2008－IOT－2 (4)
2008／7／24

認証つきサービスにおける組織間連携のための PKI と OpenID の融合

阿部 英司† 伊東 栄典‡ 笠原 義晃‡ 中國 真教‡

†九州大学システム情報科学府情報理学専攻 〒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: †eiji.abe@i.kyushu-u.ac.jp, ‡{itou,kasahara,nakakuni}@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，特定の組織・グループに属する人のみに向けた情報サービスには，利用者認証が必要である。一方，近年では複数サービスを連携して新たなサービスを構築することに対する要求が高まっている。そのため，サービス連携のための利用者認証連携について研究されている。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進められている。著者らは UPKI に参加しており，組織間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。PKI の仕組みを用いると，強固かつ安全な利用者認証が可能になるものの，認証局の設置や証明書の扱いなど，柔軟な運用が困難である。一方，近年 OpenID と名付けられた利用者認証およびシングルサインオンの仕組みが開発されている。OpenID では柔軟な認証連携が実現できるものの，認証の安全性や強度に問題がある。我々は PKI と OpenID 双方の長所を活かし，PKI と OpenID を融合した認証連携の仕組みを検討した。本稿では，PKI と OpenID を融合した組織間認証連携の機構について説明する。

キーワード PKI, OpenID, ID 統合管理, 利用者認証, ID 連携

A Fusion of PKI and OpenID for inter-domain membership services

Eiji ABE†, Eisuke ITO‡, Yoshiaki KASAHARA‡, and Masanori NAKAKUNI‡

†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: †eiji.abe@i.kyushu-u.ac.jp, ‡{itou,kasahara,nakakuni}@cc.kyushu-u.ac.jp

Abstract Recently, demand for inter-domain service is arising, such as web mash-up services. For inter-domain services, it needs inter-domain user authentication mechanism, because most services are membership oriented, and those services must implement user authentication mechanism. The UPKI project, which is started by NII since 2005, tries to realize PKI-like trust chain in universities. PKI based user authentication is strong and reliable, but it is not flexible. The OpenID mechanism is developed for distributed ID management and web user authentication. Although OpenID is a flexible user management and authentication, OpenID doesn't guarantee trustiness of user identity. We consider a fusion of PKI and OpenID user authentication and ID federation mechanism for inter-domain membership services.

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

1. はじめに

Web 上で公に提供されている情報サービスでも，組織の内部向け情報サービスでも利用者認証を伴うものが増えている。例えば，Gmail 等のメールサービスや mixi 等の SNS サービスでは，個人に特化したサービス（personalized service）を提供するため，利用者認証を行っている。企業や大学といった組織内向けの情報サービスでは，情報漏洩やプライバシー保護のため利用者認証を行うことが多い。例えば大学では，履修登録や成績確認などで利用者認証を行っている。

認証を要する情報サービスの増大に伴い，利用者認証作業が煩雑になってきた。この煩雑さを軽減するために，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）が研究開発されている。Google Apps の様に，同一組織が提供する Web 上の情報サービスでは，提供者側が SSO の仕組みを構築している。

一方，複数のサービスを連携して新たなサービスを構築することが行われるようになった。Web Service と呼ばれる規格・仕組み

が提案されており，SOAP[1], WSDL[2]等の規格制定および実装が進んでいる。また，HTTPの仕組みを用いるREST（Representational State Transfer）と呼ばれるサービス連携も行われている。これらの技術およびスタイルを用い，Web上のサービスを組み合わせて新たなサービスを構築することはマッシュアップ（Mash-up）と呼ばれている。認証を要する情報サービスを組み合わせたサービス連携を実現するには，利用者認証連携も必要である。

国立情報学研究所は，2005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[3]。CSI事業のサブプロジェクトの一つである全国共同電子認証基盤構築（UPKI）[4][5]事業は、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おり，大学間のサービス連携のための認証基盤に関する研究開発を行っている。UPKIでは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。

