3 クラウドにおけるアイデンティティ管理の課題

伊藤宏樹　日本電信電話（株）

クラウドコンピューティングとアイデンティティ管理

アイデンティティ管理（Identity Management；IdM）技術はクラウドコンピューティングの利用，特にインタークラウドやハイブリッドクラウドといった，複数事業者が管理するクラウドに跨るサービスの実施には必要不可欠な概念として，近年その重要度が非常に高まってきている．しかし，アイデンティティ管理技術はクラウドコンピューティングに特化した技術ではない．これまでにも企業，組織の情報通信ネットワークにおけるM&A，組織再編，ビジネスプロセス見直し，内部統制強化等への対応を通じて発展してきた．クラウドコンピューティングにおいて必要となるアイデンティティ管理技術も，そのほとんどは既存技術に基づくものである．

本稿では，アイデンティティ管理技術の中でも特に，主としてWebアプリケーションの相互連携に用いられるいくつかの技術の概説を行うとともに，クラウド化により改めて顕在化するアイデンティティ管理にかかる課題，クラウドコンピューティング時代に求められるアイデンティティ管理について解説する．

アイデンティティ管理とは

--- アイデンティティとは ---

「アイデンティティ管理技術」について述べるにあたり，本稿では「アイデンティティ（identity）」の定義として高橋[1]およびKantara Initiative☆1 Japan Work Groupの定義[2]を引用する．

識別子（Identifiers）	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，学生番号，電話番号
クレデンシャル（Credentials）	ある情報の正当性を示すための情報 （例）パスワード，ワンタイムパスワード，電子証明書，印鑑，生体情報
属性（Attributes）	アイデンティティを特徴づける情報 （個人の例）氏名，住所，生年月日，所属，役職，信用情報，生体情報，人間関係 （企業の例）代表者名，所在地，ロゴ，定款，格付け情報

表-1　アイデンティティの3要素

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，表-1に挙げる3つの要素「識別子（identifiers）」，「クレデンシャル（credentials）」および「属性（attributes）」からなる．これらを適切に保護，運用する「アイデンティティ管理」とは，「ユーザ・アイデンティティを，安全かつプライバシに配慮した形で活用したサービスを提供するために必要となる，アイデンティティ情報のライフサイクル」，すなわちユーザ・アイデンティティの生成から消去に至るまでの，配布，活用，更新等のプロセス管理である．特に，ネットワークを介して複数のサービス間で連携して行われる「連携アイデンティティ管理」に用いられる技術が，本稿で取り上げる「アイデンティティ管理技術」である．

クラウドコンピューティングにおける連携アイデンティティ管理も同様に，ネットワーク上へのユーザ・アイデンティティの配布，分散したユーザ・アイデンティティの相互参照，更新，追加，削除等の実施に際して当該手続きを行うユーザの適切な管理，

☆1 Kantara Initiative, http://kantarainitiative.org/

図 -1　アイデンティティ管理技術の要素

および当該アイデンティティへのアクセス権限の適切な管理が必要であり，これらの機能の実現にあたっては後述する SAML，ID-WSF，OpenID，OAuth 等の既存の技術仕様が策定されている．

--- アイデンティティ管理技術の要素 ---

アイデンティティ管理技術は認証連携，属性交換の 2 分野に大別[☆2] される（図 -1）．以下，各技術要素について述べる．

■認証連携

認証連携とは，通常はサービスごとに必要なユーザ認証，ログアウトにかかる手続きを，1 カ所（認証者）に集約し，簡素化，単純化させることである．ユーザに代わって認証者は識別子の配布や，当該ユーザのログアウト通知を行うことで，ユーザ操作が簡素化される．

認証連携の主な要素には，「シングルサインオン（Single Sign-on ; SSO）」「シングルログアウト（Single Logout ; SLO）」「アカウント連携（Account Federation）」がある．

シングルサインオンとは，あるサービス（認証者）が発行した識別子を，他のサービス（認証要求者）のユーザの特定（identify）に用いることである．認証者は識別子とともに識別子の正当性を担保するクレデンシャル（例：電子署名）を発行する．認証要求者はクレデンシャルの正当性を検証の上，識別子をもとに自サービスを提供する．

シングルログアウトとは，シングルサインオンを行い，ログイン状態にある各サービスから，一括してログアウトすることである．認証者は，ユーザの要求に応じて，当該ユーザがシングルサインオンを行ったすべてのサービスに対して，ログアウト要求を発行する．

