（Internet Key Exchange）の処理時間も測定した．認証方式は事前共有鍵とした．結果，IKE のネゴシエーション時間は 1.068 秒，通信開始までの時間は 2.994 秒となった．

表 1: ネゴシエーションのオーバヘッド

	DPRP	IKE
[i] ネゴシエーション時間	1,133	1,068,455
[ii] 通信開始までの時間	1,169	2,994,961

単位:[μ sec]

DPRP は通信開始に先立ち 1 回だけ実行される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．DPRP では認証と通信パケットの暗号化は共通鍵 GK を用いるため，処理時間が短くてすむ．一方，IKE は Diffie-Hellman 鍵交換による共通鍵生成を行うため処理が遅い．

更に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．DPRP はシンプルな構造であることから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 の再送処理が発生せず，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 は構造が複雑であるため，ネゴシエーション実行時に一般通信の第 1 パケットを破棄する．つまり，最初のパケットは TCP の再送処理に頼ることにより通信を実現しているため，通信開始までの時間が大きい．

表 2: 初期管理負荷の違い

	GSCIP/DPRP	IPsec/IKE
GES1	8	30
GEN	5	18
GES2	5	36

表 3: ネットワーク構成変化時の管理負荷の違い

	GSCIP/DPRP	IPsec/IKE
GES1	0	33
GEN	0	29
GES2	0	6

4.2 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．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．本論文では 1 つの項目を設定するのに必要な作業コストを 1 として算出する．

表 2 に各装置に必要な初期管理負荷を示す．初期管理負荷とは図 1 で表される通信環境を GSCIP および IPsec で実現するために，必要な作業コストである．GSCIP は DPRP により必要な情報を通信開始時に動的に生成ため，初期設定の管理負荷が非常に小さい．一方，IPsec では通信の処理内容を規定するセキュリティポリシーや IKE の動作を静的に設定しなければならず，大きな管理負荷が必要となる．

次にネットワーク構成が変化した場合に必要となる管理負荷の違いを示す．図 1 において GES1 が NET1 から NET2 へ移動した場合に発生する管理負荷を表 3 に示す．GSCIP ではネットワーク構成が変化しても，その都度 DPRP により動作処理情報テーブル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，移動した端末はもとより，移動していない装置にも多大な管理負荷が発生する．これはセキュリティポリシーや IKE の静的な設定に IP アドレス，即ち位置情報が含まれていることに起因している．

GSCIP は初期導入時の管理負荷を軽減でき，かつ端末の移動に伴う管理負荷が発生しないことから，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．

5 むすび

本論文では DPRP を FreeBSD に実装して検証を行った．結果，高速かつ安全に通信相手を認証することが可能で，PIT 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化時に発生する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，DPRP の拡張や IPv6 への適用などを行う予定である．

参考文献

[1] S. Kent and K. Seo, “Security Architecture for the Internet Protocol," Internet Draft, IETF, Mar. 2005.

[2] 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実現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，Vol.J84-D-I, No.3，pp. 269-284，Mar. 2001.

平成17年度名城大学大学院理工学研究科情報科学専攻
修士論文公聴会

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

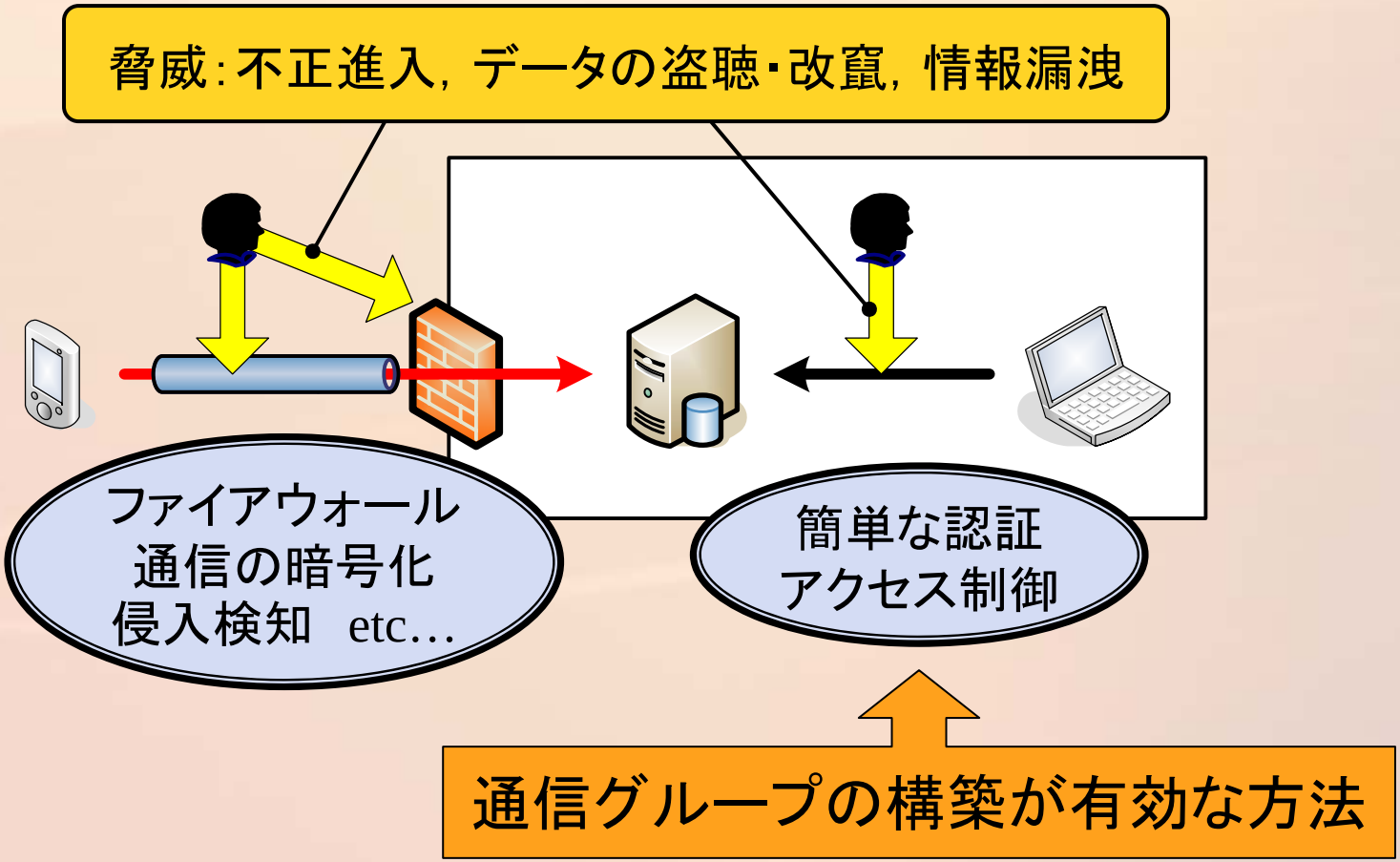
Implementation and its evaluation of
Dynamic Process Resolution Protocol in Flexible Private Network

