Vol.2012-CSEC-57 No.10
Vol.2012-IOT17 No.10
2012/5/10

認証基盤の効率化と「学認」への対応

只木進一[†1] 江藤博文[†1]
大谷誠[†1] 渡辺健次[†2]

大学の業務の情報化に伴って、認証基盤整備の重要性が増している。佐賀大学では、2010 年 3 月の更新時に、基本的情報の経路の合理化・自動化と「学認」に対応した属性整理・拡張を行った。また、評価用情報システムとの連携により、教員の所属情報の整備を行った。整備のポイントと今後の展望について議論する。

Improving the efficiency in an authentication system and its compatibility for the Gakunin federation

S. Tadaki,[†1] H. Eto,[†1] M. Otani[†1] and K. Watanabe [†2]

Integrated authentication systems are mandatory for digitalized university activities. Saga University has improved its authentication systems in March 2010. The data flow for collecting fundamental information of students and staffs is improved by simplifying the path and automatic processes. The system also became compatible with "GakuNin - Academic Access Management Federation in Japan". The data in the system are used in system for evaluation and publishing research activities. This report shows the central issues of the improvement and future issues.

1. はじめに：組織の情報基盤の重要性と課題

情報通信技術は、大学の教育・研究・診療・組織業務で不可欠な基盤となっている。大学の様々な活動がオンライン化され、対応する情報システムの数は増え続けている。また、各情報システムの利用者は、しばしば、全教員、全学生に拡がっている。たとえば、かっての教務システムは、教務系職員が学籍と成績を管理するだけのシステムであった。現在では、全学生が履修登録と成績確認を行い、全教員がシラバス登録と成績報告を行うように、利用者が全学規模となった。また、近年の「発生源入力」方式の普及により、財務や物品請求、出張管理のシステムでさへ、全教職員がアクセスするシステムとなった。

このように、ほぼ全教職員、全学生を対象とする情報システムが、多数設置されている環境下で、各情報システムが個別に利用者管理を行うことは、極めて悪い情報環境を実現することとなる。各情報システムは、利用者情報の収集に大きなコストを払うだけでなく、その情報の精度が下がり、かつ迅速に対応することが困難となる。そのため、情報システムそのものが、非効率と高コストの元凶となってしまう。更に、各利用者は、多数のユーザ名とパスワードの組を管理しなければならず、安易なパスワード設定をする傾向を示す。また、それを他人から見えるところに置くようなことが発生する。組織全体の情報基盤を担う組織は、利用者からの「パスワードを忘れた」との問い合わせに、どの情報システムのパスワードのことかを判断するところから対応しなければならなず、更に担当が違うという、利用者にとって不親切な対応をとることになる。

そこで、組織の全構成員のユーザ名、パスワード、身分、所属などを一元的に管理する統合認証システムが不可欠の基盤となってくる。統合認証システムは、データを管理するデータベースと認証を行う LDAP などの技術的仕組みだけでは動作しない。人のデータを迅速に正確に更新するための人的な仕組みが必要である。つまり、大学の場合、人事系情報システムと教務系情報システムからの円滑なデータ入力を可能とする技術的仕組みと人的体制が不可欠である。また、図書館情報システムや入退室管理システムをはじめとする全構成員情報を必要とする情報システムとの円滑な連携も必要である。そのため、統合認証システムは、運用可能性が非常に重要となるシステムである。

佐賀大学では、1998 年の全学生への利用者 ID 付与を契機に、2002 年から統合認証システムの構築と運用を行い、システムの更新のたびに改善してきた [1, 2]。少人数で運営している情報系センターが、全学生に利用者 ID を付与するためには、教務システムから効率的に学生情報を取得する必要がある。また、情報処理の演習を担当する教員の情報の取得も必要である。このような、情報リテラシ教員の普及への対応が統合認証システム構築の出発点となった。また、大学の情報システムでしばしば見られる、UNIX 系システムと Windows 系システムの混在もシステム構築の必要性であった [3]。本稿では、2010 年度末のシステム更新での改善点を中心に報告する。2010 年度末の更新では、データ入力フローの改善、シ

†1 佐賀大学総合情報基盤センター
Computer and Network Center, Saga University
†2 佐賀大学大学院工学系研究科
Department of Information Science, Saga University

