IP アドレスの経路広告調査専門家チーム
調査報告書

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

2020 年 03 月 31 日

概要

本報告書は，2020 年 02 月 01 日から 2020 年 03 月 31 日まで，日本国内の未割当 IPv4 アドレスの経路広告の調査を委嘱された専門家チームの調査結果をまとめたものである．当チームは以下のメンバーによって構成され，定期的に来社して調査作業にあたった．

[メンバー]
調査員 五島健太朗 早稲田大学 基幹理工学研究科 情報理工・情報通信専攻 内田研究室 修士課程 1 年

インターネット上の経路広告において，いかなるエンドユーザにも割り当てられていない IP prefix（以下，未割当 prefix）が観測されるという問題がある．本報告書では，こうした予期しない経路広告の実態を把握することを目的とする．調査目的達成のため，具体的には，JPNIC が APNIC より割振りを受けた prefix pool から未割当 prefix を算出し，RIPE NCC が RIPE RIS で公開する経路情報（フルルート）と比較することで，理論上は経路情報に現れないはずの未割当 prefix の経路広告を検出する．さらに，検出された prefix を RIPEstat 上で検索することで，経路広告の開始時期や規模といった当該経路広告の実態を追加調査する．本調査の結果は，未割当 prefix の経路広告は，人為的設定ミスの可能性が高いことを示唆している．

[本報告書の流れ]
本報告書では，まず第 1 節で調査計画が持ち上がるに至った背景を述べ，第 2 節で調査の目的を述べる．続いて第 3 節で実際に調査する内容と実装について触れ，第 4 節でその結果と追加調査について述べる．第 5 節で結論を述べ，第 6 節では現時点で考えられる今後の課題を示す．なお，調査に使用したスクリプトやリソース等は付録として掲載する．

1 調査背景

1.1 未割当 IP prefix の広告

本節では，未割当 IP prefix およびその経路広告について簡単に説明する．現在，インターネットの経路制御は BGP による経路情報の交換を基盤としている．異なる AS 間を接続する BGP ルータの経路広告設定は，ネットワーク管理者が手動で行うため，管理者が所有しない任意のリソースさえも設定することが可能である（本報告書では IP アドレスや AS 番号など，IANA を最上流に割振り/割当ての対象となるものをリソースと総称する）．そうした悪意の有無を問わない誤った経路情報の広告を，本報告書では「異常経路広告」と定義する．

BGP における異常経路広告には，一般的によく知られる spoofing のほかに，未割当ての IP prefix を広告

するというものがある．これは既存の他の正規ユーザの所有する prefix ではなく，どのエンドユーザにも割り当てられていない prefix が経路広告される場合を指す．こうしたケースがシステム上許容されてしまう原因は，任意のリソースを広告設定可能であるなどの，BGP がもつ設計上の特徴に由来する．ただし，BGP における異常経路広告の存在は知られているものの，その全てが悪意のある攻撃とは限らない．中でも，未割当 prefix が経路広告されているケースについての日本国内における調査はいまだ十分ではない．

1.2 経路情報の正当性を保つための取組み

本節では，現在運用されている経路情報の正当性を保つための取組みについて簡単に触れる．また，本調査との関係についても補足する．

1.2.1 IRR

IRR（Internet routing registry）は，各 ISP などのユーザが管理する経路制御に関わるリソースを登録しておくデータベースである．ただし，RADB などの一部の主要な IRR へのエントリ登録は任意のリソースに対して可能であり，登録時にも正当な管理者・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った場合，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 単体の活用だけでは異常経路広告一般への本質的な対策にはならない．

1.2.2 RPKI

RPKI（Resource public-key infrastructure）は，IP アドレスや AS 番号といった，アドレス資源の割り振りや割り当てを証明するための PKI（Public-Key Infrastructure:公開鍵基盤）である．RPKI では，リソースの割振り/割当てを行ったレジストリが，当該リソースに対して「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，認証のツリー構造はインターネットレジストリの階層構造と等しくなることが保証されており，理論的には未割当ての異常経路広告にも対処可能である．しかし，一般に普及する段階には至っていない．このため，現在は RPKI のみでは対応すべき異常経路広告についての実態を知るという目的には十分に貢献できない．

