

JPRS トピックス&コラム



■DNSSECの概要と今後の展開

～「本当に正しい」を証明するために～

インターネットの利用に欠かせないDNS。DNSの信頼性を向上させ、より安全にインターネットを使えるようにする機能が「DNSSEC」です。その概要と今後の課題について解説します。

■インターネットの基本ドメイン名の一意性

インターネットの「住所」であるドメイン名。
user@example.co.jp や http://example.jp/ などのように、
電子メールアドレスや Web アドレス(URL)で相手先を
指定する際に使われています。

同じドメイン名はインターネット上のどこで使われても、
常に同じものを示します。これをドメイン名の**一意性**と
呼び、インターネットを円滑に利用するための基本的かつ
重要な原則の一つです。

ドメイン名の一意性が実現されているおかげで、私たち
は電子メールアドレスや URL を使って、情報交換や
情報の入手がスムーズにできるわけです。

■ドメイン名の一意性は DNS により実現

DNS(Domain Name System)¹は、インターネットにお
けるドメイン名の一意性を実現するための技術です。

DNS は、ユーザーが電子メールアドレスや URL などの
形で指定したドメイン名から、電子メールの送信や
Web サイトの閲覧に必要な IP アドレスやメールサーバ
ー情報などを調べる役割を担っています(図 1)。

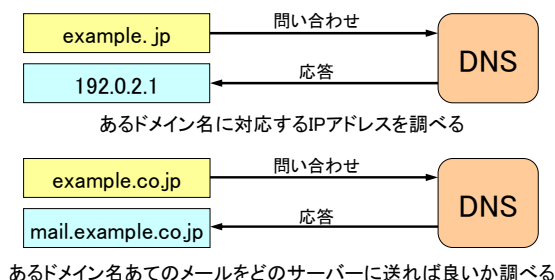


図 1: DNS の使用例

DNS が正常に機能し、ドメイン名を用いた正しい相手
先の指定が可能になることは、私たちがインターネット
を安全に利用するための必要条件の一つです。

¹DNS の動作原理については JPRS トピックス&コラム No.10「DNS のしくみと動作原理～インターネットを支え続ける DNS～」をご参照ください。

■DNS キャッシュポイズニング攻撃と DNSSEC

DNS への攻撃により動作を妨害し、インターネットの
安全な利用を妨げる行為は、インターネットが世界的に
普及し始めた 1990 年代から知られていました。

特に、DNS 応答を偽装し、偽の情報をキャッシュ
DNS サーバーに記憶させる「DNS キャッシュポイズニン
グ(DNS cache poisoning)」と呼ばれる攻撃方法につい
ては、専門家の間で早くからその危険性の高さが指摘
されていました。

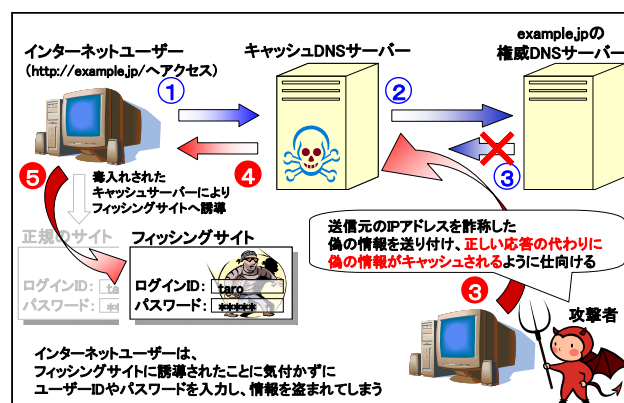


図 2: DNS キャッシュポイズニング攻撃の概要

DNS キャッシュポイズニングによって偽の DNS 情報
が仕込まれたキャッシュ DNS サーバーでは、その DNS
情報は「本物」として扱われてしまい、偽の DNS 情報で
あるということが受け取り側では判別できません。このた
め、偽の DNS 情報を信じて Web サイトにアクセスをしよ
うとしたユーザーがフィッシングサイトに誘導されたり、
電子メールが第三者に詐取されたりといった被害が発
生する可能性があります。

このため、DNS 応答の偽装を防止するための技術で
ある「DNSSEC(DNS Security Extensions)」の標準化作
業と開発が、インターネット技術の標準化推進団体であ
る IETF において進められてきました。

