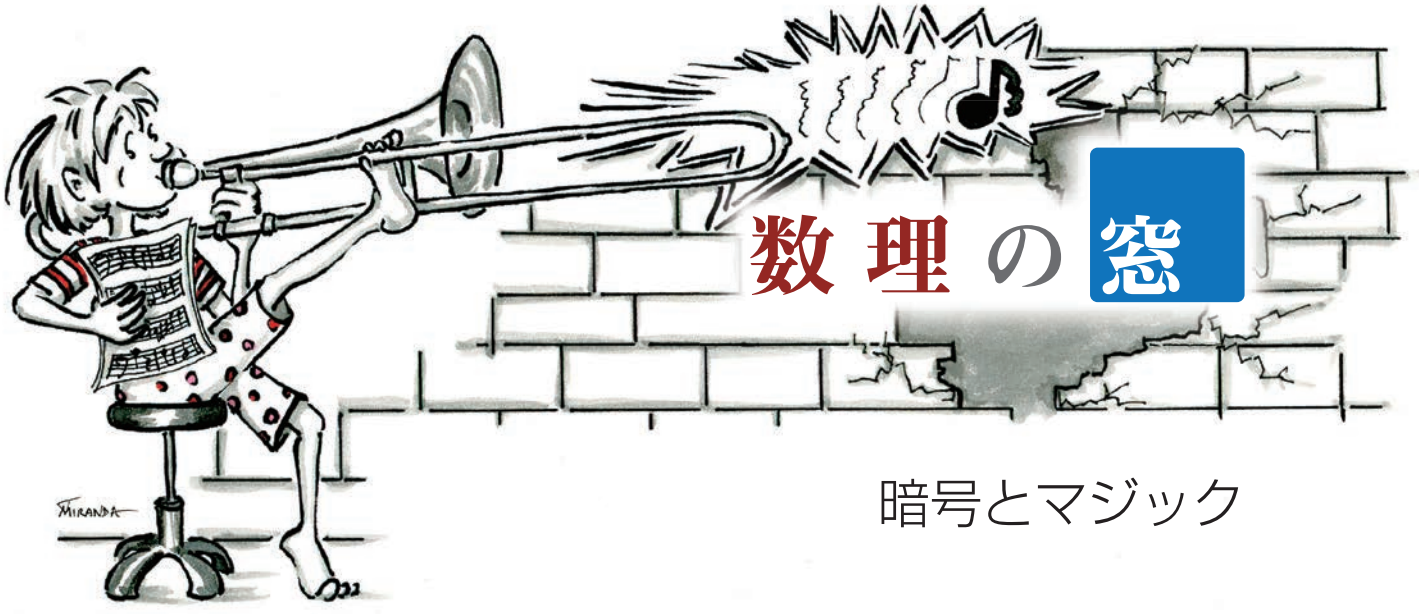


# 数理の窓

## 暗号とマジック

マジシャンが52枚のトランプから5枚を観客に選ばせる。勿論、これらは見ない。助手は選ばれた5枚を“うまくシャッフル”しながら、♠⑨、♥⑦、◆④、♣⑤、「？」と並べたとしよう。最後の1枚だけ裏向きだ。マジシャンは手を触れることなく、その1枚を当てる。

これはカードマジックの古典で、助手からの4枚のメッセージが鍵で、種明かししよう。

まず5枚中で、♠・♥・◆・♣の少なくとも1つの組でペアが生まれる。このペアを左端と右端におく。これで組は「♠」と伝わる。次は数字を当てたい。①から⑬のうち⑨を除いた12の可能性があるが、ペアの置き方の工夫で6通りに絞れる。例えば②と⑨の距離は7だが、⑨と②の距離は6である（⑬の次が①と循環している）。助手は常に距離が短くなるように、②<⑨でなく、⑨<②と置く。これで距離は必ず6以下となる。

最後に中央3枚のカードで、この距離を示せばよい。3枚がどう選ばれるか分からないため、簡単に使えるのは“大きさ”だ。♠>♥>◆>♣の順とすれば、大小関係が入り、大きさによる3枚の並べ方は次の6通りだ。

（123）（132）（213）（231）（312）（321）

ここで順に（123）が距離1を（321）は距離6を表すと決めておく。中央3枚＝♥⑦◆④♣⑤は（321）を意味し、距離は6だ。よって、♠⑨に6を足して、♠の②が答えとなる。

以上のトリックは鍵（＝変換ルール）を共有する二人の間で、一方が暗号化したデータを、もう一方が復号できれば成立する。例えばカードを使わず、助手の帽子のかぶり方等をメッセージに使ってもよい。52枚の中から1枚指定するのに、5.7ビット[1)]の情報の暗号化が必要だ。5枚全部を当てようとすると、情報量が多くなり、別のトリックが必要だ。

暗号メッセージを使ったマジックの難点は、鍵の設定や共有が面倒なことと、何度もやるとネタばれしてしまうことだ。暗号の歴史上も、鍵の配布と秘匿が一番の課題であった。暗号化も復号も共通の鍵を使う共通鍵暗号方式の弱点ともいえる。これを乗り越えるため、毎回、鍵を変える工夫や、暗号鍵と復号鍵を使い分ける“公開鍵暗号方式”が発明され、主流となっている。もしも、この方式をマジックに取り入れられれば、高度化も可能だろう。

暗号の本質は、秩序ある情報を、鍵によって無秩序なデータに変換し、隠すこと。そして鍵を“解く”ものだけが、元に素早く戻せることだ。世界は一見すると無秩序なデータの寄せ集めに見える。だが、マジシャンが変換した後の姿なのかも知れない。我々は復号鍵を手に入れられるだろうか？　（外園 康智）

1）情報量は$-\log_2(1/52)$で計算される。



野村総合研究所　金融イノベーション研究部 