統合サーバの構築と運用

内　藤　久　資　　山　口　由紀子

はじめに

電子メール及びウェブは，大学の研究・教育の場面において，必要不可欠なツールとしての位置を占めています。名古屋大学においても，電子メールサーバは部局（学部）・専攻（学科）・研究室などの種々の単位で運用され，ウェブサーバは電子メール以上に多くのホストで運用されています。一方では，電子メールサーバの管理が不十分なことに起因する spam メールの問題や，ウェブページの不正書き換え，ウェブページからの情報流出といった重大なセキュリティインシデントも少なくありません。このように，電子メール・ウェブなどの基本的なネットワークサービスは，その重要性と比例する形でセキュリティインシデントの発生源となることが多くなっています。

これらのネットワークサービスは，高度な知識と技術を持ったネットワーク管理者が適切な運用を行うことにより，安全かつ高可用性を持ったサービスとして実現されてきましたが，今日では，従来にもまして高度な知識･技術がネットワーク管理者に要求され，そのような人員を各サーバごとに配置することが困難になっています。

そのため，名古屋大学情報連携統括本部では，「統合サーバ」を構築し，電子メール及びウェブを代表とする各種のサービスの提供を開始しました。本稿では統合サーバの運用方法を中心に解説を行い，電子メール・ウェブサーバ等の統合サーバへの移行の参考として頂きたいと考えます。

Ⅰ．統合サーバについて

1．統合サーバのサービス方法

統合サーバのサービス内容を解説する前に，統合サーバでの “Service Level Agreement” (SLA) を述べておきます。“SLA” とは，サービス受益者とサービス提供者の間で合意すべきサービス内容の確認事項を指します。また，SLA で最も重要な部分は，サービス提供者がどこまで責任を持ち，どこからがサービス受益者側が情報提供または作業を行わなければならないかの「責任分界点」を明確にすることです。以下では，統合サーバのサービスにおける責任分界点を明確にする形で SLA を提示します。

まず，統合サーバでの以下の 3 者の役割を明確にしておきます。

★統合サーバシステム管理者　（以下「システム管理者」と呼びます）その名の通り，統合サー

バのシステム管理者で，情報連携統括本部が担当します。

★ドメイン管理者　統合サーバのサービスでは，すべての管理をシステム管理者が行うのではなく，サービスを受けるドメイン内部での管理者をおいていただきます。1 名または複数名を指定可能です。

★一般ユーザ　統合サーバのサービスを利用するユーザを指します。

統合サーバの SLA は，システム管理者とドメイン管理者との責任分界点を明確にします。

1.1　統合サーバシステム運用時間

統合サーバは，システム管理上必要な場合を除き，24 時間連続運転を行います。年 1 回の全学停電時もバックアップ電源を利用して運用を継続します。なお，「システム管理上必要な場合」とは以下を指します。

・システムハードウェア更新時に全システムの停止が必要になる場合があります。この場合には，事前にアナウンスを実施し，システム停止時間が最短となるように努力します。目標の最長システム停止時間は 1 時間です。

・システムの負荷分散設定変更，及びソフトウェアの更新時に，各サービスごとに数分間のサービス停止が発生します。この場合には，事前のアナウンスが行われない場合もありえます。現時点までの実績では，1 年に数回，数分程度のサービス停止時間が発生しました。

また，統合サーバ上の全データは，毎日深夜にバックアップを行います。したがって，統合サーバの運用中のディスクに障害が発生した場合には，直前のバックアップ（24 時間以内のもの）に戻すことが可能ですが，それ以上の保証は行うことはできません。なお，バックアップデータは，システム障害時のみに利用し，個別のユーザまたはドメイン管理者からのバックアップデータの参照の要求にお応えすることは行いません。

1.2　システム管理者の責任

システム管理者は，統合サーバのハードウェア，オペレーティングシステム，及びサービスを行うために必要なソフトウェアの管理を行います。また，システムログの管理，サービスに関わるログの提供を行います。システム管理者は，サービス提供開始時に提示したサービス内容を超える設定変更には応じません。すなわち，統合サーバ上でサービスを実施していない内容についてのサービスを要求されても提供することはできません。

また，ドメイン内のユーザからの問い合わせについては，システム管理者が直接対応することは行いません。ユーザからの問い合わせについては，ドメイン管理者に対応して頂くか，IT ヘルプデスクをご利用頂くこととなります。

1.3　ドメイン管理者の役割

サービスを受けるドメインの管理者は，サービス開始時に，サービスを実施する上で必要なシステム情報をシステム管理者に提供する責任があります。また，サービスを実施する上で必要なユーザ設定・ユーザ管理・データ管理はすべてドメイン管理者の役割となります。具体的には，以下の通りです。

・サービス開始時に，システム管理者が要求する既存のサーバの設定情報及びデータを提供して頂きます。具体的には，既存サーバのソフトウェアのバージョン，サーバのデータ（例えば，メールを移行する際のメールデータ，DNS を移行する際のゾーンファイル等）を提供して頂く必要があります。
・サービス開始時及びサービス開始後のユーザ設定（新規作成・削除等），ユーザ管理（ファイル容量の上限設定，利用ファイル量の監視[1]等）はドメイン管理者の責任で行って頂きます。具体例としては，メールサービスの開始時には統合サーバ上で新規ユーザ作成が必要となりますが，その際に必要なユーザの名古屋大学 ID の収集はドメイン管理者の責任において実施して頂きます。また，すべてのユーザ投入・メールエリアスの設定・メーリングリストの設定等はドメイン管理者の責任において実施して頂きます。
・サービス開始時及びサービス開始後のデータ投入。ウェブサーバのデータ投入，DHCP，DNS のデータ投入はドメイン管理者の責任において実施して頂きます。
・サービス開始後のユーザからのメール配送などに関する問い合わせのために必要となるログ分析は，ドメイン管理者の責任で実施して頂きます。

