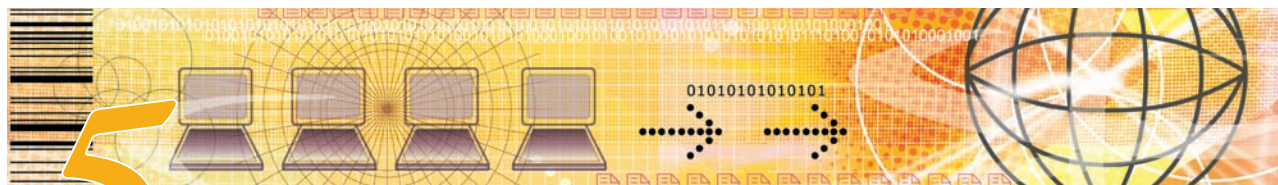


特集 新世代ネットワーク



# 新世代ネットワークを支える ルータ・スイッチと技術

矢崎武己 アラクサラネットワークス（株） 技術開発部  
 矢野大機 アラクサラネットワークス（株） 製品開発本部  
 能見元英 アラクサラネットワークス（株） マーケティング本部

新世代ネットワークには、通信基盤を担うネットワークとして、高速性、通信継続性に加えて通信品質の保証、安心・安全なサービスの提供、環境への負荷低減が求められる。本ネットワークを構成するルータ・スイッチには、高速化、高精度なQoS（Quality of Service）機能や異常フローの探知・排除機能の実装、省電力化等が必要であり、現在、これらを実現する技術の開発が進んでいる。本稿では、この技術開発における課題と、課題を解決する最新技術について紹介する。

## 新世代ネットワークとは

インターネットに代表されるIPネットワークはその低廉性から急速に普及し、我が国の60%もの国民が利用するようになった。Web、E-mailが一般的に使用され、企業サイト間の通信サービスやVoIP（Voice over IP）サービスが通信事業者より提供されるなど、IPネットワークは我々の生活や企業活動に欠かすことができない通信基盤となっている。

このIPネットワークの普及につれてトラフィックは急増し、インターネットエクステンジのトラフィックは年率40%程度で増加している<sup>1)</sup>。この増加は、ネットワークの帯域不足に起因する通信品質の劣化やネットワークを構成するルータ・スイッチの消費電力増加を招いており、たとえば、国内のルータの総電力消費は2007年に原子力発電所一基分に達するとの示唆もある。今後のネットワークには、省電力化を実現しつつ高速・高品質なサービスを提供することが求められる。

一方で、悪意あるユーザのDDoS（Distributed Denial of Service）攻撃による企業サーバの停止やネットワーク輻輳による通品品質の劣化が顕在化してきた。最近では、WinnyなどのPeer to Peerソフトウェアの利用による個人・顧客情報漏洩が社会問題となっており、ネットワークにおける安全性が求められている。これらの脅威を排除して、安心・安全なネットワークを実現すること

が、今後一層求められてくる。

以上の背景から新世代ネットワークには、新世代の通信基盤を担うネットワークとして、以下の要件を満たすことが期待される。

- (1) 急増するトラフィックを収容可能な高速なネットワーク
- (2) 通信品質を確保するネットワーク
- (3) 悪意ユーザの影響を排除し、すべてのユーザが安全に安心して利用可能なネットワーク
- (4) 電力消費が少なく環境負荷の少ないネットワーク

以下では、新世代ネットワークを構成するルータ・スイッチが実現すべき課題と、その解決技術の例を説明する。

## 新世代ネットワークを実現するルータ・スイッチと技術課題

### 高速化の実現

高速なネットワークを実現するためには、ネットワークを構成するルータ・スイッチの高速化が必要となる。**図-1**に示す通りハイエンドルータ・スイッチの転送速度（bit/s）<sup>☆1</sup>はおよそ4～5年で10倍に向上しており、

