解説

アイデンティティ管理の現状と今後

Trends in Identity Management

高橋健司

Abstract

社会，経済，生活のオンラインサービスへの依存度が増す一方で，セキュリティ被害やプライバシー侵害が深刻化しつつある．このような情勢を背景に，個人や組織に関する情報を管理する，「アイデンティティ管理」の重要性が高まっている．アイデンティティ管理とは，様々なサービスやシステムで個人や組織に関する情報の安心安全かつ容易な活用を目的に，生成から変更，消去までのアイデンティティのライフサイクル全体を管理する手法である．現在，様々なアプローチによる，アイデンティティ管理方式や技術仕様が提案されている．本稿では，特に代表的なアプローチ（SAML/Liberty Alliance，OpenID，Information Card）を例に，アイデンティティ管理の現状を概説し，今後の方向性を展望する．

キーワード：アイデンティティ管理，国際標準，プライバシー

1. はじめに

セキュリティ被害の深刻化，認証セキュリティに関する規制の強化，企業経営の更なる効率化やオンラインサービスの高度化や普及拡大の情勢を背景に，「アイデンティティ」や「アイデンティティ管理」が注目を浴びている．世界のアイデンティティ管理市場の規模は，2006年で26億米ドル，2014年には123億米ドルに達すると予測されている[1]．

また，不正に入手した個人情報の悪用，「アイデンティティ盗難」の被害は，米国では12億米ドルに達している[2]．世界各国で，個人情報の保護のための法規制が整備されている．例えば，日本の個人情報保護法や米国のインターネット上の銀行サービスの認証ガイドライン[3]等がある．企業においても，顧客や従業員の「アイデンティティ」情報の管理の更なる効率化が強く求められている．例えば，増加する企業の吸収合併に伴うシステム上の従業員・顧客情報の整理統合や，パスワードに関する顧客対応，情報漏えい対策など，アカウント管理に関するコストやリスクは増大しており，対策が求められている．

更に，経済社会のサービス化の進展が，アイデンティティ管理へのニーズ増加に拍車をかけている．例えば，SNS（Social Network Service）等に代表される先進的なサービスでの個人情報の活用が進んでいる．また，台頭してきたSaaS（Software as a Service）等のサービスのアウトソーシングにおいても，サービスやデータへのアクセスのための認証・認可が必要不可欠である．そして，電子政府等の公共サービスにおいても，プライバシー保護や利便性向上の観点から，アイデンティティ管理への取組みが活発化している[4]．このように，様々なサービスで，ユーザの「アイデンティティ」をどのように管理するかが重要な課題となってきている．

これらの個人（やユーザ）の情報の管理，認証・認可等を総合的に扱う技術分野がアイデンティティ管理である．本稿では，アイデンティティ管理技術の最近の動向について，国際標準等を交えて概説し，今後を展望する．

2. アイデンティティ管理とは？

アイデンティティ管理とは何かに答えるためには，まず，アイデンティティとは何かに答える必要がある．ここでは，「アイデンティティ」を以下のように定義する．

高橋健司　正員　日本電信電話株式会社NTT情報流通プラットフォーム研究所
Kenji TAKAHASHI，Member（Information Sharing Platform Laboratories，NIPPON TELEGRAPH AND TELEPHONE CORPORATION，Musashino-shi，180-8585 Japan）．
電子情報通信学会誌　Vol.92 No.4 pp.287-294 2009年4月

アイデンティティとは，「ある状況で個人やグループ，組織・企業を特定する情報の総体」である．これらの情報（アイデンティティ情報と呼ぶ）は，以下の三つに分類される．

・識別子：アイデンティティを識別するための情報
　例）アカウント名，メールアドレス，保険証番号，運転免許証番号，社員番号，学生番号，電話番号
・クレデンシャル：ある情報内容の正当性を示すための情報
　例）正当なユーザであることを証明するワンタイムパスワード，国籍を示す電子パスポート等
・属性：アイデンティティを特徴付ける情報
　個人の例）氏名，住所，生年月日，所属，役職，信用情報，人間関係
　企業の例）代表者名，所在地，ロゴ，定款，格付け情報，東証コード等

上記のアイデンティティの定義に基づき，「アイデンティティ管理」を以下のように定義する．

「様々なサービスやシステム上で，アイデンティティを，安全かつ簡単にプライバシーを保護しつつ活用できるように，アイデンティティ情報への適切なアクセスや操作等の機能をライフサイクル全体にわたり提供すること」

アイデンティティ管理技術を利用したサービスの代表例として，シングルサインオン及び属性共有がある．シングルサインオンとは，「ユーザが一度認証されると，その後，複数のサービスを認証手続きなしで利用可能にする」ことを指す．属性共有とは，「あるユーザに関する情報（属性情報）を複数のサービスでプライバシーを保護しつつ安全に共有する」ことを指す．