渡邊研究室

043432022　鈴木秀和

はじめに

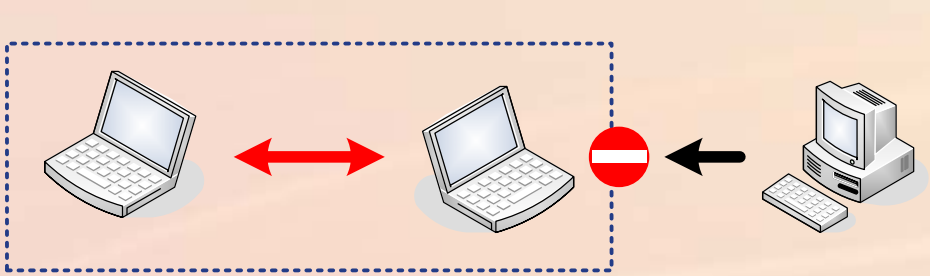
- 企業ネットワークにおけるセキュリティ対策の重要性



通信グループ

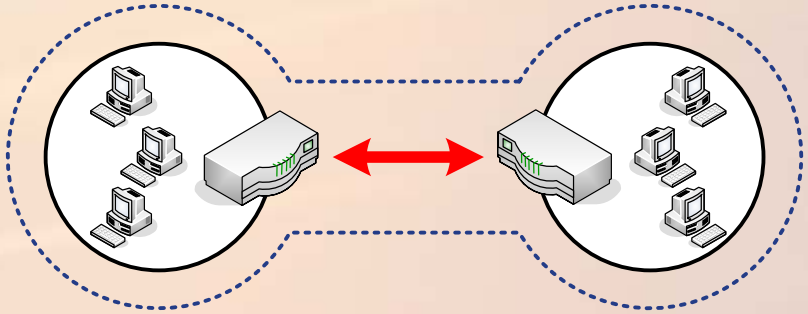
- 特定の属性に基づいたユーザの集合体
- 同一グループ内のメンバ間通信は暗号化
- 既存のネットワークインフラをそのまま利用可能

個人単位に実現する方式



- 柔軟なグルーピングが可能
- 規模が大きくなると管理負荷も増大

ドメイン単位に実現する方式



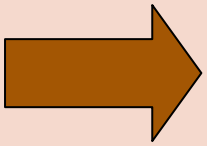
- ゲートウェイにセキュリティ機能を実装し，配下を一括管理
- きめ細かいグルーピングが困難

柔軟な通信グループを定義するために

- イントラネットにおける要求
  - 役職単位や部門単位など複数の通信グループを定義したい
  - 部門をまたがって通信グループを定義したい

個人単位・ドメイン単位が混在した方式が望ましい

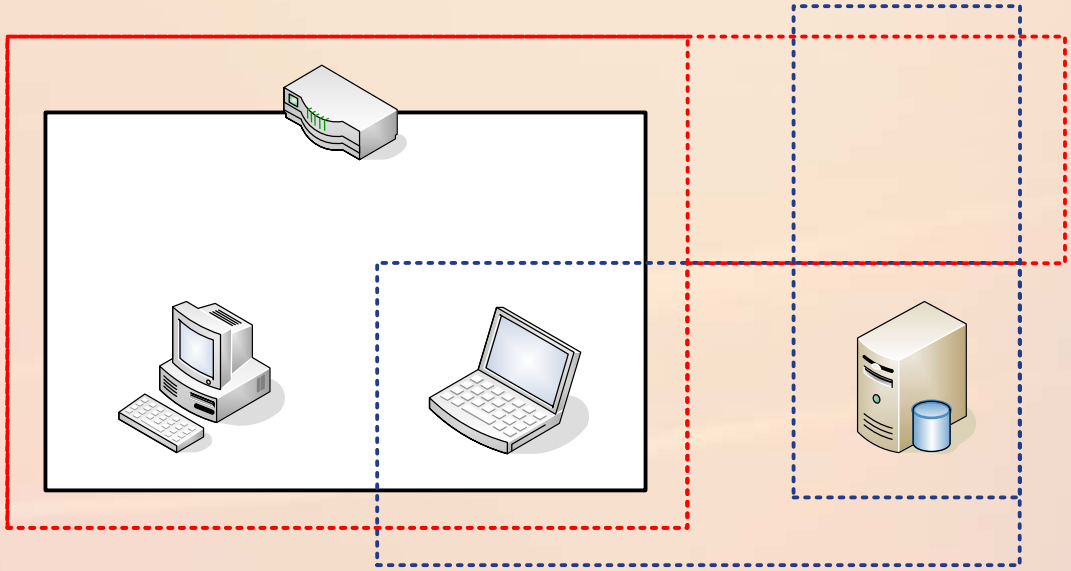
- IPsec（既存のネットワークセキュリティ技術）
  - トランスポートモード ← 個人単位
  - トンネルモード ← ドメイン単位
  - 両モードの互換性なし➔混在方式の実現は難しい



フレキシブルプライベートネットワーク
FPN (Flexible Private Network)

Flexible Private Network

- 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
  - 個人単位とドメイン単位の通信グループの混在定義に対応
  - 端末の移動によるネットワーク構成の変化に対応

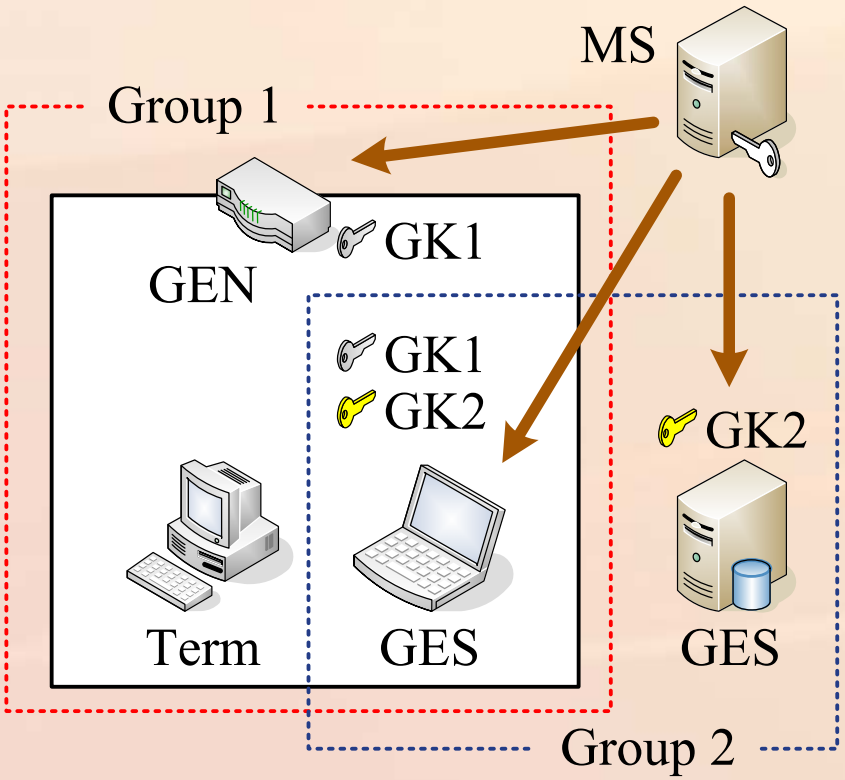


  - システムが自動的に位置の変化を学習
  - ユーザや管理者が設定を変更する必要はない

位置透過性

GSCIP（Grouping for Secure Communication for IP）

FPNを実現するための通信アーキテクチャ



- 構成要素
  - GE：GSCIP構成装置
    - GES（ホスト型）
    - GEN（ルータ型）
  - MS：管理装置
- MSからGEへ定義情報を配送
  - グループ情報，共通鍵GK
  - MS-GE間は公開鍵認証
- 通信グループの定義
  - 同一のGKを持つGEの集合
  - 通信グループとGKが1対1の関係

