

高齢化社会に向けた安心・安全なデジタル社会のあり方の 一検討

柿崎 淑郎^{1,a)} 前田 陽二² 辻 秀一³

概要：高齢化社会が進むにつれて高齢者がインターネット等のデジタル社会に参画する機会が増していく。一方で、高齢者は加齢に伴う記憶力・判断力の低下があり、様々なトラブルに遭遇する可能性が高くなる。本稿では、このような高齢化社会において、高齢者を様々な脅威から守るための安心・安全なデジタル社会のあり方について検討し、その結果を報告する。

A consideration of ideal way of safe digital society for aging society

YOSHIO KAKIZAKI^{1,a)} YOJI MAEDA² HIDEKAZU TSUJI³

1. はじめに

国民一人ひとりに番号を付与し、個人情報管理を効率化する流れが諸外国では一般的であり、アメリカの社会保障番号 (SSN)、エストニアの国民 ID 番号 (The Estonian identification code) などがよく知られている。特にエストニアは先進的であり、電子投票、受験、医療、税などの幅広い分野で利用されている。一方、日本では「行政手続における特定の個人を識別するための番号の利用等に関する法律」[1]、いわゆる「マイナンバー法」が2015年10月に施行され、2016年1月からマイナンバー制度が始まる。マイナンバー制度は社会保障と税における諸問題を解決することを目的としており、2015年9月にはマイナンバーの利用範囲を預金口座や特定健康診査に拡大した改正案^{*1}が可決成立したが、IT先進諸外国に比べて、未だに遅れを見せている。

海外では政府系サービスなどのインターネット活用が進

んでおり、今後日本でも政府系サービスのインターネット利用が普及すれば、多くの国民がインターネットを利用することになる。そのような状況では、ITリテラシが必ずしも高くない若年者や高齢者の利用増加が避けられない。そのため、悪質なサイトでフィッシングの被害にあったり、誤操作などによるトラブルが起きたり、インターネット上の脅威に晒されたりすることで、利用者の不安感が高まると考えられる。

また、IT化は高齢者の利便性を向上させる目的がある一方で、ITリテラシがないが故に、利用することができないというジレンマを抱えているため、老若男女問わず誰もが利用できるようにアクセシブルデザイン^{*2}に配慮する必要がある。ITリテラシが高くない利用者に対してのセキュリティやプライバシー対策も、このバリアフリーの考え方は重要であり、今よりも安全にインターネットを利用できる仕組みが必要となる。

総務省の情報通信白書^{*3}によれば、平成24年末において、60～64歳のインターネット利用率は71.8%であり、50～59歳は85.4%である。つまり、5～10年後には60歳以上の8割以上がインターネットを使うことが予測される。厚生労働省によれば、65歳以上の認知症有病率は

¹ 東京電機大学
Tokyo Denki University

² 日本・エストニア/EU デジタルソサエティ推進協議会
JEEADiS

³ 東海大学
Tokai University

^{a)} kakizaki@im.dendai.ac.jp

^{*1} <http://www.cas.go.jp/jp/seisaku/bangoseido/ichibukaisei.html>

^{*2} <http://www.meti.go.jp/policy/economy/hyojun/kijyun/>

^{*3} <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc243120.html>

10%程度と推定されており、また、加齢とともに有病率が上昇することが指摘されており、2020年までには認知症患者数が325万人まで増えることが予測されている^{*4}。

健康なうちにインターネットを使い始めたものの、将来にわたっては加齢による認知症が懸念され、正しい判断が行えなくなった後においても、インターネットを利用することが予想される。そのような状況下においては、例えば利用しなくなった有料サービスを契約したままになったり、判断の低下から不必要なものを購入したり、個人情報のみだりに公開したり、インターネットを利用した振り込み詐欺等の犯罪に巻き込まれたりなどの、セキュリティ・プライバシーの問題が顕在化するものと考えられる。よって、安心安全にインターネットを利用するためには、これらの利用者を支援する成年後見人のようなエージェントが必要であると考えられる。

インフラ技術における支援技術や自動化技術は、ITSやスマートメータなどの他分野では普及期に入り始めているが、インターネット分野ではまだ普及しているとはいえない。現時点においては、まだその必要性は高くないが、今後行政サービス等のオンライン化が進み、多くの情報がインターネットでやり取りされ、多くの人が利用できるようになれば、エージェントによる支援無しではユーザのインターネット活動が困難になることが予想される。

本稿では、このような状況を基据えて、リタイア世代を中心に、60歳以上のパソコン利用者層をターゲットにして、それらの利用者を様々な脅威から守るための安心・安全なデジタル社会のあり方について検討し、その結果を報告する。

