

PKI手法を用いた組織間での利用者認証連携についての検討

阿部, 英司
九州大学物理学科情報理学コース

伊東, 栄典
九州大学情報基盤研究開発センター

<https://hdl.handle.net/2324/17044>

出版情報：電子情報通信学会第19回データ工学ワークショップ (DEWS 2008), 2008-03. 電子情報通信学会
バージョン：
権利関係：



PKI 手法を用いた組織間での利用者認証連携についての検討

阿部 英司[†] 伊東 栄典[‡]

[†]九州大学物理学科情報理学コース 〒812-8581 福岡市東区箱崎 6-10-1

[‡]九州大学情報基盤研究開発センター 〒812-8581 福岡市東区箱崎 6-10-1

E-mail: [†]sc104002@s.kyushu-u.ac.jp, [‡]itou@cc.kyushu-u.ac.jp

あらまし インターネット上の個人向け情報サービスや、組織の内部向け情報サービスでは、利用者認証が必要である。利用者認証を介する情報サービスが増えるにつれて、複数サービス間の連携への要求が高まっており、そのための利用者認証連携の要求が高まっている。国内では全国共同電子認証基盤構築事業(UPKI)が行われており、大学間のサービス連携のための研究開発が行われている。我々は、UPKI に参加しており、組織間でのサービス連携のための、組織間での利用者認証連携(ID Federation)についての研究を行っている。今回、組織間の認証連携について、ID・パスワードに基づく方法や、PKI 手法を用いた方法について調査した。本論文では、認証連携の仕組みやパラダイムについての調査結果を述べる。また、我々が検討している認証連携機構についても説明する。

キーワード PKI, ID 統合管理, 利用者認証, ID 連携

A study of PKI based inter-domain ID-federation

Eiji ABE[†] and Eisuke ITO[‡]

[†]Dept. of Informatics, Kyushu University 6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581 Japan

[‡]Research Institute for IT, Kyushu University 6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581 Japan

E-mail: [†]sc104002@s.kyushu-u.ac.jp, [‡]itou@cc.kyushu-u.ac.jp

Abstract Membership oriented services must implement user authentication mechanism. Recently, demand for inter-domain service is arising, such as grid computing, web mash-up services, and so on. For inter-domain services or nationwide services, it needs inter-domain user authentication mechanism, but it is very difficult to manage the user identity database over domains. ID federation is a solution for this problem. The UPKI project is started by NII since 2005, and the UPKI project researches and develops the nationwide electronic certification platform. UPKI aims to achieve the inter-institutional exchange of user authentication and to construct mutual trust among institutions. The UPKI project tries to realize PKI-like trust framework. The authors join the UPKI project, and research PKI based inter-domain ID federation. In this paper, we study the intra-domain user authentication mechanisms. At first, we explain conventional ID/PW authentication, PKI based user authentication. After that, we describe inter-domain user authentication frameworks. Finally, we describe our inter-domain authentication mechanism, and compare our mechanism and other mechanisms.

Keyword PKI, Identity Management, User Authentication, ID-Federation

1. はじめに

インターネット上で公に提供されている情報サービスや、組織の内部向け情報サービスに、利用者認証を伴うものが増えている。例えば、Google 社の iGoogle や Gmail 等、マイクロソフト社の Windows Live, Yahoo 社の各種個人向けサービス、各社の blog サービス、mixi 等の SNS サービスでは、個人に特化したサービスを提供している。これらのサービスは利用開始時に、利用者を特定するための認証機構を用いている。

組織内向けの情報サービスでは従来から利用者認証を行うことが多かった。例えば大学は、履修登録や成績確認、講義情報提供などのサービスで利用者認証

を行っている。組織の内部向け情報サービスではプライバシー情報を扱う場合も多く、安全・安心な情報サービスを実現するための利用者認証が重要である。

このように、個人化サービス(personalized service)の提供や、プライバシー保護のために利用者認証を行うサービスが増加している。しかしながら、利用者認証を介する情報サービスが増えるにつれて、認証手続きの複雑さが問題になっている。利用者認証では従来から、利用者 ID とパスワードによる二要素認証機構を用いることが多いため、情報サービスの増大につれ ID・パスワードが増大し、そのため ID・パスワード忘れや、ID・パスワード入力の複雑さが問題になった。