3. 代表的なアイデンティティ管理方式

アイデンティティ管理は適用分野が多岐にわたるため，数多くの業界団体や標準化団体が，様々な目的に対し異なるアプローチで，アイデンティティ管理方式や技術仕様の策定に取り組んでいる[5]．ここでは，特に代表的な三つの方式（アイデンティティ連携方式，アイデンティティ統一方式，アイデンティティ選択方式）について述べる．

3.1 アイデンティティ連携方式

アイデンティティ連携方式とは，複数のアイデンティティを連携して管理する方式である．本方式は一般的に，ユーザ（端末），アイデンティティ提供者（IdP：Identity Provider），サービス提供者（SP：Service Provider）から構成される．また，相互に信頼する SP と IdP の集合をトラストサークルと呼ぶ．

アイデンティティ連携方式では，一人のユーザが，各 SP に個別のアイデンティティ（すなわち，アカウント）を持っている状況に対応できる．ユーザは，これらの個別のアカウントをリンク付けさせる（連携させる）ことにより，複数の SP に散在している自分のアイデンティティ情報を管理する（図 1）．アイデンティティを連携する際に，仮名を用いることにより，プライバシー保護を強化することができる．仮名とは，本来の識別子を秘匿するために，その代用となる識別子である．仮名としてランダムな文字列を用いることが多い．具体的には，IdP-SP の組ごとに異なる仮名を用いることにより，あるユーザが各 SP でどのようなサービスを利用したか等の情報を収集する「名寄せ」によるプライバシー侵害や，実アカウント名の不正な流出を防止する．アイデンティティ連携方式の導入は，テレコム，企業向けシステム，電子政府などの分野で進んでいる．

アイデンティティ連携方式は，以下の手順でアイデン

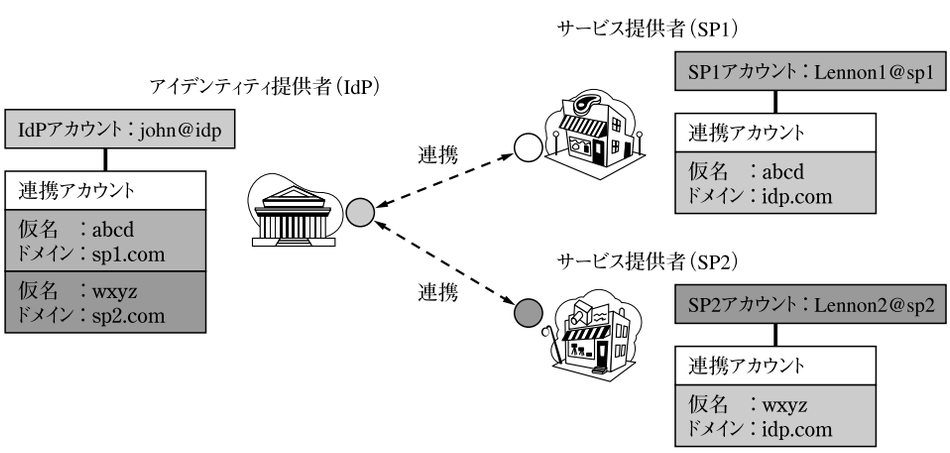

図 1　アイデンティティ連携方式　　ユーザは，サービス提供者ごとに異なるアカウント（Lennon1@sp1，Lennon2@sp2）と，アイデンティティ提供者におけるアカウント（John@idp）とを連携させて，それぞれに付随するアイデンティティ情報を管理する．

