

日本がモデルにしたオーストリア 電子政府と今後のID連携

Austrian e-Government that Japan Uses as Model and Future ID Linking

● 鈴木尊己

あらまし

2015年10月から、社会保障・税番号制度(マイナンバー制度)によるマイナンバーの付番が開始され、2016年1月からマイナンバーカードの交付が開始された。2017年10月からは情報提供ネットワークシステムの運用が始まり、マイナンバーカードを利用した情報提供等記録開示システム(マイナポータル)などのサービスや、自治体間などの行政機関の間で所得情報や資格情報などの個人情報の連携が開始される。個人情報保護の観点からはセキュリティの強化が必要となるが、利便性の観点からは市民サービスの向上、行政事務の効率化など、幅広い分野でのマイナンバーカードの利活用が望まれる。諸外国でもマイナンバーのような個人の共通IDを発行し、行政サービスにおいて様々な方式で利用・運用されている。そこで重要となるのが、個人の共通IDの管理方式とID連携方式である。

本稿では、セキュリティを担保しつつ利便性向上を図るには、どのような仕組みが望ましいのか、日本がモデルとしたオーストリア電子政府のID管理とID連携の仕組みを紹介するとともに、現在のID連携の考え方と今後のID連携の方向性について述べる。

Abstract

In October 2015, assignment of My Numbers as a national identifier based on the Social Security and Tax Number System (My Number System) started, and this was followed by the start of issuance of My Number Cards in January 2016. In October 2017, operation of the Cooperation Network System for Personal Information is scheduled to start, and it will initiate services including the Disclosure System of Personal Information Cooperation Record using the My Number Cards (Mynaportal) and linking of personal information such as income information and qualification information between municipalities and other administrative agencies. From the viewpoint of personal information protection, strengthened security is required. From the perspective of convenience, however, utilization of the My Number Cards in wide-ranging fields is desired for purposes including improved resident services and more efficient civil services. In some foreign countries, single IDs of individuals similar to the My Numbers are issued for use and operation in a variety of ways in administrative services, where the system of management of single IDs of individuals and the system of ID linking are the key. This paper presents the systems of ID management and ID linking of the e-government of Austria, which has been used by Japan as a model, from the perspective of what kind of system is desired for improving convenience while ensuring security. It also describes the concept of ID linking and the future direction of ID linking.

ま え が き

個人のID管理のモデルとしては、ドイツなどが採用するセパレートモデル、エストニアなどが採用するフラットモデル、そしてオーストリアなどが採用するセクトラルモデルの3体系が存在する。

セパレートモデルは、行政サービス分野ごとに異なるIDを管理し、それぞれの情報は相互に利用できない方式となっている。したがって共通のIDは存在しない。これは、個人情報保護の観点では利点となるが、「消えた年金問題」などに代表される情報連携に関わる問題が発生する可能性がある。

フラットモデルでは、一つの共通IDを全ての分野で利用し、効率的に情報連携できる。一方で、IDの漏えいやなりすましなど、個人情報保護の面で危険性があるため、法律面や運用面で制御が必要となり、そのための連携基盤の構築が求められる。アメリカでは、社会保障分野をベースに社会保障番号（SSN：Social Security Number）が導入されているが、様々な分野で利用されており、フラットモデルと言える。韓国、スウェーデン、デンマーク、ベルギーなど多くの国がこのモデルを採用している。

セクトラルモデルでは、セパレートモデルと同様に行政サービス分野（セクター）ごとにIDを管理する。業務別の個別IDが分野共通IDとひも付けられ、分野間での情報連携の際には分野共通IDをほかの分野共通IDに変換して情報を連携するため、各分野では共通IDそのものは利用されない。これについての詳細は後述する。

日本におけるマイナンバー制度の仕組みは、これら三つのモデルを組み合わせた方式となっている。例えば、マイナンバーの利用範囲に関しては、法律によって税と社会保障の分野に限定したセパレート方式としている。一方で、税の申告などのために民間企業や健康保険組合など広範囲にマイナンバーが利用されている点は、フラット方式に近いとも言える。ただし、その利用範囲は法律で限定され、厳格な管理体制となっている。そして、情報連携やマイナポータル利用ではマイナンバーは一切利用されないため、マイナンバーの漏えいなどが発生しないセクトラル方式となっている。そのID連携の方式は、オーストリアで採用されて

