IRR・RPKI 動向調査専門家チーム 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

2013 年 8 月 5 日

目次

1. 本報告書の概要

本報告書は、2013 年 1 月 10 日から 2013 年 6 月 26 日にわたって開催された IRR・RPKI 動向調査専門家チーム（以下、当チーム）によって行われた、JPNIC が関係する IRR と RPKI 動向および将来の JPNIC の役割とルーティング支援サービスのあり方について議論した結果をとり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、7 回にわたって検討会を開催した。

[メンバー]

チェア	吉田友哉	インターネットマルチフィード株式会社
	有賀征爾	エヌ・ティ・ティ・コミュニケーションズ株式会社
	川村聖一	ＮＥＣビッグローブ株式会社
	中野達也	KDDI 株式会社
	平井則輔	ソフトバンク BB 株式会社
	松崎吉伸	株式会社インターネットイニシアティブ
	渡辺英一郎	一般財団法人日本データ通信協会 テレコム・アイザック推進会議 (Telecom-ISAC Japan)

[検討会日程]

第 1 回　2013 年 1 月 10 日
第 2 回　2013 年 2 月 4 日
第 3 回　2013 年 2 月 18 日
第 4 回　2013 年 4 月 8 日
第 5 回　2013 年 4 月 22 日
第 6 回　2013 年 5 月 27 日
第 7 回　2013 年 6 月 26 日

本文書では、まず第 2 章で現在のインターネットにおける経路制御の現状について、脅威の実情や将来必要とされるサービスについて述べる。第 3 章では、日本や世界における IRR の動向や JPNIC が提供している JPIRR サービス動向と現在の課題について、第 4 章では、RPKI の動向について、現在の普及状況や将来の課題について述べる。最後の第 5 章では、JPNIC のインターネットレジストリとしての、経路制御コミュニティに対する将来の役割について述べる。

本報告書の骨子

- 現在のインターネットの経路制御は、不意の不正な経路広告によって複数の組織が甚大な被害を被った可能性があり、抜本的な予防策を講じる必要がある。
- 不正経路広告を防ぐための手段として ISP の経路フィルタが有効と言われている。経路フィルタを生成するための参照先データとして IRR が最も活用されており、日本では経路奉行と連携した不正経路検知機能も提供されている。
- IRR は記述の自由度も高く様々な用途で活用されているが、登録情報の信憑性に問題があり、経路フィルタ生成の参照先データとして全世界で活用していくには新たな仕組みが求められている。
- 新たに、PKI を活用した IP アドレスの正当性を担保する Resource PKI(RPKI)サービスが各 RIR で開始され、正しい、IP アドレスと Origin AS の組み合わせを記述した Route Origin Authorization(ROA)の作成と活用が進んでいる。
- 今後 JPNIC では、RPKI サービスを日本国内で速やかに開始し、インターネットの経路制御基盤のセキュリティ向上に貢献する重要な役割を担っていく責任がある。
- 具体的には、日本国内の事業者に対する ROA の発行、APNIC 地域での安定した RPKI の提供を行っていく必要がある。

2. インターネット経路制御を脅かす脅威の現状

経路制御を脅かす脅威にはさまざまなものが存在する。物理的な故障や障害によるもの、ルータのソフトウェアの不具合に起因するもの、また人為的な問題で経路制御に不具合が生じたと考えられるものなどがあげられる。特に人為的な問題で引き起こされる脅威については、本来 ISP 等での経路フィルタ設定などにより運用上防げたものから予防策が困難なものまで様々存在し、いずれの場合もインターネット全体へその脅威が伝搬してしまうケースがこれまで多数発生している。本章では、それらの脅威について、その分類と具体的な事例、また現在の対応状況について述べるとともに、今後どういった対策が必要と想定されるかについて述べる。

2.1. 経路制御を脅かす事例の紹介と分類

2.1.1. 機器故障等の物理的なもの

現在のインターネット経路制御を担う機器は主としてルータとなっている。このルータの故障や通信回線の接続リンク断を原因とした BGP/OSPF 等のセッション断が発生した場合、ルーティングテーブルの再計算が発生する。リンクのアップダウンを繰り返すフラップや機器が reload を繰り返す等これらの事象が頻発するような状態が発生すると、ネットワークの宛先制御が完了せず、パケットロスが発生するためネットワーク全体が不安定になる。このような状態が発生した場合においては、

・reload を繰り返している機器をそのネットワークから切り離す
・フラップしているリンクを手動にて強制シャットダウンする

等の対処が必要となる。

2.1.2. ルータの実装や不具合に起因するもの

ルータのソフトウェア(OSPF や BGP に関するソフトウェア)の実装上の不具合や RFC 等で正式に規定されていないプロトコル上の不正な BGP オプションが原因となり、BGP のセッション断が発生する事象が過去に発生している。

一例として、ルータが、規定されていない BGP オプションを送信してきた相手先ルータを切断する実装がなされていたため、再接続後、同じ問題が発生し接続と切断が繰り返し引き起こされるという事象が過去何度か発生している。その結果、ルーティングテーブルの再計算が発生し網全体が不安定になり、それに引きずられてパケットの転送が不安定になる。以下に具体的な事例を紹介する。

(ア) 大量の AS-PATH prepend によるセッション断
異常に長い AS-PATH を含んだ Prefix が不正なセッションとみなされ、ルータ側で BGP セッションを clear された事例
http://www.gossamer-threads.com/lists/cisco/nsp/103838
http://www.geekpage.jp/blog/?id=2009/2/20/2

(イ) 通常使わない BGP アトリビュートやオプションを付与した経路情報が原因で、経路制御が不安定になった事例
http://www.renesys.com/blog/2010/08/house-of-cards.shtml

(ウ) 4 octet AS の解釈の違いにより、不正な update と判断されセッションを clear してしまった事例
http://venus.gr.jp/opf-jp/events/showcase3/showcase3-4byte-tech.pdf

この場合においては、一般的な対策として、

・問題の発生した BGP Peer のセッションをシャットダウンする
・問題のある IP Prefix を特定してフィルタし除外する

等の対策を取る必要があり、対策を行うまでの間、継続して BGP セッションの Up/Down が繰り返される危険性がある。

2.1.3. 人為的な問題で経路制御に不具合が発生したと考えられるもの
通常の経路制御では、経路制御の最小単位となる Autonomous System(AS)が個別に接続を行う接続先 AS へ自 AS が最終送信先となる IP Prefix を通知する。通知を受けた組織はその組織の接続先にその情報を繰り返し転送することで経路の情報を交換し、インターネット全体の経路制御は成り立っている。

他組織が管理する IP Prefix の誤広告(Mis-Origination)や AS 内部の経路を誤って外部に広告してしまう事例や、上位 ISP から購入したトランジットの経路情報を誤って別の上位 ISP に広告してしまった等のトラブルが原因で、トラフィックの誤誘導が発生した事例が過去に報告されている。これらの多くは意図的に行ったものではなく、人為的なミスと考えら

れている。以降の章でそれらの事例や分類等について詳しく述べる。
(注意：経路ハイジャックや BGP Prefix hijack と呼ばれることが多くみられた。しかしながら、悪意の無いオペレーションミスが起因となることがほとんどである現状から、Mis-Origination 等の名称に見直されつつある。このような背景を考慮し、本書では、従来経路ハイジャックと呼ばれていたものを Mis-Origination と表記する。)

2.2. 人為的な問題で経路制御に不具合が発生したと考えられるものの事例分類

Mis-Origination 発生時の影響度合いは、個別の事象によって異なるが、多くの事例はトラフィックを誤って本来宛先や途中経路となるべきでない AS へパケットを誘導してしまう等の影響が発生する。これらの事例の多くは受け入れる経路情報を取捨選択する IP Prefix ベースの経路フィルタ等の対策を講じることで予防する事が可能である。しかしながら、経路フィルタの対策導入は、個々の組織の判断となっており、経路フィルタの日常のメンテナンスコストなどの関係からすべての組織で導入されている状況とはなっていない。Mis-Origination 発生時の影響度合いおよび対策の可否については、表 1 「事例ごとの影響度合い」に分類し分析した。

事例 a：
2005 年 トルコの ISP が多量の Prefix（当時のフルルート相当）を Mis-Origination したとされる事例
http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml

事例 b：
2008 年 パキスタンテレコムによる Youtube Prefix の Mis-Origination
http://itpro.nikkeibp.co.jp/article/COLUMN/20090225/325481/

事例 c：
2008 年 アフリカの ISP が所有する Prefix を Abovenet が Mis-Origination した事例
http://ddos.arbornetworks.com/2008/03/africa-online-kenya-latest-internet-routing-insecurity-casuality/

事例 d：
2008 年 ブラジルの ISP が多量の Prefix(当時のフルルート相当)を Mis-Origination したと

される事例
http://ddos.arbornetworks.com/2008/11/when-hijacking-the-internet/

事例 e :
2010 年 中国の ISP による Mis-Origination と思われる事例
http://bgpmon.net/?p=282
http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml

事例 f :
2009 年 AS-PATH を捻じ曲げて遠回りをさせた事例
http://www.renesys.com/wp-content/uploads/2013/05/blackhat-09.pdf

事例 g :
2011 年 一部日本国内の ISP が Facebook に到達する際、中国・韓国を経由した事例
http://www.bgpmon.net/facebooks-detour-through-china-and-korea/

事例 h :
2012 年 上位 ISP にマルチホーム先から受信したフルルートを誤って広告した結果、上位 ISP が孤立した事例(誤トランジット)
http://labs.apnic.net/blabs/?p=139

事例 i :
2013 年 Mis-Origination が Route Server 経由で伝搬されてしまったと予測された事例
http://mailman.nanog.org/pipermail/nanog/2013-March/056680.html

事例 j :
2013 年 AS 番号ごと詐称された事例
実在する AS が別の全く関係ない AS 配下に発生した事例。
いわゆる誤設定の一つではないかと考えられる。
JANOG メーリングリストアーカイブ([janog:11548] AS ハイジャック？)

表 1 事例ごとの影響度合い

影響度合い	事前対策が可能なもの	事前対策が困難なもの
影響大 (複数の ISP が関与するため対応が困難)	事例 a 事例 d	事例 e 事例 i
影響小 (単一 AS 等、限定的な影響で済んだ)	事例 h	事例 b 事例 c 事例 f 事例 g 事例 j

