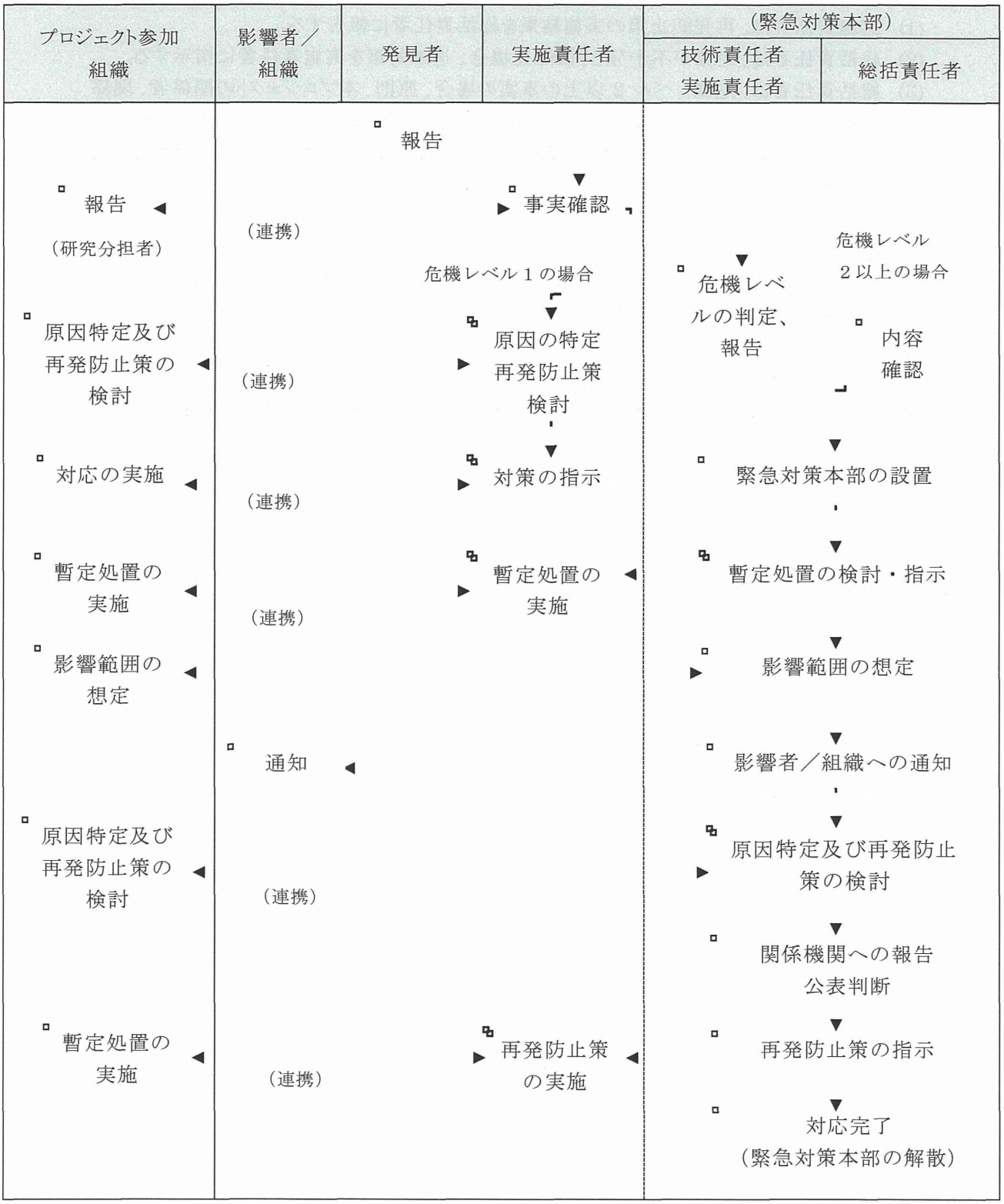
添付1:緊急時対応フロー



枠：東京大学システム部門、アプリケーションベンダー、基幹システム構築ベンダー、また緊急対処サービス等を提供するベンダー、採用を決定した再発防止策に関わる専門組織等の支援を受けて対応する。

添付2:緊急事態発生時の報告先一覧

1. インシデント発生時の報告先

報告先(人、組織)	組織名、電話番号、アドレスなど

2. インシデント発生時の支援先一覧(対応時に支援を要請する支援先)

支援先(組織、人)	組織名、所属、電話番号、アドレスなど
基幹システム構築ベンダーを記載する。	
アプリケーション提供ベンダーを記載する。	
セコムトラストシステムズ株式会社	情報漏洩緊急相談窓口　0120-39-0756 (受付時間:24 時間 365 日受付可能)
東京大学内の支援部門(情報系)を記載する	
東京大学内の支援部門(総務、法務等)を記載する。	
支援要員を記載する。	