2. 高齢者への対応

2.1 実社会での対応

2.1.1 成年後見制度

認知症、知的障害、精神障害などの理由で判断能力の不十分な人を支援する仕組みとして成年後見制度がある。成年後見制度は大きく法定後見制度と任意後見制度に分けられる。

法定後見制度では、家庭裁判所によって選ばれた成年後見人等が、本人を代理して契約などの法律行為をしたり、本人が同意を得ないで行った不利益な法律行為を取り消したりすることによって、本人を保護・支援する。

任意後見制度では、判断能力が不十分になった際に備えて、本人に十分な判断能力があるうちに、財産管理についての代理権を任意後見人に与える契約を公正証書で結んでおくものである。本人の判断能力が低下した後に、家庭裁判所が選任する任意後見監督人の監督の下で、任意後見人が本人を代理して契約などをすることによって、本人の意

^{*4} http://www.mhlw.go.jp/kokoro/speciality/detail_recog.html

思に従った適切な保護・支援が可能となる。

2.1.2 みまもりサービス

2015年4月、日本郵政グループとAppleとIBMが業務提携し、iPadを利用して高齢者の生活サポートサービスを2016年度から本格展開すると発表した^{*5}。日本郵政グループは全国2万4000カ所の郵便局を拠点に、IBMとAppleで開発した新しい高齢者向けの専用アプリ及びタブレット等を配布して、それらを活用した各種のネットサービスや郵便局社員等によるリアルな生活サポートサービスを支援し、「みまもりサービス」の拡充を計画を示している。

生活サポートサービスは、以下の3つの価値を提供している。

- (1) みまもられているという「安心」
- (2) 生活をサポートしてもらえるという「便利」
- (3) 地域・社会との「つながり」

またサービスコンテンツとして、次のようなサービスを提供予定としている。

- ICTの利活用を併用した「みまもりサービス」
- 親世代向け・子世代向けの「コミュニケーションサービス」
- 自宅での申込みによる「買い物支援サービス」
- 自治体と連携した「地域情報サービス」
- 各種相談サービス

2.1.3 らくらくホン

らくらくホンはNTTドコモが展開している高齢者層をターゲットにした携帯電話端末シリーズである。人間工学に基づき設計された万人に使いやすいデザイン、装備、機能が特徴であり、開発は主に富士通によって行われている。シリーズ累計販売台数は2014年時点で2500万台を突破している。

らくらくホンはボタンを最小限にするなどのハードウェアの工夫だけではなく、見やすい文字や聞きやすい音声などのソフトウェアの工夫も行っており、ハードウェアとソフトウェアの両面から使いやすい携帯電話端末となっている。

また、富士通はらくらくホンのノウハウを元にして、欧州の中でも高齢化が進んでいるフランスでの製品展開を2013年から行っており、国外でも成功を収めている^{*6}。

2.2 ネット社会での対応

Facebookは利用者が亡くなった場合に、その家族や友人からのリクエストに応じて、故人のアカウントを追悼アカウントに変更する機能を用意している。さらに、生前に追悼アカウント管理人を設定^{*7}することもできる。追悼

^{*5} <http://www.japanpost.jp/pressrelease/jpn/2015/20150430109906.html>

^{*6} <http://www.j-cast.com/2014/01/08193706.html?p=all>

^{*7} <http://ja.newsroom.fb.com/news/2015/05/adding-a-legacy-contact/>

アカウント管理人を設定する際に、写真や投稿などのアーカイブのダウンロードを許可するかどうかを設定できる。また、追悼アカウントに切り替えることなく、アカウントを削除することも選択できる。

Google はアカウントが一定期間使用されなくなった際に、そのアカウントを削除するアカウント無効化管理ツール^{*8}を提供している。あらかじめ設定したタイムアウト期間にログインがなかった場合に、アカウントを削除する機能を有するほか、信頼できる連絡先を設定することで、その人にアカウントデータを共有することもできる。共有されるアカウントデータはサービス毎に設定可能であり、また信頼できる連絡先に対して遺言のようなメッセージを設定することもできる。Google アカウントは Android 端末をはじめ、インターネットでは広く普及している。アカウント無効化ツールによって、かなり広範囲のデータ資産を死後にどのようにするかを生前に制御することができる。

一方で、多くの Web サービスはこのような対応を準備していない。そのため、死後に限らず、老齢期においてインターネットを利用しなくなった際に、アカウントが削除されたり、Web サービスから退会されたりせずに放置されることで、アカウント乗っ取りによるなりすましなどの脅威にさらされ続ける。