Web に公開されている一般的な情報サービスでは、一度の認証で複数のサービスを利用可能にするシングルサインオン(SSO, Single Sign-on)についての要求が利用者側から高まっている。そのためサービス提供者側は、SSOを実現するため、利用者認証の連携機構を構築している。

一方、組織内向けの情報サービスについても、連携協定を結んだ組織間でのサービス連携について研究開発が進んでいる。国立情報学研究所では、2005 年より最先端学術情報基盤(CSI: Cyber Science Infrastructure)構築の事業を行っている[1]。CSI では全国の大学や研究所といった学術機関を跨って情報サービスを行うための学術情報基盤構築を目指している。CSI 実現のため、四つのサブプロジェクト：高速ネットワーク、グリッド計算、機関リポジトリおよび全国共同電子認証基盤構築事業(UPKI)、が行われている。

UPKI[2][3]は CSI 事業における利用者認証連携の基盤構築部分を担っている。UPKI では、その名の通り PKI に基づく利用者認証情報の確認を指向しているものの、必ずしも PKI の電子証明書に限定するものではなく、ID・パスワードや他の手法を用いた認証機構についても認証連携手法を検討している。

我々も UPKI に参加しており、組織間サービス連携のための組織間利用者認証連携 (ID Federation) についての研究を行ってきた[4][5][6]。本稿では、組織間認証連携について、ID・パスワードに基づく方法や、PKI 手法を用いた方法といった認証連携の仕組みやパラダイムについての調査結果を述べる。また、我々が検討している認証連携機構についても説明する。

2. SSO の仕組みと認証機構

ここでは認証連携の前提として、SSO (Single Sign-on) の仕組みについて述べる。

2.1. SAML

認証を要するサービスが増大するにつれ、特に Web アプリにおいて、認証作業の複雑さを削減するための SSO が望まれている。Web アプリでの SSO を実現するため、セキュリティドメイン間で認証情報・認可情報を交換するためのデータフォーマットである SAML (Security Assertion Markup Language)[11] が考案された。SAML はデータ交換言語であるだけでなく、役割や処理手順といった枠組も定義している。

SAML のセキュリティドメインは、IdP (identity provider) と SP (service provider) の二種類に分けられる。IdP で認証認可の表明を作成し、SP では送られてきた表明を基に、サービス提供の可否を判断する。図 1 に SAML のサービス枠組を示す。

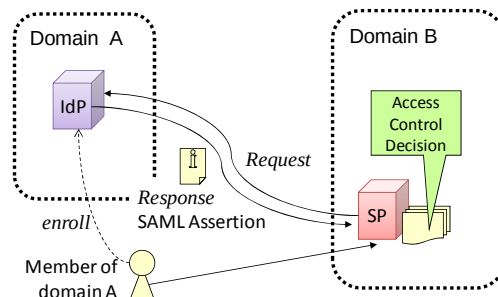


図 1. SAML のサービス枠組み

Web SSO を実現するため、OASIS[10] は「Security Services Technical Committee」を設け、上記の枠組や、データ交換フォーマット、記述項目を定め、SAML v1 として公開された。一方、多数の情報関連企業が参加しているコンソーシアムであるリバティアライアンス (Liberty Alliance)[12] でも、Web SSO についての研究開発を行っており、ID-FF と名付けられた枠組・フォーマットが提案された。その後、二つの規格は融合して SAML v2 として公開されている。現在、SAML は企業が製造する Web SSO 製品の標準として使われている。

2.2. SSO アーキテクチャ

認証を受け持つ IdP と、実際のサービスを提供する SP とを分割することにより、柔軟な SSO が可能になった。図 2 に示す様に、SSO の実現は様々な構成方法がある。SSO の入口となる Web リバースプロキシを利用する方法や、SP 側に SSO エージェントを埋め込む方法、利用者側 (Web ブラウザ側) にエージェントを埋め込む方法などが提案されている。利用者の認証としては、Web リバースプロキシやエージェントが IdP とやり取りする事で実現している。

