社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－132 (25)
2007－GN－ 65 (25)
2007－EIP－ 37 (25)
2007／9／21

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－

伊東 栄典† 笠原 義晃† のぎ田 めぐみ† 鈴木 孝彦†

†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: †{itou, kasahara, megumi, suzuki}@cc.kyushu-u.ac.jp

あらまし 情報サービスの普及と重要化に伴い，安全・安心な情報サービスのための利用者認証が重要になっている．また，組織間でのサービス連携のために，組織間の認証連携についての研究開発が行われている．本稿では，組織間の認証連携の仕組みについてのべ，現在活動している大学間認証連携（UPKI）について説明する．また，認証連携アプリケーションとしての eduroam について述べ，最後に著者らが構築した九州大学の eduroam 環境について述べる．

キーワード 電子認証，認証連携，ＩＤ Federation， UPKI， eduroam， RADIUS， LDAP

Wireless LAN roaming on ID-Federation environment
－A case study for UPKI and eduroam in Kyushu University－

Eisuke Ito, Yoshiaki Kasahara, Megumi Nogita, Takahiko Suzuki

Computing and Communications Center, Kyushu University

6-10-1 Hakozaki, Higashi-ku Fukuoka 812-8581 JAPAN
E-mail: {itou, kasahara, megumi, suzuki}@cc.kyushu-u.ac.jp

Abstract

ID federation is one of important topic for information services. User authentication mechanism must be implemented for secure and personalized services. For inter-institutional services or nationwide services, it need inter-institutional user authentication, but it is very difficult to manage inter-institutional identity data base. ID federation is a solution for this problem. Federated institutions exchange user ID data each other. UPKI project were started by NII and some universities for Japan area ID federation. UPKI team joined eduroam for an application of ID federation. Eduroam is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming. In this paper, the authors describe a case study for UPKI and eduroam in Kyushu University.

Keyword: User authentication, identity management, ＩＤ Federation, UPKI, eduroam, RADIUS, LDAP

1. はじめに

近年，様々なサービスで情報化が進んでいる．大学でも履修登録や成績確認，講義情報提供など，様々な情報サービスが普及している．成績確認などのサービスでは個人の情報を扱うため，扱っている情報が他者に漏れることのないようにする必要がある．このように，情報サービスの個人化・重要化に伴い，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になっている．

利用者認証では従来，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かった．しかし，情報サービスの種類が増大するにつれ ID とパスワードの対が増大し，ID やパスワード忘れの発生が問題になっていた．これは，サービスごとにアカウントを発行していたために発生する問題である．アカウント数が増大すると，備忘のために ID とパスワードを記載した紙を PC の近くに持つなど，他者のアカウント盗用を容易にしてしまう行為をする利用者も増え，安全上の問題になっていた．また，情報サービス提供者側でもアカウント管理の煩雑さが問題になっていた．

そこで，組織内では，組織内で提供される複数の情報システム間でアカウントを統合する ID 統合と，そのための統合認証基盤の構築が行われる様になった．さらに，組織間でも利用者認証を連携する ID Federation または ID Confederation についての研究開発が行われるようになっている．

ID 統合や ID 連携に加えて，利用者認証を ID とパスワードで行うのではなく，IC カードや USB キーなど

の認証トークンを用いた利用者認証についても研究開発および導入が進んでいる．

国内の大学間で認証連携を行うための研究開発として UPKI がある[4][5]．UPKI では，認証連携のアプリケーションとして，無線 LAN ローミング環境の eduroam を展開している[3]．本稿では，著者らの所属する九州大学における UPKI への取り組みと，eduroam 環境の実現について述べる．

2. 組織間認証連携

2.1. 組織内での ID 統合

組織間での認証連携について述べる前に，組織内の認証連携について述べる．前節で述べたように，比較的大規模な組織では，複数の内部向け情報サービスが提供されており，それらを用いるためのアカウントが利用者に対して発行されている．情報サービス毎にアカウントが発行されると利用者も情報サービス提供者側も不便であるため，組織内での利用者 ID 統合が求められている．図 1に単一組織内での ID 統合の概念を示す．