また、ネット社会では実社会とは異なる問題も起こりえる。寝たきりや認知症になり、金融機関に行けなくなった場合でも、実社会であれば委任や委譲がしやすいが、ネット社会では容易ではない。オンラインバンキングであれば、どの金融機関を利用しているか、口座番号・パスワードは何かという情報を見つけることが困難であり、本人から聞き出すことも難しいかもしれない。さらに、多くの金融機関で採用されている二要素認証（二段階認証）の場合、本人のスマートフォンを操作する必要があるなど、第三者への委任や委譲が難しい現状がある。

3. 目指すべき社会・姿

3.1 マイナンバー制度

マイナンバー法 [1] は「効率的な情報の管理及び利用並びに他の行政事務を処理する者との間における迅速な情報の授受」「便益の提供を受ける国民が、手続の簡素化による負担の軽減、本人確認の簡易な手段その他の利便性の向上を得られるようにするために必要な事項を定める」（第一条）を目的としている。利用範囲は「行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者」（第九条）に限定されており、広く民間利用に開放されているものではないが、基本理念においては、「他の行政分野及び行政分野以外の国民の利便性の向上に資する分野における利用の可能性を考慮して行われなければならない」

（第三条第二項）とされている。2015 年 9 月に可決された改正では、マイナンバーの利用範囲を預金口座や特定健康診査に拡大することが盛り込まれている。また附則第六条には、「この法律の施行後三年を目途として、この法律の施行の状況等を勘案し、個人番号の利用及び情報提供ネットワークシステムを使用した特定個人情報の提供の範囲を拡大すること並びに特定個人情報以外の情報の提供に情報提供ネットワークシステムを活用することができるようにすること」とあり、将来的には民間利用への拡大が期待される。

マイナンバー制度の概要を図 1 に示す。図 1 中の情報提供ネットワークシステムが、情報提供を許可して符号同士を紐付けており、各情報紹介・提供機関はそれぞれ異なる符号を自らが持つ利用番号と紐付けて処理を行う。また、マイナポータルを通して、各個人は自己情報を確認したり、情報提供記録を確認したり、各種サービスを利用することとなっている。なお、執筆時点において、マイナポータルは 2017 年 1 月からの運用が予定されている。

高木らはマイナンバー法では規定されていない情報連携基盤について、プライバシー保護とセキュリティ技術の観点から番号連携機能の合理的な技術的方式を提案している [3]。文献 [3] で提案されている方式は、情報連携基盤における番号変換テーブルを用いることで、別分野への拡張も考慮している。

3.2 世界最先端 IT 国家創造宣言

2015 年 6 月 30 日に首相官邸から「世界最先端 IT 国家創造宣言」^{*9} が示された。第 II 部では「目指すべき社会・姿」として、以下が示されている。

- (1) IT 利活用の進化により未来に向けて成長する社会
社会全体の IT 利活用を加速させるために、制度的、技術的環境の進展に伴った枠組みの構築について、新たな法律の制定も視野に検討を行い、法制上の措置等を講ずる。
- (2) IT を利活用したまち・ひと・しごとの活性化による活力ある社会
地方に「しごと」をつくり、「ひと」を呼び込み、それを支える「まち」につながる社会環境を構築することで、人口減少に歯止めをかけ、多様な地域社会を形成していく。
- (3) IT を利活用した安全・安心・豊かさが実感できる社会
障がい者や高齢者などの情報弱者を含む全ての国民が健康で安全・安心に暮らせるユニバーサルな新たな社会システムを構築し、様々な社会的課題の解決が図られることを具体的に実証するとともに、企業の事業改革や事業化へのチャレンジを通じて、経済性・利便性

^{*8} <https://www.google.com/settings/u/0/account/inactive>

^{*9} <https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20150630/siryoul.pdf>

