インターネットセキュリティ
―情報セキュリティポリシー実施手順書―

武蔵大学情報・メディア教育センター

2014 年 3 月 13 日版

まえがき

利用上の注意

この冊子は、「武蔵大学情報セキュリティポリシー」の実施手順書として位置づけられており、情報・メディア教育センターの管理する情報機器を操作するに当たって、必要な最小限のセキュリティに関する知識について述べたものです。多くの場合は、一般的なネットワークセキュリティと共通する内容を持っていますが、一部においては、本学のネットワークポリシーに基づいているために、必ずしも一般的なセキュリティの常識と同じでない場合があります。

利用に当たっては、以上の点に留意してください。

著者 小野成志 (武蔵大学)

本冊子の記述内容に関する著作権は、すべて武蔵大学に帰属します。
本文中に記載された会社名、製品名等は一般にそれぞれの関係会社／団体の登録商標です。本冊子では、™、®、©などのマークは省略しています。
本冊子の配布、利用は自由です。ただし、本冊子作成に当たって利用した多くの文献や画像等については、
それぞれの著作権に従います。利用に当たっては、この点に十分ご留意下さい。

Copyright © Musashi University Media Literacy Center (1998-2014).
All Rights Reserved.

改訂履歴

1998 年 4 月版
- 初版発行

1999 年 4 月版
- 第 2 章不正行為についての記述を追加

2000 年 4 月版
- ネチケットガイドライン (RFC1855) を付録に追加
- ユーザーズセキュリティハンドブック (RFC2054) を付録に追加

2002 年 4 月版
- まえがきを追加
- コンピュータウィルスに関する記述を追加
- インターネットショッピング詐欺に関する記述を追加
- ネズミ講に関する記述を追加

2003 年 4 月版
- 出会い系サイトに関する記述を追加
- 情報更新と誤字等の修正

2005 年 4 月版
- 「情報セキュリティポリシー」の制定に伴い記述を変更
- フィッシング詐欺、スパイウェアなどの記述を追加
- netnews に関する記述の削除[*1]
- 著作権の確認できない画像の全面的な差し換え[*2]
- 情報更新と誤字等の修正

2006 年 4 月版
- 組織名の変更に伴う修正を実施
- P2P に関する記述を追加
- 情報更新と誤字等の修正

2008 年 4 月版
- SNS に関する記述を追加
- 内容と関係しない画像の削除
- ネチケットガイドライン (RFC1855) を付録から削除
- ユーザーズセキュリティハンドブック (RFC2054) を付録から削除

2010 年 4 月版
- 違法ダウンロードに関する記述を追加

[*1] 学内での利用がほとんどなくなったため usenet に関する記述は削除された。

[*2] 旧版の画像の大部分は、sunsite.sut.ac.jp のアーカイブで自由に利用できるとされた配布物を利用していたが、同サイトから当該配布物が削除され、著作権の確認できない状態となったため差し換えることとした。

目次

はじめに 1

第 1 章　インターネットと自己責任 3

第 2 章　インターネットに潜む危険 4
2.1　電子メールの危険性 4
2.2　Web サービスでのトラブル 13
2.3　悪性ソフトウェア 19
2.4　街角でのインターネットでのトラブル 21

第 3 章　違法行為 —あなたが加害者になるとき— 22
3.1　インターネットに関する法律 23
3.2　嫌がらせ 24
3.3　著作権違反 24
3.4　電子メールアドレス盗用 25
3.5　ネズミ講ではありませんというネズミ講 25

第 4 章　インターネットの脅威から身を守る 27
4.1　パスワード管理がすべての基本 27
4.2　マナーを守る 30
4.3　危険を前提に行動する 31
4.4　自分のコンピュータの管理 31
4.5　暗号電子メール 33
4.6　セキュリティに配慮した Web ページを作る 33

第 5 章　情報セキュリティポリシーの遵守 35
5.1　インシデントの状況に応じた協力 35
5.2　学内の規則 37
5.3　処分 37

はじめに

武蔵大学 Web ページ (2014 年 3 月 5 日現在)

学内のコンピュータは、すべてインターネットに接続されています。従って、みなさんは、学内のコンピュータを使って、インターネットの様々な資源を自由に利用することができます。

例えば、世界中の Web ページ[*1]を見ることができます。それだけでなく、自分で Web ページを公開し、世界中の人たちに見てもらうこともできます。

もちろん、電子メールも利用することができます。

しかし、インターネットを利用できるということとインターネットを安全に利用できるということは同じではありません。インターネットはすばらしい情報を提供してくれる反面、たくさんの危険が潜んでいます。後に見るように (第 2 章参照) インターネットにも詐欺、ストーカー、違法なドラッグの取引などの犯罪が存在します。

本学では情報システムを利用するに当たって守らなければならない規約「武蔵大学情報セキュリティポリシー」を定めています。

この冊子は「武蔵大学情報セキュリティポリシー」を遵守していただくために基本的な情報を提供し、皆さんがインターネットを利用するために必要なセキュリティに関して配慮すべき事項について書かれています。

中には既に高校時代や中学時代に聞き覚えている内容が繰り返されている場合があるかもしれませんが、再確

[*1] Web ページを動かす仕掛けは、WWW とよばれていますが、その原義は World Wide Web(世界中に張り巡らされた蜘蛛の巣）という意味です。

認の意味でもう一度注意深くこの冊子を読んでください。

学内のコンピュータの利用をはじめるに当たっては、「情報セキュリティポリシー」に沿ったインターネットセキュリティに関するガイダンスを受講し、情報セキュリティポリシーを遵守することについての誓約書にサインしなければなりません。その上で所定のセキュリティテストに合格することも必要です。

第 1 章

インターネットと自己責任

情報・メディア教育センターでは、インターネットからやってくる様々な脅威に対して常に警戒し、対策をとっています。

本学に対する不正アクセスと思われるアクセスは日に 10 万件を数えます。また迷惑メールやウィルス、ワームなどのメールは大学全体に到着するメール数の 50% に近いと推定されています。

残念ながら、このような危険に対して情報・メディア教育センターの対応できることはごくわずかなものです。もちろん、情報・メディア教育センターとしてインターネットの脅威に対して万全の防御を尽くすように努めてはいます。しかし、防御を完璧に行うことは不可能に近いことですし、何よりも情報・メディア教育センターは、以下のような情報・メディア教育センター自身の資源を守ることだけしかできません。

- 学外から学内への侵入行為からの防御
- 学外からの妨害行為からの防御
- 学外からのコンピュータの破壊行為からの防御

つまり、インターネットを利用することにより、あなたの身に降りかかるかもしれない多くの危険は、情報・メディア教育センターで守ることはできません。あなた自身が危険を回避するしかないのです。インターネットで不愉快な思いをしないためにも、自分の身は自分で守るという技術を身につけた上でインターネットを利用するという姿勢が必要なのです。

これがインターネットにおける「自己責任の原則」と呼ばれるものです。

実際、多くの脅威は、個人がある程度のインターネットに関する知識を持ち、十分な注意を払っていれば防げる場合がほとんどなのです。

インターネットを利用していただくに当たって、まずみなさんに身につけていただきたいことは、自分の身を自分で守る方法です。その際に、本学の建学の三理想の一つである「自ら調べ自ら考える」精神が非常に重要な役割を果たすということもここに付け加えておくことにいたしましょう。

第 2 章

インターネットに潜む危険

インターネットは大都会の大通りにたとえられています。大都会の大通りでは多くの見知らぬ人が行き交い、素知らぬ顔をして通りすぎてゆきます。しかし、その中には通り魔や詐欺師、麻薬の密売人などが潜んでいるかもしれません。

インターネットにもやはり詐欺師、通り魔、違法なドラッグの売人などが潜んでいます。しかも、インターネットは日々急速に発展しており、日常生活では体験することのないような危険な出来事が毎日起こっています。

ここでは、そのすべてについて触れることはできません。過去に起きたインターネットでの不幸な事例を参考にしながら、インターネットに潜む危険について、かいつまんでご紹介します。

最初にインターネットの基本的なサービスとも言える電子メールでの危険性についてご紹介した後、Web ページ、掲示板サービスなどのインターネットの各種サービスでの危険な出来事についてご紹介することにしましょう。

以下に書かれていることは、コンピュータシステムからインターネットを利用する場合にのみ当てはまるわけではありません。携帯電話を利用した電子メールや Web ページ閲覧などの場合にも当てはまります。

2.1 電子メールの危険性

電子メールは、インターネットを利用した郵便サービスと言うことができます。しかも、普通の郵便よりはるかに手軽で便利なサービスということができます[*1]。電子メールはたいへん便利なサービスなので、流行り廃りの非常に激しいインターネットの歴史上でも、最も古いサービスの一つでありながら、最も利用されているサービスとなっています。

しかし、電子メールを普通の郵便の感覚で理解していると思わぬことに出会うかもしれません。また、歴史が長いだけに、電子メールは昔から様々なトラブルの事例が報告されています。

2.1.1 届かない電子メール

電子メールは相手に必ず到達するということを保証していません。また、相手に到達したかどうかや、相手が読んだかどうかも原則として確認することはできません[*2]。

電子メールが届かないケースとしては以下のような場合が考えられます。

[*1] 電子メールに対して普通の郵便のことを snail mail（かたつむり（のようにのろまな！）郵便）と呼ぶ人もいます。

[*2] ソフトの中には、受取人が電子メールを開封すると、その旨を差出人に知らせるても良いかを確認するという機能のついたものもあります。

- 宛先[*3]を間違えた
- メールを運ぶはずのコンピュータが停止してしまった
- コンピュータがメールを誤配送したり間違って捨ててしまった
- メールを運ぶコンピュータに spam メールと判断され、送信を拒否あるいは破棄されてしまった

電子メールが相手に届かなかった場合は、運が良ければ、その旨を知らせるメールが届くこともあります。しかし、何も届かないこともあります。

電子メールのこうした機能を理解していないと、メールを出した出さないで思わぬトラブルが生じることもあります。

電子メールを出すときには、常に「事故で相手に届かないかもしれない」と考えるべきです。

2.1.2 電子メールでの口論

当然ですが、電子メールは相手の表情も見えませんし声も聞こえません。こちらが何気なく言った言葉が、相手を傷付けて取り返しのつかない関係になってしまうこともあります。

