

RPKI の ROA を使った
インターネットにおける不正経路への対策
ガイドライン

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

公開日：2024年11月13日

バージョン：1.0

RPKI の ROA を使ったインターネットにおける不正経路への対策ガイドライン

目次

目次.....	1
1. ガイドラインの趣旨.....	3
1.1 本ガイドラインの活用方法.....	3
1.2 インターネットにおける経路情報.....	4
1.3 不正な経路情報のリスクや損失.....	4
1.4 対策技術 — RPKI と ROA,ROV.....	5
1.5 実施事項.....	6
2. 技術的情報.....	8
2.1 ROA/IP アドレスの分配を受けた者の実施事項.....	8
2.1.1 ROA とは.....	8
2.1.2 不正経路と IP アドレスに関する考え方.....	8
2.1.3 ROA の作成と運用管理.....	10
2.1.4 BGP 経路と ROA を一致させる手順.....	10
2.1.5 重要事項：ROA の導入に関わる三つの確認.....	11
2.1.6 例外的な処置.....	11
2.2 ROV/AS 運用をしている者の実施事項.....	12
2.2.1 不正経路への対策と考え方と ROV.....	12
2.2.2 ROV の導入に関わるコスト.....	13
2.2.3 ROA キャッシュサーバ・ROV の所在.....	14
2.2.4 ROA キャッシュサーバの構築.....	19
2.2.5 ルータにおける ROV 設定.....	19
2.2.6 ROV による経路制御の詳細.....	20
2.2.7 重要事項：ROV の導入に関わる三つの確認.....	21
2.2.8 ROV の設定例.....	23

2.2.9	運用上の注意と懸念点.....	24
3.	ROA/ROV 以外の不正経路対策.....	25
3.1	BGP におけるセキュリティの要素と考え方.....	25
3.2	AS パス検証の今後と運用について.....	25
4.	用語集.....	26
5.	おわりに.....	27

1. ガイドラインの趣旨

本ガイドラインは、国内の ISP 等、インターネットの接続性に関わる事業や技術的運用を行っている組織の経営者及び技術者の方に向けたもので、相互接続ネットワークであるインターネットにおける不正な経路情報、特に RPKI を使った対策の指針を示すものです。

不正な経路情報に起因する様々な不具合、および不正な経路情報を用いた犯罪等を抑止するにあたり、RPKI 技術を用いた対策技術を各組織や個人において導入する判断に資する事項を示します。

■ 本ガイドラインについて

本ガイドラインは令和 4 年度から令和 5 年度にかけて総務省において行われた事業「ISP におけるネットワークセキュリティ技術の導入および普及促進に関する調査」の一環で作成されたものです。この事業で行われた調査研究や実証実験の結果を踏まえた内容になっています。同時に、有識者や実験参加者および国内のインターネット運用コミュニティである JANOG 等における意見収集を経て案が作成されました。

その後、令和 6 年 4 月に総務省におけるサイバーセキュリティタスクフォース ICT サイバーセキュリティ政策分科会（第 5 回）にて案のレビューを経て、ガイドライン案は技術的に関りの深い民間の団体に引き継いだ上で「ガイドライン」として公開する運びとなりました。本ガイドラインは、国内インターネットレジストリであり、日本国内におけるリソース証明書の発行主体である当センターが引き受けることとなりました。

1.1 本ガイドラインの活用方法

第 1 章は経営的な観点での判断に資する内容になっており、第 2 章以降は技術的観点での検討や判断に資する内容になっています。

※個人の場合には、組織を個人として読み替えてください。

- 経営的な観点での本ガイドラインの活用方法
御組織において JPNIC 等から IP アドレスの割り当てを受けているかどうか、また AS を運用しているかどうかを、技術部門、もしくは JPNIC との取引を担当している部署で確認してください。いずれかが該当する場合には、第 1 章を読んで、1.5 節に記載された項目の実施を検討します。
- 技術的観点での本ガイドラインの活用方法

御組織において JPNIC 等から IP アドレスの割り当てを受けているかどうか、また AS を運用しているかどうかを確認し、対応実施事項（1.5 節）を確認します。各々の項目の実施やその判断にあたっては、第 2 章の対応する章を参照してください。御組織における導入形態などを明確化するために役立つ内容になっています。

- 実証実験の結果を受けた「三つの確証」
実証実験の結果、本ガイドラインで示される実施項目について、実験参加者において「導入しても通常は問題ない」「不正から守るために役立つ」「不具合が起きても対処できる」という三点について確証を得る作業が行われました。三つの確証の観点での記述が 2 章各節にあります。導入の判断のために活用ください。

1.2 インターネットにおける経路情報

インターネットは複数のネットワークが相互接続された形で運用されています。各々のネットワークは IP アドレスを宛先とする通信データをどこに送るのかを決定するために、BGP と呼ばれるプロトコルを使って経路情報を相互に交換しています。経路情報の正しさはインターネットを支える重要な要素であると言えます。

1.3 不正な経路情報のリスクや損失

不正な経路情報とは、インターネットにおける本来の経路とは異なるような、IP パケットの伝搬経路を誘発する経路情報を意味します。正常な通信が行えない他、通信データが誤った宛先に到達することがあります。この性質を利用して大規模な通信傍受や犯罪が行われることもあります。不正な経路情報が発生する原因として、ネットワーク機器であるルータにおける設定ミスや故意に誤った経路情報をルータに設定することが挙げられます。

インターネットに接続するユーザや組織にとって、不正な経路情報は、経済活動の機会損失だけでなく、資産を第三者に奪われることにつながる恐れのあるものであり、国際的な範囲において、特定のネットワークへの到達性を損なわせられるようなリスクもあります。また、RPKI を使った対策技術があるにもかかわらず対策を取っていないことが、不正な経路情報の影響を受けた後に発覚すると組織における十分な対策が取られていなかった点が第三者によって指摘される可能性があります。

インターネットが国民生活や国際社会において重要な位置を占めるようになった現代においては、不正な経路情報による通信の不具合や犯罪等が起きることを防止することが重要です。またこれはインターネット全体へのセキュリティにも寄与します。IP アドレスの