Vol.2012-CSEC-57 No.10
Vol.2012-IOT17 No.10
2012/5/10

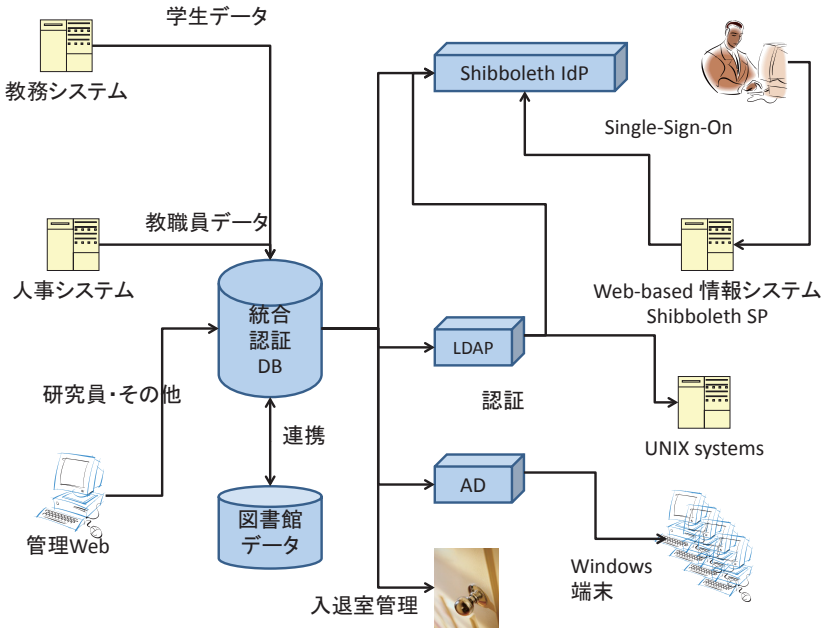

図 1 佐賀大学の統合認証のデータフロー
Fig. 1 Data flor in the authentication system of Saga University.

ングルサインオンへの対応が中心となった。

2. データの流れの改善

統合認証システムは、組織構成員の情報を迅速かつ正確に登録しなければならない。大学の構成員は、大きく分けて、教職員、学生、その他と分類することができる。教職員は人事担当課が、学生は教務担当課が人の流れを管理している。その他の構成員は、非常に複雑で、多数の部署に分散して管理されているか十分に管理されていない。しかし、その他の構成員数は、総構成員数に比べて数パーセントに過ぎない。そこで重要となるのが、人事システム及び教務システムからの迅速で確実なデータの流れの構築である。

2.1 データ入力フロー

佐賀大学の統合認証システムにおけるデータ入力フローを図 1 に示す。学生及び教職員をシステム間の通信で実現している。

佐賀大学では、2001 年度までに事務一元化が行われ、教務関連の組織は、学部の教務係から教務課の各学部担当へと組織が変更となった。教務システムの導入においても、全学利用を当初より想定したシステムとなっている。また、正規課程の学生だけでなく、科目等履修生や研究生、短期留学生、さらに連合大学院学生まで学籍管理を行っている。つまり、ここで言う「学生」と学籍番号のある者は同値である。

学生のデータについては、佐賀大学のシステムでは、従来より、教務システムからの自動入力を行ってきた。教務システムが、学生に学籍付与を行うと、夜間バッチにて統合認証システムにデータを送付する。その情報に、ログインに必要な情報、図書館利用者情報等を紐づけ、統合認証システムが教務システムに送り返す。この後に学生証が印刷されると同時に、教務システムのログイン情報が生成される。

教職員のデータについては、佐賀大学のシステムでは、従来は、やや変則的なデータ入力を行ってきた。人事システムが給与管理を主目的とするシステムのため、給与支給日を中心に作業が進む。一方、統合認証システムは、着任日にログインできるために作業を行う必要がある。両システム間に、このようなデータ登録日程に差があったため、人事担当者に不要な負荷が発生していた。人事担当課との作業手順などの長い調整を経て、2010 年度末の更新では、人事システムから夜間バッチにて発令情報を統合認証システムに直接データを送信できるように改善を行った。

