教育機関における情報漏えい事故の傾向と対策（2011 年版）

佐伯　勇

Recent trends in information leakage incidents in educational institutions and their countermeasures（2011 edition）

SAEKI Isamu

Abstract: In this study, I analyze the characteristics of personal information leakage incidents in educational institutions in the second and third quarters of 2011. As a result, I show that educational institutions should take countermeasures against lost or stolen electronic devices and records as well as operational errors in order to protect personal information. In addition, I discuss concrete methods for employing countermeasures by considering the impact on business flow and implementation costs.

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。

それから約 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。今年に入ってからでも，東京大学，九州大学，早稲田大学など，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・事故が発生した。

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 2011 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，2010 年との比較を交えて分析する。2011 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。さらに，それらの事件・事故に対する対策を具体的に提案する。

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，2011 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 208 件であり，前年同時期には 232 件であった。総数としては前年比で 1 割ほど

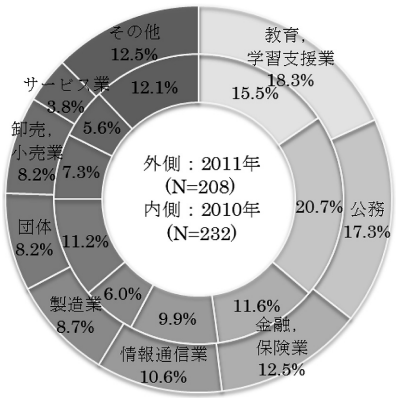

図 1　情報漏えい事件・事故件数の業種別比率

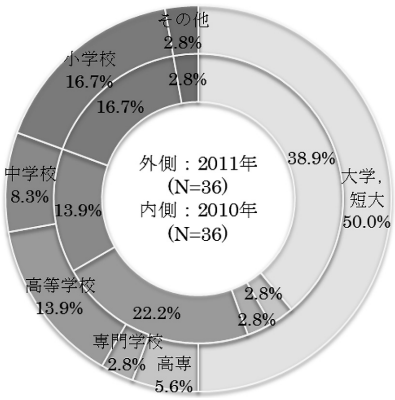

図 2　「教育，学習支援業」の内訳

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。2011 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，「教育，学習支援業」（18%），「公務」（17%），「金融業，保険業」（13%）であり，2010 年と同様に，上位 3 業種で約半数を占めている。ただし，2010 年の 1 位「公務」と 2 位「教育，学習支援業」の順位が 2011 年には入れ替わっており，今や「教育，学習支援業」は最も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。

比率が減少した業種は，「公務」と「団体」である。これらの業種は，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徐々に浸透している可能性がある。一方，「公務」や「団体」と比較して行政指導が不十分な「教育，学習支援業」は，実数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」（50%），「小学校」（17%），「高等学校」（14%），「中学校」（8%）であり，上位 4 区分で 9 割近くになる。文部科学省の平成 23 年度学校基本調査（速報）[3] によれば，教職員数（本務者）は，大学，短大が約 40 万人，高等学校が約 27 万人，中学校が約 27 万人，小学校が約 47 万人である。よって，教職員数（本務者）10 万人あたりの事件・事故件数は，大学，短大が 4.5 件，高等学校が 1.8 件，中学校が 1.1 件，小学校が 1.2 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高いという傾向がみられる。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，前年比で割合が増加した区分は，大学，短大と高専の高等教育機関であり，最も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。上から順に，全体の 2011 年と 2010 年，教育機関の 2011 年と 2010 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分類した。

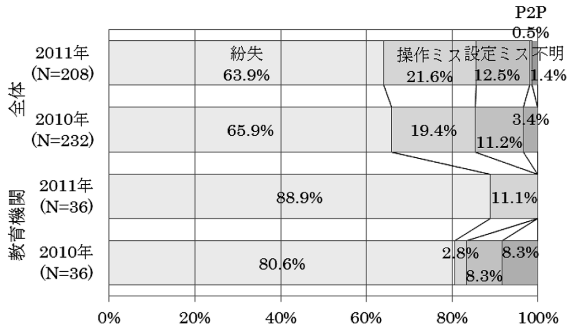

図 3　情報漏えい原因の比率

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 1 割未満であることが分かる。2011 年と 2010 年を比較すると，全体として大きな差はないものの，ファイル共有ソフトによる情報漏えいが減少傾向にあることが分かる。ファイル共有ソフトが情報漏えいのリスクを高めることは周知の事実であり，現在ではほとんどの組織において業務用 PC はもちろん自宅用 PC での使用を禁止している。2010 年 1 月に施行された著作権法の改正により，権利者に無断でアップロードされているファイルを，違法と知りながらダウンロードする行為が違法となったことや，ファイル共有ソフトを用いた著作権侵害を警察が厳格に摘発するようになったことも，ファイル共有ソフトの使用を抑制している一因であろう。しかし，ファイル共有ソフトによる漏えい以外の場合は，担当者のヒューマンエラーに起因する事件・事故がほとんどであり，情報セキュリティに対する意識の低さや技術の未熟さが主な発生要因である。

