

# カード情報盗み見防止

## 日立、暗号を乱数化

日立製作所は、店舗のカード読み取り装置から漏れ出る電磁波などを手がかりに顧客の情報を入手・解読することを防ぐため、ICカードの個人情報を読み取らせないようにする新技術を開発した。安全性が高まり、情報盗むのが不可能になる。独ダラムシユタツト工科大学との共同開発。世界標準方式として提案し、三年後をめどに実用化する。

ICカードにはRSA暗号という暗号技術が広く利用されている。新技術では、カードを読み取り装置にセットして暗号化された個人情報の内容

を元に戻す際、暗号を一変換した乱数に置き換えたうえで高速計算処理する。カード読み取り装置が稼働する際に生じる電磁波からデータは盗めず、中身を外から解読できない。乱数化に特別な装置は不要で処理時間も従来とほぼ同じという。

ICカードや、ICカード機能を持ち「財布」  
 として使える携帯電話の開発が、カード会社や鉄道会社、携帯電話会社などで始まっている。しかし、読み取り装置の電磁



波などから秘密情報を解析される恐れがあり、研究の間では対策の必要な磁気カードの場合は、読み取り装置に特殊な機器を付けることで情報を直接盗むことが可能だ。