電子メールでは、ちょっとした行き違いがなぜか感情むきだしの口論に発展してしまうことがあります。これを flames(炎) と呼ぶ人もいます。電子メールで口論になったときには、自分でも驚くほど過激になることに気づくときがあるかもしれません。そうなった時は大概手遅れです。常に冷静な行動こそがインターネットでのトラブル回避の基本です。

電子メールでの言葉遣いは、普通の手紙以上に気をつけなくてはいけません。それだけでなく、普通の手紙には無い表現方法やルールがあります。それらを知らないと相手に不愉快な思いをさせたり、思わぬ失敗をしてしまいます。

こうしたルールはネチケットと呼ばれています。ネチケットとは何かについては、第 4 章の 4.2 をご覧下さい。

2.1.3 売られた電子メールアドレス

電子メールを出すには当然相手の宛先が必要です。このようなアドレスを電子メールでは電子メールアドレスと読んでいます。例えば、本学の学生の電子メールアドレスは、< **ユーザ名**@st.musashi.ac.jp> です。インターネット上では、こうした電子メールアドレスを密かに収集し、売買する商売があります。電子メールアドレス売買の専門会社もあります。したがって、インターネットをはじめた途端、通販会社や見知らぬ人からの電子メールがやってきたとしても不思議ではありません。見知らぬ人からの電子メールの内容はもちろん様々ですが、大概以下のようなものです。

- 通販会社の広告
- ネズミ講の勧誘
- ポルノサイトの広告

特にネズミ講に参加した人[*4]は、少しでも多くの相手を探しますから、個人で大量の電子メールを出します。そのために、電子メールアドレスを購入することもあります。電子メールアドレス売買とネズミ講は関係が深いので、一つの会社が、電子メールアドレス売買とネズミ講の会社を兼ねていることも多く見受けられます。

[*3] 電子メールで使う宛先のことを電子メールアドレスといいます。

[*4] 言うまでもなく、このような行為は日本の刑法に触れます。また、あなたがネズミ講の当事者となった場合は、武蔵大学として厳正な措置を取ることは言うまでもありません。(3.5 参照)

こうした会社は、電子メールアドレスを様々な方法で入手しています。

- 個人の Web ページに書いてある電子メールアドレスを調べる
- 掲示板などに投稿した電子メールアドレスを調べる
- アンケートを装った Web ページを開設し、電子メールアドレスが書き込まれるのを待つ
- でたらめに電子メールを送って返事が来るのを待つ

最初の二つの方法で電子メールアドレスが流出した場合はやむを得ないところがあります。また、このようにして入手した電子メールアドレスが正しいかどうかは検証できないので、電子メールを売買する業者にとっても価値の高い電子メールアドレスではない可能性があります。

しかし、後者の二つの方法によって入手された電子メールアドレスは、非常に信頼性の高い電子メールアドレスとみなされる危険があります。

ショッピングや「豪華景品が当たる！」などという Web ページにアクセスして、電子メールアドレスや、まして自分の住所や電話番号を書き込まなくてはならない場面に遭遇したら、よくよく考えてから行動してください。このことについては、後でもっと詳しく触れることにします。

また、見知らぬ人から電子メールが来て、「以降メールを送って欲しくなければ、＜購読しない＞（unsubscribe）というメールを送ってください。」とか、いかにも親しげに「きっとメール下さい。お返事待ってます。」という電子メールが来たときは、それに返事を書くべきかどうかを良く考えて、さらに慎重に行動してください。その見知らぬ相手は、送った電子メールに対して返事があったメールアドレスを最も価値の高い電子メールアドレスとして売買するかもしれません。そして売買された電子メールアドレスは、後に触れる迷惑メールの対象になる危険があります（2.1.5 参照）。

2.1.4 なりすまし、盗聴、改竄

電子メールの仕組みは非常に単純なので、悪意のある者にとっては、様々ないたずらや妨害が可能です。「なりすまし、盗聴、改竄（かいざん）」は電子メールの三大脅威と言っても良いでしょう。

なりすまし

「なりすまし」というのは、具体的には、あなたの名前を語って第三者がメールを送ることを指します。電子メールでは、あなたが知らないうちに詐欺師にされていたり、嫌がらせの主にされていたりすることがあります。なりすましの手口は次のようなものがあります。

- あなたのパスワードを盗んで電子メールを出す
- あなたの電子メールアドレスを差出人のアドレス欄に埋め込む
- 電子メールの履歴情報を書き換える

今までの本学の事例ではパスワードを盗まれることがほとんどでした。パスワードを他人に知られないようにしっかりと管理していないと、思わぬ被害に遭うことになります。

盗聴

電子メールは、通常郵便の封書などとは異なり、他人に読まれてしまう機会が多いシステムです。たとえば、以下のような者は簡単に電子メールを読むことができます。

- 電子メールを経由するインターネット上のサイトの管理者

- システム管理者の権限を不正に入手した者
- LAN もしくはインターネット上で盗聴している者

特に、システム管理者はメンテナンスの必要上、電子メールを目にする機会が非常に多いのです。もちろん本学の管理者は別として[*5]、ほかのサイトの管理者が良心的である保証はありません。

また、インターネットでは不正侵入を試みる人々が、常にネットワークを盗聴しています。さらに、公的諜報機関も盗聴していると考えて良いでしょう。

電子メールは封書ではなく、葉書のようなものと心得ておくと良いでしょう。

改竄 (かいざん)

電子メールを盗聴されても困らないという人も、その内容を書き換えられては困るという人は多いでしょう。恋人に「好きです」と書いた電子メールが「嫌いです」と書き換えられてしまって、気分が良いと思うことはあまりないと思います。

しかし、電子メールが盗聴されている以上、書き換えも行えるということを知っておく必要があります。どこかのサイトの管理者が電子メールを書き換えてしまうなどという行為に及ばない保証はありません。また、インターネット上の悪意の第三者は、いつでも電子メールを書き換えられるチャンスがあるのだということを知っておく必要があります。

「なりすまし、盗聴、改竄」を防ぐには、２つの方法があります。

- 全く電子メールを使わない
- 電子メールを暗号化する

全く電子メールを使わないという方法は、たしかに電子メールに関しては安全ですが、何物をも産み出しません。後者の方法は、正しく運用すれば、全く電子メールを使わない場合と同程度の安全性が確保できます。暗号化については、後でもう少し詳しく述べることにしましょう（4.5 参照)。

2.1.5 迷惑メール、spam

電子メールは、だれでも気軽に簡単に扱える便利な道具です。しかし、その性質を悪用して特定の個人に大量に電子メールを送りつけたり、多数の人に迷惑な電子メールをばらまいたりする人々がいます。

このような電子メールを spam と呼ぶことがあります。その本当の語源は明らかではありませんが、spam という豚肉の缶詰と関係があるとされています。[*6]これはインターネットでは古くからの言い回しですが、最近は日本語では「迷惑メール」という言い方が定着してきました。英語では Unsolicited Bulk Email（UBE) と呼ばれることもあります。

迷惑メールが大量にやってくると、時には以下のようなことに遭遇します。

- 個人の郵便受け（メールボックス）があふれ、事実上電子メールが使えなくなる。
- 電子メール受信用のコンピュータが停止し、そのコンピュータが配布する全員の電子メールが使えなくなる

といった被害が発生します。[*7]

[*5] 本学のシステム管理者は「ネットワーク運用規程」等に基づく厳しい守秘義務を負っています。

[*6] この言い回しがあまりに普及したため、缶詰製造元の ”Hormel Foods” は、缶詰（商標）については ”SPAM” と大文字で、迷惑メールについては ”spam” と小文字で表記するように求めています。

[*7] 本学ではこうした大量メールの流量に十分耐えられるメールサービスを利用しています。

なぜ、このような大量の迷惑メールがやってくるのでしょうか？考えられるのは次のようなことです。

- 嫌がらせ、悪戯
- 電子メールアドレスが売買された (2.1.3 参照) 結果、多くの広告が舞い込んできた
- Web ページに書き込んだ情報を利用されたり、自分で開設している Web ページの電子メールを読み取られた

迷惑メールは世界中にそれを規制する法律があり、日本でも「特定電子メールの送信の適正化等に関する法律」（平成 14 年 4 月 17 日法律第 26 号）や「特定商取引に関する法律」（昭和 51 年 6 月 4 日法律第 57 号）で規制されています。しかし、電子メールは世界中のどこからでも発信する事ができ、一国の法律での規制になじみません。このため、迷惑メールは増加の一途を辿っているのです。

現在本学が利用しているメールサービスでは、迷惑メールを自動判定して隔離する機能が提供されており、多くの迷惑メールは着信時に除去されています。

2.1.6 デマ、チェーンメール

電子メールは、情報ツールとして非常に優れた性質を持っています。情報の伝播力もその魅力の一つです。何かおもしろい情報をメールで受け取ると、友人にそのまま転送してあげるといったことが気軽にできます。

しかし、それを悪用すれば、世界中に驚くような速さでデマを広めることができるのです。

デマにはいろいろなタイプがあります。たとえば、偽ウィルス情報というものもその一つです[*8]。偽ウィルス情報として世界で最初に騒がれたものに good time ウィルスというものがあります。

そのときは、「good time というサブジェクトのついたメールは決して開かないでください。ウィルスに感染します」という電子メールが世界中を駆け巡りました。

当時は、電子メールでウィルスを運ぶ手段がなかったので、これをデマだと見破ることは比較的簡単でした。にもかかわらず、多くの人がだまされ、それをまた友人に広めていったのです。

また、「白血病の子供を励ますために」とか、「原水爆禁止のアピールのために」とかの名目のもとに「このメールにあなたの言葉を書き足して別の人に送ってあげてください」という電子メールが来ることがあります。これはチェーンメールと呼ばれています。その大半は悪戯です。

チェーンメールはネズミ講 (3.5 参照) にも利用されています。

チェーンメールはどのような理由であれ、インターネット資源を浪費させ、デマを伝播させることにより、結果として spam と同様の被害を与えます。

デマメールやチェーンメールのもう一つの恐ろしいところは、被害者が意識しないで加害者に転じてしまっていることです (第 3 章参照)。

友人に何か情報を転送してあげようと思ったときは、事実かどうかを確認して慎重に行動することがインターネットでは求められます。

2.1.7 電子メール詐欺のいろいろ

電子メールがだれでも手軽に使えるということは、悪意のある人間にとっても手軽に使える道具となります。

「ネズミ講」(3.5 参照) の勧誘も詐欺の一種とみても良いですが、その他に「振り込め詐欺」「フィッシング詐欺」「ナイジェリア詐欺」など数多くの巧妙な手口が存在します。

