社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＱＡＩ－12　（２）
2004／7／12

オーバレイネットワークのためのプロキシ機構の提案

窪田　歩　三宅　優　田中　俊昭

株式会社 KDDI 研究所 〒356-8502 埼玉県上福岡市大原 2-1-15
E-mail: {kubota, miyake, toshi}@kddilabs.jp

あらまし　オーバレイネットワーク上で新しいネットワークサービスを実現するための種々のプロトコルが提案されているが，アプリケーションを新しいプロトコルに対応させなければ新サービスを利用できないことが普及の妨げとなっている．この問題を解決するため，既存 IP アプリケーションを改変することなく P2P オーバレイネットワークで提供される新しいサービスを利用可能とするプロキシ機構を紹介する．本稿では，i3 (Internet Indirection Infrastructure)と呼ばれるオーバレイネットワークを対象とし，i3 を用いて実現される NAT やファイアウォール透過な P2P アクセス，モビリティのサポート，セキュリティや QoS 制御のためのエンドホスト主導の通信経路設定など，様々な新しいネットワークサービスを，i3 対応のためのプロキシを直接インストールしたホストのみならず，ソフトウェアの追加が運用上もしくは実装上困難なネットワーク機器からも利用可能とする柔軟なプロキシ機構の実装と適用例について述べる．

キーワード　オーバレイネットワーク，P2P，i3，プロキシ

Proxy Mechanisms for Utilizing Overlay Networks from Legacy Applications

Ayumu KUBOTA　Yutaka MIYAKE　Toshiaki TANAKA

KDDI R&D Laboratories Inc. 2-1-15 Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan
E-mail: {kubota, miyake, toshi}@kddilabs.jp

Abstract　In order to add new network functions to the Internet, it is getting a common approach to implement them using overlay networks. By using overlay architecture, it is fairly easy to construct a whole new network with a rich function set, but in many cases it is not easy for end-users to utilize such networks because they have to adapt their applications to the new networks and the protocols. To mitigate this problem, we introduce proxy mechanisms that enable overlay networks to support legacy IP applications. In this paper, we focus on the overlay network called i3 (Internet Indirection Infrastructure) and show how legacy IP applications running in diverse environment can utilize new functions provided by i3, such as transparent P2P access to services behind NAT and firewall, mobility support, and the flexible routing mechanism for controlling QoS and security.

Keyword　Overlay network, P2P, i3, Proxy

1. はじめに

ネットワークの上で仮想的なリンクを形成し，独自のネットワークを構築するオーバレイネットワークにより，既存 IP ネットワークでは実現の困難な機能を提供する試みが行われている．オーバレイ型のネットワークとすることにより，既存 IP ネットワークを改変することなく，容易に新しいネットワーク基盤を構築することが可能であり，そのネットワーク基盤の上で，P2P ファイル交換などに適したコンテンツ志向のルーティング[1]，モビリティやマルチキャストのサポート，およびエンドホスト主導による経路制御などの新しいネットワークサービスの実現[3]，DoS 攻撃対策などのセキュリティ機構の実現[4]，ネットワーク障害に対する高い耐性の実現[6] [7]などが可能になるとされる．

ただし，一般的にこれらの新しい機能を利用するためには，アプリケーションの改変や新規開発が必要となるため，ネットワーク構築が容易であるだけでは，万人に利用可能な実用性の高い提案とはならない．このため，オーバレイネットワークの研究においては，既存の通信アプリケーションによるオーバレイネットワークの利用を仲介するプロキシ機構も提案されている[5][7]．しかしながら，これらのプロキシ機構は，互いに通信を行う双方のエンドホストにソフトウェアを追加することを前提としているため，インターネット上の一般の IP ホストとの通信や，エンドユーザによるソフトウェアの追加が困難なネットワーク機器との通

信などには適用できず，適用範囲が制限される．

そこで我々は，オーバレイネットワークの利用者が行う全ての通信においてオーバレイネットワークの新機能を活用可能とするプロキシ機構を提案し，この機構を i3 (Internet Indirection Infrastructure)[3]と呼ばれるオーバレイネットワークを対象に実装することで，その有効性の検証を行った．

