長崎国際大学薬学部医療情報学研究室情報セキュリティポリシー

令和２年６月１日

1　情報セキュリティ基本方針

1.1　情報セキュリティの基本方針

長崎国際大学薬学部医療情報学研究室（以下「本研究室」という。）において，人を対象とした臨床研究での研究対象者（以下「研究対象者」という。）の個人情報を利用して研究を実施する教員・学生・共同研究者等（以下「研究者」）や本研究室内の情報資産を保護し，本研究室における継続的かつ安定的な研究を確保するとともに，研究対象者および研究者からの安全，安心及び信頼の下に研究業務を遂行するための，情報セキュリティ対策実施の包括的な方針として，「長崎国際大学薬学部医療情報学研究室情報セキュリティポリシー」を策定する。

本研究室で研究を行うすべての者は，この目的を果たすため，本ポリシーの実施に責任を負うとともに，本ポリシーを尊重し，遵守しなければならない。

情報セキュリティポリシーによって目指すものは，次のとおりである。

① 本研究室の情報セキュリティに対する侵害を阻止

② 本研究室内外の情報セキュリティを損ねる加害行為を抑止

③ 情報資産に関して，重要度による分類とそれに見合った管理

④ 情報セキュリティに関する情報の取得を支援

1.2　対象範囲

本ポリシーの対象範囲は，本研究室の研究に使用するハードウェア，ソフトウエア，ネットワーク，記録媒体等の情報システム等(システム構成図等の文書を含む。)，及び全ての情報のうち情報システムに電磁的に記録される情報とし，本ポリシーの対象者は，全ての研究者と、システム障害時に委託する外部業者のシステム保守要員する。

1.3　組織体制

情報セキュリティ対策を推進するための組織・体制を定め，その責任及び権限を明確にする。

(1) 情報セキュリティ責任者（研究室長）

・本研究室の情報セキュリティに関する総括的な意思決定と，学内，他の組織及び学外に対する責任を負う。

(2) 情報システム管理者（研究室教員の中から研究室長が指名）

・情報システム管理者（以下「システム管理者」という。）は，情報セキュリティ責任者の指示に従い，個別のシステムに関する設定の変更，運用，更新など，情報システム管理に関する実務を行う。

(8) 利用者

・利用者とは、本研究室において行われる研究を実施するすべての研究者（教員、学生、研究協力者）であり、本研究室で研究に用いる情報システム及び情報そのものを取り扱うものである。

・全ての情報システムの利用者は，本ポリシーに定められている事項を遵守する。

2　対策基準

2.1　情報の分類と管理

2.1.1　情報の管理責任

管理責任

情報システム内の情報は，情報セキュリティ責任者が管理責任を有する。

利用者の責任

情報を利用する者は，情報の分類に従い，自己責任において適切に管理・利用する責任を有する。

重要性の効力

情報が複製又は伝送された場合には，当該複製等も分類に基づき管理する。

2.1.2　情報の分類と管理方法

(l) 情報の分類

このポリシーの対象となる本研究室内の全ての情報は，各々の情報の機密性，完全性*1 及び可用性*2 を踏まえ，次の重要性分類に従って分類する。

＜重要性分類＞

重要性分類 4　業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む。）

重要性分類 3　公開することを予定していない情報（秘の情報を含む。）

重要性分類 2　外部に公開する情報のうち業務上重要な情報

重要性分類 l　上記以外の情報

提供を受けた医療情報や個人を特定可能な研究情報は，特段の定めがない場合，「重要性分類 3」とする。これらを外部に公開するために個人を特定できないよう加工した場合には「重要性区分 2」とする。なお，ゲノム情報は「重要性分類 4」とする。

注　*1 情報資産の完全性・正確性に関する重要性

*2 情報資産の利用可能性‐継続性に関する重要性

(2) 情報の管理方法

①　情報の分類の表示

・情報システムで扱う情報の分類の表示については，第三者が重要性の識別を容易に認識できないよう，適切な管理を行う。

②　情報の管理及び取扱い

・情報について，それぞれの分類に従い，アクセス権限を定める。

・研究者は，情報セキュリティ責任者の許可がある場合を除き，重要な情報（重要性分類 3

以上）の外部への送付及び持出しをしてはならない。また，情報を複製する場合，個人情報の利用目的を変更/追加する場合は，情報セキュリティ責任者の許可を得なければならない。
・特に重要な情報（重要性分類 3）は必要に応じて暗号化を施して管理するものとし，暗号化に用いた暗号鍵及び暗号化された当該情報は，別々に適切な管理を行う。
③　記録媒体の管理
・取り外しが可能な記録媒体は，適切な管理を行う。
・重要な情報（重要性分類 3 以上）を記録した記録媒体を，外部に持ち出す場合は情報セキュリティ責任者の許可を得る。
・重要な情報（重要性分類 3 以上）を記録した記録媒体は，施錠可能な場所に保管する。
④　記録媒体の処分
・記録媒体が不要となった場合は，当該媒体に含まれる重要な情報（重要性分類 3 以上）は，記録媒体の初期化など情報を復元できないように消去を行った上で，廃棄する。
・重要な情報(重要性分類 3 以上)を記録した記録媒体の廃棄は，情報セキュリティ責任者の許可を得る。

