動的処理解決プロトコル DPRP の改良の検討

11300J075　鈴木秀和
渡邊研究室

1. はじめに

近年，増加傾向にあるイントラネット内部の犯罪に対するセキュリティ対策が重要視されている．既存技術の 1 つとして IPsec が考えられるが，頻繁にシステム構成が変わる環境では設定情報の変更が必要であるため，イントラネット内では利用されていない．

そこでイントラネット内のセキュリティと運用管理負荷軽減を両立したシステムを実現する FPN(Flexible Private Network)環境[1]を目指している．この環境では各端末にグループ鍵 GK を持たせた暗号装置 EE（Encryption Element）を用意し，同一の鍵を保持する EE の集合を閉域通信グループ CCGI（Closed Communication Group for Intranet）として構成する．CCGI 内の端末間の通信はこの GK で暗号化され，異なる CCGI の端末がアクセスすることや，通信内容を盗聴することが不可能となっている．そこで端末は通信相手が同一の CCGI に帰属しているかを確認する必要があり，そのネゴシエーションを行うのが DPRP（Dynamic Process Resolution Protocol）である．DPRP は通信に先立ち行われ，認証と動作処理情報テーブル PIT(Process Information Table)を動的に生成する．

本研究では DPRP の安全性を向上させる改良を検討したので報告する．

2. 既存 DPRP における課題

CCGI を構成する EE には，クライアント端末にソフトウェアをインストールして実現するソフトウェア型暗号装置 EES，ルータに実装させて配下の端末を保護するネットワーク型暗号装置 EEN がある．企業ネットワークでは部署や役職ごとにアクセスポリシーが異なるため，図 1 のような CCGI 構成が考えられる．

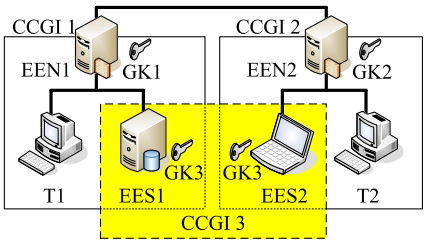


図 1　ネットワーク構成と CCGI 構成

EES1-EES2 間の通信を考えた場合，通信経路上に 3 台以上の EE が存在する縦列接続構成になっている．従来の DPRP では両終端 EE 間で End-End の事前ネゴシエーションを行っているため，中間 EE となる各 EEN を無条件に中継させていた[2]．このように制御パケットを無条件で中継させることで，EE に不正な PIT の作成や，DOS 攻撃の対象となる懸念がある．

3. 制御パケット検証機能の追加

このような課題を解決するために，中間 EE において制御パケットの検証機能を追加した．図 2 のように EEN に配下のサブネットに存在する EE の IP アドレスとグループ鍵情報を記したテーブル ECT(EE Check Table)を用意する．この情報は EES が電源投入時に REI(Report EE Information)パケットによって伝えられる．EEN は REI が MS によって証明された EE からのものであるということを確実に認証するため，安全に ECT を作成することが可能である．

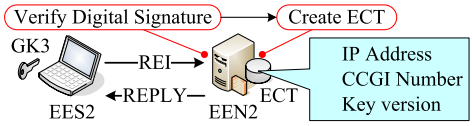


図 2　ECT 生成方法

DPRP ネゴシエーションは End-End では GK3 による認証を行い，中間 EE では ECT によって制御パケットの検証を行う．検証は制御パケットの IP アドレスとグループ鍵情報を ECT と比較して行い，一致するデータが存在すれば制御パケットの中継を許可する．

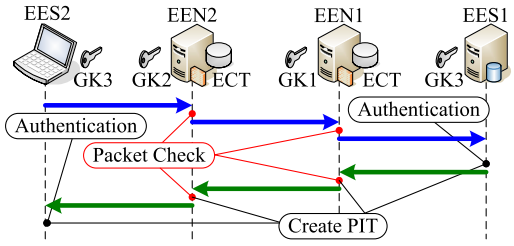


図 3　DPRP ネゴシエーション

4. 評価

中間 EE において制御パケットの検証機能を追加したことにより，確実に制御パケットの認証を行うことが可能になり，安全に PIT を作成することが可能になった．また各 EE で認証または検証することで不正なパケットを早期段階で発見し破棄することが可能になり，セキュリティの向上が見込める．

5. むすび

既存の DPRP のセキュリティ向上を図るために改良を行った．今後は DPRP の開発を進め FreeBSD カーネルの IP 層に実装して，性能評価を行う予定である．

参考文献

[1] http://www-is.meijo-u.ac.jp/~watanabe/ “研究内容”
[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，VOL.J84-D-I No.3，March 2001

