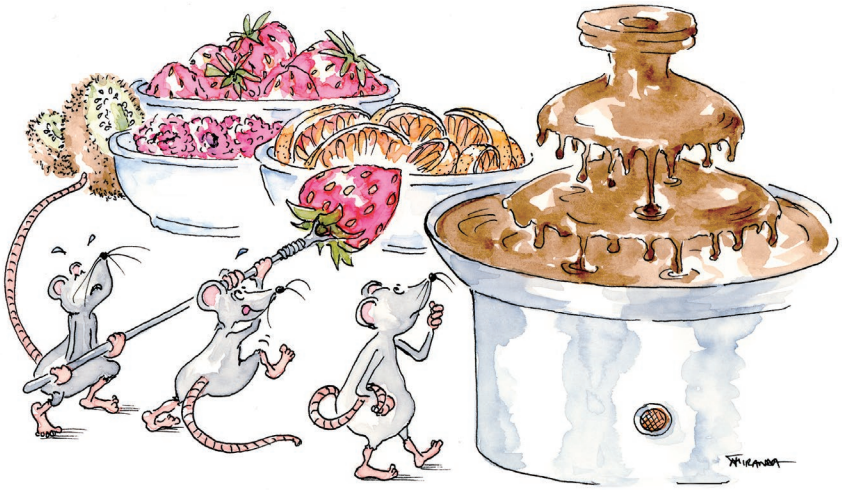
数理の窓

究極のパスワードのパラドックス



なにかのサービスにユーザー登録するときに、IDとパスワードの設定が求められる。キーボードの並びや語呂など規則性のある“平凡”なパスワードでは強度不足で拒否されてしまう。パスワードは年々長くなり、それらをすべて管理するのも大変である。それでは、強いパスワードが気軽に作れて、覚えておくにはどうしたらよいか。

有名な数を使う方法がある。「サービス名」が円周率の何桁にあるかをパスワードにするのだ。例えば、サービス「けんこう」はポケベル暗号方式で数字に直すと「24032513」になる。この数字を円周率検索サイトにかけると、

「円周率の小数点2,617,072桁目」から始まることが分かる。これをパスワードに設定するか、必要なら文字列に直せばよい。

では、この方法で“どんな長いサービス名の文字列”にも対応できるだろうか？この問いは、円周率には、宇宙のあらゆる有限数列が含まれるかと同じである。10桁程度ならば簡単に確認できる。

数学者ボレルは、無限小数列の中に0から9の各数字が一様に分布して、さらに、どんな桁の数字パターン列も出現頻度に偏りない数を正規数[1]と名付けた。ランダムな数列が無限に続くことは、すべての有限数列が存在することと同値である。よって正規数には源氏物語全文も含まれる。ただし、円周率が正規数であることは、信じられてはいるものの証明されていないという難点がある。

このように円周率（または正規数）を使ったパスワードは覚えやすいが、ここで公開してしまった以上、再現可能となり、強いとはいえない。さらに強いパスワードはできるのだろうか？これは“完全にランダム”な数列を作ることだが、かなり難しい。仮に、これこれの性質がランダムだと定義した瞬間、その定義を使ってランダムな数列が作れてしまう。よって、なにかの関数やプログラムでは計算も圧縮もできず、それ自体を並べる以外には表せないことが究極のランダム[2]の定義である。

今、仮に頭の中でランダムなパスワードを思いついたとする。しかし、それが記憶・再現できることは、ニューロ計算もできることを意味するため、究極ではない。より進んで、“頭にも記憶できない”究極のパスワードを得たとする。それをサービスで再び利用したいとすると、どこか物理的に書いておく以外に保存手段はない。今度は、パスワードは強力だが、セキュリティ上の問題が生じる。究極にランダムなパスワードのパラドックスといえよう。。

（外園 康智）

1）小数点以下に素数を順に並べたコープランド-エルデシュ定数は10進数表示の正規数であることが証明されている。
2）チャイティンのオメガと呼ばれ、正規数より強いランダム性を持つ数がある。