社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

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

鈴木　秀和† 　渡邊　晃‡

†‡名城大学大学院理工学研究科 〒468-8502 愛知県名古屋市天白区塩釜口 1-501
E-mail: †m0432022@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp

あらまし　企業内ネットワークでは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・管理が難しくなる傾向がある．そこで我々は既存技術だけでは実現が難しいセキュリティ対策と運用管理負荷の軽減を両立したシステムを可能とする FPN（Flexible Private Network）の構築を目指している．FPN 環境下では，異なるアクセスポリシーを持つ各ユーザおよび端末は部署単位や権利者単位でグループ化されており，グループ内の端末間通信は暗号化され，異なるグループ間の端末間通信は拒否される．そこで本稿では通信可否の判断や通信パケットの暗号化処理に必要な情報を動的に生成する機能を提供する動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）の仕組みについて述べる．

キーワード　セキュリティ，プロトコル，イントラネット，FPN，GSCIP

The mechanism of DPRP in Flexible Private Network

Hidekazu SUZUKI† 　Akira WATANABE‡

†‡Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan
E-mail: †m0432022@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp

Abstract　The management of network system tends to become difficult when we improve security in intranet. Therefore, we have been developing the concept of FPN (Flexible Private Network) which is compatible with security levels and simple management. Under the FPN environment, users are grouped according to their access policies and the communications between terminals in the same group are enciphered, and the communications between terminals in different groups are rejected. In this paper, we describe the mechanism of DPRP (Dynamic Process Resolution Protocol) that defines the behavior of the function in FPN.

Keyword　Security, Protocol, Intranet, Flexible Private Network, GSCIP

1. はじめに

インターネットの普及に伴い，企業業務においてネットワークの利用が必須となっている今日，不正進入，データの盗聴や改竄といった様々な攻撃へのセキュリティ対策が重要な課題となっている．一般的な対策方法として，ファイアウォール，IDS の設置や通信の暗号化，ディジタル署名などがある．これらは外部からの攻撃や第 3 者による悪意のある行為を防ぐ効果があり，広く利用されている．しかし企業ネットワークにおけるセキュリティの脅威は，インターネット経由だけではなくイントラネット内部にも存在し，企業が管理する個人情報の漏洩など社員による内部犯罪が多く報告されている[1]．イントラネット内部のセキュリティ対策として相手認証，アクセス管理や社員へのセキュリティに関する教育研修などがあげられるが，外部犯罪に対する対策と比べてあまり行われておらず，社内のインフラ保護や管理の難しさ，また社員のセキュリティに対する意識の低さが問題視されている[17]．

一般的にネットワークセキュリティの基本対策として相手認証と暗号化通信が挙げられる．この機能を併せ持った既存技術として IPsec [3]があり，現在では VPN（Virtual Private Network）[5]を構築する手段として広く利用されている．IPsec は暗号化通信に先立ち，IKE（Internet Key Exchange）プロトコル[4]によって暗号・認証に必要なパラメータを動的に生成して安全に情報の交換を行う．IKE は IPsec 以外でも利用できる汎用性を持っており，数々のオプションをクライアント端末およびセキュリティゲートウェイ（以下 SG）に設定をする必要がある．そのため設定が複雑になりやすく， IPsec を理解することが難しいため，高い安全性を実現するには設定や運用に関する高度な専門知識が要求される．また，IPsec はクライアントまたは SG

が必ず対で存在していなければならない．イントラネット内では部署ごとにアクセスポリシーが異なり，組織の構成に応じてセキュリティドメインが階層的に構築される場合がよくある．その場合，ある端末間の通信経路上に2台以上のSGとIPsecクライアントが存在する多段構成が考えられるが，IPsecでは多段構成に対応することができない．このような点からIPsecはイントラネットにおけるセキュリティ対策の手段としては適切とは言えず，普及が進んでいない．IPsecの他にSOCKS[2]やSSL[6]などの既存技術があるが，同様にイントラネットの特徴に対応しつつ，セキュリティと運用管理負荷の軽減を共に満たすことは難しい．

企業ネットワークではセキュリティ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．そこでイントラネット内のセキュリティ対策と運用管理負荷の軽減を両立できるFPN（Flexible Private Network）の環境構築を目指している[16]．FPNでは業務に応じた部門または権利者単位に安全性の確保されたグループを構築する．グループを構成する装置には，エンド端末の他にSGに類似したボックス型の装置などがあり，これらの装置を総称してここではEE（Encryption Element）[7]と呼ぶ．同一グループ内の端末間の通信は暗号化によって保護されるため，異なるグループの端末は不正なアクセスやデータの盗聴をすることができない．そこで各EEは通信相手が同一のグループに帰属しているかを確認することと，どの暗号鍵で通信を暗号化するかなどをあらかじめ決定しておかなければならない．著者らは，これらの動作処理情報を自動的に解決するためのプロトコルとして，動的処理解決プロトコルDPRP（Dynamic Process Resolution Protocol）を提案，改良してきた[7][10][15]．DPRPは各EEに事前に設定されるグループ定義情報などをもとに，EEが通信端末との位置関係を検出しながら動的に動作処理情報を生成する機能を提供する．DPRPを使うことによって，システムの物理的構成に変化があっても，EEの保持する動作処理情報が動的に再生成されるため，管理装置での作業負担が一切発生しないという利点がある．

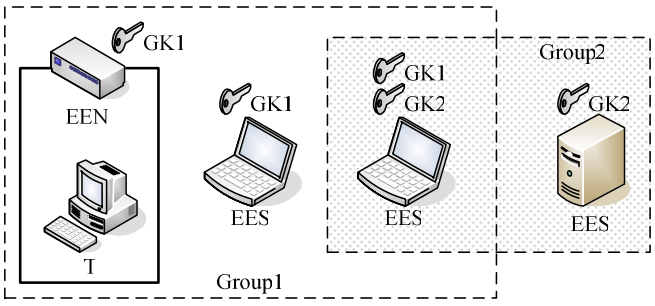


図1　GKによる端末のグルーピング

Fig 1. Grouping of Terminals with Group Key

本稿ではこれまで進めてきたDPRPの検討成果として，最終的に決定されたDPRPの仕組みについて述べる．以降，2章でFPNの概要と実現方法を述べ，3章でDPRPの動作原理についてネットワークモデルを用いて説明する．4章で実装方法を述べ，5章でまとめる．

2. FPNとGSCIP

2.1. FPN

FPNは暗号装置EE，鍵管理装置MS（Management Server）の2つの要素から構成される．EEは端末にソフトウェアをインストールして実現するEES，ルータに実装して実現するEENという2種類の装置に分類される．図1に示すようにEEはグループ鍵GKを保持しており，同一のGKを持つ端末の集合を通信グループとして定義する．GKとグループの番号は1対1で対応している．また各EEには同一グループの端末だけと暗号化通信が可能な閉域モード（CL；Close Mode）と，グループが異なる場合は平文で通信が可能な開放モード（OP；Open Mode）の2種類の動作モードの何れかが設定される．一般には移動端末は開放モード，配下のサブネットワークを保護するEENや重要なサーバは閉域モードに設定される．EEN配下のサブネットに存在する一般端末（T；Terminal）は，GKを保持しないためグループには所属していないが，EENによって保護されているため事実上EENと同じグループに所属していると見なしてよい．

FPN環境の概要を図2に示す．まずユーザはICカードなどを利用した本人認証を行う．ユーザが正しく認証されると，MSからEEのグループ番号およびそのグループに対応したグループ鍵GK，そしてシステム全体で共通に用いられるグループ共通鍵CK（Common Key）が配送される．ここまでの手順によりFPNにおけるグループ間通信の準備が完了する．

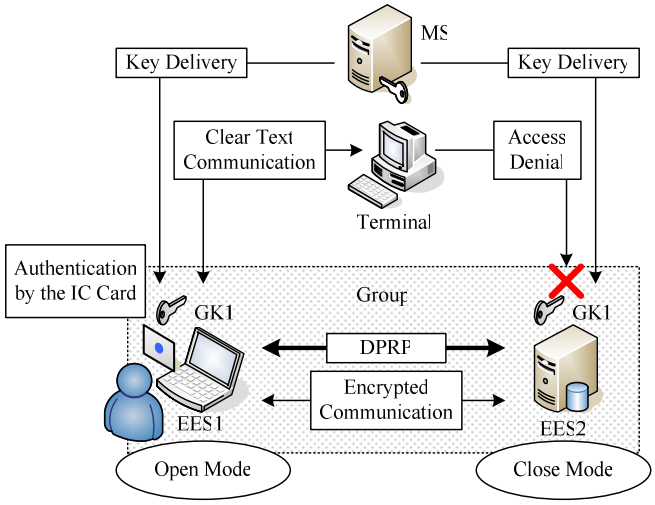


図2　FPN環境の概要

Fig 2. Outline of FPN Environment

EES1 と EES2 間の通信に先立ち DPRP によるネゴシエーションが実行され，通信可否の判断と暗号処理に必要な情報を記した動作処理情報テーブル PIT（Process Information Table）が動的に生成される．以後，EE がこの PIT を参照することにより通信が行われる．図 2 においては，EES1，EES2 の両端末は同じグループに所属しているので暗号化通信を行う．一般端末 Terminal と EES1 間の通信は，同じグループに所属していないが，EES1 が開放モードなので平文による通信が可能である．一方，Terminal と EES2 間の通信は同じグループに所属しておらず，かつ EES2 が閉域モードなのでアクセスは拒否される．

ネットワーク構成の変更やユーザの移動があっても，通信に先立ち DPRP が実行されるため，その状況に応じた設定を動的に行ってくれる．このため，グループの帰属関係が変わらない限り管理者の設定変更などの作業は一切発生しない．この機能を物理的位置透過性，またはロケーションフリー（Location Free）と呼んでいる．これにより図 3 のようにユーザが移動した場合でも，各自が所属するグループ内の端末とは安全に通信が可能である．

次に企業ネットワークでは階層的にセキュリティドメインが構築されるケースが多い．ある端末間の通信経路上に 3 台以上の EE が存在する多段構成が必要になることも考えられる．IPsec では 1 対 1 の IPsec 機器間ネゴシエーションしかできなかったが，FPN では通信経路上の EE が相互に情報を交換することで，多段構成におけるネゴシエーションが可能となっている．

現時点における DPRP では，通信中の端末の移動がない静的な状況を想定しているが，通信中に移動してもコネクションを維持して通信を保証する Mobile P2P[8]への拡張を検討している．

2.2. GSCIP

FPN を実現するために GSCIP（Grouped Secure Communication for IP；ジースキップ）[10][16]という独自のネットワークセキュリティアーキテクチャを検討している．DPRP もこの GSCIP の一機能として組み込まれる．GSCIP は DPRP 以外にも暗号プロトコル PCCOM（Practical Cipher Communication Protocol）[12]，IC カードによるセキュア認証プロトコル SPAC（Secure Protocol for Authentication with IC Card）[14]，移動端末が通信中に移動しても通信が保証される移動体通信処理プロトコル Mobile P2P[8]，グローバルアドレス空間からプライベートアドレス空間へのアクセス開始を可能とする NATF（NAT Free Protocol）[9]，多段構成ネットワークにおける鍵配送プロトコル SKDP（Secure Key Delivery Protocol）[13]という 6 つのプロトコル群とユーザの不正アクセスによく利用される多重リモートログインを行う渡り歩きの検知機能[11]が含まれる．この GSCIP によって柔軟な通信グループを構築でき，高いセキュリティを併せ持ち，かつ管理者に運用管理の負荷を与えないのが GSCIP の特徴である．

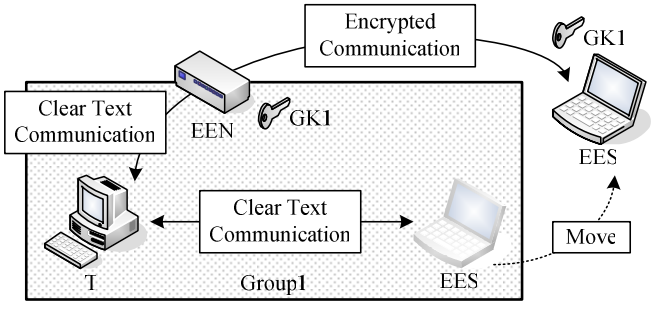


図 3　物理的位置透過性の保証

Fig 3. Location Free

3. DPRP シーケンスと制御パケット処理

DPRP ネゴシエーションの動作原理を説明するために図 4 のようなネットワーク構成を考える．各端末が所属するグループと動作モードは表 1 に示す設定とする．ここで EES1 と EES3 間の通信を考える．EES1 が通信データを送信しようとすると，まず自身が保持する PIT を検索する．検索キーは通信パケットの送信元と宛先の IP アドレスとポート番号，プロトコルタイプの 5 つの情報のハッシュ値である．検索の結果，EES1 と EES3 間に関する情報（PIT レコード）が存在しない場合，送信パケットを待避させてから DPRP を開始する．DPRP は図 5 に示される 2 往復のネゴシエーショ

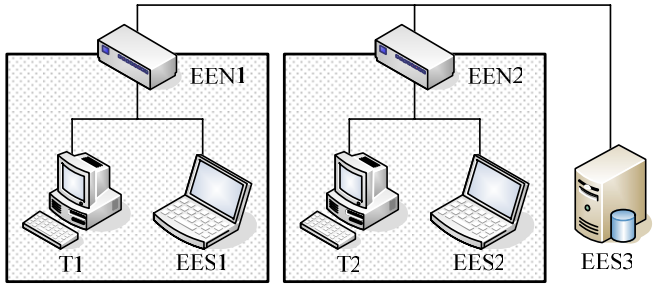


図 4　ネットワーク構成

Fig 4. Network Configuration

表 1　所属グループと動作モードの設定

Table 1. Configuration of Entities

Entity	Group Number			Process Mode
	1	2	3	
T1	○*1			—
T2		○*2		—
EES1	○		○	OP
EES2		○		OP
EES3			○	CL
EEN1	○			CL
EEN2		○		CL

*x ： Don't have GKx. The Entity is protected by EENx.