いる方式をモデルに検討され、情報提供ネットワークシステムの仕組みが構築されている。

本稿では、オーストリアの個人ID制度の仕組みとそのID管理方式、および現在のID連携と今後の方向性について述べる。

オーストリア電子政府の概況

オーストリアは人口870万人（2016年）、外国人は30万人、国土面積は8.4万km²であり、約2,350の基礎自治体（13州80区）から成っている。国土としては北海道程度の広さで、人口は神奈川県程度である。2003年から電子政府戦略をスタートし、これまで連邦政府CIOや連邦政府ICT委員会、連邦政府電子政府事務総長などを中心に活動していた電子政府の推進体制を官民一体の組織に変革し、2004年に各国に先駆けて電子政府法を制定した。そして、2006年に電子政府Digital Austriaが発足した。

2006年以降では、EUの電子政府ランキング1位となり、2010年にはEUの中で電子政府の見本と呼ばれるようになり、オーストリアの輸出産業の一つとなっている。そして2014年には、公共サービス提供分野でUnited Nation Service Awardを受賞した。また現在では、Vision 2020として更なる利便性の向上、一貫したユーザーインターフェースの向上、セキュアな個人や企業の電子IDの強化、そしてe-Government, e-Health, e-Justice, e-Learning, e-Commerce, e-Environmentの融合を目指している。⁽¹⁾ 推進体制としては、大統領府にDigital Austriaを設置し、そのCIOをグラーツ工科大学のReinhard Posch教授が務めている。

電子政府の成功は、ひとえに政府CIOのPosch教授によるところが大きく、コンセプトに基づいてDigital Austriaの仕組みの構築をトップダウンで推進したところにある。筆者が2011年にオーストリアに視察で訪れた際も、財務省などの様々な機関で仕組みについて説明を求めると「詳細についてはPosch教授に話を聞いてくれ」と言われ、教授に話を伺うまで全体の仕組みは分からなかった。強力なリーダーシップによる調整と共同作業の結果、信頼性とセキュリティの確保、互換性と標準化の推進、透明性と効率化の追求、市民中心のG2C（Government to Citizen）の実現など、成功を取

めていると言える。

オーストリアの付番体系

オーストリアにおいても、日本と同様に以前から税番号、社会保障番号、住民登録番号などの業務別管理番号が存在し、現在も使用されている。この中で、約2,350の自治体で管理されていた住民登録番号が内務省で中央住民登録簿のCRR (Central Residence Register) 番号として一元管理され、生涯不変の共通IDとなった。また外国人に対しては、SR (Supplementary Resister) 番号が同様に内務省で管理されている。⁽²⁾

ウィーンやザルツブルグなどの大都市では、独自の住民記録システムで出生などの情報を管理している。内務省のCRRシステムとはXMLを用いて連携することでCRR番号を付番し、氏名、性別、生年月日の個人情報を管理している。大都市以外は1万人にも満たない自治体がほとんどであるため、CRRシステム専用のGUIによって連携している。CRR番号の付番と並行して出生届けが社会保険機関 (SVC) に通知され、社会保障番号 (SVNR) が付番される。

オーストリアにおけるCRR番号は日本の住民基本台帳ネットワークの住民票コードに相当する。しかし、中央住民登録簿以外の公的機関のデータベースへの登録は禁止されているため、SVCではCRR番号を管理できない。公的機関の共通IDの管理と情報連携は、CRR番号 (あるいはSR番号) を

基に変換した分野別番号を管理して行っている。このため、オーストリア方式はセクトラルモデルと呼ばれている。

具体的には、まずCRR番号から暗号化処理によりICカードなどに格納される個人認証用の電子識別番号 (SourcePIN) を生成する。このSourcePINと、利用できる26の業務分野コード (表-1) を連結してハッシュ変換 (SHA-1) することによって、分野ごとのssPIN (sector-specificPIN) を生成する。この生成を行うのが、第三者機関であるデータ保護委員会 (Austria Data Protection Commission, ドイツ語の略称でDSK) である。

