技術紹介

13 個人情報保護機能対応メモリーカード用リーダー・ライタの開発

Development of the Reader/Writer for Memory Card with Personal Information Protection Function

横森　博之　Hiroyuki　Yokomori　システム機器事業部　技術部　主任

キーワード Keywords
メモリーカード、リーダー・ライタ、セキュリティー
memory card, reader/writer, security

■ 要旨

今日のインターネットの普及に伴い、企業・個人を問わず、デジタル犯罪の被害は増加の一途を辿り、企業の社会的な信頼低下、ビジネス機会の損失をもたらし、不正利用に至ってはネットビジネスに深刻な影響を与えております。

今回、従来からコンテンツ保護として実績のあるメモリーカードに、個人情報保護機能を追加した新しいセキュリティーカードが開発されました。今回開発したリーダー・ライタでは、いち早くファームウェアとドライバを開発し、このセキュリティーカードに対応致しました。

■ SUMMARY

In line with spread of the Internet usage, damage by digital crime is more and more increasing in both organizations and individuals, and is threatening social trust of corporations and business opportunities. Furthermore, computer abuse is giving serious impact to the Internet business.

JAE has developed a reader/writer for a new type security card, which adds personal information protection function to the existing memory card used for contents protection. For the new reader/writer, we have quickly adopted the firmware and driver to meet the requirement of security card.

写真１　CEATEC 出典サンプル

1　まえがき

近年、パソコンやインターネットの著しい普及に伴い、DSC（Digital Still Camera）やDVC（Digital Video Camera）などマルチメディア関連機器の需要が高まってきました。これらの機器の大部分には、画像データの保存用として様々な規格の小型メモリーカードが搭載されており、手軽にパソコンでの印刷・編集やインターネットでの配信・閲覧が可能になってきました。また、小型メモリーカードは画像データだけでなく、個人や企業にとって重要な情報の格納・運搬媒体としての役割も担っています。これらの小型メモリーカードには何種類かの規格があり、中には単にデータ保存用のものから、ID 機能・著作権保護機能・個人情報保護機能などを盛り込んだ高機能なものまで様々あります。

著作権保護機能（メモリースティックのマジックゲート機能※1、SD メモリカードの SD Secure API 機能※2）に対応したリーダー・ライタは、昨年開発してパソコンメーカーに供給することができました。今回はコンパクトフラッシュ、スマートメディア、メモリースティック、MMC/SD メモリカードに対応したリーダー・ライタをベースに、個人情報保護機能を有している小型メモリーカードとして MMC の上位互換であるセキュアマルチメディアカード（Secure MultMmediaCard）※3 の中の PIN-SecureMMC※4 も含んだリーダー・ライタを開発しましたので、紹介致します。

※1　マジックゲート機能はソニー株式会社が推奨している著作権保護機能です。
※2　SD Secure API 機能は株式会社東芝、松下電器株式会社、米国 SanDisk Corp の共同開発によるメモリーカードの著作権保護機能です。
※3　セキュアマルチメディアカードは MMCA が推奨しているメモリーカードで、マルチメディアカードにセキュリティー機能を付加したものです。
※4　PIN-SecureMMC：Personal Identification Number-Secure MultiMediaCard（個人認証番号対応セキュアマルチメディアカード）

2．PIN-SecureMMC について

2.1　特長

① IC カード等で用いられている、セキュリティー方式（PKI※5）をベースに考案されたメモリーカードで、ユーザー自身のデータや、ユーザーが属する企業・団体のデータを守る、新しいタイプのセキュアメモリーカードです。

② コンテンツ保護用のセキュアメモリーカードとして実績のある SecureMMC に、 PIN による認証機能を追加したメモリーカードです。

③ PIN による本人認証と証明書による機器認証の組み合わせにより、セキュリティーレベルを段階化することが可能です。

　例えば、パスワードをパソコンに記憶させ、カード挿入で自動的に認証を行うように、カードを物理的な鍵として使用することも可能です。さらに機器認証機能により、 認証していないパソコンからは、 カードを挿入しても証明書を発行しないように設定することで、 カードからのキーデータが送出されず、キーデータの認証をできなくなり、セキュリティーレベルの強化が図れます。

