ELSI2101 ヒト幹細胞関連情報の基盤システム運用・管理規程

第一章　総則

（趣旨）

第一条　この規程は、ヒト幹細胞関連情報の基盤システム運用基本規程第五条第二項第二号に基づき、「ヒト幹細胞を用いた再生医療の臨床実用化のための基盤構築に関する研究」に関するプロジェクト（以下「本プロジェクト」という。）におけるヒト幹細胞関連情報の基幹システム及び拠点追加機器を含めた基盤システムの運用及び管理について必要な事項を定めるものとする。

（定義）

第二条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　運用基本方針　本プロジェクトが定める「ELSI1000　ヒト幹細胞関連情報の基盤システム運用基本方針」をいう。

二　運用基本規程　本プロジェクトが定める「ELSI1001　ヒト幹細胞関連情報の基盤システム運用基本規程」をいう。

三　利用者等　利用者、臨時利用者のほか、基盤システムを取り扱う者をいう。基盤システムを取り扱う者には、基盤システムを運用・管理するだけでなく、基盤システムに係る情報を作成・利用する者も含まれる。

四　電子計算機　コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。

五　端末　利用者等が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆるPCのほか、スマートフォン、タブレット端末、デジタルペン等も該当する。

六　通信回線　これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みであり、物理的なものと論理的なものがある。

七　通信回線装置　回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるハブ及びルータ、スイッチ、ファイアウォールのほか、光回線終端装置、情報コンセントや無線ネットワークアクセスポイント等も該当する。

八　プロジェクト通信回線　物理的な通信回線を構成する回線（及び通信回線装置を問わず、基幹システムの一部として構成される論理的な通信回線をいう。

九　プロジェクト外通信回線　プロジェクト通信回線以外の論理的な通信回線をいう。

十　情報取扱区域　本プロジェクトの内外において情報を取り扱う区域をいう。情報取扱区域のうち、求める対策の基準ごとに「クラス」の区分を定める。情報取扱区域におけるクラス及びクラスにおける区分の基準は、それぞれ以下のとおりとする。

クラス	区分の基準
クラス３	クラス２より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域
クラス２	クラス１より強固な情報セキュリティを確保するための管理

	対策及び利用制限対策を実施する必要がある区域
クラス１	最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域
クラス０	クラス３、クラス２及びクラス１以外の区域であり、情報セキュリティを確保するため、利用制限対策を実施する必要がある区域

十一　要管理対策区域　施設及び環境に係る管理対策が講じられている区域であって、情報取扱区域におけるクラス１以上の区域をいう。

十四　要管理対策区域外　情報取扱区域におけるクラス０の区域をいう。

〇〇　教育研究事務　本プロジェクトに係る教育、研究業務、基盤システムの運用管理及びそれらに付随する業務をいう。

十五　要管理対策区域外での情報処理　利用者等が情報取扱区域におけるクラス０の区域において教育研究事務の遂行のための情報処理を行うことをいう。なお、オンラインで本プロジェクトに参加する各大学、研究機関の拠点以外から基盤システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。

十六　機密性　情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。機密性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
機密性３情報	本プロジェクトで取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性２情報	本プロジェクトで取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、利用者等の権利が侵害され又は本プロジェクトの教育研究事務の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

十七　完全性　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をいう。完全性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
完全性２情報	本プロジェクトで取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者等の権利が侵害され又は本プロジェクトの教育研究事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

十八　可用性　情報及び関連資産へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。可用性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
可用性２情報	本プロジェクトで取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用

	者等の権利が侵害され又は本プロジェクトの教育研究事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

十九　要機密情報　機密性２情報及び機密性３情報をいう。

二十　要保全情報　完全性２情報をいう。

二十一　要安定情報　可用性２情報をいう。

二十二　要保護情報　要機密情報、要保全情報及び要安定情報をいう。

二十三　取扱制限　情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄等その他情報の適正な取扱いを確実にするための手段をいう。

二十四　例外措置　利用者等がポリシー並びにそれに基づく規程及び手順等を遵守することが困難な状況で、教育研究事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

二十五　情報の移送　要管理対策区域外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。

二十六　情報の抹消　廃棄した情報が漏えいすることを防止するために、全ての情報を復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態ではない。

二十七　主体　原則として、基盤システムの利用者等を指す。が、基盤システムにアクセスする主体として、複数の情報システムや装置が連動して動作する場合には、他の情報システムや装置も含めるものとする。

二十八　主体認証　識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、基盤システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、この規程における「主体認証」については、公的又は第三者による証明に限るものではない。

二十九　識別　基盤システムにアクセスする主体を特定することをいう。

三十　識別コード　主体を識別するために、基盤システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

三十一　主体認証情報　主体認証をするために、主体が基盤システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

