平成23年度　修士論文

邦文題目

IPv6におけるネットワーク構成隠蔽の提案

英文題目

Proposal on the Concealment of the Network Topology in IPv6

情報工学専攻

(学籍番号: 103430010)

久保敷　透

提出日: 平成24年2月9日

名城大学大学院理工学研究科

内容要旨

グローバル IPv4 アドレスの枯渇に対する根本的な解決策として，IPv6 への移行が必須である．しかし，IPv6 へ移行した場合，NAT による副次的な利点である，ネットワーク内部が隠蔽されるという利点がなくなり，アドレスからネットワーク構成が予測される可能性がある．これを防止する方法として，NPTv6 や Mobile IPv6 を利用した方法，ルータにホストルートを設定する方法がある．しかし，NPTv6 ではアプリケーションが制約され，Mobile IPv6 では経路冗長，ホストルートでは，ルーティングテーブルの増大が課題となる．

本論文では，新たに隠蔽アドレスを定義し，インターネット上の端末に対する通信に隠蔽アドレスを用いることにより，ネットワーク構成を隠蔽する方式を提案する．その際，隠蔽アドレスではネットワーク内でのルーティングをすることができないためカプセル化することにより，ルーティングを可能にする．提案方式のカプセル化処理を実装し，評価を行った．その結果，カプセル化処理にかかるオーバヘッドによる劣化が見られないことを確認した．

目 次

第1章　はじめに

インターネットが急激に普及したことにより，グローバル IPv4 アドレスの枯渇が問題になっている．すでに ICANN（Internet Corporation for Assigned Names and Numbers）から各地域レジストリへの配布が終了しており，さらに，JPNIC（Japan Network Information Center）においても IPv4 アドレスの在庫が枯渇したと報告されている [1]．これまで，アドレス枯渇問題に対しては，プライベートアドレスを定義し，一つのグローバルアドレスを複数の端末で共有するすることにより，IPv4 を延命させてきた．プライベートアドレス空間とインターネットの接続には，NAT（Network Address Translation）が必要となる．このとき，インターネット側からプライベートアドレス空間の端末へ接続を開始しようとしたときに，ネットワーク内部の構成がわからないため，通信を開始できない弊害が生じている．これを NAT 越え問題と呼び，IPv4 の汎用性を阻害する要因となっている．また，NAT ではパケットのアドレスを書き換えるため，アドレス情報を扱う FTP（File Transfer Protocol）[2] や SIP（Session Initiation Protocol）[3] といったアプリケーションは ALG（Application Level Gateway）を使用しなければならず，また，アプリケーション毎に対応しなければならないという課題もある．

その反面，NAT を用いることによって，組織内のネットワーク構成や端末に割り当てられているアドレスを隠蔽できるという利点が副次的に生まれている．企業のネットワーク管理者はできるだけ外部に情報を漏らしたくないという考えがあり，ネットワーク内部の情報を隠蔽できることは，セキュリティ上有用であるという考えが根強い．また，PCI（Payment Card Industry）のデータセキュリティ基準（PCI Data Security Standard）[4] では，支払いカードの情報を扱う組織はインターネット側に組織内のアドレスを開示してはならないことが規定されている．

しかし，IPv4 アドレスの枯渇は深刻であり，アドレス枯渇の根本的な解決策である IPv6 [5] への移行が必須である．IPv6 は，IPv4 アドレスの 32 ビットに対し，128 ビットに拡張され枯渇の心配はない．そのため，NAT が不要になり NAT 越え問題やアプリケーションが制約されるといった問題は解消され，インターネット本来のエンドエンド通信が可能となる．しかし，NAT によってネットワーク内部を隠蔽できるという副次的な利点がなくなり，アドレスから端末やネットワーク構成が特定される可能性がある．

そこで，IPv6 へ移行した場合においても端末やネットワーク構成を隠蔽できる方法が考えられている．端末に対するプライバシー問題を解決するアドレスとして，下位 64 ビットのインタフェース ID をランダムに生成する一時アドレス（Temporary Address）[6] が定義されている．しかし，一時アドレスは端末の特定を防ぐことはできるが，実際のサブ

ネット ID が公開されるため，ネットワーク構成が予測される懸念がある．ネットワーク構成を隠蔽できる技術として，以下のような方式がある．NPTv6（IPv6-to-IPv6 Network Prefix Translation）[7] は IPv6 アドレスの変換を行う技術であり，IPv4 の NAT に類似した技術である．NPTv6 は，ネットワーク内部を隠蔽できるが，アドレス変換を行っているため，SIP などのようにメッセージにアドレス情報が含まれるようなアプリケーションは制限される．Mobile IPv6 を用いた方式 [8] は，移動透過性の技術をネットワークの隠蔽に応用する方式である．この方式では，通信開始時にホームエージェントを経由するため，経路の冗長が生じるという課題がある．ホストルートを用いる方式 [8] は，ネットワークを隠蔽するために，アドレスをランダムに生成したものを用いる．そのときのルーティングのために，ルータに全端末のホストルートを設定する方式である．この方式では，ルーティングテーブルのエントリー数が膨大になってしまいルータへの負荷が大きいという課題がある．

そこで本論文では，ネットワーク構成を隠蔽する方式として，ネットワーク内部の端末に内部通信用と外部通信用の 2 つのアドレスを持たせ，通信相手端末の位置によりアドレスを使い分ける方式を提案する．ネットワーク外部に存在する端末との通信には，サブネット ID とインタフェース ID をランダムに生成したアドレスを用いる．このアドレス宛のパケットをネットワーク内部でルーティングさせるためにトンネル技術を用いる．

