

AS 間経路制御監視システムに関する一考察

- マルチエージェントによる AS 間経路監視システム -

上水流 由香[†]

NTT ソフトウェア研究所 広域コンピューティング研究部

概要

インターネットの経路制御上の問題として、経路更新情報が頻繁に送られるような不安定な経路 - 経路フラップ - の問題がある。経路フラップを根本的に解決するためには、異常の発見と原因究明が必要であり、そのためには AS を越える経路の監視 - AS 間経路監視 - が必要である。現在利用可能な監視手法は、詳細情報の欠如、不統一なデータ形式などの問題により、フラップの発見や原因の推測を行うことができない。本論文では、経路フラップの発見や原因の推測を行う、マルチエージェントによる AS 間経路監視システムを提案する。本システムは、経路の変動履歴情報を自律的に収集、解析しフラップの発生を検出する。また必要に応じて複数のエージェントが協力して経路フラップの発生源の推測を行う。

Multi-agent System for Monitoring Inter-AS Routes

Yuka Kamizuru[†]

NTT Software Laboratories, Global Computing Laboratory

Abstract

One of the major problems in the Internet today is route flapping, where a given route rapidly fluctuates between reachable and unreachable. Detailed monitoring and analysis of multiple BGP routing logs is necessary for determining the sources of route flapping. Current monitoring information, however, does not contain sufficient detail and cannot be accessed efficiently. In this paper, a multi-agent inter-AS route monitoring architecture is proposed. In this architecture, Monitor Agents record detailed BGP route information from BGP routers. Operator Agents query multiple Monitoring Agents for specific information to efficiently determine the source and cause of route flapping.

1 はじめに

インターネット全体の経路制御には、AS (Autonomous System) を単位として経路情報を交換する BGP (Border Gateway Protocol)[1] が用いられている。現在この経路制御に関する問題の 1 つに、経路フラップがある [2]。経路フラップとは、同じ経路エントリについて経路更新情報 (announce / withdrawn) が頻繁に送られるような不安定な経路の状態のことで、機器の故障、不安定な IGP (Interior Gateway Protocol) の BGP

への変換、ルータの過負荷による経路情報の取りこぼしなどが原因である。経路フラップにより、大量の経路情報¹を扱うルータでは経路更新処理のため負荷が増大し、またフラップする経路情報にもとづく通信では接続性が低下する。最近経路フラップによるルータの負荷を抑えるために、経路情報を中継する BGP ルータでフラップの多い経路を経路表から削除して、経路全体の変動頻度を抑える Route Flap Dampening Algorithm[3] が用いられている。この方法によりルータの負荷

[†]3-9-11 Midori-cho, Musashino-city, Tokyo JAPAN.
Email:yuka@slab.ntt.co.jp

¹インターネット全体の経路情報 (フルルート) の場合、現在のエントリ数は約 50,000 で、なお増加が続いている。

は削減されるが、フラップの原因となった問題は解決できない。経路フラップを解決するためには、フラップを発見し、原因を明らかにし、それを経路情報の発信元のオペレータに通知することが必要である [4]。そのためには AS を越えた -AS 間の - 経路監視が必要だが、現在利用可能な経路監視手法では、フラップの発見や原因の推測を行うことができない。

本論文では、経路フラップの発見と原因の推測を行うための、マルチエージェントによる AS 間経路監視システムを提案する。本システムは、経路変動情報を自律的に収集、解析しフラップの発生を検出する。また必要に応じて複数のエージェントが協力して、フラップの発生源の推測を行う。以降では、AS 間経路監視の必要性と、既存の AS 間経路監視手法について説明し、問題点を指摘する。次に自律的な経路監視の必要性について述べ、そして我々が提案するマルチエージェントによる AS 間経路監視システムについて説明し、例としてフラップの発生源の推測手順を示す。

