

DNS を利用した PIX 内サーバへのアクセス手法

正岡 元 菊池 豊

高知工科大学 大学院 工学研究科 基盤工学専攻 情報システムコース

概要

地域指向のインターネットトラフィック交換方式に PIX モデルがある。PIX モデルではコンテンツを共有し、PIX 内部からの要求に対して実際にインターネットにアクセスすることなく共有コンテンツを返すことで擬似的にトラフィックを交換する。しかし標準の PIX モデルでは、インターネット上のクライアントから PIX 内部のサーバに向けたトラフィックを交換することができない。

本論文では、DNS を適切に設定することでインターネットと PIX との間においたゲートウェイサーバを用いてリクエストを転送させる手法を開発した。この手法によって複数の PIX 間の接続など、柔軟な PIX の構築が可能となる。

A method for accessing servers in a PIX using DNS

MASAOKA Hajime and KIKUCHI Yutaka

Information Systems Course, Department of Engineering, Graduate School of
Engineering, Kochi University of Technology

Abstract

PIX is a region oriented model for exchanging traffic of the Internet. A PIX makes shares of contents and will respond with them instead of real access to the internet. However standard PIXes can not allow any requests from the Internet.

We propose a DNS composition method to relay DNS queries into a PIX, which enables accesses from the Internet. This paper proposes the technique to forward a request using DNS by utilising the gateway server put between the Internet and a PIX.

1 はじめに

地域指向のインターネットトラフィック交換方式の1つにPIXモデル[2]がある。PIXモデルでは、応用層による擬似的なトラフィック交換を行う。

このモデルではPIX内部のサーバに対してインターネットからアクセスができないという欠点がある。本論文ではこの欠点に対しての解決手法を提案する。この手法によってPIXモデルにおいてPIX内部のサーバをインターネットに向けて公開することが可能となる。

この手法はPIXモデルだけでなく隣接ネットワーク間のみIP到達可能なネットワークが直列に繋がっている場合に、1つ以上のネットワークを経由してその先にあるネットワークへのトラフィックを交換する手法として応用することが可能である。

まず第2章でPIXの基本概念について述べる。第3章でPIXモデルの問題点について述べ、第4章ではその問題を解決するためのDNSの適切な設定について述べる。さらに第5章で一般的なネットワークへの応用について述べ、最後に第6章でまとめを行う。

2 PIXモデルの基本概念

PIX(Pseudo Internet eXchange)モデルの簡単な特徴をここで述べる。

PIXモデルはインターネットのトラフィック交換モデルの1つである。PIXでは地域に閉じたイントラネットを構成し、インターネットとのトラフィックの交換は全てアプリケーション層において行う。

2.1 経路制御

PIXモデルにおける経路制御単位をHAN(Harmonizing Area Network)と呼ぶ。HANは、IPデータグラムの到達可能な範囲であり、1つ以上のLANからなっている。HANの例を図1に示す。この図中の線で囲まれた領域それぞれがIP到達可能な範囲である。

HANとインターネットとは直接IP到達可能ではないが、HANとインターネットの間には両者

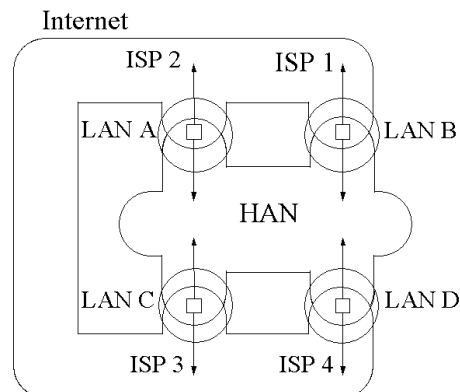


図1: PIXモデルにおけるHANの例

が重なる部分が存在し、その領域をHANボーダと呼ぶ。HANボーダはHANとインターネットとの両方に対してIP到達可能である。PIXモデルを構成する各組織はHANを通して互いに接続される。HANとインターネットとは直接IP到達可能ではないため、インターネットからはPIXモデルを構成している組織がそれぞれISP経由でインターネットに接続されているようにしか見えない。このような構成により、PIXモデル内での経路制御の混乱の影響がPIXモデルの外に伝搬することは無い。