DSKは連邦政府や州の代表など6名で構成されており、法制度に沿ったアクセス制御ポリシーの制定、情報連携の申請の許諾、情報連携のログの管理、および監査などを実施している。例えばSVCでは、社会保障番号の付番後に「業務分野コード」「氏名」「性別」「生年月日」をDSKに問い合わせる。DSKは、CRRシステムに氏名、性別、生年月日を送付してCRR番号の通知を受け、業務分野コードを使ってssPINの生成を行い、SVCに通知する。SVCは、そのssPINと社会保障番号をひも付けて管理する。財務省や統計局なども同様にssPINを取得している。

オーストリアの情報連携体系

DSKはSourcePIN Register Authorityとして機関の間の情報連携の仲介を行い、分野ごとのssPINの変換によりデータ連携を実現している。

表-1 情報連携対象の26業務分野

No	識別子	業務分野	No	識別子	業務分野
1	AR	ビジネス関係	14	LV	国防 (兵役, 軍隊の費用動員)
2	AS	公式統計	15	RT	メディア, 電気通信
3	BF	教育と研究 (学校他の教育研究機関)	16	SA	税金や関税
4	BW	建設および住宅 (住宅補助, 下水道接続)	17	SF	スポーツとレジャー
5	EA	EUと外務省	18	SO	安全と秩序 (危機管理, 市民保護など)
6	EF	輸入と輸出許可, 税関	19	SOVR	協会登録
7	GH	健康 (社会保障系, 葬儀関連)	20	SRRG	犯罪歴
8	GS	地域社会サービス (社会集団, 消費者保護)	21	SV	社会保障 (失業保険, 健康保険, 傷害保険, 年金保険)
9	GSRE	返還事務	22	UW	環境 (廃棄物管理, 自然と景観の保護)
10	JR	公証人, 弁護士, 民事裁判権など	23	VT	輸送と技術 (交通警察, テクニカルサービス)
11	KL	文化 (教会, 宗教的なコミュニティ)	24	VV	資産管理
12	KU	芸術資金提供, 保全	25	WT	エコノミー (試験機関, 産業, エネルギー)
13	LF	農林業 (農業補助金, 畜産)	26	ZP	アイデンティティと市民権 (パスポート, 選挙)

具体的には、機関Aが機関Bに情報提供を依頼して入手する情報連携の流れは、以下のとおりである。

- (1) 機関Aは、対象者の氏名、性別、生年月日と期間Aが保有するssPIN (ssPIN-A)、業務分野コード、および連携対象機関の業務分野コードをDSKに送信する。
- (2) DSKは、受け取った氏名、性別、生年月日をCRRシステムに送信し、中央住民登録簿の中の該当者のCRR番号を受領する。該当者が複数存在する場合には、全員のCRR番号が送信される。
- (3) DSKは、受領したCRR番号からSourcePINを生成し、更にssPINを生成する。生成されたssPINをssPIN-Aとマッチングし、対象者のCRR番号を特定する。
- (4) そのCRR番号から機関BのssPIN-Bを生成し、暗号化して機関Aに通知する。
- (5) 機関Aは、暗号化されたssPIN-Bを入手し、機関Bに問い合わせる。
- (6) 機関Bは暗号化されたssPIN-Bを復号し、情報検索して結果を機関Aに送信する。

SourcePINやssPINの生成は不可逆暗号化方式のため、このような仕組みとなっている。SourcePINは本人所有のICカードにのみ保存が許されるため、DSKにおいてもDBに保存することは禁止されている。ssPINは分野別番号であるため、同一分野内においては同一のssPINが格納されて税番号や社会保障番号とひも付けされており、情報検索はその番号が使われる。