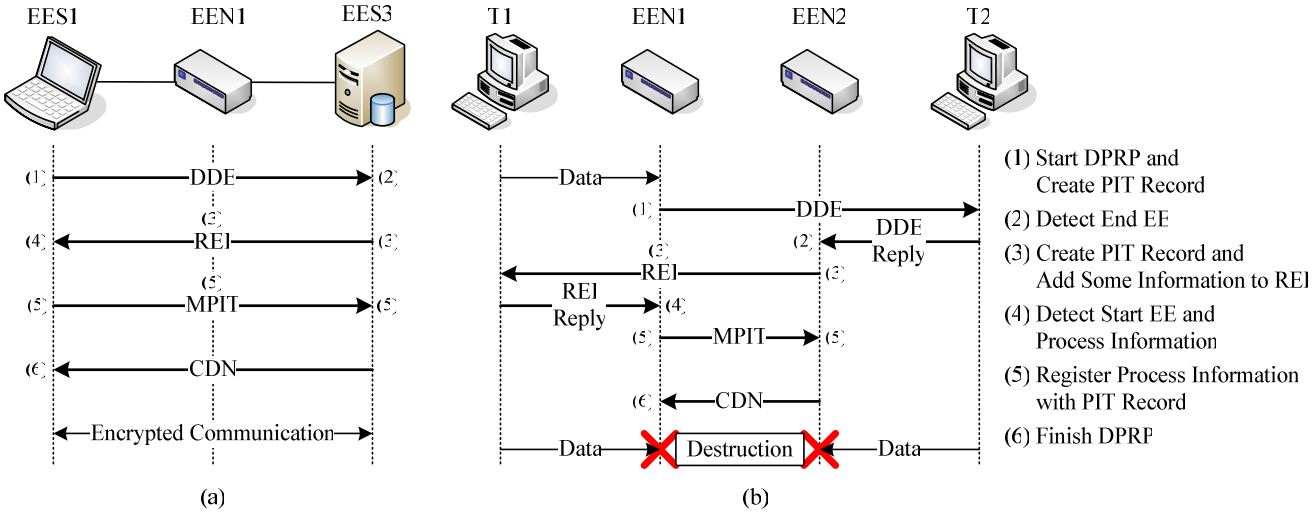


図 5　DPRP シーケンス

Fig 5. DPRP Sequences

ンを行う．通信経路上に存在する EE において，ネゴシエーション開始端末に最も近い EE を始点 EE，始点 EE から最も離れた EE を終点 EE，両終端 EE に挟まれている EE を中間 EE と呼ぶ．このネゴシエーションは DDE（Detect Destination End EE），REI（Report EE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）という ICMP をベースとした 4 種類の制御パケットで実行される．DPRP ネゴシエーションにより PIT に EES1-EES3 間の双方向の動作処理情報が動的に生成され，その情報を元にして待避させておいた送信パケットを暗号化して送信する．

以下に 4 種類の DPRP 制御パケットの果たす役割と処理内容および動作処理情報テーブル PIT について詳述する．

3.1. DPRP 制御パケットの構造

制御パケットの構造は図 6 のように示される．制御パケットは DPRP ヘッダを持ち，その後に各制御パケットのデータが設定される．DPRP ヘッダには制御パケットであることを示す DPRP ID，制御パケットの種類を示す Code，ネゴシエーション識別子（NID）などから構成されている．

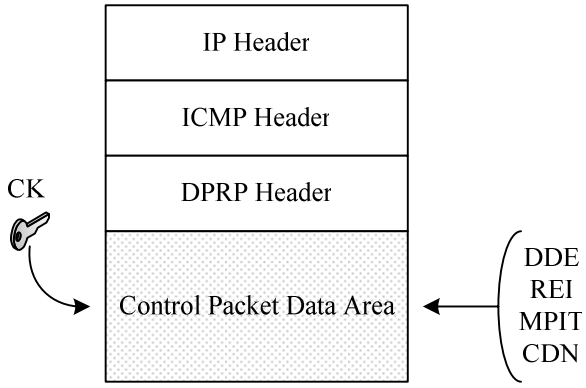


図 6　DPRP 制御パケット構造

Fig 6. DPRP Control Packet Structure

また制御パケットは図 6 の網掛けの制御パケットデータ部分が全てグループ共通鍵 CK により暗号化されているので，安全に情報交換が可能である．

3.2. DDE

DDE は ICMP Echo Request をベースに定義されている．このパケットは DPRP 開始時に送信され，始点 EE の PIT レコード生成と終点 EE の決定という 2 つの機能を持つ．PIT レコード作成中の状態で，EES1 が同じ宛先に送るパケットを送信しようとしても，そのパケットは待避バッファに移る．DDE の宛先は通信パケットの宛先と一致しており，EES は DDE を受信することで終点 EE を決定できる．ここで図 5(b)のように DDE の宛先が一般端末の場合，T2 には DPRP を実装していないため，通常の ICMP を受信したことと同じである．よって T2 からは Echo Reply が返信される．この Echo Reply を最初に受信した EE，つまり EEN2 が終点 EE となる．

DDE には PIT レコードの検索キーとなる 5 つの情報が設定される．この 5 つの情報をコネクション識別子 CID という．

3.3. REI

REI は ICMP Echo Request をベースに定義されている．このパケットは終点 EE から送信され，PIT レコード生成，通信経路の EE 設定情報などの通知，始点 EE の決定という 3 つの機能を持つ．REI の宛先は DDE によって通知された CID の送信元端末になる．ここで図 5(b)のように REI の宛先が一般端末の場合，T1 には DPRP を実装していないため，通常の ICMP を受信したことと同じである．よって T1 からは Echo Reply が

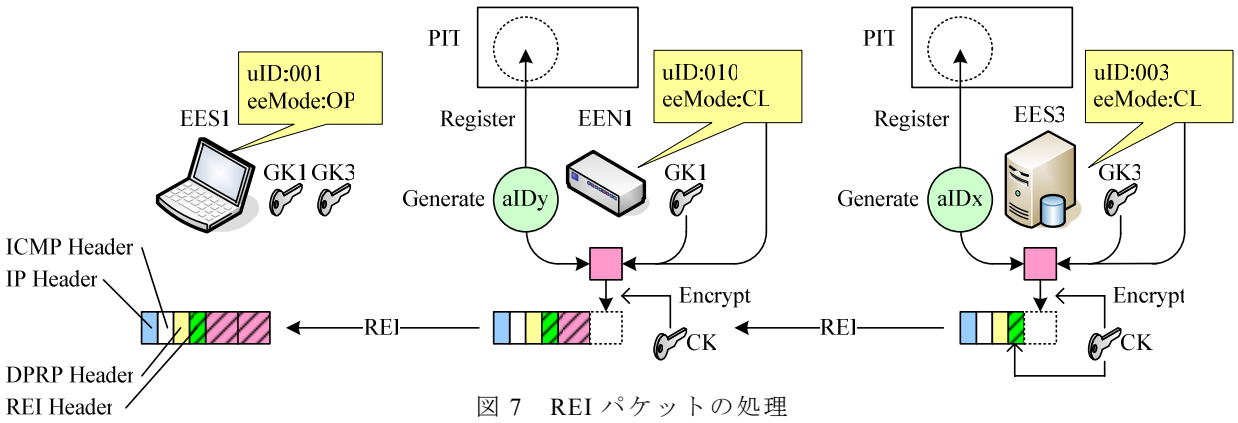


図 7　REI パケットの処理

Fig 7. Process of REI Packet

返信される．この Echo Reply を最初に受信した EE，つまり EEN1 が始点 EE となる．

REI の最も重要な機能は PIT を生成するのに必要不可欠な情報を通知することである．図 7 に示すように REI を送信する終点 EE，通信経路上の中間 EE は REI に自端末の EE 設定情報（eeInfo），グループ鍵情報（GKI）と生成した認証情報（aID）及びネットワークの内外の関係（Direction）をまとめて CK で暗号化して追加していく．ここで aID はランダムな値で，PIT に登録しておき，後の DPRP パケットの認証に利用するものである．ネットワークの内外の関係とは，図 8 に示すように EEN によって保護されているエリアの外側から内側に入るのか，内側から外側に出るのかという方向を示すものである．EEN ではそれぞれ Out to In，In to Out と表示する．EES の場合，方向は関係ないので Edge と表示する．始点 EE が REI を受信して

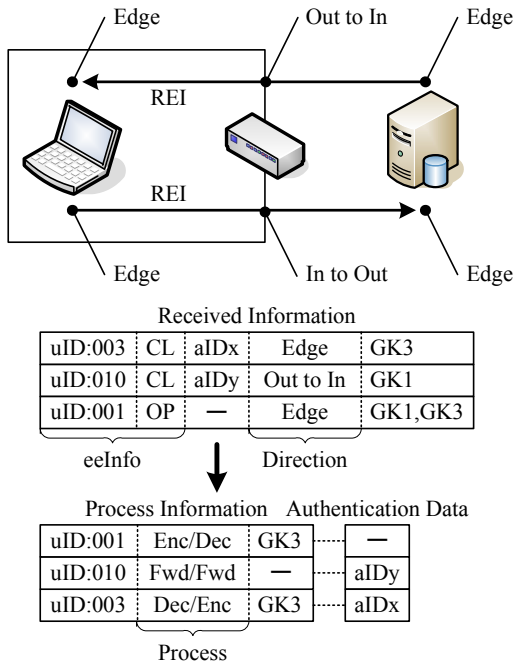


図 8　ネットワークの方向と動作処理情報

Fig 8. Network Direction and Process Information

CK で復号すれば通信経路上の全 EE の情報を取得でき，これらの情報を総合的に判断して動作処理情報（PInfo）を動的に決定する．

3.4. MPIT

MPIT は ICMP Echo Request をベースに定義されている．このパケットは始点 EE から送信され，通信経路上の各 EE に決定した動作処理情報を登録する機能を持つ．MPIT の宛先は終点 EE になる．始点 EE が動作処理情報を決定すると，図 9 に示すように自身の動作処理情報は PIT レコードに登録して，他の EE に関する動作処理情報は受信した aID と対応づける．これらの情報をグループ共通鍵 CK で暗号化して MPIT を生成，送信する．各 EE は MPIT を受信するとグループ共通鍵 CK で復号化して該当する動作処理情報と aID を取得する．取得した aID と REI 送信時に PIT レコードに登録しておいた aID を比較して認証を行う．正しく認証されたら動作処理情報を PIT レコードに登録する．

動作処理内容に暗号化が指示されていた場合，暗号化通信をする EE 間は NID によるグループ認証を行う．グループ認証は暗号化通信時に使用されるグループ鍵 GK によって暗号化された NID を復号，比較することで行われる．正しく認証されたら確実に同じグループに所属していることが保証される．暗号化通信を行うエンド EE は aID による認証も併せて行う．

3.5. CDN

CDN は ICMP Echo Reply をベースに定義されている．このパケットは終点 EE から送信され，DPRP ネゴシエーションの終了を通知する機能を持つ．CDN を受信した始点 EE は DPRP ネゴシエーションが正しく行われたと判断して，DPRP 開始のトリガーとなった送信パケットを待避バッファから戻し，PIT の情報に基づき暗号化通信を開始する．

3.6. 動作処理情報テーブル PIT

PIT は送信元/宛先 IP アドレス（sIP/dIP），送信元/

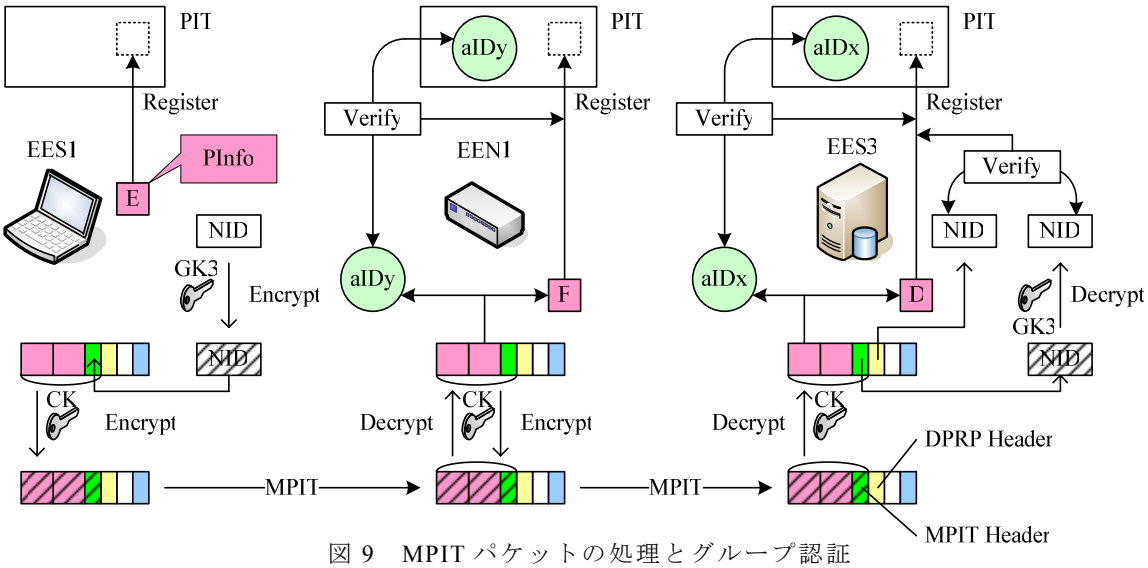


図 9　MPIT パケットの処理とグループ認証

Fig 9. Process of MPIT Packet and Group Authentication

宛先ポート番号(sPort/dPort), プロトコル番号(Proto), 動作処理内容（Proc), グループ鍵情報（GKI), カウンタ値（Cnt）の 8 つの情報から構成される. 動作処理内容としては暗号/復号（ENC/DEC）の他に, 中継（FWD), 破棄（DST）がある.

