教育機関における情報漏えい事故の傾向と対策（2012 年版）

佐伯　勇

The recent trends in the information leakage incidents and the countermeasures against them at educational institutions（2012 edition）

SAEKI Isamu

Abstract : In this paper, I analyze the characteristics of personal information leakage incidents at educational institutions in the second and third quarters of 2012. As a result, I show that they should take countermeasures against the loss or the robbery of electronic devices such as USB memories to protect personal information at educational institutions. I also suggest the concrete methods to create and manage passwords by combining a master key and convention rules.

はじめに

筆者は，『教育機関における情報漏えい事故の傾向と対策』[1]において，情報セキュリティに特化したニュース専門メディア Security Next[2]で，2010 年 4 月から 9 月の半年間に報じられた個人情報漏えい事件・事故を分析し，教育機関における事件・事故の特徴を調査した。その結果，発生頻度が高く公になりやすい，つまり重要度の高い事件・事故の特徴が，媒体としては USB メモリ，原因としては紛失・盗難にあることを明らかにした。さらに，それらの事件・事故に対する対策として，業務への影響度や実現コストを勘案したうえで，セキュア USB メモリの導入について検討すべきであると提案した。

その 1 年後には，2011 年 4 月から 9 月の半年間の継続調査を行い，教育機関の情報漏えいリスクが相対的に高まっていること，教育機関の中でも高等教育機関の情報漏えい事件・事故が増加傾向にあること，教育機関における情報漏えい原因の約 9 割は紙や電子媒体の紛失・盗難によるものであること，電子媒体の約 7 割は USB メモリであることなどを明らかにした。これらの結果から，教育機関においては USB メモリをはじめとする電子媒体の紛失・盗難対策が最も急務であり，次いで紙媒体の紛失・盗難対策，操作ミス対策の順に検討すれば，効率の良い対策が実現できることを示した[3]。さらに，それぞれの重点項目について考えられる対策を，業務への影響度や実現コストを勘案しながら述べた。最優先で進めるべき，USB メモリの紛失・盗難対策としては，オンラインストレージの普及に伴い，PC やポータブルハードディスクを含めたあらゆるストレージに対応できる汎用的な手法を検討することを提案した。

それからさらに 1 年が経過したが，個人情報漏えいの事件・事故は相変わらず毎日のように報じられている。今年度も，東京工業大学，名古屋大学，広島大学など，日本を代表する大学において相次いで個人情報漏えいの事件・事故が発生している。

いったん個人情報漏えい事件・事故を起こせば，被害者に対する謝罪と補償，メディアへの対応などでダメージを受ける上に，信用が失墜して組織の存続に影響を及ぼしかねない。それぞれの組織の業務にとって重要な部分から，継続的に対策を行っていく必要がある。

この 1 年の間に，個人情報漏えい事件・事故の数，教育機関における事件・事故の特徴，および重要度の

高い対策は変化したのか。変化したとすれば対策はどうあるべきなのか。

本稿では昨年に引き続き，Security Next で 2012 年 4 月から 9 月の半年間に報じられた個人情報漏えい事件・事故を，過去 2 年間との比較を交えて分析する。2012 年の教育機関における事件・事故の特徴を調べることによって，発生頻度が高く公になりやすい，つまり重要度の高い媒体と原因を明らかにする。一方で，オンラインストレージの普及によって，将来的には電子媒体に特化したセキュリティ対策だけでは不十分となることを指摘し，汎用的な対策としてパスワードの作成と管理技術の啓蒙が重要であることを述べる。さらに，自分が忘れない文字列と独自のルールの組合せにより強固で忘れにくいパスワードを作成する方法を，具体例を示しながら説明する。

1　教育機関における情報漏えい事件・事故の傾向

1. 1　情報漏えい事件・事故件数の業種別比率

セキュリティ関連ニュースサイト Security Next で，2012 年 4 月から 9 月の半年間に報じられた個人情報漏えい事件・事故の総数は 190 件であり，昨年および一昨年の同時期には，それぞれ 208 件および 232 件であった。総数としては前年比で約 1 割ずつ減少しているが，1 日当たり 1 件以上の事件・事故が報じられている状況に変わりはない。

