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

The Proposal of Personal Authentication System from Information Security Management

情報セキュリティ大学院大学　**内 田 勝 也**
Institute of Information Security　**Katsuya Uchida**

【概　要】

個人認証システムとして、パスワードが利用されてきたが、パスワードの問題点は 20 年以上も前から指摘されてきた。しかし、情報セキュリティ先進国と言われる米国でも継続的な調査結果をみる限り、パスワードが未だに 50%程度の企業・組織で利用されている。そこで、固定パスワードによる個人認証に若干のコストを追加するだけで、セキュリティ強度を高めるとともに利便性を向上させる仕組みを検討した。この提案により、企業・組織における情報セキュリティ強化に貢献できると考える。

提案システムでは、固定パスワード利用の延長として、パスワード候補表を作成し、その表の位置パターンを利用者が覚え、その位置パターンにある文字をパスワードに利用する。なお、パスワード候補表の縦・横の文字数、利用できる文字種、パスワードの更新頻度等は、企業・組織におけるパスワードポリシーに従って決めることができる。

キーワード： 位置記憶認証、拡張固定パスワード認証、個人認証、情報セキュリティマネジメント、パスワード、

１．パスワード利用の現状と問題点

情報システムの環境においては、個人認証の仕組みとしてパスワードが利用されている。わが国では、パスワードが比較的抵抗なく利用されるようになったのは、個人情報保護法の施行が、１つのきっかけであると思われる。

しかし､パスワードの問題は 20 年以上も前から指摘されており、その代替として、生体認証やワンタイムパスワード等が早くから提案されてきた。それにもかかわらず、パスワードの使用比率は必ずしも低下していない。

米国の CSI/FBI の調査[1]では､生体認証は 15%、PKI[1]は 35%に止まり、従来のパスワード[2]（固定パスワード）は 52%に達している（表１）。また、中央大学 21 世紀 COE 研究の一環として筆者が実施している情報セキュリティ調査[2]では、生体認証、PKI が各 7%、固定パスワードが 79%となっている（表２）。

調査年	固定パスワード	生体認証	PKI	回答数
1998 年	53%	6%	―	512
1999 年	61%	9%	―	501
2000 年	54%	8%	―	629
2001 年	48%	9%	―	530
2002 年	44%	10%	―	500
2003 年	47%	11%	―	525
2004 年	56%	11%	30%	483
2005 年	52%	15%	35%	687

表１ CSI/FBI 調査資料からの編集[3]

[1] PKI：Public Key Infrastructure は、公開鍵暗号技術と電子署名を使用して、安全な通信ができるようにするための環境。「公開鍵基盤」と訳される。

[2] 「固定パスワード（Fixed Password)」とか、「再利用可能パスワード（Reusable Password)」と呼ばれるが、ここでは固定パスワードとした。

[3] 表中の調査年は調査発表年であり、調査は前年に実施されている（表２も同様)。

調査年	固定パスワード	生体認証	ＰＫＩ	回答数
2004 年	88%	4%	5%	1326
2005 年	79%	7%	7%	1187

表２ 国内調査

このような状況を見ると、新たな個人認証システムを考えることも必要であるが、固定パスワードの仕組みの改良や固定パスワードの利用者に対して、情報セキュリティ教育や周知が、セキュリティレベルを高める上で、必要であると考える。

新しい個人認証システムを提案しても、その投資対効果や利用の容易性、さらには提案システムの物理的問題点（大きさ等）の打開策、提案システム全体の脆弱性が公開された場合の解決方法等が示されなければ、安心して提案システムを利用できないことは容易に想像できる。

２．個人認証システムについて

2.1 個人認証について

情報処理システムでは、その利用者がシステムを利用する正当な者であるかを判断する方法を個人認証と言う。

個人認証には、以下の３つの要素があり、これらの１つあるいは複数を使って個人の認証を行う。

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)

これらの内、「①持っているもの」には、磁気カードやICカード等がある。

「②知っているもの」では、固定パスワードが古くから使われてきた。

固定パスワードは、前述したように古くからその問題点を指摘[3]されてきたが、利便性、投資対効果等から、現在でも無くなる気配がない。

固定パスワード以外に、「②知っているもの」には、ワンタイムパスワードや位置記憶認証[4]（ピクチャーパスワード[4]、画像パスワード[5]等）などが提案されている。

