パターン記憶パスワード

内田勝也(Katsuya Uchida)
Assistant to CIO of City of Yokohama &
Emeritus Professor at Institute of Information Security[1]

1. はじめに

パスワードとして、gd}1Rb~4dI や }eQUuOc_Tq を割り振られたら、覚えていられるだろうか？

多分、大部分の人は無理だと回答する。10 桁の任意の文字列を記憶できる人は殆どいない。

しかし、図１の様な乱数表を考え、gd}1Rb~4dI は、5 行５列から始まり、１つ上の内容から時計回りに、10 文字を順番にみていけば、この文字列になる。 また、}eQUuOc_Tq は、図２で同じ方法で 10 文字採用したものである。

図１及び図２では、該当する文字部分に色づけをしているため、どこが該当する文字列であるかを簡単に判別できるようにしている。

パスワードポリシーとして、長い文字列がパスワードだと言われても、この方法であれば、文字列を覚えるのではなく、文字列のパターンを決めるだけであり、この様な乱数表を利用する限り、あまり問題はないと考えている。

また、パスワードとして複数が必要な場合には、この乱数表を複数作成し、同じパターンを新しいパスワードとして利用すれば、同じパスワードを利用することもないであろう。

	User-ID:								2011/12/14	
	1	2	3	4	5	6	7	8	9	10
1	3	(	P	l	2	E	U	;	v	(
2	Z	Y	=	u	5	Z	P	4	U	=
3	Y	0	o	I	A	S	G	)	H	=
4	6	R	J	d	d	}	@	W	|	W
5	x	9	A	4	g	1	[	A	C	A
6	)	}	P	~	b	R	i	V	N	g
7	f	$	g	)	0	L	3	g	H	}
8	l	I	h	[	u	)	[	T	y	;
9	;	~	!	[	N	W	q	?	6	[
10	e	l	Q	0	g	x	%	{	[	r

図１

	User-ID:									2011/12/14
	1	2	3	4	5	6	7	8	9	10
1	G	.	v	B	Z	&	_	h	5	b
2	0	I	W	I	2	*	2	?	U	3
3	P	m	0	q	1	z	:	"	U	Q
4	_	G	O	T	e	Q	{	_	i	'
5	h	O	(	_	}	U	|	"	O	p
6	0	o	K	c	O	u	z	]	X	V
7	V	A	T	?	]	B	w	9	E	n
8	o	Z	Z	B	D	\	)	c	z	#
9	8	[	`	8	I	%	d	W	,	$
10	h	6	g	e	@	B	H	S	<	_

図２

更に、一定期間毎にパスワードを更新する様なセキュリティポリシーの場合でも、この乱数表を新たに作成して、それを利用すれば、過去のパスワードと同じパスワードを利用禁止のポリシーがあっても問題はない。

2. 利用方法

(1) 乱数表の印刷

このシステムの利用者は、マイクロソフト エクセル（EXCEL）が利用できるこ

[1] Graduate School in Japan

uchidak@gol.com

とを前提にしています。

- EXCEL シートを開くと、画面上部に図３に示すような内容があります。真ん中の枠内に、１～４の数字を入力し、乱数表に利用できる文字種類を決めます。即ち、１： 英子文字と数字のみ、２： 英子文字と数字、記号、３： 英文字と数字、４：英文字と数字、記号 の４種類の乱数表を作成できます。
- １～４以外の数字を入力すると、枠下に「**Enter(1-4)**」と表示されますので、正しい値を入力し直して下さい。

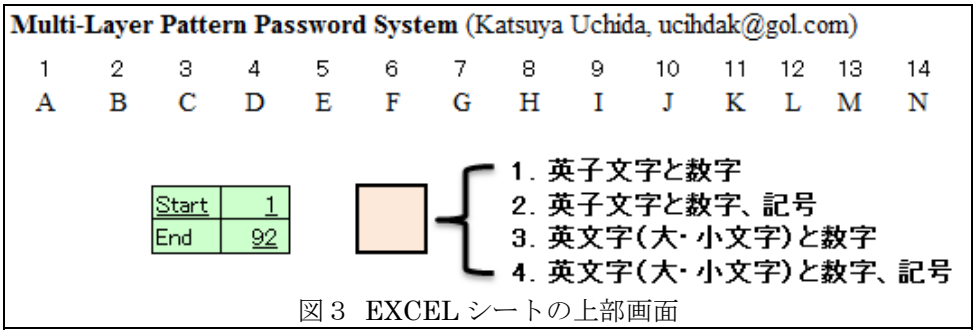


図３ EXCEL シートの上部画面

- 正しく入力ができれば、印刷が可能です。 印刷では、A4 版に６つの乱数表を印刷するようになっています。

(2) 乱数表の利用方法

- 乱数表を使うには、まず、どの様なパターンを利用するかを考えます。 あまり簡単なパターンは万一乱数表を盗まれたりした時に、推測されやすいので、図４左に示す様な １ 列目を選択し、上から順に利用するとか、図４右の１行目を左から順に利用すると言ったものは避ける方が良いでしょう。
- 乱数表で、どの様なパターンを利用するかが、このシステムを利用する場合に最も重要なことです。