IPアドレスに依存せず，論理的に通信グループの定義が可能

GSCIPの通信体系

- パケット送受信時に動作処理情報テーブルPIT（Process Information Table）を参照

- 該当情報あり
  ➔処理内容に基づいて処理
- 該当情報なし
  ➔動作処理情報を生成

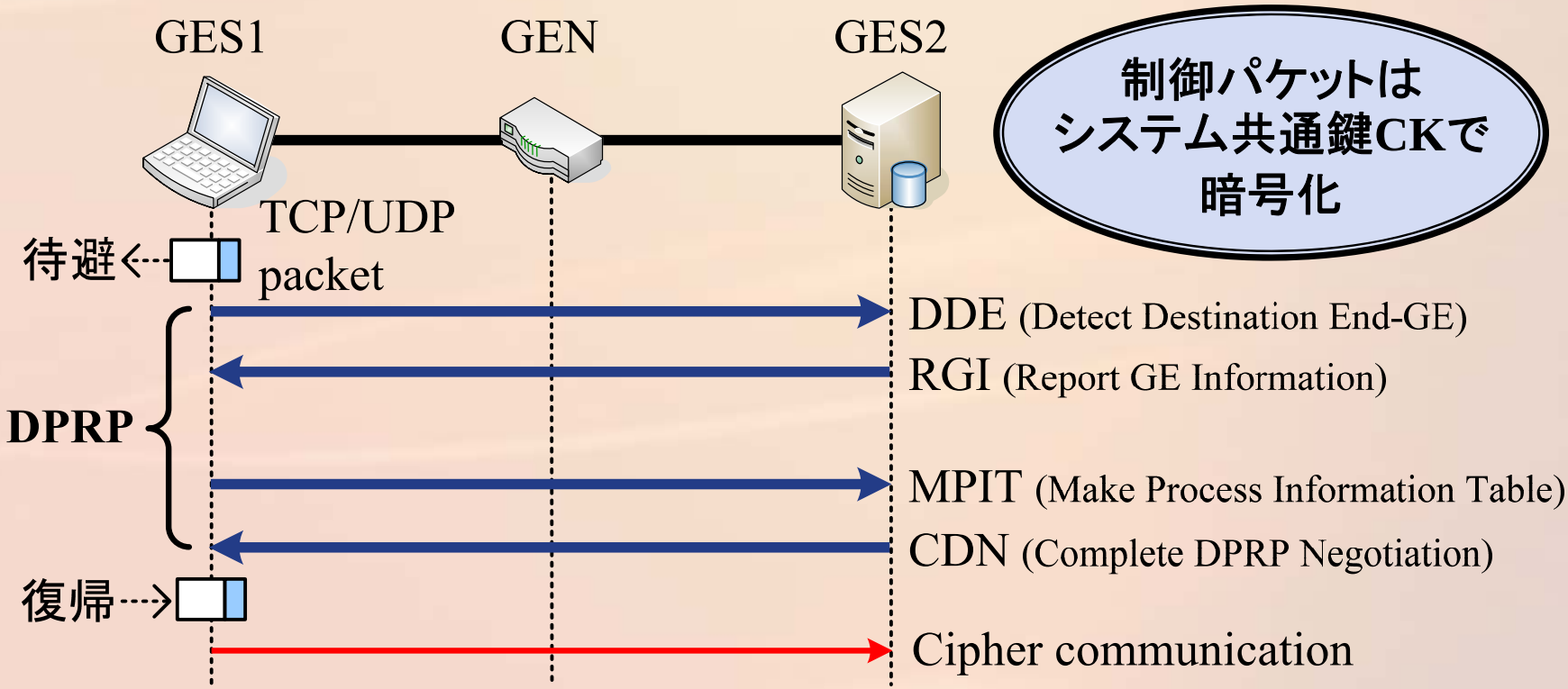
PIT on GES2

Destination	Process	Group No.
GES1	Discard	—
GES3	Encrypt	2

動的処理解決プロトコルDPRP

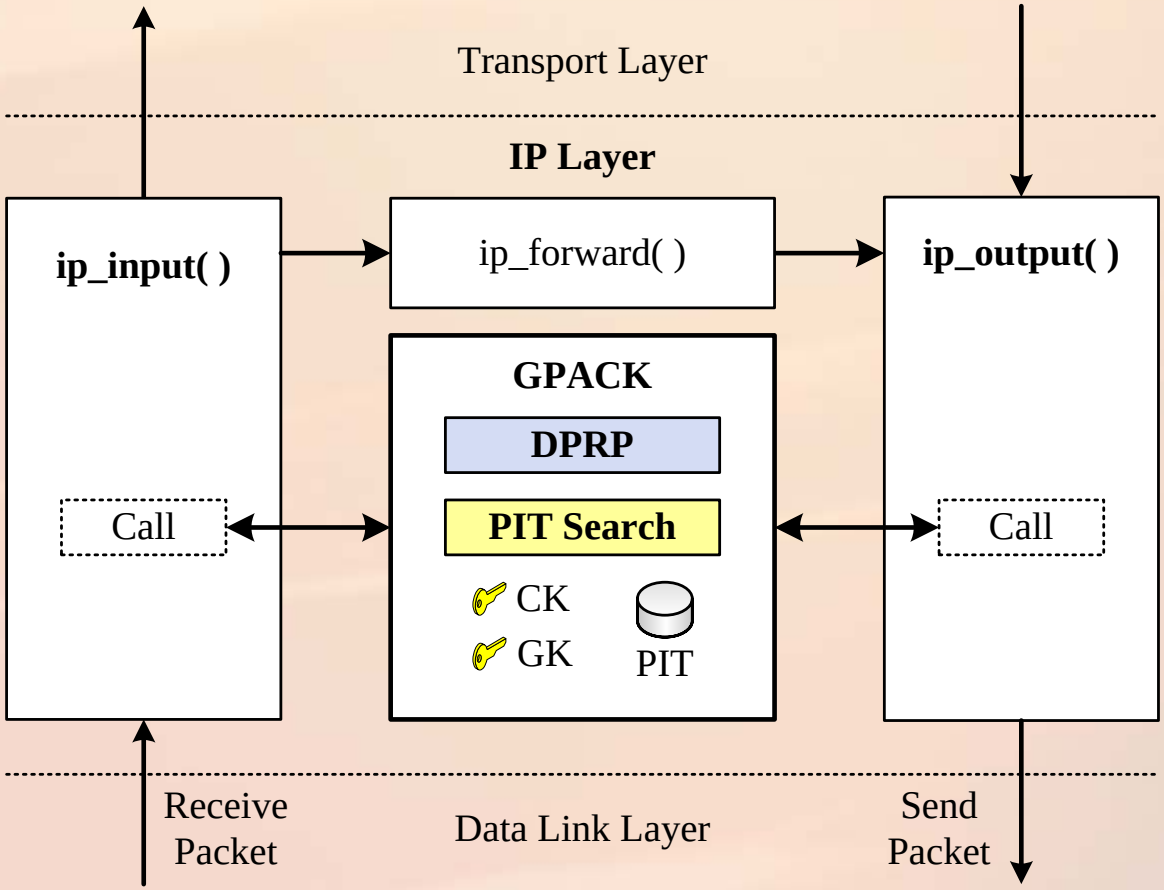
DPRP（Dynamic Process Resolution Protocol）

