# 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

Researches on Dynamic Process Resolution Protocol in Closed Communication Group for Intranet

鈴木 秀和 Hidekazu Suzuki　渡邊 晃 Akira Watanabe （名城大学）

## 1. はじめに

イントラネット内に業務に応じた部門単位または個人単位の閉域通信グループ（CCGI；Closed Communication Group for Intranet）を構築する研究が行われている．その一手段として柔軟なネットワーク構成に対応でき，ユーザの移動性を確保できる動的処理解決プロトコル（DPRP；Dynamic Process Resolution Protocol）が提案されている[1]．　本研究では，DPRP の類似技術として IPsec との比較検討を行い，さらに DPRP をより安全性を高めるための改良を行ったので報告する．

## 2. IPsec と DPRP の比較

IPsec，DPRP とも通信に先立ち相手認証のためのネゴシエーションを行うが，IPsec では暗号装置（SG や IPsec ホスト）が必ず対で存在していなければならない．例えば図 1 のように通信経路上に暗号装置（EE）が 3 台以上存在する多段構成ネットワークの実現が困難である．それに対し，DPRP は通信経路上の全ての EE が認証を含む情報交換を行うため，多段構成に対応できるグルーピング，認証処理が可能である．

ユーザが移動した場合，IPsec では暗号装置の位置関係が変わるので，暗号装置の動作を規定する動作処理情報の再生成とダウンロードが必要であり，大きな管理負荷が発生する．これに対し DPRP では EE が通信経路上の位置を自律的に学習し，動作処理情報を自動生成することができる．このため，システム構成変更に伴う管理負荷が極めて少なくなり，基本的にどこに移動してもこれまでのグルーピングの関係を維持することができる（図 2）．

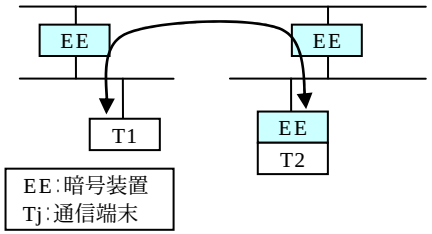



図 1　ネットワーク多段構成

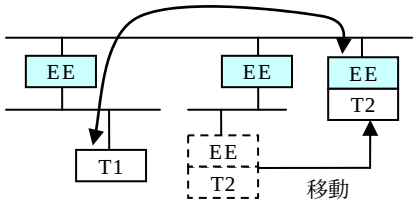



図 2　物理的位置透過性の保証

## 3. DPRP の改良

EE には同一の CCGI に帰属する通信端末との暗号通信だけが可能な閉域モードと，暗号鍵を持たない通信端末とは平文で通信を行うことができる開放モードという 2 つの動作モードがある．閉域モードは配下の端末を確実に保護するという目的がある．しかし従来の DPRP では DPRP 制御パケットが閉域モードの EE を通過してしまうという課題がある．

そこでこの課題を改善するために，終端 EE に通信経路上に存在する閉域モードの EE が保持する暗号鍵を全て保持させることとし，DPRP パケットが EE に到達するたびに上記暗号鍵を使用した認証を行うように改良した．グルーピングの関係が図 3 の場合の EE の認証処理，動作処理情報の自動生成の過程を図 4 に示す．CN 番号が同一な装置の集まりが閉域通信グループである．

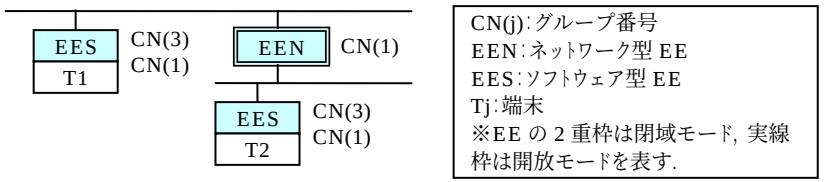



図 3　グルーピング適用例

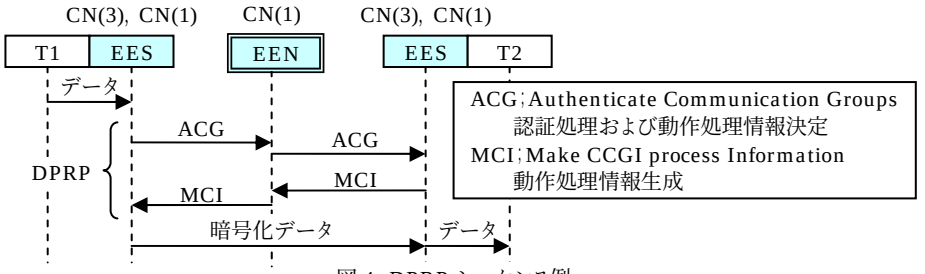



図 4　DPRP シーケンス例

DPRP が開始されると ACG パケットが送信される．このパケットは暗号鍵を使った認証処理を行い，宛先終端 EE に到達することで動作処理情報を決定することができる．決定した動作処理情報を基に MCI パケットを送り返す．各 EE がこの MCI パケットを受信することで，動作処理情報を自動的に生成する．以後，この情報に基づいて端末間で暗号通信が行われる．

