2 セキュリティ

セキュリティとは、インターネットを安心して利用するために注意を払うべき安全対策のことをいいます。インターネットは誰にでも開かれている自由な社会ですが、まだ秩序が整っていない発展途上の場という側面も持っていますので、自分の身は自分で守らなくてはなりません。したがって、侵入者や違法な行為を行う人々の存在を日頃から十分認識しておくことが大切です。

2.1 パスワードを管理すること

インターネット等に接続するために、入力したりコンピュータに設定しておいたりするユーザ ID とパスワードは、あなたが正当な利用者であることを証明する情報です。

キャッシュカードの暗証番号のように、あなたの財産とプライバシーを守っているだけでなく、コンピュータシステム全体を不正なネットワーク利用から保護する役目も果たしています。パスワードが悪意ある第三者に漏れた場合、本人のデータ等の破壊や本人になりすましての不正行為が行われるだけでなく、サーバのセキュリティが容易に破られ、サーバ上の各種情報が破壊されたり、他の利用者のパスワードが盗まれたりします。この場合、最初にパスワードを盗まれた利用者が処罰されることになります。

アカウントすなわちユーザ ID とパスワードを他人に利用されないようにすることは、インターネット利用者の大切な義務です。インターネットの利用者は、各自の責任においてアカウント特にパスワードを管理しなければなりません。「2.2 パスワードの管理方法」に示す例を参考にしてパスワードの管理を行うとともに、以下のルールに従って下さい。

- **他人のアカウントを使用しない。**
- **同一アカウントを複数のユーザで共有しない。**
- **アカウントを利用しなくなった場合は、速やかに管理者に連絡し、アカウントを停止する。**

  休眠アカウント（未使用ないし長期間利用しないアカウント）が悪用された場合も処罰の対象となる。休眠アカウントは最も狙われやすいアカウントであり、過去にもしばしば狙われた。実際パスワードが盗まれ悪用されたことで、本人が処罰されたこともある。
- **何かの理由で他人のパスワードを入手した場合は、速やかに本人にその旨を告げ、パスワードの変更を促す。**

2.2 パスワードの管理方法

- パスワードには自分の氏名、生年月日、電話番号など他人に容易に推測され易いものは使わず、**わかりにくいように工夫** する。
- パスワードを **他人に教えない**。
- パスワードを入力するときは他人に **覗かれないようにする**。
- 同じパスワードを **複数のアカウントで使わない**。パスワードを **紙に書き残さない**。
- パスワードを保存したパソコンやソフトウェアをそのまま **他人に使わせない**。
- ユーザ ID やパスワードを尋ねる **不審な問い合せには応じない**。
- パスワードを破られたことに気づいた場合は、**直ちに管理者に連絡** する。

2.3 プライバシーの守り方

なんらかの必要からインターネット上に個人情報を発信するときには、それによって生じる利益だけでなく、**不利益が発生する可能性のあることを配慮する習慣** をつけて下さい。銀行口座の暗証番号やクレジットカードの番号を人に知られないようにすることはもちろん大切ですが、あなたがどこの誰なのかを知られてしまう住所、氏名、電話番号、生年月日などの個人情報にも注意を払って下さい。

電子メール・メーリングリスト・ウェブサイトに署名をしたり連絡先を記述するときには、**個人情報の記述に注意** して下さい。懸賞やアンケート調査を装って個人情報を集め、宣伝のメールを送りつける業者もあるので、そのウェブサイトの運営者が信頼できるかどうかに注意して利用して下さい。

2.4 コンピュータウイルスに注意する

コンピュータウイルスと呼ばれる悪質なプログラムによる被害は年々深刻化しています。特に、電子メールの添付ファイルに感染するウイルスや USB メモリからの感染、ウェブサイト閲覧からの感染が多く見られます。

ウイルスに感染すると、その種類によってコンピュータが動かなくなったりファイルが壊れたりと、さまざまな障害が引き起こされます。ウイルスはプログラムやデータを媒介して伝染するので、見知らぬ相手から来た電子メールや添付ファイル、ダウンロードしたり外部から持ち込まれたりするプログラムやデータを開くときには注意が必要です。

ファイルをアップロードしたり、電子メールに添付して送信したりする場合には、あらかじめコンピュータウイルスに感染していないことを確かめる習慣をつけて下さい。

また、コンピュータウイルスは、USB メモリやスマートフォン等の外部ストレージを介して感染することもあります。他人から借りた USB メモリやスマートフォン等を使用する場合も、あらかじめコンピュータウイルスに感染していないことを確かめる習慣をつけて下さい。

ウイルスの対策にあたっては、以下のルールに従って下さい。

- **見知らぬ相手から届いた添付ファイル付きのメールは厳重注意する。**
- **親しい相手から届いたメールでも、本文に添付ファイルについての記述がないときは添付ファイルを開かない。**
- **実行形式の添付ファイルに感染するウイルスには、システムの破壊を行うなど、特に悪質なものが多いので、実行形式の添付ファイルは不用意にクリックしない。**
- **見知らぬ相手から届いたメールや迷惑メールの本文中にある URL をクリックしない。**
- **ウイルスチェックプログラムでチェックしないまま、インターネットからダウンロードしたファイルを実行したり、外部から持ち込んだ USB メモリなどを使用しない。**
- **万一のウイルス被害に備えるため、データのバックアップを行う。**
- **できるだけ、受信するメールの形式は HTML 形式ではなくテキスト形式に設定する。**

2.5 コンピュータウイルスへの対策

コンピュータウイルスの感染を即座に知らせ、これを無効にする専用のソフトウェアが市販されています。これらは一般に「ウイルス対策ソフト」と呼ばれ、あらかじめインストールしておけば、外部から持ち込まれるプログラムやデータがウイルスに冒されていないかどうかを監視してくれます。

ウイルス対策ソフトをパソコンにインストールして使用して下さい。ただし、毎日のように新種のウイルスが発見され、報告されていますから、ウイルス対策ソフトにはこまめにインターネットから **最新のデータ** （定義ファイルまたはパターンファイルと呼ばれる。） をダウンロードし、新種のウイルスにも対応できるようにしておいて下さい。

ウイルス対策ソフトを用いても、残念ながらウイルス対策は万全とはいえません。定期的にデータの **バックアップ** をとっておけば、万一ウイルスに感染しても被害を最小限に抑えることができます。

ウイルスを発見したり、ウイルス感染の被害にあった場合は、すぐに当該部局の責任者、管理者ないし担当者に **感染の経緯について報告** するとともに、周辺の利用者にも警告を行って下さい。

2.6 不正なネットワークは利用しない

アクセスすることが許されていないコンピュータシステム内に侵入したり、データを見たり、改ざんする行為、あるいはそのコンピュータシステムを利用したり、その運用を妨害したり、損傷を与える行為をしてはいけません。

また、他人のパスワードを盗むこと、他人の電子メールを偽造すること、たくさんの電子メールや容量の大きな電子メールを一度に送る、いわゆる電子メール爆弾を送る行為、インターネット上を流れているデータを盗み取ったり改ざんする行為などは、すべて不正なネットワーク利用ですから決してしてはいけません。

2.7 学内のネットワークの不正使用禁止

学内のネットワークは、許可されたコンピュータのみ接続が可能です。