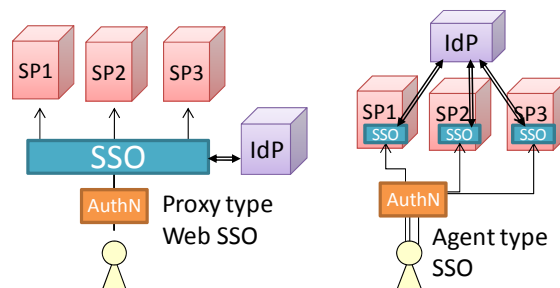


図 2. SSO 構成例

3. PKI を用いた利用者認証

ここでは、PKI を用いた利用者認証について簡単に述べる。PKI (Public Key Infrastructure) は、日本語では一般に公開鍵暗号基盤と呼ばれることが多い[13]。PKI は、公開鍵暗号方式をオープンな場で利用するための基盤である。

公開鍵暗号方式を用いると、秘匿情報を通信する際の暗号化や、本人性確認が可能になる。通信相手が既知の場合は良い。しかし相手が未知の場合、その利用者の公開鍵を信頼してよいか問題となる。送られてきた公開鍵を信頼して秘密情報を送信した所、盗聴者の公開鍵である事があるかもしれない。

このような問題を解決するために PKI が考案された。PKI では信頼できる第三者 (trusted third party) を想定し、その信頼できる第三者が身元審査を行うことで、利用者の公開鍵を真正性を保証する。また、公開鍵に加えて利用者の氏名や所属も含めることで、その利用者の本人性保証も可能になる。これにより、ネットワークでの身元証明を行う事が可能になる。

PKI では利用者の個人情報も含めた身元証明書を証明書(certificate)」と呼び、証明書を発行する信頼できる第三者機関を「認証局(certificate authority)」と呼ぶ。

以下に PKI の仕組みを用いた利用者認証を述べる。

- CA の構築
 - CA は自分自身で用いる公開鍵・秘密鍵を作成する。
 - CA の秘密鍵を用いて、CA の公開鍵を署名し、それにより自己証明書を作成する。
- 利用者からのクライアント証明書の発行要求
 - 利用者用の公開鍵・秘密鍵ペアを作成
 - 鍵ペアに、氏名や所属組織名などの情報を沿えて、CSR(証明書発行要求, certificate signing request)を作成
 - CSR を CA へ送付
- 利用者へのクライアント証明書を発行
 - CA は、送られてきた CSR の内容を審査。本人の本人性(記述内容に間違いがない事)と、実在性(本当に存在するか否か)の確認を行う。
 - 審査の後、CA の鍵を用いて署名し、CSR からクライアント証明書を作成。
- SP での利用者認証
 - (主に Web サーバである)SP は CA を信頼する。つまり、CA の自己証明書を信頼するよう SP のサーバを設定する。
 - サービスの利用開始時に、利用者は自分のクライアント証明書を SP へ提供する。SP は送られてきた証明書の内容を確認する。
 - 送られてきたクライアント証明書に CA の署名がある(CA の秘密鍵で署名されている)ならば、SP は証明書を信頼する。
 - Web 上の SSL(secure socket layer)または TLS(transport layer security)でクライアント認証を行う場合、Web サーバおよびブラ

ウザが半自動的に利用者認証処理を行う。

4. ID-Federation の仕組みと実装例

認証を受け持つ IdP と、実際のサービスを提供する SP との分割により、サービスと認証を行う組織が異なる場合の連携も可能になる。ここでは、実際に稼働している認証連携機構をいくつか示す。

4.1. Shibboleth

米国の Internet2 プロジェクトでは、Shibboleth[14]と名付けられた ID 連携による利用者認証・認可の基盤の提案および実装を行っている。Shibboleth では、組織間でのシングルサインオン機構も実現している。なお、Shibboleth での認証・認可情報は、SAML 形式でやり取りされる。

