研究室Report 学術の最先端はいま！

ID・パスワードに代わる次世代認証技術「ライフスタイル認証」

寄稿　東京大学大学院情報理工学系研究科ソーシャルICT研究センター特任准教授　山口 利恵

東京大学大学院情報理工学系研究科ソーシャルICT研究センター次世代個人認証技術講座では「ライフスタイル認証」の研究を行っている。ICT技術の利用が進む現在、PCやスマートフォンでの個人認証はサービスを受ける上で不可欠な技術である。しかし、未だにIDとパスワードによる認証の問題がたくさん指摘されているにも関わらず、第一線で活用され他の認証手段の導入が進んでいない。同研究センターの講座では、個人の生活習慣、つまり、ライフスタイルを利用することで、人々の負荷なく認証を実現することができると考え研究を進めている。

実証実験では行動パターンを反映した「占い」を鏡に表示するデモンストレーションを行った

「ライフスタイル認証」の導入経緯について

ライフスタイル認証とは、ライフログを用いて個人認証をしようという研究です。ここでは簡単ですが、なぜこのテーマを選ぶことになったのかを解説します。

我々の講座は、平成25年に三菱UFJニコス（株）からのご寄付によってできた講座で、次世代個人認証技術講座といい、その名のとおり次世代の個人認証技術を研究する講座です。今年で５年目を迎えます。三菱UFJニコス（株）はクレジットカード会社で、近年カードに関する不正が増えていることを問題視していました。同時に、対抗する手段として様々な新しい技術が出てきているのに、なかなか普及が進んでいない現状もあります。そこで、普及が進まない原因を考え、不正対策として適切な技術の研究をしてほしいという要望を受けました。

まず、これを考えるにあたり、現状を分析することから始めました。

（１）IDとパスワードの限界

平成25年に発表された大手セキュリティ会社（株）シマンテックの調査※1によると、77％のサイトはIDとパスワードを利用してユーザー認証を行っていると答えています。一方、すべてのサイトで異なるパスワードを設定しているユーザーは全体の30％弱で、全体の62％は１～３種類のパスワードを利用して複数のサイトでの利用を行っているとのことでした。また、平成25年はパスワードリスト攻撃※2と

※１　シマンテック、『「個人・企業のパスワード管理」に関する意識調査結果のご報告』
https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf
※２　アカウントリスト攻撃、リスト型攻撃という言い方もします。

呼ばれる、あるサイトから不正に取得したIDとパスワードのリストを他のサイトに不正にログインするという攻撃手法が流行することが話題になったころでもありました（図－１）。この攻撃は、既存の辞書攻撃やブルートフォース攻撃のようにIDリストとパスワードリストの組合せをすべて試す必要性がないため、成功率が高く、不正にログインされたサイトにとっては正規のユーザーのIDとパスワードでログインして何らかの不正が行われるために、アクセスが行われた時点では不正が行われたことに気がつきにくいという問題点があります。

しかし、IDとパスワードに関する問題点は平成25年に急に指摘されたわけではありません。IDとパスワードのように記憶に頼るような技術には、人間の記憶力という壁があるわけで、どうしても脆弱になると、インターネットが急速普及し始めた20年近く前から指摘がなされてきました。この指摘に対応するため、生体認証やICカードを利用した仕組みなど様々な技術が提案され、一部は社会実装もされてきました。しかし、抜本的な解決に至るような技術とはなり得ませんでした。同時に、ユーザーリテラシーを上げれば問題が解決できるはず、ということも言われてきましたが、このような教育も未だに浸透していません。