2 AS 間経路監視の必要性

BGP による経路制御では、AS を単位として経路情報の交換が行われる。AS はそれぞれが別の管理者や組織によって管理されている場合が多い²。AS 内の経路制御を管理する場合は AS 内で交換される経路情報が対象となるため、同じ管理組織に属する管理者が AS 内ルータの経路情報を参照して作業を行う。一方 AS 間経路制御の場合は、異なる管理組織 (AS) 間を伝わった経路情報により経路制御が行われる。そこで、自 AS から外に向かう経路 (outgoing route) の安定性は、自 AS 内の経路の変動を監視することによって把握できる。しかし他の AS から自 AS に向かう経路 (incoming route) の安定性を把握することは難しい。実際これは、自 AS から他 AS へ伝わった経路情報の状態に依存するが、その情報にアクセスすることができないからである。

例えば図 1 に示すように、AS1 から見た場合に、AS3 や AS2 から AS1 へ向かう incoming route は、AS1 から AS2, AS3 に伝播された経路情報をもとに決まる。もし AS1 から AS2, AS3 へ経路情報が伝播する途中に問題があり経路がフラップしていたとしても、AS1 内から AS2,

AS3 内のルータ R2, R3 のもつ経路の変動状況を知ることができず、経路フラップを検出できない。

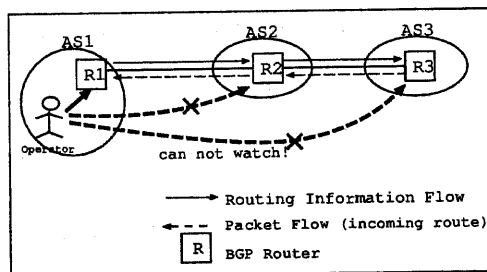


図 1: AS 間の経路情報の伝播と監視

フラップを発見しその発生源や原因を推測するためには、インターネット上の複数地点における経路の変動監視と、フラップしている経路の変動特性の分析が必要である。これは経路フラップの問題に限らず、経路情報が正しく伝播されないといった、経路情報の伝播に関する問題全般の解決に必要となる。

3 既存の AS 間経路監視手法について

ここでは既存の AS 間経路監視手法とその問題点を示す。

3.1 既存の AS 間経路監視手法

最近では以下のような情報公開サーバを利用することで、他の AS における経路の監視がある程度可能である。

- 相互接続ポイントにおける公開 BGP ルータ NAP (Network Access Point) などの相互接続ポイントに設置された BGP ルータで、経路を表示するコマンドが Web のインタフェースを用いて公開されている。これにより、代表的な相互接続ポイントにおける現在の経路の状態が監視可能である。例えば DIGEX の行っている looking glass[5] では、Mae-East, Sprint NAP, Mae-West の各 NAP でこのサービスを行っており、BGP の経路情報や、ダンペン対象となった経路の情報とダンペン対象となる経路フラップ回数の表示、ping、traceroute などのコマンドの実行が可能である³。他に telnet で BGP ルータの一部の

²大規模なネットワークを構成している場合には、1つの組織によるネットワークを複数の AS に分割して管理している場合もある。

³具体的には access-list, bgp, bgp summary, dampened-paths, environmental, flap-statistics, mroute summary, ping, trace を示すコマンドが実行可能である

コマンドを公開しているルータもある [6]。

- **IPMA (Internet Performance Measurement and Analysis) [7]** による統計情報

IPMA では NAP や RS (Route Server) における経路制御に関する以下のような統計情報を Web を用いて公開している。

- ASExplorer
NAP にある RS の BGP ピアを設定している AS に関して、AS 間接続のトポロジや経路の不安定性を視覚的に表示する。
- Internet Routing Table Statistics
各 NAP における 1 日 1 回の経路表全体のダンプ情報。
- Route Flap Statistics Generator
RS と BGP ピアを設定している BGP ルータにおける経路更新回数 (BGP の announce, withdrawn を受け取った回数) の統計情報。

