ブロックチェーンを活用した個人情報の保護

著者：アラン・モリソン
監訳：井上 康隆

デジタル社会の発展に伴い、今まで以上に自身の身分を証明するデジタルIDの重要性が増すとともに、個人情報の漏洩・盗難のリスクが高まっている。本稿ではブロックチェーンを基盤とするソブリン・ネットワークを活用し、従来のID管理では防ぎきれなかったこれらのリスクを低減できる可能性について議論する。（井上 康隆）

大規模なデータ漏洩が頻発する現代において、インターネットユーザーやオンライン上の消費者は、どうすれば自身を特定する個人情報（PII:personally identifiable information）を守れるだろうか。ユタ州政府の元CIO（最高情報責任者）やブリガム・ヤング大学CIO室の研究室長などを歴任した、ソブリン・ファウンデーションの会長フィル・ウィンドリー氏によれば、IDの共有を全て止めることが解決策の一つだという。その対象にはクレジットカードや銀行の口座、米国の社会保障をはじめとする政府関連の番号や携帯電話の番号など、被害を受ける可能性の高いIDが挙げられる。しかし、合法的な暗号化技術であるブロックチェーンを活用した「分散型台帳技術」は、個人情報の盗難リスクを排除するシステムを設計することができる。具体的には、取引参加者で共有できる個人認証用の分散型台帳を構築した上で、従来のIDに替わる"独立した識別子"を用いて取引を行うというものだ。一連のやり取りは中央集権的に管理されず、台帳を通じて記録されるため、取引の透明性も増す。

このような信頼網が機能する仕組みを理解するために、バーテンダーが客の年齢を確認する様子を想像してみよう。米国の場合、飲酒が合法となる21歳であることを証明するためには運転免許証を提示する。人々は通常、バーテンダーが免許証に記載されている名前や免許証番号を覚えようとしていないことをほぼ確信しているであろう。しかし、デジタルの世界では年齢を証明するために、運転免許証を提示しようなどと思わないだろう。世間に広く認識され、携帯しやすい身分証明書は、泥棒が特に狙いやすいものである。こうした身分証の提示に代わるものが、前述のブロックチェーンを基盤とした認証システム「ソブリン（Sovrin）・ネットワーク」だ。このアプローチを使えば、ユーザーは今まで以上に明確で改ざんできない資格を提示できる。そして、これは州政府や信頼できる機関のデジタル署名が付された年齢証明書にもなり得る。

これは「自己主権型ID（Self-Sovereign Identity、SSI）」を用いたアプローチとして知られており、個人情報の管理・保有主体を国や企業から個々のユーザーに移そうとする試みだ。ソブリン・ネットワークのメンバーはID証明のポートフォリオを自身で構築・整備することで、どの場面でどの情報を共有するか、選択できるようになる。つまり、ユーザーはオンライン上で自らIDを保有し、その管理運用をコントロールできるのだ。かつ、個人情報は事前に発行した証明書要求を通さなければ特定できないため、他者が銀行口座や秘匿性の高いアカウントへ不正にアクセスするリスクを回避できる。あわせて、国や企業も秘匿性の高い個人情報を保有し、保護する責任から解放される。

こうしたシステムはユーザーの主体性を損なわず、個人を識別するという課題の解決策にもなり得る。この課題は人道支援や

アラン・モリソン

米国PwC Center for Technology and Innovationのシニアリサーチフェロー、「Technology Forecast」のエディター。カリフォルニア州サンノゼを拠点とし、ビッグデータ、アナリティクス、モバイル、セマンティック技術などの執筆がある。

井上 康隆（いのうえ・やすたか）
yasutaka.inoue@pwc.com

PwCコンサルティング、Strategy&のマネージャー。金融およびテクノロジー分野を中心に、データ活用やオペレーション改善などについて、多様なコンサルティング経験を有する。

「『アイデンティティ・システム』と聞くと、
多くの人はユーザー名とパスワードを思い浮かべます。しかし、それは
アイデンティティというものを非常に狭く捉えた見方です」

人身売買防止に係る活動、難民支援組織の多くが直面してきた。ブロックチェーンを基盤としたこの新たな個人認証を活用すれば、IDの侵害や盗難を防ぎ、支援を受けるべき人を正しく援助でき、ある特定の政府の気まぐれに左右されることもなくなる。