添付3:研究参加組織の拠点でウィルス感染の恐れがある場合の暫定対応例

実施責任者は、以下の事項について、報告者または拠点のIT担当者に対応を指示する。また、中核拠点の技術責任者に対応を指示する。

【報告者または拠点のIT担当者への指示事項例】

※実施責任者または実施責任者が指名した事案対応者の指示に従って対応すること。

1) 利用者等の PC にウィルス侵入、感染に関わる通知メッセージが表示されていないかを確認すること。
2) 状態がおかしいと判断した PC やサーバをネットワークから切り離すこと。
3) 当該拠点のネットワークを基幹システムから切り離すこと。
4) 大学／研究機関等の独自ネットワークと接続している場合は、当該拠点のネットワークを切り離すこと。
5) 当該拠点に設置されている全システムのウィルスチェック(フルスキャン)を実施すること。
6) ウィルス感染の可能性のある PC やサーバ等のハードディスクを保全すること。
7) 当該拠点で利用する／した外付けハードディスク(外部記憶媒体)を特定し保全すること。

【技術担当者への指示事項例】

※対応が困難と判断した場合は、速やかに東京大学システム部門、アプリケーションベンダー、基幹システム構築ベンダー、また緊急対処サービス等を提供するベンダーに支援を要請し、協議を行いながら対応を行うこと。

1) サーバ管理用 PC、またウィルス対策ソフトの管理者用画面(中核拠点管理者用PC)にウィルス侵入、感染に関わるメッセージ等が表示されていないかを確認すること。
2) 中核拠点、データセンターに設置されている全システムのウィルスチェック(フルスキャン)を実施すること。
3) 全研究参加組織の IT 担当者に対して、速やかに基盤システム上のすべてのサーバ、PC 等に対するウィルスチェック(フルスキャン)を実施する旨通知すること。リモート対応可能なサーバや PC は、中核拠点から実施する。
4) 各拠点、中核拠点、データセンター設置のサーバで取得しているシステムログ(プログラム実行の記録、コマンド実行の記録等を含む)、データアクセスログ、外部(インターネット)との通信ログ等、解析に使用するログを保全すること。
5) センターサーバや管理者用 PC で利用する／した外付けハードディスク(外部記憶媒体)を特定、保全すること。
6) 各拠点、中核拠点、データセンターに設置されている全システムのウィルスチェック(フルスキャン)結果を確認すること。

7) ウィルス感染の可能性のあるPC、サーバ等のハードディスクの保全を行うこと。
8) 解析用のログを収集すること。
9) ログの分析、ウィルス感染の可能性のあるPC、サーバ等のハードディスクの解析をウィルスソフトベンダーや緊急対象サービス等の提供ベンダーに要請すること。
10) ベンダー解析結果を確認し、駆除の方法について対応を検討すること。
11) 対応策を整理し、関係各所に対応を指示すること。

別紙：成果物一覧

(1)「2. A) 情報セキュリティ対策実施手順の整備」の各業務の成果としての手順書

No.	文書番号	文署名	ファイル名	様式有無	RFP No.	数量
1	REGHW4011	インシデント対応手順.	[REGHW4011]インシデント対応手順.docx	有	2.A) (1)	1
2	REGHW4021	システム変更管理手順	[REGHW4021]システム変更管理手順.docx	有	2.A) (2)	1
3	REGHW4022	ハードウェア、ソフトウェア資産管理手順	[REGHW4022]ハードウェア、ソフトウェア資産管理手順.docx	無	2.A) (2)	1
4	REGHW4031	情報資産取扱手順	[REGHW4031]情報資産取扱手順.docx	有	2.A) (3)	1
5	REGHW3011	システム利用基準	[REGHW3011]システム利用基準.docx	無	2.A) (4)	1
6	REGHW3021	職場環境セキュリティ対策基準	[REGHW3021]職場環境セキュリティ対策基準.docx	無	2.A) (4)	1
7	REGHW3031	ソフトウェア開発管理基準	[REGHW3031]ソフトウェア開発管理基準.docx	無	2.A) (5)	1
8	REGHW4051	外部委託先管理手順	[REGHW4041]外部委託先管理手順.docx	有	2.A) (5)	1
9	REGHW3041	サーバルーム・セキュリティ対策基準	[REGHW3041]サーバルームセキュリティ対策基準.docx	無	2.A) (6)	1
10	REGHW4051	ログ管理手順	[REGHW4051]ログ管理手順.docx	無	2.A) (7)	1
		ログ管理手順(補足資料)	[REGHW4051]ログ管理手順(補足資料).docx			1
11	REGHW4061	内部監査手順	[REGHW4061]内部監査手順.docx	有	2.A) (8)	1
12	REGHW4071	是正処置手順	[REGHW4071] 是正処置手順.docx	有	2.A) (8)	1

