Vol.2012-IS-121 No.1
2012/9/10

検証された属性に関する一考察

柿崎 淑郎[1,a)]

概要：ユーザは同意の下で属性情報をサービス提供者に提供するが，サービス提供者はそれらが正しいかどうかを検証するのは簡単ではない．そのため，提供される属性が確かに正しいと示すことは，ユーザ，サービス提供者の双方にとって有意義である．本稿では，ユーザの属性をオンラインで提供する場合に，その属性を検証する手段，またその信頼度について，検討を行う．

キーワード：属性情報，属性交換，アイデンティティ管理

A Consideration of Verified Attributes

KAKIZAKI Yoshio[1,a)]

Abstract: It is not easy for the service provider to verify whether attribute information is correct though the user offers it to the service provider under agreement. Therefore, verifying exchanged attributes is significant for both users and service providers. In this report, we consider about way to verify attributes and their reliabilities, when user's attributes are exchanged online.

Keywords: Attribute Information, Attribute Exchange, Identity Management,

1. はじめに

オンラインサービスが普及し，多くの活動がネット上で行われるようになり，様々な情報の流通に大きな関心が集まっている．特に，システムやサービスのクラウド化が進み，近年ではビッグデータと呼ばれる情報資産の利活用に注目が集まっている．

こうした時代の変化に対応するため，EU では 2012 年 1 月に，ユーザがデータの削除を要請できる権利として，**忘れられる権利 (right to be forgotten)** を提唱した [1]．さらに，アメリカでは 2012 年 2 月に行政白書 [2] において，**消費者プライバシ権利章典 (Consumer Privacy Bill of Rights)** として，次の権利が提唱されている．

(1) 個人毎のコントロール
(2) 透明性
(3) コンテキストの尊重
(4) 安全性
(5) アクセスと正確性
(6) 対象を絞った収集
(7) 説明責任

このように，流通する大量の情報は資産であるとともに，個人のプライバシでもあり，慎重な検討が行われている．

一方で，ユーザ同意の下で情報を利用する場合でも，プライバシとは違う問題がある．オンラインショッピングをする際に，私たちは名前，住所，電話番号などの情報提供を要求される．また，年齢や性別を尋ねられる機会も少なくない．このように，サービス提供者から要求されるユーザに関する情報のことを，本稿では総称して**属性情報**と呼ぶこととする．ユーザは同意の下でこれらの属性情報をサービス提供者に提供したとしても，サービス提供者はそれらが正しいかどうかを検証するのは簡単ではない．そのため，提供される属性が確かに正しいと示すことは，ユーザ，サービス提供者の双方にとって有意義である．

本稿では，ユーザの属性をオンラインで提供する場合に，その属性を検証する手段，またその信頼度について，検討

[1] 東京理科大学
Tokyo University of Science
[a)] kakizaki@ee.kagu.tus.ac.jp

© 2012 Information Processing Society of Japan

を行う．まず，属性交換に関連する技術について紹介を行い，次に，実際に属性交換される可能性が高い属性について，その検証可能性を考察する．最後に，検証された属性の信頼度について検討を行う．

2. 属性情報

属性情報とは，その主体が持つ属性・権限・職責・資格・地位などであり，個人に付随し，その集合はアイデンティティを形作る．属性情報は以下の観点から分類することができる [3].

時間経過に伴って変化するかどうか

- 先天的に変化しない属性情報
  生年月日，バイオメトリクス情報など
- 後天的に付加されるが変化しない属性情報
  学歴・職歴などの経歴，賞罰など
- 時間的にあまり変化しない属性情報
  資格，免許，職業，住所など
- 時間的に変化しやすい属性情報
  所属，職責，権限，資産など

信頼できるかどうか

属性情報は通用するコミュニティの範囲が異なる場合があり，コミュニティごとに信頼される属性情報が異なる．

- 公に通用する属性情報
  住民基本情報，商業登記情報，資格，免許など
- あるコミュニティ内でのみ通用する属性情報
  職責，会員資格など

知られてもよいかどうか

- 知られてもよい属性情報
- 知られたくない属性情報

必要かどうか

- 一般的に共通な属性情報
- サービスを利用するうえで必要とする属性情報
- サービスを利用するうえで必要としない属性情報

文献 [4] ではネットワーク上に分散された個人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．属性情報プロバイダによって，ユーザ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，属性情報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

