HITACHI
Inspire the Next

NEWS RELEASE

2002年2月25日
2002-025

業界初、個人認証機能付フラッシュカード「PINセキュアマルチメディアカード」を製品化

－Personal Identification Number(PIN)照合により、第三者へのデータ漏洩を防止でき、個人情報・企業秘密データ等の保護を実現－

日立製作所 半導体グループ(グループ長＆CEO 伊藤 達)は、このたび、個人情報や企業情報などで第三者への漏洩防止が必要な秘密データの記録メディアとして、業界で初めて Personal Identification Number(PIN)(注1)による個人認証機能を持つフラッシュカード「PINセキュアマルチメディアカード(注 2)」を製品化しました。今回、第一弾として 32M バイトの「HB28D032PSM2」を2002年4月よりサンプル出荷します。

本製品は著作権保護機能を持ち、強固なセキュリティを実現した「セキュアマルチメディアカード」に、PINによる個人認証機能を追加したフラッシュカードです。暗号化した秘密データを解く鍵（ライセンスキー）を取り出すためのPINを登録しておき、入力したPINが一致した時にのみ鍵を取り出してデータを復号できるため、第三者へのデータ漏洩を防止できます。このため、個人情報や企業の秘密データをPDAなどのモバイル端末で扱う際に、万一、本カードや端末を紛失した場合でも情報の保護が可能となります。

＜背景＞

近年、PDAに代表される携帯情報端末の普及により、個人や企業の情報をこれらの端末にダウンロードし、外出先などで閲覧・利用する機会が増えています。一方、これらの個人情報・企業情報には機密性を有するデータが多く、このような利用環境下では、例えば外出先で端末を紛失した時など、秘密情報が第三者に漏洩することが懸念されています。

これに対応するため、一般的にはデータを暗号化したり、メモリカードにパスワードなどのロックをかけたりして情報の保護を図っています。しかし、このような方法では、暗号化したデータを復元するための鍵がデータと同じ端末上にあるため、ソフトウェアの解析等により鍵が発見されてしまう恐れがあったり、あるいは鍵さえあれば誰でもデータを見ることが出来るなど、セキュリティは万全とはいえず、更に強固なセキュリティを実現できるシステムへのニーズが高まっています。

さらに、このようなセキュリティシステムに対しては、専用のハードウェアを必要とせず、汎用のハードウェアで実現することも求められています。

こうしたニーズに対応するため、当社では今回「PINセキュアマルチメディアカード」を製品化、第一弾として32Mバイトの「HB28D032PSM2」を製品化しました。

＜製品について＞

本製品の主な特徴は、次の通りです。

1. 業界で初めてフラッシュカードにPINによる個人認証機能を搭載し、個人情報・企業情報の保護を実現

暗号化した秘密データを解く鍵（ライセンスキー）を取り出すためのPINを登録することによ

り、正しいPINが入力された時のみ鍵を取り出してデータを復号できるため、本人以外にはカード内の秘密データを取り出せないよう保護しています。

また、従来のセキュアマルチメディアカードで実績のある著作権保護技術も備えており、暗号化データと、それを復号するための鍵を別々に取り扱うことができます。例えば、企業内で特定個人や特定階層にのみ鍵を配布することにより、情報閲覧可能者を制限することが可能です。PINによる個人認証と著作権保護機能を組合せることにより、さらに強固で高度なデータのセキュリティシステムを構築できます。

2.ソフトウェアでPIN認証等のセキュリティ機能を実現

PINの認証、データの暗号／復号等、セキュリティに関する機能は、本カードと、端末のソフトウェアによりすべて実現できます。マルチメディアカード（注3）スロットを持つ機器であれば、これらのソフトウェアを組込むことにより、セキュリティ実現のためのハードウェア変更を特に必要とせず、秘密データの保護を実現できます。

3.ハードウェアタンパレジスタントによる高度なセキュリティの確保

本製品では、PIN認証や暗号･復号等のセキュリティ機能、およびPIN、ライセンスキー等のセキュリティ関連情報は、従来のセキュアマルチメディアカードと同様、すべてハードウェアタンパレジスタント領域（TRM）(注 4)に格納しています。カードや端末を紛失した際の第三者による解析に対し、高度なセキュリティを確保できます。

また、PINの入力回数制限の設定により、くり返し入力によるPINコードの解析を困難にする等、アプリケーションの面からも、セキュリティの強化が図れます。

本カードは、標準のマルチメディアカードの上位互換であり、外形は厚さも含めて同一の小型サイズの32×24×1.4（mm）を実現しています。

今後は顧客ニーズに応じて、他の容量の展開にも対応していきます。

＜サポートツール＞

PIN認証応用システムを設計する際のサポートツールとして、暗号、認証部を含むリファレンスソフト、ライブラリ、およびアプリケーションとのインタフェース仕様書を2002年4月から提供予定です。

(注 1)PIN(Personal Identification Number)：所有者の認証コード。
(注 2)セキュアマルチメディアカード：Secure MultiMediaCardは、コンテンツ保護などのセキュリティ機能を内蔵したMultiMediaCardの総称です。
(注 3)マルチメディアカード：MultiMediaCardは、独Infineon Technologies AGの商標であり、MMCA(MultiMediaCard Association)にライセンスされています。
日立はMMCAのボードメンバーです。http://www.mmca.org/
(注 4)タンパレジスタント領域(TRM)：タンパレジスタント技術は、半導体チップなど内部解析や改ざんを、物理的および論理的に防衛する技術です。TRMは、この技術を用いて形成･構成されるシリコン領域またはカードの領域です。

■応用機器

●個人用途

PDA 等の携帯情報端末、PC、携帯電話、デジタルカメラ等の個人用情報端末

●業務用途

・企業内情報ネットワークの端末

・営業、外交従事者の業務用モバイル端末

■価　格

製 品 名	容 量	価 格
HB28D032PSM2	32M バイト	オープン

■仕　様

項　目	仕　様
型名	HB28D032PSM2
メモリ容量	32M バイト
インタフェース	・ MultiMediaCard ・ SPI(Serial Peripheral Interface)
読出速度	1.7M バイト／秒
書込速度*	1.0M バイト／秒
動作電圧	2.7～3.6V
動作電流	読出時： 20mA(typ.)　書込時： 35mA(typ.)
動作温度	-25～85℃
外形寸法	32mm×24mm×1.4mm　７ピン
セキュリティ 関連機能	・ PKI**方式　暗号/復号機能 ・ PIN 認証機能

* 書込速度はプレーヤ側の処理時間を除いたカード自体の書込速度

** PKI：Public Key Infrastructure（公開鍵暗号技術）

■照会先

株式会社 日立製作所 半導体グループ システムメモリビジネスユニット

メディアフラッシュプロダクトマーケティングチーム

〒100-0004 東京都千代田区大手町二丁目 6 番 2 号（日本ビル）

電話 03(5201)5021(ダイヤルイン)

■報道関係問い合わせ先

株式会社 日立製作所 半導体グループ 事業企画本部 広報部[担当：依田]

〒100-0004 東京都千代田区大手町二丁目 6 番 2 号(日本ビル)

電話　03(5201)5250(ダイヤルイン)

以 上