ネットワーク・アイデンティティとリバティ・アライアンスにおける Web サービスの動向

Evolution and Trends of Web Services based on Network Identity and Liberty Alliance

下 道 高 志

要 約 2002 年 7 月 15 日 Liberty Alliance Project の第一フェーズの仕様が公開された．インターネットの進化と共に，ユーザの使用形態および要求が高度化・複雑化している E コマースでの認証・サービスの標準化をめざす第一歩となる．

順次策定されるこの仕様によって，Web サービスの世界は，現在のポータルを中心とした個人毎のコマース（Personalized Commerce）から，連携コマース（Federated Commerce）の時代の到来が期待される．また，これから本格化するであろう Web サービスの仕組みそのものにも大きな影響を与えると思われる．単に BtoC のサービスだけではなく，その裏にある BtoB，さらには企業内情報システムへの本格的な応用が期待される．

本稿では，この Liberty Alliance Project のベースとなるコンセプトである Network Identity を，BtoC，BtoB そして企業システムへの応用といった面で考察する．

Abstract The specification for the first phase of Liberty Alliance Project was released on July 15th, 2002. This is the first step to standardize authentication and services for e-commerce for which user experience and requirements are getting advance and complex on evolution of Internet.

With establishment of the specification one by one, world of web services might be expected to come from Personalized Commerce to Federated Commerce. Those might give large effect to architecture of Web Services which should gain momentum from now. Not only BtoC services but also BtoB, which are hidden from the services, moreover real deployment to enterprise information systems might be considered.

This manuscript states and considers Network Identity, which is the basic concept for Liberty Alliance Project, in scope of BtoC, BtoB and application of enterprise information systems.

1. はじめに

Web サービスのコンセプトが紹介されてから約 2 年が過ぎようとしている．多くのベンダーや団体から，Web サービスに関連した技術や製品が紹介されているが，ビジネスへの本格的適用例は未だあまり存在せず，黎明期といえるのではないだろうか．その一方で Web サービスを UDDI（Universal Description, Discovery, and Integration），WSDL（Web Service Description Language）を前提とした狭義の技術的サービス・モデルから，Web 技術を使った実装方法である，より広義なインプリメント・モデルであると唱えるベンダーも多くなってきた．そうした中で，E コマースに求められることは，現在のポータルを中心とした個人毎のコマースから，図 1 の様にアイデンティティベースの信頼のおける連携コマースへと変化してきている．この連携コマースでは，個人・企業の両面からのビジネス的要求や利便性・安全性を満足させなくてはならない．そこで，まず現状の問題定義を行い，それに対する解決策であ

り基本的な技術・ビジネスコンセプトである Network　Identity を紹介する．また，Network Identity を基本コンセプトとし，その実装方法のための技術的仕様を 2002 年 7 月 15 日に発表した，Liberty Alliance Project に関しても言及する．

図 1　インターネットの利用の高度化

2.　E コマースの進化に伴う問題

2.1　個人の問題

インターネット技術の進化に伴い，サービスは高度化・複雑化してきている．当初はメール，そして Web サイト，簡単な決裁機能の提供と共にコマースの実現，そして今は，個々人の嗜好に応じたポータル・サイトによるパーソナライズされたコマースの時代が実現されつつある．

この一方で，複数のサイトで個別に個人情報を管理・運営しているのが現状である．例えば，ID やパスワードがサイト毎に違っていたり，数個の ID・パスワードならともかく，10 個以上のサイトのメンバーシップを保持している個人も数多く存在する．このような場合，本来であれば全部の ID・パスワードを記憶・使用することが個人に求められるわけであるが，現実には不可能である．そしてそれは同時に重要であるが非常に煩雑な個人レベルでの管理を個々に求めていることにもなる．

ここでこの煩雑な管理・運営を回避する為，ID・パスワードを 1 回（もしくは一つ）のログイン行為で，複数のサイトに対して同時にログインを行えるという SSO（シングルサイン・オン）の機能への要望が高まっているのが現状である．しかしながら，単に SSO を実現し，使用者の利便性を高めるだけでは十分ではない状況になりつつある．

現状を例に考察してみよう．ある個人が各サイトのメンバーになると，そのサイトでは属性情報の集合である個人のプロファイルが作成される．このプロファイルには ID・パスワードの他，住所・クレジット・カード番号なども含まれる．このような属性（attribute）情報の集合をここではアイデンティティと呼ぶ．

例えば，引越したり，クレジット・カードが変わってしまったら，このプロファイルのアイデンティティを変更する必要が生じる．数個のサイトに対してなら，この変更を行うことは難しくはない．しかしながら，これが十個以上もあるような場合，変更の作業は非常に煩雑なものになる．SSO だけでなく，本来はこうしたアイデンティティも論理的に一元管理・運営できれば非常に利便性が高まるはずである．