動的処理解決プロトコルDPRPの改良の検討

Researches on Improvement of DPRP

名城大学理工学部情報科学科
渡邊研究室
11300J075　鈴木　秀和

研究背景

- 企業ネットワークのセキュリティ対策
  - » インターネット経由による外部からの不正アクセス
  - » イントラネット内部のユーザによる内部犯罪

内部犯罪の増加

- 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

} 既存技術　IPsec，SOCKS，SSL…

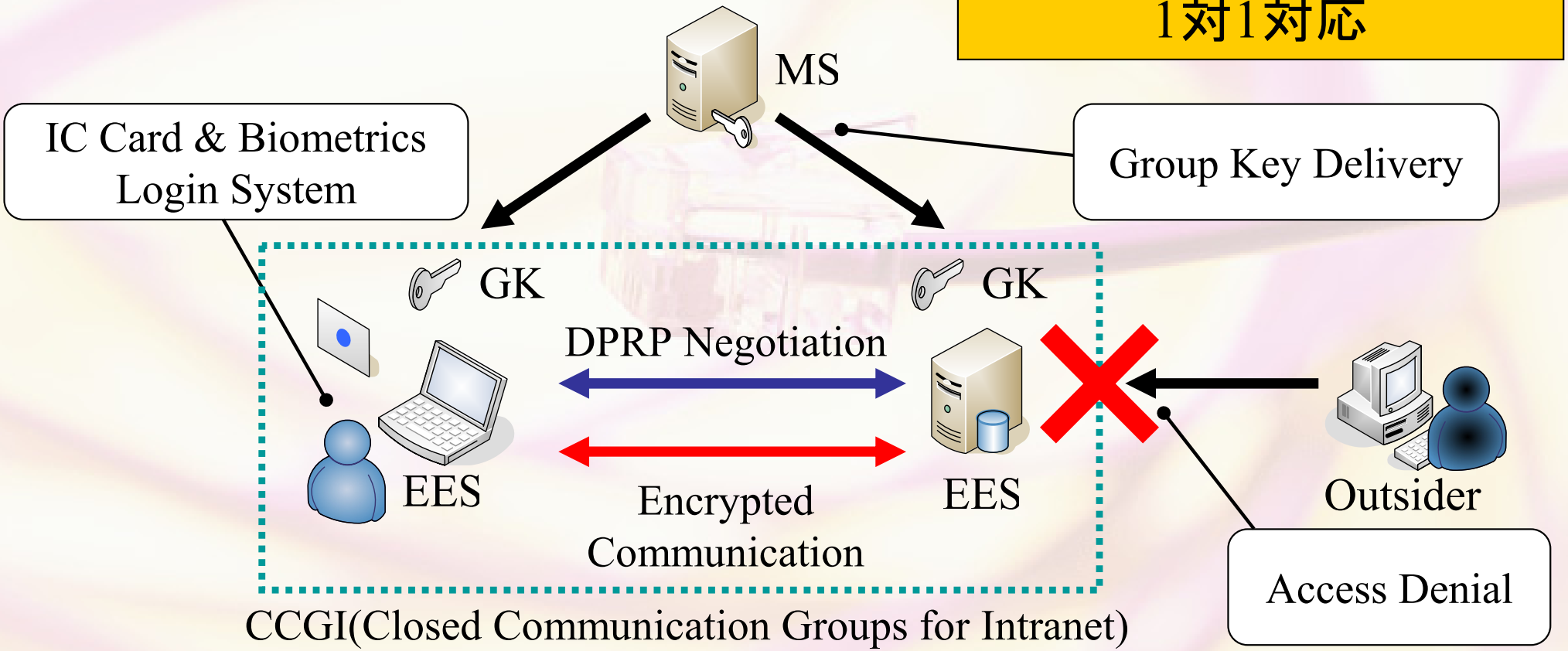
- ユーザの移動による設定情報の変更
- 暗号装置の位置関係
- NA(P)T環境における利用の問題

イントラネット特有の環境に対応した
柔軟なセキュリティ技術がない

研究背景

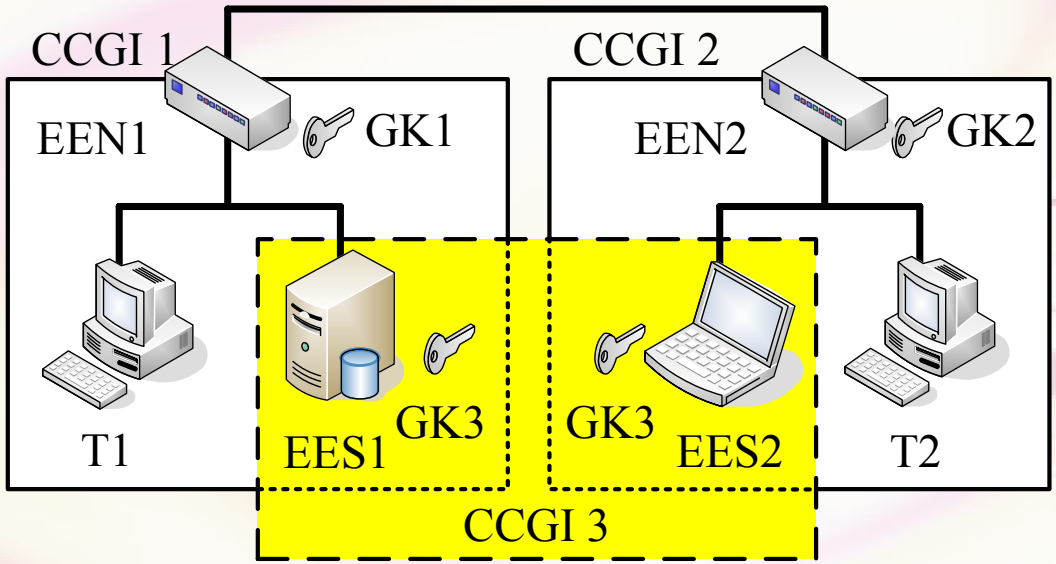
- FPN（Flexible Private Network）環境の実現
  - セキュリティと管理負荷軽減の両立が可能なシステム
  - 閉域通信グループCCGIの構築
  - DPRPによるアクセス許可と自動設定
  - ユーザの物理的位置透過性の保証

