BGPのMis-Originationの原因となる経路情報の検知技術の提案

安藤 正仁[1]　岡田 雅之[2]　金岡 晃[1]

概要：現在、インターネットの Border Gateway Protocol（BGP）の運用には、他のオペレータの設定ミスによってネットワークのプレフィックスが乗っ取られてしまう Mis-Origination という重要な問題がある。インターネット初期には大規模動画サイトへのアクセスが遮断された事例など、発生事例は多数にわたり確認されている。本論文では、RIPE や Route views によって公開されている BGP 経路情報を用いて解析することで Mis-Origination の可能性のある経路情報を検知できる技術を提案し、検知した情報を分析して Mis-Origination の傾向の基礎的な考察を行った。

キーワード：Border Gateway Protocol（BGP）, Mis-Origination, Origin Validation（OV）, Autonomous System（AS）, Internet Routing Registry（IRR）, Resource Public Key Infrastructure （RPKI）

Masahito Ando[1]　Masayuki Okada[2]　Akira Kanaoka[1]

1. はじめに

社会生活に必要な通信基盤として重要性が増大しているインターネットは、現在においても自律・分散・協調を基本的な考えとし、相互信頼の前提の上に成り立っている。インターネットに関係するセキュリティは多方面において議論・実装がなされており、技術的な内容に限らず社会的な側面も含めて様々な提案が行われている。

このような議論の中で、インターネットの通信の根本となるパケットの宛先制御である経路制御の安全性については具体的な導入が進んでいない状況であり、相互信頼を前提とする経路制御では、悪意のある無しに関わらず IP アドレスの乗っ取りである Mis-Origination がたびたび発生している。Mis-Origination は従来より経路ハイジャックと呼ばれていた行為・事象を、実際には悪意を持って行われる事例は少ないといった観点から、より事実に即した表現として近年用いられている。

有名な Mis-Origination 事例は複数あるが、インターネット初期の事例としては AS7007 に関する事例**?**や特定の大規模動画サイトへのアクセスが遮断された事例**?**など、発生事例は多数にわたりその防御手段についても複数が検討されてきた。最近では Mis-Origination を悪用し偽りのサイトの関係者を誘導し利益を奪取するといった行為も行われており、経路制御の安全確保は重要な課題となっている。

Mis-Origination を完全に防ぐためには全てのインターネットを構成する機材において、正しい IP アドレスの保持者が主張する経路情報のみを信頼し、それ以外の経路情報を破棄するといった構成が必要である。しかし、このような経路の正当性確認である OriginValidation(OV) を導入する組織と機材は非常に少ないのが現状となっている。OV の導入には、正しい IP アドレスの保持者を特定する仕組みが合わせて必要とされるが、これまでその様な仕組みを実現する台帳は存在しても実際の情報の信頼性が低いため、インターネット全体への OV の導入は進んでいない。2009 年から IP アドレス管理構造に即した PKI (Public Key Infrastructure) である RPKI (Resource PKI) の整備が RIR (Regional Internet Registry) で進むと、電子証明書を利用した正しい IP アドレス保持者を識別する情報を RPKI の活用で共有する ROA (Route Origin Authorization) の仕組みが考案されテストが現在も継続している。

OV の導入状況や OV 採用による影響に関しては、複数から分析が行われている**?**。OV の導入により Mis-Origination

[1] 東邦大学
Toho University
[2] 一般社団法人 日本ネットワークインフォメーション
Japan Network Information Center

の予防については一定の効果が定量的に見込めるようになってきた。また、Mis-Origination の観測についても国内外のさまざまな組織にて行われており、一定の頻度で発生していることが知られている。しかし、観測が一部分にとどまるものや、観測対象が登録制であるものなど、毎日起こりうる Mis-Origination がインターネット全体の中でどれだけ発生しているかはまだ把握が難しく、さまざまなアプローチで観測に臨むことが重要である。

そこで本研究では、Mis-Origination の検知手法として、毎日得られるの経路情報から Origin-AS の変更を抽出し、その変更における Mis-Origination の可能性を IRR 登録の有無により分析する手法を提案する。提案手法により、定期的な経路の Origin-AS 変更を抽出でき、Mis-Origination 疑いのあるルート情報の検知だけではなく、正しいオペレーションの中での Origin-AS の変更状況なども観測できる。

提案検知システムを提案し、プロトタイプ実装を行い、フルルート情報とルートの更新情報を得て試験的に運用させた結果、Mis-Origination 疑いのある経路情報と、正しいオペレーションならが Origin-AS の変更が高い頻度で起きていることなどの情報を得た。