ここで重要なことは，あくまで論理的一元化であって，物理的一元化ではない．少なくとも

利用者側・管理者側にとってみれば，アイデンティティ管理をネットワークを通じて行なうことが出来れば，その実装形態はあまり重要ではないはずである．

このアイデンティティを複数のサイトで安全・確実に運用するためには，同時にセキュリティの面でも強固な基盤を築く必要がある．そして同時に，アイデンティティの認証（authentication）や認可（authorization）といった技術や適用基盤も，ネットワークベースのアイデンティティ・マネジメントには必要不可欠である．このようなネットワークベースのアイデンティティを Network Identity と呼ぶ．

2.2 企業の問題

競争力の維持に必要なものは，従業員の生産性の向上，顧客との関係のパーソナライズ，サプライヤとの業務効率の改善であるが，近年これと同時に総所有コスト（TCO：total cost of ownership）の削減も必要であるとの認識が高まっている．

こうした課題に対する一つの回答としては，従業員やビジネス・パートナーや顧客との連絡網をネットワークで結び，その関係を密にすることであると指摘されている．このために E ビジネスの世界，もしくは様々な業務でコンピュータ化が進んでいる企業においては，すべてのコンピュータ・アプリケーションに対して安全なアクセスを行なうために，SSO の環境を実現することが必要となりつつある．企業内の情報システムで SSO が進むと，同時に社外のパートナーやベンダーとの間での情報交換においても，時間的な効率およびセキュリティ面での強化を図ることが可能になる．こうすることによって，顧客の要求に応じた関係を電子的に実現，つまりは顧客のプロファイルを個別に作成し，企業側から提供する商品のカスタマイズ，アフィニティ・マーケティングの強化，将来の製品に向けてのデータ・マイニングに，このプロファイルに記述された情報を確実に活用できるようになると思われる．

しかし，このような高度に連携された E ビジネス・サービスへの移行を目指すとしても，多くの企業では困難に直面することとなる．ユーザのアイデンティティは，互換性のない複数のアプリケーション間に分散されており，それらのコントロールも，社内および社外に存在する無数のグループによる管理下に置かれているからである．このように顧客，パートナー，従業員に対するエントリが一元化されていないことは，企業の財産であるデータに不整合を生じさせ，セキュリティ面での一貫性を欠く要因になる．しかもこうした問題に対して，ある程度の一貫性を確立しようとする場合，運用コストの増大や場当たり的なセキュリティ対策に陥るケースが往々にして見られ，結果として当初の目的である有用な関係を構築・強化するためのチャンスを逃がすことも散見される．

現在の情報技術を駆使することによって，ビジネス・パートナや顧客との関係を上手く活用し，千万単位のユーザ数を確保することも企業にとって不可能ではない．その際に必要なものがアイデンティティ・マネジメントであり，ビジネス・パートナ間での効率的な運用ポリシー，プライバシー保護，操作といった機能をネットワーク上で実現できるシステムが求められる．これを実現するのが Network Identity である．

2.3 Network Identity

Network Identity は信頼のおけるネットワーク・フレーム内で管理されるコンテキスト・ベースのアイデンティティ，属性，アクセス権，資格といったものである（図 2）．Network Iden-

tity を管理することは，ソフトウェア基盤やビジネス・プロセスをそのライフサイクルおよびアイデンティティの使用といった面について管理することである．現行の基盤を拡張することによって，散在する膨大な数のアイデンティティ情報を整理統合し，顧客，ビジネス・パートナ，従業員に提供することが可能となる．例えば次のような利点が考えられる．

- 企業にとっては，Network　Identity を管理することで，雑多なアプリケーション（例えば保険給付金の申請や支給）にシングルサイン・オンで従業員がアクセスできる体制を整えると同時に，アプリケーションの統合を簡略化しつつ適切なセキュリティ・レベルを設定することも可能
- 顧客およびその管理の面では，Network　Identity を利用することで，企業と顧客の間に密なコミュニケーションを確保することが出来，同時に一対一の関係を確立することで，製品提示のカスタム化や，アフィニティ・マーケティング，データ・マイニングといったものも実現可能
- ビジネス・パートナーにとっては，Network　Identity を活用することで，不正な取引の危険性を抑制し，安定した企業関係の構築を促進することが可能
- セキュリティの面では，統一されたポリシーでの管理・運営が可能なため，分散環境においても確実な対策が施される．また，不要な属性データは各々のサイトでは抱え込まないので，逐次更新等が容易・安全に行なえる
- 同時に個人情報保護という面でも，個人に関連した属性情報が保持・管理されるサイトが限定されるので，情報流失，プライバシー侵害の可能性が低い