1.3 関連調査

本調査と類似の調査は，RIR（Regional Internet registry）から下位層レジストリへ割り振られるリソースについて行われている．全世界の RIR5 つから，それぞれが管轄する地域内の NIR（National Internet registry）および ISP とエンドユーザに対してリソースを分配することを特に「割振り」と呼称する．RIR から割り振られていない「未割振 prefix」の異常経路広告についての調査はすでに行われており，以下に掲載する APNIC が管理の ftp サイトで結果が確認できる．

- IP アドレスに対する調査 `http://thyme.apnic.net/current/data-add-IANA`
- AS 番号に対する調査 `http://thyme.apnic.net/current/data-add-IANA`

ただし，上記の調査は，本調査とは適用範囲が異なる．すなわち，既存の調査は RIR における未分配のリ

ソースを対象としているが，本調査ではさらに下位層の NIR における未配分のリソースを対象とするという違いがある．

2　調査目的

本報告書では，日本国内における異常経路広告のうち，未割当 prefix が広告される場合の実態を調査することを目的とする．現在，本調査が対象とする日本国内においては，JPNIC が APNIC よりリソースの割振りを受けている．そのうち，契約を解約した IP 指定事業者などから返却されるといった特別な経緯をもつ一部の IP アドレスは，APNIC に返却するまでの間は未割振在庫として JPNIC が管理する．しかし近年，割振り・割当てが行われていない未分配の状態にある IPv4 アドレスについて，意図しない第三者により経路情報が広告される事例が発生している．そこで JPNIC で管理する未分配 IPv4 アドレスについても，インターネット上に経路広告されて使用されている事例が定常的にあるかどうかの調査を早急に実施する必要がある．以上の問題の概要を，図 1 に例示する．

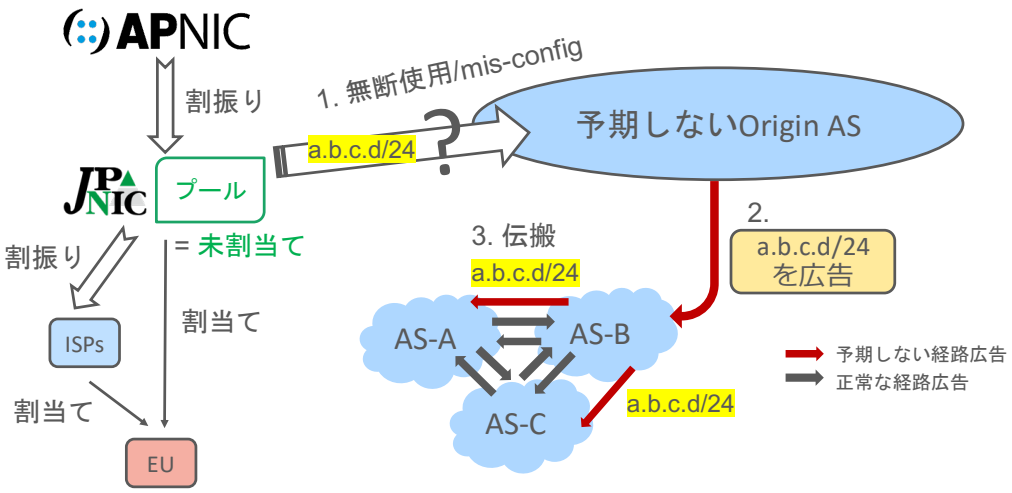

図 1　未割当 prefix の異常経路広告までの流れ

3　調査内容

本調査では，実際の経路情報と JPNIC がもつ未割当アドレスの一覧を比較し，異常経路広告に記載のアドレス範囲に含まれる未割当 prefix を検出する．データの整形から未割当 prefix の検出までを，すべて Python（version 3.6.7）で実装した．図 2 に調査の概要のイメージを示す．以下では，調査に使用するデータと実装に必要な Python ライブラリ等について触れる．

