社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－IOT－1（9）
2008/5/8

名古屋大学における統合サーバの構築と運用

内藤 久資[†,††] 山口由紀子[†††] 梶田 将司[††,†††] 平野 靖[†††] 間瀬 健二[††,†††]

† 名古屋大学多元数理科学研究科
†† 名古屋大学情報連携統括本部情報戦略室
††† 名古屋大学情報連携基盤センター
E-mail: naito@math.nagoya-u.ac.jp

あらまし 名古屋大学では，学内に数多く存在する電子メールサーバ・ウェブサーバ等を集約する統合サーバを構築した．その統合サーバの認証システムとして，統一認証基盤と緩やかな連携を持つ「システム依存認証基盤」を構築し，端末システムなどを含むさまざまなシステムを統一認証基盤と一貫して関連づける手法として LDAP ホスティングを考案した．本報告では，統合サーバのシステムとその運用方法およびシステム依存認証基盤について報告をおこなう．
キーワード 電子メールサーバ，ウェブサーバ，ユーザ認証基盤，ユーザ ID，アイデンティティマネジメント

Construction and Management of Unified-Server in Nagoya University

Hisashi NAITO[†,††], Yukiko YAMAGUCHI[†††], Shoji KAJITA[††,†††], Yasushi HIRANO[†††], and Kenji MASE[††,†††]

† Graduate School of Mathematics Nagoya University
†† Information and Communication Technology Services, Nagoya University
††† Information Technology Center, Nagoya University
E-mail: naito@math.nagoya-u.ac.jp

Abstract In Nagoya University, we have constructed Unified-Server to integrate a lot of deceterized e-mail and web servers in University. We also construct an authentication infrastructure that has loosely-coupled with Unified Authentication Infrastructure of Nagoya University as the authentication system for Unified Server. It provides authentication infrastructure based on Unified Authentication Infrastructure for other systems including File System and Terminal Services for school, departments and/or research groups in University, In this paper we report the system and methods of managements of Unified Server and the authentication infrastructure.
Key words E-Mail Server, Web Server, User Authentication Infrastructure, User ID, Identity Management

1. Introduction

研究・教育の場での電子メールおよびウェブ等の情報サービスの役割は，従来にもまして，その重要性が増大している．また，名古屋大学のような大規模総合研究大学においては，部局・学部・研究室の独立性が高く，古くから電子メールの運用が行なわれてきた場合が多いなどの歴史的な経緯もあり，各階層の部門において電子メールの運用が継続されている．一方，これらのサービスは，その重要性が高まることに比例するように，SPAM メール・ウェブページの改竄・電子メールやウェブを通じた情報流出など，セキュリティ的な驚異の発信源となることも少なくない．今日では，これらのサービスを運用するためには，高度な運用技術を必要とすることは云うまでもない．しかし，従来は，適切な運用技術を持った教職員・大学院生などにより運用されてきたこれらのサービスも，現在では適切な運用技術を持った人員をそれぞれの部門で確保することが困難になりつつある．このような状況をふまえ，名古屋大学では，2006 年秋に発足した情報連携統括本部において，電子メール・ウェブを中心とした，各種サービスを集約するサーバ（「統合サーバ (Unified Server)」）を構築することを開始した．

一方，名古屋大学では，アイデンティティマネージメントの下での統一認証基盤を新たに構築し，その下での情報サービスを行なっている (cf. [1]〜[7]). 統一認証基盤の目的のひとつは，学内の種々の情報サービスの ID を一元化し，各情報サービス

提供者を個々のユーザの管理から開放することにある．しかし，一般に，電子メール・ウェブサーバおよび端末システム等の運用を行なうためには，それらの認証環境に，個々に異なった `uidNumber`, `userId` などを割り当てる必要が生じ，個々のサーバに対する認証情報をそのまま統合認証基盤データベースに格納することが困難である．そこで，我々は，統合認証基盤データベースと緩やかな結合をもつ，個別のシステムごとの認証システムをいかに構築すべきかを考察した．その結果，我々が「LDAP ホスティング」と呼ぶ，個々の UNIX ライク認証を必要とする個々のシステムごとの認証環境を実現し，実際に複数のシステムの認証を，それぞれ独立に運用することが可能となった．