2. 研究背景

2.1 BGP

BGP はインターネットの通信に使用される経路制御プロトコルである。BGP は AS 単位で経路交換をし、インターネット全体での宛先解決には必要なプロトコルである。AS は共通のポリシーや同じ管理下で運用されているネットワークの集合体を意味する。AS には識別するための AS 番号が割り当てられており、BGP による経路制御はこの AS 番号を用いて経路制御が行われます。AS 番号は地域インターネットレジストリ（RIR）によって、ISP（Internet Service Provider）やコンテンツプロバイダに割り当てられている。

2.2 Mis-Origination

インターネットにおける経路情報の交換は Border Gateway Protocol (BGP) に基づいて行われている。BGP はルータが受け取る経路情報の正しさの検証を行わないため、設定ミス等で誤った経路情報が送信された場合でも、判別を行わず受信しその内容にしたがったパケット転送を行う。こういった誤った経路情報は Mis-Origination と呼ばれている。

Mis-Origination が発生した場合、一部の AS は間違った BGP の広告を受信し、不正な経路情報を他の AS に渡したり、トラフィック自体を受信したりしてしまう。この状況の例を図 2 は Mis-Origination とその影響の例を示す。この例では、AS666 が経路情報を不正に広告した場合であり、本来の所有者である AS1 にトラフィックが流れなくなる。この例では、AS 666 が不正な経路情報を広告し、IP アドレスの所有者である AS1 はトラフィックを受信できない。

いくつかのインシデントは意図的に間違った情報を広告し、トラフィックが自身の AS を通過するようにしている（図 3）。この例では、AS666 を介して経路情報を広告している。最後には IP アドレスの所有者はトラフィックを受信する。何の問題もないように見える状況であるが、AS666 は AS1 へのトラフィック情報を不正に得ることができる。これは中間者攻撃 (Man-in-the-Middle) と呼ばれる問題である。

Mis-Origination は設定ミスや故意の設定により起こる。事例としては 1997 年の AS 7007 の事例や、2008 年の YouTube の事例**?**、最近では 2015 年 11 月のインドの事例**?**などがある。

2.3 Origin Validation

Origin Validation (OV) はインターネット経路制御の中では、経路フィルタリングといった形で継続して用いられてきた。BGP Update ごとに経路の有効性を検証する仕組みが提唱される以前と以後では背景が異なっており、このような仕組みが提唱される以前では、BGP ピアごとに受け入れる経路を IP アドレス単位で手動設定することがほぼ唯一の OV 手段となっていた。この手動経路フィルタによる、OV は人が BGP ピアを認識し、そのピアから広報されるはずの経路の許可リストを BGP ルータへ設定する仕組みとなっている。経路フィルタは現在でも有効でインターネット経路制御の中で必須項目と言われる反面、手動による運用ミスや、そもそも手動であることの運用コストから導入が敬遠される場合があり、そのような設定の穴からインターネット全体へ不正経路が伝播し、結果として定期的に経路のインシデントが発生しているのが現状である。

2004 年ごろから、BGP の経路制御セキュリティが提唱し始められ、IETF の Secure InterDomain Routing (SIDR) ワーキンググループにて標準化が進み**?**、2009 年ごろからは有志で OV の自動化実験が国内でも開始された。手動フィルタリングの時代では、フィルタを生成する生成基は接続相手先とのメールによる情報交換であったり、限定的ではあるが IP アドレスと AS の組み合わせを登録、参照する Internet Routing Registry (IRR) が活用されていた。しかしながら、IRR は登録者は正しい情報を登録するという性善説の前提に立っており、悪意を持った情報を拒否する仕組みなども無く、経路フィルタの参考情報として人が参照し、異常な情報は都度運用者が判断する中途半端なデータベースとなっている。

