2009-IOT-4 (10)
2009 / 3 / 5

本人確認基盤と公開 ID の提案
－Web 横断的な匿名本人確認と OpenID の有用性について－

岡下　綾

日本電気株式会社サービスプラットフォーム研究所 〒211-8666 神奈川県川崎市中原区下沼部 1753
E-mail:　aya@az.jp.nec.com

あらまし　ウェブ上の多くの仮想世界において，ユーザのプライバシーを保護するために本人確認を行うことなく匿名でのアカウント登録が行われている．そのためユーザは複数のアカウントとそれに付随した権利を不正に利用することができる．また，属性の類似した仮想人格（ペルソナ）同士が同一視されてしまうことで，ユーザの権利が他者によって不正に利用され得るという問題がある．ユーザのペルソナは複数の仮想世界をまたいで利用され得る．そのため，ユーザが情報資源の所有権を主張したり他者によるなりすましを回避するためには横断的なペルソナ同一性の証明手段が必要である．本研究ではペルソナに対応した公開 ID に関して考察を行う．また分散認証技術である OpenID を利用した本人確認基盤アーキテクチャを提案する．

キーワード　OpenID，認証，本人確認，匿名，ペルソナ

A Proposal of Distributed Authentication Platform and Public Identifiers
－On Appropriateness of Web Traversal Anonymous Authentication using OpenID－

Aya OKASHITA

Service Platforms Research Laboratories, NEC Corporation　1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa 211-8666, Japan

E-mail:　aya@az.jp.nec.com

Abstract　In many virtual worlds on the Web, the account registration by anonymity is done without doing the personal identification to protect user's privacy. Therefore, a user can easily have many rights as multiple accounts. Moreover, it is difficult for third party to distinguish users' virtual characters(which is called persona) that have similar attributes. Users may manage some different persona comprehensively. Hence, the means of persona identification is necessary for the user to insist on the property right of information resources and to avoid the identity theft by others. This paper proposed a distributed authentication platform with OpenID, and the necessary condition of public identifiers which is corresponds to user's personas.

Keyword　OpenID，Authentication，Personal Identification，Anonymous，Electorical Persona

1. はじめに

ウェブ上に点在する仮想世界，例えばオンラインゲームや SNS などのコミュニティサービスにおいて，一人のユーザが多重アカウントを取得することで複数の権利を取得したり，他者になりすますことで他者の権利を利用することが容易に行えることが問題となっている．例えば，一人のユーザが独立した多数の人格として認識されることによる自作自演詐欺や投票・多数決における不正行為，口コミ情報の誘導や，アンケートやランキング結果の操作，オークションにおける価格吊り上げ，グループメンバーの不正な水増しなどを行うことで，情報の信頼性を激しく低下させるなど深刻な影響があり，悪質なユーザを迅速に発見してペナルティを与えることなどが求められている．しかしながら,個人情報の取扱いには厳重な注意が必要であり，複数のアカウント取得を阻止するためにユーザの本人確認を行うことは容易ではない．さらに，複数の仮想世界をまたいでユーザのペルソナ（仮想人格）が利用されていることから，ペルソナの所有者同一性が第三者機関によって保証されることが求められている．

本研究では仮想世界におけるユーザのペルソナに対応可能な公開 ID の要件について検討し，ユーザの実体に対応したサービス固有の本人 ID と公開 ID とをサービス運営者に提供するための本人確認基盤アーキテクチャを提案し, OpenID を採用することの有用性について検討した．

以下，2 章では仮想世界で用いられるペルソナと多重アカウントに関する用語の定義や背景となる課題について述べ，3 章において本人確認基盤について説明し，4 章でまとめと今後の課題について述べる．

2. 背景

2.1. ペルソナ

ユーザの実体をペルソナの集合と定義する．ペルソナとは個人の属性の部分集合であり，個人の社会的な顔であると定義されている[1]．ある男性が会社では社会人の顔を持ち，家では父親という顔を持つとき，これらの立場的な顔もペルソナと呼ばれる．ユーザは実世界において一つの実体を持ち，実体に紐付いた多数のペルソナを所有している．ユーザが自ら意識してペルソナの使い分けをする場合，ユーザ自身が設定したセグメンテーションによって切り分けが行われるのが自然と考えられる．例えば，ブログに記述する内容を仕事とプライベートな趣味に関するものに切り分けるために，二つ以上の異なるブログを管理することは現在でも行われている．