グループ鍵GKとCCGIが1対1対応

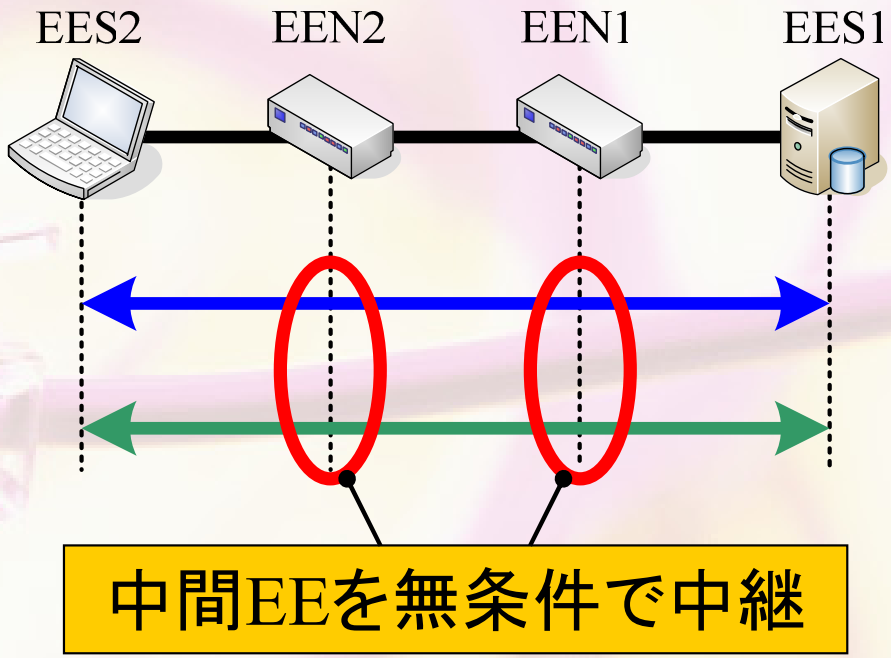


動的処理解決プロトコルDPRPの概要と課題

- DPRP（Dynamic Process Resolution Protocol）
  - 通信に先立ち実行
  - 相手認証，動作処理情報テーブルPIT（Process Information Table）の生成



