# 属性情報プロバイダ：安全な個人属性の活用基盤の提言

千 葉 昌 幸[†] 漆 嶌 賢 二[††] 前 田 陽 二[†††]

インターネットおよび E コマースの進展により，氏名，住所，資格情報などの “個人属性” 情報がインターネットを通じて様々な場所で交換されているが，同時に個人情報漏洩のリスクもまた急速に大きくなってきている．インターネットサービスにおいても個人情報保護法を遵守し，適切に個人属性を管理できる仕組みが求められている．本稿では，オープンな標準技術に基づき相互運用性の高い環境の下，個人属性を安全に交換，管理する情報化基盤「属性情報プロバイダ」を提案する．属性情報プロバイダは，運用システムの安全性について第三者機関の認定が得られた複数のサービス事業者により構成されるものである．利用者は，属性情報プロバイダに個人属性を登録および委託することで，以後は直接取引相手に渡すのではなく，利用者の同意を得たサービス提供者にのみ属性情報プロバイダを介して個人属性を安全に渡す．ネットワークプロバイダ，PKI などとともに今後，情報ネットワークの重要な基盤になると期待される．

# Personal Attribute Provider: A Secure Framework for Personal Attribute Exchange on the Internet

Masayuki Chiba,[†] Kenji Urushima[††] and Yoji Maeda[†††]

According to explosive growth of the Internet and e-commerce “personal attribute” information such like a name, a postal address and some qualifications have been exchanged on it. However privacy risk has been rapidly raised at the same time. Thus proper personal attribute management has been required conforming to the Personal Data Protection Law enacted in April 2005. In this paper we will propose the “Personal Attribute Provider” which is an infrastructure for secure exchange and management of personal attribute based on open standards that will provide higher interoperability. Some part of personal information will be registered and entrusted to the provider which should be founded by trusted authorized organization then user, attribute provider and service provider which can be online shopping site can exchange the personal attribute on the agreement with the user. Distributed management of personal attribute which relies on the federation of multiple attribute providers can reduce irreparable damage of privacy and digital signature technology used in the attribute provider can offer authenticated personal attribute to service provider. This paper describes the investigation result for it as it should be important commonly used infrastructure on the information network as well as network providers and PKI are in the future.

## 1. はじめに

インターネットにおける多くのビジネスでは，サービス事業者はあらかじめ利用者から個人情報の提供を受けたうえでサービスを実施している．現行，利用者はサービスごとに同じ個人情報を複数のサービス事業者に直接提供している．サービス事業者には個人情報保護法などにより利用者の個人情報を厳格に管理することが求められているものの，具体的な管理方式が定められているわけではなく，その水準はまちまちである．

インターネットサービスの場合，些細な事故や不注意で，利用者の個人情報が際限ない範囲に流出してしまうリスクがある．サービス事業者側の管理水準の向上だけでこうしたリスクを低減させようとするには限界がある．インターネットサービス体系として個人情報を安全に守れる仕組みの実現が不可避である．

本稿では，ネットワーク上に分散された個人情報を仮想的に集約，提供する共通基盤を介して個人情報を管理，活用するビジネスモデルを提案する．これにより，サービス事業者は，自らが個別に利用者の個人情報を管理するのではなく，必要時に最小限の情報をこ

† 株式会社三菱総合研究所
MITSUBISHI RESEARCH INSTITUTE, Inc.
†† セコム株式会社
SECOM Co., Ltd.
††† 次世代電子商取引推進協議会
Next Generation Electronic Commerce Promotion Council of Japan

の共通基盤から提供してもらえばよい．また，利用者側にはネット上に登録した自分の情報の内容や所在を確認でき，新たなサービス事業者への送付や変更手続きが簡易に行えるメリットがある．

なお，本稿では，以後，広義の個人情報と区別するために氏名や住所，所属先など，個人情報における個別要素のことを個人属性と呼ぶこととする．

## 2. 現状のサービスにおける個人属性の取扱いの課題

**図 1** は利用者から特定の個人属性を得てサービスを実施するビジネスフローを示したものである．

サービス実施の際，サービス事業者は利用者から「正しい個人属性値」を提供してもらう必要がある．現実社会におけるサービスの場合は，事業者は利用者から公的機関など信頼できる第三者の証明書の送付をもってその属性が正しい（真正である）ことを確認している[1),2)]（**図 2**）．

一方，インターネットビジネスにおける個人属性の取扱いについては，大半のビジネスは利用者が自己申告で画面から入力した属性をそのまま使っており，真正性の確認もされていない状況である[3)]．また，法的に本人確認が求められているようなビジネスの場合でもサービス開始の段階で公的機関の証明書をサービス事業者に郵送するだけで，その後の取引場面で逐一属性を証明したり，確認したりすることは行われていない．

現実社会の証明書の送付という手段は，利用者側からすると，入手に時間，費用がかかるうえ，本来サービスに直接関連のない情報まで提供を強いられていることになる．また，サービス事業者に情報が渡った後は，提供した情報がどのような場面で利用され，適切に保管されているかなど，サービス事業者に確認することは容易にはできない状況にあった[1)~3)]．

個人情報保護法の施行により利用者は，サービス事業者が保有する利用者自身の情報の開示（25 条）や利用停止（27 条）の請求が可能となった[4)]．しかし，個人情報保護法は，具体的な個人属性が記載された帳票種類や情報システムの設計仕様，セキュリティ対策内容の公開までを規定したものではないため，利用者がサービス事業者の対策が十分なレベルであるか判断するのは依然として難しい状況にある．

