情報流通連携のための オープンな ID 連携プラットフォームにおける プライバシー保護機能の高度化

中村素典[†1] 西村健[†1] 山地一禎[†1] 佐藤周行[†2] 岡部寿男[†3]
山崎崇生[†4] 南剛志[†4] 崎村夏彦[†4]

これまで一つの大学や企業などの内部に閉じて利用されてきたシングルサインオン技術に基づく認証基盤を，オープン化し組織の壁を越えた社会的な ID 連携プラットフォームとして実用化する動きが始まっている．民間では OpenID の仕組みを活用した認証連携が進む一方，学術では SAML (Security Assertion Markup Language)を用いた認証連携の枠組みが，国を単位として世界的に立ち上がってきている．OpenID や SAML では，認証結果とともに，認証された利用者に関する属性情報をサービス提供側に受け渡す仕組みが用意されているため，単なる利用者の本人確認にとどまらない，高度な情報連携の可能性を秘めているが，その一方で，個人情報の流通を的確に制御しプライバシーを保護することが求められる．そこで，ID 連携におけるプライバシーの保護を考慮しつつ利便性を低下させない，さらには利便性の向上につながる安全なプライバシー情報の管理・加工・利用技術の開発を行った．

Privacy Enhancement for Open Federated Identity/Access Management Platforms

Motonori NAKAMURA[†1] Takeshi NISHIMURA[†1] Kazutsuna YAMAJI[†1]
Hiroyuki SATO[†2] Yasuo OKABE[†3]
Takao YAMASAKI[†4] Tsuyoshi MINAMI[†4] Natsuhiko SAKIMURA[†4]

1. はじめに

これまで一つの大学や企業などの内部に閉じて利用されてきたシングルサインオン技術に基づく認証基盤を，オープン化し組織の壁を越えた社会的な ID 連携プラットフォームとして実用化する動きが広まりつつある．認証基盤をオープン化することができると，インターネット上に存在するあらゆるサービスに対してユーザごとに一元化された認証情報を用いて本人確認ができるようになるとともに，本人確認のためのセキュリティ技術を効果的に向上させることが可能となる．

ID 連携プラットフォームを社会において本格的に実用化するためには，その上でやりとりされる個人情報の流通を的確に制御し，プライバシーを保護することが求められる．オープンな ID 連携基盤を実現する手法として，これまで SAML (Security Assertion Markup Language) [1]や OpenID[2]といった国際的な規格が標準化され，これらに基づいた ID 連携プラットフォームの構築が進められてきている．ID 連携プラットフォームでは，ユーザ認証を行う ID 管理側と，ユーザにサービスを提供するサービス提供側との間で情報のやりとりが行われるが，まず ID 管理側において個々のユーザの認証を行った後，そのユーザに関する属性情報を ID 管理側からサービス提供側に提示し，それに基づいてサービス提供側が認可判断を行う形態をとる．ここで提示される属性情報には個人情報が含まれうるため，その開示範囲が必要最小限となるような配慮が望まれる．また，誰がどのようなサービスにアクセスしたかという情報もプライバシー情報として保護されるべきものであり，本来必要としない者に対して提供されるべきではなく，関係者に対しても必要以上に開示されるべきではない．

しかしながら，現時点では，まずは認証連携を機能させ相互接続性を確保することが優先されているため，個人が特定可能な属性情報の安直な利用を前提とした仕組みが前提となっていることが多く，個人情報の送信の際のユーザ同意をどのように取得するか，という個人情報の開示に関する法制度等のみを考慮したものにとどまっており，プライバシー保護に関する考慮が十分ではない．このように，組織の壁を越えた社会的な ID 連携プラットフォームとして実用化するためには，ID 連携プラットフォーム上でやりとりされる個人情報の流通を制御しプライバシーを保護することが可能な技術の開発と，その仕様(API)の標準化，さらには授受される個人情報の扱いについて，事前に合意した上で情報を提供するオープンな仕組みとその可視化が重要である．

そこで我々は，ID 連携におけるプライバシーの保護を考

†1 国立情報学研究所
National Institute of Informatics
†2 東京大学
The University of Tokyo
†3 京都大学
Kyoto University
†4 株式会社 野村総合研究所
Nomura Research Institute, Ltd.