以上

東京大学医科学研究所 御中

「幹細胞関連情報の基盤システム」に係る
情報セキュリティ対策の整備支援業務

情報セキュリティに関するコンサルティング報告書

平成27年3月20日

セコムトラストシステムズ株式会社
コンサルティング部

目　次

1.本書の目的

「幹細胞関連情報の基盤システム」(以下「基盤システム」という)は、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」の研究事業参加者および研究協力者が、互いに非公開の実験データ等を、相互貢献の精神に基づいて共有することを可能にするために導入され、開発を推進しているものである。

さらに当該基盤システムについて、今後機能拡張し、研究参加機関拠点外からのデータ共有システムの構築・運用(外部へのWebサイトの公開、準会員制の導入)などが予定されている。

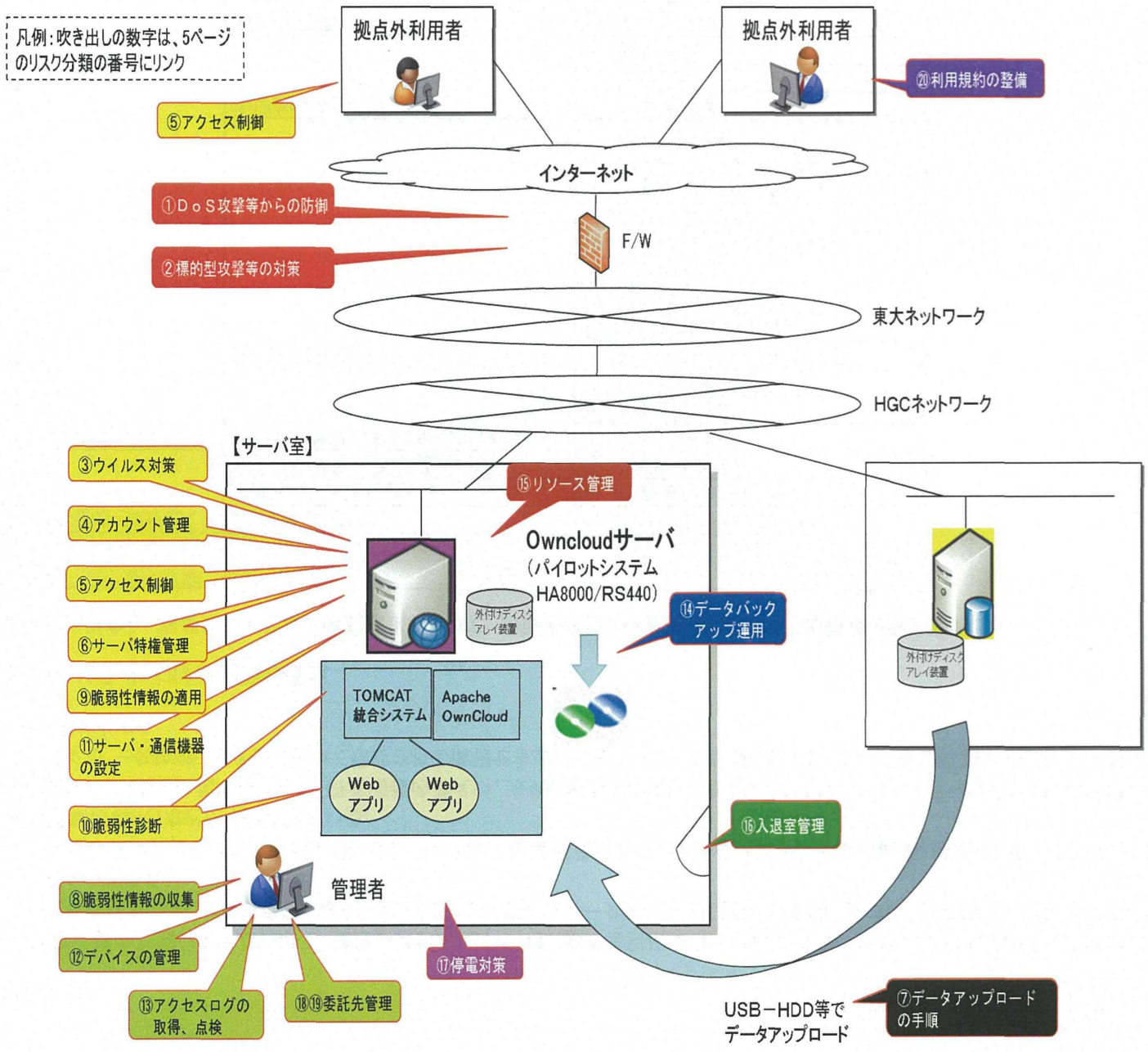
当然ながらこれらの機能拡張においても、研究情報の漏えい、滅失、および毀損を予防するという情報セキュリティの強化は重要課題であり、本書においては、本拠点外からのデータ共有システムにおいて想定される情報セキュリティリスクと、求められる対策、および考慮事項をまとめることにより、システム構築・運用時の指標とすることを目的とする。