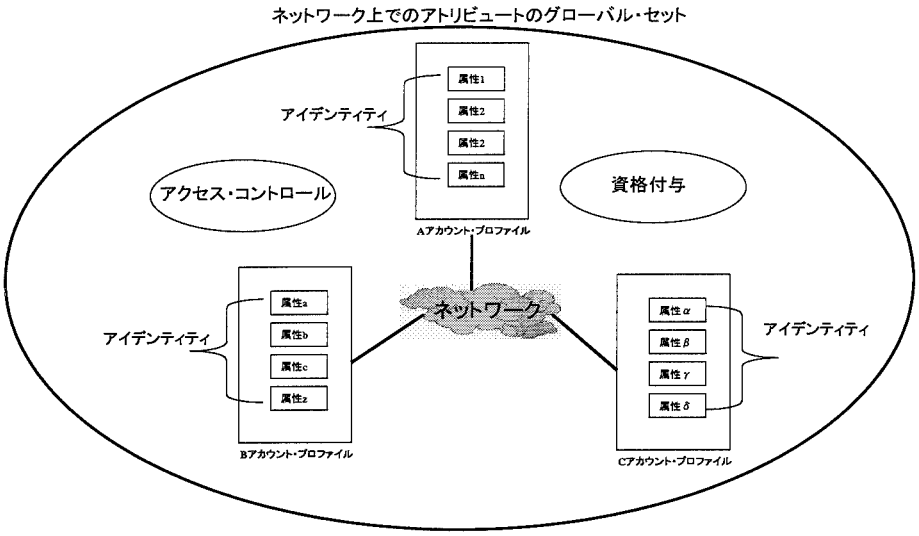

図 2　ネットワーク・アイデンティティ

3.　E コマースの実現形態

3.1　集中化モデルの限界

Network Identity を実現するためのシステム構築を BtoC の世界で考えてみる．最も簡単な方法は，すべてのアイデンティティ情報を一箇所のサーバーに集中する方法である．この場合は技術的には比較的平易で，むしろルール設定や，運用上のセキュリティといったものが最も

重要となる．これを一般的には集中化モデル（Centralized Model）と呼ぶ．

ここで例として BtoC ビジネスでの適用を考察する．今，本の物販サイトであるナイル・ドット・コムと医療診断・情報サービスのドクター・ドット・コムという二つのサイトを想定する．ナイル・ドット・コムのプロファイルには属性情報として ID・パスワード・クレジット・カード番号・本の嗜好・デリバリ方法があると仮定する．（本の嗜好という属性情報によって，ナイル・ドット・コムは個人毎の嗜好に合わせたダイレクトメールを送るといったような個人毎のマーケティングが可能になる．）一方，ドクター・ドット・コムのプロファイルには，ID・パスワードの他，社会保険番号・血液型・食事の嗜好といった属性情報があると仮定する．

従来の技術によるシステム構築においては，この二つのサイトが独立して運用されているとすると，この二つのサイトが保持するプロファイルも完全に独立して存在する．例えばドクター・ドット・コムで，「高血圧．食事に注意」という診断がされたとしよう．ユーザがこの診断結果を見て，ナイル・ドット・コムで書物を購入しようとした場合，ユーザはナイル・ドット・コムのサイトに自らログインし，例えば「高血圧の人のための食事レシピ集」を，キーワードを駆使しながら（例えば食事の嗜好も加味しながら）独力で探す必要があった．

3.2　オープン連携型モデル

ところでこの二つのサイト，ナイル・ドット・コムとドクター・ドット・コム間で，属性情報をバックチャネルを通して双方向に自動的に流せると仮定してみよう．ドクター・ドット・コムの診断に続いて「高血圧の貴方にナイル・ドット・コムよりレシピ集の紹介があります」というメッセージを出力し，さらにそこに表示されているリンクをクリックすることによってナイル・ドット・コムへ自動的にログインされ，「高血圧の人のための和食全集」をその個人に提示するといったマーケティングが可能になる．これは各サイトが持っている複数の属性情報，すなわちアイデンティティを，ネットワークを通じて交換し，新たなサービスを生み出すという例である．図 3 にそのイメージを示す．この実現されるコマース形態を連携コマース（Federated　Commerce）と呼ぶ．今，この連携型コマースの時代がやって来ようとしている（図 1）．

