Internet インターネット 10分講座

今月のテーマ

lame delegation

今回の10分間講座は、
lame delegationについて解説します。

lame delegationとは、DNSにおいて、ゾーンの委任が適切に行われていない状態を表します。今回は、lame delegationの解説とともに、その理解に必要となるDNSの分散管理構造と、ゾーンの委任についておさらいします。

またJPNICでは、今後、APNICなどで既に行われている、lame delegationとなっている逆引きネームサーバへの委任停止などの改善の取り組み開始を予定しています。それについても簡単に紹介します。

■DNSとは

DNS（Domain Name System）とは、インターネット上でドメイン名に関する情報を管理する分散データベースです。ホスト名とIPアドレスの対応を検索する、メール配送時に配送先サーバを調べるなど、さまざまな目的に使用される、インターネットにおける重要な技術の一つです。

■ドメイン名の分散管理

DNSは、特定のサーバでドメイン名の情報を一括管理せず、インターネット上に存在する多数のサーバで、データを分散して管理しています。

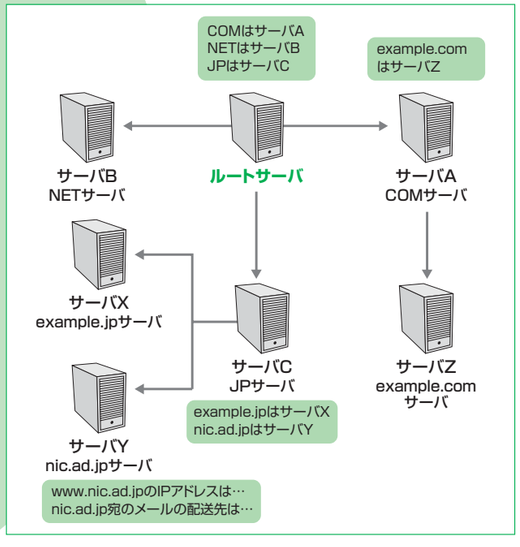
DNSデータベースの起点には、「ルートサーバ※1」と呼ばれるサーバが存在します。ルートサーバは、ドメイン名の情報を全て持っているわけではなく、たとえば、'JP'や'COM'など、トップレベルドメイン（Top Level Domain, TLD）※2の管理を、インターネット上に存在するどのDNSサーバ（ネームサーバ）に任せているかという情報を保持しています。

また、TLDのネームサーバでは、それぞれのドメインに含まれるドメイン名、たとえば、JPドメインのTLDネームサーバは、'example.jp'を管理するネームサーバがどこにあるのかという情報を保持しています。

そして、管理を任されたネームサーバが、他のネームサーバへドメイン名の管理を任せずに、自身でドメイン名の情報を持っていれば、そのネームサーバがホスト名などの情報に関する問い合わせに対して回答します。

このようにDNSは、ドメインの一部分（ゾーン）の管理を、別の複数のサーバへ任せる（ゾーンを委任する、委譲する、delegationする）ことを繰り返し、階層的な形（木構造）で構成されています。（図1）