すなわち，統合サーバ管理者は，各ドメインのデータの投入・削除に関しては，一切の責任を持ちません。

また，サービスを実施する上でのトラブルの初期対応はドメイン管理者に責任があります。具体的には，メールの送受信・ウェブへのアクセス・DNS 及び DHCP 設定の不具合の初期対応はドメイン管理者に行って頂きます。そのために必要なログは自動的に提供されます。システム管理者は，これらのトラブル解決におけるご相談に応じます。

ウェブサーバ・メーリングリストソフトウェアについては，ドメインごとに，その設定の軽微な変更を行うことができます。しかし，設定変更に伴うすべての責任はドメイン管理者に帰着します。

2．統合サーバのサービス内容

統合サーバがサービスする内容及び対象は以下の通りです。

・メールサーバ
・ウェブサーバ
・DNS サーバ
・DHCP サーバ
・ファイルサーバ

メール・ウェブ・DNS については，`nagoya-u.ac.jp` のサブドメインを対象とし，ドメインごとにサービスを行います。したがって，「`xxx.yyy.nagoya-u.ac.jp` のメールサーバ」のみ

1　ユーザのファイル利用量のデータは，必要があればシステム管理者からドメイン管理者に提供することが可能です。システム管理者は，ユーザファイル利用量を監視し，極端な利用が行われている場合には，ドメイン管理者に警告を行う場合があります。

を統合サーバを利用するといった利用法が可能です。また，DHCP については，現在の NICE の構成上「建物単位（サブネット）」でのサービスとなります。

以下では，各サービスのサービス内容について詳細を解説します。

2.1 ユーザ認証

電子メール及びウェブサーバの個人ページ，ファイルサーバ等の利用には，ユーザの認証が必要となります。統合サーバでは，ユーザアカウント作成の基本に名古屋大学 ID を利用する一方で，電子メールアドレス `userid@XXXX.nagoya-u.ac.jp` 及び，ウェブの個人ページ `http://www.XXXX.nagoya-u.ac.jp/~userid` などで利用される `userid` の部分を各ドメインで自由に設定可能なユーザ認証体系を利用しています。

- メールサーバまたはウェブサーバを統合サーバ上で利用する各ドメインごとに「ユーザ名」は独立に指定可能です。
- メールサーバにアクセスする，ウェブサーバにデータをアップロードする等のシステムを利用する際のユーザ ID は，`userid@XXXX.nagoya-u.ac.jp` の形の ID を利用します。
- 上記ユーザ ID のパスワードは，名古屋大学 ID のパスワードと同期します。

通常は，`userid` の部分のみをユーザ ID としますが，統合サーバでは，異なるドメインで同一の `userid` を持つユーザが存在する可能性があるため，`@XXXX.nagoya-u.ac.jp` の部分もユーザ ID の一部と考えています。また，そのユーザの ID 作成時に名古屋大学 ID を指定した場合（これが標準です）には，ユーザが名古屋大学 ID のパスワードを変更した際には，統合サーバのユーザ ID のパスワードも同一のものに変更されます。このような認証体系を利用することによって，統合サーバではドメインごとの運用の可用性を保証しています。なお，すべてのユーザが名古屋大学 ID を持つことを要求しているわけではなく，名古屋大学 ID とは無関係なユーザ ID を設定することは可能ですが，システム管理者はこれを推奨していません[2, 3]。

2.2 メールサーバ

基本的な考え方は，各ドメイン（部局・専攻・研究室等）で運用している電子メールサーバを統合サーバ上で実現することを目的としています。統合サーバのメールシステムは，利用者の利便性とセキュリティを考慮した結果，サーバへのアクセスは以下の条件を課しています。

メール受信

- imap over SSL または pop3 over SSL のみしか利用できません。ただし，システム管理者は imap over SSL の利用を推奨します。
- インターネット上どこからでもアクセス可能です。
- ウェブメールの利用が可能です。

2　名古屋大学 ID の考え方では，名古屋大学構成員または，以前に名古屋大学の構成員であった方，名古屋大学内で情報システムを利用しようとする方は，すべて名古屋大学 ID を所有していると考えています。したがって，「名古屋大学 ID と無関係な ID」の代表例として複数人が共有する ID が考えられます。複数人が共有する ID は，セキュリティ低下の原因となりますので，そのような利用法は極力避けるべきと考えます。

3　一つの名古屋大学 ID に対して複数の統合サーバ上の ID を作成することは可能です。

メール送信

・送信時の認証（SMTP-AUTH）を必要とします。

・送信時には smtpd over SSL または submission with TLS の利用が必要です。

・インターネット上どこからでもアクセス可能です。

メール受信に関しては，標準的な 2 種類のプロトコル（imap と pop3）を採用していますが，ネットワーク上にユーザ ID 及びパスワードが流れるため，その通信を暗号化する必要があります。そのため，imap 及び pop3 ともに SSL による暗号化通信を要求しています。

メール送信において「送信時認証」を採用するメールサーバは必ずしも多くはないのですが，送信時認証を採用しない場合には，メールの不正中継（spam メールの発信）を避けるため，学内からの利用に限定するなどの制限を必要とする場合が多いと考えられます。今回，統合サーバでは，送信時認証を採用することにより，正当なユーザであるかぎりは，インターネット上のどこからでもメール送信を可能になるように設定しました。この場合も，ユーザ ID とパスワードの流出を防ぐため，通信の暗号化が必要となり，そのため smtpd over SSL または submission with TLS を要求しています。

