BBJ データ取扱いセキュリティガイドライン（利用者向け）

2018 年 9 月 14 日制定

はじめに

ゲノム研究バイオバンク事業　バイオバンク・ジャパン（以下、BBJ）は、BBJ 試料等利用ガイドライン（以下、利用ガイドライン）に則ってバイオバンクを運営している。このガイドラインは、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したものである。

BBJ が提供するデータは匿名化されているが、他の情報と照合されることによって個人識別が可能になるデータが含まれている場合もあり、データごとに BBJ が指定したセキュリティレベル(標準レベル【TypeⅠ】又はハイレベル【TypeⅡ】）の対策を講じることが求められる。

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、この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、所属組織のセキュリティ規則や他のガイドライン[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求められる。

この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。

１．用語定義

（１）データ

BBJ が提供したデータ。

（２）研究代表者

データ利用申請時に登録した研究代表者。

（３）データ利用者

研究代表者ならびに研究分担者。

（４）所属組織 LAN

データ利用者が所属する組織の 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。

（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。

２．標準レベル [Type Ⅰ]セキュリティにおいて必要な対策

２－１．データ利用の原則

BBJ が提供するデータは以下の原則に基づいて利用すること。

（１）データは、所属組織 LAN に接続する制限公開データサーバ（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こと）、またはネットワークに接続しない制限公開データサーバに保存し、当該制限公開データサーバ外に移動しないこと。

（２）所属組織 LAN 内で、やむを得ず一時的に制限公開データサーバ外にデータを移動しなければならない場合は、利用後速やかに消去すること。

（３）データのコピーは作成しないこと。ただし、以下の場合は例外とする。

・データをバックアップする場合。

・データ移動時に一時的に作成する場合。

・ソフトウェアによって一時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、端末からのみ行うこと。

（５）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、この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、所属組織のセキュリティ規則や他のガイドライン[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。

２－２．研究代表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

①BBJ 試料等取扱いセキュリティガイドラインをデータ利用者に周知して遵守させること。

②データ利用者と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電子ファイル等で台帳管理し、変更が発生する都度、内容を更新すること。なお、変更履歴が確認できるように管理を行うこと。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。

③BBJ 試料等利用審査会あるいは BBJ から依頼された第三者が実施する、セキュリティ対策の実施状況についての監査に応じなければならない。

④利用申請時ならびに、毎年８月に、「BBJ 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」をバイオバンク・ジャパン事務局に提出すること。ただし、利用開始日から６か月以内に８月末日を迎える場合は、当該８月の提出は不要とする。

（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。やむを得ずデータ利用者でないユーザー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すること。

②ネットワークに接続する場合は所属組織 LAN に接続し、以下の条件を満たすこと。

・できる限り最新のセキュリティパッチを適用すること。

・最低限 OS 付属のファイアウォール機能（例：iptables（Linux の場合））を有効にし、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、かつ、他人が類推できない十分な強度のパスワードを設定すること。

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についても上記１～５を満たすこと。

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。

２－３．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設定すること。

（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。画面上に表示されたデータをコピーしてローカルディスクに保存できない端末の利用が望ましい。

（４）端末にデータを自動的に保存する機能（いわゆるキャッシュ機能）がある場合は当該機能を無効にすること。

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

（６）端末には最新のセキュリティパッチを適用すること。

（７）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、「２－２．研究代表者が遵守するべきこと〈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：テープ、USBメモリ、CD-ROM、ノートPC）に保存する場合は、データを暗号化し、使用後は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。

（８）やむを得ず一時的なデータ移動に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。

（９）やむを得ずデータを印刷する場合には、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処理すること。

（10）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こまめに消去することが望ましい。

３．ハイレベル[Type Ⅱ] セキュリティにおいて必要な対策

上記「２．標準レベル [Type Ⅰ]セキュリティにおいて必要な対策」に加え、制限公開データサーバに関して以下の対策を講じること。

以下の条件を全て満たすサーバ室に制限公開データサーバを設置すること。

（１）以下の３つの認証方法の内、２つ以上を組み合わせた多要素認証により入室者を限定すること

・生体認証（例：静脈、指紋、虹彩、顔）

・所有物認証（例：IC カード、ワンタイムパスワード、USB トークン）

・知識認証（例：パスワード）

（２）入室記録を自動取得し、後日監査可能であること。

（３）申請した用途専用のサーバ室であること。専用サーバ室を確保できない場合は、常時施錠された専用のサーバラックに制限公開データサーバを格納すること。

４．本ガイドラインに関する連絡先

バイオバンク・ジャパン事務局

〒108-8639　東京都港区白金台 4-6-1

電話・Fax：03-5449-5122

参考文献

[1]. NIH Office of Science Policy. NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy, Updated: 09 MAR 2015. https://osp.od.nih.gov/wp-content/uploads/NIH_Best_Practices_for_Controlled-Access_Data_Subject_to_the_NIH_GDS_Policy.pdf

[2]. Wellcome Trust Sanger Institute. WTSI Human Data Security Policy (October 2015). https://www.sanger.ac.uk/legal/assets/wtsi-hgdsp-201510hpfinal.pdf

[3]. 厚生労働省. 医療情報システムの安全管理に関するガイドライン第 5 版, 2017 年 5 月. https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf

以　上