

大学における情報セキュリティマネジメントに関する考察

A Study on Information Security Management in Universities

赤 林 隆 仁

AKABAYASHI, Takahito

本論文では大学における情報セキュリティについて、その歴史的背景や経緯、公的認証の取得動向等について論述し、実際のセキュリティインシデントの実例とその傾向を日米について分析比較した。その結果明らかになった日米の違い、インシデント原因の傾向から、リスクマネジメントの立場より今後のあるべき方向について考察・提案を行った。

はじめに

21世紀に入り大学の情報化が進展するとともに情報セキュリティマネジメントは重要な経営要素になりつつある。既に多くの大学で情報セキュリティポリシーが策定され、継続的な情報セキュリティマネジメントが開始されている。本論文では更にこれを実効性あるものにして行くための方策について、過去の傾向、最近の情報インシデント事例等からの考察を試みた。なお本論文の内容は筆者の私見を述べたものであり、本学の経営や政策とは直接関係がない。

1. 初期の情報セキュリティ

大学には早期からコンピュータシステムが導入され、1990年代初期にインターネットを一早く利用開始して育てたのも大学であった。しかし研究用の用途が主であったことや、初期のインターネットは「自由でオープンな

ネットワーク」という考え方で運用されていたためビジネス用のコンピュータシステムと比べて情報セキュリティに対する意識は高いとは言えなかった。1990年代後半に学内のネット化が進展すると、インターネットのオープン性を悪用したハッキング、情報漏洩、ネットの不正利用、ソフトの不正コピー、機器の盗難等が顕在化してきた。当時の大学には専門的・組織的な情報セキュリティ体制は確立されておらず、研究室単位の自主的な努力に任されていた面が多かったため、外部からのシステム攻撃の格好な標的とされる傾向にあった。2000年に私立大学情報教育協会が加盟472校（大学、短期大学）に調査した結果では、回答した加盟校の30%が何らかの不正侵入を受けており、特に不正メール中継（38%）、他機関攻撃の踏み台（21%）など社会一般に悪影響を及ぼす行為に利用されている点が目立った。また発覚した不祥事の7割は被害を受けた外部からの指摘によるもので、

キーワード: 情報セキュリティマネジメント、リスクマネジメント、個人情報、大学

Key words : Information Security Management, Risk Management, ISMS, Individual Information, University

自覚に乏しい状況であったことも推測される。この傾向はその後もしばらく続き（株）ラックが2003年に調査した結果では日本におけるシステム不正侵入インシデントの40%が大学等の学術研究機関で起きていた。

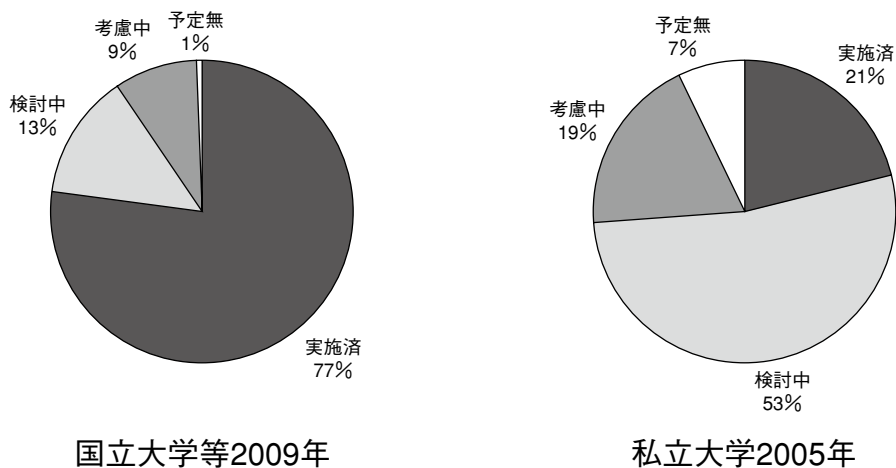
この頃より、一般業界での情報セキュリティ重視の傾向、学内のネット化の更なる進展、業務のシステム化等を背景に大学においても情報セキュリティに対する取組が本格的に開始された。

2. 情報セキュリティポリシー

日本では2000年より政府主導で日本型IT社会の実現を目指す「e-Japan戦略」が発動された。またこの時期に官公庁webページに対する不正アクセスや攻撃が相次いだことから政府内部でも急激に情報セキュリティに対する関心が高まり、2000年7月に情報セキュリティ対策推進会議より「情報セキュリティポリシーに関するガイドライン」が一般産業向けに発表された。

