情報セキュリティ標準

東京大学　医科学研究所

バイオバンク・ジャパン

事務局

第 4.0 版　2017 年 6 月 8 日

承認：バイオバンク・ジャパン定例会議 作成：事務局

目次

1. 目的 2
2. 用語 3
3. 対象とする脅威 5
4. 適用範囲 5
5. 遵守義務 6
6. 情報セキュリティ対策 6
7. 監査および自己点検の実施 6
8. 評価、改訂 7
9. 情報セキュリティ対策基準 7
10. 情報セキュリティ実施手順 8
11. 改訂履歴 8
12. その他 9

1. 目的

2003 年度から文部科学省リーディングプロジェクトとして「オーダーメイド医療実現化プロジェクト」は、47 疾患、約 20 万人（約 30 万症例）を対象に診療情報と血液などから抽出した DNA と血清を収集し、これらを保管するために、バイオバンク・ジャパン（以下、本バンク）を設立した。2008 年度からは登録者の追跡調査も実施している。

また、本バンクに収集された試料・情報は、研究機関や企業に提供されている。提供された試料と情報などを用い、日本人における遺伝情報と病気、薬剤の効果、副作用等との関係を解明することにより、病気の原因の解明を図るとともに個々の体質に応じた医療を可能とするオーダーメイド医療実現に向け、研究成果が継続的に発表されている。

2013 年度からは、引き続き国からの支援を受け、新たに 38 疾患を対象に診療情報と血液などから抽出した DNA を収集している。さらに 2014 年度に血清・血しょうの保管庫を増設し、新たに組織保管庫も新設した。2015 年度からは、外部からの試料の受け入れおよび保管が可能となり、バイオバンク機能を強化させた。

本バンクにおいて取り扱う情報の多くは、提供者の診療情報および重要な個人情報であり厳格な管理のもとで取り扱われるべきものである。このため、万一トラブルが発生した場合は、個人情報保護を最優先課題とした対応を図らなければならない。2015 年 9 月に個人情報保護法の改正が行われ、2017 年 5 月 30 日の施行が決定した。改正個人情報保護法では、「個人識別符号」と「要配慮個人情報」が新たに規定された。本法の新たな定義に基づき、本バンクが DNA を構成する塩基配列と病歴などの情報を組み合わせて使用する場合には、配慮を要すべき個人情報を扱うという認識が必要となる。

このような背景から、「情報セキュリティ標準」（以下、本文書）は、本バンク関係者が提供者の個人情報を厳格に保護し、バンク業務を安全に遂行するため、情報セキュリティ保護に関する基本的な遵守事項を示すものである。

本バンクの関係者ひとりひとりが本文書を理解、遵守し、セキュリティ侵害発生時においても、本バンクが提供者の人権を侵すことなく安全に運用されることを目的とする。

2. 用語

1. 情報セキュリティ
情報資産の機密性、完全性及び可用性を維持すること。

2. 情報セキュリティポリシー
情報セキュリティ方針及び情報セキュリティ標準のこと。

3. 機密性・完全性・可用性
「機密性」とは、情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保すること。
「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保すること。
「可用性」とは、情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

4. ネットワーク
コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

5. 情報システム
コンピュータ、ネットワーク及び電磁的記録媒体ソフトウェア等で構成され、情報処理を行う仕組み。

6. 情報資産
業務に関わるすべての物品（固定資産及び消耗品等を含む）、情報システム、紙媒体情報、電子情報（ハードディスク等の各種媒体に保存される情報、情報システム上の情報）、その他の情報（音声や知識情報、媒体に保存されない情報）等。

7. 試料・情報
「試料」とは、提供を受けた血液又は組織および、それらより抽出されたＤＮＡおよび血清をいう。「情報」とは、提供者の診療情報、遺伝情報その他死者に係るものを含む情報をいう。

8. 診療情報
診断および治療を通じて得られた疾病名、投薬名、検査結果等の情報をいう。

9. 個人情報
ヒトゲノム・遺伝子解析研究に関する倫理指針（平成 13 年 3 月 29 日（平成 29 年 2 月 28 日一部改正）以下、ゲノム指針という）に基づき、以下のように「個人情報」を定義する。

