Vol.2010-MBL-55 No.9
2010/9/2

[奨励講演] 安全性と移動性を両立する柔軟なグループ通信アーキテクチャに関する研究

鈴木秀和[†1]　渡邊晃[†1]

ユビキタスネットワークでは，暗号化通信，移動通信，エンドツーエンド通信を同時に実現することが重要である．本研究では安全性と柔軟性を両立させたネットワークの概念として FPN（Flexible Private Network）を提唱し，これを IPv4/IPv6 ネットワークで実現するための通信アーキテクチャとして GSCIP（Grouping for Secure Communication for IP）を提案する．本稿では GSCIP の概要および提案アーキテクチャによる IPv4 ネットワーク特有の移動透過通信システムについて紹介する．

[Encouragement Talk] A Study on Flexible Group Communication Architecture Compatible with both Security and Mobility

Hidekazu Suzuki[†1] and Akira Watanabe[†1]

In ubiquitous networks, it is important to simultaneously realize an encrypted communication, a mobile communication and end-to-end communication. The study advocates Flexible Private Network (FPN) as the concept of a network which balances security with flexibility, and we propose a communication architecture GSCIP (Grouping for Secure Communication for IP) that can realize an FPN in IPv4/IPv6 networks. This paper introduces the outline of GSCIP and an IPv4-specific mobility system based on the proposed architecture.

†1 名城大学理工学部
Faculty of Science and Technology, Meijo University

⋆1 本稿は会誌「情報処理」（Vol.52 No.1）の特集「研究会推薦博士論文速報」に掲載予定の内容に関するものである．なお，紙幅の都合により提案方式の詳細は省略している．プロトコル仕様や性能評価結果については，関連する参考文献を参照されたい．

1. はじめに

近年の携帯端末の高性能化・小型化により，いつでも，どこでも，誰でもネットワークにアクセスできるユビキタスネットワーク技術への期待がますます高まっている．ユビキタスネット社会では，あらゆるユーザが自宅，外出先，職場などを自由に移動しながら個人間の通信を行う状況が想定されるため，通信の安全性とユーザの移動性を両立できる技術が求められる．これらの要求を満たす技術として IPsec[1] や MobileIP[2),3)] などがあるものの，IPv6 ネットワークでの運用を前提としているものが多いため，エンドユーザレベルでの利用は進んでいない．IPv4/IPv6 環境が当分の間混在することを鑑みると，両環境において暗号化通信，移動透過通信，エンドツーエンド通信を同時に実現することが重要である．

本研究では上記 3 つの通信を同時に実現できるネットワークの概念として FPN（Flexible Private Network）を提唱し，IPv4/IPv6 混在環境で FPN を実現するためのグループ通信アーキテクチャGSCIP（Grouping for Secure Communication for IP ; ジースキップと発音）を提案する．暗号鍵と 1 対 1 に対応したセキュア通信グループをメンバ間で構築し，このメンバ間では暗号化通信，移動透過通信，エンドツーエンド通信に必要な情報をユーザが設定するのではなく，システムが自律的にネットワーク構成の変化を学習して動的に設定することができる．

本論文は主に 4 つの研究成果を取りまとめたものであり，GSCIP は下記プロトコルにより構成されている．

(1) エンドノード間の通信に先立ち，認証および通信の暗号化に必要な情報を相互に交換し，設定情報を動的に生成するプロトコル DPRP（Dynamic Process Resolution Protocol）の提案[4]．
(2) NAT やファイアウォールを通過することが可能で，本人性確認，パケットの完全性保証，高スループットを実現する暗号化通信方式 PCCOM（Practical Cipher Communication）の提案[5]．
(3) アドレス変換処理により IP アドレスの変化を隠蔽するエンドノード主導型移動透過性プロトコル Mobile PPC（Mobile Peer-to-Peer Communication）の提案[6]．
(4) 外出先から自宅の NAT（Network Address Translator）のポートマッピングを行う外部動的マッピング方式の提案と NAT-f（NAT-free）プロトコルの設計[7]．

本稿では紙幅の関係上，FPN と GSCIP の概要および上記 (3)・(4) を融合した IPv4 ネットワーク特有の移動透過通信システムについて述べる．

Vol.2010-MBL-55 No.9
2010/9/2

2. FPN と GSCIP

2.1 FPN（Flexible Private Network）

図 1 に FPN の概念を示す．FPN では個人単位とドメイン単位の要素が混在する環境に対してセキュア通信グループの定義ができる．同一グループに属するノード間の通信はその安全性が保証され，異なるグループに属するノードからのアクセスを拒否したり，平文で通信したりすることができる．ノードおよびドメインは複数のグループに多重帰属することが可能で，個人単位やドメイン単位というグループの違いを意識する必要はない．またセキュリティドメインが階層的に構築されていたり，セキュリティドメイン内に異なるグループに属するノードが存在するような環境（多段構成ネットワーク）であってもかまわない．

