令和２年 ３月 １日

学術ネットワーク セキュリティ実施手順

はじめに

この「手順」は、学校法人日本医科大学学術ネットワーク運用細則第５条（情報セキュリティ）に基づいて、教職員等が情報セキュリティ対策を行うための、具体的な手順を定めたものである。

１ 情報の管理

学校法人日本医科大学（以下「本法人」という。）が保有する情報については、重要度を分類し、適正に管理を行うこと。

⑴ 情報の管理方法

①機密性３情報（関係者外秘情報）

関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、必要な対策を取ること。

【実施事項】

・個人フォルダに保存する。部署別の共有フォルダに保存する場合には、関係者のみにアクセス権限を設定する。

・ファイル自体に適切なパスワードを設定するか、ファイルを暗号化する。

②機密性２情報（本法人外秘情報）

本法人内者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、必要な対策を取ること。

【実施事項】

・共有フォルダに保存する場合には、本法人内者のみにアクセス可能なように設定する。

・ファイル自体に適切なパスワードを設定するか、ファイルを暗号化する。

③機密性１情報（公開情報等）

公開情報は不特定の者がアクセス可能であるため、情報の改ざんや偽情報の流布の防止策のために、以下の例を参考に必要な対策を取ること。

【対策例】

・公開情報の修正等の作業は限られた者のみが行えるようにパスワード等を設定する。

⑵ 情報の複製、持ち出し及びメール送信

情報を複製、持ち出し及びメール送信する場合も、情報の分類に応じて、以下のことを必ず実施するとともに、必要な対策を取ること。

①機密性３情報（関係者外秘情報）

【実施事項】

・本法人内の安全性のある場所に保管し、原則として、保管場所からの複製及び持ち出しはしない。

・やむを得ず保管場所以外に複製及び持ち出す場合は、学術ネットワーク管理責任者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報の持ち出し時には、必ず目の届く場所にデータを置き、盗難、紛失等に十分注意する。

②機密性２情報（本法人外秘情報）

【実施事項】

・本法人内の安全性のある場所に保管し、原則として、保管場所からの複製及び持ち出しはしない。
・やむを得ず保管場所以外に複製及び持ち出す場合は、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報の持ち出し時には、必ず目の届く場所にデータを置き、盗難、紛失等に十分注意する。

③機密性１情報（公開情報等）

【実施事項】

・情報の持ち出し時には、目の届く場所にデータを置き、盗難、置き忘れ等に十分注意する。

⑶ 機密性３情報及び機密性２情報の開示について

原則として、機密性３情報及び機密性２情報は、開示してはならない。
ただし、やむを得ず一部又は全部を第三者に開示する場合は、学校法人日本医科大学個人情報保護に関する規程に基づき以下のことを必ず実施するとともに、必要な対策を取ること。

【実施事項】

・開示の要求を受けた情報を管理している部署は、開示要求の理由が適正か判断し、当該情報を開示して問題ないか十分に協議する。
・個人情報の漏えい、プライバシーや著作権の侵害に十分注意し、場合によっては、開示する情報の抽出や統計処理による秘匿措置などを行う。
・開示する場合は、開示を要求した第三者以外に開示されないように、開示を要求した第三者に対して指導、監督する。

⑷ 情報処理機器の廃棄について

情報処理機器の廃棄をする際には、情報の分類に関係なく、データの消去等を確実に行い、情報の漏えい防止策のために、以下の例を参考に必要な対策を取ること。

【実施事項】

・データの消去には、破砕処理や、磁気によるデータの消去、データ消去ソフトウェアを用いた消去等を行い、データの復元ができないようにする。
・情報機器の記憶媒体を保守契約により交換する場合又はリース機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても保守業者に確認を取り、データ消去を確実にする。
・データの消去を外部に委託する際には、データ消去証明書等の提出を義務付ける。

２ セキュリティの確保

利用者は、本法人が保有する情報を守るため、当該情報を管理している部署長の指示の下、セキュリティ対策を実施する。

⑴ 物理的セキュリティ

① 情報システムのセキュリティ対策

パソコン等の情報システムについては、以下の例を参考に必要な対策を取ること。

【パソコン、サーバ類の対策例】

・機器に適切なパスワードを設定し、不要なアクセスを防ぐ。
・パソコンを離れる際には、ロック画面（スクリーンセーバー）にするなど、他人にパソコンを閲覧されないようにする。