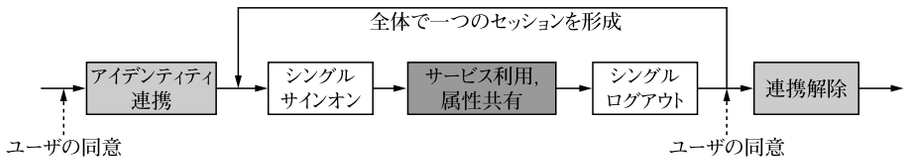

図2　アイデンティティ連携方式における処理手順の概要

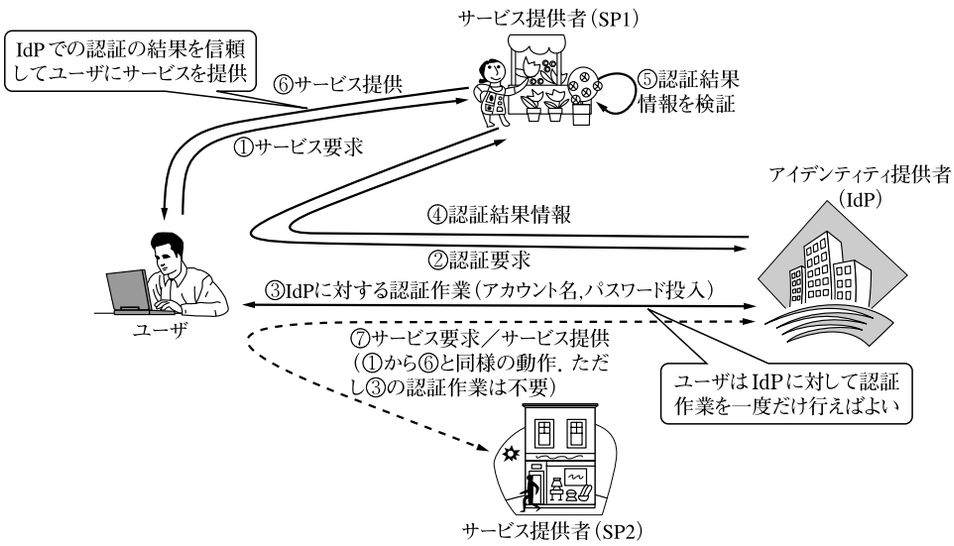

図3　アイデンティティ連携方式におけるシングルサインオンの処理の流れ（SAML2.0の場合）

ティティを管理する（図2）．

（0）　複数のIdP及びSPがトラストサークルを形成（ビジネスや技術面での情報交換及び合意形成）
（1）　ユーザがあるIdPのアカウントと複数のSP（例：SP1，SP2）のアカウントとのリンクを確立（一度確立したら（4）でリンクを解消するまではユーザ作業は不要）
（2）　ユーザが複数のSPにシングルサインオンや属性共有を実施する
（3）　ユーザがシングルサインオンしたSPから一度にログアウトする（シングルログアウトと呼ぶ）
（4）　ユーザが確立したリンクの幾つか（もしくはすべて）を削除する

（注：ユーザの同意を得て自動的に各アカウントを一括してリンクしたり，アカウントのないサイトにも一時的に利用できる仕組み等も後述のSAML2.0では定義されている．）

3.1.1　アイデンティティ連携方式に基づくシングルサインオン

アイデンティティ連携方式では，アイデンティティの連携状況に応じて各SP間で認証結果を共有することにより，シングルサインオンを行う．このようなシングルサインオンの仕組みを規定する代表的な技術仕様としてSAML2.0（Security Assertion Marku Language 2.0）がある[6]．本節では，SAML2.0仕様を例に，シングルサインオンの仕組みを説明する．SAML2.0では，認証，認可，属性に関する情報の表現形式及び送受信手順が定義されている．過去にLiberty ID-FF1.2[7]，SAML1.1[8]，Shibboleth[9]とそれぞれ独立に開発されていた仕様群が，SAML2.0として統一された．現在，業界団体（OASIS SSTC：Organization for the Advancement of Structured Information Standards，Security Services Technical Committee[10]）がSAML2.0仕様を維持管理している．また，業界団体（Liberty Alliance[11]）ではSAML2.0の相互運用テストを実施している．米国連邦政府機関である一般調達庁（GSA：General Service Administration）では，この相互運用テストの合格を米国連邦政府への調達の条件としている[12]．

SAML2.0仕様は，目的に応じて様々な実装形態を可能にするように体系的に規定されている．ここでは，一例としてWebブラウザを介したシングルサインオンの仕組みについて説明する（図3）．

まず，ユーザがSP1でサービス利用を要求する（①）．SP1は，まだユーザの認証をしていないのでユーザが利用しているブラウザを介して，認証要求をIdPに送る（②）．IdPはユーザを何らかの手段で認証する（③）．ここで，どのような認証手段を用いるかはSAML2.0では規定しておらず，ユーザ，IdP，SP間の合意に基づき

決定される．ただし，SAML2.0には，「認証コンテキスト」をSPに伝える仕組みが規定されている．認証コンテキストとは，SPが認証結果をどれくらい信頼できるかを判断するために，認証が行われた経緯を説明する情報である．例えば，認証コンテキストには，どのような認証手段を使ったか，そもそもクレデンシャルはどのように作成，保存されているか等の情報が含まれる．次のステップ（④）で，認証コンテキストを含む認証結果がIdPから，ユーザのブラウザ経由で，SP1に返送される．SP1は，認証結果に基づき，サービス提供の可否を決定する(⑤)．ユーザが他のサービスを用いる場合は，ユーザが直接認証作業を行うステップ③を除いて，同様の処理が繰り返される．

このようにして，ユーザが一度認証作業をすれば，更なる認証作業なしで複数のサービスが使える，「シングルサインオン」が実現されている．

SAML2.0仕様体系には，このような手順のほかに，認証結果をブラウザを介さずにやりとりする手順や，ブラウザ以外のクライアントやプロキシサーバに対応した手順など，ネットワークや端末等の要求条件に応じた実装形態を可能にするような仕様が規定されている．

