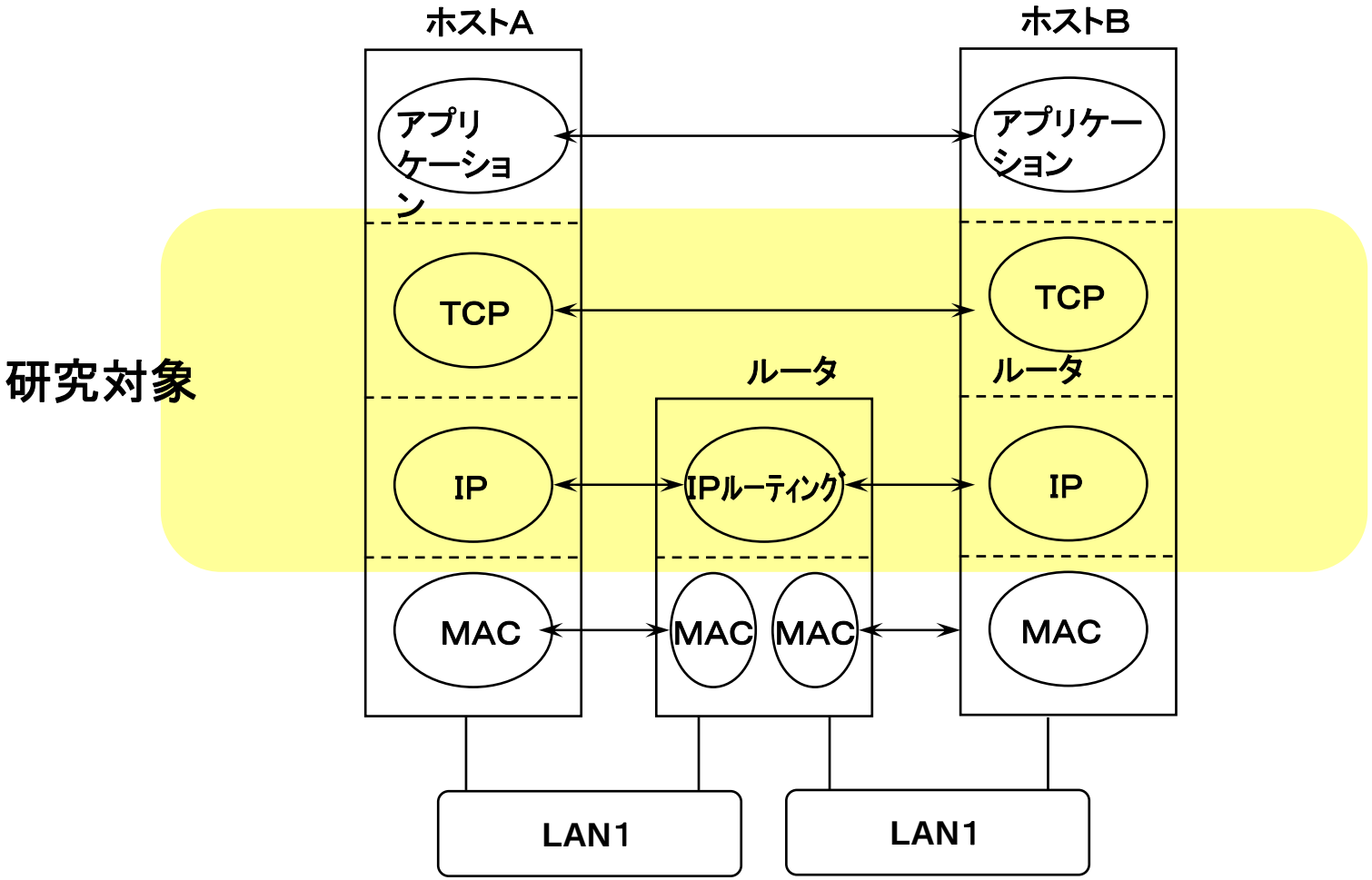
研究テーマの紹介

H17,11,11

名城大学　理工学部　情報工学科

渡邊　晃

研究対象となるのは主に下図の部分です。ただし、これに限らず範囲を広げています。



研究のキーワード

- ユビキタスネットワーク

  ユビキタス社会を実現するためのネットワーク基盤
  - いつでも、誰でも、どこからでも

- ネットワークセキュリティ

  ユビキタスネットワークを安全に使うしくみ
  - 盗聴，改ざん，なりすましの防止，プライバシーの保護

具体的研究テーマ

フレキシブルプライベートネットワーク

研究のねらい

- 自由に動ける
- 安全に使える
- ネットワークの多段構成
- 多重帰属

FPN (Flexible Private Network)

柔軟性とセキュリティを兼ね備えたグルーピング通信を可能とするネットワークシステム

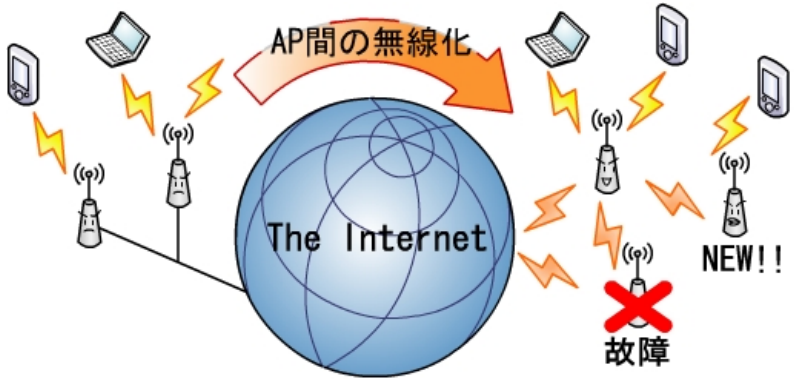
実際に作って検証する
シミュレーションで確認する

無線アクセスポイントリンク
－アクセスポイント間を無線で接続－

・無線LAN環境を迅速に整備

・車車間通信への応用

・災害時に緊急通信網を構築



IP電話

・ファイアウォールを通過するIP電話
・リング型IP電話会議

不正アクセスの研究
－クラッカーの攻撃とそれを防止する方法－

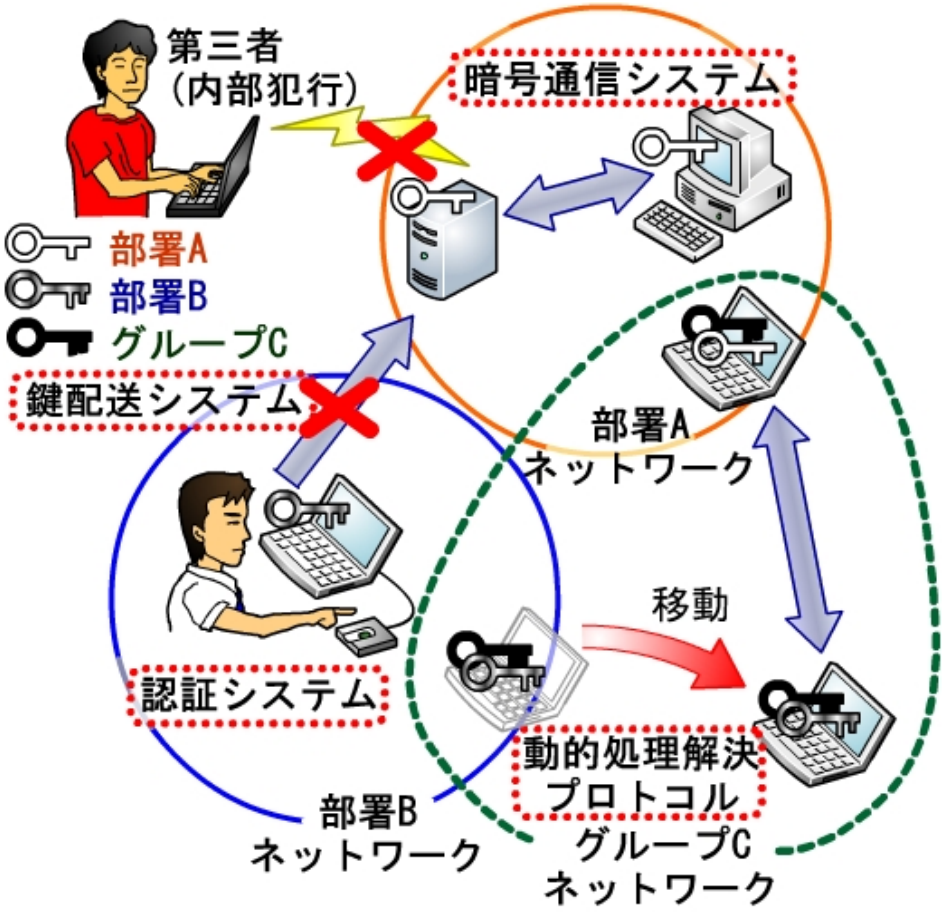
フレキシブルプライベートネットワーク

・ネットワークの物理構成を自動学習

・通信中にIPアドレスが変わっても通信を継続

・ｸﾞﾛｰﾊﾞﾙｱﾄﾞﾚｽ空間とﾌﾟﾗｲﾍﾞｰﾄｱﾄﾞﾚｽ空間を跨る自由な通信

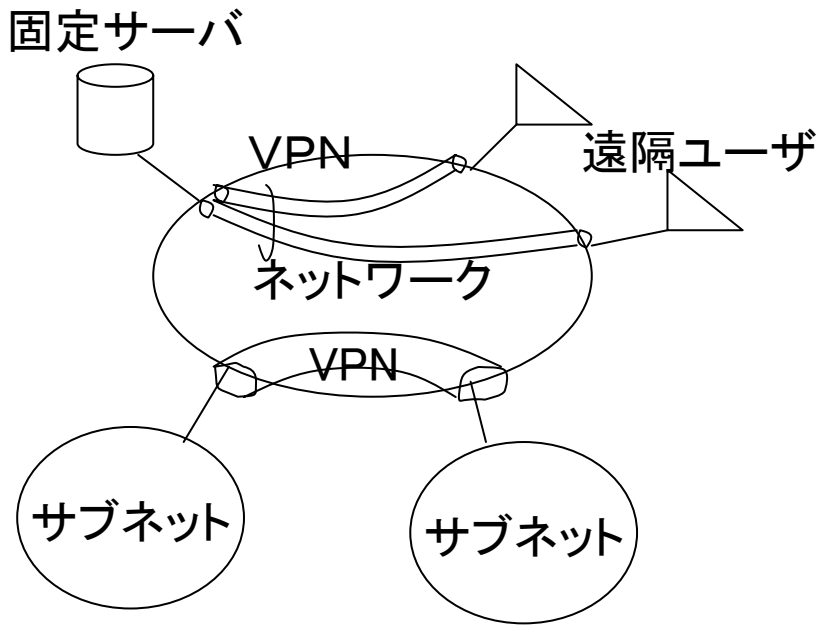
・NATやファイアウォールと共存できる暗号化通信



VPN (Virtual Private Network)

既存技術

ネットワークのインフラを共有する手段として有効



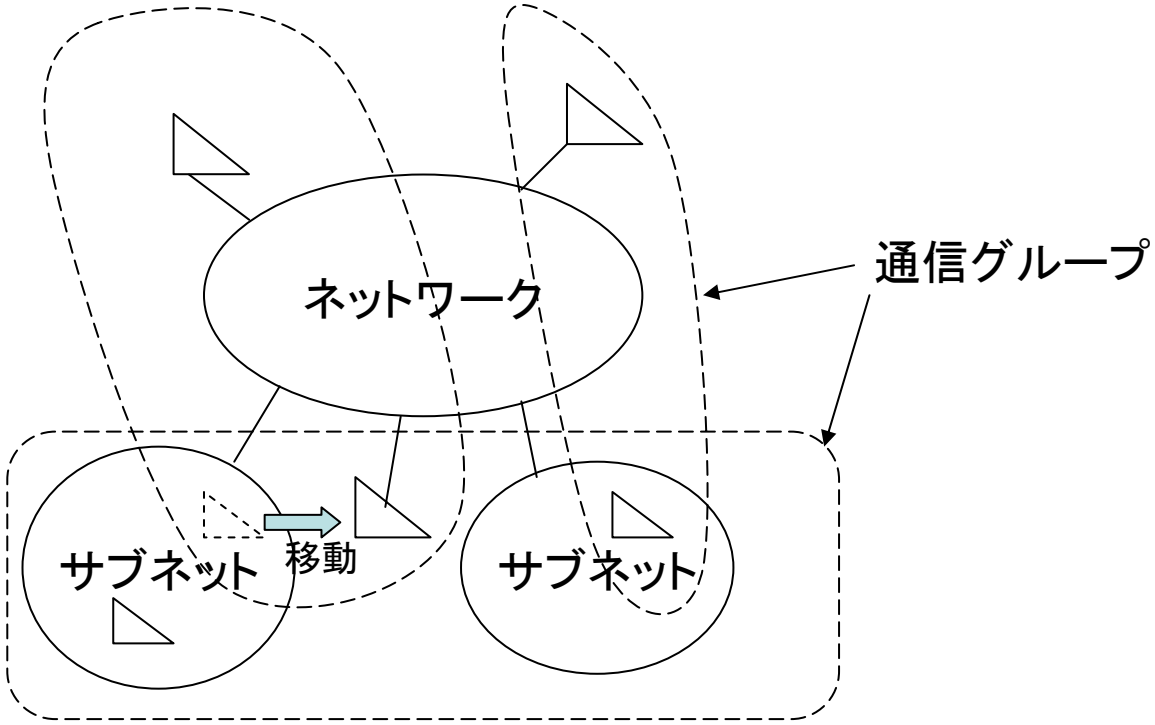
VPNの課題

・サブネットは固定、サーバは固定

・ネットワークは平坦

提案技術

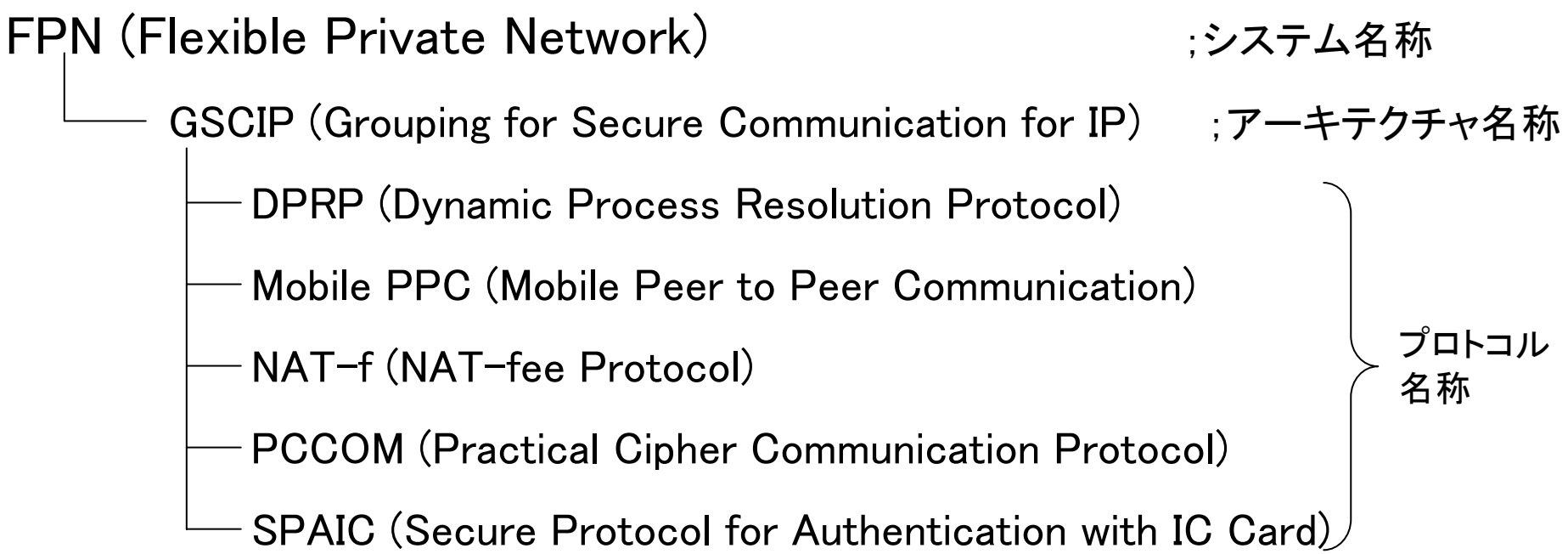
FPN (Flexible Private Network)

