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

内藤 久資 (Hisashi NAITO)* ‡ 梶田 将司 (Shoji KAJITA)† ‡
平野 靖 (Yasushi HIRANO)† 間瀬 健二 (Kenji MASE)† ‡

本論文では, CAS^2 (Central Authenticatin and Auhorization Service, CAS-Square) を核とした名古屋大学におけるアイデンティティマネジメントの現状と課題について述べる. CAS^2 は, JA-SIG が提供している CAS (Central Auhentication Service) を独自に拡張したもので, CAS^2 を核とした名古屋大学のアイデンティティマネジメントに関するサービスは, 25 のアプリケーションシステムで利用される「ユーザ認証・権限管理」のための情報基盤サービスである. 本論文では, まず, 大学におけるアイデンティティマネジメントのあり方を議論する. そして, CAS^2 の導入の背景及び現行システムについて述べるとともに, CAS version 3 への対応, Security Hierarchy の導入, プロビジョニングの改善, 職員証・学生証の IC カード化, フェデレーション等, 生涯 ID として 2007 年秋に導入される「名古屋大学 ID」をベースとした次期システムについて述べる.

1 はじめに

大学が担っている社会的役割は, 教育・研究活動によって生み出される「知」や「知」を生み出す人材を広く社会に還元することである. その意味において, 「Open であり続けること」は大学に課せられた極めて重要な社会的要請であり, その実現は大学が達成すべき使命であり, TCP/IP という Open な標準技術をベースに築かれてきたインターネット時代を, その黎明期から支え続けてきた組織が「大学」であったことは「必然」といえる. 最近では, JA-SIG (Java Architecture Special Interest Group) Foundation や Sakai Foundation などが牽引する Open Source の潮流や, MIT OpenCourseWare に代表されるオープンコースウェア, さらに, Open Access 運動に端を発した機関リポジトリ (Institutional Repository) など, 「Open であり続けること」という大学の使命の実現は, 新たな形で展開している.

しかし, 迷惑メール, DoS (Denial of Service) 攻撃, フィッシング, 個人情報漏洩など, 最近のセキュリティに関する問題により, 「Open であり続けること」を使命とすべき大学でさえ, 規制を強化し, 「Open にしない」方向へと誘導されつつある. このような状況において, 「Open かつ Secure」という相反する概念を育みながら大学の情報化をいかに進めるかは, 各大学に課せられた極めて重要な課題になってきている. 特に, 大学が持つ様々なサービスやリソースについて, 『「誰に」「何を」「いつ」「どこから」「どのように」利用させるか』という問題は, 現在, 「アイデンティティマネジメント」という言葉でその重要性と実行が語られている. 実際, 情報技術活用の先進国である北米の大学では, EDUCAUSE の Top-Ten Current IT Issues 2006 において No. 1 に挙げられていることからも各大学の真剣さが伺える [1].

しかしながら, 「アイデンティティマネジメント」の実装の道は, 単なる技術的な問題でなく, 業務やポリシーに関わる問題でもある [2]. このため, 組織体制, 人的資源, 予算, 技術力, IT 戦略など, それぞれの大学の実情に合ったそれぞれのやり方を模索する必要がある. 我々も, 名古屋大学ポータルの構築の必要性から, 「全学的な統一 ID の導入」をきっかけに, 「シングルサインオン (Single Sign On, SSO)」の実現のための CAS (Central Authentication Service)[3] の導入と改良等, アイデンティティマネジメントに関する取り組みを 2002 年度から行ってきた [4, 6].

本論文では, まず, 大学におけるアイデンティティマネジメントについて, これまでの取り組みを通じて得られた経験・知見をベースに文献 [2, 5] を参照しつつ整理する.

そして, CAS^2 の導入の背景及び現状を述べるとともに, 生涯 ID として 2007 年秋に導入される「名古屋大学 ID」や, 職員証・学生証の IC カード化について述べながら将来の課題を明らかにする.

*名古屋大学多元数理科学研究科
Graduate School of Mathematics, Nagoya University
†名古屋大学情報連携基盤センター
Information Technology Center, Nagoya University
‡名古屋大学情報連携統括本部情報戦略室 (兼務)
Information and Communication Planning Office, Nagoya University

2 大学におけるアイデンティティマネジメント

2.1 ディジタルアイデンティティのライフサイクル管理

アイデンティティマネジメントで対象となるサブジェクトまたはエンティティは, リソースへのアクセス要求を行う人・組織・ソフトウェアプログラム・マシンあるいはその他のものであり, 「リソース」とは, ウェブページやデータベース中のデータであったり, クレジットカードに対するトランザクションであったりする [2]. そして, アイデンティティとは, サブジェクトに関するデータの集合で, 属性やプリファレンス, 特徴を表すものである [2]. この「ディジタルアイデンティティ」のライフサイクル管理は, 一般的に「プロビジョン (Provision)」「伝達 (Propagate)」「利用 (Use)」「保守 (Maintain)」「プロビジョン解除 (Deprovision)」の 5 つからなる [2]. 大学の場合, 「ゆりかごから寄付まで」[8] という言葉で例えられるように, 優秀な学生との入学前からの関係構築や, 同窓会や職業人大学院への再入学, 寄付など, 卒業・退職後における旧構成員との関係を保つ方向で各大学の様々な取り組みが始まっていることから, 「プロビジョン (Provision)」「伝達 (Propagate)」「利用 (Use)」「保守 (Maintain)」がディジタルアイデンティティの基本的なライフサイクル管理と考えられる (図 1 参照).

