ネットワークのリスク管理を考慮した情報教育

武田俊之　雄山真弓
関西学院大学情報処理研究センター

概要

コンピュータ・ネットワークの急激な普及に伴いインターネットをはじめとするコンピュータ利用においてリスクが増大している。今後の情報教育においては、従来のリテラシー教育や倫理教育だけでなく、リスク管理を個人の責任においておこなうことが出来るような内容を組み入れた教育が必要であると思われる。そのためには（1）パスワードやファイルなどは個人が責任をもって管理すべきであるという認識、（2）資源へのクラッカーなどによる利用権限の違反への対処、（3）他者の著作物などの知的所有権を侵害しない、などを教える必要がある。

The Prevention of Risks in Computer Network as Part of Introductory Computer Science Education

Toshiyuki Takeda(takeda@kwansei.ac.jp)
Mayumi Oyama(oyama@kwansei.ac.jp)
Information Processing Research Center
Kwansei Gakuin University

Abstract

The rapid expansion of the use of computer network is followed by increased problems in its risk management. It is no longer sufficient for computer science education to deal with only computer literacy. Students taking computer science courses should be made aware of various risks involved in the management of computer network and should be introduced to possible ways of preventing them. The most serious issues are: (1) the administration of individual passwords and files, (2) the defense against crackers and hackers, and (3) the protection of individual copyrights.

1．はじめに

現代はリスクにあふれた時代だといわれる。もともと自然災害や病気などのリスクは存在したが、社会の発達とともに個人のリスクは次第にコミュニティに共通のリスクにひろがっていった。さらに交通網や電子的ネットワークの発達によって地球が狭くなると地球規模のリスクの存在が大きな課題となってきた。そして社会の変化の激しさもリスクを増大させる原因となっている。

特にインターネットに代表されるようにここ１０年のコンピューティングは急激に変化、発達をつづけている。もはやコンピューティング活動なしで企業経営は成立しえないし、家庭生活もまったくコンピューターの影響なしの暮らしは考えられない。

それにもかかわらず、急激に大きくなった社会的影響にくらべて、その情報技術の性質は充分に解明されているとはいいがたい。たとえば、ネットワークだけをとりあげても、誹謗中傷の蔓延するコミュニケーションやプライバシーの公開の問題、知的所有権の侵害、ポルノの問題、コンピューター・ウイルスの蔓延、クラッカーによる不正などさまざまなリスクが問題視されている。実現した現象だけをとりあげてインターネットは危険であるとか規制すべきであるという意見も少なくない。

もちろんネットワークは効用があるからこそ発展をとげてきたのであり、大きな効用が得られる一方で負の結果をもたらす可能性もある。問題はどのような損失があり、それはどれほどの頻度で発生するか、発生した損失の大きさはどれぐらいかということを事前に予測することであり、その予想される損失をいかにしておさえるかである。

このような危険を管理する手段として、企業経営ではリスク管理を発達させてきた。本

稿ではコンピューティングにおけるリスクの分類と性質を論じた上で、情報教育の中にリスク管理を組み込むことを提案する。

2．リスク管理とは何か[1]

リスクはどこにでもあり、どのような行動にもつきまとうものである。予想される行動の結果のうち、損失を発生せしめる可能性がある状態がリスクである。したがって、完全に知ることはできず、あくまでも不確実性をともなうものだけがリスクである。不確実でないなら予測可能で完全にコントロールできるものであるのでリスクではない。リスクとは与えられた状態の元で一定期間中に起こりうる結果の変動であるということも可能である。結果の変動において、損失を減少するための管理活動がリスク管理である。

2.1 リスクの分類

日本語で「危険」といわれる語は、英語では、リスク（risk)、ハザード（hazard)、ペリル（peril）の３つに使い分けられる。

ペリルは損失発生の直接の原因を指す概念である。たとえば、「自動車の衝突」というリスクはペリルである。ペリルは以下のように分類ができる。

1. 人命に関するペリル
2. 資産に関するペリル
3. 責任に関するペリル
4. 輸送用具の運行に関するペリル

コンピューティングにおいては、主に資産と責任に関するペリルが考えられる。

ハザードはペリルによって生じる損失の頻度と強度を増加させる状態を表す。「自動車の衝突」というペリルに対して、「凍った道路」がハザードの一つとしてあげられる。ハザードには(1)物理的ハザード、(2)モラル・ハザード、(3)モラール・ハザードの３つがよくあげられる。モラル・ハザードは損害に無関心であるか、故意に損害発生の防止や軽減に努めないことである。モラール・ハザードは一般的には保険をつけたために発生した損害に無関心な態度をとることである。それ以外にも精神的ハザードとして、否定的あるいは消極的精神状態が損害の頻度や強度を増す状態を上げる場合もある。