この節ではいくつかの事例をご紹介します。

[*8] ここでの事例は、古い時代のものです。最近の偽ウィルス情報の例は、2.1.8 で紹介します。

振り込め詐欺

電話での振り込め詐欺は、新聞などの報道の通りですが、電子メールを利用した振り込め詐欺も多く発生しています。多くはポルノサイトを見た会員料の未納に対する架空請求などですが、電子メールに添付されている画像などを誤ってクリックすると、自動的に Web ブラウザが起動し、違法なサイトに誘導されて高額請求が表示されるものなどもあります。

この場合、Web で表示される料金請求画面では、IP アドレスや、プロバイダ名（musashi) などが表示され、「振り込まない場合は、そこに請求する」とか「暴力団が債権回収に行く」などの表記があります。

このようなケースでも、本学から個人情報が漏れることは基本的にはありません。

このような場合、絶対に相手方と連絡をとってはいけません。学生生活課などにご相談いただくか、警察に相談しても良いでしょう。

フィッシング詐欺

フィッシング (Phishing) 詐欺とは、クレジットカード会社や銀行、あるいはショッピングモールからのお知らせ等に見せかけた電子メールを送りつけ、そこに書かれている Web サイトにアクセスさせて、クレジットカード番号などを入力させ、詐取しようとする手口です。

あたかも本物のようなフィッシング詐欺のメール

この手口は現在日々巧妙になっており、やってくるメールもクレジットカード会社や銀行からの真性の電子メールアドレス*9で、そのお知らせ内容も詐欺と見破るのが難しくなっています。

そこに表示された Web ページのアドレスも銀行のものと見分けがつきにくいようになっており、アクセスしてみると、表示される画面からは、偽物とはとても判断できないほど巧妙な作りとなっています。

しかし重要なことは、銀行やクレジットカード会社は、どんな場合でもインターネット上のページでクレジットカード番号の確認は行わないという事実です。

またショッピングモールからの電子メールでも、そのメールの誘導する Web ページにクレジットカード番号を入力させることはありません。

このことを念頭に入れておかないと思わぬ被害に遭うことになります。

電子メールでやってくるフィッシング詐欺はこの点を十分注意していれば、ある程度防ぐことができます。

しかしこの問題は、最近さらに巧妙化しています。

電子メールの誘導するサイトにアクセスしてみると、そこには一般的な内容のことしか書かれていないけれども、アクセスした瞬間に悪意のあるプログラムが自動的にダウンロードされて、重要な機密が盗まれるという仕掛けを用意していることもあるのです。

従来の電子メールでのフィッシング詐欺をソーシャル型、後者をステルス型と呼ぶこともあります。ステルス

*9 もちろん、なりすましによる偽装です。

型については Web に関するトラブルの章でもう一度取り上げることとします。

この場合の対策は、一番は相手にしないことですが、どうしても本物かどうか見分けがつかなければ、電子メールに書かれたリンクを直接クリックしないで、まず本物とわかっているサイトのアドレスを手で入力してから、そこのリンクをたどってみるなどの方法をとるべきです。

本物にそっくりな偽装ページ

2.1.8 コンピュータウィルスとコンピュータワーム

コンピュータウィルスとは、電子メールや CD、USB フラッシュメモリなどの電子媒体を通じてコンピュータに侵入し、侵入したコンピュータの正常な動作を妨害したり、破壊活動を行ったり、あるいは、他のコンピュータへの侵入を試みたりすることを目的に作られたプログラムのことをいいます。

かつて、コンピュータウィルスはインターネットとは関係のないものとされていました。なぜなら、その多くはフロッピーディスクや CD などのメディアから感染したものであり、ネットワークでの感染はごくまれにしか発生しなかったからです。

しかし、今日では、コンピュータウィルスの多くが電子メールや、Web サイトからのダウンロードファイルから感染すると言われています。また、最近では不用意なファイル共有ソフトウェアの利用[*10]によって感染を広げているケースも多く見受けられます。

その他にも、コンピュータワームと言われるプログラムもあって、こちらは侵入経路が主としてネットワーク経由であることでコンピュータウィルスと区別されています。コンピュータワームは、コンピュータウィルスと異なり、古くからインターネットを悩ませてきました。

かつては意味のあった両者の区別ですが、侵入経路が同じケースであることもあり、最近では両者の区別がやや曖昧になっています。ここでは一括してコンピュータウィルスと言うことにします。

いずれにしましても、今や、みなさんがコンピュータによるインターネットの利用を始めて、最初に悩まされるものが、コンピュータウィルスやコンピュータワームであるかも知れません。

完全な駆除は難しい

コンピュータウィルスの種類は非常に多岐にわたり、その手口も非常に巧妙になってきているため、みなさんにおすすめする防御方法も完全なものを示すことは難しいのです。しかし、以下のようなことは少なくとも守ってください。

- 見知らぬ人からのメールを安易に開かない
- 添付ファイルは、知っている人からのメールでも相手が確実に送って来たものだと確信が持てないときは開かない

また、情報・メディア教育センターでは、以下の対策を講じています。

- 電子メールサーバでのウィルスチェック
- センター管理コンピュータへのウィルスチェックソフトの導入
- センター管理コンピュータのすべてのソフトウェアの定期的なセキュリティバージョンアップ

しかし、いずれの方法も完全ではありません。たとえば、ウィルスの中には、電子メールを開かなくても、感染してしまうタイプのものが多くあります。また、ウィルスチェックをすり抜けるものもあります。

情報・メディア教育センターでは、ウィルスの発生が確認された場合に、被害を最小限に食い止めるために、一時的にコンピュータを停止したり、該当者のアカウントを利用停止にしたりする場合があります。

[*10] ファイル共有ソフトウェアの危険性ついては 4.4 節を参照してください。

偽ウィルス

先に見たように (2.1.6 参照) インターネット上の情報には、多くの虚偽の情報が含まれています。ウィルスに関する情報も虚偽情報がたくさんあります。

たとえば、以下のような電子メールがあなたのところに来たらどう思いますか？相手は見知らぬ人かも知れませんが、親しい友人である可能性もあります。

> いきなりですが本当に申し訳ございません。
> 私のコンピュータがウイルスにかかりました。アドレスリストに入っている人全員に自動的に感染してしまうという悪質なウイルスです。ウイルスに先にかかった知り合いのアドレスリストに私のアドレスがあったので私も感染しました。
> ですから、みなさんのコンピュータの中に既にウイルスがいます!!!!!!。十四日間は眠っているのですが、それを過ぎてしまうとハードディスクドライブを壊してしまいます。
> 私もこのメールを受けたときはびっくりしました。そして実際に検索したところ、そのファイルがあり、下に表示してあるステップに従ってウイルスを駆除しました。
> 本当に申し訳ないんですが、今直ちにウイルスを駆除してください。そしてあなたのアドレスリストにある人は既に感染していますので、このメールをリストにある全員に送っていただけないでしょうか。本当に申し訳ございません。

これをみたら、あなたはすぐ親切に友人に転送し、自分のコンピュータをこの指示にしたがって操作するでしょうか？

しかし、一見親切そうなこのメール指示にしたがって操作をすると、実はコンピュータが動かなくなるのです。

こうした情報に惑わされないために、ウィルスの正確な情報を提供しているホームページなどで、必ず真偽を確認するようにしましょう。

また、安易に友人へメールを転送して、チェーンメール化しないように注意することも肝要です。

ウィルス情報は、以下のページで確認することができます。

IPA **情報処理振興機構** `http://www.ipa.go.jp/security/isg/virus.html`

Trend Micro `http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=jp&tab=malware`

Symantec `http://jp.norton.com/security_response/`

McAfee `http://www.mcafee.com/japan/security/latest.asp`

2.2 Web サービスでのトラブル

今や、インターネットと言えば Web サービスを利用すること、というぐらいに多くのサービスが Web 上で利用可能です。Web ページを見るだけなら特別の手続きも必要なく世界中の情報が簡単に手に入ります。自分が Web に情報を発信することも簡単に行うことができます。

しかし、Web サービスはその手軽さゆえに思わぬトラブルに巻き込まれやすいのも事実です。

2.2.1 Web ページを見ただけなのに

あなたは、Web ページを見るだけなら危険はないと考えてしまうかもしれません。しかし、それは正しくありません。Web ページは閲覧する度に、「どこから、いつどんなページを見たか」といった情報がサーバに記録されます。あなたの個人情報が、こういったところから漏れてしまうことがあります。そして、知らぬ間に、その情報が利用されているかもしれません。

たとえば「本学のサーバで学生たちがどれくらいの時間ポルノサイトを見ているか」という集計を取るつもりになれば、できないことではありません。(実際に大学としてそのような試みをしようという計画は存在しませんが)

同じように、ポルノサイトも本学の学生がどれくらいの時間自分のサイトを見たかを知ることは簡単にできます。ポルノサイト側としても、本学の学生が自分のサイトを良く見てくれるようなら、spam メールを出して、さらに勧誘してみようと思い立っても不思議ではありません。

ただ、これは防ぎようのない情報流出です。Web ページを見るときに、その情報が利用されるかもしれないということを承知した上で利用するという心構えが必要です。

さらに、注意が必要なのは、「アンケートに答えて景品をもらおう」といった Web ページへのアクセスです。Web ページに住所や氏名や電子メールアドレスを書き込めば、当然のことながら相手にその情報を渡すことになります。また、インターネットの途中に潜む盗聴者 (2.1.4 参照) に知られることにもなるかもしれません。

もちろん、ここで言いたいのは、アンケートに答えるなということではなく、アンケートに答えることにはそれなりのリスクを背負うということです。

これは、実はインターネットの外でもみなさんが知らないうちに背負っているリスクでもあります。みなさんは、レンタルビデオやレンタル CD を利用することがあるかもしれません。気づいた方もいらっしゃるはずですが、レンタルショップの中には、契約条項に、入手した個人情報を第三者に譲り渡すことがあるという条項を入れています。みなさんは、個人情報流出に対するリスクを背負ってビデオを借りていることになります。

2.2.2 見知らぬ請求書

Web ページは無償のものばかりとは限りません。お金を払わなくては見ることのできないページもあります。しかし、ここでよく考えてください。

- その Web サービスの開設者は信頼のおける相手でしょうか？
- インターネットの途中に潜む盗聴者 (2.1.4 参照) に知られることはないのでしょうか?