分配を受けているすべての組織やインターネットに接続する AS を運用している組織は、適切な対策を取ることが必要です。

■不正な経路情報の事例

2017 年 8 月に Google による作業ミスにより誤った経路情報が広告され、日本でも大きな ISP で一定期間通信ができない状況が発生しました(下記 A)。広告元の AS は正しいものでしたが、通常の広告とは異なって、優先されるプレフィックス長の経路情報を広告していたこともあり、RPKI を用いた対策技術が導入されていればある程度被害を抑えられていたと考えられます。

意図的に行われたと推察される不正経路により、既存の経路が意図的に変更される事象も報告されています。例えば、2018 年 4 月に仮想通貨が盗まれる被害が発生しました(下記 B)。これは DNS サービスの一種である Amazon Route 53 の経路情報を別の AS が不正に広告することでユーザは偽サイトへ誘導され、暗号資産が第三者に不正に送信されたとされています。

- A) 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,
平成 29 年 12 月電気通信事故検証会議

https://www.soumu.go.jp/main_content/000525814.pdf

- B) What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum
Cryptocurrency Wallets - Internet Society

<https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>

1.4 対策技術 — RPKI と ROA,ROV

RPKI(Resource Public Key Infrastructure)は IP アドレスなどの番号資源の分配を証明する証明書、リソース証明書の発行に使われる公開鍵認証基盤です。これは不正な経路情報を判別するために「正しい経路情報」を示すデータ、ROA(Route Origin Authorization)の作成に使われます。

ROA は IP アドレスの分配を受けた者が作成するもので、経路広告する IP アドレスのプレフィックス(以下、プレフィックスと呼ぶ)と最大プレフィックス長、経路広告する組織(AS 番号)を指定します。ROA はリソース証明書で検証可能な電子署名が施されています。

ROV(Route Origin Validation)は、ROA を用いて、経路情報が正しいかどうかを判定することです。ROV の導入にはいくつかの方式が挙げられます。

1.5 実施事項

本ガイドラインに関係する立場を以下に示します。挙げられている組織や個人は、各々の項目を実施して、全体としてすべての項目が実施されることが推奨されます。

■JPNIC や APNIC から IP アドレスの分配を受けているすべての組織や個人

○ROA を作成します (必須事項)。

管理下にある IP アドレスに関する ROA を必ず作成してください。これを行わないとその IP アドレスに関する ROV を行うことができず、インターネットにおいて不正な経路情報への対策を取ることができません。

⇒ 「2.1 ROA/IP アドレスの分配を受けた者の実施事項」を参照してください。

○ROA が実際の経路情報と一致するように保ちます (必須事項)。

作成した ROA と経路情報が一致するように保ってください。これを行わないと正常な経路情報であるにもかかわらず、ROV を行っているルータにおいて不正な経路情報と判定されてしまうことがあります。

⇒ 「2.1 ROA/IP アドレスの分配を受けた者の実施事項」を参照してください。

■インターネットに接続する AS を運用している組織や個人

○ROV を行う等の処置を行います (推奨事項)。

これによって ROA に基づいた不正な経路情報への対策を行うことができるようになります。処置の方式として以下の三つが挙げられます。適するものを特定して、それを実施することが推奨されます。

方式 A ROA キャッシュサーバを自組織で運用して ROV を実施する。

方式 B IXP 等で提供される ROA キャッシュサーバを利用して ROV を実施する。

方式 C ROV が行われているトランジット経路を利用する。

※これ以外の方式の採用を妨げるものではありません。

⇒ 詳しくは「2.2 ROV/AS 運用をしている者の実施事項」を参照してください。

推奨される事項を実施している組織および個人は、不正な経路情報への対策を取っているとしてその旨を公に示すことができます。またその実施に関して民間において認定され、今後、各種調達においてその認定状況が参照されることがあります。確実な実施のためには、試験から運用に至るまでに時間を要することがあります。

以降では、推奨される事項の実施に資する技術的情報を示します。

2. 技術的情報

この章では RPKI を用いた不正経路対策の技術的情報について述べます。

本節では、現時点での技術的情報をまとめますが、今後も最新の技術的な情報を参照できるようにするために本章の内容を含む技術情報が掲載されるサイトを以下に示します。情報の正確性や最新性はサイトの運営者に寄りますが、RPKI を用いた不正経路対策は多岐にわたる技術であるため、読者および有識者は国内における最新技術情報の共有に協力することが望まれます。

当センターにおける RPKI に関する情報をまとめたサイトは以下の通りです。

- リソース PKI (RPKI) <https://www.nic.ad.jp/ja/rpki/>

2.1 ROA/IP アドレスの分配を受けた者の実施事項

本節では ROA の作成について述べます。主に IP アドレスの分配を受けている組織の管理者および技術者に向けた情報です。

2.1.1 ROA とは

ROA とは IP アドレスの分配を受けた者が、その IP アドレスの範囲に含まれる経路情報を AS 運用者から広告することを認めた（認可した）ことを示すものです。IR から IP アドレスの分配を受けた組織は、BGP によって広告される経路情報とその最大プレフィックス長および広告元になる AS の組を持つ ROA を作成します。ROA を間違っって作成すると、インターネットの接続性に直ちに影響を及ぼす可能性があるため、作成は慎重に実施する必要があります。