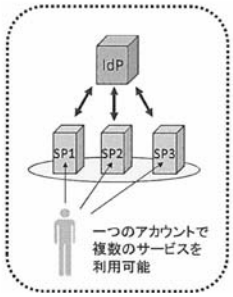

図 1　組織内での ID 統合

ここで，利用者の ID(Identity)の管理・提供元を IdP(Identity Provider)と呼び，情報サービスの提供元を SP(Service Provider)と呼ぶ．組織内の場合，一つの IdP が複数の SP へアカウント情報を提供することに，あまり問題は無い．同一の組織内であれば，利用者は組織内部の者に限られており，通常の組織であれば利用者となる人間の情報は，組織の本部で保持しているためである．企業ならば総務部や人事部，学校であれば事務部といった部門が，組織内の構成員情報を把握している．これらの部門が IdP として利用者 ID 情報を提供すれば，組織内のサービス提供者も IdP の情報を信頼する．利用者認証時には，SP から IdP へのアカウント情報の確認を行う．

2.2. 組織間での ID 連携

近年，情報サービスの拡大に伴い，組織間での認証連携も行われるようになっている．認証連携は，大きく分けて，Web 上の情報サービスでの認証連携，グリッドコンピューティング，無線 LAN 接続環境等の接続サービスの三つがある．最も顕著なのは Web 上の情報サービスでの認証連携である．

Web の拡大に伴い，様々なサービスが Web 上で提供されるようになってきている．近年では，Mash up の様に，複数のサイトで提供されるサービスを跨って一つのサービスとすることが実現されている．また，複数のサイトがサービス内容で連携することもある．例えば，@cosme と Yahoo では利用者の書込み情報を共有している．将来，これらのサイト間で ID 連携が行われる可能性もある．他にも，航空券の購入サイトがクレジットカード決済のサイトと連携するなど，様々な連携が実現されている．

複数の組織が連携して，各組織の所属者にサービスを提供する場合，図 2 に示すように，ある組織の利用者が，別の組織のサービスを利用することになる．その場合，組織間で ID 情報交換についての取り決めを行い，実際に IdP 間で利用者情報のやり取りが行われることになる．

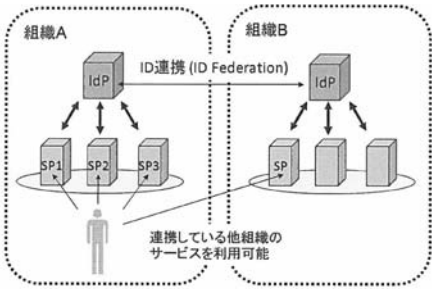

図 2　組織間での ID 連携

2.3. SAML

企業による情報サービスでの認証連携を行うために，リバティアライアンスと名付けられた技術開発・標準化プロジェクトがある[11]．ここではサービス提供者の関係や，利用者の身元情報の交換についてのモデル化を行っている．また Web サービスの分野で認証情報を交換する方式の提案を行っている．身元情報交換のために，SAML(Security Assertion Markup Language)を定義し，公開している．いくつかの Web 関係の Single Sign On システムでは SAML が利用されている．

2.4. Shibboleth

一方，オープンソースの分野でも ID 連携についての研究開発が行われている．例えば米国の Internet2 プロジェクトでは，Shibboleth 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[9]．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 3 に示す．利用者が ID を入力すると，WAYF によりその利用者が所属する組織の IdP を特定し，そちらで利用者本人の認証情報を確認する．これにより多様な組織での認証連携を可能にしている．

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[12]と連携するために，Globus 対応の認証ミドルウェアである GridShib も開発している[10]．