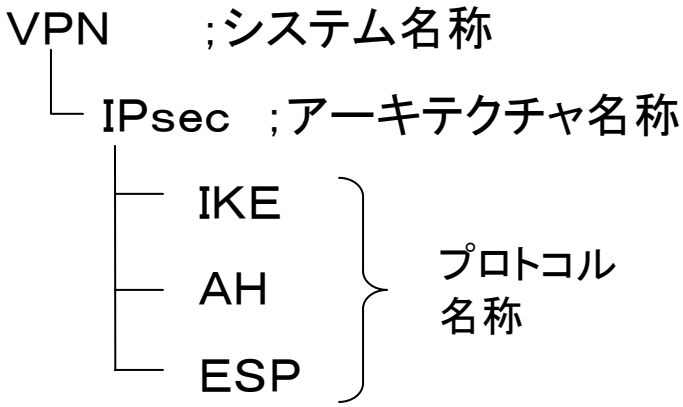


FPNの特徴

・すべてのサブネット/ホストが動くことを想定

・サブネット単位，ホスト単位のグループが混在


FPN (Flexible Private Network)
;システム名称
GSCIP (Grouping for Secure Communication for IP)
;アーキテクチャ名称
DPRP (Dynamic Process Resolution Protocol)
Mobile PPC (Mobile Peer to Peer Communication)
NAT-f (NAT-fee Protocol)
PCCOM (Practical Cipher Communication Protocol)
SPAIC (Secure Protocol for Authentication with IC Card)
プロトコル
名称


VPN
;システム名称
IPsec
;アーキテクチャ名称
IKE
AH
ESP
プロトコル
名称

FPNで実現すべき機能

多段構成ネットワーク環境において、以下の透過性を実現する

(1)位置透過性

　あらかじめ定義した通信グループが端末の物理的位置にかかわらず維持される

(2)移動透過性

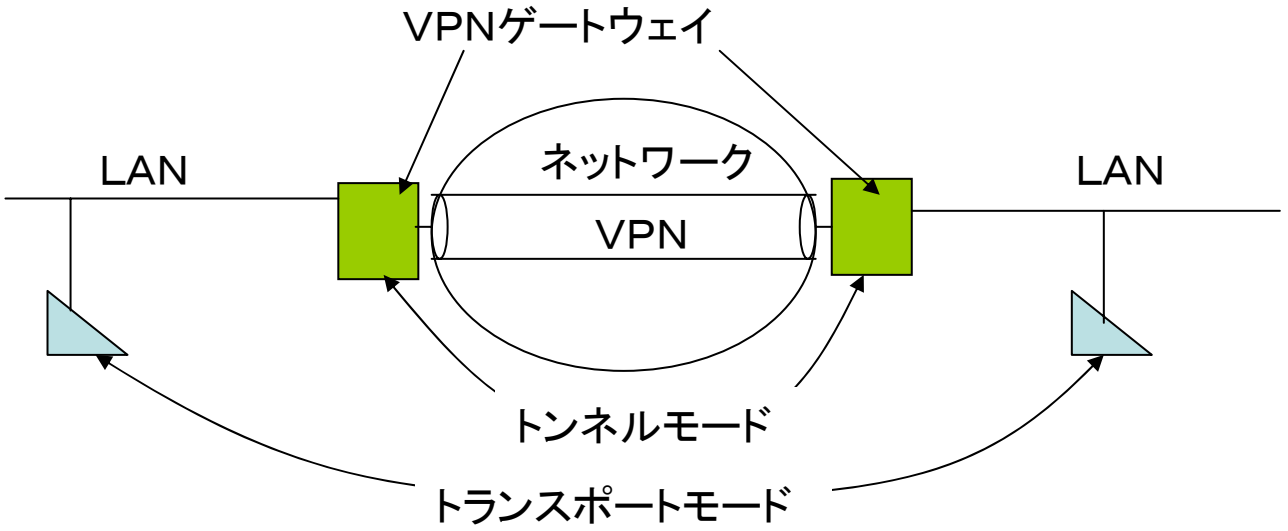
　通信中に端末が移動しても通信が継続される

(3)アドレス空間透過性

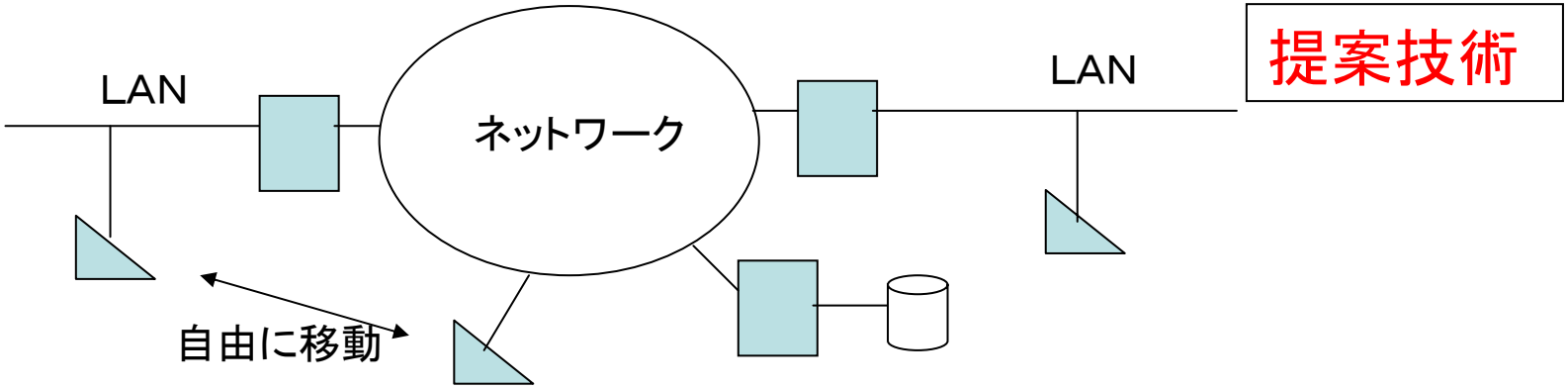
　グローバルアドレス空間とプライベートアドレス空間の間で自由な通信ができる

多段構成ネットワーク環境への対応

IPsecはトンネルモードとトランスポートモードに互換性がない→多段構成に柔軟に対応できない

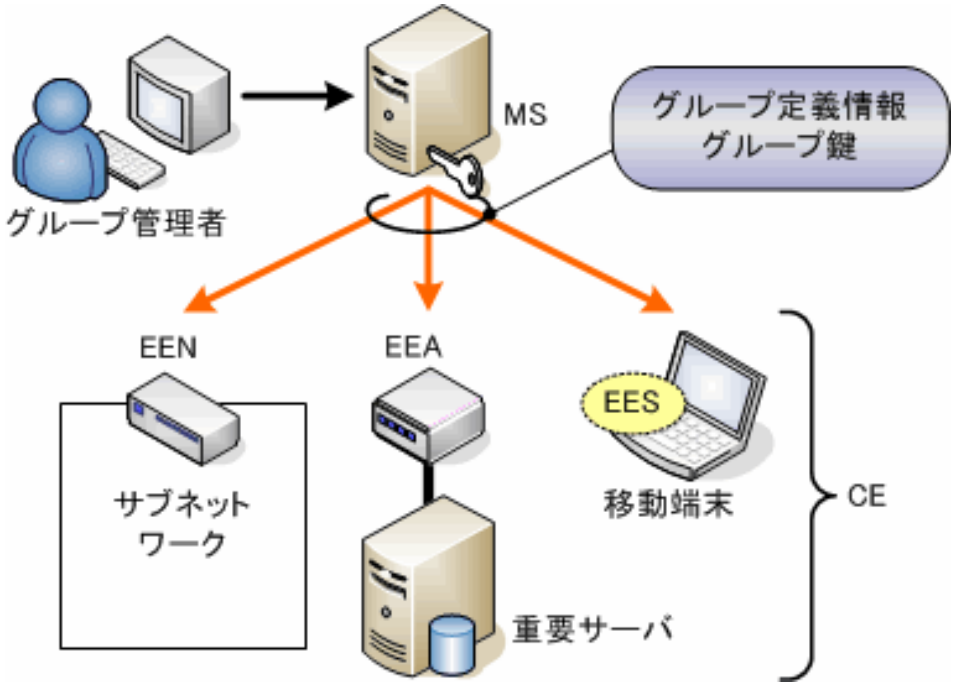


GSCIPはすべての暗号装置が対等→多段構成に対応可能

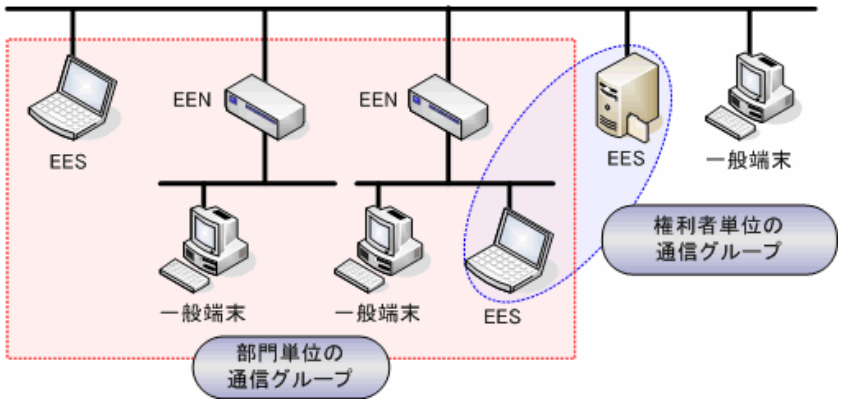


GSCIPの基本；共通暗号鍵を用いた通信グループの定義

提案技術



通信グループと共通暗号鍵を1対1に対応づける



多段構成ネットワークでも同様に定義する

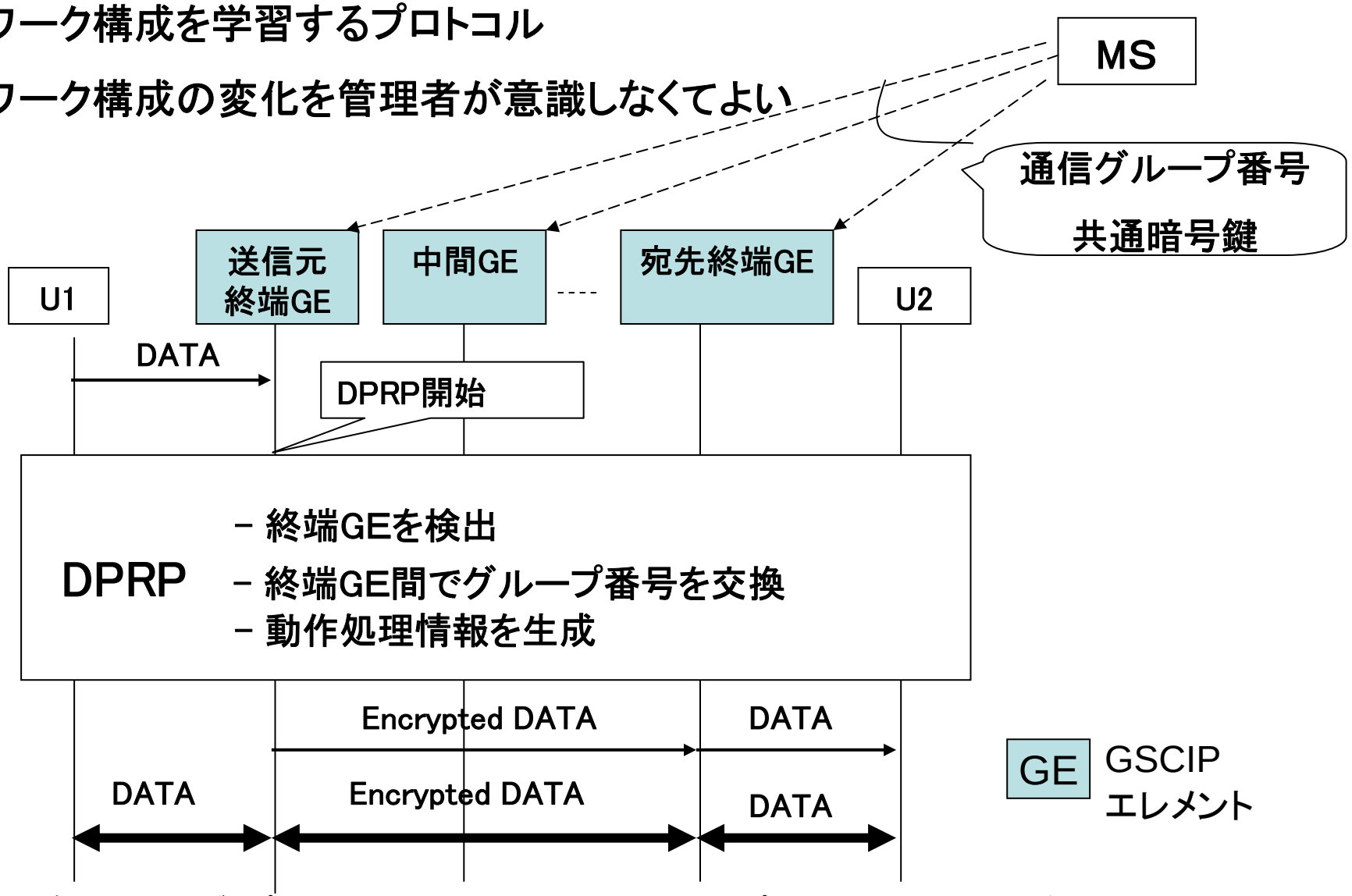
位置透過性の実現

提案技術

DPRP (Dynamic Process Resolution　Protocol)