三十二　主体認証情報格納装置　主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、基盤システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

三十三　共用識別コード　複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、基盤システム上の制約や、利用状況等を考慮して、１つの識別コードを複数の主体で共用する場合もある。

このように共用される識別コードを共用識別コードという。組織に貸与され共有で使用するユーザ ID 等がこれに当たる。

三十四　アクセス制御　主体によるアクセスを資格と必要性に基づいて制限することをいう。

三十五　権限管理　主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

三十六　アカウント　主体認証を行う必要がある基盤システムにおいて、主体に付与された正当な権限をいう。アカウントの付与は、主体認証情報（識別コードと主体認証情報を含む。）の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

三十七　最少特権機能　管理者権限を実行できる範囲を管理作業に必要な最少の範囲に制限する機能をいう。

三十八　不正プログラム　コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。

三十九　不正プログラム定義ファイル　アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。

四十　その他の用語の定義は、運用基本規程の定めるところによる。

（適用範囲）

第三条　この規程は、基盤システムを運用・管理する者に適用する。

第二章　導入

第一節　組織・体制

（組織・体制）

第四条　基盤システムの運用・管理は、運用基本方針及び運用基本規程に従い、総括責任者、実施責任者、技術責任者、情報セキュリティアドバイザー等の審議を経て、総括責任者が執り行うものとする。

（基盤システム利用の責任者の設置）

第五条　運用基本規程第十一条に基づき、各拠点に基盤システム利用の責任者を設置する。

２　利用の責任者は、管理組織における情報セキュリティ対策に関する事項全般を統括すること。

３　研究分担者は、基盤システム利用の責任者を置いた時及び変更した時は、実施責任者にその旨を報告すること。

４　実施責任者は、基盤システム利用の責任者に対する連絡網を整備すること。

（禁止事項）

第七条　本プロジェクトを組織するすべての者は、次に掲げる事項を行ってはならない。

一　情報資産の目的外利用

二　守秘義務に違反する情報の開示
三　総括責任者の許可なく通信回線上を送受信される通信内容を監視し、又は通信回線装置及び電子計算機の利用記録を採取する行為
四　法令又は本プロジェクトの諸規則に違反する情報の発信
五　管理者権限を濫用する行為
六　上記の行為を助長する行為

第二節　違反と例外措置

（違反への対処）
第八条　利用者等は、情報セキュリティ関係規程への重大な違反を知った場合には、総括責任者にその旨を報告すること。
2　総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせること。
3　総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、総括責任者は実施責任者、技術責任者、情報セキュリティアドバイザー等のもと協議・審議を行い、その結果を ELSI 委員会及び報告が必要と判断する組織に報告すること。なお、拠点における重大な違反の場合における協議・審議には、拠点の研究分担者や基盤システム利用の責任者を含めて行うこと。

（違反に対する措置）
第九条　総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認すること。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取すること。
2　総括責任者は、調査によって違反行為が判明したときには、次号に掲げる措置を講ずることができる。
一　当該行為者に対する当該行為の中止命令
二　技術責任者およびＩＴ担当者に対する当該行為に係る情報発信の遮断命令
三　技術責任者およびＩＴ担当社に対する当該行為者のアカウント停止命令、または削除命令
四　その他法令に基づく措置
3　総括責任者は、前項第二号及び第三号については、拠点の研究分担者を通じて同等の措置を依頼することができる。

（例外措置）
第十条　総括責任者は、例外措置の適用の審査手続を整備すること。申請を審査する者（以下本条において「許可権限者」という。）は、総括責任者または総括責任者が指名した者とする。
2　利用者等は、例外措置の適用を希望する場合には、本プロジェクトが定める審査手続に従い、許可権限者に例外措置の適用を申請すること。ただし、教育研究事務の遂行に緊急を要する等の場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又

は規定されている方法を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。利用者等は、申請の際には申請理由、例外措置の内容等をを明確にすること。

3　許可権限者は、利用者等による例外措置の適用の申請を、本プロジェクトが定める審査手続に従って審査し、許可の可否を決定すること。また、決定の際には、審査者、申請内容、審査結果を含む適用審査記録を作成し、総括責任者に報告すること。

4　利用者等は、許可を受けた例外措置が終了した時に、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

5　許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な措置を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

6　総括責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずること。

第三章　運用

第一節　情報セキュリティ対策の教育

（情報セキュリティ対策の教育）

第十一条　実施責任者は、情報セキュリティ関係規程について、技術責任者、技術責任者が指名する担当者、プロジェクト支援チームのスタッフ、また必要に応じて本プロジェクトに参加する組織の研究分担者や IT 担当者等の利用者等（以下「教育啓発対象者」という。）に対し、その啓発をすること。

