KeyMobile を用いた安全なデータ持ち出し

Carrying Data Securely in KeyMobile

近年，利便性の高い USB メモリやメモリカードの紛失，盗難，P2P ソフトなどによる情報漏えい事故が多発し，社会問題となってきている。そのため，企業では，USB メモリやメモリカードの使用を禁止するなどの対策を進めている。しかし，このような使用禁止によってデータの保存，持ち出しの利便性が低下してきている。そこで，フラッシュメモリと IC カードを併せもつ KeyMobile を用いて第三者や P2P ソフトがメモリカードに格納されたファイルを容易に取り出すことのできない技術を開発した。これにより，メモリカードの利便性を損なうことのない安全なデータの持ち出しの実現を目指す。

岡崎　司　Okazaki Tsukasa
畠山　誠基　Hatakeyama Seiki
佐藤　隆一　Sato Ryuichi

１．はじめに

近年，情報漏えい事故が社会問題となってきており[1)]，企業では情報セキュリティ対策の一つとして USB メモリやメモリカードの使用禁止などの処置をとってきている。しかし，このような使用禁止によってデータの保存，持ち出しなどの利便性が低下してきている。また，この対策の一つとして，メモリカードには認証機能や暗号化などのセキュリティ機能が追加されはじめている。しかし，メモリカードを装着した PC にインストールされていた Winny などの P2P ソフトを通じて情報がインターネット上に漏えいした場合，たとえ暗号化してあったとしても，企業は信用を失うことが避けられない。

一方，このようなメモリカードの一つとして，フラッシュメモリに加え，強力な認証機能を提供する IC カードを備えた KeyMobile[2)]というデバイスがある。これは従来の USB メモリと同様に使用することができる。これまで KeyMobile は，主にネットワーク認証の認証因子として使用されてきたが[3)]，認証機能を利用し，フラッシュメモリに格納されたデータへのアクセスをコントロールすることで，安全な記録メディアとしての利用が期待できる。

そこで，メモリカードの利便性を損なうことなく安全なデータの持ち出しの実現を目的として，KeyMobile を利用し，第三者や P2P ソフトなどがメモリカードに格納されたファイルを容易に取り出すことのできない技術を開発した。

２．従来手法とその課題

USB メモリは，フラッシュメモリを搭載し，外部記憶装置として認識するための仕様である USB マスストレージクラスの仕様に準拠している。Windows が標準搭載しているドライバでアクセスすることができ，ハードディスクと同様のファイル操作が可能である。

USB メモリに格納されたファイルは，例え暗号化してあっても，USB メモリを PC に装着すれば，Windows の標準機能でファイルの存在が明らかとなり，標準機能のファイル操作で持ち出すことができる。同様に，P2P ソフトからも標準のインタフェースでファイルの存在を知ることができ，ファイルを取り出すこともできる。

ファイルの特定を困難にする方法として，ファイルシステムそのものを暗号化したセキュアファイルシステムがある[4)]。この方法では，ファイルだけでなく，管理情報も暗号化するため，暗号の鍵を知らない者はファイルを特定することはできない。しかし，ファイルシステムが存在することはわかる。さらに，この方法でも，ファイルシステムが USB マスストレージクラスの仕様に準拠しているパーティションに格納されているため，標準のインタフェースでファイルシステムごと取り出すこと

はできる。

これに対し，USB マスストレージクラスの仕様に準拠せず，独自の仕様を用いた製品もある [5]。この製品は専用ハードウェア化しているので，格納されるファイルにアクセスするためには，専用ソフトウェアを必要とする。したがって，それ以外の手段でファイルを取り出すことはできない。しかし，この方法は特定メーカーの記録メディアに限定され，ユーザの選択肢は少ない。これは普及にとって大きなデメリットとなる。

このように従来の方法では，ファイル単位またはファイルシステムごと USB メモリから取り出すことができるため，P2P ソフトでの漏えい対象となり得る危険性がある。したがって，標準機能だけではファイルの存在を知ることができず，またファイルを取り出すことのできない技術が望まれる。さらに，ユーザが記録メディアを幅広く選択できるようにするため，標準の仕様に準拠したインタフェースでアクセスできる技術が求められる。