3.1.2 アイデンティティ連携方式に基づく属性共有

アイデンティティ連携方式に基づく属性共有では，ユーザが，サービス利用に必要な属性情報を，オンデマンドにSP間で共有することを許可する．例えば，新規サービスにユーザ登録する場合に，必要な情報（住所，氏名など）を既に登録してあるサービスから引用することにより，ユーザ登録の手間を省くことができる．また，オンラインショッピングで買った商品を配送する場合に，住所録サービスから届け先を引用して，入力の手間を省くことが可能になる．

ここでは，アイデンティティ連携方式に基づく属性共有の仕組みを規定する技術仕様（Liberty ID-WSF：Liberty Identity Web Service Framework）を例に説明を行う[13]．Liberty ID-WSFは，以下の四つの要素から構成される：ユーザ（ユーザ端末），アイデンティティ提供者(IdP)，探索サービス(DS：Discovery Service)，サービス提供者（SP）．IdP及びSPは前述のSAML2.0で定義されたものと同じである．DSは，ユーザの各アイデンティティ情報へのアクセス情報を管理しており，SPの要求に応じてそれらのアクセス情報を提供する．

例えば図4において，ユーザがオンラインショッピングのSP1で商品を買って配送するときに，住所情報を住所録サービス(SP2)から届け先を取得する利用例では，以下のように処理が進む．まず，ユーザはシングルサインオンをして，SP1の買物サービスを利用する(①)．SP1は届け先を取得するために，探索サービス（DS）を利用して，どこにユーザの住所情報があるかを問い合わせる（②）．このときにSP1は，その問合せがユーザのために行っていることを証明するために，SAML形式で記述された認証結果を提示する．認証結果が確認できたら，DSはアクセス情報（アクセス先及びSP1の要求の正当性を示す情報をSAML形式で記述）をSP1に与える（③）．SP1は，そのアクセス情報を利用してSP2にアクセスし必要な属性情報（住所情報）を要求する（④）．このときにSP2は，SP1への属性情報提供に関する同意をユーザから直接得る（⑤）．そして同意に従い，SP2はSP1へ属性情報を提供する（⑥）．以上の処理を経て，SP1はユーザに品物を送り届ける(⑦)．

3.2 アイデンティティ統一方式

アイデンティティ統一方式とは，あるユーザが，一つの識別子で様々なサービスにアクセスする利用形態を前提にしたアイデンティティ管理方式である．この方式に

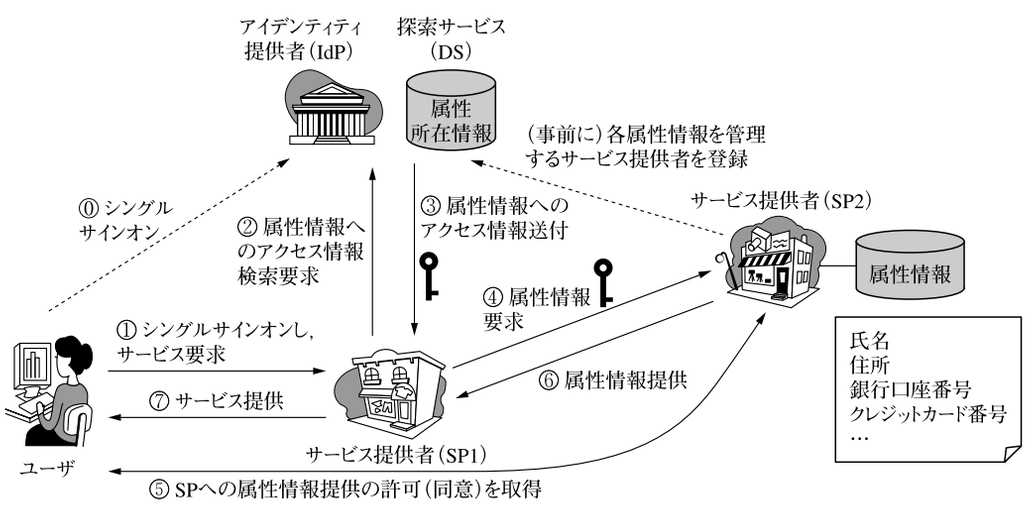

図4 アイデンティティ連携方式における属性共有の処理の流れ（Liberty ID-WSFの場合）

対応した代表的な技術仕様としてOpenID2.0がある[14],[15]．現在，OpenID2.0仕様は業界団体（OpenID Foundation[16]）で維持管理されている．本節では，OpenID2.0を例にアイデンティティ統一方式の概要を解説する．