この方式を採用することで，DPRP がより安全性の高いものとなり，従来の物理的位置透過性はこれまで通り実現できる．

## 4. むすび

本研究ではイントラネット内における閉域通信グループを構築する DPRP の利点と DPRP の改良について検討を行った．今後は DPRP を実現するためにモジュールの構築を行い，BSD 系 OS に実装して動作の確認をすると共に，既存技術である IPsec との管理負荷やオーバーヘッド等の比較を行っていく．また将来的に PDA や移動型 IP 電話などの移動端末に実装させることで，ネットワーク環境に依存することなくセキュアなネットワークを構築できるように改良を進める．

### 参考文献

[1] 渡邊，井手口，笹瀬 “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

# 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

名城大学理工学部情報科学科
鈴木　秀和　　渡邊　晃

# 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
  - » イントラネット内のユーザによる内部犯罪

- **業務に応じた部門単位、個人単位の閉域通信グループを構築**
  - » SSL
  - » SOCKS

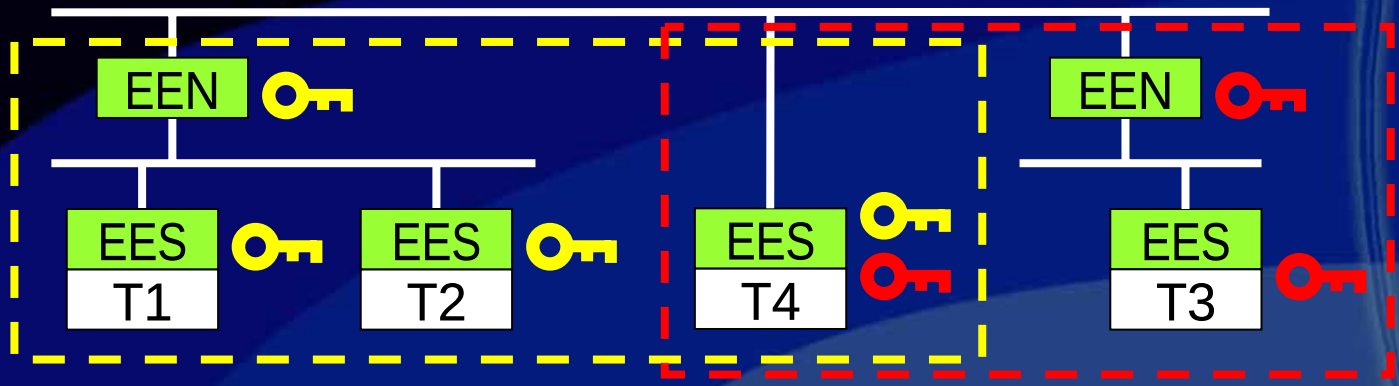
  トランスポート層（セション層含む）

  - » IPsec
  - » DPRP

  ネットワーク層

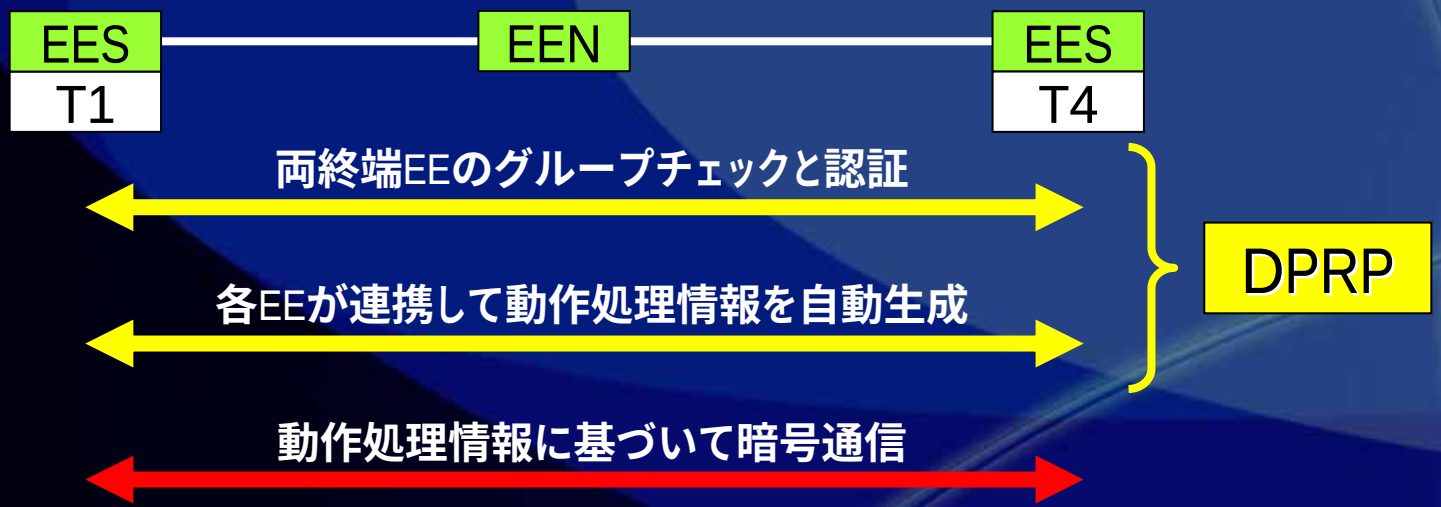
**IPsecとDPRPの比較検討**
**DPRPの安全性向上のための改良**