文献 [5] では，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．

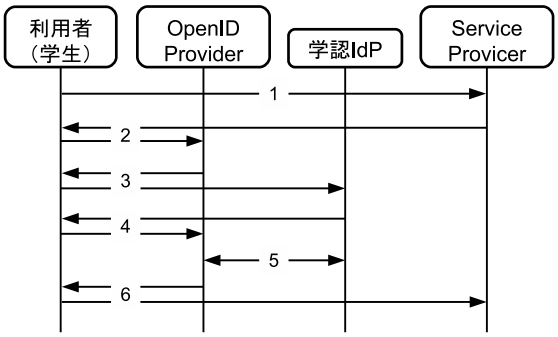

図 1 SITF による学割のシーケンス図

- 散在する登録機関
- 困難な手続き
- 選択できない属性項目
- 本人確認手段の限界
- 属性値保証の限界
- 公的登録制度のない属性

本稿では上記課題のうち，「散在する登録機関」および「属性値保証の限界」について検討を行う．「散在する登録機関」とは属性は多数の独立した機関で登録・管理されており，登録機関同士での情報の交換（同期）を行うことはなく，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問題のことである．「属性値保証の限界」とは属性値が変化しやすい属性の問題である．発行された属性の証明書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を反映しているとは限らない．状況によっては，各種属性値をリアルタイムに要求されることもあり，その保証をどのように行うのかは課題である．

3. 関連技術

3.1 学生 ID 向けトラストフレームワーク

OpenID ファウンデーション・ジャパンと学術認証フェデレーション（学認，GakuNin）[6] が検討しているトラストの仕組みとして**学生 ID 向けトラストフレームワーク (Student Identity Trust Framework; SITF)** がある．SITF では，大学 IdP が学生であることを保証することによって，オンラインで学割を実現するフレームワーク案を示している．

SITF のプレイヤとして，学割を利用しようとする利用者（学生），利用者が通常利用している OpenID プロバイダ，学生属性を提供する属性プロバイダとしての学認 IdP (Identity Provider)，学割を提供するサービスプロバイダの 4 者がある．OpenID プロバイダは，OpenID プロバイダと学認 IdP 間でポリシ合意があれば，学認に属する大学以外の民間企業が運営していても良い．また，サービスプロバイダは OpenID に対応するリライングパーティ（RP）である．

図 1 に SITF による学割のシーケンス図の例を示す．学

© 2012 Information Processing Society of Japan

表 1 学認で扱う属性

属性名	内容
mail	メールアドレス
sn	姓
o	組織名
ou	組織内所属名称
givenName	名
displayName	表示名
eduPersonAffiliation	職種
eduPersonPrincipalName	フェデレーション内共通識別子
eduPersonEntitlement	資格
eduPersonScopedAffiliation	組織内職種
eduPersonTargetedID	フェデレーション内匿名識別子
jasn	姓（日本語）
jaGivenName	名（日本語）
jaDisplayName	表示名（日本語）
jao	組織名（日本語）
jaou	組織内所属名称（日本語）

割の利用時は以下の手順を行う．

(1) 利用者は学割を提供しているサービスプロバイダにアクセスする．
(2) サービスプロバイダは利用者を認証できる OpenID プロバイダに利用者を転送する．
(3) OpenID プロバイダは利用者を認証後に，学生属性を得るために利用者を学認 IdP に転送する．
(4) 学認 IdP は利用者を認証後に，リソースアクセスに必要な情報を付けて，利用者を OpenID プロバイダに転送する．
(5) OpenID プロバイダは学認 IdP にアクセスし，学生属性を取得する．
(6) OpenID プロバイダは認証結果と学生属性を付けて，利用者をサービスプロバイダに転送する．

