水平統合とオントロジ①
： 産学官のシームレスな連携ﾎﾟｰﾀﾙ構築に向けて

木村吉博 (kimura@ecom.jp)
東京大学大学院新領域創成科学研究科環境学専攻博士課程
[東日本電子認証普及促進協議会(EPKI)「次世代技術による住民志向型 WEB サービス研究会」、
電子商取引推進協議会(ECOM) 認証公証 WG TF7「SAML 利用検討 SWG」 技術顧問]

概要

近年、組織内･組織間での情報システム統合が多数なされている。特に、異なる文脈(セマンティック)を有する組織間での水平的なシステム統合においては、情報の共有と連携にあたり、個人情報保護法等の要請を満たすためにさまざまな工夫が必要とされよう。

本稿では、web サービス仕様等を用いたシステム統合における現状と課題を概観する。次いで、米国連邦政府の e-Authentication Initiative の動向等を参照し、産学官をシームレスに連携させての文脈共有をめざす、次世代型のワンストップ･ポータル構築にむけた機能要件を抽出する。

※ 次稿「ハイブリッド型 P2P による産学官連携ポータルの解」においては、本稿を受け、web ｻｰﾋﾞｽ技術と組合せたハイブリッド型の P2P による水平統合ﾎﾟｰﾀﾙのﾓﾃﾞﾙ解を提出する予定である。

はじめに 情報システム統合とポータル化

企業･政府等、現代の組織はさまざまな情報システムを有している。近時、これらのシステムをインターネットなどを通じ外部からアクセス可能としていく取組みが盛んである。情報システムの統合が適切になされることにより、業務プロセスが効率化し、さらに、紙資源の節約等のﾒﾘｯﾄも生じると考えられている。

その一方で、異なる時期に異なるベンダーの手によって作られたものであることが通例である情報システムの統合には、しばしば困難が伴うことは既に周知の事実となっている。また、組織間でシステム統合をなし、情報共有をしようとする場合には、両組織の思惑を一致させることなどにおいて、さらなる困難も生じうる。

本稿では、こうした課題を認識しつつ、組織間の文脈の違いを乗り越えての情報システム統合のﾒﾘｯﾄを引き出すための考察をなしたい。その上で、W3C が仕様化中のwebオントロジ言語OWL又は、コレオグラフィ(choreography)記述言語の WSCI･BPEL4WS を活用した、次世代型のワンストップ･ポータル構築に向けた機能要件を抽出する。

1 情報システム統合の現状と課題

1.1 情報システム統合のための技術

初めに、情報システム統合のための技術を概観したい。当初、これらの技術は、情報システム間での相違を乗り越えて相互接続していくことにより、内部的な業務プロセスを効率化することを目指すものであった。だが、文脈(セマンティック)の全く異なるシステムを接続するために生み出された技術は、その後、組織間の情報システムを「疎」に統合していくためにも用いられていくようになっている。そうした技術は、例えば、W3C や OASIS といった国際的団体により、分散コンピューティングのための web サービスのプロトコル群(SOAP, WSDL, SAML 等)として仕様化されている。

また、インターネットが広く普及するにつれ、突発的なアクセス集中が起こりうるサイト(例、証券の売買サイト)での可用性維持が課題となったことも、情報システムの統合を進める要因となりつつある。近時、長らく科学技術計算のために用いられてきたｸﾞﾘｯﾄﾞ･ｺﾝﾋﾟｭｰﾃｨﾝｸﾞ技術を転用し、サイト間でサービス負荷を分散させる取組みも国際的団体 OGSA を中心に取組

まれている。そのために、特定の計算機環境に依存しない形に、サービス記述を抽象化していく試みがなされている。その結果、特定組織のためのサービスが組織の物理的な所在とは無関係なサーバに存在することが可能になると考えられている[1]。サービス記述の抽象化は記述の標準化をも伴うため、情報システムの統合をより容易なものとすることに資すると考えられる。

さらに、こうしたクライアント・サーバのモデルとは別途の出自を持つ技術モデルとして、ピア・ツー・ピア型（以下、P2P）の各種プロトコルも生み出されている。P2P は、コミュニティを運営にあたっての情報共有をしていくためのプロトコルとして用いられはじめている[2]。こうしたアプローチの例としては、日本発の産官学連携 P2P フレームワークの SOBA プロジェクトがある。

1.2 垂直的な統合過程、水平的な統合過程

次いで、情報システムの統合における課題を概観し、課題解決の方向性について考察したい。

第一の課題は、統合対象となる情報システムが、それぞれの目的で、時期的にもばらばらに構築されたに由来するものである。これらのシステムは、初期認証やデータの呼出し・書込みのプロセスが相互に相違するのが通例である。相異なるプロセスを協調させるために要するコストは大きい。加えて、データ構造の相違も、協調を困難にさせている。そこで、異なる構造をマッチングさせるために、メタ情報を用いる等の新たなシステム化の組み込みが必要となる。

また、統合に至るためには各組織に何らかのメリットが必要である。だが、そもそも何がメリットであるかは、それぞれの立場に依存している。このことが、（情報システム外のものではあるが）、第二の、そしてより大きな課題である。全体的にはメリットのある統合であっても、局所的なデメリット（もしくはデメリット感）が、統合の取組みを頓挫させてしまうことはしばしば起こりうることである。