図 1 に，当該期間に報道された個人情報漏えい事件・事故件数の業種別比率を示す。図 1 から，幅広い業種で事件・事故が発生しており，個人情報漏えいのリスクが普遍的に存在していることが分かる。2012 年に着目すれば，事件・事故件数の多い業種は上位から順に，「公務」（16.8%），「教育，学習支援業」（15.8%），「金融業，保険業」（13.7%）であり，昨年および一昨年と同様に，上位 3 業種で約半数を占めている。上位 3 業種の占める割合は年々減少傾向にあり，他業種に広がりを見せるようになってきた。2011 年の 1 位「教育，学習支援業」と 2 位「公務」の順位が 2012 年には入れ替わっているが，相変わらず「教育，学習支援業」は個人情報漏えい事件・事故報道が多い業種となっている。なお，「公務」は中央官庁と地方自治体を，「教育，学習支援業」は，大学（大学病院，大学院を含む），短期大学，高等専門学校，専門学校，高等学校，中学校，小学校，幼稚園，学習塾を，「金融業，保険業」は銀行業，証券業，保険業を分類した。

1 位の「公務」と 3 位の「金融業，保険業」は，行政による監督・指導が効果を発揮しやすい分野であり，個人情報漏えい対策が推進されていると同時に，軽微な事件・事故であっても報告が徹底される傾向にある。一方，行政指導が不十分な「教育，学習支援業」は，報道の実数から推測される以上に情報漏えいリスクが高い業種であると言わざるを得ない。

1. 2　教育機関の内訳

図 2 に，事件・事故が報道された「教育，学習支援業」の内訳を示す。事件・事故件数の多い区分は上位から順に，「大学，短大」（56.7%），「高等学校」（16.7%），「中学校」および「小学校」（10.0%），（8%）であり，上位 4 区分で 9 割以上になる。文部科学省の平成 24 年度学校基本調査（速報）[4] によれば，教員数