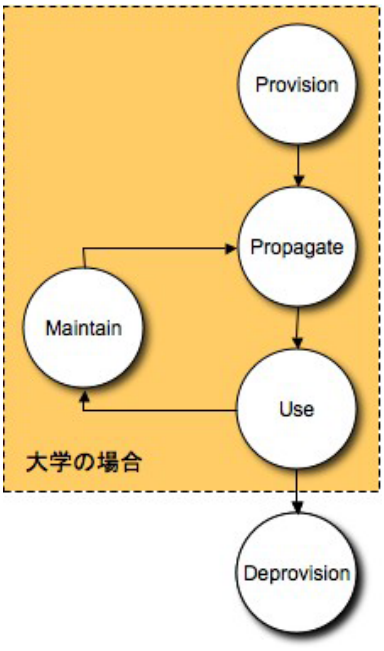

図 1: ディジタルアイデンティティ管理のライフサイクル [5] と大学の場合.

2.2 アイデンティティマネジメントに求められる機能

大学におけるアイデンティティマネジメントに関する基本調査を EDUCAUSE ECAR 研究として行った Yanosky はアイデンティティマネジメント (Identity Management, IdM) のコア機能として次の項目を盛り込み, 調査を行っている [2]:

アイデンティティの確立 (Establishing identity)
検証済みのアイデンティティ情報と実在する人物を関連づけるプロセスで, ディジタル識別子の発行やユーザアカウントの作成に先立つもの.

ユーザ認証 (Authentication)
ディジタルアイデンティティを用いる人物が, 使用の資格を与えられた人物（すなわち, 本人）であることを確認するプロセス.

権限管理 (Authorization)
ある特定の人物がアプリケーションや機能, あるいはリソースを使用するためにアクセスできるかどうかを決定するプロセス.

エンタープライズディレクトリ (Enterprise Directory)
大学の構成員やサービスに関するデータを保持している全学的な参照リポジトリ. ユーザ認証や権限認証プロセスに情報を提供する.

シングルサインオン (Reduced or single sign-on)
ある特定のネットワークにユーザがログインし, ある一定期間であれば, 必要な認証情報を他のアプリケーションに送ることにより, アプリケーションごとにユーザ認証を行うことなくリソースが使用できるようになるユーザ認証の一手法.

アイデンティティのフェデレーション (Federated identity)
異なる IT ドメイン間における疎結合で標準に基づいたアイデンティティ属性の交換. 互いに権限認証結果を認め合うパートナー間で実行される.

プロビジョニング (Provisioning)[1]
アイデンティティレコードの作成および正しい属性情報を投入し, ユーザに対してサービスを提供するために行われる IT システムの準備を行うプロセス [5].

Yanosky は, これらのアイデンティティマネジメントに求めらる機能に沿って, 各大学のアイデンティティマネジメントに関する動向を調査し, 次のようにまとめている:

[1] Yanosky は調査の都合上, プロビジョニング (Provisioning) については対象外にしている.
[2] 名古屋大学 ID の導入に伴い, 将来的に廃止予定.

表 1: IdM に求められる機能の現行システムでの対応状況.

IdM に求められる機能	現行システムでの対応状況
アイデンティティの確立	全学 ID[2]の導入.
ユーザ認証	LDAP および CAS によるユーザ認証により実現.
権限管理	CAS[2] により実現.
エンタープライズディレクトリ	LDAP サーバをベースとした全学ディレクトリサービスにより実現.
シングルサインオン	CAS により実現.
フェデレーション	特になし.
プロビジョニング	教職員については総務部人事労務課から, 学生については学務部からマスタデータの供給を受けて個人属性情報を登録.

- IdM に関する興味関心は非常に高く, 回答者は IdM によってもたらされるベネフィットの重要性をよく理解している.

- しかし, IdM テクノロジのうち, 全面的に運用されているものは一般的に少なく, フェデレーションについては, 博士課程を持つ一部の研究大学に限られており, ネットワーク認証についても限定的なドメインのままである.

- ほとんどの大学では, IdM イニシアチブに関するリソースが限られており, 今後 3 年間, 限られた全学的 IT 投資の中で取りかかるとのことである.

- しかし, IdM に関する具体的な計画やアプローチに関しては「わからない」という回答が著しく多く, IdM に関して多くの大学が「様子見の状態」である.

3 名古屋大学におけるアイデンティティマネジメントに関するこれまでの取り組み

2002 年度の情報連携基盤センター創設以来, 我々は, 名古屋大学ポータルの構築の一環として, 全学 ID や全学ディレクトリサービスの導入, CAS[2] によるユーザ認証・権限管理の一元化を行ってきた [4, 6]. これらは, 上述の IdM に求められる機能の内, 「アイデンティティの構築」「エンタープライズディレクトリ」の導入および「ユーザ認証」「権限管理」「シングルサインオン」に相当する機能の実装に対応する (表 1 参照).

