TYCOON統合認証システムの仮想化による構築とその概要

森河良太[1]，倉田香織[2]，宮川毅[1,2]，小杉義幸[2]，土橋朗[2]

1．インターネットにおける「識別」と「認証」の違い

インターネットに接続されるコンピュータ端末とそれを操作する人間は，単にハードウェアとソフトウェアといった違いだけでは説明できない大きな差異がある．しかもその差異は時として混同され，逆転することさえある．それ故にサイバー時代の只中にある現代社会では，そのことを根本原因とした様々な問題や事件が発生してる．その中で常に問われることが「あなたは誰？」ということであり，それをサポートする舞台装置が「**ユーザ認証**」なのである．

インターネット（Internet）とは，狭義にはTCP/IPという通信プロトコル（通信手順）に基づいたコンピュータネットワーク間のネットワークと定義される．このことは，特定の集中した責任主体が存在しないというインターネットの歴史的発展経緯からも適切な定義と言えるだろう．しかしながらコンピュータ端末をインターネットへ自由に接続して通信を行えるかと言えば，必ずしもそうではない．少なくともコンピュータ端末には，接続するネットワークの設定に応じた「IPアドレス」と呼ばれる固有の番号を割り当てなければ，データ通信を行うことはできない．それは排他的・防御的な目的からではなく，オーソドックスな手紙や電話のやり取りにおいて住所や電話番号が必要であるように，端末間のデータのやり取りのための技術的要請である．事実，コンピュータ端末の接続と分離を頻繁に行うようなネットワークや一般家庭におけるLAN(Local Area Network）では，DHCP（Dynamic Host Configuration Protocol）と呼ばれる，端末にIPアドレス等のネットワーク情報を自動で割り当てるサービスが稼働している．すなわちコンピュータ端末に対してIPアドレスがテンポラリ（一時的）に割り当てられたとしても，TCP/IPという約束に沿ってデータ通信を行いさえすれば，何の障害も発生しないということである．すなわちIPアドレスは，コンピュータ端末を「**識別**」するための「一般的な特徴」と考えられる．

それではインターネットに接続された端末を操作して利用する人間（ユーザ）の場合はどうであろうか．ユーザは様々な目的を達成するために，「**意志**」に従ってコンピュータ端末を操作している．そしてその操作によって生まれた「新しい情報」に対して，創作者であるユーザは「**所有権**」を主張することができるし，逆にそれに対する責任を認めなければならない状況が生じうる．それらのことを証明するために，その操作の主体が自分自身であることの証（あかし），すなわち「**認証**」が必要となってくる．この点が，単にインターネットに接続された機械的端末における「**識別**」との違いである．

[1] 生命科学部コンピュータ委員会
[2] 情報教育研究センター

2015年10月，本学では学内ネットワーク（TYCOON）[1]に接続された多くのサーバにおける「**ユーザ認証**」を一手に引き受ける「**統合認証システム**」が更新された．以下，そのシステムの技術的内容の概略を説明し，最後にインターネットにおける「**認証**」の在り方について，簡単に考察したいと思う．

2．TYCOONにおける認証システムの発展

2-1. /etc/passwdとNISによるユーザ認証の時代（1992年～2004年）

2015年の本学統合認証システム（TYCOON統合認証システム）の話に入る前に，本学TYCOONにおけるユーザ認証の歴史について少し述べたい．本学では1992年10月，薬学部の4研究室を中心とした学内LANにおいて，UNIX系OSを搭載したSilicon Graphics社製のワークステーションが導入された．このサーバにログインするための手続きが，本学ネットワークにおける最初の「ユーザ認証」である．その後，研究3号館（生命科学部）においてWIDEインターネットとのTCP/IP接続（1994年9月）が行われたことを契機に，TYCOONと命名された学内ネットワークは急速に成長し，1997年8月には医療薬学研究棟のネットワークセンターを中心とした4つの研究棟と図書館棟，厚生棟，そして教育2号館のコンピュータ端末室を結ぶ全学的LAN回線網に拡大した．またTYCOONに接続していた約850台のパソコン端末では，電子メールの送受信やWebサーバへの自作コンテンツの公開，MEDLINEによる文献検索，そして電話回線による学外からTYCOONへの接続（PRAMS）等が頻繁に行われており，それぞれのサービスは学内に設置された15台強のサーバによって提供され，そのうち10台ほどのサーバにおいて**ユーザ名**と**パスワード**を用いたユーザ認証が行われていた．

