

# 新暗号システム開発

## 情報セキュリティの世界最先端

開発したICチップを入れた試作品(右手)を紹介する高木教授。左手はUSBメモリー



### 未来大・高木剛教授ら

公立ほこだて未来大学情報アーテ  
クチャ学科の高木剛教授(38)と富  
士通の子会社FDK(東京)などは  
15日、情報セキュリティ(安全対  
策)の世界最先端技術となるICチ  
ップの試作品開発に成功した、と発  
表した。次世代の暗号技術として注  
目を浴びている「ペアリング暗号」  
を使用した新たなシステムで、IC  
チップの計算速度は従来の製品の1

000倍、消費電力も1000分の  
1という。数年以内の実用化を目指  
している。

インターネットや携帯電話を使っ  
た決済、電子メールなどで使用する  
パスワード(暗号)の流出や第三者  
による攻撃などで、情報ネットワー  
クのセキュリティ対策が求められ  
ている。ペアリング暗号は国際暗号  
学会で認知されており、世界で初め  
て試作品が完成した。

高木教授によると、ペアリング暗  
号のチップは高速性だけでなく安全  
性に優れ、非常に高度な技術がなけ  
れば暗号の解読はできない。応用す  
ることでデジタルの映像や著作物の  
不正コピーの防止、コンテンツの不  
正利用防止などができる。住基カー  
ドなどに入っている国や道、市のデ  
ジタル署名をコンパクトにしたり、  
見られたくない情報にシステムを応  
用した鍵をかけることもできる。

新エネルギー・産業技術総合開発  
機構(NEDO)から3億1800万  
円の研究費を得て、2005-07年  
度の3カ年で開発した。未来大、F  
DKのほか、筑波大と情報セキュリ  
ティ大学院大学による共同研究で、  
高木教授は暗号部分を担当した。

試作品は約3センチ×2センチの大きさ  
で、高木教授は「ICチップはUS  
Bメモリー(小型の記憶媒体)に入  
る程度まで小さくしたい。研究開発  
をしている企業のセキュリティ対  
策など幅広い利用ができる」と話し  
ている。

(高柳 謙)