慮しつつ利便性を低下させない，さらには利便性の向上につながる安全なプライバシー情報の管理・加工・利用技術の開発を行った．本稿では，その概要について述べる．

2. 認証フェデレーション

2.1 シングルサインオン

サービス毎に異なる ID およびパスワードを用いて認証を行うことは，システム管理者とユーザの双方にとって煩雑である．複数のサービスで共通の ID とパスワードを利用するためには，まず LDAP[3]等を用いて ID およびパスワードを保持する認証データベースを統合し，各サービスから同一の認証データベースを参照する方法が考えられる．

さらにそこから，各サービスから認証機能を分離し，サービス共通の認証サーバを作り，ユーザは ID とパスワードをその認証サーバに入力して認証結果のみを各サービスに伝える，という形態に発展させることにより，シングルサインオンが実現される．認証サーバが認証に成功したことをしばらくの間保持し，その間に他のサービスからも認証要求が来た場合は，同一ユーザに対する再認証（ID とパスワードの再入力）を求めない仕組みを持たせることにより，いわゆるシングルサインオンとしての機能が実現される．このシングルサインオンの機能を，一つの組織内で閉じて利用するだけでなく，他の組織と連携させる形で活用する形態は「認証フェデレーション」あるいは単に「フェデレーション」と呼ばれる．

2.2 フェデレーションの基本アーキテクチャ

認証フェデレーションを実現するための枠組みを提供する代表的なものに SAML と OpenID がある．いずれも，Web ブラウザをクライアントとしてアクセスするサーバ群に対するシングルサインオン技術で，HTTP Cookie[4]や HTTP リダイレクト[5]といった要素技術の上に成り立っており，システムを構成するエンティティに大きな違いはない．

主要なエンティティとしては認証サーバとサービス提供サーバの 2 つがあるが，複数のサービスにおいて共通に利用される認証サーバのことを，SAML では IdP (Identity Provider)と呼び，OpenID では OP (OpenID Provider)と呼ぶ．一方，この認証サーバにおける認証処理の結果に基づいて実際にサービスを提供するサーバのことを，SAML では SP (Service Provider)と呼び，OpenID では RP (Relying Party)と呼ぶ．SAML と OpenID で名称は異なるが，基本的には同様の機能を提供するものである．

一組織の中に閉じたシングルサインオンでは，IdP/OP は一つだけ存在するのが一般的であるが，認証フェデレーションの場合は，フェデレーションに参加しサービスを利用する組織毎に IdP/OP を構築する分散型の構造となる．

2.3 属性送信と送信同意

SAML や OpenID によって提供されるシングルサインオン機構では，IdP/OP は認証結果として認証の可否を SP/RP に伝えるだけでなく，併せて認証されたユーザに関する情報を伝達する機能を持つ．このような情報は属性情報と呼ばれる．認証フェデレーションでは，他の組織に対して属性情報を送信する場合が生じるが，このような情報の送信は業務委託によるサービス利用でない限り第三者提供にあたる．属性情報のうちの一部は個人情報に相当するものであり，プライバシー保護のための考慮が求められる．日本においては，プライバシー保護に関する法律[6][7]が定められており，一般には事前の同意 （オプトイン; Opt-In）あるいは事後の求めによる提供停止 （オプトアウト; Opt-Out）に対応することが求められる．特に国立大学は，独立行政法人に準じるため，オプトインをサポートする必要がある．公立大学については地方公共団体が定める条例に従うが，大半は独立行政法人に準じた扱いとなっている．オプトインを実現するには，ユーザから情報提供を受ける際に事前の同意を得ておく方法もあるが，情報の提供先であるサービスが頻繁に追加されることを考えると，IdP/OP において，情報を送信する際に同意を得る仕組みを提供することが望ましい．

2.4 SAML によるフェデレーション

SAML は XML ベースの認証プロトコルであり，OASIS[8]により初期バージョンが 2002 年に策定された．現在は SAML 2.0 が広く利用されている．学術分野においては，SAML に基づいた認証フェデレーションの構築が主流となっており，国を単位として欧米を中心に構築が進んでいる[9]．日本においても，国立情報学研究所を中心に 2009 年より構築を開始し，2010 年より学術認証フェデレーション「学認」として実運用を行っている[10][11]．学術分野において広く用いられている SAML をサポートしたプラットフォームとしては，Shibboleth [12]や SimpleSAMLphp [13]などがある．