図1　DNSのドメインのツリー図



■ゾーンの委任

ゾーンの委任は、以下の2点によって行われます。※3

（1）あるネームサーバAが、自身が管理するゾーンに含まれるサブドメインXについて、NSレコードと呼ばれる情報に委任先のネームサーバBを指定

（2）ネームサーバBが、任されたドメインXについて、Xに関する情報を保持し、問い合わせに正しく回答を行うように設定（図2・図3）

図2　サーバAからBへサブドメインXを委任する例

ネームサーバAが持つsome.domainゾーンの情報

some.domainのSOAは…
X.some.domainのNSはサーバB

ネームサーバBが持つx.some.domainゾーンの情報

X.some.domainのSOAは…
X.some.domainのNSはサーバB

図3　nic.ad.jpゾーンからsub.nic.ad.jpゾーンを委任する例

ネームサーバAが持つnic.ad.jpゾーンの情報

nic.ad.jpのSOAは…
sub.nic.ad.jpのNSはサーバB

ネームサーバBが持つsub.nic.ad.jpゾーンの情報

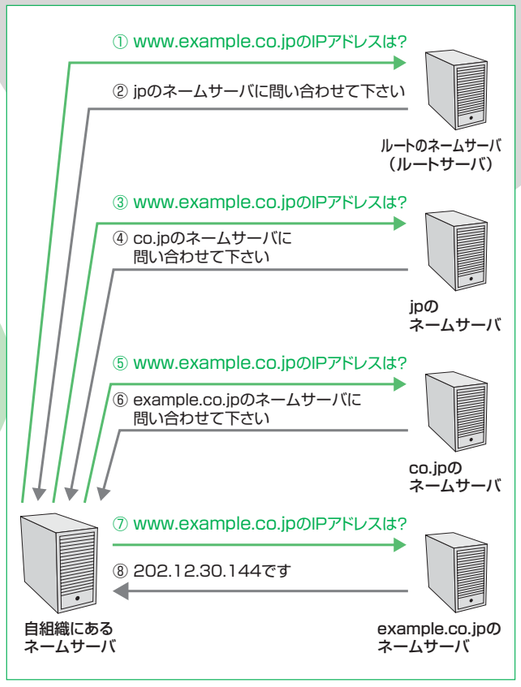
sub.nic.ad.jpのSOAは･･･
sub.nic.ad.jpのNSはサーバB

※1 ルートサーバ
DNSの最上位に存在する、「ルートゾーン」を管理するネームサーバです。例えば、JPネームサーバのIPアドレスは、ルートサーバに登録されています。ルートサーバは世界で13システムあり、個々のシステムはエニーキャストアドレスを使った複数台のサーバで構成されています。Mサーバの管理主体は日本のWIDEプロジェクトで、他にもFサーバ、Iサーバ、Jサーバ、Kサーバの一部が日本で運用されています。

■名前解決とキャッシュ

DNSにおけるデータベースの検索（名前解決）は、ルートゾーンから目的のゾーンまで委任を順に辿っていき、最終的に検索目的のデータを保持しているネームサーバを探し出して、そのサーバから結果を得ます。（図4）

図4　名前解決の例



※2 トップレベルドメイン（TLD：top level domain）
ドメイン名を構成するラベル（ピリオドで区切った文字列）のうち、一番右のラベルをTLDと呼びます。たとえば、「NIC.AD.JP」というドメイン名では、「JP」がTLDにあたります。TLDには、「JP」のようにカントリーコードを使ったccTLDや、「COM」のようなgTLDなどがあります。

※3 DNSにおいてゾーンの委任が正しく行われるための条件
ゾーンの委任が正しく行われるためには、

1. ゾーンの委任元において、委任先となるネームサーバを正しく指定すること
2. 委任先のネームサーバにおいて、委任されたゾーンについて正しい回答を返せるように設定すること

の二つの条件を満たす必要があります。

このとき、問い合わせを繰り返して処理するネームサーバやリゾルバは、名前解決の途中で得たネームサーバや委任の情報などを一時的にローカルに保存することができます。この処理をキャッシング（caching）といいます。同じデータが後で必要になった場合は、他のネームサーバへ問い合わせることなく、ローカルにキャッシュとして保持しているデータを元にして検索します。こうすることで、DNSでは、名前解決にかかる時間の短縮を図っています。

また、名前解決の途中で「そのドメイン名は存在しない」といった回答を得た場合、その情報もキャッシュとして保存します。これをネガティブキャッシュといい、上記と同様に名前解決の途中で必要となった場合には、データが存在しないという情報として再利用します。

このキャッシュの仕組みは、名前解決を高速化するだけでなく、短時間に何度も同じ問い合わせを行わないようにする、つまり他のネームサーバへ問い合わせを集中させないようにするといった効果もあります。

