パスワード生成・管理とユーザの心理学的特性

高橋　優[1]

情報化社会の中でパスワードはユーザ認証の鍵として広く用いられている。生体認証やシングルサインオンなど，新たなユーザ認証の方法が生まれているが，特殊な装置を必要とせずさまざまな場面で利用できるパスワードは依然としてユーザ認証の中心的存在である（Herley, Oorschot, Patrick, 2009）。

コンピュータ・情報通信ネットワークの利用において，強度の高いパスワードを生成し安全に管理することがユーザには求められてきた。こうしたパスワードの適切な運用は，コンピュータやネットワークの利用が一般化した1990年代以降，技術者やオペレータといった特定の者だけではなく「普通の人」においても求められるようになっている。

パスワードの適切な運用のためには，ユーザのパスワードに関する行動特性の理解が必要である。ユーザがどのようなパスワードを生成し，どのように管理しているかを知ることではじめて，どう対応すべきかが明確になる。その意味で，心理学はセキュリティを考えるための多くの示唆を与える（Anderson & Moore, 2009; 北神・原田・桝野・鵜野, 2011）。誰もがパスワードを利用するようになる中で，ユーザの心理学的特性を知ることはセキュリティを確保する上でいっそう重要になっている。また，ユーザの振る舞いを理解してはじめて，効果のある訓練や，安全に使える認証システムの構築が可能となる。

一方，ユーザのパスワード環境は変化しつつある。今日，多くのユーザはメールやSNS，ショッピングやオンライン・バンキングなど，さまざまなネットワーク・サービスを利用している。利用するサービスの増加は，

1　埼玉工業大学基礎教育センター工学部会

本稿をまとめるにあたり，上田卓司先生（早稲田大学）より多くの有益なご指摘を頂戴しました。また，本研究の実施にあたり電気通信普及財団の助成をいただきました。記して謝意を表します。

それに対応するパスワードもまた増えていることを意味するが，多くのユーザは記憶の負荷を避けるためにパスワードを使い回している（谷津, 2004; IPA, 2014）。こうした使い回しは近年，リスト型攻撃のターゲットとなっており（勝村, 2014; IPA, 2014），セキュリティにおける重大な問題となっている。ユーザがネットワークにアクセスする際に利用するデバイスも多様化している。スマートフォンやタブレットの普及により，従来とは異なる入力デバイスによりパスワードは入力されるようになっている。

本稿では，ユーザがどのようにパスワードを運用しているか，ユーザの属性との関係とあわせて概観した上で，改善のための行動科学的あるいは心理学的アプローチを紹介する。また，パスワード環境の変化がユーザの行動にどのような変化をもたらしているかを検討し，そこに心理学がどのように貢献できるかを検討する。

パスワードの運用におけるユーザ行動

パスワードの強度

パスワードを適切に運用するためには，強度の高いパスワードを生成すること，生成したパスワードを他者に知られないよう管理することの２点が重要である。

パスワードの強度を高めるためには，より長いパスワードを付けること，より多様な文字種をパスワードに含めることが求められる。また，ユーザ名などユーザに関する情報や辞書掲載語をパスワードに用いることは，パスワードの推定を容易にするため望ましくない。

しかし，こうしたガイドラインを，多くのユーザは必ずしも満たしていない（Herley et al., 2009; IPA, 2014）。

Cazier & Medlin（2006）は，eコマースサイトのパスワードを対象に強度評価を行っている。２人はパスワード解析ソフトを用いて，99.2%のパスワードの解析に成功した。３割近いパスワードは１分未満で解析が完了したという。文字長の平均は7.37字で58.3%はアルファベットのみで構成されていた。Horcher & Tejay（2009）も同様の手法によってある企業の従業員のパスワードを調べ，12時間で93%のパスワードを解析することができた。

Florêncio & Herley（2007）はツールバーを用いてウェブのパスワード

利用に関する50万件ものデータを収集した。ビット長により示されたパスワードの強度は平均40.54ビットで，大文字・小文字・数字で構成された場合の９文字のビット長（53.39）を下回る程度である。

国内においても状況は同様である。谷津（2004）は大学生を対象に，使用しているパスワードの特性を調査した。それによると，パスワードの文字長の最頻値は８で，全体の49.2%がアルファベットと数字により，15.3%がアルファベットのみもしくは数字のみで構成されていた。アルファベット・数字・記号を組み合わせたものは18.6%に留まった。また，情報処理推進機構（IPA）の調査では，自分もしくは家族の名前や誕生日に基づくパスワードであるという回答がそれぞれ２割程度を占めていた（IPA, 2014）。