大学に関しては2002年3月に「大学における情報セキュリティポリシーの考え方」が「大学の情報セキュリティポリシーに関する研究会」によって発表され、大学においても情報セキュリティマネジメントの基本となる情報セキュリティポリシーを作成し、基本理念、組織体制、利用する情報セキュリティ技術、守るべき電子化情報についての方針を明確化して、本格的に情報セキュリティマネジメントに取り組むことが推奨された。2003年1月には「高等教育機関におけるネットワーク運用ガイドライン」が電子情報通信学会等により作成発表され、大学を含む高等教育機関のネットワークセキュリティの基準が示された。2007年10月には「高等教育機関の情報セキュリティ対策のためのサンプル規程集」が国立情報学研究所により発表され、情報セキュリティポリシーに基づく組織的な情報セキュリティマネジメントシステム策定の機運が高まって行った。

図1に大学における情報セキュリティポリ



国立大学等：平成21年 独立行政法人等の情報セキュリティ対策の現状について
 私立大学：平成17年版私立大学情報環境白書

図1 情報セキュリティポリシーの実施・検討状況

大学における情報セキュリティマネジメントに関する考察

シーの設定状況を示す。内閣官房情報セキュリティセンターが2009年2月に発表した「独立行政法人等における情報セキュリティ対策にの現状について」によると、国立大学法人・大学共同利用機関法人・独立行政法人の中で情報セキュリティポリシーを策定実施済の法人は77%、検討中は13%であった。私立大学に関しては平成17（2005）年度版私立大学情報環境白書によれば、実施済21%、検討中53%であった。私立大学の場合調査より4年が経過しているため検討中のものが2009年現在ではほぼ実施されているとすると、現状では全体の8割程度の大学が情報セキュリティポリシーを策定して情報セキュリティ対策を行っている状況といえる。この割合は独立行政法人メディア教育開発センターが2006年にITを活用した教育を行っている大学等683機関に対して実施した調査において、情報セキュリティに対する対応を行っていない機関が18.3%、であったことでもほぼ裏付けることができる。但し約20%の大学はまだ組織的対策を行っていないとも言える。

情報セキュリティマネジメントシステムはPLAN→DO→CHECK→ACTIONを繰り返して、運用結果、実際のインシデント等の発生結果から情報セキュリティポリシーを定期的に見直しして、リスク分析を繰り返し、定期的な改善を通してより良い状態のセキュリティシステムを維持するリスクマネジメントのシステムである。図2に2009年の国立大学等における情報セキュリティポリシーの見直し状況を示す。これによれば定期的に情報セキュリティポリシーを見直しているケースは全体の10%強に過ぎず、規則等の遵守状況の把握についても30%程度に留まるなど、情報セキュリティマネジメントシステムにおけるCHECK、ACTIONの動作がまだ十分に機能していない状態であることが分かる。また独立行政法人メディア教育開発センターが2006年に行った調査では外部の第三者が公正な立場で情報セキュリティ監査を行っている教育機関の率は1.9%に留まり殆ど行われていない状況であった。

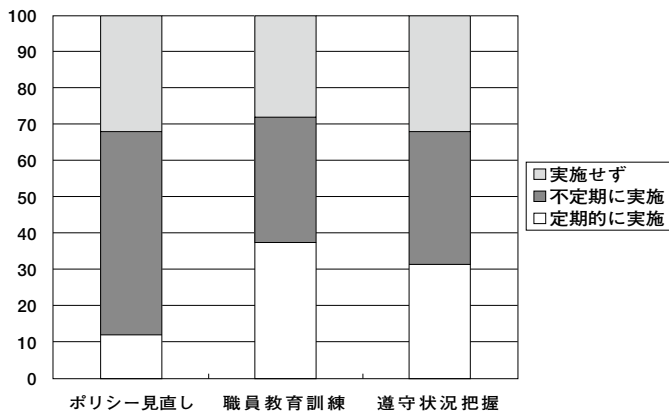


図2 2009年 国立大学等 情報セキュリティポリシーの見直し状況
(平成21年 独立行政法人等の情報セキュリティ対策の現状について)