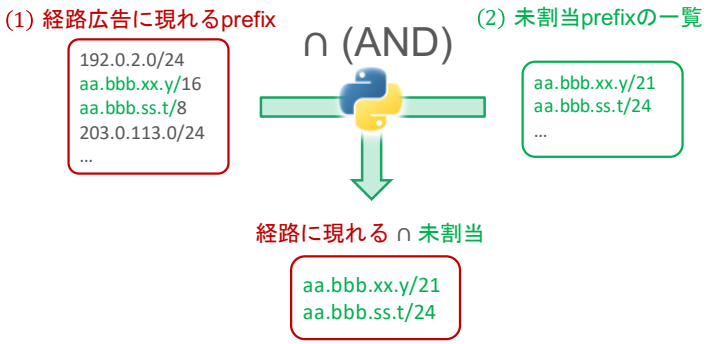

図 2　調査手続きの概要

3.1　使用するデータ

本調査は，日本国内の経路情報と JPNIC が管理する未割当 IP アドレスのリストという 2 種類のデータを必要とする（形式やサイズなどの詳細は表 1 に記載）．

一つ目の経路情報については，RIPE NCC が世界各地の IX から収集し，RIPE RIS において公開している MRT 形式のフルルート経路情報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 のものが更新されるが，更新自体が不安定であり，さらにタイムゾーンが不明なため，データの収集の際には cron で 2 日前時点のものを自動取得するよう実装した．なお，ファイルの命名規則は `rcc06.net/{yyyy}/{mm}/{dd}/bview.{yyyy}{mm}{dd}.{hh}00.gz` である．gz ファイルを解凍して得られる mrt 形式の元ファイルを，bgpdump によってテキストデータ化したものをスクリプトで読み込む．

一方，二つ目の未割当 IP アドレスのリストについては，JPNIC が管理する IPv4 prefix のデータベースから，すでに ISP やエンドユーザに割り振った/割り当てたものを除外する処理を施したものを使用する．未割当 prefix 全体の計算は 2019 年 12 月 10 日に行ったので，その時点のアドレス分配状況を元に調査を行った．

以上の 2 つをもとに，経路情報中に含まれる未割当 prefix を検出する．

表 1　調査に使用したデータの詳細

概要	名称等	形式	出典	規模（/24 換算）	規模（行数）
経路情報	bview	mrt	RIPE RIS	15,341,353	800,000
未割当 prefix 一覧	N/A	txt	JPNIC 内部情報	14,497	（省略）

3.2 調査の実装

以下に，使用した Python ライブラリを示す．また，mrt 形式データの前処理に使用したツールについても記載する．

- bgpdump
  ubuntu 用の公式ドキュメント `https://launchpad.net/ubuntu/+source/bgpdump/1.6.0-1`
- pandas
  公式ドキュメント `https://pandas.pydata.org/pandas-docs/version/0.23.1/`
  データの読み込み
- netaddr
  公式ドキュメント `https://netaddr.readthedocs.io/en/latest/introduction.html`
  IPSet() により，2 つの IP prefix の共通部分や差集合の計算が容易になる
  最小/32 で計算可能
- ipaddress
  公式ドキュメント `https://docs.python.org/3/library/ipaddress.html`
  str 型の IP アドレスを IPv4Address オブジェクトに変換する

4 調査結果

本調査によって，3 つの異なる/24 の prefix が国内外から経路広告されている事例を検出した．本節では，調査の結果検出された異常経路広告の prefix を，RIPE stat 上で検索した結果を図 3，図 4，図 5 に示す．また，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 prefix 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となるため，ここでは詳細な prefix，origin AS の AS 番号，AS の管理組織名といった情報は伏せる．

4.1 日本国内の AS からの異常経路広告

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と IRR のエントリ登録解除が確認できた．原因については，連絡をとった際の情報より判断すると，この AS を origin とする異常経路広告は，過去に JPNIC に返却されたものの，経路広告設定が更新されていなかったことに起因すると考えられる．

