

## 推薦論文

# ブロードバンドアクセスサーバにおける AS 透過 BGP 経路制御方法の提案

柘 植 宗 俊<sup>†</sup> 滝 広 眞 利<sup>†</sup> 平 田 哲 彦<sup>†</sup>

ADSL 等の安価な常時接続広帯域アクセス回線（ブロードバンド回線）の普及が個人ユーザだけでなく企業ユーザにまで広がりを見せており、今後はこのような回線を通して、ISP 網や他拠点網等と BGP による経路制御を行う企業ユーザも現れる。個人向けを主としたブロードバンド回線では、ユーザの PPPoE/oA/oEoA セッションを多数収容する機能を備えたブロードバンドアクセスサーバ（BAS）と呼ばれるルータが用いられている。本論文では、BAS を経由して、ISP 網と企業ユーザ網、もしくは企業拠点網と拠点網との間で BGP 経路制御を行う場合のネットワーク構成について述べ、その構成における BAS 向けの BGP 経路制御処理方法を提案する。

## A Proposal of the AS-transparent BGP Routing Method on Broadband Access Servers

MUNETOSHI TSUGE,<sup>†</sup> MASATOSHI TAKIHIRO<sup>†</sup>  
and TETSUHIKO HIRATA<sup>†</sup>

Permanently connected broadband access lines (ADSL etc.) are widely used by not only personal users but also enterprise users, and some enterprise users which perform BGP routing with their sites or an ISP will be appear. A Broadband Access Servers (BAS) is a router which has a function to accept many PPPoE/oA/oEoA sessions from broadband access line users. In this paper, we will explain network structures at which BGP routing is performed between an ISP and enterprise users, or an enterprise site and other sites, via a BAS. And then, we will propose a BGP route processing method for the BAS at one of the structures.

### 1. はじめに

日本・韓国・欧米等を中心に、従来のダイヤルアップ型インターネット接続に代わり、ADSL (Asymmetric Digital Subscriber Line) や FTTH (Fiber To The Home) をはじめとする安価な常時接続広帯域アクセス回線（以降、ブロードバンド回線と称する）が個人ユーザ向けに急速に普及している。多くの ISP (Internet Service Provider) は、このブロードバンド回線を用いてインターネット接続サービスを個人ユーザ向けに提供している。また、個人ユーザ用のブロードバンド回線と共通のインフラを、企業の小規模拠点や SOHO (Small Office/Home Office) 企業のアクセス回線に適用する形で、ユーザにとって安価で導入が容易な、企業ユーザ向けアクセス回線を提供する ISP/

NSP (Network Service Provider) やキャリアも現れ始めている。

個人ユーザ向けを主としたブロードバンド回線では、ユーザの認証や、ユーザへの IP (Internet Protocol) アドレス割当て等を行うために BAS (Broadband Access Server) を用いることが多い。BAS は、主に PPPoE (Point to Point Protocol over Ethernet)<sup>1)</sup>、PPPoA (PPP over ATM)、PPPoEoA (PPPoE over ATM) 等のプロトコルを用いて、ユーザからのセッション接続要求を受け付け、そのセッション上で認証処理と IP アドレスの割当てを行い、BAS の上流網（主に ISP 網や企業の主拠点網）へのアクセシビリティをユーザに提供する。これらの PPP ベースのプロトコルは、OSI (Open System Interconnection) 参照モデルのデータリンク層（レイヤ 2）に属するポイント・

<sup>†</sup> 株式会社日立製作所中央研究所  
Central Research Laboratory, Hitachi, Ltd.

本論文の内容は 2003 年 11 月の分散システム/インターネット運用技術研究会にて報告され、DSM 研究会主催により情報処理学会論文誌への掲載が推薦された論文である。

ツー・ポイントの protocols であり、BAS はこれらの protocols による PPP セッションを終端して、セッションと上流ネットワークとの間で IP パケットを中継する。すなわち、BAS は、OSI 参照モデルのネットワーク層（レイヤ 3）にあたる IP レイヤでパケット中継を行う、IP ルータの一種である。このため、たいいてい BAS 製品はいくつかの IP 経路制御 protocols に対応しており、これによって上流ルータ（上流網内に存在し、レイヤ 2 以下の回線で BAS に接続されているルータ）との間で動的経路制御を可能としている。

一方、個人ユーザ向けブロードバンド回線の企業ユーザによる利用が進み、その回線のバンド幅が向上するに従い、従来の企業ユーザ網のアクセス回線に用いられてきた専用線や ATM (Asynchronous Transfer Mode)、フレームリレー等による接続と同様に、ユーザルータ（企業ユーザ網内に存在し、レイヤ 2 以下の回線で BAS に接続されているルータ）と上流網との間で IP 経路制御 protocols を用いた動的経路制御を行うニーズも増えてくる。この場合、IP レイヤでユーザのすぐ上流に位置する BAS が、ユーザルータとの間で直接経路情報の交換を行うルータとなる。個人ユーザと小規模な企業ユーザを、BAS を含む同一のアクセスインフラの下に収容することにより、運用コストの抑制が可能となるためである。

BAS を経由してユーザルータと上流ルータとの間に適用する IP 経路制御 protocols としては、RIP (Routing Information Protocol)、OSPF (Open Shortest Path First)、BGP (Border Gateway Protocol)<sup>2)</sup> といったいくつかの候補が考えられる。ただし、ユーザルータは BAS とも上流ルータとも異なり、ユーザ自身の管理下に置かれることを考えると、互いに異なる管理下に置かれたルータの間で用いられることを前提とした経路制御 protocols である BGP を用いるのが最も自然である。加えて、ユーザがマルチホーム接続や IP-VPN (Virtual Private Network) といったサービスを受けたい場合や、ポリシー経路制御（経路情報に付加された属性情報等を参照して行う、管理者の意思に従った経路制御）を行いたい場合は、BGP を使わざるをえない。

そこで本論文では、ブロードバンド回線上で BAS を経由して、ユーザ網と上流網との間で BGP による動的経路制御を行う場合のネットワーク構成案を示す。そして、その構成における BAS 向けの BGP 経路制御方法として、AS 透過 BGP 経路制御方法を提案する。

本論文では、2 章で BAS の利用形態を述べ、ブロー

ドバンド回線を通してユーザ網と上流網との間で BGP 経路制御を行う場合のネットワーク構成案を示す。そして、3 章で最適な構成案において BAS が行う AS 透過 BGP 経路制御方法を提案する。4 章では、AS 透過 BGP 経路制御方法の有用性を示す。