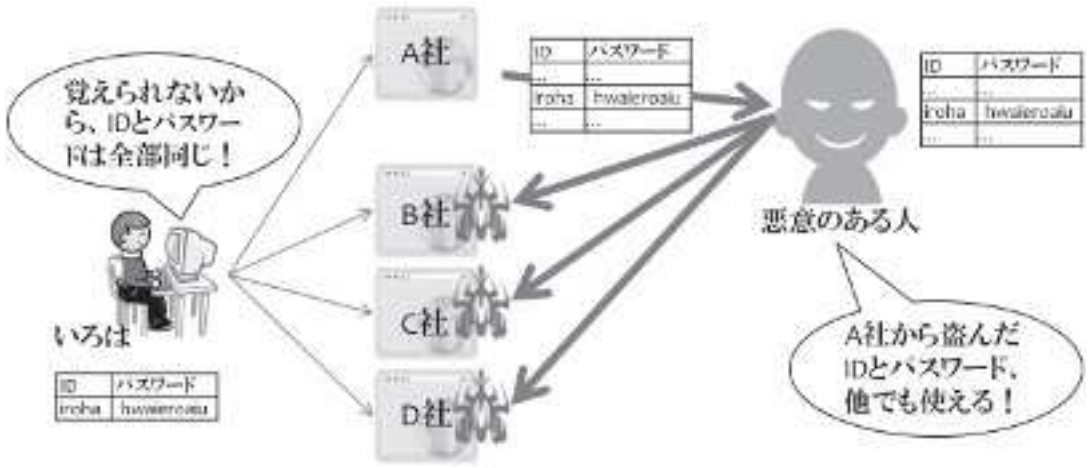
20年間もの長い間「セキュリティが高く、利便性が高い認証技術が必要」という言葉だけで、この問題を解決することができなかった現状がありました。

（２）情報セキュリティだけに目を向けない

既存の研究は「セキュリティを完全に」ということを重視した上で、「その中でも利便性が高い」という観点での研究を行ったものでした。そこで、我々はこの観点の見直しから検討を始めることとし、インターネット上でのセキュリティの研究だけでなく、現状の社会システムでのセキュリティがどのようになっているのかを考えることにしました。

たまたま寄付元がクレジットカード会社だったこともあり、クレジットカードの枠組みでどのようにセキュリティを保っているのかについて考えてみました。クレジットカード会社ではセキュリティも重視していますが、それ以上にユーザーの受容性も重視しています。クレジットカードの流れで考えてみると、不正が行われた場合にはユーザーに明細を送って確認することで後から確認して不正を発見する、という枠組みを利用しています。つまり、利用時のセキュリティについてはある程度重視するもの

図－１　パスワードリスト攻撃



の完全なものを求めていなかったのです。この不正な利用があった場合には「ユーザーに後から保証する」ということがあるために、不正な利用を完全に止めることを目指すというよりは、導入コストと不正金額のバランスを考えて、不正が起きる割合を調整するという手法を取っていました。

このように、実際の社会は不正が起きることを前提とした社会システムとして設計されているのです。もちろん被害金額が多額となり、導入コストよりも高くなってはいけませんから、ある程度のセキュリティは確保する必要性があります。しかし、今の情報セキュリティ技術研究の多くは、１ヵ所でも不正が起きないような技術を議論する枠組みがほとんどです。

そこで我々は、「不正を完全になくす」というよりは「不正を減らしていく」技術の研究を進めていく必要性があると考えました。

（３）ユーザー利便性が高い技術

また、ユーザーに負担をかけないような認証技術が全くないのか、というとそういうわけではありません。ユーザーの動作を求めずに、サーバ側の情報のみで認証を行おうという取組みがありました。リスクベース認証です。リスクベース認証は、ユーザーが利用している端末のIPやOSの情報を利用して、ある基準を満たさない場合には本人かどうか疑わしいと判断し、別の認証の入力を求めるというものです。今は情報が少ないため、疑わしいということしか分からず、たとえ本人が入力していたとしても不正かどうかをはっきりと見つけきることができません。

しかし、この技術が発展し、本人かどうかを確認することができるのであれば、ユーザーの動作なしに認証を行うことができるようになります。この発展のためには今利用している端末のIPやOSの情報だけでなく、高機能なスマートフォンなどから取れる情報やウェアラブル端末等、もっと多様な情報を利用するのがよいでしょう。また、解析技術についても、ヒューリスティックな手法に加え、機械学習を基にした人工知能の技術を活用することが考えられます。

