複数データセンターにおける IPv6/IPv4マルチホーミング・ネットワーク設計

都竹 高広

IPv6 and IPv4 Multi-homing Network Design on Multiple Data Center

Takahiro Tsuzuku

企業のネットワークにおいて，ビジネス継続性を背景とした複数データセンター運用の必要性が高まってきている．また2011年4月にIPv4アドレスの在庫が枯渇し，IPv4とIPv6の両方に対応したネットワーク設計が必須となっている．本論文では，実際のお客様事例を題材として，複数データセンターにおいてIPv6およびIPv4のデュアル・スタックを前提とした専用機型のマルチホーミングのネットワーク設計手法を提案する．またこのネットワーク設計によって複雑化する通信経路を可視化するソリューションの重要性についても述べる．これにより，IPv4/IPv6のデュアル・スタック環境へ移行した場合でも，複数データセンター構成における災害時自動切り換えおよびアプリケーション単位での負荷分散要件への対応が可能となる．

In the Enterprise Network, the necessity for system operation among multiple data centers is increasing because of business continuity. Moreover, IPv4 address pool has already been drained in April 2011, and the network design corresponding to both IPv4 and IPv6 is indispensable. This paper described the design method of the IPv4 / IPv6 multi-homing network with network appliance in multiple data centers based on actual customer network design. In addition, this paper also described the importance of the solution which visualizes the network traffic pathway and application responses. As a result, the requirements for application load balancing and disaster recovery network in multiple data centers can be satisfied even after transition to the IPv4 / IPv6 dual stack environment,

Key Words & Phrases：ビジネス継続性，マルチホーミング，IPv6，災害対策，グローバル負荷分散
Business Continuity, Multi-Homing, IPv6, Disaster Recovery, Global Server Load Balancing

1. はじめに

企業内のさまざまなITシステムにおいて，ビジネス継続性（Business Continuity）を前提とした要件定義や設計の必要性は依然として高まる傾向にある.その中で，特に日本においては2011年3月11日に発生した東日本大震災を意識し，システムを2重化することはもちろんのこと，地理的に離れた拠点およびデータセンターでシステムを運用する必要性が高まっている．また,クラウド・コンピューティングの分野では，IBM Managed Cloud Computing Services（MCCS）などのプライベート・クラウド・データセンターやパブリック・クラウド・サービスを併用したハイブリッド型クラウドの利用も次第に増加し，複数のデータセンターに分散したシステムを運用する形態が多くの企業で見られるようになってきている[1][2].

提出日:2011年9月20日　再提出日:2012年5月28日

このような複数データセンター構成においては，データセンターへのアクセス通信の負荷分散や災害時の迅速な切り替えが重要なネットワーク要件となる．インターネットからデータセンターへのアクセス経路となるインターネット回線の冗長化（マルチホーミング）もその1つとして挙げられる.

マルチホーミング・ネットワーク（Internet Service Provider（ISP）への接続の冗長化）では，古くからBorder Gateway Protocol（BGP）や専用機を用いた実装が行われてきた．2011年4月15日にJPNIC［3］でIPv4アドレスの在庫が枯渇しニーズが高まっているIPv6においては，マルチホーミングの実装方法としてアドレス変換の妥当性を主な論点にさまざまな議論がなされている最中にある［4］［5］［6］.

本論文ではお客様事例を題材に，さまざまな議論のあるIPv6マルチホーミング技術の中で，特に製品実装が進んでいるマルチホーミング専用機を用いた，複数のデータセンター環境におけるマルチホーミング・ネットワー

クの設計について論じる.

以下, 2 章ではマルチホーミングの技術の比較とIPv6 でのマルチホーミングの課題, 3 章では複数データセンターにおけるマルチホーミングの要件, 4 章ではそのネットワーク設計と考慮点を述べ, 5 章では当設計に関する考察を行う.

2. マルチホーミングとは

2.1 マルチホーミング実現方法とその技術比較

複数データセンターの議論の前に, 単一データセンターにおける 3 つのマルチホーミング技術を比較する. 企業ネットワークにおけるマルチホーミングは, 単一の拠点またはデータセンターからインターネットへの接続ネットワークにおいて, 複数の ISP と接続した構成を指す. 複数の ISP 回線接続を持つことにより, 可用性の向上やトラフィックの負荷分散が可能となる構成である.