## 2. ブロードバンド・アクセス網における BGP 経路制御

本章では、まず、ブロードバンド回線用アクセス網のネットワーク構成と、その構成における BAS の位置を示す。次に、そのような BAS を挟む形態のネットワーク構成の下で、ユーザホストの代わりに企業ユーザを想定したユーザ網を接続し、上流網とユーザ網との間で BGP を用いた経路制御を行う場合を考える。そして、この場合の BGP ピアや AS の構成案をいくつか示し、その中からアクセス網に最適な構成案を選択する。

### 2.1 ブロードバンド・アクセス網の構成と BAS の役割

図 1 に、ブロードバンド・アクセス網のネットワーク構成を示す。実際にはこのほかに、DSLAM (Digital Subscriber Line Access Multiplexer) 等のレイヤ 2 以下の処理を行う機器や、L2TP (Layer 2 Tunneling Protocol)<sup>3)</sup> トンネル等のレイヤ 2 仮想回線もネットワーク上に存在する場合があるが、IP レイヤの経路制御を説明するうえでは不要なため、省略した。

BAS は、単一の上流網に接続され、ユーザホスト（またはユーザ網内のブロードバンドルータ）との間の PPP セッション（もしくは、PPP でカプセル化されていない IP パケット）を直接収容し、ユーザと上流ルータとの間で IP パケットの中継を行う。この PPP セッションの認証を行う際に、BAS は、上流網内に置かれた RADIUS (Remote Authentication Dial-In User Service) サーバからユーザ認証情報を受け取り、その情報をもとにユーザとの PPP セッションの認証

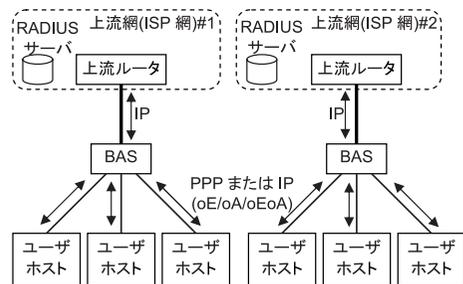


図 1 ブロードバンド網のネットワーク構成  
Fig.1 A structure of broadband network.

を行う。

2.2 BAS・上流ルータ間の BGP 経路制御

現状のBASの用途では、ユーザホストは単一のBASと単一のPPPセッションを設け、ユーザホスト側が持つグローバルIPアドレスはPPP接続時に与えられた単一のアドレスのみとなるのが普通である。この場合、BASはPPPセッションによる直結経路のみをユーザ側の経路として持てばよく、ユーザホスト側もその単一のPPPセッションをデフォルト経路とすればよいので、BASとユーザホストの間の動的経路制御は特に必要ない。

一方、上流ルータとBASとの間については、動的経路制御が行われることもありうる。たとえばユーザホストに割り当てたIPアドレスをBASから上流ルータ側へ広告させたい場合、1台のBASが複数の上流ルータと接続されていてそれらの回線を使い分けたい場合等が、ここでの動的経路制御の用途として考えられる。

ここで用いられる経路制御プロトコルとしては、RIP, OSPF, BGP等、様々なものが利用可能であるが、本論文では以下の理由により、ここで原則としてBGPを用いることとする。現在の国内のADSL・FTTH回線では、サービスの効率的な広域展開等の理由で、アクセス網(BASおよび、BASとユーザホストや上流ルータとの間の接続回線)を管理するアクセス回線業者と、上流網(ISP網)を管理するISP業者は別であることも多い。この場合はBASと上流ルータが互いに異なる管理下に置かれていると見なすことができる。そこで、互いに異なる管理下のルータ間で用いられ、柔軟なポリシ経路制御が可能な経路制御プロトコルである、BGPを用いるのが望ましい。

図2に、BASと上流ルータとの間の、BGP経路制御の運用形態例を示す。BASと上流ルータは、互いに異なるAS(Autonomous System)に属し、AS間で経路情報を交換するためのTCP(Transmission Control Protocol)接続であるEBGP(External BGP)ピア接続を両ルータ間に設ける。ここで、ASとは、同一の管理下にあり、単一のAS番号が割り当てられたネットワーク範囲を指す。

2.3 上流網・ユーザ網間の BGP 経路制御

本節では、2.1節、2.2節で述べた状況をふまえたうえで、上流網とユーザ網との間でBGP経路制御を行う場合の、BGPピアとASの構成を説明する。

2.3.1 BASを経由しないBGPピア構成

図3は、BASを経由せずに、上流網とユーザ網とを直結した場合の、BGPピアとASの構成を示して

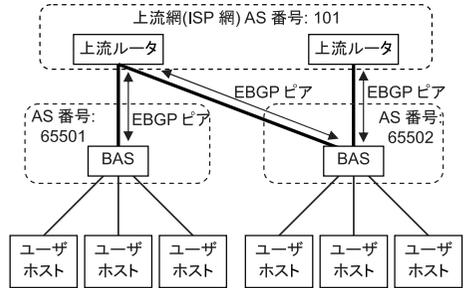


図2 BAS・上流ルータ間の BGP 経路制御 Fig.2 BGP routing between BASes and its upper level routers.

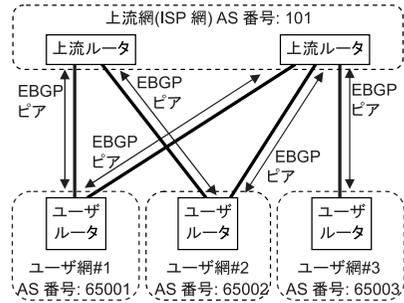


図3 BASがない場合の BGP ピア構成 Fig.3 A structure of BGP peers without BAS.

いる。従来の専用線やATM、フレームリレー等の回線を用いたAS間の相互接続がこの場合にあってはまる。

この場合、上流網のASとユーザ網のASとは互いに隣接したASとなるため、たとえばMED(Multi Exit Discriminator)属性のように、隣接AS間のみで伝わるBGP属性情報も用いて、自由度の高いポリシ経路制御を行うことができる。

なお、このMED属性とは、BGPの経路情報に付加される属性情報の1つで、2つの隣接AS間が複数の回線で接続されている場合に、IPパケット転送時に優先して使用すべき回線を、一方のASから他方のASへ指定するために用いられる。同一の隣接ASから、MED属性の値が異なる複数の経路情報を受信したBGPルータは、MED属性よりも優先すべき各種の経路選択条件が同一であれば、最もMED属性の値が小さい経路を選択する。

一般的にMED属性は、1つのユーザ網が複数の上流網と接続する形態のマルチホーム接続では意味をなさない。一方、AS番号割当機関から正式なAS番号を得ずにアクセス回線を冗長化する場合等に、同一の上流網と複数の回線接続を設けることもある。このようなときに、品質やコストの異なる複数の回線をポリシ経路制御で使い分けるにはMED属性が有効である。

