

情報セキュリティ実施マニュアル
(教育・研究系) 利用者編

平成27年 8月28日

情報管理センター

はじめに

建学以来、産業保健及び産業医学の振興に寄与し、働く人々の健康を守り増進するために蓄積した全ての情報は、本学にとってかけがえのない重要な資産である。

今日の情報化社会において、これらの情報の収集、記録、伝達、報告等の多くは、コンピュータ等の情報機器及び情報ネットワークに依存しているが、これらの情報機器及び情報ネットワークは、利便性が高い反面、情報の盗難、改ざん、漏えい等の危険性を常に孕んでおり、それらが故意、過失等に関わらず本学に教育・研究活動の停滞、信頼の喪失などといった重大な被害を与える恐れがある。

したがって、教職員、学生のみならず、全ての関係者が不断の努力をもって情報資産のセキュリティの保持に努めなければならない。

このため、本学の情報システムを利用する者は、情報資産の運用、利用について定めた、学校法人産業医科大学の情報システムにおける情報セキュリティに関する規程及び情報セキュリティ実施マニュアルを遵守しなければならない。

目次

－ 情報セキュリティ実施マニュアル（教育・研究系）利用者編 －

1. 利用について	1
2. 情報機器の取扱い	2
3. 記録媒体等の取扱い	2
4. 教育・研究系ネットワークの取扱い	3
4. 1 教育・研究ネットワークの接続	3
4. 2 電子メールの利用	3
5. 情報の取扱い	3
6. 情報機器の持出し	3
7. 事故等の対応	4
8. 違反の措置	4
9. 実施マニュアルの改廃	4
付録（用語の定義）	5

学校法人産業医科大学の情報システムにおける情報セキュリティに関する規程（以下「規程」という。）に基づき、情報セキュリティの維持及び向上を図るため、教育・研究系ネットワークの利用者が遵守するための具体的な事項を定める。

各講座等には、情報セキュリティの推進を図るため、情報セキュリティ推進者を置く。情報セキュリティ推進者は、利用者に対し情報セキュリティの周知を図るとともに、情報システムの適切な利用を求める。

利用者は、次の各項目に留意しなければならない。

1. 利用について

(1) 学校法人産業医科大学（以下「本学」という。）の^{※1}教育・研究系ネットワークに^{※2}情報機器の接続を希望する者は、ネットワーク利用申請書（様式第1号）により、情報管理センター長の許可を得なければならない。また、不要になった場合は、ネットワーク・電子メール利用停止申請書（様式第6号）を情報管理センター長に提出すること。

なお、情報管理センター長は、個人所有の情報機器についても、ウィルス対策等の適切な措置が講じられているときは教育・研究系ネットワークへの接続を許可することができる。

(2) 本学の電子メールの利用を希望する者は、電子メール利用申請書（様式第2号）により、情報管理センター長の許可を得なければならない。また、不要になった場合は、ネットワーク・電子メール利用停止申請書（様式第6号）を情報管理センター長に提出すること。

(3) 本学代表電子メールの利用を希望する者は、代表電子メール利用申請書（様式第3号）により、情報管理センター長の許可を得なければならない。また、不要になった場合は、ネットワーク・電子メール利用停止申請書（様式第6号）を情報管理センター長に提出すること。

(4) 本学が管理する情報資産が閲覧可能な部屋への入室及び本学情報機器を使用する者は、本学が指定した名札又は身分証明証を着用すること。

(5) 個別認証のための磁気・ICカード等は、取扱い及び保管に注意し、盗難等による機器の不正利用を防止すること。特に、磁気カードは強力な磁気を発生するスピーカー及びテレビに近づけると磁気情報が壊れることがあるので注意すること。