3. 個人情報保護法の施行

「e-Japan戦略」が実施されつつある中で、2002年には住民基本台帳ネットワークの稼働が開始され、個人情報の漏洩が問題視されるようになった。そこで個人情報の漏洩や不適切な利用を法律で規制する「個人情報保護に関する法律」（以下「個人情報保護法」と称する）が2003年に成立し、2005年から施行された。国立大学等には別途「独立行政法人の保有する個人情報の保護に関する法律」が適用され同様の規制下に置かれるようになった。個人情報保護法は5000人を越える個人情報の保持者に適用され、また対象とする個人情報の定義として特定の個人を識別できる情報（氏名、生年月日等）の他、他の情報と容易に照合することができることによって特定の個人を識別することができる情報（学生名簿等と照合することで個人を特定できるような学籍番号等）も含まれることが明確にされている。従って、大学の有する学生に関する情報もその対象となる。個人情報保護法では個人情報の管理（漏洩防止）と利用に関する規制が定められており、大学を含む学術研究団

体は利用に関する規制に関しては一部適用除外が行われているが、個人情報の管理については他の機関と同様に法的義務を負うことになっている。また個人情報漏洩インシデントが発生した場合に、それまでは公表されることが少ない傾向にあったが、法律施行以降は積極的に公表が求められるようになり、大学でもプレスリリース等で公表するようになった。

4. 情報セキュリティ対策

図3に平成17（2005）年度版私立大学情報環境白書による私立大学における情報セキュリティ対策の実施状況を示す。それによればウイルス対策（ワクチン等）、ファイアウォールなどの基礎的な対策はほぼ実施されていることがわかる。しかし教職員・学生等への周知を目的とした利用者教育は60%強にとどまり、運用組織構築、危機管理対策まで行っているところは半数以下であった。独立行政法人メディア教育開発センターが2006年に行った調査では特に職員への周知・研修を行っている大学等の比率は29.1%と更に低いレベルであった。つまり対策ツールを準備し

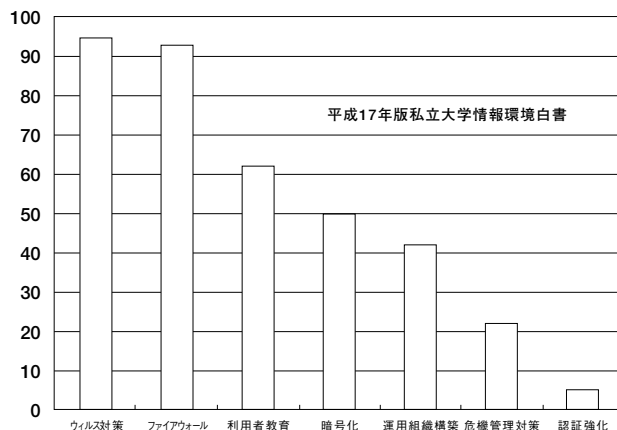


図3 大学の情報セキュリティ対策 私立大学 2005年

て、周知・教育を一部行っているが、組織的展開は開始されたばかりの状況と言える。

5. 公的認証の取得状況

情報セキュリティマネジメントの組織的かつ継続的な実行を保証する目的で、日本においては、初期においてはBS7799、国際規格化以降はISO-27001に基づく情報セキュリティマネジメントシステム（ISMS）の公的認証が行われている。情報セキュリティマネジメントで先行する大学の中にもこれを取得したところが既に出てきている。BS7799規格は下記のように南山大学（大学では世界2例目、国内初）、京都大学がいち早く取得した。

南山大学 名古屋キャンパス・瀬戸キャンパス（教務関連業務）

京都大学 大学院医学研究科医療経済学分野（研究・開発・教育業務）

ISO-27001に関しては、2009年8月現在大学でこれを取得しているのは以下の6校である（日本情報処理開発協会 JIPDECによる）。同期日で、全体では3,252団体が取得しているので、この数は多いとは言えない。

國學院大學 渋谷キャンパス（運営管理業務）

宇都宮大学 総合メディア基盤センター（運営管理業務）

静岡大学 総合情報処理センター（管理運営業務）

日本福祉大学 美浜キャンパス（情報管理全般）

山口大学 大学情報機構メディア基盤センター（管理運用業務）

早稲田大学 メディアネットワークセンター（システム開発・運用業務）

キャンパス全体を対象に認証を受けている

のは南山大学、國學院大學（パッケージ化して他大学等への横展開も予定している）及び日本福祉大学である。他は情報センターまたは研究科単位である。これは認証取得の手間や費用を考慮した結果、情報の集中する重要部門で認証を取得しておき、同じ手法を順次他部門に展開普及させて行くという意図に基づくものと考えられる。

