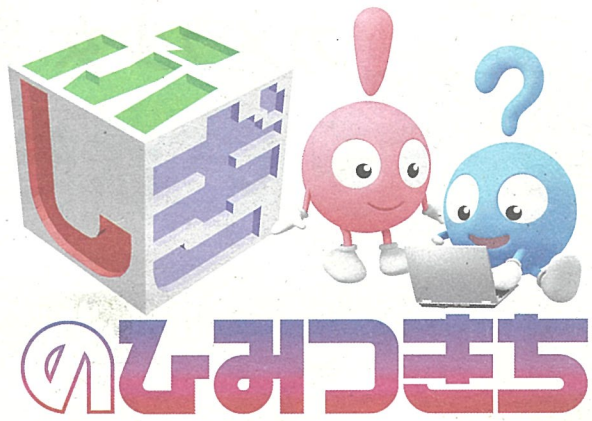
今回のテーマ

データをかく したまま計算



No.074

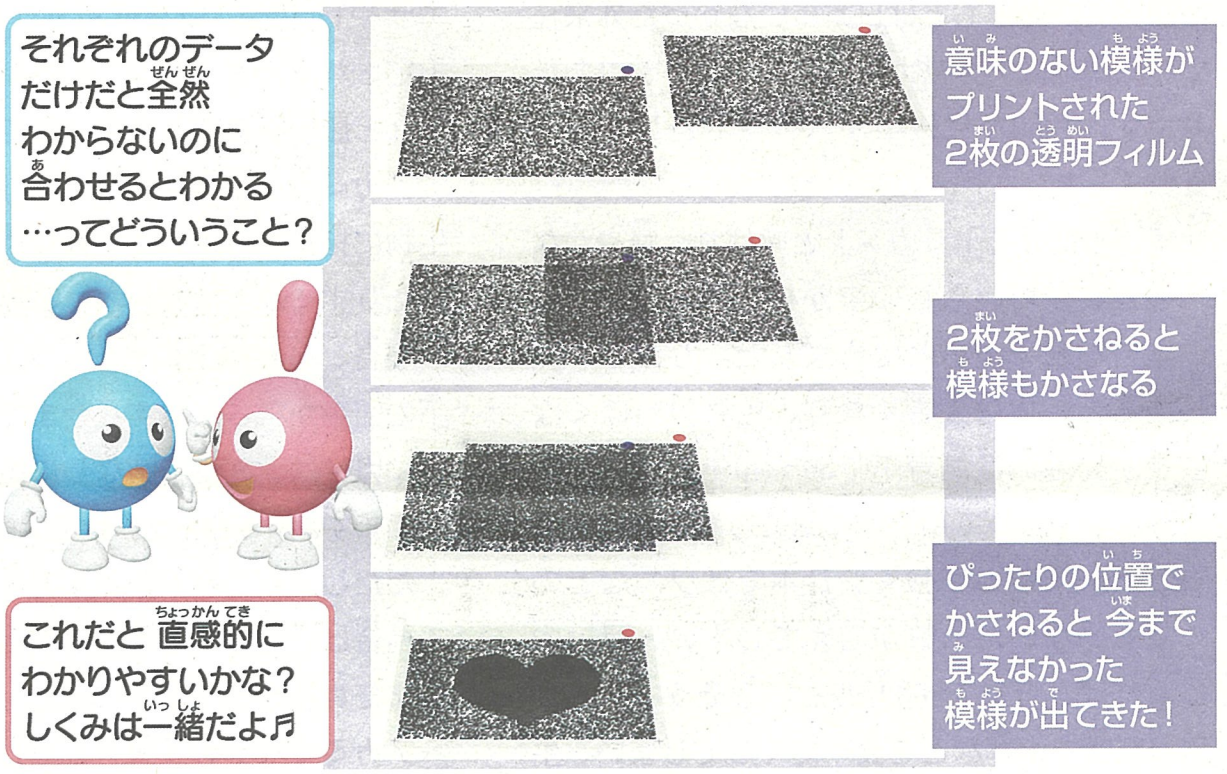
知られたくない情報を守りながら、そこから導き出される答えを得るにはどうしたらよいでしょうか？

コンピューターの発達によって、今まではわからなかったことも調べられるようになりました。例えば、私たちはからだの遺伝子を調べることで、どんな病気にかかりやすいのかを知ることができます。遺伝子の情報を扱うには、とても多くの計算や処理が必要です。コンピューター無しでは、かかりやすい病気を判断することはできません。でも、あなたの遺伝子の情報を他の人に渡してしまうと、あなたがひみつにしたい病気のことまで知られてしまうかもしれません。

◇情報をバラバラにして

そういったひみつを守るために、いま「ひみつ計算」の実用化が進められています。ひみつ計算は、何の情報かをかくしたまま、コンピューターで答えを出す技術です。

代表的なひみつ計算では、コンピューターに処理させるひみつ情報を他の人がわからないようバラバラにして、この状態のまま別々に計算します。最後にそれぞれの結果を合わせて、最終的な答えを出します。



◇計算結果をくっつける

でも、たとえバラバラにしても、その情報がもともと誰のどんなひみつなのか、他の人にわかってしまうのではないかと心配かもしれません。そこで重要になるのがバラバラにする方法です。そしてさらに、バラバラのまま計算を進め、その計算結果を、またくっつけられるようにすることにこそ工夫が必要になるんです。

元の情報がわからないようバラバラにする技術の例を見てみましょう。ひみつにしたい情報がハートの絵だとします。ひみつ計算の技術を使うとハートを全く意味のない２枚の模様にすることができます。この２枚の模様をかさねると、元どおりのハートにすることができます。二つにわけられた状態では、誰も元の情報はわかりませんが、２枚を合わせることで元の情報をとりだせます。

大切な情報を安全に扱うためにも、情報技術の進化はますます重要になるでしょう。

今日の先生

花岡悟一郎さん

「情報をかくすだけでなく、かくしたままでいろいろなことを調べられる『暗号』を作っています」

産業技術総合研究所（産総研）サイバーフィジカルセキュリティ研究センター。専門は暗号技術。出身小学校は東京都中野区立武蔵台小。

さんそうけんって？

日本で最大級の公的研究機関なんだ。茨城県つくば市など、全国12か所の研究拠点があって、日本の産業や社会に役立つ技術について研究を進めているよ。

キッズむけウェブページはこちら ⟶
（さんそうけんサイエンスタウン）