※5　PKI：Public Key Infrastructure

2.2　PKI の原理

　電子データの保護を目的として注目されるのが PKI で、 公開鍵暗号方式という暗号化技術を使用したセキュリティーインフラです。公開鍵暗号方式は従来から存在する共通鍵暗号方式の問題点を解決するものとして考案されました。

　共通鍵暗号方式は、 暗号化するための鍵とそれを復号化する鍵を共通のものを使用するため、 あるデータを暗号化した時に使用した鍵は、 復号化する時にも必ず必要となります。そのため、複数の相手とデータのやり取りを行う場合、相手の数だけ鍵を保管し、それを厳重に管理する必要があります。

　図 1 に共通鍵暗号方式の暗号化と復号化の仕組みを示します。

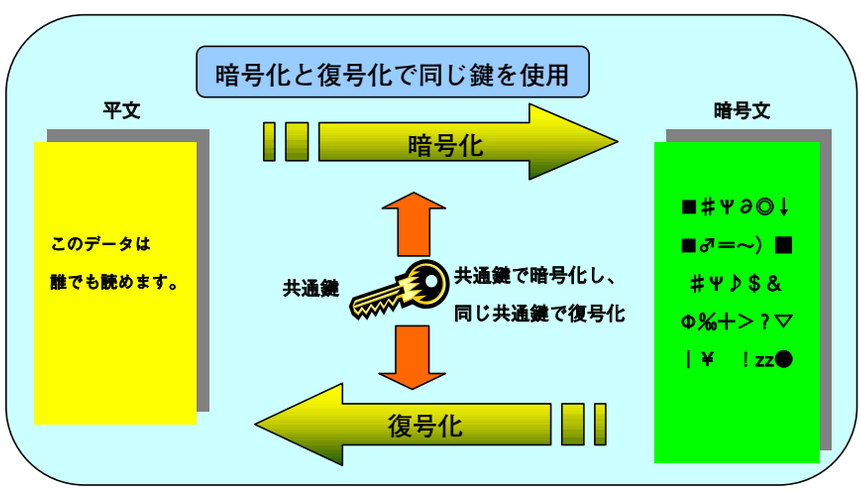

図 1　共通鍵暗号方式の暗号化と復号化の仕組み

これに対して公開鍵暗号方式では暗号化と復号化で異なる2つの鍵（キーペアと呼ばれる一対の鍵）を生成し、片方の鍵で暗号化したものはそれと対になっているもう一方の鍵を使用しなければ復号化できなくなります。この一対の鍵は「秘密鍵」と「公開鍵」と呼ばれています。

図２に公開鍵暗号方式の暗号化と復号化の仕組みを示します。

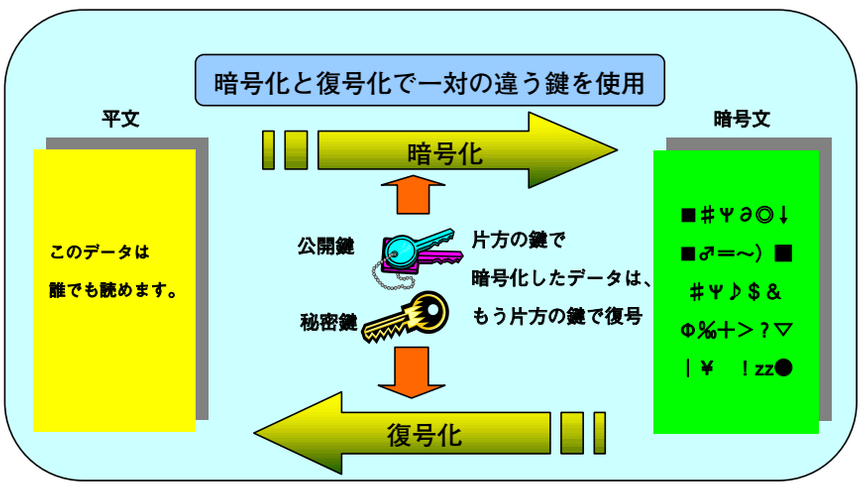

図２　公開鍵暗号方式の暗号化と復号化の仕組み

B氏がA氏に暗号データを送付する場合の実例を下記に示します、

① B氏はA氏の公開鍵を入手します。
　・この鍵の内容に機密性はないためA氏は電子メールで転送しても、ホームページで公開しても問題はありません。）

② B氏はA氏の公開鍵を入手し、その鍵を使用して送付したいデータを暗号化し、A氏に送付する。

③ A氏は自分の秘密鍵で暗号データを復号化する。

このようにA氏の公開鍵で暗号化したものは、A氏の秘密鍵以外では復号化できないため、暗号化されたデータの内容が漏れることはありません。逆に、A氏の公開鍵を持っていれば、誰もがA氏との暗号データのやり取りができることになります。

