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
2020 年 12 月 23 日　改定
2022 年 12 月 2 日　改定

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】・ハイレベル【TypeⅡ】・統計法レベル）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]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）機関外サーバ

データ利用者が、所属機関が所有するサーバ以外に、BBJ が提供するデータの保管や計算処理を行うことが可能なサーバあって、ヒトに関するデータを解析する環境が整っており、かつ、ハイレベル【TypeⅡ】もしくは同等のセキュリティ対策が実施されているサーバであることを BBJ 事務局が確認済みであるサーバ。利用可能な機関外サーバは別紙を参照のこと。

（６）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で、データ利用者またはデータ利用者の所属機関が所有するもの、または別紙に定める機関外サーバ。なお、データサーバを含む IT 環境は、前提条件として以下の①～④を満たすことが必要（「機関外サーバ」のみ利用の場合は除く）。

①ノート PC 等の移動性が高く紛失や盗難のリスクが高い機器を利用していないこと。

②データサーバの機器およびデータを格納する記憶装置/媒体は、それらを所有する機関によって管理されていること。

③データサーバを LAN 内に設置する場合､LAN はデータ利用者の所属機関が所有するものであること。また、データサーバを設置した LAN（以下、データサーバ設置 LAN）は、所属機関のネットワーク管理者によって、外部ネットワークとデータサーバ設置 LAN 間の通信を制限するファイアウォールが設置され、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こと。

④データサーバ設置 LAN 内に､データ利用者以外の者が利用するコンピュータが存在する場合は､ファイアウォール機能で他のコンピュータとの間の通信が適切に管理されていること。

（７）端末

データがローカルに永続的に保存されることなく、データサーバ内のデータにアクセスできる機器。尚、データアクセス端末とデータサーバ間のデータ伝送の際に、データサーバ設置 LAN 外の通信経路を介する場合は、全ての通信経路を十分な強度で暗号化、またはデータ自体を暗号化した上で伝送することが必要。

（８）死因情報

人口動態調査の調査票情報をもとに作成した、研究参加者の死因を ICD-10 コードに変換したデータ。死因情報の利用は、厚生労働省への申し出を行い、承認を得た者に限定される。なお、ここでの死因情報には協力医療機関の診療情報等をもとに作成された死因に関する情報も含む。

（９）死因情報等

死因情報及び、死因情報の解析・集計段階等において結果表等の最終生成物が完成するまでに生成される入出力帳票、チェック済データ、マッチング済データ等、人口動態調査の調査票情報を含んだ生成物。

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、データサーバに保存し、原則、データサーバ外に移動しないこと。

（２）やむを得ず一時的に、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、利用後速やかに復元不可能な方法で消去すること。

（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。これらの場合も、利用後速やかに復元不可能な方法で消去すること。

・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、データサーバまたは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]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データ利用者が、所属機関等の実施する情報セキュリティに関する教育を、受講していることを確認すること。

③データ利用者とデータサーバ（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。

④BBJ 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。

⑤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。

⑥データの漏えい等セキュリティに関する事故が発生した場合、BBJ 試料等利用ガイドライン「３データ利用者の責務」に記載の手順に従い、バイオバンク・ジャパン事務局への通知等の処置を実施すること。

（２）データサーバについて

「機関外サーバ」を利用する場合には、研究代表者が「機関外サーバ」との責任分担を利用規約等で整理しておくこと。

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データサーバ設置 LAN 内にデータ利用者以外の者が利用するコンピュータが存在する場合は、最低限 OS 付属のファイアウォール機能（例：iptables（Linux の場合））や同等の機能を有効にし、データサーバ設置 LAN 内からの通信を適切に制限すること。

③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データサーバにインストールした全てのソフトウェアについて、できる限り最新のセキュリティパッチを適用すること。

⑤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。

⑥ウィルス対策ソフトをインストールし、データサーバ外からファイルを取り込む場合はその場でウイルススキャンを実施すること。またウィルス対策ソフト及びウィルス定義ファイルは最新の状態を維持すること。

⑦OS 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。

⑧セキュリティ監視として、データサーバの各種ログの取得・分析を定期的に行うことが望ましい。

⑨データを保存した機器を廃棄する場合には、データの保存領域を復元不可能な方法で初期化すること。もしくは、復元不可能となるように物理的に破壊すること。

⑩データの漏えい等セキュリティに関する事故が発生した場合、研究代表者は、直ちにデータサーバ設置 LAN からデータサーバやデータアクセス端末を切り離し、バイオバンク・ジャパン事務局への通知等の処置を実施すること。

２－３．データ利用者が遵守すべきこと

（１）所属機関等が実施する情報セキュリティに関する教育を受講し、所属機関が定めるセキュリティ規則を遵守すること。

（２）ユーザーID やパスワードを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。

（３）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。

（４）端末には最新のセキュリティパッチを適用すること。

（５）端末から離れる場合は、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。

（６）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。

（７）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。

（８）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。

（９）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。

(10) フリーWi-Fi やセキュリティ対策が適切に行われていない無線 LAN などからデータにアクセスしないこと。

(11) 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〈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、使用後はデータを復元不可能な方法で消去すること。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。

