インターネット 10分 講座

MANRS (Mutually Agreed Norms for Routing Security)とは

1 はじめに

MANRSとは、“Mutually Agreed Norms for Routing Security”（相互に合意されたルーティング・セキュリティに向けた合意規範）の略で、国際的なインターネット運用におけるレジリエンシー（回復力・復旧能力）の向上を図る活動です※1。Internet Society（ISOC）によって推進されています。MANRSは、“マナーズ”と読まれます。

ネットワークの国際的な相互接続によって成り立っているインターネットにおいては、後述するような、さまざまなリスクがあることが知られています。そこでMANRSでは、活動に参加する通信事業者、クラウド事業者等のオペレーターが、実施項目のチェックリストに則って情報を公開することで、リスクへの対策が取れるということが相互に分かるようになっています。さらに、対策項目をBCOP - “Best Current Operational Practices”（現時点での最善の実施方法）と呼ばれるガイドラインとして公表することで、MANRSに賛同し対策を取とうとするオペレーターによって参照され、一定の方法に沿う形でインターネット全体のレジリエンシーが高められるというのがMANRSのめざすものです。

本稿では、インターネットを構成するネットワークの仕組みとリスクについて解説した後、MANRSについて解説します。

※1 Mutually Agreed Norms for Routing Security（MANRS）| Internet Society　https://www.internetsociety.org/issues/manrs/

2 インターネットとルーティングにおけるインシデント

インターネットは、さまざまな組織がそれぞれのネットワークを相互接続したネットワークです。ISPやコンテンツプロバイダー、大学や企業といったネットワークは、APNICやJPNICといったインターネットレジストリから分配されたAS番号とIPアドレスを用いて構成されており、2020年現在、世界中では7万程度※2のネットワークが相互に接続しています。

すべてのネットワークを直接的に接続することは不可能であるため、直接接続できないネットワーク（Autonomous System、自律システム、AS）に対する通信は、宛先のネットワークへの到達性を有するネットワークに転送を依頼しています。この時、ルータでは、AS間で接続できる先の一覧（到達情報・経路）を交換し、交換した経路情報を基に、最適な転送先のリスト（経路表）を作成しています。

ルータ間で経路情報を交換するためのプロトコルをBGPと言い、経路交換のためBGPによりASが接続することをピアリングと言います。

BGPが制定された初期のインターネットでは、すべてのネットワークは信頼できるという性善説に基づき設計や運用がなされていたため、BGPも他ASと交換する経路情報はすべて信頼できるものとして設計されていました。

そのため、誤った経路情報を受け取ったとしても、受け取った側はそれが正しい経路情報か確認することができません。結果として、2018年だけでも12,000件を超えるインシデントが発生し、今日もインシデントが発生※3しています。インシデントは決して他人事ではなく、2,700ものネットワークが少なくとも年1回は、このインシデントの影響を受けています。

インシデントは、意図しない設定ミスによるものもあれば、悪意のある攻撃によるものもあり、これらインシデントにより大規模な通信障害や経済的な損失が引き起こされています。

※2 CIDR REPORT「AS count」より　https://www.cidr-report.org/
※3 主要なルーティングインシデントは https://bgpstream.com/ で確認することができます。

3 ルーティングに対する脅威

過去のインシデントから、インターネットを支えるグローバルなルーティングシステムにはいくつかの脅威が存在することが判明してきました。ここでは、代表的な三つの脅威を挙げます。

● 経路/プリフィクスハイジャック

あるASが正当な権限を有しないIPアドレス（IPアドレスプリフィクスもしくはプリフィクスと言います）の経路情報を、他ASに対して広告する行為を経路ハイジャックもしくはBGPハイジャックと言います。誤って広告されたIPアドレスへの通信（パケット）は、本来届くべきASではなく、広告を行ったASに届けられることから、ハイジャックと呼ばれます。

経路ハイジャックについて、詳しくは過去のインターネット10分講座や※4、JPNIC Web※5で解説していますので、ご覧ください。

● 経路漏洩

経路ハイジャックは、他組織（他AS）のプリフィクスが許可なくBGPにより自組織（自AS）のものとして広告されることで、意図する通信が行えなくなる障害です。一方、広告元（Origin）は正当ですが、何らかの理由により他AS宛の通信の経路に自ASが含まれることで、通信が本来の経路とは異なる経路に迂回される事象を経路漏洩（もしくは経路リーク）と呼びます。