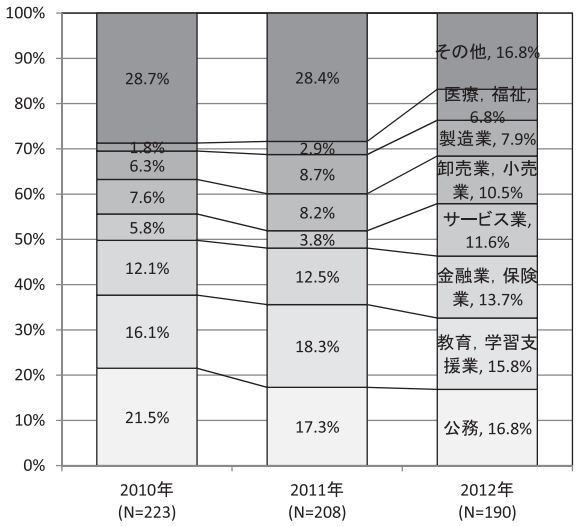

図 1　情報漏えい事件・事故件数の業種別比率

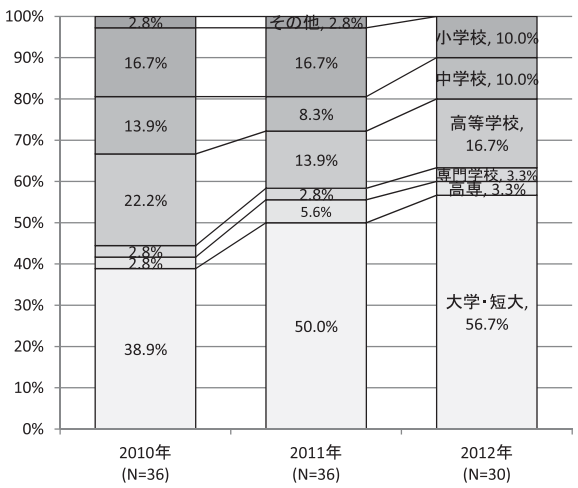

図 2　「教育，学習支援業」の内訳

（本務者）は，大学，短大が約 19 万人，高等学校が約 24 万人，中学校が約 25 万人，小学校が約 42 万人である。よって，教員数（本務者）10 万人あたりの事件・事故件数は，大学，短大が 8.9 件，高等学校が 2.1 件，中学校が 1.2 件，小学校が 0.7 件となり，上位 4 区分の中では，大学，短大における事件・事故の報道可能性が抜きん出て高いという傾向が見られる。サンプル数が少なく，統計的な結論を得ることは難しいが，大学，短大は前年比で最も割合が増加した区分であり，個人情報漏えい対策が難しく，事件・事故の報道数の増加に歯止めをかけることができない状況がうかがえる。

1. 3　教育機関における情報漏えい原因の特徴

図 3 に，全業種と教育機関における情報漏えい原因の比率を示す。左から順に，教育機関の 2010 年から 2012 年，全体の 2010 年から 2012 年のデータを表している。ここで，「紛失」は帳票類，PC, USB メモリ，携帯電話などの盗難や紛失を，「操作ミス」は機器操作の間違いや郵便物の封入間違いなどを，「設定ミス」はアクセス権の設定間違いやプログラムミスなどを，「P2P」はファイル共有ソフトによる流出を，「故意」は意図して情報を漏えいさせた事件を分類した。

図 3 から全業種では，個人情報漏えい事件・事故の約 3 分の 2 が紛失，約 2 割が操作ミス，約 1 割が設定ミスによるものであり，ファイル共有ソフトによる漏えいはわずかであることが分かる。2010 年から 2012 年の期間に，全体として大きな変化は見られないが，2012 年は新たに「故意」による情報漏えい事件が 3 件報じられた。内訳は Twitter による個人情報の投稿が 2 件，職員による個人情報売却が 1 件である。

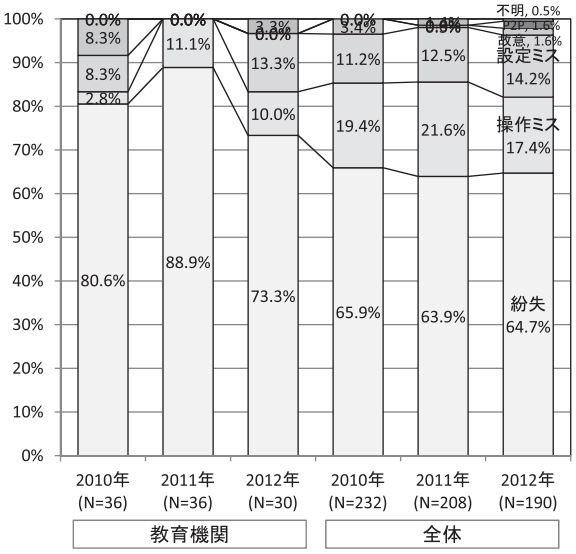

図 3　情報漏えい原因の比率

教育機関に限れば，紛失による事件・事故の割合は約 7 割から 9 割に達しており，全体と比較して紛失の割合が大きいという特徴が見られる。教育機関では一般的に情報の管理や持ち出しに関する規定や運用が甘く，個人情報保護に関する教育も不十分である。学校内，自宅，通勤途中での USB メモリ，PC，ハードディスク，書類などの紛失，盗難，置き忘れが多いため，教育機関としては，まず紛失対策を最優先に考え，安全性を高めるための業務手順の確立や教育を急ぐ必要がある。

2011 年には見られなかった，教育機関における「設定ミス」を原因とする情報漏えい事件・事故は，2012 年には 1 割程度発生している。これらの原因による事件・事故はもともと数が少なく，必ずしも傾向が変化したとは言えないが，サーバーの管理が不十分なために情報漏えいが発生する事案には引き続き警戒が必要であろう。

