IC タグにおける暗号技術応用機能の開発

１．目的

コンピュータ応用製品の受注生産を行う企業にとってインターネット対応型自社製品の機能を向上させる努力は必要不可欠であり，IC タグは応用の広い注目のデバイスである．しかしながら応用システムの制作には数学的知識と経験に基づいた暗号処理技術が必要になる．

そこで，IC タグにおける暗号機能のアルゴリズムとデータベースの高速演算処理に関する技術について企業課題対応型共同研究を実施した．

２．方法

２－１．応用製品の企画とインターフェイス機能

施設で使用する入退出管理用にICタグを応用した商品が提案された．IC タグの一枚あたりの価格は三百円まで下げることができるが，現在のところ，継続的に使用できる分野へ応用するという結論になった．（その他，書換え可能なラベルを併用して数百回程度の循環利用ができる物流分野等への応用は可能である．）

非接触の無線ICタグがアンテナ圏外に出た場合には、インターネットを利用して予め登録された電子メイルアドレスに通知することができる．

アンテナ周辺を通過する複数のICタグを個々に識別し，その内容を読み取ったり短い情報を書き込んだりするインターフェイスソフトウエアを試作した．（I･Code，ISO15693-3,13.56MHz，図１～４参照）

図１
カード型 IC タグ

図２
防水型として利用できる封入型 IC タグ

図３
カード情報アクセス用インターフェイス

図４
アンテナ USB 接続用デバイスドライバー

２－２．高速演算機能の開発

情報を暗号化すると探索空間が広がり同じ内容の情報もデータサイズが大きくなる．また復号処理計算の処理工程が追加される．そこで，アクセス負荷の大きいデータベースを扱うために必要な高速演算機能を提案し，複数の CPU を用いてジョブを並列処理する方式を採用して試作した．今回は並列処理演算器の製造技術の取得を目的としたので安価な筐体，５個の Intel-CPU とギガビットイーサネットを用いた．

図５
CPU ユニット
(全部で 5 つ)

現在，動作が不安定であり調整を続ける必要はあるが，基本的な機能を有する実験装置が得られた．（図５参照）

３．結果

(1) IC タグをインターネット設備で利用するノウハウが得られた． (2) 暗号の高速演算処理に必要な実験装置が得られた．

企画情報課　岡田雅史　　（有）アイシーランドマツノ