研究内容のご紹介

2009年9月4日

名城大学理工学部
渡邊　晃

研究テーマ

ユビキタスネットワーク
- フレキシブルプライベートネットワークの提案
- NAT越え
- 移動通信

メッシュネットワーク
- 災害時の通信対策
- 無線LANのインフラ構築

セキュリティ
- 踏み台攻撃対策
- DoS攻撃対策
- ウイルス対策

フレキシブルプライベートネットワーク（FPN）とは？

FPN（Flexible Private Network）とはユビキタスネット社会に向けて、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、ネットワークのあるべき姿を示したものです。FPN は以下の 3 種類の透過性を満たすネットワークです。

位置透過性

ノードやネットワークが移動しても、システムが動的にその変化を学習してセキュア通信グループの関係が維持される機能

移動透過性

通信中にノードが移動しても、確立されたコネクションを維持し続けて通信を継続できる機能

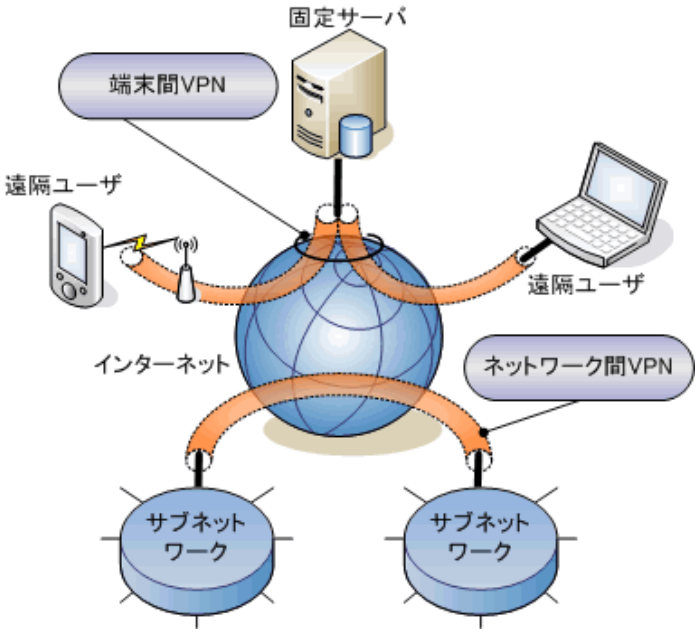
アドレス空間透過性

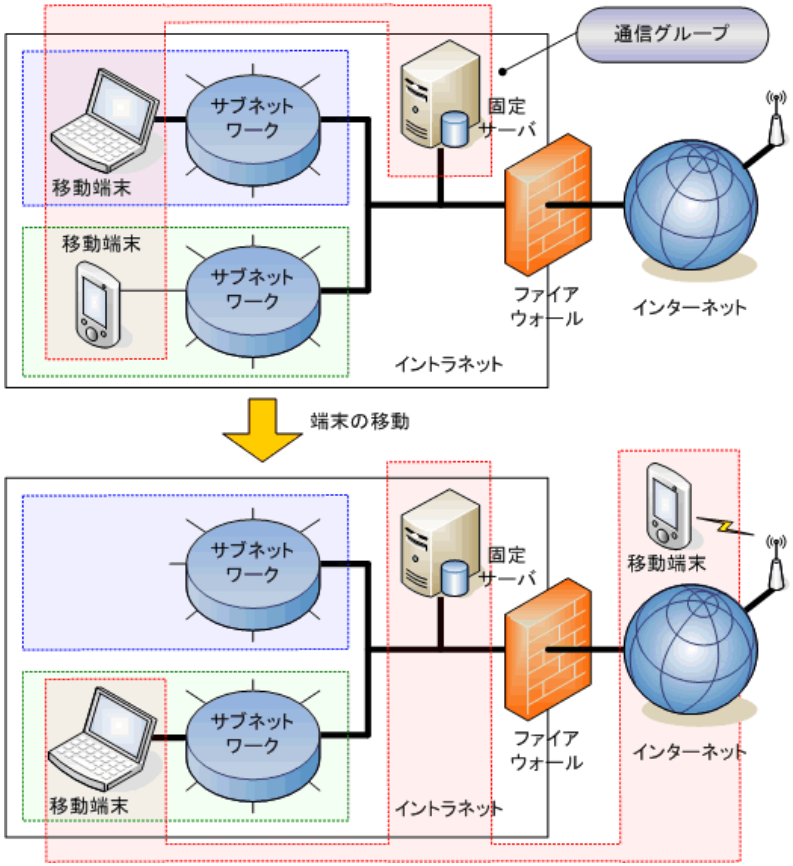
アドレス体系が異なるノード同士でも自由に通信できる機能

当研究室は FPN という統一した概念のもとで研究開発を行ってきました。Mobile PPC と NAT-f は FPN の研究成果の中から産まれました。

VPNからFPNへ

VPNでは、
・サブネットワークの位置が固定
・通信開始はリモート端末側からのみ





FPNでは、
・すべてのサブネット、ホストが動くことを想定
・ネットワークが階層構造になっていてもよい
・IPv4（プライベートアドレス、グローバルアドレス）、IPv6が混在してもよい