インターネットにおけるビジネスでもこうした状況は変わらない．むしろ，日ごとに新たなセキュリティホールが発見されるような状況下では，サービス事業者すべてが最新かつ最高水準の情報管理，セキュリティレベルを維持するのは不可能であり，実際に対応できているサービス事業者は一握りと思われる．

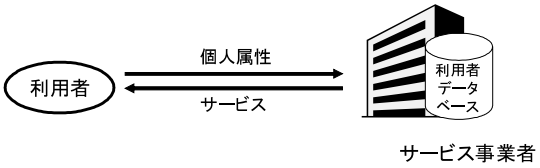


**図 1** 標準ビジネスフロー
Fig. 1 Business flow.

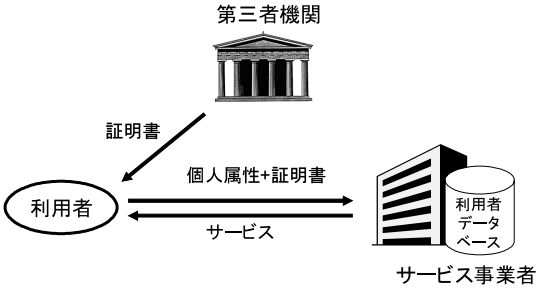


**図 2** 証明書を用いたビジネスフロー
Fig. 2 Business flow with certificate.

インターネットで事件や事故により情報が漏洩した場合，流出範囲や経路を調べることがきわめて難しいことを考えると，重要な個人属性を提供できるサービス事業者や享受できるサービスの種類は限られてしまうことになる．

これではインターネットから中小規模の企業やベンチャー企業の参入を締め出すことになり，新たなビジネスの発展を削ぐことになりかねない．とはいえ，利用者側が不安，抵抗をかかえたまま利用するという事態も解決しなければならない．

利用者が安心して自らの真正な属性を積極的にインターネット内に登録し，サービス事業者側でもその属性を安全に取り扱えるようにするためには，現行のインターネットで不足している下記のような仕組みを構築する必要がある．

**(a)** 利用者がインターネット上に属性を簡単に登録し，その内容を確認できる仕組み

**(b)** 属性を提供するすべてのサービス事業者の情報システムに安全にデータを送り，保管できる仕組み

**(c)** 属性の真正度合いを判断し，レベルに応じてサービスを提供できる仕組み

## 3. 関 連 研 究

本章では，2 章であげた課題について，現行実用化に向け進められている情報化技術，研究事例を示すと

ともにその限界点，課題について述べる．

### 3.1 属性の真正性を保持する技術

インターネットにおいて，送信時の属性の値が確実に受信時に保つための情報技術としては，これまで下記のような方式が検討され，国際標準化もしくは実現段階となっている．

(1) PKC（公開鍵証明書）[5),6)] の属性追加

(2) AC（属性証明書）[5),7),8)]

(1) は，公開鍵証明書のフォーマットにおける subject や extension フィールドに属性およびその値を記載する方式である．この場合，ビジネスフローは**図 3** のようになる．

(2) は，ITU-T 勧告 X.509 などで規定されているもので，認証局（CA: Certificate Authority）と属性認証局（AA: Attribute Authority）とを協調してビジネスを実施する方式である（**図 4**）．

公開鍵証明書や属性証明書を用いて個人の属性情報を交換する仕組みは，ディジタル署名の技術を用いて，信頼できる情報（信頼点）をもとに，そこからの連鎖をたどることにより属性が真正であることを保証し，だれもがこれを検証できるとするものである．この場合，証明書発行時に第三者である認証機関で利用者は属性を登録することになるが，認証機関による属性値の確認方法（現実の値とのマッチング）が厳密に定められているわけではない．また，これらの方式で取扱い対象としている属性情報とは特定の情報システムへのアクセス権限を判別するための保有資格や所属先を示す情報に限られ，その他多くの属性をこの証明書中に含ませることはできない．

公開鍵証明書や属性証明書による属性の活用は，扱う属性が証明書のライフサイクルに依存するようになるので，数年や 1 カ月といった期間を扱うものであり，動的に変更されやすい属性には向かない面がある．

なお，公開鍵証明書は近年発行および運用のコストが下がってきており，発行・運用・利用・検証の部分を含め COTS（コマーシャルオフザシェルフ）製品が活用できる利点がある．これに比較し，属性証明書を扱える汎用製品はまだ少ない．

このほか，利用者の属性をデータベースにより管理し，通信を暗号化する方法があるが，企業内システムなど閉じたシステムとして利用されるにとどまっている．これは，オープンな環境で利用するためには，個々の情報へのアクセス権限の設定，セキュリティ対策，属性情報の送受信履歴，属性情報の真正性などを管理するのにローカルでない汎用の枠組みが必要となるためである．このため，企業内やある一部の製品の内部，もしくは医療分野などの属性の厳密性を問う限られた領域で使用されることはあるが，一般の利用者間や企業サイトといったオープンな環境での属性情報の交換にこれらの方式を利用する例はほとんど見られていない．