FPN は上記に加えて，以下に示す位置透過性，移動透過性，アドレス空間透過性を同時に実現する．

- **位置透過性（Location Transparency）**
  ノードやドメインは移動可能であり，かつノードが特定のドメインの内外を移動するなどしてネットワーク構成が変わっても，あらかじめ定義されているグループの関係は維持される．このときグループの設定情報や暗号化通信に必要な情報をユーザが更新する必要はなく，システムが自動的にネットワーク構成の変化を学習する．位置透過性は暗号化通信を低い管理負荷で実現するために必要な機能である．
- **移動透過性（Mobility Transparency）**
  ノードは通信中の状態において移動することもありうる．通信中に別のネットワークへ移動したり，複数の通信デバイスを切り替えたりすると，ノードの IP アドレスが変化するため，そのままでは通信が継続できない．上位アプリケーションに対して IP アドレスの変化を隠蔽することにより，通信の継続を実現できる．移動透過性は快適な移動通信を実現するために必要な機能である．
- **アドレス空間透過性（Address Area Transparency）**
  IPv4 の通信環境においては，NAT によりプライベートアドレス空間がグローバルアドレス空間から隠蔽されるため，グローバルアドレス空間側からプライベートアドレス空間側のノードに対して通信を開始することができない（NAT 越え問題と呼ばれている）．NAT とノードが連携することにより，アドレス空間の違いを意識することなく自由に通信できる．アドレス空間透過性は IPv4 ネットワークにおいてエンドツーエンド通信を実現するために必要な機能である．

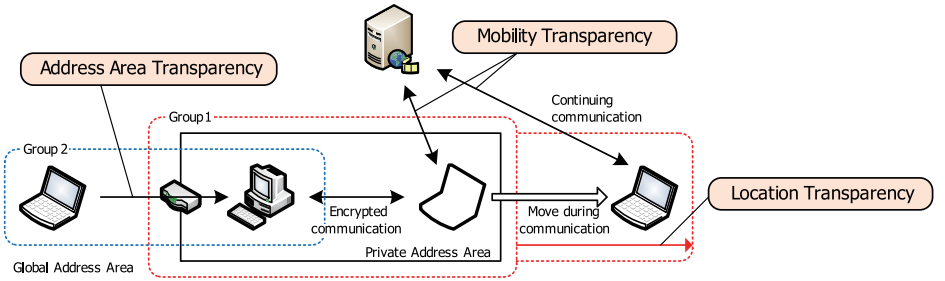

図 1 FPN の概念
Fig. 1 The concept of FPN.

表 1 GSCIP アーキテクチャを構成するプロトコル
Table 1 Protocols making up GSCIP architecture.

プロトコル	実現する透過性	実現する通信・機能
DPRP	位置透過性	端末間の認証および暗号化通信に必要な情報の動的生成
PCCOM	—	暗号化通信
Mobile PPC	移動透過性	移動透過通信
NAT-f	アドレス空間透過性	IPv4 ネットワークにおけるエンドツーエンド通信

FPN の概念を実現するには様々な方式がありうる．たとえば，既存技術では IPv6 ネットワークを基盤として IPsec と Mobile IP を利用する方法がある．IPv4 においても実現することもできるが，Mobile IP は IPv4 と IPv6 の互換性がないため別々のシステムを構成する必要がある．また，IPv4 ネットワークにおいてエンドツーエンド通信を実現するために，NAT 越え技術を適用する方法が考えられるが，従来の NAT 越え技術は IPsec や Mobile IP との連携を考慮せずに検討されている．IPsec や Mobile IP は NAT との相性が悪く，NAT 越えを行うために別途カプセル化処理などを行う必要がある[8)–10)]．したがって，これらの技術と親和性を保ちながら連携することが可能か別途議論する必要がある[11),12)]．

2.2 GSCIP（Grouping for Secure Communication for IP）

本研究では FPN を実現するために，統一した概念のもとに**表 1** に示すプロトコルを新たに定義し，これらを統合してグループ通信アーキテクチャGSCIP として設計する．各プロトコルは IPv4/IPv6 のいずれにおいても同様のアーキテクチャを採用しており，両者の互換性を有する設計となっている．さらに，個々のプロトコルが連係して動作することはもちろん，単独で動作することも可能である．

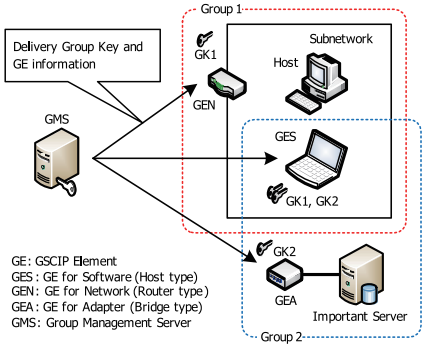

図 2 通信グループの定義方法
Fig. 2 Definition method of communication group.