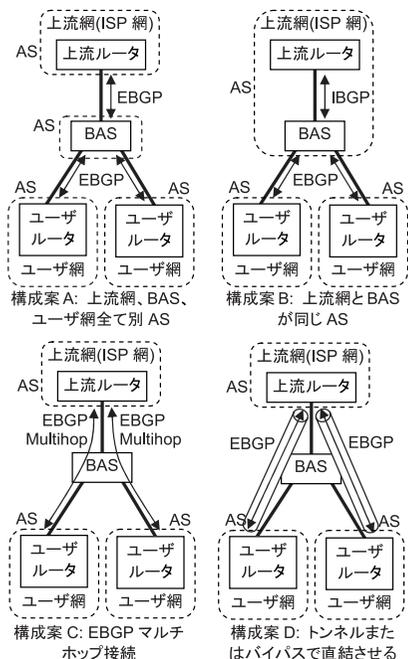


図 4 BAS を挟んだユーザ網・上流ルータ間の BGP ピア構成案  
 Fig.4 Structure patterns of BGP peer connections between an upper level router and user networks via a BAS.

### 2.3.2 BAS 経由の BGP ピア構成案

一方、2.1 節で想定したブロードバンド・アクセス網を通して上流網とユーザ網を接続する場合は、両者の間に BAS, すなわちルータを挟む構成となる。一般的に、EBGP ピア接続では接続を行うルータどうしが直結回線上にないと、ピアルータ (ピア接続を行うルータどうしの一方から見た他方のルータ) への到達経路が分からず、ピア接続を設けることができない。この問題を解決する BGP ピア構成方法としては、以下の 4 つの案が考えられる。また、これらの構成案を図に表すと図 4 のようになる。

**構成案 A** 上流網, BAS, ユーザ網をすべて異なる AS に属させ, 上流ルータと BAS, BAS とユーザルータ双方で EBGP 接続する。

**構成案 B** BAS を上流網と同じ AS に属させ, 上流ルータと BAS を IBGP (Internal BGP) 接続, BAS とユーザルータを EBGP 接続する。

**構成案 C** EBGP マルチホップ接続 (直結回線上にないルータとの EBGP ピア接続) を用いて, 上流ルータとユーザルータを直接 EBGP 接続する。

**構成案 D** トンネリングプロトコルを用いて, もしくは BAS をバイパスして, レイヤ 2 以下で BAS を通過させ, 上流ルータとユーザルータを直接 EBGP

接続する。

これらのうちで, 構成案 A は, 上流網, BAS, ユーザ網すべてを異なる AS として扱うので, それぞれの管理独立性を維持しやすく, それぞれの間で EBGP ピア接続を通してポリシー経路制御も行うことができる。加えて, 上流ルータやユーザルータには通常の BGP 経路制御以外の特別な設定 (BGP 以外による BAS 側回線の経路設定や, トンネリングの設定等) が必要ない。ただし, 上流網とユーザ網との間に別の AS を挟む形になるので, MED 属性のように, 隣接 AS のみで適用可能な属性を用いたポリシー経路制御を行うことができないことと, BAS に BGP 経路制御のための設定が必要であることが, 構成案 A の欠点といえる。特に後者の欠点を解決するには, 多くのユーザルータが接続される BAS の BGP 設定 (経路フィルタ等を含む) を効率良く行い, 上流網側が望む BGP 設定を BAS に反映させることが可能な管理インターフェースが必要になる。

**構成案 B** は, 上流網の AS とユーザ網の AS とが隣接するため, 隣接 AS のみで適用可能な属性を利用したポリシー経路制御を行うことができ, ユーザルータに通常の BGP 経路制御以外の特別な設定を行う必要もない。しかし, BAS が上流網の AS に属することになるため, 上流網と BAS との間で管理独立性を維持しにくいことに加え, BAS には BGP 経路制御のための設定だけでなく, 上流網とユーザ網との間のポリシー経路制御に関する設定も必要になる。しかも, 上流ルータと BAS との間は IBGP ピア接続 (AS 外から得た BGP 経路情報を同一 AS 内の他の BGP ルータへ通知するためのピア接続) であり, AS 内の経路制御には通常用いることができないため, 上流ルータと BAS との間で RIP, OSPF といった IGP (Interior Gateway Protocol) による AS 内経路制御, もしくは静的経路設定を別途行う必要がある。

**構成案 C** は, EBGP マルチホップ接続機能を用いることにより, BAS を挟んでいても, 上流ルータとユーザルータが直接 BGP 経路制御を行うことができる。このため, 隣接 AS のみで適用可能な属性を利用したポリシー経路制御を行うことができることに加え, BAS には BGP 経路制御のための設定が不要である。しかし, EBGP マルチホップ接続を行うには, 上流ルータとユーザルータの双方にピアルータへの経路をあらかじめ (ピア接続前に) 静的経路または IGP で設定する必要があることに加え, BGP 経路情報は BAS で解釈されずに通過するので, BAS への経路情報の設定も別の手段で行う必要がある。さらに, 直結され

ていないBGPルータ間のEBGPピア接続を許すことになるため、送信元IPアドレスの詐称を悪用した、不正なBGPピア接続要求・接続奪取・切断要求や、ルータのBGPポートへのDoS(Denial of Service)攻撃の可能性もある<sup>4)</sup>。

構成案Dでは、上流ルータとユーザルータがレイヤ2相当の回線で直結され、直接BGP経路制御を行うことができるため、隣接ASのみで適用可能な属性を利用したポリシ経路制御も行うことができることに加え、BASにはBGP経路制御のための設定が不要である。しかし、上流ルータとユーザルータとの間でトンネリングを行う場合、トンネリング機能とその設定、およびトンネリングのためのピアルータへの経路設定が、ユーザ側、上流側側の両ルータで必要になる。また、BGP経路情報はBASを通過してしまうので、BASへの経路情報の設定を別の手段で行う必要もある。一方、BASをバイパスする場合は、BASを通らないバイパス回線を設置する必要があるのに加え、BASをバイパスするために、従来はBASで行っていたユーザ認証処理等を、上流ルータ自身が行わなければならない。

以上より、上流網、BAS、ユーザ網それぞれが異なる管理下にあるブロードバンド・アクセス網においては、上流網とユーザ網との間のポリシ経路制御に制限があるものの、構成案Aが最も有力な選択肢である。一方、構成案Bは上流網とBASとの間の管理独立性、構成案Cはセキュリティ、構成案DはユーザルータやBASの管理負担とユーザ認証手段に問題があるため、このようなアクセス網への適性は構成案Aに劣る。