アカウント連携とは，シングルサインオン，シングルログアウトに必要な，認証者と認証要求者との間の，ユーザ識別子の紐付け作業である．

■属性交換

属性交換とは，属性提供者が管理する住所，氏名，メールアドレス，行動履歴等のユーザ・アイデンティティの，ユーザ同意に基づく属性要求者への提供である．

属性交換の主要な技術要素には，属性提供者が管

☆2　リバティ・アライアンス：リバティ仕様アーキテクチャ（2003）．

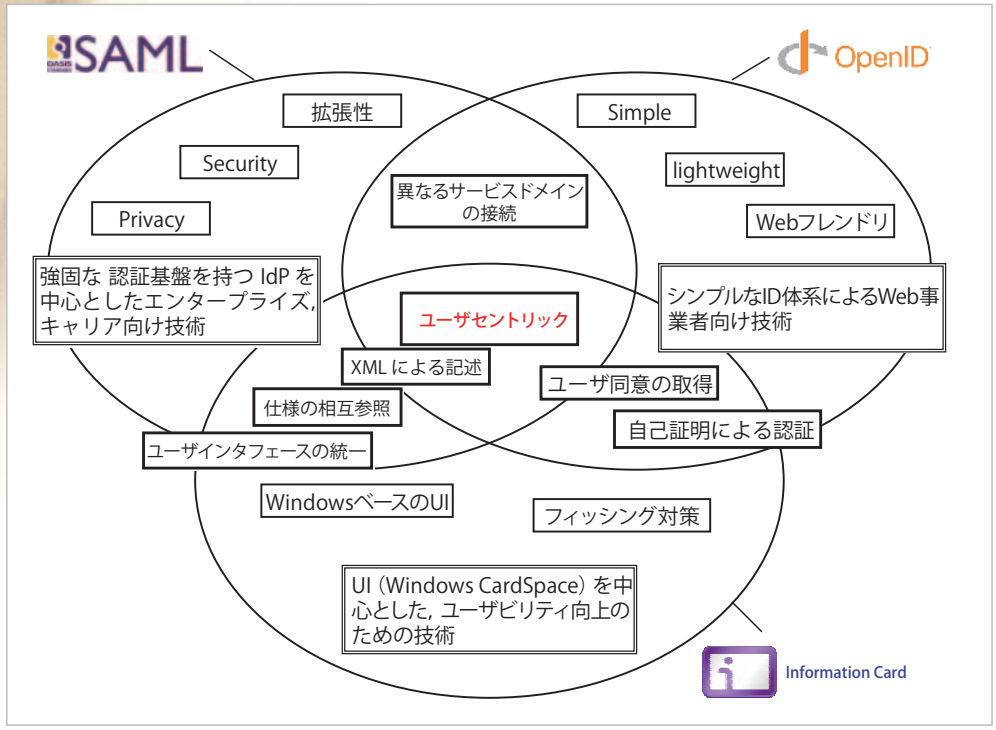

図 -2　主要認証連携方式の相互比較

理するユーザ・アイデンティティの属性要求者に対する提供方式，個々のユーザ・アイデンティティの記述方式，属性要求者による，ユーザ・アイデンティティの更新，削除方式，ユーザ合意の取得方式が挙げられる．

また，属性提供者による属性要求者へのユーザ・アイデンティティの提供は「探索（Discovery）」，「認可（Authorization）」，「交換（Exchange）」の 3 つの手続きに分類される．

探索とは，アイデンティティ管理にかかわるサービス（認証者，属性提供者等）のポインタ（当該サービスを特定する URL 等）の取得である．探索は個別のサービスが利用可能なポインタを保持し，ユーザの要求に応じて能動的に探索する方式と，ユーザが指定するサービスに対し探索する方式の，2 通りに大別できる．

認可とは，属性要求者と，属性提供者との間での，属性交換時の一時的なアクセス権限取得（権限委譲）である．属性交換時に，属性提供者は属性要求者に対しアクセス権限（認可トークン）を一時的に委譲（配布）する．属性要求者は，有効な認可トークンを属性提供者に提示し，ユーザ認証や，確認作業を経ることなく，ユーザ・アイデンティティを取得する．

交換とは，属性要求者が認可トークンを基に属性提供者からユーザ・アイデンティティを取得する際の，サービス間でのデータ転送方式である．

--- 主要アイデンティティ管理技術 ---

現在，アイデンティティ管理に関する多数の技術標準が策定ないしは策定作業中にある．個々の技術標準は異なる思想に基づき規定されており，Maler[☆3] により認証連携の観点（図 -2），および属性交換の観点（図 -3）から差別化，視覚化が行われている．本節では主要アイデンティティ管理技術の概要を述べる．

■ SAML 2.0

SAML（Security Assertion Markup Language）とは，認証連携に必要な，証跡文書（Assertion）記述方式および，Assertion のサービス間での共有方式で，OASIS[☆4] Security Services Technical Committee（SSTC）[☆5] にて 2006 年に規定された（図 -4）．

☆3 Maler, E. : Venn of Identity, http://vennofidentity.org/
☆4 Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org/
☆5 OASIS Security Services Technical Committee, http://www.oasis-open.org/committees/security/