（1）「個人情報」とは、生存する個人に関する情報であって、次に掲げるいずれかに該当するものをいう。

ア）当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は他の方法を用いて表された一切の事項（個人識別符号を除く。）をい

う。以下同じ。）により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

イ）個人識別符号が含まれるもの

(2)「個人識別符号」とは、次に掲げるいずれかに該当する文字、番号、記号その他の符号のうち、個人情報の保護に関する法律施行令（平成 15 年政令第 507 号）その他の法令に定めるものをいう。

ア）特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

(3)「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要する記述等が含まれる個人情報をいう。

(4) ヒトゲノム・遺伝子解析研究において扱う情報が、個人情報に該当しない場合であっても、遺伝情報、診療情報等個人の特徴や体質を示す情報は、ゲノム指針の第 5 の 12 ①及び②に基づき適切に取り扱わなければならない。

10. 遺伝情報
試料等を用いて実施されるヒトゲノム・遺伝子解析研究の過程を通じて得られる個人の遺伝子、ゲノム情報。

11. 匿名化
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（個人識別符号を含む）の全部又は一部を削除すること（当該記述等の全部又は一部を当該個人と関わりのない記述等に置き換えることを含む。）をいう。
安全管理措置の一環として特定の個人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取り除き、当該情報を単に「匿名化されている情報」として規程する。

12. 対応表
匿名化された情報から、必要な場合に提供者を識別することができるよう当該提供者と匿名化の際に置き換えられた記述等とを照合することができるようにする表その他これに類するものをいう。

13. 提供者
本プログラムのために試料等を提供する人をいう。

14. 個人情報管理者
試料・情報の提供が行われる機関を含め、個人情報を取り扱う研究を行う機関において、当該機関の長の指示を受け、提供者等の個人情報がその機関の外部に漏えいしないよう個人情報を管理し、かつ、匿名化する責任者をいう。

15. メディカルコーディネーター
ゲノム指針に基づきインフォームド・コンセントの履行補助者としてメディカルコーディネーター（以下、MC）をおく。MC は、本プログラムの内容および意義等について十分に理解した上で、本プログラムにおける試料、診療情報収集、インフォームド・コンセント取得および匿名化の実務を行う者をいう。
各病院で本プログラム業務を遂行する職員であり、提供者の個人情報を保護するための守秘義務を負っている。但し、外部の者がインフォームド・コンセントを受ける業務を行う場合には、原則法的な守秘義務を負っている者を選定しなければならない。

16. 従事者
業務に従事する作業者、研究者、その他守秘義務契約等に基づく者。

17. 情報セキュリティ管理者
情報システムや入退室管理装置に対して、利用者の操作履歴を管理し、不正な操作等を監視する者。情報セキュリティ対策の構築、運用指導を行なう者。

18. 情報システム管理者
情報システムに対する管理責任者で、対策の指示や指導、緊急時の対応、トラブル後の対応指示を行なう者。

19. 冗長化
一部の設備が故障してもシステム全体の機能を維持し続けられるように、設備またはシステム二重化もしくは代替機やバックアップを用意してシステムを構築すること。耐障害性、信頼性を高めるための技法のひとつ。

20. 情報セキュリティインシデント
望まないまたは予期しない単独または一連の情報セキュリティ事象（情報セキュリティ基本方針への違反もしくは管理策の不具合の可能性など）で、事業運営を危うくする確率およびセキュリティを脅かす確率が高いもの。

3. 対象とする脅威

以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震、落雷、火災等の災害による業務の停止等

(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

適用対象の機関は、バイオバンク・ジャパン、バイオバンク・ジャパンに試料または臨床情報を提供する機関または団体、検査会社、試料または臨床情報の提供を受ける機関または団体とする。

