

# IPv6 の広大な空間活用により多様なサービス利用と安全な通信を実現する コンテンツセントリックネットワーキングの研究開発 (121803042)

Research and Development of the Contents Centric Networking that Enables  
Various Services and Secure Communications by Using Huge IPv6 Address Space

## 研究代表者

北村 浩 日本電気株式会社  
Hiroshi KITAMURA NEC Corporation

## 研究分担者

阿多 信吾<sup>†</sup> 村田 正幸<sup>††</sup>  
Shingo ATA<sup>†</sup> Masayuki MURATA<sup>††</sup>  
<sup>†</sup>大阪市立大学 <sup>††</sup>大阪大学  
<sup>†</sup>Osaka City University <sup>††</sup>Osaka University

研究期間 平成 24 年度～平成 26 年度

## 概要

(1) コンテンツセントリックネットワークに適したアドレッシングアーキテクチャ、(2) コンテンツ名表現の解決メカニズム、(3) 柔軟な粒度を持つセッション連動型透かし入りコンテンツアドレスによるセキュリティ機構を研究開発する。広大なアドレス空間を持つ IPv6 のネットワークを利用することで、新たなセキュリティ機構を導入できるのに加え、クライアント、サーバ、およびネットワークの現有的資産の修正の最小化あるはそのまま活用することができ、既存の使い勝手はほぼそのままに、ユーザ側で特別な意識をすることなく容易に利用することができるコンテンツセントリックネットワークを実現できる。

## 1. まえがき

新しい基盤ネットワークとしてのコンテンツセントリックネットワークならびに関連する基盤技術の研究開発を行う。IPv6 の広大なアドレス空間を活用することにより多様なサービス利用と安全な通信を実現できるネットワークアーキテクチャを構築する。ユーザ側の変更を最小化し、既存ネットワークと共存混在して段階的に導入できる方法を用いることで、既存資産を最大限に活用でき、ユーザにもサービス提供者にも有益で且つ安全な通信が行えるコンテンツセントリックネットワークを容易に実現する。

## 2. 研究開発内容及び成果

本研究開発において取り組んだ課題を以下に述べる。

### 課題1:コンテンツセントリックネットワークに適したアドレッシングアーキテクチャの検討

本課題では、IPv6 アドレスを利用したコンテンツセントリックネットワークに適したコンテンツリソースの名前表現方法、およびアドレスへのエンコード方法について検討する。

### 課題2:コンテンツ名表現の解決メカニズムの実現

本課題では、コンテンツセントリックネットワークの IPv6 ネットワーク上への展開について重要となる、指定されたコンテンツ名をどのように IPv6 アドレスに解決し、コンテンツアドレスを用いたルーティング機能を実現するかについて検討する。

### 課題3:柔軟な粒度を持つセッション連動型透かし入りコンテンツアドレスによるセキュリティの向上

IP アドレスが従来ノードごとに固定であるという概念を根本から変え、異なる IPv6 アドレスを通信セッションごとに独立して与える。これによってセッションごとに IPv6 アドレスが異なるようになる。IP アドレスをセッション単位で割り当てることで、通信セッションごとに異なる IP アドレスを使用した通信が可能となる。