UNIX系OSにおける基本的なユーザ認証は，etcと呼ばれるディレクトリに置かれたpasswdというファイルを参照して行われている（**/etc/passwd** と書く）．このファイルの中には，OSへのログインのためのユーザ名と暗号化されたパスワードの他に，ユーザを表す数字（ユーザ番号），所属するグループを表す数字（グループ番号），ユーザ名に該当する人の氏名やホームディレクトリなどが記載されている（現在はセキュリティの向上のため，パスワード情報については別ファイルに分散配置されている）．つまり認証の必要なサーバが10台あれば，少なくとも10個の/etc/passwdファイルの作成が必要となる．サーバ管理者にとって，このファイルにおけるユーザの追加や削除，編集は，大変面倒な作業である．そこで/etc/passwdと同等の情報をサーバ間で共有するサービスであるNIS（Network Information Service）を，PS（薬学部），LS（生命科学部），BUS（事務局）の各ドメインのメールサーバにおいて立ち上げ，ドメイン内におけるファイルサーバやメールサーバのユーザ管理を一元化した．このようにNISは，各ドメインのユーザ管理者の負担を軽減させることに大いに貢献した．

2-2. ディレクトリサービスの導入（2004年～2010年）

しかしながらドメイン横断的にユーザ情報を大規模管理することは，NISの基本仕様では荷が

重く，またUNIX以外のOSやサーバアプリケーションとの連携についても，それらはNISにおいて十分にサポートしていない．TYCOONを管理運営していたネットワーク運営委員会（現・情報教育研究センター）でも，2003年頃から拡大するマルチプラットホーム環境でのユーザ管理の方法について議論が行われるようになり，中でもLDAP(Lightweight Directory Access Protocol)がクローズアップされるようになった．

LDAPはディレクトリサービスに接続するための通信プロトコルであり，先行して設計されていたDAP（Directory Access Protocol）をTCP/IPによるインターネット通信のために軽量化したものである．ディレクトリサービスとは，/etc/passwdやNISで扱っていたユーザ情報だけでなく，ユーザのグループ情報や接続端末（ノード）情報を含めた，より広範囲のネットワーク上の資源（リソース）の属性情報を収集，記録，検索できるようにしたサービスである．よって先述のNISもディレクトリサービスの一つであり，LDAPとの情報の互換性はRFC 2307bisによる属性情報の定義をLDAPに追加することで実現する．オープンソースによって提供されるOpen LDAP（あるいは単にLDAP），Apple社のMac OS Xに組み込まれているOpen Directory(OD)，またMicrosoft社のWindowsに対応したActive Directory(AD)などは，ディレクトリサービスを実現する具体的なサーバアプリケーションである．

さてWebメールサービスの導入（当時はGracemailを使用）によるサーバの増加とそれに伴うユーザ管理における負担増，また教育2号館127A番教室（現・2107コンピュータ室）に設置されたiMac端末の利用におけるセキュリティ向上のためのユーザ認証の必要など，TYCOONへのLDAPの導入を後押しする状況は顕著となってきた．そして2004年12月，ODを提供する2台のLDAPサーバ（マスターとレプリカ）がMac OS X Server（筐体はXserve G5）上に構築され，TYCOONに接続されたメールサーバやファイルサーバなど，ユーザ認証を必要とするUNIX系サーバやLMS（Learning Management System:学習管理システム）サーバであるWebClass，そして127A番教室のiMac端末とそのファイルサーバに対してディレクトリサービスを開始した．これにより，本学でドメインを横断する認証システム（TYCOON認証システム）が初めて設置され，その運用が開始された．

