個人の遺伝情報に応じた医療の実現プロジェクト
情報セキュリティ標準

第 2.0 版

2005 年 6 月 13 日

個人の遺伝情報に応じた医療の実現プロジェクト

目　次

1. はじめに ____ 3
1.1. 目的 ____ 3
1.2. 適用範囲 ____ 3
1.3. 用語の定義 ____ 3
2. プロジェクト体制 ____ 6
2.1. 役割と責任 ____ 6
2.2. 兼務条件 ____ 7
3. 情報セキュリティ対策 ____ 8
3.1. 人的セキュリティ対策 ____ 8
3.1.1. 体制整備 ____ 8
3.1.2. 機密保持契約 ____ 8
3.1.3. 情報セキュリティ教育 ____ 8
3.2. 情報資産に関するセキュリティ対策 ____ 9
3.2.1. 情報種別定義 ____ 9
3.2.2. 特に取り扱いに注意すべき情報資産 ____ 11
3.3. 情報システムに関するセキュリティ対策 ____ 12
3.3.1. 情報システムの構築、運用 ____ 12
3.3.2. 情報システムの管理 ____ 13
3.4. 情報保護施設に関するセキュリティ対策 ____ 14
3.4.1. セキュリティ環境の整備 ____ 14
3.4.2. 施設管理 ____ 14
4. セキュリティ侵害への対応策 ____ 15
4.1. 初動措置 ____ 15
4.2. 暫定措置 ____ 15
4.2.1. 対策の決定 ____ 15
4.2.2. 対策の実施 ____ 15
4.2.3. 報告、周知 ____ 15
4.3. 恒久措置 ____ 15
5. 監査 ____ 16
6. 遵守義務及び罰則 ____ 16
7. 関連ドキュメントの作成 ____ 17
8. 本文書の評価、改定 ____ 17

1. はじめに

1.1. 目的

「個人の遺伝情報に応じた医療の実現プロジェクト」（以下、本プロジェクト）は、文部科学省リーディングプロジェクトの課題のひとつであり、約 30 万人の提供者から試料等の提供を受け、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共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た研究基盤を構築するものである。

本プロジェクトにおいて取り扱う情報の多くは、提供者の臨床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。

このような背景から、「個人の遺伝情報に応じた医療の実現プロジェクト情報セキュリティ標準」（以下、本文書）は、本プロジェクト関係者が提供者の個人情報を厳格に保護し、本プロジェクト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。

本プロジェクトの関係者一人一人が本文書を理解、遵守し、セキュリティ侵害発生時においても、本プロジェクト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。

1.2. 適用範囲

本文書は、本プロジェクト業務に関わる、人、情報資産、情報システム、情報保護施設など、情報セキュリティに関するあらゆるものに適用される。

1.3. 用語の定義

本文書では、以下のように用語を定義する。

(1) 提供者
本プロジェクトのために試料等を提供する人。

(2) 臨床情報
診断及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。

(3) 試料
本プロジェクトにおいて提供を受けた血液又は組織及び、それらより抽出されたゲノムＤＮＡ及び血清。なお、臨床情報を含める場合は、「試料等」という。

(4) 個人情報
個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができる情報。他の情報と容易に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ものを含む。

(5) 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、又は既に試料等に付随している子孫に受け継がれ得る情報で、個人の遺伝的特徴及び体質を示すものをいう。

(6) 匿名化
ある人の個人情報が法令、本文書、「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 16 年 12 月 28 日全部改正））」（以下、倫理指針）又は研究計画に反して外部に漏洩しないように、その個人情報から個人を識別する情報の全部又は一部を取り除き、代わりにその人と関わりのない符号又は番号を付すこと。試料等に付随する情報のうち、ある情報だけでは特定の人を識別できない情報であっても、各種の名簿等の他で入手できる情報と組み合わせることにより、その人を識別できる場合には、組合せに必要な情報の全部又は一部を取り除いて、その人が識別できないようにすること。
なお、本プロジェクトでは倫理指針にある連結可能匿名化の手法を用いる。

