大学のセキュリティ～IT ガバナンスの視点から～

上原 哲太郎
京都大学学術情報メディアセンター

概要：大学は少子化時代を迎えて強い逆風に晒されている。国立大学ですら急速な運営費削減を求められるなど、その経営効率化は喫緊の課題である。しかし大学に十分な IT ガバナンスがないと、人件費削減に最も有効であるはずの IT 投資が過度に刈り込まれる。この際、情報セキュリティ関連の投資が不要不急として優先的に刈り込まれることがある。本稿では、IT 投資による効率化と情報セキュリティの確保の両立を、大学における IT 投資という視点から考える。

キーワード：情報セキュリティ

1. 大学の情報セキュリティ上の脅威

かつてと比較すれば、ネット社会に占めるウェイトは小さくなったとはいえ、大学はそれでも決して小さな組織ではない。そのため、ウイルスや踏み台などで他の組織に迷惑をかけないように対処することはトッププライオリティである。また、ひところに比べるとだいぶ少なくなったが、大学で発生したインシデントがマスコミを賑わせることがあり、それが大学のブランドを傷つけることになっていた。

そして、先進的であるべき大学は情報セキュリティの脆弱性を解消すべきだという社会からの要請も強い。さらに社会の情報セキュリティに対する意識の高まりと共に、大学は情報セキュリティを担保する技術を研究するべきとか、情報セキュリティ教育を施した人材を社会に送り出すべきという意見も増えている。

2000 年以降、国から情報セキュリティに関する号令がかかるようになっている。現在は第二次情報セキュリティ基本計画に沿って、国の機関の末端である国立大学を中心にした高等教育機関も対策を取るように指示されている。現在、大きなウェイトを占めているのがネットへの個人情報漏洩で、個人情報保護法のコンプライアンスの問題である。実は個人情報漏洩と、個人情報保護法へのコンプライアンスは微妙に違うのだが、世の中では混同されたまま理解されていて、個人情報漏洩を重大視する経営者は多い。そして最後に訴訟リスクへの対応がある。

実際の脅威として大学に降ってくるものとして、外部からのネット越しのハッキングやクラッキングがある。それから、部外者による不正利用も問題になる。分かりやすいのは踏み台だが、公開端末が不正利用されることも起きている。掲示板荒らしの犯人を突き止めてみると、図書室の公開端末が使われていたことなどがある。大学のように開かれた場所では、公開端末と無線 LAN は問題になることが多い。これら以外で外部からの脅威として大きいのが、物理的な盗難である。

こうした外部からの脅威は比較的分かりやすいのだが、内部からの脅威はより深刻な問題である。大学の構成員によるネットワークの不正利用はたまに起きていて、学生によるアタックや P2P ファイル交換などが散見される。

また、現在のところ顕在化していないが、情報の持ち出しや漏洩は情報セキュリティ上の大きな脅威として挙げられる。現在 Wikileaks が話題になっているが、あの手のことが大学で起こることを想像すると戦慄を覚える。入試問題の下書きなどが漏洩した際のインパクトは計り知れない。

これらの番外として、不祥事がある。最近の事例としては、ある教員が自分のブログに不適切な記事を掲載し、ネット上で瞬く間に広がり大騒ぎになったことがある。その結果、大学の電話が鳴り止まず、果ては DOS アタックを受けたりしている。最後は著作権問題で、これはセキュリティの問題ではないが、情報倫理上の問題である。

2. 大学の情報セキュリティの背景

インターネットは大学の実験から始まった歴史的な経緯があり、大学の構成員にとって、大学は無料で通信し放題、サーバ立て放題のプロバイダと化している面がある。そうした既得権を利用して、事件が起きることになる。まず、サーバ管理を学生ボランティアが行っていることが問題の温床となっている。IT システムが本業ではない学科や専攻では、要員や経費などのリソースも不十分なため、学生ボランティアがシステム管理を行うことが

