DNS サーバの安定運用のための構成

廣友 雅徳，松原 義継

佐賀大学総合情報基盤センター

1　はじめに

Domain Name System（DNS）はネットワークの基幹システムです．DNS サーバによってホスト名と IP アドレスの関連付けがなされ，インターネット上に公開されます．その重要性から，一般に一組織において複数台の DNS サーバで管理，運用されます．佐賀大学（以下，本学）においても，総合情報基盤センター（以下，本センター）でこれまで 2 台の DNS サーバを運用していました．DNS サービスを安定して運用するためには，DNS サーバを適切に配置し管理することが必要です．本センターでは，DNS サーバの安定性と安全性を向上させるため，2012 年 8 月から 12 月にかけて DNS サーバの構成を変更しました．本稿では，その DNS サーバの構成変更について紹介します．

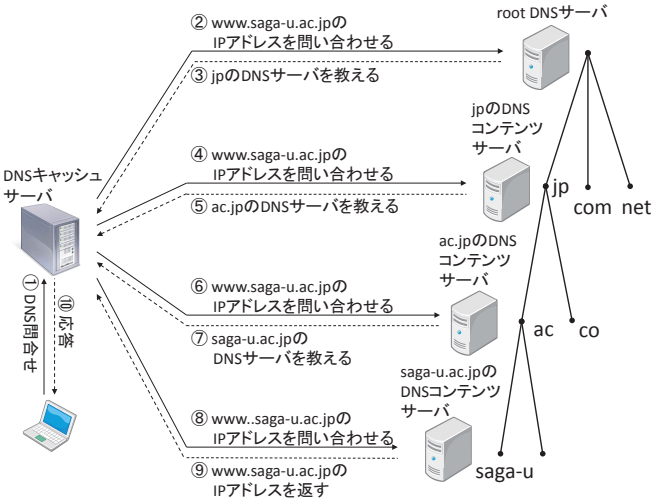

図 1: DNS 名前解決の例

2　DNS の仕組み

DNS はホスト名と IP アドレスを関連付ける仕組みです．その仕組みは名前空間の階層化と権限移譲による分散管理によって実現されています．クライアント端末が DNS サーバに問い合わせてホスト名から IP アドレスを名前解決する例を図 1 に示します．

DNS サーバには 2 つの役割があります．一つは自ドメインの情報を管理し公開する DNS コンテンツサーバです．もう一つはクライアント端末からの DNS 問合せに応じて DNS コンテンツサーバを検索し，DNS 名前解決を提供する DNS キャッシュサーバです．DNS コンテンツサーバと DNS キャッシュサーバは，広く普及している DNS サーバプログラムである BIND [1] で明確に分離されていなかったことなどの歴史的経緯から同一のサーバで動かしている例が多く見られます．しかし，安全面を考えると，それらの役割は異なるサーバで運用すべきです．DNS コンテンツサーバと DNS キャッシュサーバを同一のサーバで運用している場合，脆弱性が見つかるたびに，その脆弱性の影響がないか，設定を見直さなければなりません．BIND は従来から広く利用されているサーバプログラムですが，現在でもいくつかの脆弱性が報告されています [2][3]．万が一にも，設定の不備などによって DNS の脆弱性を悪用されると，フィッシングサイトやマルウェア配布サイトへ誘導されるため，非常に危険です [4][5]．

3　DNS サーバの構成変更

3.1　旧構成

2012 年 8 月まで本センターで運用していた DNS サーバの構成を図 2 に示します．本センターでは saga-u.ac.jp ドメインを 2 台の DNS サーバ sagagw.cc.saga-u.ac.jp（以下，sagagw）と chisato.cc.saga-u.ac.jp（以