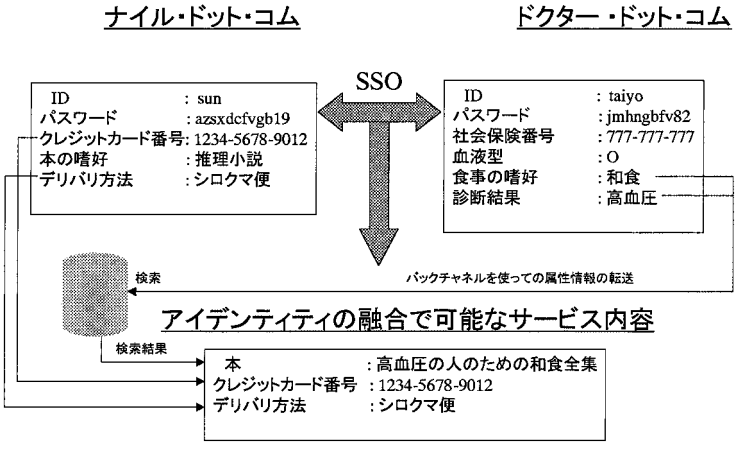

図 3　連携コマース

さて，ここで重要なことは，ナイル・ドット・コムの持っているアイデンティティとドクター・ドット・コムのそれとは各々独立であることである．本の嗜好といったものはドクター・ドット・コムには不要な情報であり，逆に一連の医療情報もナイル・ドット・コムには不要である．またユーザの立場で考えても，不必要な情報を第三者が常に保持するということに関し嫌悪感を抱く人も多いと思われる．

ビジネス上必要な事は，新たなサービスを行うために関係するサイト同士のみが，必要な属性情報をネットワークを通して交換・融合し，それに対して認証・認可を行って Network Identity を実現することである．前述した集中化モデルに対して，この形態をオープン連携型モデル（Open Federated Model）と呼ぶ．これを比較したのが図 4 である．

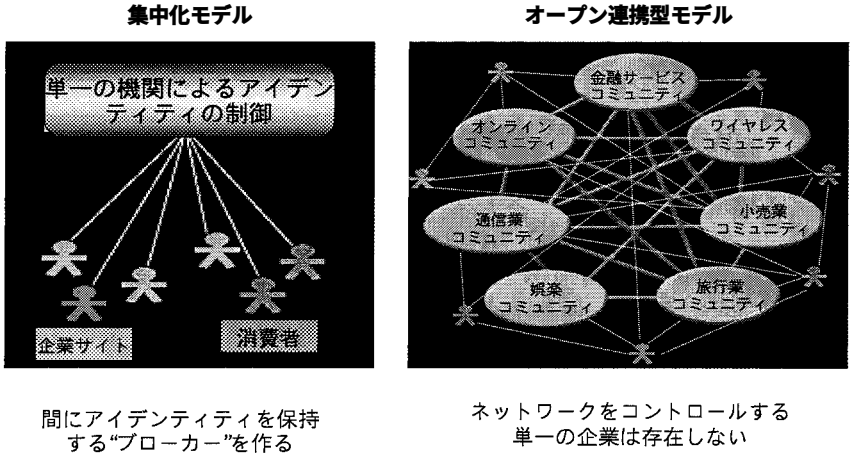

図 4　オープン型連携モデル

図 4 で示すオープン連携型モデルが，図 3 におけるナイル・ドット・コムとドクター・ドット・コムとによる連携コマースである．集中化モデルの場合，すべてのアイデンティティ情報が一箇所に集中される．つまり各サイト，図 3 の場合はナイル・ドット・コムとドクター・ドット・コムが保持している顧客のアイデンティティ情報を放出し，どこか他のサイトに預けることとなる．このことは単に情報システムのアーキテクチャの問題に留まらず，ビジネス・アーキテクチャの問題として提起されることとなる．

4.　Network Identity の進化

図 5 に示すように，Network　Identity は複数のステージを経て進化する．ステージが進むほど，より高度なアイデンティティ利用型サービスが可能となる．

Stage 1 : Multiple，Mutually Exclusive Relationships :

最も単純なアイデンティティフォームで，現在最も広範囲に適用されている．消費者や企業は，一対一の関係をオンライン商店との間で築くが，関係毎に個別のプロファイル管理を行う必要があり，非常に煩雑なものとなる．このシステムでは相互提携型のサービス・フォームはサポート不可能である．また消費者に関するデータは信頼できるかどうかは別として個々の企業が保持するため，プライバシーの侵害やアイデンティティの漏洩の危険性が存在する．