表 1 では、影響度合いが影響大であり、かつ、事前対策が可能と考えられた事例が複数見受けられる。このように事前に対策ができたであろうにもかかわらず影響が発生していることから、Mis-Origination の対策を個々の組織で進めるための継続した普及啓発が必要とも考えられる。尚、「事前対策が可能」としたものでも、ISP など個々の組織の運用ポリシーとして配下の接続 AS に対して経路フィルタを適用していない場合も存在するため、根本的な対策が難しい場合も考えられる。
その一方で対策が困難な事例も多く見受けられる。中には影響が世界中に及んだものも複数存在する。これらの事例は、現時点においては、従来一般的に行われてきた実装可能な運用方式や対処方式では対策が難しく、何らかの抜本的な改善が必要となってくる。
次節では、本節で述べた脅威への対策についてその対策の詳細を解説する。

2.3. 経路運用者の脅威への対応状況

経路制御における Mis-Origination 等の脅威への対応は、現在、大きく二つに大別することができる。本節では、自らが脅威とならないことを目的とした対応と外部からの脅威発生時の影響緩和を目的とした対応の二つについて詳細を説明する。

(1) 自らが脅威とならないことを目的とした対応(自組織が Mis-Origination の発生源とならないための対策)
(2) 外部からの脅威への対応(接続先組織から発生した Mis-Origination の影響を緩和するための対応)

・自らが脅威とならないことを目的とした対応
前節で触れているように、経路制御を脅かす脅威は Mis-Origination 等、人為的な問題に起

因することも多いと言われている。このような問題が背景となっていることから、経路運用者は自らが設定ミスを犯すことを前提に、自らが脅威とならないために、AS の内部および外部への接続ポイントにおいて運用しているルータに適切な経路フィルタを設定することが求められている。おおむね日本国内の ISP や AS においては、これまで大きなトラブル事例が報告されていないため、適切な経路フィルタがなされていると考えられている。このように ISP や AS の接続形態ごとに推奨される経路フィルタについては、日本ネットワークオペレータズグループ(JANOG)によりとりまとめが行われており、以下の技術ドキュメント中の経路フィルタの事項にまとめられている。

・JANOG Comment 1000
「xSP のルータにおいて設定を推奨するフィルタの項目について」
http://www.janog.gr.jp/doc/janog-comment/jc1000.txt

・JANOG Comment 1001
「xSP のルータにおいて設定を推奨するフィルタの項目について ～ トランジット接続部分編」
http://www.janog.gr.jp/doc/janog-comment/jc1001.txt

・JANOG Comment 1002
「xSP のルータにおいて設定を推奨するフィルタの項目について ～ ピア接続部分編」
http://www.janog.gr.jp/doc/janog-comment/jc1002.txt

・JANOG Comment 1003
「xSP のルータにおいて設定を推奨するフィルタの項目について ～ 顧客接続部分編」
http://www.janog.gr.jp/doc/janog-comment/jc1003.txt

・JANOG Comment 1006
「xSP のルータにおいて設定を推奨するフィルタの項目について（IPv6 版)」
http://www.janog.gr.jp/doc/janog-comment/jc1006.txt

・外部からの脅威(Mis-Origination)への対応
外部からの脅威として、Mis-Origination が疑われる事象が発生した場合を想定し実際に有効と思われる対応を検討した。検討の結果、必要な対応は以下の通り、検知、情報確認および分析、対処の 3 段階の対応が必要と考えられた。必要な対応とその詳細について以下にまとめた。

(1)検知

Mis-Origination の検知は、常に経路情報を監視する必要性や外部の経路情報の収集が必須であるため個々の組織が独自に行うことは困難と考えられている。そのため、経路運用者のコミュニティが個々に運営する検知システムを活用することが推奨される。具体的には、Mis-Origination が疑われる事象が発生したことを検知するために、あらかじめ検知し、通知サービス等を行うシステムへ事前登録をする必要が存在する。日本国内では、JPNIC や一般財団法人日本データ通信協会テレコム・アイザック推進会議(Telecom-ISAC Japan)が運営する Mis-Origination 検知システム「経路奉行」と連携し、 JPIRR のオブジェクト登録者に対して Mis-Origination 情報の通知が行われているおり、経路奉行と JPIRR を活用するケースが多いと言われる。またこのような検知・通知サービスを複数活用することで、局所的、地域的な脅威発生時も検知を漏らす可能性を低減し、検知精度を高め、検知システムのメンテナンス等による検知サービス停止の影響を矮小化することが可能となっている。 このような、Mis-Origination 等の脅威を検知することを主目的として外部経路を監視し、通知するサービスとしては、次のようなものが存在する。

A) JPIRR/経路奉行

https://www.nic.ad.jp/ja/ip/irr/jpnic-keirobugyou.html

JPNIC や Telecom-ISAC Japan が運営する Mis-Origination 検知システム「経路奉行」と連携し、JPIRR のオブジェクト登録者に対して Mis-Origination に関する情報通知が行われている。

B) ISAlarm(MyASN)

https://www.ripe.net/is/account/login (事前登録必要)

RIPE NCC が運営する、経路情報に関する情報通知サイト。Prefix と Origin AS、電子メールアドレスを登録し、異なる Origin AS を検知した場合に通知するサービスが存在する。また RIPE NCC では Routing Information Service(RIS)では国内外 20 サイトの経路情報を収集し、保存公開が行われており、これを活用し過去の脅威を調査することも可能となっている。

(2014 年 2 月現在、上記リンクは存在しない。RIPE NCC では類似のツール（RIPE stat、Route Status）が別途提供されている。)

C) BGPMON

http://bgpmon.net/ (事前登録必要)

戦術の RIS や有志組織からの提供経路情報を活用し、リアルタイムデータを使った経路情報に関する警報を行うサービス。経路情報の Origin AS の問題を検知することだけでなく、経路情報の AS-PATH をあらかじめ設定した正規表現と比較し、マッチしない場合に通知す

るなど Origin AS に関する脅威だけでなく、途中の AS-PATH 経路の脅威を検知する機能を有する。

(2)脅威発生時の情報確認および分析

経路に関する脅威の通知サービス等により Mis-Origination が疑われる事象が確認された後、次のアクションとして影響範囲や発生規模などの情報確認を行う。必要な確認事項としては、第一に、脅威が発生したとされる対象 IP Prefix が自 AS 内でどのようなサービスに使われているのか、どの地域に割り当てられたものなのか確認し、可能な範囲で影響を確認する。また、並行し外部の経路情報確認サイトにおいても同様の情報収集を行う。

A) 疑われる状態となった経路情報の IRR や WHOIS への登録状況を確認

IRR を検索する場合、国内外には 40 程度の IRR が存在し、大規模 AS の顧客情報や地域インターネットレジストリ毎の情報となっている。このように複数の IRR を個別に検索することは手間を増大させるため、RADB の検索サービスを活用することで、RADB とミラーリングを行う他の IRR の情報も一括検索されるため有効である。尚、2013 年 10 月現在、RADB では主要な IRR はすべて一括して検索が可能となっている。

B) 対象経路情報の自 AS 内での確認および外部の Looking Glass での確認

インターネットには経路制御の最適化を目的として、有志の組織が当該組織の様々な経路情報をリアルタイムに公開している。このような公開情報システムを Looking Glass と言い、その時点でのその組織内部での個別の経路情報の見え方などを参照することが可能となっている。

自 AS の経路情報と外部 Looking Glass の経路情報の内容に差異が存在する場合、トラフィック傾向をトラフィックグラフの波形などから目視確認し、トラフィック傾向に変動が確認された場合、Mis-Origination 等の影響により、どこかの AS へ本来は自組織へ到達するはずのパケットが別の AS へ吸い込まれ、パケットの送信者が期待する正常な通信が出来ない状態となっていることや、AS 規模の Man In The Middle 攻撃の発生が考えられる。

C) 外部の経路監視サイトをチェック

・Routing Information Service(RIS)
  http://www.ripe.net/ris/(事前登録必要)

RIPENCC が運営している経路情報のアーカイブサイト。世界各地の IX 等で収集された経路情報を保存。最古は 1997 年より存在。Web による個別 IP Prefix ごとの検索だけでなく、MRT 形式で経路情報をアーカイブしたバイナリファイルが公開されており、libbgpdump などで ASCII へ変換し、活用が可能となっている。

・University of Oregon Route Views Project

http://www.routeviews.org/

オレゴン大学による経路収集サイト。古くからの経路も集積、公開されている。RIS と同様に MRT 形式の経路情報が公開され、同様に libbgpdump などで活用が可能となっている。

(3)対処

情報確認および分析により、Mis-Origination が疑われる事象の発生要因が推測できた場合、Mis-Origination の発生原因となっている AS に対しコンタクトを試みる。Mis-Origination が発生し、被疑状態が発生しても、Mis-Origination 自体が故意である場合は概して少なく、オペレーション等に起因し自組織の IP アドレスを設定する際のタイプミスであったり、IX 接続インターフェイスの Connected IP アドレスの誤った Redistribute であったりと、オペレーション上の問題が要因である事象が大多数を占めると言われている。このような要因である事から、相手先へのコンタクトは悪意を糾弾・指摘することは避け、事実を落ち着いて通知することが効果的となっている。このような外部組織とのコンタクトに必要なコンタクト先情報を得るためには、IRR や WHOIS、PeeringDB などがコンタクト先データベースとして活用されており有効である。また、原因 AS だけでなくその上位 AS として接続していると思われる AS へコンタクトすることも、上位 AS として不正な Mis-Origination の伝播を根元の位置で停止することが可能であり解決に向け有効なアクションとなっている。

A) PeeringDB によるコンタクト先の検索

https://www.peeringdb.com/

情報閲覧はゲストアカウントで可能。自 AS の情報を登録するには、ユーザー登録後、PeeringDB の運営者の AS 適切性確認後に情報登録が可能になる。尚、PeeringDB への登録は AS であることが必須の条件となっており、登録後、PeeringDB の運営側が新規登録 AS の妥当性を WHOIS 情報等いくつか確認してから後、詳細情報の登録を開始することが可能となっているため、新規の登録時にはある程度余裕をもった状態であることが望ましい。

