●事例紹介●

情報化社会における自己防衛

村川　浩幸
（神奈川大学　学生生活支援部　事務部長）

はじめに

携帯電話やパーソナルコンピュータ（PC）の普及により急激に情報量が増加した。特にインターネットの利用による情報の検索は著しく便利になり、現在の日常生活の中では情報通信のためのPCや携帯電話のツールは、必需品になりつつある。

大学からの連絡や履修登録手続きなども、これらの情報技術を使った手段がとられるようになってきた。

情報技術の進歩と携帯電話やPC等の情報ツールの普及により、以前と比べて距離と時間を超越して大量の情報が流通しているのが現在の情報化社会である。便利な機能を備えた情報伝達ツールと情報サービスにより様々な恩恵を受けられるようになった。

しかし、その一方でこれらの情報サービスに関してのトラブルや犯罪が発生し、深刻な社会問題となっている。情報の漏洩や搾取、誹謗中傷や架空請求詐欺などの犯罪は、情報技術の進歩ともに、新たな犯罪手口が発生している。情報化社会の中で安全で便利に情報サービスを利用するためには、その裏側に潜んでいる危険を十分に理解して、被害にあわない、また知らぬ間に加害者にならないための知識を身につける必要がある。

本編では、情報に関するトラブルや犯罪とその防止対策について事例をもとに紹介する。

トラブル・被害と防止策

・インターネット掲示板への書き込み

SNS（Social Networking Service）などの会員制コミュニティーサイトの利用者が増えているが、この中には不適切な書き込み（ルール違反やモラルに反した行為、第三者への誹謗中傷等）によるトラブルが発生している。

特定のメンバーで限られた範囲でしか開示されないと安心してか、プロフィールに本人の氏名や大学名を掲載しているため、大学に抗議が寄せられ、場合によっては、当該行為者の処分を求められるケースがある。未成年の飲酒や法律違反など社会のルール・モラルに反することなどを安易な気持ちで書き込んだことが大きな問題へと発展することもある。法律違反やモラルに反することをしないのは当たり前のことだが、個人情報を安易に公開することにより、そこから新たな被害につながる危険があることを自覚しなければならない。

また、インターネットを使った個人への誹謗中傷行為は、名誉毀損罪や侮辱罪といった罪に問われることもあることを理解させ、そのような行為をさせないことが必要である。

・架空請求

PCのアドレスや携帯電話に身に覚えのない請求が送られてくるといった相談が毎年大学に寄せられる。これらの被害については世間では一般に広く知られるようになったが、いまだに被害にあう学生がいる。消費者センターや恐喝まがいの請求には警察に相談するように指導している。

以下は、大学のホームページで掲載した事例である。

［注意］コンテンツ利用料金請求メールについて

最近、コンテンツ利用料金などの名目で、下記のような架空の料金請求メールによる詐欺行為が多発していますのでご注意ください。

学内に届いた電子メールの例（一部略）

〈ご入金のお願い〉

これが最後のお願いです。

あなたがご利用の、インターネット・コンテンツ利用料金が未だに確認できません。現在までに何度かお願いの連絡をしましたが、入金の確認が取れません。

これ以上入金をお待ちする訳には行きませんので、○月○日○時までにお支払い下さい。

（中略）

尚、これは最終的な通知であり、また、個々のお客様に対応する事は物理的に不可能であるため、メール・お電話でのお問い合わせは受け付けておりません。

下記要領にてお支払い頂ければ、迅速に延滞リストから削除しますので、重ねてご入金お願いいたします。

［振込先］　○○銀行　　○○支店

［入金額］　￥＊＊＊，＊＊＊円

（以下略）

・ファイル交換ソフトからのウィルス感染

大学生活の中では、講義や就職活動でＰＣを使ってメールやファイルの交換をする機会が増えている。本人が気がつかないうちにコンピュータウィルスに感染し、個人情報が盗まれたり、大事なデータが破壊されたりといった本人の被害だけではなく、知らない間にインターネットを通して友人や第三者のＰＣ、大学のネットワークにウィルスが持ち込まれるといった被害が出ている。

