経済産業省委託調査

平成１６年度ＥＣ技術基盤の相互運用性に関する調査研究

（取引相手先の属性認証技術等の調査）

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～

平成17年２月

電子商取引推進協議会

財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１６年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「平成１６年度ＥＣ技術基盤の相互運用性に関する調査研究（取引相手先の属性認証技術等の調査）」の成果を取りまとめたものです。

序文

認証公証WGでは、平成15年度に情報ネットワーク上でサービスを受けるために提供する個人の属性情報について、その活用と保護の両面から検討し報告書「属性情報利用システム－2010年の市民生活」としてまとめた。この中でこれまで個々のサービス提供者が収集し管理していた属性情報の管理・運用を主な業務とする「属性情報プロバイダー」の基本概念を提案した。さらに、この「属性情報プロバイダー」を実現する技術として、SAML(Security Assertion Markup Language)の調査を行い「SAML利用検討報告書」にまとめた。このSAMLは新しい認証・認可の仕組みとして標準化されたシングルサインオン(SSO)のメカニズムを提供すると同時に、プライバシーに考慮した個人情報の管理方法を提供するものとして注目されている技術である。

今年度は、これらの検討結果に基づいて「属性情報プロバイダー」の実用に向けた検討を進めた。

本報告書では、平成17年4月より施行される「個人情報の保護に関する法律」をはじめとするプライバシー保護にかかわる法律の調査結果の紹介、及びプライバシー保護を考慮したオープンな仕様提供しているLiberty Alliance Projectの調査結果の紹介を行う。さらに、これらの調査に基づいて検討した「属性情報プロバイダー」の機能や技術要件、及び法的要件について解説するとともに、Liberty仕様によるSAMLを用いた「属性情報プロバイダー」のユースケースを紹介する。

本報告書が、属性認証の利用を検討している企業、機関の方々にとって一助になることができれば幸いである。

平成17年2月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目　次

1．はじめに

1.1　背景

現在のオンラインサービス、オンラインショッピングでは、個人情報をそのサービス毎に氏名・年齢・住所・電話番号・嗜好などの情報を提供しサービスを享受しているが、本来サービスの提供に必要とは思えない情報を収集していたり、また、その企業や自治体等が持つ持つ個人情報が大量に流出する事件が相次ぐなど企業における個人情報の取り扱いが社会問題化しており、消費者は企業で扱われる自身の個人情報について不安を抱いている。

表 1-1 最近の主な個人情報の流出事故

発覚時期	企業名	流出規模
2003 年 6 月	ローソン	56 万人
2003 年 10 月	ファミリーマート	18 万人
2004 年 1 月	三洋信販	120 万人
2004 年 2 月	ヤフーBB	660 万人
2004 年 3 月	ジャパネットたかた	66 万人
2004 年 3 月	アッカ・ネットワークス	34 万人
2004 年 3 月	東武鉄道	13 万人
2004 年 4 月	コスモ石油	92 万人
2004 年 4 月	日本信販	10 万人
2004 年 6 月	阪急交通社	62 万人
2004 年 10 月	三重県立図書館	13 万人

この対応策として「個人情報の保護に関する法律」(以下、個人情報保護法) [1]が 2005 年 4 月に施行され、また、事業分野毎に監督省庁による個人情報保護ガイドラインが策定されている。個人情報保護法では、過去 6 ヶ月にわたり 1 日でも 5001 人以上の顧客の個人情報を事業用途で利用した事業者は個人情報取扱事業者として個人情報を扱う際の義務が発生する。

これにより、組織の持つ個人情報管理に係る情報セキュリティ基準に基づき、個人情報を管理するサーバーおよびネットワークのセキュリティ対策はもちろんのこと、権限のあるものしかデータにアクセスできない事、サーバールームへのフィジカルアクセスについての管理、監査ログ、取扱者教育等の厳重なデータの取り扱いが必要とされサーバールームへの入退管理や監視カメラによるチェックなど、管理義務を満足するためのコストが大幅に増大することが容易に想定できる。

企業規模のあまり大きくない個人商店のような電子商取引サイトや情報サービスなどでは、管

理体制に幾つかの問題点を抱えてしまうか、個人情報を預かることをあきらめざるを得ないような状況が発生するかもしれない。

これまで ECOM 認証公証 WG では、個人の属性情報を活用し、且つ安全な電子商取引の利用拡大を目的として属性証明書による属性の管理や、属性情報データベースについて検討を重ねてきた。属性情報データベースもこれを遵守した形で提供されるものでなければならない。単にデータベースをネットワーク越しに共有するという仕組みでは、安全に属性情報を管理することはできないのである。

1.2 目的

前節で述べたような現状を踏まえ、以下の目的で報告書を作成する。

【目的】
インターネット上で個人情報を安全・安心・便利に管理し活用するための社会基盤となる属性情報プロバイダーを定義し、サービスを行うにあたり、知っておくべき事柄を総括し、サービスの提供者はもちろんの事、利用者においてもその遵守すべき注意事項を示すことを目的とする。

属性情報プロバイダーはそのような問題を解決するための情報基盤であり、ここ数年間 ECOM 認証公証ワーキンググループで検討されてきた属性情報活用サービスを総括するものである。サービスの利用者は属性情報プロバイダーに情報を預け、サービス提供側は必要な属性情報のみを属性情報プロバイダーに要求する。サービス提供者側は一時的に必要なだけの属性情報を預かってサービスを提供するのみであり、個人情報管理の義務の大部分をアウトソースすることができる。

個人情報保護の係る法制度およびガイドラインの拡充や、個人情報保護に関する世論の高まりから、本報告書で示される属性情報プロバイダーの考え方に基づくサービスが属性を保護しながら属性情報を活用していくという情報基盤のキーサービスになると思われる。

今回検討した属性情報プロバイダーには以下のような特徴がある。

- **全ての属性情報を一元管理するようなサービスではない。**
- **サービス利用者／提供者は複数の属性情報プロバイダーが連携した情報を取得し、サービスを利用することができる。**
- **標準技術に基づいており特殊なプロトコル、実装を必要としない。**
- **利用目的の開示**
- **自己情報コントロール権を扱うためのフレームワーク**

2 章では前年度までの調査報告に基づく属性情報プロバイダーの基本概念を示し、法制度およ

び技術の側面から検討する必要性について説明し、3 章ではプライバシー保護に関連した法制度を解説する。4 章では属性情報プロバイダーの法制度面からの要件を定義する。5 章では、安全な認証情報の連携および属性情報利用のための標準技術である Liberty に基づく属性情報プロバイダーについて述べ、6 章では、Liberty だけではカバーできない要件の実装方法について検討する。

1.3 表記

1.3.1 参考文献

参考文献は“［文献略号］”の形式により表記する。参考文献の一覧は 8 章に示す。

1.3.2 法制度およびガイドラインへの参照

法制度やガイドラインの条項を参照するために“{制度略号 A.B.C}”の形式により表記する。“A”、“B”および“C”は条項の番号であり、例えば“A 条 B 項の C”を意味する。参照記号の一覧を以下に示す。制度の引用が明らかである場合には括弧“{“および”}”を省略することもある。

参照記号	法制度やガイドラインの名称
{ox}	OECD の 8 原則
{ex}	EU 指令
{個 x.x}	個人情報の保護に関する法律(平成十五年法律第五十七号)
{令 x.x}	個人情報の保護に関する法律施行令(政令第五百七号)
{方 x.x}	個人情報の保護に関する基本方針(平成 16 年 4 月 2 日 閣議決定)
{事 x.x}	経済産業省 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
{信 x.x}	総務省 電気通信事業における個人情報保護に関するガイドライン
{放 x.x}	総務省 放送受信者等の個人情報の保護に関する指針
{金 x.x}	金融庁 金融分野における個人情報保護に関するガイドライン(案)
{法 x.x}	法務省 法務省が所管する分野における事業者等が取り扱う個人情報保護に関するガイドライン(案)
{財 x.x}	財務省 財務省所管分野における事業者に対する個人情報の保護に関する指針(案)
{交 x.x}	国土交通省 国土交通省所轄分野に係る個人情報保護に関するガイドライン(仮称)(案)
{農 x.x}	農林水産省 個人情報の適正な取扱いを確保するために農林水産分野における事業者が講ずべき措置に関するガイドライン
{雇 x.x}	厚生労働省 雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針

2．属性情報プロバイダー

2.1　平成 15 年度属性情報利用システムの検討

ECOM では平成 15 年度 EC 技術基盤の相互運用性に関する調査研究事業(取引相手先の属性認証技術等の調査)における報告書「属性情報利用システム－2010 年の市民生活－」において、下記のように属性情報活用基盤の基本的な概念を示した。

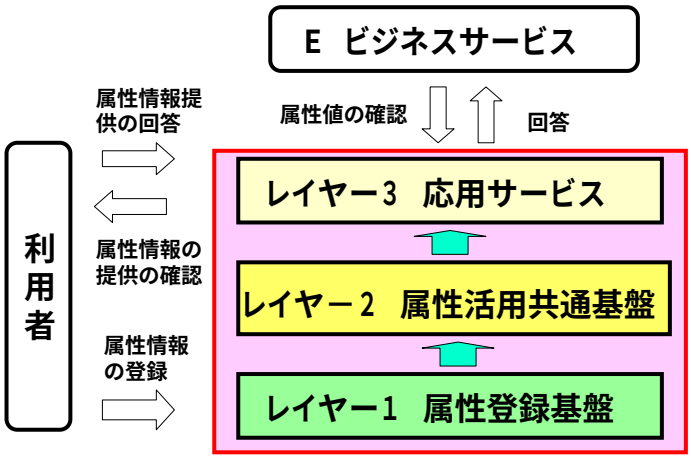


図 2-1 属性情報活用基盤の基本概念図

属性情報プロバイダーの基本的な概念は、利用者と E ビジネスサービスサイトが直接利用者に関する属性を送受信することなく、E ビジネスサービスサイトは属性情報プロバイダーを通じて利用者の属性に関する情報を得るというものである。現行のように直接、利用者と E ビジネスサービスサイト間が属性をやりとりするモデルでは双方に次のようなリスクがあった。

表 2-1 現行のネット上の属性利用のリスク

対象	リスク
利用者	・取引先の数、種類が多く、複数のサイトに重要な個人情報を提供しなければならない。 ・取引の種類によってはサイトに住民票や免許証の写しなどの郵送が課せられる。 ・自分の属性(個人情報)の管理方法が不明で、どのような情報が登録されているのかが掴めない。 ・1 ヶ所からでも情報が漏れると、被害の範囲、影響が甚大となる。
E ビジネス サービスサイト	・情報提供者は本当に本人か、確実な保証の仕組みがない。 ・ネットで提供(申請)された属性(情報)が、真正かどうか判別するのに別の証明が必要である。あるいは自己申告レベルでのサービス範囲を余儀なくされる。 ・属性の収集、管理に莫大なコストがかかる。そのための技術要員や社員教育、等が必要とされる。

こうした利用者、E ビジネスサービスサイト双方のリスクを軽減させるため、両者を仲介する

属性情報プロバイダーには次のような仕組みを備えていることが必要であるとした。

- **利用者が自分の正しい(真正な)個人属性を簡単かつ確実に属性情報プロバイダーに登録する仕組み(サービスレイヤー1)**
- **登録された利用者の個人情報を安全に管理、メンテナンスし、利用者の要求によりEビジネスサイトに必要な属性に関する情報を通知する仕組み(サービスレイヤー2)**
- **特定のビジネス領域に特化して、複数の利用者の属性値を元に統計(トレンド)やビジネス条件に対する判別を行なう仕組み(サービスレイヤー3)**

このような仕組みが実現すると、表 2-1 に示した双方のリスクは下記のように大きく軽減するとともに、これまでにはなかった属性を活用した新たなサービスが実現する可能性もある。

- **第三者が証明した属性をインターネットで利用できることが可能になる**
- **登録された属性を変更することが容易になる。また、その属性を利用しているEビジネスサービスサイトに、一斉に属性変更の通知を行なうことができる。**
- **E ビジネスサービスサイトに必要な属性だけを通知することができる。公的機関の証明書(住民票等)を送付する必要がなくなる。**
- **登録属性をもとにした質問や第三者が情報機器操作の証明を行なうことにより、なりすまし対策を強化できる。**
- **E ビジネスサービスサイトを利用できる諸条件(年齢、住所地域等)を判定し、条件をクリアしている商取引要求だけをEビジネスサービスサイトに送ることができる。**
- **登録した個人属性(統計値)を参照させることにより、特典が得られる新しいサービスが期待できる。**

このように、H15 年度の調査では基本的な概念やそれによるビジネス・サービス形態の変化について検討、整理を行なったが、属性情報プロバイダー事業自体の法制度上の対応や実現に向けての実装技術の詳細については課題となっていた。本 WG では H15 年度の内容を引き継ぎ、上記の課題について、法制度面では、特に「個人情報保護法」を中心に事業実施で留意すべき点を、また実装技術としてサイト間で同じ属性値を共有できる仕組みの 1 つである Liberty Alliance Project で提唱されている概念を元に実装モデルを作成し、考察を試みた。次章以降に、これらの結果を示したい。

2.2　属性情報プロバイダーとは

本報告書が扱う属性情報プロバイダーを定義し、その事業モデルを提示する。

属性情報プロバイダーは前節で述べた属性情報活用基盤におけるレイヤー1(属性の登録)およびレイヤー2(属性の管理､提供)を提供する事業者にあたり､以下の機能を基本とするものである。

- ◆ 利用者に対し属性情報を登録する手段を与える
- ◆ 利用者の属性情報を安全に管理する
- ◆ 利用者の不利益にならない形で、属性情報をオンラインで他の事業者へ提供する

従来のオンラインにおける属性情報の利用方法としては、単体のサイトで属性情報を管理し自身のサービスに利用するもの(図 2-2)、あるいは、グループ内のサイトで属性情報を一元管理し共有するもの(図 2-3)がある。グループ内での属性共有の例としては、グループ企業内での利用や、会員店舗を募ったショッピングモールサイトのような形態がある。このような従来型の利用形態は、統一された属性情報の運用ポリシーが適用できる閉じられた事業者グループといえ、属性情報共有の仕組みについてもグループ内で閉じられた独自の仕様に基づくものが多い。

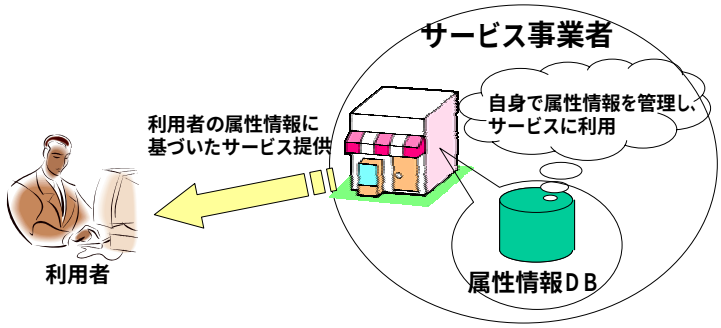


図 2-2 従来型サービス事業者(単体サイトでの属性管理)

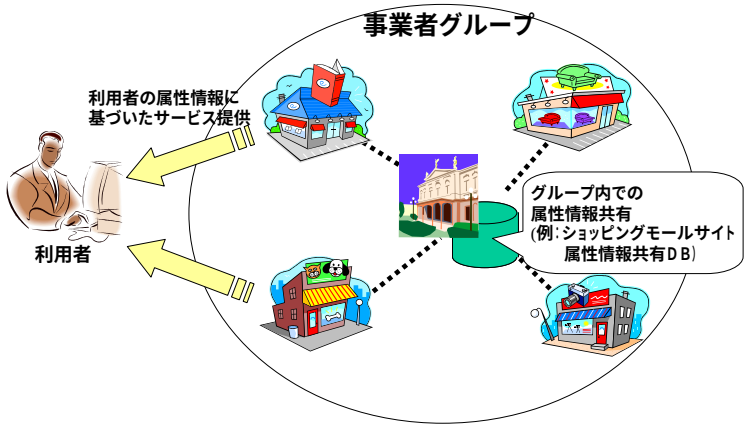


図 2-3 従来型サービス事業者(グループ内での属性共同利用)

属性情報プロバイダーはオンライン上で他の事業者へ利用者の属性情報を提供する事業者であるが、提供先となる事業者は必ずしも同じグループに属するわけではなく、そのため従来型の事業者とは異なる特徴をもつ。以下に属性情報プロバイダーのモデルを示し、従来型の事業者との相違点について述べる。

属性情報プロバイダーは大別して 2 種類の事業モデルが考えられる。

一つ目のモデルは属性情報プロバイダーが自身で管理している利用者の属性情報を利用してサービスを提供する一方で、利用者の属性情報を他の事業者へ提供するものである(図 2-4)。このような属性情報プロバイダーとしては、サービス事業のために既に利用者の属性情報を管理しており、その属性情報自体を提供する新たな事業を行う事業者が考えられる。

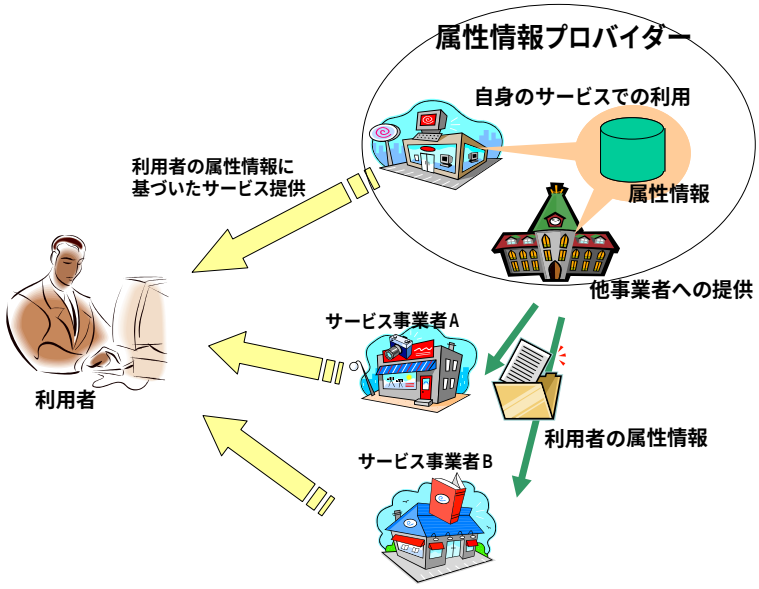


図 2-4 属性情報プロバイダー　モデル 1(兼サービス事業者)

もう一つのモデルは、他の事業者へ利用者の属性情報を提供することを専門とする属性情報プロバイダーである(図 2-5)。このような形態をとる属性情報プロバイダーは利用者の属性情報について真正性を確認可能な権威ある機関といえ、例えば、利用者の資格認定を行い、その資格についての証明書を発行する機関が考えられる。

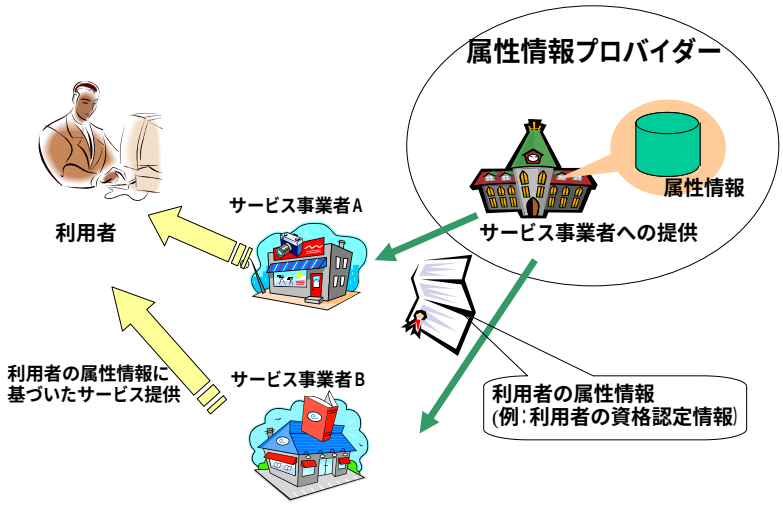


図 2-5 属性情報プロバイダー　モデル 2(属性情報提供のみ)

これらのモデルに見られるように、属性情報プロバイダーは運用ポリシーの異なる多数の事業者に属性情報を提供するため、従来型事業者モデルと比較し以下の点が特に課題となる。

- **従来型の事業者モデルと異なり利用目的をあらかじめ特定することが難しい場合がある。利用者の属性提供に際しての同意確認が重要となる。**
- **属性提供のメカニズムとしてはオープンな仕様が望ましい**

従来型事業者モデルと属性情報プロバイダーの比較を
表 2-2 に示す。

表 2-2 従来型事業者モデルと属性情報プロバイダー

	従来型事業者モデル	属性情報プロバイダー
属性提供の範囲	企業グループ内など閉じられた環境	外部の事業者への提供
運用ポリシーなど	グループ内で統一されたポリシー	事業者毎に異なる可能性がある
属性提供のメカニズム	独自の仕様でもよい	オープンな仕様が望まれる

2.3　属性情報プロバイダーの利用モデルの例

属性情報プロバイダーを利用するサービス事業者について 2 つのモデルを例示する。

図 2-6 のモデルは、サービス事業者自身は利用者の属性情報を管理せず、属性情報プロバイダーにアウトソースするモデルである。サービス事業者は利用者の属性情報が必要になる毎に属性情報プロバイダーより取得する。複数の属性情報プロバイダーに委ねるケースも考えられる。

このモデルではサービス事業者は利用者の個人情報を管理するリスク・コストを低減することができる。一方で統計やマーケティング等の利用に不自由さがあるため、個人情報管理のリスク

を重視する中小規模サービス事業者において可能性のあるモデルである。

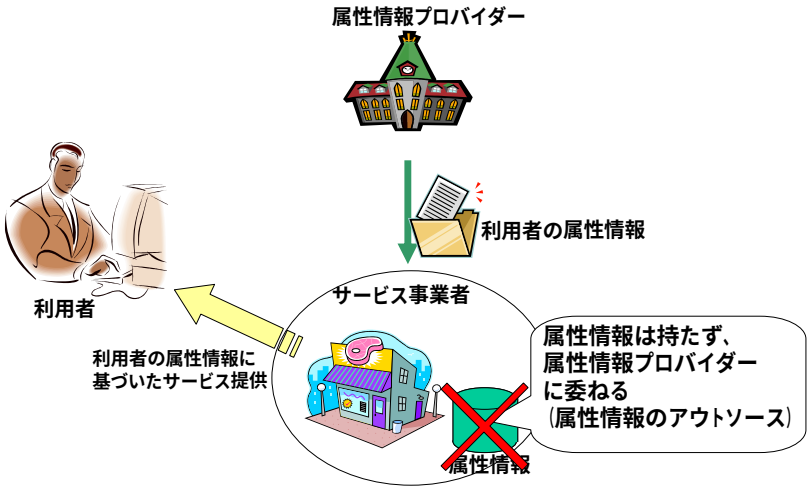


図 2-6 属性情報プロバイダーの利用(アウトソース)

図 2-7 のモデルは属性情報プロバイダー兼サービス事業者(図 2-4 のモデルと同様)が、他の事業者と利用者の属性情報を交換し連携するモデルである。各事業者は自身で管理する属性情報は必要最低限のものにとどめ、他の属性情報が必要な場合には必要に応じて他の属性情報プロバイダーから取得する。事業者間はそれぞれが対等な立場であるといえ、企業アライアンスによる事業連携などで可能性のあるモデルである。

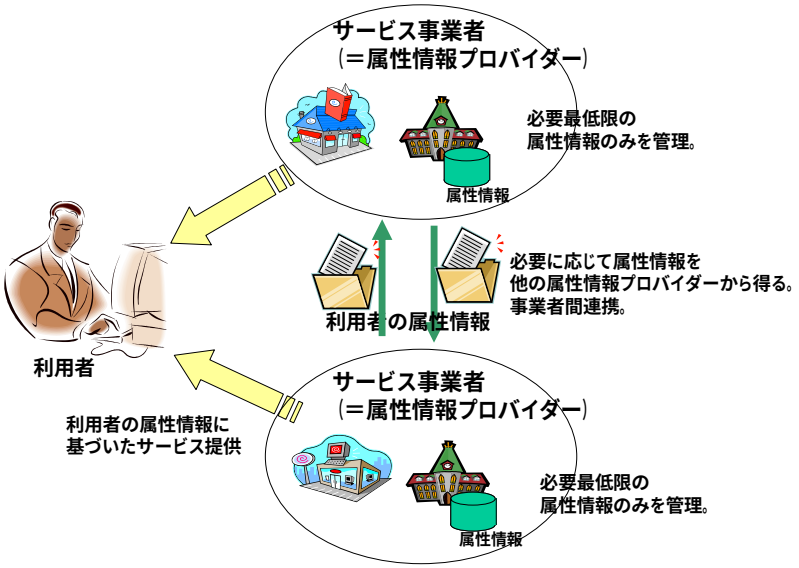


図 2-7 属性情報プロバイダーの利用(連携)

2.4　属性情報プロバイダーの機能要件

- **属性情報の提供**

ユーザが情報サービスやオンラインショッピングを利用する際に必要となる属性情報を提供する。

- **属性の保管先**

属性を集約的に一元的に管理した場合、情報漏洩した場合の影響は大きい。基本的には属性は属性情報サービスで管理可能な属性のみを分割して管理し必要の無い属性は持たないものとする。また、ユーザは属性の保管先として、任意のサービスを選択することが可能である。属性を集約的に一元的に管理した場合、情報漏洩した場合の影響は大きい。基本的には属性は属性情報サービスで管理可能な属性のみを分割して管理し必要の無い属性は持たないものとする。また、ユーザは属性の保管先として、任意のサービスを選択することが可能である。

- **認定された属性**

属性には、ユーザの意思のみで登録可能な属性と、認定された属性が存在する。認定された属性は、その属性値を持つべきアイデンティティおよび、属性値の真正性を確認可能な機関が受理し、属性の管理登録を行う。属性登録機関として別の組織にアウトソースすることも可能であるとする。

- **複数の属性情報プロバイダーの連携利用**

「属性の保管先」で述べたように属性は、複数の属性情報プロバイダーに保管することが可能であるが、これらを連携させて利用することが可能とする。ただし、連携は属性の主体者である利用者の意思に基づいてなされるものとする。また、固定 ID による連携は、集約管理と同等かそれ以上の漏洩リスクを持つこととなるので、この対策を行う。例えば医療関係の組織が、利用者の資産状況などの与信情報や、音楽の嗜好など組織に関係の無い属性情報は管理する必要がない。属性情報はその種類毎に複数の信頼できる属性情報サービス事業者に委託されるあるサービスを受ける場合に、ユーザの合意に基づき複数のサービス事業者にある情報を連携させて利用できる。

- **匿名、仮名、実名での利用**

サービスの種類によっては、匿名や仮名を用いて、個人情報漏洩リスクに配慮しながらサービスを提供できるものとする。匿名や仮名のアイデンティティを利用することにより、不要な個人情報を集めないままサービスインできるものとする。

- **プライバシーポリシーの告知と同意の獲得**

属性情報サービス事業者はプライバシーポリシーを開示し、利用者に対して告知し、事前(オプトイン)または事後(オプトアウト)に同意を得る。属性情報サービスプロバイダーおよび、その属性を消費する情報サービス事業者(情報サービスやオンラインショッピングなど)は、オプトイ

ン、オプトアウトの双方に対応している必要がある。

- **紛争解決の手段を明示する**

- **監査ログ**

ID および、これに紐付けされた属性の利用および操作のログを監査用に記録する。紛争解決にはこれを用いる。

- **標準技術への準拠**

利用者認証や属性情報の仕組みは標準技術に則ったものとし、相互運用性を確保する。

3．プライバシー保護の法制度

オンラインサービスの利用者が個人の属性情報を安心して預け、利用するためには、属性情報プロバイダーがプライバシー保護に関連する法制度等に準拠することが必要である。本章では、プライバシー保護に関係する国内外の法制度やガイドラインについて説明する。

プライバシー関係の法制度およびガイドラインの関係を示したのが図 3-1 である。経済協力開発機構(以下、OECD)が定めたプライバシー保護に関するガイドラインに基づき各国法制度が整備もしくは見直しされ、さらに日本では分野毎に準拠すべきガイドラインをより具体的な表現で策定している。以降、各制度の詳細について説明する。

図 3-1 個人情報保護に関する法制度・ガイドラインの関係

3.1　個人情報保護法

2005 年 4 月 1 日に全面施行される個人情報保護法は日本における個人情報保護のため事業者が持つ顧客情報等の個人情報の取扱い義務を定めた法律である。個人情報保護関連 5 法のうちの 1 つであり、その中で民間を対象にした唯一の法律である。

- **個人情報の保護に関する法律(基本法制)**
- **行政機関の保有する個人情報の保護に関する法律**
- **独立行政法人等の保有する個人情報の保護に関する法律**
- **情報公開・個人情報保護審査会設置法**
- **行政機関の保有する個人情報の保護に関する法律等の施行に伴う関連法律の整備等に関する法律**

以下に個人情報保護法の章構成を示す。

- **第 1 章　総則**
- **第 2 章　国及び地方公共団体の責務等**
- **第 3 章　個人情報の保護に関する施策等**
- **第 4 章　個人情報取扱事業者の義務等**
- **第 5 章　雑則**
- **第 6 章　罰則**

1 章から 3 章までは、官民を通じて適用される基本法部分であり、民間事業者を監督すべき立場にある官公庁や地方公共団体が先行して成立･公布された時点である 2003 年 5 月に同時に施工されている。4 章以降は 2005 年 4 月より施行される民間事業者の個人情報の取扱いルールを定めたものである。第 4 章で述べられている個人情報取扱事業者の義務については、顧客個人情報を扱う一般的な事業者に対して広く適用されるものであるため、特に把握しておく必要があるものである。以下の義務を定めている。

- **利用目的による制限**
- **適正な取得**
- **安全管理措置**
- **第三者提供の制限**
- **開示・訂正・利用停止**
- **その他**

これまで、個人情報の不正な取扱いについては、民事で解決するか、プライバシー情報に含まれるものであれば名誉毀損罪などで解決することができたが、個人情報保護法は事業分野毎に所轄官庁が監督し、違反があった場合には主務大臣が勧告あるいは命令などの行政処分を行なうことができ、刑事罰を与えることができる点が異なる。勧告、命令を出すかどうかどうかの基準は事業分野ごとのガイドラインとなり、ガイドラインは実質的に強制力を持つものと考えられる。