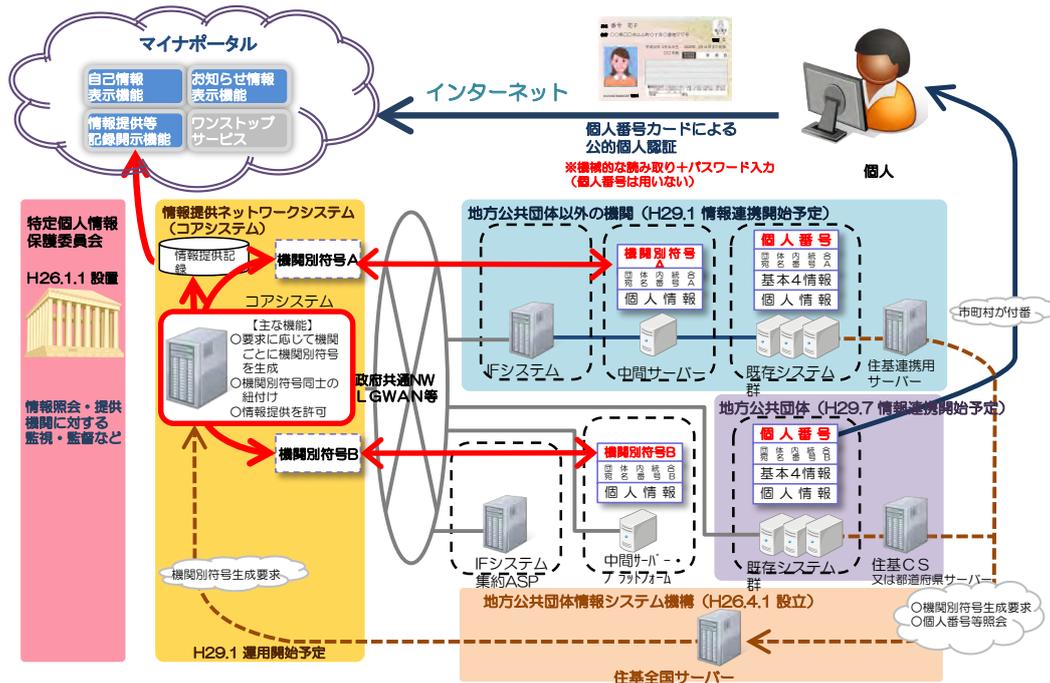


図 1 マイナンバー制度の全体像 (文献 [2] p.5 より引用)

の高い新しいサービスを創出することにより、健康で安心して快適に生活できる、世界一安全で災害に強い社会を実現する。

(4) IT を利活用した公共サービスがワンストップで受けられる社会

全ての行政サービスが電子的に受けられることを原則とし、クラウド及びマイナンバー制度の徹底活用により、オープンで利便性の高い公共サービスを提供し、電子行政サービスがワンストップでどんな端末でも受けられる「便利なくらし」社会を実現する。

また、第 III 部では「目指すべき社会・姿を実現するための取組」として、個別具体論が述べられている。

「IT を利活用した安全・安心・豊かさが実感できる社会」を実現するための取組として、「効果的・効率的で高品質な医療・介護サービスの展開」が挙げられている。具体的には、利用者の実態に即した適切な医療・介護や生活支援サービスを提供するために多様な主体が情報共有・連携を行うこと、医療機関の窓口において医療保険資格をオンラインで確認できるシステムを整備すること、個人が自らの医療・健康情報を一元的・継続的に管理すること、患者自身が服薬情報をいつでも・どこでも入手し、薬局薬剤師等から適切な服薬指導等を受けられることなどを挙げている。

「IT を利活用した公共サービスがワンストップで受けられる社会」を実現するための取組として、「個人番号カード

の普及・利活用の促進」が挙げられている。この中では、個人番号カードのキャッシュカードやクレジットカードとしての利用、健康保険証やその他行政が発行する各種カードとの一体化、各種免許等における各種公的資格確認機能の付与、ATM 等からのマイナポータルへのアクセス実現、住民票等のコンビニ交付などが挙げられている。「マイナポータル」の構築・利活用では、官民連携による官民の証明書類提出や引っ越し・死亡等に係る行政手続きのワンストップ化などが挙げられている。

EU においても A Digital Agenda for Europe^{*10} として同様の文書が公開されており、以下の 7 つを課題として挙げている。

- (1) 断片化しているデジタルマーケット
- (2) 相互運用性の欠如
- (3) ネットワークにおけるサイバー犯罪の増加と低信頼のリスク
- (4) ネットワークへの投資不足
- (5) 不十分な研究とイノベーションの努力
- (6) デジタルリテラシとスキルの欠如
- (7) 社会の課題に対処する機会の逸失

4. 高齢者支援シナリオ

ここでは、現実により得る状況を想定したシナリオに基

^{*10} [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R\(01\)](http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01))

づいて、現状を分析し、理想的な解決策を考察する。

4.1 シナリオ 1：引っ越しの手続き

住民票の移動には転出元の役所へ転出届を提出し、転出証明書を発行してもらい、それを転入先の役所へ転入届とともに提出する必要がある。住基カードを用いる場合、転出証明書が不要になるが、転入手続きは必要である。転入手続きが行われると、転入先での住民票が発行できるようになる。

運転免許証の記載事項変更には、新住所へ送付された消印付はがき、公共料金の領収書などの新住所を確認できる書類等が必要だが、すぐに変更したい場合は住民票を用いることが一般的である。