B) 各国の Network Operators Group(NOG)との相談

JANOG や North America Network Operators Group(NANOG)のような、技術者のコミュニティへ相談し、サポートを求めることも実際事例発生じに解決策として行われており、各国の NOG の運用者が当該経路の状況を調査することが結果として影響範囲の確認にもつながり、Mis-Origination 状態の解決につながったケースも多くみられる。

C) 優先経路の広報

上記対応でも回復が見られない場合は、Mis-Origination の対象となった経路よりも細かい経路をインターネットに広報することで、経路選択優先順位を上位とすることで回復を図り取り返す行為を行うことが最終手段となる。表 2 と表 3 に取り返す行為の概要を示す。細かい経路を広報する際、隣接 AS が細かい経路を受け入れ可能か確認および調整が必要である。また、細かい経路を広報することはインターネットルーティングテーブルへの影響があるため、十分な考慮が必要である。その他、留意点として、対応しているうちに直ってしまう場合が多いことや、時間とともに回復していることがある。最終的には Mis-Origination が発生する前の状態に戻すことが望ましい。

表 2 サブネットマスク長が同様の場合

自組織の正常経路情報　　：192.168.0.0/22 AS A Mis-Origination 経路情報：192.168.0.0/22 AS B この場合、サブネットマスク長が同じであるため、原則経路情報を受け取った側の AS-PATH 長が短い経路が選択され、AS によっては誤った AS へパケットを転送する。

表 3 経路を分割した場合

自組織の正常経路情報　　：192.168.0.0/24 AS A 192.168.1.0/24 AS A 192.168.2.0/24 AS A 192.168.3.0/24 AS A Mis-Origination 経路情報：192.168.0.0/16 AS B この場合、Origin AS A のサブネットマスク長が Mis-Origination 経路よりも長いため、原則経路情報を受け取った側は、/24 の経路が選択され通信は正常化される。

2.4. 本章のまとめと将来必要とされるサービス

前項までに、現在のインターネットにおける経路制御の現状およびその問題に対する運用者の実際の対応をまとめてきた。本章のまとめとして、現在の脅威およびその対応を鑑みて、将来必要とされるサービスについて述べる。

前項でまとめた脅威への現状における対応は、完全に防ぐことは不可能であり、自らが脅

威とならないための対応と、実際に外部からの脅威が発生した場合の対応を行っても、その対応は運用者のオペレーションによるのが実情である。脅威発生後の対応では、自 AS 外との調整や脅威の恣意性を見極めるなど、影響の大小にかかわらず対応に一定の時間を要している。

将来必要とされる経路情報に対する脅威を軽減するサービスを考察するにあたり、現在の脅威の具体事例の分類を検知システムでの検知可否によって分類表を修正した。

表 4 検知システムを考慮した事例分類

	事前対策可能	事前対策困難
検知システムでの検知可能	事例 a 事例 d	事例 e 事例 i
検知システムでの検知不可	事例 h	それ以外の事例

上記表 4 の分類を考察すると、本章で紹介したいくつかの事例は、検知システムがあれば検知が可能であったと想定され、検知困難であったものも事前対策は可能なものに留まっている。また、本章で紹介しなかった多くの Mis-Origination の事例でも検知システムでの検知が可能と考えられる。しかしながら、経路制御の脅威に対する発生後に検知できたとしても、外部からの脅威に対する事前対策が十分に行えないこと、および、事後対策に一定以上の時間を要してしまうことが大きな課題であることが明確となっている。
つまり、検知できたことが問題解決でゴールというわけではなく、最終的には Mis-Origination が解消されることが重要である。現状、運用者の対応はあくまでも発生後の事象解消でしかない状態である。理想としては事象が起きないように抑制することであるが、まずは、発生後の対応プロセスが円滑に進められること、最終的には Mis-Origination が発生と解消することが同時に行われることが望ましい。

前項で触れたとおり、事象が発生した際に運用者が行っている対応プロセスとしては、

表 5 脅威発生時の対応プロセス

1.	Mis-Origination 検知の通知を受信する
2.	Mis-Origination 経路の広告元 AS の調査、その連絡先の調査
3.	Mis-Origination 経路の広告元 AS へ Mis-Origination を停止するよう連絡
4.	連絡が取れない場合、Mis-Origination への対抗策を取る(詳細経路の広告等)

といったものになる。対応プロセスが円滑に実施されるためには必要なサービスもしくはサービスへの要求事項は以下と考える。

A) 検知漏れや検知遅延無く Mis-Origination 検知の通知が受けられること
現状、単一の検知サービスをよりどころとした場合、サービスの停止で検知や通知が受けられないという事態になる恐れがある。また、冗長化のため、複数の検知サービスを用いるが、ひとつのサービスでは検知しているが、一方のサービスでは検知されないという情報の不一致が発生するケースがある。このようなケースでは、通知のあったサービスと通知の無かったサービスの対象監視経路から影響地域を推測することも可能となる。

B) 広告元 AS の調査および広告元への連絡が円滑にできること
自らが広告元となってしまった場合にすぐに連絡を受けられるよう、自身も連絡先を適切に WHOIS や IRR の情報を更新することが望まれる。

C) 検知サービスが IPv4 だけでなく、IPv6 にも対応している事
コンフィグレーションミスによる Mis-Origination が IPv4 以上に多く発生すると考えられる。そのため IPv6 にも問題なく対応できる機能が求められている。

D) 対応スキームを策定するにあたってのガイドラインの提供
AS 運用者もすべてが Mis-Origination への対応ができるとは限らない。運用者が Mis-Origination への対処をするにあたって、指針となるガイドラインまたはそれに準ずるものが望まれている。

最終的なゴールである Mis-Origination の発生と解消が同時に行われるためには、AS の内部および外部接続ポイントにおいて、Mis-Origination 検知と Mis-Origination 経路の破棄が必要となる。このような機能を実現するために、経路の Origin AS を第 3 者による公的証明や、経由する AS-Path を証明するサービスが将来必要となると考えられる。

最後に、今後、より安定した経路制御を維持するためには次のような情報共有、合意形成が必要と考えられる。

短期的な観点：
- Mis-Origination 等の問題を検知、通知する機能やサービス
- 広告元 AS に関する情報を一元的に提供するサービス
- 対応にあたってのガイドライン

長期的な観点：
- Mis-Origination が発生しないような機能実装
- 機能実装を実現するためのサポート体制

次章以降、短期的、および長期的観点で述べた機能を実装、提供を目指すにあたり、関連する技術動向と今後のさまざまなサービスへの活用等について述べる。

3. IRR の動向

本章では、IRR の国内外の動向や経路制御における IRR 活用の課題について述べる。

3.1. IRR サービスの運営状況

IRR サービスの運営状況について、日本国内の主要 IRR である、JPIRR とそれ以外の国際動向に分けて状況を解説する。

3.1.1. JPNIC が運営している JPIRR の状況

JPNIC では 2000 年に IRR 研究会、2001 年に IRR 企画策定専門家チームを組織して、日本における IRR の必要性を検討してきた。2002 年 8 月には IRR 企画策定専門家チームと共同で JPIRR の試験サービスを開始した。この試験サービスで得られた知見をもとに、JPNIC は 2006 年 8 月より JPIRR を正式に無償サービスとして提供開始し、現在に至っている。

JPIRR は他の IRR と登録情報のミラーリングを行っている。JPIRR をミラー元とした登録情報の提供は JPNIC が管理するアドレスブロックもしくは AS 番号を実際に利用している組織、あるいは登録情報の提供が適切であると JPNIC が判断した組織に限られている。JPIRR は原則として他の IRR からの登録情報を受け付けないが、APNIC、RIPE NCC、RADB からは登録情報の提供を受けている。RIPE NCC、RADB とのミラーリングは APNIC を経由する形で階層的な構成となっている。

JPIRR のオブジェクト登録者は IP アドレス管理指定事業者、JPNIC 管理下のプロバイダ非依存アドレス(PI アドレス)あるいは AS 番号の割り当てを受けている組織または個人に限定され、JPNIC の定める手続きを経ることで登録者としての権限が付与される。JPIRR への登録オブジェクト数は年々増加しており、主な登録オブジェクトは Maintainer を始め、Route、Route6、Aut-Num、AS-SET オブジェクト等である。

表 6 JPIRR サービスにおける登録オブジェクト数

	2010 年	2011 年	2012 年	2013 年
Maintainer	181	193	215	233
Aut-Num	277	307	339	356
AS-SET	94	105	117	124
Route	4151	4724	5133	5923
Route6			175	217

(注意：毎年 4 月時点での数値)

2011 年に JPNIC が行った調査では JPIRR に登録されている Route オブジェクトの内、8 割程度は他の IRR、特に RADB にも同様の内容が重複して登録されていた。つまり、JPIRR 登録者が他の IRR を併用している状況がうかがえる。また、RIPE RIS(*1)等の経路情報サービスで JPNIC から割り当てられた AS を観測すると、その 7 割強程度の AS が JPIRR に Route オブジェクトを登録している状況にあり、日本における JPIRR の認知度が高まってきている様子がうかがえる。

(*1) https://www.ripe.net/ris/

JPIRR では IRR として基本的なオブジェクトの登録、更新、参照機能に加えて、補助的な機能も提供されている。

IRR オブジェクトガーベージコレクターは一定期間更新の無いオブジェクトを自動的に削除する機能で、現実のネットワークと登録情報が乖離してしまう事を防ぐための機能である。現状では登録や更新から 1 年間を更新期間とし、それを過ぎても更新されなかったオブジェクトはその 3 ヵ月後に閲覧不可処理が行われ、さらにその 1 年後に削除処理が行われる。更新を促すために電子メールでの連絡も行っているが、更新を行わず削除後に再登録を行う Maintainer オブジェクトも観測されている。2011 年に JPNIC が登録者向けに行ったアンケートでは 5 割弱程度の登録者がガーベージコレクターの何らかの改善を望んでいた。

Mis-Origination が疑われる状態の通知は、JPIRR に登録された Route、Route6 オブジェクトと実際の経路変化とを比較し、異なる Origin をもつ経路情報を検知した際に、登録された電子メールアドレス宛てに通知を行う機能である。2008 年度より行って来た通知実験を 2013 年 3 月末に一旦終了し、現在は JPNIC 経路奉行の検知情報を用いて、特にサービスの終了期限を設けずに通知機能を提供している。2011 年のアンケートでは、3 割弱の登録者がより詳細な通知等の機能改善を望んでおり、また 7 割弱の登録者が現状維持や継続的な機能提供を望んでいた。