つまり、高いセキュリティーを維持したまま、インターネットのようなオープンなインフラを利用できる訳です。

2.3 PIN-SecureMMC 対応のリーダー・ライタ開発

PIN-SecureMMC を開発したメーカーと当社は、それぞれがメモリーカードとリーダー･ライタを開発しているメーカーという関係から以前より交流があり、今回の開発では当社がリーダー・ライタを同時に開発することになりました。

当社が開発を担当した部分は、リーダー･ライタ（ハードウェアおよびファームウェア）とWindows 上で動作するセキュア・ドライバです。すでに、基本となる MMC のリーダー・ライタ開発の経験や資産があったため、それらの有効活用を前提に短期間での完成を目標としました。ハードウェアに関しては既存の製品を流用しました。図 3 にハードウェアブロックを示します。

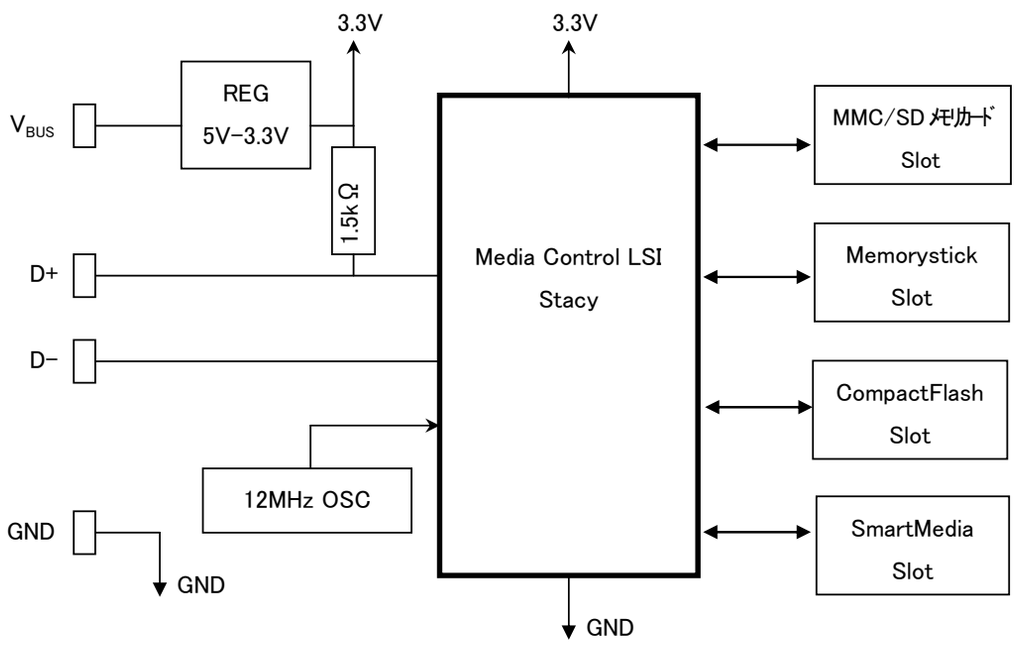

図 3　ハードウェアブロック図

ハードウェアの主な構成として、メモリーカード、USB を制御しファームウェアを搭載する LSI、12 MHz の発振子、電圧レベル変換のレギュレータ IC および各種メモリーカードのスロットがあります。この LSI は航空電子の仕様を基に製作したもので、データの転送効率を高めるための DMA コントローラが内蔵されています。

ファームウェアおよびドライバに関しては既存製品の設計資産をベースにして、PIN-SecureMMC および API（Application Programming Interface）の仕様に基づき開発を行いました。図4にソフトウェアブロック図を示します。図中の破線部が、今回開発を担当した、リーダー･ライタとセキュアドライバです。