以下，2 章で既存技術の詳細を説明し，3 章で提案方式について述べる．4 章で実装評価，5 章でまとめを行う．

第2章　既存技術

2.1　一時アドレス

IPv6 の特徴の 1 つとして，DHCP を使用せずに，アドレスを生成することができるステートレスアドレス自動生成機能がある．通常生成される IPv6 アドレスは図 2.1 のように構成されている．端末はルータから通知されるプレフィックス広告から上位 64 ビットのグローバルルーティングプレフィックスとサブネット ID を取得する．そして，下位 64 ビットをインタフェース ID を MAC アドレスから生成する．しかし，この方法により生成されたアドレスは，MAC アドレス情報が含まれるため端末が特定されやすい課題がある．そこで，乱数によりアドレスを生成する一時アドレス（TA：Temporary Address）が定義された．図 2.2 に一時アドレスの構成を示す．一時アドレスは，下位 64 ビットのインタフェース ID を，ランダムに生成することにより，端末を特定されにくくする．しかし，サブネット ID はインターネット上にそのまま公開されるため，ネットワーク構成が推測されるおそれがある．

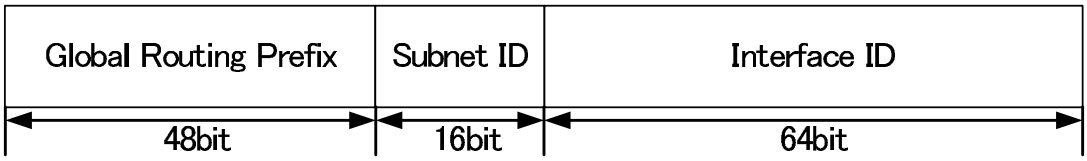

図 2.1　IPv6 アドレスの構成

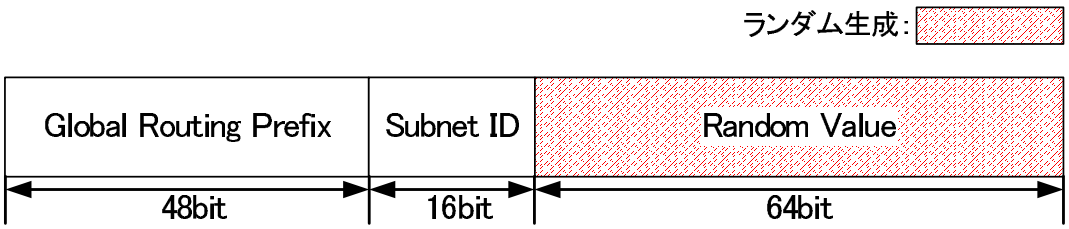

図 2.2　一時アドレスの構成

2.2 NPTv6

NPTv6 は，IPv4 の NAT のように，IPv6 アドレスを変換する方式である．

本来，IPv6 はアドレスの数が豊富であるため，アドレスを変換する必要はない．しかし，ネットワーク管理者は NAT を使用し，組織内をグローバルアドレス空間から切り離したアドレス空間にすることにより，アドレス管理が容易になると考えている．また，NPTv6 の第一の目的ではないが，IPv4 における NAT のように，副次的な利点としてネットワーク構成を隠蔽することができる．NPTv6 の動作を図 2.3 に示す．NPTv6 は，マッピングテーブルを保持せずに，アドレスを一対一に対応させることができるため，双方向の通信が可能であり，IPv4 のような NAT 越え問題は生じない．NPTv6 機器のインターネット側にはグローバルアドレス，ネットワーク側には，ローカルネットワークでのみ有効なアドレス ULA（Unique Local Unicast IPv6 Address）[9] が割り当てられる．ULA のアドレス構成を図 2.4 に示す．ULA は，アドレスのスコープとしてはグローバルであるが，ネットワーク内部のみでの使用を目的として定義されたアドレスである．ULA はグローバル識別子である 40 ビットをランダムに生成している．そのため，万が一アドレスが漏れた場合でもアドレスが重複する可能性を低減している．

アドレスを変換するときは，変換アルゴリズムに従い，下位 64 ビットのインタフェース ID だけを残し，プレフィックスを変換する．このときアドレス変換前と後でトランスポート層のチェックサムが変わらないようにサブネット ID の値を工夫する．しかし，この方式では，ペイロード内にアドレス情報を含む FTP や SIP などのアプリケーションが制約されてしまうという，IPv4 の NAT と同様の課題が残り，IPv6 へ移行したときの利点が損なわれてしまう．