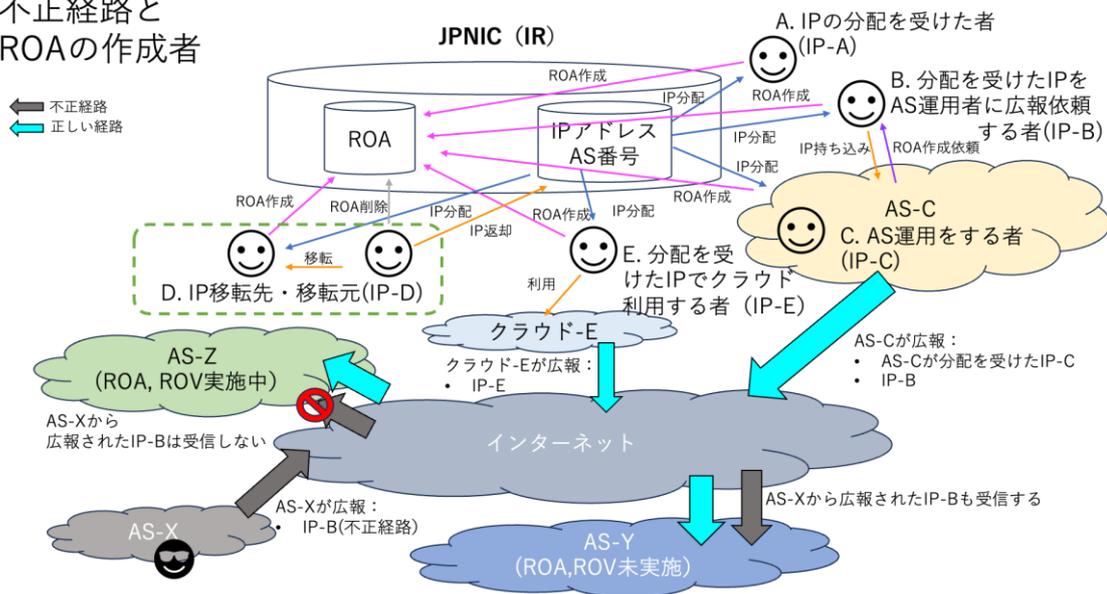
- インターネット用語 1 分解説～ROA とは～ - JPNIC
<https://www.nic.ad.jp/ja/basics/terms/roa.html>

2.1.2 不正経路と IP アドレスに関する考え方

IP アドレスの分配を受けた者が ROA を作成することで経路情報の発信元の検証 (ROV) を行うことが可能になり、不正経路への対策につながります。

ここでは次の図に示す A～E について説明します。

不正経路と ROAの作成者



ROA 作成と不正経路

- ROA を作成することで、あるプレフィックスがどの AS から経路生成を許可されているかを明確にすることができます。より多くのプレフィックスが ROA による検証が可能になるよう可能な限りすべてのプレフィックスに対する ROA を作成します。
- IR から IP アドレスの分配を受けた者は、経路広告を担当する AS 運用者と連携し、広告経路に適した ROA を作成します。
- 経路広告を担当する AS 運用者は、自身が生成する経路に対応する ROA を作成する、もしくは広告依頼する者から作成を依頼します。顧客が分配を受け持ち込んだ IP アドレスについても当該 IP アドレスの分配を受けた者に ROA の作成を依頼する必要があります。RADb などの IRR とは異なり、ROA の作成は代理で行うことはできません。

DDoS 対策 (DDoS mitigation) サービスの中には、そのサービス提供者が AS を運用し、保護対象のプレフィックスを一時的に代理で経路広告するものがあります。この場合、このサービス提供者の AS 番号を指定した ROA を作成しておく必要があります。この DDoS 対策における ROA 作成について RFC9319 で記述されています¹。

¹ RFC9313: The Use of maxLength in the Resource Public Key Infrastructure (RPKI)
<https://datatracker.ietf.org/doc/html/rfc9319>

- D IP アドレスを移転する場合には ROA の内容を正しく保つ必要があります。基本的に、移転元となる IP アドレスの分配を受けた者が ROA を削除し、移転先の者が新たに ROA の作成を行います。
- E 分配された IP アドレスをパブリッククラウド等へ持ち出す場合
当該プレフィックスの経路情報がクラウド事業者等から広告される場合は、クラウド事業者等の AS 番号を指定した ROA を作成する必要があります。

IP アドレスをクラウドサービス等に持ち込んで利用する、いわゆる BYOIP (Bring Your Own IP) を行う場合には、ROA の作成が必要になることがあります。その ROA ではオリジン AS として利用するクラウドサービス等の AS 番号を指定します。

経路広告を行わないプレフィックスについては明確に意図的に広告しない経路情報であることがわかるよう、AS0 の ROA を作成します。

2.1.3 ROA の作成と運用管理

ROA を作成できるのは IP アドレスの分配を受けている組織や個人です。ROA は IP アドレスの分配元である各 IR が提供するシステムを利用して作成します。JPNIC から IP アドレスの分配を受けている場合には、JPNIC の RPKI システムを使って ROA を作成します。利用方法の詳細は下記のページを参照してください。

- RPKI - JPNIC
<https://rpk.nic.ad.jp/>
- ROA の作成と管理の方法 - JPNIC
<https://www.nic.ad.jp/ja/rpki/howto-create-roa.html>

2.1.4 BGP 経路と ROA を一致させる手順

ROA の作成と維持にあたり、ROV が行われるルータにおいて BGP 経路が Invalid と判定されることを避けるためには以下の手順が考えられます。

1. BGP 経路を変更する業務フローの中に ROA の状態を確認する項目を入れておきます。ROA の状態を確認するには次の 2 を参照してください。
2. ROA の状態が確認できるインターフェース (IR の提供している Web サイト等) に

アクセスし、作成した ROA に関連する経路情報が Valid になっていることを複数のサイトで確認します。サイトの例を以下に示します。

- Routinator - RIPE NCC - <https://rpki-validator.ripe.net/>
- NetOX - APNIC - <https://netox.apnic.net/>

2.1.5 重要事項：ROA の導入に関わる三つの確認

ROA の作成にあたり、次に示す三点の確認により判断を行います。ROA の作成において下記を留意せずに作成すると、BGP 経路との差異ができる等により、その BGP 経路が国際的に Invalid と判定されてしまうリスクがあります。三点の確認を通じて ROA の導入がリスクとならないように判断することが重要です。

考え方	ROA に関する確認事項	実施事項
導入しても通常は問題ない。	○ ROA を作成しても通常は問題ない。	○ BGP 経路を変更したときには必ず ROA が一致するような運用フローにする。
導入することで不正から守られる。	○ ROA を作成することで ROV された際に不正な BGP 経路から守られる状態である。	○ ROA 作成もしくは修正を行ったときに、国際的にいくつかのサイト(下記)で ROV の結果を確認する。
導入による不具合が起きても対処できる。	○ ROA と BGP 経路に不一致が起きても ROA を修正して Valid な状態に戻すことができる。	○ BGP 経路に対する ROV 結果を定期的に確認および監視する。 ○ 適切な人員が ROA を修正できる状態であることを確認する。