(7) プロジェクト参加機関
本プロジェクトの業務を行う東京大学医科学研究所、理化学研究所及び、本プロジェクトに関して両研究所と契約を交わした組織。

(8) 外部の組織
プロジェクト参加機関以外の組織。なお、プロジェクト参加機関の中で本プロジェクトに関わっていない別の組織も外部の組織とみなす。

(9) 個人情報管理者
試料等の提供が行われる組織において、その組織の長の指示を受け、提供者等の個人情報がその組織の外部に漏洩しないように個人情報を管理し、かつ、匿名化する責任者。個人情報管理者は本プロジェクトにおいて提供された試料等を用いて、ヒトゲノム・遺伝子解析研究を行うことが禁止される。なお、個人情報管理者は法的な守秘義務を負う必要がある。
個人情報管理者の指示、監督の下、提供者等の個人情報を管理し、かつ、匿名化する担当者を個人情報管理補助者という。

(10) メディカルコーディネーター
本プロジェクトの内容及び意義等について十分に理解した上で、本プロジェクトにおける試料、臨床情報収集、インフォームド・コンセント取得及び匿名化の実務を行う者。
各病院で本プロジェクト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。

(11) 情報システム管理者
各組織において、本プロジェクトで使用する情報システムの管理責任を負う者。

(12) データ管理者
各組織において、本プロジェクトで使用する情報システムの内部で取り扱う情報資産の管理責任を負う者。

(13) ネットワーク管理者
各組織において、本プロジェクトで使用するネットワークの管理責任を負う者。

(14) プロジェクト関係者
東京大学医科学研究所、理化学研究所及び、本プロジェクトに関していずれかの研究所と契約を交わした組織において、本プロジェクト業務を遂行する者。

(15) セキュリティ侵害
犯罪、過失、システム障害、自然災害などにより、提供者の個人情報が流出する可能性が生じるなど、本プロジェクトの遂行に支障を来たす危険性がある事象。

(16) 監査
本プロジェクトを倫理的、法的、社会的側面から適切に運営するため、プロジェクト参加機関に対して本文書、関連法令、倫理指針の遵守状況を監督、検査すること。
(17) 情報資産
提供者から提供を受けた試料等及び本プロジェクト業務に関わるすべての物品（固定資産及び消耗品等）、情報システム、紙媒体情報、電子情報（ハードディスク、フロッピー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。
(18) 情報システム
本プロジェクト業務に関わるコンピュータ機器、通信機器、ソフトウェア等。
(19) 情報保護施設
情報資産及び情報システムを保護する施設。

2. プロジェクト体制

2.1. 役割と責任

本プロジェクトにおける会議体及び、組織の役割と責任について以下に示す。

(1) 推進委員会
本プロジェクトの基本方針の策定、年次計画の策定、研究運営上の指導助言などプロジェクトの適正かつ円滑な実施に必要な重要事項の審議、決定を行う会議体。本プロジェクトの基本方針に関する全ての責任を負う。委員長は委員がこれを互選する。

(2) 実施会議
推進委員会の下に置かれ、本プロジェクト年次計画案の準備や研究実施上必要な調整を行う。その他、推進委員会の求めに応じ所要の処置を講ずる。
プロジェクトリーダーは、本プロジェクトの研究遂行の責任を負い、実施会議の議長を務める。

(3) プロジェクト事務局
プロジェクト方針に従い、プロジェクトを円滑に運営するため、プロジェクト参加機関への連絡、調整、教育、監査等を行う組織。本文書に基づいた各種ドキュメントの作成、管理を行う。また、医療機関相談窓口、提供者相談窓口として苦情・相談を受ける。

(4) 緊急対策委員会
重大なセキュリティ侵害が発生した際、プロジェクトリーダーにより召集され、緊急対応策の決定とプロジェクト内部の関連組織への指示を行う会議体。重大なセキュリティ侵害への対応と推進委員会、実施会議への報告責任を負う。

(5) 臨床検査会社
病院にて提供された試料からの DNA 抽出及び、試料の輸送を行う組織。病院からバイオバンクジャパンまでの試料取り扱い（DNA 抽出、輸送）に関する責任を負う。

(6) 協力医療機関
本プロジェクト業務遂行のために、法人及び行政機関で構成された病院群の総称。各協力医療機関には協力医療機関代表及び協力医療機関連絡責任者を置き、各病院における本プロジェクト業務に関する監督、業務状況のプロジェクト事務局への報告に関する責任を負う。