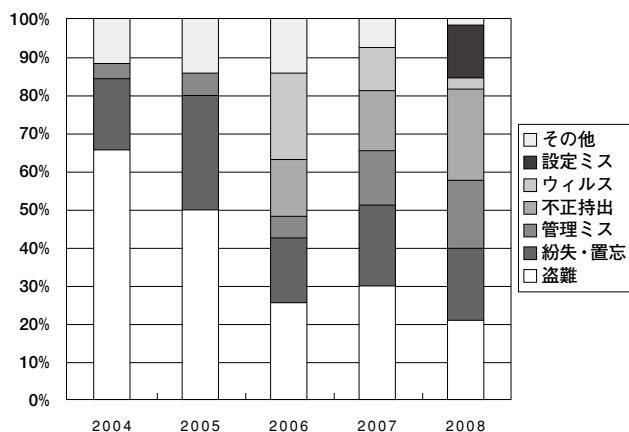
6. 情報セキュリティインシデントの状況（日本）

大学における情報セキュリティインシデントは散発的には報告されているが、情報漏洩事件以外は公表資料が少ない状況である。そこで公表資料の比較的多い情報漏洩事件から最近の傾向を分析して見ることにする。日本ネットワークセキュリティ協会が毎年発行している「情報セキュリティインシデントに関する調査報告書」における業種「教育・学習支援業」（大学のほか予備校、専門学校等が含まれている）の過去5年間のデータから大まかな傾向を把握して見る。

図4に2004-2008年における情報漏洩インシデントの原因内訳を、図5に情報漏洩手段の内訳、表1に発生件数・漏洩数を示す。

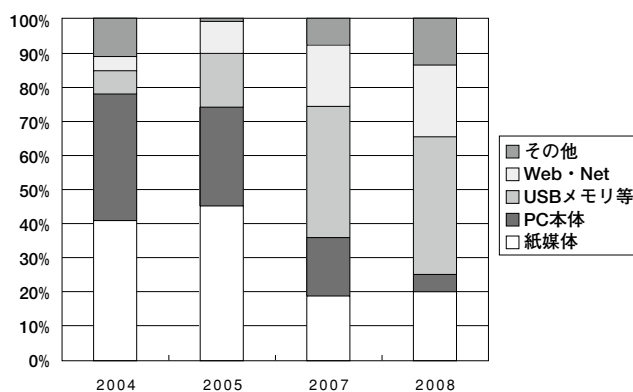
これらより次の事項が考察される。

- ・発生件数は2007年には一時減少しているが、全体的には4年間で7倍の伸びとなっている。
- ・漏洩数は平均的には横這い傾向で、一件当たりの漏洩件数は500-2000件で多くはない。
- ・全産業内での「学校・教育支援業」の比率は年々増加しつつあり、他産業よりも発生件数の伸びが大きい。
- ・原因別では盗難の割合がやや減少しつつあり、管理ミス、不正持出の割合が増加して



(参考：日本ネットワークセキュリティ協会 情報セキュリティインシデントに関する調査報告書)

図4 学校・教育支援業 情報漏洩インシデント原因内訳



(参考：日本ネットワークセキュリティ協会 情報セキュリティインシデントに関する調査報告書)

図5 学校・教育支援業 情報漏洩手段内訳

表1 学校・教育支援業 年次別情報漏洩発生件数・漏洩数等

年	2004	2005	2006	2007	2008
発生件数 (件)	23	81	110	83	163
漏洩数 (万人)	5.0	8.0	4.2	10.8	9.0
全産業内 発生件数比率 (%)	7.4	8.1	11.1	10.2	13.0

(参考：日本ネットワークセキュリティ協会 情報セキュリティインシデントに関する調査報告書)

いる。紛失・置忘は一定割合で発生し、ウィルスによる比率は小さい。

・情報漏洩手段では紙媒体、PC本体の割合が減少し、USBメモリ、Web・Net (Winny等P2Pウイルスによる流出が含まれる)が

激増している。

個人情報保護法との関連で、情報漏洩事例についてはプレスリリース等で公表されるため個別にもインシデント事例の傾向を知ることができる。「大学職員ネット」では毎月プ

大学における情報セキュリティマネジメントに関する考察

レスリリースのあった個人情報漏洩インシデント事例を掲載している。そこに掲載された事例を参考にして公表されたプレスリリースを集計することでその一端を知ることが可能である。表2に2004-2008年の間で集計したインシデント事例を示す（個別の事例を取り上げるのが目的ではないので、大学名、学部名は除いてある、大学付属病院の事例を含む）。

