

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

新暗号システム開発

情報セキュリティの世界最先端

公立ほこだて未来大学情報アーテック学科の高木剛教授(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す。インターネットや携帯電話を使うた決済、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度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、FDK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USB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)