「③自分自身」を利用するものには、バイオメトリックス（生体）認証がある。

個人認証を行う場合、一般的には、利用者、認証サーバの二者間で行われるが、信頼できる第三者を含めた形で行われるものもある。

2.2 固定パスワードについて

固定パスワードは古くから利用されているが、パスワードポリシーは認証側（認証サーバ）が決め、個別のパスワードは利用者が決める。

最近のコンピュータでは、パスワードポリシーを相当詳しく設定[6]できるが、管理の煩雑さ等から、詳細な設定を行わない場合もある。

初期段階では、パスワードの重要性の認識が低かったため、あまり詳細なパスワードポリシーは設定しにくかったようである。

これらに対処するため、管理・運用面から、良いパスワードや悪いパスワードについて書籍などで取り上げられていることが多かったと考える[7]。

例えば、良いパスワードとは、利用者が覚えやすく、他人には推測し難いもので、以下の特徴を持つものと言われている。

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 覚えやすく、書き留めておく必要がない
⑤ 最低７文字または８文字からなっている
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

一方、悪いパスワードは、以下の特徴を持つと言われている。

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

[4] 「位置記憶認証」：筆者の造語で、利用者側から位置情報を認証サーバに送付し、その情報を基に認証を行うもの。代表的なものには、絵や写真を複数表示し、クリックした位置や順番情報を使って認証する。

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 一種類の文字のみを使用するもの
⑦ キーボード上の単純な文字パターン
⑧ 1234567 等の連続した番号
⑨ 上記を逆順にしたもの
⑩ 上記の先頭、最終に１文字だけ追加したもの

しかし、これらを理解できても、多くの利用者は良いパスワードを具体的に作成・使用することは難しい。このため、安易なパスワードを利用したり、紙に書いて貼っておくこともある。

良いパスワードを作成するために必要な教育・周知方法が分からなかったり、明確なパスワードポリシーがないことも原因の１つと考えられる[5]。

例えば、2000 年に米国 Washington Post 紙に掲載された米国エネルギー省におけるパスワードの調査記事[8]によると、パスワードポリシーがないため、多くの従業員は、姓やイニシャル等を使っており、更に単純なケースでは、「password」という文字そのものをパスワードに利用していると述べている。

一方、この様な状況を打破するために、良いパスワードを作成するための提案[9]も行われている。

① Compound words: 短い言葉を２つ選び、特殊文字や番号でそれらを繋ぐ。
・Flower Paper ⇒ Flower+Paper
・Tunafish ⇒ toona&Fish2
② Phrase acronym: 文章や歌などを利用して、各フレーズの先頭の文字を利用してパスワードを作成する。
・Twinkle, twinkle, little star. How I wonder what …. ⇒ Ttl*Hiww
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 Keyboard patterns：キーボード配列を利用する。
・ｒから始まり、文字を上下のジグザグで利用する ⇒ r5t6y&u8

これらの提案も１つのパスワードしか使っていない場合は便利で、利用しやすい。しかし、複数のパスワードを持っており、1～2 ヶ月ごとに１回、パスワードを変更しなければならない利用者は、パスワード変更時に、その直前に必要な数のパスワードを考えて準備しておく必要がある。このため、利用者の多くは、全てのシステムで、同一パスワードを使用したり、いくつかのパスワードを適当な間隔で使いまわす傾向がある。

最近、国内金融機関のキャッシュカードに関連した事件で、ゴルフ場のロッカーに保管したキャッシュカードがスキミングされた。ゴルフ場等のロッカーの暗証番号とキャッシュカードの暗証番号が、多くの場合、同一[10]で、また、複数の金融機関の暗証番号が全て同じであったため、多額の現金を窃取された。この例からも適切なパスワードや暗証番号を使うことが実務的に極めて困難なことは明らかである。

しかしながら、各企業等でのパスワード教育はあまり実施されていないという問題がある[6]。

---

[5] 1997 年１月、（財）データ通信協会が、賛助会員、ネットワークセキュリティ登録事業者協議会会員等を対象にしたアンケートでは、パスワードの定期的変更を実施しているのは、約 31%、検討中 44%、予定なし 25%。社員のパスワード管理が徹底しているは 27%、一部守らない 65%、ほとんどが守らない 8%となっている。

