Vol.2010-CSEC-49 No.9
2010/5/11

パスワードの脆弱性と対策－認知心理学の知見を生かして

桝野隆平

株式会社ニーモニックセキュリティ

パスワードとは，一般的には「合い言葉」の意味であるが，情報システム分野で使用する場合はユーザが本人認証をするために入力する文字・数字列を指す．本人認証に使われるパスワードはセキュリティ全体の強弱を実質的に左右し，安易な作り方をするとセキュリティを崩壊させかねない．従来様々なパスワード脆弱性対策が謳われてきたが，人間の心理や記憶の特性を考慮していないが故に実効的な意味は薄く，またパスワード代替手段についての議論も，認証という行為の本質に立ち至ることなく表面的な技術比較にとどまっていた．本論文では認知心理学の知見を参考にしてパスワードの脆弱性対策を論じ，人間の記憶特性に沿った解決策を提案する．

Passwords and Cognitive Psychology

RYUHEI MASUNO

Mnemonic Security, Inc.

Little need be said of the crucial role which passwords take in the user authentication. But it is also too well known that passwords are vulnerable because human memories are limited. The issue of passwords should preferably be debated along with basic understanding of cognitive psychology. In this paper we present real problems of passwords and propose some possible solutions in terms of the balance of security and user-friendliness.

1. これまでの脆弱性対策の問題点

コンピュータシステムの認証方法として現在最も多く使われているのはパスワードによる本人認証である．パソコン自体へのログイン，LAN 経由での社内システムへの，インターネット経由での各種システムへのログインなど，大半のコンピュータシステムで「ID・パスワード」がユーザ本人認証手段となっている．さまざまな認証方法のうち，コンピュータシステムにとって手軽で扱いやすく，セキュリティも確保できるように思われるのがパスワードだったからである．

しかしながら不正使用や犯罪防止の点から見るとパスワードには大きな欠陥がある．すなわち，「覚えやすく思い出しやすいパスワードは破られやすく，破られにくいパスワードは覚えにくい」という人間の記憶力の特性からくる制約である．この制約の中で何とかしてパスワードを使いこなそうとさまざまな対策が考えられてきた．

1.1 実効性のない対策

従来提唱されてきたパスワード脆弱性対策には，「短いパスワード，名前に関連するもの，生年月日，辞書にある単語を避け，最低 6 文字以上，大文字/小文字/数字/記号などを含むものとし，できるだけエントロピーの大きなものを使うこと」[a] といった条項が並んでいる．そのほかに謳われている事項として，定期的に変更すること，複数のアカウントに同じパスワードを使い回さないこと，などがある．

それでは強力なパスワードを作成するにはどうすればよいのか，例えばマイクロソフト社の HP で説明されている方法は以下の通りだ．
（http://www.microsoft.com/japan/protect/yourself/password/create.mspx）

・長くする．8 文字以上が望ましく，理想は 14 文字以上
・文字，数字，記号を組み合わせる
・自分では覚えやすく他人が推測するのは難しい単語やフレーズを使用する
そして，具体的な作成の手順を以下のように指導している．
・覚えられる文章を考え，
・コンピュータやオンラインシステムでパスフレーズが直接サポートされているかどうかを確認し，
・パスフレーズがサポートされていない場合は考えた文章をパスワードに変換し，
・複雑さを追加し，
・最後に，特殊文字で置き換える

a)参考文献[1]410 頁．

Vol.2010-CSEC-49 No.9
2010/5/11

こうして，"My son Aiden is three years old"という覚えられる文章から出発して，"MySoN 8N i$ 3 yeeR$ old" というパスフレーズや，"M$8ni3y0" というパスワードにたどりつきなさい，というわけである．頭の体操としては大変面白いが，一般のユーザが簡単にできるようには思われない．