■DNSSECの概要

DNSSECは、受け取ったDNS応答が「本当に正しい」ものかどうかを検証することで、DNSのセキュリティを向上させるための拡張機能です。

▼信頼の連鎖により「本当に正しい」ことを検証

受け取ったDNS応答が「本当に正しい」ことを検証するためには、受け取ったデータについて以下の2点の確認が必要になります。

- ① 本当にその相手が登録したデータであること
(データ出自の認証: Data origin authentication)
- ② 通信途中で書き換えられたり、一部が失われたりしていないこと(データの完全性: Data integrity)

DNSSECではこの二つを、DNSの権限委任の構造に合わせた形で図3に示す「信頼の連鎖(Chain of trust)」を構築することにより実現しています。

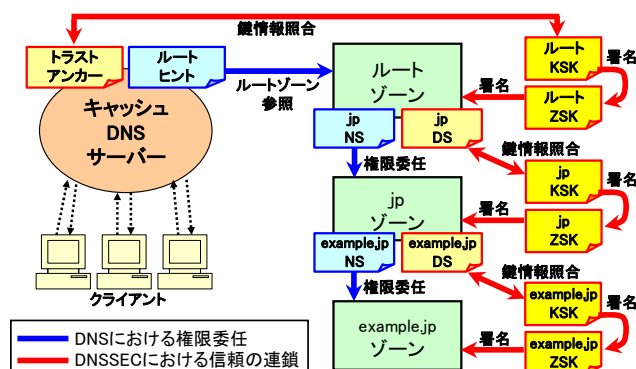


図3: DNSの権限委任とDNSSECの信頼の連鎖

▼DNS応答に「署名」の情報を付加

DNSSECではDNS応答にデジタル署名(以下、単に「署名」とします)を付加した応答を送ります。これまでのDNSでは応答を受け取った際に「正しい応答に違いない」と信じることはできませんが²、DNSSECでは送られてきた署名の情報により「正しい応答である」ということを、受け取った側で検証できるようになります(図4)。

² これまでのDNSもDNSキャッシュポイズニングなどによる攻撃のリスクを減少させるためのさまざまな仕組みを備えていますが、リスクを完全に回避することはできません。

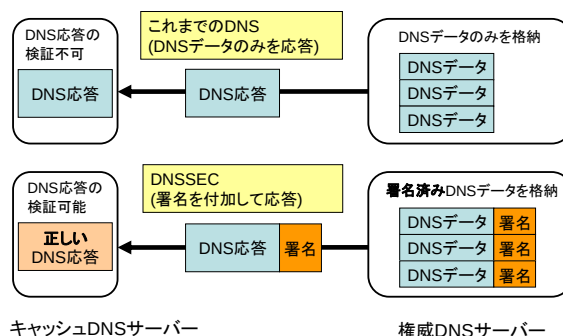


図4: これまでのDNSとDNSSECの応答の違い

■ルート・TLDにおけるDNSSEC導入が進行

社会インフラとしてのインターネットの重要性が増す中、DNSSECの導入により安全性の向上を図ろうとする機運が世界的に高まっています。このような背景から.jpや.com/.netなどを含む主要なccTLD/gTLDがDNSSECへの対応を相次いで表明し、2010年7月にはDNSSECの本格運用実現のために不可欠となる、ルートゾーンでのDNSSECの正式運用が開始されました。

JPRSでは2009年7月にJPドメイン名へのDNSSECの導入を表明し、2011年1月からJPドメイン名サービスにおけるDNSSECの正式運用を開始しました。また、世界最大のTLDである.comにおいても、2011年3月にDNSSECの正式運用が開始されています。

■DNSSECの導入・普及における検討課題

DNSSECでは、DNS情報を管理する側と検索する側双方の対応が必要になります。そのため、DNSSECの普及を進めるためには関係するすべてのDNSサーバーで、DNSSEC対応を進めていく必要があります。

また、DNSSECの導入により必要となるコンピュータの性能(CPU、メモリなど)や、DNSデータの増加に対応するためのネットワークの増強などについても、具体的な検討を進めていく必要があります。

更に、DNSSECに関連する情報の登録管理やDNSへの設定を実現するため、ISPやASPといったサービス提供者における業務システムや業務フローへの影響についても、十分な検討が必要になります。

このようにDNSSECの導入、普及を進めるためには、各関係者においてさまざまな検討を進め、それぞれの立場における課題解決を図っていく必要があります。