インターネット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

インターネット利用の多様化に伴い、DNSに関しては要素機能が細分化されるとともに、gTLDの追加とIDNの浸透が進んでいる。同時に、セキュリティや攻撃などへの対応も課題となっている。

■DNS

DNSはドメイン名に対応した資源情報について応答する名前解決を提供しており、インターネットで利用されている多くのアプリケーションは実質、DNSによる名前解決に依存している。DNSは主に、ホスト名に対応したIPアドレスやメール配送先の検索に利用されている。たとえばウェブブラウザーでアクセス先となるURLを指定する際も通信先をホスト名で記述している場合が多いが、ホスト名はDNSを使って名前解決され、ウェブブラウザーはそこで得られたIPアドレスに対して通信を行っている。

DNSの構成要素としては権威サーバーやキャッシュサーバーなどが認知されてきたが、多様なサービス形態の広がりとともに機能が細分化されてきている。役割としてはこれまでとほぼ同じく、上位のネームサーバーから権威委譲を受けて該当ドメイン名に係るゾーン情報の応答が期待される権威サーバーや、エンドホストやスタブリゾルバからの問い合わせを受けて名前解決した結果の応答が期待される参照用サーバーなどが挙げられるが、これらを実現するための要素機能を異なるサーバーで分担して実現する運用が広がっている。

要素機能としては①保持している資源情報への問い合わせに応答するコンテンツサーバー機能②反復問い合わせで名前解決を行うフルリゾルバ機能③他のネームサーバーから得られた応答結果を一時的に記憶して次回の問い合わせ時にはそこから応答するキャッシュサーバー機能④他のネームサーバーに問い合わせを転送するフォワード機能――などが挙げられる。

権威サーバーは主にコンテンツサーバー機能のみで構成される場合が多いが、処理能力の向上や高度なフィルター機能の提供を目的として、権威サーバー向けにキャッシュサーバー機能とフォワード機能のみを提供するサービスも存在する。ISPやネットワーク管理者が運用する参照用サーバーにはフルリゾルバ機能とキャッシュサーバー機能を持つものが多く、運用上、不要な問い合わせの流出を防ぐため、プライベートアドレスの逆引きゾーン情報などをコンテンツサーバー機能によって参照用サーバーに組み込んでいる運用も多く見られる。コンシューマー向けブロードバンドルーターにも参照用サーバーを担うものがあるが、これらの多くは利用者からのDNS問い合わせをフォワード機能で他の参照用サーバーに転送しているほか、一部のブロードバンドルーターではユーザーからのDNS問い合わせにいち早く応答するためにキャッシュサーバー機能を備えてい

るものもある。

■DNSの変化

インターネットに関わる人から、より多様な利用を求める声が高まり、DNSでも変化が続いている。

1つめは、新規のTLD（Top Level Domain）としてgTLD（generic TLD）が徐々に追加されてきていることである。2012年に行われた新規gTLDの募集では、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件もの応募があった。そして、所定の審査と手続きを経たgTLDが2013年10月から登録され始め、2015年11月末時点で、すでに790件を超えた。申請の中には取り下げられたものもあるが、いまだ500件を超える申請が審査中であり、今後、手続きの完了とともに順次登録されていくと考えられる。

2つめは、IDN（Internationalized Domain Names、国際化ドメイン名）の状況である。IDNはドメイン名を構成するラベルの記述にASCII文字以外も利用できるようにしたもので、たとえば日本語ドメイン名などで利用されている技術だ。すでにウェブブラウザーでは広く対応が進んでおり、ほとんどのブラウザーでIDNを用いたURLで指定のウェブページにアクセスできるほか、メールアドレスもIDNや多言語を利用できるように標準化されており、メールサーバーやクライアントでの対応が広がってきている。

セキュリティも、依然として大きな課題である。対応の一つとして、なりすましなどによる偽装応答攻撃を防ぐために、DNSに公開鍵暗号技術を導入し、DNS応答の完全性などを検証できるようにした「DNSSEC」が標準化されている。「.jp」などのccTLDをはじめとした既存のTLDの多くがDNSSEC署名に対応しているほか、新gTLDではDNSSEC対応が義務付けられているため、現状で1108登録されているTLDのうち8割以上の935がDNSSEC署名に対応し、ルートから連なるDNSSECの検証を可能にしている。

そのほか、このDNSSECによる信頼を根拠に、サーバーの各種サービスで利用しているTLS（Transport Layer Security）の電子証明書情報への問い合わせに応答する「DANE」が標準化され、アプリケーションでの対応が進んできている。

■DNSに関連した攻撃

DNSは、参照サーバー側に広くキャッシュサーバー機能が実装されているため、同じドメイン名を繰り返し問い合わせされても権威サーバー側に問い合わせることなく利用者に応答することができる。しかし、ドメイン名の一部でも異なっていれば、該当するドメイン名のゾーン情報を提供している権威サーバーに問い合わせが発生する。