(6) 電子メール及び代表電子メール利用のためのユーザ名及びパスワードの取扱いについて次の点に留意すること。

ア パスワードは6桁以上で、英字と数字等を組み合わせたものとする。

イ 他者に知らせてはならない。なお、止むを得ない事情で、他者に教えた場合は、必要に応じパスワードの変更を情報管理センター長に申請する。

- ウ 他の利用者のもを聞き出してはならない。
 - エ 他者（学内・学外を問わず）からの聞き取りに応じてはならない。
 - オ 他の利用者のもを、本人の許可無く使用してはならない。
 - カ メモ等に記載してはならない。
 - キ 情報機器に記憶させてはならない。
- (7) 情報機器の画面に情報を表示したまま又は情報が閲覧可能な状態で離席しないこと。
 - (8) 施設（研究室、居室等）の施錠に留意し、情報機器の盗難防止に努め、施錠が困難な場合は、セキュリティワイヤーの活用等により盗難防止に努めること。
 - (9) 集線装置（ハブ）及び中継装置（ルータ）等の情報機器は、施錠が可能な場所に設置し、通信線等の敷設及び情報機器の設置にあたっては、歩行の妨げにならない等の安全に留意すること。
 - (10) 情報資産に対して、不正なアクセス等によりこれを侵害しないこと。
 - (11) 利用にあたり不明な点は、情報セキュリティ推進者に相談すること。

2. 情報機器の取扱い

- (1) コンピュータ実習室（6号館2階）の情報機器については、情報管理センターがウィルス対策、OS等の情報セキュリティ対策を行うこと。
- (2) 各講座等で使用する情報機器については、各講座等において責任をもって管理すること。
- (3) 教育・研究系ネットワークには個人所有の情報機器の接続を許可しているため、個人所有の情報機器は、所有者の自己責任において管理を行うこと。
- (4) 情報機器（各講座等で管理する情報機器及び個人所有の情報機器を含む。）を業務に使用する場合は、機器の故障、情報漏えいの防止、情報の破壊等を防止するため、次の点に留意すること。
 - ア 情報機器にコーヒー、お茶等を近づけない。
 - イ 人、情報機器の転倒を防止するため、電源ケーブル、プリンターケーブル等を整理する。
 - ウ 情報機器の盗難を防止するため、部屋の施錠、セキュリティワイヤー設置等の対策を講じる。
 - エ 情報機器を携帯する場合は、盗難防止対策に努める。
 - オ 出所不明なソフトウェアは、インストールしてはならない。
 - カ Winny等のファイル交換ソフトウェアは、インストールしてはならない。
 - キ 不必要な外部記録装置は接続しない。
 - ク ウィルス対策ソフトウェア、定義ファイル、スクリーンセーバの設定等のセキュリティ対策がなされていない情報機器を教育・研究系ネットワークに接続してはならない。
 - ケ ウィルス対策ソフトウェアの定義ファイルは可能な限り頻繁に更新をする。また、Windowsアップデート等のOSや主要なソフトウェアの情報セキュリティ対策を必要に応じて実施する。

- コ 情報機器を修理、廃棄及びリース・レンタル機器の返却をする場合は、ハードディスク等の記録装置内のデータを全て消去又は読み取り不能な状態にしなければならない。

3. 記録媒体等の取扱い

- (1) 情報機器のうち、CD-R、CD-RW、DVD 及び USB メモリ等の記録媒体並びに外付ハードディスク等の外部記憶装置（以下「記録媒体等」という。）は、紛失しないように適切に管理すること。
- (2) 記録媒体等は、必要に応じて指紋認証等のセキュリティ機能付きのものを使用すること。
- (3) 記録媒体等を修理、廃棄及びリース・レンタルの記録媒体等の返却をする場合は、記録媒体内のデータを全て消去又は読み取り不能な状態にする、又は物理的に破壊し読み取り不能な状態にしなければならない。

4. 教育・研究系ネットワークの取扱い

4.1 教育・研究系ネットワークの接続

- (1) 端末、無線 LAN 装置等の情報機器を教育・研究系ネットワークへ接続するときは、規程第 4 条に規定する情報セキュリティ責任者（以下「責任者」という。）の承認を得て行うこと。
- (2) 責任者は、上記(1)の接続についての状況を記録すること。
- (3) 公衆回線を教育・研究系ネットワークに接続しないこと。
- (4) 公衆回線、公衆 PHS 回線又は携帯回線に接続したままの情報機器を、教育・研究系ネットワークに接続しないこと。
- (5) 病院内では、病院総合医療情報システムへの影響が考えられるため、無線 LAN 装置を使用して教育・研究系ネットワーク及び事務系ネットワークへの接続はしないこと。