ネットワーク構成を学習するプロトコル

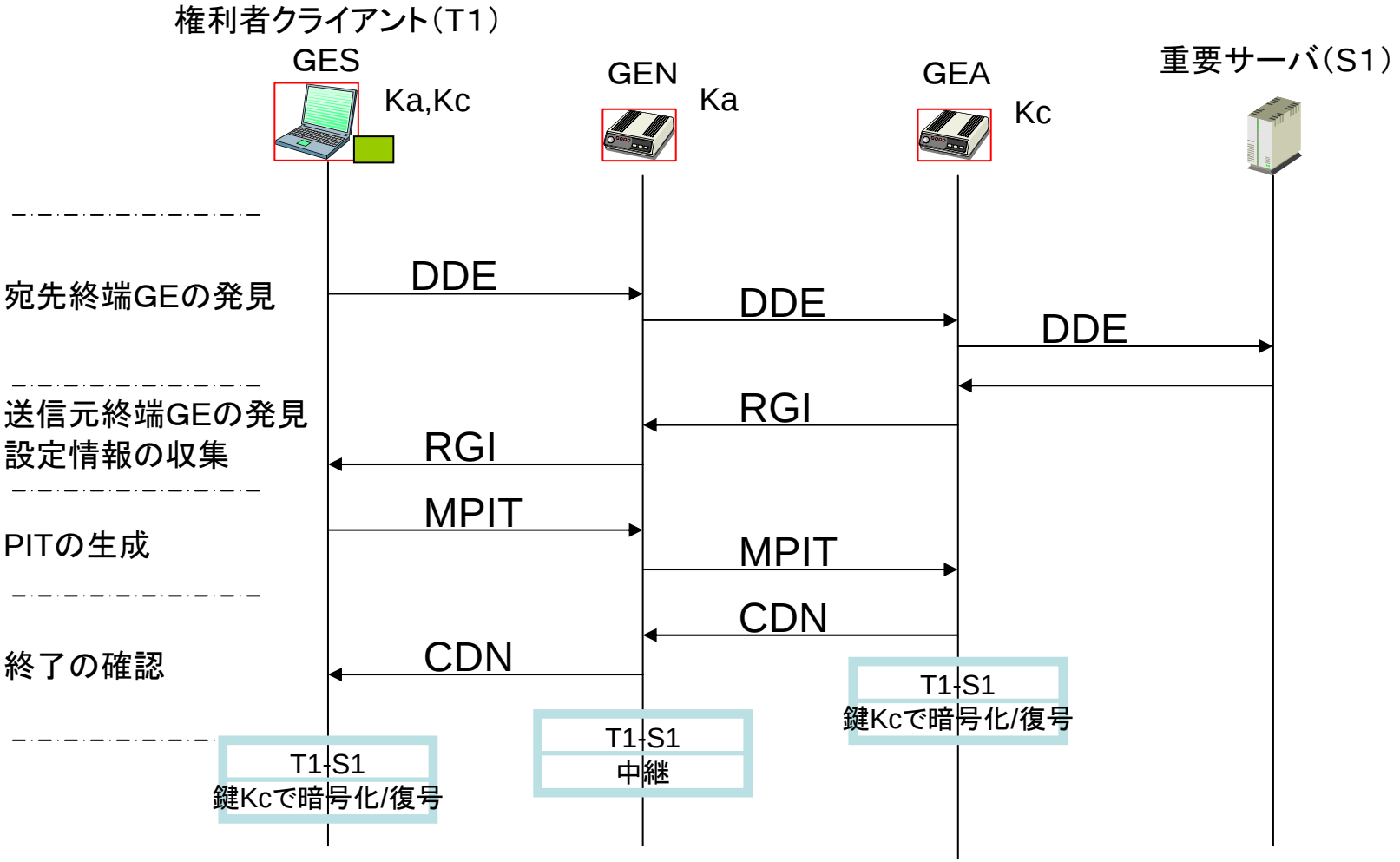
ネットワーク構成の変化を管理者が意識しなくてよい



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.

DPRP（動的処理解決プロトコル）

提案技術



DDE; Detect Destination End GE

RGI; Report GE Information

MPIT; Make Process Information Table

CDN; Complete DPRP Negotiation

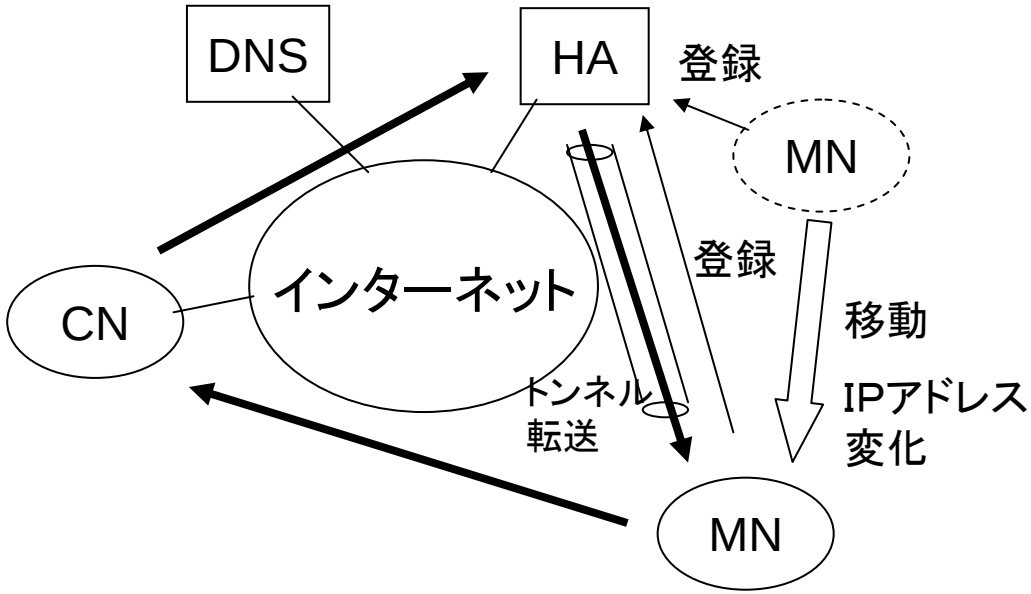
処理テーブルの内容

移動透過性の実現

既存技術

Mobile　IP

通信中に移動しても通信を継続できる技術



モバイルIPの課題

・特殊な装置（HA）が必要となる

・通信経路が三角経路となる

・HAとMN間はトンネル転送となる

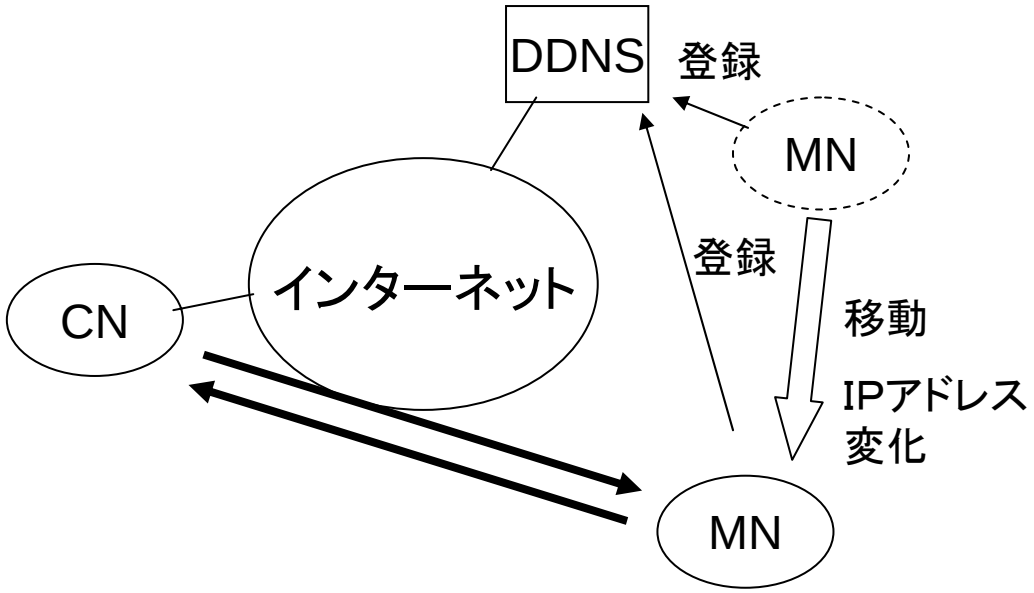
・MNの送信パケットが破棄される可能性

Mobile　PPCの提案

移動透過性の実現

提案技術

Mobile　PPC　(Mobile Peer to Peer Communication)



初期IPアドレスの解決にはDDNS (Dynamic DNS)を使う。

エンドエンドで通信を開始。

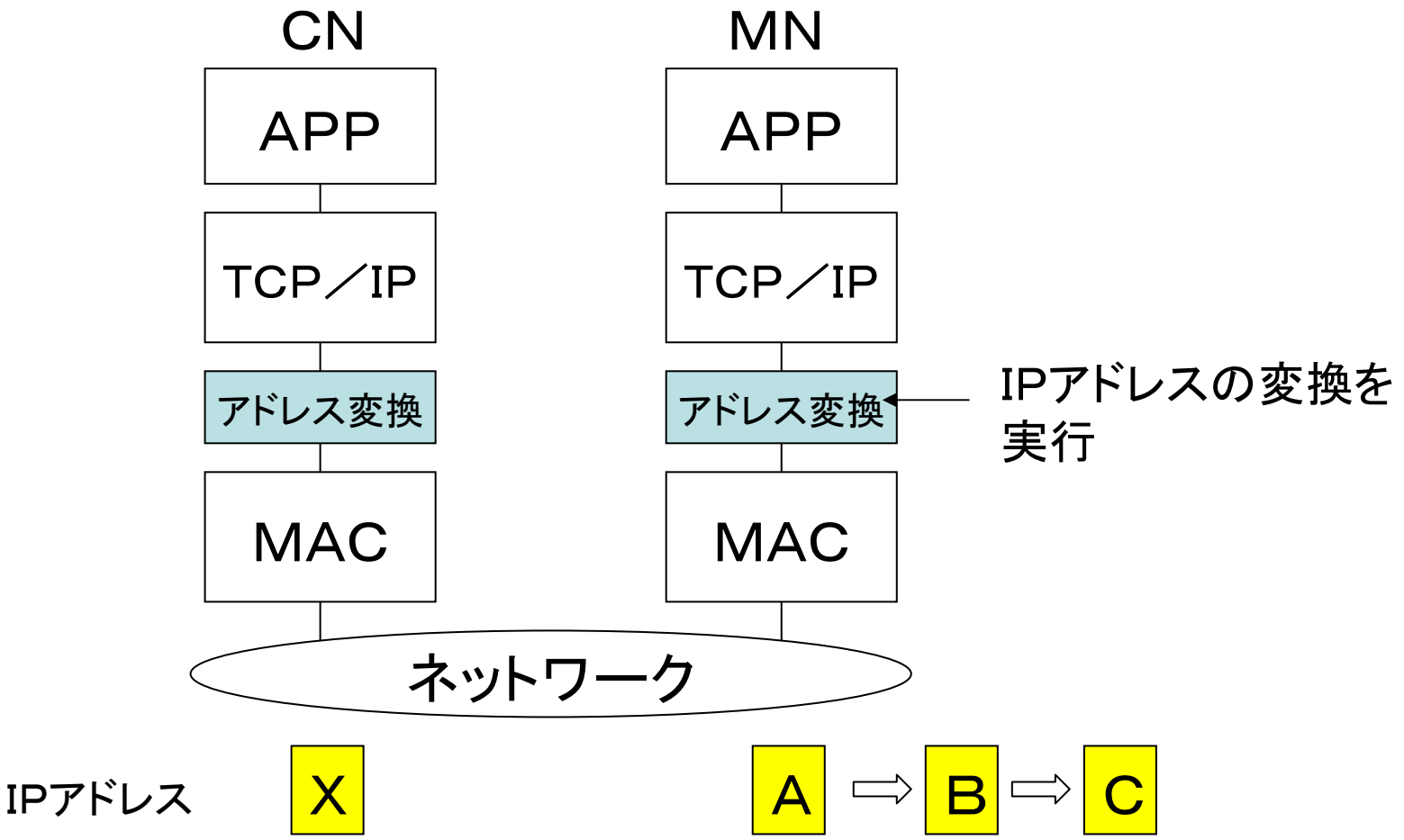
IPアドレスの変更はエンドエンドで通知する。アプリケーションはIPアドレスの変化に気付かない。

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”，DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.125-128，Jul.2005.