我々もUPKIに参画しており，組織間サービス連携のための，組織間認証連携の研究を行ってきた[6][7][8]。PKIの仕組みを用いると，強固かつ安全な利用者認証が可能になるものの柔軟な運用が困難である。一方，近年OpenIDと名付けられた分散認証システムが開発されている。OpenIDでは柔軟な認証連携が実現できるものの，認証の安全性や強度に問題がある。我々はPKIとOpenID双方の長所を活かし，PKIとOpenIDを融合した認証連携の仕組みを検討した。本論文では，PKIとOpenIDを融合した認証連携機構について説明する。

2. PKIによる利用者認証の課題

2.1. PKIを用いた認証

PKI（Public Key Infrastructure）は，公開暗号方式をオープンな場で利用するための基盤である[9]。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相互の公開鍵を利用した安全な通信ができるものの，未知の相手の場合には悪意のある者のなりすましが発生する可能性があり，公開鍵を信頼してよいかが問題となる。この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）を設定する。信頼できる第三者が身元審査を行うことで，利用者の公開鍵の真正性を保証する。また，公開鍵に加えて利用者の本人保証も可能になる。これにより強固なエンティティ（自然人やサーバ）認証，つまり身元証明が可能になる。更に通信の暗号化やデータへの署名も可能になる。

PKIでは利用者の公開鍵と個人情報の証明を併せて「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（CA:certificate authority）」と呼ぶ。図1にPKIを用いた利用者認証の概念図を示す。CAは自分用の秘密鍵および公開鍵を作成し，さらにCAの秘密鍵を用いて公開鍵に署名する。これをCAの自己署名証明書と呼ぶ。

サーバや自然人などのエンティティは，自分用の公開鍵・秘密鍵を作成する。このうちの公開鍵に，氏名などの個人情報を添えてCAに送り，CAの秘密鍵での署名を求める。審査を経てCAの秘密鍵で署名されたものが「証明書」になる。

PKIの証明書による，サーバ認証および利用者認証は，証明書の真正性の確認と，公開鍵と秘密鍵を用いた秘密情報交換で行う。証明書の真正性は，CAによる署名がCAの自己署名証明書中の公開鍵で検証できることで確認できる。

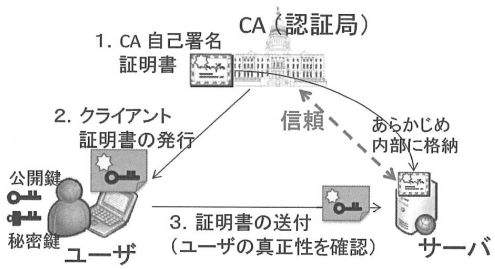

図 1. PKIと証明書による利用者認証

2.2. PKIを用いた組織間認証連携の問題点

PKIの仕組みを用いると強固な認証と安全な通信が可能になる。ただし，証明書の検証に証明書を発行したCAの自己署名証明書が必要である。

サーバ向けの証明書は様々な場面で用いられている。公的（パブリック）CA の自己署名証明書は，多くの Web ブラウザに標準で格納されており，追加の手続きなしに証明書の真正性の確認が可能である。また，公的 CA の証明書は高価であるものの，サーバの信頼性向上に対する費用対効果が十分であるため，証明書の購入・設置が積極的に行われている。

一方，証明書による利用者（クライアント）認証には課題がある。公的 CA の証明書は高価であるため，多くの利用者へ証明書を発行するには経済的な問題がある。

私的（プライベート）CA による証明書発行も考えられる。この場合，利用者認証を行うサーバ側に，私的 CA の自己署名証明書を設置する必要がある。大学などの組織内サービスの場合，その組織が構築した私的 CA の自己署名証明書を各サーバに格納することは，さほど問題が無い。各サーバへの格納や設定作業が煩雑である場合も，SSO 機構の導入などで補うことができる。