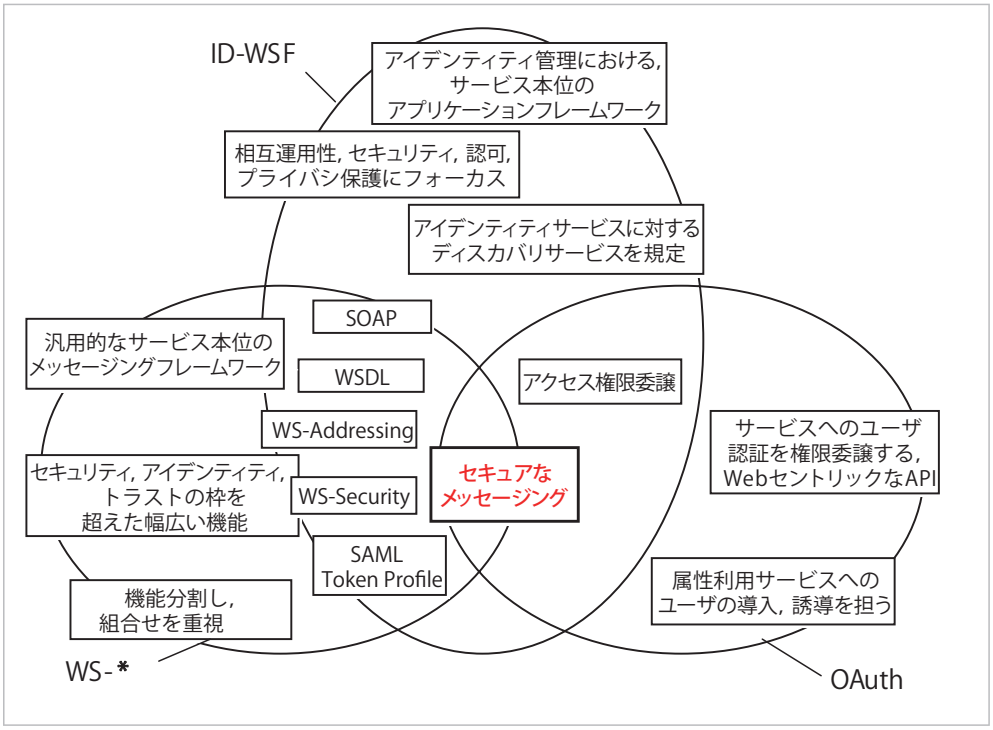

図-3　主要属性交換方式の相互比較

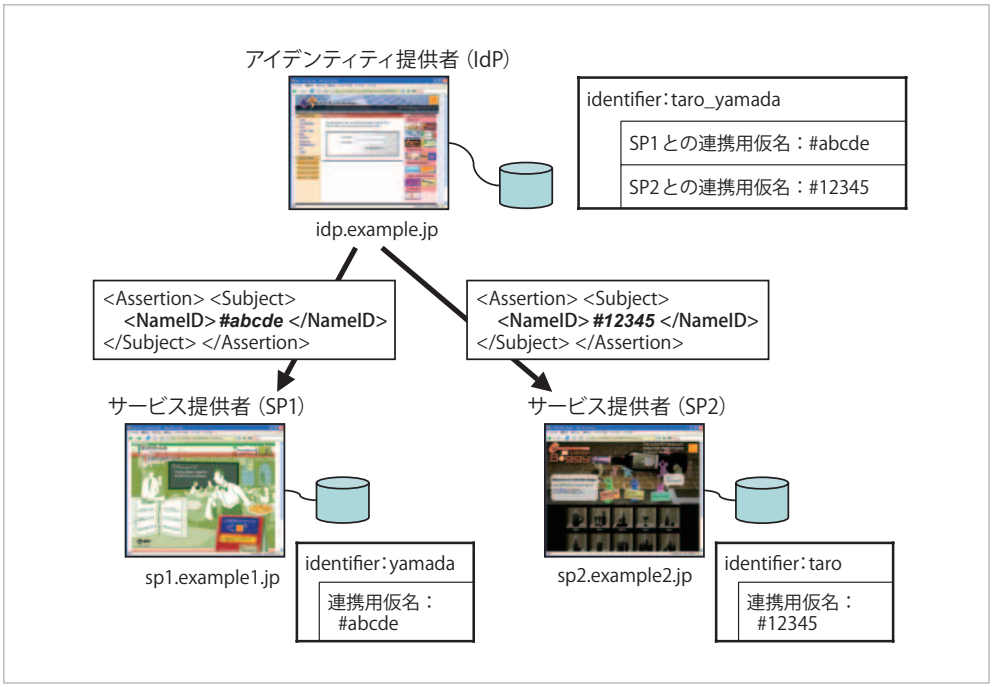

図-4　SAML 2.0 にてサービス間で共有されるユーザ・アイデンティティ

SAML は，アイデンティティ提供者（Identity Provider ; IdP）と，サービス提供者（Service Provider ; SP）との間の相互信頼（Circle of Trust ; CoT）構築を前提とする．契約関係にある企業集団等が，Web アプリケーションのポインタや，文書に付加される署名，暗号化の検証に必要な公開鍵等にかかる情報（メタデータ）を事前に相互共有する．

