ネット社会のリスクと大学の対応

新保史生（しんぽふみお）
（筑波大学大学院　図書館情報メディア研究科　准教授）

一　はじめに

大学におけるネットワーク利用は、インターネットアクセスや電子メールなどの基本システムの整備から、グループウェアを利用した授業支援や履修登録、成績管理、Wikiを利用したシラバス作成など、Web2.0時代に対応した様々なシステムの導入が進んでいる。これにより、ネットワークの利用による様々な恩恵を享受することができるようになった。その一方で、日常的にネットワーク利用をめぐる様々な問題が生じている。

ところが、ネットワークにおいて生ずる様々な問題については、大学が把握することができる事案は文字通り氷山の一角である。万引きや喧嘩など、実社会において目に見える形で発生し対応しなければならない問題とは異なり、目に見えず実態がよくわからないところが対応に苦慮する最大の要因となっていると言えよう。

二　大学におけるネットワーク関連の危機管理

では、大学としては、どのように対応すべきか。常日頃から問題が発生する前に、リスク管理のために必要な対策を事前に講ずることが望ましいと考えられるが、事前にすべての対応を検討し実施することはなかなか難しいのが現状であろう。

最近では、組織が事業を継続するにあたって想定されるリスクを事前に把握し、そのリスクが顕在化した場合の対応を事前に策定する「コンティンジェンシー・プラン」のような緊急時対応計画の策定の必要性が認識されている。

ところが、大学における危機管理対応は、事前対応がなされている部分は極めて少なく、事後対応によることが大部分ではないだろうか。リスクが顕在化してから、ようやく会議を開いて対応を検討するようでは適切な対応ができるはずもないが、現実はそうであろう。

企業が危機管理対応を誤った結果、事業の継続が困難になる事例が発生していることは周知の事実であるが、大学はそういった問題とは無縁であるはずがないにもかかわらず、危機感に欠ける部分があることは否めない。

三　具体的な問題

ネットワーク利用との関係で、大学で対応しなければならない問題は非常に多く、対応事項は日々増加の一途をたどっている。

現実に生じている問題として日常的に対応が必要な事例としては、ファイル共有ソフトを悪用した著作権侵害への対応、インターネットの掲示板やSNS（ソーシャル・ネットワーキング・サービス）における名誉毀損や誹謗中傷への対応、架空請求などの振り込め詐欺被害の防止、犯行予告情報への対応などが対応事項としては頻度が高いように思われる。

四　ファイル共有ソフトの利用に伴う問題への対応

P2Pによるファイル交換の問題は、大学におけるネットワークの危機管理との関係で、様々な問題が複合的に生じている事例といえる。

P2Pの利用と大学のネットワーク管理との関係においては、①ネットワークのトラフィックの増大、②違法コンテンツの流通、そして、③情報漏えいの原因などの問題が生じている。

1　ネットワークのトラフィックの増大

大学のネットワーク資源は限られており、特定の時間帯に大量のファイル交換が行われることで、ネットワークに

相当な負荷が掛かり、インターネットのトラフィックが増大することで、ネットワークの「渋滞」を引き起こす要因にもなっている。

対策としては、違法コンテンツや情報漏えいなどの対策とあわせて、学内ネットワークに接続されるコンピュータからファイル交換ソフトを排除することはもとより、当該ソフトがインストールされたコンピュータの接続の制限を学内に周知することが重要である。その上で、ファイル交換ソフトの利用を検知・遮断するツールの導入を検討するなど、ネットワーク管理にあたって必要な対策を講ずることとなる。

2　違法コンテンツの流通

違法なコンテンツの流通については、無断複製した音楽ファイルや映画、アプリケーションのやりとりなど、著作権法違反にあたるコンテンツのやりとりが横行しているが、P2Pのファイル交換ソフトを利用して行われる場合、その大部分が違法に複製されたコンテンツであるといっても過言ではない。

現行の著作権法では、私的使用のための複製（著作権法三〇条）であれば、たとえ違法に複製されたコンテンツであっても、そのコンテンツをダウンロードする行為は私的使用のための複製として著作権侵害には当たらない。しかし、P2Pのファイル交換ソフトの仕様上、「純粋なダウンロード行為」のみを行うことは困難であり、通常は、ダウンロードされたコンテンツを他の利用者が検索可能な状態に置かれている。よって、違法コンテンツが送信可能化状態におかれていることが多いため、不正コピーしたコンテンツをネット上で公開しているのと同様であり、公衆送信権侵害にあたる可能性が高い。

ファイル共有ソフトの利用に伴う著作権侵害への対応については、事前と事後の両方の対応が必要となる。

事前対応については、学内ネットワークから排除することであるが、その対応は前述の通りである。

一方、事後対応は、違法コンテンツの流通について学外組織から著作権侵害にあたるとの指摘を受けて対応する場合と、情報漏えいが発生した場合の対応である。

教職員や学生が個人的にファイル交換ソフトを利用して著作権侵害を行っている場合、学内ネットワークを経由したファイル交換ソフトの利用が制限されている場合には、法令遵守について指導不足という道義的責任は問われるものの、大学の管理責任が直ちに問われる可能性は低い。

