パスワードに関する教育とその効果

八城年伸†

安田女子大学　現代ビジネス学部†

はじめに

ユーザ認証に用いられるパスワードは、定期的に変更する、他人から推測されにくいものにすることが求められ、それらを支援する様々な試みがなされてきた。しかしながらセキュリティ上は必要なことであっても、往々にしてユーザの反発を招いてきている。筆者はこれまで取り上げられる機会の少なかった、ユーザのパスワードに対する意識について、情報に関する詳しい知識を持ち合わせていない段階の女子大学生を対象に調査を行ってきた。

その結果、パスワードを変更しない理由として「忘れてしまいそう」とする不安を４割以上の学生が抱えていることがわかった[1]。またパスワードを作成する際には、レンタルビデオ店の会員登録の際に記入する程度の情報を基にして、記憶のしやすさを優先したと思われる学生が相当数いる状況も明らかになった[2]。

これらの結果を踏まえ、パスワードの作成方法を教授することで、パスワードの強度が向上するかについての調査結果を報告する。

調査の概要

安田女子大学の１年次生が受講する情報ネットワークに関する講義の中で 2008 年 12 月に調査を実施した。調査は調査票方式で、以下の手順で行った。

- アンケートの表面に回答する（約５分）
- 使用中のパスワードの強度の判定
- パスワードの作り方の講義（約２０分）
- 作成したパスワードの強度の判定
- アンケートの裏面に回答する（約５分）

対象は日本文学科（日文）と現代ビジネス学科（現ビ）の学生で、回収数は 97 である。当該科目は習熟度別の２クラス編成となっているが、いずれも習熟度が高い方のクラスで調査を実施したものである。日文の情報関連科目は全学共通科目のみであるのに対し、現ビは情報関連の基礎専門科目が１年次に３科目あり、さらにはノートパソコン必携の環境にある。

Education and effect about password management

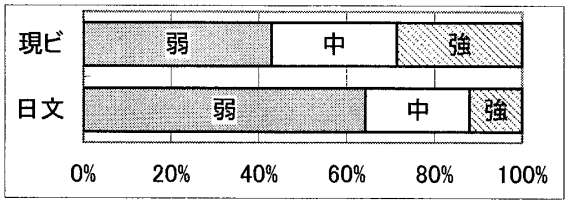
† Toshinobu YASHIRO , Yasuda Women's University

情報教育環境については両極端な学科であるが、回答の傾向は一部を除いて有意な差は認められなかった。そのため、差が認められなかった設問については学科別の集計は割愛する。

パスワードの強度

自分で作成したパスワードがあるかとの設問については、作成したことがないのは全体の 10%の学生に過ぎず、さらには全体の 78%の学生が普段から使用していると回答している。

自分で作成したパスワードの強度について、マイクロソフトが公開している「パスワードチェッカー」[3]を用いてチェックさせた。同チェッカーは簡易判定的なものであるが強度の傾向は判断できると思われる。



判定結果を妥当と考えるかとの設問には、「弱」と判定された学生のうち 65%が妥当と答えており、弱いと自覚がありながら使い続けている状況が明らかになった。

パスワード作成方法の教授

自分で作成したパスワードの強度をチェックした後に、パスワードの重要性と作成方法を約２０分かけて教授した。

パスワードの作成手順や手法には様々なものがあるが、マイクロソフトが公開している「強力なパスワード ： その作り方と使い方」[4]を参考にした。ただし学内情報システムにおいては、英大小文字・数字・記号の４種類を各々１字以上用い、６字以上８字以下という字数制限があるため、それに合致するように修正を加えている。

