

○PCその他情報機器の取扱いに関する細則

2011年（平成23年）7月21日

制定

（目的）

第1条 この細則は、「東京経済大学情報システムの利用に関する規程」第7条に基づき、情報資産の保護の観点から、PC及びスマートフォン、その他情報機器（以下「情報機器」という）の利用に関して、必要な事項を定めることを目的とする。

（適用対象情報機器及び対象者）

第2条 この細則は、本学が管理する情報機器、本学の情報資産を取り扱う情報機器、本学ネットワークに接続する情報機器を適用対象とし、その対象情報機器を管理・利用するすべての者に適用する。

（用語の定義）

第3条 この細則において、次の各号に掲げる用語の意味は、当該各号に定めるところによる。

- (1) 利用者とは、この細則が対象とする情報機器を操作する者をいう。
- (2) 管理責任者とは、この細則が対象とする情報機器の運用管理に対する責任を持つ者をいう。

（管理責任者の指定）

第4条 この細則が対象とする情報機器について、管理責任者は、次に定めるとおりとする。

- (1) 情報機器が設置されている教室及びPCコーナーの情報機器は、その情報機器を設置した委員会の委員長を管理責任者とする。
- (2) 研究個室に設置される情報機器は、その個室を利用している教員を管理責任者とする。
- (3) 特任講師室に設置される情報機器は、その情報機器を設置した委員会の委員長を管理責任者とする。
- (4) 職員が使用する事務処理用の情報機器は、その情報機器を設置した委員会の委員長を管理責任者とする。
- (5) 各組織・委員会が独自に導入設置した情報機器は、それぞれの組織・委員会の長を管理責任者とする。
- (6) 教職員・学生が持ち込み、本学ネットワークに接続する個人所有の情報機器は、持ち込んだ者を管理責任者とする。

（利用者の責務・物理的損傷行為の禁止）

第5条 利用者は、情報機器に物理的損傷を与える可能性のある次に掲げる行為をしてはならない。

- (1) コネクタ等を引き抜く行為や、キーボードやマウス等周辺機器を取り外す行為。
- (2) DVDドライブ等、開口部に異物を詰める行為。
- (3) キーボードの乱打、USBメモリ等の乱暴な抜き差し。
- (4) その他、情報機器が物理的に損傷する可能性のある行為。

(利用者の責務・共用情報機器利用上の遵守事項)

第6条 利用者は、学内共用情報機器を利用する場合には、次の各号に掲げる事項を遵守しなければならない。

- (1) 共用情報機器を長時間占有しないこと。
- (2) PCL教室やPCコーナー等の共用スペースで、大声で騒ぐ行為や、ごみを放置する行為を行わないこと。
- (3) 共用情報機器が設置してある場所で飲食しないこと。
- (4) 共用情報機器の不具合、プリンタの紙詰まりや紙切れ、トナー切れ等の不具合を放置しないこと。
- (5) 本学ネットワーク帯域を極度に圧迫する行為を行わないこと。
- (6) 情報機器を操作中に離席しないこと。
- (7) 使用後は情報機器等の電源を切ること。
- (8) その他、他の利用者の利用を妨げないこと。

(利用者の責務・移動可能情報機器利用上の遵守事項)

第7条 利用者は、移動可能な情報機器を利用する場合には、次の各号に掲げる事項を遵守しなければならない。

- (1) 短時間であっても、情報機器を放置しないこと。
- (2) 教職員は、移動可能な情報機器を保管する際は施錠可能な場所に保管すること。
- (3) 要保護情報を移動可能な情報機器に保存する場合は、暗号化やパスワード保護等、情報漏えいを防止する対策を講ずること。
- (4) 要保護情報を移動可能な情報機器に保存する場合は、必要最小限のファイルのみを保存し、不要となった時点でただちに削除すること。
- (5) 移動可能な情報機器が、盗難・紛失・画面の覗き見等による情報漏えいのおそれがあることを十分に認識したうえで、細心の注意を払い使用すること。
- (6) 学生は、要保護情報が保存された移動可能な情報機器の紛失及び盗難の場合は、ただちに学生課に報告すること。
- (7) 教職員は、要保護情報が保存された移動可能な情報機器の紛失及び盗難の場合は、ただちに総務課に報告すること。職員の場合は上長を通じて報告すること。

(利用者の責務・ソフトウェアのインストールにおける遵守事項)

第8条 利用者は、ソフトウェアのインストール及び使用することに関して、次の各号に掲げる事項を遵守しなければならない。

- (1) 本学が管理する情報機器に、管理責任者の許可なくソフトウェアをインストールしてはならない。教育・研究目的及びそれらを支援する目的でソフトウェアのインストールが必要な場合は、その目的とソフトウェア名等を管理責任者に申請し、事前に承認を得なければならない。
- (2) ソフトウェアの利用条件に従って利用しなければならない。

