Vol.2020-IOT-48 No.7
2020/3/2

DNSサービスBCP対策のための ネットワーク管理データベースの学外移行

針木 剛[1,a)]

概要：京都大学では情報コンセント VLAN，DNS レコードといった利用者からの利用申請を受理し，ネットワーク機器へ設定反映するデータベースサーバを運用している．本サーバは学内オンプレミスにて学内 IP アドレス制限で運用していたが，DNS サービスの BCP 対策のため学外データセンタに移行した．本論文では学外からも安全に利用するために行った各種対策について詳細をまとめる．また商用クラウド移行した場合を想定した検討結果も併せて報告する．

キーワード：DNS，BCP 対策，クライアント証明書，GeoIP，クラウド，VPN

Migration of Network Management Database to External Data Center for BCP (Business Continuity Plan) of DNS service

1. はじめに

京都大学では DNS 正引きとして kyoto-u.ac.jp など 3 ドメイン，また学内で利用するグローバル IP アドレスやプライベート IP アドレスの DNS 逆引きを管理しており，それらは大学からの情報発信や大学内での情報共有など研究教育活動を担う情報サービス運用に欠かせない重要な基盤サービスである．

特に京都市大規模災害発生を想定して事業継続計画 (BCP) を考える上で，最新の被害情報や復旧情報を提供したり構成員の安否確認をするための情報システムを運用するためには DNS サービス自体の継続運用は必須であるが，加えて被害状況や環境の変化に応じて各種サーバを柔軟に追加構築したり運用変更するためには DNS レコードを適宜更新する手段も継続運用できている必要がある．

本稿ではまず平常業務で DNS レコードの変更申請や反映までのフローをサーバ構成を含めて詳細に説明し，DNS サービス及び DNS レコード更新機能を有するネットワーク管理データベースサーバを学外データセンタに移行する際に行った作業をまとめる．特に学外ネットワークへの接続許可についてセキュリティに配慮した各種対策について詳細に説明する．

また遠隔地データセンタではなく一般的な商用クラウドを利用した場合についても併せて検討した結果をまとめる．

2. 学内ネットワーク環境と管理データベース

京都大学の学術情報ネットワークシステム（Kyoto University Integrated information Network System, 略称:KUINS）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 IP 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 IP アドレス「KUINS-II」を運用している。

京都大学ではそれら KUINS-II 及び KUINS-III のネットワーク情報を一元管理する「KUINS-DB」と呼ばれるデータベースシステムを 2002 年より運用している．[1], [2]

教職員は「KUINS-DB」の Web フォームから希望する IP アドレスやネットワークと利用したい研究室や居室の情報コンセント名と紐付けて申請を行う．受理された申請内容に VLAN 情報やゲートウェイ機器情報等を付加したデータベースの内容をネットワーク機器の設定に変換し，各機器へ自動的に投入することで全学ネットワークの運用を行っている．

