USB 接続による暗号化装置の認識の改善

A recognition improvement of the encryption device by USB interface

055131　古尾谷 悦基

（指導教員　木村 誠聡　教授）

1　はじめに

21 世紀初頭の情報社会においては様々なデータを保存するため、交換式記憶媒体が用いられてきている[1]。その中で USB フラッシュメモリは USB インターフェースを持ち、安価で持ち運びも便利なため広く普及している。しかしながら、その反面、置き忘れや盗難等による重要データの流出が問題になっている[2]。人為的なミスを完全に防ぐのは不可能だと考えられる。この問題を解決するためにソフトウェアでの暗号化やUSBフラッシュメモリ自体に認証機能を持たせる技術が開発されてきている。しかし、前者は OS に後者はハードウェアに依存するという問題がある。その問題を解決するべく、USB 接続による暗号化装置が開発された。しかしながら、この USB 接続を用いた暗号化装置は、装置に対して USB フラッシュメモリを予め差しておく必要があり、利便性の問題が存在する。この問題を解決する方法を提案し、その実装を行う。すなわち、USB フラッシュメモリと暗号化装置の差し込みの順序を意識することなく使用可能とし、利便性を上げることを目的としている。

2　USB 暗号化装置

この暗号化装置は、認証機能や暗号化機能を持たない USB メモリに対して認証・暗号化機能を付加するというもので、ユーザは PC と USB メモリの間に暗号化デバイスを接続するだけで暗号化を行うことができる[3]。この暗号化装置と他の暗号化の比較を表1に示す。

ソフトウェアの場合は、処理が高速なのと暗号化の強度が高いという長所があるが、ユーザによる操作が必要のためパソコン初心者の人に扱いづらく、OS と PC に依存してしまう短所がある。

機能付加の場合は、USB メモリに対して指紋認証機能などを付加する方法で複雑な計算をしないため転送速度は速い、操作はハードウェアの操作だけだが認証機能を持たない USB メモリに対して互換性がないという欠点がある。そこで、この暗号化システムは両者の欠点を解決するため、暗号化と認証機能を PC・USB メモリから切り離して開発されている。

表1、暗号化法の比較

	評価		
項目	ソフトウェア	機能付加	暗号化装置
処理速度	○	○	×
操作性	×	△	△
互換性	×	×	◎

2．1　暗号化装置の問題点

従来法は、USB メモリが接続状態の暗号化装置を PC に差し込むことで、PC に USB メモリであることを認識させている（図1）。

しかし、USB メモリが接続状態でない暗号化デバイスを PC に差し込んだ後、USB メモリを接続しても PC は先に差し込まれた暗号化装置の初期情報を保持したままなので USB メモリがあることを認識してくれないという問題がある（図2）。

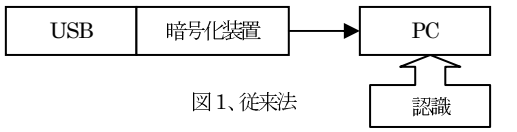

図1、従来法

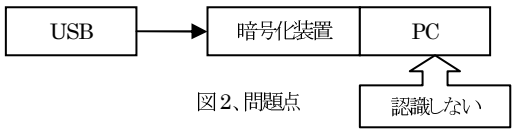

図2、問題点

3　提案する接続方法

この方法はリコネクトという論理的に切断するリセット法を考案して考えた接続方法である。その流れを図3に示す。まず、USB メモリが差し込まれてない暗号化装置を PC に接続したとき論理的に切断状態にする。その後に USB メモリが暗号化装置に接続されたら、ディスクリプタの読み出しを行い、論理的に切断状態になっているのを解いて接続状態に戻し、ここで PC は USB メモリを認識することができると考える。

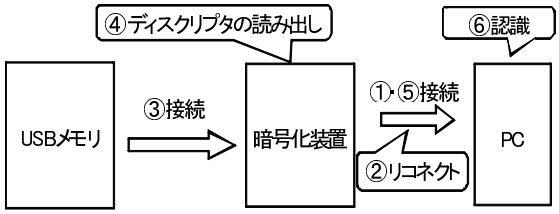

図3、提案する接続方法

4　まとめ

本稿で提案した接続方式で後差しと差し替えの実験を行い、認識の改善に成功した。今後は、暗号化強度の強化、処理速度の高速化が挙げられる。その結果を図4に示す。

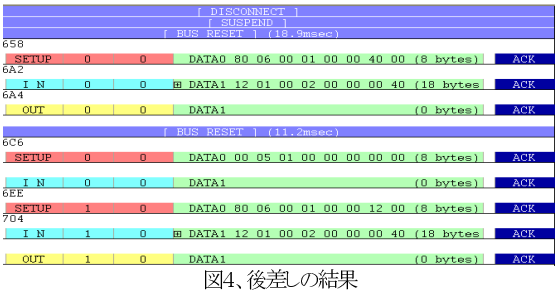

図4、後差しの結果

参考文献

[1]　トランジスタ技術 2007 年 2 月号　PP.107－109
CQ 出版社　2007 年 2 月 1 日発行

[2]　朝日新聞 “社員個人情報1万人紛失” PP.34
2005 年 5 月 25 日発刊

[3]　八木橋和宏、木村誠聡、田口亮
：USB 接続による暗号化デバイスの開発、P507、
第 21 回 回路とシステム軽井沢ワークショップ論文集