SAML を用いてやりとりされる属性情報の種類および内容は，IdP と SP の双方が合意した取り決めが必要であり，原則としてフェデレーションごとに定められる．例えば，学認では，システム運用基準[14]において 15 種類の属性情報を定義している．これらの多くは Internet2 で定義されている eduPerson オブジェクトクラス[15]のものをベースとしているが，例えば，その中の eduPersonAffiliation はユーザの身分を示す属性情報であり，student (学生)，faculty (教員)，staff (職員)などの値を持つ．

SAML での属性情報のやりとりは，大きく通りの方法がある．1 つはバックチャネル，もう 1 つはフロントチャネルと呼ばれる（図 1）．後者は SAML 2.0 からサポートされた方式であり，属性情報のやりとりをブラウザに対するリダイレクトに含めてしまうことにより，IdP と SP が直接通信する必要がない．しかし，必ずユーザの操作を伴う処理となるため，任意の時点に属性情報を要求したい場合は，バックチャネルを用いる必要がある．

個人情報の送信同意のためには，スイスの学術フェデレーション SWITCHaai [16] を運営する SWITCH が開発した，Shibboleth IdP において利用可能なプラグインである uApprove[15]を利用することができる．学認では，日本語に対応するとともに，よりきめ細かな制御ができるようにするために改良した uApprove.jp を提供している[17].

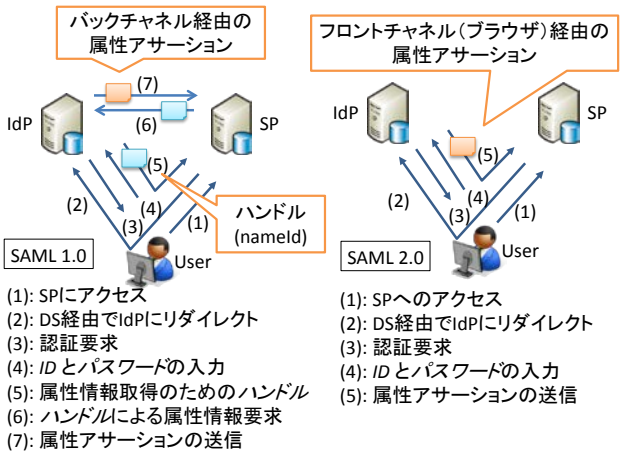

図 1 SAML の認証フロー

Figure 1. Flow of SAML Authentication

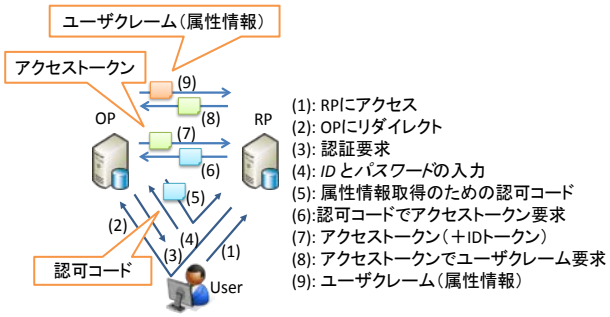

図 2 OpenID Connect の認証フロー

Figure 2. Flow of OpenID Connect Authentication

2.5 OpenID によるフェデレーション

OpenID は 2005 年に登場し，現在は OpenID 2.0[18]が主流である．商用サービス提供事業者においては，OpenID の活用が進んでおり，Aol，Facebook，Google，mixi，Yahoo! などに登録されたアカウントを利用して，他のサービスにログインできるようになっている[19]．OpenID はその思想からプロトコルが非常にシンプルであり，SAML に比較して実装が容易であるが，Ruby や PHP などに対応したライブラリも提供されているため，ほとんどの場合 OpenID の認証処理自体を自分で実装する必要はない．最近では OAuth 2.0 [20] をベースとして設計された OpenID Connect[20]が策定され，そちらへの移行が始まりつつある[21].

