北海道師範塾「教師の道」　塾頭通信

第345号　平成24年7月6日

解けないはずを解く

情報通信研究機構と九州大学等による研究チームは、解読に数十万年かかるとみられていた「ペアリング暗号」を、コンピューター２１台を使って１４８日で解くことに成功したそうです（６月１９日付読売新聞）。

暗号といえば、身近なところではクレジットカードなどの暗証番号や、ネットで買い物をする際パスワード等がありますが、これらで使用される記号はせいぜい４桁から８桁位のものです。しかし、今回のペアリング暗号は２７８桁ということで、どんな暗号なのか皆目見当もつきませんが、解くのはほぼ不可能というのは理解できます。

そもそも、現代の暗号の世界は、分からないことだらけで、まず、ペアリング暗号なるものが分かりません。色々調べてみましたが、資料を見れば見る程、私の能力では理解不能だという事を自覚しました。何はともあれ、極めて複雑な数学の計算問題を解くようなものだと思うしかありません。

さて、暗号というものは、通信の内容を第三者に知られないように、特別の知識がなければ解読できないものに置き換えて表記するものですが、古くは、紀元前19世紀ごろの古代エジプトの時代に、既に暗号文が使用されていたようです。

時代は下って、１８９５年にモールス信号による無線通信が出現すると、文書による通信と違って、電波による通信は味方だけでなく敵も傍受することが可能となりますので、暗号は無線通信を行う場合の必需品になっていきます。

暗号といえば、かつて太平洋戦争中、日本軍の暗号はアメリカ軍に筒抜けだったといわれておりますが、日本は軍隊同士の戦いだけでなく情報戦争でもアメリカに敗北していたといえるでしょう。

更に、第二次世界大戦後はコンピューターの時代に入り、文章の暗号化も暗号の解読も飛躍的に高度化し発展することになります。

今や、日常生活においてクレジットカードを使ったネットショッピングは当たり前の世の中になっていますが、ここでも、重要な情報が漏れないよう暗号が使用されています。それでも、コンピューターの進歩に伴い暗号の解読技術

も向上しており、情報漏れの事故や事件が後を絶ちません。

　こうした中、企業においては、情報セキュリティや個人情報保護のため、より安全の高い暗号が求められており、こうした中で開発されたのが前述のペアリング暗号といわれるものです。この暗号は、解読はほぼ不可能といわれて来ましたが、研究チームはペアリング暗号を解読する新しい「攻撃法」を開発したという訳です。

　研究チームによると、ペアリング暗号は「思ったより脆弱であることが実証された。より大きい桁数の暗号を使う必要がある（６月１９日付読売新聞）」としていますが、これではイタチゴッコで際限のないゲームをしているようなものです。

　「人間が考え出したものである以上、人間に解けないはずはない。」ということでしょうか。げに恐ろしきは、人間の知恵ですね。（塾頭　吉田　洋一）