2.1.6 例外的な処置

ROA の導入に関する例外的な処置について以下に示します。

- 隣接組織間でトラフィックコントロールなどのために ROA で指定されているものより長いプレフィックスの経路情報の交換を要する場合は、適切な配慮を行なう必要があります。

- ROV 導入時に、組織内部でプライベート AS を利用している等で網内に ROA で指定されている以外のオリジン AS の経路情報がある場合は、意図的に ROV の設定を適用しない、BGP ルータにおける経路フィルタで除外する、ROA キャッシュサーバにおいて SLURM を設定する等、別途対処を検討する必要があります。

運用上の注意

指定する最大プレフィックス長は、実際に広告する経路情報のプレフィックス長と一致させておきます。プレフィックス長が/19 なのにもかかわらず/24 まで許可した場合、サブプレフィックス攻撃と呼ばれる方法によって、より長いプレフィックス長を持つ不正な経路情報の影響を受ける可能性があります。ただ、最大プレフィックス長の指定が禁止されているわけではなく最小限にすることが推奨されています[RFC9319]。

- サブプレフィックス攻撃とは攻撃者の BGP ルータが ROA に記載されたオリジン AS を使って不正な経路情報を広告するものです。運用上の条件が限定されている他、これまでの報告例はまだありません。

経路情報に変更になる、もしくはオリジン AS が変更になる際には、ROA の変更が必要になります。経路広告する数日前に ROA を適切に追加作成し、経路広告後に古い情報を削除します。

2.2 ROV/AS 運用をしている者の実施事項

この章では RPKI を用いた不正経路対策について、ROV の実施について述べます。主に AS 運用を行なっている組織の管理者および技術者に向けた情報です。

2.2.1 不正経路への対策と考え方と ROV

ROA によって正しい経路広告の AS 番号、IP アドレス、プレフィックス長は把握できますが、一方で、不正経路の受信や広告を防止するには後述する ROV が必要です。ROA の情報をルータが参照し、ルータで受信する経路情報が正当なものか、そうでないのかを判定し、採用するのかを経路制御ポリシーにより判定します。この ROA の情報を参照して経路情報が正しいかどうかを判断する仕組みを ROV と呼びます。

電子署名されている ROA 情報の検証をルータ自身で行うとそのルータに負荷がかかるため、ROA の署名検証は「ROA キャッシュサーバ」を設置して行われます。検証済の ROA の内容 (VRP (Validated ROA Payload) と呼ぶ) が一時的に保持されたものを ROA キャ

ッシュと呼びます。ルータはこのキャッシュを参照して当該経路情報の正当性を判断します。ROA キャッシュサーバとルータ間は RPKI-RTR プロトコル(RPKI to Router Protocol)で接続が行われます。

なお、自組織内の全てのルータで ROV を行なう必要はなく、基本的には不正経路の流入もしくは流出を防止したい箇所(例えばトランジットを受ける、他 AS と BGP Peer を張る)のルータでのみ ROV を有効化すればよいでしょう。

- インターネット用語 1 分解説～ROV (Route Origin Validation)とは～ - JPNIC
<https://www.nic.ad.jp/ja/basics/terms/rov.html>

ROV では、ROA に一致する経路情報(Valid)、ROA が作成されていない経路情報 (Not found あるいは Unknown, 以下 Not found と記述する)、作成されている ROA と矛盾する経路情報(Invalid)という状態が存在します。これらの取り扱いをどうするかを各組織のポリシーによって決めることが ROV の鍵となります。

運用上の注意

- ROA に一致する経路情報のみを採用するようなポリシーにすると、ROA による分配済み IP アドレスに対するカバー率が 100%に至らない現状では、ROA が作成されていない IP アドレスの経路情報をも不採用にしてしまう設定になりますので注意が必要です。

2.2.2 ROV の導入に関わるコスト

ROV を実施する上で、ROV 実施前と比べ、次のようなコスト増が挙げられます。これらを踏まえつつ ROV 導入の判断が必要となります。

- ROA 作成依頼のコスト
- ROV 可能なルータの設備コストと運用コスト
- CPU 負荷やメモリ使用量増
ROV 対応ルータであれば特に問題となる増加量ではありませんが、RPKI 非対応ルータからのリプレースが必要な場合や、現時点で CPU 利用率がかなり高いようなルータについては考慮が必要です。

2.2.3 ROA キャッシュサーバ・ROV の所在

ROV を導入するにあたり、大きくわけて本節で挙げる 3 方式が考えられます。それぞれ、各組織の運用技術や体制、提供するネットワークサービスと顧客への影響度によってどの方式を選択するかを検討します。

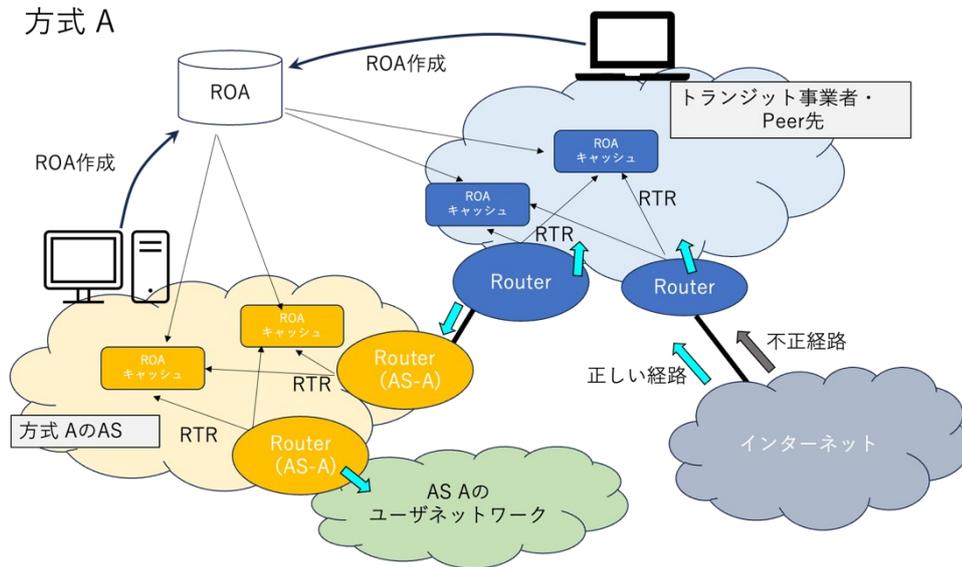
重要なネットワークサービスを提供する組織はインターネットを介した公開 ROA キャッシュサーバを利用することにはリスクがあります。例えば、ネットワーク障害によってルータが ROA キャッシュサーバを参照できなくなった場合についてのリスクがあります。公開されている組織外の ROA キャッシュサーバを利用した場合、キャッシュサーバの ROA キャッシュが改竄されるとこれを検知することは難しく、当該パブリック ROA キャッシュサーバを利用している全ての利用者に影響が及ぶことが考えられます。また、VRP が平文であるため、経路上での改竄による影響も考えられます。ROA キャッシュサーバが自組織における運用が行われるものではない場合、その利用によって、ROV の結果が適用している者の意図しないものになる可能性が高まります。従って、自社網内などの閉じた環境で ROA キャッシュサーバを構築することが望ましいと考えられます。