仮想世界におけるペルソナは実世界のペルソナと同一のものとして扱われる場合もあり，全く異なる架空の存在として区別される場合もある．オンラインゲームなど世界観や役割に合わせたキャラクターを演じて楽しむロールプレイが目的とされる場合，ユーザのペルソナは個人の実体とは異なる属性を持ち得る．ユーザは複数の仮想世界において複数のペルソナを多次元的に管理し，状況に併せて使い分けている．

仮想世界 W におけるユーザの実体の集合を Ew, ペルソナの集合を Pw，アカウントの集合を Iw，属性の集合を Aw とする．Ew, Pw, Aw の各要素をノードとし，$\forall e \in Ew$ に対して e に紐付いたすべてのペルソナに対応する Pw のノードにリンクが存在し，$\forall p \in Pw$ に対して p が持つすべての属性に対応する Aw のノードにリンクが存在するようなグラフをペルソナモデルと定義する．ペルソナモデルの例を図 1 に示す．仮想世界における実体の像として認識されるペルソナは，アカウントとの組で実体により管理される．図 2 に示すアカウントの例において，佐藤という実体はアカウント guest によってペルソナ「匿名」を管理し，アカウント sato によってペルソナ「父親」と「部長」を管理している．アカウント guest は複数人によって用いられることを前提とした共有アカウントであり，利便性を高めるために用いられることがある．本研究では共有アカウントは検討範囲に入れておらず，アカウントに紐付く実体は一つであることを前提としている．また，複数の実体によって管理される共有ペルソナについても検討せず，ペルソナに紐付く実体は一つとする．従って，ペルソナ p1,p2 の所有者が同一であるとは，各ペルソナを所有する実体の集合 Ep1,Ep2 に対して Ep1=Ep2，|Ep1|=|Ep2|=1 が成り立つことである．

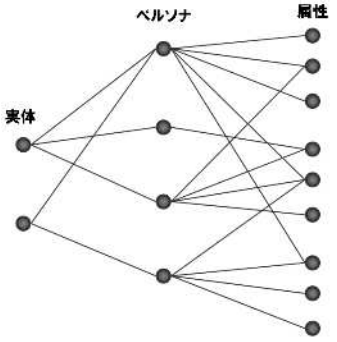

図 1：ペルソナモデルの例

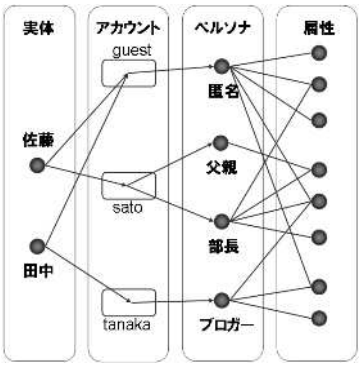

図 2：アカウントの例

仮想世界においてペルソナは社会的評判や人間関係などの情報資源を所有している．よって，異なるペルソナの所有者が同一であると認められる場合には情報資源の併合が行われ得ることから，所有者同一性は重要な要素となる．

ウェブサービスの多様化により，複数の仮想世界にまたがってペルソナを管理するユーザは確実に増加しており，今後も増え続けることが予想される．異なる仮想世界 W1,W2 においてユーザ u が管理しているペルソナをそれぞれ P1，P2 とする．ペルソナと実体との紐付け情報はプライバシー保護のために隠蔽されるため，通常の場合 P1 と P2 の所有者がユーザ u であることを知ることができるのはユーザ u のみである．サービス運営者または第三者による名寄せを防ぐために仮想世界ごとに異なるペルソナとして認識されたいユーザがいる一方で，自己を晒す欲求や仮想世界におけるステータス形成のためにペルソナの所有者同一性証明を必要とするユーザも存在する．また他者が自身のペルソナと類似の属性を持つペルソナを持つことで，第三者から所有者同一性を疑われた場合には，二つのペルソナの所有者が同一ではないことを証明したい場合もある．