2　実施責任者は、情報セキュリティ関係規程について、教育啓発対象者の役割に応じて教育・訓練すべき内容を検討し、企画・立案し、定期的に教育・訓練を実施する。必要に応じて、外部の講習会等への参加考慮すること。

3　実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況について、総括責任者に報告すること。

4　総括責任者は、ELSI 委員会に対して、教育啓発対象者に対する情報セキュリティ教育の実施状況を定期的に報告すること。報告には、実施時期、教育内容、参加した者または組織を含めること。

二節　インシデント対応

（インシデントの発生に備えた事前準備）

第十四条　総括責任者は、情報セキュリティに関するインシデント（障害・事故等を含む。以下「インシデント」という。）の発生に対応するために、以下の役割及び機能を有する体制を整備すること。

一　インシデントに対応する責任者の決定

二　インシデントの発生の報告

三　インシデントの発生報告の受付

四　関係する組織へのインシデントの発生に関する速やかな連絡
五　応急措置の実施（被害の拡大防止）
六　インシデントからの復旧
七　原因調査の実施
八　再発防止策の策定及び実施
九　再発防止策の実施の確認

2　実施責任者は、インシデントについて報告手順を整備し、当該報告手段を全ての利用者等に周知すること。周知に当たっては次の方法を含めて検討し、緊急時に利用者等がすぐに行動に移れるようにすること。
一　定期的な教育・訓練
二　報告の手順を明記した文書の配布
三　利用者等の執務室や研究室への掲示

3　実施責任者は、インシデントが発生した際の本プロジェクト内外との情報共有を含む対処手順を整備すること。本プロジェクト外とは、基幹システムの保守、管理業務の委託先、本プロジェクトに参加する研究室等が所属する研究機関、医療施設、大学法人等を指す。

4　実施責任者は、インシデントに備え、教育研究事務の遂行のため、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。緊急連絡網には、総括責任者、実施責任者、技術責任者、プロジェクト支援スタッフの他、採用している外部サービスの提供事業者、基幹システムの保守、管理業務の委託先、監督官庁等を含める。

5　実施責任者は、インシデントへの対処の訓練の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。訓練体制には、必要に応じて基幹システムの保守、管理業務の委託先などの外部事業者、また外部の専門家の参加を考慮すること。

6　利用者等は、インシデントへの対処の訓練に関する規定が定められている場合には、当該規定に従って、インシデントへの対処の訓練に参加すること。

7　実施責任者は、インシデントについて本プロジェクト外から報告を受けるための窓口を設置し、その窓口への連絡手段を公表すること。

（インシデントの発生時における報告と対処の流れ）

第十五条　利用者等は、インシデントの発生を知った場合には、それに関係する者に連絡するとともに、実施責任者が定めた報告手順により、インシデントに対応する責任者、及びインシデントに対応する責任者を通じて総括責任者にその旨を報告すること。ただし、緊急やむを得ない事情により、インシデントに対応する責任者に報告することができない場合は、定められた報告手順に従って、総括責任者に報告すること。

2　インシデントに対応する責任者は、被害の拡大防止等を図るための応急措置の実施及びインシデントからの復旧に係る指示又は勧告を行うこと。

3　利用者等は、インシデントが発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

4　利用者等は、インシデントが発生した場合であって、当該インシデントについて対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、インシデントによる被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

５　総括責任者は、報告を受けたインシデントについて、定められた対処手順に従って、本プロジェクト内外の関係部門と情報共有を行うこと。

（インシデントの原因調査と再発防止策）
第十六条　実施責任者は、インシデントが発生した場合には、インシデントに対応する責任者が実施した内容も踏まえ、インシデントの原因を調査するとともに再発防止策を策定し、その結果を報告書として総括責任者に報告すること。
２　総括責任者は、実施責任者からインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。

（インシデントの発生するおそれがある場合の対処）
第十七条　総括責任者、実施責任者、技術責任者又はインシデントに対応する責任者は、インシデントの発生するおそれがある場合においては、この章の各遵守事項に準じて、必要な措置を講ずること。
２　利用者等は、インシデントの発生するおそれがある場合においては、第十四条の規定による報告手順や対処手順等に基づき、適切な措置を講ずること。

第四章　評価

第一節　情報セキュリティ対策の自己点検

（自己点検に関する計画の策定）
第十八条　実施責任者は、自己点検計画を策定し、総括責任者の承認を得ること。自己点検は、その実施時期を決め、定期的に実施されるように計画すること。

（自己点検の実施に関する準備）
第十九条　実施責任者は、自己点検票及び自己点検の実施手順を整備すること。自己点検は、本プロジェクトの基幹システムの保守、運用を担当する組織および本プロジェクトに参加する組織を対象とする。