☆1 転送速度（bit/s）とは、ルータ・スイッチにおいて、ある回線から他の回線に1秒間に転送可能な最大データ量（bit）である。

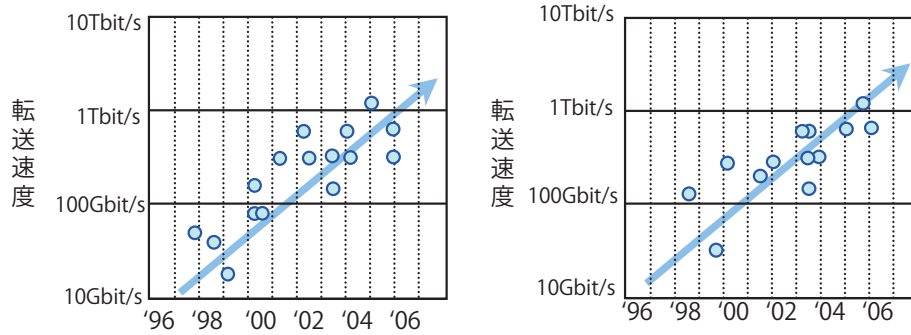


図-1 ハイエンドルータ(左)とハイエンドスイッチ(右)の転送速度の推移

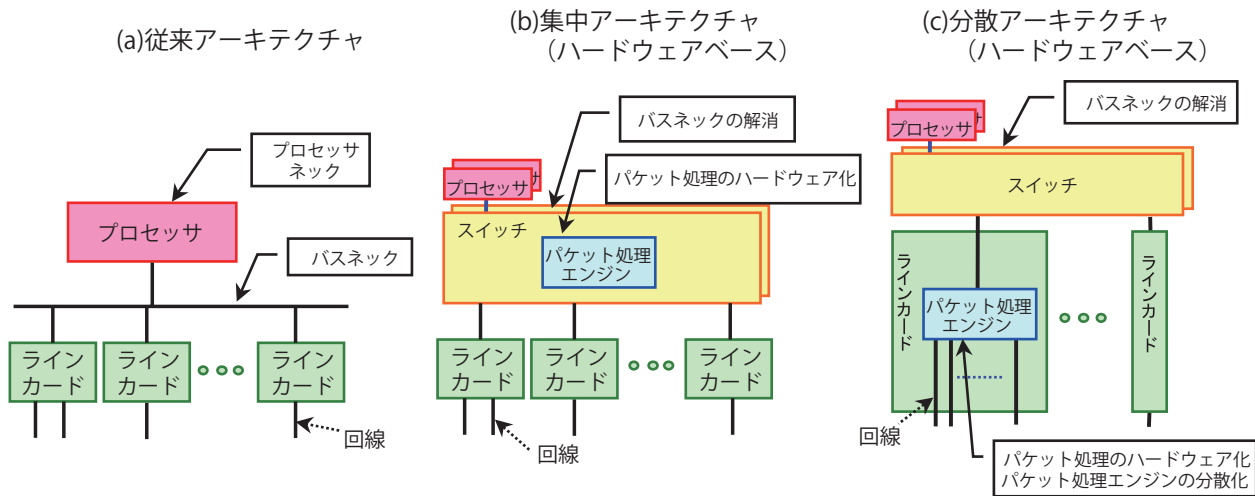


図-2 従来のルータアーキテクチャとハードウェアベースのアーキテクチャ

現在では 1Tbit/s を超えるルータ・スイッチも登場している。今後も継続的に増加するトラフィックに対応するため、さらなる高速化が必要となる。

現在の高速ルータ・スイッチは、図-2(b), (c) に示すハードウェアベースの集中アーキテクチャや分散アーキテクチャを採用するのが一般的である。1980年代の商用ルータは、図-2(a)の示すように、パケットを送受信するラインカードとパケット処理を行うプロセッサが1つのバスにより接続されており、バスやプロセッサに性能のボトルネックがあった。ハードウェアベースの集中アーキテクチャは、バスネック解消のため、複数のラインカードをスイッチで接続する。さらに、プロセッサの高負荷なパケット処理をスイッチのパケット処理エンジンが高速実行することで、高速化を実現している。一方、分散アーキテクチャは、パケット処理エンジンをラインカードに分散配置する。集中アーキテクチャと比べてコスト面では不利であるが、さらなる高速化に適したアーキテクチャである。

新世代ネットワークのルータ・スイッチにおいては、ハードウェアベースのルータ・スイッチのパケット処理エンジン、スイッチの高速化が主要課題となる。

## QoS 機能

通信品質を確保するルータ・スイッチの機能としてシェーパやポリサーなどの QoS (Quality of Service) 機能がある。シェーパは、パケットをいったん蓄積するバッファを複数備え、それぞれのバッファからの読み出し帯域やバッファ間の読み出し順序を調整して、パケットを回線に送信する機能である。一方、ポリサーは、回線から入力するパケットの帯域をフローごと<sup>☆2</sup>にチェックし、設定した帯域以上のパケットを廃棄したり、優先度を下げたりする機能である。ネットワーク管理者は、適切な QoS 機能をネットワークに配置し、必要な通信品質を実現することとなる。

