インターネットの基盤技術の現状と展望

松崎 吉伸 ●株式会社インターネットイニシアティブ シニアエンジニア

DNSSECやRPKIなど、DNSやBGPでの認証技術の対応が始まっている。DNSを悪用したDoSや、経路爆発、AS番号の枯渇、BGPのエラー制御などの課題も。

DNSとIPルーティングは、それぞれインターネットで名前解決と到達性確保を担っており、多くの通信が実質的に両者に依存している。ここでは、DNSについてDNSSECを始めとするセキュリティ対策やアクセス制御への利用を取り上げ、IPルーティングについては動的経路制御、特にBGP関連の技術動向を取り上げて解説する。

■ DNSとDNSSEC

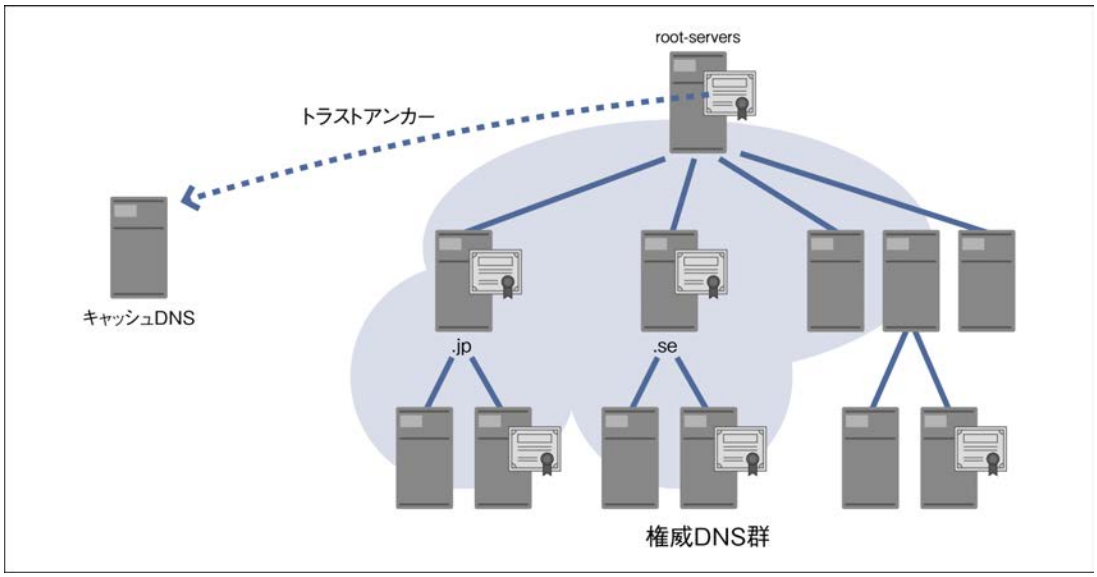
DNSは主にホスト名に対応するIPアドレスを検索するために利用されている。ほとんどの機器にはDNSを参照する機能が組み込まれている。DNSを参照する利用者はその設定を意識することはあまりない。ISPやシステム管理者が提供するキャッシュDNSが、DHCPやDHCPv6、PPPを通じて通知され、端末に自動設定されている場合が多い。

DNSの問い合わせにはUDPとTCPがともに利用できる。IIJが2013年4月に行ったキャッシュDNSの計測調査によると、99.99％程度はUDPによる問い合わせであった。

UDPでは簡易に通信できる反面、なりすましなどによる攻撃の可能性が懸念される。この攻撃への対応は古くから議論されている。対策として、DNSに公開鍵暗号技術を導入し、DNS応答の検証に完全性や認証などのセキュリティ機能を利用できるようにしたDNSSECが、IETF（Internet Engineering Task Force）で標準化されている。