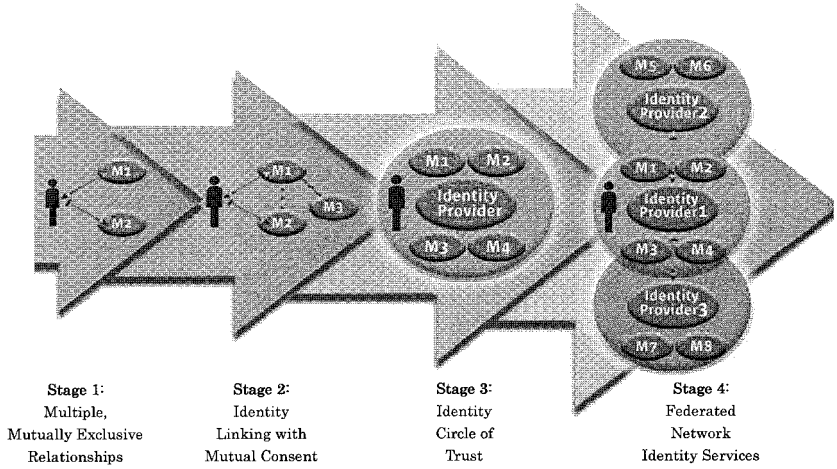

図 5　Network Identity の進化

Stage 2 : Identity Linking with Mutual Consent :

このステージでは，複数のマーチャント間である程度のユーザアイデンティティが共有される．この共有は，消費者とマーチャントとの合意に基づいて行なわれるが，個々のマーチャントとの取引にあたっては，それぞれの固有のアイデンティティプロファイルが必要となる．消費者はマーチャントとの直接の関係を継続するのと同時に，他のマーチャントのサービスを紹介することも可能である．

Stage 3 : Identity Circle of Trust :

このステージを特徴付けるのは“Circle of Trust”の構築であり，ここではユーザとサービス・プロバイダの双方がアイデンティティの認証に関する信頼できるソースとして，Identity Provider を利用することになる．消費者がマーチャントを利用するにあたっては，自分のアイデンティティを直接提供するのか，あるいは Identity Provider 経由で提供するのかを選択できる．Identity Provider は，消費者の代理としてそのプロファイルを管理し，マーチャントはこの Identity Provider を利用してアイデンティティの認証を行なう事で，商取引をスムーズに進行させる．

Stage 4 : Federated Network Identity Services :

複数の Circle of Trust を連結して，peer to peer 型ネットワークを構成し，信頼できる Network Identity Provider 間でアイデンティティを共有するステージである．Federated Network Identity を実装したビジネスモデルが生み出すビジネス・チャンスは莫大なものと予想されており，同時に内外の企業にも大きな影響を及ぼすことになると予想される．ステージ 3 の Circle of Trust モデルでも，消費者とマーチャントはある程度のメリットを受けられるが，複数の Circle of Trust を連携化（federation）することによって更に大きな恩恵を受けることが可能になる．アイデンティティを連携化することで，消費者は複数の Circle of Trust を自由に利用できるようになり，認証用の情報登録を何度も繰り返すことなく，必要なサービスにアクセスできるようになる．

5. Network Identity のコンポーネント・モデル

アイデンティティ共有を行う企業間では，共通のアイデンティティ・インフラを確立し，アイデンティティ・マネジメントを行う必要がある．そうすることによって初めてこれからのWeb サービスとそれに対応したアプリケーションを実現することが可能になると考えられる．そのためには企業は次に示す項目の実現を念頭に置き，情報システムに実装する必要がある．

- 安全で信頼のおけるアイデンティティの作成と管理を実現し，ビジネスにおいてユーザの識別を容易にし，認証を行いコストの削減を可能にすること．
- ロールやルールを利用することでユーザ，デバイス，アプリケーションに対して権限を与え，企業のリソースであるユーザを認証すること．
- セキュリティを侵害することなく，適切な時間と場所で企業リソースへのアクセスが可能かつ便利になること

Sun Microsystems は，共通のアイデンティティおよびそれに付帯するコンポーネントを表す Network Identity のコンポーネント・モデルを図 6 の通り定義している．