SSIの一種である「ソブリンID」や同ネットワークの開発・運用に携わる国際的な非営利団体が、ソブリン・ファウンデーションだ。個人情報へのアクセス制御や管理を目指す組織は増えつつあり、その一つのマイクロソフトも分散型認証を提唱し始めている。両者はともに分散型ID認証ファウンデーション（Decentralized Identity Foudation、DIF）のメンバーでもある。

ウィンドリー氏は長年ユーザー中心のID管理に関心を抱いており、2005年には作家のドク・サールズ氏やコンサルタントのカリヤ・ハムリン氏とともにID管理に携わる技術者会合「インターネット・アイデンティティ・ワークショップ（IIW）」を創設した。

PwC Strategy&が発行するビジネス誌『strategy+business』の編集部は2017年12月、デジタル界のリーダーらを対象とした一連のインタビューの中で、ウィンドリー氏に電話で話を聞いた。

＊　＊　＊　＊　＊

編集部: 企業はなぜ、分散型認証のアプローチに関心を寄せているのでしょうか。

ウィンドリー氏: 企業におけるアイデンティティ証明は、自前のシステムよりも優れたソリューションが求められています。認証方式の模範例として、銀行や医療機関のシステムを支持する人がいないのは明らかでしょう。しかし、その一方で、彼らは信頼性の観点から他者に認証を委託できず、ジレンマを抱えています。

自社サービスをフェイスブックやグーグル、ツイッターのアカウントと連携させ、顧客にこれらのIDでログインさせる企業も多くみられます。しかし、これはやっかいな状況。なぜなら、企業がこうしたSNS運営企業に依拠し、その動向に左右されることになるからです。例えば、フェイスブックがログイン機能を段階的に廃止することにビジネス上の利益があると考えた場合、彼らはすぐに実行するでしょう。世の中はそういうものなのです。

編集部: ソブリンのアイデンティティ・システムは、どのように機能しているのですか。

ウィンドリー氏: 「アイデンティティ・システム」と聞くと、多くの人はユーザー名やパスワードを思い浮かべます。一度でもこれらで個人を認証したシステムは、そのIDに関連付けられた権限やアクセス制御リスト、ポリシーを取得する可能性があります。そして、その個人が何をすることが許可され、どのようにシステム上でそれらにたどり着けるのかが決定されます。

しかし、これはアイデンティティというものを非常に狭く捉えた見方です。実生活におけるアイデンティティの在り方は、ウェブ上よりもはるかに多様です。誰もがさまざまな目的を持ち、複数の身分証明書を持ち歩いています。例えば、私の財布にはユタ州の運転免許証や多くの銀行・金融機関のクレジットカード、健康保険証などが入っています。おそらく、近所の食料品店のポイントカードもあるでしょう。ある意味、それぞれのカードがそれぞれのレベルの信用を補完する身分証明書なのです。例えば、銀行のカードはATMで暗証番号などを入力し、現金を引き出すための信用をもたらします。

一方、オンライン上では、私たちはアイデンティティというものを広義で捉えたことがないのです。ソブリンIDやソブリン・ネットワークのような新しい自己主権型IDシステムの多くは、アイデン

ティティを包括的に定義しようとしています。個人であれ、組織であれ、他の何かであれ、特定の存在について語っていることを証明するために、識別子を持つ必要は確かにあります。しかし、この識別子以上に、商店のポイントカードから国が発行するパスポートまで幅広く使え、実証かつ信頼に基づく認証手法を作ることが重要なのです。

編集部: ソブリン·ネットワークは、識別子をどのように管理しているのですか?