OpenID 2.0 で扱う属性情報は，その拡張仕様である Attribute Exchange[22]において規定されている．また，OpenID Connect で扱う基本的な属性情報はおよび拡張方法は OpenID Connect Messages 1.0[23]に規定されている．

OpenID Connect における属性情報のやりとりは，SAML でいうところのバックチャネルの形態をとるが，属性情報の取得にアクセストークンを用いるため，手順が若干増える（図 2）.

2.6 仮名・匿名アクセスによるプライバシー保護

シングルサインオンにおける認証では，RP/SP における認可判断においてユーザの区別が必要でない場合，IdP/OP は，必ずしもユーザに関する情報を SP/RP に送る必要はなく，正しいユーザであることを確認したという事実を伝えるのみで良い．そのため，SAML や OpenID では，このようなユーザ認証の匿名化（アノニマイズ，anonymize）機能を持つ.

また，ユーザの区別は必要だが，具体的に誰であるかについての情報が不要である場合は，仮名化（スードニマイズ, pseudonymize）されたユーザ識別子を利用することも可能である．このような仮名識別子は，OpenID では Pairwise Pseudonymous identifier (PPID)，SAML を用いる学認等では eduPersonTargetedID (ePTID)と呼ばれる．仮名識別子は SP/RP ごとに異なる値となり，これを利用することで，SP/RP をまたがったユーザアクセスに関する名寄せが困難となるため，仮名識別子の利用はプライバシー保護への配慮につながる．なお，インシデントが発生した場合は，IdP/OP との協力によりユーザの特定が可能である.

2.7 属性情報プロバイダ

ユーザに関する属性情報は，ユーザ認証を行う IdP/OP から提供される場合が多いが，バックチャネルの形態を利用すれば，IdP/OP とは別のサーバから属性情報を取得することも可能である．このようなサーバのことを，属性プロバイダ(AP; Attribute Provider)と呼ぶ．あるユーザに関する情報は必ずしも 1 カ所に集約されているわけではなく，それぞれの情報について，責任をもって提供できる組織が属性プロバイダを運用することが望ましい．共同研究プロジェクトのような，複数の大学にまたがる仮想的な組織(VO; Virtual Organization)のメンバ管理等でも利用される[26]. SAML も OpenID Connect も，属性プロバイダの利用が可能である.

3. 認証フェデレーションの展開における課題

SAML と OpenID の 2 つの認証フェデレーションは，これまで個別かつ排他的に利用されることが多かったが，前述のように，アーキテクチャの類似点は多く，属性情報の受け渡しに関する検討事項にも共通点が多い．また，民間で提供される商用サービスは，その充実と高度化により，学術分野において，これらを研究教育に採用する例が増加してきている[27][28][29]. 他方，民間サービスにおいては，

福利厚生的利用を含め，学術関係者の利用に対して割引を提供する慣例が古くからあり，割引をオンラインサービスにおいても同様に実現しユーザを確保したいという要望もある．そのため，2 つのフェデレーションを技術的に接続し，両者を連携させることにより，より大きな認証フェデレーションを構築することも可能であり，両者にとってメリットも大きい．

しかし，このような連携も含め，属性情報の効果的な活用による認証フェデレーションの将来的な発展を考えると，属性情報の扱いをはじめとして，いくつかの問題点が浮かび上がってくる．そこで我々は，まず，以下に示す 5 つの課題を取りあげ，対策手法について検討を行うこととした．

3.1 認証非同期の属性情報要求に関する課題

ユーザが利用するサービスの形態によっては，ユーザの属性情報を，ユーザのアクセス時だけでなく，ユーザがアクセスしていない間も取得したいことがある．特に継続的な課金を伴うサービスでは，ユーザからのアクセスの有無にかかわらず，常に最新の属性情報を取得しておきたいという要求がある．既に学認では，UQ コミュニケーションズが提供する「モバイル WiMAX キャンパスネットワーク接続サービス」[30]がこのような形態のサービスを提供しているが，定期的な在籍確認には SAML を利用していない．