● IPスプーフィング

IPスプーフィングとは、他者のIPアドレスを騙ったパケットを発信することで、実際に利用しているIPアドレスを開示することなく、通信を行う手法です。IPパケットには発信元のIPアドレスを含むフィールドがあり、本来発信元には発信元のIPアドレスを含むことが期待されています。しかし、他者のIPアドレスを含むことも技術的には可能であることから、他者のIPアドレスを含めることで他者になりすまして通信を行うことができます。

サーバやネットワーク機器では、セキュリティ対策としてアクセスできるIPアドレスを制限していることがあります。こうした制限もIPパケットに含まれる発信元を基に判定していることから、発信元を偽ることでこうした制限を突破することが可能になります。この仕組みを悪用することで、攻撃先に大量のトラフィックを送りつけるDDoS攻撃が多発しています。

※4 No.50 インターネット10分講座：ルーティングセキュリティ最新動向 https://www.nic.ad.jp/ja/newsletter/No50/0800.html
※5 インターネット用語1分解説～Mis Originとは～ https://www.nic.ad.jp/ja/basics/terms/mis-origination.html

4 脅威への対策と課題

ルーティングに対する脅威は、2000年頃にはすでに指摘されていましたが、現在に至るまで根本的な解決には至っていません。その理由の一つとして、経路ハイジャック・漏洩とIPスプーフィングに共通して、問題の解決には、被害を受けているネットワークではなく、意図的かどうかに関わらず問題を引き起こしているネットワークにおける対応が必要ということが挙げられます。

通信障害や経路をモニタリングするサービス※6などにより、経路ハイジャックや経路漏洩の対象となってしまったことを検知することはできますが、経路ハイジャック・経路漏洩をしているネットワークに経路の広告を取り下げてもらうまで解決に至りません。IPスプーフィングについても同様に、送信元のIPアドレスを偽った通信を発信元のネットワークにおいて遮断してもらう必要があります。

インシデント発生時は、問題を引き起こしているネットワークへの連絡が必要で、通常WHOISやIRR（Internet Routing Registry）※7などを用いて問題を引き起こしたネットワークの運用者に電話やメールで連絡を取ります。しかし、WHOISやIRRに登録された情報が正しくなく連絡が取れない場合や、経路漏洩やIPスプーフィングにおいては、問題を引き起こしているネットワークの特定が困難である場合、対応してもらうまでに時間がかかり、この間通信障害が解消しないことも少なくありません。

こうしたインシデントの多くは設定ミスにより引き起こされていますが、ネットワークによっては対策を講じるための十分な知識やリソースを有していないことや、悪意をもった攻撃の場合は意図的に引き起こされていることも、ルーティングに対する脅威が今日も存在する大きな要因です。

※6 JPNIC経路奉行 https://www.nic.ad.jp/ja/ip/irr/jpnic-keirobugyou.html
※7 No.27 インターネット10分講座：IRR https://www.nic.ad.jp/ja/newsletter/No27/100.html

5 MANRSの元になった「Routing Resilience Manifesto」

こうしたルーティングに関する問題の解決のために、2011年ごろからグローバルなルーティングシステムのセキュリティとレジリエンシーを向上させるための活動が開始されました※8。この活動は当初「Routing Resilience Manifesto（ルーティング回復力のための宣言）」というドキュメントを公開していました。

このドキュメントでは、ルーティングにおけるレジリエンシーの原理原則を、相互依存（協力を含む）、ベストプラクティス（後述）へのコミット

メント、ピアや顧客への推奨といった項目として定め、重要なものと位置づけしました。さらに、BGPの経路フィルター、IPスプーフィングへの対策、調整と協力といった実施項目をガイドラインとして示しました※9。

最初は少数のネットワーク・オペレーターが集まって最小限の内容になるように作成作業が進められていました。各々のネットワークにおいて、最低限、実施していることが互いに分かるようになっていたのです。

※8 Collective responsibility and collaboration for Routing Resilience and Security, Routing Resilience Manifesto,
https://ripe68.ripe.net/presentations/365-20140515-Routing_Resilience.pdf
※9 History https://www.manrs.org/about/history/

6 MANRS

「Routing Resilience Manifesto」はコミュニティからのフィードバックののち、「Mutually Agreed Norms for Routing Security（MANRS、ルーティングセキュリティに向けた合意規範）」という名前に変更となりました。そして、MANRSはルーティングに関する共通の脅威からインターネットを守るためにISOCにより支援され、2014年8月31日にグローバルな活動になります※10。