■lame delegation とその原因

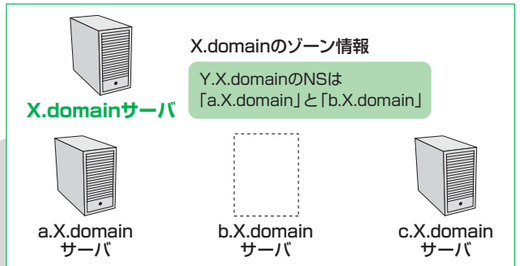
lame delegationとは、DNSにおいてゾーンの委任が正しく行われていない状態を指します。これは上述した二つの条件※3が満たされない状態であり、主に以下のような原因によって発生します。

(1)ゾーンの委任元における委任に関する設定ミス

ゾーンの委任元において、委任先となるネームサーバの指定が誤っている場合にはlame delegationになります。

このような状態となるよくある原因として、委任先のネームサーバを廃止・変更したにもかかわらず、委任元ゾーンで指定しているNSレコードを変更していない、委任されるネームサーバのホスト名に誤りがある、などが挙げられます。(図5)

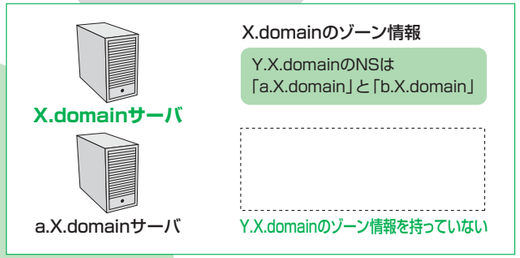
図5　ホスト名を間違えた例



(2)ゾーンを委任されたネームサーバでの設定ミス

ネームサーバの設定に誤りがあるなどの理由により、委任されたネームサーバが正しく動作していない場合や、委任されたゾーンについて正しく回答できるように設定が行われていない場合もlame delegationになります。(図6)

図6　ゾーンの設定をしていない例



(3)ゾーン転送の失敗

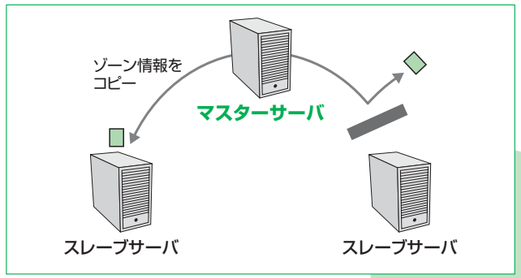
ゾーン転送とは、ゾーンのデータを持っていないネームサーバが、ゾーンデータを持っている別のネームサーバから、ゾーンのデータを取得する仕組みです。ゾーン転送が行われる際に、送信側となるサーバをマスタサーバ、受信側となるサーバをスレーブサーバといいます。

このゾーン転送の失敗が原因でlame delegationとなる場合があります。

例えば、ゾーン転送が正しく行われず、保持しているゾーンの情報がマスタネームサーバとスレーブネームサーバの間で異なる状態になり、ゾーンに関する情報について更新が行われなかった場合、lame delegationになる可能性があります。

ゾーン転送が失敗する理由としては、ゾーンデータを変更した際に、更新されたか否かを表すゾーンのシリアル番号を変更し忘れる、スレーブネームサーバのディスク容量が不足している、マスタとスレーブサーバの間でネットワーク障害が発生している、などがあります。(図7)

図7　ゾーン転送に失敗した例



■lame delegation の影響

ゾーンの委任がlame delegationとなっている場合、インターネットからそのゾーンに関する情報の検索ができなくなります。また、検索ができなくなるだけでなく、インターネットへ影響を及ぼすことがあります。lame delegationによる主な影響としては、以下のものがあります。

(1) lame delegationとなっているゾーンを参照するときに名前解決に時間がかかる、もしくは名前解決できないため、DNSを利用するサービスが遅くなる、利用できなくなる

(2) 名前解決の再試行が繰り返し行われるなどで、問い合わせ元と、ルートゾーンからそのゾーンまでのゾーン情報を保持する各ネームサーバ間で、無駄なDNSトラフィックが増大する