このような課題をより詳細に分析するために、本稿では、統合過程を「内部的・垂直的なもの」と「対外的・水平的なもの」とに分けて把握したい。

内部的・垂直的な統合過程とは、事業者内(inB)・政府内(inG)又は系列事業者内(inBs)等、おおよそ固定されたメンバー間での関係におけるものである。また、対外的・水平的な統合過程とは、事業者消費者間（B2C）・事業者事業者間(B2B)・事業者政府間(B2G)等の対外的でオープンな関係におけるものである。

両過程では、統合に向けての課題の「質」に基本的な相違がある。すなわち、内部的な統合過程では、効率化等の要請を実現するための技術的な課題が主となるのに対し、対外的な統合過程では、組織間の取決めをいかにするかといった非技術的な課題がより顕在化しやすい。

むろん、現実の統合過程が、きれいに「水平」か「垂直」に二分できるわけではない[3]。しかし、意思決定が上意下達的になされるルートが既に存在する垂直的な関係における統合過程 *（以下、適宜、垂直統合）*と、固定された意思決定のルートが存在せず、いわば交渉ゲーム的な関係が存する水平的な過程 *（以下、適宜、水平統合）*とを区別することが課題の把握に役立つと思われる[4]。一般に、組織内での垂直的な統合の方が先行している。上記のような、意思決定の「難易度」の違いがその一因であろう。水平統合には、システム化の課題のみならず、他の選択肢へも開かれた

[1] ただし、個人情報保護法上の適切な安全管理措置等、法律的な義務を果たす必要があるのは当然である。

[2] P2Pは、当初、著作権を侵害する態様でのファイル交換に用いられたことによりネガティブなイメージが先行してしまっている。だが、著作権侵害の問題は、デジタル・データはコピーが極めて容易である、という事実に由来するものであり、通信プロトコルの問題は副次的なものである。

[3]現実の水平的関係においては、例えば、政府－私企業間、元請企業－下請企業間のように力関係が非対称的な場合は多く存在する。形の上では複数の意思決定者が存在し水平型に分類されようシステム統合でも、e-Japan戦略下、構築された行政への電子申請のように、一方の業務効率化が主に念頭に置かれてなされることが多い。非対称性が大きい例としては、国交省の「入札」に事業の多くを拠っている企業の場合があげられよう。この場合、行政側の作成した入札システムを採用しないという選択肢は事実上ない。従って、行政側は、少なくとも理論上は、相手方となる企業の利得は考えずに自己の利得のみを最大化する行為をなすことが可能となる。

[4] これは、いわばイントラネットとインターネットとでのシステム構築に際する相違に比す事ができよう。そこで、WAN接続の標準的な解をもたらすプレイヤーとしてインターネット・サービスプロバイダ(ISP)各社が登場したように、水平統合の標準的な解をもたらすプレイヤーの登場が期待されることとなる。

関係を特定の取決め事へと落とし込んでいくという、より困難な課題が存するのである。

垂直統合では、大臣・担当官僚・経営者・親会社の担当者など、システム全体を代表しうる上位の意思決定者が、(少なくともモデル上)存在する。そのため、これらの意思決定者が統合に業務上のメリットありと判断し予算を配分しさえすれば、統合は開始されることとなろう[5]。すなわち、業務プロセスの効率化といった単一の目的設定をなすことが容易である。現に、各種の情報システムを統合し、業務の効率化を図った事例が、専門誌や Web サイトにおいて紹介されることも多い。

また、多数の業者が作り上げる部品を最終的な完成品へと組み上げていく必要のある自動車やコンピュータ業界では、インターネットを通じての迅速なマッチングは既に欠かせない要素となっている。その製造工程では、上流から下流までのプレイヤーが比較的固定的な関係にある。取扱われる部品・半製品を無駄な在庫品とさせずに迅速にマッチングさせることは、トータル・コスト削減を目指す各プレイヤーの共通の関心事である。その結果、RossettaNet のような特別のフォーマットに基づく B2B 市場が成立しているものと考えられる。利害の共通性・固定的な関係という点で、こうした B2B 市場も垂直統合の一例といえよう。

一方、さらにオープンな関係での水平的な統合が実現すると、単なる業務の効率化以上のメリットが生じると考えられる。

例えば、検索エンジンや各種のワンストップ・ポータル(Yahoo!等のように、両者はしばしば一体となっている)は、インターネット上の情報をシームレスに連携させる、基本的ではあるが重要な水平統合と言える。

爆発的に情報が増大している Web の世界では、情報を適切に整理し結び付けていくことは最大級の課題と言える。そこで、サイト間を適切なリンクづけていく標準的な解として、検索エンジンやポータルが用いられており、現在、Web はこれらによりまさしくクモの巣状(weblike)に結び付けられるようになっている。地方にいながらにネットに接続するだけで、サイトをまたいで必要な情報を探すことが可能となっている。また、適切な価格情報下で、多くの商品を安価に買うことが可能となっている[6]。