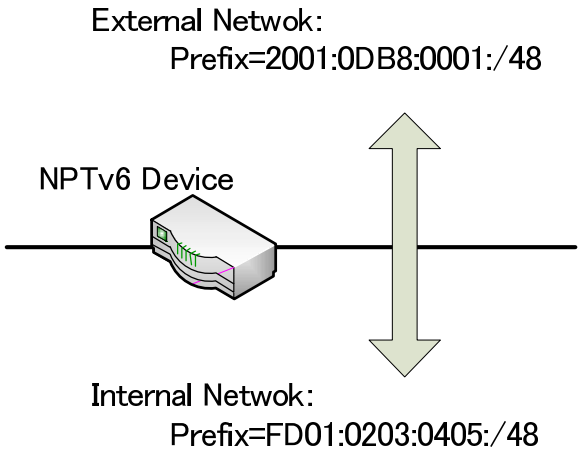

図 2.3　NPTv6 の動作

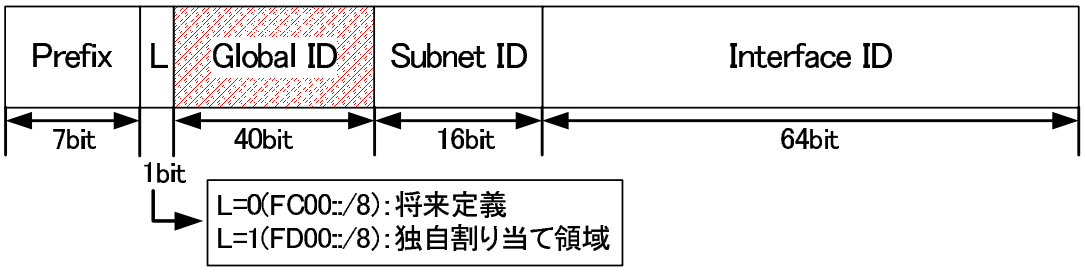

図 2.4　ユニークローカル IPv6 ユニキャストアドレスの構成

2.3　Mobile IPv6 を用いた方式

この方式では，移動透過性の技術である Mobile IPv6 を利用し，ネットワーク構成を隠蔽する方式である．Mobile IPv6 は，移動ノードである MN（Mobile Node）と通信相手である CN（Correspondent Node）の通信において，HA（Home Agent）を経由し，CN に対して MN の移動を隠蔽することにより，移動後でも通信を継続させることができる技術である．図 2.5 に Mobile IPv6 によるネットワーク構成隠蔽の例を示す．ゲートウェイが HA，内部端末 IN（Internal Node）1，2 が MN，インターネット上に存在する外部端末 EN（External Node）が CN の役割を果たす．IN1 にはホームアドレス（HoA：Home Agent）として，任意に設定したアドレスを割り当てる．この任意に設定したサブネット領域を論理サブネット（Logical Subnet）と呼ぶ．論理サブネットは，実際のネットワーク構成とは関係ないため，ネットワーク構成を隠蔽することができる．また，気付けアドレス（CoA：Care-of Address）として，ネットワーク構成に応じたアドレスが割り当てられる．IN1 が EN と通信する場合は，IN1 は送信元アドレスを HoA に設定する．そして，このパケットを送信元アドレス CoA でカプセル化してゲートウェイへ送信する．ゲートウェイまで届けられたパケットはデカプセル化され，EN まで届けられる．これにより，EN に届けられたパケットの送信元アドレスは，サブネット ID が任意の HoA であるため，EN は実際のネットワークを知ることができない．

しかし，この方式では以下のような課題がある．Mobile IPv6 には経路最適化という機能があり，この機能が有効であると移動後に取得したアドレスを通信相手に通知し，HA を経由せずに直接通信を行おうとする．つまり，この方式で経路最適化をしてしまうと，CoA を EN に通知することになり，実際のネットワーク構成が知られてしまう．そのため，経路最適化機能は無効にしなければならない．この機能を無効にしているときは，常に HA を経由した通信になるため，例えば，IN2 との通信においても，ゲートウェイと経由した通信になり経路冗長となる．内部端末と直接通信を行いたい場合は，経路最適化を有効にする必要があるが，経路最適化の制御パケットをインターネット上に流さないように，ゲートウェイでフィルタリングする必要がある．しかし，このときにも通信開始時に HA を経由してしまうことは避けれられない．

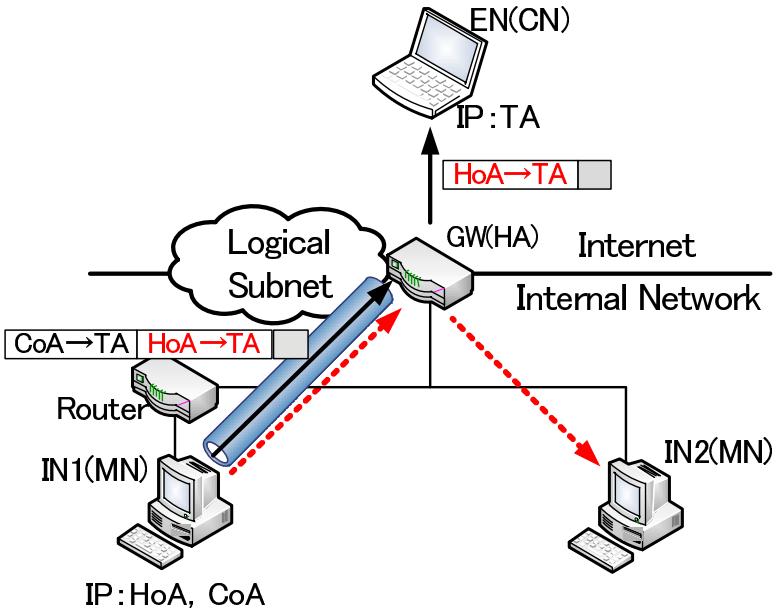

図 2.5　Mobile IPv6 によるネットワーク構成隠蔽

2.4　ホストルートを用いた方式

ホストルートを用いた方式では，サブネット ID を任意の値に設定したアドレスを端末に割り当て，このアドレスのルーティングのために，ホストルートを全ルータに設定するものである．ホストルートとは，ルーティングテーブルに端末ごとのルートを設定するものである．ホストルートでは，サブネット ID がどのような値であってもルーティングが可能である．しかし，端末数だけルータにホストルートを設定しなければならないため，組織の規模が大きくなるほど，ルーティングテーブルのエントリ数が膨大になり，ルータに負荷がかかる可能性がある．また，ルーティングテーブルの管理が煩雑になる．

第3章　提案方式

3.1　システム構成

提案方式では，内部端末に2つのアドレスを保持させ，通信相手端末の位置に応じてアドレスを使い分けることにより，ネットワーク構成を隠蔽する．外部端末との通信時には，ランダムに生成したアドレスを用いて通信し，内部端末との通信には，ローカルでのみ有効なアドレスを用いて通信する．提案方式のシステム構成を図 3.1 に示す．ネットワーク内部には IN1 と IN2 が存在し，インターネット上には EN があるとする．内部端末には外部通信用アドレス CA（Concealed Address）と内部通信用アドレス ULA（Unique Local IPv6 Unicast Address）の 2 つのアドレスが割り当てられる．CA は提案方式で新たに定義する隠蔽アドレスである．また，外部との通信パケットを中継し，かつ隠蔽アドレスの管理を行う隠蔽アドレス管理サーバ（Concealed Address Management Server：以下 CAM Server）をゲートウェイ直下に設置する．内部端末 IN1 が EN と通信する場合，IN1 は EN がインターネット上に存在していると判断したときは，CA1 を IN1 のアドレスとし，IN1，CAM Server 間でトンネル経路を生成することにより通信を行う．通信相手が IN2 である場合には，お互いに ULA を用いて通信を行う．

