Computer Security Symposium 2020
26 - 29 October 2020

未割り当てIPアドレスの経路広告の実態調査

五島 健太朗[1,a)]　澁谷 晃[2]　岡田 雅之[3]　内田 真人[1]

概要：インターネット上の経路制御において，いかなるエンドユーザにも割り当てられていないIPアドレスが経路広告されるという問題が知られている．これは，現在のBGPによるインターネットの経路制御の仕組みでは，未割り当てIPアドレスでさえも経路広告が可能であることに起因する．しかし，問題の技術的な原因が明らかな一方で，実態は明らかでなく，調査手法も確立されていない．そこで本研究では，日本国内を対象に未割り当てIPアドレスの経路広告の実態調査を行い，その簡便かつ有効な手法を提案する．提案手法では，日本が割り振りを受けたアドレスプールから未割り当てIPアドレスを抽出し，インターネット上で公開されている経路情報と比較する．検出された経路広告の詳細を追加調査した結果，国内外のASから数年間にわたり未割り当てIPアドレスが経路広告されていたことや，そのいずれもがネットワーク管理者の設定誤りによるものあったことが明らかとなった．以上の問題はレジストリやISP，通信事業者に限らず，一般のエンドユーザにも影響するものであり，本研究が経路広告設定の正当性を保つための注意喚起となることを期待する．

キーワード：経路広告，未割り当てIPアドレス，NIR

Analysis of Route Announcements of Unassigned IP Addresses

Kentaro Goto[1,a)]　Akira Shibuya[2]　Masayuki Okada[3]　Masato Uchida[1]

Abstract: It is known that some of the unassigned IP addresses are announced as legitimate routes, even though they are never assigned to any end-user. The reason for this is that the current routing system of the Internet regulated by BGP allows unassigned IP addresses to be announced as well. On the other hand, actual situation is still unclear and there is no solid method for such an investigation. Thus, we conducted the very first investigation in Japan and proposed a simple and effective method. In our proposed method, we compare the address pool delegated to Japan and the actual route information that is available online. As a result, we have revealed that some unassigned IP addresses had been announced from both within Japan and overseas for several years because of human-setting-error. These problems affect not only registries, ISPs or carriers but also general end-users as well.

Keywords: Route announcement, Unassigned IP address, NIR

1. 序論

BGPはAS単位で経路情報を交換するための標準プロトコルである．経路情報をインターネット上に通知することを「広告」と呼ぶ．経路情報には，通信の宛先となるIPアドレスや，宛先に到達するまでに経由するASパス，複数のパスの優先度など，通信の到達性に関する情報が含まれる．しかし，BGPには経路制御の安全性に関わる機構は十分に備わっておらず，誤って広告された経路情報であっても，場合によっては広範囲のネットワークに伝播し，それが大規模な通信障害の原因となることもある [1], [2].

本研究では，悪意の有無を問わず，このような誤った経路広告を「異常経路広告」と呼ぶ．異常経路広告の中には，

[1] 早稲田大学
Waseda 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センター
Japan Network Information Center
[3] 長崎県立大学
University of Nagasaki
[a)] kentaro.goto@asagi.waseda.jp

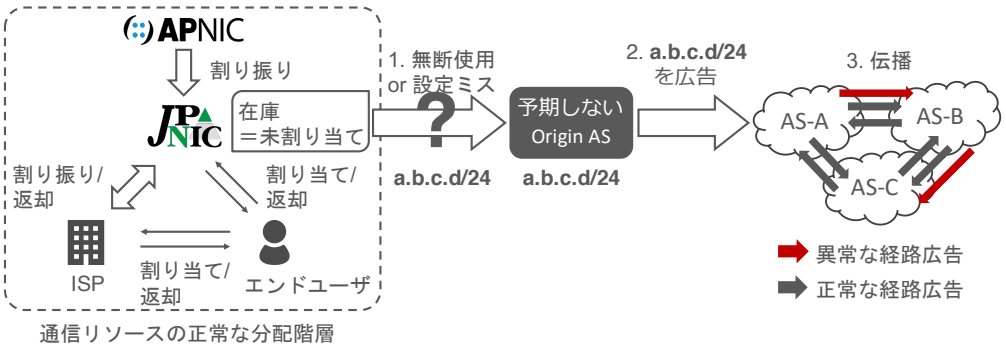

図 1　未割り当て IP アドレスの異常経路広告までの流れ

いかなるエンドユーザにも割り当てられていない未割り当て IP アドレスが経路広告されるものがある．未割り当て IP アドレスが経路情報として使用された場合，大きく 3 つの脅威が生じる．一つ目の脅威は，正常な通信に必要なリソースの一意性が損なわれることである．なお，本稿では IP アドレスや AS 番号といった通信に必要な識別子をまとめて「通信リソース」と呼ぶ．二つ目の脅威は，無秩序に使用され続けられた未割り当て IP アドレスが「汚れた IP アドレス」となり，通信リソースとして空費されてしまうことである [3]．ここで「汚れた IP アドレス」とは，不適切な使用が原因で，実質使用不能の欠番扱いになった IP アドレスを指す．こうした IP アドレスの汚染には，悪性活動に利用されてブラックリストに掲載される場合や，到達可能な経路であるにもかかわらず，無用なトラフィックの増大に関わったとして使用不能にされる場合がある [4]．三つ目の脅威は，未割り当てであるがゆえに，悪意の有無を問わず発見が遅れる傾向にあることである．未割り当て IP アドレスの経路広告には，他者の通信リソースを乗っ取る場合のように直接の被害者が存在しないため，発見に時間がかかる．したがって，通常の IP アドレスよりも長い期間，検出されることなく悪意のある通信が可能となる．

