情報処理学会論文誌　Vol. 51　No. 9　1–11 (Sep. 2010)

推薦論文

通信グループに基づくサービスの制御が可能なNAT越えシステムの提案

鈴木 秀和[†1,†2,*1]　渡邊 晃[†1]

外出先からホームネットワーク内の通信機器に対してアクセスする場合，NAT 越え問題を解決する必要がある．筆者らは，外部ノードとホームゲートウェイが連携して NAT のマッピングを動的に生成することにより NAT 越え問題を解決する NAT-f（NAT-free protocol）を提案している．しかし従来の NAT-f は，外部からの通信が許可された内部ノードに対して自由に NAT のマッピングを生成できるため，誰でもホームネットワーク内にアクセスできてしまう課題があった．本論文では従来方式に通信グループの概念を導入したセキュアな NAT 越えシステムを提案する．通信グループを内部ノードが提供するサービスに対応付けることにより，外部ノードからのアクセス制御とサービスの制御を同時に実現することが可能となる．

A Proposal for NAT Traversal System with Communication Group-based Service Control

Hidekazu Suzuki[†1,†2,*1] and Akira Watanabe[†1]

A NAT traversal problem has to be solved if you access communication devices in a home network from the outside. To solve the problem, we have proposed NAT-free protocol (NAT-f) that creates a NAT mapping dynamically by cooperating with an external node and a home gateway. However, the existing NAT-f system has security issues that anyone can access internal nodes in a home network. This paper presents a secure NAT traversal system that combines the existing NAT-f technology and the concept of the communication group. By making the communication group be related to services provided by internal nodes, it is possible to provide the access control of external nodes and the service control simultaneously.

1. はじめに

現在のホームネットワークは IPv4 プライベート IP アドレスを適用するのが一般であり，インターネットの接点には NAT（Network Address Translator）を設置する必要がある．しかし，NAT によりエンドツーエンド接続性が失われ，NAT の外部から内部のネットワークへ通信を開始できない，いわゆる NAT 越え問題が表面化してきた．近年では携帯デバイスの高性能化，小型化やブロードバンドの普及に伴い，IP 電話やマルチメディア通信など個人間の通信が増加している．このような利用形態では，インターネット側からホームネットワーク内の PC や情報家電機器に向けて通信を開始することも想定される．そのため NAT 越え技術の必要性が高まっており，様々な NAT 越え方式が提案されている[1)–4)]．

筆者らは，宅外の外部ノード（以下 EN; External Node）と NAT が実装されたホームゲートウェイ（以下 HGW）に機能を追加することにより，NAT 越え問題を解決する NAT-f（NAT-free protocol）[5)] を提案している．NAT-f では仮想 IP アドレスを導入することにより，EN がプライベートネットワーク上の内部ノード（以下 IN; Internal Node）を仮想的に認識する．仮想的に認識した IN へ通信を開始する際，EN は HGW に対して NAT-f によるネゴシエーションを実行し，IN と通信するために必要な NAT マッピング情報を生成する．以後，EN が送信するパケットの宛先を仮想 IP アドレスから，マッピングされた HGW の外部 IP アドレス・ポート番号に変換することにより，HGW を通過して IN へアクセスすることを可能としている．しかし，従来の NAT-f は要求があれば無条件に NAT マッピング情報を生成してしまうため，外部からの接続を許可された IN に対して誰でもアクセスできるという課題があった．

そこで，本論文では既存の NAT-f に通信グループの仕組みを適用し，EN のアクセス制御と IN のサービス制御を実現する NAT 越えシステムを提案する．EN と IN を特定の属性に基づいてグルーピングし，そのグループで利用可能なサービスを定義する．通信開始時に実行する NAT-f ネゴシエーションに EN が帰属する通信グループの情報を付加する．HGW はこの情報により，EN と IN が同一通信グループのメンバであるかを確認してか

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 日本学術振興会特別研究員 PD
Research Fellow of the Japan Society for the Promotion of Science
*1 現在，名城大学理工学部
Presently with Faculty of Science and Technology, Meijo University

ら NAT マッピング情報を生成する．また，同一通信グループの End-to-End 間，または End-to-GW 間の通信は暗号化され，その安全性は保証される．

以下，2 章で NAT-f の基本的仕組みと，提案方式に係わる要素技術について説明する．3 章で提案方式の詳細について述べ，4 章で提案方式を実装したシステムの性能評価結果と，セキュリティおよび利用シーンについて考察する．5 章で関連研究との比較を行い，最後に 6 章にてまとめる．

2. 要 素 技 術

2.1 NAT 越え

NAT-f は，EN と HGW が連携することによりホームネットワーク内の IN に対して通信を開始できる NAT 越え技術である．**図 1** に NAT-f による通信シーケンスを示す．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，IP 層において 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 IP 層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 IP 層内に生成する．

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 には既に 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．

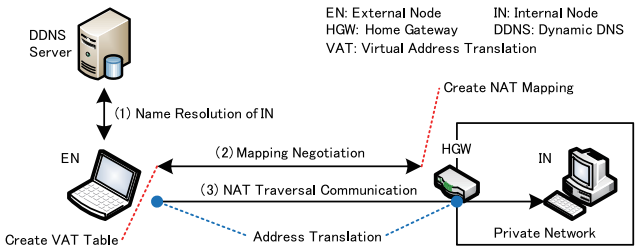


図 1　NAT-f による通信シーケンス
Fig. 1　Communication sequence with NAT-f.

