4W-08

BGPにおける経路設定ミスの要因分析とその対策手法の提案

近藤 匠 †　　山口 由紀子 ††　　嶋田 創 ††　　高倉 弘喜 ††
† 名古屋大学工学部電気電子情報工学科　　†† 名古屋大学情報基盤センター

1 はじめに

現在、インターネット上の通信はBGPによる経路制御を受けている。これまでに経路制御の障害によるインターネット全体の混乱が複数回発生し、その主要因は1つのAS管理者の経路設定のミスであることが判明している。BGPは各AS管理者が流した経路情報を原則として信用し各ASへの経路を決定しているため、どこかで誤った経路情報が流されると全世界に影響が及ぶことがある。本稿ではそのような障害発生を防止するため、過去に起きた障害から経路設定ミスの要因分析を行い、フィルタリング手法の提案を行う。

2 障害事例

BGPにおける障害は年に数回起きており、決して少ない頻度ではない。また障害からの復旧には長ければ数日に渡ることもある。本節では障害を未然に防ぐための対策手法を提案するために、過去に起きた実例を基に障害の原因を説明する。

2.1 ASパスの長さによる障害

日本時間2009年2月17日1時23分頃、局所的にISP間のBGP接続が切れ通信不能となった。さらに、その影響がインターネット上で伝播し、1時間弱の世界規模の障害となった。本件では、255以上という非常に長いASパスが流されたが、このようなASパスを記憶できない仕様のルータが存在したことが原因であった[1]。

2.2 未定義値の設定による障害

RFCで定義されていない値に対しては実装ごとに異なる例外処理を行っている。そのため、定義されていない値を含むメッセージを受けるとgated由来の実装ではBGP接続を切断したが、他の実装では当該メッセージを破棄して次のメッセージの転送を行ったため、2007年の12月に経路情報の伝播ができなくなった[2]。また、2009年の3月と8月にも、同様な問題で障害が発生した[2]。

2.3 ルータ処理の欠陥による障害

2011年11月8日、BGP UPDATEの処理の欠陥により、Juniper社製ルータのダウンが発生した。本欠陥に対処したOSは同年8月8日に公開されていたが、未更新のルータが各地に存在していたため、障害が発生した[3]。

2.4 経路数の限界による障害

2014年8月12日から数日の間、インターネットのスループットの低下や一部サイトへのアクセスが出来なくなる現象などが発生し、米国や欧州で騒ぎとなった。この問題の要因はBGPのルーティングテーブルが肥大化し、世界規模で通信を行っているルータの一部が処理しきれなくなったことであった[4]。

3 対策手法の提案

さまざまな障害の例のうち、最も深刻なのは経路数の限界による障害である。経路数の増大を防ぐために過去の障害例を参考に経路を取捨選択する対策手法を提案する。

3.1 ASパスに対するフィルタ

ASパスの長さ原因で障害が起きた事例より、ASパスの長さにフィルタをかける。表1はインターネット内におけるASパスの平均の長さを表している[5]。なんらかの理由により、同一ASを何度も経由させて意図的にASパスを長くする場合があり、そのようなものをprependと表記する。なお、Longest AS-Path prepend lengthとは、prependなASパスの中で最長のものを表しており、prependの長さに対してフィルタをかける際の参考にする。これらの情報を元にASパスの長さの閾値を設定し、受け取ったメッセージのASパスのprependの長さとprependを除いた時の長さを調べ、それぞれの長さに対してフィルタをかけることで不適切なメッセージを摘出する。

Implementation of automated evaluation and configuration functions for segmented intra-network design
Takumi KONDO† Yukiko YAMAGUCHI†† Hajime SHIMADA Hiroki TAKAKURA††
†Electrical and Electronic Engineering and Informaition Engineering, Nagoya University
††Information Technology Center, Nagoya University

表 1: AS パス平均長 [5]

Average AS-Path length	4.59
Longest AS-Path length, including prepends	96
Longest AS-Path length, without prepends	12
Longest AS-Path prepend length	92

[2014/12/22 04:00:02]