【外部記憶装置の対策例（USBメモリ、外付けハードディスクなど）】

・外部記憶装置は、セキュリティ機能付きのものを使用する。
・本法人で購入した外部記憶装置は、原則として本法人管理外のパソコン等へは接続しない。やむを得ず一時的に接続しなければならない場合は、必ずウイルスチェックを行う。

② 入室の制限

サーバ室のように重要な情報機器が設置してある部屋の管理については、以下の例を参考に必要な対策を取ること。

【対策例】

・施錠管理し不正な入室を防ぐ。
・特に重要な部屋については電子錠により施錠管理し、入退室の自動記録を行う。
・入室できる者を制限する。また、入室を予定していない者が入室を行う際には、入室権限を持つ者が同行する。
・入退室記録の管理や防犯カメラ等を設置し、不正な入室が行われないようにする。

③ 盗難の防止

情報システム及び情報の盗難を防ぐため、以下の例を参考に必要な対策を取ること。

【対策例】

・パソコンやプリンタなど、持ち運びのできる物は盗難防止のため、セキュリティワイヤー等で固定のうえ施錠する。
・情報システム及び情報を管理するキャビネット等は、施錠管理を行う。

④ 災害対策

サーバ機器のような重要な情報処理機器のシステム停止を可能な限り防ぐために、以下の例を参考に必要な対策を取ること。

【対策例】

・情報処理機器の備え付けにあたっては、耐震対策を充分に考慮する。
・災害により情報システムが停止しないように、構築時に必要な冗長化を行う。
・災害等によりデータが消失することがないようにサーバ機器は定期的にバックアップを取る。
・停電等による不測のシステム停止によりハードウェア障害が起きないように、無停電電源装置等を用いて、電源断時に自動で終了処理を行う。

⑤ ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、以下を参考に必要な対策を取ること。

【対策例】

・有線LANを使用する場合は、悪意又は過失によるケーブルの切断を防ぐ対策を行う。

⑵ 人的セキュリティ

① 情報の管理

部署長の指示の下、情報の重要度を適切に分類し、以下の例を参考に情報の管理を行なうこと。

【対策例】

・情報の重要度を適切に設定する。（不要に重要度を高くすると、利便性が著しく低下し、業務や研究等に支障が出ることも考えられるため、重要度の分類は適切に行う。）

・機密性３情報の権限範囲が適切であるか定期的に確認する。

・情報台帳等を作成し、守るべき情報を整理する。

② パスワードの設定

利用者等は、パスワードの設定を行う際には、以下の例を参考にパスワードを設定すること。

【パスワードを設定する基準例】

・推測しにくいパスワードを設定する。

・8文字以上のパスワードにする。

・英字・数字・記号を組み合わせる。

【パスワードを保護するための対策例】

・初期に設定されているパスワードは使用せず、必ず変更する。

・パスワードをメモしたものを人目の付くところに置かない。

・パスワードを他人に教えない。

・複数のシステム（メールアカウントやSNSのアカウントなど）に同じパスワードを設定しない。

③ プリンタ印刷のセキュリティ対策

プリンタ印刷の際には、情報の漏えいを防ぐために以下の例を参考に必要な対策を取ること。

【対策例】

・印刷した情報の取り忘れ、取り間違いに注意する。

⑶ 技術的セキュリティ

① 情報システムのセキュリティ対策

パソコン等の情報システムについては、以下の例を参考に必要な対策を取ること。

【パソコン、サーバ類の対策例】

・定められたウイルス対策ソフト又は同等レベルのソフトをインストールし、リアルタイム検索を有効化すること。また、定期的（最低でも月に1回）にウイルス感染チェックを行う。

