サイエンティフィック・システム研究会　　2006 年 1 月 18 日
システム技術分科会 2005 年度第 2 回会合資料

名古屋大学のユーザ認証基盤の現状紹介

名古屋大学情報連携基盤センター
平野 靖
hirano@itc.nagoya-u.ac.jp
名古屋大学大学院多元数理科学研究科
内藤 久資
名古屋大学情報連携基盤センター
梶田 将司，小尻 智子，間瀬 健二

[アブストラクト]
名古屋大学では全構成員に統一的な ID を付与しており，情報連携基盤センターはこの ID と付随するパスワードを用いて学内情報サービスにおけるユーザ認証を行っている．この認証機能は，教務システム，図書館システム，大学ポータルなど，すでに実運用されているシステムで利用されている．利用の仕方は CAS 認証と LDAP 認証の 2 種類があり，前者は Web ベースの学内情報サービスで，後者はそれ以外のサービスで用いられている．
さらに，Yale 大学で開発された CAS(Central Authentication Service)に認可(Authorization)の機能を追加した上で, Web ベースの学内情報サービスの Single Sign-On を実現した. 本発表では，情報連携基盤センターが提供するユーザ認証基盤の概要を述べる．

[キーワード]
全学認証基盤，LDAP 認証，CAS 認証

1. はじめに

大学の情報化が進むにしたがって，学生や職員が有する ID/パスワードが増え続けている．具体的には，個々の部局(学部，大学院，学内センターなど)が運用する情報サービスのために個別に ID とパスワードを発行してきたことによって，大学内には 1 人にいくつもの ID が付与されてきた．このことは複数の ID を覚える手間をユーザに強いるばかりでなく，手帳やディスプレイに貼られたポストイットに ID とパスワードの組を記述することなどにより，これらの漏洩の危険性を拡大してきた．そのため，個々の部局で独自の ID 体系を用いるのではなく，全学的に統一された ID 体系が必要である．さらにはこのような ID 体系によるユーザ認証システムを特定の部局で集中的に管理・運用することが望ましい．

名古屋大学では，事務局総務企画部人事労務課，財務部情報企画課，および学務部との協力体制のもと情報連携基盤センターが全学 ID 運用部局となり，複数の学内情報サービスプロバイダ(全学向け・部局向け情報サービスを提供する名古屋大学の職員，あるいは学内団体)に認証機能とユーザ情報の提供を行っている．本稿では名古屋大学におけるユーザ認証基盤の概要を述べる．

2. 全学 ID

名古屋大学では，構成員(名古屋大学に所属する学生，研究生，常勤職員，非常勤職員など)を対象に，多くの部局が教務システムや図書館システム，あるいは教育用計算機システムなどの情報サービスを提供している．以前は，これらのサービスごとに ID とパスワードが発行されており，ユーザはサービスごとに複数の認証情報を覚え，使い分けなくてはならなかった．このことはユーザに対して煩雑性を強いるだけでなく，手帳やポストイットなどに認証情報を書き留めてしまうことによって，悪意のある第３者による情報サービスへの不正アクセスなどの危険性も拡大させる．名古屋大学では全学的に統一された ID 体系(全学 ID と呼ぶ)を構築し，平成 14 年 2 月から学内情報サービスプロバイダのための共通の ID として使用している(図 1)．全学 ID は名古屋大学の全学生，全職員(教職員，事務職員，および技術職員)，および全非常勤職員(非常勤講師や研究員も含む)に発行されている[1]．またユーザ認証基盤には全学 ID とパスワードのほか，氏名や所属部局など(属性情報)が格納されており，学内情報サービスプロバイダに提供することができる．パスワード以外の情報は毎月更新しているので，氏名変更や異動があった場合にも，比較的迅速に最新の情報を学内情報サービスプロバイダに提供できる．このようなユーザ認証基盤の構築によって，学内情報サービスのユーザ，学内情報サービスプロバイダ，および大学のそれぞれには下記のメリットが生じる．

