＜研究ノート＞

大学における個人情報保護の監査と対策
－ある大学でのリスク管理における個人情報保護－

Audit and measure of personal information protection in a university
－ Personal information protection in a risk management at a certain university －

松田　貴典
Yoshinori Matsuda
大阪成蹊大学名誉教授

概要

大学という独立閉鎖的な環境のなかで、個人情報保護の監査を個人研究室まで対象にした事例は非常に少ないと言える。本稿は、A 大学で実施された個人情報保護の監査を非常に短期間で意思決定され実施し、成果をあげた事例である。監査での指摘事項は、その部署のなかで対策案が出され、承認されたのちに実施し高い成果がでた。その理由として、①大学でのガバナンス強化のために経営体制を刷新し、経営と教学の意思決定を迅速に実行できる「経営・教学本部会議（仮称）」の設置がなされたこと、②大学の経営を取り巻く多様なリスクへの対応が急務であることの共通認識が図られたことが挙げられる。また、大学の環境のなかで、非常に難しい問題が発生するのではないかといった懸念もあったが、結果的には、ガバナンス強化による基本的な対策の実行であった。

キーワード：個人情報の漏洩、USR、ガバナンス改革、個人情報保護監査、リスク対応、緊急改善対策の実施

1．はじめに

最近、見かけることが少なかった大学における個人情報の流出ニュースが、平成 27 年 1 月 20 日に報じられた。東京の公立大学である S 大学は、「20 日までに、学生や入試合格者らの氏名、住所、電話番号などの個人情報が外部から閲覧可能な状態になっていた。今月 5 日までに学外から約 1 千件のアクセスがあり、外部に流出した可能性もある。閲覧可能だったファイルは約 38 万件。個人情報の悪用は確認されていない」という。「昨年 8 月の機器交換時、外部アクセスを無効にする設定変更を怠ったことが原因で、大学側は多大な迷惑をかけ､おわびする。教職員に情報セキュリティの教育・指導を徹底する」としている（平成 27 年 1 月 20 日　日本経済新聞 Web ニュース）[1]。

大学における個人情報の漏洩の事故や事件が、これまで全く発生していなかったというわけではない。ただ、マスコミに取り上げられることが少なくなったことは事実である。その理由として、①個人情報の漏洩は、大学の社会的責任（USR：University Social Responsibility）や法的責任を問われることになり、個人情報の保護や管理の教育が行き届いたこと、②マスコミがニュースとして取り上げるほどの話題性がなくなって来たことなどが挙げられる。

しかし、現状では大学に個人情報の保護や管理が、十分に教職員に徹底されているとは考えられず、これからも個人情報の漏洩事故や事件の発生するリスクは非常に高いといえる。しかも、大学の事務や教務業務、研究の情報化が高度化することで、学生情報や研究情報を含めた個人情報の漏洩が、深刻な問題を起こす要因となる脆弱性が複雑且つ広範囲に拡がっている。

筆者が大学の教員と経営に携わった平成 25 年に､大学内の個人情報を含めた重要情報の監査（システム監査等を含む、以後、「監査」と言う。）を

実践指導した。その結果、どの大学においても問題なる共通の課題が浮き彫りになった。この経験をもとに大学における個人情報の保護と監査及び対策について考察する。

2. 大学の個人情報漏洩事故・事件の状況と分析

2.1 過去 10 年間の個人情報漏洩件数の分析

表 1 は、大学職員 Net － Blog/News －で Web 公開された個人情報流出データの 2005 年から 2014 年をもとに、漏洩原因別に集計したものである [2]。

公開されたデータは、流出した個人情報のすべてを網羅しているわけではないが、表から ICT (Information Communication and Technology: 情報通信技術）の進展と密接に関連しているといえる。PC（Personal Computer）の盗難は、人間の物理的なセキュリティ対策の甘さに起因するものが大半である。近年、PC の盗難が減少しているのは、盗難対策が強化されたことも言えるが、PC そのものの携行機会が減少したとも言える。USB メモリー等の媒体紛失は、近年になり大きく減少している。これは、PC の HDD（固定ディスク）の大容量化で持ち歩きしなくなったといえるが、むしろ通信技術の高度化で情報の共有化が進み、ネットワークを介して情報活用できるようになり、あえて USB メモリー等の媒体に記録しなくなったともいえる。なお、ここでいう USB メモリー等とは、外部電磁的記憶媒体のことで、約 10 年前の頃は FD（Floppy Disc）が中心であったが、時代ともに、FD は CD（Compact Disc）や DVD となり、記録密度の向上で大容量化が進んだ。現在は USB メモリーや SD メモリーが主流になってきており、保存される情報も文書データのみならず、動画も記録されるようになった。USB メモリー等のコンパクト化と大容量化は、多様な情報が大量に保存できる「効用」がある反面、紛失すれば大量の情報を一瞬にして漏洩するという「脆弱性」が内在している [3]。