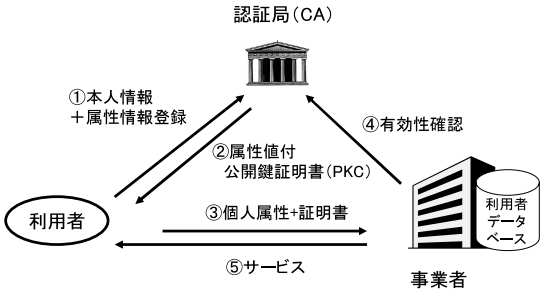


**図 3** 証明書を用いたビジネスフロー
Fig. 3 Business flow with attribute in certificate.

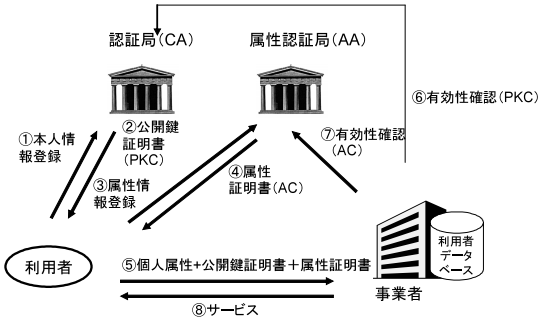


**図 4** 属性証明書（AC）を用いたビジネスフロー
Fig. 4 Business flow with attribute certificate.

2 章の最後であげた現行課題との対応の点では，（c）の属性の真正性については技術的に一部対応できているが，（a），（b）についての対応は仕様や目的から離れており，この技術をベースとした属性活用策を考えるのは困難と考えられる．

### 3.2 インターネット上で属性情報を安全に交換する技術

インターネット上で利用者の認証情報や属性情報を安全に交換するための仕組みとして最近注目されている技術に SAML [9)] や Liberty [10)] がある．

SAML（Security Assertion Markup Language）は XML 応用技術の標準化団体である OASIS（Organization for the Advancement of Structured Information Standard）で策定された 1 回のログイン認証で複数のサーバ上のサービスを利用できるようにするシングルサインオンのための仕様である．

Liberty は IT 企業，金融，運輸，政府および学術系の 150 ほどの組織が参加する非営利のアライアン

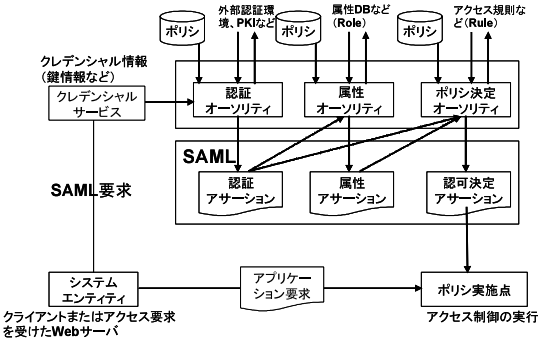


**図 5** SAML のモデル（文献 9) より引用）
Fig. 5 Model of SAML (Original source 9)).

スである Liberty Alliance により策定された前述の SAML を拡張したユーザ認証情報および属性情報の安全な交換のための仕様である．

### 3.2.1 SAML

SAML はセキュリティ情報と呼ばれる主体，すなわち人またはコンピュータが持つ認証結果情報，属性情報，アクセス権限情報を XML 形式で交換するために，要求と応答のプロトコルおよび，応答に含まれる XML 形式のデータの構文仕様を規定したものである．

**図 5** に SAML のモデルを示す．利用者であるシステムエンティティは最初に認証オーソリティに対し自身の持つ認証に必要なクレデンシャル情報，たとえば ID パスワードや PKI による認証を用いて認証を行い，利用者の本人性を示すためのセキュリティ情報である認証アサーションを発行する．これを属性オーソリティもしくはポリシ決定オーソリティに示すことにより利用者の属性情報や情報リソースへの認可権限などを判断し，属性アサーションや認可決定アサーションを発行し，実際にアプリケーションのアクセス制御を行うポリシ実施点にアサーションを渡し情報リソースへの細かいアクセス制御を行うことが可能となる．

すべてのアサーションは XML 署名や SSL/TLS 暗号通信などの技術を用いて改竄ができないような仕組みとすることも可能であり，認定された属性管理局から利用者の真正な属性情報を安全に配信することが可能である．また，通信プロトコルには HTTP や SOAP といった技術を用いることによりアプリケーションの相互運用性が高いことも特徴としてあげられる．

資格や所属など，権限のある組織により発行された真正性を保証された属性情報をリアルタイムにインターネット上で交換するために，SAML は優れた仕組みを提供している．

登録時に属性情報を確認する手順や，属性情報がプライバシ個人情報である場合の第三者提供や本人同意の仕組みなど SAML 仕様で規定されていない部分については，サービスで利用する場合には検討が必要となる．

### 3.2.2 Liberty

Liberty はセキュリティおよびプライバシ保護に配慮しつつ，複数の組織で管理されているネットワークアイデンティティと呼んでいる本人情報を連携させ，シングルサインオン認証や属性情報の交換を行う SAML を拡張した標準仕様である．Liberty は 3 つの仕様により構成されている．

- ID-FF（Identity Federation Framework）：シングルサインオンとアイデンティティ連携
- ID-WSF（Identity Web Services Framework）11：アイデンティティサービスのための Web サービスフレームワーク（属性情報の交換）
- ID-SIS（Identity Services Interface Specification）12：アイデンティティ連携と Web サービス関連付加価値サービス（交換する属性セットの仕様）

