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（IIJ） シニアエンジニア

情報の正当性を検証できるように暗号技術の導入が続いているが、環境の変化に対応するため一部運用の見直しも求められている。

■DNS

DNSはドメイン名に対応した資源情報を応答する名前解決サービスで、主にホスト名に対応したIPアドレスを検索したり、メールの配送先を調べたりするために利用されている。インターネットで利用されるドメイン名の名前空間はルートを頂点とした階層構造を成しており、ドメイン名の一意性を担保するためTLD（Top Level Domain）ごとにレジストリと呼ばれる管理組織が指定され、運用管理されている。

■新gTLDと127.0.53.53

インターネットの利用が拡大し、より多様なgTLD（generic TLD）を求める声が高まったため、段階的に新規のgTLDが追加されてきた。特に、2012年に行われた募集では要件に沿う申請であればすべて認可される方針であったため1930件もの応募があり、所定の審査と手続きを経た新gTLDが2013年10月から登録され始め、その登録数は既に400を超えて増え続けている。新gTLDの導入では、名前衝突の可能性が懸念として挙げられた。これは、新たに登録されたgTLDと既に使用されているドメイン名がぶつかってしまうというものである。名前衝突が発生すると、接続障害や情報漏洩などを引き起こす危険性がある。

インターネットではレジストリがドメイン名の一意性を担保しているためこういった事態は発生しないように思えるが、レジストリの管理の及ばないところで名前衝突が発生する可能性がある。1つめは社内や組織内などで独自のTLDを勝手に利用していた場合、2つめはドメイン名を補完するサーチリスト機能を使ってドメイン名を一部省略した相対ドメイン名でサーバーなどにアクセスしている場合である。どちらの場合も利便性向上のために導入された実装であり、これまではうまく動いていたかもしれない。だが、問題を回避するためには、インターネットの変化に対応していく必要がある。

対策としては、組織内のみで利用しているドメイン名であってもレジストリに登録されたドメイン名を利用したり、サーチリスト補完に頼らないようにホスト名は常に完全なドメイン名で指定したりすることなどが挙げられる。

なお、新gTLDでは名前衝突問題を検出しやすくするため、登録認可後から一定期間はAレコードの問い合わせに対して「127.0.53.53」を応答することになっている。エラーメッセージなどにこのIPアドレスを見つけた場合は名前衝突の問題に遭遇している可能性があるため、関連する設定を見直すことが推奨されている。

■DNSSEC

なりすましなどによる偽装応答攻撃を防ぐため、DNSに公開鍵暗号技術を導入し、DNS応答の完全性の確認や認証などを行えるDNSSECが標準化されている。ccTLDの「.jp」をはじめとした既存のTLDの多くがDNSSEC署名しているほか、新gTLDでもDNSSEC対応が義務付けられたため、現状で7割以上のTLDがDNSSECでの電子署名を完了している。

これらTLDでは、ドメイン名の登録者が望めばDSレコードを登録してDNSSEC対応できる状態となっている。さらに、ほとんどのネームサーバーのソフトウエア実装が既にDNSSEC対応になっているため、DNSSEC署名を行う側の準備は整ってきている。

検証する側に関しては、クライアントが参照するキャッシュDNSで署名検証するモデルの実装が進んでいる。キャッシュDNSは接続サービスに付随して指定される場合がほとんどで、DHCPやDHCPv6、PPPなどを通じて自動的にクライアントに設定されている。

日本でも一部ISPがDNSSEC検証を有効にしたキャッシュDNSサービスを提供しているが、大手ISPでは主要なキャッシュDNSで検証を有効にしておらず、大部分の利用者はDNSSECを利用していない状況である。

一方、スウェーデンなどではISPでDNSSEC検証を実装しており、多くの利用者がDNSSEC検証を利用している。名前解決機能を提供する公開DNSサービスの一部でも検証を実施しているため、これら公開DNSサービスを参照先として使っている利用者もDNSSEC検証を利用できている。

APNIC Labsの調査では、アジア圏においてベトナムのDNSSEC検証利用者が突出している。ベトナムでは、これら公開DNSサービスの利用者が多いことによるものである。