名簿盗難は、学外に名簿を持参し、自宅での紛失や自動車内で車上荒らしにあった等のケースである。名簿情報の紛失は、帰宅途中でカバンを電車の網棚に置き忘れたり学内外で紛失した等の場合である。メール誤送信は、学生情報をメールに添付し、大学の内外に間違ったアドレスや必要のない人まで送信をしてしまった等で、メールの多様化とアドレスの増加により誤送信はまだまだ発生するであろう。PC 盗難、名簿情報紛失、メール誤送信といったケースは、大学の職員のケアレスミスによる場合が多いが、移動や外出の多い大学教員が犯しやすい個人情報漏洩事故でもある。

一方、不正アクセスは他人の ID やパスワードを悪用して権限者以外の者が情報アクセスする場合である。対策不良は、セキュリティ設定をしていなかったり、設定ミスをしたりして学生の成績情報等が閲覧可能な状態で放置されていた場合などであるが、ネットワークシステムの変更や新システムの導入時などに発生しやすい事故である。また、不正プログラムであるマルウェア (malware) によりシステム設定が書き換えられたりすることもある。コンピュータ・ウイルス（以後、「ウイルス」という。）やファイアーウォール (Fire Wall) の設定不良で個人情報が漏洩する場合も対策不良としている。ウイルス対策用ワクチンソフトのパラメーター更新がなされていないことによるものも含まれている。企業や大学でのインターネットの拡大は、対策不良が今なお続いている要因である。

ファイル交換ソフトは「Winny」や「Share」等を介して学生情報や大学病院の患者データが流出した場合であるが、ファイル交換ソフトがウイ

表 1　過去 10 年間の原因別個人情報の漏洩件数

原因／西暦 20××	14	13	12	11	10	09	08	07	06	05	合計
不正アクセス	1		1	1							3
対策不良	1	2	1	1	3	1	4	1	4	1	19
ファイル交換ソフト					1		3	2	5		11
PC 盗難		2		1	5	3	8	9	4	5	37
USB メモリー等媒体紛失	1	2	1	4	2	5	2	11	4	3	35
メール誤送信	1	1	1	2	1	2		1			9
名簿盗難				1		1			1		3
名簿情報紛失				1			2	3	4	4	14
その他（不正開示）										1	1
合　計	4	7	4	11	12	12	19	27	22	14	132

ルスに犯されて流出した場合も含んでいる。ファイル交換ソフトの利用は、多くの大学において禁止されたり厳しく指導されたりして大幅に減少している。ウイルス感染はICTの能力不足より、少なくとも実施すべきウイルス対策をしていないことによる場合も多い。その一方で、最近発生している不正アクセスは、ネットワークの脆弱性を突いたケースである。近年は充分なセキュリティ対策をとりながら不正アクセスされることも多く、セキュリティ対策の難しさの所以である。

2.2 個人情報漏洩原因の考察

前項の個人情報漏洩の原因は、ICTの進化ともに少しずつ変化していることが理解できる。しかも、年が進むにつれセキュリティ対策の実効性が高まり、個人情報の漏洩事故や事件の件数が減少していることとも言える。しかし、大半は基本的なセキュリティ対策が実施されていたならば、防げたケースである。

例えば、少しの時間でもあっても研究室を出るときには、部屋の鍵をかけPCをシャットダウンさせる。個人情報の記載された資料等は、中が見えないキャビネットに保管し、常時鍵をかける。PCや個人情報の記載された資料は持ち帰らないようにする。もし、持ち帰る時には、帰宅途中での立ち寄りは絶対にしないようにする。資料の入ったカバンは、常に手でもち網棚等に置かない。PCやUSBメモリーには、個人情報は記録させない。その上でパスワードによるセキュリティ・ロックをかける。パスワードは毎月変更し、同じパスワードの使い回しをしない。個人情報の入ったファイルはメールで送信しない。ファイル交換ソフトは私物のPCであっても利用しない等、これらの遵守事項はセキュリティ対策の基本行動である。

セキュリティ機能の基本は「難さ（にくさ）」である。分かりやすく言い換えると「面倒くささ」である。人は誰もが時間が経ち、慣れとると「難さ」を回避する行動を起こすのである。そしてセキュリティ機能の強度の低下が始まる。特に、大学の場合には教員研究室という閉鎖的な環境の中で、注意喚起をされることも少なくセキュリティに対する認識は徐々に薄れていく。

3. 大学でのリスク対応と重要情報の管理の監査の事例

大学のおける個人情報と中心とした重要情報の監査事例は、あまり耳にしたことがない。大学には、在学中の学生情報をはじめ受験生や入学希望者（募集要項等の資料請求者、オープンキャンパス来校者等）など個人情報が山積している。これらの個人情報は取り扱いには最善の注意が必要であるが、大学という独立閉鎖的な環境のなかで、全学統一的に徹底した保護対策を実施しているところは少ない。ましてや、教員組織や研究室まで対象として個人情報保護の監査やシステム監査が実施されたことはほとんど例をみない。