新世代ネットワークでは、各ユーザの帯域の確保、企業サイト間の通信や VoIP などの重要通信の品質確保、さらにはユーザごとの帯域を確保しつつこの帯域の範囲内で重要通信を優先するなど、ネットワークが提供するサービスに応じた通信品質の確保が求められる。QoS 機能は、これらの通信品質を確保するため、(a) ユーザご

☆2 フローとは、パケットヘッダ内のフィールド(IPアドレスなど)を組み合わせて作成した条件に一致する一連のパケットをいう。

との帯域制御, (b)重要度に応じた帯域制御および(c)ユーザごと, 重要度ごとの帯域制御など, 多様な帯域制御を実現することが必要となる。

### 異常フローの検知・排除

安心・安全なネットワークを実現するためには, ネットワークは悪意ユーザの異常フローを検知し, 排除することが必要である<sup>☆3</sup>。

企業ネットワークにおいては, 異常フローを排除してサーバやネットワークを防御するため, ファイアウォールやIDS (Intrusion Detection System) などの対異常フロー防御装置の利用が広がっている。これらの装置は全コネクションの状態を管理して異常フローの高精度な検知を実現する。

一方, 広域ネットワークにおいても, 異常フローがネットワークを占有するため, リアルタイムに異常フローを検知・排除することが求められている。前述のIDSは最大1Gbit/s程度の性能であり, 10ギガビットイーサネットが一般的に使用される広域ネットワークでは, 性能が不足することも考えられる。そのため, 新世代のルータ・スイッチにおいては, 高速回線対応の異常フローの検出・排除方式の実現が課題となる。検知・排除機能はルータ・スイッチ以外の装置で実装されてもよいが, 装置増加によりネットワーク管理コストや装置コストが増加するため, ルータ・スイッチへの実装が期待される。

### 消費電力の低減

ルータ・スイッチの高速化に伴い消費電力も増加し, 現在では10,000Wを超えるハイエンドのルータも登場している。この増加は半導体チップの進化と関係している。半導体チップのトランジスタ密度や動作周波数は, 半導体プロセスが一世代進化するごとにそれぞれ2倍, 1.5~2倍に向上してきた<sup>2)</sup>。これらの向上は高速化には効果的だが, 電力の増加を招いてしまう。低電圧化や動作不要な回路へのクロックを停止するゲーテッド・クロックなどの消費電力削減施策も実施されてきたが, 高速化に伴う消費電力増加に追いつかず, 結果としてルータ・スイッチの消費電力増加を招いている。

さらに, 最近では消費電力の大きなCAM (Content Addressable Memory) が後述のテーブル検索処理で一般的となってきた。CAMは高速化には効果的だが, 通常のメモリに比べると消費電力が大きく, 装置全体の消費電力の増加を招く場合がある。

☆3 異常フローとしては, DDoS攻撃などが代表的である。本攻撃では, 攻撃者が攻撃用プログラムを多数の端末(踏み台)に侵入させ, これらの端末がサーバやネットワークに対して一斉に攻撃用パケットを送信する。

新世代ネットワークのルータ・スイッチにおいては, これらのデバイスの使用により高速化を実現しつつ, 高速化につれて増加する消費電力を最小限に抑えることが必須となる。

## 新世代ネットワークのルータ・スイッチを支える技術

以下では, 前述した課題を解決する技術の例について説明する。

### 高速化技術

ルータ・スイッチの高速化は, 構成する半導体チップの高速化に大きく依存する。一般的に周波数が2倍のLSI, メモリを用いれば2倍の高速化を達成できる。しかし, CAM等の新たなデバイスや新規アルゴリズムによるパケット処理の効率化により, さらなる性能向上を期待できる。以下では, パケット処理エンジンにおいてネックとなるルーティングテーブル検索の効率化技術について説明する。

本検索処理は, **図-3(a)**に示すルーティングテーブルに基づいて, パケットを送信する宛先ネットワーク等の宛先情報を判定する処理である。ルーティングテーブルには宛先IPアドレスの条件と, このアドレスに対応する宛先情報が格納される。ヘッダ内の宛先IPアドレスと一致する条件を検索し, この条件に対応する宛先情報をパケットの宛先情報と判定する。