SAML Assertion は XML で記述され，他のアプリケーションで容易に再利用できる．たとえば後述する Information Card ではユーザ・アイデンティティを示すトークンに SAML Assertion を適用可能である．

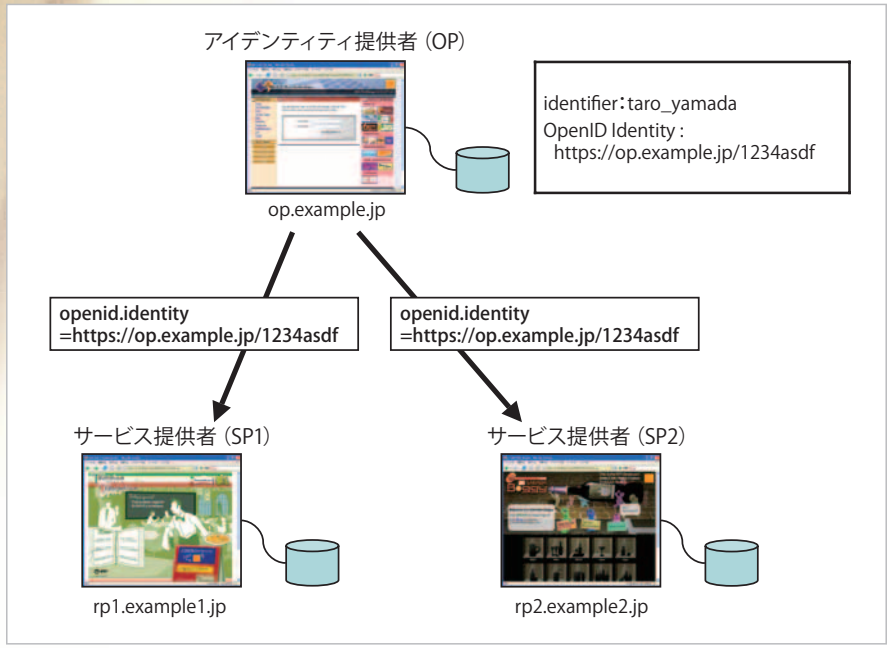

図 -5　OpenID 2.0 にてサービス間で共有されるユーザ・アイデンティティ

■ OpenID Authentication 2.0

OpenID とは，認証連携に用いられる，URI，XRI☆6 形式で記述される識別子等のユーザ・アイデンティティの配布方式で，OpenID Foundation☆7 にて規定されている．

OpenID では，アイデンティティ提供者（OpenID Provider ; OP）によって管理されるユーザ・アイデンティティが，サービス提供者（Relying Party ; RP）に配布される．識別子は OP が個々のユーザに対し発行するユーザ固有の URI 形式等を用いる．このため，RP は OP に依存せず，グローバルに一意にユーザを特定可能とする（図 -5）．

■ Information Card

Information Card とは，認証連携の一形態で，ユーザ端末上でユーザ・アイデンティティを「カード」の形で可視化させ，ユーザが端末上の「カードセレクタ」（Identity Selector）により簡単，確実な操作，利用を可能とする技術である．現在，技術仕様が OASIS Identity Metasystem Interoperability（IMI）☆8 TC にて策定中で，Information Card Foundation☆9 による広報，白書作成等の普及活動が行われている．

Information Card では，個々のユーザを特定する識別子や，氏名，メールアドレス等，個々のユーザ属性の要素名を「クレーム」と呼ぶ．属性要求者（Relying Party ; RP）は，必要なクレームをユーザ端末に通知すると，ユーザ端末は，属性提供者（Security Token Server ; STS）に当該クレームに対応するユーザ属性を含むトークン（Security Token）発行を要求する．Security Token はユーザ端末を経由して RP に送信される．

STS と RP とは信頼関係を構築し，RP は信頼する STS が発行した Security Token のみ受け入れることを前提とする．これは SAML における CoT と類似の思想である（図 -6）．

SAML，OpenID は一般的な Web ブラウザをユーザ端末（User Agent）の前提とするのに対し，Information Card は，ユーザ端末上で動作する Identity Selector を必要とする．Identity Selector の実装例として，マイクロソフト社による Windows CardSpace☆9, 10，オープンソースソフトウェアプロジェクトとして Higgins☆11 等が存在する．

☆6 OASIS Extensible Resource Identifier Technical Committee, http://www.oasis-open.org/committees/xri/
☆7 OpenID Foundation, http://www.openid.net/
☆8 OASIS Identity Metasystem Interoperability Technical Committee, http://www.oasis-open.org/committees/imi/
☆9 Information Card Foundation, http://www.informationcard.net/
☆10 Windows CardSpace Home Page, http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx
☆11 Higgins Project, http://wiki.eclipse.org/I-Card