(7) 病院
本プロジェクトにおいて試料等の提供を受ける組織。メディカルコーディネーターより提供者からインフォームド・コンセントを取得し、試料等の提供を受け、提供者の個人情報を匿名化する。病院内で遂行される本プロジェクト業務に関する全ての責任を負う。

(8) 主幹研究機関
本プロジェクトにおいて試料等の保管、研究の遂行をする組織。東京大学医科学研究所及び理化学研究所遺伝子多型研究センター。

(9) バイオバンクジャパン
本プロジェクトにおける試料、臨床情報、遺伝情報及び解析結果を管理する主幹研究機関の部門（バイオバンク、統合臨床データベース管理部、データ管理バンク）の総称。
(10) バイオバンク
病院から送られた試料を保管・管理し、研究機関からの要請に従い分配を行う部門。試料の管理に関する責任を負う。
(11) 統合臨床データベース管理部
病院から提供された臨床情報を整理統合する統合臨床データベースを管理する部門。臨床情報の管理責任を負う。
(12) データ管理バンク
研究機関から提供された遺伝情報の保管、蓄積している遺伝情報と臨床情報を用いた解析、及びバイオバンクジャパン内の業務管理を行う部門。東京大学医科学研究所から委託された組織が管理、運用を行う。
(13) 共同研究機関
本プロジェクトに関して主幹研究機関と共同研究に関する契約を結んだ公的又は民間の研究機関及び、法人及び行政機関。契約内容に関する責任を負い、また試料等が提供された場合は、その管理責任を負う。
(14) 文部科学省
本プロジェクトの監督官庁であり、主幹研究機関に本プロジェクト業務を委託する。
(15) ELSI（倫理的・法的・社会的問題）委員会
本プロジェクトに関する倫理的、法的、社会的問題全般についての調査及び、助言を行う組織。

2.2. 兼務条件

前項「2.1. 役割と責任」に挙げた組織の一部は、倫理指針及び、本文書「3.2.2. 特に取り扱いに注意すべき情報資産」に従い、以下の兼務条件に留意しなければならない。

- 病院に属する個人情報管理者は、研究機関（主幹研究機関、共同研究機関）と兼務することができない。
- バイオバンク、統合臨床データベース管理部、データ管理バンク、プロジェクト事務局に属し、情報システム操作や試料等を直接取り扱う者はそれぞれ互いに兼務することができない。

3. 情報セキュリティ対策

情報セキュリティ侵害の発生を予防するために、対象となるプロジェクト関係者、情報資産、情報システム、情報保護施設にあるリスクの分析を行い、どのようなリスクが存在するかを事前に把握し、適切な対策を講じなければならない。

3.1. 人的セキュリティ対策

人的セキュリティの侵害には、プロジェクト関係者が故意に引き起こす内部犯罪や過失による紛失、事故等が存在する。これらを防ぐために、守秘義務を含んだ契約や情報セキュリティ教育を行わなければならない。

3.1.1. 体制整備

各組織の長は、適切な者に業務の一部を委託でき、自組織のすべてのプロジェクト関係者及び、再委託先の選定についての責任を負い、それらを監督しなければならない。また、プロジェクト関連業務の一部を再委託する際は、再委託の内容をプロジェクト事務局に報告しなければならない。

3.1.2. 機密保持契約

本プロジェクト業務に従事するものは、業務遂行に際して知り得た情報やノウハウを、業務遂行上認められる場合を除き、その職を辞した後も第三者に開示、提供、漏洩してはならない。特に個人情報を取り扱う際は、セキュリティ侵害が発生しないように注意する。

また、東京大学医科学研究所と本プロジェクトに関わる機密保持の契約を直接的、もしくは間接的に交わしていなければならない。機密保持条項には以下の点を含むようにする。

- 機密保持の範囲
- 権利義務の譲渡
- 契約終了時の義務
- 契約期間

3.1.3. 情報セキュリティ教育

プロジェクト参加機関は、本文書導入時、新規採用時及び、定期的にセキュリティ教育を実施し、プロジェクト関係者に情報セキュリティに関する義務と責任の周知徹底を図る。

プロジェクト事務局は、本文書変更時における広報、利用者支援を実施し、最新の本文書を周知させ、情報セキュリティに対する意識の維持、向上を図る。

3.2. 情報資産に関するセキュリティ対策

情報資産のセキュリティ侵害には、プロジェクト関係者や外部の者が引き起こす盗難、盗聴、不正利用等があり、またプロジェクト関係者の過失による紛失、破損等がある。これらを防ぐために情報種別を設定し、種別ごとに情報資産を適切に管理しなければならない。