DNSSECでは、DNS応答を検証する側が、信頼の拠点となる公開鍵情報をトラストアンカーとしてゾーンの管理者から取得する。これを基点に信頼の連鎖をたどることで、そのサブドメインに関してもDNS応答を検証可能としている（資料4-3-1）。IANA（Internet Assigned Numbers Authority）機能を運用しているICANNは、rootゾーンのトラストアンカーを公開しており、これを信頼の拠点にすればDNSツリー全体を網羅することができる。そのため、キャッシュDNSなどでDNSSEC検証する場合には、rootのトラストアンカーを取得して運用する場合が多い。

資料 4-3-1 キャッシュ DNS での DNSSEC 検証



出典：筆者作成

DNSSEC の署名も徐々に進んでいる。ICANN の調査によると、2013 年 10 月 25 日時点で root ゾーンに登録されている 323 のトップレベルドメイン中、128 ドメインが DNSSEC 署名をしている。このうち、119 ドメインはそのトラストアンカーを DS レコードとして root ゾーンに登録している。そのため、root のトラストアンカーからたどることで、これらのドメインについても DNSSEC 検証可能となっている。

.jp ゾーンでも、2010 年に DNSSEC 署名と root ゾーンへの DS レコードの登録が完了している。2011 年には JP ドメイン名サービスで DNSSEC への対応を開始している。これにより、JP ドメイン名の登録者が望めば、DS レコードを登録し、DNSSEC に対応できる状態となっている。

APNIC Labs による DNSSEC の利用に関する調査によると、2013 年 8 月時点でスウェーデンでの利用が突出しており、8 割弱程度のユーザーが DNSSEC 検証を利用している。そのほか、スロベニアやルクセンブルク、ベトナムなどでも、6 割弱から 4 割弱程度のユーザーが DNSSEC 検証を利用している。

日本でも、一部 ISP では DNSSEC 検証を有効にしたキャッシュ DNS を提供している。しかし、大手 ISP ではまだ主要なキャッシュ DNS で DNSSEC 検証を有効にしておらず、大部分のユーザーは DNSSEC を利用していない状況である。

■ DNS と攻撃

DNS では UDP による応答は 512 オクテットまでと規定されている。しかし、DNSSEC や IPv6 対応により、応答パケットサイズが肥大する傾向にある。そこで、より大きなデータサイズに対応するための EDNS0（Extension Mechanisms for DNS）が標準化されている。すでに多くの実装が EDNS0 に対応しており、UDP のまま 512 オクテットよりも大きな DNS 応答が可能となっている。

一方で、この DNS によるトラフィックの増幅

に注目し、DoS（Denial of Service、サービス不能）攻撃に悪用する事例も発生している。現在、キャッシュDNSでは、攻撃に関与することを防ぐため、適切な範囲にのみサービスを提供するようアクセスコントロールを適用するなどの対策が進められている。一方、権威サーバーは、インターネットのどこからの問い合わせにも応答しなければならず、単純なアクセスコントロールを適用できない。このため、DNS RRL（DNS Response Rate Limiting）などの対応策を試行しながら、適切な対応を模索している状況である。

■ DNSを利用したアクセス制御

DNSを利用した端末のアクセス制御も、さまざまな利用が広がっている。

ユーザーは、ホスト名を指定してインターネットのサービスを利用する。そのため、名前解決に利用されるDNSの応答を制御することで、利用者のアクセスの制限や誘導ができる。

広域なコンテンツ配信では、DNSが応答するIPアドレスを適切に変えることで、ユーザーをその近傍のコンテンツサーバーに誘導している。また、国によっては、好ましくないサイトへのアクセスをDNSで制御して制限している場合もある。

日本でも、一部ISPのキャッシュDNSでは、児童ポルノ画像の流通阻止のために児童ポルノサイトへのアクセスを制限する実装が導入されている。また、IPv6閉域網による遅延やアクセス障害といった影響を軽減するためにIPv6のIPアドレスを示すAAAAレコードの応答を抑制する、AAAAフィルタ実装が導入されている場合もある。

■ BGPと経路爆発

インターネットでは、ネットワーク間の経路交換プロトコルにBGPが利用されている。インターネットの広がりとともに、そのすべての経路数、いわゆるフルルートの経路数が増え続けている。