本節では, 名古屋大学における IdM の中核的システムである CAS[2] に関するこれまでの経緯をまとめ, 運用中の現行システムについて述べる.

3.1 CAS[2] 導入の背景

教職員・学生などの構成員に対する情報サービスは, 一元的に管理されるものではなく, 種々の部署によって提供されている. 具体的には, 学生の履修情報に関するサービスは学生サービス部門によって提供され, 研究者の成果データベースは研究部門を掌握する部門によって提供されている. また, 各学部が, 学部特有のサービスを提供している場合も少なくない. そればかりか, 卒業生等の構成員以外に対して情報サービスを提供している場合もある.

このような大学内に多くの情報サービスが乱立する状況においては, 従来は, 情報サービスあるいは学部等の組織ごとに ID が発行されてきたが, 近年の情報管理の徹底化の流れの中で, ID 発行のための個人情報管理や, システムリソースへのアクセス管理等を統一的に行う必要が生じてきた. そのための第一歩として, 名古屋大学では「全学 ID」および「全学ディレクトリサービス」による全学的な「統一認証基盤」を導入した [4]. しかしながら, 単に統一認証基盤を導入するだけでは, 各情報サービスが独立に認証を行うこととなり, 同時に複数の情報サービスを利用する状況では, 必ずしもエンドユーザの利便性は向上しない. これを解消するためには, SSO を導入する必要があり, 名古屋大学では, 「名古屋大学ポータル」と「教務システム」間での SSO 実現のために, CAS を導入した [4, 6].

一方, 大学における情報サービスは, その目的に応じたアクセス権限管理を行う必要がある. 例えば, 「成績入力アプリケーション」の場合, 教員のみがアクセス可能にしなければならないが, 通常の SSO では, 認証を受けたユーザが教員であるかどうかをアプリケーション側で判断する必要が生じる. このため, ユーザが教員かどうかの情報を, 事前にまたはオンデマンドに統一認証基盤から受け取る必要がある. このように, 単なる SSO だけでは, ユーザ属性情報の取得のために統一認証基盤へのアクセスが生じるため, 必要としないユーザ属性値を個別に保護する必要があるなど, 統

一認証基盤管理の複雑化をもたらすこととなる．その結果, 統一認証基盤のセキュリティが低下する危険性がある．

このような情報環境を適切にコントロールする認証及べアクセス権限管理環境として, 我々は CAS^2 を導入した．

3.2 CAS^2 とは

CAS^2(Central Authentication and Authorization Service) とは, Web アプリケーションを対象とした SSO と権限管理を行うシステムであり, Yale 大学で開発され, 現在では JA-SIG によって開発が継続されオープンソースとして提供されている CAS (Central Authentication Service) を拡張し, 統一的な権限管理を行うための機構を導入したものである [6].

CAS^2 の特徴を述べるためには, オリジナルの CAS が持つユーザ認証機構としての特徴と, CAS^2 で追加されたアクセス権限管理機構としての特徴を別個に考える必要がある．

3.2.1 CAS のユーザ認証機構

ユーザ認証機構としての CAS は次の特徴を持つ:

- CAS 自身はユーザ認証データベースを持たない．
- CAS を認証機構として利用するウェブアプリケーションは, エンドユーザからの principal 情報 (ユーザ ID など) と credential 情報 (パスワードなど) を受け取らず, CAS のみが principal/credential を受け取る．
- CAS の認証過程で利用されるメカニズムは, Cookie, http redirection, JavaScript などの標準的なものだけである．
- CAS は Java Servlet として記述されているため, プラットフォーム非依存である．

なお, ウェブアプリケーションに CAS による 認証機構を導入するためには, アプリケーションの記述言語における CAS クライアントモジュールを導入するだけである．CAS クライアントモジュールは, Java, Perl, PHP など, 標準的な言語に対して用意されている．

実際の CAS を利用した認証過程は次のように行われる (図 2〜図 4 参照)

Step 1 ユーザが最初にウェブアプリケーションにアクセスしたとき, ウェブアプリケーション内の CAS クライアントモジュールは CAS サーバへのリダイレクションを発行する．

Step 2 リダイレクションにより, ユーザが CAS サーバにアクセスした際に, CAS サーバはユーザ（ブラウザ）が適切な Cookie を保有しているかどうかを検査する．Cookie を保有していない場合には, 認証情報の入力を要求し, ユーザ認証を行う．

Step 3 ユーザ認証にパスした場合には, ユーザに対して Cookie を発行する．

Step 4 Step 2 で Cookie を保有している場合, 及び Step 3 でユーザ認証にパスした場合は, アプリケーションへのアクセスのための One Time Ticket とともにリダイレクションを発行する．

Step 5 Step 4 で発行された One Time Ticket を保有してアクセスを受けたアプリケーションは, One Time Ticket を CAS サーバに送信し, One Time Ticket の検証を行う．検証にパスすれば, 正当なユーザであると判断し, アプリケーションへのアクセスを許可する．