3.2.1. 情報種別定義

本プロジェクトに関する情報資産を適切に管理、運用するために、すべての情報資産に対して、プロジェクトの方針に従い情報種別を定め、開示範囲を明らかにしなければならない。指定した情報種別及び開示範囲については、各組織の長の承認を得なければならない。

また、プロジェクト関係者は定められた情報種別の取り扱い方法に従い、情報資産を取り扱わなければならない。

本プロジェクトの情報種別及び取り扱い方法は以下の通りとする。

■　情報種別：レベル 3

提供者の個人情報を指し、極めて機密性が高く、限られた者しかアクセスできない情報、物品を指す。

【電子情報】

取得：　正当な理由がある場合に限り、病院内の限られた者のみ提供を受ける。

複製：　正当な権限を持つ者であっても、原則として複製を禁止する。止むを得ず行う場合は、複製物の所在と複製数を記録し、原本と同等に管理しなければならない。

保管：　必要最小限の利用者に閉じてアクセス制御を行うとともに、原則として暗号化して保存する。また、操作履歴を必ず取得する。法、または推進委員会、実施会議の定めた保管期間の間、厳重に保管しなければならない。

送受信：　実施会議が認めた接続方式以外のいかなる場合においてもネットワークで暗号化されないまま伝送することを禁止する。また、送受信記録を必ず取得する。
紛失、誤送がないよう細心の注意を払う。

消去：　復旧コマンド等でも復元ができないように削除する。

【物品、紙媒体情報】

取得： 正当な理由がある場合に限り、病院内の限られた者のみ提供を受ける。

複製： 正当な権限を持つものであっても、原則として複製を禁止する。止むを得ず行う場合は、複製物の所在と複製数を記録し、原本と同等に管理しなければならない。

保管： 保管庫にて施錠管理する。また、保管庫の鍵管理記録もしくは物品の利用記録を必ず取得する。法、または推進委員会、実施会議の定めた保管期間の間、厳重に保管しなければならない。

授受： 封書を用いる等、内容を秘匿できる状態で行う。ＦＡＸ等の公衆回線の利用を禁止する。外部者を利用する場合は送達を確認できる手段を利用する。また、授受記録を必ず取得する。

廃棄： 細断や破壊など適切な所要の措置をとる。また、廃棄記録を必ず取得する。

■ 情報種別：レベル２

機密性が高く、本プロジェクトの業務を遂行するにあたり重要な情報、物品を指す。

【電子情報】

取得： 正当な理由がある場合に限り、正当な権限を持つ者からのみ、提供を受ける。

複製： 正当な権限を持つものであっても、必要数以上複製してはならない。複製物に関しては、所在と複製数を記録し、原本と同等に管理しなければならない。

保管： あらかじめ指定された開示範囲に基づきアクセス制御を行う。また、操作履歴を取得する。法、または推進委員会、実施会議の定めた保管期間の間、厳重に保管しなければならない。

送受信： インターネットや組織内の既存 LAN 等の外部ネットワークにおいては、暗号化して伝送しなければならない。
紛失、誤送がないよう十分注意する。

消去： 復旧コマンド等でも復元ができないように削除する。

【物品、紙媒体情報】

取得： 正当な理由がある場合に限り、正当な権限を持つ者からのみ、提供を受ける。

複製： 正当な権限を持つものであっても、必要数以上複製してはならない。複製物に関しては、所在と複製数を記録し、原本と同等に管理しなければならない。

保管： 限定された者のみ利用可能な部屋、もしくは保管庫にて施錠管理する。法、または推進委員会、実施会議の定めた保管期間の間、厳重に保管しなければならない。

授受： 封書を用いる等、内容を秘匿できる状態で行う。ＦＡＸ等の公衆回線の利用を禁止する。

廃棄： 細断や破壊など適切な所要の措置をとる。

■ **情報種別：レベル１**

機密性が低い本プロジェクトに関する情報、物品を指す。

【電子情報】
取得： 正当な理由がある場合に限り、正当な権限を持つ者からのみ、提供を受ける。
複製： 正当な権限を持つ者であっても、必要数以上複製してはならない。
保管： あらかじめ指定された開示範囲に基づきアクセス制御を行う。法、または推進委員会、実施会議の定めた保管期間の間、厳重に保管しなければならない。
送受信： 紛失、誤送がないよう注意する。
消去： 適切に削除する。