最初の点については、最も注意しなくてはなりません。過去にこんな事例があります。

- ポルノサイトを、一度だけ見るつもりでクレジットカード払いで有料の Web ページを見た。その後一度も見ていないのに毎月請求書が届くようになった

- Web ページのショッピングで一度だけ買い物をしたところ、その後見知らぬところから身に覚えのない請求書が届くようになった

この二つの事例は、いずれも購入の際に提示したクレジットカード番号を悪用されたものと考えられます。

その上、インターネットでは、相手方だけではなく、盗聴者がいることも忘れてはなりません。信頼のおける相手でも、クレジット番号を Web ページに入力すれば、盗聴者の知るところとなります。

このような危険を避けるため、ほとんどの通販会社等では、暗号化されたデータを受け付ける Web ページを開いています。会社によっては、それ以外での受注を受けないところもあります。暗号化されたデータを受け付けるホームページかどうかは、Web ページのアドレスを見ればわかります。

普通の Web ページは、`http://`で始まります。一方、暗号化されたデータを受け付ける Web ページは`https://`で始まります。クレジットカード番号などの重要な情報を入力する時は、Web ページアドレスが`https://`で始まっているかどうかを確認するのも良いでしょう。

これは SSL と呼ばれる方式です[*11]。しかし、これが有効なのはインターネット途中の第三者に盗聴されないということを意味しているだけです。その他のさまざまな脅威には有効ではありません。この点は注意が必要です。

架空請求／不当請求

振り込め詐欺（2.1.7 参照）の節でも述べたように，最近はそもそも身に覚えのない請求書が届くようになりました。あるいは、誤って有料サイトの入会手続きをしてしまったという場合もあり得ます。

このような場合には、自分で直接相手と交渉すると、ますますトラブルに巻き込まれる可能性もありますので、学生生活課までご相談下さい。

[*11] 本学では、WebMail などパスワード入力が必要な Web ページに採用されています。

2.2.3 出会い系サイトでの犯罪

インターネットの楽しみの一つは、未知の人との出会いにあることは間違いありません。しかしながら、見知らぬ人との出会いが思わぬトラブルを呼ぶこともまた確かなことです。実際に、出会い系サイトでの犯罪も多数発生しており、このようなサイトの利用には十分な注意が必要です。

また最近ではコミュニティサイト[*12]で犯罪に巻き込まれるケースも増えており、いわゆる出会い系サイトでなくとも注意して利用する必要があります。

2.2.4 インターネットショッピングでのトラブル

最近は、気軽にインターネットショッピングができる環境が整ってきました。

しかし、それにつれて詐欺等の事件も頻発しています。「代金を振り込んだのに商品が届かない」、「商品を送ったのに連絡がつかない」といった詐欺まがいのトラブルが増加しており、これによる詐欺被害も増加しています。

詐欺の犯人は、実際には商品がないのにインターネット上に嘘の情報を流し、架空口座に代金を入金させてだまし取り、その後ネット上から消えて連絡がつかなくなるケースが多いのです。インターネット上の取引での一番の問題点は、お互いの身元を確認できないことです。商品を売買する際には、相手の身元をしっかりと確認することがトラブルや被害を回避するために必要な手段です。

また、簡単な作業で高収入が得られるなどの条件の良い内職を Web ページや電子メールで広告して、希望者から内職用の機材や材料と称して、高価なコンピュータなどを購入させ、これを使って仕事をしても、業者から商品の買い取りを拒否され、結局、収入を得ることができず、損をさせられたりするといったトラブル・被害も増加しています。

2.2.5 フィッシング詐欺

電子メールの項（2.1.7 参照）でも述べたとおりフィッシング詐欺は、非常に巧妙になっています。（内容を良く覚えておられない方は是非再読してください）

この傾向はまだ当面続くと考えられます。

現時点では、電子メールに添付されてくる Web ページのリンクをクリックしないで、手入力するというのが、面倒でも、防衛できる数少ない手段の一つです。

可能な限りそのような手段で正当なサイトかどうかを確認しましょう。

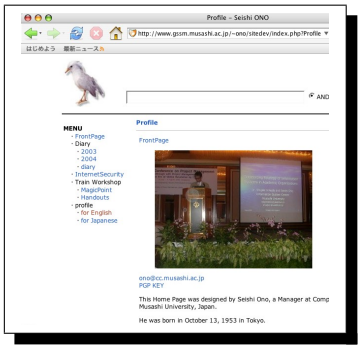
この他にも後に述べるネズミ講 (3.5 参照）は、自らが被害者となるだけでなく、加害者にもなる犯罪です。

甘い誘いには十分注意しましょう。うまい話などまずないと思っていた方が賢明です。「うまい話には必ず裏がある。」ことをよく考えてみましょう。

[*12] 「コミュニティサイト」とは、SNS、プロフィールサイト等、ウェブサイト内で多人数とコミュニケーションがとれるウェブサイトのうち、出会い系サイトを除いたものの総称

2.2.6 Web ページと個人情報

インターネットをしばらく体験していると、Web ページを見るだけでなく、自分で持ってみたいと考えるのは自然なことです。blog サイトのような個人向けの Web ページ開設サービスを利用すれば手軽に個人の Web ページをもつことができます。しかし、Web ページの開設に当たっては、Web ページを見るとき以上に危険に対する配慮が必要です。



個人情報の掲載されたページの例

個人で Web ページを開設すれば、それは個人のプライバシーを世界中にさらけ出すことを意味します。そして、その結果を悪意のある人たちに利用されたとしても、別に不思議はありません。顔写真、住所、電話番号などの掲載を計画する場合は、それが非常に高いリスクを持っているのだということを考慮する必要があります。

以下では、個人の Web ページを公開したことによって生ずる様々なリスクについてご紹介しましょう。

Web ページに顔写真を載せる

Web ページが実験的に公開されていた時代には、個人 Web ページに顔写真を載せることは、別に珍しいことではありませんでした。その時代に Web ページを見る人たちは、研究機関などのごく限られた人だけであり、悪意のある人たちがいないわけではありませんでしたが、被害があったとしても限定的なものに過ぎませんでした。

しかし、現在のように非常に多くの人たちが Web ページを見るようになると、悪意を持った人たちのことも考慮しないわけにはいかなくなりました。

あなたの Web ページは、インターネットという大都会の大通りに掲示された掲示板のようなものです。そういうところに顔写真と住所を載せたりすることが決して安全なことではないということは、すぐに想像がつくでしょう。

ここでは、過去の事例から、Web ページへの顔写真掲載に伴う幾つかのトラブルの可能性を指摘しておきます。

- 顔写真の無断転載
  インターネット上の女性の顔写真を収集して勝手に載せている Web ページが実際に存在します。そこには電子メールアドレスも載せられています。その結果見知らぬ人から不愉快なメールを、しかも多数受け取るといったトラブルに巻き込まれます。
- 顔写真の盗用
  顔写真を加工されて、猥褻画像と合成されたりすることがあります。
- 誘拐、ストーカー行為インターネットで見掛けたという理由で、見知らぬ相手に付け狙われる危険があります。

  2003 年 12 月 19 日 N 大学工学部で個人の写真を公表していることがきっかけで、ある事件が起きました。当時工学部に在学していた女子学生が、自分で開設していた Web ページに自分の写真を掲載していました。これをはるか米国の地で見た若者が、この女子学生に恋着したあげく、わざわざ米国から渡来し、あろうことか学内に立て籠って面会を強要したのです。インターネットを媒介にすると、常識的にはあり得ないと思うような事件が実際に起こるのです。

Web ページに住所や電話番号を載せる

住所や電話番号は、顔写真よりさらに様々なトラブルのもとになると考えられます。

住所や電話番号がわかっていると、本人に「なりすます」ことが容易になるからです。また、誘拐、ストーカー行為に際しても、顔写真の場合よりも、さらに危険の度合が高いと思われます。

Web ページに電子メールアドレスを載せる

電子メールアドレスの掲載も場合によっては、迷惑な結果をもたらします。見知らぬ人からのメールは、電子メールの楽しみの一つでもありますが、薄気味の悪いメールや不愉快なメールをもらうことも覚悟しなくてはなりません。

電子メール掲載に伴うトラブルとしては、以下のものが考えられます。

- 見知らぬ人からのストーカーメール
- ポルノの案内やネズミ講の勧誘メール
- そのほかの様々な迷惑メール

基本的には、電子メールは無視することができますから、これらのトラブルを承知で Web ページに電子メールアドレスを載せている人も少なくありません。

Web ページに誕生日を載せる、履歴を載せる

自分の誕生日や経歴を載せることは、Web ページを見る人に親しみを与えますが、親しみを覚えてほしくない人にまで親しみを与えることも事実です。その結果、ストーカー行為のきっかけになることがあります。

また、経歴がわかっていると、本人への「なりすまし」が容易になります。

Web ページに家族の情報を載せる

家族の情報も自分の経歴と同様に「なりすまし」の手がかりとなることがあります。

また、ストーカーなどの迷惑行為を家族に広げてしまう可能性もあります。

SNS での注意点

インターネット上の交流を通して、社会的ネットワークを構築する Facebook 等の Social Networking Services (SNS) では、昔の友人との思わぬ再会があったり、同じ趣味を持つ人や同じ地域に住んでいる人を簡単に探すことができたりと、ユーザ同士の積極的な交流が楽しみの一つとなっています。そのため、知り合いに見つけてもらうためや、話が盛り上がってしまって、つい内輪の情報や個人情報を書き込んでしまいがちです。

しかし、サービス内には悪意を持ったユーザも存在することが多く、彼らはそれらの情報をねらっています。あなたが限定的に公開している情報にアクセスできる「友人」として登録してもらうために、さまざまなアピールをしてくることもあります。自分の情報を守るためにも、知らないユーザを不用意に友人として登録したりしないようにし、もしそうするなら、通常の Web ページと同じように公開する情報を自ら選択する必要があります。