3.2 不正な値に対するフィルタ

RFC によって定義されていない不正な値が設定されていた場合は、そのメッセージを通してしまうと他のルータで障害が発生する可能性があるのですべて破棄するフィルタをかける。

3.3 更新情報の増減に対するフィルタ

BGP の更新が通常より多い場合、なんらかの障害が発生している可能性が疑われる。従って、過去の BGP 更新の統計情報をもとに、閾値以上の更新が観測された場合は、当該経路において障害が発生していると推定する。表 2 は BGP メッセージの様々な更新情報を表しており、毎秒の BGP 更新のメッセージは平均して 3.34 個送られている [6]。また、BGP メッセージにはプレフィックスの更新情報も含まれており、プレフィックスに関する更新頻度も考慮に入れる。毎秒の BGP 更新の最大値なども参考に閾値を設定しフィルタをかけ評価する。

表 2: BGP の更新頻度 [6]

Average BGP Update Messages per second	3.34
Average Prefix Updates per second	5.44
Peak BGP Update Message Rate per second	3113
Peak Prefix Update Rate per second	2687

[2014/12/31 00:00- 2015/1/6 23:59 (UTC+1000)]

4 実装

図 1 にフィルタの実装評価環境を示す。提案機構はルーティングプロトコル対応のルーティングソフトウェアを動作させている PC(PC ルータ) に対し、ルーティングソフトウェアに渡す BGP メッセージにフィルタをかける形で実装する。ルータとインターネットとの接続点にファイアウォールを設置する。ファイアウォールは不正 BGP メッセージ送信 PC による BGP メッセージとインターネットから受信する BGP メッセージを統合させて PC ルータへ送信するとともに、不正 BGP メッセージがインターネットに流出することを防止する。

PC ルータ内のフィルタは受け取った BGP 更新情報を閾値をもとにフィルタリングし、正常なメッセージはルーティングソフトウェアに送り、不正と検出されたメッセージは隔離して記録する。

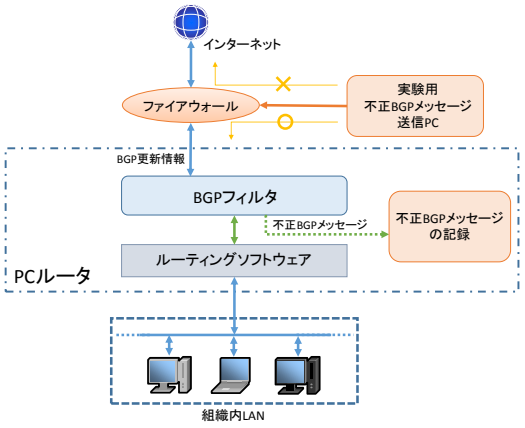

図 1: フィルタの実装予定図

5 おわりに

BGP の不正なメッセージに対するフィルタリング手法を提案した。BGP の障害例と統計情報を基にフィルタ機能実装後、実環境での運用を行い、新しく発生した障害に対しても正しくフィルタリング出来るかを評価して細かなパラメータを調整を行う。

参考文献

[1] あきみち, ”2009 年 2 月 17 日 世界的インターネット経路障害解説”, http://www.geekpage.jp/blog/?id=2009/2/20/2, (2015/01/07)

[2] あきみち・空閑洋平 (2011), 「インターネットのカタチもろさが織り成す粘り強い世界」, P44, 株式会社 オーム社

[3] ”Juniper の BGP バグにより大規模障害発生”, https://www.grep.co.jp/news/index.php?page=article&storyid=458, (2015/01/07)

[4] ”米国全土でインターネットサービスの途絶が発生–BGP ルーティングテーブルの巨大化で”, http://japan.zdnet.com/article/35052352/, (2015/01/07)

[5] ”BGP/ASN Analysis Report”, http://www.cymru.com/BGP/summary.html, (2015/01/07)

[6] ”BGP Routing Table Analysis Reports”, http://bgpupdates.potaroo.net/instability/bgpupd.html, (2015/01/07)