3.2 既存の経路監視手法の問題

以上のような手法によって、他 AS からの経路の監視はある程度可能である。しかしこれらの方法には、以下のような問題がある。

- **スケーラビリティの問題**
公開ルータは、インターネット上の多くの AS から問い合わせを受ける。公開ルータの方法では、問い合わせを受けるたびにルータでコマンドを実行するため、多くの問い合わせが集中するとルータが過負荷になる⁴。
- **経路変動履歴の欠如**
経路フラップの発見や原因推測のためには、経路の変動履歴 (いつ、どの経路が変動したか。また、どのような属性に変動したか) が必要である。公開ルータによる方法や、統計情報による方法では、経路の詳しい変動履歴が得られない。ルータで BGP の route dampen が設定されている場合には、フラップの発生回数の統計情報が得られるが、経路フラップの発生源や原因を推測するためには不十分である。
- **不統一なデータ形式**
経路フラップの発見や原因推測のためには、

⁴実際、digex の looking glass では、*.jp ドメインからの定期的な問い合わせによる負荷が大きくなったため、一時 *.jp ドメインからのアクセスは拒否されていた。

経路の変動状況の分析が必要である。しかし、Web によって表示された結果では分析などの処理が難しい。また、サーバによって出力形式が異なるため、複数の監視サーバから得られる結果を総合した分析は困難である。

4 マルチエージェントによる経路監視の必要性

前に挙げたような既存の監視手法は、もともと経路フラップの解決のために作られたシステムを用いたものではない。そこで、経路フラップを発見し原因を明らかにするための、AS 間経路監視システムについて検討する。

経路フラップの解決のためには、まず経路フラップの発見が必要である。そのためには、継続的で、かつ多地点での経路の監視と、監視結果の経路発信元へのフィードバックが必要である [4]。そこで、BGP ルータの全ての経路変動履歴を記録するサーバをインターネット上に複数設置し、そのデータを公開する方法を考える。管理者は経路変動履歴サーバのデータを検索して、自 AS を発信元とする経路の変動状況を調べることができる。同じサーバを各 AS に設置することで、異なる AS で観測された変動履歴の比較や分析も可能になる。しかしこの方法では、管理者が複数の監視サーバから履歴データ収集して処理するため、履歴サーバから管理者へ大量のデータが送られるという問題がある。またデータの分析は、データを一ヶ所に集めて集中的に行われる。

大量のデータ転送や、集中処理の問題を解決するためには、それぞれの監視地点における局所的な問題発見と分析が必要である。また、経路変動の特性を分析するためには必要に応じて各観測地点で得られた情報の交換も必要である。AS 間経路監視システムの要件は、以下のようにまとめられる。

- 多地点における経路監視
- 各観測地点における局所的な問題発見と自律的な分析
- 必要に応じたデータの交換と分析

これらを実現するためには、分散的かつ自律的に問題を解決するマルチエージェントによるアプローチが適している。そこで管理者に代わって自律的に問題を発見し原因を推測する、マルチエージェントによる経路監視手法を提案する。エージェントはあらかじめ決められたルールを用いて異常

の発見や分析を行う。インターネット上の各 AS に配置された複数のエージェントは、それぞれが継続的に経路を監視し、自律的に経路フラップなどの異常を検出する。また、必要に応じて情報を交換して、経路フラップの発生源や原因の推測を行う。スケーラビリティの問題については、情報の問い合わせなどにより過負荷にならないようエージェント間で調整を行う。エージェントによる方法で、異常を発見し原因を明らかにするという一連の作業の一部を、自動化することができる。