JPIRR の登録情報を検索する問い合わせは、稀に大量クエリが発生する事があるものの比較的一定数のクエリ数を観測している。JPIRR における過去 100 日程度のデータを見ると、Route オブジェクトが 1 日 8000 クエリ程度、Maintainer オブジェクトが 1 日 4000 クエリ程度、AS オブジェクトが一日 160 クエリ程度の問い合わせで推移しており、何らかの自動化ツールなど機械的な問い合わせが行われていることが推測される。ただし、日によっては突然 70 万クエリまで問い合わせが増えた例も観測されている。2011 年のアンケート

では、3 割程度の登録者がより安定性の高いシステムを求めているが、7 割弱程度の登録者が現状と同程度の安定性を維持して欲しいと回答している。

3.1.2. 世界の IRR の状況

IRR の基本的なコンセプトは 1980 年代に NSFNet で利用されていた Policy based Routing Database (PRDB)にさかのぼる。NSFNet に接続する組織は Network Announcement Change Requests (NACR)を、PRDB を運用する Merit Inc.へ送っていた。Metric は送られてきた NACR をチェックした後、データベースへ登録し、Exterior Nodal Switching Subsystem (ENSS)と呼ばれるルータの設定ファイルを生成、各ルータへ送って経路制御プロセスを再起動、設定内容の反映を行っていた。(*2, *3)

NACR はネットワークアドレス、ネットワークの名前、組織名、組織の住所、origin AS 番号、AS パスリストなどを含み、ほぼ現在 IRR で利用されているポリシー情報と同じ情報を含んでいた。

その後 1995 年の NSFNet の終了にともない各プロバイダの接続地点(Network Access Point)での経路制御のために Routing Arbiter プロジェクトが発足、ポリシー情報も PRDB を原型とし RIPE/NCC によって開発された RIPE-181(RIPE-81+とも呼ばれた)に変更された。RIPE-181 では NACR に加え、より細かな経路の広告・受信ポリシーが記述できるようになっていた。その後、RIPE-181 は IETF での標準化を経て、RFC1786 となり、さらにはより一般化した Routing Policy Specification Language (RPSL)として標準化が続けられ、RFC2280/RFC2622/RFC4012 と更新が加えられていった。

(*2) WIDE プロジェクト 1994 年度 研究報告書
http://www.wide.ad.jp/project/document/reports/pdf1994/index.htm
(*3) JPNIC における IRR サービスに関する検討報告書
https://www.nic.ad.jp/ja/materials/irr/irr-report-2003.html

当初 IRR サービスを提供していたのは限られた組織であったが、1999 年後半に Metric が RADB を有料化するにあたって、IRR サーバソフトウェアを無償で提供開始し、当初 5 か所程度であった IRR サービスは現在では、Merit が管理しているリスト(*4)に載っているものだけでも 35 にも達している。RIR/NIR や研究組織などによって運営されている IRR サービスが多いが、IX や ISP などの営利組織によって運営されているものも多い。

(*4) List of Routing Registries

http://www.irr.net/docs/list.html

2013-07-15 現在、各 IRR サービスで保持されている route object の数は次の通り。(括弧内が route object の数を示す。名称は source: より。)

---

radb ********** (556849)
ripe ********** (216679)
nttcom ********** (173142)
level3 ******** (87882)
savvis ******** (84921)
apnic ******** (83583)
bell ** (29497)
reach ** (25073)
arin ** (20785)
altdb * (12346)
epoch ……..(8658)
jpirr ……(6242)

('*' = 10,000 '.' = 1,000)

上記より、IRR サービスの中では RADB が最もよく使われており、次いで RIPE、NTTCOM の IRR、そして Level3、Savvis、APNIC の IRR へ多くのデータが登録されていることが分かる。

なお、IRR のデータは経路フィルタの作成にしばしば使われており、下述「IRR の活用動向」で述べる理由により多くの「無駄な」(つまり、実際の経路広告と一致しない)データが登録される場合があるため、登録されているデータの量がすなわち利用状況とはならないが、一つの目安にはなるだろうと考えている。

また、route object の重複登録の状況を確認したところ、RADB に登録されている route object のうち約 2/5 が、RADB 以外の IRR にも登録されていることが分かった。(なお、route object の合計が上記の数字と異なるのは、下記では RADB 内で重複して登録されている route object を排除するからである。)

**********..... (496726)
198060 298666

('*' = exist in radb AND other IRR '.' = exist ONLY in radb)

同時に RADB における約 3/5 のデータは RADB にしか存在しておらず、IRR サービスにおける RADB の重要性が表れている。(にもかかわらず過去に、RADB の会員資格を更新し損なったことによって IRR のデータが削除され、経路障害につながった事例は多く存在する。)

次に、IRR サービスへの経路の登録状況を見てみると、下述「IRR の活用動向」の通り、IRR のデータを経路フィルタに使っている ISP が複数存在する(主に欧州の ISP に多い)ため、多くの ISP が IRR へ経路の登録を行っている。そのような中で大手では、AT&T、Sprint、Verizon が IRR への登録を行っていないことが知られている。(各社ともいわゆる Tier1 ISP であり、Tier1 ISP 同士は細かい経路フィルタを行っていないため、IRR への登録の必要性が低いものと推測される。)

また、nLayer の Steenburgen による 2008 年の調査(*5)によると、BGP で経路広告されているにも関わらず IRR に登録されて*いない*経路が 30%以上も存在していたことが分かっている。つまり IRR への登録は一般的にはなっているが、そのデータに基づいた経路フィルタは必ずしも一般的にはなっていないことを示している。(ただし、70%程度の経路は IRR に正しく登録されていた、ということも示している。) 同調査によると当時 IRR に登録されていた約 37 万経路のうち約 24 万経路は BGP によって広告されておらず、IRR におけるデータの信頼性は必ずしも高くなかったと言える。(IRR を経路フィルタに使う場合、ユーザー側に古いデータを削除する積極的な理由が発生しないためと推測できる。) これらが主因となり、経路フィルタに IRR のデータが広く使われてはいなかった理由の一端であると思われる。

(*5) Examining the validity of IRR data
http://www.nanog.org/meetings/nanog44/presentations/Tuesday/RAS_irrdata_N44.pdf

他方、2010 年の RIPE NCC の調査(*6)によると、RIPE NCC から割り当てられ BGP で広告されている IPv4 経路のうち 95%が ripe の IRR に登録されていたことが分かっている。これは欧州における IRR のネットワークオペレーションへの利用率の高さと、IP アドレスの割り当てと IRR の運用を一体で行うことの有効性を示していると考えられる。

(*6) Interesting Graph - How Complete is the RIPE Routing Registry
https://labs.ripe.net/Members/mirjam/interesting-graph-how-complete-is-the-ripe-routing-registry

しかし同時に、2011 年 10 月から 2012 年 9 月の期間に Arbor Networks が行った調査(*7)によると、調査対象 ISP のうち 48%しか IRR への顧客経路の登録を行っていなかった。つまり、今日においても未だに IRR への経路の登録状況は、調査の母集団(地域・ISP)によって大きな差異が存在していると言えるだろう。

(*7) Worldwide Infrastructure Security Report
http://pages.arbornetworks.com/rs/arbor/images/WISR2012_EN.pdf

3.2. IRR の活用動向

現在、もっとも典型的な IRR の活用方法は、ISP による BGP 顧客へ(もしくはピアリングパートナー同士)の経路フィルタの自動生成だろう。ISP の顧客は route object、aut-num object、as-set object などの IRR オブジェクト(データ形式)を利用して ISP へ BGP にて広告する経路を登録する。ISP は BGP 顧客の AS 番号や、顧客に指定された as-set object をキーに IRR を検索、顧客が広告してくる経路のリストを得る。その後、経路のリストをルータの設定ファイルへと整形し、実際の設定へと反映させる。ルータの設定ファイルへの整形に関しても、IRRToolSet (*8)に含まれる RtConfig を使用することで access list や prefix list、ある程度の経路ポリシーの設定などを IRR のデータから自動的に生成することができる。そうすることで、同一ネットワーク内で一つのデータベース(IRR)から一貫した設定を生成・使用することができるようになる。

(*8) IRRToolSet
http://www.isc.org/software/irrtoolset

具体的には以下の通り。まず、IRR へ広告する経路(route object)を登録する。その際、併せて origin AS となる AS(Aut-Num object)も登録する。登録は通常、メールで簡単に行える。

```
route:   192.41.192.0/24
origin: AS2515
mnt-by: MAINT-AS2515
source: RADB

aut-num: AS2515
as-name: ASN-JPNIC
mnt-by:   MAINT-AS2515
```

```
source:  RADB
```

経路情報の登録は以上で終わり。あとは、ISP が登録された情報を検索するだけだが、その際のキーとしてたとえば AS 番号を使うと、

```
% whois -h whois.radb.net ¥!gAS2515
A113
192.41.192.0/24  202.12.30.0/24  211.120.248.0/24  211.120.240.0/21  202.12.30.0/24
192.41.192.0/24 211.120.240.0/21
C
```

といった具合に、AS2515 が IRR へ登録した「AS2515 が広告する経路」を簡単に列挙することができる。あとは、このリストを使い、

```
routing policy for as2515 {
        if included in (list of routes from as2515);
        then accept;
        else reject;
}
```

などと(実際のルータの設定ファイルの形式で)書くことができる。

このような手法で経路フィルタを生成している ISP は複数存在するが、それによって顧客による「無駄な」データの登録が発生する場合がある。たとえば、顧客が複数の ISP と契約をしており、何らかの基準に基づいてそれらの ISP を使い分けたい場合、BGP の attribute によって優先経路を操作する場合もあるが、一方経路広告そのもの(経路広告の有無、経路の最長一致の操作)によって使い分ける場合もある。後者の場合、顧客は ISP に対して経路を広告したり停止したり、より長いマスク長の経路を広告するなどをする場合がある。もし ISP が exact match による経路フィルタをしていた場合、新しい経路の広告時や、マスク長の異なる経路の広告時には都度 IRR への経路の登録が必要となり、即時性が求められる場合には障害となる。そこで、たとえば通常広告している経路が/16 とした場合、/16 から/24 までの考えられるすべてのプレフィックス(256 個)を IRR に登録している例も存在する。この場合、通常は/16 しか経路広告していないとすると、IRR における残りの 255 個のデータは「無駄な」ものとなる。