このような定期的な在籍確認のための，ユーザによるアクセスを伴わない属性情報の取得を，以下では認証非同期な属性情報の取得と呼ぶ．従来の認証に同期した属性情報取得の場合は，ユーザによる ID およびパスワードの入力操作に連続して，提供される属性情報の内容確認が可能であるのに対して，認証非同期な属性情報取得の場合は，ユーザによる ID およびパスワードの入力操作のタイミングとは無関係に属性情報のやりとりが行われることになるため，事前にどのサービス(SP)に対してどのような属性情報を提供しても良いかについて確認し，それに基づいた属性情報の提供が必要となる．今後，SAML と OpenID という異なるプロコトルの相互接続によるフェデレーション連携も始まるであろうことも考慮すると，プライバシーを考慮した認証非同期な属性情報の取得のための枠組みの検討[31]を早急に始めておくことが重要である（図 3）．

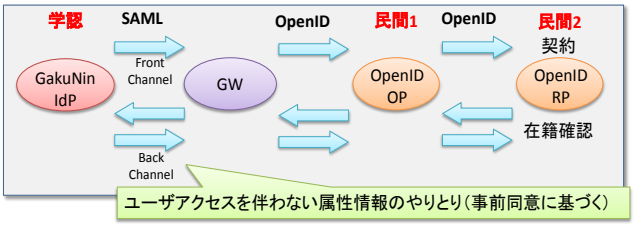

図 3 認証非同期な属性情報の受け渡し

Figure 3. Attribute Request/Response without Authentication

3.2 属性プロバイダの利用に関する課題

認証フェデレーションにおいて，AP（属性プロバイダ）を活用する場合，従来の実装では SP/RP が AP を固定的に指定する方法が提供されているのみであるため自由度がない．本来，AP はユーザ毎に選択できるようになっているべきであり，どの AP を利用するかが SP/RP によってのみ決まりユーザが選択できないことは将来的な実サービスへの展開の上で大きな制約となりうる．

また，AP を利用する上でのもう一つの制約として，ユーザの識別問題がある．IdP/OP と SP/RP の連携の場合には，PPID といった仮名化された識別子が利用可能であるが，AP に対しても属性情報を要求するためには，IdP/OP と AP との間で共通となる識別子を用いるのが一般的である．AP に対する属性情報の問い合わせは SP/RP から行うことになり，必然的に SP/RP も共通の識別子を知る必要があるため，SP/RP ごとに仮名化された識別子の意義が薄れてしまうという問題がある（図 4）．このため，IdP/OP の属性提供機能を AP として分離した ID 連携プラットフォームの本来の柔軟性が損なわれ，実社会への展開における AP の活用に向けて大きな制約を受ける懸念がある．そこで，AP を利用する際にも仮名化された識別子によるアクセスが可能となる技術の確立が望まれる[32]．

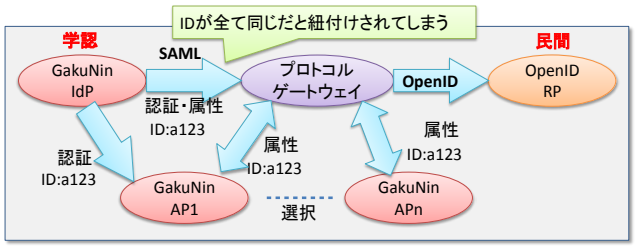

図 4 グローバルな ID による AP へのアクセス

Figure 4. Access to APs with universal unique ID

3.3 属性提供サーバに対するプライバシー保護

一般に，ユーザが認証を経て SP/RP にアクセスすると，どの SP/RP にアクセスしたかという情報は IdP/OP や AP に知られることとなる．しかし，このような情報はプライバシーにかかわるものであり，本来，知らせる必要がない場合も多い．例えば，大学が発行する従来からの学生証を提示して学割サービスを受ける形態では，大学はどのようなサービスに対して当該ユーザが学割サービスを受けたかについて関知しないのが一般的である．そこで，このような仕組みをオンライン上で実現することで，プライバシー情報を IdP/OP あるいは AP から隠蔽することを考える．

このような仕組みを実現するためには，IdP/OP と SP/RP が直接やりとりしないよう，間に認証連携プロキシを導入する方法がある．認証連携プロキシを導入することにより，属性情報を用いて SP/RP が認可判断を行う際に，IdP/OP お

