DNSSECって何?

DNSSEC（ディー・エヌ・エス・セック；DNS Security Extensions）は、DNS応答に添付された署名を受信側で検証することにより、正しい相手から届いた正しいデータであることを確認できるようにするための技術です。

DNSSEC導入により、DNS応答の偽造によるフィッシング詐欺サイトへの誘導や情報の詐取を図る「DNSキャッシュポイズニング」を検知し、攻撃を防ぐことができます。

ここでは、インターネットや情報セキュリティに関する基本的な内容について説明します。

一般利用者向け

サーバー管理者向け

情報提供元：株式会社日本レジストリサービス（JPRS）

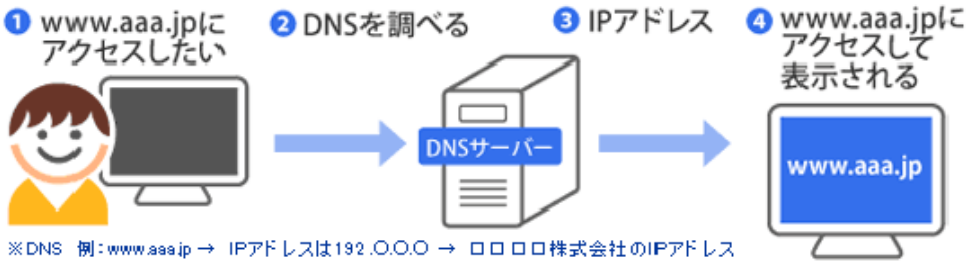
Copyright 2003－2011 総務省

DNSの仕組み

インターネットを利用していると、「DNS」という言葉を耳にすることがあると思います。まずはDNSについて、改めて説明します。

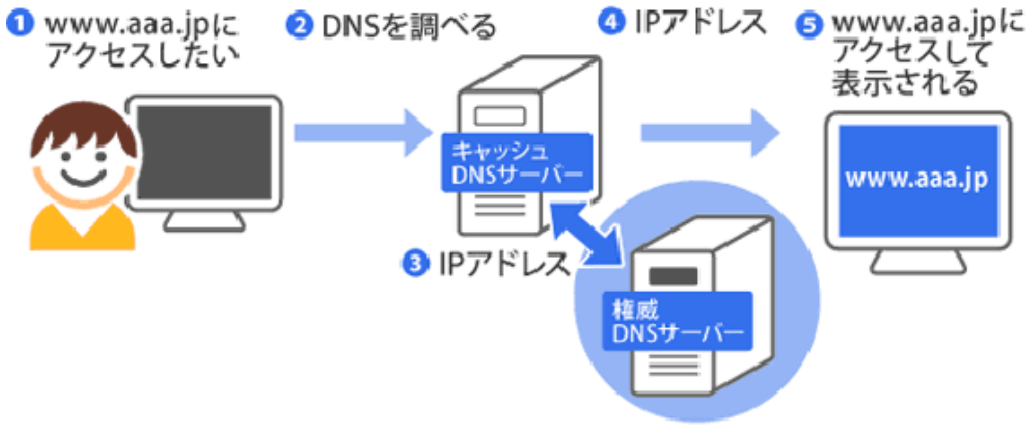
DNSは、インターネットにおけるドメイン名の一意性を実現するための技術です。
DNSは、ユーザーが電子メールアドレスやURLなどの形で指定したドメイン名から、電子メールの送信やWebサイトの閲覧に必要なIPアドレスやメールサーバー情報などを調べる役割を担っています。

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。



■正常なアクセス（1回目）

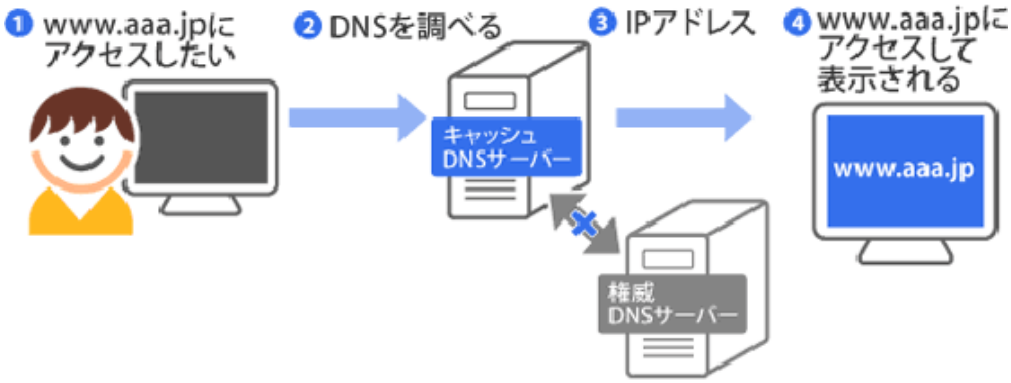
Webサイトにアクセスする際、ドメイン名から権威DNSサーバーにIPアドレスを確認し、調べたIPアドレスを使用して目的のサイトにアクセスします。
その際、権威DNSサーバーにアクセスが集中しないよう、キャッシュDNSサーバーを経由します。キャッシュDNSサーバーでは、受け取った応答をしばらくの間、保持します。