こうした脅威に対処するためには，未割り当て IP アドレスの経路広告についての実態調査が必要である．そこで本研究では，JPNIC の IPv4 アドレス分配に関するレジストリデータと RIPE NCC が世界中の観測地点から集約・公開している経路情報を比較して，未割り当て IPv4 アドレスの異常経路広告を検出する．なお JPNIC は日本国内の IP アドレスを管理する NIR (National Internet Registry) であり，著者らの把握する限り本研究は NIR レベルの分配状況を考慮した初めての調査である．

調査の結果，日本国内の未割り当て IPv4 アドレスについて，国内の AS から 1 件，海外の異なる AS から 2 件の異常経路広告が検出された．検出された経路情報は 3 件とも /24 空間であり，詳細の追加調査によって数年間にわたって広告が継続していたことが判明した．さらに JPNIC よりそれぞれの AS を管理する組織に連絡をとったところ，原因はいずれも管理者の設定ミスであったことが判明し，最終的に停止させるに至った．

本研究の主な貢献は次の 2 点である．

- 任意の組織における IP アドレス分配状況に基づいた未割り当て IP アドレスの経路広告を検出する手法を提案した
- 日本国内で初めてとなる未割り当て IP アドレスに関する異常経路広告の実態調査を行った

本稿の構成は次の通りである．第 2 節で BGP による経路制御と，その正当性を保つための既存の取り組みについて触れる．第 3 節では，本研究の調査手法や着目した点について述べ，第 4 節でその結果を示す．第 5 節では本研究の制約や今後の課題について検討する．第 6 節では関連研究を紹介し，第 7 節で結論を述べる．

2. 異常経路広告を取り巻く現状と課題

2.1 JPNIC が在庫管理する未割り当て IP アドレス

図 1 に，未割り当て IP アドレスの異常経路広告の発生から第三者による観測までの流れを示す．アジア・太平洋地域の RIR (Regional Internet Registry) である APNIC から JPNIC が割り振りを受けた IP アドレスは，さらに国内の ISP やエンドユーザに割り振り/割り当てされる．なお，「割り振り」とはレジストリや ISP に通信リソースが分配されることを指し，「割り当て」とはエンドユーザに通信リソースが分配されることを指す．また，本稿では両者をまとめる場合には単に「分配」と表記する．

JPNIC が割り振りを受けた IP アドレスの中には，ISP やエンドユーザへの分配の対象外となるものや返却されたものなど，JPNIC が在庫として直接管理を続けるものがある．こうした在庫の IP アドレスは未割り当てであり，本来はいかなる経路においても観測されるべきではない．しかし，任意の AS 管理者が未割り当ての IP アドレスの一部を何らかの方法で知り，あるいは人為的ミスによって自身の BGP ルータに設定してしまった場合，その AS 外に位置し，かつ対策 (第 2.3 節参照) が不十分なネットワークでも当該の未割り当て IP アドレスが経路として認識さ

れてしまう．なお「対策が不十分なネットワーク」とは，対策をとっていない，あるいは採用している対策自体が有効でないという意味で「対策が不十分」な状態にあるネットワークを指す．現在主な対策は二通りある．

そのうち一方の IRR はそれ自体の効力が不十分であり，採用していたとしても未割り当て IP アドレスの異常経路広告の完全な防止はできない．もう一方の対策である RPKI は，それ自体の効力は十分であるものの現状では普及率が低いという課題がある．すなわち，(a) 何の対策も講じていないネットワーク (b) IRR は活用しているが RPKI は活用していないネットワークのいずれかである場合は，対策が不十分であるといえる．

なお，2003 年まで NIR は将来の分配のために IPv4 アドレスを保管することが許されていたのに対し，現在の JPNIC では割り当ての都度必要な分の通信リソースを APNIC から割り振られる．すわなち，JPNIC で在庫として保管される未割り当て IP アドレスは，ほとんどが過去に返却されたもの，あるいは 2003 年以前に割り振られたあと一度も割り当てられずにいたものである．