- 通信経路上の終端GE間で2往復のネゴシエーション
  - 1往復目：経路上のグループ情報を収集➔動作処理情報を決定
  - 2往復目：動作処理情報を通知➔認証後，PITを生成



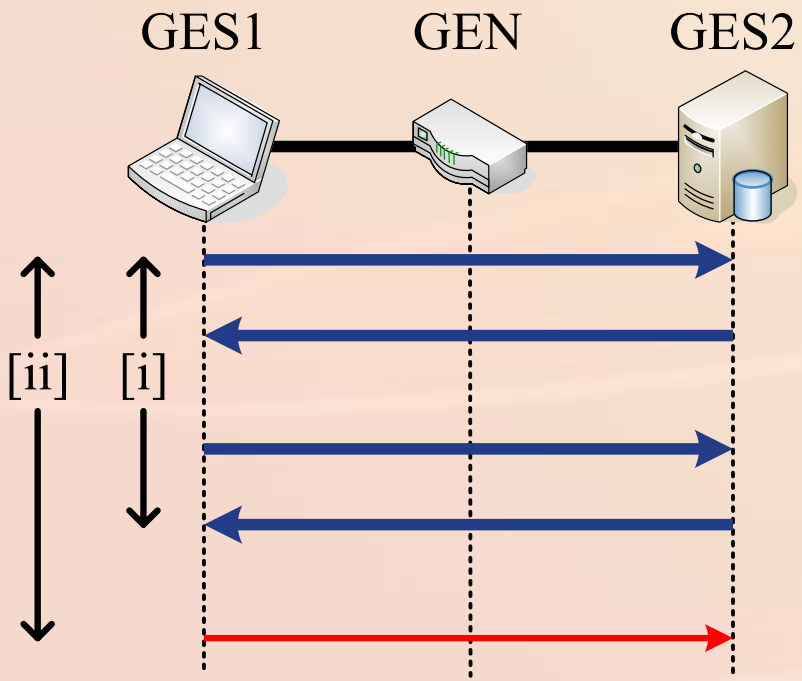
実装方式

- FreeBSDのIP層にモジュールGPACKを実装
  - PIT，MSから配送された定義情報，鍵はカーネルメモリ空間へ保存



DPRPの性能評価

- 100BASE-TX環境下においてGES1がGES2にFTP接続
  - DPRPネゴシエーションのオーバヘッドを測定
    i. ネゴシエーション時間
    ii. 最初の通信が開始されるまでの時間



スペック
» CPU: Pentium4 3.0[GHz]
» RAM: 512[MB]
» OS: FreeBSD 5.3-Release

参考
» IKEを同一条件下で測定
・認証方式：事前共有鍵

測定結果

単位:ミリ秒	DPRP	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

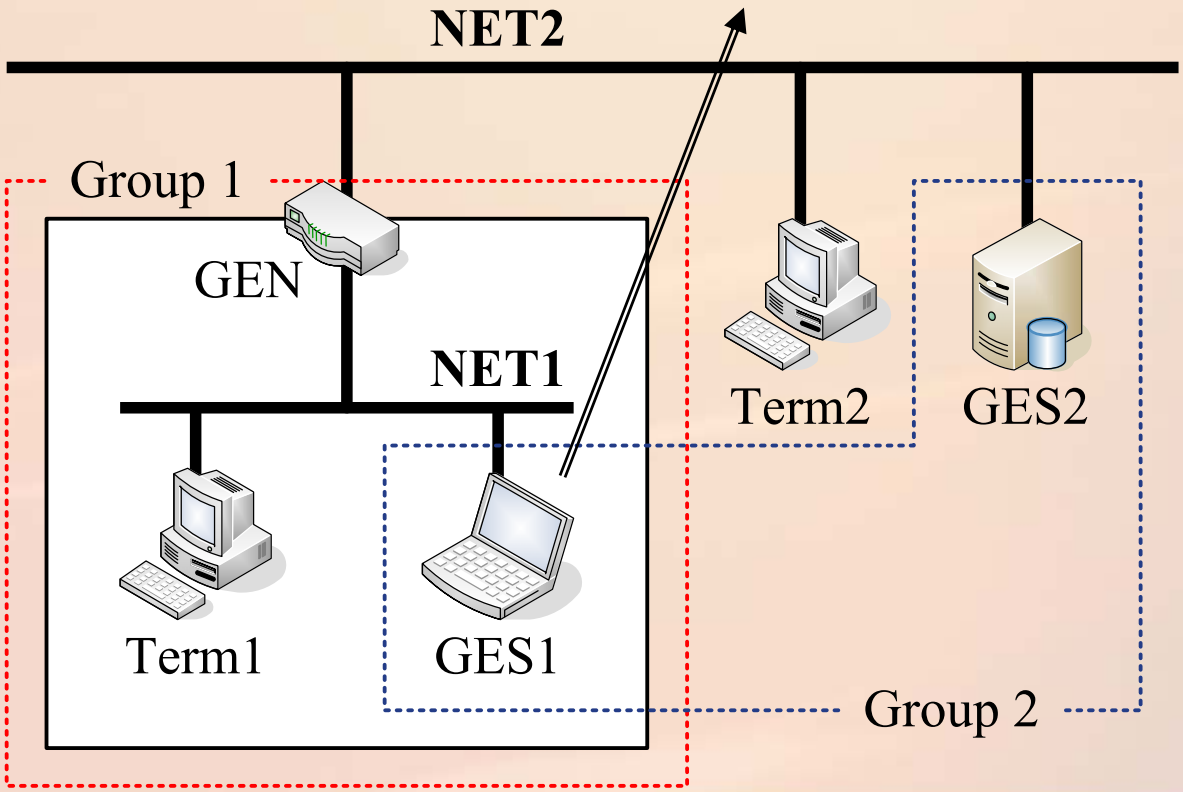
- ネゴシエーション時間 （DPRP:約1ミリ秒　IKE:約1秒）
  - DPRPは暗号化に使用する共通鍵GKをMSから取得済み
  - IKEはDiffie-Hellman鍵交換により共通鍵を生成

- 通信開始までの時間 （DPRP:約1ミリ秒　IKE:約3秒）
  - DPRPはパケットの待避・復帰処理が可能 ➔ TCP再送処理なし
  - IKEはトリガーパケットを破棄してからネゴシエーションを実行
    ➔ TCP再送処理に頼ることで通信を開始

DPRPは一般の通信にほとんど影響を与えない

GSCIPとIPsecの管理負荷評価

- 導入時に発生する初期管理負荷
- ネットワーク構成変化時に発生する管理負荷
  - GES1がNET1からNET2へ移動した場合



初期管理負荷

コスト	GSCIP/DPRP	IPsec/IKE
GES1	8	30
GEN	5	18
GES2	5	36

- GSCIP/DPRP
  - グループ鍵，定義情報　←MSからの配送情報
- IPsec/IKE
  - 共有鍵（認証用），セキュリティポリシー，IKE　←すべて静的設定

※1つの項目を設定するのに必要な作業コストを1として算出

ネットワーク構成変化時に発生する管理負荷

コスト	GSCIP/DPRP	IPsec/IKE
GES1	0	33
GEN	0	29
GES2	0	6

- GSCIP/DPRP
  - 通信開始時にその都度，DPRPによりPITが動的に再生成
- IPsec/IKE
  - 移動していない装置にも多大な管理負荷が発生
    ➔セキュリティポリシーやIKEの設定項目にIPアドレスを含むため