2.2 純粋リスクと投機的リスク

リスクには純粋リスク(pure risk)と投機的リスク(speculative risk)がある。純粋リスクは自然災害や病気などのようにその実現が損失しかもたらさないものである。一方投機的リスクは事業計画や金融投資のようにその実現の結果、利益と損失のどちらの可能性もあるものである。

一般に純粋リスクは大数の法則が成り立ち、それゆえ保険によるロス・コントロールが可能になる。投機的リスクは保険が成立しないといわれてきたが、昨今の金融商品やカントリーリスクではロス・コントロールの技術が確立しつつある。

コンピューター犯罪は純粋リスクであるとされる。しかし、コンピューティング活動の視点においては、個人の生産性向上という利得で見れば、投機的リスクの意味合いが強いといえる。個人はリスクを内在している活動としてコンピューティングをとらえるべきであり、ロス・コントロールを活動に組み入れなければならない。

---

[1] 本節の定義は主に文献 1)による。

2.3 リスク管理の計画

リスク管理の手順は以下の５つのプロセスに従って行う。

(1) 危険の発見・確認
まずリスクを発見し、確認する必要がある。もし、ここでリスクを見逃すと、リスクへの対策をとる機会を失うことになる。

(2) リスクの測定
次に発見されたリスクに関連する損失を測定しなければならない。損失がどれぐらいの確率で起こりうるかという頻度と、損失の影響がどの程度の影響があるかという強度の２つが主な測定項目となる。

(3) リスク処理手段の選択
測定されたリスクの頻度あるいは強度を減少させるための手段を選択する。

(4) リスク処理手段の実行
選択されたリスク処理手段を実行する。

(5) リスク処理手段の監査
実行されたリスク処理手段が適切に実行されているか、また、上記プロセスが適切であったかについて監査する。

3．コンピューティング・リスクの発見

情報教育にリスク管理を組み込む場合、上記の５つのプロセスに従ってリスク管理を教えなければならない。その中でも特に重要なのはリスクの発見と処理手段の実行である。本節ではまずリスクの発見について述べる。次節でリスクへの対策について述べる。

3.1 個人のリスクの分類

コンピューティング活動における個人のリスクには次の２種類があり、具体的な例は以下のようなものがあげられる。

1.コンピューティングの利用によるリスク
以下のような内容が考えられる。
(1)故障やフロッピーの破損などの物理的破壊
(2)間違った削除などの操作ミス
(3)システム管理者など他者の操作ミス
(4)システムのバグやその他の障害による問題
(5)本来アクセス可能な資源へのアクセス不能
(6)不正利用などのクラッキング
さらに広くとらえると、
(7)自分が公開した文書やデータにおける知的所有権の違反
(8)本来以外の目的でのプライバシー情報の利用

過去のコンピューティング活動においては、(1)から(5)のリスクだけを意識していればほぼ問題なかった。ロス・コントロールとしては操作の上達とデータのバックアップが主であり、システムの問題が発生したとしてもそれ以外の活動に時間をあてればよかった。しかし、今日では生活のかなりの部分がコンピューティングに依存しているために、その影響は大きくなっている。

2.コンピューティングの発達によるリスク

コンピューターが普及する以前にはそのコミュニティが小さかったためにさほど問題にならなかったことが、インターネットのようにネットワーク・コミュニティを爆発的に普及させる仕組みが出現した結果大問題になることがある。たとえば、以前なら個人の住所のようなプライバシー情報が本人の意思に反して公開されたとしてもそれを知ることができた人は少なかっただろう。しかし、今日 WWW で同じことがされれば、プライバシーが多くの人にさらされることになる。そしてそれを強制的にやめさせることは法律的には非常にむずかしい。

