信頼できるID情報の確立のために
―米国が取り組むIdentity Ecosystem―

利便性とセキュリティを両立させた信頼できるオンライン環境を構築する取り組みが各国で進んできている。米国では、オンライン環境の信頼性を確保し、ID連携によってサービスの利便性や質を高めるため、官民の枠を超えた仕組みづくりが進められている。本稿では、この米国の取り組みを概説し、民間IDの連携や活用のための条件について考察する。

サイバースペースの問題点

2010年６月に、米国の国土安全保障省が「National Strategy for Trusted Identities in Cyberspace：NSTIC」（サイバースペースにおける信頼できるアイデンティティのための国家戦略）を発表した（http://www.dhs.gov/xlibrary/assets/ns_tic.pdf）。

サイバースペース（オンラインネットワーク環境）は、いまやコミュニケーションの基盤としてなくてはならないものとなっており、サイバースペースにおけるセキュリティは、経済活動にとどまらず国家の安全にも欠かせないものである。

NSTICでは、サイバースペースの問題点として主に以下の３つがあげられている。

①貧弱なアイデンティティソリューション

身元確認（ID情報の登録）、本人確認（認証）、認可のプロセスが貧弱なため、オンライン詐欺、ID情報の窃盗、なりすましなどの被害を招いている。

②ユーザー中心でないオンライン環境

ユーザーがさまざまなWeb上のサービスを利用するようになったことでID、パスワードが増え、ユーザー自身が管理しきれなくなっている。また、ソーシャルメディアのようにID情報（個人の情報や他者との関連性の情報）を持つサイトが増えたことによりID情報暴露の危険性が高まっている。

③サービスの内容とセキュリティレベルの不整合

サービスの内容に見合った適切なセキュリティレベルが確保されておらず、セキュリティリスクが存在する場合がある。

NSTICではこれらの問題を解決するため、適切に身元確認・当人確認・認可された“信頼できるデジタルアイデンティティ”を確立・維持することに主眼を置く。これを実現するための仕組みがIdentity Ecosystemである。NSTICではIdentity Ecosystemの構築に官民あわせ国全体で取り組むことが必要であると訴えている（政府の役割は“リーダーシップを発揮すること”とされている）。

Identity Ecosystem構築の取り組み

NSTICによれば、Identity Ecosystemとは「市民・組織が安心・簡単にオンラインサービスを利用できるための、ユーザー中心のエコシステム（持続的な仕組み）」である（図１参照）。Identity Ecosystemが実現すれば、

野村総合研究所
基盤ソリューション事業本部
DIソリューション事業部
主任システムコンサルタント
山崎崇生（やまさきたかお）
専門はデジタルアイデンティティに
関するサービスの企画・営業

図1　ユーザー中心主義のIdentity Ecosystem

プライバシー保護と参加の自由

- トランザクションに必要な最低限の情報のみを連携させ、その他の情報は漏らさない。
- 厳密なアクセスコントロールにより、情報の不正利用リスクを減らす。
- Identity Ecosystemを利用するかどうかは個人・組織ともに自由選択とする。

相互運用性（Interoperability）

- 強力で相互運用性のある技術とプロセスにより、ステークホルダー（利害関係者）間の“適切な信頼レベル”を実現する。*
- 1つのアイデンティティをさまざまなWebサイトで利用できるようにする。また、サービス提供者がさまざまなクレデンシャルや認証メディアを受け入れられるようにする。
- さまざまな官・民のアイデンティティから自分の好きなものを利用できるようにする。

ユーザー中心主義のIdentity Ecosystemにより、ユーザーは、

- サービスの性質に応じて適切な（かつ相互運用可能な）クレデンシャルを選択して利用できる。*
- ユーザーは必要な情報以外を連携しないようにコントロールできる。
- サービス提供者による個人情報やクレデンシャルの名寄せを禁止することができる。

＊常に高信頼（高セキュリティ）を求めることは、ユーザーにとって不便であり、サービス利用促進の妨げとなる。

ユーザーは行政サービス、民間サービスを問わず自分の好きなIDを使って利用でき、その際に自分のどのID情報を連携させるかを自分自身でコントロールできるようになる。また、サービスの内容に応じたセキュリティに見合う認証手段が提示されるため、リスクを最小限に抑えることができる。