Origin Validation を自動化するためには IRR のような DB を基に、あいまいな情報から人が判断する必要なく、IP アドレス保持者が真に期待する Origin AS 番号を参照す

t

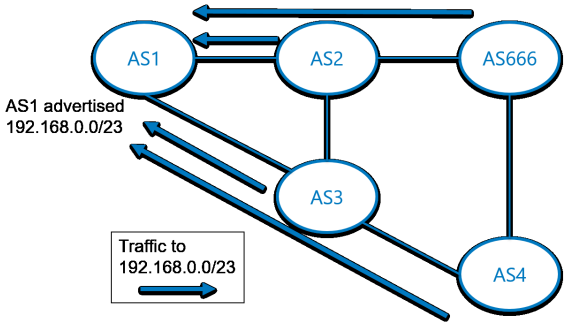

図 1　正常

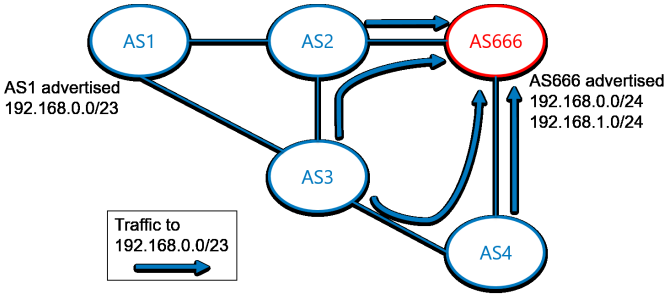

図 2　Mis-Origination

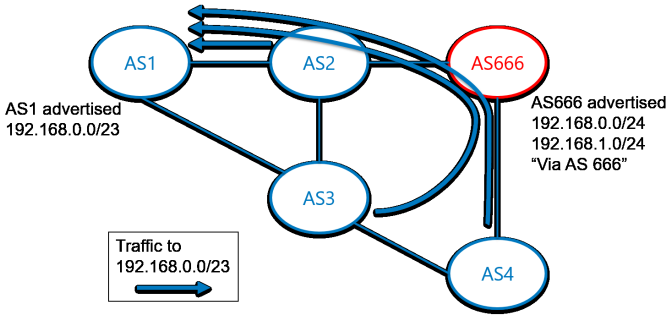

図 3　Man-in-the-Middle

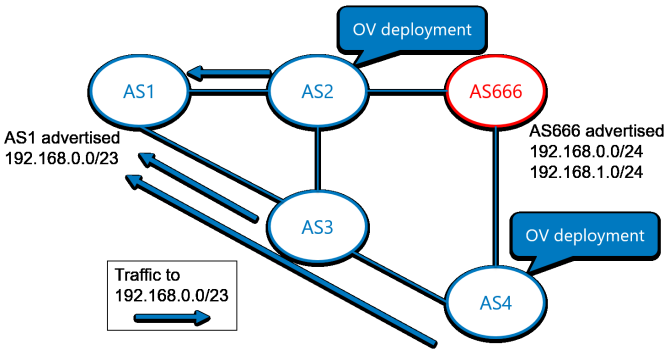

図 4　Origin Validation

図 5　Mis-Origination などの状況例

る仕組みが必要であり、この仕組みとして Resource PKI (RPKI)/Route Origin Authorization (ROA) が整備されてきた?。RPKI は IANA を頂点とする IP アドレス管理階層に沿った PKI であり、IP アドレスレジストリは IP アドレスの割り振り情報を基に PKI の仕組みを活用し、ある IP アドレスの Origin AS 番号に電子署名をすることで IP アドレスと AS 番号の組み合わせである ROA を検証可能とした。このような、仕組みが整ったことで、ルータによる OV 自動化を実際にやってみようという活動が活発化され、RPKI の活用ツールも複数提供される用になってきた?。

OV の効果については、Iamartino らが考察を行っている?。しかし、そこでは定性的であった。2017 年になり、Gilad ら?や安藤ら?らが定量的な分析を行い、その効果が定量的に示されるようになってきた。

2.4　既存の Mis-Origination 検出・通知システム

国内外において Mis-Origination を検出・通知してくれるシステムがいくつか存在する?。例えば、国内においては JPNIC が提供している「経路奉行」というシステムがあり、日本国内において異常な経路情報が発生した場合に検出して通知する機能がある。国外では BGPmon というシステムがあり、ネットワーク監視や異常通知する機能がある。また、この BGPmon は RPKI モニタリング機能があり、ROA 検証をすることができる唯一のシステムである。

2.5　本研究の目的

本研究は Mis-Origination の発生件数や傾向などの情報を分析して考察することを目的とする。2.2 にて述べた通り、Mis-Origination は一定の頻度で発生し、様々な組織によって観測されている。しかし、YouTube の事例やインドの事例のように、影響範囲が大きいインシデントでないと大々的な情報として扱われず、影響範囲が小さい Mis-Origination 発生情報までは大々的に扱われない。既存のシステムらでは経路情報の事前登録や有償版を導入することでそれらの情報が得られるが、ネットワーク管理者でないと登録ができなかったり、システムの仕様が細部までどのような構成になっているのかわからないため、私たちの観測したい情報が得られないかもしれない。そこで、私たちは自らの Mis-Origintaion の検知するための手法を提案し、検知システムを作成して Mis-Origination を検知し、その情報を分析することで Mis-Origination の発生件数や傾向などの情報を明らかにすることにした。