3.2　個人情報保護法の系譜

個人情報保護は、国際的には 1980 年の OECD「プライバシー保護と個人データの国際流通についてのガイドライン」をきっかけに OECD 加盟国を中心に諸外国で法整備が進められている。日本では OECD8 原則に準拠し、国の行政機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定された。1995 年に採択された「EU 個人情報保護指令(EU 指令)」では、第 25 条にて EU 域外の各国と個人データを流通する際の規定が定められており、日本でもこれに対応することが必要になった。2000 年に「個人情報保護法制に関する大綱」が決定され、これをうける形で主に民間部門を対象に「個人情報の保護に関する法律案」が国会に提出されたが、一部メディアの反発に合い、廃案となった。しかし、2003 年に修正された同名の法案

が国会に再提出され、5 月に成立となった。2005 年 4 月 1 日に全面施行が決定している。

	日本	諸外国
1980 年(S55)		・OECD「プライバシー保護と個人データの国際流通についてのガイドライン
1988 年(S63)	・「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」公布	
1995 年(H7)		・「EU 個人情報保護指令」採択
1999 年(H11)	・高度情報通信社会推進本部「個人情報保護検討部会」設置	
2000 年(H12)	・個人情報保護法制化専門委員会「個人情報保護法制に関する大綱」	
2001 年(H13)	「個人情報保護に関する法律案」提出(廃案)	
2003 年(H15)	「個人情報保護に関する法律案(修正案)」提出(成立：平成 17 年 4 月 1 日全面施行)	

3.3 OECD の 8 原則

OECD は、1980 年に「加盟国は、国内法および国内政策の相違にもかかわらず、プライバシーと個人の自由を保護し、かつプライバシーと情報の自由な流通という基本的ではあるが競合する価値を調和させることに共通の利害を有すること、個人データの自動処理及び国際流通は、国家間の関係に新しい形態を作り上げるとともに、相互に矛盾しない規則と運用の開発を要請すること、個人データの国際流通は経済及び社会の発展に貢献すること、プライバシー保護と個人データの国際流通に係わる国内法は、そのような国際流通を妨げる恐れがあること、を認識し、加盟国間の情報の自由な流通を促進すること及び加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避することを決意し」(出展：外務省ホームページ「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告(仮訳)」)「プライバシー保護と個人データの国際流通についてのガイドライン」[24][25]の理事会勧告を採択した。

1. 収集制限の原則(合法的な手段により入手し利用者への通知・同意を得る)
2. データ正確性の原則(個人情報は利用目的に即したものである)
3. 目的明確化の原則(利用目的に必要な範囲で正確・完全・最新である)
4. 利用制限の原則(要求された目的以外で利用してはならない)
5. 安全保護の原則(紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置が必要)
6. 公開の原則(個人データに係る開発・実施・政策は一般に公開される)

7. 個人参加の原則(自己データの存在を利用者がいつでも確認できる)
8. 責任の原則(管理者は上記を全うする責任を持つ)

上記勧告では、個人データの取り扱いに関して、上記表に示す 8 つの基本原則を示し、これを加盟国の国内法に含むことを考慮するよう求めている。

3.4 JIS Q 15001

1997 年、通産省(当時)は「EU 指令」への対応措置として「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を公表した。

このガイドラインをより体系的なマネジメントシステム規格(表 3-1)として整理し、日本のローカルルールとして 1999 年に制定したものが日本工業規格 JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」である。

JISQ15001 は、企業による個人情報保護の自主的取組のための全経営活動に統合されたマネジメントシステム(コンプライアンス・プログラムと呼ぶ)の策定・実施・維持・継続的改善の必要性を指摘し、そのようなコンプライアンス・プログラムの最小限の要求事項を規定している。これは法的要求ではないが、企業は自社のコンプライアンス・プログラムが JISQ15001 への適合していることを示すことで、個人情報を適切に取り扱っていることを訴求することができる。

JIS Q 15001 は制定後 5 年の改訂時期を迎えており、2005 年 4 月に本格施行され法的要求となる個人情報保護法との整合性確保のための見直しが行われている。

なお、適合性を客観的に評価する第三者認証制度としてプライバシーマーク制度(3.5 節参照)が運用されている。

表 3-1 JISQ15001：1999 目次と PDCA マネジメントシステム要素の対応

0. 序文			4.4.2 -5 情報主体以外から間接的に収集する場合の措置	D
1. 適用範囲			4.4.3 個人情報の利用及び提供に関する措置	
2. 引用規格			-1 利用及び提供の原則	
3. 定義			-2 収集目的の範囲外の利用及び提供の場合の措置	
4. コンプライアンス･プログラム要求事項			4.4.4 個人情報の適正管理義務	
4.1 一般要求事項	P		-1 個人情報の正確性の確保	
4.2 個人情報保護方針			-2 個人情報の利用の安全性の確保	
4.3 計画			-3 個人情報の委託処理に関する措置	
4.3.1 個人情報の特定			4.4.5 個人情報に関する情報主体の権利	
4.3.2 法令及びその他の規範			-1 個人情報に関する権利	
4.3.3 内部規程			-2 個人情報の利用又は提供の拒否権	
4.3.4 計画書			4.4.6 教育	
4.4実施及び運用	D		4.4.7 苦情及び相談	
4.4.1 体制及び責任			4.4.8 コンプライアンス･プログラム文書	
4.4.2 個人情報の収集に関する措置			4.4.9 文書管理	
-1 収集の原則			4.5 監査	C
-2 収集方法の制限			4.6 事業者の代表者による見直し	A
-3 特定の機微な個人情報の収集の禁止				
-4 情報主体から直接収集する場合の措置				

P：Plan(計画)、D：Do(実施及び運用)、C：Check (監査)、Act(見直し)

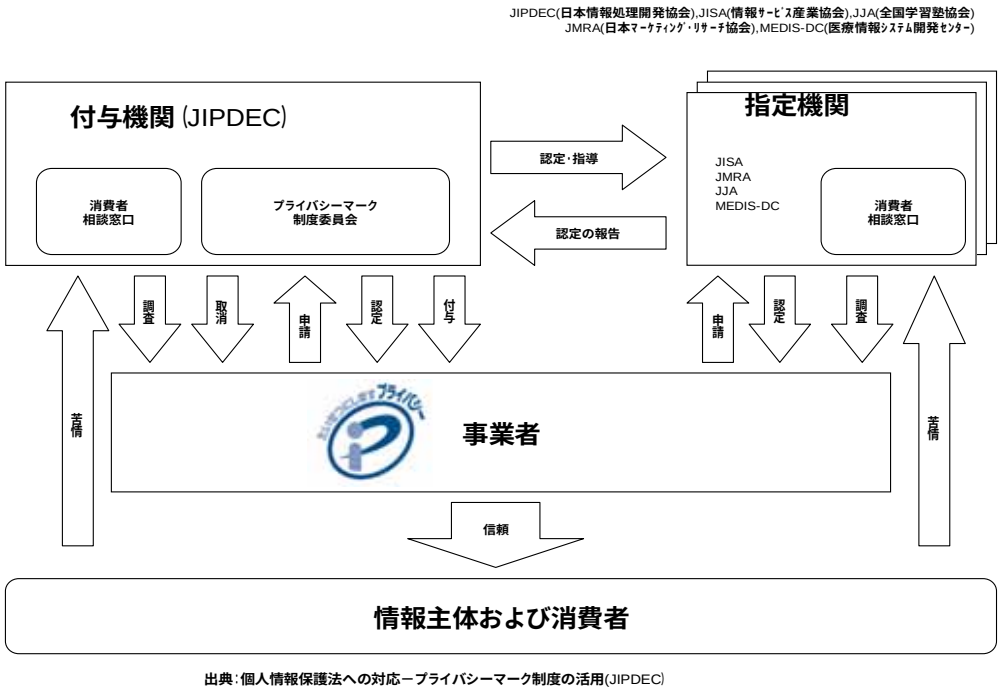
3.5　プライバシーマーク制度

1998 年に開始されたプライバシーマーク制度は、事業者が個人情報の取扱いを適切に行う体制を整備していることを認定し、そのことを消費者の目に見えるプライバシーマークで表示することを許すことによって、事業者に個人情報保護推進のためのインセンティブを与えることを目的としている。

同制度の運用開始時は通商産業省(当時)告示の「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」の遵守を認定基準としていたが、1999 年の JISQ15001(前節参照)の制定に伴い、同規格への適合性が認定基準として採用されることになった。

適合性の認定は財団法人日本情報処理開発協会(JIPDEC)および指定機関(JIPDEC が指定する業界団体)が行う。プライバシーマークの取得を希望する事業者は JIPDEC に、所属する業界団体が指定機関となっている場合は指定機関に申請し、書類審査・現地調査を受査しなければならない(図 3-2 参照)。

プライバシーマークの有効期間は 2 年間であるが、更新手続きにより 2 年間の延長を行うことができる。以降、2 年ごとに更新を行うことができる。マークの取得により法的義務は発生しないが、個人情報の不適切な取扱いが判明した場合は、プライバシーマーク付与の取消が行われその旨が公表されること、取消により 2 年間は再申請ができなくなることなどによって、制度の実効性が担保されている。



出典：個人情報保護法への対応－プライバシーマーク制度の活用(JIPDEC)

図 3-2 プライバシーマーク制度

3.6 各国個人情報保護法

欧米では1960年代後半より個人情報保護の必要性が認識されるようになり検討が進められた。1970年に、米国公正信用報告法および旧西ドイツヘッセン州データ保護法が制定され、スウェーデンは1972年、世界に先駆けて国家として個人情報の保護に関する法律を制定した。これに続いて以降、米国、ドイツ、ノルウェー、フランスなどが個人情報法を制定したが、制定された条項・内容に関して各国法が異なっていた。そのため、国際的に個人情報を流通させる際に、その差異が問題になっていた。

この問題を受け1980年、OECDは個人情報を国際流通させるために遵守すべき最低限のルールとして8つの原則を勧告において規定した。1980年以前に個人情報保護法を制定した国はOECD8原則に沿って改正されている。

また、EUは、1995年に「EU指令」として、上記OECD8原則を踏まえて個人データ処理の適法性に関する一般準則を定め、特にその第25条で「個人データの第三国への移転は、この指令に従って採択された国内規定の順守を損なうことなく、当該第三国が十分なレベルの保護処置を確保している場合に限って行うことができることを定めなければならない」と規定している。

各国の個人情報保護法をまとめたのが以下である。(表 3-2)

表 3-2 各国の個人情報保護法

制定年	最終改正年	国名	個人情報保護法の名称	対象	
				官	民
1973	1998	スウェーデン	Personal Data Act	○	○
1974	1988	米国	Privacy Act of 1974	○	
1977	1990	ドイツ	Federal Data Protection Act	○	○
1978	1994	ノルウェー	Act Relating to Personal Data Registers	○	○
1978	1994	オーストリア	Federal Data Protection Act	○	○
1978	1994	フランス	Act on Data Processing、 Data Files and Individual Liberties	○	○
1979	―	ルクセンブルグ	Nominal Data(Automatic Processing)Act	○	○
1982	―	カナダ	Privacy Act	○	
			Personal Information Protection and Electronic Documents Act(1999)		○
1987	1999	フィンランド	Personal Data Act	○	○
1988	2000	オーストラリア	Privacy Act	○	○
1988	―	アイルランド	Data Protection Act	○	○
1988	1993	オランダ	Data Protection Act	○	○
1988	―	日本	行政機関の保有する電子計算機に係る個人情報の保護に関する法律	○	
			独立行政法人等の保有する電子計算機処理に係る個人情報の保護に関する法律	○	
			個人情報の保護に関する法律(2003)		○
1989	―	アイスランド	Act Nr.121 Concerning the Registration and Handling of Personal Data	○	○
1991	1998	ポルトガル	Protection of Personal Data Act	○	○
1992	1999	ベルギー	Law on the protection of privacy regarding the processing of personal data	○	○
1992	―	ハンガリー	The Law on Protection of Personal Data and Disclosure of Data of Public Interest	○	○
1992	1999	スペイン	Law on the Regulation of the Automated Processing of Personal Data	○	○
1992	―	スイス	Federal Law on Data Protection	○	○
1993	―	ニュージーランド	Privacy Act	○	○

1994	1998	イギリス	Data Protection Act 1998	○	○
1994	－	韓国	The Protection of Personal Information by Public Organizations Act(公的機関を対象)	△	
1995	－	EU	EU 指令		
1996	－	イタリア	Law on Protection of Individuals and Other Subjects Regarding the Processing of Personal Data	○	○
1997	－	ギリシャ	Protection of the Individual Against Processing of Personal Data	○	○
1997	－	ポーランド	Act on the Protection of Personal Data	○	○
1999	－	チェコ	The Protection of Personal Data in Information System Act	○	○
2000	－	デンマーク	The Act on Processing of Personal Data	○	○

各国の個人情報保護法は以下に示す 3 つの種類に分類することができ、日本では現在セグメント方式を採用している。

- **オムニバス形式(EU 諸国で採用)**
  公的部門と民間部門を単独法で包括的に規制対象とする方式
- **セグメント方式(現在、日本で採用)**
  公的部門と民間部門を個別法で規制対象とする方式
- **セクトラル方式(米国)**
  規制対象を限定して個別領域毎に規制を行なう方式

3.7　日本における事業分野別個人情報保護ガイドラインについて

3.7.1　事業分野を所轄する省庁によるガイドライン

IT 関係省庁連絡会議幹事会にて、民間の保有する個人情報の大量漏洩事件が多発する状況を鑑みて 2004 年 3 月 12 日に、所管の業界等に関する個人情報保護ガイドラインの策定、見直しを要請した。その結果、2004 年 6 月以降、各業界を管轄する省庁から分野別のガイドラインが公表されている。

2004 年 12 月現在、省庁の定める事業分野毎の個人情報保護ガイドラインは策定中のものを含め以下の分野となる。

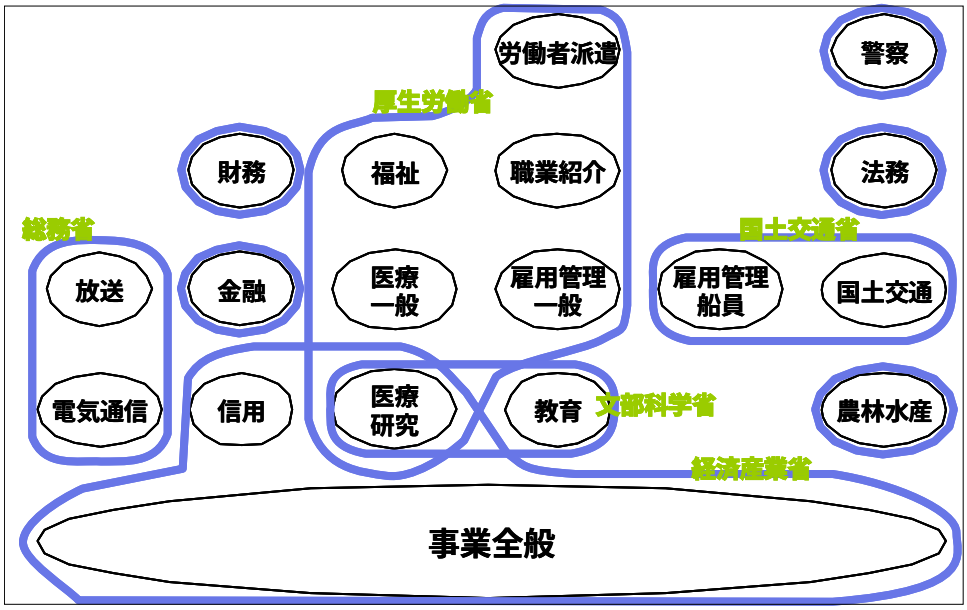


図 3-3 省庁の定める事業分野毎の個人情報保護ガイドラインのマップ

ある分野の事業者が個人情報保護法の違反があった場合、その分野主務大臣は是正するよう勧告または命令などの行政処分ができるが｛個 34｝、その基準として分野毎のガイドラインが参照されるとの見方もあり、事業者はどの分野に属しどのガイドラインに従うべきか検討しておく必要がある。

事業分野毎に定められたガイドラインの特長は以下のようになる。

- **事業分野毎に規定された、事業者および利用者向けのガイドラインでありガイドラインの対象となる主体の定義が最初になされている**
- **事業を鑑みた個人情報の内容とその利用・収集の例外規定を定めている**

代表的なガイドラインについて、その特徴を述べる。

- **経済産業分野(経済産業省)**
  - **一般の事業者が考慮すべき内容をわかりやすく記述**
  - **利用目的を具体的に特定し公表する必要性の言及**
  - **安全管理措置を細分化(組織的、人的、物理的、技術的)**
  - **監督者が従業員と事業主(役員)の双方を含むことの明記**
  - **委託した場合の定期的監督と不当な負担を強いないことの明記**
  - **第三者提供でのオプトインを要求**
  - **JISQ15001**
- **金融分野(金融庁)**
  - **例外規定(生命の危険、犯罪の誘発、国際信頼の失墜にあたらない)**
  - **収集・利用目的の特定**
  - **機微(センシティブ)情報の定義**
  - **与信と第三者提供**
  - **実務指針。従業者に役員を含める｛金 11｝**
- **電気通信事業(総務省)**
  - **「電気通信事業者」「利用者」などの用語定義**
  - **利用収集の例外規定**
  - **情報の種類＝通信履歴・利用明細・発信者位置・不払い利用者・電話番号とその取り扱い**
  - **通信の秘密**

属性情報プロバイダーとなる事業者で、医療、金融、放送、通信等の特別な業種に属さない場合には、経済産業省の定める指針や、通信販売業者、電子商取引事業者(ECOM)、インターネットプロバイダーなどの業界団体が自ら定めた指針に従うことになる。

3.8　その他の法律

プライバシー保護に関係する法律は個人情報保護法だけではない。本節では、それらの法律について、プライバシー保護に関する法的責任(罰則)の構成について改めて概説する形で説明する。

一般に、ある事件に関する法的責任(罰則)は、

- **民事責任(民事罰)**
- **刑事責任(刑事罰)**
- **対行政責任(行政罰)**

の 3 つから構成される。例えば、交通事故を例に取ると、

- **民事責任：加害者の被害者に対する責任→損害賠償などの罰則**
- **刑事責任：犯罪者の社会に対する責任→懲役刑や罰金刑などの罰則**
- **対行政責任：犯罪者の行政に対する責任→自動車免許に関する違反点数や反則金などの罰則**

となる。以下、これをプライバシー保護に適用して考える。

まず、個人情報保護法では、行政責任と刑事責任に関する規定がある。行政責任については、主務大臣への報告を行うこと {個 32} や、主務大臣からの勧告／命令 {個 34} に従うことなどを定めている。刑事責任については、前述の行政責任で掲げた義務に違反した際の、行為者／管理責任者／法人への懲役刑／罰金刑 {個 56～58} などを定めている。

また、個人情報保護法に関し各省庁から出されたガイドラインに違反すると、当該企業等が所属する業務分野の所管省庁から、行政指導や業務停止命令、免許剥奪などの行政罰を受けることがある。

ここで注意しなければならないのは、上述以外の条項に違反しても責任／罰則を負わないわけではないという点である。即ち、例えば個人情報漏洩事件が起きた場合、これらの行政責任／刑事責任の他に、民事上の賠償責任を負う可能性は常に存在する。従って、個人情報保護法だけを見て、罰則規定がない特定の条項に違反しても罰せられないという認識は誤りであり、そのような行為は厳に謹まなければならない。

また、もう一つ注意しなければならないのは、個人情報保護法では、主務大臣への対応を行う管理責任者や法人に対する罰則だけが規定されており、個人情報漏洩を実際に犯した従業員やクラッカーへの罰則は定められていないという点である。即ち、そうした従業者の責任は、個人情報保護法では問えない。

こうした実際の漏洩者の責任を問う手段としては、刑事責任に関しては、刑法上の窃盗罪や、不正競争防止法／不正アクセス禁止法違反などが考えられる。

例えば、従業員が情報漏洩行為の際に企業の資産であるハードディスクなどの有体財を持ち出していれば、窃盗罪が成立する。しかし、単に情報をコピーして持ち出した場合、情報などの無体財に対しては窃盗罪は成立しない。これに関しては、今後の刑法改正で、無体財の窃盗に関する「情報窃盗罪」の新設が検討されている。

企業や団体の「営業秘密」として個人情報を管理していた場合には、対象が有体財でも無体財でも、情報を持ち出した従業員を不正競争防止法違反に問うことができる。特定の情報を不正競争防止法上の営業秘密として守るためには、「アクセス制限され秘密であることが明らかなこと」

「公に知られている情報ではないこと、またこれが区別されていること」など幾つかの要件を満たす必要がある。従って、個人情報保護に不正競争防止法を活用しようという企業は、これらの要件に十分配慮しなければならない。

ネットワークなどの電子メディアを介した不法侵入により個人情報が外部に持ち出された場合は、それらの情報を管理していた企業は、不正アクセス禁止法違反に基づき持ち出した者の刑事責任を問うことができる。不正アクセスについても、「不正」が成立する前提として、システムが適正に管理されていることが求められており、企業はそれらの適正管理措置に十分配慮すべきである。

また、漏洩者に対しては、上述のさまざまな刑事責任の成立に関わりなく、常に損害賠償などの民事責任を問うことは一般的に可能である。この場合、漏洩者は、漏洩した情報を管理していた企業等からのみならず、漏洩した個人情報の持ち主である本人からも民事責任を問われる可能性がある。

この他、プライバシー保護に関わる法的問題としては、いわゆるプロバイダー責任制限法との関係などにも注意する必要がある。プロバイダー責任制限法は、ネットワーク上の情報発信に関し、プロバイダーなど(いわゆるISPだけでなく、掲示板などの運営者も該当する可能性がある)の「電気通信役務提供提供者」の責任の限界を規定するものだが、同法には、責任制限の一環として、情報発信者に関する情報の開示に関する規定がある。こうしたIPアドレスなどの発信者情報は、個人情報保護法上の個人情報に該当する可能性が高い。従って、プロバイダー責任制限法に基づく発信者情報の開示を要求された場合、個人情報保護法との関連に留意した上で対処しなければならない。

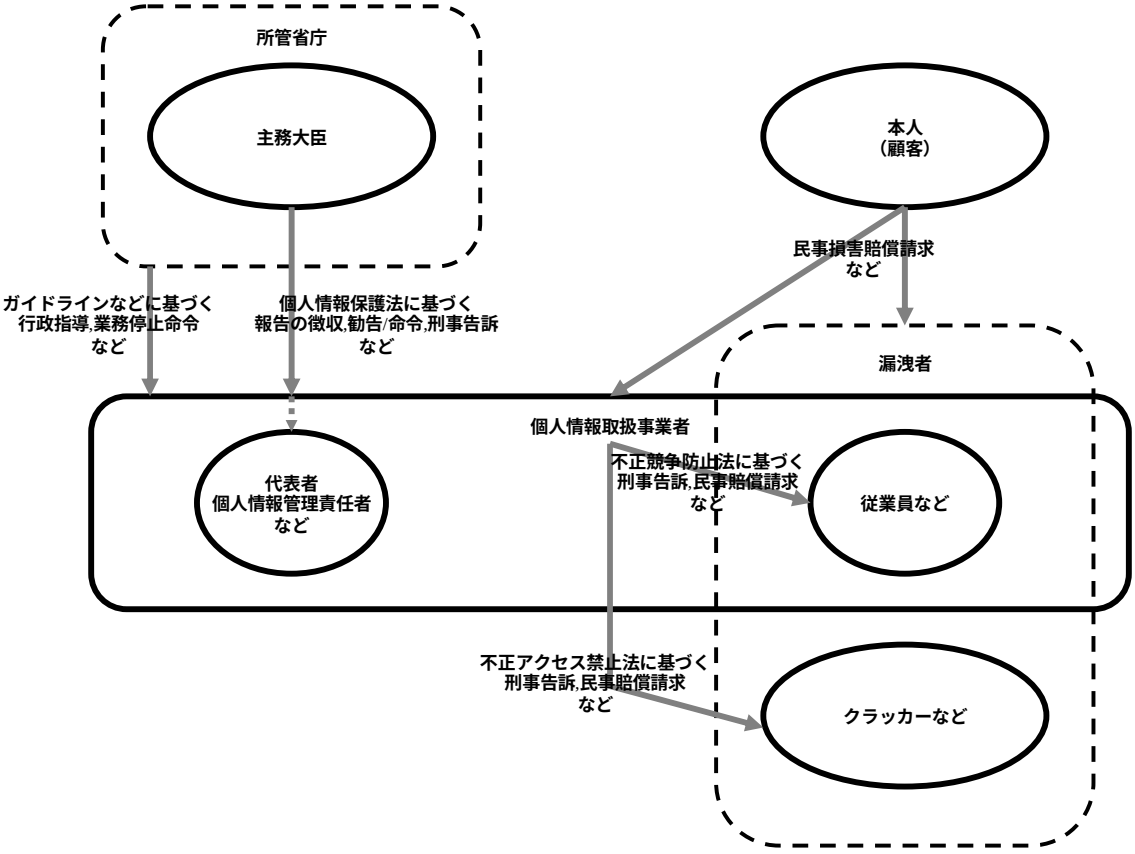


図 3-4 個人情報取扱事業者を取り巻く法的責任

3.8.1 顧客情報と不正競争防止法との関係

属性情報プロバイダーが預かっている顧客情報の不正流出に対し不正競争防止法により保護することができる。保護対象とするためには、それが企業秘密であることを区別して管理してあることがポイントとなる。本節では顧客情報管理にフォーカスして不正競争防止法について説明する。

不正競争防止法は、不正な競争行為を禁止し、公正な競争を維持し健全な経済活動に寄与することを目的として平成 5 年に制定された法律であり、営業上の利益を害される者(だけ)が差し止めや損害賠償請求を行うことにより自らの営業活動を保護する権利を持つことを規定している。

一見、属性情報プロバイダーとは無関係に思われるかもしれないが、平成 15 年 5 月の個人情報保護法成立と時期を同じくして、企業の持つ「営業秘密」を保護するための改正が行われたことで大きな関連を持つようになった。

不正競争防止法は具体的には、以下のような行為を禁止することにより健全な営業活動を維持するものである。

- **混同誤認するような社名、商標、商品名、ドメイン名、商品内容等の禁止**
- **コピー商品の禁止**
- **営業秘密に係る不正行為**
- **コピープロテクトを外す行為の禁止**
- **虚偽に基づく他社毀損**

不正競争防止法でいう「営業秘密」には属性情報プロバイダーの持つ「顧客情報」が含まれるため、個人情報保護法と並んで考慮する必要があるのである。具体的には、営業秘密には以下が含まれる。

- **顧客情報**
- **製造ノウハウ**
- **販売マニュアル**
- **特許出願前の技術データ**
- **事業に必要となる管理された秘密情報**

営業秘密が侵害された場合には、以下の権利を行使することができる。

- **不正流出した営業秘密の利用の差し止め請求**
- **不正取得した営業秘密の廃棄**
- **損害賠償請求**
- **営業上の信用回復措置の請求(＝謝罪広告等)**

属性情報プロバイダーが管理する顧客の個人情報を不正競争防止法によるところの営業秘密とするためには以下を満足する必要がある。

- **事業活動を行っていること**[1]
- **アクセス制限され秘密であることが明らかな事(マル秘、Confidential マーク)**
- **公に知られている情報ではないこと、またこれが区別されていること**
- **事業活動に必要な有用な営業情報であることを示すこと**

機密管理されていないために、営業秘密として認定されなかった判例が出ているので、これに関しては十分注意する必要がある。

[1] 日本の不正競争防止法では営業利益を害される者が保護対象となり、非営利団体では保護されない。元となっているパリ条約ではそのような区別はない。

4．属性情報プロバイダーに求められる法的要件

属性情報プロバイダーはインターネットを通じて、利用者の各種の属性情報を利用者自身や事業者(サービス提供者)に提供するビジネスを実施するため、個人情報取扱事業者に相当する。今後、インターネットを通じて個人情報を取扱うにあたっては、個人情報保護法をはじめとする法規や業界指針(ガイドライン)に沿った運用が求められる。

本章では、属性情報プロバイダーを設立するにあたり個人情報取扱事業者として必要となる、あるいはあるのが望ましいと思われる業務的、システム的な機能やその課題を OECD8 原則の項に沿って整理する。

(以下、業務的に必要な機能の場合は［■業務機能］、システム的に必要な機能の場合は［■システム機能］というように表す。)

(1) 目的明確化の原則、利用制限の原則

個人情報保護法では関連条項として、15 条(利用目的の特定)、16 条(利用目的の制限)、23 条(第三者提供の制限)がある。

これらの条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア)E ビジネスサービスサイトにおける利用者属性の利用目的確認機能

■業務機能　□システム機能

利用者の属性を送信する先となる事業者(サービス提供者)について、当該ビジネスで必要とされる利用者属性の種類やその使用目的、管理方法等を事前に調整し、契約等により適切に運用されるようにする。

イ)利用目的通知機能

■業務機能　■システム機能

属性情報プロバイダー自身、また提携する個々の事業者(E ビジネスサービスサイト)が、利用者のどの種類の属性をどういう目的で利用するのか、利用者に通知する。また、利用者が必要時に随時システムを通じて確認できるようにする。

ウ)利用同意確認機能

□業務機能　■システム機能

属性情報プロバイダーから事業者(E ビジネスサービスサイト)に送信する属性について、その種類や条件を利用者に確認し、同意をとりつける。

エ)利用制限機能

□業務機能　■システム機能

利用者から同意が得られた部分(属性の種類、送信先)にのみ必要な情報を事業者(E ビジネ

スサービスサイト)に送信し、他の属性や第三者への転送を防ぐようにする。

(2) 収集制限の原則

個人情報保護法では関連条項として、17 条(適正な取得)がある。

この条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア) 属性収集(登録)方法確認機能

■業務機能　■システム機能

属性情報プロバイダーに登録する方法や手順、またその属性の値が真正であることを証明するための方法を明確化し、利用者に通知する。また、利用者が自らの属性を確認する機能の中に各属性の登録日時や場所に関する情報を照会できるようにする。

(3) データ内容の原則

個人情報保護法では関連条項として、19 条(データ内容の正確性の確保)がある。

この条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア) 登録属性正確度確認機能

□業務機能　■システム機能

利用者が登録した各属性についてその値の正確性(真正性)のレベルを他者に示せるようにする。具体的には、自己申告の値か、第三者が確認した値か、公的な証明書に記載されている値か、など。

イ) 登録データメンテナンス機能

□業務機能　■システム機能

属性の種類ごとに登録時点からの有効期間を設け、登録データが最新であるようにする。合わせて有効期限が近づいた場合、そのデータを更新するように利用者に通知(督促)する、期限が過ぎた場合に失効にする、などの機能ももたせる。

(4) 安全保護の原則

個人情報保護法では関連条項として、20 条(安全管理措置)、21 条(従業者の監督)、22 条(委託先の監督)がある。

これらの条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア) 個人情報保護に関する十分な安全管理機能

■業務機能　■システム機能

各省庁から公表されている個人情報保護のガイドライン等に示されている組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置について業務上もシステム上も最高水準の措置を実施し、必要に応じて利用者に状況を開示する必要がある。