[6] Goo Research," 企業の情報セキュリティに関する調査結果" 2003 年 6 月調査、
http://research.goo.ne.jp/Result/000129/index.html
なお、2005 年 12 月、セキュリティベンダーがパスワード教育用ソフトが無償公開した。
http://www.securityfriday.com/jp/contents/ninjutsutaikai.htm

2.3 バイオメトリックス認証について

バイオメトリックス（生体）認証は、人間の体の一部を認証情報として利用する個人認証である。現在、バイオメトリックスとしては、①指紋、②網膜、③虹彩、④顔、⑤静脈、⑥声紋、⑦DNA 等がある。システムの価格、大きさ、判断までの時間等により、現時点では、パソコンで利用できるのは、指紋、指静脈程度に限定される。

バイトメトリックスは、実装段階でいくつかの問題点も指摘されている。

① サーバ側にソフトウェアを導入するだけでなく、利用者側（PC）にも認証用ソフトウェアやハードウェアを実装する必要がある。

② ハードウェア､ソフトウェアの導入費用が高い。最近、指紋認証システム等では、１万円を切るものもあり、従来からみると安価になった。しかし、端末機１台ごと/システム全体と対比してみると、相対的にコスト増になっている。

③ パソコンに組み込まれている指紋認証では、認証できない場合を考慮し、固定パスワードでの認証も許している。このため、固定パスワードを知っていれば、なりすましが可能になる。

④ 複数のシステムへの対応が難しい。 複数システムでバイオメトリックスを利用する場合、パソコンに対して認証（機器認証）を行い、その後の手順は固定パスワードの処理手順で行う等の対応が必要になることもある。

⑤ 実装段階で本人を拒否(本人拒否率)したり、他人を受容する（他人受容率）可能性をゼロにできない（図１）。また、生体を利用しているため、登録できない個人が発生することがあり、多数が利用するシステムでは、設計に当たり登録不能の利用者を前提にシステムの構築を考える必要がある。

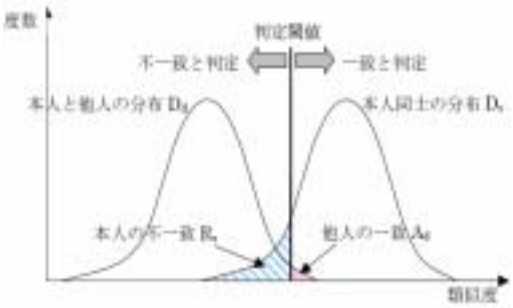

図１　本人拒否と他人受容の関係
(財) 情報処理振興協会､「本人認証技術の現状に関する調査報告書」2003 年 より

・ 本人と判定する閾値の設定(中央縦棒の位置)により、本人を拒否(図のＲｓの部分)したり、他人を受容(図のＡｄの部分)することがある

⑥ 社会的受容性を考慮する必要がある。[11] 例えば、指紋認証は、日本では刑法犯や外国人登録に長年利用されてきたため、指紋認証について社会的な受容性を高める必要がある。

⑦ 人間の「生体」を利用しているため、その一部を切り取られる事件[12]が発生している。指紋認証等の場合には、こうした事件が現実の世界でも起きる可能性があることを示している。

⑧ システムの構築方法により､生体データが漏洩した場合、システム全体が崩壊してしまう可能性がある。

⑨ 偽造などを含めたバイオメトリックスへの攻撃研究が進んでいないため、実際にどの様な脆弱性があるかについての研究[7]はまだ遅れている。

2.4 ワンタイムパスワードについて

① サーバ側にソフトウェアを導入するだけでなく、利用者側（PC）にも認証用のソフトウェアやハードウェアを実装する必要がある。

② 導入費用が高い。

③ 複数のシステムへの対応が難しい。

---

[7] 山田浩二，松本弘之，松本勉，" 指紋照合装置は人工指を受け入れるか"，2001，情報処理学会

④ サーバ側と同期を取る必要があるため、何らかの理由で同期がずれると、認証ができなくなることがごく希に発生する。
⑤ トークンと呼ばれる機器を利用している場合、機器を落としたり、ぶつっけて、壊してしまう問題がある。
⑥ また、トークンは電池を利用しているため、数年毎にトークンを配布しなおさなければならない。