以下では，2 節で関連研究について述べ，3 節でオーバレイネットワークのためのプロキシに必要な要件を整理した後，4 節でそれに基づいたプロキシ機構の提案を行い，5 節で i3 を対象としたプロキシ機構の実装とその有用性に関する考察を行う．

2. 関連研究

前節でも述べたとおり，オーバレイネットワークに対して[5][7]で提案されているプロキシ機構はローカルホスト上で動作させることを前提としているため，プロキシ機構をインストールした特定のホスト間でしかオーバレイネットワークの機能を利用できない．

新しいネットワークプロトコルへの既存の IPv4 アプリケーションの対応に関しては，IPv6 への移行技術の研究や開発において種々の成果が得られており，それらのいくつかはオーバレイネットワークへも応用することが可能である．ただし，IPv6 関連研究においては最終的にアプリケーション自身が IPv6 へ対応することを建前としているため，こうした変換技術により IPv4 アプリケーションからの IPv6 利用シーンを広げることはさほど重視されておらず，限定的な利用形態をカバーするものにとどまっている．

NAT 透過な P2P 通信の実現に関して，オーバレイネットワークを使わない手法として，STUN[8]などの提案がなされているが，アプリケーション個別の対応が必要となる．

以上を踏まえ，我々はオーバレイネットワークのためのプロキシ機構の検討にあたり以下を目標とした．

- アプリケーションの改変が不要
- ソフトウェアの追加等が困難なネットワーク機器にも対応
- プロトコル変換に加えオーバレイネットワークの提供する新機能の積極的な活用を実現
- プロキシ利用者の全ての通信をオーバレイネットワークで伝送可能

3. プロキシに対する要件

ここでは，オーバレイネットワークのプロキシ機構がサポートすべき通信形態を整理し，プロキシに対する要件をまとめる．

オーバレイネットワークは誰もが構築可能であり，かつ，本来その利用を誰に強制されるものでもない．そのため，オーバレイネットワークを意識しない一般ホスト同士の通信を強制的にオーバレイネットワーク経由で行わせることはここでは検討せず，オーバレイネットワークの提供する機能に有用性を認めた利用者達が管理するホスト間の通信，もしくは，それらのホストと一般ホストの間の通信が，全てオーバレイネットワーク経由で行われることになれば上述の第 4 項の目的を達するに十分であると考える．この前提に立てば，プロキシに求められる要件は以下の 2 つに整理できる．

- 利用者が管理するホストやネットワークを OS の種別などによることなく容易にオーバレイネットワークへ対応させること
- オーバレイネットワーク対応となったホスト同士の通信だけでなく，一般ホストとの通信をもオーバレイネットワークを経由させること

4. プロキシ機構の提案

上記で整理した要件に基づき，ホストやネットワークをオーバレイネットワーク対応にするためのプロキシ機構と，オーバレイネットワーク対応となったホストと一般ホストとの通信を仲介するプロキシ機構の 2 つに分けて，その具体的な実現方式を提案する．

4.1. オーバレイネットワーク対応のためのプロキシ

ここで提案するプロキシ機構は，対象ホストをオーバレイネットワークに対応させ，その上で動作する既存アプリケーションによるオーバレイネットワークの利用を実現するものである．

4.1.1. 基本方式

既存アプリケーションをオーバレイネットワークに対応させるにあたり，ドメイン名から IP アドレスへの名前解決処理にプロキシを介在させ，オーバレイネットワークのホストに対する名前解決要求に対して仮想的な IP アドレスを返させる仕組みをとった．これにより，オーバレイネットワーク上のホストへの通信が，アプリケーションからは通常の IP ホストへの通信に見えることになる．この状態で，仮想アドレスへのパケットをプロキシがキャプチャし目的のホストへ転送することで，既存アプリケーションによる IP 通信が実際にはオーバレイネットワーク経由で行われることになる．つまり，名前解決要求パケットと仮想アドレスへのパケットをキャプチャし，それらへの応答パケットを返す仕組みを用意すれば，オーバレイネットワークへの対応が可能となるのである．