GSCIP/DPRPは導入時，構成変化時の管理負荷を大幅に軽減

まとめ

- 動的処理解決プロトコルDPRPの実装と評価
  - 高速かつ安全に
    - 通信相手を認証することが可能
    - 動作処理情報テーブルPITを動的に生成することが可能
  - 一般の通信に与える影響がほとんどない
  - ネットワーク構成変化時に発生する管理負荷を大幅に軽減

- 今後の課題
  - DPRPの拡張
    - 端末の移動先が異なるアドレス空間の場合
      ➔FPNの適用ドメインをホームネットワークからインターネットへ
  - IPv6への適用を検討

平成17年度名城大学大学院理工学研究科情報科学専攻
修士論文公聴会

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

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

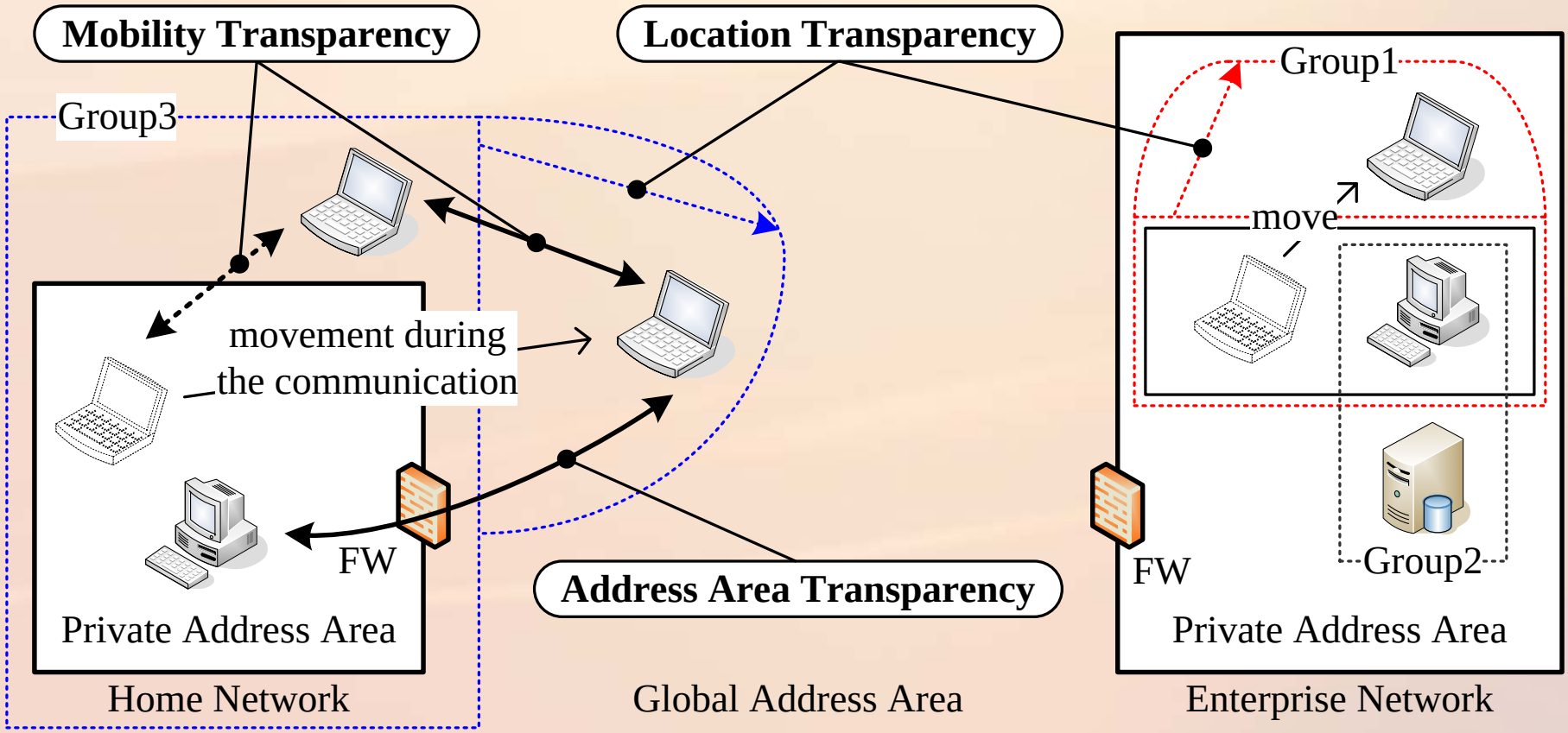
渡邊研究室

043432022　鈴木秀和

FPNで実現する3つの透過性と対応プロトコル

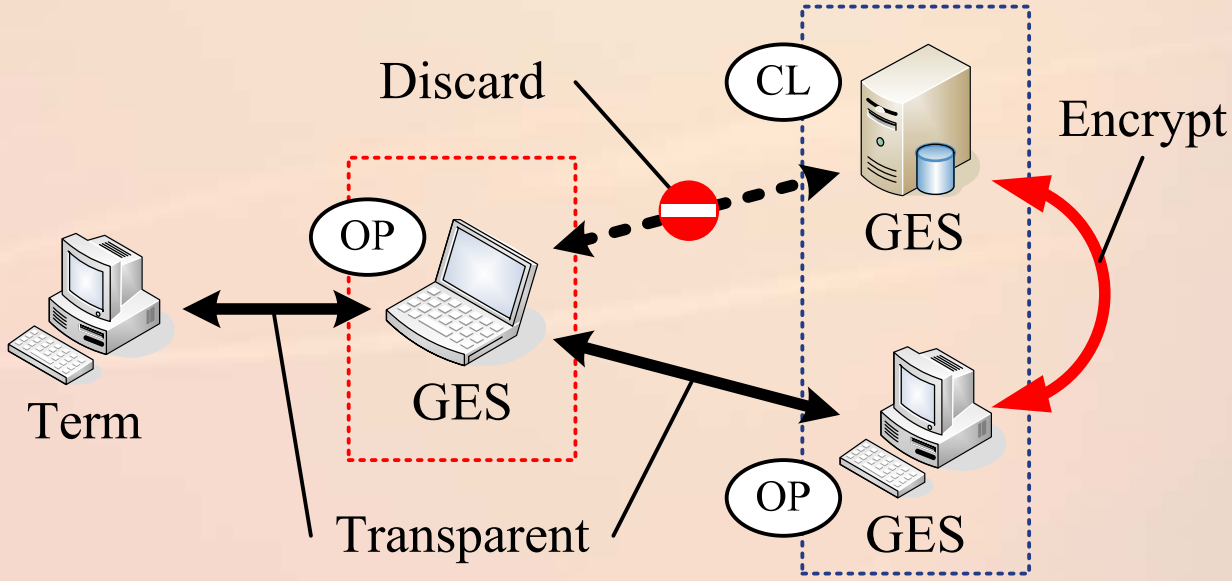
- 位置透過性（Location Transparency）
  - 端末が移動してもシステムが自動的にネットワーク構成の変化を学習➔DPRP
- 移動透過性（Mobility Transparency）
  - 通信中に移動しても通信を継続➔Mobile PPC
- アドレス空間透過性（Address Area Transparency）
  - NATの外部から内部へアクセス開始を実現➔NATF