2.5 「位置記憶認証」について

位置記憶認証には、複数の写真や絵を利用者画面に登録して、その位置情報をもとにして認証を行うものである。

① サーバ側にソフトウェアの導入するだけでなく、利用者側（PC）にも認証用のソフトウェアを実装する必要がある。

なお、最近、利用者画面に複数の数字をマトリックス形式で表示し、認証を行うごとに数字を変えてマトリックスを表示し、事前に登録した位置情報に従って数字をクリックする方法がPassLogic[8]という製品名で発売されている。位置記憶認証とワンタイムパスワードの長所を利用したものである。PassLogicでは、ハードウェアを利用しない点の良さはあるが、サーバにソフトウェアを導入するため、そのための費用を考えておく必要がある。

2.6 固定パスワード認証の拡張

(1) 基本的な考え方

固定パスワードの問題点是正のために、2.2で述べたように固定パスワードの作成方式も提案されているが、利用者になかなか浸透せず、情報セキュリティ上の脆弱性の一つになっている。

固定パスワードの問題点として、以下のことが指摘されている。

① パスワードを覚えるのが面倒である
② 安易なパスワードを選択しがちである
③ 複数のシステムを利用する場合、複数のパスワードを記憶することが難しいため、同じパスワードを利用する傾向がある
④ 定期的なパスワード変更への対応が弱い

更に、パスワード作成の実例を教えると、それを使われてしまう恐れがあるとの指摘[9]もある。

このような問題の解決方法として固定パスワードの考え方を高度化して解決する方法がないか検討した。即ち、固定パスワードに求められている以下のような条件を満足できないか検討した。

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

更に、固定パスワードの高度化の条件として、

① 認証サーバは固定パスワード利用と同一でよい。
② 利用者も、原則として固定パスワードの利用と同様でよい。

そこで、以下のような**パスワード候補表**（以下、**PW表**とする）を作成し、それを利用者に使わせることにする。

① 乱数を利用して作成したPW表から、利用者が考えた場所の文字列を固定パスワードとして利用する。
② 固定パスワードについては、認証サーバのパスワードポリシーに従う。　即ち、パスワードの長さ、文字種、有効期間、履歴等はパスワードポリシーで決められたルールに従う。

---

[8] PassLogic、http://www.passlogy.com/

[9] 脚注５の調査で、良いパスワードの例示をすると、「そのまま使う利用者がいる」、「例示した時点で良いパスワードでなくなる」等で反対（11%）が一部にあった。

③ 利用者が覚えやすく､他人から類推し難くするため、パスワードそのものを覚えるのではなく、利用者は表の入力パターンを覚えるだけでよい

④ パスワードの変更は､新しい PW 表を作成し、固定パスワード手順で行っていたパスワード変更手順を認証サーバで行う

例えば､表３に示すような 10 行×10 列の PW 表を作成し、利用可能な文字種類の中からランダムに選択した 100 個の文字を配置する。

利用者は、パスワードとして利用したい任意のパターンルールを考える。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と考えたと仮定すると、

「#Z!’”a89e0」がパスワードになる。なお、表３では分かり易いように網掛け部分がパスワードとして選択するパターンとして示したが、実際に利用する場合には、網掛けをしない。

従来のパスワードシステムでは文字列を覚える必要があるため、「#Z!’”a89e0」と言ったパスワードそのものを覚える必要があったが、この方式では、例えば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った利用者が自分自身で決めた PW 表中でのパターンルールを覚えるだけでよい。

	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３ 乱数を利用して作成した PW 表

この PW 表を印刷して持っていても､どの様なパターンルールを使っているかを知られない限り、他人がパスワードを類推することは難しい。

また、表３では、10 行×10 列の PW 表を作成したが、表の大きさは、組織のパスワードポリシーに従って、適当に作成して構わない。

パスワードとして利用する文字位置は利用者が自分で最も覚えやすいものを選択すれば良いため、単純に行とか列を利用するのではなく、左上から右下斜めの文字列を利用するとか、左下から右上斜めの文字列を利用するとか、三角形、ＫやＬなどの文字の形を利用することもできる。