以降では、構成案AのBGPピア構成を想定し、その欠点を解消して柔軟なポリシ経路制御を可能とする、AS透過BGP経路制御方法について説明する。

### 3. AS透過BGP経路制御方法の提案

本章では、2.3.2項の構成案Aにおいて、上流網のASとユーザ網のASとの間にBASのASを挟むことにより発生する問題を整理し、それらの問題の解決案を示す。

#### 3.1 前提条件と課題の整理

##### 3.1.1 アクセス網構成に基づく前提条件

アクセス網においては、その一般的な網構成や利用形態に基づいて、次の前提が成り立つ。

通常BASの利用形態では、BASが上流網(主にISP網)のユーザの接続認証を行うことを考えれば、1台のBASの上流網は1つであるのが一般的である。また、上流網はユーザとインターネットとの間

や、ユーザとユーザとの間のIPパケット中継を提供する立場であり、BASを所有するアクセス回線業者はあくまでユーザと上流網との間の回線を提供する立場である。BASに接続されるユーザは個人や企業といったエンドユーザなので、ユーザ網はトランジットAS(自AS以外を宛先とするパケットを、自AS外から受け取り、中継するAS)として動作する必要はない。

以上より、本章では次の5つの前提条件を設ける(これらの前提条件が成り立たない場合に関する考察は、付録において行う)。

前提 i 1台のBASは複数の上流ルータと複数の回線

を通じて接続してもよいが、それらの上流ルータは必ず1つのAS、すなわち1つの上流網に属する。

前提 ii BASは上流網と上流網の間でのデータパケット中継を行わない(上流ルータから届く経路情報を上流ルータへ再広告せず、上流ルータから届くパケットの中継にも使わない)。

前提 iii BASはユーザ網とユーザ網の間でのデータパケット中継を行わない(ユーザルータから届く経路情報をユーザルータへ再広告せず、ユーザルータから届くパケットの中継にも使わない)。

前提 iv BAS どうしが直接データパケットの送受信を行うことはない(必ず上流網を介する)。

前提 v ユーザ網はトランジットASとして動作しない。ただし、完全にそのユーザ網の配下にあるAS(そのユーザ網を通り抜ける以外に、他ASへの到達経路を持たないAS)のトラフィックについてのみ、トランジットすることがある。

##### 3.1.2 要求条件と課題

図5に、あるネットワーク構成で2.3.2項の構成案AのBGPピア接続構成を適用した場合の、ASパス属性とMED属性が付加された経路情報の伝播例を示す。このように、通常BGP経路制御方法では、ユーザルータと上流ルータとの間でMED属性等のASを通過しない属性が伝わらず、これらの属性を用いたポリシ経路制御を行うことができない。

そこで、以降では、3.1.1項の前提の下で、構成案Aにおける次の要求条件を満たす解決方法の提示を目標とする。

要求条件 MED属性等のASを通過しない属性情報が、ユーザルータと上流ルータとの間で伝わるようにし、ユーザ網と上流網との間でポリシ経路制御の手段が制限されないようにする。

しかし、図5の経路情報伝播例を見ると分かる通り、この要求条件を満たすためには、次の3つの付随

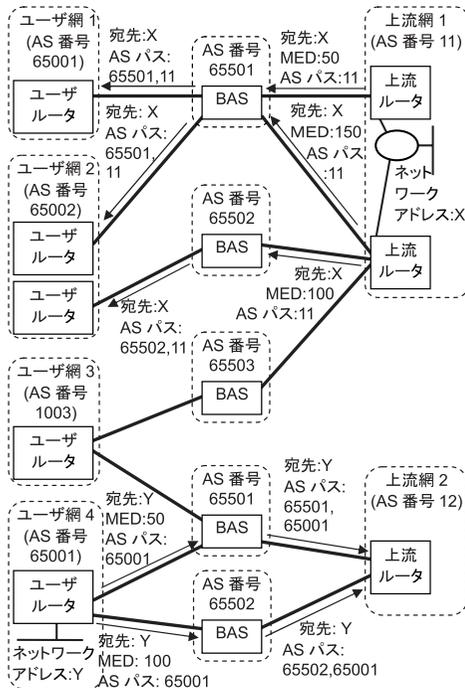


図5 構成案 A の BGP ピア構成における、経路情報の伝播例  
 Fig. 5 An example of propagation of routing informations on a BGP peer structure based on the structure pattern A.

的な課題も解決する必要がある。

**課題 1** ユーザルータから上流ルータへ広告された経路情報を別のユーザルータへ広告することを可能にするためには、同一の上流網に接続されている BAS それぞれに、異なる AS 番号を割り当てる必要がある。もし、同一の AS 番号を持つ BAS が存在すると、あるユーザルータから受け取った経路情報を別のユーザルータへ再広告する際に、BAS が経路情報のループと間違えてその経路情報を破棄してしまうことがある。

**課題 2** 仮に、BAS がユーザルータと上流ルータとの間で、MED 属性を単純に通過させても、BAS はそれぞれが異なる AS 番号を持つため、MED 属性が有効に働かない。異なる BAS を通って届いた MED 属性付き経路情報は、それらの経路情報の受信側 AS では、それぞれ異なる隣接 AS から届いた経路情報であると見なされる。このため、通常設定のルータでは、最適経路決定の際に MED 属性の比較が行われない。

**課題 3** ユーザ網の視点からは、上流網の AS ではなく、BAS の AS (通常、上流網側が独自に割り当てたプライベート AS 番号を用いると考えられる) が

隣接 AS に見える。さらに、ユーザ網が複数の上流網とマルチホーム接続していた場合に、隣接 AS の AS 番号重複等の問題を引き起こす。

**3.2 課題を解決する BGP 経路制御方法の提案**

以下、本節では、3.1.2 項で述べた課題を解決し要求条件を満たす、AS 透過 BGP 経路制御方法を提案する。なお、本節では、AS を通過しない属性のうち、MED 属性のみを検討対象とする。AS を通過しない他の属性については、3.3 節で述べる。

AS 透過 BGP 経路制御方法では、すべての BAS に同一の AS 番号を割り当て、BAS はユーザ網に対して自 AS が上流網の AS であるかのように振る舞う。そのうえで、上流網とユーザ網との間で MED 属性を通過させることにより、ユーザ網と上流網との間で MED 属性が有効に働くようにする。以下、AS 透過 BGP 経路制御方法の詳細を述べる。