TYCOON認証システムはアプリケーションのアップグレードや設定の微調整を受けつつ，その後も順調に稼動した．一方，この時期に流行したWeb 2.0[2]の流れを受け，学内の個別のサーバ管理者からは，自分の管理するサーバとTYCOON認証システムを連携させ，ユーザ管理の負担を軽減したいという依頼を受けるようになった．この結果，UNIX系OSを搭載した基幹サーバ以外にも，Webアプリケーションを含む次のようなネットワークサービスにおけるユーザ認証に対して，TYCOON認証システムは認証サービスを提供するようになった．

1. 医療薬学研究棟設置の無線LANアクセスポイント（2006年2月）
2. PRAMS廃止に伴って設置されたVPN機器（2006年10月）
3. 図書館システム（2007年1月）
4. LMSサーバCodex（2007年2月）

5. 東薬学生ポータル（2008年4月）
6. キャンパスライフ支援システム（2008年9月）
7. TYCOONメールシステムZimbra（2008年9月）

なお当時，2項目のVPN機器はLDAPに対応しておらず，単純な認証サービスのみを提供するRADIUS（Remote Authentication Dial In User Service）による認証のみ有効であった．しかしTYCOON認証システムの基盤となるMac OS X Serverは，Open DirectoryとRADIUSが連携された状態で提供されていたので，認証システムの構築工数を減らすことができ，そのため構築コストも削減された．

2-3. メタディレクトリサービスへの進展（2010年～2015年）

Web 2.0という言葉がクラウド（雲）という新たなバズワードに置き換えられる流れの中で，大学内にも様々なWebサービスが乱立してきた．同時にそれらのユーザ認証に関して，統一性が求められるようになってきた．しかし現実問題として，Windows系サーバなどOpen LDAPを認証プロトコルとして実装できないサーバや認証スイッチングハブなどの基幹ネットワーク機器が，TYCOONから淘汰されることはなかった．一方，日本語表記の氏名や組織内での階層的な所属，電子メールアドレス等，DB（データベース）としての付加価値を認証システムに加えたいという意見も，各ドメインのサーバ管理者から寄せられるようになった．

そこで2010年3月，複数のディレクトリサービスをより上位から統括，管理することのできる統合認証管理システム（メタディレクトリシステム）を新たに導入した．当時，統合認証管理システムとしては，Oracle社のIdentity Managerやエクスジェン・ネットワークス社のLDAP Managerが比較的広く市場に出回っていたが，次の優位性を持つことから，セシオス社のLISM (LDAP Identity Synchronization Manager)が選定された．

- 情報漏洩対策として，非Windows系OS上で動作すること
- 軽量なOpen LDAPをバックエンドDBとしていること
- CUIによる詳細なコマンド操作が可能であること
- 将来への自主的拡張性が確保されているオープンソースであること
- 低価格で導入できること

具体的には次の通りである．LISMはLinuxやBSD等のUNIX系OS上で動作し，Open LDAPをバックエンドDBとして持つメタディクレトリシステムである．よってLDAPは勿論のこと，ODやAD，一般的なRDB，CSV等で管理されている認証情報を自らのディレクトリツリーに取り込んで一元管理することができる．従ってLISM上での認証情報の変更は統括された各ディレクトリサービスに迅速に同期し，その操作内容は監査ログとして記録される．またOpen LDAPのPerlバックエンド上で動作するので，通常のOpen LDAPにアクセスするのと同様に，LDAPクライアントからLISMにアクセスすることができる．よってLDAP Browser/Editor等のLDAP管理用アプリケーションからLISM上の情報にアクセスすることもできる．なおLISMにはSecioss Administrator

と呼ばれるブラウザ表示対応の管理ツールが用意されており，管理者はこのツールを使ってユーザの登録や変更，削除を行うこともできる．勿論，CUI から LISM コマンドを入力することによって，CSV ファイルからユーザ情報一覧を読み込む等，詳細な認証管理を行うことも可能である．さらに LISM では Perl モジュールで作成されたハンドラを呼び出して実行することができるので，管理対象となるシステムに対して必要なスクリプトを実行することができる．実際，この仕様は新規ユーザ作成時に Zimbra メールサーバ[3]において，連携してユーザを作成するというスクリプトで使用されている．

