1ZE-10

学校向けUSBメモリ貸出システムにおける不用意な情報持ち出しへの対策強化

上枝 俊太† 納富 一宏†
神奈川工科大学大学院†

1. はじめに

近年のコンピュータ機器の普及に伴い，学校にも様々な情報機器が導入されている．しかし，一方でUSBメモリなどの情報機器が個人情報流出事故の原因にもなっており，問題視されている．

NPO 日本ネットワークセキュリティ協会(JNSA)の公表する「2011 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」[1]では 2011 年に「教育，学習支援業」において発生した個人情報流出事故件数は 216 件とされており，前年の調査より増加している．一方で個人情報流出被害者数は 99,271 名とされており，前年の調査の数値からは減少したものの依然として見過ごせない数値となっている．

本研究では，学校で起こる個人情報流出事故の防止と被害の抑制を目的とした，USB メモリ貸出システムの開発と検討を行っている．

本稿では，前研究までの USB メモリ貸出システムの完成という観点から，近年の個人情報流出事故の原因で大きな割合を占める「不正な情報持ち出し」への対策の強化を行い，システムの更なる改善を目指す．

2. USBメモリ貸出システム

学校で発生した個人情報流出事故統計の調査，学校教育に関する識者へのヒアリングやアンケートを行い，学校で求められている個人情報流出事故抑制のシステムを検討した．以下にシステムの要件を列挙する．

・個人情報の管理ミスの抑制を行うこと
・USBメモリへの対策をとること
・流出事故1件あたりの被害者数を抑制すること
・十分なセキュリティを有すること
・私物のUSBメモリを利用させないこと

以上を踏まえ，学校の個人情報流出事故を抑制するUSB メモリ貸出システムを考案し，開発した．これについて以下に述べる．

2.1 システムのセキュリティの概要

USBメモリのセキュリティを保つために，私物のUSBメモリの持ち込みを厳しく制限し，十分なセキュリティを有する USB メモリの用意と管理を学校側が行い，必要に応じて貸出を行う．

学校側で用意する USB メモリは安全性を高めるため，暗号化仮想ドライブ作成ソフトウェア TrueCrypt[2]を用いて USB メモリの暗号化仮想ドライブ化を行い，英数字で構成される 20 字のランダムな文字列を USB メモリのロック解除のパスワードとして設定する．パスワードは返却の度にプログラムが新しく生成と更新を行う．パスワードは WEB メールを通じて利用者にのみ送信し，第三者に USB メモリが渡った際の不正利用の抑制を行う．

USB メモリの貸出の際に，利用教員の氏名や貸出日時などの情報をデータベースに登録する．また，USB メモリの管理責任者全員に貸出報告メールを送信して情報を共有し，USB メモリと個人情報の管理ミスの抑制を行う．

