DNSSECの導入にむけて

**DNSは、インターネットに欠くことができないサービスです。
ここでは、DNSの役割を改めて振り返るとともに、昨今懸念されているDNSへの
脅威に対応する技術、「DNSSEC」について導入の課題と展望について説明します。**

2.1 DNSの役割

DNSは、問い合わせに対応したリソースレコードを応答するという単純なサービスですが、インターネットで事実上必要不可欠なサービスです。例えば、ユーザ自身はあまり認識していませんが、Webブラウザでのページ閲覧やメールの送受信など、日常的なインターネット利用の舞台裏でもDNSが活躍しています。もちろんDNSがなくても通信はできます。ただし、通信先のIPアドレスを覚えておく必要があるなど、インターネットの利便性が大きく損なわれてしまうため、現実的には多くのユーザがDNSに依存していると言ってもよいでしょう。

DNSでは、ゾーンと呼ばれる範囲ごとに分散管理できるようになっています。インターネットではルート(.)ゾーンを頂点とし、必要に応じてサブドメインを設定して管理を権威委譲することで、ツリー状の分散管理が実現されています。例えば.jp ccTLDは株式会社日本レジストリサービス(JPRS)に権威委譲され、登録されたドメインはJPDNSと呼ばれるコンテンツDNSサーバ群を通じて公開されています。問い合わせを行う側は、このツリー状に権威委譲され、分散管理されているコンテンツDNSサーバをたどって必要なリソースレコードを見つけます。

多くの場合、手元の端末はこの作業を自分自身で行わずに、ISPやネットワーク管理者の運用するキャッシュDNSサーバに要求します。キャッシュ DNSサーバは、端末からの要求に応じてコンテンツDNSサーバをたどって必要なリソースレコードを検索し、結果を端末に返します。DNSが正常に稼働していないと、目的のサービスにアクセスできないといった障害が発生してしまいます。実際に、DNSのトラブルによってWebサイトにアクセスできないといった障害は、世界中でたびたび発生しています。

2.2 DNSSECの必要性

さて、DNSサーバの運用で一番起こしてはならないトラブルは何でしょうか。それは「嘘を答えること」です。誤ったリソースレコードを応答してしまうと、応答を受け取った側はそれを信じてしまうため、間違いの内容によってはかなり困った状況になってしまいます。世の中には悪いことを考える人がいるもので、この嘘の応答を意図的に注入する攻撃が存在しています。この攻撃が成功すると、あるWebサイトにアクセスしようとするユーザを、まったく別な任意のWebサイトに

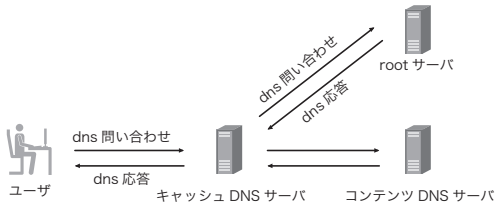

図-1 DNSへの問い合わせと応答

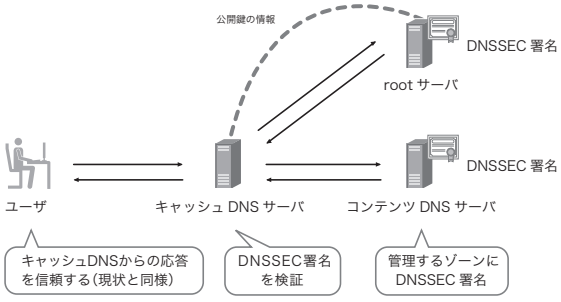

図-2 DNSSECの導入

誘導できてしまいます。これによって、アカウント情報を盗まれるといったような被害が容易に想像できます。さらに悪いことに、この攻撃は、現在の端末の性能や回線速度であれば実現可能です。

このような攻撃を想定して、DNSの応答が正しいかどうかを検証可能にする技術が検討されてきました。それがDNSSECです。DNSSECでは、公開鍵暗号方式を用いた電子署名をDNS応答に付加することで、応答の送信者を認証し、応答内容の完全性を確認できるようにしています。

