教育機関における情報漏えい事故の傾向と対策

佐伯　勇

Recent Trends in Information Leakage Incidents and Countermeasures Against Information Leakage in Educational Institutions

SAEKI Isamu

Abstract : In this paper, I analyze the characteristics of personal information leakage incidents in educational institutions in the second and third quarters of 2010. As a result, I show that they should take countermeasures against lost or stolen electronic devices and papers, improper managements of server computers, and use of file-sharing software to protect personal information in educational institutions. I also mention the concrete methods to realize key points of countermeasures taking into account the impact upon business flow and implementation costs.

はじめに

ICT（情報コミュニケーション技術）の進展に伴い，個人情報保護の重要性が一層高まっている。業務を効率化するため各種の書類や帳票がディジタル化されると，データの蓄積，改変，コピー，転送などが容易に行えるようになった。今では多くの組織で，アルバイトや非正規の職員にも一人一台 PC を貸与し，インターネットや組織内ネットワークを介して日常的に情報共有や交換が行われている。USB フラッシュメモリ，ポータブルハードディスク，携帯端末をはじめ，持ち運び可能な大容量の媒体が普及し，個人情報が頻繁に持ち運ばれ，高速の回線で瞬時に世界を駆け巡る時代になった。一方，ディジタル化によりペーパーレス時代を迎えたわけではなく，むしろ高速かつ低価格のプリンタが普及したことにより大量の書類が生まれ，日々持ち運ばれ廃棄されるようになった。

日本ネットワークセキュリティ協会によれば，2009 年には 1539 件の個人情報漏えい事件・事故が報道され，過去最高の件数を記録した[1]。単純平均すれば一日 4 件以上の報道があったことになるが，その裏には公表されない案件が多数存在している。

教育機関には，個人を特定可能な情報が書類やディジタルデータの形で大量に保存されている。在学生（生徒，児童），卒業生，受験生，研究者，教員，職員などの構成員や関係者のマスターファイル，成績，健康診断記録，相談記録，申請書，給与，人事評価など，数多くの個人情報が日常的に業務処理されている。これらのデータ管理が不適切だったために，個人情報が外部に漏えいする事故が後を絶たない。

この背景には対策の難しさがある。個人情報閲覧の制限といった業務手順の厳格化をはじめ，適切なアクセス権の設定，データの暗号化，個人情報を扱うパソコンの隔離，入退室管理を含むアクセス記録など，実施すべき対策は多岐にわたる。しかも個人情報はあらゆる部門で使用されているので，組織全体での取り組みが不可欠となる。

とはいえ，対策が難しいからといって放置するわけにはいかない。いったん情報漏えい事件・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。

重要な対策を特定するためには，日本ネットワークセキュリティ協会の「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」における，情報漏え

い事件・事故の分析が参考になる。しかし，一般企業とは事情の異なる教育機関では，情報漏えい事件・事故の傾向も全業種の平均とは異なっているのではないだろうか。

そこで本稿では，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事件・事故の特徴を明らかにする。さらに，それらの事件・事故に対する対策を，業務への影響度や実現コストを勘案しながら述べる。

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，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・事故の総数は236件である。この中には同一事件・事故の続報が4件含まれており，実質的な件数は232件となる。

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。事件・事故件数の多い業種は上位から順に，「公務」（21%），「教育，学習支援業」（15%），「金融業，保険業」（12%）であり，上位3業種で約半数を占めている。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（短期大学，大学病院，大学院を含む），高等専門学校，専門学校，高等学校，中学校，小学校，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。

「公務」と「金融業，保険業」は個人情報保護に関する行政指導が徹底している業種であり，他の業種では非公表とするような事案であっても公表することが多い。したがって，これらの業種における事件・事故件数が多いからといって，直ちにリスクが高いと判断することはできない。一方，「公務」や「金融業，保険業」と比較して行政指導が不十分であるにも関わらず，「教育，学習支援業」は事件・事故件数の業種別比率で第2位を占めている。実質的には，「教育，学習支援業」は情報漏えいリスクが非常に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」（39%），「高等学校」（22%），「小学校」（16%），「中学校」（14%）であり，上位4区分で9割を超える。文部科学省の平成22年度学校基本調査[3]によれば，教職員数（本務者）は，大学（短期大学を含む）が約39万人，高等学校が約29万人，中学校が約14万人，小学校が約59万人である。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（短期大学を含む）が3.6件，高等学校が2.8件，中学校が3.6件，小学校が1.2件となり，上位4区分の中では，大学（短期大学を含む）と中学校における事件・事故の発生確率が高いという傾向がみられる。

