NBDC ヒトデータ取扱いセキュリティガイドライン

（データ利用者向け）

２０１３．４．２５　Ver. １.０
２０１５．２．２５　Ver. ２.０
２０１６．２．２９　Ver. ３.０
２０１８．８．３１　Ver. ４.０
２０２１．６．２２　Ver. ５.０
２０２２．４．　１　Ver. ６.０
２０２４．２．　１　Ver. ７.０

はじめに

大学共同利用機関法人情報・システム研究機構 データサイエンス共同利用基盤施設 ライフサイエンス統合データベースセンター（以下、DBCLS）は、NBDC ヒトデータ共有ガイドライン（以下、共有ガイドライン）に則って NBDC ヒトデータベースを運営している。このガイドラインは、共有ガイドラインで定義する登録者公開データならびに制限公開データを、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。

制限公開データには、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、データごとにデータ提供者が指定したセキュリティレベル（標準レベル【Type Ⅰ】又はハイレベル【Type Ⅱ】）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、制限公開データの保存や計算処理で利用する IT 環境をよく理解し、各 IT 環境の管理者が定める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．制限公開データ、データ
　共有ガイドラインで定義している「制限公開データ」。
２．登録者公開データ
　共有ガイドラインで定義している「登録者公開データ」。
３．研究代表者
　共有ガイドラインで定義している「研究代表者」。
４．データ利用者

制限公開データの利用がヒトデータ審査委員会による審査において承認されたデータ利用者、データ利用者からの委託を受けてその監督のもと従事する者、ならびに、登録者公開データ利用の登録が完了した登録者公開データ利用者。

5．データサーバ（図１参照）

データ利用者が制限公開データの保存や計算処理を行うためのコンピュータで、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、共有ガイドラインで定義している「所属機関外利用可能サーバ（以下、「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。

6．データアクセス端末（図１参照）

データがローカルに永続的に保存されることなく、データ利用者がデータサーバ内のデータにアクセスするための機器。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する、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。