しかしながら，異なる組織の間で認証連携を行う場合，私的 CA によるクライアント証明書は問題である。組織 A の私的 CA_A が発行した証明書を，組織 B のサーバが信頼するには，CA_A の自己署名証明書を組織 B のサーバに設定する必要がある。組織同士が密な連携関係にあるならば，自己署名証明書の設置は可能かもしれない。しかし分散環境で多数の組織が連携する場合，他組織の私的 CA を信頼して良いのか分からず，CA の自己署名証明書がどこにあるのかも分かりにくい。

複数の CA 間で，信頼連鎖（trust chain）を構築するために，ブリッジ構造や木構造が検討されている。しかし現在のところ有効な信頼関係連鎖機構とは言い難い状況である。

3. OpenID

3.1. OpenID とは

OpenID は，Brad Fitzpatrick によって開発された，Web アプリケーションのための分散認証システムである[10][11]。OpenID の仕組みを図 2 に示す。

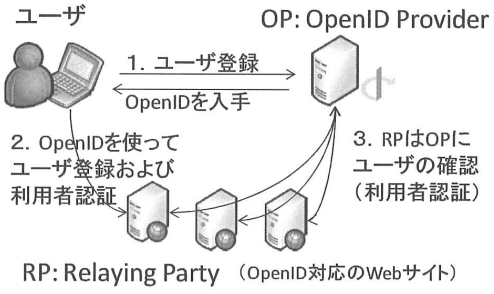

図 2　OpenID の仕組み

OpenID 2.0 では，OP（OpenID Provider）[1] が利用者へのユーザ ID（識別子）を提供する。利用者は OP に登録することで，自分のユーザ ID（OpenID）を得る。また，OP は認証機構（普通はパスワード認証）を持つ。

情報サービスを提供する側は，OpenID では RP（Relaying Party）[2] と呼ばれる。これは，利用者認証を OP にリレーすることから名付けられた。

OpenID はオープン，分散，フリーの認証枠組みであるため，インターネット上にサーバを持つ者なら誰でも OpenID の OP を構築できる。また，サービス側も，認証機能を OpenID 対応の RP とすることが自由にできる。

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[12]形式（および上位互換性のある XRI 形式）になっていることが挙げられる。URI 形式の識別子を用いることで，各 OP 内で一意性を保つだけで，全世界での一意性を保つことができる。また URI 形式にすることで，IdP サーバ発見機構を省略することを可能とした。

OpenID 2.0 からは，利用者が入力する識別子を，http://op.kyushu-u.ac.jp/userid のような形ではなく，op.kyushu-u.ac.jp とだけで指定することが可能になった。これは，利用者の利便性を向上するためのものである。内部の処理は，OpenID 1.1 と同じ URI 形式で表現できるものに対応づけられる。

3.2. OpenID の問題点

OpenID の問題点を二つ述べる。一つは OP

[1] OpenID 1.1 では IdP (Identity Provider)
[2] OpenID 1.1 では Consumer

の信頼性である。OpenIDは，オープン，分散，フリーの認証枠組みであるため，柔軟で便利な面があるものの，見知らぬOPを信頼して良いのかの判断が必要になる。OpenIDの枠組みでは，サービスを提供するRP側は，OPが認証した利用者にサービスを提供することとなる。そこで，信頼できる運営主体により提供されているOPを経由した利用者のみにサービスを提供するような制限が必要となる。

二つ目の問題は，認証の弱さである。多くのOPでは，ID・パスワードによる利用者認証を行っている。そのため，信頼できる運営主体が提供するOPであっても，パスワードを破られると，他人がなりすまして別の利用者となることが可能になる。

組織の重要情報や，プライバシーなどの個人情報を扱うサービスの場合，これらの問題は無視できない。

4. PKIとOpenIDを融合した分散認証

本論文では，PKIとOpenIDの仕組みを融合した認証機構を検討している。PKIの信頼性・強固さと，OpenIDの柔軟性・可用性という双方の長所を活かした分散認証基盤を構築し，それをWeb上のサービスで用いることを考えている。