3．KeyMobile とその特長

KeyMobile は，図 1 に示すように IC カード，フラッシュメモリ，コントローラから構成されている。PC からのコマンドは，コントローラを介して制御され，IC カードまたはフラッシュメモリのそれぞれをコントロールする。

形状および外寸は RS-MMC(Reduced Size-Multi-media Card)と同形状，同外寸である。フラッシュメモリは，SD/MMC 規格に準拠しているため，通常のメモリカードとしても利用できる。メモリ容量は 64M バイトの製品と 128M バイトの製品がある。

IC カード内に格納された情報にアクセスするためには，PIN(Personal Identification Number)コードと呼ばれる所有者本人があらかじめ設定した文字列の入力が要

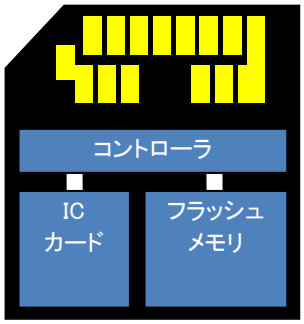


図 1　KeyMobile

求される。IC カードは，耐タンパ性と呼ばれる物理的にも論理的にもハッキングを防御する機能で守られている。一般的な IC カードのセキュリティレベルは，以下の三種類である。

(1) IC カード内部に書き込まれた情報が不正に取り出されたり，改ざんされることがない
(2) ニセの IC カードが作成されることがない
(3) IC カードそのものが本来の所有者以外の人物に不正に使用されることがない

このように IC カードは強固に守られている。したがって，PIN コードが漏えいすることがなければ，IC カード内に格納された情報が不正に読み出されることはない。そのため，PKI(Public Key Infrastructure)で利用する秘密鍵やバイオメトリクス情報を IC カード内に格納し利用することで，高度な認証が可能になる。

4．安全なデータ持ち出し技術

2 章で述べた課題を解決するために KeyMobile のフラッシュメモリに格納されたデータを第三者や P2P ソフトが取り出すことのできない方式を開発した。本方式では，第三者や P2P ソフトがアクセスできない領域を秘匿エリアと呼ぶ。フラッシュメモリ領域を秘匿エリアと通常エリアの二つに分割し，一方を秘匿エリアとしてアクセスコントロールの対象とする。領域内での通常エリアの位置やサイズの情報は，従来と同様にフラッシュメモリの MBR に格納する。通常エリアは，USB マスストレージの仕様に準拠しており，Windows の標準機能を用いてアクセスすることができる。一方，秘匿エリアの位置やサイズの情報は，IC カードに格納する。これにより秘匿エリアの情報にアクセスできるのは IC カードの PIN コードを知る所有者だけとなる。また，IC カードへのアクセスは Windows では標準的に使用される PC/SC[6]インタフェースを用いる。

秘匿エリアの実現イメージを図 2 に示す。IC カードから秘匿エリアの情報を取得し，秘匿エリアに格納されたデータにアクセスするための手段として，認証を介したアクセス手段を用意する。本開発では，Explorer ライクなビュワーとして作成した。本ビュワーを起動すると，IC カードの PIN コード入力を要求する。ビュワーは，入力された PIN コードを IC カードに問い合わせ，正しい PIN コードであれば，秘匿エリアの情報を取得し，秘匿エリアへのアクセス手段を提供する(図中(1))。PIN コードが間違っている場合は，プログラムを終了する。正