FPNのイメージ図

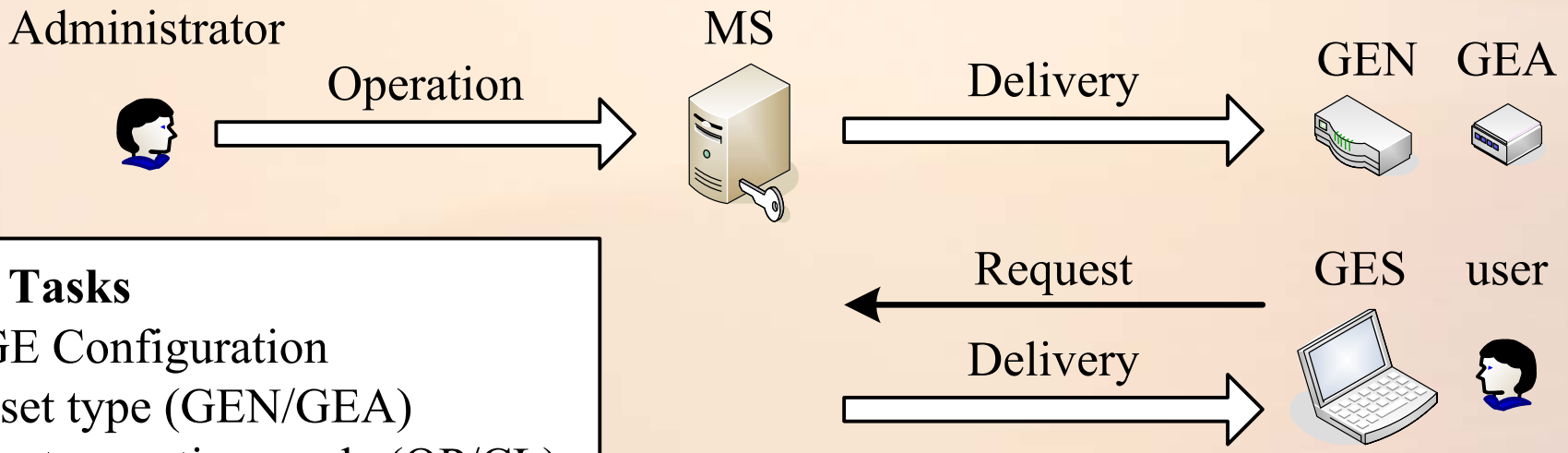

Mobility Transparency
Location Transparency
Group3
movement during
the communication
FW
Private Address Area
Home Network
Address Area Transparency
Global Address Area
Group1
move
Group2
FW
Private Address Area
Enterprise Network

動作モードOM（Operation Mode）

- 閉域モードCL（Closed Mode）
  - 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
- 開放モードOP（Open Mode）
  - 異なる通信グループの端末とは平文での通信が可能



管理装置MS（Management Server）



MS Tasks

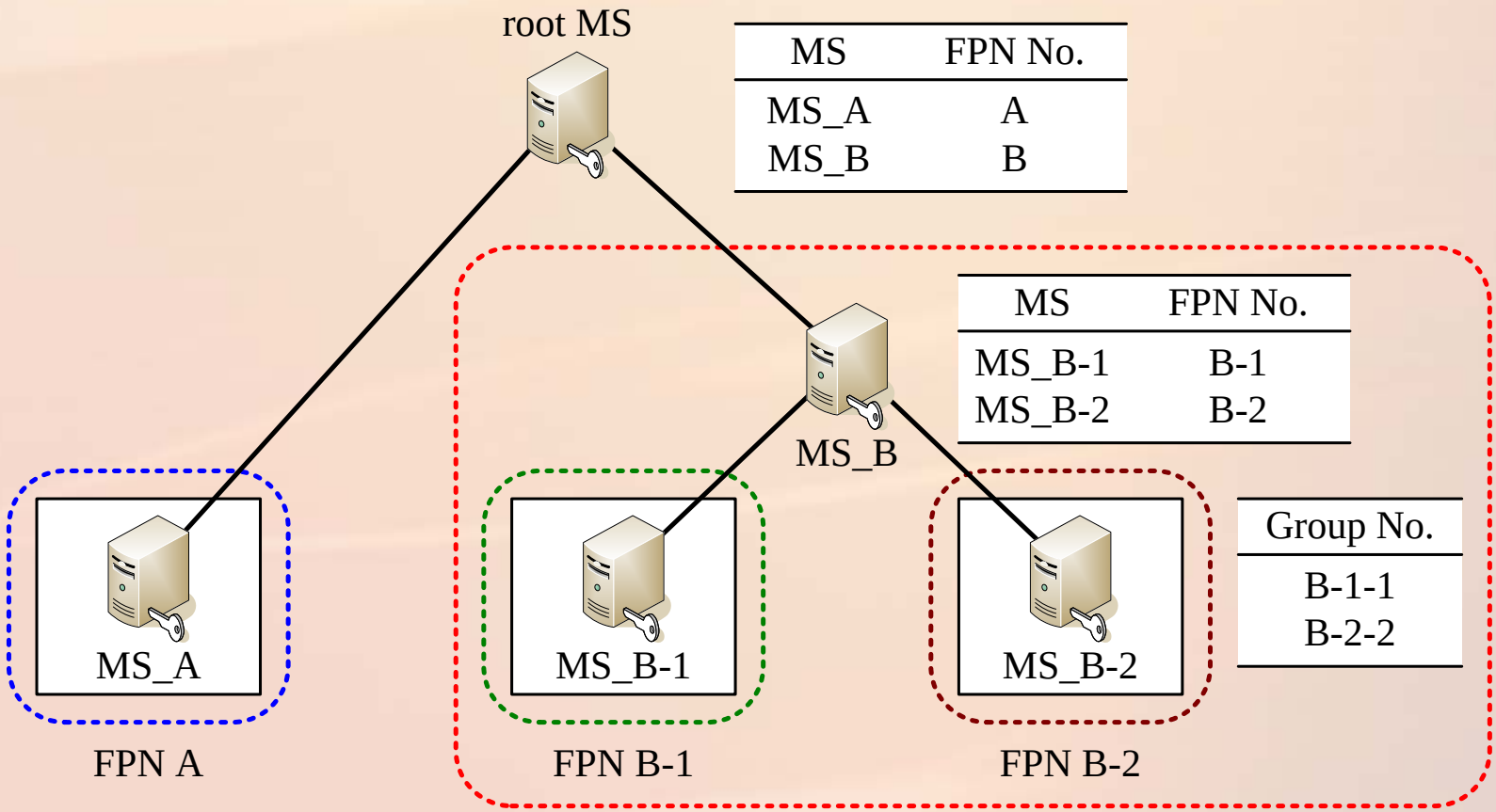
- ❖ GE Configuration
  - set type (GEN/GEA)
  - set operation mode (OP/CL)
  - set groups that belongs
- ❖ User Configuration
  - add/delete user
  - set operation mode (OP/CL)
  - set groups that belongs
- ❖ Group Configuration
  - add/delete group
- ❖ Key Generation / Update

Delivery Information

- ❖ GE Information
  - Group No.
  - Operation Mode
- ❖ Group Key, Common Key
- ❖ Group Key Information
  - Group No.
  - Version