（12）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。
（13）データの利用を終了した場合は、全機器からデータを復元不可能な方法で消去すること。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。
（14）データの漏えい等セキュリティに関する事故が発生した場合、直ちにデータサーバ設置 LAN からデータサーバや端末を切り離したのち、研究代表者に報告すること。「機関外サーバ」利用の場合には、機関外サーバの利用規程等に従って、直ちに対策を実施するものとする。

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、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データサーバを格納すること。

４．統計法レベルセキュリティにおいて必要な対策

死因情報等を利用する場合は、データ利用者は、死因情報等の利用終了まで、統計法および統計法施行規則を遵守し、「統計法第 33 条に基づく調査票情報の提供に係る厚生労働省事務処理要領」[3]に基づき申し出た管理方法により、適正に管理をしなければならない。死因情報等を適正に管理するために、以下の措置を講じて利用すること。
（１）死因情報等の利用場所（死因情報データファイルの保管を含む）は、死因情報等が持ち出されないよう施錠可能な物理的な場所（日本国内）に限定し、死因情報等の利用時に利用場所に存在する者が確認されるよう、利用場所への入退室管理を行うこと。
（２）死因情報等は限定された媒体に格納し、当該媒体は施錠可能なキャビネット等に保管し、死因情報等を利用するデータサーバや端末は、ワイヤー等によって固定または未使用時は施錠可能なキャビネット等に保管すること。さらに、利用場所から不正に死因情報等が持ち出されないように保安対策を講じること。
（３）死因情報等の削除、死因情報等が記録された機器等の廃棄は、専用ツールを用いるなどにより復元不可能な手段で行うこと。
（４）死因情報等を利用する情報システムに識別及び主体認証、スクリーンロック等の不正操作対策を図り、データ利用者以外の者が死因情報等を保管しているデータサーバや端末にアクセスできないようにすること。
（５）死因情報等を利用する情報システムに、コンピュータウイルス対策、セキュリティホール対策等の

不正アクセス行為防止措置が図ること。
（６）外部ネットワークに接続する可能性のあるデータサーバや端末や利用者以外の者が使用するデータサーバや端末を利用する場合は、オフラインで集計作業等を行い、作業後は当該データサーバおよび端末に死因情報等を残留させない、ダウンロードやアップロードの監視を行うなど、死因情報等（廃棄物含む）の漏えい等事故を防止するための措置を行うこと。
（７）「死因情報に係る管理簿」を用いて、データ利用者ごとの利用状況を記録すること。また、死因情報等の保管・管理は、研究代表者が実施すること。
（８）死因情報等の漏えい、滅失又は毀損の発生又はその兆候を把握した場合は、直ちに、被害拡大の防止、二次被害や類似事案の発生防止等の措置を図るとともに、バイオバンク・ジャパン事務局に報告すること。

５．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：03-5449-5122、Fax：03-6409-2060

参考文献

[1]. Wellcome Trust Sanger Institute. WTSI Human Data Security Policy (October 2015). https://www.sanger.ac.uk/wp-content/uploads/wtsi-hgdsp-201510hpfinal.pdf
[2]. 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 5.2 版（令和 4 年 3 月） https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
[3]. 厚生労働省. 統計法第 33 条に基づく調査票情報の提供に係る厚生労働省事務処理要領, 令和元年５月１日. https://www.mhlw.go.jp/toukei/sonota/dl/manual-02.pdf

変更履歴

版数	日付	内容
第１版	2018 年 9 月 14 日	第１版制定
第２版	2020 年 12 月 23 日	第２版制定 ・「はじめに」に記載しているセキュリティレベルに、「統計法レベル」を追加 ・「はじめに」で参考資料として示している、他のガイドラインの[3]を削除 ・１．用語定義に、（７）死因情報と（８）死因情報等を追加 ・２－２の dbGaP Best Practices Requirements に関する記載を削除 ・「４．統計法レベルセキュリティにおいて必要な対策」を追加 ・５．本ガイドラインに関する連絡先　電話・Fax としていたが、電話と Fax を別の番号に変更 ・参考文献[1]としていた「NIH Security Best Practices for Controlled Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy」を削除し、[2]以降の文献番号を繰り上げ ・参考文献[3]として、「統計法第 33 条に基づく調査票情報の提供に係る厚生労働省事務処理要領」を追加
第３版	2022 年 12 月 02 日	第３版制定 ・１．用語定義（５）として「機関外サーバ」を追加 ・１．用語定義（６）の「制限公開データサーバ」を「データサーバ」に変更し、IT 環境の前提条件を変更。１．用語定義（６）以降に記載の「制限公開データサーバ」は、全て「データサーバ」に変更 ・１．用語定義（７）の「端末」に、データサーバとのデータ転送方法の要件を追加 ・２－１のデータ利用の原則を、機関外サーバの利用が可能な規定に変更し、データ消去方法を追加 ・２－２および２－３を機関外サーバの利用に対応した規定に変更し、改正個人情報保護法に対応した安全管理措置対策を追加