# 動的処理解決プロトコルDPRPの動作概要




※EEN：ネットワーク型暗号装置　EES：ソフトウェア型暗号装置

**通信グループと暗号鍵を　1対1　で対応**



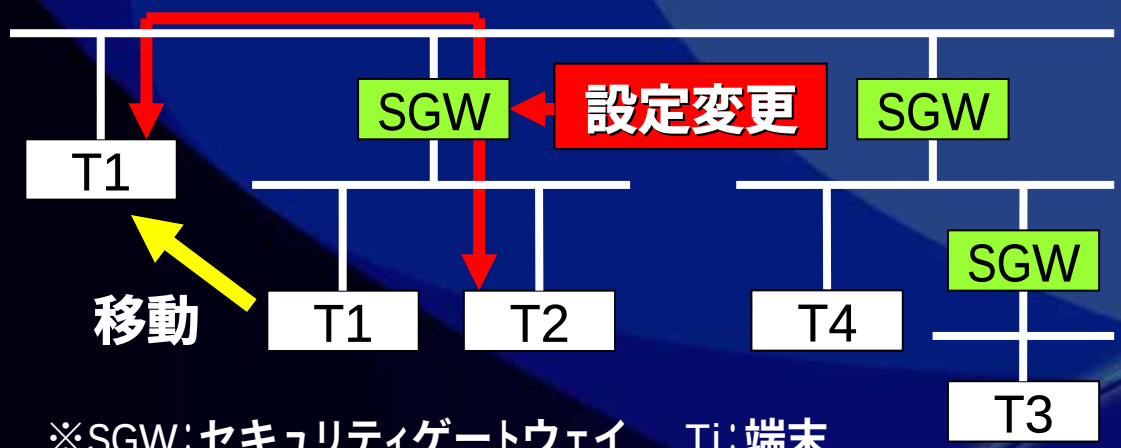
# IPsecでグループ構築した場合の問題点

- 暗号装置が通常対で存在しなければならない
  複雑な設定をしなければならない

**多段構成ネットワークにおけるグルーピングの実現が困難**

- ユーザが移動した場合、暗号装置の位置関係が変化

**動作処理情報の再生成等による管理負荷の発生**




※SGW：セキュリティゲートウェイ　Tj：端末

T1-T2：トランスポート
T1-T3：×（トランスポート）
T1-T4：トンネル

# DPRPによる問題解決

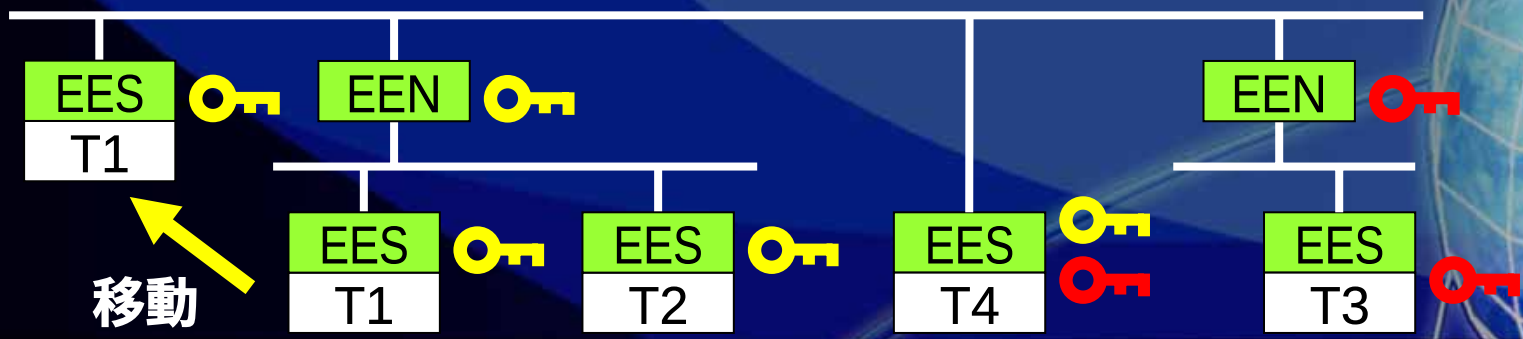
- すべてのEEが認証を含む情報交換を行う

**多段構成ネットワークでの柔軟なグルーピングが可能**

- EEが通信経路上の位置を自律的に学習し、
  動作処理情報を自動生成

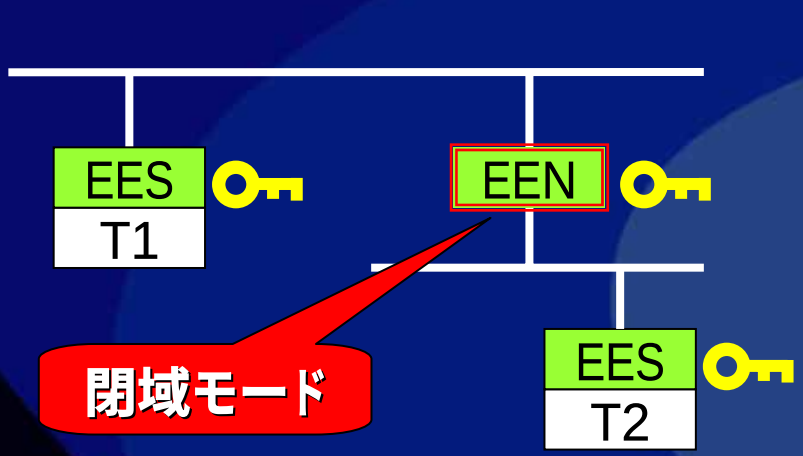
**管理負荷を発生させずにグルーピングの関係を維持**

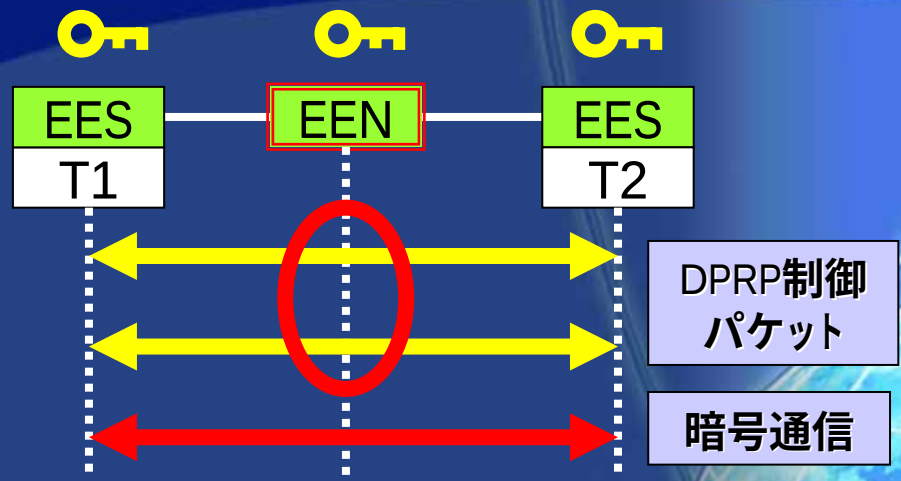
**どこに移動してもDPRPにより物理的位置透過性が保証**



# 既存DPRPの問題点

- EEには2つの動作モードが存在
  - » 開放モード：暗号鍵を持たない端末間の通信は平文で通過
  - » 閉域モード：同一グループに帰属する端末の暗号通信のみ通過