また Shibboleth では、組織間での ID 連携のために、WAYF (Where Are You From?) と名付けられた仕組みを導入している。WAYF の概要を図に示す。WAYF を用いる場合、利用者は利用者 ID の入力と、自分が所属する組織名を入力する(指定する)。これにより、どの組織の IdP を用いるかが特定でき、その IdP で利用者認証を行う。これにより様々な組織間での連携が可能になる。

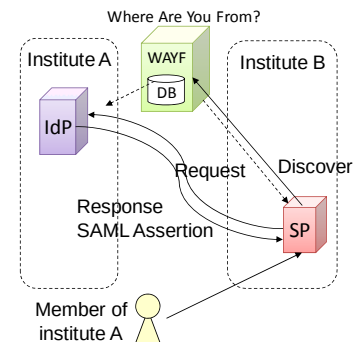


図 3. Shibboleth のサービス枠組

さらに、Shibboleth の開発者は、グリッドのミドルウェアである Globus Toolkit[16]と連携するために、Globus 対応の認証ミドルウェアである GridShib[15]も開発している。

4.2. Web アプリケーションにおける認証連携}

Web 系のアプリケーションでは近年、ASP(Application Service Provider)や SaaS (software as a service) といった名称で呼ばれる、ソフトウェアの機能をサービスとして提供する事が普及しつつある。従来から Web 系のアプリケーションでは LDAP サーバ用いた認証機構を使う場合も多く、サービスと認証機構が連携する仕組みが出来ていた。

Web 系のアプリケーションでの組織間認証連携の具体例として Google Apps Education Edition[17] を示す。Google Apps Education Edition は、Google 社が提供する各種サービスを大学で利用できるサービスである。ウェブベースの管理画面で利用者管理ができるほか、API を使用して Google Apps を既存のシステムに統合することができる。大学が持つ認証機構と組み合わせて使う場合、組織間の認証連携となる。

大学側の認証サーバが IdP に、Google Apps 側が SP になる。図 4. Web アプリでの認証連携例 (Google Apps) に連携の仕組みを示す。

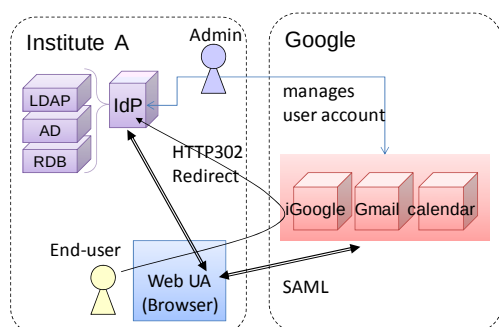


図 4. Web アプリでの認証連携例 (Google Apps)

4.3. eduroam

eduroam [18][19] は「Education Roaming」から名付けられたもので、教育研究機関の間で相互に無線 LAN 接続環境を提供しあうものとして欧州の TERENA[22] で開発・展開されている。無線 LAN への接続時には 802.1X による利用者認証を行い、認証情報確認には RADIUS を用いている。当初 eduroam は欧州を中心に展開されていたが、2004 年にオーストラリアの大学が eduroam に参加し、その後は APAN[23] に関係のある大学が eduroam に参加している。2006 年には日本の大学も eduroam 参加している [20][21]。

eduroam の基本的な構造を図 5 に示す [18]。ある eduroam 参加機関の所属者は、他の eduroam 参加機関に訪問した際、自分の所属組織が発行した身元情報証明を用いることで、訪問先の eduroam 無線 LAN に接続できる。ここで身元情報証明とは ID・パスワード、もしくは PKI の電子証明書を意味する。ただし、どのような通信を許すのかという接続ポリシーは無線 LAN 環境提供機関のポリシーに依存する。

利用者認証に ID・パスワードを用いる場合、ID として所属組織を表す文字列を付加する。この ID は RFC2486 で定義される Network Access Identifier[24] の形式、つまり user@kyushu-u.ac.jp のように表記される形式をしている。ここで '@' 以降の自組織を示す部分は realm と呼ばれる。RADIUS サーバは realm 文字列