これらの仕組みを用意する上で，IPv4 アプリケーションの IPv6 対応手法である BIS(Bump-in-the-Stack)や BIA(Bump-in-the-API)のように TCP/IP スタックやソケットライブラリへの実装を行うと，プロキシの移植性が低下するだけでなく，プロキシ機構を実装したホストに対してしか変換サービスを提供できないことに

なり，オーバレイネットワークへ対応させられる対象が限定されてしまう．これに対し，名前解決要求と仮想アドレスへのパケットがプロキシへ配送されるような経路制御が行われることだけを前提にしてプロキシ機構を設計すれば，プロキシが動作しているローカルホスト上のアプリケーションとリモートホスト上のアプリケーションとの区別なくプロキシサービスを提供することが可能となる．この場合，DNS サーバの指定や経路の追加が可能であれば，どのような IP 通信機器やネットワークもオーバレイネットワークへ対応させられ，利用者によるソフトウェアの追加が困難な家電ネットワーク機器などをオーバレイネットワークへ対応させたり，ホームネットワーク全体をオーバレイネットワークへ対応させたりすることも可能になる．

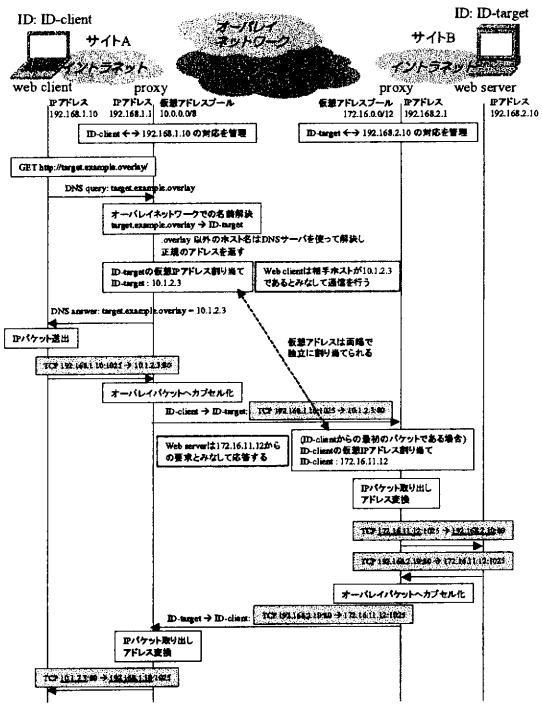

図 1　プロキシの動作シーケンス

4.1.2. 動作の概要

以上の考察を基にした提案プロキシ機構の動作を，2 つのサイト間の web 通信を例に示したものが図 1 である．図 1 のサイト A,B のプロキシはイントラネット内の各機器にオーバレイネットワークの ID を割り当て，各機器の IP アドレスとの対応を管理するとともに，それらの ID をもつノードとして他のオーバレイネットワークのノード(ここでは相手サイトのプロキシ)と相互に通信できるものとする．オーバレイネットワーク上のホストを指定するための仮想的なドメインを“.overlay”とし，“target.example.overley”などのホスト名からオーバレイネットワークでのホスト ID を取得する手段は，オーバレイネットワークに備わっているものとする．また，各サイトのプロキシは仮想アドレスに利用するアドレスプールを，それぞれ 10.0.0.0/8，172.16.0.0/12 と決めているものとする．図中の動作シーケンスの概略は以下の通りであり，これによりオーバレイネットワークを介した web client と web server 間の通信が実現される．

1. サイト A のプロキシは名前解決要求のホスト名(target.example.overlay)から web server のホスト ID(ID-target)を得，サイト B のプロキシは，サイト A のプロキシとの通信により web client のホスト ID(ID-client)を得る
2. 両プロキシは，相手ホストの仮想アドレスを各々独自に割り当て，クライアントホスト，相手ホスト ID 及び仮想アドレスの対応を管理する
   web client ←→ (ID-target, 10.1.2.3)
   web server ←→ (ID-client, 172.16.11.12)
3. web client は 10.1.2.3 への web アクセスを行い，web server は 172.16.11.12 からのアクセスに応答する形となり，これを実現するよう，双方のプロキシはオーバレイネットワーク経由で送受する IP パケットのアドレスを書き換えてクライアントホストへ転送する．