**3.2.1 自 AS 番号の通知**

まず、課題 2 のうちでユーザルータへの経路情報広告に関する部分と、課題 3 を解決するために、BAS はユーザルータに対して、上流網の AS 番号を自 AS 番号と見せかけて通知する。一方、上流ルータに対しては、上流網の AS 番号を BAS の自 AS 番号として通知すると、そのピア接続は IBGP として扱われ、構成案 A に沿わないピア接続構成になる。このため、同一の上流網の下にある BAS には、上流網ともユーザ網とも異なる、すべて同一の AS 番号を自 AS 番号として割り当て、この自 AS 番号を上流ルータに対して通知することにより、課題 2 のうちで上流ルータへの経路情報広告に関する部分を解決する。

BGP ルータがピアルータへ自ルータの AS 番号を通知する機会は、ピア接続確立時に送信する OPEN メッセージと、広告する経路情報に付随する AS パス属性の先頭要素の、2 種類がある。このうち前者の OPEN メッセージに、本節で述べた AS 番号の通知方法を適用した例を、図 6 に示す。後者の AS パス属性への適用については、他の課題の解決とともに、次節で詳しく説明する。

**3.2.2 属性情報の処理**

3.2.1 項の変更を行うと、課題 1 で述べたように、経路情報の破棄が起こる。この解決のために、BAS は、上流ルータから受信した経路情報の AS パス属性に自 AS 番号が含まれていても、その経路情報を破棄せずに処理する。そして、その経路情報をユーザルータへ広告する際には、AS パス属性の先頭に自 AS 番号を追加せず、AS パス属性から自 AS 番号をすべて削除してから広告する。

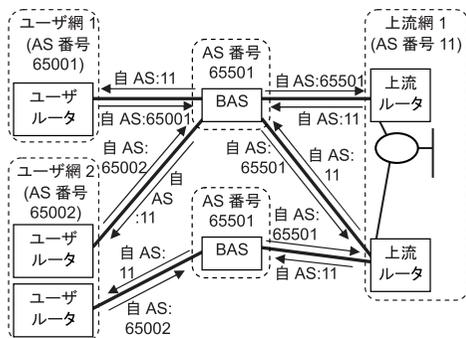


図 6 AS 透過 BGP 経路制御方法に基づく、AS 番号割当てと OPEN メッセージ

Fig. 6 AS number assignments and OPEN messages based on the AS-transparent BGP routing method.

BAS が上流ルータから受信した経路情報の AS パス属性の先頭要素には、もともと上流網の AS 番号が入っている。このため、BAS が自 AS 番号を AS パス属性の先頭に追加しないことにより、BAS からユーザルータへ広告する経路情報の AS パス属性の先頭要素も上流網の AS 番号となり、ユーザ網からは BAS が上流網の AS に属しているように見える。加えて、BAS からユーザルータへ広告する経路情報の AS パス属性に BAS 自身の AS 番号を含めないことにより、ユーザ網に対して BAS 自身の AS の存在を隠蔽することができる。

また、ユーザルータから受信した経路情報については、自 AS 番号の代わりに上流網の AS 番号を用いて、経路情報のループチェックを行う。これは、ユーザ網からは BAS が上流網の AS に属しているように見えることを考えると、通常の BGP 経路情報ループチェックと同様である。この経路情報を上流ルータへ広告する際には、その AS パス属性の先頭に自 AS 番号を追加して広告する。これも、上流網からは BAS が上流網と異なる自 AS 番号を持っているように見えることを考えると、通常の BGP の AS パス属性処理と同様である。しかも、BAS の自 AS 番号をすべて同一としたので、ユーザ網から BAS を経由して上流ルータに届いた経路情報は、上流網にとってはすべて同じ隣接 AS から届いたように見える。

以上の変更に加え、BAS は、上流ルータから受信した経路情報をユーザルータへ広告する際には、受信した際に付加されていた MED 属性をそのまま付加する。ユーザルータから受信した経路情報を上流ルータへ広告する際も同様である。

以上で述べた AS パス属性と MED 属性の処理変更を、図 5 のネットワークに適用した例を、図 7 に示す。

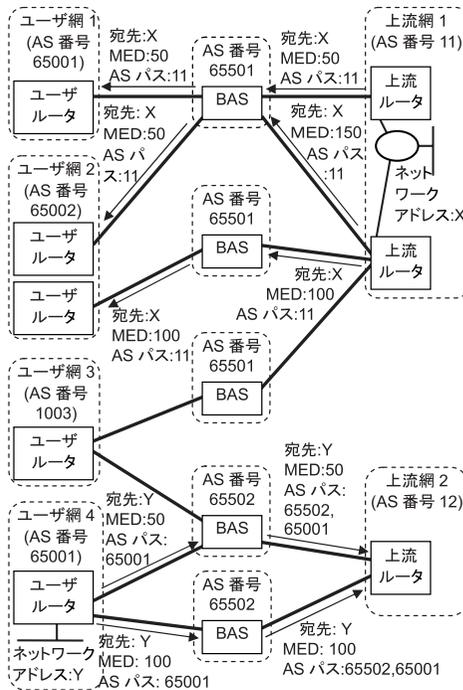


図 7 AS 透過 BGP 経路制御方法に基づく、経路情報の伝播例  
Fig. 7 An example of propagation of routing informations based on the AS-transparent BGP routing method.

この処理変更により、独立した AS をなすルータである BAS を間に挟んでいるにもかかわらず、ユーザ網と上流網の間で MED 属性が通過するようになる。その結果、MED 属性を用いたポリシー経路制御が可能となり、要求条件を満たすことができる。

### 3.3 MED 属性以外の AS 非通過属性の扱い

AS を通過しない属性としては、MED 属性以外に、いくつかの周知コミュニティのコミュニティ属性<sup>5)</sup>をあげることができる。

コミュニティ属性とは、経路情報に任意の値を付加情報として与えるための属性である。ネットワーク管理者は、コミュニティ属性の値とその意味の対応付けに従って、ある特性を有する経路情報へのコミュニティ属性の付加や、あるコミュニティ属性が付加された経路情報に対する処理をルータに設定することができる。コミュニティ属性の値には、対応する意味が標準で定められている周知コミュニティと、ネットワーク管理者が独自に意味を定めることができるプライベートコミュニティがある。

一般的にコミュニティ属性は AS を通過できるため、AS 透過 BGP 経路制御方法の下でも問題なく使用できる。しかし、周知コミュニティに含まれる NO\_EXPORT および NO\_ADVERTISE コミュニ

ティ値は、AS 外やルータ外へ経路情報を再広告してはならないことを示すコミュニティ値である。このため、ユーザルータと上流ルータとの間に独立した AS 番号が割り当てられた BAS が存在する状況では、ユーザルータと上流ルータとの間でこれらのコミュニティ値を付加した経路情報が伝わらない。