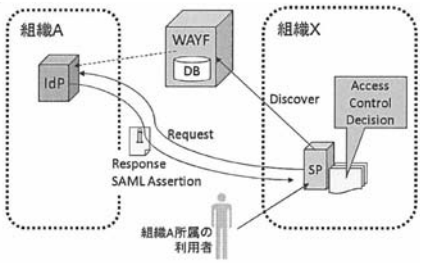

図 3 WAYF

2.5. OpenID

また近年では，無料で Web サイト利用のための利用者 ID（とパスワード）を作成し SP に提供する OpenID[6]というサービスが構築・提供されている．OpenID では，利用者の身元確認するための ID を，URI の形式で構成している．OpenID サイトが IdP となり，ここでは誰もが自分の ID（身元情報）を作成・管理することができる．またサイト作成者は誰でも OpenID を利用するサイトを構築することができる．

3. UPKI

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[15]．CSI では全国の大学や研究所といた学術機関をまたがった情報サービスを行うための学術情報基盤の構築を目指している．そのためには全国に広がる高速ネットワーク，ネットワーク上に提供されるサービス（グリッドやリポジトリ），サービスを利用する人間を制限するための利用者認証基盤が必要である．

UPKI[4][5]は CSI 事業における認証基盤の部分を担っており，大学間連携のための全国共同電子認証基盤について研究開発を行っている．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・パスワードを利用した認証機構についても大学間認証連携の実現を目指している．

UPKI では，各大学における PKI 証明書発行のための指針の提示，認証局 CA 構築のための仕様策定，CA 運用のための方針である CP/CPS の雛型作成などを行っている．これらは利用者の身元情報を PKI の証明書として提示するためのものである．一方，サービス提供者のために，HTTPS サーバ等で使えるサーバ証明書の配布事業も行っている．

UPKI では，認証を用いた大学間連携のアプリケーションの一つとして eduroam[1]の展開を行っている．著者らの所属する九州大学は，国立情報学研究所が主催する CSI 事業および UPKI に参加しており，eduroam の接続・展開実験にも参加している．

4. eduroam

4.1. eduroam とは

eduroam 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 [13]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，認証情報の確認には RADIUS を用いている．

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 ネットワークに接続できる．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，どのような通信が許されているかといった接続ポリシーは無線 LAN 提供機関のポリシーに依存する．

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[14]に関係のあるアジア太平洋諸国の大学が eduroam に参加している．現在 eduroam は連携の連携(federation of federations)，つまり con-federation として発展している．一つの federation を国内での連携とすると，eduroam は欧州の TERENA と，アジア太平洋地域の APAN[14]の，二つの confederation で活動している．

4.2. eduroam の構造

duroam の基本的な構造を図 4 に示す[2]．

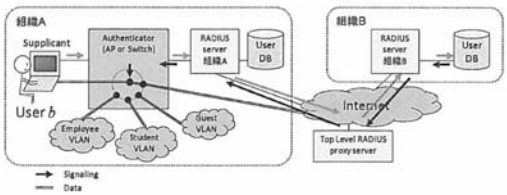

図 4 eduroam の基本的構造

組織 B に所属する利用者 *b* が，組織 A を訪問中であるとする．組織 A が提供する SSID が'eduroam'である無線 LAN 環境において，利用者 *b* は組織 B が発行した身元情報証明書を用いて接続を試みる．組織 A の RADIUS サーバは，利用者 *b* の ID を見て自組織の所属者か否かを判定する．利用者が他組織所属の場合，Proxy として上位の RADIUS サーバに認証情報を転送する．上位の RADIUS サーバによって利用者の ID 文字列に対応する組織の RADIUS サーバが判明した場合（図 4の例では組織 B と判明），その組織の RADIUS サーバに利用者認証の確認を問い合わせる．

具体的には，eduroam を利用する際に利用者は自分の ID として自組織内で利用する ID 文字列に加えて所属組織を表す文字列を付加したものを用いる．利用者 ID は RFC2486[16]で定義される Network Access Identifier 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．ID として入力した文字列の realm を見ることで，RADIUS サーバは利用者の所属組織を探す．realm 文字列が組織 A のものと異なる場合，上位の RADIUS サーバへ認証のための情報を転送する．上位の RADIUS サーバが realm 文字列に対応する組織の RADIUS サーバを知っている場合，そちらに利用者認証の確認をさらに転送することで，最終的に利用者の確認が可能となる．