これらの送受信設定は，近年のメールソフトウェアではサポートされている例が多いのですが，一部のフリーウェアまたは古いソフトウェアではサポートされていない例もあります。メールソフトウェアの対応状況及びそれらの設定方法については，情報連携統括本部のページ［6］をご覧ください。

また，一人あたりのメールの保存量の上限は統合サーバのシステムとしては定めておらず，必要であれば，各ドメインごとに上限（quota）を設定可能となっています。

一方，近年非常に多くなってきている「迷惑メール」の対策については，現行のメールサーバでの運用をそのまま引き継ぎます。すなわち，統合サーバ独自の対策を取るのではなく，名古屋大学の Mail Gate における Virus チェックと spam フィルタを利用します。

その他の電子メールに関連するサービスとして，統合サーバでは，メールエリアスと GNU Mailman によるメーリングリストをサポートしています[4]。これらはともにドメインごとに自由に設定可能です。他のメーリングリストソフトウェアの利用は，現時点ではサポートしていません。

2.3　ウェブサーバ

ウェブサーバについても，各ドメインで運用している（1 台の）ウェブサーバを統合サーバ上で運用することを目的としています。しかしながら，ウェブについては，CGI などを始めとする動的なページの運用方法が複数のドメインの間で衝突する可能性があるため，現時点ではサービスに制限を設けています。制限の詳細については後述します。

ウェブサーバについては，通常のページのほか，ユーザの個人ページ及び複数のユーザによる

4　GNU Mailman の基本機能である，メーリングリストのメールの保存及び Web による閲覧もサポートしていますが，標準設定では，Web による閲覧機能は無効（private モード）になっています。

グループのページの利用も可能です。ユーザの個人ページへのデータ投入は，メールサーバへのアクセスと同様なユーザ認証を経て scp（ssh によるリモートコピー）を利用してアクセスします。また，「グループ」はメールサーバにおける「エリアス」と同時に実現し，該当のグループに属するユーザは，各個人のユーザ ID とパスワードを利用した認証を経て，scp によってデータ投入を行うことが可能です[5]。なお，ウェブサーバへのデータ投入のための scp アクセスは，インターネット上のどこからでもアクセス可能ですが，DNS 逆引きが可能なホストからのアクセスに限られます[6]。

2.4 DNS サーバ

DNS サーバについては，管理者レベルのサービスであり，一般ユーザが関係する内容ではありません。しかし，DNS サーバを確実に運用することが電子メールの到達性などを保証する根拠となるため，ネットワーク的には極めて重要なサービスです。

DNS サーバを統合サーバで運用する際には，各ドメインの「正引き」ゾーンだけでなく，移行対象の DNS サーバが「逆引き」ゾーンを提供している場合には，それも同時に運用を行うことが必要です。また，`nagoya-u.ac.jp` 直下のサブドメインの場合（`XXXX.nagoya-u.ac.jp` の場合）には，従来の NICE の運用方針を継承し，secondary DNS server は `nu104.nagoya-u.ac.jp`（名古屋大学の primary DNS サーバ）が行うように設定できます。すなわち，従来の各ドメインで運用していた DNS サーバの機能のすべてを移行可能となっています。

DNS サーバの設定は，初心者には極めて面倒なものですので，後述する「管理用 GUI」を用意し，統合サーバ移行後に DNS のゾーンデータの管理が容易になるように工夫されています。

2.5 DHCP サーバ

DHCP サーバは，本来は「ドメイン」とは無関係にサブネットごとに実施されるサービスであり，通常はサービスを行うサブネット内に DHCP サーバを設置します。統合サーバでの DHCP サービスは，建物内に流れる DHCP による IP アドレス割り当て要求をルータによって統合サーバまでリレーすることによって実現していますので，サブネットごと（建物ごと）に DHCP サービスを実施することとなります。

統合サーバの DHCP サービスでは「MAC アドレスによる制限つきの静的または動的アドレス割り当て」を行うことを基本方針としています。すなわち，各 DHCP ドメイン（DHCP サービスを行うサブネット）ごとに，アドレス割り当てを許可するホストの MAC アドレスを登録し，登録されているホストにのみ静的または動的にアドレス割り当てを行います。この場合，登録されていないホストからのアドレス割り当て要求は拒否されます。DHCP サーバのアドレス割り当て及び MAC アドレス設定も「管理用 GUI」を通じて行うことができます。

なお，DHCP サービスに関わる注意点は以下の 2 点です。

5　「グループ」を定義すると，自動的にそのメンバーに対する「メールエリアス」を作成することとなります。また，「メールエリアス」を設定すると，自動的にそのメンバーに対する「グループ」が作成されます。

6　学内であっても，逆引き不可能なホストからのアクセスは認めていません。

・DHCP サービスを行う対象となるアドレスは，原則として，NICE のアドレスに限ります。NICE 上に論理的に Local Private アドレス空間を利用している場合には，その空間に対して DHCP サービスを行いたい場合にはシステム管理者にご相談ください。
・Local Private アドレス空間を利用する場合には，Secure NICE のサービスの一環として DHCP を利用することも可能です。Secure NICE については［4］をご覧ください。

2.6　ファイルサーバ

統合サーバではウェブサーバのサービスの一環として WebDAV によるファイルサーバの提供も可能です。WebDAV とはウェブの技術（https によるアクセス）とユーザ認証を組合せ，ファイルサーバを実現する技術です。