マルチホーミングの主要な実現方法としては, BGP プロトコル, 専用機（回線負荷分散装置）, Domain Name System（DNS）Round Robin がある. **表 1** にこれらの 3 つの技術の比較を示す.

これらの中で, 負荷分散および障害検知による動的な切り替えとアプリケーション単位での経路制御が可能な専用機型が機能的に優れている. 本論文でもこの専用機型を採用したマルチホーミングのお客様事例をモデルにしている.

2.2 IPv6におけるマルチホーミング

IPv4 では, 特に大規模ネットワークなどにおいて BGP によるマルチホーミング構成も古くから実装されてきた. BGP によるマルチホーミングでは, Provider Independent（PI）アドレスというプロバイダーに依存しない特殊なグローバル IP アドレスが必要になる. しかし, IPv6 ではアドレス集約の観点で, 当初 PI アドレスは定義されなかった.

2005 年頃には, Layer3※3 と Layer4 の間に shim 層と呼ばれる新しい Layer を定義するマルチホーミング技術 shim6 も提唱され, 2009 年には RFC5533 として定義された［4］［7］［8］. しかし, shim6 は, ホスト単位でアドレスを切り替えてマルチホームするため, ネットワーク全体のトラフィック制御が効きにくいという問題があり, またその複雑性から実装はあまり進んでいない. 逆に, これらの背景から再び IPv6 PI アドレスのニーズが高まり, 2008 年には JPNIC で IPv6 での PI アドレス配布が開始された[9].これにより,IPv6 でもBGP でのマルチホーミングが可能となっている.

専用機型のマルチホーミングにおいては, 各 ISP に固有のグローバル・アドレスで接続するために Network Address Translation（NAT）が使用される. IPv4 ではアドレス節約の理由で発展した NAT だが, IPv6 では双方向の End to End 通信を行うために, NAT を原則排除する思想が根強い. しかし, IPv4 からの移行期や, 組織内ネットワーク隠ぺいなど, NAT のニーズも強く残り, 独自仕様のまん延を防ぐために IPv6 to IPv6（NAT66）

表1. マルチホーミング実現方法の技術比較

技術	BGP	専用機	DNS RR
概要	ISP から受信した BGP 経路情報によるダイナミック・ルーティング	DNS 応答の A レコード※1 切り替えと通信負荷分散機能による負荷分散	DNS 応答で複数 A レコードを返すことによる Inbound 負荷分散
回線障害への対応	ダイナミック・ルーティングによる迂回	ポーリングによる障害検知と迂回	なし
回線負荷分散（Inbound 通信※2 ／ Outbound 通信）	Inbound: なし utbound:BGP メトリックによる分散	Inbound: 応答 A レコードの切り替えによるルールベースの分散 Outbound: 通信分散装置による分散	Inbound: 複数 A レコードによる自動分散 Outbound: 不可
アプリケーション単位の制御（TCP/UDP）	不可	可（FQDN, TCP/UDPポート番号単位）	不可
回線障害時のセッション断	なし	あり（IP アドレスの切り替え）	あり
主な用例	大規模データセンター	大～中規模データセンターや拠点	中～小規模データセンター
機器コスト	中～大（BGP フルルート受信する場合）	中～大（専用機）	小（DNS サーバー）

※1 ドメイン名（ホスト名）と IP アドレスを対応付ける DNS 設定情報. 本論文に登場するレコードは, A レコード（ホスト名と IPv4 アドレスの対応）, AAAA レコード（ホスト名と IPv6 アドレスの対応）, MX レコード（ドメインにおけるメール・サーバーの指定）.

※2 Inbound 通信はデータセンターへのアクセス通信（外部からのメール受信等）, Outbound 通信はデータセンターから外部への通信（メール送信や外部 Web サイトの閲覧等）を指す.

※3 “Layer” は OSI 参照モデルの層を指す. Layer2 はデータリンク層（MAC アドレス等）, Layer3 はネットワーク層（IP アドレス等）, Layer4 はトランスポート層（TCP/UDP ポート番号等）.