利用した USB メモリは，返却時にフォーマットを行うことにより情報の蓄積を防ぎ，新しいパスワードで再度暗号化仮想ドライブ化し，次回の貸出に備える．

2.2 システム利用の流れ

USBメモリ貸出システムにおける，USBメモリの貸出から返却までの流れをフローチャートとして図 1 に示し，説明を行う．

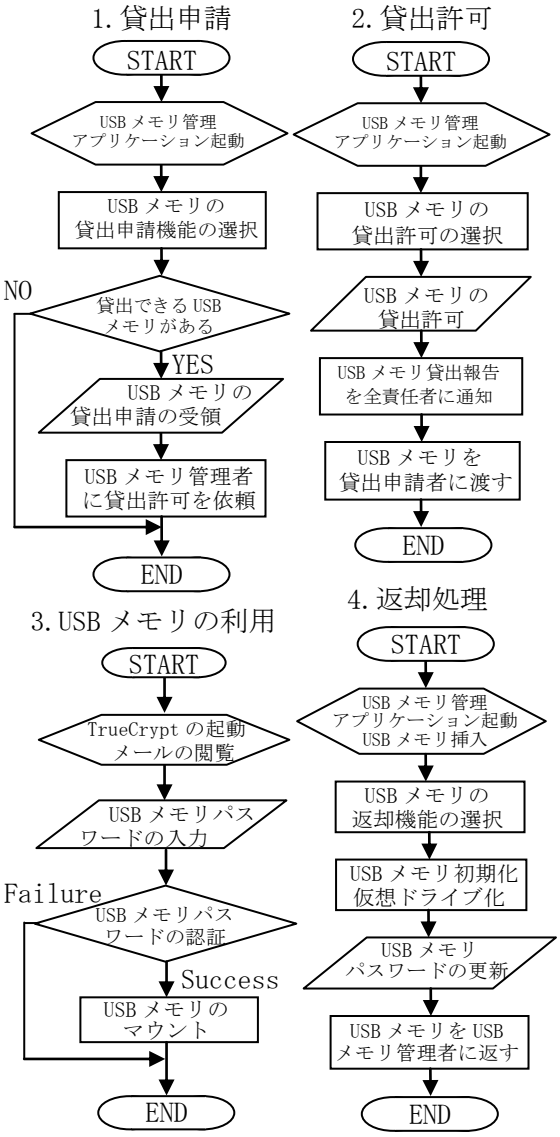

図1 システムのフローチャート

USB flash drive management system to unfair use of a USB flash drive at school
†Shunta Kamieda , Kazuhiro Notomi
†Graduate School of Engineering, Kanagawa Institute of Technology

2.2.1 USB メモリの貸出申請

USB メモリの貸出を希望する教員は，共用パソコンの USB メモリ管理アプリケーションを立ち上げ，自身の ID とパスワードでログインし，貸出申請を行う．

2.2.2 USB メモリの貸出許可

貸出を希望する職員に貸出許可を依頼された USB メモリ管理責任者は，USB メモリ管理アプリケーションを用いて，返却予定日等の情報を入力し，申請に対し貸出許可を行う．許可の内容は学校における責任者全員に，アプリケーションがメールによって通知を行う．利用希望者に対しては，USB メモリを利用するために必要なパスワードが記載されたメールが送信される．貸出許可の処理が終了した後，所定の場所に保管されている USB メモリを持ち出し，利用希望者に対して貸出を行う．

2.2.3 USB メモリの利用

学校側の用意した USB メモリを利用するパソコンにインストールしておいた USB メモリマウント用アプリケーションを起動し，メールに記載されているロック解除用のパスワードを入力することで，利用可能になる．

2.2.4 USB メモリの返却

USB メモリをパソコンに挿入した状態で，USB メモリ管理アプリケーションの返却処理機能を実行する．アプリケーションは USB メモリをフォーマットし，新しいパスワードによって，再度暗号化仮想ドライブ化する．処理の終了後，USB メモリを管理責任者に返却する．

3. 不正な情報持ち出しへの対策強化

前研究においては，前章で述べた USB メモリ貸出システムについて短期間の運用実験と評価アンケートを実施し，良好な結果を得た．

本研究においては，近年の教育現場における個人情報流出事故の原因で高い割合を占める，不正な情報持ち出しに着目し，対策を行う．

3.1 不正な情報持ち出し

JNSA の 2011 年の調査報告書で示されている，2011 年に「教育，学習支援業」で発生した 216 件の個人情報流出事故の原因の割合を次の図 2 に示す．