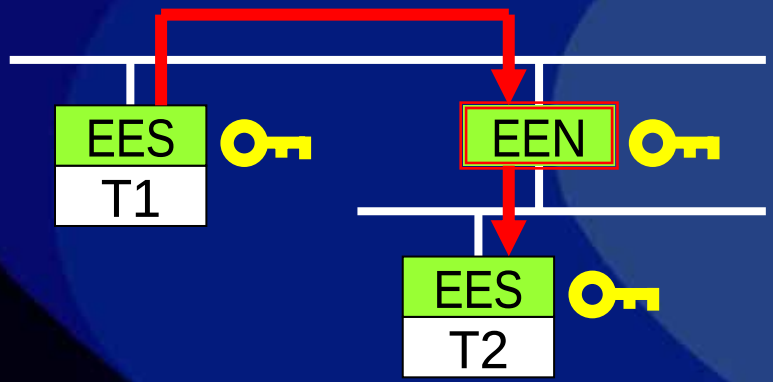

- 今まではネゴシエーションを行うためのDPRP制御パケットが閉域モードのEEを無条件で通過

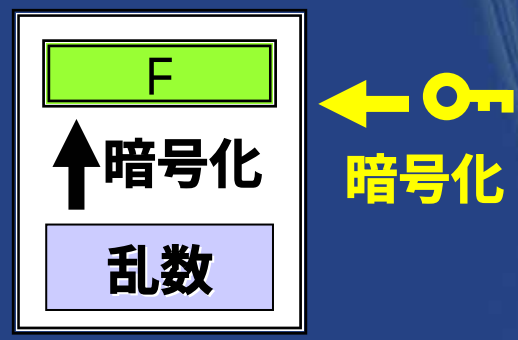
**通信経路上の全EEでの認証処理の追加**

# DPRPの改良点

- **認証鍵の導入による各EEでの認証処理の追加**
  - » 予め各EEに固定パターンFを設定（全て共通の値）

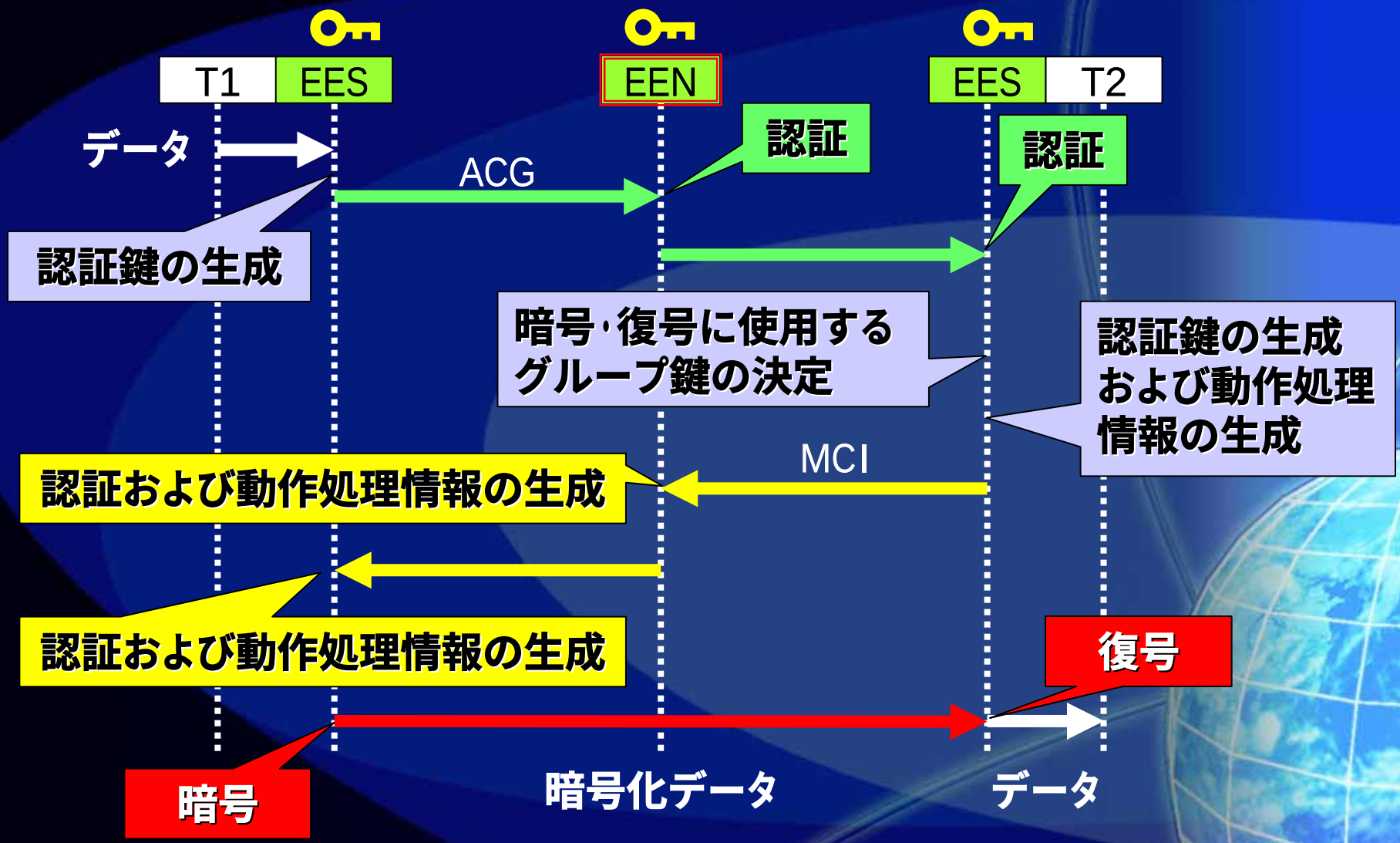
1. 乱数RNjを発生
2. 固定パターンFを乱数RNjで暗号化→eRNj(F)
3. eRNj(F)と乱数RNjをグループ鍵EKjで暗号化→認証鍵




**各EEは受信した認証鍵をグループ鍵で復号して得るFと予め設定されているFを比較して認証を行う**

# DPRPシーケンスと動作処理の概要




※ACG：Authenticate Communication Groups　MCI：Make CCGI process Information

# 評価

- DPRPを利用するにあたりIPsecと比較すると...
  - 多段構成ネットワークで柔軟なグルーピングが容易に可能
  - ネットワーク構成の変更に伴う管理負荷が減少
  - セキュリティの面に関してはIPsecの方が強固
    - DPRPにおける暗号通信に関しては別メンバーにより研究中（別セッションで発表）
    - パケット長不変で高スループットを実現
    - NAT/NAPTの通過が可能など実用性を重視