2.2 BGP による経路広告

一般に各ホストを識別するための宛先情報には IP アドレスが用いられる．ただし，全世界のホストの宛先情報を管理するには膨大なメモリが必要となるため，個々のユーザが直接管理することは不可能である．そこで，BGP によって拠点ごとに経路情報をやりとりすることで負荷を分散している．インターネットは AS と呼ばれる経路制御の単位ごとに分割されており，それぞれに識別のための世界で唯一の番号が割り当てられている．BGP は AS 間の経路制御に用いられるプロトコルであり，各 AS は自組織内の IP アドレスや，隣接 AS から受け取った外部の宛先情報を転送するといった経路広告を行う．なお，以下では通信相手が所属する AS を表す AS 番号とホスト自体を識別する IP アドレスの組を単に BGP における宛先情報と呼ぶ．

IP アドレスの分配は，IANA を最上流に RIR，さらに NIR へと割り振られ，最終的に ISP やエンドユーザへ割り当てられる階層構造をとる．ただし各階層がもつ IP アドレスの全てに使用者がいるのではなく，未分配のアドレスが経路として現れるのは原則として起こりえない．JPNIC が管理する IP アドレスのうち，実際の経路情報として出現するのが妥当なものは，JPNIC からさらに下の階層に分配された IP アドレスのみである．しかし，BGP では任意の通信リソースを経路情報として広告設定可能であり，原則として受信した経路情報の正当性の確認も行われないため，経路広告は必ずしも通信リソースの分配状況に即したものにはならない．したがって，悪意の有無によらず，誤った宛先情報であっても隣接 AS に転送されてしまうことがある．

以上を踏まえ，BGP の経路広告は正常な経路広告，異常経路広告，特殊な経路広告の 3 種類に大別できる．正常な経路広告の場合には，当該の宛先情報が実際の分配状況と一致する．一方で異常経路広告の場合には，当該の宛先情報が実際の分配状況と一致せず，悪性の経路広告である可能性がある．ただしそのすべてが悪性であるわけではなく，ネットワーク管理者などによる人為的ミスである場合も存在する．異常経路広告には，すでに存在するホストに割り当てられた IP アドレスを，第三者がその所有を主張して経路広告する spoofing と，いかなるホストにも割り当てられていない未割り当て IP アドレスを経路として広告する場合の二通りがある．その他にも，上記に当てはまらない特殊な経路広告がある．例として DDoS mitigation などの意図的かつ良性の乗っ取りが挙げられる [5]．DDoS mitigation とは，自 AS で処理しきれない大量のトラフィック (DDoS 攻撃) を，一時的に合意の上で他 AS に「乗っ取らせる」ことで攻撃を回避することを指す．DDoS mitigation の際には通常時とは異なる経路広告が発生するが，目的は通信リソースの不正利用ではないため，良性とみなされる．

2.3 経路情報の正当性を保つための取り組み

異常経路広告に対応するため，ルータごとに送受信する経路広告に条件を課すフィルタリングなどが導入されることもあるが，運用の煩雑さやルータ間での一貫性のなさといった課題がある．そこで，複数の BGP ルータが共通で参照できるデータベースの作成や，経路情報の観測と定期的な公開などの対策が提案され，一部で運用されている．

IRR (Internet Routing Registry) はインターネット上の経路に関する情報を登録しておく公開データベースである．IRR の登録情報は誰もが参照可能であり，主として経路広告の正当性の確認やフィルタリング設定の生成を目的として利用される．すなわち，経路制御を担当する運用者が，IRR 上に登録された情報を BGP ルータに設定しておけば，ルータは経路広告を受けとった際にその広告の正当性を確認することができる．実際に日本国内においては JPNIC が運営する JPIRR が稼働している．ただし，RADB などの一部の世界的に主要な IRR へのエントリ登録は任意の通信リソースに対して可能であり，登録時にも正当な管理者・通信リソースであるかを確認する機構は備わっていない．したがって，一度誤った情報が登録されてしまうと，それが更新あるいは削除されない限り，正当な経路として IRR 上に残ることになる．また，IRR は複数存在し，互いをミラーしているものやそうでないものがあるため，登録された情報は一貫性に欠ける場合がある．以上の理由から，IRR の活用だけでは異常経路広告発生の抑止には限界がある．

RPKI (Resource Public-Key Infrastructure) は，IP アドレスや AS 番号といった アドレス資源の分配の正当性を

証明するための公開鍵基盤である．すなわち，ルータが受け取った経路広告に記載の通信リソースが，実際に経路広告に記載された管理者に割り当てられたものであるかを確認可能であるという点において，IRR とは異なる．RPKI では，通信リソースの分配を行ったレジストリが，当該通信リソースに対して「リソース証明書」を発行し，経路情報の認証に用いるという仕組みをとる．したがって，認証結果はインターネットレジストリの階層構造に即したものになることが保証されており，理論的には未割り当ての異常経路広告にも対処可能である．しかし広く一般に普及する段階には至っておらず，現時点の RPKI では異常経路広告の対策として十分ではない．

以上より，IRR と RPKI の両方が存在していても，実際には異常経路広告の発生を防ぎきれていないという現状につながっている．本研究では，こうした現状の対策が講じられているうえで取りこぼされている異常経路広告のうち，未割り当て IP アドレスが関わるものに着目した実態調査を行う．

