

デジタルアイデンティティマネジメント の興隆

NRIパシフィック 渡辺 哲

インターネットの普及により急速に拡散してしまった個人情報をいかに管理するか、あるいはWebサービスなどで本人認証をいかにスムーズに行うか。これらの課題に対応するため、近年米国で注目を浴びているのがデジタルアイデンティティマネジメントである。本稿では、デジタルアイデンティティマネジメントの基本要件を定義し、技術や標準化の動向を紹介する。

散在する個人情報とその管理

現代社会では「私」に関する情報、すなわち個人情報があちこちに散在する。クレジット会社には「私」の購買履歴、区役所には「私」の住民登録、勤務先には「私」の健康保険の情報があるといった具合である。「私」であることを同定でき、それをデジタル情報として保管したものは「デジタルアイデンティティ」と呼ばれる。そしてデジタルアイデンティティの作成から廃棄に至る全過程を管理することを「デジタルアイデンティティマネジメント」と定義することができる。

個人情報は、インターネットが普及し、オンラインショッピングなどの各種サービスで住所や電話番号などの個人情報を入力する機会が増えたことによりさらに拡散していった。そして本人であることを認証するために各サイトで個別に求められるIDとパスワードの管理が利用者の大きな負担になっている。

デジタルアイデンティティマネジメントの基本要件

デジタルアイデンティティマネジメントには、このような負担を解消することとあわせ

て、個人情報管理に必要なさまざまな機能が求められる。その基本要件をまとめると以下のようなになる。

認証情報共有による一度限りのログイン（シングルサインオン）

利用者の個人情報にアクセスする権限を管理できること。

権限管理規則に基づいてアクセスが行われていることを保証するため監査証跡（ログ）が取れること。

複数の環境に分散した個人情報の相互運用性を確保できること。

盗難やなりすましを防ぐため個人情報のセキュアな保管ができること。

米国における実用化に向けた動き

現在、こうした要件についてのコンセンサス自体が十分ではない状況である。しかし米国では、デジタルアイデンティティマネジメントの実用化に向けたさまざまな動きがみられる。

ディレクトリサービスによる製品群

従来からの個人情報の属性管理のスキームであるディレクトリサービスを使用した製品がIBM社、ノベル社などからリリースされて

いる。しかし異なったベンダーのディレクトリサービス間で互換性が十分に保証されているわけではない。

シングルサインオンを実現するサービス

シングルサインオンのサービスとしては、マイクロソフト社の「.NET（ドットネット）パスポート」がある。個人情報管理は、情報を1カ所で管理する集中管理方式である。

一方、サンマイクロシステムズ社を中心とする共同プロジェクト「リバティアライアンス」では、オープンかつ自由な相互認証と安全な個人情報管理の標準策定を進めている。昨年11月にバージョン1.1が公表され、このなかでシングルサインオンが規定された。個人情報管理は、個々のアイデンティティプロバイダー（個人認証機関）同士が連携して認証を行う分散管理方式である。今夏公開予定のバージョン2.0以降では、認証情報に加えて属性情報の交換も盛り込むとしている。

デジタルアイデンティティマネジメントの標準化

Webサービスの標準化団体であるOASIS（構造化情報標準促進協会）によって2003年1月に設置されたXRI（Extensible Resource Identifier）は、非営利団体XNSORGが策定したXNS（Extensible Name Service。先にあげた基本要件を取り込んでいる）をもとにデジタルアイデンティティマネジメントの標準化を進めている。現在はデータ、システム、サービス、人といったネットワーク上のすべ

てのリソースを識別可能にする手法の考案を当面の目標にしている。NRI（野村総合研究所）もXRIの仕様策定に参加している。

Webサービスソフトウェアの互換性保証

IBM社、マイクロソフト社を中心とした団体であるWS-I（Web Services Interoperability organization）でも、属性情報に必要なセキュリティ仕様への取り組みを表明している。

米国政府の動き

米国国防総省と連邦調達局が2003年3月にリバティアライアンスへの参加を表明した。米国政府が推進する電子政府構想の一環として、共通の認証システムを使って電子情報を一元化する手段を検討することが目的である。同様の動きは州レベルでもみられる。

デジタルアイデンティティマネジメントの将来展望

標準化が十分に進んでいない現在では、多数の企業に跨がる大規模なBtoB（企業対企業）、BtoC（企業対消費者）への適用は難しい。この分野への本格的な展開は、標準仕様の策定が進む1～2年先と考えられている。現在最も有望なのはBtoE（企業内ポータル）への展開で、また日本でも個人情報保護法との関連でデジタルアイデンティティマネジメントの検討が進むと思われる。デジタルアイデンティティマネジメントの技術と標準化の行方を注視しつつ、その動向に速やかに対応していく必要がある。 ■