（４）現状の社会システムに合わせる

不正が減って利便性が高い技術ならば導入されるのか、そうとも限りません。導入コストも大事です。導入コストには二つの要素があります。システムの費用及びユーザーがどの程度負担を感じるかのユーザー受容性のコストです。両コストとも、現在既に普及しているシステムからどのくらい変化したものになったのか、に大きく依存します。ユーザー全員に何かを配ったりとか、インフラシステム全体を大きく変えるような構成など、全体を変更させるような構成は導入コストが非常に高くなります。

現状普及している社会システムがどういったものであろうかと振り返ってみてみると、インターネットは人々の生活に欠かすことのできないようなインフラとなり、だれもが常にネットワークにつながっているのが当たり前になりました。また、スマートフォンが爆発的に普及し、人々が高機能な端末を持ち歩くような時代です。このような高機能な端末だけでなく、ウェアラブル端末の普及など、人々の周りにあるありとあらゆる端末がネットワークにつながるようになってきており、「IoT時代」と言われています。同時にこういった端末から得られるすべてのデータを利用しようとする、「ビッグデータ時代」も同じように言われてきました。

IoT時代、ビッグデータ時代に適したシステムがどういったものであるのかを考える必要性があります。

（５）実データの必要性

利用しようとする技術群は決まり、また対象のデータも決まりました。単にそれを組み合わせたら簡単に実現できそうですが、決してそういうことはありません。データごとに利用できる技術はどのアルゴリズムが最適か、どういったパラメーターが適切なのかについて議論をする必要性があるのです。

そこで我々は、既存サービスで利用されているデータに加え、スマートフォン上で取得することができるライフログデータの解析が不可欠と考えまし

た。しかし、このようなライフログデータは、たとえ研究用であっても簡単に手に入るわけではありません。このライフログデータを取得するために、平成29年１月に実証実験を行うことにしました。