3. 調査手法

本研究の提案手法では，調査対象の組織が割り振りを受けた IP アドレスのリストと，実際に観測される経路広告を比較することで異常経路広告を検出する．本研究と類似の調査では，NIR の上位組織である RIR がもつ IP アドレス分配データを用いた例がある [6], [7]．こうした調査は，RIR から先に分配されていない通信リソースもまた，経路情報中に表れるべきではないという点については本研究の場合と共通する．しかし RIR からの分配の段階に関するデータでは，ISP などの下位組織に割り振られたもののエンドユーザには割り当てられていない通信リソースについては把握できないという課題がある．そこで本研究では NIR レベルでの分配に焦点をあて，経路情報中に表れる未割り当て IPv4 アドレスが関わる異常経路広告を検出し，その実態を調査することを目的とする．

3.1 使用するデータ

今回の調査対象は日本国内の通信リソースであるため，日本のユーザによる使用を目的として JPNIC が APNIC より割り振りを受けた IP アドレスのリストを使用した．一方，実際の経路情報については，RIPE NCC がインターネット上で公開している RIPE RIS[*1] に掲載の経路広告データのうち，日本国内の観測拠点から提供されているもの[*2] を使用した．表 1 に使用したデータの規模について示す．また，検出された未割り当て IP アドレスの異常経路

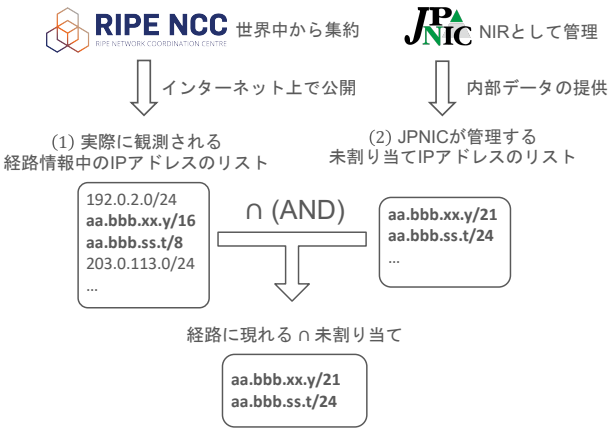

図 2 提案手法の概観

広告の詳細について追加調査する際には，RIPE NCC が運用する RIPEstat[*3] を利用した．RIPEstat 上で任意の IP アドレスやそのプレフィクス，AS 番号などの通信リソースを検索すると，その通信リソースに関する whois の情報や経路上での観測状況などが一覧で表示される．

表 1 調査に使用したデータの詳細

概要	規模 (/24 換算)	規模 (行数)
経路情報	15,341,353	約 800,000
未割り当て IP アドレス一覧	14,497	非公開

3.2 調査手順

本研究では，以下に示すように二種類のデータを取得し，それらの共通部分をとる簡便な手段によって異常な経路広告を検出した．

経路情報の取得

公開されている経路情報には二種類あり，その観測結果を収集した時点での全経路広告を表すフルルートと，一定時間ごとの差分のみを表すアップデートにわかれる．本研究では RIPE RIS より MRT (バイナリ) 形式のフルルートデータをダウンロードして使用する．フルルートは毎日 00:00，08:00，16:00 時点のものがアップロードされるが，更新時間が一定であるとは限らず，かつタイムゾーンが不明なため，データの収集の際には 2 日前時点のものを自動取得した．続いてダウンロードしたデータをテキスト形式に変換するため，bgpdump を使用した．最後に得られたテキスト形式のデータより，IP アドレス空間の記述部分を抽出して経路情報を取得した．

未割り当て IP アドレスのリストの取得

JPNIC がもつレジストリデータより，正当なエンドユーザが登録されていない未割り当てのものを抽出する．なおレジストリデータは非公開データであり，今回は調査を目的として JPNIC より提供されたものを使用した．

[*1] https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data

[*2] rrc06.ripe.net, at Otemachi, Japan. Collects route updates announced by JPIX members from August 2001.

[*3] https://stat.ripe.net/

以上のようにして得られた経路情報と未割り当て IP アドレスのリストの共通部分をとる (図 2 参照) ことで，正当な所有者がいないにもかかわらず経路に現れる IP アドレスを検出する．なお図中の数値は例であり，実際のデータや検出結果を表すものではない．

提案手法によって検出された IP アドレスについて，それがいつから経路情報に現れるようになったかなどの詳細を調査するにあたって，RIPEstat 上での検索を行った．さらに，経路広告の送信元組織に連絡をとり，原因の特定を試みた．検出結果に対し，本研究では以下の点に着目した．

- 検出された異常経路広告の送信元 AS
- 送信元 AS を管理している組織
- 当該経路広告の観測され始めた時期および継続期間
- 異常経路広告発生の原因
- 当該経路広告が観測された地点数の推移