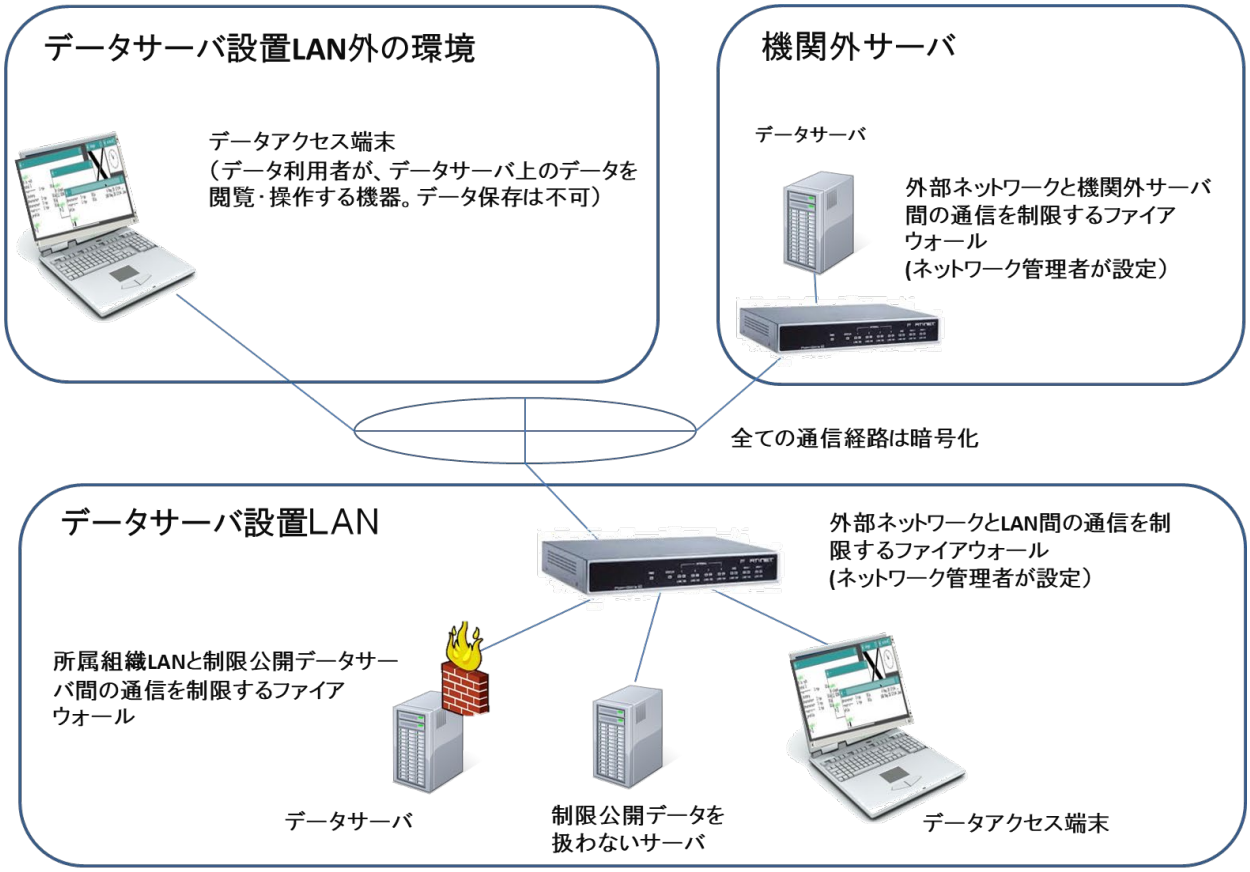

図 1　データサーバ設置 LAN、機関外サーバ、データサーバ、データアクセス端末

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

データ利用者は、制限公開データを以下の原則に基づいて利用すること。

1．データ利用者は、制限公開データを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．データ利用者は、制限公開データを、やむを得ず一時的に、データサーバ設置 LAN 内でデータサーバ外に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．データ利用者は、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．制限公開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データアクセス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。データ利用者はデータの保存やデータの計算処理で利用する IT 環境をよく理解し、各 IT 環境の管理者が定める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．研究代表者が遵守すべきこと

＜利用全般について＞

1．研究代表者は、NBDC ヒトデータ取扱いセキュリティガイドライン（データ利用者向け）を、データ利用者に周知して遵守させること。
2．研究代表者は、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．研究代表者は、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。
4．研究代表者は、ヒトデータ審査委員会、あるいは DBCLS 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ること。
5．研究代表者は、データ利用申請時ならびに、1 年毎に、“NBDC ヒト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”をヒトデータ審査委員会事務局に提出すること。
6．研究代表者は、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、共有ガイドライン「データ利用者の責務」に記載の手順に従い、DBCLS への通知等の処置を実施すること。

＜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．研究代表者は、データ利用申請で申請した用途専用のデータサーバ（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に限定すること。
2．研究代表者は、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．研究代表者は、データサーバのユーザ 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。（8 文字以上であること。数字、英大小文字と記号を組合せたものが望ましい。氏名、電話番号、誕生日等の推測し易いものを利用しないこと。）
4．研究代表者は、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．研究代表者は、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．研究代表者は、ウイ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。またウイルス対策ソフト及びウイルス定義ファイルは最新の状態を維持すること。
7．研究代表者は、OS 起動時等に不要なプロセスはできるだけ起動させないこと。
8．研究代表者は、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．研究代表者は、制限公開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すこと。

２－３．データ利用者が遵守すべきこと

１．から７．は登録者公開データのデータ利用者ならびに制限公開データのデータ利用者が遵守する項目、また、８．から１３．は制限公開データのデータ利用者のみが遵守する項目とする。

1．データ利用者は、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．データ利用者は、ユーザ 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。（８文字以上であること。数字、英大小文字と記号を組合せたものが望ましい。氏名、電話番号、誕生日等の推測し易いものを利用しないこと。）
3．データ利用者は、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．データ利用者は、データアクセス端末には、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．データ利用者は、データアクセス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、データアクセス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データアクセス端末画面がロックされるように設定すること。
6．データ利用者は、データアクセス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。
7．データ利用者は、やむを得ず登録者公開データ閲覧画面や制限公開データを印刷する場合には、登録者公開データのデータ利用者もしくは制限公開データのデータ利用者以外の目に触れることがないよう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。
8．データ利用者は、データアクセス端末から、データサーバ設置 LAN 外の通信経路を介してデータサーバにログインする場合は、データアクセス端末とデータサーバ間のデータ伝送の都度、全ての通信経路を十分な強度で暗号化する、またはデータ自体を暗号化した上で伝送すること。データサーバ設置 LAN 内からデータサーバにログインする場合も、同様の暗号化を行うことが望ましい。
9．データ利用者は、データアクセス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。データアクセス端末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データアクセス端末の利用が望ましい。

10. データ利用者は、データの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。
- データサーバに保存すること。
- 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。

11. データ利用者は、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。

12. データ利用者は、データの利用を終了した場合は、バックアップも含めてデータを全機器から復元不可能な方法で消去すること。紙や移動可能機器で、上記方法での消去ができない場合には、裁断等により復元不可能となるように物理的に破壊すること。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。

13. データ利用者は、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データアクセス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（「機関外サーバ」のみ利用の場合は除く）

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。

1．研究代表者は、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．本ガイドラインに関する連絡先

データ共有分科会事務局
humandbs@dbcls.jp

参考文献

[1]. **NCBI.** NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy. (オンライン) 2015 年 3 月 9 日.
https://www.ncbi.nlm.nih.gov/projects/gap/cgi-bin/GetPdf.cgi?document_name=dbgap_2b_security_procedures.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 版 2017 年 5 月.
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf

