

集中管理における属性情報委譲に関する一考察

柿崎 淑郎^{†1}

近年、OpenID などによるシングルサインオン技術に利用が普及し始めている。シングルサインオン技術により、1 つの ID で複数のサービスを利用することができる。また、ID を管理している主体に名前やメールアドレスなどの属性情報を登録しておくことで、あるサービスを利用する際に必要なアカウント作成や情報の登録に際して、属性情報を交換することで、利用者の負担を軽減することができる。このように、ID を管理している主体が属性情報を集中管理することで、属性情報の活発で簡便な利活用が可能になるが、信頼できる属性情報の集約には問題がある。一般に、信頼できる属性情報は信頼できる第三者機関によって証明されているか、またはその属性情報を付与された本人が証明できなくてはならない。そのため、ID を管理している主体が様々な属性情報を全て証明することは困難であり、属性認証局等の異なる機関によって証明された属性情報を委譲されて管理する必要がある。本稿では、属性情報を集中管理する際における、委譲に関して考察を行い、現在利用可能な技術によって、その利用可能性を検討する。

A consideration of delegation for attribute information in centralized management

KAKIZAKI YOSHIO^{†1}

Recently, Single-Sign-On technique has spread widely. Many services can be used with only one ID and password by Single-Sign-On technique. Moreover, the user's load can be reduced by registering attribute information which is exchanged at the account creating. Thus, attribute information becomes more useful because ID provider intensively manages it. However, there is a problem in consolidating attribute information that can be trusted. In this paper, I consider the delegation when attribute information is intensively managed, and examine the possibility of usage.

1. はじめに

Web サービスを利用する際に、我々はいくつかの個人情報を提供している。その中でも、住所、年齢、性別などはユーザの属性を示す情報で、本稿では属性情報と呼ぶ。属性情報は有効期間の長さや効果の範囲などの違いにより、数多く存在し、その取り扱いも様々である。属性情報は Web サービスの登録時や利用時などに利用され、その都度、サービス提供者の要求に基づき、利用者が属性情報を提供することが多い。そのため、属性情報の再利用などの有効活用は、利用者の利便性を向上させる意味でも重要である。

多くの属性情報は利用者の主張に基づくことが多い。利用者の属性情報を厳密に確認しようとした場合、利用者が主張するか属性情報が正しいかどうかを検証し、証明できる主体はごく限られた機関だけである。また、その主体が全ての属性情報を証明できるかといえば、そうではない。例えば、学会は学会員であることを証明できるが、その人がどこの所属であるかについては証明できない。逆もまた然りで、大学は所属する学生を証明できるが、どこの学会に所属しているかは証明できない。

一般的に各属性情報はそれを証明することができる機関によって発行されるので、その管理もその機関に依るところが大きい。しかしながら、実際に属性情報を利活用することを考えた場合、一カ所に集中して管理されている方が良い。属性情報を属性プロバイダ等に集中管理する場合、各認証機関から属性プロバイダに権限委譲を行う必要がある。つまり、トラストアンカーを各認証機関から属性プロバイダに委譲することで、属性プロバイダが属性情報を提供することができるようになる。

属性情報を有効に利活用するためにはその利便性が重要となる。数多くある属性情報をその利用用途に合わせて使う場合に、利便性を重視すると各属性情報が集中管理されることが望ましい。しかしながら、ID 情報の集中管理と異なり、属性情報の集中管理には、その属性情報の正当性や有効性の検証が必要となる。そのため、属性情報を集中管理する機関はその管理する属性情報が確かであることを証明できることが必要になる。一般的に、属性情報の正当性を証明することは特定のエンティティしかできない場合が多い。例えば、

市在住であることを証明できるのは市役所などの公的機関に限られ、それ以外の機関では属性情報を主張しているに過ぎず、信頼できる根拠が与えられない。そのため、属性情報

^{†1} 東京理科大学
Tokyo University of Science

を集中管理するには大きな障害がある。

文献 1), 2) では属性情報が集中管理されている状況下で, OpenID AX を用いて属性交換をする際の信頼度に関する提案が行われている。しかしながら, 属性情報の集中管理をどのように実現するかについては示されていない。本稿では, 属性情報を集中管理する際の問題点について検討する。特に, 属性情報を検証し, 保証することができる機関は, 限定されていることが多い。そのため, 属性情報の委譲について検討を行う。