2.2 トラフィックの交換

ここでは、あるプロトコルのトラフィックをPIXモデルによりHANを通して交換する手法について述べる。

特定のプロトコルに対し、各組織のHANボーダが以下のサーバ機能を持つものとする。

- 共有すべき情報を維持することができる。
- クライアントからの要求を受け、それに対し応答を返す。
- 他サーバに要求を転送する。
- 他サーバからの要求を受け、それに対し応答を返す。

一般的に、他サーバに要求を転送する機能を実装するサーバをアプリケーションゲートウェイ(以

下、単にゲートウェイ)と呼ぶ。PIX モデルにおいてこれらのサーバ群は図2のように構成される。このサーバを図3のように連携させることでトラフィックを交換する。この図は組織 X のクライアントが組織 Z のサーバに対して行った要求が PIX モデルにおいて交換される様子を示している。

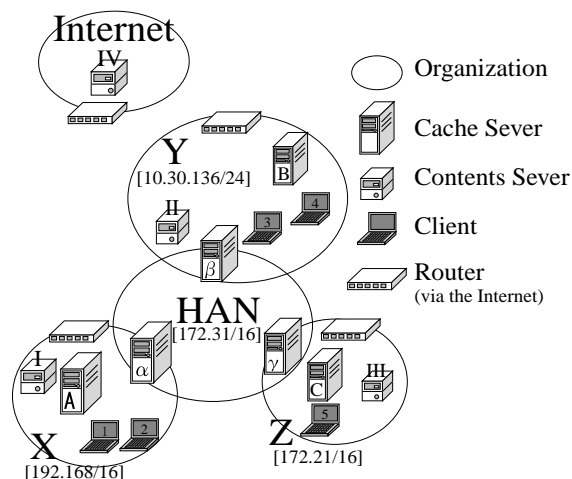


図 2: KPIX における WWW サーバ群の構成

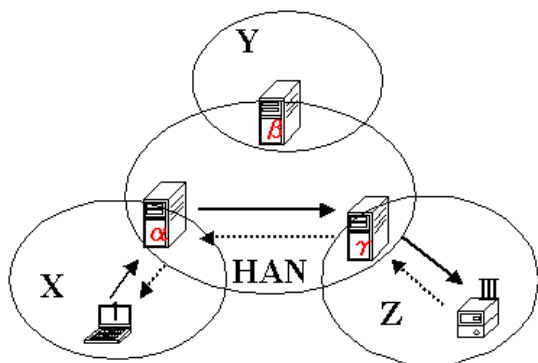


図 3: トラフィックの交換

クライアントからの要求はサーバ α が受け、サーバ β に転送する。サーバ β はサーバ α からの要求を受け、サーバ γ に転送する。サーバ γ は要求に対する応答をサーバ β に対して返す。同様にして応答は転送され、クライアントは要求に対する応答を受け取ることができる。

ここでは各組織内のサーバに対するトラフィックを HAN を通して交換する手法を述べた。サー

バは各組織内だけでなく、HAN ボーダや HAN 内に設置することも可能である。この場合も同様にゲートウェイで要求を転送することによってトラフィックの交換を実現できる。

3 PIX モデルの問題点

PIX モデルでは前章までに述べたように、さまざまなプロトコルのトラフィックを交換することが可能である。しかし、PIX モデルでは交換できないトラフィックも存在する。

本章では、この PIX モデルにおけるトラフィック交換に関する問題点について述べる。

3.1 IP 到達不可能な範囲

今まで述べたトラフィック交換は、PIX モデル内部で完結している場合か、要求が HAN からインターネットに向き、それに対する応答がインターネットから HAN に向いている場合であった。