Step 6 アプリケーション側で必要な処理を施し, 応答する．

この認証過程から分かるとおり, Cookie は 「ユーザが認証されているかどうか」を表しているものであり, CAS では “Ticket Granting Cookie (TGC)” と呼ばれる．また, アプリケーション自身は, ドメインが異なる CAS サーバが発行した TGC を読み取ることができないため, アプリケーションが認証されたユーザによるアクセスかどうかを知るために One Time Ticket が使われている．CAS では, この One Time Ticket を “Service Ticket (ST)” と呼ばれる．

また, ウェブアプリケーションの構築のためには, 通常 SSL による通信路暗号化が必須である． しかし, 「サーバ証明書の導入が面倒である」, 「サーバ証明書の扱いが分からない」などの理由により, 現実には大学においては SSL によるアクセスを実現できていない例も少なくない．CAS を利用することにより, エンドユーザ・アプリケーション間の通信には credential が流れないため, アプリケーション管理者が SSL を導入しなくても, 「パスワードが平文としてやりとりされない」ことになり, 最低限の安全性を保証することができる．

3.2.2 CAS^2 のアクセス権限管理機構

次に, CAS^2 で導入された, アクセス権限管理機構を説明する．CAS^2 では, 「どのアプリケーションに対して」「誰が」「いつ」「どこから」アクセスしたかを元に, ウェブアプリケーションへのアクセス許可するか否かという意味での権限管理機構を導入した．具体的には, CAS ユーザ認証過程の Step 4 において Service Ticket を発行する際に, 当該ユーザがアクセスしようとしているアプリケーションに対するアクセス権限を持つか否かを判断し, アクセス権限を持つ場合にのみ Service Ticket を発行する．また, Step 5 において, ア

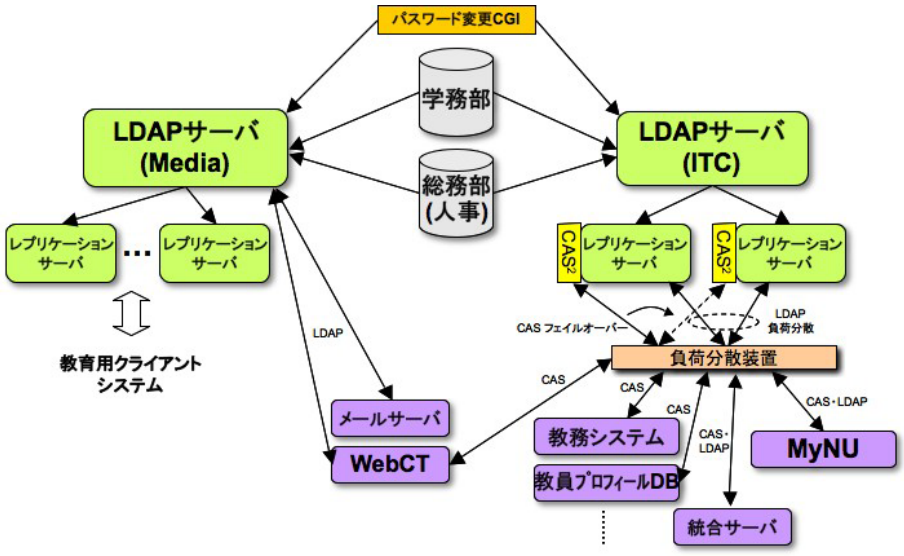

図 5: CAS^2 を核とした現行システム構成.

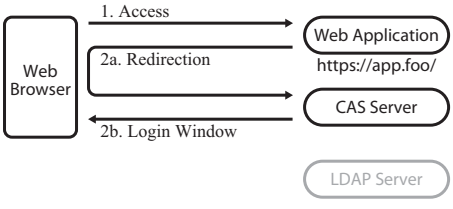

図 2: CAS のユーザ認証過程 (1)

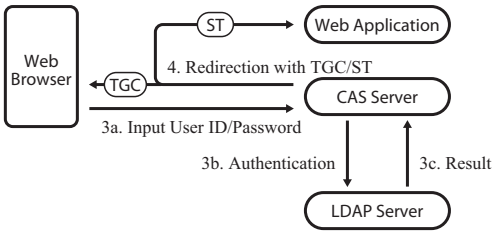

図 3: CAS のユーザ認証過程 (2)

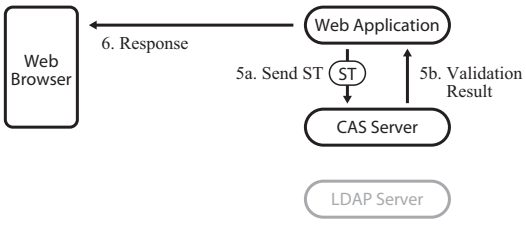

図 4: CAS のユーザ認証過程 (3)

プリケーションからの One Time Ticket の検証要求の際にも, その Service Ticket がアクセス権限を持つユーザに対して発行されたものかを検証している[3].