のドラフトが提唱されるなど，その是非はいまだに議論が続いている［10］［11］．また，マルチホーミング専用機はサーバー負荷分散装置をベースにした製品が多いが，サーバー負荷分散装置はその仕組み上 NAT が必須機能となっており，IPv4 と IPv6 または IPv6 と IPv6 を双方向に NAT 可能とする実装も進んでいる．このため，実質的には NAT66 となる専用機型も，IPv6 でのマルチホーミングの現実解として選択肢に挙がっている．

3. 複数データセンターにおけるマルチホーミングの要件と方式の選択

ビジネス継続性を考慮した複数データセンターのネットワークにおいては，以下のようなネットワーク機能・非機能要件が考えられる．

(1) 災対
データセンター規模の障害や災害発生時に,他のデータセンターでサービス継続させる
(2)トラフィック分散
各データセンターを Active/Active で運用し，正常時はトラフィックをデータセンター間で負荷分散する
(3)アプリケーション応答時間
トラフィックをネットワーク遅延の少ないデータセンターへ誘導することで，アプリケーション応答時間を目標値以内に保つ
(4)アプリケーション単位での処理
負荷分散や災対発動または復旧の処理は，アプリケーション単位（Full Query Domain Name（FQDN）や TCP/UDP ポート番号単位）で実装する

特に単一のデータセンターから複数データセンターへ移行する過程においては，システムまたは業務アプリケーションごとに災対または負荷分散の要件を実装していくケースが考えられる．それには「(4) アプリケーション単位」で切り替えが可能なシステムであることが重要なポイントとなる．

4. 複数データセンターにおけるマルチホーミング設計

複数データセンターにおけるマルチホーミング・ネットワークの設計要素としては，グローバル／プライベート・アドレス設計（IPv6），回線負荷分散ルール方式，Demilitarized Zone（DMZ）ネットワーク構成（Layer2 ネットワーク延伸）などが考えられる．アプリケーションとしてメール受信も含まれる場合は，DNS でメール・サーバーを示す MX レコードのグローバル負荷分散も挙げられる． 本論文で対象とする複数データセンターの構成を図 1 に示す．この構成は，製造系のお客様事例をモデルにしている．2 つのデータセンター（DC1/DC2）に IPv4/IPv6 デュアル・スタックのインターネット回線（ISP 接続）を 1 本ずつ収容し，データセンターをまたいだ回線負荷分散を行う．各データセンターには，負荷分散および災対要件のあるアプリケーション（SrvA），災対要件のあるアプリケーション（SrvB），片側データセンターのみに存在し負荷分散および災対要件のないアプリケーション（SrvC）が混在している．

マルチホーミング機能の実装は，アプリケーション単位での制御が可能な専用機型を採用した．ただし，製品性能や DNS 機能を考慮した結果，回線負荷分散装置 1 セットではなく，Outbound 負荷分散と Inbound 負荷分散を別々の装置で実装した．すなわち，Outbound 負荷分散を実装するトラフィック負荷分散装置（一般的にサーバー負荷分散装置／ Server Load Balancer（SLB））と，Inbound 負荷分散を実装する DNS ベースのグローバル負荷分散装置 /Global Site Load Balancer（GSLB）である．