OpenID2.0に基づく方式は，一般的にユーザ（ユーザ端末）及び，アイデンティティ提供者（OP：OpenID Provider），サービス提供者（RP：Relying Party）から構成される．ユーザは，URL等で表現されたグローバルにユニークな識別子を持ち，複数のRPで利用する．ここでは，識別子はユーザを識別するという本来の役割以外に，それが代表するユーザのアイデンティティ情報へのアクセス方法も示す役割も果たしている．このように役割を重複させると，ユーザ識別子（アカウント）のOP間におけるポータビリティの低下やアイデンティティ情報の分散的な配置の阻害を招くリスクがあるので，システムやサービス設計時にこのようなリスクを考慮する必要がある．

OpenID2.0仕様の手順は，3.1で例として取り上げた，SAML2.0仕様体系の中のある処理の流れ（図3）に類似している．SAML2.0におけるIdPがOPに，SPがRPに対応している．ただし，SAML2.0とは異なり，RPはOPをURL等で表現された識別子から動的に発見しアクセスする．また，SAML2.0と比較すると，仕様の簡素さや実装の簡便さを重視していると考えられる．更に，OpenID2.0は，SAML2.0のような様々な端末や送信手段に対応した仕様体系を持たない．例えば，仕様には通信の暗号化や送受信証跡の保存を前提にしておらず，また送信手順はHTTPリダイレクションを利用する手順だけを規定している．

実運用面では，仕様上は事前にOPやRP間の信頼関係を構築する必要がなく，各アカウントをリンクする必要もない．しかし，何らかの手段で事前に信頼関係が構築されていなければ，信頼レベルが確認できない相手とアイデンティティ情報をやりとりすることになり，セキュリティ上のリスクは高まる．また，グローバルでユニークな識別子を複数のサービスで用いる場合は，前述の「名寄せ」によるプライバシー侵害のリスクも高まる．現在，OpenID2.0は，セキュリティ要件が比較的軽微なサービス（SNS，ブログ等）を中心に広まっている．将来の発展に向けて，対象サービスや利用目的に応じて，セキュリティやプライバシー等に関して，ユーザ，OP，RP間で合意が必要な事項を明確にしていく必要があると考える．

図5は，OpenID2.0の処理の流れの概要を示している．まず，ユーザがRPでサービス利用を要求する（①）．RPは，まだユーザの認証をしていないので，ユーザにアカウント名（URL）の投入を要求する（②）．RPは，投入されたURLを用いてIdPを発見する（③，④）．次に，RPは，ユーザのブラウザを介して，認証要求をOPに送る（⑤）．OPはユーザを何らかの手段で認証する（⑥）．ここで，どのような認証手段を用いるかはOpenID2.0では規定しておらず，ユーザ，OP，RP間の合意に基づき決定される．次のステップ（⑦）で，認証結果がOPから，ユーザのブラウザ経由で，RPに返送される．RPは認証結果に基づき，サービス提供の可否を決定する（⑧）．ユーザが他のサービスを用いる場合は，ユーザが直接認証作業を行うステップ⑥を除いて，