Copyright 2003－2011 総務省

■正常なアクセス（2回目以降）

2回目以降に同じWebサイトにアクセスしようとすると、DNSキャッシュサーバでは、以前のアクセスと情報が一致していれば、権威DNSサーバーに確認することなくキャッシュサーバーで応答し、IPアドレスに変換します。



Copyright 2003－2011 総務省

DNSに関するセキュリティ上の脅威

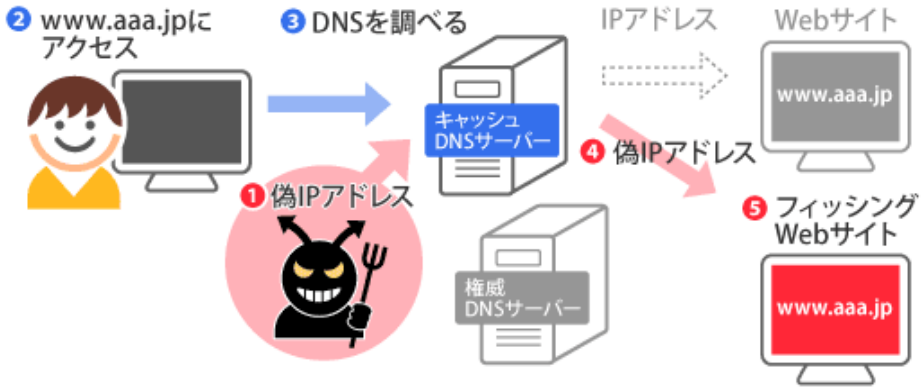
DNSキャッシュポイズニングとは？

2回目以降にWebサイトへアクセスする場合に、キャッシュDNSサーバーに保存されているIPアドレスを確認することになります。

そのキャッシュDNSサーバーに対して、偽の情報をキャッシュさせることにより、問い合わせた人に偽のIPアドレスで応答してフィッシング詐欺サイトにアクセスさせることが、DNSへのキャッシュポイズニングです。

■DNSへのキャッシュポイズニングの方法

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詐欺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。



DNSキャッシュポイズニングの方法でISPのキャッシュDNSサーバーが狙われた場合、ISPの利用者全員が被害に遭うことになります。

Copyright 2003－2011 総務省

DNSキャッシュポイズニングの特徴

・ユーザが正常なアクセスを行っても、フィッシング詐欺サイトに誘導される
ー攻撃されたことに気付きにくい
・同じキャッシュサーバーのユーザ全員が影響を受ける
ーISPのキャッシュサーバーが攻撃されると被害が甚大
・攻撃そのものの検出が容易ではない
ーキャッシュへの攻撃は、見た目は通常のDNSパケットであるため、正常な応答と攻撃の別が容易ではない。

DNSキャッシュポイズニングの対策方法

・他者からの攻撃手法への対策
ー攻撃成功確率を下げるパッチや、その手法を取り込んだ実装の採用
※ただし、対症療法であり、執拗な攻撃には無力
・キャッシュポイズニングへの根本対策
ーDNSプロトコルそのものが持つぜい弱性であり、完全対処にはDNSのセキュリティ面でのプロトコル拡張が必要

→このための技術が**DNSSEC**

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。

Copyright 2003－2011 総務省

DNSのセキュリティ上安全な仕組み(DNSSEC)

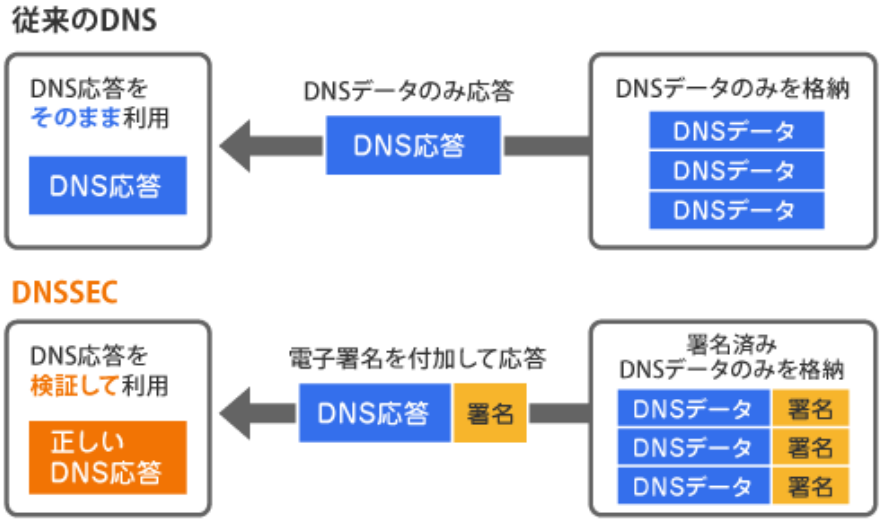
DNSSECは、受け取ったDNS 応答が「本当に正しい」ものかどうかを検証することで、DNSのセキュリティを向上させるための拡張機能です。