さらに, Step 5 において, アプリケーションに対して Service Ticket の検証結果を送信する際に, CAS^2 サーバにおいてアプリケーションごとに指定されたユーザ属性情報を送信する. これによって, 認証データベースに保存されている, いかなるユーザの属性情報をもアプリケーションに CAS^2 サーバを通じて送信することが可能となり, アプリケーションが認証データベースに直接アクセスする必要をなくしている. 実際に, 我々が CAS Access Control List (CAS-ACL) と呼ぶ, CAS^2 で利用するアクセス権限管理データベースは以下のように記述されている.

```
dn: cn=uPortal,ou=cas,o=NU
cas-service: https://app\.mynu\.jp/.*
cas-allow:
  (&(dn=.+,ou=faculty,ou=people,o=NU)
  (ip=133.6.0.0/16))
cas-attributes: uid,mail,sn,givenName
```

これは, CAS-ACL の一つのエントリであり, アクセス先の URL が cas-service 属性値に一致[4]する CAS-ACL エントリが選択される. アクセスが許可されるか否かは, 一致した CAS-ACL エントリ内の cas-allow 属性値の論理式に一致するか否かで判断される. この例の場合には, 認証データベース内でのユーザのエントリ が `dn=.+,ou=faculty,ou=people,o=NU` に一致し, さらにアクセス元が `133.6.0.0/16` で示されるネットワークに属しているときにのみアクセスが許可されることを示している. また, cas-attributes 属性には, CAS^2 サーバがアプリケーションに対して送信す

[3] この検証を行わない場合には, アクセスが許可されたアプリケーションに対して発行された Service Ticket と入れ換えることによる不正アクセスを防止することができない.

[4] 正規表現の意味で.

るユーザ属性を記述してある．すなわち, アプリケーションごとに, 送信するユーザ属性を CAS^2 サーバ側で制御可能である．

3.3 CAS^2 を核とした現行システムの構成

全学 ID, 全学ディレクトリ (LDAP) をベースに, CAS^2 によりユーザ認証・SSO が強化された現行システムの構成を図 5 に示す．全学ディレクトリを構成する LDAP サーバは, 情報メディア教育センターのレンタルシステムの一部として導入されたベンダー製のものと, 情報連携基盤センター (Information Technology Center, ITC) が導入したベンダー製のもので構成されている．レンタルシステムのカスタマイズに関わる経費負担を回避するため, このような 2 種類の LDAP サーバによる構成となっている．LDAP サーバについては負荷分散装置により 2 台のレプリケーションサーバに対して負荷分散を行い, CAS^2 サーバについては同じ負荷分散装置によりアクティブ・スタンバイ型のフェールオーバー構成をとっている．

この CAS^2 を核とした現行システムは, 2003 年 2 月からの LDAP サーバの試験運用を皮切りに, 2005 年 1 月からは本運用が開始され, 2006 年度末現在, 学内の 25 のアプリケーションにより利用されており, そのうち, CAS^2 は, Java, PHP, Perl, PL/SQL, mod_cas 等により開発されている 11 のアプリケーションにより利用されている[5][6](表 2 参照).

4 さらなる改善に向けて

こうして本格運用が開始した現行システムであったが, 時を同じくして「個人情報の保護に関する法律」が施行されることになり, 個人情報保護に関する情報サービス提供側の責務が厳しく問われる状況になってきた．これに対応するため, 職員番号や学生番号をベースとして識別名が決められている全学 ID そのものが問題となり, 「名古屋大学 ID」という新たな ID 体系の導入が検討され始めた．また, 全学の情報サービスの一元化と戦略的な対応を可能にする組織作りが同時に進行し, 2006 年度から CIO を長とする情報連携統括本部 (ICTS) が立ち上がり, 名古屋大学 ID の検討が続けられた結果, 2007 年度中に名古屋大学 ID をベースとした新しいシステムが稼働することとなった．

本節では, 現行システムの問題点に焦点を当てながら, 名古屋大学 ID をベースとした次期システムについて述べる．本節で述べる「名古屋大学 ID」の導入は, 「全学 ID」のセキュリティ問題を解決するとともに生涯 ID 化により「アイデンティティの確立」の面で強化を図っている．また, 「ユーザ ID の頑健性の追求」や「職員証・学生証の IC カード化」, 「CAS version 3 対応および Security Hierarchy」は「ユーザ認証」「権限管理」面での強化を, 「安否確認」や「職員録の電子化」を通じて, 「プロビジョニング」面での強化を図っている (表 3 参照).

4.1 名古屋大学 ID の導入

「名古屋大学 ID」とは, 名古屋大学における情報サービスの利用において「生涯利用可能な利用者識別名」であり, 情報連携基盤センターが発行してきた「全学 ID」に代わって情報連携統括本部が導入する新しい利用者識別名である [10]．全学 ID の利用が広がるとともに, (1) 個人情報保護の観点からの懸念[7], (2) 同一人物に複数の全学 ID が発行される問題, (3) 卒業生や退職者用の全学 ID の必要性, から検討を行っている．

4.2 CAS Version 3 対応と Security Hierarchy

我々が, 2005 年に CAS をもとに CAS^2 を 構築した後に, CAS 自身が大幅に改良され, 現在は version 3 系列となっている．CAS version 3 では, Spring Framework を利用して記述されている．我々は 2006 年後半から CAS^2 を CAS version 3 を元に再構築した際 に, Spring Framework での記述の利点を利用し, 認証とアクセス権限管理に対して, Security Hierarchy を導入した [9].