そこで、AS 透過 BGP 経路制御方法では、これらのコミュニティ値が付加された経路情報を BAS が受信しても、BAS はコミュニティ値に従った処理を行わず、コミュニティ属性をそのまま付加して経路情報を再広告する。これにより、ユーザルータと上流ルータとの間で、これらのコミュニティ値が付加された経路情報が伝わるようになる。

ただし、上記の対策を施すと、経路情報を上流ルータから BAS のみへ広告し、その先のユーザルータへ広告しないようにする目的では、NO\_EXPORT や NO\_ADVERTISE コミュニティ値を使用できない。この問題を解決するには、プライベートコミュニティの特定の値を、BAS が再広告しない経路情報を示すコミュニティ値と定め、それに従った経路フィルタを BAS に設定すればよい。

#### 3.4 スケーラビリティに関する考察

AS 透過 BGP 経路制御方法を用いて、BAS が多数のユーザルータとの間で BGP ピア接続を設けると、多量のピア接続や経路情報に BAS が性能的に耐えられるかが問題になる。本節では、次の 2 つの観点からスケーラビリティに関して考察する。

##### (1) 経路数のスケーラビリティ

BGP は AS 間の経路制御に用いられるプロトコルであり、インターネットの基幹網においては、インターネット上の全経路が BGP を用いて広告されている。この全経路は現時点で 16 万経路以上もの大きさであり、このすべてを複数のピア接続で扱うことは BAS にとって大きな負担である。

しかし、3.1.1 項の前提で述べたとおり、本論文ではユーザ網がトランジット AS として動作しないことを前提としている。この場合、ユーザ網は全経路を扱わなくても、部分経路とデフォルト経路のみで十分実用的な BGP 経路制御を行うことが可能である。以上の理由により、スケーラビリティの観点からは、経路数は問題にならない。

##### (2) ピア数のスケーラビリティ

一般的な BAS は、数千～数万ユーザの PPP セッションを収容可能である。一方、一般的な BGP ルータはせいぜい数百本程度の BGP ピア接続しか設けることができない。よって、BAS の収容ユーザすべてが BGP

ピア接続を設けることは性能的に困難であり、収容可能な PPP セッション数とは無関係に、最大 BGP ピア数を数百程度に抑えざるをえない。

しかし、BGP による経路制御を望む企業ユーザは、BGP が不要なユーザ（個人および企業）に比べて少ない比率である。よって、BGP が不要な数千～数万のユーザと、BGP が必要な数十～数百の企業ユーザの双方を同時に収容可能な BAS であれば、それぞれのユーザのために別個の装置を用意するよりも効率的な運用が可能であり、十分に実用的である。

#### 4. AS 透過 BGP 経路制御方法の有用性

以上で述べた AS 透過 BGP 経路制御方法により、BAS を通して接続されたユーザ網と上流網との間で、MED 属性や周知コミュニティを用いた経路制御が可能となる。これにより、ユーザ網が同一の上流網との間に 2 つ以上の回線を設けている場合において、たとえそれらの回線の両方もしくはいずれかに BAS が存在しても、存在していない場合と同様の BGP ポリシ経路制御を行うことができる。加えて、ユーザ網側から見ると、BAS に割り当てた AS 番号ではなく、上流網の AS 番号が隣接する AS 番号に見える。このため、ユーザ網側は BAS を介さずに上流網と直結されている場合と同じ感覚で BGP の設定を行うことができる。

以上の利点を具体例で示すために、AS 透過 BGP 経路制御方法の適用例を図 8 に示す。この例では、ユーザ網が L2TP 網（L2TP トンネルを設けるための IP 網）を介して、LNS（L2TP Network Server）として運用されている複数の BAS に接続されている場合に、MED 属性を用いて、ユーザルータにより適切な LNS を経由した経路を選択する。

この例では、主拠点網がここまで述べた上流網、副拠点網がユーザ網にあたる。各副拠点のルータ S1, S2, S3 は、2 台の LNS N1, N2 までの PPP セッションを設けており、それらを通して EBGP ピア接続を行っている。各 LNS は主拠点網内にある 2 台のルータ M1, M2 と接続する回線を持ち、そのうえで EBGP ピア接続を行っている。また、主拠点ルータと LNS との間の回線については、M1 と N1, M2 と N2 を接続する回線を優先的に利用する。

このネットワーク構成において、主拠点網内で M1 に近い位置にあるネットワークの IP アドレスプレフィックス Z に関する経路情報を、各副拠点へ広告する場合を考える。この場合、図のように、主拠点ルータ M1 から LNS N1 へは MED 属性値 50 を、M2 から N2

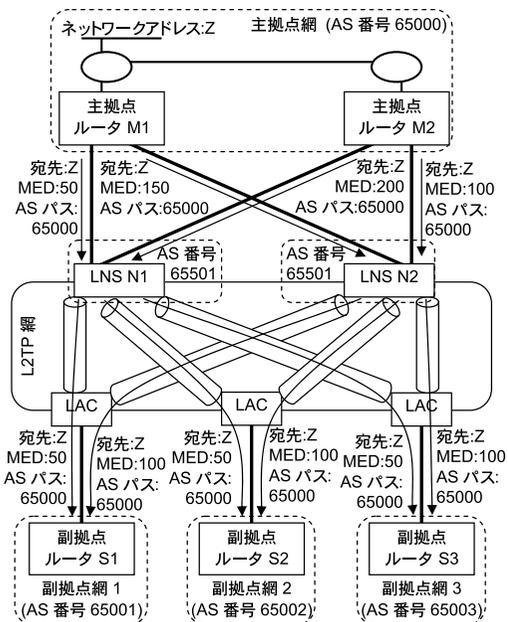


図 8 AS 透過 BGP 経路制御方法の応用例

Fig. 8 An application example of the AS-transparent BGP routing method.

へは 100 を, M1 から N2 へは 150 を, M2 から N1 へは 200 を付けた経路情報を広告する. このようにすることで, 主拠点ルータと LNS との間の回線がこれらの MED 属性値の小さい順で利用されるように, 副拠点からの Z 宛のトラフィックが LNS へ届くようになる. たとえば, 主拠点ルータと LNS との間の回線に何も障害がなければ, 副拠点からの Z 宛の IP パケットは, 必ず LNS N1 と主拠点ルータ M1 を経由して届くが, もし N1 と M1 との間の回線に障害が発生すれば, N2 と M2 を経由して届くように切り替わる.