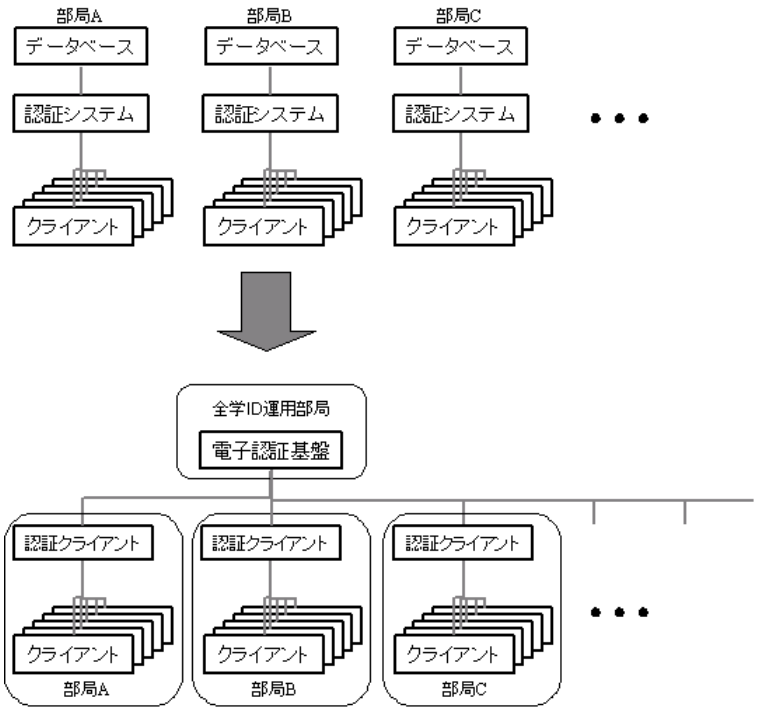

図 1 認証システムの統合

学内情報サービスのユーザ

全学 ID が広く使われるようになれば，サービスを提供する主体が異なっても，認証部分は共通化できる．したがって，誰が提供するサービスであっても，共通の ID とパスワードを用いることでサービスを受けることができる．

学内情報サービスプロバイダ

ユーザ情報の管理の手間を削減できる．とくに，ID とパスワードの生成や，異動による所属情報の変更，利用資格の付与・抹消などの手間から解放される．さらに，氏名や所属部局などのユーザ情報をユーザに入力させたり，プロバイダが入力したりすることなく入手できる．

大学

学内情報サービスに必要となる総所有コスト(TCO, Total Cost of Ownership)の低減化が実現でき，これまで必要以上に使われてきた情報化関係経費を別の目的やさらなる情報化などに使用できる．

学内情報サービスで全学 ID を用いて認証を行うことには，情報連携基盤センターにディレクトリサービス利用申請書を提出すればよい．なお，名前や所属部局などの個人情報が漏洩することは大きな問題であるため，暗号化されていないパスワードが情報連携基盤センター外のネットワークに流れないような措置，通信路の暗号化，およびアクセス制御などを行うとともに，学内情報サービスプロバイダには責任者，および実務担当者の氏名・所属などを明記していただいている．

3. ユーザ認証基盤

3.1 認証システム

名古屋大学のユーザ認証基盤では，認証データベースに LDAP(Lightweight Directory Access Protocol)[2][3]サーバを用いている．学内情報サービスは LDAP サーバに直接接続し，ユーザ認証，および属性情報の取得を行うことができる．また，我々は，高等教育機関における多様な情報システムの認証基盤の統一化を実現するための一つの方法として，Yale 大学による CAS(Central Authentication Service)[4]を拡張し，強力な権限管理機構を持つ CAS² (Central Authentication and Authorization Service)を開発した[5][6]．CAS サーバに接続することによっても，LDAP サーバに接続する場合と同様の情報を取得することができる．以下，LDAP サーバで認証を受け，情報を取得すること，および CAS サーバで認証を受け，情報を取得することを，それぞれ LDAP 認証，および CAS 認証と呼ぶことにする．CAS 認証は主に Web アプリケーションに対して，LDAP 認証はそれ以外のサービスに対して認証機能を提供している．このことは，CAS 認証がクッキー(Cookie)をベースに行われていることに起因する．

図 2 に CAS 認証の概要を示す．認証情報や属性情報は，ユーザと CAS サーバ間，および LDAP サーバと CAS サーバの間で送受信され，必要に応じて属性情報は学内情報サービスに送信される．なお，学内情報サービスプロバイダには，CAS サーバで認証されたか否かの情報のみが渡され，パスワードは渡されない．そのため，通信路においてパスワードを盗聴されないようにするためには，ユーザと CAS サーバの間のみを https 化するだけでよい．すでに CAS サーバにはサーバ証明書をインストールしてあるので，学内情報サービスプロバイダは新規にサーバ証明書を取得する必要はない．一方，CAS 認証を導入しない場合には，盗聴を防ぐために，各学内情報サービスとユーザの間を https 化する必要があり，学内情報サービスの数だけサーバ証明書が必要になる．