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。

・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）
・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「信頼の連鎖（Chain oftrust）」を構築することにより実現しています。

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」と信じることしかできませんが、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。



私たちにできること
ご自分の使用しているホスティングサービスがDNSSECに対応しているかを確認しましょう。
詳しくは、ご利用のプロバイダにお問い合わせください。

Copyright 2003 - 2011 総務省

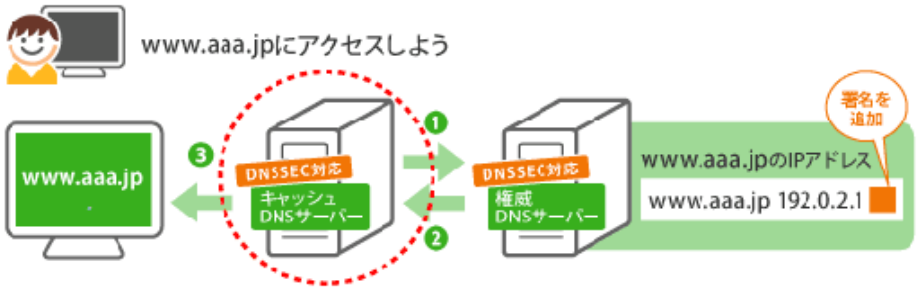
DNSSEC対応のために必要なこと

DNSを構成するそれぞれの立場での対応が必要となります。

・キャッシュDNSサーバーにおける対応
　－ISPなど
　－個々のキャッシュDNSサーバーのDNSSEC検証の有効化
・権威DNSサーバーにおける対応
　－DNSプロバイダ、ホスティング事業者など
　－個々の権威DNSサーバーにおけるDNSSEC署名の追加
・ドメイン名登録管理における対応
　－指定事業者（レジストラ）、リセラー
　－レジストリ
　－鍵情報の取り次ぎ、登録の実施

キャッシュDNSサーバーにおける対応

署名情報のやり取りとDNSSEC検証の処理により、キャッシュDNSサーバーのトラフィックが増加し、CPUの負荷が上がります。



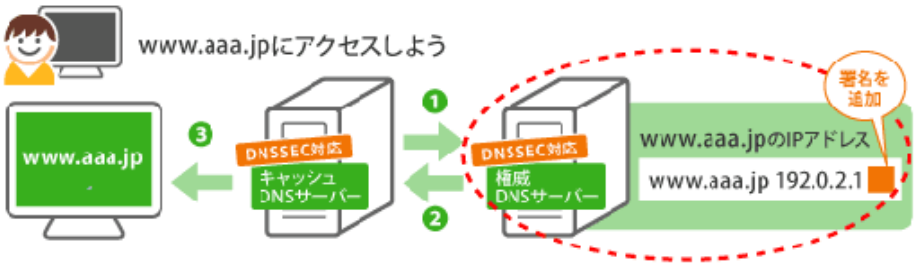
■運用者の対応内容

・キャッシュDNSサーバーのソフトウェアをDNSSECに対応しているものに更新
・DNSSEC検証の有効化
・必要に応じたCPU、メモリ、ネットワーク資源の増強
・トラストアンカー（ルートゾーンの公開鍵）の入手と設定

Copyright 2003－2011 総務省

権威DNSサーバーにおける対応

署名情報の格納と提供の処理により、権威DNSサーバーのトラフィックが増加し、CPUの負荷が上昇します。



■運用者の対応内容

・権威DNSサーバーのソフトウェアをDNSSECに対応しているものに更新
・必要に応じたCPU、メモリ、ネットワーク資源の増強
・ゾーン署名の実施
・ DSレコードの登録と鍵・署名の適切な管理運用

ドメイン名登録管理における対応

・ドメイン名のツリー構造における全階層で対応が必要
・ルートゾーンにおける対応
・TLDレジストリにおける対応
・レジストラ・リセラーにおける対応

■参考資料

・DNSSEC関連情報（JPRS）
→http://jprs.jp/dnssec/

・DNSSECジャパン
→http://dnssec.jp/
→http://dnssec.jp/?page_id=307（技術資料）

Copyright 2003－2011 総務省