京都大学における DNS サービスの改善

針木 剛 [1)]

1) 京都大学 企画・情報部

hariki.tsuyoshi.3r@kyoto-u.ac.jp

Improvement of DNS service in Kyoto University

HARIKI Tsuyoshi[1)]

1) Information Dept., Kyoto Univ.

概要

京都大学では学内外の利用者に向けた外向け権威 DNS サービス、及び学内利用者に向けた内向け権威 DNS サービス、キャッシュ DNS サービスを提供している。そのうちキャッシュ DNS サービスに関して過去に 4 回障害が発生し、Web やメールを含む全ての情報サービスが利用不可となった。各障害について原因対策は行ったが、別途 DNS サーバ構成に関して冗長化と分散化を再検討し改善を行った。また外向け権威 DNS サービスに関してもクラウドサービスを利用した分散化の改善を行った。

1 はじめに

2 学内ネットワーク環境

京都大学では学内利用者が研究室 VLAN でパソコンやプリンタを利用するためのプライベートアドレス「KUINS-III」と、学外への通信や学外公開のためのグローバルアドレス「KUINS-II」を運用している。教職員は希望に応じて「KUINS-DB」と呼ばれる Web フォームからそれらを利用申請し、申請内容を保存したデータベースの内容を適宜ネットワーク機器の設定に反映することで運用を行っている。図 1 にあるように KUINS-DB では IP アドレス申請と併せて DNS レコードの申請も可能であり、同時に DNS 権威マスターサーバとして動作している。京都大学では主に外向きとして「kyoto-u.ac.jp」の正引きと KUINS-II の逆引き、内向きとして「kuins.net」の正引きと KUINS-III の逆引きを管理しており、外向き用と内向き用それぞれの別の DNS 権威スレーブサーバにゾーン転送して分散運用を行っている。通常の学内利用者が情報リソース利用の名前解決に、それらとは別に DNS キャッシュサーバを運用しており、内向きのゾーンに関しては直接 DNS 権威スレーブサーバを参照し、それ以外は DNS ルートサーバへ問い合わせをしている。そのため外向きのゾーンの名前解決は DNS ルートサーバを経て問い合わせされる。また DNS キャッシュサーバでは内向きのゾーンを除き DNSSEC 検証を有効にしており、加えて KUINS-DB にて外向きのゾーンの正引きに自動で DNSSEC 署名をしている。

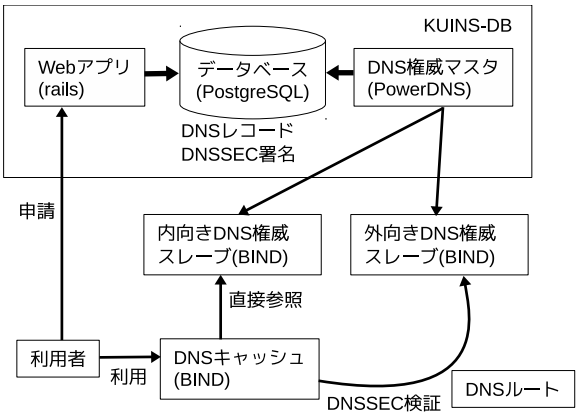

図 1 DNS サーバ

3 DNS キャッシュサーバ障害とその改善

3.1 過去の障害

DNS キャッシュサーバで発生した障害一覧を表 1 にまとめる。原因はそれぞれ全く違ったため対策もそれぞれ違う方法となった。

表 1 DNS キャッシュサーバ障害

日時	原因	対策
2015-04-16	多量アクセスで クエリログ処理不能	クエリログ停止
2016-11-11	ループ流入で仮想化 基盤ストレージ障害	ループ検知自動遮断
2017-05-31	BIND バグクラッシュ	BIND アップデート
2017-09-22	DNSSEC 鍵更新エラー	KUINS-DB バグ修正

DNS キャッシュサーバは負荷分散と冗長化のため 2 台構成で運用しているが、2 番目と 3 番目の障害に関しては 2 台とも同じシステム内で同じ構成、同じソフトウェアだったため、片系がバックアップとして機能せず、両者が同時にダウンし障害となっている。DNS キャッシュサービスが障害となると、外部への Web 接続やメール送受信、その他各種情報サービスが利用不可となりその被害の範囲が甚大となる。各障害に関して個々の再発防止対策も必要だが、それと併せて障害内容次第ではサーバ分散化と冗長化によって被害回避が可能となるため、具体的な改善方法を検討した。