4.2.1 ユーザ ID の頑健性の追求

一般に, 統一認証データベース内部では, 「ユーザ ID」は, 必ずしもユーザフレンドリな文字列で記述されているわけではなく, また, 「ユーザ ID」自身が, より意味のある個人情報である場合も少なくない．例えば, 従来名古屋大学で利用されてきた「全学 ID」は, 職員番号及び学生番号を元にした ID 体系であり, 「名古屋大学 ID」はランダムに生成された文字列となっている．この中で, 全学 ID は, 職員番号を基礎としているため, それが公になることは, セキュリティ上望ましくないと考えられる．一方で, 名古屋大学 ID はランダムな文字列であるため, セキュリティ上の不安は少ないが, ユーザの利便性は低いと考えられる．

情報システムにおける「ログイン ID」(principal) とは, 認証データベース内において, ユーザの一意識別可能性を保証するものであればよい．したがって, 「全

[5] CAS^2 を導入することにより, 統一認証基盤を利用するアプリケーションの開発が容易になり, 統一認証基盤の利用が増大したと考えている．

[6] CAS^2 の導入後も LDAP を利用する新規アプリケーションがあるが, eduroam 等の CAS^2 を利用することが困難な構成のアプリケーション, 及び, CAS^2 の全学への公開以前から計画されていたアプリケーションなどがそれに相当している．

[7] 職員番号は文部科学省共済番号であり, それをベースにした全学 ID はメールアドレスにも使用されていた．

表 2: LDAP, CAS^2 を利用している学内アプリケーション数の推移.

年度	LDAP	CAS^2	合計	備考
2003 年度	5		5	名古屋大学ポータル, WebCT, 全学メールシステム等
2004 年度	4	4	8	CAS^2 運用開始. 教務システム, 名古屋大学ポータル等で CAS^2 を利用
2005 年度	3	4	7	教員プロフィール DB, 法科大学院学習支援システム等で CAS^2 を利用
2006 年度	3	3	6	医学部会議室予約システム等で CAS^2 を利用
合計	15	11	26	
(2007 年度)	(2)	(2)	(4)	利用予定を含む

名古屋大学ポータルは LDAP, CAS^2 の両方を利用しているため, 総アプリケーション数は 25 となる.

表 3: 現行システムの問題点と次期システムでの対応.

IdM に求められる機能	現行システムでの問題点	次期システムでの対応
アイデンティティの確立	全学 ID は職員番号・学生番号をベースとした ID であるため, 個人情報保護上の問題や, 同一人物に複数個の ID を発行する問題が発生. また, 卒業生・退職者に対する全学 ID の付与の必要性がでてきた.	生涯利用可能で, ランダムに生成された「名古屋大学 ID」を導入.
ユーザ認証	principal として全学 ID または登録済みメールアドレス (CAS 認証の場合), credential としてパスワードしか利用できない.	名古屋大学 ID, 登録済みメールアドレス, MyNU ID, X.509 クライアント証明書, Subscriber ID を用い, ログイン ID の頑健性を向上. IC カードの利用も可能.
権限管理	CAS version 2 に基づいた CAS^2 の実装.	CAS Version 3 への対応. Security Hierarchy の導入.
ディレクトリ	2 種類の LDAP サーバで構成.	1 種類に統合.
シングルサインオン	CAS version 2 により実現.	CAS version 3 に対応.
フェデレーション	特になし.	Shibboleth, OpenID の利用を検討.
プロビジョニング	人事マスタ・学務マスタ間の連携なし.	人事マスタを基準に全学的な標準化を検討.

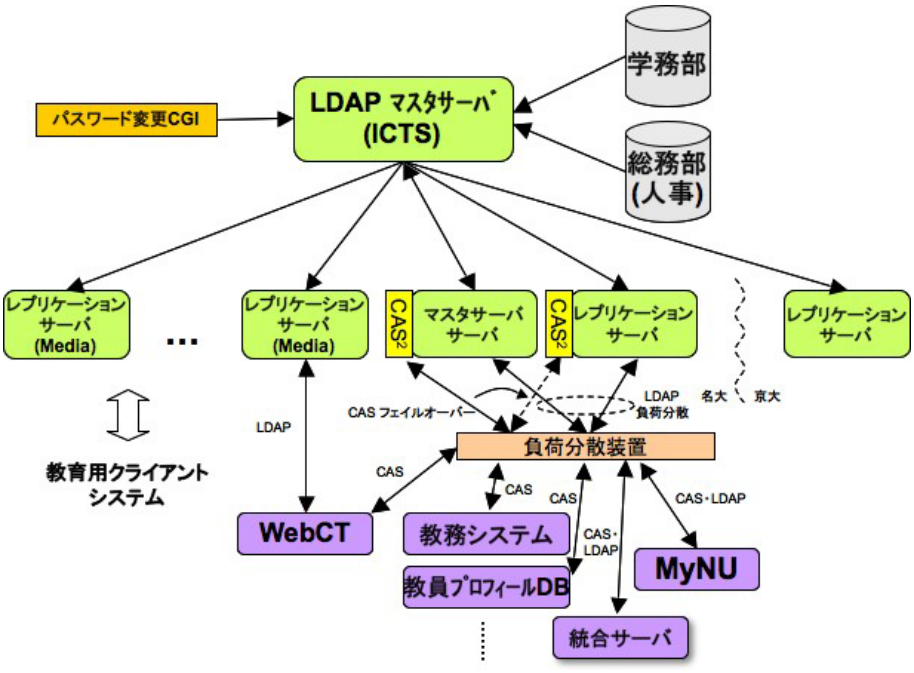

図 6: 「名古屋大学 ID」をベースとした次期システムの構成.

