N-023

情報流出事故を考慮した学校における USB メモリ貸出システム

USB flash drive management system in school to prevent information leakage incidents

上枝 俊太† 納富一宏†
Shunta Kamieda Kazuhiro Notomi

1. はじめに

近年のコンピュータの普及により，教育現場にも様々な情報機器が導入されている．しかし教育現場への情報機器の導入は，情報機器を媒体とした生徒の個人情報流出事故の原因になっている．生徒の身の安全を守るため，保護者からの信頼を裏切らないためにも，生徒の個人情報流出は絶対に起こしてはならないものである．

本稿では，教育現場での個人情報流出事故の統計データや教育現場の実態調査を元に，生徒の個人情報流出被害の防止と抑制を目的とした，学校での USB メモリ貸出システムの検討を行う．

2. 実態調査

学校で起きた個人情報流出事故の統計の調査，学校教育の識者へのインタビューやアンケートを行い，学校で求められている個人情報保護システムの要件を検討する．

2.1 JNSA の情報流出事故の調査報告書

NPO 日本ネットワークセキュリティ協会(JNSA)による「2009 年 情報セキュリティインシデントに関する調査報告書」[1]には，2009 年に起きた個人情報流出事故に関する統計が纏められている．それによれば，①管理ミス，②紛失･置忘れ，③盗難，④不正な情報持出しの 4 点で，教育･学習支援業における個人情報流出事故の原因の約 9 割の説明が可能とされる．

また，同調査報告書によると教育・学習支援業における情報流出事故の経路の四割強は USB メモリ等の可搬記録媒体であるとされている．

2.2 神奈川県立総合教育センターへのインタビュー

教育者としての能力が高く，教務の内容全般について熟知している識者の意見を知るため，神奈川県立総合教育センターに協力を仰ぎ，学校における情報セキュリティに関するインタビューを実施した．

学校で用いられるシステムに必要な要件として，情報セキュリティ強度が十分であること，なるべく安価で高い費用対効果があることが挙げられた．

2.3 学校における USB メモリの利用状況の調査

学校における USB メモリの利用状況の調査として，本大学の教員・学生の内，教育実習を含め中学校や高等学校への勤務経験のある者に協力を仰ぎ，学校内での USB メモリの利用状況に関するアンケートを実施した．

アンケートの結果，アンケート対象者の約 3/4 程度が勤務中に USB メモリを利用したと回答し，その内半数以上が学校において私物の USB メモリを利用したことがあると回答した．また，私物の USB メモリにパスワードの制限をかけていると回答したのは 1 名のみであった．また，私物の USB メモリを利用した理由としては，学校側で USB メモリを用意していると知らなかった，学校に USB メモリが用意されていなかったなどの意見が散見された．

† 神奈川工科大学大学院工学研究科 Graduate School of Engineering , Kanagawa Institute of Technology

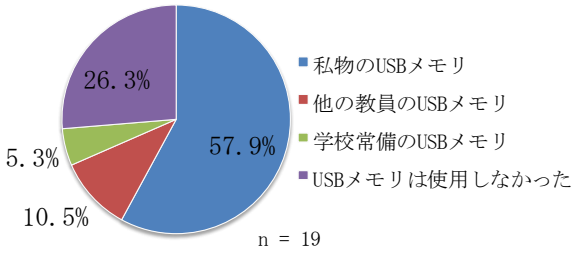


図 1 教務経験者へのアンケート

3. USB メモリ貸出システム

2 章の調査にて，以下に列挙する事柄が学校における個人情報保護には必要であることが分かった．

- USB メモリへの対策
- 安価で費用対効果が高いこと
- 十分なセキュリティを有すること
- USB メモリの管理ミスや紛失･置忘れ等への対策
- 私物の USB メモリを利用させないこと