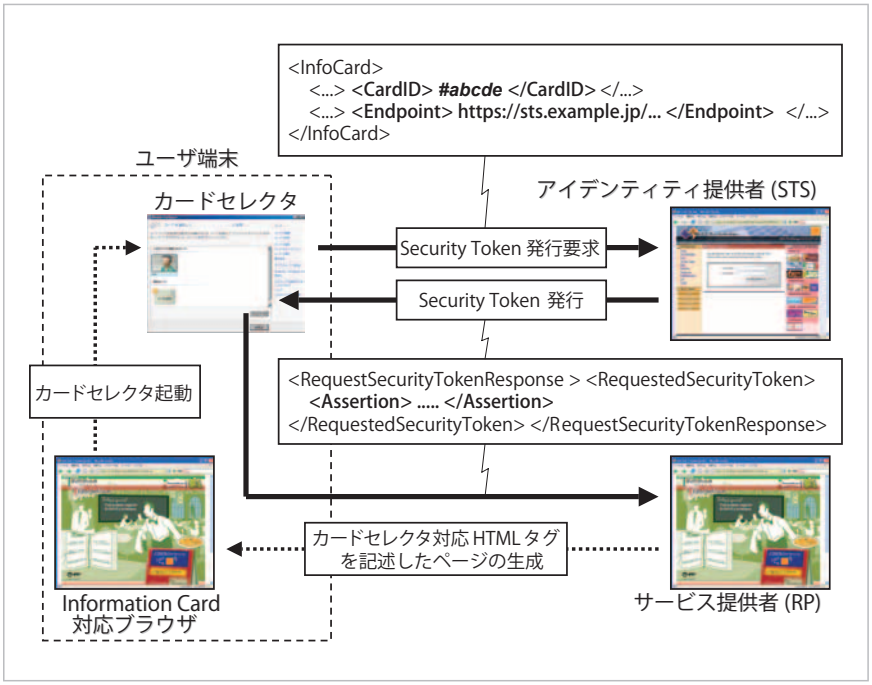

図 -6 Information Card にてサービス間で共有されるユーザ・アイデンティティ

■ ID-WSF 2.0

ID-WSF（Identity Web Services Framework）とは，属性交換を目的としたユーザ・アイデンティティ提供方式で，2006 年に Liberty Alliance にて規定された．

ID-WSF は，SAML 2.0 で規定する CoT を前提とし，CoT 内でユーザ属性の取得等に必要な，探索機能，認可機能，交換機能を規定する．これらの機能に必要な認証トークンには主に SAML 2.0 で規定される SAML Assertion が用いられる．

■ OAuth

OAuth とは，属性交換に必要な認可トークン配布に特化した，Web アプリケーション向け認可取得方式である．2007 年にオープンコミュニティ☆12 で仕様策定に着手し，現在では IETF のワーキンググループ☆13 が形成されている．

クラウドコンピューティングにおけるアイデンティティ管理

本章では，クラウドコンピューティングにおけるアイデンティティ管理の導入，運用に関する課題を，企業，組織等における既存の Web ベースの情報システムをクラウドに移行する場合をモデルケースとして，(1) エンドユーザ視点，(2) アプリケーション開発者視点，(3) サービス開発者視点，の視点から考察する．本ケースでは，ユーザ認証基盤等の基幹サービスを自社内のプライベートクラウドとして保有し，周辺アプリケーションの一部をパブリッククラウドに移行する，ハイブリッドクラウドを想定する．

--- エンドユーザ視点における課題 ---

複数事業者が提供するアプリケーションをエンドユーザがストレスなく利用するためには，ユーザ動線およびユーザ同意取得の明確化が必要である．

ユーザ動線の明確化には，認証連携，属性交換等の実施時に，認証要求者 Web サイトから認証実施者 Web サイトにユーザを混乱させることなくユーザ画面を遷移させることや，当該手続きの中止時に正確なユーザ誘導を行うことが挙げられる．

ユーザ同意取得の明確化とは，ユーザの意図しない認証トークン，ユーザ属性がサービス間で流通するのを防ぐために，ユーザ同意を確実に取得することである．たとえば，ID-WSF ではユーザ同意の取

☆12 OAuth, http://oauth.net/
☆13 http://datatracker.ietf.org/wg/oauth/

得証跡を第三者が担保する Interaction Service が規定されている．

--- アプリケーション開発者視点における課題 ---

クラウド移行に伴う開発上の課題例として，セキュリティレベルの整合，異種アイデンティティ管理技術の相互接続，アクセスコントロールが挙げられる．

セキュリティレベルの整合の例として，相互運用するサービス間の認証レベルの整合がある．

情報システム内で管理されるユーザ・アイデンティティには，高いレベルで秘匿とすべき情報と，そうではない情報とが混在し，これらを一律に同一手段にて保護することは適切ではない．各アイデンティティの開示に必要な認証手段は，アイデンティティ保証フレームワーク（Identity Assurance Framework；IAF）等を参照し，規定できる．

