Vol.2021-DPS-186 No.17
Vol.2021-CSEC-92 No.17
2021/3/15

仮想的BGPリンクの分類と検知手法の検討

長坂 明紀 [1]　相田 仁[1]

概要：仮想的 BGP リンクは現在のインターネットにおいて防ぎづらい不正経路の一種であるが, その基本的な性質についての議論は未だ不十分である. 本研究では仮想的 BGP リンクをその形態ごとに分類し, その基本的な性質を分析する. またこれに基づいて具体的な検知手法についても議論する. 本分析から, 仮想的 BGP リンクは非常に多様な形態で実現可能であり, その影響範囲や動機, 検知可能性も様々であることがわかった. 影響範囲の大きい不正経路広告はその分検知されやすく, AS 同士の協力なしに検知可能であることが示された. また比較的単純な形態の仮想的 BGP リンクの検知が重要であり, 上流の AS が検知に参加することが重要であることがわかった. 複雑な形態の仮想的 BGP リンクはより検知しづらいものとなるが, どの様に検知範囲を広げてゆくべきかについて議論した.

Classification of virtual BGP links and consideration of their detection methods

1. はじめに

現在のインターネットは Autonomous System（AS）が相互に接続されることで形成されており，これらが経路情報を互いに交換することでデータの到達性が実現されている．Border Gateway Protocol（BGP）は AS 間で経路情報を交換するためのデファクトスタンダートであり，現在のインターネットの接続性を提供するにあたり重要な役割を担っている．一方で BGP の脆弱性はよく知られているところであり，現在でもその対応は不十分である [1], [2], [3]. 今日においても不正な経路広告が拡散し，本来の接続性が損なわれるといった事態が世界各地で起きている [4], [5]. そのような不正な経路への対策として，Resource Public Key Infrastructure（RPKI）[6] や，更に信頼性を高める BGPsec[7] が存在するが，これらを用いても防ぐことのできない不正な経路広告が存在することが確認されている [8], [9].

仮想的な BGP リンクはトンネル上に形成される直接接続されていない AS 間の BGP セッションであるが，これは正にそのような不正経路となる．これまで仮想的 BGP リンクの影響範囲や検知手法に関していくつかの分析が存在するが [8], [10], [11]，仮想的 BGP リンクの基本的な性質に関する分析は不十分な部分も多い.

本研究では仮想的 BGP リンクをモデル化した上で特徴ごとに分類・分析を行い，より複雑な形態についても取り扱う．またこれら分析に基づいた検知手法を提案し，その検知率や実現性・軽量性について評価と考察を与える．本研究では仮想的 BGP リンクを形成する動機や sibling AS についても考慮し，インターネットにおける仮想的 BGP リンクに関する総合的な知見を与える.

2. 研究の背景

2.1 仮想的 BGP リンク

通常の BGP セッションは物理的なリンクの上に張られるが，トンネルにより物理的なリンクを伴わない，仮想的なリンクを構築する事が可能である．すなわち直接接続されていない二つの AS が，BGP レイヤでは接続されることになる.

このような BGP リンクはまさに不正な経路であり，経路ハイジャックと呼ばれる攻撃に相当するものである．しかし BGP レイヤは物理レイヤから独立しているため，これは正当なリンクのように振舞う.

仮想的な BGP リンクの問題点は，まずその対策の難しさにある [3]．仮想的な BGP リンクは BGP レイヤから見て全く正しいものである．すなわち BGP レイヤのみではこれを完全に防止・検知する事ができない．RPKI や BGPsec などの技術が完全に有効となった場合であっても，仮想的

[1] 東京大学大学院工学系研究科

リンクによる不正経路を防ぐことはできない．広告されたそのような経路が物理的リンクによるものであるかは，外部から確認する事ができないからである．

また Traceroute などのデータプレーンでのツールはトラフィックの経路を調べることが可能であるが，本手法ではトラフィック自体をトンネリングできるため，このようなツールで検知することもできない．多くの種類のハイジャックを検知可能なツール [12] であっても，仮想的リンクを検知するには至らない．

別の問題点として実現しやすさもある．二つの AS が協力してトンネルを張るだけで実現可能であり，物理的距離が離れているどの二つの AS であってもこれを張ることが可能である．以降の分析で分かるようにこの実現しやすさは非常に本質的な問題であり，簡単な手法と低いコストによって RPKI などのセキュリティを回避して行われる，影響の大きい不正経路広告を検知することが重要となる．

2.2 関連研究

2.2.1 影響・検知手法

これまで述べたようにこの不正経路を未然に防止することは難しいため，既存研究ではその影響の大きさや検知手法に関する検証が取り上げられている．

Li ら [10] は仮想的な BGP リンクによる不正な経路広告の影響について，AS の大きさ（カスタマーの数の多さ）で分類して検証している．Li らによれば，最大で 89%ものAS が影響を受ける．

検知手法については，Youssef らの提案 [11] や Li らの提案 [8] などがある．Li らの提案 [8] では，後述する network flow watermarking[13] と呼ばれる技術を利用して，トラフィックがトンネルされているかを検証する．