Web サイトの多くは、より大勢の人々に訪れて欲しいと願っている。一方、検索エンジンやワンストップ・ポータル・サイトは、検索機能やワンストップ・サービスの提供によりアクセス数を確保し、広告収入等をベースとしたビジネス展開を図っている。検索エンジンやポータルが一般化した背景には、両者の思惑の一致があるものと思われる。

だだし、既存の検索エンジンやポータルでの情報の統合の多くは、表面的なものに留まっている。すなわち、検索エンジンが結び付けているのは、あくまで、ユーザが打ち込んだキーワードと、インターネット上に公開されロボット(エージェント)により収集された文字列等である。収集された情報が Web の適切な構成を反映しているとは限らない。ユーザの検索にかかりやすくするために検索エンジン対策を取るサイトは多く、また、逆に検索用ロボットによるアクセスを妨げようとするサイトもある。ポータルにおいて、整理され結び付けられているのはサイト側が発信する情報である。

近時、「楽天」等の電子モール・ポータルにおいては、ユーザは一度入力した自己情報を、電子モール内の個別サイトでの商品購入のために使うことのできるワンストップ化が進んでいる。しかし、RossettaNet のような B2B 市場とは異なり、そこで入力する自己情報には、商品購入のために必要な情報(氏名と届け先等)であることだけが求められる。即ち、虚偽の情報を混ぜ込むことは、事実上、何ら禁じられていない[7]。

このように水平的な統合が表面的なものに留まっており、虚偽の情報・断片化した情報が混在している現状は、インターネットのさらなる発展へのボトルネックとなっているものと思われる[8]。今後、さらに水平統合が

[5] むろん、上位の意思決定者に業務用のアプリケーション統合(EAI)のメリットを納得させること自体、難しいことではあるが。

[6] むろん、検索エンジンを活用できる情報リテラシーと、そして何よりも、情報を理解する文字通りのリテラシーが必要とされるが。

[7] もっとも、商品の詐取等の目的で偽りの情報を入力した場合には、詐欺罪等の刑法犯に問われることは、当然ありうる。

[8] むろん、分散型のオープンなネットワークであるインターネットにおいては、全て真正の情報となることはありえないことが前

本格化すると、ネットワークを用いての業務コラボレーションやコミュニティ運営などが求められるようになっていこう。そうした場合、個々の情報に虚偽が混じり込んでいることは、業務やコミュニティの運営にとっての、大きなリスクとなりうる。水平統合では、組織間・コミュニティ間で、情報の真正性を担保していくことが求められよう。

1.3 本格的な水平統合に向けて

体制や考え方の異なる組織間においてシステムを統合していった場合、社会的な費用節減（例、データの再入力の手間が省かれる）や組織間でのマッチングの容易化といったメリットが生じうる。このように、水平統合には、大きな対投資効果(ROI)が見込まれる。しかし、水平統合の進展は、情報の漏洩や改ざんといったリスクの増大をも伴うこととなる。以下の章では、こうした問題を乗り越えて、さらなる水平統合を進展させるための基本的な考え方を整理していきたい。

インターネット等を通じての通信では、一般に「なりすまし」や「事後否認」のおそれがある。そして、直接にお互いを知らない水平的なシステムの運営の場面では、なりすまし・事後否認等による実害が生じるおそれはより大きくなる。

オープンな環境での情報システム利用においては、こうしたリスクへの技術的対処策として、例えば、公開鍵暗号方式を用いる PKI などを活用するさまざまな初期認証、権限管理、そして永続化（含、ログ管理）の仕組みが用意されている。

だが、相互の検証・ポリシ策定、鍵の交換等、発生する費用はかなりのものとなりうる。近時では、認証・権限管理等を専門のサービスに担わせることも試みられるようになっている。これは、それ自体が水平統合の促進であり、前述のような非技術的な課題（組織間の責任分担など[9]）を顕在化させることにつながりうる。

以下、このような新たな試みとその課題を視野にいれつつ、初期認証・権限管理というプロセスについて、水平統合のあり方を考察していきたい。

1.4 入口段階での水平統合 ： 認証情報を共有するｼﾝｸﾞﾙ・ｻｲﾝｵﾝ

ネットワーク上の情報システムには、情報の不正な書換えや読取りのリスクがある。そこで、通常のシステムは、使用権者か否かを確認するための何らかの認証手段を有する。

水平的なシステム統合においては、ユーザの利便のため、もしくは、システム運用を容易とするため、認証情報を何らかの形で共有・再利用することが試みられている。すなわち、ある一連の目的のためにインターネットを使用するユーザにとり、サイトを移動し、一つ一つの目的を達成しようとするたびに認証を求められることは不便である。例えば、旅行の予約に際しては、A航空会社のサイトで航空券を予約する際に認証を受けたならば、別サイト（B,C・・・）で、空港からの交通手段や宿泊施設などを予約する際には再度の認証を求められない方が利便にかなう。また、サイトAからサイト B・C 等へと認証情報を渡すコストの合計が、サイト毎での予約のたびに認証するコストより安価であるならば、こうした運用は効率的でもある。