(利用者の責務・外部記録媒体利用上の遵守事項)

第9条 利用者は、USBメモリ等の外部記録媒体を利用する場合には、次の各号に掲げる事項を遵守しなければならない。

- (1) 外部記録媒体を放置しないこと。
- (2) 放置してある又は出所が定かでない外部記録媒体を情報機器に挿入しアクセスしてはならない。そのような媒体を発見した場合は、学生課に届けること。
- (3) 使用済みの外部記録媒体を譲渡又は破棄する場合は、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。
- (4) 職員は、要保護情報を外部記録媒体に保存する必要がある場合には、大学が配布する外部記録媒体を利用すること。
- (5) 職員は、要保護情報を大学が配布する外部記録媒体以外に保存する必要がある場合は、その目的と外部記録媒体の種類等について、上長の承認を得なければならない。
- (6) 職員は、大学が配布する外部記録媒体以外を本学ネットワークに接続した情報機器で利用する必要がある場合は、当該外部記録媒体がウィルス等に感染していないことを本学ネットワークに接続していない情報機器で事前に確認したうえで利用しなければならない。
- (7) 利用者は、USBメモリ等外部記録媒体が盗難・紛失・ウィルス感染等のおそれがあることを十分に認識したうえで、細心の注意を払い使用すること。
- (8) 学生は、要保護情報が保存された外部記録媒体の紛失及び盗難の場合は、ただちに学生課に報告すること。
- (9) 教職員は、要保護情報が保存された外部記録媒体の紛失及び盗難の場合は、ただちに総務課に報告すること。職員の場合は上長を通じて報告すること。

(管理責任者の責務・情報漏えいに関わる遵守事項)

第10条 管理責任者は、自らが管理する情報機器に関して、次の各号に掲げる事項を遵守しなければならない。

- (1) 利用者が情報機器を認証なしで利用できないようにすること。情報機器が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。
- (2) ネットワークを経由して、不特定多数の第三者が情報機器にアクセスできないようにすること。ただし、情報発信のためにWebサーバー等を公開する場合は、第13条の定めに従うことを前提に、この限りではない。
- (3) 盗難による情報漏えいを防止するために、設置場所・保管場所に施錠等の措置をとるとともに、必要に応じて機器にワイヤーロック等の盗難防止措置をとること。
- (4) 情報機器を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要保護情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

(管理責任者の責務・ソフトウェアのインストールにおける遵守事項)

第11条 管理責任者は、自らが管理する情報機器にソフトウェアをインストールする場合には、次の各号に掲げる事項を遵守しなければならない。

- (1) 本学が管理する情報機器に、教育・研究目的及びそれらを支援する目的に合致しないソフトウェアをインストールしないこと。
- (2) インストールするソフトウェアの利用条件に従ってインストールすること。
- (3) ソフトウェアをインストールする前に、ウィルス対策ソフトウェア等により、有害ソフトウェアが含まれていないことを確認すること。
- (4) 出所の定かでないソフトウェアをインストールしないこと。
- (5) 教育・研究目的及びそれらを支援する目的において、情報漏えいや他利用者への迷惑行為となる可能性のあるソフトウェアをインストールする必要がある場合は、情報セキュリティ委員会に申請し、事前に承認を得ること。

(管理責任者の責務・セキュリティ脅威への対応)

第12条 管理責任者は、情報機器がウィルス、ワーム等に感染しないように、次の各号に掲げる事項を遵守しなければならない。

- (1) 利用しているOS、ソフトウェアの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。
- (2) ウィルス対策ソフトウェアをインストールするとともに、ウィルス情報データベースを常に最新に保っておくこと。

(管理責任者の責務・学外からの利用における遵守事項)

第13条 管理責任者は、自らが管理する情報機器に対して、利用者が学外のネットワークから当該情報機器にアクセスできるようにする場合は、次の各号に掲げる事項を遵守しなければな

らない。

- (1) 教育・研究目的及びそれらを支援する目的において、自らが管理する情報機器に対して利用者が学外からアクセスできるようにする場合は、情報セキュリティ委員会に申請し、事前に承認を得ること。
- (2) 管理責任者は、当該情報機器が悪意のある攻撃・不正アクセス・盗聴等による情報漏えいのおそれがあることを十分に認識し、情報漏えいを防止する対策を講ずること。

(改廃)

第14条 この細則の改廃は、情報セキュリティ委員会の議を経て、大学運営会議が行う。

付 則

この細則は、2011年（平成23年）7月21日から施行する。