2.情報セキュリティにおける対策の視点

ヒアリングの結果から、本基盤システムの機能拡張において、対策を検討すべき視点として以下の事項を取り上げた。

No.	リスク分類		
	大分類	中分類	小分類
1	外部からの侵入	外部からの防御	① DoS攻撃等からの防御
2		外部との不正通信対策	② 標的型攻撃等の対策
3		不正プログラム等の侵入対策	③ ウイルス対策
4	内部での管理	アクセス管理と不正持ち出し対策	④ アカウント管理
5			⑤ アクセス制御
6			⑥ サーバ特権管理
7		セキュリティ運用	⑦ データアップロードの手順
8			⑧ 脆弱性情報の収集
9			⑨ 脆弱性情報の適用
10			⑩ 脆弱性診断
11			⑪ サーバ、通信機器の設定
12			⑫ デバイスの管理
13			⑬ アクセスログの取得、点検
14			⑭ データバックアップ運用
15			⑮ リソース管理
16		物理的セキュリティ対策	⑯ 入退室管理
17			⑰ 停電対策
18			⑱ 契約締結
19		委託先管理	⑲ 委託先評価
20		その他	⑳ 利用規約の整備

3.拠点外からのデータ共有システムにおけるセキュリティ上のポイントについて



4.リスク分類と対策、考慮事項について

No.	リスク分類		求められるセキュリティ対策	本システムにおける考慮事項等
1	外部からの防御	①DoS攻撃等からの防御	・DoS攻撃、リスト型攻撃等、外部からの攻撃を検知・防御する仕組みを整備する。(IPS、IDS、WAF等)	・DoS攻撃はサービスの提供に甚大な影響を与え、また、リスト型攻撃はなりすましによる重要情報の窃取につながり、これらの攻撃を受けた場合、重要情報の漏えいはもちろん、社会的な影響(貴法人の信頼性の低下、管理体制の不備を問われる等)にも発展する可能性があるため、この仕組みを整備することが重要である。 ただし、本システムの場合、インターネットとの接続においては東京大学ネットワーク経由となるため、東京大学のネットワーク管理部門との協議を行いながら検討を進める必要があると思慮する。
2	外部との不正通信対策	②標的型攻撃等の対策	・内部から外部に対する不審な通信(ウィルス等による通信)が行われていないか監視する。 ・内部から外部への不正なインターネットアクセスを制限する仕組み(フィルタリングソフト等の導入)を講じる。	・インターネットアクセスの監視は、不正なサイト情報を収集し、ブラックリストに反映することでアクセスを制限することも含めて対処が必要だが、現状のプロジェクトの管理要員だけ対応すのは困難なため、専門の外部組織への当該業務委託も選択肢に入れて検討する。 ・フィルタリングの導入については、東京大学ネットワーク管理部門との協議が必要
3	不正プログラム等の侵入対策	③ウイルス対策	・ウイルス対策ソフトを導入する。 ・定期的にフルスキャンによるウイルスチェックを行う。 フルスキャンによってウイルスを発見した際、即座に対処できる体制を整える。	・ownCloudには、オープンソースのサーバ用ウイルス対策ソフト「Clam AntiVirus」が標準サポートされている。 ・「Clam AntiVirus」では、設定により毎日自動的にウイルス定義ファイルの最新化とownCloudのdataディレクトリのウイルススキャンを行うことが可となっている。 ・「Clam AntiVirus」では、ownCloudにファイルがアップロードされる際にウイルスチェックを行い、ウイルスが検出されると当該ファイルが自動的に削除され、画面上
4	アクセス管理と不正持ち出し対策	④アカウント管理	・アカウントの発行・削除手続きを整備する。アカウントには、管理スタッフ、データ提供者(会員)、及びインターネット経由の利用者(準会員)がいるが、管理スタッフ、データ提供者(会員)に対するアカウントの発行手続きを明確に定めておく必要がある。インターネット経由の利用者(準会員)についても、サービスに応じた発行の仕組みが必要である。 ・すべてのシステムのパスワード変更を定期的に実施する。	・管理スタッフ、データ提供者(会員)アカウントの発行・削除では必ずエビデンスにて申請、承認の手順を経ることとし、また、アカウント台帳を作成し、定期的に(最低年1回)台帳の棚卸しを行う。 ・準会員の扱いについては、準会員資格の審査手続きも考慮した発行手続きとその仕組みが必要になると思慮する。 ・管理スタッフ、データ提供者(会員)のパスワード変更はセキュリティ上最低でも90日程度毎の変更とし、かつシステムによる強制変更と合わせて検討する。ただし、コスト等の観点から手動変更とする場合、確実に期限内に変更されていることを確認できる方策も検討する。 ・準会員については、サービスの約款に謳うなどの処置が必要と思慮する。可能であ