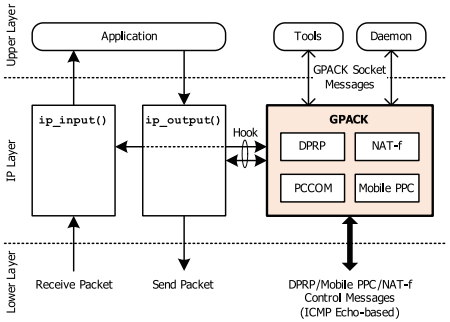

図 3 GSCIP のシステム構成
Fig. 3 System configuration of GSCIP.

図 2 に GSCIP の基本となる通信グループの定義方法を示す．GSCIP におけるグループの構成要素を GE（GSCIP Element）と呼び，ソフトウェアをインストールして実現するホストタイプの GES（GE for Software），サブネットを構成するルータタイプの GEN（GE for Network），重要なサーバの直前に設置して GES と同じ役割を果たすブリッジタイプの GEA（GE for Adapter）がある．GEN の配下に存在する一般ノード（Host）は，GEN により一括して保護される．

GSCIP では同一の暗号鍵を所持する GE の集合を同一グループとして定義する．この暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．グループとグループ鍵を 1 対 1 に対応づけるため，IP アドレスに依存することなく論理的にグループを定義でき，個人単位/ドメイン単位が混在したり，1 ユーザに対して複数のグループを重複して定義したりできる．またサブネット内に存在する個々の GE に対して，そのサブネットとは別のグループを定義することもできる．なお，セキュア通信グループの定義は管理装置 GMS（Group Management Server）で行われ，グループ鍵 GK の生成・更新処理なども行う．

通信開始時に，通信相手とグループ情報を交換して同一グループに属しているか確認し，暗号化通信に必要な動作処理情報を生成する．

2.3 提案アーキテクチャのシステム構成

図 3 に GSCIP のシステム構成の概要を示す．GSCIP はあらゆるアプリケーション間でやりとりされる TCP/UDP パケットを対象とするため，OS の IP 層へモジュールを実装する．カーネルに実装されるモジュールを GPACK（GSCIP Package）と呼ぶ．GE が送受信する TCP/UDP パケットは IP 層の入出力処理部から GPACK へフックし，3 種の通信を実現するための処理が行われる．処理に必要な情報がない場合は，処理中の TCP/UDP パケットを一旦待避させてから各プロトコルによるネゴシエーションが行われる．ネゴシエーション完了後は待避していたパケットを復帰させ，生成された情報に基づいて暗号化などの処理が行われる．その後，TCP/UDP パケットは IP 層の入出力処理部へ差し戻され，通常の送受信処理が行われる．

このような仕組みとすることにより，プロトコル処理をユーザランドで行う場合と比較して高速に行えることや，カーネルへの変更を最小限に抑えるなどの利点がある．なお，上記処理の手順は各プロトコルが単独で動作する場合も同様である．

カーネルに実装するモジュール以外に，ユーザランドで動作する各種設定ツールや，GMS 間との通信や移動検知などを行う各種デーモンがある．これらはソケットを通じて GPACK と相互に情報交換することができる．

3. IPv4 ネットワーク特有の移動透過通信システム

IPv4 ネットワークでは NAT の存在により，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に対して通信を開始できなかったり，また NAT がパケットの IP アドレスとポート番号を変換したりするなど，IPv4 ネットワーク特有の現象が発生する．このようなネットワークにおいて移動透過通信システムを実現するためには，NAT による弊害を除去する必要がある．本章ではアドレス空間透過性を実現する NAT-f を既存の移動透過性プロトコル[⋆1]と組み合わせることにより，新たな通信ケースを実現する手法について提案する[13]．

3.1 要素技術の概要

3.1.1 NAT-f

NAT-f は，グローバルネットワーク上の外部ノード EN（External Node）とホームゲートウェイ HGW（Home Gateway）が連携することによりホームネットワーク内の内部ノード IN（Internal Node）に対して通信を開始できる NAT 越え技術である．**図 4** に NAT-f による通信手順を示す．EN は通信開始時にホームネットワーク内に存在する IN の名前解決処理を行う．この過程において，EN は HGW のグローバル IP アドレスを取得するが，

⋆1 文献 13) では Mobile PPC と Mobile IP に適用する場合について述べられているが，本稿では Mobile PPC に適用する場合を取り上げる．

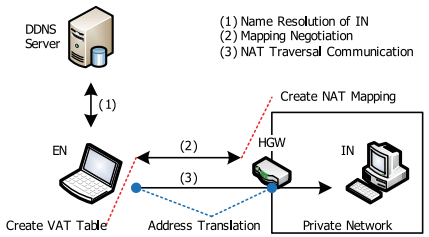

図 4 NAT-f による通信手順
Fig. 4 NAT-f communication procedure.