以下、ある大学におけるリスク対策と個人情報を中心とした重要情報の監査の事例である。監査での指摘事項は、どの大学の組織や教職員にとっても共通的に言えることであろう。

3.1 A私立大学の新体制でのガバナンス強化とリスク対応

社団法人日本私立大学連盟経営委員会リスクマネジメント分科会偏「学校法人における内部統制の整備」のなかで、「ガバナンス、リスクマネジメントと内部統制」について「大学の経営を取り巻く環境が大きく変化し、大学が社会的責任を果たしつつ持続可能性を維持していくためには、適切なガバナンスの強化を図る必要がある。また、職務が複雑化してくるなか、多様なリスクへの対応等の強化が求められてきた。」[4]と提言している。具体的には、自然災害、競争の激化、18歳人口の減少、グローバル化の対応といった大学を取り巻く外部的要因と情報システムのトラブル、会計処理の誤謬・不正行為の発生、個人情報及び高度な経営判断にかかわる情報の流失または漏洩といった組織のなかで生ずる内部的要因など、様々な脅威が現実化するリスクが増大化している。大学の経営にあたっては、こうしたリスクに常に配慮し必要な対応をとることが急務である。こうしたなか、A私立大学（以後、「A大学」という。）がガバナンス強化のために経営体制を刷新し、経営改革を実現するために、四つの改革を掲げ実行した。

第一は、経営の意思決定をと迅速に実現するための組織改革である。すなわち、これまでの経営と教学の独立性を堅持しつつ、経営計画にもとづく事業活動の統一的の実行体制の確立である。理事長をトップとした法人組織と学長をトップとする大学組織の幹部が席を同じくした「経営・教学本部会議（仮称）」を設置して、直面する問題を

毎週討議し、その結果を迅速に事務組織及び教員組織に下ろして実行を促した。この組織改革はガバナンス強化のために最も重要な課題であった。物事を決め実現していくためには、事務組織と教員組織が協力体制をしくことなく推進することは不可能である。組織改革の成功により、第二、第三、第四の改革の推進が円滑に実現できた画期的なことであった。第二は、教育改革と学生サービスの支援強化である。具体的には教育カリキュラムの改訂は、教員会議にて審議されたのちに、「経営・教学本部会議」に諮られることになった。大学経営の厳しい環境のなかで、求められる教育内容が大学経営に密接に関係するからである。また、学生支援サービスの強化では、学生の就職活動の支援を徹底的におこなった。大学内での企業就職セミナーを大幅に増やして、学生が大学内で就職セミナーを受講し、面接試験を受ける機会を増大化させたのである。さらに、学生の就職活動データベースを構築して、就職希望の相談から、企業エントリー、模擬面接指導、就職先決定、フォローアップまでの一連の就職活動情報を一元化し、職員と教員が学生の就職にむけて徹底した進捗管理と支援体制を確立した。この状況は毎週のごとく、「経営・教学本部会議」に報告され、課題解決が図られた。第三は、リスク対応である。大学のリスク対応は、まず、経営目標の達成に影響を及ぼすリスクを評価し、その中から１４の重点リスクを選定し、年度内にリスク改善をすべく内部監査の実施を決定した。個人情報保護の問題は、大学における重要情報の管理の一環として実施された。表２は、A大学が選定した対応すべき重点リスク事項である。本件の詳細については次節で論述する。第四は、環境改善とマナー向上である。「挨拶運動」からはじまり、学内外の全面禁止を実施した。学生、教職員はもとより来客まで全面禁煙の協力をお願いした。禁煙運度は地域住民からも賛同をえて、市から地域の全面禁止地域の指定を受けるまでに運動が広がったのである。この環境改善とマネー向上は、授業への出席率の向上、学生生活態度の改善にもなり、就職活動にも好影響を及ぼした。

表２ A大学における重点リスク事項

①重要情報の管理
②学生・父母からのクレーム対応
③学生等のけが・事故予防
④教職員の健康管理の取り組み
⑤学生相談等支援体制
⑥不審者学内侵入時の危機管理
⑦ハラスメント防止
⑧知的財産権への対応
⑨入試のミスの予防
⑩公印管理・金貨管理の強化
⑪地域社会との連携強化
⑫災害時の緊急対応
⑬広報体制の整備・充実
⑭学生・教職員のコンプライアン

