外部用コンテンツサーバの移行 ～上位ゾーンで内部用コンテンツサーバを運用している場合～

白石　啓一＊　　高城　秀之＊　　粂川　一也＊

Migration of Contents Server for External Network when Contents Server for Internal Network is operated in Higher Zone

Keiichi SHIRAISHI,　Hideyuki TAKAJO　and　Kazuya KUMEKAWA

Abstract

On Domain Name System, contents server has zone information and answer for dns name resolutions. Migration of contents server for external network when contents server for internal network is operated in higher zone is described in this paper.

Keywords : DNS, Contents Server, Migration

1. 緒言

DNSは，インターネットにおいて，ドメイン名やホスト名とIPアドレスを相互変換する仕組みである。WWW等で使用されるURLの一部やメールアドレスの一部にドメイン名，ホスト名が使用され，DNSがないと，事実上，WWWやE-mailを使えないほど，DNSは基本的なサービスである。

本稿では，DNSコンテンツサーバの移行について，特に，移行対象のDNSコンテンツサーバの上位ゾーンにて，外部ネットワーク用と内部ネットワーク用のDNSコンテンツサーバを分けて運用し，移行対象側ゾーンの公開サーバを上位ゾーンから利用している場合の注意点に言及することを目的とする。

2. DNS

DNS(Domain Name System)の用語と情報セキュリティについて，簡単にまとめる。

＊ 香川高等専門学校　通信ネットワーク工学科

2.1 用語

DNSで使用される用語は，同じことをいくつかの視点から見て呼ぶため，表記の揺れがある。本稿では，文献[1,2,3,4,5]を参考に，以下の用語を使う。

- DNSサーバ：　DNSサーバには，コンテンツサーバとキャッシュサーバがある。
- コンテンツサーバ：　ゾーン情報を管理するサーバである。非再帰的問合せに対して，そのゾーンの情報を返す。ゾーンサーバ，権威(authority)サーバとも呼ぶ。
- キャッシュサーバ：　(DNSの意味での)クライアント(PC，サーバ等)のリゾルバからの再帰的問合せを受け付け，キャッシュを確認し，対応する情報をキャッシュしていれば，その情報を返す。キャッシュしていなければ，コンテンツサーバへ問い合わせ(非再帰的問合せ)，返って来た情報をリゾルバへ返答するとともにキャッシュする。
- ゾーン：　コンテンツサーバが管轄する(権威を持つ)ドメインの範囲である。下位のコンテンツサーバに対して，ゾーン(一部のサブドメインの

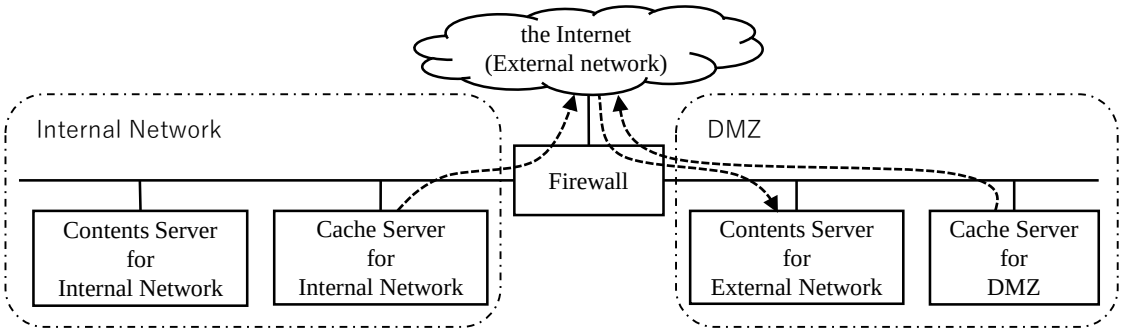

図2　DNS サーバの設置位置とファイアウォールが許可する通信

ゾーン）の管理を移すことを委任または委譲（delegation）という。図1は，domain zone のコンテンツサーバが domain, sub1.domain を管理し，sub2.domain.zone のコンテンツサーバが sub2.domain を管理する様子を示す。コンテンツサーバ上，ゾーン情報を記述したファイルをゾーンファイルと呼ぶ。