高速ルータ・スイッチのルーティングテーブル検索方式として, 二分木ツリー検索や検索用のデバイスであるCAMを用いた方式等が一般的である。以下では, 特に高速化に適したCAMによる検索方式について説明する。CAMは, 条件を記載するエントリを複数備え, 検索キーが入力されると検索キーと一致するエントリのアドレスのうち, 最も小さいアドレスを高速に出力するデバイスである。エントリと検索キーを同時に比較する回路を備え, 一致と判定したエントリのうち最も小さなアドレスをプライオリティ・エンコーダと呼ばれる回路を用いて判定し, 出力する。

本検索方式の概念図を**図-3(b)**に示す。本図はIPアドレスの条件をエントリに記載するCAMと, 各エントリに対応した宛先情報を格納するメモリで構成される。パケットが入力するとヘッダ内の宛先IPアドレスが抽出され検索キーとしてCAMに入力される。CAMは一致するエントリを高速に検索して, 一致したエントリのアドレスのうち最も小さなアドレス値を出力し, メモリはこのアドレスに対応した宛先情報を出力することとなる。CAMは, この検索を高速に実行できるため, 高速なル

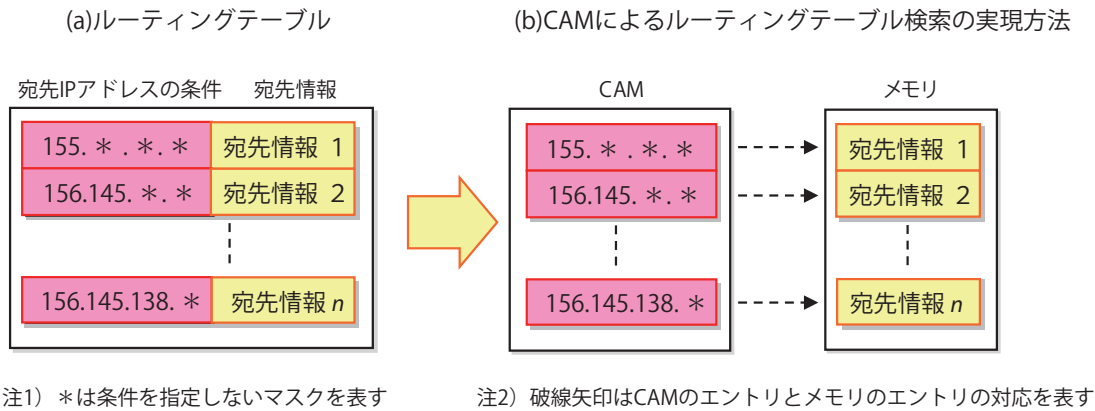


図-3 ルーティングテーブルとCAMによるルーティングテーブル検索の実現方法

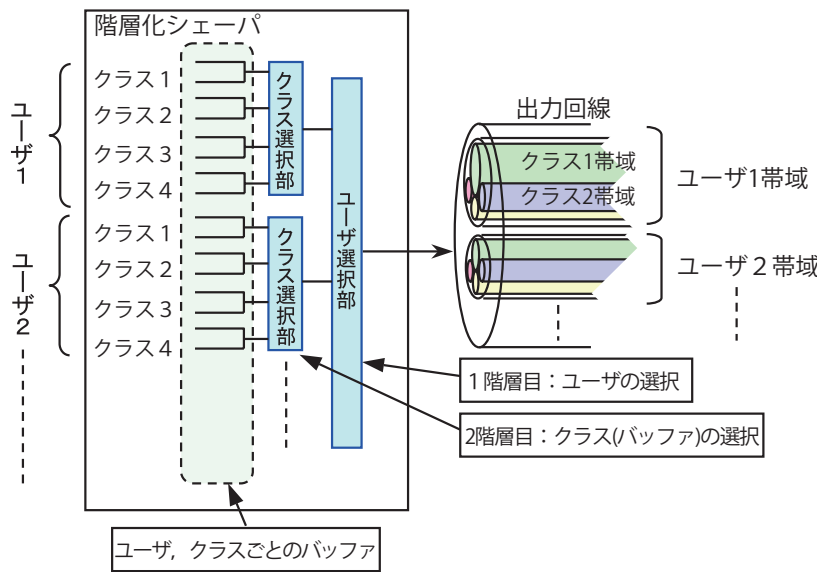


図-4 階層化シェーパのブロック図

ルーティングテーブル検索が実現される。たとえば、最新のCAMは1秒間に100M回以上の高速検索を行うことが可能で、CAM1つにより10ギガビットイーサネット6回線以上に対応する検索を実現可能である<sup>☆4</sup>。

