固定パスワード（Reusable Password）再考

内田　勝也‡

情報セキュリティ大学院大学‡

１．はじめに

情報処理システムでは、利用者が誰であり、その利用者がシステムを利用する権限を保持しているかの判断を行う方法を個人識別、個人認証と言っている。

個人認証機能は３つの種類がある。

① 持っているもの(SYH: Something You Have)
② 知っているもの(SYK: Something You Know)
③ 自分自身(SYA: Something You Are)

個人認証の仕組みとして、古くから固定パスワード（Reusable Password）が使われてきたが、簡単に類推できるか、そうでないものは覚えにくいといった問題点が指摘されてきた。

これを解決するため、新しい概念の認証方式として、ワンタイムパスワードやバイオメトリック（生体認証）を利用したものが提案され、使われているが、従来型の固定パスワード方式がなくならない。この様な現状を考え、固定パスワードによる認証方式を進化させることも大切ではないかと考えた。

２．現行の固定パスワードについて

どの様な固定パスワードが良いパスワードであり、悪いパスワードは何かといったことはについて、いくつかの例が挙げられている[1][2]。良いパスワードとしては、利用者には覚えやすく、他人には推測し難いもので以下のものが良いパスワードと言われている。

① 大文字と小文字が混在している
② 文字だけでなく数字や記号が含まれる
③ 制御文字や空白文字が含まれる
④ 覚えやすい、書き留めておく必要がない
⑤ 最低７文字または８文字である
⑥ 肩越しにのぞかれても覚えられないように素早く入力できるもの

また、悪いパスワードとしては、

① 利用者や配偶者、子供、同居人、友人、同僚、小説、映画、テレビ、漫画等の登場人物などの名前
② ありふれた人名
③ 利用ＯＳ名やコンピュータのホスト名
④ 電話番号、自動車のナンバープレート番号
⑤ 地名や固有名詞
⑥ 一種類しか文字を使わないもの
⑦ キーボード上の単純な文字パターン
⑩ 1234567 等の連続した番号
⑪ 上記を逆さまにしたもの
⑫ 上記の先頭、最終に１文字け追加したもの

具体的には良いパスワードとして以下のようなものが考えられる。

① 短い言葉を２つ選び、特殊文字や番号でそれらを繋げる。例えば、「robot4my」や「eye-con」等。
② 自分の知っている文章、歌などを利用してパスワードを作成する。例えば、「Ttl*Hiww」（Twinkle, twinkle, little star. How I wonder what ….）
③ The vanity plate（１つのフレーズ等を他の英数記号で置き換える）
　・Too late again ⇒ 2L8again
④ Compound words（合成語）
　・Tunafish ⇒ toona&Fish2
⑤ Keyboard patterns（キーボード配列の利用）
　・An horizontal zigzag starting with the letter 'r'（ｒから始まって上下の文字を利用するもの）⇒ r5t6y&u8

３．新概念の個人認証の特徴

ワンタイムパスワード、バイトメトリックス等の新しい認証方式も多くの長所があるが、実装段階ではいくつかの問題点も指摘されている。

① 個人認証が必要な機器（パソコンや PDA）に、認証用のソフトウェアやハードウェアを追加しなければならない。
② 追加のためのハードウェア、ソフトウェアの導入費用が必要になる。
③ 複数のシステムへの対応が難しい。

個人認証システムの実装段階におけるこのような問題が固定パスワードによる個人認証に多

Effective use for a reusable password

‡「Katsuya Uchida, Institute of Information Security」

くの問題がありながら、普及しない要因になっていると思われる。

４．固定パスワード方式に対する新提案

現行の固定パスワードの問題点や解決方法について２で述べたような方法を現場レベルでは提案されているが、利用者になかなか浸透しない。この原因は色々あるが、方法を覚えるのが面倒、複数のパスワードを利用する場合、いくつものパスワードを記憶できないといった問題が指摘されている。更に、パスワードの作成方法を教えることに問題であるとの指摘もある。