日本の場合に当てはめてみると、CRR番号が住民票コード、SourcePINがIDコード、ssPINが符号に該当するが、符号は分野別の管理ではなく、自治体などの行政機関ごとの管理となっている。また、日本では氏名が単純なアルファベットではなく、様々な字体を持つ漢字などによって住民基本台帳が管理されている。このことから、オーストリアで採用されたマッチング方法では本人の同定が不可能であるため、可逆暗号化方式によって情報提供ネットワークシステムで符号の変換が行われている。なお、日本ではオーストリアと同様に符号変換は行いが、機関別符号やIDコードがDBに格納されることはない。ただし、ログなどの管理用符号はその限りではない。

オーストリアの市民ポータルサイト

オーストリアの大統領府が管轄している市民ポータルサイトは、1997年に公開された。このポータルサイトへのアクセスをよりセキュアな方式とするため、2009年にDigital Austriaのプラットフォームが開発され、ICカードのみに格納されたSourcePINと分野別番号のssPINを利用したオーストリア方式の連携方式が確立された。ICチップを搭載した市民カードによる認証のほかに、ワンタイムパスワードを利用したMobile Phone Signatureによる認証方式も用意されている。2013年の11月には、市民ポータルサイトの利用者は1,000万人を超え、アクセス数も2009年の2倍以上の4,000万件を超えている。また、200以上のライフイベントで350以上の手続きが可能であり、出生、運転免許、パスポート・査証、自動車関連、税関連、年金関連などの利用が多い。

社会保障ポータルサイトや税ポータルサイトなどに接続する際に、ICカード内でSourcePINをそれぞれのssPINに自動で変換する方式となっている。これによって、ポータルサイトではssPINから社会保障番号や税番号に変換して必要な情報を取得できる。実際のID連携の仕組みについては、次章で紹介する。

Digital Austria ID連携のアーキテクチャー

本章では、まずDigital AustriaのID連携を理解するための前提となるアイデンティティの概念およびID連携の基礎を解説し、Digital AustriaのID連携のアーキテクチャーについて説明する。

● アイデンティティの定義

Digital Austriaにおけるアイデンティティは、単なる一意の識別子のみを指すわけではない。アイデンティティ情報とは、以下の三つの構成要素から成る。⁽³⁾

(1) 識別子

人や機器、プログラムやデータなどの対象とするオブジェクトを認識・特定するための情報を識別子と呼ぶ。識別子は、対象とするオブジェクトごとに割り付けるのが通常である。

(2) クレデンシャル

認証を要求するオブジェクトを概念的に主体と

呼ぶが、こうした主体やデータそのものの正当性を示す情報のことをクレデンシャルと呼ぶ。ID管理技術において、クレデンシャルは個人のアイデンティティを一意に識別するために認証システムに提示する情報の意味で利用されることが多く、識別と認証に用いられるセキュリティの根幹となる情報である。クレデンシャルの具体例としては、パスワード、X.509証明書や指紋、静脈といった生体情報などが挙げられる。

(3) 属性情報、プロフィール情報

主体またはデータのような対象となるオブジェクトの属性を表す情報の集合が、プロフィール情報である。例えば、人のプロフィール情報には、氏名、住所、生年月日、性別といった静的な属性情報や、GPSで観測される位置情報などの動的な属性情報がある。また、消費者としては、過去の購買動向から分析された情報もプロフィール情報である。

人間の場合のアイデンティティの概念を図-1に示す。

● ID連携

単一ドメイン内でのWebシングルサインオンから、複数の異なるドメイン間（例えば、複数の異なる組織が運用するクラウド間）での連携シングルサインオンに至る、様々な認証を実現するためのオープンな仕様が策定されている。このように、ドメインAのIDによるログイン後に、別のドメインBのサービスが利用できる連携シングルサインオンのことをID連携と呼ぶ。ID連携のオープン

な仕様の代表的な例としては、SAML (Security Assertion Markup Language)やOpenID Connectが挙げられる。ID連携の概念を図-2に示す。

● Digital Austriaのクライアント型モデル

Digital Austriaのアイデンティティにおけるセクショナルモデルは、図-3に示すクライアント型モデルをベースに実装されている。

e-IDカードの適格証明書 (Qualified Certificate)を利用して利用者を認証後、SAMLによるID連携機能を使うことで、市民カードによって身元保証された認証機能の利用が可能になる。すなわち、民間のサービス事業者は、電子政府の認証基盤を利用してサービスを提供できる。

