第一節　要管理対策区域外での情報処理の制限

（安全管理措置についての規定の整備）

第六十七条　実施責任者は、要保護情報について要管理対策区域外での情報処理を行う場合の安全管理措置についての規定を整備すること。

2　実施責任者は、要保護情報を取り扱う基盤システムを要管理対策区域外に持ち出す場合の安全管理措置についての規定を整備すること。

（許可及び届出の取得及び管理）

第六十八条　利用者等は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外で情報処理を行う場合には技術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 IT 担当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情報である情報について要管理対策区域外で情報処理を行う場合には技術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 IT 担当者に届け出ること。ただし、技術責任者、又は IT 担当者が届出を要しないとした場合は、この限りでない。

3　技術責任者及び IT 担当者は、要管理対策区域外での要保護情報の情報処理に係る記録を取得すること。情報処理に係る記録」には、情報処理の組織、実施者、利用システム、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めること。

4　技術責任者及び IT 担当者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、終了の報告を求めること。期間の延長が必要な場合は、利用者等に改めて許可を得るよう求めること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

5　技術責任者及び IT 担当者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば利用者等に改めて届出をさせる等の措置を求めること。

6　利用者等は、要保護情報について要管理対策区域外で情報処理を行う場合には、教育研究事務の遂行に必要最小限の情報処理にとどめること。

7　利用者等は、機密性３情報、完全性２情報又は可用性２情報を取り扱う基盤システムを要管理対策区域外に持ち出す場合には、技術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 IT 担当者の許可を得ること。

8　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情報である情報を取り扱う基盤システムを要管理対策区域外に持ち出す場合には、技術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 IT 担当者に届け出ること。ただし、技術責任者、又は IT 担当者が届出を要しないとした場合は、この限りでない。

9　技術責任者及び IT 担当者は、要保護情報を取り扱う基盤システムの要管理対策区域外への持ち出しに係る記録を取得すること。持ち出しに係る記録には、持ち出し者、持ち出す機器、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることを考慮すること。

１０　技術責任者及び IT 担当者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う基盤システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、報告漏れである場合には、報告を求めること。期間の延長が必要な状況であれば、利用者等に改めて許可を得るように求めること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

１１　技術責任者及び IT 担当者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う基盤システムを要管理対策区域外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば、利用者等に改めて届出を求めること。

１２　利用者等は、要保護情報を取り扱う基盤システムを要管理対策区域外に持ち出す場合には、教育研究事務の遂行に必要最小限の基盤システムの持ち出しにとどめること。

（安全管理措置の遵守）

第六十九条　利用者等は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずること。

２　利用者等は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

３　利用者等は、要保護情報を取り扱う基盤システムの要管理対策区域外への持ち出しについて盗難及び亡失の防止策、操作や画面の盗み見の防止策など、定められた安全管理措置を講ずること。

４　利用者等は、機密性３情報、完全性２情報又は可用性２情報を取り扱う基盤システムを要管理対策区域外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

第二節　本プロジェクト支給以外の情報システムによる情報処理の制限

（制限処理の原則）

第七十条　基幹システムに保存された要保護情報および『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』のレベル３以上の情報（以下、本節において保護対象情報という）は、本プロジェクトの基盤システム以外の他の情報システム（以下、本節において外部情報システムという）での情報処理を禁止する。また、基盤システム内で処理され保存される保護対象情報においても同様に禁止する。

（許可及び届出の取得及び管理）

第七十一条　利用者等は、やむを得ない事由により、基盤システムに保存された保護対象情報を外部情報システムを使用して情報処理を行う必要がある場合には、当該保護対象情報の保護に関する安全管理措置、管理責任等を含め、ELSI 委員会に申請を行い、ELSI 委員会は当該事案の是非を審査する。

3　技術責任者は、許可事案に対して外部情報システムでの情報処理に係る記録を取得すること。外部情報システムでの情報処理に係る記録には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を考慮すること。

4　技術責任者は、保護対象情報について外部情報システムでの情報処理を許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、報告漏れである場合には、報告させること。期間の延長が必要な状況であれば、利用者等に改めて許可を得るよう求めること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

（安全管理措置の遵守）

第七十二条　利用者等は、基盤システムに保存された保護対象情報について外部情報システムでの情報処理が許可された場合は、前条 1 項の申請内容に基づいて保護対象情報に対して安全管理措置を講じること。

