JROADデータを用いた医療の質の向上に資する産学連携公募研究

セキュリティ計画書（国循以外でデータ利用する場合）　ver1.0.0

20　　 年 　月 　日

「循環器疾患診療実態調査データを用いた医療の質の向上に資する研究公募」について、

国循以外の研究機関におけるセキュリティ対策を以下のとおり定める。

1. 管理体制

ア 本研究における匿名化データを適切に管理するため、IT/Database 部会が承認した研究実施施設のデータ利用申請者（データ管理責任者）：（　　　　　　　　　）を保護管理者とする。

イ 保護管理者を補佐し、匿名化データの管理に関する事務を担当するため、保護管理者は保護担当者：（　　　　　　　　　）をおく。

1. 作業者の責務

本共同研究において匿名化データを取り扱う者（以下「作業者」という。）は、関連する法令及び規程等の定め並びに保護管理者及び保護担当者の指示に従い、匿名化データを取り扱う。

1. 個人情報の取扱い

ア 当該匿名化データにアクセスする権限を有する作業者はIT/Database 部会が承認した研究のデータ利用申請者及び共同研究者に限定する。

イ 当該匿名化データにアクセスする権限を有する者を変更・追加する場合は、保護管理 者及び本部会の許可を得て行うこととする。

ウ 作業者は、分析目的を達成するために必要な範囲以外で匿名化データにアクセスし ない。また、特定の個人を再識別化しない。

オ　匿名化データを取扱う場所はIT/Database 部会が承認した研究実施施設内に限るものとする。なお、作業する端末は、作業者の退席後１０分間操作がない場合は、スクリーンセーバーにより画面をロックし、復帰時には再度認証を行う。また、保護管理者以外の者はプログラムのインストールをできない設定とする。

カ 保護担当者は、匿名化データが記録されている媒体を定められた鍵付きのキャビネットに保管し、施錠を行う。

キ 作業者は、匿名化データ又は匿名化データが記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該匿名化データの復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。

ク 当該匿名化データの利用及び保管等の取扱いの状況について台帳に記録し、定期的に保護管理者が確認する。

1. 情報システムにおける安全の確保等

ア 作業を行う端末は外部ネットワークから遮断されたスタンド・アローンで運用するとともに、パスワードによる認証を行う。また、作業者ごとに異なるＩＤ、パスワードを設定し、その利用状況を確認できるようにする。

イ 作業者は、パスワードを定期的に変更することとし、パスワードの読取防止対策を行う。保護担当者は、パスワードの管理に関する定めの整備（その定期又は随時の見直しを含む。）を行う。

ウ 作業を行う端末及び当該匿名化データへのアクセス状況を記録する。また、その記録

（以下「アクセス記録」という。）をデータ利用期間の最大２年間保存し、本部会へ報告する。

エ 保護担当者は、端末で作業を開始する前にアクセス記録のチェックを行い、保護管理者は定期的にそれを確認する。

オ アクセス記録の改ざん、窃取又は不正な消去の防止のためにアクセス記録の保存、端末のパスワード管理、入退室管理を徹底する。

カ 作業を行う端末は、保護管理者が特別に必要と認めた場合以外には移動しない。

キ コンピュータウイルスによる匿名化データの漏えい、滅失又はき損の防止のため、最

新の対策ファイルに随時更新したウイルス対策ソフトを導入し、コンピュータウイルスの感染を防止する。また、全ファイルのスキャンを１カ月に１回以上行う。

ク 匿名化データを保存する外部記憶媒体には、パスワードを用いてファイルを暗号化し、分析用の端末以外では復号化できないように設定する。

ケ 保護管理者は、匿名化データを取り扱う端末をIT/Database 部会が承認した研究実施施設内の一台に限定し、当該端末の盗難又は紛失の防止のため、セキュリティワイヤーによる端末の固定を行う。

＊作業者は、データを外部メディアに書き出す場合は、保護管理者の許可を得たうえで

パスワードを用いて暗号化を行う。またログを記録し、定期的に保護管理者が確認する。

サ 作業者は、保護管理者が必要あると認めるときを除き、(4)ケの端末を外部へ持ち

出さない。また、当該端末の使用に当たっては、匿名化データが第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する。

シ 作業を行う端末には、許可された外部メディア以外は接続できないように設定を行う。

ス 分析結果を外部へ持ち出す場合には、集計情報となっていることを保護担当者が確認を行い、外部への持ち出しを許可する。

1. 情報システム室等の安全管理

ア 保護管理者は、匿名化データを取り扱う端末を設置する室（以下「情報システム室」という）をIT/Database 部会が承認した研究実施施設内とし、入室する権限を有する者を限定するほか、用件の確認、入退室の記録、部外者についての識別を行う。

イ 原則として部外者の入室を禁ずるが、例外的に部外者が入室する場合は、職員の立会を条件に行う。

ウ 情報システム室の入退室について、台帳に記録し、定期的に保護管理者が確認する。鍵は保護担当者が管理を行う。

エ 作業者は、文書の出力は必要最小限とし、鍵付きのキャビネットで管理する。当該文書を情報システム室から持ち出す場合には、保護管理者の許可を得たうえで、台帳に目的、作業者名、持参先を記録し、定期的に保護管理者が確認する。また、返却の際はほかの作業者が現物の確認を行う。

オ 作業者は、(5)エの規定により出力した文書について不要となった場合は、保護管理者の許可を得たうえで、速やかに当該文書をシュレッダー処理する。

カ 外部からの不正な侵入に備え、情報システム室に施錠を行い、警備員を定期的に巡回させる。

1. 安全確保上の問題への対応

ア 匿名化データの漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った作業者は、速やかに保護管理者に報告する。

イ 保護管理者は、被害の拡大防止又は復旧等のために対策を講ずるとともに、事案の発生した経緯、被害状況等を直ちに日本循環器学会 本部会長に報告する。

ウ 保護管理者は、事案の発生した原因を分析し、再発防止のために対策を講ずるとともに、その対策について日本循環器学会 本部会の承認を得る。

エ 日本循環器学会およびIT/Database 部会が承認した研究実施施設は、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応を行う。

オ 上記ア～オの対応を行うための連絡体制図を作成し、日本循環器学会 本部会に提出する。また、作業者に周知を行うとともに、常に作業場所に設置しておく。