自分だけが知る情報を不特定多数の第三者に証明することは困難であり，他者に対して自身の所有するペルソナの所有者同一性を証明する手段は共通 ID を

利用していない限り基本的には自己申告によって行われている．ペルソナの主体を SNS などの連絡が可能な場に常駐させ，関係者に対してブログなどで同一性を公開することで信頼性を高める手法もとられているが完全ではない．

以上により，仮想世界をまたいでペルソナの所有者同一性を隠したい場合は隠し，公開したい場合には公開でき，異なる所有者によるペルソナは異なるものであることを証明できる手段が必要と考えられる．

2.2. 多重アカウント

ある仮想世界においてユーザ u が多重アカウントを持つとは，ある同一の時間的タイミングにおいて u の実体のみが利用可能なアカウント集合の濃度が 2 以上であることと定義する．

ユーザが多重アカウントを所持することで，ペルソナを利用した詐欺行為が容易となる．例えば，ユーザが自身の利益または他者の不利益のために自作自演による詐欺行為を行うこと，捨てアカウントを作成することで不正行為によるアカウント停止処分を受けた場合の損失影響を小さくすることなどが考えられる．

ユーザが時間と資源と気力の許す限り多重アカウントを作成し続けることで，実体は一人であっても多数派であるように見せかけることが可能であり，また多数の権利を得ることができる．サービス運営者によってはユーザに対して多重アカウントを禁止したり，違反者の ID を一時停止または削除するといったペナルティ対応をとっている．また，違反常習者のアカウント登録を拒否することでサービス価値を守ることも行われている．

しかし，ユーザが同一人物であるかどうかを判断するための手段は非常に少ない．サービス運営者はユーザの行動ログ，IP アドレス，Cookie，携帯電話の端末識別番号などの情報から総合的に判断するしかないが，完全な判断は不可能である．例えば，同じ PC 環境を利用している家族の ID や，友人同士で ID とパスワードを共有している場合，ネットカフェなど不特定多数のユーザが利用可能な共有環境での利用，ID 盗難や ID 共有による不正アクセスなど見分けのつかない状況も多く存在する．また，本人確認をせずにユーザ同士が同一人物ではないことを知るための確実性の高い手段はほとんど存在しない．

個人情報による本人確認には多大な運用コストがかかる上に，ユーザは信頼のないサービス運営者に対して個人情報を伝えたくない場合がある．このような理由から，個人運営などの小規模サービスにおいて本人確認を行うことは非常に難しい．

2.3. 公開 ID

ユーザが同一の仮想世界において多数の権利や他者の権利を行使することを禁止するためには，運営者が行為の主体であるペルソナの所有者同一性を把握する必要がある．また，ユーザが第三者に対するペルソナ同一性の公開を自らの意思で制御できるようにするためにはペルソナに関する公開情報が必要である．ペルソナの所有者同一性は公開情報にできないため，これらの問題を解決するためには一つの識別子では足りず，運営者に対する ID と第三者に対する ID の二つが必要と考えられる．

サービス運営者に対してユーザが実世界の誰なのかを明かすことなく本人であることを証明できるような個人に一つの ID（以下，本人 ID と呼ぶ）を発行する必要性や技術については様々な検討が行われている [2,3]．

第三者に対してペルソナの同一性に関する情報を通知するためには，すべての仮想世界に共通の ID が必要であり，ユーザが労力を費やすことなくすべての第三者に連絡するためには公開された ID を用いることが有効であると考えられる．

公開 ID の要件について，次にまとめる．

(1) ユーザの個人情報を用いることなく同一性を確認できること，
(2) ユーザが自身の意思で同一性を証明できること，
(3) ユーザが自身の意思で同一性を隠蔽できること，
(4) 異なる実体に紐付いている公開 ID は異なるものとして認識されること，
(5) 以上の項目をユーザが仮想世界をまたいで実現できること．

3. 本人確認基盤

ユーザが一つしかない本人 ID を使って各サービス運営者に認証を要求する場合，各サービス運営者がパスワードを共有しなければならずセキュリティ上の問題がある．よって外部の認証機関に認証を委託する分散型の認証連携技術が有効である．

ウェブサイトをまたいだ認証連携を普及させるためには技術的課題だけでなく，ID プロバイダによる政治的な課題も解決されなければならない．ID プロバイダが ID によるユーザの囲い込みを望んだとしても，すべてのユーザを独占することは現実問題として困難であり，ユーザ自身が ID プロバイダを自由に選択できる環境を用意することが全体としての利用者増加に繋がると考えられる．