住所変更を一括で行える引越れんらく帳^{*11}がある。しかしながら、日本全国が対応しているわけではなく、個別に手続きを行う必要もある。

引越時の主な住所変更先として、電気、水道、ガス、電話、通信、金融、クレジットカード、保険、新聞、通信販売などが挙げられる。郵便物の転送には郵便局への転居届が必要であり、宅急便転送にはヤマト運輸への申込みが必要である。

解決策

このように、引っ越しに伴う手続きは煩雑である。一箇所で、例えば住民票移動を行えば、住所変更が全ての箇所で一括して変更されることが望ましい。

4.2 シナリオ 2：医療費助成申請

ある日、男性はひどい体調不良により内科を受診したところ、診断結果は厚生労働省指定難病であり、即時入院となった。男性は入院中に医療ソーシャルワーカーより、指定難病は特定疾患医療受給者証（以下、医療券）を申請することで、医療費助成を受けられることを知らされた。医療費助成は、生計中心者の所得税額によって、自己負担額上限が定められ、それを超過した分についての助成を受けられる。

医療券の申請には、臨床調査個人票、住民票、課税証明書などを市区町村窓口で申請する必要がある。臨床調査個人票は難病指定医が記入し証明した診断書である。住民票と課税証明書は市区町村窓口等で発行が必要となる。

男性は退院前に臨床調査個人票を受け取り、3ヶ月後に退院し、医療券申請を行った。男性の申請は受理され、医療券が交付された。医療券の有効期間の開始日（申請日）から医療券が届くまでに支払った医療費等は還付請求が可能であるが、発症日あるいは確定診断日から申請日までに支払った医療費等は還付対象ではなかった。

解決策

男性は医療ソーシャルワーカーから医療費助成があることを知らされなければ、当該制度があることを知る由もなかった。そのような助成制度がある場合、必要になった時点で受動的に知らされるべきである。また、指定難病であることが確定診断された段階で、医療券申請が可能になるので、医療機関から直接申請できる仕組みがあるべきである。医療券の申請においても、申請先は市区町村窓口であり、住民票と課税証明書の発行も部署は異なるが同じ市区町村窓口であるので、内部での情報連携でワンストップに行われることが望ましい。申請日から医療券が届くまでに支払った医療費等も、係る医療機関等と情報連携し、自動的に還付される仕組みが期待される。

4.3 シナリオ 3：フィッシングサイトへの誘導

男性の元に金融機関からの電子メールが届いた。マイナンバー法施行に伴い、マイナンバーの登録が必要という内容であった。男性はメールにあったリンクをクリックし、リンク先へ遷移した。リンク先は日頃利用している金融機関のサイトと同じ見た目であったため、IDとパスワードを入力してログインし、画面の指示に従ってマイナンバーを登録した。

直後に、金融機関から振込受付の電子メールが届いた。ここで男性は先ほどのリンク先が偽サイトであり、IDとパスワードをフィッシングされたことに気がついた。

解決策

金融機関を騙るフィッシング行為は現在においても、多く報告されている。フィッシングとは、金融機関などを装った電子メールを送り、口座番号、クレジットカード番号、住所、氏名、電話番号などの個人情報を取る行為である。このシナリオでは、男性の利用しているオンラインバンキングのIDとパスワードが詐取され、攻撃者はただちにそのIDとパスワードを利用し、正規のオンラインバンキングへログインし、男性の口座から攻撃者の口座に送金することで、金銭をだまし取ったものである。

IEやChrome、Firefoxなどのブラウザではアンチフィッシング機能があり、フィッシングサイトを検知してブロックすることができるが完全ではない。金融機関によっては、リスクベース認証や二段階認証、トランザクション認証などによって、不正ログインや不正送金を防止する施策を実施しているが、利用は任意のこともあり、また対応していない金融機関もある。

パスワードマネージャはIDとパスワードを管理し、入力欄に自動入力したり自動ログインしたりする機能を持つソフトウェアである。パスワードマネージャを利用していれば、見た目が同じクローンサイトであっても、ドメイン名が異なっていれば自動入力されないため、偽サイトであることに気がつくことができる。

^{*11} <http://www.hikkoshi-line.jp/>

4.4 シナリオ 4：判断力低下による危機

男性は会社では仕事熱心に勤め上げたが、定年退職による反動で、認知症を患いつつある。会社員時代から休日の楽しみはネットショッピングであり、今でもネットショッピングを楽しんでいる。

