# 事務電算システム利用心得

事務システムを使用する前に以下のことを読み、守ってください。

## 1 はじめに

事務システムでは氏名、住所、成績等学生に関する大量のデータを管理している。これらの情報の多くは永久保存すべきデータであり、また学生と大学の信頼関係のもとに大学が管理しているものである。当然ながら、データの改ざん・漏洩等は厳しく罰せられるものであり、意図的でない間違いであっても大学と学生の信頼関係を大きく損なうものである。

そのため、事務システムの操作については、操作そのものに注意を払うだけでなく、常にモラルをもって臨まなくてはならない。

## 2 ID とパスワード

全ての作業の権限制御と操作記録は個人 ID で管理されています。従って、トラブルが発生した際にはその ID の所有者が第一に責を負うことになる。ただし、個人 ID は職員番号なので本人以外が知っていることもあるため、その ID で作業するのが本人であるかどうかはパスワードで判断します。従って、例え上司、同僚、部下、システム管理者、家族であっても、自分のパスワードは他人に絶対に教えないようにしてください。パスワードを教えた結果、トラブルが発生した場合は、ID 所有者がまず処罰対象となります。また、パスワードは簡単に推測できるものは避け、一定期間毎に必ず変更するようにしてください。

## 3 作業中において

ID とパスワードに注意を払っていても、事務システムを開いたまま席を外せば他人が操作することが可能です。したがって事務システムを使用しているときは席を外さないようにし、席を外すときは必ず事務システムを閉じるよう心がけてください。

## 4 手続について

事務システムを利用することにより、業務は迅速に処理することができます。ただし、これは手続きが簡略化された訳ではありません。従来どおり、成績変更や学籍異動、成績判定の変更等は確認・了承を書面上で必ず受けるようにしてください。また、確認・了承印のない処理依頼、例えば電話やメールによる依頼は絶対受けないようにしてください。

正式な手続きをせずに処理を行うと、改ざんでない場合でも、個人で勝手に行ったとして、処罰を受けることもあります。

# 5 最後に

事務システムにおいて、不明な点やトラブルが生じた場合は、個人で判断しないで事務システム管理者に早急に連絡し、判断を仰ぐようにしてください。

# 参考資料

## 個人情報に関して

### 個人情報とは

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号、画像若しくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することにより当該個人を識別できるものを含む。）をいう。（民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン－1997 年 3 月 4 日通商産業省告示第 98 号－）

### 個人情報の中でも特に取り扱いに慎重を要する項目

事務システムで取り扱っている個人情報には非常に多くの項目が含まれています。その中でも特に以下の項目の取り扱いは慎重に行ってください。

(1) 本人および保証人の連絡先に関する事項

住所、電話番号、e-mail アドレス等、個人の所在や連絡先を特定する項目です。不用意に教えてしまうとストーカー行為をはじめ犯罪に巻き込まれる可能性もあり、女子学生や 1 人暮らしをしている学生を抱える大学としては、特に情報管理に注意を払うべきです。

(2) 成績評価に関する事項

成績は個人に対する評価の項目です。

(3) 学籍異動に関する事項

停学等の賞罰や休学といった学籍異動処理によるものだけでなく、進級卒業の成績判定を含んだ内容を指します。

### 個人情報守秘義務

個人情報を取り扱う大学教職員は、職務に関して知り得た個人情報の内容を他に知らせ、又は不当な目的に使用してはならない。その職を退いたときも同様とする。

## 懲罰規定

個人情報の流出及び改ざん行為は、「大学が定める規定に違反したとき」または「故意または重大な過失によって大学に不利益をおよぼしたとき」にあたり、懲戒処分の対象となり、損害賠償の義務が発生することがあります。当然のことながら、上司も責任が問われます。

## 情報開示の条件

大学にとって学生は構成員であると同時に顧客でもあるわけです。顧客情報と考えれば、その存在の有無でさえ、原則として本人の了解なしに本人以外に情報を提供してはならない。以下に個人情報開示のガイドラインによる開示条件の概要を示しておきます。

(1) 理事会、教授会、学部長会議等の決定による場合。

(2) 法令に基づく、あるいは官公庁からの申請による場合。

(3) 本人の同意に基づく場合。

(4) 大学が業務遂行のために収集した目的のために利用する場合。

(5) 個人の生命、身体、財産の保全上緊急に必要とする場合。

(6) 社会的に必要かつ相当な理由があり、開示しても本人の不利益になる恐れがないと判断する場合。

## パスワード

パスワードは家で言えば、玄関の鍵にあたります。他人に教えないだけでなく、他人に分からないようにする必要があります。上限である文字数で作成するよう心がけてください。また、こまめに変更するという対応も忘れないようにしてください。その他パスワードに関する注意事項をまとめておきます。

(1) 英文字（大文字・小文字）や数字、記号を組み合わせて使用する。

(2) ユーザ ID と同じものや、名前、電話番号、誕生日などを避ける。

(3) 辞書に載っているような単語は避ける。普通の英語辞典であれば、全検索でも 45 分程度で終わってしまいます。

(4) メモしない。メモしなければ覚えられないようなものは不適切である。

(5) 他人に教えない。システム管理者であってもパスワードを尋ねることはない。

(6) パスワードをパソコンに登録しない。

また、不正アクセス行為の禁止に関する法律（2000 年 2 月 13 日施行）では不正なパスワード使用について以下のように定められています。

(1) 勝手に他人の ID やパスワードを使う（一年以下の懲役又は 50 万円以下の罰金）

(2) 勝手に他人の ID やパスワードを教える（30 万円以下の罰金）

## 個人情報保護の基本的原則

個人情報は、明確な利用目的のもとに、適当な場合には当事者の同意を得て、適法かつ公正な手段で収集されなければならず、提示した利用目的以外に使用すべきではない。また、情報は正確かつ安全にたもたれなければならない。そして、情報に係る政策、所在、管理者は明らかにされなければならず、当事者の申し出によるデータの修正、削除が保証されなければなりません。データの内容及び利用に決定権限を持つ者はこれらを実施するための措置に従う責任を負うべきとされます。

1980 年に OECD（経済協力開発機構）は「プライバシー保護と個人データの流通についてのガイドラインに関する理事会報告」、通称 OECD プライバシー・ガイドラインと呼ばれる 8 原則を提唱しました。これはその後に大きな影響を与え、日本でも個人情報保護を検討する際の基礎となっています。

(1) 収集制限の原則

個人データの取集は適法かつ公正な手段によるべきであり、適当な場合にデータ主体に通知又は同意を得て行うべき。

(2) データの正確性の原則

個人データは、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、完全、最新に保たねばならない。

(3) 目的明確化の原則

収集目的は収集時より遅くならない時期に明確化されなければならず、その後の利用は収集目的と両立し、かつ明確化されたものに制限するべき。

(4) 利用制限の原則

個人データは明確化された目的以外に使用されるべきでない。

(5) 安全保護の原則

個人データは紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

(6) 公開の原則

個人データに係る開発、実施、政策は一般に公開されなければならない。また、データ管理者を明示する手段を容易に利用できなければならない。

(7) 個人参加の原則

自己に関するデータの所在を確認し、知らしめるべき。また、自己に関するデータについて異議申立ができ、異議が認められた場合には、データの消去、修正、完全化、補正ができなければならない。

(8) 責任の原則

データ管理者は、以上の原則を実施するための措置に従う責任を有するべき。

以上