（自己点検の実施）
第二十条　実施責任者は、自己点検計画に基づき、各組織に対して、自己点検の実施を指示すること。
２　各組織は、実施責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施すること。

（自己点検結果の評価）
第二十一条　総括責任者は、各組織による自己点検が行われていることを確認し、その結果を評価すること。

２　プロジェクト支援チームは、自己点検の結果を取りまとめ、総括責任者へ報告すること。

（自己点検に基づく改善）

第二十二条　各組織は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、実施責任者にその旨を報告すること。

２　総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には実施責任者に改善を指示すること。

第二節　情報セキュリティ対策の監査

（監査計画の策定）

第二十三条　総括責任者は、情報セキュリティ監査責任者に対して、定期的に監査が実施されるよう、監査計画の立案及び監査の実施を指示すること。

２　総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合は、都度情報セキュリティ監査責任者に対して監査の実施を指示すること。

（監査の実施に関する指示）

第二十四条　情報セキュリティ監査責任者は、総括責任者の指示に基づき監査計画を策定し、総括責任者の承認を得ること。なお、監査計画には、次の事項を含めること。

一　重点とする監査対象及び監査目標（情報漏えい防止、不正アクセス防止等）

二　監査実施期間

三　監査業務の管理体制

四　外部委託による監査の必要性及び範囲

五　監査予算

六　過去の監査結果で明らかになった課題及び問題点の改善状況

（個別の監査業務における監査実施計画の策定）

第二十五条　情報セキュリティ監査責任者は、監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定すること。監査実施計画には次の事項を含めること。

一　監査の実施時期

二　監査の実施場所

三　監査実施者及び担当職務の割当て

四　準拠性監査（情報セキュリティ関係規程に準拠した手続が実施されていることを確認する監査）のほか、必要に応じて妥当性監査（実施している手続が有効な情報セキュリティ対策であることを確認する監査）を行うかについての方針

五　実施すべき監査の概要（監査要点、実施すべき監査の種類及び試査の範囲を含む。）

六　監査の進捗管理手段又は体制

（監査の実施に係る準備）

第二十六条　情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

2　情報セキュリティ監査責任者は、情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、外部の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、外部の者に監査の一部を請け負わせること。その場合、情報セキュリティ監査企業台帳に登録されている事業者や情報セキュリティ監査人資格者の監査業務への関与を考慮すること。

（監査の実施）

第二十七条　情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施すること。

2　情報セキュリティ監査実施者は、情報セキュリティ関係規程がポリシーに準拠していることを確認すること。

3　情報セキュリティ監査実施者は、基盤システム及び取り扱う情報の管理、運用に係る手順が情報セキュリティ関係規程に準拠していることを確認すること。

4　情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していることを次の事項を含めて確認すること。

一　自己点検結果に基づく担当者への質問、記録文書の査閲、機器の設定状況の点検等の方法により、運用の準拠性の確認

二　必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かの妥当性の確認

5　情報セキュリティ監査実施者は、監査の実施記録として監査調書を作成すること。

6　情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、総括責任者へ提出すること。監査報告書には、遵守内容の妥当性に関連して改善すべき課題及び問題点等の検出事項を含めるだけでなく、検出事項対する改善への助言や提案を含めることが望ましい。

（監査結果に対する対処）

第二十八条　総括責任者は、監査報告書の内容を踏まえ、被監査部門の責任者に対して、指摘されたことに対する対処の実施を指示すること。

3　実施責任者は、監査報告書等に基づいて総括責任者から改善を指示されたことについて、対処計画を策定し、報告すること。対処計画が本プロジェクトに参加する組織の管理、運用に大きく依存する場合は、当該組織に対して対処計画の作成を指示し、対処計画について報告を求めること。

4　総括責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。

（監査への協力）

第二十九条　被監査部門となる組織やその他の関係者は、情報セキュリティ監査責任者の行う監

査の適正かつ円滑な実施に協力すること。

第五章　見直し

第一節　情報セキュリティ対策の見直し

（情報セキュリティ対策の見直し）

第三十条　情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、利用者等の本プロジェクトの関係者すべてに周知を図ること。

２　利用者等は、情報セキュリティ関係規程に課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談すること。

３　情報セキュリティ関係規程を整備した者は、情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合は、その是非を検討し、情報セキュリティ関係規程の見直しや、逆に利用者等の理解不足が原因であると思料する場合は、再教育や再周知等の必要な措置を講ずること。

第六章　その他

第一節　外部委託

（役務の適用範囲）

第三十一条　この章の規定は、本プロジェクトによる貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次の各号に掲げる営業品目に該当するものに適用する。