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，本データベースサーバは同時にそ

[1] 京都大学 Kyoto Uniersity
[a)] hariki.tsuyoshi.3r@kyoto-u.ac.jp

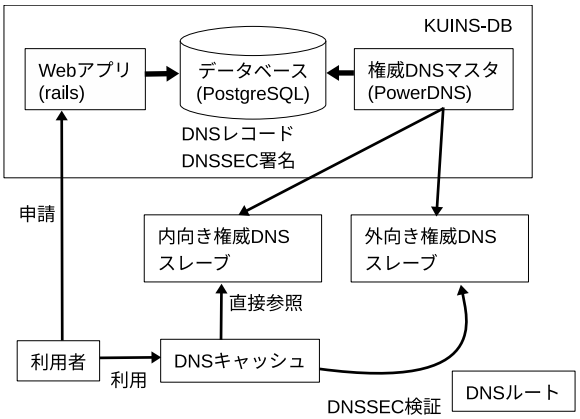

図 1　DNS サーバ構成

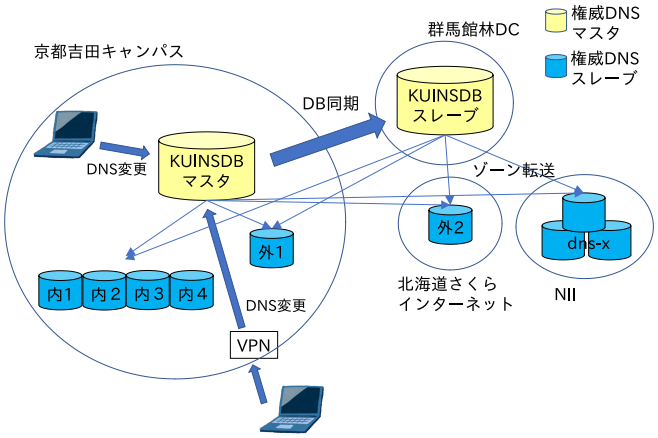

図 2　KUINSDB 移行前

れら DNS レコードを提供する DNS 権威マスタサーバとしても動作している．

京都大学では外向きとして「kyoto-u.ac.jp」「kyoto-u.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，**図 1** にあるように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．

学内利用者が情報リソース利用のための問い合わせ先として DNSSEC 検証を有効にした 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する問い合わせは DNS 権威スレーブサーバへ転送し，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 ルートサーバを経由して問い合わせされる．KUINS-DB ではこの外向きの正引きゾーンに対し自動で DNSSEC 署名をしている．

また KUINS-DB を運用するサーバには KUINS-II と KUINS-III がそれぞれ 1 アドレス割り当てており，KUINS-II では外向きゾーン提供用 DNS サーバや Web サーバ，KUINS-III では内向きゾーン提供用 DNS サーバや，ネットワーク機器の管理用 IP アドレスが同じく KUINS-III であるため，それら機器へのコンフィグ投入用に利用している．

3. KUINS-DB バックアップ構成

3.1 KUINS-DB 移行前の構成

図 2 にあるように KUINS-DB は京都市内京都大学吉田キャンパスのオンプレミス仮想化基盤内にて運用を行っており，データベース情報については適宜富士通社の群馬県館林データセンタ内のハウジングサーバに同期させて 2 系統での運用を行っていた．

館林データセンタは SINET5 の群馬ノードに接続しており，その SINET5 の「L2VPN サービス」により，京都ノードに接続している吉田キャンパスのネットワーク KUINS-III と L2 で接続している．グローバル IP アドレスについては同じく SINET5 の「インターネット接続 (IPv4/IPv6 Dual) サービス」により SINET から 26 ビットマスクの IPv4 アドレス帯が割り当てられており，こちらは京都大学とは独立したネットワーク経路で利用可能である．館林データセンタの KUINS-DB のサーバには吉田キャンパス同様 KUINS-III を割り当てているが，KUINS-II については代替として SINET の IP アドレスを割り当てて運用している．

また外向き権威 DNS サーバに関しては京都だけでなくさくらインターネット社の北海道データセンタ内の仮想マシン上に DNS サーバを構築して運用しており，さらにと SINET5 の「分散セカンダリ DNS」を利用しているため，地理的にもネットワーク的にも分散した運用ができている．

そのため京都市大規模災害を想定した場合でも外向きの DNS サービスは継続して運用が可能であったが，館林側のデータベースがスレーブ状態のため通常運用と同じように一般の教職員が Web フォームからの DNS レコード更新は不可であり，そのためには館林データセンタの仮想マシンを操作可能な限られた管理者によるデータ修正作業，あるいはデータベース切替セットアップ作業が必要であった．

3.2 KUINS-DB 移行後の構成

京都市大規模災害を想定した場合，その被害規模にも依るが同市内かその近郊在住の管理者も被災する可能性も高く，適切なオペレーションを行うことが困難となることも想定する必要がある．

図 3 にあるようにマスタ機をあらかじめ館林データセンタで運用を行っていれば，京都市大規模災害発生時でも特に追加作業不要で KUINS-DB が継続運用可能である．この構成であればもし館林データセンタ側で大規模災害が発生した場合には，管理者の職員が手動で京都吉田キャンパス内のサーバへ切り替えオペレーションを行い，システムを復旧する対応が可能となる．

