耐タンパー性を備えた暗号処理ボードの試作

2L－8

竹原 明　中川路 哲男
三菱電機（株）　情報技術総合研究所

1．はじめに

近年、インターネットやイントラネットの普及に伴い、これらのネットワークを利用した情報通信が一般的になりつつあるが、データの盗聴や改ざんの危険があり、暗号技術を応用したセキュアアプリケーションのニーズが高まっている。データの暗号化や電子署名などで必要となる暗号処理やその暗号鍵の保管には高度な安全性が要求されるが、従来は暗号処理や暗号鍵の保管は計算機上で行われ、パスワードにより保護されているのみであり、安全上問題があった。そこで、暗号鍵を安全に管理することを目的とした暗号処理ボードを試作した。本稿では試作した暗号処理ボードの概要を報告する。

2．設計方針

本暗号処理ボードは以下の点を考慮して設計を行った。

① 暗号鍵の漏洩を防止するための安全性の高い仕組みを実現する。

② 標準のインタフェースに準拠することにより他の鍵格納デバイスとの互換性を実現する。

③ 暗号アルゴリズムの追加も考慮して拡張性を持たせる。

3．実装

3．1 ハードウェア構成

暗号鍵の漏洩を防止するために、従来コンピュータのハードディスク上に格納されていた暗号鍵をPCI ボード上で管理する。そのために PCI ボードに以下の機能を実装した。

(1) PCI ボードの内部に鍵情報を完全に隠蔽するため、暗号鍵の生成、暗号鍵の保管、暗号処理を実行する機能。

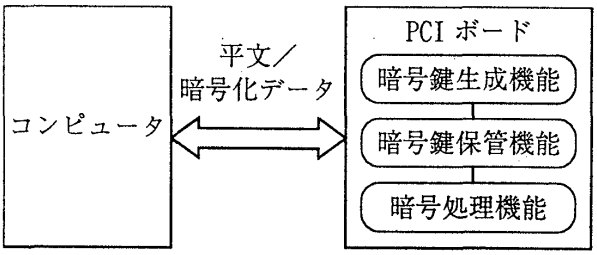

図1

(2) ボード上の信号の読み取りを防ぐ仕組みと、不正なアクセス（以下、タンパーと記す）を検知して保持している暗号鍵情報を消去する機能

以上の機能を実現するため、図2に示すハードウェア構成とした。

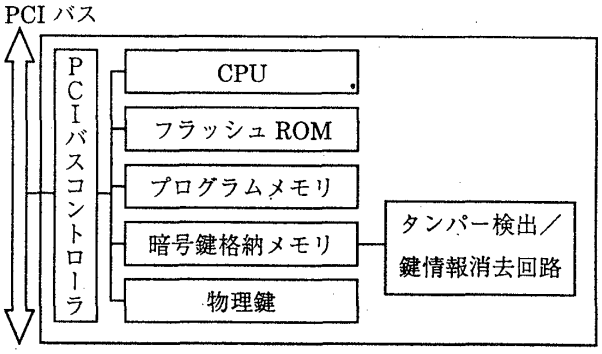

図2　ハードウェア構成図

(1)の暗号鍵の生成／暗号処理は、拡張性を考慮してソフトウェアにより実行する方式を取った。そのために必要となる CPU、プログラム実行用メモリ、プログラム格納用のフラッシュ ROM を搭載している。また、暗号鍵は暗号鍵格納用メモリに格納される。

(2)の暗号鍵の消去は、タンパー検出回路がボード上のカバーの取り外しやボードの抜き取りなどの不正なアクセスを検出し、暗号鍵格納メモリ内に格納されている鍵情報を瞬時に消去する。この仕組みは①ハードウェアで鍵情報を管理する。②タンパー

A Prototype of Tamper Evident Cryptographic Board
A.Takehara , T.Nakakawaji
Information Technology R&D Center ,
Mitsubishi Electric Corporation