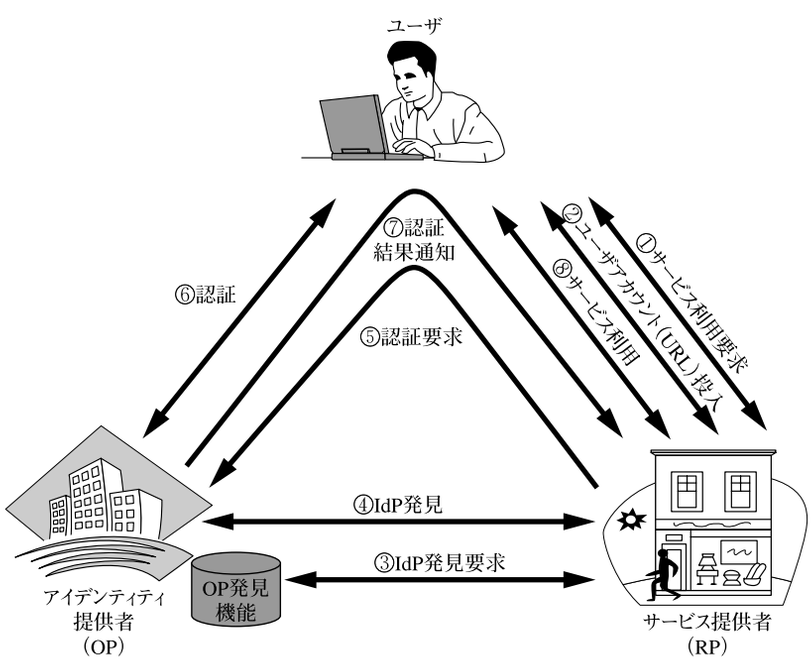

図5　アイデンティティ統一方式におけるシングルサインオンの処理の流れ（OpenID2.0の場合）

同様の処理が繰り返される．このようにして，シングルサインオンが実現されている．

OpenID2.0 では，属性情報を交換する方式も仕様化されている[16]．その処理手順は，認証結果を交換する場合（図 4）とほぼ同じである．

3.3　アイデンティティ選択方式

アイデンティティ選択方式は，ユーザがアイデンティティを複数持っており，それらをサービスごとに選択して用いる，アイデンティティ管理方式である．代表的な技術仕様として Information Card があり，業界団体（Information Card Foundation）が仕様化及び普及を進めている[17]．また，実装例として，Microsoft 社の Windows CardSpace® があり，同社の OS に標準装備されている．また，Higgins プロジェクトなどでは，オープンソース版も開発されている[18]．

Information Card では，「カード」のメタファでアイデンティティを使い分ける．例えば，このカードは，電子的な身分証明書，クレジットカードや会員証などである．アイデンティティ選択方式では，認証と属性交換の明確な区別はなく，ユーザがサービスの利用認可に必要なアイデンティティ情報（例：「20 歳以上である」）を選択して提示する．Information Card 仕様は，シングルサインオンの手順を規定していない．

アイデンティティ選択方式では，ユーザ端末には，ユーザがアイデンティティ（カード）を選択し送受信するための Identity Selector 機能が組み込まれている．また，アイデンティティ提供者として Security Token Server（STS），また，サービス提供者として Relying Party（RP）が配置される．Information Card は，Microsoft 社のサービス等を中心に普及が進んでいる．

図 6 は，Information Card の処理の手順を示している．まず，ユーザが RP でサービス利用を要求する（①）．RP は，まだユーザの認証をしていないので，ユーザにアイデンティティ情報を要求する（②）．ユーザは Identity Selector を用いて，必要なアイデンティティ情報を選択し（③），STS から取得する（④）．そして，ユーザがアイデンティティ情報を RP に送付する（⑤）．RP は，送付されたアイデンティティ情報に基づき，サービス提供の可否を決定する（⑥）．

3.4　相互運用性確保の取組み

従来，上記の三つの方式は，それぞれ独立に仕様が策定されてきた．しかし，これらの仕様間の相互接続を実現するための取組みがなされている．例えば，Concordia Project[19] や Liberty Alliance Web Services Harmonization Special Interest Group[20] での取組みがある．Concordia Project では，これまでに Information Card と SAML2.0 との相互接続に，また，現在では，OpenID2.0 と SAML2.0 との相互接続に取り組んでいる．例えば，この取組みでは，SAML2.0 に対応したアイデンティティ提供者に登録しているユーザが，OpenID2.0 対応のサービスへもシングルサインオンできる利用シナリオの実現を目指している（図 7）．このシナリオは，ユーザ，OpenID2.0 対応サービス提供者，OpenID2.0 と SAML2.0 の両方に対応するアイデンティティ提供者，SAML2.0 対応アイデンティティ提供者の四者から構成される．このシナリオでは，OpenID2.0 対応サービス