多い。そのため、野放図な管理になっているサーバが出てきてしまうのだが、その根底にはシステム管理は誰でもできるものという幻想がある。

それでは管理を厳しくすればいいのかといえば、厄介なのが学生の存在だ。学生は、大学の構成員として組織統制の中に明確に位置付けられる存在ではないからだ。大学にとってはある意味顧客でもあるので、学則以上に細かいルールを作って守らせようとしてもおのずと限界がでてきてしまう。そのため全体の数パーセント程度であるが、善悪の判断のつかない学生が出てきてしまうのだが、この人たちの対処法は悩ましい。

いろいろなトラブルが起きて対策が必要となると、メディアセンターとか情報センターの出番となるのだが、対策を実施するたびに何かしらの文句を受けることになる。例えば、京都大学はかなり以前からクライアント系のパソコンをローカル IP に閉じ込めているのだが、これは企業では常識だが、大学では必ずしも一般的なことではない。大学でパソコンにグローバルアドレスを振ることは珍しくないのは、ローカルアドレスに閉じ込めてしまうと、研究できないと苦情がくるためだ。外から繋ぎに来る接続アプリケーションを前提とした研究ができないから何とかしろといわれたりする。

一定以上の規模の企業では、アンチウイルスソフトウェアを全てのパソコンにインストールするために強制的なルールが設定されている。しかし、京都大学のように構成員が多い大学で「本学は何々というウイルス対策ソフトのライセンスを全学で取得したので、PC に導入してください」とアナウンスしても絶対に 100％にはならない。その会社は嫌いという人、ウイルス対策ソフトは軽いのが一番という人、セキュリティが一番だからあの製品にしろという人など、いろいろな意見を主張する人がいて、大騒ぎをした挙句にインストールされないことになる。電子メールでも、メールサーバにウイルス対策ソフトをインストールすればいいのだが、京都大学にあるメールサーバの台数は誰も知らないし、どこにあるかも把握できていない状態である。

最近はファイアウォールを導入しない大学はさすがに無いが、そのポートの開け閉めでも問題がおきる。5 ～ 6 年前の事例だが、変なパケットが出ているのでウイルスに感染したかと思って問い合わせると、他大学と Windows の共有ファイルを使ってファイル交換をしようとしていて驚いたことがある。セキュリティ上はありえない話しなのだが、それができないと研究できないと主張する人がいる。

それでは IDS を導入して監視すれば問題ないかといえば、また大学固有の問題にぶつかる。監視するといった途端に、「それは検閲だ」という人がいるのである。

3. 情報セキュリティに対する京都大学の対応

京都大学は KUINS と呼ぶネットワークを持っているが、これは日本の大学の中でもかなり凝ったネットワークの 1 つである。京都大学は歴史的経緯によりクラス B を 2 つ持っているが、図 1 の通りローカル IP に大半のクライアントを閉じ込めた上で、学外に出るときにはグローバル IP VLAN に置いたサーバを踏み台にしないと出ていけない仕組みを全学的に作っている。しかも学内といえども、研究室が違えばローカル IP 同士も通信できないようにすることによって、ウイルスの感染を予防する仕組みになっている。

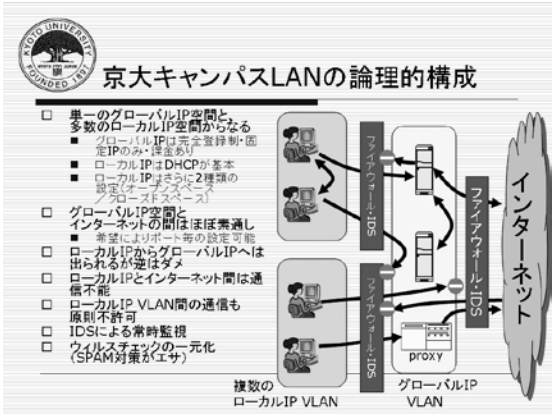

図 1. 京大キャンパス LAN の論理構成

京都大学の情報セキュリティで自慢できることがあるとすれば、全学的なインシデントレスポンスを真面目にやってきた点であろう。外部からの通報、あるいは IDS の監視結果から不正アクセスやボット感染が発見されると、役員クラスを含むネットワーク危機管理委員会が起動するようになっている。この委員会は 24 時間稼動で、連絡に気がついた委員が対処を発議すると、1 人以上の賛同