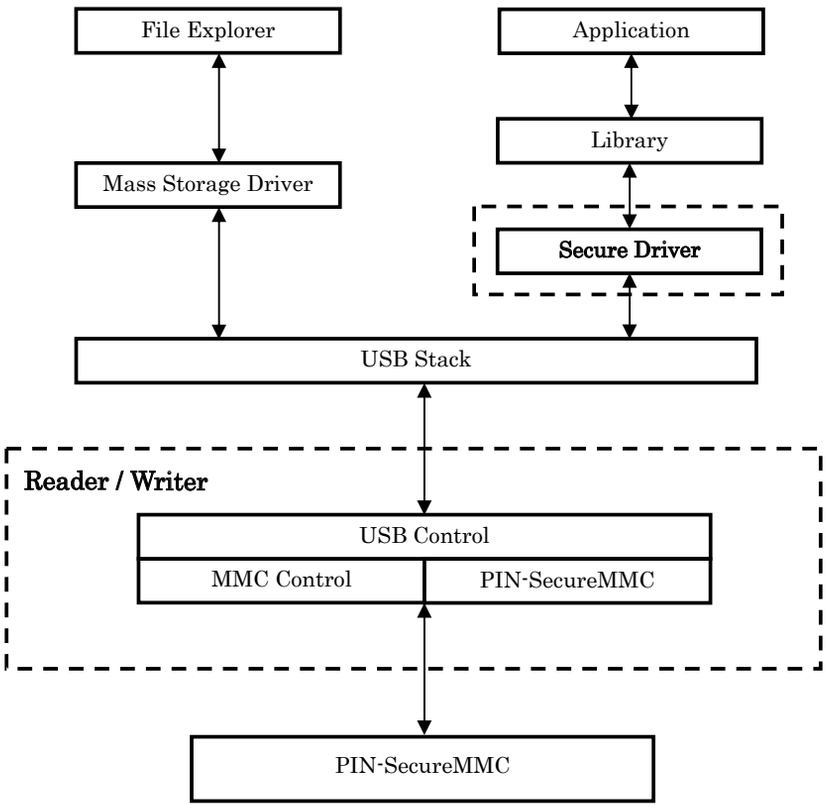

図 3 ソフトウェアブロック図

ソフトウェアの構成はマスストレージドライバを通して、ファイルの入出力、初期化、リード／ライトの処理を行う部分と、セキュアドライバを通して、PIN による認証コマンドの処理を行う部分に分かれます。またライブラリは PIN-SecureMMC に対し、PIN による認証等を行う関数群と、データの暗／復号を行う関数群で構成されます。

開発当初、 PIN-SecureMMC がまだメーカーで開発中であったために、 リーダー・ライタの試験や評価用に必要な PIN-SecureMMC の入手時期がかなり遅れることが予想されました。そこで、その入手時期を早めるために、航空電子での設計からプログラミングを短期間に行い、早めに技術試作サンプル（ドライバおよびリーダー・ライタ）をメーカーに提出することによって、カード開発メーカーにおける PIN-SecureMMC 開発期間の短縮を目標としました。

まず、 PIN-SecureMMC と API に依存しないドライバとファームウェア間のインターフェースを先行して決め、 それからそれぞれの仕様書に関する部分の開発を独立して進めました。また、 仕様書に関する質問や当社の設計情報をカード開発メーカーに迅速に伝えて、 情報の共有化を計りました。

2.4　リーダー・ライタ仕様

2.4.1　USB 仕様

①ホスト PC 接続時、USB Mass Storage Class に準拠した USB 大容量記憶デバイスとして認識されます。
② USB 1チャネルを通じて同時に4種類のメモリーカードにアクセス可能です。（対応するメモリーカードは6種類です。）
③ Windows XP 搭載のパソコンに接続時は、OS 標準搭載のドライバ（usbstor.sys）を使用するため、専用のデバイスドライバが不要です。
④ USB データ転送プロトコルは、 Bulk only 転送（12Mbps）に対応しております。
⑤ USB データ転送用コマンドは UFI コマンドを使用しております。
⑥バスパワーでの使用ができます。

2.4.2　ストレージ仕様

① CompactFlash は 3.3V/True IDE Mode に対応しております。
② SmartMedia は 3.3V 版に対応しております。
③ SmartMedia の ID 機能には対応していません。
④ CompactFlash の I/O 系（モデム、 LAN など）のカードには対応していません。