Liberty の重要な特徴の 1 つにプライバシの保護がある．ネットワークアイデンティティを連携させてサービスを提供する場合に，これを連携させる方法として一意的な ID を用いた場合，その ID を通じて利用者がどのような組織に属しどのような活動を行ったかといったプライバシ情報が特定される場合がある．そのため Liberty では連携させる際に仮名と呼ばれる動的に生成された ID 情報を用いて連携させ，利用情報が漏洩した場合でも本人を特定し難い仕組みを採用している．また，プライバシ情報の自己コントロールのための仕組みも検討されている．

### 3.2.3 現行技術の課題

SAML や Liberty はインターネットで複数の主体間で属性情報を交換，共有する標準技術であるが，一般利用者が自らの属性情報を安心して提供し，活用するための情報基盤としては下記のような 2 点の課題がある．

1 点目は SAML や Liberty などの技術は属性情報の利用のためだけに設計されたものではないため，属性情報の活用とは直接関係のないコンポーネントが多くあり，仕様が複雑に見えてしまう点である．また逆にあってしかるべきコンポーネントが不足しており，追加開発が必要となる部分も多い．通信プロトコルや電文フォーマットに関しても実際のサービスの提供の際に必要な設定項目などを制限するといったプロファイリングの概念が十分に対応されるに至っていない．

2 点目としてこれらはまだ要素技術の域を出ておら

ず，情報基盤として必要な運用面を配慮した機能設計がされていないことがある．

たとえば，属性を管理する主体が行うべき運用作業フロー，またサービス提供者および利用者の管理主体へのサービス要求など，具体的なビジネス場面での様々な場面におけるトランザクションパターンや例外処理への対応は仕様外であり，外部で補わなければならない．

2 章であげた現行課題との対応の点では，（b）の通信過程については規定の仕様に基づいた通信を行えることで，送信相手のシステム環境や安全性レベルが確認できる．また，送信時に利用者の同意を確認できる機能もある．ただし，送信後の属性情報については仕様範囲外であり，この仕組みを採用していることがサイト全体の安全性を示すものではない．

また，SAML，Liberty ともにサイトに登録する時点での属性値の信頼性（真正性）については仕様外である．これは，いわば自己申告した属性情報を複数のサイト間で共有していることにすぎず，（c）の課題を解決できるものではない．

なお（a）については現行，Liberty 対応しているサイト自体がほとんどないため評価できないが，操作性については大きな課題はないと考える．

## 4. 属性情報プロバイダ

本章では，インターネットにおいて利用者の真正な個人属性を安全に取り扱うビジネスを展開するために，3 章で示した研究，技術を活用しつつ，現行の仕様では不足しているインターネット上で個人属性情報を実サービスで安全かつ簡単に取り扱うことができるための共通的な仕組み，新たな情報基盤の必要性を述べる．また，この仕組みの中で特に，個人属性を登録し，管理および活用するための新たな基盤を「属性情報プロバイダ」として提案する．

### 4.1 属性情報共通活用基盤モデル

#### 4.1.1 インターネットにおける属性情報活用のための要件

インターネット上に利用者が自らの真正な属性を積極的に登録し，活用していくには 2 章であげた現行のサービスに欠けている点のうち，3 章で明らかになった現行の関連情報技術ではカバーできていない点，すなわち「インターネット上で個人属性情報を実サービスで安全かつ簡単に取り扱うこと」に対応する必要がある．以下，具体的内容について述べる．

（1）属性のタイプに則した登録書式や型の統一化

現在，同様な属性であってもサービス事業者（サイト）ごとで書式やコード体系は様々である．各種の属性について共通に利用できる型やコードを規定することにより，異なるサービス事業者間での属性の交換，共有を容易にすることができる．

（2）属性の真正性の確認情報の付加

インターネット上に登録した属性について，第三者が確認した場合に，確認者や手段などの情報を付加できるようにする．これにより利用時点での属性の信頼度合いを属性を利用する側が判断できるようになる．

（3）属性確認・更新のワンストップ化

インターネット上の異なるサービス事業者（サイト）に登録された本人の属性を集約して照会し，また必要に応じて更新できるようにする．これにより，属性が変わった場合でも各サービス事業者（サイト）に逐一通知する負担や忘失を減らすことができる．

（4）属性データの保存，送受信システム仕様の共通化および外部監査による安全性レベル維持

共通の属性データの保存，通信仕様を策定し，その仕様に準じたシステムを構築し，技術的な安全性レベルについて認定された機関がチェックを行えるようにする．これにより，利用者は自らの属性を登録する先や利用する先への安全性について事前に評価することができる．

#### 4.1.2 属性情報の共通活用のためのネットワーク基盤

前述の要件を実現するには，インターネットの各サービス事業者（サイト）が独自の方式で属性を管理するのではなく，インターネット上で利用者の属性情報を一元管理し，なんらかのサービス場面で必要となった際のみに最小限の情報を安全な方法で送信（提供）できるようなサービス事業者間共通で使用できる情報基盤が必要と考える．

ただし，単一の機関が個人属性を集約管理し，各サービス事業者に情報を送信するようなモデルはセキュリティリスクやビジネス展開の点で困難と考えられる．

むしろ，分散管理というインターネットの特長を活かし，規定のセキュリティレベルを達成している複数の機関間で，各事業分野に関連した属性を分散管理し，インターネット上で仮想的に集約する方式の方が適していると考える．