学 ID」「名古屋大学 ID」の他に, 各ユーザごとに一意な「メールアドレス」が認証データベース内に保存されているのであれば, principal として用いることが考えられる. しかしながら, この場合, 「ユーザ ID の頑健性」という観点でセキュリティ上の懸念が生じる. すなわち, 名古屋大学 ID のようにランダムに生成された文字列を ID として用いる場合, ユーザ ID として有効な文字列を類推することは容易ではない. しかし, メールアドレスは公になっているものであり, パスワードの類推だけで「なりすまし」を行うことが可能となる. したがって, 「名古屋大学 ID」と「メールアドレス」の principal としての頑健性を比較したとき, 「名古屋大学 ID」の方が優れていると判断できる.

また, 近年では, 高度なセキュリティを要求される情報システムに対しては, X.509 クライアント証明書を利用したアクセスを要求する場合がある. しかし, SSO 機構 の中に X.509 認証を取り入れることにより, すべての情報システムに X.509 認証を要求することにもなりかねない. 学生・教職員を含め, 万単位の多様なユーザを抱える大学では, ユーザの利便性を下げる結果になりかねず, あまりに高度な要求と考えられる.

4.2.2 Security Hierarchy の導入

このような考察から, 我々は CAS に “Security Hierarchy” という概念を導入した [9]. Security Hierarchy とは, CAS^2 が扱うアプリケーション群に対して, アクセス権限管理の一環として, principal の強度で制御する考え方である. 例として, 以下の 3 つのアプリケーションを考えてみる.

- 「教職員・学生に開放された BBS システム」誰もが容易に利用できることが要求される. したがって, 「メールアドレス」のような簡易な pricipal の利用が望ましい.
- 「学生の履修登録システム」高度なセキュリティが要求される. しかし, 学生の利便性を考慮すると, 「どのこからでも」アクセス可能であることが必要とされる. したがって, 学生証に記載のある「名古屋大学 ID」の利用が望ましい.
- 「成績入力システム」高度なセキュリティが要求され, 原則として, 学内の個人端末からのみアクセスされる. したがって, 職員証内に搭載された「クライアント証明書」の利用が望ましい.

すなわち, これらのアプリケーションは, いずれも異なるセキュリティ階層に属していると定義される. CAS^2 の CAS version 3 対応では, ユーザが「どのような認証をパスしたか」により, 「ログインレベル」を格納する. また, CAS-ACL 内に, 各アプリケーションに対してアクセスが許可されるための最小のレベルを記載することにより, 低いログインレベルのユーザは, 必要なレベルの再認証を行わない限り, アクセスが許可されないという機構を導入した. (図 7〜図 9 参照) この「ログインレベル」管理は, CAS^2 が Spring Framework で記述される利点を利用し, Dependency Injection を記述する Servlet 定義ファイル内で記述可

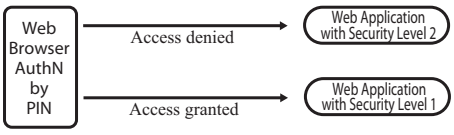

図 7: Security Hierarchy(1)

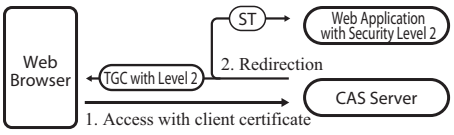

図 8: Security Hierarchy(2)

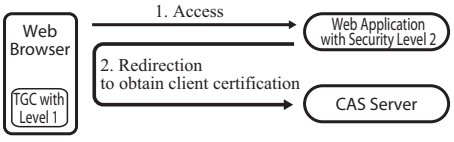

図 9: Security Hierarchy(3)

能とした. したがって, CAS^2 管理者が種々のログインレベルを自由に定義することが可能となり, 単に「ログイン ID と credential 情報の入力」という旧来の認証方法だけでなく, X.509 クライアント証明書による認証も可能となっている.

さらには, 携帯電話のブラウザからのアクセスに対応するため, 携帯電話のブラウザが持つ “Subscriber ID” を認証の principal/credential として利用することも可能である.

4.3 IC カードと PKI

名古屋大学では, 2007 年度内に職員証を IC カード化する予定である. また, 2008 年 4 月入学生から学年進行で, 学生証を IC カード化する予定である.

名古屋大学で採用した IC カードは, 接触・非接触ハイブリッド, 非接触インターフェース Type-B の Java カードであり, 初期搭載アプリケーションは, 既存および建築進行中の建物の入退館システムとコンパチブルな入退館アプリケーション及び, カード固有 ID の 2 つとなっている. また, PKI アプリケーションを搭載可能な設計となっている.