■公開DNSサービスとEOS

公開DNSサービスに関しては、利用者が直接手動でクライアントに設定するほか、一部のISPなどがクライアントに自動設定している場合もある。その利用は徐々に広がっているとみられ、米Akamai Technologiesの報告によると特に発展途上国での利用が伸びているとのことである。

公開DNSサービスの普及により、一部のコンテンツ配信事業者の配信制御に影響があることも報告されている。DNSを配信制御に利用するコンテンツ配信事業者は、利用者は各ネットワーク管理者が用意するキャッシュDNSを利用しているとの前提に立ち、利用者が使うキャッシュDNSのIPアドレスを手掛かりにして所属するネットワークを推測し、近傍の配信サーバーのIPアドレスを応答していた。このため、公開DNSサービスが利用されると推測が実際と大きく異なってしまい、適切なIPアドレスを応答できなくなってしまう。

この問題に対応するため、ECS（EDNS Client Subnet）という方式がIETFで提案されている。これは、公開DNSサービスが利用者からDNS問い合わせを受けて名前解決のために他のネームサーバーに問い合わせを送出する際に、利用者の所属するネットワークの情報をDNS問い合わせに付加する仕組みである。コンテンツ配信事業者側では、付加されたネットワーク情報を基にその近傍の配信サーバーのIPアドレスを応答することができる。主要な公開DNSサービスでは既にこの仕様が採用されており、コンテンツ配信事業者でも徐々に対応が進んでいる。

キャッシュDNSをECS対応にするには、応答のキャッシュをネットワークごとに保持する必要があるなど設計上注意しなければならない点もあるが、公開DNSサービスを利用してもコンテンツ配信の最適化が行えるといったメリットも大きいため、今後は公開DNSサービスやコンテンツ配信事

業者での採用が進むと考えられる。

■IPルーティング

IPルーティングは、インターネットでパケットの到達性を担っている。基本的にはIPパケットの宛先を基に経路を決定しており、各ルーターはルーティングテーブルと呼ばれる宛先ネットワークと、それに対応する次の転送先のリストを保持している。つまり、IPルーティングは一方向の経路制御であり、双方向の通信が成立するには行き経路だけではなく、帰りの経路に関しても矛盾なく経路制御されている必要がある。

ルーティングテーブルを適切に保つために、静的な経路設定のほか、OSPFやIS-IS、BGPなどさまざまな動的経路制御プロトコルが利用されている。ISP間や巨大なネットワーク間ではBGPが標準的な経路制御プロトコルとして採用されている。

■経路増加

インターネットの広がりとともにグローバルなBGP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28万経路程度だったが、2014年4月には50万経路を超えている。IPv6に関しても2009年4月に1500経路程度であったが、2010年ごろから急激に増加し始め、2014年4月には1万7000経路を超えた。近年はIPv4とIPv6共に経路数は線形に増加し続けており、ルーターの空きメモリを圧迫する要因となっている。

BGPで他者の通信を仲介しないリーフと呼ばれるネットワークではフルルート運用をやめ、デフォルト経路とトラフィック制御に必要な一部の経路のみでの運用に切り替えたネットワークもある。これまで日本ではそれほど多くない運用形態だったが、ハードウエアの更新コストがフルルート運用のメリットに見合わないと判断したネットワークでは今後、徐々に広がっていくと考えられる。

一方で、多くのネットワークと相互接続しているような巨大なネットワークでは、必然的にフルルートあるいはそれに近い経路情報を保持しなければならず、今後も続くとみられる経路増加に対応していく必要がある。

■経路ハイジャック

BGPでは世界中のネットワークが経路情報を交換しており、経路フィルタなどで適切な予防策が講じられていないと、何らかの原因で生成された不正な経路情報が流通してしまうことがある。ほとんどの不正経路は設定ミスなどによる意図しない経路広報だと考えられており、経路ハイジャックと呼ぶには実態と懸け離れていると指摘されていた。