IRR へは通常「広告する経路」を登録するものであり、上記のような登録は変則的であるため、たとえば ISP 側で exact match だけではなく、longer な経路を受け取るなどの対応をとるか、そもそも BGP attribute を使った経路操作をするのが現実的だろう。

3.3. ルートサーバなどでの IRR 活用事例

ルートサーバとは、広義には経路収集、監視サーバなど経路情報管理に関するサービス全体も含まれるが、本報告書では、IX 上でトラフィックを運ぶために BGP 経路交換を仲介する機能を担うルートサーバの活用事例を解説する。

ルートサーバは、BGP の運用に伴い必然的に発生する、ピアリング交渉や経路広報管理の負荷を緩和することを主目的とした機能である。通常、IX などにおける経路交換は経路情報の交換を希望する組織同士が交渉し、それぞれピアを設定することで成立する。当然、ピア数が 1,2,3,,,N と増えていくごとにピアの Prefix や AS-PATH の管理も増大する。

ルートサーバを使うことで、ピアは個別に経路交換交渉をすることなく、ルートサーバに参加する組織全体で経路交換を一つのピアで行うことができるため、前述のような管理コストの増大が緩和される。

実際のルートサーバの動作は、基本的にルートサーバに参加するピアから経路広報された経路の BGP Attribute を変更せず、他の参加ピアへ経路広報する。

このとき、正しい経路のみをルートサーバ参加ピアへ経路広報するためのツールとして IRR が活用されている。IRR を使わない場合、個別にルートサーバへ Prefix フィルタや AS-PATH フィルタを設定する作業が必要であるが、ルートサーバ利用者が IRR に as-set オブジェクトなどを登録することにより、ルートサーバシステムはそれを展開し各種フィルタを作成することができる。これにより、ルートサーバ利用者は IRR の情報をメンテナンスするだけで、自動的にルートサーバの経路フィルタを更新させることができる。さらに高度な利用方法として、AMS-IX(*9)では IRR の import/export フィールドに RPSL で記載されたルーティングポリシーをルートサーバに反映させ、経路広報先をルートサーバ上で制御させる活用事例がある。

(*9)https://www.ams-ix.net/technical/specifications-descriptions/ams-ix-route-servers

他に IRR がよく使われる場面はネットワークのトラブルシューティングだろう。ネットワークのトラブルシューティングに際しては、たとえば traceroute などを使い通信経路を把

握した上で問題が発生していると考えられるポイントのIPアドレスを管理している組織にコンタクトをする。その際、参考にするのが、IP アドレスそのもののレジストリ情報に加え、そのIPアドレスを含むネットワークのIRRへの登録、及びそのネットワークを広告するASの登録を参照する。それによって管理組織のメールアドレスなどのコンタクト先だけでなく、IRRに登録されている経路のマスク長・origin ASなどと実際の経路広告を比較することができ、経路広告が正しく行われているかを簡単にチェックすることができる。(ただし、IRRの登録が実態に即していない(最新の情報に更新されていない)ことも多く、差異があるからといって即、不正とは限らないため、いずれにせよ管理組織への確認は必要となっている。)

さらに前述の通り、上記のようなチェックを自動的に行うことでMis-Originationの検知や、より一般的に経路ポリシーに反している経路広告の検知などにも使われている。

3.4. 経路制御におけるIRR活用の課題

IRR ではオブジェクトの登録・更新は簡便に行える一方、利用者側の立場にたつと登録情報の扱いが難しい事が課題として挙げられる。例えば、登録場所、名前空間、データの信頼性など登録情報を参照する際に利用者が配慮しなければならない事項がある。

まず、利用者は登録情報を参照する際に適切なIRRを選ばなければならない。
IRRでは広く利用されているRADBの他、レジストリが運用するIRRやISPが顧客の情報を登録するために利用しているIRR等があり、登録者がどのIRRに情報を登録したかを探して参照する必要がある。IRR は利用者に便宜を図るため、ミラーリングで登録情報を受け付けて、他のIRRの登録情報が参照できるようにしているが、全てが網羅されているわけではない。また、どの時点でミラーリングされたデータかも分かりにくいため、一部ISPでは参照に必要なIRRの登録情報を手元にミラーリングして利用している。

オブジェクトの名前空間はIRR毎に独立している。このため、複数のIRRの登録情報を比較した場合、同名でありながらも異なるオブジェクト登録されている場合がある。これは登録者がオブジェクトの名前を決められるMaintainerオブジェクトやAS-Setオブジェクト等で発生する課題である。AS-Setオブジェクトではmembersとして他のAS-Setオブジェクトを登録することが可能であり、利用者はこれを経路フィルタに展開する際に適切に再帰参照しなければならない。しかも一部オブジェクトではIRRを跨ってAS-Setオブジェクトを再帰参照させる事例も有り、利用者はこれらオブジェクトを参照する際は特に注意が必要となる。

そして何より参照で得られた登録情報の信頼性が課題となる。RIR 等のインターネットレジストリが提供する IRR では、割り振られたアドレスブロックしか Route, Route6 オブジェクトに登録できないなど、一定の制限をかけられている場合もあるが、広く利用されている RADB では登録者が好きなオブジェクトを登録できるため、登録された情報をどれだけ信頼できるかは利用者側で判断するしかない。登録者によっては、受信した顧客経路情報をそのまま IRR に代理登録する様な運用を行っているところもあり、信頼性という観点からはかなり疑問が残る。JPIRR ではガーベージコレクター機能を導入して不要になったオブジェクトの削除に取り組んでいるが、他の IRR では登録者が削除するまで登録されたままとなっている。

この様な状況で ISP によっては IRR に必要な情報は登録するものの、信頼性に疑問が残るので経路フィルタを自動生成するといった登録情報の活用を止めてしまった所もある。一方で、自らが登録した情報であれば信頼できるため、自社の経路制御ポリシーを細かく IRR に記述し、そこからルータの設定を自動生成する ISP もある。また、IRR では Aut-Num オブジェクト等に自由書式でピアリングのポリシーや連絡先を記載する事例もあったが、PeeringDB 等、別なサービスを利用してこれら情報を登録する事例も増えて来ている。

IRR の活用においては IRR サービスの安定稼働も課題となる。IRR のサービスが停止すると、登録情報の更新が行えないばかりか、登録情報の参照が出来ない場合もある。経路制御の運用に IRR を活用するためには、少なくとも IRR が継続的に提供されるサービスであり、ある程度の安定稼働が担保される必要がある。ただ、IRR という性質上、それほど緊急の更新は多くないため、定期的なメンテナンス程度は許容範囲だと考えられる。

4. RPKI の動向

本章では、RPKI に関する国内外の動向、RPKI の活用モデル、また普及に向けた今後の課題について述べる。

4.1. RPKI の国際動向

4.1.1. レジストリのサービス提供状況

各 RIR では早い段階から RPKI の標準化に参加したり、実験サービスを行ったり、などを継続して RPKI の実現に関わってきた。現時点で全ての RIR が RPKI の正式サービスを開始しており、ROA の発行等が出来る状況にある。

Table 1 各 RIR の RPKI サービス紹介ページ

AfriNIC
- https://www.afrinic.net/en/initiatives/resource-certification
APNIC
- https://www.apnic.net/services/services-apnic-provides/resource-certification
ARIN
- https://www.arin.net/resources/rpki/
LACNIC
- https://lacnic.net/en/rpki/
RIPE NCC
- https://www.ripe.net/lir-services/resource-management/certification

RIR は LIR/NIR 向けにポータル web サイトを運用しており、そのシステム自体やそのユーザー認証システムを利用して、ユーザーが RPKI の操作を行えるシステムを構築している。どのシステムも web サイトを通じて最低限 ROA の生成と発行までの機能は持っている。また AfriNIC 以外は、NIR/LIR が独自の認証局と RPKI システムを運用できるように、up/down プロトコルも既にサポートしている。RIPE NCC が公開している情報(*10)によると、各 RIR で発行されているリソース証明書は概ね増え続けており、特に RIPE 地域でここ数年継続的な伸びを見せている。

(*10)http://certification-stats.ripe.net/

一部 RIR では RPKI の普及促進のために、付加的なサービスを提供している。

RIPE NCC ではRPKIデータの収集と検証を行えるようにRPKI Validator(*11)というツールを開発して提供している。このツールを RPKI Cache として動作ささせ、実際の経路情報と比較できるテストベッドルータも公開されている。また LACNIC では web インターフェイスで実際の経路と RPKI データを検証できるように Origin Validation Looking Glass(*12)を運用している。

(*11)https://www.ripe.net/lir-services/resource-management/certification/tools-and-resources
(*12)https://www.labs.lacnic.net/rpkitools/looking_glass/

各 RIR がそれぞれ RPKI の信頼の拠点となるトラストアンカーを公開しているが、その構成は RIR によって異なっている。例えば APNIC はインターネットリソースの割り振り元に応じて 5 つのトラストアンカーで運用しているが、他のすべての RIR ではそれぞれ 1 つのトラストアンカーで運用している。また、どのインターネットリソースに証明書を発行するかのポリシーも異なっている。例えば RIPE NCC では AS 番号のリソース証明書を発行していないし、Early Registration Transfer(ERX)のアドレスブロックや歴史的 PI アドレスに関しては各 RIR でまだ完全には網羅されていない。つまり現状ではインターネットリソースに網羅的に証明書を発行できる状況にはまだ至っておらず、また、ERX や移転されたインターネットリソースなどに関しては、各 RIR で一部重複した証明書が存在する状況でもある。
APNIC 等の一部地域では NIR が RIR と協力しながらインターネットリソースの分配を担っている。これら NIR 配下で RPKI を利用しようとした場合には、NIR での RPKI 対応が必須となる。現状では JPNIC を始め、どの NIR も RPKI に対応しておらず、NIR から分配されたインターネットリソースには証明書を発行できない状況である。