2.4.3　対応規格

① USB 規格に関して下記に準拠しております。
・Universal Serial Bus Specification Version 1.1
・Universal Serial Bus Mass Storage Class Specification Version 1.0
② CompactFlash 規格に関して下記に準拠しております。
・CompactFlash Specification Version 1.4
③ SmartMedia 規格に関して下記に準拠しております。
・SmartMedia Version 1.10
④ Memorystick 規格に関して下記に準拠しております。
・Memorystick Version 1.3
⑤ SD メモリカード規格に関して下記に準拠しております。
・SD Memory Card Specification Version 1.0
⑥ MMC 規格に関して下記に準拠しております。
・MultiMediaCard Specification Version 1.0
⑦ SecureMMC 規格に関して下記に準拠しています。
・SecureMultiMediaCard System Specification Version 1.00

2.4.4　対応 OS

下記の OS 対応しております。

・Microsoft Windows XP Professional

・Microsoft Windows XP Home Edition

また、別途要求に応じ、下記 OS にも対応可能です。

・Microsoft Windows 2000 Professional

2.4.5　その他

① SD メモリカードの著作権保護機能（SD Secure API）に対応しています。
（別途専用のジュークボックス用アプリケーションが必要となります。）

② SD メモリカードの著作権保護機能を利用するための、SD secure API 対応ドライバソフトを提供致します。
（別途 SDA※6 との NDA 契約において入手するドライバソフトもあります）

③メモリースティックの著作権保護機能（マジックゲート）には対応していません。

④ PIN 認証機能に対応しています。

⑤ UDAC-MB 規格にも対応可能です。

※ 6　SDA は（株）東芝、松下電器産業（株）、米国 SanDisk 社が設立した団体です。

写真 1 は今回開発した 6 種類のメモリーカードに対応したリーダー・ライタで、2002 年の CEATEC に出展致しました。表面に CompactFlash 用コネクタと Memorystick 用コネクタ、裏面に MMC/SD メモリーカード用コネクタと SmartMedia 用コネクタを配置しであります。今回、マイクロドライブカードにも対応しましたので、計 6 種類のカードに対応致しました。

パソコンとの接続用に USB コネクタを実装しており、それぞれのメモリーカードに対応したアクセス用 LED も実装しています。

3　PIN-SecureMMC を使った製品応用例

3.1　パソコンを制御する制御

① OS の起動およびログオンを制御することにより無断な使用を排除できます。
②スクリーンセーバーをロックすることにより、安心して離席することができます。
③ファイルやフォルダの暗号化により不正なアクセスを禁止することができます。

3.2　ユーザー制御

①パスワードを3つまで管理できるため
・3人で1枚の PIN-SecureMMC を共有使用
・3つのパソコンを1枚の PIN-SecureMMC で使用
・パスワードの階層化によるセキュリティーの階層化により豊富な認証手法を構築できます。
②鍵となるデータの有効期限や回数制限を行うことにより使う人のレベル（管理者、役員社員、パート等）に応じてセキュリティーを強化することができます。
③鍵となるデータはローカルで発行・運用することができるので、企業内でのシステム構築が容易にできます。

4　むすび

今回の開発では今日までに培ったファームウェア、ドライバ開発技術の展開として、新たに PIN-SecreMMC を使用した PIN による認証機能をサポートすることができ、他社とは差別化したリーダー・ライタを開発することができました。

小型メモリーカードが持つセキュリティー機能は、音楽配信や映像データ等の著作権保護だけでなく、個人または企業における情報の保護としての機能を持つことで、さらなる展開が期待されます。今後のメモリーカードの高速化への対応や、USB2.0 への対応も検討中です。またパソコンを中心とした業界以外への展開を考え、USB 以外のインターフェースへの対応や、システム LSI 化への取組みも検討中です。

（注 1）　メモリースティック、マジックゲートメモリスティックは、ソニー株式会社の登録商標です。
（注 2）　コンパクトフラッシュ（Compact Flash™）は米国 SanDisk Corp. の登録商標です。
（注 3）　スマートメディア（SmartMedia™）は株式会社東芝の商標です。
（注 4）　ＳＤメモリーカードは株式会社東芝、松下電器株式会社、米国 SanDisk Corp の共同開発によるメモリーカードです。
（注 5）　マルチメディアカード（MultiMediaCard ™）は独 Infineon Technologies AG の登録商標です。
（注 6）　Microsoft および Windows は米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。