MSの管理範囲

- 1つの管理ドメインに対して1台設置
- 複数台設置する場合はDNSのようにツリー構造で管理



MS	FPN No.
MS_A	A
MS_B	B

MS	FPN No.
MS_B-1	B-1
MS_B-2	B-2

Group No.
B-1-1
B-2-2

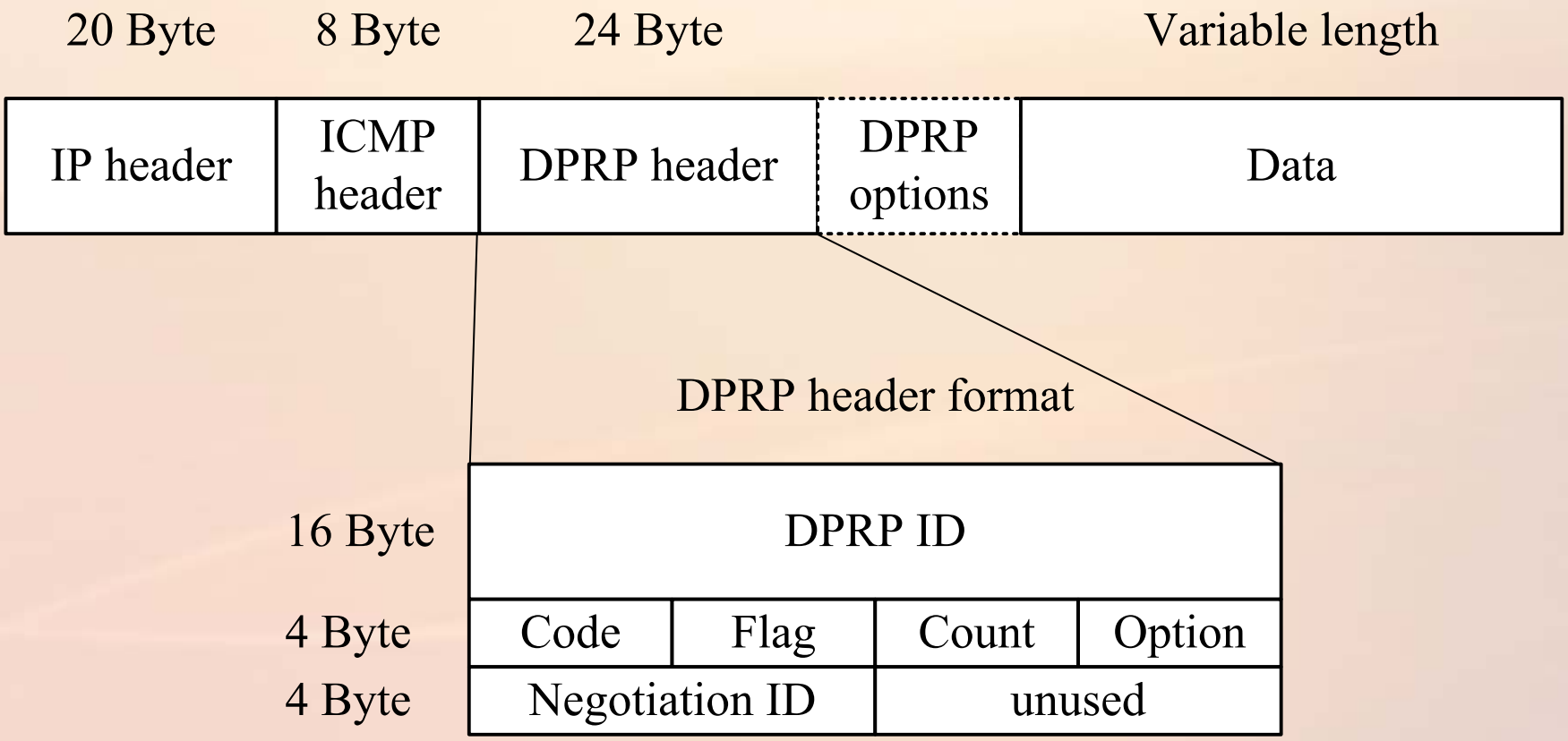
動作処理情報テーブルPIT

- Connection ID
  - 送信元/宛先IPアドレス，ポート番号，プロトコルタイプ
- 動作処理情報
  - 処理内容，通信グループ番号，バージョン番号

PIT

saddr	daddr	spor	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

DPRP制御パケットフォーマット



DDE(Detect Destination End GE)

- 終点GEを決定

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

- $NODE_{daddr}$がGEの場合
  - » $NODE_{daddr}$が終点GEに決定
- $NODE_{daddr}$が一般端末の場合
  - » 一般端末が返答するICMP ECHO REPLYを最初に受信したGEが終点GEに決定

RGI（Report GE Information）

- 始点GEを決定
- 通信経路上の全GEの定義情報を収集

$$GE_{DST} \rightarrow NODE_{saddr}: \quad RGI = HDR, CK(CID, N_1)$$

$$N_1 = UID_1, OM_1, aID_1, DIRECT_1, CNT_1, GKI_1$$

$$GKI_1 = \{(GNO_c, VER_c) \mid c = 1, \cdots, CNT_1\}$$

$$RGI = HDR, CK(CID, N_1, \cdots, N_i)$$

- $NODE_{saddr}$がGEの場合
  - $NODE_{saddr}$が始点GEに決定
- $NODE_{saddr}$が一般端末の場合
  - 一般端末が返答するICMP ECHO REPLYを最初に受信したGEが始点GEに決定

MPIT（Make Process Information Table）

- 決定した動作処理情報を通知

$$GE_{SRC} \rightarrow GE_{DST}: \quad MPIT = HDR, CK(CID, D_{n-1}, \cdots D_1)$$

$$D_i = \begin{cases} UID_i, GK_D(aID_i), P_i & if \quad PROC_i = Decrypt \\ UID_i, aID_i, P_i & if \quad PROC_i \neq Decrypt \end{cases}$$

