情報セキュリティの手引き

危機管理委員会 情報セキュリティ部会

－手引きの目的－

本手引きは、2006 年度に本学で制定された「情報セキュリティ対策ガイドライン」がベースとなっており、業務の中で起こり得る情報セキュリティ上のリスクに対応する上で留意すべき事項を、教員の皆様に提供することを目的としています。

私生活においても役立つ情報が含まれておりますので、情報セキュリティ管理を行う際の参考情報としてご活用ください。

1. ID とパスワードの管理について

Web ページの更新作業をゼミ生等に依頼するため、自分の ID とパスワードを教えたい。

学生だけでなく、どんなに親しい間柄であってもパスワードを教えることには様々な危険が伴います。パスワードは教えないようご注意ください。

⇒パスワードは 6 文字以上で容易に推測できないものを設定してください。

（参考）

銀行等からのメールを装い、メールの受信者に偽りのホームページにアクセスするように仕向け、そのページにおいてクレジットカード番号や ID、パスワード等を不正に入手する「フィッシング詐欺」と言われる手口が横行しています。

また、もっともらしい会社名を名乗り、「裁判所」「自宅へ回収員を・・・」などの文章で攻める「架空請求」といった、様々なインターネット詐欺も横行しています。身に覚えの無い場合は完全無視に徹してください。

2. 重要情報の取り扱いについて

ゼミ生等に連絡をとりたい場合があるため、学生の携帯電話番号を収集したい。

学生の個人情報の収集は、大学が業務上行うことになっています。
授業の運営上必要な場合には、学生個人の同意を得てから収集してください。

Web ページでクラス、ゼミ生の名簿を公開したい。

本人の同意なしで Web ページに名簿を掲載したり、第三者に渡さないようご注意ください。また、公開はもちろん、名簿を作成する時点で本人の同意が必要です。

自宅で採点作業を行うため、名簿や成績情報を持ち帰りたい。

大学経営に関わる個人情報や機密情報等のデータを学外へ持ち出す場合は、認証機能付き電子媒体の使用やデータの暗号化を行ってください。また、盗難による情報漏えいを防止するため、移動の際には、媒体を車の中等に放置せず、必ず身に付けるようにしてください。

※万が一、紛失や盗難の被害にあった場合には、速やかに各校舎総務課長（個人情報保護委員会幹事）まで届け出てください。（2005 年 4 月 1 日付「個人情報の適正管理の徹底について」参照）

データ入力作業を業者に委託したい。学生名簿をメールで送信したい。

委託業者と個人情報保護に関する契約や守秘義務契約を締結してください。

⇒収集した個人情報の入力や処理等を業者に委託する場合は、情報漏えいが起こらないようご配慮ください。

学生名簿をメールで送信したい。

送信先のアドレスを十分に確認し、添付ファイルは暗号化、もしくは開封パスワードの設定を行ってください。

FAX を使用する場合は、送信先に事前に連絡し、送信後電話で受領確認を行ってください。

不要となった用紙、FD や CD、パソコンを廃棄したい。

名簿や答案用紙、成績等の個人情報が記載された書類はシュレッダーで処理し、FD や CD 等は物理的に破壊するなど、読み取りができないようにしてから廃棄してください。また、パソコンを廃棄する際は、専用のソフトウェアを用いてハードディスクに記録されているデータを消去してから廃棄してください。

研究室で飲食を行っている。

汚損、損傷等を防ぐため、書類や記録媒体、情報機器の近くでの飲食は行わないようにしてください。

教員用ファイルサーバに成績情報を保存したい。

成績等の重要情報は保存しないようにしてください。
教員用ファイルサーバは、学生のアクセスも可能となっています。

3. 個人所有パソコンの管理について

個人所有のパソコンを学内のネットワークに接続したい。

接続する前に、情報メディアセンターへの接続申請手続きをお願いいたします。
接続する際、ウィルス感染によりパソコンに保管している個人情報が流出することを防ぐため、ウィルス対策ソフトウェアを導入し、常にウィルスパターンファイルを最新の状態に保つようにしてください。詳しくは情報メディアセンターまたは教員ヘルプデスクまでお尋ねください。

ファイル交換ソフトウェアを使用したい。

研究上の必要性から利用する場合には、成績等の個人情報等、重要なデータは、そのパソコンで扱わないでください。また、当該ソフトウェアに限らず、出所の不明な添付ファイルやダウンロードファイルは利用しないようにしてください。

⇒他大学や企業等において、ウィルスに感染したパソコンで Winny 等のファイル交換ソフトウェアを使用して、個人情報や機密情報が流出してしまった事件が多数報告されています。

4. 研究室の入退室、離席について

数分の離席であれば、研究室の施錠は行っていない。

数分であっても離席時は研究室の扉を施錠する、または、個人情報を保管しているパソコンや、名簿、答案用紙、採点簿等の個人情報が掲載されている書類が保管されたキャビネットは施錠するように心がけてください。

⇒重要情報を扱っているときは学生や部外者を入室させないようにし、当該情報を扱っていない場合であっても学生を研究室に残したまま席を離れないことも大切です。

共同利用のパソコンにログインしたまま離席した。

席を離れる場合はログアウトしたり、操作をロックすることを心がけてください。

⇒ログインしたまま離席すると、作業内容を盗み見られたり、情報が改ざんされる可能性があります。

5. 著作権管理について

ゼミ用 Web ページの管理は学生に任せている。

ゼミ用の Web ページを作成する場合には、著作権違反のないようご注意ください。

⇒ゼミ生が勝手に違法コピーしたと思われる音楽や映像ファイルを公開したり、著作権のあるキャラクタの画像を無断利用している場合、指導教員の管理責任が問われる場合があります。

以上