PIT フォーマットを図 10 に示す. sIP から Proto までのフィールドは, DDE および REI によって通知される情報が登録される. Proc および GKI のフィールドは MPIT によって通知される情報が登録される. REI 送信時に各 EE で生成した認証情報 aID は PIT の予備スペースに登録しておく. MPIT 受信時に実行する DPRP パケットの認証処理が終わると登録しておいた aID は削除される.

FPN 環境におけるアクセス制御や暗号化通信は, PIT の情報により全てが制御されている. そのため PIT には信頼ある情報が格納されている保証が必要である. これらの情報は DPRP 実行中に全て暗号化されているため, PIT 生成に必要な情報を盗聴することはできない. また, 制御パケットを改竄された場合は受信時の復号処理でエラーが発生するため, パケットは破棄され PIT は生成されない. 第三者が IP アドレスを偽造して既に生成されている PIT を悪用しようとしても, PIT で指定された GK を保持しない限り通信することはできない. GK は予め管理者によって各ユーザに設定されているものしか配送されないため, GK を偽造, 盗難することは困難である.

sIP	dIP	sPort	dPopt	Proto	Proc	GKI	Cnt	Rsv
EES1	EES3	xx	yy	TCP	ENC	3	128	—
EES3	EES1	yy	xx	TCP	DEC	3	128	—

図 10　PIT フォーマット

Fig 10. PIT Format

4. DPRP の実装

DPRP は IP 層に実装されるプロトコルで, アプリケーションに依存しない. DPRP は GSCIP の一部として組み込まれるもので, GPACK（GSCIP を実現するモジュール群）の一部として現在開発中の段階である.

実装対象となる OS はオープンソースで, IP 層に関する情報や処理内容の資料が多い FreeBSD を採用した. GPACK はカーネルレベルと, アプリケーションレベルに役割を分担させている. 図 12 に GPACK の実装概要について示す. IP 層で行われる既存の処理にいっさいの変更を加えず, パケットの種類を判別して GPACK に処理を渡す. PIT 検索の結果, 該当するレコードが無い場合, DPRP モジュールを実行する. DPRP モジュールでは制御パケットを生成して, IP 出力関数 ip_output に送る. DPRP に加え, PCCOM, Mobile P2P, NATF, 渡り歩き検出機能がカーネルレベルで動作する.

アプリケーションレベルでは 3 つのデーモンを起動する. SPAC デーモンはユーザの本人認証を行う. SKDP デーモンは各種鍵の取得を行い, PIT と同様に保存するエリアをカーネル領域に確保する. SKDP デーモン起動時に EE のユーザ ID や動作モード, EEN では外向きのネットワークインタフェースの名前を記述した設

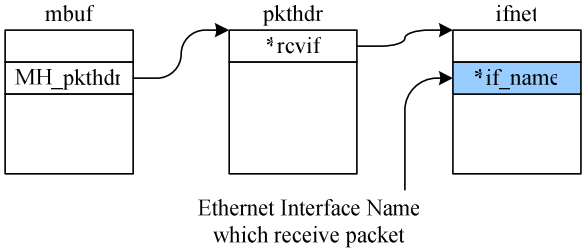


図 11　パケット受信インタフェース名の取得

Fig 11. Getting of a receiving packet Interface Name

定ファイルから初期設定を行う．インタフェース名は DPRP ネゴシエーションにおけるネットワークの方向を決定するために用いる．図 8 に示したようなネットワークの方向を判断するには，受信したパケットがどのインタフェースで受信したか判断すればよい．受信したインタフェース名は図 11 に示すように，mbuf に格納されている情報から取得できる．

DPRP 制御パケットを暗号化するために PCCOM を利用する．

PIT はハッシュテーブルとして実装する．ハッシュ検索アルゴリズムにはチェイン法を用いている．実装される PIT の形式は図 10 で示したフォーマットの最後尾に，次の PIT レコードを示すポインタを格納するフィールド*next が追加されている．PIT 検索時に検索キーから算出したハッシュ値が示す箇所に，別レコードがあると衝突が発生する．この場合，*next を辿ることで目的のレコードを検索することができる．PIT のサイズは 2048 レコードである．

PIT 管理デーモンにより無通信状態にある PIT のカウンタ値をデクリメントしていく．この値が 0 になると該当する端末間の通信が行われていないと判断され，デーモンは PIT レコードを削除する．削除対象となる目安の時間はレコード作成中が約 30 秒，作成済みレコードが約 5 分である．レコードが削除される前に通信が発生したら値を初期化する．PIT 管理デーモンはアプリケーションレベルで動作するため，カーネル領域にある PIT にアクセスするためにはシステムコールを利用する．

5. まとめ

本稿では通信可否の判断や通信パケットの暗号化処理に必要な情報を動的に生成する機能を提供する DPRP の仕組みを述べた．DPRP を利用することで，煩わしい設定事項を動的に生成することで FPN 環境を実現することが可能である．

今後の課題として，DPRP の実装を進め動作確認と性能評価を行う．現段階では DPRP 単独で NAT/NAPT をはさんだ環境に対応することは難しいが，GSCIP に含まれている NATF を利用すること方法が考えられる．グローバル空間とプライベート空間をまたがった DPRP ネゴシエーションが可能になれば，FPN の環境をインターネット領域に拡張することができる．これにより支社間接続やユーザの出張先からのリモートアクセスもイントラネットと同様に，特別な設定を加えることなくセキュアな通信環境が構築できると思われる．

さらに Mobile P2P への拡張を進める予定である．通信中の端末が移動した場合，拡張した DPRP を利用することで通信相手の認証を行いながら，移動情報を通知することが可能になる．この情報をもとに Mobile P2P はコネクションを維持した通信を行うことになる．拡張された DPRP と Mobile P2P によって，ユーザは特別な操作を一切することなく自由に移動して通信することが可能になるため，柔軟なロケーションフリーおよび FPN を実現することができると考えられる．

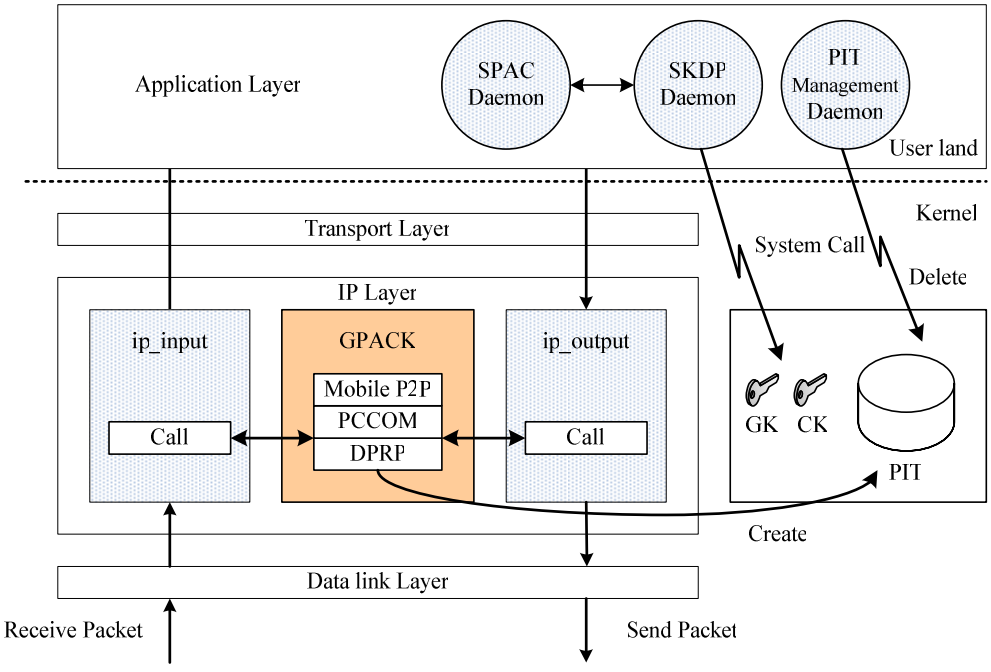


図 12　GSCIP 実装概要図

Fig 12. Outline Figure of GSCIP Implementation

文　献

[1] R.Richardson, "Issues and Trends: 2003 CSI/FBI Computer Crime and Security Survey", CSI Press Release, June 2003.

[2] M.Leech, M.Ganis, Y.Lee, R.Kuris, D.Koblas, L.Jones, "SOCKS Protocol Version 5", RFC1928, March 1996.

[3] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC2401, November 1998.

[4] D.Harkins, S.Carrel, "The Internet Key Exchange (IKE)", RFC2409, November 1998.

[5] E.Rosen, Y.Rekhter, "BGP/MPLS VPNs", RFC2547, March 1999.

[6] P.Hoffman, "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC3207, February 2002.

[7] 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", 信学論（D-I), vol.J84-D-I, No.3, pp.269-284, March 2001.

[8] 竹内元規, 渡邊晃, "移動体通信におけるコネクションを維持した通信方式の研究", 情報処理学会第 66 回全国大会 講演論文集 3-463, March 2004.

[9] 加藤尚樹, 渡邊晃, "NAT を意識しない個人ネットワークを管理する Home Fire Wall の提案", 情報処理学会第 66 回全国大会 講演論文集 3-469, March 2004.

[10] 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 3-479, March 2004.

[11] 竹尾大輔, 渡邊晃, "GSCIP を構成する渡り歩き検出機能の仕組みの検討", 情報処理学会第 66 回全国大会 講演論文集 3-481, March 2004.

[12] 増田真也, 渡邊晃, "閉域通信グループにおける暗号化通信方式の検討", 情報処理学会第 66 回全国大会 講演論文集 3-483, March 2004.

[13] 保母雅敏, 渡邊晃, "多段構成ネットワークにおける鍵配送方式の一検討", 情報処理学会第 66 回全国大会 講演論文集 3-495, March 2004.

[14] 前羽理克, 渡邊晃, "生体認証を利用したセキュアネットワーク通信", 情報処理学会第 66 回全国大会 講演論文集 3-503, March 2004.

[15] 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", 電気関係学会東海支部連合大会 pp.359, October 2003.

[16] Flexible Private Network, Watanabe lab. Division of Information Sciences , Meijo University , http://www-is.meijo-u.ac.jp/~watanabe/research/fpn.html.

[17] Information Technology Association Of America, http://www.itaa.org.