IPv4では、2009年4月に28万経路程度であったが、2013年4月時点では44万経路を超えている。IPv6に関しても、2009年4月には1500経路程度であったが、2010年頃から急激に増加し始め、2013年4月に1万3000経路を超えている。IPv4、IPv6ともに経路数は増加し続けており、ルーターの空きメモリを圧迫する要因となっている。これにより、フルルートでの運用を続けるにはルーターハードウェアの適切な増強や交換などの対応が必要となっている。

こうしたフルルート運用の負担を軽減するために、複数のグループ化されたルーターで分担して経路情報を扱うなどの技術提案がある。ただし、ネットワーク構成に制限が発生するなど、課題がそれぞれにある。そのため、これまでのところ、フルルート運用する必要のあるネットワークではハードウェア増強以外に広く受け入れられている対応策はない。

■ RPKI

BGPでは、誰がどんな経路情報を広報するか分からない。経路の広報元やそれをトランジットするネットワークが、経路フィルタを厳密に適用するなどして注意しておかないと、単純なミスなどによって生成された不正な経路情報が流通してしまう可能性がある。実際、インターネットでは不正な経路の広報による事案が発生している。

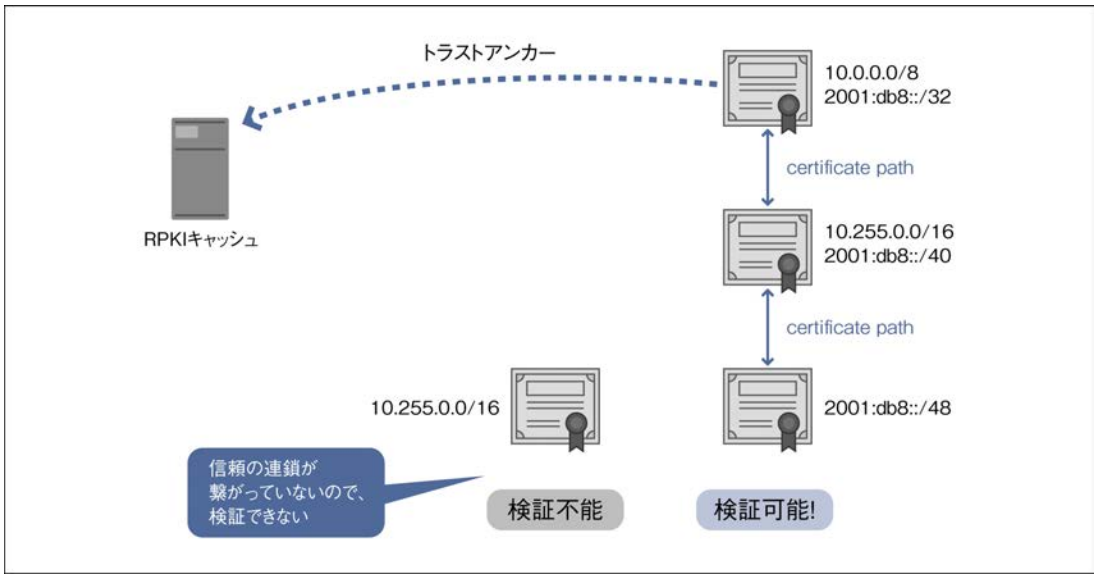
この問題に対応するため、RPKI（Resource Public Key Infrastructure）を利用した経路認証技術が提案されている。RPKIは、IPアドレスやAS番号といったインターネットの番号資源を割

り振るインターネットレジストリが、電子証明書によって資源の利用権利を示す仕組みである。すでにAPNICを始めとする世界のRIR（Regional Internet Registry、地域インターネットレジストリ）は、すべてRPKIによる電子証明書の発行に対応している。