パスワードから公開鍵までの認証技術を説明した浩瀚な書籍『認証技術　パスワードから公開鍵まで』（参考文献[2]）では，パスワードについて詳細に論じた「第６章ＰＩＮとパスワードの選び方」で「結局のところ，古典的なパスワード選択の規則は次のようにまとめることができます.パスワードには記憶不可能なものを選ぶこと(ただし，メモ書きは厳禁)」と簡略かつシニカルにまとめている．また，ユーザに強力なパスワードを強要すれば，ユーザは「自分たちの記憶力の限界とパスワード選択の規則との折り合いをつけるために，この問題を別の形へと変容させ」パスワードをメモに書いてマウスパッドの下に置くという解決策に走ると,耳の痛い指摘も加えている．
ではどうすればよいのか．同書ではランダムに選んだ単語 2 個を連結する方法や詩歌を利用する方法などパスワードへの攻撃に耐えるためのアイディアをいくつか提示するものの，最後には人間の記憶力という壁にぶつかるという指摘で終わっている．

1.2 派生する問題

破られにくい，即ち強いパスワードには「長大・ランダム・無機質」であることが求められるが，一般のユーザにとってこうした強いパスワードをしかも複数個覚えることはきわめて困難である．メモに書いて常時携帯するということで対応せざるを得ず，メモの管理という新たな問題を引き起こすことになる．

また，何とか無理をして一つの強いパスワードを覚えると，これを多くのアカウントに使い回すケースが出てくる．このパスワードの使い回しも大きな問題をはらんでいる．ユーザとしてログインするシステムやウェブサイトの中にはパスワードをハッシュ暗号化して保管するところもあるが，平文のままでの保管も少なくない．セキュリティレベルの低い後者からパスワードが漏洩した場合には，結果として前者のアカウントまで破られてしまうことになりかねない．

従来の議論から導かれるのは，パスワードの脆弱性対策は人間の記憶の特性を考察することなくしては論じられないということのようである．そこで次節では人間の認知活動を情報処理の観点から考察する「認知心理学」での記憶に関する知見を参考に人間の記憶の特性について触れ,次に今後の脆弱性対策について論じることとしたい．

2. 記憶に関する認知心理学の知見

20 世紀後半になって人間の知能を情報処理の観点から理解しようとする認知諸科学が誕生した．認知心理学は知覚，記憶，注意，学習など人間の認知機能を研究対象とする学問であり，脳科学や情報科学とも深いかかわりを持つ．認知心理学の知見によれば，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，情報を一時的に保持する「短期記憶」と長期にわたって保持する「長期記憶」に大別される．[b]

2.1 短期記憶

短期記憶とは短時間（約 20 秒間）保持される記憶で，時間の経過とともに忘却されていく．アメリカの心理学者 George A. Miller は 1956 年に発表した論文（参考文献[3]）のなかで，人間にとって短期記憶が可能な情報量を 7±2 とする「マジカルナンバー７」理論を打ち出した．数字 1 文字も，人名，地名のような言葉も，1 単位の塊り（チャンク）としてみたうえで，塊り 7 個前後が短期記憶の限界としたもので，認知心理学における基礎理論の一つとして認められている．

「マジカルナンバー7」は人間の瞬間的情報処理能力の基準となり，ユーザビリティの点でも参考にされてきた．郵便番号や，金融機関で使われる口座番号は 7 桁であり，大都市の電話番号も以前は 7 桁だった．7 という数字は，日～土の曜日やドレミの 7 音階のほか 7 不思議，7 変化など様々なところに登場する親しみやすい数字でもある．パスワードを考える場合も Miller の理論が大いに参考となる．パスワードの長さを 7±2 以上に増やすと，短期記憶がしにくくなり，メモ等に転記することになってしまうのは科学的に説明できるのである．

2.2 長期記憶

記憶を多段階からなるシステムと考える認知心理学での代表的モデルの一つである「アトキンソン・シフリンの二重貯蔵モデル」（簡略図を「図 1」に示す）では，視覚，聴覚などの「感覚登録器」に入力された情報のうち注意を向けられたものだけが「短期貯蔵庫」に入り，そのなかで復唱するなどの記銘処理を行ったものが「長期貯蔵庫」に送られて長期記憶になると説明されている．

b)短期記憶とは別の概念として、何かの認知的な作業を行いながら，そのために必要な情報を一時的に保存するような記憶システムとして「作動記憶（ワーキングメモリー）」というモデルも提唱されているが，ここでは詳細に立ち入らない．