3.2 重要情報の管理での個人情報の保護と監査

重要情報の管理をテーマに実施された監査は、重点リスクの対応を進めるなかで、当時、A大学では経営改革のために優先課題として学生募集強化を目標に掲げていた。学生募集を強化するためには、オープンキャンパスに来校する高等学校の生徒の志望アンケート調査や新入学生の入学動向調査、卒業生の協力などが必須であり、この実施にあたっては個人情報の取り扱いについて見直しをおこなったところ、アンケートで記載する住所や氏名、志望動機等の個人情報の利用目的が記載されていなかったり、表現が不十分であったりしたことが判明した。また、同窓会での協力にあたっては卒業生の個人情報の提供が、本人の同意を得ているのか、個人情報保護の規程がありながら、その遵守やマニュア作成による徹底が不十分であることが問題となった。本稿は、重点リスク事項のうち、「①重要情報の管理」で実施された個人情報の保護と監査の事例である。

重要情報の管理をテーマに実施された監査は、法人組織から大学組織まで全組織に渡った。全組織を対象に監査を実施した背景には、大学における重要情報には個人情報や経営情報等があり、それが漏洩した場合には、行政処分、賠償責任、利益滅失、信用失墜等、レプテーションリスクは甚大なものであり、大学の社会的責任 (USR) を問われることになる。重要情報の管理については、経営陣のリスク認識が高く、監査対象が事務部門のみならず教員の個人研究室まで含まれる画期的なことであった。特に個人研究室まで監査の対象になった背景には、パソコンの盗難、試験問題の紛失及び盗難、提出レポートの紛失・氏名書き換え、成績情報の漏洩、アカデミック・ハラスメントの発生など、学生のセンシティブな情報が大量に保管されており、また、個人研究室には学生や

来客の出入りが多く、個人情報の漏洩リスクは非常に高いと認識されたからである。しかし、これまで個人研究室は鍵があり、重要な情報はキャビネットに入れられて保管されており、セキュリティ機能は高いという前提のもとに監査対象になることは少なかった。また、教員と事務職員との非干渉関係、教員と学生との師弟関係など監査の実施に難しい面があることも否定できない。

事前監査では、まず、重要情報の自己チェックからはじめ、それぞれの事務組織や個人研究室にはどのような重要情報が管理されているのか、重要情報管理調査表の提出が求められた。表３は、個人研究室で管理されている重要情報の調査例である。教員の役職や担当する委員会組織により、保有する重要情報は異なっているが、共通的に保有するものは多い。しかし、個人情報の記録媒体の管理や保管方法、保管期間など統一的な規程がなく、管理は教職員に委ねられていた。特に、授業科目を担当教員が実施する期末試験の採点は自宅に持ち帰って行うことが多く、採点結果は返送されるものの、非常勤の教員の採点済み試験問題の返却・保管・廃棄や退職後の手続きなど改めて問題となった。

3.3 監査の結果と指摘事項

監査は２ヶ月間に渡り実施され、全体的指摘事項と個別指摘事項が「経営・教学本部会議」で報告された。以下、主な指摘事項である。筆者は、これらの指摘事項は、当該大学での特徴的なものではなく、多くの大学で共通的に指摘される事項と考える。

（１）全体的指摘事項

①個人情報を含め重要情報の保管は、各部署ともキャビネットに施錠管理されていた。しかし、一部の研究室では、期末試験の採点途中の試験問題が、施錠されていないキャビネットや机上に放置されていた。

②一部研究室では、学内勤務中に研究室の施錠がされていなかった。例：会議中、授業中、食事中等

③各部署には個人情報保護の統括責任者及び個別データ管理責任者が選定されているが、年度毎に変更があっても更新がなされていなかった。

④教員（常勤、非常勤）の採点済み試験問題の保存期間、廃棄・返却のルールがない。

⑤個人情報の取得時に、利用目的の特定及び本人の同意が不十分な場合や、学生情報の第三者提供について、事前に本人の同意がとられていない事例が散見された。

（２）個別的指摘事項

①人事部

・個人情報の統括管理組織に選定されているが、個人情報保護委員の改選管理及び定期的な委員会の実施をしていない。

・個人情報の開示請求に対するルールが設定さ

表３　個人研究室が保有する重要情報調査例（一部抜粋、件数は事例：研究室により異なる）

情報名	項目	媒体	保管場所	管理	件数	保管期間
試験問題（採点済）	学籍番号、氏名、採点	紙	キャビネット	鍵	180	卒業迄
学生カルテ情報	住所、電話、履修科目・単位、出身校、保護者情報、奨学金関係等	データ	学生サーバ	PW	—	学生部
学生成績表	受講生成績、履修状況、科目区分	紙 データ	机引出し 教務サーバ	鍵 PW	32	卒業迄 教務部
学生レポート等	研究レポート、指導内容	紙	キャビネット	鍵	25	焼却
学生異動情報	休学、退学、停学等	紙	キャビネット	鍵	5	教務部
学生指導情報	授業出欠、アルバイト、クラブ活動、ゼミ指導、研究指導、就職指導等	紙 データ	キャビネット 教務サーバ	鍵 PW	35	卒業迄 教務部
履歴書（採用審査）	本人の履歴・業績書、採用受験者等	紙	キャビネット	鍵	—	総務部
組織人事情報	組織、教職員人事、職位	データ	事務サーバ	PW	—	人事部
教員会議資料	学生部、教務部	紙	机引出し	鍵	—	焼却
研究費申請書	個人研究費・外部研究費等申請	紙	キャビネット	鍵	—	総務部

