JPRS トピックス＆コラム

■DNSサーバーの引っ越し ～トラブル発生を未然に防ぐ手順とポイント～

サービスプロバイダーの変更などの際に必要となる、いわゆる「DNSサーバーの引っ越し」について、作業時のトラブル発生を未然に防ぐ、本来あるべき手順とポイントを解説します。

■「DNS サーバーの引っ越し」とは

サービスプロバイダーやレジストラ（JP ドメイン名では指定事業者）の変更に伴い、その対象となるドメイン名の権威 DNS サーバーが変更されることを、「**DNS サーバーの引っ越し**（以下、引っ越し）」と呼ぶことがあります。今回は引っ越しの中でも特に、

(A) **すべての権威 DNS サーバーのホスト名と IP アドレスが変更**される

(B) Web サーバーやメールサーバーなど、**権威 DNS サーバー以外のサーバーのホスト名は変更されず、IP アドレスのみが変更**される

場合について、作業時のトラブル発生を未然に防ぐ、**本来あるべき手順**について解説します。

なお、以降では「引っ越し」を、上記（A）及び（B）の二つの条件をともに満たす場合に限定して使うものとし、今回の解説では DNSSEC の運用については考慮しないものとします。

■引っ越しの際に考慮すべき二つの事項

引っ越しの際に考慮すべき重要な事項として、

① インターネット上のキャッシュ DNS サーバー群からの名前解決要求を、いかにして引っ越し先の権威 DNS サーバーに向けさせるか

② インターネット上のキャッシュ DNS サーバー群に、いかにして新しい DNS データ（ゾーンデータ）を提供するか

の二点が挙げられます。そして、これらはそれぞれ、前述の（A）と（B）に対応しています。

▼重要なのは手段ではなく本来の目的の達成

引っ越しの担当者は①と②のうち、権威 DNS サーバーの変更の反映、つまり①に大きな関心を寄せているようです。そして、引っ越しに当たり、いわゆる「**DNS の浸透**」や「**DNS の伝搬**」が**うまくいかない**という、②に起因するトラブル事例が数多く報告されています。

①は、引っ越しに際し必ず考慮すべき重要な事項です。しかし多くの場合、サービスプロバイダーやレジストラの変更における**本来の目的**は②（各種サービスを提供するサーバーの移行）であり、①は②を実現するための**手段**の一つに過ぎません。そして、この**本来の目的を円滑に達成する**ことが、引っ越しの際に考慮すべき、最重要事項となります。

■引っ越しにおける具体的な作業手順

以上を踏まえた、作業時のトラブル発生を未然に防ぐための、具体的な作業手順について解説します。

図1の引っ越し前の状態では、権威 DNS サーバーが保持する NS レコードが、自身が権威 DNS サーバーであることを示し、親が保持する NS レコードが、対象となるドメイン名の管理の委任先を示しています。