適用対象の者は、試料の保管・管理に従事している者とその管理者（または責任者）、対象の研究に関わる者とその管理者（または責任者）、次項の情報を取り扱う者とする。

適用対象の情報は、次のとおりとする。

(1) 試料と臨床情報およびそれらの記録媒体

(2) 業務を遂行するためのネットワークおよび情報システム、業務記録

(3) 情報システムの仕様書およびネットワーク図等のシステム関連文書

※ いずれも印刷した文書を含む

5. 遵守義務

適用対象者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び関連法令、倫理指針を遵守しなければならない。

バイオバンク・ジャパンと連携する研究グループおよび医療機関、検査会社等に属する者は、所属する団体の情報セキュリティポリシーまたは実施手順書を優先する。

6. 情報セキュリティ対策

対象とする脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7. 監査および自己点検の実施

定期的または必要に応じて情報セキュリティ監査および自己点検を実施する。

技術面および物理面での具体的な安全対策は各方面の技術革新などにより見直しが必要になる場合があるため、年１回以上実施する。

8. 評価、改訂

情報セキュリティ監査及び自己点検の結果、本文書の見直しが必要となった場合、情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には該当箇所を見直し、対策を講じる。

本文書の改定にあたっては、関連法規、倫理指針との整合性に留意する。評価結果と改定内容については、バイオバンク・ジャパンの定例会議で承認を受けてから施行することを原則とする。

9. 情報セキュリティ対策基準

具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

(1) 組織体制

- 情報セキュリティ責任者
- 情報セキュリティ管理者
- 兼務の禁止
- 窓口の設置

(2) 情報資産の分類と管理

- 分類方法
- 分類
- 情報資産の管理

(3) 物理的セキュリティ

- 管理区域
- サーバ等の管理
- 通信回線及び通信回線装置の管理
- 端末や記録媒体等の管理

(4) 人的セキュリティ

- 基本的な遵守事項
- 退職時等の遵守事項
- 非常勤及び臨時担当者への対応
- 情報セキュリティポリシー等の掲示
- 外部委託事業者に対する説明
- 研修・訓練
- 情報セキュリティインシデントの報告
- ID 及びパスワード等の管理

(5) 技術的セキュリティ

- コンピュータ及びネットワークの管理
- アクセス制御
- システム開発、導入、保守等
- 不正プログラム対策
- 不正アクセス対策
- セキュリティ情報の収集

(6) 運用

- 情報システムの監視
- 情報セキュリティポリシーの遵守状況の確認
- 侵害時の対応等
- 例外措置
- 法令遵守
- 情報セキュリティポリシーが遵守されなかった場合の対応
- 外部サービスの利用
- 約款による外部サービスの利用
- ソーシャルメディアサービスの利用

