

漫画作品や歴史からひもとく暗号のしくみ

ご購入はこちら

安田 翔也

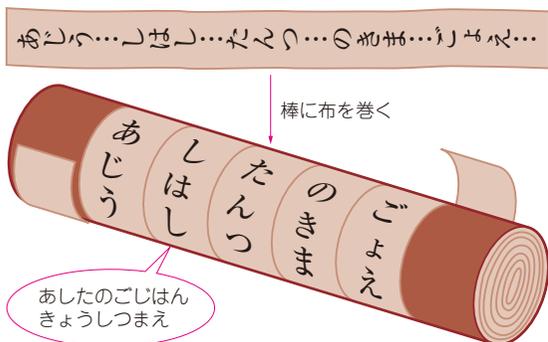


図1 スキュタレー暗号
木に文字がかかれた布をまくことでメッセージを読むことができる

本稿では、古代のシーザー暗号から、ヴィジユネル暗号、エニグマ、そして現代のRSA暗号に至るまで、暗号の歴史と仕組みをたどります。時代とともに、暗号は単なる文字の置き換えから、数学的な困難さを武器にするものへと進化してきました。

難しい数学的な理論には深入りせず、暗号のアイデアや、なぜそれが安全だと考えられてきたのか、逆に、どんな弱点が見つかり、どのように克服されてきたのかを、ストーリーとして楽しみながら学んでいきます。

また、Pythonコードを用いて、実際に暗号化と復号の動きを体験できるようにしています。自分の手で動かしてみることで、仕組みの理解がより確かなものになるでしょう。

漫画に出てくる暗号タイプのいろいろ

私たちは普段の生活の中で、暗号の存在を意識することはほとんどありません。なぜなら、暗号はシステムに組み込まれ、目立たない形で機能しているからです。しかし、探偵やスパイを描いた漫画やアニメでは、暗号がストーリーを動かす場面をしばしば目にします。ここでは漫画を例に代表的な暗号タイプを示します。

- 文字の順番を並び替えて暗号化…転置式暗号
『名探偵コナン』(青山剛昌, 小学館)に登場する「ス

七	六	五	四	三	二	一
あ	あ	や	ら	よ	ち	い
ひ	さ	ま	む	た	り	ろ
も	き	け	う	れ	ぬ	は
せ	ゆ	ふ	る	そ	る	に
す	め	こ	の	つ	を	ほ
ん	み	え	お	ね	わ	へ
	し	て	く	な	か	と
						七

図2
上杉暗号の変換表

「スクユタレー暗号」を見てみます(図1)。送り手は、木の棒に細長い布を螺旋状に巻き付け、布を横断する方向に文章を書きます。受け手は同じ太さの棒に布を巻き直すことで、正しい文章を読むことができます。図1の例では、「あしたのごじはんきょうしつまえ」と読むことができます。このように、文字の順番を並び替えるタイプの暗号は転置式暗号と呼ばれます(1)。

● 余計な文字を混ぜて暗号化…分置式暗号

『SPY×FAMILY』(遠藤達哉, 集英社)に登場する「たぬき暗号」を紹介します。たぬき暗号では、暗号文から「た」の文字を抜くことで復号ができます。例えば、「みたみたかたたき」は「みみかき」になります。他にも、「けむし暗号(けを無視)」や「こけし暗号(こを消す)」など、バリエーションも豊富です。このように、余計な文字を挿入して隠すタイプの暗号は分置式暗号と呼ばれます。

● あらかじめ決めておいた変換表で置き換え…換字式暗号

『Dr. STONE』(原作: 稲垣理一郎, 作画: Boichi, 集英社)では「上杉暗号」が活躍します。例えば「三六四二一」という暗号文が送られてきたら、2文字ずつペアにして変換表(図2)に照らし合わせることで「ねむい」と復号できます。上杉暗号は、文字を別の文字に置き換える換字式暗号の代表例と言えるでしょう。