C-07

経路ハイジャック検知手法としてのプレフィックスによる経路解析

川橋　裕†　　米谷 昭徳†

1. 研究背景

インターネットは AS(Autonomous System)と呼ばれるネットワークが相互接続することで構成されている。

また AS 間の通信経路の制御は BGP(Border Gateway Protocol)が役割を担っている。BGP ではインターネット上にある複数の BGP ルータが経路制御表を伝搬することで正確な通信経路を確立している。

しかし BGP ルータが経路制御表を受け取る時、その経路制御表が本当に正しいかどうかを判定せずに受け取るため、誤った経路が参照されてしまうことがある。この事象は経路ハイジャックと呼ばれる。これによって回線圧迫やデータの誤誘導といった通信障害が発生する。

経路ハイジャックは AS 管理者による設定ミス、もしくは悪意のある第三者の攻撃によって引き起こされる。

2. 従来の経路ハイジャック対策

従来の経路ハイジャック対策として、IRR(Internet Routing Registry)を用いた手法がある[1]。この手法では、あらかじめ IRR に経路制御表を登録しておき、実際に伝搬されている経路制御表と差分がないかを監視する。差分が出れば経路ハイジャックが発生した可能性があることを AS 管理者に通知をおこなうことで、迅速な対処が可能となる。

しかしこの手法は各 AS 管理者の協力関係で成り立っており、この関係を保つためにも IRR に誤った情報を入力してはならないので、より慎重な管理が求められる。そのため AS 管理者に負担がかかることになる。また登録される経路情報が不足しているという問題点もあるためこの手法は経路ハイジャック対策としては不十分である。

別の対策にルータの認証機能を用いた手法がある[2]。電子証明書や公開鍵基盤などを用いて送られてきた経路制御表が正しいかどうかを判定することで経路ハイジャックを未然に防ごうとするものなのだが、認証機能を持つルータはコストがかかることやインターネット全体に技術を普及させることが困難といった問題点がある。

3. 研究目的

２節で述べたように、従来の経路ハイジャック対策にはいくつかの問題点が挙げられる。これらを克服するためには、IRR や認証機能に頼らない経路ハイジャック対策、つまり単一でさらに従来のルータで対策できる手法が求められる。

本研究では新たな経路ハイジャック対策を提案し、その有用性を確認することを目的とする。有用性を確認できれば、提案した手法を用いることで経路ハイジャック対策が手軽になり、インターネット上で普及し、経路ハイジャックによる被害をより小規模に抑えることができると考える。

†和歌山大学

4. 提案手法

はじめ traceroute で通信経路上にある各ルータ IP アドレスを割り出す. 次に BGP ルータにて show ip bgp コマンドを用いてその IP アドレスが属するプレフィッ クスを割り出す. そして取得したプレフィックスをもとに，IANA が管理する IP アドレス管理表からそのプレフィックスをもつ国を割り出す. 取得した情報をもと に通過する国による経路を作成する. この流れを定期的に行い，時間軸による変化を観察する.

5. 検証

今回の検証は，本研究で提案した経路観測手法が経路ハイジャックの予防策として有用であるかを確かめることを目的とする. 検証では，送信元の端末に和歌山大学の BGP ルータを，宛先 IP アドレスはこちらで選択した複数の IP アドレ スを指定し，BGP ルータから traceroute を実行することで，各通信経路を取得する. その通信経路から，プレフィックスによる経路および経由する国による経路を割り出す. この作業を，2 月 2 日から 2 月 8 日の午後 5 時頃におこなった. この検証によって，経由する国の観点からみて遠回りしていると思われる経路や，時間軸の観点でみた変化が著しい経路などの，経路ハイジャックの疑いがある経路を観測することを目的とする.

6. 検証結果と考察

検証した結果、時間軸での観測および通過する国の観点から見た経路において経路ハイジャックの疑いのある経路の検知に成功した。また上記の観測とは別に、BGP の経路表に登録されていないプレフィックスが使われた経路を検知した。それぞれの観測結果について述べていく。

まず 8.8.8.8 の通信経路について、観測期間中にプレフィックスが消失と出現を繰り返すといった、時間軸による変化がいくつも見られた。以下に観測結果の一部を提示する。これは Google が相手先は世界中で利用されているので、回線の負荷分散をするために１つの IP アドレスに対して複数の通信経路を容易しているためだと考える。

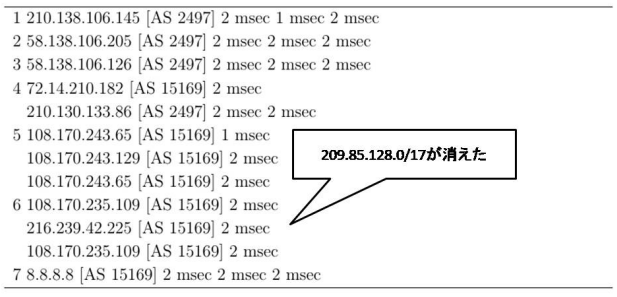

図1 8.8.8.8 までの通信経路

次に 43.225.32.1 の通信経路について経由している国を観測したところ少し気になる結果を得られた(図２)。オーストラリアは地図上では日本の真下に位置しているのに対して、経路上では左方向に通信をたどっていた。ただ左へたどる通信経路は１つの AS 内での経路なのでその AS 管理者が意図して結果のような経路を設定していると思われる。

210.138.0.0/16(日本)
↓
58.138.0.0/17(日本)
↓
103.232.16.0/22(香港)
↓
89.149.128.0/18(ドイツ)
↓
173.205.0.0/18(アメリカ)
↓
103.30.216.0/22(オーストラリア)
↓
43.225.32.0./22(オーストラリア)

図2　43.225.32.1 までの通信経路

続いて、54.39.31.69 までの通信経路について、経路上にて使われていないはずの IP アドレスを検出された(図 3)。これはIPアドレスからプレフィックスを割り出す過程で発見することができた。

```
 1 210.138.106.145 [AS 2497] 1 msec 1 msec 2 msec
 2 58.138.106.245 [AS 2497] 2 msec 2 msec 3 msec
 3 58.138.88.126 [AS 2497] 115 msec 116 msec
   58.138.88.118 [AS 2497] 114 msec
 4 58.138.81.249 [AS 2497] 171 msec
   206.132.169.145 [AS 2497] 169 msec
   206.132.168.113 [AS 2497] 165 msec
 5 206.126.236.35 [AS 2907] 179 msec 176 msec 179 msec
 6 54.239.111.248 [AS 16509] [MPLS: Label 307312 Exp 0] 188 msec 198 msec
   54.239.111.228 [AS 16509] [MPLS: Label 305601 Exp 0] 193 msec
 7 54.239.108.93 [AS 16509] 165 msec
   54.239.109.7 [AS 16509] 163 msec
   54.239.111.55 [AS 16509] 171 msec
```

図3　54.39.31.69 までの通信経路

以上の検証結果により、提案した経路ハイジャック手法は有用性があると考える。

図３。

7. 今後の予定

本研究での経路観測は全て手動で行ったものである。この状態では経路を観測する度にネットワーク管理者は調査に時間を要してしまう。したがって経路観測を自動化する必要があると考える。そのために、経路観測を自動で行うようなサーバを構築することを検討している。

8. 参考

[1]吉田友哉 “IRR を用いた次世代 BGP 経路制御アーキテクチャーの提案“ 電子情報通信学会技術研究報告

[2]岡田雅之，勝野恭治，金岡晃，岡本栄司 “インターネットにおける経路ハイジャック対策手法の調査 “ 情報処理学会研究報告コンピュータセキュリティ