EES：ソフトウェア型暗号装置
EEN：ネットワーク型暗号装置
Tx：通常の端末



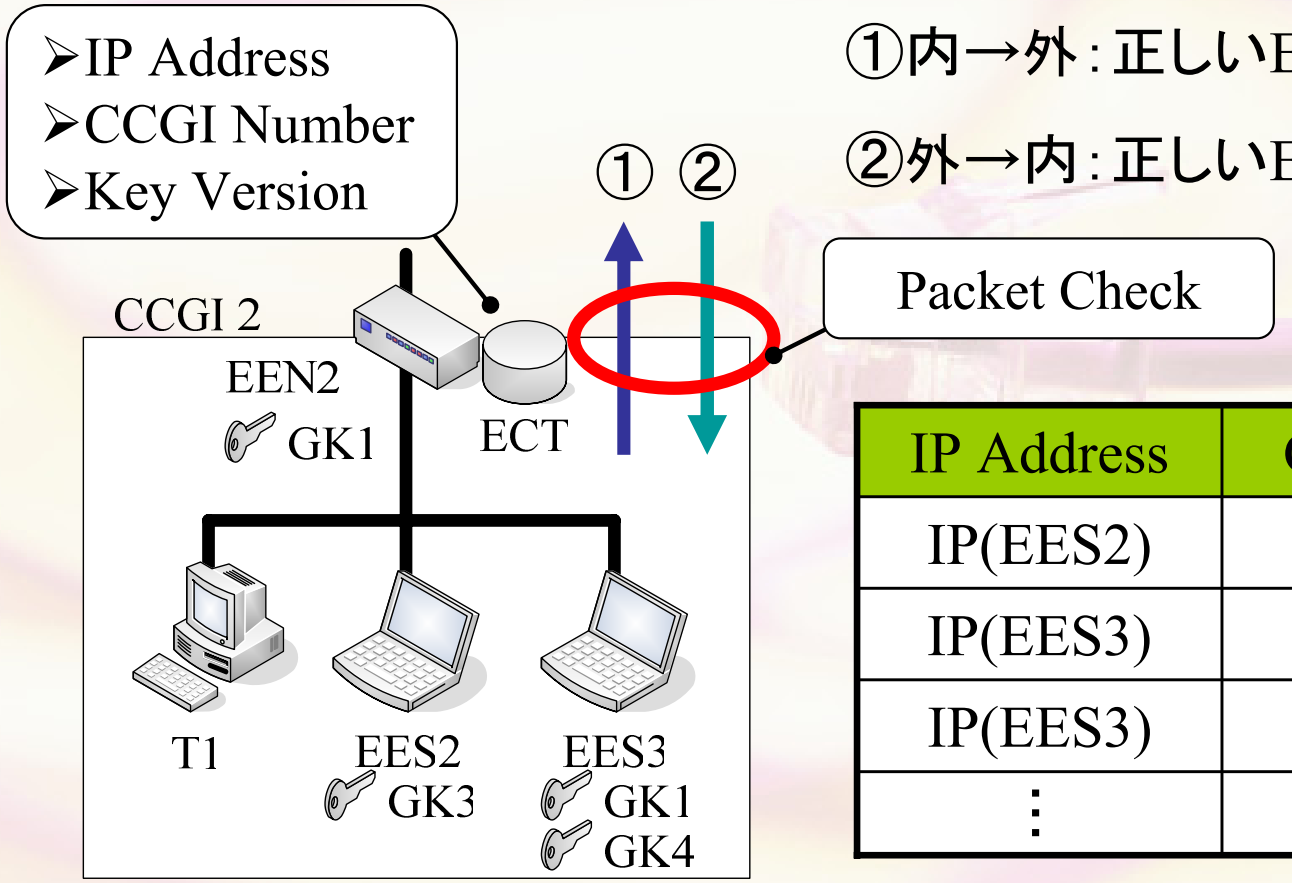
不正なPITの生成

DoS攻撃の対象

DPRP改良方式の概要

- 中間EEにおける制御パケットチェック機能の追加
  - EENにECT（EE Check Table）を保持させる

配下のサブネットに存在するEE情報の把握



①内→外：正しいEEから送信されているか？

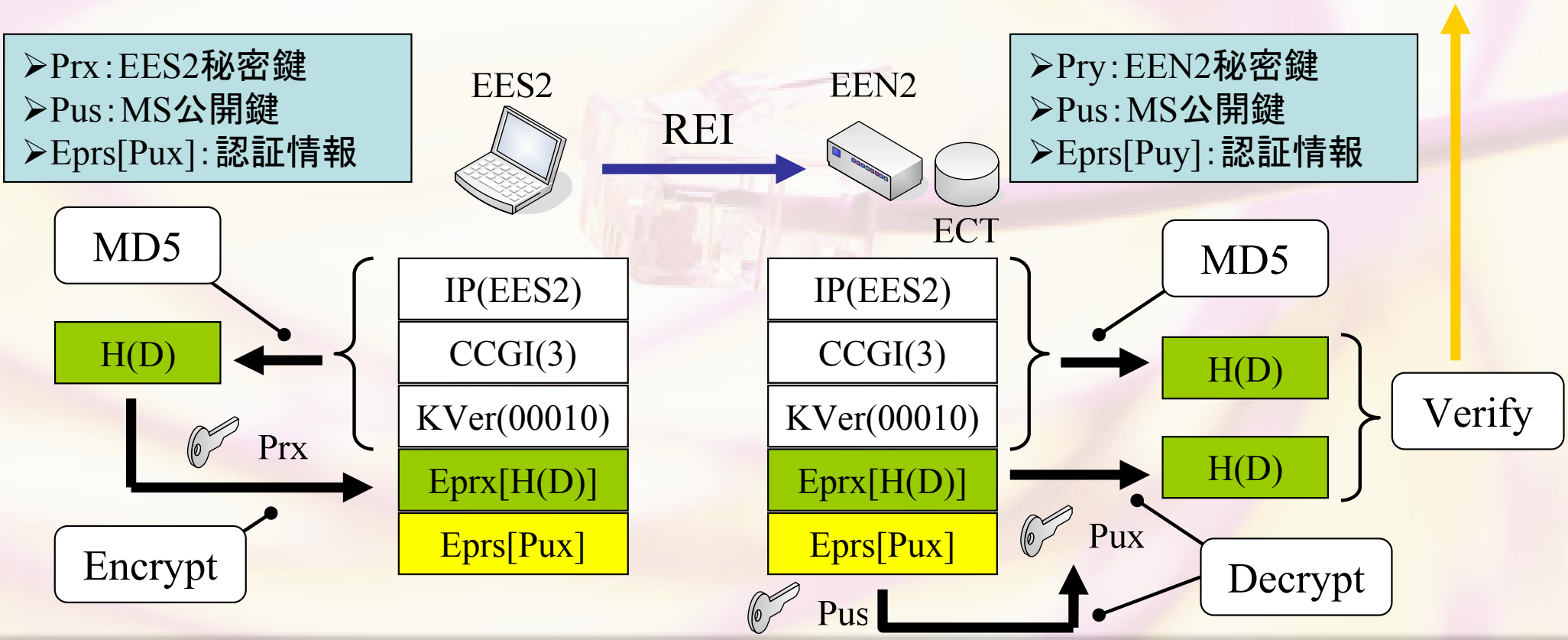
②外→内：正しいEEへ送信されているか？

IP Address	CCGI No.	Key Version
IP(EES2)	3	00010
IP(EES3)	1	00020
IP(EES3)	4	00060
⋮	⋮	⋮

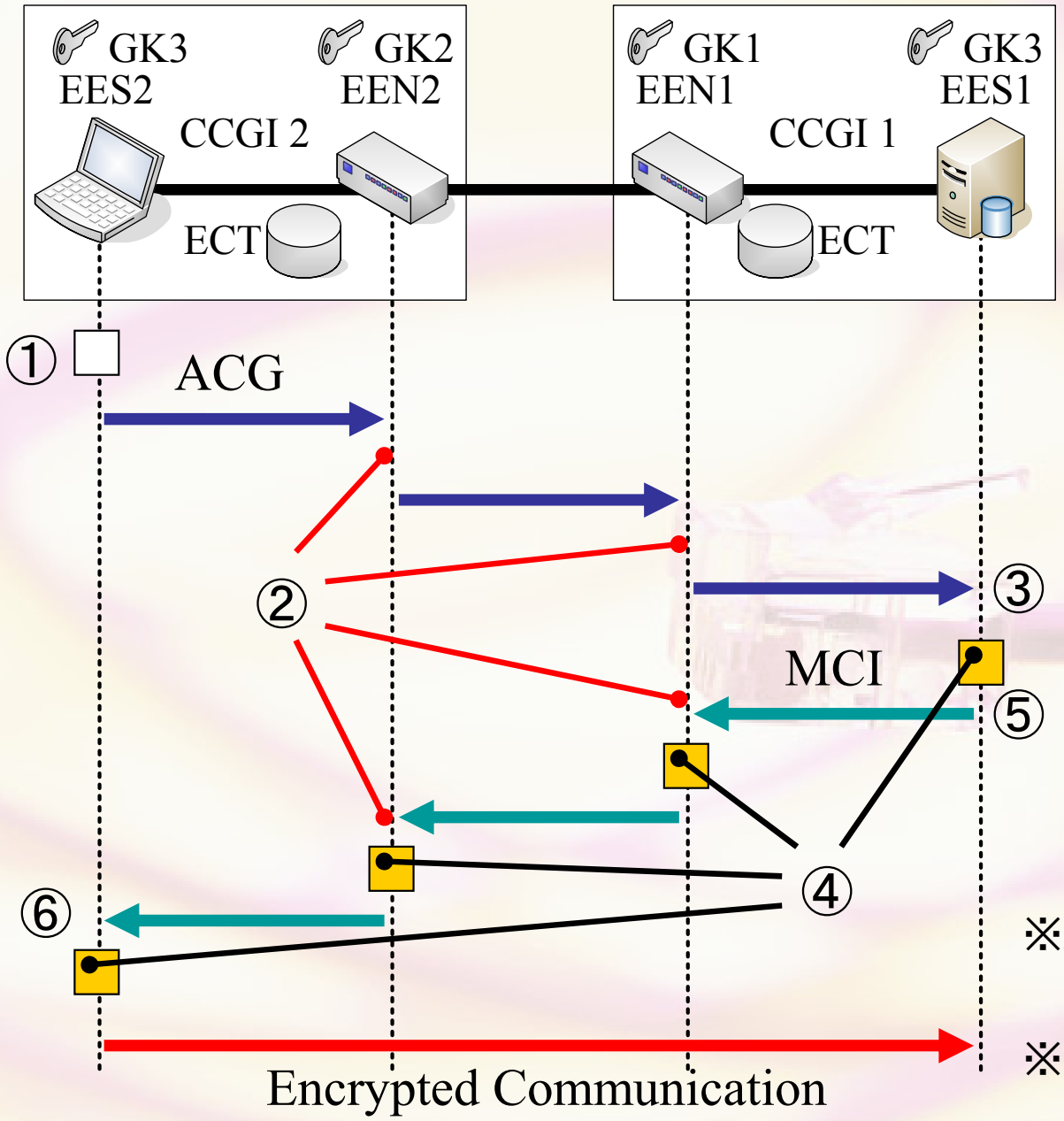
ECTデータ生成方法

- REI（Report EE Information）[ICMP]
  - EES電源投入時またはネットワーク接続時に送信
  - 自端末のEE情報をEENへ伝える
  - ディジタル署名検証の利用