イ) 取引相手監査・監視機能

■業務機能　□システム機能

属性情報プロバイダーの連携先の事業者(E ビジネスサービスサイト)が実施すべき安全措置について、定期的な監査やネットワーク監視により問題がないか確認する。また、問題判明の際は、改善の勧告や提携の停止等の措置を行なう。

(5) 公開の原則、個人参加の原則

個人情報保護法では関連条項として、18 条(取得に際しての利用目的の通知等)、24 条(保有個人データに関する事項の公表等)、25 条(開示)、26 条(訂正等)、27 条(利用停止)がある。

これらの条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア) 登録属性照会・更新機能

□業務機能　■システム機能

利用者が属性情報プロバイダーに登録した自らの情報を簡単に確認できる機能。また必要に応じて、各属性や提供先に関する情報をメンテナンス(追加、変更、削除)できるようにする。

イ) 登録属性利用停止機能

■業務機能　■システム機能

利用者が属性利用停止要求に応じて、属性情報プロバイダーに登録した特定の属性に関する情報の提携先への送信を停止する、また既に転送している分について提携先での利用を止める(また無効化する)。

(6) 責任の原則

個人情報保護法では関連条項として、31 条(個人情報取扱事業者による苦情の処理)がある。

この条項に示された要件を満たすためには属性情報プロバイダーには下記のような機能があるのが望ましい。

ア) 苦情(問合せ)対応機能

■業務機能　□システム機能

利用者からの苦情や問合せについて応対し、適切に回答を行う機能。対面や電話、またインターネットを通じた問合せにも応じられるようにする。

以上の検討結果と 2003 年度報告書の検討結果である機能要件との関係を表 4-1 と表 4-2 に示す。表 4-2 は本年度の検討で新たに登場した機能である。

表 4-1 2003 年度報告書掲載機能と本年度検機能の比較

機能名	内容	実行場面	2004 年度検討対象
①属性登録条件提示	その機関で登録できる属性について、種類、信用性レベル(法的証拠能力)、有効期間、その時点で提携しているレイヤー2、レイヤー3 の機関、サイト等を利用者に予め提示す	(常時)	―
②属性真正確	利用者が登録しようとする属性について、その真正レベル(度合い)をチェックする。機関や属性の種類により異なるが、確認には以下のような手段がある。 ・直接対面 ・公的証明書(役所、病院等) ・第三者による証明(保証) ・(自己申告)	・利用者の属性の登録 ・申込時	―
③属性システム登録	確認した属性を情報システムに登録し、保存する。属性の証明者や確認手段も一緒に記録される。	・利用者の属性の登録 ・申込時	―
④属性送信	連携しているレイヤー2 の属性集約機関に新規に登録または更新された属性値、また失効情報を安全に送信する。 登録時にリアル社会の証明書等を受取っている場合は、郵送等により配送する	連携先のレイヤー2 機関と定めたタイミング	―
①更新属性受信・集約・管理	レイヤー1 の各登録機関から送信された利用者の更新された属性値(ディジタルおよび証明書現物)を受信し、利用者ごとに属性を集約し、安全に管理する。	連携先のレイヤー1 機関と定めたタイミング	4(4)ア　個人情報保護に関する十分な安全管理機能
② 属性加工･2 次属性生成	集約した属性を各種 E-ビジネスで取扱いやすい形式に変換、編集する。(以下例) ・○月×日時点で△地区在住で 18 歳以上なら○○投票の資格資格有 ・大学卒で○○資格を所有していれば、○○試験の 1 次試験は免除	・属性データ更新時 ・ビジネス要求実装時	―
③登録属性照会	登録されている利用者自身の属性を照会(表示、送信)する。	利用者の照会要求時	4(5)ア　登録属性照会・更新機能
④提供属性範囲、管理方法提示・提携先審査	レイヤー3 の E ビジネスサイト、企業に対し、提供できる利用者属性の種類や範囲、受信やその後の管理の方針、方式等を提示する。希望するサイトについて事前審査および定期的な監査を実施する	・サービス内容更新時 ･E ビジネス側からの利用申込時	4(1)ア　E ビジネスサービスサイトにおける利用者属性の利用目的確認機能 4(4)イ　取引相手監査・監視機能
⑤属性状況通知	有効期限の迫った属性について利用者に警告を行う、また失効したことを通知する	・各属性の有効期限時 ・特定のビジネスイベント時	4(3)イ　登録データメンテナンス機能

⑥属性送信	利用者の特定の属性を依頼先の E-ビジネスサイトへ安全に送信する。	連携先のレイヤー3 機関を通して利用者属性の提供依頼が適正と判断した時	―
⑦属性利用アプリケーション提供	E-ビジネスサイトが暗号化された利用者属性データを持つ場合などに、アプリケーションを提供する。	E ビジネスサイト、企業との連携契約時、サービス更新時	―
⑧属性送信許可証発行	属性登録者の要望により、特定の属性項目の公開を許可する「許可証」を属性登録者向けに発行し、送信する。	登録者からの要求時	―
⑨属性送信依頼証確認	レイヤー3のEビジネスサイトから送信された登録者の属性送信依頼証が真正であることや有効期限等の諸条件を確認する	連携先のレイヤー3 機関を通して利用者属性の提供依頼を受けとった時	―

表 4-2 本年度検討の新たな機能

(1) イ　利用目的通知機能
ウ　利用同意確認機能
エ　利用制限機能
(2) ア　属性収集(登録)方法確認機能
(3) ア　登録属性正確度確認機能
(5) イ　登録属性利用停止機能
(6) ア　苦情(問合せ)対応機能

5. Liberty Alliance Project

本章は属性情報プロバイダーを実現する技術の一つとしてLibertyを取り上げ、その属性情報交換の仕組みについて説明する。

Liberty は利用者のプライバシー保護を重視したアイデンティティ(利用者の識別情報。以下、ID と記述)連携、属性情報の連携を可能とする仕組みであり、主に以下のような特徴をもっている。

- **ID 連携や属性情報の連携は常に利用者の同意の元で行われる**
- **ID や属性情報を特定の事業者に一極集中させるのでなく分散管理を可能にするため、利用者はプライバシーやセキュリティのリスクを軽減することができる**
- **ID 連携時には統一された利用者 ID ではなく各事業者間では仮名が使用されるため、利用者の追跡などのプライバシー問題を防ぐことができる**
- **Web サービスをベースとしたオープンな仕様である**

これらの特徴は、異なる事業者間で利用者の属性情報を連携する属性情報プロバイダーで不可欠な機能である。

5.1 Liberty Alliance Project について

Liberty Alliance Project(以下 Liberty あるいは Liberty Alliance と省略することもある)は、幅広い分野の企業／組織からなる団体で、消費者と企業がプライバシーとセキュリティを保ちながら電子商取引に参加できる世界の実現を目的としている。具体的には、消費者のアイデンティティ情報の取り扱いについて、セキュリティとプライバシーを考慮したオープンな仕様を提供することで、異なるオンラインサービス間の連携を可能にする。これにより、安全かつシームレスな電子商取引体験が実現されることになる。

Liberty がこうした活動を始めた背景には、まず、個々のオンラインサービスがそれぞれ独自に顧客である消費者の情報を取り扱っているという現状がある。こうした状況下では、消費者にとっては、サービスごとに個人情報を入力し認証を受けなければならないという問題や、サービスごとにセキュリティやプライバシーの水準がまちまちで安心して個人情報を預けられないという問題がある。またオンラインサービスの提供者にとっても、自社／他社を問わず複数のサービスを動的に組み合わせてより魅力的なサービスを提供したり、サービスを効率化したりすることが難しいという問題がある。

これらの問題を解決する方法の一つとして、かつての.NET Passport のような、単一の統合された認証／個人情報管理センターを利用するモデルが考えられる。しかしこの方法では、センターが単一の攻撃対象となるため、ひとたびセキュリティが破られたときの被害が大きくなりすぎ、リスク管理の面からは必ずしもいいことばかりではない。また各オンラインサービスの提供者にとっては、顧客との関係構築／維持を完全にセンターに依存することになり、自律性の維持や独自性の確立が困難になる。さらに消費者にとっても、センターのプライバシー／セキュリティ水準が満足のいくものであるかどうかに関わらず、いやおうなく個人情報を該センターに預けなければならず、選択の機会が奪われるという問題がある。

そこでLibertyでは、上述したようなさまざまな問題を解決するために、各オンラインサービスが、顧客の認証結果や属性情報を、顧客である消費者の意志に基づいて相互に流通することを可能にするというアプローチを採用した。これにより、消費者は自らの選択に基づいて個人情報を預ける先を選べるとともに、認証結果や属性情報がどのように流通されるかを制御しながら、複数のサービスをシームレスに連携させて利用することが可能になる。

一方でLibertyは、トラストサークル(Circle of Trust)という概念を提示し、オンラインサービスを提供する企業の側にも選択の機会を提供している。トラストサークルは、顧客の認証結果や属性情報の流通の範囲を、企業間のビジネス上の合意に基づき定めるものである。すなわち、基本的に、認証結果／個人情報はトラストサークルの外には流通せず(注：認証結果をトラストサークル間で流通するIdP introductionという仕様も規定されているが、これもトラストサークル間での契約が前提になっている)、消費者の選択と制御はトラストサークル内に閉じて機能するということになる。これにより、サービス提供企業は、例えば自社の顧客情報がライバル企業に流通するということを防ぐことが可能になる。一方でトラストサークルは、契約に基づいて一定水準のセキュリティ／プライバシー保護を参加企業に強制することもできるので、消費者にも信頼性の判断が容易になるというメリットをもたらす。

これまで述べてきたような機能を実現するため、Libertyの仕様では、これまで2つの開発フェーズを経て、以下のような事項を規定している。

Phase1では、サービス提供者間で認証結果を流通することにより、顧客アイデンティティの連携とシングルサインオンを実現する、アイデンティティ連携フレームワーク(ID-FF)仕様を定めている。ID-FFについては、ECOM 2003年度報告書「SAML利用検討報告書」[26]に記述されているので参照されたい。

Phase2では、まず、アイデンティティに基づくWebサービスの構築／管理のためのプラットフォームとして、サービス提供者間でリソース(例えば消費者の属性情報など)を可能にする枠組みであるID-WSF(Identity Web Service Framework)仕様を定めている。さらにPhase2では、ID-WSFの上で動作するサービスのインターフェイス仕様(ID-SIS)として、個人情報を扱うID-SIS-PP(Personal Profile)仕様と、被雇用者情報を扱うID-SIS-EP(Employee Profile)仕様を定めている。

さらにLibertyでは今後の活動計画であるPhase 3で、ID-SISとして位置情報サービスやプレゼンスサービスなどを追加し、アイデンティティに基づくWebサービスのバリエーションを増やしていく予定である。

図 5-1は各仕様の関係を記述したものである。ID-SISはID-WSFに依存した仕様である。ID-FFと、ID-WSFおよびID-SISの2つは独立した仕様であり、それぞれ単独で実装することも可能である。

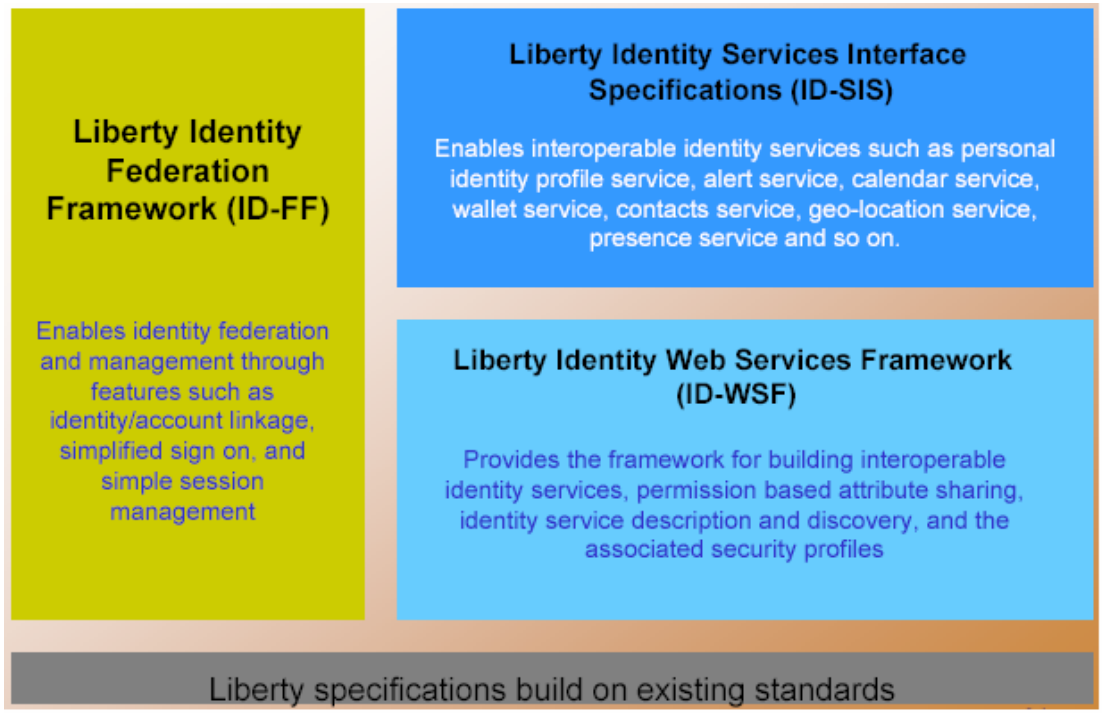


図 5-1 Liberty 仕様構成

(引用元：Liberty Alliance Developer Tutorial)

5.2 Liberty サービスモデル

5.2.1 Liberty のサービス要素

Liberty は機能毎に分かれた複数のサービス要素が互いに協調することで ID 連携や属性情報の提供／取得の機構を実現している。Liberty ID-FF、ID-WSF で登場するサービス要素のイメージを図 5-2 に、各サービス要素の役割を表 5-1 に示す。

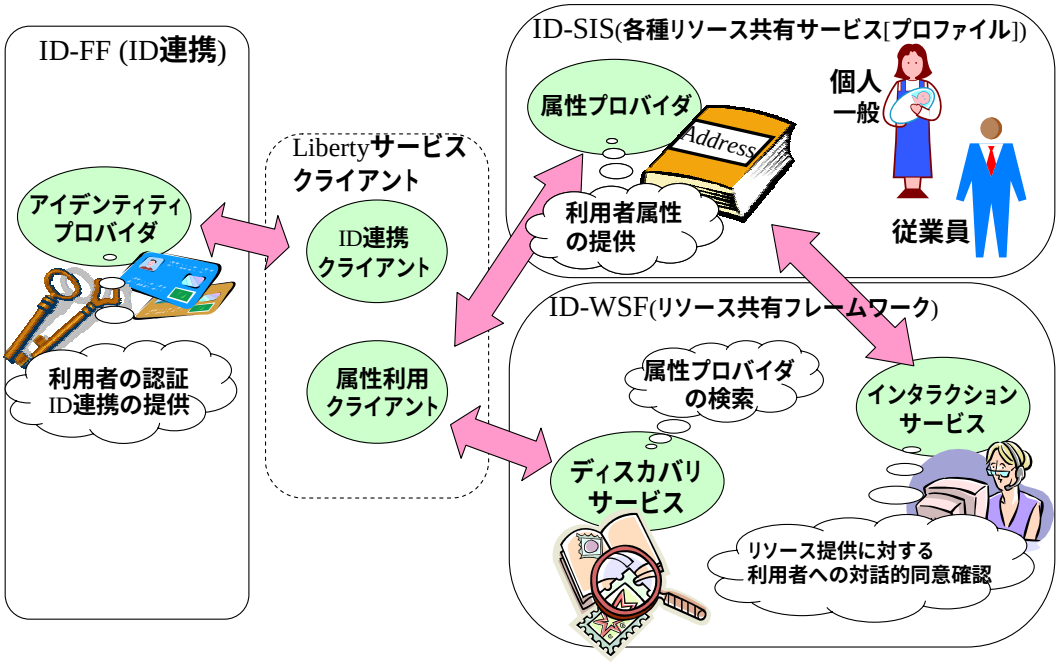


図 5-2 Liberty サービス要素のイメージ

表 5-1 Liberty サービス要素の役割

フレームワーク仕様	サービス要素	役割
ID-FF	アイデンティティプロバイダ (IdP：Identity Provider)	利用者のアイデンティティ情報を管理し、利用者の認証を行う。認証を行った結果を示す認証アサーションをSPに与え、ID連携を実現する。
	ID連携クライアント	IdPや他のID連携クライアントとID連携を行いシングルサインオン等を実現する。
ID-WSF	属性利用クライアント	APより利用者の属性情報を取得するクライアント。
	ディスカバリサービス (DS：Discovery Service)	WSCが必要としているリソースを持つWSPの検索を行うサービス。主にIdPを行う事業者が提供するサービスである。
	インタラクションサービス[2] (IS：Interaction Service)	WSPがWSCへリソースを提供する際、そのリソースの所有者に同意確認を行うサービス。 同意確認はWSPが行う方法や、外部サービスであるISが代行して行う方法がある。
ID-SIS	属性情報プロバイダー (AP：Attribute Provider)	利用者の属性情報を管理し、利用者の合意の下で属性情報を属性利用クライアントへ提供する。利用者の合意を得るために、外部のISを利用することもできる。

ID-FFの解説でサービスプロバイダ(SP)という用語がよく使われるが、本報告書では混乱を避けるためにこの用語を使用せず、代わりにID連携クライアントと呼ぶことにする。また、ID-WSFではWSP(Web Service Provider)やWSC(Web Service Consumer)という用語が登場する。これらはWebサービス上の役割を表すもので、サービスを提供する側をWSP、サービスを受ける側をWSCと呼ぶものである。ID-WSFは利用者の属性情報やサービスに関するフレームワークであり、具体的なサービスを定義しているものではない。実際に属性連携等に使用するためには、ID-WSF上で稼動するプロトコルやスキーマを設計する必要がある。このプロトコルやスキーマがID-SIS仕様であり、現在は個人情報を扱うPersonal Profile(ID-SIS-PP)や従業員情報を扱うEmployee Profile(ID-SIS-EP)が公開されている。また、独自に取り決めたプロトコルやスキーマ(つまり独

[2] 最近ではROI(Resource Owner Interaction)と呼ばれている

自の ID-SIS 仕様)を用いて実装することも可能である。本報告書では ID-WSF に合わせて利用者の属性情報に関する ID-SIS(例えば ID-SIS-PP)を実装した WSP を属性情報プロバイダ(AP)と呼び、その AP を利用するクライアントを属性利用クライアントと呼ぶことにする。ID-SIS-PP/EP については 5.2.5 節で紹介する。

各サービス要素と本報告書で扱う属性情報プロバイダーとの関係については 6 章で説明する。

図 5-3 はサービス要素と Liberty の仕様文書との関係を記したものであり、図中における文書の名称は表 5-2 で示した略記を用いている。

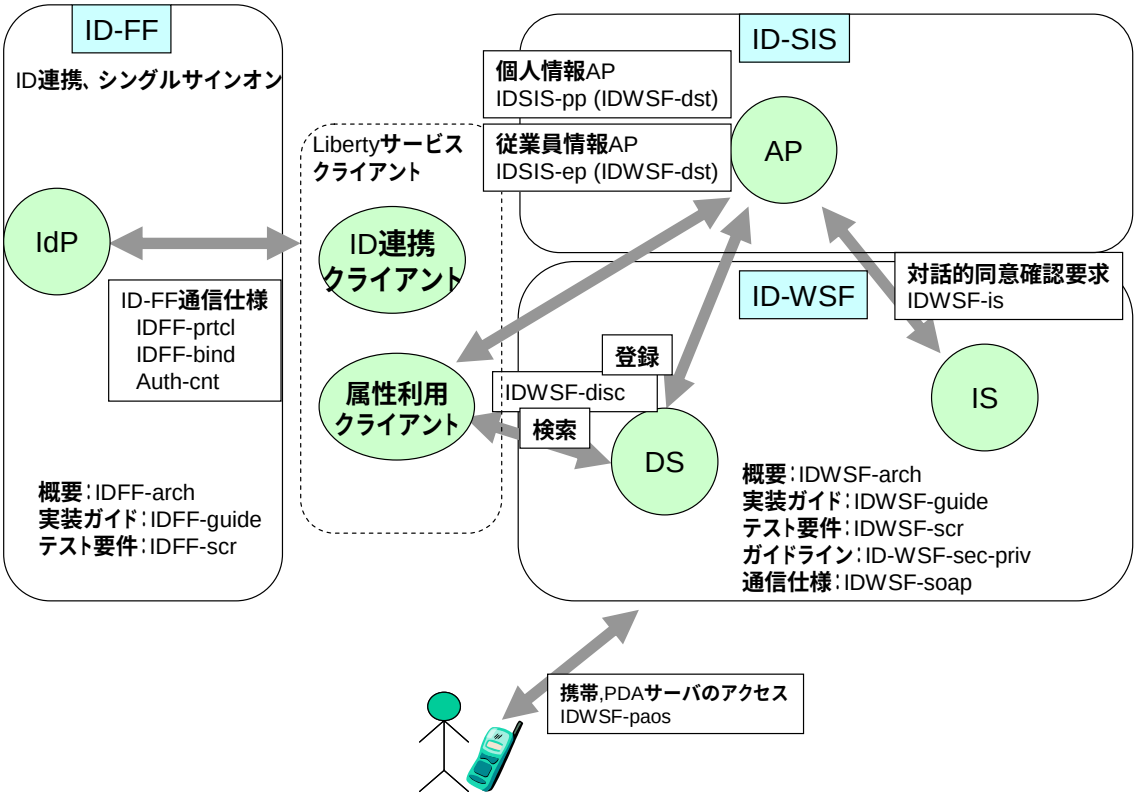


図 5-3 サービス要素と仕様文書の関係

表 5-2 Liberty 仕様文書一覧

略記	文書名 [ ]内は参考文献の表記
IDFF-arch	Liberty ID-FF Architecture Overview[2]
IDFF-bind	Liberty ID-FF Bindings and Profiles Specification[3]
IDFF-prtcl	Liberty ID-FF Protocols and Schema Specification[4]
IDFF-guide	ID-FF Implementation Guidelines[5]
IDFF-scr	Liberty ID-FF Static Conformance Requirements[6]
Auth-cnt	Liberty ID-FF Authentication Context Specification[7]
Metadata	Liberty Metadata Description and Discovery Specification[8]
IDWSF-sec-priv	Liberty ID-WSF Security and Privacy Overview[9]
IDWSF-disc	Liberty ID-WSF Discovery Service Specification[10]
IDWSF-soap	Liberty ID-WSF SOAP Binding Specification[11]
IDWSF-sec-mech	Liberty ID-WSF Security Mechanisms[12]
IDWSF-is	Liberty ID-WSF Interaction Service Specification[13]
IDWSF-dst	Liberty ID-WSF Data Services Template Specification[14]
IDWSF-arch	Liberty ID-WSF Architecture Overview[15]
IDWSF-client	Liberty ID-WSF Client Profiles Specification[16]
IDWSF-auth	Liberty ID-WSF Authentication Service Specification[17]
IDWSF-guide	Liberty ID-WSF Implementation Guide[18]
IDWSF-scr	Liberty ID-WSF 1.0 Static Conformance Requirements[19]
IDWSF-paos	Liberty Reverse HTTP Binding for SOAP Specification[20]
IDSIS-pp	Liberty ID-SIS Personal Profile Service Specification[21]
IDSIS-ep	Liberty ID-SIS Employee Profile Service Specification[22]

5.2.2 ID-FF を用いた ID 連携・シングルサインオン

本節では ID-FF による ID 連携およびシングルサインオンのシーケンスの概要を述べる。

IdP と ID 連携クライアントによる ID 連携の手続きのイメージを図 5-4 に示す。図 5-4 の各シーケンスの説明を以下に示す。

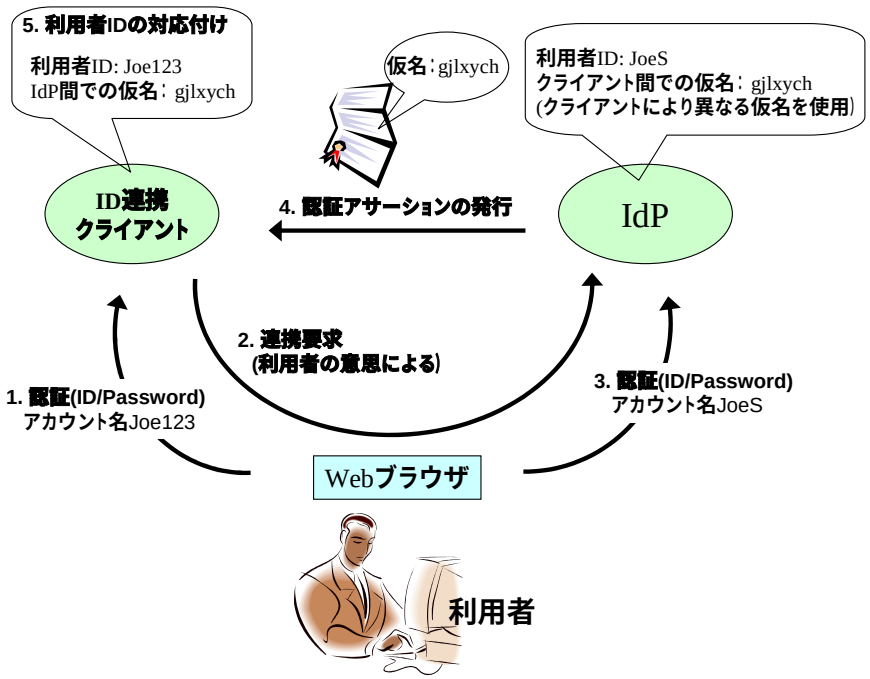


図 5-4 ID-FF による ID 連携

- **利用者は ID 連携クライアントで認証を受ける。認証は ID 連携クライアントが管理する利用者のアカウントにより行う。**
- **利用者は ID 連携を要求し、ID 連携クライアントは IdP に対し ID 連携のリクエストを送信する。**
- **利用者は IdP で認証を受ける。認証は IdP が持つ利用者のアカウントにより行う。**
- **IdP は利用者を認証した後、利用者に ID 連携クライアントとの間で使用される仮名(ランダムの文字列)を付け、ID 連携クライアントへ認証アサーション(認証したことの証)と共に送信する。**
- **ID 連携クライアントは IdP が発行した認証アサーションを受け、自身が持つ利用者のアカウントと IdP が生成した仮名の対応付けを行う。**

上記の手続きは ID 連携を行う ID 連携クライアント毎に行われ、プライバシー保護のため、IdP が発行する利用者の仮名はそれぞれの ID 連携クライアントで異なる文字列を使用する。

認証アサーションの送信の方法には、HTTP の POST メソッドにより利用者経由で送信する方法(POST Profile)や、アーティファクトを用いる方法(Artifact Profile)がある。アーティファクトは認証アサーション問い合わせに用いられる比較的サイズの小さなメッセージであり、ID 連携クライアントはこのアーティファクトを受信した後、再度 IdP に認証アサーションを問い合わせる。このアーティファクトによるアサーション送信方法は HTTP リクエストのメッセージサイズに制限のある利用者端末の環境(携帯電話など)で有効な方法である。

ID 連携の手続きを行った後、利用者はシングルサインオンが可能となる。シングルサインオンのイメージを図 5-5 に示し、図 5-5 の各シーケンスを以下に述べる。

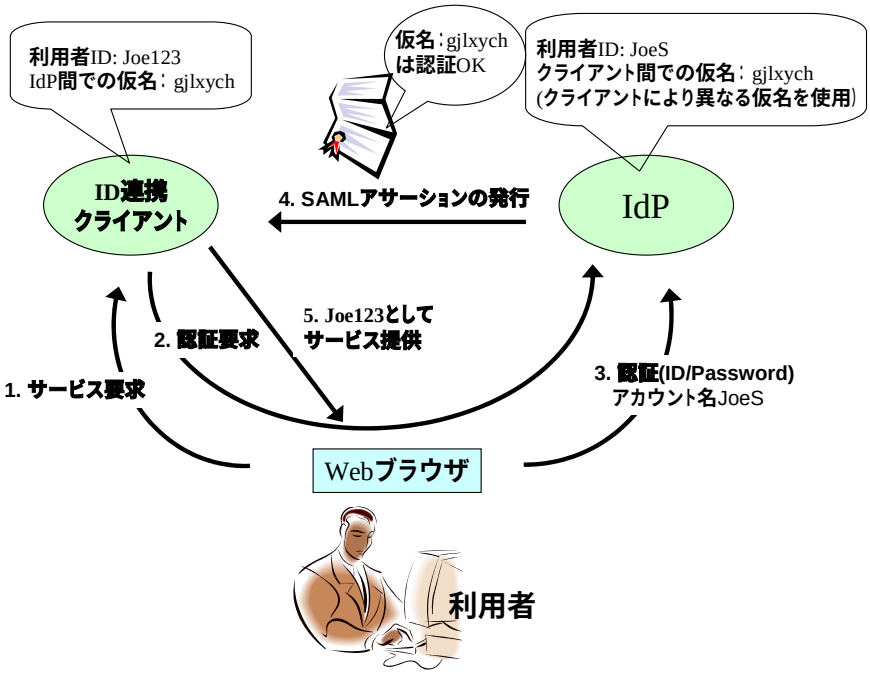


図 5-5 ID-FF による SSO

- **利用者は ID 連携クライアントへ接続する。**
- **利用者はまだ認証を受けていないため、ID 連携クライアントは IdP へ利用者をリダイレクションし、認証を要求する。**
- **利用者は IdP で認証を受ける。認証は IdP が持つ利用者のアカウントにより行う。**
- **IdP は ID 連携のプロセスで決定された利用者の仮名を含めた認証アサーションを発行し ID 連携クライアントへ送信する。ID 連携手続きで述べたように、認証アサーションの送信方法には POST やアーティファクトの方法がある。**
- **ID 連携クライアントは IdP より発行された認証アサーションを得て、自身が持つ利用者のアカウントとして認証されたものと判断する。**

他の ID 連携クライアントが認証を要求したときは上の手順と同様に行うが、IdP は一度、利用者の認証が済んだ後は認証アサーションを発行するのみとなる。

ID-FF は利用者の認証方式自体は定義していないため、事業に応じて様々な認証方式を採用することができる。

5.2.3 ID-WSF/ID-SIS を用いた属性連携

ID-WSF は利用者のリソース情報を扱うためのフレームワークであり、サービス仕様である

ID-SIS と共に実装することで、属性情報連携等を実現することができる。本節では ID-WSF/ID-SIS のメカニズムの概要を説明する。ID-SIS としては利用者の属性情報の提供・取得を行うサービスを実現するものとする。