2004-2008年に報告された個別発表事例59例を分析すると次のような点が考察できる。

- ・漏洩した情報量は数件～数百件が多く、前述の「情報セキュリティインシデント調査

報告書」の考察結果と一致している。

- ・漏洩した情報は大学本校の場合学生の成績、医学部付属病院の場合患者の病歴等の個人情報が大半であり、クレジットカード番号等経済的に悪用され易いデータは少ない。
- ・原因別では媒体（紙、USBメモリ、FD、HD等）の紛失・盗難によるものが最も多く21件と全体の36%を占める、次いでPCの盗難が19件（32%）、学内サーバ等の管理ミスが8件（14%）、P2Pウイルスによるものの7件（12%）であった。
- ・意図的な漏洩は一件のみで、他はすべて教

表2 大学別個人情報漏洩事例一覧（2004-2008）

発生	漏洩情報	件数	原因
2004	授業料納付預金口座振替依頼書	68	職員個人が紛失
2004	学生情報	6660	委託先業者の従業員が紛失
2004	学生情報	約40000	情報の入ったパソコン盗難
2005	在籍学生の成績をインターネット上に公開	180	成績データファイルの管理不良
2005	同学科の同窓会名簿、研究室OB名簿	1600	PC 8台HD 4台盗難
2005	公開講座受講者・講師・留学生・職員名簿	不明	PC 8台盗難
2005	文科省補助事業申請書類	1	学長が学内に漏洩、その後学外に流失
2005	学生・卒業生の個人情報	不明	PC 1台の紛失または盗難
2005	卒業生・新入生名簿	約6000	同窓会に速達で送付したCD-ROMが郵送途中で行方不明
2005	学籍簿	54	誤廃棄
2005	入学予定者手続き書類	12	紛失
2005	学部生・大学院生名簿	2133	登録委託業者でノートPC入りの鞆を車に放置し盗難
2005	期末試験答案	114	教員が出張先の外国で鞆を盗難
2005	患者名簿、診療情報	130	学生がPCと名簿の入った鞆を学内で紛失
2005	USBメモリーに入った患者情報	259	学生が車上荒らしに遭う
2006	付属病院の患者データ	41	学生のPCがWinnyウイルスに感染
2006	学生成績簿	63	教員の自宅PCの盗難
2006	成績簿	165	事務室で誤廃棄
2006	夏季集中講義の採点簿	不明	教員から郵送中に紛失
2006	成績簿	不明	教員が車上荒らしに遭う 後で未開封で発見
2006	入試可否判定情報インターネット上に流失	不明	委託業者に渡したサンプルがWinnyウイルスにより流失
2006	学内専用HPの学生情報が外部から閲覧可能	86	ファイルのアクセス件設定忘れ
2006	学生情報システムで登録データ改竄（他学生アクセス可能）	657	ソフトの不具合
2006	学生成績情報	不明	教員がインターネットカフェにHDを置き忘れる
2006	学生情報	13	委託会社の社員PCがWinnyウイルスに感染
2006	教員情報	453	教員がUSBメモリーを紛失
2006	受験合格者のアンケート	864	宅配便で運送中に紛失
2006	専門職大学院学生・教職員データ	1005	無関係のところにメール送信 削除に気づかず
2006	履修者成績情報がインターネット上に流出	506	学生が無断コピー、自宅PCがSharesウイルスに感染
2006	患者情報	9000	PC 8台メモリー6個HD 2台が盗難