No.	リスク分類		求められるセキュリティ対策	本システムにおける考慮事項等
5		⑤アクセス制御	・管理スタッフのアクセス制限を担当業務等に応じて、厳格に行う。 ・既存システムからのデータ移行手続きと作業手順の確立が必要である。 ・定期的(最低年1回)に、発行アカウントに対するアクセス権限の棚卸しを行う。	・セキュリティの基本である、資格と必要性(業務上必要な人へ、必要なときに、必要な権限を付与する)という考え方に基づく運用を確立することが重要となる。
6		⑥サーバ特権管理	・サーバ特権アカウントの利用者は必要最低限のシステム管理者に限定する。 ・使用ログを取得する。 ・システム管理者は、使用の都度、特権アカウントの申請を行い、アカウント、パスワードの払い出しを受ける運用とする。	
7	セキュリティ運用	⑦データアップロードの手順	・既存システムからのデータの移行については、ルールに基づき許可を得たものであることを確認する手続きを整備する。(現状では、媒体による移行が前提となる)	・許可を得たことを確認する手順として、事後の確認も可とするか要検討である。また、データの移行の手段として、今後ネットワーク経由を可とする場合は、基幹システムとの接続に対するセキュリティを考慮する必要がある。
8		⑧脆弱性情報の収集	・対象システムのOS、ミドルウェア、アプリーケーションに係る脆弱性情報(原則毎日)を収集する仕組みを構築する。	・脆弱性情報は基本的には定例(月次等)の配信の他、緊急性の高いものは随時、各ベンダーから配信されている。自組織でこれらの情報の収集が難しい場合には、脆弱性情報の収集連絡サービスを提供している外部業者に委託することも選択肢に入れ検討する。
9		⑨脆弱性情報の適用	・脆弱性修正プログラムは速やかに適用し、適用されていることを確認する。	・対象システムに関係する脆弱性修正プログラムが配信された場合は、まずテスト環境で検証し、当該プログラムの適用が他のアプリケーション等に影響がでないことを確認した後、速やかに適用することが求められる。 ・脆弱性情報の本システムへの影響度、適用の判断や適用期限等に関して、手順を整備することも考慮する。
10		⑩脆弱性診断	・ネットワーク診断(サーバ、ネットワーク機器に存在する脆弱性を洗い出す)、Webアプリケーション診断を定期的に行う。	・リスクの高さを考慮するとネットワーク診断(サーバ、ネットワーク機器に存在する脆弱性を洗い出す)は4半期に1回程度(PCIDSS規格検討値)、Webアプリケーション診断(Webの脆弱性を洗い出す)は最低年1回程度、及び大幅な構成変更をした都度実施することを検討する。
11		⑪サーバ、通信機器の設定	・サーバ、通信機器の業務上不要なポート、サービスを停止する。	・ウィルス等の不正プログラムが侵入した場合に悪用される可能性があるため、業務上不要なポート、サービスをとめることが必要である。