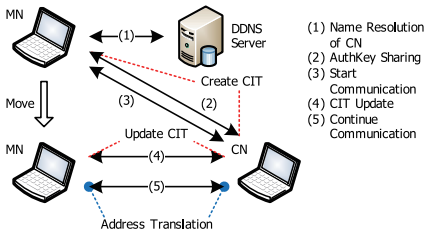

図 5 Mobile PPC による通信手順
Fig. 5 Mobile PPC communication procedure.

GPACK において DNS 応答メッセージを解析し，取得した IP アドレスを IN の FQDN をもとに生成した仮想 IP アドレスに書き換えて上位層へ渡す．

アプリケーションは仮想 IP アドレス宛に TCP/UDP パケットを送信することになるが，このとき EN は GPACK において送信パケットを一時的に待避させ，HGW に対してマッピング処理を行う．このマッピング処理により，HGW は EN と IN が通信するために必要な NAT マッピングを生成する．EN は仮想 IP アドレスと HGW で割り当てられたマッピングアドレスの対応関係を示した仮想アドレス変換テーブル（VAT Table）を GPACK 内に生成する．

EN は VAT テーブルに基づいて，待避させていた TCP/UDP パケットの宛先を仮想 IP アドレスから HGW のマッピングアドレスに書き換えて送信する．HGW にはすでに NAT マッピングが生成されているため，通常の NAT によるアドレス変換処理を実行し，EN からのパケットを IN へ転送する．

このような処理により，エンドツーエンド通信を確立する．NAT 越え技術としてよく知られている STUN（Session Traversal Utilities for NAT）[14] などと比較して，NAT-f は IN に NAT 越えにかかわる機能をいっさい実装する必要がないため，一般の PC はもちろん，情報家電機器などをそのまま利用することができる．

3.1.2 Mobile PPC

Mobile PPC は，エンドエンドで移動透過性を実現する方式であり，移動ノード到達性[⋆1]と通信継続性[⋆2]を明確に分離した点に特徴がある．移動ノード到達性には DDNS（Dynamic DNS）サーバを利用し，通信継続性に関わる機能を Mobile PPC で実現する．

図 5 に MN（Mobile Node）から CN（Correspondent Node）へ通信を開始する場合における Mobile PPC の通信手順を示す．MN は DDNS サーバを利用して CN の名前解決を行い，IP アドレスを取得する．MN と CN は通信開始に先立ち，Cookie 交換及び Diffie-Hellman（以下 DH）鍵交換による 2 往復の認証鍵共有ネゴシエーションにより認証鍵を共有する[15]．更に TCP/UDP パケットのコネクション識別子 CID（Connection ID）[⋆3]を用いて，CIT（Connection ID Table）と呼ぶアドレス変換テーブルを GPACK 内に生成しておく．なお，移動前は CIT によるアドレス変換は行われない．

MN が通信中に移動して IP アドレスが変化した際，CN に対して移動前後の IP アドレスの関係を CIT Update（以下 CU）処理により直接通知する．CU 処理では通信開始時に共有しておいた認証鍵による相手認証を行い，CIT を更新する．その後両ノードは更新した CIT に基づいて，該当するすべての TCP/UDP パケットに対してアドレス変換処理を行う．これにより，IP 層より上位では移動前の IP アドレスとして処理される．その結果，上位層から IP アドレスの変化を隠ぺいすることができる．

3.2 通信ケースの定義

従来の IPv4 における移動透過通信の研究では，MN の移動前・移動後のネットワークの組み合わせにより，以下の 4 つのパターンが検討されている．

Pattern 1: グローバルネットワークからグローバルネットワークへの移動
Pattern 2: グローバルネットワークからプライベートネットワークへの移動
Pattern 3: プライベートネットワークからグローバルネットワークへの移動
Pattern 4: プライベートネットワークから異なるプライベートネットワークへの移動

Pattern 1 は最も基本的な移動パターンである．Pattern 2，Pattern 3 は移動前もしくは移動後の通信経路上に NAT が介在することになる．Pattern 4 はプライベートネットワークが階層的に構築された環境での移動が想定される．いずれのパターンにおいても，CN はグローバルネットワークに存在することが前提である．

一方，近年では外出先からホームネットワーク内の情報家電機器と通信するための研究が盛んに行われている[16),17]．このような場合，既存技術の前提とは異なり，CN はプライベートネットワーク内に存在することになる．そこで上述した MN の移動パターンに CN

⋆1 相手ノードがどこにいても通信を開始ができる性質
⋆2 通信中に一方のノードが移動しても通信を継続できる性質
⋆3 TCP コネクション，または UDP ストリームを識別するための情報であり，送信元/宛先 IP アドレス，ポート番号とプロトコルタイプの 5 つの値の組からなる．

表 2　IPv4 ネットワークにおける通信ケースの定義
Table 2　Definition of communication case in IPv4 network.