4.2 電子メールの利用

電子メールの利便性は高いが、セキュリティ上の信頼性は低く、利用にあたって次の項目に注意すること。

- (1) コンピュータウィルスがメールに添付されて送られてくる可能性があるため、出所不明なメールは開かず削除すること。
- (2) 送信者はなりすまし可能なため注意すること。
- (3) 個人情報等の重要な情報の授受については、通信経路での盗聴が可能であるため使用しないこと。やむを得ず使用する場合は、匿名化、暗号化等の対策を講じること。

5. 情報の取扱い

(1) 原本の証明

ホームページ等電磁的媒体のみで公開する情報は、原本を保存する。

(2) 印刷物の取扱い

- ア 印刷物の閲覧は運用を十分に考慮して必要最小限の閲覧とする。
- イ 印刷物の廃棄は、原則シュレッダーを使用し、必要に応じて廃棄業者に委託する。
- ウ 個人情報等の重要な情報は可能な限り印刷を抑制する。
- エ 印刷物は出力したまま放置せず、施錠可能な場所等で適切に保管する。

6. 情報機器の持出し

本学が管理する情報機器は原則として学外への持ち出しを禁止する。ただし、やむを得ず、情報機器を学外へ持ち出す場合は、学校法人産業医科大学固定資産及び物品管理規程第12条第3項の取り扱いによること。

7. 事故等の対応

利用者は、情報機器の盗難、情報ネットワークへの不正な侵入、情報の改ざん等を発見したときは、直ちに責任者に報告すること。

また、不正プログラムの感染が疑われる場合、情報セキュリティ推進者と連携し LAN ケーブルを抜く等、ネットワークから切り離すこと。

8. 違反の措置

規程第16条に、違反の措置に関する規定があるので、必ず規程を一読すること。

9. 実施マニュアルの改廃

この実施マニュアルの改廃は、情報管理センター運営会議の議を経て行うものとする。

付録（用語の定義）

※1 教育・研究系ネットワーク

教育・研究系ネットワークとは、教育・研究系システムが稼動している情報ネットワークをいう。教育・研究系システムは、学内研究業績システム、情報教育システム、学内図書文献検索サービス等で構成され、教育・研究系ネットワーク上で稼動している。

※2 情報機器

端末、CD-R、CD-RW、USB メモリ等の記録媒体並びに外付ハードディスク等の外部記憶装置、プリンター、ネットワークシステムの集線装置及び中継装置等の情報処理のための全ての機器の総称。

※3 事務系ネットワーク

事務系ネットワークとは、事務系システムが稼動している情報ネットワークをいう。事務系システムは、管理会計システム、人事給与システム、施設設備管理システム、進路指導支援システム、図書館システム、学籍システム等で構成され、事務系ネットワーク上で稼動している。

※4 暗号化

暗号化とは、ネットワークを通じて文書や画像などのデジタルデータをやり取りする際に、通信途中で第三者に盗み見られたり改ざんされたりされないよう、決まった規則に従ってデータを変換することをいう。

※5 医療系ネットワーク

医療系ネットワークとは、医療系システムが稼動している情報ネットワークをいう。医療系システムは、電子カルテシステムを中心として稼動しており、検体検査システム、生理検査システム、輸血システム、細菌システム、給食システム等のサブシステムで構成され、医療系ネットワーク上で稼動している。

※6 情報ネットワーク

本学情報ネットワークは、教員及び学生が教育、研究を目的として利用する「教育・研究系ネットワーク」、事務業務用としての「事務系ネットワーク」及び大学病院の診療を中心とした「医療系ネットワーク」で構成されている。