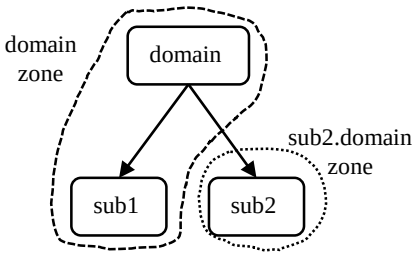

図1 ドメインとゾーンの関係

- ルートサーバ：　コンテンツサーバの最上位のサーバである。
- FQDN(Fully Qualified Domain Name，完全修飾ドメイン名)：　ホスト名とドメイン名を組み合わせ，TLD まで明示した名前を言う。ゾーンファイル中など，FQDN であることを明示するため，最後に「.」を付けることがある。例：www.kagawa-nct.ac.jp，www.kagawa-nct.ac.jp.
- TLD(Top Level Dmain)：　ルートサーバが管理しているドメイン，FQDN の最後のドメインを言う。com や org などの gTLD，jp や us などの ccTLD がある。
- A レコード：　ゾーンファイル中，ドメイン名の IPv4 アドレスを示すレコードである。ドメイン名から IPv4 アドレスへの変換（正引き）に使われる。
- NS レコード：　ゾーンファイル中，ドメインのコンテンツサーバ（ネームサーバ）を示すレコードである。正引きの際，ルートサーバから対象のドメインのコンテンツサーバを探す際に使われる。

2.2 DNS の情報セキュリティ

DNS には情報セキュリティ上の脆弱性が知られており，機密性と完全性を保つために以下の 4 種類のサーバへ分けて（図 2），可用性を保つためにそれぞれを 2 台以上で運用することが推奨されている[3,4]。

- 外部用コンテンツサーバ：　外部ネットワークに対して，サービスする。自社ネットワークの DMZ や外部データセンターに置く，クラウドサービスを利用する，などが考えられる。
- DMZ 用キャッシュサーバ：　自社ネットワークの DMZ に置いてあるクライアントのリゾルバからの再帰的問合せに応答する。それ以外からの問合せを拒否する。
- 内部用コンテンツサーバ：　内部ネットワークに対して，サービスする。外部用コンテンツサーバに含まれるゾーン情報に加え，内部ネットワーク専用のゾーン情報（外部公開しない，内部ネットワーク専用サーバの情報）を保持する。
- 内部用キャッシュサーバ：　内部ネットワークのクライアントのリゾルバからの再帰的問合せに応答する。それ以外からの問合せを拒否する。

特に，キャッシュサーバは，キャッシュポイズニング攻撃を防ぐため，外部ネットワークからの問合せに応答してはいけない。そもそも，外部ネットワークに対してサービスする必要がない。また，内部用コンテンツサーバと内部用キャッシュサーバは，同一のサーバソフトウェアで実現している場合がある。その場合，内部ネットワーク専用のゾーン情報の関する応答，キャッシュサーバの動作を行う。