IC カード導入時には, カード固有 ID を名古屋大学 ID 認証システムデータベースに登録し, カード固有 ID を読み取ることにより, ユーザ識別が可能となるように名古屋大学 ID 認証システムを構築している. また, PKI を導入した場合には, クライアント証明書の CNAME 等の属性値を名古屋大学 ID 認証システムに登録し, ウェブアプリケーション等に対して, 本節で述べた Security Hierarchy を用いた X.509 認証が可能となる.

4.4 プロビジョニングの強化

現行システムでは, 教職員は人事マスタ, 学生は学務マスタをベースに個人属性情報が登録されているが, 所属情報・身分などの表記やコードが異なるため, 安否確認のような全構成員を対象としたアプリケーションの構築において問題が生じている [12]. また, 職員証・学生証の IC カード化や職員録の電子化を通じて, 氏名の英語表記・カタカナ表記や顔写真, 内線番号等の収集が行われている. これら「人に関する情報」を全学的に適切に収集・維持管理するため, 情報連携統括本部が IdM の観点からイニシアチブを発揮し, 人事マスタを基準とした全学的な標準化する等, 現在検討が開始されたところである.

4.5 フェデレーション対応

電子ジャーナルの購読に関して Shibboleth によるフェデレーションが情報連携基盤センター大学ポータル専門委員会で検討されている. また, 最近, 急速に広がりつつある OpenID の利用も視野に入れつつ, さらなる検討が必要である.

4.6 次期システム構成

情報メディア教育センターのレンタルシステム更新に伴い, 次期システムでは, 情報連携基盤センターが運用してきた全学 ID をベースとした現行システムをベースに, 名古屋大学 ID をベースとした次期システムの構築を現在行っている (図 6 参照).

5 まとめ

本論文では, CAS^2 を核とした名古屋大学におけるアイデンティティマネジメントの現状と課題について, 大学におけるアイデンティティマネジメントについて整理するとともに, 全学 ID をベースとした現行システムと名古屋大学 ID をベースとした次期システムを対比しながら述べた.

本論文で述べたように, 大学におけるアイデンティティマネジメントは, 組織体制, 人的資源, 予算, 技術力, IT 戦略など, それぞれの大学の実情に合ったそれぞれのやり方を模索する必要があるが, 我が国では各大学の IdM に関する網羅的な情報はほとんどない. EDUCAUSE では, 北米・欧州・オーストラリアの大学を対象としたアイデンティティマネジメントに関する広範なサーベイを現在実施している [13]. 我が国においても, 各大学におけるアイデンティティマネジメ

ントに関する知見・経験を共有できるコミュニティづくりが必須である.

謝辞

本研究の一部は, 文部科学省平成 16 年度〜19 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) の助成を受けて実施されている.

また, 本論文で述べたアイデンティティマネジメントに関わる事項は, 情報連携基盤センター大学ポータル専門委員会や, 情報連携統括本部情報戦略室・情報サポート部での議論・運用支援により行われている. アイデンティティマネジメントに関係しているすべての名古屋大学関係者にこの場をお借りして感謝の意を表します.

参考文献

[1] Barbara I. Dewey et al., “Top-Ten IT Issues, 2006”, EDUCAUSE Review, Vol. 41, No. 3, pp. 58–79 (2006.5)

[2] Ronald Yanosky with Gail Salaway, “Identity Management in Higher Education: A Baseline Study”, EDUCAUSE ECAR Key Findings, http://connect.educause.edu/library/abstract /IdentityManagementin/41164 (2006.4)

[3] JA-SIG CAS, http://www.ja-sig.org/products/cas/ (2007)

[4] 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”, 情報処理学会研究報告 (分散システム/インターネット運用技術), Vol. 2007, No. 72, pp.1–6 (2007.7)

[5] Phillip J. Windley, “Digital Identity”, O’Reilly Meia, Inc. (2005)

[6] 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, Vol. 47, pp.1127–1135 (2006).

[7] CAS^2 (CAS Square), http://www.math.nagoya-u.ac.jp/ ˜ naito/cas-square/

[8] Richard N. Katz and Associates: “Web Portals & Higher Education”, Jossey-Bass 2002.

[9] H. Naito, S. Kajita, Y. Hirano and K. 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.

[10] 間瀬健二, 平野靖, 梶田将司, ” 名古屋大学 ID の導入についてー (I) 概要ー”, 名古屋大学情報連携基盤センターニュース, Vol. 5, No. 4, pp. 316–320 (2006.11)

[11] 平野靖, 間瀬健二, 梶田将司, ” 名古屋大学 ID の導入についてー (II) 全学 ID からの移行ー”, 名古屋大学情報連携基盤センターニュース, Vol. 6, No. 2, pp. 140–145 (2007.5)

[12] 梶田将司, 太田芳博, 若松進, 林能成, 間瀬 健二, ‘大規模災害時における事業継続性確保のための安否確認システムの構築と運用”, 情報処理学会研究報告 (分散システム/インターネット運用技術), Vol.2007 (2007.5)

[13] Richard N. Katz and Ted Dodds, “International Study of Identity Management and IT Security in Higher Education”, EDUCAUSE ECAR, http://connect.educause.edu/library/abstract /InternationalStudyof/44621 (2007.7)