5 マルチエージェントによる AS 間経路監視システム

AS 間経路監視を行う、マルチエージェントシステムについて説明する。まずエージェントの構成を示し、次に各エージェントの機能を説明し、最後に動作の例を示す。

5.1 エージェントの構成

システムは、BGP ルータで経路の変動を監視する「モニターエージェント (Monitor Agent: MA)」と、MA から経路の異常通知や変動履歴データを受けとり、それを分析して結果を人間に提示する「オペレータエージェント (Operator Agent: OA)」の 2 種類のエージェントから構成される。OA は、ネットワークの管理者に代わって経路フラップなどの問題を発見し、その原因の推測を行う。MA は、監視対象となる BGP ルータの全ての経路の変動を継続的に監視する。エージェントの構成を図 2 に示す。

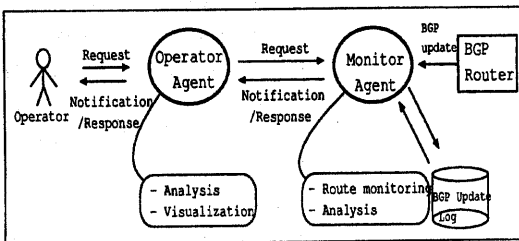


図 2: エージェントの構成

MA はインターネット上の複数の AS に配置され、それぞれが BGP ルータの経路変動を監視する。OA は MA に、特定の経路の異常検出や、変動履歴データの検索を依頼する。OA は MA から異常通知や分析結果などを受けとり、複数の MA から得られる変動履歴データや MA

による分析結果を用いて、原因の推測や分析結果の可視化などを行う。

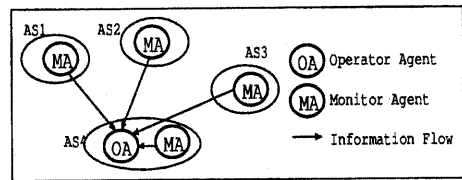


図 3: OA から見た 2 種類のエージェントの関係

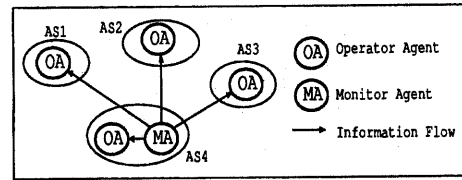


図 4: MA から見た 2 種類のエージェントの関係

図 3 に示すように、OA は複数の MA から情報を受けとることで、インターネット全体への経路情報の伝播状況について把握する。また逆に、図 4 に示すように、MA は依頼された複数の OA へ情報を伝える。

5.2 モニタージェント (MA) の機能

MA は BGP ルータで経路の変動を監視し、OA から依頼された経路の異常検出を行う。MA の主な機能は、(1) 経路の変動監視と変動履歴の記録を行う「監視」、(2) OA からの要求によって履歴データを検索しその結果を返す「データ検索」、(3) 発見した異常を OA に伝える「通知」、(4) 変動履歴データから変動特性などの分析を行う「分析」、(5) 他の MA に情報を中継する「中継」である。

監視機能は、監視対象となる BGP ルータから BGP を用いて経路の更新情報を受けとり、それを経路エン트리ごとのデータベースに記録することで実現する。記録する内容は、現在の経路の状態や属性、変動回数のカウンタ、過去の経路更新の履歴などである。これらの経路変動履歴は、データ検索機能により、経路エントリや AS パスをキーとして検索できる。通知機能は、OA から依頼された経路の変動状況を監視し、経路フラップなどの異常を発見するとそれを OA に伝える機能である。分析機能は、経路フラップの発生源の推測な

どのために観測された経路の変動履歴の分析を行う機能である。MA では BGP ルータで観測される全経路の変動履歴が利用できるため、他の経路と比較するといった分析を行う。MA による、経路フラップの発生源の推測例を後に示す。中継機能は、OA から MA への通信が障害などによって不可能な場合に、情報を中継する機能である。

5.3 オペレータエージェント (OA) の機能

OA はあらかじめ定義されたルールにもとづいて自律的に動作し、経路情報の伝播に関する問題の発見や原因の推測を行う。OA の主な機能は、(1) MA に異常検出を依頼し、異常発生を知り、必要な情報を受け取る「監視依頼」(2) データを分析して問題の原因を推測する「分析」、(3) 関連情報を獲得する「DB アクセス」(4) 人間とのインタラクションを行う「ユーザインタフェース」である。