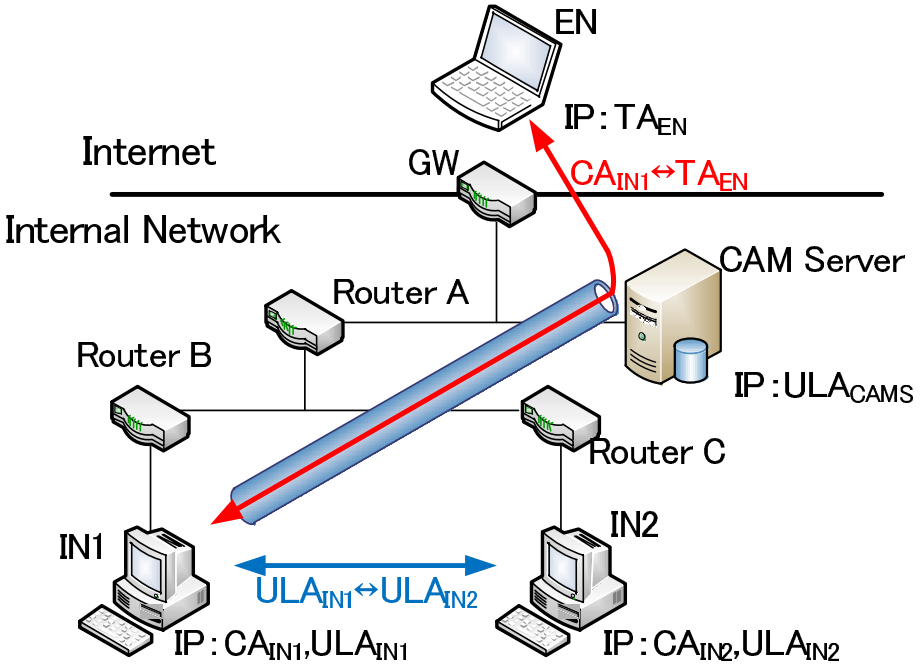

図 3.1　提案方式のシステム構成

3.2 アドレスの定義

提案方式で使用するアドレスについて以下に述べる．通信相手がネットワーク内部に存在する場合，ネットワーク内でルーティングできるアドレスで良い．そこで提案方式では，既存技術の NPTv6 でも使用している ULA を，内部端末同士の通信に使用する．

通信相手がインターネット上の端末の場合は，新たに定義した CA（Concealed Address）を用いる．CA のアドレス構成を図 3.2 に示す．CA はサブネット ID を含めた下位 80 ビットを独自に生成し，グローバルルーティングプレフィックスと組み合わせて構成されている．80 ビットのうち上位 4 ビットを CA 判定ビットとして，CA であることを判断する領域とする．それ以下の 76 ビットはランダム生成した値を用いる．また，CA には期限を設け，常に同じアドレスを使い続けないようにする．CA はサブネット ID の部分までランダムに生成することにより，ネットワーク構成を隠蔽することが可能となる，しかし，ネットワーク内でのルーティングに必要なサブネット ID の値がランダムであるため，このままではルーティングすることができない．そのため，CA を使用する場合には，CAM Server との間でトンネルを構築することで，ルーティングを可能とする．新たに付加する IP ヘッダには ULA を使用する．CA は，CAM Server において重複しないアドレスを生成し，各端末へ配布する．

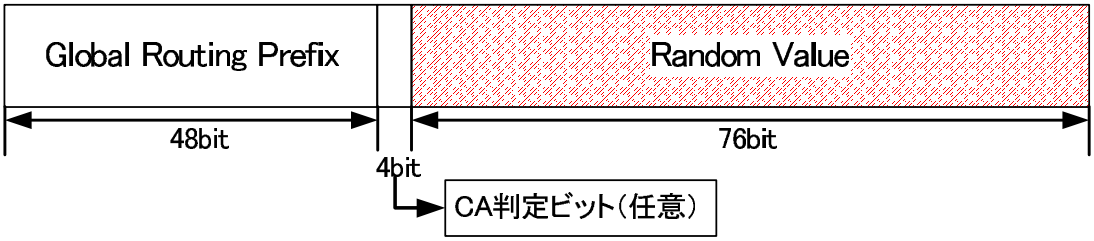

図 3.2　隠蔽アドレスの構成

3.3 CAM Server

CAM Server の主な機能として，CA の生成，再配布，および内部端末が外部端末との通信に必要となるトンネルを構築する役割を担う．図 3.3 に IN が CA を取得するときの動作を示す．IN1 は起動時に，ステートレスアドレス自動生成により，ルータから ULA のプレフィックス広告を受ける．取得したプレフィックスと自身で生成したインタフェース ID を組み合わせ ULA_{IN1} を生成する．次に，ULA_{IN1} を用いて CAM Server へ CA を要求するパケット（CA Request）を送信する．これに対して CAM Server は重複しないように CA_{IN1} を生成し，IN1 へ CA_{IN1} を通知する（CA Response）．また，CA_{IN1} と ULA_{IN1} の関係を登録する．そして，CA を用いた通信を可能とするために，IN と CAM Server 間で ULA によるトンネル経路を構築する．また，CA には期限を設けているため，新たに CA