また、対策技術として Origin Validation が存在しているにも関わらず、導入している組織などが少ないのが現状であるが、Mis-Origination の発生状況や件数を分析することで Origin Vadalition を導入することの必要性などについて考察できるだろう。

3.　Mis-Origination 検知手法

検知手法概要としては異なる時間帯の経路情報を二つ用いて、解析していくことで Mis-Origination の可能性があ

る経路情報を検知するといった手法となっている。この検知手法 6 の具体的な処理内容について説明していく。検知システムを作成するにあたって使用したプログラミング言語は Python3 系である。

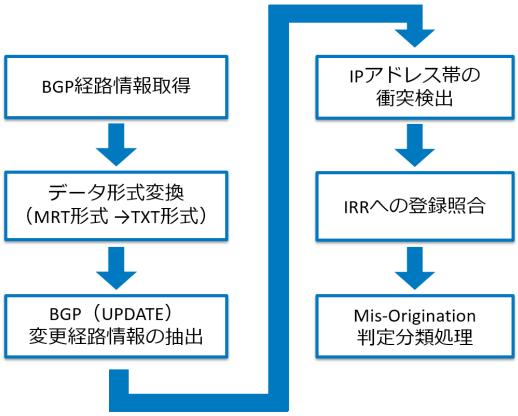

図 6 Mis-Origination 検知手法の全体概要

3.1 BGP 経路情報取得処理

まず、解析するにあたって経路情報を取得する必要があるので、異なる時間帯の経路情報を二つ取得する。BGP の経路情報は RIPE NCC?やオレゴン大学の Route View Project?によってアーカイブが公開されており、本研究では RIPE NCC が公開しているものをクローリングをすることで経路情報を取得した。また、公開されている経路情報には 2 種類あり一つはフルルートの経路情報、もう一つは BGP の UPDATE 経路情報となっている。RIPE NCC の場合、フルルートは毎日 8 時間毎の 3 回分、UPDATE は毎日 5 分毎の経路情報がアーカイブとして公開されている。

この用いる経路情報によって 2 種類の解析工程がある。まず 1 種類としてはフルルートの経路情報を二つ用いる解析工程である。そしてもう 1 種類はフルルートの経路情報をひとつと BGP の UPDATE 経路情報を用いる解析工程である。前者は 6 通りの流れで処理を行っていくが、後者の場合には 3.3 の工程が必要なくなる。

3.2 データ形式変換処理

次に、BGP の経路情報は圧縮ファイルカテゴリーのファイルの一つである MRT 形式で扱われており、このままの状態では解析できない。公開されている経路情報も同様な形式であるため、MRT 形式から TXT 形式に変換する処理を、mrtparse?という Python ライブラリを用いて行った。

また、ここの処理では経路情報から解析するために必要な OriginAS 番号と IP アドレス帯のふたつを紐づけたまま抽出をした。私たちの提案する手法では主にこの二つの情報を解析のために用いる。

3.3 BGP 変更経路情報の抽出処理

BGP の経路情報を解析できる状態の TXT 形式に変換した後に、BGP の変更された経路情報を抽出する処理を行った。具体的な抽出方法としては、異なる前後時間帯の経路情報（前時間データと後時間データ）を二つ比較し、後時間データには存在して前時間データには存在しないものを抽出し、前後時間データ両方に同様の経路情報がある場合は変更されていない経路情報として抽出しないような方法とした。存在するしないの判定としては OriginAS 番号と IP アドレス帯が全く同じであれば両方のデータに存在し、そうでない場合には存在しないとした。このようにして変更経路情報を得る処理を実装した。

3.4 IP アドレス帯の衝突検出処理

BGP の変更経路情報を抽出した後に、それらの変更された経路情報で他の経路情報に対して、IP アドレス帯の範囲が衝突しているかを確認し、衝突している経路情報を抽出する処理を行った。具体的な処理としては、先ほどの抽出した BGP の変更経路情報をフルルート内の広告している経路情報すべてと比較し、IP アドレス帯が衝突しているかつ、Mis-Origination の要因となる IP プレフィックスがフルルート内で比較した経路情報より大きい場合の変更経路情報を抽出する処理を IPy?という Python ライブラリを用いて行った。