メタディレクトリサービスとして LISM を導入することにより，管理者の人的負担を始めとするシステムの管理コストは大きく減少した．そして将来的に肥大化かつ複雑化すると予想されるユーザ認証の運用に対して，十二分に耐えうる統合認証システムへと発展し，次に挙げる学内システムも次々と統合認証システムに接続された．

8. 2107 コンピュータ室 Window 端末 71 台へのログイン認証（2010 年 4 月）
9. TYCOON 無線 LAN システム（2011 年 1 月～，現在も拡張中）
10. 学生会館における有線 LAN 向け認証スイッチングハブ（2011 年 1 月）
11. 図書館電子リソース学外利用システム EZ-Proxy（2011 年 1 月）
12. 事務系施設における有線 LAN 向け認証スイッチングハブ（2013 年 3 月）
13. 教育 4 号館における有線 LAN 向け認証スイッチングハブ（2013 年 3 月）
14. 東薬調達システム（2014 年 4 月）

この中の項目 8 では，AD 認証による Windows Vista へのログインを行うために，AD サーバと LDAP サーバの連携が必要となった．また項目 9 は Meru 社の無線 LAN コントローラ，項目 10, 12, 13 は日立電線の認証スイッチングハブ Apresia を用いて構築されているため，それらの機器は RADIUS による認証のみ対応していた．しかし LISM を中心として構築された本学の統合認証システムでは，それら複数の認証プロトコルと連携・吸収し，それらを一元管理することができた．

このように異なるユーザ認証方法を持つネットワーク機器を同一組織内の LAN に複数接続せざるを得ない状況は，ICT 社会の至る所で生じていた．よってメタディレクトリを配置して運用することは，組織内 LAN における標準仕様となりつつある．