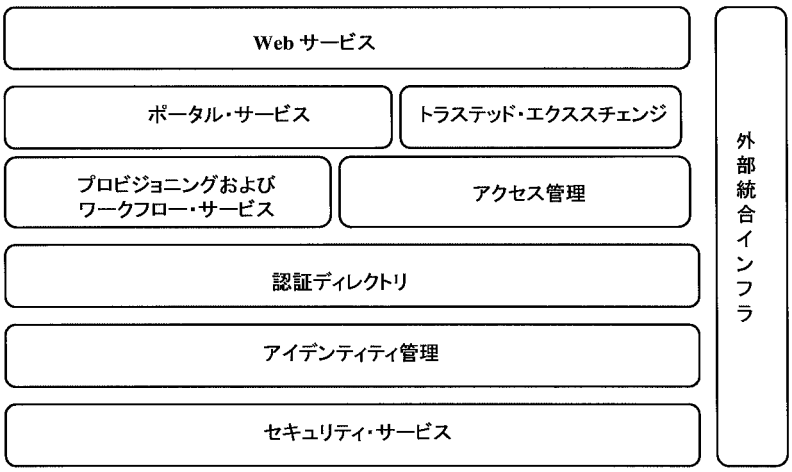

図 6 Network Identity のコンポーネント・モデル

Network Identity のコンポーネント・モデルでは， 共通のアイデンティティ・インフラは，セキュリティ・サービス，アイデンティティ管理，認証ディレクトリ，アクセス管理，プロビジョニングおよびワークフロー・サービスで構成されている．さらにポータル・サービス，トラステッド・エクスチェンジ，外部統合インフラの各コンポーネントを加えてフレームワークを完成させている．そしてこのフレームワークによって Network Identity 対応の Web サービスを提供する基盤として定義され提供している．

5.1 共通のアイデンティティ・インフラにおける五つのコンポーネント

Network Identity の実装が成功するか否かは，共通のアイデンティティ・インフラを構成する五つのコンポーネントのシームレスな共存が必要である．次に各コンポーネントの機能を説明する．

1) セキュリティ・サービス

アイデンティティの識別・認証・認可の機能を提供する．同時にこの機能はセキュリティの基盤も実現する．セキュリティ・サービスは，企業のリソースに対してユーザの安全なアクセスを保証し，組織内におけるそのロールも決定させる．そうすることによって，企業内のビジネス・ポリシーの統治方法をセキュリティ・サービスとして提供することが可能となる．

2) アイデンティティ管理

属性・資格認定，資格供与を含めたアイデンティティの作成・維持を行うインフラを提供する．アイデンティティ管理の機能としては，一元管理，セルフ・サービス，更新，第三者からのアサーション等が挙げられる．またユーザに対する正しいリソースのアクセス管理といった一連のアイデンティティの認証プロセスも含まれる．

3) 認証ディレクトリ

アプリケーションやネットワーク・リソースだけでなくアイデンティティ・プロファイルを維持・管理する統合リポジトリを実現する．このディレクトリには，公開鍵証明書，パスワード，暗証番号といった情報が保管される．アプリケーションやサービスは，この認証ディレクトリからアイデンティティ情報を取り出す．また，データベース，アプリケーション，ネットワーク OS といったものに分散するアイデンティティ情報を同期化するメタ・ディレクトリという実装も存在する．

4) アクセス管理

アイデンティティ情報が「いつ」「どうやって」使われるかを管理する．Web ページやアプリケーション，あるいはサービスに対するユーザのアクセスを規定するために，ユーザ認証を管理する．具体的には認証，セッション管理，アクセス監査といった機能が含まれる．

5) プロビジョニングおよびワークフロー・サービス

プロビジョニングは，アイデンティティに関するロールとルールといった，ビジネス・ポリシーを実行するプロセスである．このプロビジョニング・プロセスは集中化も分散化も可能であり，アプリケーションやデータだけでなく，クレジット・カード，テレフォン・カード，PC のようなネットワーク関連のデバイスも含まれる．ワーク・フローは，高度の自動化により，プロビジョニング・プロセスの生産性を向上させる．

5.2 共通のアイデンティティ・インフラをサポートするコンポーネント

Network Identity 環境において，Web サービスの活用を最大限に生かすために，サポート・コンポーネントは共通のアイデンティティ・インフラには無い機能を以下のコンポーネントで提供する．

1) ポータル・サービス

ポータルは，ユーザのロールと嗜好に基づいてコンテンツとサービスを集約し，提供する．Web サービスの機能とデリバリの機能を分離することによって，デバイス非依存にすることが可能となる．

2) トラステッド・エクスチェンジ

複数のビジネス間でのトランザクションのアカウンタビリティとトラッキングを提供し，トランザクションの信頼性を保証する．このトラステッド・エクスチェンジのインフ

ラを利用することによって，アイデンティティの認証を自動化することが出来，結果としてオペレーションに関連したコストを削減し，暮れベルのセキュリティを実現することが可能となる．

3） 外部統合インフラ

標準化プロセスやオープン・スタンダード準拠のテクノロジーを提供することによって，複数のアイデンティティ・システムとの通信が可能となる．また，標準技術を用いることによって，コンポーネントのアウトソーシングも実現できる．