このような処理により，インターネット側からホームネットワーク内の機器への通信開始を実現できる．NAT 越え技術としてよく知られている STUN[2] や UPnP[4] などと比較して，NAT-f は IN に NAT 越えに係わる機能を一切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．しかし，マッピング処理には認証機能がないため，誰でも NAT マッピングを生成して IN にアクセスできてしまう課題がある．そのため，私的なコンテンツを特定のユーザに限定して公開することができない．

2.2 通信グループの構築

特定の属性に基づくユーザあるいはノードを集合させて通信グループを構築する技術は，通信の安全性を確保する上で有用である．これにより，通信グループ内のメンバ間の通信は暗号化され，第三者による盗聴や改ざんから保護される．

通信グループの構築方法として，例えば GSCIP（Grouping for Secure Communication for IP）[6] が採用しているエリア定義方式[7] がある．この方式では通信グループとグループ鍵と呼ぶ暗号鍵を 1 対 1 に対応付けているため，ユーザが複数のグループ鍵を所持することにより，容易に複数の通信グループに多重帰属することができる．また通信グループの定義が容易であり，IP のサブネットワークに依存しないグループの定義が可能である．

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 暗号化通信

アプリケーションを意識することなく通信パケットを暗号化する技術は，様々なアプリケーションの利用が想定される NAT 越えシステムにも有効である．IP レベルの暗号化通信を実現する技術として，IPsec ESP[8] や PCCOM（Practical Cipher Communication Protocol）[9] がある．

IPsec は強靱なセキュリティ機能を提供する一方，TCP/UDP ヘッダのポート番号とチェックサムフィールドが暗号化範囲および完全性保証の範囲に含まれているため，NAT を通過すると偽造パケットと見なされ，エンドノードで破棄されてしまう．ESP パケットを UDP によりカプセル化して NAT 越えする方法[10] もあるが，ヘッダ追加に伴うオーバヘッドの増加やフラグメントの発生，またヘッダ部のセキュリティが低下するなどの課題が生じる．従って，IPsec は NAT やファイアウォールとの相性が悪いといえる．

PCCOM は IPsec の課題を解決できる暗号通信方式である．PCCOM は本人性確認とパケット全体の完全性保証を，暗号鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，独自の TCP/UDP チェックサム計算を行うことにより実現する．暗号化範囲は TCP/UDP ペイロード部であるため，NAT を通過することができ，かつファイアウォールによるトラヒック制御が可能である．パケットヘッダの IP アドレスとポート番号の完全性は動作処理情報の検索過程で保証されるため，改ざんを防止することができる．この方式によると，NAT やファイアウォールと共存することが可能で，かつパケットフォーマットを変えないため，ヘッダオーバヘッドやフラグメントが発生せず，高スループットを実現できる．

3. 提 案 方 式

3.1 概　　要

本論文で提案する NAT 越えシステムは，従来の NAT-f に通信グループの概念と暗号化通信を導入し，以下の機能を新たに追加する．

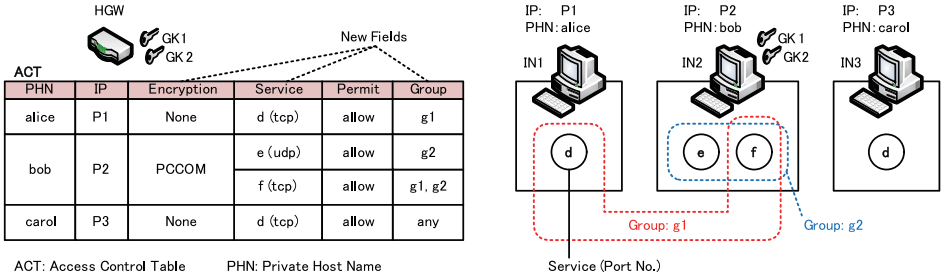
- HGW において通信グループに基づくアクセス制御を実現する．
- グルーピングの概念をノード単位からサービス単位に拡張し，柔軟なサービス制御を実現する．
- EN と HGW 間，または EN と暗号化通信機能を有する IN 間の通信を暗号化する．

通信グループの構築は 2.2 節で示したグループ鍵による方法を採用する．EN は HGW に自身が所属する通信グループを通知するために，NAT-f 制御メッセージを拡張する．これにより，NAT マッピングおよび VAT テーブルに加えて，新たにパケットの暗号化に必要な動作処理情報テーブル PIT（Process Information Table）を生成する．暗号化通信には PCCOM を採用し，拡張した NAT-f により生成された PIT に基づいて TCP/UDP パケットを暗号化する．なお，以後本論文で用いる記号は付録 A.1 に示す．

3.2 グルーピングに関する概念の拡張

図 2 に拡張した ACT（Access Control Table）とサービスのグルーピングイメージを示す．ACT とは NAT-f を実装した HGW が保持する情報で，IN のプライベートホスト名（PHN）[⋆1] とプライベート IP アドレス，および外部からのアクセス可否を示すフラグから構成される．提案方式では新たに Encryption，Service，Group の 3 つの項目を追加する．

⋆1 PHN はホームネットワーク内で自由に設定可能であり，外部の DNS に登録する必要はない．



PHN	IP	Encryption	Service	Permit	Group
alice	P1	None	d (tcp)	allow	g1
bob	P2	PCCOM	e (udp)	allow	g2
			f (tcp)	allow	g1, g2
carol	P3	None	d (tcp)	allow	any

図 2　拡張した ACT とサービスのグルーピング
Fig. 2　Extended Access Control Table and service grouping.

Encryption には該当する IN が暗号化機能（PCCOM）をサポートするか否かを設定する．Service には該当する IN が外部に公開するサービスが設定され，対応するポート番号を指定する．Group には該当するサービスにアクセス可能な通信グループを指定する．HGW は上記情報に基づいて，外部からのアクセス制御および IN のサービス制御を行う．

図 2 では，alice のサービス d と bob のサービス f がグループ $g1$ にグルーピングされている．このサービスは，グループ $g1$ に対応付けられたグループ鍵 $GK1$ を所持する EN だけが利用することができる．一方，carol のサービス d は ACT によるとグループ “any” と設定されている．これは，例えば公開 Web サーバのように誰でもアクセス可能であるノードであることを示しており，どの通信グループにも設定されない．

従来の NAT-f システムでは，IN を特別な機能を有さない一般ノードと想定していたため，このような IN にグループ鍵を保持させることができない．そこで提案方式では HGW に全てのグループ鍵を保持させ，かつ ACT に登録された情報を利用することにより，IN を通信グループに所属しているかのように扱う．ただしこの場合，HGW と IN 間の通信は暗号化されず，平文となる．EN から IN までのエンドエンド間を全て暗号化する場合は，IN に提案方式を実装してグループ鍵を保持させることになる．例えば図 2 の設定がされたホームネットワークに対して，グループ $g1$ に属する EN1，グループ $g2$ に属する EN2，および一切のグループ鍵を保持しない EN3 が通信を開始する場合の通信可否は**表 1** のようになる．

3.3 通信シーケンス

提案方式の前提条件は以下の通りである．EN は移動ノードでデータ通信デバイスを利用して携帯網に接続する場合を想定し，グローバル IP アドレスが割り当てられるものとする．ただし，本論文では通信中の移動に伴う IP アドレスの変化は考慮しない．HGW は ISP か

表 1　ノード間の通信可否と暗号化範囲
Table 1　Availability of communication between ENs and INs and its encryption range.