学生データの場合には、統合認証システムは、教務システムから来たデータに対して、自動で利用者情報を生成する。しかし、教職員の場合には、自動登録をすることはできていない。過去に雇用されたいた職員には、確認のうえ、過去に使用していた ID を使用して頂く必要がある。学生が事務補佐員として雇用される場合があるので、学籍番号のある職員には ID を生成してはいけない一方、職員が学生になる場合があるので、個別に確認が必要となる。非常勤講師や一部の職員には ID を生成する必要がない。このような処理を確実に行うために、管理用画面からの確認作業を行った後、登録を行うこととしているためである。

大学には、その他の様々な名称の構成員が居る。例えば研究員には、日本学術振興会特別研究員のように大学が正式に受け入れている者から部局単位、場合によってはさらに細かい単位での受け入れまで様々な形態がある。特任、客員、特命など様々な形容詞が付いた教授、准教授もおり、大学との雇用関係の無い単なる称号の場合もある。近年は、派遣職員や契約職員など人事雇用でない短期の職員もいる。そのため、その他の構成員は、担当部署の総務を通じた申請をうけ、管理用画面から個別に登録している。センターで、個々の申請者

Vol.2012-CSEC-57 No.10
Vol.2012-IOT17 No.10
2012/5/10

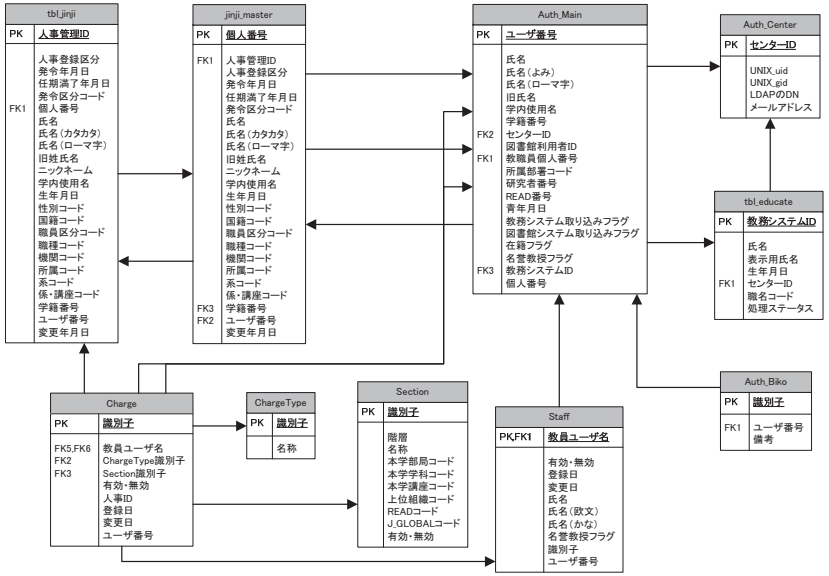

図 2 統合認証に係るデータベース関連の概要
Fig. 2 Relations between tables for the authentication system.

の在籍確認を行うことが出来ないため、直接的申請は受け付けず、必ず受け入れ担当部署の総務担当を通すこととしている。

2.2 データベースの構成とデータ更新

佐賀大学の統合認証システムでは、図 1 に示したように、データベースシステムが最上位に位置し、LDAP や AD などの認証システムを下位に従える構成をとっている。認証に不要な情報を流さない、多バイト文字を扱わない、柔軟なデータ更新を可能とすることが目的である。

統合認証用データベースの概要を図 2 に示す。センター ID、職員番号、学籍番号、図書館利用者 ID、そして教務システム ID を結びつける `Auth_Main` テーブルが中心に位置している。

ここでは、教職員の人事異動を例に、データ更新手順を説明する。各人事異動は、`tbl_Jinji` テーブルに記録され、最新のものが `Jinji_Master` テーブルに保存される。新任者の場合には、二つのテーブルを生成する。人事異動にともなう、職名や所属の変更は、`chaarge` テーブルに記録される。変更内容を `Auth_Main` テーブルに反映する。

教員の異動の場合には、後述の評価基礎情報システムや研究成果データベースが利用する現在の所属情報を集めた `Staff` テーブルに変更を反映する。新任教員の場合には、教務システムの ID 生成が必要であるフラグが生成され、教務システムでの作業を待つ状態となる。

2.3 附属図書館との連携

情報系センターとともに、附属図書館も、全構成員の情報を必要としている部署である。近年のようなオンラインサービスの発生以前より、附属図書館では、少なくとも全学生及び全教員への図書貸出、全教員からの図書購入依頼とコピーサービスのため、利用者管理が必要であった。そのため、多くの図書館用業務システムには、利用者管理機能が含まれている。