6. Liberty Alliance Project

オープン連携型モデルを実現するためには，多くの技術的な困難が伴う．それを解決するにはプロファイルや相互認証のための業界標準が必要であった．都度個別にプロトコル，API等を規定・作成するとコストもかかる上，独自仕様のために相互接続性を確保するのが困難となることが予想された．新しいサービスや商品の提供のためには，これら Network Identity を標準化する作業が必要とされた．この標準化を策定するための alliance が Liberty Alliance Project（以下，LAP と記述する）である．

LAP ではフェーズに区切って仕様を策定・公開する予定である．2002 年 7 月 15 日に第一フェーズとして，Liberty Spec 1.0 が公開された．

認証情報受け渡しのために SAML（Security Assertion Markup Language：OASIS により策定された仕様）を取り入れた SSO，ならびに既存アカウントを関連付ける Account Federation の機能を中心とした仕様 1.0 が公開された．

Liberty Spec 1.0 では次の六つの項目について定義されている．

① 選択可能なアカウント・リンク
② リンクされたアカウントでのシンプルなサイン・オン
③ 認証コンテキスト
④ グローバル・ログ・アウト
⑤ Liberty Alliance クライアント仕様

以下，上記①–③を簡単に紹介する．

「選択可能なアカウント・リンク」および「リンクされたアカウントでのシンプルなサイン・オン」は，Opt-in account linking 仕様を指す．従来の SSO では，新たなアカウントを発行して，複数のサイトでの SSO を実現するのが一般的であった．しかしながら，現実には既にユーザがアカウントを持っているサイトで，そのアカウントを使っての複数サイトへの SSO を実現したほうがユーザにとって利便性が高い．これを実現する為に，account federation という機能を使い，既存のアカウント同士をリンクさせる．具体的には明示的なアカウント名を交換する代わりに，発行人（issuer）によってのみ解決可能な不透明なハンドル（オペイク・ハンドル）を交換することによって実現させる（図 7）．

「認証コンテキスト」は，認証のためのメッセージング・コンテクストに OASIS（Organization for the Advancement of Structured Information Standards）によって策定された SAML（Security Assertion Markup Language）を使用する．SAML は B 2 B 等複数サーバーへの XML メッセージングを想定しており，HTTP/SOAP メッセージへ付加される．図 8 に SAML の例を示す．

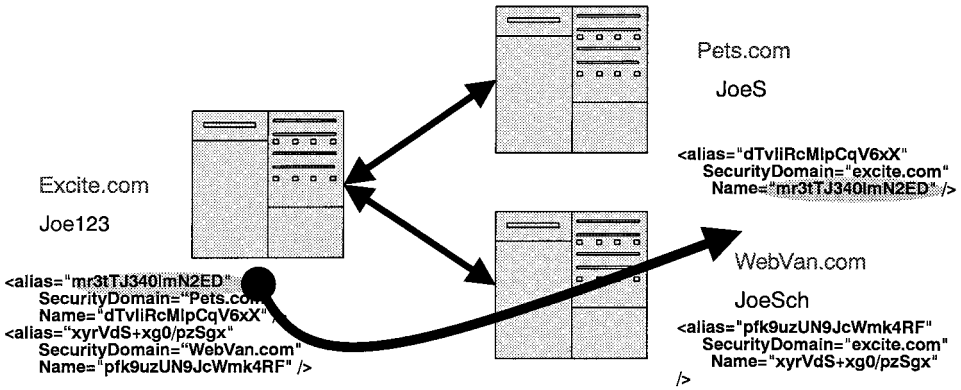

図 7　オペイク・ハンドルによる account federation

```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees//security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV-Body>
        <samlp:Request xmlns:samlp="…" xmlns:saml="…" xmlns:ds="…">
            <ds:Signature> … </ds:Signature>
            <samlp:AuthenticationQuery>
            …
           </samlp:AuthenticationQuery>
        </samlp:Request>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SAML による認証取得の例

```
Content-Type: text/xml
Content-Length: nnn
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV-Body>
        <samlp:Response xmlns:samlp="…" xmlns:saml="…" xmlns:ds="…"
             StatusCode="Success" >
          <ds:Signature> … </ds:Signature>
          <saml:Assertion>
            <saml:AuthenticationStatement>
            …
           </saml:AuthenticationStatement>
          </saml:Assertion>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