移動透過性の実現

提案技術

Mobile　PPC（つづき）



TCP／IPとMACの間でアドレス変換を実行することによりアプリケーションはIPアドレスが変化したことに気づかないようにすることができる。

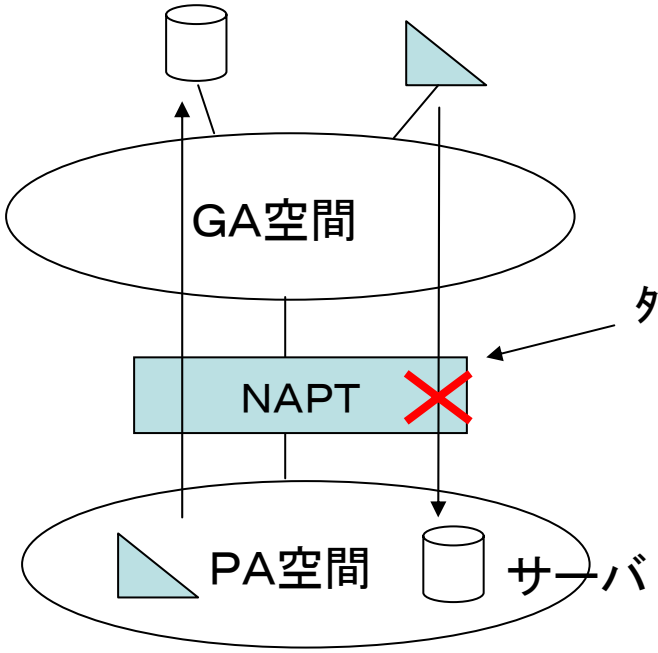
FreeBSDに実装して確認済み。

アドレス空間透過性の実現

既存技術

NAPT（IPマスカレード）

NAPTがIPアドレス変換を行うことによりプライベートアドレス（PA）空間からグローバルアドレス（GA）空間のサーバへのアクセスが可能となる



NAPT越えの課題

・GA空間からPA空間への通信の開始ができない。

⇩

NAT-fの提案

アドレス空間透過性の実現

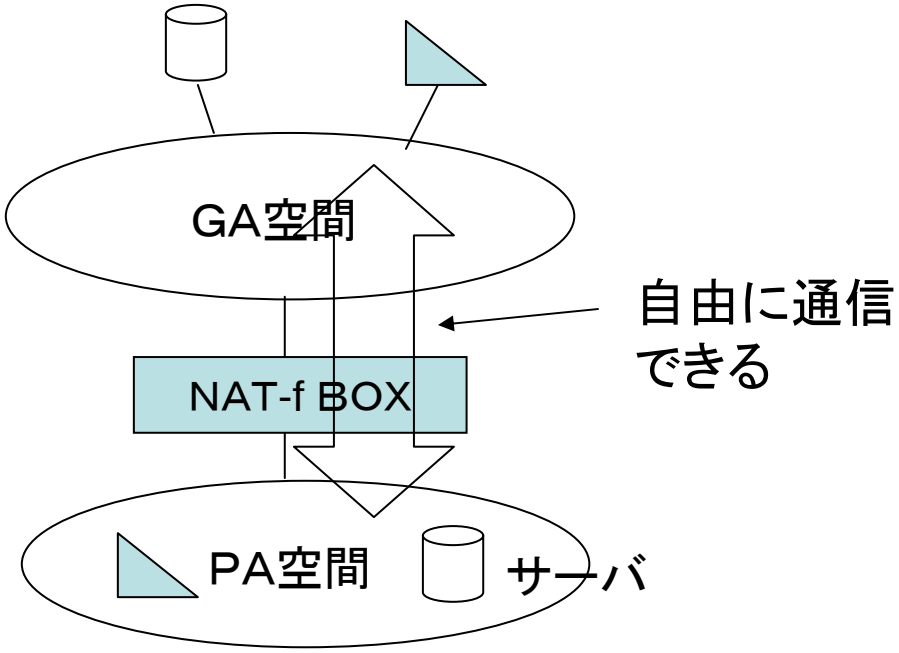
提案技術

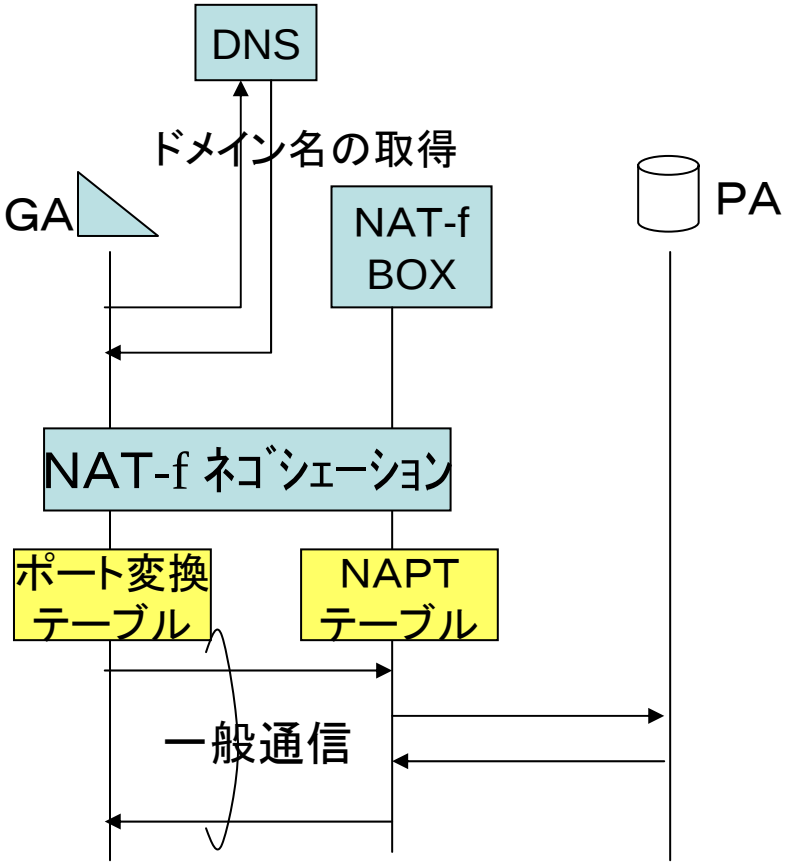
NAT-f (NAT-free Protocol)

GA空間の端末とPA空間の端末が自由に通信できる。

NAT-f により、NATFBOXとGA端末がポート番号の情報を交換する。

NAT-f BOXがアドレス/ポート番号変換、GA端末がポート番号変換を行う。





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”，WiNF2005論文集，pp.142-146，Sep.2005.

アドレス空間透過性の実現

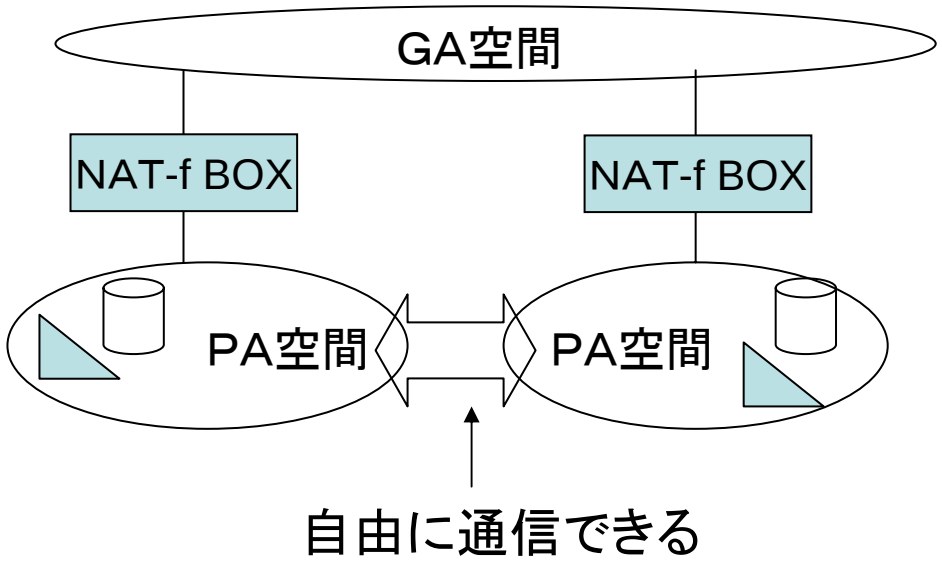
提案技術

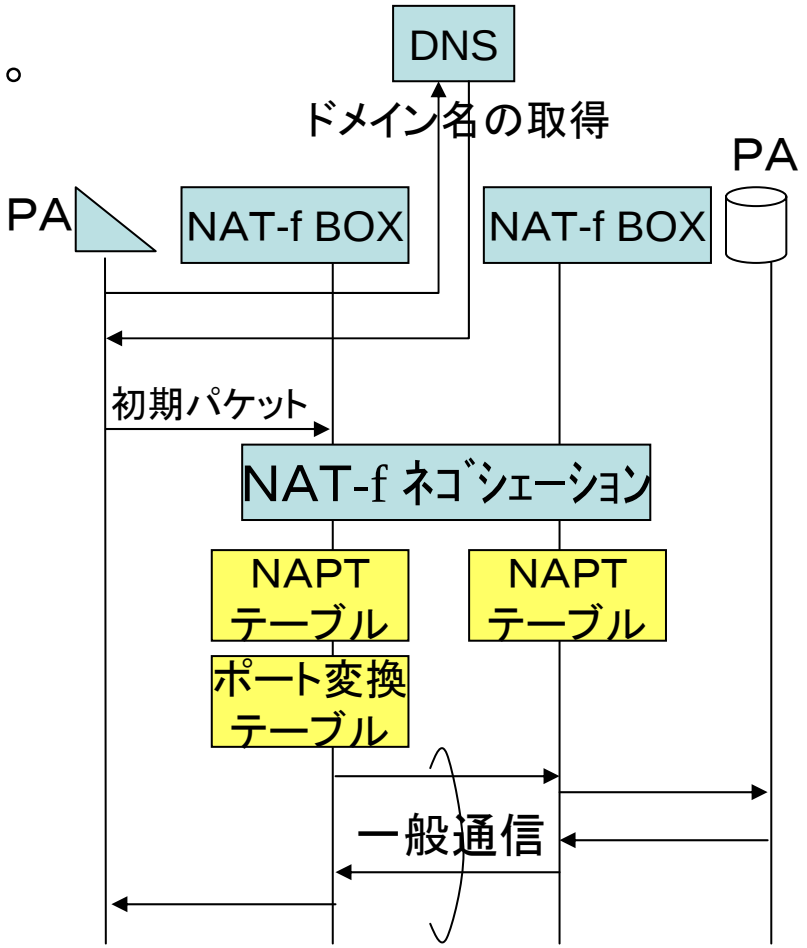
CIPA（Communication between terminals in Independent Private Address area）

GA空間を介して異なるPA空間の端末どうしが自由に通信できる。

NAT-f によりNAT-f BOXどうしがポート番号の情報を交換する。

一方のNAT-f BOXがポート番号変換を行う。



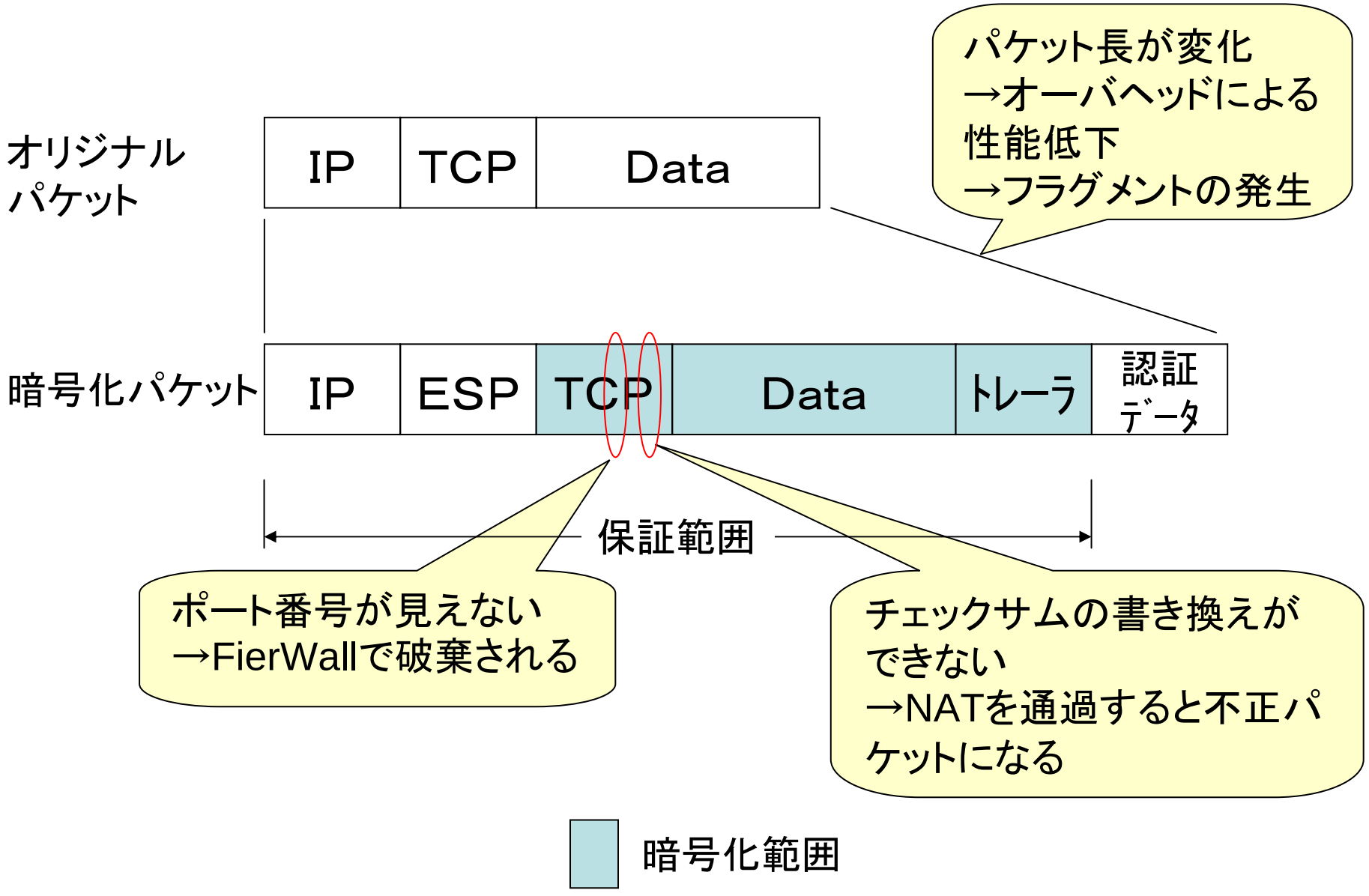


柳沢信成，加藤尚樹，鈴木秀和，渡邊晃，“異なるプライベートアドレス空間端末の通信（ CIPA ）の提案”，DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.369-372，Jul.2005.