本報告では，統合サーバのシステムと運用方法を報告するだけではなく，統合サーバに伴って構築を行なった LDAP ホスティング認証環境の概要も解説し，統合サーバおよび学生教育用計算機システムに対して LDAP ホスティングを適用した事例を通じて LDAP ホスティングの利点を考察したい．

2. 統合サーバ

統合サーバの目的は，大学内の部局・学部・研究室（以後，誤解のない限り「ドメイン」と呼ぶ）などで運用されている電子メールサーバなどを，情報連携統括本部が運用するサーバに集約し，各ドメインごとに行なわれているハードウェア・システムなどの管理業務を軽減することにある．単に電子メール利用環境を提供するだけであれば，名古屋大学構成員であることを利用資格とする「全学メールサービス」を利用すればよいが，現実的には，従来通りの電子メールアドレスの利用を希望するユーザも多く，また，研究グループや学年単位などのメールエリアス，メーリングリストなど，各ドメインごとに様々なメールサーバの利用形態が考えられるため，少なくとも現時点では，各ドメインの電子メールサーバのハードウェア及びシステム管理を情報連携統括本部で行なうことが望ましいと考えた．

また，各ドメインでは，電子メールサーバのみならず，DNS サーバ，ウェブサーバ，DHCP などの運用が行なわれている．したがって，電子メールサーバの移行のみでは，ドメイン管理者の負担を必ずしも軽減することにならないため，統合サーバではウェブ・DNS・DHCP・WebDAV サービスも行なっているが，以下では，主に電子メールサーバについて，名古屋大学で構築した統合サーバについて述べる．

2.1 統合サーバのシステム

統合サーバは，単一のホストではなく，以下に述べる複数台のホストによって構成されている (2008 年 4 月現在)．

- Apple Xserve (MacOS X Server 10.4.x) 6 台．
- RAID ファイルシステム（ファイバチャネル接続）
  - 運用システム: 500 GB × 14 × 2, 実効容量 8.3TB,
  - バックアップ: 500 GB × 12, 実効容量 6.0TB.
- ホスト・ファイルシステム間は Storage Area Network.

なお，6 台のホストのうち 2 台は Storage Area Network のディスクコントローラとしてのみ利用となるため，実質的にサービスを提供するホストは 4 台となる．また，電子メール・ウェブ・DNS・WebDAV 各サービスを実施するためのソフトウェアは，MacOS X Server にバンドルされたものを利用している(注1)．MacOS X Server のソフトウェアアップデートによりサービスソフトウェアのアップデートも同時に行なえるため，保守コストを多少なりとも軽減することになる．

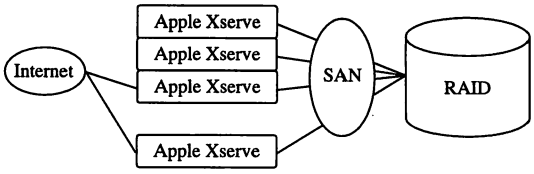

図 1 ホスト構成図

なお，年 1 回行なわれる，電気設備保守によるキャンパス全体にわたる停電時には，統合サーバのみならず，期間ネットワーク設備に対しては，電源車による電源バックアップが行なわれ，キャンパス全体の停電時にもキャンパス外から統合サーバへのアクセスが可能である．

2.2 運用における責任分界

統合サーバは，システム設置主体とエンドユーザという単純な運用形態ではなく，システムの設置主体である情報連携統括本部，サービスを受けるエンドユーザの間に，実際のサービスを実施しているドメイン管理者が存在している．そのため，システム運用責任について，明確な責任分界点を設定し，運用責任を明確にすることが重要となる．

今回の統合サーバの運用では，以下に述べるポリシにしたがって責任分界点を設定しサービスを実施している．

- ハードウェア・オペレーティングシステム・サービスのためのソフトウェアの保守管理は，システム設置主体者である情報連携統括本部が責任を持つ．
- ソフトウェアの設定（例えばウェブサーバの設定等）は，デフォールトの状態であれば，システム設置主体者である情報連携統括本部が責任を持つが，ドメイン管理者に許された範囲内の設定変更後は，ドメイン管理者が責任を持つ．
- ユーザ管理・コンテンツ管理・DNS ゾーンデータ管理等はドメイン管理者が責任を持つ．
- エンドユーザ対応の最初のステップはドメイン管理者が行なう．