この分散した複数機関が利用者の属性を連携して管理する仕組みのことを本稿では以後，属性情報共通活用基盤と呼び，**図 6** に示したような 3 つのシステムを連携させるモデルを提案する．

「データ登録・管理システム」とは利用者の現実社会における各種の属性を登録し，安全に管理するための

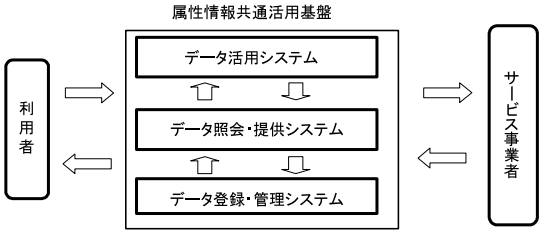


**図 6**　属性情報共通活用基盤
Fig. 6　Framework of personal attribute management.

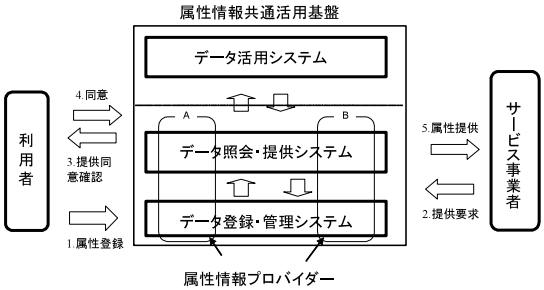


**図 7**　属性情報プロバイダ
Fig. 7　Personal Attribute Provider.

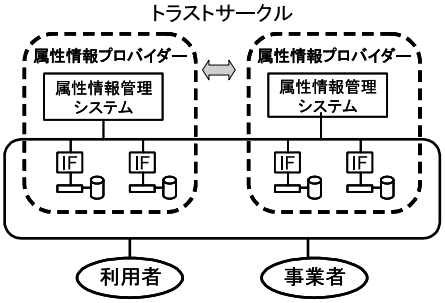


**図 8**　属性情報プロバイダ概念図
Fig. 8　Image of Personal Attribute Provider.

情報システムを含んだサービス体系のことをいう．利用者は「データ登録・管理システム」を担当する機関に自分の各種の個人属性を登録すれば，以後インターネット内でその属性を属性情報共通活用基盤を通じて各種サービス事業者に提示することが可能になる．また，登録の際に現実社会における各種の証明書などをその属性の真正性の根拠として登録することができる．このシステムは 4.1.1 項の（1），（2），（4）の要件に対応している．

「データ照会・提供システム」とは，分散された「データ登録・管理システム」で管理されている利用者の属性情報を当該利用者の要求に応じて，検索，集約し照会する情報システムを含めたサービス体系のことをいう．また，利用者の要求に応じてサービス事業者にサービスを受けるのに必要な属性情報を送る機能もある．このシステムは 4.1.1 項の（3），（4）の要件に対応している．

「データ活用システム」は属性情報共通活用基盤上に蓄積された利用者の各種の属性を統計的に処理し，インターネットマーケティング用のデータとしてサービス事業者に情報を提供する情報システムを含めたサービス体系のことをいう．このサービスは利用者がインターネット上に自分の属性を登録することで対価を得られるというビジネスモデルであり，属性登録を促進する効果が見込める．

このように今回提案する属性情報共通活用基盤は全体として 4.1.1 項で示した各要件に対応している．また，基盤の構成を 3 つのシステムに分けることにより，この基盤サービス実施を行う場合でも，サービス範囲を選択することが可能となる．

### 4.2　属性情報プロバイダの提案

#### 4.2.1　属性情報プロバイダの概念モデル

属性情報共通活用基盤のうち，「データ登録・管理システム」，「データ照会・提供システム」の 2 つは 4.1.1 項であげた各要件に対応しているもので，利用者，サービス事業者双方が現行課題と考えている点を解消できるサービスモデルである．

この 2 つのシステムで必要とされる情報通信の基礎技術には，3 章で示した現行の属性交換に関連する情報通信技術を用いることができると考えられる．

したがって，利用者から属性を得る場面やサービス事業者に提示する場面などのサービス手順や運用方式を規定することができれば，実際に情報システムを構築できる可能性も大きい．

そこで，この 2 つのシステムを連携して，利用者から特定のビジネス分野で必要とされる個人属性を収集し，必要に応じてサービス事業者に提供するサービスモデルを以後，「属性情報プロバイダ」と呼び，具体的なサービス要件や情報システムで実現すべき機能要件を述べる．

**図 7** は属性情報共通活用基盤における属性プロバイダの位置づけと，利用者，サービス事業者とで属性を送受する手順を示したものである．属性プロバイダは複数の機関から構成されており，それぞれ提供先のサービス分野（業種）に応じて取り扱う属性種類や提供方式が異なる．

こうした複数の特定の業種に特化した属性情報プロバイダが各分野の標準的な基盤になりうれば，**図 8** のように異なる分野の属性情報プロバイダ間が信頼関係を結び必要な情報を提供し合うトラストサークルに展開することも可能となる．

属性情報プロバイダを介して利用者とサービス事業者間で属性を安全に管理，提供するためには，データ登録・管理システム，データ照会・提供システムに下記のような機能を備えておく必要がある．

（1）データ登録・管理システム

（1－1）個人属性確認・登録機能

利用者の個人属性を確認し，保有する情報システムに登録するもので，この際に属性そのものの値のほか，属性の信頼性に関する情報（真正性証明資料，有効期限，失効条件など）についても同時に登録する．

