公立大学法人金沢美術工芸大学情報セキュリティ対策基準

平成 31 年４月１日

内規第 20 号

（目的）

第１条　この対策基準は、公立大学法人金沢美術工芸大学（以下「法人」という。）の情報セキュリティに関し、その確保のための体制及び方策に係る基本的な事項を定めることにより、情報資産をさまざまな脅威から守り、法人の情報セキュリティレベルの維持・向上につなげることを目的とする。

（情報セキュリティを確保するための体制）

第２条　法人の情報セキュリティを確保するため、法人に最高情報セキュリティ責任者、統括情報セキュリティ責任者及び情報システム管理者並びに情報セキュリティ委員会及び情報セキュリティ緊急対応チームを置く。

（最高情報セキュリティ責任者）

第３条　最高情報セキュリティ責任者は、理事長をもって充てる。

２　最高情報セキュリティ責任者は、法人における情報セキュリティの確保に関する最終決定権限及び責任を有する。

（統括情報セキュリティ責任者）

第４条　統括情報セキュリティ責任者は、事務局長をもって充てる。

２　統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐し、法人全体に係る共通的な情報セキュリティを確保する権限及び責任を有する。

３　統括情報セキュリティ責任者は、教職員等に対して、情報セキュリティに関する研修及び訓練を定期的に実施しなければならない。

４　統括情報セキュリティ責任者は、法人の情報セキュリティを脅かす事件又は事故に際し、最高情報セキュリティ責任者の指示に従い、必要な措置を実施する権限及び責任を有する。

（情報システム管理者）

第５条　情報システム管理者は、情報システムの規模、取り扱う情報資産の種類等に応じて、情報システムごとに最高情報セキュリティ責任者が指名する者をもって充てる。

２　情報システム管理者は、次に掲げる職務を行う。

(1)　実施手順を定め、維持すること。

(2)　所管する情報システムにおける開発、設定の変更、運用、見直し等を行うこと。

(3)　必要に応じて、統括情報セキュリティ責任者又は情報セキュリティ委員会に対して、所管する情報システムに関する相談や報告を行うこと。

(4)　その他所管する情報システムの運用及び保守に関すること。

（情報セキュリティ委員会）

第６条　法人の情報セキュリティ対策を統一的に実施するため、定期的に情報セキュリティ委員会を開催する。

２　情報セキュリティ委員会の委員は、教育研究審議会の委員をもって充てる。

３　情報セキュリティ委員会は、次に掲げる事項について、調査審議する。

(1)　情報セキュリティポリシー及び情報セキュリティ関連規程の制定及び改廃

(2)　情報システムの運用や利用に係る規程の制定及び改廃

(3)　法人の情報セキュリティを脅かす事件又は事故の再発防止策の検討及び実施

(4)　その他法人の情報セキュリティの確保に関する基本的な事項

（情報セキュリティ緊急対応チーム）

第７条　情報セキュリティ緊急対応チームは、法人の情報セキュリティを脅かす事件又は事故に対応する。

２　情報セキュリティ緊急対応チームの責任者及び構成員は、最高情報セキュリティ責任者が指名する。

（事故対応）

第８条　教職員等は、法人の情報セキュリティを脅かす事件又は事故を自ら認知し、又は外部から通報を受けた場合は、速やかに統括情報セキュリティ責任者に報告しなければならない。

２　報告を受けた統括情報セキュリティ責任者は、当該事象を確認し、速やかに最高情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、情報セキュリティ緊急対応チームと連携して対応を行うものとする。

４　情報セキュリティ緊急対応チームは、統括情報セキュリティ責任者の指示に従い、法人の情報セキュリティを脅かす事件又は事故による被害の発生、拡大の防止等を図るため、応急措置の実施や情報システムの停止又は復旧に係る指示を行うものとする。

５　情報セキュリティ緊急対応チームは、法人の情報セキュリティを脅かす事件又は事故の原因を究明し、その結果から再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

６　最高情報セキュリティ責任者は、必要な再発防止策の実施を指示するものとする。

（制限）

第９条　この対策基準に定められた最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ緊急対応チームの権限は、その行使によって必要以上に教員の教育・研究の自由を侵害することがあってはならない。