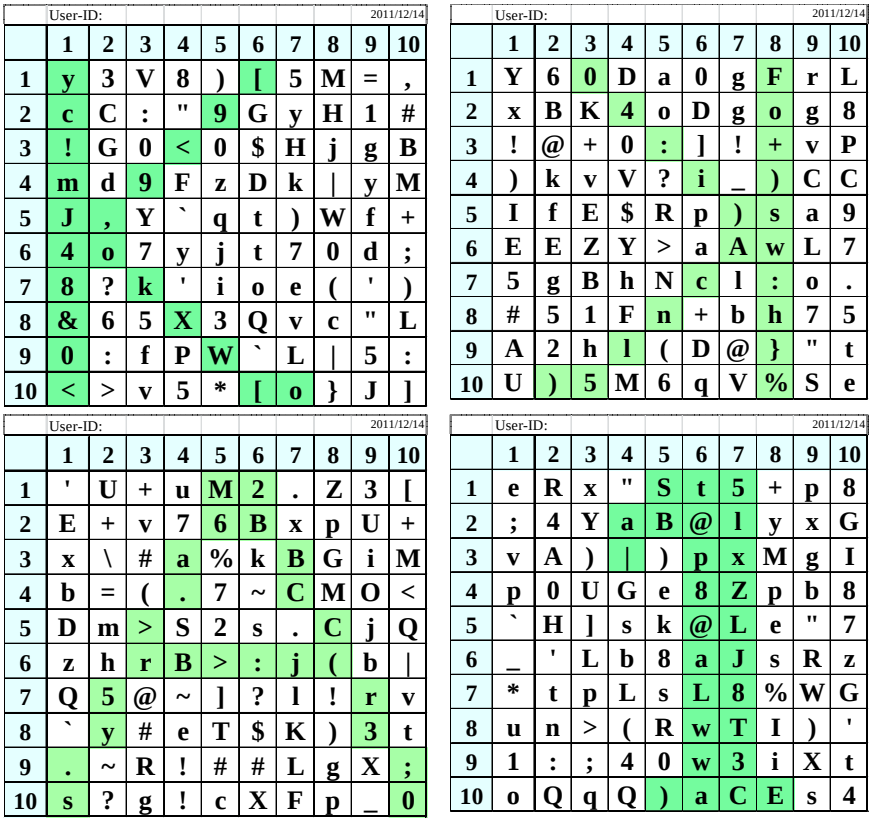
	User-ID:								2011/12/14	
	1	2	3	4	5	6	7	8	9	10
1	n	z	n	t	1	m	P	"	*	E
2	:	:	n	u	x	+	>	2	\	+
3	`	h	3	t	!	V	r	0	9	R
4	+	:	~	v	s	a	U	j	f	a
5	b	{	N	n	w	W	h	;	5	W
6	E	_	\	~	]	2	p	M	6	}
7	*	"	k	+	%	!	K	z	6	e
8	h	f	P	x	'	[	n	4	j	~
9	<	j	@	n	Y	H	B	%	Y	@
10	#	A	[	9	u	!	m	t	f	8

	User-ID:								2011/12/14	
	1	2	3	4	5	6	7	8	9	10
1	n	z	n	t	1	m	P	"	*	E
2	:	:	n	u	x	+	>	2	\	+
3	`	h	3	t	!	V	r	0	9	R
4	+	:	~	v	s	a	U	j	f	a
5	b	{	N	n	w	W	h	;	5	W
6	E	_	\	~	]	2	p	M	6	}
7	*	"	k	+	%	!	K	z	6	e
8	h	f	P	x	'	[	n	4	j	~
9	<	j	@	n	Y	H	B	%	Y	@
10	#	A	[	9	u	!	m	t	f	8

図４ 良くない例

- 図５に例を示しましたが、左上の乱数表では英文字「K」をパターン化していますが、全ての文字を利用（「yc!mJ48&0<[9<9,okXW[o」）することも可能ですが、上から、左・右の順で文字を選択（「y9!9Jo8X0」）することも考えられます。
- 要は、自分が覚えやすいが、簡単には類推できないパターンを考えてみることが大切です。

- もう 1 つ重要なことは、図５では、例として分かり易くパターンを塗りつぶしていますが、パターンを塗りつぶすのはお勧めしません。　パターンを覚えていれば、他人にこの乱数表を見られても、パスワードを類推される可能性は低くなります。



User-ID: 2011/12/14

	1	2	3	4	5	6	7	8	9	10
1	y	3	V	8	)	[	5	M	=	,
2	c	C	:	"	9	G	y	H	1	#
3	!	G	0	<	0	$	H	j	g	B
4	m	d	9	F	z	D	k	|	y	M
5	J	,	Y	`	q	t	)	W	f	+
6	4	o	7	y	j	t	7	0	d	;
7	8	?	k	'	i	o	e	(	'	)
8	&	6	5	X	3	Q	v	c	"	L
9	0	:	f	P	W	`	L	|	5	:
10	<	>	v	5	*	[	o	}	J	]

