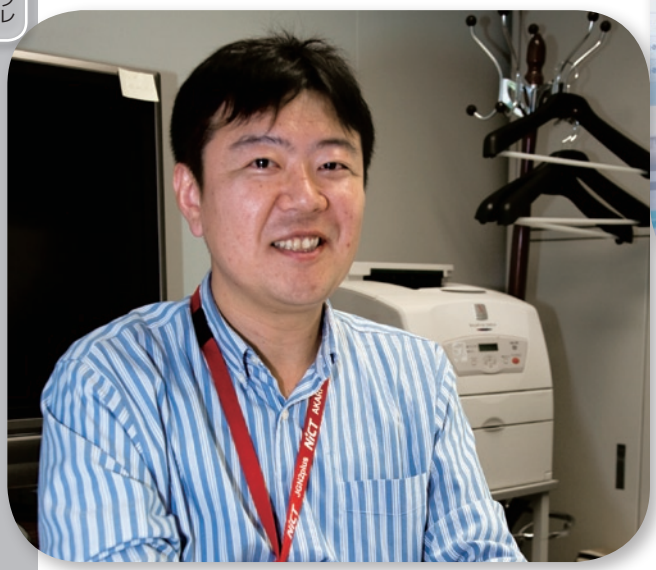
ID・ロケータ分離による新世代ネットワークアーキテクチャ



「我々が提案するHIMALISというID・ロケータ分離方式を紹介します。これは、異種間ネットワーク通信、移動通信、マルチホーム、セキュリティ対応等に適した方式です。」

原井 洋明 (はらい ひろあき)
光ネットワーク研究所
ネットワークアーキテクチャ研究室 室長

入所当時の光ネットワーク分野を含めて、現在はより幅広く新世代ネットワークの研究開発に従事。2007年IEEE ComSoc Asia-Pacific Young Researcher Awardにおいて Outstanding Young Researcher表彰。2009年文部科学大臣表彰若手科学者賞受賞。趣味はプロ野球のナイトゲームを見ることだが実践できていない。たまに、野球観戦・ゴルフ・スキー。

Ved P. Kafle (ベド カフレ)
光ネットワーク研究所
ネットワークアーキテクチャ研究室 主任研究員

現在、新世代ネットワークの設計、実装、評価、アルゴリズム最適化、プロトコル及びアーキテクチャの研究開発に従事しています。現在の関心事は、新しいネーミング及びアドレス方式、ID・ロケータ分離アーキテクチャ、名前またはIDの解決メカニズム、異機種ネットワーク層プロトコルの統合、ユビキタスセンシングとコンピューティングのためのインターネットへのリソースに制約のあるセンサーネットワークの統合、分散移動管理機能、通信ネットワークのプライバシ、セキュリティ及び信頼性にあります。2009年に新世代ネットワークアーキテクチャの標準化への貢献に対し、日本ITU協会賞を受賞しました。同じ年に、国際会議ITU-T Kaleidoscopeにおいて論文賞を受賞しました。休みには2人の娘と遊んだり、日本のネパール人のコミュニティでボランティア活動をしたり、バドミントンやジョギングを楽しんでいます。

はじめに −なぜ新世代ネットワークなのか−

今やインターネットは、私たちの日常生活になくてはならないものになっています。近い将来には、インターネットには、家電製品、乗り物、健康・環境監視センサーなどの多種多様なデバイスが相互接続される日が来るでしょう。しかし、40 年前に設計されたインターネットは、当時遠方の知人のコンピューターとの通信をするためのもので、携帯･微小デバイスの無線接続、セキュリティとサービス品質の提供、低消費電力での大容量のデータの効率的な転送などは考慮されていませんでした。アプリケーションがこのような要求をするようになって、様々な機能がオリジナルのインターネットアーキテクチャに、全体の最適化を考えることなく、ランダムに追加されてきました。その結果、現在のインターネットには負荷がかかり過ぎ、本来あった拡張性という特徴が次第に失われてきました。それゆえ、前述した要求を、さらに将来に生じる要求も満たすようにするために、私たちは白紙から新世代ネットワークを設計してきました。

新世代ネットワークは、海外では、“Future Internet”とか“Future Network”などと呼ばれていますが、現在のインターネットでの制約条件は継承しません。新世代ネットワークは、膨大な数の多種多様な移動デバイスを想定し、様々なネットワークプロトコルをサポートします。この記事では、このような目標を達成するために必要な ID・ロケータ分離という概念について、現在のインターネットのアーキテクチャと比較しながら説明します。