4.2 韓国内の AS からの異常経路広告

JPNIC から当該組織に対して連絡をとったところ，2020 年 01 月 14 日までに広告の停止が確認できた．原因については，連絡をとった際の情報より判断すると，この AS を origin とする異常経路広告は，人為的な mis-config に起因すると考えられる．

4.3 香港市内の AS からの異常経路広告

JPNIC から当該組織に対して連絡をとったところ，2020 年 02 月 07 日までに広告の停止が確認できた．原因については，連絡をとった際の情報より判断すると，この AS を origin とする異常経路広告は，人為的な mis-config に起因すると考えられる．

（以下の図 3,4,5 は，RIPE stat [https://stat.ripe.net] の画像データを元に、該当 prefix 情報を伏せる加工を行ったものである）

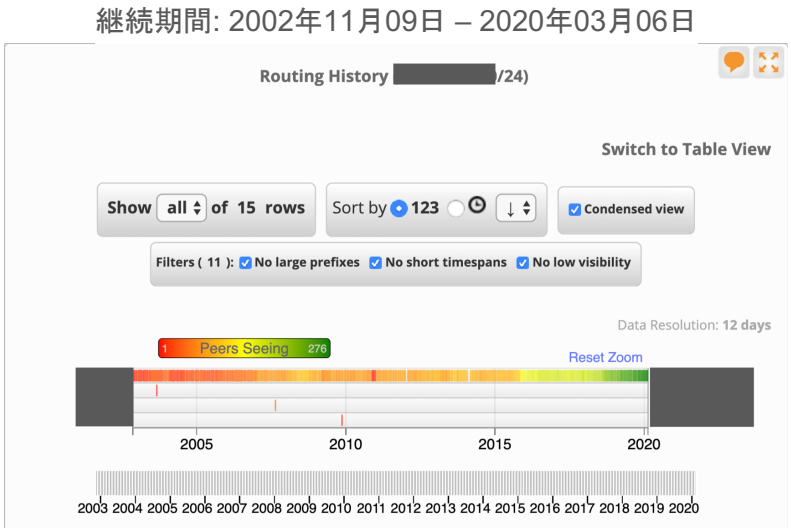

図 3　日本国内の Origin AS からの異常経路広告の経時変化を表すヒートマップ

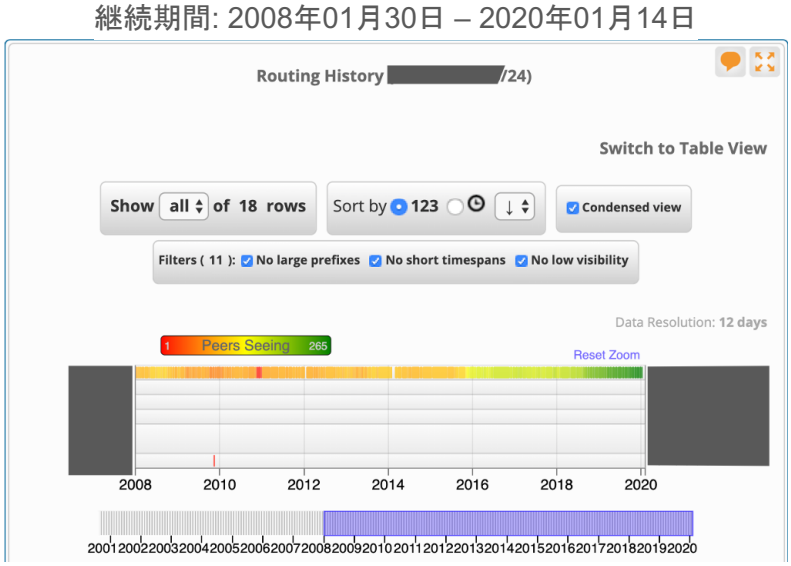

図 4　韓国内の Origin AS からの異常経路広告の経時変化を表すヒートマップ

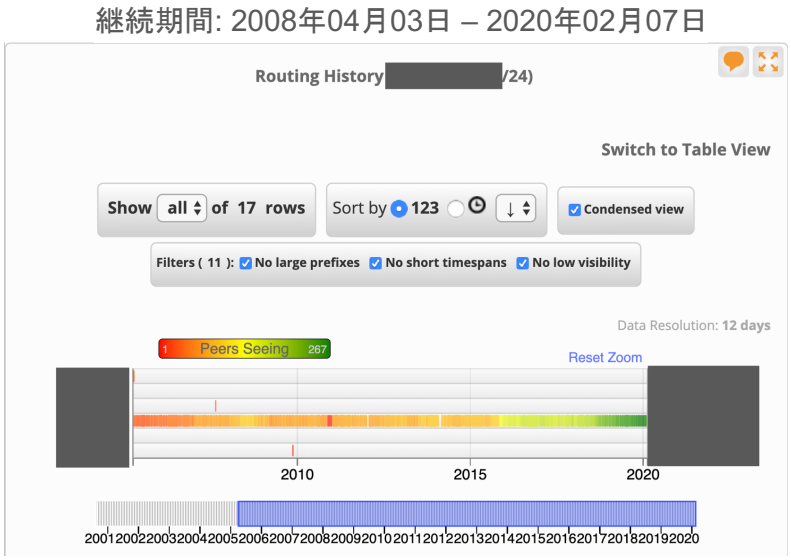

図 5　香港市内の Origin AS からの異常経路広告の経時変化を表すヒートマップ

5　結論

今回の調査によって，日本国内で観測できる経路広告には年単位で未割当 prefix を含むものが 3 件あったことが確認された．本調査の対象地域や組織は日本国内に限定されているが，BGP の性質は地域や組織に依存しない．そのため，任意の地域や組織においても，日本国内同様に未割当 prefix が広告され，あるいは不正に使用されている可能性は否定できない．したがって，今後も継続的に調査を行うとともに，他地域および日

本国内の組織，ネットワーク管理者，ユーザなどに経路広告設定の正当性/一貫性を保つよう要請することが必要である．

6 議論