これらの検証では各仮想的 BGP リンクの検知方法について議論しているが，仮想的な BGP リンクの一般的な性質については十分な議論が行われていない．一口に仮想的 BGP リンクと言っても様々なタイプを考えることが可能であり，それぞれの状況においてその影響や動機及び効率的な検知方法は変わってくると考えられる．上記の既存手法では非常に単純なトンネルの形のみが考慮されているが，より複雑な形を考えることも可能である．また既存手法では検知候補の範囲が非常に広く，効率的な検知手法であるとは言いづらい．検知候補の範囲を狭めより効率的な検知を実現するためには，仮想的 BGP リンクの適切な分類・分析が重要となる．影響を正しく評価するためには，BGP レイヤのみでなくトラフィックについても考慮する必要がある．また攻撃手法として仮想的 BGP リンクを捉える場合，攻撃者側の経済的な動機やその実現しやすさを考慮することも重要であり，そこから正味の被害や有効な検知手法を考える事が可能となる．本研究ではこれまで議論されることが少なかったこのような点に言及し，仮想的 BGP リンクをそれぞれの形態によってモデル化しその性質を分析する．またそれに基づいてその影響の大きさ，実現しやすさ，動機及び検知のしやすさについて評価し，具体的な検知手法を考える．

2.2.2 Network Flow Watermarking

Network flow watermarking（NFW）は通信の経路を検証するための技術である．トラフィックに watermark と呼ばれる情報を含ませることで特徴を持たせ，これを観測することでその通過を判定可能とするものである．文献 [13] によると，NFW はその手法によって主に四つの方式が存在する．エンコーダはこれらの方式によってトラフィックに watermark を埋め込み，デコーダは観測したトラフィックからこれら情報を読み取ることで，トラフィックがその地点を通過したことを確認可能となる．本研究においても検知手法として NFW を利用するが，どのような NFW を用いるか，及びその具体的手法に関しては言及しない．

3. 分類・分析

3.1 モデル化

以下では仮想的 BGP リンクの分類・分析のためのモデル化について示す．AS 間の接続には以下の二種類がある．

トランジット

AS がインターネットへ接続するために，トラフィック量に対して料金を支払うような，より大きな AS との接続．上流 AS をプロバイダ，下流 AS をカスタマーと呼ぶ．

ピアリング

AS 同士が合意して無料でトラフィックを交換する接続．各 AS をピアと呼ぶ．

よって AS は，プロバイダ経由のトラフィックが増加するとより多くのコストが発生し，カスタマー経由のトラフィックが増加するとより多くの利益を得る．すなわち，一般に AS はカスタマー経由の経路を最も好み，次にピア経由，最後にプロバイダ経由の経路を選択する．そこで，次の Gao-Rexford モデル [14] を用いることができる．

Gao-Rexford モデル

(1) AS は自身が自身の間接的なカスタマーにはならない．
(2) AS が a から b への経路を広告するのは，a か b が自身のカスタマーである場合に限る．
(3) AS はベストパスとして，カスタマーからの経路を最も好み，次にピアからの経路，最後にプロバイダからの経路を選択する．

実際のインターネットにおける BGP は各 AS の個別のポリシーに基づいて動作するが，多くの AS は Gao-Rexford のポリシーに基づいて動作し [15]，これに基づいた AS レベルのモデル化によって分析が行われている [16]．よって本分析でも Gao-Rexford モデルを採用し，ベストパスの選択手順を以下のように定める．

Vol.2021-DPS-186 No.17
Vol.2021-CSEC-92 No.17
2021/3/15

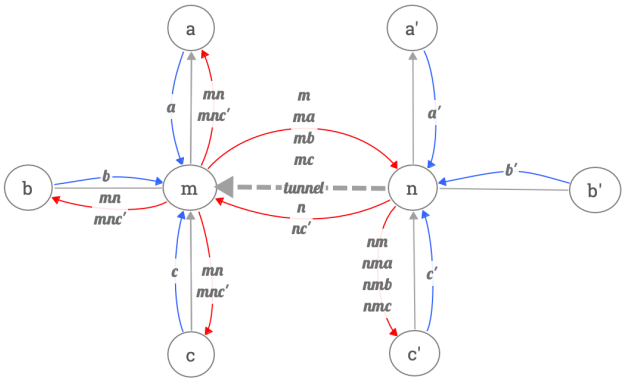

図 1　一本のトンネル上の仮想的トランジット
Fig. 1　Virtual transit on one tunnel.

ベストパス選択手順

(1) カスタマー経由の経路を最優先し，次にピア経由，最後にプロバイダ経由の経路を選択する．
(2) AS PATH が最も短い経路を選択する．
(3) AS 番号が最も若い AS からの経路を選択する．

Valley-free 構造

Gao-Rexford の条件から，インターネットにおける経路広告及びトラフィックは Valley-free と呼ばれる性質に従う．経路広告は上流経由で下流に伝搬することはあるが，下流を経由して上流へ伝搬することはない．この性質を Valley-free と呼び，Gao-Rexford 条件の元では経路広告とトラフィックはこの性質に従う．特に直接接続されていない二つの AS に注目した場合，この AS 間の通信は必ずどちらかの AS のプロバイダを通過する．これら性質は仮想的 BGP リンクのトンネルの形成方法及びトラフィックの流れに特徴を与え，以降での分類・分析及び次章における検知手法での議論で重要な役割を果たす．