ID・ロケータ分離の概念

図 1(a) は、現在のインターネットのプロトコルの階層構造を示します。IP アドレスは、アプリケーション層とトランスポート層で、端末やセッションやサービスの識別子(ID) として利用され、同じ IP アドレスが、ネットワーク層ではネットワーク内での端末の接続位置(ロケータ) として利用されます。1 つの IP アドレスを ID とロケータの両方に使用することは、異種のプロトコル、移動通信、マルチホーム接続、セキュリティ、経路制御の拡張などに適していません。端末が、ネットワークを移動した場合、端末の IP アドレス(ID とロケータの両方) が変更され、元の IP を識別子として用いた現在進行中のセッションが切れます。また、マルチホーム接続は、接続しているネットワークが混雑・切断した場合に、別のインターフェースに切り替えるためのものですが、それぞれのインターフェースは独自の IP アドレスを持っている

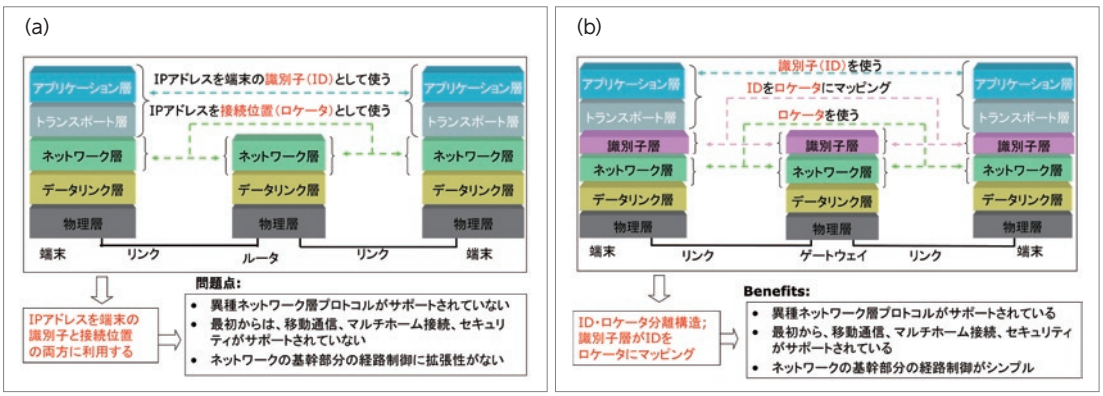


図1　プロトコル階層図　(a) 現在のインターネットの場合　(b) ID・ロケータを分離した新世代ネットワークの場合

ため、接続切り替え時にセッション ID が変更になり、通信セッションの滑らかな継続は困難です。同様に、IP アドレスに紐付いたセキュリティ情報は、端末の IP アドレスの変更で無効になります。さらに、コアネットワークは、それぞれのエッジネットワークまたはアクセスネットワークごとの経路表を作成しますが、エッジネットワークのサイズが小さく、数が非常に多くなった場合には、基幹の経路表のサイズは非常に大きくなり、エッジネットワークの IP アドレスの設定が頻繁に変更になると、基幹の経路表を更新する処理負荷が高くなり、最終的には、基幹の経路制御の機能に支障が出るでしょう。

従って、新世代ネットワークのプロトコル階層は、図 1(b) に示すように ID とロケータを切り離す(ID・ロケータ分離)必要があります。トランスポート層とネットワーク層の間に挿入された識別子層は、ID をロケータにダイナミックにマッピングし、端末の移動やマルチホーミングによってネットワーク層がロケータを変更した場合にも、アプリケーション層やトランスポート層は、端末や通信セッションの識別用に同じ ID を使い続けることができます。この特徴は、ネットワーク層で別の種類のプロトコルを使うことを可能とします。データのパケットのヘッダには、送信元と宛先の両方の ID とロケータが含まれています。ゲートウェイは、パケットがエッジネットワークとコアネットワークを横断する際に、ID をヘッダの中のネットワークプロトコルやロケータの値を変換するための参照値として使います。これにより、新世代ネットワークでは、エッジネットワークやコアネットワークで異なるタイプのネットワーク層プロトコルの利用が可能となります。

HIMALIS アーキテクチャ

ID・ロケータ分離の概念に基づき、NICT は HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation: ロケータと ID を分離することによる異質性の許容と移動への適応) アーキテクチャを提案してきました。図 2 は HIMALIS アーキテクチャの主要な構成要素であるエッジネットワーク、コアネットワーク、論理制御ネットワークを示しています。コアネットワークはエッジネットワーク同士を接続するために高速なルータとリンクで構成されています。

