サービス継続と異種 OS 異種 LDAP サーバソフトウェア間の安全な移行を考慮した LDAP サーバの構築と移行

佐々木 七夏海 [1)], 柘植 朗 [1)], 田島 尚徳 [1)],
田島 嘉則 [1)], 服部 昌祐 [1)], 嶋田 創 [2)]

1) 名古屋大学 情報連携統括本部 情報推進部
2) 名古屋大学 情報基盤センター

sasaki@icts.nagoya-u.ac.jp

Construction and Migration of LDAP Server with Considering Service Continuity under Different OSes and LDAP Server Software

Nanami Sasaki [1)], Akira Tsuge [1)], Hisanori Tajima [1)],
Yoshinori Tajima [1)], Masahiro Hattori [1)], Hajime Shimada [2)]

1) Technology Services Department, Information and Communications, Nagoya University
2) Information Technology Center, Nagoya University

概要

名古屋大学の認証基盤システムとして運用している LDAP サーバには, 名古屋大学 ID をはじめとする本学全構成員の様々な情報を格納している．認証基盤システム構築当初から運用していた LDAP サーバの老朽化に伴い，OS および LDAP サーバソフトウェアの異なる新規の LDAP サーバを構築し移行を行うことになった．本論文では，平成 30 年 3 月に行われた，旧システム依存のクライアントへのサービスの連続性を考慮した LDAP サーバの移行方法等について報告する．

1 はじめに

名古屋大学では，「生涯利用可能なユーザ ID」である「名古屋大学 ID」を導入している．生涯 ID という特性上，名古屋大学 ID の総数は，減ることはなく増え続け，現在，総数は既に 120,000 件を超えている．名古屋大学では全ての名古屋大学 ID を LDAP サーバに格納している[1], [2].

膨大な数の名古屋大学 ID を格納するために，導入当時はスケーリングに優れていると判断された Solaris10 上で動作させた Sun Java™ System Directory Server（以下 SJSDS）という LDAP サーバソフトウェアを使用してきた．しかしながら，SJSDS および Solaris ともに開発は停滞しており，増加しつつづける名古屋大学 ID の認証基盤として，将来的に渡っての安定運用に不安がある OS および LDAP サーバソフトウェアと判断した．そのため，今回の移行を機に，現時点で活発に開発が行われている Red Hat Enterprise Linux 上で動作させた 389 Directory Server（以下 389DS）に変更することが決まった．

本論文では，サービスの継続および旧システムに依存があるクライアントへのサービス移行期間を考慮しつつ，異なる OS の上に異なる LDAP サーバソフトウェアがインストールされている環境のもとでの，LDAP サーバの移行方法について報告する．

2 LDAP

2.1 LDAP とは

LDAP (Lightweight Directory Access Protocol)とは，ディレクトリサーバと通信し，各種の情報を読み書きするためのプロトコルである．この情報は，運用目的にあわせて任意の情報を追加することが可能である[3], [4], [5].

また，2018 年現在において，LDAP サーバとは LDAPv3 をサポートする任意のディレクトリサーバを指すことが一般的である[6], [7], [8].

2.2 389 Directory Server とは

389DS とは，Red Hat 系列のオープンソース

LDAP サーバソフトウェアである[9]．Red Hat Directory Server は 389DS の商用版である[10].

389DS は Fedora Directory Server（以下 FDS）から発展した LDAP サーバソフトウェアである．この FDS は，SJSDS は同じく Netscape Directory Server から発展した LDAP サーバソフトウェアである[11], [12]．そのため，389DS と SJSDS は親和性があると考える．

3 LDAP サーバの移行

3.2 新旧 LDAP サーバの基本情報

- 新 LDAP サーバ
  OS　　: Red Hat Enterprise Linux Server
  LDAP : 389DirectoryServer
  Server : PRIMERGY RX2530 M2
  ※　物理サーバ，2 台購入
- 旧 LDAP サーバ
  OS　　: Solaris10
  LDAP : Sun Java™ System Directory Server
  Server : Sun Blade T6320 Server Module
  ※　物理サーバ，4 台購入