前述のように、佐賀大学の統合認証は、全学生の情報を、情報処理センターが一括して受け取り、附属図書館と共有することで始まった。2002 年の統合認証システムの開始時には、当時の学術情報処理センターが投入したデータに附属図書館の利用者番号を付して、それをキーとして、それぞれが独立した利用者管理を行った。

附属図書館の利用者管理は、利用者の書籍の貸出・返却を管理することを主目的としている。そのため、学生の場合には、連絡先などの個人情報も保持する形式となっていた。しかし、その情報の更新手段も十分ではなく、また個人情報であることから保持しない方向で検討を進めてきた。2010 年度末の更新においては、附属図書館側に利用者情報を保持することをやめ、完全な一元化を実現した。

3. データの認証以外での活用

統合認証システムの最も重要な用途は認証情報の端末等の情報システム群への提供である。同時に、統合認証は人の異動情報を保有しており、人に紐づいた情報システムの管理の基盤でもある。ここでは、教員の異動情報を活用した、評価基礎情報システムと研究業績データベースについて述べる。

近年、大学の諸活動の自己点検評価及びその公開が求められている。大学の最も基本的な活動は教育と研究であり、その担い手は教員である。そのため、教員一人ひとりの教育、研究、社会・国際貢献などを適切に把握し、教員個人評価、部局自己点検評価などを実施しなければならない。

佐賀大学では 2001 年度に「評価基礎情報システム」を導入し、各教員の教育、研究、社会・国際貢献などの活動を、各教員が登録できる仕組みを構築した。このシステムは、各教

員の経歴や研究テーマなどを公開するシステムの入力インターフェイスともなっている。そのため、単に各教員が入力できるだけでなく、その所属も正確かつ迅速に更新しなければならない。そこで、統合認証システムから評価基礎情報システムへの異動情報取り込みのバッチを定義し、2001 年度の導入当初より連携を強化している。

研究業績データベースは、教員の研究成果となる論文等の情報を登録、公開するシステムである。近年、大学等の研究成果を、単なる書誌情報だけでなく、その本文など一次情報も含めて、大学等が管理し、公開する仕組みが、国立情報学研究所の「学術機関リポジトリ構築連携支援事業」の下に進められている。本学の研究業績データベースは、この機関リポジトリの入力インターフェイスとしても機能している。

このシステムは、2001 年度より稼働してきたシステムだが、2010 年度末の更新時には、統合認証システムとの連携を強化し、教員の異動を自動的に反映できるように改修を行った。教員の最新の異動情報が `Staff` テーブル (図 2) に登録されており、それを参照することで実現している。

認証以外の利用のもうひとつは、入退室管理である。佐賀大学では、学生証・図書館利用証を用いた入退室管理を行っており、統合認証データベースから入退室管理サーバへのデータ更新を定期的に行っている。

4. シングルサインオンと「学認」との連携

4.1 シングルサインオンの導入

組織内の情報システムでユーザ名とパスワードの組を統合することだけでは、利用者の利便性向上とセキュリティレベル向上は十分ではない。一つの Web ブラウザ内であっても、他の情報システムに移るたびに認証が必要になり、利便性は未だ低いレベルである。また、各情報システム毎にパスワードを送るため、パスワード漏えいの危険がある。

シングルサインオンの仕組みは、認証済み情報を管理するサーバだけがパスワードを受け付け、各サービスサイトは、認証済みの情報だけで利用を許可する仕組みである。これにより、利便性とセキュリティレベルの両面での向上を図ることができる。

ユーザ認証機能を組織内の認証管理サーバに集中させることで、外部組織からも、ユーザの存在を確認することができる。これにより、組織間の認証連携が可能となる。このように、組織内での認証統合だけでなく、大学等の認証基盤を緩く連携させることで、大学の構成員であることを確認して、電子ジャーナル等の利用を円滑に行う仕組みが構築されている。国立情報学研究所が進める学術認証フェデレーション「学認」である [4]。