IAF とは Kantara Initiative にて規定された，アイデンティティ連携を行うサービス間で流通する証跡文書の，認証者により担保される 4 段階の保証レベルと，各レベルの担保に必要な事業者のサービス設計，運用基準を定めた標準文書である．アイデンティティ連携を行うサービスを，重要性，秘匿性等から 4 段階に分類し，各レベルにおける基準を定めている．

アイデンティティ開示時に必要な手段よりも簡易なユーザ認証方式を用いるとコンプライアンス上の課題が生じ，強固な認証方式で統一するとユーザ利便性低下や，運用コスト増大が生じる．IAF はこのような課題を未然に防ぐための標準文書である．

IAF は異種アイデンティティ管理技術の相互接続時にも有効である．OpenID と SAML 等，異なるアイデンティティ管理技術が実装されたサービス間の接続時に，IAF，Kantara Initiative Concordia Discussion Group が策定したガイドライン 等を参照して，接続するサービス間のセキュリティレベルを整合できる [3]．

SAML における保障レベル記述方式として認証コンテキスト拡張スキーマ（SAML V2.0 Identity Assurance Profiles），OpenID において Provider Authentication Policy Extension（PAPE）が規定されている．SAML, OpenID の 2 つのアイデンティティ管理技術標準間で証跡文書を相互変換し，複数のサービスを運用させる場合，本ガイドラインに基づく設計，実装，運用が統一基準として有効である．

クラウドではサービスに跨るアクセスコントロールが課題となり得る．たとえば，部門ごとに分散管理され，個々に開示，編集等の許可レベルが設定された文書群への一括検索に伴うアクセス制御が考えられる．OASIS eXtensible Access Control Markup Language（XACML），Liberty Alliance Identity Governance Framework（IGF）等の技術標準が存在する．

--- サービス運用者視点における課題 ---

クラウド移行に伴う運用上の課題例として，アイデンティティサービスの単一障害点化がある．

シングルサインオンにおける認証実施者，属性交換における属性管理者が単一障害点化の要因となり得るため，これらのサービスには非常に高い水準の可用性，一貫性が求められる．代替の認証手段や，属性管理手段が必要な場合も考えられる．

また，クラウド環境では，アプリケーション，オペレーションシステム，仮想マシン等の各レイヤでのユーザアカウントの分散管理，レイヤ間のアカウント連携の複雑化が生じる．あるレイヤで問題が生じた際に，他のレイヤのアカウントとの接続解除性（Unlinkability）が必要である．

アイデンティティ管理技術の今後の展望

--- クラウドにおけるアイデンティティ管理 ---

クラウドコンピューティングにおいて必要となるアイデンティティ管理のほとんどの要素は，アイデンティティ管理技術標準策定過程にて検討がなされた事柄である．今後，クラウドを用いた新たなサービスや，既存サービスの再構築が進捗するに従い，個々のケースでコンプライアンス確保，ユーザ操作