ここで、インターネットから HAN に向けて要求が来る場合について考える。この場合、サーバが HAN ボーダに存在する場合は特に問題なくインターネットからの要求に応答することが可能である。しかし、サーバが HAN 内にある場合には、インターネットから HAN 内のサーバに向けた要求を交換することはできない。これは第 2.1 節で述べた通り、インターネットから HAN へは IP データグラムが到達不可能であるためである。

3.2 アプリケーションゲートウェイの構成

もう 1 つの理由として、PIX モデルにおけるトラフィック交換は第 2.2 節で述べたようにゲートウェイの連携を必要とすることがあげられる。

たとえば HTTP の場合はブラウザのプロキシ設定によって、ゲートウェイを用いることを指示することが可能である。その他の交換可能なプロトコルも同様にクライアント側で指示できるか、もしくはゲートウェイ側で強制することが可能である。しかし、インターネット側の多数のクライアントに対してはそのような設定を行うことは現実的ではなく、一般的には不可能であるといえる。

4 DNSとの連携

第3.2節では、ゲートウェイをインターネット上のクライアント側に設置することが困難であることを述べた。ここでは、複数のDNSを連携させて構成することでHANボードのゲートウェイにおいてインターネットからHAN内への要求を転送させる手法を述べる。

4.1 DNSの構成

HAN内のサーバをインターネットから名前解決でき、かつそのIPアドレスはインターネットからIP到達可能である必要がある。

これを実現するために、名前空間を以下のように2つ設置する。HANボードはHAN内に属する。

- インターネット向け
- HAN内向け

その上でインターネット向けに、HANボードのゲートウェイのIPアドレスをHAN内のサーバとして広告する。またHAN内向けにHAN内のサーバ自身を広告する。

4.2 リクエストの転送

このようにDNSを構成し、インターネットからHAN内のサーバに対して要求を行う。ここで、サーバ、ゲートウェイのホスト名、IPアドレスは以下の通りとする。

- HAN内のサーバ
www.pix.sample:192.168.100.100
- ゲートウェイ
gw.lan-a.sample

インターネット上のクライアントが、www.pix.sampleというサーバにアクセスを試みる。クライアントはDNSを用いてwww.pix.sampleのIPアドレスを取得する。DNSはインターネット向けにgw.lan-a.sampleを返す。これはHANボードに設置したゲートウェイの名前である。そのため、クライアントはgw.lan-a.sampleに対して要求を行う(図4)。

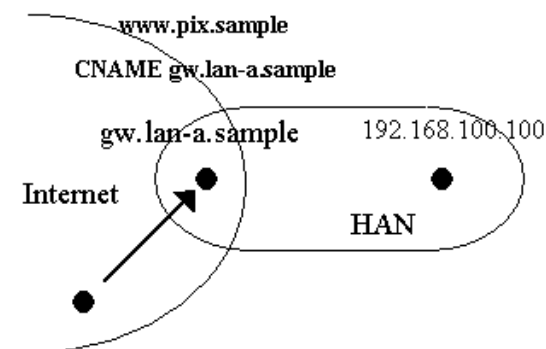


図4: クライアントからゲートウェイへの要求

クライアントからの要求を受けたgw.lan-a.sampleは、www.pix.sampleを名前解決する。DNSはHAN内向けに192.168.100.100を返す。これはHAN内のサーバである。HANボードからHAN内へはIP到達可能であるため、ゲートウェイはHAN内サーバに対して要求を行う(図5)。