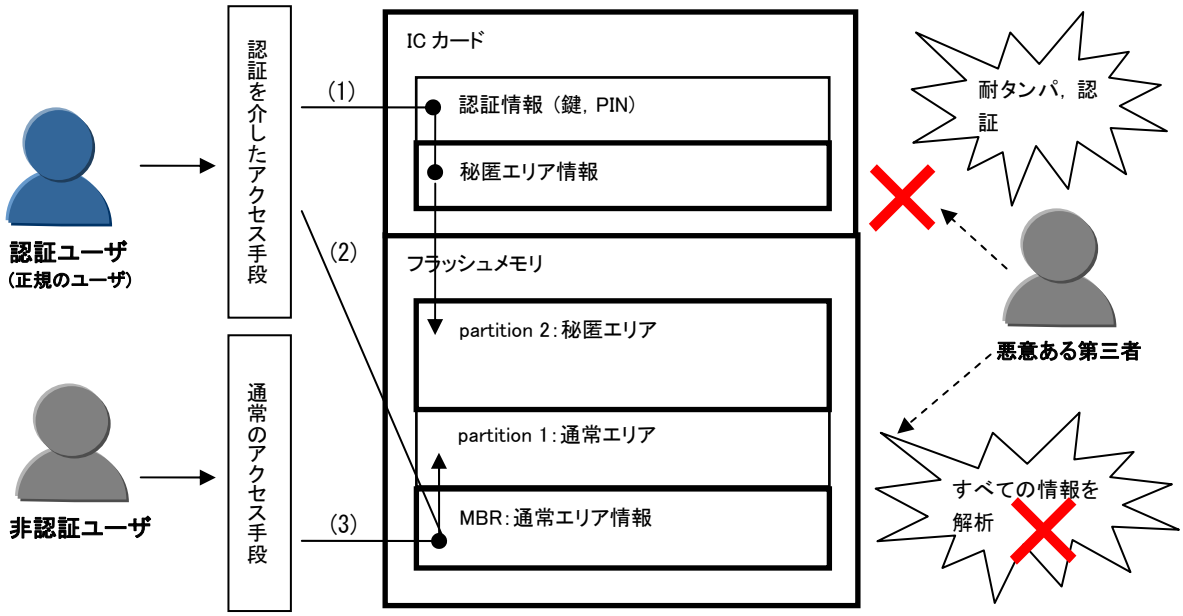


図 2　秘匿エリアの実現イメージ

規のユーザは，正しい PIN コードを知り得るためビュワーを介して秘匿エリアにアクセスすることができる。また，通常エリアはこれまでと同じく MBR を参照しアクセスすることができる(図中(2))。

一方，正しい PIN コードを知りえない非認証ユーザは，通常のアクセス手段しか提供されないため，秘匿エリアへアクセスすることはできない。アクセスできるエリアは，通常エリアだけであり，通常のアクセス手段を介してアクセスする(図中(3))。

PIN コードを知らない悪意ある第三者には，通常エリアしか見えないため，秘匿エリアの存在に気付かず，攻撃する動機を起こし難い。もし，攻撃しようとしても，IC カードは耐タンパ性で守られ，秘匿エリアの情報を取得することができない。したがって，フラッシュメモリ内のすべての情報をダンプしても，そこからファイルを復元することはできない。また，P2P ソフトは，Windows のドライブに割り当てられたパーティションにアクセスし，そこに格納されたファイルを転送しようとする。しかし，秘匿エリアのパーティションは Windows のドライブに割り当てられることがないため，P2P ソフトからアクセスできない。

このように秘匿エリアを設け，その情報を IC カードに格納することで，正しい PIN コードを知らない第三者がファイルを取り出すこととファイルの存在を知ることを困難にできる。

図 3　Windows Explorer での参照結果

5．評価

フラッシュメモリの容量が 128M バイトの KeyMobile を用い，簡易なファイルシステムを実装して実験をした。図 3 に Windows Explorer による参照結果を示す。通常エリアは 100M バイト，秘匿エリアは 10M バイトに設定した。図中のリムーバブルディスク(F:)が通常エリアである。図から明らかなように，このエリアの容量はほぼ 100M バイトであり，通常エリアであることを示している。100M バイトより少なく表示されているのは，ファイルシステムの管理情報の分である。リムーバブルディスクとして一覧表示されているドライブは，A，F，Z

だけである。A および Z はそれぞれフロッピーディスクドライブ，CD ドライブであり，秘匿エリアのドライブは表示されていない。このことから，リムーバブルディスクとして一覧表示され，ファイルコピーなどの通常のアクセス手段が提供されるのは，通常エリアに対してだけであることがわかる。秘匿エリアは，その存在さえ確認することができない。

さらに，Windows API を使って，すべてのドライブを表示させるプログラムを作成して実験したが，秘匿エリアのドライブを得ることはできなかった。これは，P2P ソフトが Windows API を使って秘匿エリアにアクセスできないことを示している。