2. 関連技術

2.1 OpenID

OpenID^{3),4)} は URI (Uniform Resource Identifier) または XRI (Extensible Resource Identifier) を識別子とするユーザ中心の分散認証サービスである。OpenID では以下の 3 つのエンティティを用いる。

OP OpenID Provider はユーザが主張する identifier を認証するエンティティ。

RP Relying Party はユーザを認証するために OP に認証を依頼するエンティティ。

ユーザ ユーザは自身の ID である identifier を主張し OP より認証される。

認証を必要とする場面では, 認証者は被認証者を認証するために, 例えば ID とパスワードの対などが必要となる。このとき, 異なる認証者に対して, 同じ ID とパスワードの対を利用している場合, 悪意ある認証者が被認証者になりすまし, 他の認証者を欺くことが可能となる。OpenID では, 各 RP はユーザを認証するための情報は持たず, OP のみがユーザを認証するための情報を持っている。そのため, RP はユーザを認証することができないので, OP に対してユーザの認証を依頼し, RP はその認証結果を用いる。この際, ユーザが主張する ID は 1 つの identifier であるため, OpenID の仕組みを用いる RP に対して, OpenID はシングルサインオン環境を提供することができる。

OpenID Attribute Exchange (AX)⁵⁾ は属性交換のための OpenID 拡張仕様の 1 つである。AX は OpenID に対応した Web サイト間でやり取りするユーザの属性情報の交換方法について定めていて, AX によって, RP は OP が管理しているユーザの属性情報を取得および更新することができる。AX で交換可能な属性情報の種類は axschema.org^{*1} や openid.net^{*2} などによって, あらかじめいくつかの型が定義されている。また, 属性交換

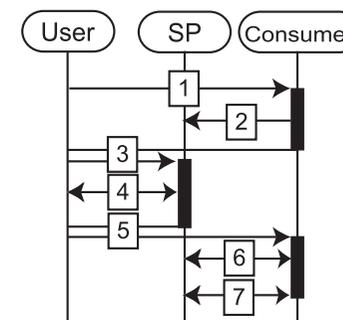


図 1 OAuth の認可フロー

において取得のみができ, AX よりも限定された属性情報のみを取り扱える sreg (Simple Registration) もある。

2.2 OAuth

OAuth⁶⁾ はトークンを利用することで認証を必要とせず, ユーザの同意の下に API へのアクセス権を認可する仕組みである。API へアクセスする単純な方式として, 利用者の ID とパスワードを利用して, API にアクセスすることが考えられるが, 認証に必要な ID とパスワードを用いるために利用者の持つ全権限を行使できてしまう問題がある。それに対して, OAuth では利用者の ID とパスワードを教えることなく, ある特定の API へのアクセスを認可したトークンを用いることで, 必要以上の権限が行使できないようにすることができる。OAuth の認可フローを図 1 に示す。OAuth の認可は以下のように行われる。

- (1) User は Consumer に対して OAuth の開始を指示する。
- (2) Consumer は SP にアクセスし, 未認可のリクエストトークンを取得する。
- (3) Consumer は未認可のリクエストトークンを付けて, User を SP にリダイレクトする。
- (4) SP は User を認証し, Consumer の認可を行う。
- (5) SP は認可済のリクエストトークンを付けて, User を Consumer にリダイレクトする。
- (6) Consumer は User から認可済のリクエストトークンを受け取り, それを用いて SP からアクセストークンを取得する。
- (7) Consumer はアクセストークンを用いて User の権限を行使する。

ユーザは手順 4 においてコンシューマのアクセス権を認可している。この際, コンシューマがどのような API にアクセスするかは, ユーザが確認できるようになっている。また,

*1 <http://www.axschema.org/types/>

*2 <http://openid.net/specs/openid-attribute-properties-list-1.0-01.html>

手順 6 以降、コンシューマはアクセストークンを用いることで、API にアクセスする毎にユーザの許可を得る必要がなくなる。以後、ユーザがコンシューマの API へのアクセスを取り消したい場合は、SP に対してアクセストークンを無効にするように指示すればよい。

3. 集中管理における属性情報委譲

本研究の位置付けは千葉らの提案している属性プロバイダ⁷⁾に近い。文献 7) ではネットワーク上に分散された個人情報情報を仮想的に集約、提供する共通基盤によって、個人情報を管理、活用するビジネスモデルとして、属性情報プロバイダが提案されている。属性プロバイダによって、利用者はネットワーク上に登録した自分の情報の内容や所在を確認でき、新たなサービス事業者への送付や変更手続きが簡易に行うことができる。また、属性プロバイダの要件として、以下の 4 点を挙げている。