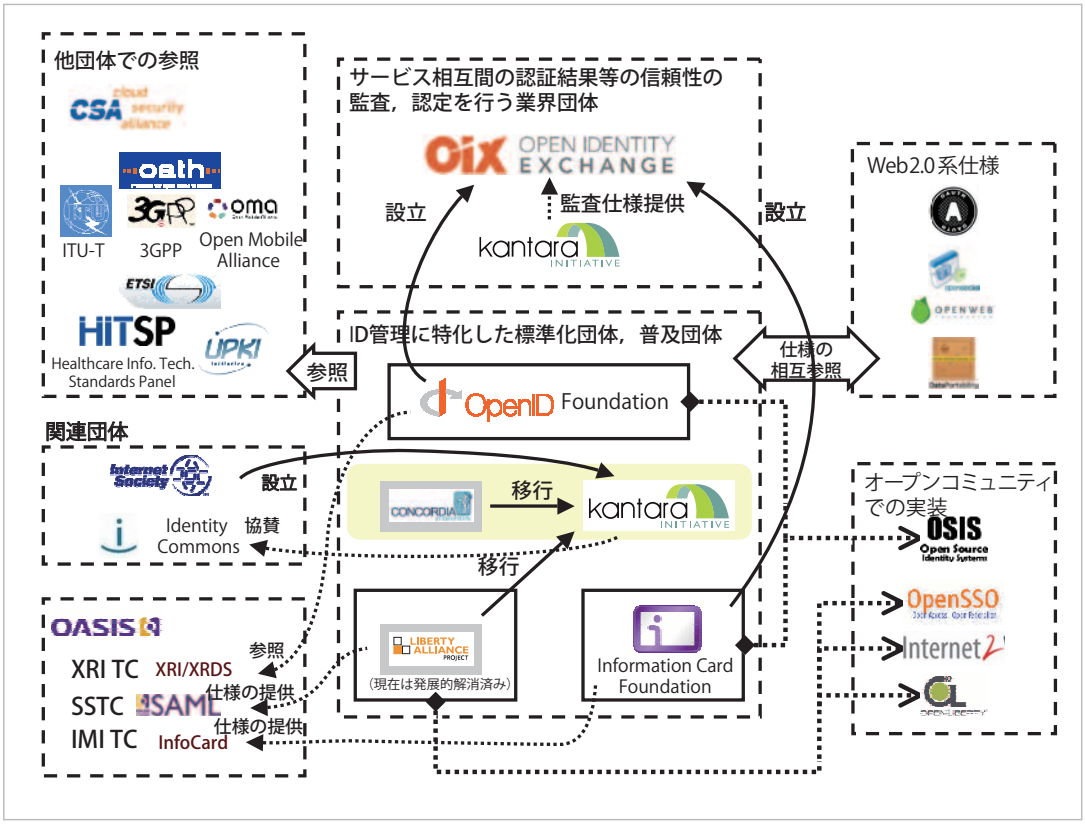

図 -7　アイデンティティ管理技術にかかる主要標準化団体，普及団体

の証跡管理，リスクマネジメント，複数サービスに跨るユーザ・アイデンティティのライフサイクル管理といった課題が予想されるが，基本的には既存のアイデンティティ管理技術の組合せにより解決可能であると考えられる．

ただし，クラウド化に伴い業務フローが多社間に跨る等のケースでは，ユーザ目線での単純化がアプリケーションの単純化に必ずしも繋がらない可能性がある．個々の業務フローで，多数の事業者が管理するユーザ・アイデンティティを統合的に利用することに対する，説明責任の担保，訴訟リスク回避等の検討が必要であり，このための適切なアイデンティティ管理技術の設計，利用が重要である．

--- アイデンティティ管理技術の今後の展望 ---

アイデンティティ管理技術においては，「アイデンティティ管理とは」および参考にて述べるように個々の技術標準の標準化はおおむね完了している．今後は適切なアイデンティティ管理の適用，実装，運用および，アイデンティティ管理技術を実装したサービス間の相互運用の確立に必要な，周辺文書等の整備等を通じて，当該技術に対する正しい認知の拡大が必要である．

(参考)アイデンティティ管理技術の標準化動向

現在，アイデンティティ管理技術の策定，普及活動にかかわる団体がいくつもあり，相互接続や，個々のニーズに特化した個別仕様策定等が行われている．図 -7[☆14] はアイデンティティ管理技術に関係する主要な標準化団体，普及団体を列挙したものである．以下，いくつかの団体の概要を記す．

---Liberty Alliance---

認証連携方式 Identity Federation Framework (ID-FF)，属性交換方式 ID-WSF 等の策定，セキュリテ

☆14 カンターラ・イニシアティブ発足記者説明会配布資料（2009 年 6 月 23 日），http://kantarainitiative.org/confluence/download/attachments/16646237/090623_KI_press_briefing.pdf，18 ページ

ィ評価，技術標準に基づく実装の相互運用性試験等の実施を目的として，2001 年から 2009 年まで存在していた標準化団体である．

現在では Kantara Initiative（後述）に吸収される形で発展的に解消している．

---OpenID Foundation---

OpenID 仕様の策定，普及活動実施を目的として 2007 年に設立された業界団体である．日本国内での普及活動を担う OpenID ファウンデーション・ジャパン☆15 が 2008 年 10 月に設立され，仕様翻訳，日本国内における意見集約，提言等の活動を行っている．

---Kantara Initiative---

Liberty Alliance 等，アイデンティティ管理に関係する 7 団体により 2009 年に設立されたオープンコミュニティである．アイデンティティ管理技術に関し，特定技術に依らない，より広い視点でのオープンな議論の場を提供し，技術間の相互連携を図ることを目的の 1 つとしている．

Kantara Initiative の活動の中心は Concordia Discussion Group，IAF，および電子政府向けアイデンティティ管理方式(拡張プロファイル策定)である．

Concordia とは異種アイデンティティ管理技術の相互運用性確保に必要な技術方式や，相互運用ポリシー等の検討，提案を目的としたコミュニティである．2007 年に設立され，Kantara Initiative（後述）設立に参画し，現在，同団体の一分科会（Concordia Discussion Group）に位置付けられている．

SAML，ID-WSF，OpenID，OAuth，WS-*，Information Card 等の技術標準の相互運用に必要な要件定義，ユースケースシナリオ策定等の検討，コミュニティ参加者に対する対外アピールの場の提供を実施している．

---OASIS---

Web サービス，電子商取引等，セキュリティおよび e ビジネスに関する技術標準策定を目的として 1993 年に設立された業界団体である．SSTC で SAML 仕様，IMI TC で IMI 仕様を策定しているほか，2010 年には Identity in the Cloud Technical Committee（Cloud TC）が設立され，「クラウドにおけるアイデンティティ管理」に関するユースケース収集，白書作成等の活動に着手している．