CAMは、テーブル検索処理の高速化にきわめて有効なデバイスであるが、消費電力は10W以上と大きいといった課題もある<sup>3)</sup>。そのため、今後、CAMを用いない高速検索方式の開発やCAMを使用した低電力高速検索方式の開発が必要となる。

## QoS 技術

多様な帯域制御を実現するQoS機能の例として、課題

☆4 パケット長を最短の64バイト、イーサネットにおけるパケットあたりのオーバーヘッド（プリアンプルとインターフレーム間ギャップ）を20バイトと仮定。この際、10Gbit/sの回線からは、最大15Mパケット/s（ $= 10G / ((64 + 20) \times 8)$ ）でパケットが入力するため、10ギガビットイーサネット6回線（ $\approx 100M/15M$ ）以上に対応する検索が可能。

に記した(a)～(c)を実現する階層化シェーパ<sup>4)</sup>を説明する。

図-4に階層化シェーパのブロック図を示す。ユーザごと、ユーザが備えるクラス(重要度)ごとのバッファを備え、1つのユーザ選択部とユーザごとのクラス選択部がユーザ数×クラス数のバッファからパケットを送信するバッファを選択し、パケットを出力回線に送信する。

ユーザ選択部は各ユーザの設定帯域と送信するパケット長より決まる送信間隔を計算し、各時刻においてパケット送信するユーザを選択する。この設定帯域としては、最大帯域と最低帯域がある。最大帯域の場合、各ユーザの帯域がこの帯域を超えないようユーザを選択し、最低帯域の場合には、各ユーザの帯域が常に最低帯域を超えるように制御しつつ、回線に余剰帯域がある場合、この帯域を各ユーザに振り分けるようにユーザ選択を行う。

選択されたユーザのクラス選択部は、あらかじめ設定された帯域割り当てのポリシーに従いパケットを送信するクラス(バッファ)を選択する。このポリシーとしては、完全



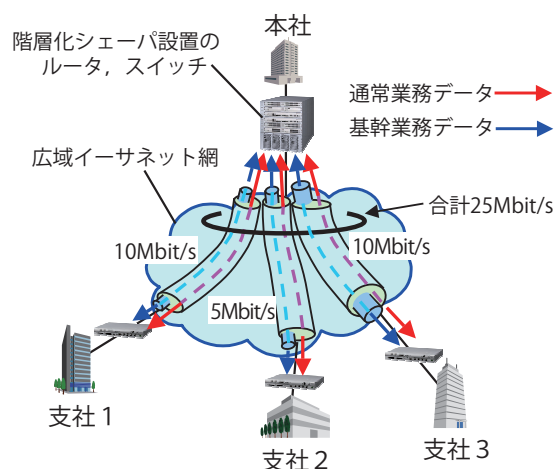


図-5 広域イーサネット網への階層化シェーパの適用例

優先制御や WFQ (Weighted Fair Queuing) などがある。完全優先制御では優先度が高いクラスを優先的に選択し、WFQ では各クラスの帯域が“重み”に比例するように選択する。

以上のユーザ選択部とクラス選択部の動作により、ユーザごとの帯域とユーザが備える各クラスの帯域を同時に制御できる。さらに、使用するクラス数やユーザ数を“1”とすれば、クラスごとあるいはユーザごとの制御が可能となる。

階層化シェーパの適用例を図-5 に示すネットワークを用いて説明する。本図は広域イーサネット網により本社と支社 1～3 が接続されたネットワークである。本社と各支社間で基幹業務データと通常業務データの通信が行われ、本社と広域イーサネット網間の通信に対して 25Mbit/s の帯域が保証されている。

本社から各支社への通信を考えると、本社からある特定支社への過剰なパケット送信が、本社と広域イーサネット網間の保証帯域である 25Mbit/s を占有し、本社と他の支社間の通信が不通となることも考えられる。さらに、通常業務データが保証帯域を占有し、基幹業務データの通信品質が劣化することも考えられる。これらの課題を解決するため、本社のエッジに位置するルータ・スイッチに階層化シェーパが配置される。階層化シェーパは、支社 1～3 への最大帯域をそれぞれ 10Mbit/s、5Mbit/s、10Mbit/s に制限し、完全優先制御を用いて各支社への基幹業務データを優先転送する。これらの制御を行うことで、本社から支社 1～3 への帯域を確保して本社から支社への通信継続を維持すると同時に、基幹業務データの優先転送によりこのデータの廃棄を防止することが可能となる。