4.1.2. ルータとサーバの実装状況

RPKI による ROA Origin Validation を実現するためには、大別すると以下の 5 つの機能が必要である。

機能 A) CA(Certificate Authority)機能
Prefix や AS のリソース証明書および ROA を発行または公開する機能。

機能 B) ROA キャッシュサーバ(RPKI RTR サーバ)機能/RFC6810
CA サーバから取得した ROA を検証し、キャッシュとして保存する機能。また、RPKI RTR クライアントに対して、正当な ROA を提供する機能。

機能 C) RPKI RTR クライアント機能/RFC6810
定期的に ROA キャッシュサーバと通信し、ROA を取得する機能。

機能 D) BGP Prefix Origin Validation 機能/RFC6811
取得した ROA をルータ内（のメモリ上）に保存し、受信した BGP UPDATE の内容と比較検証する機能。

機能 E) BGP 経路制御機能
機能 D の検証結果に基づき、受信した BGP UPDATE の制御を行う機能。実装依存であるが、例として、以下のような制御が可能である。

例 1)Invalid 経路を RIB にインストールしない
例 2)判定結果に応じて Local Preference 値を変更する
例 3)iBGP ピアに該当の BGP UPDATE を伝播させる際に、判定結果に応じた Extended Community を付与する（draft-ietf-sidr-origin-validation-signaling）

上記の 5 つの機能のうち、一般的に機能 A は”Issuing Party”、機能 B～E は”Relying Party”と呼ばれる。 機能 B および C の実装状況は、2012 年 3 月時点での資料であるが、draft-ietf-sidr-rpki-rtrt-impl にまとめられている。 この報告によると、ルータベンダの実装としては、

・IOS(Cisco)
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-s/irg-origin-as.html

・IOS-XR(Cisco)
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.2/routing/configuration/
guide/b_routing_cg42asr9k_chapter_01011.html

・JUNOS(Juniper)
http://www.juniper.net/techpubs/en_US/junos12.2/information-products/topic-collections/
release-notes/12.2/junos-release-notes-12.2.pdf

の３つが存在し、その他オープンソースなどによるソフトウェア実装として、

・RPKI Tools(rpki.net)
https://trac.rpki.net/

・RPKI Validator(RIPE NCC)
https://github.com/RIPE-NCC/rpki-validator

・RPSTIR(BBN Technologies)
http://sourceforge.net/projects/rpstir/

・RTRlib/quagga(rpki.realmv6.org)
http://rpki.realmv6.org/

の４つが存在する。また、RPKI RTR プロトコルの機能において、未実装もしくはテスト段階のものも見受けられる。特に、ルータベンダ系の OS としては Serial Notify を受信（ROA キャッシュからの差分更新）する機能や RPKI RTR プロトコルのセッション暗号化機能が未実装のものがあることがわかる。

本報告の他にも、2013 年 7 月現在では以下の３つの実装が公開されている。

・IOS-XE(Cisco)
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-origin-as.html
・BGP-SRx/quagga(NIST)
http://www-x.antd.nist.gov/bgpsrx/
・bird(CZ.NIC)
http://bird.network.cz/

これらの実装について、前述の 5 つの機能の主な実装状況をまとめたものが下表である。

表 7 RPKI システムの実装状況一覧

	機能 A	機能 B	機能 C	機能 D	機能 E
RPKI Tools	YES	YES	NO	NO	NO
RPSTIR	NO	YES	NO	NO	NO
RTRlib/quagga	NO	NO	YES	YES	YES
RPKI Validator	NO	YES	NO	NO	NO
IOS, IOS-XE, IOS-XR	NO	NO	YES	YES	YES

JUNOS	NO	NO	YES	YES	YES
BGP-SRx/quagga	NO	NO	YES	YES	YES
Bird	NO	NO	NO	YES	YES

4.2. RPKI の標準化動向

RPKI の標準化は IETF の SIDR ワーキンググループを母体として行われている。以下に 2013 年 7 月時点での RPKI 関連文書の概要を示す。

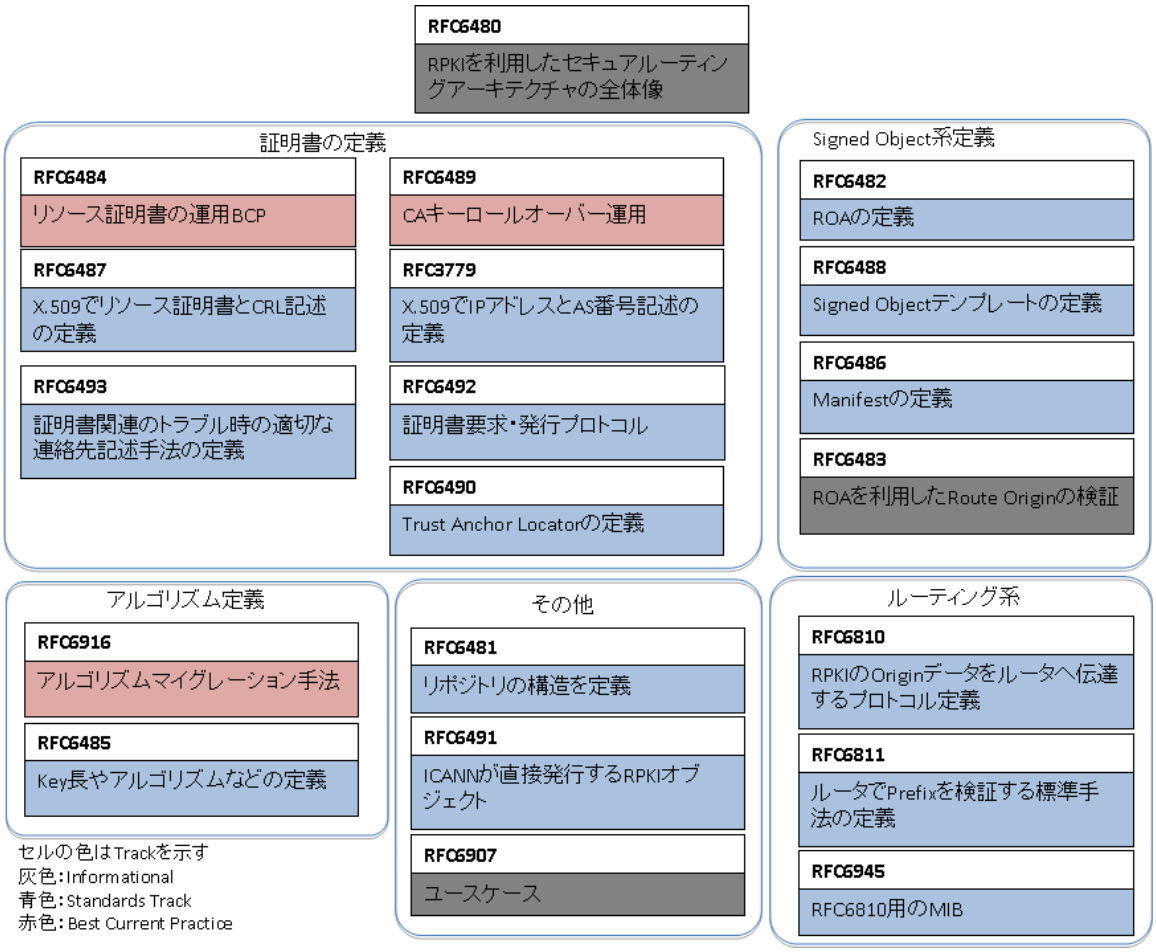

図 1 RPKI 関連 RFC の分類

RFC6480 が RPKI を利用したセキュアルーティングアーキテクチャを記述した文章である。2007 年 2 月に初版がでてから 2012 年 2 月に RFC として発行、RFC 発行までの間約 5 年もかかっている(この間に筆者が 1 名入れ替わっている)。5 年の年月を要しているが、これは同時に 14 個の文章を RFC 化しており、各文書が相互に補完関係を持つなど非常に複雑な標準化プロセスであった事が要因の一つである。またこの初期発行 RFC のほとんどが BBN Technologies と APNIC の社員によって書かれている事も特質すべき点である。

RPKI の根幹部分となるリソース証明書や Signed Objects に関する標準化は大部分が完了しており、標準化の議論はより実用面にフォーカスしたフェーズへと移行している。特に、初期段階では Origin Validation に特化して議論を進めていたが、現時点では Path Validation(draft-ietf-sidr-bgpsec-req)の実現手法に議論が及び、実現手段としての BGPSEC 標準化に向けた作業が進められている。同時に、運用事例やテスト運用を通して発見された課題の解決に向けた議論が活発になってきている。

IETF で標準化されたリソース証明書を RIR/NIR がサービスとして提供し（適切なリソースホルダーであるという事と証明）、それを用いて Origin Validation を試す実験がオペレータ有志で行われ、その結果がまた IETF 標準化へ反映されるプロセスが行われている。実際に RPKI をサービスへ用いている ISP はほとんどいないが、標準化を進めながら ISP 運用者の知見が反映されながら標準の改善が継続的に行われている。

4.3. RPKI の国内動向

4.3.1. 国内の RPKI に関する活動

日本の RPKI に関する活動は、国内の専門家による IETF SIDR ワーキングループへの参加や internet-draft への提言を行ってきた。最近は、標準化動向の把握と国内への周知がここ数年にわたり実施されている。

具体的な普及・啓発活動としては、2010 年 1 月に東京 IIJ オフィスにて開催された IIJ Randy 氏、松崎氏らによる RPKI workshop 以後、複数の普及・啓発活動が行われている。2010 年の RPKI workshop では、RPKI に関するソフトウェアやルータの初期実装を集まった参加者で試行錯誤をしながら試す形で行われた。RPKI workshop では、経路運用者による RPKI の今後に関する議論が行われ、今後必要な機能や実装について意見交換を行うに至った。

2011 年には、主要な BGP ルータベンダより、RPKI による Origin AS Validation が商用リリースされ、先進的な経路運用者の興味が高まりつつあった。

その後、2012 年になり、RPKI ソフトェアと複数ルータの実装が出揃い、JPNIC とインターネットマルチフィード社による検証が行われ、RPKI の機能を搭載したルータの技術検証が行われた。一部のソフトウェアに問題はあるものの、基本的な RPKI 関連機能は十分試用に耐えうることが明らかとなった。またルータの機能追加や実装上の不具合等を発見するなど、いくつかフィードバックの実施も行われ、APNIC31 国際会議での RPKI Bof(**)でも取り組み状況が報告された。