- (1) 属性のタイプに則した登録書式や型の統一化
- (2) 属性の真正性の確認情報の付加
- (3) 属性確認・更新のワンストップ化
- (4) 属性データの保存、送受信システム使用の共通化および外部監査による安全性レベル維持

本稿では特に、属性プロバイダの要件 (2) 「属性の真正性の確認情報の付加」についての検討を行う。

電子商取引推進協議会の報告書⁸⁾では、実社会での現行の属性の登録・照会の仕組みにおける課題として、以下を挙げている。

分散する登録機関 属性は多数の独立した機関で登録・管理されており、登録機関どうしての情報の交換を行うことはない。このため、各機関ごとに属性変更の手続きを行わなければならない、大変な手間となっている。

困難な手続き 不動産登記などの一部の手続きでは、登録の手続きが複雑で、本人が手続きすることが難しく、専門家・専門業者が代行する状況である。

選択できない属性項目 証明書には複数の属性項目が記されているが、これらすべての属性項目が必要とは限らない。戸籍情報など、必要以上の属性を第三者にさらすことは、トラブルの原因になることもあり、好ましいとはいえない。

本人確認手段の限界 実社会では窓口担当者が対面および簡単な書類で確認するのが限界であり、なりすましによって、重要な属性を照会されたり、属性が変更されることがある。また、属性が変更されたことを本人に別途通知する制度・仕組みがないため、本人

は属性が変更されたことに気付くことができない。

属性値保証の限界 属性によっては属性値が変化しやすい属性がある。紙媒体の証明書では属性の状態が交付時のものであり、リアルタイムの属性値ではない。情報の処理速度向上にともない、各種属性値がリアルタイムに要求される可能性がある。

公的登録制度のない属性 顔写真やサインなど、今後のビジネスシーンで使われることが予想される属性であっても、公的な登録の仕組みがないものがある。

本稿では上記課題のうち、「分散する登録機関」および「属性値保証の限界」について検討を行う。

これら文献 7), 8) は属性情報の有効活用を考えたときに解決すべき課題を挙げている。特に、利用者の利便性を向上させ、負担を軽減するために、属性情報の集中管理が取り上げられている。しかしながら、次節で説明するように、属性情報は ID 情報と違い、認証者以外が代理で認証を行うことが困難である。そのため、属性情報を集中管理するためには、その属性情報を適切に委譲する必要がある。

3.1 信頼点委譲の問題点

ID とパスワードの対を用いて利用者認証を行う場合、認証者は被認証者が主張する ID とパスワードの対が正しいかどうかを確認することで、利用者認証を実施することができる。このとき、ID とパスワードの対を認証者から代理認証者に委譲することで、代理認証者は被認証者が主張する ID とパスワードの対が正しいかどうかを確認ことができ、認証者が行う利用者認証と同じことを実施することができる。

これらの利用者認証を代理認証者が行うことができるのは、ID とパスワードの対や電子証明書などが利用者認証を行うための根拠となっているためである。そのため、認証者が用いる利用者認証に必要な根拠を持ち合わせれば、認証者以外の主体に対して認証の権限を委譲すれば、権限を委譲された主体は認証者に替わり代理で認証を行うことが可能である。

しかしながら、属性情報は ID 情報と異なり、認証に必要な情報 (根拠) を委譲すれば誰でもが認証できるものではない。

属性情報は多種多様に存在するが、種類によっては特定の主体しかその属性情報の正当性を証明することができない属性情報もある。多くの場合、属性情報は

そのため、特定の主体のみが利用者の属性情報を認証することができても、それ以外の主体が属性認証を行うことは一般的に困難である。

文献 1), 2) では OpenID AX を用いて、集中管理されている属性情報を属性交換する際

に、交換される属性情報がどの程度信頼できる情報なのかを示す付加情報を付けることで、属性情報をより有効活用しようとする試みが提案されている。しかしながら、これら文献においても、属性情報を集中管理する際における属性の管理権限または認証権限の委譲に関する考察が行われていない。そこで、本稿では文献 1), 2) の方式で検討されていない属性管理における権限委譲に関する考察を行う。