3.5 IRR への登録照合処理

先ほどの処理によって抽出された経路情報は Mis-Origination の発生源となっている可能性が高いが、正常な経路情報の変更な場合も有り得るため、経路情報を確認する処理を行った。具体的に確認する方法としては、IP アドレスと AS の組み合わせを登録、参照することができる IRR への whois 検索で照合する処理で行った。ここでは照合結果を取得するのみで、Mis-Origination であるかどうか、正常な経路情報の変更であるかの判定は次の処理で行う。

3.6 Mis-Origination 判定分類処理

先ほどの whois 検索による IRR への照合結果を用いて,「IRR への登録あり ＋ AS 番号一致」,「IRR への登録あり ＋ AS 番号相違」,「IRR への登録なし」の 3 種類に分類する。この分類処理によって Mis-Origination である可能性が高い経路情報をより絞り込むことができる。「IRR への登録あり ＋ AS 番号一致」の場合には、正常に変更された経路情報と判定することができる。そして、「IRR への登録あり ＋ AS 番号相違」,「IRR への登録なし」の場合には Mis-Origination の可能性がより高いと判定できる。

4. 評価

4.1 基礎的な分析結果

フルルートの取得とルート更新情報の取得を行い、そこで「IRR への登録アリ＋ AS 番号一致」「IRR への登録あり＋ AS 番号相違」「IRR への登録なし」の 3 種類の検出数を測った。

2017 年 8 月 22 日の情報では、検出総数 167 件のうち、「IRR への登録アリ＋ AS 番号一致」が 67 件（40.12%)、「IRR への登録あり＋ AS 番号相違」が 77 件（46.11%)、「IRR への登録なし」が 23 件 (13.77%) という結果になった。

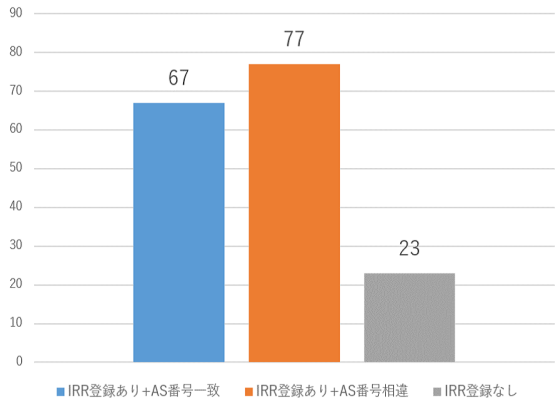

図 7 判定結果概要：2017 年 8 月 22 日

4.2 判定結果を Slack へ投稿する Bot

判定分析システムからの結果を Slack へ投稿する Bot を開発した。これにより、関係者が結果通知をリアルタイムに受け取ることを可能にした。

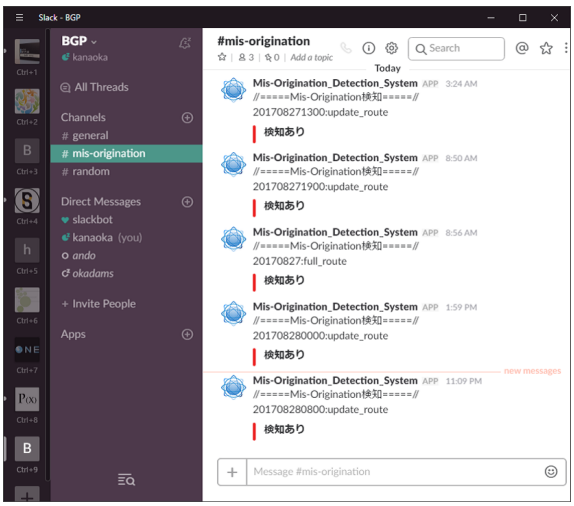

図 8 判定結果投稿 Bot による検知結果通知画面

5. 考察

検知システムについて、いくつか課題や改善点がある。

例えば、検知する情報にリアルタイム性として課題がある。なぜならば、経路情報は静的なデータを用いるかつ、検知手法の処理時間が大きくかかるからである。フルルートを二つ用いて解析検知する方法の場合の処理時間は 16 時間以上かかる。また、フルルートと UPDATE 情報を用いて解析検知する場合には 8 時間以上かかる。今回は Mis-Origination の発生件数や傾向などを分析するためのデータを取得するためであるため、リアルタイム性にそこまで重視していなかったが、本研究の手法を実用的な検知システムとするのであれば処理の高速化などが必要となる。