MANRSでは、「脅威への対策と課題」で述べた課題を解決するために、次の四つを目的として掲げ、技術とコミュニティによる協調の両面からアプローチをとっています※11。

1. 増えていく賛同者たちとそのコミットメントを示すことによる意識の向上と行動の促進
2. グローバルインターネットのルーティングシステムの回復力とセキュリティに向けた責任共有の文化・思想の促進
3. 責任共有の精神に基づいた、グローバルインターネットのルーティングシステムの回復力とセキュリティに関する検討課題への業界による対応力の証明
4. グローバルインターネットのルーティングシステムの回復力とセキュリティに関する課題についてISPの理解を深め、対応を支援する枠組みの提供

※10 MANRSの詳しい歴史については、History - MANRS（https://www.manrs.org/about/history/）をご覧ください。
※11 ルーティングセキュリティに向けた合意規範 https://www.nic.ad.jp/ja/translation/isoc/20140924.html

7 ルーティングセキュリティの底上げをめざす

インシデントの原因となったネットワークでは、ルーティングセキュリティに対する知識やリソースが不足しており、誤った経路広告やIPスプーフィングへの対策に至っていないと考えられています。そこでMANRSでは、こうしたネットワークでも簡単に対策が行えるよう具体的な手順を示すことで、セキュリティレベルの底上げをめざしています。実施すべき対策はベストカレントプラクティス※12（現時点での最善の実施方法）として、具体的な設定手順を含めて提供している他、チュートリアル※13やハンズオンを提供しています。

具体的には、ネットワーク運用者に対し、四つのアクションを求めています。

1. 不正な経路を出さないFiltering

ネットワーク運用者はルーティングポリシーを定め、プリフィクスやAS-Pathのレベルで顧客および自ネットワークから隣接するネットワークに対する経路広告が正しいものとするような仕組みを導入することで、誤った経路情報を広告や伝播を防ぐことができます。具体的には、以下の対策が挙げられます。

○ ネットワーク運用者は隣接するネットワークと正しいプリフィクスに関する情報の共有ができること。

○ 顧客の経路広告の正しさについてデューデリジェンスを行うこと。とりわけ顧客が合法的にAS番号や広告するIPアドレスを保有しているか確認すること※14が重要です。

2. 送信元IPアドレスを偽装したパケットを出さないAnti-Spoofing

送信元IPアドレス検証を行うことで、他ネットワークのIPアドレスを送信元としたトラフィックを防ぐことができます。

○ 加えてAnti-Spoofingフィルタリングを実施することで、誤った送信元IPアドレスを含むパケットが自ネットワークに出入りすることを防ぎます。

3. グローバルなコミュニティとの円滑なやり取りを行うためのWHOISやIRRなどのデータベースへの登録更新

情報を最新にしておくことで、問題が起こった際の連絡をスムーズにすることができます。登録先としては、WHOISやIRRの他にPeeringDBと呼ばれるピアリングのための情報を登録するWebサイトも推奨されています。

4. IRRやRPKI（リソースPKI）※15 ※16への登録によるValidationへの協力

広告するプリフィクスやAS Pathに関する情報をIRRやRPKIに登録することで、他のネットワークによる誤った経路広告の検出を容易にし、インシデントの拡大を防ぐことができます。

アクションを実行することで、誤った経路が自ネットワークから広

告・伝播されることや、DDoS攻撃の攻撃側となることを防ぐことができます。また、IRRやRPKIへの登録により、自ネットワークが経路ハイジャックの対象となった際にも被害を低減することができます。

※12 MANRS Implementation Guide https://www.manrs.org/isps/bcop/
※13 Tutorials https://www.manrs.org/resources/tutorials/
※14 過去に基となる書類が偽造された例が報告されています。経路ハイジャックされた話 https://www.janog.gr.jp/meeting/janog36/download_file/view/163/179
※15 リソースPKI(RPKI; Resource Public Key Infrastructure) https://www.nic.ad.jp/ja/rpki/
※16 RPKI and BGP: our path to securing Internet Routing https://blog.cloudflare.com/rpki-details/

8 輪を広げることでインターネットを安全に

MANRSが提案しているアクションを実行することで、自ネットワークにより引き起こされるインシデントが減ることはご理解いただけたと思います。しかし、自ネットワークがインシデントの犠牲になることを減らすには、他のネットワークの対応に依存しており、この点がこれまでの課題でした。