ある時、男性の妻は預金残高が大きく減っていることに気がついた。調べてみると、クレジットカードによる引き落としが多額であった。このクレジットカードの使用者は男性であり、この件について男性に尋ねたところ、覚えがないとのことだった。クレジットカード明細を確認したところ、確かに購入した商品が届いており、なりすまし使用などではないことが確認できたが、男性は同じ商品を何度も購入していたことが分かった。さらに、1度利用したものの、その後は一切利用していない Web サービスが解約されておらず、毎月の使用料を請求されていることが発覚した。

解決策

認知症などによって判断力が低下している場合における異常行動について気付ける仕組みが必要である。物理的な物を購入している場合は第三者でも気が付くことができるが、電子マネーや Web サービス利用料などの電子的な購入物は第三者では容易に気が付くことができないため、なんらかの方法でそれらの情報を得る方法が望まれる。Web サービス等の定期的な契約更新については、使っていない不要と思われるサービスを無駄に契約更新しないだけでなく、活用しているサービスの契約更新をし忘れることへの気付きも重要になる。これらを管理し、利用者に知らせる仕組みが求められる。

5. 安心・安全なデジタル社会のあり方

本稿では、我々の興味と関心および本稿の主目的から、「世界最先端 IT 国家創造宣言」の「目指すべき社会・姿」(3)と(4)について取り扱う。

マイナンバー制度により、行政手続きのワンストップ化はマイナポータルで実現されることが期待される。行政手続きのワンストップ化あるいは自動化が実現すれば、利用者の負担は減り利便性は大きく向上する。マイナンバーの民間利用は将来的には計画されており、現在においても様々な専門家によって検討・議論が行われている。

本稿では、これらの現状を踏まえた上で、本稿で想定する環境を図2に示す。

5.1 構成要素

情報ポータルサイト

情報ポータルサイトはアイデンティティプロバイダ、属性プロバイダを内包し、インタフェース機能を通じて、外部アイデンティティプロバイダ、属性提供機関、サービスプロバイダなどと連携し、ユーザのネット活動を集約管理

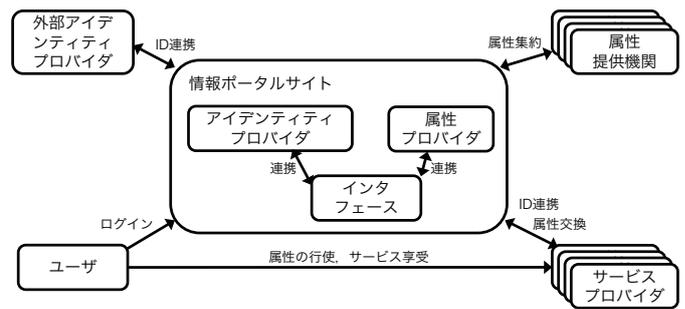


図2 想定する環境

して支援する。

アイデンティティプロバイダ

アイデンティティプロバイダはアイデンティティ連携の中核を担うプレイヤーである。アイデンティティプロバイダはユーザが信頼する任意の外部アイデンティティプロバイダと連携する。外部アイデンティティプロバイダとアイデンティティ連携することで、自らが管理するデジタルアイデンティティの本人性確認を行い、さらに属性プロバイダと連携することで、ユーザの属性をサービスプロバイダに提供する。

属性プロバイダ

属性プロバイダはユーザの属性情報を集中管理するプレイヤーである。属性プロバイダはアイデンティティプロバイダとアイデンティティ連携し、ユーザの属性を各属性提供機関から集約し、管理する。属性プロバイダは必要に応じて各属性提供機関と通信し、最新の属性が反映されるように、管理を行う。属性プロバイダはユーザが許可した範囲内で、アイデンティティプロバイダが要求する属性を開示する。

サービスプロバイダ

サービスプロバイダはユーザにサービスを提供するプレイヤーである。サービスプロバイダはアイデンティティプロバイダとアイデンティティ連携し、アイデンティティプロバイダから提供される属性に基づいて、ユーザにサービスを提供する。

ユーザ

ユーザはサービスプロバイダのサービスを利用しようとするプレイヤーである。ユーザはアイデンティティプロバイダにユーザ登録を行い、自らが信頼する外部アイデンティティプロバイダとアイデンティティ連携させることで、その本人性を証明する。ユーザは自らの属性を証明する属性提供機関からその属性を属性プロバイダに集約させ、サービスプロバイダの属性要求に伴い、必要な属性を属性プロバイダからサービスプロバイダに開示するよう要求する。

外部アイデンティティプロバイダ

外部アイデンティティプロバイダは民間企業などが運営し、複数存在するプレイヤーである。ユーザは複数ある外部

アイデンティティプロバイダから、自らが信頼する外部アイデンティティプロバイダと情報ポータルサイト内のアイデンティティプロバイダを連携させて情報ポータルサイトを利用する。