今後，本論文では上記に記載するサーバを「新 LDAP サーバ」及び「旧 LDAP サーバ」と表記する．なお，新旧 LDAP サーバともに，1 台の物理サーバ上で 1 つの LDAP サーバソフトウェアを動作させる構成となっている．

3.3 目標

- 新 LDAP サーバの設定（パスワードの暗号化方式，検索可能件数の制限解除等）をなるべく旧 LDAP サーバの設定と同じ設定にすること．
- 旧 LDAP サーバを止めずに移行すること．すなわち，認証基盤システムの停止時間が無いように移行すること．
- 旧 LDAP サーバの設定に依存するクライアントの存在を想定し，旧 LDAP サーバと新 LDAP サーバを並行動作させる移行期間を設けること．

3.1 移行方法

ここでは，別々の LDAP ソフトウェア間のマルチマスターレプリケーションに重点を置いて報告する．

図に関する説明は下記の通りである．

- 四角（青）：マスターレプリカ
- 四角（緑）：コンシューマーレプリカ
- 矢印（赤）：読み書き可能な通信経路
- 矢印（青）：読み取り専用の通信経路
- 矢印（緑）：テスト専用の通信経路
- 矢印（黒）：レプリケーションの方向
- 外枠（黄）：新 LDAP サーバ群

1. 新 LDAP サーバの各種設定
   旧 LDAP サーバの設定資料を参考に，Log，検索可能エントリ数の拡大，ldif ファイルをインポートする際の構文チェック機能の設定を行う．

2. 段階移行 第 1 段階
   図 1 のように，新 LDAP サーバ 2 台をコンシューマーレプリカに設定し，レプリケーション及び参照のテストを行う．

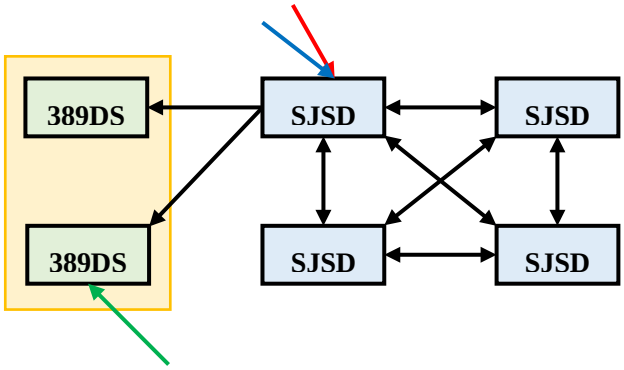

図 1：移行中のレプリケーション構成図(1)

3. 段階移行 第 2 段階(1)
   マルチマスターレプリケーションは最大 4 台までしかできないという規定があるため，4 台の旧 LDAP サーバのうち 2 台をコンシューマーレプリカに降格する．
   また，新 LDAP サーバ 2 台もあらかじめマスターレプリカに昇格しておくだけではなく，マルチマスターレプリケーションを行うように設定しておいた．

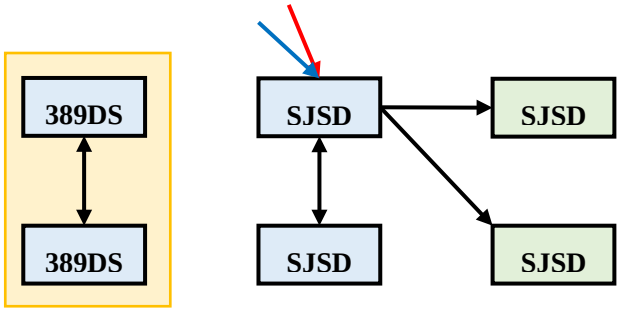

図 2：移行中のレプリケーション構成図(2)

4. 段階移行 第 2 段階(2)

当初，旧 LDAP サーバと新 LDAP サーバの双方向のレプリケーションを行いながら移行する方針であったが, 新 LDAP サーバから旧 LDAP サーバに対してレプリケーションする際に不具合が生じたため, 別の方法を模索した.