しかし2014年には、スパム送信者による意図した経路ハイジャックが観測された。以前からスパム送信のためにBGPで意図的に不正経路を広報している事例が論文などで指摘されていたが、2014年は特に数多くの事例が報告された。

メールサーバーでは、スパムの受信を防ぐために、送信元IPアドレスを基に受信の可否を決める運用を行っているものがある。例えば、スパムの送信に利用されたIPアドレスをリストにしておき、そこからの受信を拒否するといったものだ。スパム送信側はこのリストによる制限を回避するためにBGPで他者のネットワークの経路情報を広報し、そのIPアドレスを利用してスパムを送信したと考えられる。経路ハイジャックの被害を受けたネットワークにおいては、突然スパムに関する苦情が大量に届いたことをきっかけに経路ハイジャックに気が付いたという事例も報告されている。

■IRRとRPKI

このような不正経路の流通を防ぐ対策としては、

経路フィルタが有効である。手動による経路フィルタ更新では規模が大きな場合に動的経路制御の変動に対応するコストが高くなるため、自動化された手法が利用されている。

現時点で広く利用されているのは、IRR（Internet Routing Registry）を利用した経路フィルタの生成である。これは、各ネットワーク管理者が、自身が広報する経路情報をrouteオブジェクトやas-setオブジェクトとしてIRRのデータベースに登録し、これを利用側が参照することで経路フィルタの自動生成や確認に利用する手法である。

著名なIRRとしてはRADBがあるほか、RIR（Regional Internet Registry）やISPが独自に運用するIRRも存在する。多くの利用者がRADBを主要なIRRとして利用しているが、RADBでは利用料金さえ払えば誰でもどんなオブジェクトでも登録できるため、誤登録や情報の古いオブジェクトがあるなど、データの信頼性が大きな課題となっている。

JPNICが運用するJPIRRをはじめ、RIRなどによって割り振りを受けたIPネットワークブロックのみを登録できる制御機構を持つIRRも運用されている。しかし、世界的にはそれほど普及しておらず、RADBが主要なIRRとして参照されている現状ではIRR全体の信頼度向上には至っていない。そこで、RPKI（Resource Public Key Infrastructure）を利用した電子証明書の利用が提案されている。

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。既にIETFで標準化されており、世界の5つのRIRはすべてRPKIによる電子証明書の発行に対応している。

■ROAとRPKIキャッシュ

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。これを利用すると、経路の広報元ASを検証することが可能となる。

ROAの検証側では、RPKIキャッシュと呼ばれる電子証明書の収集と検証を担うサーバーを運用する。RPKIキャッシュは、RIRなどが公開するTAL（Trust Anchor Locator）と呼ばれる信頼の起点から電子証明書をたぐり、すべてのROAを含めた電子証明書を取得後に電子署名で信頼の連鎖を検証することで、有効なROAを識別してキャッシュに保持する。ルーターはこのRPKIキャッシュから有効なROAのリストを受け取り、BGPで受信した経路の判別に利用する。

国内でも公開RPKIキャッシュが試験的に運用開始されており、手元のルーターでRPKI実装を試したい場合やRPKIの動作を確認するために利用可能な状態となっている。ルーターがROAによる広報元ASを検証した後の、実際の経路制御に影響のある挙動に関しては、各ネットワーク運用者の判断に任されている。BGPの標準的な経路操作が利用できるため、RPKIの広報元ASの検証結果に応じて優先度の変更や経路フィルタ、BGP communityによるタグ付けなどが可能であり、各ネットワークに応じたポリシーを柔軟に実装できる。

ROAの発行も順調に進んでいる。2015年10月時点で、世界で有効なROAオブジェクトは3000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発行数を増やしてきている。

■終わりに

DNSやIPルーティングはインターネット通信で重要な役割を果たしており、ほぼすべての通信

が実質的にこれらの技術に依存している。このような技術も、利用形態の変化や社会環境の変化、新たな脅威の出現とともに変化を続けている。

今後もこのような変化は続くと考えられ、技術的には複雑さを増していく。したがって、その運用技術の向上も併せて進めていく必要があることが課題となっている。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［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～2015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