ファイアウォールは，DNS に関し，上記に必要な通信のみ，許可する。図2では，応答を省略している。

- 外部ネットワークから外部用コンテンツサーバへの通信，および，その応答

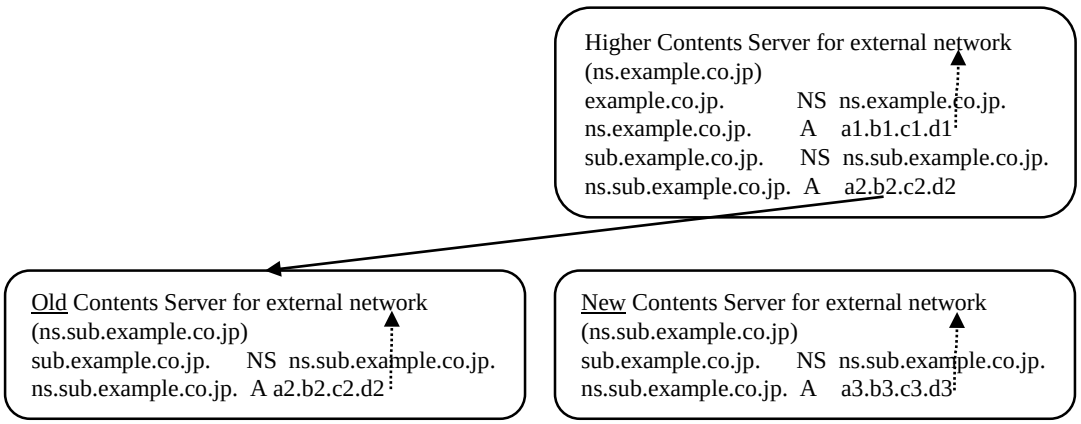

図3　コンテンツサーバの移行前

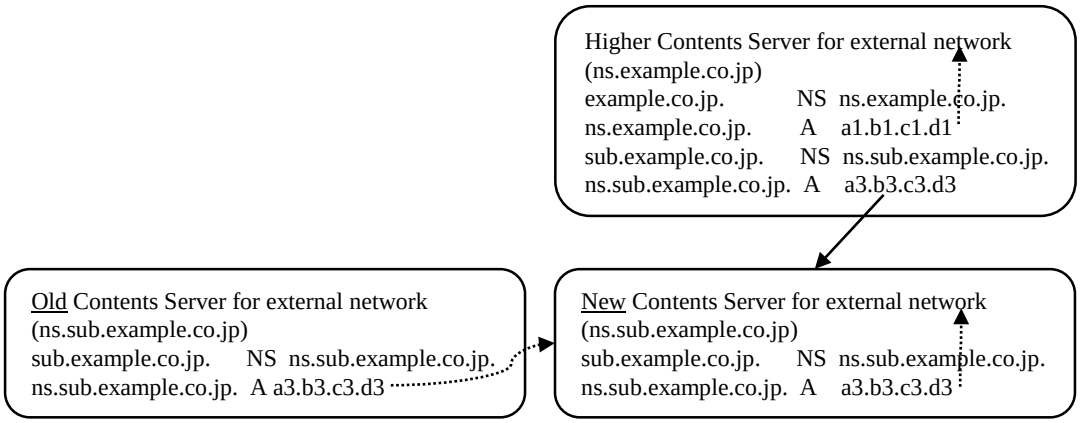

図4　コンテンツサーバの移行後

- DMZ 用キャッシュサーバから外部ネットワークのコンテンツサーバへの通信，および，その応答
- 内部用キャッシュサーバから外部ネットワークのコンテンツサーバへの通信，および，その応答

3. 外部用コンテンツサーバの移行

外部用コンテンツサーバの移行方法について，3.1 節に一般的な方法，3.2 節に内部用コンテンツサーバを運用している場合の注意点を述べる。なお，図 3-6 中の「a?.b?.c?.d?」は，IPv4 アドレスの例示である。IPv4 アドレスにより，自身や移譲するサーバを指し示す。example.co.jp.ドメインを使い，例示する。ゾーン情報は，DNS サーバソフトウェア BIND のゾーンファイルのフォーマットを参考に，必要な情報のみ記述し，各行 3 個の情報からなる。2 個目の NS，A は，レコードの種類であり，それぞれ NS レコード，A レコードを示す。1 個目のドメイン名が 3 個目のドメイン名，または，IPv4 アドレスであることを示す。

3.1 外部用コンテンツサーバの移行方法

外部用コンテンツサーバの移行方法は，以下のとおりである（図 3，4）[5)]。

1. 「移行先のサーバ」（New Contents Server for external network）を新たに構築する（図 3）。
2. 「上位のサーバ」（Higher Contents Server for external network），「移行元のサーバ」（Old Contents Server for external network）の ns.sub.example.co.jp.が「移行先のサーバ」を指すよう IPv4 アドレスを変更する（図 4）。
3. 並行運用期間（TTL 値の時間）が経過したら，「移行元のサーバ」を停止する。

3.2 内部用コンテンツサーバを運用している場合

上位ゾーンで内部用コンテンツサーバ（Higher Contents Server for internal network）を運用している場合，こちらにも「移行元のサーバ」の情報がある（図 5）ので，「移行先のサーバ」の情報へ変更する必要がある（図 6）。これを怠ると，上位の内部用コンテンツサーバが，いつまでも「移行元のサーバ」が参照し続ける。もし，「移行元のサーバ」を停止すると，上位ゾーンの内部用コンテンツサーバの利用者が，sub.example.co.jp のサーバを使用したいとき，そのド