以上の課題を解決すべく，本研究ではウェブ横断的な認証技術である OpenID に着目し，本人 ID としての

有用性について検討を行った．

3.1. OpenID

OpenID は複数のウェブサイトに共通の ID でログインするための分散認証技術である．ユーザに OpenID を発行し認証を行う主体を OP(OpenID Provider）と呼び，ユーザが利用するサービスを提供する主体を RP(Relying Party)と呼ぶ．OP は複数存在し，ユーザはどの OP の OpenID を用いるかを選択できる．また，RP は認証を外部機関に委託できるため，管理コストを低減できるといったメリットがある．

OpenID2.0 の仕様において，ユーザが OpenID を用いて RP にログインする際の大まかな流れは次のようになる．

(1) ユーザが OP のドメイン名を RP に通知する，
(2) RP はユーザを OP のログイン画面にリダイレクトする，
(3) ユーザはログイン画面で OP のローカルなユーザ ID とパスワードを入力する，
(4) OP はユーザの認証を行い，検証が成功した後で RP がユーザを識別するための ID(Claimed Identifier)を RP に通知する，
(5) OP はユーザを RP にリダイレクトし，処理は終了する．

RP がユーザを識別するための Claimed Identifier は図 3 に示すような URL 形式の ID であり，OP のドメイン情報を表すドメイン部とユーザを識別する情報を表すユーザ識別部とから成る．

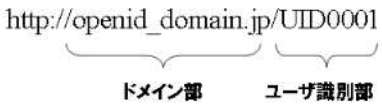

図 3：Claimed Identifier の例

各 OP がユーザ識別部に本人 ID を記述することで，RP に対してユーザの本人性を証明することは可能であると考えられる．しかしこの場合，複数の RP に対して共通の本人 ID を用いると RP 同士が本人 ID とユーザの紐付け情報を開示することで名寄せが可能となり，ユーザのプライバシーが守られないといった問題がある．

3.2. 本人確認基盤のアーキテクチャ

サービス運営者による名寄せを防ぐために本人 ID は RP ごとに異なるサービス固有の ID(以下，サービス固有 ID と呼ぶ)を用いることが有効である．本人確認用 ID に OpenID を用いることで，ユーザは一つの ID を記憶するだけで名寄せを防ぎつつ複数のサービスにログインすることができるため，有用性が高いと考えられる．本節では，ウェブにおいて OpenID を自らの身分証明書のように利用するためのプラットフォームとして本人確認基盤を提案する．図 4 に本人確認基盤の概要を示す．

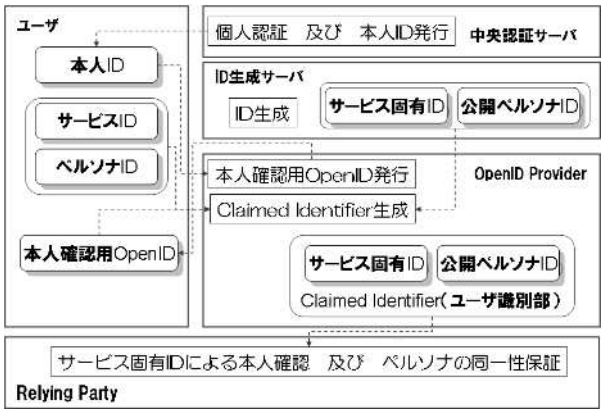

図 4：本人確認基盤の概要

本人確認基盤はユーザとユーザが利用するサービスの運営者である RP の他に，ユーザの個人認証と本人 ID の発行を行う中央認証サーバと，本人確認用 OpenID の発行と RP に認証結果として返すための Claimed Identifier の生成を行う OP とサービス固有 ID と公開ペルソナ ID を生成する ID 生成サーバとがプレイヤーとして存在する．本研究では RP による名寄せを回避するために，本人 ID に対してサービス固有 ID となるよう ID 変換を行う．またサービスをまたいだペルソナの所有者同一性を証明するために，ペルソナに対応した公開 ID を採用する．

本人確認基盤の処理の流れは ID 発行と ID 利用の二つの段階から成る．ID 発行は次の順序で行われる．

(1) 中央認証サーバがユーザに本人 ID を発行する
(2) ユーザが利用したい OP に本人 ID を通知する
(3) OP がユーザに本人確認用 OpenID を発行する