すなわち，デフォールト設定のままでの運用を行なう限りは，ドメイン管理者はユーザ管理およびコンテンツ管理等とエンドユーザ対応のみを行なえばよい．なお，ドメイン管理者は SSH によって統合サーバの `chroot` により制限された範囲へのログインが可能であり，それによって電子メール送受信ログ・ウェブサーバアクセスログ等の主要なログの参照が可能となっている．したがって，エンドユーザからの「メールが届かない」などの苦情に対しての一次対応をドメイン管理者が行なうことを可能とした．

なお，このような責任分界点を設定することにより，ドメイン管理者の負担を軽減することができた (cf. 表 1)．

(注1)：DHCP サーバのみは，MacOS X Server にバンドルされたものを使っていない．

業務内容	統合サーバ利用前	統合サーバ利用後
ハードウェア管理	あり	なし
ソフトウェア管理	あり	なし
ユーザ管理	あり	あり

表 1　統合サーバ利用によるドメイン管理者業務の変化

2.3　サービス実装方法

ここでは, 統合サーバでの具体的なサービス方法を解説する. はじめに, サービス実装方法の概略とその利点と欠点を述べ, その後, 各サービスにおけるドメイン管理者の管理方法とエンドユーザへの制限等を述べる.

2.3.1　サービス実装方法の概略

統合サーバでは, 複数のドメインに対する電子メール・ウェブ等のサービスを複数台のホストに分散させ, それぞれのドメインに対する電子メールおよびウェブサービスは, 全て異る仮想 IP アドレス上で, 異るプロセス（および設定ファイル群）を用いて実施している. 具体例を示せば次のようになる.

- `d1.nagoya-u.ac.jp` と `d2.nagoya-u.ac.jp` の Postfix は異るプロセスが動作する. また, それぞれ異る IP アドレスを利用する.
- `d1.nagoya-u.ac.jp` と `d2.nagoya-u.ac.jp` の Apache は異るプロセスが動作する. また, それぞれ（上記 Postfix とも）異る IP アドレスを利用する.

この方法の利点は次のように考えることができる.

- ドメインごとに異るプロセスで動作することにより, ドメインごとに設定を変更することが可能となる.
- プロセスごとに異る IP アドレスを利用することにより, SSL 利用時にサーバ証明書を, それぞれの FQDN に即したものを利用することが可能となる.
- プロセスが実行されているホストのハードウェア障害またはソフトウェアアップデートによる停止時には, 図 2 に示すように, 利用している仮想 IP アドレスを他のホストに割り当てることにより, 短時間の停止の後に, 他のホストでサービスを開始することが可能となる(注2).

なお, この方法の最大の欠点は, IP アドレスを多く消費することであると考えられる.

2.3.2　各サービスの詳細

エンドユーザへのアクセス制限として, 電子メールについては, エンドユーザがインターネット上どこからでもメールの送受信を可能とするため, 受信プロトコルは IMAP over SSL および POP3 over SSL に限定し, 送信には SMPTD over SSL または Submission with TLS 上で SMTP-AUTH を必須とした(注3). また, ウェブについても, コンテンツ投入方法を scp または sftp に限定した.

一方, 電子メールにおいては, 研究グループ単位などへのメールエリアスも必要であり, ウェブについても, それらの単位でのウェブページの設置などが求められる. 統合サーバでは, これらの単位を「グループ」として定義し, メールエリアスを実現すると同時に, グループ単位でのウェブページの設置も可能とした.

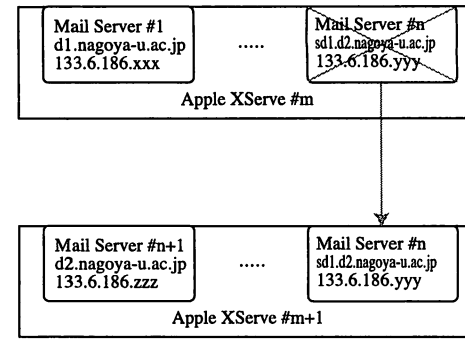

図 2　ホスト停止時のサービス切り替え

なお, エンドユーザのユーザ ID 体系およびパスワードについては, 3. 節で詳細に述べる.