WebDAV は，ユーザ認証を経て個人またはグループのファイルフォルダにアクセス可能になります。WebDAV を利用したネットワークファイルサーバは“.Mac”などで広く利用されている技術であり，統合サーバの WebDAV サーバに対しては，SSL を利用したアクセスを行うため，インターネット上のどこからでもアクセス可能なファイルサーバを実現しています。Windows ファイル共有及び AppleShare ファイル共有の機能を提供する予定はありません。

なお，WebDAV によるファイル共有を行う場合に，ファイル利用量には上限を設定することが必要となりますが，システム構成の制限により，「ユーザあたり」の制限ではなく，「ドメイン内の全ユーザの総ファイル容量」に対する制限となることを御理解ください。

3．統合サーバのサービスの制限

前節でも述べた通り，統合サーバでは，それぞれのサービスに対して多少の利用形態の制限があります。この制限は，同一システム上で複数ドメインに対するサービスを実施する上で，サービスの衝突を防ぐための制限です。なお，今後，この制限を超えるサービスを（一部）実施するために，現行の統合サーバとは別に「拡張統合サーバ」のサービスを実施する計画もありますので，この制限を超えるサービスを希望されるドメインの方は，情報連携統括本部にご相談ください。

★全サービスに対する制限

・nagoya-u.ac.jp 以外のドメインに対するサービスは実施できません。

★メールサービスに対する制限

・メーリングリストソフトウェアは GNU Mailman 以外のものは利用できません。
・procmail 等のフィルタリングソフトウェアは利用できません。統合サーバでは sieve を利用したフィルタリングが利用可能です。

★ウェブサービスに対する制限

・動的なページはサポートできません。ただし，簡易な CGI/SSI は，ファイル書き込みを伴わないものに関しては，ドメイン管理者及びシステム管理者の許可の下で利用可能です。
・ウェブサーバ上で Java，データベース，CMS 等のアプリケーションは利用できません。

★ DHCP サービスに関する制限

・Local Private 空間に対する DHCP による IP アドレスの提供は困難な場合があります。

4．統合サーバの利用について

統合サーバの利用を希望されるドメインの方は，情報連携統括本部情報戦略室にお問い合わせください。なお，統合サーバを利用する際には，利用ドメインごとに費用負担をお願いしています。負担して頂く費用については，情報連携統括本部の統合サーバのページ [5] をご覧ください。なお，統合サーバのサービス料金は，統合サーバのシステム更新・増強のために利用します。

また，統合サーバは「学内ドメイン」に対するサービスですので，「個人的にウェブサーバを立ち上げたい」などの個人的なサービスは行いません。

Ⅱ．統合サーバへの移行の方法と例

統合サーバは，2007 年秋には稼動を開始し，すでにいくつかのドメインに対してのサービスを実施しています。2008 年 3 月末現在で，統合サーバ上で稼動しているサービスは以下の通りです。

・電子メールサーバ
- icts.nagoya-u.ac.jp：情報連携統括本部
- tokyo-office.sat.nagoya-u.ac.jp：本部東京事務所
- rep.provost.nagoya-u.ac.jp：本部研究推進室
- *.mbox.nagoya-u.ac.jp：全学メールサービス
- law.nagoya-u.ac.jp：法学研究科
- lit.nagoya-u.ac.jp：文学研究科

・ウェブサーバ
- icts.nagoya-u.ac.jp：情報連携統括本部
- law.nagoya-u.ac.jp：法学研究科
- lit.nagoya-u.ac.jp：文学研究科

・DNS サーバ
- icts.nagoya-u.ac.jp：情報連携統括本部
- sat.nagoya-u.ac.jp：総務部学外連絡所ドメイン
- tokyo-office.sat.nagoya-u.ac.jp：本部東京事務所
- rep.provost.nagoya-u.ac.jp：本部研究推進室
- *.mbox.nagoya-u.ac.jp：全学メールサービス
- law.nagoya-u.ac.jp：法学研究科
- lit.nagoya-u.ac.jp：文学研究科
- educa.nagoya-u.ac.jp：教育発達学研究科

・DHCP サーバ
- 133.6.154/23：法学研究科
- 133.6.36/23：文学研究科

以下では，実際にこれらのサービスを統合サーバで実施する手順を解説します。いずれの場合

も，既存のドメインでそれらのサービスを実施していることを前提としています。また，いずれの場合も，実際のサーバ移行の手順よりも，事前調査に時間を必要とします。十分な事前調査を行っておけば，実際のサーバ移行は比較的容易に行うことが可能です。

1．電子メールサーバの移行手順

ステップ１：データ移行の調査

電子メールサーバの移行には，次の２パターンが考えられます。

- 既存の電子メールサーバを完全に停止し，既存サーバ上のデータも統合サーバに移行する場合。
- 既存の電子メールサーバは「読み出し専用」として運用を行い，既存サーバ上のデータは移行しない場合。

前者の場合には，既存サーバで利用しているメールソフトウェア及び電子メールの保存形式をご連絡いただきます。これは，電子メールのサーバソフトウェアは，ソフトウェアごとにメール保存形式が異なるため，統合サーバのメール保存形式への変換が可能か否かの検証を行うために必要なステップです。場合によっては，メール保存形式の変換の検証にある程度の時間を頂く場合があります。