RPKIでもDNSSECと同様に、電子証明書を検証する側が、信頼の拠点となる情報をトラストアンカーとして取得しておく必要がある。RPKIの現状では、APNICなど5つのRIRがそれぞれトラストアンカーを公開しており、これらを基点にして信頼の連鎖をたどることで、それぞれのインターネットレジストリなどが発行している電子証明書を検証できる仕組みになっている。RPKIキャッシュなど検証を行う側では、トラストアンカーからすべての電子証明書をたどって収集し、信頼の連鎖に基づいて電子証明書の検証を行う（資料4-3-2）。

将来的にはDNSSECと同様にトップレベルのトラストアンカーが運用されるかもしれないが、現状ではまだ特に決まった方針は示されていない。

資料4-3-2 RPKIキャッシュでの証明書検証



出典：筆者作成

■ RPKIを利用した広報元AS検証

RPKIでは、ROA（Route Origin Authorization）と呼ばれる電子証明書を発行できる。この証明書は、IPアドレスブロックとAS番号の情報を含んでおり、そのIPアドレスブロックの管理者がどのAS番号から経路広報するかを表明できる。これを利用して、経路の広報元ASの検証が可能になりつつある。

すでに、世界のRIRではROAの発行にも対応している。2013年10月時点で、世界で有効なROAオブジェクトは1700以上になっている。特にRIPE地域で継続的な増加が見られるほか、他の地域でも徐々にその数を増やしている。

発行されたRPKIの電子証明書を収集して検証するためのRPKIキャッシュも、いくつか開発が続いている。またルーターベンダーでは、RPKI

に対応したファームウェアを開発している。ルーターでROAの検証結果を受信し、実際の経路情報と突き合わせて経路制御に利用できるファームウェアである。このように、徐々に利用に向けて環境が整ってきている。

ただし、BGPの経路広報では広報元ASを偽装することも可能である。そのため、より厳密な確認のためには、経路が広報されて来たAS Pathを含めた検証が必要となる。現在、IETFなどでAS Pathまで含めた検証方式の議論が続けられている。

■4オクテットAS

BGPで利用されているAS番号としては、2オクテットの整数値が使われてきた。しかし、インターネットの広がりにともない、AS番号の在庫の枯渇が懸念されるようになった。

このため、AS番号を4オクテットに拡張する技術が標準化された。2007年から徐々に4オクテットASの割り当てが開始されている。現状では特に区別なく割り当てが行われているが、運用している機器が古くて対応していないなどの理由で、2オクテットのAS番号を要求するネットワーク運用者もまだ存在する。

2013年10月時点で、IANAの2オクテットAS番号資源在庫は残り500弱となっており、徐々に4オクテットのAS番号しか割り当てできない状況に進みつつある。ルーターも最近のものであれば問題なくサポートしている。AS番号は今後、徐々に単なる4オクテットの整数値として認識されていくと考えられる。

■BGPとエラー制御

BGPではエラー制御に関しても見直しが進んできた。

例えば、属性値が不正な経路情報を受信した場合に、単にBGP接続を切断するなどの実装があることが分かっている。こうした実装により、AS Path長が異常に長い経路情報や不明なBGP属性値を受信した際に、世界のあちこちでルーターがBGP接続を切断してしまう事例が発生した。

そのため、エラー処理に関して再検討が行われた。無闇にBGP接続を切断するよりも、単にその経路情報を無視した方がネットワーク運用上好ましい場合もあり、実装の見直しが進んだ。そのほか、IETFで新たな属性値などを標準化する際にはエラー処理を厳密に記述することが合意された。

■展望

DNSとIPルーティングでは、それぞれセキュリティ対応が迫られるなど、今までになかった制御方法の導入が進んできている。特に電子証明書を利用した厳密な検証では、署名側にも検証側にもより細やかな運用が要求されるため、今まで以上に精緻な運用が必要となってくる。

今後は、こうした新たな技術導入にともなう運用技術の向上と並行して、より網羅的な運用状態の観測と有用な異常の検出、それらを適切に関係者に伝えられる仕組みも必要となると考えている。

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2014年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先　株式会社インプレスR&D　✉ iwp-info@impress.co.jp