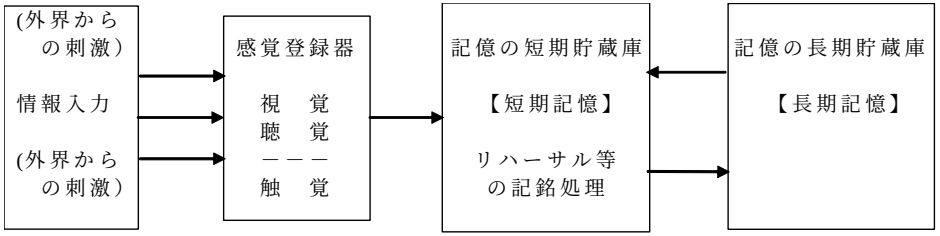

図 1　アトキンソンとシフリンの「記憶の二重貯蔵モデル」

長期記憶は，言語によって記述できる事実に関する記憶である「宣言的記憶」と，自転車の乗り方のように体で覚えた記憶「手続き記憶」に分類される．さらに「宣言的記憶」は，「鯨は哺乳類である」のような一般的知識に代表される「意味記憶」と，特定の時間的・空間的文脈の中に位置づけることのできる出来事に関する「エピソード記憶」に分けられる．エピソード記憶には特定の時間や場所が関係し，経験者の印象を伴う．エピソード記憶のなかでも，自分の人生を振り返っての思い出の記憶は「自伝的記憶」と呼ばれ，イメージと情緒を伴っている．[c]

長期記憶の想起には，思い出したことを再現する「再生」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」とがあり，再生より再認のほうがたやすいことは実験により明らかとなっている．[d]　また，記憶材料の特性が保持に影響し，「絵」が「語」より記憶成績が良いことは「画像優位性効果」として知られている．[e]

記憶の忘却については，時間の経過を原因とする減衰説と覚える項目が増えると項目の類似性が干渉することが原因とする干渉説とがある．[f]　銀行カードのわずか 4 桁の暗証番号でさえ複数個の暗証番号をたやすく使いわけられないのは，数字 4 桁という同じ形式のものの数が増えれば増えるほど類似性による干渉が起こるためで，人間の記憶の特質からくるものと理解される．

また，咽喉まで出かかっているのに思い出せないという現象は，貯蔵された情報の中から求める情報を探し出す「検索」の失敗という観点から理解される．[g]

c)参考文献[4]15 頁，123 頁，237 頁.
d)参考文献[4]147 頁.
e)参考文献[4]104 頁.
f)参考文献[4]75～76 頁,155～157 頁.
g)参考文献[5]56 頁.

2.3 記憶力

記憶力は成人期以後高齢化するにつれて次第に衰えていくのが一般的であるが，高齢者の記憶減退は再認より再生でより顕著なものとなる．[h]

成人の記憶力，特に本論文の対象としているパスワードに関する記憶の実態については，認知心理学者の谷津貴久氏（早稲田大学）が大学生（平均年齢 19.6 歳）を対象として行った『パスワードの利用状況と忘却経験調査』（参考文献[6]）で興味深い結果を発表している．「調査の結果，パスワード入力を求められる機会は概ね 5 つ以下，設定するパスワードは 3 種類以下であった．複数パスワードの管理を求められる人については，半数以上が忘れる可能性を減らすためにパスワードを使い回していることが示された.」また，「過去 1 年間にパスワードを忘れた経験のある人が 40%を超えたことも示された.」

