# 業務用サーバにおけるファイル保護機能の開発

## １．目的

平成17年度から事業者等に個人情報の管理責任を課す制度（個人情報保護法）が施行されるようになったが，ウイルスメールやハッキング攻撃は多発しており，必ずしもファイアウォール装置でこれらの攻撃を防ぐことができないでいる。
本研究はこの問題を解決するために必要なサーバの保護機能を開発することを目的とした．

## ２．方法

顧客情報などを記録した情報はインターネットに接続されたサーバに電子ファイルとして格納されている．本研究ではこのサーバのファイル自体を暗号化して保護する方法を採用し，公開鍵方式と可変長のブロック構造の物を提案した．

情報を暗号化すると，探索空間が拡張されてファイルのサイズが元のサイズよりも大きくなって，暗号化や複合化の工程にも数値演算で負荷がかかる．そこで，並列処理方式を採用した高速演算処理装置を試作した．

**図１　1CPU&1000Base-T 格納ユニット**

通常，並列処理型の高速演算処理装置は複数の CPU を搭載した薄型マザーボードケースを縦型ラックに積み上げて作成するが，今回は１個の CPU を搭載したマザーボードと安価な筐体を５組使用した．マザーボード間のデータ通信はギガビットイーサネット回線を使用した．

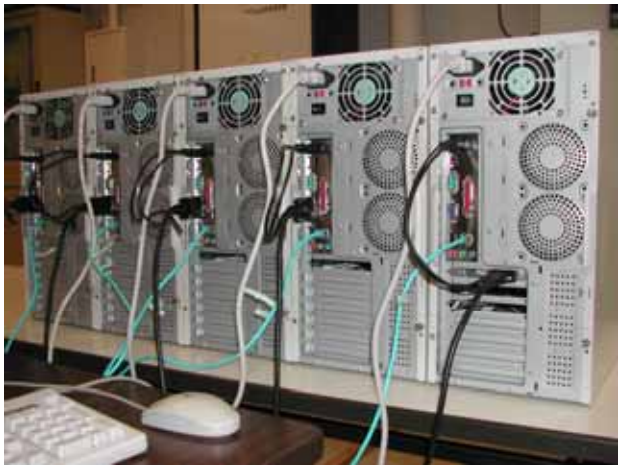

**図２　５個のユニットを連結した並列処理マシン**

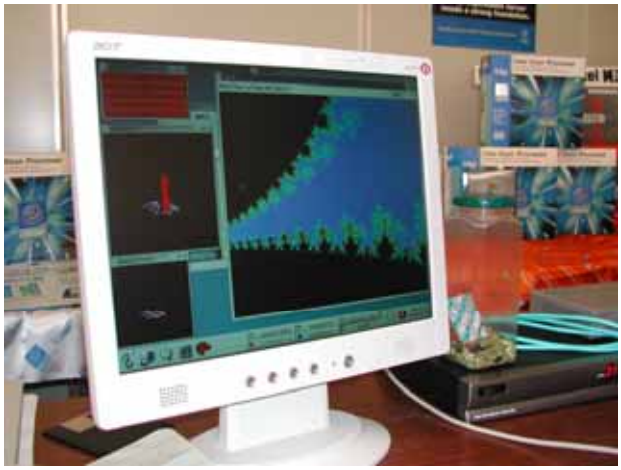

**図３　並列マシンの動作検証作業**

## ３．結果

システム開発環境としてフリーの LinuxOS を採用したため動作が不安定なところがあり，連続運転にはまだ調整が必要であるが以下の成果が得られた．
（１）ファイル保護機能に必要な暗号の高速演算処理に必要な実験装置を得ることができた．
（２）並列処理型高速演算装置を安価に作成するためのノウハウが得られた．

企画情報課　岡田雅史