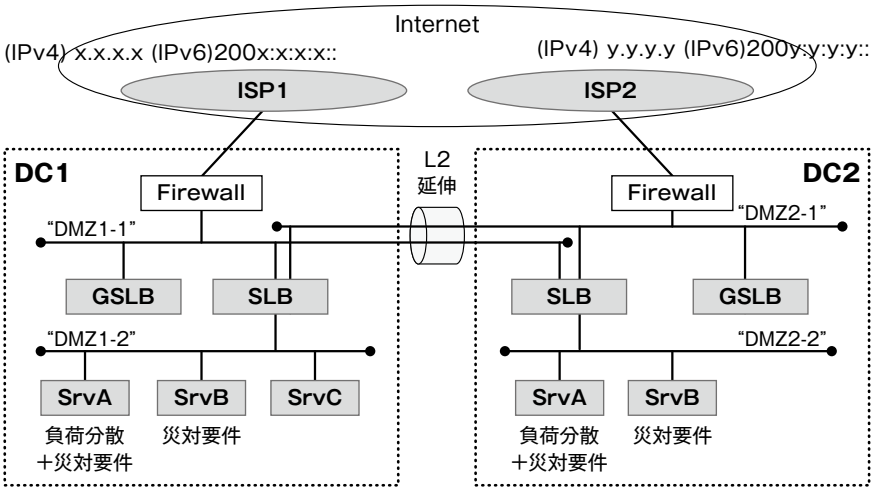


図1. 複数データセンターおけるマルチホーミング基本構成

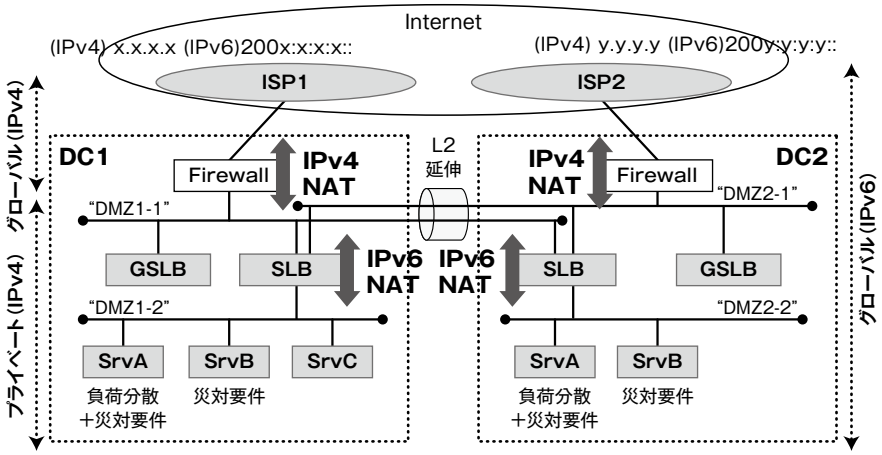
以降に，図 1 の構成におけるネットワーク設計要素を述べる.

4.1 アドレス設計

アドレス設計では,「グローバル・アドレス／プライベート・アドレスと NAT 境界」および「マルチホーミング時のサーバーの公開アドレス」の2つの設計ポイントが挙げられる.

(1)グローバル・アドレス／プライベート・アドレスとNAT境界

IPv4 では，一般的に外部 Firewall または DMZ の SLB または内部 Firewall でグローバル／プライベート・アドレスを NAT する構成が多い．今回の構成においても，IPv4 では外部 Firewall で NAT する構成を採用した．しかし，IPv6 にはプライベート・アドレスの概念が原則として存在しないため,ISP から払い出されたグローバル・アドレスを IPv6 ノードすべてにアサインする必要がある．一般的に IPv6 マルチホーミング環境では，複数の ISP グローバル・アドレスをアサインするマルチプレフィックス問題が生じるが，今回のマルチホーミング環境では，図 2 のように回線負荷分散装置で IPv6 to IPv6 の NAT を実装することで，内部サーバー（SrvA,B,C）には片側の ISP アドレスのみをアサインした.



NWセグメント	IPv4アドレス	IPv6アドレス
“DMZ1-1”	Private1	200x:x:x:1::/64(ISP1)
“DMZ1-2”	Private1	200x:x:x:2::/64(ISP1)
“DMZ2-1”	Private1	200y:y:y:1::/64(ISP2)
“DMZ2-2”	Private1	200y:y:y:2::/64(ISP2)

図2. IPv4/IPv6アドレス設計

(2) マルチホーミング時のサーバー公開アドレス

DMZ のサーバーをインターネットに公開する際のアドレスは，1 つのサーバーに対して複数のアドレスを用意する必要がある．ISP1 と ISP2 の両方で公開するサーバー（SrvA,B）は,各 DC 内のサーバー 1 台に対して 2 つの公開アドレスを用意し，2 つの DC 合わせて合計 4 つの公開アドレスが必要となる．例として，図 3 に SrvA の公開アドレスを示す．DC1 の SrvA 用に，ISP1 および ISP2 経由でアクセスするための IPv4 アドレス（x.x.x.A1，y.y.y.A1）および IPv6アドレス（200x:x:x:x::A1，200y:y:y:y::A1）を用意し，負荷分散あるいは災対切り替え用のサーバーである DC2 の SrvA にも同様に IPv4/IPv6アドレス（x.x.x.A2，y.y.y.A2，200x:x:x:x::A2，200y:y:y:y::A2）を用意する.この8つのアドレスを回線負荷分散装置（今回の構成ではGSLB）に登録し,DNS応答を切り替える.