よび AP は具体的な個々の属性情報の値を秘匿しておきたい，逆に SP/RP も認可の条件を秘匿しておきたい，という要求に対応することも比較的容易になる．例えば，就職活動のための情報提供サイトにおいて，ある企業が，学生の大学での成績のうち，英語の成績と数学の成績の和がある閾値以上であれば，採用プロセスの一部を免除するようなケースがあったとする．大学が学生の全科目の成績の素点をサービス提供サーバに伝えることを避けるためには，英語と数学の和が閾値を超えているかどうかの結果だけを企業に伝えれば良いが，企業として，判定ルールを大学に開示することは避けたい（英語と数学しかみていないとかいうようなことは大学側には開示したくない）という要求があるとすると，従来の手法による実現は難しい．間に認証連携プロキシを置くことによって，両者の要求をかなえることができると考えられる[33]（図 5）．

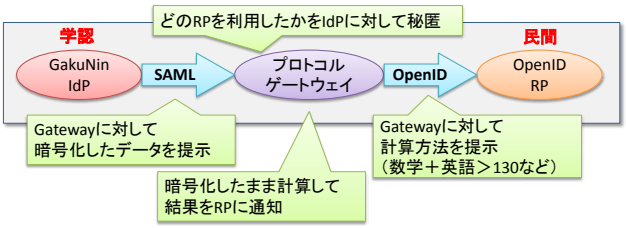

図 5 属性情報と認可条件の相互秘匿
Figure 5. Mutual Concealment of Attribute Values and Authorization Conditions

3.4 プロキシに対するプライバシー保護

ユーザ認証を経てそのユーザの属性情報を IdP/OP あるいは AP が SP/RP に提供する際，ユーザがどのサービス提供サーバに対してアクセスしたかというプライバシーにかかわる情報を保護するためには，プロキシの導入が必要となる（3.3 節）．しかし，単純にプロキシを導入すると，ユーザのプライバシーにかかわる情報がプロキシに開示されてしまう．この問題を回避するためには，属性アサーションの内容を暗号化することが必要である．従来の実装でも暗号化はなされているが，通信経路上での情報漏洩を回避することが目的であるため，送信先に対応した公開鍵暗号方式に基づく公開鍵が暗号化に利用される．前項で掲げた，IdP/OP と SP/RP が相互にわからないようにするという前提をも考慮するためには，さらなる工夫が必要である[34].

また，このようなプライバシー保護を配慮しつつ，ユーザの同一性を確認する方法についても検討する．例えば，学割サービスの提供において，SP/RP 側には 1 人のユーザに対する割引の適用回数に，ある上限を設けておきたいという要求がありうるが，その一方で，IdP/OP 側は，プライバシー保護の観点からユーザを特定する情報となるグローバルユニークな識別子情報を出すことを避けたいという要求がある．このため，SP/RP 側においてユーザの同一性が容易に確認できず，ID 連携の組み合わせが複数ある場合には，同一のユーザが制限を超えた回数の割引を受けられてしまう抜け道が生じうる．そこで，属性提供サーバからは仮名識別子を提供しつつ，同一のサービスに対してその利用回数等を制限することができる仕組みが望まれる（図 6）．

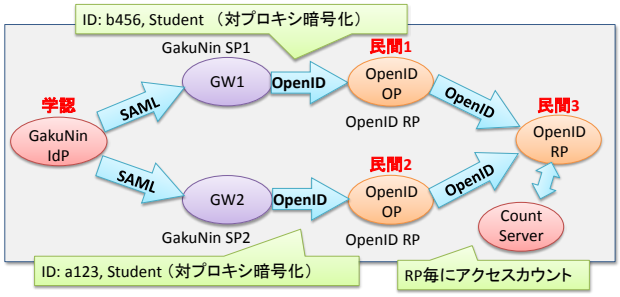

図 6 仮名性を維持した同一性確認
Figure 6. Confirmation of identicalness with pseudonymous ID

3.5 Web 以外のサービスへの対応

Web をベースとしたサービスにおいては，ID の氾濫とそれに伴うセキュリティ上の問題から，シングルサインオン技術を活用した，いわゆる No Password の取り組みが始まっている．しかし，HTTP を利用する Web とは異なる仕組みで実現されている，メール等の他のサービスでは，従来通りのサービスごとの ID，パスワードを使うしかない状況が続いている．これらの Web 以外のサービスにおいても，No Password の仕組みを構築することで，ID 窃盗の問題等への対応を行う事が可能となる．そこで，SMTP や IMAP 等のパスワードベースのプロトコルに対して，OpenID Connect のアクセストークンを受け入れたログインを実現するための技術の開発を試みる[35][36]. なお, SAML では，Moonshot Project[37]による試みがある．