NBDC ヒトデータ取扱いセキュリティガイドライン

（データ提供者向け）

２０１３．４．２５　Ver. １.０
２０１８．８．３１　Ver. ２.０
２０２３．２．　１　Ver. ３.０

はじめに

大学共同利用機関法人情報・システム研究機構 データサイエンス共同利用基盤施設 ライフサイエンス統合データベースセンター（以下、DBCLS）は、NBDC ヒトデータ共有ガイドライン（以下、共有ガイドライン）に則ってヒトデータベースを運営している。データ利用者向けには NBDC ヒトデータ取扱いセキュリティガイドライン（データ利用者向け）（以下、データ利用者ガイドライン）を定めている。一方、データ提供者（以下、提供者）に対しては、共有ガイドラインで定義する制限公開データに加えて、公開待機データ（特許取得や論文発表前のデータ）も扱うため、データ利用者と同等以上のセキュリティが求められる。本ガイドラインは、データ利用者向けガイドラインをベースに提供者が講じるべきセキュリティ対策について示したものである。

１．データ利用者ガイドラインの適用について

制限公開データならびに公開待機データを扱う場合は、データ利用者ガイドラインの標準レベル【Type Ⅰ】の適用を原則とし、必要に応じてハイレベル【Type Ⅱ】セキュリティ対策を実施すること。また、提供するデータは、特定の個人（死者を含む）を識別することができることとなる記述等の全部又は一部を除き、代わりに当該個人とかかわりのない符号又は番号を付し、その後、さらに符号又は番号の振りなおしを施したデータに限定する。

また、「１．用語定義」の一部を以下のように読み替え、データ利用者ガイドラインの「２．標準レベル【Type Ⅰ】セキュリティにおいて必要な対策」以降の部分を準用する。

４．データ利用者
　研究代表者ならびに研究代表者の管理下でデータにアクセスする者。

NBDC ヒトデータ取扱いセキュリティガイドライン

（データベースセンター運用責任者ならびに「機関外サーバ」運用責任者向け）

２０１３．４．２５　Ver.1.0
２０１８．８．３１　Ver.2.0
２０２１．６．２２　Ver.3.0
２０２４．２．　１　Ver.4.0

はじめに

大学共同利用機関法人情報・システム研究機構 データサイエンス共同利用基盤施設ライフサイエンス統合データベースセンター（以下、DBCLS）は、NBDC ヒトデータ共有ガイドライン（以下、共有ガイドライン）に則ってヒトデータベースを運営している。データ利用者向けには、「NBDC ヒトデータ取扱いセキュリティガイドライン（データ利用者向け）」（以下、データ利用者ガイドライン）を定めている。一方、データ提供者からデータを預かりデータ利用者に提供するデータベースセンター（以下、DB センター）に対しては、共有ガイドラインで定義する制限公開データや公開待機データ（特許取得や論文発表前のデータ）も扱うため、データ利用者と同等以上のセキュリティが求められる。なお、DB センターが取扱うデータは、特定の個人（死者を含む）を識別することができることとなる記述等の全部又は一部を除き、代わりに当該個人とかかわりのない符号又は番号を付し、その後、さらに符号又は番号の振りなおしを施したデータに限るものとする。

この文書は、データ利用者ガイドラインをベースに DB センターが講じるべきセキュリティ対策について示したものである。また、データ利用者に対して、データの保存や計算処理を行うためのリソースを提供する、共有ガイドラインで定義している「所属機関外利用可能サーバ(以下「機関外サーバ」)」についても、本ガイドラインに準拠するものとする。

なお、DB センターや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。DB センター毎に、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．制限公開データ、データ
　共有ガイドラインで定義している「制限公開データ」。
２．運用責任者

DB センター責任者、または、「機関外サーバ」責任者。

3．作業者
DB センターまたは「機関外サーバ」の運用に係る作業のため、運用責任者がデータサーバに保存されたデータへのアクセスを許可した者。

4．データ利用者
共有ガイドラインで定義している「データ利用者」。

5．データサーバ
DB センターにおいて、データ提供者から提供されたデータの保存や暗号化等の処理、データ利用者への制限公開データの送信、などを行うための計算機環境。または、「機関外サーバ」において、データ利用者が制限公開データの保存や計算処理を行うための計算機環境。

6．データアクセス端末
データがローカルに永続的に保存されることなく、作業者がデータサーバ内の取扱いデータにアクセスするための機器。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する、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。