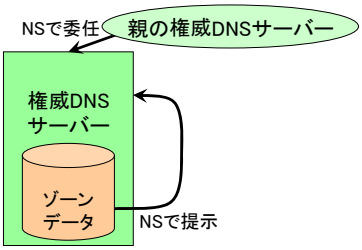

図1：引っ越し前の状態

前準備：権威 DNS サーバー以外のサーバーの構築

作業を始める前に、引っ越し先の Web サーバーやメールサーバーなどをあらかじめ構築しておきます。

手順 1：引っ越し先の権威 DNS サーバーの構築

新しいゾーンデータ（引っ越し先の Web サーバーやメールサーバーなどの情報）を管理する、引っ越し先の権威 DNS サーバーを構築します（次ページ図2）。

※掲載内容は2011年6月現在のものです。

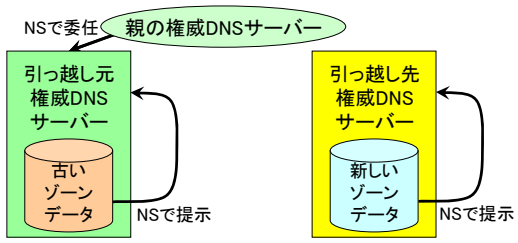

図2:引っ越し先の権威 DNS サーバーの構築

手順 2:引っ越し元の権威 DNS サーバーのゾーンデータの切り替え

引っ越し元の権威 DNS サーバーのゾーンデータを、NS の指定やグルーレコードの指定なども含め、**まるごと新しいゾーンデータに切り替えます**(図3)。

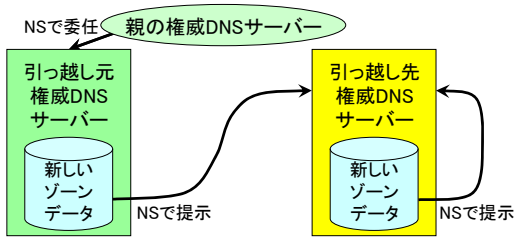

図3:ゾーンデータの切り替え

手順 3:親に登録した委任情報の切り替え

親に登録している委任情報(NS、必要に応じてグルー)の変更を申請し、引っ越し先の権威 DNS サーバーを示すものに切り替えます(図4)。

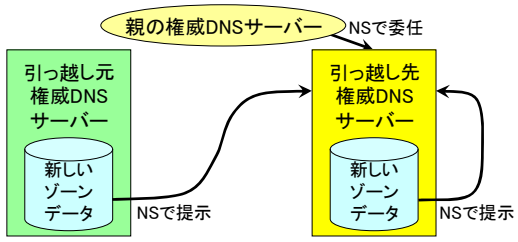

図4:委任情報の切り替え

手順 4:双方の権威 DNS サーバーを並行運用

すべてのキャッシュ DNS サーバー群が引っ越し先の権威 DNS サーバーのみを参照するようになるまで、具体的には以下の時間が経過するまで、双方の権威 DNS サーバーをこの状態で並行運用します(表1)。

並行運用期間(以下の双方の時間が経過するまで)
1. 手順2の完了時点から起算した、引っ越し元の権威DNSサーバーのNSで指定していたTTL値(子の古いNSのTTL)
2. 手順3の完了時点から起算した、親の権威DNSサーバーのNSで指定されていたTTL値(親のNSのTTL)

表1:必要となる並行運用期間

手順 5:引っ越し元の権威 DNS サーバーの停止

引っ越し元の権威 DNS サーバーを停止し、並行運用を終了します(図5)。

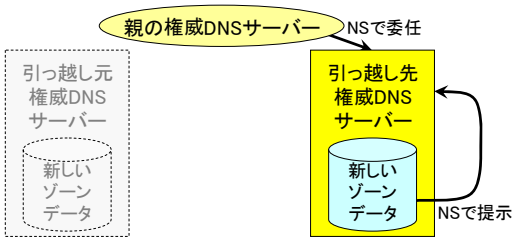

図5:引っ越し元の権威 DNS サーバーの停止

■ポイントは「新しいデータによる並行運用」

この方法のポイントは、引っ越し先の権威 DNS サーバーの構築後(手順1)、親に登録した委任情報の切り替え(手順3)の**前に**引っ越し元の権威 DNS サーバーのゾーンデータを**新しいものに切り替え**(手順2)、同じゾーンデータをもつ双方の権威 DNS サーバーを所定の TTL 値で定められた一定期間**並行運用する**(手順4)ことにあります。

この方法では手順2の完了後、インターネット上のキャッシュ DNS サーバー群に新しいゾーンデータのみが提供されるようになるため、古いゾーンデータはそれぞれの TTL 値[1]で指定されていた時間の経過後、**確実に消滅**します。つまり、この方法ではいわゆる「DNS が浸透しない」や「DNS が伝搬しない」と呼ばれるトラブルの発生を、未然に防ぐことができます[2]。

▼正しい委任成立のための三つの条件

DNS の仕様では正しい委任を成立させるために、

① 親が NS で示したすべての権威 DNS サーバーが、権威を持つ応答を返す

② 子が NS で示したすべての権威 DNS サーバーが、権威を持つ応答を返す

③ ①と②の権威 DNS サーバーが同じ応答を返す

の三つの条件をすべて満たしている必要があります。作業時のトラブル発生を未然に防ぐためには、これらの条件を満たす形で引っ越しを進めることが重要です。

[1] 作業開始前に該当する TTL 値の短縮が可能な場合、サーバーの切り替えに要する時間を短縮できます。
[2] トラブルが発生した場合、その原因を当該キャッシュ DNS サーバーの動作不良であると確定できます。