4. 調査結果

本調査によって，3 つの異なる/24 の IP アドレス空間が国内外から経路広告されている事例を検出した．調査の結果，検出された異常経路広告が広告していた IP アドレス空間を RIPEstat 上で検索した結果を図 3，図 4，図 5 に示す．3 つの図は検出された異常経路広告を観測した地点数の継時変化をヒートマップで表しており，赤に近づくほど少ない地点で，緑に近づくほど多い地点で観測されたことを意味する．いずれのヒートマップにおいても，時間が経過するにしたがって単調に観測地点が増加していく様子が現れている．

以下では，これら 3 つの事例について，それぞれ広告されるに至った原因と，JPNIC からの対応およびその結果も併せて記載する．なお，検出された具体的な IP アドレス空間については JPNIC 事務局に報告したが，個別の組織に関わる情報であるため，ここでは IP アドレスプレフィクスや広告元 Origin AS の AS 番号，AS の管理組織名といった詳細は伏せる．

4.1 日本国内の AS からの異常経路広告

日本国内のある AS から発信されていた未割り当て IP アドレスの経路広告は，1994 年 1 月に JPNIC から割り当てた/18 空間のうち，2012 年 2 月に部分的に返却されたものが，その後も BGP ルータに経路広告設定されたままになっていたことで発生していた．JPNIC から当該組織に対して連絡をとったところ，2020 年 03 月 05 日までに広告が停止したこと，さらに IRR のエントリ登録解除が確認できた．

4.2 韓国内の AS からの異常経路広告

韓国内のある AS から経路広告されていた未割り当て IP

継続期間: 2002年11月09日 – 2020年03月06日

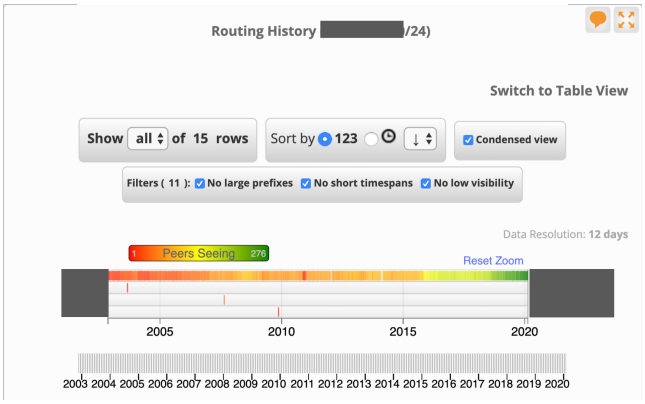

図 3 日本国内の Origin AS からの異常経路広告の経時変化を表すヒートマップ (RIPEstat: https://stat.ripe.net/)

継続期間: 2008年01月30日 – 2020年01月14日

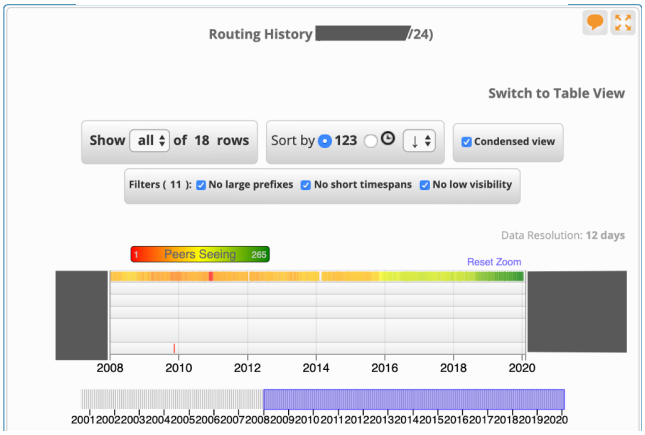

図 4 韓国内の Origin AS からの異常経路広告の経時変化を表すヒートマップ (RIPEstat: https://stat.ripe.net/)

継続期間: 2008年04月03日 – 2020年02月07日

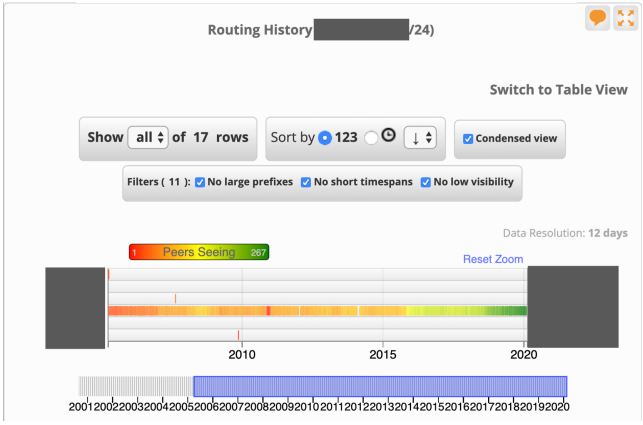

図 5 香港市内の Origin AS からの異常経路広告の経時変化を表すヒートマップ (RIPEstat: https://stat.ripe.net/)

アドレスは，2002 年に日本国内のある組織から JPNIC に返却されたアドレス空間で，2006 年ごろから経路情報で観測されるようになったものであった．JPNIC から当該組織に対して連絡をとったところ，原因は設定ミスであった