大学生という記憶力のよい年代を対象とした調査でも，教科書に書いてあるような推測されにくいパスワードを作って使いこなすことがいかに困難であるかが明確に示される調査結果[i] となっており，結論部では以下のような提言がなされている．
「パスワードは ID ごとにすべて変えよと原則論を教育し続けることも可能だが，実効性は低いと思われる．今回の調査で示されたように，少数のパスワードしか設定しないのはパスワードを忘れないための利用者側の工夫だからである．そのような現状を考慮し，利用者の設定するパスワードが 3 種類程度であることを前提として，パスワードの生成ならびに使い分けのしかたを教育していく必要がある.」

3. 実効性ある脆弱性対策のために検討すべき事項

3.1 パスワードは長ければよいのか

認知心理学の知見を視野に入れた上でパスワードの脆弱性対策を考えてみよう．先ず，短期記憶についてはマジカルナンバー7 という容量の限界を考慮に入れねばなら

h)参考文献[4]181 頁.
i)上記調査で記憶力に直接関連する項目を見ると，受験勉強という記憶力のトレーニングを終えたばかりの学生たちを対象としているだけあって，パスワードを記憶しているのか記録しているのかという質問（複数回答可）に対しては「自分の頭の中だけで憶えている」という回答が最も多かったが(63.4%),「自分の頭の中で憶えているが，記録もしている」という回答がこれに次いで多かった(38.1%).
忘れたときの状況は，「一部は思い出せたが，全部を思い出すことができなかった」 が最も多く(40.7%),「何も頭に浮かばず，まったく思い出せなかった」(25.4%)が 2 位,「ほかで使用しているパスワードを そこでのパスワードと思い込んで入力していた」(20.3%)が 3 位となっている.

ない．一般に人間の覚えられる桁数は 7±2 ということから，5〜9 桁を超えるパスワードを強制すると暗記が困難になりメモに頼らざるを得なくなるのは当然のことと想定すべきであろう．

例えばパソコンのログインパスワードの場合であれば，パスワードクラッキングソフトで簡単に破られない程度にまでセキュリティを高めようとすると，ユーザに 15 桁以上のパスワードを要求する必要がある．要求されたユーザはメモしておくしかなくなり，パソコンの裏やマウスパッドの下にメモを貼り付けて対処することが十分に予想される．攻撃者の立場に立てば「オフィスにあるコンピュータの周囲を探しさえすれば,パスワードのメモが簡単に入手できる」[j] という状況が其処此処で発生する．メモを禁止すれば無理やり覚えこんだ長大パスワードを多くのアカウントに使い回すようになり，1.2 で記述した通り厄介な問題が派生することになる．

暗号鍵の場合は長大であればあるほど安全性が高まる．しかし，パスワードに関しては単純に長大なものを要求すればよいというわけにはいかない．長大なパスワードを要求した場合はメモの扱い方についてもガイドライン[k] を決めておく必要がある．

3.2 パスワードは頻繁に変更するのがよいのか

パスワードを定期的に変更させるのはシステム管理者の側から見るとセキュリティを向上させる手段である．しかしながらユーザにとっては，せっかく覚え込んだパスワードを捨てて新たなパスワードを覚え直すというのは大きな負担となる．

パスワードを覚えようとすると，意味のない文字の羅列であれば繰り返し暗唱するなどの方法で符号化し意味記憶として定着させねばならないが，これが人間にとって苦痛であることは暗記物の勉強に苦しんだ経験を待つまでもない．江戸幕府は 1603 年，室町幕府は 1338 年と機械的に覚えるより，「いい国（1192）つくる鎌倉幕府」などと語呂合わせをした方が覚えやすい．既に記憶している単語との結びつきに加えて発音したときのリズムなどが記憶の定着にプラスになるからである.（語呂合わせによる長期記憶の強化は認知心理学で「意味的符号化」[l] といわれる方法である.）

しかしながらパスワードの場合，既に自分の記憶しているもの（生年月日，電話番号，人名など）と直接結びつけるのは好ましくなく，また英数字の組み合わせとなると語呂合わせもままならない．無理やり丸暗記しても，変更が頻繁であればあるほど覚えられるパスワードの候補が減っていき，安易なパスワードに先祖返りするかメモに頼らざるを得なくなってくる．メモを禁止すれば，前項 3.1 に記載の通りパスワードの使い回しという問題が派生することになる．