オーストリアのクライアント型モデルに対して、日本の情報提供ネットワークシステムのアイデンティティにおけるセクショナルモデルの実装は、サーバ型モデルである。また、セクショナルモデルに基づいたID連携は、情報提供ネットワークシステムではサポートされていない。サーバ型セクショナルモデルの概念を図-4に示す。

今後のID連携の方向性

企業では、オンプレミス環境（イントラネット）とパブリッククラウドとの間をID連携させることによるシングルサインオンでサービス利用が可能な運用が拡大している。図-5は、オンプレミス環境から他社のクラウドのパブリックサービスをSAMLによるID連携で利用する事例である。

最近では、FUJITSU Partner Cloud Service for

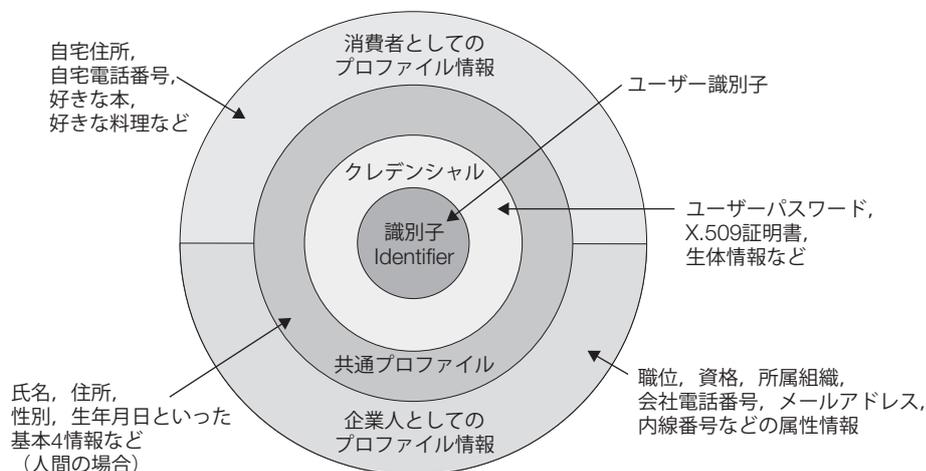


図-1 アイデンティティの概念

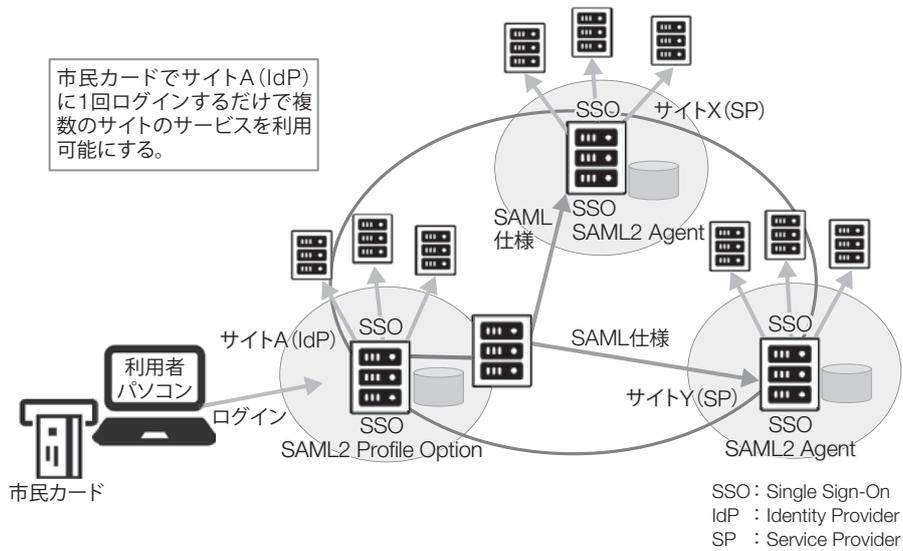
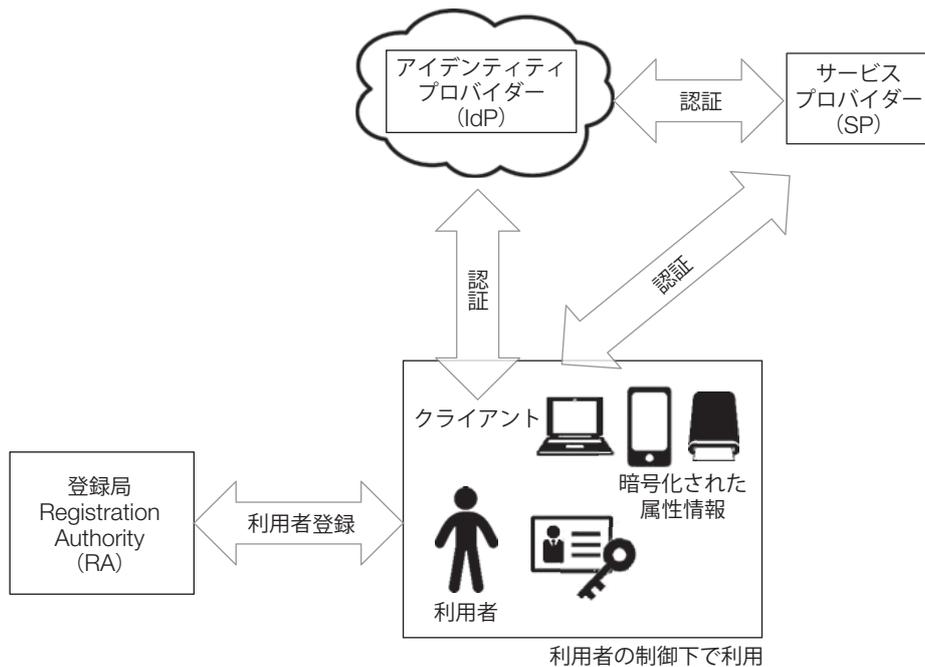