そのほかにも、見知らぬ人とのコミュニケーションから、出会い系サイトと同様の問題も起こりえます。

SNS では、サービスへの参加を招待制にしているものもありますが、招待制のサービスだからといって悪意のあるユーザが居ないと保証されているわけではありません。悪意のあるユーザが一人でも入り込んでしまえば、いくらでも仲間を招き入れることができますし、退会するユーザのアカウントを買いとったりすることもありま

す[*13]。

欠陥プログラムを利用される

Web ページをいくつか覗くと、その中には、アクセスするたびに表示が変わる、アクセスする人によって表示がかわるなど、状況に応じて変化するようにプログラムされているものがあります。これらのプログラムは、Web アプリケーションと呼ばれます。Web ページ上で動かすプログラムはたくさんあり、本学の Web ページにも、実はたくさんのプログラムが使われています。Web アプリケーションは、Web サイト更新を簡単できるため、多くのホームページで採用されています。

最近では Web 上で様々なサービスが展開されており、利用者は居ながらにして時間を気にせずそれらのサービスを受けることができるようになりました。一方でサービスを提供しているアプリケーションが複雑になったことでサービスを構築する過程で発生した不具合に気づかずそれらが残されたまま運用されていることもあります。正式にサービスを提供しているサイトであっても、そのような弱点を利用されることで知らないうちに悪意のあるサイトに誘導されたり，利用者の情報を盗まれたりすることもあります。

どのようなサービス・システムであれ、ネットワーク上に情報を書き込む場合には常にどのようなリスクがあるかを考えるようにしましょう。

[*13] もちろんこれらの行為は、通常は規約で禁止されており、違反行為となります。

2.3 悪性ソフトウェア

インターネットの様々なサービス上には、多種多様なソフトウェアが公開されており、無料で使える有益なソフトウェアも数多く存在します。

しかし、なかには便利なソフトウェアを装って、悪性のソフトウェアをインストールするものがあったり、悪性とまでは言わないものの、完成度が低くコンピュータの動作に支障をきたしてしまうようなものもあります。

本節ではいくつかの代表的な悪性ソフトウェアについて解説します。

2.3.1 スパイウェア

スパイウェアとは、他のプログラムに同梱されて個人のコンピュータにインストールされたり、Web 閲覧の結果、コンピータにインストールされ、そのコンピュータを監視してデータを外部に流出させるプログラムを指します。

もともとは、マーケティング会社が個人がどのような Web を閲覧しているかを収集するために、本人の同意を得てインストールされるものでした。

しかし、当初から「本人の同意」と言ってもインストール途中で気づきにくいタイミングで同意ボタンを押すだけだったりするケースが多く、問題とされていました。

スパイウェアがインストールされると、

- 個人情報の流出
- コンピュータの性能低下
- スパムメールの増加

などの問題に遭遇します。

もともと問題の多かったスパイウェアですが、最近は悪意のあるスパイウェアも増えつつあります。

キーロガー

キーロガーと呼ばれるプログラムがインストールされると、そのコンピュータからキー入力する情報がすべて読み取られてしまいます。暗証番号、クレジットカード番号などの重要な情報は、どんなに暗号化されていてもキーボード入力だけは無力です。

集められた情報は一定時間毎にインターネット経由で作成者などに送信されます。

このため機密情報が第三者に流出する危険を常に抱えることになります。

しかもインストールされてしまったことに気づきにくく、対策も難しいスパイウェアと言えます。

アドウェア

アドウェアは、インストールされると起動するたびに、今まで表示されたこともない広告が表示されるようになったり、閲覧先を勝手に変えてしまって、本来のサイトではない広告サイトにたどり着くようになったりします。

巧妙なものとして、Yahoo などの著名なサイトにアクセスするとそのバナー広告を勝手に置き換えてしまい、別の広告を表示させたりするものがあります。

悪質なアドウェアのことを特にマルウェアと呼ぶこともあります。

このようなスパイウェアを駆除するソフトも存在します。しかし、駆除ソフトと偽ったスパイウェアもあった

りするので注意が必要です。[*14]

[*14] wikipedia(http://ja.wikipedia.org) に掲載された、現在十分安全とされている駆除ソフトは以下の通り。(類似名のスパイウェアもあるのでインストール時にはよく URL などを確認する必要がある。)(1) Ad-Aware (http://www.lavasoft.de) — スパイウェア対策ソフトの先駆者(2) Spybot - Search & Destroy (http://www.safer-networking.org/en/home/index.html) — 十分認知された除去ツール(インストール後、日本語で使える)

2.4 街角でのインターネットでのトラブル

最近は、ホットスポットと呼ばれる無線 LAN などの環境が整備され、街にモバイルコンピュータを持ち出して気軽にインターネットが楽しめるようになりました。また手ぶらで街に出ても、街角には、ところどころにインターネット端末が設置されており、そこからインターネットを利用できます。

しかし、そこにもまた、十分注意しなければならない危険が潜んでいます。

キーロガー

キーロガーとは、既に 2.3.1 で述べたように、キーボード入力された情報がすべて読み取られてしまう悪意あるプログラムのことです。

インターネットカフェなどでは、こうしたプログラムが仕掛けられている可能性があるということは常に意識しておくべきです。電子メールなどを読むためにパスワードを入力すればその情報が読み取られてしまうかもしれませんし、クレジットカード番号などはさらに危険です。この状況はもちろん世界中で変わることはありません。海外旅行などでインターネットカフェを利用する場合には十分注意する必要があります。

盗聴

インターネットでは、盗聴 (2.1.4 参照) は常にされていると考えるべきです。無線 LAN で個人の持ち込んだコンピュータであれば、キーロガーの心配は緩和されますが、盗聴は避けられません。特にコンピュータの設定をしっかりしておかないと、無線 LAN を経由してコンピュータの内部に容易に侵入されてしまうことになります。

最近のコンピュータは容易に第三者を侵入させないファイヤーウォールの仕掛けが用意されているものが多くあります。それらの設定を有効にしておくだけでも効果があります。

街角でインターネットを楽しむ場合でも、インターネットセキュリティに関する一通りの知識があれば、被害に遭うことは滅多にありません。反対に不用意な利用方法は思わぬトラブルに巻き込まれる危険性があります。

第 3 章

違法行為 ―あなたが加害者になるとき―

「インターネットは無法地帯」などと言う人がいますが、もちろん、そんなことはありません。法律に違反すれば当然罰せられます。法律以外にも、インターネット上で定められた様々な規約に違反すれば相応の処分が行われます。

また、十分な知識がなかったために、知らないうちにインターネット上の利用規則や法律に違反してしまうこともあるかもしれません。そうなれば、知らなかったでは済まされません。

軽い気持でしたことが、思わぬ重大な結果を招くことになります。

3.1 インターネットに関する法律

インターネットは、当然ながら我々が日常生活で律せられている法律の適用も受けています。しかしながら、インターネットの特性からそれだけでは律しきれない部分について、新たな立法措置がなされています。

現在その立法措置の効果については、さまざまな議論がなされていますが、はっきりしていることは、法的な知識が不十分なままでのインターネット利用は、思わぬ落し穴が待っていると考えるべきです。

インターネット関連の最も重要な法律は、「不正アクセス行為等の禁止に関する法律」（平成 11 年 8 月 13 日法律第 128 号）です。この他に、すでに述べた（2.1.5 参照）迷惑メールに関する法律などがあります。

また、民法上の名誉損壊などの定めや、著作権法、無限連鎖に関する法律など従来の法律もインターネットに深く関係しています。

不正アクセス禁止法の概要[*1]

3.1.1 不正アクセス禁止法

「不正アクセス行為等の禁止に関する法律」は通称「不正アクセス禁止法」と呼ばれています。この法律には、コンピュータに不正に侵入した者だけではなく侵入を幇助した者についても罰則が定められています。

そうなると、知らぬうちに法に触れる行為を犯してしまう可能性も排除できません。とりわけパスワードの貸し借りといった行為は、不正アクセス禁止法の観点から問題にならないとは言い切れません。

友達との間でもこうした行為は厳禁です。

3.1.2 適用事例

ここでは、2010 年に実際に発生した不正アクセス禁止法違反の検挙事例を見てみましょう[*2]。

[*1] 警察庁「不正アクセス行為等の禁止に関する法律の概要」（平成 12 年 1 月 17 日）
URL:http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm

[*2] 国家公安委員会他「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（平成 22 年 3 月 3 日）より転載

フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を不正に入手し、インターネットショッピングにおいて商品をだまし取った不正アクセス禁止法違反及び詐欺事件

無職の男（32）らは、平成 20 年 9 月から平成 21 年 11 月までの間、フィッシングにより他人の ID・パスワードやクレジットカード番号等を入手し、会員専用サイトに不正アクセスを行い、個人情報を入手した上、それを用いて他人になりすましてインターネットショッピングにおいて商品をだまし取った。平成 22 年 8 月までに、不正アクセス禁止法違反及び詐欺罪で検挙した（広島、岡山、静岡、福岡、愛媛）。

スパイウェアにより他人のＩＤ・パスワードを不正に取得し、オンラインゲームに不正アクセスするなどした不正アクセス禁止法違反事件

会社員の男（29）らは、平成 22 年 4 月から 6 月までの間、スパイウェアを組み込んだウェブサイトを開設して他人の ID・パスワードを不正に取得し、それを用いてオンラインゲームに不正アクセスを行い、入手したオンラインゲーム上のアイテムを現金に換金した。平成 22 年 11 月、不正アクセス禁止法違反で検挙した（神奈川）。

ここに掲げられた行為は確かに悪質ですが、それほどではなくとも友人のパスワードを使ってコンピュータにアクセスしたり、他人の電子メールを盗み見ることは、それだけで、不正アクセス禁止法の対象になり得ます。

またこの場合、パスワードを貸与した友人なども処罰の対象になるでしょう。

3.2 嫌がらせ

「インターネットは匿名性が高い」などという人がいますが、これは必ずしも本当ではありません。この言葉を信じて、日頃の恨みをこっそりインターネットで晴らそうなどと思うと、思わぬことになります。