また図 2 の状態で災害発生を検知して自動でマスタとスレーブを切り替える方法も考えられるが，正常に切り替わらないリスクもあるため今回は一旦検討から外した．

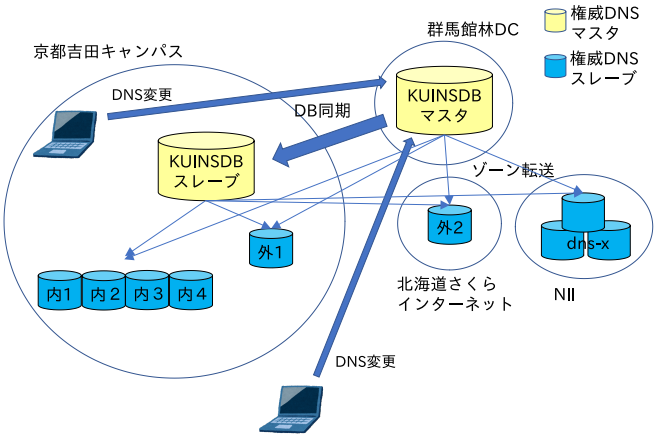

図 3　KUINSDB 移行後

本移行に伴い，Web サイト接続を KUINS の IP アドレス限定としている運用ポリシーも学外 IP アドレスの利用者に対しても接続許可とする方針に変更した．ただしそのまま公開するだけではセキュリティ水準をただ低下させるだけであり，なんらかの制限または対策が必要であると考えられる．

またシステム管理者による SSH ログインについても学外から利用できるような検討を行う．こちらも同様に適切な制限を検討する．

4. KUINS-DB サーバの学外公開のための変更点

KUINS-DB は移行時最新の CentOS7.6.1810 を利用して構築を行った．以下構築作業に記載されたオープンソースソフトウェアはそのディストリビューションにバンドルされたパッケージをそのまま利用している．

4.1 Web サーバ設定及び DNAT ポート転送設定

KUINS-DB の Web サイトでは利用時に Shibboleth による全学アカウントの認証またはシステム内のローカルアカウントである役職アカウントでの認証を行っている．新たな制限には NII の「UPKI 電子証明書発行サービス」でのクライアント証明書を利用する．Web サイトのログイン認証はそのままで，全ての HTTPS 接続に関して

- KUINS の IP アドレスからの接続は従来のまま
- KUINS 以外の IP アドレスからの接続では HTTPS 接続にクライアント証明書を必須とする

設定を行った．

Web サーバである Apache HTTP Server の具体的な設定を以下に示す．

```
 :
<Directory [DocumentRoot]>
SSLVerifyClient optional
SSLVerifyDepth 2
SSLRequireSSL
SSLOptions +StrictRequire
<RequireAny>
  Require ip [KUINS-II]
  <RequireAll>
    Require ssl-verify-client
    Require expr \
    %{SSL_CIPHER} !~ m/^(EXP|NULL)/
    Require expr \
    %{SSL_CLIENT_S_DN_O} == 'Kyoto University'
  </RequireAll>
</RequireAny>
</Directory>
SSLCACertificateFile [NII CA cert]
SSLCARevocationCheck leaf
SSLCARevocationFile [NII CA crl]
 :
```

クライアント証明書発行サービスは複数の研究機関に利用されているため，検証時には所属名も確認している．

これだけで要件は満たすが，何らかのクライアント証明書がインストールされたブラウザではポップアップで証明書選択画面が出力される．KUINS からの接続であればキャンセルして接続可能になるのだが，利用者の混乱を避けるため今回は別の方法を検討した．

443 番ポートの HTTPS サービスはクライアント証明書必須設定とし新たな 8443 番ポートで証明書不要の HTTPS サービスを仮想ホスト機能を用いて設定する．本設定は学内の KUINS-II アドレスからの 443 番ポートへの接続に対し，firewalld の設定で 8443 番ポートへのポート転送をすることで対応する．ここで firewalld の設定は以下のようになる．

```
<rule priority="0" table="nat" ipv="ipv4" \
chain="PREROUTING">-d [Server IP] \
-s [KUINS-II] -p tcp --dport 443 -j DNAT \
--to-destination [Server IP]:8443</rule>
```

また 8443 番は同じく firewalld で KUINS でアクセス制限とした．

ただしこの場合では 8443 番に接続した際に Shibboleth-SP に渡されるエンドポイント URL が 8443 番ポートとなってしまうため Apache HTTP Server で以下のように明示的に 443 番を指定する設定が必要となる．

```
 :
<VirtualHost _default_:8443>
ServerName [Server FQDN]:443
 :
</VirtualHost>
 :
```