ネットワークの世界では、サイト間でのこのような認証情報の再利用は「シングル・サインオン」と呼ばれ、近時、脚光を浴びている。

例えば、既存のワンストップ・ポータルにシングル・サインオンを組合せることで、リアルワールドで古くから行われてきたサービスをより迅速化したり高度化したりできるかもしれない。古くから、旅行代理店は、航空券・現地での移動手段・宿泊施設を、適宜パッケージ化してきた。また、不動産売買において、不動産会社は、しばしば、契約書作成、登記移転、抵当権設定のサービスを斡旋している。これらはリアルワールドでの

提である。

[9] 水平統合が促進すると、いざ責任追及が必要となった場合に、損害を算定し、また、相手方又は第三者の行為を認定し最終的な責任者を特定する等において、さらなる付加的なコストが必要となりうる。雇用関係もしくはそれに類似した人的関係の存する垂直統合の場面では、雇用契約・雇用規則等が存在しており、悪意ある振る舞いをなした内部者への責任追及は比較的容易であるため、こうした問題は比較的顕在化しにくいものと思われる（むろん、第三者からの不正アクセスを十分に防止できることが条件ではあるが）。

ワンストップ・サービスといえよう。

近時、旅行代理店サービスについては、かなりの部分について、インターネット上のポータル・サイトでも実現できるようになりつつある[10]。こうしたポータル・サイトの中には、自らは電子モールの運営者に専念するところもある。こうしたサイトは、具体的な商品の購入や旅客サービスの申込み等については、それぞれを得意とする事業者に電子モールに担ってもらう分業体制を実現している。その際、(その名であえて呼ばれないにしても)認証情報を一括管理するシングル・サインオンが必要となる。認証情報を一括管理し、サイト間で組織をまたいで共有していくためには、いくつかの技術的ハードルを乗り越えていかなければならず、相応のコストが必要となる。

共有を進めていくにあたり、とりわけ、ネットワークを介しての認証技術が多様でありその信頼性・強度[11]において等価ではないことが、大きなハードルとなりうる。

情報システム全体から見て、認証はあくまで「入口」における一手段である。玄関だけが立派で住み心地が良くない家や逆に玄関で入るのを躊躇してしまう家はいささか困りものである。認証手段についても、情報システムが扱う情報資産に見合った過不足ないものであることが求められよう。

そこで、一般には、サイトで取扱われる情報資産が重要であればあるほど強い認証が求められることとなろう。だが、何がより強い認証なのかを決めることは簡単ではない。認証技術には、共通鍵暗号を用いるKerbelos・公開鍵暗号を用いる PKI をはじめ、パスワードやバイオメトリクスを用いるものなど種々のものがある。Kerbelos 方式や PKI 方式では、秘密とされる鍵情報(共通鍵又は私有鍵)は、IC カードや USB トークンなどの耐タンパ・デバイスに格納され、その所持者が情報システムの正当な使用権者とみなされることとなる(PKI においては、公開鍵と対応する私有鍵の所持者について認証局が、証明書を発行する)。また、パスワード方式では一定のパスワードを記憶する者が、バイオメトリクス方式では、他者と異なるある種の身体的特徴(指紋・虹彩・掌など)を有する者が、それぞれ正当な使用権者とみなされる[12]。

これらの認証の「強度」について、例えば、パスワードによるよりも PKI による方が強いと言われる。だが、「パスワードによる認証」といっても、用いるシステム等により、その強度・信頼性は大きく異なる。インターネット上を平文でパスワードが流れる単純な方式も、チャレンジ・アンド・レスポンス等により認証を受ける度に異なるパスワードを用いるワンタイム方式も、共に「パスワード方式」として括ることはできようが、その信頼性は大きく異なる。そして、認証情報を管理するシステム運営(ログ取得・解析、機密情報にアクセスするにあったての入退室管理等)がいかに行なわれるかは、認証の信頼性に決定的な影響を及ぼす。

また、認証を受ける主体の意識も、その信頼性に大きな影響を及ぼす。記憶のしやすさから家族の生年月日などをベースとしたパスワードを設定したり、パスワードをポストイットに書き出して自らの机に張ったり、といった行為が危険なことは周知となりつつあろうが、いまだに多く行なわれているものと思われる。また、外部からの情報読取りに対し強い耐タンパ性を有する IC カードであっても、それがカード・リーダーに挿しっぱなしであったり、部屋の中に放置されたりしているようでは本来の効用は発揮できない。

認証の強さ・信頼性に、これらの要因のうちいずれがより大きな影響を及ぼすのかについては、(一般的な考え方はあるものの)一義的には決まらず、情報資

[10] 重要な財産である不動産の得喪等については、公的な登記制度を通じた公示を持って、第三者に対抗できることとされている(民法177条)。公的な制度と一般の人々とのインターフェースについては、PKIを用いた「電子申請」として、現在、システム化が進められている最中である。それらをワンストップ化する試みは、もう少し先になるものと思われる。

[11] 認証の「強度」は、正当な権限者を確実に認証させること、正当でない権限者を認証してしまわないこと、という二つの意味があり、両者は一定程度トレードオフの関係に立つ(例、指紋による認証では、厳格な一致を求めると本人の指紋でも認証に失敗することがしばしば生じてしまうこととなる。そのため、使いやすくするためには、ある程度のあいまいさを許容することとなるが、その場合、本人以外の者の指紋でも認証されてしまうことが起こりやすくなる)。