一　ソフトウェア開発（プログラム作成、システム開発等）

二　情報処理（統計、集計、データエントリー、媒体変換等）

三　賃貸借

四　調査・研究（調査、研究、検査等）

五　基盤システムの運用管理、保守

六　保管（紙媒体、外部記憶媒体、データ等の保管）

（情報セキュリティ確保のための共通の仕組みの整備）

第三十二条　実施責任者は、外部委託の対象としてよい基盤システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。

２　委託先の選定基準及び選定手続は、原則、本プロジェクトの中核機関が属する組織の定めにに基づく。

３　総括責任者は、本プロジェクトの中核機関が属する組織が定める委託先の選定基準要件の適用が妥当でないと判断した場合は、個別にまたは当該選定基準の要件見直しを行うこと。

４　本プロジェクトの目的、特性から、原則、委託先は国内事業者とし、かつ委託する業務や扱

う情報について国内法が適用される場所に制限できるようにすること。

（委託先に実施させる情報セキュリティ対策の明確化）第三十三条　技術責任者は、外部委託に係る業務遂行に際して次の事項を委託先候補に事前に周知すること。

一　情報セキュリティ対策の内容

二　情報セキュリティが侵害された場合の対処方法

三　情報セキュリティ対策の履行状況を確認するための方法及び履行が不十分である場合の対処方法。

（委託先の選定）

第三十四条　技術責任者は、本プロジェクトの中核機関が属する組織が定める委託先の選定基準及び選定手続に基づき、委託先を選定すること。ただし、三十三条第三項に該当する場合は、個別にまたは見直された当該選定基準要件に従って委託先を選定すること。

（外部委託に係る契約）

第三十五条　委託先との契約においては、原則、本プロジェクトの中核機関が属する組織の定めに基づき契約を取り交わすこと。

２　総括責任者は、本プロジェクトの中核機関が属する組織が定める契約内容の適用が妥当でないと判断した場合は、契約内容の見直しを行ったうえで、契約の取り交わしを行うこと。

（外部委託の実施における手続）

第三十六条　委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。

一　委託先に情報を提供する場合は、安全な受渡し方法によりこれを実施し、提供した記録を取得すること。

二　外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消（全ての情報を復元が困難な状態にすることをいう。以下同じ。）させること。

２　技術責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、取り交わした契約の対処方法に従い、委託先に必要な措置を講じさせること。

３　技術責任者は、取り交わした契約の対処方法に従い、委託先における情報セキュリティ対策の履行状況を確認すること。

（外部委託終了の手続）

第三十七条　技術責任者は、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認すること。

第二節　業務継続計画及び基幹システム運用継続計画との整合的運用の確保

（業務継続計画及び基幹システム運用継続計画と情報セキュリティ対策との間の整合性の確保）
第三十八条　統括責任者は、本プロジェクトにおいて基幹システムの稼動を損なう地震及び風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、並びに情報機器の故障等を踏まえ、業務継続計画、基幹システム運用継続計画又は情報セキュリティ関係規程を整備する場合には、業務継続計画及び基幹システム運用継続計画と情報セキュリティ関係規程との間の整合性の確保のための検討を実施責任者、技術責任者に指示すること。
２　実施責任者、技術責任者は、本プロジェクトにおいて業務継続計画及び基幹システム運用継続計画を整備する場合には、基幹システムについて、当該業務継続計画及び基幹システム運用継続計画との関係の有無を検討すること。
３　実施責任者、技術責任者は、本プロジェクトにおいて業務継続計画及び基幹システム運用継続計画を整備する場合には、業務継続計画及び基幹システム運用継続計画との整合性を考慮し、必要な措置を講ずること。
一　通常時において業務継続計画及び基幹システム運用継続計画と情報セキュリティ関係規程との整合的運用が可能となるよう必要な措置を講ずること。
二　事態発生時において業務継続計画、基幹システム運用継続計画及び基幹セキュリティ関係規程との整合的運用が可能となるよう、基幹システムの稼働水準、復旧までの所要時間の目標を定め、その達成を図る様々な対応の具体的な実施手順の整備等の必要な措置を講ずること。

（業務継続計画及び基幹システム運用継続計画と情報セキュリティ関係規程との間の不整合の報告）
第三十九条　利用者等は、本プロジェクトにおいて業務継続計画及び基幹システム運用継続計画を整備する場合であって、業務継続計画、基幹システム運用継続計画及び情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、インシデントが発生した際の報告手順により、実施責任者にその旨を報告して、指示を得ること。