暗号通信方式

既存技術

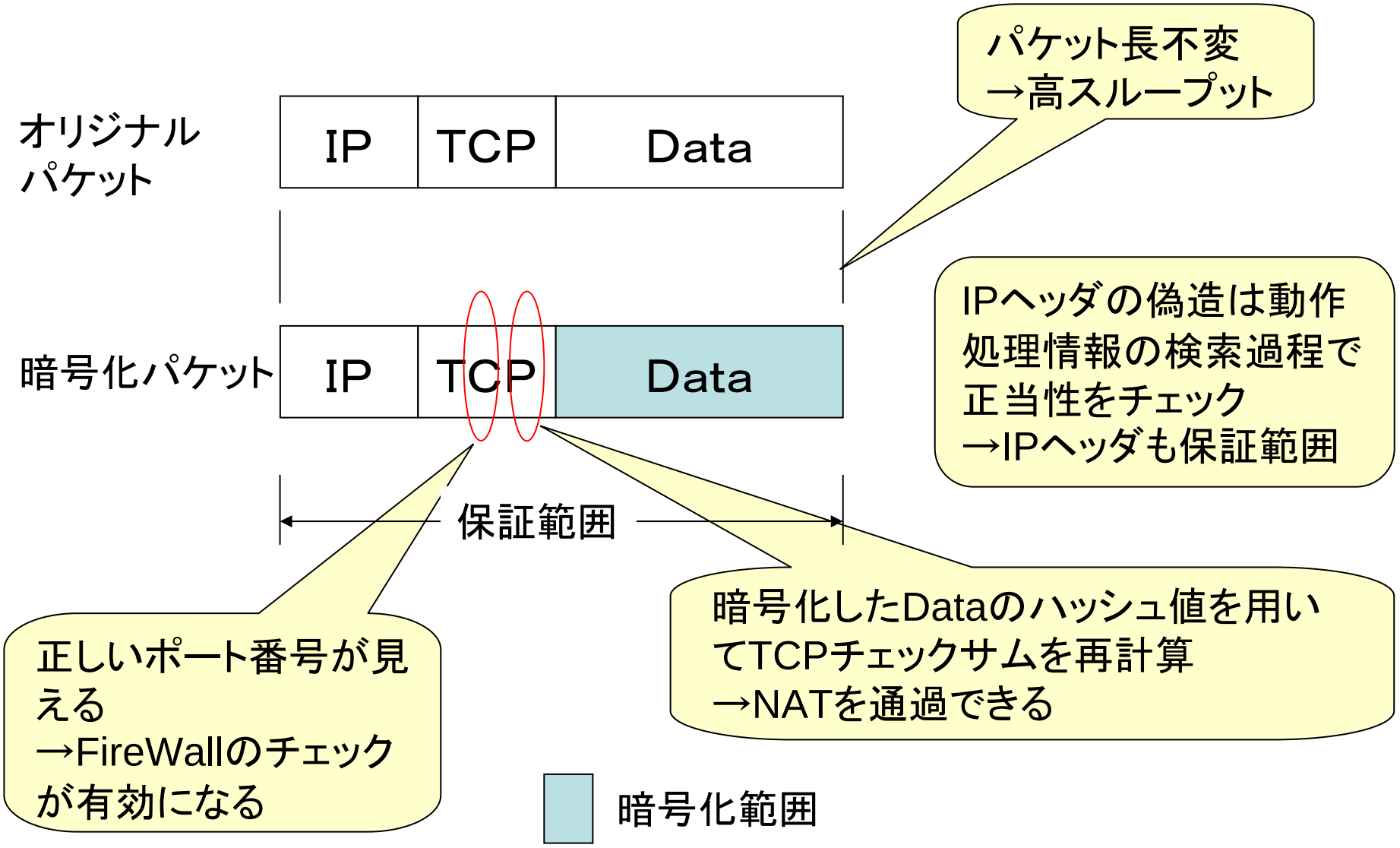
IPsec　ESP（Encryption Security Payload）



暗号通信方式

提案技術

PCCOM（Practical Cipher COMmunication Protocol）



増田真也，渡邊晃，“実用暗号通信 PCCOM の実装と評価”，情報処理学会研究報告，2005-CSEC-28, pp.205-210 ， Mar.2005.

GSCIPの現状

・実装完了（FreeBSD）

DPRP，MobilePPC，PCCOM

・実装中

NATF，CIPA

MobileNPC (Mobile Network to Peer Communication)

・検討中

MobilePPCv6

GSCIPの統合

SPAIC（ICカードによる認証/鍵配送プロトコル）

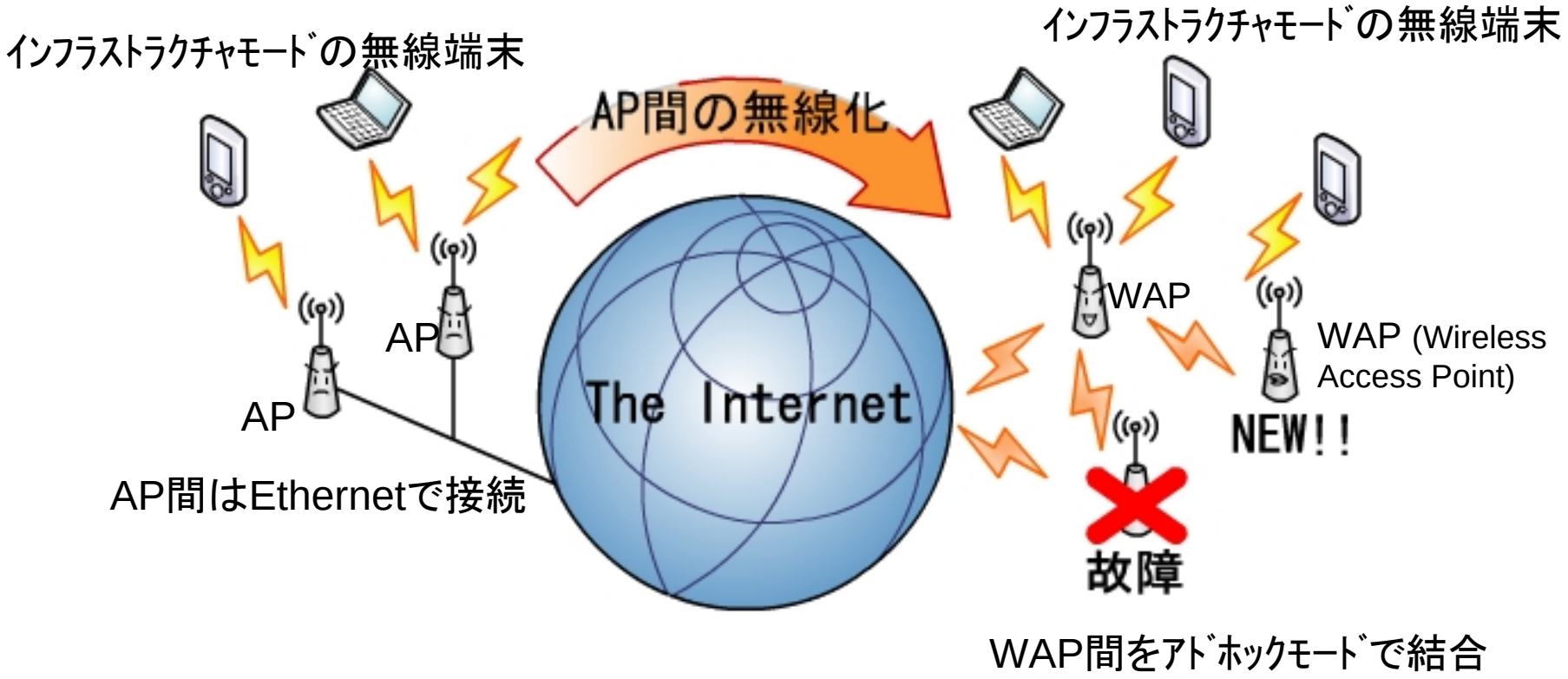
パケットロスなしハンドオーバ

Windowsへの実装

ソースコードの公開

無線アクセスポイントリンク
－アクセスポイント間を無線で接続－

WAPL (Wireless Access Point Link)

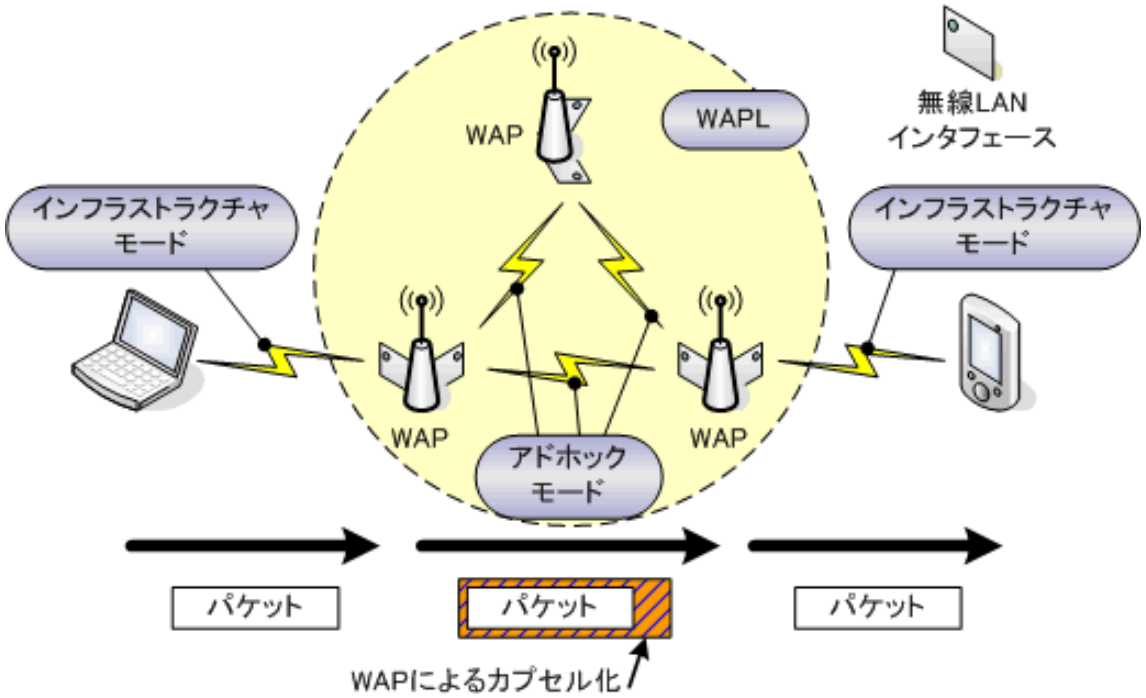


WAPL (Wireless Access Point Link)

提案技術

無線LANのAP(Access Point)をアドホックネットワークで結合しAP群を1つのLANに見せる。

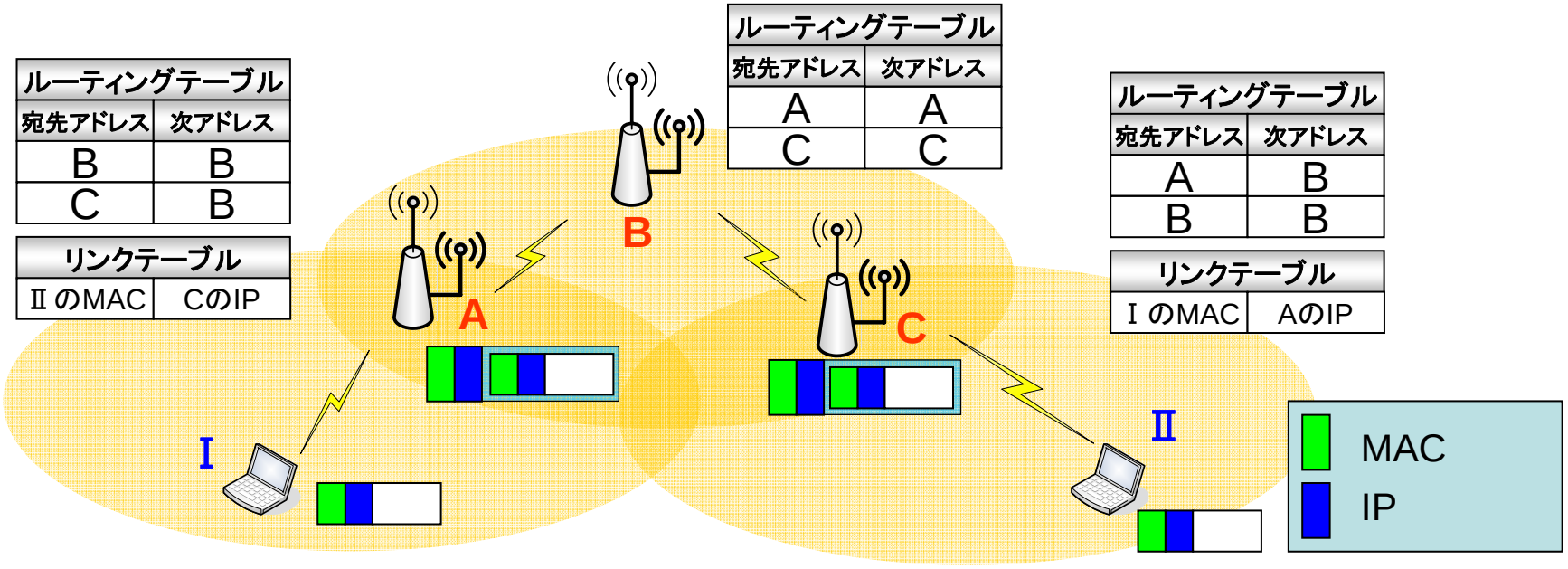
端末はインフラストラクチャモードのままでよい。APを設置していくだけで無線LANエリアが広がる。



WAPL (Wireless Access Point Link)