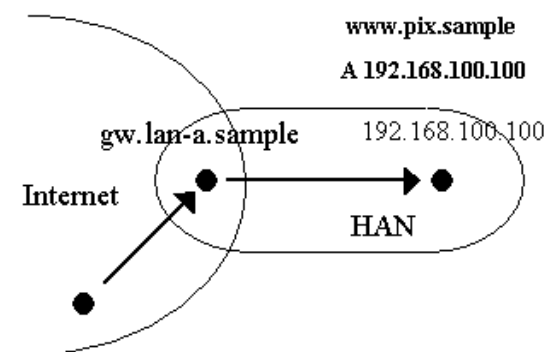


図5: ゲートウェイからHAN内サーバへの要求

その後ゲートウェイは、HAN内サーバより得た結果をクライアントに渡す。

このように、DNSの構成を工夫し、適切に設定されたゲートウェイを組み合わせることでインターネットからHAN内へのトラフィックを交換することが可能となった。

5 HANボードが複数ある場合の応用

本章では、HANボードが複数ある場合における第4章で述べた手法の応用について述べる。

5.1 DNSによる負荷分散

第4章で述べた構成に加え、PIXに接続する他の組織のHANボーダにもゲートウェイを設置できたならば、図6のように、さらにインターネット向けにwww.pix.sampleとしてgw.lan-b.sampleを広告することでDNSのラウンドロビン機能による負荷分散[1]を期待できる。

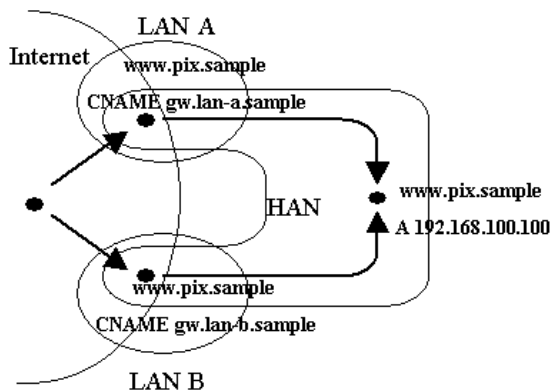


図 6: DNSによる負荷分散

5.2 HANの入れ子

このPIXモデルにおいて、入れ子構造を導入すること、すなわちHANの奥に独立したHANを構成することは容易である。第4.1節をもとにDNSを構成し、第図のようにインターネットから入れ子の奥のHAN内のサーバに対して要求を転送することができる。

5.3 直列に接続されたLAN

PIXを広域に拡大した場合や近隣のPIXが相互に接続した場合など、複数のLANが数珠繋ぎに接続される状況が想定される。このモデルをCLAN-(Cascaded LAN)と呼ぶ。このCLANにおいて、トラフィックを交換する手法を示す。

5.3.1 DNSの構成

それぞれのLANはHANと同等の性質を持ち、隣接するLANとはIP到達可能ではない。また、

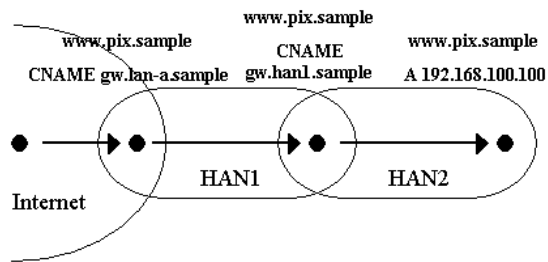


図 7: 入れ子の内側のHAN内サーバへの要求

それぞれのLANの境界には重なった領域があり、両側のLANに対してIP到達可能である。この条件下のCLANにおいてDNSの設定を工夫し、またゲートウェイを用いて、あるLANから直接IP到達可能でない他のLANへの要求を転送する手法を示す。

CLANにおいても、各LANに対応して名前空間を複数用意する。ここで示すネットワークは図8のように3つのLANが直列に接続されており、それぞれのLANをX, Y, Zと呼ぶ。CLANでは名前空間は以下のようにわかる。

