分かると快感！

Z会ナビ

▶算数　理科　社会

お題

公開かぎと秘密かぎ

イラスト・瑞木匠

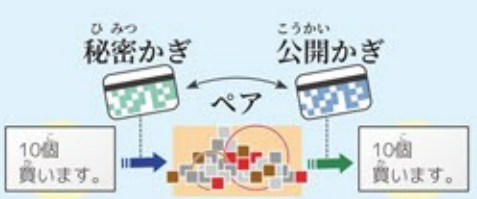
今回は、はんこの代わりに使うことができる「秘密かぎ」と「公開かぎ」の仕組みの話をしましょう。

秘密かぎを使うと、書類を人間の読めないデータ（暗文といいます）に変換することができます。しかも、もとの書類が１文字でも異なっていたら、できる暗文は予想もつかないほど異なったものになります。

また、同じ書類であっても、別の人の秘密かぎでは、これまた予想もつかないまったく別の暗文ができるのです。

公開かぎは、秘密かぎとセットで作るもう一つのかぎです。このかぎを使うと、秘密かぎで変換してできた暗文をもとの書類に戻すことができます。

ただし、暗文をちゃんとした書類に戻せるのは、暗文を作った秘密かぎとセットになっていた公開かぎだけです。



他のかぎで無理やり戻そうとすると、人間の読めないデータになります。

では問題です。ある店に商品を注文するとき、Ａさんという客が注文書を提出します。この注文書を、書類のものではなく、客が自分の秘密かぎで変換して作った暗文を提出するというルールにしてみましょう。

すると、いくつかの不正行為や事故を防ぐことができるのですが、それは次の①から④のうちどれでしょうか？

ただし、秘密かぎはそれを作ったＡさん本人だけが使えるものとし、一方、秘密かぎとセットになっている公開かぎは、誰にでも手に入るとします。

①注文書の送り先を間違えたとき、他人に注文内容を知られる。

②店が、Ａさんから届いた注文書に書き足して、内容を変えてしまう。

③知り合いが、勝手にＡさんの名前で注文書を作り、注文してしまう。

④Ａさんが、本当は注文したのに、「注文しなかった」とうそをつく。

秘密かぎと公開かぎを使って書類をやり取りすることについてのお話です。

今回紹介した方式のポイントは、暗文を作ることは本人しかできないが、もとに戻すのは誰でもできるという点です。はんこも、印の押された書類を作れるのは本人だけですから、その点は同じですね。①～④を順に見てみましょう。

「かぎを使えるのは誰？」

①は誤りです。間違って受け取った人は、Ａさんの公開かぎを使えば、もとの注文書を読むことができます。今回のやり取りの方法には、書類の内容を秘密にする機能はありません。

②は正解です。店では、書き足した注文書を、Ａさんの秘密かぎで暗文にすることができません。そのため、Ａさんが「私が提出したという暗文を見せてみろ」と言えば、本物の暗文を出すしかありません。それをＡさんの公開かぎで戻せば、正しい注文書が取り出せます。

③はどうでしょうか。知人は、にせの注文書を作っても、それを暗文にすることができません。知人が自分自身の秘密かぎを使って暗文を作ることならもちろんできますが、その暗文はＡさんの公開かぎではまともな書類に戻らないので、すぐに、にせものだとばれるわけです。

④も重要です。Ａさんがシラを切っても、店にはＡさんから受け取った暗文があり、Ａさんの公開かぎを使うと、もとの注文書が出てきます。Ａさんの公開かぎで戻せることが、Ａさんの秘密かぎで作った暗文である証拠です。

正解は②③④の三つです。　（Ｚ会・宮坂聡）

今回の教訓

公開かぎとセットになった秘密かぎを使うと、はんこの代わりになります。

宮坂聡さん　2006年にＺ会入社。理数系やプログラミングの教材編集に携わり、現在は中学生・高校生向けの数学を担当。長野県諏訪市生まれ。