MSによって証明された
EEからのパケットと認証



DPRPネゴシエーション



EES2→EES1への通信

① PITを検索してデータが存在しない場合，ACGを送信

② ECTによるパケットチェック

③ グループ鍵による認証処理後，動作処理情報を決定

④ 決定した情報に基づいてPIT生成

⑤ MCI送信

⑥ グループ鍵による認証処理

※ACG
Authentication Communication Groups

※MCI
Make CCGI Information

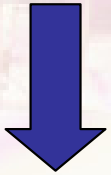
評価

- 中間EEにおいてMSに証明されたEEから送信された制御パケットであるか検証可能

✓ 確実に制御パケットの認証処理が可能

✓ 安全に動作処理情報テーブルPITの作成が可能

✓ 不正パケットの早期発見による破棄が可能



セキュリティの向上が見込める

まとめと今後の課題

- DPRPの安全性を向上させる改良の一検討
  - 従来方式に比べてセキュリティの向上が見込める
  - 他の検討案を含めて精査し，DPRPの仕様を固める
  - より柔軟なネットワーク構成に対応するための更なる改良
- 現在開発中の動作テストプログラムの完成
  - 各検討案のDPRPネゴシエーションテスト
  - 性能評価の実施（一部分は測定済み）
- OSへの組み込み
  - FreeBSDのIP層への組み込み
  - Linuxへの移植
- FPN環境の実現