「学認」対応のシングルサインオンは、Shibboleth と呼ばれる仕組みに基づいている [5]。この場合、認証は、認証情報を管理する IdP (Identity Provider) だけがパスワード認証を行い、各情報システムは、SP (Service Provider) として、IdP の認証済情報に基づいてサービスを提供する。こうした組織外のサービスとして、もっとも重要なものの中には、電子ジャーナル利用を、契約組織の IP アドレスによる認証から人の認証へと変更し、キャンパス外からの利用を可能とするものがある。そのほかにも、「学認」対応のシングルサインオンを学内の認証基盤として活用する事例が多数報告されている。例えば、金沢大学では、学内の多数のサービスがシングルサインオン化されるだけでなく、ファイル転送等の外部向けサービスが提供されている [6]。佐賀大学では、2010 年度末の更新時に、シングルサインオンを本格導入し、「学認」の運用に参加した。

IdP は、LDAP の情報を基に認証情報を提供することが想定されている。LDAP は、ユーザ名、パスワード、ホームディレクトリパスなど、必要最小限の認証情報しか保持していない場合が多い。認証に不要な情報を流さない、多バイト文字を扱わない、柔軟なデータ更新を可能とすることを目的として、佐賀大学でも最小の情報しか流通させていない。一方で、IdP では、和文及び欧文での氏名、所属、職名などを提供する可能性がある。そこで、佐賀大学では、LDAP の情報に加えて、統合認証システム内の利用者データベースから直接に氏名等の付加情報を追加する仕組みとした。

表 1 に、佐賀大学の IdP が提供する属性を示す。LDAP から直接取得している属性は、`uid`、`principalName` 及び `ComputedId` の僅か三つである。氏名、組織名、職名等は DB から生成している。

4.2 認証ネットワーク opengate のシングルサインオン化

教員や学生が持ち込む私有のノート型パーソナルコンピュータ (PC) は、教員が講義で移動しながら利用するノート型 PC を無視した大学のネットワーク構築は許されない。佐賀大学では、2000 年より特殊な機器やソフトウェアを必要としな認証ネットワーク opengate を開発し運用している [7]。この認証ネットワークの導入には、その当時に統合認証がほぼ稼動していたことが大いに影響している。

2010 年度末のシングルサインオン導入においては、もっとも最初の SP として opengate を対象とした開発を行った [8]。ノート型 PC または公開端末の利用者は、ネットワーク利用許可を得ることとシングルサインオン環境へ参加することが同等となる。利用開始後は、学内外の全ての SP へのシームレスなログインが可能となる。

Vol.2012-CSEC-57 No.10
Vol.2012-IOT17 No.10
2012/5/10

表 1 IdP の属性取得方法と SP ごとに取得可能な属性
Table 1 Methods for collecting properties in IdP and properties available for SPs.

属性名		情報の取得方法					SP ごとに取得可能な属性				
		LDAP	DB	Static	Script	その他	デフォルト	学内	CiNii	Ovid	Elsevier
transientId	IdP, SP 間で認証処理を実現するために生成するセッションごとに異なる ID					○	○				
uid	ユーザ ID（外部には公開しない情報）	○						○			
principalName （eduPersonPrincipalName)	フェデレーション内で一意となる匿名の利用者識別子 UID 保護のため、UID と特定の文字列からハッシュ値にドメイン名を付加して生成。	○			○		○	○			
eduPersonTargetedID	フェデレーション内で一意かつ，SP サイト毎に異なる永続的な匿名の利用者識別子。ComputedId 属性より生成する。					○		○	○		
ComputedId	UID と特定の文字列から生成する匿名の利用者識別子	○				○					
eduPersonEntitlement	特定のアプリケーションを利用する資格情報			○				○			○
jaOrganizationName	組織名称の日本語			○			○	○	○		
organizationName	組織名称の英字			○			○	○			
jaDisplayName	日本語氏名（表示名）		○					○			
displayName	英字氏名（表示名）		○					○			
jaou	組織内所属名称の日本語		○					○			
ou	組織内所属名称の英字		○					○			
eduPersonAffiliation	利用者の職種等		○								
eduPersonScopedAffiliation	利用者が所属する組織内での職種		○					○		○	
mail	電子メール		○					○			