一方, 2. 2 節で述べた通り, ユーザ管理はドメイン管理者の責任となる. しかし, 統合サーバの設置ポリシを考えると, ドメイン管理者の負担の軽減が必要であり, また, ドメイン管理者への技術レベルとしてあまり高度なことを要求することは望ましくない. そのため, これらの管理業務を実施するための Java Servlet による「管理 GUI」を開発し, ドメイン管理者への利便をはかっている. なお, 「管理 GUI」では, 新規ユーザ作成・ユーザ削除・メールクォータ・ディスククォータなどのユーザ管理, 上述のグループ管理, DNS ゾーン管理, DHCP 静的アドレス割り当てリスト管理などの業務を行なうことができる.

2.4　運用実績

2008 年 4 月現在, 統合サーバで運用されているサービスとそれを利用しているドメイン数などは表 2 の通りである.

サービス	ドメイン数	ユーザ数
メール	15	20,000
ウェブ	3	
DNS	11	
DHCP	2	

表 2　運用状況：ユーザ数は概数である. DHCP の「ドメイン数」は「サブネット数」をあらわす.

3.　LDAP ホスティングにおけるシステム依存認証

本節では, 統合サーバシステム構築時に同時に設計を行なった, 統合認証基盤と緩やかな連携を持つ Unix ライクシステムに対する認証システムである LDAP ホスティングサービスについて解説を行なう.

通常, LDAP を用いた UNIX 認証を行なうためには, 各ユーザのエントリとして `posixAccount` オブジェクトを与え

(注2)：Storage Area Network のディスクコントローラも二重化してあるため, 適切な順序でホストの停止・起動を行なうことにより, ディスクコントローラホストも含めて, サービス停止を最短にしてソフトウェアアップデートを行なうことが可能となった.

(注3)：Mailing List の利用, 及びウェブメールの利用も可能とした.

る必要がある (cf. [9]). すなわち, 各ユーザに対して uid, cn, uidNumber, gidNumber, geCos, homeDirectory, loginShell, userPassword 属性を与える必要がある. 仮に, 統一認証基盤の各ユーザエントリにこれらの属性を設定すると, 統一認証基盤で UNIX 認証を行なう全ての情報システムが, 同一の uidNumber, homeDirectory などを用いることとなり, 各情報システムのシステム設計に大きな制限を与えることとなる.

名古屋大学の統一認証基盤においては, 「システム依存属性を登録しない」とのポリシを定めた. その理由は, アイデンティティマネージメント (Identity Management, IdM) の基本ポリシである「ユーザ基本情報のみを登録する」ことだけではなく, 統一認証基盤の設計と, それを利用する情報システムの設計の間に本質的ではない制限を与えることを避けることが念頭にあった.

ここでは, 複数のドメイン (以下では d1.nagoya-u.ac.jp と sd1.d2.nagoya-u.ac.jp とする) が統合認証基盤を用いた認証をベースに電子メールサービスを実施する場合を考えてみる. この場合, それぞれのドメイン管理者およびユーザにとっては, ユーザプリンシパル (ユーザ ID, 電子メールアドレスの "@" 以前の部分) は, それぞれのドメインで独自に設定したいと考えるのが自然である. しかし, これを実現するための通常のユーザ認証のフレームワークでは, auser@d1.nagoya-u.ac.jp と auser@sd1.d2.nagoya-u.ac.jp の 2 つのメールアドレスに対応する "User Pricipal" はともに auser であるため, 通常にユーザ認証 framework を用いると, 複数のドメインで一致するユーザプリンシパルを用いることができない. これを統合認証基盤上で実現しようとすると, それぞれのサービスごとの属性を設定することになり, 場合によっては, 一人のユーザエントリに対して, 多数の user pricipal を格納することにもなりかねない.

さらには, ウェブサービスでも「個人ページ」を運用する際には, ウェブページデータのファイル所有権を確保するため, 全てのユーザの subject として, LDAP の posixAccount オブジェクトを割り当てる必要がある (cf. [9]). すなわち, uidNumber をはじめとする, UNIX 認証フレームワークを用いる必要が生じる. この場合には, 認証基盤を利用する全ての情報サービスの個々のユーザに対して異なった uidNumber を割り当てる必要が生じる.

