

# 情報セキュリティは“カオス”で安全に

## 小型デバイス向けの暗号の開発

インターネットでの盗聴、データの改ざん、相手の認証によるなりすましなどの犯罪には、どのようにして対策をたてるのかご存知ですか？ 日々進化している中、このような犯罪に対策として応用されるのが、暗号設計です。ID パスワードなどを鍵とすると鍵を知らない第三者にとって、解読が困難であることが安全対策として求められます。暗号設計は、認証情報、個人情報、注文情報、カード番号などを通信の秘匿性や認証を実現するセキュリティの基板技術です。そこで重要なことは、「いかに実装効率を上げ、解読出来ない難しさを持たせることができるか？」が課題となっています。私の研究室では、簡単な方程式に基づく不規則で複雑な現象である“カオス”を応用する暗号の研究を行っています。世界中で通信端末の小型化のニーズが高まっておりますので、効率よく実装できる軽量暗号を実現し、情報の安全に役に立ちたいと日々研究しています。

情報学部 情報学科 **吉岡 大三郎** 教授



**崇城大学**  
SOJO UNIVERSITY

薬学部	生物生命学部	工学部			情報学部	芸術学部			
薬学科	応用微生物工学科	応用生命科学科	機械工学科	ナノサイエンス学科	建築学科	宇宙航空システム工学科	情報学科	美術学科	デザイン学科

〒860-0082

熊本市西区池田 4-22-1

問い合わせ(入試課直通)

TEL:096-326-6810

そうじょう大学