こと，2020 年 3 月 5 日までに広告が停止したこと，さらに IRR のエントリが登録解除されたことが確認できた．

4.3 香港市内の AS からの異常経路広告

香港市内のある AS から経路広告されていた未割り当て IP アドレスは，それを包含するアドレス空間を別の海外の通信事業者が 2008 年ごろに RADB に登録したことにより，正当な経路とみなされて広告が続いていたものであった．JPNIC から当該組織に対して連絡をとったところ，2020 年 2 月 7 日までに広告の停止が確認できた．なお，RADB (IRR) における登録解除は確認できていない．

5. 議論

5.1 調査結果から得られる知見

今回の調査で検出された 3 件の異常経路広告は，いずれも数年間という長期に渡って継続していたことが判明した．この事実は，未割り当て IP アドレスの経路広告は，そのプールを管理している主体（レジストリや ISP など）が意識的に調査しなければ見えてこないということを示唆している．

また，図 3，図 4，図 5 のいずれにおいても観測地点数が単調増加している．このことについて，可能性のある原因を 2 点挙げる．AS 間での経路情報は，途中のフィルタなどで意図的に止められない限り，伝播していくという特徴をもつ．すなわち，広告元が停止しない限り，他の地点での当該経路広告の観測数が減ることはない．さらに，今回使用した RIPE NCC が公開している経路情報のデータは，世界各地の IX でピアしている先から収集されるものである．RIPE NCC は年々その計測元の拠点を増やしており，このことも影響して観測地点の数が単調増加することにつながっていると考えられる．加えて，未割り当て IP アドレスに特有な性質も，観測数の増加に寄与している．プライベートアドレスや特別な目的で確保されている IANA 予約アドレスなどの経路情報として不適当な IP アドレスの広告は，AS でフィルタをして遮断されることがある．しかし，未割り当て IP アドレスの場合は，それを管理するレジストリ以外の第三者には判別しづらく，結果的にそのまま広範に流れやすくなる．以上のような背景から，未割り当て IP アドレスの異常経路広告は，悪性の乗っ取りや DDoS mitigation のような特殊な運用の経路広告と同様に注意深く調査し，実態を把握する必要がある．

5.2 提案手法の適用領域

本研究の調査では，NIR のレジストリデータと実際に観測される経路情報を用いて，本来は存在しないはずの経路情報を検出した．今回は JPNIC のもつレジストリデータを使用しており，調査の対象は日本国内全体の IP アドレスの分配状況である．しかし，IP アドレスの分配状況を表すデータを差し替えれば，同様の手法で，任意の組織・地域単位における分配状況に合わせた経路情報の正当性を調査することができる．すなわち，ネットワーク運用者が本研究の提案手法と同様の調査を行うことで，自身の管理する IP アドレスが他のネットワークにおいて無断使用されていないか監視することができる．また，本研究では IPv4 アドレスに限定して調査を行ったが，IPv6 アドレスについても同様の手法が適用できる．なお，今回 IPv6 アドレスについて調査を行わなかったのは，IPv4 アドレスと比較して分配の歴史が浅く，2003 年に現在の割り当ての仕組みに移行した結果 (第 2 節参照)，未割り当ての状態にある在庫数自体が少ないことに由来する．

今回検出された未割り当て IP アドレスの異常経路広告の原因は，3 件とも設定ミスであると判断された．しかし，結果的にインターネットに大きな悪影響を及ぼす以上，異常経路広告の発生は，原因を問わず早期に発見し，対処すべき問題である．したがって，

- 悪意のない設定ミス
- スパム送信やフィッシングサイト運用といった悪性活動を目的とする意図的かつ異常な経路設定

の両方を抑制するため，今後も継続的に本研究と同様の調査を行っていく必要がある．特に悪性利用に対しては，本研究のような検出方法が存在すること自体が抑止力となることを期待する．

5.3 制約と今後の課題

本研究の提案手法には，データの収集や処理にかかる時間がボトルネックとなり，リアルタイム性に欠けるという問題がある．まず，データの収集にかかる時間を短縮することを考える．第 3.2 節でも述べた通り，本研究の提案手法で使う経路情報のデータは 8 時間ごとに更新されるものであり，厳密にはアップロードされる時刻も一定ではないため，調査はリアルタイム性に欠ける．また，フルルートのデータファイルは表 1 に示す通り規模が大きく，計算環境や調査対象のネットワークの規模によってはそのダウンロードや，その後のデータ処理に時間を要する場合もある．しかし，フルルートの代わりにアップデート (更新は 5 分ごと) を用いることで調査時間の短縮が期待できる．

次に，経路情報とレジストリデータの比較に要する処理時間を短縮する方法について検討する．今回の調査では，Python で IP アドレス空間の計算に用いられる netaddr ライブラリを使用してデータの共通集合を計算した [8]．この処理を高速化するため，Bloom Filter を適用することが有効である [9]．Bloom Filter とは複数のハッシュ関数を用いることで，ある要素が集合に属するどうかを確率的に評価して高速で判定するためのデータ構造であり，経路情報とレジストリデータの比較に要する時間を短縮できる可能性がある．