提案技術

アドホックネットワークによりEthernetを完全にエミュレーションする

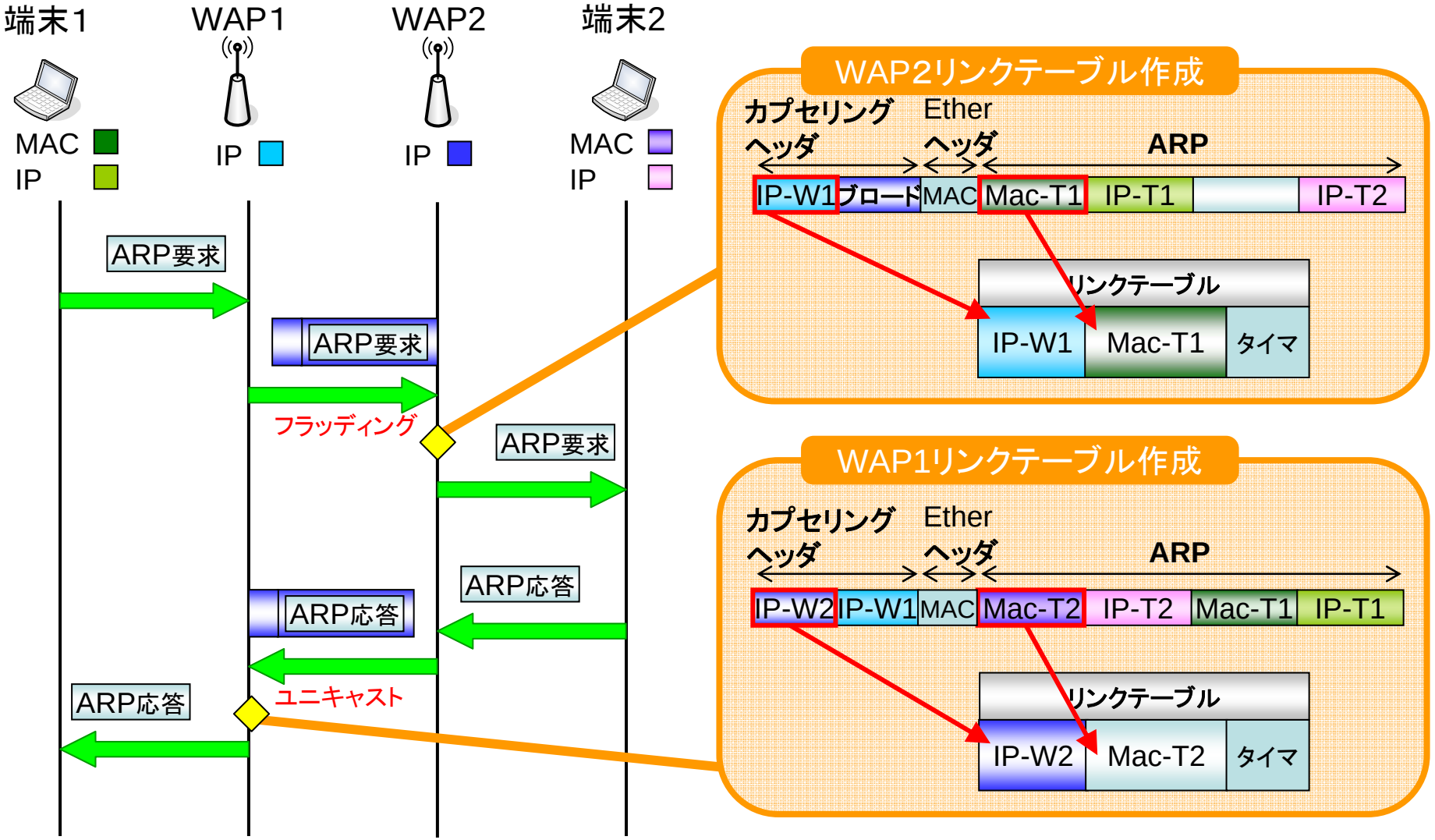


- WAP間通信はアドホックモード
- WAP-端末間はインフラストラクチャモード
- WAPでイーサフレームを
  カプセル化・デカプセル化

- リンクテーブルはARPを用いて必要に応じて生成
- アドホックプロトコルは用途に応じて変更可能

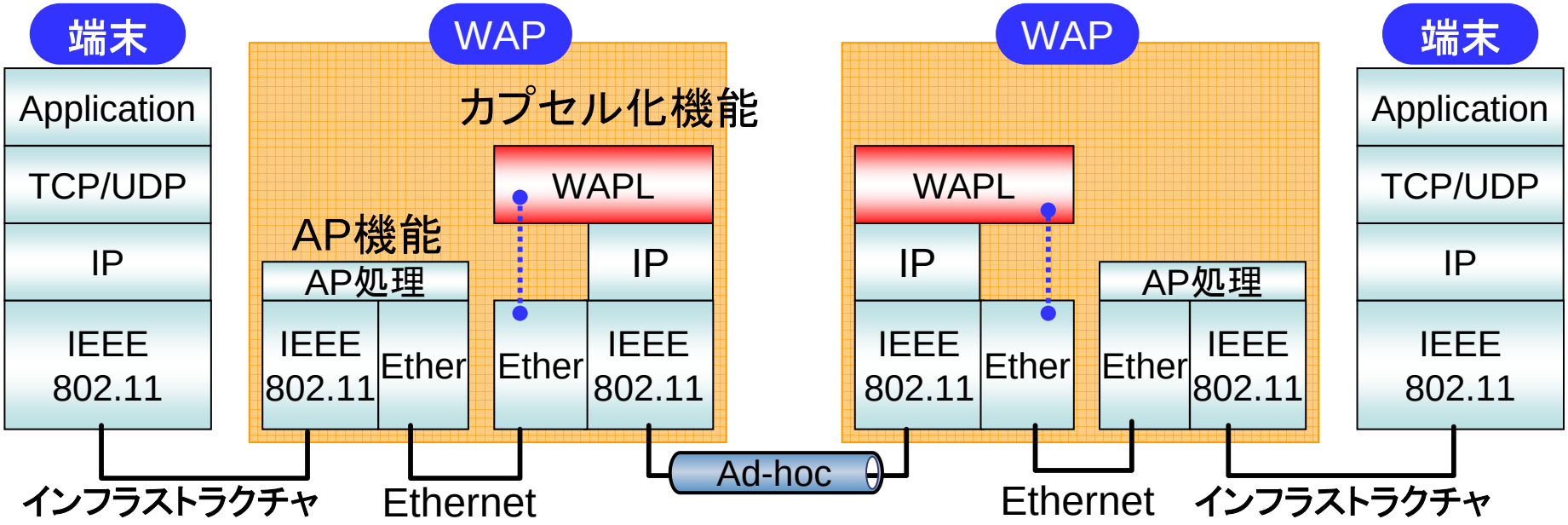
リンクテーブルの生成方法

提案技術

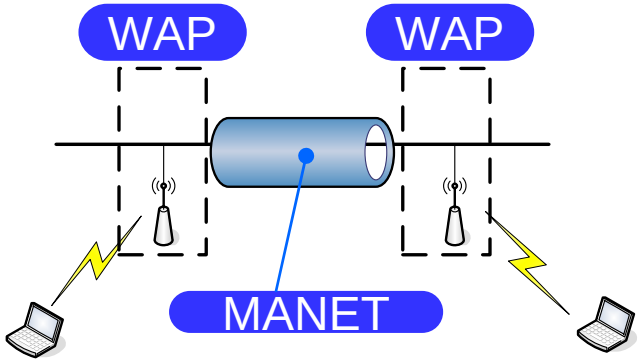


WAPLのアーキテクチャ

提案技術

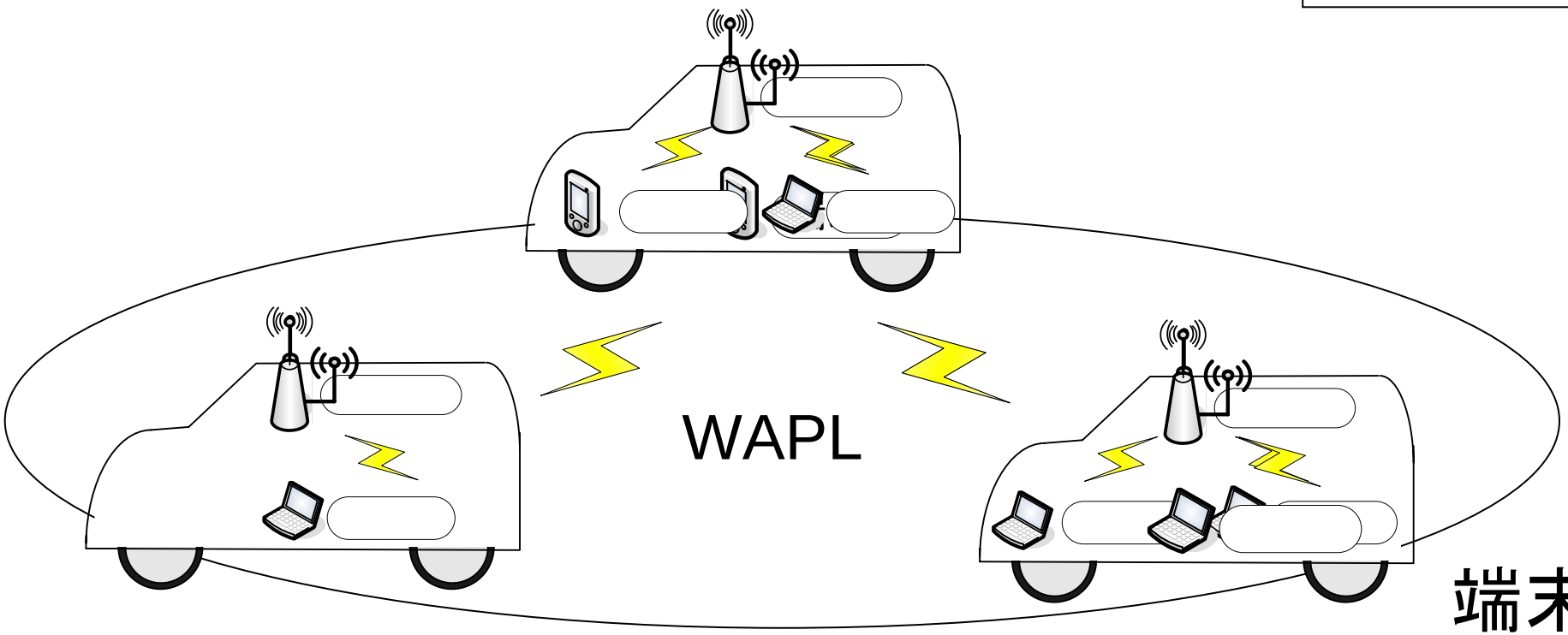


- WAPはAP機能とカプセル化機能で構成される
- アドホックネットワークでEthernetを完全にエミュレートする



車車間通信への応答

提案技術

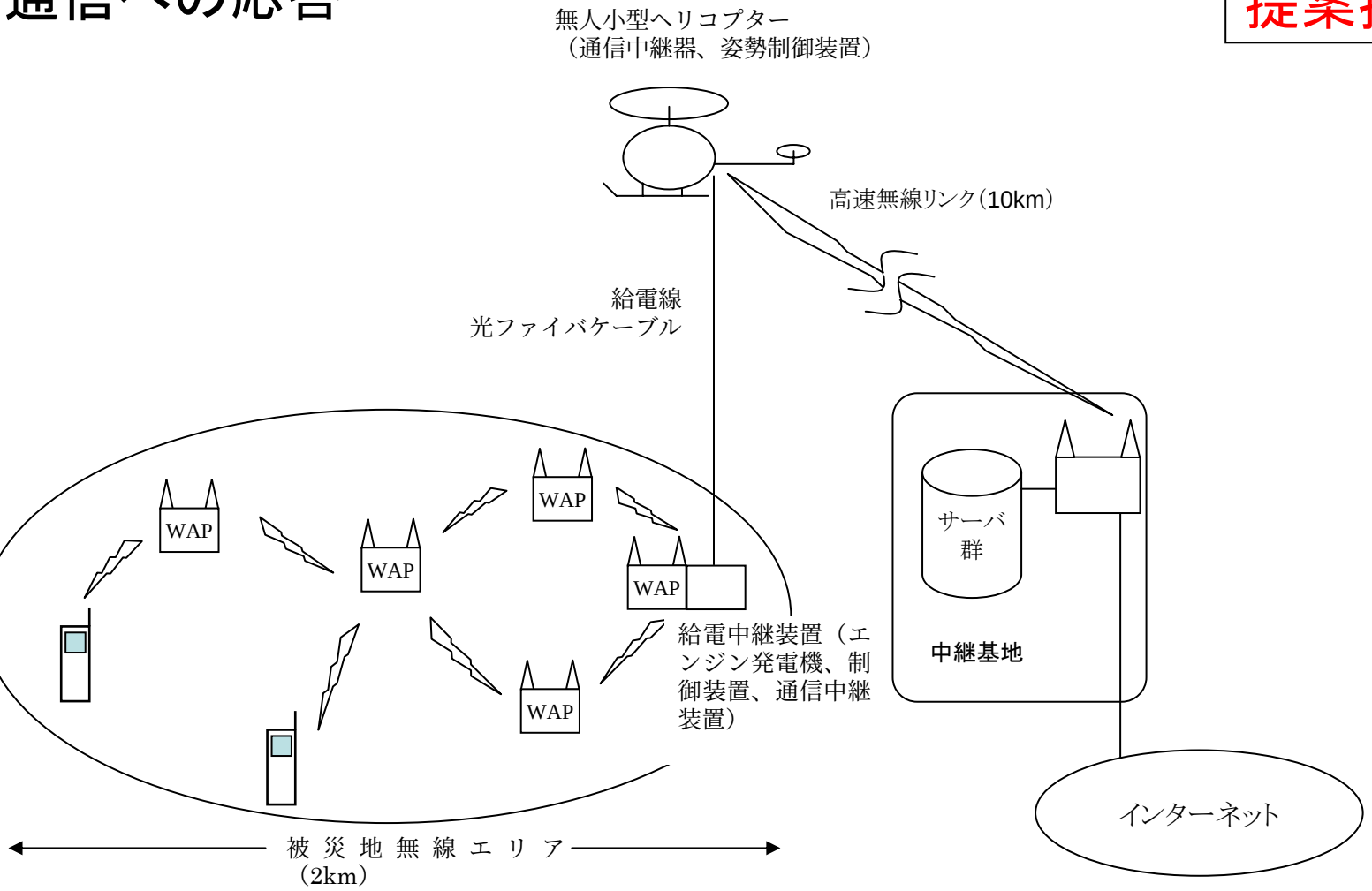


- WAP
  - ✓ アドホックモードで通信
  - ✓ 車両から電力供給
- 端末
  - ✓ インフラストラクチャモードで通信
  - ✓ 乗客の乗降に合わせて移動