者が出てきて、1時間異議がなければその対処が実行されるスピーディーな体制が実現されている。

そのため、ボット感染がIDSの監視に引っかかると、最初の委員が気づいてから遅くとも1時間以内に、感染したマシンは学内から切り離されることになる。しかも、感染したマシンの管理者は報告書を部局長に上げた上で、部局長名で役員に報告書を提出しないと隔離が解除されないというペナルティが課せられるようになっている。これは、きちんと対処しないと後々面倒臭いことになるので一定の効果は出ているが、インシデントはゼロにはなっていない。

管理運営側で最近もっている疑念は、インシデント数は減っているのだが、これはIDSの補足率が落ちているためではないかというものである。具体的には、以前から感染していたらしいウイルスが、パターンファイルの更新で発見されるケースが増えているためである。

あと、ネットワークのセンター側はインシデントレスポンスができているのだが、エッジ側は不備な状況が続いている。京都大学は部局自治の原則が明確なので、役員クラスといえども部局の中の構成員の動きはタッチできないので、そこで何が起こっているかよく分からない。その上、対応能力が十分でなくても、現場の人たちが部局自治だからといって頑張ってしまうので、手が出せないことがある。

技術的な問題に比べると、人的問題が発生したときの対応は重くなる。この場合はネットワーク危機管理委員会とネットワーク倫理委員会が起動するのだが、倫理委員会が起動するとプロセスはひどく重くなる。本人が何をやったのか、それが大学の倫理綱領なり何に抵触するのかを一つ一つ積み上げないと、対応が決まらないからである。最近の例では、そのプロセスに半年近くかかったことがあった。技術的な対応だけでは限界はやってくるのである。

インシデントの発生が増えると、ネットワーク危機管理委員会からユーザ教育の強化が指示される。それに応えるべくユーザ教育用にe-ラーニングシステムを数年前から導入しているが、これがまた大変な問題を抱えている。全学認証が稼動しているので全ての教職員と学生がe-ラーニングコンテンツを学習できるようになっている。しかし4月に入学した学生に口を酸っぱくして、ゴールデンウィークまでにe-ラーニングの受講を完了するように伝達したのだが、12月現在で受講率は2割程度の状態である。教職員に対してもいろいろな機会を捉えて受講を呼びかけているが、温度が低い部局は動かない。最近、部局長名で未受講者に通知が行く仕組みを作り、受講率を上げるべく努力しているが、なかなか結果になっていない。

あと、京都大学はセキュリティポリシー作成にも力を入れている。だが、マネジメントがうまく咬み合っていないので、部局によってはセキュリティポリシーがあるだけという状態になっている。マネジメントの欠乏は、根本的な問題として残っている。

一般的に情報セキュリティマネジメントとは、情報資産を決定し、それに対していわゆる情報のCIA（機密性・完全性・可用性）を維持することである。セキュリティポリシーはこの目的達成のために、セキュリティ基本方針、実施対策基準、実施手順という三段階の文書を作成するようになっている。本学では、基本方針と実施対策基準の中間に規定を作成し、実施手順は各部局が雛形を使って穴埋めで完成できるようにしている。こうして出来上がったセキュリティポリシーを活用してPDCAサイクルを回すことになる。

京都大学でセキュリティポリシーの全改訂が行われたのは1回だが、追加規定を作成したので、大きくいうと2周したという感じだ。国は毎年PDCAを回すように指導しているが、とてもそのようなスピードでは回らない状況である。セキュリティ監査も全部局対象に毎年実施するのは困難なため、五部局ずつ監査するのが精一杯だ。

4. 大学の組織的問題点

ガバナンスに関して一番大きい問題は、命令指揮系統がよく分からないことだ。国立大学は図2のような構成員で出来上がっている。学長や総長の下に役員がいるところまでは法律で決まっていて、最高の了承機関として部局長会議がある。その下に部局があり、さらにその下に小さな会議体があり、最後に講座があるというピラミッド構造になっている。

図 2. 大学の組織的問題点

このピラミッドの他に、事務方が存在している。京都大学では本部事務を廃止したが、総務担当理事の下に本部で働く職員が直接ぶら下がる格好になっただけで、実質はあまり変わっていない。