5.4 NIR による通信リソース管理

本研究で NIR のレジストリデータに着目した理由は，RIR レベルでの調査では見えてこない経路制御の実態が存在することにある．この事実を踏まえ，NIR について簡単に考察する．階層を問わず，レジストリが通信リソースを管理する目的は，各々の担当範囲内で通信リソース分配の一意性を保つことにある．そうした中，配下に NIR をもたない RIR が正常に機能しなくなると，その担当地域内の下位組織やエンドユーザのもつ通信リソースの所有権を他のネットワークに対して示すことができなくなる．すなわち，NIR と RIR は相互補完的に機能しているといえる．よって，本研究のような異常経路広告の調査活動や，その結果に基づいた対策を講じることによって，NIR の機能をより確かなものにする必要がある．

6. 関連研究

本節では，異常経路広告などの誤った経路情報や，不要な経路情報の更新の原因となる不適切な経路広告を監視するための既存手法と調査について紹介する．また，国内外で実施されている経路情報の正当性を保つための取り組みについても触れる．

6.1 異常経路広告の検出に関する既存手法

文献 [10] では，BGP 経路制御における無効な経路広告を検出する手法を提案している．この研究では，無効な経路広告を次の 4 つのいずれかであると定義している:(1) 特別な用途のために予約済みであるプレフィクスの経路広告，(2) 未割り振りのプレフィクスの経路広告，(3) 乗っ取られたプレフィクスの経路広告，(4) AS パスが改竄された経路広告．この中で，(2) の未割り振りのプレフィクスの経路広告を検出する際には，アドレス分配状況の情報と，BGP ルータの通信で観測される経路広告の中の所有者に関する情報を突き合わせるという方法をとる． この手法は RIR からの割り振り状況と経路情報を比較するものだが，手法の発想は NIR からの割り当て状況を使用する本研究の提案手法と類似する部分がある．ただしこの研究は手法の提案にとどまっており，実際に調査した結果は提示されていない．

文献 [11] では，MOAS (Multiple Origin AS) に起因する異常経路広告を検出する手法を提案し，調査を行っている．MOAS とは，同一の IP アドレス空間が複数の異なる送信元 AS から経路広告される現象を指す．すなわち，対象の IP アドレス空間について，その正当な管理者の AS の他に，何らかの理由によって別の AS が所有を主張する経路広告が流れることを意味する．MOAS の原因は必ずしも悪意のある攻撃だけではなく，BGP ルータの設定ミスや意図的な良性の特殊な経路広告 (第 2.1 節参照) である場合も存在する．この研究の提案手法では，ヒューリスティックに作成されたホワイトリストやルールベースによる Typo 除外フィルタなどの適用を経て，経路の悪性の可能性を示すスコアリングを付与することで，多岐にわたる不適切な経路広告の中から悪性である疑いの強い MOAS を検出する．なお，意図的な良性の異常経路広告の判別に使用するため，RIR の提供する通信リソースの国情報や whois DB などの公開情報を活用することでホワイトリストを作成している．2018 年の 1 年間分の経路情報に対して提案手法を適用した結果，50 億件以上の経路広告の中から悪性 MOAS である可能性の高いものを約 15 万件 (2.59%) にまで絞り込むことに成功している．こうした結果から，直近 10 年で MOAS の件数全体が増加していることや，今後も意図的な良性の MOAS の利用拡大が見込まれることなどが報告されている．本研究のように未分配リソースに着目した経路情報の調査を行う際にも，この研究のように経路情報の属性から得られる情報を駆使することで，より効率的かつ高精度な異常経路広告の検出/分類が可能になると期待できる．

文献 [12] では，公開されている経路情報と IRR を用いた異常経路広告の分析を行い，その発生件数や傾向を調査する手法を提案している．まずフルルート同士やアップデート同士など複数の経路情報の組合せの変化をそれぞれ観察し，Origin AS の変更があった IP アドレス空間を抽出する．そうして得られた IP アドレス空間について IRR を参照することで，異常経路広告の候補の簡単な検出が可能となる．2017 年のある一日の経路情報に提案手法を適用した結果，経路情報同士の比較によって得られた 167 件の候補のうち，40% が IRR で登録が確認され AS 番号も一致したもの，46% が IRR で登録が確認されたものの AS 番号が一致しなかったもの，13% が IRR で登録が確認されなかったものであったと報告されている．以上のように，この研究では IRR に登録された情報を基に経路情報の正当性を評価しているという点において，本研究とは異なる．ただし，IRR には所有者情報についての厳密性が欠けていることや，IRR 情報更新のタイミング次第で調査結果が変わること，さらに提案手法では時間の経過による Origin AS の正当な変更などの可能性が考慮されていないことといった課題がある．

6.2 異常経路広告の調査・監視に関する国内外の取り組み

調査 [6]， [7] では，APNIC が管理する通信リソースのうち，経路広告されている未割り振りの IP アドレスと未登録の AS 番号がリストされている．このリストは毎日更新され，世界の 7 地域で同様の調査を行った結果を掲載している．ただし，ここに掲載されている情報は全て RIR レベルでの通信リソース分配を対象とした調査結果であり，本研究で調査したような NIR レベルで未分配の通信リソースの経路広告の実態については把握できない．