パスワードの使い回し

パスワードの運用では，よいパスワードであることに加え，そのパスワードを他者に知られないように管理することが求められる。誰かに見られることのないよう，パスワードはメモせず頭の中だけに記憶しておくことがしばしば求められる。しかし，これはそれほど簡単なことではない。前述の谷津（2004）によれば回答者の43.7%が過去１年間にパスワードの忘却を経験していた。多くのパスワードを管理する必要があれば，それに応じて負担も増大することになる。

この負担を軽減するためにしばしばパスワードの使い回しが行われる。谷津（2004）では，パスワードの入力機会が複数ある者の67.9%がパスワードを使い回していると回答した。Notoatmodjo & Thomborson（2009）は，半数近くが少なくとも１つの重要サイトでパスワードを使い回していることを報告した。IPA（2014）によれば，金銭に関連したサイトであっても，回答者の25.4%がパスワードを使い回していた。日常生活場面におけるパスワードの利用を検討するために日記法を用いたGrawemeyer & Johnson（2011）でも，調査で収集された175のパスワードのうち，86個は使い回され，20個は別のパスワードに部分的に再利用されていた。また，Florêncio & Herley（2007）の調査によれば，平均的なユーザはパスワードを3.9のサイトで使い回していた。

こうしたパスワードの使い回しをしている場合，あるサイトで漏洩したIDとパスワードにより他のサイトへのアクセスを試みるリスト型攻撃

によって，パスワードを破られる危険がある（勝村, 2014; IPA, 2014）。Harque, Wright, & Scielzo（2013）は実験的なアプローチによる検討を行っている。実験ではまず，セキュリティ水準の異なるサイトのためのパスワードを実験参加者に生成させた。その後，セキュリティの低くてよいサイトのために生成されたパスワードを利用して，高いセキュリティを求められるパスワードに対する辞書攻撃を行ったところ，33.1%のパスワードを解析できた。このことから，セキュリティの低いパスワードが漏洩すると高いセキュリティの必要なパスワードまで危険にさらされると指摘した。

セキュリティに関する意識とパスワード管理

ユーザのセキュリティに関する意識およびユーザ自身の属性と，パスワードの管理行動との関連について，Gebauer, Kline, & He（2011）はユーザのリスク認知がパスワードの文字長や更新回数といったパスワード管理に影響を及ぼしていることを報告した。八城（2010）もまた，パスワードの更新を促すには，パスワード忘却に対するユーザの不安を取り除く必要のあることを指摘している。

ユーザ属性とパスワード強度やセキュリティ意識の関係について，中澤・加藤・漁田・山田・山本・西垣（2010）はセキュリティ意識とパーソナリティに関する調査の中で，社会的外向性，規律性，持久性とセキュリティ意識の間の関連を見いだしている。Yahoo! ユーザのパスワード約７千万件を収集した Bonneau（2012）は，パスワード強度とユーザの属性（性別，年齢，言語等）との関連を検討し，若年者が年長者よりも簡単なパスワードを用いる傾向にあることを指摘している。また，Notoatmodjo & Thomborson（2009）は回答者の知覚するセキュリティ水準と，パスワード再生の困難性との間に相関があることを報告した。

パスワードの運用改善への適用

ユーザに対するパスワード訓練

行動科学によるセキュリティ対策のひとつとして，セキュリティに関する訓練によってパスワード運用の改善を図る試みを挙げることができる（Charoen, Raman, & Olfman, 2008; Horcher & Tejay, 2009; D'Arcy &

Hovav, 2009)。こうした訓練は，パスワードの生成や管理行動の改善を目的としている。さまざまな研究の中で，ここでは実験的あるいは心理学的アプローチの研究を取り上げる。

Campbell, Ma, & Kleeman（2011）はパスワードの生成方針を課すことにより，生成されるパスワードの強度が変化するかを検討している。その結果，生成方針を課した群では生成されたパスワードの辞書掲載語との距離が統制群と比べて増大した。しかし，有意味語やパスワードの使い回しに関しては効果が見られなかった。

福田（2006）は，初心者の場合パスワード強度の推定に認知的バイアス（アルファベットに数字が加えられた場合，強度を過大視する）が存在することを明らかにした上で，パスワードの強度推定に関するヒューリスティックスを実験参加者に与えることにより正しく強度を推定できるようになることを報告した。ただし，その効果は長期的なものではなく，２週間後には消失した。