3.3 工夫で解決できるのか

文字パスワードは工夫次第で使いこなせるはず，現に私はこんなやり方をしています，という記事が時々新聞，雑誌やネット上に登場する． 1.1 にご紹介した強いパスワードの作り方の類が多いが，記憶力の壁をメモで補完するという正しい問題意識の元で記憶力を要求するというやや倒錯気味の工夫も披露されている．安全にメモするには，パスワードの一部を伏せ字にして自分が忘れそうな個所だけ書いておくこと，パスワードが「P@$$W0rD」なら，「PxxxWxxx」や「x@$$xxxx」としておく，というものだ．少しでもヒントがあれば思い出しやすいという点では一応の工夫だが，難点は伏字の部分が思い出せないときには無力であるということ．かといって書きすぎると安全性はなくなってしまう．

工夫を提唱するのは工夫を必要としないほど記憶力のよい人なのではないかとも思えてくる．私にはできるのだからあなたもできるはず，できないのは覚える気がないか努力が足りないかですよ，という前提で人間の記憶特性を無視したようなパスワード運用規定を作っておいて工夫でカバーしようとしても根本的な解決にはならない．

3.4 ワンタイムパスワードは「パスワード」か

毎回異なる，意味のない文字列をパスワードとする「ワンタイムパスワード」を使うとパスワードに関する悩みが解決するだろうか．パスワード生成器（トークン）に表示される文字列をその都度打ち込めばよいのだから，覚える必要もなく，使い捨てなのでスニッフィングを気にする必要もない．一見理想的なパスワードのように思える．しかしよく考えてみると,「ワンタイムパスワード」とは呼ばれるが，機械によって生成される一時乱数が証明するのはトークンの真正性だけであって,「記憶によって認証する」パスワードとは別の認証手段であることが分かる．

つまり，ワンタイムパスワードはパスワードの脆弱性を解決した上位技術ではなく，IC カードや USB トークンといった，本人ならば持っているはずの所持物による認証方法の一つと考えるべきである．[m]

j)参考文献[2]141 頁.
k)例えば，長大なパスワードはメモされるということを前提とし，メモを認めて保管基準を提示する．最重要なパスワードには 15 桁以上のランダムな英数字を要求し、メモは鍵のかかる金庫等へ保管してもらう．その他のパスワードについては手帳へのメモを認めるが，パソコンやディスプレイなど機器への貼り付けやパソコンの近くにメモを置くことは禁止する，など.
l)参考文献[7]23 頁.
m)参考文献[8]においてもワンタイムパスワードは「所持による認証」として取り扱われている.

3.5 人間の記憶の特性を考慮に入れると

脆弱性対策を実効あるものとするには人間の記憶の特性を考慮に入れなければならない．認知心理学の知見のなかから対策立案に参考となる部分を以下に抜粋する．

- 無機質な数字や文字の一時的記憶ではマジカルナンバー7 の呪縛を受ける
- 覚える項目数が増えると干渉により想起しにくくなる
- 再生より再認のほうがたやすい
- 「語」より「絵」のほうが記憶しやすい
- 自伝的記憶にはイメージと情緒が伴う

どう工夫しようが長い桁数の文字パスワードをメモなしで入力するというのは一般の人間にとって苦痛であり困難でもある．そこで，文字を再生するより画像を再認するのが得意であり，自伝的記憶のようにイメージを伴った記憶は忘れにくいという記憶の特性を生かして脆弱性対策を立てることが有効となる．つまり，自伝的記憶を惹起するようなシンボルやイメージなどをパスワードとして使えるように既存のパスワードシステムを拡張することが実効的な脆弱性対策につながると考えられる．