属性提供機関

属性提供機関はユーザの属性を証明することができるプレイヤーである。ユーザの属性を証明できるのは限られた機関だけである。例えば、「学生」属性を証明できるのは、その学生が属している大学だけである。そのため、属性提供機関は属性に応じて複数存在する。属性提供機関はユーザからの要求に伴い、属性プロバイダに属性を集約させる。

5.2 情報ポータルサイト

情報ポータルサイトはアイデンティティプロバイダ、属性プロバイダを内包し、ユーザがサービスプロバイダを利用する際に、ユーザとサービスプロバイダの間を仲介し、ユーザのネット活動を集約管理し、必要に応じてユーザを支援する。

ユーザが情報ポータルサイトを經由して、サービスプロバイダを利用することで、情報ポータルサイトは、いつ、どのサービスプロバイダと、どのような情報をやり取りしたかを集約管理することができる。また、情報ポータルサイトが持つアイデンティティプロバイダの機能により、ユーザはシングルサインオンで様々なサービスプロバイダを利用することができる。さらに、情報ポータルサイトが持つ属性プロバイダの機能により、サービスプロバイダが必要とする属性、例えばメールアドレス、住所、性別などを提供することができる。また、ユーザの属性値が変更になった際も、サービスプロバイダへの属性提供は情報ポータルサイトを介して行われるので、情報ポータルサイトで属性変更を行えば、全てのサービスプロバイダに波及させることができる。

我々は、このような情報ポータルサイトのインタフェースとしての役割を担い、ポリシーやルールに従って、ユーザのネット活動を支援する役割を担う **e-執事** について検討を行ってきた [4-6]。e-執事の主たる役割を図3に示す。

e-執事は情報ポータルサイト内のインタフェースとして機能し、エージェントのように振る舞う。e-執事はユーザとサービスプロバイダの間に介在し、サービスプロバイダからの属性要求に基づき、その属性交換を実施する。e-執事はサービスプロバイダの属性要求に基づき、ユーザにその属性開示可否を確認したり、属性プロバイダから取り出した属性をポリシーに基づいて加工したりする。その際に、e-執事は一般的に理解しづらいポリシーをユーザ視点から解りやすい内容に説明したり、属性開示によるリスクを定量的に示したりする。また、同じサービスプロバイダに同じ属性を提供する場合などにおいては、一度ユーザが許可した後であれば、以降は変化がない限り、ユーザに無確認で

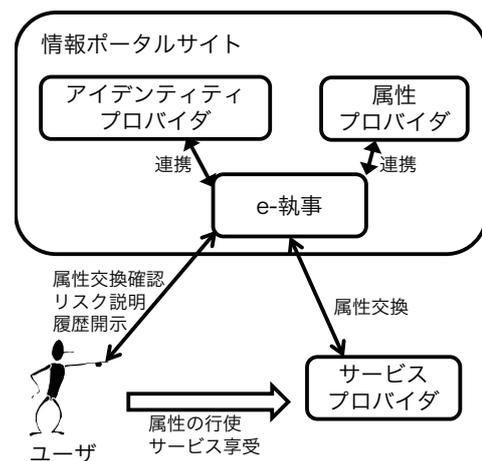


図3 e-執事

属性交換をすることで、本当に確認が必要なときにだけユーザの確認を求めることができる。また、パスワードマネージャの機能を持つことで、ID連携によるシングルサインオンが利用できない場合でも、パスワード管理の諸問題を緩和する。

e-執事はユーザとサービスプロバイダの間に介在することで、ユーザのネット活動をログインすることができる。これにより、どのサービスといつどのような取引をしたかが記録され、その情報に基づいたユーザ支援が可能となる。

6. 考察

情報ポータルサイトのような中核的なポータルサイトが実現すれば、様々なネット活動の起点となり得る。情報ポータルサイトへのログイン方法は様々考えられ、IDとパスワードによる認証、ICカードなどをリーダーにかざすことによる認証、指紋などによるバイオメトリクス認証など、ユーザの利便性と安全性を考慮して選択できることが望ましい。ユーザは情報ポータルサイトへログインしてしまえば、それ以降の各サービスプロバイダへのログインは、アイデンティティプロバイダの機能であるID連携でシングルサインオンが可能となる。ショッピングサイトなどで必要となる配送先情報なども、属性プロバイダの属性交換によって、簡単に提供できる。

情報ポータルサイトの実装はネット上の、いわゆるクラウドサービスを想定しているが、e-執事の実装については検討の余地がある。e-執事はユーザを支援することが主目的であり、ユーザに最も近い場所で実装されていることが望ましい。そのため、ユーザのPCやタブレットなどのインターネット端末に実装することが考えられる。しかし一方で、公衆端末の利用やシンクライアントが普及していくとすれば、e-執事は情報ポータルサイトに近い場所で実装されることが望ましいと考えられる。