第三節　情報取扱区域

（情報取扱区域のクラス、管理及び利用制限の決定）第四十条　実施責任者は、情報取扱区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限対策を決定すること。なお、決定する内容は、別途定める。
２　実施責任者は、要管理対策区域については、当該区域を管理又は利用する利用者等がクラスについて認識できる措置を講ずること。本プロジェクトに参加する組織に対して、各組織の研究分担者に処置を講じる旨要請すること。
３　各研究分担者は、自組織の拠点における個別の管理対策及び利用制限対策を決定する必要性の有無を検討し、必要と認めた場合は、当該対策を決定し、実施責任者に報告すること。

（情報取扱区域の管理）
第四十一条　実施責任者、各研究分担者は、要管理対策区域を管理する場合には、当該区域のク

ラスを確認し、別途定める管理対策を講ずること。また、個別の管理対策を決定している場合には、同様に対策を講ずること。

（情報取扱区域における利用制限）
第四十二条　実施責任者、研究分担者は、情報取扱区域のクラスを確認し、別途定める利用制限対策を講ずること。なお、個別に利用制限対策を決定している場合には、同様に講ずること。
２　利用者等は、情報を取り扱う場合には、情報取扱区域のクラスを確認し、別途定める利用制限対策に従って利用すること。なお、個別の利用制限対策を決定している場合には、同様に従うこと。

第七章　情報の取扱い

第一節　情報の作成と入手

（教育研究事務以外の情報の作成又は入手）
第四十三条　利用者等は、教育研究事務の遂行以外の目的で、情報を作成し、又は入手しないよう努めること。

（情報の作成又は入手時における格付と取扱制限の決定）
第四十四条　利用者等は、情報の作成時及び他の利用者等、また本プロジェクト外の者が作成した情報を入手したことに伴う管理の開始時に格付及び取扱制限の定義に基づき、格付及び取扱制限を決定すること。
２　利用者等は、元の情報の修正、追加、削除のいずれかにより、他の利用者等が決定した情報の格付及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。

（格付と取扱制限の明示等）
第四十五条　利用者等は、情報の格付及び取扱制限を決定（再決定を含む。以下同じ。）した際に、当該情報の参照が許されている者が認識できる方法を用いて明示等すること。

（格付と取扱制限の加工時における継承）
第四十六条　利用者等は、情報を作成する際に、参照した情報又は入手した情報が既に格付又は取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

第二節　情報の利用

（教育研究事務以外の利用）第四十七条　利用者等は、教育研究事務の遂行以外の目的で、情報を利用しないよう努めること。

（格付及び取扱制限に従った情報の取扱い）

第四十八条　利用者等は、利用する情報に明示等された格付に従って、当該情報を適切に取り扱うこと。格付に加えて取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。

（格付及び取扱制限の複製時における継承）
第四十九条　利用者等は、情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

（格付及び取扱制限の見直し）
第五十条　利用者等は、情報を利用する場合に、元の格付又は取扱制限がその時点で不適切と考えるため、他の利用者等が決定した情報の格付又は取扱制限そのものを見直す必要があると思料する場合には、その決定者（決定について引き継いだ者を含む。）または決定者が属する組織の責任者（以下この条において「決定者等」という。）に相談すること。
２　利用者等は、自らが格付及び取扱制限の決定者等である情報に対して、見直しの必要があると認めた場合には、当該情報の格付又は取扱制限を再決定し、それを明示等すること。また、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知すること。

（要保護情報の取扱い）第五十一条　利用者等は、教育研究事務の遂行以外の目的で、要保護情報を要管理対策区域外に持ち出さないこと。
２　利用者等は、要保護情報を放置しないこと。
３　利用者等は、機密性３情報を必要以上に複製しないこと。
４　利用者等は、要機密情報を必要以上に配付しないこと。
５　利用者等は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。
６　利用者等は、情報を機密性３情報と決定した書面のうち、必要なものには、一連番号を付し、その所在を明らかにしておくこと。

第三節　情報の保存

（格付に応じた情報の保存）
第五十二条　利用者等は、情報の格付及び取扱制限に応じて、基幹システム及び本プロジェクトが許可したシステムに本プロジェクトが指定する方法に従って、情報を適切に保存すること。
２　利用者等は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。
３　利用者等は、要機密情報を電磁的記録媒体に保存する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。
４　利用者等は、要機密情報を電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
５　利用者等は、要保全情報を電磁的記録媒体に保存する場合には、電子署名の付与を行う必要

性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

6　利用者等は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。バックアップ又は複写した情報は、紛失、盗難、不正アクセス等から保護する為、アクセス制限や暗号化等の対策を講じること。

7　利用者等等は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、遠隔地保管を行うなどの適切な措置を講ずること。

（情報の保存期間）

第五十三条　利用者等は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

第四節　情報の移送

（情報の移送に関する許可及び届出）

第五十四条　利用者等は、機密性３情報、完全性２情報又は可用性２情報を移送する場合には、実施責任者の許可を得ること。本プロジェクトに参加する各拠点の組織の場合は当該組織の研究分担者の許可を得ること。