埼玉学園大学紀要（経営学部篇） 第9号

2006	「情報処理」履修生の個人情報	204	個人情報を大学サーバーの学外公開用ファイルに保存
2007	履修者成績	300	教員がPC・USBメモリーの入った鞆を電車内で盗難
2007	履修者の個人情報	1267	教員宅よりPC盗難
2007	履修者個人情報・ID・PW	213	教員宅よりPC盗難
2007	学業成績	302	事務室よりPC3台盗難
2007	合格者名簿	972	委託業者がFDを紛失
2007	同窓会名簿	約8000	教員が電車内でHDの入った鞆を盗難
2007	卒論ゼミ履修生個人情報	45	教員の自宅でPCが盗難
2007	履修者成績・個人情報	1026	教員が車上荒らしでUSBメモリー盗難
2007	受講者個人情報	101	教員がUSBメモリー紛失
2007	学会員個人情報インターネット上に流失	17617	職員の自宅PCがSahresウイルスに感染
2007	付属病院の患者情報	85	学生（研修医）が電車内でPC紛失
2007	付属病院の患者情報	22	学生（研修医）がUSBメモリー紛失
2007	付属病院の患者情報	約23万	PCが盗難 データ閲覧困難（ID PW 独自セキュリティ）
2007	寮生の振込データ	215	職員がFDを学外に持ち出し車上荒らしに遭う
2007	患者情報がインターネット上に流出	127	学生の自宅PCがWinnyウイルスに感染
2007	患者個人情報	200	PC16台が盗難
2008	学生の個人情報	337	講義室で教員持参のPCが盗難
2008	学生の個人情報	145	海外出張時持参したPCを盗難
2008	留学生情報等	749	教員が海外出張中PCを盗難
2008	学生個人情報	2550	キャンパスで23台のPC盗難
2008	学生成績情報	800	PC1台の盗難
2008	学生の氏名・学籍番号が2年間以上閲覧可能	1169	データの削除忘れ
2008	成績情報が外部から閲覧可能となる	不明	教員が個人的に外部サーバーに成績情報を入れていた
2008	成績情報が外部から閲覧可能となる	49	教員が個人的に外部サーバーに成績情報を入れていた
2008	学生情報・写真	654	職員が出勤途中でUSBメモリーを紛失
2008	在学生・保証人・卒業生個人情報ネット上で閲覧可能	3198	職員が公開用フォルダーに誤って個人情報をアップロード
2008	ハラスメント質問・相談情報がネット上に流出	719	職員がデータを自宅に持ち帰り、Winnyウイルスに感染
2008	学生・卒業生・名誉教授の個人情報	60	研究室のPCが盗難

職員・学生個人、研究室単位での不注意（単純な盗難はこれに含める）、誤操作によるものである。

- ・学内・学外の別では全体の42%が学内、51%が学外、7%が委託先で発生している。
- ・外部からのハッキング、ウイルス等による被害は報告されていない。
- ・漏洩した情報の悪用等による被害の報告はない。（単に紛失、漏洩のみ）

7. 米国との比較

米国における状況は日本とはかなり異なった様相を示している。米国の大学では2004年に多くの大学で不正アクセス事件が多発した。

中には連続して同様の手口で被害を受けた大学もあった。表3に米国での主要なインシデント事例を示す（大学名は省略、出所は前記「大学職員ネット」等）。

- その傾向を考察すると以下の通りとなる。
- ・セキュリティ対策が実施されている学内のサーバを狙った不正アクセス、情報が入っているPCの意図的盗難が多い。
- ・1回の不正アクセスにより非常に大量の学生、卒業生、職員の個人データが漏洩している。
- ・個人データにはクレジットカード番号、社会保障番号（social security number）など

表3 米国大学個人情報漏洩事例（2004－2008）

発生	流出情報	件数	原因
2004	学生個人情報	59,000	不正アクセス
2004	学生個人情報（写真、社会保障番号、IDカード番号）	32,000	不正アクセス
2004	学生個人情報	700	不正アクセス
2004	学生個人情報（社会保障番号、クレジットカード番号）	106,000	不正アクセス
2004	学生個人情報	145,000	ノートPCの盗難
2004	学生個人情報（IDなど）	7,000	不正アクセス
2005	学生個人情報	98,369	ノートPCの盗難、後に調査して回収
2006	学生情報・特許情報等	約20万	各学部のサーバに3回に渡る不正アクセス
2006	卒業生・在校生・教職員情報	約80万	不正アクセス
2007	卒業生・学生・教職員情報	約70,000	PC3台盗難
2007	在校生・教職員個人情報	約46,000	不正アクセス
2007	在校生・教職員個人情報	22,396	不正アクセス
2008	学生の個人情報・入学願書	約10,000	不正アクセス
2008	学生個人情報	約97,200	旧システムのサーバーに不正アクセス

経済、権利に直接関連した利用価値の大きいものが多数含まれる。

ここで特筆すべきは大学で有する学生等の情報が日本と異なる点である。大学経営の中で「エンロールマネジメント」（学生の入学前から、在学中、卒業後まで細かく支援する）が重視されている結果、在学生のみならずその後の寄付・寄贈等のために卒業生も含めたクレジットカード番号や社会保障番号等個人情報情報が細かく管理されている。米国における社会保障番号は国民の背番号ともいうべきもので、自動車免許取得、クレジットカード作成、銀行口座開設、電話の申込、住宅の契約、公共サービスの利用に必須の情報であり、クレジットカード番号と同等かそれ以上の社会的価値がある。その結果クレジットカード番号、社会保障番号の取得と不正利用・売買を目的として、組織的に不正アクセス等の犯罪行為が実行され利用価値のある情報が一度に大量に取得されていると考えられ、日本に多い不注意・誤操作によるインシデントと比べて集団的犯罪による被害としての傾向が顕著に見られる。