また、単純に、１列目の文字列を利用する場合でも、６行目から始まり、０行までの５文字と１行目から５行目までの５文字の合計 10 文字をパスワードとして利用すると言った考えもできる。

どの様なパターンルールを利用するか等は、情報セキュリティ教育（パスワード教育）で、教育・周知することが大切になる｡他人に PW 表やパターンを教えない、PW 表をなくした場合、速やかに必要な対応を取る等の教育・周知は大切になる。

また､PW 表は偏りのない乱数を使って作成することが望ましいが、情報システムの重要度を勘案して、簡易に行うことが問題なければ、EXCEL 等を使って PW 表を作成することも考えられる。

(2) 問題点について

固定パスワードの利用の高度化を考えたものであるため、問題点もいくつかある。

(A) キーロガーに対応できない（注1）

基本的な考え方は固定パスワードと同じであるため、キーロガーには対応できない。

最近、キーボードからの入力データをキャプチャーするだけでなく、マウスでクリックした内容をキャプチャーするキーロガーも発見されている。[13] このため、「位置記憶」認証方式でもパスワードをキャプチャーされる可能性がでてきた。 現時点ではこのようなキーロガーはまだ少ないが、今後増加すれば、「位置記憶」認証方式も安全でなくなる可能

性がある。

（注１）キーロガー以外にも、ソーシャルエンジニアリングと呼ばれる技術により、電話を利用してパスワードを聞き出して、正面からシステムへの侵入を図る事件や Phishing と言われる電子メールを利用して、偽のウェブサイトに利用者をおびき寄せて、パスワードを盗む事件等も発生している。
ソーシャルエンジニアリングによって、PW 表のパスワードパターンや利用しているパスワードなどを聞き出されてしまう危険性はある。これらに対抗するには、システム利用者への教育・周知を徹底して行う方法が、現在最も有効なものになっているのが現状である。

(B) PW 表を紛失した場合

バイオメトリックス以外の個人識別手法については、忘れてしまったり、紛失してしまう可能性がある。また、バイオメトリックスでも 2.3 で述べたように、利用している身体の一部を切り取られるという事件を見ると、消失の可能性がないとは言えない。

本提案システムでは、利用者が PW 表を印刷して保持していても他人には理解できないため、１枚は常時利用するために使い、もう１枚は封印した封筒に保管しておくことも考えられる。　万一、利用している表を紛失してしまった場合、封印保管してある封筒を開封して PW 表を利用する。

紛失後の対応は、新しい PW 表を印刷して、そこから新しいパスワードを利用し、古い PW 表のパスワードを廃止することが望ましい。紛失した PW 表からパスワードを類推される可能性があるためである。**（注2）**

(注 2) 金融機関等で利用する乱数表との相違
提案方式で利用している PW 表は、金融機関等がインターネットバンキングで利用している乱数表と同じものではない。金融機関等で利用する乱数表は事前に配布された一覧表を用いて、「チャレンジレスポンス」方式で、センター側から指定された位置の文字（多くは数字）を入力するものである。
金融機関等で利用している乱数表は、事前に送付（一種の鍵配送）しなければならないため、その送付に伴うリスクや少数の文字をチャレンジレスポンス方式で利用することに起因する問題点[14]がある。

(C) 回線上での盗聴

固定パスワードと同じ仕組みであるため、パスワードも平文で回線上を流れる。これを防止するには、SSL や SSH 等で回線上を暗号化して利用することでの対応が考えられる。

ワンタイムパスワード等でも、VPN 回線を利用しており、より安全にするには、SSL 等の方法によって補強することが必要になる。

(D) PassLogic との相違

2.5 で述べたように、PassLogic は、センター側から PW 表を利用者側の PC 等に送付し、画面上で位置をクリックして利用するもので、位置認証とワンタイムパスワードの良さを取り入れたものである。

このシステムでは、認証サーバ側にソフトウェアの導入が必要であり、その初期費用及び、保守費用を考慮する必要がある。

３．情報セキュリティマネジメントからの考察

3.1 固定パスワードの将来

個人認証の問題は、古くて新しい問題であるが、2005 年 9 月に調査会社が開催した「IT Security Summit」において、「2008 年までに、80%の企業が現在のパスワード利用を別の方法に変更するだ