1. 4　教育機関における情報漏えい媒体の特徴

図 4 に，全業種と教育機関における情報漏えい媒体の比率を示す。図 3 と同様，左から順に，教育機関の 2010 年から 2012 年，全体の 2010 年から 2010 年のデータを表している。ここで，「紙」は書類，帳票類，名簿，手帳などを，「電子媒体」は PC, USB メモリ，ハードディスク，CD, DVD，携帯端末などを，「メール」は電子メールを，「サーバー」は Web やデータベースのサーバーを，「P2P」は Winny や Share などのファイル共有ソフトウェアを分類した。

図 4 から全業種では，約 4 割の情報漏えい事件・事

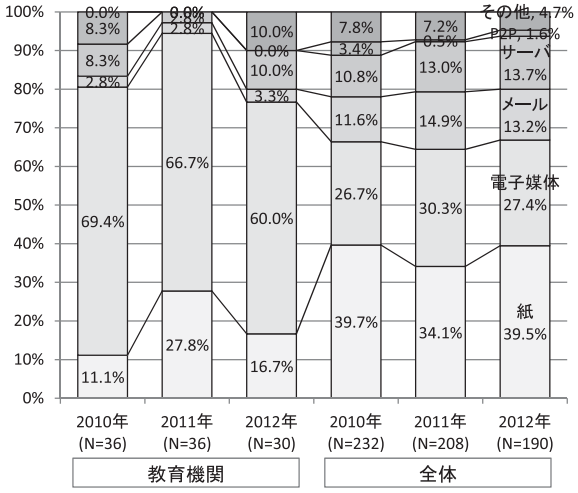

図 4　情報漏えい媒体の比率

故が紙媒体を，約 3 割が電子媒体を，それぞれ 1 割強がメールおよびサーバーを介したものであることが分かる。紙はどのような業種や職種であっても多用される媒体であるため，必然的に漏えいの可能性も高くなる。紙媒体によって漏えいした原因は，紛失，盗難，誤廃棄，誤送付といった「紛失」や「操作ミス」によるものが多い。ただし，大量の書類を持ち運ぶ頻度は低いため，電子媒体に比べると被害者数は少ないという傾向がある。

漏えい媒体比率第 2 位の電子媒体の多くは，USB メモリである。営業職など組織外での仕事が多い職種では，携帯型 PC を紛失する例もあるが，最近は USB メモリを介した漏えい事件・事故が増加している。USB メモリは，高速化・大容量化・低価格化しており，非常に小型で紛失しやすい媒体である。USB メモリによる漏えいが発生した業種は，教育，学習支援業，公務，医療，福祉，卸売業，小売業など広範囲に及ぶ。USB メモリをはじめとして，電子媒体は大量のデータを容易に持ち運べるという特徴があり，大規模な情報漏えいを招きやすいため，使用を制限したり禁じたりする組織が多い。にもかかわらず，電子媒体による個人情報漏えい事件・事故が後を絶たないという事実は，利便性の高い機器の使用を制限することがいかに難しいかを物語っている。今後はより重点的な対策が必要な分野であろう。

第 3 位のメールによる漏えいは，ほぼ全てが担当者の操作ミスによるものである。本来送信すべきアドレスとは異なるアドレスに送信した場合や，お互いに知り合いでない人々をメールの宛先欄または Cc 欄に列挙して送信したため，受信者間で宛先アドレスが閲覧可能になってしまった場合が多い。いずれの場合も流出先が特定可能であるため，それほど大きな問題にまで発展しないことが多く，特に後者の場合は漏えい情報がメールアドレスのみであるため，影響は軽微であるとも考えらえる。

第 4 位のサーバーによる漏えいは，約半数がサーバーの設定ミスかプログラムミスによるものである。報道では「不正アクセスによる」とされている場合でも，多くの場合は，サーバーを運営する側の設定ミスや管理ミスが不正アクセスを誘発している。2011 年はソニーや任天堂など大規模な Web サイトへの組織的攻撃による情報漏えい事件が報じられたが，2012 年は比較希少規模の Web サイトからの情報漏えい事件が数多く報じられている。小規模な組織では予算や人的資源不足のためにサーバー管理が疎かになる傾向にあり，明らかな管理ミスがなくとも漏えいが生じる可能性がある。業種としては，卸売業，小売業とサービス業が多く，インターネットを利用して顧客に直接サービスや商品を提供する組織では，サーバーを介した漏えいのリスクが高いと考えられる。