5. まとめと今後の課題

本稿では、佐賀大学の統合認証の整備について、入力データフローの効率化、データの活用、そして「学認」に対応したシングルサインオンを中心として報告した。1988 年から全学生の利用者 ID を管理するために、当初は少ない工数で確実に利用者情報を取得することと、UNIX 系 OS と Windows 系 OS に共通のユーザ名・パスワードの組を提供することを目的として統合認証システムの構築を開始した。その後の継続的な効率化と提供システムの拡大の後、2010 年度末からは、データの入り口の自動化と Shibboleth によるシングルサインオンによる「学認」対応を導入した。これにより、利用者からみるとひとつのユーザ名・パスワードの組でシームレスに情報システムを移動できる利便性が大きく向上した。管理者側からみると、効率化とともにセキュリティレベルの向上を実現した。

以下にいくつかの課題を述べる。統合認証システムの配下には、演習室端末群が含まれている。利用者は、端末ログインの後に Web ブラウザ起動によりシングルサインオンの認証画面にて再度認証されている。Windows 端末に対して、AD での認証によりシングルサインオン認証を行う事例が報告されている。端末の認証をシングルサインオンとすることで、Web 起動時に個人に特化したお知らせを直ちに表示することが可能となり、利便性の一層の向上が可能となる。

認証の統合により、組織内の情報システムの稼動には、認証システムが稼動していることが不可欠な前提となる。LDAP の場合には、クライアントに常時、複数に認証サーバを認識させ、認証サービスの冗長化が可能となっている。Shibboleth の場合には、「認証済み」情報を IdP 間で共有化する冗長化が報告されている [6]。佐賀大学では、電源管理の強化により「止まらない」ための対策を進めているが [9]、IdP そのもの冗長化・多重化が必要になる。

統合認証システム、あるいは IdP は、利用者が本人であることと、IdP を運営する組織

Vol.2012-CSEC-57 No.10
Vol.2012-IOT17 No.10
2012/5/10

の一員であることを証明することを目的としたシステムである。LDAP や IdP には、組織内の所属や職名など、各情報システムがログインを認可するするために参考とすることができる属性が含まれている。全学共通システムならばこの共通属性で認可を行える場合がほとんどであろう。しかし、特殊な用途の学内システムだけでなく、学会等のサービスの場合には、大学の IdP からの情報では認可を決することができない。学会等の学外組織がその組織への所属情報を認証フェデレーションへ提供する仕組みの提案が行われている [10]。大学内においても、共通的属性を越えた認可をサポートする仕組みが必要である。

謝辞 統合認証のシステム構築、シングルサインオンの活用する各種 SP の構築を支援していただいた NTT データ九州に感謝いたします。

参 考 文 献

1) 江藤博文，渡辺健次，只木進一，渡辺義明：全学的な共通情報アクセス環境のための統合認証システム，情報処理学会研究報告. DSM, [分散システム/インターネット運用技術]， Vol.2002, pp.31–36 (2002).
2) 江藤博文，渡辺健次，只木進一，渡辺義明：大学における情報基盤整備の中核となる統合認証システム，情報処理学会シンポジウムシリーズ，Vol.2003, No.6, pp.43–48 (2003).
3) 江藤博文，小野隆久，平良　豊，只木進一，渡辺義明：UNIX と Windows の共存する教育用システムにおける利用者管理と端末管理，学術情報処理研究，No.2, pp.14–26 (1998).
4) 国立情報学研究所：学術認証フェデレーション，`https://www.gakunin.jp/docs/fed/`.
5) Internet2: Shibboleth, `http://shibboleth.internet2.edu/`.
6) 松平拓也，笠原禎也，高田良宏，東　昭孝，二木　恵，森　祥寛：大学における Shibboleth を利用した統合認証基盤の構築，情報処理学会論文誌，Vol.52, No.2, pp.703–713 (2011).
7) 渡辺義明，渡辺健次，江藤博文，只木進一：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，Vol.42, No.12, pp.2802–2809 (2001).
8) 大谷　誠，江藤博文，渡辺健次，只木進一，渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌，Vol.51, No.3, pp. 1031 – 1039 (2010).
9) 只木進一，田中芳雄，小野隆久，渡辺健次：情報系センターの停電対策と電源管理，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol.2011, No.8, pp.1–5 (2011-09-30).
10) 山地一禎，片岡俊幸，中村素典，曽根原登：シボレスシステムを用いた属性連携基盤の開発，情報処理学会研究報告. 情報学基礎研究会報告， Vol.2009, No.10, pp.1–8 (2009).