図 1 に本研究課題で実現するコンテンツセントリックネットワークにおけるコンテンツへのアクセス手順を示す。

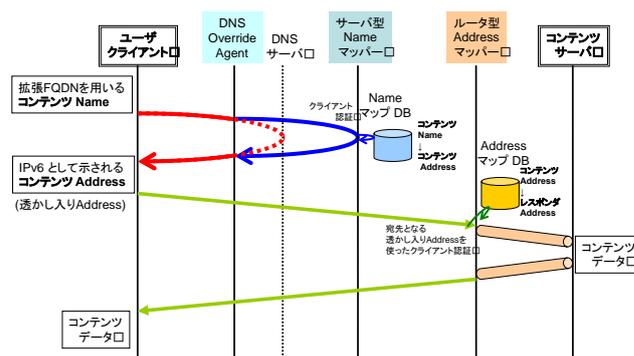


図 1 本研究開発により実現するコンテンツアクセスの手順

ユーザは FQDN を拡張するコンテンツ Name によりコンテンツを指定する。その後 DNS 名前解決ライブラリを通じて、アドレスの解決が行われる。本研究開発では DNS override 技術により拡張 FQDN によるアドレス解決リクエストは Name マップデータベースに転送され、そこでコンテンツ Address にマッピングされる。その後クライアントはコンテンツ Address を用いてパケットを送出する。コンテンツ Address が宛先に指定されたパケットは途中の Address マップデータベースによって処理され、コンテンツデータを持つノードのアドレスに向けて例えばトンネリングによって転送される。まず、このうち Name マップデータベース (NMDB) の初期実装を行う。NMDB は、ユーザが指定したコンテンツ Name を対応するコンテンツ Address にマッピングする処理を行うデータベースである。既存の IP ネットワークでは、ホスト名 (FQDN; Fully Qualified Domain Name) から IP アドレスへ解決する機構として DNS (Domain Name Service) があるが、本研究開発では DNS の機構を拡張することによって Name マップデータベースの構築を実現する。これまで本課題外で DNS query をオーバーライドし、サーバ側の情報をクライアントに伝える機能を開発しており、本研究開発では、その成果を応用し開発された機能を変更して導入することとし、システムとして完成させる。

一方、Address マップデータベースについては、コンテンツセントリックネットワークの規模および制御可能な管理ドメイン、AS との接続状況によって必要性が大きく異なる。

本研究開発課題では、コンテンツアクセスおよびコンテンツサーバに対する攻撃防御などのセキュリティを向上させるため、コンテンツの通信セッションごとに異なる IP アドレス用い、ワンタイムによる使用で使い捨てる新しい通信アーキテクチャを導入する。従来の IP 通信ではコンテンツを持つサーバの IP アドレスは永続的に利用されていた。本研究開発では、コンテンツごとに独立したアドレスを割り当て、使用後直ちに抹消し使用不可とすることで、使い捨て型のアドレスを実現する。

コンテンツサーバのクライアントに対するアクセス制限を実現するため Address マップデータベースに対するクライアントからのアクセス認証技術を導入する。認証はパケットの送信元アドレスのチェックにより行うものとする。そしてさらにセキュリティを向上させる方法として、ワンタイムアドレスを導入する。これによりたとえばコンテンツのダウンロードごとに異なるアドレスが必要となるため、アドレスの再利用によるアタックや不正ダウンロードが防止できることが期待される。さらに、クライアントのロケーションプライバシー保護のため、コンテンツセントリックネットワークにおける Ephemeral Address を実現する。

これを実現するため、これまでの研究開発で設計および実装した Unified Multiplex 通信アーキテクチャを本研究開発で導入したタブレット端末でも動作させた。これにより、現在 ARM ベースのタブレット端末を用いた本研究開発によるコンテンツセントリックネットワークの実現ができています。

さらに、DNSO において Ephemeral Address による認証を導入し、コンテンツごとにアクセス可能なアドレスの正当性を検証する機構を実装する。さらに、DNSO とコンテンツサーバの連携により、コンテンツサーバの持つコンテンツごとに独立した IPv6 (Specific Service Address) を割り当て、DNSO を通じてそのアドレスをクライアントに通知することで、特定のクライアントが特定のコンテンツに対するアクセスのみに有効となるコンテンツ Address の提供を実現する機構を設計実装する。これらは、コンテンツのアクセスのみ、かつ一度だけ有効なワンタイムアドレスとなることから、アドレスの変更によるコンテンツ保護が容易に実現できる。

本研究では、セッション連動型コンテンツアドレス利用に新しい概念を取り入れることでセキュリティや使い勝手を向上させる。これは、Address の利用目的を決める (意味付けする) 処理であり、この処理を Coloring と呼んでいる。Coloring とは Address をその利用目的毎にグループ分けし、色をつける処理である。従来の Address は特別な意味を持たず、いわば無色の状態であり、EA や SSA には着色するという考え方である。色に相当するのはどのグループに属するかを示す情報でありこれを Tag と呼んで本機能を設計実装している。