4. パスワード代替の認証は可能か

パスワードを使いこなすのが難しいのならＩＣカードによる認証や生体認証といった別の認証方法に移行したほうがいいのではないか，という考え方が出てきてもおかしくない．ただでさえ覚えられないパスワードを頻繁に変更させられることに比べてはるかにユーザフレンドリーであり，現に銀行カードでは静脈認証の ATM が増えてきているはないかという考え方だ．

しかし，パスワードに代表される記憶認証の代替手段には「認証」という行為の基本にかかわる大きな問題点があり，そう簡単にパスワードがお役御免とはならない．以下その理由を考察する．

4.1 認証と識別

従来の説明では，認証とは本人しか持ち得ない属性を元にその属性を確認して本人であることを証明することであり，「記憶照合：What we know」「所持物照合：What we have」「生体照合：What we are」の三種類がある，とされてきた．しかしながらこの説明は大きな問題をはらんでいる．例えば所持物や指紋だけで認証できるとすると，対象となる当人が死亡ないし意識不明であっても認証が可能となってしまうのだ．もちろん相手の実在性が確認できる対面交渉の場ではこのようなことは起こりようもないが，経済行為がモバイルやインターネットといった非対面の世界に大きく広がってしまったため，旧来の区分では問題が生じるようになったのである．

IPA セキュリティセンターの『本人認証技術の現状に関する調査報告書』（参考文献[8]）では，「認証とは何らかのサービスを提供する側が相手の真正性を確認する行為である．」と定義しているが，サービス提供側の確認する相手は当然ながら「サービス提供を求めている」ユーザである．サービス提供を求めるという本人の意思があって初めて認証という行為が起こるのであり，「本人の意思」という前提なしには「認証」ということも起こらない．

「認証」と並んで「識別」という別個の概念があり，この二つの差異は当人の意思の有無確認において顕著に現れる．先に述べた通り「認証」は何かをしたいと思っている人の要求に基づいて行われる（例えばＰＣのログイン認証など）のに対し，「識別」は識別の対象となる人の意思とは無関係に行われる（例えば死体の識別など）からである．[n]

個人識別と本人認証を英語で表現すると差異が分かりやすくなるかもしれない．
個人識別：Who is this person ?
本人認証：Is he or she the person who claims to be ?

「個人識別」とは，対象とする人を特定の個人と認める行為であり，肉体的特長や所持物などが識別手段となる．「本人認証」とは，サービス提供を受ける資格のある当該個人であると主張する人の真正性を確認する行為であり，認証に用いられる代表的手段が「合い言葉」としてのパスワードであった．

4.2 意思的行為としての本人認証

法的観点から考察するならば，すべての契約行為において，契約主体には権利能力，意思能力，行為能力の三つの能力が要求される．つまり，意思を持っていることが契約成立の前提の一つとなっており，契約当事者が泥酔や心神喪失状態にあるときは意思能力を認められない．また，民事訴訟法第228条4項に「私文書は，本人又はその代理人の署名又は押印があるときは，真正に成立したものと推定する．」と規定されているように，「署名・捺印」は本人の意思発現の象徴とみなされている．

n)識別と認証との差異に関しては，『次世代電子行政サービスの安全運用を支える本人認証基盤の確立に向けて』（参考文献[9]）で詳細な検討がなされている．

さらに，商法第32条では「この法律の規定により署名すべき場合には，記名押印をもって，署名に代えることができる．」と規定されており，法律では，署名を第一議とし，記名押印に署名と同等の効果を認めるという考え方を取っていることが示されている．それ自体に意思発現効果があるわけではない印章に対して法律が大きな役割を認めていることについては，興味ある問題ではあるが本論文の主題からやや離れるので別の機会に論ずることとしたい．

モバイルやインターネットなど対面交渉を前提としない世界においては，サービス提供側にとって向こう側にいる眼に見えないユーザの「意思」を確認するのは容易ではない．登録したパスワードを入力するという行為はユーザ本人の「認証してもらいたい」という意思の発現と解釈できるので，「ＩＤ・パスワード」が認証方法として使われてきた．しかしパスワードの代替手段として登場してきた所持物照合や生体照合を単独で用いる場合，特定の物（ICカードや携帯電話など）を持っていることや肉体（指紋や静脈など）の特徴が登録されたものと一致していることをもって意思の発現とするにはやや問題がある．酩酊状態や意識のない状態でも可能だからである．