MANRSはアクションを実行すると宣言したネットワークをWebサイトで公開することで、セキュリティに対して先進的なネットワークであるということをアピールすることができるようにしています。また、参加ネットワークはMANRS Observatoryと呼ばれるインシデントの統計サイトにアクセスし、自ネットワークが関わるインシデントやMANRSで求められる四つのアクションに対する対応状況を確認することができます。

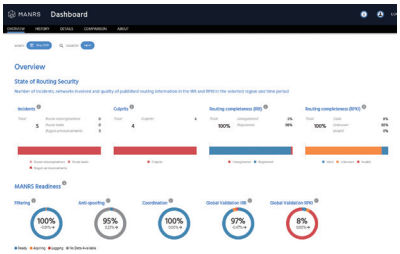

図1 https://observatory.manrs.org/#/overviewで、画面下の世界地図から対象地域を選択して状況を確認できます。

こうしたインセンティブはインシデントを直接的に減らすことにはつながりませんが、MANRSに参加するネットワークが一つまた一つと増えることで、インターネットがより安全に近づきます。そのため、MANRSの活動をサポートするISOCではさまざまな地域ネットワーク運用者のミーティングにおける広報や、ISOCの地域支部(チャプター)と連携した各地域での広報を通じて参加ネットワークを増やす活動をしています。

また、IXP(インターネットエクスチェンジ)は多くのネットワークの接続点となり、ルーティングにおいて重要な役割を果たしています。そのため、MANRSではネットワーク運用者向けのプログラムとは別に、IXP向けのプログラム※17も実施しています。

IXP向けプログラムでは、厳格な経路フィルタリングの他、接続する組織に対してMANRSを推進する、ピアリング基盤に対するアクション、Looking Glassといった、障害が発生した際の切り分けに有効なツールの提供などをアクションとしています。

2020年4月にはCDN※18やクラウドプロバイダー向けのプログラム※19を開始し、IXP向けプログラムと同様にピアリングによって接続する組織に対するMANRSの推進などが盛り込まれています。

※17 MANRS IXP Programme https://www.manrs.org/ixps/
※18 インターネット用語1分解説〜CDNとは〜 https://www.nic.ad.jp/ja/basics/terms/cdn.html
※19 MANRS for CDN and Cloud Providers https://www.manrs.org/cdn-cloud-providers/

9 より安全なインターネットに向けて

2018年ごろ60程度であったMANRSに参加するネットワークが、2020年5月には365になりました。しかし全世界約7万のASのうち、マルチホーム(二つ以上のASと経路交換をしており、MANRSに参加することでインパクトがある)であるAS数、約1万と比較すると、その数はまだ一握りのネットワークに限定されていると言わざるを得ません。なお、MANRSのWebサイトによると、日本を地域に指定している参加ネットワークは2020年5月の時点では16です。

しかし良い兆候も見られます。2017年と2018年を比較すると、インシデントの原因となったネットワークが着実に減少していることは統計データから明らかになっています。2019年に入ってから、MANRSでも推進している経路ハイジャック・漏洩を防ぐ仕組みであるRPKIのオリジン認証のディプロイ(展開)も加速し、自分のISPがRPKIのオリジン認証を行っているか確認できるWebサイト※20が登場するなど、より安全で強固なインターネットに近づきつつあります。

また、BGPをより安全にする仕組みとして、BGPsec※21などの新しい技術の標準化も進んでいます。ネットワークを運用するコミュニティとネットワークプロトコルを策定するコミュニティが協調して、インターネットをより安全にするために取り組んでいます。

ISOCの担当者によると、日本からのMANRSへの参加は少ないが、MANRSの四つのアクションと同様の取り組みをすでに実践しているネットワークは多い※22とのことでした。MANRSへの登録は、所定の要件を満たして申請することで完了します。

また、MANRSでは、この輪を広げる活動に注力する仲間を特にMANRSアンバサダーと呼び、公募しています※23。ネットワーク運用者の皆さんはぜひMANRSに登録し、アンバサダーとなりこの輪を広げていきましょう。

中島 博敬 (株式会社メルカリ・Kamoike.net LLP)

※20 Is BGP safe yet? https://isbgpsafeyet.com/
※21 インターネット用語1分解説〜BGPsecとは〜 https://www.nic.ad.jp/ja/basics/terms/bgpsec.html
※22 ネットワーク運用者の皆様!MANRSをご存知ですか。 https://blog.nic.ad.jp/2019/2265/
※23 MANRS Ambassadors https://www.manrs.org/ambassadors-programme/ambassadors/