Bonneau & Schechter（2014）は心理学的な知見をパスワードの学習訓練に応用したものとして興味深い。Bonneauらは間隔反復（spaced repetition）により56ビットのランダムコードの学習を実施している。６語もしくは12文字に符号化された記憶コードを，入力欄よりも少し遅らせて表示することにより，参加者が記憶にもとづいてコードを入力するよう促した。正しくタイプされると，次のコードを提示して入力を求めることで，学習を進めさせた。訓練の結果，最終的に94%の参加者が秘密鍵全体を記憶で入力することができるようになった。ランダムパスワードの強度と想起成績について検討し，想起の困難性を指摘したYan, Blackwell, Anderson, & Grant（2004）とは保持期間も異なるため一概に比較できないが，訓練方法がパスワード強度を改善できる潜在的な可能性を示したものといえるだろう。

認証システムへの心理学の適用

行動科学の適用はユーザの向上だけでなく，ユーザの利用するシステムの向上にも貢献しうる。心理学の知見を利用してユーザの認知的な負荷を低減する，さまざまな支援ツールや認証システムが提案されている。

パスワードの生成に関しては，Forget, Chiasson, Oorschot, & Biddle（2008）のパスワード生成支援ツール（Persuasive Text Passwords, PTP）

を挙げることができる。このツールではパスワードの生成（改変）をシステムが提案することによりユーザの負荷の低減を図っている。

TweetPassも同様に，パスワードの生成を支援するツールである（小倉・坂松・ビスタ・高田, 2014; 坂松・小倉・ビスタ・高田, 2014）。TweetPassはTwitterでのユーザのツイートを参照し，その内容をもとに12の語を提示する。ユーザがその語の中からいくつかを選択すると，語呂合わせでパスワードを作成するよう促す。ユーザ自身のツイート内容から抽出された語をもとにパスワードを生成するため，ユーザのエピソード記憶による想起性の向上を期待できる。

認証システムに関して，北神他（2011）は画像を認証システムに用いる意義を指摘している。画像優位性効果（Shepard, 1967）により，画像はパスワードのような文字列よりも保持しやすいであろうと期待できる。また，複数ある画像の中から鍵の絵を選ぶ再認形式で認証するため，再生形式と比べて認知的負荷が低い。どちらもユーザの認知的な負荷を緩和するものといえる。画像の再認による認証システムは，Dhamija & Perrig（2000）やWiedenbeck, Waters, Birget, Brodskiy, & Memon（2005）のような提案・検証段階を経て，Windows 8の「ピクチャパスワード」のような実用段階のものも出現している。

増井（2013）はユーザ自身の記憶にもとづいてあらかじめユーザが用意しておいた問いに答えることで認証を行うEpisoPassというシステムを提案している。これも，ユーザのエピソード記憶を利用することにより，強度の高いパスワードの生成・管理を図ろうとするアプローチである。

パスワード環境の変化とユーザ行動

管理アカウントの増大

冒頭で述べたように，パスワードをめぐる環境の変化として，管理すべきアカウントおよびパスワードの増加が挙げられる。Florêncio & Herley（2007）によれば，パスワードの必要なアカウントをユーザは平均して25ほど管理していた。こうした管理アカウント・パスワードの増大は，パスワードのメモや安易なパスワード設定などの不適切なユーザ行動を招いている（Adams & Sasse, 1999）。前述のパスワードの使い回し（Notoatmodjo & Thomborson, 2009; Grawemeyer & Johnson, 2011; Harque et al., 2013;

Bonneau & Schechter, 2014）も，そうしたひとつといえる。

複数の異なるパスワードを管理するひとつの方法がパスワード管理ソフトの利用だが，これは必ずしも普及しているとはいえない（Gaw & Felten, 2006）。Bonneau & Schechter（2014）は，マスターパスワードの強度によって保存されているすべての情報の強度が決まってしまう点を指摘しており，パスワード管理ソフトさえあればすべての問題が解決するわけではない。

利用デバイスの多様化

パスワードをめぐるもうひとつの環境の変化として，ネットワークにアクセスする際にユーザが利用するデバイスの多様化がある。10年前であれば，ネットワークへのアクセスはパーソナルコンピュータかフィーチャーフォンだったが，今日ではフィーチャーフォンからスマートフォン，タブレットへの移行が進んでいる。総務省（2014）によれば2013年の国内のスマートフォンの利用率は52.8%と，半数以上に達している。また，タブレットの利用も15.4%と，前年と比べて倍増した。キーボードを備えるパーソナルコンピュータとは異なり，スマートフォンやタブレットはタッチスクリーン上に表示されるソフトウェアキーボードによって文字入力が求められる。パスワードも同様である。表示面積の制約により，数字や記号を入力する場合は盤面を切り替える必要があるため，ハードウェアキーボードと比べて，数字や記号，大文字の入力は負担が増大している。