3.2　不正経路広告の種類による分類

通常の AS 間の接続と同様に，トンネリングによる仮想的な接続もトランジットとピアリングの二種類を考えることができる．多くの AS に広告するほど経路を吸い込む確率は高まるが，そのような広告が無条件に行われた場合，これはルートリークとして外部から観測可能であるため，通常の接続であるトランジットとピアリングのみを考える．

3.2.1　トランジット型

図 1 はトンネリングによるトランジットを表す．ここで各ノードは AS を表し，AS 番号と共に描かれる．ノード同士を繋ぐ灰色のエッジは AS 間の接続を表し，有向エッジは AS 間のトランジット接続を，無向エッジはピアリング接続を表す．トランジット接続では矢印側がプロバイダ AS に，逆側がカスタマー AS に対応する．青色の矢印は通常の経路広告であり，矢印上の文字列は AS PATH を表す．赤色の矢印は不正経路広告を表す．AS m と AS n が協力する AS であり，m が仮想的プロバイダ，n が仮想的カスタマーである．AS a，b，c 及び AS a’，b’，c’ はそれぞれ m 及び n のプロバイダ，ピア，カスタマーである．m は仮想的プロバイダとしてトンネリングによる n からの経路を接続する全ての AS に広告し，接続する全ての AS からの経路を n に広告する．n は仮想的カスタマーとしてトンネリングによる m からの経路をカスタマーにのみ広告し，カスタマーからの経路のみを m に広告する．

影響範囲・動機

トランジット型ではプロバイダ経由で上流へ経路広告が拡散するため，多くの経路を吸い込む事が可能である．よってその影響の大きさを考えると十分な動機がある．一方で経済的な動機を考える場合，二つの AS の位置関係が重要となる．本モデルで示すように，プロバイダ・ピアへの広告はカスタマーの経路でない限り損益となる．よって仮想的プロバイダにとって，トンネルトラフィックがカスタマー経由である場合に限り利益があり，それ以外では費用が発生する．これは一本のトンネルによる仮想的リンクの場合では，n が m の間接的なカスタマーであるような状況に限られる．この場合 m は上流から吸い込んだトラフィックをトンネルとしてカスタマーに送出するため，経済的な利益も発生している．このような形の時，仮想的リンクは多くの経路を吸い込みかつ経済的な利益も発生するため，この形成により強い動機を持ちやすく，従ってこの形の仮想的リンクの検知は重要である．

検知可能性

仮想的トランジットでは不正経路広告はインターネット全体に広がり得るため，その影響範囲が大きい一方でより検知しやすいものとなる．多くの AS がこの経路広告を受け取り，特に上流の AS がその情報を取得可能となるが，そのような情報は様々な方法で公開されている．Tier1 などの大きな AS や様々な組織はインターネットの経路情報やトラフィック情報を提供していることも多く，例えば RIPE RIS[17] や Route Views[18] などからこの経路情報を取得可能である．よってどの AS であってもこの経路の存在を知ることが可能となる．特にトンネルされている AS もこのような経路広告を受け取る場合，自身を通過するトンネルトラフィックと比較することで，その AS のみで仮想的トランジットを検知することが可能となる．

3.2.2　ピアリング型

図 1 において，m から出る赤色の矢印が c にのみ伸びる状況が仮想的ピアリングに相当する．m と n は互いに仮想的ピアであるため，互いにカスタマーからの広告のみを，カスタマーのみに広告する．

影響範囲・動機

ピアリング型では不正経路はカスタマーにしか広告されないため，二つの AS の位置関係がどのような場合であっても利益となる．よって経済的な動機はより強くなる．一方で不正経路広告は下流にしか拡散しないため，その影響

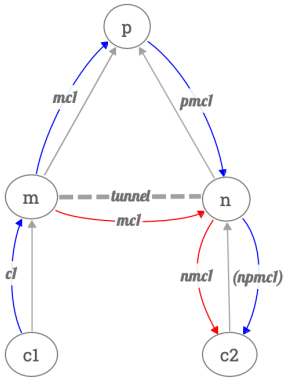

図 2　仮想的 BGP リンクの形成前後でトラフィックが変化しない状況

Fig. 2　The traffic does not change after the virtual BGP link between near ASes.

範囲はトランジット型と比較してだいぶ小さい．またその影響は適切に判断するためには，実際にどのようなトラフィックの変化が発生するのかを考慮した正味の影響を考える必要がある．

例として二つの AS m と n が，共通のプロバイダを経由したトンネルによって仮想的ピアリングを形成する，**図 2** のような状況を考える．不正経路を受け取る以前の c2 の c1 宛のベストパスが npmc1 だった場合，仮想的ピアリングにより不正経路 nmc1 を受け取ると，これをベストパスとして選択する．すると c2 は仮想的な BGP リンクを存在するとして通信するため騙されることにはなるが，実際のトラフィックはその前後で変わらない．元々 npmc1 がベストパスでない場合は，AS PATH の差が小さいので影響は最も小さい形になると考えられる．すなわちこののような仮想的ピアリングはローカルな性質があるため，より検知しづらい一方で，正味の影響も小さい．

検知可能性

ピアリング型では不正な経路広告はプロバイダに広告されないため，この経路情報はインターネットに広くは拡散しない．よって下流の AS がこれに気付く必要がある．トンネルが上流を経由して張られている場合，不正な経路広告を受け取った下流 AS はトンネルトラフィックを運ぶ上流 AS と協力することで検知できる可能性がある．