● ネットワークアクセス機能

端末(図 2 の端末 1) がエッジネットワークに接続するとき、DHCP (Dynamic Host Configuration Protocol) 等の初期設定プロトコルの実行や AA、LNS、GW の ID やロケータ等のエッジルータのパラメータを入手します。端末は次に、認証と登録のために AA にコンタクトします。認証が済むと、端末には新しいロケータが割り当てられます。端末の端末名、端末 ID、ロケータ、公開鍵は LNS のホストテーブルに保存され、端末 ID とロケータは GW の ID テーブルに保存されます。端末にはアクセスキーも割り当てられ、信頼性の証明や AA、LNS、GW との暗号化メッセージのやりとりに使われます。端末は新しいロケータを HNR に、ロケータ更新メッセージを送ることによって登録します。こうしてこの端末は他の端末と通信する準備ができました。

● セッション初期化機能

端末 1 が端末 2 と通信したいとき、端末 1 は端末 2 の端末名しか知らないため、端末 1 は端末 2 の ID、ロケータ、公開鍵を LNS に問い合わせます。LNS は DNR、HNR から情報を入手して端末 2 の ID、ロケータ、公開鍵を受け取り端末 1 に送ります。こうして端末 1 は端末 2 に対して制御パケットを交換し始め、セキュリティコンテキスト(セッションキーなど)

を確立し、両方の GW の ID テーブルに ID・ロケータのマッピングを保存します。GW は ID テーブルから ID・ロケータのマッピングを使うことによってパケットのヘッダの中のネットワークプロトコルやロケータの変換を行います。

● 移動通信機能

(a) 移動端末(たとえば端末 1) は 移動して新エッジネットワークにアクセスして新しいロケータを得て、(b) 旧 GW にある端末 1 のロケータ情報を新しいロケータに更新し、移行中にも旧 GW が新しい GW にパケットが転送されるようにし、(c) 端末 2 とその GW の情報を更新し、新しい位置にいる端末 1 にパケットを転送できるようにする、(d) 端末 1 の HNR レコードを更新し、(e) 旧エッジネットワークから切断する、という手順で信号をやりとりします。HIMALIS アーキテクチャでは、ネットワークアクセスやセッション初期化のプロセスで確立されたセキュリティコンテキストを移動管理機能の安全確保にも使用できます。

実装の様子

HIMALIS アーキテクチャに基づく ID・ロケータ分離の技術は NICT における新世代ネットワークの研究の重要な要素です。私たちは HIMALIS アーキテクチャを、ローカルなテストベッドネットワーク上で実装してきました。DNR と HNR の機能は PlanetLab(約 1,000 ノードから成る地球規模のオーバーレイテストベッドネットワーク) のノードにも実装し、実験しています。最近では、HIMALIS を Linux のカーネルに実装し、それを JGN-X に接続して実験・検証できるようになっています。このように HIMALIS アーキテクチャを継続的に改良し、広範な検証を通じて、HIMALIS が普及するよう研究開発をしていきます。

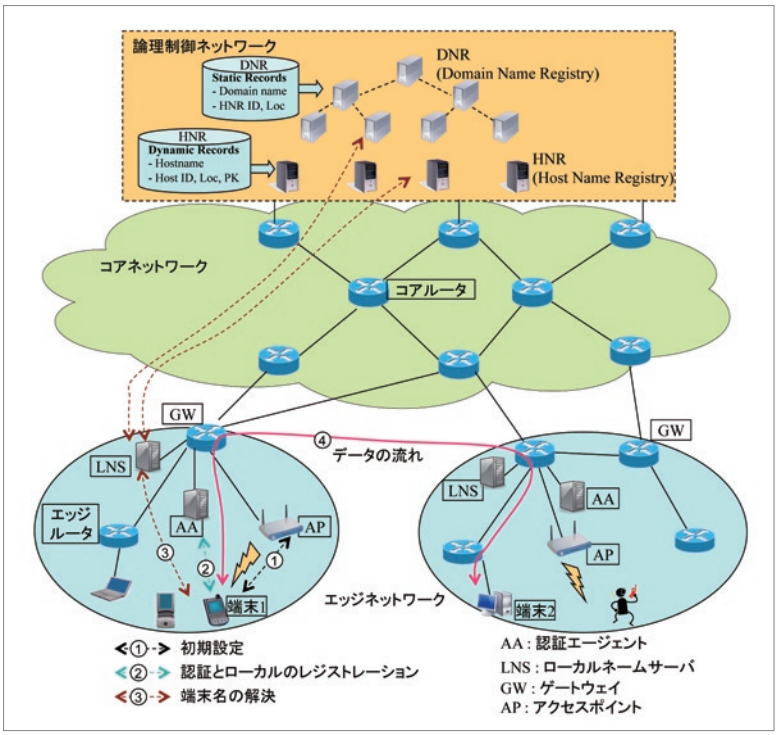


図2　HIMALISアーキテクチャの構成要素