れていない。
②情報システム部
・組織共有のパスワードがあり、退職者の変更がなされていない。
・PC を一定時間使用しない場合のスクリーンセーバーの設定がなされていない PC がある。
③教務部
・採点済み試験答案用紙の保存期間及び返却・廃棄のルールがなく、返却された場合には受領確認もなく、ランダムに保管されている。
④入試広報及び学部事務
・オープンキャンパスでの生徒アンケートに、個人情報の利用目的が記載されていないもの、不適切な表現がある
⑤総務部
・同窓会への卒業者名簿の提供に、本人の同意を得ていない。
⑥スポーツ＆カルチャーセンター
・スポーツ傷害保険会社への個人情報提供に本人の同意を得ていない。
⑦教育・研究支援センター
・公開講座での一部チラシ、申込書に個人情報の利用目的が記載されていないものがある。
⑧就職部
・就職セミナーの受講申込は就職部前の一覧形式の申込書への記載であり、誰もが自由にセミナー受講申込者の名簿が見られる。
⑨図書館
・図書貸出の返却期限超過者の学籍番号、氏名、貸出図書名、返却期限が掲示されており、本人の同意を得ていない。
⑩教員個人研究室・共同研究室
・一部個人研究室には重要情報が施錠管理されずに、書類が机上に積み上げられていた。
・共同研究室が、無人で施錠されていないケースがあった。
・共同研究室のコピー室に、試験問題が残っていた。

これらの指摘事項は大学経営のトップである理事長と学長に報告され、「経営・教学本部会議」にて対策が討議され、緊急に実施すべき事項については直ちに改善策が実行された。

3.4 緊急改善対策の実施

緊急改善策の策定はそれぞれの部署で行われた。大学の個人情報の大半は、学生情報と生徒情報であり、その使用目的、利用状況、保管状況は明白であることから、指摘事項の内容からの対策は、基本的に遵守すべき事項である。むしろその保護の重要性の認識をいかに徹底させるかの難しさがある。教職員に学生という個人情報の保護の重要性の認識と漏洩することが、どれほどの社会的責任者（USR）を問われることになるか徹底することの難しさである。以下、実施された有効な対策事例である。

①教員の「教員の管理する重要情報の漏洩防止のために遵守事項」の策定
前項「2．10 年間の個人情報漏洩事故・事件の状況 」から漏洩の原因を分析すると、企業における漏洩原因と共通することが多いが、前述のように大学教員であるが故に、管理の徹底が重要な側面がある。本遵守事項は、教員が中心になって策定し教員会議のなかで徹底されたものである。表 4 は、「教員の管理する重要情報（個人情報保護及び機密情報）の漏洩等防止のための遵守事項」である。

②学生個人情報の取扱と収集・利用目的・管理の同意
学生が入学すると、大学の事務から直ちに学生の証明書発行や健康管理、連絡先住所・電話番号等、多くの個人情報の記載を求められるが、それがどのような目的で使われるのかオリエンテーションで説明があるものの、統一的な同意を得るようのことはしていなかった。ついては、入学式後のオリエンテーションにて、学生個人情報の取扱と収集・利用目的・管理の同意を得る手続きを行うようにした。表 5 は、「学生個人情報の取扱と収集・利用目的・管理の同意」の資料である。なお、オリエンテーションでは、学生個人情報の収集・利用目的や管理の詳細について配布する学生便覧にて丁寧に説明するとともに、詳細の内容は学生ウェブサイトにも掲載していることを説明することとした。

③教職員への個人情報保護の教育
個人情報の保護と管理について指導・教育は、これまでここの部署にて管理者が説明形式で実施されてきた。教員に対しての指導・教育は皆無であった。もちろん、教員のなかには個人情報保護法やセキュリティの専門家はいた。しかし、これらの専門教員が個人情報の保護やセキュリティ対策について、高い認識

のもとで個人情報を保護できたとは言い難い。一般の教職員と同様に、定期的な指導・教育を受講してもらうことで、モチベーションが維持できるのである。A大学では、定期的に教職員対象の個人情報保護やハラスメント防止教育を、外部講師を招いて実施するとともに、教員会議においても緊急改善対策の実施を徹底指導し、成果を上げることができた。

④指摘事項の改善策の策定と実施

指摘事項の改善策は、主にその部署で策定され、組織長のもとで承認を得て、「経営・教学本部会議」に報告される。改善策は「経営・教学本部会議」にて、その実施計画、実施スケジュール、対策の有効性が審議され、承認が得れば実行に移される。実施状況は、フォローアップされて、3ヶ月以内に再度監査を受ける。