2.2　物理的セキュリティ

2.2.1　サーバ等の管理

システム管理者は，以下の項目を実施しなければならない。
(1) サーバの管理
・重要性分類 3 以上の情報を取り扱う基幹的なサーバ等は，管理区域（以下「研究ブース」という。）に設置し，管理する。
(2) 研究ブースの管理
・外部からの不正な侵入に備え，研究ブースに施錠装置等を設置し，必要に応じて警報装置，監視設備等を設置する。
(3) 入退室の管理
・研究ブースに入室する権限を有する者を定めるとともに，用件の確認，入退室の記録，部外者についての識別化，部外者が入室する場合の立会い等を行う。また，重要性分類 3 以上の情報を記録する媒体を保管するための施設を設けている場合においても，必要があると認める時は同様の措置を講ずる。
・必要があると認める時は，研究ブースの出入口を特定することにより入退室の管理を確実に行えるようにし，所在表示の制限（重要な情報やサーバが存在すること等をあからさまに表示しないこと）等の措置を講ずる。
・研究ブース及び保管施設の入退室の管理について，必要があると認める時は，入室に係る認証機能を設定する。その際，パスワード等の漏洩防止のために，パスワード等を適切に管理する。
(4) 装置の設置等
・重要性分類 3 以上を取扱うシステムの設置を行う場合は，火災，水，埃，振動等の影響を

可能な限り排除した場所に設置し，必要に応じ容易に取り外せないよう適切な固定等の必要な措置を施す。
・重要性分類 3 以上を取扱うシステムでは許可された研究者以外の者が容易に操作できないように，利用者 ID，パスワードの設定等の措置を施す。
。
2.3　人的セキュリティ
2.3.1　研究者に関する管理
・研究者については，研究室配属時又は共同研究開始時にポリシーのうち守るべき内容を理解させ，本人の同意を得た上で，実施及び遵守させる。
2.4　技術的セキュリティ
2.4.1　端末
・　重要性分類 3 以上を取扱う端末（以下「特定端末」という。）への各ユーザのログインは，ローカルパワーユーザとする。
・特定端末の，本来用途以外の使用を禁止する。
・特定端末には，ウィルス対策ソフトを導入する。
2.4.2　ネットワーク接続
・特定端末は特に必要でない限りはネットワークへ接続しない。
・特定端末をネットワークに接続する際には，事前に情報セキュリティ責任者に申請し承認を得る。
・接続が許可された場合は，ウィルス対策ソフトを導入し，パターンファイルを最新にアップデートする。
2.4.3　利用者管理
・特定端末のユーザ認証は，ユーザ ID＋パスワードで行う。
・他人のユーザ ID の利用は厳禁とし，不正運用発覚時はユーザ ID の停止及び罰則の対象となり得る。
・期間が設定された利用者（有期雇用採用者等）及び利用期間が明確な利用者の場合は，必ず利用期間制限を行う。
・一旦登録した利用者が，再就職ないし休職からの復帰の際は，以前と同じユーザ ID を利用する。
2.4.4　システム保守等
(1) 機器の修理及び廃棄
・記録媒体の含まれる機器について，外部の業者に修理させ，又は廃棄する場合は，その内容が確実に消去された状態で行う。
・機器の故障等で保存データを救済する必要が生じ、やむを得ず外部の業者に個人情報にアクセスできる可能性がある作業を委託する場合には、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行える業者を選定する。

（2）保守契約書・マニュアル等の文書の管理

・システムの保守契約書・マニュアルはシステム管理者が保管する。

・システム管理者は必要に応じ研究者へマニュアルを用いて使用方法を指導する。

3　　運用

3.1　　ポリシー遵守状況の確認，システム監視

システム管理者は，ポリシーが遵守されているかどうかについて，また，問題が発生していないかについて，確認を行う。

(1)システム管理者は，サーバ等のシステムの設定がポリシーを遵守しているかどうか，また，問題が発生していないかについて，定期的に確認を行う。

4　　法令遵守

職員等は, 職務の遂行において使用する情報資産についで, 次の法令を遵守し, これに従う。

・不正アクセス行為の禁止等に関する法律

・著作権法

・独立行政法人等の保有する個人情報の保護に関する法律等

5　　情報セキュリティに関する違反に対する対応

ポリシーに違反した者について，その重大性，発生した事案の状況等に応じて本学の懲戒処分等の対象となり得る。なお，処分の決定は本学の判断にゆだねる。

6　　監査

研究室長が指名する監査責任者による監査を，定期的(年１回)に行う。

7　　情報漏洩時の対応

研究者は、情報の漏洩が発覚した場合には、すみやかに情報セキュリティ責任者に報告する。情報セキュリティ責任者は、状況を把握し、適切な対策を講じる。

附　則

この規定は令和２年７月１日から施行する。