その結果，図 3 のように，同じ LDAP ソフトウェア同士はマルチマスターレプリケーションを行うように設定し，異なる LDAP ソフトウェア間のレプリケーションは「旧 LDAP サーバ(SJSDS) → 新 LDAP サーバ(389DS) 」のみ行うようにした.

この段階より，LDAP クライアントの新 LDAP サーバへの移行を開始した. 学内部局のシステムを含めた, LDAP の読み出しのみを行う LDAP クライアントは，新 LDAP サーバ側にアクセスを行うように変更を依頼した(図 3 青矢印). 新 LDAP サーバへの変更で不具合が発生した LDAP クライアントについては，クライアント側の問題解決までの間，従来通り旧 LDAP サーバへのアクセスを許可する形で移行期間を設けた(図 3 青破線矢印). 一方，データ更新を必要とする LDAP クライアントは引き続き旧 LDAP サーバ側に対してアクセスを行う(図 3 赤矢印).

また，この第 2 段階では，なんらかの不具合で新 LDAP サーバに更新が行われた場合，データの不整合が発生してデータベースにとって致命傷になってしまうため, 2 つ対策を取った. 詳しくは，「3.2 段階移行における注意点」に記載する.

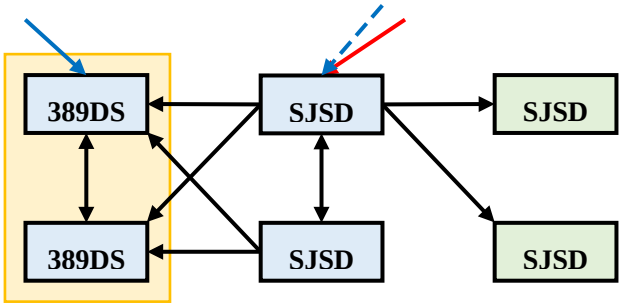

図 3：移行中のレプリケーション構成図(3)

5. 段階移行 第 3 段階(1)

図 4 の通り，全ての通信経路が新 LDAP サーバに行くように，参照先のサーバを旧 LDAP サーバから新 LDAP サーバに変更する. エントリの検索だけではなく，エントリもすべて正しく更新されているか確認する.

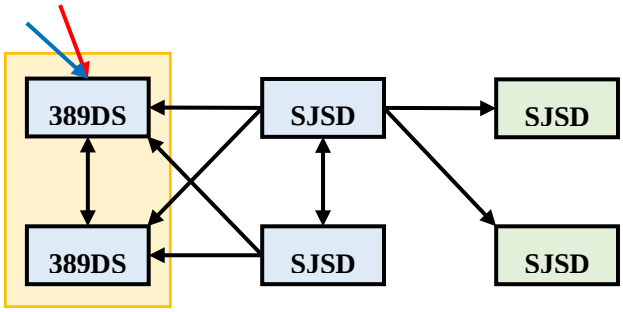

図 4：移行中のレプリケーション構成図(4)

6. 段階移行 第 3 段階(2)

新 LDAP サーバと旧 LDAP サーバ間でレプリケーションを続けると障害が起こる可能性があること，参照先を新 LDAP サーバに変えたことから旧 LDAP サーバにはエントリの検索も更新も行われないため，図 5 のように，旧 LDAP サーバの取り外しを行った.