4. おわりに

大学という独立閉鎖的な環境のなかで、個人情報保護の監査を個人研究室まで対象にした事例は非常に少ないと思われる。それも、非常に短期間で意思決定され実施できたのは、①大学でのガバナンス強化のために経営体制を刷新と、統一的な意思決定のプロセスの迅速化の組織改革にあった。すなわち、理事長をトップとした法人組織と学長をトップとする大学組織の幹部が席を同じくした「経営・教学本部会議」の設置である。②大学の経営を取り巻く環境が大きく変化し、大学が社会的責任を果たしつつ持続可能性を維持していくためには、多様なリスクへの対応が急務であることの共通認識が図られたことである。

筆者は、当該大学での監査の結果は、非常に成果があったと考えている。特に、大学の教員は学生の個人情報の取り扱いについては、注意をしなければならないと感覚的には感じていたようであるが、どこからも強制的な注意や指導がなく日常管理で終始していたようである。それが、個人研究室の監査が実施されるということで、教員会議に報告されると何が起こったのかと反対意見をだす教員もいた。しかし、同僚の教員からの重要問題であると提議されることで、同意が得られ実施できたのである。また、大学の環境のなかで非常に難しい問題が発生するのではないかといった懸念もあったが、結果的には、基本的な対策で十分の成果をあげることができたのである。それは、この度の問題が教員にとっても認識が高い個人情報の保護であったからである。

前項の「表2 A大学における重点リスク事項」に掲げたように、まだまだ対応すべきリスクが非常に多く残っている。この中には、組織間の利害関係の問題がおこることも考えられ、新体制でのガバナンス強化とリスク対応は、今後も続くことになる。

参考文献

[1] 「首都大、情報流出の恐れ　5万1000人分」日本経済新聞　電子版 http://www.nikkei.com/article/DGXLASDG19HE7_Q5A120C1CR0000/ 2015.1.20 参照

[2] 「情報漏洩アーカイブ」 大学職員Net－Blog/News http://blog.university-staff.net/archives/1/cat16/ 2015.1.20 参照

[3] 松田貴典著 「ビジネス情報の法とセキュリティ」 白桃書房 2005

[4] 日本私立大学連盟経営委員会リスクマネジメント分科会偏 「学校法人における内部統制の整備・充実」平成21年3月 2009

[5] 「文部科学省所管事業分野における個人情報保護に関するガイドライン」(平成24年3月29日文部科学省告示第62号)

表４　教員の管理する重要情報（個人情報保護及び機密情報）の漏洩等防止のための遵守事項（一部改訂）

教員の管理する重要情報（個人情報保護及び機密情報）の漏洩等防止のための遵守事項

教員が管理する重要情報（個人情報及び大学の機密情報等）は、基本、施錠のある個人研究室にて保管されており、物理的セキュリティ面では保護されている。しかし。その使用は、原則、個人研究室であっても、学生や外部からの訪問者が多く、細心の注意をはらわなければならない。また、ICT（情報通信技術）の高度化と多様化により、教員業務が自宅や携帯端末から行われることもあり、重要情報の管理・保護は、法的・倫理的セキュリティ問題に拡がってきた。そこで､重要情報の漏洩等は､教員個人の責任のみならず､大学の社会的責任（USR: University Social Responsibility）を問われることになる。　以下、重要情報の漏洩，滅失，毀損の防止のために，厳守すべき事項である

