大阪医科薬科大学総合医学研究センタートランスレーショナルリサーチ部門

Osaka Medical and Pharmaceutical University BioBank (OMPUBB)

データ取扱いセキュリティガイドライン

2020年7月 制定

2022年5月　修正

目 次

第１ はじめに p.1

第２ 用語定義 p.2

第３ セキュリティ管理において必要な対策 p.3

# 第１ はじめに

大阪医科薬科大学総合医学研究センター トランスレーショナルリサーチ部門 (OMPU Center for Medical Research and Development , Translational Research Program)（以下、「TR部門」という)が運営するバイオバンク（以下、「OMPUBB」という）では、OMPUBB試料等利用ガイドライン（以下、「利用ガイドライン」という）に則ってバイオバンクを運営している。本ガイドラインでは、利用ガイドラインで定義するデータを、外部に漏えいすることなく安全に研究活動に利用するために最低限遵守すべき内容を示す。

OMPUBB が提供するデータはすべて匿名化されているが、他の情報と照合することで個人識別につながるデータが含まれている可能性を考慮すべきであり、セキュリティ管理における対策を講じることが望ましい。

なお、データ利用者をとりまく IT 環境は千差万別で、日々変化しているため、本ガイドラインを遵守するだけでセキュリティが十分に保証されるとは限らない。データ利用者は自身の IT 環境をよく理解し、本セキュリティガイドラインの内容に加え、他のガイドライン[1] [2] [3]も参考にしながら、必要に応じて追加のセキュリティ対策を講じることが必要である。

本ガイドラインについては、IT 環境の進展に応じ、適宜見直しを行うものとする。

# 第２ 用語定義

本ガイドラインにおける用語の定義は、次の通りとする。

（１）OMPUBBデータ

「大阪医科薬科大学総合医学研究センタートランスレーショナルリサーチ部門　Osaka Medical and Pharmaceutical University BioBank (OMPUBB)試料等利用ガイドライン」の第３ 用語定義の　（６）OMPUBBデータ、（７）OMPUBB臨床情報データ、（８）OMPUBB予後情報データ、（９）OMPUBB試料由来データ、（１０）二次データを対象とする。

（２）研究責任者

研究責任者とは、データ利用申請時に登録した研究責任者をいう。

（３）データ利用者

データ利用者とは、データ利用申請時に登録した研究責任者ならびに研究分担者をいう。

（４）所属組織LAN

データ利用者が所属する所属組織のローカルエリアネットワーク (LAN)。ネットワーク管理者が管理するファイアウォールで外部とのアクセスが必要最小限(例：アクセス元、アクセス先のIPアドレスやポートが限定されている）に管理されており、高いセキュリティが保たれているネットワーク。

（５）制限公開データサーバ

データの保存や計算処理を行うための移動しないコンピュータ。所属組織LANに接続している場合は、ファイアウォール機能で所属組織LANの他の機器との間の通信が適切に管理されている。

（６）端末

データがローカルに永続的に保存されることなく、制限公開データサーバ内のデータにアクセスできる機器。

# 第３セキュリティ管理において必要な対策

１ データ利用の原則
OMPUBB が提供するデータは以下の原則に基づいて利用する。
データ利用者をとりまくIT環境は日々変化しているため、データ利用者は所属機関でのネットワークの管理状況や自身のIT環境をよく理解し、本セキュリティガイドラインの内容に加え、他のガイドライン等も参考にしながら、必要に応じて追加のセキュリティ対策を講じること。

（１）データ利用申請で申請した用途に限定する専用のサーバ（仮想サーバを含む）やファイルシステムを用意すること。共同でサーバ等を利用する場合は、データが保存されたフォルダのアクセス権限を、予めTR部門事務局に登録をしているデータ利用者グループに限定し、管理状況についてTR部門事務局に提出すること。

（２）やむを得ず上記（１）のデータサーバ以外にデータを移動しなければならない場合は、事前に手段と期間を明示してTR部門事務局に届けた上で一時的な移動とし、利用終了後は速やかに消去すること。

（３）原則、データのコピーは作成しないこと。やむを得ず以下の動作を行う場合は、TR部門事務局へ所定の様式をもって届け出を行い、コピーを行った媒体の視認できる場所に作成日、削除日、責任者名を記載すること。
・データをバックアップする場合。
・データ移動のために一時的に作成する場合。
・ソフトウェアによって自動的に作成される場合。