3.3　仮想的 BGP リンクの形成形態による分類

3.3.1　一本のトンネルによる仮想的 BGP リンク

仮想的 BGP リンクの最もシンプルな形として，一本のトンネルによるものが考えられる．仮想的 BGP リンクを形成する二つの AS は，自身の所持するプリフィックスのうち一部をこのトンネルのために使用し，この上で BGP セッションを維持する．すなわちトンネルトラフィックの送信元と送信先のアドレスは，仮想的 BGP リンクを形成する二つの AS のものとなる．また 3.1 節で示した Valley-free の構造から，トンネルトラフィックは二つの AS のうちどちらかのプロバイダ側を必ず通過する．これら性質を利用する事でより効率的な検知手法を考えることができ，次章ではその具体的手順を検討する．

3.3.2　複数本のトンネルによる仮想的 BGP リンク

三つ以上の AS が協力して複数本のトンネルを繋ぎ，その上で一つの仮想的 BGP リンクを形成することが可能である．これは一本のトンネルによる仮想的 BGP リンクを，更なる協力 AS を中継点として分割したようなものとなる．このような方式を採用することで，一本のトンネルの場合と比較して，より仮想的 BGP リンクを検知されづらいものにすることが可能となる．この方式ではトンネルの中継 AS が存在するため，トンネルトラフィックの送信者アドレス及び送信先アドレスは，仮想的 BGP リンクを形成する二つの AS の持つ IP アドレスであるとは限らない．よってそのようなアドレスを対象とした検知手法ではこの方式の仮想的 BGP リンクを検知できない．

また複数本のトンネルを経由するため，仮想的 BGP リンクとしてのトンネルトラフィックは Valley-free の制約を受けない．よって Valley-free を想定した上流での検知を回避することが可能となる．

ここで，sibling AS について考える必要がある．sibling AS とは，別の AS 番号であっても同じ組織によって運営されている AS のことである．例えば Google（AS15169）に対し YouTube（AS36561）があるが，これは利便性などを考えて別の AS として運営されている．このような構成は珍しくなく，むしろ大きい ISP は複数の AS 番号を所有していることも多い．このような状況では，ある組織が二つ目以降の AS 番号をうまく利用することで，簡単に仮想的 BGP リンクを検知されづらくすることが可能となる．

ところでそのような状況を想定すると，より複雑な構成をいくらでも考えることが可能であるが，そのようなものが検知できない事はある意味当然であり，また検知する必要もないことがわかる．同じ組織の AS のみによる仮想的リンクであっても，BGP レイヤから見ればやはり不正なリンクとなり得る．直接接続されていないに二つの AS が， BGP レイヤから見て そうであるような経路広告を行うからである．しかしそのような状況ではトンネルトラフィックを運ぶ AS として外部の AS が巻き込まれることはなく，協力 AS 同士のみのやりとりとなる．すなわちこれら AS が結合したより大きな AS のように見え，トンネルトラフィックは内部ネットワークでのやりとりと同義である．よってこれを外部の AS が検知する事は当然不可能であり，検知する必要もないと考えられる．より複雑な構成として，更に複数の AS が複数のトンネルによって仮想的 BGP リンクを形成した場合であっても，協力 AS によるクラスターのような構造がトンネルトラフィックを自由

に制御できるため，検知する事はできない．

むしろ仮想的 BGP リンクの本質的な問題は，ただトンネルを用いるという簡単な手法によって，既存のセキュリティである RPKI などを回避して不正広告を実行可能であるという点であると考えられる．よって仮想的 BGP リンクの検知対象としては，複雑すぎるものを考える必要はないということが分かる．特に一本のトンネルによる仮想的 BGP リンクを検知することが重要である．本研究でも検知対象としては比較的単純な形をまず想定し，段階的に検知対象の範囲を広げることを考える．

4. 検知手法

4.1 検知手順の提案

4.1.1 条件・範囲

検知対象としては，新規の仮想的 BGP リンクのみを考えることにする．現在のインターネットにおいて既に仮想的 BGP リンクが存在している可能性は十分にあるが，考えられる候補の数は膨大であり，その全てを検証する事は現実的ではない．仮想的 BGP リンクを形成し得る 2AS の候補は，観測される全ての経路広告の AS PATH に含まれる，全ての連続した 2AS である．そしてそれら候補がどのトラフィックをどのようにトンネルしているかも限定できない．仮想的リンクが外部から見て全く問題なく機能している状況では，完全に通常のリンクと同様に扱われ，これを疑う手がかりが存在しない．よって既存の仮想的リンクを検知するためには，網羅的な検証が必要となってしまう．そこで検知対象の範囲を新規リンクに限定する事で，検証候補を現実的な範囲に設定可能である．これら候補を AS PATH に含む経路広告を受け取ったとき，AS はベストパスとして採用するもののみを検証すれば良い．なぜならどのような不正経路であっても，それを利用する AS が一つも存在しなければ被害を受ける AS は当然存在せず，実質的になんの意味も持たなくなるからである．

以上のような特性を踏まえて，検知手法の形式としては各 AS が受け取った経路広告に対し，それぞれ実行するようなものとする．その方がそれぞれの状況に対し利用しやすいものとなり，適応的に検知可能であると考えられる．観測された多くの経路やトラフィックデータを元に静的に解析する手法では，先に述べたように網羅的なものとなってしまう．