後者の方法とは，既存の電子メールサーバは既存データの保存用としてのみ用いる方法ですので，データの移行を伴わないため，このステップを省略することが可能です。

ステップ２：メールアカウント作成とエリアスの移行

新規電子メールサーバを利用するユーザのメールアカウントを作成します。原則として，統合サーバ上のメールアカウントは名古屋大学 ID に対応したものとなりますので，ユーザの名古屋大学 ID を収集し，メールアカウントを作成します。また，既存サーバに設定されているメールエリアスを統合サーバ上に設定します。なお，既存サーバ上の各ユーザのメール転送設定も，メールアカウント設定後に統合サーバ上に設定します。

これらの作業はドメイン管理者に行って頂きますが，統合サーバ担当者がお手伝いすることも可能です。

ステップ３：メーリングリストの移行

既存サーバにメーリングリストが設定されている場合には，統合サーバに新規にメーリングリストを作成して頂きます。

ステップ４：統合サーバへの移行

上記ステップが終了すると，統合サーバ上で電子メールを運用することが可能となります。最初に，既存サーバでのメール着信を停止し，データ移行を行う場合には，サーバ上のデータを統合サーバ上に展開します。その後，DNS 設定を変更し，統合サーバでのメールサーバソフトウェアを起動します。このステップに要する時間は，データ移行を行う時間を除いて，メールの送受信テストを含めて１時間程度となります。

なお，電子メールの移行に際しては，ユーザのメールソフトウェアの設定変更を必要とします。

メールソフトウェアによっては，設定変更が面倒なものもありますので，事前にユーザの利用環境に応じたアナウンスを十分に行っておく必要があります。

2．ウェブサーバの移行手順

ステップ１：データ移行の調査

サービスの紹介でも書いた通り，統合サーバのウェブサービスでは，動的なページをサポートすることが困難です。したがって，最初に既存ウェブページ内に動的なページが含まれるか否かを調査することが必要となります。

ステップ２：データの移行

既存サーバに入っているウェブの全データを，個人ページのデータ等も含めて，統合サーバに投入します。その後，統合サーバで正しくデータを表示できるかを調査します。

ステップ３：統合サーバへの移行

上記ステップが終了すると，統合サーバ上でウェブサーバを運用することが可能となります。最初に，既存サーバを停止し，その後，DNS 設定を変更し，統合サーバでのウェブサーバソフトウェアを起動します。このステップに要する時間は，テストを含めて 20 分程度となります。

3．DNS サーバの移行手順

DNS サーバの移行は，ユーザとは無関係に行うことができるため，極めて簡単です。

ステップ１：データ移行の調査

既存 DNS サーバでサービスを行っているゾーンデータを統合サーバ管理者にお送り頂きます。統合サーバ管理者は，頂いたゾーンデータを「ドメイン管理 GUI」のデータとして投入します。その後，「ドメイン管理 GUI」が動作する統合サーバ上の IP アドレスを，既存 DNS サーバに登録して頂きます[7]。

ステップ２：データの確認

ドメイン管理者の方に「ドメイン管理 GUI」にアクセスして頂き，ゾーンデータが正しいことを確認して頂きます。

ステップ３：統合サーバへの移行

上記ステップが終了すると，統合サーバ上の DNS サーバを起動し，その上位ドメイン管理者に DNS サーバの IP アドレスを変更してもらうことにより，DNS サーバの移行が完了します。このステップに要する時間は，テストを含めて 20 分程度となります。

なお，ドメイン内のユーザのコンピュータが DNS サーバとして既存サーバを参照するように設定されている場合も少なくありません[8]。そのようなコンピュータに対しては，DNS サーバの

7　この手順により，「ドメイン管理 GUI」を利用して頂くことが可能になります。

8　最近は DHCP サーバから DNS サーバの IP アドレスを渡している場合が多いため，「手で」DNS サーバを指定しているものは必ずしも多くありませんが。

IP アドレスを変更して頂く必要があります。なお，統合サーバでは「DNS キャッシュサーバ」も運用していますので，統合サーバでの「DNS キャッシュサーバ」を，パソコン等の DNS サーバとして設定して頂くのがよいと考えます。

4．DHCP サーバの移行手順

DHCP サーバの移行も，ユーザとはある程度無関係に行うことが可能ですが，既存サーバ上で「アドレス動的割り当て」を行っている場合には，対象の全機器を停止する必要が生じます。

ステップ 1：データ移行の調査

既存 DHCP サーバでサービスを行っている configuration データを統合サーバ管理者にお送り頂きます。

ステップ 2：データの確認

ドメイン管理者の方に「ドメイン管理 GUI」にアクセスして頂き，configuration データが正しいことを確認して頂きます。このステップで，統合サーバ上の DHCP サーバにデータを登録します。

ステップ 3：統合サーバへの移行

統合サーバで稼働中の DHCP サーバを利用するためには，各サブネットのルータ（NICE で管理されているルータ）の設定変更が必要となります。設定変更を行う直前には，サブネット内のすべての DHCP サーバを停止させる必要があります。なお，「アドレス動的割り当て」を行っている場合には，既存サーバの「リースファイル（lease file）」を統合サーバにコピーするか，動的割り当てによって IP アドレスを取得している機器をすべて停止する必要があります。統合サーバ管理者は後者の方法を推奨します。

これらの準備が終了した段階で，サブネットのルータの設定変更を行い，DHCP サーバの移行が終了します。

5．統合サーバの管理 GUI

統合サーバでは，ドメイン管理者が利用する「管理 GUI」を用意しています。管理 GUI では，

- ユーザの新規作成（cf. 図 2）・削除・ディスク使用量表示（cf. 図 3）（メール，ウェブサーバ運用に必要）
- グループ（メールエリアス）の作成・変更・削除（cf. 図 4）（メール，ウェブサーバ運用に必要）
- DNS ゾーン設定（cf. 図 2.5）
- DHCP サーバ設定