1. 重要情報の定義
　重要情報とは、学生の成績、判定評価、試験（採点）結果、面談・相談票（メモ）、入試成績、学生処分、学生異動（退学、除籍等）等の学生に関わる情報であり、機密情報とは、学園の経営情報（経営計画等）、試験問題等の情報である。
2. 重要情報の入った書類や電磁的記録の鍵保管
　重要情報の入った書類や電磁的記録は必ず鍵のかかる机，キャビネットに施錠保管すること。
3. 研究室の施錠
　個人研究室を離れる場合には施錠すること。食事やトイレ等に行く短時間の場合であっても施錠すること。もし，来客や学生等を研究室に入れる場合（作業をさせる場合も含む）には，重要情報が見えないように、机やキャビネットにしまい、施錠すること。
4. 個人研究室の整理整頓
　個人研究室は、試験問題・結果、成績評価、学生指導情報、出席・欠席情報、健康管理情報、保護者情報、教授会・会議資料等、紙媒体の個人情報が保管されている場所となっている。研究室は常に整理整頓し、個人情報が散在し、研究室に入る学生や他人から個人情報が見られたり、アクセスされたりしないように、厳重管理すること。
5. 携行ノートパソコン等の鍵（暗号やパスワード等）の施錠
　暗号やパスワード設定や指紋認証等の鍵機能を使ってシステム施錠すること。私物の携行ノートパソコンであっても，大学の教務・人事業務を行う場合は同様とする。
6. 携行メモリー・電磁的記録等の鍵（暗号やパスワード等）の施錠
　携行を目的とするUSBフラッシュメモリー等は必ずパスワード設定等の鍵機能付のものを使用し，携行するときには必ず鍵をかけること。また,CD／DVDディスク等を携行したり郵送したりするときには必ずデータを暗号化して書留郵便で送付すること。
7. 携行ノートパソコン等への重要情報の保存禁止。
　私物を問わず携行ノートパソコン等やメモリー等には、学生名簿や成績表、教職員名簿などのセンシティブな個人情報の保存を原則禁止する。もし，保存が必要な時には，パソコン等に鍵機能を設定するか暗号化して保存のこと。
8. 携行時の盗難等の防止対策
　携行ノートパソコンやメモリー等の機器が入ったカバンやバッグを持ち出す場合には、それらを常に手もとにおき、盗難、置き引き、置き忘れがないように万全の注意を払うこと。特に、電車の中では網棚に置きわすれないように、手持ちすること。
9. ウィニー等ファイル交換ソフトのダウンロード禁止
　ウィニー等のファイル交換ソフトを携行ノートパソコン等や研究室パソコン等にダウンロードして使用しないこと。
10. 不正・不適切なサイトへのアクセス禁止
　興味本位に出会い系サイトなどの不正・不適切なサイトへのアクセスや登録を行わないこと。コンピュータ・ウイルス等の不正なソフトウェアの侵入原因となる。
11. 重要情報のメール，ＦＡＸ送信の禁止
　個人情報の入った情報（学生の名簿，成績表等）は原則，メールやＦＡＸで送信しないこと。もし，送付する必要が発生した場合には情報データを暗号化するか，紙情報である場合には書留郵便で送付すること。
12. パスワードや暗証番号等の教示・開示の禁止
　パソコンのパスワード，共同研究室の暗証番号など，重要なセキュリティ機能を解除する情報は絶対に他人に教えたり，開示したりしないこと。

以上

表５　学生個人情報の取扱と収集・利用目的・管理の同意（一部改訂）

○○年度入学生の皆さん
保護者各位

学校法人　○○○○
○○大学学長

○○大学における個人情報の取り扱いについて

学校法人○○では、○○年４月１日から「個人情報保護法」の施行にともない、「個人情報の取扱いについて※」を公表し、生徒・学生並びに保証人等、教職員等の個人情報を安全かつ適正に管理・運用することに努めております。

○○大学では、この指針に則り、学生・保護者・保証人（以下、学生等という）の個人情報を適正に管理・運営に努めます。つきましては、収集しました個人情報を、教育研究、学生支援、大学運営上、必要と認められる範囲で、以下の目的で利用いたします。

【利用目的】
○入学願書業務処理、入学試験合否判定業務並びに入学手続き管理業務
○学籍管理、履修登録、成績管理、授業運営等、授業出欠管理・携帯電話学修支援業務
○健康管理、保健衛生管理等、生活健康管理業務
○奨学金管理、奨学金相談手続支援業務
○学生証、各種証明書の発行業務
○学生生活・課外活動支援業務
○学生連絡掲示・携帯電話連絡業務
○就職・進学関係情報の管理等、進路就職支援業務
○授業料等学費情報管理業務
○学内施設・設備の利用管理業務
○図書返却期限超過者の掲示、図書館利用情報管理業務
○成績通知書の保護者（保証人）への通知及び保護者（保証人）との成績、修学状況相談業務
○大学・学校の新聞、広報誌、大学案内等の広報業務
○卒業後の各種案内送付業務
○卒業後の同窓会（○○会）への名簿提供並びに同窓会運営業務
○国、行政及びその他の団体からの各種調査、認証評価等の業務
○その他、傷害保険の付与、卒業アルバムの作成、企業・学校実習など上記に附随する業務

【共同利用の範囲】
学校法人○○では、業務遂行にあたり、上記利用目的の達成に必要な範囲において、法人、○○大学、○○高等学校、○○幼稚園の間において共同利用致します。

【個人情報に関する相談、開示等】
本大学では、個人情報の関する相談、開示、訂正、利用停止の請求の総合受付を総務部にておこなっていますが、内容の如何によっては、教務部、学生部においても相談を受け付けております。