【物品、紙媒体情報】
取得： 正当な理由がある場合に限り、正当な権限を持つ者からのみ、提供を受ける。
複製： 正当な権限を持つ者であっても、必要数以上複製してはならない。
保管： 整理整頓し、適切に管理する。法、または実施会議の定めた保管期間の間、厳重に保管しなければならない。
授受： 紛失、誤送がないよう注意する。
廃棄： 適切な所要の措置をとる。

■ **情報種別：レベル０**

機密性がない、あるいは極めて機密性が低く、プロジェクト業務を円滑に遂行するために本プロジェクト関係者等に限らず広く一般に開示される情報、物品を指す。

【電子情報、物品、紙媒体情報】
紛失等に注意し、適切に取り扱う。

3.2.2. 特に取り扱いに注意すべき情報資産

特に取り扱いに注意すべき情報資産に関しては､原則的に以下の項目に従わなければならない。また、提供者からの同意撤回が行われた際は、上記の情報資産について、困難な場合を除きすべて削除または廃棄することとする。

■ 個人情報
提供者の個人情報が付された情報資産は、病院以外では扱うことができない（病院内で提供者の個人情報の匿名化を施すため、病院外の組織においてはレベル 3 の情報資産は存在しないこととなる)。
プロジェクト関係者の個人情報については、各組織内のルールに従い適切に管理しなければならない。
但し、個人情報の開示や訂正の請求があった場合は、関連法令及び倫理指針に遵守した上で対応しなければならない。

- 試料
  病院にて提供された試料は、本プロジェクトに参画している病院、臨床検査会社、バイオバンク以外では扱うことができない。但し、推進委員会、実施会議において生命倫理の有識者と共に検討した上で許可を受けた場合はその限りではない。
- 臨床情報
  匿名化された臨床情報は、病院、統合臨床データベース管理部、データ管理バンク以外では扱うことができない。但し、推進委員会、実施会議により許可を受けた場合はその限りではない。
- 遺伝情報
  遺伝情報は、データ管理バンク以外では扱うことができない。但し、推進委員会、実施会議により許可を受けた場合はその限りではない。
  また、本プロジェクトで得た遺伝情報は、直接的に提供者の利益にならないこと、並びにセキュリティ維持のため提供者には開示しないこととする。
- 匿名化対応表
  匿名化に用いた対応表は、各病院の個人情報管理者及び個人情報管理補助者以外は扱うことができない。

3.3. 情報システムに関するセキュリティ対策

情報システムのセキュリティ侵害には、プロジェクト関係者や外部の者が引き起こす不正アクセス、盗聴等があり、また過失による操作ミスや、偶発的な障害等がある。これらを防ぐために、以下の項目に留意しなければならない。

3.3.1. 情報システムの構築、運用

情報システムは、以下の点に留意して構築、運用されなければならない。

(1) 識別、認証
情報システムは、利用者を一意に識別できる仕組みを設けなければならない。プロジェクト関係者は、情報システムを利用するにあたり、利用者を一意に特定するために付与される識別子（ＩＤ）によって識別され、指紋やパスワード等によって認証される。また、プロジェクト関係者は原則として付与されたＩＤのみを利用し、他者と共有してはならない。パスワードが他人に漏れないように運用しなければならない。

(2) アクセス制御
情報システムは、電子情報の登録、参照、変更、削除に関して、正当な権限保持者が正当な手段を利用してのみ実行できるように構築、運用されなければならない。

(3) 暗号化
情報資産は情報種別に応じて、アクセス権限を持つ者以外には解読、改ざんできないように暗号化を行う等対策を講じなければならない。また、暗号及び復号の際に用いる鍵の管理には管理者を置き、適切に運用されなければならない。