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

The mechanism of DPRP in Flexible Private Network

名城大学 大学院 理工学研究科
鈴木秀和　渡邊晃

研究背景

» 企業ネットワークにおけるセキュリティ脅威

外部からの
ウィルス感染 / 不正アクセス

- ✓ PCウィルス対策
- ✓ GWウィルス対策
- ✓ パッチ/更新管理
- ✓ FW
- ✓ IDS

内部関係者による
不正アクセス / 情報漏えい

- ✓ ファイル操作の権限管理
- ✓ 従業員教育・研修

- 対策ツールが多い
- ほとんどの企業が導入済み

- 社内インフラの保護・管理の難しさ
- 社内にセキュリティ専門家がいない
- 社員のセキュリティに対する意識の低さ

内部犯罪の増加が重要な問題

既存技術による対策とその限界

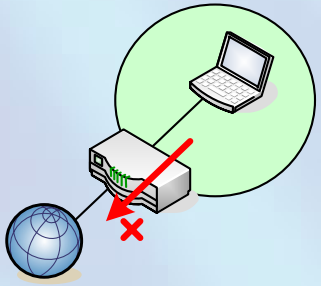
» ネットワークセキュリティの基本対策
- 相手認証
- 暗号化通信

IPsec → VPN構築手法として普及

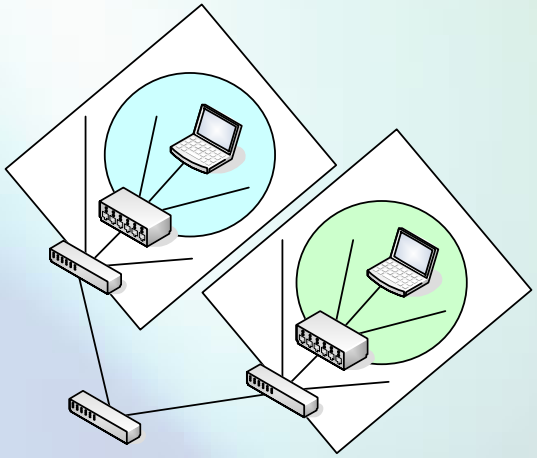
» イントラネット内に適用すると…

設定が煩雑で難しい

管理者が通信を把握できない



NAPTとの相性問題



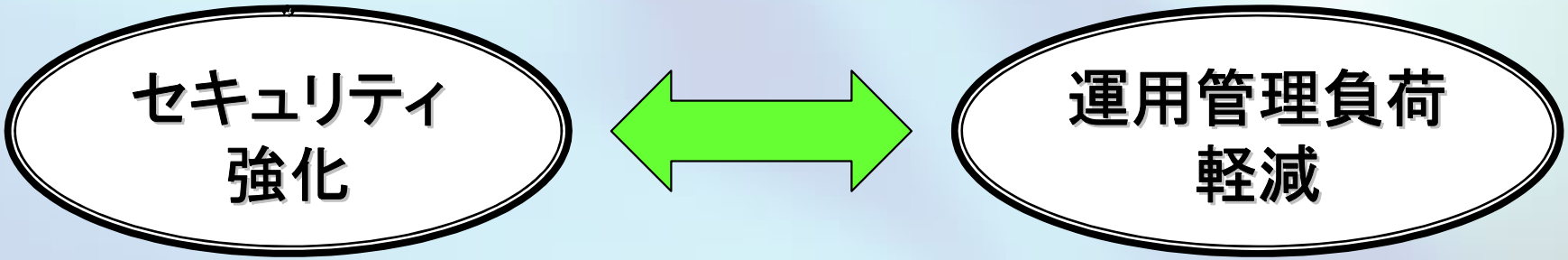
多段構成(階層構成)に対応できない

イントラネット内のセキュリティ対策の手段としては適切でなく，VPN以外で普及が進んでいない．

導入におけるポイント

» イントラネットの特徴に対応した技術が導入のカギ

- セキュリティ強化
- 運用管理において管理者の負担が少ない
- イントラネット環境に柔軟に対応できる
- ユーザが意識することがない



相反する2つの目的を両立できるネットワーク環境

FPN （Flexible Private Network）

FPNの概要

» フレキシブル（柔軟）でセキュアな通信グループを実現することができるネットワーク環境
- 通信ペアの両端末が互いに移動が可能
- 特定サブネットの中にいながら個別に他の通信グループに帰属することが可能
- 同じ通信グループに帰属する端末間は暗号化通信

システム構成の変化やユーザの移動に伴うネットワーク管理の負荷を発生させない

一度定義した通信グループは，ユーザがどこに移動しても保存されていればよい

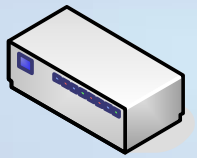
ロケーションフリー（物理的位置透過性）

FPNを構築するために

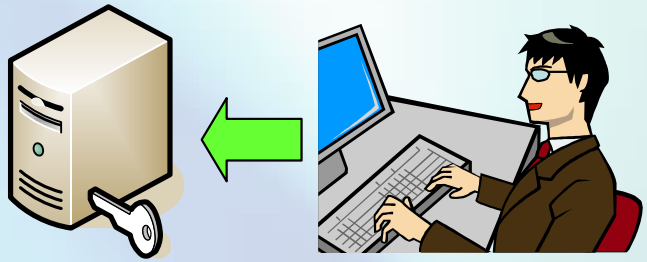
» GSCIP（Grouped Secure Communication for IP）という独自のセキュア通信アーキテクチャを提案している
  - 6つのプロトコル群やセキュリティ機能から構成
  - ロケーションフリーを暗号鍵によって実現

グループを構成するために
GSCIPを実装した装置EE
（Encryption Element）を用意

EES
ソフトウェアをインストール
した移動端末・サーバ



EEN
部門単位でグループを
構成するルータタイプ

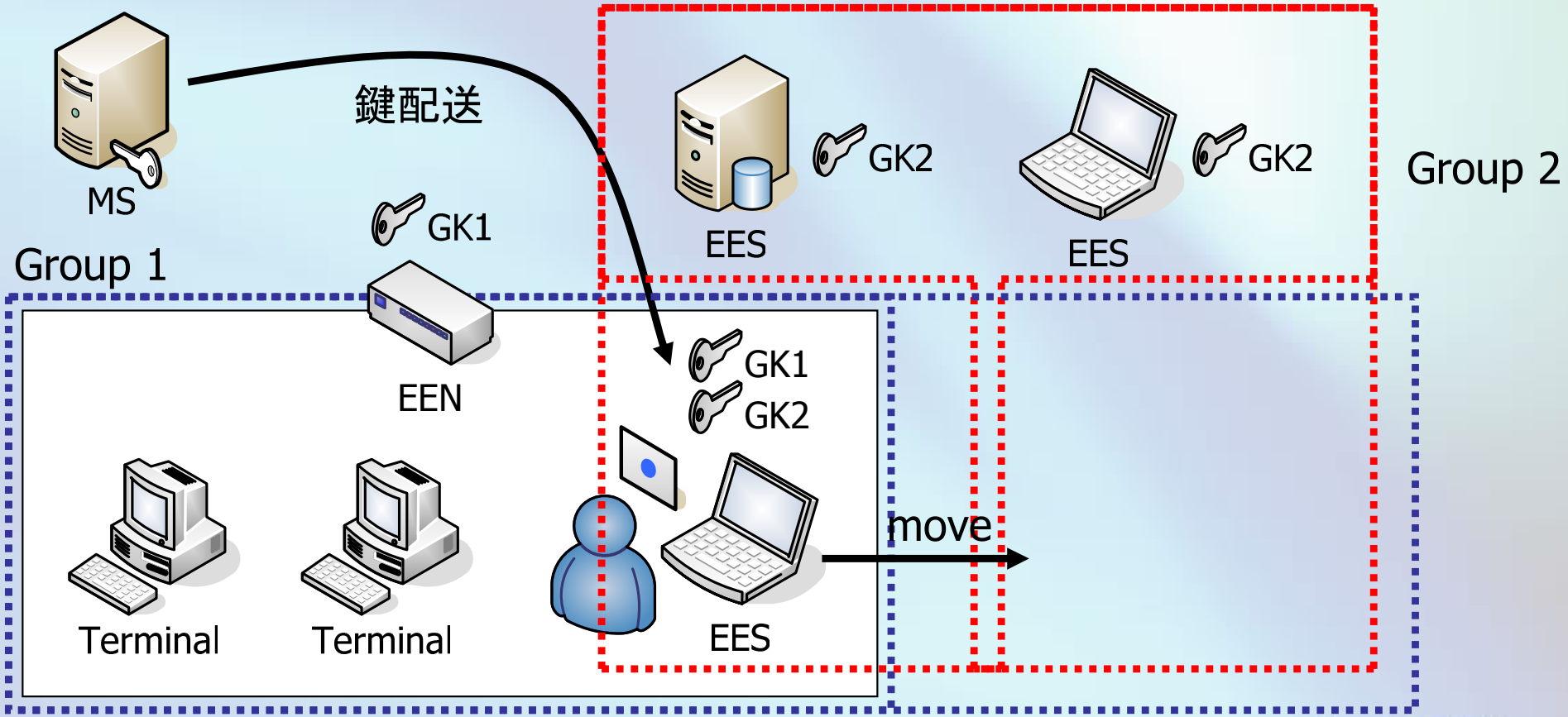


管理者がグループ管理装置
MS（Management Server）に
対して，ユーザが所属する通
信グループを定義

GSCIPによるロケーションフリーの実現

» MSが各ユーザに対して設定されているグループに対応する暗号鍵(グループ鍵GK)を配送
  - グループ共通鍵CKも同時に配送
» 同じグループ鍵を持つEEをグルーピング

GKとグループが1対1で対応

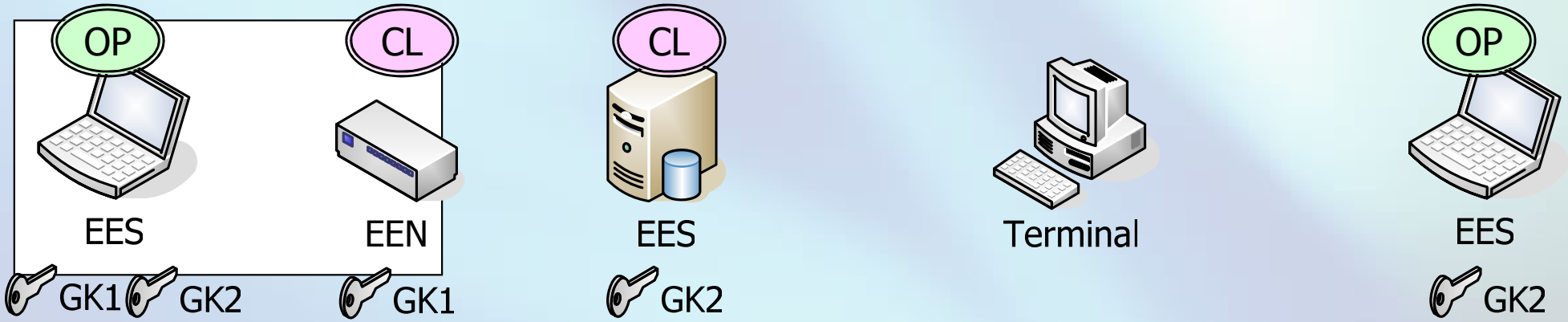


GSCIP実装後の通信

» 通信開始時にネゴシエーションを実行
- 通信可否の判断(グループ，動作モードのチェック)
- 暗号処理に必要な情報の自動生成
  - 動作処理情報テーブルPIT (Process Information Table)に保存

OP 開放モード
全ての通信が可能

CL 閉域モード
暗号化通信のみ可能



鍵が一致
→GK2で暗号化通信

鍵が不一致でCL
→通信拒否

鍵が不一致でOP
→平文通信

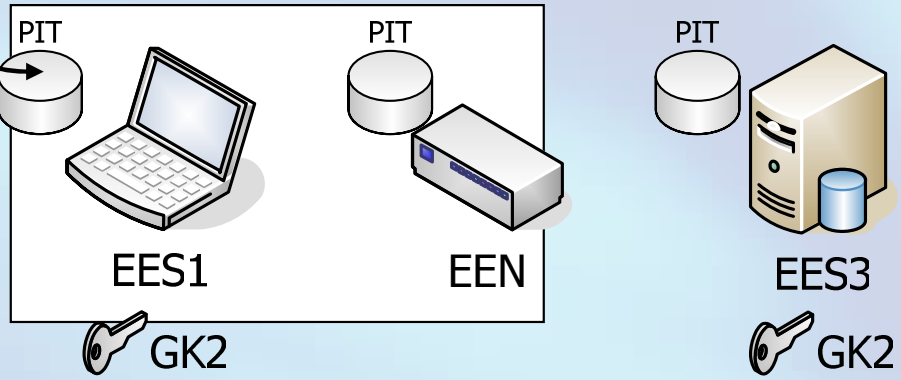
GSCIP実装後の通信

動作処理情報テーブルPIT

sIP	dIP	sPort	dPort	Proto	Proc	GKI
EES1	EES3	xx	yy	TCP	ENC	2
EES3	EES1	yy	xx	TCP	DEC	2

sIP/dIP: 送信元/宛先IPアドレス
sPort/dPort: 送信元/宛先ポート番号
Proto: プロトコルタイプ
Proc: 動作処理内容
GKI: グループ鍵情報