図-2 SAMLによる ID連携の概念

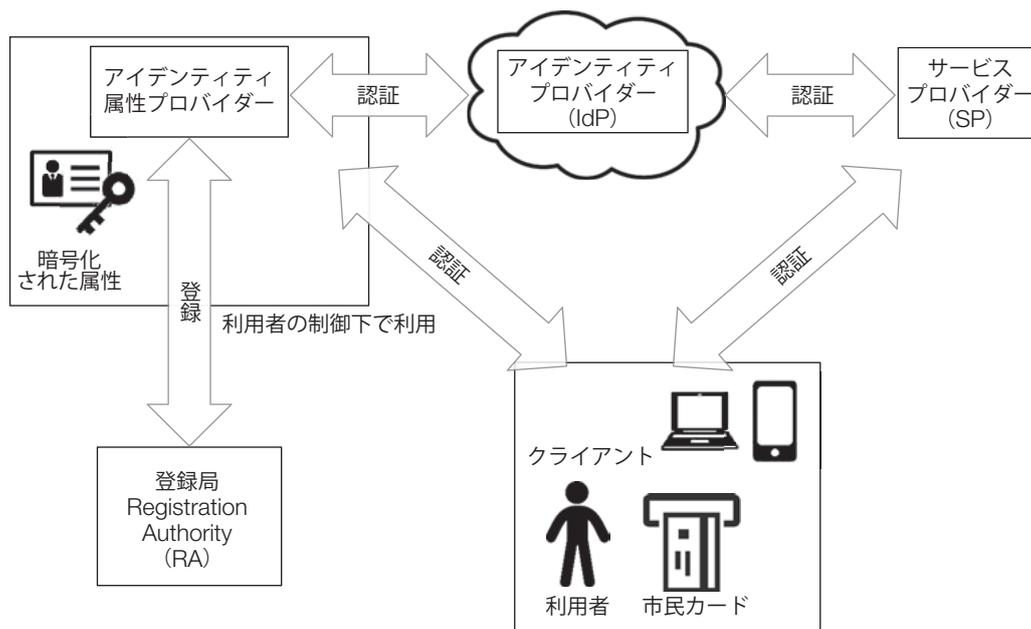


出典 User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosureで掲載の図を基に作成

図-3 Digital Austriaのクライアント型モデルの概念

Microsoft Azure⁽⁴⁾やFUJITSU Cloud Service K5⁽⁵⁾といった、パブリッククラウドのPaaS (Platform as a Service)上のWeb API(Application Programming Interface)で提供されるサービスを利用する際にも、ID連携の protocols である OpenID ConnectやOAuthを利用する運用が急速に増加している。今後、アプリケーションやIoT