宛先		送信元ノード（所属グループ）		
ノード	サービス	EN1 ($g1$)	EN2 ($g2$)	EN3 (nothing)
IN1	d	$E1$ [EN1-HGW]	×	×
IN2	e	×	$E2$ [EN2-IN2]	×
IN2	f	$E1$ [EN1-IN2]	$E2$ [EN2-IN2]	×
IN3	d	$E1$ [EN1-HGW]	$E2$ [EN2-HGW]	C

Ex: グループ鍵 GKx で暗号化 [始点-終点]　C: 平文通信　×: 通信不可

らグローバル IP アドレスが割り当てられており，EN からの通信を受信できるものとする．

EN1，EN2，HGW および IN2 は共通の暗号鍵 CK と，各通信グループに対応したグループ鍵 GK を保持しているものとし，通信グループの関係は図 2 と表 1 に示したものと仮定する．なお，NAT-f システムの事前設定として，HGW には図 2 に示した ACT が，また DDNS（Dynamic DNS）[11] サーバには HGW の FQDN “*home.example.net*” とグローバル IP アドレス $G4$ の対応関係が，ワイルドカード A レコード[12] として登録されているものとする．

3.3.1　IN が PCCOM をサポートしない場合

図 3 に IN が PCCOM をサポートしない場合の通信シーケンスを示す．これは，グループ $g1$ に所属し，グローバル IP アドレス $G1$ が割り当てられた EN1 が IN1 のサービス d にアクセスを開始する場合を想定している．提案方式は以下の 3 フェーズから構成される．

(1)　DNS 名前解決部

EN1 は HGW の FQDN の先頭に IN1 の PHN を付加した “*alice.home.example.net*” を IN1 の FQDN として，DDNS サーバに対して名前解決を行う[⋆1]．DDNS サーバは IN1 の FQDN に対して，HGW のグローバル IP アドレス $G4$ を回答する．ここで，EN1 の IP 層において，受信した DNS 応答を一時待避してから HGW 宛に Support Check Request を送信する．これは HGW が NAT-f に対応しているかを確認するためのメッセージであり，ノンス値 N_{EN} が記載される．

$$Support\ Check\ Request := N_{EN1} \tag{1}$$

HGW が NAT-f に対応している場合は，Support Check Response を応答する．このメッセージは受信したノンス値の HMAC[13] とノンス値 N_{HGW} が記載される．

$$Support\ Check\ Response := HMAC_{CK}(N_{EN1}) \mid N_{HGW} \tag{2}$$

上記メッセージを受信した EN1 は受信した HMAC を検証し，CK の共有を確認する．さらに，待避していた DNS 応答に記載された HGW の IP アドレスを，$G4$ から仮想 IP アドレス $V1$ へ書き換えて上位層へ渡す．このとき，PHN と HGW のグローバル IP アドレス，および仮想 IP アドレスの関係を NRT（Name Relation Table）に記録しておく．これにより，IN1 宛のパケットは宛先が仮想 IP アドレス $V1$ となる．

HGW が NAT-f に対応していない場合は，正しい Support Check Response が応答されないため[⋆2]，EN1 は待避していた DNS 応答をそのまま上位層へ渡す．この場合，以下のフェーズは実行されないため，NAT-f による NAT 越えは行われない．

(2)　マッピング処理部

アプリケーションが IN1 のサービス d 宛に通信を開始すると，IP 層には送信元 “$G1:s$”，宛先 “$V1:d$” の TCP パケットが渡される．ここで宛先が仮想 IP アドレスの場合，VAT（Virtual Address Translation）テーブルを検索する．最初は該当エントリが存在しないため，送信パケットを一時待避させてから Mapping Request を HGW へ送信する．これは

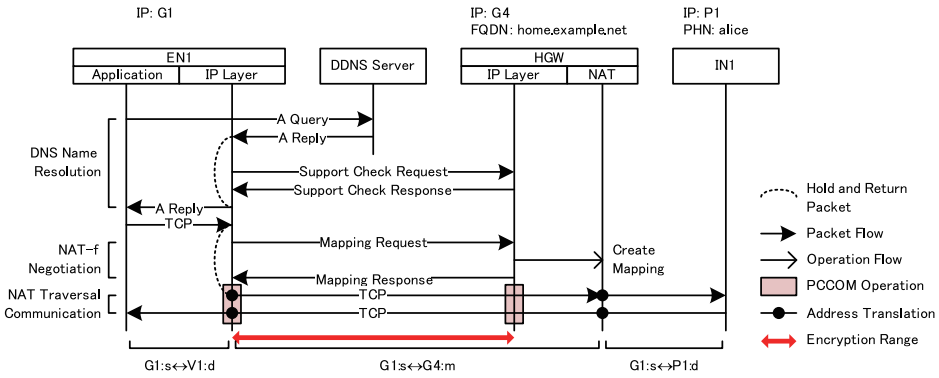


図 3　IN が PCCOM をサポートしない場合の通信シーケンス
Fig. 3　Communication sequence in the case IN does not support PCCOM.

⋆1 EN が IPv6 をサポートする OS で動作している場合，A レコードのクエリに加えて AAAA レコードのクエリも実行する．提案方式のベースである NAT-f では A レコードのクエリのみを処理対象とするため，図 3 以降のシーケンス図では AAAA レコードのクエリの記載を省略する．クエリ動作の詳細は付録 A.2 に示す．

⋆2 NAT-f 制御メッセージは ICMP Echo をベースに定義されている．従って NAT-f 非対応ノードが本メッセージを受信したら，Request と同じ内容の ICMP Echo Reply を応答する．

HGW に対して IN1 との通信に必要な NAT マッピングの生成を要求するメッセージであり，提案方式では既存の NAT-f の Mapping Request の情報[⋆1]に加え，HGW から受信したノンス値の HMAC と EN1 のグループ情報を付与して通知する．

$$Mapping\ Request := HMAC_{CK}(N_{HGW}) \mid E_{CK}(G1 \mid s \mid V1 \mid d \mid tcp \mid alice \mid g1 \mid HMAC_{GK1}(N_{HGW})) \quad (3)$$