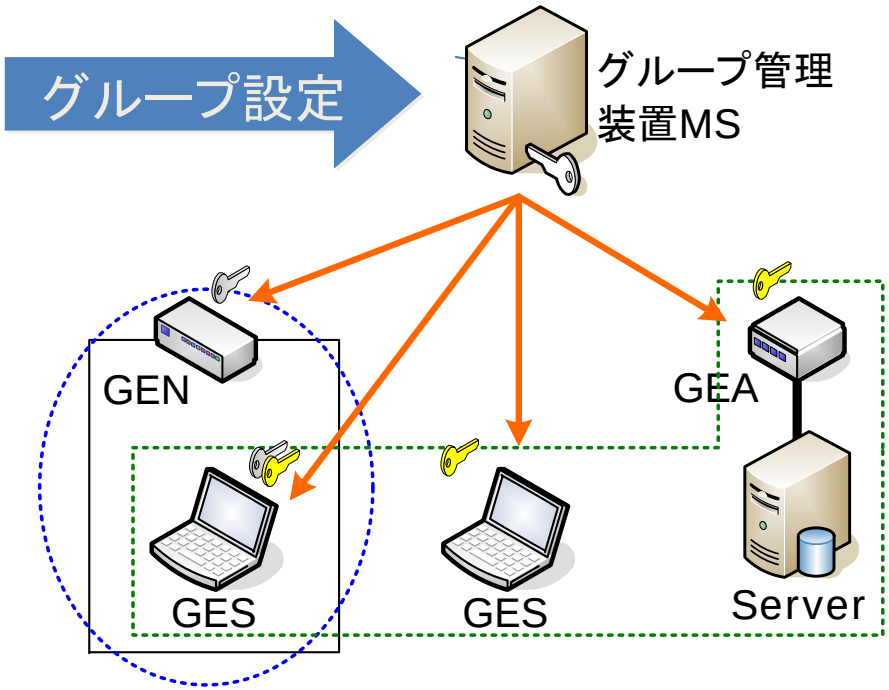
GSCIP (Grouping for Secure Communication for IP)

FPNを実現するためのアーキテクチャ
3種類の透過性を実現するためのプロトコルの集合

通信グループの定義方法

同一通信グループに同一の暗号鍵を対応づける
IPアドレスに依存しないグルーピングが定義できる
サブネット/ホストが移動してもグループの定義を維持できる

管理者

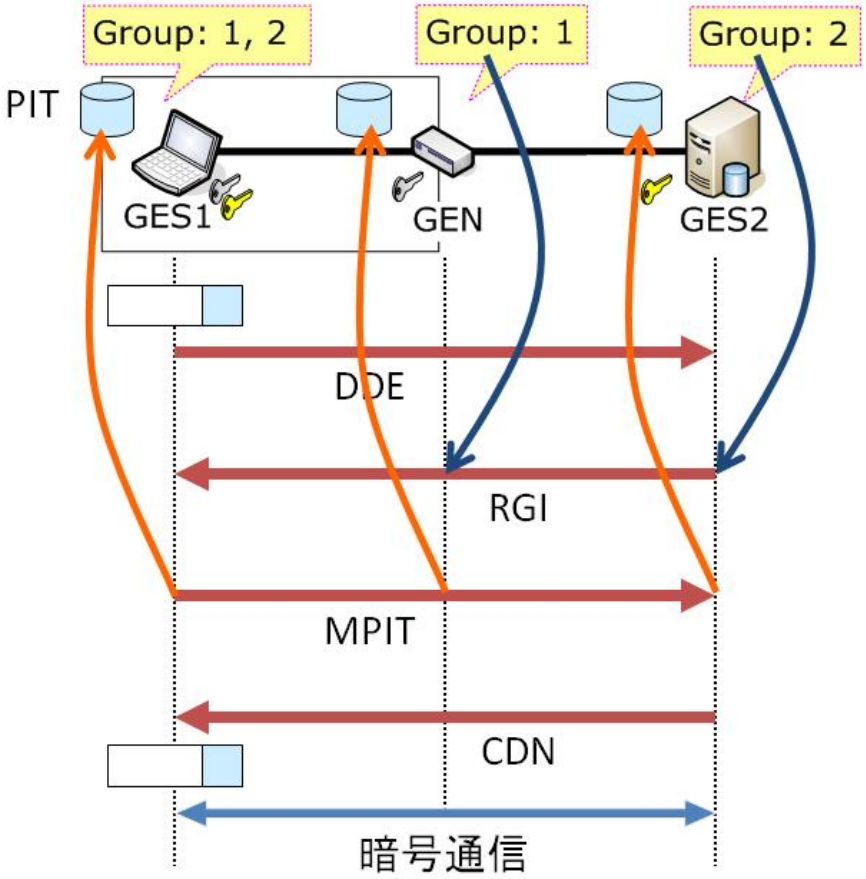


GE（GSCIP Element）

- **GES**（Software型）
  - ＞ クライアントに実装
- **GEN**（Network型）
  - ＞ ルータとして動作
- **GEA**（Adapter型）
  - ＞ ブリッジとして動作

DPRP (Dynamic Process Resolution Protocol)

位置透過性を実現するためのプロトコル



通信開始時に通信経路上のGEが情報交換し、GEの動作を動的に決定する。

移動しても通信グループが維持される
管理者にはいっさい負担がかからない

特長

- 個人のグループとサブネットワークのグループが共存できる
- 管理負荷が大幅に軽減される
- 高スループット

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の実装と評価
情報処理学会論文誌，Vol.47，No.11，pp.2976-2991，Nov.2006.

増田 真也，鈴木 秀和，岡崎 直宣，渡邊 晃
NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装
情報処理学会論文誌，Vol.47，No.7，pp.2258-2266，Jul.2006.