第一に、少なくとも本学の施設を利用する以上、インターネットへのアクセスはすべて記録されています。インターネットは、決して匿名ではありません。

第二に、電子メールにしろ Web ページにしろ、すべての発信記録がどこかに残されます。名誉損壊などで訴えられたときに、動かぬ証拠とされてしまうでしょう。

また、あからさまに相手の名誉を傷つけようとは思わない人にも危険はあります。メールやニュースでは、相手の顔が見えないだけに、ついつい過激な発言が飛び出します。インターネット上での口論がエスカレートして、訴訟沙汰に巻き込まれるという事態も起こります。

3.3 著作権違反

3.3.1 画像

Web ページをあちこち覗いていると、楽しい画像をたくさん発見します。しかし、気軽に自分の Web ページに貼り付けていいかどうかは、よく判断しなければなりません。

映画やテーマパークなどの Web ページをよく見ると、画像の転載禁止をうたっているものがあるはずです。これらの画像を勝手に自分の Web ページに貼り付けることは著作権違反であり、厳しく罰せられます。

また、本や雑誌から画像を取り込んで Web ページに掲載することも、著作権に触れる行為です。

さらに、自分でとった写真でも、被写体が著作権で保護されているかもしれません。ブランドものの洋服やバッグなどもそれに該当します。

Web ページへの写真や画像の掲載は、著作権に十分配慮することが必要です。

3.3.2 替え歌など

著作権で保護されている歌詞を掲載することは、もちろん著作権違反ですが、面白い替え歌を考えたからといって、原著作者の許諾なしにネットニュースや Web ページに掲載するのも、著作権違反に問われます。

3.3.3 違法ダウンロード

これまでは、自分がコンテンツをネットワーク上に作成する、アップロードするときの話でしたが、ネットワーク上においてあるコンテンツをダウンロードする際にも著作権違反に問われることもあります。

2009 年 12 月 31 日までは、違法にアップロードされたファイルであっても、そのダウンロードについては私的使用のための複製の範囲に含まれていましたが、2010 年 1 月 1 日に施行された改正著作権法により、違法にアップロードされた映像、音楽ファイルを、そのファイルが違法アップロードされたものであると知りつつダウンロードすることも著作権法違反となります。

3.4 電子メールアドレス盗用

本学から匿名で発信できないからといって、他人のパスワードを使ってメールを出すなどという行為に及んだ場合はもちろん、一時的にせよ友人の設定を手伝ってあげるためにパスワードを利用することも、法的に見れば不正アクセスが成立します。

たとえ刑事罰に至らないとしても、本学においては、そのような行為が見つかった場合は、不正なパスワード使用として利用停止等の措置を受けます。

アカウント停止の措置を受けると、コンピュータ関係の授業が受けられないなどの大きな不利益を被ります。結果として卒業できないというケースも出てくることがあります。

気軽にパスワードを教えたり、教えられたりなどという関係を作らないようにしましょう。

3.5 ネズミ講ではありませんというネズミ講

ネズミ講は、法律用語では無限連鎖講と呼ばれており、「無限連鎖講の防止に関する法律」により厳しく取り締まられています。たとえ、そうとは知らずに参加してしまっても罪に問われます。

ネズミ講勧誘メールは、最近下火の傾向にありますが、なくなったわけではありません。当初は海外からの英語のものが多かったのですが、日本語のものも多く存在します。その典型的なメールは以下のようなものです。

> あなたにも素晴らしいチャンスを
> ＊＊　違法でなく２０００万円儲かるビジネスネットのご紹介　＊＊
> 簡単なマネーゲーム（小遣い稼ぎ）をやってみませんか？ 私がやったことは、書き換えたファイル（この文書です）をニュースグループやＢＢＳの電子掲示板などに（出来るだけ多くの！）アップロードすると、お金がどんどん銀行口座に振りこまれてくるんです。

この仕組みは、たとえば以下のようなものです。

> まず、名簿にある 4 人の口座に 1000 円ずつ振り込む。すると、レポートと称するものが送られてくる。それを受け取ったら名簿の一番上の名前を消して、４番目に自分の名前と口座を登録する。その更新された名簿をなるべく多くの人に電子メール等で送る。

仕組みはあきらかにネズミ講なのですが、こうしたメールには、たいてい、「これは違法ではない」とか「ネズミ講ではない」と書かれ、以下のような理由が述べられていることがあります。

- 1 人参加すると、最上位の 1 人が組織から抜けるため、「無限連鎖」ではない
- レポートという商品が介在しているため、金品配当組織ではなく無限連鎖講に当たらない

しかし、実際には警察はこうした商法を検挙しています。その理由は以下の通りであると考えられます。

- 法律上は、組織が無限に広がってゆくことを無限連鎖講であるための要件とはしていない
- レポートと称するものは、商品としての価値はまったくない（仮に価値があるものであれば、今度はマルチ商法とみなされるだけです）

他にも「不景気な時代なので互いに助けあうために、現金書留でお金を送り名簿に登録してもらおう」という例や、外国に本部を置くねずみ講の組織が「ドルを送金し、名簿を５人に送れば確実にもうかる」と日本国内の会員を勧誘しているケースもあります。外国から勧誘されたり、外国に送金した場合でも日本の法律は適用されますから、参加した場合は処罰の対象となります。

ねずみ講には、絶対に参加してはいけません。

無限連鎖講に加入することを勧誘した者は、二十万円以下の罰金に処せられます。

第 4 章

インターネットの脅威から身を守る

ここまではインターネットの恐ろしげな実体について様々なお話しをしてきましたが、実はそうした脅威は、インターネットにおける基本的な常識を身につけていれば、ほとんどの場合、防ぐことができます。この章では、そうしたインターネットでの基本的な常識についてお話しするつもりです。本章での内容を要約すると、以下のようになります。

- 自分のパスワードをしっかり管理する
- ネチケットを守る
- リスクを知り、リスクに応じた行動をとる
- プライバシーを守るための基本的な技術を身につける

4.1 パスワード管理がすべての基本

パスワードは、セキュリティの最後の砦であり、ユーザのモラルが試される場です。パスワードをしっかり管理することを覚えれば、自分自身が不愉快な思いをしないで済むということばかりでなく、学内全体のセキュリティ向上に貢献することにもなります。

4.1.1 パスワードが盗まれる時

最初に、パスワードは、どのようにして盗まれるのかについてお話ししましょう。

辞書攻撃

本学では、パスワードは、8 文字以上のアルファベットと数字で設定することになっています。8 文字のパスワードは、推測されにくいパスワードであれば、現在の最高速のコンピュータを使っても解読にある程度の時間が必要となります。反対に、推測されやすいパスワードの場合は、一瞬にして破られてしまいます。

推測されやすいパスワードとは、以下のようなものを言います。

- 自分の名前やユーザ名が含まれている
- 短い
  (例)`hmk,3r6j,r7tuk`
- 地名や人名が含まれている
  (例)`tokyo1,K_Yokota`
- タレントや有名人、漫画のキャラクター等の名前が含まれている

(例)doraAB,SMAP@,

- 有名な本や詩の一説が含まれている
  (例)letitbe,to_be_or
- 辞書に載っている単語が含まれている
  (例)dolphin,sakuraX
- 生年月日の年号等が含まれている
  (例)#990401,801025

これらの推測されやすいパスワードのことを、弱いパスワードとも言います。弱いパスワードは、辞書攻撃と呼ばれる方法で破られてしまいます。特に、自分の名前やアカウントが含まれているパスワードは最悪です。

辞書攻撃とは、誰もが使いそうな単語を集めた辞書を用意し、片端からパスワードに当ててみるというパスワード破りの常套手段のことを指します。

反対に、強いパスワードとは、こうした辞書攻撃に強いパスワードのことを言います。強いパスワードであるためには、以下の要件を満たしていなくてはなりません。

- 少なくとも 8 文字で構成されている
- アルファベットの大文字小文字と、数字のすべてが使われている

ところが、これは十分条件ではありません。つまり一概に何を強いパスワードというかは難しいところがあります。

たとえば、ここで「<Ttl*Hiw9> は強いパスワードです。」などと紹介してみても、誰かがこのマニュアルを読んで、辞書にこのパスワードを登録してしまえば、弱いパスワードになってしまいます。

力まかせ攻撃（ブルートフォース）

辞書攻撃で破れないパスワードは、力まかせに破るしかありません。つまり、aaaaaa、aaaaaaab、aaaaaaac…といったように、順にすべての文字の組合わせを試すのです。このような方法をブルートフォースと言います。

ブルートフォースは、一文字パスワードが長くなるだけで、解読に非常に時間がかかってしまいます。

1 秒間に 1 千万回の解読ができるコンピュータで、パスワードを力まかせに解読した時の予測時間を下表に示します。

文字数	文字の種類	解読予測時間
6 文字	英小文字のみ	15 秒
7 文字	英小文字のみ	6 分 30 秒
8 文字	英小文字のみ	3 時間
8 文字	英大小文字	30 日
8 文字	英大文字小文字数字	127 日
8 文字	英大小文字数字記号	1 年 2 ヶ月

見てわかる通り、使っている文字数と種類が増えるほど劇的に解読は困難になっていきます。ブルートフォースへの対抗手段は「できるだけ長いパスワード」ということがわかります。

ソーシャルエンジニアリング

パスワードを盗もうとする試みは、辞書攻撃やブルートフォースのようにコンピュータ上で行われるだけではありません。

侵入者たちがソーシャルエンジニアリングと呼んでいる方法は、コンピュータを使うことなしに、しかも割と簡単にパスワードを盗むことができる方法として好んで使われています。その主な方法をご紹介しましょう。

ショルダーサーフィン コンピュータに向かっている人の背後に回り、パスワードを入力するところを盗み見る
盗み読み パスワードを手帳などに記入してあったり、机の中に隠してあったり、コンピュータに貼り付けてあったりすると、それを盗み読む
詐称 システム管理者などを装い、本人からパスワードを聞き出す
なりすまし ユーザになりすまし、システム管理者からパスワードを聞き出す