[12] コンピュータも、バイオメトリクス認証以外の客体になることができる。Webサービスによる分散コンピューティングにおいては、多くのサーバは、通信内容により、認証主体にも認証客体にもなる。

産の管理者等が評価し定めることとなる。

そこで、後述の Liberty Alliance のように、認証情報の水平的な共有のための標準的な解を提供するために「認証コンテクスト」を仕様化する動きもある。

サイト間で、認証のあり方（文脈・コンテクスト）をこうして共有することは、その後のさまざまな情報資産へのアクセスや書換えの根拠となる。そこで、いかなる認証をなすべきか（例、対象は本人性か、本人の属性情報等か）、あるいはどの程度の強さと考えられる認証をなすべきか、といった問題は、情報資産へのアクセス権限管理の問題と直結する。以下、認証と権限管理との関連について考察したい。

1.5 水平統合の根幹 ： 情報資産へのアクセス権限の管理

インターネットの各サイトは、アクセスを開放している公開領域と特定の権限者だけにアクセスを許す非公開領域とからなることが一般である。非公開領域には、事業者の営業秘密や従業員や顧客の個人情報となる機密情報など、漏洩が許されない情報資産が多量に格納されている。

事業者はこのような情報資産を適切に活用し、利潤を上げる等の事業目的を達成していかなくてはならない。今後、事業者間等で水平的に情報システムを統合し、それぞれの情報資産を有効活用していくことは、事業目的達成の重要な手段となろう。そこで、情報資産に対するアクセスの適切なコントロールは、水平統合の成否を決する根幹的な要素となると考えられる。

こうした考えから、電子商取引推進協議会（ECOM）の認証・公証ワーキンググループでは、分散コンピューティングにおける認証と権限管理のための基盤仕様と目されている SAML 仕様の活用を検討する研究会（SAML 利用検討サブワーキンググループ、通称 TF7）をスタートさせている。

国際的なベンダー団体の OASIS により定められた SAML 仕様は、認証や認可の情報を伝えるメッセージを XML ベースで定義している。SAML メッセージは、その要素に対し XML 署名（電子署名）を付して生成することができ、ファイアウォールに対し透過的な SOAP エンベロープなどにより伝達される。SAML メッセージングを適切に活用すれば、あるサイトでなされた認証をベースとして、別のサイトにおける情報資産のアクセスコントロールを行なうことができるようになると期待されている。

ECOM TF7 では、参加する各ベンダーの代表者により、SAML を用いたサイト横断的なユースケースの作成が行なわれている。現在、電子政府、医療、金融等の具体的な業務領域が検討の対象とされている。これらは、その業務は相互に全く性質の異なるものであるとしても、用いられる情報システムについては、認証・権限管理のプロセスにおいて、共通するところが多い。また、システム中で個人情報が扱われるため、プライバシーの確保が問題視されることも多い。

そこで、ECOM TF7 では、SAML によるシングル・サインオンをベースに個人情報の保護の仕組みを充実させたフレームワークである Liberty 仕様[13]の考え方を参考としている。2001 年にサン・マイクロシステムズ社を中心として設立された標準化団体 Liberty Alliance の手による Liberty では、個人情報の集合をアイデンティティと呼び、その管理を主にアイデンティティ・プロバイダ（以下、IdP）と呼ばれるドメインに委ねていくこととしている。また、IdP からアイデンティティを必要に応じ受け取りサービスを提供していくドメインをサービス・プロバイダ（以下、SP）と呼んでいる。

顧客（ユーザ）は、各種の情報サービスを受けるために、IdP に個人情報の適切な管理を委託する。ユーザは、IdP から認証を受けた後、サービスを利用する。その際、IdP は、ユーザがサービスを受けるために必要な限りの情報を SP に流すこととなる。顧客が選んだサービス群は、個人情報をサービス提供に必要な限度で共有していく「信頼の輪（Circle of Trust）」を形成する。

この「信頼の輪」は、IdP と SP の水平的な分業体制をベースとする。*（Liberty 自体は、メッセージングを定めた仕様であり、分業のあり方そのものを規定しているわけではないが）*、その分業は例えば、以下のように

[13] IBM、マイクロソフト、ベリサイン社などの手によるWS-Federation仕様もおおよそ同旨の考え方を採用している。

行なわれると考えられる。すなわち、IdPの役割は、ユーザを適切な手段で認証し、その認証情報と管理するユーザの属性情報を SP へと適宜提供することである。SP の役割は、IdP から受け取った情報と自ドメイン内の管理情報等をベースに、保有する情報資産に対するアクセス権限管理を行なうことである。

こうした分業体制が成り立つためには、IdP が、信頼点としての振舞いをなすことが前提となる。すなわち、「信頼の輪」が文字通り信頼に値するものであるために、IdP サイトの情報セキュリティが十分に確保されてなければならない。また、IdP は個人情報を継続的に取扱わねばならないため、その運営母体には、個人情報の取扱いに熟達していることと経営が安定していることとが求められよう。また、今後は、個人情報保護法上の要請にも応えていかねばならない。その結果、IdP の運営には相対的にコストがかかることとなる。Liberty 仕様を日本において広めるための活動に精力的に取組んでいる Liberty Japan においても、IdP の担い手と目されているのは、NTT ドコモ・ボーダフォーンなどの携帯キャリア、NTT 東日本・西日本、各地域の電力企業などの大手企業であるとのことである[14]。