第十章　基盤システムのセキュリティ要件

第一節　基盤システムのセキュリティ要件

（基盤システム計画）

第七十三条　技術責任者は、基盤システム全般にわたってセキュリティ維持が可能な体制の確保を、総括責任者に求めること。

2　技術責任者は、本プロジェクトの情報セキュリティ関係規程内の事項及び基盤システムの業務、取り扱う情報又は利用・運用の環境等の要因による基盤システム固有の要件を考慮して基盤システムのセキュリティ要件を決定すること。また、決定したセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくこと。

3　技術責任者は、基幹システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに基幹システムの構成要素についての対策について、本プロジェクトの情報セキュリティ関係規程内の事項及び基盤システムの業務、取り扱う情報又は利用・運用の環境等の要因による基盤システム固有の要件に基づき定めること。

4　技術責任者は、構築する基幹システムの構成要素のうち製品として調達する機器及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を基幹システムの構成要素として選択すること。

5　技術責任者は、基幹システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。IT 担当者は、拠点追加機器に対する情報セキュリティの侵害又はそのおそ

れのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。必要な措置には次の各号の事項を含めて検討すること。

一　設定する監視機能、監視対象を定める。

二　監視の運用体制を定める

三　監視によりプライバシーを侵害する可能性がある場合は、当該利用者等への説明について定める。

6　技術責任者は、構築した基幹システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。IT 担当者は、追加拠点機器を運用段階へ導入するに当たって、情報セキュリティの観点から、技術担当者と実施する導入のための手順及び環境を協議し、定めること。

（基盤システムの構築及び運用）

第七十四条　技術責任者は、基幹システムの構築、運用に際しては、セキュリティ要件に基づき定めたセキュリティ対策を行うこと。セキュリティ対策には、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに基幹システムについての対策及び監視の実施を含めること。追加拠点機器については、IT 担当者が技術担当者と協議のうえセキュリティ対策を行うこと。

（基盤システムの移行及び廃棄）

第七十五条　技術責任者は、基幹システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに基幹システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。追加拠点機器については、IT 担当者が同様の措置を講ずること。

（基盤システムの見直し）

第七十六条　技術責任者は、基幹システムのセキュリティ対策について見直しを行う必要性の有無を定期的、また適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。追加拠点機器については、IT 担当者が同様の措置を講ずること。

第十一章　基盤システムに係る規定の整備と遵守

第一節　基盤システムに係る文書及び台帳整備

（基盤システムの文書整備）

第七十七条　技術責任者は、所管する基幹システムについて以下の事項を記載した文書を整備すること。拠点追加機器については、IT 担当者が、技術責任者と協議のうえ必要な文書を整備すること。

一　基幹システムを構成する電子計算機関連事項

・電子計算機の管理者及び利用者を特定する情報

・電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン

・電子計算機の仕様書又は設計書

二　基幹システムを構成する通信回線及び通信回線装置関連事項
・通信回線及び通信回線装置の管理者を特定する情報
・通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン
・通信回線及び通信回線装置の仕様書又は設計書
・通信回線の構成
・通信回線装置におけるアクセス制御の設定
・通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応
・通信回線の利用部門
三　基幹システムの構成要素のセキュリティ維持に関する手順
・電子計算機のセキュリティ維持に関する手順
・通信回線を介して提供するサービスのセキュリティ維持に関する手順
・通信回線及び通信回線装置のセキュリティ維持に関する手順
四　インシデントが発生した際の対処手順
2　技術責任者及び技術責任者が指名した担当者は、基幹システムについて整備した文書に基づいて、基盤システムの運用管理においてセキュリティ対策を行うこと。IT 担当者は、整備した文書に基づいて、拠点追加機器の運用管理においてセキュリティ対策を行うこと。

（基盤システムの台帳整備）
第七十八条　実施責任者は、基盤システムに係る以下の事項を記載した台帳を整備すること。台帳の整備にあたっては、基幹システム内のシステム、機器等と、それ以外のシステム、機器等とを区別すること。
一　情報システム名
二　技術責任者の氏名及び連絡先
三　システム構成
四　接続するプロジェクト外通信回線の種別
五　取り扱う情報の格付及び取扱制限に関する事項
六　基盤システムの設計・開発、運用、保守に関する事項
また、情報処理業務を外部に委託する場合は、以下の事項を記載した台帳を整備すること。
七　役務名
八　技術責任者の氏名及び連絡先
九　契約事業者
十　契約期間
十一　役務概要
十二　ドメイン名（インターネット上で提供されるサービス等を利用する場合）
十三　取り扱う情報の格付及び取扱制限に関する事項
2　技術責任者は、基盤システムの台帳を最新の状態で維持すること。基盤システムを新規に構築し、又は更改する際には、基盤システムの台帳を作成、又は更新し、速やかに記載事項について実施責任者に報告すること。