No.	リスク分類		求められるセキュリティ対策	本システムにおける考慮事項等
12		⑫デバイスの管理	・デバイスに量は制限し、必要な都度、申請に基づいて利用を許可する。 ・外部記憶媒体は、プロジェクトが許可したものを利用する運用とする。	・デバイスにの接続を自由にしていた場合、外部記憶媒体を接続し、大量の重要データを不正に持ち出すことができる他、私有のUSBメモリ等の接続により、ウイルス等の不正プログラムの侵入を招く恐れがあるため、デバイスは必要な都度、許可された媒体のみの利用とすることが必要である。
13		⑬アクセスログの取得、点検	・サーバへのアクセスログ（管理者のDB操作ログ、データへのアクセスログ、システムへのログイン・ログアウトログ、システムログなど）を取得し、定期的に点検を行う。	・サーバへのアクセスログを取得し、点検することにより、不正な行為を早期に発見でき、不正行為の被害を最小限にすることが可能であり、また不正行為に対する牽制効果が期待できる。
14		⑭データバックアップ運用	・データバックアップを定期的に取得する。 ・バックアップは、外部媒体、内側のネットワーク、または遠隔地に保管する。 ・機密性の高いデータのバックアップデータは暗号化する。 ・バックアップ手順、リストア手順は定期的に検証する。	・データはバックアップ取得の重要性のみならず、必要時に確実にリストアできるよう、平常時から定期的にバックアップ／リストア手順を検証しておくことが重要である。
15		⑮リソース管理	・メモリ、CPU、Disk容量等のリソース管理の運用の仕組みを整備する。	・リソース管理はサービスの提供に直結するため、重要な業務となる。実際には、それぞれの管理項目に対して閾値を設定し、それを超えた場合、メールにアラート通知される方法が一般的である。 ・ただし、本業務を自組織のみで対応することは、担当者への負荷をかかるため、外部業者への委託（24時間365日の監視）も検討する。
16	物理的セキュリティ対策	⑯入退室管理	・サーバルーム（東大医科学研究所8F）への入退室制御を行い、入退室のログを取得して定期的に点検する。	・入退室ログは、取得のみならず、定期的な点検の実施も運用に含めることを検討する。（休日、夜間等に不自然な入退室が繰り返されていないか等。）
17		⑰停電対策	・停電の発生時に、システムの正常停止が可能な電源を確保するため、UPSを設置する。	・UPSはあくまでも一時的な電源供給であり、今後サービスの拡張、利用者の増加等に伴って高いサービス水準が求められるような場合には、データセンターへの移設も検討する。
18	委託先管理	⑱契約締結	・委託先とは、明文化された機密保持事項を網羅した契約を締結する。 ・契約に含める秘密保持事項に変更が生じた場合、速やかに再契約等の処置を行う。	・昨今、委託先でのインシデント事案の発生が多発していることもあり、委託先での管理状況の確認、定期的な評価の実施が求められる。
19		⑲委託先評価	・委託先の評価基準は定期的に見直しを行う。 ・委託先にはアンケートやヒアリングによる再評価を定期的（1年に1回程度）に実施し、必要に応じて改善要請を行う。	

No.	リスク分類		求められるセキュリティ対策	本システムにおける考慮事項等
20	その他	⑳利用規約の整備	・以下のような項目を含む利用規約を整備する。 （データ提供者、及びインターネット経由の利用者に係る利用要件、問い合わせ窓口の運用範囲、及びサービス可用性の基準等）	・可用性の基準については、サービス稼働率のコミット等SLAの要素が求められる場合、当該サービスレベルの検討も行う。

【備　考】
現時点では、当面はパイロットシステムとしての運用を前提としているため、本来考慮されるべきデータやサービス機能の冗長化、負荷分散といった連続可用性に関しては、考慮していない。
パイロット運用から本格運用への移行に際しては以下を考慮する必要がある。

・データの二重化
・サーバの冗長化（またはバックアップシステムのホットスタンバイ等）
・負荷分散の仕組みの導入
・バックアップサイトの手配
・ユーティリティ機能（電源、空調等の設備）の強化
・データセンターでのシステム運用

以上

2014年度　内部監査計画書（パイロット運用版）

承認日	2015年3月13日	
承認者 （総括責任者）	中井 謙太	印

作成日	2015年3月10日	
作成者 (監査責任者)	黒澤 隆	印

1．監査の目的

(1)内部監査のパイロット運用を目的に実施する。
(2)運用基本方針、運用基本規程、運用管理規程の規定内容の運用が行われているかを確認する。

2．監査の範囲

ヒト幹細胞関連情報の基盤システム（以下「本基盤システム」という。）は、「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）における次の組織の作業エリア
(1)東京大学医科学研究所　総合研究棟 8F　中井研究室　本プロジェクト運営エリア
(2)東京大学医科学研究所　臨床研究 A 棟 3F　本プロジェクト参加組織の研究エリア

3．監査の内容

(1)ルールの浸透度
(2)基本的な運用の状況

4．監査対象組織

(1)東京大学医科学研究所　ゲノム解析センター　機能解析イン・シリコ分野　本プロジェクト中核機関
(2)東京大学医科学研究所　先端医療研究センター　分子療法分野　（医科研病院拠点）

5．監査期間

実施時期：2015年3月

6．監査体制

(1)監査責任者：
(2)監査実施者：監査責任者の指揮のもと、下記の者が担当する。

	監査員所属	役　職	監査員名
1	セコムトラストシステムズ（株）	主任コンサルタント	田辺　裕也
2	－	－	－

7．監査の実施要領

ヒヤリング、文書類の確認、職場観察で得られる証拠により確認する。

8．監査報告書予定時期

2015年3月20日

2014年度　内部監査実施計画書（パイロット運用版）

作成日：2015年3月9日

作成	承認（監査責任者）
田辺(STS) 2015/03/09	黒澤 隆 (IMSUT) 2015/03/10

1. 監査方針　　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）の情報セキュリティ対策規程の理解状況とその運用状況を確認する。