逆に、SP サイトでの情報セキュリティは、サイトが取扱う情報資産を保護するために必要な限りで確保されていればよいと考えられる。したがって、SP については、NPO やベンチャー企業等が、簡易に構築していくことも十分可能と思われる。

以上のような認識を受け、東日本電子認証普及促進協議会(EPKI)においては、東北地方（宮城県、山形県、岩手県）等の参加者による「次世代技術による住民志向型 WEB サービス研究会」を開催し、地域情報サービスの分散的な構築のために SAML・Liberty 等を活用していく可能性を検討している。

以下では、ECOM と EPKI の両検討会での検討を参考とし、地域情報サービスのための次世代ポータルのあるべき姿について考察したい。

[14] Liberty Japanに早くから参加し、また、WS-Security仕様の日本語版編者などにおいても活躍を続けている日本ベリサイン株式会社　田口慶二課長の談（参考、「ITなるほどインタビュー webサービスのセキュリティ　どんなビジネスチャンスをとらえることができるのか！」 *Digital Xpress,* Oct-Nov, 2003）。

2 次世代型の水平統合ポータルに向けて

2.1 米国連邦政府の考え方

米国は、州政府による分権的な統治をなす連邦制を採用している。連邦制には各地域の個性を活かすことができるという長所があるが、一方で、地域間の制度的整合性の確保が困難であるいう短所も存在する。電子政府の構築においても、この短所が顕在化してきた。例えば、各州は独自に PKI の認証局を構築してきたが、それぞれが発行する証明書は相互の運用性を欠くことが多く、州を越えての認証を行ないにくくなっている。そのため、相互の認証局をつなぐブリッジ認証局(BCA)の構築が試みられてきた。しかし、ブリッジ認証局を介した PKI システムには、パス検証時のパフォーマンスや認証局のサーバ鍵交換時の問題など、数多くの課題がある。

近時では、投資対効果(ROI)を重視するエンタープライズ・アーキテクチャ(EA)の見地から、電子政府構築における非効率性を問題視する声も高まっていた。そこで、ブッシュ政権下の米国連邦政府では、Liberty 等の web サービス仕様をベースとする認証インフラ e-Authentication の構築を開始することとした[15]。e-Authentication は、クリントン政権下に構築された電子政府ワンストップ・ポータルの FirstGov をフロントエンドとすることが予定されている。e-Authentication により、地方自治体・教育機関・医療機関等をまたいだシングル・サインオンが可能になると考えられている。その際、Liberty 等の仕様により、個人情報を直接に流さない半匿名的なメッセージングが行なわれる予定である。また、市民の認証においては、負担軽減のため、IC カードの使用を要求しない方向で検討が進められている[16]。

[15] 参考、www.cio.gov/eauthentication/presentations/forum_timchak.ppt

[16] Liberty仕様では、パスワード、ソフトトークン（ブラウザのアプレット等）ベースのPKI、ICカードベースのPKI、バイオメトリクス等の認証の態様に関する情報を、IdPとSPの間で交換することが可能である。e-Authenticationにおける市民の認証では、当初、パスワードとソフトトークンベースのPKIが活用されていくこととなろう。なお、カナダ政府は、市民の認証について、e-Passと呼ばれるソフトトークンベースのPKIを既に採用している。

2.2 日本の現状 ～ 公的個人認証基盤の登場

2003 年夏、日本では公的個人認証基盤の運営が開始された。これにより、1 千万人を超える人々が住基カード等を用い、PKI による電子署名・認証をなすようになるのではないか、と期待する声もある。

しかし、当面、公的個人認証基盤の用途は、住民票取得や確定申告といった年にせいぜい数度あるだけのものに限られることとなりそうである。確かに、こういった用途であっても、人々に多少の利便はあろう。だが、本来、IC カードは所持による本人性確認手段である。年に数度の使用するだけの IC カードでは、紛失しても気が付かない人も多かろう。日常的に用いられない IC カードは、情報セキュリティの観点からはむしろリスク要因となる。

目を民側に転ずると、私有鍵を格納可能な物理的な耐タンパデバイスは、既に多くの人々に日常的に使用されている。第三世代携帯電話(3G 携帯)は既に 1000 万台を超える普及をし、用途開発はこれからであるものの、少なくとも人々に日常的に所持されている。交通系 IC カードの Suica や Icoca も発行枚数数百万枚を誇り、自動改札のみならず（Edy と同等の）電子マネーとしての使用も開始されようとしている。

人々に身近なものか否か（手に届くところに所持されているか否か）という観点からすると、この分野での官民格差は大きいと言わざるを得ないであろう。

むろん、3G 携帯を使いこなすのは若年層が中心であり、交通系 IC カードを日常的に使えるのは都市部の住民に限られる。また、両者を活かしたネットワーク上の応用アプリはいまだ少ない。対して、公的個人認証基盤は、公的なインフラとして少なくとも制度上は、全国民を対象とする。だが、普段、コンピュータを日常的に使う必要のあまりない人々も多い。そのような人々にも、現状では互換性に乏しいカード・リーダーを購入し、これまた互換性に乏しいドライバを自らのパソコンにインストールして使うことを要求するという、公的個人認証基盤のアプローチには、旧態依然の「お上」の発想が見え隠れするのではなかろうか。