要するに詐欺なのですが、案外これにひっかかってしまう人は多いのです。

4.1.2 悪いパスワード、良いパスワード

パスワード破りの手口がわかれば、対抗手段もおのずから決まってきます

パスワードはメモしない

ショルダーサーフィンに対抗するためには、背後に誰もいないことを確認してからパスワードを入力する習慣を身につけるべきでしょう。

さらに大事なことは、ショルダーサーフィンや盗み読みに対抗するためには、パスワードをメモなどにしておかないという習慣を身につけるべきです。

パスワードはみだりに口にしない

詐称や、なりすましに対抗するため、本学のシステム管理者は、電話やメールでパスワードを問いただすことは決してありません。また、みなさんからのパスワードに関する質問も、センターの窓口以外で受けることはありません。パスワードをみだりに口にしないというのも大事な心掛けです。

パスワードの定期的な変更

パスワードは、定期的に変更すべきです。どんな強いパスワードを作っても、知らないうちにパスワードが何者かにチェックされているかもしれません。その場合、今のコンピュータを使ってもパスワードは３ヶ月程度で破られてしまう可能性があります。

そこで、90 日程度でパスワードを変更していれば、万が一パスワードをチェックされても、破られた頃にはそのパスワードは役に立たなくなっていることになります。

パスワードの定期的な変更は面倒くさいし、幾つもパスワードを覚えなくてはならないので、つらいのですが、変更するだけの価値は十分にあります。

忘れにくく推測されにくいパスワード

パスワード管理の心得をまとめると、以下のようになります。

- 推測されにくい
- 書き留めない

- 忘れない
- 教えない
- 定期的に変更する

これらの各項は、互いにトレードオフの関係にあります。推測されにくいパスワードを作れば、覚えにくくなってしまうかもしれません。定期的に変更すれば、パスワードは忘れやすくなります。

過去に、いくつかの本で推測されにくいパスワードの作り方が紹介されましたが、今度は、パスワードを破る側がそれに対応する攻撃方法を編み出したりするというイタチごっこになることもあります。

とはいえ、今でもある程度有効と思われるパスワードの作り方の方法を紹介しましょう[*1]。

- 短い言葉を 2 つ選び記号や数字で連結する
  (例)`robo@4my,eye-con7`
- 自分には意味があるけれど、他の人には意味のない略語
  (例)Ttl*Hiw9(Twinkle,twinkle,little star. How I wonder...)

言うまでもないことですが、ここに紹介した例そのものは、今では弱いパスワードになっています。そのまま使ってはいけません。

また、パスワードを自動生成してくれるプログラムを使ったり、さいころを使ってパスワードを決めるなどの方法もあります。この中でも後者の方法は、理論的には、特に強いパスワードができると言われています。

4.2 マナーを守る

かつて、学術研究が中心であった時代のインターネットは、右も左もわからない初心者に対して寛容であり、大抵のわからないことは、ネットニュースに投稿すると、誰かが教えてくれたものです。そうして、初心者は次第にインターネット特有のマナーを覚えていったのです。この時代のインターネットは、いわば学術という村の社会の慣習が守られていたのでした。

大都会となってしまった今日のインターネットでは、様相は一変してしまいました。何せインターネットという街は、初心者があふれ、マナーを心得ない初心者同士のトラブルは後を絶ちません。

こうしたトラブルを未然に避けるためのインターネット上のマナーを「ネチケット」と呼んでいます。ネチケットという言葉は、「インターネット」と「エチケット」という言葉から造られた造語ですが、インターネットの標準規格である RFC[*2]の文書にちゃんと載っています。その文書とは、RFC 文書番号 1855 のことで、「ネチケットガイドライン」というタイトルがつけられています。

この文書には、今までこのマニュアルで述べてきたことの多くがカバーされています。

Web ページアドレスは、

```
http://www.cgh.ed.jp/netiquette/rfc1855j.html
```

です。

「ネチケットガイドライン」には、この他に電子メールやネットニュース、それにチャットなどにおける最低限のマナーなどが書いてあります。これらのマナーを知らずにインターネットに出かけることは、今や裸で街に

[*1] S. Garfinkel et al. *"Practical UNIX and Internet Security"*,1996,O'Reilly より

[*2] RFC は Request For Comments つまり「コメントを下さい」という意味の言葉の略称です。標準規格なのに「コメントを下さい」という言い回しはおかしいのですが、これにはインターネットの歴史的な経緯が関係しています。残念ながらここでそのことに触れる余裕がありませんので、興味のある方は調べてみてください。

出かけるようなものです。必ず目を通しておいてください。

その精神を一言で言えば、「冷静に慎重に寛大に」ということになります。これは、案外できそうで、難しいことではあります。それだけにインターネットを利用しようと思うときには肝に銘じておくべきことでしょう。

4.3 危険を前提に行動する

みなさんが車を運転したことがあるとしたら、時おり山道などで「落石注意」という看板を見掛けることがあるかもしれません。しかし、こんな看板に意味はあるのでしょうか？落石に注意しろと言っても注意のしようがないではありませんか。

一見無意味に見えるこの看板も、実は大事な意味があるのです。実際に落石が起ったときに、一瞬「何が起ったかわからない！」と思うか「あっ!落石」と思うかで行動は異なります。呆然としている間に落石に埋め尽くされてしまうか、適切な回避行動をとれるか、回避行動がほんの数秒でも遅れれば、それが決定的な差になります。落石注意の看板は、運転中に異常事態が起ったときに、ドライバーが、これは落石かもしれないと思い浮かべるための警告としての機能を持っているのです。「予知して未然に防ぐ」というリスクマネージメントの基本的なコンセプトがここにあります。

主として第 2 章でご紹介したインターネットの中で出会う様々な危険は、誰もが必ず出会うというものではありません。しかし、落石よりははるかに頻繁に出会うはずです。

インターネットを利用していると、いつかは「一瞬頭が空白になる」とか「ぞっとして手足が冷たくなる」とかいう瞬間がやってきます。その時にとるべき行動の指針は「冷静に慎重に寛大に」です。

インターネットを利用するときには、「予知して未然に防ぐ」というリスクマネージメントの心得が重要なのです。

4.4 自分のコンピュータの管理

今までのお話は、主として情報・メディア教育センターなどの、自分の所有しないコンピュータを利用する場合の問題をお話ししてきました。しかしながら、ご自身でコンピュータを所有しておられる方は、自分が利用者であると伴に、情報・メディア教育センターと同等のシステムの管理者になっているということを忘れてはなりません。

ウィルスやワーム

ウィルスやワームは学校のコンピュータであれば、システム管理者である学校が除去してくれます。しかし、自分のコンピュータはウィルス対策ソフトウェアを購入し、毎年更新する。定期的にウィルスチェックをするといった作業が今日では必須です。

それを怠ると、知らないうちにウィルスやワームに犯され、たくさんのウィルス付きのメールをばらまいてしまったり、ワームをインターネットに垂れ流すことになります。

脆弱性対策

コンピュータで使われているソフトウェアは基本ソフトを初めとして、かならず潜在的なセキュリティホールがあります。このようなソフトウェアの脆弱性は、毎日のようにインターネットに公表され、すばやく対策しなければ、悪意のある第三者にコンピュータを乗っ取られます。

各種の基本ソフトは、こうした脆弱性をインターネット経由で自動的に修復してくれる機能がついています。これらの機能を常時活用し、適切な脆弱性対策を施す必要があります。

踏み台にされる

以上のような対策を怠ると、あなたのコンピュータはたちどころに侵入され大事な情報が流出したり、また多くの場合、悪意のある第三者に利用されます。すなわち、あなたのコンピュータを誰かが支配し、別のサーバ（多くは各国政府や大きな会社）の攻撃に知らないうちに参加させられてしまいます。

このような状態を「踏み台」にされるといいます。ある調査によると、買ったばかりのコンピュータ何台かを何の対策もしないでインターネットに繋げておいたところ、ほぼ 30 分で何らかの侵入を受けたそうです。

P2P ファイル共有ソフトウェア (Winny など) の利用

Winny は、P2P（Peer To Peer）と呼ばれる仕組みを用いたファイル共有ソフトウェアの一つですが、作者が刑事告発されたり、官公庁や企業などからの情報漏洩の原因となるなど、問題のあるソフトウェアと見なされることがあります。

しかし、 P2P ファイル共有ソフトウェアは、コンテンツを効率よく取得する方法として非常に便利であり、有益な道具でもあります。様々な脅威があることを十分に認識した上で利用するか否かを決定する必要があります。一般にインターネットやコンピュータに対する知識が十分にあることが利用の前提と考えるべきです。

P2P の脅威

以下では、コンピュータ緊急対応センター「JPCERT-ED-2006-0001」に基づき解説致します。

P2P ファイル共有ソフトウェアネットワークからファイルを取得する際には、主にキーワード検索を利用してのファイルを取得します。このようなファイルは不特定多数のユーザ端末に保存されており、中には巧妙に細工された（例: プログラム以外のファイル名を装ったり、テキストファイルやフォルダのアイコンを持った実行形式のプログラム) 悪意のあるプログラムが含まれている事があります。

一般的には、P2P ファイル共有ソフトウェアには公開するファイルを指定する機能がありますが、上記のような悪意のあるプログラムを意図せず実行することにより、ユーザの端末内のファイルを公開してしまう可能性があります。さらに、端末内にある任意のファイルだけではなく、原理的には如何なる情報もファイルの形で公開してしまう可能性があります。

これまでに漏洩した情報の例として、以下のようなものがあります。

- 電子メールの履歴
- ブラウザに保存された Cookie 情報
- Word 等のワープロソフトの文書ファイル
- Excel 等の表計算ソフトのファイル
- デジタルカメラなどで撮影した画像ファイル

P2P ファイル共有ソフトウェアネットワークでは、ネットワークを形成しているユーザですら、公開、流出した情報を完全に回収する事は非常に難しく、被害の回復はほぼ不可能である事を認識する必要があります。

これに対するユーザが採るべき対策としては以下 2 点があります。

- P2P ファイル共有ソフトウェアを使う端末には重要なデータを保存しない。また重要なデータが入った、外部記憶装置 (USB メモリ、HDD 等) も接続しない
- ウィルス対策ソフトを導入し、パターンファイルを常に最新にしておく