4.1.2 具体的手順

トンネルの検知には，2 章で紹介した network flow watermarking を利用する．各 AS が実行する検知手法として，以下のような手順を考えることができる．

(1) AS は新規リンク mn を含む経路を受け取る．
(2) これをベストパスとして採用する場合，このプリフィックス宛に watermark を入れたトラフィックを送信する．
(3) 自身を通過する対象トラフィックの watermark を確認する（watermark self-check）．
(4) m と n の周辺 AS と協力し，対象トラフィックの watermark を確認する．

watermark self-check では，自身がトンネルとして利用され，その上で仮想的 BGP リンクが形成されているかを判定可能である．この段階で検知され得る仮想的 BGP リンクは主にトランジット型であり，上流を経由してきた経路広告が主な対象と考えられる．この方法は複数トンネルによる仮想的リンクにも有効であり，自身が不正なトンネルトラフィックの送信に気付かないうちに加担していないかを確認する一般的な方法となる．watermark self-check では各 AS が他の AS と協力する必要なく，自身の都合によって検証が可能なため，より汎用的であると言える．よってまずは self-check を行い，その後他の AS と協力して検知するような手順を取る．

協力する AS の候補としては，m または n の周辺 AS を考える．仮想的 BGP リンクであるならば隣接する AS のいずれかはトンネルされていることになるため，sibling AS による仮想的 BGP リンクでない限り，全ての隣接 AS と協力することで必ず検知することが可能である．しかし多くの AS と接続している AS も一般的であり，全ての隣接 AS と協力するには大きなコストが必要となる．一方で AS の接続形態には偏りがあり，プロバイダの数はピア及びカスタマーの数と比べて少ないため，プロバイダ AS と優先的に協力することでコストを削減できる可能性がある．3.1 節で述べたようにトラフィックは Valley-free に従って上流を流れやすく，プロバイダとの協力が重要であると言えため，初めはプロバイダ側の AS と協力し，次にピア，カスタマーと範囲を広げていくことでコストを抑えつつ検知可能性を上げていくことが可能である．以上のような仕組みによって段階的な検知が可能であり，各 AS の接続状況やリソースに応じて柔軟に対応可能なものとなる．コストの具体的な評価は 4.2 節で議論する．

watermark を自身で検証する場合であっても他の AS と協力して検証する場合であっても，どのトラフィックを検証対象とするかも重要となる．ISP には大量のトラフィックが流れているため，その全てを検証対象とする事は効率的ではない．この対象トラフィックに対しても，段階的な適用を考えることが可能である．以下では AS m に属するアドレスから，AS n に属するアドレスへのトラフィックを（m，n）と書く．まず一本のトンネルによる仮想的 BGP リンクでは，トンネルトラフィックは（m，n）または（n，m）であるため，このようなトラフィックの watermark を検証すれば良い．複数のトンネルによる仮想的リンクを検知したい場合，まず（m，*），（n，*），（*，m），（*，n）が候補となる．ただし*は任意の AS 番号である．この拡張によって m または n を端とするトンネルまで検知可能となる．更に sibling AS によるトンネルを検知するためには，

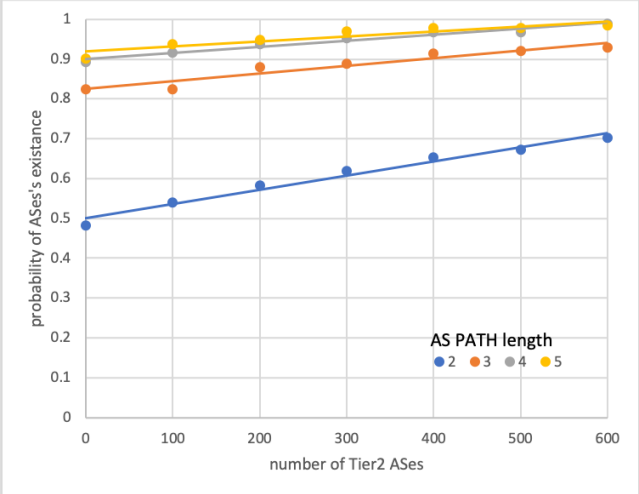

図 3 検知参加する Tier2 AS が Tier2 AS と Tier3 AS 間のトンネル上に存在する確率（Tier2 AS から Tier3 AS へのベストパス）

Fig. 3 Probability that Tier2 ASes that join the detection exist on the tunnel between Tier2 ASes and Tier3 ASes (best paths from Tier2 ASes to Tier3 ASes).

（sm，*），（sn，*），（*，sm），（*，sn）まで対象とする必要がある．ただし sm 及び sn は m 及び n の sibling AS である．このように検証対象トラフィックについても，状況に応じ段階的な適用が可能である．

4.2 性能に関する評価及び考察

4.2.1 検知率についての評価及び考察

上のような検知手順によってどの程度仮想的 BGP リンクが検知可能であるか検証する必要があるが，これまでの分析によりその検知率は仮想的 BGP リンクの形や AS の接続関係及び状況によって幅広く変わると考えられる．そこで本研究ではより一般的な議論を行うために，まず AS の接続関係からトンネル上に AS がどのように存在するかを検証し，これに基づいてそれぞれの状況における仮想的リンクの検知率を考える．