IC カードという「ものづくり」の技術においては、日本は世界でトップクラスの水準にあるものと思われる。対して、IC カードを用いるためのアプリケーションの作りこみについては、とりわけ、公的分野における課題が大きい。

※ *紙面の関係で、公的個人認証基盤をはじめとする公的な認証基盤の課題についての詳しい記述は省略する。こうした課題については、電子署名・認証パートナーシップ JESAP において幅広く議論されており参考とされたい。*

2.3 汎用的な市民サービスのための電子政府

現状ではいくつかの課題があるものの、IC カードと PKI を組合せたネットワーク上の認証には、事後否認が困難である等のメリットがある。アクセスにより行政処分を伴う場合のある電子政府は厳格な運営が必要とされるため、IC カードと PKI の適切かつ積極的な活用が求められているといえよう。

そこで、米国連邦政府が採用する e-Authentication のような、シングル・サインオン認証基盤を日本の電子政府でも構築していくことも考えられよう。

しかし、先に述べたように、米国には、クリントン大統領からのトップダウンの指令により構築され、多くの人々に用いられている電子政府ワンストップ・ポータルの FirstGov がある。したがって、米国では、多くの人々が電子政府へのアクセスに利用している玄関（ゲートウェイ）の FirstGov の発展形として、横断的な認証基盤である e-Authentication が導入可能であった。

一方、日本の電子政府のポータルは省庁タテワリ型に構築されており、相互のリンク付けは不十分である。すなわち、各種の情報システムを水平統合していくための「きっかけ」が不十分である。日本では、広く用いられているゲートウェイは、Yahoo!や Infoseek などの民側のポータルである。ポータルは、単なるリンク集であると言ってしまえばそれまでであろうが、人々に受け入れられているという事実は大きい。従って、可能ならば、こうしたポータルとの連動が図られることが望ましいと思われる。

ただし、日本の電子署名法は、「本人でなくてはなしえないような態様で」電子署名をなすことではじめて

民事訴訟法上の書証と同等の証拠能力を認めている。現状で、この要件を満たすものは、IC カードなどの物理的耐タンパデバイスを用いた電子署名である。前述のように、ICカードやUSBトークンなどの耐タンパデバイスにはドライバのインストールや互換性の問題などが存在する。従って、そのようなデバイスを使いこなせるのは、IT 関連業務従事者のように情報リテラシーの高い者に限られることとなろう。

そこで、近時、普及が著しい 3G 携帯や交通系の耐タンパデバイス、さらには IC カードを組み込んだクレジットカードなどを電子政府においても活用していくことが考えられよう。一方、米国のように、電子政府での市民の認証において耐タンパデバイスの使用を求めない解も考えられる。以下では、この双方を用いる汎用的なポータルのイメージについて概説したい。

電子政府ポータルでは、市民の個人情報が多く取扱われることになる。そのため、限られた予算下で汎用性の追求と共にプライバシーを十分に保護していくことが目指されねばならない。

現時点でのバックエンドにおける解が、前述のように、Liberty 仕様のようなシングル・サインオンの枠組みであろう。この枠組みでは、利用者が自らの必要に応じ、個人情報を共有する範囲（Liberty 仕様では「信頼の輪」）を形成していく。流される個人情報は最小限にとどめられ、必要に応じ半匿名化などプライバシーへの配慮が図られている。

だが、電子政府サービスを一般化させていくためには、日頃、コンピュータを使用しない、もしくはあまり使用する必要のない人々にも、使いやすいものでなくてはならない。

そのための一つの解として、サンダル履きで行けるような、市民に身近な施設に使いやすい端末を設置し、そこにおいて認証から実サービス（の申し込み）までを受けられるようにすることを提案したい。

私はこうした端末を、「コンパクト・クライアント」と呼ぶ。これは、人口規模 2 万人程度の中学校区に都市機能を集約し、自動車なしでも日常生活・経済生活が行なえるようにする、というコンパクト・シティの考え方にならったものである。こうした考えを背後に持つコンパクト・クライアントは、経済効率性の見地から導入が進められた web サービスの考え方に公共性を持たせるための一工夫である。

コンパクト・シティの考え方を具現化する鍵が、コンパクト・クライアントとその裏方（バックエンド）に当たる、シングル・サインオン基盤と考える。

以下、その概要を述べる。コンパクト・クライアント端末を操作しようとする人々は、何らかの手段（職員との対面、ローミング鍵、バイオメトリクス等）で本人性についての認証を受ける（コンパクト・クライアント端末は、職員の IC カードや住民自身のバイオメトリクス情報を読み取れるようになっており、それらが認証の起点となる）[17]。ユーザは、その後、希望するサイトを訪れる。サイトの民・官のサービス提供者（Liberty 仕様の SP）は、コンパクト・クライアントから本人性と認証手段についての通知を受け、IdP 等が保有する情報と照らし合わせた上で、各種サービスを提供する。