3.2 信頼点委譲の考察

文献 1), 2) では、属性情報を認証した主体ではない属性プロバイダに情報を集中管理させることで、OpenID AX における属性交換がより広範に利用できるようになることを期待し、信頼できる根拠を付加する目的で、OpenID AX のパラメータを拡張した。しかしながら、そのパラメータが与えるべき根拠となる信頼点が未だ属性を管理する属性プロバイダではなく、属性を認証した主体のみである。また、OpenID AX を用いて、属性を認証した主体から属性プロバイダに対して、属性に関する情報を譲渡してはいるが、3 節で説明したように、属性情報は多種多様であり、その有効期限も様々である。そのため、OpenID AX を用いる属性情報の譲渡では信頼性が十分ではない。これは OpenID AX プロトコルが必ずユーザを介する必要があるためである。つまり、属性プロバイダが属性情報の信頼性を確保するために、属性を認証した主体から最新の情報を取得しようとした場合、必ずユーザを介して要求する必要がある。

3.3 OAuth を利用した属性情報の委譲

そこで、本稿では最新情報の取得の度にユーザの同意を取ることなく、属性プロバイダが任意のタイミングで属性を認証した主体から属性情報の委譲を受けられるようにするため、OAuth を利用した属性情報の委譲を提案する。本稿では OpenID AX と OAuth によって、属性情報委譲の実現を考える。以下に各エンティティの説明をする。属性プロバイダ AP は属性情報を集中管理する信頼できる第三者機関であり、OpenID Provider (OP) でもある。サービスプロバイダ SP は利用者の属性情報を認証した上で管理している機関である。リライティングパーティ RP は属性情報を取得しようとする機関である。利用者 User は RP のサービスを利用するために、OpenID AX によって AP から属性情報を RP に提供する。

図 2 に OAuth による属性情報委譲のフローを示す。図 2 中の赤矢印は OpenID、緑矢印は API、黒矢印は OAuth の通信を示している。

- (0) User は AP に OpenID でログインを行う。
- (1) User は AP に対して OAuth の開始を指示する。
- (2) AP は SP にアクセスし、未認可のリクエストトークンを取得する。

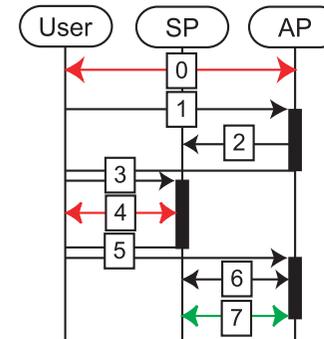


図 2 OAuth による属性情報委譲のフロー

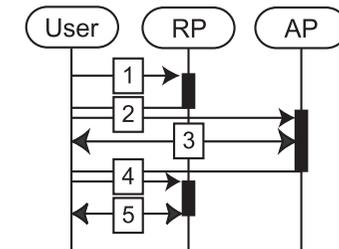


図 3 OpenID AX による属性交換のフロー

- (3) AP は未認可のリクエストトークンを付けて、User を SP にリダイレクトする。
- (4) SP は OpenID で User を認証し (手順 0 にて既に認証済)、AP の認可を行う。
- (5) SP は認可済のリクエストトークンを付けて、User を AP にリダイレクトする。
- (6) AP は User から認可済のリクエストトークンを受け取り、それをを用いて SP からアクセストークンを取得する。
- (7) AP はアクセストークンを用いて User の権限を行使し、属性情報を取り出す。

AP が SP に OAuth でアクセスするに先立ち、AP は User を認証しておく必要がある。ここでは属性交換に OpenID AX を用いることから、AP での認証も OpenID を用いることで、AP と SP でシングルサインオンが利用できる状況としている。手順 1 から 6 は 2.2 節で説明した手順通りである。ここで、手順 4 において SP は User を認証する必要があるが、手順 0 にて OpenID を用いた認証が行われているので、SP ではシングルサインオンを利用して認証済の状態となる。また手順 4 では、AP が要求している属性情報の取り出しを SP が User に問い合わせた上で、認可判断を行う。最後に手順 7 で、AP は SP から User から認可を受けた権限を行使して、User の属性情報を取り出す。これによって、AP は User から認可された状況下で、SP から属性情報の委譲を受けることができ、SP にある属性情報の信頼点を AP に委譲することができる。

なお、この手順には OpenID OAuth Extension ^{*1} を適用することで、いくつかの手順を

*1 OpenID Extension の 1 つであり、OpenID プロトコルと OAuth プロトコルの一部を共有することで、OAuth プロトコルの一部を簡略化することができる。