2．セキュリティ対策について

原則、データ利用者ガイドライン「3．ハイレベル【Type Ⅱ】セキュリティにおいて必要な対策」と同等の対策を実施すること。

2－1．運用責任者が遵守すべきこと

＜運用全般について＞

1．運用責任者は、NBDC ヒトデータ共有ガイドライン及び NBDC ヒトデータ取扱いセキュリティガイドラインに準拠した運用を行うこと。

2．運用責任者は、作業者一覧を作成し、常に最新の状態を維持すること。

3．運用責任者は、NBDC ヒトデータ取扱いセキュリティガイドラインを、作業者に周知して遵守させること。

4．運用責任者は、運用責任者及び全ての作業者に、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させること。

5．運用責任者は、作業者とデータサーバ（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、運用責任者及び作業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。

6．運用責任者は、DBCLS あるいは DBCLS 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ること。

7．運用責任者は、システム構築時及び 2~3 年に一度を目途に、システムセキュリティの専門家によ

る監査を自主的に実施すること。監査結果の写しを、DBCLS に提出すること。

8．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、運用責任者は直ちに対策を実施するものとし、速やかに DBCLS に報告すること。

＜データサーバについて＞

1．運用責任者は、以下の条件①～③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で、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 専用のサーバ室であること。専用の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。

2．運用責任者は、データサーバのデータ保存領域、及びデータ利用者がデータの保存や計算処理に利用する領域について、適切にアクセス制御を行うこと。データサーバやインターネットを介して、作業者及びデータ利用者のみが、許可されたデータのみにアクセスできるよう管理すること。

3．運用責任者は、データサーバを設置している LAN と外部ネットワークとの間にファイアウォールを設置し、外部とのアクセスを必要最小限(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）に管理して高いセキュリティを保つこと。

4．運用責任者は、データサーバを設置している LAN からの通信に対しても、最低限 OS 付属のファイアウォール機能（例：iptables（Linux の場合））等により、適切に制限を行うこと。

5．運用責任者は、データサーバのユーザ ID やパスワードは、データ利用者間での共有を認めないこと、かつ、パスワードは他人が類推できない十分な強度に設定させること。（8 文字以上とすること。数値、英大小文字と記号を組合せたものが望ましい。氏名、電話番号、誕生日等の推測し易いものを利用しないこと。）

6．運用責任者は、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。

7．運用責任者は、サービスに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。

8．運用責任者は、ウイルス対策ソフトをインストールし、データサーバ外から NBDC ヒトデータベースを介して入手したデータ（制限公開データ[Japanese Genotype-phenotype Archive: JGA]、制限共有データ[AMED Genome AGD]、非制限公開データ[DDBJ Sequence Read Archive: DRA, Genomic Expression Archive: GEA]以外の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、ウイルス対策ソフト及びウイルス定義ファイルは最新の状態を維持すること。

9．運用責任者は、OS 起動時等に不要なプロセスはできるだけ起動させないこと。

10．運用責任者は、データサーバでのアクセスログを取得し、定期的に確認すること。

11．運用責任者は、取扱い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。

12. 運用責任者は、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、直ちに対策を実施するものとする。

2－2．作業者が遵守すべきこと

1．作業者は、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すること。
2．作業者は、データアクセス端末から、データサーバが設置されている LAN 外の通信経路を介してデータサーバにログインする場合は、データアクセス端末とデータサーバ間のデータ伝送の都度、全ての通信経路を十分な強度で暗号化する、またはデータ自体を暗号化した上で伝送すること。データサーバが設置されている LAN 内からデータサーバにログインする場合も、同様の暗号化を行うことが望ましい。
3．作業者は、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．作業者は、データアクセス端末には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．作業者は、データアクセス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、データアクセス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データアクセス端末画面がロックされるように設定すること。
6．作業者は、運用責任者またはデータ利用者から許可を得ていないデータにはアクセスしないこと。
7．作業者は、データアクセス端末画面上の取扱い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。データアクセス端末画面上に表示された取扱いデータを、コピーしてローカルディスクに保存することができないデータアクセス端末の利用が望ましい。
8．作業者は、データアクセス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。
9．作業者は、取扱いデータのコピーを作成したり、取扱いデータをデータサーバ外に移動したりしないこと。但し、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。
・取扱いデータをバックアップする場合
・取扱いデータの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
10. 作業者は、データの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。
・データサーバに保存すること。
・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、取扱いデータを暗号化し、使用後は復元不可能な方法で消去すること。また、移動可能機器及びバックアップした取扱いデータについて、「２－１．運用責任者が遵守すべきこと ＜運用全般について＞ ５．」に記載の台帳に記録し、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。
11. 作業者は、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。

12. 作業者は、やむを得ず取扱いデータを印刷する場合には、作業者以外の目に触れることがないよう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。
13. 作業者は、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、直ちに対策を実施するものとし、運用責任者に報告すること。

但し、上記９．～１２．については、「機関外サーバ」は対象外とする。