### 高速異常フロー検知技術

広域ネットワークに対応する高速な異常フロー検知技術の一例としてサンプリング型の検知方式<sup>5)</sup>を説明する。

本方式では、サンプリングされたパケットに存在する特定フローのフロー数の大小関係から異常フローの発生を検知する。サンプリングにより処理するパケットが減少するため 10 ギガビットイーサネット等の高速回線に対応可能である。以下、図-6 を用いて本方式による SYN flood の検知方法を説明する。SYN flood は、ネットワークの帯域を消費し、広域ネットワークにて問題となる DDoS 攻撃である。

図-6 のネットワークは、1 台の正常端末、多数の攻撃端末(踏み台)および攻撃対象である Web サーバより構成されている。正常端末が送信する SYN パケット(赤矢印)を契機に TCP コネクションが確立され、Web サーバはデータパケット(青矢印)を返送する。一方、攻撃端末は詐称した送信元 IP アドレスの SYN パケット(赤矢印)を送信して Web サーバを攻撃する。この際、TCP コネクションは確立されず Web サーバがデータパケットを送信することはない。

本方式で SYN flood を検知する際には、以下の 2 つのフロー数をカウントする。

- フロー数 1：宛先 IP アドレスが Web サーバのアドレスであり、送信元 IP アドレスが異なる SYN パケットのフロー数(赤矢印の数)
- フロー数 2：送信元 IP アドレスが Web サーバであるデータパケットのフロー数(青矢印の数)

SYN flood においては、Web サーバがデータ送信する宛先数に対して、SYN パケットの送信元が極端に多くなるため、パケットがサンプリングされていてもカウントしたフロー数 1 と 2 の大小比較を行えば SYN flood の検知を行うことができる。サンプリングを行っているため攻撃の発生を完全に検知することは難しいが、従来の検知方式では難しかった高速回線における検知技術として期待される。

### 省電力化技術

高速化と省電力化を両立する技術の一例として、FDB (Filtering Data Base)検索における省電力化方式を説明する。

FDB 検索は、FDB に設定された複数の MAC アドレスの条件と、パケットの宛先 MAC アドレスや送信元 MAC アドレスを一致比較するスイッチ処理である。この検索の後、スイッチは宛先 MAC アドレスと一致した条件に対応する出力回線にパケット送信することとなる。

本検索処理の高速化には、前述した CAM の適用が有効である。図-7(a) に示す通り、CAM に MAC アドレスの条件を格納し、パケットヘッダ内の宛先 MAC アドレスや送信元 MAC アドレスを検索キーとして CAM に入力すればよい。本方式では CAM による高速検索が実現されるが、

前述の通り消費電力が大きくなるという課題がある。

このような背景から消費電力増加を抑止して、最小限の消費電力でCAMによるFDB検索を実現する方式が提案されている<sup>3)</sup>。この方式は、CAMが備える複数の物理バンクのうち、必要な物理バンクに限定して電力供給可能であることに着目した方式である。本方式のFDBを図-7(b)に示す。MACアドレスの条件がこのアドレスのハッシュ値から決まるCAMの物理バンクに設定され、検索時には、パケット内のMACアドレスのハッシュ値から決まる物理バンクに限定して検索用の電力を供給し、検索を実施する。単一の物理バンクに電力が供給され、他の物理バンクに待機電力のみが供給されるため、消費電力が削減される。

CAMの各物理バンクにおける待機電力と検索用電力の比率が、SRAM(Static Random Access Memory)における待機電力とアクセス時の電力比率である0.02程度と仮定すると、従来方式に対する本方式の最大負荷時の電力は、バンク数 $n$ を用いて、 $1/n + 0.02 \times (n - 1)/n$ と表すことができる。ここで、 $n$ を8とすると、本方式の消費電力は約14%となり、大幅な電力削減が実現される。

## まとめ

新世代ネットワークには、高速性、通信継続性に加えて通信品質の保証、安心・安全なサービスの提供、環境への負荷低減が求められる。このネットワークを構成するルータ・スイッチには、高速化、高精度なQoS機能や異常フローの探知・排除機能の実装、省電力化等が必要であり、現在、これらに対する技術開発が進んでいる。