SITF では，学認の一部の機能を使い，学生属性の保証を目指している．通常，学生であるかどうかを保証できる機関はその当人が所属する大学 IdP だけである．学認では，それら大学 IdP を 1 つのトラストフレームワークにまとめることができ，SITF は対象の学生が確かに学生であることを保証することができる．サービスプロバイダに学生属性を提供する OpenID プロバイダは，学認 IdP とポリシ合意をしているため，OpenID プロバイダから提供される学生属性は検証された正確な情報である．そのため，学生属性を利用しようとするサービスプロバイダは学認からの属性を活用することができる．

学認は SAML を利用しており，SITF で使われる学生属性以外の属性も利用されている．表 1 に学認で扱う属性を示す[*1]．この中で，SITF では組織名と職種を提供し，学生であることを証明する．職種は属性値として，”faculty”，”staff”，”student”，”member”，無し（空白）を取り得る[*2]．学生であるかどうかは，職種の属性値が”student”であるかどうかで判別される．

[*1] https://www.gakunin.jp/docs/fed/technical/attribute

表 2 OpenID Connect で予約されている属性

属性名	内容
name	表示可能なフルネーム
given_name	ファーストネーム
family_name	ラストネーム
middle_name	ミドルネーム
nickname	ニックネーム
preferred_username	略記名
profile	プロフィール
picture	プロフィール写真
website	Web ページまたはブログ
email	E メールアドレス
gender	性別
birthday	生年月日
phone_number	電話番号
address	住所

3.2 OpenID Connect

OpenID Connect[7] は OAuth 2.0[8] をベースにした技術であり，アクセストークンを用いて属性を取得することができ，OpenID の次期標準として策定が進められている．OpenID の次期標準であり，現在策定が進められている．OpenID Connect で予約されている属性の一部を表 2 に示す[*3]．

表 2 の中で，email には email_verified があり，検証済みの場合は”true”，そうでなければ”false”を示すことができる．それ以外の属性には検証済みかどうかを示す項目はなく，得られた属性値が信頼できるかどうかは不明である．

4. 属性の検証と信頼度

2 章で示したように，文献 [4] では属性プロバイダの要件を挙げている．属性を払い出す IdP が属性プロバイダとして機能するためには，これらの要件を満たす必要がある．現状においては，属性プロバイダの要件 1,4 は満たされているため，本稿では，要件 2「属性の真正性の確認情報の付加」および要件 3「属性確認・更新のワンストップ化」について検討する．文献 [4] では，要件 2 は「登録した属性について，第三者が確認した場合に，確認者や手段などの情報を付加できるようにする．これにより利用時点での属性の信頼度合いを属性を利用する側が判断できるようになる」としており，要件 3 は「サービス事業者に登録された本人の属性を集約して照会し，また必要に応じて更新できるようにする．これにより，属性が変わった場合でも各サービス事業者に逐一通知する負担や忘失を減らすことが

[*2] https://www.gakunin.jp/docs/fed/technical/attribute/eduPersonAffiliation
[*3] http://openid.net/specs/openid-connect-basic-1_0.html#id_res

© 2012 Information Processing Society of Japan

できる」としている．

学認の場合，大学がIdPを担っているため，属性値の信頼度は高く，また大学は表1に挙げられている属性が正しいかどうかを確認することができる．例えば，組織名，職種は正確であるし，メールアドレスも自らが発行したものであれば正確である．一方で，改姓があったや職種が変わった場合などに，その情報を正しく反映させているかどうかは，各IdPの運用による．

次に，OpenID Connectの場合，IdPは一般的なポータルサイトなどが担うことが多い．ポータルサイトは利用登録の際に，いくつかの属性情報をユーザに要求する．しかし，その属性の多くを検証することなく，ユーザの主張をそのまま登録することが少なくない．そのため，これらの属性はUserInfo requestのために予約されているものの，どのような手段で登録されたか，どのように検証されているかについては保証しない．よって，SPは属性交換によってユーザの属性を簡単に取得できるが，その信頼性は従来と変わらず低く，属性プロバイダの要件は満たされない．

4.1 機械的に検証可能な属性

OpenID Connectのような一般的なIdPが属性の信頼性のために，属性の検証を行い，登録・管理をすることを考える．まず，機械的に検証可能な属性について検討する．