属性情報を実際に利用する場面を想定した場合、以下の動作シーケンスに分けることができる。

- **AP への利用者の属性登録**
- **DS への AP 登録**
- **属性利用クライアントによる AP の発見**
- **属性利用クライアントによる属性要求と AP による属性提供(利用者の同意確認)**
- **属性情報を利用したサービス提供**

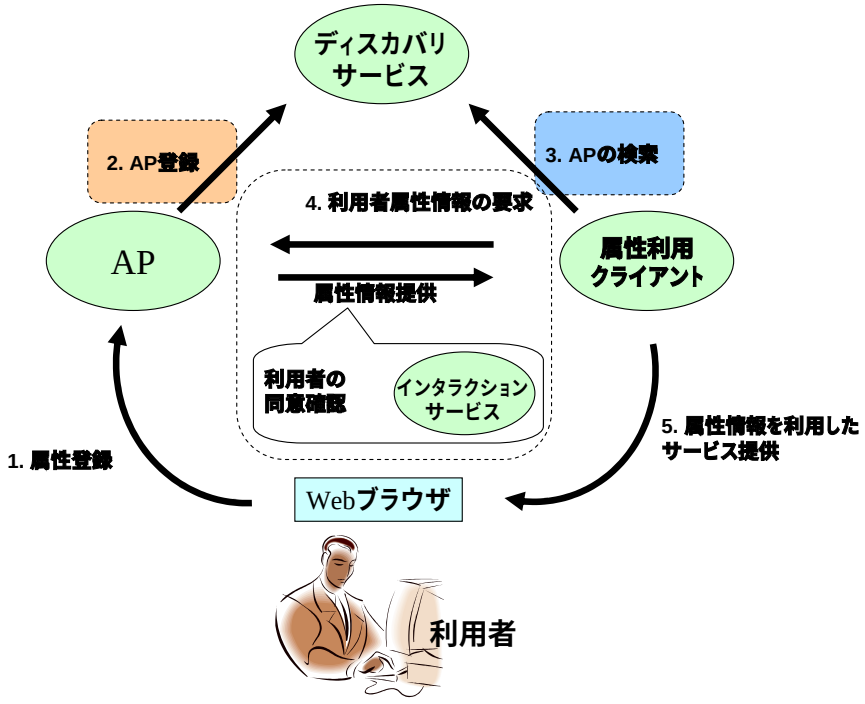


図 5-6 ID-WSF/ID-SIS 動作シーケンス

各シーケンスを図 5-6 に示している。図 5-6 の点線で囲んだ部分が Liberty で規定されているものである。各シーケンスの動作は次のようになる。

- **1.AP への利用者の属性登録**

利用者の属性登録の方法については Liberty では規定してない。それぞれ独自の方法で実装する必要がある。AP となる属性情報プロバイダーはその業務の形態により属性登録方法は異なるだろう。例えば、利用者の対面により登録したり、あるいは、Web の入力フォームなどのオンライン上で行うことが考えられる。

- **2.DS への AP 登録**

多数の AP が存在するとき、属性利用クライアントが問い合わせるべき AP を知ることができるように DS を置くことができる。AP は属性利用クライアントが DS から発見できるように、事前に DS へ必要な情報を登録しなければならない。

DS へ登録する情報は属性問い合わせのための接続先(サービスのエンドポイント)や利用者の ID が含まれている。利用者の ID はプライバシーを保護するため、AP を行う事業者が事業に用いている利用者の ID を直接用いるのではなく、属性問い合わせのために使用される仮名が用いられる。

- **3.属性利用クライアントによる AP の発見**

属性利用クライアントが必要とする利用者の属性情報について、どの AP へ問い合わせるべきか知らない場合には、DS へ AP 検索の要求を行う。

DS は検索結果として、AP のエンドポイントなど属性要求に必要な情報を返却する。

- **4.属性利用クライアントによる属性要求と AP による属性提供**

属性利用クライアントは DS から得られた情報を元に AP へ利用者の属性情報を要求する。

AP はこの要求に対して利用者へ属性提供に対する意思を確認する。

利用者の意思確認については、大きく分けて次の 2 種類が考えられる。

・属性利用クライアントへの属性提供に対して事前同意を得る

・属性利用クライアントへの属性要求の度に同意を得る

前者のケースは、利用者は属性利用クライアントへの属性提供に対し全面的な同意を行う場合で、AP は主にその同意確認を「2.DS への AP 登録」の段階で行う。

後者のケースでは、このリソース提供の段階において利用者の同意確認を行う。

どのように同意確認するかについては Liberty では規定していない。それぞれ独自に実装する必要がある。

また、AP 自身が同意確認を行う場合以外にも、属性利用クライアントが行うケースや同意確認を代行する外部サービスである IS を利用するケースもありえる。これらの同意確認のモデルについては 5.2.4 節で述べている。

AP は利用者からの同意が得られていることが確認した後、属性利用クライアントへ要求されたリソースを返却する。

- **5.属性情報を利用したサービス提供**

属性利用クライアントとなる事業者は AP より取得した属性情報を元にサービスを提供する。

5.2.4　リソース提供に関わる利用者同意確認方法

Liberty では、利用者の選択と制御に基づく属性情報の提供を実現するため、2 種類の方法を提供している。一つは、予め利用者が設定したポリシーに基づき属性情報リクエストを評価する方法、もう一つは、属性情報リクエストを受けた時点で逐次利用者の意向を確認する方法である。

前者のポリシー評価を実現するための仕組みとして、Liberty ID-WSF SOAP Binding Specification[11]では用途指示子 Usage Directives が用意されている。属性情報を要求する属性利用クライアントは、要求している属性情報をどのように使うかという意向を、属性情報リクエスト内に用途指示子として記述する。リクエストを受け取った AP は、その用途指示子を、利用者が予め設定したポリシーに基づいて評価し、提供の諾否を決定する。

用途指示子や利用者ポリシーの記述言語については、現在の Liberty 仕様では標準を特に定めないとされているため、Liberty サービスの実装者は、トラストサークル Circle of Trust ごとに定められた任意の記述言語を利用することになる。但し、将来的には、記述言語の参照仕様または標準仕様を定める方向で、現在仕様策定作業が進行中である。

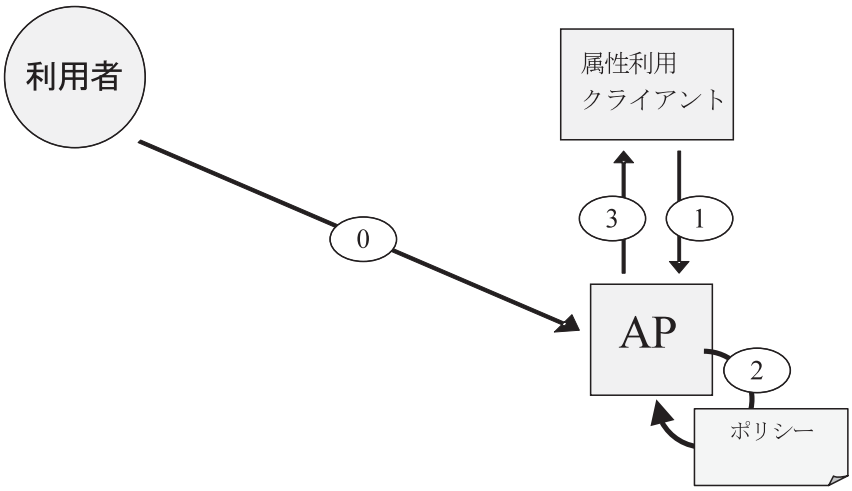


図 5-7 AP が事前に同意を確認する方式

一方、後者の逐次確認を実現するための仕組みとして、Liberty 仕様ではインタラクションサービス(IS：InteractionService) [13]を用意している。IS における利用者同意確認方法として、利用者のクライアントとしてウェブブラウザーが用いられる場合(＝通信プロトコルとして HTTP のみを利用する場合)について 2 通り(a,b)、ブラウザー以外のクライアントが利用可能な場合(＝通信プロトコルとして HTTP 以外が利用可能な場合)について 1 通り(c)の、計 3 つのパターンが示されている。

- **(a) AP が直接利用者と対話して同意を確認する方式**

HTTP-redirection を用いて利用者のブラウザーを AP のサイトに誘導し、AP-利用者間で直接対話して同意確認を行う方式である(図 5-8)。以下にシーケンスを示す。

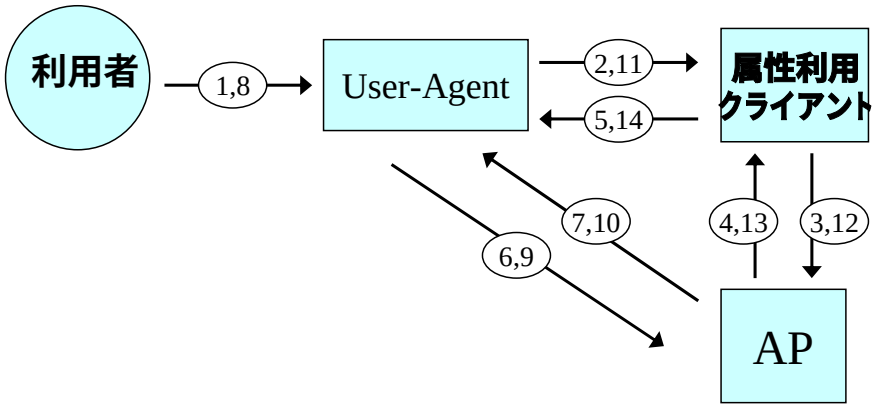


図 5-8 AP 直接の同意確認

1．利用者は User Agent(Web ブラウザなど)を操作する。
2．属性利用クライアントとなる事業者のコンテンツを要求する。
3．属性利用クライアントは AP へ利用者の属性情報を要求する。
4．AP はリダイレクション要求を含む SOAP Fault を返却する。
5．リダイレクション要求で指定された AP のページへリダイレクション
6．AP の同意確認ページを要求する。
7．AP は同意確認ページを提示する。
8．利用者は同意確認ページの質問事項に答える。
9．利用者の回答を送信する。
10．戻り先として指定された属性利用クライアントのページへリダイレクション
11．属性利用クライアントのページを要求する。
12．属性利用クライアントは AP への属性要求メッセージを再送する。
13．AP は属性利用クライアントの要求に対し応答する。
14．利用者から同意が得られた場合には属性情報を提供する。

- **(b) AP が属性利用クライアントを経由して利用者の同意を確認する方式**

AP が属性利用クライアントに利用者の同意を求めるよう指示し、属性利用クライアントはその指示に基づいて利用者と対話、同意確認の結果を AP に返す方式である。この方式では、属性情報の要求元である属性利用クライアントが同意確認の中継者となるため、属性利用クライアントに(同意確認結果を偽らない)高い信頼性が求められる(図 5-9)。以下にシーケンスを示す。

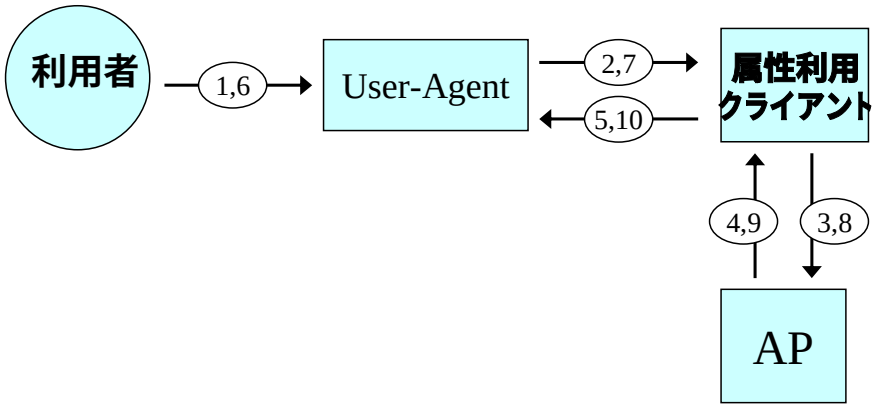


図 5-9 WSC 経由の同意確認

1. 利用者は User Agent(Web ブラウザなど)を操作する。
2. 属性利用クライアントとなる事業者のコンテンツを要求する。
3. 属性利用クライアントは AP へ利用者の属性情報を要求する。
4. AP は利用者への同意確認を要求するメッセージを属性利用クライアントに返却する。
5. 属性利用クライアントは利用者へ同意確認ページを提示する。
6. 利用者は同意確認ページの質問事項に答える。
7. 利用者の回答を送信する。
8. 属性利用クライアントは利用者への同意確認の結果を示すメッセージを AP に送信する(手順 4 に対する応答)
9. AP は利用者から同意が得られた場合には属性利用クライアントへ属性情報を提供する。
10. 属性利用クライアントは利用者へコンテンツを提供する。

- **(c) AP が外部サービスである IS を経由して利用者の同意を確認する方式**

AP が外部サービスである IS に利用者の同意確認を依頼し、IS が利用者となんらかの方法で対話して同意確認を行い、その結果を AP に通知する。対話方法は Liberty 仕様の範囲外で、例えばインスタントメッセージや WAP Push など、インタラクティブなものであればなんでもよい。AP は ROI サービスの発見に DS を利用することもできる。この方式では、AP-IS 間と利用者-IS 間に信頼関係が必要になる。

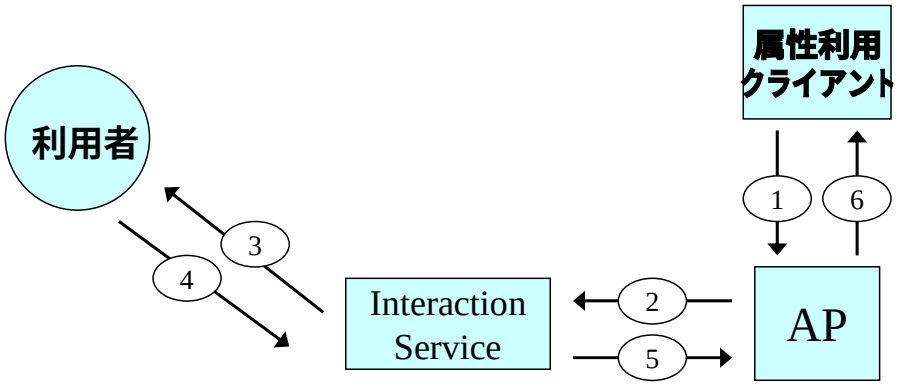


図 5-10 外部 IS 経由の同意確認

1．属性利用クライアントは AP へ利用者の属性情報を要求する。
2．属性利用クライアントは IS へ利用者への同意確認を要求する。
3．IS は利用者へ同意を求める。
4．利用者は IS の同意要求に対して返答する。
5．IS は利用者の回答を含んだメッセージを AP に返却する。(手順 2 に対する応答)
6．AP は利用者から同意が得られた場合には属性利用クライアントへ属性情報を提供する。

以上、3 つの同意確認モデルを示した。事業の形態に応じて、適した同意確認のメカニズムを選択することができる。また、事前設定ポリシーによる同意確認と、IS による逐次同意確認は、排他的なものではない。例えば、まず利用者ポリシーを評価し、その結果リクエストの許可／拒否が確定した場合はそれに従って処理し、それ以外の場合(利用者が IS を行うようポリシーに記述している場合や、ポリシーに記述されていないリクエストが来た場合など)は IS による同意確認を行うというような、組み合わせての利用も可能である。

5.2.5 ID-SIS-PP/EP

Liberty Phase2 では ID－WSF に基づくプロファイルとして ID-SIS Personal Profile (ID-SIS-PP)と ID-SIS Employee Profile(ID-SIS-EP)を定めている。ID-SIS-PP は一般的な個人情報を取り扱うためのスキーマを定めており、一方の ID-SIS-EP は従業員の情報を取り扱うためのスキーマである。ID-SIS-PP で定めている主な属性情報を表 5-3 に示す。これら以外の属性を新たに定義して使用することも可能である。これらのプロファイルに従った属性情報プロバイダーを運営することもできる。あるいは、これらのプロファイルとは異なる独自に取り決めたスキーマや操作のプロトコルによって運用することも可能である。

表 5-3 ID-SIS-PP の主な属性情報

属性	内容
InformalName	個人のログインネーム(screen name)
CommonName	個人の呼称
LegalIdentity	個人の法的な ID
EmploymentIdentity	職業上の ID 情報
AddressCard	住所
MsgContact	連絡先(電話、e-mail など)
Facade	個人の外観情報(顔、音声など)
Demographics	言語、年齢、性別、タイムゾーンなど
SignKey	署名検証用の公開鍵(証明書)
EncryptKey	暗号用の公開鍵(証明書)
EmergencyContact	緊急連絡先

ID-SIS-PP/EP の特徴のひとつとして国際化対応が挙げられ、例えば、属性情報に非アスキー文字を使用可能にする XML 要素(たとえば、住所を表す LPostalAddress など)や、日本語で使用されるふりがなを表記可能な script 属性などが定義されている。

属性情報の具体例として AddressCard の一例を以下に示す。

AddrType の指定により居住地(domicile)を表している。他の AddrType には仕事先の work や帰省先の home などがあり、異なる意味をもつ“住所”を表現することができる。

ID-SIS-PP が定める属性情報の一例(住所／居住地)

```
<AddressCard> <AddrType>urn:liberty:id-sis-pp:addrType:work</AddrType>
<Address>
<PostalAddress>Shiba-Kouen 99999</PostalAddress>
<LPostalAddress>芝公園 99999</LPostalAddress>
<LPostalAddress script="kana">しばこうえん 99999</LPostalAddress>
<PostalCode>105-9999</PostalCode> <L>Mitato-ku</L> <LL script>港区</LL>
<LL script="kana">みなとく</LL>
<St>Tokyo</St>
<LSt>東京都</LSt>
<LSt script="kana">とうきょうと</LSt>
<C>jp</C>
</Address>
<Nick>Taro Work</Nick>
<LNick>太郎職場</LNick>
</AddressCard>
```

5.3 Liberty のプライバシー保護に関する取り組み

Liberty Alliance ではプライバシーを極めて重視しており、そのプライバシー／セキュリティに関する見解／指針を示す文書『Privacy and Security Best Practices(プライバシーとセキュリティの最善慣行)』を公開している。

本節ではまず、同文書を読み解く上で必要な、Liberty で用いられるプライバシー関連の用語／概念について簡単に説明する。

Liberty では、個人情報保護法の「本人」に相当する概念を表す言葉として「主体者(principal)」が使われる。この主体者という言葉は、法律用語でいうところの「自然人」や、IT 分野で使われる「ユーザ」の同義語としても、しばしば用いられる。本報告書では主体者＝「ユーザ」「利用者」として扱う。

一方、個人情報保護法の「個人情報」に近い概念を表す言葉については、Liberty では「属性(attribute)」「個人識別情報(PII：Personally Identifiable Information)」の二つがある。前者は、主体者＝利用者の特性(characteristics)」を意味する。個人情報保護法のように「個人を特定可能」という条件は付されていないため、より広い概念と考えるのが適当だろう。後者は、特定の個人を識別したり位置を示したりするデータを意味する。こちらは、個人情報保護法のように「組み合わせて特定可能な場合を含む」という条件が付されていないため、より狭い範囲を表す定義と考えられる。場合によっては、こうした違いを意識する必要があるかもしれないが、ほとんどの場合、「個人情報」と「属性」「個人識別情報」を峻別する必要はないと考えられるため、本報告書ではこれらを同等なものとして扱う。

また Liberty ではしばしばアイデンティティ(identity)やネットワークアイデンティティ(network identity)という言葉が用いられるが、これらは、ある一人のユーザに関する属性＝個人情報の集合という意味で用いられる。例えば、John Smith 氏は「仕事用アイデンティティ」「プライベート用アイデンティティ」を持ち、仕事用アイデンティティには「職場の電話番号」「会社のメールアドレス」などの属性で構成され、プライベート用アイデンティティには「自宅の電話番号」「私有の携帯電話のメールアドレス」などの属性で構成される、というイメージである。このような概念は個人情報保護法には存在しないが、Liberty の文書を読む上では知っておくと役に立つであろう。

先に紹介した文書『プライバシーとセキュリティの最善慣行』では、プライバシー保護法制に関する各国／地域の動向の概要を紹介するとともに、それらを参考に作成された「Liberty Alliance Privacy Recommendations(Liberty プライバシー勧告)」(表 5-4)を、本節で述べた用語／概念を用いて示している。

表 5-4 Liberty プライバシー勧告

① Notice：利用者(＝主体者)への告知	誰が何の情報をどのようにして集めるかを告知する。選択、アクセス、セキュリティ、関連性、適時性を提供する方法について告知する。情報の取得元、情報の配布先を告知する
② Choice：個人情報の流れの選択	利用者は何の情報が集められ、その情報が提供された目的を超えてどのように使われるかを選択できる。利用者は過去の同意や棄却を、後になって参照、検証、更新することができる。
③ Principal Access to Personal Identifiable Information：個人情報へのアクセス	サービス提供者は関連法規に準じ、要求を満足するように個人情報を管理する。利用者が、自身の個人情報へアクセスするわかりやすい手段を提供する。
④ Quality：個人情報の品質保持	サービス提供者は、利用者に対し保持している個人情報の修正のためのわかりやすい手段を提供しなければならない。
⑤ Relevance：個人情報の利用目的の一致	サービス提供者は個人情報が収集された目的、もしくは利用者が同意した目的のためにのみ個人情報を利用しなければならない。
⑥ Timeliness：個人情報の利用可能期限	サービス提供者は利用者に対し、個人情報の必要期間のみ、もしくは、利用者が認めた期間のみ個人情報を保持しなければならない。
⑦ Complaint Resolution：苦情処理	サービス提供者は利用者に対し、利用者の個人情報が誤った利用をされていると感じた場合に申し立てできる苦情処理の仕組みを提供しなければならない。
⑧ Security：個人情報保持のセキュリティ	サービス提供者は、管理する個人情報を適切なセキュリティレベルで保護し、提供するための手順を取らなければならない。

この勧告で挙げられた 8 つの項目は、Liberty 仕様の設計や Liberty サービスの運用の上で守るべき指針と位置付けられている。特にユーザの「選択」に基づく許可は Liberty のビジョンの中枢であり、Liberty 仕様ではこれを可能にするためのさまざまなツールを提供している。

6．Liberty を用いた属性情報プロバイダー

6.1　属性情報プロバイダーと Liberty サービス要素の関係

ここでは本報告書の定める属性情報プロバイダーと Liberty ID-FF、ID-WSF/ID-SIS の各サービス要素の関係について述べる。属性情報プロバイダーやサービス事業者の実装方法は事業形態に依存して決まるものであり、さまざまなモデルが存在しうる。以下のモデルは Liberty の実装方法を規定するものではなく、あくまで代表的な例として与えるものである。したがって、これとは異なる方法で、Liberty 仕様を利用した属性情報プロバイダーを実装することも可能である。

属性情報プロバイダーに主として関係するのは ID-WSF/ID-SIS である。本書のモデルでは、属性情報プロバイダーの機能は、ID-SIS の PP(Personal Profile)サービスとして実現される。

また、Liberty の枠組みでは、特定の消費者の特定の属性情報が、どこで(どの属性情報プロバイダーのどの保管場所で)提供されているかを検索するために、ID-WSF の DS(Discorvery Service)が必要になる。属性情報プロバイダーではこのような機能は陽に定義されていないが、ここではこれを「本人認証代行事業者」と呼ぶことにする。DS の機能を提供する事業者は、後述する IdP の役割も兼ねることが多いため、本書のモデルでもこの 2 つの役割を同一の事業者が兼ねる構成を取る。「本人認証代行事業者」は、主に IdP の役割に注目した名称である。

このほか、属性情報プロバイダーにおける利用同意確認機能の一端を担うものとして、利用同意の確認を消費者と対話的に行う機能が、ID-WSF の IS(Interaction Service)仕様で定義されている。この機能は単独のサービスとして実装されることもあるが、属性情報プロバイダー自身やサービス事業者自身が同意確認を行うことも可能であり、この場合など独立した事業者は必要ではない。IS を含めた同意確認の方法については 5.2.4 節を参照されたい。

ID-FF と ID-WSF/ID-SIS は独立した仕様であり、ID-WSF/ID-SIS の実装には ID-FF は必ずしも必要ではない。しかし、属性情報プロバイダーやサービス事業者を運用する際、属性情報の登録／修正／確認や利用者同意の取得などのプロセスにおいては利用者の認証が必要になる。こうしたプロセスは複数のプレイヤーが連携する中で実施されることが多いが、各プレイヤーごとに利用者認証が発生するのはあまり実用的とはいえない。このような理由から、以下のモデルでは属性情報プロバイダーによる属性提供は ID 連携の仕組みの上で実施されることを想定している。

ID 連携を行う場合、IdP の役割を果たす事業者が必要である。IdP は属性情報プロバイダーやサービス事業者に ID 連携の機能を提供する。またシングルサインオンを行う際、利用者は IdP の認証を受ける。本書のモデルでは、IdP を担う事業者は、後述する ID-WSF の DS の役割も兼ねる構成をとっている。

表 6-1 Liberty サービス要素と事業者の関係

事業者	Liberty サービス要素	必要性
属性情報プロバイダー	ID 連携クライアント(ID-FF)	ID 連携を行う場合に必要
	AP(ID-WSF/ID-SIS)	属性情報プロバイダーの基本となる機能として必要
サービス事業者	ID 連携クライアント(ID-FF)	ID 連携を行う場合に必要
	属性利用クライアント(ID-WSF)	サービス事業者の基本となる機能として必要
本人認証代行事業者	IdP(ID-FF)	ID 連携を行う場合に必要
	DS(ID-WSF)	属性情報プロバイダー検索サービスを行う場合に必要

6.2 個人情報保護

個人情報保護法では 15 条～36 条において個人情報取扱事業者の様々な義務を示しており、本報告書第 4 章では、これに基づき属性情報プロバイダーに求められる要件を示した。本節では、Liberty の属性情報プロバイダーを実装・運用する際、個人情報保護法上考慮すべき点を、第 4 章で示した要件に基づき明らかにする。

6.2.1 要件(1) 目的明確化の原則、利用制限の原則

関連条文：15 条(利用目的の特定)、16 条(利用目的の制限)、23 条(第三者提供の制限)

機能：(ア) E ビジネスサービスサイトにおける利用者属性の利用目的確認機能
利用者の属性を提供する属性情報プロバイダ(AP)は、提供先であるサービスプロバイダ(SP)に対し使用目的や管理方法などを事前に調整し契約する必要がある。

関連する Liberty プライバシー勧告：Relevance
Liberty では、属性の利用目的を指定する方法として、SP や AP の属性要求／応答メッセージにおいて用途指示子(Usage Directives)を定義している。ここに属性の利用ポリシーを記述することで、サービスクライアントからの利用目的の通知や、利用者からの利用目的の指定が可能になる。

留意点：属性利用ポリシーの記述／処理方法は、現時点では Liberty 仕様では規定していないため、実装／運用にあたっては各事業者間やトラストサークル内でそれらを規定する必要がある。但し将来の Liberty 仕様では、利用ポリシーに関し何らかの仕様が提示される可能性がある。

機能：(イ) 利用目的通知機能
属性情報プロバイダー自身や提携する事業者が属性の利用目的を利用者へ通知する。

関連する Liberty プライバシー勧告：Notice

留意点：(ア)に同じ

機能：(ウ) 利用同意確認機能
属性情報プロバイダーは他のサービスプロバイダへ提供しようとする属性の種類や利用目的、条件を利用者に確認し同意をとりつける。

関連する Liberty プライバシー勧告：Notice、Choice
Liberty における属性共有は利用者の同意に基づいて行われる。同意の確認については、事前に利用者が設定した属性利用ポリシーのみを用い自動的に行う方法と、利用者と通信し対話的に行う方法がある。後者を実現する方法として、Liberty ではインタラクションサービス仕様を提供している。

留意点：属性利用ポリシーを用い自動的に判定する場合、(ア)に同じ

機能：(エ) 利用制限機能
利用者が許可した属性情報のみが、許可した提供先にのみ送信される。

関連する Liberty プライバシー勧告：Choice
Liberty では、属性情報プロバイダーのテンプレートを提供する IDWSF-dst 仕様において、複数リソースの同時取得要求の取扱いについて、リソース所有者＝利用者の許可が確認できたもののみを返送するよう定めている。従って、正しく実装された属性情報プロバイダーであれば、左記の利用制限機能を満たすと考えられる。

留意点：複数リソースの同時取得要求の取扱いについては、リソース所有者の許可以外にも影響を与える要員がいくつかある。詳しくは IDWSF-dst 仕様を参照のこと。

6.2.2 要件(2) 収集制限の原則

関連条文：17 条(適正な取得)

機能：(ア) 属性収集(登録)方法確認機能
属性情報プロバイダーに属性を登録する方法や手段を明確化し利用者へ通知する。

関連する Liberty プライバシー勧告：なし

留意点：Liberty では属性を登録する手段についての仕様は規定されていない。属性情報プロバイダーやトラストサークルで独自に定める必要がある。

6.2.3 要件(3) データ内容の原則

関連条文：19 条(データ内容の正確性の確保)

機能：(ア)登録属性正確度確認機能
利用者が登録した属性の正確性(自己申告の値か、第三者が確認した値か、公的な証明書に記載されている値かなど)を他者に示せるようにする。

関連する Liberty プライバシー勧告：Quality
Liberty では、IDWSF-dst 仕様において、属性収集コンテクスト(ACC:Attribute Collenction Context)をオプショナルな仕様として定めている。属性収集コンテクストの定義済の値としては、“ urn:liberty:dst:acc:unknown ”(有効性を確認できないあるいは自己申告)、“urn:liberty:dst:acc:incentive”(ユーザに正しい値を入力するよう何らかのインセンティブを提供)、“ urn:liberty:dst:acc:challenge ”(なんらかの検証メカニズムで有効性を確認)、“urn:liberty:dst:acc:secondarydocuments”(二次文書に基づき有効性を確認(例:電子請求書から取得した住所))、“urn:liberty:dst:acc:primarydocuments”(一次文書に基づき有効性を確認(例:パスポートから取得した住所))などがある。属性収集時に、収集方法に応じてこれらの値を属性収集コンテクストに格納しておけば、その属性の品質を測る目安として利用できる。

留意点：属性収集コンテクストはオプショナルな仕様であるため、全ての Liberty 実装がサポートしているとは限らない。
上記の定義済の値以外にも、独自に属性収集コンテクストの値を拡張して定義することは可能である。

機能：(イ) 登録データメンテナンス機能
属性の登録時点からの有効期間を設け、登録データが最新であるようにする。有効期限が近い場合に利用者へ

更新を促したり、期限経過後は失効にする。

関連する Liberty プライバシー勧告：Timeliness、Quality
Liberty には、属性に有効期限期限を設けたり、失効が近い属性の更新を利用者に促すというような、左記の機能を直接対応する機能はない。しかし、これらを実現するために必要な機能として、IDWSF-dst 仕様において、属性の変更日時を modificationTime でサポートするとともに、これを用いて要求対象の属性をフィルタリングするための仕様として、changedSince/notChangedSince を設けている。