を要求する必要がある．端末からの CA 更新要求に対して CAM Server は，新たに CA を生成し CA と ULA の関係を更新する機能を有する．

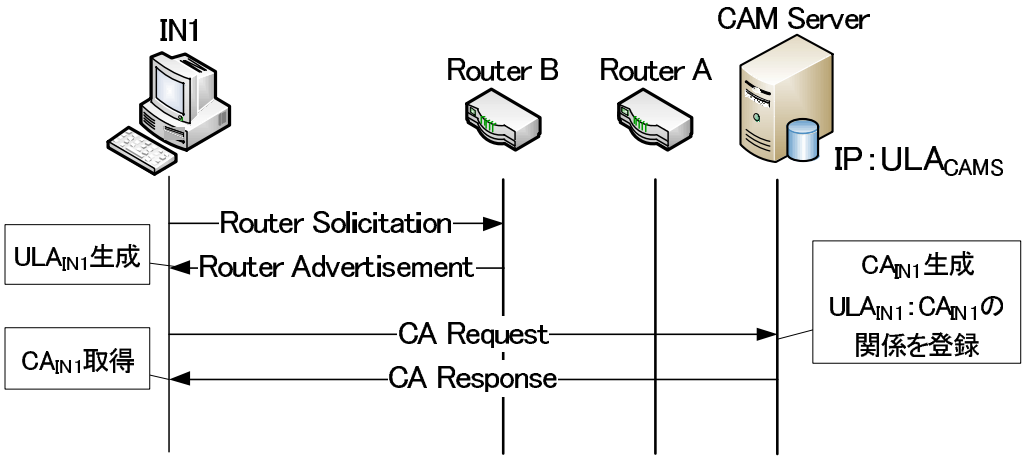

図 3.3　CA の取得動作

3.4　通信動作

図 3.4 に提案方式の通信動作を示す．ネットワーク構成は図 3.1 と同様である．すでに内部端末 IN1 は，CA_{IN1} を取得しているものとする．IN1 は CA_{IN1} と ULA_{IN1} の 2 つのアドレス，CAM Sever には ULA_{CAMS} が割り当てられている．そして，外部端末 EN には一時アドレス TA_{EN} が割り当てられている．また，通信パケットを

{ 送信元アドレス→宛先アドレス }

のように表す．

IN1 は通信開始時に通信相手の位置により，送信元アドレスを決定する．送信元アドレスの決定には，RFC3484 [10] で定義されているソースアドレス選択機能が用いられ，宛先アドレスのプレフィックスから複数割り当てられているアドレスの一つを送信元アドレスとして決定する．この機能を利用し，通信相手が外部端末であれば，CA_{IN1} を送信元アドレスとして決定する．カプセル化ヘッダの送信元アドレスを ULA_{IN1}，宛先アドレスを CAM Server のアドレス ULA_{CAMS} とする．パケットが CAM Server に到達したとき，CAM Server はデカプセル化し，送信元アドレス CA_{IN1}，宛先アドレス TA_{EN} のパケットを取り出し，EN へ送信する．EN から IN1 宛にパケットが送信されてきた場合，CA_{IN1} のグローバルプレフィックスを参照することにより，組織のゲートウェイまで届く．ゲートウェイまで届けられたパケットの宛先アドレスの CA 判定ビット領域が CA として登録されているアドレスであれば，CAM Server へ転送する．CAM Server では，予め CA

の生成時に CA_{IN1} と ULA_{IN1} の関係が登録しているため，この情報を利用し送信元アドレス ULA_{CAMS}，宛先アドレス ULA_{IN1} の IP ヘッダでカプセル化し IN1 に送信する．

相手端末が IN2 であった場合，相手端末の位置がネットワーク内部であるので，送信元アドレスを ULA_{IN1}，宛先アドレスを ULA_{IN2} 設定し，カプセル化を行わずに通常の通信を行う．

以上により，提案方式では CA を用いることによりインターネット上の端末からネットワーク構成を隠蔽することができる．また，エンドエンド通信を実現し，アプリケーションの制限も生じない．

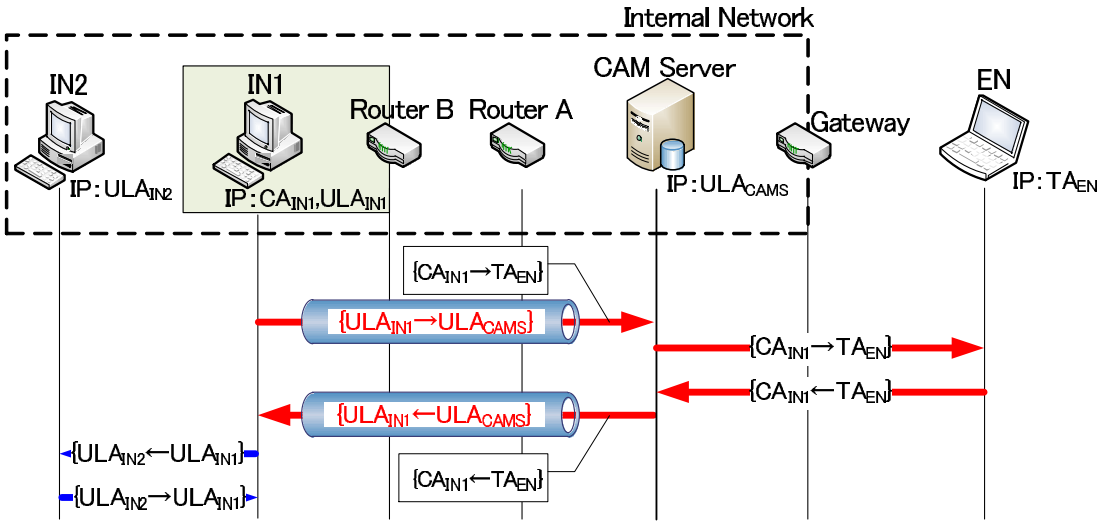

図 3.4　通信動作

3.5　CAM Server の負荷分散

提案方式では，ネットワーク規模が大きくなり，ネットワーク内の端末数が増加すると，CAM Server へのトラフィックが集中し，CAM Server の負荷が増す可能性がある．そこで，CAM Server を複数台設置し，処理を分散させる．CAM Server が複数設置している場合は，CAM Server 毎に CA 内で定義された CA 判定ビットを任意に設定することで，CA がどの CAM Server によって管理されているのかを判断する．これにより，CAM Server の管理負荷を低減することができる．

