JSSM プレスリリース

No.2011-001　　2011/09/15

日本セキュリティ・マネジメント学会，〒160-0073 東京都新宿区百人町 1-20-3 バラードハイム、
TEL　03-3371-5183,　FAX　03-3371-5185,
E-MAIL office@jssm.net,　URL　http://www.jssm.net

この号の内容

JSSM キャッチフレーズ

「法・経営・技術・倫理の融合する情報セキュリティ総合科学の創造」

お知らせ

社会への提言
「誰でも安心して使えるパスワードの実現に向けて」

日本セキュリティ・マネジメント学会（Japan Society of Security Management; 略称 JSSM　会長　佐々木良一）は、情報システムのセキュリティ全般に関する学際的、業際的な調査研究を実施し、より健全な高度情報社会の構築に貢献することを目的として 1985 年に設立され、今年で 25 周年を迎えました。この創立 25 周年の節目に、“社会に役立つ、会員に役立つ”をコンセプトに、三つの事業に取り組んでいます。

JSSM 25 周年記念事業

1. 社会への提言
2. 「セキュリティマネジメント学　～理論と事例～」の編纂
3. 「JSSM アーカイブ」の編集

この発表は、「社会への提言」の第一弾です。

個人情報の保護研究会からの提言 「誰でも安心して使えるパスワードの実現に向けて」を発表するものです。

社会への提言では、セキュリティマネジメント学の成果を応用し、実社会に適用することで現代社会の課題のいくつかに新たな解決の糸口を見つけることをテーマに、この 1 年間に様々な単位で社会への具体的な提言案のまとめに取り組んでいます。

今後も社会に役立つ提言をシリーズで発表する予定です。ご期待ください。

誰でも安心して使えるパスワードの実現に向けて

1. はじめに

本稿は、今後利用機会が広がり重要性が高まると考えられる「電子的本人認証」の現状に関する問題点の分析に基づき、問題解決に向けた本人認証手法ならびにその利用促進を社会に向けて提言するものである。

ユビキタス技術の進展により端末デバイスの数が爆発的に増えることにより確実な本人認証を要求するサービスが今後、更に増加することが予想される。近々ではスマートフォンの普及によりインターネット上で提供されるアプリケーションサービスが増え、ユーザーが本人認証を要求される機会が今まで以上に増加している。また、電子行政サービス構想の実現に伴って、国民一人一人が確実な本人認証を行う必要がある社会へと移行していく。

パスワードは代表的な電子的本人認証手段として様々な場面で使われ、社会に大きく貢献してきた。政府の安全対策基準（電子政府ガイドライン作成検討会セキュリティ分科会「オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン」2010年8月）においても、パスワードは定義された全ての保証レベルで共通項目として挙げられており、生体認証や所持物認証など、他の認証方式が利用される場面であってもパスワードを利用しない状況は想定しにくい。

このようにパスワードは記憶認証として必要不可欠であるにもかかわらず、現状の文字によるパスワードは「覚えられない」「メモ書きする」「使い回す」等、後述2項に記載するように、その運用と安全性に様々な問題を抱えているのが実情である。具体的には、平成21年中の不正アクセス禁止法違反事件における不正アクセス行為の検挙件数2,532件のうち、識別符号窃用型（他人の識別符号を入力して不正に利用する行為）は2,529件にあがると報告されている（総務省「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」平成22年3月4日）。

以上の背景から、本稿ではパスワードを多くの人々が安全に使いこなすにはどのようにしたらよいかについて、以下に問題点の考察と、問題解決のための提言を行うものである。

2. 現状の問題点

パスワードや暗証番号は端末ログオン、ウェブサイトへのアクセス、入退室、ATM利用など、いろいろな場面で使われ定着している。しかしその運用は、例えば「6 桁以上のランダムな英数字特殊文字の無意味な組合せ、メモ禁止、3 ヶ月毎定期変更」など利用者の安全性と利便性を両立させることが難しい状況が続いている。このパスワードの運用に関する状況については広く国民の間で議論されているとは言えない。特に顕著な問題点を以下に述べる。

①メモと使い回し： 人間の記憶力には限界があり、多くのパスワード（特に、良質なパスワード）を記憶し続けることは困難なため、パスワードを記載したメモを携帯するか、あるいは1 つのパスワードを複数のシステムに共用するのが実情である。前者はパスワード漏洩に対する脆弱性となり、また後者はセキュリティ管理レベルの低いシステムでのパスワード漏洩が、同じパスワードを用いる他のシステムへの不正アクセスを誘発することにより、いずれもセキュリティ・リスクを高める結果となっている。