（1－2）属性情報要求受付/送信機能

連携している「データ照会・提供システム」からの要求に応じて，管理している属性の値や関連する情報を「データ照会・提供システム」に送信する．

（2）データ照会，提供システム

（2－1）属性集約機能

複数の「データ登録・管理システム」が管理している利用者の各種属性をネットワークを通じて集約し，仮想的に一元管理しているように取り扱う．

（2－2）属性照会・利用停止機能

属性情報プロバイダに登録した自らの全属性情報を一度の操作で確認するもの．また，必要に応じて登録した属性を削除，無効化したり，提供をやめたりすることを行う．

（2－3）属性情報要求受付・検証機能

利用者からサービス事業者に送信された属性提供許可証を受け付け，その内容が適正であるかを検証する．

（2－4）情報提供同意確認機能

サービス事業者に利用者の属性情報を提供する際に，提供の同意（許可）を得る機能．

（2－5）属性情報提供機能

利用者から提供要求を受けたサービス事業者向けに，利用者の属性の値そのものや関連する情報を他に流用できないような安全なデータ形式かつ通信方式により送信する．

**図 9** は，属性情報プロバイダにおけるこれらの機能の使用場面と利用者，サービス事業者との関連を表したものである．

#### 4.2.2 属性情報プロバイダへの Liberty 適用イメージ

属性情報プロバイダに必要な情報システム間の通信や情報連携の要素技術には，相互運用性の高いプロトコルや通信過程での強い安全性，提供の際の本人への確認という点に対応が要求される点をふまえ，Liberty 仕様を適用し，現行技術仕様で対応できていない機能要件を拡張する方式が実用に適していると考える．

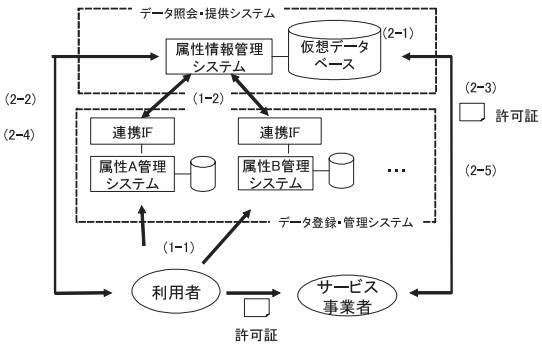


**図 9** 属性情報プロバイダ利用イメージ
Fig. 9 Usage of Personal Attribute Provider.

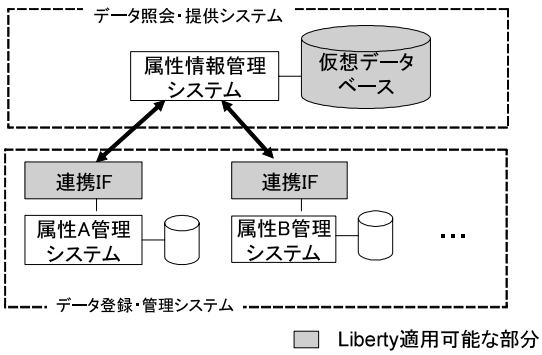


**図 10** 属性情報プロバイダにおける Liberty 適用部
Fig. 10 Liberty components of the Personal Attribute Provider.

Liberty では特定の利用者の本人認証を行った後，複数のサービス事業者の同じ利用者の ID を連携させ，要求された属性を探索する仕組みがある．これは図 9 で示したデータ登録・管理システムとデータ照会・提供システム間のデータ連携に関わるインタフェース（1－2）と仮想データベース関連機能（2－1，2－2）に応用できると考える（**図 10**）．

Liberty は公開された仕様であり，これを要素技術に適用した場合，もともと属性情報プロバイダとして構築されたのではない情報システムでも比較的容易に属性情報プロバイダ仕様に拡張することができる．

したがって，すでに多くの利用者の属性情報を保有しているような企業で，利用者から同意を得ることができれば，既存の情報システムに簡単なインタフェースを組み込むだけで属性情報プロバイダのメンバになることが可能である（**図 11**）．また図 8 で示したトラストサークルの実現の点でも汎用性のある Liberty 仕様の適用は有利である．