ここで述べる LDAP ホスティングサービスは, このような統一認証基盤が内在する矛盾を解決する一つの手段と考えられる.

3.1 LDAP ホスティングサービス

LDAP ホスティングサービスの基本的な考え方は, 統合認証基盤とは別個のデータベースに, UNIX ライク認証を必要とするシステムごとの認証データベースを構築することである. しかし, 単に別個のデータベースを構築するのではなく, 統合認証基盤のユーザエントリを必要な属性の参照またはコピーを適切に設定することに重点をおいて設計を行なう. この事実が, 上記の述べた「統合認証基盤との緩やかな結合」の意味するところである.

具体的に名古屋大学において実施した LDAP ホスティングの基本アイデアは以下のものである.

(1) LDAP サーバ上に統一認証基盤の基本 DIT (o=nagoya-u) とは独立した, 別の "LDAP ホスティング DIT" (o=otherhosts) を構築する.

(2) LDAP ホスティング DIT を利用する情報システムごとに LDAP ホスティング DIT のサブ DIT を作成する (ex. ou=service1,o=otherhosts).

(3) LDAP ホスティング DIT のサブ DIT は, 各情報システムごとに管理される.

すなわち, あるシステム (service1) の場合には, ou=service1,o=otherhosts が LDAP ホスティング DIT のサブ DIT として割り当てられ, このサブ DIT 内には, LDAP サーバで利用可能なスキーマ定義に従う限り, 適切なユーザエントリを設定を許可する. このように, システムごとにサブ DIT を校正することにより, 他の情報システムと属性値の衝突を起すことなく, ユーザ管理を実施可能となる.

また, 統一認証基盤管理者は, それらサブ DIT に対して適切なアクセス制限を実施する一方で, 学内情報システムの構成によっては, o=otherhosts のレプリケーション, インデキシングなどを行なうことにより, 統一認証基盤へのシステム負荷を軽減することができる.

3.2 ユーザパスワードの同期

ここまでの LDAP ホスティングサービスの議論では, 単に統一認証基盤とは別に LDAP DIT を構成したにすぎず, このことは, 統一認証基盤の基本作業方針である「学内の認証情報の一元的管理」と矛盾する. また, エンドユーザの立場からみると, 統一認証基盤のプリンシパル-クレデンシャル (User ID-password) 対応と全く異なる ID が追加されたことにほかならない. 今回 LDAP ホスティングを設計するにあたり, エンドユーザが余分なパスワードを保有しない認証体系を前提条件とした.

そこで我々は LDAP ホスティングサービスの各ユーザエントリに含まれる userPassword 属性を, 以下の方法で同期することを行なった(注4).

(1) LDAP ホスティングサービスの各ユーザエントリには, parentDN 属性を設定する. この属性には, そのエントリに対応するユーザの名古屋大学 ID を設定する.

(2) 統一認証基盤および LDAP ホスティングサービスのユーザエントリのパスワード変更は, 「パスワード変更ユーティリティ」からのみ実施可能とする.

これにより, LDAP ホスティングサービスを利用する情報システムのパスワードは名古屋大学 ID のそれと同期することとなり, エンドユーザにとっては, 「ユーザ ID は個別の ID であり, パスワードは名古屋大学 ID とおなじ」との利便性の高い環境を提供した.

なお, 他のユーザ属性 (例えば geCos など) も, parentDN を

(注4) : LDAP ホスティングサービスのユーザエントリすべてにこの条件を要求しているわけではない. 名古屋大学 ID と同期しないユーザエントリの作成も可能である.

