HIC解析環境の利用に当たっての運用管理規程

（参考例）

〇〇〇○年○月○日　○○大学○○部○○研究室

１．基本方針と管理目的

本運用管理規程は、○○大学における臨床研究の発展を推進するとともに研究成果の社会還元に寄与するため、○○大学○○部○○研究室の運用において、情報資産のセキュリティ対策に必要な事項を定める。特に本運用管理規程は、情報資産毎のリスク分析を踏まえたセキュリティ対策を担保するための運用管理規程である。本規程を基準にPDCAサイクルを回し、情報漏えい防止を適切に行う。厚生労働省から提供を受けたNDBデータの取扱者が、本学にて策定・公開している個人情報保護に関する基本方針、個人情報を取り扱う情報システムの安全管理に関する方針に基づき、個人情報保護と情報セキュリティの観点から遵守すべき事項を規定するものである。

２．用語の定義

|  |  |  |
| --- | --- | --- |
| No. | 用語 | 定義 |
| 1 | HIC | 厚生労働省が用意する医療・介護データ等解析のためのクラウド基盤 |
| 2 | NDBデータ | NDBから抽出・加工され提供されるデータ |
| 3 | NDBデータ等 | NDBデータ、中間生成物、及び最終生成物を総称したもの |
| 4 | 生成物 | 提供されたNDB データを用いて利用者が生成したもの |
| 5 | 最終生成物 | 生成物のうち、最小集計単位等の公表の基準を満たしたもの |
| 6 | 中間生成物 | 生成物のうち、最終生成物以外のもの |
| 7 | 成果物 | 最終生成物のうち、厚生労働省による公表前確認で承認を得て、取扱者以外に公表可能になったもの |
| 8 | 取扱者 | 提供申出書に記載されたNDBデータ等を取り扱う個人 |
| 9 | 手続担当者 | 厚生労働省との書類の授受や連絡の窓口を担当する取扱者 |
| 10 | 利用場所 | NDBデータ等の参照及び解析が可能な場所 |
| 11 | 保管場所 | NDBデータ等を物理的に保存する場所 |
| 12 | 取扱区域 | 利用場所及び保管場所を合わせた区域 |

３．適用範囲

厚生労働省から提供を受けたNDBデータ~~はHIC解析環境でのみ利用することとし、本運用管理規定はNDBデータ~~、及びそれから派生する全ての生成物に携わる業務、部局及び情報技術等に適用するものとする。

４．運用管理

（１）取扱者・管理責任者

* ~~NDBデータの~~取扱者は、予め厚生労働省に申出を行い厚生労働大臣に承諾された者のみに限られ、その他の者はNDBデータ等にアクセスしてはならない。
* 管理責任者は、NDBデータ等の運用管理を担う責任者である。日常的なシステムの安全管理や、安全管理に必要な資料の作成や報告を行い、これらの安全管理に係る業務に必要な承認権限等を有する。○○研究室の○○○○がこれを担う。

（２）端末の利用~~・保管~~場所へのアクセス制限

* ~~HIC利用端末の取扱区域は、○○大学○○部○○研究室のみとする。~~
* HICの利用場所（●●大学●●学部●●研究室）は、職員証のある者、研究室の鍵を持つ者等に制限する。
* ~~当該研究室は、管理責任者が認めた者のみが入室できることとする。~~
* 当該研究室は、管理責任者が認めた者以外の立ち入りを原則認めない。ただし、管理責任者が認めた者が不在の際は施錠を行うこととする。

（３）利用・保管方法

* ~~NDBデータの~~申出にて発生する厚生労働省の文書、研究方法のマニュアル等、契約書等は、○○研究室で適切に管理する。
* NDBデータ等の端末内への保存、HIC利用中の画面の撮影・録画・スクリーンショットの取得、及び帳票によるデータ出力は行わない。
* 端末にログインする際には二要素認証方式により取扱者の識別と認証を行い、取扱者以外の者がアクセスできないこととする。パスワードについては~~、二要素認証（~~生体認証＋13文字以上の英数字と記号を混在させた推定困難なPW~~）~~を用いること。また、窃視を防止するため、パスワード付のスクリーンセーバーを設定すること。 スクリーンセーバーが起動するまでの時間~~設定値~~は15分とする。
* 端末にはコンピューターウイルス対策ソフトを導入し、情報漏洩、改ざんなどが発生しないよう対策を施す。さらに、不正ソフトウェア対策ソフトのパターンファイルの更新やOSのセキュリティパッチ等のアップグレードを行い、常に最新の定義ファイルに更新する。
* 端末はファイヤーウォールを備えた学内インターネット回線を経由してHICに接続するものとする。また、公衆無線LANには接続しない。
* ~~台帳管理している外付けHDD、USB等の記録媒体以外の記録媒体を接続してはならない。~~
* 端末には、不特定多数へのファイル交換を可能とするソフトウェアや安全性が確認できないアプリケーションなどはインストールしない。
* （利用端末を追跡かつ遠隔からの命令等によりデータ消去する機能を設けた場合）利用端末には、専用ソフト（○○）により追跡・遠隔で消去できる機能を搭載する。
* （利用端末を追跡かつ遠隔からの命令等によりデータを消去する機能を設けなかった場合１）デスクトップ型HIC利用端末は持ち出しを防止するため、施錠したチェーンによって固定することとする。
* （利用端末を追跡かつ遠隔からの命令等によりデータを消去する機能を設けなかった場合２）ノートパソコン型HIC利用端末は当該研究室内の鍵付きロッカーに保管し、HIC利用以外はロッカーを常時施錠しておくこととする。端末は利用する区画から持ち出さない。