留意点：modificationTime や changedSince/notChangedSince は必須仕様ではないため、全ての Liberty 実装がサポートしているとは限らない。
失効が近い属性の更新を利用者に促す機能はないが、そのベースとなるものとして、登録した利用者に通知を行う subscription/notification 機能の採用が phase3 で検討されている。

6.2.4 要件(4) 安全保護の原則

関連条文：20 条(安全管理措置)、21 条(従業者の監督)、22 条(委託先の監督)

機能：(ア) 個人情報保護に関する十分な安全管理機能
組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置について業務上もシステム上も最高水準の措置を実施し、必要に応じて利用者に状況を開示する必要がある。

関連する Liberty プライバシー勧告：Security
Liberty ではセキュリティを重視しており、さまざまな仕様の中でセキュリティを高めるツールやセキュリティ水準を示す規範を定義している。しかし、それらはあくまで左記の「技術的安全管理措置」の範囲に留まるものであり、また Liberty サービスが動作するプラットフォームのセキュリティの向上は保証していない。

留意点：個人情報管理における組織的安全管理措置、人的安全管理措置、物理的安全管理措置については、本来的に技術でカバーできるものではないため、Liberty 仕様の採用／不採用に関わらず、別途対策を講じる必要がある。また技術的安全管理措置についても、Liberty 仕様を採用すれば完全になるという性質のものではないため、プラットフォームまで含めたより広い範囲の対策が必要である。

機能：(イ) 取引相手監査・監視機能
属性情報プロバイダーの連携先の事業者が実施すべき安全措置について、定期的な監査やネットワーク監視により問題がないか確認する。また、問題判明の際は、改善の勧告や提携の停止等の措置を行なう。

関連する Liberty プライバシー勧告：なし
Liberty のプライバシー勧告では提携先の事業者に対する監督の指針はない。

留意点：左記の機能を実現するためには、事業者間が互いに正しく運用されていることを監督するための規約を、事業者間あるいはトラストサークルで規定する必要がある。

6.2.5 要件(5) 公開の原則、個人参加の原則

関連条文：18 条(取得に際しての利用目的の通知等)、24 条(保有個人データに関する事項の公表等)、25 条(開示)、26 条(訂正等)、27 条(利用停止)

機能：(ア) 登録属性紹介・更新機能
利用者が属性情報プロバイダーに登録した自らの情報を簡単に確認でき、各属性や提供先に関する情報をメンテナンスできるようにする。

関連する Liberty プライバシー勧告：Principal Access to PII、Quality

Liberty 仕様では、属性情報プロバイダーに登録した属性情報の提示方法や修正方法については規定していない。

留意点：左記の機能を実現するためには、属性情報プロバイダーやトラストサークルで独自に規定し、実装・運用する必要がある。

機能：(イ) 登録属性利用停止機能
利用者の属性利用停止要求に応じて、属性情報プロバイダーに登録した特定の属性に関する情報の提携先への送信を停止する、また既に転送している分について提携先での利用を止める(また無効化する)。

関連する Liberty プライバシー勧告：Principal Access to PII、Quality
Liberty では、属性利用停止要求に直接対応する機能は仕様化されていない。しかし、属性情報のディスカバリサービスへの登録を削除することにより、これと同等の機能が実現可能である。既に転送済の属性情報の、提携先での利用停止／無効化を実現する機能は、Liberty では提供されていない。

留意点：転送済属性情報の利用停止／無効化については、トラストサークルや事業者間の取り決めを通じて独自に実現する必要がある。

6.2.6 要件(6) 責任の原則

関連条文：31 条(個人情報取扱事業者による苦情の処理)

機能：(ア) 苦情(問い合わせ)対応機能
利用者からの苦情や問合せについて応対し、適切に回答を行う機能。対面や電話、またインターネットを通じた問合せにも応じられるようにする。

関連する Liberty プライバシー勧告：Complaint Resolution:
Liberty 仕様では、苦情処理や紛争解決の方法については規定していない。

留意点：左記の機能は、トラストサークルや事業者間、あるいは属性情報プロバイダーにおいて、独自に規定を作成し、実装・運用を行う必要がある。

6.3 ユースケース

本節では、Liberty を用いた属性情報プロバイダーのユースケースについて述べる。このユースケースでは利用者の認証に ID-FF による ID 連携を行うものとする。

6.3.1 登場するサイト

ユースケースでは以下の 3 つのサイト(表 6-1 の事業者)登場する。

(1) ポータルサイト(本人認証代行事業者に相当)
(2) 旅行代理店サイト(サービス事業者かつ属性情報プロバイダー)
(3) レンタカーサービスサイト(サービス事業者)

上記 3 つのサイトでトラストサークルを形成している。(1)のポータルサイトは、ユーザの認証を行う IdP として振る舞う。また DS もホストする。(2)の旅行代理店サイトは、ユーザが出張する際の宿泊及び航空券等の手配を行う。またユーザの同意に基づき、他のサイトへ属性情報を

提供する AP として振る舞う。そして(3)のレンタカーサービスサイトは、出張先でのレンタカーの手配をする。手配に必要な情報は、ユーザの属性情報として旅行代理店サイトから取得する。

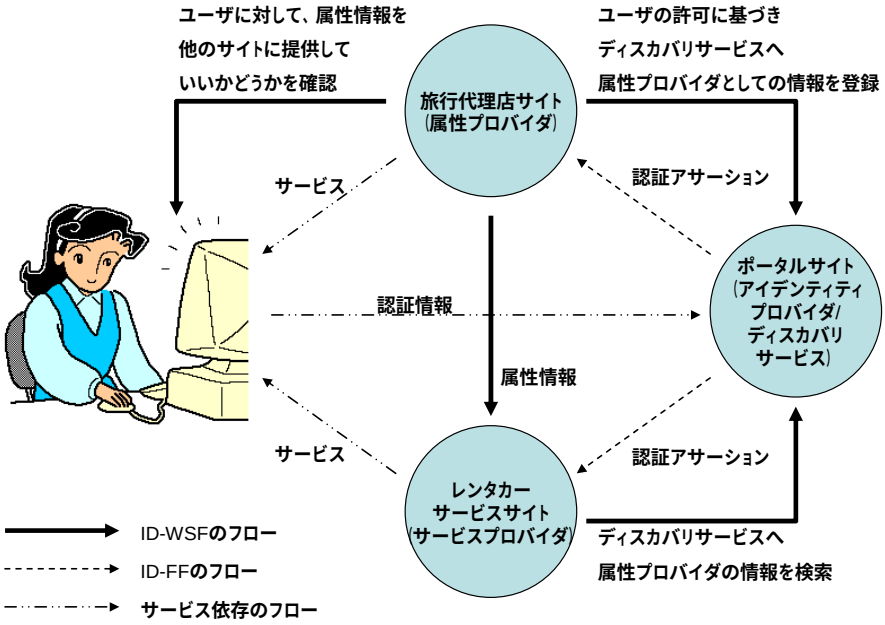


図 6-1 ユースケースに登場するサイトの役割と関係

また本ユースケースは、ユーザは Web ブラウザーから各サイトへアクセスすることを前提とする。

本ユースケースは、ユーザが出張する際に、その手配を旅行代理店サイトとレンタカーサービスサイトで行うものである。

6.3.2 トラストサークルへのシングルサインオン

ユーザはトラストサークルにシングルサインオンするために、IdP であるポータルサイトに認証される必要がある。認証方法は Liberty ID-FF では規定されていない。本ガイドラインでも認証方法の詳細については述べない。

一度 IdP に認証されると、IdP は要求に基づき、他のサイト(本ユースケースでは旅行代理店サイトとレンタカーサービスサイト)に対して、ユーザが認証済みであることを示す認証アサーションを発行する。他のサイトは認証アサーションを検証することにより、ユーザが認証済みであることを確かめる。従ってユーザは、認証情報を各サイトに提出する必要はない。

6.3.3 旅行代理店サイトへのアクセス

ユーザはトラストサークルにシングルサインオンしているため、旅行代理店サイトには認証情報を送信する必要はない。旅行代理店サイトにおいてユーザは、出張の日程や出張先の情報を提出し、宿泊先、航空券等の手配を行う。いつも利用する旅行代理店サイトであるため、ユーザの

氏名、支払いのための情報、そして好みの航空会社といった情報は、ユーザの属性情報として、本サイトに既に登録されている。

旅行代理店サイトにおける手続きを終了すると、ユーザには図 6-2 のような画面が表示されるかもしれない。図 6-2 では、ユーザ及びこの出張に関する属性情報を、旅行代理店サイトが、同じトラストサークル内の別のサイトに提供してもよいかどうかをユーザに確認している。

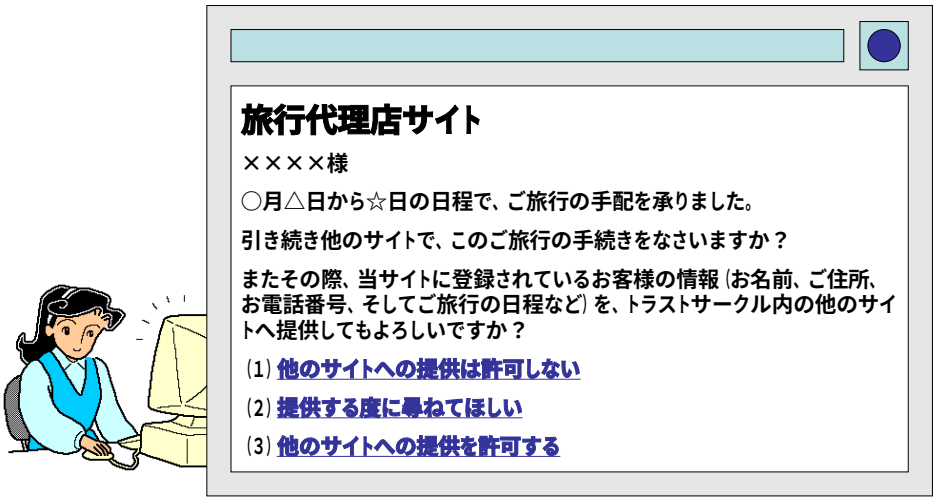


図 6-2 ユーザの属性情報を他のサイトと共有していいかどうかを確認する画面

図 6-2 では、ユーザに 3 つの選択肢を用意している。

「(1)の他のサイトへの提供は許可しない」をユーザが選択した場合、属性情報は他のサイト(プロバイダー)といっさい共有されない。

「(2)の提供するたびに尋ねて欲しい」をユーザが選択した場合、旅行代理店サイトは、他のサイトから属性情報の提供要求を受けるたびに、提供していいかどうかをユーザに確認する。ユーザに尋ねる部分には、Liberty ID-WSF Interaction Service 仕様[13]が利用される。

「(3)の他のサイトへの提供を許可する」をユーザが選択した場合、旅行代理店サイトは、他のサイトから属性情報の提供要求を受けると、ユーザに確認することなく要求元サイトへ属性情報を提供する。

「(2)」の場合も「(3)」の場合も、旅行代理店サイトは Liberty ID-WSF Discovery Service Specification[10]に従って、属性情報プロバイダーとしての情報を、ポータルサイトがホストしているディスカバリサービスに登録する。

本ユースケースでは、ユーザは「(2)」の「提供するたびに尋ねて欲しい」を選択したものとする。

6.3.4　レンタカーサービスサイトへのアクセス

ユーザはトラストサークルにシングルサインオンしているため、レンタカーサービスサイトには認証情報を送信する必要はない。レンタカーサービスサイトにおいてユーザは、出張先で借りるレンタカーを予約しようとしている。ユーザには図 6-3 のような画面が表示されるかもしれない。

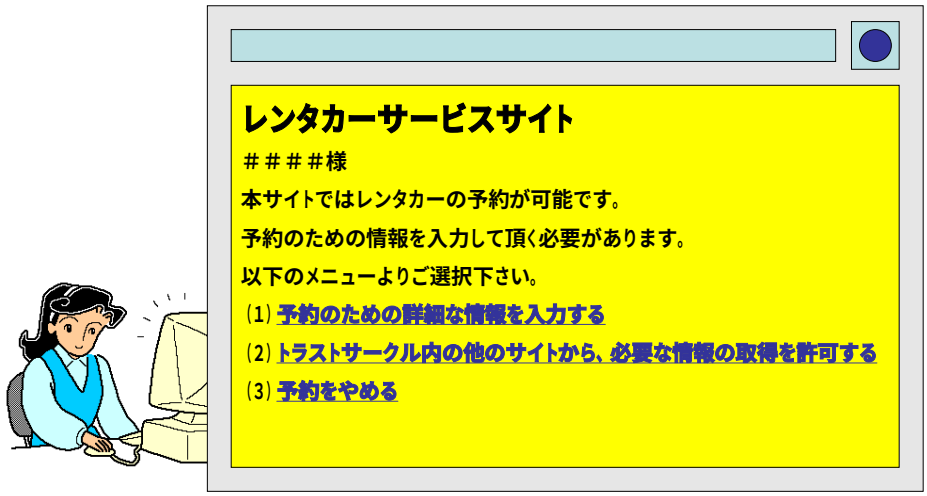


図 6-3 レンタカーサービスサイトでレンタカーを予約する画面

図 6-3 は、ユーザに 3 つの選択肢を用意している。

(1)の「予約のための詳細な情報を入力する」をユーザが選択した場合、ユーザはレンタカーサービスサイトに対して、予約のための情報(氏名や日程等)を入力する必要がある。

(2)の「トラストサークル内の他のサイトから、必要な情報の取得を許可する」をユーザが選択した場合、レンタカーサービスサイトはトラストサークル内の他のサイトから、予約のために必要な出張に関する属性情報を取得しようと試みる。この場合レンタカーサービスサイトは、Liberty ID-WSF Discovery Service [10]に従って、トラストサークル内で関連する属性情報を提供できる属性情報プロバイダーを検索し、検索結果に基づき、属性情報プロバイダーに属性情報を要求する。

(3)の「予約をやめる」をユーザが選択した場合、レンタカーサービスサイトは何もしない。

このユースケースでは、ユーザは(2)の「トラストサークル内の他のサイトから、必要な情報の取得を許可する」を選択したものとする。

6.3.5　属性情報提供のためのユーザとのインタラクション

レンタカーサービスサイトから属性情報の要求を受け付けた旅行代理店サイトは、属性情報をレンタカーサービスサイトへ提供していいかどうかについて、ユーザが設定しているプライバシーポリシーを確認する。このユースケースでは、6.3.3 節において「提供するたびに尋ねて欲しい」とユーザが設定しているため、旅行代理店サイトは、Liberty ID-WSF Interaction Service [13]に従って、ユーザに図 6-4 のような画面を表示する。

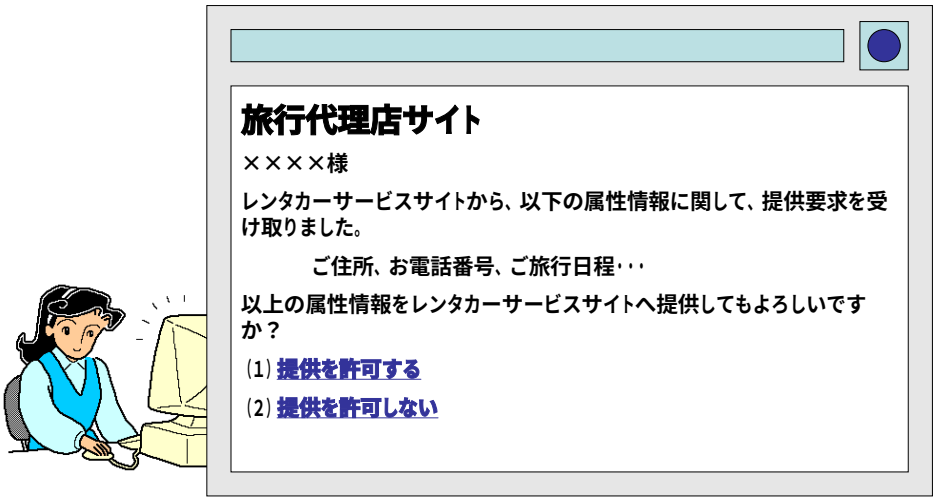


図 6-4 ユーザの属性情報をレンタカーサイトと共有して良いか確認する画面

図 6-4 では、ユーザに 2 つの選択肢を用意している。

(1)の「提供を許可する」をユーザが選択した場合、旅行代理店サイトはレンタカーサービスサイトに対して、要求された属性情報を提供する。

(2)の「提供を許可しない」をユーザが選択した場合、旅行代理店サイトはレンタカーサービスサイトに対して、要求された属性情報を提供しない。

このユースケースでは、ユーザは(1)の「提供を許可する」を選択したものとする。

6.3.6 属性情報の受け取りとサービス提供

レンタカーサービスサイトは、旅行代理店サイトから属性情報を取得し、その情報に基づき、レンタカーの予約手続きを行う。図 6-5 はその確認画面を示している。

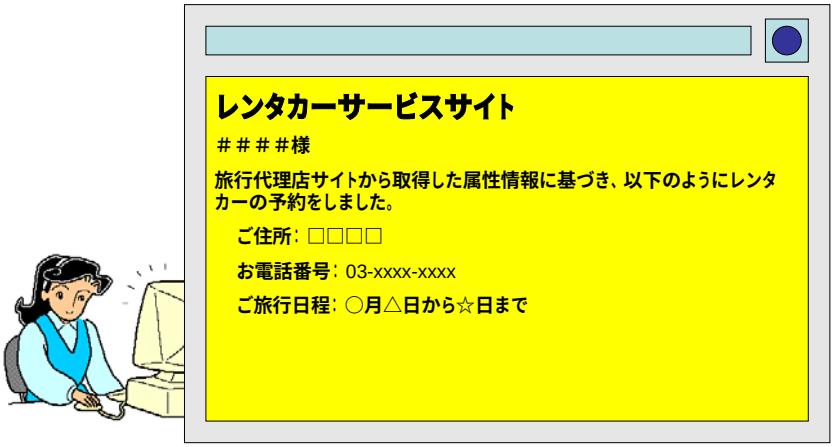


図 6-5 レンタカーサービスサイトでのレンタカー予約確認画面

ユーザは予約のために必要な、詳細な情報をレンタカーサービスサイトへ、直接入力することなく、レンタカーの予約ができたことになる。

なお、このユースケースは理解しやすいように、詳細は省略している。実際には、各サイトにおけるプライバシーポリシーや属性情報の利用意図等に関して、ユーザが承認している必要がある。

6.4 ユースケース詳細

ここでは前節のユースケースを各プロバイダーの視点から眺めた動作フローを記述する。図中のメッセージはLiberty仕様を簡略化したイメージを記載している。

6.4.1 旅行代理店サイトへの接続

ユーザがポータルサイトの認証を済ませ、旅行代理店サイトへの接続が完了するまでの過程。ID-FFに従った手順となる。旅行代理店はID連携クライアント、ポータルサイトはIdPとして機能する(図 6-6)。以下のステップで実行される。ユーザは旅行代理店のサイトへ訪れる。

1．旅行代理店サイトはユーザの認証を必要とするため、ユーザをポータルサイトへ転送する。
2．ポータルサイトはユーザを認証する。
3．ポータルサイトは旅行代理店サイトへ利用者の認証アサーションを発行する。認証アサーションには ID 連携手続きで決定された仮名(abcdef)が含まれている。旅行代理店サイトは認証アサーションを受け、その仮名と旅行代理店サイト自身がもつユーザのID(xxxx)をマッピングし、ユーザへの接続を完了する。

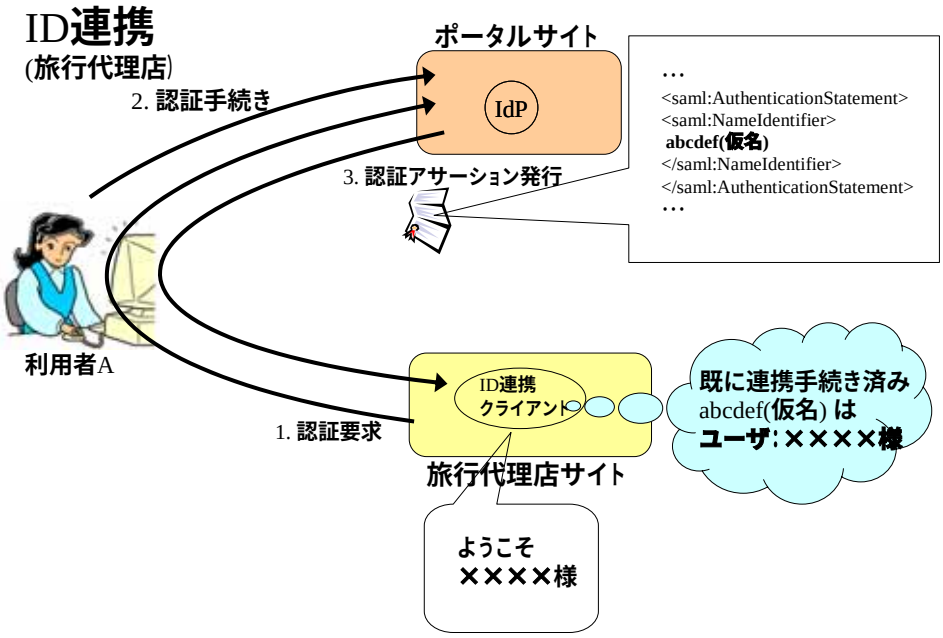


図 6-6 旅行代理店サイトへのログイン

6.4.2　DS(ポータルサイト)への AP(旅行代理店)登録

旅行代理店サイトはユーザに対し、属性情報を他のサイトへ提供するか否かの問い合わせを行う。旅行代理店サイトはユーザより属性情報提供の同意が得られた後、他の属性利用クライアント(この例ではレンタカーサイト)から参照されるように DS(ポータルサイト)へ登録を行う(図 6-7)。登録する情報は、提供するサービス(属性情報を提供するサービスを表す ID など)、属性情報の問合せに必要な情報(サービスのエンドポイント、利用者の仮名など)、提供する属性の種類といったものである。

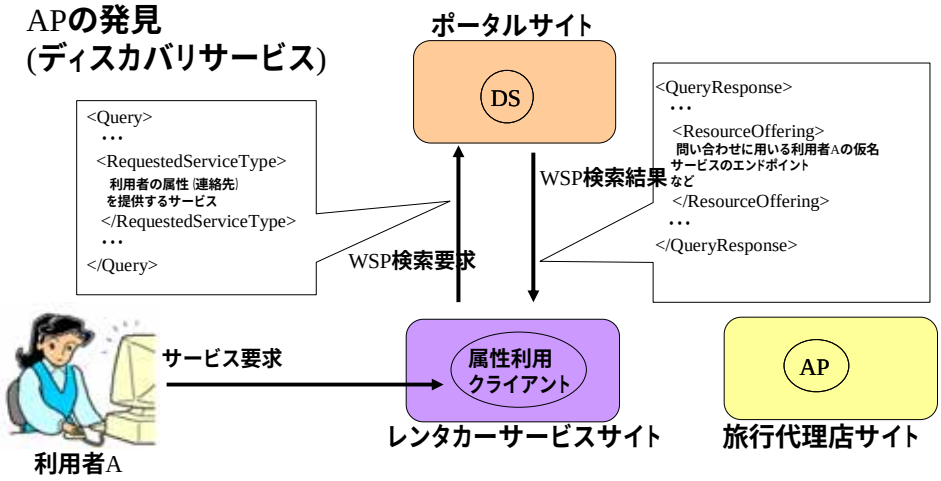


図 6-7 DS への登録

6.4.3　レンタカーサイトへの接続

ユーザは旅行代理店サイトからのサービスを受けた後、レンタカーサイトへ訪れる。6.4.1 節の手順と同様に、ID-FF に基づくシングルサインオンが実行される(図 6-8)。

1．レンタカーサイトはユーザの認証を必要とするため、ユーザをポータルサイトへ転送する。

2．ポータルサイトは既にユーザを認証済みなので、レンタカーサイトへ認証アサーションを発行する。認証アサーションには ID 連携手続き時に決定された仮名(uwxyz)が含まれている。レンタカーサイトは認証アサーションを受け、その仮名とレンタカーサイト自身がもつユーザの ID(####)をマッピングし、ユーザへの接続を完了する。また、ポータルサイトから発行される情報には認証アサーションと共に、後の DS による AP 検索を要求するために必要な情報(エンドポイントや利用者 A の仮名など)が含まれており、レンタカーサイトは後の過程でこの情報を使用する。

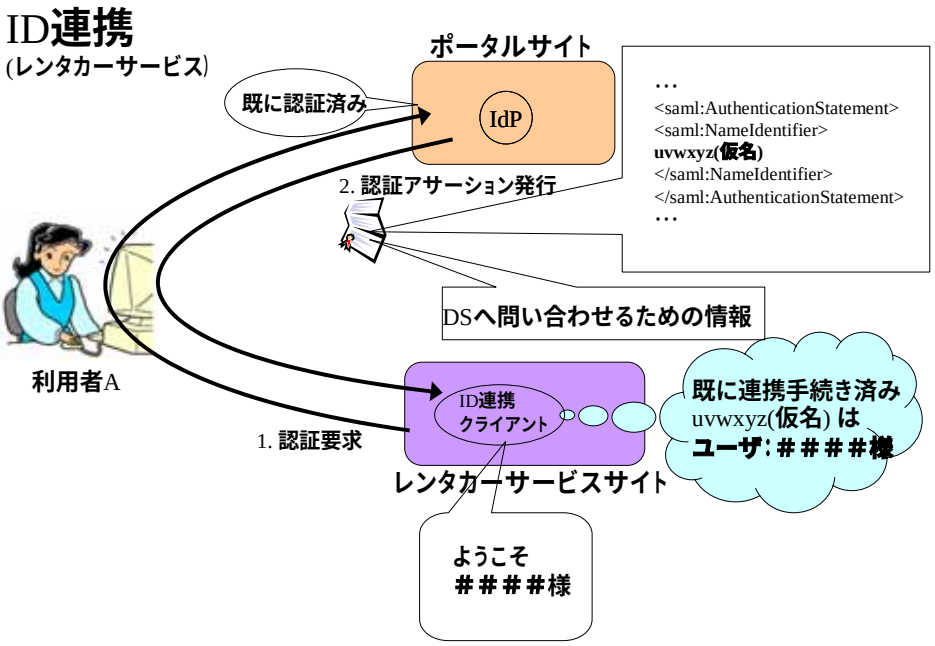


図 6-8 レンタカーサイトへのログイン

6.4.4 属性利用クライアント(レンタカーサイト)による AP(旅行代理店サイト)の発見

レンタカーサイトは利用者へのサービス提供に他の AP が持っている利用者の属性情報(例えば住所など)を必要とする。レンタカーサイトは必要とするユーザの属性情報をどこへ問い合わせるべきか知るために、DS(ポータルサイト)へ AP 発見の問い合わせをする(図 6-9)。この問い合わせは ID 連携時にポータルサイトから得られた情報を元に行われる。この情報には AP 検索用につけられた利用者 A の仮名が含まれているが、この仮名は旅行代理店サイト(AP)が DS へ登録した際に用いられた利用者 A の仮名(6.4.2 節)とは異なるものである。つまり、旅行代理店サイト(AP)とポータルサイト(DS)間、レンタカーサイト(属性利用クライアント)とポータルサイト(DS)間で使用される利用者 ID を分けることで、利用者のプライバシーを保護している。

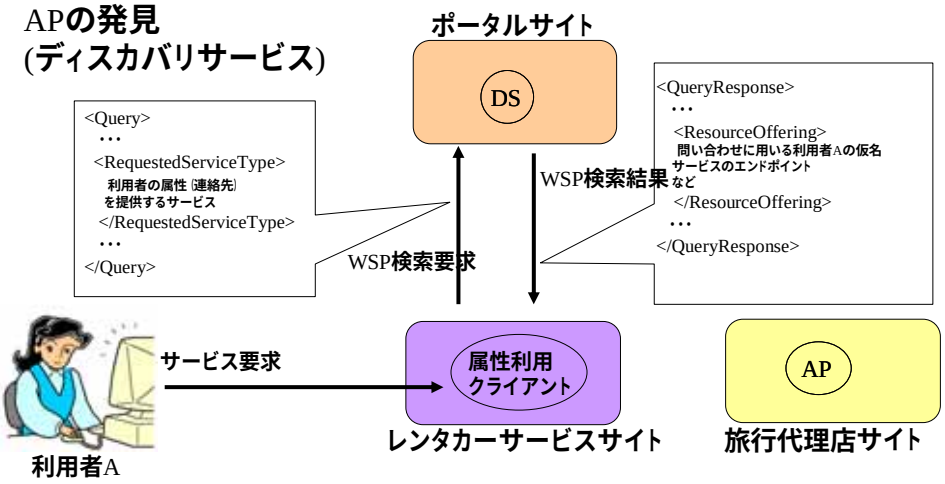


図 6-9 AP(旅行代理店サイト)の発見

6.4.5 AP(旅行代理店サイト)からの属性取得

属性利用クライアントであるレンタカーサイトは DS の検索結果より、必要とする属性情報は旅行代理店サイトが提供していることを知り、旅行代理店サイトへ属性要求を行う。レンタカーサイトは旅行代理店へ利用者の属性情報を要求する。要求には DS より取得した ResouceOffering を指定する(図 6-10)。

1. 旅行代理店サイトはレンタカーサイトへの属性提供について、利用者に対して同意確認を行う。
2. 旅行代理店サイトは利用者より属性提供の同意が得られた後、レンタカーサイトへ属性情報を提供する。
3. レンタカーサイトは利用者の属性情報を取得しサービスを提供する。