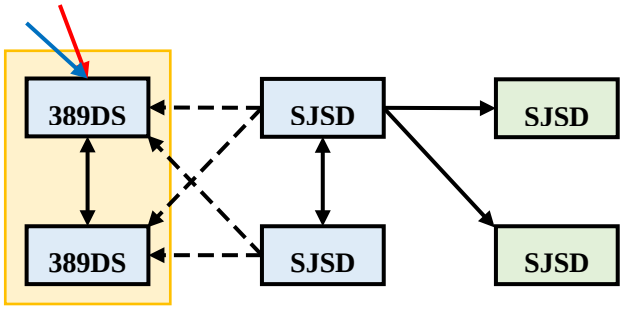

図 5：移行中のレプリケーション構成図(5)

7. 移行完了

図 6 のように，旧 LDAP サーバを新 LDAP サーバから完全に取り外し, LDAP サーバの移行作業は完了である.

2018 年 3 月以降は，新 LDAP サーバ 2 台での運用を行っている. まだ構想段階だが, LDAP への負荷増大などに応じて，1〜2 台程度，サーバの追加と負荷分散を検討している.

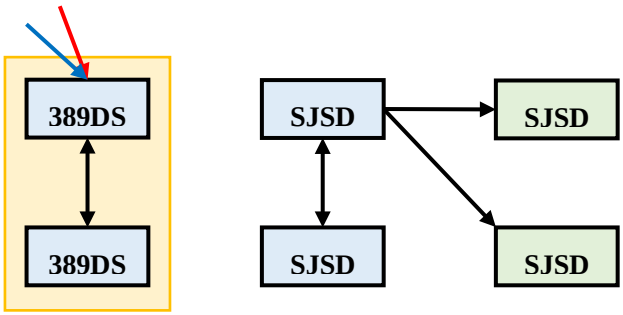

図 6：移行後のレプリケーション構成図

3.2 段階移行における注意点

段階移行の第 2 段階に当たる部分では，なんらかの不具合で新 LDAP サーバにデータ更新要求が送信されて更新が行われた場合，旧 LDAP サーバと新 LDAP サーバのデータ間に不整合が起きてしまう. そのため, 必ず新 LDAP サーバに更新が行われるのは防がなければならない.

新 LDAP サーバへの更新を未然に防ぐため，下記の 2 つの対策を行った.

- 読み取り専用の ACL (Access Control List) を作成し，新 LDAP サーバに適用する.
- 元々，読み書き可能な通信経路や読み取り専用の通信経路は存在せず，1 つの通信経路を使用していた．そのため，新たに読み書き可能な通信経路を作成した．同時に，LDAP サーバに更新を行うシステムの管理者に依頼し，システム内の DNS を書き換え作業も行った.

上記の 2 つの対策を実施することで，新 LDAP サーバに更新が行われることは無く，安全に移行を行うことができた.

3.3 負荷分散

図 6 の通り, 現在, 負荷分散は行っていない. なぜなら，2018 年 3 月下旬に行ったエントリの更新処理を行った際に，サプライヤーの更新が終わる時間とコンシューマーの更新が終わる時間に差があったからである．タイムラグ自体はそれほど大きくはないが，利用者にも影響が出る可能性が有り，現在は負荷分散を行っていない.

ただ，3 月と 9 月の一括処理時を除き，普段の更新は即時反映なので，一括処理時前に「新入生一括追加により LDAP 更新(パスワード変更など)の反映が遅くなります」という事前アナウンスを行うことにした上で負荷分散も検討の余地がある.

3.4 採用されなかった移行方法（直截移行）

今回の移行方法の他にもう 1 つ方法があった. この方法は，検討の末，障害が起きたときのリスクヘッジができないこと，一時的に LDAP サーバへの更新ができなくなること，新 LDAP サーバ以降後に旧 LDAP サーバの設定に依存があるクライアントが発見された場合の対応が難しいという理由で, 採用を見送った. しかし, LDAP サーバの移行における検討事例の参考としてとして，記載しておく.

この直截移行は，別々の LDAP ソフトウェアをレプリケーションすることはないので，読み取り専用の ACL や新たに通信経路を作成する必要はない.