MN の移動パターン	CN の位置	
	GNW	PNW
Pattern 1（from GNW to GNW）	Case 1	Case 5
Pattern 2（from GNW to PNW）	Case 2	Case 6
Pattern 3（from PNW to GNW）	Case 3	Case 7
Pattern 4（from PNW to PNW）	Case 4	Case 8

GNW : Global Network, PNW : Private Network

の位置を組み合わせた通信ケースを定義する．**表 2** に IPv4 ネットワークにおける通信ケースを示す．既存技術は CN がグローバルネットワークに存在することを前提としているため，Case 1 から Case 4 に対応している．Case 5 から Case 8 のような新たな通信ケースを実現するためには，CN 側の NAT 越えを実現する必要がある．

3.3　NAT-f と移動透過性プロトコルの融合

CN 側の NAT 越え問題を解決するために，NAT-f を移動透過性プロトコルと融合することにより，新たな通信ケースを実現する．NAT-f は Mobile IP，Mobile PPC のどちらとも共存することが可能であるが，ここでは Mobile PPC を中心にその方法を述べる．NAT-f は通信開始時，Mobile PPC は移動時にアドレス変換テーブルを生成する．そのため，両者の技術には独立性があり，かつ大きな修正を加えることなく組み合わせることができる．

3.3.1　システム構成

図 6 に想定するシステム構成を示す．グローバル IP アドレス G_{MN} を持つ MN が，HGW 配下のプライベートネットワークに存在する CN へ通信を開始する．その後，MN は CN と通信中にルータ R1 配下のネットワークから R2 の配下ネットワークに移動して，新しいグローバル IP アドレス $G_{MN}{}^2$ を取得したことを想定する．R1 と R2 は DHCP サーバ機能を有していると仮定する．MN と HGW はそれぞれ NAT-f と Mobile PPC を実装しており，CN はこれら機能を有さない一般ノードでよい．

NAT-f を利用するための必要な事前設定として，DDNS サーバには HGW のホスト名 “*home*” とグローバル IP アドレス G_{HGW} の対応関係がワイルドカード A レコードとして，また HGW には CN の名前 “*cn*” とプライベート IP アドレス P_{CN} の対応関係がアクセス制御テーブル ACT（Access Control Table）に登録されているものとする．

3.3.2　通信開始手順

図 7 に通信開始時にシーケンスを示す．MN は CN の IP アドレスを取得するために，ホスト名 “*cn.home*” の名前解決を行う．DDNS サーバは HGW の IP アドレスを応答する．MN は受信した DNS 応答を GPACK 内に一時待避させてから，HGW と Support Check ネゴシエーションを行う．これは HGW が NAT-f に対応しているかを確認する処理であり，MN は HGW が NAT-f に対応していることを確認したら，待避させた DNS 応答に記載されている IP アドレスを仮想 IP アドレス V_{CN} に書き換え，アプリケーションへ通知する．

以後，3.1.1 項で述べた NAT-f の一連の処理を行うが，Mapping ネゴシエーションが完了した後，続けて 3.1.2 項で述べた Mobile PPC の通信開始時の処理を行う．上記の処理が完了すると，MN には VAT テーブルと CIT が，HGW には NAT マッピングと CIT が生成され，また両者に認証鍵が共有される．MN は待避していた TCP/UDP パケットを復帰させ，NAT-f に基づく通信を開始する．MN と CN 間で送受信される TCP/UDP アドレス

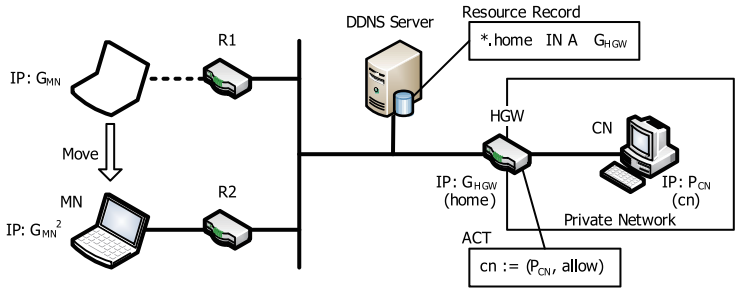

図 6　システム構成と事前設定
Fig. 6　System configuration and initial settings.

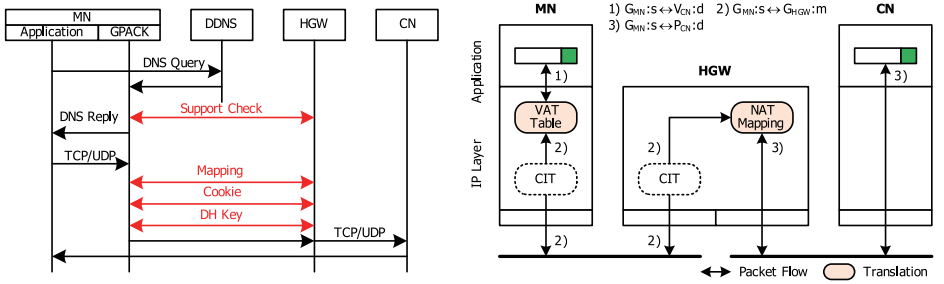

図 7　通信開始時のシーケンスと TCP/UDP パケットの IP アドレス/ポート番号の遷移
Fig. 7　Sequence when MN starts communication and IP address/port number transition of TCP/UDP packets.