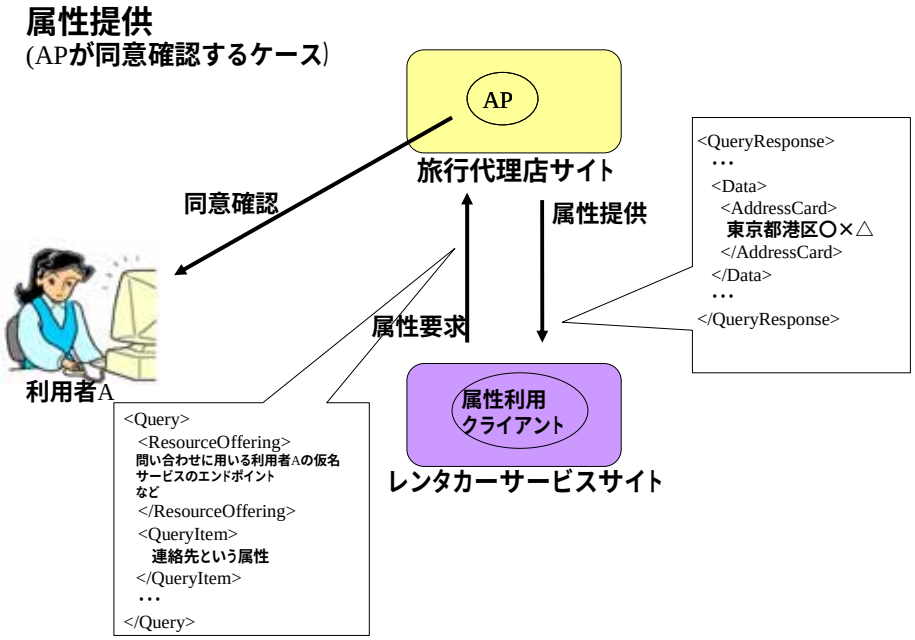


図 6-10 AP(旅行代理店サイト)の属性提供

7. まとめ

今日のインターネット社会において個人情報を活用した様々なサービスが提供されており、多くの利便性を享受できるようになったが、その反面、個人情報が不当な扱われ方をされた場合の影響は大きい。そのために個人情報を扱う組織が負うべき責任を示した基本法と一般的な事業者が負うべき責任を示したのが 2005 年 4 月に施行される個人情報保護法である。

この法律は過去 6 ヶ月の間に一度でも 5001 人以上の人を特定できるような個人情報を事業で利用した事業者は個人情報取扱事業者となることとなり、オンラインショッピングサイトやネットワーク上のサービス事業者に留まらず顧客データを扱う多くの組織・事業者が対策を講ずる必要があるという社会的インパクトの大きなものである。

こうした状況で、信頼できる事業者に個人情報を幾つかのサービスに分割し委託し、必要に応じてこれらを連携利用するという本報告書で提案した「属性情報プロバイダー」と呼んでいるサービス基盤により、漏洩の被害規模を低減しながら「安全な形で安心して」個人情報を交換でき、生活を「便利」にするサービスを享受することができる。

これが独自プロトコルによる提案であったならば、このようなサービスは日の目を見ることは無かっただろうが、SAML や Liberty といった Web サービスの認証認可技術を用いることにより、高い相互運用性を持つことができ、こうしたフレームワークは、米国やフランスなどの電子政府ポータルや、携帯電話サービス、産業界で徐々に広まりつつあり、海外でも日本と同様、文書の長期保存とシングルサインオン認証が最もホットなトピックとなっている。日本でもこのような SAML や Liberty の技術を持いたソリューションの提供が徐々に始まりつつあり、これらの技術を用いてシングルサインオンのために本人認証を行なう基盤サービスや属性情報を扱うサービスが立ち上がる日も遠くないと思われる。

今回は属性情報プロバイダーを提供するために属性情報プロバイダー側の検討を行なってきたが、今後は、これを利用するサービスプロバイダーやサービス利用者からの観点で同様に次に示す項目についての検討が必要である。

- **属性情報プロバイダーを利用するサービスプロバイダーの要件**
  - **事業者責任**
  - **プライバシーポリシー**
  - **運用要件**
- **サービス利用者の要件**
  - **利用者責任**
  - **プライバシーポリシーの利用法(同意確認の基準)**

8．参考文献

[1] 個人情報の保護に関する法律(平成十五年法律第五十七号)、
http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html

[2] "Liberty ID-FF Architecture Overview", Version 1.2, Liberty Alliance Project,12 November 2003, http://www.projectliberty.org/specs

[3] "Liberty ID-FF Bindings and Profiles Specification", Version 1.2-errata-v2.0, Liberty Alliance Project, 12 September 2004, http://www.projectliberty.org/specs

[4] "Liberty ID-FF Protocols and Schema Specification", Version1.2-errata-v2.0, Liberty Alliance Project, 12 September 2004, http://www.projectliberty.org/specs

[5] "Liberty ID-FF Implementation Guidelines", Version 1.2,Liberty Alliance Project, , http://www.projectliberty.org/specs

[6] "Liberty ID-FF Static Conformance Requirements", Version 1.0, Liberty Alliance Project, , http://www.projectliberty.org/specs

[7] "Liberty ID-FF Authentication Context Specification", Version 1.2-errata-v1.0, Liberty Alliance Project, 12 September 2004, http://www.projectliberty.org/specs

[8] "Liberty Metadata Description and Discovery Specification", Version 1.0-errata-v2.0, Liberty Alliance Project, 12 September 2004, http://www.projectliberty.org/specs

[9] "Liberty ID-WSF Security and Privacy Overview", Version 1.0, Liberty Alliance Project, 8 October 2003, http://www.projectliberty.org/specs

[10] "Liberty ID-WSF Discovery Service Specification", Version 1.1, Liberty Alliance Project, 21 April 2004, http://www.projectliberty.org/specs

[11] "Liberty ID-WSF SOAP Binding Specification", Version 1.1, Liberty Alliance Project, 3 May 2004, http://www.projectliberty.org/specs

[12] "Liberty ID-WSF Security Mechanisms", Version 1.0, Liberty Alliance Project,12 November 2003, http://www.projectliberty.org/specs

[13] "Liberty ID-WSF Interaction Service Specification", Version 1.0, Liberty Alliance Project, 12 November 2003, http://www.projectliberty.org/specs

[14] "Liberty ID-WSF Data Services Template Specification", Version 1.0, Liberty Alliance Project, 12 November 2003, http://www.projectliberty.org/specs

[15] "Liberty ID-WSF Architecture Overview", Version 1.0, Liberty Alliance Project, , http://www.projectliberty/specs

[16] "Liberty ID-WSF Client Profiles Specification", Version 1.0, Liberty Alliance Project, , http://www.projectliberty/specs

[17] "Liberty ID-WSF Authentication Service Specification", Version 1.0, Liberty Alliance Project, , http://www.projectliberty/specs

[18] "Liberty ID-WSF Implementation Guide, Draft Version 1.0-08, Liberty Alliance

Project, , http://www.projectliberty/specs
[19] "Liberty ID-WSF 1.0 Static Conformance Requirements", Version 1.0-08, Liberty Alliance Project, , http://www.projectliberty/specs
[20] "Liberty Reverse HTTP Binding for SOAP Specification", Version 1.0-errata-v1.0, Liberty Alliance Project, , http://www.projectliberty/specs
[21] "Liberty ID-SIS Personal Profile Service Specification", Version 1.0, Liberty Alliance Project, , http://www.projectliberty/specs
[22] "Liberty ID-SIS Employee Profile Service Specification", Version 1.0, Liberty Alliance Project, , http://www.projectliberty/specs
[23] "Privacy and Security Best Practices", Version 2.0, Liberty Alliance Project,12 November 2003,http://www.projectliberty.org/specs
[24] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 23 September 1980, http://www1.oecd.org/publications/e-book/9302011E.pdf
[25] プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告(1980 年 9 月仮訳)、外務省、
http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html
[26] 平成 15 年度 EC 技術基盤の相互運用性に関する調査研究事業(取引相手先の属性認証技術等の調査)SAML 利用検討報告書、Mar 2004、電子商取引推進協議会 ECOM、財団法人 日本情報処理開発協会 電子商取引推進センター
[27] 平成 15 年度 EC 技術基盤の相互運用性に関する調査研究事業(取引相手先の属性認証技術等の調査)属性情報利用システムー2010 年の市民生活ー、Mar 2004、電子商取引推進協議会 ECOM、財団法人 日本情報処理開発協会 電子商取引推進センター
[28] "Liberty architecture framework for supporting Privacy Preference Expression Languages(PPELs)", Version 1.0, Liberty Alliance Project, 12 November 2003, http://www.projectliberty.org/specs

用語集

【あ】

アイデンティティ

エンティティの本質のことであり、しばしばその特性によって表される。

ID-FF

Identity Federation Framework の略。Web シングルサインオンおよび ID 連携のための HTTP ベースのプロトコルを定義する Liberty 仕様セットの一部。

ID-WSF

Liberty Identity Web サービスフレームワーク仕様セット

ID 連携

トラストサークル内のさまざまな LibertyAlliance エンティティにおいて、主体者の複数アカウントを関連付けたり、バインドすること

IdP

Identitiy Provider の略。主体者のアイデンティティ情報を生成、保管、管理し、主体者の認証をトラストサークル内の他のサービスプロバイダーに提供する Liberty 対応のエンティティ。

Web サービス

HTTP/HTTPS プロトコルを用いてアクセス可能なアプリケーションコンポーネントを呼び出す仕組み。Web サービスでは XML 形式でデータの交換を行い、データへアクセスするプロトコルとして SOAP(Simple Object Access Protocol)を使用している。

OECD

経済協力開発機構。加盟国の協力により経済の安定成長と貿易の拡大に目的として 1961 年に発足した。先進国のほとんどが加盟しており、日本は 1964 年に加盟した。

オプトアウト

事後承諾のこと

オプトイン

事前承諾のこと

【か】

仮名

所定の信頼当事者に対して主体者を確認するために、信頼当事者間でのみ有効となるようにアイデンティティプロバイダまたはサービスプロバイダーによって割り当てられる任意の名前。

個人情報保護法

個人情報を事業用途で扱う事業者が果たすべき義務を定めた法律。事業者は本人同意のない個人情報の不正な利用が規制され、個人情報の管理責任を負う。2005 年 4 月より施行される。

個人情報取扱事業者

個人情報を容易に検索できるようなデータベースを持つ 5000 人を超える個人情報を持つ事業者。個人情報で定められた個人情報の管理責任を負う。

【さ】

SP

Service Provider の略。

(1) システムエンティティにより提供されるや役割。

(2) 主体者の観点から、サービスプロバイダーは典型的にはサービスおよび／もしくは商品を提供するウェブサイト。

シングルサインオン

アイデンティティプロバイダ A との間に存在する認証セッションの証明を使用して、アイデンティティプロバイダ B との新たな認証セッションを作成できること。

属性証明書

主体者の役割、権限、所属、グループなどを証明するために属性認証局から発行される証明書。X.509 および RFC 3281 で規定されている。

SOAP

Simple Object Access Protocol の略。XML データを伝送するためのメッセージング・プロトコル。

【た】

トラストサークル

ユーザが安全でシームレスな環境で取引できるような、Liberty アーキテクチャおよび運用協定に基づくビジネス関係を持っているサービスプロバイダーとアイデンティティプロバイダとの連携。

WSP

Web サービスを通じてデータを提供するエンティティ。

WSC

Web Service Consumer の略。Web サービスへのリクエストを作成する際のシステムエンティティにより割り当てられた役割。

DS

Discovery Service(ディスカバリサービス)の略。

ディスカバリサービス

ID-WSF サービスインスタンスの登録と結果となる検索の機能を持つサービス。

【な】

認証アサーション

主体者の認証を行なったことを証明するための短時間有効な乱数に基づくデータ。シングルサインオンではこれを交換することによりログイン認証を省略することができる。

【は】

プライバシーマーク制度

民間の個人情報保護の取り組みに対する認定制度として(財)日本情報処理開発教会が定めたもの。認定・監査を受けた事業者はプライバシーマークを使用することが認められる。

【ら】

Liberty

XML メッセージングに基づく幅広いドメインで利用可能な相互運用性の高いシングルサインオン、属性情報交換のためのセキュリティ技術仕様。

Liberty Alliance Project

Liberty 仕様を定める IT ベンダー、通信キャリア、携帯電話会社、航空会社、政府機関、学術機関など幅広い組織が参加し、仕様策定・啓蒙・広報活動を行なっているプロジェクト。

ROI

Resource Owner Interaction の略。Resource Owner Interaction サービスは、リソース所有者とのやり取りを公開する Liberty アイデンティティサービスを指す。これにより、クライアント(通常は WSP。WSP が ROI サービスに対しては WSC として機能する)はリソース所有者に同意、認可決定などの問い合わせを行うことができる。ID-WSF で同意確認をとる際に用いられるプロトコル。ROI サービスは以前インタラクションサービス(IS)と呼ばれていたこともある。

参考資料

参考 1　個人情報の保護に関する法律

個人情報の保護に関する法律(平成十五年法律第五十七号)

目次

第一章　総則

(目的)

第一条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

(定義)

第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

2　この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

3　この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

一　国の機関

二　地方公共団体

三　独立行政法人等(独立行政法人等の保有する個人情報の保護に関する法律(平成十五年法律第五十九号)第二条第一項に規定する独立行政法人等をいう。以下同じ。)

四　地方独立行政法人(地方独立行政法人法(平成十五年法律第百十八号)第二条第一項に規定する地方独立行政法人をいう。以下同じ。)

五　その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

4　この法律において「個人データ」とは、個人情報データベース等を構成する個人情報

をいう。

5　この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

6　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

(基本理念)

第三条　個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

第二章　国及び地方公共団体の責務等

(国の責務)

第四条　国は、この法律の趣旨にのっとり、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。

(地方公共団体の責務)

第五条　地方公共団体は、この法律の趣旨にのっとり、その地方公共団体の区域の特性に応じて、個人情報の適正な取扱いを確保するために必要な施策を策定し、及びこれを実施する責務を有する。

(法制上の措置等)

第六条　政府は、国の行政機関について、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

2　政府は、独立行政法人等について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

3　政府は、前二項に定めるもののほか、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする。

第三章　個人情報の保護に関する施策等

第一節　個人情報の保護に関する基本方針

第七条　政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針(以下「基本方針」という。)を定めなければならない。

2　基本方針は、次に掲げる事項について定めるものとする。

一　個人情報の保護に関する施策の推進に関する基本的な方向

二　国が講ずべき個人情報の保護のための措置に関する事項

三　地方公共団体が講ずべき個人情報の保護のための措置に関する基本的な事項

四　独立行政法人等が講ずべき個人情報の保護のための措置に関する基本的な事項

五　地方独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項

六　個人情報取扱事業者及び第四十条第一項に規定する認定個人情報保護団体が講ずべき個人情報の保護のための措置に関する基本的な事項

七　個人情報の取扱いに関する苦情の円滑な処理に関する事項

八　その他個人情報の保護に関する施策の推進に関する重要事項

3　内閣総理大臣は、国民生活審議会の意見を聴いて、基本方針の案を作成し、閣議の決定を求めなければならない。

4　内閣総理大臣は、前項の規定による閣議の決定があったときは、遅滞なく、基本方針を公表しなければならない。

5　前二項の規定は、基本方針の変更について準用する。

第二節　国の施策

(地方公共団体等への支援)

第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その

他の必要な措置を講ずるものとする。

(苦情処理のための措置)

第九条　国は、個人情報の取扱いに関し事業者と本人との間に生じた苦情の適切かつ迅速な処理を図るために必要な措置を講ずるものとする。

(個人情報の適正な取扱いを確保するための措置)

第十条　国は、地方公共団体との適切な役割分担を通じ、次章に規定する個人情報取扱事業者による個人情報の適正な取扱いを確保するために必要な措置を講ずるものとする。

第三節　地方公共団体の施策

(地方公共団体等が保有する個人情報の保護)

第十一条　地方公共団体は、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

2　地方公共団体は、その設立に係る地方独立行政法人について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

(区域内の事業者等への支援)

第十二条　地方公共団体は、個人情報の適正な取扱いを確保するため、その区域内の事業者及び住民に対する支援に必要な措置を講ずるよう努めなければならない。

(苦情の処理のあっせん等)

第十三条　地方公共団体は、個人情報の取扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない。

第四節　国及び地方公共団体の協力

第十四条　国及び地方公共団体は、個人情報の保護に関する施策を講ずるにつき、相協力するものとする。

第四章　個人情報取扱事業者の義務等

第一節　個人情報取扱事業者の義務

(利用目的の特定)

第十五条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的(以下「利用目的」という。)をできる限り特定しなければならない。

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(利用目的による制限)

第十六条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

2　個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3　前二項の規定は、次に掲げる場合については、適用しない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(適正な取得)

第十七条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

(取得に際しての利用目的の通知等)

第十八条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しな

ければならない。

2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。)に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

4　前三項の規定は、次に掲げる場合については、適用しない。

一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

三　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四　取得の状況からみて利用目的が明らかであると認められる場合

(データ内容の正確性の確保)

第十九条　個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

(安全管理措置)

第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

(従業者の監督)

第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

(委託先の監督)

第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

(第三者提供の制限)

第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

3　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

4　次に掲げる場合において、当該個人データの提供を受ける者は、前三項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

5　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

(保有個人データに関する事項の公表等)

第二十四条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければならない。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的(第十八条第四項第一号から第三号までに該当する場合を除く。)

三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続(第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。)

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。

一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

二　第十八条第四項第一号から第三号までに該当する場合

3　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(開示)

第二十五条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示(当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。)を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

3　他の法令の規定により、本人に対し第一項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には、当該全部又は一部の保有個人データについては、同項の規定は、適用しない。

(訂正等)

第二十六条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの

内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除(以下この条において「訂正等」という。)を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨(訂正等を行ったときは、その内容を含む。)を通知しなければならない。

(利用停止等)

第二十七条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているという理由又は第十七条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去(以下この条において「利用停止等」という。)を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第二十三条第一項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3　個人情報取扱事業者は、第一項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(理由の説明)

第二十八条　個人情報取扱事業者は、第二十四条第三項、第二十五条第二項、第二十六条第二項又は前条第三項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

(開示等の求めに応じる手続)

第二十九条　個人情報取扱事業者は、第二十四条第二項、第二十五条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め(以下この条において「開示等の求め」という。)に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

2　個人情報取扱事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。

3　開示等の求めは、政令で定めるところにより、代理人によってすることができる。

4　個人情報取扱事業者は、前三項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

(手数料)

第三十条　個人情報取扱事業者は、第二十四条第二項の規定による利用目的の通知又は第二十五条第一項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。

2　個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

(個人情報取扱事業者による苦情の処理)

第三十一条　個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

2　個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

(報告の徴収)

第三十二条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができる。

(助言)

第三十三条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し必要な助言をすることができる。

(勧告及び命令)

第三十四条　主務大臣は、個人情報取扱事業者が第十六条から第十八条まで、第二十条から第二十七条まで又は第三十条第二項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

2　主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

3　主務大臣は、前二項の規定にかかわらず、個人情報取扱事業者が第十六条、第十七条、第二十条から第二十二条まで又は第二十三条第一項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

(主務大臣の権限の行使の制限)

第三十五条　主務大臣は、前三条の規定により個人情報取扱事業者に対し報告の徴収、助言、勧告又は命令を行うに当たっては、表現の自由、学問の自由、信教の自由及び政治活動の自由を妨げてはならない。

2　前項の規定の趣旨に照らし、主務大臣は、個人情報取扱事業者が第五十条第一項各号に掲げる者(それぞれ当該各号に定める目的で個人情報を取り扱う場合に限る。)に対して個人情報を提供する行為については、その権限を行使しないものとする。

(主務大臣)

第三十六条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、個人情報取扱事業者が行う個人情報の取扱いのうち特定のものについて、特定の大臣又は国家公安委員会(以下「大臣等」という。)を主務大臣に指定することができる。

一　個人情報取扱事業者が行う個人情報の取扱いのうち雇用管理に関するものについては、厚生労働大臣(船員の雇用管理に関するものについては、国土交通大臣)及び当該個人情報取扱事業者が行う事業を所管する大臣等

二　個人情報取扱事業者が行う個人情報の取扱いのうち前号に掲げるもの以外のものについては、当該個人情報取扱事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

3　各主務大臣は、この節の規定の施行に当たっては、相互に緊密に連絡し、及び協力しなければならない。

第二節　民間団体による個人情報の保護の推進

(認定)

第三十七条　個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人(法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。)は、主務大臣の認定を受けることができる。

一　業務の対象となる個人情報取扱事業者(以下「対象事業者」という。)の個人情報

の取扱いに関する　第四十二条の規定による苦情の処理

二　個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

三　前二号に掲げるもののほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

2　前項の認定を受けようとする者は、政令で定めるところにより、主務大臣に申請しなければならない。

3　主務大臣は、第一項の認定をしたときは、その旨を公示しなければならない。

(欠格条項)

第三十八条　次の各号のいずれかに該当する者は、前条第一項の認定を受けることができない。

一　この法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者

二　第四十八条第一項の規定により認定を取り消され、その取消しの日から二年を経過しない者

三　その業務を行う役員(法人でない団体で代表者又は管理人の定めのあるものの代表者又は管理人を含む。以下この条において同じ。)のうちに、次のいずれかに該当する者があるもの

イ　禁錮以上の刑に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者

ロ　第四十八条第一項の規定により認定を取り消された法人において、その取消しの日前三十日以内にその役員であった者でその取消しの日から二年を経過しない者

(認定の基準)

第三十九条　主務大臣は、第三十七条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。

一　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに必要な業務の実施の方法が定められているものであること。

二　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに足りる知識及び能力並びに経理的基礎を有するものであること。

三　第三十七条第一項各号に掲げる業務以外の業務を行っている場合には、その業務を行うことによって同項各号に掲げる業務が不公正になるおそれがないものであること。

(廃止の届出)

第四十条　第三十七条第一項の認定を受けた者(以下「認定個人情報保護団体」という。)は、その認定に係る業務(以下「認定業務」という。)を廃止しようとするときは、政令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。

2　主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

(対象事業者)

第四十一条　認定個人情報保護団体は、当該認定個人情報保護団体の構成員である個人情報取扱事業者又は認定業務の対象となることについて同意を得た個人情報取扱事業者を対象事業者としなければならない。

2　認定個人情報保護団体は、対象事業者の氏名又は名称を公表しなければならない。

(苦情の処理)

第四十二条　認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。

2　認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができる。

3　対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

(個人情報保護指針)

第四十三条　認定個人情報保護団体は、対象事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手続その他の事項に関し、この法律の規定の趣旨に沿った指針(以下「個人情報保護指針」という。)を作成し、公表するよう努めなければならない。

2　認定個人情報保護団体は、前項の規定により個人情報保護指針を公表したときは、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとるよう努めなければならない。

(目的外利用の禁止)

第四十四条　認定個人情報保護団体は、認定業務の実施に際して知り得た情報を認定業務の用に供する目的以外に利用してはならない。

(名称の使用制限)

第四十五条　認定個人情報保護団体でない者は、認定個人情報保護団体という名称又はこれに紛らわしい名称を用いてはならない。

(報告の徴収)

第四十六条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務に関し報告をさせることができる。

(命令)

第四十七条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務の実施の方法の改善、個人情報保護指針の変更その他の必要な措置をとるべき旨を命ずることができる。

(認定の取消し)

第四十八条　主務大臣は、認定個人情報保護団体が次の各号のいずれかに該当するときは、その認定を取り消すことができる。

一　第三十八条第一号又は第三号に該当するに至ったとき。

二　第三十九条各号のいずれかに適合しなくなったとき。

三　第四十四条の規定に違反したとき。

四　前条の命令に従わないとき。

五　不正の手段により第三十七条第一項の認定を受けたとき。

2　主務大臣は、前項の規定により認定を取り消したときは、その旨を公示しなければならない。

(主務大臣)

第四十九条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、第三十七条第一項の認定を受けようとする者のうち特定のものについて、特定の大臣等を主務大臣に指定することができる。

一　設立について許可又は認可を受けている認定個人情報保護団体(第三十七条第一項の認定を受けようとする者を含む。次号において同じ。)については、その設立の許可又は認可をした大臣等

二　前号に掲げるもの以外の認定個人情報保護団体については、当該認定個人情報保護団体の対象事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

第五章　雑則

(適用除外)

第五十条　個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。

一　放送機関、新聞社、通信社その他の報道機関(報道を業として行う個人を含む。)　報道の用に供する目的

二　著述を業として行う者　著述の用に供する目的

三　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的

四　宗教団体　宗教活動(これに付随する活動を含む。)の用に供する目的

五　政治団体　政治活動(これに付随する活動を含む。)の用に供する目的

2　前項第一号に規定する「報道」とは、不特定かつ多数の者に対して客観的事実を事実として知らせること(これに基づいて意見又は見解を述べることを含む。)をいう。

3　第一項各号に掲げる個人情報取扱事業者は、個人データの安全管理のために必要かつ適切な措置、個人情報の取扱いに関する苦情の処理その他の個人情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

(地方公共団体が処理する事務)

第五十一条　この法律に規定する主務大臣の権限に属する事務は、政令で定めるところにより、地方公共団体の長その他の執行機関が行うこととすることができる。

(権限又は事務の委任)

第五十二条　この法律により主務大臣の権限又は事務に属する事項は、政令で定めるところにより、その所属の職員に委任することができる。

(施行の状況の公表)

第五十三条　内閣総理大臣は、関係する行政機関(法律の規定に基づき内閣に置かれる機関(内閣府を除く。)及び内閣の所轄の下に置かれる機関、内閣府、宮内庁、内閣府設置法(平成十一年法律第八十九号)第四十九条第一項及び第二項に規定する機関並びに国家行政組織法(昭和二十三年法律第百二十号)第三条第二項に規定する機関をいう。次条において同じ。)の長に対し、この法律の施行の状況について報告を求めることができる。

2　内閣総理大臣は、毎年度、前項の報告を取りまとめ、その概要を公表するものとする。

(連絡及び協力)

第五十四条　内閣総理大臣及びこの法律の施行に関係する行政機関の長は、相互に緊密に連絡し、及び協力しなければならない。

(政令への委任)

第五十五条　この法律に定めるもののほか、この法律の実施のため必要な事項は、政令で定める。

第六章　罰則

第五十六条　第三十四条第二項又は第三項の規定による命令に違反した者は、六月以下の懲役又は三十万円以下の罰金に処する。

第五十七条　第三十二条又は第四十六条の規定による報告をせず、又は虚偽の報告をした者は、三十万円以下の罰金に処する。

第五十八条　法人(法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。)の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前二条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。

2　法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

第五十九条　次の各号のいずれかに該当する者は、十万円以下の過料に処する。

一　第四十条第一項の規定による届出をせず、又は虚偽の届出をした者

二　第四十五条の規定に違反した者

附　則

(施行期日)

第一条　この法律は、公布の日から施行する。ただし、第四章から第六章まで及び附則第二条から第六条までの規定は、公布の日から起算して二年を超えない範囲内において政令で定める日から施行する。

(本人の同意に関する経過措置)

第二条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第十五条第一項の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは、第十六条第一項又は第二項の同意があったものとみなす。

第三条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第二十三条第一項の規定による個人データの第三者への提供を認め

る旨の同意に相当するものであるときは、同項の同意があったものとみなす。

(通知に関する経過措置)

第四条　第二十三条第二項の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。

第五条　第二十三条第四項第三号の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同号の規定により行われたものとみなす。

(名称の使用制限に関する経過措置)

第六条　この法律の施行の際現に認定個人情報保護団体という名称又はこれに紛らわしい名称を用いている者については、第四十五条の規定は、同条の規定の施行後六月間は、適用しない。

附則(平成十五年法律第百十九号)抄

(施行期日)

第一条　この法律は、地方独立行政法人法(平成十五年法律第百十八号)の施行の日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　第六条の規定　個人情報の保護に関する法律の施行の日又はこの法律の施行の日のいずれか遅い日

(その他の経過措置の政令への委任)

第六条　この附則に規定するもののほか、この法律の施行に伴い必要な経過措置は、政令で定める。

参考 2　プライバシーポリシー交換技術 P3P と APPEL

属性サービスプロバイダー事業者が個人情報を扱う場合、個人情報の所有者である利用者に同意を得る必要がある。Liberty アーキテクチャでは Interaction Service を利用することによりこれを行うとしているが、SAML では仕様の範囲外である。

従って、SAML を利用した属性情報サービスの場合には、何らかの別の手段により利用同意を得る方法を確保しなければならない。

利用者同意を得る方法としては、ウェブ上で利用規約を文章により提示し、ウェブフォームで利用者の意思を入力させるという方法が広く一般に使われているが、ウェブ技術の標準化団体 W3C で定められた P3P(Platform for Privacy Policy Project)やその機能拡張である APPEL(A P3P Preference Exchange Language)といった技術を使うことにより、利用者の自己情報コントロールや予め定められたプライバシーポリシーの提示、確認を自動化することができる。

(1) P3P(Platform for Privacy Policy Project)

P3P(Platform for Privacy Preferences Project)は、W3C(World Wide Web Consortium)により進められている Web サイトのプライバシーポリシーをマシンリーダブルな形式で記述し警告などを自動的に処理するためのフォーマットの標準化である。本報告執筆時点(2004 年 11 月)で 2002 年 4 月 16 日に P3P 1.0 勧告が発表されている。

閲覧者であるユーザが要求した際に返信されるプライバシーポリシーのデータは XML により与えられ、以下の情報を含むことができる。

- **ユーザまたは Web サイトがアクセスできる個人情報の種類**
- **ユーザまたは Web サイトが個人情報取扱い関する紛争を解決する方法**
- **Web サイトが個人情報を利用する目的**
- **Web サイトにより個人情報が第三者に送られる場合、その受領者**
- **Web サイトにより個人情報が保管される期間**

以上のデータのリクエストおよびレスポンスは HTTP プロトコルのヘッダおよびボディを介してやりとりされる。

ここでいう個人情報は単にユーザが明示的に登録した属性情報だけでなく、クッキーなどに自動的に保存される情報も含まれるので注意が必要である。

一方、P3P に対応したブラウザーを使用している閲覧者であるユーザは、自らの個人情報の開示に関して、どのような条件なら開示するか、ブラウザーに含まれる P3P を扱うエンジンの設定を行うことができ、その設定と受信したプライバシーポリシーとを比較して、自動的に警告を出したりすることができる。

P3P 自体には、転送される個人情報や、プライバシーポリシードキュメント自体について

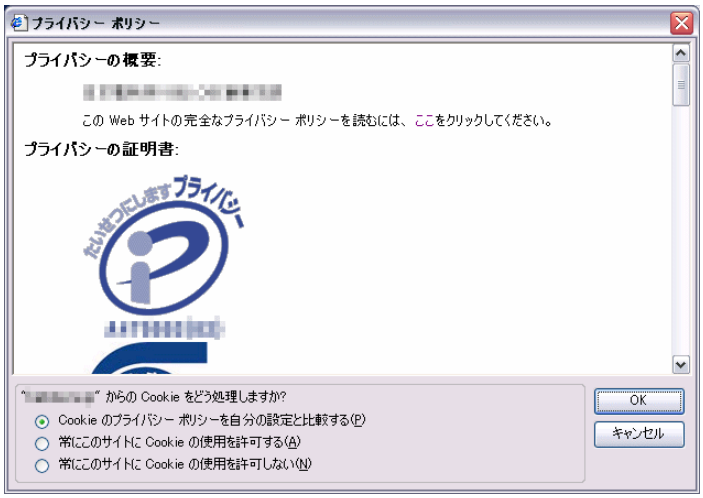
SSL/TLS や XML 署名といった転送されるメッセージの改竄を防ぐ手段については何ら規定がないため、ウェブサイトでは、これらの対策が必要となる。P3P の XML 署名については A P3P Assurance Signature Profile が W3C ノートとして公開されている。これは、プライバシーポリシーの XML ドキュメントに改竄無いことを示すだけでなく、どのような目的で署名しているのかを宣言するものである。