を行うことが可能です。なお，「DNS ゾーン設定」，「DHCP サーバ設定」では，GUI を利用した形式の他に，それぞれ，ゾーンファイルや DHCP configuration ファイルをドメイン管理者が作成し，それを upload する形式での利用も可能です。

管理 GUI は，名古屋大学 ID による認証を経て利用する形式を取り，管理者以外がアクセスすることはできないようになっています。

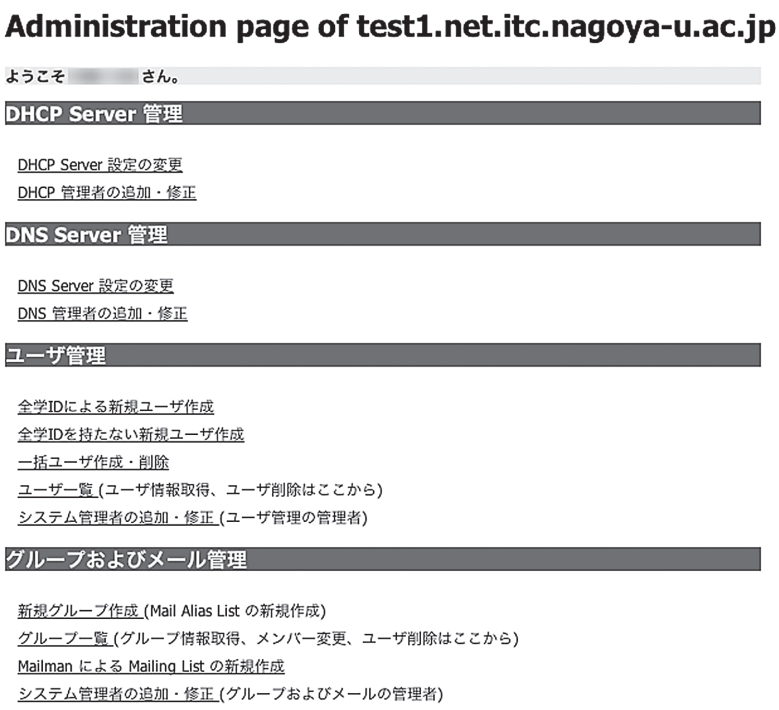

図１　管理 GUI top ページ

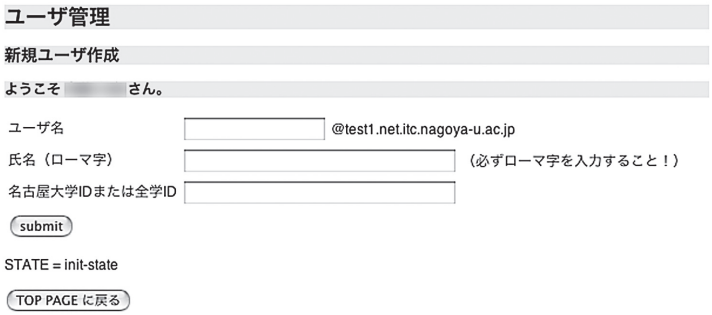

図２　新規ユーザ作成ページ

Ⅲ．統合サーバに関する技術内容

最後に，統合サーバの技術内容について解説を述べておきます。

１．統合サーバのハードウェア構成

統合サーバは，１台の高速かつ大容量なホストで構成されているのではなく，複数台のホストを組合せたクラスタを用いて実現しています。また，ディスクストレージもファイバチャネルネットワークを用いたストレージエリアネットワーク（SAN）を用いて，複数台の大規模スト

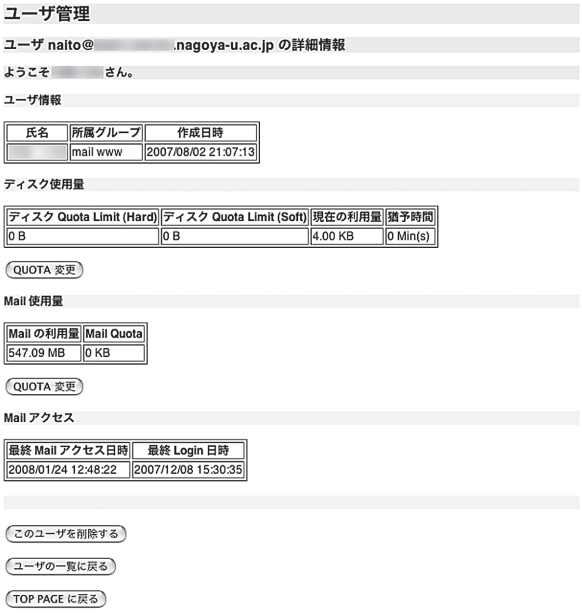

図３　ユーザ情報ページ

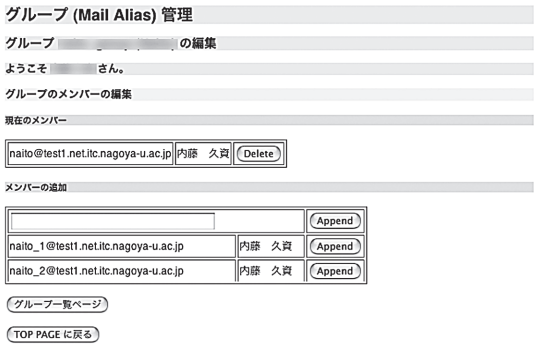

図４　グループ（メールエリアス）作成ページ

レージへの同時アクセスを利用しています。このような構成を行うことにより，サービス対象の増加に対して，ホスト及びディスクの増設が容易になり，スケーラブルな対応が可能になるばかりか，ソフトウェアアップデート，ホストの障害時にサービスを行うホストを切り替えることにより，ダウンタイムを最小限にすることが可能となりました。