・OS又はインストールされているソフトウェア等で、セキュリティの脆弱性が発覚した場合には、速やかにセキュリティアップデートを行う。

・不正なアクセスや攻撃を防ぐために、不要な常駐プログラム等を停止する。
・アカウントの管理者は、アカウントの整理を定期的に行い、不要なアカウントは削除する。
【ネットワーク接続機器の対策例（プリンタ、スキャナなど）】
・機器の利用はIPアドレス等で、利用可能な範囲を制限する。
・保守用途等で遠隔から機器にアクセスする際は、IPアドレス制限やパスワード等でアクセスを制限し、不特定多数のアクセスを禁止する。
・不正なアクセスを防ぐため、不要なサービスは停止する。
【ネットワーク接続型の記憶装置の対策例（NAS等）】
・パスワード等の設定を行い、アクセスできる者を制限する。
・IPアドレスでの利用制限の設定を行い、不要なアクセスを防ぐ。
【通信制御装置の対策例（無線LANのアクセスポイント、ルーターなど）】
・登録されたMACアドレスやサブネット、IPアドレス以外から接続できないように設定する。

② ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、以下を参考に必要な対策を取ること。

【対策例】
・ケーブルを接続するだけで学術ネットワーク及びインターネットが利用できるようになるDHCPサーバの設置は行わない。
・ルータモードを持つ機器の設置は行わない。

３ 禁止事項

当法人内の情報を利用するにあたり、以下の行為はしてはならない。

(1) 法令に違反する行為

・閲覧権限及び利用権限のない情報へ不正にアクセスする。
・情報を破壊及び改ざんする。
・コンピュータウイルスを配布する。
・有償ソフトウェアを無断でコピーして使用する。
・その他、法令に違反するとみなされる行為。

(2) 公序良俗に反する行為

・他人になりすまして、ネットワークを利用する。
・事実と異なる情報を意図的に流す。
・人権、性別、思想信条などに基づく差別的な文章等をSNS(Facebook、LINE、Twitter等)等のインターネット等で公開する。
・他人のファイル等を無断で参照及び複製する。
・その他、公序良俗に違反するとみなされる行為。

(3) 本法人の運営目的等に反する行為

・運営目的でないソフトウェアを学術ネットワークに持ち込んで使用する。
・部署長の指示に従わない。
・その他、本法人の運営目的等に反するとみなされる行為。

４ インシデントに対する対応と報告

インシデントが発生した場合には、その被害を最小限に抑えるため、以下のとおり対応しなければならない。

⑴ 重要度の区分

インシデントが発生した場合には、その事象から、以下のように重要度を区分する。

【重要度：高】

・本法人の信用や利益を大きく損なうもの。
・本法人の業務・運営に支障があるもの。
・違反行為の内容が法律等に違反するもの。
・事象が重大で解決に時間を要するもの。
・その他、重要度が高いと認められるもの。

【重要度：低】

・本法人の信用や利益を損なう可能性がないもの。
・本法人の業務・運営に支障が少ないもの。
・事象が軽微ですぐに対応が可能なもの。

⑵ インシデントに対する対応

①利用者等は、インシデントを発見した場合には、速やかに当該事象が発生している部署の責任者に連絡をしなければならない。

②当該事象が発生している部署の責任者は、インシデントが発生した場合には、速やかに事実関係の確認、問題の解決に努めるとともに、再発防止策の検討及び実施をしなければならない。

③当該事象が発生している部署の責任者は、発生したインシデントの重要度に関わらず、学術ネットワーク管理責任者にインシデントの内容や対応状況、再発防止策等について報告しなければならない。 この場合、学術ネットワーク管理責任者は当該事象の重要度（４⑴）について判断する。

⑶ 「重要度：高」と判断されたインシデントへの対応

①報告

イ　当該事象が発生した部署の責任者は、「インシデント報告書」を作成し、学術ネットワーク管理責任者に報告しなければならない。

ロ　学術ネットワーク管理責任者は、部署長からインシデントの報告を受けた後、ICT推進センターを通して学校法人へ報告しなければならない。

②対応等

イ　学術ネットワーク管理責任者は、調査結果に基づき、以下の対応を行う。

・原因が、当該事象が発生した部署にある場合
部署長に対して、手順の遵守を徹底させる。

・原因が、手順の不備にある場合
ICT推進センターに対して、手順の見直しを進言する。

以上