パスワード生成に対する初期パスワードの影響

○上田卓司¹・高橋 優²

(¹早稲田大学教育学部・²埼玉工業大学基礎教育センター)

キーワード：パスワード生成方針 初期パスワード, 情報セキュリティ

Effect of the initial passwords on password composition

Takashi UEDA¹, and Masaru TAKAHASHI²

(¹Waseda Univ., ²Foundation Study Center, Saitama Institute of Technology,)

Key Words: password composition policy, initial password, information security

目 的

Campbell & Kleeman (2011) は、パスワード生成場面において厳格な生成指針を明示することが、有意味度の低い安全なパスワード生成につながることを示したが、高橋・上田 (2012) の報告では、使用文字長や文字種の多様性という点で単に生成指針を明示するだけでは不十分であることを示唆している。この原因として考えられる事は生成指針における具体性の欠如である。「アルファベットの大文字小文字の両種を含むこと」といった指針は生成における制約条件として機能するが、指針に完全に準拠し生成したとしても、制約を満たす文字列は無数に考えられ、それらのパスワードとしての安全度は一様ではない。また、ユーザはなるべく記憶負荷が低い／簡便なものを選ぶであろうことを考慮すると、生成されるパスワードは相対的に安全度の低いものになることが予想される。そこで考えられる方策が具体例の提示である。長く複雑な文字列を例として提示することで、ユーザは使用可能文字列集合の中から、具体例に近い文字列を生成するようになるのではないか。本研究ではこの予想の下、文字列の長さや複雑さ（文字種の多様性）を変化させた初期パスワードを例示することが、パスワード生成文字列にどのように影響するかを検討した。実験条件は4つ（長いがシンプル；Ls, 長く複雑；Lc, 文字列長は短い複雑；Sc, 短くシンプル；Sc）とし、初期パスワード例を提示しない（Ct1）統制条件を設けた。

方 法

実験参加者 大学生 81 名（男性 39, 女性 42, 平均 19.3 歳）をランダムに4つの実験条件と統制条件の5群に割り当てた。

材料・装置 4 条件について、表 1 にまとめた文字列を初期パスワードとした。課題制御、刺激の提示及び反応取得は全てコンピュータ・プログラムを作成し実行した。

手続き 実験参加者は、まず新規に利用するネットワークサービス用のパスワードを生成することが求められた。生成用の入力画面には、Campbell & Kleeman (2011)、高橋・上田 (2012) と同様に厳格なパスワード生成指針が提示され、また、統制条件群以外の実験参加者には同時に生成例として初期パスワードが提示された。教示として、これまでに未使用の新奇なパスワードを生成することが強調された。パスワード生成ステージに引き続き、課題として日本語版 RST (リーディングスパンテスト) を実施した。本課題はパスワードの生成・管理方針と記憶との関連を検討するためのもので、同じコンピュータ・プログラム上で行われた。課題終了直後に、RST 得点のフィードバックを行ったが、画面表示の際に実験参加者は、生成したパスワードを入力することが要求された。3 回続けてパスワード入力を誤った参加者に対しては、警告画面の後に RST 得点のフィードバックを行った。最後に、普段のパスワード更新頻度や利用しているネットワークサービス数等のアンケートを実施し、1 名あたり約 15 ～ 20 分の実験セッションが終了した。

表 1 提示した初期パスワード

complexity	Password Length	
	Long	Short
simple	very1nice2see3u	9abc
complex	=&s33kQr12+5M\$2	J+4w

結 果

個人情報保護の観点から、アンケートにおいて生成させたパスワード文字列を分析対象に含めることに同意した 64 名 (79%) 以外については、文字長以外のパスワード情報を記録・保存せずにプログラムの実行を終了した。また同意の可否を度外視し、アンケートへの回答から、氏名等の個人情報を含むパスワード文字列を生成した場合や、既存パスワードと同一文字列を生成した場合にも同様の措置をとった。この結果、文字種の組み合わせ等、生成パスワード自体の性質の分析に関しては、81 名中 40 名分のデータのみを使用した。

文字長に対する効果 例示条件ごとのパスワード生成文字長中央値は Ls=9, Lc=7, Ss=8, Sc=7.5, Ct1=8 であり、例示条件による生成文字長に差は見られなかった。

文字種や組み合わせに対する効果 生成文字列判明分の 40 データについて文字列の詳細を分析したところ、23 名分については、英語もしくはローマ字読みの日本語として発音可能なトリグラム以上の文字列が存在し、そのうちの 17 については有意味な単語であると推測された。使用文字種については、4 種（小文字、大文字、数字、記号）の全てを用いてパスワード生成を行ったのは 1 名分であり 37 名 (92%) の実験参加者は 2 種までの文字種でパスワードを生成した。文字種の組み合わせは小文字→記号 (17 名)、小文字のみ (8 名) 小文字→数字→小文字 (4 名)、数字のみ (4 名) の順でのパターンが見られた。なお、生成文字列のパターンや文字種の多様性に対する初期パスワードの明確な影響は確認されなかった。

考 察

今回の実験からは、厳格な指針の明示に加え初期パスワードを例示しても、安全度の高いパスワード生成を必ずしも促すとは限らないことを示唆するものであった。セキュリティ面より強固なパスワード生成・管理行動を促すためには、リスク知覚や性格・行動特性といった、本研究のものとは異なった側面からのアプローチも必要であると考えられる。

引用文献

- Campbell, J., Ma, W. & Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behavior & Information Technology*, 30 (3), 379-388.
 高橋 優・上田卓司 (2012). 生成されたパスワードに及ぼす生成方針の効果. 日本心理学会第 76 回大会発表論文集, 1AM822.