利用者認証を PKI のエンティティ証明書，すなわち PK12 形式(X.509 形式)で記述された電子証明書を用いて行う場合もある．この場合，RADIUS サーバ側で証明書発行した CA を信頼するならば，問い合わせは発生しない．証明書に記載された内容を信頼することで利用者認証を済ませる

4.3. eduroam.jp

eduroam.jp[3]は UPKI から派生した活動として，国立情報学研究所のネットワーク運営･連携本部 認証作業部会 eduroam グループにより 2006 年に設立された．現在，表 1に示す 6 機関が参加している．

表 1　eduroam.jp 参加組織

機関名	AuthN Used	Access Granted
国立情報学研究所	802.1x	VPN
北海道大学	802.1x	
東北大学	802.1x, TKIP, PEAP	VPN
高エネルギー加速器研究機構	802.1x	
京都大学	802.1x	eduroam_standard
九州大学	802.1x	VPN

eduroam.jp では，研究開発や国内への eduroam の展開のほかに，eduroam の国内レベル RADIUS サーバの運用を行っている．

5. 九州大学における eduroam 環境の構築

ここでは我々が構築した九州大学の eduroam 環境について述べる．図 5に大まかな構成と，表 2に機器構成を示す．

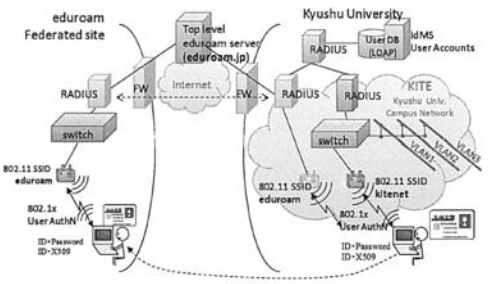

図 5　九州大学の eduroam 環境

表 2　機器構成

用途	機器
802.1x 無線 LAN アクセスポイト	アライドテレシス社製 TenQ AT-TQ2403
RADIUS サーバ	FreeBSD6.2 FreeRADIUS 1.1.6 eduroam.jp 提供 realm 用パッチ

5.1. 接続ポリシー

表 1 には eduroam.jp の接続機関名のほかに，各機関が許している接続形態がある．接続形態として，eduroam standard と，VPN のみの二つがある．eduroam 全体としては，他の接続ポリシーもあるが，日本国内には 2 種類のポリシーしか今のところない．eduroam standard としては，以下の通信プロトコルは制限しない事が求められている[1].

- IPSec VPN, PPTP VPN, SSH, HTTP, HTTPS, IMAP2/3/S, POP/POP3, Passive FTP, SMTP/SMTPS, RDP

一方，VPN のみの場合，訪問者が利用可能な通信プロトコルは VPN しか利用できない．

VPN のみを許す設定にしているのは，自組織内の情報サービスと，組織の IP アドレスが密接に関わっている事や，セキュリティ上の問題があるからである．日本の学術機関では，組織内の情報サービスでのアクセス制御方法として，IP アドレスによる制限をする場合が多い．例えば，電子ジャーナルの閲覧は，自組織の IP アドレスからは可能といった制御をしている．eduroam の接続ポリシーを eduroam standard にすると，契約外の来訪者が電子ジャーナルを閲覧できるといった問題がある．他にも，eduroam standard ならば様々な通信が可能であるため，もし来訪者の PC がウィルス

等に感染している場合などに，他の端末への迷惑がかかる恐れがある．

VPN 接続のみの場合，来訪先のネットワークから直に外部へ接続するではなく，自組織の VPN サーバを経由してインターネットへ接続することになる．この方法であれば，来訪者に自組織内のサービスを使われることもないし，セキュリティ上の問題も回避できる．

5.2. 802.1x での認証方法と認証情報格納方法

九州大学には現在教職員の認証情報を格納した LDAP サーバと，学生の認証情報を格納した Active Directory サーバが存在する．従って，これらのサーバと eduroam の FreeRADIUS サーバが連携することができれば，eduroam の利用者を大学の構成員ほぼ全体に拡大することができる．