3.2 改善の実施

既存の DNS キャッシュサーバが稼働している基盤コンピュータシステムと称する学内仮想化基盤 (以下基盤コンとする) ではなく、汎用コンピュータシステムと称する別の学内仮想化基盤 (以下汎用コンとする) にサーバを新たに構築する。またソフトウェアについてはバグ混入のあった BIND を避けて unbound を選択した。unbound に関しては京都大学内で導入実績がなかったため、一旦利用者数の少ない学外者用無線ネットワークにて 2 ヶ月間の試験運用で検証を行い、問題がないことを確認した後で全学導入を行った。また DNS キャッシュサーバは内向き用 DNS 権威スレーブサーバを直接参照しているため同様にサーバを追加構築した。こちらも同様に汎用コン上に構築し、BIND を避けて nsd を選択した。表 2 に既存のサーバと新しく構築したサーバをまとめる。キャッシュサーバと権威サーバは既存サーバ同士、新サーバ同士の組で運用する設定とした。全学への導入は DHCP オプションにて配布する DNS サーバ IP アドレスに新しく構築した DNS キャッシュサーバを追加することで実施した。導入後は特に大きな問題は発生しておらず安定運用ができている。

表 2　既存と新サーバ

	役割	台数	サーバ基盤	ソフトウェア
既存	キャッシュ	2	基盤コン	BIND
	内向き権威	2	基盤コン	BIND
新	キャッシュ	2	汎用コン	unbound
	内向き権威	2	汎用コン	nsd

4　その他 DNS サーバの改善

4.1 権威マスターサーバの現状

KUINS-DB は現在基盤コンと富士通社の群馬県館林データセンタ内ハウジングサービス内の仮想化基盤 (以下館林 DC とする) の 2 箇所にてサーバを稼働させており、通常運用では主たるデータベースは基盤コン、バックアップを館林 DC としている。両者はマルチマスタで随時データ連携しており片方のデータセンタに問題が発生した場合はもう一方のデータセンタにて代行運用可能となっている。図 2 にあるように 3.2 で構築した新サーバも含め、全てのスレーブは両マスターから取得するよう設定している。

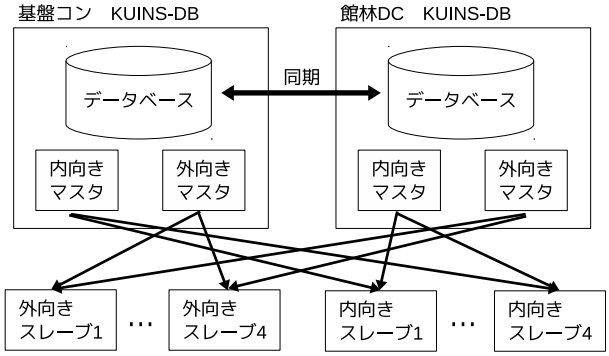

図 2　権威 DNS サーバ構成

4.2 外向き権威スレーブサーバのクラウド化

外向き DNS 権威スレーブサーバは図 2 にあるように 4 台構成で、物理位置が基盤コンに 2 台と館林 DC に 1 台と愛知県犬山キャンパスに 1 台と分散していた。このうち犬山キャンパスの物理サーバの老朽化に伴いリプレースを検討したが、サーバを分散させるために既存の大学の仮想化基盤内ではなく、新たにクラウド IaaS へとサーバ移行した。具体的には学内から離れた場所としてさくらインターネット社の北海道石狩データセンタ (以下石狩 DC とする) を選択し、ネットワークも同サービスで提供された IP アドレスをそのまま利用した。また外向き DNS 権威スレーブサーバは従来はすべて BIND で動作していたが、石狩 DC と館林 DC を nsd に変更している。外向き DNS の所有するデータは公開情報であり今後も積極的にクラウド利用をすすめていく方針である。ただし、今回 nsd に移行した際に 利用していた nsd-4.1.20 に DNSSEC 検証のバグがあり特定のゾーン更新時に子プロセスが停止し更新に失敗するという問題が発生した。正確には 4.1.18 以降からバグが存在し、当該バグは nsd のコミュニティに報告しその後リリースされた nsd-4.1.22 からは修正されている。

5　まとめ

- DNS サーバを追加構築または変更し分散化と冗長化を強化した。
- 今後も大学の仮想化基盤やクラウドサービスを適宜活用し、分散化と冗長化した信頼性の高いサービス運用を目指す。