第二節　機器等の購入

（適用範囲）

第七十九条　この節の規定は、機器等の購入（購入に準ずるリース等を含む。以下同じ。）に適用する。

（機器等の購入に係る規定の整備）

第八十条　実施責任者は、本プロジェクトで定めるポリシー並びにそれに基づく規程及び手順等の要件を満たし、本プロジェクトのセキュリティ水準を維持可能な機器等の選定基準を整備すること。

２　実施責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。

３　実施責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

（機器等の購入に係る規定の遵守）

第八十一条　技術責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。

２　技術責任者または技術責任者が指名した担当者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。

第三節　ソフトウェア開発

（ソフトウェア開発に係る規定の整備）

第八十二条　実施責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を技術責任者に求めるための規定を整備すること。

一　技術責任者は、セキュリティに係る対策事項（第三号から第十四号までの遵守事項をいう。）を満たすことが可能な人員、機器、予算等を含めた開発体制を確保すること。

二　技術責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（第三号から第十四号までの遵守事項をいう。）を含む事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について契約書又は付随する確認書等の文書によって保証させること。

三　技術責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。外部に委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を明示すること。

四　技術責任者は、ソフトウェアの作成及び試験を行う開発・テストシステムについては、情報セキュリティの観点から運用中の基盤システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。動作確認のために使用するデータについても、基盤システムに保存されたデータは利用しないこと。

五　技術責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。

六　技術責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能について、真正確認及び権限管理等のセキュリティ機能を管理するための機能のほか、故障、事故及び障害等の発生時に行う対処及び復旧に係る機能、事故発生時の証跡保全の機能等の管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。

七　技術責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

八　技術責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータについて、処理の誤りや意図的な改ざん等を検出するための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等、情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。

九　技術責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価及び ST 確認を受けること。ただし、当該ソフトウェアを要素として含むソフトウェアについてセキュリティ設計仕様書の ST 評価及び ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。ソフトウェア開発を外部委託する場合には、納品までに ST 評価及び ST 確認を受けさせる事項を契約時の条件として含め、契約書または確認書等に含めること。

十　技術責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。

十一　技術責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。規定を整備するにあたり、システムの脆弱性を排除するために、業界標準のセキュアコーディングガイドライン等を必ず採用すること。

十二　技術責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

十三　技術責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する試験項目及び試験方法を定め、これに基づいて試験を実施すること。試験に当たっては、脆弱性の診断を含めること。

十四　技術責任者は、情報セキュリティの観点から実施した試験の実施記録を保存すること。

（ソフトウェア開発に係る規定の遵守）

第八十三条　技術責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。

第四節　主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順

（主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備）

第八十四条　実施責任者及び研究分担者は、所管するシステム、機器について本プロジェクトにおける主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を、以下の事項を含めて定めること。

一　技術責任者及び IT 担当者は、所管するシステム、機器について、主体認証を行うこと。

二　技術責任者及び IT 担当者は、所管するシステム、機器のアクセス制御を行うこと。なお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』のレベル 3 以上に該当する場合は、アクセス制御を行う必要があると判断すること。

三　技術責任者及び IT 担当者は、権限管理を行うこと。

四　実施責任者及び IT 担当者は、所管するシステム、機器について証跡管理を行う必要性の有無を検討すること。取得する証跡には、次の事項を含めて検討すること。、

- 識別コードの発行等の管理履歴
- 各識別コードへのアクセス権設定の管理履歴
- それらの権限管理者の許認可そのものの管理履歴
- 利用者による基盤システムへのログインやデータアクセス等の操作記録
- システムの管理運用に携わる者等によるシステム、機器の操作記録
- ファイアウォール、侵入検知システム（Intrusion Detection System）等通信回線装置の通信記録
- プログラムの動作記録

五　実施責任者及び IT 担当者は、所管するシステム、機器の証跡を取得する必要があると認めた場合は、証跡として取得する情報項目及び証跡の保存期間を定めること。

六　実施責任者及び IT 担当者は、所管するシステム、機器の証跡を取得する必要があると認められた場合は、すべての利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

七　技術責任者及び IT 担当者は、所管するシステム、機器について、データの完全性、可用性を保証するため、データの 2 重化（RAID 等）、バックアップの対策を行う必要性の有無を検討すること。