ウィンドリー氏: ユーザーが何らかの選択をしない限り、デフォルトの設定として、関係ごとに新たな識別子を発行しています。これにより、関連付けが行われるリスクが低下します。例えば、私は雇用主と銀行、両者と独立した関係を持っているとしましょう。私がそれぞれに別の識別子を持っていた場合、私の知らないところで雇用主と銀行が結託し、私に関する情報を交換することはできません。

もちろん、法的な必要性から両者に私の社会保障番号を渡した場合、彼らは関連付けを行うためにその番号を使うことができます。しかし、彼らがソブリン·ネットワークから得られる情報だけでは、関連付けは不可能です。

携帯電話の番号を例に、これをもう少し掘り下げて考えてみましょう。個人の携帯電話一台に一つの電話番号を割り当てる方法は、もはや時代遅れといえます。電話番号を記憶し、電話をかける度に番号を手入力する人はいないでしょう。連絡先リストから見つけ、クリックするだけです。そうなると、通話相手ごとに異なる番号を生成するというシステムを考えることができます。電話番号を関連付けることのできない長い糸のようなものにしても、システムは問題なく機能するでしょう。

情報を関連付けずとも、必要なことを全て成し遂げる識別子を生み出すシステムが登場しつつある今、従来のシステムの使用は減っていくことになるでしょう。少なくとも、私たちはそう願っています。

バイオメトリクスの管理

編集部: 関連付けが可能な情報のもう1つの例として、バイオメトリクス(網膜や指紋など、個人を特定できる生体認証)があります。ソブリン·ネットワークでは、バイオメトリクスはどのように扱われているのでしょうか。

ウィンドリー氏: 私たちのシステムは、台帳自体に個人を特定できる情報を保存することは絶対にありません。バイオメトリクスもその一種という意味では、私たちが台帳に保存しない多くの情報のサブカテゴリーに過ぎません。同ネットワークは基本的に、個人を特定できるもの以外で、証明に必要な情報を保存しています。例えば、関連付けを避けるため、それぞれの関係に基づいて生成する識別子などです。

バイオメトリクスは、デバイスレベルで非常に役立ちます。iPhoneの顔認証やアンドロイドおよびiOSのTouch IDは、デバイスへのアクセスにバイオメトリクスを活用する良い例です。バイオメトリクスはデバイス内に保存されますが、デバイスがアップルなどのプロバイダーに情報を提供することはなく、情報の盗難や不正利用もありません。

私たちのパートナーである非政府組織iRespondは人道支援活動において、サービスを提供する人々の識別·追跡にバイオメトリクス技術を活用しています。iRespondのエグゼクティブ·ディレクターであるピーター·シンプソン氏は、ソブリン·ファウンデーションの役員会に名を連ねています。一例を挙げると、iRespondはアフリカやアジアにおける予防接種に際し、接種対象者の眼球の虹彩パターンで記録·照合を行っています。住む場所を失った人々は、携帯電話や身分を証明できるものを持っているとは限らないからです。バイオメトリクスは、こうした人々にとって理想的なソリューションなのです。

データの秘匿性が重要な理由

編集部: 一部の中央政府や州政府が、ソブリンのシステムを使い始めているのですよね?

ウィンドリー氏: そうです。イリノイ州政府の取り組みであるイリノイ·ブロックチェーン·イニシアチブは、ソブリンのアイデンティティ·システムを活用し、出生証明書の発行を開始すると発表しました。同証明書は政府が発行する基本的な身分証明書であり、私たちの誰もがさまざまな目的で使用できるものです。

また、カナダのブリティッシュコロンビア州政府は、法人登記システムを導入しました。

さらに、フィンランドでは政府や大学、産業リーダーによるコンソーシアムと協力し、官営プロジェクトを含む多様な目的で作成する文書の信用補完として、システムをいかに活用できるかを検討しています。

編集部: 関連付けを抑制することが、そうしたイニシアチブのカギになるようですね。

ウィンドリー氏: その通りです。関連付けを減らせるチャンスはたくさんあります。関連付けの抑制が重要な理由は、プライバシーの保護につながるからです。プライバシーとは、それ自体にお金を払うものではないと人々は言うでしょう。それには私も同意します。しかし、同時に、プライバシーはその他の重要な機能を利用するために欠かせないものだと考えています。

プライバシー機能が欲しいかと聞かれたら、人はノーと答えるでしょう。しかし、自分の情報が利用されることを制御したいかと聞かれれば、イエスと答えるでしょう。どのような言葉で質問するかによるのです。プライバシー機能がなければ、制御はできません。情報が一度流出してしまえば、その事実は変えられず、もはや制御はできません。したがって、プライバシーは個人情報の管理·開示における主権を人々に与える全てのシステムにとって、不可欠な要素の一つなのです。

"Phil Windley Thinks He Can Protect Your Data" by Alan Morrison, strategy+business, March 8, 2018