#### 4.2.3 利用場面例（シナリオ）

本項では，属性情報プロバイダを経由して利用者が

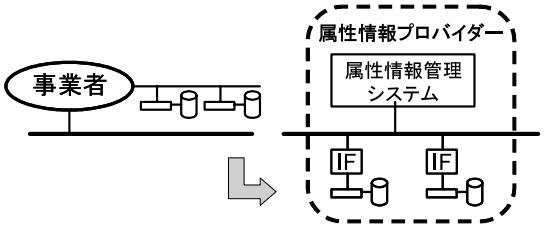


**図 11**　属性情報プロバイダ移行図
Fig. 11　Sift to Personal Attribute Provider.

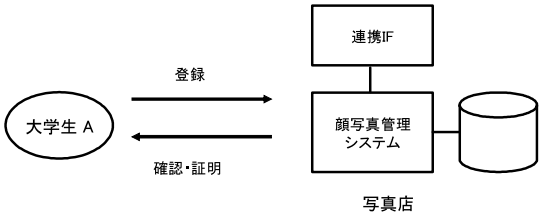


**図 13**　属性情報プロバイダ利用例（属性の登録）
Fig. 13　Use case of the Personal Attribute Provider (A step of attributes registration).

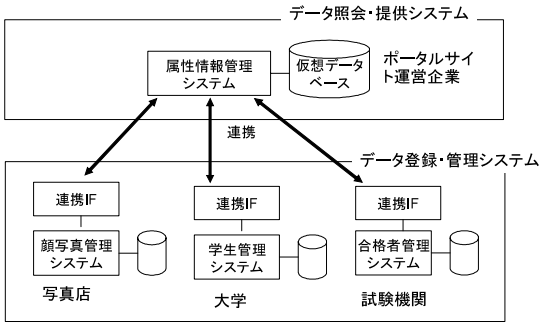


**図 12**　属性情報プロバイダ利用例
Fig. 12　Use case of the Personal Attribute Provider.

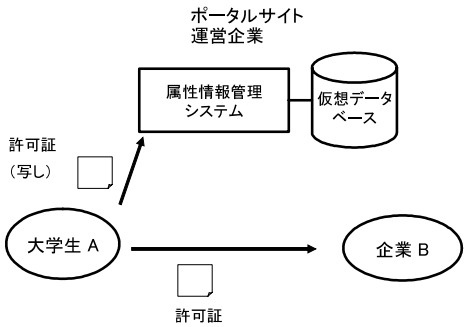


**図 14**　属性情報プロバイダ利用例（許可証の送信）
Fig. 14　Use case of the Personal Attribute Provider (A step of getting permissions).

特定の属性をサービス事業者に渡すというビジネスフローをもとに現行の課題が解消されるようになるか確認する．

ここでは，写真店，大学，試験機関，ポータルサイト運営企業から構成される属性情報プロバイダ（**図 12**）を想定する．写真店，大学，試験機関はデータ登録・管理システムのサービスを，ポータルサイト運営企業がデータ照会・提供システムのサービスを担当する．

大学生 A が企業 B のアルバイトに応募する場面で，インターネットを通じて企業 B に次の属性を送る手続きを考えてみる．

**a)**　顔写真
**b)**　大学在籍証明
**c)**　保有資格

（1）インターネットへの真正属性の登録

大学生 A が企業 B に送る属性のうち，b）大学在籍と c）保有資格についてはすでに大学と試験機関がそれぞれ大学生 A の在籍情報，試験合格の情報を所有しており，自ら管理する情報システムに登録している．

a）顔写真についてはインターネット上に登録されていないため，大学生 A は写真店を通じて顔写真を属性情報プロバイダに登録する必要がある．

大学生 A は写真店に出向き，顔写真を撮影してもらう．写真店では同時に自ら管理，運営する「顔写真管理システム」に大学生 A の顔写真データを登録する．この際，写真店では大学生 A の本人性（本人であるか）を現実社会における証明書（運転免許証など）で確認する．確認手段や確認者についても第三者が参考にできるようデータとして登録する（**図 13**）．

（2）属性提供許可証の送信

大学生 A は次のような記載を含む「許可証」を作成し，企業 B および属性情報プロバイダに送信する（**図 14**）．

- 企業 B（指定アドレス）への大学生 A の顔写真データの提供
- 企業 B（指定アドレス）へ A が大学生であり，応募に必要な資格を所有していることの証明（確認者）の提供

（3）属性の調査

企業 B は，大学生 A から送られた許可証を属性プロバイダの属性情報管理システム（ポータルサイト運営企業）に送信し，必要な情報の調査，提供を要求する．

属性情報管理システムでは，許可証の有効性を検証した後，データ登録・管理層の連携先機関に大学生 A の属性の問合せを行い，必要なデータや真偽の回答を得る（**図 15**）．

（4）属性の提供

属性情報管理システムは連携先機関から得られた情報を整理し，必要な情報を企業 B に送る（この場合

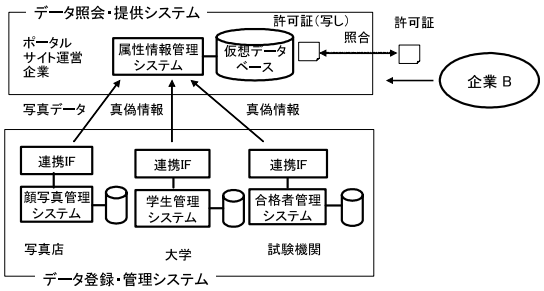


**図 15** 属性情報プロバイダ利用例（属性の検証）
Fig. 15 Use case of the Personal Attribute Provider (A step of attribute verification).

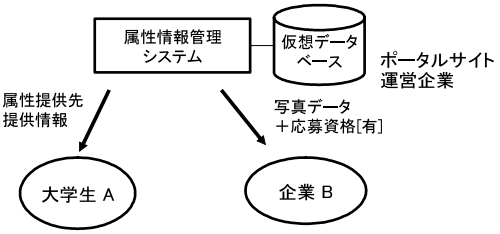


**図 16** 属性情報プロバイダ利用例（属性の提供）
Fig. 16 Use case of the Personal Attribute Provider (A step of supplying attributes).

は写真データと応募資格有という情報）．また同時に大学生 A に属性提供先（企業 B）と提供した属性内容を通知する（**図 16**）．

この一連のサービスを 2 章の最後にあげた 3 つの課題に照らし合わせてみると，（a）については属性を登録する先が普段の行動圏に設定可能なことやインターネット上で属性を集約照会できることで対応できていることが分かる．（b）については，属性情報プロバイダからは利用者の必要最小限の情報を安全な形式で送っており，また値そのものは送らない，という対応も可能としている．（c）については，信頼できる機関の属性情報プロバイダ参加や第三者確認という対応により課題を解決している．