監視依頼機能は、日常的な経路監視を MA に依頼する場合と、問題が発生した場合にさらに必要な情報を MA に依頼する場合がある。分析機能は、複数の MA から得られた結果を用いてフラップの発生源や原因を推測する機能である。必要に応じて関連する情報を獲得しながら分析を行う。例えば複数の MA から得られるデータを用いて、フラップの発生源の推測を行うことができる。

例として、OA が、route-A の異常検出を依頼している MA の 1 つである MA1 から、route-A の経路フラップ発見の通知を受信したときに起動するルールの例は、以下の通りである。

- if MA1 以外の全ての MA からフラップ発見の通知を受信
then より OA に近い AS の MA に route-A の変動履歴のチェックを依頼
- if 観測を依頼しているそのどの MA からもフラップ発見の通知を受信しなかった
then より遠い AS の MA に route-A の変動履歴のチェックを依頼
- if MA1 から route-A のフラップ発生源の分析結果を受信
then 他の分析結果と比較

そして OA による分析結果と MA から送られた推測結果を総合して、フラップ発生源を推測する。

DB アクセス機能は、IRR (Internet Routing Registries) [8] など関連する情報を必要に応じて

獲得する機能である。ユーザインタフェース機能は、人間からの要求を受けつけ、また分析結果をグラフや図などの形に視覚化して提示する機能である。視覚化の例としては、経路の変動状況のグラフによる表示や、AS 間接続を示す地図上への表示などがある。

5.4 MA、OA に共通な機能

両方のエージェントに共通の機能として、作業履歴 (フラップの検出やデータ分析の結果など) を記録する「作業履歴」がある。作業履歴を用いて、異常発生時の観測データとその原因との関係の学習することができる。

5.5 経路フラップの発生源の推測例

経路フラップの発生源を推測する例を示す。

5.5.1 単一モニタエージェントによるフラップ発生源の推測

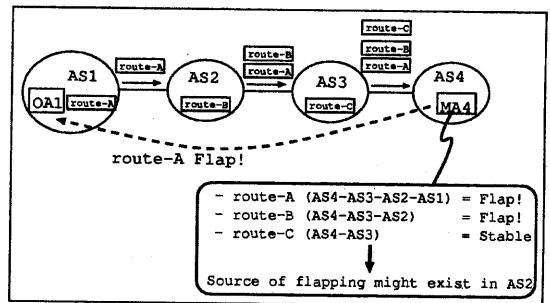


図 5: 単一 MA によるフラップ発生源の推測例

1 つの MA における観測データをもとに、フラップの発生源を推測する例を示す。図 5 に示すように、AS1 を発信元とする route-A と、AS2 を発信元とする route-B と、AS3 を発信元とする route-C の経路情報が、AS4 へ伝播されていたとする。AS1 のオペレータエージェント OA1 は、AS1 を発信元とする route-A の監視を AS4 のモニタエージェント MA4 に依頼する。

MA4 は AS4 における route-A の監視を開始する。すると MA4 で route-A の経路フラップが発見されたとする。MA4 はフラップの発生源を推測するために、route-A の AS パス (AS4 - AS3 - AS2 - AS1) と AS パスが重なる他の経路が変動していないか、もし変動していればその変動周期が route-A と同期していないか分析する。分析の結果、route-B (AS パスが AS4 - AS3 -

AS2) は route-A と同期してフラップし、 route-C (ASパスが AS4 - AS3) はフラップしていなかったとする。この場合、MA4 は、AS2 にフラップの原因があると推測することができる。