2008 年 3 月末現在での具体的なハードウェア構成は以下の通りです。

★サーバホスト　Apple Xserve（CPU: Intel Xeon dual core 2.0GHz × 2，2GB Memory）with Apple MacOSX Server を 6 台利用し，これらのうち，2 台をディスク装置コントロールホスト，4 台をサービスを行うホストとして設定しています（cf. 図 6）。

★サーバディスク間接続　2Gb/s ファイバチャネルネットワークで接続し，Apple XSan ソフト

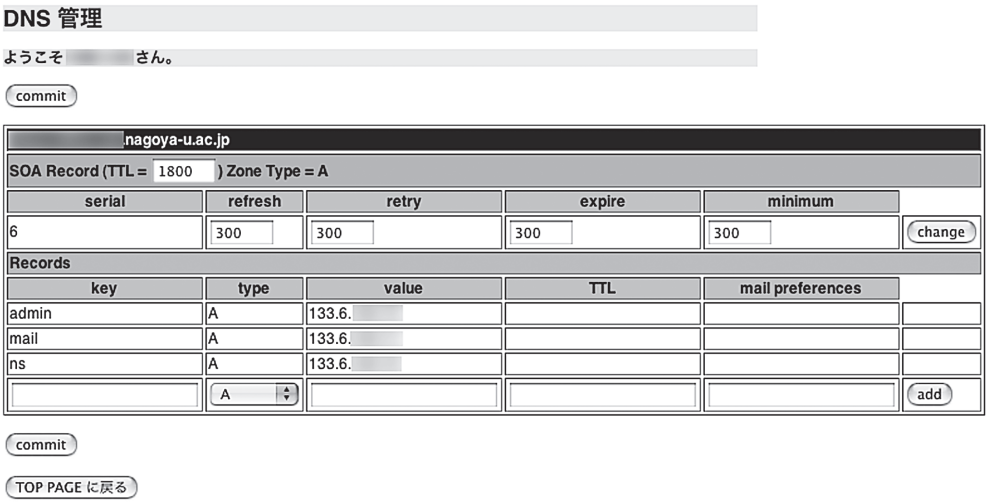

図５　DNS ゾーンデータ管理ページ

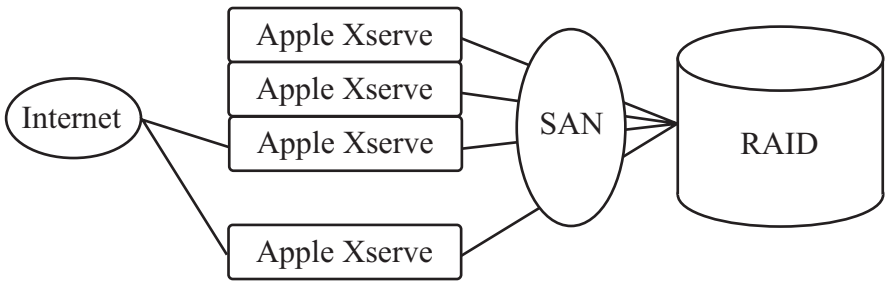

図６　サーバ構成

ウェアを利用した SAN を構成しています。

★ディスク装置　有効ディスク容量 8.3TB. Apple Xserve RAID × 2 で構成しています。これ以外にバックアップ用ディスクシステムを利用しています。

一般には，複数台のホストから単一のディスクに対して，同時に読み書きを行うことはできません。通常, そのようなことを実現するためには, 1 台のホストをディスクサーバとして設定し, ディスクサーバを経由したアクセス（NFS）を行うか，Network Attached Storage（NAS）を利用する方法が広く用いられてきました。しかし，NFS では極めて高速なディスクサーバを用意しない限り，ディスク I/O のボトルネックが発生します。また，NAS は，単一のデバイスですので, 稼働後にディスク増設が容易ではありません。統合サーバでは, 近年大規模データベースサーバなどで用いられる，ストレージエリアネットワーク（SAN）を用いることにより，複数台のホストから単一ディスク装置への同時アクセスを実現することが可能になりました。SAN においても，複数台からのディスク I/O を“SAN コントローラホスト”が制御しているため，コントローラホストの能力がボトルネックとなる可能性もありますが，NFS と比較して，高速なディ

スク I/O を実現することができます。また，SAN では，ディスク装置を後から追加することが容易であり，ホストから見たときには，ディスク装置全体を単一のデバイスとみなすことが可能です。

2．統合サーバのソフトウェア構成

統合サーバでは，オペレーティングシステムとして Apple MacOSX Server を利用し，サービスを実施するソフトウェアとして，MacOSX Server にバンドルされているものを利用しています。バンドルソフトウェアを利用することにより，OS のソフトウェアアップデートと同時にサービスを実施するソフトウェアのアップデートが可能となり，システムメンテナンスの人的負荷を軽減することができました。

具体的に利用しているソフトウェアは以下の通りです。

メールソフトウェア　postfix（version 2.1.5）及び cyrus imap（version 2.2.10）
ウェブサーバソフトウェア　apache（version 1.3.33）
DNS サーバソフトウェア　ISC bind（version 9.2.2）
DHCP サーバソフトウェア　ISC dhcpd（version 3.0.5）

