メモリカード用暗号デバイスドライバ

1H-06

遠田 潤一　　鮫島 吉喜
日立ソフトウェアエンジニアリング（株）

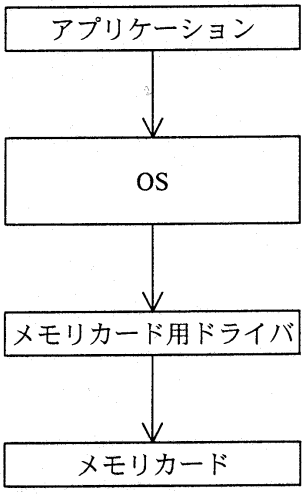
1. はじめに

記憶容量が少ない携帯 PC の普及に伴い、Flash-ATA カードやコンパクトフラッシュカードなどのメモリカードに機密データを保存し、携帯 PC 上で機密データを参照･更新する例が増えている。これらのメモリカードが盗まれると、中に保存しておいたデータの内容を簡単に参照できてしまう。このため、メモリカード盗難時のデータ漏洩を防止する仕組みが必要である。

本論文では、メモリカード内のデータを自動的に暗号化する機能を持つデバイスドライバを提案する。なお、提案するドライバは FAT ファイルシステムを対象としている。

2. セクタ単位での I/O 処理

メモリカードの I/O 処理について述べる。例として、アプリケーションがメモリカード内のファイル foo.txt へデータ abc…xyz を書き込む場合を示す。概要は図 1 のとおりである。



説明

①アプリケーションは、OS に対して、ファイル foo.txt の書き込み位置を指定し、ファイルへの書き込みデータ abc…xyz を渡す

②OS は、BPB(BIOS Parameter Block)を参照して、ファイル foo.txt の書き込み範囲がメモリカードのセクタ番号 0095H であることを割り出す

③OS は、メモリカード用ドライバに対して、書き込みを行うセクタ番号 0095H を指定し、セクタへの書き込みデータ…abc…xyz…を渡す

④メモリカード用ドライバは、メモリカードに対して、0095H 番のセクタへデータ…abc…xyz…を書き込む

図 1　メモリカードへの書き込み処理

BPB には総セクタ数・ FAT 数・ルートディレクトリのエントリ数などの FAT ファイルシステムに関する情報が記録されており [1]、メモリカードが携帯 PC へ挿入された際に OS があらかじめ取得しておく。

3. 暗号処理方法

提案する暗号ドライバは、メモリカードに対する OS からの I/O をフックして暗号・復号を行う。OS からメモリカード内へデータの書き込み要求があったときには、その要求を横取りして書き込みデータを暗号化してからメモリカードへ保存する。暗号ドライバはメモリカード用ドライバから暗号データ書き込み完了の応答が返ってくると、OS に平文データを書き込んだと認識させるために、暗号データを平文データへ戻

Cryptographic Device Driver for Memory Card
Junichi Enda, Yoshiki Sameshima
Hitachi Software Engineering Co., Ltd.

してOSに対して平文データ書き込み完了の応答を返す。概要を図2に示す。

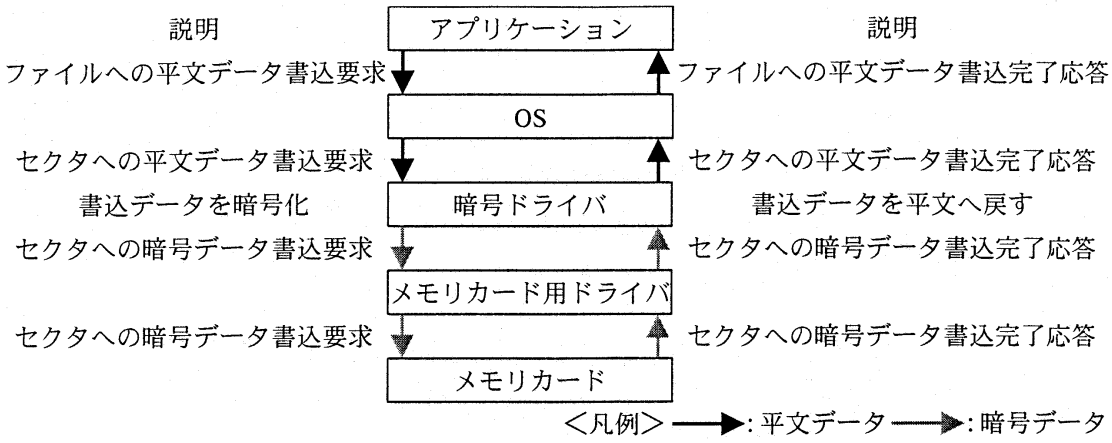


図2　暗号ドライバを組み込んだシステムでの書き込み処理

一方、メモリカード内データの読み出し要求があったときには、その要求の結果を横取りして読み込んだデータを復号してから要求を出したOSへ渡す。

4. 暗号鍵の隠蔽方法

複数の携帯PCやデスクトップPCとの間でメモリカード内のデータを利用できるようにするために、暗号鍵はメモリカード内に保存しておいた方がよい。ところが、暗号鍵を通常の方法で保存しておくと、ユーザの誤操作によって消去されてしまうおそれがある。そこで、ユーザから暗号鍵の存在を隠し、暗号鍵を消去されないようにする方法を考案した。図3に方法の概要を示す。

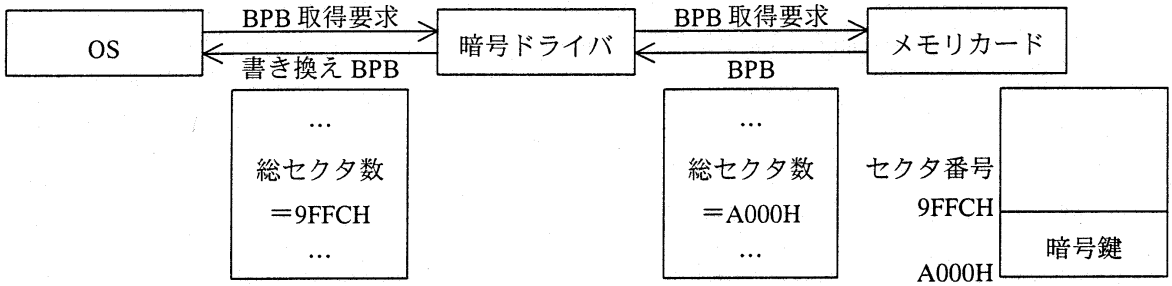


図3　BPB書き換えによる暗号鍵の隠蔽

(1) あらかじめメモリカードのセクタ番号9FFCH番以降のセクタに暗号鍵を格納しておく。

(2) メモリカードの携帯PCへの挿入時にOSがBPBを取得する際、暗号ドライバがBPBの総セクタ数の部分をA000Hから9FFCHに書き換える。

(3) OSからはセクタ番号 9FFCH 番以降のセクタはメモリカードの領域外であると認識されるため、暗号鍵を隠蔽することができる。

5. まとめ

OSからメモリカードへのI/Oをフックして入出力データを暗号処理することで、メモリカード内に保存するデータの盗み見を防ぐことができる。また、OSからの BPB 取得要求をフックして総セクタ数の部分を書き換えることで、メモリカード内に保存する暗号鍵をユーザから隠すことができる。

参考文献

[1] PCMCIA ： PC Card Standard – Release 7.0(1999)