Eメールアドレスは，オンラインにおける数少ない連絡手段であるため，その有効性確認を行うことは珍しくない．一般的には，ユーザ登録時に登録確認メールを対象のEメールアドレスに送り，そのメール内に書かれている本登録ためのURLにアクセスすることで，受信者が確かに登録したユーザであると確認することができ，その有効性確認が行われる．

Webページやブログの所有者を確認する手段としては，いくつかの方法がある．OpenIDのHTML-Based discovery [9]では，HTML中に特定のタグを入れ込む方法を使っている．Google SitemapやAnalyticsでは，特定のファイルを置いたり，HTML中に特定のスクリプトファイルを設置したりすることで，確認を行っている．

電話番号の有効性検証ではなく，セキュリティを強化する目的で，Google [*4] やFacebook [*5] が電話番号やSMS (Short Message Service) を用いた本人確認を採用している．この方法では，ユーザの電話に音声またはSMSでPINコードが送られ，それをユーザが正しく受け取れることで，その所有権を確認している．この背景には，携帯電話の契約に際しては，キャリアが現実世界での本人確認を厳密に行っていることが挙げられる．

[*4] https://support.google.com/accounts/bin/answer.py?hl=ja&answer=114129
[*5] https://www.facebook.com/help/security/security_features#approvals

表 3 属性の検証可能性

属性名	検証可能性
name	△
given_name	△
family_name	△
middle_name	△
nickname	×
preferred_username	×
profile	×
picture	△または×
website	○
email	○
gender	△
birthday	△
phone_number	○
address	△

4.2 非機械的に検証可能な属性

次に，機械的または即時的には検証できないが，何らかの手段で検証可能な属性を検討する．

オンラインアイデンティティが持つ名前，性別，生年月日を検証するのは難しい．日本においては，個人の氏名，住所，性別，生年月日を基本4情報と呼んでいる．そのため，これらの検証をするためには，オンラインアイデンティティと現実世界の個人が結びつかなくてはならない．つまり，行政機関の発行する証明書やそれに類するものが，検証には必要となる．具体的には，現実世界におけるパスポートや免許証などによる身分証確認に相当する行為が必要となる．

ポータルサイトでもショッピングサイト等の実世界における配送を伴う場合，配送した荷物が到達することによって，住所の真正性は確かめられる．Google AdSenseでは，PINコードを郵送することでユーザの住所を確認している[*6]．

5. 検討・考察

以上の結果を表3に示す．表3において，○は機械的に，△は非機械的に検証可能，×は検証不可能または検証不要を表す．表3の結果は属性の検証可能性を示したもので，必ずしも検証されるとは限らない．

表3より，オンラインで検証可能な属性は，機械的に検証可能である．対して，非機械的に検証可能なものは，オンラインでの検証が困難な属性である．現状では，氏名，住所，性別，生年月日のいわゆる基本4情報のオンラインにおける公的登録制度はないため，現実世界における本人確認が必要となる．また，ニックネームや略記名を検証する手段はなく，検証の必要性もない．

このように，属性交換される属性においても，その検証

[*6] https://support.google.com/adsense/bin/answer.py?hl=ja&answer=157667

© 2012 Information Processing Society of Japan

可能性を考えた場合に，検証が容易でない属性が多くあり，その信頼度は十分にあるとは言いがたい状況である．

SITF の場合，信頼できる学生属性を保証できる機関は，その当人が所属する大学 IdP だけである．この時，大学 IdP は属性プロバイダに相当する役割であり，連携先である OpenID プロバイダに学生属性が集約され，OpenID プロバイダが属性を払い出す IdP としての属性プロバイダとして機能する．SITF における IdP は属性プロバイダの要件 [4] の全てを満たしている．サービスプロバイダに払い出される学生属性は，SITF の仕組みで保証されているため，要件 2「属性の真正性の確認情報の付加」を満たしている．また，要件 3「属性確認・更新のワンストップ化」については，OpenID プロバイダに属性が集約されており，容易に属性交換が可能であり，満たされていると考えられる．

SITF の場合，学生属性という限定された属性だけだが，学認 IdP が利用者の存在確認と属性の検証を行っているため，信頼度が高い属性交換が行える．この属性交換はオンラインで行われるが，属性検証などの保証にかかる部分は現実世界での接点があり，現実世界の実体と属性の紐付けが信頼性の基本となっている．

