

教育機関における情報漏えい事故の 傾向と対策（2013 年版）

佐 伯 勇

The Recent Trends in the Information Leakage Incidents and the Countermeasures Against them at Educational Institutions (2013 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 2013. As a result, I show that they should take countermeasures against the loss or the robbery of electronic devices such as USB memories and PCs to protect personal information at educational institutions. I also suggest that the management of servers, online storage services, and cloud services should be exactly and efficiently performed.

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 Next²⁾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³⁾。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。

翌年には、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。

さらにその翌年には、2012 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⁴⁾。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。

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、京都大学、名古屋大学、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 2013 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 3 年間との比較を交えて分析する。2013 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。

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 2013 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 188 件であり、1 年前、2 年前および 3 年前の同時期には、それぞれ 190 件、208 件および 232 件であった。総数としては前年比で約 1 割ずつ減少してきたが、今年度は減少の速度が低下している。また、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。

2013 年に着目すれば、事件・事故件数の多い業種

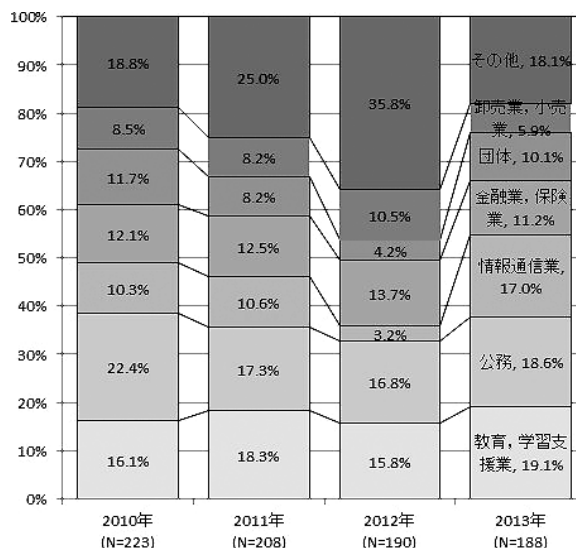


図 1 情報漏えい事件・事故件数の業種別比率

は上位から順に、「教育, 学習支援業」(19.1%), 「公務」(18.6%), 「情報通信業」(17.0%) であり, 上位 3 業種で半数以上を占めている。昨年度までは上位 3 業種の占める割合が減少傾向にあり, 他業種に広がりを見せていたが, 今年度は逆に業種の偏りが大きくなった。「教育, 学習支援業」と「公務」は 4 年間常に 1 位と 2 位を占めているが, 2013 年には不正アクセスの増えた「情報通信業」が第 3 位に躍り出ている。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, 「情報通信業」は通信業, 放送業, 情報サービス業, インターネット付随サービス業, 映像・音声・文字情報制作業を分類した。

2 位の「公務」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。2013 年において事件・事故報道数の多い区分は上位から順に, 「大学, 短大」(52.8%), 「小学校」(16.7%), 「高校」および「中学校」(それぞれ 8.3%) であり, 上位 4 区分で約 9 割を占める。文部科学省の平成 25 年度学校基本調査 (速報)⁹⁾ によれば, 教員数 (本務者) は, 大学, 短大が約 19