こうした，新しいデバイスの登場に伴い，ユーザのパスワード行動に変化が生じる可能性がある。この件に関してはまだ知見が蓄積されておらず，調査や実験によるデータの収集が必要とされている。

パスワード環境の変化と認知心理学

Herley et al.（2009）が指摘するように，パスワードはもうしばらく利用されることになると思われる。パスワードをめぐる環境の変化により，ユーザの行動がどのように変わるかを見極めるとともに，適切な運用を確保するための方法論を，変化に対応させていくことが求められる。

そうした中で，心理学がこれまでに明らかにしたさまざまな知識を活用することが期待される。これまで，パスワード利用における心理学の応用は，ユーザの行動改善に向けての説得的コミュニケーションや動機づけ，

攻撃手法としてのソーシャルエンジニアリングなど，社会心理学的なものが中心的だった。しかし，認知的な負荷や人間の内的情報処理過程については，認知心理学を活用できる場面が少なくない。

たとえば，前述の認証システムもその一例である。画像優位性効果を用いた画像再認による認証や，エピソード記憶に基づく認証は，認知心理学の実践への適用といえる。再認形式の認証であることも，ユーザの負担を軽減することにつながるだろう。

管理すべきパスワードの増加による記憶負荷の増大という状況の変化に対しても，理解と対策の検討にも認知心理学を活用できる。多くのパスワードを管理する際に，新たなパスワードを覚えるのに困難を覚えたり，あれこれ覚えているうちに古いパスワードを忘れてしまったりすることは，古典的な「記憶の干渉」により解釈することができる。前者のように先行項目によって後続の項目の記憶が妨害されることを順向干渉，後者のように後続項目が既習の項目の記憶に影響することを逆向干渉という。項目の種類が変わると後続項目の記憶成績が回復する順向干渉の解除（Wickens, 1972）のように，一定の条件下では，こうした干渉は抑制される。

有意味性の低い項目を覚えるという点では，複数の項目をひとつにまとめることで実質的な記憶容量を拡大するチャンキング（Chase & Ericsson, 1982）も役立つかもしれない。適切なチャンキング手法を開発できれば，より多くのパスワードを覚えることが可能となる。

認知心理学の知見の適用は，適切なパスワードの運用に資するだけでなく記憶理論の精緻化にもつながる。認知心理学と情報セキュリティの双方に有益な進展をもたらすだろう。

Reference

Adams, A., & Sasse, M. A.（1999）. Users are not the enemy. *Communications of the ACM*, 42（12）, 40-46. doi: 10.1145/322796.322806

Anderson, R., & Moore, T.（2009）. Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A*, 367, 2717-2727. doi: 10.1098/rsta.2009.0027

Bonneau J.（2012）. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. *IEEE Symposium on Security and Privacy*.

〈http://www.jbonneau.com/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf〉(January 30, 2015)

Bonneau, J., & Schechter, S. (2014). Towards reliable storage of 56-bit secrets in human memory. *Proceedings of the 23rd USENIX Security Symposium*, 607-623.

Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, 30, 379-388. doi: 10.1080/0144929X.2010.492876

Cazier, J.A., & Medlin, B.D. (2006). Password security: An empirical investigation into E-commerce passwords and their crack times. *Information Security Journal: A Global Perspective*, 15, 45-55. doi: 10.1080/10658980601051318

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice & Action Research*, 21, 55-72. doi: 10.1007/s11213-007-9082-4

Chase, W. G., & Ericsson, K. A. (1982). Skill and working memory. In G. H. Bower (Ed.), *The psychology of learning and motivation*, 16. Academic Press.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89, 59-71. doi: 10.1007/s10551-008-9909-7

Dhamija, R., and Perrig, A. (2000). Déjà Vu: A user study using images for authentication. *Proceedings of the 9th Usenix Security Symposium*. 〈https://www.usenix.org/legacy/publications/library/proceedings/sec2000/full_papers/dhamija/dhamija.pdf〉(February 4, 2015)

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, 657-666. doi: 10.1145/1242572.1242661

Forget, A., Chiasson, S., van Oorschot, P. C., & Biddle, R. (2008). Persuasion for stronger passwords: Motivation and pilot study. *Persuasive Technology*, 140-150. doi: 10.1007/978-3-540-68504-3_13

福田健 (2006). 識別符号の秘匿強度推定におけるヒューリスティックス.