User-ID: 2011/12/14

	1	2	3	4	5	6	7	8	9	10
1	Y	6	0	D	a	0	g	F	r	L
2	x	B	K	4	o	D	g	o	g	8
3	!	@	+	0	:	]	!	+	v	P
4	)	k	v	V	?	i	_	)	C	C
5	I	f	E	$	R	p	)	s	a	9
6	E	E	Z	Y	>	a	A	w	L	7
7	5	g	B	h	N	c	l	:	o	.
8	#	5	1	F	n	+	b	h	7	5
9	A	2	h	l	(	D	@	}	"	t
10	U	)	5	M	6	q	V	%	S	e

User-ID: 2011/12/14

	1	2	3	4	5	6	7	8	9	10
1	'	U	+	u	M	2	.	Z	3	[
2	E	+	v	7	6	B	x	p	U	+
3	x	\	#	a	%	k	B	G	i	M
4	b	=	(	.	7	~	C	M	O	<
5	D	m	>	S	2	s	.	C	j	Q
6	z	h	r	B	>	:	j	(	b	|
7	Q	5	@	~	]	?	l	!	r	v
8	`	y	#	e	T	$	K	)	3	t
9	.	~	R	!	#	#	L	g	X	;
10	s	?	g	!	c	X	F	p	_	0

User-ID: 2011/12/14

	1	2	3	4	5	6	7	8	9	10
1	e	R	x	"	S	t	5	+	p	8
2	;	4	Y	a	B	@	l	y	x	G
3	v	A	)	|	)	p	x	M	g	I
4	p	0	U	G	e	8	Z	p	b	8
5	`	H	]	s	k	@	L	e	"	7
6	_	'	L	b	8	a	J	s	R	z
7	*	t	p	L	s	L	8	%	W	G
8	u	n	>	(	R	w	T	I	)	'
9	1	:	;	4	0	w	3	i	X	t
10	o	Q	q	Q	)	a	C	E	s	4

図５　パターンの例

注）乱数表にパターンのマークを入れないようにする

- 図６では、乱数表を実際に利用する場合の例を示しました。　この例では、User-ID を書いてありますが、この様な方法もパスワードが分からなければ問題ありません。
- また、A4 版用紙に６つの乱数表を印刷しますので、一定期間毎にパスワードを変更するようなパスワードポリシーの場合でも、それらを１つづつ使っていけば、同じパスワードになることも殆どありませんので、A4 用紙で６回分のパスワードを利用できます。　更に使う場合には、再度、印刷をすれば問題問題ありません。

uchidak@gol.com

User-ID: Google ID 2011/12/16

	1	2	3	4	5	6	7	8	9	10
1	N	w	)	)	[	l	<	F	L	1
2	u	g	t	l	!	$	b	&	3	\
3	X	l	f	z	H	S	R	)	m	f
4	)	e	9	O	$	d	P	M	%	6
5	f	l	~	&	C	w	\	J	K	w
6	e	h	W	F	%	:	B	L	b	Z
7	J	8	(	S	l	i	\	Y	u	}
8	p	V	#	M	}	7	(	z	B	u
9	?	S	f	#	N	$	M	'	Q	w
10	m	]	T	.	@	3	;	o	G	k

図６ 乱数表の例

3. まとめ

(1) パスワードポリシー

- 強力なパスワードポリシーとして、例えば、
  - パスワード長が 10 桁以上必要
  - パスワード文字種には、英文字、数字、記号の全てを含む
  - パスワードは３０日毎に変更しなければならない
  - 新しいパスワードは、過去６つのパスワードと同じではならない

  と言うようなものでも、全く問題なく利用できる

(2) その他

- このシステムの目的はワンタイムパスワードや生体認証等の認証システムを代替するものでなく、既存のユーザ ID／パスワードシステムへの対応を考えたもの。　特にウェブサイトのサイバー攻撃により、パスワードが流出し、短いパスワードやユーザ ID と同じパスワードが解読されたり、同じパスワードを複数のシステムで利用するケースなどを避ける目的です。
- このシステムでは、今まで利用しているサーバやクライアント側のソフトウェアを何ら変更せずに利用できる。
- また、このシステムでは、スパイウェアなどが導入されている場合には有効でない。

(3) 今後の課題

- このシステム全体をスマートホン等で利用できるようにしたい。

Note:

乱数表作成プログラム

http://www2.gol.com/users/uchidak/research/RandomPassTable_JPN.xls

本説明文書

http://www2.gol.com/users/uchidak/research/RandomPassTable.pdf

Reference

[1] 内田勝也, “情報セキュリティマネジメントからの個人認証システムの提案”, 2006.04, JSSM　http://www.uchidak.com/papers/20060406_Uchidak.pdf

uchidak@gol.com