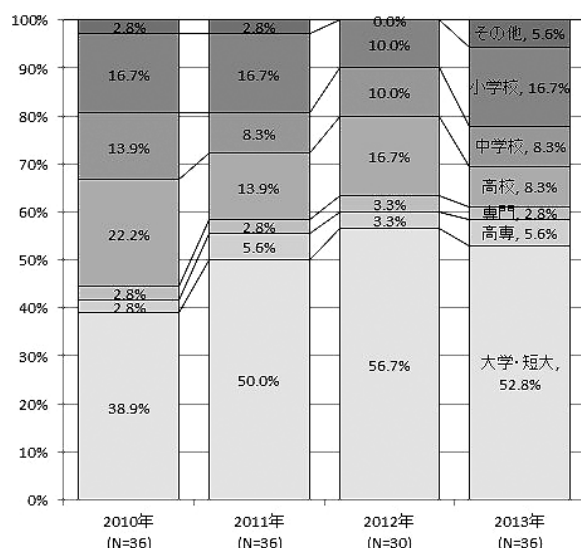


図2 「教育、学習支援業」の内訳

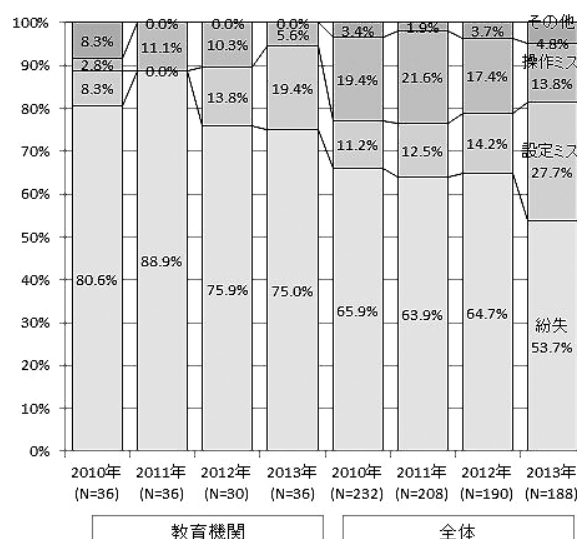


図3 情報漏えい原因の比率

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・事故件報道数は、大学、短大が約10.0件、高校と中学校が約1.2件、小学校が約1.4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、短大における情報漏えい事件・事故報道数は高止まりしており、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2013年、全体の2010年から2013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、「その他」はファイル共有ソフトによる流出や故意に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、2013年には個人情報漏えい事件・事故の約半数が「紛失」、約3割が「設定ミス」、約1割が「操作ミス」によるものであり、「その他」の原因による漏えいはわずかであることが分かる。2010年から2012年の期間には、全体として大きな変化は見られなかったが、2013年は「紛失」が減少し、「設定ミス」が増加している。紛失対策が進む一方で、サーバーの管理が不十分で不正アクセスを受

けるケースが増加しているものと考えられる。「その他」に分類しているが、2012年に3件だった「故意」による情報漏えい事件は7件に増加しており、従業員のモラル教育の重要性が増している。

教育機関に限れば、紛失による事件・事故の割合は約4分の3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、2013年とその数を増している。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加えて、Googleグループなどインターネット上のサービスを業務利用して個人情報が閲覧可能状態で放置されていたケースが多く、今後は紛失対策に次いで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2013年、全体の2010年から2013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、「サーバー」はWebやデータベースのサーバーを、「電子媒体」はPC、USBメモリ、

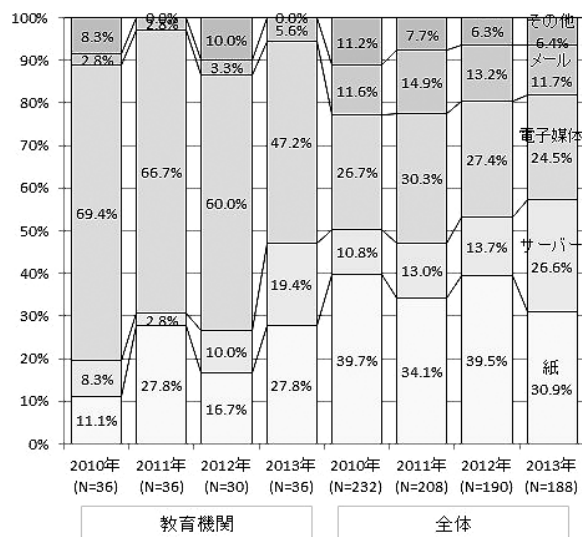


図 4 情報漏えい媒体の比率

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, 「その他」は Winny や Share などのファイル共有ソフトウェア, FAX, 郵便物を分類した。