10.情報セキュリティ実施手順

適用対象の団体は、情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定すること。

なお、情報セキュリティ実施手順は、公にすることにより運営に重大な支障を及ぼすおそれがあることから非公開とする。

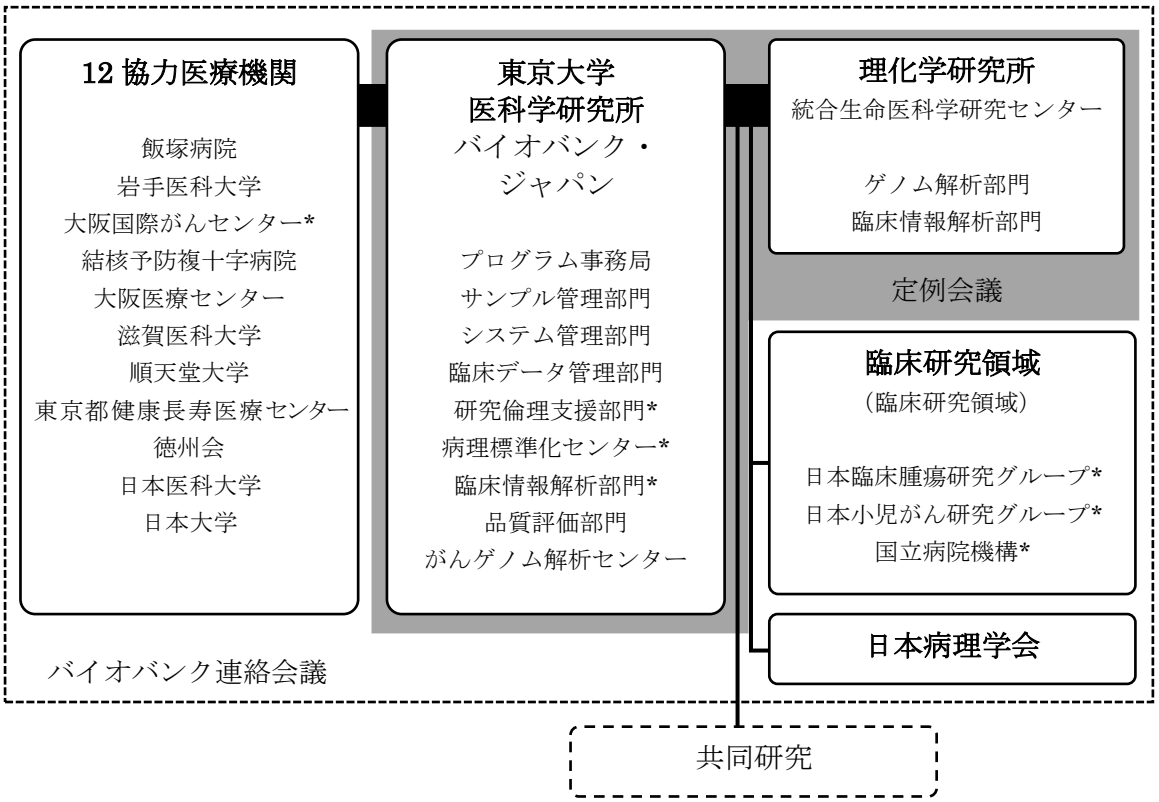
11.改訂履歴

2004 年 3 月 2 日　第 1 版発行

No.	年月日	変更内容／理由	修正後版数
1	2005 年 6 月 13 日	「ヒトゲノム・遺伝子解析研究に関する倫理指針」改定に伴う変更。 個人情報保護法施行に伴う変更。	第 2.0 版
2	2017 年 5 月 29 日	「ヒトゲノム・遺伝子解析研究に関する倫理指針」改定に伴う変更。 個人情報保護法施行に伴う変更。	第 3.0 版
3	2017 年 6 月 8 日	ISO9001、ISO27001:2013 対応における見直し	第 4.0 版

12.その他

1. オーダーメイド医療の実現プログラム実施体制



大阪国際がんセンター*（大阪府立成人病センター）、研究倫理支援部門*（ELSI 検討委員会を含む）、病理標準化センター*（東大病院）、臨床情報解析部門*（臨床情報研究グループを含む）、日本臨床腫瘍研究グループ*（JCOG）、日本小児がん研究グループ*（JCCG）、国立病院機構*（NHO）

2. 会議体の役割と責任

(1) バイオバンク連絡会議

試料と診療情報の収集を実施する協力医療機関連絡責任者と、バイオバンク・ジャパンの運営を実施する東京大学医科学研究所、協力研究機関である理化学研究所統合生命医科学研究センターの担当者によって構成されている。また、試料・情報の提供が行われる機関を含め、個人情報を取り扱う研究を行う機関において、当該機関の長の指示を受け、提供者等の個人情報がその機関の外部に漏えいしないよう個人情報を管理し、かつ、匿名化する責任者をおく。

(2) バイオバンク・ジャパン定例会議(以下、定例会議)

本バンク年次計画案の準備や研究実施上必要な調整を行う。

(3) 研究倫理支援部門（ELSI 検討委員会を含む）

本プログラムの適正な推進のために研究倫理に関する諸課題について支援する部門を置く。また、本部門には、ELSI（Ethical, Legal and Social Issues、倫理的・法的・社会的問題）について、本プログラムの推進から独立した立場にある有職者を招聘し、助言指導を行う ELSI 検討委員会を設置する。

(4) 試料等配布審査会

バイオバンク・ジャパンで保管・管理されている試料の配布や情報の提供を希望する研究者又は研究機関に対して、その研究計画が科学的に妥当であるか、審査を行う。