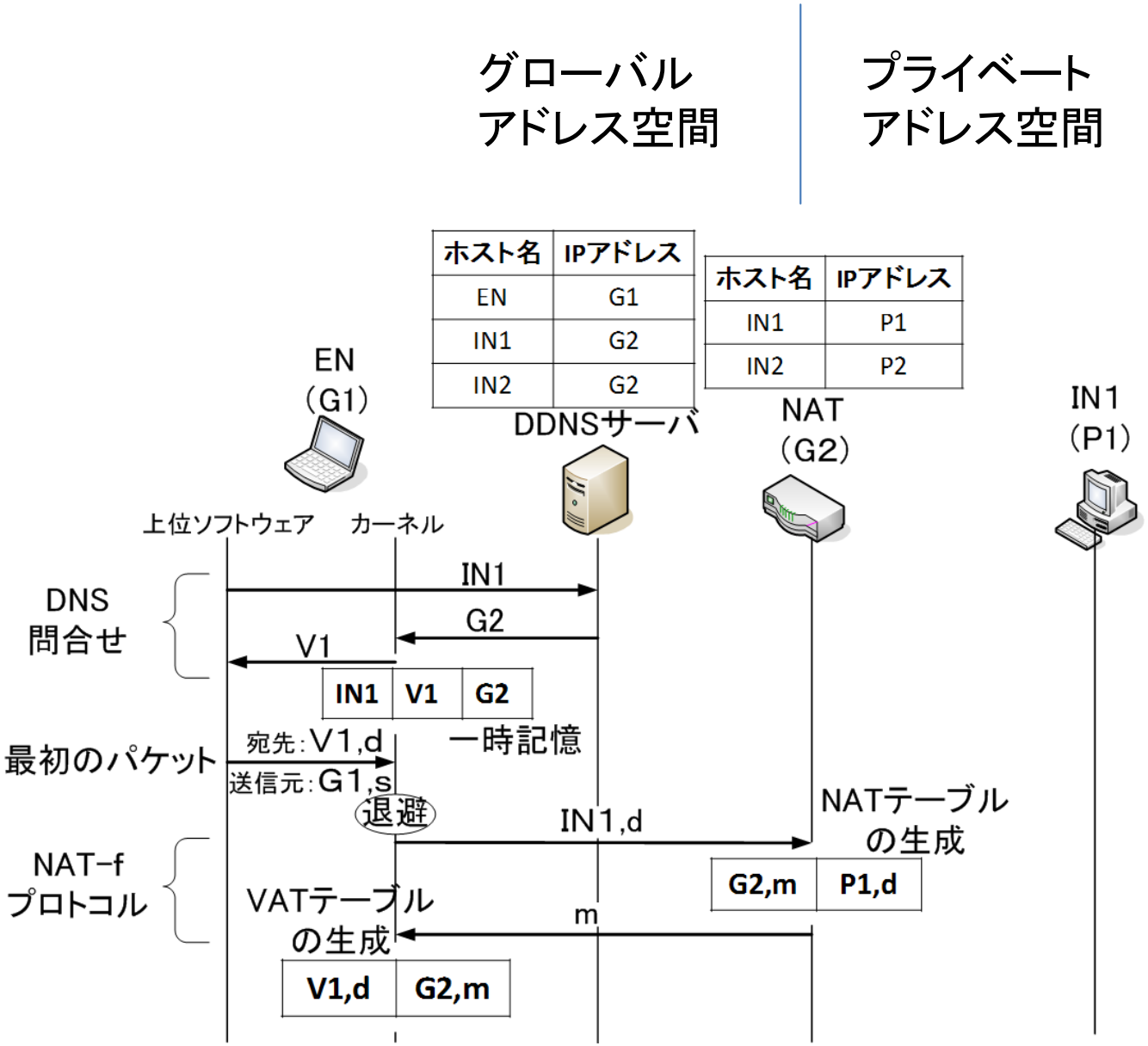
NAT-f (NAT-free protocol)