これらから属性情報プロバイダは現行の課題 3 点を同時に解決するポテンシャルを持つ基盤ということができる．

## 5. 考察・今後の展開

インターネット上の利用者（個人）の属性情報を安全に集約管理し，活用するための共通的な仕組みとして，属性情報共通活用基盤というビジネスモデルを考案した．その中の利用者から属性情報を集め，サービス事業者に提供する仕組みを特に「属性情報プロバイダ」として，機能設計や実装技術を考案した．また，利用シナリオを作り，属性情報プロバイダの機能の利用場面や属性情報のフローについて実用性を検証した．その結果，属性情報プロバイダを介して属性を送信することで，利用者は送り先に対し，必要以上の属性を送らずに済み，また，属性の提供を受けるサービス事業者も不必要な個人情報を取得することなく，個人情報管理リスクを軽減できるというメリットを明らかにすることができた．

このビジネスモデルでは，利用者は一度属性情報プロバイダに属性を登録すれば，各種のサービスでその属性を繰り返し利用することが可能となる．また，属性登録の際，第三者がその値が真正であることを証明することにより，属性値の信頼性を大幅に高められ，これまでインターネットでは実現しにくかった新たなサービスの創出が見込める．

属性プロバイダは技術的な実現可能性という点では，SAML や Liberty など既存の通信技術やセキュリティ技術を適用可能であり，さらに，これらの技術を最大限に活用することですでに運用されている各種の情報システムの拡張を可能とし，高い信頼性のある属性情報を低コストで多量にインターネット上に集積することが見込める．ただし，交換するメッセージフォーマットのプロファイルや利用者の同意確認手段の規定という点は課題である．

属性情報プロバイダは特定の業界のビジネスにおける属性の提示，提供を目的としたものであるが，異なる属性情報プロバイダどうしをさらに連携することでインターネット上の複数の業界間で属性を安全に取り扱う共通的な基盤に展開させることができる．連携するシステムの規模が大きくなることで，4.1.2 項で示した「データ活用システム」を属性情報プロバイダの機能として組み込むことも可能である．

ただし，属性情報プロバイダのシステム運営や連携するサービス事業者の審査方式など運用面については大きな課題であり，実現化にあたっては分散化された情報の管理責任範囲の明確化，基盤全体としての安全性を第三者が評価できる仕組みなどについても今後十分な検討が必要である．

**謝辞** 本研究は経済産業省の「平成 16 年度 EC 技術基盤の相互運用性に関する調査研究」の一環として実施した．

## 参 考 文 献

1) 電子商取引推進協議会認証公証 WG：属性情報利用システム―2010 年の市民生活，p.121，電子商取引推進協議会 (2004).

2) 電子商取引推進協議会認証公証 WG：属性情報プロバイダーの検討—個人情報保護に配慮した属性情報活用基盤，p.102，電子商取引推進協議会 (2005).
3) 前田陽二，千葉昌幸：属性情報登録・活用基盤モデルの考察，情報処理学会研究報告 2003-IS-86 (2003).
4) 個人情報の保護に関する法律 (2003). http://www5.cao.go.jp/seikatsu/kojin/houritsu/
5) ITU-T Recommendation X.509 Information technology — Open systems interconnection — The Directory — Public-key and attribute certificate frameworks.
6) Housley, R., et al.: RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, The Internet Society (2002).
7) 電子商取引推進協議会認証公証検討チーム：属性認証ハンドブック，p.104, 電子商取引推進協議会 (2005).
8) 牧野二郎ほか：電子認証のしくみと PKI の基本, p.335, 毎日コミュニケーションズ (2003).
9) Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 (2003).
10) Liberty ID-FF Architecture Overview Version 1.2, Liberty Alliance Project (2003).
11) Liberty ID-WSF Web Services Framework Overview Version 1.1, Liberty Alliance Project.
12) Liberty ID-SIS Personal Profile Service Specification Version 1.0, Liberty Alliance Project.

(平成 17 年 6 月 16 日受付)
(平成 18 年 1 月 6 日採録)

**千葉　昌幸**

1966 年生．1990 年東京工業大学工学部卒業．同年（株）三菱総合研究所入社．1999 年筑波大学大学院経営・政策研究科修了．主に情報セキュリティ，システム監査，情報化政策に従事．システムアナリスト，公認システム監査人．

**漆嶌　賢二**

1988 年早稲田大学理工学部電気工学科卒業，同年セコム株式会社入社．2002 年より PKI，認証分野の研究開発に従事．2005 年 10 月よりエントラストジャパン株式会社．

**前田　陽二**（正会員）

1972 年早稲田大学理工学部電気通信工学科卒業，1974 年同大学大学院修士課程修了，同年三菱電機（株）入社．主に文字・画像認識分野の研究開発に従事．2001 年より電子商取引推進協議会主席研究員．現在，電子署名および認証の分野を中心に調査研究に従事．次世代電子商取引推進協議会セキュリティWG 主席研究員．東海大学総合情報センター非常勤講師．共著『電子文書保存のしくみと実務』電子情報通信学会会員，工学博士．