このように 2010 年ごろから徐々に日本国内でも RPKI に関する様々な活動が開始されてきており、経路運用者の RPKI に関する関心度も高まってきた。のち 2013 年 1 月に日本ネットワークオペレーターズグループにおいて、RPKI に関するワーキンググループ「RPKI ルーティングを試す会」が立ち上がった。

4.3.2. 国内の RPKI に関する最新状況

- JANOG ワーキンググループ「RPKI ルーティングを試す会」（RPKIWG）

RPKI WG は、RPKI を使ったルーティングに関わる現在の実装状況とそして今後どのような運用の形になっていくかをテーマとする WG である。主に RPKI の実装を動かしてみることを通じて構造や運用のポイントなどについて情報共有することを目標としている。

RPKIWG の具体的な活動として、RPKI を使ったルーティングに関わる現在の実装状況と今後運用にどのような影響があるのかを確認したり把握したりすることを目的としており、実際に RPKI を使ったルーティングを体験し試用する活動として、2013 年 1 月から 7 月にかけての半年間でハッカソン(hack-athon：アプリケーションをインストール・改善をマラソンのようにプログラミング言語、OS 設定を調整しながら試行する活動)、ハンズオンといった体験型のイベントを行い、ディスカッションを通じて課題点を挙げるといった活動が行われた。実施された活動は「(1)RPKI ハッカソン」「(2)RPKI ハンズオン」「(3)RPKI セッション」の三つに大別される。

表 8 RPKI を試す会 メンバー概要

＊RPKI ルーティングを試す会	
－チェア	
インターネットマルチフィード	吉田 友哉
JPNIC	木村 泰司
－試す会メンバー	約 50 名

(1)RPKI ハッカソン

RPKI ハッカソンは、RPKI の実装についての資料が比較的少ない中で 2 回行われた。RPKI ソフトウェア開発者による 2010 年の RPKI Workshop と同様の位置付けで開催された。

表 9 RPKI ハッカソンの開催概要

2013 年 1 月 23 日(水) 15:00-18:30 IIJ 会議室(*13)
2013 年 2 月 20 日(水) 10:30-18:00 JPNIC 会議室(*14)
(*13)第 1 回 RPKI ハッカソン

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1053.html

(*14)第 2 回 RPKI ハッカソン
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1058.html

第 1 回のハッカソンでは、一部の参加者のみ動作確認に成功した。1 回目の結果を受け、RPKI Tools の開発者が毎回来日し、逐次修正を加えていくことで、第 2 回のハッカソンでは全員が RPKI を使った BGP ルータにおける Validation 結果を確認することができた。またハッカソンのラップアップとして、第 1 回と同時期に行われた JANOG31 ミーティングにおいて BoF が開催された。

RPKI ハッカソンの経過と感想（JANOG31 BoF）
http://www.janog.gr.jp/meeting/janog31/program/RPKI.html

(2)RPKI ハンズオン

RPKI ハッカソンに引き続き、より"一連の動作を体験する"ことに注目したのが RPKI ハンズオン活動である。

表 10 RPKI ハンズオン開催概要

2013 年 4 月 26 日(金) 13:00-17:00 ENOG20(新潟)(*15)
2013 年 5 月 17 日(金) 10:00-13:00 電力系 NCC 勉強会(仙台)

(*15) ENOG20 Meeting 開催のお知らせ
http://enog.jp/archives/902

RPKI ハンズオンは、前半に RPKI を知るための勉強会を行い、後半に実際の動作を体験する形で実施された。特に後半は、あらかじめ必要なソフトウェアがインストールされた仮想マシンを使って、ステップバイステップでコマンド入力などを行った。

(3)RPKI セッション
JANOG32 における「RPKI セッション」と「RPKI routing WG 報告」

2013 年 7 月には JANOG32 において、チュートリアルとして「RPKI セッション」と、"RPKI ルーティングを試す会"の活動報告として「RPKI routing WG 報告」の二つが行われた。

表 11 RPKI を試す会 JANOG でのアクティビティ

2013 年 7 月 3 日(水) 13:00-18:30 JANOG32 チュートリアル(大阪)(*16)
2013 年 7 月 5 日(金) 15:10-16:00 RPKI routing WG 報告(*17)

(*16) RPKI セッション | JANOG32 Meeting
http://www.janog.gr.jp/meeting/janog32/tutorial/RPKI.html

(*17) RPKI routing WG 報告 | JANOG32 Meeting
http://www.janog.gr.jp/meeting/janog32/program/rpki.html

RPKI セッションは、RIR のミーティングなど同様のセッションを開かれている Randy Bush 氏によるハンズオン形式のセミナーであり、RPKI routing WG 報告の時間には、これまでの活動を通じて見えてきた、RPKI ルーティングの全体像や導入の具体的な課題が紹介された。

- 国内の RPKI ルーティング導入の課題に関する議論

RPKI ルーティングは、BGP を使って伝播していく経路情報のうち、誤って経路広告されたもの、具体的には本来の IP アドレスの割り当て先とは異なる AS による間違った経路情報を途中でフィルタリングし、インターネット全体から見て局所化することのできる技術であると言える。

これまでのハンズオンや JANOG32 における WG のセッションで議論されてきたことを踏まえ、RPKI ルーティングの導入にあたっての課題をまとめた。

○RPKI のリソース証明書と ROA に関わる業務に関する課題

RPKI を使うためには、JPNIC の IP レジストリシステムや JPIRR に加えて、ISP 等の IP アドレスの割り振り先組織によって、リソース証明書を発行し、また AS 番号が記載された ROA を発行する必要がある。つまり、ISP 等における IP アドレスの管理を担当者や場合によっては IP アドレスの割り当てを受ける顧客が、インターネットとの接続性を持つための AS 番号を把握し、ROA を発行することが必要となっている。この一連の流れの制度設計自体が課題とされた。

○BGP を使ったルーティングの安定運用

リソース証明書や ROA を使った検証結果が Invalid、すなわち無効となるような経路が検知された場合、その経路の取り扱いに注意が必要とされる。実際には Invalid となった経路は参照せずに破棄すべきと考えられるが、RPKI・ROA が経路運用に与える影響を考慮すると、全 AS で一律にそうすべきであるのか、今後の議論が必要と考えられる。

- 今後

2013 年 8 月現在、JPNIC の実験による RPKI システムが国内運用者に提供されて おり、経路運用者の RPKI 体験が増えるに連れ今後議論が活発になり、普及に向けた課題解決と新たな問題への取り組みがなされると予想される。

4.4. RPKI 活用モデル

RPKI の活用モデルとしては、ROA を利用した経路情報の検証やインターネットリソースを保持していることの証明が考えられる。

1) 不整合検知

経路奉行などと同じく、パケット転送と直接関わりのないところで BGP の経路 情報と RPKI Cache を比較し、単に不正経路が発生していないかを監視するモデ ル。不正経路の流通をいち早く把握し、その後の対応を行うために運用する。 また、RPKI の登録情報に異常が無いかを確認するためにも有効である。

2) 顧客経路フィルタ

顧客 AS から受信する経路と RPKI Cache を比較し、検証成功した経路のみにトラ ンジットを提供するモデル。顧客向け経路受信フィルタの運用を自動化することが可能となるが、RPKI に依存した構成となるため、トラストアンカーの選定やホワイトリストの併用などを検討する必要がある。

3) ピア/上流からの受信経路制御

ピアや上流から受信する経路と RPKI Cache を比較し、検証結果に応じて経路フィルタや優先度制御、タグ付けを行うモデル。経路フィルタを行うことで不正広報の流通を即座に阻止できる可能性があるが、RPKI に依存した構成となるため、トラストアンカーの選定やホワイトリストの併用などを検討する必要がある。優先制御では、場合によっては最適経

路の選出プロセスで不正広報が AS 内で採用されてしまう可能性も残る。タグ付けに関しては、AS 内で別途経路制御を行ったり、RPKI 環境を持たない顧客向けに検証の結果を経路情報に付加して提供したり、といった活用方法が考えられる。

4) IX の route-server

幾つかの IX で接続 AS 間の経路交換用に route-server が提供されている。ここで交換されている経路情報と RPKI Cache を比較し、検証結果に応じて経路フィルタや優先度制御、タグ付けを行うモデル。経路フィルタを行うことで不正広報の流通を即座に阻止できる可能性があるが、RPKI に依存した構成となるため、トラストアンカーの選定やホワイトリストの併用などを検討する必要がある。優先制御では、場合によっては最適経路の選出プロセスで不正広報が採用されてしまう可能性も残る。タグ付けに関しては、RPKI 環境を持たない接続 AS 向けに検証の結果を経路情報に付加して提供するといった活用方法が考えられる。

5) IRR への自動オブジェクト登録

登録された ROA の情報を元に、自動的に Route や Route6 オブジェクトを生成して IRR で公開するモデル。IRR と RPKI を併用する利用者の負荷を軽減でき、既存の IRR を活用する自動化ツール群もそのまま利用できる可能性が高い。ただし、RPKI では ROA でプレフィックス毎に広報し得る最長プレフィックス長を設定できる。これは IRR には無い機能であり、全ての対応するプレフィックス長に展開して IRR のオブジェクトとして登録すると、膨大なオブジェクト数になる可能性もあるため、どのように登録するかの検討が必要である。

6) 持ち込みアドレスの認証

ISP に PI アドレス等、ユーザーが保持しているアドレスブロックを持ち込んで利用する場合に、利用の正当性を RPKI の証明書を利用して検証可能とするモデル。APNIC ではファイルやテキストに RPKI の証明書を付加できる機能を提供しており、これを利用して ISP 側で正当性を検証する事ができる。 リプレイ攻撃のリスクを軽減するため証明書を付加するファイルやテキストを工夫したり、証明書の有効期限に注意したりする必要が有る。あるいはユーザーが ROA を発行することで、確かにアドレスの保持者が ISP に経路広報を委託したことを検証することもできる。

7) リソース保持の証明

IP アドレス移転を行う際等に、該当リソースの保持を RPKI の証明書を利用して検証可能とするモデル。 APNIC ではファイルやテキストに RPKI の証明書を付加できる機能を提供しており、これを利用して正当性を検証する事ができる。リプレイ攻撃のリスクを軽減