---Open Identity eXchange（OIX）☆16---

認証結果等の信頼性の監査，認定実施を目的として OpenID Foundation，ICF により 2009 年に共同設立された業界団体である．OIX では当初，米国連邦政府の下部組織が規定する“ICAM Profile”を監査プロファイルとして採用していたことに加え，2010 年 7 月に Kantara Initiative が策定する IAF が監査プロファイルとして新たに採用された．

（参考）アイデンティティ管理技術に関連したクラウド技術の標準化，普及動向

前章ではアイデンティティ管理技術の策定，普及に関連した団体を示した．本章では，相互連携や，文書の相互参照を行うなど，アイデンティティ管理技術にかかわりを持つクラウドコンピューティング関連団体の概要を記す．

---Cloud Security Alliance（CSA）☆17---

クラウドコンピューティング上のセキュリティ調査，分析，およびユーザ，ユーザ企業に対するセキュリティ啓蒙等を目的とし，2009 年に設立された国際業界団体である．

正式発足と同時公開された白書[4]ではクラウドコンピューティングにおけるセキュリティを 13 個のドメインに分類し，うち 1 個のドメインにてアイデンティティ管理に関し記述している．

白書ではシングルサインオン方式として SAML，

☆15 OpenID ファウンデーション・ジャパン，http://www.openid.or.jp/
☆16 Open Identity eXchange, http://openidentityexchange.org/
☆17 Cloud Security Alliance, http://www.cloudsecurityalliance.org/

WS-Federation，アクセス制御方式として XACML の利用を推奨し，推奨方式の採用により，独自方式のアプリケーションによるロックインが防げるとしている．インタークラウド向けにアイデンティティ管理技術標準間のメッセージ相互変換方式の必要性に言及している．

--- グローバルクラウド基盤連携技術フォーラム☆18---

クラウドコンピューティング技術に関連して，クラウド間連携システムに関するオープン化，インタークラウドの普及拡大に向けた啓蒙活動を目的として 2009 年に設立された国内産学官連携団体である．2010 年 6 月に公開した白書[5] はインタークラウド構築に関するユースケース，機能要件抽出等を行っており，10 種の機能要件のうち 1 つに認証連携が挙げられている．

インタークラウドにおける先駆けた検討は，ITU-T Cloud Computing Focus Group，IEEE Cloud Computing Standards Study Group 等からも高い関心が寄せられている．

--- スマート・クラウド研究会☆19---

次世代のクラウドコンピューティング技術等に関する検討を行う総務省主催の研究会である．2009 年 6 月に第 1 回会合が開催され，2010 年 5 月に報告書が発行された．同報告書「第 5 章 クラウド技術の標準化等」にて相互運用性確保の観点でアイデンティティ管理技術の要件に言及している．

--- オープンガバメントクラウド・コンソーシアム☆20---

政府系クラウドコンピューティングの実現に必要な技術要件，IT 統制要件，人材育成に関する議論等を目的とし，2009 年に設立された国内業界団体である．

OGC は活動内容の中で，クラウド事業成功の 4 要件の 1 つとして，「Cloud 間でのサービス利用を実現するための，Cloud 間認証連携の実現すること」と挙げている．

参考文献

1) 高橋：アイデンティティ管理の現状と今後：電子情報通信学会誌，Vol.92, No.4 (2009).
2) カンターラ・イニシアティブ・シンポジウム 2009「アイデンティティ管理の『現在・過去・未来』」，http://kantarainitiative.org/confluence/display/WGJ/Kantara+Initiative+Symposium+2009
3) Deployment Guide for Proxying Assurance between OpenID and SAML, http://kantarainitiative.org/confluence/display/concordia/Deployment+Guide+for+Proxying+Assurance+between+OpenID+and+SAML
4) Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, http://www.cloudsecurityalliance.org/csaguide.pdf
5) グローバルインタークラウド基盤連携技術フォーラム：インタークラウドのユースケースと機能要件（2010），http://www.gictf.jp/doc/GICTF_Whitepaper_20100628.pdf

（平成 22 年 8 月 31 日受付）

☆18 グローバルインタークラウド基盤連携技術フォーラム，http://www.gictf.jp/
☆19 スマート・クラウド研究会，http://www.soumu.go.jp/main_sosiki/kenkyu/smart_kuraudo/
☆20 オープンガバメントクラウド・コンソーシアム，http://www.open-gov-cloud.jp/

伊藤宏樹（正会員）| itoh.hiroki@lab.ntt.co.jp

2004 年東京工業大学大学院総合理工学研究科修士課程修了．同年日本電信電話（株）入社．2009 年東京理科大学総合科学技術経営研究科修了（技術経営修士）．アイデンティティ管理技術の研究開発，標準化に従事．