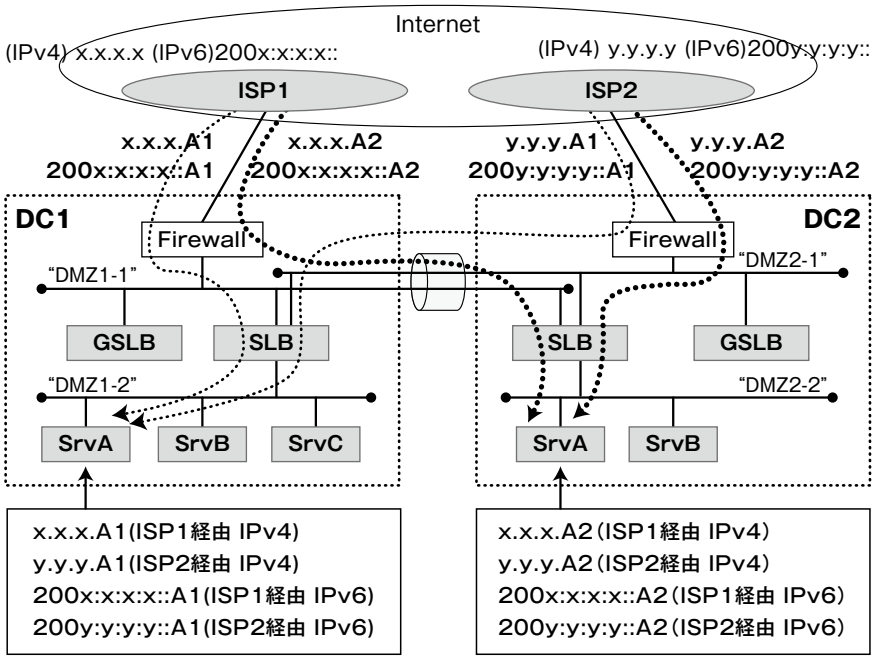


図3. サーバーの公開アドレス

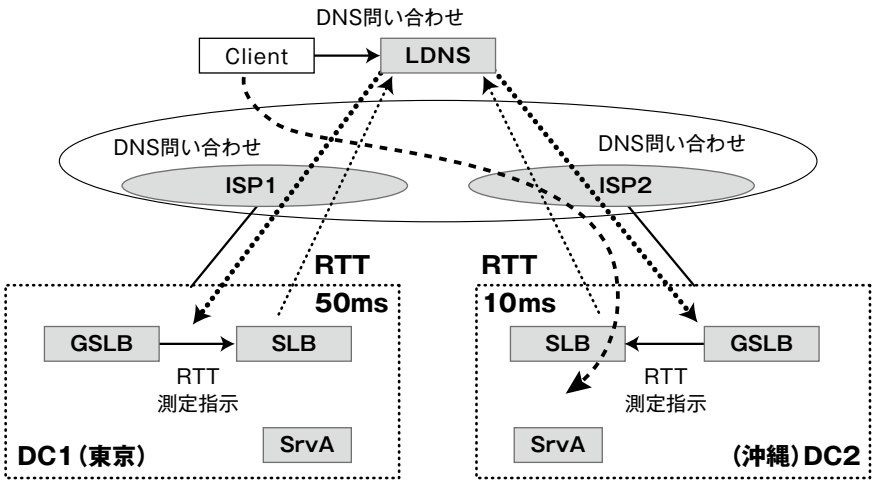


図4. ネットワーク近接性による分散

4.2 負荷分散設計

負荷分散機能は，Inbound 通信では GSLB による DNS 応答（A/AAAA レコード）切り替えによって，Outbound 通信では SLB によるトラフィック分散によって実現する．回線負荷分散装置では，複数の回線またはサーバーへのトラフィック経路をアプリケーション単位でルール付けし負荷分散することが可能である．負荷分散ルールとして，DC1 と DC2 のサーバーを均等または重み付けした負荷分散する方式のほかに，DC1 のサーバーをメインとし DC2 のサーバーをバックアップとする災対切り替え方式も可能である［12］．