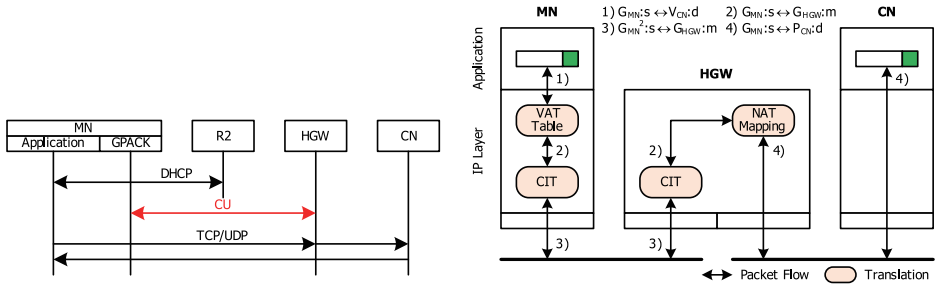

図 8 MN 移動後のシーケンスと TCP/UDP パケットの IP アドレス/ポート番号の遷移
Fig. 8 Sequence after MN moves and IP address/port number transition of TCP/UDP packets.

の IP アドレスとポート番号は，図 7 右のように遷移する．すなわち，MN では VAT テーブルに基づくアドレス変換処理により，宛先が仮想 IP アドレスとポート番号 “V_{CN} : d” から HGW にマッピングされたアドレスとポート番号 “G_{HGW} : m” となり送信される．HGW では NAT により宛先が “P_{CN} : d” へ変換され，CN へ転送される．

3.3.3 通信継続手順

図 8 に MN が R2 配下へ移動した後の通信シーケンスを示す．MN は別のネットワークに移動したことを検知すると，DHCP 処理を実行して新しい IP アドレス $G_{MN}{}^2$ を取得する．アドレス取得後，MN は IP アドレスの変化を通知するために Mobile PPC の移動通知処理，すなわち HGW に対して CU ネゴシエーションを行う．この処理でやりとりされるメッセージは通信開始時に共有した認証鍵を用いて署名を付加され，認証処理を終えた後に CIT を更新する．MN も HGW と同様に自身の CIT を更新する．

上位層から渡された TCP/UDP パケットは，図 8 右に示すように，VAT テーブルに基づくアドレス変換，及び CIT に基づくアドレス変換が行われる．すなわち，送信元が移動前から移動後の IP アドレスへ，あて先が仮想 IP アドレスからマッピングアドレスへ変換され，HGW へ送信される．HGW は受信パケットに対して，CIT に基づくアドレス変換及び NAT に基づくアドレス変換が行われる．すなわち，送信元が MN の移動後から移動前の IP アドレスへ，あて先がマッピングアドレスから CN のプライベート IP アドレスへ変換され，CN へ転送される．

以上の処理により，MN の上位アプリケーションと HGW の NAT アドレス変換処理部及び CN は，移動が発生して MN の IP アドレスが変化したことに気づくことなく，通信を継続することができる．

表 3 装置仕様
Table 3 Device specifications.

	MN	CN	HGW
CPU	Pentium M 1.73 GHz	Core2 U7600 1.20 GHz	Geode LX800 500 MHz
Memory	512 MByte	2037 MByte	256 MByte
OS	FreeBSD 6.1	Windows Vista	FreeBSD 6.1

表 4 Iperf による TCP スループット測定値
Table 4 TCP throughput on the proposal method using Iperf.

	スループット [Mbps]
NAT-f/Mobile PPC 未実装時	69.3
NAT-f/Mobile PPC 実装時（移動前）	69.1
NAT-f/Mobile PPC 実装時（移動後）	67.9

3.4 性能評価

MN と HGW で行われるアドレス変換処理が，MN と CN のエンドツーエンドのスループットに与える影響を明らかにするために，Iperf を用いて TCP スループットを測定した．また，通信開始時に発生するオーバヘッド及びデーモンによる移動検知から通信継続までに要する時間，すなわち通信断絶時間を測定した．

測定環境は図 6 に示す構成とし，HGW，DDNS サーバ及び R1/R2 を 100BASE-TX スイッチで接続した．**表 3** に各装置の仕様を示す．MN の移動は UTP ケーブルを R1 から R2 につなぎなおすことでエミュレートした．Cookie と認証鍵の生成に用いるハッシュ関数には MD5 を使用し，DH 鍵交換における DH グループは Group 1（768 bit）とした．