（利用者 ID 及びパスワードの管理）

第 10 条　教職員等は、自己の利用する利用者 ID に関し、次の事項を遵守しなければならない。

(1)　自己が利用している利用者 ID を他人に利用させてはならない。

(2)　利用者 ID を共用で利用する場合は、共有で利用する者以外に利用させてはならない。

２　教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(1)　パスワードを他人に知られないように管理しなければならない。

(2)　パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

(3)　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

(4)　複数の情報システム間で、同一のパスワードを用いてはならない。

(5)　情報システムにパスワードを記憶させてはならない。

（物理的セキュリティ領域）

第 11 条　教職員等が利用する研究室は、教職員等が同行することなしに、外部の第三者を入室させてはならない。

（情報システム機器の設置、保守・修理、廃棄）

第 12 条　統括情報セキュリティ責任者は、法人が管理する情報システム機器の盗難防止措置を講じなければならない。

２　情報システム管理者は、情報システムへのログインに際し、利用者 ID 及びパスワードの入力を必要とするように設定しなければならない。

３　情報システム管理者は、サーバー等の機器の重要度に応じ、機器の電源について、停電等の電源供給の停止に備え、当該機器が適正に停止するまでの間に必要な電力を供給する容量の予備電源を備え付けなければならない。

４　情報システム管理者は、サーバー等の機器の重要度に応じ、機器の定期保守を実施しなければならない。

５　情報システム管理者は、記憶装置を内蔵する機器を外部の事業者に修理させる場合、当該事業者との間で、秘密保持契約を締結しなければならない。

６　情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置からすべての情報を消去のうえ、復元不可能な状態にする措置を講じなければならない。

（アクセス制御）

第 13 条　統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、教職員等に対する利用者 ID の登録、変更、抹消等の方法を定めなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、利用されていない利用者 ID が放置されないよう、定期的に点検しなければならない。

（バックアップ）

第 14 条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムに保存された情報について、必要に応じて定期的にバックアップを実施しなければならない。

（ログの取得等）

第 15 条　統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得して一定期間保存しなければならない。また、必要に応じて、取得したログの点検・分析を実施しなければならない。

（ネットワークの接続制御）

第 16 条　統括情報セキュリティ責任者及び情報システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

２　無線 LAN 利用時は、以下を例とする対策を講ずること。

(1)　SSID の隠蔽

(2)　無線 LAN 通信の暗号化

(3)　MAC アドレスフィルタリングによる端末の識別

(4)　無線 LAN 回線利用申請手続の整備

(5)　無線 LAN 機器の管理手順の整備

（クラウドサービスの利用）

第 17 条　教職員等は、外部のクラウドサービスを利用する場合は、あらかじめ統括情報セキュリティ責任者へ届け出なければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、届出のあったクラウドサービスが継続的に適切な利用環境にあることを適宜評価する。

（暗号化）

第 18 条　教職員等は、情報資産の重要度に応じた分類による取扱制限に従い、外部記録媒体へデ

ータを保存する場合又は外部へデータを送る場合には、暗号化、パスワード設定等のセキュリティ対策を施さなければならない。

（不正プログラム対策）

第 19 条　統括情報セキュリティ責任者は、法人で管理している情報システム、パーソナルコンピューター等に対して、不正プログラム対策ソフトウェアを導入しなければならない。ただし、当該情報システム上で動作可能な不正プログラム対策ソフトウェアが存在しない場合を除く。

（外部委託事業者との契約）

第 20 条　法人が外部委託事業者との間で情報処理又は情報システムの構築、改修若しくは情報機器の修繕に関する契約を締結する場合は、必要に応じて、次に掲げる事項をその契約書に明記しなければならない。

(1)　情報セキュリティポリシー及び実施手順の遵守

(2)　外部委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

(3)　提供されるサービスレベルの保証

(4)　外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

(5)　外部委託事業者の従業員に対する教育の実施

(6)　提供された情報の目的外利用及び受託者以外の者への提供の禁止

(7)　業務上知り得た情報の守秘義務

(8)　再委託に関する制限事項の遵守

(9)　委託業務終了時の情報資産の返還、廃棄等

(10)　委託業務の定期報告及び緊急時報告義務

(11)　法人による監査、検査

(12)　法人による情報セキュリティを脅かす事件又は事故発生時の公表

(13)　情報セキュリティポリシーが遵守されなかった場合の損害賠償等

（雑則）

第 21 条　この対策基準に定めるもののほか、必要な事項は、理事長が別に定める。

附　則

この対策基準は、平成 31 年 4 月 1 日から施行する。