NAT越えを実現するプロトコル（グローバルアドレス空間からの通信開始）

IN1の名前解決でNATのアドレスを取得
ENは仮想アドレスを生成

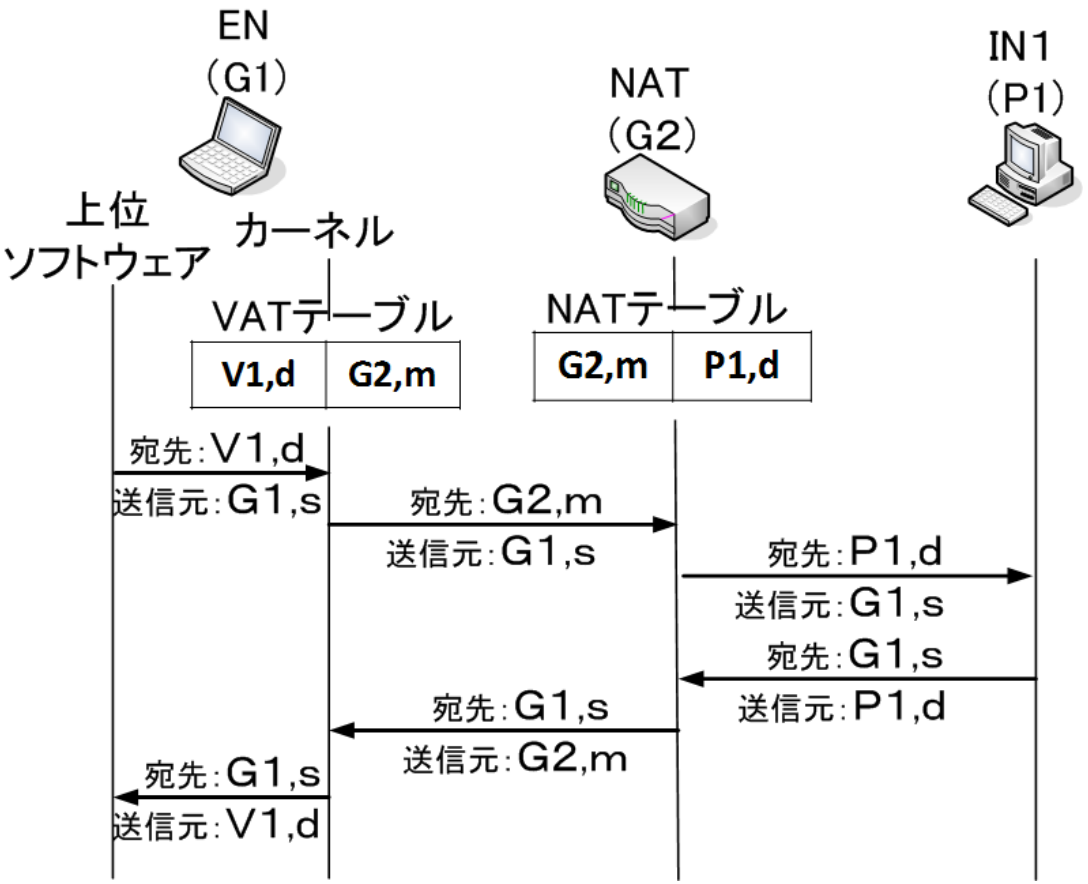
通信開始時にENとNATが情報交換し、NATテーブルを生成

ENはNATテーブルに合わせてVATテーブルを生成



NAT-fつづき

通信時のアドレス変換の様子



VATとNATでアドレス/ポート変換することにより、EN側からの通信開始が可能

特長

- 第三の装置が不要
- アプリケーションに影響がない
- 高スループット
- NATの効用を損なわない

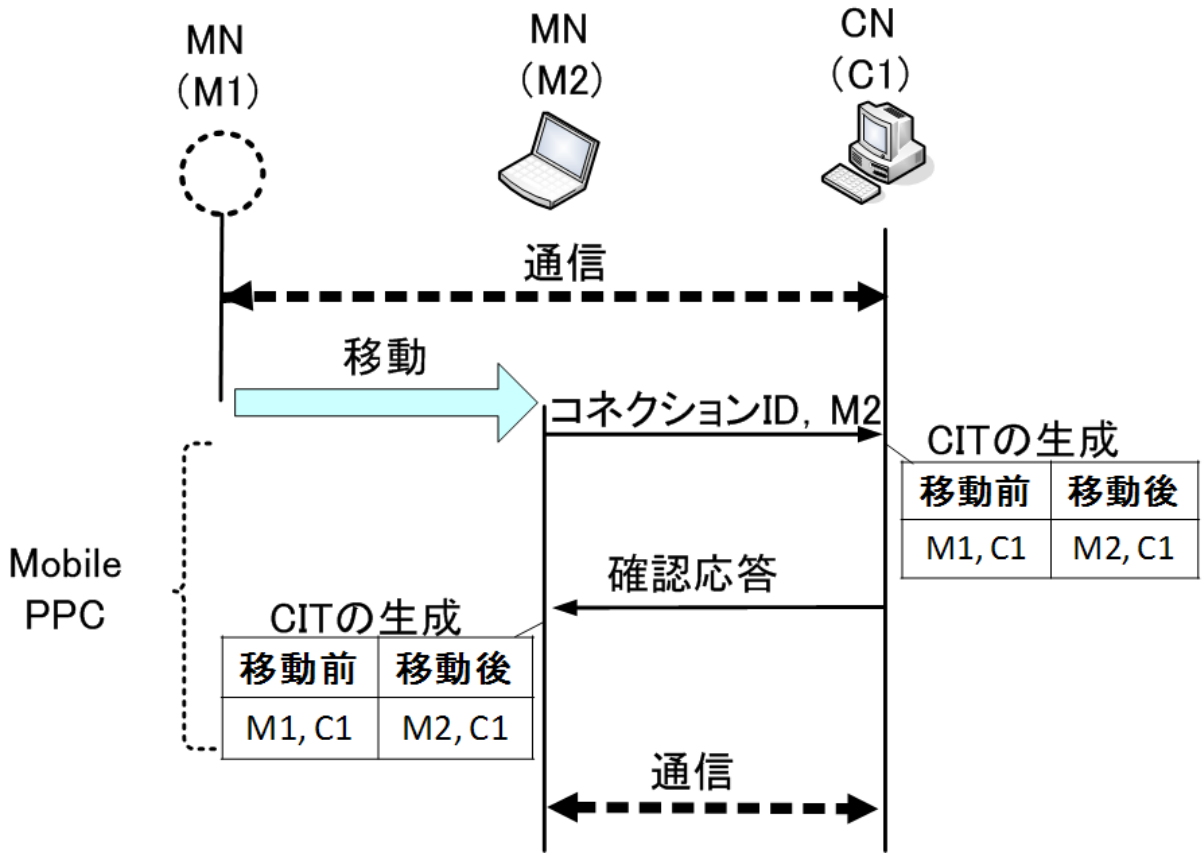
•鈴木 秀和，宇佐見　庄五，渡邊 晃
外部動的マッピングによりNAT越え通信を実現するNAT-f の提案と実装
情報処理学会論文誌，Vol.48，No.12，pp.3949-3961，Dec.2007.