他には、検知情報が実際のネットワーク状況との整合性があるかどうか課題である。なぜならば、検知に用いている経路情報としては静的なデータあるかつ、アーカイブの保存日時が大きく異なるため、経路情報の更新状態にラグがあるからである。RIPE NCC が公開している経路情報の場合、フルルートは 1 日に 3 回更新（UTC:0 時,8 時,16 時）となっており、フルルートを二つ用いて解析検知する場合の処理には 8 時間のラグによって 3.3 の変更経路情報の抽出に影響があるだろう。

また、3.3 の処理において、現状の処理では、完全新規な経路情報か、元々存在しており変更された経路情報かどうかの違いを判断していない。変更情報として抽出した経路情報の分類ができると、Mis-Origination の分析の要素として用いることができるかもしれない。

3.5 の処理において、照合する際に IRR の登録状況が正しい経路情報として反映されているかどうかによって、最後の 3.6 の処理にも影響が出てしまう。IRR への反映のタイミングや詳細がわかれば調整することは可能であるが、この点を考慮するとより確かな情報を検知できることになるだろう。

6. まとめ

BGP 経路制御は相互信頼に基づきパケットの宛先情報をやり取りしている。2017 年 8 月 25 日にはある組織のオペレーションにより日本のインターネットの接続性が悪化した。とはいえ、自律分散協調のインターネットが継続したことから、数時間程度で回復することで来た。本研究としてはさらなる経路障害の検知、復旧をめざし手法を考えてゆきたい。

7. 参考文献

参考文献

[1] Misel, Stephen. ”Wow, AS7007!.” Merit NANOG Archive, apr 199.7 (1997): 1997-04.
[2] Brown, Martin A. ”Pakistan hijacks youtube.” Renesys

Blog, Feb (2008).
[3] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, Haya Shulman, “Are We There Yet? On RPKI’s Deployment and Security”, 24th Annual Network and Distributed System Security Symposium (NDSS 2017), 2017
[4] M. Ando, M. Okada, A. Kanaoka, “Simulation Study of BGP Origin Validation Effect Against Mis-Origination with Internet Topology”, The 12th Asia Joint Conference on Information Security (AsiaJCIS 2017), 2017
[5] A. Toonk, ”Large scale BGP hijack out of India”, 入手先 ⟨http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/⟩, 2015
[6] Secure Inter-Domain Routing (sidr) 入手先 ⟨https://datatracker.ietf.org/wg/sidr/charter/⟩
[7] Lepinski, M., Kent, S., Kong, D., A Profile for Route Origin Authorizations (ROAs). RFC 6482, IETF
[8] Bush, R., and Austein, R. The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810, IETF.
[9] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and Austein, R. BGP Prefix OV. RFC 6811, 2013.
[10] Bush, R., Austein, R., Patel, K., Gredler, H., and Waehlisch, M. Resource Public Key Infrastructure (RPKI) Router Implementation Report. RFC 7128, IETF, 2014.
[11] RPKI Dashboard,
[12] Wahlisch, M., Holler, F., Schmidt, T. C., and Schiller, J. H. RTRlib: An Open-Source Library in C for RPKI-based Prefix OV. In Proc. of USENIX Security Workshop CSET’13 (Berkeley, 2013), USENIX Assoc.
[13] Matthias Wahlisch, Robert Schmidt, Thomas C. Schmidt, Olaf Maennel, Steve Uhlig, and Gareth Tyson, RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV), 2015
[14] Iamartino, Daniele, Cristel Pelsser, and Randy Bush. ”Measuring bgp route origin registration and validation.” International Conference on Passive and Active Network Measurement. Springer International Publishing, 2015.
[15] 経路奉行入手先 ⟨http://www.nic.ad.jp/ja/ip/irr/jpirrexp.html⟩
[16] BGPMON 入手先 ⟨http://bgpmon.net/⟩
[17] Cyclops 入手先 ⟨http://cyclops.cs.ucla.edu/⟩
[18] RIS Raw Data 入手先 ⟨https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data⟩
[19] University of Oregon Route Views Project 入手先 ⟨http://www.routeviews.org/⟩
[20] mrtparse package in Ubuntu 入手先 ⟨https://launchpad.net/ubuntu/+source/mrtparse⟩
[21] IPy 0.83 : Python Package Index 入手先 ⟨https://pypi.python.org/pypi/IPy/⟩