ここで，グループ情報とは通信グループの番号と，そのグループ鍵による受信ノンス値の HMAC のセットであり，EN が所属している通信グループの数だけ記載される．

Mapping Request を受信した HGW は，受信した HMAC を検証して CK の共有を確認後，メッセージを復号する．次に，受信した PHN をキーとして ACT をチェックする．該当エントリの Permit が “$allow$” で，かつ Service と Group が受信した情報と一致したら，対応するグループ鍵により HMAC を検証して $GK1$ の共有を確認する．その後，取得した通信識別子と IN1 のプライベート IP アドレスを用いて，NAT マッピングを生成する．

$$NAT: \quad G1 : s \leftrightarrow \{G4 : m \Leftrightarrow P1 : d\} \quad [tcp] \quad (4)$$

これは IN1 のポート番号 d と HGW のポート番号 m がマッピングされたことを示しており，“$G4 : m$” をマッピングアドレスと呼ぶ．さらに提案方式では，EN1 からマッピングアドレス宛のパケットを $GK1$ で復号するような PIT を生成する．HGW は上記マッピングアドレスと一致した通信グループ番号を Mapping Response により応答する．

$$Mapping\ Response := E_{CK}(G1 \mid s \mid V1 \mid d \mid tcp \mid g1 \mid E_{GK1}(G4 \mid m \mid proc)) \quad (5)$$

ここで，$proc$ には EN1 における動作処理情報が記載されるが，ここでは「暗号化する」ことが設定される．

EN1 は受信した Mapping Response を復号後，記載されている情報から VAT テーブルを生成する．

$$VAT: \quad G1 : s \leftrightarrow \{V1 : d \Leftrightarrow G4 : m\} \quad [tcp] \quad (6)$$

これは仮想的に認識した IN1 のトランスポートアドレス “$V1 : d$” 宛の通信を HGW のマッピングアドレス “$G4 : m$” にマッピングすることを示している．さらに提案方式では，EN1 からマッピングアドレス宛のパケットを $GK1$ で暗号化するような PIT を生成する．以上で NAT-f によるネゴシエーションを完了し，先ほど待避していた送信パケットを復帰する．

(3)　仮想アドレス変換処理部

以後，EN1 から IN1 のサービス d 宛の TCP パケットは，EN1 において VAT テーブルに基づくアドレス変換処理により，宛先が “$V1 : d$” から “$G4 : m$” に変換される．このパケットは PIT に基づいて $GK1$ で暗号化されてから，HGW へ送信される．HGW では上記パケットを復号後，NAT により宛先を “$G4 : m$” から “$P1 : d$” に変換してから IN1 へ転送する．

以上の手順により，EN1 から IN1 へのアクセスを実現できる．IN1 から EN1 への応答は上記と逆の順序により，アドレス変換処理および暗号化処理が行われる．

3.3.2　IN が PCCOM をサポートする場合

図 4 に IN が PCCOM をサポートする場合の通信シーケンスを示す．これは，グループ $g2$ に所属し，グローバル IP アドレス $G2$ が割り当てられた EN2 が IN2 のサービス e にアクセスを開始する場合を想定している．

EN2 は 3.3.1 項と同様に，“$bob.home.example.net$” により IN2 の名前解決を行い，アプリケーションには仮想 IP アドレス $V2$ を通知する．その後，送信元 “$G2 : t$”，宛先 “$V2 : e$” の UDP パケット送信をトリガに，HGW に Mapping Request を送信する．

HGW も前述した通り，ACT をチェックする．ここで，該当する IN が暗号化機能をサポートしているため，新たに定義した PIT Request を IN2 へ送信する．これは IN2 に対して EN2 との暗号化通信に必要な PIT の生成を要求するメッセージであり，Mapping Request に記載されていた EN2 のグループ情報などが記載される．

$$PIT\ Request := E_{CK}(G2 \mid t \mid P2 \mid e \mid udp \mid N_{HGW} \mid g2 \mid HMAC_{GK2}(N_{HGW})) \quad (7)$$

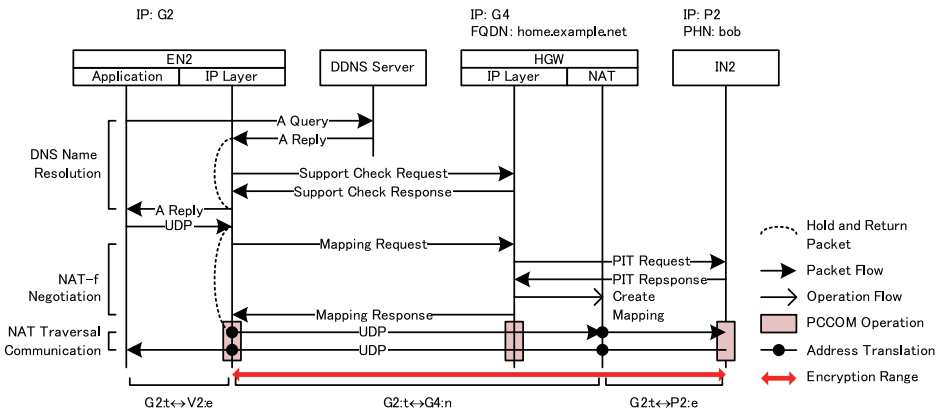


図 4　IN が PCCOM をサポートする場合の通信シーケンス
Fig. 4　Communication sequence in the case IN supports PCCOM.

⋆1 待避させた TCP/UDP パケットの通信識別子（$G1, s, V1, d, tcp$）と通信相手のホスト名（$alice$）．

上記メッセージを受信した IN2 は CK により復号後，グループ鍵 $GK2$ で復号して取得したハッシュ値と自身で計算した $h(N_{HGW})'$ を比較して，$GK2$ の共有を確認する．グループ鍵の共有を確認したら，IN2 は EN2 からサービス e 宛のパケットを $GK2$ で復号することを示す PIT を生成して，PIT Response を応答する．

$$PIT\ Response := E_{CK}(G2 \mid t \mid P2 \mid e \mid udp \mid g2 \mid E_{GK2}(N_{HGW} \mid proc)) \quad (8)$$

ここで，$proc$ には HGW における動作処理情報が記載されるが，ここでは「暗号化/復号しない」ことが設定される．

PIT Response を受信した HGW は，ハッシュ値の比較により $GK2$ の共有を確認してから，記載されている情報から NAT マッピングを生成する．

$$NAT: \quad G2 : t \leftrightarrow \{G4 : n \Leftrightarrow P2 : e\} \quad [udp] \quad (9)$$