また、ROA キャッシュサーバはその冗長性と安全性について考慮が必要となります。ROA キャッシュサーバは、組織外部からの接続性は必要ないため、組織内に外部からの接続性を遮断したキャッシュサーバを複数(ハードウェアおよび ROA キャッシュソフトウェア)設置することにより、上記のリスクを低減できます。

以下では ROA キャッシュサーバの利用方式を示します。

[導入方式 A] ROA キャッシュサーバを自組織で構築して ROV を実施する方式

構成を以下に示します。



ROA キャッシュサーバを自組織で構築して ROV を実施する方式

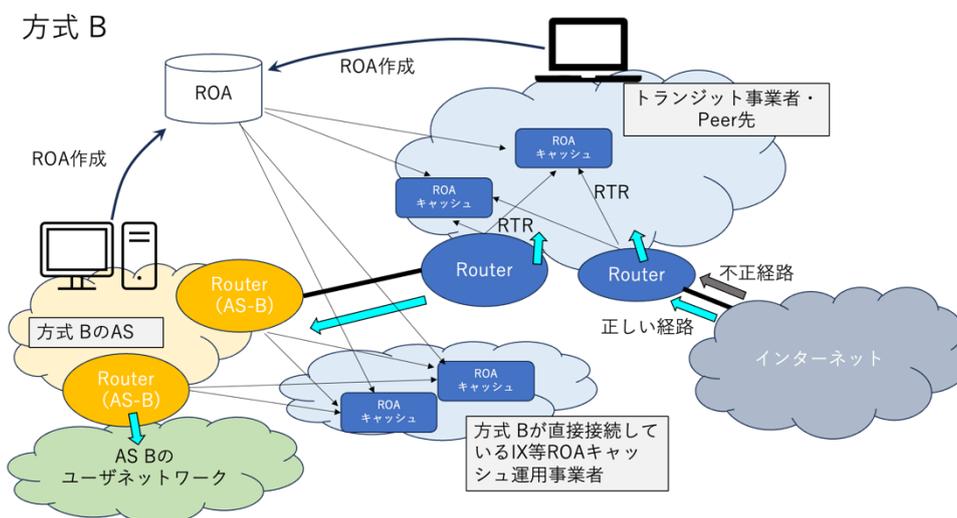
ROA キャッシュサーバを自組織内に複数構築しルータで参照して ROV を実施する方式です。

特徴

- ROA キャッシュサーバを自組織で構築運用するため、ルータと ROA キャッシュ間が自組織内に限ることができ、ルータ起動時に網内の経路情報のみで素早く RTR の接続を確立することができます。また前述のリスク低減が図れますが、導入方式 B の IX 等で提供する ROA キャッシュサーバの利用よりも運用コストは高いと言えます。また、網内で完結するため、保守等で網外のキャッシュサーバへの到達性が失われる場合でも問題なく利用できます。ルータと ROA キャッシュの距離が近い=経路箇所が少ないことから耐障害性にも優れます。
- SLURM による例外処理を ROA キャッシュサーバ側で行うことができるため、多くのルータで ROV を行う必要がある場合などではルータ設定の省力化が図れる場合があります。

[導入方式 B] IX 等で提供する ROA キャッシュサーバを利用して ROV を実施する方式

構成を以下に示します。



IX 等で提供する ROA キャッシュサーバを利用して ROV を実施する方式

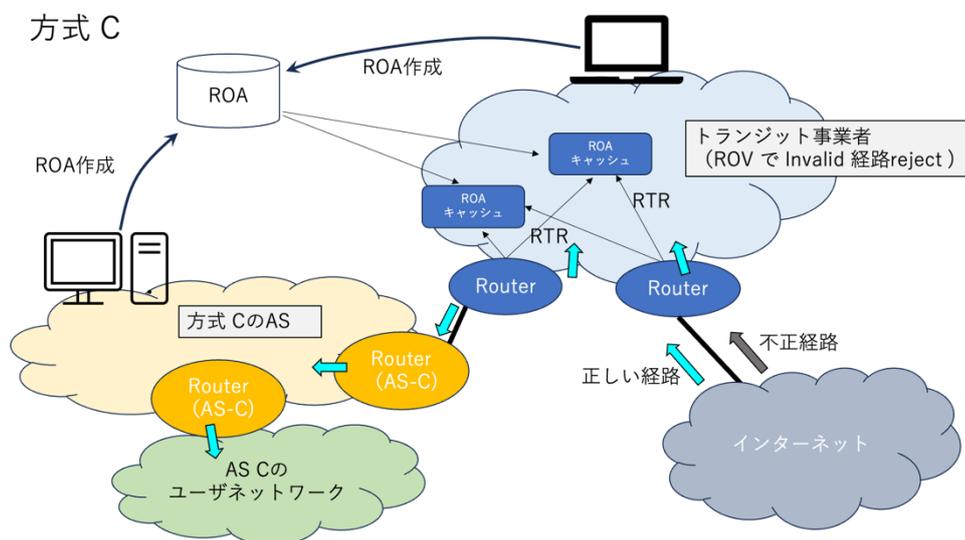
ROA キャッシュサーバを自社で構築せず、IX 等自組織と直接接続性のある事業者が構築提供する ROA キャッシュサーバをルータで参照して ROV する方式です。