また，複数データセンターを地理的に離れた場所に設置する場合は，ネットワーク伝送遅延のより少ないデータセンターへ Inbound 通信を誘導することでアプリケーション応答時間を改善させる，ネットワーク近接性ベースの負荷分散が非常に有効である．ネットワーク近接性ベースの負荷分散では，図 4 のように各データセンターからユーザー側の Local DNS（LDNS）サーバーまでの往復伝送遅延時間 Round Trip Time（RTT）を測定し，RTT がより少ないデータセンターに属する DNS レコードを応答する．主に Inbound 通信の負荷分散で用いられる方法である．注意点として，RTT は各データセンターの SLB から LDNS までの往復遅延を測定していることが挙げられる．クライアントが使用する LDNS が，インターネット内でネットワーク遅延的に近い位置に存在する場合は有効であるが，遠い位置に存在したり，海外で公開されている LDNS を設定していたりするケース等では，このネットワーク近接性による分散は効果が低い．

4.3 DMZネットワークのLayer2延伸

図 1 のように，複数データセンターにおいて専用機型のマルチホーミングを構成する場合，外部 Firewall 配下の DMZ ネットワークを Layer2 ネットワークレベルで共有する（いわゆる Layer2 延伸 Wide Area Network（WAN））必要がある．Layer2 延伸 WAN は，広域 Ethernet などの Layer2 WAN サービスや，自営 Dense Wavelength Division Multiplex（DWDM）網，ダーク・ファイバーなどの利用が考えられるが，データセンター間が地理的に遠い場合や国をまたがるケースではこれらの Layer2 WAN サービスが利用できないこともある．その場合は，IP Virtual Private Network（IP VPN）などの Layer3 WAN サービス上に仮想的な Layer2 VPN を張る L2TP や各種 Ethernet over Multi-Protocol Label Switching（MPLS）技術を用いることで Layer2 延伸が可能となる．ただし，これらの Layer2 VPN 技術はフレームのヘッダー部分が増加する点に注意が必要である．IPv6 は経路上での IP フラグメントに対応していないため，Layer2 延伸ネットワークを通す場合は Maximum Transmission Unit（MTU）サイズに気を付ける必要がある．また,これらの Layer2 VPN 技術は , 他のネットワーク技術よりも難易度が比較的高い傾向があり，企業ネットワーク内での採用事例も少ないため検討の際は注意が必要である．

4.4 メール・サーバーのマルチホーミング対応

専用機を用いたマルチホーミングでは，Web サーバーなどの汎用的な外部公開サーバーは DNS の A レコード（IPv4）や AAAA レコード（IPv6）の応答の切り替えによって負荷分散を実現するが，メール・サーバーは A/AAAA レコードのほかに MX レコードを使用するため注意が必要となる．なぜなら，今回使用している GSLB を含むマルチホーミング専用機では，A/AAAA レコードの負荷分散のみに対応し，MX レコードの負荷分散には対応していない製品が多いためである．

これに対応するため，図 5 のようにマルチホーミング対応するメール・サーバーに対する MX レコードを 1 つとし，A/AAAA レコードを複数持たせる DNS 構成が考えられる．この A/AAAA レコード部分は GSLB による負荷分散機能を実装する．MX レコード部分は，外部 DNS サーバーを別途立てることも可能だが，本論文で

はGSLB上のDNSサーバー機能にDNSゾーンを持たせてMXレコードを登録する方法を採用した．これにより，すべてのDNSゾーン情報の管理をGSLBに統一することが可能となる．