教育機関に限れば，紛失による事件・事故の割合は約 8 割から 9 割に達している。他業種と比較して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 年は，教育機関における「設定ミス」と「P2P」を原因とする情報漏えい事件・事故が報じられていない。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。

ここでは，教育機関の情報漏えい事件・事故原因のほとんどが「紛失」や「盗難」であることは明らかであり，紛失対策を最優先にすることにより，効果の高い対応が可能となることを改めて指摘しておきたい。

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，上から順に，全体の 2011 年と 2010 年，教育機関の 2011 年と 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」は Web やデータベースのサーバを，「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。

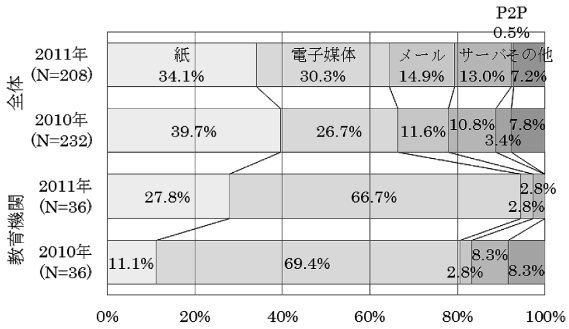

図 4　情報漏えい媒体の比率

図 4 から全業種では，約 3 分の 1 の情報漏えい事件・事故が紙媒体を，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・事故が急増している。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，金融業，保険業，情報通信業，製造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 位のサーバによる漏えいは，約半数がサーバ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。ただし，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も散見されるようになり，明確な管理ミスがなくとも漏えいが生じる可能性も示唆されている。業種としては，情報通信業と製造業が多く，インターネットを利用して顧客に直接サービスを提供する組織では，サーバを介した漏えいのリスクが高いと考えられる。

全業種の 2011 年と 2010 年の情報漏えい媒体の比率を比較すると，紙媒体が減少し，電子媒体，メール，サーバによる漏えいが増加していることが分かる。全体としては，紙媒体よりも電子媒体等を利用する機会が増加しており，電子媒体等による情報漏えい対策の重要性が高まっていると考えられる。

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 3 割で全体平均とも大きな差がないのに対し，約 3 分の 2 が電子媒体による漏えいである。メール，サーバ，P2P による漏えいは，上位 2 つの漏えい媒体と比較すると非常に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，紙媒体を持ち運ぶこと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機会は稀であり，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 3 分の 2 を占める電子媒体は，その約 7 割が USB メモリで，残りの約 3 割が PC とポータブルハードディスクである。USB メモリを介した漏えい事件・事故の約 7 割が教育機関で発生しており，幼稚園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を利用して学務や教育を行っているため，件数が少なくても漏えいの危険性を認識しておく必要がある。

2011 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。前述した法律改正や取り締まりの強化により，今後も引き続き少ない件数で推移するか否か，動向を見守っていきたい。

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 2011 年と 2010 年の情報漏えい媒体の比率を比較すると，紙媒体の情報漏えい事件・事故が 2 倍以上増加している。1 年の間に紙媒体を使用する頻度が高まったとも考えられず，全体平均を超えているわけでもないため，2010 年の数値が偶然小さかったと考えられる。具体的な事件・事故内容を調べると，単純な紛失や車上荒らしなどが大半で，1 年間に大きく傾向が変化したとは考えられない。

1. 5. 教育機関における情報漏えい対策の重点項目

以上から，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，サーバ管理と操作の適正化，ファイル共有ソフト利用の禁止の順に対策を検討すれば，効率の良い対策が実現できると考えられた。2011 年は，電子媒体の紛失・盗難対策，紙媒体の紛失・盗難対策の順に対策を進めればよいことに変わりはないが，操作ミス対策の重要性が増してきたと判断できる。