2　利用者等は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面を移送する場合には、実施責任者に届け出ること。本プロジェクトに参加する各拠点の組織の場合は当該組織の研究分担者に届け出ること。ただし、実施責任者、又は研究分担者が届出を要しないと定めた移送については、この限りでない。

（情報の送信と運搬の選択）

第五十五条　利用者等は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、実施責任者に届け出ること。本プロジェクトに参加する各拠点の組織の場合は当該組織の研究分担者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録の移送であり、実施責任者、又は研究分担者が届出を要しないと定めた移送については、この限りでない。

（移送手段の決定）

第五十六条　利用者等は、要保護情報を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、実施責任者に届け出ること。本プロジェクトに参加する各拠点の組織の場合は研究分担者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面の移送であり、実施責任者、又は研究分担者が届出を要しないと定めた移送については、この限りでない。

（記録媒体の保護対策）

第五十七条　利用者等は、要機密情報が記録又は記載された記録媒体を運搬する場合には、情報の格付及び取扱制限に応じて、外見ではその内容が要機密情報であると知られないこと、「親展」の指定を行うこと、専用ケースに格納して施錠すること等、安全確保のための適切な措置を講ずること。

（電磁的記録の保護対策）第五十八条　利用者等は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。

2　利用者等は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

3　利用者等は、要保全情報である電磁的記録を移送する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

4　利用者等は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めたときは、情報のバックアップを取得すること。

5　利用者等は、要安定情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送する等の措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

6　利用者等は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、秘密分散技術（複数の情報に分割してそれぞれ異なる移送経路を用いて移送する技術の必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

第五節　情報の提供

（情報の公表）

第五十九条　利用者等は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

2　利用者等は、電磁的記録を公表する場合には、予め当該情報の当該情報文書ファイルのプロパティ情報や作成履歴などの付加情報等を除去、また特定の部分の情報を削除又は置き換えるなどの措置を講じるなど、不用意な情報漏えいを防止するための措置を講ずること。

（他者への情報の提供）

第六十条　利用者等は、機密性３情報、完全性２情報又は可用性２情報を本プロジェクト外の者に提供する場合には、実施責任者の許可を得ること。

2　利用者等は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報である書面を本プロジェクト外の者に提供する場合には、実施責任者に届け出ること。本プロジェクトに参加する各拠点の組織の場合は当該組織の研究分担者に届け出ること。ただし、実施責任者、又は研究分担者が届出を要しないと定めた提供については、この限りでない。

3　利用者等は、要保護情報を本プロジェクト外の者に提供する場合には、提供先において、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるように、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定するなどの措置を講ずること。

4　利用者等は、電磁的記録を提供する場合には、予め当該記録の当該情報文書ファイルのプロパティ情報や作成履歴などの付加情報等を除去、また特定の部分の情報を削除又は置き換えるなどの措置を講じるなど、不用意な情報漏えいを防止するための措置を講ずること。

第〇節　本プロジェクトにおける実験、研究データの共有・公開

（『厚労省科研費「ヒト幹細胞を用いた再生医療の臨床実用化のための基盤構築に関する研究」データ共有・公開に関するルール』の適用）

第〇〇条　本プロジェクトに参加する利用者等は、本プロジェクトの実験、研究の目的で共有・公開を行うデータは、本規程の定めに従うことを原則とするが、本プロジェクトに参加する組織間で了解されるべき基本的な合意事項である『厚労省科研費「ヒト幹細胞を用いた再生医療の臨床実用化のための基盤構築に関する研究」データ共有・公開に関するルール』に定めがあり、それに該当する場合は、当該ルールが優先する。

第六節　情報の消去

（電磁的記録の消去方法）

第六十一条　利用者等は、電磁的記録媒体を廃棄する場合には、全ての情報を抹消または読み取り不能な状態にして廃棄すること。抹消に当たっては、下記の各号を含めて最適な方法を検討すること。

一　データ消去に関する世界標準規格に準拠したデータ抹消ソフトウェアを使用する。

二　磁気で完全消去する消磁装置を使用する。

三　読み取りできない状態に物理的に破壊する

2　利用者等は、電磁的記録媒体を他の者へ提供する場合には、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

3　利用者等は、電磁的記録媒体について、設置環境等から要機密情報を抹消する必要性の有無を検討し、必要と認めたときは、当該電磁的記録媒体の要機密情報を抹消すること。