本人認証は何らかの経済的・法的行為の入り口となるものであるから，泥酔状態にあっても遂行可能な認証方法を単独で用いるわけにはいかない．従って，非対面の世界を含む場合において，主たる認証手段は記憶照合に頼らざるを得ず，所持物照合や生体照合は記憶照合と組み合わせて使う補助手段として機能させるべきであろう．

5. 結論

本人の意思能力の証明ともなる記憶照合方法として現実的な手段がパスワードであり,現に大半のシステムが認証をパスワードで行うことを前提として組まれている．所持物照合や生体照合を利用する場合においても，誤照合時の救出用にはパスワードが使われており，また，本人の意思確認という点でもパスワードを組み合わせた 2 要素認証とするのが望ましい．従って，パスワードシステムをいかに使い勝手のよいものにしていくかは今後ともセキュリティ上の重要問題であることを再確認するとともに，脆弱性克服のため以下の提案を行いたい．

「3−5」で記述した通り，イメージと情緒を伴うエピソード記憶である自伝的記憶を惹起するようなイメージ画像，例えば思い出の写真などをパスワードとして使えるように既存のパスワードシステムを拡張してユーザの選択肢を増やすことである．

長大な文字パスワードを複数個使いこなせるという人には従来通りのパスワードを提供し，記憶力に自信のない人にはパスワードの素材を拡張して，自伝的記憶に結びつくイメージ画像などを暗証画像（パス画像）として登録し，登録したものを正しく選ぶことで認証できるようにする．パスワードとして文字を入力するのは「再生」だが，写真を選ぶのは「再認」であり，それだけでも記憶の負担が少なくなるのは認知心理学の知見から見ても明らかである．強固な文字パスワードの作り方を勉強するより自分の気に入った写真，好きな人の顔写真を選ぶほうが楽しいという副次的効果も出てこよう．

画像をパスワードに使う手法は既にいくつか登場しているが未だ普及しているとは言いがたい．人間の記憶の特性に沿っている手法なので，多くのユーザが実際に使うなかでその使い勝手を改善していくことがパスワードの脆弱性対策に寄与することになる．

政府ではデジタル利活用のための諸問題解決に着手しており，近い将来ほとんどの国民が情報システムの利用者として本人認証を行う時期の到来することが予想される．そこでは人間の記憶の特性を考慮に入れ，ユーザに使い勝手のよい新しいパスワードシステムが登場しなければならない．本考察がその参考になることを願っている．

参考文献

1) 日本ネットワークセキュリティ協会編：情報セキュリティプロフェッショナル総合教科書，秀和システム(2005)
2) Richard E. Smith:：認証技術 パスワードから公開鍵まで，稲村雄監訳，オーム社(2003)
3) George A. Miller ：The Magical Number Seven, Plus or Minus Two : Some Limits on our Capacity for Processing Information, Psychological Review,63,81-97,(1956) http://psychclassics.yorku.ca/Miller/
4) 高野陽太郎編：認知心理学 2 記憶，東京大学出版会(1995)
5) 海保博之編：朝倉心理学講座 2 認知心理学，朝倉書店(2005)
6) 谷津貴久：大学生のパスワード利用状況とその忘却経験 http://www.waseda.jp/mnc/RESEARCH/mnc_comm/papers/tanitsu/index.html
7) 岡市広成：行動科学ブックレット 1 覚える，二瓶社(2007)
8) 情報処理振興事業協会（IPA）セキュリティセンター：本人認証技術の現状に関する調査報告書(2003.03)
9) 鵜野幸一郎,小泉雄介：次世代電子行政サービスの安全運用を支える本人認証基盤の確立に向けて，日本セキュリティ・マネジメント学会第 23 回全国大会研究報告書(2009.07)