（主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の遵守）

第八十五条　実施責任者及び技術責任者は、本プロジェクトにおける主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定に基づいて、基幹システムの導入を行

うこと。拠点追加機器においては、必要に応じて実施責任者及び技術責任者の助言を受け研究分担者及び IT 担当者が導入を行うこと。

（取得した証跡の点検、分析及び報告）

第八十六条　技術責任者及び IT 担当者は、所管するシステム、機器の証跡を取得する必要があると認められた場合は、取得した証跡を定期的に又は適宜点検及び分析することの必要性の有無を検討し、情報セキュリティの侵害が特定された又はその兆候が発見された場合など、措置が必要と認めたときは、当該措置を講じ、その結果に応じて必要な情報セキュリティ対策を講じる。

２　技術責任者は、前項について実施責任者に報告すること。IT 担当者は、実施責任者に報告を行う場合、原則研究分担者経由での報告とする。

第五節　暗号と電子署名の標準手順

（暗号と電子署名に係る規定の整備）

第八十七条　実施責任者は、本プロジェクトにおける暗号化及び電子署名のアルゴリズム及び運用方法を、以下の事項を含めて定めること。

一　電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。

二　新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。

三　アルゴリズムが危殆化した場合の緊急対応計画の必要性の有無を検討し、必要と認めたときは、緊急対応計画を定めること。

２　実施責任者は、暗号化された情報（書面を除く。以下この節において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の第一号から第三号の手順（以下「鍵の管理手順等」という。）を定めること。

一　鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等

二　鍵の保存手順

三　鍵のバックアップ手順

３　実施責任者は、本プロジェクトにおける暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を全国大学共同電子認証基盤（UPKI）が発行している場合は、それを使用するように定めること。

（暗号と電子署名に係る規定の遵守）

第八十八条　利用者等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、本プロジェクトが定めたアルゴリズム及び方法に従うこと。

２　利用者等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

3　利用者等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

第六節　学本プロジェクト外の情報セキュリティ水準の低下を招く行為の防止

（措置についての規定の整備）

第八十九条　実施責任者は、本プロジェクト外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。規定の整備に当たっては、次の事項を含むことを考慮すること。

一　不適切なソフトウェア及びサービスの使用を暗黙又は明示的に要求する行為

二　PC の OS やウェッブブラウザなどのソフトウェアのセキュリティ設定の下方修正を暗黙又は明示的に要求する行為。

三　本プロジェクトのウェブ等のコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や機能の停止または削除を暗黙又は明示的に要求する行為。

（措置についての規定の遵守）

第九十条　利用者等は、本プロジェクト外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。

第七節　ドメイン名の使用についての対策

（ドメイン名の使用についての規定の整備）

第九十一条　実施責任者は、アクセスや送信させることを目的としてドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）を告知する場合は、本プロジェクトのドメイン名であることが保証されるドメイン名（以下本プロジェクトドメイン名という）を使用すること。

二　利用者等は、本プロジェクトに係る情報にアクセスさせることを目的として教育研究事務の遂行に係る情報を保存するためにサーバを使用する場合には、本プロジェクトにて構築したサーバまたは本プロジェクトが個別に保存場所として指定するサーバだけを使用すること。

（ドメイン名の使用についての規定の遵守）

第九十二条　利用者等は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。

第八節　不正プログラム感染防止のための日常的実施事項

（不正プログラム対策に係る規定の整備）

第九十三条　実施責任者は、不正プログラム感染の回避を目的として、以下の措置を利用者等に求める規定を整備すること。

一　利用者等は、アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

二　利用者等は、アンチウイルスソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。最新の状態を維持するに当たり、稼動の検証等を要する場合を除き、原則自動更新による仕組みとすること。

三　利用者等は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を常に有効にすること。機能の無効化は厳禁とすること。

四　利用者等は、アンチウイルスソフトウェア等により定期的に全ての電子ファイルに対して、不正プログラムの有無を確認すること。

五　利用者等は、外部からデータやソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、ウィルス対策ソフトを使用して不正プログラム感染の有無を確認すること。

六　利用者等は、不審なメールに添付されたファイルの実行、メール本文に記載された URL のクリック、安全性が不明なファイルのダウンロード等を避け、不正プログラム感染の予防に努めること。具体的な対策が指示される場合にはそれに従うこと。

七　利用者等は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講ずること。また、技術責任者または技術責任者が指名した担当者にその旨報告し、指示を仰ぐこと。

（不正プログラム対策に係る規定の遵守）

第九十四条　利用者等は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。