# 次世代ネットワークにおける高速アドレス隠蔽機能

加藤　圭　　芝　修吾

次世代ネットワークにおいて，ユビキタスサービスの浸透に伴い，端末間のシームレスな通信が必須となる。すなわち，場所に関わらず同じ端末で通信が可能となるが，それに伴い，通信相手または第三者に対し，通信者の「場所」に関連する情報が公開される可能性がある。最も大きな問題は，ローミング時に送信元IPアドレスが容易に解析できるために，通信者の場所が通信相手または第三者に特定されてしまうことである。これを解決するための1手段として，送信元IPアドレスの隠蔽がある。次世代ネットワークのインフラストラクチャーでは，このような要求が頻繁に起こることが想定されるため，アドレス隠蔽を高性能・低遅延に実施することが望まれる。本稿では，これらの要求を満たすアドレス隠蔽機能を具備したネットワーク装置の試作を紹介すると共に今後のネットワークにおける本機能の必要性を示す。

## はじめに

端末の移動に伴い，頻繁にアクセスポイントが変更できるインフラを構築する必要があり，そのようなインフラのための技術向上，あるいは標準化が現在進行中である。アクセスポイントが動的に変わることで，端末のIPアドレスの変更が起こりうる。IPアドレスは，アクセスポイントから付与されるため，このIPアドレスがアクセスポイントの物理的な場所と相関関係がある場合，通信者の端末の場所が，通信相手または第三者に概ね特定されてしまう可能性がある。これはプライバシーの侵害にもなり得るため，何らかの対処が必要となる。

現状，移動網の標準化団体である3GPP（Third Generation Partnership Project）では，IMS（IP Multimedia Subsystem）網の網間の接続機能として，

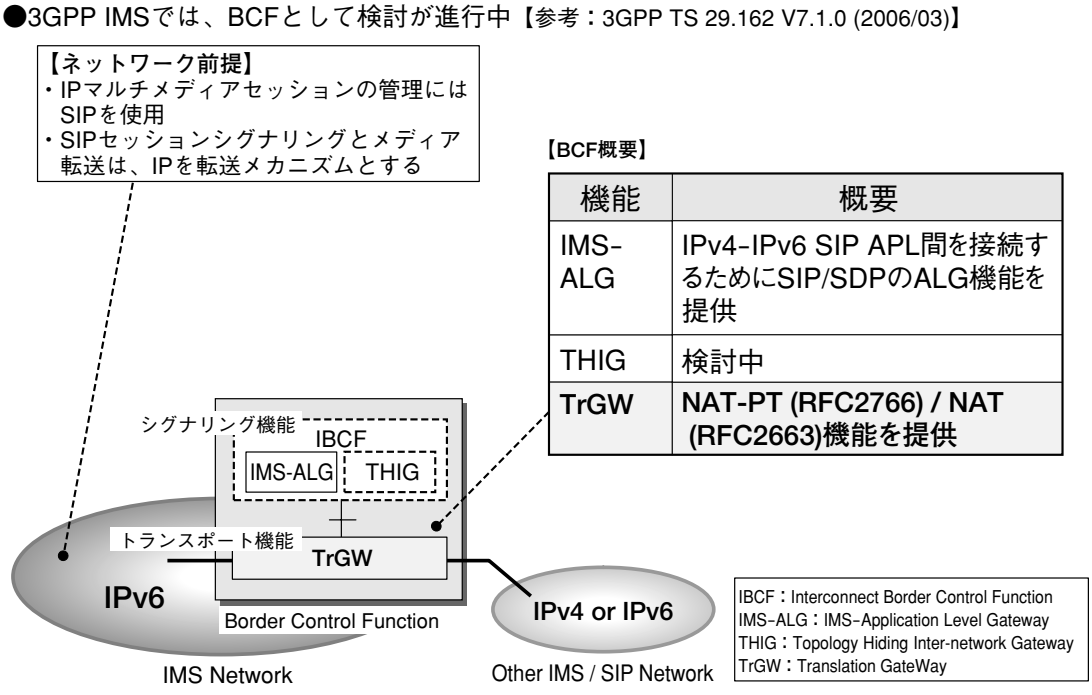


図１　3GPPにおける網間接続機能の標準化

BCF（Border Control Function）の標準化が進行中である（**図1**）[1]。BCFは，IBCF（Interconnect Border Control Function）およびTrGW（Translation Gateway）からなり，前者がシグナリング，後者がトランスポートに関わる網間接続機能をつかさどる。このうち，TrGWには，アドレス形態の異なる網（IPv6-IPv4網）に対してIPトランスレーション機能，同じ網（IPv6-IPv6網，あるいはIPv4-IPv4網）に対してアドレス変換機能が求められている。これら2つの機能が実装されているTrGWを用いることで，TrGW通過後のパケットから通過前のIPアドレスを推測することが困難となる。すなわち，IPトランスレーション機能とアドレス変換機能をアドレス隠蔽機能と見なすこともできる。