を見て、自組織の認証機構を使うか上位 RADIUS サーバへ認証情報を転送するかを決める。最終的に realm 文字列に対応する組織の RADIUS サーバで利用者認証を行い、無線 LAN への接続の許可不許可を決める。

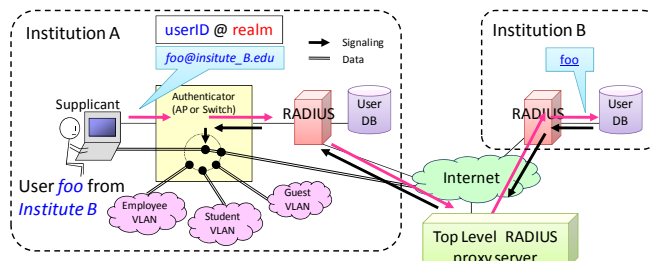


図 5. eduroam のサービス枠組

4.4. OpenID

OpenID は分散 SSO システムで [25]、Web サイト利用のための利用者識別子 (利用者 ID) とパスワードを作成する IdP と、認証情報を SP に提供する仕組みを構築・提供している。OpenID では、多くの IdP が誰でも自分の OpenID (利用者識別子と身元情報) と登録することができるようにしている。インターネット上にサーバを持つ者なら誰でも OpenID の IdP を構築でき、また OpenID 用ソフトウェアを導入すれば、誰でも OpenID 対応サイトを構築することができる。図 6 に OpenID のサービス枠組を示す。

OpenID の大きな特徴として、利用者を特定するための識別子が URI 形式になっていることが挙げられる。URI 形式は様々な利点となる。識別子 (identifier) は、名前空間内で一意であることが必要である。識別子を URI 形式にすることで、各 Web サーバ内 (あるいはインターネットドメイン内) で一意であれば、全世界での一意性を保つことができる。

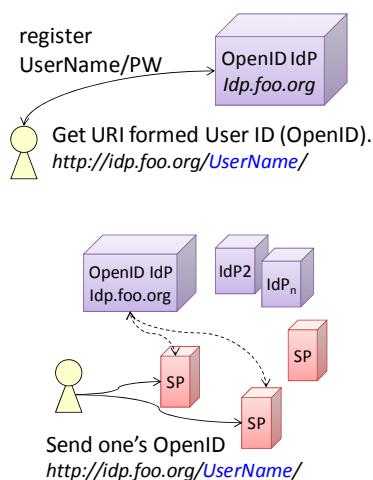


図 6. OpenID のサービス枠組

5. PKI 手法を用いた組織間認証連携の問題点

5.1. クライアント認証の課題

PKI の仕組みを用いると、強固なエンティティ認証を行うことができ、かつ通信路の暗号化や、データへの署名を実現できる。現在、サーバについては証明書を利用することが一般に行われている。しかしながら、利用者側（クライアント）の認証における証明書利用は一部の大学内・企業内でしか行われておらず、普及が進んでいない。

多数の利用者へサービス提供する SP では公的証明書を用いることが多い。通信の暗号化による秘密保持に加え、サーバ自身の信用性向上が実現できるため、高価な公的証明書を用いても十分な効果がある。しかし、利用者認証（クライアント認証）での公的証明書利用は、利用者が多いと過剰コストになるため、私的 CA の署名による証明書（私的証明書）を使用する事が多い。この場合、SP はクライアント証明書に署名した私的 CA を信頼（私的 CA の自己証明書を SP に設置）しなければならない。組織内サービスの場合、その組織が構築した CA の署名によるクライアント証明書でも問題は無い。同一組織内ならば CA と SP を両方とも信頼でき、組織内の私的 CA の自己証明書を安心して SP に設定できる。しかし、CA の自己証明書を全 SP に設定することは簡単ではない。