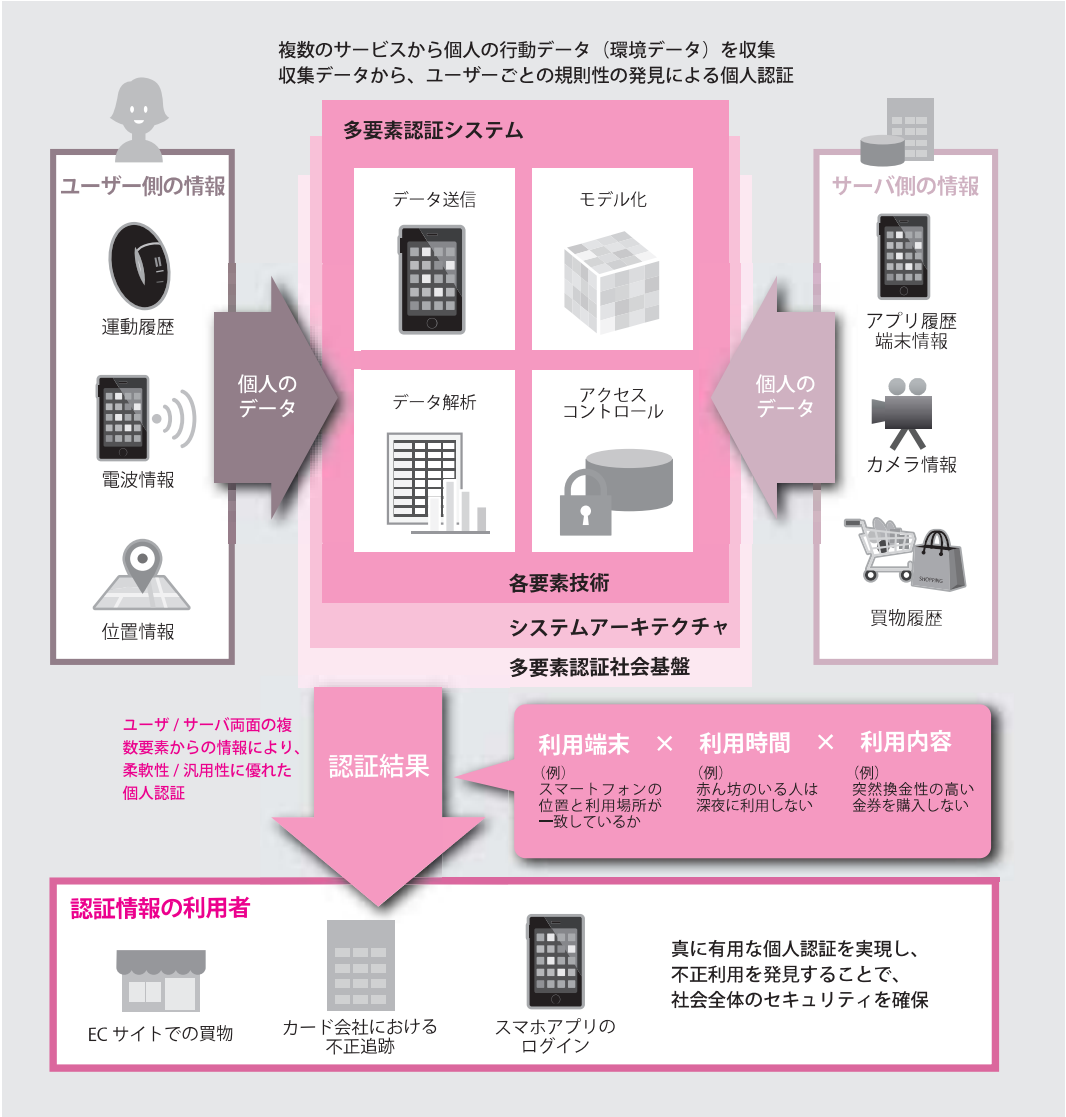
システムの概要と実証実験の内容・結果・分析等について

（1）ライフログデータを用いたライフスタイル認証

ライフログを使ったライフスタイル認証とはどういうことなのでしょうか。

ライフログとは、スマートフォンなど様々なICT技術を使った個人ごとの利用履歴を指します。ライフログを活用し、個人の生活習慣を認証することをライフスタイル認証と呼びます。個人の生活習慣で認証するとは、例えばスマホの位置情報が自宅や職場など普段の行動範囲から離れていないかを確認したり、購入しようとしている商品がこれまでに見た広告やサービスの利用実績と合っているのかを確認し、大きくかけ離れていると判断した場合には「本人ではない」とします（図－２）。本人ではないと

図－２　ライフスタイル認証の概要図



判断され続ける場合には、他の認証手段を能動的に追加することも可能です。

（2）研究のデータ取得を目的とした実証実験

しかし、このライフスタイル認証がどの程度役に立つのかを確かめるためには、実際のユーザーデータを解析しなければなりません。我々が行った実証実験「MITHRA Project」では、今のスマホから取得できる情報を、実際に被験者の皆様にご提供いただいて集めることにしました。このためには、ユーザーの同意を得ることがとても大事です。我々の実証実験では、プライバシー保護に大変詳しい弁護士に文案を作ってもらい、ユーザーに示しました。ここまで同意を得ている実証実験はなかなか少ないと思います。

この実証実験で、５万人以上の方にご参加いただくことができました。実証実験協力企業13社の皆様に、様々な立場でご協力いただきました。システムの実装だけでなく、被験者の皆様への特典提供、デモンストレーション会場の提供等、従来大学で行う実証実験で考えられるような規模を超えた広い範囲での協力をいただきました。

データをくださった被験者の方々、ご協力をいただいた企業の皆様、実証実験に関わったすべての皆様に心から感謝しています。

今後の展望、ICT化・ICTの利活用への期待、提案など

ライフスタイル認証は、ICT技術だけでの完全性を目指さず、社会全体での安全性を目指しています。まだ結果は出ていませんが、より多くの場で利用され、社会全体が少しだけ安全になると信じています。

安全・安心を重視することは大事ですが、コストや利便性とのバランスを考えることもとても大事です。導入後の利用率なども考える必要性があるでしょう。例え話ですが、すごく立派な金庫を買って複雑な鍵を10個ぐらいつけたとしても、守られているのが100円玉だとすれば割に合いません。ICT技術は柔軟ですから、適切なバランスを持った技術を導入することが大事でしょう。

実証実験アプリ画面（一部）


実証実験データ解析イメージ


カレッタ汐留でのデモンストレーション