OpenID Connect のような任意の IdP では，SITF のようなトラストフレームワークの仕組みがまだない．そのため，属性プロバイダの要件 2,3 が満たされない．特に，要件 3 を満たすためには，SITF と同様に，トラストフレームワークが必要になると考えられる．

先述したように，基本 4 情報の信頼性は求められる一方で，公的登録制度が無いために，高い信頼性は与えられない．しかし，現実には一定の信頼性を確保する手段はある．例えば，住所属性の場合，宅配業者であれば，配送するという確認手段によって，その属性の妥当性を検証しているといえる．そのため，宅配業者が住所属性を（ある程度）保証する属性プロバイダとなることは考えられる．同様にして，電話番号であれば，その電話番号を払い出す通信事業者が保証すれば，その信頼性は高くなる．

このように，OpenID Connect のような任意の IdP が連携する場合においても，属性を検証可能な属性プロバイダから提供された属性か否かによって，その信頼度に差が出ることとなる．このような側面から，文献 [10] においては，複数の属性認証機関から属性プロバイダに属性を集約する際に，その属性値の保証手法について検討している．また，文献 [11] においては，OpenID Connect の distributed claims を用いることで，複数の分散した属性プロバイダから属性を集約できることが示されている．

6. まとめ

本稿では，属性交換される属性情報について，その検証可能性と信頼度について検討を行った．E メールアドレスや電話番号など，オンラインで検証可能な属性は，機械的に検証可能であるのに対して，氏名，住所，性別，生年月日などのオンラインで検証が困難な属性は，非機械的にのみ検証可能が可能であることを示した．また，ニックネームや略記名などの一部の属性は，属性交換される属性ではあるが，検証の必要性はない．このように属性の検証可能性に差があるため，属性交換で得られた属性に必ずしも信頼性があるとは限らない．さらに，SITF においては，学生属性という限定された属性のみであるが，学認 IdP が属性プロバイダとしての要件を満たしていることを示した．

参考文献

[1] The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF, accessed Jul. 30, 2012.
[2] Consumer Data Privacy in a Networked World. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, accessed Jul. 30, 2012.
[3] 電子商取引推進協議会. 属性認証ハンドブック, 2005. http://www.jipdec.or.jp/archives/ecom/results/h16seika/h16results-08.pdf, accessed Aug. 6, 2012.
[4] 千葉昌幸, 漆嶌賢二, 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.
[5] 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.jipdec.or.jp/archives/ecom/results/h15seika/h15results-15.pdf, accessed Aug. 6, 2012.
[6] 学術認証フェデレーション. https://www.gakunin.jp/ja/, accessed Aug. 1, 2012.
[7] OpenID Connect 1.0 draft, 2012. http://openid.net/connect/, accessed Aug. 1, 2012.
[8] D. Recordon and D. Hardt. The OAuth 2.0 Authorization Framework, Internet-Draft, 2012. http://oauth.net/2/, accessed Aug. 1, 2012.
[9] OpenID Authentication 2.0, 2007. http://openid.net/specs/openid-authentication-2_0.html, accessed Aug. 1, 2012.
[10] 柿崎淑郎, 前田千徳, 岩村惠市. 属性交換における属性値保証. コンピュータセキュリティシンポジウム 2011, pp. 247–252, 2D1-2, 2011.
[11] Y. Kakizaki and H. Tsuji. A decentralized attribute management method and its implementation. *International Journal of Information Processing and Management*, Vol. 3, No. 1, pp. 61–69, 2012.
[12] 柿崎淑郎, 岩村惠市. 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, E6-4, 2009.
[13] 柿崎淑郎. 属性情報の集中管理における委譲と利用. 情報処理学会論文誌, Vol. 52, No. 2, pp. 723–731, 2011.
[14] 柿崎淑郎, 前田千徳, 岩村惠市. OpenID における属性情報の登録と活用に関する提案. コンピュータセキュリティシンポジウム 2010, pp. 435–440, 2F2-3, 2010.

© 2012 Information Processing Society of Japan