② パスワード失念対応コスト： セキュリティを重視して強固なパスワードの登録を強制すると、失念や混乱により不明となったパスワードの再発行のために、ヘルプデスクへの問い合わせが増加し、運用サイ

ドに少なからぬコストが発生している。

③ パスワードの乱用： 必要以上に強固なパスワードを求めるシステムや、パスワードを短期間で変更させるシステムが多く存在するために「メモと使い回し」が助長されている。セキュリティを強化するはずの対策が、逆にセキュリティを低下させたり、また「パスワード失念対応コスト」の増加にも繋がっている。

これらの問題点はいずれも、人間の記憶力に限界があることが原因であり、人間の記憶力の限界を考慮したパスワードの運用ができていないといえる。無意味で長い文字列を数多く覚えることを要求されても、大方の人間は対応できないのである。

3. 提言

「文字によるパスワードが脆弱であることを踏まえ、本人にとって再認しやすい画像などを活用した電子的本人認証手法を広く利用することを提言する。」

文章を圧縮したりパターン記憶を活用したりといった様々なパスワード記憶の工夫方法が確かに存在する。また、シングルサインオン等のID 連携を利用すれば、より少ないパスワードの管理で済み、ユーザーの記憶への負担を軽減することが可能である。しかし、ともに特定のユーザーないし特定の分野における有用性は評価できるものの、パスワード記憶力が有限であるという問題を本質的に解決する方策ではない。

認知心理学においては、記憶とは「符号化」「貯蔵」「検索」からなる一連の情報処理過程であり、記憶の想起には、思い出したことを再現する「再生（解答記入式）」と、提示された項目の中から記憶しているものを選ぶ「再認（解答選択式）」とがある。再生より再認のほうが容易なことは多くの実験結果により明らかとなっている。例えば「ぜいじゃく」という漢字を思い出して「脆弱」と書くよりは、「繊細、静寂、脆弱、贅沢」などと提示された候補の中から選ぶ方が容易なことは明らかであろう。
また昔の友人の名前が思い出せなくても顔は思い出せることがよくあるように「言葉（文字列）」より「画像」のほうの記憶成績が良いことが「画像優位性効果」として知られている。

記憶度合比較 （再生と再認　文字と画像）

●再生と再認

再生（解答記入式）

（ぜいじゃくを漢字で表記せよ）

□ ＜

再認（解答選択式）

（ぜいじゃくの正しい漢字を選択せよ）

繊細　静寂　脆弱　贅沢

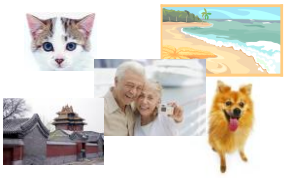
⇨ *再認（解答選択式）は再生（解答記入式）より解答成績がよい*

●文字と画像

文字

猫 犬 夫婦 城 海岸 ＜

画像



⇨ *「画像」は「文字」より記憶成績が良い　：画像優位性効果*

こうした再生に対する再認の優位性ならびに言葉（文字列）に対する画像の優位性に着目すると、記憶された画像などをパスワードとして利用する解決策が登場してくる。

この中に私自身が登録した愉しく懐かしい画像がいくつか？何時でも何処でも私には難なく見つけられる。全て正しく見つけられるのは世界中で私だけ。

自伝的記憶につながる画像を登録し無感動な画像を囮としていれば災害時のパニック状態でも速やかに識別して選択できる可能性が高い。

画像利用パスワードに関する議論は古くからあったが、自伝的記憶につながる画像を低コストで簡便に扱える仕組みが長く不在であった。しかし、最近にいたってプロセッサーの高速化技術や情報処理デバイスのコストダウン、及び高速通信インフラとデジタルカメラ付き携帯端末の普及により画像を活用する本人認証方式は実現可能なテーマとなっている。