以上を踏まえ開発している，情報流出事故を考慮した学校における USB メモリ貸出システムについて以下に述べる．

3.1 システムのセキュリティの概要

USB メモリを流出経路とする個人情報流出事故の防止のためには，教員の所有する USB メモリの利用を禁止した上で，学校側が用意した十分なセキュリティを保持している USB メモリを利用することが必要である．

学校の用意した USB メモリのセキュリティを保つため，暗号化仮想ドライブ作成ソフト TrueCrypt[2]を用い，USB メモリを暗号化仮想ドライブ化する． USB メモリの仮想ドライブ化解除に用いるパスワードを，英数字で構成された 128 字のランダムな文字列とし，定期的に更新する．以降，このパスワードを USB メモリパスワードとする．

ロバストなパスワードの管理を人間が行うのは現実的でない．USB メモリや教員の情報を記録したデータベースである USBDB から USB メモリパスワードを引き出し，USB メモリマウント用 WEB ページを媒介に自動入力する．

USB メモリマウント用 WEB ページの不正利用を防ぐため，正規利用者の固定 IP アドレス以外からのアクセスを拒否するとともに，ワンタイム･パスワードである WEB パスワードによる認証を行う．

3.2 システムの利用の流れ

USB メモリの貸出を希望する教員は，共用パソコン内にある USB メモリ管理アプリケーションを起動し，機能の 1 つである貸出申請を行う．USB メモリの管理責任者に USB メモリ貸出申請の許可を依頼し，管理責任者はアプリケーションの機能から貸出許可を実行する．貸出の際，申請した教員や USB メモリの情報などをデータベースに書き込み，学校における管理職全員に USB メモリの貸出報告メールを送信することで貸出情報の共有を行う．

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.

USB メモリを利用する際，仮想ドライブ化を解除するための専用の WEB ページで，貸出時に提示された WEB パスワードを用いて認証を行う．認証が通れば USB メモリの情報を保存しているデータベースより USB メモリのパスワードを引き出し，USB メモリのマウントを行う．WEB パスワードは，利用の度に更新され，データベースに登録してある利用者のメールアドレスに送信される．

USB メモリを返却する際には，返却する USB メモリを差し込んだ状態で USB メモリ管理アプリケーションの返却処理を起動する．アプリケーションは USB メモリのフォーマット，USB メモリの暗号化仮想ドライブ化，USB メモリパスワードの更新，更新した USB メモリパスワードの登録を行う．一連の動作完了後，利用者は USB メモリを管理者に返却する．

それぞれの処理の流れをフローチャートで示す(図 2).