ただし，ISC dhcpd は MacOS X Server の bundle version ではないものを利用しています。

3．統合サーバでのサービスの仕組み

ハードウェア構成で述べた通り，統合サーバは複数台のサービス実施ホストを利用しています。ここでは，これらをどのように利用してサービスを行っているかを，具体的な例を挙げて解説します。

例えば，全学メールサービスは，2008 年 4 月現在では，`a.mbox.nagoya-u.ac.jp` から `h.mbox.nagoya-u.ac.jp` の 8 個のサブドメインを用いて運用しています。すなわち，これら 8 個のサブドメインを 8 つのメールサーバを用いてサービスしていることとなります[9]。統合サーバでは，これら 8 つのメールサーバに対して，それぞれ別の IP アドレスを与え，4 台のホストにそれら 8 つの IP アドレスを「仮想アドレス」として割り当てます。また，各メールサーバソフトウェアは，指定の IP アドレス上でのみ LISTEN を行うように設定してあります。一方では，SAN を用いて，メールのデータ及び設定ファイル等が格納されているディスクは，どのホストからでもアクセス可能となっています。

この方法であれば，4 台のホストのうち 1 台が停止する事態が発生しても，仮想アドレスを他のホストに割り当て直して，該当するドメインのサーバソフトウェアを新ホスト上で起動するこ

9　その気になれば，1 つのメールサーバ（ソフトウェア）で運用可能かもしれませんが……

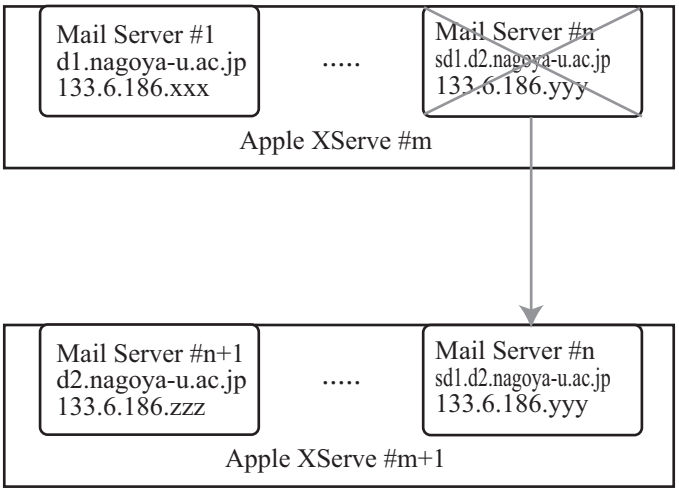

図７　サービス割り当ての変更

とにより，最短のダウンタイムの間にサービスを再開することが可能になっています（cf. 図 7）。

４．統合サーバの認証体系

統合サーバでは，名古屋大学 ID LDAP サーバで行われている“LDAP Hosting Service”を利用して認証を行っています。統合サーバでは，複数のドメインのサービスを行うため，ドメイン間で「ユーザ ID」の重複を許す ID 体系の利用が必要となりました。そのため，通常利用されている“naito”といった形の識別名ではなく，電子メールアドレス形式（“naito@icts.nagoya-u.ac.jp”）全体を識別名として利用する設定となっています。

Ⅳ．終わりに

サーバの運用コストを考えると，大学内のサーバ運用は集中化の方向を取らざるをえないと考えられます。サーバ運用の集中化を行ったとしても，サーバ運用技術をもった人材の育成を行わなくてもよいというわけではありません。学内に多くのサーバ運用技術をもった人材が配置され，種々のレベルでの管理運用を分担することにより，集中化されたサーバでは運用そのものに重点を置いた仕事を行い，一方では，エンドユーザに近い立場で仕事を行うといった役割分担が成立してサーバの集中化が成功すると考えています。

統合サーバの運用により，従来の各部局・学科・研究室での運用を行ってきた人材を，よりそれぞれのエンドユーザに近い立場での仕事に重点を移して頂くことができます。これは，そのような人材が必要でなくなるのではなく，そのような人たちに，名古屋大学全体としての情報システムの運用にそれぞれの立場で携わって頂きたいと考えているからです。

なお，統合サーバの立ち上げに関しては，情報連携統括本部・情報推進部情報基盤課の川田良文さん，石原正也さんに多くのご協力を頂きました。また，統合サーバ構築の経費として，2007 年度総長裁量経費を利用しました。

参考文献

[1] 梶田将司，平野靖，間瀬健二，名古屋大学 ID の導入について（I）―概要―，名古屋大学情報連携基盤センターニュース，**5**，316−320，（2007）

[2] 梶田将司, 平野靖, 間瀬健二, 名古屋大学 ID の導入について（II）―全学 ID からの移行―，名古屋大学情報連携基盤センターニュース，**6**，140−145，（2007）

[3] 梶田将司，平野靖，間瀬健二，名古屋大学 ID の導入について（III）―将来構想―，名古屋大学情報連携基盤センターニュース，**7**，11−17，（2008）

[4] 八槙博史，Secure NICE の運用開始，名古屋大学情報連携基盤センターニュース，**6**，349.353，（2007）

[5] 名古屋大学情報連携統括本部，統合サーバ，
http://www.icts.nagoya-u.ac.jp/service/unified-server/

[6] 名古屋大学情報連携統括本部，統合サーバメール設定，
http://www.icts.nagoya-u.ac.jp/service/mbox/setting.html

（ないとう　ひさし：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）

（やまぐち　ゆきこ：名古屋大学情報連携基盤センター）