第4章　実装評価

4.1　カーネルモジュールの実装

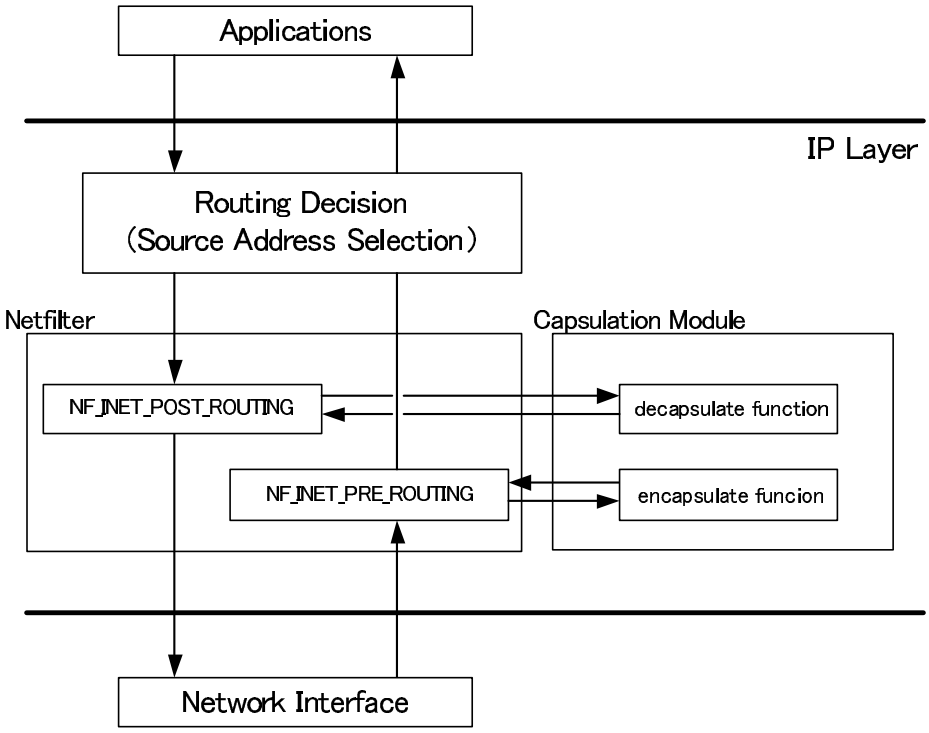

図 4.1　Linux における Capsulation Module の実装

Linux における提案方式の実装設計を図 4.1 に示す．送信元アドレスが CA である場合，ネットワーク内部でのルーティングを可能とするために，カプセル化を行う．パケットのカプセル化はカーネルモジュールにより実現する．処理中のパケットをフックするには，Linux カーネル内で実装されている Netfilter を用いる．また，パケットのカプセル化をカーネル内で実現することにより，パケットデータをユーザ空間へ渡し，カプセル化する手法よりも，カプセル化のオーバヘッドを抑える．送信時，送信パケットがアプリケーションから IP Layer へ渡されルーティング処理に入る．この時に，3.4 節で述べたソースアドレス選択の機能により送信元アドレスが決定され，宛先アドレスに応じた送信元アドレスが設定されている．その後，Netfilter の NF_INET_POST_ROUTING で送信パケットデータをフックし，カプセル化処理を行う Capsulation Module へ渡される．

Capsulation Module ではソースアドレス選択により決定された送信元アドレスをチェックし，CA であった場合，カプセル化処理を行った後，カプセル化パケットを通常のルーティング処理へ戻す．送信元アドレスが CA でない場合は，カプセル化処理は行わず，そのまま送信パケットを戻す．受信時は，受信パケットが Interface から IP Layer へ渡されたときに，Netfilter の NF_INET_PRE_ROUTING で受信パケットデータをフックし，カプセル化されている受信パケットであるかどうかを判断する．カプセル化されている受信パケットである場合，デカプセル化処理を行い Netfilter へ差し戻し，ルーティング処理を行う．CAM Server が内部端末と通信を行う場合は 2 通り考えられ，一つは，CA をルーティングするためのカプセル化通信．もう一つは，CAM Server と内部端末が通常の通信を行うときである．CAM Server はデカプセル化するかどうかの判断をするためにパケットのポート番号を見て判断する．カプセル化通信の場合，カプセル化通信用のポート番号を設定してカプセル化を行うことで，カプセル化されたパケットであると判断する．以上により，パケット毎に Capsulation Module で送信元アドレスをチェックしカプセル化，デカプセル化の処理をカーネルモジュール内で行う．

4.2 評価

提案方式のカプセル処理を行うモジュールを実装し，カプセル化処理にかかるオーバヘッドを測定した．測定環境を図 4.2 に示す．IN1 と CAM Server との間を LAN ケーブルで接続し，この間でカプセル化通信を行わせた．ping6 を送信したときの RTT を測定し，カプセル化処理のモジュールを追加したときの RTT の変化を測定した．表 4.1 に測定に使用した機器の諸元を示す．

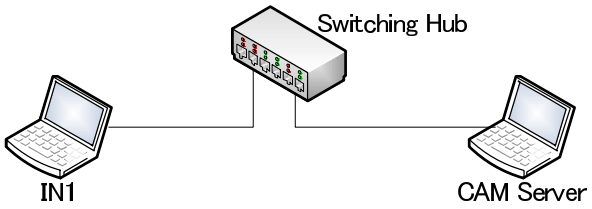

図 4.2　測定環境

表 4.1　諸元

	OS	Kernel version	CPU	Memory
IN1	Linux(Ubuntu10.04)	linux-2.6.32-21-generic	Intel 2.4Ghz	2GB
CAM Server	Linux(Ubuntu10.04)	linux-2.6.32-28-generic	Intel 2.4Ghz	2GB

結果を表 4.2 に示す．結果は ping6 を 100 回送信した RTT の平均値である．この結果

より，提案方式のモジュールを導入したときの RTT が通常時と変わらないことがわかる．これにより，カプセル化処理における劣化は見られないことを確認した．

表 4.2　測定結果

	RTT(ms)
通常時	0.570
提案方式	0.569

第5章　まとめ

本論文では，IPv6 へ移行した場合に，IPv4 環境で隠蔽されていたネットワーク構成が隠蔽されなくなる問題を取り上げた．そこで，IPv6 においても，ネットワーク構成を隠蔽する方式が示されている．NPTv6 では，インターネット本来のエンドエンド通信をスつことが出来ず，Mobile IPv6 を用いた方式においても，経路冗長や導入の難しさも課題となる．