4.1. PKIとOpenIDを融合した認証連携の仕組み

本研究で考えた，PKIとOpenIDを融合した認証連携の仕組みを述べる。図3にその概念図を示す。

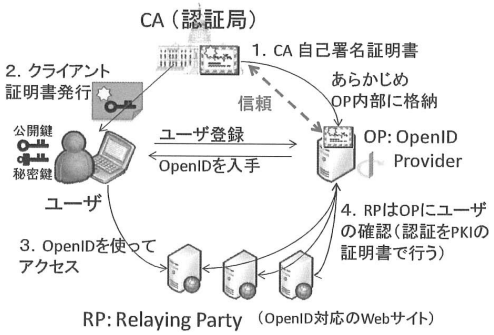

図3　PKIとOpenIDを融合した認証

利用者は，OpenIDのRPとなっている情報サービスで，認証のためのOpenIDを入力フォームに入れる。RPは，OpenIDの文字列から，その利用者のOPを特定し，認証処理のためにOPへリダイレクトする。利用者は，OP側で認証処理を行う際，クライアント証明書を用いた認証を行う。OPは認証結果をRPに送り，RPはサービス提供の可否を決める。

4.2. システムの試作および評価

PKIとOpenIDを用いた認証システムを試作した。まず，FreeBSD上でOpenSSLを用いて利用者証明書を発行するCAを構築した。CA用の公開鍵および秘密鍵を作成し，自己署名証明書を発行した。次にOPを，Ruby on Railsのパッケージの一つであるruby-openid libraryを用いて構築した。Ruby on RailsにはWebサーバ機能が含まれるため，構築したOPをWebサーバとしての動作させることができた。OPが持つべきPKIの証明書による利用者認証機能は，Rubyのopensslおよびbase64モジュールを用いて作成した。最後に，RP側の具体的なサービスとしてはWikiを提供した。試作システムは環境を表1に示す。なお，試作した認証システムは，OpenID 1.1のみに対応している。

表1　試作システムの環境

種類	名称	Version
OS	FreeBSD	6.2
SSL library	OpenSSL	0.9.8
言語	Ruby	1.8.5
Web Application Frame Work	Ruby on Rails	1.2.5
OpenID package	Ruby-openid	1.1.4

試作したシステムを用い，PKIとOpenIDによる認証が可能であるかを確認した。RPとなるサービス提供サイトに初めてアクセスすると，認証済みではないため，図4のRPの認証要求ページへリダイレクトされた。OpenID入力フォームにOpenIDを入力すると，図5のOPへリダイレクトされた。そこで，CAが発行したクライアント証明書を用いて認証を行った。認証に成功すると図6のサービス提供ページ(Wiki)が利用可能になった。

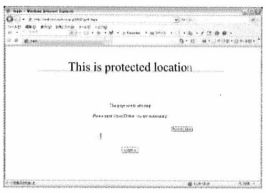

図 4　RP での OpenID 入力

図 5　OP での認証

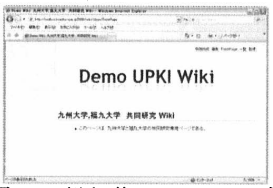

図 6　認証後の RP ページ

次に処理速度を調べた。OP での認証時に利用者が証明書を送付してから，認証成功後に RP にリダイレクトされるまでの平均時間は，約 2msec だった。サービスの認証処理速度としては実用的といえる。しかし，この処理時間調査は単一アクセスにおける処理であった。一般のサービスでは認証要求が集中する場合も多い。今後，並列アクセスでの処理時間調査が必要である。

5. 組織間認証連携における提案方式の有効性

5.1. 認証連携

本論文で提案する PKI と OpenID を融合した分散認証環境を，組織間の認証連携に適用する場合について述べる。

まず，想定する前提を述べる。サービスを受ける利用者はどこかの組織に属しているものとし，その組織は所属者のアカウントを管理するものとする。また，その組織は，自組織の所属者を認証するための OP を運用するものとする。最後に，組織は所属者に認証用のクライアント証明書を配付するものとする。クライアント証明書を発行する CA は，公的 CA でも私的 CA でもかまわない。その組織の提供する OP が，組織所属者の持つクライアント証明書を検証できればよい。

