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

2018/10 Ver1

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
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			
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。		
2－2. 研究代表者および研究分担者が実施すべきこと			
＜利用全般について＞			
1	BBJ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。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。		
3	BBJ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。		
＜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、[illegible]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コピーされる各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。		
2－3. データ利用者が実施すべきこと			
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[illegible]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	バックアック取得の際は、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[illegible]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			
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制限公開データサーバを格納すること。		

日付　　**セキュリティ状態を確認した機関 および 記入者署名**

年　月　日

※本申請書は、BBJ試料等利用審査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。