また，表示されたエリアのすべてを占有するサイズのファイルを書き込み，秘匿エリアにデータが書き込まれていないことを確認した。さらに，通常エリアのサイズより大きいサイズのデータを書き込もうとしても書き込めないことも確認した。以上により，通常のアクセス手段である Windows Explorer からは，秘匿エリアにアクセスできないことが実証されたと言える。

秘匿エリアの実現方式は，一般的なファイル単位の暗号化と比較すると次に示すような優位性がある。

(1) ファイル単位の暗号化では，暗号化されたファイルの存在が第三者に知られるのに対して，秘匿エリアは，ファイルの存在が知られない。
(2) ファイル単位の暗号化では，暗号化されたファイルを取り出して解析することができるのに対して秘匿エリアは，ファイルを取り出すための情報が隠蔽されているため，容易に取り出せない。
(3) ファイル単位の暗号化では，暗号化のパスワードだけを解析すればよいのに対して，秘匿エリアは，ファイルシステムそのものの解析に加え，セクタ単位にデータを連結するソフトウェアを開発しない限りファイルを復元できない。

このように秘匿エリアの位置やサイズの情報を KeyMobile の所有者本人しかアクセスできない IC カードのメモリに格納することにより，第三者や P2P ソフトがアクセスすることができないファイルシステムを実現できる。

本技術と同様に秘匿エリアを持つ USB メモリがあるが，専用ハードウェア化されている [7]。本技術は，ソフトウェアだけで構成できるため IC カードを搭載した MMC や SD メモリカードであれば KeyMobile 以外のカード，例えば smartSD にも応用が可能である。したがって，ユーザは，これらのカードの中から目的に応じて適切なカードを選ぶことができる。

６．おわりに

KeyMobile のフラッシュメモリ領域に秘匿エリアを設け，その位置やサイズの情報を IC カードに格納することにより，第三者や P2P ソフトが容易にファイルを取り出すことができないようにする技術を開発した。これにより，紛失し第三者に拾われたり，P2P ソフトがインストールされた PC に装着された場合でも，格納されたデータの漏えいを防止することができる。本技術は，「KeyMobile 簡易発行システム」の拡販活動を通じて得た顧客ニーズに対応したものである。KeyMobile そのものが持つ高度なセキュリティ機能を活かし，社会問題とされている情報漏えいの対策に効果を発揮すると期待できる。本論文では，簡易なファイルシステムを用いて評価し，秘匿エリアが隠ぺいされることを確認した。しかし，さらに安全性を向上させるためにファイルシステムの暗号化は必須である。今後は，この課題を解決し，早期の実用化を目指す。

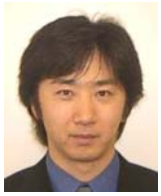
参考文献

1) NPO 日本ネットワークセキュリティ協会：2007 年情報セキュリティインシデントに関する調査報告書, http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1.6.pdf
2) (株)日立製作所：セキュリティデバイス KeyMobile, http://www.hitachi.co.jp/products/secure_ubiquitous_office/keymobile/
3) 畠山，他：ユビキタスカードビジネス向け「KeyMobile 簡易発行システム」の開発，日立 TO 技報 第 11 号，pp.54-59(2005.11)
4) 川島，他：メモリカードのためのセキュアファイルシステム SAS の提案，信学技報，Vol. 105, pp.19-24(2005.5)
5) エレコム株式会社：セキュリティ機能搭載 高速版 USB メモリ MF-JU2BK2 シリーズ, http://www2.elecom.co.jp/data-media/usb-flash/mf-ju2/bk2/
6) PC/SC Workgroup：PC/SC Workgroup, http://www.pcscworkgroup.com/

7) (株)アイ・オー・データ機器 : EasyDisk - セキュア USB メモリー, http://www.iodata.jp/product/usbmemory/easydisk/ed-s2a/

岡﨑　司　　1985 年入社
研究開発部　研究開発グループ
生産計画技術の研究, 組込みソフトウェア技術の研究
okazaki@hitachi-to.co.jp

畠山　誠基　　1991 年入社
組込みソフト開発第 1 グループ
KeyMobile ソリューションの提供
sehatake@hitachi-to.co.jp



佐藤　隆一　　1986 年入社
組込みソフト開発第 2 グループ
組込みソフトウェアの開発
ryu@hitachi-to.co.jp