さらに通知された $proc$ に示された通り，EN2 からマッピングアドレス “$G4 : n$” 宛の UDP パケットを暗号化/復号しないことを示す PIT を生成してから，Mapping Response を応答する．

EN2 は HGW からの応答に基づいて，VAT テーブルを生成する．

$$VAT: \quad G2 : t \leftrightarrow \{V2 : e \Leftrightarrow G4 : n\} \quad [udp] \quad (10)$$

その後，マッピングアドレス宛の UDP パケットを $GK2$ で暗号化するような PIT を生成する．

以後，EN2 から IN2 のサービス e 宛の UDP パケットは，EN2 において VAT テーブルに基づくアドレス変換処理により，宛先が “$V2 : e$” から “$G4 : n$” に変換される．このパケットは PIT に基づいて $GK2$ で暗号化されてから，HGW へ送信される．HGW では上記パケットを暗号化されたまま，NAT により宛先を “$G4 : n$” から “$P2 : e$” に変換してから IN2 へ転送する．IN2 は PIT に基づいて，受信パケットを $GK2$ により復号する．

以上の手順により，EN2 から IN2 へのアクセス開始と，NAT を挟んだエンドエンドの暗号化通信を実現できる．

4. 評　　価

図 5 に示す実験環境をローカルネットワーク内に構築し，100BASE-TX で各装置を接続した．提案方式は IP 層で動作する従来の NAT-f モジュールを拡張し，PCCOM モジュールと連係できる仕組みとした．提案方式を実装した EN が PCCOM をサポートしない IN に HTTP 接続を行った時に発生するオーバヘッドを測定して，実環境での利用が可能か確認する．EN および HGW の各機器仕様は**表 2** のとおりで，IN はホームサーバ機能を持つ市販の NAS（Network Attached Storage）⋆1を用いた．DDNS サーバはインターネット上で実働しているものを利用した．

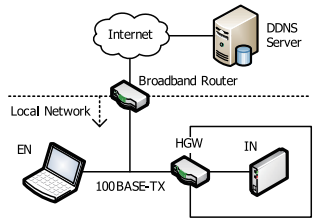


図 5　測定環境
Fig. 5　Measurement environment.

表 2　装置仕様
Table 2　Device specification.

	仕様
CPU	Atom N270 1.6 GHz
Memory	1.0 Gbyte
NIC（EN）	Atheros AR8113
NIC（HGW）	RealTek RTL8201L
	PLANEX GU-1000T（USB）
OS	FreeBSD 8.0-RELEASE

EN および HGW が保持する暗号鍵の鍵長は 128 bit であり，暗号化アルゴリズムおよびハッシュアルゴリズムは AES（CFB モード）と MD5 とした．なお，比較のため同一装置により提案方式を実装していない通常のシステムについても測定した．この場合は HGW の NAT にあらかじめ静的マッピングを設定し，EN が IN に通信を開始できるようにした．試行回数はそれぞれ 10 回であり，以下に示す測定結果はその平均値である．

4.1　セッション確立時のオーバヘッド

表 3 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．DNS 名前解決処理部，マッピングネゴシエーション処理部の処理時間はパケットアナライザ Wireshark ⋆2 での測定値であり，総オーバヘッドは EN が DNS パケットを送信してから最初の TCP SYN を送信するまでの時間である．また，各処理部における EN 側および HGW 側の詳細なメッセージ処理時間は RDTSC（Read Time Stamp Counter）[14] により測定したものである．

DNS 名前解決部では，EN が DNS サーバに対して A レコードと AAAA レコードの問合せ（計 2 往復）を行っており⋆3，静的マッピングの場合は 12.64 ms で完了するのに対して，提案方式では 14.40 ms であった．この増加分は，IP 層に実装されたモジュールにおける DNS 応答メッセージの解析時間（14.29 μs），Support Check メッセージの交換時間（1RTT; Round Trip Time）および EN 側および HGW 側でのメッセージ処理時間（それぞれ 27.54 μs，21.41 μs）によるものであり，DNS 名前解決処理の度に発生する．ただし，

⋆1 I・O DATA 社の HDL-GS500.
⋆2 Wireshark: http://www.wireshark.org/
⋆3 動作の詳細は付録 A.2 を参照.

表 3　通信開始時に発生する処理時間の内訳
Table 3　Details of overhead when EN starts communication.

処理内容	提案方式		静的マッピング	
DNS 名前解決部	14.40	[ms]*	12.64	[ms]
EN 側（DNS 応答メッセージ解析）	14.29	[μs]		
EN 側（Support Check Request 送信時）	15.74	[μs]		
EN 側（Support Check Response 受信時）	11.80	[μs]		
HGW 側	21.41	[μs]		
マッピング処理部	0.39	[ms]*	なし	
EN 側（Mapping Request 送信時）	28.58	[μs]		
EN 側（Mapping Response 受信時）	15.90	[μs]		
HGW 側	67.72	[μs]		
総オーバヘッド	15.29	[ms]	13.19	[ms]

* EN〜HGW 間のメッセージ交換に要した 1RTT を含む

DNS 応答メッセージの解析や Support Check メッセージ処理は短時間で完了しているため，実質的な増分は EN と HGW 間の 1RTT 分と見なせる．

一方，マッピング処理部は提案方式独自のオーバヘッドであり，セッションを確立する度に発生する．このオーバヘッドは 0.39 ms であり，その内訳は Mapping メッセージの交換時間（1RTT）とそのメッセージ処理時間（EN 側が 44.48 μs，HGW 側が 67.72 μs）である．実験環境は極めて小さな RTT であるが，実環境における RTT に対してメッセージの処理時間は極めて小さく，ほとんど無視できる．

従って，提案方式では EN と HGW 間の 2RTT 分オーバヘッドが増加すると見積もれるが，その増加分は十分に小さく，実用上問題ないといえる．実際に実環境下で利用して IN の Web ページを表示したが，提案方式と静的マッピングの両者でアクセスした場合の違いを体感することはなかった[⋆1]．