を検知して保持している鍵情報を自動消去する。の2点を実現しており、米国政府調達基準であるFIPS（Federal Information Processing Standards）140-1のレベル3に相当する高い安全性を実現している。

また、3個の物理鍵を備え、暗号処理や暗号鍵のバックアップなどを実行するために必要な物理鍵の個数を設定したり、処理ごとに特定の物理鍵を割り当てることにより、実行できる担当者を分けるなど、物理鍵とパスワードによるアクセス制限を行うことにより、安全性を向上させている。

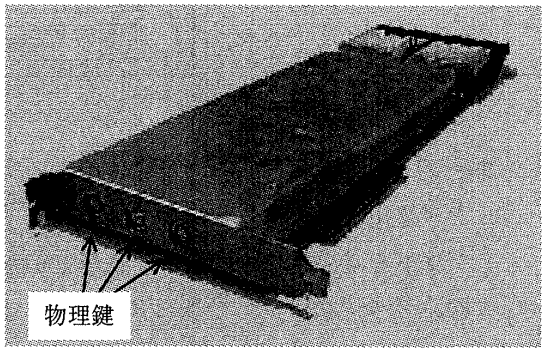

図3　暗号処理ボードの外観

試作した暗号処理ボードの外観を図3に示す。PCIボード上の回路はカバーで覆われており、表面には物理鍵の鍵穴を備え、鍵保存用のバッテリーを搭載している。

3．2 ソフトウェア構成

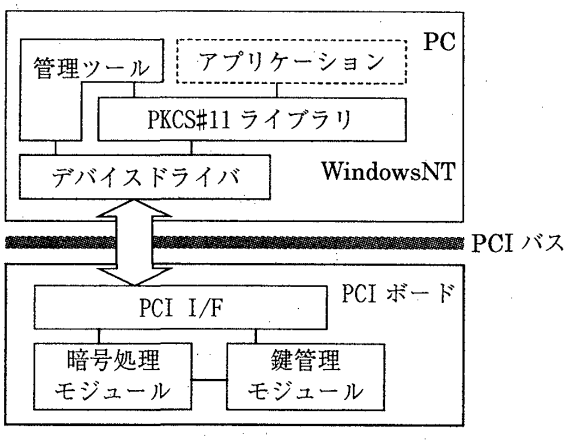

図4　ソフトウェア構成

ソフトウェア構成を図4に示す。PCIボード上の暗号処理モジュールは現在RSAのみサポートしているが、モジュールの更新により比較的容易に他の暗号アルゴリズムの拡張が可能である。

コンピュータ側には暗号処理ボードの状態やタンパー検出情報を取得するための管理ツールと、PKCS（Public-Key Cryptography Standards）#11のインタフェースを提供するライブラリを用意している。本暗号処理ボードを使用するアプリケーションはPKCS#11インタフェースでアクセスすることにより、他のPKCS#11準拠の鍵格納デバイスとの互換性が保たれる。また、PKCS#11は本来ICカードのようなシングルユーザー向けのインタフェースであり、マルチユーザーによる1デバイスの共有はできないが、本暗号処理ボードでは図4中のPKCS#11ライブラリで1台の暗号処理ボードを論理的に複数のデバイスとして扱うようにしていることにより、PKCS#11の仕様を変えることなくマルチユーザーでの使用を可能にしている。

5．適用

本暗号処理ボードは、当社の製品である認証サーバ<CERTMANAGER>や認証ライブラリ<CertMISTY>における秘密鍵の格納媒体として組み合わせて使用することが可能となっており、電子商取引システムやCALSシステムなど、安全性の高いセキュリティシステムを構築することができる。

6．まとめ

本稿では、試作した暗号処理ボードの概要、および実装方式について述べた。

今後は、処理速度の向上、安全性向上のための検討を行う。

参考文献

[1]Security requirements for cryptographic modules,
http://csrc.nist.gov/fips/fips1401.htm

[2]RSA Laboratories, "PKCS#11 Cryptographic Token Interface Standard,"1997