本節では，第 4 節で述べた調査手法のリミテーションについて触れ，それを補うものを含めた今後の課題/展望について簡単に述べる．また，本調査について APRICOT2020 BGP&Routing Operations で発表した際に得られた知見を交えた今後の調査展望についても触れる．

まず本調査手法で検出される prefix に対して，今後能動的に調査を行うことができる．すなわち，検出された prefix のアドレスレンジ内の全アドレスに対して ping を送信してスキャンをかけ，未割当アドレスの不正使用を監視することができる．さらに踏み込んだ調査を行うならば，検出された prefix 内のホスト上で開いている port を調べ，それを判断材料に偶発的な人為ミスによるものなのか，悪意を持ったリソースの不正使用なのかを推測することも可能である．

他の外部情報に頼る場合，IRR での検索が有効となる場合がある．検出された異常経路広告の prefix が BGP ルータの設定と IRR の登録の両方で確認された場合，全く異なる 2 ヶ所での typo（fat finger）が続くことは考えにくいため，当該 prefix は不正利用されている可能性が高まる．また，IRR の登録情報の日時も経路広告の過去の履歴を追う上で参考となる．

また，結論の節でも述べた通り，調査の対象を拡大することが望ましい．未割当 prefix の経路広告は地域や組織に依存しないため，広範囲での継続的な調査が必要である．加えて，APRICOT2020 での発表の質疑応答では，IPv6 に対する調査を求める意見が挙がった．これについても，本調査では IPv4 に限定したが，同様の方法で IPv6 に対しても調査が可能であるため，今後の課題とする．

7 付録

- 本調査に使用した Python script を公開している github repository のリンク
  `https://anonymous.4open.science/r/0d8ee868-194c-48b0-a17d-c58b17837596/`
- APRICOT2020 で発表したセッション
  `BGP&Routing Operations`
  `https://2020.apricot.net/program/schedule/#/day/9/bgp--routing-operations`