ただし、AS を通過する経路と AS を発生源とする経路では、経路情報が通過するルータや回線が異なる場合があるため、仮に AS2 内に原因があったとしても両方の経路情報が同じようにフラップするとは限らない。このような場合には、後に示す複数の MA の観測データを用いた分析結果などの他の手法による分析結果とあわせて、最も確からしい推測結果を示す。

5.5.2 複数モニタエージェントによるフラップ発生源の推測

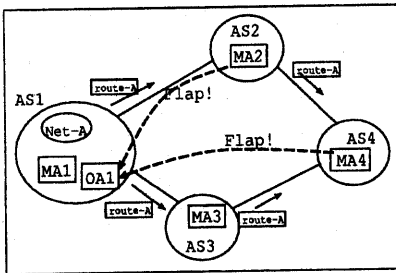


図 6: 複数 MA によるフラップ発生源の推測例

図 6 に示すように、AS1 ~ AS4 それぞれに MA が設置され、AS1 のオペレータエージェントである OA1 が各 AS のモニタエージェントである MA2, MA3, MA4 に自 AS を発信元とする経路情報 route-A の監視を依頼する。

MA2, MA3, MA4 は、OA1 からの依頼を受け route-A の監視を開始する。すると MA2, MA4 が route-A の経路フラップを発見したとする。OA1 は MA2, MA4 から route-A のフラップ発見の通知と、その変動履歴を受け取る。OA1 はフラップ発生源を推測するために、他の MA における route-A の変動状況と比較する。MA3 からは route-A のフラップが通知されない。そこで OA1 は、AS1 → AS2 間、もしくは AS2 が経路フラップの発生源であると推測することができる。

6 おわりに

AS 間経路制御では、経路フラップなど経路情報の伝播に関する問題を解決するために、AS 間経路監視が必要である。本論文では自律的に異常

の発見と原因の推測を行うマルチエージェントによる AS 間経路監視システムを提案した。経路監視システムは、BGP ルータで経路を監視し異常を発見するモニタエージェントと、モニタエージェントに、特定の経路についての異常検出を依頼し、異常が検出されるとモニタエージェントから得られる変動履歴の分析を行うオペレータエージェントから構成される。マルチエージェントによる経路の監視によって、経路フラップの発見やフラップ発生源の推測などが可能になる。現在モニタエージェントの監視機能の一部を実装し、経路変動履歴の蓄積と検索が可能となっている。

今後は、モニタエージェントとオペレータエージェントの機能の詳細化と実装をすすめていく。実際にインターネット上で交換されている BGP の経路情報を用いて、フラップに代表されるような経路情報の伝播に関する問題を発見し、原因を推測する手順の定式化を行っていく。また経路フラップだけでなく、ポリシーに反した経路の検出や、AS パスの変動する経路の検出など、経路情報の伝播に関する問題を解決するシステムとして一般化していく。

謝辞

本研究の機会を与えて頂いた NTT ソフトウェア研究所広域コンピューティング研究部の市川晴久部長ならびに御指導を頂いた村上健一郎グループリーダーに感謝致します。また本研究に対して重要なコメントを頂いた NTT 基礎研究所 菅原俊治主幹研究員ならびに NTT ソフトウェア研究所 明石修氏に感謝致します。

参考文献

- [1] Y. Rekhter, T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC1771, March, 1995.
- [2] Recommendation for Internet Routing, <http://compute.merit.edu/help.html>
- [3] Curtis Villamizar, "Controlling BGP/IDRP Routing Traffic Overhead", ANS, October 1993.
- [4] 上水流由香、村上健一郎、"インターネットルーティングの動的特性に関する一考察", 電子情報通信学会 1996 年ソサエティ大会
- [5] Looking Glass, <http://nitrous.digex.net/>
- [6] telnet://route-server.cerf.net/
- [7] Internet Performance Measurement and Analysis (IPMA), <http://nic.merit.edu/ipma/>
- [8] IRR Registries, <http://www.ra.net/RADB.tools.docs/.databases.html>