$$P_i = (PROC_i, GKI_D) \quad (1 \leq i < n)$$

- PITに記憶していたaIDと受信したaIDを比較して認証
  - 認証成功➔動作処理情報をPITに登録
  - 認証失敗➔MPITを破棄

CDN（Complete DPRP Negotiation）

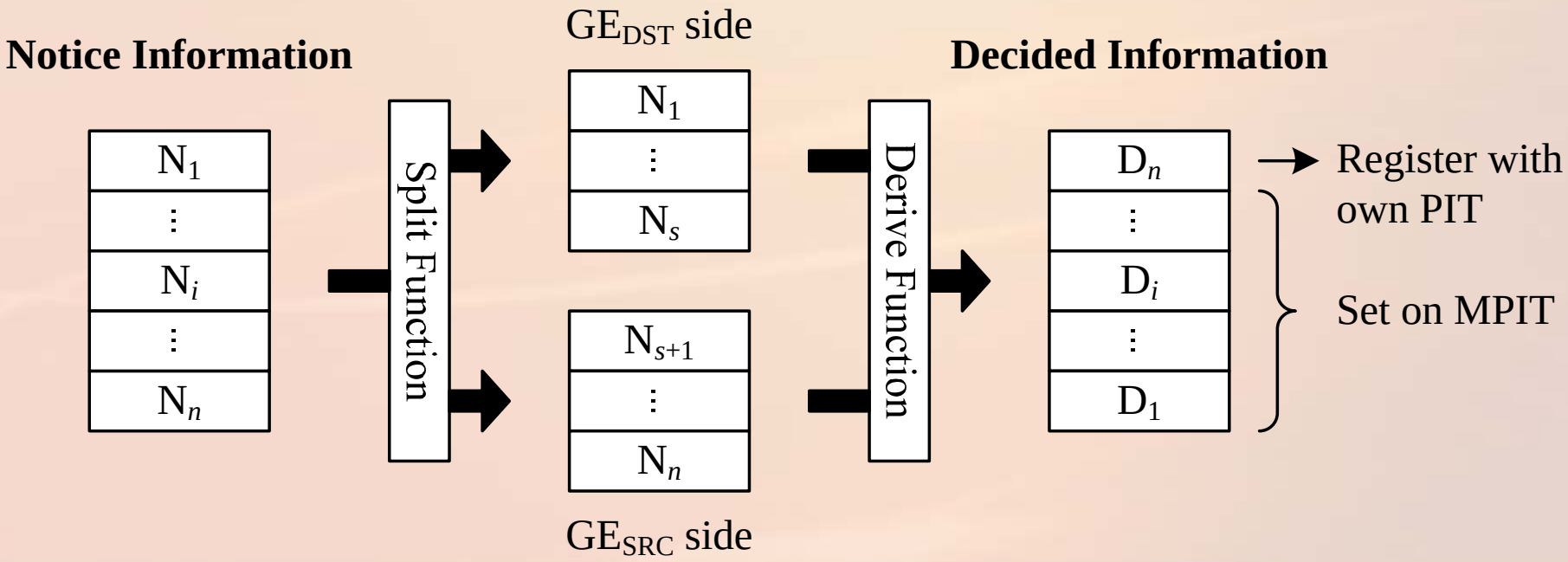
- DPRPネゴシエーションの完了を通知

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

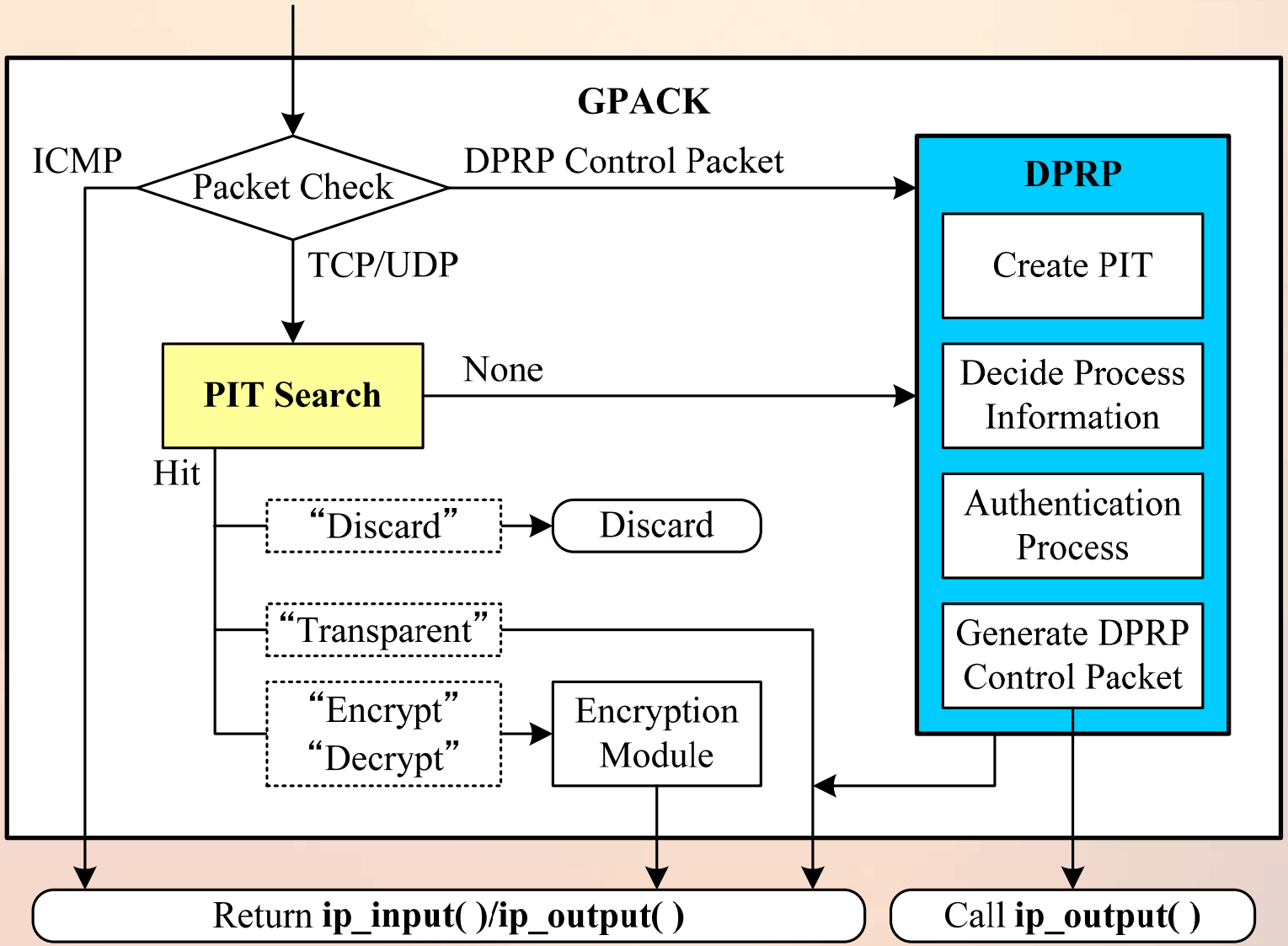
- 待避していた通信パケットを復帰

動作処理情報の決定

- RGIにより取得した通知情報から動作処理情報を導出
  - 通信グループ番号，動作モード，ネゴシエーションの方向情報から総合的に判断
  - 始点GEに関する情報はPITに登録
  - その他の情報はMPITに記載して送信



GSCIPモジュールの処理フロー



DPRPの性能測定(2)

- GEにおける内部処理時間
  - 測定ツール:RDTSC

単位:μsec	GES1	GEN	GES2	合計
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

- FTPスループットの違い
  - 測定方法:500MBのファイルをnullデバイスにダウンロード

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

GSCIPとIPsecの設定内容と項目数の比較

GSCIP	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 ❖通信グループ番号
項目数	3	2

IPsec	IKE用共有鍵	SP	IKE
設定内容	❖通信相手識別子 ❖鍵データ	❖通信ペア識別子 ❖処理内容 ❖適用プロトコル ❖モード ❖SGWペア識別子 etc...	❖通信相手識別子 ❖自端末識別子 ❖交換モード ❖暗号アルゴリズム ❖認証方式 etc...
項目数	2	8(N,D) 14(Tra) 16(Tun)	12

初期管理負荷の詳細

GSCIP	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用共有鍵	SP	IKE	合計
GES1	4	14(Tra)	12	30
GEN	2	16(N+D)	0	18
GES2	2	22(T+D)	12	36

- GES1-GES2: GES1,GES2=Transport, GEN=None
- GEN,GES2 are CL: GEN,GES2=Discard

ネットワーク構成変化時の管理負荷の詳細

IPsec	IKE用共有鍵	SP	IKE	合計
GES1	0	20	13	33
GEN	1	16	12	29
GES2	1	4	1	6

- GES1
  - SP: change Transport=4, add Tunnel=16 (GES1-GEN)
  - IKE: change=1, add=12 (GES1-GEN)
- GEN
  - SP: add Tunnel=16 (GES1-GEN)
  - IKE: add=12 (GES1-GEN)
- GES2
  - SP: change Transport=4
  - IKE: change=1