コンパクト・クライアントは、人々に「目に見える安心」を提供するためのものでなくてはならない。その際、普段、PKI を使う機会のない一般の人々のためには、本人性の確認手段として IC カード以外を用いるべきである。具体的には、以下のようなものが考えられる。

市町村の図書館等の公的施設は、対面で、公的な身分証明証による確認を行い、図書カード等のローカルな身分証を発行している。こうした身分証は、同等の公的サービスについての信頼の起点となりうる。したがって、同様の対面での身分確認に基づいて、これらの施設において、ワンタイムのソフトウェア・トークンを発行すること（米国連邦政府の e-Authentication、カナダ政府の e-Pass 相当）が考えられる。またその登録プロセスにおいて、職員の対面での確認に加えて、バイオメトリクス（指紋・掌等）の登録をなすことも考えられる。この場合は、二度目以降は対面での認証過程を省略できる。

これらの手段は、日常的に PKI を用いている人々にとってはかえって煩わしいことかもしれない。しかし、特定の電子申請等を行なうために一回限りで PKI を

[17]例えば、一度限りの行政の電子申請においては、職員との対面による認証が一般化するかもしれない。

用いる必要があるといったシチュエーションでは、ICカードを取得しカード・リーダーを買いドライバをインストールするといった手順を踏むより、サンダル履きで近所の端末に向かいそこで職員の指示に従って操作を行なう方が人々の負担は少ないであろう。

また、携帯電話キャリア等やクレジットカード会社は既に多数の顧客の個人情報を管理している。これらの情報も、公的な機関の管理する個人情報と何らかの形で連携可能であるならば、本人性の認証手段として活用可能であろう。

2.4 次世代型ポータルの機能要件 ： 知識体系・コレオグラフィ記述とハイブリッド化

以上の議論のポイントは、次の 2 点であった。

第1に、電子政府への入口段階にあたる認証手段は、人々が普段使用する多様なデバイスが用いられることが望ましい。また、電子的なデバイスを普段使用していない人々のためには、ワンタイムで使用できる認証手段を用意することが望まれる。

第2に、多様な入口からの認証情報を適切に関連付けて、情報資産に対するアクセス権限管理をなす、バックエンドのシステムを用意する必要があろう。

これまで、電子政府の構築は、GPKI・公的個人認証基盤等、「入口」の認証部分に大きな比重が置かれてきた。認証基盤の基幹部分がおおよそ完成した今、必要なのは、認証の「質」をサーバが理解した上で、受け情報資産へのアクセス権限管理を行なっていくことである。

こうした要請は、基本的には民側で進展中の水平統合でも同様であるが、複数のサービスを連携させる等の複雑な作りこみは、官民ともにこれからである。Web サービスにより、バックエンドでのサーバの分散化が急速に進む中、次世代型のワンストップ・ポータルでは、複数サービスを自然に連携させていく機能が求められるであろう。そこで、知識体系記述やコレオグラフィ記述の検討を進めていくべきと考える。

必要とされるのは以下の機能であろう。

第一に必要となるのは、認証の評価体系と情報資産の権限管理とのマッチング機能である。

権限管理は、これまでローカルなポリシ記述により行なわれてきた。しかし、近時では、OASIS の XACML のように管理記述をオープンな仕様としていこうという動きもある。特に、電子政府においては、可能な限り公開性を維持しなければならない。そこで、ある情報資産に対しアクセスを望むユーザが、いかなる属性を持って認証を受ければアクセスが可能となるのか、検索ができることが望ましい。こうした記述を得意とするのは、W3C が仕様化中の web オントロジ言語 OWL である。OWL は、コンピュータによる意味解釈を可能とするための知識体系の記述をなす言語である。また、OWL をベースとした、web サービスの知識体系記述言語[18]も策定されようとしている。

第二に必要とされるのは、予約・決済などのプロセスを（キャンセル処理などを含め）協調的に行なっていく機能である。そのためには、web サービスをビジネス・プロセス・フローとして連携させていく必要がある。そこで、web サービスのコレオグラフィを記述する WSCI(W3C に提案中)又は BPEL4WS(OASIS に提案中)といった仕様を使用することが考えられよう[19]。これらは、サービスの論理的なインターフェース記述を行なう WSDL をベースに、操作呼出の順序や他の web サービスとの関係を記述するための仕様である。

また、通例、サービスが一般に普及するに従い、急速に問合せ窓口も必要となる。次世代型のポータル構築に際しては、問合せ窓口として SIP 等をベースとした電話やテレビ電話を活用することが考えられよう。その際、多量のトランザクションを発生させる動画のやり取りを行なうならば、web サービスのような集中的な処理よりも、P2P 型の双方向メッセージングの方が望ましいと思われる。そこで、SOBA のような P2P フレームワークをwebサービスとハイブリッド化し、サービス窓口としていくことが考えられよう。ハイブリッド化においても異なる知識体系の関連記述が不可欠となる。

次稿では、こうした仕様を活かした次世代型のポータル作成に向けた提言をまとめることとしたい。

---

[18] DAML-Sの後継としてのOWL-S

[19] 前者についてはSun、BEA等が提案、後者についてはIBM，マイクロソフト等が提案