•鈴木 秀和，渡邊 晃
プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式
•電子情報通信学会論文誌(B)，Vol.J92-B，No.1，pp.13，Jan.2009.

Mobile PPC (Mobile Peer to Peer Communication)

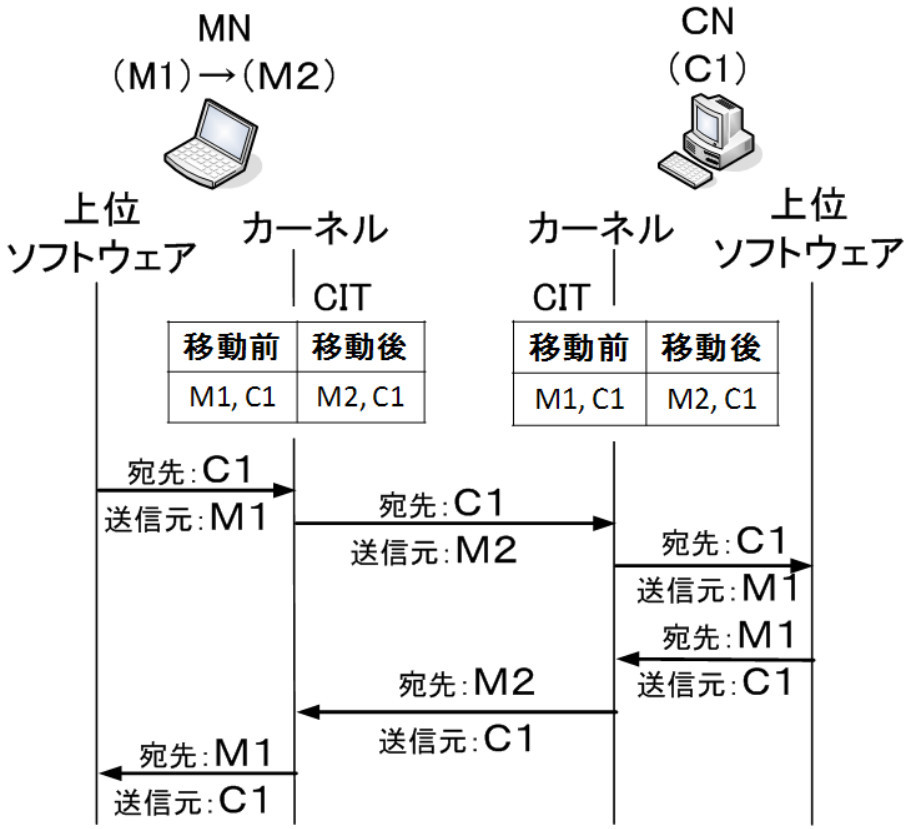
通信中に移動しても通信を継続できるためのプロトコル

移動時にMNがCNに移動情報を通知
MNとCNはIP層にアドレス変換テーブル（CIT)を生成



Mobile PPCつづき

アドレス変換の様子



IP層でアドレス変換することにより、MN、CNともアドレスが変化したことに気づかないで通信が継続される

特長

- 第三の装置が不要
- アプリケーションに影響がない
- 高スループット
- 既存端末と上位互換

•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の提案と実装
情報処理学会論文誌, Vol.47, No.12, pp.3244-3257, Dec.2006.

•金本 綾子, 鈴木 秀和, 伊藤 将志, 渡邊 晃
IPv4移動体通信システムにおけるパケットロスレスハンドオーバの提案
情報処理学会論文誌, Vol.50, No.1, pp.133-143, Jan.2009.

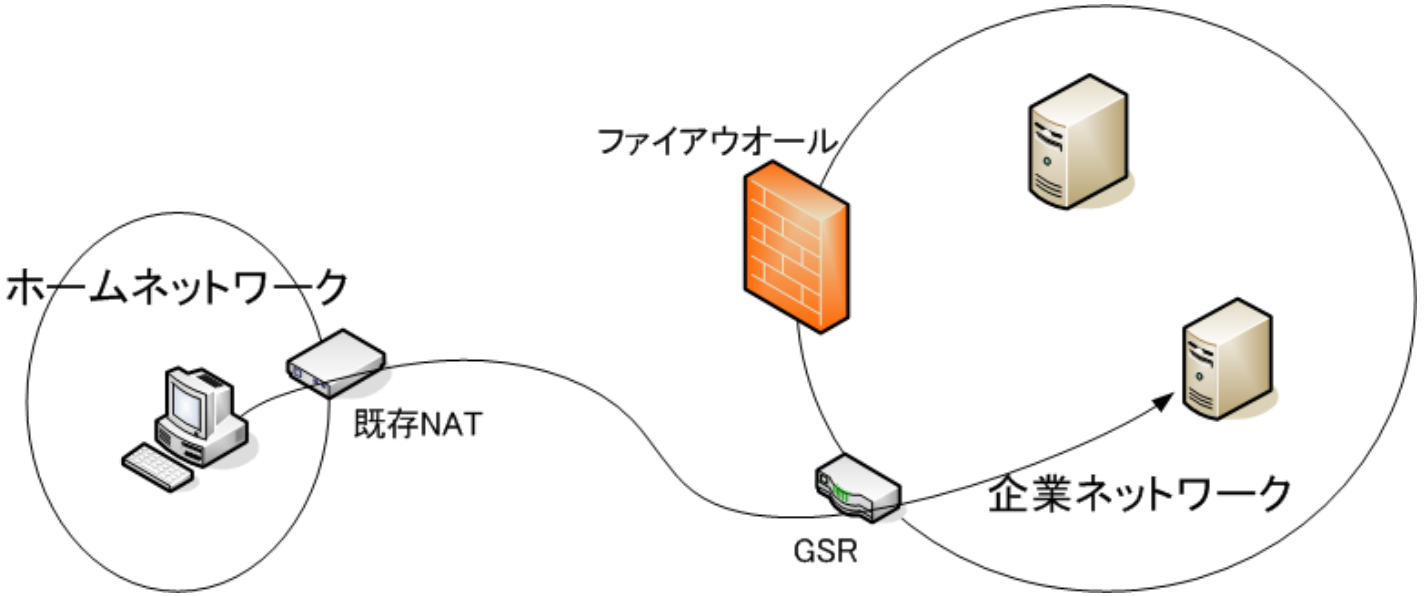
•瀬下 正樹, 鈴木 秀和, 伊藤 将志, 渡邊 晃
分割Diffie-Hellman鍵交換による移動ノードの鍵共有方式の提案
情報処理学会論文誌, Vol.50, No.7, pp.1725-1734, Jul.2009.