（書面の廃棄方法）

第六十二条　利用者等は、要機密情報である書面を廃棄する場合には、シュレッダーによる細断処理、焼却又は溶解等により復元が困難な状態にすること。また、外部の廃棄処理業者へ業務委託する場合には、機密保持に関する契約を締結した業者とし、廃棄処理証明書の取得、廃棄処分作業への立会い等により、書面が確実に廃棄されていることを確認すること。

第八章　基盤システムの利用

第一節　基盤システムの利用

（識別コードの管理）

第六十三条　利用者等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて、基盤システムを利用しないこと。

2　利用者等は、自己に付与された識別コードを他者が主体認証に用いるために付与及び貸与しないこと。

3　利用者等は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。

4　利用者等は、教育研究事務のために識別コードを利用する必要がなくなった場合は、その旨を技術責任者または技術責任者が指名した担当者に届け出ること。ただし、個別の届出が必要ないと、技術責任者が定めている場合は、この限りでない。

5　技術責任者は、管理者権限を持つ識別コードを付与された利用者等に、管理者としての業務遂行時に限定して当該識別コードを利用させる必要性の有無を検討し、必要と認めたときは、管理者としての業務遂行時に限定して当該識別コードを利用させること。必要に応じて、管理者権限の識別コードの利用状況を監視すること。

6　利用者等は、管理者権限を持つ識別コードを付与され、かつ技術責任者が求めた場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。管理者権限が必要でない場合は、ユーザ権限等の識別コードを利用すること。

（主体認証情報の管理）

第六十四条　利用者等は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに技術責任者又は技術責任者が指名した担当者にその旨を報告すること。

2　技術責任者又は技術責任者が指名した担当者は、主体認証情報が他者に使用され、又はその危険が発生したことを知った場合には、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるシステムへのアクセス停止等の必要な措置を講ずること。

3　利用者等は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

一　自己の主体認証情報を他者に知られないように管理すること。

二　自己の主体認証情報を他者に教えないこと。

三　主体認証情報を忘却しないように努めること。

四　主体認証情報を設定するに際しては、容易に推測されないものにすること。そのために、原則 6 文字以上、数字だけでなく、アルファベットの大文字及び小文字、更に特殊記号等の文字種から最低 2 種類以上を混在させて主体認証情報を構成すること。

五　異なる識別コードに対して、共通の主体認証情報を用いないこと。

六　主体認証情報は、定期的に変更すること。システム的な対応によって強制的に定期的な変更を利用者とうに促すことが可能な場合は、それを採用すること。。

4　利用者等は、所有による主体認証を用いる場合には、以下の管理を徹底すること。

一　主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管

理すること。

二　主体認証情報格納装置を他者に付与及び貸与しないこと。

三　主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに技術責任者又は技術責任者が指名した担当者にその旨を報告すること。

四　主体認証情報格納装置を利用する必要がなくなった場合には、これを技術責任者又は技術責任者が指名した担当者に返還すること。

5　技術責任者又は技術責任者が指名した担当者は、主体認証のために取得した情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、生体情報を取り扱うような場合には、個人情報として厳格に管理し、漏えい、第三者からの悪用等から保護すること。

（識別コードと主体認証情報の付与管理）

第六十五条　技術責任者は、基幹システムにおいて、共用識別コードの利用許可については、原則与えないものとする。基幹システムの制約や利用状況などから、共用識別コードの利用が適切と判断できる場合に限り、利用を認める。拠点追加機器についても同様とし、その判断は基盤システム利用の責任者が行う。

2　技術責任者は、基幹システムにおいて、権限管理について、以下の事項を含む手続を定めること。拠点追加機器については、基盤システム利用の責任者が同様の手続を定めること。

一　主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続

二　主体認証情報の初期配布方法及び変更管理手続

三　アクセス制御情報の設定方法及び変更管理手続

3　技術責任者は、基幹システムにおいて、権限管理を行う者を定めること。拠点の追加拠点機器については、基盤システム利用の責任者が権限管理を行う者を定めること。

（識別コードと主体認証情報における代替手段等の適用）

第六十六条　技術責任者は、基幹システムにおいて、付与した識別コードが使用できなくなった利用者等から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であること、申請理由が妥当であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。代替手段の提供にあたっては、付与された識別コードに対する主体認証情報を提示可能な状態になるまでの間とすること。拠点追加機器についても同様とし、その対応は IT 担当者が行う。

2　技術責任者及び技術責任者が指名した担当者は、基幹システムにおいて、識別コードの不正使用を知った場合には、直ちに当該識別コードによる使用を停止させ、インシデントの対処に係る遵守事項にしたがって対処を実施すること。拠点追加機器についても同様とし、その対応は IT 担当者が行う。なお、基幹システムに影響がある又はその可能性があると判断される場合は、技術責任者又は技術責任者が指名した担当者に、必要な対処を技術責任者に要請する。

第九章　情報処理の制限