以下では AS をカスタマーの数によって分類し，文献 [19] と同様にカスタマーの数が 250 より多いものを Tier1，25 より多く 250 以下のものを Tier2，1 以上 25 以下のものを Tier3，0 の（すなわちカスタマーを持たない）ものを Stub と呼ぶ．また Tier1 AS は全て検知手順を実行可能であるとし，その上で Tier2 レベルの AS がどの程度検知に参加するかによってどの程度検知率が変化するかを検証する．測定はシミュレーションによって行い，CAIDA AS-relationship[20] の 2019 年 7 月のデータを用いた．

図 3 は Tier2 AS と Tier3 AS が一本のトンネルを張った場合に，そのトンネル上に検知手順を実行可能な Tier2 AS がどの程度の割合で存在するかを，その Tier2 AS の数とトンネルの AS PATH の長さ毎に示したものである．

図 3 から AS PATH が長いトンネルほど検知率が高いことがわかる．特に AS PATH が 4 以上の場合，Tier2 AS が一切検知しない状況，すなわち Tier1 AS のみが検知する状況であっても 9 割程度検知可能であり，600 程度の Tier2 AS が検知に参加することで，ほとんど検知可能であるということがわかる．トンネルの AS PATH は長いほどトンネルトラフィックを運ぶ AS も多くなり，また被害 AS はより長い RTT を感じやすくなるため，長い AS PATH によるトンネルの検知率が 9 割以上ある事は，仮想的 BGP リンクの被害の軽減に大きな意味を持つ．

AS PATH の長さが短くなると検知率は下がり，特に長さ 2 の場合，すなわち二つの AS が一つの AS を介してトンネルを張る場合，検知率は大きく下がる．これはこのトンネルを検知可能な AS がその AS 一つのみとなるからである．このような短い（AS PATH 上の）距離でのトンネルは検知しづらく，最大でも 7 割程度となる．

以上で得られたトンネル上の AS の存在確率から，様々な形・状況の仮想的リンクに対して検知手順がどの程度有効であるかを議論することができる．

例えば Tier2 AS と Tier3 AS が一本のトンネルの上で仮想的トランジットを形成し，新規のプリフィックスを不正に広告する場合，その検知率はそのまま図 3 で考えることができる．新規プリフィックスはそれまで広告されていなかったため，この広告は必ず採用され，よってその経路は必ずベストパスとして選択される．よってこの経路はインターネット全体に必ず到達し，全ての AS が仮想的リンクの検証が可能である．これら AS がどの程度 watermark self-check を実行するかによってどの程度検知可能であるかは，まさに図 3 と対応すると言える．

AS 同士の協力による検知の場合であっても，これら存在確率を基準に考えることができる．例えば最もシンプルな形として sibling AS などが存在しない，Tier2 AS と Tier3 AS 間の一本のトンネル上の仮想的ピアリングの検知率を考える．これを検知するためには不正経路広告を受け取った AS が，トンネル上の AS と協力して watermark の検証を行う必要がある．よって実際にどの程度協力可能な AS がトンネル上に存在するかがその検知率を決定し，これはまさに図 3 で示されるものとなる．

仮想的 BGP リンクが複数本のトンネルの上に形成されていた場合，検知率は一本のトンネルにおける存在確率を合成して考えれば良い．例えば二本のトンネルによって形成される仮想的 BGP リンクについては，それぞれのトンネルの検知率を r_1，r_2 とすれば $1-(1-r_1)(1-r_2)$ となる．ただし実際には二つのトンネルは独立とみなせるとは限らないため，その分検知率は変化すると考えられる．二つのトンネルはある AS を中継点としており，その AS の周辺 AS が両方のトンネルに共通して含まれる可能性がある．

4.2.2 実現性・軽量性の評価

本検知手法ではそれぞれの AS が新規リンクを仮想的

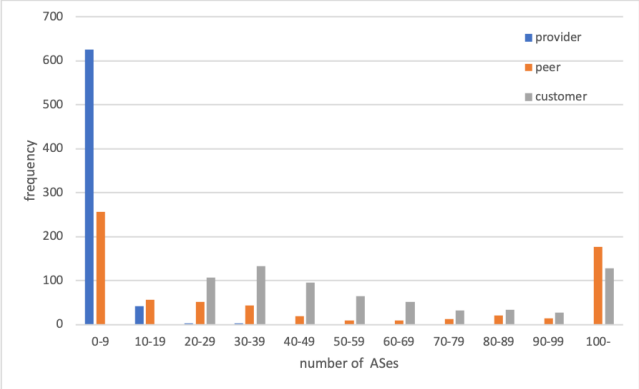

図 4　隣接 AS の数ごとに分類された Tier2 AS の度数分布
Fig. 4　Histograms of Tier2 ASes classified by the number of their neighbor ASes.