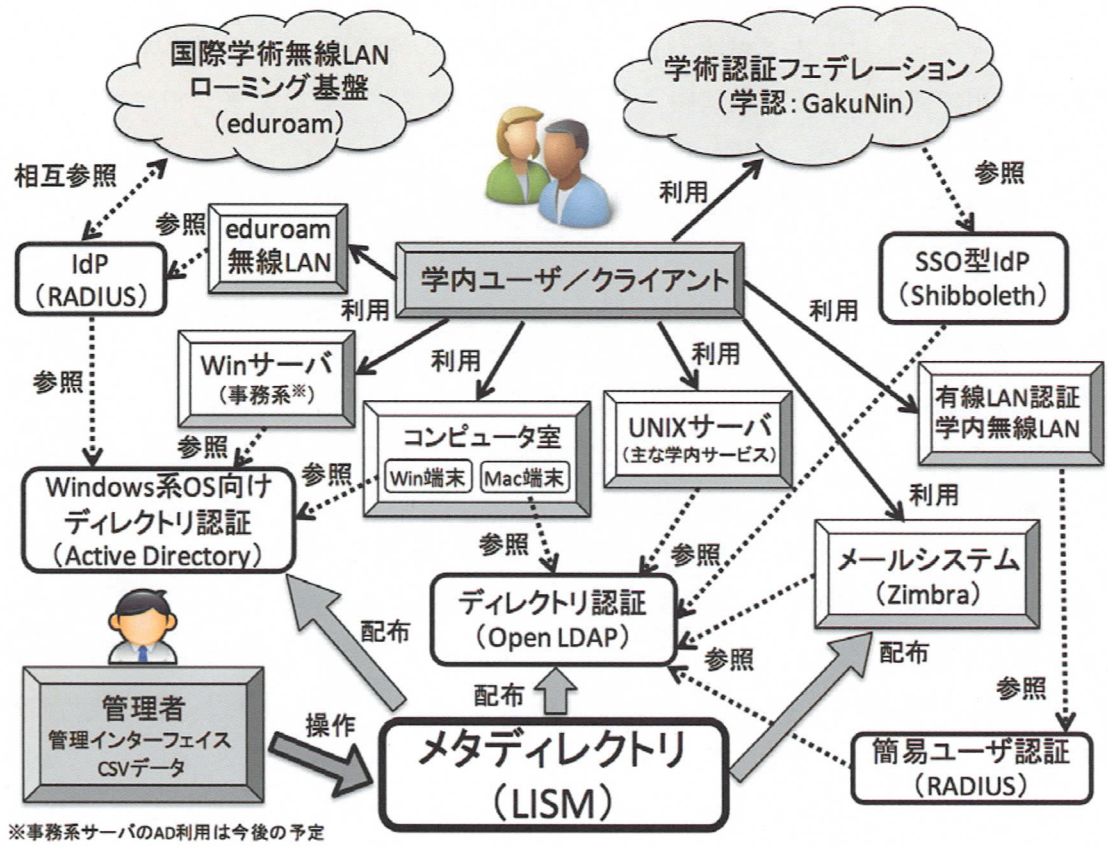
3．統合認証システムの仮想化による更新

3-1. TYCOON 統合認証システムの誕生（2015 年）

2010 年に一通りの体裁を整えた統合認証システムは，それ以前に導入したサーバ機器を利用していたこともあり，全部で 5 台の IA サーバから構成されていた．しかし 2015 年には，これら全ての機器の利用年数は 5 年を経過し，保守期限も切れる予定であった．そこで従来の統合認証システムを拡張強化した新統合認証システム（**TYCOON 統合認証システム**）への更新が，2015 年 10 月に行われた．その際，次の 3 要件を認証システムの重点仕様として，追加または強化することとなった．

- Shibboleth の導入による**学認**への参加と eduroam への接続
- AD(Active Directory)**認証**の強化
- **仮想化**による耐障害性サーバシステムの構築

TYCOON 統合認証システムにおけるこれらの新仕様は，**国立情報学研究所**(NII)を中心とした大学間連携の流れと学内における事務系サーバの増加，そして耐障害性に関する ICT 技術の向上を考慮した内容となっている．



(図1)TYCOON 統合認証システムにおける様々な認証の連携

3-2. 学認への参加と eduroam への接続（学外の学術組織との連携）

国立情報学研究所（NII）が提供する大学間の認証連携（**学術認証フェデレーション**，**学認**：GakuNin）は全国に拡大浸透しており，2016 年 1 月現在，179 の大学や研究機関が参加している．この学認に参加するには，NII に参加を申請するだけでなく，学内のユーザ情報を他大学と ID 連携（フェデレーション）するための SSO(**シングルサインオン**)型の認証基盤を設置しなければならない．具体的には SAML（Security Assertion Markup Language）によって記述された認証基盤のアーキテクチャである Shibboleth(**シボレス**)を実装する IdP(ID Provider)サーバを構築する必要がある．この学認に参加すると，他の学術関連機関が提供するオンラインの学術雑誌や学習システム等，様々なサービスにアクセスすることができる．ただし大学組織として契約の必要なも

の（有料の場合もある）もあるので注意が必要である．

一方，学術機関が相互に無線 LAN の接続認証をセキュアに共有する仕組みとして，**eduroam(エデュローム)**と呼ばれる**国際学術無線 LAN ローミング基盤**が存在する．これは欧州の情報通信技術開発を支援する組織である TERENA（Trans-European Research and Education Networking Association）で開発された互恵の精神に基づく無線 LAN 接続サービスであり，国際的デファクト・スタンダードとなっている．日本からは **eduroam JP** の名称でこれに接続しており，東日本大震災の際に強い耐障害性を示したことで評価され，2016 年 1 月の時点で 129 の大学や研究機関が参加している．なお学内の認証システムと eduroam が連携して認証を行うためには，RADIUS による IdP サーバの設置が必要となる．