簡略化することが可能である。

次に、委譲された属性情報を文献 1), 2) の方式で属性交換することを考える。OpenID AX による属性交換のフローを図 3 に示す。

- (1) User は RP に OpenID でログインを行う。
- (2) RP は User を認証できる AP に User をリダイレクトすると同時に、OpenID AX による属性交換を要求する。
- (3) AP は User を認証し、要求されている属性交換の許可を取る。
- (4) AP は認証結果と User によって許可された属性情報を付けて、User を AP にリダイレクトする。
- (5) RP は属性交換によって得られた属性情報を用いて、User にサービスを提供する。

User は RP のサービスを利用するために、手順 2 において IdP である AP で OpenID 認証を受けると同時に、RP からの OpenID AX による属性交換要求を AP に伝える。AP は User を OpenID 認証した後に、RP からの属性交換要求に応じた属性交換の可否を User に確認する。手順 4 において、通常の OpenID では認証結果のみが返される所、RP が要求し User が許可した属性情報も、OpenID AX によって同時に RP へ送られる。この際に OpenID AX で交換される属性情報は、OAuth によって AP が SP から取得した属性情報である。

4. 検討・考察

文献 1), 2) の方式は、交換する属性情報に信頼できる根拠を付加することで、属性情報の有効活用を行う方式である。しかしながら、OpenID AX で属性情報を有効活用する場合、属性情報を集中管理する必要があり、属性情報の譲渡・委譲の問題があった。OpenID AX の仕組みで属性情報の委譲を行う場合、AP が SP から属性情報を取り出すそうとする度に、必ず User の同意を必要とする。つまり、User を介さなくては、AP は SP から属性情報を取り出すことができない。

本稿では属性情報を取り出す度に User を介する非実用的な方法を改善すべく、OAuth を用いる方式を提案した。OAuth を用いる場合、User によって許可された AP はアクセストークンを用いて、SP にアクセスする度に User の同意を得ることなく、許可された範囲で SP へのアクセスが可能となる。OAuth によって AP は SP の持つ属性情報へのアクセス権を持つ。そのため、User や RP から見た場合、AP は SP の代理人のように見える。

属性情報の委譲ならびに SP へのアクセスは、OAuth のアクセストークンによって許可

されている。そのため、AP のアクセストークンを無効にすれば、SP へのアクセスはできなくなる。

5. ま と め

本稿では文献^{1),2)}の方式に対して、属性情報の信頼度のための根拠を与えるために、OAuth を用いた属性情報の委譲に関して考察を行った。OAuth を用いることで、属性情報の取得に際して、その都度ユーザの介入を必要とせず、またユーザが属性情報の公開を取りやめたい場合に、即座に属性情報の取得を停止させることができる。これによって、属性情報を委譲して集中的に管理することができようになり、OpenID AX などを用いた属性交換がより容易に行える。

参 考 文 献

- 1) 柿崎淑郎, 岩村恵市. 属性登録と属性交換の保証についての考察. コンピュータセキュリティシンポジウム 2009, pp. 637-642, October 2009. E6-4.
- 2) Y.Kakizaki and K.Iwamura. A consideration of the reliability of registration and attribute exchange. In *Proc. of Fifth International Conference on Availability, Reliability and Security (ARES-2010)*, pp. 574-579. IEEE CS, February 2010.
- 3) D.Recordon and D.Reed. OpenID 2.0: a platform for user-centric identity management. In *Proc. of the second ACM workshop on Digital identity management (DIM '06)*, pp. 11-16, New York, NY, USA, 2006. ACM.
- 4) OpenID Authentication 2.0, 2007. <http://openid.net/specs/openid-authentication-2.0.html>.
- 5) D.Hardt, J.Bufu, and J.Hoyt. OpenID Attribute Exchange 1.0, 2007. <http://openid.net/specs/openid-attribute-exchange-1.0.html>.
- 6) The OAuth Core 1.0 Protocol, 2009. <http://tools.ietf.org/html/draft-hammer-oauth-08>.
- 7) 千葉昌幸, 漆嵐賢二, 前田陽二. 属性情報プロバイダ: 安全な個人属性の活用基盤の提言. 情報処理学会論文誌, Vol.47, No.3, pp. 676-685, 2006.
- 8) 電子商取引推進協議会. 属性情報利用システム - 2010 年の市民生活 -, 2004. <http://www.ecom.jp/results/results15.html>.