4.2 SSH サーバ設定

大規模災害時でもサーバメンテナンスできるように管理者用 SSH サービスに関しても学外からの接続を許可する必要がある．しかしそのまま公開すると攻撃対象となるため

(1) TCP ポート番号の変更
(2) パスワード認証と公開鍵認証の両者を必須
(3) GeoIP で日本国内の IP アドレスからの接続に制限

とした．(1) と (2) については OpenSSH で設定を行った．22 番ポートは firewalld でバッチ処理クライアントからのみ許可し，その場合は公開鍵のみの認証も許可している．

```
Port 22
Port 8022
AuthenticationMethods publickey,password
 :
Match LocalAddress [Server IP] LocalPort 22 \
  Address [Client IP]
        AuthenticationMethods publickey
Match LocalAddress [Server IP] LocalPort 22 \
  Address *,![Client IP]
        PubkeyAuthentication no
        PasswordAuthentication no
```

(3) について 3.2 で述べたように Web サイトの DNS 情報の更新は多くの情報システムの管理者が広く利用できることに配慮したことに対し，サーバ管理に関しては管理者職員や Web アプリメンテナンス業者も含め限定的で，日本国内からの利用という制限下でも運用は十分可能と判断した．

GeoIP の情報は MaxMind 社の GeoIP2 データベースを利用した．本データベースは無償利用においてダウンロード頻度が制限されているので週 1 回程度の更新とした．具体的な制限機能とバッチ処理は firewalld の ipset 機能を利用した．予め設定済みの ipset 名「jp」での接続許可を行った後，バッチ処理で以下のようなコマンドで ipset の IP アドレスリストの更新のみ行うようにした．

```
firewall-cmd --ipset=jp \
  --remove-entries-from-file=[del list file]
firewall-cmd --ipset=jp \
  --add-entries-from-file=[add list file]
```

5. 商用クラウドサービスの検討

京都大学では館林データセンタにて本 KUINS-DB や Shibboleth-IdP 認証システム，教職員メールや大学トップ Web サイトなど重要な学内システムのバックアップ用途として比較的規模の大きな仮想化基盤システムを導入したが，商用クラウドサービスの充実に伴い，個々のシステム毎に最適なクラウドサービスを選択し利用することで，より低コストで遠隔地運用が実現可能となってきた．

しかしながら KUINS-DB サーバは DNS サービスだけでなくネットワークサービス全体のデータベースであり，KUINS-III アドレスと連携して運用しているため

- 学内のネットワーク機器へのコンフィグ投入
- 学内の内向き権威 DNS スレーブサーバからの情報取得

のように KUINS-III 同士での双方向通信が必要となり移行は容易ではない．

例えば大手 Amazon 社の AWS サービスでは SINET5 の「クラウド接続サービス」を用いて大学内ネットワークと L2 で接続することは可能であるが，その場合でも仮想マシン本体に KUINS-III アドレスを直接割り当てることはできず，クラウド事業者から割り当てられたプライベートネットワークと学内に設置した BGP ルータを経由して通信する方式となる [5]．

今回は一般的な商用クラウドのサーバ単体規模において，KUINS-III との双方向通信を簡易的に実現できるか検討を行った．

5.1 学内機器

京都大学では国内各地の遠隔地に点在する小規模な観測所や研究施設に学内ネットワークを VPN で提供するために京都吉田キャンパスと遠隔地の双方に NEC 製 VPN ルータ機 [4] を設置し運用している．

本機器は L2TP/IPsec サーバ機能を有しており，吉田キャンパス内の VPN ルータ機に商用クラウド向けの L2TP/IPsec の設定を追加した．接続時にはクライアントに KUINS-III ネットワークに割り当てる設定となっており設定内容を以下にまとめる．

```
ike proposal ike1 encryption aes-256 \
  hash sha2-256 group 1024-bit
ike policy pol1 peer [KUINS-DB IP] \
  key [secret] ike1
ipsec autokey-proposal sec1 \
  esp-aes-256 esp-sha
ipsec autokey-map map1 sec-list \
  peer [KUINS-DB IP] sec1
!
ppp profile lns1
  authentication request chap
  authentication password [user] [password]
  lcp pfc
  lcp acfc
  ipcp ip-compression
!
interface GigaEthernet0.0
  ip address [VPN Server IP]
  no shutdown
!
interface GigaEthernet1.0
  ip address [KUINS-III Server IP]
  ip proxy-arp
  no shutdown
!
interface Tunnel0.0
  ppp binding lns1
  tunnel mode l2tp ipsec
  ip unnumbered GigaEthernet1.0
  ip tcp adjust-mss auto
  ipsec policy transport map1
  no shutdown
```

