NBDC ヒト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）

２０１３．４．２５　Ver．１.０

２０１４．１２．８　Ver．２.０

はじめに

独立行政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。

制限公開データは匿名化前のいわゆる個人情報には該当しないが、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 ヒトデータベースから取得した制限公開データ。

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制限公開データサーバ（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、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。

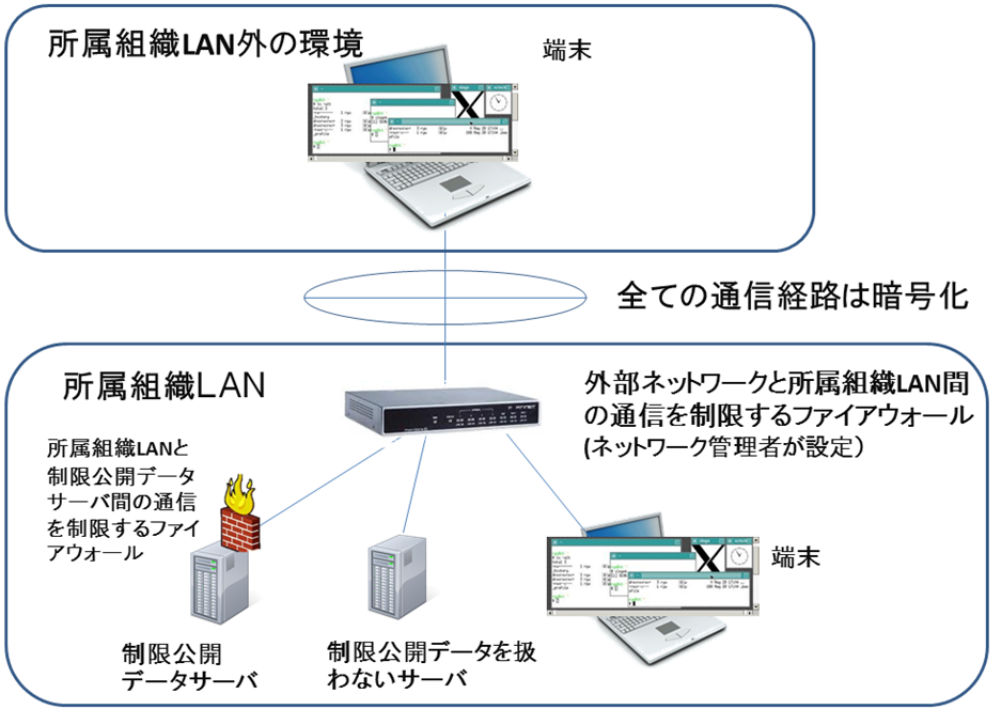

図 1　所属組織 LAN、制限公開データサーバ、端末

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

NBDC が提供する制限公開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．研究代表者が遵守すべきこと

＜利用全般について＞

①　NBDC ヒト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。

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。

＜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　制限公開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。
- 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（※　Ver. ２.０改定における特記事項も参照のこと）。
  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

NBDC データ共有分科会事務局
e-mail address

参考文献

[1]. **NCBI.** dbGaP Best Practices Requirements SECURITY BEST PRACTICE - Level 2b. (オンライン) 2008 年 11 月 8 日.
http://www.ncbi.nlm.nih.gov/projects/gap/pdf/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

Ver.2.0 改定における特記事項

Ver.1.0 の Type II レベルセキュリティでは生体認証のみを要求していたが、Ver.2.0 では生体認証の場合でもさらに所有物認証または知識認証のいずれかを要求することとした。Ver.1.0 に則った入室者管理を既に導入済みの場合は、認証装置の更新などの適切な時期に Ver.2.0 に準拠すること。

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

はじめに

独立行政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（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、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、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

制限公開データならびに公開待機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、制限公開相当データならびに公開待機相当のデータ
- 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）

２０１３．４．２５
Ver. 1.0

はじめに

独立行政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、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。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

制限公開データならびに公開待機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
  - DB センターで取り扱う制限公開データならびに公開待機データ
- 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者

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。
② オープンデータについても不正侵入などによる改ざんを受けないように、オープンデータを取り扱

うサーバ、ネットワーク機器等についても適切に管理すること。