LDAP との連携において問題になるのが，eduroam で無線端末の認証に利用する 802.1x プロトコルでの認証方法である．802.1x で主に用いられている代表的なプロトコルに EAP-PEAP と EAP-TTLS がある．これらは非常に似通った設計で実装されているが，互換性はない．EAP-PEAP は ID とパスワードの確認に MS-CHAPv2 を利用する．EAP-TTLS は MS-CHAPv2 以外に PAP 等も利用でき，自由度が高い．Windows 系 OS には標準で EAP-PEAP が搭載されている．

PAP や MS-CHAPv2 を使用する場合，パスワードの格納形式が問題となる．平文パスワードが RADIUS サーバもしくは連携する LDAP サーバなどに登録されていれば，任意のプロトコルで認証が可能である．しかし，一般に平文パスワードをサーバ側に保持することは避けるべきであるため，LDAP のパスワードはハッシュされていることが多い．このような場合，RADIUS サーバ側で LDAP から利用者のパスワードを取得しても認証に利用することができない．

解決方法としては以下の２つが主流である．

(A) パスワードの NThash/LMhash を用意する手法

(B) LDAP 側に認証を移譲する手法

以下，それぞれについて説明する．

(A) パスワードの NThash/LMhash を用意する手法

EAP-PEAP では MS-CHAPv2 を使用しなければならないため，Microsoft 独自の方式（NThash または LMhash）でハッシュしたパスワード文字列が必要である．通常 LDAP はこの形式でパスワードを保持しないが，別途属性を定義しこの形式のパスワードを格納しておき，これを RADIUS サーバから参照可能にすることにより，MS-CHAPv2 での認証が可能となる．問題点としては，LDAP 標準の格納方式ではないため，利用者や管理者のためのパスワード変更インターフェイスが NThash/LMhash でハッシュされたパスワードを生成し LDAP サーバに格納するように実装する必要がある．また，プロトコル的にはこのハッシュされたパスワード文字列があれば認証は可能であるため，これらの文字列は平文パスワードと同様に外部に漏れないよう保護する必要がある．なお EAP-TTLS でも MS-CHAPv2 は利用可能である．

(B) LDAP 側に認証を移譲する手法

NThash/LMhash されたパスワードが用意できず，また LDAP 側に平文パスワードを格納し公開もできない場合，利用者側からパスワード自体を平文で提供してもらうしかない．すなわち，PAP を利用することになる．EAP-PEAP では PAP は利用できないため，この場合は EAP-TTLS しか使用できない．EAP-TTLS では通信は TLS の暗号機能により保護されるため，PAP を利用しても経路上でパスワードを盗聴される恐れはない．

しかし，RADIUS サーバには平文パスワードが見えてしまうことに注意する必要がある．RADIUS サーバに平文パスワードが通知されると，RADIUS サーバは LDAP サーバに対し通知された ID・パスワードで bind を試みる．これが成功すれば，LDAP 側に当該利用者のアカウントが存在することが分かるため，認証が可能となる．ただし，FreeRADIUS 実装では認証時にまずその ID が LDAP サーバに存在するかどうかの検索を実行するため，FreeRADIUS サーバに対し LDAP サーバを検索する権限のあるユーザアカウントを提供し，設定する必要があった．

この手法の問題点としては，認証に PAP を使用しているため，もし悪意のある第三者が eduroam を名乗る基地局と偽の RADIUS サーバを用意すると，そこに接続した利用者の ID とパスワードを盗むことができる，という問題が想定される．この問題を防ぐためには RADIUS サーバの真正性を確認する必要がある．サーバ証明書を RADIUS サーバ側に設定し，利用者側でその証明書の CA を登録しておくことで証明書および RADIUS サーバ真正性を確認できる．

Active Directory は通常外部にパスワード情報を提供しないため，連携するためには RADIUS サーバが Windows ドメインに参加し，利用者から提供されたアカウント情報に基づいて認証可能かどうかを Active Directory に問い合わせる必要がある．FreeRADIUS を利用する場合は，samba を利用してドメインに参加し，samba に付属する外部コマンドを RADIUS サーバから呼び出すことで認証を確認する手法が知られている．