- DPRPの改良点は...
  - 認証鍵の導入
    - 認証機能の追加による安全性の向上
    - 1往復で認証処理および動作処理情報生成の実現

# まとめと今後の方針

- 閉域通信グループを構築するIPsecとDPRPとの比較
- DPRPの安全性を向上させるための改良

- DPRPのモジュール作成およびBSD系OSへの実装
- IPsecとの管理負荷やオーバーヘッド等の比較

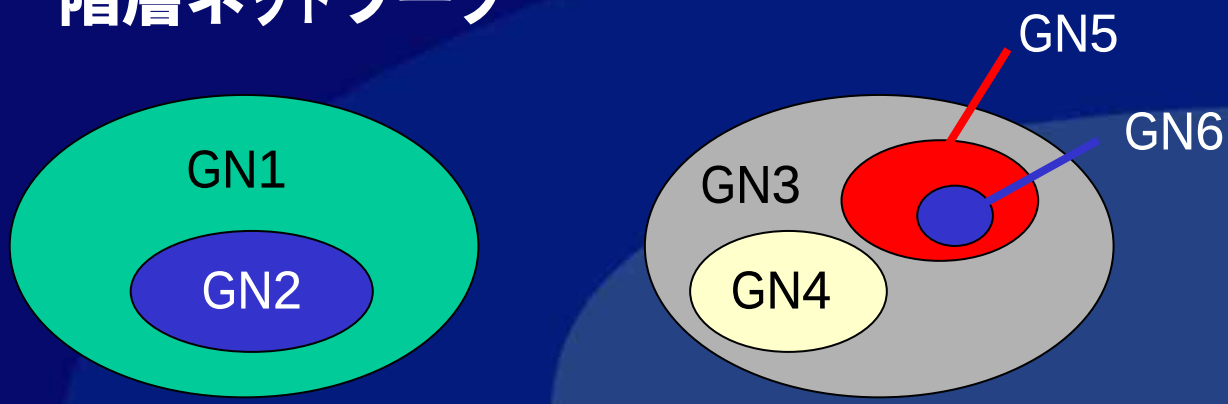
- DPRPの改良を進め、移動端末への実装
  - » PDA、IP電話
  - » ユビキタスネットワーク