Proc内容
ENC=暗号化　DEC=復号化
FWD=転送（処理無し）　DST=破棄



PITに該当する情報が無い場合，ネゴシエーションを実行

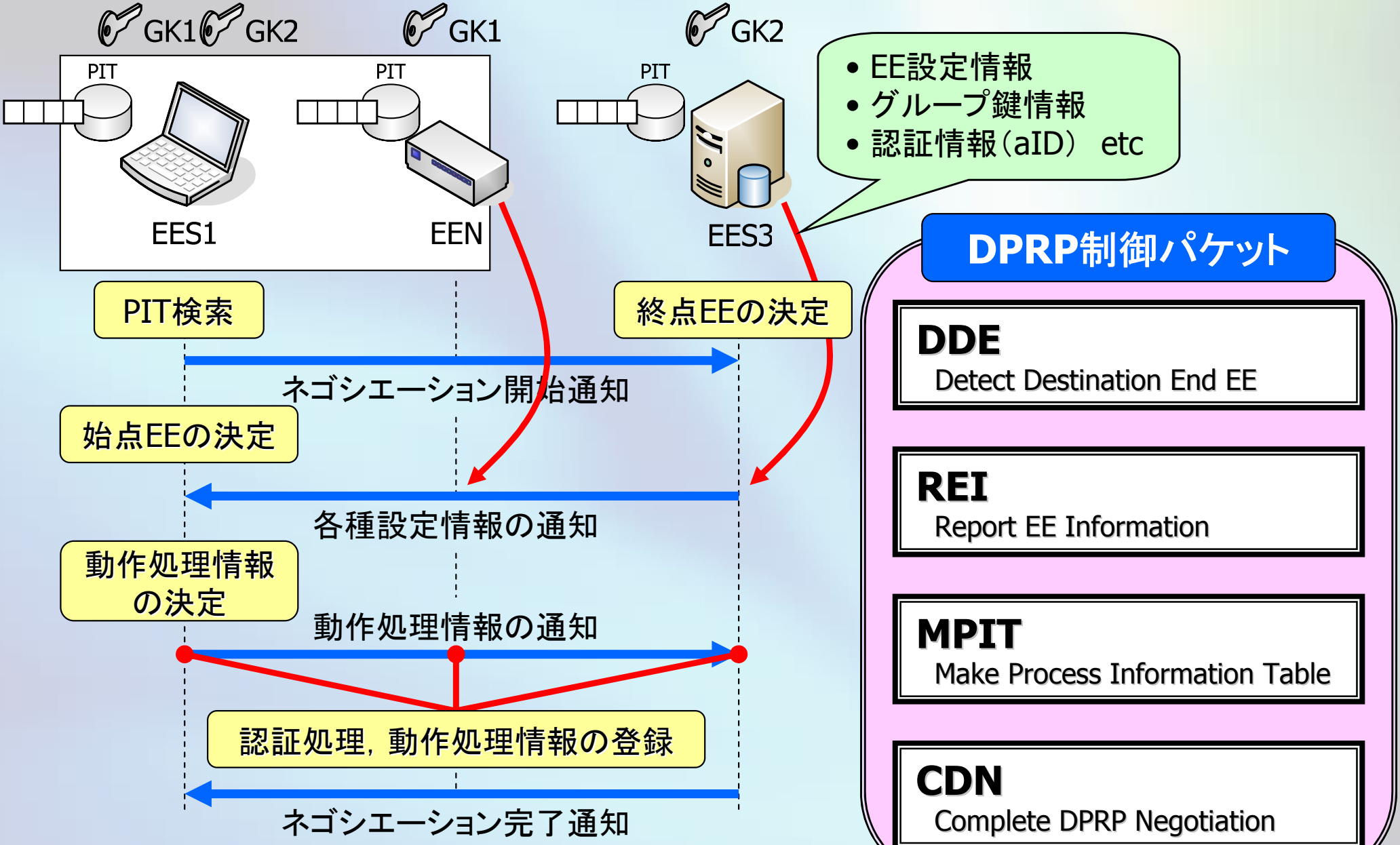
ネゴシエーション

暗号化通信

PIT作成後は該当するレコードが削除されるまで，この情報に基づいて通信パケットを処理する

動的処理解決プロトコルDPRP
（Dynamic Process Resolution Protocol）

動的処理解決プロトコルDPRP



DPRP制御パケット

DDE
Detect Destination End EE

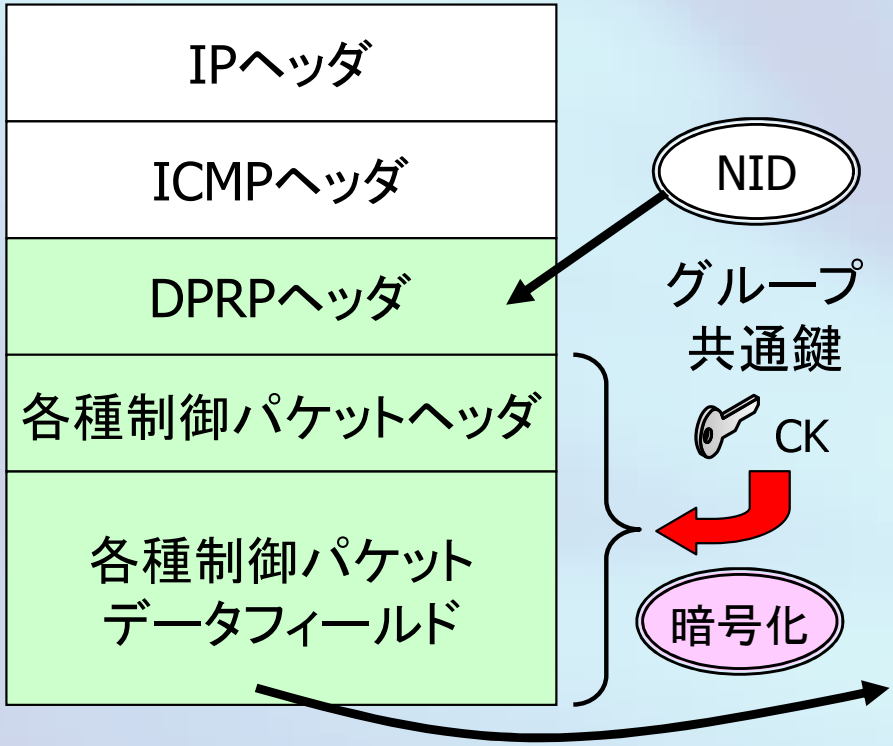
REI
Report EE Information

MPIT
Make Process Information Table

CDN
Complete DPRP Negotiation

DPRP制御パケット

- ICMPをベース（ECHO,ECHO REPLY）
- DPRPヘッダを付加して制御パケットを識別
- ネゴシエーション識別子NIDによるネゴシエーションの区別
  - ネゴシエーション中は不変な値
  - グループ認証処理にも利用
- データ部分はグループ共通鍵CKにより暗号化

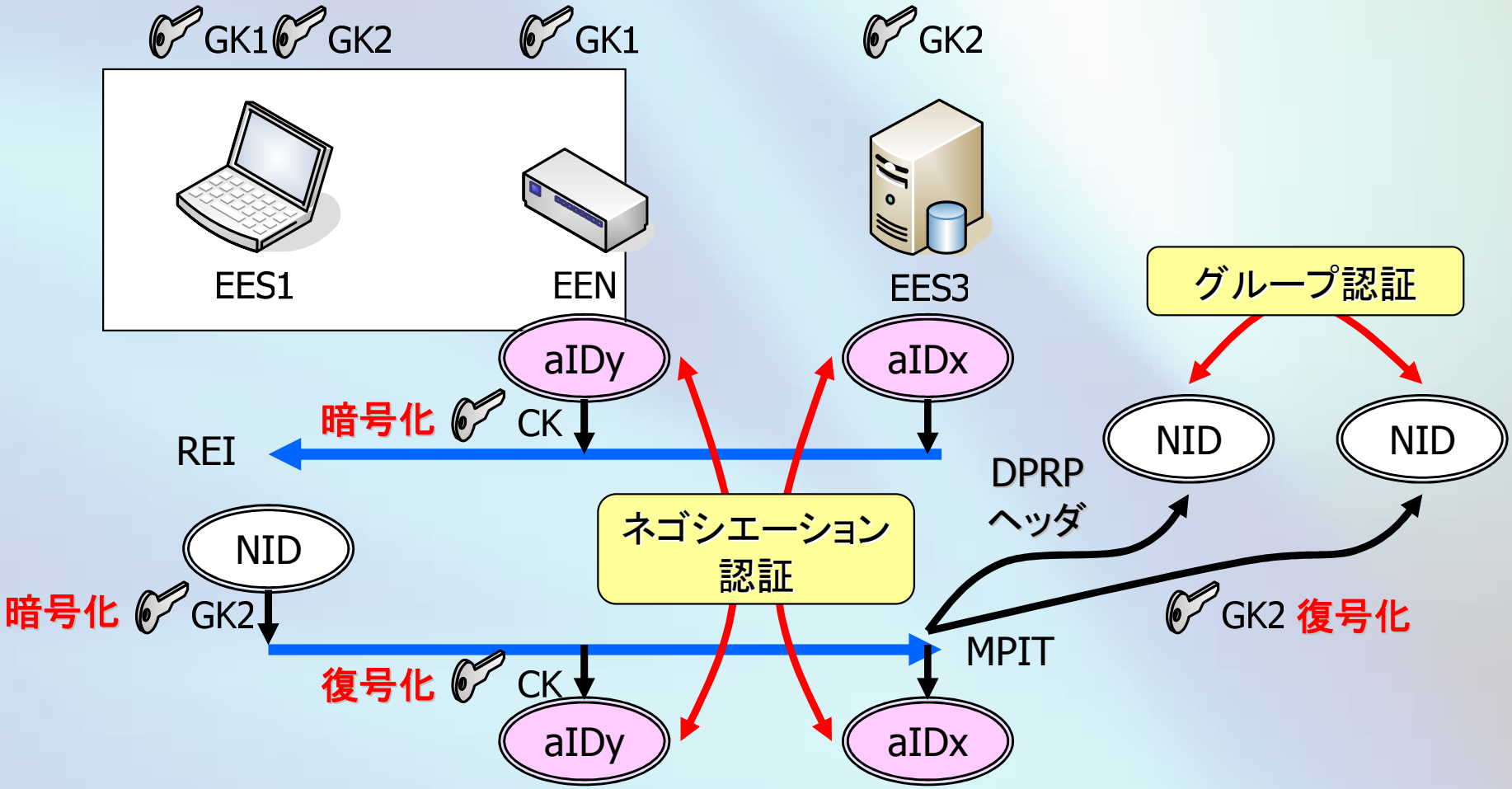


**DPRPネゴシエーションは
安全に情報交換が可能**

- DPRPネゴシエーションを実行している端末間の IPアドレス，ポート番号，プロトコルタイプ
- EE設定情報，グループ鍵情報
- 認証情報（aID）
- 動作処理情報

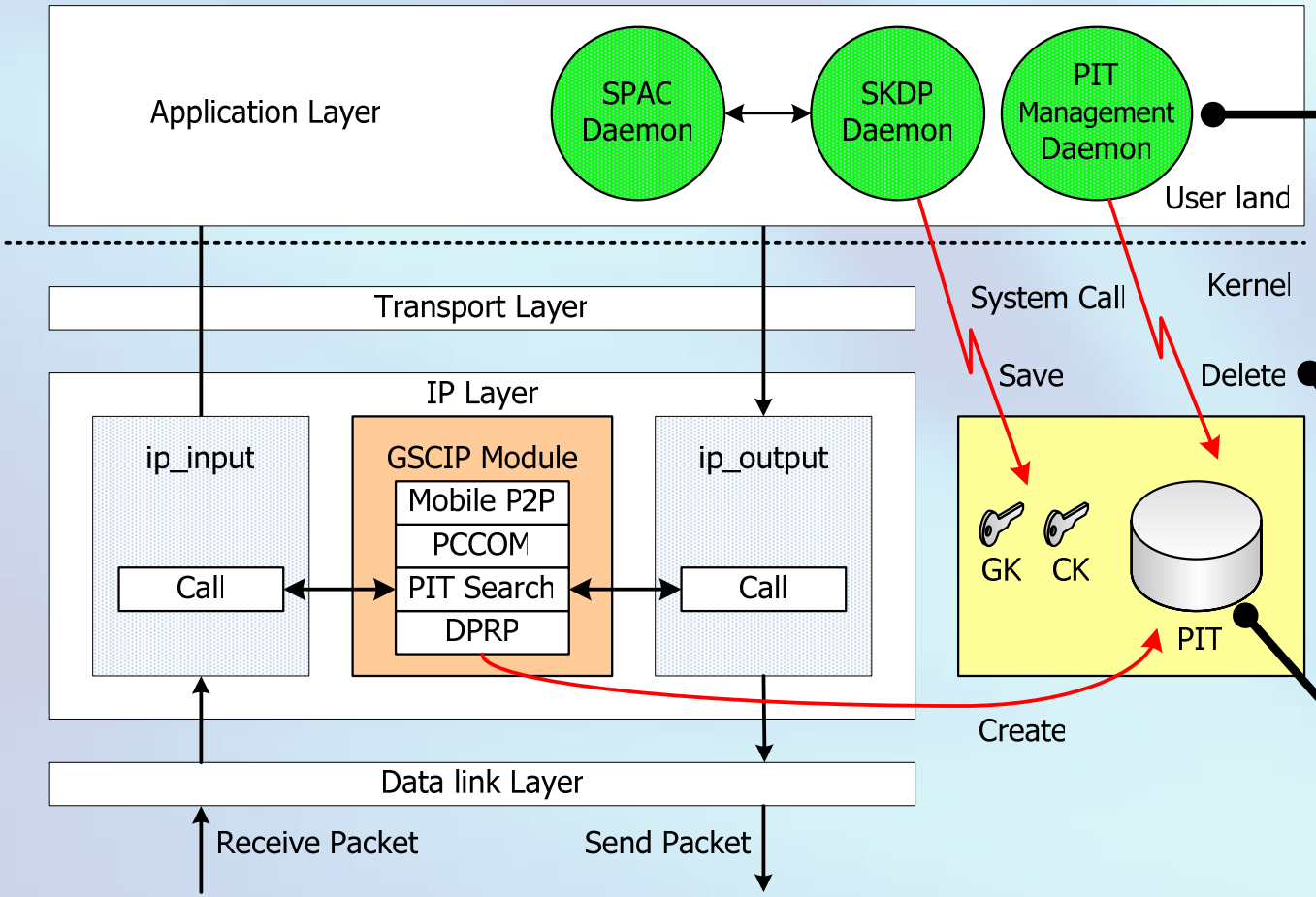
認証処理について

- REI送信時に認証情報aIDをランダムに生成
- MPITに受信したaIDをのせて比較して認証
  - 暗号化通信する両端末間ではNIDによるグループ認証も行う