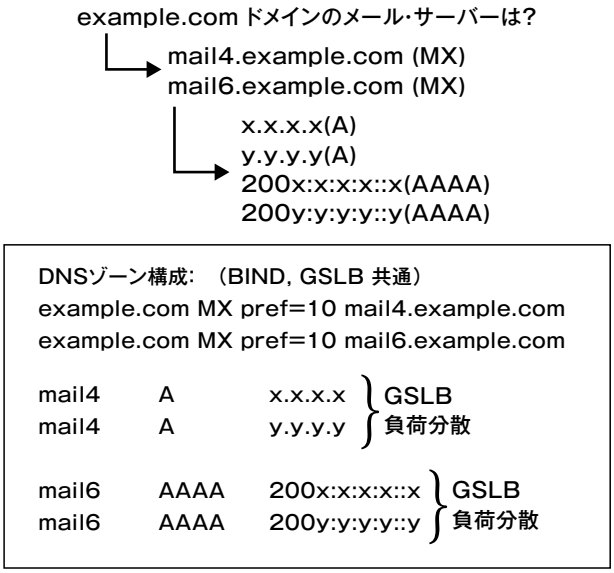


図5. メール･サーバーのマルチホーミングに対応したDNSゾーン設計

5. 考察

マルチホーミングおよびIPv6/IPv4のデュアル・スタックに関するその他のネットワーク設計考慮点を以下に考察する．

(1)ネットワークの可視化

複数データセンターでさまざまなアプリケーション通信を運用する場合，通信経路が複雑になるため，障害時の影響把握やアプリケーション・レスポンス悪化時の原因究明に時間がかかる恐れがある．これらの問題切り分けを迅速に行うための仕組みとして，トラフィック可視化のソリューションを組み合わせることが考えられる．各社さまざまな可視化ソリューションがあるが，ネットワークではNetFlow［13］やsFlow［14］などのフロー可視化技術を実装した製品が豊富に存在する．ネットワーク可視化のソリューションは，それ自体は業務要件的には必要とされないため導入が見送られるケースが多いが，複数データセンターにおけるマルチホーミングなど複雑な通信経路が生じるケースでは，運用要件として含めて検討することが望ましい．

(2)マルチホーミング方式の選択

回線の冗長化とOutbound負荷分散のみを主眼とした要件においてはBGP方式も選択可能である．しかし，さまざまなアプリケーション・サービスを提供するデータセンターでは，前項に述べた「アプリケーション単位での負荷分散」や「アプリケーション応答時間に基づくInbound負荷分散」の要件に柔軟な対応が可能となる専用機型に優位性がある．

(3)マルチホーミングでのIPv6アドレス設計

IPv4/IPv6デュアル・スタックでのマルチホーミングにおけるIPv6アドレス設計について，サーバーに複数のISPから割り当てられたIPv6アドレスをアサインする方法も考えられるが，このIPv6マルチプレフィックスのノードにおいては送信元IPアドレスの選択が一意に定まらない可能性がある．通常，Outbound通信の送信元IPv6アドレスが上位のISPのアドレス・レンジに含まれない場合，ISPでその接続は拒否されてしまう．そのため，マルチホーミング専用機のOutbound負荷分散ルールに合わせて，**表2**に示したポリシー・テーブルの変更などIPv6送信ノードの送信元アドレス選択のルール［12］を設定変更する必要ある．ただし，不特定多数との通信が発生するインターネット環境においては，宛先アドレスを用いた選択ルールの設定はほぼ不可能である．逆

表2. IPv6における送信元および宛先アドレスの選択ルール

送信元アドレス選択ルール

1. 宛先アドレスと同じアドレス
2. 宛先アドレスのスコープにより近いスコープのアドレス
3. DAD状態が「優先（preferred）」のアドレス
4. ホーム･アドレス（Mobile IPv6）
5. 出力インターフェースのアドレス
6. ラベルが同じアドレス（ポリシー･テーブル）
7. パブリック･アドレス
8. 最長一致プレフィックスを持つアドレス

宛先アドレス選択ルール

1. 到達可能なアドレス
2. スコープが一致するアドレス
3. DAD状態が「優先（preferred）」のアドレス
4. ホーム･アドレス（Mobile IPv6）
5. ラベルが同じアドレス（ポリシー･テーブル）
6. 優先順位の高いアドレス（ポリシー･テーブル）
7. トンネル経由ではないアドレス
8. より小さいスコープのアドレス
9. 最長一致プレフィックスを持つアドレス
10. ソート前リストで上位のアドレス

に，本論文のように片側の ISP アドレスのみをアサインし専用機で NAT を行う構成であれば，このようなマルチプレフィックス環境での構成上の課題は解消される．なお，PI アドレスを用いた BGP 構成でも，ISP 側で拒否されないアドレスを用いるためこの問題は発生しない．

(4)マルチホーミング専用機でのIPv6NAT

IPv6 NAT 自体の是非はまだ議論が行われていることは 2 章に述べたが，双方向性を確保した 1 対 1 の IPv6-to-IPv6 NAT として NPTv6［15］も新たに提唱されている．この NPTv6 は，プライベート・アドレスである Unique Local Address（fc00::/7）とグローバル・アドレスを，プレフィックス部分のみを変換することで 1 対 1 のアドレス変換を実現する方式である．本論文の専用機におけるグローバル・アドレス間 IPv6 NAT とは厳密には異なるが，同様に 1 対 1 の NAT を踏襲するように設計することが望ましい．すなわち，NPTv6 に対応している専用機を選択するか，NAT ルールにおいてプレフィックス部のみの変換を行うように設定することで実現が可能となる．