5.3. 証明書付き RADIUS サーバ

九州大学の eduroam 環境では，全学的な認証基盤である LDAP サーバへ利用者情報の問い合わせを行うようにしている．また，認証基盤となるサーバ群の一つにサーバ証明書を設置した RADIUS サーバを用意している．eduroam 用の RADIUS サーバは，proxy になり認

証基盤側の RADIUS へ利用者認証情報の問い合わせを行う．図 6 にシステム構成を示す．

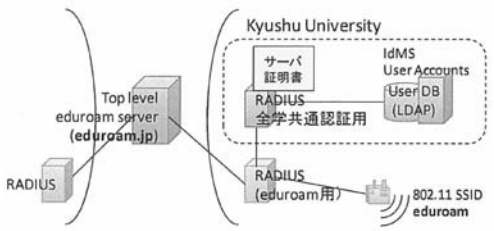

図 6　RADIUS サーバの構成

図 6 に示す方法の利点は，複数の RADIUS サーバがある場合に便利になる．図 5に示すように，九州大学では学内専用の無線 LAN 環境もある．複数のサーバに証明書を設置するのは大変であるため，代表となる一つのサーバに証明書を設置し，後の RADIUS サーバには証明書を設置しないことにした．

5.4. 電子証明書と Windows の 802.1x サプリカント

UPKI 活動の一環で，国立情報学研究所は大学等の学術機関向けにサーバ証明書を発行している[4]．国立情報学研究所が発行する証明書を RADISUS サーバに適用した．証明証用の CSR (Certification Signing Request)は OpenSSL で作成した．

サーバ証明書は Valicert 社が発行するもので，Web ブラウザの HTTPS 通信を行う場合は問題がない．しかし，Windows XP が標準で装備する 802.1x サプリカントとの相性が悪い．図 7に示すように，明示的に信頼されたルート証明機関に入れなければならない．この問題については，改善要求を行う予定である．

図 7　信頼されたルート証明機関の設定

6. おわりに

本稿では，組織間の認証連携の仕組みと，大学間認証連携 UPKI について述べた．また，認証連携アプリケーションとしての eduroam について説明し，著者らが構築した九州大学の eduroam 環境について述べた．九州大学の認証基盤である LDAP サーバと連携する eduroam 環境は構築できた．しかし，Windows XP の 802.1x サプリカントとサーバ証明書との関係に問題があることが分かった．今後は Active Directory との連携や，IC カード等の認証トークンを利用した利用者認証についても調査する予定である．

文　献

[1] eduroam, http://www.eduroam.org/ .

[2] Licia Florio, Klaas Wierenga, “Eduroam, providing mobility for roaming users,” Proc. of EUNIS 2005, June 2005.

[3] eduroam.jp, http://www.eduroam.jp/, 2006.

[4] ＵＰＫＩイニシアティブ, https://upki-portal.nii.ac.jp/ , 2005.

[5] 曽根原登, 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」, Jun 2006.

[6] OpenID, http://www.openid.ne.jp/ .

[7] Simson Garfinkel, Gene Spafford 共著, “UNIX&インターネットセキュリティ第 2 版”, 山口英（監訳）, 谷口功（訳）, オライリージャパン, 東京, pp.245, 1999.

[8] 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.13, 2006.

[9] Shibboleth, http://shibboleth.internet2.edu/, 2000.

[10] Tom Barton, Jim Basney, Tim Freedman, Tom Scavo, Frank Siebenlist, Von Welch, Rechana Ananthakrishanan, Bill Baker, Monte Goode, 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, April 2006.

[11] リバティアライアンス, http://projectliberty.org/jp/, 2005.

[12] Globus Alliance, http://www.globus.org/, 2003.

[13] TERENA:The Trans-European Research and Education Networking Association, http://www.terena.org/ .

[14] APAN:Asia-Pacific Advanced Network, http://www.apan.net/ .

[15] 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.

[16] RFC 2486, “The Network Access Identifier”, January, 1999.