ろう」[10]と述べている。

しかし、１章で述べたように、固定パスワード問題は、20 数年前から指摘されてきたが、米国でも未だ 50%以上の企業・組織が固定パスワードを利用しており、国内では、更に高く、80%近くの企業が固定パスワードを利用しているのが現実である。

3.2 固定パスワードが破られる場合

固定パスワードが破られた場合、関連する情報の破壊、改ざん、漏洩、盗聴等のリスクが発生する可能性がある。

パスワードが破られる原因としては、以下のものが考えられる。

① 固定パスワードの解読
② 有害プログラム（コンピュータウイルス、ワーム等）による被害
③ 社内利用者の不適切利用:権限を持っている者が、コンピュータを適切に利用しなかったために起因するもの。　社内利用者等により、情報窃盗
④ ノート PC 等の盗難など
⑤ ハードウェア故障／ソフトウェアのバグ
⑥ 自然災害等の物理的障害

これらの脅威に対して、投資の優先順位、投資対効果等を明確にし、適切なセキュリティ対策を講じなければならない。この問題に対しては、項をあらためて論ずることとする。

3.3 情報セキュリティのリアルタイム性

情報セキュリティの分野では、ある一定の時間にそれが解読される可能性がなければ、情報セキュリティ強度は、100%に近い強度があると考えられる。逆のケースでは、時間の経過とともに限りなく強度が低くなることもある。

例えば、英数字の 62 文字[11]を利用した 8 文字のパスワードを考えた場合、可能なパスワード個数は、62 の 8 乗（約 2.2×10^{14}）となる。

１秒間に 100 万件のパスワードをチェックできるコンピュータを利用して総当たりでチェックした場合、全てをチェックするには、約 85 ヶ月（約 7 年）[12]かかる。

もし、１ヶ月に１回パスワードを変更するパスワードポリシーで運用されていれば、パスワードが解読される可能性は、約 85 分の 1（1.2%）となる。

また、自分のパスワードが狙われる確率まで考えると、更に低下するであろう。

重要な情報を扱っている場合には、パスワードの有効期間を短縮すれば、パスワードが解読される可能性は更に低くなる。

このように、管理・運用等を含めて考えることにより、システムの脆弱性を限りなくゼロに近づけることを「情報セキュリティのリアルタイム性」[13]と定義する。

ワンタイムパスワードは、このリアルタイム性を利用[14]していると考えることができる。もし、毎回同じ値が入力されれば簡単に解読できてしまう程度の桁数の数値を使っているが、利用している値が毎回変化するために、解読される可能性は低い。

このため、技術的に考えた場合、高い安全性を確保できないシステムについては、情報セキュリティマネジメントの立場からは、「情報セキュリティのリアルタイム性」を考え、管理・運用面から安全性を高める対策を行うことが重要になる。このような対策を行うことによって、情報セキュ

---

[10] Gartner 「IT Security Summit in London」Mr. A. Allan, 2005.09

[11] 英字：26 文字×2（大文字・小文字）、数字：10 文字

[12] パスワード解読の場合には、平均するとその半分の 3.5 年になる

[13] 筆者の造語：なお、以下も参照
http://it.nikkei.co.jp/business/column/njh.aspx?ichiran=True&i=20020408s2000s2s2&page=21

[14] 通常、VPN 回線を利用しているので、回線上を流れる数字を解読することは、簡単ではない。

リティ技術や手順は、一定以上の安全性を確保できる可能性がでてくる。

４．おわりに

筆者は、長年、固定パスワードがバイオメトリックス等に代替されない現実をみてきた。また、ワンタイムパスワードの変種的な方法[15]を利用してきたこともある。

情報セキュリティは、技術面だけでなく、管理・運用面を含めて、推進していくことが重要である。

今回の固定パスワード認証の拡張を考えた最大の目的は、固定パスワードの改善利用によるリスクの減少である。多くの企業・組織で固定パスワードの利用に代えて、提案した「拡張方式」を利用すれば、組織全体のセキュリティレベルは明らかに向上する。

本稿の提案は、現在一般に利用される固定パスワード認証に若干のコストを追加するのみで、利用者の利便性を高め、しかもパスワードの強度を高めることが目的である。更に、パスワードを忘れる可能性も低下するため、そのために費やされるヘルプデスク等に相当する部門の人件費[16]等が減少し、現在の固定パスワード認証より、費用対効果は相当程度高まると考えている。