2. 監査範囲　　基盤システム運用基本方針、基盤システム運用基本規程、基盤システム運用管理規程の定める範囲とする。

3. 内部監査実施計画

日時		監査対象部門	監査時のポイント	場所	監査担当
2015年3月17日	14:00-15:30	東京大学医科学研究所　先端医療研究センター　分子療法分野　（医科研病院拠点）	ルールの浸透状況及び運用状況	東京大学医科学研究所　臨床研究A棟 3F	チーム1
	15:30-17:00	東京大学医科学研究所　ゲノム解析センター　機能解析イン・シリコ分野（本プロジェクト中核拠点）	ルールの浸透状況及び運用状況	東京大学医科学研究所　総合研究棟8F	チーム1

4. 監査体制

監査チーム	チーム1	チーム2	チーム3
監査リーダ	田辺(セコムトラストシステムズ(株))		
監査員1			
監査員2			
監査員3			

内部監査チェックリスト

No.	チェック項目内容	中核拠点スタッフ	拠点IT担当者	確認要	現場・証跡確認※	適合の判定の目安	判定 適合	判定 不適合	判定 N/A	指摘・提案内容	備考
4	情報セキュリティ基本方針について構成員に周知しましたか。	●	●			全利用者等に周知されていること。					
6	セキュリティ関連文書は、全利用者が閲覧可能となっていますか。	●	●			諸規則は必要なときに、必要な場所で閲覧のみ可能であり(可用性)、外部への流出(機密性)、書き換え(完全性)等が生じない対策が施されている事。					
24	情報セキュリティの基本方針について理解していますか。	●	●			理解していること。または、公開場所を理解していること。					
25	情報セキュリティの基本方針はどこにありますか。	●	●								
41	要機密情報を含む文書はどのように管理していますか。	●	●			個人情報、研究結果等を含む要機密情報文書は施錠保管していること。					
43	台帳の保管状況を見せて下さい。要機密情報を施錠保管していますか。	●	●	●	現場確認	要機密情報の保管状況を確認し、施錠保管されていること。 取り扱う要機密情報が一覧化され、また保存期間等がわかるようになっていること。					
45	要機密情報やデータを要管理対策区域外に持ち出すことはありますか。持ち出す場合、どのようなセキュリティ対策を行っていますか。	●	●			要機密情報を社外に持ち出す際のセキュリティ対策がルール通り行われていること。 ＜例＞ ・施錠できるケース等に入れて持ち運んでいる。 ・常に携帯し、電車の網棚や空いている座席に置かない。 等、基準を遵守している。					
46	PCやiPadを要管理対策区域外に持ち出す場合、どのような手続きが必要ですか。	●	●			PCを社外に持ち出す時の手続きが確認できること。 ＜例＞ ・責任者の承認後、機器貸出担当者の承認を得ている。					
51	外部記憶媒体や要機密情報等はをどのように処分していますか。	●	●			外部記憶媒体がルール通りに廃棄されている事。 ＜例＞ ・システム部が媒体を物理的に破壊した後、廃棄する。 ・シュレッダー処理、専用廃棄ボックスへ投函など。					
53	媒体を配送することはありますか。その時、どのようなセキュリティ対策をとっていますか。	●	●			媒体を配送する際のセキュリティ対策について明確である事。 ＜例＞ ・組織が認めた輸送方法を用いている。 ・緩衝材等を使用している。 ・専用ケースを使用している。					
60	利用者へのIDの付与はどのように行われていますか。また利用者IDは誰が管理していますか。	●				利用者へのID付与の具体的な方法とIDの管理責任者について確認できること。 ＜例＞ ・利用者は『アカウント申請書』に必要事項を記入し、運用管理者に申請する。登録完了後、運用管理者は利用者に口頭でIDと初期パスワードを通知する。 ・利用者IDは運用管理者が管理している。					
61	人事異動や退職により利用者IDが不要となる場合、利用者IDの抹消はどのように行われていますか。(利用者IDとは、システムまたはアプリケーションの利用者IDです。)	●	●			手順が明確になっていること。					
62	利用者のIDを管理している台帳を見せて下さい。	●		●		登録者がもれなく管理され、変更、抹消等の処置が確実に行われていること。					
	特権は資格と必要性に基づき利用されていますか。 例：都度貸出(PW変更) 利用者限定など	●									