すなわち、インターネットの存在自体がもはやリスクであり、それは利用するかどうかにかかわらない。現代社会に生活する以上その影響からのがれることはできない。宮台(1996)はインターネット以前からテレクラなどのように不特定多数の参加するｎ×ｎコミュニケーションには同様の問題点があったことを指摘している。宮台はその問題を回避するには倫理による規制ではなく、メディア・リテラシーの習得と個人の自立が必要であるとしている。

3.2 利用権限の維持の必要性

従来個人のセキュリティ対策としてはパスワードを守ることが一番にあげられてきた。しかし、パスワードは単に認証の一手段であって、本当に重要なのは資源に対する利用権限を守ることである。近い将来には現在主流の８文字程度のパスワードにかわるさまざまな認証が低いコストで実現されるであろうし、資源の利用目的や利用場所によって認証手段が使い分けられることが当たり前になるであろう。すでにインターネット経由の資源利用においては、OTP(One Time Password)がよく使われているが、普通のパスワードとなぜ使い分けなければならないかは、資源を利用するための通信経路の信頼性についての知識がなければ理解できないであろう。

今後の情報教育においては、コンピューティングにおける資源とその利用が最重要であり、認証や暗号化などは利用権限の正当性を保つために使われることを理解させなければならない。そのために妥当な利用権限のポリシーを考えなければならない。

パスワードは正常なアクセス制御のための比較的コストが低く運用が可能である。パスワードに安全性を依存する大部分のシステムにおいて、ずさんな個人のパスワード管理がシステム全体のアクセス制御の統一性が崩す原因であることを認識させる必要があるだろう。

3.3 クラッキングについて

現実に被害にあわない限り、クラッキングは遠い世界の出来事のように思えるかもしれない。リスク管理のためには現実にあるクラッキングについてどのような種類があるかについて知っていなければならない。

例をあげると、侵入、データ破壊、データ改竄、なりすまし、いやがらせメール、盗聴といったものがあげられる。

3.4 コンピューター・ウイルス

コンピューター・ウイルスは家庭へのパソコンの普及やインターネットの発達によって社会的な問題になっている。特にマクロ・ウイルスといわれるものは非常に容易に感染するために影響が大きい。

学習者が家庭と学校の間でフロッピーを通じて媒介している可能性はかなり高いだろう。学校においてウイルス感染しないようにすることはシステム提供者の責任であり、家庭で感染防止することは個々の学習者の責任であることを教えておかなければならない。

4．リスクへの対策

4.1 学習者と教師とシステム提供者の関係

ほとんどの情報教育は組織のリスク管理上のポリシーの制約をうける。なぜなら、教育で使われる資源はその組織から提供されることがほとんどであるからである。通常の教育においてもそれはかわらないはずであるが、あまり大きな制約を感じることはない。しかし、コンピューターによる実習をともなう授業では、インターネットにつながったことによって個人の情報受発信が非常に容易であり、セキュリティ・ポリシーにかかわる違反が組織にとって現実のリスクとなっている。

授業に参加する教師と受講者が大学などから提供を受けている資源の例として、コンピューター本体はもちろん、教室でのネットワークやメールなどのためのアカウントなどがあげられる。利用者は権利と引き替えにそれらの資源の利用権限を維持する責任を負っているといえる。

この考え方はパスワードやファイルなどについては受け入れやすいと思われるし、個人の情報発信の権利についても同様に考えることができるだろう。

たとえば、WWW(World Wide Web)で学習者個人のページをつくらせることを課題とした場合を考えてみる。全世界からアクセス可能なページ上に個人ホームページをのせて、それが世界からメール等でコメントが来ることがある。その教育効果が非常に高いことについてはさまざまな報告がなされている。しかし、教育として行う以上ページ上で著作権の侵害などがあった場合、どんな理由があろうとシステム提供者は責任を免れないというリスクをはらんでいる。したがって教育はセキュリティ上の配慮をもってなされるよう、教師は組織のセキュリティ違反が学習者にないかチェックしなければならない。

4.2 パスワードを守る

利用権限を守るための最も基本的なロス・コントロールはパスワードを守ることである。

しかし、悪いパスワードを示すことは容易であっても、よいパスワードを示すことはむずかしい。なぜならよいパスワードの具体例は2度と使えない悪いパスワードだからである。また、悪いパスワードの規則を列挙するのも理解に限界がある。