(4) ネットワーク構築
本プロジェクトにおけるネットワークの構築運用に際しては、情報種別によって専用回線の敷設、暗号化の処理等、第三者に情報資産が漏洩しないための予防策を講じなければならない。
特に、情報種別レベル 2 及びレベル 3 の情報は、プロジェクト外部のネットワークにおいて、暗号化せずに取り扱ってはならない。

(5) ウィルス対策
情報システム管理者は、情報システムで利用される全ての機器に対し、コンピュータウィルス（以下「ウィルス」とする。）対策を可能な限り実施しなければならない。また、ウィルスの感染予防、発見、駆除及び、情報システムの原状復帰等に関する指示を行なわなければならない。

(6) データ保護
情報システムは、セキュリティ侵害が発生した際、すみやかに復旧できるように、バックアップを取ることができるよう構築、運用されなければならない。また、バックアップ記録を保存した媒体等は適切に保管されなければならない。

(7) 誤動作防止
情報システムには、可能な限りプロジェクト関係者の過失による誤操作を防ぐ仕組みを備えなければならない。

(8) 操作履歴の取得
情報システムは、必要な操作履歴を一定期間残し、それらの完全性を保たれなければならない。

(9) 停電対策
情報システムは、無停電電源装置を用いるなどして可能な限り停電、瞬断等の影響を受けないような対策を講じなければならない。

(10) 盗難防止
情報システムは、端末の不正持ち出しや、システムへの不正アクセスによるデータの不正利用を防ぐため、必要に応じて物理的（ハードウェア）もしくは論理的（ソフトウェア）対策を講じなければならない。

3.3.2. 情報システムの管理

情報システムは､以下の点に留意して動作確認時も含めて適切に管理されなければならない。

(1) ユーザー管理
情報システム管理者は、業務遂行のため情報システムの利用が必要なプロジェクト関係者に対して、必要とする期間及び範囲の情報システムの利用を許諾し、また、定期的に利用の記録を監視、分析しなければならない。

(2) ネットワーク管理
本プロジェクトにおけるネットワークの運用に際しては、ネットワーク管理者等を置き、不正アクセス、情報漏洩、故障等による情報セキュリティの侵害を未然に防止し、業務の効率的かつ安全な遂行に資するように適切に管理しなければならない。

(3) システム管理
- 本プロジェクトに関する情報システムは、各組織にてシステム管理者を選定し、マニュアル整備等を行うことで積極的に情報システムのセキュリティレベルと安定した稼働の維持に努めなければならない。

- システム自体を管理する者と、システム内部で取り扱うデータを管理する者の権限を分散させるため、必要に応じてデータ管理者を選定しなければならない。特に統合臨床データベース管理部、データ管理バンクにおいては、システム管理者とデータ管理者を兼任しないよう、それぞれの管理者を個別に選定しなければならない。
- システムメンテナンスの外部への委託は、機密保持契約を締結した組織でなければならない。その際は、情報システム管理者の監督の下に行われなければならない。

3.4. 情報保護施設に関するセキュリティ対策

情報保護施設に起因するセキュリティ侵害には、プロジェクト関係者や外部の者の侵入による情報資産の盗難や、自然災害等による情報保護施設及び情報資産の損壊等がある。これらを防ぐために地震、火災、停電等に対処できる施設にて、以下の対策を行わなければならない。

3.4.1. セキュリティ環境の整備

情報資産の保管場所及び情報システム関連設備の設置場所は、専用部屋を用意する、又は入退室管理を行える仕組みを設けるなど、情報種別に基づいて物理的に制限された環境を整備しなければならない。

3.4.2. 施設管理

情報資産の保管場所及び情報システム関連設備を収容する場所については、必要に応じて管理者を置く。また、その利用に際しては可能な限り履歴を残さなければならない。管理者は、利用履歴の定期的な確認を行わなければならない。

4. セキュリティ侵害への対応策

4.1. 初動措置

プロジェクト参加機関は、セキュリティ侵害の発生を把握したときは、直ちにセキュリティ侵害の内容、発生場所、発生時間、発見者、具体的状況、必要な対応の判断、意見等をプロジェクト事務局に報告して必要な指示を仰ぐとともに、早急に応急措置実施体制を確立しなければならない。なお、セキュリティ侵害が発生した組織で容易に対処できるものについては、所定の方法で対処をした後、プロジェクト事務局に詳細を報告しなければならない。