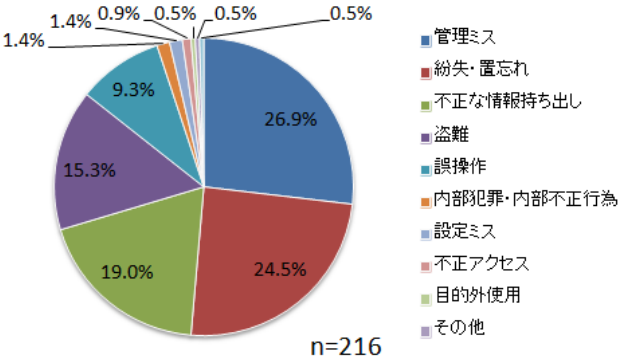

図 2 個人情報流出 事故原因の割合

同調査書では「教育，学習支援業」は『他の業種に比べて突出しており，「不正な情報持ち出し」が最も多い業種』であるとされ，問題視されている．そこで「不正な情報持ち出し」について，学校側の管理していない不正な USB メモリの利用への対策からアプローチを行う．

3.2 実施した不正な情報持ち出し対策

USB メモリの挿入を検知し， USB メモリ固有のシリアルコードを調査することにより，挿入された USB メモリが学校側の用意した正当な USB メモリなのか，利用の許可を得ていない不正な USB メモリなのかを識別する USB メモリ監視アプリケーションを作成した．アプリケーションの挙動を図 3 に示す．

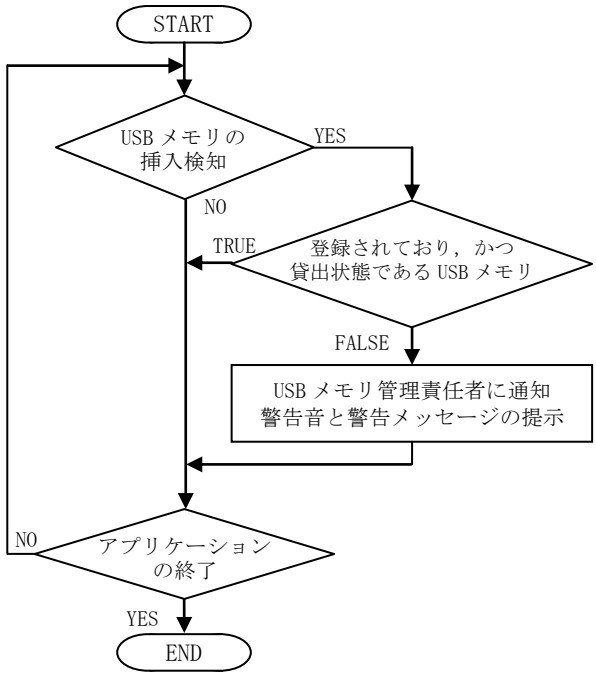

図 3 USB メモリ監視アプリケーションの挙動

挿入された USB メモリがデータベースに登録されている学校の用意した USB メモリであり，かつ貸出手続きによって貸出状態になっている場合は何の問題もない．そうでない場合は，不正 USB メモリの使用の事実を USB メモリ管理責任者全員にメールで通知し，USB メモリ利用者に対し警告音と警告メッセージを提示する．

3.3 考察

前研究においては，不正な USB メモリの持ち込みに対しては厳罰という形で対策をしていたが，本研究ではそれに加えてアプリケーションによって常時監視を行う．そのため，前研究よりも不正な情報持ち出しが抑制できると判断できる．また，職員室には常に数名の教員が在室していることがほとんどであり，職員室の共用パソコンに不正な USB メモリが挿入された場合，警告音によって，その場にいる教員に不正な USB メモリの利用を示唆する効果も望めると考えられる．

4. おわりに

本研究では，前研究までの成果である USB メモリ貸出システムについて，近年の教育現場の個人情報流出事故原因の中でも問題視されている，不正な情報持ち出しについての対策強化を行った．USB メモリの利用について監視を行う USB メモリ監視アプリケーションを作成し，不正な USB メモリの利用を抑制することにより，不正な情報持ち出しへの対策を行うことができた．

今後の研究課題として，正当な手続きを踏んで貸出された USB メモリを介した不正な情報持ち出しへの対策が，改善点として考えられる，

参考文献

[1]NPO 日本セキュリティネットワーク協会:「2011 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/incident/2011.html
[2]TrueCrypt http://www.truecrypt.org/