このような問題を解決方法として従来の固定パスワード方式の延長上での解決方法を検討した。即ち、以下のような条件を満足できるものを実現できないかを検討した。

① 簡単に類推できないパスワードの利用
② 辞書攻撃で解読できないパスワードの生成
③ また、総当たり攻撃でも耐えうる長いパスワードも利用できる
④ 簡単に作成でき、利用も簡単にできる
⑤ 複数の個人認証にも同一方法で対応できる
⑥ 簡単に覚えることができる

このため、以下の条件を満足する表を作成し、それを利用者に使わせることを考えた。

① 乱数を利用し、利用できる文字種類の中から選択できるようにする
② どの様な長さのパスワードにも対応できるように、多くの文字種類の中から必要な長さを選択できるようにする
③ 利用者が覚えやすく、他人から類推し難くするために、パスワードそのものを覚えるのではなく、入力パターンを覚えればよい

例えば、10 行×10 列の表を考え、利用可能な文字種類の中からランダムに選択した 100 個の文字を一覧表にしたものが表１である。

例えば、１列目と２列目を縦に１文字おきに 10 文字をパスワードとして利用する場合には、「**#Z!'"a89e0**」（表１網掛けがある部分）がパスワードになる。

従来の固定パスワードでは文字列を覚える必要があり、10 桁のパスワード「**#Z!'"a89e0**」を覚える必要があったが、この方式では、１列目と２列目の文字を１つおきにパスワードとするというように利用者が覚えやすいパターンを覚えるだけで良いため、この表を印刷して持っていても、何をパスワードとして利用しているか分からない。

表１では、10 行×10 列の表を作成したが、行列の値は適当なものを利用できる。

また、パスワードとして利用する文字位置も利用者が自分で最も覚えやすいものを選択できるため、単純に行とか列を利用するのではなく、左上から右下斜めに利用するとか、左下から右上斜めに利用するとか、三角形、KとかUなどの文字形を利用することも考えられる。

	1	2	3	4	5	6	7	8	9	0
1	#	a	o	*	I	g	A	U	\	3
2	$	b	p	}	J	j	D	X	[	6
3	Z	8	l	;	F	d	x	R	|	_
4	(	f	t	.	N	h	B	V	@	4
5	!	9	m	+	G	i	C	W	`	5
6	Y	7	k	{	E	c	w	Q	~	?
7	‘	e	s	<	M	b	v	P	=	/
8	e	y	S	−	1	f	z	T	^	2
9	“	0	n	:	H	&	d	r	,	L
0	%	c	q	]	K	a	u	O	)	>

表１ 乱数を利用して作成したパスワード表

また、複数パスワードを利用する場合には、１つの表から複数のパターンを利用してもよい。あるいは、表を複数作成して、各システムによって表を使い分けることも可能であろう。

なお、表については最も簡単に作成するのであれば、MS Excel 等の表計算ソフトを利用して作成して利用者に配布する方法を使って実際に作成したが、特に問題になるような事はなかった。

大規模な場合には、独自に乱数を利用して作成することも１つの選択肢として考えられる。

５．今後の課題

この方法では、パスワードは一定期間固定であり、また、通常のパスワード方式を利用している限り、プレーンな文字列が回線上を流れるため、ワンタイムパスワードのように回線上で盗聴が行われている場合には、パスワードが漏洩してしまう恐れがある。

これを防止するためには、単純な固定パスワード方式を採用するのではなく、この考えを更に発展させ、疑似的なワンタイムパスワード方法の採用も考えられ、更に安全な仕組みを構築できると考えている。

参考文献

[1] S. Garfinkel, G.Spafford(山口英監訳),『UNIX &インターネットセキュリティ』, オーム社、1998
[2] http://www.securityawareness.com/files/protectit demo.pps