4.2. 暫定措置

4.2.1. 対策の決定

プロジェクト事務局は、プロジェクト参加機関からセキュリティ侵害発生の連絡を受けた際、発生場所、発生時間、発見者、具体的状況を把握し、プロジェクトリーダーに必要な対応の判断を仰ぎ、セキュリティ侵害のレベルを判断する。

提供者に不利益を与えるなど、セキュリティ侵害のレベルが大きく、プロジェクト事務局で対応できないと判断した場合は推進委員会委員長に報告すると共に、緊急対策委員会を召集し、他の関連組織と共に対策を検討しなければならない。また、セキュリティ侵害のレベルに応じて、他の関連組織へ報告しなければならない。

対策を決定する組織は、セキュリティ侵害発生の連絡を受けた後、早急に対策を決定し、セキュリティ侵害が発生した組織に指示を出さなければならない。

4.2.2. 対策の実施

セキュリティ侵害が発生した組織は、対策を決定する組織から指示を受け、必要な措置を取った後、プロジェクト事務局に実施した内容についての詳細を報告しなければならない。

4.2.3. 報告、周知

セキュリティ侵害への対策の実施後、プロジェクト事務局は詳細をセキュリティ侵害のレベルに応じて、推進委員会と実施会議に報告しなければならない。また、同様のセキュリティ侵害が他のプロジェクト参加機関においても発生する恐れのある場合は、必要に応じてセキュリティ侵害の発生内容及び対処法を他のプロジェクト参加機関へ周知し、再発防止を呼びかけなければならない。

4.3. 恒久措置

セキュリティ侵害が発生した場合、プロジェクト事務局は報告を元に、セキュリティ侵害が発生した組織と共に改善策を検討しなければならない。改善策に対し、その後、必要に応じて実施会議は本文書及び関連文書の見直し及び、改定作業を行う。

5. 監査

プロジェクト参加機関は、実施会議の指示のもと、プロジェクト事務局が実施する情報セキュリティに関する監査を受けなければならない。

プロジェクト事務局は、監査結果を実施会議に報告し、実施会議より改善要請を受けた被監査機関は、是正状況を実施会議に報告しなければならない。また、被監査機関は、円滑に監査が実施できるように協力しなければならない。

なお、プロジェクト事務局が実施する監査以外に、ELSI 委員会等による監査が実施される場合がある。

監査において以下の点を注意しなければならない。

- プロジェクト事務局は必要と認められる方法により定期監査ならびに抜打ち監査を実施し、プロジェクト参加機関が本文書、関連法令、倫理指針を遵守しているかどうか運用実態を把握、評価し、実施会議に報告しなければならない。
- プロジェクト事務局は監査の際、被監査機関と機密保持契約を結び、公正不偏の態度で監査を行う。
- 改善の要請を受けた被監査機関は、速やかに改善措置を行わなければならない。
- 監査実施機関は、監査により知り得た情報を正当な理由なく漏らしてはならない。その職を辞した後も同様である。

6. 遵守義務及び罰則

適用範囲で規定したすべての者は、本文書、関連法令、倫理指針の遵守を義務づけるものとする。

プロジェクト関係者及びプロジェクト参加機関が、遵守義務に反する行為を行った場合は、実施会議等やその他各組織に定められた規定により罰則について検討される場合がある。

7. 関連ドキュメントの作成

プロジェクト事務局は、本文書に基づき、具体的な情報セキュリティ保護に関する遵守事項を定めた実施要領等のドキュメントを作成する。

プロジェクト参加機関はこれらの文書に基づき、組織内の業務に則したより具体的なマニュアルなどを作成し、プロジェクト関係者に対して情報セキュリティ保護に関する教育、啓発を行わなければならない。

8. 本文書の評価、改定

- 実施会議は、随時または定期的（年一回を目途）に本文書の妥当性について継続的に点検、評価する。
- 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しなければならない。
- 本文書の評価結果と改定内容については、推進委員会で審議し承認を受けてから施行することを原則とする。

改版履歴

2004 年 3 月 2 日 第 1 版発行

変更点

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			
3			
4			
5			

個人の遺伝情報に応じた医療の実現プロジェクト
情報セキュリティ標準 第 2 版

承認　　：推進委員会
作成　　：実施会議
問合せ先 ：プロジェクト事務局