DPRPの実装について

» FreeBSDにGSCIPの一部として実装
- Kernelレベル（IP層）→DPRP，PIT検索 etc
- User landレベル　→PIT管理デーモン etc



各種デーモンの働き

SPAC：ICカードによる認証
Secure Protocol for Authentication with IC Card
SKDP：鍵配送
Secure Key Delivery Protocol
PIT Management：PIT管理

PITレコード削除時間

- ネゴシエーション中：約30秒
- 作成済み：約5分

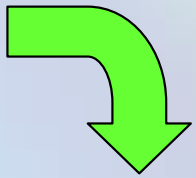
PIT：ハッシュテーブル（チェイン法）

まとめと今後の展開

» DPRPの仕組みについて
- 通信可否の判断
- 通信パケットの暗号処理に必要な情報の動的生成

» 今後の展開
- DPRPの実装と動作確認および性能評価
- NAT/NAPTをはさんだ環境の対応
- Mobile P2Pに対応させる拡張
  - 移動端末が通信中に移動しても通信が保証される移動透過プロトコル

拡張DPRPとMobile P2Pにより，ユーザは特別な操作を一切することなく自由に移動して安全に通信することが可能



柔軟なロケーションフリー，FPN環境の実現へ

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

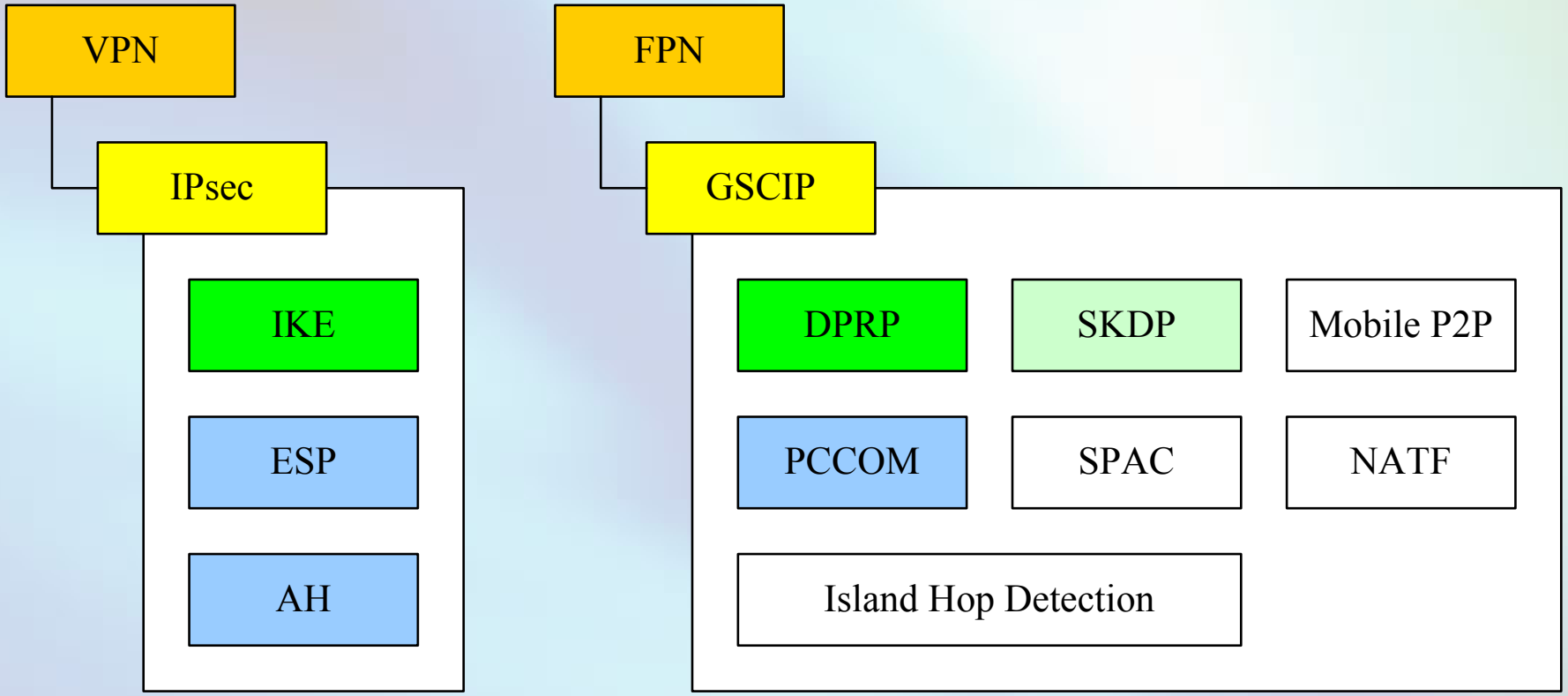
The mechanism of DPRP in Flexible Private Network

終了

本研究は（財）栢森情報科学振興財団の
助成を受けて実施したものである

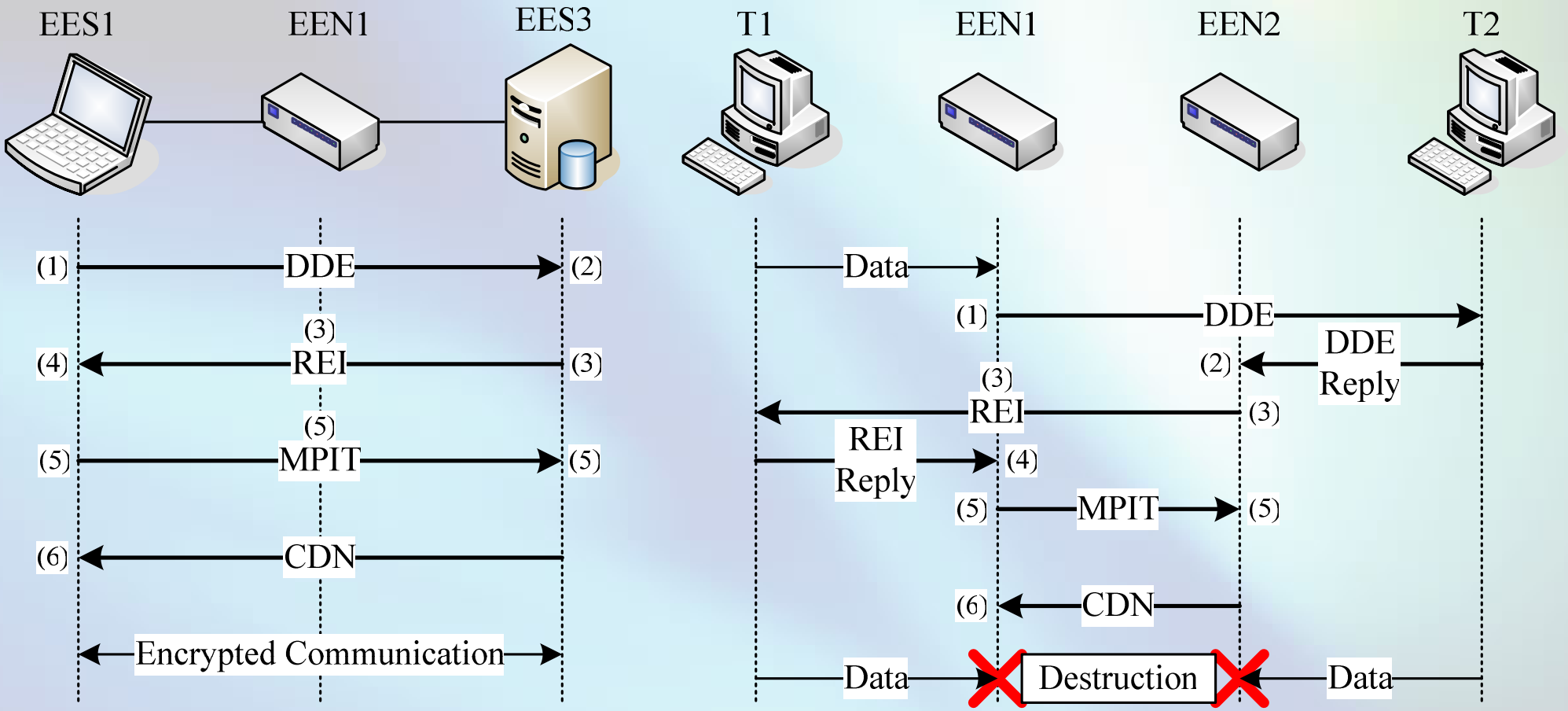
GSCIP (Grouped Secure Communication for IP)

» FPNを実現するための独自のセキュリティアーキテクチャ



DPRP ; Dynamic Process Resolution Protocol
PCCOM ; Practical Cipher Communication Protocol
SKDP ; Secure Key Delivery Protocol
SPAC ; Secure Protocol for Authentication with IC Card
NATF ; NAT Free Protocol

DPRPシーケンス



(1) Start DPRP and Create PIT Record

(2) Detect End EE

(3) Create PIT Record and Add Some Information to REI

(4) Detect Start EE and Process Information

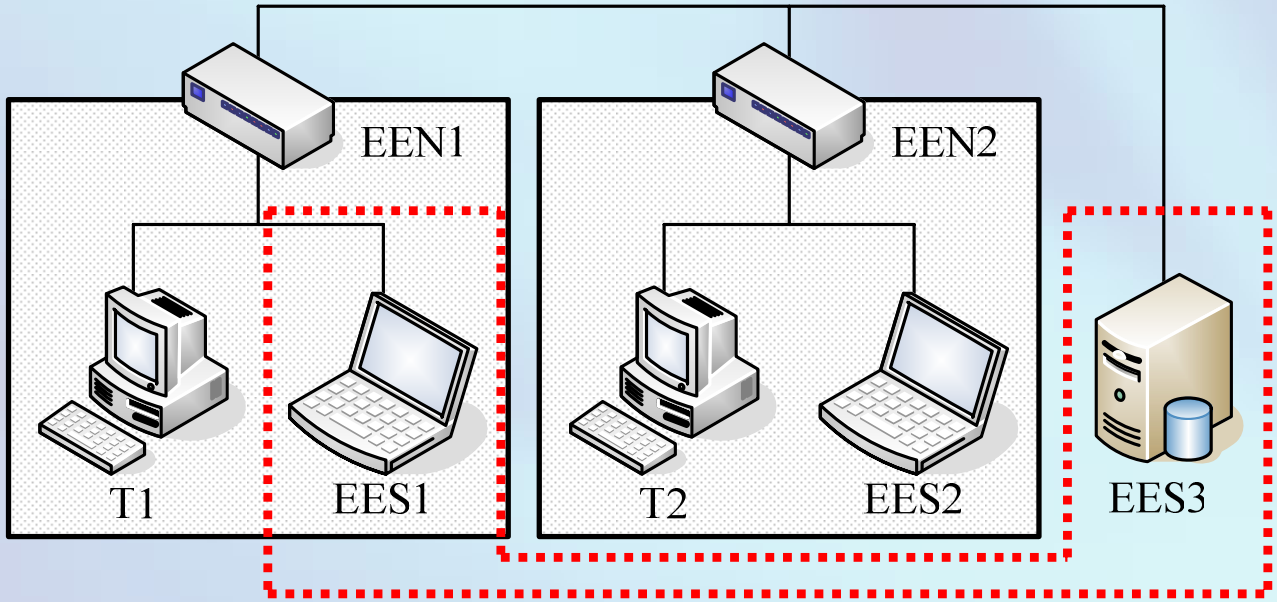
(5) Register Process Information with PIT Record

(6) Finish DPRP

ネットワーク構成とEE設定情報

» 以後，下のネットワーク構成およびEE設定情報を基準にしてDPRPの動作原理を説明
  - EES1からEES3への通信に着目
    - 始点EE＝EES1　　中間EE＝EEN1　　終点EE＝EES3