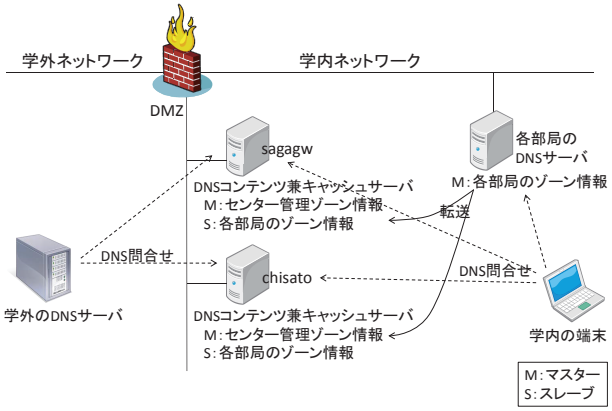

図 2: DNS サーバの旧構成

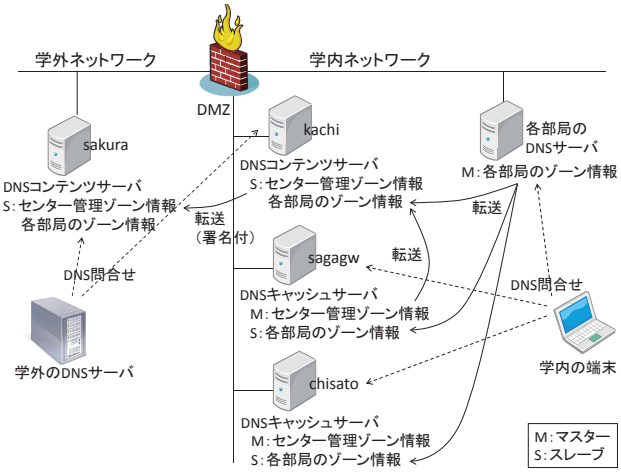

図 3: DNS サーバの新構成

下，chisato）で管理していました．sagagw と chisato の第一の役割は saga-u.ac.jp ドメインを管理する DNS コンテンツサーバであり，saga-u.ac.jp ドメインをインターネット上に公開していました．また，いくつかの部局ではサブドメインを管理するために DNS サーバを運用しているため，それらの DNS サーバとマスター・スレーブ関係を結び，部局 DNS サーバから転送されてくるサブドメインのゾーン情報を受け，インターネット上に公開していました．sagagw と chisato の二つ目の役割は学内端末に対する DNS キャッシュサーバであり，学内で動いている端末に対して DNS 名前解決を提供していました．

このように 2 台の DNS サーバによって運用していましたが，それらは同一設定，同一機能を持たすレプリカとしての冗長化であり，機能を分けるようなことは行っていませんでした．

3.2 新構成

2012 年 12 月以降の DNS サーバの新しい構成を図 3 に示します．この構成変更の目的は次の 2 つです．

- セキュリティ向上： 脆弱性の影響を最小化する．DNS キャッシュ汚染攻撃への耐性を持たす．
- BCP（事業継続計画）対策: 災害発生時や学内ネットワークの障害発生時においても saga-u.ac.jp ドメインを継続して運用可能にする．

新構成における各サーバの役割は次のようになります．

- DNS コンテンツサーバ：
  sakura.cc.saga-u.ac.jp，kachi.cc.saga-u.ac.jp
- DNS キャッシュサーバ：
  sagagw.cc.saga-u.ac.jp，chisato.cc.saga-u.ac.jp

このような構成変更に伴い，saga-u.ac.jp ドメインの NS レコードも 2012 年 11 月 21 日に sagagw と chisato から sakura.cc.saga-u.ac.jp（以下，sakura）と kachi.cc.saga-u.ac.jp（以下，kachi）に変更しています．

新構成では，DNS サーバを学外に 1 台（sakura），DMZ に 1 台（kachi）新規に追加しました．学外で DNS サーバを運用することによって，学内ネットワークの障害発生時においても saga-u.ac.jp ドメインを継続して運用できます．この目的のために，sakura を saga-u.ac.jp ドメインを公開する DNS コンテンツサーバとして構築しました．また，そのセカンダリサーバとして kachi を DMZ に配置しました．これにより，DNS コンテンツサーバの機能を sagagw と chisato から切り離し，sagagw と chisato を学内端末向けの DNS キャッシャサーバ専用として運用できるようになりました．

新規 DNS サーバには仮想サーバを利用しています．学外ネットワークで稼動している sakura は商用仮想レンタルサーバで構築し，DMZ で稼動している kachi は本センターで運用している仮想システム上の一つの仮想サーバとして構築しています．DNS コンテンツサーバは DNS キャッシュサーバに比べてクエリ数が少なく，メモリの使用量とディスクの I/O 負荷が小さい

ため，仮想サーバで十分運用することができます．

saga-u.ac.jp ドメインを sakura と kachi によって公開するためには，これまで sagagw と chisato で管理していたドメイン情報を sakura と kachi へ移す必要があります．これまでのドメイン情報の管理方法を引き継ぐために，それはゾーン転送によって実現しました．また，各部局の DNS サーバでは，これまでの sagagw と chisato へのゾーン転送に加えて，kachi へゾーン転送するように設定して頂きました．一方，sakura へのゾーン転送はインターネット経由で行われるため，転送データの改竄や転送元サーバのなりすましによって，sakura へ偽のゾーン情報を混入される危険があります．これらを回避するため，sakura へ転送されるゾーン情報には電子署名を付与して，kachi から送信しています．sakura は転送されてくるゾーン情報を電子署名で検証し，仮に署名を受理しない場合はその転送データを破棄できます．この機能は BIND の TSIG（トランザクション署名）によって実現しています．

また，セキュリティ向上のため，DNS コンテンツサーバである sakura と kachi では DNS キャッシュサーバの機能を無効にし，DNS キャッシュ汚染攻撃への耐性を持たせています．DNS キャッシュサーバである sagagw と chisato は学外ネットワークからのアクセスをファイアウォールで遮断することで，学外からの DNS キャッシュサーバに対する攻撃を防ぐことができます．

4 まとめ

本稿では，本センターで運用している DNS サーバの新構成を紹介しました．この構成変更によって，DNS サーバの BCP 対策とセキュリティ向上が実現できました．最後に，DNS サーバの構成変更に伴い，設定変更等でご協力頂いた各部局 DNS サーバの管理者の皆様に感謝申し上げます．

参考文献

[1] BIND，https://www.isc.org/software/bind.

[2] JPCERT/CC，ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起，http://www.jpcert.or.jp/at/2012/at120018.html.

[3] JPCERT/CC，ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2012-4244) に関する注意喚起，http://www.jpcert.or.jp/at/2012/at120029.html.

[4] JPNIC，インターネット 10 分講座：DNS キャッシュポイズニング，http://www.nic.ad.jp/ja/newsletter/No40/0800.html.

[5] JPRS,「ghost domain names（幽霊ドメイン名）」脆弱性について，http://jprs.jp/tech/notice/2012-02-17-ghost-domain-names.html.