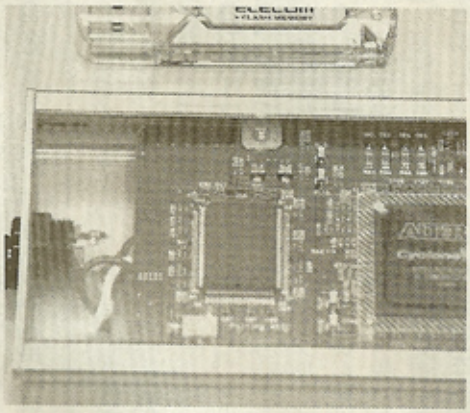
北海道新聞　　2008 年 4 月 16 日

世界初、専用ＩＣ開発

次世代暗号技術実用化へ



はこだて未来大などの研究チームが開発した世界初の「ペアリング暗号」専用ＩＣ（下側基盤中央のチップ）

【函館】公立はこだて未来大など国内三大学と民間企業の共同研究チームは十五日、インターネットなどの情報通信でデータ漏えいを防ぐ次世代暗号技術「ペアリング」の実用化を可能にする専用集積回路（ＩＣ）を、世界で初めて開発したと発表した。処理速度が従来のコンピューターの約千倍となり、低コストで一段と安全な情報管理が実現できるとしている。

低コスト、処理速度千倍

はこだて未来大

はこだて未来大のほか、筑波大、情報セキュリティ大学院大（横浜）、富士通グループの電子部品メーカーＦＤＫ（東京）が共同開発した。独立行政法人、新エネルギー・産業技術総合開発機構（ＮＥＤＯ）から総額三億一千八百万円の助成を受け、二〇〇五年度から研究を始めた。

ペアリングは、情報通信で第三者に情報が漏れるのを防ぐために広く用いられている公開鍵暗号の処理手順（アルゴリズム）の一つ。従来型に比べ、通信コストを抑え安全性を高められるものの、公開鍵の作成などの計算量が大きく、時間を要することが難点だった。

試作された専用ＩＣは縦三ミリ、横二ミリ程度で、ペアリング一回の処理速度は百万分の四十七秒と、従来のコンピューターを使った場合の約千倍。今後、五年程度かけて一層の小型化を進め、携帯電話や家電製品などへの内蔵を目指す。

アルゴリズム改良を担当した高木剛はこだて未来大教授は「専用ＩＣはデジタル放送のコンテンツ不正コピー防止などにも広く利用できる」と話す。