ウィルス感染の予防対策としてアンチウィルスソフトが有効であるが、ソフトの更新の度に費用が発生するためウィルス対策をとっていない利用者も少なくない。そのため、本学では、神奈川大学から統合アカウントを受けて、本学総合ネットワークに接続している者には無料でインストールできるアンチウィルスソフトを導入し、学内でのウィルスによる被害の減少に努めている。

・防止対策

被害に遭わないためには、安易に個人情報を提供しない、ファイル交換ソフトを使用しない、アンチウィルスソフトを導入するなど、使用者側の情報サービスや情報ツールの正しい利用方法の理解と注意が必要である。

本学では「神奈川大学情報倫理ガイドブック」を作成し、授業でのＰＣ利用方法や情報リテラシーについて各種のガイダンスや初年次教育のＦＹＳ（ファースト・イヤー・セミナー）で情報リテラシー教育を行っている。その他、ホームページでも随時、被害状況や新しい犯罪手口などを紹介し注意喚起を促している。以下に「神奈川大学情報倫理ガイドブック」に掲載している「脅威トラブルと対処法」を紹介するので参考にしていただければ幸いである。

「神奈川大学情報倫理ガイドブック」表紙

脅威のケース	当事者		被害内容	主な原因	対策	
	加害者	被害者			推奨対処方針	技術的対策
⑴ 掲示板での誹謗中傷	不特定多数の他人	自分	名誉毀損・ストーカー行為など	自分を特定できる情報を教えたこと	自分の情報は教えない	監視と管理者への削除依頼
⑵ 個人情報の流失	自分	名簿掲載者	振り込め詐欺、勧誘電話・手紙など	名簿の紛失	名簿には必要最小限の情報掲載とし、厳重管理を促す	鍵のかかる所への保管。電子データの場合、暗号化して保管
⑶ 出会い系サイトへのアクセス	不特定多数の他人	自分	脅迫など	名前が特定できない人と待合せたこと	知らない人とは会わない（第三者の信用できる人を介する）	アクセス者の管理を強化する
⑷ 著作権侵害・肖権侵害	自分	作家、アイドルなど	文書・写真をWEBに掲載	著作権を考慮しなかったこと	著作権者が許可しない行為はしない	（提供者が監視、写真には透かしをつける）
⑸ ファイル交換ソフトの利用	自分	映画製作社など	映画などの複製	著作権を考慮しなかったこと	著作権のあるデータ（DVDなど）は放置しない／他人に渡さない	（提供者が暗号をかける）
⑹ 暗証番号のホームページへの書き込み	不特定多数の他人	自分	身に覚えのない銀行口座からの引出し	暗証番号が第三者に知られたこと	セキュリテイ対策のない所では書き込まない	・URL（httpアドレスの確認）と出典署名確認 ・鍵マーク表示の確認
⑺ クレジット番号のホームページへの書き込み	不特定多数の他人	自分	身に覚えのない支払い	クレジット番号を第三者に知られたこと	セキュリテイ対策のない所では書き込まない	・URL（httpアドレスの確認）と出典署名確認 ・鍵マーク表示の確認

注） 神奈川大学情報倫理ガイドブックより

脅威・トラブルと対処法

おわりに

情報化社会が提供する情報サービスや技術は、日常の生活に様々な利便をもたらせてくれる。今後も情報技術の進歩により新しい情報サービスが生まれ、新しい情報ツールが提供されるであろう。これらのサービスを快適に使いこなすためには、利用者が利用上の正しい知識とその裏側にあるリスクを理解したうえで適切に使用しなければならない。新しい技術とそれに付随して発生する犯罪手口とその対処・防衛法は、いたちごっこの様相を呈しているが、利用者側の注意や知識で未然に防止できることが大半である。目に見えない情報と目に見えない相手が対象であるからこそ、それを利用する者は、十分な注意とともにルールを守りモラルを持って利用する必要がある。インターネットや携帯電話は情報通信・情報伝達の一手段であり、人と人との対面のコミュニケーションに替わるものではないことを認識し、必要に応じて適切なコミュニケーションの手段を選択する必要がある。快適に情報化社会での生活を継続できるように、大学は、学生を含めた組織の構成員に対して適正に情報サービスや情報ツールを利用できるように情報リテラシー教育をしていく責務がある。