全業種の 2010 年から 2012 年の情報漏えい媒体の比率を比較しても，大きな変化は見られない。情報通信技術が発達してデジタルデータの情報セキュリティに注目が集まる中，紙媒体による情報漏えいが 4 割を維持していることには，十分な注意を要する。

次に，教育機関における情報漏えい媒体比率の特徴を述べたい。教育機関では，漏えい媒体の比率が全体とは大きく異なっている。紙媒体による漏えいは約 2 割で全体平均の約半分であるのに対し，約 6 割が電子媒体による漏えいである。メール，サーバー，P2P による漏えいは，上位 2 つの漏えい媒体と比較すると少ないことが分かる。

教育機関において紙媒体による漏えいが比較的少ない理由は，紙媒体を持ち運ぶ機会が少ないからだろう。教職員が紙媒体を携えて学生・生徒・児童の自宅や他校に訪問する場面は稀であり，成績処理などの業務を自宅に持ち帰る際には電子媒体を利用することが多いと考えられる。

一方で，教育機関における漏えい媒体の約 6 割を占める電子媒体は，その約 3 分の 2 が USB メモリで，残りの約 3 分の 1 が PC，ポータブルハードディスクおよび IC レコーダーである。USB メモリを介した漏えい事件・事故の約 6 割は教育機関で発生しており，小学校から大学まで比較的緩やかな情報管理体制のもとに，日常的に個人情報を持ち歩いて漏えいのリスクに晒している様子がうかがえる。データの持ち出しを一切禁止すると，夜遅くまでの残業や休日出勤を強いることになるため，データを持ち運ばなくても業務が円滑に遂行できる組織的・技術的支援を検討する必要がある。

教育機関におけるサーバーを介した漏えい事件・事故は，全て大学で発生している。高等教育機関ほどインターネットに接続したサーバーを利用して学務や教育を行っているため，件数が少ないとはいえ漏えいの危険性を認識しておく必要がある。

2012 年は，教育機関におけるファイル共有ソフトを介した個人情報漏えい事件・事故の報道は見られない。多くの教育機関では，ファイアウォールによって不要な通信を制限しているため，基本的には学校内でファイル共有ソフトを使用することはできない。しか

し，全体ではファイル共有ソフトによる情報漏えい事故が 3 件報じられており，予断を許さない状況であると考えられる。

教育機関では，メールを介した情報漏えいの割合が平均と比較して小さい。学生・生徒・児童が日々学校に通い，教室の中で直接コミュニケーションを取ることが主たる業務であるため，他業種よりメールの使用頻度が低くなることが要因であると考えられる。

教育機関の 2010 年から 2012 年の情報漏えい媒体の比率を比較すると，2011 年に紙媒体による情報漏えいが増加してメールやサーバーによる情報漏えいが減少したものの，2012 年には 2010 年と類似の分布を示している。この 2 年の間には情報漏えい媒体に関する大きな傾向の変化は見られないと言えよう。

1. 5　教育機関における情報漏えい対策の重点項目

ここで，教育機関における個人情報漏えい対策の重点項目をまとめたい。2010 年から 2 年間の情報漏えい事件・事故の原因には大きな変化が見られず，教育機関では，USB メモリをはじめとする電子媒体の紛失・盗難対策が最も急務である。