NSTICは、Identity Ecosystemを以下のように統制、管理、実行の3つのレイヤーから構成されるとしている（次ページ図2参照）。

①統制レイヤー

IdP（Identity Provider：ユーザーのID情報を提供する事業者）、RP（Relying Party：IdPが提供するID情報を利用してサービスを提供する事業者）、AP（Attribute Provider：ユーザーの属性情報を保管・提供する事業者）の三者のサービスを信頼付与機関が監査し、各事業者に監査レベルに応じたトラスト（信頼）マークを付与する。この仕組みを信頼フレームワークと呼ぶ。

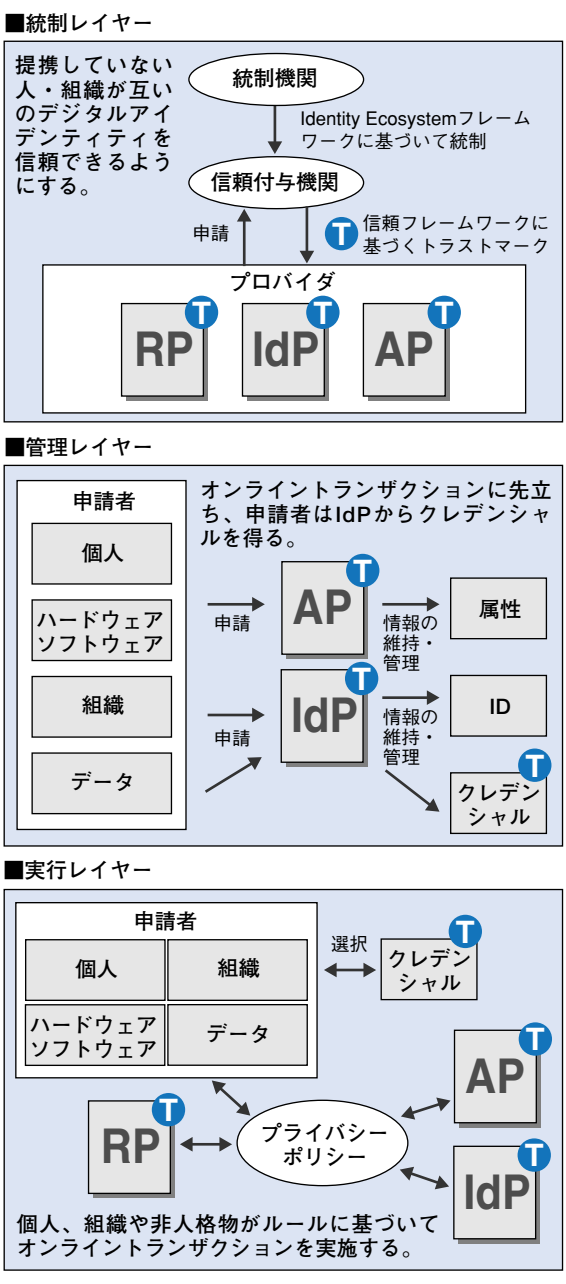
②管理レイヤー

ユーザーがインターネット上のサービスの利用登録を行う際に、ユーザーの身元確認を行い、IDや“クレデンシャル”（パスワード、電子証明書、指紋など自分であることを証明する手段）を発行する。

③実行レイヤー

ユーザーがサービスを利用する際に、各サービスの間での情報連携の可否や、やり取りされる情報の内容をユーザーが決定する。連携できるのは、サービスの利用に必要な最低限の情報のみである。

図2　Identity Ecosystemの3つのレイヤー



利用例（妻が夫の医療情報を参照する場合）

統制機関はトラストマークを付与するためのルールを決め、信頼付与機関の認定を行う。信頼付与機関は、信頼フレームワークを基に、個人を除くすべての参加者の検証とトラストマーク付与を行う、管理レイヤーの事項に先立って以下を実施する。