相手が犯罪者であるため、学内の兼任では対応が不可能な場合が多く、大規模な大学（例えばStanford University）では専門のInformation Security Office（ISO）を設置してITセキュリティ専門職による対応、学内権限の行使（インシデント報告義務、対策実施勧告等）を行っているケースが多い。この傾向は米国だけでなく欧州の大学にも見られる。

公的認証については米国の企業自体取得が低調（取得数で日本の2%程度）なこともあり、あまり盛んではないが、BS7799はThe University of Texasがいち早く取得しており、度重なる不正アクセスで手痛い打撃を被ったGeorgia State UniversityなどもISO27001を取得している。

8. 全体考察

以上の点をまとめると全体的には次の諸点が考察される。

① 情報セキュリティ対策

ウイルス対策（除去ソフトの導入等）、ファイアウォール等の定番的な対策はほとんどの大学に導入され、学内では所期の効果を上げ

ていると見られる。

② 情報セキュリティポリシーの見直し

2000年代初期のウイルス、不正アクセス対策に重点を置いた情報セキュリティポリシーは多くの大学で設定されている。しかし実際に起きたインシデント、対策の効果測定、監査等に基づく内容の見直しは組織的に行われておらず、マネジメントサイクルが円滑に運用されているとは言えない状況である。

③ 学外での対策

学外でのインシデントが半分以上を占めているにも拘わらず、これに対する効果的な対策があまり行われておらず、件数は増加する傾向にある。民間企業と異なり、大学では情報を取り扱う関係者が、事務職員だけでなく、専任教員、非常勤教員、学生、出入業者等多岐に渡ることが対策の阻害要因となっていると考えられる。

④ インシデントの原因

日本の大学の場合インシデントはその大半が単純なミス（置き忘れ、紛失、操作ミス等）または不注意（盗難、P2Pウイルスによる流出）によるものである。しかもこれらは既に設定されている情報セキュリティポリシーに基づく規則・規定では禁止（個人情報の無断持ち出し禁止等）または、注意義務を課せられていると推測される事項が大半である。

⑤ 経営に与える影響等

日本では情報悪用等の顕著な社会的被害は報告されていない。また大きな損害賠償事例も知られていない。しかし管理が不十分な状態で個人情報等が流出した事実だけで慰謝料請求等の訴訟対象となる可能性がある（他産業ではそのような事例・判例が生じている）。更に問い合わせへの対応、謝罪の費用等が直接的費用として発生し経営に直接的なインパ

クトを与える恐れもある。悪意がなく、被害が生じていなくてもインシデントの発生事実のみで大学名も含めて公表の対象となるため、大学イメージの低下を招き応募学生の減少等長期的な経営にも悪影響を与える可能性も否定できない

⑥ その他（不正アクセス等）

米国の大学と比べて不正アクセス、悪意による不正取得の件数の報告は極めて少ない。既に行われた各種対策の効果も認められるが、基本的には大学の有する機微情報が少なく、組織的な不正アクセス等の犯罪行為によって情報を取得するメリットが少ないことを意味している。このことは逆の立場から言えば学生に対する「エンロールマネジメント」の役割が米国と比べて少ない結果であり、今後この役割が重視され大きくなって行けば米国と同様の問題が発生する可能性は否定できない。

9. 今後の対策

① 情報セキュリティポリシーの定期的見直し

1-2年に一度は、自校、他校でのインシデント発生状況を勘案して対策の効果を測定し、重点項目の見直しを行うことを行うべきであり、そのための規則（毎年の実施時期）や組織（委員会等）を作成しておく必要がある。学内または第三者（専門機関）による定期的な監査を行い、その結果に基づいて学内の専門員会等で見直しを行うことが有効である。見直しの方向は各校の実状によって異なるが、現状のインシデント傾向から見て次に述べる「単純ミス」、「不注意」への対策に重きを置く方向が望ましい。

② マネジメント組織等の整備

情報セキュリティシステムの運用は大規模な組織になるほど専任組織で行うことが望ま

しい。しかし現状の職員や教員を専任化することは一般的に困難を伴うと考えられ、各大学関係者の報告等からもそのことが伺える。通常の兼任組織での負担が過多になる場合や、リスクの大きさが看過し得ない場合には、十分な事前確認と管理との下で、サーバの管理・監視（ハウジング・ホスティング）や情報セキュリティに関する教育の一部を公的認証取得済の外部機関に委託する方法も検討する必要がある。なお「平成17年度版私立大学情報白書」によれば2005年に私立大学で人的に情報関連の外部委託を行っている割合は約50%であった。またマネジメント組織を補助する仕組みとして、端末における情報入出力を物理的・ソフトウェア的に不可能としたり、セキュリティポリシーに反する行為が行われた場合に自動的に通報・警告する仕組みを組み込むことも有効であると思われる。

