耐タンパーセキュアボード“TURBOMISTY”

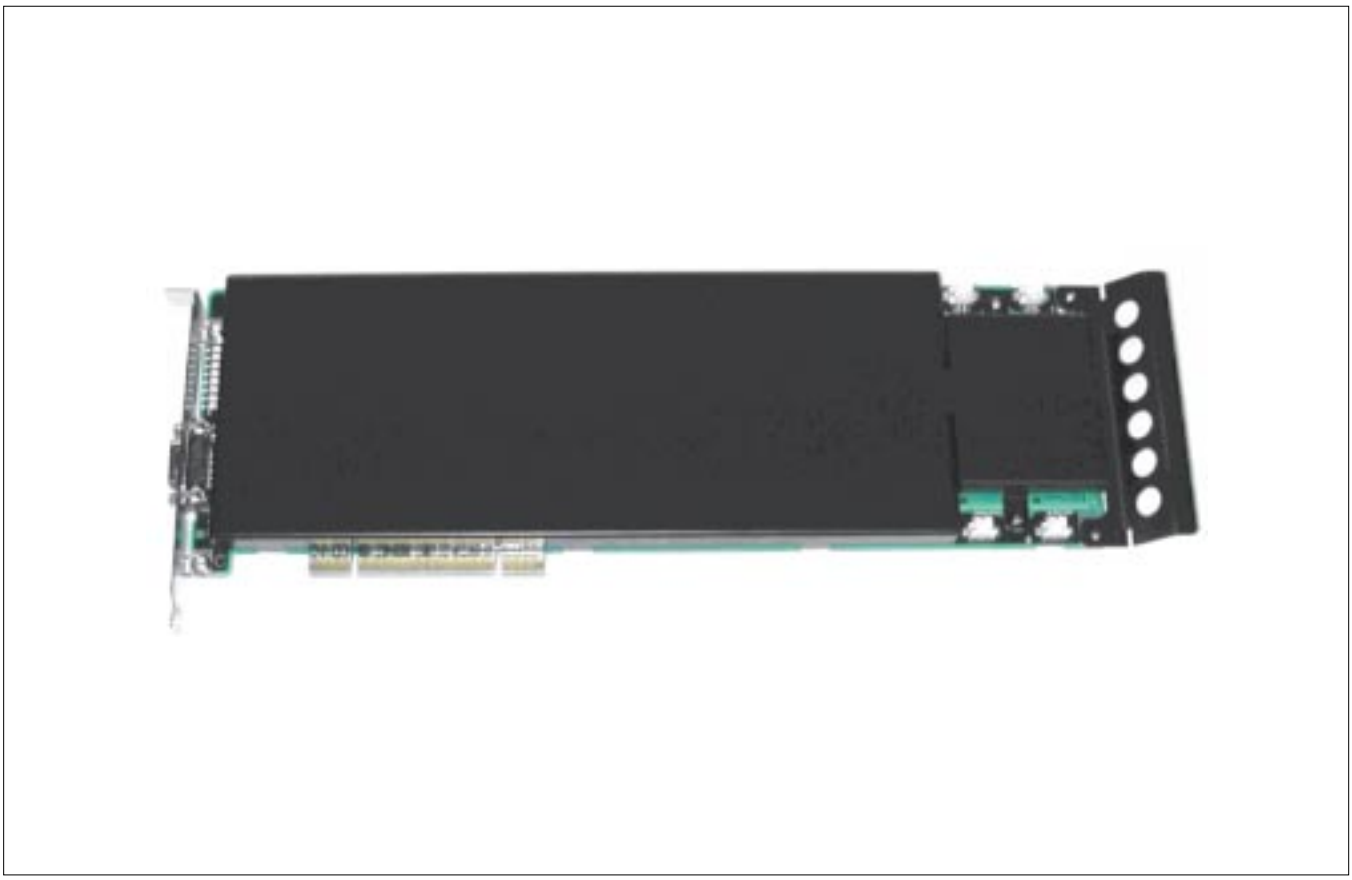
中川路哲男*
竹原　明**

要　旨

暗号機能の実装において，パソコンやUNIX(注)などの汎用的なアーキテクチャの計算機上でのソフトウェアによる実現では，解析される可能性が残るため，安全性に限界がある。耐タンパーセキュアボード“TURBOMISTY”は，この点を解決するための専用ハードウェアであり，暗号演算を安全にかつ高速に実行する機能を持っている。計算機内のPCI(Peripheral Component Interconnect)バススロットに装着可能なボードであり，RSAやMISTYなどの暗号処理をボード上で実行する。その特長は“耐タンパー”と呼ばれる不正アクセス防止機構であり，ボードの引き抜きや不正解体などのボード上の機密情報への不正アクセスを検知すると，自動的に機密情報を消去することによってその盗難を防止する。また，アプリケーションプログラムへ提供するインタフェースとしては，ICカード等で業界標準となっているインタフェースを採用している。

今後のセキュリティシステムの本格的実用化に向けては，認証サーバやSSL(Secure Socket Layer)サーバなどのセキュリティ確保がますます重要になってくる。これらでのセキュリティ要件をソフトウェアによる実現だけで満足することはできないため，このような専用ハードウェアの必要性が増大すると予想される。実際，米国では，政府調達基準(Federal Information Processing Standards：FIPS)において耐タンパー性のレベルを分類・規定しており，このような専用ハードウェアによる実現を調達の要件としているシステムも増えつつある。

本稿では，耐タンパーセキュアボードTURBOMISTYの機能，特長などについて述べる。



耐タンパーセキュアボード“TURBOMISTY”

このボードは，パソコンやUNIXサーバのPCIスロットに装着されるボードである。１台の計算機に４枚まで装着可能である。

*情報技術総合研究所(工博)　**同研究所