3.4.1 スループット性能

Iperf により MN から CN に対して TCP トラフィックを 60 秒間送信した．NAT-f と Mobile PPC を実装したシステムにおいて，移動前と移動後のスループットを測定した．また比較のため，同一装置により NAT-f と Mobile PPC を実装していない通常のシステムにおいても測定した．この場合は HGW にあらかじめ静的マッピングを設定し，MN が CN へ通信を開始できるようにした．

表 4 に TCP スループット測定結果を示す．未実装時のスループットが 69.3 Mbps であったのに対して，実装時の移動前は 69.1 Mbps，移動後は 67.9 Mbps であった．実装時の移動前は MN において VAT テーブルに基づくアドレス変換処理が加わるが，スループットに対する影響はほとんどないといえる．実装時の移動後は，更に MN と HGW において CIT

表 5 MN の通信開始時に発生する処理時間の内訳
Table 5 Details of overhead when MN starts communication.

処理内容	処理時間	
a) DNS 応答書き換え	2.74	[msec]*1
b) マッピング処理	5.49	[msec]*2
c) Cookie 交換	3.28	[msec]*2
d) DH 鍵交換	98.72	[msec]*2
e) 認証鍵生成（MN）	5.40	[msec]
f) 認証鍵生成（CN）	38.92	[msec]
通信開始までの総オーバヘッド（a+b+c）	11.51	[msec]

*1 処理時間 +1RTT（RTT は MN〜DDNS 間の RTT）
*2 処理時間 +1RTT（RTT は MN〜HGW 間の RTT）

に基づくアドレス変換が加わるため，未実装時のスループットから約 2 % 低下していた．低下の要因は HGW における CIT のアドレス変換処理にあることがわかった．

なお，提案方式の実装の有無に関わらず 70 Mbit/s 程度のスループットしか得られなかったが，この原因は NAT アプリケーションに FreeBSD 標準の `natd` を採用したためである．`natd` はユーザランドで動作し，受信したパケットを IP 層から Divert socket により取得する．このとき，カーネルではフラグメントされたパケットの再構築処理と，カーネルとユーザランド間のメモリコピーがパケットを処理するたびに発生するため，装置の仕様に応じてスループットが大幅に低下してしまう．

以上の結果より，NAT-f と Mobile PPC を組み合わせても，スループットの低下は十分に小さく，実用上問題ないといえる．

3.4.2 通信開始時のオーバヘッド

表 5 に通信開始時に発生するオーバヘッドとその内訳を示す*1．MN が最初の TCP/UDP パケットを送信する際，カーネルに一時待避させてから実際に送信されるまでに行われる処理は表 5 のうち，a) NAT-f による DNS 応答書き換え，b) マッピング処理，及び c) Mobile PPC の Cookie 交換の合計処理である．したがって，通信開始までのオーバヘッドは上記処理時間の合計，すなわち 11.51 msec となる．認証鍵共有処理の後半部分（DH 鍵交換と認証鍵生成）は Cookie 交換後に開始される TCP/UDP 通信のバックエンドで行われるため*2，通信開始時のオーバヘッドには含まれない．

⋆1 測定結果における RTT（Round Trip Time）の数値は実験環境における小さな値によるものである．
⋆2 カーネルモジュールの GPACK ではなく，MN と HGW のデーモン間で鍵交換処理が行われる．

表 6 通信断絶時間の内訳
Table 6 Details of communication break time.

処理内容	処理時間	
ネットワーク移動（手動）	1.64	[sec]
移動検知（デーモン）	28.70	[msec]
アドレス取得（DHCP）	2.11	[sec]*1
アドレス重複確認（カーネル）	0.69	[sec]
CU 処理（Mobile PPC）	41.26	[msec]*2
総通信断絶時間	4.51	[sec]

*1 処理時間 +2RTT（RTT は MN〜R2 間の RTT）
*2 処理時間 +1RTT（RTT は MN〜HGW 間の RTT）

上記結果より，NAT-f と Mobile IP を組み合わせたシステムにおいても，通信開始時に発生するオーバヘッドは十分許容できる範囲であるといえる．

3.4.3 通信断絶時間

表 6 に移動時の通信断絶時間とその内訳を示す．表中の処理内容はそれぞれ下記の間の処理である．

- ネットワーク移動：UTP ケーブル抜線〜挿線
- 移動検知：リンク確立判断〜ping タイムアウト
- IP アドレス取得：DHCP Discover 送信〜IP アドレス設定
- アドレス重複確認：Gratuitous ARP 送信〜タイムアウト
- CU 処理：CU Request 送信〜CIT 更新

通信断絶時間の合計は 4.51 sec であった．このうち，ネットワークの移動に 1.64 sec を要しているが，実際は無線 LAN における L2 ハンドオーバに該当するため，50〜400 msec になると推測される[18]．上記時間を除いた通信断絶時間に着目すると，DHCP によるアドレス取得と Gratuitous ARP によるアドレス重複確認の合計が 97.6 % を占める結果となった．一方，提案方式特有の処理時間は十分に短いことがわかる．