平成 17 年 12 月時点で，LDAP 認証，および CAS 認証を利用している部局，および学内情報サービスの数は下記の通りである．括弧内の数字がそれぞれの部局で運用されている学内情報サービスの数を表す．これらには開発予定，および開発中のものを含む．

LDAP 認証：

本部(2)，附属図書館(1)，
理学部(1)，情報科学研究科(1)，
情報メディア教育センター(2)
情報連携基盤センター(6)

CAS 認証：

本部(3)，法学部(2)，
高等教育研究センター(1)，
情報メディア教育センター(2)，
情報連携基盤センター(1)

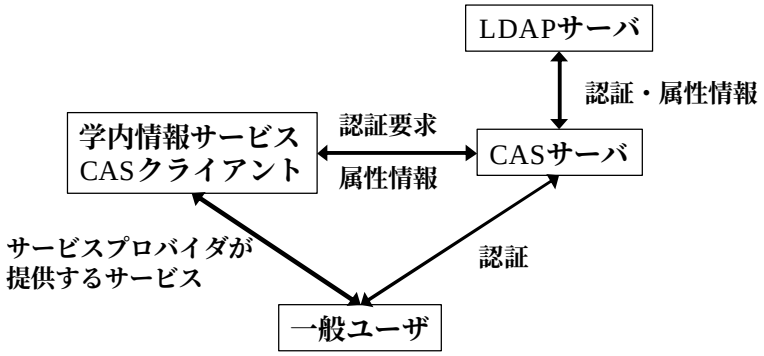

図 2　CAS 認証の概要

例えば, LDAP 認証は情報メディア教育センターでの教育用計算機システムや附属図書館での図書館システムに, CAS 認証は情報メディア教育センターでの WebCT や学務情報システム推進委員会の教務システム，情報連携基盤センターでの大学ポータルなどで利用されている.

3.2 ユーザ認証基盤の冗長化，および暗号化通信

多数の学内情報サービスが情報連携基盤センターに設置されたユーザ認証基盤を利用しているため，ハードウェアの故障などでサーバが停止するとユーザや学内情報サービスプロバイダに与える影響が大きい．そこで，図 3 に示すように，複数台の CAS サーバと LDAP サーバを用意し，負荷分散装置によって負荷分散するとともに，１台のサーバが故障などによって停止しても残りのサーバで認証サービスを継続できるようにしてある．各 LDAP サーバはマスターとなる LDAP サーバのレプリカを持っており，マスターサーバの内容を更新した場合には，ほとんど遅延なく各レプリカに更新内容が伝播されるため，すべての LDAP サーバは常に同一の内容を格納している．また，負荷分散装置は SSL アクセラレータやポートフィルタリングの機能も有し，不正アクセスの防止対策を行っている.

4. CAS 認証による Single Sign-On

名古屋大学では CAS 認証によって Single Sign-On(SSO)を実現している．この方法では，個々の学内情報サービスは認証情報を知ることなく認証結果だけを得ることが可能である．また，標準的な Web 技術だけを用いて実装することができ，Java，PHP，Perl，PL/SQL，Python など，数多くのプログラミング言語のために CAS クライアント構築用のライブラリが用意されている．また，標準的な Web ブラウザをユーザインタフェースとする．2005 年 6 月現在，30 を越える大学で採用されるなど，北米を中心に豊富な採用実績を持つ.

前章のように，名古屋大学では Yale 大学で開発された CAS を改良し，権限管理機構を付加するとともに，不必要な通信の削減，service パラメータの改ざんによる許可されていない URL への不正アクセス(Man-in-Middle)の防止，任意の属性情報によるログイン機能などの追加を行った.