一方，事件・事故の報道数には表れない新たな傾向を指摘しておきたい。近年，データをインターネット上のサーバーに置くオンラインストレージサービスが急速に普及しており，USB メモリなどの電子記憶媒体は近い将来ほとんど使われなくなる可能性が高い。オンラインストレージはクラウドと呼ばれる仮想化されたサーバー群で管理されており，実際のデータがどの国のサーバーで保管されているか知ることは困難である。データの保全は各国の法律に従うため，業務上重要なファイルはクラウドシステムには置かないよう定めている組織も多い。まして，いつサービス内容を変更するか分からない無料のオンラインストレージサービスを業務に使用することは，一般的な企業では認められていない。しかし，大学など高等教育機関では，従来から USB メモリや PC によるデータの持ち出しについても厳しい制限を課してこなかったため，オンラインストレージサービスの利用を禁止することも難しい。そこで，これからの情報漏えい対策を検討する上では，USB メモリという個別の媒体に特化したものではなく，オンラインストレージサービスなどにも対応した汎用的な対策を考える必要がある。

オンラインストレージに保存するファイルの機密性は 2 つのパスワードによって守られる。1 つはサービス認証のためのパスワード，もう 1 つはファイル自体にかけられるパスワードである。USB メモリを使用する場合でも，セキュリティ対応型の USB メモリにパスワードを設定し，ファイルにもパスワードをかけておくことが望ましい。PC を持ち運ぶ場合でも，BIOS, OS，ファイルなど多段のパスワードを設定することがセキュリティの向上につながる。このような例から，汎用的なセキュリティ対策の要はパスワード管理であると考えられる。

そこで次項では，複雑ながら忘れにくいパスワードをいかに生成して管理するかについて，パスワードの破られ方を整理しながら論じていきたい。

2　パスワードの作成と管理の技術

パスワード破りには，大きく分けて 3 つの方法がある。

①推測による方法

身近な人物が，被害者の誕生日，家族やペットの名前など，パスワードに使用しそうな個人情報に関連する文字列を推測して破る方法。

②ツールによる方法

一般の辞書に掲載されている単語に加えて，パスワードとして設定されることが多い文字列が収められた，パスワード破り専用の辞書データを用いてパスワードを破る方法。

③流出したパスワードを利用する方法

①と②は不明なパスワードを発見する方法だが，最近はパスワードデータが流出する事件が相次いでいる。原因の多くは，Web サーバーの脆弱性を突いた不正アクセスだが，メールを使ってウイルスを送り込み，パスワードを盗み出す手口もある。

次に，これら 3 つの方法への対策について述べる。①は自分の個人情報に関わる文字列をパスワードとして利用しなければよい。②に対しては，辞書に掲載されている単語を避けて複雑なパスワードを設定することが必要になる。ところが，いくら複雑なパスワードを設定しても③のようにパスワード自体が流出してしまえば意味がなくなる。そこで，パスワードを使い回さず，定期的に変更することが重要になる。

一方で，パスワードの強度と作成・管理の負荷はトレードオフの関係にある。使用するサービスごとに，大文字･小文字･記号を混在させた長い文字列のパスワードを作成し，頻繁に変更しようとすると，パスワー

ドを覚えていることが難しくなり，結局理想的な方法は諦めて，安易な文字列のパスワードを長期間使い回すことになりかねない。実際に，流出したパスワードの中で最もよく利用されている文字列は，「123456」，「12345678」，「111111」，「password」，「abc 123」など単純なものが多い。

パスワード作成・管理の現実解については，勝村がパスワードの新常識[5]として次のような方法を提唱している。『できるだけ複雑な文字列をマスターキーとして作成する。その文字列に，サービスごとに異なる短い文字列を追加して，パスワードを作る。この方法なら，十分な強度を期待できるともに，比較的容易に新しいパスワードを生み出せるだろう。』以下では具体例を使って説明したい。

まず，座右の銘や好きな詩や歌詞など自分が忘れない文章を独自のルールで変換し，無意味な文字列を生成する。例えば，水戸黄門の主題歌「あゝ人生に涙あり」を使用してみよう。「人生楽ありゃ苦もあるさ…」というフレーズから，子音だけを抽出して「jsrkrykmrs」としたり，1 文字おきに抽出して「jnerkaykmaua」としたり，文節の最初の文字を抽出して「jrknand」とする。次に，文字列の一部を大文字にしたり，記号や数字に置き換えたり，挿入したりして強度を増す。例えば，4 小節ごとの先頭を大文字にして「JrkNand」としたり，さらに「k」を「|<」，「a」を「@」として「Jr|<N@nd」として，マスターキーを作成する。