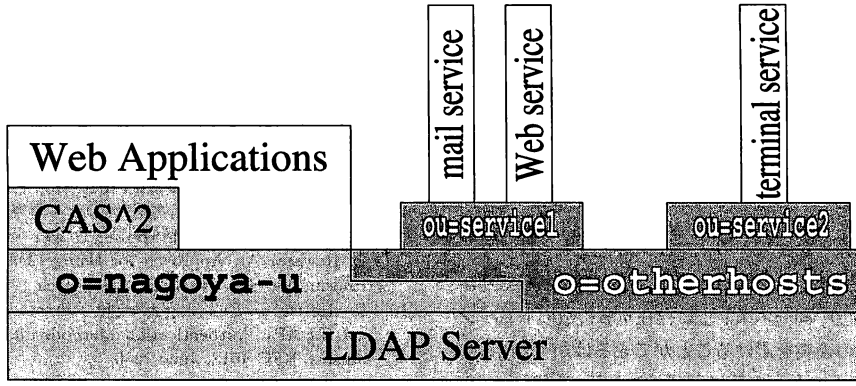

図 3 LDAP ホスティングサービスの位置付け: 薄いグレイの部分は従来の統合認証環境を, 濃いグレイの部分は LDAP ホスティングサービスを示す.

利用することにより, 容易に属性値の同期をとることが可能である.

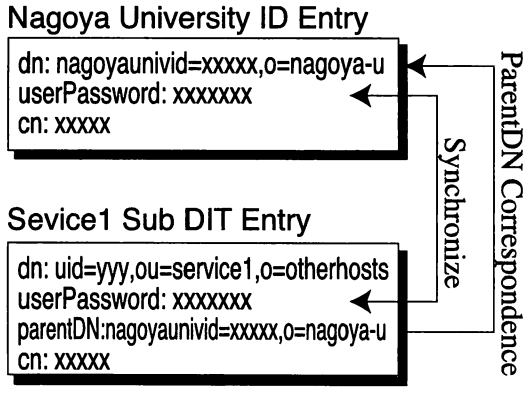

図 4 Password の同期

3.3 LDAP ホスティングを用いたサービス

ここでは, LDAP ホスティングサービスの利用例としての統合サーバ, および LDAP ホスティングサービスを利用した他の例として教育用端末システムでの利用形態を述べる. なお, 教育用端末システムは LDAP ホスティングサービスの標準的な利用形態を用いているため, これを先に解説する.

3.3.1 教育用端末システム

名古屋大学においては, 従来から学生向けシステムとして, 全学 ID をログイン ID とした教育用計算機システム (Linux, MacOSX, Windows) を運用している. 従来は, 全学 ID DIT 内にこのシステムの認証のための属性を格納して運用していたが, 名古屋大学 ID DIT のポリシに従い, このシステムの認証データベースに LDAP ホスティングを利用した.

名古屋大学の統合認証基盤は [7], [8] などで述べた通り, 2008 年 1 月に, 旧来の全学 ID から名古屋大学 ID への移行を行なった. その際, 当面の間, 統合認証基盤を用いたサービスは全学 ID と名古屋大学 ID の両方で利用可能とするとのポリシを定めた. これは, いずれの ID を用いても同一の環境へログイン可能であることを求めていることに他ならない. したがって, このシステムにおいても, いずれの ID でもログイン可能とする必要が生じた. そのため, このシステムの LDAP ホスティングサブ DIT `ou=media` では, 以下の設定を行なった.

通常, UNIX ホストの LDAP を利用した認証は以下のように行なわれる (cf. [10]).

(1) LDAP クライアントで指定された属性に対して LoginID を検索し, ログイン ID に対応する識別子 (`dn`) を得る.

(2) その結果得られた `dn` に対して, 入力されたパスワードとともにシンプルバインドを行なう.

また, 「LDAP client で指定された属性」には, `uid` または `cn` が利用されることが標準的である(注5). すなわち, この過程の 1 で唯一つのエントリを得るものであれば, 何であってもユーザプリンシパル (Login ID) として利用できることがわかる. 言い換えれば, 「検索対象 DIT 内で一意的な値を (複数) 設定することにより, いかなる文字列であっても, その一意性が保証されている限り, それをユーザプリンシパルとして利用可能」ということである. したがって, `ou=media` の各ユーザエントリ (`ObjectClass` として `posixAccount` をもつエントリ) の `uid` 属性として

- `uid:` 全学 ID
- `uid:` 名古屋大学 ID

の 2 つの値を設定することで, 当初の要求条件を満すことができた.

3.3.2 統合サーバ

Section 2. で述べた通り, 統合サーバは一つのシステム上で複数のドメインが共通に利用する形態を取っている. したがって, 以下のような, 通常の LDAP ホスティングサービスよりも複雑な状況が生じている. すなわち, 同一のホスト上に

- `user1@d1.nagoya-u.ac.jp`
- `user1@d2.nagoya-u.ac.jp`

(注5): [9] によれば, `uid` を利用すると定められているが, OpenDirectory LDAPv3 plugin では `cn` も利用可能である.