③ 紛失・盗難対策

規則や教育では注意するように定めていても、人間の行うことであるため紛失・盗難等は一定確率で常に生起する可能性がある（「残留リスク」が存在する）ものであり、現実にもインシデント原因の中で大きな比率を占めている。情報セキュリティの本来の目的は「情報資産の維持」であるため、紛失や盗難の発生確率を完全にゼロとする対策を考えるよりも、むしろ残留リスクとしてそのような事項が生起しても情報資産が維持され、残留リスクを受容できる対策を考え方が適切である。情報の持ち出しを絶対に禁止することが不可能な場合に効果的なのが、代わりに暗号化を義務付け、その実施状況をチェックすることである。情報を持ち出す場合はUSBメモリの暗号化領域（暗号化機能付の指定USBメモリーを配布・管理し、それ以外の使用を

禁止する方法もある）に入れ、PCやサーバに蓄積する場合にはファイル単位で暗号化（成績表等はExcel/Wordで保存されている事が多いので、Excel/Wordファイルのセキュリティ機能を利用してパスワードを設定し、更に市販の暗号化ソフトまたはWindows標準の暗号化機能でファイルを暗号化しておく）しておき、学内備置のノートPCなど可搬型のPCはディスク全体を暗号化しておけば、紛失・盗難が生じてても情報資産が流出するリスクは非常に少なくなる。USBメモリーやPC本体の価格は下落傾向が続いており、ハードウェアが失われることによる資産価値の損失は内部にある情報の資産価値や不祥事発生時の対応・回復費用と比べると極めて小さいと言えるからである。2007年9月に患者データ23,000件の入ったT大学医学部のPCが盗難に遭ったが、PC自体に独自セキュリティを施してあり閲覧困難な状況にしておいたため大事に至らなかったのはこの好例である。

大学教員は自分の担当する講義に関する学生のデータを持ち歩かざるを得ない事が多く、その場合には必ず紛失・漏洩のリスクを伴うので、このような対策は必須であると考えられる。効果を確実にするために自己チェックリスト等による実施の確認・報告、定期的な実施状況の把握も必要である。

④ P2Pウイルス対策

教職員であっても自宅のPCは家族と共用する場合があります、自己管理を行っているつもりでも他の家族の利用によりP2Pウイルス等に感染するリスクが大きく、実際にそのようなインシデントが多発している。職場のデータは持ち帰らないことの徹底が重要であるが、教員については上記のように学外に持ち歩かざるを得ない事情があるため、③と同様に蓄

積データを暗号化して保存する事を義務付けるのが最も実際である。Excel/Word等にセキュリティ機能と暗号化ソフトによる暗号化の組合せにより、万が一データ流出が起きても具体的な内容が明らかになるのを防止する事が出来るからである。

おわりに

大学も一般企業と同様に、運営上の多数のリスクを内包している。情報セキュリティリスクもその代表的なもので、対策費用が継続的にかかる上に、インシデントが発生すれば直接対応、事後対応等の経済的負担に加えてイメージの低下等見えざる資産価値の減少もきたすリスクがある。不正アクセス、情報漏洩等のインシデントの場合見かけ上は大学が被害者であるが、対策を怠っていた場合は損害賠償や慰謝料請求の対象となる恐れさえある。既に行っている情報セキュリティ投資の効果を生かすためにも、継続的・定期的な見直しを伴う情報セキュリティマネジメントを実践してゆくことが必要である。

参考資料

1. 加盟大学におけるネットワーク不正侵入と対策
私立大学情報教育協会 2000年
2. 侵入傾向分析レポート (株)ラック 2003年
3. 大学における情報セキュリティポリシーの考え方
大学の情報セキュリティポリシーに関する研究会 2004年
4. 独立行政法人等における情報セキュリティ対策
にの現状について 内閣官房セキュリティセンター 2009年
5. 平成17年版私立大学情報白書 私立大学情報教育協会 2005年
6. 大学等におけるICT活用と個人情報保護

ディア教育開発センター 2006年

7. 2004年版-2008年版 情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会 2006-2009年
8. 大学職員ネット <http://blog.university-staff.net/>
9. 大学における情報セキュリティマネジメントの諸問題 京都大学 上原哲太郎 CTCアカデミックユーザアソシエーション 2004年