### 3. 今後の研究開発成果の展開及び波及効果創出への取り組み

本研究開発課題で取り組んだコンテンツセントリックネットワーク CCN あるいはほぼ同様の意味で用いられる ICN (Information Centric Networking) の研究開発の活動は、インターネットの標準化を行う IRTF (Internet Research Task Force) で RG (Research Group) が発足したり、学会でも研究会が発足したりするなどしてこの 3 年間で注目を集める大きな活動に育ってきている。また、本研究開発課題のもう一つの特徴である IPv6 に関しても、世界中の多くの ISP で default で使えるようになったり、Google や Yahoo など有力な Service Provider においても普通に IPv6 でサービスを提要求するようになったりするなど、その利用状況は大きく発展してきている。更にはインターネットのセキュリティは E. Snowden の告発などもあり、

世界的な大きな関心事になってきている。

本研究開発課題はそれらの社会的な変化を予見して先取りして対応したものであり、今後の産業や社会に対して大きく貢献できる技術になるのではないかと考えられる。特に多くの CCN/ICN のプロジェクトが既存のインターネットからの移行や共存を考えないクリーンスレート的なアプローチで研究開発されているのに対し、本研究開発では IPv6 の広大な空間を活用することにより、既存のインターネットからの移行が容易で共存可能となることに大きな特長のある、地に足の付いた実用的な CCN の利用環境を提供する研究開発を行ってきた。

### 4. むすび

CCN/ICN を多くの人が使えるようになるような広く社会に普及するには時間がかかると思われるが、本件の研究開発がその普及を進めるのに大きく貢献できると期待される。また、サービスの提供方法とそのセキュリティを確保する方法に関しても、既存の方式と共存する形での新たな方式の研究開発とその機能の検証を行っており、この面においてもセキュアなインターネット通信を容易に実現するといった、社会を変革していくことに活用されることにも期待される。

#### 【誌上発表リスト】

- [1] S. Ata, H. Kitamura and M. Murata, "Towards Early Deployable Content-Centric Networking Enhanced by using IPv6", ManFI 2013 (Ghent, Belgium) (May 27-31, 2013)
- [2] S. Ata, H. Kitamura and M. Murata, "Information-Centric Communication Architecture for Vehicular Networking", ICCVE2013 (Las Vegas, USA) (December 02-06, 2013)
- [3] R. Maeda, S. Ata and H. Kitamura, "Name Completion for Improving Flexibility of Names in Information-Centric Networking", International Conference on Green and Human Information Technology (ICGHIT 2015) (Da Nang, Vietnam) (February 4-6, 2015)

#### 【国際標準提案リスト】

- [1] IETF · 85th Atlanta IETF meeting, <draft-kitamura-ipv6-auto-name-03.txt>, "Corresponding Auto Names for IPv6 Addresses" Internet Draft, October 16, 2012
- [2] IETF · 87th Berlin IETF meeting, <draft-kitamura-ipv6-zoneid-free-00.txt> "Free from Using Zone Identifier for IPv6 Link-Local Address" Internet Draft, July 10, 2013
- [3] IETF · 92nd Dallas IETF meeting, <draft-kitamura-tcp-sharp-close-00.txt> "Sharp Close: Elimination of TIME-WAIT state of TCP connections" Internet Draft, March 9, 2015

#### 【参加国際標準会議リスト】

- [1] IETF · 85th Atlanta IETF meeting, Atlanta GA USA, November. 4, 2012
- [2] IETF · 87th Berlin IETF meeting, Berlin Germany, July 28, 2013
- [3] IETF · 92nd Dallas IETF meeting, Dallas TX USA, March 22, 2015

#### 【受賞リスト】

- [1] Ryo Maeda, Shingo Ata and Hiroshi Kitamura, Best Paper Award of ICGHIT 2015, "Name Completion for Improving Flexibility of Names in Information-Centric Networking", February 4-6 2015

#### 【本研究開発課題を掲載したホームページ】

<http://www.anarg.jp/achievements/web2014/>