

○公立大学法人福岡県立大学情報保全規則

(情報セキュリティポリシー)

法人規則第88号

平成20年11月1日

(目的)

第1条 通信ネットワークの急速な発達に伴う情報化時代において、個人情報を始めとする情報資産の機密性、完全性及び可用性を維持するための情報セキュリティ対策については、厳格な対応を求められるとともに、その漏えいに関しては、社会的責任を強く求められている。このような状況の下、この規則は、公立大学法人福岡県立大学（以下「法人」という。）における情報セキュリティ方針を定め、もって、その適切な運用を図るものとする。

(定義)

第2条 この規則において、各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

本規則をいう。

(5) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(対象とする脅威)

第3条 情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

(規則の対象者)

第4条 この規則は、次に掲げる者（以下「対象者」という。）に適用するものとする。

- (1) 法人職員（非常勤職員及び人材派遣会社からの派遣職員等を含む。）
- (2) 法人業務を受託した者
- (3) その他理事長が必要と認めた者

(対象とする情報及び情報資産)

第5条 この規則の対象となる情報（以下「対象情報」という。）は、社会通念上、情報が漏えいすることによりその責が及ぶ情報とし、おおむね次の各号に掲げるものとする。

- (1) 住所、氏名、電話番号、電子メールアドレス又は成績等の学生（卒業生及び本学受験生を含む。以下同じ。）及び教職員の個人情報
- (2) 試験問題、答案用紙又は入札情報等の漏えいすることにより公平性を著しく欠くおそれのある情報
- (3) 第三者から入手した個人情報又は共同研究における共用情報等の漏えいすることにより第三者に対して損害を与えるおそれのある情報
- (4) ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
- (5) ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- (6) 情報システムの仕様書及びネットワーク図等のシステム関連文書

(規則の遵守)

第6条 対象者は、この規則を遵守しなければならない。

- 2 前項に反した者は、公立大学法人福岡県立大学職員就業規則（平成18年法人規則第10号）及び公立大学法人福岡県立大学非常勤職員就業規則（平成18年法人規則第30号）及びその他関係規定並びに契約等により法人が受けた損害に対して賠償責任を負い、かつ、処分を受けるものとする。

(情報セキュリティ対策)

第7条 第3条の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講

じる。

(1) 組織体制

法人の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

法人の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し対策を講じる。

(4) 物理的セキュリティ

サーバー、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、本学が定めた危機管理基本マニュアルに則って対応する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第8条 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて

情報セキュリティ監査及び自己点検を実施する。

(情報セキュリティポリシーの見直し)

第9条 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

(禁止事項)

第10条 対象者は、次の各号に掲げる行為をしてはならない。

- (1) 対象情報を保存したメディアの学外持ち出し
- (2) 対象情報の私費購入メディアへの保存
- (3) 電子メールを用いた対象情報の学外組織への伝達
- (4) 対象情報を学内でファイル共有
- (5) 対象情報をオンラインストレージに置くこと
- (6) 対象情報の悪意ある利用
- (7) 学内サーバー室への入室（生命に危機の及ぶ可能性がある等の緊急時を除く。）
- (8) その他理事長が必要と認める行為

2 前項は、第6号を除き、次の各号に掲げる場合においては、これを免じるものとする。

- (1) 別途理事長が指定した者の許可を得た場合
- (2) 成績等を除く学生の個人情報について本人の同意を得た場合
- (3) その他理事長が必要と認めた場合

(注意事項)

第11条 対象者は、次の各号に掲げる行為に努めなければならない。

- (1) 悪意ある可能性のあるウェブサイトへのアクセス回避
- (2) 長時間の離席時におけるパソコンのシャットダウン
- (3) 対象情報を保存したメディアの盗難及び紛失防止
- (4) その他理事長が必要と認める行為

(学内利用パソコンの管理)

第12条 対象者は、法人内でパソコンを利用する場合には、インターネットへの接続の有無にかかわらず、次の各号に掲げることを行わなければならない。

- (1) ウイルス対策ソフトウェアのインストール及びウイルス定義ファイルの定期的更新
- (2) オペレーションシステム及びアプリケーションソフトの修正プログラムの適用
- (3) ログオン時におけるパスワードの設定
- (4) その他、理事長が必要と認める行為

2 前項は、法人内で利用する法人費購入以外のパソコンにおいてもこれを適用する。

- 3 理事長は、故障等の理由により対象者がいたずらに私費購入パソコンを法人内に持ち込まないために、対象者へ一時貸与できるパソコンを整備しなければならない。

(対象メディアの廃棄)

第13条 対象メディアを廃棄する場合は、破砕等の方法により完全に再利用できない状態にする場合を除き、データ消去ソフトウェアにより、対象情報を完全に抹消しなければならない。

(外部侵入者からの防衛)

第14条 理事長は、外部侵入者からの情報防衛のため、次の各号に掲げることを行うものとする。

- (1) 来学者に対する、警備員室での名簿記帳及び入室許可証の貸与
- (2) 入室許可を得た場合を除く外交販売員等の事務室カウンター内及び研究室への立入制限
- (3) 事務室及び研究室の施錠の徹底

(情報セキュリティ対策の推進体制)

第15条 理事長は、情報資産の保護及び情報保全を推進するため、法人内に総合情報委員会（以下「委員会」という。）を置く。

- 2 委員会は、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ技術管理者及びその他理事長が必要と認める者で構成し、次の各号に掲げる業務を行うものとする。
 - (1) 情報セキュリティ規則の検討に関すること。
 - (2) 理事長に対する情報セキュリティの提言に関すること。
 - (3) その他、情報セキュリティの実施推進に関すること。
- 3 情報セキュリティ責任者は、副理事長の職にある者を充て、法人の情報セキュリティに関するすべての責任及び権限を有するものとする。
- 4 情報セキュリティ管理者は、経営管理部長の職にある者及び情報処理センター長を充て、情報セキュリティの実施推進及び緊急時における情報セキュリティ対策に関することを行うものとする。
- 5 情報セキュリティ技術管理者は、理事長が指名する者複数人を充てるものとし、情報セキュリティの実施推進及び緊急時における情報セキュリティ対策に関する技術的な業務、助言及び提言を行うものとする。
- 6 委員会に関し必要な事項は、理事長が別に定める。

(情報漏えい時における報告義務)

第16条 対象者は、情報の漏えいを知ったとき又はそのおそれが生じたときは、直ちに、情報セキュリティ管理者に報告しなければならない。

- 2 情報セキュリティ管理者は、直ちに、情報セキュリティ技術管理者と連携の上、応急措置を講じた後、速やかに情報セキュリティ責任者にその旨を報告して、その取扱いの指示を受けなければならない。

(雑則)

第17条 この規則に定めるもののほか、情報セキュリティの取扱いに関し必要な事項は、理事長が別に定めるものとする。

(改廃)

第18条 この規則の改廃は、総務人事委員会の議を経て、理事長が行う。

附 則

(施行期日)

この規則は、平成20年11月1日から施行する。

附 則

(施行期日)

この規則は、平成22年3月16日から施行する。

附 則

(施行期日)

この規則は、平成25年12月24日から施行する。

附 則

(施行期日)

この規則は、令和2年4月1日から施行する。

附 則

(施行期日)

この規則は、令和3年5月18日から施行する。

附 則

(施行期日)

この規則は、令和8年5月28日から施行し、令和8年4月1日から適用する。