プロキシがオーバレイネットワークでのコネクション設定やパケット送受信の際の設定を適宜行うことで，オーバレイネットワークの機能を活用することが可能である．なお，プロキシをローカルで動作させた場合もサイト内での経路制御がホスト上での経路設定に変わるだけで，動作自体は同様である．

4.1.3. サイト単位でのプロキシの運用について

プロキシは一定時間使用しなくなった仮想アドレスを解放しアドレスプールに返すことで仮想アドレスの再利用を行うため，長期的にみれば接続可能なホストの数に制限はないが，仮想アドレスの数により同時に確立可能なセッション数は制限される．プロキシがサイト単位で運用される場合，この制限が深刻な問題となりうるが，仮想アドレスはサイト内でしか意味を持たないことから，サイト毎の責任において豊富にある未割り当ての IANA 予約アドレスを使用することで，実用上解消可能である．

なお，オーバレイネットワークによるモビリティのサポートを考えた場合，プロキシをローカルに動作させ，ホスト単位でオーバレイネットワークに対応させることが望ましいが，ネットワーク単位での対応で

あっても，DSL等により常時インターネットに接続されたホームネットワークなど，LAN上の各ノードのプライベートアドレスは固定で，外部接続用のグローバルアドレスが時折変更されるネットワークの場合，ネットワーク単位ではモビリティがサポートされることにより，リモートアクセスなどの利便性は向上する．またオーバレイネットワークで実現される NAT 透過なP2Pアクセスや各種セキュリティ機能等は活用可能である．

4.2. 一般ホストとの通信のためのプロキシ

ここで提案するプロキシ機構は，4.1のプロキシ機構と連携することで，オーバレイネットワーク対応ホストと，一般ホストとの通信をオーバレイネットワーク経由で行わせるためのものである．以下ではまず，こうした通信形態をサポートすることの必要性について述べた後，一般ホストへの通信と，一般ホストからの通信に分けて，その実現手法を述べる．

4.2.1. 対一般ホスト通信のサポートの必要性

4.1のプロキシ機構により，オーバレイネットワークの機能を既存アプリケーションから活用したいと考える利用者は，自身の管理するホストやネットワークを容易にオーバレイネットワークへ対応させることができるが，これだけではオーバレイネットワークの利用が，対応ホストやサイト間の通信に限定されるため，実際上はモバイルホストからホームネットワークへのアクセス等，極めて限られた用途でしか活用できないことになる．例えば，オーバレイネットワーク上でファイアウォールやネットワーク侵入検知等のサービスが実現され，モバイルホストに対してホストのロケーションに依存しないセキュリティ機構を提供できたとして，それが一般ホストとの通信の際に適用できなくては実用上意味をなさない．こうした観点から，一般ホストとのオーバレイネットワークを介した通信の実現が極めて重要となる．これに対して我々は，オーバレイネットワーク上に一般ホストとの通信を仲介するプロキシゲートウェイ(プロキシ GW)を配備し，オーバレイネットワーク対応ホスト(もしくはサイト)とプロキシGWとの間の通信はオーバレイネットワーク経由，プロキシGWと一般ホスト間の通信は直接IPで行うことでその実現を図った．

4.2.2. 一般ホストへの通信

プロキシGWを介して一般ホストへの通信を行う場合の模式図を図2に示す．簡単に言えば，プロキシGWがNATの役割を果たし，内部ホストとして扱われるオーバレイネットワーク対応ホストからインターネットへの通信を仲介する仕組みとなっている．