（４）データの持ち込み及び持ち出しについて

* HIC解析環境にデータを持ち込む場合は、事前にウイルスチェックを行い、不正なソフトウェア等が混入していないことを確認した上で、厚生労働省の指定の窓口に持ち込みたい情報を申し出る。
* HIC解析環境から持ち出す対象のデータは副生成物および成果物のみとし、厚生労働省の指定の窓口で所定の手続を行ったのち、HIC利用端末にダウンロードしたデータを、台帳管理している記録媒体を用いて持ち出す。個票を含む生成物は持ち出さない。

（５）情報セキュリティ事故発生時の対応

* ~~NDBデータ及び~~HICに携わる~~利用者~~、取扱者は、情報セキュリティ事故が発生し、又は発生したと思料する事象を発見した場合には、原因の特定、被害拡大の防止、証拠保全等必要な措置を講ずるとともに、速やかに厚生労働省に報告する。

（６）利用の終了及びデータの廃棄

* ~~NDBデータ~~HICの利用後は、遅滞なくHICの利用終了報告書を厚生労働省に提出する。HICの利用終了とともに~~NDBデータ~~生成物を含むHIC環境の廃棄が行われることを認識しておく。

（７）機器の保守

* ~~NDBデータ及び~~HICの利用期間中に、端末の保守を行う場合には、○○研究室内でオンサイトにて行うこととする。その場合は、管理責任者が保守作業に立ち会う。

（８）運用状況の記録・保存

* （利用端末を追跡かつ遠隔からの命令等によりデータを消去する機能を設けた場合）本規定に定める運用が適切に行われているか確認できるようにするため、端末追跡機能のログは、~~NDBデータ~~HIC環境の利用期間終了後、１年間保存すること。
* （利用端末を追跡かつ遠隔からの命令等によりデータを消去する機能を設けなかった場合）本規程に定める運用が適切に行われているか確認できるようにするため、端末へのアクセスログは、~~NDBデータ~~HIC環境の利用期間終了後、１年間保存すること。

（９）緊急時の事業継続等

* 大規模災害等の不測の事態により、取扱区域に不特定多数が立ち入る、取扱区域の損壊等があった場合には遅滞なく厚生労働省へ連絡し、事後の対応を協議する。
* 予期せぬデータの滅失による研究事業の遅滞、中断等の事態を避けるため、HIC内における生成物については、定期的にバックアップをとることに努める。

４．内部監査

本規程に定める運用が適切に行われているか確認することを目的として、「NDBデータ及びHIC解析環境の利用に当たっての~~内部監査（~~自己点検~~）~~規程」を作成する。この規程に基づき、内部監査（自己点検）を6ヶ月毎に実施する。

厚生労働省から、利用状況についてNDBに関する利用規約に定める管理状況報告書の提出を求められた場合には、速やかに当該~~内部監査（~~自己点検~~）~~規程に従った監査を行い、その結果を厚生労働省へ報告する。

５．外部からの問い合わせ

NDBデータの利用にあたっては、国民の理解を得ることが重要であるため、当該利用について外部から問い合わせがあった場合には、原則として管理責任者が対応することとする。

付表１

記憶媒体利用記録台帳

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 番号 | 日付 | 利用開始  時間 | 利用終了  時間 | 氏名 | 備考  (用途、持出の有無、  格納した中間生成物等) |
|  | /　　/ | ： | ： |  |  |
|  | /　　/ | ： | ： |  |  |
|  | /　　/ | ： | ： |  |  |
|  | /　　/ | ： | ： |  |  |

（適宜、行を追加して使用）