4. おわりに

SAML や OpenID といったオープンな枠組みをベースとする ID 連携プラットフォームの活用では，プライバシー保護の考慮が不可欠である．本稿では，プライバシー保護を中心として取り組んできた 5 つの課題について紹介した．それぞれの問題の解決方法の詳細については，別途報告していく予定である．

将来の社会をとりまく ICT 環境のさらなる充実と高度化のためには，ID 連携フラットフォームの利用は不可欠であり，ID 連携プラットフォームを将来的にさらに活用していくためには，プライバシー保護を考慮したシステムデザインが求められる．我々は，今回とりあげた 5 つの課題にとどまらず，さらにより良い ID 連携プラットフォームの実現を目指して取り組んでいきたいと考えている．

謝辞

本報告の内容の一部は，総務省「戦略的国際連携型研究開発推進事業」（平成 24 年度，情報セキュリティに関する研究開発課題の委託）による支援を受けて「情報流通連携のためのオープンな ID 連携プラットフォームにおけるプライバシー保護機能の高度化の研究開発」として実施したものである．

参考文献

1) S. Cantor, J. Kemp, R. Philpott, and E. Maler ed., “Security Assertion Markup Language (SAML) V2.0,” http://saml.xml.org/saml-specifications, March 2005.
2) OpenID Foundation, “OpenID Foundation website,” http://openid.net/, last visited May 15, 2013.
3) M. Wahl, T. Howes, S. Kille, “Lightweight Directory Access Protocol (v3),” The Internet Society, RFC2251, 1997.
4) A. Barth, “HTTP State Management Mechanism,” The Internet Society, RFC6265, 2011.
5) R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1,” The Internet Society, RFC2616, 1999.
6) 総務省, “個人情報の保護に関する法律,” 法令データ提供システム, http://law.e-gov.go.jp/htmldata/H15/H15HO057.html, 2003.
7) 総務省, “独立行政法人等の保有する個人情報の保護に関する法律,” 法令データ提供システム, http://law.e-gov.go.jp/htmldata/H15/H15HO059.html, 2003.
8) OASIS: Advancing open standards for the information security, https://www.oasis-open.org/, last visited May 15, 2013.
9) REFEDS (Research and Education Federations), “REFEDS Federation Survey”, https://refeds.terena.org/index.php/Federations, last visited May 15, 2013.
10) 西村健, 中村素典, 山地一禎, 大谷誠, 岡部寿男, 曽根原登, “日本における学術認証フェデレーションとその役割および効果,” 信学技法, Vol. 111 No. 375, IA2011-55 pp.5-8, 2012.
11) 島岡政基, 西村健, 古村隆明, 中村素典, 佐藤周行, 岡部寿男, 曽根原登, “学術機関のためのサーバ証明書発行フレームワーク” (ネットワーク管理・オペレーション, <特集> 若手研究者のためのフロンティア論文), 電子情報通信学会論文誌, Vol.J54-B, No.7, pp.871-882, 2012.
12) Shibboleth Consortium, http://shibboleth.net/, last visited May 15, 2013.
13) SimpleSAMLphp, http://simplesamlphp.org/, last visited May 15, 2013.
14) 国立情報学研究所, “学術認証フェデレーション システム運用基準 (Ver.1.2),” 2011.
15) Internet2, “eduPerson & eduOrg Object Classes,” http://middleware.internet2.edu/eduperson/,
16) L. Hämmerle, “SWITCHaai: shibboleth-based federated identity management in Switzerland,” Proceedings of CESNET 2006 Conference, 2006.
17) The SWITCH Foundation, “uApprove,” http://www.switch.ch/aai/support/tools/uApprove.html, last visited May 15, 2013.
18) Tananun Orawiwattanakul, Kazutsuna Yamaji, Motonori Nakamura, Toshiyuki Kataoka , Noboru Sonehara: User Consent Acquisition System for Japanese Shibboleth-based Academic Federation (GakuNin), International Journal of Grid and Utility Computing (IJGUC), Vol. 2, No. 4, pp. 284-294, 10.1504/IJGUC.2011.042944, 2011.
19) OpenID Foundation, “OpenID Authentication 2.0 - Final,” 2007.
20) OpenID Foundation, “Surprise! You may already have an OpenID”, http://openid.net/get-an-openid/, last visited May 15, 2013.