4.2　セキュリティに関する考察

提案方式では，本機能を実装している機器はグループ鍵に加えて共通暗号鍵 *CK* を保持している．Mapping メッセージは暗号化されるため，EN と HGW 間および HGW と暗号機能を実装した IN 間で交換される情報の安全性は保証される．これらの暗号鍵は EN，HGW および IN の各装置間に個別に割り当てる事前共有鍵方式を採用している．ホームネットワークのように規模が比較的小さな構成であれば問題ないが，規模が大きい場合は鍵管理センタから配送したり，エンティティ間で鍵を共有する方式を利用することもできる[15),16)]．

提案方式は従来の NAT-f にグループ認証機能を追加したことにより，特定のユーザだけが NAT マッピングを生成できるようになった．今回の実装で利用した FreeBSD の NAT デーモン `natd` は，タイムアウト発生時[⋆2]，または TCP の FIN/RST 検出時にマッピングエントリを削除する．ここで，EN が移動ノードであることを想定した場合，TCP 通信中に異なるネットワークへ移動すると，以後使用されないはずの NAT マッピングエントリが一定の時間残ることになる．そのため，通信グループ外の第三者に正規の手順により生成された NAT マッピングを利用されてしまう可能性が考えられる．これは以下の手段により防止可能である．

提案方式における HGW は外部から受信したパケットに対して，NAT 処理の前に PIT 検索処理を行う．ここで受信パケットの通信識別子と一致する PIT エントリが存在しない場合は，ホームネットワーク内へ転送することが許可されていないパケットと見なして破棄することができる．仮に第三者が生成されている NAT マッピングに合致するように送信元を偽装した場合，PIT エントリが存在するため HGW は受信パケットに対して復号処理を行う．しかし，通信グループ外の第三者は正しく暗号化できないため，HGW はパケットの復号処理時に異常を検出することができる．また，一般に NAT とファイアウォールは連動して処理が行われるため，マッピング処理を正しく完了した EN からのアクセスだけを通過させるようなフィルタを動的に設定することも可能である．このように，外部からの不正なアクセスを多重チェックできるため，正規の NAT マッピングを第三者に利用される可能性は極めて低いと考えられる．

4.3　利用シーン

提案方式はホームネットワーク内の様々なシステムに応用することが可能である．近年，DLNA（Digital Living Network Alliance）[⋆3] に対応した情報家電機器が充実しつつあり，外出先からこれらの機器に保存されたコンテンツを利用する様々な方式が提案されている[17)–19)]．文献 20) では，HGW にてアクセス制御ポリシの設定を行うことにより，宅内コンテンツを特定のユーザに提供できる方式が提案されている．しかし，DLNA 準拠の情報家電に蓄積されたコンテンツしかアクセス制御の対象となっていない．筆者らも文献 21) に

⋆1 EN に EMOBILE のデータカード D02HW（7.2 Mbps）を装着してインターネットに接続し，大学の DMZ（Demilitarized Zone）に設置した HGW 配下の IN に HTTP 通信を開始した場合．

⋆2 UDP は 60 秒，コネクション確立後の TCP は 24 時間．

⋆3 DLNA: http://www.dlna.org/

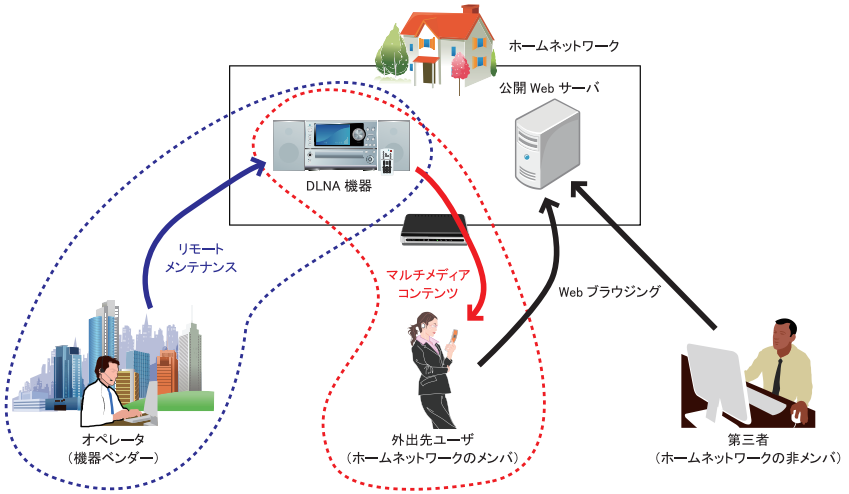


図 6　ホームネットワークにおける利用シーンの一例
Fig. 6　Example usage for home networks.

おいて NAT-f をベースとした遠隔 DLNA 通信方式を提案しており，本提案方式と組み合わせることにより，**図 6** のようにホームネットワーク内のマルチメディアコンテンツだけでなく，一般のサービスについても特定の外部ノードに限定して利用させることができる．

また情報家電機器の増加に伴い，ユーザの機器管理負荷が増加することが想定される．そこで，機器ベンダーがインターネットを介してユーザが購入した機器を遠隔でメンテナンスするサービスがある．このようなサービスをグルーピングすることにより，ユーザは安全かつ容易に機器のメンテナンスを委託することも可能と考えられる．

4.4　残された課題

本論文では，EN がグローバル IP アドレスを保持することを前提としたが，近年の移動ノードは Wi-Fi によりネットワークに接続できるため，移動先によってはプライベートネットワークに接続することが考えられる．EN がプライベートネットワークに接続した場合は，EN 側の NAT を改造しないですむことが望まれる．筆者らは文献 22) にて，Hole Punching の原理を応用した Binding シーケンスを提案している．この方式は移動ノードがグローバルネットワークとプライベートネットワークをまたがって移動する場合に，既存の NAT を変更しないまま移動透過性[⋆1]を実現するものである．この方式を拡張した Binding シーケンスを導入することにより，まず EN 側 NAT のマッピングを行い，その情報を利用して HGW の NAT マッピングを生成すれば，Home-to-Home の通信が実現できると考えられる．

次に，IPv4 の延命策として LSN（Large Scale NAT）[23] の導入が検討されている．LSN が導入されると NAT が多段になり，EN から HGW へ直接制御メッセージを送信できなくなる可能性がある．解決方法として，LSN にも提案方式を実装し，HGW と協調してマッピングを行うことが考えられるが，LSN に機能追加することは現実的ではない．そこで，HGW が例えば STUN などを用いて LSN に対してマッピングを行い，マッピングで開けられた穴を通じて EN と HGW が制御メッセージを交換することが考えられる．この場合は制御メッセージを現状の ICMP ベースから UDP ベースへ変更し，さらに LSN にマッピングされた IP アドレス・ポート番号とホームネットワークの関係を管理するサーバの設置，EN が名前解決時に管理サーバから必要な情報を取得する仕組みの導入などが必要になると考えられる．