» EEはGKの他にグループ共通鍵CKを保持している

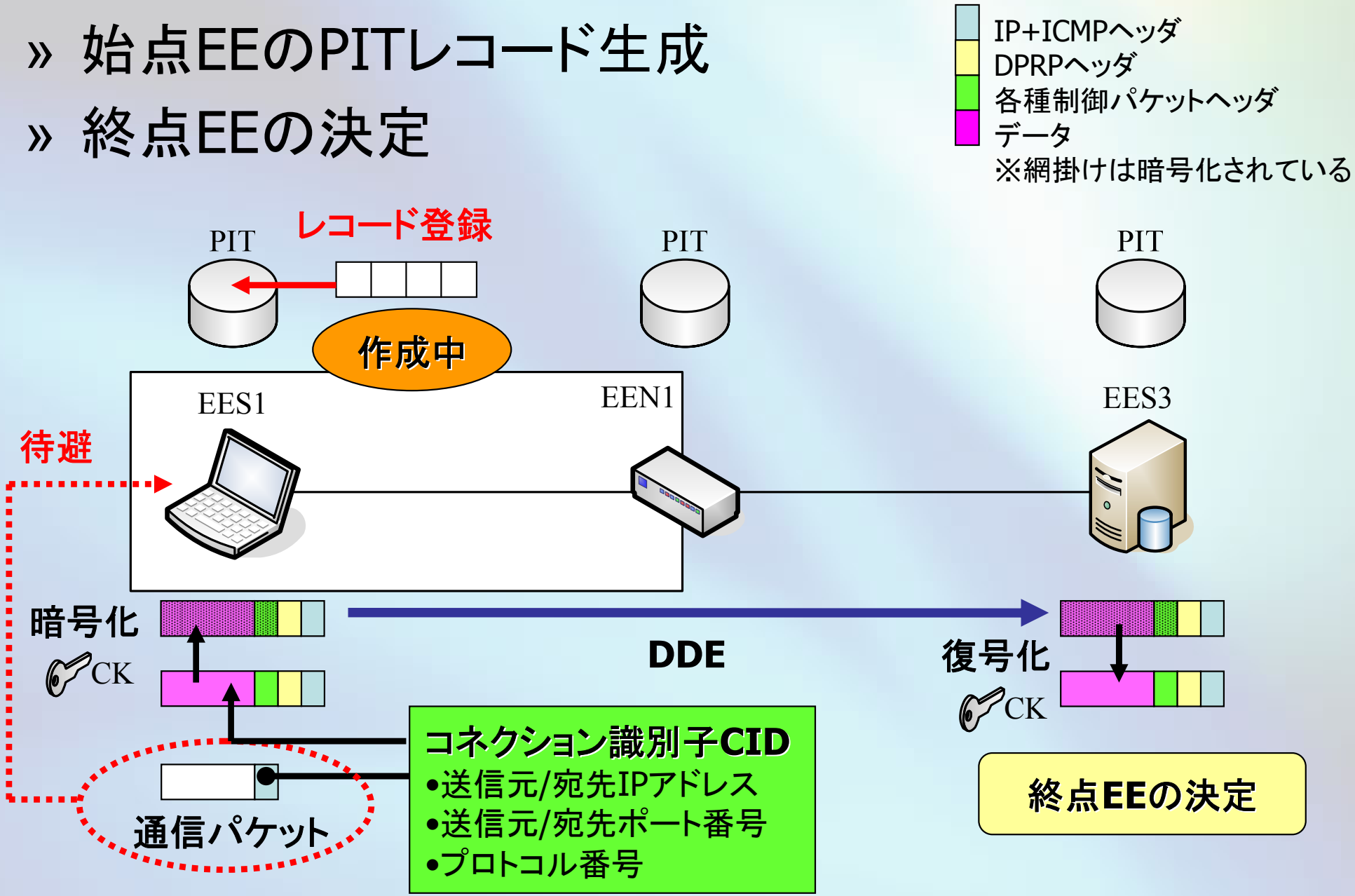


Entity	GK	Mode
EES1	1, 3	OP
EES2	2	OP
EES3	3	CL
EEN1	1	CL
EEN2	2	CL

DDE (Detect Destination End EE)

» 始点EEのPITレコード生成

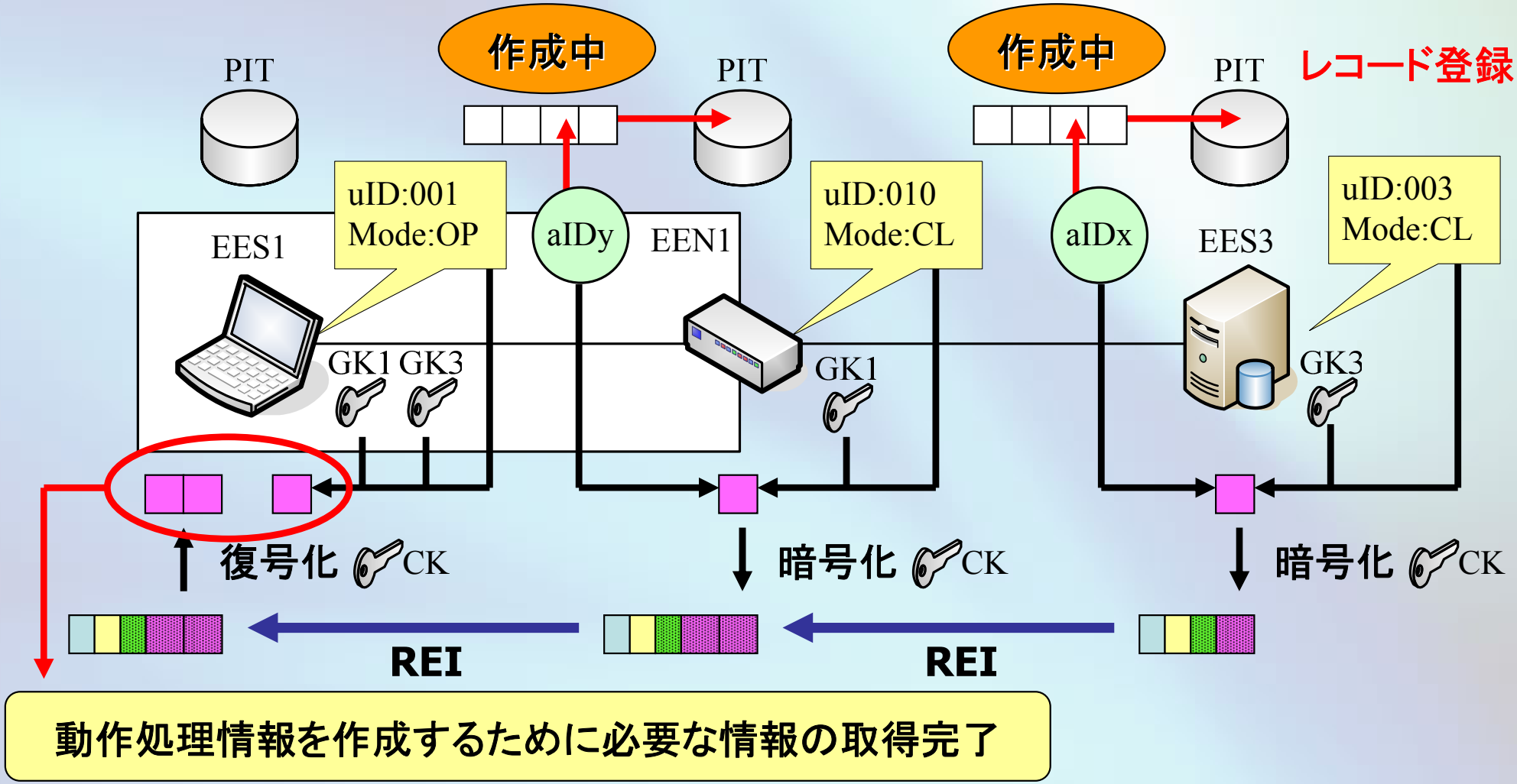
» 終点EEの決定



REI (Report EE Information)

» 各EEの設定情報，グループ鍵情報の通知

» 始点EEの決定



動作処理情報の決定

» 動作処理情報生成に必要な情報
- EE設定情報（uID，動作モード）
- グループ鍵情報（番号，バージョン）
- ネットワークの内外の関係（Edge，Out to In，In to Out）

Received Information

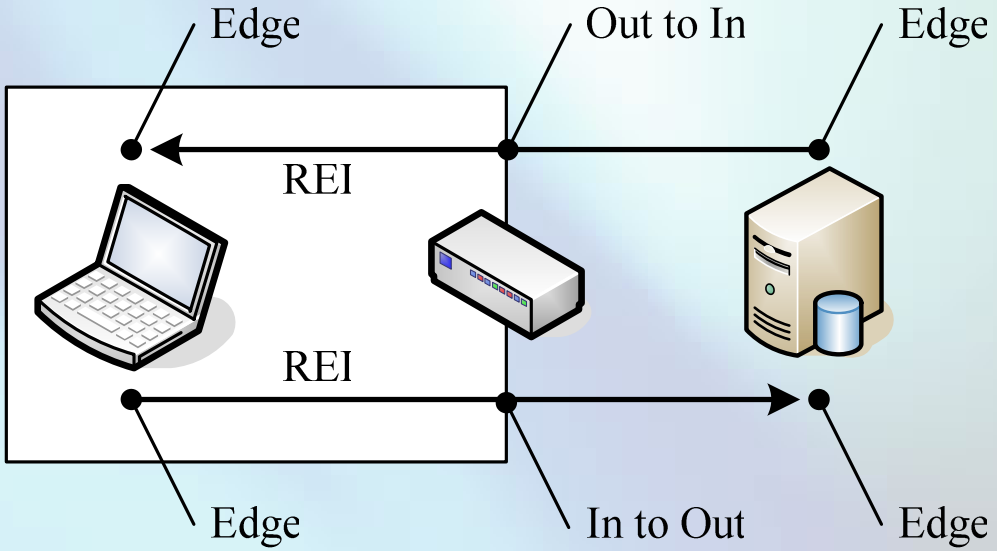
uID:003	CL	aIDx	Edge	GK3
uID:010	CL	aIDy	Out to In	GK1
uID:001	OP	—	Edge	GK1,GK3

eeInfo　　Direction

Process Information　Authentication Data

uID:001	Enc/Dec	GK3	—
uID:010	Fwd/Fwd	—	aIDy
uID:003	Dec/Enc	GK3	aIDx

Process

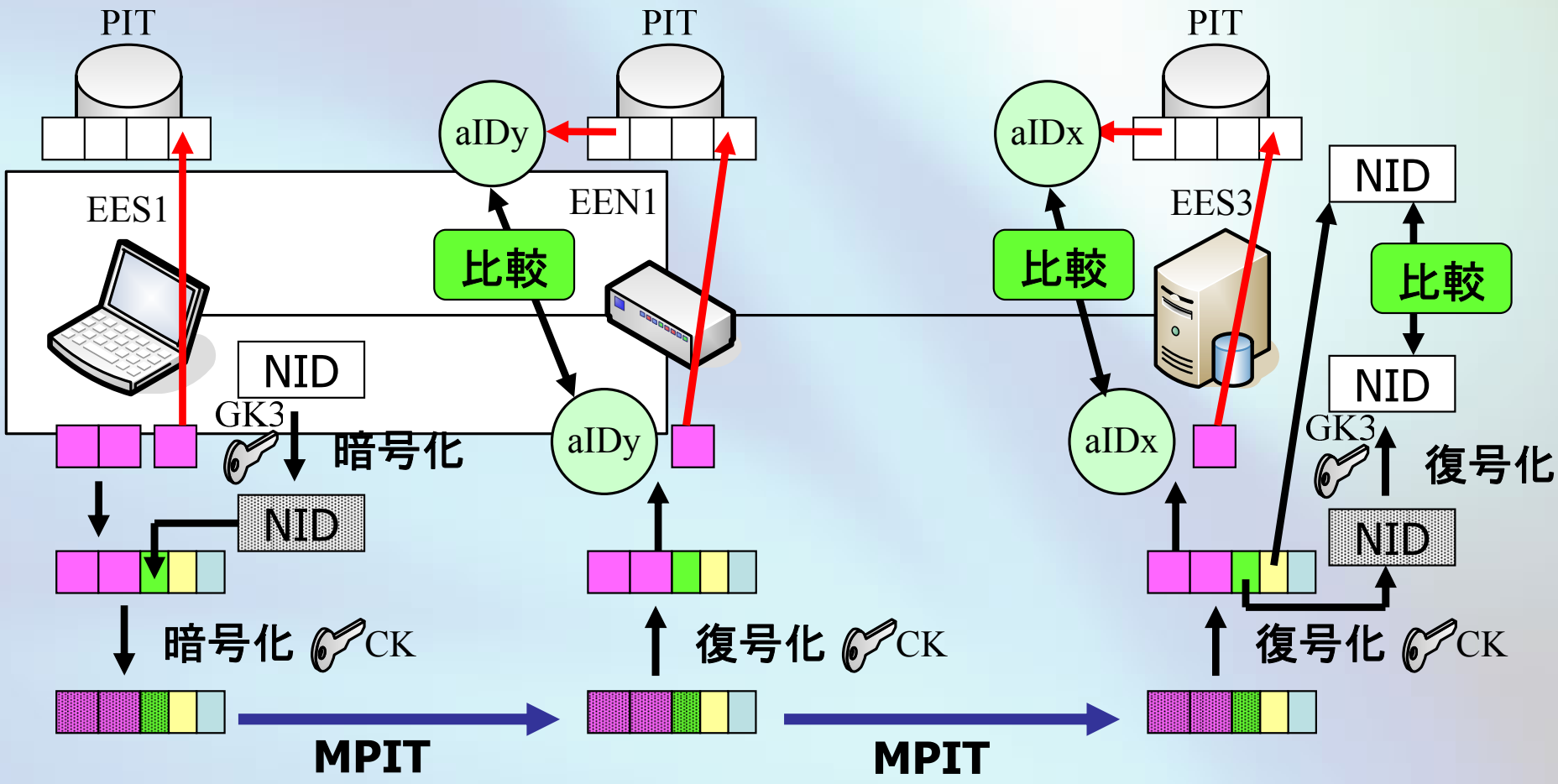


認証情報aIDは決定した情報に紐付ける

MPIT (Make Process Information Table)