(Internet of Things) 利用などのマルチクラウド環境におけるクラウド間連携でも、ID連携を基盤技術として利用した運用が急速に拡大していくと予測されている。将来、電子政府の厳格な本人確認を利用することで、セキュリティを確保した官民のID連携に基づくサービス利用が進展していくと考えられる。



出典 User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosureで掲載の図を基に作成

図-4 サーバ型セクトラルモデルの概念

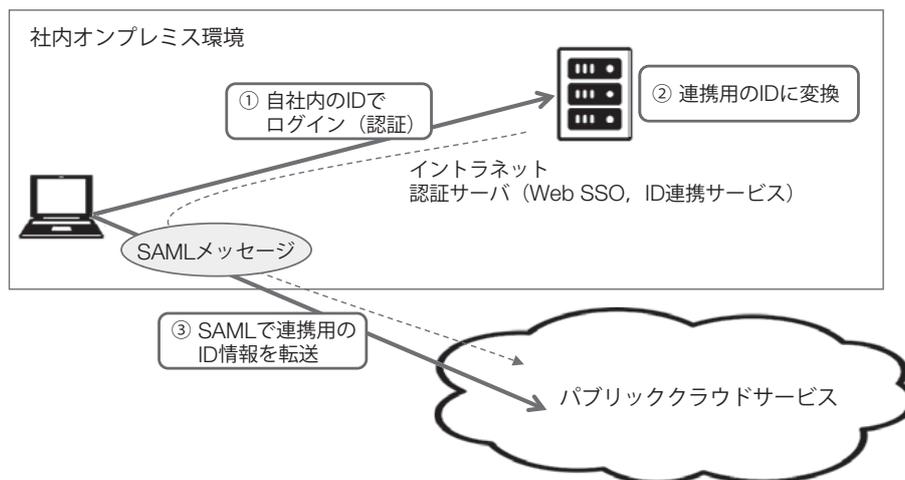


図-5 パブリックサービスのID連携運用事例

む す び

日本のマイナンバー制度は、情報提供ネットワークシステムでの情報連携の仕組みにおいて、オーストリアと同様にセクトラルモデルを採用しているが、実装方式は異なっている。一方でID連携という観点からは、日本の電子政府やマイナポータルでもオーストリアの電子政府と同様に、将来官民連携においてID連携の運用が拡大していくと予想される。

また、幅広いマイナンバーカードの利活用推進のためには、現在検討されているマイキープラットフォームや医療等IDなど様々な分野においてもID連携の利用が見込まれる。今後、ID連携を基盤技術とした制度設計や運用の仕組みづくりが必要となる。そのため、総務省の「個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会」の「制度検討サブワーキンググループ」では、ID連携、トラストフレームワークの在りかたの検討が2017年3月より開始されており、日

本でも電子政府におけるID連携の制度設計が始まっている。

参考文献

- (1) The ABC guide of eGovernment in Austria.
Austrian Federal Chancellery, Federal Platform
Digital Austria, May 2014.
- (2) 前川 徹：国民ID 導入に向けた取り組み。NTT出版,
2009年。
- (3) 下江達二：アイデンティティ管理関連技術の進展
と変遷。人工知能学会誌, Vol.24, No.4, p.504-511
(2009)。
- (4) 富士通：FUJITSU Partner Cloud Service for
Microsoft Azure.
<http://jp.fujitsu.com/solutions/cloud/iaas/azure/>
- (5) 富士通：FUJITSU Cloud Service K5.
<http://jp.fujitsu.com/solutions/cloud/k5/>

著者紹介



鈴木尊己 (すずき たかみ)

行政システム事業本部
第一ソリューション事業部
個人番号の付番、情報連携業務に従事。