また、P3P は対象の Web サイトがプライバシーポリシーに則って運用されているか、虚偽の申告がなされていないかを保証するものではなく、これらは紛争解決の手段で提示された方法により法的に解決することとなる。

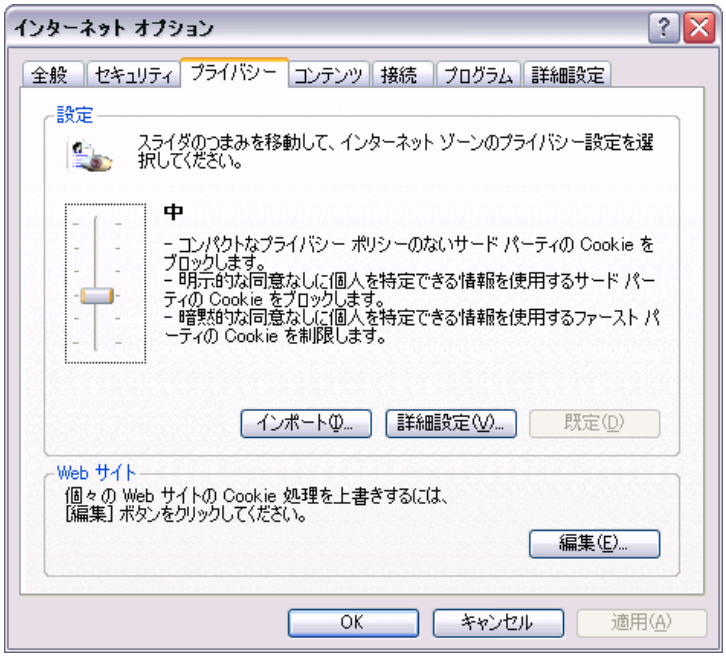
財団法人ニューメディア開発協会のサイトでは、Web サイトを P3P 対応にするための技術文書や P3P プライバシーポリシーの XML ドキュメントを生成するウィザードなどを公開している。

Netscape Navigator 7.0 や、Microsoft Windows XP 上の Internet Explorer 6.0 や、プライバシーポリシーの表示や、クッキーの制御が可能になっている。

例えば Internet Explorer 6 では、現在表示中のウェブサイトのプライバシーポリシーを表示させたい場合、メニューの「表示(V)→プライバシー レポート(V)...」を選択することによりウェブサイトのレポートが表示され、リスト中のサイトを選択し「概要」のボタンを押すとプライバシーポリシーを人が読める形に変換し表示される。



また、同様にメニュー「ツール(T)→インターネット オプション(O)...」を選択し、「プライバシータブ」を選択すると、コンパクトポリシーによるクッキーの送信制御が 6 段階で設定可能であり、プライバシーポリシーの有無や個人情報の暗黙的／明示的同意の必要性などを基準にクッキーの送信をブロックすることが可能となっている。


インターネット オプション
全般
セキュリティ
プライバシー
コンテンツ
接続
プログラム
詳細設定
設定
スライダのつまみを移動して、インターネット ゾーンのプライバシー設定を選択してください。
中
- コンパクトなプライバシー ポリシーのないサード パーティの Cookie をブロックします。
- 明示的な同意なしに個人を特定できる情報を使用するサード パーティの Cookie をブロックします。
- 暗黙的な同意なしに個人を特定できる情報を使用するファースト パーティの Cookie を制限します。
インポート(I)...
詳細設定(V)...
既定(D)
Web サイト
個々の Web サイトの Cookie 処理を上書きするには、[編集] ボタンをクリックしてください。
編集(E)...
OK
キャンセル
適用(A)

(2) APPEL(A P3P Preference Exchange Language)

APPEL(A P3P Preference Exchange Language)は、P3P と同じく W3C で提案されている標準であり、P3P により提示された Web サイトのプライバシーポリシーに対し、サイト閲覧者が許諾するルールのドキュメントフォーマットを定めた物である。報告書執筆時点(2004 年 11 月)で、2004 年 4 月 15 日にバージョン 1.0 が W3C ワーキングドラフトとして公開されている。

最初に明らかにしておく事として、APPEL は現在ワーキングドラフトであり、仕様書にフィードバックするための実験的プロトタイプ開発は許可されているが、将来の仕様書の記述に影響を与えるような実装は許可されていないので現状では APPEL ドラフトに基づく実装によりサービス開始することはできないことに注意しておく必要がある。

実運用では現状 APPEL を使う事はできないが、プライバシーポリシーの処理を自動化し利用者と協議するためのインタラクションや、属性の種類、ポリシーの内容について参考にすべき点があり、参考情報として本節で説明することとする。

ウェブサイト閲覧者は P3P によりサイトのプライバシーポリシーをダウンロードし、ユーザの意図した設定情報と比較して、そのままでは受け入れられない場合、プライバシーポリシー中で提示された個人情報の第三者への提供や、保存期間、利用用途などについて、ユーザが許容可能な範囲に絞込み、これをサイトへ送信する。サイト側は、ユーザが送信したポリシーでサービス提供可能か判断し、ユーザに提示されたポリシーの変更を許容できるか判断し、許容可能であればサービスを提供する。

即ち、P3P では単にサイトが提示したプライバシーポリシーに対し、ユーザが許諾可能かどうか YES/NO で応答する一方向的なものであるが、APPEL は、サイトとユーザ間で許諾可能なプライバシーポリシーを協議することが可能となっている。これにより、P3P 単体よりもユーザ自身の個人情報がどのように扱われるかを自己コントロールできる範囲を拡大するものである。

Liberty architecture framework for supporting Privacy Preference Expression Languages(PPELs)[28]では、Web サービスの提供者と利用者間でプライバシーポリシーを協議するための仕組みについて解説されている。

参考 3　属性情報活用事例調査報告書(要約版)

(1) はじめに

本調査では、インターネットの利用者の個人属性が、主要サイトにおいて現在どのように取得、利用されているかを WEB サイトおよび複数のサイト運営会社へのインタビューにより調査し、その傾向や課題を分析した。また、今後、そうした属性(個人情報)を利用者、サイト双方が安全、安心して活用していくためのモデルとして H15 年度の調査報告書「属性情報利用システム－2010 年の市民生活－」の中で提案した「属性情報登録・活用基盤」の実務面の課題を整理し、本格的な展開に向けた複数のシナリオを示している。

(2) 主要ネットサービス分野における個人属性の取扱い傾向

(A) 主要サイトにおける利用者の属性の取扱い状況

現在インターネットでビジネスサービスを行っている主要な分野について、利用者から収集している属性の種類やその方法、またサービス場面でその属性がどのように利用されているか、WEB サイトの調査およびインタビューにて明らかになった結果を記す。

主要なビジネス分野における代表的なサイトが、利用開始時に、利用者から直接収集している属性の種類を記の表 参考 3-1 に整理した。

なお、表中の分類に示した文字の意味は次の通りである。

ポ・・・　一般ポータルサイト
シ・・・　オンラインショッピングサイト
就・・・　就職支援サイト
オ・・・　ネットオークションサイト
ア・・・　ネットアンケートサイト
コ・・・　コミュニティ形成サイト
銀・・・　ネットバンキングサイト
証・・・　ネット証券サイト
生・・・　生命保険サイト

表 参考 3-1 サイト利用開始時に利用者が登録する属性情報

分類	ポ	ポ	シ	シ	就	オ	ア	ロ	銀	証	生
サイト名	YAHOO！(会員登録)	goo(会員登録)	楽天(会員登録)	アマゾン(アカウントサービス	リクナビ(会員登録)	YAHOOオークション(入札登	gooリサーチ(会員登録	トモモト(会員登録)	ソニー銀行(口座登録)	マネックス証券(口座開設登	アクサ生命(相談申込
任意ID	○	○	○		○	○	○				
ニック(ハンドル)ネーム			△					○			
氏名		○	○	○	○		○	○	○	○	△
氏名ふりがな		△	○	○	○		○		○	○	△
パスワード	○	○	○	○	○	○	○	○		○	
郵便番号	○	○	△	○	○	○	○		○	○	
住所(都道府県)								○			
住所			△	○			○		○	○	△
電話番号(自宅)			△	○	○		○		○	○	△
FAX番号							△		△		
性別	○	○	△			○	○	○	○	○	△
生年月日	○	○	△			○	○	○	○	○	△
メールアドレス	○	○	○	○	○	○	○	○	○	○	△
血液型								○			
職業	○	○				○	○	○	○	△	
所属(会社)先名			△	△			△		△	△	
部署名･役職			△				△		△	△	
秘密の質問/答え	○		△		○	○					
画像認証	○	○				○					
関心のあるジャンル、趣味	△	△				△		△	△		
インターネット接続環境		○									
クレジットカード番号				○		○					
学歴					○						
自己紹介						△					
BLOG								△			
利用(開設)のきっかけ									△	○	
利用(開設)の理由									△	△	
取引銀行口座										△	
年収										△	
金融資産額(予定運用額)									△	△	
キャッシュカード暗証番号									○		
家族情報							△				
所有物(車、PCなど)							△				

(○は必須、△は任意)

表 参考 3-1 から、基本情報(氏名、住所、性別、生年月日)の他、インターネットにおける連絡先である「メールアドレス」を登録(取得)対象としているサイトが多いことがわかる。その他の属性については、ビジネス分野によって違いが見られるが、現時点では個々のサイトが

取得できている利用者の属性は多くはない。これは、多種類の属性を管理する負荷やリスクが大きいという理由がある一方で、利用者が属性を提供する仕組みが複雑で、できるだけ負担をかけないためには現行の技術では、この程度が限界といった理由もあるようだ。

また、実際のサービス利用時では、各分野では個人属性は次のように利用されている。

① 一般ポータルサイト

登録した属性の一部が「本人プロフィール」として、他の利用者に公開される。掲示板などに投稿した場合、投稿者にリンク付けがされ、そのプロフィールのページに飛べるようになっている。公開内容はサイトによって異なる。

② オンラインショッピングサイト

商品購入時に、入力操作を軽減するよう住所など一部の属性が配送先、連絡先の候補として画面表示される。

③ 就職支援サイト

就職希望先に一部の属性が転送される。また、応募状況や採用状況などを統計処理を行なうのに一部の属性が利用される。またサイトによっては、登録者同士の情報交換用に一部属性が公開(プロフィール)されるようになっている。

④ オークションサイト

出品者の「本人プロフィール」他、それまでに出品した商品や購入(落札)者からの評価、コメントが公開されるようになっている。

⑤ ネットアンケートサイト

登録した属性内容に応じて、アンケート主催側が希望する対象先として選定される。また、回答内容の分析にあたって登録属性の内容(年代、住居地域)が統計処理に使用される。アンケート謝礼の発送に登録住所が使用されるようなこともある。

⑥ コミュニティ形成サイト

①と同様、登録した属性の一部が「本人プロフィール」として、他の利用者に公開される。投稿者にリンク付けがされ、そのプロフィールのページに飛べるようになることも同様である。また一部の属性は利用者間のコミュニケーション促進用の統計処理に利用されている。

⑦ ネットバンキングサイト

一部の属性が取引の確認連絡や各種証書の送付用に利用されている。また、取引時の本人認証用として利用される属性もある。

⑧ ネット証券サイト

⑦と同様、一部の属性が取引の確認連絡や各種証書の送付用に利用されている。取引時の本人認証用として利用される属性もある点も⑦と同様である。

⑨ 生命保険サイト

その後の取引のための連絡用として利用されている。(新規申込自体はオフラインが基本となっている)

この他、社員が自らの給与情報をインターネットを通じて確認できるようなサービスを行なっているサイトについては、社員の所属会社から直接サイトへ人事や給与関連の情報が送信され社員個人のみが自分の情報にアクセスできる運用が行なわれており、他のサイトにデータを提供するようなことはないことがインタビューによりわかった。

登録属性の削除については、いくつかのサイトへのインタビューした結果、一度登録した会員でも本人の希望があればもちろんのこと、長期間全くアクセスがないような場合は連絡先に警告した後、会員をはずす(脱会)手続がとられていることがわかった。この場合、取得した属性も削除されることになるが、サイトによっては後のトラブル、クレームに備えて一定期間は削除対象の個人属性を保存しているところもあった。

(B) インターネットビジネスライフサイクルにおける属性取扱い傾向

インターネットの現行のビジネスサイトのサービスでは利用者の個人の属性はビジネスのライフサイクル(サービス申込時、サービス利用時、サービス解約時)の中で次のように取り扱われているといえる。

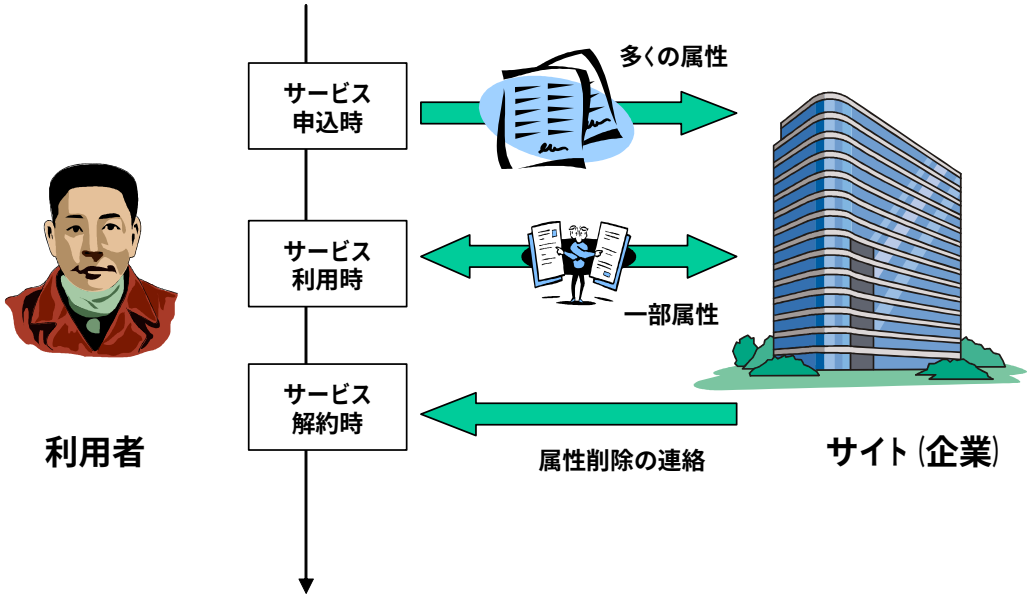


図 参考 3-1 属性のライフサイクル

［サービス申込時］

・サービスを利用するのに必須である、またはサービスを利用資格があるかを企業側が判断するために、基本的な属性情報およびその分野に特有な属性情報がサイトに登録される。原則一度のみ利用者からサイトにむけて送信され、その後はサイト側で保管され、インターネット自体で流通はしない。

・サイトを利用する「会員」になるために登録する属性としては下記のようなものがある。

A) ID、メールアドレスなど、サイト内の本人識別や認証のために最低必要な情報

B)　A に加え、氏名や住所、など基本的な情報
C)　B に加え、会社や学校などの所属や趣味などの情報
D)　サイトを利用するのに必要な銀行口座やクレジットカード番号の情報

B)C)はサービスの種類によっては他の利用者に公開される場合もある。また、D については真正を確認するため、公的機関が発行した証明書の送付が必要になる場合もある。

［サービス利用時］
・サービス利用開始時に登録された属性のうち、一部の属性が取引時に利用者とサイト間でやりとりされる。サービス分野によっては利用者本人だけでなく、他の利用者(第三者)にも提供されることもある。

［サービス解約時］
・利用者から利用終了の希望通知や一定の条件(アクセスが長期間ない、など)によりサイト側が取得した属性を削除する。利用者には、削除する(した)旨が連絡される。

この他、調査を通じて次のようなことが判明した。
現在の多くのサイトでは登録されている属性情報は自己申告による情報が多く、また、公的機関等の証明書の送付を必要としているサイトでも、その属性を照合するのはサービス利用開始時の資格審査にだけであった。
つまり各サービス場面では、一度、ログイン時に本人認証がされた後は、逐一利用者の属性情報の真正性までを確認していない(そのようなサービスモデルは現時点では現れていない)といえよう。

(3) インターネットでの属性共有、活用の傾向、課題

主要サイトへのインタビューを通して判明したインターネットのビジネスサイトにおける利用者の属性の取り扱いの傾向や課題について整理する。

(A) 利用者意識の変化

ポータルサイトやソーシャルネットワーキングサイトへのインタビューの結果、1997-98 年ごろのインターネット初期普及期に比べ、ネット利用者がサイトの会員登録などで自分の属性を登録する抵抗感は格段に小さくなっていることがわかった。
このことは利用者が自分の属性を登録し、他の利用者に公開することがサービスの基幹であるソーシャルネットワーキングサイトが広く受け入れられ始めたことにも表れている。ソーシャルネットワーキングサイトは、国内では 2004 年よりサービスが開始され、まだ 1 年も経っていないのにもかかわらず、その会員層は単なる新しモノ好きの層を通りこし、今や会員の中心は一般利用者(フォロワー)層になっているという。

これは、インターネットの普及が進むにつれ、インターネットが一部マニア向けを通り越し、一般家庭で日常的に利用される道具(ツール)になったこと、サイトでも安全性が重要視され、登録画面についての暗号化措置や運営会社(IT 企業)が上場するなど社会的な認知度が高まった、などが背景としてあると思われる。

属性の取扱いについては、すでに法人(会社、団体)内部の場合は、インターネットを介して属性情報を含む重要な情報を送受信することはもはや当然のこととなった。VPN などの技術により、自社内の複数の事業所間あるいは関連会社間で社員の個人属性を含むデータが送受信されている他、社員個人に対しても外部から人事や給与関係の属性情報を閲覧したり、採用希望者(新卒、中途)がインターネットを通じて自分の情報を企業に向けて送ることが違和感なく行われている。

一般利用者とインターネットのサイト間でも、様々な属性が送受信されるようになってきている。ただし、現時点でインターネットを介してサイトで利用されている個人の属性情報は、一部を除くと利用者が自己申告する形でネット上のサイトに登録したものであることが多く、属性の種類や内容自体も現実の正しい状態が反映されているとは言いがたい。一方で利用者側でもそうした事情をよく理解しており、サイトによって他の利用者が公開している属性の真正性を見分け、うまく使い分けていることが多いという。しかし、一方で、一部の利用者はそこまでの知識がなく、詐欺などの犯罪に巻き込まれることも多々あるという。

(a) 世代差・国民意識差

現在、インターネットサービスの中心利用者層は 20 代後半～30 代後半となっている。この中心層より若い 10 代後半～20 代前半の世代では WEB サイトを利用するよりは、携帯電話のメールや機能を多く利用している。

サイトへのインタビューなどを通じ、インターネットの利用や自分の属性をインターネットに登録することについて世代間で次のような意識差が見出せた。

- 若年層(10 代後半～20 代前半の世代)

  自分の属性をインターネットなどを通じて第三者に公開することに対する抵抗感は少ない。ただ、現実の利用は個対個のコミュニケーションが中心であり、広く一般利用者やビジネスサイト(企業)に自分の属性を提供したり、活用するような機会(場面)自体が少ない。

- 中心層(20 代後半～40 代前半)

  インターネットを個人や家庭の生活を快適にする道具として積極利用しており、メリットに感じられるサービスについては自分自身の属性情報を提供することについても抵抗が少ない方であるが、一部の属性(顔写真、性別、生年月日)については閉じた範囲でのみ流通を希望する。

- 保守層(40 代後半～)

  インターネットを個人の趣味や興味先として利用している。このため、積極利用する者とほとんど利用しない者に分かれるが、積極利用する者はリスクを恐れず、各種機能を深

く使いこなす傾向がある。属性の登録についても自己申告で真正な内容を登録し、任意となっている種類でも積極的に登録する。

一方、国民意識の差については、国の歴史や社会制度の事情の違いにより、属性の種類によってはインターネット登録や利用に対する抵抗感が大きく異なることがわかった。例えば、顔写真や指紋データについては、日本ではまだ抵抗感が強いが、韓国では抵抗が少ないという。日本では現実の社会システムでも顔写真、指紋の登録が行なわれていないことが少なからず影響している。また、韓国ではブロードバンドが家庭まで普及しているわけではなく、ネットカフェ等、複数の人が共用する端末からアクセス機会が多いことから個人を確実識別できるバイオメトリクスのような属性については関心が高く受け入れられているところがある。

また、米国に対しヨーロッパ諸国やオーストラリアでは、個人情報の管理について敏感であり、インターネットにおける属性の取扱いについても厳しい安全管理が求められており、IDマネジメントのような一部属性を情報システムに活用する仕組みの実用化、普及化が進んでいる。

(B) 属性の利用場面と有効期限

(a) 属性の利用場面

インターネットの各サイトが利用者の属性を収集し、利用する場面を分類すると下記のようになる。

(ア)サイトを利用する利用者の識別情報として利用する

(イ)利用者がサイト(サービス)を開始するにあたり、利用する資格があるかを審査する

(ウ)サイトのサービス実施に必要な情報の一部として利用する

(エ)利用者の属性を他者や企業などに示すこと自体がサービスの本質のもの

(ア)の例としては、ポータルサイトがある。ポータルサイトを自分用に使いやすい画面構成に改変したり、掲示板、会議室などに投稿するための会員区別として、自己登録 ID や個人属性(性別、年齢、趣味など)が設けられている。登録自体も任意かつ自己申告であり、その値についても特にサイトが確認していないことが多い。このため属性の真正性は著しく低く、利用者も他の利用者の登録属性が真正であることは期待しておらず、偽情報が登録されていることを前提とした利用が行われている。

(イ)の例としては、ネット銀行や証券サイトがある。この場合、単にサイトに自分の属性を自己申告で登録するだけではなく、現実社会の各種証明書を送る必要があり、真正な情報を取り付けられているのが特徴である。ただ、一度審査などに通った後は、インターネットでその属性情報が頻繁に交換(送受信)されるようなことは通常はない。また、定期的に属性が変っていないかサイト側から確認するようなことも通常はない。

(ウ)の例としては、ショッピングサイトやアンケートサイトがある。この場合、登録する属性は基本的に自己申告(例：配送先の住所など)であるが、虚偽の情報を登録した場合はサービスを享受すること自体ができなくなるため多くの場合は正しい情報が登録される。ただし、いやがらせやいたずら目的で虚偽の情報(他人の名前や偽の住所など)が登録されるようなケー

スもあり、現在のサービス手順ではこのような場合の対処は難しい。

(エ)としては、ソーシャルネットワーキングサイトのようなネット上で新たなコミュニティを形成するサービスがある。サイトのサービスの目的が利用者(会員)間のコミュニケーション促進であるため、利用者の属性情報自体を互いに公開し合う(送受信する)ことが他と異なる大きな特徴である。会員が登録する属性情報は基本的に自己申告であり、特にサイト側でその属性値が真正かどうかを調べたり、証明書等で確認したりしてはいない。このような場合、虚偽の属性が登録されがちであるが、ソーシャルネットワーキングサイトでは、会員を紹介制にしている故に虚偽の情報登録が少なくなっている。ただし、該当する属性でもそれを登録するかどうかは個人差があり、サイトに登録された内容だけでは現実の会員の姿が類推できるまでには至っていない。

(b) 属性の有効期限

個人の属性というのは、調査時点の値が永続するものばかりではない。時期や年代により大きく変るものや随時値が変わるもの、など様々である。2 章で調査した現行のサイトで取扱われている主な属性を、{A.変わらない属性}{B.定期的に見直す必要のある属性}、{C.値や程度が随時変わる属性} に分類すると下記のようになる。

表 参考 3-2 主要属性における有効期限

属性種類	A.不変	B.定期	C.随時
氏名	○		
性別	○		
生年月日	○		
住所		○	
メールアドレス		○	
勤務先(職種)		○	
趣味･興味分野		○	
クレジットカード番号		○	
電話番号		○	
家族情報(構成、配偶者)		○	
年収		○	
血液型	○		
容姿(写真)		○	
取引口座番号		○	
食事メニュー			○
健診(脈拍値など)			○
成績	○		
スケジュール			○
所有株式価格			○

表 参考 3-2 に示されたように、既に現行のネットのサイトでも 3 分類のいずれの属性も取扱われている。このうち、A については利用者に一度だけその属性の真正確認を行なえばよい。

B、C については本来なら定期的に属性値が変更されていないかどうかを確認する必要がある。しかし、サイト側で各属性に対して有効期限を定め、期限後にその属性の内容を抹消したり、失効するようなサービスは現在のところは見られない。

(C) サイトにおける属性情報管理

個人情報保護法の施行により、今後、各サイトには利用者から得た属性情報について厳格な管理が求められる。

現在、サイトを運営する企業の規模はまちまちであり、インターネットにおける様々な脅威から最新の技術を用い、十分な管理コストをかけて安全対策を行なえる企業ばかりではない。

規模の異なる複数のサイト運営会社へインタビューした結果、大企業が運営するサイトでは、利用者の情報を安全に管理する情報システムや運用の仕組みが既に検討、構築されている状況にあり、今後についても自社で管理していく方針であることがわかった。利用者の属性情報はサイトにとって貴重な資産であり、サイト内の行動と照らし合わせることで、購買パターンなどマーケティング分析の貴重なデータになる可能性があるため、多少のコストがかかっても自ら収集・管理する価値がある、というような意見も得られた。

これに対し、ベンチャー企業など中小規模の企業が運営するサイトからは、今後の利用者の属性情報管理への対応について厳しい意見が相次いだ。これらの企業体力では、社内部から情報漏洩が起きないよう人的な対策体制を整える程度が対応の限界で、今後インターネットにおける新たな脅威の技術的な対応は人員的にもコスト的にも難しい。情報漏洩による利用者への賠償事例も大きな懸念で、利用者から属性を取得、管理することで経営リスクが大きくなるようなら、むしろ所有せずにすむようにサービス自体を見直す方向にいくのではないか、という意見も伺えた。

(D) 自己申告属性の特徴

コミュニケーションサイトへインタビューした結果、利用者(会員)が自己申告で登録する自らの「趣味・興味分野」等の属性の登録には次のような傾向、特徴があることがわかった。

(ア)現実における趣味・興味のすべてを忠実に登録しているわけではなく、選別して、登録している。

(イ)初期登録時に全ての属性を登録するのではなく、利用の過程で、随時追加、変更している

(ウ)趣味・興味として登録した属性が、必ずしも現実の行動にマッチしているとは限らない

(ア)については、サイト内の雰囲気(盛り上がっている話題や発言者の性格など)も影響があるという。例えば、サイト内で「野球」に関する話題が活発な場合は、そうした話題の場に参加したくて、それまで登録していなかった「好きなスポーツ：野球」という属性を追加するようなことがあるという。逆に自分が登録した趣味についての話題が一向にでないような場合は、属性からはずしてしまうことも少なからずあるという。

上記(ウ)に関連するが、現在主流である属性の登録方式(候補項目へのチェックイン、アウト)では、実際にどの程度チェックした趣味や興味分野に思い入れがあるのか計ることができ

ないため、現実に商品の購入などを行う見込みがあるのか判断するのが難しいという。

(E) クローズドコミュニティのニーズ

(a) 実社会のコミュニティの移行

ソーシャルネットワーキングサイトへのインタビューによれば、サイトの使い方として、本来の意図した「新たな友人の開拓や知らない同士のコミュニケーションの場」というよりは、むしろ実社会での友人同士がネット上のコミュニケーションの場として利用しているケースが多いという。特に所属、住居などの変更により現実の生活ではなかなか会えなくなってしまった旧来のグループの利用頻度が高いということである。

例えば、社会人における学生時代の仲間のように、昔なじみだが普段はあまり会えなくなってしまったグループが、ネット内で互いの近況報告をする、共通の話題で盛り上がる、などのコミュニケーションに使用されることが多いという。アクセス時間も夜よりも(オフィスにいる)日中の時間の方がむしろ多いということである。退会についても、個人で入会した会員が中心で、こうしたグループが集団で退会するケースはこれまでのところ見られていないという。

(b) 同じ境遇のコミュニティ

特殊な病気を持つ人や深刻な悩みを抱えている人にとって、同じ立場(境遇)の人同士で相談し合えたり、意見を交換できる場があるのは心強い。ただし、現実には身近にそのような人がいて直接会えるようなケースは限られている。また、自分の名前を公開したり、大勢に顔を知られたくないようなケースもある。

インターネットの普及により、現在上記のような同じ立場の人同士が情報を交換できる仮想の場(コミュニティ)が実現した。実際に様々なサイトが立ち上げられており、今や全国規模で情報交換、交流が行われている。

ただし、こうしたコミュニティでもいくつか新たな課題が発生している。情報交換している相手(投稿者)が、本当に現実社会で同じ立場かどうかがネット内の行動だけではわからない点である。当初は親切な助言をしてくれた人が、後日、薬や器具、壷などの霊感商品などを売り込み、断ると誹謗、中傷を行なうようなケースもあるという。精神的にタフでない人にとって、このような行為は堪えがたく、以後利用を止めたり、インターネットにおけるコミュニティ自体を不審に思うようになる可能性もある。

(4) 今後のインターネットにおける属性活用の可能性

サイト利用者の真正な属性値が取得できることで、これまでに実現が難しかった新しいサービス、ビジネスが実現できないだろうか。これまでの調査により判明した内容を踏まえ、インターネットで実施可能な各種のサービスに共通する属性活用のポイントについて考えてみたい。

(A) 真正な属性のニーズ

現在コミュニケーションサービス(サイト)などでは、利用者の各種属性を公開し、利用者間が互いの属性を確認し合うことで新たな友人関係を作るサービスが現れている。

ただし、このサービスでも現時点では自己申告した属性が基本となっている。このため、登録された属性が真正であるか正確にはわからない。真正な属性が公開され、利用者間が確認し合えるようなサービスはまだ本格的には展開されていない段階ともいえる。もし、簡単な方法で下記ように各種の属性が真正であることを示せるようになれば、これまでにない新しいサービスが実施できる可能性がある。

- 現実社会でどのような容姿、体格をしているか
- どの機関(会社や学校)に所属しているか、または出身か
- 特定の資格、免許を持っているか
- 特定の病気などで通院や治療歴があるか

その一方、属性の真正を確認しなくても十分に事業として成立するサービスも多々あることは忘れてはならない。つまり、既に利用者は、そうした環境を受け入れており、自分が行ないたい用途によってサイトの使い分けができるようになっている。例えば、仮想な人格を登録してコミュニケーションをとる「アバター」などのように完全に別の人格を楽しんだり、インターネットを通じて知り合った人と写真を交換する(あるいはサイトに登録する)など、遊びやスリルを味わう場として活用しているのである。