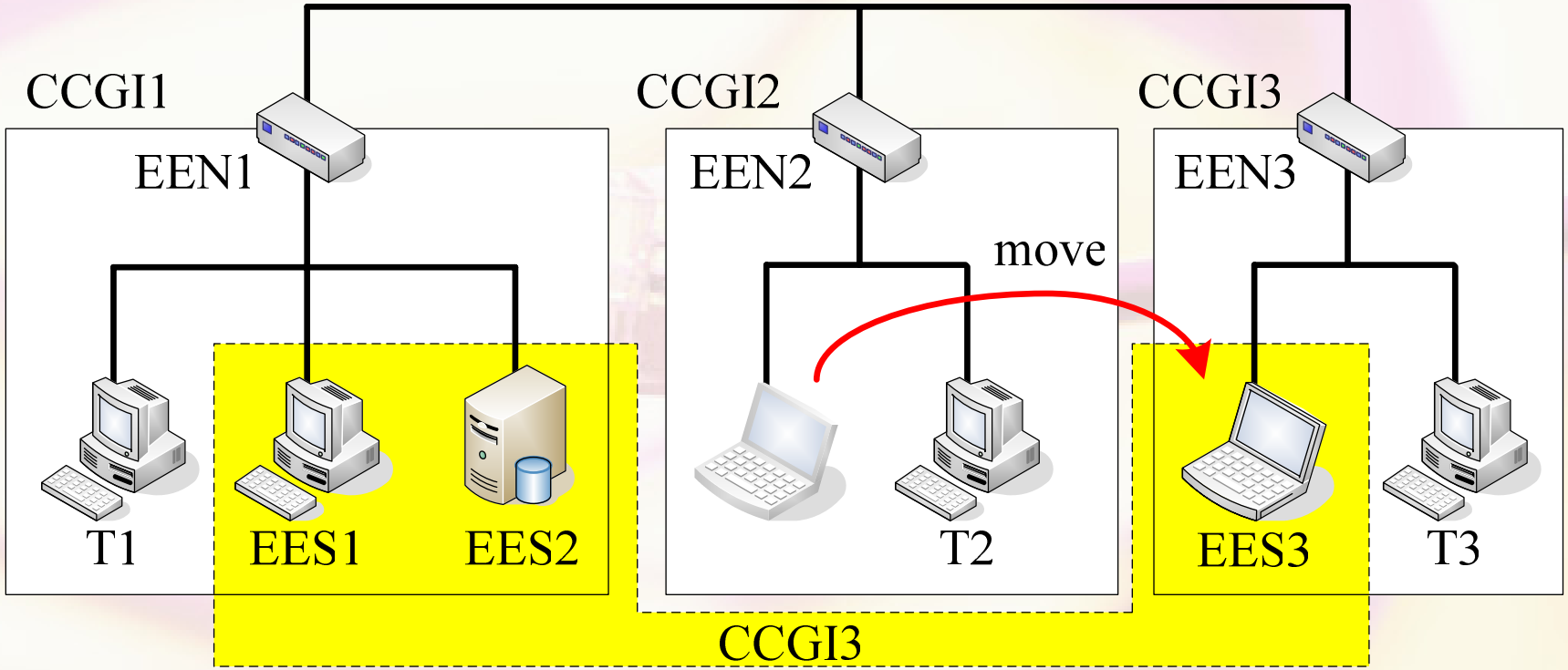
動的処理解決プロトコルDPRPの改良の検討

Researches on Improvement of DPRP

終了

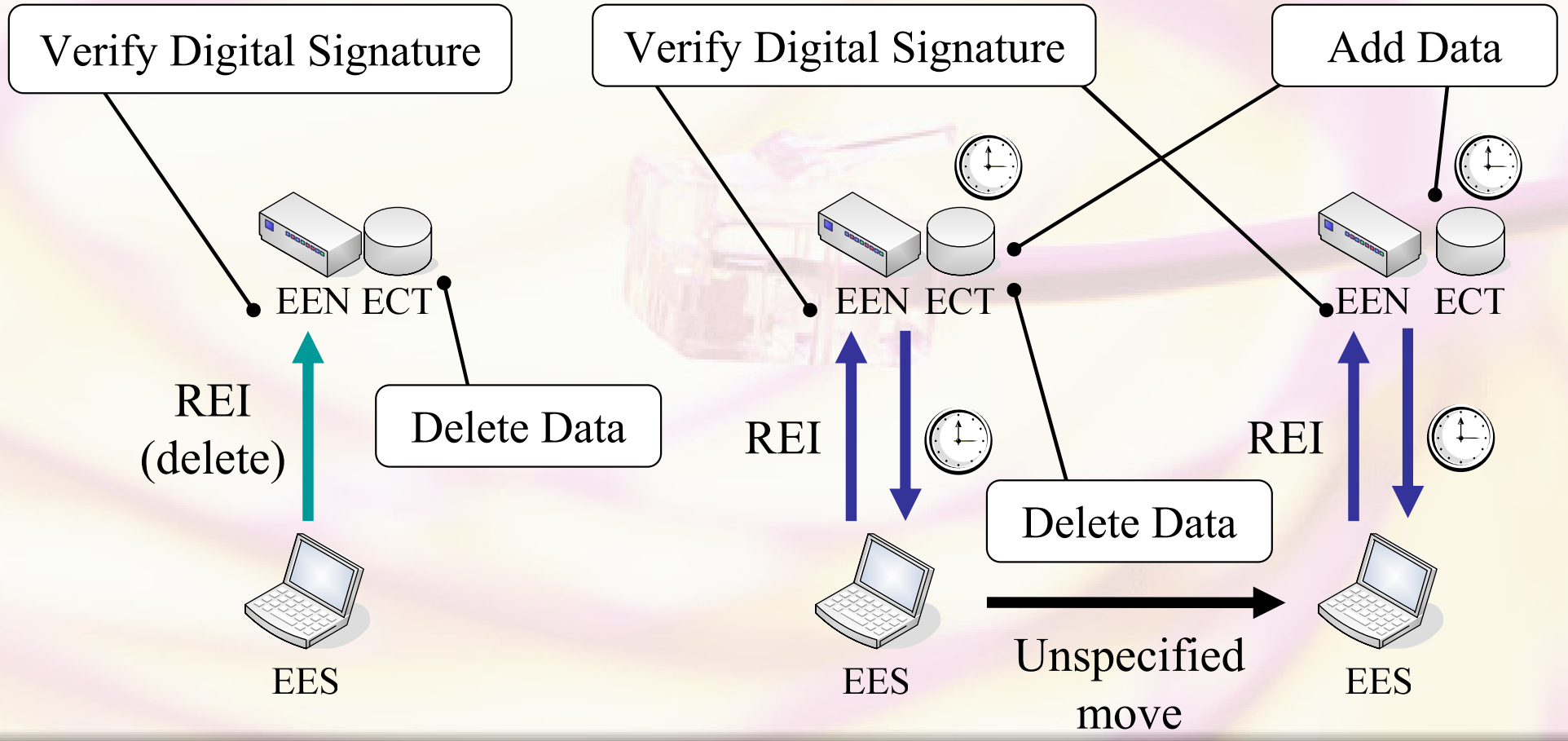
物理的位置透過性(ロケーションフリー)の保証

- CCGI定義情報に基づくグルーピングの定義
  - » ユーザの移動に対してもCCGI情報設定を保持
  - » 出張や部署間移動の場合に利用者・管理者の負荷は発生しない