なお，LSN の導入と同時に Step-by-Step で IPv6 を導入することが検討されており，これには Softwire[24]，DS-lite（Dual Stack lite）[25]，6rd（IPv6 Rapid Deployment）[26] と呼ばれるいくつかの技術がある．これらの技術では HGW/IN と LSN またはその外部との間にトンネルを確立するため，このトンネルを通じて制御メッセージを交換する方式についても検討する余地がある．

5. 関 連 研 究

ホームネットワーク内のノードに外部からアクセスするためには VPN を利用する方法がある．例えば IPsec や SSL，SSH を利用した VPN がよく知られているが，リモートユーザの管理や外部からアクセス可能なサービスをコントロールすることが難しい．また，一般にネットワークレベルの VPN を利用すると EN がホームネットワーク内に参入する形となるため，本来アクセスを許可していない IN と通信できたり，例えば EN がウィルスに感染しているとその影響がホームネットワークに及ぶ危険性も考えられる．

一般的な VPN は接続機器間で予め IP アドレスや暗号化アルゴリズムなどを設定しておく必要がある．これに対して，通信開始前にこれらの設定を動的に行って柔軟に VPN を構築する技術としてオンデマンド VPN がある．文献 27) では，e-Key チップと呼ばれる 2

⋆1 通信中に移動しても通信が切断されない性質．

階層 PKI 技術を実装した耐タンパ IC チップにより厳密な機器認証を行った後，VPN 管理サーバで生成される IPsec 構成情報を VPN 機器に配信することにより，オンデマンドに VPN を構築する方式が提案されている．この方式は組織名やノードの種別・時間帯・ユーザの属性情報といった単位でアクセス制御ができるが，e-Key チップが組み込まれた VPN 機器を利用する必要がある．そのため，医療機関や行政，企業などを対象とした大規模な拠点間 VPN 構築には適しているが，本論文でターゲットとしている移動ノードとホームネットワーク間での導入は難しいと考えられる．

文献 28) では，NGN（Next-Generation Network）の特徴である電話番号に基づいた認証を行う方式を提案しており，ホームネットワークでの利用も対象としている．NTT コミュニケーション社のマルチポリシー VPN[29] では SIP（Session Initiation Protocol）技術と IPv6 技術を融合させた m2m-x 技術を利用することにより，グループ/ノード単位での VPN 接続を可能としている．しかし，これらのサービスを利用するためには対応プロバイダに変更したり，接続元と接続先の両ゲートウェイを専用装置に変更する必要がある．

異なるネットワーク間のノードを接続する方法としてオーバレイネットワークの構築が挙げられる．文献 30) では PeerPool と呼ばれる分散スマート環境接続技術が提案されており，DNS クエリを利用して通信ノードを仮想的に認識する点，機能拡張が困難な一般ノードをサポートしている点が本提案方式と類似している．移動ノードとホームネットワーク間で PeerPool を適用する場合，移動ノードに特別な機能を実装しなくてすむが，移動ノードが接続しているネットワークに PoolGW と呼ぶ制御用ホストが設置されていることが必須条件となる．移動ノードがどのネットワークに移動するか定まっていない以上，上記条件を満たすことは困難であると考えられる．また，本論文で想定しているサービス単位での制御までは考慮されていない．

フリービット社の Emotion Link ⋆1 ではアプリケーション毎に専用の VPN を構築できるため，一般の VPN より柔軟なアクセス制御が可能である．しかし HGW を越えるために，両エンドノードはインターネット上の専用サーバに対して IP トンネルを構築して，通信を中継させる必要がある．また，両エンドノードに専用のアプリケーションを実装したり，専用の USB トークンを装着する必要がある．

本論文による提案方式では，アプリケーションが利用するポート番号とグループを対応づけてアクセス制御するため，アプリケーションごとに異なる VPN を構築する場合と同様の効果が得られる．HGW の取り替えが必要ではあるが，EN に専用のハードウェアは必要なく，提案方式の機能を実装していればプロバイダに影響されないことから，一般的なデバイスと環境での利用が容易である．また，トンネリングを行わないセキュアなエンドツーエンド通信を実現でき，かつ一般の VPN より少ない管理負荷で柔軟なリモートアクセスを実現できる．

6. ま と め

本論文では，NAT 越え問題を解決する NAT-f に通信グループの概念と暗号化通信を導入したセキュアな NAT 越えシステムを提案した．従来の NAT-f はプライベートネットワークへのアクセス手段を提供していたが，不特定多数の外部ユーザがホームネットワークなどの内部ノードに自由にアクセスできてしまう問題があった．提案方式では，これまでノード単位でのグルーピングを行っていた通信グループの概念を内部ノードが提供するサービス単位へと拡張し，従来の NAT-f システムに導入した．これにより，外部からのアクセス制御と内部のサービス制御を同時に実現できることを示した．提案方式を実装したシステムを評価した結果，実用上問題ないオーバヘッドであることが確認できた．

今後は提案システムを一般公開する予定であり，ソースコードおよびドキュメントを整理を行う．興味のある方は筆者らのウェブサイトにアクセスされたい⋆2．

謝辞　本研究の一部は，日本学術振興会科学研究費補助金（特別研究員奨励費 20・1069）の助成を受けたものである．

参 考 文 献

1) Srisuresh, P., Ford, B. and Kegel, D.: State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs), RFC 5128, IETF (2008).
2) Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
3) Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet-draft, IETF (2009). http://tools.ietf.org/id/draft-ietf-behave-turn-16.txt
4) UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp
5) 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