本人認証の可用性を考える上では災害時の配慮も必要である。大災害に遭遇しパニックの中で財布も免許証も手帳も携帯電話も失い、周囲に身元を証明してくれる人が誰もいないという状況での本人認証を考慮しておくことが求められる。一切の所持物を失ったところから出発して身体の負傷も視野にいれると記憶照合が最も確実で信頼できる本人認証手段となる。記憶照合のなかでも画像方式ならばパニック状態を想定しても可用性を維持して所期の目的を果たすことができる可能性が高いと考えられる。平時の落ち着いた屋内環境で使えるからといって災害時に屋外で使えるとはかぎらないが、災害時に屋外で使えるものであれば平時にはどのような環境であっても使えることにも留意したい。

可用性における画像利用パスワードの優位性は上述のように示せるが、本人認証手段としては併せて機密性の検討が欠かせない。主に問題となるのは「覗き見」、「数学的強度」、「推測攻撃」の３つである。

①覗き見（ショルダーハッキング）：　覗き見（ショルダーハッキング）に対しては文字パスワードのタ

イプ入力に比べて画像選択型は脆弱であるとの見解がある。しかし、文字であれ画像であれ利用者が無防備であれば共に覗き見され得るし、注意して画面や指の動きを遮蔽すれば肉眼によるものであれビデオ盗撮であれ共に覗き見を防げる。画像だから文字より脆弱ということはない。

②数学的強度： 任意の文字パスワードと同じ数学的強度になるように画像を登録することができるので、手動の総当り攻撃に対して画像方式は文字方式に対して優位でも劣位でもない。利用者は守るべき情報資産の価値と利用時の手間隙のバランスを図って適切なマトリックスサイズと登録画像数を選べばよい。

③推測攻撃： ある特定の利用者の好悪・人脈・趣味などの情報を入手しての推測攻撃に対しては以下のようなガイドラインの提示で対応することが可能である。

- 日頃から好きだと公言している人やブランドばかりで正解データを作るのは不可。
- いつも自宅外で持ち歩いているものを正解データにすることは不可。
- 家族から情報を守るのが主目的の人が家族・親族の画像を正解データに使うのは不可。
- 雛型の上に追加したものを全て正解画像として登録することは不可。
- 正解データは全て古い写真ばかりで、囮は全て新しい写真ばかりは不可。
- 位置やパターンの場合は、四隅・直線・斜線・単純なアルファベットやカナを使うのは不可。

可用性における優位性と併せて鑑みると、画像活用方式は、一定の可用性を維持しつつ文字方式よりも高い機密性を実現し、あるいは一定の機密性を維持しつつ文字方式よりも高い可用性を実現出来るものであると考えられる。

4. 提言を進める上での課題

提言で述べてきた画像を使った本人認証方式を具体的に実現していくためには、以下のような課題があると認識している。

①実証実験の実施： 画像などの再認を活用するパスワード・システムについて、現実的有効性や利用に伴う新たな問題点を検証するために、認知心理学などの最新の知見を動員し、定量的評価を含む実証実験の実施が望まれる。

この課題に関連するもので、文字を入力する「再生」から、画像を選ぶ「再認」に移行するだけでも記憶の負担がはるかに軽くなり、さらに自分の気に入った画像を選ぶのは楽しいという副次的効果についての実証的評価も望まれる。また、想い出深い画像には一般的効用として認知症の進行抑制や孤独感の軽減などの効果があることがわかってきている。懐かしく愉しい想い出の画像をネットワーク上に保管しておき、一方ではこうした一般的な効用の期待できる用途で活用しつつ、他方では、災害時などに持ち物がない場合でも不自由なく実行できる本人認証に利用するといった連携システムの可能性についても視野に入れたい。

②実現手法の評価： 高度な数学的強度を謳うことができたとしても可用性/利便性に欠ければ利用可能な本人認証技術ではない。また、いくら使い易いと謳うことができても機密性/保全性に欠けるものはそもそも本人認証技術たり得ない。第三者機関が画像などを利用する本人認証手法を客観的に評価し、認証マークの付与などを通じて信頼性を向上することが望まれる。

③啓発・教育： 文字パスワードに関する諸問題の周知や、画像などを利用した電子的本人認証手法の利用促進に向けて、産官学ならびにメディアなどでの活発な啓発活動を推進していくことが望まれる。

5. おわりに

電子行政サービス構想の導入が真剣に検討されているまさに今、サイバー社会において国民一人一人が安全・安心に使いこなせる電子的本人認証の基盤を確立することは喫緊の課題である。持続的で健全なサイバー社会の確立に当提言が寄与できれば幸甚である。

以上