このプロキシGWを介して一般ホストへの通信を行う場合，一般ホストを対象とする名前解決要求(target.example.net)を受けたクライアント側のプロキシは，正規のDNSサーバに問い合わせを行って正しいアドレスをクライアントへ返す代わりに，このホストへの通信の中継をプロキシGWに依頼する．この要求を送る際に，同一クライアントから異なるホストへ通信を行う場合の識別を可能とするためセッションID(s1)を付与して一緒に送付する．プロキシGW側は，ホスト名の解決を行い(12.34.56.78)，当該セッション用の仮想アドレス(10.2.3.4)を割り当て，それらを要求元のホスト ID(ID-client)及びセッション ID(s1)と対応付けて管理する．以上の処理が完了したらクライアント側のプロキシは，target.example.net に独自に仮想アドレスを割り当て，それをクライアントに返す．以降，クライアントがその仮想アドレスへ送るパケットは，クライアント側のプロキシによりセッション ID(s1)を付与してオーバレイネットワーク経由でプロキシ GWへ送られる．プロキシ GW はクライアントのID(ID-client)とセッション ID(s1)を基に，受け取ったパケットの宛先アドレスを 12.34.56.78，送信元アドレスを 10.2.3.4 に書き換え，NAT を利用してインターネットへ送信する．この際，送信元アドレスは NAT によりプロキシGWのアドレス(11.22.33.44)に書き換えられ，ターゲットホストからの応答も同アドレスへ返ってくるが，これは NAT により 10.2.3.4 へ書き戻されるため，このアドレスをキーにして，クライアントのID(ID-client)を求め，オーバレイネットワーク経由でクライアント側のプロキシへ転送し，通信を成立させる．

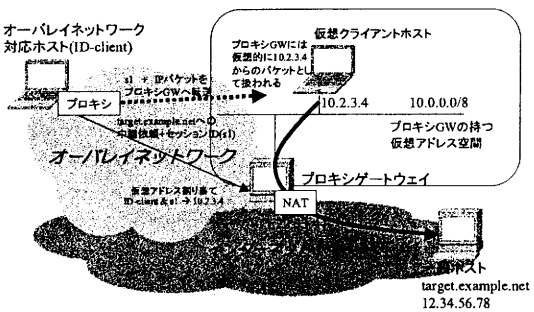

図 2　一般ホストへの通信

以上の仕組みにより，オーバレイネットワーク対応ホストは，一般ホストへ通信を行う際にもオーバレイネットワーク上で実現されるモビリティサポートなどの機能を利用することが可能となる．

4.2.3. 一般ホストからの通信

一般IPホストからの通信の場合，まず，既存のドメインの配下などにオーバレイネットワーク用のドメインを正規に登録し，正規のDNSサーバと連携させてプロキシを動作させる必要がある．この場合，DNSサーバが返す仮想アドレスはグローバルアドレスである必要があるため，利用可能なアドレス数が限定され，ここまで述べてきた仮想アドレスによるコネクションの識別は困難となる．ここで，同様の状況においてIPv4ホストからIPv6ホストへの通信を実現する[9]の手法を用いると，少数のグローバルアドレスにより多数のオーバレイネットワークホストへの接続を実現させることが可能となる．

ただし，この手法ではアプリケーションが1回名前解決を行った後，解決されたアドレスに対して複数回コネクションを設定するような場合に通信が行えないという問題があり，特に複数のTCPコネクションを利用するWebアクセスにおいてこの問題が顕在化する[1]．Webアクセスへの対処に限れば，以下に述べるWebトラヒック専用のプロキシ機構を追加で設けることにより対応が可能である．これは限定的な解ではあるが，Webアクセスが主流を占めるインターネットの現状において実用上の問題をほぼ解消可能であると考える．

まず，オーバレイネットワーク対応ホストの上でWebのトランスペアレントプロキシを動作させ，これを一般ホストからのWebアクセス専用のプロキシとする．オーバレイネットワーク対応ホスト上で動作するWebのトランスペアレントプロキシは，他のIPアプリケーション同様，4.1のプロキシにより，どのオーバレイネットワーク対応ホストのWebサーバとも相互に通信することが可能である．ここで，上述のプロキシ機構において，Webトラヒックのみを Webアクセス専用プロキシにリダイレクトさせる．Webアクセスに使われているHTTP/1.1プロトコルでは，HTTPリクエストの中に接続先ホスト名が必ず含まれているため，パケットを受け取ったWebのトランスペアレントプロキシは，この情報を元にオーバレイネットワーク上のWebサーバへリクエストを送信し，受けた応答をクライアントにインターネット経由で送り返すことで一般ホストからのWebアクセスを成立させられる．