特徴

- 自組織内に ROA キャッシュサーバがある方式 A と比べると ROA キャッシュサーバとルータ間で経由するネットワークが増えるため、耐障害性は下がりますが運用コストが抑えられます。セキュリティ的にも VRP とルータ間のやりとりは IX や事業者内のネットワークを介するにとどまるため、インターネット上のパブリック ROA キャッシュサーバを利用する場合より好ましいです。

[導入方式 C] ROV が行われているトランジット経路を利用する方式

構成を以下に示します。



ROV が行われているトランジット経路を利用する方式

上記は ROV を実施しているトランジットからのみ経路情報を受信する場合の図です。ピア接続がある場合には、そこから流入してくる経路情報に対して ROV を行うことが考えられます。

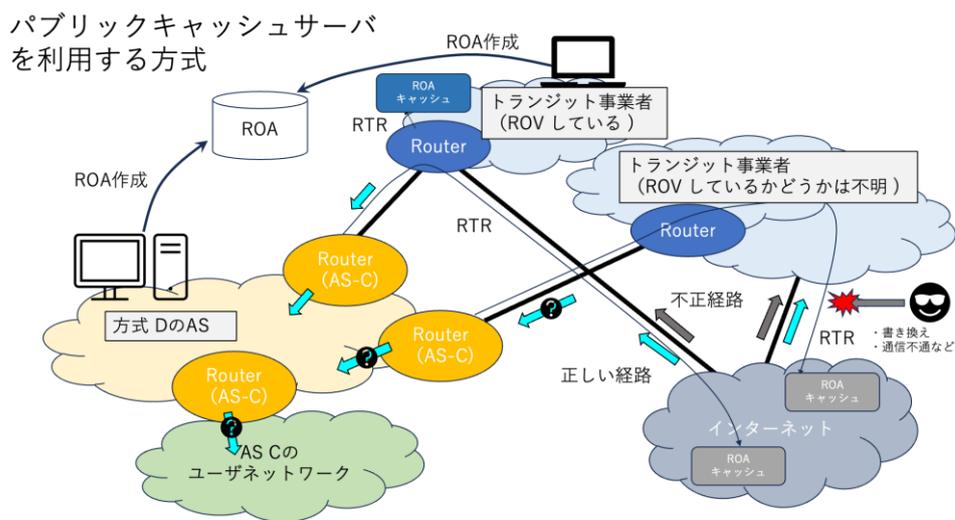
特徴

- ROA 作成を実施する必要があるありますが、ROA に関わるコスト (ROA キャッシュ ユーサーバや ROV 可能なルータの導入、運用) を抑えることができます。
- ROV による経路制御ポリシーについてトランジットプロバイダに依存することになります。例えば、トランジットのミスを自組織で防ぐことはできません。

[その他の方式] パブリックキャッシュサーバを利用する方式

公開 ROA キャッシュサーバ（パブリックキャッシュサーバ）を利用して ROV を行う方式です。構成を以下に示します。

この方式は以下の特徴に述べたように導入しやすいというメリットがありますが、パブリックキャッシュサーバへの到達性や RTR の完全性が保証されないため、止むを得ない場合以外の利用は推奨されません。



パブリックキャッシュサーバを利用する方式

特徴

- 自身で ROA キャッシュサーバを用意する必要がなく、キャッシュサーバ導入・運用コストはかかりません。
- パブリックキャッシュサーバを利用する場合には以下のような点に注意する必要があります。
- パブリックキャッシュサーバへの到達性はサーバの問題や途中経路の問題などで保証はされません。
- RTR は暗号化されていないため、通信経路上で改竄される可能性があります。
- 通信経路上で偽の ROA キャッシュサーバに誘導される可能性があります。
- パブリックキャッシュサーバはインターネット公開されているため、攻撃の対象になるリスクがあり、侵入され改竄される可能性があります。
- 同様に DDoS を受けるなどにより利用できなくなる可能性があります。

これまでに述べた導入方式の比較表を以下に示します。

方式	セキュリティ	耐障害性	SLURM	設備コスト	構築／運用コスト
A 自網内に構築	○	○	○	高	高
B IX 等利用	△	△	×	低	低
C ROV 済みトランジット	△	△	×	無	無
他 ROA パブリックサーバ	×	×	×	低	低

2.2.4 ROA キャッシュサーバの構築

オープンソースソフトウェア (OSS) でいくつか ROA キャッシュサーバの開発がされています。現状ではこれらを選択するかもしくは、自社開発を行います。OSS については開発が終了しているものもあるので、注意が必要です。代表的な ROA キャッシュサーバを以下に示します。

- FORT
<https://nicmx.github.io/FORT-validator/>
- Routinator3000
<https://www.nlnetlabs.nl/projects/rpki/routinator/>
- rpki-client
<https://www.rpki-client.org/>

VRP を生成する機能は有しますが、RTR サーバの機能を持っていないため別途準備する必要があります。RTR サーバ機能の実装として StayRTR、GoRTR があります。

2.2.5 ルータにおける ROV 設定

前述の方式(A~C)について A もしくは B を採用することを決定後のルータ側 ROV 設定について示します。なお、その他の (パブリックキャッシュサーバを利用する) 方式を止むを得ず採用する場合も同様の設定を行います。

ROV を導入する箇所の検討

先に述べたように自組織内全てのルータで ROV する必要はありません。主に次のような箇所に設置されるルータでの実施を検討します。それぞれについての必要可否は、相手組織

のリスクを自組織が受容できるのか、そのリスクが自組織でサービス提供する相手に対しての影響度合いを鑑みて検討します。

- (1) トランジット事業者と接続している箇所（トランジット接続）
- (2) IX やプライベートピアなど他 AS と接続している箇所（ピア接続）
- (3) 顧客と BGP 接続している場合は、顧客と接続している箇所（カスタマー接続）