一方、学内ネットワークにおけるファイル交換ソフトの利用を特に制限をしていない場合には、学内ネットワークを通じて行われる違法行為に関して大学の管理責任が問われる可能性がある。

そのような行為が発覚した場合の具体的な対応は、ケース毎に異なるものの、ファイル交換ソフトのインストール事実の確認、著作物の無断複製事実の確認、著作権侵害にあたると指摘された無断複製データの存在の有無の確認、ファイル交換ソフトを利用したダウンロード行為及びアップロード行為の有無の確認、ウィルス対策実施の有無の確認、ファイル交換ソフトへのウィルス感染事実の確認など、問題がどのように発生し、どのような著作権侵害事実があったのか的確に把握することが必要となる。

3　情報漏えいの原因

個人情報の漏えいをはじめとして、ファイル交換ソフトの利用が情報漏えいの要因となっていることも周知の事実である。

大部分の大学は、大学が管理するコンピュータへのファイル交換ソフトのインストールは排除していると考えられるが、情報漏えいは、教職員や学生個人が自宅で使用しているパソコンから起きている。

とりわけ、教職員からの漏えいについては、本人はファイル交換ソフトの危険性を認識しており、パソコンにインストールしていなかったものの、家庭内でパソコンを他の家族と共同で利用している場合に、家族がファイル交換ソフトを教職員本人には知らないうちにインストールして利用した結果、情報漏えいが発生してしまったという事例が散見される。漏えいの発生原因は、ファイル共有ソフトの設定に不慣れな結果、インターネットで共有されるフォルダに情報が保存されてしまっていたり、ウィルス対策ソフトの導入を怠っていたりウィルスの定義ファイルを更新していなかったりと、大部分が人為的要因によるものである。

なお、情報漏えいを予防するために、ノートパソコンの持ち出し禁止などを規則で定めるところも増えてきているが、大学の場合、持ち出しを禁止したとしても持ち出さざるを得ない状況が多いのが現状である。その結果、ノートパソコンそのものは持ち帰ることができないため、USBのメモリスティックなどに保存して持ち帰るなどして、自宅のパソコンで作業をすることとなる。これにより、帰宅途中でUSBメモリを紛失してしまうことや、自宅のパソコンのウィルス感染や、不知のうちにインストールされ家

族が利用しているファイル共有ソフトなどから、大規模な個人情報の漏えい事件が発生している。

個人情報などの管理が必要な情報を安全に管理する際に、このような問題を防止するためには、現状にそぐわない規制を設けないこと、不必要な情報は持ち歩かないこと、持ち出す場合には漏えいや紛失を防止するための対策を講ずることが重要である。

五　名誉毀損・誹謗中傷への対応

真面目に講義を受講している学生であっても、インターネットの掲示板では他人を誹謗中傷する発言を繰り返していたり、友人や男女関係のもつれなどによって他人の名誉を毀損する書き込みをしてしまったりすると事例も多い。また、最近では、ＳＮＳのコミュニティでも同様の問題が生じている。

インターネットでは、ごく普通の学生が容易に犯罪に走ってしまう可能性があるだけでなく、自分の行為が犯罪として処罰の対象となっているという自覚がない点が恐ろしいところである。名誉毀損が刑法に定められている犯罪であると認識している学生が、どれほどいるであろうか。

1　プロバイダ責任制限法に基づく対応

学内のネットワークを経由してネット上で他人の誹謗中傷や名誉毀損に該当する書き込みがなされた場合、大学としては、プロバイダ責任制限法（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）に基づく発信者情報の開示や書き込みに対する削除要求への対応を行わなければならないことがある。

プロバイダ責任制限法は、ネットワークにおいて権利を侵害された人物が、発信者を特定するために発信者情報の開示を求める手続と、権利を侵害されたと主張する者から、侵害情報の削除要求がなされたときの手続を定めた法律である。

2　発信者情報開示

発信者情報開示とは、ネット上での書き込みによって自分の権利を侵害されたと主張する者からなされる、情報の発信者を特定する上で必要な情報の開示請求のことをいう。

開示請求に応じるには、①侵害情報の流通によって開示の請求をする者の権利が侵害されたことが明らかであるとき、及び、②開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるときの、二つの要件を満たしていることが必要となる。

3　削除要求

学内で管理している掲示板などの書き込みについて大学に削除要求がなされた場合には、書き込みを削除するか否か検討しなければならない。

権利を侵害されたと主張する者から、大学の管理下にある掲示板の書き込みについて侵害情報の削除要求がなされたときに、大学が削除を行わなかった場合、権利を侵害されたと主張する被害者に対する賠償責任を負うことになりかねない。なお、①他人の権利が侵害されていることを知っていたとき、又は、②違法情報の存在を知っていて、他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるときに該当しない場合には、侵害情報を削除しなかったことによる被害者に対する賠償責任を負わない。

一方、侵害情報の削除を行った場合には、情報の発信者との関係での責任が問題となるが、この場合は、①他人の権利が侵害されていると信ずるに足る相当の理由があったとき、又は、②権利を侵害されたとする者から違法情報の削除の申出があったことを発信者に連絡し、七日以内に反論がなく削除した場合には、発信者に対する賠償責任を負わない。

