「カオス」を使って、見破られにくい暗号技術を開発する

情報学部 情報学科
吉岡 大三郎 准教授

暗号はセキュリティの基盤技術

インターネットでは、非公開にしたい機密情報を安全かつ確実にやりとりする必要があります。そんなときに利用されるのが、セキュリティ技術です。その中心に暗号があります。現在の暗号は情報を秘密にするだけでなく、その情報が改ざんされていないか確認し、通信相手が本人であることを保証する認証においても重要な役割を担っています。

見破られにくい暗号にするために「カオス」を利用

暗号は、もちろん第三者に見破られないことが大切ですが、複雑すぎると計算に時間がかかり、利用しにくくなります。そこで、手続きが簡単で見破られにくい暗号技術が重要になります。そのような暗号を設計するためのアプローチとして、「カオス」を利用する方法があります。

数式には、何度も計算を繰り返すうちに、しだいに結果の予測が難しくなるものがあります。気象予測を考えてみてください。時間的に近い予報は当たりやすいですが、遠い先になると当たりにくくなります。あとになるほど、誤差が増大して複雑な振る舞いとなり、予測が難しくなるのです。これと同じように、計算規則に従いつつ複雑で不規則な振る舞いが得られることを「カオス」と呼んでいます。式自体は簡単なので、カオスが生じる式を使えば、計算コストを抑えてセキュリティを高くできるのです。

小型センサーは複雑な計算はできない

ユビキタスセンサネットワークといって、身の回りの多くのところに埋め込まれた小型センサーを主とした情報のやりとりが、今後ますます増えていくと考えられます。そこで使用されるのは、小型化されたセンサーなので、暗号化するにしても複雑な計算はできません。また、すばやく反応させる必要があるため、手続きを簡単にすることは避けて通れないのです。そのためにも、手続きは複雑ではなく、しかしセキュリティの高い暗号技術が求められるのです。

株式会社フロムページ 夢ナビ編集部監修