- 各LAN向け
- 2つのLANの重なる部分向け

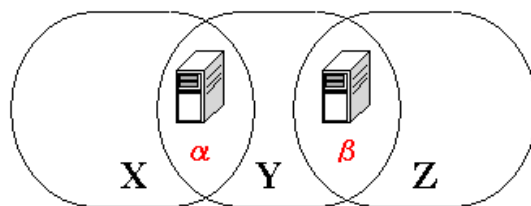


図 8: 直列に接続された複数のLANのモデル

	X	X-Y間	Y	Y-Z間	Z
X	X	X	α	α	β
Y	α	Y	Y	Y	β
Z	α	β	β	Z	Z

表 1: 名前空間ごとのDNSの広告内容

CLANのいずれかの名前空間において、いずれかのLANにあるサーバの名前解決を行うと、ど

のような答えが得られるかを表 1 に示す。縦サーバのある LAN の名前を、横に名前空間をとり、名前解決をして得られる答えを表中に示した。

5.3.2 リクエストの転送

ここでは、X のクライアントから Z のサーバに要求を行う場合について述べる。このネットワーク全体のドメインは clan.sample であり、各 LAN は x, y, z のサブドメインを設定する。LAN どうしの重なる部分は図 8 をもとに alpha, beta のサブドメインを持つ。また、サーバのホスト名は www であり、ゲートウェイのホスト名は gw である。

これらのホスト名を以下にまとめる。

- LAN Z のサーバ
www.z.clan.sample
- LAN X-Y 間のゲートウェイ
gw.alpha.clan.sample
- LAN Y-Z 間のゲートウェイ
gw.beta.clan.sample

X のクライアントは Z のサーバの www.z.clan.sample を名前解決する。その答えとして表 1 により、gw.alpha.clan.sample を得る。この結果、X のクライアントは gw.alpha.clan.sample に要求を行う (図 9)。gw.alpha.clan.sample も同様に名前解決を行い、答えとして gw.beta.clan.sample を得て、要求を行う (図 9)。gw.beta.clan.sample も名前解決を行い、答えとして 192.168.150.100 を得る (図 9)。このアドレスは Z のサーバであるので、gw.beta.clan.sample は結果を得て、gw.alpha.clan.sample に渡す。gw.alpha.clan.sample は受け取った結果をクライアントに渡す。

6 まとめ

地域指向擬似 IX モデルにおいて、HAN 内に設置したサーバにインターネットからアクセスする手法を示した。また、DNS のラウンドロビン機能を用いた負荷分散や、HAN の構造が複雑になった場合の設計について述べた。

さらにこの設計手法を一般化した。すなわち、DNS の構成と適切に設定されたゲートウェイを用

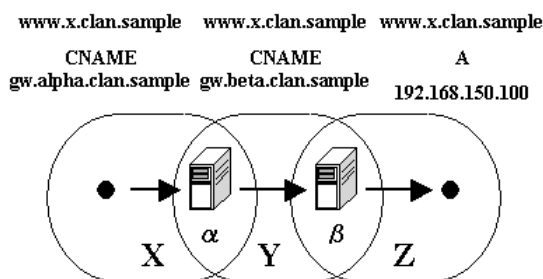


図 9: X のクライアントから Z のサーバへの要求

いて、複数のネットワークが直列に接続されている場合に任意のネットワークのクライアントから任意のネットワークのサーバにアクセスさせる手法を示した。

これらの手法を用いることで、コンテンツサーバの設置場所にとらわれることなくネットワークを構成することができ、より柔軟な PIX の構築を行うことができる。また、複数のネットワークが接続した場合に、ネットワーク層における複雑な経路制御の設定を行うことなく自由にサーバにアクセスすることが可能となる。

謝辞

本実験研究は、通信・放送機構の平成 11 年度地域提案型研究開発制度 (研究開発名「インターネットにおける地域指向型トラフィック交換モデル」と、科学研究費補助金 (課題番号 11450153) との助成を受けています。

参考文献

- [1] 馬場始三, 山口英. DNS を用いた広域負荷分散の実装. 情報処理学会研究報告 98-DSM-9, pp. 37-42. 分散システム運用技術研究会, 1998. ISSN 0919-6072.
- [2] 菊池豊, 菊地時夫. 応用層によるインターネットトラフィック交換モデル. コンピュータソフトウェア, Vol. 16, No. 4, pp. 46-58, July 1999.