# 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

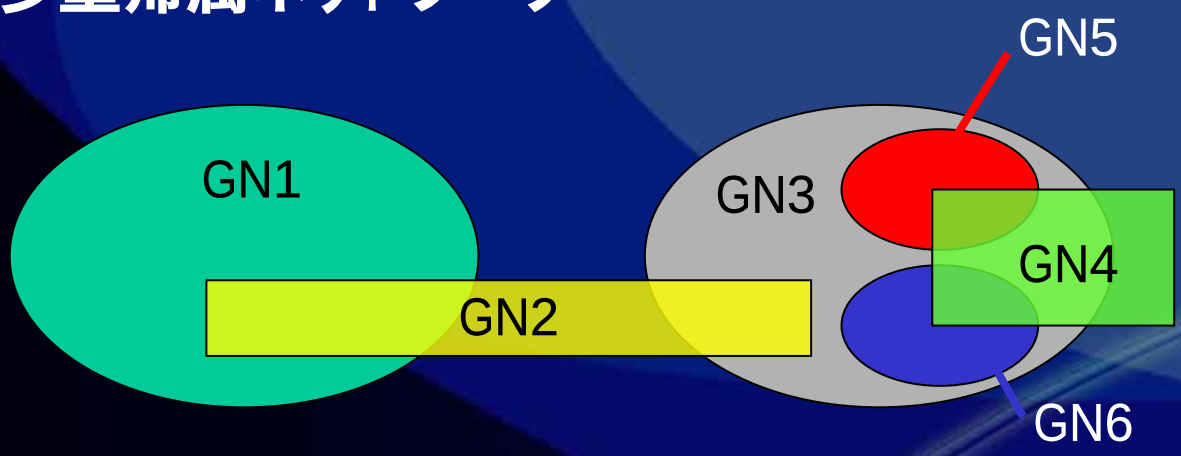
**終了**

# 多段構成（多重帰属）ネットワーク

**多段構成ネットワーク**
**階層ネットワーク**




**多重帰属ネットワーク**

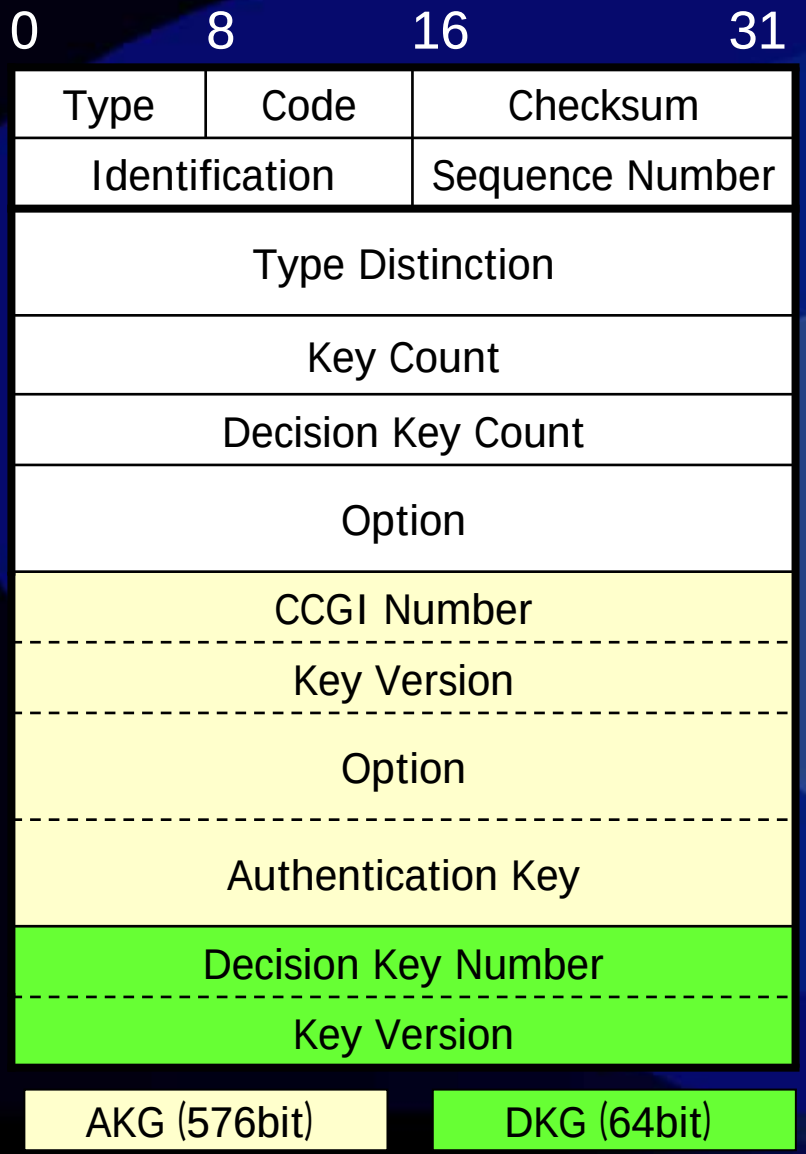


# 暗号装置と動作処理情報

- 暗号装置は3種類
