

# NBDCヒトデータ取扱いセキュリティガイドラインおよび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（「機関外サーバ」運用責任者向け）

2018/8 Ver.1.0

項番	チェック内容	チェック欄	実施不可能な場合は理由を記入すること
<b>2. セキュリティ対策について</b>			
<b>2-1. 運用責任者が実施すべきこと</b>			
<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 / NBDCヒトデータグループ共有ガイドライン及び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に準拠した運用を行うこと。	実施します	
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。	実施します	
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 / 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、作業者に周知して遵守させること。	実施します	
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。	実施します	
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。	実施します	
6	運用責任者は、NBDCあるいはNBDC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。	実施します	
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受けること。監査結果の写しを、NBDCに提出すること。	実施します	
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NBDCに報告すること。	実施します	
<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。	実施します	
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アクセスできるよう管理すること。	実施します	
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。	実施します	
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。	実施します	
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。）	実施します	
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。	実施します	
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。	実施します	
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。	実施します	
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。	実施します	
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。	実施します	
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。	実施します	
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。	実施します	
<b>2-2. 作業者が実施すべきこと</b>			
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。	実施します	
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。	実施します	
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。	実施します	
4	作業者は、データアクセス端末には出来る限り最新のセキュリティパッチを適用すること。	実施します	
5	作業者は、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。	実施します	
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。	実施します	
7	作業者は、データアクセス端末画面で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。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端末の利用が望ましい。	実施します	
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。	実施します	
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	対象外	
10	作業者は、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。	対象外	
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。	対象外	
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、データ利用者以外の目に触れることがないように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。	対象外	
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。	実施します	

※本申請書は、NBDCヒトデータ審査委員会による各種審査に関わる業務以外での目的では一切使用いたしません。

日付

セキュリティ状態を確認した機関・部署名

2018/11/27

東北メディカル・メガバンク機構 ゲノムプラットフォーム連携センター

記入者名

木下 賢吾