図 7 に，組織間での認証連携の様子を示す。各組織の所属者は，サービス利用時に RP から自組織の OP へリダイレクトされる。そこで，自組織から発行されたクライアント証明書を用いて利用者認証を行う。

私的 CA の発行するクライアント証明書でも利用できるため，経済的な問題が少なく，導入しやすい。

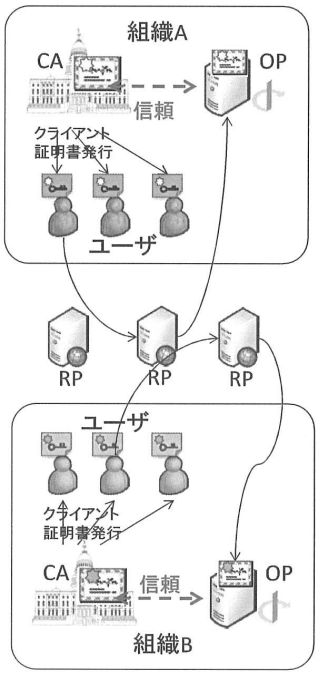

図 7　PKI と OpenID を融合した組織間認証連携

5.2. 信頼性確保方法の検討

元々の OpenID では OP を個人または組織で自由に設立可能であり，認証ポリシーも自由に決定可能である。そのため，PKI と OpenID を融合した組織連携では，三つの信頼性問題が発生する。

一つ目の問題は，利用者から見た OP の信頼性である。この問題に関しては，OP 側にサーバ証明書を導入することにより OP サーバのなりすましを防止できる。

二つ目の問題は，OP から見た利用者の信頼性である。これは OP と利用者間の認証に PKI を用いることにより利用者のなりすましを防止できる。

三つ目の問題は，RP から見た OP の信頼性である。前述のように，OP にサーバ証明書を導入することで，OP サーバの真正性を確認できる。加えて，信頼できる OP のリストを RP 側で共有する方法（共有ホワイトリスト）も考えられる。

UPKI で想定する大学間認証連携では，大学が提供する OP のホスト名を，ある種の名前に制限することで，信頼性を向上することが可能かもしれない。

6. おわりに

インターネット上の個人向けサービスや，組織内向け情報サービスなど，個人に特化したサービスやプライバシー情報を扱うサービスでは利用開始時に利用者認証が必要である。利用する利用者認証を介する情報サービス数が増加するにつれ，利用者側から複数サービス間の連携への要求が高まってきており、そのための利用者認証連携が求められている。

本論文では PKI と OpenID についてその仕組みやパラダイムについて述べた。それを踏まえて，著者が研究・開発している PKI と OpenID を融合した認証連携について述べた。またシステムを試作し実用性を確認した。

今後の課題として，実用システムとしての規模適応性の検証や利用者増大時の処理速度測定等の評価が必要である。評価を行うとともに，その結果に基づいた改良を加え，PKI と OpenID を融合した認証連携の機能面と性能面の両面でより実用レベルに近づける。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を実現していきたい。

文　献

[1] E. O'Tuathail et al.: “SOAP version 1.2 Part 0: Primer (Second Edition)”, http://www.w3.org/TR/soap12-part0/ , 27 April 2007.

[2] Christensen, et al.: “Web Services Description Language （ WSDL ） 1.1”, http://www.w3.org/TR/wsdl , 15 March 2001.

[3] 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.

[4] UPKI: “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」, 2006.

[6] 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.

[7] 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.

[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.2006.

[9] IPA, “PKI 関連技術解説,” http://www.ipa.go.jp/security/pki/ .

[10] OpenID, http://www.openid.net/ .

[11] OpenID Authentication 2.0 － Final, http://openid.net/specs/openid-authentication-2_0.html , Dec. 2007.

[12] T. Berners-Lee et al.: “Uniform Resource Identifier (URI),” RFC3986, Jan. 2005.