以降の章では，アドレス隠蔽機能を有するTrGWを実現する上で，その課題と解決策について説明する。

## 課　題

TrGWにアドレス隠蔽機能を実装する上で，もっとも大きな課題は，いかに高性能，低遅延な実装方式が実現できるかということである。IMSのような次世代網は次世代のネットワークキャリア網であり，数千万の加入者が同時に利用する可能性がある。したがって，TrGWに対しても，数十～数百万の同時セッションに対してアドレス隠蔽機能を実現することが求められる。さらに，低遅延の性能を確保することが重要である。これは，今後の網では，音声・映像トラヒックが中心となり，トラヒックのショートフレーム化が進行することが予想されるためである。インターネット（The Internet）のトラヒックは，ミニマムフレーム（64byte）とマキシマムフレーム（1500byte）に偏って分布しているが，これと比較しショートフレームの多い網では，遅延要因となる単位時間のパケット処理量が増大するため，遅延が顕在化する可能性がある。したがって，高品質なサービス提供を行うためには，TrGW内での遅延を極力減らすことが重要となる。

現在，これらの課題を解決するため，TrGWの試作を実施中である。これにより，高性能，低遅延なアドレス変換機能の実装を目指す。次の章では，この試作の実装方式を説明する。

## 実　装　方　式

アドレス隠蔽機能を実現するにあたり，我々はネットワークプロセッサ（NPU：Network Processing Unit）による実装を選択した。**図2**に示すように，TrGWの機能を汎用PCのアーキテクチャで実装した場合，ネットワークインタフェース機能を持つNIC（Network Interface

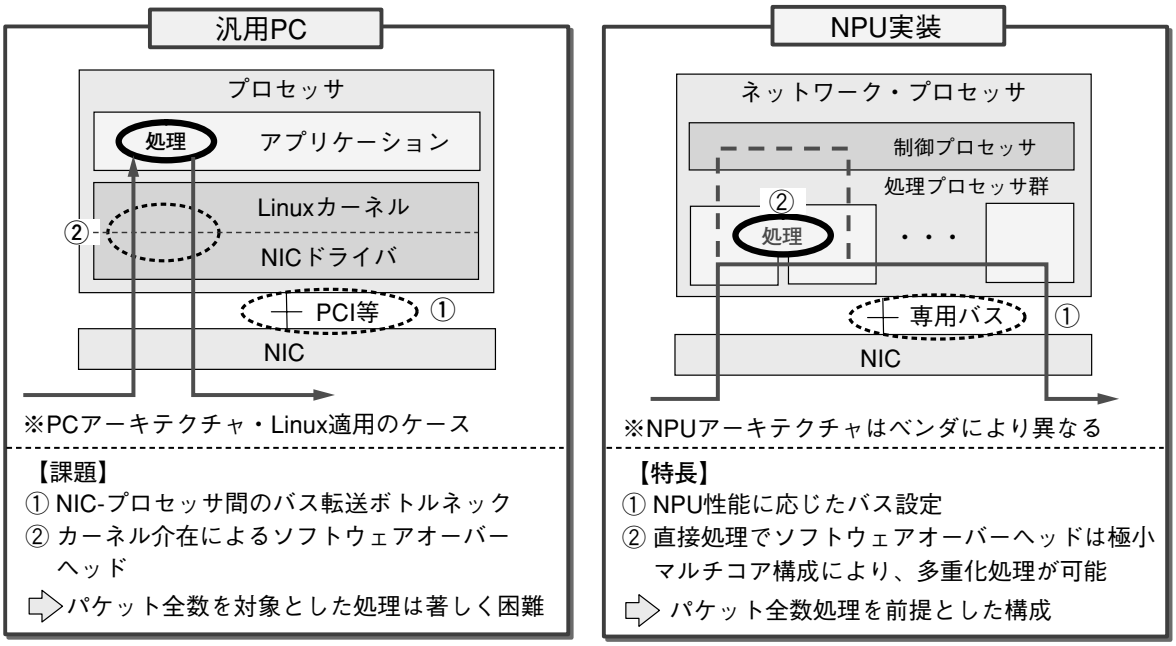


図2　汎用PCとネットワークプロセッサによる方式の違い

Card）とプロセッサの間にPCI等を利用しているため，どうしても転送ボトルネックが生じてしまう。さらに，OSカーネルを介した処理となるために，ソフトウェアのオーバヘッドも無視できない。これらの特徴は，先述の高性能，低遅延化を達成する上で大きな障害であり，汎用PCでの実現は著しく困難である。一方，NPUでの実装の場合，パケット処理のためにチューニングされたアーキテクチャを持ち，NPUの性能に応じたバスが設定されているため，転送ボトルネックは生じない。さらに，OSカーネルを介さず直接パケット処理が可能であること，マルチコア構成による多重化処理が可能といったメリットを持つ。

**図3**に本試作の実装方式を示す。実装に用いた標準としては，IPトランスレータ機能（IPv4-IPv6）では，SIIT: Stateless IP／ICMP Translator（RFC2765）[2] を，アドレス変換機能（IPv4-IPv4,IPv6-IPv6）ではRFC3022[3] を適用した。RFC3022はIPv6-IPv6変換は規定していないが，IPv4-IPv4とのアナロジーで，独自方式による実装を行った。