  - EEN：ネットワーク型暗号装置（セキュリティドメイン）
  - EES：ソフトウェア型暗号装置（クライアントソフト）
  - EEA：アダプタ型暗号装置（サーバ保護）

- 動作処理情報は各暗号装置がテーブルとして保存
  - SPD（Security Policy Database）
  - 一定時間通信が無かった場合、鍵バージョンが更新されると自動的に削除

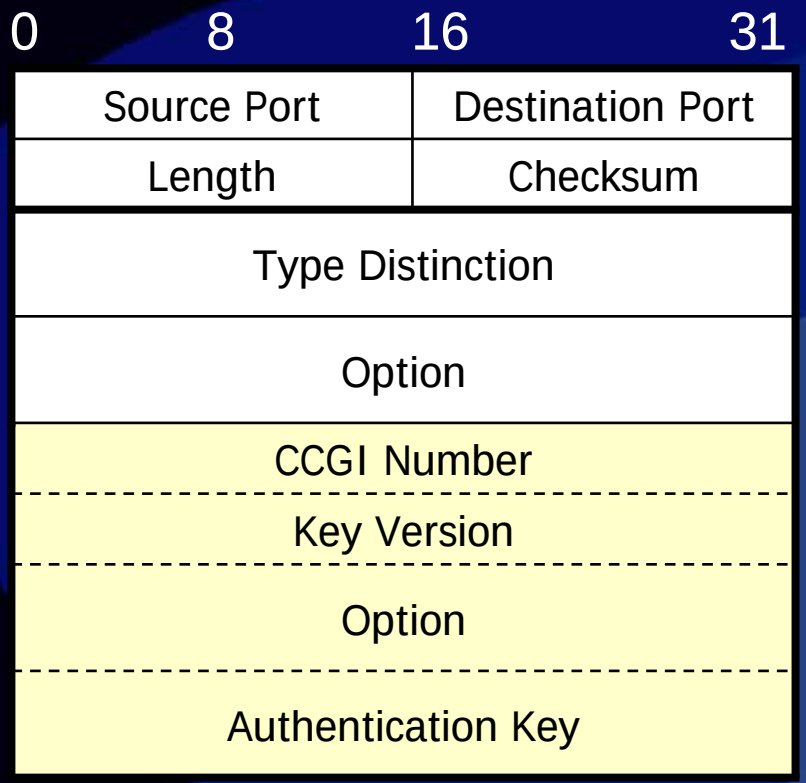
# ACG（Authenticate Communication Groups）