①病院（RP）は携帯電話事業者（IdP）からクレデンシャルを受け取ることについて、信頼付与機関から認定を受ける。
②携帯電話事業者は、IdPとして振る舞ってよいかについて、信頼付与機関から認定を受ける。
③かかりつけ医（AP）も、APとして振る舞ってよいかについて、信頼付与機関から認定を受ける。

実行レイヤーの事項に先立って以下を実施する。

①妻は、携帯電話事業者によるサービスに加入する際、デジタルアイデンティティを確立しておく。
②携帯電話事業者は、身元確認標準に従って身元確認を行い、クレデンシャルを発行する。
③妻は、病院サイトにクレデンシャルを事前登録しておく。
④かかりつけ医は、医療情報を開示してよいという夫の承諾のもとに、属性情報を適切に検証・保持する。
⑤夫は、医療情報開示同意の際、妻の名前と携帯電話番号を登録する。
⑥病院サイトはEV証明書を取得し、フィッシングサイトではないことを証明できるようにする。

①妻は、携帯電話をUSB接続でPCにつなぎ、病院サイトにアクセスする。
②携帯電話内に携帯電話事業者より発行されたPKI（公開鍵暗号）があり、携帯電話内のTPM（信頼プラットフォームモジュール）により認証され、認証結果が病院サイトに送られる。
③病院サイトは、認証結果を受けて、夫のかかりつけ医から医療情報を取得する。かかりつけ医は、病院サイトから受けた認証を基に、妻が夫の病歴参照を許可されているかを確認し、情報を連携させる。

出所）「National Strategy for Trasted Identities in Cyberspace」に基づきNRI作成

上記の各レイヤーにおいて、ユーザーは利用するIdP、AP、クレデンシャルを自由に選ぶことができる。例えば、医療情報を扱うサービスでは信頼度の高いトラストマークが付

与された銀行のIDとワンタイムパスワードを使い、公立施設の予約のような場合には一般のポータルサイト（GoogleやYahoo!など）のIDとパスワードを利用するといった具合である。いずれの場合も、ID連携によってユーザーネームやパスワードの入力なしにサービスにログイン可能である。

以上の3つのレイヤーにより、利便性とプライバシー保護を両立させたユーザー中心の仕組みが実現される。また、各サービス事業者は信頼フレームワークによって信頼レベルが認定されているので、事業者は他の事業者との連携可否を機械的に判断することができる。Identity Ecosystemは、サービス提供者側（政府、民間事業者）にとっても利便性が高い仕組みなのである。

世界的に進む取り組み

NSTICは市民、有識者からのパブリックコメントを反映させた最終版が発表される予定になっている。NSTICが掲げる、信頼フレームワークによる事業者間の信頼関係の構築と民間IDの連携の仕組みはOITF（Open Identity Trust Framework）モデルと呼ばれ、米国での政府や民間サービスの今後のトレンドとなることは確実である。

Web技術に関する国際的な標準化団体OASIS（Organization for the Advancement of Structured Information Standards）においても、各国の電子政府システムをユーザー中心モデルに作り変えるため2010年9月に「Transformational Government Framework Technical Committee」が設置されており、NSTICと同様に信頼フレームワークと民間IDの連携を中心に据えた電子政府構築のガイドラインを作成しようとしている。

日本でも、「OpenID」（対応するWebサイトで共通に使えるURL形式のID）の普及団体である「OpenIDファウンデーション・ジャパン」を中心に、日本版OITFモデルの検討が始まっている。政府でも、高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）が2010年5月に「新たな情報通信技術戦略」を発表し、「国民が主導する社会」を実現するための国民ID制度を打ち出している。その中では、「インターネットを通じて利便性の高いサービスを提供するため、民間IDとの連携可能性を検討する」とされている（http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf）。

また、総務省に設置された電子政府推進対応ワーキンググループも、2010年10月の報告書（案）で、「民間IDの利活用」や「認定制度（信頼フレームワーク）の確立」に言及している（http://www.soumu.go.jp/main_content/000087340.pdf）。野村総合研究所（NRI）は、国内外における信頼フレームワークの構築に向けた政府および民間の活動を強く支援することで、ID連携サービスの市場拡大に寄与していきたいと考えている。 ■