※「個人情報の取り扱いについて」詳細
○○大学ウェブサイト：http://www.○○及び学生便覧に掲載しています。

個人情報の取り扱いに関する同意書

年　　月　　日

○○学長　殿

○○大学における個人情報の取り扱いについて書かれている個人情報の収集、利用目的、管理などを理解し、個人情報の取り扱いに同意します。

学籍番号　　氏　名（自筆署名）

研究論文投稿規則

1987 年 7 月 28 日制定
1990 年 3 月 20 日改訂
2005 年 8 月 22 日改訂

第１条（学会誌の機能と目的）
　本学会誌は、システム監査に関する領域における理論ならびに方法の発展および普及のために、会員の独創的な研究成果を公表することを主なる目的として刊行する。
第２条（投稿の資格）
　論文の執筆者は、原則として名誉会員、正会員とする。
第３条（基本的要件）
　論文は、上記領域における理論ならびに方法などに関する新しい内容であって、まとまった研究成果を発表するものであり、その研究目的と結論が明確であること。
２．研究の予告的性格のもの、単なる事象を列挙しただけのものでないこと。
３．論文原稿は、他の刊行物に未発表のものであること。
第４条（表題）
　論文はその内容を表す表題を付けること。
２．論文が一連の研究の部分をなす場合には、その一連の研究の名称とそれとの関連を副題として付記することができる。
３．表題には英文をそえること。
第５条（要旨）
　論文には 400 字以内の要旨をそえること。
第６条（字数）
　投稿論文の長さは、15,000 字を目安とする。
第７条（採否および学会誌掲載）
　投稿された論文の学会誌掲載の採否は、２名以上の論文査読委員の審査結果に基づき、編集委員会が決める。
２．審査の結果、内容の訂正などを要請することがある。
３．訂正を求められた場合は、３か月以内に再提出しなければならない。
４．３か月を超えて提出された場合は、原則として新規投稿とみなす。
５．投稿原稿、再提出原稿の受理日は編集委員会（学会事務局）に到着した日とする。
６．採択された論文の会誌への掲載は、原則として受付順とする。
７．同一人（共同執筆を含む）の論文掲載は、年１本とする。
８．英文による投稿も認める。
第８条（執筆要領）
　論文は、別途定めるシステム監査学会執筆細則に従うこと。

附則
この規則は、1987 年 7 月 28 日から施行する。
この規則の改訂は、1990 年 3 月 20 日から施行する。
この規則の改訂は、2005 年 8 月 22 日から施行する。

システム監査学会誌執筆細則

1990 年 3 月 20 日制定

1．投稿原稿の種別

（1）研究論文

（2）事例研究論文

（3）その他

２．投稿手続き

（1）投稿に使用する原稿用紙

①原稿を手書きする場合は、400 字詰原稿用紙（横書き）を投稿者自身が手配し、使用すること。

②原稿をワープロ等で作成する場合は、A4 版の用紙を使用し、字詰めは、40 字 ×35 行にすること。

③論文の長さは、当学会投稿規則に基づき 15,000 字を目安とする。学会誌刷り上がり 10 ページ程度（図表含む）とする。

（2）原稿の送付先および問い合わせ先

〒 105-0011　東京都港区芝公園 3-5-8　機械振興会館内

システム監査学会事務局　　TEL03-3432-3166

なお、原稿の投稿は郵送によること。

（3）原稿の整え方

①表題

日英両文で書く。原稿の種別を表題の左肩に明記すること。

②著者名・所属

氏名、所属を日英両文で書く。

③概要

論文の要約を 400 字以内にまとめて書く。

④キーワード

研究内容に直接関係する重要な語句を３～７個記述する。

⑤本文

原則として「はじめに」、「本論」、「おわりに」の順とする。「本論」の見出し付け、筋立ては自由とする。

⑥注、参考文献

論文に関連する重要な文献については、本文中の関連個所の右肩に注番号もしくは文献番号を書き、本文の末尾にまとめてその文献を記述する。

原則として次の形式に従う。

・雑誌の場合

注番号）著者；「論題」, 雑誌名 , 巻 , 号 , ページ（発行年）

（例）

3）吉田一雄稿；「システム監査とセキュリティ」, システム監査 ,Vol.13,No.2,pp.10 ～ 15（1989）

4）Anthony,T.；Audis Trail,Journal of? Systems Audits, Vol.33,No.5, p.41（1989）

・単行本の場合

注番号）著者；署名 , 発行所 , ページ（発行年）

（例）

6）太田良雄著；システム監査論 , 東京出版 ,p.180（1987）

7）Davis,G.B.；Audits and Control,Prentice-Hall,p.132(1988)

⑦図および表

・図および表は「図表－ 1」のように通番と名称をつけること。
・本文中の図表の挿入箇所は、本文原稿の欄外に明記すること。
・図および表を他から引用した場合は、その出典を、注、参考文献と同じ要領で図表の下部に付記すること。
・図表の刷り上がり寸法の 2 倍程度で記述（トレース）すること。
・図表の数、大きさは、学会誌への論文収録ページ数が図表を含んで 10 ページ程度となることを前提にして決めること。

4．投稿原稿の扱い

(1)「2. (3) 原稿の整え方」に従って一式が投稿されたときは、受付通知を受付後 1 週間以内に発行する。
(2) 採否および学会誌掲載は、投稿規則第 3 条および第 7 条に従う。
(3) 編集委員会が採否の決定をした場合は、その通知をする。投稿原稿は返却しないので、一式は手元に保管する。
(4) 採択された場合は、校正その他について編集委員会の指示に従う。