（４）データへのアクセスはデータ利用者に限定し、専用の端末のみで行うこと。

２ 研究責任者および研究分担者が遵守すべきこと

（１）利用全般について

①研究責任者は研究分担者等のデータ利用者に対して「OMPUBB試料等取扱いセキュリティガイドライン」を周知して遵守させること。

②データ利用者は、データ利用申請時に登録した内容に従い、制限公開データサーバ（ファイルシステム内での格納場所を含む）に関する情報をデータ利用者のみがアクセス可能な端末で管理・保存し、変更履歴が確認できるようにしておくこと。また、ユーザーの認証や通信・操作などのアクセスログを取得し、適切な証跡管理を行なうこと。

③制限公開データサーバ、利用端末についてはTR部門の指示に従い、その端末の管理者が最新のセキュリティパッチを適用し、適用日を記録すること。
具体的な手法としては、週初めの出勤日は電源を落とさず最新のセキュリティパッチが導入できる状態とすること。

④OMPUBB試料等利用審査会あるいはOMPUBBから依頼された第三者機関が実施する、セキュリティ対策の実施状況に関する監査に応じること。

⑤利用申請時ならびに、毎年4月末、10月末に「OMPUBBデータ取扱いセキュリティガイドラインチェックリスト」をTR部門事務局に提出すること。利用開始日から６か月以内に提出日を迎える場合も提出は必須とする。

（２）制限公開データサーバについて

①データ利用申請で申請した用途に限定する専用のサーバ（仮想サーバを含む）やファイルシステムを用意すること。共同でサーバ等を利用する場合は、データが保存されたフォルダのアクセス権限をデータ利用者グループに限定し、管理状況についてTR部門事務局に提出すること。

②ネットワークに接続する場合はアップデートの自動更新を有効化し、管理者が週初めの出勤日は電源を落とさず最新のセキュリティパッチが導入できる状態とし、ファイアウォール機能を有効にした上で所属組織LANからの通信を管理者が適切に制限すること。

③制限公開データサーバのユーザーIDやパスワードはデータ利用者間であっても共有せず、他人が類推できない十分な強度のパスワード（英大文字、 英小文字、数字、記号のすべてを含む8文字以上）を設定すること。

④不要なソフトウェアをインストールしないこと。特にファイル共有（ファイル交換、P２P）ソフト（例：Winny、BitTorrent）をインストールしないこと。

⑤OS起動時等に自動起動する不要なプロセスはできるだけ停止すること。

⑥分散処理等でデータが複数のサーバにコピーされる場合は、コピー先の制限公開データサーバ、処理の内容、期間について事前にTR部門事務局に申請し、コピー先の制限公開データサーバについても上記①～⑤を適応させること。
また処理期間を明示し、処理が終了した後は速やかにコピーを削除すること。
なお、dbGaP Best Practices Requirements [1]の Appendix A: Best Practice Security Requirements for dbGaP Data Recipients の OS 別 Configuration Guide に示される設定を行うのが望ましい。

３ データ利用者が遵守すべきこと

（１）制限公開データサーバにログインする場合は、通信経路を十分な強度で暗号化すること。

（２）端末から離れる場合は、制限公開データサーバからログアウトするか、端末をロックすること。また、一定時間（１５分程度を目安）以上無操作の場合は画面がロックされるようにあらかじめ確認し、設定しておくこと。

（３）端末画面上のデータをコピーしてローカルディスクに保存しないこと。

（４）端末にデータを自動的に保存する機能（キャッシュ機能）がある場合は機能を無効にしておくこと。

（５）不特定多数が利用する機器（ネットカフェのPCなど）上の端末からデータにアクセスしないこと。

（６）バックアップ取得の際は、以下のいずれかの条件を満たすこと。
・サーバなどの固定機器に保存する場合は、「第３－２ 研究責任者および研究分担者が遵守すべきこと ＜第３－２－（２） 制限公開データサーバについて＞」を満たすこと。
・移動可能機器（例：USBメモリ、CD-ROM、端末登録届け出済のノートPC）に保存する場合は、利用するPCのOS標準搭載機能によってデータ暗号化し、使用後は速やかにデータを消去すること。また、移動可能機器はデータ利用者のみがアクセス可能な電子ファイル等で台帳管理し、盗難や紛失の可能性を最小限にするとともに、当該事実が発生した場合の早期発見を可能にすること。

（７）一時的なデータ移動にやむを得ず移動可能機器を利用する場合もバックアップデータと同様に取り扱うこと。

（８）データの印刷を必要とする場合には、データ利用者以外の目に触れることがないようデータ印刷物を厳重に管理し、利用終了時にはシュレッダー処理すること。

（９）データの利用を終了した場合は、全機器からデータを消去すること。また計算途中で発生した一時ファイルも頻回に消去することが望ましい。