これらの課題を考慮し，本提案では，通信相手に応じて，CA と ULA の 2 つのアドレスを使い分ける．また，CA を管理するために，CAM Server を設置し，CAM Server では CA の生成，ネットワーク内で CA をルーティングさせるためのトンネル構築の役割を担う．提案方式のカプセル化を行うモジュールを実装し，評価を行った結果，カプセル化処理におけるオーバヘッドが非常に小さいことを確認した．

今後は，残りの実装の完了と，CAM Server が管理する端末が増加した場合の負荷について検討を行う．

謝辞

本研究に関して，多大なる御指導，御助言を賜りました，渡邊晃教授に心より熱くお礼申し上げます．論文作成にあたり，快く査読を引き受けて下さった，副査の柳田康幸教授，旭健作助教，鈴木秀和助教には貴重なコメントや至らないところを指導していただき深く感謝いたします．また，本研究を行うにあたり，本研究室の皆様にも多くの方々から多大な助言と協力を承り，深く感謝しております．最後に，研究を進めていく中，いつも暖かく支えて頂いた両親に心より感謝いたします．

参考文献

[1] Task Force on IPv4 Address Exhustion: IPv4 アドレス枯渇対策タスクフォース. http://www.kokatsu.jp/blog/ipv4/.

[2] Postel, J. and Reynolds, J.: FILE TRANSFER PROTOCOL (FTP), RFC 959, IETF (1985).

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC 3261, IETF (2002).

[4] PCI Security Standards Council, LLC: PCI Security Standards Council. https://www.pcisecuritystandards.org/.

[5] Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6), RFC 2460, IETF (1998).

[6] Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, IETF (2007).

[7] Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prefix Translation, RFC 6296, IETF (2011).

[8] de Velde, G. V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6, RFC 4864, IETF (2007).

[9] Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, RFC 4913, IETF (2005).

[10] Draves, R.: Default Address Selection for Internet Protocol version 6 (IPv6), RFC 3484, IETF (2003).

[11] Matsumoto, A., Fujisaki, T., Hiromi, R. and Kanayama, K.: Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules, RFC 5220, IETF (2008).

研究業績

学術論文

なし

国際会議（査読あり）

1. Toru Kuboshiki, Hidekazu Suzuki, and Akira Watanabe, “Proposal on the Concealment of the Network Topology in IPv6,” IEEE 11th International Symposium on Communications and Information Technologies (ISCIT2011), pp.53-57, Oct.2011.

国内会議（査読あり）

1. 久保敷透, 寺澤圭史, 鈴木秀和, 渡邊晃, “IPv6 におけるネットワーク構成隠蔽に関する検討,” マルチメディア, 分散, 協調とモバイル（DICOMO2010）シンポジウム論文集, Vol.2010, No.1, pp.1153-1158, Jul.2010.
2. 久保敷透, 寺澤圭史, 鈴木秀和, 渡邊晃, “IPv6 におけるネットワーク構成隠蔽の提案,” マルチメディア, 分散, 協調とモバイル（DICOMO2011）シンポジウム論文集, Vol.2011, No.1, pp.323-328, Jul.2011.

研究会・大会等

1. 久保敷透, 寺澤圭史, 鈴木秀和, 渡邊晃, “企業ネットワークにおける IPv6 アドレスの隠蔽方式” 平成 21 年度電気関係学会東海支部連合大会論文集, Sep.2009.
2. 久保敷透, 寺澤圭史, 鈴木秀和, 渡邊晃, “IPv6 におけるネットワークの隠蔽方式に関する検討,” 情報処理学会第 72 回全国大会講演論文集, Mar.2010.

受賞歴

1. 2010 年 7 月　マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム　ヤングリサーチャー賞

付 録A　CA 生成方法

CA の生成方法を図 A.1 に示す．CA のランダムな値は SHA-1 に生成された値を用いる．SHA-1 に用いる値として，IPv6 と同じ 128 ビットの値を用いる．この値は，ルータから受け取るグローバルプレフィックスの 48 ビットと，履歴バッファ 80 ビットを用いて生成する．履歴バッファが存在しない場合は，ランダムな値を用いる．次に，SHA-1 ハッシュ関数によりハッシュ化し，180 ビットのハッシュ値が出力される．このハッシュ値の下位 80 ビットは，次に生成する CA のための履歴バッファとして記憶しておく．そして，グローバルプレフィックスの 48 ビットと，CA 判定ビットの 4 ビット，出力されたハッシュ値の上位 76 ビットを組み合わせ，CA が生成される．