このように、現在のインターネット環境は真正な属性が必要とされるサービスと、必要がない(少なくてよい)サービスに 2 分化されてきているように見られる。問題は、この区分が理解できている人ばかりではなく、後者のサービスは一部の出会い系サイトのように詐欺やいたずらなどの犯罪に結びつく危険性がある。

真正な属性を取扱うサイトか、虚偽を前提としたサイトかの区別が明確につくようにした上で、どちらのサービスも発展させていければよいだろう。

(B) 属性公開の特典

利用者の住居地域や年代、趣味、興味分野や保有資格、体のサイズなど容姿に関する属性は様々なサイト(企業)にとって、自社の商品の宣伝、案内や販売戦略用のデータとして取得したいものである。

利用者からより多くの属性を提供してもらうためには、利用者が自らの属性を提供することで特典が得られるような仕組みがあるとよいだろう。自らが登録した属性の情報が、他者や企業などから参照されるごとにポイントが加算され、溜まったポイントは商品と交換できるようにすれば、利用者は自分の属性をある種の「商品」として売り込めるようになる。

ただし、サイト毎に同じ属性を何度も登録させるのでは、利用者に過度の負担を強いることになるため、できるだけ 1 度登録した属性を(利用者の許可の範囲内で)共通に使えるような仕組みを作る必要がある。

(C) 属性の真正性の証明方法

インターネットで利用者の属性が真正であるかを判断するには、公的機関や(所属先の)民間企業や学校等が属性の認証局(CA)となり、その機関に登録されている利用者の属性について証明書発行サービスを行なうのが最も理想的である。この方式の場合は確実に真正な属性値が得られるが、認証局の設立や維持には多大な労力やコストがかかるのが難点である。

とろこで、現実世界においては、自分の属性が正しいことを示す証明書などを提示する以外に、『信頼のある第三者から証明(書面や口頭)を得る』という方法もある。インターネットにおける属性を活用するサービスでもこのような方式で十分なサービスが実施できるものは意外に多くあるのではないだろうか。

上記の方式の場合、必ずしも認証局の仕組みは必要ないが、属性登録を受付ける機関の設定や第三者がいかにして証明をするか等、技術的な仕組みや運用の検討が必要である。注意したいのは、この場合、利用者から属性を受付ける機関は、その値が真正であることを「保証」するまではできない、ということである。各属性の信頼性をどのようなレベルで判断してサービスに組入れるかは今後の技術や各サイトの運用次第、ということになる。

(D) リアルタイムの属性値

現実社会における、保有金融資産(預金残高や株式評価額など)や健康状況など時々刻々と変わるような属性を取扱うサービスでは、通常属性の種類により有効期限(調査時点から○○日以内など)が設けられており、その期間内のみでサービスが実施される形がとられている。実際は有効期限内でも属性の内容が大きく変わってしまうこともあり、それが原因で不適切な取引が行なわれてしまったり、詐欺事件が発生するようなケースもでている。

インターネットで属性を取得する仕組みは、このようなリスクを大きく軽減できる可能性がある。値の変化が大きい属性でも、インターネットを使用すれば、相手が要求した時点でのリアルタイム値を瞬時に提示することができる。また、属性の有効範囲や条件を設定しておくことで、その条件にあてはまらなくなった場合に、警告や取引を無効化するようなシステムが現れることも期待できる。

(E) 所属証明が必要な場面

今回の調査やインタビューの結果、現行のインターネットのサイトやアプリケーションには利用者の所属先や職位などを活用するサービスが意外に少ないことがわかった。

企業など団体所属情報については、所属先以外に照会するサービスは見受けられなかった。サービスを広げるには、所属先の会社が、所属者の情報を自社以外に証明することで特典が得られるような仕組みがないか検討する必要があるだろう。

また、自営業や営業地域が限られている中小規模の企業に勤務する人の場合、現実社会でも自分の所属を他者に示すような場面が少ない。従って、こうした利用者の所属について現実社会には見られない新たに活用の場面やアプリケーションを使うメリットについて十分に検討していく必要があろう。

(F) 新しい種類の属性

現実社会では取扱われていない、また価値あるものとしてみられていないような種類の属性がインターネットでは重要になるようなことも考えられる。

例えば、特定の利用者がインターネットへどの場所(自宅、ネットカフェなど)からアクセスしているか、というデータは現実社会では利用価値は高くないが、インターネットではアクセス先サイトにとって非常に重要なデータの１つである。

また、「現実社会における行動」を第三者が証明することでこれまで実現できなかったサービスの実現が可能になる。特定の時間、場所で特定の人がアプリケーション操作を実施したことが証明できれば、これまでインターネットでは替玉操作対策が難しかった各種の遠隔試験などのビジネスなどが可能となろう。

その他、写真や身長、体格(体形)などの属性は、コミュニケーションサイトや食品、化粧品関係等の会社に有償で提供できる価値を持つ属性といえるだろう。

(G) 属性のマーケティングへの活用

利用者の属性と商品購買の相関を分析することで効果的なマーケティングが期待できる一方で、インターネットならでは特有の行動パターンには注意する必要がある。

例えば、現実社会の場合なら通常、スーパーマッケットなど１つの店で一度に複数の商品を購入するので、商品の陳列順序や同時に購入されやすい商品などを分析すればよいことになる。しかし、インターネットにおけるネットショッピングの場合、利用者は１つのサイトで複数の種類の商品を「まとめ買い」するよりは、「特定の商品」のみを丹念に調べ、複数のサイトごとに種類や価格を比較し購入を検討する傾向がある。ポータルサイトへのインタビューによると、旅行や不動産(購買、賃貸)については特にこの傾向が顕著であるという。

このため、ショッピングサイト(モール)内のみの行動(操作)と利用者の所有属性の相関を分析しても、期待する結果(「この属性の人はA商品の購入の後に、B商品を購入する傾向がある」など)は得にくいかもしれない。

これに対し、複数の同系列のショッピングサイト間やポータルサイト間などで特定の利用者の属性を共有し、購買行動パターンなどを分析することが可能ならば、実際の行動に則した質の高いマーケティングデータが得られそうである。

異なるサイト間で、どのように利用者属性を共有していくか、というのは今後の属性活用の鍵になるのではないだろうか。

(H) 他サイトとの差別化戦略としての属性活用

ポータルサイトなどでは、会員向けに価値のある情報や機能の提供を有料で実施しているところがある。

利用者から真正な属性を取得し、必要に応じて提供するという一連のサービスは、これまでのインターネットサービスにはないものであり、他の関連するサービスと連携できる機能として有料サービス化することも可能ではないだろうか。

例えば、ネットオークションの出品者の氏名や住所が真正であることを落札者が事前に確認で

きれば、詐欺などの被害を軽減することが可能になる。また、「荒らし」の起き難いコミュニティ(会議室、掲示板等)を設営することも可能になるだろう。

(1) 属性活用サービス実施主体

利用者の真正な属性を取得し、様々な用途に活用するサービスは、本来は現実社会で既に同様の業務を実施している公的機関(市役所、登記所等)が行なえれば利用者からも支持が得られやすい。しかし、現行の社会情勢から、こうした新たな基盤整備にはクリアしなければならない諸所の課題があり、早期実現は厳しいと思われる。

それでは民間機関を中心とした基盤作りは可能であろうか。現実社会においては民間機関においても下記のように利用者の属性を証明しているケースが既にある。

(ア) 所属先の機関が発行する証明書などを必要に応じて提出する
例： 所属・職位、保有資格、卒業大学、学業成績

(イ) その他取引等がある民間企業等が発行する証明書などを必要に応じて提出する
例： 預金残高、健康状態

こうした機関に加え、3.6.3 に示したように、信頼ある第三者の証明を着けた属性の登録を受け付ける新たな機関を設立すれば、民間機関主導で取引相手として必要な属性を確認できるサービスが実現できると思われる。むしろ、公的機関よりも民間機関主導で基盤を作っていく方が、利用者の抵抗も少なくてよいかもしれない。(国や自治体などが、こうした基盤整備に取り掛かると、すぐに国民総背番号制などが連想されがちである。)

(5) 属性活用のための共通基盤の展望

平成 15 年度に取りまとめた報告書「属性情報利用システム－2010 年の市民生活－」では、インターネットの各サイトが共通に利用者から収集した属性を利用できる図 参考 3-2 のような「属性情報活用のためのサービスレイヤーモデル」を提案した。

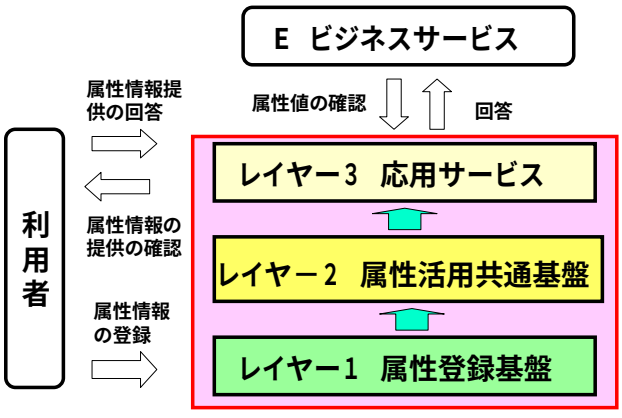


図 参考 3-2 属性情報活用のためのサービスレイヤーモデル

このモデルは、インターネット上において共通基盤の利用者から得た真正な各種の属性を集積し、必要に応じての任意のサイトに対し必要な属性情報を配信するというものである。

このモデルではインターネットで実現するサービスでは、利用者の属性が真正であることが最重要ととらえていたが、本年の主要サイトにおける調査等から、現行のサービスサイトでは下記のように必ずしも属性が真正であることが絶対条件ではなく、現行の仕組みでも活用されている分野もあることが判明した。

- 属性の真正性を担保する方法として、直接現実社会の証明書を取り付ける以外の方式で運用できているビジネス分野がある。
- 利用者の属性が真正でないことが前提でも、業務に大きく支障をきたすことなく成立しているビジネス分野がある。

これらをイメージしたものを図 参考 3-3 に示す。

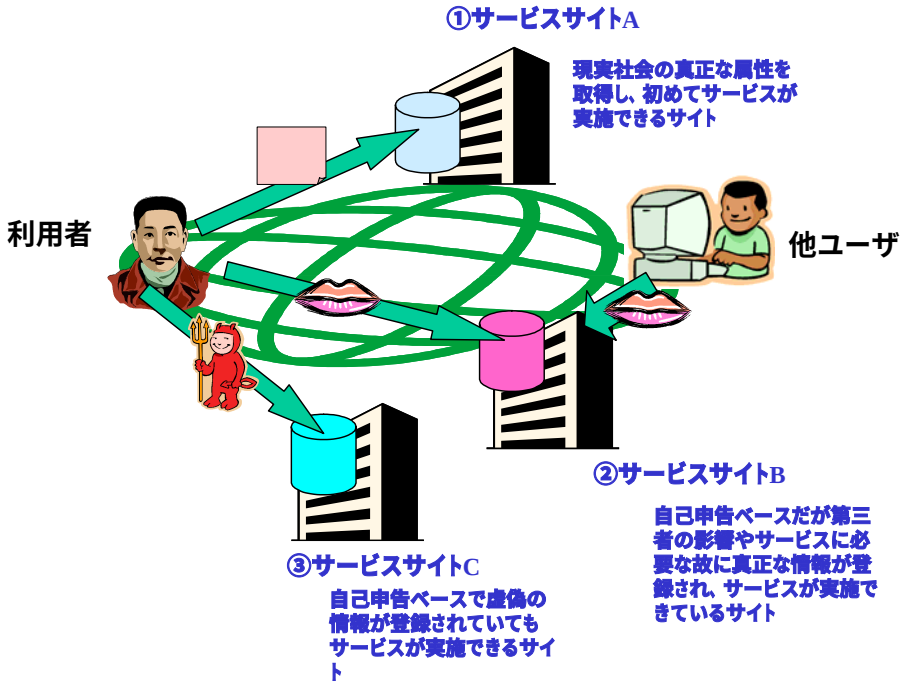


図 参考 3-3 現行のサイトにおける利用者の属性の利用のされ方

平成 15 年度に示したモデルは図 参考 3-3 のうち、①、②のサービスの質を向上させるのに役に立つものであると思われる。ただし、現行の方式でもサービスが成立していることから、現行方式に取って代わるものではなく、当分は併用されるものと思われる。

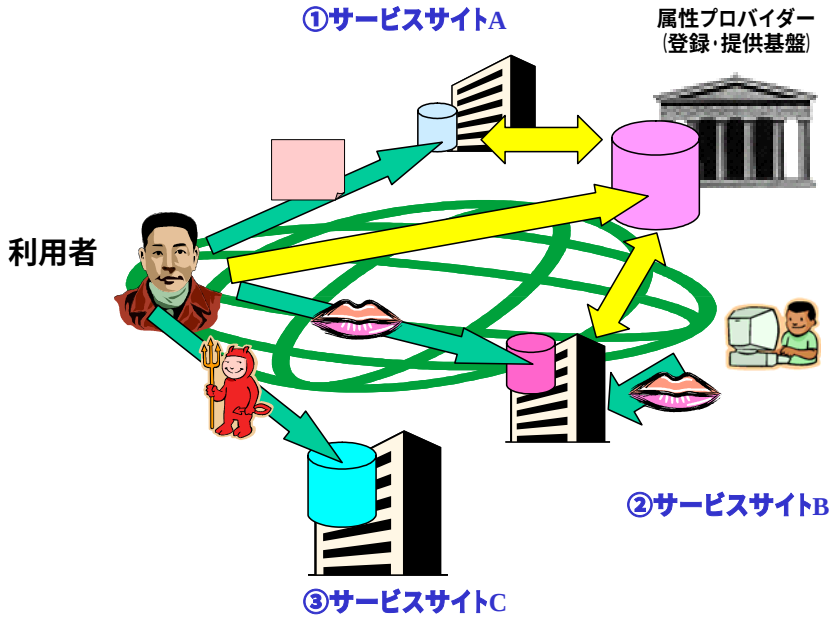


図 参考 3-4 属性情報プロバイダーを介するサイトの属性の利活用イメージ

なお、今年度、複数のサイト運営先へのインタビューの結果、このモデルに関して実務的な視点から次のような指摘を受けた。

- 利用者属性をサイト間共通で使用できるという点についてはメリットが大きい。しかし、業界により利用する属性の種類や、十分に管理、監視可能なサイトは限られており、初めから適用対象を全サイトとするのは困難ではないか。
- サイト側だけでなく、利用者(登録者)側にもこれまでなかったような便利さや割得さを実感できるようなメリットを強く出す必要があると思われる。

こうした意見を踏まえると、属性共通基盤を一斉に展開する施策はあまり得策でない。現実的な展開としては、業種・分野の特徴や現行の動向などを踏まえて、次章に示すように、ビジネス分野毎に特に必要性の高い属性を中心に中心的なサイトが真正性の高い属性を収集、管理し、他サイトと連携しながら属性を供与、共有化するような展開がよいように思われる。(図 参考 3-5)

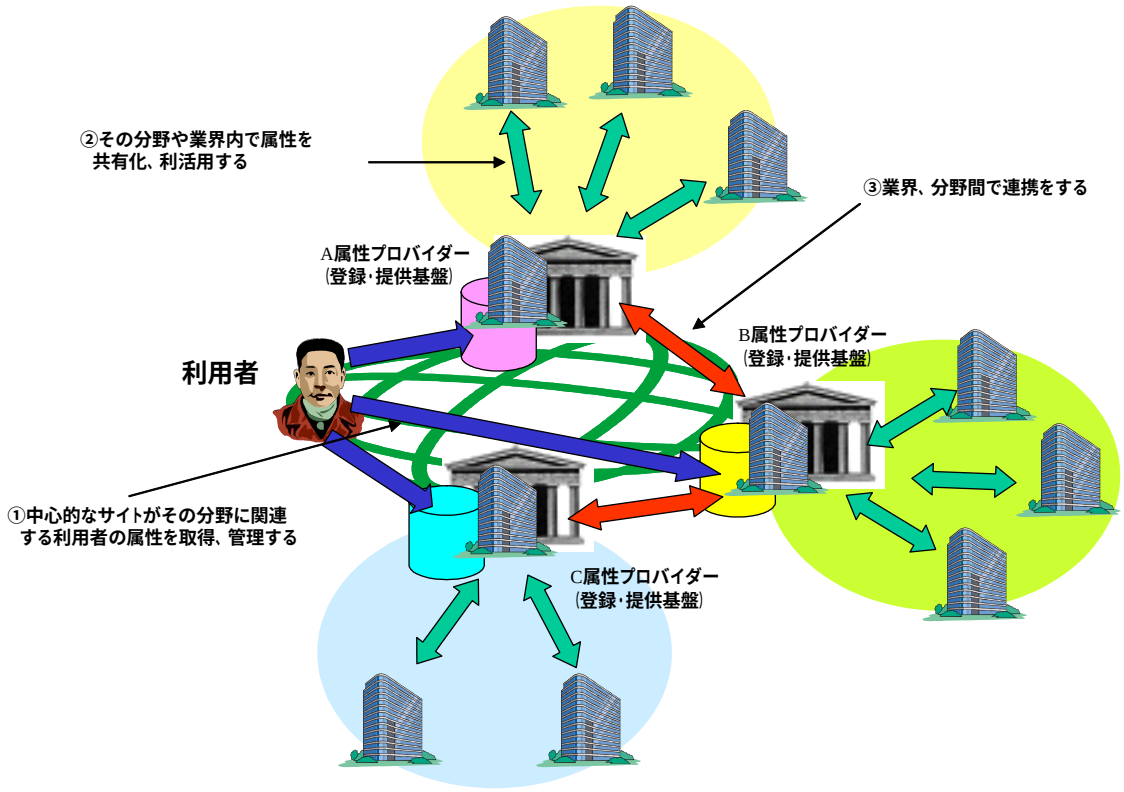


図 参考 3-5 属性活用展開イメージ

(6) 属性活用サービスの展開シナリオの提案

前章の指摘を踏まえ、実務的な視点から「属性情報活用のためのサービスレイヤーモデル」を構築し、普及促進していくのに適切と思われるサービス分野や展開の手順を考察し、いくつかの展開シナリオを示してみたい。

(A) 可能性のあるサービス分野

(ア)ポータルサイトからの展開

ポータルサイトは、現在、インターネット利用者に最も利用されている分野の１つであり、斬新なコンテンツや機能が利用者に受入られやすい要素をもっている。既に様々なサービス機能を自ら所有していると同時に、各種分野のサイトと連携し、一部機能や情報共有が実現している。このことより、まずポータルサイトが会員登録時の付加機能として、真正属性を収集する窓口となり、連携先のサイトに対して会員の属性を提供する方法が考えられる。

(イ)マッチングビジネスサイトからの展開

結婚相手紹介、就職支援、不動産売買等、膨大なエントリ数の中から条件に合う相手を見つける作業は非常に困難なことが多く、通常はある程度、希望する条件に合う候補相手を選別(絞り込む)した上でベストの相手を探す方式がとられている。このような分野では本人に代わって選別や候補先を紹介するマッチングサービスも盛んである。

属性情報活用のためのサービスレイヤーモデルによりマッチングが必要とされる複数のサービス分野が連携して、必要な情報を取り出す、または登録するような仕組みができれば、これまでサイト毎に作られていた利用者データベースが不要となる可能性がある。

(ウ)コミュニケーションサービスからの展開

ソーシャルネットワーキングサイトのように、サイト利用者(会員)が、他の利用者に自らの属性を公開することで新たなコミュニケーションが始まったり同じ属性を持つ利用者間でコミュニティを掲載されるような分野は、利用者の属性が真正であることが非常に重要である。

現時点では自己申告による属性登録が主流であるが、相手を確認する際に、公的、民間機関からの証明書が取り付けられていたり、属性の内容を証明するような根拠が示してもらえらば、これまで利用を敬遠していたような層にも安心してサイトを利用してもらえるようになると考えられる。

(エ)マーケティングサービスからの展開

複数のショッピングサイトが、特定の利用者の属性と行動データをマーケティングデータとして共通的に利用できるようにするものである。利用者には属性を提供してもらう見返りに、提供時に一定の特典ポイントが与える他、その属性の参照や属性を通じたダイレクトメール発信数に応じてポイントが加算されるものである。

(オ)ISP サービスからの展開

一般利用者のインターネットへアクセス環境を提供する ISP(インターネットサービスプロバイダー)は、もともと利用者から基本的な属性(氏名、住所、電話番号など)が提供されている上、利用料の徴収などで定期的に現実社会における利用者と連絡がとれる企業である。こうしたサービスを既に実施できていることは属性活用サービスを行なうには非常に有利な立場にあるといえ、ISP を起点とした展開も有望と考えられる。

(カ)教育機関からの展開

大学、高等学校等の教育機関も元より多くの所属者、卒業生の属性情報を所有している機関である。特に大学は最終学歴の場かつ研究機関であることから卒業後でもなんらかの関わりをもっていることが多い。このため、1 人の利用者に関し、最も多種類かつ長期間の属性を所有している機関ということもできる。⑤の ISP と同様、すでにこうした仕組みがあることは属性活用サービスを行なうには非常に有利な立場にあるといえる。近年、大学においても独自の収益モデルや他大学との差別化が求められていることから、大学が在籍生や卒業生の属性活用サービスを行なうという展開も期待できると考えられる。

(B) 展開具体手順例

ここでは、前節の(ア)ポータルサイトからの展開について、具体的な属性活用のための基盤の構築、展開の手順を示してみたい。

① 属性登録レイヤーの構築

ポータルサイト自身が、利用者(会員)の真正な属性を受け付けるサービスを実施する。サイト会員のうち希望者から会員登録した基本情報(氏名、住所、生年月日)を証明する資料(免許証、住民票)を郵送してもらい、会員 ID に関する属性を確認する。また、必要に応じて、社員証や学生証(または卒業証明書)の写しなども受付け、本人の写真や出身校、勤務先などの属性を確認する。

② ポータル内機能・メニュー間での共有・活用

ポータル内の商品交換サービスやコミュニケーションサイト等で、①で登録した属性を共有・活用する。具体的には、購入した商品の配送先や登録者の許可のもと別の利用者からの要求に応じて登録されている属性を照会する。

③ ポータル提携サイト間での共有・活用

ポータルと提携しているネットショッピングサイトや仕事探しサイトに、利用者からのリクエスト(商品購入や利用申込など)に応じて①で登録した属性うち、必要な情報だけを送信する。また、逆にこうしたサイトから要求があった場合に、アクセス者のプロフィールの統計情報を送信する。(属性登録者には参照に応じてポイントがつく特典をつける)

④ ポータルサイト間での共有・活用

信頼ある別のポータルサイトと提携し、利用者が商品検索などで途中から違うサイトを利用しても必要な属性を送信する。

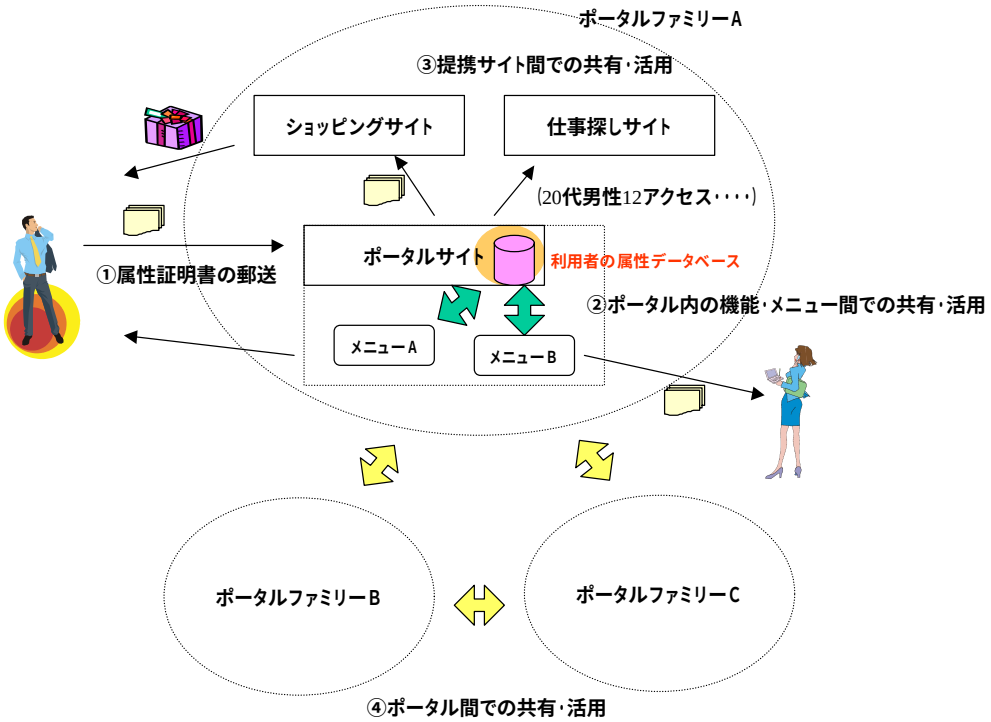


図 参考 3-6 ポータルサイトからの展開イメージ

(7) 属性活用にむけての実務面の課題

(A) 属性利用サイトの監査

利用者の属性を取扱う機関にとって、その属性を提供する相手(企業)を監査、監視する仕組みは非常に重要である。利用者が十分安心して自分の属性を預けられる仕組でなければ、利用者はあえて共通的に属性を利用するようなリスクはとらず、直接利用したいサイトにのみ、自分の情報を登録することを選ぶだろう。

属性活用の機関が取扱っている利用者の数や所有情報量も重要である。利用者の数や利用できるサイトの数が一定レベルを越えられれば、双方側が利用価値を認め、さらにサービス種類や登録者の数が多くなる好循環が生じるであろう。

(B) 複数機関への属性登録と集約

前章で示したように、属性を活用する基盤は１つ機関がすべてのサービスモデルへ提供を行なう方式ではなく、分野を限定した複数の機関が設立され、徐々に連結・統合していくという展開の方が現実的である。

このため、当初は利用者の属性は複数の機関に散らばることになり、場合によっては同じ種類の属性が散在することもありうる。この場合、同じ属性でも内容やその真正を証明する根拠が異なるようなことも在り得るため、ネットに登録されている属性を集約する仕組みや証明方法の格付けの仕組みなども必要となってこよう。

(C) 属性の提供範囲とアクセス権

利用者本人以外への属性内容の提供は、属性の種類によっては提供(開示)範囲が非常に難しいものがある。

例えば、病状や健康状況の情報などは家族に限っても一律に開示というわけにはいかないものである(息子にはいいが、嫁や兄弟には見せたくない、など)。また、病状と健康状況では、そもそも開示したい目的が異なっており、個々の属性ごとに提供してよい範囲やアクセス権を定められるようにする必要がある。

(D) ネット上の脅威への対応

インターネット上のコミュニケーションで危険視されていることに、アクセス者が(若い)女性ということが判明した場合、公開された電子メールアドレス向けに、いやがらせやからかいを目的とした大量の電子メール(メール爆弾)が、その人向けに行なわれ、事実上、そのアドレスが使用不可能になってしまうことがある。電子メールのような個対個のコミュニケーションの場合は、サイトでの制御は行なえないため、電子メールアドレスは提供や開示対象としない、などのより細かな配慮、機能設計が必要である。

また、利用停止要求についても速やかに応じる必要がある。要求があったにもかかわらず、属性の開示、提供サービスが続くことは法的にも問題となるため、要求時はもちろんのこと、長期

間サイトへの利用がないような場合にも、属性の開示、提供の停止を検討するのがよいと思われる。

［参考サイト］

YAHOO! JAPAN	: http://www.yahoo.co.jp/
goo	: http://www.goo.ne.jp/
楽天	: http://www.rakuten.co.jp/
アマゾン	: http://www.amazon.co.jp/
リクナビ	: http://www.rikunabi2005.com/
Yahoo! オークション	: http://auctions.yahoo.co.jp/
goo リサーチ	: http://research.goo.ne.jp/
トモモト	: http://www.tomomoto.net/index.cgi
ソニー銀行	: http://www.moneykit.net/
マネックス証券	: http://www.monex.co.jp/
DCS(給与配信)	: http://www.dcs.co.jp/products/prosrv_index.html
明治大学(実証実験)	: http://www.between.ne.jp/a-univ/gp/meiji/
健康サービス(実証実験)	: http://www.medis.or.jp/2_kaihatu/file/sendai.pdf

メンバーリスト

事務局

前田　陽二	電子商取引推進協議会(ECOM)	主席研究員
川松　和成	電子商取引推進協議会(ECOM)	主席研究員

顧問

大山　永昭	東京工業大学　教授
菅　　知之	関西大学　　教授
平田　健治	大阪大学　大学院　教授

編集メンバー

氏名	会社名
武藤　　裕	NTT コミュニケーションズ株式会社
岩崎　公寛	株式会社 NTT データ
古田　健一	共同印刷株式会社
鈴木　優一	セコム株式会社
漆島　賢二　＊＊	セコム株式会社
佐藤　雅史	セコム株式会社
佐藤　永子	セコム株式会社
海川　正洋	株式会社帝国データバンク
古賀　祐匠	日本電信電話株式会社
千葉　昌幸	株式会社三菱総合研究所
坂上　　勉　＊＊	三菱電機株式会社
本山　信久	三菱電機株式会社
鍛冶　俊彦　＊	株式会社日本電子貿易サービス
有馬　純一郎＊	三菱電機情報ネットワーク(株)
谷口　展郎　＊	NTT 情報流通プラットホーム研究所

(注)　＊　はオブザーバ　　＊＊はリーダ

SWG1. 2 メンバー(上記以外)

氏名	会社名
横井　雅彦	NTT コミュニケーションズ株式会社
石津　晴崇	NTT コミュニケーションズ株式会社
関野　公彦	株式会社 NTT ドコモ
黒木　美和	株式会社損害保険ジャパン
菅野　健司	株式会社帝国データバンク
浜田　　誓	電気事業連合会
小林　智恵子	株式会社東芝
島　　成佳	日本電気株式会社
冨田　清次	日本電信電話株式会社
井上　晴司	日本ベリサイン株式会社
下江　達二	富士通株式会社
冨高　政治	富士通株式会社
糸岡　　崇	富士電機ホールディングス株式会社
田中　　稔	三菱電機株式会社
増井　久之　＊	香川大学
東山　栄一　＊	NEC ソフト株式会社
篠崎　政久　＊	株式会社東芝

(注)　＊　はオブザーバ

平成 16 年度　経済産業省　受託事業
EC 技術基盤の相互運用性に関する調査研究
(取引相手先の属性認証技術等の調査)
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～
平成 17 年 2 月発行

発行所　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園三丁目 5 番 8 号
機械振興会館　3 階
TEL：03(3436)7500
印刷所　　新高速印刷株式会社
東京都港区新橋五丁目 8 番 4 号
TEL：03(3437)6365

この資料は再生紙を使用しています。