六　振り込め詐欺被害の防止

振り込め詐欺とは、サービスなどを何ら利用していないにもかかわらず代金を請求する「架空請求詐欺」、家族などを名乗ってお金を振り込ませる「オレオレ詐欺」、お金を貸すのでとりあえず保証金を振り込むように指示をする「融資保証金詐欺」、そして、公的機関から還付金があると偽って振込を行わせる「還付金請求詐欺」などがある。

振り込め詐欺に関する詳細な情報については、警視庁「振り込め詐欺」<http://www.keishicho.metro.tokyo.jp/seian/koreisagi/koreisagi.htm>（二〇〇八年七月二〇日確認）を参照されたい。

大学に関連する事例としては、学生が自宅でアダルトサイトなどを閲覧して、架空の代金請求画面が表示されてしまい、親にバレるのではないかといったことをおそれて架空請求に応じて代金を支払ってしまう架空請求詐欺や、卒業式の直前に、大学の職員を名乗った人物から学費未納の

ため卒業が取り消されるとの電話があり、卒業式までに残りの学費を納付するよう指示するオレオレ詐欺などがある。

真面目な学生ほど、詐欺犯の指示通りに期限までに請求された代金を支払ってしまう傾向があるように思われる。また、学生本人との連絡を、日頃からメールだけの連絡ですませている親ほど、本人と連絡がとれず詐欺犯に学費を支払ってしまうおそれすらある。

たとえ日頃から本人と電話で連絡をとっていたとしても、こういった電話がかかってくるのは、午前一〇時から午後二時までの時間帯が多いといった傾向もあることから、日中、講義を受講中の本人とは連絡がとれない可能性も高い。

振り込め詐欺への対策は、「すぐにお金を振り込まない」ことである。ところが、利用していないサービスには代金を支払う必要がないことは誰でも知っており、オレオレ詐欺が世間でこれほど問題になっていることも誰もが知っているにもかかわらず、お金を支払ってしまう事例が後を絶たない。

つまり、サービスを利用していないにもかかわらず、ウェブサイトにアクセスした後に、代金請求の画面が表示されてしまうと、あたかも利用してしまったかのような気になったり、自分がアクセスした時のＩＰアドレスや大学のドメイン名が画面に表示され、相手が自分の個人情報を把握していると勘違いしてしまい、代金を支払わなければ大変なことになると思いこんだりしてお金を支払ってしまうのである。

架空請求については、冷静に考えて代金を支払わないようにするほか対策はないことから、そのように周知徹底するよりほかない。

一方、オレオレ詐欺については、まさか自分のところにオレオレ詐欺の犯人から電話があろうとは夢にも思わないというのが被害に遭ってしまう大きな要因のようである。

そこで、本人との間では、携帯や自宅の電話など、本人と確実に連絡がとれる方法で日頃から連絡をとりあうことが重要である。また、大学や公的機関からの電話の場合は、「コールバック」が有効である。コールバックとは、こちらから折り返し電話を掛けて確認をすることであるが、確認のために、着信した番号に折り返し電話をしてしまうと、詐欺犯やその関係者に電話を掛けてしまうことになり、要件内容の確認にはならない。くれぐれも、着信履歴にコールバックしてはならない。

コールバックをする電話番号は、事前に大学から通知されている連絡先電話番号や、それがわからない場合は、大学の「代表電話」である。また、公的機関についても、電話帳や１０４の電話番号案内から代表電話を調べ、代表電話にコールバックした上で内線で担当者につないでもらうという方法がよい。

七　おわりに

大学におけるネットワーク関連の危機管理が難しいのは、具体的にどのような対策をとればよいのか、何をどの程度教えればよいのか、対策を講じる側にとっても実感が湧かないことが多い点にある。

その理由は、情報化社会における問題の多くが日々変化し、違法・不正行為等が関係者の不知・不識のうちに発生していることが多く、実社会における問題とは異なり事案の深刻さに対する実感が薄いことが影響していると考えられる。例えば、事務室などに泥棒が入ると大騒ぎになるが、コンピュータへの不正アクセスによる情報漏えいや不正利用には気がつかないことさえあるであろう。

大学におけるネットワーク社会における危機管理には、ネットワーク管理に必要な具体的対策と、法令遵守意識の社会的高まりに応じた情報教育が求められている。

しかしながら、短時間にすべての疑問を解決する上で必要な情報を提供することは困難である。そのため、結果的に問題解決への適切な「解」を見いだせないまま対応せざるを得ない状況を残しているのも事実である。

ネットワーク関係のリスクに対応するためには、学内において総合的・包括的な支援体制を構築した上で、学内規則の整備や対応手順の明確化、対策を講ずる上で利用可能な情報の所在の把握、時宜に応じた的確な対応、関係機関・専門職種との適切かつ迅速な連携に取り組むことが求められており、これらを最大限活用することで具体的取り組みへの実感（バランス感覚）が涵養されることを期待したい。