BGP リンクの候補として検知手順を実行する．そして検知率を上げるためにはより多くの AS が協力し，より広い範囲で network flow watermarking を実行する必要があるため，これがどの程度の実現性を持つか，及びより軽量に実現するための手法についても議論する必要がある．

まず network flow watermarking（NFW）自体の性質について考える．本検知手法では AS はベストパスとして採用する経路に対し，通常のトラフィックに watermark を入れ込んで検知を行うため，AS 間の通信時間や必要パケット数は問題にならない．文献 [13] では NFW の各方法の計算量や必要リソースなどの，共通の枠組みの中での適切な比較が不十分であるという指摘もあるが，必要パケット数は 1500 以下のものが多く，軽量なものでは数百程度の手法もある．NFW では一般に送信者とエンコーダが同一である必要はないが，本検知手法では送信 AS が watermark をエンコードする．よって送信 AS は事前にエンコードしておき，自身のタイミングでこれを送信すれば良いため，エンコード時間も問題にならない．また本手法ではトンネルの中継 AS がこれをデコードするが，これ自体はリアルタイムである必要はない．中継 AS は通過したパケットの情報（パケットの通過間隔など）を記録しておき，あとでこれを解析すれば良い．よってデコード時間も問題とならない．

次に検知手順を実行し得る AS の数について考える．ある AS と隣接する AS をその接続形態ごとに分類し，どの程度の AS が検知に参加するべきかを議論する．**図 4** は前節で使用したものと同様のデータセットにおいて，Tier2 AS をそのプロバイダ，ピア，カスタマー及びプロバイダのプロバイダの数ごとに分類した度数分布表である．図から 9 割以上の Tier2 AS は 10 未満のプロバイダ AS としか接続していないことがわかる．一方でピアに関しては，4 割程度の Tier2 AS は 10 未満のピアとしか接続していないが，2.5 割程度は 100 以上のピアと接続していることがわかる．カスタマーについては，20 未満のカスタマーとしか接続しない Tier2 AS はほとんどなく，比較的多くのカスタマーを持つ傾向があり，100 以上のカスタマーを持つものは 2 割程度存在することがわかる．このように Tier2 AS はプロバイダ AS よりもピア AS 及びカスタマー AS と多く接続していることがわかる．

以上の結果から検知参加する AS の範囲を限定し，より効率的な検知が可能である．これまで議論したように簡単な仮想的 BGP リンクの検知においてはプロバイダ AS の検知参加が重要であるため，このような検知対象に対しては比較的少ない AS との協力で十分であることがわかる．

次に一つの AS がどの程度検知手順を実行する必要があるかについて考える．検証リンクの候補として全ての既存リンクを考える場合，本分析で使用したデータセットでは Stub AS 以外の AS は 10000 程度あるため，非 Stub AS 同士のリンクを考えてもその候補数は ${}_{10000}C_2 = 5 \times 10^7$ となる．本手法では新規リンクのみを考えており，Isolario Project[21], [22] によると 1 日に観測される新規リンクは 200 程度である．AS 同士の協力においては上で示したように，プロバイダ側とのみならその数は最大で 10 程度である．

また実際には検知手順は並列実行可能であり，watermark を入れた一連のトラフィックに対し，これを自身と全ての協力 AS が確認すれば良い．すなわち 10 程度の AS と協力するとして，watermark を設定した一連のトラフィックを送信し，これを自身で検証し，協力 AS も検証すれば良い．また検知手順は複数の新規リンクに対して同時に実行可能である．

次に多くの AS が検知手順を実行した場合の，新規リンク周辺の負荷について考える．検知手順を実行することで watermark の入った検証トラフィックが発生するため，多くの AS が同時に検知手順を実行すると，その宛先 AS と経路で負荷が上昇する．新規の経路広告によって経路が吸い込まれトラフィック量が増加すること自体は本来の挙動であるため，多少の負荷の上昇は自然な領域であるとみなせるが，同時多発的な検知手順の実行があった場合はそれを超える負荷となり得る．よって負荷を軽減するためには，検知手順を実行するタイミングが集中しないようにするか，実行する AS の数を減らすことが考えられる．

トランジット型の不正経路広告の場合，多くの AS が上流を経由してこれを受け取りベストパスとして採用する可能性がある．そのような受け取り方をする AS や，不正経路の AS PATH が比較的長くなるような受け取り方をする AS は必ずしも検知手順を実行する必要はない．可能な限り AS 間の協力の必要なく（watermark self-check で）検知したい場合，多くの AS が watermark を入れたトラフィックを送信する必要があるが，AS 間の協力を十分認める上ではそのような AS の数が多い必要はない．例えば AS は Tier1 経由で下ってきた広告に対しては検知手順を実行し

ないとすることができる．あるいは本検知手順の段階的な性質から，軽量な手順のみを実行するということも可能である．一方で直接の上流または下流の AS は，全ての検知手順を実行することが望ましいと言える．このように直接の上流または下流の AS が十分に検知手順を実行する場合，その数は図 4 で示されるような範囲に限定される．検知手順における協力 AS の数についての議論と同様に，一本のトンネルの場合ではプロバイダ側 AS が検知手順に参加すれば十分であり，その数はピア側またはカスタマー側と比べて十分限定的である．よってそのような仮想的リンクの検知では負荷は十分抑えられる．

5. おわりに

本論文では RPKI などの技術によっても防ぐことのできない BGP 上の問題として仮想的 BGP リンクを取り上げ，これをその特徴によって分類し，これまで議論が不十分であった様々な性質について分析した．仮想的 BGP リンクは様々な形・状況で実現可能であり，その影響範囲や動機，検知可能性も様々であることがわかった．更にこれら分析に基づいて検知手法を考え，その検知率や実現性・軽量性について評価及び考察を与えた．本手法は段階的にその検知範囲を広げることが可能であり，柔軟な運用が可能となる．影響範囲が大きい仮想的 BGP リンクはより検知しやすく，AS 同士の協力なしに検知可能なものもあることがわかった．また比較的単純な形態の検知が重要であり，上流 AS の検知参加が重要であることを示した．複雑な形態の仮想的リンクはより検知しづらいものとなるが，どのように検知範囲を広げるべきかについて示した．

参考文献

[1] Li, Q., Liu, J., Hu, Y., Xu, M. and Wu, J.: BGP with BGPsec: Attacks and Countermeasures, *IEEE Network*, pp. 1–7 (online), DOI: 10.1109/MNET.2018.1800171 (2018).