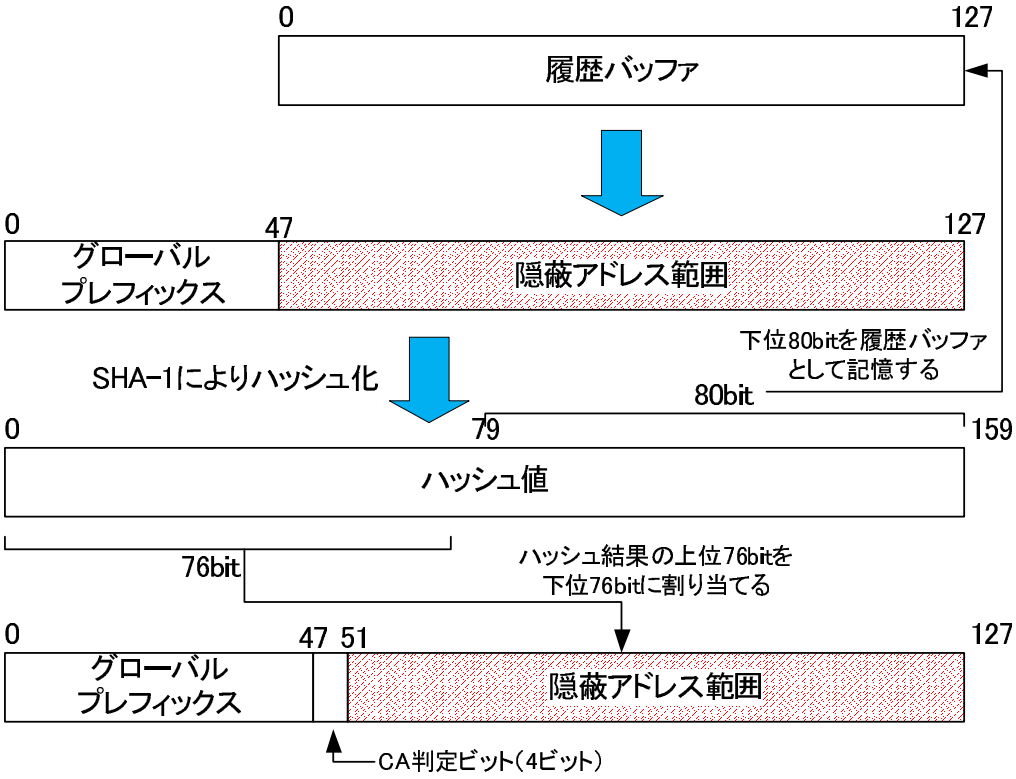

図 A.1　CA 生成方法

付 録B　CAの更新，移動通知の動作

図 B.1 に CA の更新，解放の動作を示す．CA の更新は，CA の期限が近づいたときに行い，CAM Server へ新たな CA を要求する CA Update を送信する．CA Update を受け取った CAM Server は，新たな CA を生成し，今まで登録されていた．AC と ULA の関係を更新する．その後，CA Response によって新しく生成した CA を通知する．端末がネットワークを移動した場合，ULA のアドレスが変更されるため，CAM Server へ通知が必要である．このときも，CA の更新と同様の手順により，新たに CA を要求して CAM Server の CA と ULA の関係を更新する．

また，端末が電源をオフ，またはログオフした際には，取得している CA を CA Release により開放し，登録されている CA と ULA の関係を削除する．

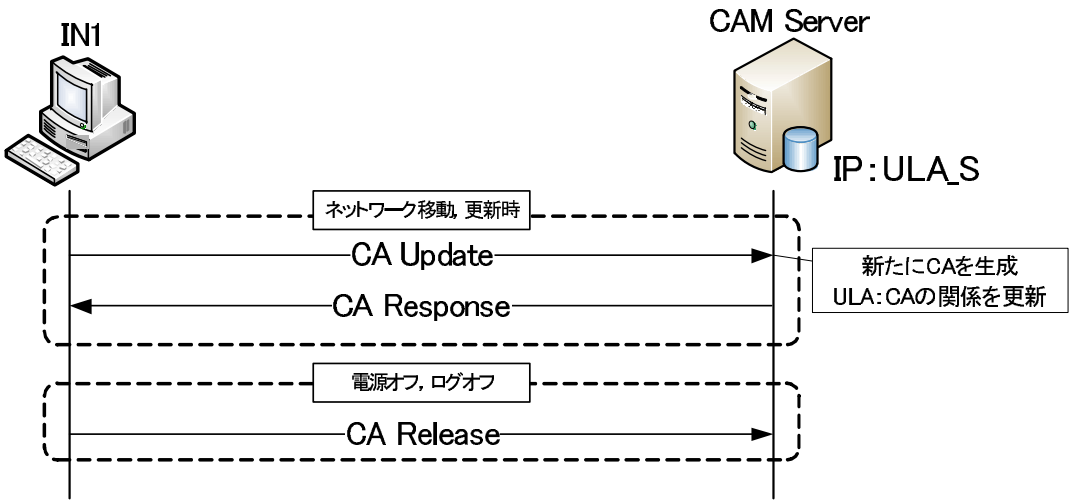

図 B.1　CA の更新，解放の動作

付 録C　DNSのゾーン設定

端末は通信を開始しようとしたときに，端末のアドレスを解決するために名前解決を行う．そのとき，内部端末のアドレスを同一ネットワークの端末が解決しようとすると，CA と ULA を通知することになる．この場合，内部端末同士の通信であっても送信元アドレスが CA になり，カプセル化による通信を行うようになる可能性がある．そのため，DNS のゾーンを設定することで，内部端末が同一ネットワーク内の端末と通信をしたいときの DNS 応答を ULA のみにする．

付 録D　ソースアドレス選択方法

提案方式は相手端末の位置によりアドレスを使い分ける．そのため，アドレスごとに送信元アドレスを使いわける必要がある．これにはソースアドレス選択という機能を用いる．IPv6 には，複数のアドレスを割り当てることができるようになっている．そのため，宛先アドレスに応じて，適切なアドレスを選択する必要があり，様々なパターンを考慮しなければならない [11]．この選択の規則についてはポリシーテーブルによって決められている．図 D.1 に Linux で初期に設定されているポリシーテーブルを示す．それぞれのプレフィックスが登録されており，宛先アドレスに近いプレフィックスの送信元アドレスが選択される．本提案の内部端末同士での通信に用いる ULA のプレフィックスは，すでにポリシーテーブルに追加されており，`fc00::/7` がこれに該当する．宛先が ULA の場合はプレフィックスの値が近いアドレス，すなわち自身の ULA が送信元アドレスに設定される．このポリシーテーブルは変更が可能であり，今後，様々なアドレスに対応して送信元アドレスを決定させたい場合は，適宜変更が必要である．

```
prefix ::1/128 label 0
prefix ::/96 label 3
prefix ::ffff:0.0.0.0/96 label 4
prefix 2001::/32 label 6
prefix 2001:10::/28 label 7
prefix 2002::/16 label 2
prefix fc00::/7 label 5
prefix ::/0 label 1
```

図 D.1　ルーティングポリシー