図 4 から全業種では, 2013 年には約 3 割の情報漏えい事件・事故が紙媒体を, 3 割弱がサーバーを, 約 4 分の 1 が電子媒体を, 1 割強がメール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 位のサーバーによる漏えいは, ほぼ全てがサーバーの設定ミス, プログラムミス, 管理不足によるものである。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。2012 年は比較的少規模の Web サイトからの情報漏えい事件が数多く報じられていたが, 2013 年はヤフー, OCN, ニフティ, GREE, じゃらんなどインターネットサービスを専門に手掛ける会社の情報漏えい事件・事故が多く報じられた。業種としては, 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。

第 3 位の電子媒体の多くは, USB メモリと PC である。2013 年は USB メモリを介した漏えい事件・事故が減少して PC の紛失や盗難が増加している。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が, 最近は小型軽量の PC も持ち運んで業務に使用されるようになってきた。USB メモリや PC 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が, 特に教育, 学習支援業と公務が多い。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 4 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れる。

全業種の 2010 年から 2013 年の情報漏えい媒体の比率を比較しても, 紙が減少しサーバーが増加した程度で, 大きな変化は見られない。ただし, 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 3 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 割で全体平均と変わらないのに対し, 約 5 割が電子媒体による漏えいである。サーバーによる漏えいも 2 割と多い。メールやファイル共有ソフトによる漏えいは, 上位 3 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 5 割を占

める電子媒体は、その約 5 割が USB メモリで、約 4 割が PC、ポータブルハードディスクおよび SD カードである。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、全て大学と高专で発生している。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、件数は少ないものの、漏えいの危険性を認識しておく必要がある。

2013 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 1 件報じられており、未だに楽観でき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 2013 年の情報漏えい媒体の比率を比較すると、電子媒体による漏えいが減少する一方で、サーバーによる漏えいが増加している様子が見えてくる。件数が少ないため、統計的に傾向があるとは言えないが、教育機関においては、業務データを USB メモリなどの電子媒体に保存して移動するのではなく、インターネット上のサーバーに保存して活用するケースが増加しており、USB メモリや PC の持ち運びに注意するだけでは対策として不十分になりつつあると考えられる。

1. 5. 教育機関における情報漏えい対策の重点項目

ここでは、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 3 年間の情報漏えい事件・事故の原因の推移から、まず USB メモリや PC などの電子媒体の紛失・盗難対策、次いで、オンラインストレージやクラウドサービスの厳格な公開

設定やサーバー管理が最も急務である。ただし、初中等教育では紙媒体の個人情報を持ち歩くケースも多く、紙媒体の管理にも十分な注意を要する。

今後の傾向としては、USB メモリなどの電子記憶媒体は徐々に使われなくなり、オンラインストレージのようなインターネット上のサービスが主流となる可能性が高い。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は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簡単ではない。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。

2013 年は、何らかの原因で漏えいした ID とパスワードを用いて他のインターネットサービスのログインを試みるという不正アクセスが多発した。ID としてはメールアドレスが用いられることが多く、パスワードを使いまわしていると容易に他のサービスへのログインを許してしまうことになる。このため、インターネットサービスごとに異なるパスワードを設定し、定期的に変更するというパスワード管理手法が求められることになる⁶⁷⁾。

ま と め

本稿では、2013 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、1 年前、2 年前および 3 年前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・事故の報道数が約半数であること、教育機関における情報漏えい原因の約 4 分の 3 は紙や電子媒体の紛失・盗難によるものであること、電子媒体の約半数は USB メモリであること、サーバーによる漏えいが約 2 割に達してい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まず、USB メモリや PC などの電子媒体の紛失・盗難対策、次いでオンラインストレージやクラウドサービスの厳格な公開設定やサーバー管理が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。

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) 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) 佐伯勇, 2013, 『教育機関における情報漏えい事故の傾向と対策 (2012 年版)』, 甲南女子大学研究紀要人間科学編, Vol.49, pp.145-151.
- 5) 文部科学省, 2013, 『学校基本調査－平成 25 年度 (速報) 結果の概要－』, http://www.mext.go.jp/b_menu/houdou/25/08/attach/1338337.htm, (2013 年 11 月 3 日アクセス).
- 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 三訂版 IT 時代の危機管理入門』, 実教出版.