### 5. おわりに

本論文では, BAS を経由して上流網とユーザ網との間で BGP 経路制御を行う場合を想定し, その場合の AS やピア接続の構成の案を示した. そして, それらの案のうちの一つである, 上流網, BAS, ユーザ網それぞれに異なる AS 番号を割り当てた場合の構成において, 隣接 AS でなければ通常は伝播も作用もしない MED 属性を有効に作用する形で伝播させ, かつ, ユーザ網側に対して BAS に割り当てた AS 番号を隠蔽する, AS 透過 BGP 経路制御方法を提案した. また, その BGP 経路制御方法の有用性や応用例も示した.

本論文で述べた AS 透過 BGP 経路制御方法により, BAS のようなレイヤ 3 中継装置を挟んで接続された

AS 間において, 柔軟な BGP ポリシ経路制御が可能になる. 特に, 一方の AS においては, 中間のレイヤ 3 中継装置に割り当てた AS 番号が完全に隠蔽され, レイヤ 3 中継装置なしに直結されている場合と同様に BGP の設定を行うことができる.

今後の課題としては, 誤設定を行った場合に発生している問題の分析およびその対策, 本論文で述べた経路制御方法の実装による検証があげられる.

### 参考文献

- 1) Mamakos, L., Lidi, K., Evarts, J., Carrel, D., Simone, D. and Wheeler, R.: A Method for Transmitting PPP Over Ethernet (PPPoE), RFC2516 (1999).
- 2) Rekhter, Y. and Li, T.: A Border Gateway Protocol 4 (BGP-4), RFC1771 (1995).
- 3) Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B.: Layer Two Tunneling Protocol "L2TP", RFC2661 (1999).
- 4) Murphy, S.: BGP Security Vulnerabilities Analysis, Internet Draft (draft-ietf-idr-bgp-vuln-01.txt, work in progress) (2004).
- 5) Traina, P., Chandrasekeran, R. and Li, T.: BGP Communities Attribute, RFC1997 (1996).

### 付 録

#### A.1 前提条件が成立しない場合の考察

3 章では, 3.1.1 項で示した前提条件を置くことにより, 実用的な範囲で課題を絞って AS 透過 BGP 経路制御方法を提案した. 本章では, これらの前提条件が成立しない状況において, 提案した AS 透過 BGP 経路制御方法を実施した場合に生じる問題と, その解決策について述べる.

##### A.1.1 BAS の上流 AS が複数存在する場合

まず, 前提 *i* を取り除き, 1 台の BAS に複数の上流 AS が存在することを許した場合における, AS 透過 BGP 経路制御方法の適用を考える. この場合, BAS はユーザルータに対してどの上流 AS に属しているように見えるかをあらかじめ決めておく必要がある (以降, この上流 AS を主上流 AS と呼ぶことにする). これは, BGP のプロトコル仕様上, BGP ルータはピアルータに対して一貫してただ 1 つの AS に属しているように見える必要があるためである.

BAS は, 主上流 AS とユーザルータに対しては, AS 透過 BGP 経路制御方法を通常どおり適用する. そして, 主上流 AS 以外の上流 AS に対しても, BAS は主上流 AS に属しているかのように動作するが, AS 透

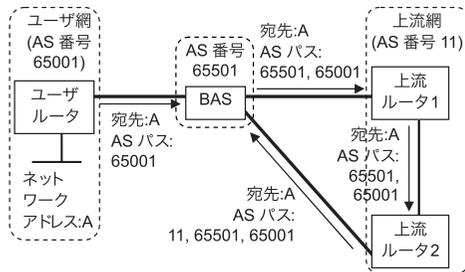


図 9 前提 ii を取り除いた場合における経路ループの発生例

Fig. 9 An example of occurrence of routing loop when the precondition ii is removed.

過 BGP 経路制御方法のような, MED 属性等の操作は行わない. これにより, 主上流 AS 以外の上流 AS は, 主上流 AS を介してユーザルータに接続されているのと同等の状況になる. ただし, 主上流 AS 以外の上流 AS は, ユーザ網との間で AS 非通過属性を用いることはできない.

A.1.2 BAS が上流網から上流網へ中継する場合次に, 前提 ii を取り除き, 上流網から上流網への BAS を介したパケット中継を可能にした場合における, AS 透過 BGP 経路制御方法の適用を考える. この場合は, 次に示すように, 経路ループが発生する可能性がある.

たとえば, 図 9 において, ネットワーク A に関する経路情報がユーザルータから BAS, 上流ルータ 1, 上流ルータ 2, BAS の順に伝わる場合を考える. 上流ルータ 2 から BAS へ伝わる経路情報の AS パス属性には BAS の AS 番号が含まれているため, 通常の BGP 経路制御方法では BAS のループチェック処理が経路ループであると判断し, この経路情報を破棄する. しかし, AS 透過 BGP 経路制御方法ではこのループチェック処理を行わないため, 経路情報を受け取ることとなる. この状態で, 仮にユーザルータから BAS へネットワーク A に関する経路の削除が行われると, ネットワーク A を宛先とする IP パケットは BAS と上流網との間でループする.

この経路ループの発生を回避する対策としては, コミュニティ属性を用いて BAS 単位のループ検出を行う方法が考えられる. まず, 同一の上流網の下での BAS すべてに一意的識別番号 (BGP ルータ ID 等) を割り当てる. BAS は, 上流ルータへ経路情報を広告する際に, 自身に割り当てられた識別番号のコミュニティ属性を経路情報に付加する. そして, BAS は上流ルータから経路情報を受け取った際に, 自身に割り当てられた識別番号のコミュニティ属性が付加されていれば, その経路情報を破棄する.

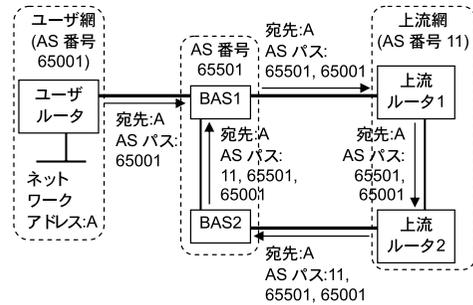


図 10 前提 iv を取り除いた場合における経路ループの発生例

Fig. 10 An example of occurrence of routing loop when the precondition iv is removed.

### A.1.3 BAS がユーザ網からユーザ網へ中継する場合

前提 iii に従った場合, 同一 BAS 下の異なるユーザ間での通信を可能にするには, ユーザルータから届く経路を包含し, ネットマスク長がより短い IP アドレス空間の経路 (たとえば, デフォルト経路) を, 上流ルータから BAS を介してユーザルータへ配布する必要がある. そして, 同一 BAS 下のユーザからユーザへのパケット中継を, BAS の代わりに上流網が行う.