(3) lame delegationは発生したドメイン全てに影響が発生する

lame delegation になっているゾーンについては、ゾーンに関する正しいデータが得られず、また「存在しない」という情報、つまりネガティブキャッシュも得られません。そのため、キャッシュの仕組みがうまく働かず、そのゾーンに関する名前解決が行われるたびに問い合わせが行われます。その結果として、トラフィックの増加、ルートサーバをはじめとした他のネームサーバへの問い合わせの集中、名前解決のタイムアウト待ち、名前解決に失敗するなどの影響を引き起こすことになります。

■JPNICにおけるlame delegationに対する取り組み

JPNICでは、IPアドレスとドメイン名との対応付けを行う逆引きDNSを提供しており、IPアドレス管理指定事業者が管理するIPアドレスや、プロバイダ非依存アドレス（PIアドレス）※4からドメイン名への変換ができるようになっています。

実際に逆引きを利用するためには、割り当て先組織が逆引きのためのネームサーバ（逆引きネームサーバ）を設置する必要がある他、JPNICのデータベースに、その逆引きネームサーバに関する情報（ホスト名）を登録する必要があります。JPNICでは、データベースに登録された情報に基づいて、JPNIC（またはAPNIC）が管理する逆引きのためのシステムに、その逆引きネームサーバに関する情報を自動的に登録しています。これらの処理を経て、逆引きゾーンが設定され、逆引きが行えるようになります。

これまで説明してきたように、設定の不備などで正しく機能してない（lame delegationの状態にある）ネームサーバが増えると、正常な通信にまで影響を及ぼすことがあるため、APNICやJPNICなどのインターネットレジストリにおいても、lame delegationの状態にある逆引きネームサーバへの委任停止など、健全なインターネットの運用に向けた取り組みが進められています。

※4 プロバイダ非依存アドレス（Provider Independent Address）
PIアドレスやポータブルアドレスと呼ばれる、IPアドレス指定事業者に割り振られた空間以外から割り当てられたIPアドレスのことです。以前は非CIDRアドレスと呼ばれていました。

APNICでは既に2004年10月から、逆引きDNSのlame delegation改善に向けた取り組みを行っています。逆引きDNSを提供するJPNICにおいても、APNICと同様に正しく機能していない逆引きネームサーバの委任停止などの、lame delegation改善の取り組みを開始する予定です。

◇　　◇　　◇

ここからは、JPNICで実施を予定している逆引きネームサーバのlame delegation改善に向けた取り組みについて簡単に紹介します。JPNICでは、JPNICデータベースに登録されている、対象となるIPアドレス（表1参照）の逆引きDNSとしてJPNICデータベースに登録されているサーバに対して、表2の基準に沿って正しく設定されているかどうかの確認を、1日1回行います。いずれかの基準に該当する場合、そのネームサーバはlame delegationの状態にあり、適切に設定されていないネームサーバであると判断します。

表1　逆引きDNSにおけるlame delegation改善に向けた取り組みの対象となるIPアドレス

- IPアドレス管理指定事業者が管理するIPアドレス
- 特殊用途用プロバイダ非依存アドレスの割り当て先組織が管理するIPアドレス
- 歴史的経緯をもつプロバイダ非依存アドレスのうち、「歴史的経緯をもつプロバイダ非依存アドレス割り当て規約」に同意し、JPNICと確認書による手続きを完了した組織が管理するIPアドレス

表2　設定が正しくないとされる逆引きネームサーバの判定基準

- UDPポート53番へのDNSクエリに応答しない場合
- 委任された逆引きゾーンのSOAレコードについての問い合わせに対して、サーバから応答が無い場合
- 委任された逆引きゾーンのSOAレコードについての問い合わせに対して、サーバからAAビットを含まない返答がある場合

判定基準の策定にあたっては、JPNICオープンポリシーミーティング、IPアドレス管理指定事業者連絡会、各種のメーリングリストなどで、ネームサーバの運用経験に基づいたご意見を数多くいただきました。表2の基準は、これらのご意見をもとに検討を重ねて策定された基準になっています。