PKI を一般のサービスで用いる際の、最初の障壁を解消するため、Gutmann らは Plug-and-Play PKI システムを提案している[31]。PKI の認証機構が普及しない理由を分析し、PKI の登録作業を DHCP のように簡単にして PKI の立ち上げサービスを目指している。Gutmann らの PKIBoot は、クライアントと証明書発行者間の相互信頼の初期確立に二つの方法を使うことができる。最初の方法はパスワードの様な秘密共有方式で、二つ目の方法は baby-duck セキュリティモデルの変型で、クライアントは one-time bootstrap 操作を行った最初の発行者を信用する。

Welch らは、MyProxy を提案し[29][30]、かつ MyProxy ミドルウェアの提供[28]も行っている。利用者は MyProxy サーバでのみ利用者認証を行う。その認証方式は ID パスワードや証明書認証を用いる。その後のサービス利用時には、MyProxy が発行する Proxy 証明書を用いる。これにより、セキュリティを考慮しつつ、利用者にとって簡易な利用者認証を実現している。

5.2. 認証局間の信頼関係構築

PKI 手法を用いての利用者認証を単一組織内で行うことは問題が少ない。しかしながら、組織間でサービスを連携する際は問題がある。組織 A の発行した証明

書を、組織 B の SP が信頼するには、予め信頼関係を結ぶ必要がある。組織同士が連携関係にあるならば、信頼関係の構築は可能かもしれない。しかし、公開された環境で多数の組織が連携する場合、他組織の CA を信頼して良いのか分からず、そもそも CA が何処にあるのかも分かりにくい。

そこで、CA の間で信頼関係を構築するために、CA と CA の間をネットワーク構造、ブリッジ構造、木構造で結び、信頼関係を連鎖する仕組みが検討されている。しかし、検討はされているものの現在のところ有効な信頼連鎖機構とは言い難い状況で、PKI 手法での利用者認証連携を構築できていない。

我々は現在、OpenID の仕組みを融合した認証機構を検討している。ネットワーク構造による CA 間の信頼連鎖には、ネットワーク構造の把握が問題になる。OpenID 的な分散機構を考え、CA の信頼度を動的に算出し、その信頼度に基づきサービス提供の可否を決められことのできる仕組みを構築したいと考えている。

6. おわりに

インターネット上の個人向け情報サービスや、組織内向け情報サービスなど、利用者認証を要するサービスが増えている。複数の認証を要するサービスを連携するための、利用者認証連携(ID Federation)が求められている。本稿では組織間の認証連携について仕組みやパラダイムについて述べた。また、我々が研究開発している PKI 手法を用いた認証連携についても説明した。

今後は計画を以下に述べる。まず、PKI と OpenID の仕組みを融合した認証機構を実現する。利用者側の PKI 証明書には、CN の記述形式を OpenID の記述形式とあわせる。SP 側(OpenID のコンシューマ側)には、PKI 証明書処理モジュールの組込みを可能とする。また、全国共同電子認証基盤構築事業(UPKI)に寄与できるように、研究成果や開発システムの公開と、具体的な大学間サービス連携の実現していきたい。

文 献

- [1] 国立情報学研究所: “最先端学術情報基盤 CSI (Cyber Science Infrastructure),” <http://www.nii.ac.jp/research/project-j.shtml#01>, 2005.
- [2] UPKI: “UPKI イニシアティブ,” <https://upki-portal.nii.ac.jp/>, 2005.
- [3] 曾根原登, 岡田仁志, 岡部寿男, 島岡政基, 谷本茂明, 片岡俊幸, 峯尾真一, 渡辺克也: “全国大学共同電子認証基盤 (UPKI) の構築 — 大学間連携電子認証基盤の実現に向けた「UPKI イニシアティブ」構想の提案 —,” シンポジウム「最先端学術情報基盤(CSI) の構築に向けて」, 2006.
- [4] Eisuke Ito, Yoshiaki Kasahara, Megumi Nogita and Takahiko Suzuki: “Institutional authentication platform for trustful inter/intra-institutional