情報処理学会研究報告．コンピュータと教育研究会報告，130, 53-60.

Gaw, S., & Felten, E. W.（2006）. Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*, 44-55. doi: 10.1145/1143120.1143127

Gebauer, J., Kline, D., & He, L.（2011）. Password security risk versus effort: An exploratory study on user-perceived risk and the intention to use online applications. *Journal of Information Systems Applied Research*, 4, 52-62.

Grawemeyer, B., & Johnson, H.（2011）. Using and managing multiple passwords: A week to a view. *Interacting with Computers,* 23, 256-267. doi: 10.1016/j.intcom.2011.03.007

Harque, S.M.T., Wright, M., & Scielzo, S.（2013）. A study of user password strategy for multiple accounts. *Proceedings of the Third ACM Conference on Data and Application Security and Privacy,*173-176. doi: 10.1145/2435349.2435373

Herley, C., van Oorschot, P. C., Patrick, A. S.（2009）. Passwords: If we're so smart, why are we still using them? *Financial Cryptography and Data Security*, 230-237. doi: 10.1007/978-3-642-03549-4_14

Horcher, A.-M., & Tejay, G. P.（2009）. Building a better password: The role of cognitive load in information security training. *Intelligence and Security Informatics, 2009. IEEE International Conference on*, 113-118. doi: 10.1109/ISI.2009.5137281

IPA（2014）. オンライン本人認証方式の実態調査報告書．〈http://www.ipa.go.jp/files/000040778.pdf〉（February 1, 2015）

勝村幸博（2014）. あなたはパスワードをいくつ覚えていますか（IT pro・記者の目）.〈http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/081800029/?ml〉（January 31, 2015）

北神慎司・原田悦子・桝野隆平・鵜野幸一郎（2011）. 人の視点から考えるパスワード問題：認知心理学の観点からの提言．電気情報通信学会情報セキュリティ心理学とトラスト研究グループ研究発表会資料.

増井俊之（2013）. EpisoPass：エピソード記憶にもとづくパスワード管理. コンピュータセキュリティシンポジウム 2013 論文集, 933-940.

中澤優美子・加藤岳久・漁田武雄・山田文康・山本匠・西垣正勝（2010）.

Best Match Security：性格と本人認証技術のセキュリティ意識との相関に関する検討．情報処理学会研究報告．CSEC, 21, 1-8.

Notoatmodjo, G., & Thomborson, C.（2009）. Passwords and perceptions. *AISC '09 Proceedings of the Seventh Australasian Conference on Information Security,* 98, 71-78.

小倉加奈代・坂松春香・ベッドバハドゥールビスタ・高田豊雄（2014）．想起性と安全性を両立するパスワード生成過程の分析．日本認知科学会第31回大会論文集, 662-671.

坂松春香・小倉加奈代・ベッドバハドゥールビスタ・高田豊雄（2014）．TweetPass：ツイートから想起性と安全性の高いパスワード作成を支援するシステムの提案．インタラクション2014論文集，B６-１, 525-528.

Shepard, R. N.（1967）. Recognition memory for words, sentences and pictures. *Journal of Verbal Learning & Verbal Behavior,* 6, 156-163.

総務省情報通信政策研究所（2014）. 平成25年 情報通信メディアの利用時間と情報行動に関する調査〈速報〉.〈http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2014/h25mediariyou_1sokuhou.pdf〉（August 18, 2014）

谷津貴久（2004）. 大学生のパスワード利用状況とその忘却経験．*MNC Communications*, 7.〈http://dspace.wul.waseda.ac.jp/dspace/bitstream/2065/44323/1/MediaNetworkCenter_07_Tanitsu.pdf〉（January 30, 2015）

Wickens, D. D.（1972）. Characteristics of word encoding. In A. Melton & E. Martin（Eds.）, *Coding processes in human memory*. Winston.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. & Memon, N.（2005）. Authentication using graphical passwords: Effects of tolerance and image choice. *Proceedings of the 2005 symposium on Usable Privacy and Security*, 1-12. doi: 10.1145/1073001.1073002

Yan, J., Blackwell, A., Anderson, R., & Grant, A.（2004）. Password memorability and security: Empirical results. *IEEE Security & Privacy*, 2（5）, 25-31. doi: 10.1109/MSP.2004.81

八城年伸（2010）. パスワードの使用に関する意識調査：定期的な変更に関する考察．安田女子大学紀要, 38, 187-195.