ここで次のことを補足してまとめとしたい。すなわち、2.6「固定パスワード認証の拡張」で述べた方法は固定パスワード認証よりは優れてはいるが、この方式が他の認証方式すべてに優先し代替するものではない。 3.2 で述べたように、情報セキュリティ投資予算は、リスクに対応して投資の規模と範囲を決定する。個人認証の適否に関して巨額のリスクを抱える金融機関等の場合、認証に多額の投資が可能であれば、それを支出すべきである。

しかし企業経営上、リスクがあっても、それだけの予算を支出できない場合は、少なくも現在の固定パスワードよりも安全と思われる仕組みとして、「固定パスワード認証の拡張」（「拡張マトリックスパスワード」と表現することもできる）（注3）の導入を推進すべく提案するものである。

（注３）必要に応じ「セキュリティのリアルタイム性」活用などの強化手法を含む

[15] 80 年代中頃に、ダイアルアップ回線で Electronic Banking を行っていたが、ログイン時に、ID、パスワード以外に FD（フロッピーディスク）をセットし、ログインごとに FD が更新されるため、FD を複製しても、次回のログイン時には、いずれか一方の FD は利用できない仕組みになっていた

[16] 年間 1,000 人の利用者の場合、ヘルプデスクコストは、95,000 ドルになるとの試算もある
http://www.rsasecurity.com/japan/content_library/Password_Really_Free-J.pdf

参考文献

[1] Computer Security Institute, “CSI/FBI Computer Crime and Security Survey” http://www.gocsi.com/

[2] 内田勝也, 「第２回情報セキュリティ調査」なお、第１回目の調査は、内田勝也, 「情報セキュリティ調査からみた日米セキュリティ比較」、日本セキュリティ・マネジメント学会全国大会 分科会報告、2004, http://www2.gol.com/users/uchidak/research/index.html

[3] D. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security”, Proceedings of the USENIX Security Workshop, Summer 1990

[4] NIST, “Picture Password: A Visual Login Technique for Mobile Devices” http://csrc.nist.gov/publications/nistir/nistir-7030.pdf

[5] 鹿島一紀,“画像の位置情報による本人認証方式の研究開発　画像パスワード GATESCENE（ゲートシーン）”, 情報処理学会、コンピュータセキュリティ, Vol.2000 No.68, pp121-127, 2000 年 7 月

[6] マイクロソフト「ステップバイステップ ガイド : 強力なパスワード ポリシーの強制」 http://www.microsoft.com/japan/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/strngpw.mspx
[7] S. Garfinkel, E.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
[8] Vernon Loeb, “Energy Chief Touts Security Upgrades at Nuclear Labs”, Washington Post, 2000.01.26
[9] Security Awareness Incorporated, “Security Training, Awareness & Reference Tool: Password Construction”, http://www.securityawareness.com/password.htm
[10] 共同通信、「同じ暗証番号で引き出し ゴルフ場でボックス盗撮」、2003 年 9 月 3 日配信記事
[11] 中山靖司／小松尚久,「バイオメトリックスによる個人認証技術の現状と課題」, 金融研究, 日本銀行金融研究所, 2000.04
[12] BBC News 「Malaysia car thieves steal finger」 http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
[13] Anti-Phishing Working Group, “Screen Scraper”, Phishing Activity Trends Report, July 2005, http://antiphishing.org/APWG_Phishing_Activity_Report_Jul_05.pdf
[14] 松本勉／岩下直行, 「インターネットを利用した金融サービスの安全性について」, 金融研究, 日本銀行金融研究所、2002.06

著者略歴

内田 勝也（うちだ・かつや） 2002 年より、中央大学にて、２１世紀ＣＯＥプロジェクト「電子社会の信頼性向上と情報セキュリティ」にて事業推進担当、2003 年より、情報セキュリティ人材育成プロジェクトの推進等. 2004 年４月より、情報セキュリティ大学院大学 助教授. 現在、情報セキュリティマネジメントシステム、有害プログラム、検疫システム、情報法科学（Information Forensics）等の研究・教育に従事。正会員.