ROV をどのピアに適用するかの検討

AS のすべての BGP ピアにおいて ROV を設定することが理想的です。しかしながら、一度にすべてにおいて導入することは、運用者にとって不安がありリスクを伴う作業になる可能性があります。従って、多くの BGP ピアがある AS においては段階的な ROV の導入が行われ、その導入期間も長くなることが考えられます。段階的に導入する場合に、不正経路への対策という意味で効果が高いと考えられる導入の順番とその考え方を以下に示します。

はじめにトランジット接続に ROV を導入することが考えられます。これは国際的な多くの経路情報を受信することから、不正な経路情報が入り込む可能性が高いと考えられるためです。次にピア接続に導入します。不正な経路情報を受信する可能性はトランジット接続よりは低く、次に述べるカスタマー接続よりも高いと考えられます。最後にカスタマー接続に導入します。

トランジット接続の先の AS が既に ROV を導入している場合には、その接続における ROV の導入について優先順位を下げるものが考えられます。ただし不正経路への対策として他 AS が行っている ROV に頼ることになりますので、その点に留意して導入判断を行うこととなります。またカスタマー接続において、接続先の AS から受信する経路情報に対するプレフィックス・フィルターや AS パス・フィルターを導入している場合、ROV の導入を見送ることも考えられます。研究目的、経路情報の異常を検知するためのモニタリング、もしくは不正経路によって被害が発生しないようなケースでも ROV の導入を見送ることが考えられます。

2.2.6 ROV による経路制御の詳細

BGP ルータにおいて ROV を行うことで BGP を通じて受信した経路情報の一つ一つに対して次に述べる判定を行うことができます。

- Valid 当該の経路情報は ROA に記載されたプレフィックスおよびオリジン AS

と一致し、有効である。

- Invalid 当該の経路情報は ROA に記載されたプレフィックス・最大プレフィックス長およびオリジン AS と一致しておらず、有効ではない。
- Not Found 当該の経路情報を内包するプレフィックスが記載された ROA は存在しない。ROA が作成されていない状態。

これらの判定を行うか否かは、経路情報を受信する BGP ピアごとに設定します。また判定を行った結果をどのように扱うかを設定します。ここでいう扱いとは IP パケットの経路制御のために使われる経路表 (FIB 等) に入れるかどうか、もしくは local-preference 値等を使って優先するかどうかなどが挙げられます。一部の機器では明示的に設定を行わなくても既定で Invalid と判定された経路情報を経路表に入れないものがあります。また BGP の拡張コミュニティ属性を用いて、ROV 処理を行っていない他の BGP ルータに判定結果を伝えることができるものがあります。運用する BGP ルータがこれらのうち、どのような機能を有しているかを確認します。

ROV の判定結果を受けてどのように経路制御を行うかを検討します。Valid と判定された経路情報を採用し、Invalid と判定された経路情報を不採用にする例を以下に示します。Not Found と判定された経路情報は、いわば従来のインターネットの状態であり、この経路情報を採用しない設定を行っても問題がないことを、実施する前に確認する必要があります。特に ROA キャッシュサーバとの接続 (RTR 接続) が影響を受けないように留意する必要があります。

ROV に関する典型的な例を以下に示します。

- (1) Valid : 許可する
- (2) Invalid : 不許可とする
- (3) Not found : 許可する

これらの処理は BGP の接続先ごとに行われるため、例えばトランジットや顧客からの経路情報に対して適用しても、ROV を適用していないピア接続先からの経路情報が意図せずに適用されてしまうことがあります。ROV は不正な経路情報を受信する可能性のあるすべての接続先に対して適用することが望ましいと言えます。

2.2.7 重要事項：ROV の導入に関わる三つの確認

ROV の適用にあたり、次に示す三点の確認を行ってからその判断を行います。ROV の導

入にあたり、下記を留意せずに適用すると、ASの運用上、意図しない結果になることがあります。三点の確認を通じてROVの導入がリスクにならないように判断することが重要です。

考え方	ROVに関する確認事項	実施事項
導入しても通常は問題ない。	○ ROVを適用しても通常は問題ない。	○ Invalidな経路情報でも採用する設定のROVを適用し、BGPルータの負荷やメモリ等の面で正常に稼働することを確認する。 ○ ROVを適用することで不採用となる経路情報に顧客のIPアドレス等、使われるものが含まれていないことを確認する。
導入することで不正から守られる。	○ ROVを行うことで不正な経路情報から守られる。	○ Invalidと判定される経路情報を観察して意図通りに採用されないことを確認する。(Invalidとなる経路情報にRouting Beaconがある。情報源を以下に示す。)
導入による不具合が起きても対処できる。	○ 特定のROAが作成者の意図と異なる判定をされてしまう状態が起きても、その採用不採用を制御するなど、対処できる。	○ ROAキャッシュサーバにおけるROVに関する例外処理SLURM等の設定を行って、Invalidと判定される経路情報を経路表に採用できるようにする。 ○ BGPルータにおいて特定の経路情報については採用・不採用を制御できることを確認する。

■Invalidとなる経路情報の情報

- RIPE Atlas docs | Routing Beacons | Docs
<https://ris.ripe.net/docs/routing-beacons/#current-beaconing-setup>

2.2.8 ROV の設定例

本節では ROV 設定のシナリオについて述べたあと、そのシナリオに沿った各ベンダの設定例を示します。

■ROV 設定のシナリオ

次の要領で ROV の設定を行います。ROV を実施するまでの手順としては 1,2 のみです。この他に CPU やメモリの状態をみたり、意図しない Invalid 判定に対処したりする手順を「ケースごとの手順」として記述します。

1. ROA キャッシュサーバを指定し、VRP を受信できることを確認します。
2. ROV の判定結果に従って経路情報を扱うルールを設定します。
3. ケースごとの手順 — ROV 設定前後の CPU やメモリの消費状況を見る。
4. ケースごとの手順 — ROV の設定を解除して元に戻す。
5. ケースごとの手順 — ルータを再起動させたときの動作を確認する。
6. ケースごとの手順 — ROA キャッシュサーバへの再接続時間を確認する。
7. ケースごとの手順 — 意図しない Invalid に対処する。