» 動作処理情報の通知およびPITレコードへの登録

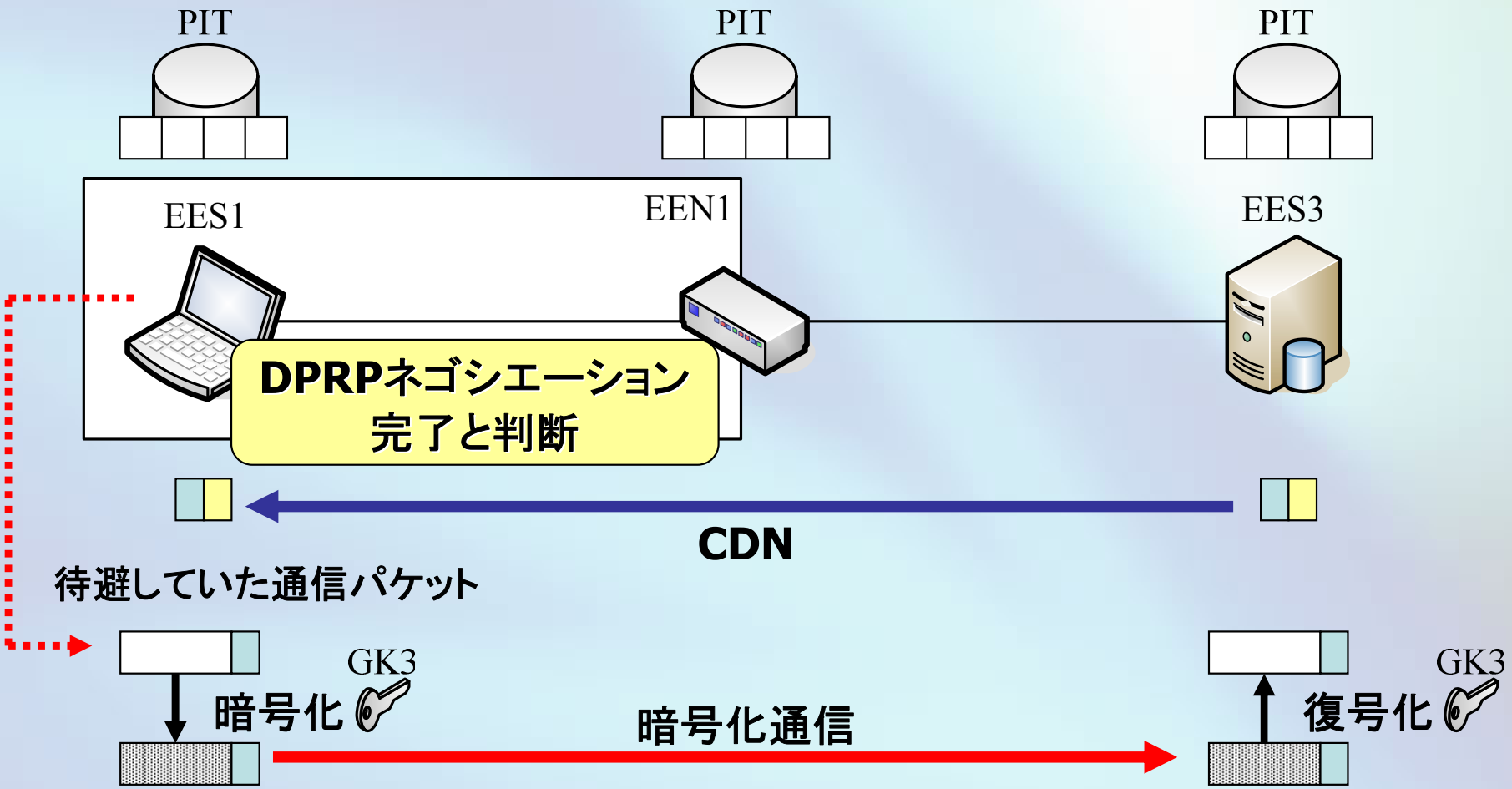
» 制御パケットの認証処理



CDN (Complete DPRP Negotiation)

» DPRPネゴシエーション完了の通知

- CDN受信後，待避していたパケットを動作処理情報に基づいて処理



安全性

» FPN環境では，PIT情報によりアクセス制御・暗号化処理を制御
→PITには信頼ある情報が格納されている保証が必要

ネゴシエーションの盗聴は？

→ 制御パケットは全て暗号化されているため盗聴不可能

ネゴシエーションの改竄は？

→ 受信時の復号処理でエラーが発生しパケット破棄

IPアドレスの偽造は？

→ PITで指定されたグループ鍵を持っていない限り安全

管理者によって予め設定されたGKしか配送されないためGKを偽造・盗難することは困難

Mobile P2P

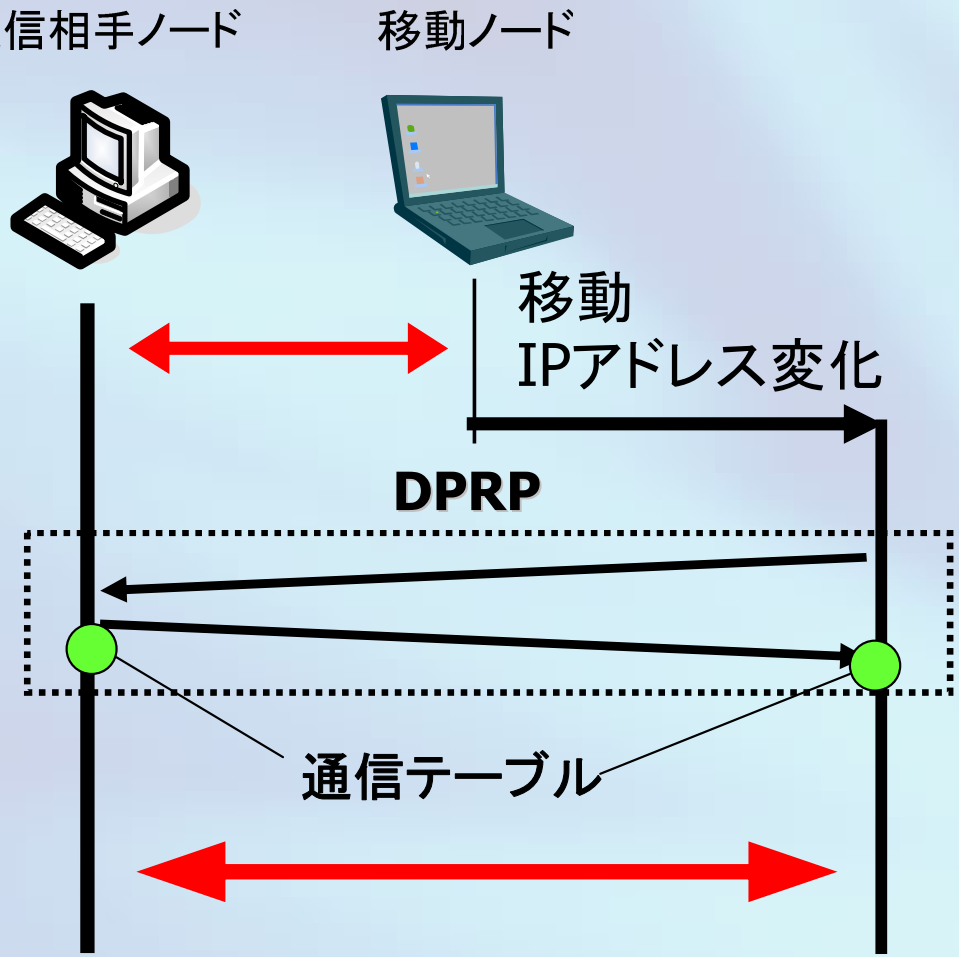
- モバイル端末がIPアドレスの変化に影響されず，常時P2P通信が可能な環境を提供
- Mobile IPなどの既存移動透過プロトコルにおける基本的な問題を解決
  - HAなどの特殊な装置を必要としない
  - 既存環境を利用
  - エンド端末間で通信を継続させる方式

初期IPアドレスの解決
DDNS（Dynamic DNS）を利用

継続IPアドレスの解決
両端末でアドレス変換を行う

Mobile P2P

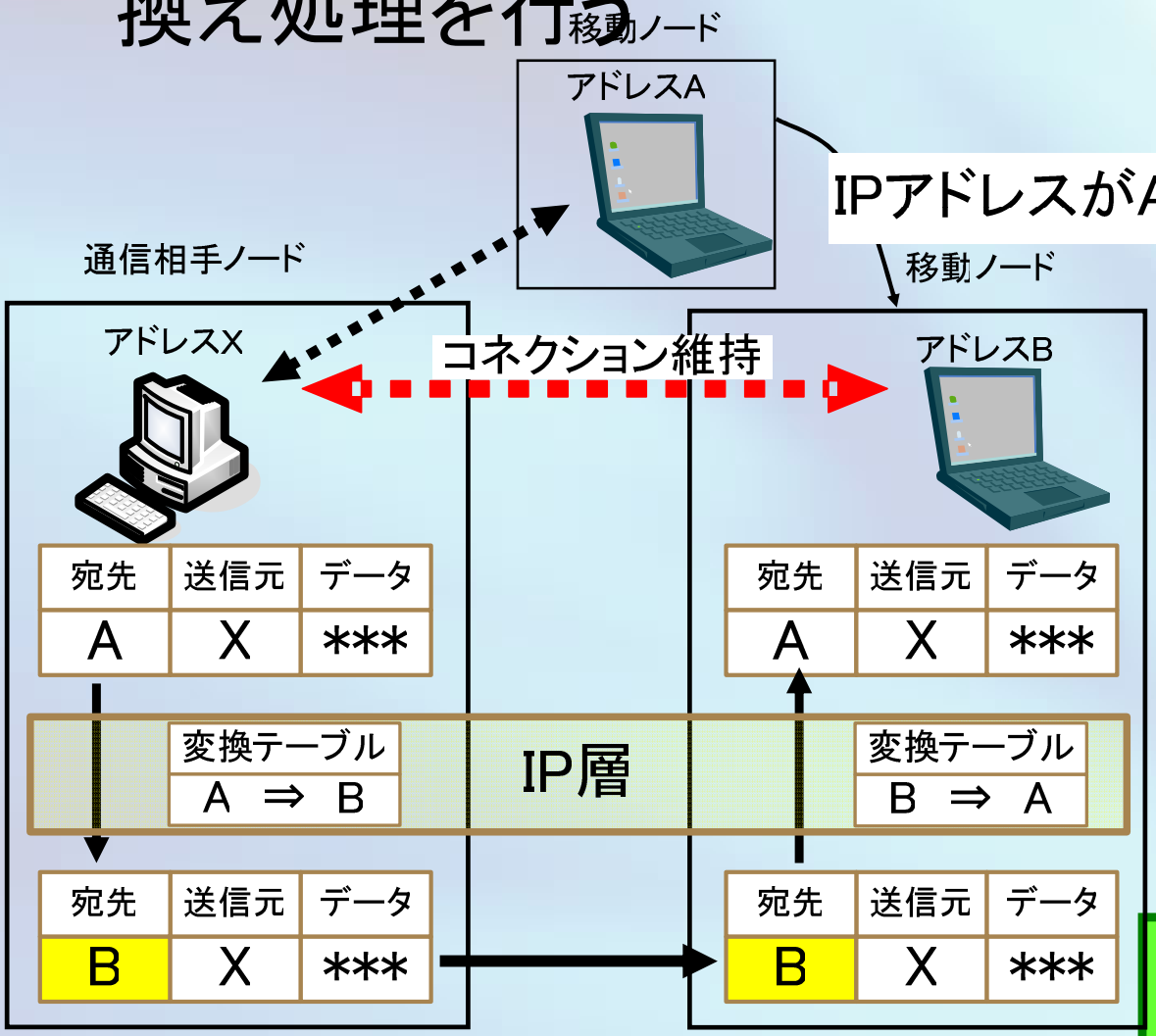
» 移動後に拡張DPRPによって端末間の認証および新IPアドレスの通知を実行



通知後には、新旧IPアドレスの関係を表す通信テーブルが両端末間で作成される

Mobile P2P

» 作成された通信テーブルを元に，IP層でアドレスの書き換え処理を行う



送信時

正しくルーティングされるように、現在端末が持つIPアドレスになるようにアドレス変換

受信時

通信開始時のアドレスの組と一致するようにアドレス変換

上位層では、IPアドレスが変化したことには気づかない