WAP1

災害通信への応答

提案技術



通信設備が破壊された被災地

- 擬似メールサーバ
- 災害用HP
- 管理サーバ

WAPLの現状

・実装完了（FreeBSD）

WAPのEthernetエミュレーション

・実装中／実施中

NS2によるトラヒックシミュレーション

擬似メールサーバ

車車間通信特有のアドレス取得、アドレス解決

・検討中

WAPのインターネット接続／二重化

レスキュー隊と被災者の連絡方法

災害通信に関わるフィールド試験

IP電話，セキュリティ

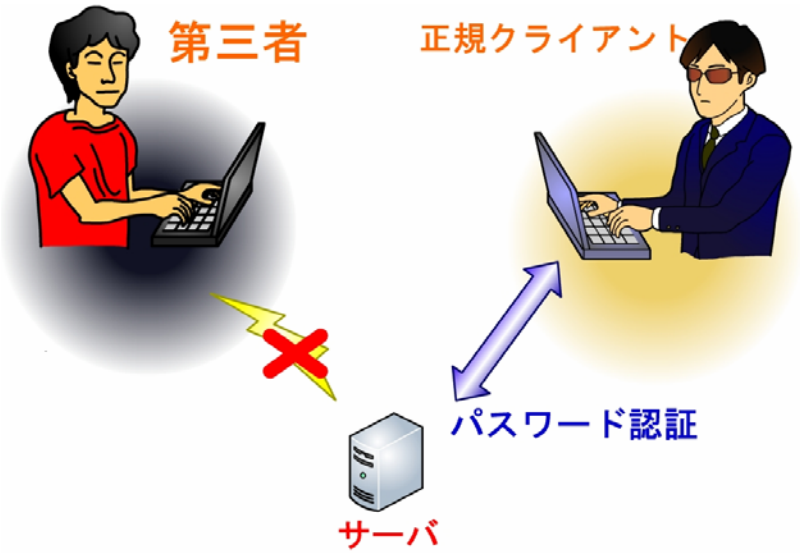
・IP電話だけはファイアウォールを安全に越えられる

・IP電話会議

・渡り歩きを検出する

・DoSの攻撃者を見つける

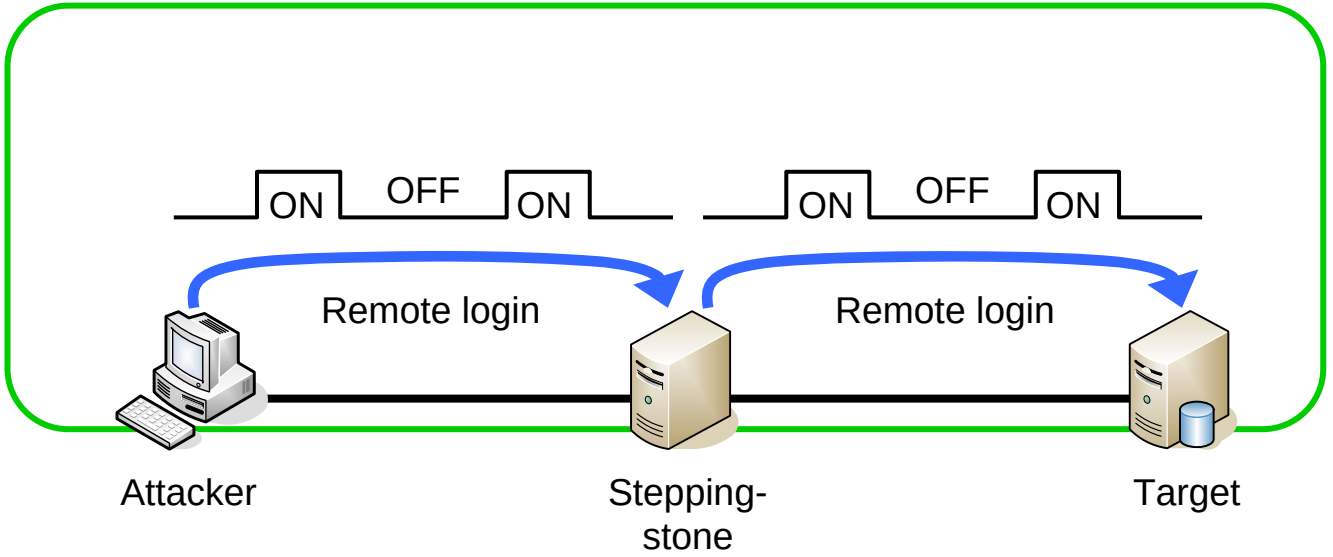
・企業向け公開鍵認証基盤



渡り歩きの検出（タイミングベース方式）

既存技術

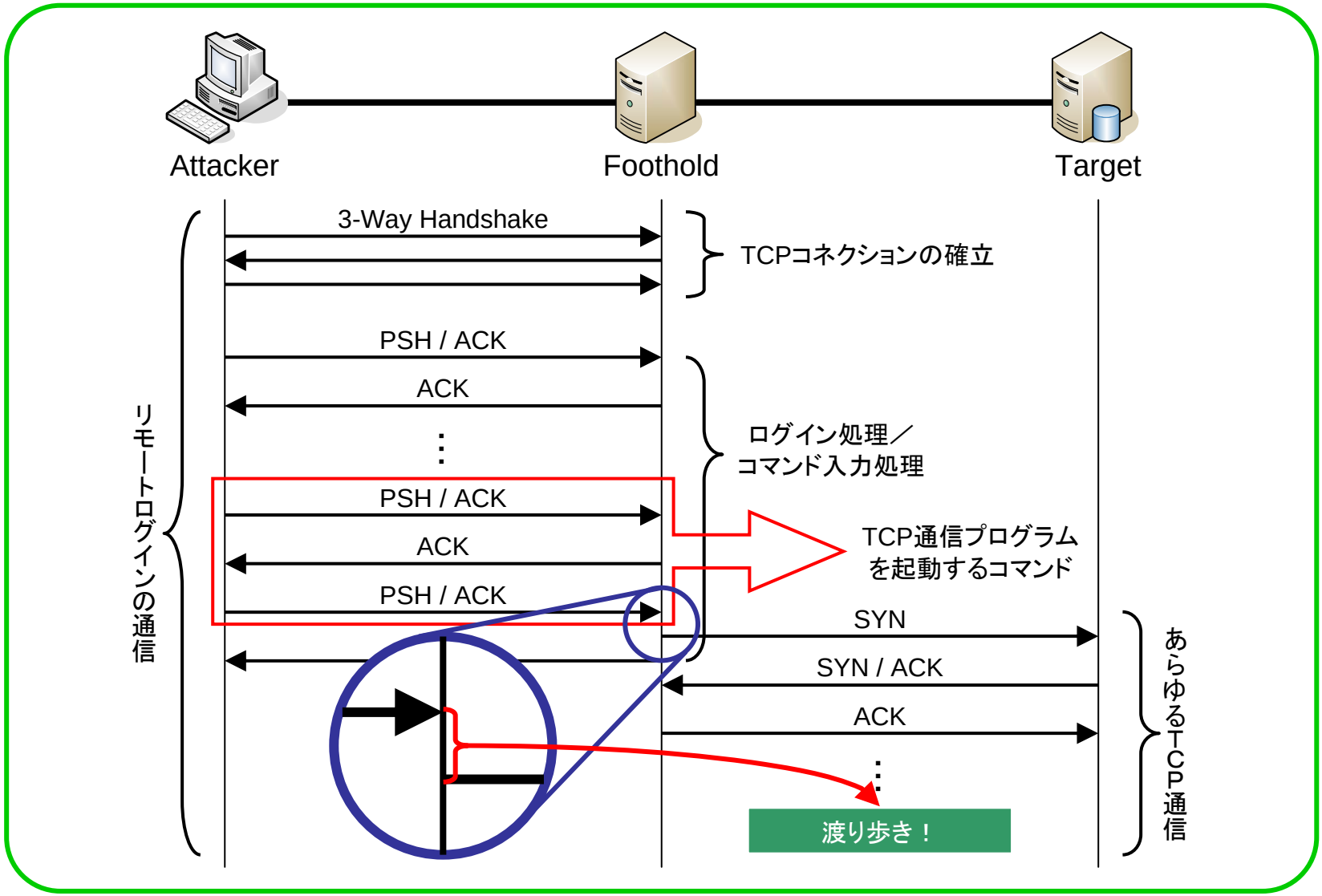
- リモートログインストロークの相関関係から踏み台攻撃を検出
  - キーストロークに特徴があることに着目
  - インタラクティブ型の踏み台攻撃のみ対象
  - 所定の時間以上の相関関係を見る必要あり



渡り歩きの検出（コネクション検出方式）

提案技術

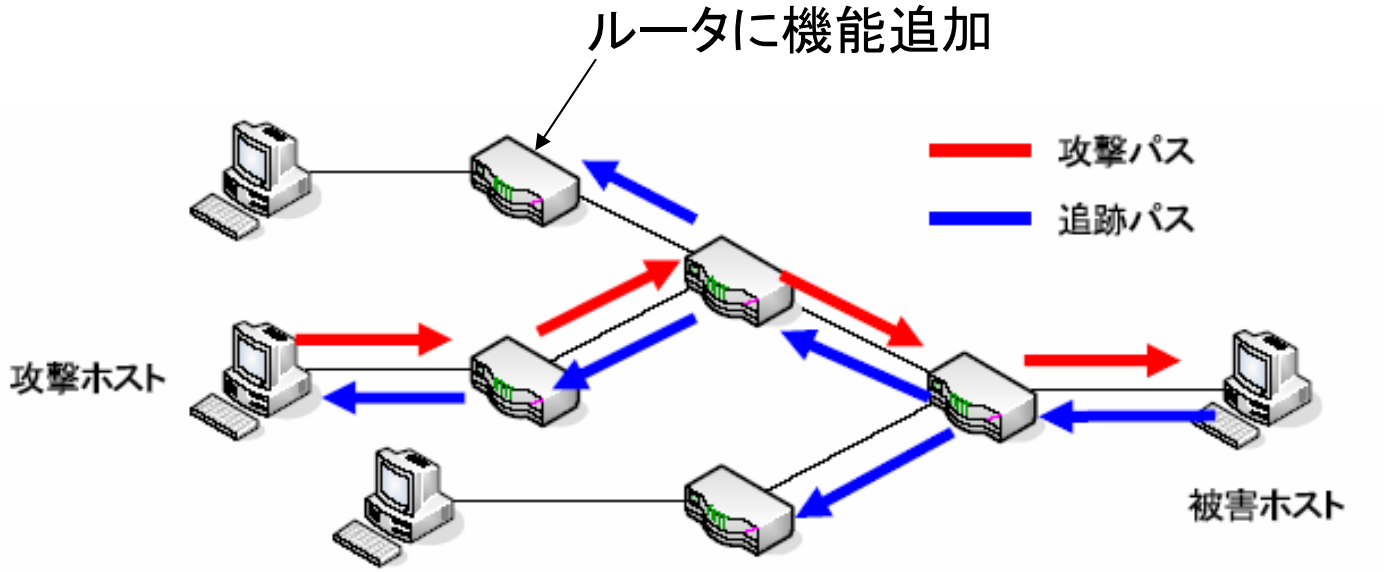
攻撃発生時にTCPコネクション確立要求が必ず送信されることに着目



リアルタイム性高い，あらゆるTCP通信に対応，見逃し率ゼロ

IPトレースバック（DoSの攻撃ホストを検出する技術）

既存技術

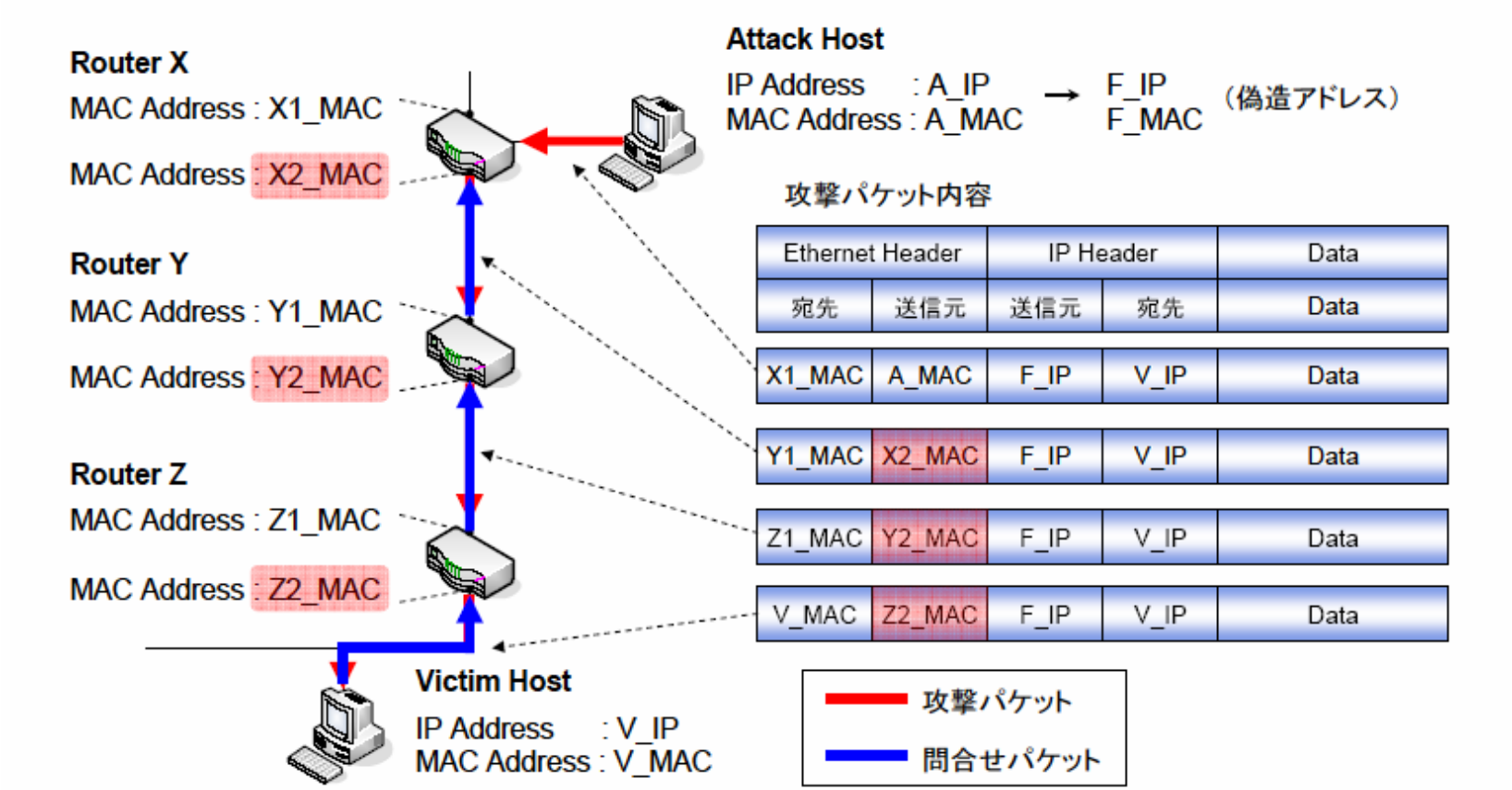


マーキング方式；
　通過パケットにある確率でマーキングを行い、被害ホスト側で攻撃ホスト側のエッジルータを統計的に解析する方式
　→膨大な情報量が必要
Hash-Based方式；
　全パケットのハッシュログを記録する方式
　→ルータへの負荷が大きい