基本的にはアドレス変換，および，それに伴う他のヘッダ項目の変換機能が実装のキーとなる。**図3**に示すように，処理前段に配備したFPGAによりパケット識別（IPv4かIPv6か）を行い，処理後段に配備したNPUによりIP/ICMP変換を実施する方式となっている。前段のパケット識別をNPUではなく，FPGAで実施しているのは，①IPv6アドレス検索では，NPUでもソフトウェア処理における負荷が大きく，性能確保が困難であること，②パケット識別機能自体汎用性が高く，他のアプリケーションでも利用できるため，ハードウェアの機能として分離するメリットがある，という理由による。

一方，後段のIP／ICMP変換では，一例として，MTUが異なる場合，パケットのフラグメントや，再フラグメントを行う必要がある。これは相当の遅延を発生させる可能性があるが，NPUでは，複数処理プロセッサを具備しているため，このような処理も並行処理することで，高速に実現することが可能である。

## まとめと今後の方向性

次世代ネットワークでは，ユビキタスサービスの浸透に伴い，アドレス隠蔽機能が必須になるという前提で，ネットワークプロセッサ（NPU）を用いた，ネットワーク上の高速アドレス隠蔽機能を実装した。NPUは，パケット転送処理向けにチューニングされており，高性能，低遅延な実装が期待できる。今回，FPGAとの分担や，NPUの処理プロセッサ群への機能振り分けを最適化するような実装を行い，課題である高性能・低遅延化を目指した

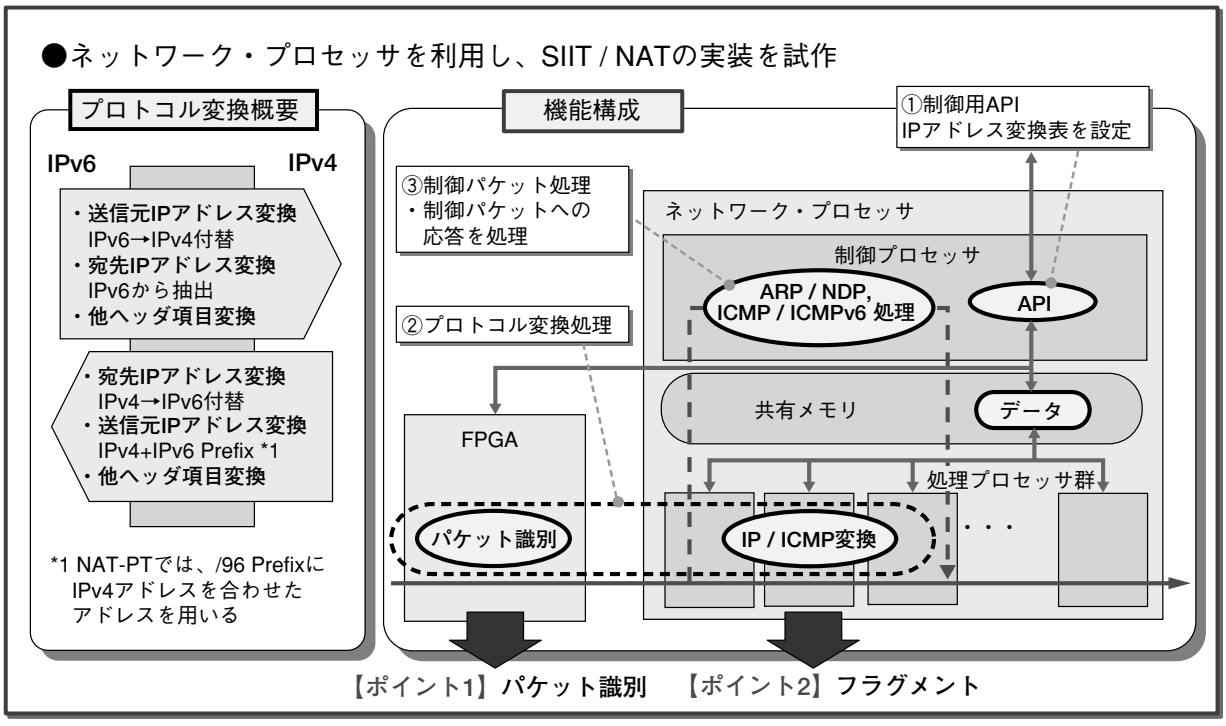


図 3　実装方式概要

試作を実施した。今後は試作した装置をさまざまなネットワーク環境で評価し，改良する予定である。評価を通じて更なる性能の向上を目指す予定である。 ◆◆

## ■参考文献

1）3GPP TS 29.162 V7.1.0，2006年
2）SIIT: Stateless IP / ICMP Translator（RFC2765），2000年
3）Traditional IP Network Address Translator （Traditional NAT）（RFC3022），2001年

## ●筆者紹介

加藤圭：Kei Kato. ネットワークシステムカンパニー ネットワークシステム本部 サービスプラットフォームマーケティング部
芝修吾：Shugo Shiba. ネットワークシステムカンパニー ネットワークシステム本部 通信プラットフォーム開発部