

NBDC ヒトデータグループ共有データ取扱いセキュリティガイドライン（案）

（データ利用者向け）

2016.00.00 Ver. 1.0

はじめに

国立研究開発法人科学技術振興機構（JST）バイオサイエンスデータベースセンター（以下、NBDC）は、NBDC ヒトデータグループ共有ガイドラインに則って NBDC ヒトデータグループ共有データベースを運営している。このガイドラインは、NBDC ヒトデータグループ共有ガイドラインで定義する NBDC ヒトデータグループ共有データ（以下、グループ共有データ）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。

1. グループ共有データは、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、データ利用者を取りまく 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
NBDC ヒトデータグループ共有データベースから取得したグループ共有データ。
- 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代表者がデータ利用申請時に登録した研究代表者と同一機関に所属する研究分担者。
- ④ 所属組織 LAN（図 1 参照）
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 グループ共有データサーバ（図 1 参照）
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 (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、グループ共有データサーバ内のデータにアクセスできる機器。

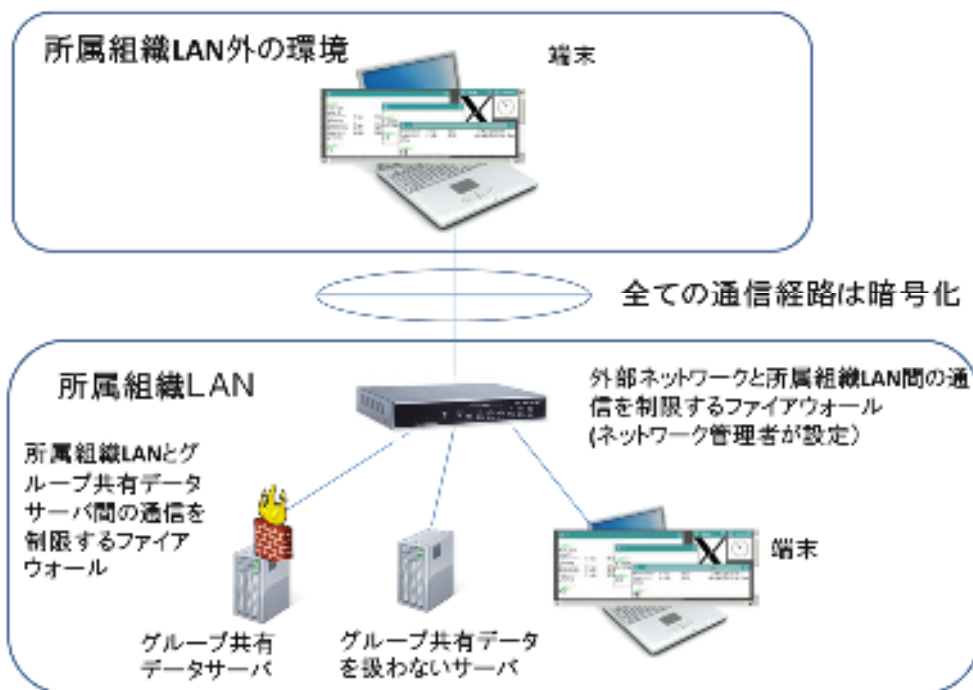


図 1 所属組織 LAN、グループ共有データサーバ、端末

2. 標準レベル [Type 1]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

NBDC が提供するグループ共有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 に接続するグループ共有データサーバ (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グループ共有データサーバに保存し、当該グループ共有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グループ共有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 データ利用者にとりまく 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. 研究代表者が遵守すべきこと

<利用全般について>

- ① NBDC ヒトデータグループ共有データ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 データ利用者とグループ共有データサーバ（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。
- ③ NBDC あるいは NBDC が指定する第三者が実施する監査に協力すること。
- ④ データ利用申請時ならびに、原則、毎年 8 月に“書式 5) NBDC ヒトデータグループ共有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 NBDC ヒトデータ審査委員会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。

<グループ共有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閲覧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 グループ共有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。
- ⑤ OS 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、コピー先のグループ共有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 グループ共有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、グループ共有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べきこと <グループ共有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に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、グループ共有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グループ共有データサーバを設置すること。

- ・ 以下の①～③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
 - ①生体認証（例：静脈、指紋、虹彩、顔）
 - ②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）
 - ③知識認証（例：パスワード）

- ・ 入室記録を自動取得し、後日監査可能であること。
- ・ 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グループ共有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

NBDC データ共有分科会事務局
Humandbs 〈AT〉 biosciencedbc.jp

参考文献

- [1]. **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
http://www.ncbi.nlm.nih.gov/projects/gap/cgi-bin/GetPdf.cgi?document_name=dbgap_2b_security_procedures.pdf
- [2]. **Wellcome Trust Sanger Institute**. HUMAN GENETICS DATA SECURITY POLICY. (オンライン) 2011年2月.
http://www.sanger.ac.uk/datasharing/assets/wtsi_humgendatasecurity_policy.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. (オンライン) 4.1, 2010年2月.
<http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf>

NBDC ヒトデータグループ共有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)

2016.00.00

Ver. 1.0

はじめに

国立研究開発法人科学技術振興機構 (JST) バイオサイエンスデータベースセンター (以下、NBDC) は、NBDC ヒトデータグループ共有ガイドラインに則って NBDC ヒトデータグループ共有データベースを運営している。データ利用者向けには「NBDC ヒトデータグループ共有データ取扱いセキュリティガイドライン (利用者向け)」 (以下、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、NBDC ヒトデータグループ共有ガイドラインで定義する NBDC ヒトデータグループ共有データ (以下、グループ共有データ) を扱うため、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、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. 利用者ガイドラインの適用について

グループ共有データを扱う場合は、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、提供するデータはすべて二重匿名化済みのものに限定する。

また、「1. 用語定義」の一部を以下のように読み替え、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。

- ・ データ
 - データ提供者がデータベースセンターに提供するグループ共有データ
- ・ 研究代表者
 - データ提供申請時に登録した研究代表者
- ・ 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 ヒトデータグループ共有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向け)

2016. 00. 00

Ver. 1.0

はじめに

国立研究開発法人科学技術振興機構（JST）バイオサイエンスデータベースセンター（以下、NBDC）は、NBDC ヒトデータグループ共有ガイドラインに則って NBDC ヒトデータグループ共有データベースを運営している。データ利用者向けには、「NBDC グループ共有データ取扱いセキュリティガイドライン（利用者向け）」（以下、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、NBDC ヒトデータグループ共有ガイドラインで定義する NBDC ヒトデータグループ共有データ(以下、グループ共有データ)を扱うため、データ利用者と同様以上のセキュリティが求められる。この文書は、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。

1. 利用者ガイドラインの適用について

グループ共有データを扱う場合は、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、保管するデータはすべて提供者側で二重匿名化済みのものに限定する。

また、「1. 用語定義」の一部を以下のように読み替え、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」以降の部分為準用する。

- ・ データ
 - DBセンターで取り扱うグループ共有データ
- ・ 研究代表者
 - DBセンター責任者
- ・ データ利用者
 - DBセンター責任者ならびに DBセンターにおいてデータにアクセスする作業員

2. DBセンターで独自に行うセキュリティ対策について

- ① システム構築時及び数年に一度を目途に、システムセキュリティの専門家による監査を受けること。