表2の基準により確認が行われ、設定が正しくない状態であると15日連続して判定された場合には、そのIPアドレスの割り当て先組織と、該当するIPアドレスを管理するIPアドレス管理指定事業者に対して、電子メールで通知を行います。それでもなお設定が正しくない状態が30日間連続し、初めて設定が正しくないと判定された日から45日連続でlame delegationの状態であると判定された場合には該当するネームサーバに対して逆引きゾーンの委任を停止するとともに、lame delegationの状態にある逆引きネームサーバであることをWHOISなどで表示します。（図8）

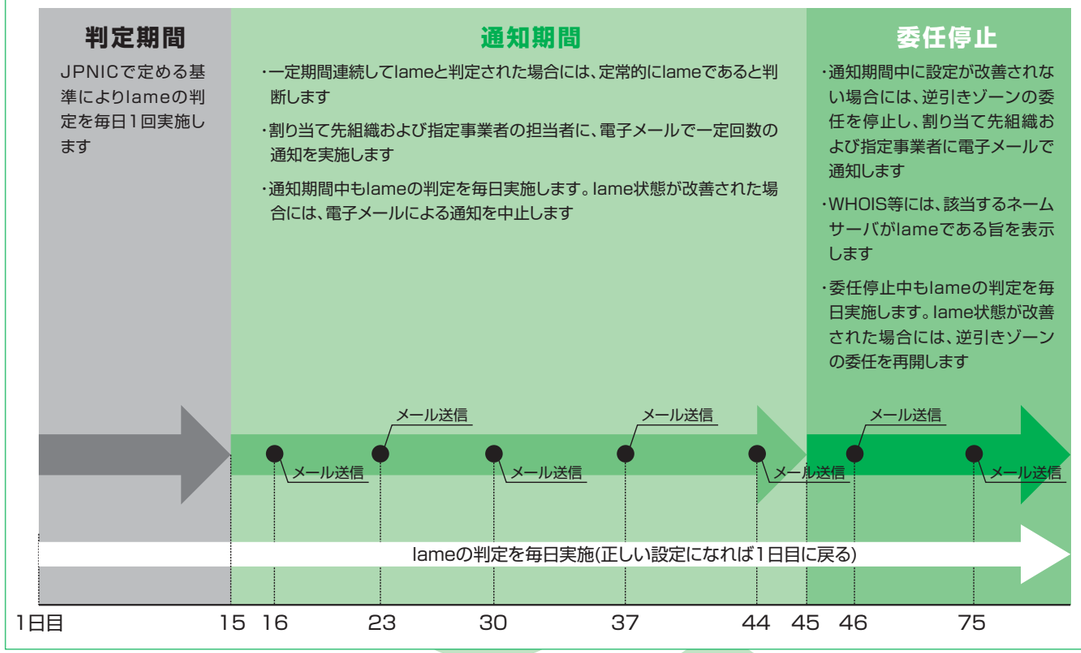
lame delegationの状態にあるかどうかの確認は毎日行います。逆引きゾーンの委任停止後にも、逆引きネームサーバの設定を修正したり、正しく設定されたネームサーバに変更するなどにより、ネームサーバが正しい設定の状態であることがJPNICで確認できれば、順次委任が再開されます。

◇　　◇　　◇

lame delegationの状態にある逆引きネームサーバに対して、ゾーンの委任が停止されることにより、該当するネームサーバへの問い合わせが行われなくなります。その結果、問い合わせ元に正しくない応答が返ることや、タイムアウト待ち、再試行などによる無駄なDNSトラフィックを発生することを防ぎます。

DNSは分散して管理されるものですので、皆様のご協力があって初めて正しく機能します。今回の取り組みにおける趣旨をご理解いただき、健全なインターネットの運用にご協力いただければ幸いです。

図8　JPNICで実施する、lame delegationとなっている逆引きネームサーバの委任停止までの流れ



（JPNIC 技術部 小山祐司／IP事業部 川端宏生）