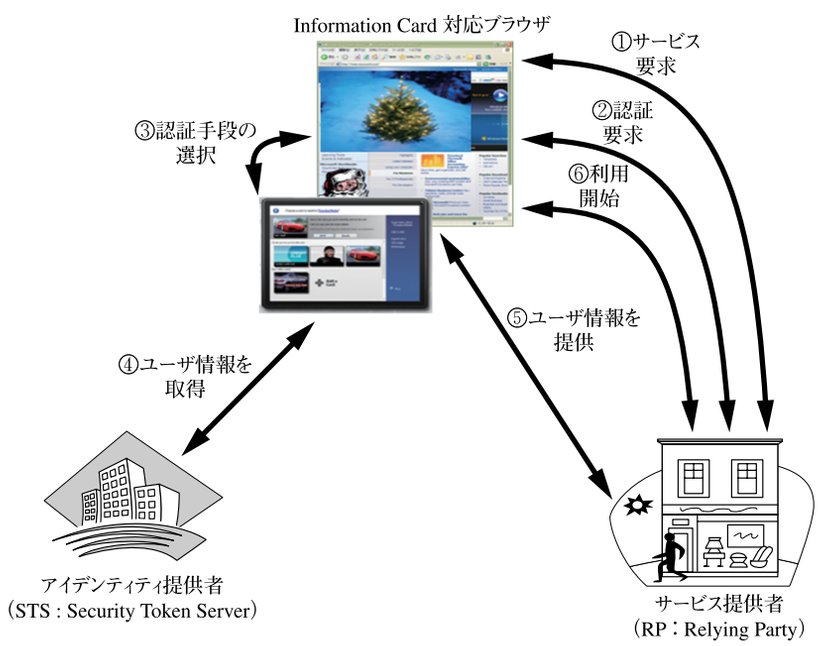

図 6　アイデンティティ選択方式の処理手順

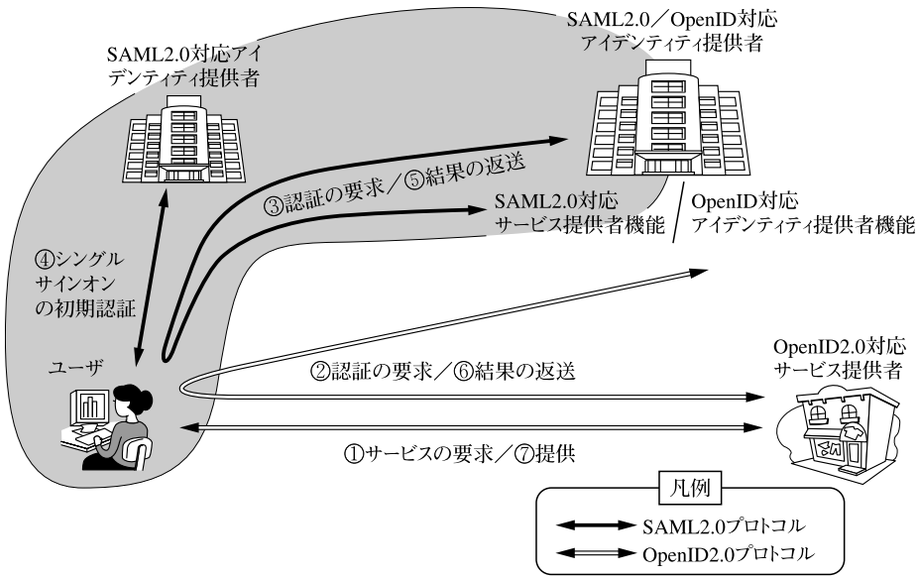

図7　SAML2.0とOpenID2.0の相互接続の処理の流れ

提供者は，OpenID2.0とSAML2.0の両方に対応するアイデンティティ提供者を介して，SAML2.0対応アイデンティティ提供者が行ったユーザ認証の結果を取得する．

4.　まとめ及び今後の課題

情報通信技術の適用分野が，ネットワーク装置やデータをつなぐ利用シーンから，「アイデンティティ（人，組織）」と「アイデンティティ，データ，サービス」をつなぐ利用シーンへと普及拡大していく中で，アイデンティティ管理は，ますます重要度を増していくと考えられる．アイデンティティ管理がもたらすビジネス上の利点として，セキュリティやプライバシー保護の強化以外に，認証作業の簡便化による利用頻度の向上や，ユーザ獲得や定着が期待できる．また，同分野の研究活動も活発化しており，専門の国際的なワークショップが開催されたり[21]，PrimeLife等の国際的な研究プロジェクトが進行している[22]．

今後のアイデンティティ管理の課題としては，以下がある．

（1）　各技術の相互運用性の向上[23]

相互運用性には二つのレベルの側面がある．技術仕様レベル及び実装レベルの側面である．前者については，例えば前述のConcordia ProjectやOSIS（Open Source Identity Systems）[24]で検討が進められている．このような異種仕様の組合せ時の重要な技術課題として，認証結果の信頼度の表現及び解釈の方法の共通化がある．また，実装レベルの相互運用性については，例えば，Liberty AllianceではSAML製品やLiberty ID-WSF製品の仕様準拠認定テストを実施し相互運用性を確認している．

（2）　ライフサイクル全体の包括的なサポート

これまでに，シングルサインオンや属性交換は，技術標準の確立及び商用サービスへの導入もなされてきたが，それらはアイデンティティのライフサイクル全体から見ると「利用」の一部分でしかない．今後は，アイデンティティの作成，変更，削除等を包括的にサポートする技術や標準仕様が求められる．その中でも，アイデンティティ管理に係るサービス提供者やユーザがいかに信頼関係を構築し管理するかは重要な研究テーマになっている[25],[26]．

（3）　プライバシー保護の強化

ユーザ自身によるアイデンティティ情報の制御を可能にする技術の確立は，アイデンティティ管理及びプライバシー保護においても中心的な課題である[27],[28]．また，ユーザが主体的にアイデンティティ情報を管理するアプローチの研究が活発に進められている[29]．

（4）　モバイル・ユビキタス環境への対応

モバイル・ユビキタス環境において，ユーザが場所や時間を問わず様々なネットワークや端末，サービスを使いこなすために，一貫したアイデンティティ情報を提示できることが必要不可欠である．また，携帯電話は，いつでも持ち歩くパーソナルな機器で様々な認証セキュリティ機能を有するので，アイデンティティ情報を格納し管理するために重要な役割を果たすことが期待される[30]．