ID 利用は次の順序で処理が行われる．

(1) ユーザは利用するサービスとペルソナに対応する ID を OP に通知する
(2) OP はユーザの本人 ID とサービス ID とペルソナ ID を ID 生成サーバに通知する
(3) ID 生成サーバはサービス ID と本人 ID の組に対して一意なサービス固有 ID と，ペルソナ ID と本人 ID の組に対して一意な公開ペルソナ ID を生成し，OP に通知する
(4) OP はユーザ識別部にサービス固有 ID と公開ペルソナ ID を含む Claimed Identifier を生成し，RP に対して通知する
(5) RP はサービス固有 ID によってユーザの本人性を

確認し，公開ペルソナ ID を用いることでペルソナの同一性保証を行う

3.3. 本人確認用 OpenID の発行

本節では，本人確認用 OpenID の生成手法について説明する．

ユーザは中央認証サーバに対して自分自身であることを証明できる情報を提示する．例えば，パスポートや免許証といった証明書や，IC カードなど所有物による認証，指紋・虹彩などの生体情報を用いた認証など様々な認証方式が考えられる．個人認証は様々な団体によって行われており，外部認証機関による本人確認を経た証明書の提示によって認証を行うことも自然な在り方であろう．中央認証サーバはユーザから提示された個人情報から本人 ID を生成し，正規の ID であることを示すための電子署名を付加してユーザに対して発行する．

次にユーザは本人 ID を OP に対して通知する．本人 ID が確かにユーザ自身のものであることを確認するために，ユーザはパスワードや公開鍵証明書などのクレデンシャルを OP に提示する．

OP はユーザ識別部に本人 ID が含まれるような OpenID を生成し，ユーザに対して発行する．

3.4. サービス固有 ID と公開ペルソナ ID の生成

本節ではユーザのサービス固有 ID と公開ペルソナ ID を生成する手法について述べる．ユーザは OP が発行する本人確認用 OpenID を所有していることを前提とする．

ユーザは利用したい RP のサービス ID とペルソナ ID を OP に対して通知する．サービス ID は RP のコールバック URL などのサービス固有の URL など，ペルソナ ID はユーザが指定する文字列などが考えられる．OP は本人 ID とサービス ID とペルソナ ID を ID 生成サーバに渡し，ID 生成サーバによって生成されたサービス固有 ID と公開ペルソナ ID を得る．サービス固有 ID はサービス ID と本人 ID の組に対して一意であり，公開ペルソナ ID はペルソナ ID と本人 ID の組に対して一意であり，さらにこれらの ID からは本人 ID，サービス ID，ペルソナ ID が復元できないように生成する．例えば，サービス固有 ID は本人 ID とサービス ID をマージして暗号化したもの，公開ペルソナ ID は本人 ID とペルソナ ID をマージして暗号化したものなどが考えられる．また，ID 生成サーバが電子署名を付加したものであっても良い．

OP はサービス固有 ID と公開ペルソナ ID をユーザ識別部に含んだ Claimed Identifier を生成し，RP に通知する．

図 5 のサービス 1 に対して提示される Claimed Identifier の例を図 6 に示す．ユーザ識別部にサービス固有 ID と公開ペルソナ ID が付与される．