経路情報の正当性を保つため，すでに国内で運用されている取り組みとして，経路奉行がある．経路奉行は，一般社団法人 ICT-ISAC と JPNIC が日本国内で運用している経路ハイジャック検出システムである [13]．経路奉行では，国内 ISP が観測・提供する実際の経路情報を基に，JPIRR に通信リソースを登録しているユーザに対して経路ハイジャックの疑いのある経路情報の発生を通知する．こうしたシステムの活用によって，IRR 登録情報の悪意のない更新漏れを防止することができるため経路情報の正確性向上が見込まれる．さらにその結果として悪意のない異常経路広告が減少すれば，経路ハイジャックの検出精度自体の向上といった効果がある．本研究の成果の社会的な応用の際には，このような取り組みを通して得られた知見が参考となる．

7. 結論

本研究では，RIR レベルの調査では把握しきれないような，日本国内における異常経路広告の実態を調査した．また，調査を行うにあたって，新たに簡便かつ有効な手法を提案した．提案手法では，日本国内の ISP やエンドユーザ用に JPNIC が管理するレジストリデータと，RIPE NCC が公開している実際の経路情報を比較して，未割り当ての IP アドレスの経路広告を検出した．調査の結果，国内外の AS から数年間にわたって/24 の未割り当て IP アドレス空間が経路広告されていた事例を 3 件検出した．さらに追加調査によって，それらの原因が BGP ルータの設定ミスであることが判明した．以上より，ルータの設定次第で任意の組織から未割り当て IP アドレスが経路情報として流れているという実態が示された．

現在の経路制御の仕組みでは，異常経路広告の発生は完全には解消できない問題であり，既存の対策を講じても発生防止には限界がある．加えて，未割り当て IP アドレスの経路広告の問題は地域や組織に依存しないため，より広範囲かつ継続的な調査も必要である．こうした状況に対処する中で，提案手法が経路情報の設定における人為的ミスの防止や，未割り当て IP アドレスの悪性利用への対策として活用されれば，本研究がインターネットの安定運用に資することが期待できる．ただし提案手法には，データの入手や異常経路広告の検出処理自体に時間がかかることで，リアルタイム性を損なうといった課題もある．異常経路広告にかかる問題の本質的な解決と共に，さらに軽量に実態を調査する手法を提案することは今後の課題とする．

謝辞 本研究の一部は，日本学術振興会における科学研究費補助金基盤研究（C）（課題番号 20K11800）による支援を受けている．ここに記し謝意を表す．

参考文献

[1] 総務省： 平成 29 年 8 月に発生した大規模なインターネット接続障害に関する検証報告，https://www.soumu.go.jp/main_content/000525814.pdf (2017).
[2] 総務省: 大規模なインターネット障害発生時の対策について，https://www.soumu.go.jp/main_content/000539523.pdf (2018).
[3] JANOG32: 汚れた IPv4 アドレスのクリーニングについて考えよう，https://www.janog.gr.jp/meeting/janog32/program/cleaning.html (2013).
[4] APNIC: APNIC Labs enters into a research agreement with Cloudflare, https://blog.apnic.net/2018/04/02/apnic-labs-enters-into-a-research-agreement-with-cloudflare/ (2018).
[5] 西塚要: 今を知り今後に備える！ルーティングセキュリティ DDoS 対策最新動向，https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s06/s6-nishizuka.pdf (2017).
[6] Smith, P.: Advertised Unallocated Addresses, http://thyme.apnic.net/current/data-add-IANA (2020).
[7] Smith, P.: UNREGISTERED but announced ASes, http://thyme.apnic.net/current/data-unregAS (2020).
[8] Moss, D. P. D.: netaddr 0.7.20 documentation, https://netaddr.readthedocs.io/en/latest/ (2008).
[9] Bloom, B. H.: Space/Time Trade-Offs in Hash Coding with Allowable Errors, *Commun. ACM*, Vol. 13, No. 7, p. 422–426 (online), available from ⟨https://doi.org/10.1145/362686.362692⟩ (1970).
[10] Wang, H. and Hao, W.: Detection of Invalid BGP Routes, (online), DOI: 10.1109/WICOM.2010.5601413 (2010).
[11] 今井宏謙，岡田雅之，金岡晃ほか: BGP における広告元特徴を取り入れた分析による不適切経路広告の検出，コンピュータセキュリティシンポジウム 2019 論文集，Vol. 2019, pp. 1071–1078 (2019).
[12] 安藤正仁, 岡田雅之, 金岡晃ほか: BGP の Mis-Origination の原因となる経路情報の検知技術の提案，コンピュータセキュリティシンポジウム 2017 論文集， Vol. 2017, No. 2 (2017).
[13] JPNIC: JPNIC 経路奉行，https://www.nic.ad.jp/ja/ip/irr/jpnic-keirobugyou.html (2019).