実世界における人々のアイデンティティの在り方は，長い歴史を経て形作られ，現在も日々問われ続けている．

仮想世界におけるアイデンティティの確立への道のりは遠く，まだ端緒についたところである．アイデンティティなくして真の意味で世界は成立し得ない．今後は，より善きアイデンティティに向けて，技術だけでなく，生活，文化，社会制度も含めた観点からの学際的な取組みの更なる活発化が期待される．

文　　献

(1) A. Cser and J. Penn, Identity Management Market Forecast: 2007 To 2014, Forrester Research Inc., 2008.
(2) Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, 2008. http://www.ftc.gov/opa/2008/02/fraud.pdf
(3) Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, 2005. http://www.ffiec.gov/pdf/authentication_guidance.pdf
(4) P. Seltsikas, M. Dunlap, G.K. Marsh, B. Crossland, and D. Combs, "Digital government's critical enabler: identity management?," Proc. 2008 Int. Conf. on Digital Government Research, pp.437-438, Montreal, Canada, 2008.
(5) E. Maler and D. Reed, "The venn of identity: Options and issues in federated identity management," IEEE Secur. Priv., vol.6, no.2, pp.16-23, March-April 2008.
(6) OASIS SSTC, Security Assertion Markup Language Version 2.0 (SAML 2.0), http://saml.xml.org/saml-specifications
(7) Liberty Alliance Project, Liberty Identity Federation Framework 1.2, http://www.projectliberty.org/liberty/content/download/1266/8160/file/liberty-idff-1.2-20050520.zip
(8) OASIS SSTC, Security Assertion Markup Language Version 1.1 (SAML1.1), http://saml.xml.org/saml-specifications
(9) Shibboleth Architecture, Protocols and Profiles, 2005. http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf
(10) Organization for the Advancement of Structured Information Standards, Security Services Technical Committee (OASIS SSTC), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
(11) Liberty Alliance Project, http://www.projectliberty.org
(12) General Services Administration, "Interoperability testing," http://www.cio.gov/eauthentication/documents/InteroperabilityTesting.pdf
(13) Liberty Alliance Project, Liberty Identity Web Services Framework 2.0 (Liberty ID-WSF), http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates
(14) OpenID Foundation, OpenID Authentication 2.0, http://openid.net/specs/openid-authentication-2_0.html
(15) OpenID Foundation, http://www.openid.net/foundation
(16) OpenID Foundation, OpenID Attribute Exchange 1.0, http://openid.net/specs/openid-attribute-exchange-1_0.html
(17) Information Card Foundation, http://www.informationcardfoundation.org
(18) Concordia Project, http://www.projectconcordia.org
(19) Higgins Project, http://www.eclipse.org/higgins/
(20) Liberty Alliance Web Harmonization Services Special Interest Group, http://wiki.projectliberty.org/index.php/Web_Services_Harmonization_SIG
(21) The Fourth ACM Workshop on Digital Identity Management, http://www.primelife.eu/
(22) PrimeLife Project, http://www.primelife.eu/
(23) Special Issue on Interoperable Identity Management Systems, Computer, to appear (April 2009).
(24) F. Paci, D. Bauer, E. Bertino, D.M. Blough, and A. Squicciarini, "Minimal credential disclosure in trust negotiations," Proc. 4th ACM Workshop Digital Identity Management (DIM 08), pp.89-96, 2008.
(25) Open Source Identity Systems, http://osis.idcommons.net/
(26) Proc. Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 08), Trondheim, Norway, 2008.
(27) J. Camenisch and E.V. Herreweghen, "Design and implementation of the idemix anonymous credential system," Proc. 9th ACM Conf. Computer and Communications Security (CCS2002), pp.21-30, Washington DC, USA, 2002.
(28) T. Kojima and Y. Itakura, "Proposal of privacy policy matching engine," Proc. 4th ACM Workshop on Digital Identity Management, pp.9-14, Fairfax, Virginia, USA, 2008.
(29) A.B.-Spantzel, J. Camenisch, T. Gross, and D. Sommer, "User centricity: A axonomy and open issues," J. Comput. Secur., vol.15, no.5, pp.493-527, 2007.
(30) T. Abe, H. Itoh, and K. Takahashi, "Implementing identity provider on mobile phone," Proc. 2007 ACM Workshop Digital Identity Management (DIM07), pp.46-52, Fairfax, Virginia, USA, 2008.

(平成20年12月8日受付　平成20年12月19日最終受付)

高橋（たかはし）　健司（けんじ）（正員）
昭59東工大・工・情報卒．昭61同大学院修士課程了．同年日本電信電話(株)入社．現在，NTT情報プラットフォーム研究所主幹研究員．アイデンティティ管理技術に関する研究開発及び国際標準化に従事．博士（工学）．