21) D. Hardt, Ed., “The OAuth 2.0 Authorization Framework,” RFC6749, Internet Engineering Task Force (IETF), 2012.
22) OpenID Foundation, “Welcome to OpenID Connect,” http://openid.net/connect/, last visited Apr. 1, 2013.
23) Yahoo! Japan, “YConnect(OAuth2.0/OpenID Connect)をリリースしました！,” http://techblog.yahoo.co.jp/web/auth/yconnect/, 2012.
24) OpenID Foundation, “OpenID Attribute Exchange 1.0 – Final,” 2007.
25) N. Sakimura, J. Bradley, M. Jones, B. de Modeiros, C. Mortimore, E. Jay, “OpenID Connect Messages 1.0 – draft 18,” OpenID Foundation, http://openid.net/specs/openid-connect-messages-1_0.html, 2013.
26) 西村健, 中村素典, 井上仁, 山地一禎, 曽根原登, “電子書籍閲覧における組織横断型認証のためのグループ管理,” 情報処理学会 研究報告 2011-IFAT-102(5), pp. 1-6, 2011.
27) Google Apps for Education, http://www.google.com/intl/ja/enterprise/apps/education/, last visited May 15, 2013.
28) マイクロソフト, “Office 365 導入事例”, http://www.microsoft.com/ja-jp/office/365/showcase.aspx, last visited May 15, 2013.
29) Yahoo! Japan, “Yahoo!メール Academic Edition”, http://business.yahoo.co.jp/ymacademic/, last visited May 15, 2013.
30) UQ コミュニケーションズ, “モバイル WiMAX キャンパスネットワーク接続サービス,” http://www.uqwimax.jp/service/corporate/campusconnect.html, last visited May 15, 2013.
31) 中村素典, 西村健, 山地一禎, 佐藤周行, 岡部寿男, “学割サービス実現のための SAML-OpenID ゲートウェイの試作,” 情報処理学会 研究報告, 2013-IOT-21 (28), pp. 1-7, 2013.
32) Motonori NAKAMURA, Takeshi NISHIMURA, Kazutsuna YAMAJI, Hiroyuki SATO, Yasuo OKABE, “Privacy Preserved Simple Attribute Aggregation to Avoid Correlation of User Activities Across Shibboleth SPs,” Proceedings of The 7th IEEE International Workshop on Middleware Architecture in the Internet (MidArch 2013), (in Proceedings of The 37th Annual International Computer Software & Applications Conference (COMPSAC 2013)), 2013. （掲載予定）
33) 岡部寿男, 佐藤周行, 西村健, 山地一禎, 中村素典, “属性提供サーバに対してサービス提供サーバを秘匿する匿名化プロキシ”, 情報処理学会 DICOMO2013 シンポジウム, 2013. （掲載予定）
34) Hiroyuki SATO, Yasuo OKABE, Takeshi NISHIMURA, Kazutsuna YAMAJI, Motonori NAMAMURA, “Privacy Enhancing Proxies in Attribute Release:Two Approaches,” Proceedings of The 7th IEEE International Workshop on Middleware Architecture in the Internet (MidArch 2013), (in Proceedings of The 37th Annual International Computer Software & Applications Conference (COMPSAC 2013)), 2013. （掲載予定）
35) N. Sakimura, B. Kihara, K. Shimizu, “Structured Access Token for Sharing Authorization Grant between a Resource Server and an Authorization Server,” Internet Draft, IETF, draft-sakimura-oidc-structured-token-01, https://datatracker.ietf.org/doc/draft-sakimura-oidc-structured-token/, 2013.
36) N. Sakimura, B. Kihara, K. Shimizu, “Access Token as per Client Password for Non-Web Protocols,” Internet Draft, IETF, draft-sakimura-oidc-extension-nonweb-01, https://datatracker.ietf.org/doc/draft-sakimura-oidc-extension-nonweb/, 2013.
37) Project Moonshot, http://www.project-moonshot.org/, last visited May 15, 2013.