- ubiquitous services”, Proc. of the 2nd International Conference of Ubiquitous Information Technology (2nd ICUT), pp. 103-108, Dec.2007.
- [5] 伊東栄典, のぎ田めぐみ, 笠原義晃, 鈴木孝彦: “認証連携による無線 LAN ローミング環境 —九州大学における UPKI・eduroam の連携—,” 情報処理学会 研究会報告 2007-DPS-132/2007-GN-65/2007-EIP-37, pp.141-146, Sep.2007.
- [6] のぎ田めぐみ, 笠原義晃, 伊東栄典, 鈴木孝彦: “利用者認証に用いる識別子の決定方法に関する考察,” 電子情報通信学会 信学技報 ISEC2006-112, pp. 67-72, Dec.2006.
- [7] 新里卓史, 飯田勝吉, 岸本幸一, 太刀川博之, 昆野長典, 山崎孝治, 伊東利哉, 渡辺治: 大学内の業務・システムと連携するキャンパス共通認証認可システムの構築と運用,” 電子情報通信学会 信学技報 NS2006-197, pp.201-206, Dec.2006.
- [8] 間瀬健二, 平野靖, 梶田将司: “名古屋大学 I D 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, vol.5, no.4, pp. 316-320, Nov.2006.
- [9] 平野靖, 間瀬健二, 梶田将司: “名古屋大学 I D の導入について— (II) 全学 I D からの移行—,” 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, May 2007.
- [10] OASIS, <http://www.oasis-open.org/> .
- [11] OASIS Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security .
- [12] リバティアライアンス, <http://projectliberty.org/jp/> , 2005.
- [13] IPA, “PKI 関連技術解説,” <http://www.ipa.go.jp/security/pki/> .
- [14] The Shibboleth Project, <http://shibboleth.internet2.edu/> , 2000.
- [15] Tom Barton, Jim Basney, Tim Freedman, Tom Scavo, Frank Siebenlist, Von Welch, Rechana Ananthakrishnan, Bill Baker, Monte Goode and Kate Keahey: “ID Federation and Attribute-based AuthZ through the Globus Toolkit, Shibboleth, GridShib, and MyProxy,” Proc. of Internet2 5th Annual PKI R&D Workshop, Apr.2006.
- [16] Globus Alliance, <http://www.globus.org/> , 2003.
- [17] Google, “Google Apps Education Edition,” <http://www.google.com/a/edu/?hl=ja> .
- [18] Licia Florio and Klaas Wierenga: “Eduroam, providing mobility for roaming users,” Proc. of EUNIS 2005, June 2005.
- [19] eduroam.org, <http://www.eduroam.org/> .
- [20] eduroam.jp, <http://www.eduroam.jp/> .
- [21] 後藤英昭, 曾根秀昭: “大学間無線 LAN ローミング eduroam-JP の導入,” 第 29 回全国共同利用情報基盤センター・連合発表会 研究開発論文集 (ISSN: 0910-8769)}, pp.25-27, Oct. 2007.
- [22] TERENA: The Trans-European Research and Education Networking Association, <http://www.terena.org/> .
- [23] APAN: Asia-Pacific Advanced Network, <http://www.apan.net/> .
- [24] B. Aboba and M. Beadles: “The Network Access Identifier,” RFC2486, Jan. 1999.
- [25] OpenID, <http://www.openid.net.jp/> .
- [26] T. Berners-Lee et al.: “Uniform Resource Identifier (URI),” RFC3986, Jan. 2005.
- [27] S. Tuecke, V. Welch, et al.: “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile,” RFC3820, Jun. 2004.
- [28] MyProxy credential management service, <http://grid.ncsa.uiuc.edu/myproxy/> .
- [29] Jason Novotny, Steven Tuecke and Von Welch: “An Online Credential Repository for the Grid: MyProxy,” Proc. of 10th IEEE Int'l Symposium on High Performance Distributed Computing (HPDC-10'01), p.104-111, 2001.
- [30] Jim Basney, Marty Humphrey and Von Welch: “The MyProxy online credential repository,” Software—Practice & Experience, vol.35, issue 9 , pp. 801-816, Jul. 2005.
- [31] Peter Gutmann: “Plug-and-play PKI: a PKI your mother can use,” Proc. of 12th USENIX Security Symposium, pp.45-58, 2003.