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。同心円の外側が全体を，内側が教育機

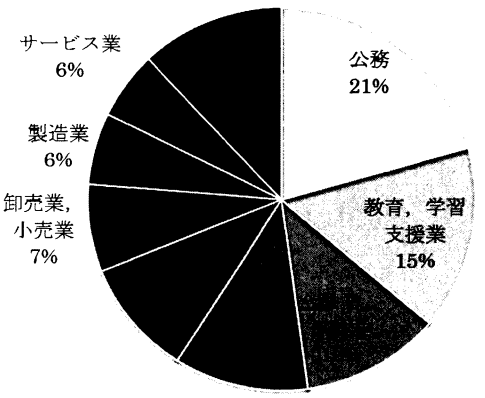

図1　情報漏えい事件・事故件数の業種別比率（N＝232）

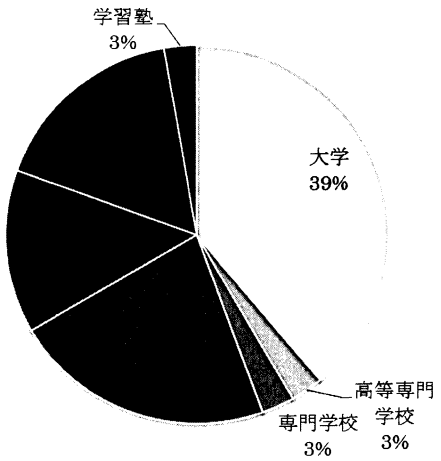

図2　「教育，学習支援業」の内訳（N＝36）

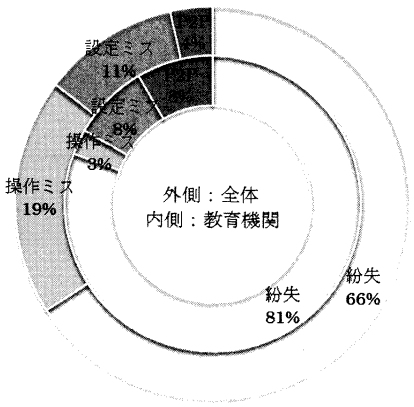

図3　情報漏えい原因の比率（N＝232, 36）

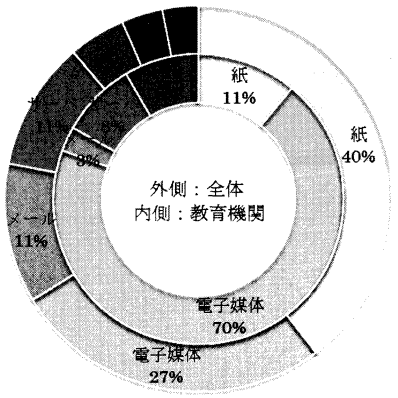

図4　情報漏えい媒体の比率（N＝232, 36）

関を表している。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。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 での使用を禁止している。にもかかわらず，ファイル共有ソフトを介した個人情報の漏えいが根絶されていないということは，漏えいを誘発した本人がリスクを承知の上でファイル共有ソフトを利用し，結果的に事件・事故を発生させたということになるだろう。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と推測できる。

教育機関に限れば，紛失による事件・事故の割合は約８割に達している。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。

全体と比較すると，教育機関ではファイル共有ソフトによる情報漏えいも多い。ファイル共有ソフトでは，ダウンロード時に経由した PC 全てにデータが保存されるため，一度漏えいしたデータを完全に回収することは極めて困難である。このような特性に着目した悪意のあるプログラマが「暴露ウイルス」と呼ばれる，ファイル共有ネットワーク上で情報漏えいを引き起こす不正プログラムを広めている。ファイル共有ソフトを利用している限り常に高い情報漏えいリスクにされていることを十分に認識し，決してファイル共有ソフトを使わないことが重要である。

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，同心円の外側と内側にそれぞれ，全業種と教育機関のデータを示している。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，「郵便」は郵便物を，「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・事故が紙媒体を，約３割が電子媒体を，それぞれ約１割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 を紛失する場合もあるが，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・大容量・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，団体，医療，福祉，運輸業，郵便業であった。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。上述した業種は，電子媒体による内部情報の持ち出しに対する規制が比較的少ないと考えられる。

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。

同率第3位のサーバによる漏えいは，8割以上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」とされていることもあるが，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。業種としては，卸売業，小売業，サービス業，情報通信業が多く，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。

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1割にとどまり，約7割が電子媒体による漏えいである。サーバを介した漏えいは約1割で全体と大差ないが，P2Pによる漏えいも約1割であり無視できない媒体になっている。

教育機関において紙媒体による漏えいが少ない理由は，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7割を占める電子媒体は，その約9割がUSBメモリで，約1割がPCである。USBメモリを介した漏えい事件・事故の実に約6割が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を介した3件の漏えい事件・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，漏えいの危険性が高まっているのだろう。

ファイル共有ソフトを介した漏えいの約4割は教育機関で発生している。多く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。よって，自宅に持ち帰った業務用のPCか，個人使用のPCにファイル共有ソフトをインストールしている可能性が高い。しかも一般的には，ファイル共有ソフトによる情報漏えいは，ソフトをインストールし，共有されているファイルをダウンロードして実行した結果発生することが多い。家族で共有しているPCに子供がファイル共有ソフトをインストールしていることを知らずに，親が仕事のデータを持ち帰って漏えいする場合もあるが，ファイル共有ソフトを介した漏えいは，当事者がリスクの高い行為を能動的に行っているという点で，他の媒体による漏えいよりも当事者の責任が問われやすいのである。