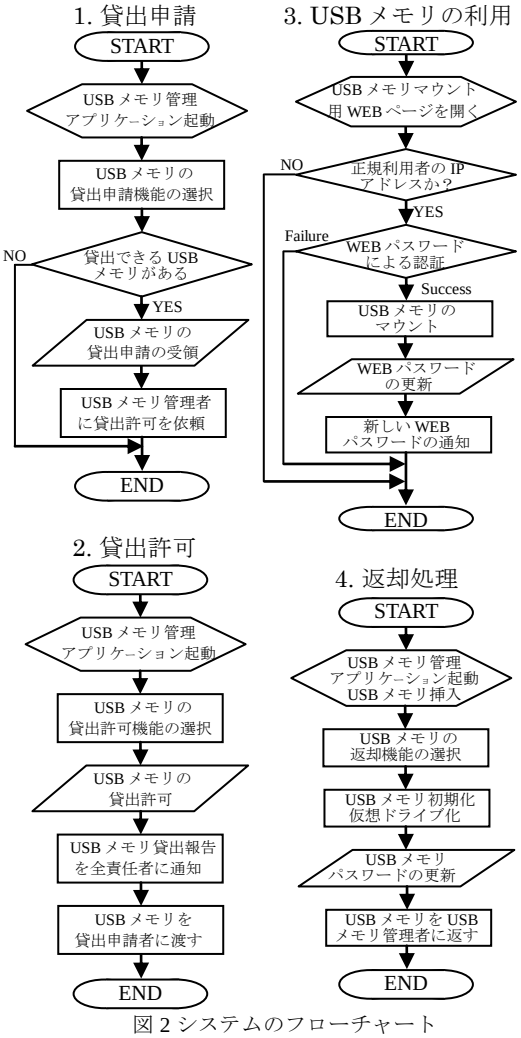


図 2 システムのフローチャート

3.3 USB メモリ管理アプリケーションの開発

USB メモリ管理アプリケーションの貸出申請，貸出許可，返却処理の機能の実装を完了している．

図 3 は USB メモリ管理アプリケーションで，USB メモリ管理者が貸出許可を行った際の画面である．この時点で学校の管理職全員に貸出報告メールが送信されている．

図 4 は USB メモリ管理アプリケーションで，USB メモリの利用者が返却処理を行った際の画面である．USB メモリをフォーマットし，新たな USB メモリパスワードを用い，TrueCrypt で再度暗号化仮想ドライブ化している．

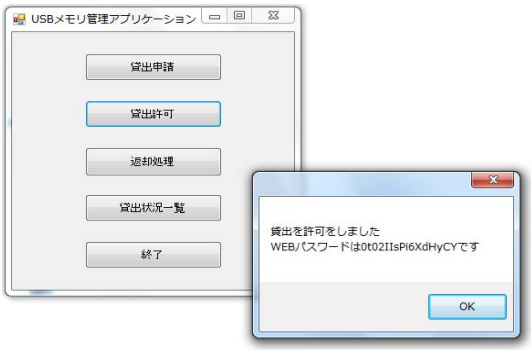


図 3 USB メモリ貸出許可

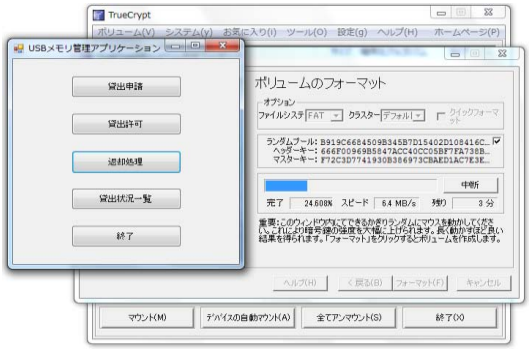


図 4 USB メモリ返却処理

4. 考察

3 章で列挙したシステムへの要件について考察を行う．

オープンソースの TrueCrypt を用いることで，安価で費用対効果があるという条件は満たされていると判断できる．ロバストな USB メモリパスワード，ワンタイム･パスワードである WEB パスワードを用いることで，十分なセキュリティが確保されており，紛失や盗難に遭った場合でも個人情報流出を防ぐことが可能と判断できる．私物の USB メモリを利用する理由は，2 章 3 節に記載した通りであり，USB メモリの貸出制度を周知させ，USB メモリの数を十分に用意することにより，私物の USB メモリの利用を防ぐことが可能と判断できる．

本システムへの神奈川県立総合教育センターの評価は「機能としてはこれで問題が無いように感じられる」「USB メモリ経由のウィルス被害も防げたらなおよい」などであった．

5. おわりに

本研究では，学校における USB メモリの利用実態や，学校で起きた生徒の個人情報流出事故の統計データを元に，学校における USB メモリの貸出システムの設計と，USB メモリ管理アプリケーションの実装を行った．

今後の課題としては，USB メモリマウント用 WEB ページの作成をし，システムを完成させることが第一である．また，教員の転勤や転居，昇進に対応するため，データベースに登録されている教員の情報の更新や削除を，USB メモリ管理アプリケーション上で行えるようにすることも課題として考えられる．

参考文献

[1]NPO 日本セキュリティネットワーク協会:「2009 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/2009.html

[2]TrueCrypt http://www.truecrypt.org/

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.