また各部局の中に、部局の学生の成績を管理する事務方が存在する。本部事務が教務用サーバを一括管理しているため、業務フローの観点からすると、本部事務と部局事務のあいだで仕事が完結してしまうことが多い。このため、部局に関する権限は部局長にあるにもかかわらず、部局事務が部局長にお伺いを立てることは多くないのが実情である。部局事務は、本部事務と部局の二重統治のような格好になっている。

さらに学内にはいろいろな種類の壁が存在する。まず部局自治という壁がある。講座の教員と部局の関係は、個人商店主と商店街の関係に似ていて、組織の論理よりは教員のエゴが優先されるところがある。

特に、IT に関していうと、予算システムがボトムアップ調達になっているための問題が起こっている。ボトムアップ調達では部門間の調整が働かず、IT システムは縦割りの体制が残りやすい面がある。さらに、事務方は IT が絡むと逃げ腰になる文化があり、業者に丸投げするか、情報センターの教員に任せる傾向がある。

そして、学生はそもそもマネジメントの枠外にある。私物パソコンの持ち込みが禁止できればウイルス対策も楽になるが、そうはいかないので大変だ。対策として検疫ネットワークを導入すればよいのだが、そんな費用的余裕はない。そして留学生に至っては、常識が違う。特に著作権関係のトラブルは、特定の国々の留学生に対しては大問題になる可能性がある。

5. 危機がやってきた

2010 年、国公立大学に前代未聞の予算削減圧力がかかり京都大学も大騒ぎになった。国が決定した中期財政フレームの中で、3 年間で 10％ほどの経費削減することになったのだ。人件費に手をつけずに 10％の経費削減を実現しようとすると、運営経費を 2 割から 3 割程度削減しなければならなくなる。

そのため、大学は血眼になって削り代を探しているが、狙われているのが IT だ。レンタル予算は金額が大きく目立つし、その上レンタルは大変厄介な存在だ。計算機センターで調達するコンピューターシステムは、レンタル契約が 5 年間から 6 年間続くので、その期間中は落札金額の支出が継続して発生することになる。そうなると、今回のようなケースで 3 年間で 2 割の経費削減を指示されても対応は困難だ。そのため、財政官から 5 年後に経費を削られても耐えられるような調達をするようにいわれている。そうした費用削減に耐えられる調達を行うためは削り代が必要だが、セキュリティは不要不急と判断されかねない。

現状の CIO や CIO 補佐官は、個人情報保護やセキュリティも大事で、サービス低下も認めないとの立場だ。一般的に調達は、業務効率化・利便性向上・安全性確保の三つのバランスが取れていることが望ましいが、今のままでは安全性確保が削り代に使われる可能性が高い状況だ。

6. IT を使った大学の業務改善

IT を使った業務効率の改善をうまくできればセキュリティ予算も確保できるはずだが、これがまた壁にぶつかる。そもそも業務改善は定型業務を集中管理して、事務的な中間チェックを中抜きして、場合によっては外注や無人化をするのが常套手段だ。

大学でいえば同一の業務を探し出して、同一システムに集約すればいいわけである。京都大学には 10 学部あるが、歴史的事情があって 10 学部の業務システムは別調達のパッケージが使われている。これを集約にあたっての致命的な問題は、学部毎に運用ルールが全く違っていることだ。単位認定ルールなどは複雑怪奇で、カスタマイズ費用ばかり掛かって、同一システムに集約することは不可能

に近いのだ。

そこで統合の前提として業務をテンプレート化して、この範囲の中で我慢するよう説得を行っている。一方でシステムを連携させるためには認証の一元化が必要である。そこで京都大学も認証統合を行い、全教職員が一つの ID とパスワードでいろいろなシステムが使えるようになった。それから教職員ポータルと学生ポータルも構築した。2010 年度から電子メール管理の一元化が始まり、教職員に全学共通メールアドレスが配られるようになり、さらに 2010 年 12 月には学生用と教職員用のメールシステムの統合が実現している。

また KULASYS という教務システムを学内で開発して、教務システムの統一展開ができるようになり、手を挙げた学部から導入が始まっている。それから、グループウェアも一元運用されるようになった。

さらに大きいのは情報メディアセンターが、仮想環境を使ったホスティングサービスを学内に展開するようになったことだ。学内に転がっているサーバのセキュリティ確保を一元化する素地ができたわけである。