1. 新 LDAP サーバの各種設定
   旧 LDAP サーバの設定資料を参考に，Log，検索可能エントリ数の拡大，ldif ファイルをインポートする際の構文チェック機能の設定を行う.
2. 更新の拒否及びデータの登録
   一時的に全ての旧 LDAP サーバへの更新を拒否する．ただし，検索は可能である.
   更新を拒否している間に旧 LDAP サーバの全エントリのデータをエクスポートし，そのデータを新 LDAP サーバにインポートする.
3. 移行完了
   参照先のサーバを旧 LDAP サーバから新 LDAP サーバに変更して，移行完了である.

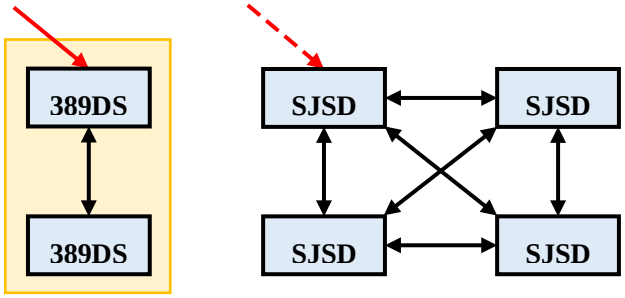

図 7：直截移行

4 成果と今後の課題

約 1 ヶ月間かけて 1 段階ずつ移行していき，2018 年 3 月に新 LDAP サーバへの移行が完了した．移行期間のうち，最もクリティカルな状態で

ある第 2 段階(2)には 1 週間を取った．この期間に LDAP サーバ側に発生したトラブルは無く，LDAP クライアント側に，移行を機会に廃止するサブツリーを参照していた物が 1 件存在したのみである．その後，新たな属性を LDAP スキーマに追加する作業等を行うという大きめの改変も含めた通常運用を行っている．現在，大きな障害は発生しておらず，問題なく稼働している．

ただし，ごく稀に新 LDAP サーバへの接続が失敗することと，新 LDAP サーバ間のマルチマスターレプリケーションが上手く行かないことがあるため，今後は更なるシステムの安定化に努めたい．また，システムの安定化に加え，負荷分散の方法や災害時の対策も引き続き考察したい．

参考文献

[1] 梶田将司，太田芳博，田島嘉則，田島尚徳，平野靖，内藤久資，間瀬健二，"生涯利用可能な名古屋大学 ＩＤ の導入に伴う名寄せ問題とその解決法"，情報処理学会研究報告インターネットと運用技術（IOT），2008-DSM-048, pp.73-78, 2008.3

[2] 太田芳博，梶田将司，田島嘉則，田島尚徳，平野靖，内藤久資，間瀬健二，"生涯利用可能な名古屋大学 ID の新規発行における名寄せ方法に関する検討"，情情報処理学会研究報告インターネットと運用技術（IOT），2008-IOT-001, pp.109-114, 2008-05

[3] https://tools.ietf.org/html/rfc4511

[4] 平野靖，"入門 LDAP 認証（１） ―準備―"，名古屋大学情報連携基盤センターニュース，Vol.4, No.1, pp.33-46, 2005.2

[5] 平野靖，"入門 LDAP 認証（２） ―検索と認証―"，名古屋大学情報連携基盤センターニュース，Vol.4, No.2, pp.122-141, 2005.5

[6] https://tools.ietf.org/html/rfc3377

[7] 平野靖，"入門 LDAP 認証（３） ―検索と認証（セキュア編）―"，名古屋大学情報連携基盤センターニュース，Vol.4, No.3, pp.200-210, 2005.8

[8] 平野靖，"入門 LDAP 認証（４） ―LDAP 認証付きアプリケーション―"，名古屋大学情報連携基盤センターニュース，Vol.4, No.4, pp.303-306, 2005.11

[9] http://directory.fedoraproject.org/index.html

[10] https://tech-lab.sios.jp/archives/7571

[11] http://www.asahi-net.or.jp/~aa4t-nngk/389ds.html

[12] https://www.ossnews.jp/oss_info/389_Directory_Server