DNSSECでは、ゾーンごとに電子署名を行います。この署名を検証するためには、それぞれの公開鍵の情報が必要です。DNSSECでは、サブドメインで署名に利用した公開鍵の情報をリソースレコードとしてゾーンに登録できます。このようにすることで、あるゾーンの公開鍵の情報を手に入れれば、その配下のドメインに関しては、登録された公開鍵の情報をたどることで検証可能になります。この信頼の連鎖によって、任意のゾーンからDNSSECを検証することも可能ですし、信頼の連鎖がきちんと繋がっていればルート(.)の公開鍵の情報さえ得ていれば、署名されたゾーンすべてが検証可能になります。

2.3 DNSSEC対応のための作業

ゾーンの管理者としてDNSSECへの対応を考えたときには、2つの作業が必要になります。1つはゾーンへの署名作業で、もう1つは署名に利用した公開鍵の情報を上位ゾーンに登録する作業です。ゾーンへの署名作業は、鍵の運用と密接な関係にあり、公開鍵暗号の知識、継続的な鍵の更新と署名の実施が必要になります。また、上位ゾーンに公開鍵の情報を登録する際には、上位ゾーンを管理するレジストリでのDNSSEC対応はもちろんのことですし、登録窓口となっているレジストラのDNSSEC対応も必要となります。.jp ccTLDでは、2010年10月17日にJPゾーンのDNSSEC署名を開始し、2011年1月16日にレジストリでの対応、つまり公開鍵の情報登録受け付け開始を予定しています。

問い合わせ側においては、まずISPやネットワーク管理者の運用するキャッシュDNSサーバでDNSSEC検証が行われ、端末がその検証結果を信頼するというモデルが普及すると考えられます。このようなDNSSEC検証を行うキャッシュDNSサーバでは、検証したい範囲に応じて信頼の拠り所となる公開鍵の情報を得ておく必要があります。ルート(.)がDNSSEC署名された現状では、ルートの公開鍵の情報を設定しておく方法が簡単な運用方法だと考えますが、運用ポリシによっては必要な範囲のみを検証可能にすることもありえるでしょう。いずれにせよ、これらの公開鍵の情報は、鍵の更新タイミングに追従して更新していく必要があります。

実際には、DNSSEC運用に関わるトラブルがすでに数多く報告されています。その内容は、更新作業を怠ってしまったという単純なケースから、運用ツールに問題があったというケースまでさまざまです。DNSSECでトラブルが発生すると、ほとんどの場合で署名検証に失敗し、キャッシュDNSサーバがエラーを応答します。すると、ユーザ側では、DNSから必要な応答を得られません。実際に、前述のトラブルでは、多くのユーザがWebサイトにアクセスできないといった大きな影響がありました。せっかくセキュリティ向上を目指してDNSSECを導入しても、きちんと運用できなければ、アクセスできないなどのトラブルを発生させてしまいます。

DNSSECでは、公開鍵暗号の知識や継続的な更新作業が必要であり、これまで以上にきちんとDNSを運用する必要があります。残念ながら現状では、気軽に導入できるようなものではありません。それでもDNS応答を検証できる機能は、重要なものであり、DNS応答を偽られたときに大きな被害が出るサービスにとっては、運用体制を作って導入を検討する価値があるものです。IIJでは、これまでにDNSSECの導入に向けてさまざまな試験や調査を行ってきました。また、いくつかのトップレベルドメインでのDNSSEC導入にも積極的に協力してきています。今後、これらの知見を生かして、DNSSECによるより安全な利用環境を提供できればと考えています。

執筆者:
松崎 吉伸（まつざき よしのぶ）
IIJ ネットワークサービス本部 ネットワークサービス部 技術推進課 シニアエンジニア。あれこれ面白しろそうな事を見つけては頑張っている。
IIJ-SECTメンバ、The Asia Pacific OperatorS Forum co-chair、APNIC IPv6 SIG chair、JPCERT/CC専門委員。