2　教育機関における情報漏えい対策

本節では，前節で述べた教育機関における個人情報漏えい対策の優先事項について，業務への影響度や実

現コストを勘案しながら解説していきたい。

2. 1. 電子媒体の紛失・盗難対策

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，USB メモリ等の電子媒体の紛失・盗難対策には，「電子媒体によるデータの持ち出しを一切禁止する」方法と，「データの持ち出しは許可するが漏えい防止の対策を取る」方法とがあることを示した。また，前者は，セキュリティポリシーとしては設定可能だが，実際の運用は極めて難しいこと，後者は，紛失や盗難があることを前提に上司の許可や記録を取り，第三者が内容を読み取れないように暗号化することにより実現できることを述べた。具体的には，PC であれば，BIOS によるパスワード起動制限，OS のログイン制御，NTFS などの OS によるハードディスク暗号化を組み合わせる方法があり，USB メモリであれば，パスワードや暗号化により内部のデータを保護する仕組みを備えた製品（セキュア USB メモリ）を選ぶ方法があることを示した。

セキュア USB メモリには，指紋認証タイプとソフトウェアまたはハードウェア暗号化タイプとがある。前者は操作が簡易であるものの，認証ミスを防ぐことが不可能であり，後者は完全な認証が可能であるものの，パスワードを忘れた場合の復旧が困難である。管理者パスワードを別途用意し，使用者がパスワードを忘れた場合でも管理者が解除できる機能を持った製品もあるが，2 GB モデルで 1 万円強（2011 年 10 月現在）と非常に高価であり，全構成員への一括導入には相当の費用が必要になる。

一方，データを PC 間で共有する方法としてオンラインストレージが普及し始め，いずれは USB メモリにとって代わる可能性が高い。オンラインストレージとは，インターネット経由でファイルをアップロードしておき，インターネットに接続された機器からダウンロードできるようにファイルを保管するサービスである。PC の特定のフォルダにファイルを置いておけば，オンラインストレージと自動的に同期する機能もあり，Linux，スマートフォン，タブレット端末などでも使用できるため，データを持ち運ぶ必要がなくなるのである。情報漏えい対策という視点から考えれば，USB メモリの紛失・盗難対策だけではなく，PC 本体やポータブルハードディスクなどの紛失・盗難，オンラインストレージによる情報漏えいなど，多様なストレージに対応しうる方法を検討する必要がある。

そこで，全てのストレージに対して汎用的に使用できる方法の 1 つとして，オープンソースの暗号化仮想ドライブソフト TrueCrypt[4]の導入を提案する。TrueCrypt は，暗号化された仮想ディスクを作成・利用する無償のソフトウェアである。メリットとしては，ストレージを選ばず，MacOS にも対応し，外出先 PC へのインストールの必要がなく，偽隠しボリューム（外殻）の中に本当の隠しボリュームが作成できるという特徴が挙げられる。デメリットとしては，設定には多少の技術的知識が必要なため，構成員全員に設定作業をさせることは困難であることや，フリーソフトなのでサポートがないことが挙げられる。しかし，低コストでどのようなストレージでも対応できる暗号化ソリューションとして，今後運用試験を行っていきたいと考えている。

2. 2. 紙媒体の紛失・盗難対策

『教育機関における情報漏えい事故の傾向と対策』で述べたとおり，紙媒体の紛失・盗難対策は，伝統的な手段に頼るほかない。どのような情報資産があるか把握しておくこと，書類は整理をして鍵をかけた場所に保管しておくこと，書類の閲覧やコピーには管理者の許可を得て誰がどの情報にアクセスしたかを記録しておくことなど，基本的な管理手法を徹底することに尽きるのである。

2. 3. 操作ミス対策

教育機関で発生した操作ミス関連の主な情報漏えい事件・事故は，メールの誤送信とサーバへの不適切なアップロードであった。メールの誤送信に対しては，全構成員への教育と，現場での複数人によるチェックを徹底すれば防げるものと考えられる。サーバへの不適切なアップロードについては，サーバにアクセスするだけの知識を持っており，実際にファイルをアップロードしなければならない，あるいはしたいと考えている構成員を特定し，このような構成員を対象に定期的に研修会を開催すれば，意識の向上を図ることができるだろう。

今回の調査では事例が見つからなかったが，サーバの利用者ではなく管理者のミスで情報漏えいする場合も考えられる。組織の中核システムに管理者としてアクセスする教職員に対しても，継続的な研修が不可欠であろう。

ま　と　め

本稿では，2011 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，前年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。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。

本学においても，本稿で明らかにした重点対策項目を考慮して，個人情報漏えいの技術的対策や教職員に対する啓もう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）文部科学省，2010，『学校基本調査－平成 23 年度（速報）結果の概要－』，http : //www.mext.go.jp/b_menu/toukei/chousa 01/kihon/kekka/k_detail/1309148.htm,（2011 年 10 月 23 日アクセス）.
4）True Crypt, http : //www.truecrypt.org/.
5）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.
6）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.