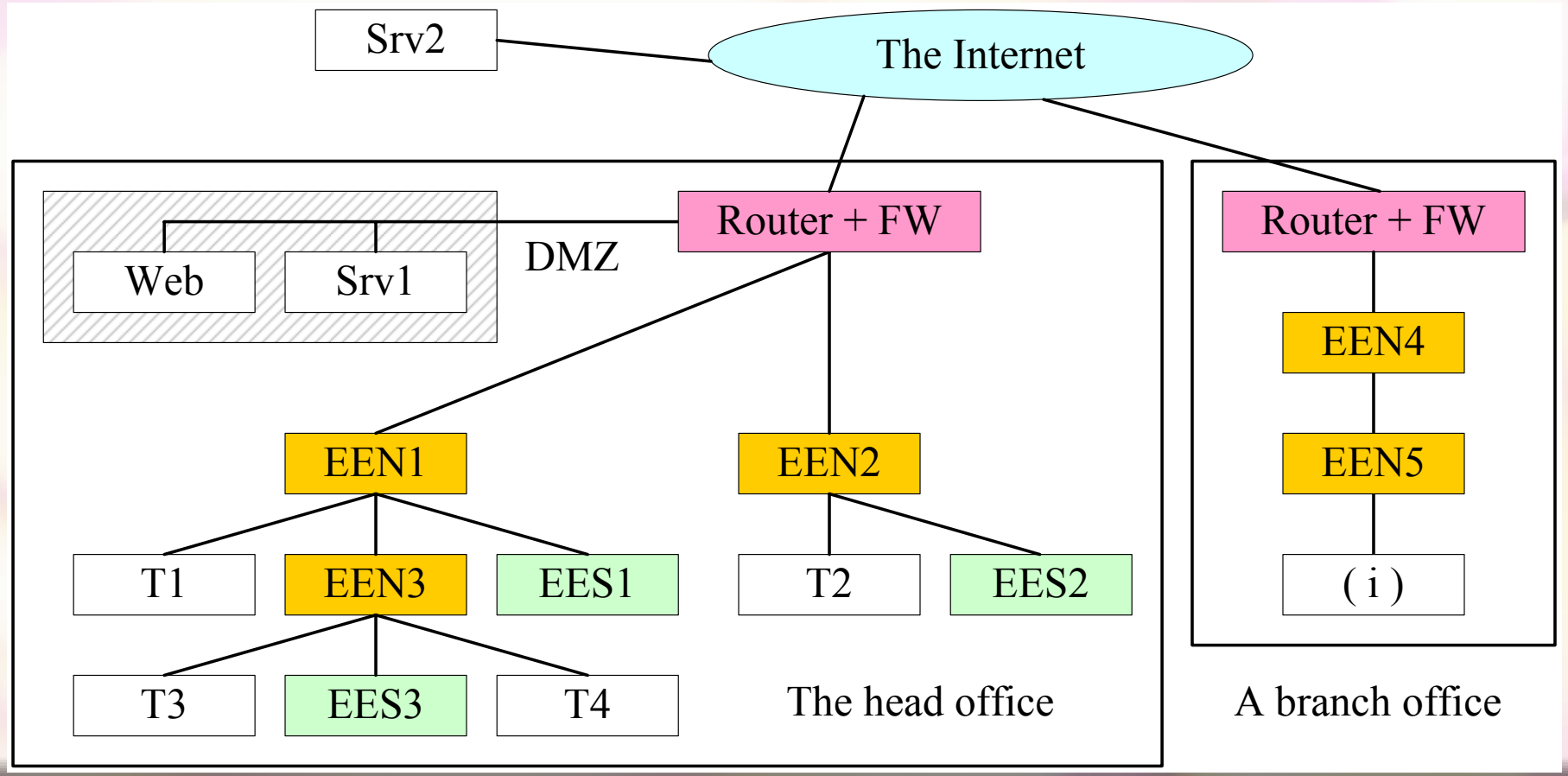
端末の移動を考慮したECTデータ削除方法

- 不要なデータは削除
  - » EES電源切断時または明示的なネットワーク離脱時
  - » ECT生存時間の超過による自動削除



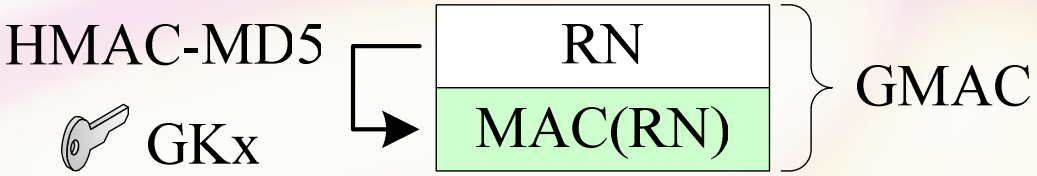
REI送信先

- REIブロードキャストによる隣接EEN宛
- EEN縦列接続の最上位に位置するEEN宛
- DMZ内に設置するサーバまたはルータ，FW
- インターネット上に設置したサーバ宛

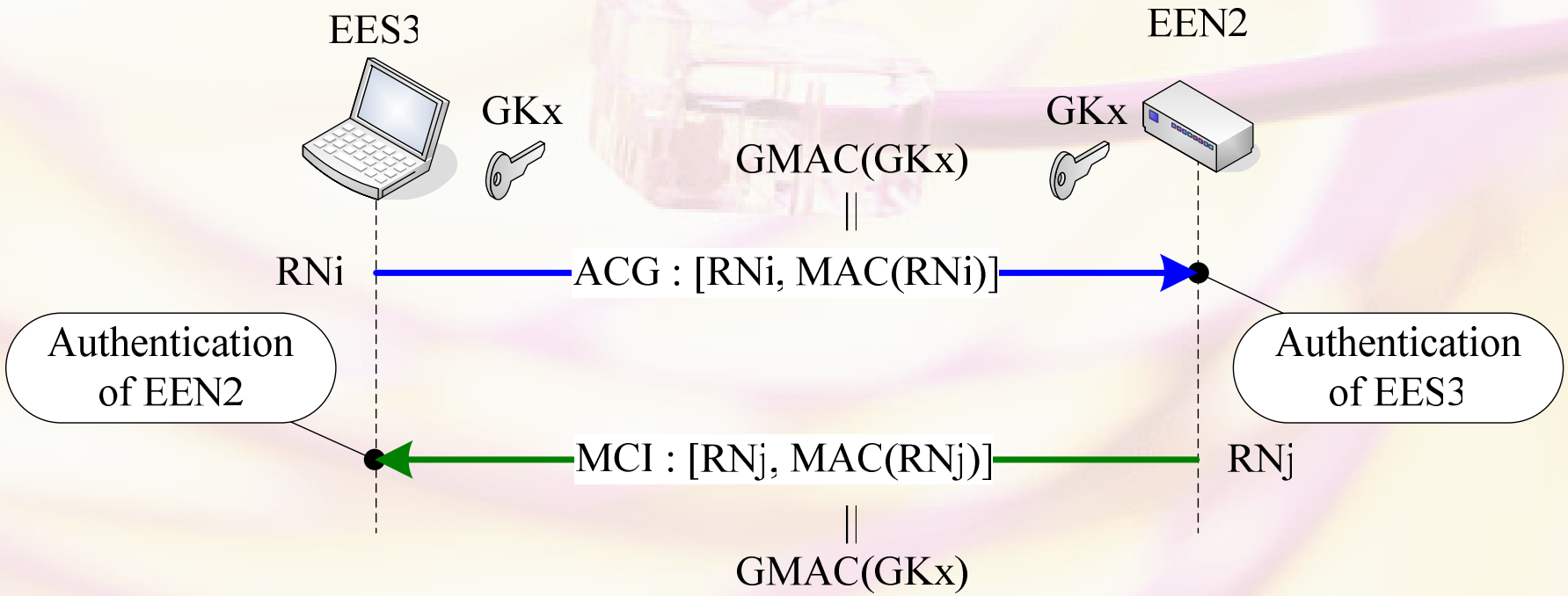


GMACによるグループ鍵認証

- GMAC（Group Message Authentication Code）
  - 乱数にグループ鍵を加えてMD5でダイジェストをとったMAC
  - 鍵の影響を強化したMACの改良版



- ✓ 改竄の検出
- ✓ 送信元認証
- ✓ CCGI同一性検証



動作処理情報テーブルPIT（Process Information Table）

➢ 通信パケットの処理内容を定めた情報

sIP	sPrt	dIP	dPrt	No	Ver	Proc	CF
EES2	100	EES3	150	3	200	Enc	0
EES3	150	EES2	100	3	200	Dec	0