6. おわりに

本論文で述べたマルチホーミング・ネットワーク設計により，事業継続のための複数データセンター構成を求める企業において，インターネット接続部分のネットワークにおいてコスト対効果の高い実装が可能となる．また，IPv4 の枯渇に伴って IPv6 の実装も徐々に増えており，IPv6 の過去の議論や製品の成熟，および今後の IPv6 技術の方向性を意識したネットワーク設計や製品選定が求められる．今後も，IPv6 やマルチホーミングが求められるネットワークにおいて，本論文で述べた設計とその考慮点を踏まえ，さらに発展した要件への検討を進めていきたい．

謝辞

本論文の設計のモデルとなったお客様事例において設計のご協力をいただいた木幡麻由美氏，また IPv6 技術に関して多くのアドバイスをいただいた細川雅也氏，久保田裕司氏に感謝いたします．

参考文献

［1］ JEITA: “IT ユーザトレンド 2010 ならびにクラウドコンピューティングの需要動向調査 ,” 2011 年 6 月
［2］ IDC Japan：“国内インターネットデータセンター市場 2010 年の実績と 2011 年～ 2015 年の予測 ,” 2011 年 8 月
［3］ 社団法人 日本ネットワークインフォメーションセンター http://www.nic.ad.jp/ja/
［4］ “NAT を用いない IPv6 マルチホーミング方式 ,” JPNIC News & Views vol.772【臨時号】, 2010.8.27, http://www.nic.ad.jp/ja/mailmagazine/backnumber/2010/vol772.html
［5］ “IPv6 設計運用に関する Tips,” 2005 年 3 月 IPv6 普及・高度化推進協議会 http://www.v6pc.jp/pdf/060227ja-11-v6trans-tips.pdf
［6］ 奥谷泉：“IPv6 におけるマルチホームの実現に向けて ,” 2006 年 11 月 JPNIC 通信 第 3 回
［7］ “Site Multihoming by IPv6 Intermediation (shim6),” https://datatracker.ietf.org/wg/shim6/
［8］ “Shim6: Level 3 Multihoming Shim Protocol for IPv6,” RFC5533, IETF
［9］ “IPv6 PI アドレスの割り当て開始のお知らせ ,” 2008 年 1 月 JPNIC http://www.nic.ad.jp/ja/topics/2008/20080108-02.html
［10］“IPv6-to-IPv6 Network Address Translation (NAT66) ,” Internet-Draft, IETF http://tools.ietf.org/html/draft-mrw-behave-nat66-02
［11］“IAB Thoughts on IPv6 Network Address Translation,” RFC5902, IETF http://www.ietf.org/rfc/rfc5902.txt
［12］“ますます高機能化するロードバランサーの技術 ,” ASCII.jp x TECH, 2010 年 3 月 29 日 http://ascii.jp/elem/000/000/509/509787/index-2.html
［13］“Cisco Systems NetFlow Services Export Version 9,” RFC3954, IETF http://www.ietf.org/rfc/rfc3954.txt
［14］“InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks,” RFC3176, IETF http://www.ietf.org/rfc/rfc3176.txt
［15］“Default Address Selection for Internet Protocol version 6 (IPv6),” RFC3484, IETF http://www.ietf.org/rfc/rfc3484.txt
［16］“IPv6-to-IPv6 Network Prefix Translation,” RFC6296, IETF http://www.ietf.org/rfc/rfc6296.txt

日本アイ・ビー・エム
システムズ・エンジニアリング株式会社
システム基盤ソリューション
ネットワーク・システムズ
アドバイザリー IT スペシャリスト

都竹 高広 Takahiro Tsuzuku

［プロフィール］
2002年,日本IBMシステムズ・エンジニアリング(ISE)入社.大規模な金融ネットワークの構築業務を経験した後,CiscoやF5等の他社ネットワーク製品を中心に,さまざまな業種のお客様に対するネットワーク提案・構築・運用の技術支援を担当.CCIE #29319.
ttsuzuku@jp.ibm.com