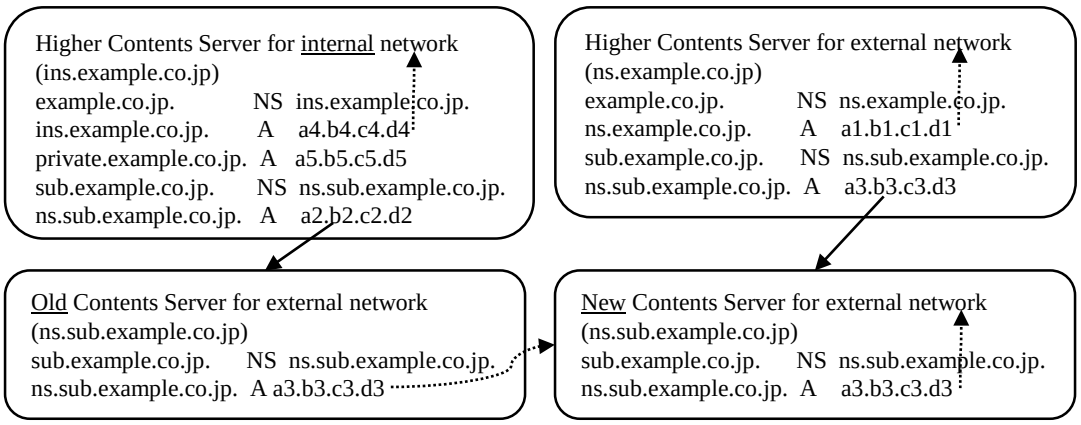

図5　内部用コンテンツサーバを運用している場合の移行前

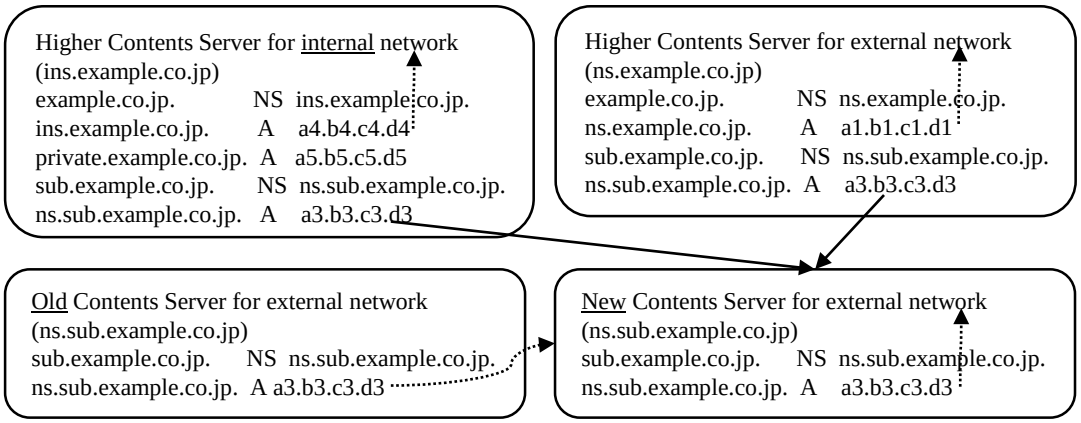

図6　内部用コンテンツサーバを運用している場合の移行後

メイン名を引けなくなり，そのサーバをFQDNで使用できなくなる。

なお，2.2節で述べたとおり，内部ネットワーク専用のゾーン情報は，内部用コンテンツサーバに保持され，外部用コンテンツサーバに保持されない。例えば，図5では，private.example.co.jp.がそのような情報である。

4. 結言

DNSにおいて,外部用コンテンツサーバの移行について，特に，移行対象の外部用コンテンツサーバのゾーンの上位ゾーンで，外部ネットワーク用と内部ネットワーク用のコンテンツサーバを分けて運用している場合の注意点を述べた。上位ゾーンの内部用コンテンツサーバに保持されているゾーン情報内の移行対象ゾーンの外部用コンテンツサーバに関する情報を更新しなければ，移行対象側ゾーンの公開サーバを上位ゾーンから利用できなくなる。

なお，本稿で記述した内容は，詫間キャンパスのコンテンツサーバを移行した際に確認した。情報セキュリティ上の懸念から，香川高専の実例に合わせた記述を見合わせた。ご了承願いたい。

参考文献

1) 網野 衛二: 3分間DNS基礎講座, pp.110-115, 技術評論社(2009)
2) 中島 能和: Linux サーバーセキュリティ徹底入門, pp.208-235,翔泳社(2013)
3) 上原 孝之: 情報処理教科書 情報処理安全確保支援士 2021 年版, pp.42-45, pp.128-133, pp.249-253, 翔泳社(2020)
4) NIST, IPA(訳): セキュアなドメインネームシステム (DNS) の導入ガイド, IPA(2009) https://www.ipa.go.jp/files/000025348.pdf (2022-2-8 参照)
5) 日本レジストリサービス: 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～, JPRS トピックス&コラム, 19,日本レジストリサービス(2015) https://jprs.jp/related-info/guide/019.pdf (2019-4-17 参照)