これを悪用して、サブドメイン部の一部を変化させながらDNS問い合わせを送り続けることで同じ権威サーバーに問い合わせが集中するような、いわゆるDNS水攻め攻撃が2014年ごろから発生している。この攻撃では外部から利用できる参照用サーバー、いわゆるオープンリゾルバが踏み台として悪用されている。不適切な管理で何ら制限のかかっていない参照用サーバーや一部のブロードバンドルーターでは、DNSのフォワード機能がインターネット側からも利用可能になっているものがあり、これらがオープンリゾルバとして知られている。権威サーバー側では多数の参照用サーバーから問い合わせが殺到するように見え、これらが処理能力を超えた場合にはDoS（Denial of Service、サービス不能）攻撃が成立する。また、権威サーバー側が無応答になると参照サーバー側でも応答待ちの問い合わせが滞るため、性能劣化などの影響を受ける場合がある。

そのため、現在はオープンリゾルバの地道な撲

減や、参照サーバー側から権威サーバー側への問い合わせ数の制限などの対応策を試行・模索している状況である。

■IPルーティング

IPルーティングは、インターネットにおけるIPパケットの到達性を担っている。インターネットでは多くのルーターが相互に接続してネットワークを構成し、IPパケットを宛先まで転送している。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。

この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（Open Shortest Path First）やIS-IS（Intermediate System to Intermediate System）、BGP（Border Gateway Protocol）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。コンシューマー向けのブロードバンドルーターではデフォルト経路や宅内の経路など数個の静的なエントリーのみのルーティングテーブルを保持している場合がほとんどだが、ISPのバックボーンを構成するルーターではグローバルなBGPのすべての経路、いわいゆるフルルートの情報をBGPで交換しているため、56万エントリーを超えるルーティングテーブルを保持している。IPルーティングでは、これら途中経路上のすべてのルーターが矛盾なく宛先まで経路制御されて、初めてIPパケットが宛先に届けられる。BGPの経路情報は近年、IPv4で毎年4万経路強の増加、IPv6では毎年5000経路の増加と、共にほぼ線形に増え続けており、今後もこの増加傾向はしばらく継続すると考えられる。そのため、引き続きルーターの増強などの対応が必要となる。

■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、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。

たとえば2015年1月に、IIJが管理するIPアドレスブロックが米国のISPから勝手にBGPで経路広告される事象が発生した。このときは、経路ハイジャックの行為者が偽装した書面や偽の連絡先を用意して該当の米ISPにIPアドレスの持ち込みを信じさせることに成功したことが原因だった。残念ながら、行為者がどのような用途をもくろんで経路ハイジャックをしたかといった詳細は判明していないが、偽の書面の準備など相当リスクの高い手段を選んでいることから、何らかの悪意があったと推測している。今回の場合、該当の米ISPが提出書面や関連情報を十分に審査すれば防げた事例かもしれない。

一方で、IPアドレスの割り振りの根拠となるWhois情報は、検索に多少の事前知識が必要となる。RIR（Regional Internet Registry）やNIR（National Internet Registry）、LIR（Local Internet Registry）での階層的な割り振りや割り当て、RIR体制が成立する以前に分配されたIPアドレスの扱い、IPアドレスの移転が発生した場合の情報など、歴史的事情や現在の登録制度を理解していないと結果を適切に読み解けない。今回、IIJが経路ハイジャックされたIPアドレスブロックはこれらすべての場合に該当し、米ISPの担当者が読み解けなかったとしても理解できる点はある。

日本では早くからインターネットが取り入れられたため、当時に割り当てを受けたIPアドレスブロックが多い。これらはIIJの場合と同様にWhois検索が難しく、経路ハイジャックを意図する側からすると狙いやすく見えてしまう可能性が

ある。

このように、IPアドレスを管理している場合は、Whois情報の適切な更新やBGP経路広告の開始、不正経路広告の監視などの対策を講じる必要がある。

■RPKI

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の割り振りを電子証明書で証明するRPKI（Resource Public Key Infrastructure）は標準化されており、すでに世界の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。

RPKIでは、番号資源の保有者が文章などにIPアドレスブロック対応の電子証明書で電子署名することもできる。これにより、先の経路ハイジャック事例のようにIPアドレスをISPに持ち込んで利用する場合でも、書面に付加された電子署名を検証することで正当なIPアドレスブロックの保有者かを確認することができる。

また、RPKIでは経路の広告元ASを検証可能にするために、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。ISPではこれらROAを検証し、ルーターでの経路制御に反映することができる。ルーターの実装を見てもROAを利用した広報元AS検証の実装が進んでおり、徐々に利用環境が整ってきていると言える。

RPKIは番号資源の強固な認証基盤となり得るが、その真価を発揮するにはネットワーク運用者が適切に利用する必要がある。そのためには、公開鍵暗号の基礎や電子証明書の運用、その検証方法が広く認知されるような環境づくりが必要だと考えている。

■おわりに

DNSやIPルーティングはインターネットで基盤的な役割を果たしており、ほぼすべての通信が実質的に依存している重要な技術である。これら技術には世界の多くの開発者や研究者、運用者が関わっており、電子証明書技術の導入など世界的な協調が必要な部分では長期的な展望とともに着実な検証と実装が必要となっている。

今後も広く知見を共有し議論を積み重ねながら、より良いインターネットの実現に向けて頑張っていきたい。

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～2016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