マスターキーができたら，サービスに関連する短い文字列を加えてそれぞれ異なるパスワードを作成する。サービス名そのものを文字列として使用すればパスワードの類推が可能になるので，独自のルールによってサービス名を自分なりの文字列に変換することが重要だ。例えば，「Dropbox」のパスワードを作成する場合，「o」を「0」に，「x」を「><」にして「D0r0pb0><」としたり，「落ち箱」と日本語に変換して「Ochi-Bako」としたりした後に，マスターキーと組み合わせる。その結果，「Jr|<D0r0pb0xN@nd」や「OchiJr|<N@ndBako」のような Dropbox 専用のパスワードが作成できる。

作成したパスワードの強度を確認するには，日本マイクロソフトが運営するパスワードチェッカー[6]が利用できる。文字列を入力すると，パスワードの強度を 4 段階で表示する。入力した文字列はサーバーに送信されることはない。本稿で Dropbox 用に作成したパスワードの強度は，共に上から 2 段階目の「強い」であった。

自分が忘れない文字列と変換ルールの組合せで強固なパスワードを作成し，変換ルールを変更することで定期的なパスワード変更も可能になる。

ま　と　め

本稿では，2012 年 4 月から 9 月の半年間に報じられた個人情報漏えい事件・事故の特徴について，昨年および一昨年の同期間との比較を行いながら，教育機関を中心に分析した。その結果，教育機関の情報漏えいリスクが高止まりしていること，教育機関の中でも大学・短大の情報漏えい事件・事故が増加傾向にあること，教育機関における情報漏えい原因の約 6 割は紙や電子媒体の紛失・盗難によるものであること，電子媒体の約 3 分の 2 は USB メモリであることなどを明らかにした。これらの結果から，教育機関においては USB メモリをはじめとする電子媒体の紛失・盗難対策が引き続き最重要であることを示した。

一方で，オンラインストレージの普及によって，将来的には電子媒体に特化したセキュリティ対策だけでは不十分となることを指摘し，汎用的な対策としてパスワードの作成と管理技術の啓蒙が重要であることを述べた。さらに，自分が忘れない文字列と独自のルールの組合せにより強固で忘れにくいパスワードを作成する方法を，具体例を示しながら説明した。

本学においても，ストレージ環境の変化に先んじて実質的な情報セキュリティ水準を高めるため，教職員に対するパスワード作成・管理技術を始めとした実践的な講習会を定期的に開催し，啓蒙活動を推進していきたい。

参 考 文 献

1）佐伯勇，2011，『教育機関における情報漏えい事故の傾向と対策』，甲南女子大学研究紀要人間科学編，Vol.47, pp.89–94.
2）Security NEXT, http : //www.security−next.com/.
3）佐伯勇，2012，『教育機関における情報漏えい事故の傾向と対策（2011 年版）』，甲南女子大学研究紀要人間科学編，Vol.48, pp.97−102.
4）文部科学省，2012，『学校基本調査－平成 24 年度（速報）結果の概要－』，http : //www.mext.go.jp/b_menu/houdou/24/08/attach/1324865.htm,（2012 年 11 月 15 日アクセス）.
5）勝村幸博，2012，『パスワードの新常識』，日経パソコン 2012 年 1 月 9 日号，pp.46–55.
6）日本マイクロソフト，『パスワードチェッカー』，https : //www.microsoft.com/ja−jp/security/pc−security/pass-

word−checker.aspx.
7）土居範久監修，独立行政法人情報処理推進機構，2009,『情報セキュリティ教本　改訂版　組織の情報セキュリティ対策実践の手引き』，実教出版.
8）独立行政法人情報処理推進機構，2009,『情報セキュリティ読本　三訂版　IT 時代の危機管理入門』，実教出版.