という2つのユーザプリンシパルが重複するユーザが存在する可能性がある. そこで, 教育用システムで用いたことと同様なアイデアを用いて, auser@d2.nagoya-u.ac.jp をメールアドレスとするユーザの属性に

- cn: auser-d2
- cn: auser@d2.nagoya-u.ac.jp

の2つの属性値を設定した. 前者は, メールソフトウェアがユーザのメールボックス名などで利用する「システム用のプリンシパル」であり, 後者をエンドユーザに「ユーザ ID」として通知した(注6). これにより, 同一ホスト上に存在する複数のドメイン間でのユーザ ID の衝突を避けることができるばかりか, エンドユーザは「メールアドレスをユーザ ID として利用」して, メール送受信・ウェブページコンテンツのアップロードなどを行なうことが可能となり, エンドユーザの利便性を向上することができた.

4. まとめ

本報告では, 学内に散在する多くの電子メール・ウェブ・DNS などのサーバを集約する統合サーバの構築と運用に関する報告を行なった. 特に, 各ドメイン管理者の負担を軽減 (表 1 参照) し, エンドユーザの利便性を損わないシステム構築と運用形態に重点を置いて解説した. さらに, 統一認証基盤と緩やかな結合を持つ LDAP ホスティングによる UNIX ライクシステムの認証環境の構築例を報告した. この認証環境を利用することで, 統合認証基盤データベースを整合性を保ったまま, これまでの統合認証基盤の議論では余り触れられることが少なかった, 多数の UNIX ライクシステムの認証環境を適切に構築することが可能となった. この認証環境は, 統合認証ミドルウェアに付随する, 新たなミドルウェアサービスとして考えることができる.

これらの実装例を通じて, 統合認証基盤の広範囲な利用の可能性として, 個々のシステムに対する認証データベースを柔軟に設計できることを示した.

文　献

[1] 梶田将司, 内藤久資, 小尻智子, 平野靖, 間瀬健二, CAS によるセキュアな全学認証基盤の構築, 情報処理学会 DSM 研究会研究報告, **DSM-39** (2005), pp. 35–40.

[2] 梶田将司, 内藤久資, 小尻智子, 平野靖, 間瀬健二, CAS によるセキュアな全学認証基盤による名古屋大学ポータルの運用, 第 3 回 WebCT コンファレンス予稿集, (2005), pp. 115–120.

[3] 内藤久資, 梶田将司, 小尻智子, 平野靖, 間瀬健二, 大学における統一認証基盤としての CAS とその拡張, 情報処理学会論文誌, **47** (2006), pp. 1127–1135.

[4] Hisashi Naito, Shoji Kajita, Yasushi Hirano, Kenji Mase, Multiple-tiered Security Hierarachy for Web Applications Using Central Authentication and Authorization Service, Proceeding of Middleware Workshop on IEEE International Symposium on Applications and the Internet (SAINT 2007), Hiroshima, JAPAN, (2007), 27.

[5] 梶田将司, 内藤久資, 平野靖, 瀬川午直, 小尻智子, 間瀬健二, 名古屋大学ポータルによる情報サービスの統合と課題, 電子情報通信学会技術研究報告 (IA), **107-151** (2007), pp. 1–6.

[6] 内藤久資, 梶田将司, 平野靖, 間瀬健二, 名古屋大学における CAS^2 を核としたアイデンティティマネジメントの現状と課題, インターネットコンファレンス 2007 論文集, (2007), pp. 31–40.

[7] 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, **DSM-48** (2008), pp. 73–78.

[8] 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 の新規発行における名寄せの方法に関する検討, 情報処理学会 IOT 研究会 (発表予定)

[9] L. Howard, An Approach for Using LDAP as a Network Information Service, RFC 2307, March 1998.

[10] R. Harrison, Ed., Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms, RFC 4513, June 2006.

(注6): 同一のユーザが複数のドメインでメールを利用する可能性があるため, プリンシパルとして名古屋大学 ID を利用することはできないことに注意が必要である.