•坂本 順一, 鈴木 秀和, 伊藤 将志, 宇佐見　庄五, 渡邊 晃
プライベートアドレスによるネットワークモビリティを実現するMobile NPCの提案
情報処理学会論文誌, Vol.50, No.10, pp.1-13, Oct.2009.

現在の研究テーマ

GSRA (Group-based Secure Remote Access)

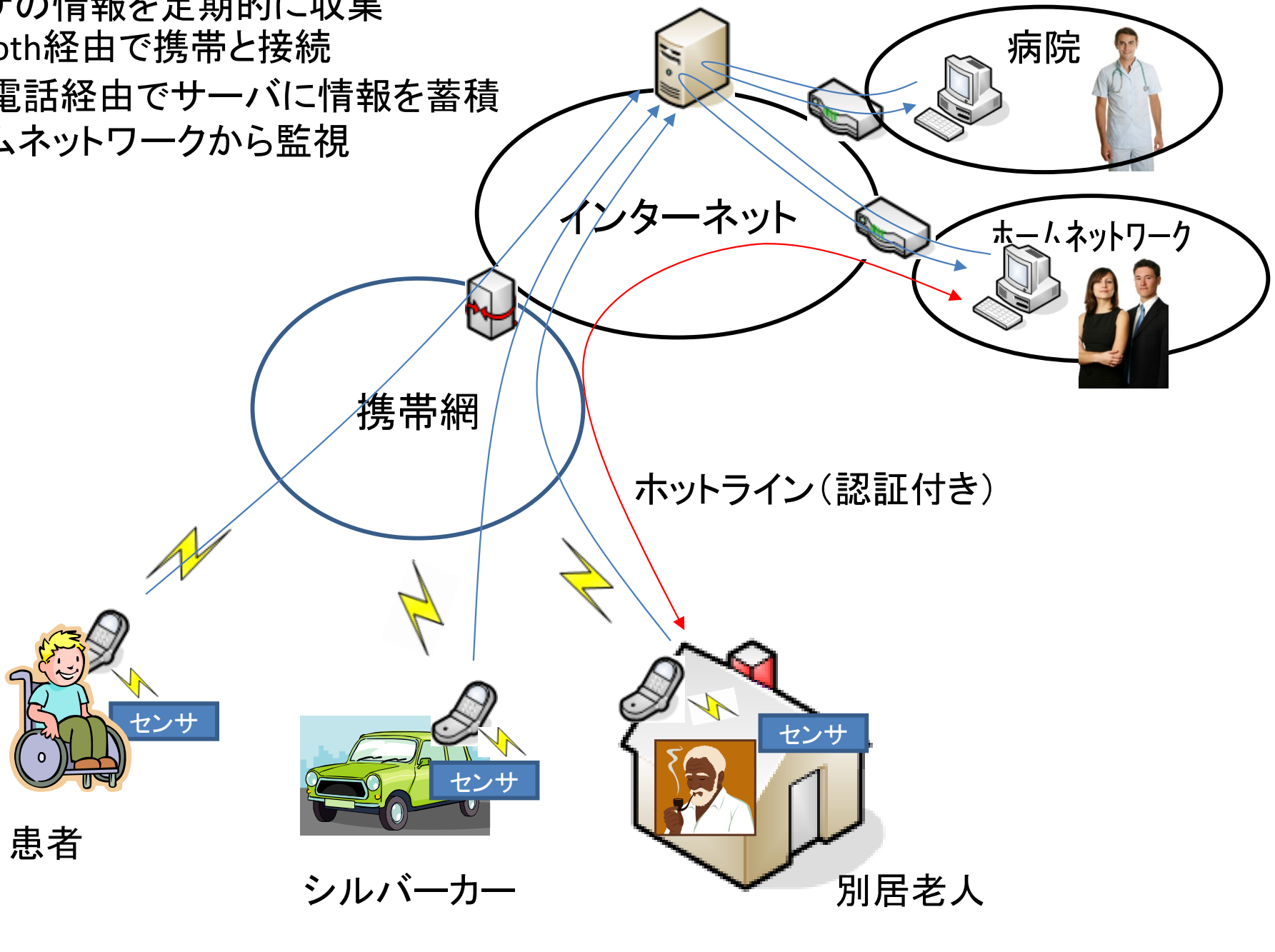
家庭ネットワークから組織内のサーバに安全にアクセス
安全な裏口
家庭内NATは既存のもの
サーバは組織内の任意の場所