本 SSO システムは，平成 16 年度後期以降の成績入力，および平成 17 年度前期以降の履修登録

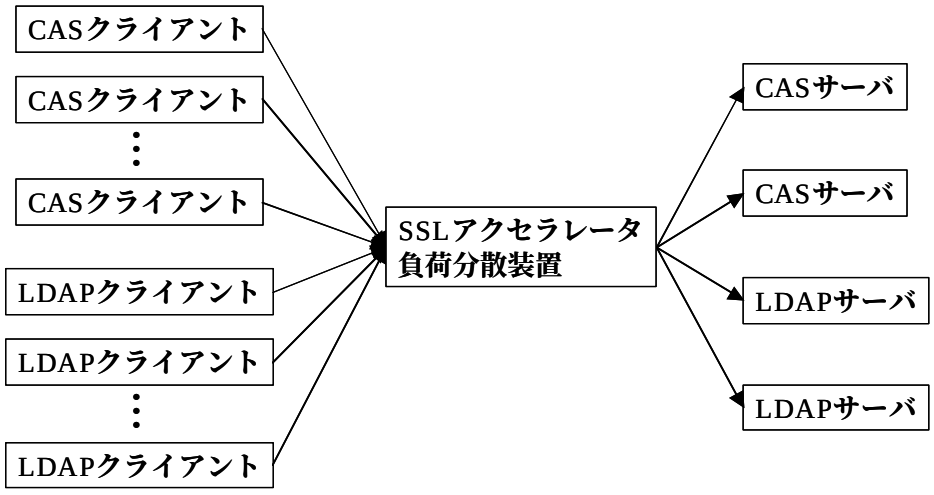

図 3　冗長化，および SSL 化

で教務システムにおける認証に用いられた．平成 16 年度後期には約 1000 人の教員が行う約 4000 科目の成績入力を 19 日間にわたって行い, 平成 17 年度前期には約 6500 人(学部 2〜4 年生)を対象に 9 日間にわたって履修登録を行った．いずれの場合も別段の問題は発生せずに成績入力・履修登録が終了した．

5. まとめと今後の課題

本文では名古屋大学での統一的な ID 体系である全学 ID の必要性と，ユーザ認証基盤の現状を概説した．また，我々が拡張した CAS² を用いて構築した SSO 環境の概要を述べた．

今後，全学 ID の説明会などを行い，既存の学内情報サービスの認証機能の情報連携基盤センターが運用するユーザ認証基盤への移行，および今後運用が開始される学内情報サービスにおいて全学 ID を利用するように促すなどのさらなる努力が必要であると考えられる．

大学においては，他大学からの訪問者に対してサービスを提供しなければならない場面も少なからずある．このような場面においては他大学・機関などで動作している CAS サーバを経由して認証結果などの交換が必要となる．また，大学間での Authentication，および Authorization サービスの実現を目的としている Shibboleth[7]との比較検討も必要である．これらの機能の実現により，より大規模かつ広範囲な統一認証基盤の実現が可能と考えられる．

現状では，学内情報サービスが CAS を利用するために必要な ACL(Access Control List)の作成やアクセス制限の変更などは，情報連携基盤センター大学ポータル専門委員会の委員(著者のうち内藤)が行っている．この作業はアクセスを許可するユーザ群の全学 ID を基に手作業で ACL を作成しなければならない点や，各学内情報サービスプロバイダ自らが運営するサービスのアクセス制限をコントロールできない点などの問題がある．そこで，このような問題点を解消するための運用ツールの作成を行っている．また，CAS² をパッケージ化することにより，他機関でも容易に CAS² を利用できる状況にする計画である．

なお，名古屋大学では全学 ID の番号体系と，格納すべき属性情報の再検討，運用体制の強化を行っており，さらに使いやすく，安全なユーザ認証基盤の構築を目指している．

謝辞

名古屋大学情報連携基盤センターに設置されているユーザ認証基盤の一部は Sun Microsystems 社からの寄贈を受けた．CAS の機能拡張に関しては，文部科学省平成 16 年度「知的資産の電子的な保存・活用を支援するソフトウェア技術基盤の構築」研究開発課題「ユビキタス環境下での高等教育機関向けコース管理システム」(研究代表者：間瀬健二)，および文部科学省科学研究費基盤研究(A)「地域学術コンソーシアムにおける e-Learning 地域ハブに関する研究」(研究代表者：梶田将司，課題番号：15200054)の助成を受けて実施されている．また，CAS のパッケージ化，および運用ツールの作成は，国立情報学研究所による CSI(Cyber Science Infrastructure)経費の一部による．

[参考文献]

[1] http://www2.itc.nagoya-u.ac.jp/center/id.htm

[2] Gerald Carter：LDAP System Administration，O'Reilly & Associates Inc.，2003

[3] Gerald Carter：LDAP －設定・管理・プログラミング－，でびあんぐる 監訳，オーム社，東京，2003

[4] Yale University ITS Technology & Planning (http://tp.its.yale.edu/)

[5] 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 Conference 予稿集，pp. 115-120 (2005)

[6] 梶田 将司，内藤 久資，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(採録決定)

[7] Internet2 Working Group, Shibboleth Project (http://shibboleth.internet2.edu/)