以上2種類のプロキシ機構を組み合わせることで，一般ホストからの通信も実用上問題のないレベルで実現できることになる．

[1] DNSの応答はTTLを0にして返すため，手前のDNSサーバでアドレスがキャッシュされることはなく，コネクション設定のたびに名前解決要求を出すアプリケーションでは問題とならない．

5. オーバレイネットワークi3への適用と考察

以上で提案したプロキシ機構をオーバレイネットワークi3へ適用する形で実装し，その有効性を検証した．以下では，i3の概要，今回行った実装の特徴とその利点，プロキシによってi3を利用することの有用性に関する考察について述べる．

5.1. i3の概要

i3ではエンドノードが256-bitのIDを持ち、このIDを介して相互に通信を行う．ノードのIDと，その配送先IPアドレスもしくは次ホップのノードIDとの対応をi3トリガーと呼び，P2Pのオブジェクトルックアップに用いられるChord[2]を利用してi3ネットワークによって管理される．i3において通信経路はこのi3トリガーを介して間接的に確立されるため，i3トリガーを更新したり追加したりすることで簡単にモビリティのサポートやマルチキャストなどを実現できる．また，パケット送信時に宛先IDをスタックしたり，連鎖したトリガーを登録したりすることで，エンドノード主導での経路設定も可能となり，QoSルーティングなどの高度なネットワークサービスに応用できる．

i3を利用するクライアントに対しては，トリガーの登録(更新)，宛先IDを指定してのデータの送信，トリガーの削除という3種類の操作を行う簡潔なAPIが提供されており，その他の付随的な処理を行う関数群を含むアプリケーション作成用のライブラリが公開されている．

5.2. i3用プロキシ機構の実装

提案したプロキシ機構をi3に適用するにあたっては，図1のシーケンスに，各プロキシによるi3トリガーの登録，プロキシ間でのi3 IDの交換，i3 IDと仮想アドレスの対応づけ等の処理を追加した．モビリティを実現するトリガーの動的な更新はi3の提供するライブラリによって実現されておりプロキシ自体は関与する必要がない．コネクション個別の通信経路の設定など，i3クライアント自身によって設定すべき機能は，トリガーの登録処理などにおいてプロキシによって制御される．

一方，名前解決要求パケット及び仮想アドレスへのパケットのキャプチャとそれらへの応答処理など，i3に依存しないプロキシの基本部分については，様々なOSで利用可能となっている仮想トンネルインタフェースデバイス(TUN/TAPデバイス)を利用して実装する方法を取った．これは，モビリティサポートなどのオーバレイネットワークの機能を活用する上では，ローカルホスト上でプロキシが動作することが望ましく，プロキシの本体は移植性の高い実装がなされていることが重要と考えたためである．これにより，パケットの送受，カプセル化などを行うプログラムは一般ア

プリケーションとして作成することが可能となり，TUN/TAPデバイスをサポートするOSへの移植性が高まった．同時に，ホストOS側への要求も，名前解決要求パケットと仮想アドレス向けパケットを仮想トンネルインタフェースへ出力するというネットワーク設定だけにとどまり，プロキシの動作のOSへの依存性も低くなっている．プロキシは当初Linuxで開発したが，TUN/TAPデバイスがOpenVPNプロジェクトによってWindows 2000/XPへ移植されたことにより，Windowsでも動作可能になっており，また，同様にTUN/TAPデバイスの搭載されているBSD系のOSへの移植も容易であると考えている．

5.3. プロキシによるi3利用の有用性

プロキシがi3関連の制御を行うため，アプリケーション自体を改変することなくi3の種々の機能を活用することが可能となった．具体的には，i3のグローバルIDを用いたNAT透過なP2Pアクセス，モビリティのサポート，相手ホストに対するアドレス情報の隠蔽などが挙げられるが，プロキシがi3での経路設定を行うことで，i3上で実現されるネットワークセキュリティやQoSルーティングなどのサービスを利用するなどの，更に高度な活用も考えられる．