- ✓ sIP：送信元IPアドレス　sPrt：送信元ポート番号
- ✓ dIP：宛先IPアドレス　dPrt：宛先IPアドレス
- ✓ No：CCGI番号　Ver：鍵バージョン
- ✓ Proc：動作処理情報　CF：カウンタフィールド
  - Enc：暗号化　Dec：復号化
  - Fwd：転送　Dst：破棄
  - Cre：作成中

タイマーによる
CFチェック
↓
規定値以下のデータ
削除

DPRPの実装

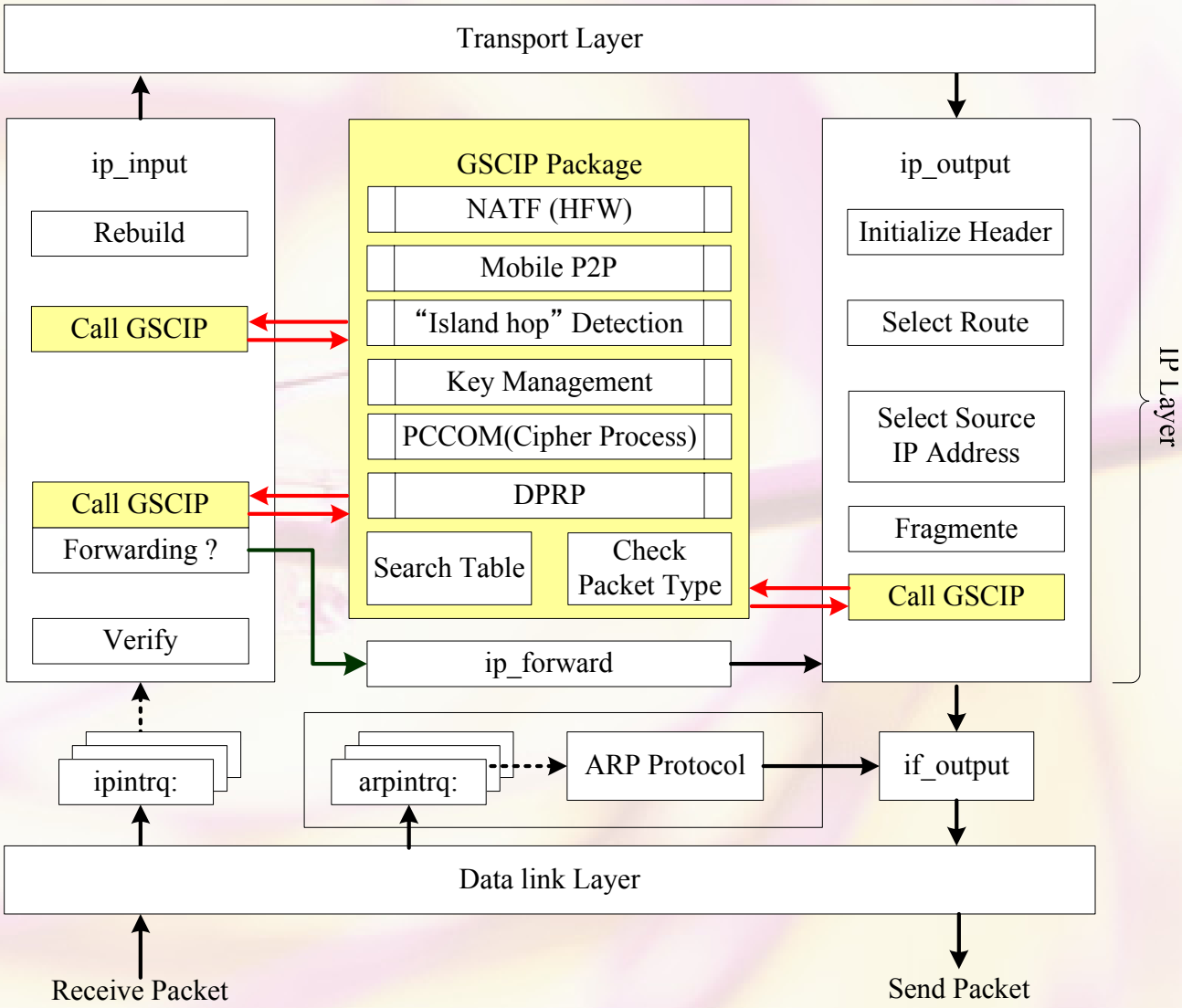
➢ GSCIP（Grouped Secure Communication for IP）

» FPNを実現するための独自のネットワークセキュリティアーキテクチャ

» 5つのプロトコル群と2つの機能から構成

- DPRP
- PCCOM
- SPAC
- Mobile P2P
- NATF

- Key Management
- “Island hop” Detection



評価プログラムによる性能評価

	PC1	PC2
CPU	Pentium4 2.4GHz	PentiumII 233MHz
RAM	1024MB	196MB
OS	FreeBSD 5.1-Release	FreeBSD 5.2-Release

- 実験条件
  - GMAC生成、ACG生成を10,000回繰り返し、1回当たりの処理時間の導出
  - 上記処理を10回試行した場合の平均値を算出
  - 端末にグループ鍵を3つ保持（ACG生成の場合）

	PC1 [μ sec]	PC2 [μ sec]
GMAC生成	12.185	90.547
ACG生成	39.609	288.203
グループ鍵認証	9.219	63.984

今回検討した4案の機能評価

	従来方式	検討案1	検討案2	検討案3	改良方式
中間EEにおけるパケットの中継処理	無条件通過	グループ鍵認証	ディジタル署名検証	MAC認証	ECT検証
DPRPネゴシエーションの処理時間	◎	△	×	△	○
シーケンス数	2 往復	1.5 往復	1 往復	1 往復	1 往復
CCGI管理負荷	○	×	○	△	○
EEに対する追加設定	―	•グループ鍵（複数）	•鍵配送時に使用する公開鍵情報	•共通秘密鍵	•鍵配送時に使用する公開鍵情報 •ECT
End-End認証	暗号化乱数の交換	GMAC認証	GMAC認証	GMAC認証	GMAC認証
安全性の向上	―	△	◎	○	◎