インターネット上における文字認証システムの問題点と具体的な解決方法の提案

木下研究室　　蓑和　玲 (200803026)

1　まえがき

近年、インターネットの普及により、インターネット上でのサービスが多くみられる。その中でも、ユーザーの登録を行い、ユーザーごとに情報を管理し、サービスの質の向上をしているものについては、使用者がその本人であるという証明のために認証が必要であり、その認証に、最も多く使われているのが、パスワードを用いた文字認証である。

しかし、その反面、アカウントハック（パスワードを何らかの方法で盗む、あるいは解析などをして損害を与える、もしくは利益を得る行為）などが大きな問題となっており、これについては、ユーザーのセキュリティに対しての関心、危機感が不十分であることが原因となっていると考えられる。

今回の研究では、ユーザーのセキュリティに対する考え方がどのようなものかを確認したうえで、それに対する具体的な対策方法を提案することを目的とする。

2　パスワードについての調査など

2.1　良いパスワードとは

パスワードの良し悪しの基準として、以下のものが挙げられる

セキュリティ面から見た要素
- ・パスワードの長さ
- ・非連想
- ・文字種類の多様性
- ・他のアカウントとの非重複

ユーザーから見た要素
- ・覚えやすさ
- ・入力のしやすさ

この他に、状況によって、パスワードを変更することが求められる。

セキュリティ面から見た要素と、ユーザーから見た要素がトレードオフの関係になっていることは明白であり、この相違を埋めるシステムを考える必要があるといえる。

2.2　パスワードに関しての意識について

現状、パスワードに対しての危機意識は一般的に低いものと考えられる。米 SplashDate 社が発表した 2011 年の「最悪なパスワード」では、1 位に Password、2 位に 123456、などといった結果が示されている。また、日本の衆議院ではサイバー攻撃を受けたにもかかわらず、パスワードの変更を行った議員は半数に満たないなど、意識の低さが浮き彫りとなっている。

3　具体的な提案方法

今回提案する方法は、パスワードの入力を変換して、出力させる方法である。変換を行うため、変換前の入力、すなわちユーザーが入力するワードにセキュリティを求める必要はなく、機械的に変換を行うため、実効パスワードは無機的な文字列であるため、セキュリティを確保することが可能であるため、セキュリティとユーザーの需要を両立することが可能である。

変換に用いるアルゴリズムは、アスキーコードを用いるなどいくつか考えられるが、固有性、利便性を考慮し、図 1 に示すアルゴリズムを提案する。

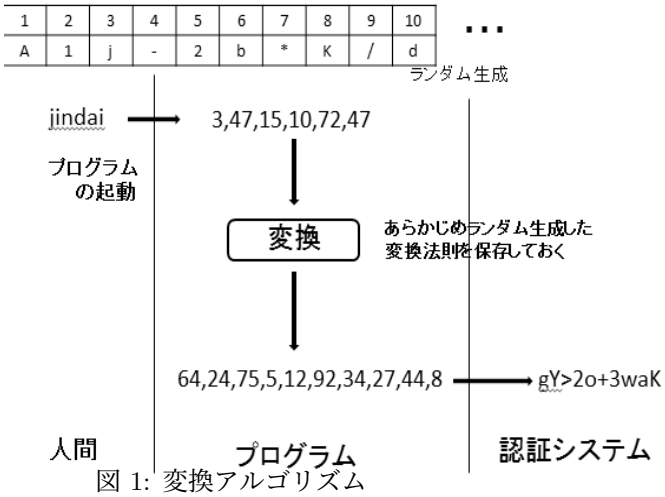

図 1: 変換アルゴリズム

このアルゴリズムでは、文字列と数字を一意に対応させた表を用いて、入力した文字列を数字に変換して演算する。その結果を文字列に直すことで、無機的な長いパスワードに変換する。対応表は初回起動時に作成させるため、ユーザーごとに異なり、固有性が確保できる。また、演算の内容もそれぞれ別途に生成することで、異なるアカウントやパスワードの変更といったニーズにも対応することが可能である。さらに演算法則の指定に条件を付け加えれば、文字数の指定や、使用できない記号を指定することも可能になるといった利点がある。これらは前述したアスキーコードによる変換では実現できないため、このアルゴリズムに有効性があると考えられる。