するため証明書を付加するファイルやテキストを工夫したり、証明書の有効期限に注意したりする必要が有る。

4.5. RPKI 普及に向けた課題

RPKI 普及の最大の課題は大きく二つに分類できる。

(ア) PKI は多くのネットワーク技術者にとって難解な仕組みである事である。
今までその運用にあまり慣れていないため、リスクポイントの判断、安定に運用するための工夫、必要となる投資のレベル感などのスキルが不足している。
(イ) ルーティングセキュリティを保つ投資対効果の不透明性
今までルーティングのセキュリティを向上させるためにプロバイダがコストをかける必要はほとんど存在しなかったと言われる。ルータそのもののセキュリティはベンダへ委ね、プロトコルの脆弱性に起因する経路 Mis-Origination への対応は発生後に運用で対処しており、それ以外の事例については、基本的に一時しのぎで対応してきた。

1 点目に関しては、既にテストベッドを通してネットワーク技術者の感を養う土壌ができつつある。また、RPKI に関するチュートリアルを通して、技術者を育成する取組も国内外で徐々に増えつつある。
ただし、DNSSEC でも明らかなように、どんなに準備して運用に望んでも、PKI の運用では、致命的な断を発生させてしまう失敗が発生する可能性がある。また DNS 運用とルーティング運用が PKI に関するノウハウを共有しながら運用していく事で、この改善は期待できる。一方で、DNS やルーティングを運用する必要のある技術者は、今まで PKI を運用する技術者の数よりも圧倒的に多い。様々なレベルの技術者の関与がインターネットの発展に貢献してきた事を考えると、RPKI 依存にしてしまう事で、ネットワーク技術数が格段に減り、インターネットの発展を阻害する要因になってしまう懸念もあるため、これを防ぐべく、RPKI の普及に取り組む必要性も考えられる。

2 点目に関してはより深刻な課題である。RPKI で防げたはずのセキュリティインシデントは、国内ではあまり知られておらず、またその金銭的な被害額も報告されていない。経営者は、この適切な投資額を判断する基準を今持っていない。さらに、RPKI を導入する事で逆に障害を発生させるリスクも含めて判断する事になるため慎重な姿勢をとらざるをえない。米国では、DHS(Department of Homeland Security：国土安全保障省)の投資の元ルーティングセキュリティがもたらすリスクとその対策の研究が行われており、RPKI の研究もこの一環となっている。IETF SIDR-WG の中心人物はこの予算で動いている人間も少なく

無い一方で、末端の ISP までこの状況が伝わっていないのは米国でも同様と考えられる。今後は RPKI の普及に ISOC がグローバルレベルで関与する事になっている事から、経営視点で必要となる情報の流通が期待される。但し、RIR/NIR と深く関与する RPKI は、Internet Registry の団体と密接にこのような必要性観点のデータも研究していく必要があると予想される。

5. インターネットレジストリの役割とルーティング支援サービスの将来像

これまでのインターネットレジストリの役割は、IP アドレスや AS 番号資源を適切に運用管理し、利用者に配布することであった。しかし前章までに述べられてきた通り、インターネットにおける不正経路広告は日常頻繁に観測されており、抜本的な予防策を将来に渡って講じていく必要がある。それに伴ってインターネット全体の運用やインターネットレジストリが担っていく役割も変化していく必要がある。

実際に IP アドレスや AS 番号の資源利用者の正当性を保証する仕組みとして RPKI 基盤の運用が 2012 年以降各 RIR で開始されており、全世界で統一された RPKI 基盤の運用が徐々に始まっている。

日本においては、元々古くから同様の問題意識の元、インターネットレジストリが正しい IP アドレスと AS 番号の台帳を担うべきではないか、という考え方に基づき、レジストリが運用する IRR である JPIRR が誕生した。特に日本国内では多くの ISP 事業者に様々な用途で活用されている。
しかしながら、現在の IRR は、登録されている情報の正当性や、その情報流通の可用性を確実に担保するだけの基盤を元々備えているものではないため、不正経路広告の防止を全世界中で、かつ動的に経路制御に反映するような基盤を構築するためには、あらたな仕組みづくりが必要である。元々IRR は、オブジェクトを検索する際に、複数存在する IRR からどのデータベースを参照先として選択したら良いか一意に特定できないという問題がある。また IRR は、地域毎あるいは通信事業社のサービス毎にそれぞれ存在し、それぞれの用途で運用されているため、ポリシーが異なったり、登録されている情報もまちまちであったり、全世界で統一された不正経路広告を防止する抜本的解決策に活用するのは困難であると言える。

それを解決可能な手段が RPKI の仕組みとその基盤の確立である。第 4 章で述べたとおり、IETF の sidr WG において標準化が一通り完了し、サービス提供に必要なアプリケーションの開発やルータへの実装も徐々に整ってきている。

日本国内においても速やかに RPKI 基盤を構築しサービス提供を開始することが望ましい。これにより世界中で統一された IP アドレスと AS 番号資源の正しい組み合わせをインターネットレジストリが提供し、ISP 事業者におけるインターネット経路制御が適切に行えるよう、その基盤を提供していくことが今後のインターネットレジストリの責務であると言える。

具体的には、以下のサービスや情報提供を今後 JPNIC が実施することが望ましい。

１）RPKI サービスの基盤提供
リソース証明書の発行
ROA オブジェクトの発行

２）経路比較サービスの提供
経路情報と ROA 情報とを突合し比較結果をユーザーに提供する、現在の経路奉行相当の機能提供

３）IRR データベース連携機能
IRR データベースにおけるルートオブジェクトと ROA オブジェクトの情報連携機能

１）に関しては、JPNIC の指定事業者に対して、RPKI のソース証明書と ROA オブジェクトを発行できる仕組みとインターフェイスを設けてサービス提供するというものである。既に全世界の RIR ではサービス提供が開始されているが、今後のサービス提供に向けては以下の 2 つの課題があると考えられる。

１つは、サービスの可用性をどのように担保していくか、もう１つはリソース証明書や ROA オブジェクトの発行・取得に関わる業務整理の課題がある。前者については、現在の JPNIC のシステムの中に適切に組み込まれる事が必要であり、APNIC とのシステム連携も含めて、エンドユーザーから確実に参照できる環境を整えていく必要がある。従来の WHOIS サービス以上にインターネット全体の経路制御との関連性が高まることが想定されるため、今後検討が必要である。またサービス提供当初から当面の間は、該当のサーバ自体が不正経路広告によって参照できなくなる可能性もあるため、外部要因にあまり左右されることのない IX 等のネットワークを活用した情報提供および情報参照が望ましいと言える。また後者については、リソース証明書や ROA オブジェクトの発行・取得者が現在の IRR とは将来異なってくる可能性があり、業務整理が必要であると考えられる。IRR は、基本的には経路広告を実施する ISP 事業者がオブジェクト情報を登録することが多いが、現在の RPKI の考え方は、IP アドレスの所有者がどの AS から経路広報するかを ROA オブジェクトに記述する、つまり AS 所有者ではなく IP アドレス所有者が主体となって発行業務を行うことが想定されている。この点については今後 JPNIC でも実証実験等を実施していく中で制度設計や運用設計に関して議論を重ねて検討していく必要があると考えられる。

２）については、現在の IRR データベースを活用した、不正経路情報と疑われる情報の検知とその情報提供に相当するサービスを提供するというものである。RPKI を活用した本格的な経路制御が実施されるまでの当面の間は、不正経路情報の検知や通知等に活用されることが想定される。従来の IRR ベースのサービスに比べて、参照元となる情報が RPKI によって証明された ROA 情報となるため、精度向上が期待される。

また３）については、ROA オブジェクト情報から IRR のルートオブジェクトの自動生成を実施する等の情報連携機能である。元々IRR のルートオブジェクトは、IP アドレスのプリフィックス情報と origin AS 情報が記述されており、ROA オブジェクトと同等相当の情報を有しており、将来にわたり二重に登録業務や情報管理業務を実施していくのは望ましいとは言えないため、現在 APNIC コミュニティでは、IRR の登録業務負荷を下げる試みとして提案されている。ただし、ROA 情報には、広報が許容されている最大プリフィックス長が記述されており、今後 IRR のルートオブジェクトを自動生成する際には、最大のプリフィックス長のみのルートオブジェクトを生成し、RPKI から生成されたことを何らか description フィールド等に記載するなど、情報の生成方法なども含め今後継続的な検討と議論が必要であると考えられる。

現在日本国内では JPNIC が中心となり RPKI の実験サービスが開始され、今後本格的に RPKI サービスの提供に向けて基盤整備等が実施されていく。将来 JPNIC が RPKI 基盤を運用していくにあたり、インターネットレジストリが今後担っていく役割として重要なポイントは、インターネットレジストリはあくまで ISP 事業者の適切な経路制御基盤における、正当な IP アドレスと AS 番号資源の台帳を提供するということであり、インターネットの経路制御を担保するものではないということである。最終的には ISP 事業者が従来通りインターネット経路制御が適切に行えるよう最終的な責任を担うという点である。あくまでインターネットレジストリは、その元となる情報管理、提供の役割を担うということである。

しかし当然ながら、IANA を頂点とした APNIC 配下の証明書を適切に JPNIC が運用管理し、ISP 事業者に混乱なくその情報を提供する責務はある。データの信憑性、参照先データの分散冗長化、トラブル時の迅速な情報提供など、経路制御インフラの重要な基盤の一端を担うという点においては、もっとも重要な役割を果たすことになる。一方 ISP も同様に、自身の経路制御が適切に行われるよう、万が一の事態にも対応できるように ISP 内部にキャッシュデータベースを複数設置しルータが参照したり、想定外の事象や障害発生時にも対応したりできるよう、ISP 側でも適切な準備や対応が必要である。

また、これまでの IRR サービスが今後必要ないということではない。IRR はその情報自体、あるいはその活用の性質上様々な利用がなされており、経路制御ポリシーの記述やコンタクト情報の参照など、今後も継続的な活用が見込まれるため、引き続き JPNIC において運用されていく必要がある。

最後に、インターネットの経路制御を安心・安全に行っていくために、JPNIC が今後果たしていく役割は大きい。より一層 ISP 事業者と協調し、日本国内に留まらず、インターネット全体の高信頼化に向けた活動に期待する。

以上