[2] McDaniel, T., Smith, J. M. and Schuchard, M.: The Maestro Attack: Orchestrating Malicious Flows with BGP, *CoRR*, Vol. abs/1905.07673 (2019).

[3] Mitseva, A., Panchenko, A. and Engel, T.: The state of affairs in BGP security: A survey of attacks and defenses, *Computer Communications*, Vol. 124, pp. 45 – 60 (online), DOI: https://doi.org/10.1016/j.comcom.2018.04.013 (2018).

[4] BGPmon: Large hijack affects reachability of high traffic destinations, Cisco (online), available from ⟨https://www.bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/⟩ (accessed 2021-02-09).

[5] BGPmon: BGP leak causing internet outages in Japan and beyond, Cisco (online), available from ⟨https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/⟩ (accessed 2021-02-09).

[6] Lepinski, M. and Kent, S.: An Infrastructure to Support Secure Internet Routing, Technical Report RFC 6480 (2012).

[7] Lepinski, M. and Sriram, K.: BGPsec Protocol Specification, Technical Report RFC 8205 (2017).

[8] Li, Q., Zhang, X., Zhang, X. and Su, P.: Invalidating Idealized BGP Security Proposals and Countermeasures, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 3, pp. 298–311 (online), DOI: 10.1109/TDSC.2014.2345381 (2015).

[9] Song, Y., Venkataramani, A. and Gao, L.: Identifying and Addressing Protocol Manipulation Attacks in "Secure" BGP, *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pp. 550–559 (online), DOI: 10.1109/ICDCS.2013.32 (2013).

[10] Li, Q., Hu, Y.-C. and Zhang, X.: Even rockets cannot make pigs fly sustainably: Can BGP be secured with BGPsec, Workshop SENT' 14, 23 February 2014, San Diego, USA, Copyright 2014 Internet Society: Proceedings, Internet Society (2014).

[11] Gahi, Y., Israr, J. and Guennoun, M.: Wormhole Detection in Secured BGP Networks, *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 7–11 (online), DOI: 10.1109/CSCloud.2016.38 (2016).

[12] Sermpezis, P., Kotronis, V., Gigis, P., Dimitropoulos, X., Cicalese, D., King, A. and Dainotti, A.: ARTEMIS: Neutralizing BGP Hijacking Within a Minute, *IEEE/ACM Transactions on Networking*, Vol. 26, No. 6, pp. 2471–2486 (2018).

[13] Iacovazzi, A. and Elovici, Y.: Network Flow Watermarking: A Survey, *IEEE Communications Surveys Tutorials*, Vol. 19, No. 1, pp. 512–530 (online), DOI: 10.1109/COMST.2016.2604405 (2017).

[14] Gao, L. and Rexford, J.: Stable Internet Routing Without Global Coordination, *IEEE/ACM Trans. Netw.*, Vol. 9, No. 6, pp. 681–692 (online), DOI: 10.1109/90.974523 (2001).

[15] Gill, P., Schapira, M. and Goldberg, S.: A Survey of Interdomain Routing Policies, *SIGCOMM Comput. Commun. Rev.*, Vol. 44, No. 1, pp. 28–34 (online), DOI: 10.1145/2567561.2567566 (2013).

[16] P. Gill, M. Schapira, and S. Goldberg: Modeling on Quicksand: Dealing with the Scarcity of Ground Truth in Interdomain Routing Data, *SIGCOMM Comput. Commun. Rev.*, Vol. 42, No. 1, p. 40–46 (2012).

[17] RIPENCC: RIPE RIS, Réseaux IP Européens Network Coordination Centre (RIPE NCC) (online), available from ⟨https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris⟩ (accessed 2021-02-09).

[18] RouteViews: Route Views, University of Oregon (online), available from ⟨http://www.routeviews.org/routeviews/⟩ (accessed 2021-02-09).

[19] Goldberg, S., Schapira, M., Hummon, P. and Rexford, J.: How secure are secure interdomain routing protocols?, *Computer Networks*, Vol. 70, pp. 260–287 (2014).

[20] Dimitropoulos, X., Krioukov, D., Fomenkov, M., Huffaker, B., Hyun, Y., claffy, k. and Riley, G.: AS Relationships: Inference and Validation, *SIGCOMM Comput. Commun. Rev.*, Vol. 37, No. 1, p. 29–40 (2007).

[21] Gregori, E., Improta, A. and Sani, L.: Isolario: a Dout-des Approach to Improve the Appeal of BGP Route Collecting, *CoRR*, Vol. abs/1611.06904 (2016).

[22] IsolarioProject: Isolario Project website, Registro.it and Istituto Italiano di Tecnologia (online), available from ⟨https://www.isolario.it/⟩ (accessed 2021-02-09).