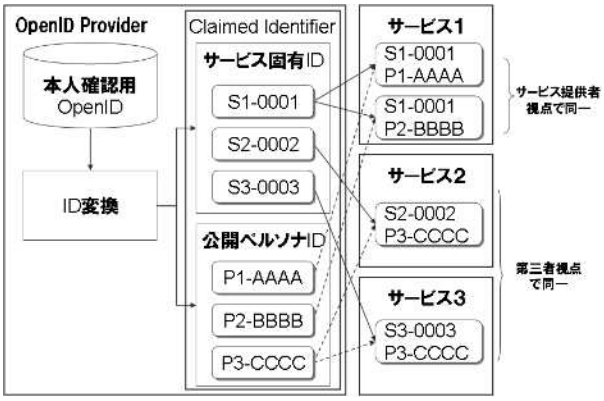

図 5：Claimed Identifier のユーザ識別部の例

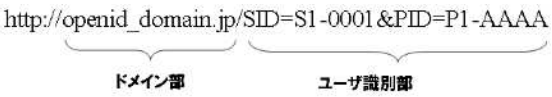

図 6：生成される Claimed Identifier の例

3.5. 本人確認とペルソナの同一性証明

RP は Claimed Identifier からサービス固有 ID と公開ペルソナ ID を抽出する．サービス固有 ID はユーザの実体に一意に紐付いており，本人性を確認できる．もしすでに同じサービス固有 ID によってアカウント登録が行われていれば，ユーザの実体の同一性を確認できる．またユーザの多重アカウントを防止するために登録を拒否することも可能である．

公開ペルソナ ID はユーザの公開プロフィールなどに提示することで，ユーザが自身の意思によってペルソナの同一性を証明するための情報として利用可能である．

RP は複数の OP による本人確認用 OpenID の認証結果を照合することで，セキュリティを強化することもできる．

4. まとめと今後の課題

本研究では，ユーザの個人情報やプライバシーを守りつつ，サービス運営者がユーザの本人性を確認し，ユーザが自身の本人性を第三者に証明するための公開 ID について提案を行った．

中央サーバはユーザの個人情報と本人 ID の紐付け情報のみを持ち，OpenID Provider と ID 生成サーバはユーザの本人 ID と利用サービスとペルソナの紐付け情報のみを持ち，サービス運営者はサービス固有 ID と公開ペルソナ ID の紐付け情報のみを持つ．このためサービス運営者側において，サービス固有 ID と公

開ペルソナ ID はユーザの個人情報や本人 ID とは紐付かない．よって，ユーザのプライバシーが保たれる．

また，ユーザがサービス ID やペルソナ ID を意識しなくても本人確認用 ID を利用できた方が利便性が高くなるため，ペルソナ ID のデフォルト値とサービス ID をコールバック URL に設定するなどの工夫が必要と考えられる．その場合には，サービス ID が変更された場合にも対応できるしくみが必要である．

本人確認用 OpenID は OP に依らずユーザ識別部が同じ ID とすることができる．そのため，ユーザはどの OP を利用しても同じサービス固有 ID と公開ペルソナ ID を得ることができる．RP は本人確認用 OpenID であることさえ分かれば，どの OP によるものであってもユーザを同一として認識できる．よって，ユーザがこれまで利用していた OP が認証サービスを停止しても他の OP による本人確認用 OpenID に切り替えることが可能であろう．RP がそのような運営を行うことでユーザは一つの OP に頼り切ることなく ID を利用でき，RP における情報資源を守ることができる．

次に今後の課題として検討すべき項目について述べる．

まず，公開ペルソナ ID の利用上の規約について検討する必要があると考えられる．ユーザが一つの仮想世界において複数のペルソナを利用することを許容するサービス運営者も多数存在することが考えられるが，その際にサービス運営者はユーザの複数の異なるペルソナの所有者が同一であることを知り得る立場にある．サービス運営者が異なるペルソナの所有者が同一人物であることを公開することで，ユーザのプライバシーが侵害されたり個人が特定される可能性があるため注意が必要と考えられる．公開ペルソナ ID は本人 ID に紐付けるだけでなく，あるグループへの所属に紐付けるといった緩やかさを持たせたい場合も考えられる．そのため単純な乱数や文字列ではなく構造化されたデータであっても良く，さらには画像などに自動変換するなど見ただけで直感的に違いが分かる程度に認識性を向上させる必要がある．

また中央認証サーバが本人 ID を発行する際に，個人認証の方式や本人性はどの程度信頼できるのかといった情報を OP や RP に伝えるための手段が必要があると考えられる．

文　献

[1] 山崎 重一郎，“「非集中的な私」の情報資源をコントロールする Web の新技術とその課題，”2008 信学技報 SITE2008-33, vol.108, no.244, pp.17-20, Oct.2008.

[2] Judith S. Donath, “Identity and deception in the virtual community,” Communities in Cyberspace, Routledge, 1998.

[3] 吉井 大介，安倍 広多，石橋 勇人，松浦 敏雄，“プライバシー保護と個人単一 ID を両立する認証基盤の提案，”2008 情報処理学会 研究報告 2008-DPS-134，pp.1-6，Mar.2008.