学内ネットワークで試使用の予定
（授業のレポート提出、オフィスのダウンロードサービスなど）

高齢者/弱者を見守るシステム

・センサの情報を定期的に収集
・blutooth経由で携帯と接続
・携帯電話経由でサーバに情報を蓄積
・ホームネットワークから監視



IPv6のアドレス隠蔽システム

外部から組織内のネットワーク構成を隠蔽するしくみ
エンドエンドのリーチャビリティを持つ（既存NATとの違い）

解決すべき課題：
IPv4グローバルアドレスの不足　→　IPv6の導入は必須
ただし、そのまま導入すると組織内部のアドレスが見えるため安全性が低下する

既存の対策：
サイトローカルアドレスの導入
（IPv4のプライベートアドレスに対応するアドレス）
　→　IETFにて却下（理由：アドレス重複の可能性、移動困難、NATの出現を助長する）

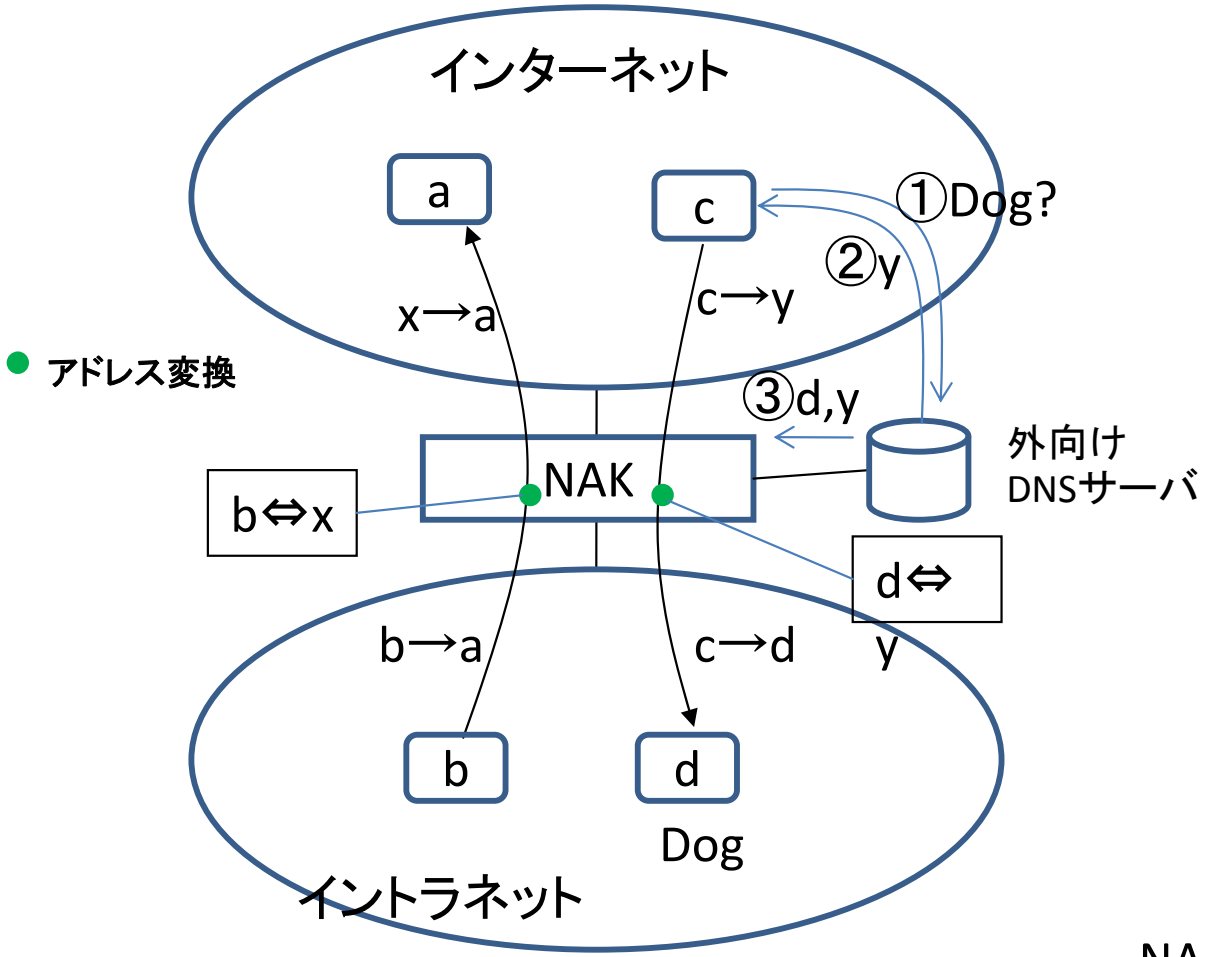
一時アドレスの導入
（IPv6ホストのIPアドレスをランダムに生成し、ホストを特定できなくするしくみ）
　→　サブネットIDは隠蔽できないのでネットワーク構成までは隠蔽できない