集中管理により､経費の削減ばかりでなく、セキュリティの向上も期待できる。いいかげんなサーバ管理者からサーバを剥ぐことができ、システム全体に同一のセキュリティポリシーが適用しやすくなるからだ。

一方でサーバ上のアプリケーションのセキュリティはなかなか向上しない。業務システムを外注するとパッケージを買うことになるが、大学という狭い市場向けの WEB パッケーにはセキュリティホールはよくあることだ。

それから、サーバを一元管理すると、そのシステムが停止すると大学全体のシステムが止まってしまうインパクトの大きさがある。これを改善するために、京都大学では電源対策を行っているが結構なコストが掛かっている。

さらに統合認証の頭が痛いところは、一旦破られると終わりというところだ。同じ ID とパスワードで電子メールも給料明細も見られるシステムなので、簡単なパスワードにしていると大変なことになる。かといって認証方式を強固にすると、面倒くさいといわれて使われないことになる。京都大学では電子メール ID とグループウェア ID が同一なので、学外からメールを読む手段は安易に提供したくないのだが、それに反対する意見があって戦いが起きている。これらの対策としては複数の認証方式を提供するしかないが、実装には悩むところが多い。

7. これからの大学に必要なこと

そもそも、大学にとって本質的な IT リスクはどこにあるのだろうか。

経営陣も教員であり、情報センターも教員組織であるため、これまでのインシデントは研究用サーバとか学生のパソコンなどの教研系システムに関するものが多かったが、本質的なリスクは事務系システムの方が大きいといえるだろう。研究用サーバがクラックされるのも問題なのだが、学生の成績が全部入ったサーバをクラックされるよりはずっとましだからだ。そのため事務系システムにセキュリティ対策を施す必要性は高いのだが、教員である役員の事務系システムに対する現場勘は限界がある。そこで、役員の近くに IT と業務とセキュリティに強い人材を置いて、その判断を助ける必要が出てくると考えている。発生する問題は技術だけでなく、法律、会計など多岐の分野にわたることが予想されるので、理想としてはそうした広範な知識を有していて、なおかつ役員方とコミュニケーションがとれる人材が望ましい。これは世の中で不足している人材で、インターネットセキュリティ計画において高度セキュリティ人材とか高度 IT 人材に定義されている。

この人材に必要となるスキルを整理すると、業務効率化の牽引力、システムデザイン能力、セキュリティ対応能力になる。これらの能力はかつて IT 技術者としては当たり前だったもので、これは誰でも到達できる水準だと考えている。

今後は、それらに加えさらに異なる能力も必要になるはずである。それは、まずインシデント対応力である。今後、Wikileaks や YouTube に情報漏洩したコンテンツが公開される可能性もあり、そうした場合の対応、あるいは防止対策が必要になってくるからだ。また、刑事事件が起きる可能性があり、大学に警察が入ってきた場合にフォレンジック技術が必要になってくる。つぎに大学もコンプライアンス対応が厳しくいわれるようになってきているので、個人情報保護法を理解していることが必要だし、セキュリティポリシーが展開できる能力や、会計も IT 化されると不正が発生する可能性が高まるので IT 統制の能力が必要になる。いわばスーパーマ

ンのような人材を学内に抱えることが必要になるのだろう。

大学は最高学府であり、最高級の教員がいるのだから、率先して IT 統制など先進的なことに取組むべきで、そうした中で高度 IT 技術者を育てるべきである。そのためには、IT 人事設計を見直し、広義の IT 投資として取り組むことが必要となる。

これまでの大学はガバナンスが効かないために、セキュリティもうまくいっていなかった。しかし、いまや予算削減圧力は大変厳しく、IT ガバナンスや IT 統制が不可避な状況になってきている。こうした現状の危機的状況を逆にチャンスにして、大学に IT 統制を導入し、メリハリをつけてセキュリティも確保できるならば、一挙両得になるではないかと考えている。

注記

本原稿は 2010 年 12 月 8 日の CAUA シンポジウム 2010 in 大阪での講演を、CAUA 事務局が文書に纏めたものです。従いまして文責は CAUA 事務局にあります。