［小樽商科大学　情報総合センター］

情報セキュリティやネットワーク利用マナーについて

1、OSやソフトウェアは常に最新の状態にする【脆弱性対策】

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

2、ウイルス対策ソフトを導入し適切に利用する【ウイルス対策】

ユーザID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。

3、無線LANの盗聴や無断使用を防ぐ【無線LANのルール】

適切なセキュリティ設定がされていない無線LANは、通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があります。無線LANの盗聴対策や無断使用を防止するようにセキュリティ設定をしましょう。

4、バックアップを励行する【バックアップのルール】

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えてしまうことがあります。このような不測の事態に備えて、バックアップを取得しておきましょう。

5、インターネットを介したトラブルを防ぐ【ウェブ利用のルール】

悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性があります。また、SNSや掲示板へ悪ふざけ投稿や秘密情報の意図せぬ掲載で大学に被害を及ぼすことがあります。

6、マナーも意識しつつ、メールの活用のときのトラブルを防ぐ【メール利用のルール】

メールに添付されたファイルを開いたり、メール本文中に記載されたURLリンクをクリックしたりすることでウイルス感染する事故が続いています。身に覚えのないメールの添付ファイルやURLリンクへのアクセスに気をつけましょう。

また、重要情報をメールで送るときは、メールの本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付します。パスワードはそのメールには書き込まず、電話等の別の手段で通知することが必要です。

【メール利用上のマナー】

1. 一度送信してしまったメールは取り消せません。送信前に送信先等を確かめた上で送信しましょう。
2. 他の人に同じ内容のメールを転送する事を要求するメールのことを「チェーンメール」と言います。このような メールが届いた際には、その送信元が親しい間柄の人でもその要求に従うのは控えましょう。
3. 心当たりのない差出人からのメールの取り扱いには注意しましょう。こういったメールは「開かない」、「添付ファイルをダブルクリックしない」といった対応が、情報流出を避けるために重要です。
4. 場合に応じて電話や FAX も併用しましょう。電子メールだけが連絡手段ではありません。適切な連絡手段を選択できるようになりましょう。
5. 電子メールの件名は分かりやすく、簡潔に書きましょう
6. 電子メールの本文の最初に送付先の宛名を記載しましょう。特に就職活動のメールでは必ず「企業名」と「部署」も含め間違いのないように記載してください。
7. 宛名を記載した次に自分の氏名を記載しましょう。大学の先生や職員に向けたメールの場合は学生番号も記載してください。
8. メールの最後には、誰からメールが送られてきたかがわかるように、メール送信者の「氏名」や「メールアドレ ス等の連絡先」を記載しましょう。ただし、住所や電話番号等の個人情報については必要以上に公開しないよう注 意しましょう。
9. 送信先にメールを読んでもらうためにも、「イタズラメール」や「コンピュータウィルス」と間違われるような件名のメールを送信するのは避けましょう。
10. 添付ファイルを送信するときは、添付ファイル名を本文中に記載しましょう。
11. 添付ファイルの容量には注意しましょう。特別な理由がない限りは、2〜3MByte 位までが一つの目安です。

7、その他

1. 各種パスワードは絶対に他人に教えないでください。そのパスワードを用いて他人が悪質な行為を働いたとしても、その悪質な行為の責任はパスワードの管理責任を持つあなたにあるとみなされます。
2. 他人のユーザ ID・パスワードを不正に取得したり、その取得したユーザ ID・パスワードの利用は絶対に行わないでください。不正アクセス行為として刑法で処罰されます。