⋆1 EmotionLink: http://www.freebit.com/el/index.html

⋆2 鈴木：http://www.ucl.meijo-u.ac.jp/　渡邊：http://www.wata-lab.meijo-u.ac.jp/

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).
6) 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).
7) 渡邊　晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌， Vol.38, No.4, pp.904–914 (1997).
8) Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).
9) 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).
10) Huttunen, A., Swander, B., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).
11) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).
12) Lewis, E.: The Role of Wildcards in the Domain Name System, RFC 4592, IETF (2006).
13) Krawczyk, H., Bellare, M. and Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, RFC 2104, IETF (1997).
14) Intel Corp.: *Using the RDTSC Instruction for Performance Monitoring* (1998). http://developer.intel.com/drg/pentiumII/appnotes/RDTSCPM1.htm
15) Okamoto, E. and Tanaka, K.: Key distribution system based on identification information, *IEEE Journal on Selected Areas in Communications*, Vol.7, No.4, pp. 481–485 (1989).
16) Brusilovsky, A., Faynberg, I., Zeltsan, Z. and Patel, S.: Password-Authenticated Key (PAK) Diffie-Hellman Exchange, RFC 5683, IETF (2009).
17) 武藤大悟，吉永　努：ルールベースアクセス制御機能を持つ DLNA 情報家電の遠隔共有支援機構，情報処理学会論文誌， Vol.49, No.12, pp.3985–3996 (2008).
18) 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).
19) Motegi, S., Takase, K., Idoue, A. and Horiuchi, H.: Proposal on Wide Area DLNA Communication System, *Proc. of IEEE CCNC 2008*, pp.233–237 (2008).
20) 田坂和之，茂木信二，磯村　学，井戸上彰：特定ユーザとの宅内コンテンツ共有方式，電子情報通信学会技術研究報告，IN2008-165, Vol.108, No.458, pp.197–202 (2009).
21) 鈴木秀和，渡邊　晃：NAT-f を用いたホームネットワーク間相互接続方式の検討，マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム論文集，Vol.2008, No.1, pp.1675–1682 (2008).
22) Suzuki, H., Terazawa, K. and Watanabe, A.: Implementation of NAT Traversal for Mobile PPC with the Principle of Hole Punching, *Proc. of IEEE TENCON 2009* (2009).
23) Yamagata, I., Nishitani, T., Miyakawa, S., Nakagawa, A. and Ashida, H.: Common requirements for IP address sharing schemes, Internet-draft, IETF (2010). http://tools.ietf.org/id/draft-nishitani-cgn-04.txt
24) Li, X., Dawkins, S., Ward, D. and Durand, A.: Softwire Problem Statement, RFC 4925, IETF (2007).
25) Durand, A.: Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, Internet-draft, IETF (2010). http://tools.ietf.org/id/draft-ietf-softwire-dual-stack-lite-04.txt
26) Despres, R.: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), RFC 5569, IETF (2010).
27) 高橋成文，東川淳紀，山本修一郎，小尾高史，谷内田益善，大山永昭：2 階層 PKI を用いたオンデマンド VPN システム，情報処理学会論文誌， Vol.46, No.5, pp.1129–1136 (2005).
28) Mizuno, S., Haruyama, T., Yamada, H., Abe, T., Kawashima, M. and Mizuno, O.: Adopting IPsec to SIP Network for On-Demand VPN Establishment between Home Networks, *Proc. of IEEE GLOBECOM 2008*, Vol.2008, No.13, pp.5672–5676 (2008).
29) NTT コミュニケーションズ：SIP と IPv6 でつくるオンデマンド VPN，NTT 技術ジャーナル，Vol.20, No.2, pp.28–31 (2008). http://www.ntt.co.jp/journal/0802/files/jn200802028.pdf
30) 榎堀　優，中野悦史，新井イスマイル，西尾信彦：PeerPool: DNS クエリを操作に用いた分散スマート環境間接続技術，情報処理学会論文誌コンピューティングシステム（ACS）， Vol.2, No.4, pp.37–47 (2009).
31) 北口善明：クライアント OS の IPv6 実装事情，*Interop Tokyo 2009* (2009). http://www.kokatsu.jp/blog/ipv4/data/interop2009/03_ClientOS_KITAGUCHI.pdf

付　　録

A.1 記号の定義

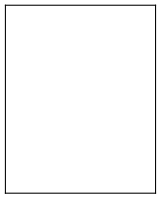
- Gi; グローバル IP アドレス
- Pi; プライベート IP アドレス
- Vi; 仮想 IP アドレス
- $A:p$; トランスポートアドレス（IP アドレス A とポート番号 p の組）
- gx; 通信グループ番号 x

- GKx; 通信グループ gx に対応するグループ鍵
- CK; 共通鍵
- Nn; ノード n が生成したノンス値
- $x \mid y$; データ x と y の連結
- $HMAC_K(M)$; 暗号鍵 K によるメッセージ M の HMAC
- $E_K(M)$; 暗号鍵 K によるメッセージ M の暗号化
- $S \leftrightarrow D$; S と D 間の通信
- $\{S \Leftrightarrow D\}$; S から D，または D から S へのアドレス変換

A.2　DNS 名前解決の詳細

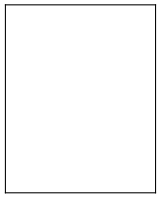
通信開始時に行われる DNS クエリは，EN のリゾルバ（OS）により挙動が異なる．現在の主要な OS は IPv6 に対応しているため，A レコードだけでなく，AAAA レコードのクエリも行う．文献 31) によると，Windows Vista，Windows 7，Mac OS X，FreeBSD は A レコード，AAAA レコードの順でクエリを実行する．ここで，提案方式では IP 層に実装したモジュールが受信した IPv4 の DNS 応答パケットをトラップし，メッセージを解析する．A レコードに関するクエリ結果であれば，提案方式に基づいた処理が行われ，それ以外の場合は何も処理を行わない．仮に IN が IPv6 アドレスを持っている場合，両クエリが成功することになるが，AAAA レコードの結果が優先され，IPv6 アドレス宛に通信を開始する．この優先順位は RFC3484 のポリシテーブルに基づいて決定されており，ほぼ全ての OS に実装されている．従って，IPv6 移行期に考えられるホームネットワークの IPv4/IPv6 混在環境において，提案方式が IPv6 通信に影響を及ぼすことはないと考えられる．

(平成 22 年 1 月 7 日受付)
(平成 22 年 6 月 4 日採録)



鈴木　秀和（正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．2009 年同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．2008 年日本学術振興会特別研究員．2010 年より名城大学理工学部情報工学科助教．ネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事．博士（工学）．電子情報通信学会，IEEE 各会員．



渡邊　　晃（正会員）

1974 年慶應義塾大学工学部電気工学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．