一時アドレスの構成

48ﾋﾞｯﾄ ｸﾞﾛｰﾊﾞﾙﾙｰﾃｨﾝｸﾞﾌﾟﾚﾌｨｯｸｽ （オープンな情報）	16ﾋﾞｯﾄ ｻﾌﾞﾈｯﾄID 匿名化不可	64ﾋﾞｯﾄ ｲﾝﾀﾌｪｰｽID 一時アドレスにより匿名化可能

案1：ゲートウエイ方式
　ゲートウエイで変換テーブルを持ち、アドレス変換する方式

返還テーブルの生成方法：
・中から外への通信
　最初の通信時に変換テーブルを生成
・外から中への通信
　DNS問い合わせ時に任意のアドレスを回答同時に変換テーブルを生成



利点：
・変更ヵ所はゲートウエイ部分のみ

欠点：
・メッセージにIPアドレスが含まれるアプリケーション（SIPなど）への対応策

NAK; Network Address Keeper

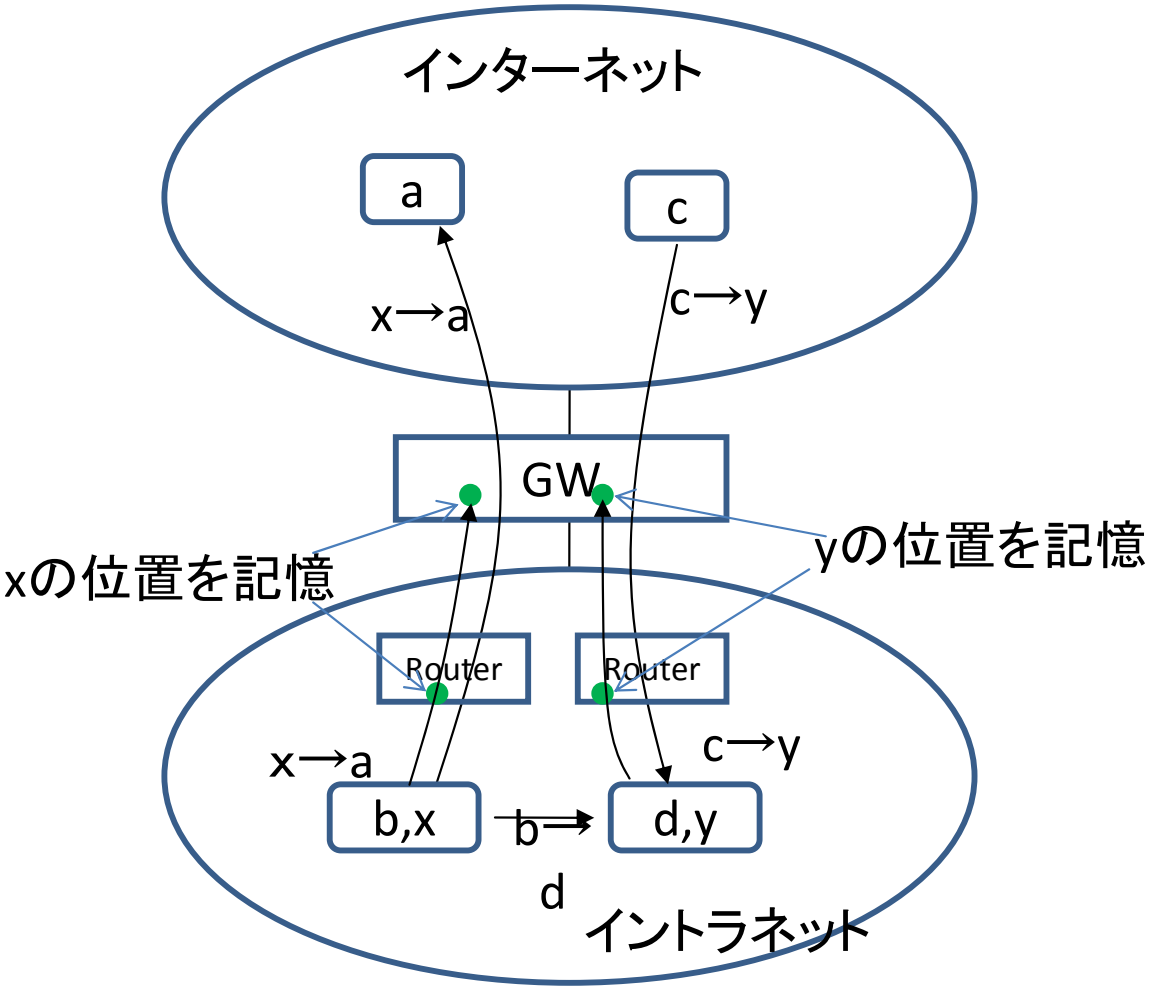
案2：エンドエンド方式

エンドノードが一般のアドレスと外部通信用の2つのアドレスを持つ方式

ルータがエンドノートの位置を記憶する方法（案）：

・電源投入時にホストがGWに向けて記憶用パケットを送信

・上記パケットを受信したときにホストの位置を記憶



利点：

・どのようなアプリケーションにも対応できる

欠点：

・GW、ルータ、ホストが機能を保持する必要がある

QUESTION

・IPv6へ移行するのか。その方法は
・CGNを導入するのか
・携帯網をどう考えているのか。共存or対抗
・移動透過性の重要度は。携帯網があれば不要なのか
・企業内アドレスの隠蔽はどれほど要求されるのか