一方で，IPによる通信をオーバレイネットワーク経由で行うことにより，通信オーバヘッドが増大する欠点もある．元のIPパケットにi3のヘッダが付加された上で，更にIPとUDPもしくはTCPのヘッダが付加されてネットワークへ送出されるため，ヘッダのオーバヘッドが極めて大きくなる．また，フラグメンテーションを避けるためMTUサイズを小さくすると，更にヘッダの比率が増して通信効率が下がる．加えて，パケットの伝送が常にi3サーバを介して行われるため，IPネットワークからみた通信経路は最適とはならない．通信経路のIPレベルでの最適化に関しては，i3をトリガーの参照にのみ用いて，実際のデータの送受は直接ホスト間で行う方法も考えられる．この場合，i3による通信の柔軟性は失われるが，利用状況によっては有効なオプションになると考えられる．

現状のプロキシの実装においては，両端のプロキシにおいて独立に仮想アドレスの割り当てを行い，パケット受信時にその宛先と送信元アドレスを各々が割り当てた仮想アドレスに書き換えている．これにより，他のホストが使用する仮想アドレスとは無関係に自ホストもしくはサイト内で使用する仮想アドレスを決定することが可能となる一方で，FTPなどのNATと親和性のないアプリケーションは利用不可能となり，これが大きな制限事項となっている．これに対しては，NAT同様にプロキシにおいてアプリケーション個別の対応を行う手法の他，セッション開始時にプロキシ間で交渉を行い両者が合意した仮想アドレスを利用することでアドレス変換を不要とする手法が考えられる．なお，アプリケーションのIPv6対応が進めば，仮想アドレスに潤沢なIPv6アドレスを利用することが可能となり，この問題や，4.2.3の問題がより簡潔に解決されることが期待される．

6. おわりに

オーバレイネットワーク上で実現される新しいネットワーク機能は，プロキシを利用することで様々な環境で動作するホストから既存のIPアプリケーションによっても活用可能であり，オーバレイネットワークによるネットワークの機能拡張が，極めて実用性の高いアプローチとなりうることを示した．今後，オーバレイネットワークを利用したセキュリティ機構の実現など，オーバレイネットワーク上で提供されるサービスの高度化について検討を行う予定である．

謝辞

本研究は平成15年度にカリフォルニア大学バークレー校と株式会社KDDI研究所との間で行われた共同研究の中で実施された．バークレーにおいて本研究の機会を与えて頂いたIon Stoica教授とDoug Tygar教授ならびに関係の学生諸氏に深謝する．

文　献

[1] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network", in Proc. NOSSDAV, Port Jefferson, NY, Jun. 2001, pp. 11-20

[2] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications", In Proc. Of ACM SIGCOMM, 2001.

[3] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, "Internet Indirection Infrastructure", In SIGCOMM, 2002.

[4] Daniel Adkins, Karthik Lakshminarayanan, Adrian Perrig, Ion Stoica, "Towards a More Functional and Secure Network Infrastructure", UCB Technical Report No. UCB/CSD-03-1242, 2003.

[5] Shelley Q. Zhuang, Kevin Lai, Ion Stoica, Randy H. Katz, Scott Shenker, "Host Mobility using an Internet Indirection Infrastructure," *First International Conference on Mobile Systems, Applications, and Services (ACM/USENIX Mobisys)*, May, 2003.

[6] Ben Y. Zhao, Ling Huang, Jeremy Stribling, Sean C. Rhea, Anthony D. Joseph, and John Kubiatowicz, "Tapestry: A Resilient Global-scale Overlay for Service Deployment", *IEEE Journal on Selected Areas in Communications, January 2004, Vol. 22, No. 1.*

[7] Ben Y. Zhao, Ling Huang, Jeremy Stribling, Anthony D. Joseph and John D. Kubiatowicz, "Exploiting Routing Redundancy via Structured Peer-to-Peer Overlays", Appears in *Proceedings of 11th IEEE International Conference on Network Protocols (ICNP)*

[8] J.Rosenberg, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC3489, IETF, March 2003

[9] 屏　雄一郎，窪田　歩，堀田 孝男，山崎 克之，"IPv4-IPv6相互通信方式の提案と実装、評価"，電子情報通信学会和文論文誌B，Vol.J86-B, No.8, pp.1523 - 1532, 2003年8月