図 8　SAML による認証要求の例

LAP には仕様公開時点で，全世界から 70 近い企業・非営利団体・政府関連団体が参加した．(2002 年 12 月末時点で約 150 社）LAP ではあくまで商業的な利用を促進するための標準技術仕様を策定することを目的とし，製品やサービスは提供しない．それらは各企業がビジネスとして行なうこととなる．また策定される標準仕様は，スキーマや API，プロトコルといったものであり，XML で表現されている．仕様では，サービスを受ける対象となるデバイスは PC 等の端末だけでなく，将来的には PDA・携帯電話・KIOSK 端末・IC カードといったものも想定している．また，各国・地域の法規制等を考慮した上での標準化策定も，LAP の大きな特徴となっている．

7. 次世代 Web サービスの実現

E コマースや Web サービスが提唱される一方，本格的な商用サービスが実用化されないのが現実である．多くのメディアの調査によって，消費者がセキュリティの面で信用が置けないことがその最たる理由であることが明らかにされている．ところが問題にされているセキュリティの内容を調べてみると，それは殆どがアイデンティティの管理・運営についてであった．つまり，属性・認証・認可をインターネット/イントラネット上で安全・確実に使用できれば，多くの消費者が安心してサービスを利用できることになる．これは即ち，Network Identity は Web サービスの基盤であることを意味している（図 9）．

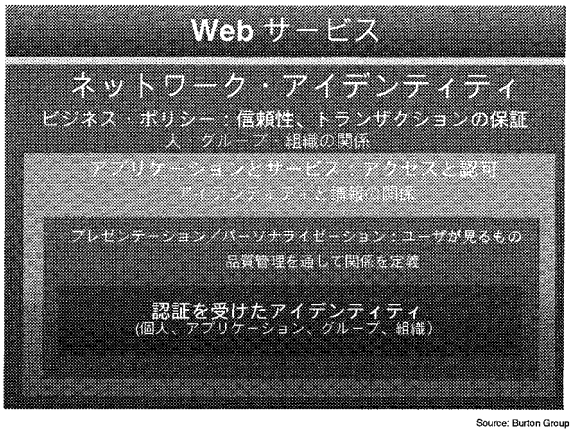

図 9　Web サービス基盤としての Network Identity

Network Identity は Identity Management の側面と，それをベースとしたサービスである Identity Service から成り立つ．そして Liberty Alliance Project は Network Identity ベースの Web サービスのための技術標準化における中心的存在である．順次公開される仕様は，Web サービスの高度化に大きく影響すると思われる（図 10）．

次の段階の新たな E-コマースである Web サービスを実用化するためには，Network Identity を正しく理解し，サービスに実装することが必要である．同時にそれは消費者やユーザの

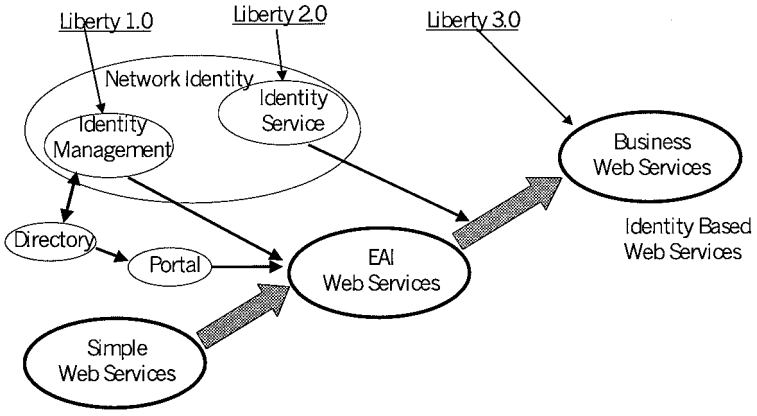

図 10　Web Services の進化過程

要求を満たし，企業にとっても ROI の極大化という恩恵をもたらすと思われる．

参考文献
［1］ Liberty Alliance Project（2002）: Liberty Architecture Overview
［2］ Sun Microsystems（2002）: Strategic Implications of Network Identity
［3］ Sun Microsystems（2002）: How to Implement Network Identity
［4］ Takashi Shitamichi（2002）: Web+Design vol 10 : Network Identity

執筆者紹介 下　道　高　志（Takashi Shitamichi）
慶應義塾大学商学部卒業（計量経済学専攻）．日本ユニシス(株)，(株)アルゴ 21 を経て現在サンマイクロシステムズ(株)に勤務．中小企業診断士，システムアナリスト，(前）公認情報システム監査人（CISA）主な著書：経林書房「小売サービス業勝ち残る店はここが違う」（共著），日本能率協会「SAP　R 3 ハンドブック」（共著），日経マグロウヒル「UNIX System V 上級プログラマ・ガイド」（共訳），日経マグロウヒル「スーパーユーザのための UNIX」（共訳）他多数．