一方, 前提 iii に従わない場合については, このような制約はない. この場合, 同一 BAS 下の異なるユーザ間の通信は, 上流網をまったく介さずに, BAS のみを介して中継されることになる. BAS は, ユーザルータから受信した経路情報を, 上流網を介さずに別のユーザルータへ再広告する際には, その経路情報の AS パス属性の先頭に上流網の AS 番号を付加する.

### A.1.4 BAS どうしが直接データパケットの送受信を行う場合

次に, 前提 iv を取り除き, BAS どうしを直接接続してデータパケット中継を可能にした場合における, AS 透過 BGP 経路制御方法の適用を考える. この BAS 間直接接続は, 接続された BAS どうしの上流網が同一の場合と異なる場合が考えられるが, 異なる場合は A.1.1 節の場合と同様の対策が適用可能であるため, 以下では同一の場合のみ考える.

同一の上流網の下にある BAS どうしを直接接続してデータパケット中継を可能にした場合は, 前提 ii を取り除いた場合と同様に, 経路ループが発生する可能性がある. 経路ループの発生例を図 10 に示す.

前提 ii に従う場合における, この経路ループの発生の回避方法としては, BAS 間でコミュニティ属性を用いる方法が考えられる. 各 BAS は, 上流網側から受け取った経路情報を別の BAS へ直接広告する際には, 上流網側から受け取ったことを表すコミュニティ

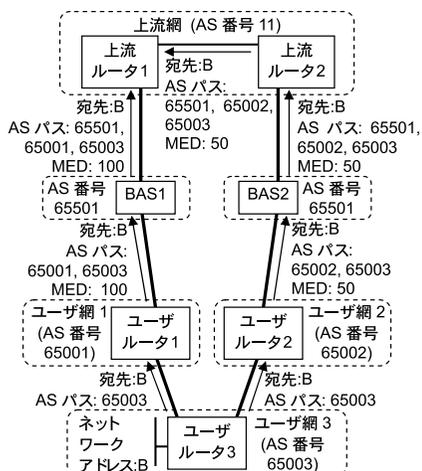


図 11 前提 v を取り除いた場合における MED 属性の伝播例  
 Fig. 11 An example of propagation of routing information when the precondition v is removed.

値を経路情報に付加して広告する。他の BAS から経路情報を直接受け取った BAS は、その経路情報にそのコミュニティ値が付加されていれば、自身がその経路情報を上流網側から受信した場合と同様に扱う。

前提 ii に従わない場合の対策としては、次のいずれかが有効である。

- A.1.2 節と同様に、コミュニティ属性を用いて通過した BAS の履歴を記録する。ただし、A.1.2 節の場合と異なり、通過 BAS は 1 つとは限らない。
- 上流網を介さずに接続された BAS どうしを同じ AS 番号、されていない BAS どうしを異なる AS 番号とし、BAS は上流網から広告された経路情報に対して自 AS 番号を用いてループチェック処理を行う。この場合、ユーザ網から上流網へ広告する MED 属性を用いた経路制御が、3.2 節で述べたとおりには動作しなくなる。

A.1.5 ユーザ網がトランジット AS となる場合

最後に、前提 v を取り除き、ユーザ網がトランジット AS として動作する場合における、AS 透過 BGP 経路制御方法の適用を考える。

たとえば、図 11 のように、複数のユーザ網 1, 2 の先に共通のネットワークアドレス B が存在し、その経路情報をユーザ網 1 と BAS1, ユーザ網 2 と BAS2 の 2 経路を通して上流網に広告する場合を考える。この場合、BAS の AS が上流網の隣接 AS として扱われるので、上流ルータ 1, 2 はこれらの経路情報を同一の隣接 AS から広告された経路として扱う。このため、これらの経路情報はそれぞれ異なるユーザ網 1, 2 を通ったにもかかわらず、上流ルータにおける経路選

択で MED 属性が用いられる。結果として、図 11 において上流網からネットワーク B へ向かうパケットはすべてユーザ網 2 を経由する。

一方、BAS を挟まずに上流網とユーザ網 1, 2 が直結された場合は、ユーザ網が上流網の隣接 AS として扱われるため、上流ルータにおける経路選択で MED 属性は用いられない。BGP ルータは、MED 属性によって選択経路が決まらなければ、学習元のピア接続が EBGP である経路を選択する。結果として、上流ルータ 1 からネットワーク B へ向かうパケットはユーザ網 1 を、上流ルータ 2 からネットワーク B へ向かうパケットはユーザ網 2 を経由することになる。このように、BAS を挟むか否かによって、ユーザ網から上流網へ広告する経路の MED 属性の働きが変化する。

この問題の対策としては、次のいずれかが有効である。

- 各 BAS に相異なる AS 番号を割り振る。この場合、単一のユーザ網から相異なる BAS を経由して上流網へ広告された経路どうしても、MED 属性が比較されなくなる。
- 上流ルータは、BAS から受信した経路情報の AS パス属性から BAS の AS 番号を削除し、削除後の AS パス属性の先頭に格納されている AS から受信した経路情報として扱う。この場合、上流ルータがこのような特殊な経路制御方法に対応している必要がある。

(平成 17 年 3 月 25 日受付)

(平成 17 年 11 月 1 日採録)

推薦文

本論文では、安価なブロードバンド環境において BGP を用いて自由度の高い経路制御を行える冗長化方式が提案されている。この方式は新規性があるだけでなく、潜在的な需要がかなり多く見込まれることから高い有用性があると思われる。以上の理由により本論文は推薦論文に値すると判断した。

(分散システム/インターネット運用技術研究会主査 松浦敏雄)



柘植 宗俊（正会員）

平成 5 年京都大学工学部情報工学科卒業。平成 7 年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了。平成 10 年大阪大学大学院基礎工学研究科情報工学専攻博士後期課程退学。同年（株）日立製作所入社。以来、ルータの経路制御，ブロードバンドアクセス網に関する研究に従事。現在，同社中央研究所ネットワークシステム研究部研究員。電子情報通信学会会員。



平田 哲彦（正会員）

昭和 59 年東京工業大学工学部機械工学科卒業。同年（株）日立製作所入社。以来，コンピュータネットワーク，テレコムネットワークに関する研究に従事。現在，同社中央研究所ネットワークシステム研究部長。電子情報通信学会会員。



滝広 眞利

平成 5 年岡山大学大学院工学研究科情報工学専攻修士課程修了。同年（株）日立製作所入社。以来，ATM ネットワークの QoS 保証方式，ルータの経路制御に関する研究に従事。現在，同社中央研究所ネットワークシステム研究部主任研究員。電子情報通信学会会員。

---