3-3. AD(Active Directory)認証の強化（学内事務系サーバの収容）

2013 年 3 月に行われた TYCOON における事務系ネットワークの分離構築以降，事務系サービスを行うサーバの新規導入や更新が相次いでいる．これらのサーバ機器の多くでは，アプリケーションの仕様上，やむなく Windows 系サーバ OS を採用しているため，ユーザ認証においては AD との親和性が LDAP よりも高い．そして AD は LDAP と比べてサーバへの稼働負荷が大きい．よって TYCOON 認証システムを事務系サーバで利用する可能性が高い状況では，AD 認証の強化，特にサーバ機器のスペックの向上と冗長化が要請される．なお eduroam の RADIUS-IdP サーバは PEAP 方式の認証が必要なため，この AD サーバと連携して稼働している．また教育 2 号館 2107 コンピュータ室の Windows 端末でも，TYCOON 認証システムを用いた AD 認証を行っている．

3-4. 仮想化によるサーバシステムの構築（耐障害性の向上）

Shibboleth や eduroam の新規導入，システムの冗長化や障害発生時における修復対応の迅速化を考慮した場合，TYCOON 統合認証システムを構成するには少なくとも 8 台のサーバ機器が必要となる．しかしこれではサーバ管理も大変であり，故障率も増加する．そこでこれらのサーバ群を**仮想化技術**によって 2 台のサーバ機器（HP 社製 DL360 G9, 12core CPU, 80GB RAM）と 1 台の共有ストレージ（HP 社製 MSA 1040 FC, 900GB SAS×7）に集約することとした．また仮想化アプリケーションとしては，実績のある VMware 社の vSphere Essential Plus を用いた． 2 台のサーバ機器によって，それぞれ 5 つの仮想マシン(計 10 つ)が構築されており，そのうちの一つが vCenter Server となって仮想化全体を統括管理している．LDAP と RADIUS, AD については，それぞれの機器に 1 つずつ仮想マシンが割り当てられる冗長化構成となっている．LISM や Shibboleth, eduroam のための RADIUS-IdP については，1 つの仮想マシンでそれぞれを担っている．

その他，仮想マシン間の通信も **SSL(Secure Sockets Layer)**による暗号化でセキュリティを強化しただけでなく，個々の仮想マシンの起動と終了をまとめて行えるようになり，システム全体の管理も簡略化された．

4．認証システムの複雑化と認証の本質

TYCOON におけるユーザ認証の発展の歴史を，システムの変遷に着目して辿ってみた．概観して

言えることは，認証を伴う学内ICTサービスの増加に対して，管理者とユーザの負担をできる限り減らす方向（利便性の向上）を優先して更新を繰り返してきたということである．勿論，それに伴うセキュリティの向上についても，暗号化の強化やパスワードの設定文字数を8〜16文字にするなど（2010年），個別の技術の中で努力を行ってきた．しかし人間は楽をしたい生き物である．Webサービスへのログインパスワードをブラウザに記憶させたり，メーラに東薬IDのパスワードを憶えさせたりすることを繰り返し，その結果として自分のパスワードを記憶から消失してしまうケースも見受けられる．

さらに「ICカードで認証すれば良い」，「指紋認証が便利だ」など，安易に新技術を賞賛し，それだけに依存しようとする人もいる．しかしICカードや指紋認証の場合，ユーザが酒を飲んで酩酊状態にあれば，当人の意思とは関係なく認証を成立させてしまうことが可能である．これは私文書の成立に関する法律条項（民事訴訟法第228条4項）から逸脱する行為である．「ユーザ認証」とは，自分という「個」としての存在をインターネット上で確立するための手続きであり，それは主体的な行為であることを常々忘れないようにしたいものである．

【参考文献】

[1] 森河良太，林昌樹，宮川毅，土橋朗，東京薬科大学研究紀要，第1号（1998）77-84.

[2] 森河良太，宮川毅，林昌樹，東京薬科大学研究紀要，第10号（2007）77-82.

[3] 森河良太，倉田香織，宮川毅，小杉義幸，土橋朗，東京薬科大学研究紀要，第18号（2015）27-34.