上記の結果より，移動にともなうパケットロスを減らすためには，アドレス取得に関する処理時間を短縮することが重要である．これについては複数の無線インタフェースを効果的に切り替えることにより，パケットロスを無くす方法を別途提案している[19]．

3.5 各通信パターンへの対応

移動透過アーキテクチャの実用性を評価する上で，対応可能な通信ケースの広さは重要な指標と考えられる．本章では 3.2 に示した Case 5 の実現方法を取り上げたことになる．提案方式が他の通信ケースを実現する可能性について考察した．

Mobile PPC では Pattern 2 から Pattern 4 に対応するため，NAT 越え技術として知られている Hole Punching の原理を導入する方法を提案している[20]．通信開始時の認証鍵共有処理または移動後の CU 処理において通信経路上に NAT [⋆1]の存在を確認すると，MN から CN に対して Hole Punching を実行し，MN 側の NAT にマッピング情報を生成する．MN は CN からの応答により MN 側 NAT の外側に割り当てられた IP アドレスとポート番号を取得する．これにより，CN は MN 側 NAT のアドレス変換に対応した CIT を生成することができる．提案方式は移動透過性プロトコルの機能をそのまま利用しているため，そのまま Case 2 から Case 4 に対応することができる．

Case 6 はグローバルネットワークからプライベートネットワークへの移動のため，Case 5 とは移動後の処理だけが異なる．移動後の処理に着目すると，Mobile PPC に関する処理しか行わない．したがって，Case 2 と同様の処理を行うことにより Case 6 は実現可能である．Case 7 についても，Case 3 と同様の処理を提案方式に適用すれば実現可能である．Case 8 は Case 4 の実現方法と同じ考え方で対応することが可能である．すなわち，Case 7 の通信開始時の処理と Case 6 の移動後の処理を組み合わせることで実現できる．

4. おわりに

本研究では柔軟性とセキュリティを兼ね備えたセキュア通信グループを構築できる FPN と呼ぶネットワークの概念を提唱し，位置透過性，移動透過性，アドレス空間透過性を同時に実現するための通信アーキテクチャとして GSCIP を提案した．暗号化通信，移動通信，エンドツーエンド通信を IPv4 ネットワークにおいて同時に実現できることを確認し，ユビキタスネットワークを実現できるアーキテクチャとしての有効性を示した．

参考文献

1) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
2) Perkins, C.: IP Mobility Support for IPv4, RFC 3344, IETF (2002).
3) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, RFC 3775, IETF (2004).
4) 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 (2006).
5) 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 (2006).
6) 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 (2006).
7) 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 (2007).
8) Kivinen, T., Swander, B., Huttunen, A. and Volpe, V.: Negotiation of NAT-Traversal in the IKE, RFC 3947, IETF (2005).
9) Huttunen, A., Swander, B., Volpe, V., Diburro, L. and Stenberg, M.: UDP Encapsulation of IPsec Packets, RFC 3948, IETF (2005).
10) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
11) Wing, D., Rosenberg, J. and Tschofenig, H.: Discovering, Querying, and Controlling Firewalls and NATs, Internet-draft, IETF (2007). http://tools.ietf.org/id/draft-wing-behave-nat-control-stun-usage-05.txt
12) Tschofenig, H. and Bajko, G.: Mobile IP Interactive Connectivity Establishment (M-ICE), Internet-draft, IETF (2008). http://tools.ietf.org/id/draft-tschofenig-mip6-ice-02.txt
13) 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.109–121 (2009).
14) Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
15) 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 (2009).
16) Oh, Y.-J., Lee, H.-K., Kim, J.-T., Paik, E.-H. and Park, K.-R.: Design of an Extended Architecture for Sharing DLNA Compliant Home Media from Outside the Home, *IEEE Transactions on Consumer Electronics*, Vol.53, No.2, pp.542–547 (2007).
17) Motegi, S., Tasaka, K., Idoue, A. and Horiuchi, H.: Proposal on Wide Area DLNA Communication System, *Proc. CCNC2008*, pp.233–237 (2008).
18) Mishra, A., Shin, M. and Srbaugh, W.: An Empirical Analysis of the IEEE802.11 MAC Layer Handoff Process, *ACM SIGCOMM Computer Communication Review*, Vol.33, No.2, pp.93–102 (2003).
19) 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 (2009).
20) 鈴木秀和，寺澤圭史，渡邊　晃：Hole Punching を用いた NAT 越え Mobile PPC の実装，情報処理学会研究報告，Vol.2009-MBL-49, No.17, pp.1–7 (2009).

⋆1 MN がプライベートネットワークに存在する場合，そのネットワークの上流にある NAT を指す．