講義で用いた方法と例文は以下の通りである。

１．元となる文章を考える。例示したのは安田女子大学の学園訓と平家物語の一節である。
【やさしくつよく】

2．各単語の先頭の文字を取る。例文は７文字と短い和文のためローマ字表記の子音のみとする方法を示した。
【ｙｓｓｋｔｙｋ】
3．複雑さを追加する。「for を 4」、「くを 9」とするなど英文と和文の双方における方法を示した。
【ｙｓ４９ｔ４ｋ】
4．特殊文字で置き換える。似た形状の記号に置き換える方法として、「a と@」、「2 や S と$」を示した。
【ｙ＄４９ｔ４ｋ】
5．パスワードに使用すべき文字種や字数などのポリシーを満たすための修正を加える。
【Ｙ＄４９ｔ４ｋ@】

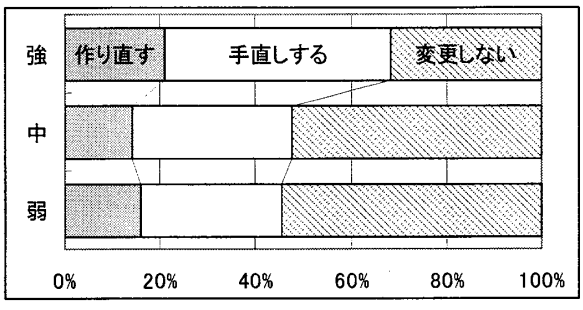
逆に禁止事項として示したのは以下の５点である。

1．連続した文字を使う（キー配列等の擬似的にランダムに見えるものを含む）。
2．辞書に載っている単語を使用する。
3．携帯電話のメールアドレス等、他で使用しているフレーズを元の文章として用いる。
4．誕生日や記念日等、他人に知られやすい文字や数字を使用する。
5．記号に「-（ハイフン）」を使用する。

最後の項目は補足説明が必要であると思われる。これはパスワードクラック用の辞書に登録されている文字列において、使用比率が極めて高いとの調査結果があるためである[5]。

リスクがあっても変更しない

講義を終えたところで、新しいパスワードを作るかとの設問には興味深い結果が表れた。パスワード強度が「弱」または「中」と判定された学生の 55%が「多少のリスクはあっても現在のパスワードを使い続ける」と回答している。



過去の調査の分析において、パスワードを変更しないのは、作成方法を含めたパスワードの管理方法を知らないため、「忘れそう」との理由をつけているものと考えていた。しかしながらリスクと作成方法について講義してなお変更しないとする回答が少なくないため、パスワードそのものへの愛着など他の要因を考える必要があると思われる。その要因によっては、強制的にパスワードを変更させる状況は、システム管理者に対する心情が好ましからぬ状況になりかねないことを示していると言えよう。

強度の変化

パスワードを作り直す、または手直しするとした学生には、作成後に再度パスワードの強度をチェックさせた（N=46）。

		講義後			
		弱	中	強	最強
講義前	弱	2	9	9	2
	中		4	8	
	強			12	

講義後に作成したパスワードは、講義前に比べて弱く判定されたケースは皆無である。さらに講義前には「弱」と判定されていながら、講義後には「最強」と判定されるパスワードが作成できたケースもある。これらのことから、講義には一定の効果があったと考えられる。

まとめ

今回の調査により、パスワードの作り方の講義には一定の効果があることがわかった。しかしながら実際にパスワードに手を加えた学生は半数に過ぎず、作り直さなかった学生の事由分析と指導方法の検討が必要であると思われる。また、調査時期や調査対象の習熟度を変えるなどして、講義の実施に適した時期を求めることも今後の課題としたい。

[1] 八城年伸,「パスワードに関する意識調査と考察」,平成 18 年度情報教育研究集会,pp588～591,2006
[2] 八城年伸,「パスワードに関する継続的な意識調査と考察」,平成 19 年度情報教育研究集会,pp463～466,2007
[3]https://www.microsoft.com/japan/protect/yourself/password/checker.mspx
[4]https://www.microsoft.com/japan/protect/yourself/password/create.mspx
[5] 守屋英一,「本当に怖いパスワード破り」,IT Pro,日経 BP 社,2006,
http://itpro.nikkeibp.co.jp/article/COLUMN/20061110/253343/