- 認証処理および動作処理情報の決定
- ICMP ECHOパケット

| 可変 | ICMP ECHOパケットのデータフィールド |
|---|---|
| 128 | ACGパケットだと認識させるためのデータ |
| 32 | AKG (Authentication Key Group) の数 |
| 32 | 中間EEで決定したグループ番号の数 |
| 256 | ACGの拡張用オプションフィールド |
| 32 | 送信元終端EEが所属するグループ番号 |
| 32 | グループ鍵のバージョン |
| 256 | AKGの拡張用オプションフィールド |
| 256 | 認証鍵 |
| 32 | 中間EEで決定したグループ番号 |
| 32 | 決定したグループ鍵のバージョン |

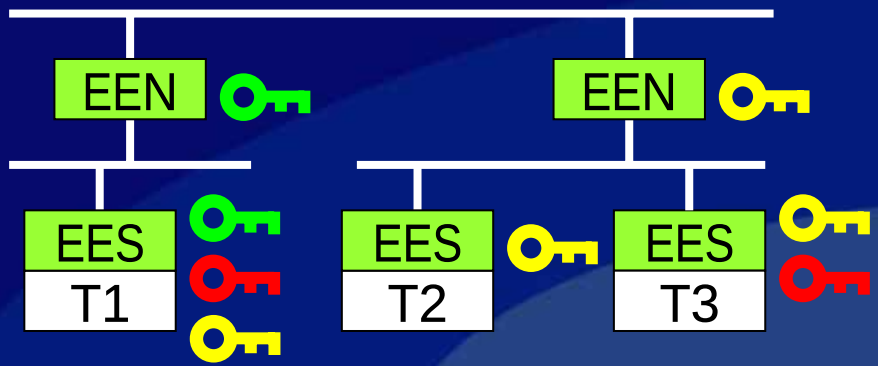
# MCI（Make CCGI process Information）




- 認証処理および動作処理情報の生成
- UDPパケット

| 可変 | UDPパケットのデータフィールド |
|---|---|
| 128 | MCIパケットだと認識させるためのデータ |
| 256 | MCIの拡張用オプションフィールド |
| 32 | 各EEが使用した鍵のグループ番号 |
| 32 | グループ鍵のバージョン |
| 256 | AKGの拡張用オプションフィールド |
| 256 | 認証鍵 |

# 現在検討中の課題




- T1に を配送するとT3と通信するために上位のEENを通過できるが、本来アクセスできないはずのT2と通信できてしまう
- T3が別のグループに移動した場合、そのグループ鍵をT1がはじめから所持していないと通信できなくなる

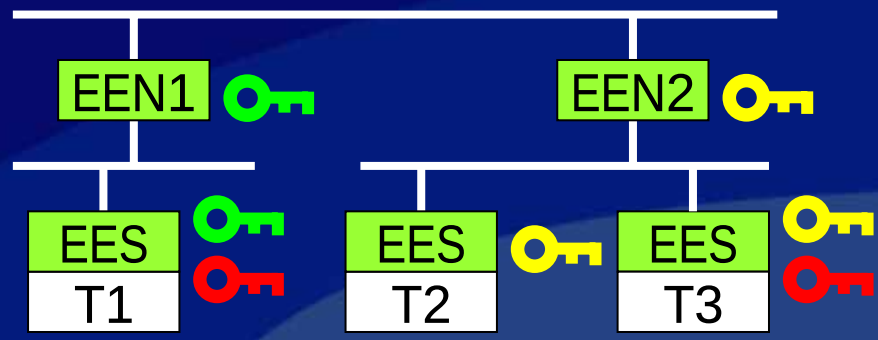
**初期段階でどの鍵を配送するか決定する時の管理負荷が発生**

**鍵の増加でアクセス可能になってしまう場合が発生**

# 現在検討中の認証モデル

EEN1配下存在グループテーブル

| T1 IP Adr | |
|---|---|
| ⋮ | ⋮ |




EEN2配下存在グループテーブル

| T2 IP Adr | |
|---|---|
| T3 IP Adr | |
| ⋮ | ⋮ |

- ACGパケットがEEN2に到達したとき、EEN2はT1から送られてきた認証鍵を復号できないが、配下存在グループテーブルを参照してその中に送信先IPアドレスと復号できるグループ鍵が一致したら通過させる
- このときEEN2からT3へ送信されるACGパケットはT1からのパケットでなくEEN2からのパケットなので、閉域モードを無条件で通過しているわけではない