

1 はじめに

ネットワークのオープン化により、情報交換における利便性が飛躍的に向上した。それに伴いそのオープン性・ボーダレス性ゆえに漏洩、改ざん等の情報セキュリティ上のリスクへの対応が重要課題となってきた[1]。本文では従来のユーザIDとパスワードの2つの認証情報に、パスワード入力時のキーストロークにより刻まれるリズムを加えた認証システムについて述べる。リズムというのは感覚的な情報であるため、盗用は難しいので全体的にシステムの安全性を高めるのに有効な方法である。本認証システムでは、第1段階としてリズム細分化方式を提案した[2]。これはリズムを10拍に固定している。パスワードの入力間隔値の比率によって細かくリズム化しているため不正チェックの厳密さは高いがタイピング技術が低いユーザは認証されない場合があった。今回はリズム化選択方式を採用し両者の比較検証を行った。

2 本認証システムの方式

本認証システムの全体的な流れを図1に示す。まず、クライアント側にはリズム化プログラムを搭載しておく。ユーザがサーバの管理するデータにアクセスする際に、ユーザ ID・パスワードの入力時にあらかじめ決めておいたリズムを付けて入力する。ユーザがパスワードを1文字入力するごとにリズム化プログラムがそれぞれの入力間隔を計測し、それらを逐次記録していく。これらのユーザ ID、パスワード、パスワード入力時のリズムの3要素をコード化してサーバ側に送り、サーバ側でクライアントから送られてきた内容とリズムデータとの比較を行う。

送られてきたデータと格納されたデータが一致した場合には、正規のユーザであると認証され、ユーザのアクセスは許可される。認証作業の失敗許容回数はサーバの管理者が設定できるようになっている。

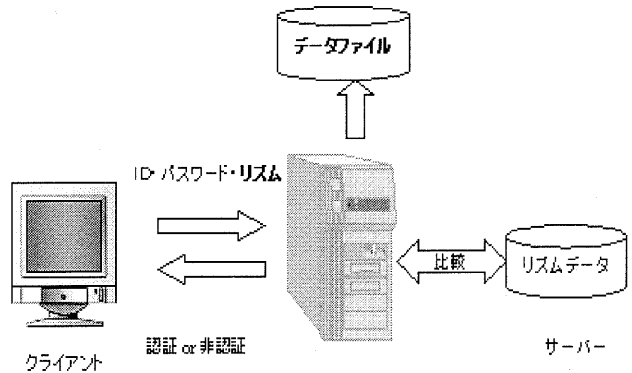


図1 認証システムの全体図

3 リズム化の方法

リズム化にあたっては、リズムを表す数字であるリズム要素を2個と3個からユーザが選べるようにした。まず、リズム要素を2個使用する場合、リズムを“長”と“短”の2つの要素を用いてリズム化する。パスワードを1文字ずつ入力する間隔値を計測し、その間隔値の平均を基準にリズム要素を作成する。このリズム化の場合では各間隔値が間隔値の平均未満であればリズム要素を1、間隔値の平均以上であればリズム要素を2とする。リズム要素を2つ使用する場合は“11212”のように1と2だけで、リズムが作成される。次に、リズム要素を3個使用する場合では、リズムを“長”、“中”、“短”の3つの要素を用いてリズムを作成する。各間隔値が平均値の0.5倍以下であればリズム要素を1にし、2倍以上であればリズム要素を3、それ以外の場合はリズム要素を2とする。この場合は“22312”のように1と2と3でリズムが作成される。

図2にリズム化の例を示す。

パスワード	a	b	c	d	e	f
間隔値	200	270	450	130	390	[ms]
リズム要素2個使用	1	1	2	1	2	
リズム要素3個使用	2	2	3	1	2	

図2 リズム化の例

4 各ソフトウェアの機能と動作

本認証システムは4つのソフトウェアから構成される。

- ・認証ソフトウェア(クライアント側): ID、パスワード、リズムコードを入力する。リズムコードの欄にはユーザが選択したリズム要素数(02, 03)を入力する

- ・認証ソフトウェア(サーバ側): クライアントから送られてきたデータとユーザ登録情報との比較を行う。一致した場合はクライアントに認証コード、一致しない場合は非認証コードを返し再入力を求めるメッセージを表示させる。

- ・ユーザ管理ソフト: このソフトウェアはユーザの情報を管理するため使用する。ID、パスワード、リズムデータを記録したファイルの編集を行う

- ・リズム練習ソフト: ユーザがパスワード入力時のリズムを決定し、正しくリズムが刻めるように練習を行う場合に使用するプログラムである。

5 比較検証

リズム細分化方式とリズム化選択方式のリズム練習の前後での認証率の変化について検証を行った。今回は比較的タイピング技術が低いパソコン歴1年未満の人を対象とした。

それぞれの被験者にはリズム化選択方式、リズム細分化方式の両方を使用してもらった。A1、A2、A3は正規ユーザとして登録者であり、B1、B2、B3は仮の不正利用者である。不正利用者には正規ユーザのIDとパスワードをあらかじめ教えておいた。リズム練習前の結果を表1にリズム練習後の結果を表2に示す。表の中の数字は認証回数/作業回数=認証率を表している。リズム化選択方式、リズム細分化方式共にリズム練習前は認証率が低かった。リズム練習後では、リズム化選択方式では認証率が90%以上

に向上し、リズム細分化方式では認証率は向上したが、60%程度となってしまった。タイピング初心者にはリズム細分化方式よりリズム化選択方式の方が実用的であるという結果になった。不正利用者は1回も認証される事はなく、セキュリティが向上したといえる。

表1 リズム練習前の実験結果

	リズム化 選択方式	リズム化 選択方式	リズム 細分化方式
リズム要素	2個	3個	10個
正規利用者			
A1	24/50 48%	20/50 40%	11/50 22%
A2	19/50 38%	21/50 42%	9/50 18%
A3	18/50 36%	14/50 28%	13/50 26%
不正利用者			
B1	0/50 0%	0/50 0%	0/50 0%
B2	0/50 0%	0/50 0%	0/50 0%
B3	0/50 0%	0/50 0%	0/50 0%

表2 リズム練習後の実験結果

	リズム化 選択方式	リズム化 選択方式	リズム 細分化方式
リズム要素	2個	3個	10個
正規利用者			
A1	47/50 94%	46/50 92%	35/50 70%
A2	48/50 96%	49/50 98%	29/50 58%
A3	46/50 92%	44/50 88%	33/50 66%
不正利用者			
B1	0/50 0%	0/50 0%	0/50 0%
B2	0/50 0%	0/50 0%	0/50 0%
B3	0/50 0%	0/50 0%	0/50 0%

6 まとめ

本システムでは幅広いユーザの使用を目的としている。今後、ユーザに実際に使用してもらい、問題点をあげていき、インターフェース等、様々な点の改良を施していく。

7 参考文献

[1] 情報処理 vol.41 通巻 419号

“不正アクセスの実体と対策” P64~P65

[2] 富永、小泉: “パスワード入力にリズムを取り入れた個人認証方式の開発” マルチメディア、分散、協調とモバイルシンポジウム論文集P 351