今までお話ししてきたようなインターネットセキュリティの知識を良くわきまえて自分のコンピュータをしっ

かりと管理することは、自分自身のためだけでなく、世界中に迷惑をかけないための重要な心構えと言えます。

4.5 暗号電子メール

ここまでは技術的な話はほとんどしないで済ませてきましたが、最後に少しだけ技術的な話をしておきます。

前に電子メールは葉書のようなものだというお話をしました (2.1.4 参照)。これは RFC1855「ネチケットガイドライン」(4.2 参照) にも次のように書かれています。

> 自分が暗号化装置（ハードウェアかソフトウェア）を使っている場合を除き、インターネット上のメールは安全ではないものと考えておかなければならない。自分が葉書に書かないようなメッセージ〔クレジットカード番号やパスワードなど他人に知られたくない個人情報や非公開情報など〕は決してメールに含めてはいけない。

これを反対に言えば、適切な暗号化を行えば、葉書ではなく封書の電子メールを送ることができるということになります。このようなことを実現する暗号化ソフトはたくさんありますが、その中では、PGP(Pretty Good Privacy) というソフトが比較的普及しています。どのようにしたら PGP が使えるかということについては、ここでは触れません。

暗号化は、現在のところ電子メールのプライバシーを守る最良の方法といえます。暗号化された電子メールは、以下の問題を解決します。

- なりすまし
- メールの内容の盗聴
- メールの内容の改竄

しかし、良いことばかりではありません。同時に、次のような問題を抱えています。

- メールを出す側も受け取る側も暗号化ソフトを持っていなくてはいけないし、暗号化の方法を知っていなければならない。
- 暗号化は戦略物資として輸出規制が設けられている。

前者の問題は、インターネットを検索するなり、誰かに教えてもらうなりすれば解決できます。

しかし、後者の問題は注意が必要です。うかつにアメリカのサイトからソフトをダウンロードすれば、違法な輸出と見なされ、違反すれば 100 万ドルの罰金または 10 年の禁固刑に問われることがあります[*3]。暗号化ソフトのダウンロードをするときには、そのサイトのホームページの注意書をよく読んでから行ってください。

また、ダウンロードしたソフトは、暗号輸出を禁止されている国々へ持ち出すことはできません。うっかりコンピュータに入れたまま、そうした国に持っていってしまうなどということのないようにしてください。

4.6 セキュリティに配慮した Web ページを作る

第 2 章の第 2.2 節で Web ページをめぐる危険性を幾つか指摘しました。Web ページを作成しようと思い立っても、そこで指摘された危険をすべて避けようとすれば、面白いページにならないと思われたかもしれません。

しかし、そんなことはありません。

第一に、それはデザインの問題ですから、工夫次第で、安全で、しかも気の効いた Web ページは幾らでもできるはずです。

[*3] 最近の米国では年々規制緩和が進んできています。しかし、完全に規制がなくなったわけではありません。

第二に、危険を承知で Web ページを作成するというアプローチもあります。

ただし、そのような Web ページを作成した以上、それに伴うリスクは覚悟しなくてはなりません。

電子メールアドレスを掲載した以上、不愉快な電子メールが来たり、spam メールが来たりするのはやむを得ないことです。そのような電子メールは来るものだと割り切っていれば、不愉快な電子メールは無視して捨ててしまうでしょう。

写真がどこかに流出したとしても、それほど影響のない写真なら良いという判断もありえます。

一方、Web ページ上で動くプログラムを自分でダウンロードして使っている場合は、そのプログラムに欠陥があるかどうかに、いつも注意を払っていないといけないでしょう。そのためには、「コンピュータ緊急対応センター」[*4]のメーリングリストに参加して、そこからやってくるメールに、自分が使っているプログラムについて何か情報が流れていないかをいつも注意しているとか、セキュリティ関係の Web サイトのニュースなどから情報を収集する等が考えられます。

そのような管理ができないのであれば、自分でプログラムをダウンロードして使うということは、すべきではありません。

セキュリティに配慮した Web ページとは、それぞれの人が自分のスキルに応じてリスク管理を行っている Web ページということができるでしょう。

つまり、危険なことが起きたときに手に余るようなことのない Web ページ作りが大事なのです。

[*4] Web ページアドレスは http://www.jpcert.or.jp です。

第 5 章

情報セキュリティポリシーの遵守

本学では、平成 16 年 6 月に「武蔵大学情報セキュリティポリシー」を策定しました。このことにより学内のセキュリティ対策は一層充実することとなりました。

しかしながら、ポリシーは存在するだけでは意味がありません。このリーフレットを読まれる皆さんが遵守し、さらにポリシーの実現に協力していただくことによってはじめて維持することができるものです。

5.1　インシデントの状況に応じた協力

「武蔵大学情報セキュリティポリシー」（平成 16 年 6 月 18 日）では、まずコンピュータセキュリティインシデントというものを定めています。

セキュリティポリシーでは、セキュリティインシデントとは、「学内への不正アクセス、サービス妨害攻撃、コンピュータワームやコンピュータウィルスの学内への蔓延等、人為的事象に起因して、本学の情報資産に脅威を与えるような事象、およびそれに至るための行為または事象のこと。」と定められていますが、学内での何らかのコンピュータを巡るトラブルと考えていただいてよいでしょう。

このインシデントの区分をセキュリティポリシーでは 5 段階に分けています。

インシデントの大きさ	説明	Web ページの表示	カラー
高い	危機管理が必要とされる状態	深刻	赤
	深刻な被害の発生した状態	重大	橙
	実際の被害が確認された状態	高い	黄
	発生が確認された状態	注意	青
低い	発生が確認されていない状態	低い	緑

この状態は本学のイントラネットの上部には常に表示されており、インシデントの状態が変化すれば、表示が変更されるようになっています。

この表示にしたがって、それぞれの状態に応じた皆さんの協力をお願いする必要があります。

5.1.1　緑：通常

通常の状態です。しかしこの状態はみなさんに常に注意を払っていただきたい状態でもあります。以下のような状態が発生したら情報・メディア教育センターに速やかにお知らせ下さい。

- コンピュータを利用していたらウィルスチェッカーの警告が出た
- スイッチを入れても起動しないコンピュータがある。
- コンピュータは起動したが動作がいつもと異なる（遅い、見なれぬ画面になっている、利用中に突然リセットする）
- 見知らぬところからメールがたくさん届いた
- Web ページに全くアクセスできない

この他にも異常に気づかれた場合には情報・メディア教育センターに直ちに御連絡下さい。

5.1.2 青：注意

インシデントが調査中となっている状態です。すなわち何らかのトラブルは確認されたが、学内への影響は極めて限定的である場合です。

この時は、本学のイントラネットなどに情報・メディア教育センターからのお知らせが掲載されます。

そのお知らせにしたがって、さらに情報提供をいただくなどの御協力をお願いいたします。

5.1.3 黄：高い

インシデントが学内全体に影響を及ぼし始めた状態です。

この時は、本学のネットワークの一部が切り離されるなど、場所によってインターネットに接続できなくなるなどの障害が発生します。

授業等に支障が出る可能性もありますので、状況については Web ページなどを通じて皆様にお知らせ致します。

ご協力いただく内容は、Web ページおよび掲示板などに掲示されます。

> 本学では、2003 年 8 月から 9 月にかけて、学内にワームが発生し、その外部からの影響を最小限にとどめるためにダイヤルアップサーバなどの一時切り離しが行なわれました。こうした状況がここでいう「黄」の状態に当たります

5.1.4 橙：重大

本学の基幹ネットワーク等に影響が及んだ場合です。学内の多くのコンピュータがネットワークに接続できなくなるなどの事態が想定されます。

発生状況によっては、皆様に個別のお願いをする場合もあります。また、特別に事情をお聞きする場合も想定されます。

これらの措置は情報・メディア教育センターの手を離れて学長を中心とした情報システム会議の決定により実施されます。

情報公開は場合によっては一部制限されるかもしれません。

5.1.5 赤：深刻

不正アクセス禁止法などに違反する事例が発生したことを意味します。状況によっては皆様に情報を提供できない場合もありますが、極力お伝えできる情報はお伝えいたします。

学内のコンピュータの利用が一時完全に停止されるかもしれません。

5.2 学内の規則

情報セキュリティポリシーが制定される以前においても、本学においてネットワークポリシーはなかったわけではありません。「武蔵大学ネットワーク利用規程」がそれです。その中では、ユーザは以下の事項を遵守することになっています。

第 15 条 利用者は、次に掲げる事項を遵守しなければならない。

(1) 教育・研究及びその支援を目的として使用すること。
(2) 営利を目的に使用しないこと。
(3) 通信の秘密を侵さないこと。
(4) 個人情報を侵さないこと。
(5) 著作権を侵さないこと。
(6) ネットワークの正常な運用のために協力し、ネットワークに支障を来す行為を行わないこと。
(7) 法令又は公序良俗に反する行為を行わないこと。

これらの規則に違反した場合の処分は、次のように定められています。

第 16 条 センター長は、前条各号のいずれかに違反し、不正なネットワーク利用又はネットワーク運用に重大な支障を来す行為を行った利用者に対し、利用資格の制限その他の次に掲げる措置をとることができる。

(1) ID を一時的に抹消し、学長に報告する。
(2) その後の処置については、その不正利用者の身分に応じ、処罰に関する機関の決定に従う。

ここで定められている内容は「情報セキュリティポリシー」が施行されて以降も有効です。「情報セキュリティポリシー」は、この規程をさらに詳細に定めたものとなっているに過ぎません。

5.3 処分

情報・メディア教育センターが不正行為と認めたときは、関係法令に基づく処分を受ける他、以下の処分を受けることがあります。これらの処分は、情報・メディア教育センターの上位機関である「情報システム会議」にて最終的には決定されることになります。

- アカウント永久停止等の利用資格の制限
- 退学等の学籍上の処分

この結果、情報処理関係の科目を受講しなければ卒業できないという場合などは、利用資格制限を受けただけで科目受講が不可能になり、卒業できなくなる場合もあります。

インターネットセキュリティは一定のセキュリティ上の知識と注意力、そして自己に対する責任感さえあれば、それほどの被害に遭うことも、ましてや処分を受けてしまうこともそうそうはありません。

一方で、軽い気持ちでセキュリティ上の問題をすり抜けようとすると思わぬ落とし穴が待っています。

快適なインターネット利用のためにも、情報セキュリティポリシーをしっかりと身につけ遵守されるようにお願いいたします。