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。

1.5　教育機関における情報漏えい対策の重点項目

以上をまとめると，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，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

USB メモリ等の電子媒体の紛失・盗難対策は，「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」方法とに分けられる。

「電子媒体によるデータの持ち出しを禁止する」方法は，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。USB ポートや書き込み可能な光学ドライブの機能を排した特殊な PC を教職員に配布し，それ以外の PC を学内ネットワークに接続することを認めず，個人の PC を業務に利用することを禁止すれば，電子媒体によるデータの持ち出しはできなくなる。さらにクラウドコンピューティングの技術を利用して，PC の処理やデータ保存機能をデータセンターに移管し，手元の PC からデータセンターの PC 機能の画面を呼び出して使用させれば，学校の内外で仮想的な業務用 PC を使った業務を行えるようになり，原理的には個人情報を保存した電子媒体を持ち運ぶ必要がなくなる[4,5]。しかしこのような方法を取ろうとすると，業務手順の全面的見直しに関わる人的負担とシステム移行の経済的負担が発生するうえ，学外の組織とのデータ交換のために電子媒体の読み書きを例外的に許可せざるを得ず，結果的には個人情報がインターネット上のデータ保管サービスや電子メールで飛び交うという事態を招きかねない。

一方，「電子媒体による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。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る。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）を選べばよい。通常の USB メモリと比べて高価であるが，組織から貸与する形でセキュア USB メモリを提供すれば，紛失・盗難による情報漏えいをある程度防げるのではないだろうか。

2.2　紙媒体の紛失・盗難対策

第 2.1 節で述べたとおり，認証，暗号化，ファイアウォール，メール・Web フィルタリングなど，コストをかけて様々な技術を組み合わせれば，ディジタルデータの情報漏えい対策は実現可能である。しかし，そのような技術を応用しづらい紙媒体に対して，高度な情報漏えい対策を実現することは困難である。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　ファイル共有ソフト対策

情報処理推進機構によれば，ファイル共有ソフトからの情報漏えいを防ぐには，次のような対策が考えられ，それらを組み合わせて実施することが有効とされている[6,7]。

(1) 職場のパソコンだけでなく，自宅のパソコンにもファイル共有ソフトをインストールしない。
(2) 職場のパソコンに許可なくソフトウェアを導入しない，または，できないようにする。
(3) 職場のネットワークに，私有パソコンを接続しない，または，できないようにする。
(4) 自宅に業務データを持ち帰らない。
(5) 職場のパソコンから USB メモリや CD 等の媒体に情報をコピーしない，または，できないようにする。
(6) 漏えいして困る情報をメールで送らない，または，送れないようにする。
(7) ウイルス対策ソフトを導入し，最新のパターンファイルで常に監視する。
(8) 不審なファイルは開かない。

これらの対策の中で，(7) は費用をかければ比較的容易に実現が可能であり，(1) と (8) は教職員に対する教育によって実現に向けて努力することができるだろうが，特に大学のような拘束力の弱い組織では，それ以外の対策は実現が難しいのではないだろうか。禁止規定を作成し注意喚起を継続していくことで教職員の意識を向上させる以外に，現実的な選択肢はないように思われる。

2.4　サーバ管理と操作の適正化

教育機関で発生したサーバ関連の 3 件の情報漏えい事件・事故は，全て大学で発生している。いずれの場合も，教職員がアップロードしたファイルのアクセス管理が不十分なため，個人情報が外部から閲覧可能な状態になって放置されていた。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

る教職員の数はそう多くはなく，個人を特定可能であろう。このような教職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は，継続的な研修が不可欠であろう。

ま　と　め

本稿では，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・事故の特徴について，教育機関を中心に分析した。その結果，教育機関は情報漏えいリスクの高い業種であること，教育機関における情報漏えい原因の約8割は紙や電子媒体の紛失・盗難によるものであること，電子媒体による情報漏えい件数は紙媒体による漏えい件数の約7倍に達していること，電子媒体の約9割はUSBメモリであること，教育機関ではファイル共有ソフトによる情報漏えいの可能性が全体平均よりも高い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，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。

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）日本ネットワークセキュリティ協会，2010，『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）Security NEXT, http : //www.security-next.com/.
3）文部科学省，2010，『学校基本調査』，http : //www.mext.go.jp/b_menu/toukei/chousa 01/kihon/1267995.htm.
4）井上春樹，他3名，2010，『クラウドコンピューティングの全面適用とその効果』，財団法人私立大学情報教育協会平成22年度教育改革ICT戦略大会予稿集，pp.127-132.
5）井上春樹，他6名，2010，『クラウドコンピューティング全面適用のインパクト』，静岡学術出版.
6）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.
7）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　改訂版　IT時代の危機管理入門』，実教出版.