近年では、Microsoft Office や Adobe 製品など様々なソフトウェアがクラウド化されている。これにより、セキュ

リティアップデートなどの対応が迅速に行え、ユーザは常に最新のソフトウェアを利用できるメリットがある。同様に、セキュリティ対策に詳しくない一般的な大多数のユーザにおいては、ブラウザこそがOSのような状態になりつつある。このようなユーザ層に対しては、シンクライアントによる環境提供を行うことで、セキュリティ対策をサーバ側で行うことができる。さらには、情報ポータルサイトにアクセスするだけの端末であっても、多くのWebサービスが利用できる昨今においては、十分かもしれない。このような状況であれば、情報ポータルサイトが十分に機能していれば、ユーザのセキュリティ意識によらず、多くの危険からユーザを守ることができるようになる。

情報ポータルサイトの属性交換を利用できれば、シナリオ1の問題は解決される。多くのWebサービスがID連携し、属性交換ができるようになることが望ましい。理想的には、行政が提供するマイナポータルで住民票の移動手続きをすれば、必要な箇所への届け出が自動的に行えることが期待される。シナリオ2も行政と民間との間で情報連携がシームレスに行われれば、ユーザが煩雑な手続きをする必要はなくなる。

シナリオ3の場合、単なるフィッシングであれば、アイデンティティプロバイダと属性プロバイダが提供するID連携や属性交換を利用することにより対処することができる。フェーミングされている場合はID連携やドメインチェックでは対処できないが、情報ポータルサイトが複数のDNS情報と突合することで、緩和することができる。

シナリオ1~3は高齢者のみに限定したものではなく、一般的に多くのユーザに意味がある。特に、シナリオ3は低リテラシ層に対しても効果があり、フィッシングに対する潜在的な被害者を減らすことが期待できる。

シナリオ4では、e-執事のネット活動ログを利用することで効果的な対処が可能である。同じ商品を何度も買った際に注意を促したり、過去の購買傾向から異常な購買行動を検出したりできる。また、一般のユーザに対しても、利用履歴から長期間利用されていないWebサービスの継続確認を促すことや、契約更新時期の自動通知や自動更新手続きなどが可能となる。さらには、あらかじめ指定した成年後見人のような第三者にこのような通知を行うことで、ユーザ自身が適切な判断を下せない場面でも、柔軟な支援を受けることができる。

このようなユーザのネット活動を集約管理する情報ポータルサイトの仕組みは「監視」と捉えられることもある。しかしながら、これまでに説明したように、ユーザには多くのメリットがある。ユーザに対する十分な説明と情報開示による透明性の確保、ユーザとの契約やポリシーの明確化、第三者による監査などにより、その障壁を減らすことができると考えられる。

アベノミクス第二弾では「一億総活躍社会」*12が目標にされている。この実現のためにも、高齢者になっても安心してネットを利用して、社会経済活動を継続できる環境が必要であり、ネット社会における高齢化対策が重要となるだろう。

参考文献

- [1] 行政手続における特定の個人を識別するための番号の利用等に関する法律. <http://law.e-gov.go.jp/announce/H25H0027.html>, accessed Sep. 9, 2015.
- [2] マイナンバー 社会保障・税番号制度 民間事業者の対応. <http://www.cas.go.jp/jp/seisaku/bangoseido/download/slidejigyousiryous.pdf>, accessed Oct. 2, 2015.
- [3] 高木浩光, 山口利恵, 渡辺創: 国家による個人識別番号とその利用システムのあり方~プライバシーの観点から~, 情報処理学会研究報告, pp. 1-8 (2013). Vol.2013-CSEC-61 No.29.
- [4] 柿崎淑郎, 前田陽二, 辻秀一: ユーザ中心の属性プロバイダ, 情報処理学会研究報告, pp. 1-7 (2013). Vol.2013-IS-124 No.1.
- [5] 柿崎淑郎, 前田陽二, 辻秀一: e-執事: ユーザ中心の高信頼ポータルサイト, 情報処理学会第76回全国大会, pp. 479-480 (2014). 5G-7.
- [6] Kakizaki, Y., Maeda, Y. and Tsuji, H.: e-butler: A User-centric High Reliability Personal Portal Site, *Proc. of 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA-2014)*, IEEE CS, pp. 102-107, DOI: 10.1109/WAINA.2014.30 (2014).

*12 <http://www.kantei.go.jp/jp/headline/ichiokusoukatsuyaku/>