そこで、たとえばクラッキング・プログラムの原理を学ぶことが考えられる。どのようなパスワードが推理されやすいかをアルゴリズムの学習ともリンクさせて学ぶことは意義があると思われる。

また、社会的クラッキングとよばれるような、システム管理者を騙ってユーザーをだましてパスワードをとることもしばしばおこなわれる。さらにはパスワード入力中に後ろから盗み見るなどの簡単な方法でパスワードを盗まれることもあることを知らなければならない。

4.3 不正利用の事例

プライバシーにかかわる事例や誹謗・中傷によるコミュニケーション障害について知る必要もあるだろう。これらは実際に当事者にならない限りなかなか理解しにくい。実例を一度学んでいれば、電子会議などでのフレーミングを未然に防げるかもしれない。

また、自分のプライバシーを公開することがどれほど危険なことであるかを理解した上でホームページの作成をはじめた方がよいであろう。ほとんどの場合は何も問題ないと思われるが、ストーキングのような実社会において問題になってしまった場合のリスク強度は非常に大きい。

さらに、クラッキングが明るみに出た事件についても知っておく必要があるだろう。た

とえば、文献 3)や文献 4)の著作は実際の事件にもとづいており、クラッキングを理解するには非常に有益である。

5．リスク管理教育におけるその他の問題

5.1 システム提供者の責任

以上のリスク管理を教育としておこなうためには、システム提供者がそのセキュリティ・ポリシーを可能な限り公開していなければならない。もしポリシーが公開されていなければ何をどう守るかの個人のポリシーを設定することがむずかしいからである。

しかし、残念ながらネットワーク・セキュリティに関するリスク管理の手法は充分確立しているとはいいがたい。アメリカ国防総省の Orange Book はセキュリティに関して詳細に検討した上で作成された文書であるが、一般の組織においてそのまま適用できるものではない。また、ファイアーウォールなど個別のツールに関する議論は多くなされてきているが、情報システムのマネジメントにおいて利便性とセキュリティのバランスをどうとるかについてはほとんど明らかにされていない。

よりよいセキュリティ教育のためには論理的に設営可能でかつ一般的に合意されたネットワークにおけるリスク管理の研究が必要であろう。

5.2 情報倫理

ネットワークにおけるコミュニケーションの作法としての情報倫理は比較的以前から紹介されてきた。とくにネチケットというネットワーク上のマナーはさまざまな形で形成されている。

しかし、ネチケットは悪意に対する防御にはなりえない。ネチケットはネットワークにおける知的共同作業における生産性向上のための行動基準であり、守らなければ罰せられるような義務ではない。

自由主義の枠組みにおいては、個人に「他人に迷惑をかけないかぎり何をしてもいい権利」（他者危害の原則(harm to others)）がある。したがって、自由主義は個人（や組織）に倫理的（美徳的）な行動を強制できない。いかなる倫理も全員に義務づけることはむずかしい。どんなにすぐれた倫理綱領があり、それをもとにした倫理教育がひろくおこなわれたとしても全員がそれに従うことはありえないと思った方がよい。

もちろん、組織として、あるいは教室において情報倫理を用意することは意義があるし、また望ましいことであろう。それは快適なネットワークの一員としての個人の自覚を高めることになるし、そのことが組織内の不正に対するロス・コントロールにもなるからである。

なにより重要なことはコンピューティングの先達が倫理的行動を身をもって示すことではないかと思われる。たとえば、教師が知的所有権に関して倫理的行動を求めながら、自分はコピー・ソフトを使っていれば倫理規定もその教師も信用を得られないだろう。倫理についての信頼感は些細な行動からくずれうることを忘れてはならない。

参考文献

1)南方哲也:リスクマネジメントの基礎理論、晃洋書房(1993)
2)宮台真司:見当違いの倫理主義を排斥せよ、へるめす、1996
3)Stall,C.: The cuckoo's egg, Doubleday(1989) 日本語訳: 池央耿訳「カッコウはコンピュータに卵を産む」、草思社（1991）
4)Tsutomu S. and Markoff, J.:Takedown: The Pursuit and Capture of America's Most Wanted Computer, Hyperion,(1996) 日本語版:近藤純夫訳、「テイクダウン」、徳間書店(1996)