今後は、地上波デジタル放送の再送信に代表される新サービスやアプリケーションの登場によりユーザやネットワークの利用形態がより多様化、変化し、新たな課題が生じると予想される。たとえば、地上波デジタル放送の再配信に起因するマルチキャストパケットのコピー性能向上は新規課題の候補である。今後、既存課題に対する技術開発を推し進めるとともに、新規課題にも柔軟に

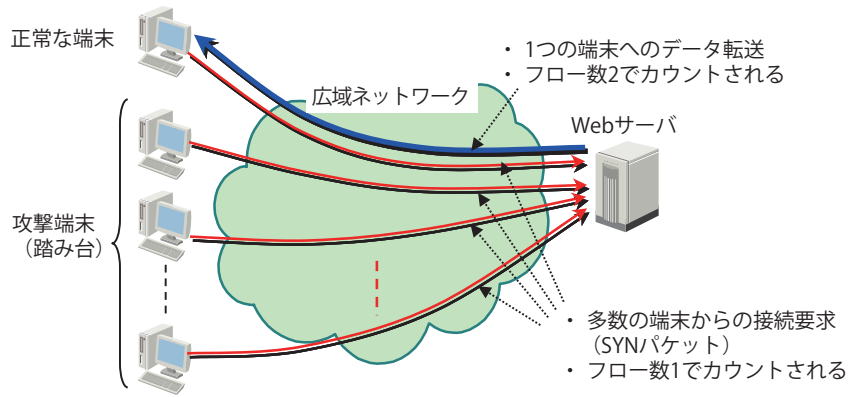


図-6 SYN flood 発生時のネットワーク

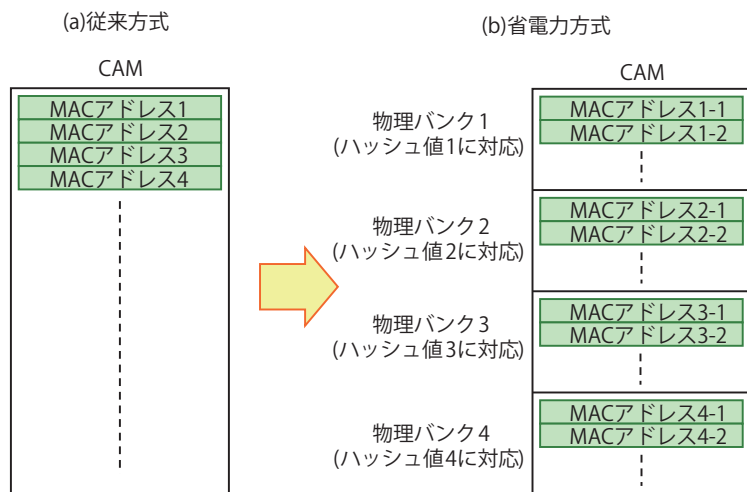


図-7 省電力FDB検索方式の概念図

対応していく必要がある。

### 参考文献

- 1) <http://nspixp.wide.ad.jp/3/>
- 2) リーク電流と闘う, 日経エレクトロニクス, No.882, pp.99-127, 日経BP社(Apr. 26 2004).
- 3) 奥 他: ネットワークノードにおける転送用データベース検索の省電力化方式. 2005年電子情報通信学会総合大会, B-6-153.
- 4) 矢崎他: IPv6対応階層化シェーパの評価実験, 信学技報, Vol.103, No.660, CQ2003-114, pp.1-6(2004).
- 5) 磯部他: 広域ネットワーク網向け異常通信の探知機能の検討, 信学技報, Vol.105, No.178, IN2005-47, pp.109-114(2005).  
(平成18年9月11日受付)

●矢崎武己(正会員) | yazaki@alaxala.com  
アラクスネットワークス(株)技術開発部所属, 1995年(株)日立製作所入社, ルータ・スイッチのアーキテクチャの研究開発に従事, 電子情報通信学会会員。

●矢野大機 | yanohiro@alaxala.com  
アラクスネットワークス(株)製品開発本部所属, 1999年(株)日立製作所入社, ルータ・スイッチのハードウェアに関する研究開発に従事。

●能見元英 | motohide.noumi@alaxala.com  
アラクスネットワークス(株)マーケティング本部所属, 1996年(株)日立製作所入社, ルータ・スイッチのソフトウェアに関する研究開発に従事。