MAC-Based IPトレースバック

提案技術

MAC情報を用いて上流ルータを特定する



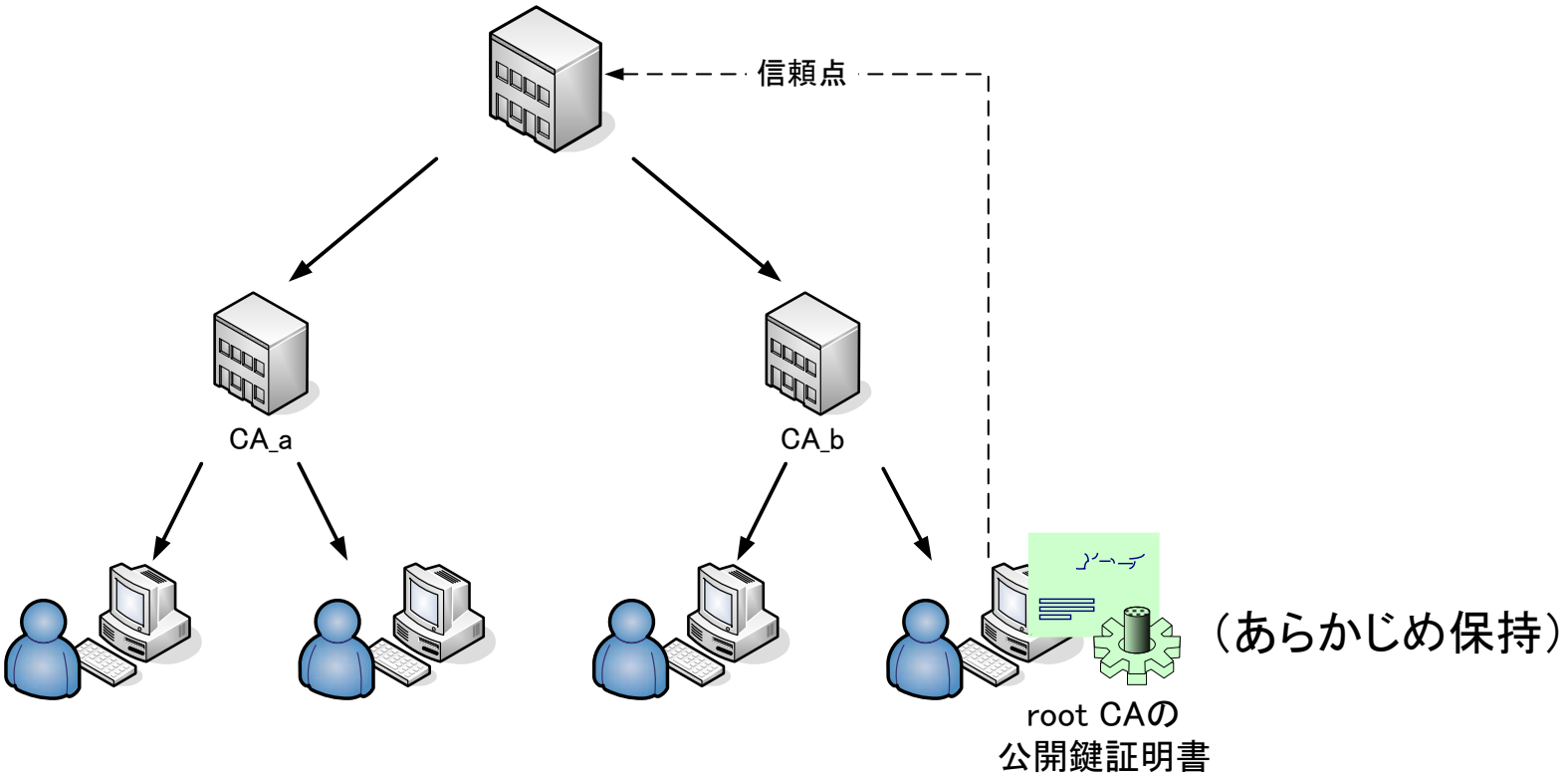
ルータの処理:

一定時間内にトラヒックの閾値を越えたパケットの上流MACアドレスを記憶する。

企業向け認証基盤(PKI)

既存技術

・信頼の関係を階層的に構築
・rootCAの公開鍵証明書を信頼の拠点とする
・証明書の失効はCRL(失効情報)により行う



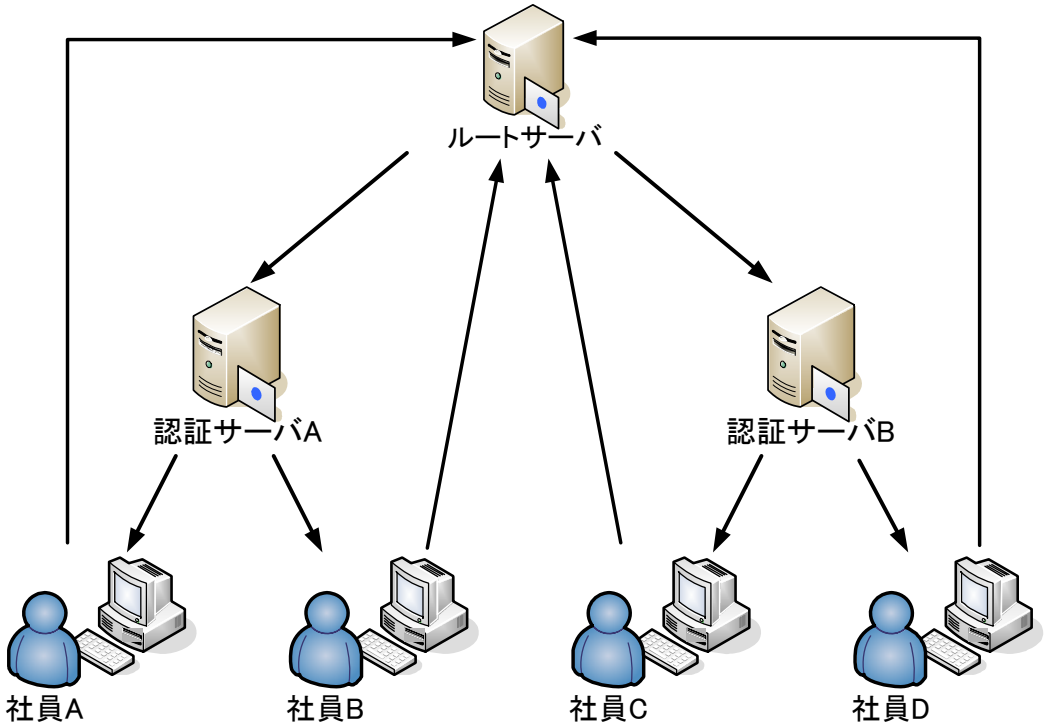
・rootCAの公開鍵証明書は偽造が可能
・証明書が最新のものとは限らない
・CRLの管理が必要

root CA

企業向け認証基盤（ASE; Authentication System for an Enterprise network）

信頼関係を環状にする
公開鍵証明書は発行者が保持し，自ら管理する
信頼関係はオンデマンドで検証する

提案技術

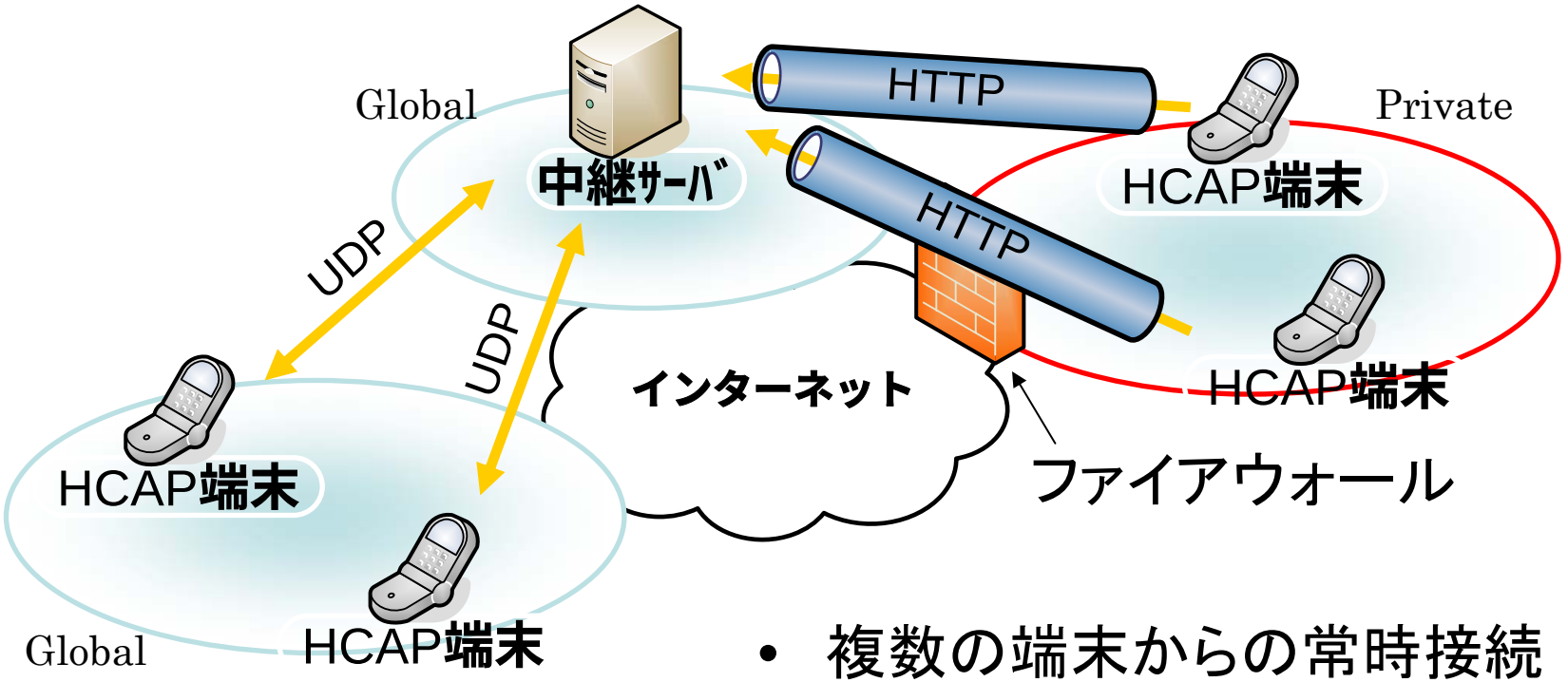


証明書の偽造は不可
失効情報の管理が不要
リアルタイム性に優れている

ファイアウォールを越えられるIP電話（HCAP）

既存技術

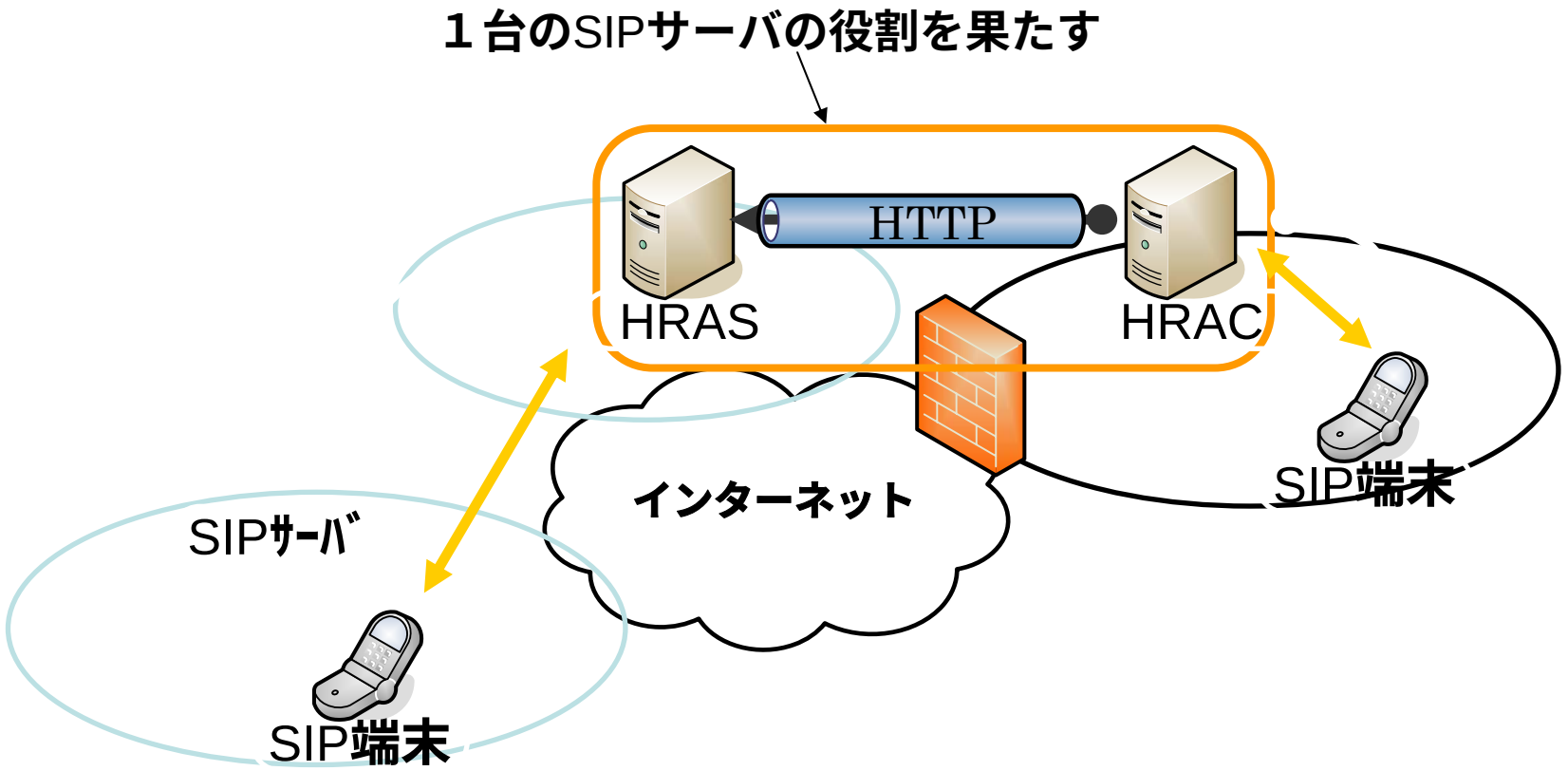
専用端末と中継サーバ間にHTTPトンネルを生成し、ダイアルと音声ストリームを中継する



- 複数の端末からの常時接続
  - FW上の無駄なトラヒック
  - 専用端末の導入

ファイアウォールを越えられるIP電話（SoFW）

提案技術



HRAS（Half Relay Agent Server）：**外部に設置**

HRAC（Half Relay Agent Client）：**内部に設置**

- 一般のSIP端末
- トンネルによるトラヒックを集束
- 既存の設備はそのまま

各テーマの状況

・渡り歩き・・・実装／評価済み

・MAC-Based　IPトレースバック・・・実装済み

・企業向け認証基盤・・・検討中

・SoFW・・・ほぼ実装済み

その他

・リング型IP電話会議・・・検討を開始