■ルータごとの設定例

設定方法が分かっているルータの設定例を、本ガイドラインの Web サイト²において別紙として示します。

- Arista EOS
- Cisco IOS-XE
- Cisco IOS-XR
- Juniper Junos
- NOKIA SR OS

² <https://www.nic.ad.jp/ja/rpki/guideline/>

2.2.9 運用上の注意と懸念点

[1] ROA キャッシュサーバの構築・維持

現在、入手できる ROA キャッシュサーバの実装は OSS によるもののみとなっています。ソースコードが無償公開されているため利用可能ではありますが、自組織で構築運用するにあたり問題が生じ、これに対処する場合には、ソースコードを読んで実装を理解し、トラブルシューティングを実施する必要があります。

[2] 監視

ROA キャッシュサーバの正常性確認のためには以下の監視を行うことが考えられます。

- ROA キャッシュサーバの死活監視、プロセス監視、リソース監視などサーバ自体の監視 ※なお、RTR セッションが落ちても通信影響へは直結しない。
- ROA キャッシュの転送プロトコル (rsync や RRDP など) の失敗検出および回復
- ROA キャッシュの中身についても可能であれば検証する。複数の ROA キャッシュのデータを 1 日 1 回比較し、大幅な変更が発生した場合通知する等

[3] ROA キャッシュサーバと通信できない状態が発生した場合の対応

一般的には RTR セッションが切断された場合でも直ちに通信に影響することはないが、通信できない状態が、設定された hold time を超える可能性がある場合には以下の対応をする必要がある。

- BGP neighbor 毎もしくはルータごとの ROV の停止、もしくは ROA キャッシュサーバにおける SLURM を利用した VRRP 結果の変更等、Invalid / Not Found となる経路情報を破棄しないようにする。
(Invalid / Not Found となる経路情報を不許可・破棄といった設定をしている場合)

3. ROA/ROV 以外の不正経路対策

3.1 BGP におけるセキュリティの要素と考え方

ROV は不正経路対策として有効な手段ですが、全ての場合において不正経路の対策ができるわけではありません。ROV は特定のアドレスブロックがどの AS から広告されるかというオリジン検証を行うための技術であるため、BGP の経路情報における AS パス属性へ不正な AS 番号が挿入された場合に対処することはできません。

BGP ルータにおいては、他にも考慮すべきルーティングセキュリティ事項があります。参考になるものとして MANRS (Mutually Agreed Norms for Routing Security, <https://www.manrs.org/>) があります。MANRS で設けられたセキュリティ事項を満たし、確認することによりルーティングにおけるセキュリティを高めることができます。

3.2 AS パス検証の今後と運用について

BGP の経路情報に含まれる AS パス属性 (AS PATH) が正しいかを検証する AS パス検証という仕組みがあり、ASPA (Autonomous System Provider Authorization) という技術が検討されています。これを ROV と組み合わせることでよりセキュアな BGP 運用が可能となります。

ROA と ROV は標準化と開発が進み国際的に導入が進んでいる段階です。一方、AS パス検証は有効性の検証や標準化が進みつつありますが、開発は途上にあつて、国際的な動向を把握し、今後の適切な導入が ROV と同様に望ましい位置づけにあると考えられます。

ASPA を使った AS パス検証を行うためには、AS 番号の割り当てを受けている IR を通じて ASPA オブジェクトを作成する必要があるでしょう。

4. 用語集

用語	説明
PKI(Public Key Infrastructure=公開鍵暗号基盤)	公開鍵暗号方式による暗号通信や電子署名に用いる、公開鍵とその公開鍵の持ち主の対応関係を保証するための仕組み。
AS(Autonomous System = 自律システム)	インターネットにおいては同一ポリシーに基づいた IP ネットワークの集合を指す。本書では AS 番号を割り当てられた組織が管理するネットワークを指す。
BGP(Border Gateway Protocol)	AS 間で経路情報を交換するためのプロトコル [RFC4271]。
IR(Internet Registry)	インターネットで使用される番号資源(IP アドレス、AS 番号)を管理している組織。5つの地域 IR(ARIN,RIPE NCC,APNIC,LACNIC,AFRINIC)がそれぞれの地域に対してサービスを行なっている。下部組織として各国の NIR(National Internet Registry,日本においては JPNIC)が存在する。
SLURM	ROA キャッシュサーバに例外を記述する方式[RFC 8416]

5. おわりに

本ガイドラインは、1「ガイドラインの趣旨 ■本ガイドラインについて」に記載の通り、令和4年度総務省事業「ISPにおけるネットワークセキュリティ技術の導入に関する調査」及び令和5年度総務省事業「ISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査」の結果として同実証事業へ参加した実証事業者の意見・有識者検討会メンバーの意見を基に案が作成されました。

その後、総務省から当センターがガイドライン案を引き受け、「ガイドライン」として公開するにあたり、総務省における実証事業時に有識者検討会メンバーとして活躍された次のメンバーに、引き続き当センターの「RPKIガイドライン専門家チーム」メンバーとしてもご尽力いただき、レビューと改訂を行いました。そしてここに正式なガイドラインとして公開するに至りました。

- BBIX 株式会社 芦田宏之氏
- 大阪大学 猪俣敦夫氏
- 長崎県立大学 岡田雅之氏
- ノキアソリューションズネットワークス合同会社 小川怜氏
- ジュニパーネットワークス株式会社 清水一貴氏、
- 株式会社まほろば工房 高田寛氏
- アリスタネットワークスジャパン合同会社 土屋師子生氏、
- 慶應義塾大学 中村修氏、
- シスコシステムズ合同会社 服部亜希子氏
- 株式会社インターネットイニシアティブ 松崎吉伸氏
- 株式会社まほろば工房 三ツ木絹子氏
- 株式会社インターネットイニシアティブ 蓬田裕一氏
- NTT コミュニケーションズ株式会社 渡辺英一郎氏
- ジュニパーネットワークス株式会社 渡邊貴之氏

本ガイドラインに関するご意見・お問い合わせは、以下のあて先に電子メールにてお願いいたします。

- 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 (JPNIC)
- RPKI 担当：rpki-query@nic.ad.jp