特に NEC 社製 VPN ルータ機でなくとも L2TP/IPsec 機能を有する機器であれば同様に利用できると考えられる．

5.2 KUINS-DB の設定

KUINS-DB では L2TP/IPsec のクライアントとして IPsec のための strongSwan と L2TP のための xl2tpd を用いて以下のような設定を行った．それぞれ順に strongSwan の接続設定と事前共有キーの設定，xl2tpd の接続設定と ppp オプションの設定である．

```
conn %default
        closeaction=clear
        keyexchange=ikev1
        authby=secret
        type=transport
        reauth=no
        ike=aes256-sha256-modp1024!
        esp=aes256-sha1!
conn k3
        left=[KUINS-DB IP]
        leftprotoport=17/1701
        right=[VPN Server IP]
        rightprotoport=17/1701
        auto=start
```

```
: PSK [secret]
```

```
[lac client]
lns = [VPN Server IP]
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd.client
length bit = yes
local ip = [KUINS-III Client IP]
autodial = yes
```

```
ipcp-accept-local
ipcp-accept-remote
refuse-eap
require-mschap-v2
noccp
noauth
mtu 1410
mru 1410
nodefaultroute
debug
connect-delay 5000
name [user]
password [password]
```

グローバル IP アドレスのみのサーバに ppp0 インターフェースで 1KUINS-III アドレスが割り当てられ，L2 で双方向通信が可能であることが確認できた．

5.3 実現方法の考察

既存機器の機能とオープンソースのツールを利用することでサーバ単体規模で低コストで簡易的な KUINS-III アドレス利用環境が構築できた．

さらにこの方法であれば各商用クラウドの事業者が提供するプライベートネットワーク機能に依存せず，SINET5 の「クラウド接続サービス」非対応な事業者でも利用できるため，多様な商用クラウドで利用可能という長所がある．

しかしながら運用実績がないため，現時点でどのような不具合が内在しているか不明である．特に対象サーバが DNS 権威マスタという重要なサービスであるため安易に導入することが難しい．

今後試験機を用いて長期稼働させた場合の検証や VPN のリカバリ動作確認なども行い，また大学全体としての商用クラウド利用動向なども勘案して総合的に導入を判断する予定である．

6. おわりに

- ネットワーク管理データベース KUINS-DB を遠隔地データセンタに移行することで，京都市大規模災害発生時にも DNS サービス及び DNS レコード変更機能の継続を実現できた．
- 学外からのデータベース利用やメンテナンス接続にもセキュリティに配慮して対応することができた．
- より低コスト化を目的として商用クラウド利用についても検討を行った．実現可能であったが他の方法も含め引き続き検討する予定である．

参考文献

[1] 宮崎修一 他：KUINS 接続機器登録データベースの概要，第 2 7 回全国共同利用情報基盤センター研究開発連合発表講演会 研究開発論文集 pp.47-51 (2005)
[2] 高見好男 他：京都大学学術情報ネットワークシステム接続機器管理システム『KUINS-DB』の更新，第 3 4 回全国共同利用情報基盤センター研究開発連合発表講演会 研究開発論文集 pp.53-57 (2012)
[3] 針木剛：京都大学における DNS サービスの改善，大学 ICT 推進協議会 2018 年度年次大会 https://axies.jp/ja/qruv9l/conf2018papers/1bv0s0 (2018)
[4] NEC 社製ルータ https://jpn.nec.com/univerge/ix/ (参照 2020-01-30)
[5] 学術研究機関での SINET5 を経由した AWS の利用 https://aws.amazon.com/jp/blogs/news/sinet5-aws-explain/ (参照 2020-01-30)