内部監査チェックリスト

No.	チェック項目内容	中核拠点スタッフ	拠点IT担当者	確認要	現場・証跡確認※	適合の判定の目安	判定 適合	判定 不適合	判定 N/A	指摘・提案内容	備考
64	特権の付与はどのように行われていますか。また特権は誰が管理していますか。	●	● 拠点サーバ			特権の付与の具体的な方法と特権の管理者が誰か確認できること。 ＜例＞ ・特権利用の申請者は申請書を運用管理者に提出する。 ・特権の管理は運用管理者が行っている。					
65	人事異動や退職により特権が不要となる場合、特権の抹消はどのように行われていますか。	●	● 拠点サーバ			特権の抹消の具体的な方法について確認できること。 ＜例＞ ・人事異動や退職により特権が不要となる場合、直属の上司が特権の抹消を申請する。処理終了後、直属の上司が抹消の確認を行う。					
69	システムあるいはアプリケーションにログインする画面を見せてください。あなた以外にパスワードを知っている人はいませんか。	●	●	●	現場確認	PCのパスワードが利用者の責任で適正に管理されている事。					
74	外来者の執務室への入退室についてどのような規制措置を行っていますか。	●	●			外来者の入退室に関する規制措置が確認できること。 ＜例＞ (1)セキュリティ境界の設置 ・ICカードによる入退室規制 (2)人的管理 ・受付電話（インターフォン）による利用者等の呼び出し					
75	サーバルームへは許可された者だけが入室できるようになっていますか。	●	●			入室を許可された者が特定されていること。					
76	サーバルームの入退出時の手順について教えて下さい。	●	●			手順に従った運用が行われていること。					
77	サーバあるいはアプリケーションの不正操作を防ぐためにどのようなセキュリティ対策を行っていますか。	●	●			サーバへの物理的アクセスを制限する仕組みがあること。					
82	サーバやアプリケーションのデータバックアップはどのように行っていますか。	●	●			サーバのデータバックアップについて適切に実施されていることが確認できること。 ＜例＞ ・重要なサーバのデータは定期的にバックアップを取得している。					
83	バックアップ媒体をどのように保管していますか。	●	●			バックアップ媒体の保管が適切に行われていること。 ＜例＞ ・バックアップ媒体は施錠保管している。					
84	ログは取得していますか。ログは改ざんされないように保護していますか。	●				取得を決めたログが取得されていること。またログへのアクセス制限が関係者だけに限定されていること。					
85	アクセスログやシステムログの監視レベル（範囲、内容）が適正であるか見直しを行っていますか。	●				監視レベルの見直しを定期的に行っていること。 ＜例＞ ・内部監査でアクセスログやシステムログの監視レベルについてチェックしており、適正でない場合、監視の範囲、内容を変更している。					
92	システムを変更（ハードウェアやソフトウェアを変更）する場合、どのような手続きが必要ですか。	●	●			システム変更の手続きを説明できること。 ＜例＞ ・システム変更の場合は申請書を作成し、開発責任者及び運用責任者の承認を得ている。					
追加											
	セキュリティパッチの情報を定期的に取得していますか。また、適用が必要と判断したパッチがすべてPC、サーバ等に適用が完了していることを確認していますか。	●				定期的に脆弱性情報を取得していること。 パッチの適用状況を追跡管理していること。					

内部監査報告書（パイロット版）

作成日	2015年3月17日
作成者	田辺　裕也

管理No.2	※敬称略
被監査部門	東京大学医科学研究所　先端医療研究センター　分子療法分野（医科研病院拠点） （監査対応者：澤田　幸子）
監査実施日時	2015年3月17日　14:00～15:10
監査人名	監査チーム1　　田辺　裕也（セコムトラストシステムズ（株））
監査責任者	黒澤　隆
監査テーマ	(1)内部監査のパイロット運用を目的に実施する。 (2)運用基本方針、運用基本規程、運用管理規程に定めた運用が行われているかを確認する。
監査内容	(1)ルールの浸透度 (2)基本的な運用の状況

指摘事項	□ メジャー（0件）　□ マイナー（0件）　□オブザベーション（0件）
監査結果	要機密情報扱いされる研究データは、基盤システム運用・管理規程に基づいて取り扱いわれていることが確認できた。本監査において、指摘事項は発見されなかった。 補足： 今後、本プロジェクトに関わる個別のセキュリティ運用の基準・手順等のリリースに伴い、先端医療研究センターの定める基準・手順と対応が異なる場合が想定される。そのような場合は、先端医療研究センターのセキュリティ推進部門及び本プロジェクトの実施責任者が協議を行い、採用する基準、手順を決定することが望まれる。（他の拠点も同様に対応を行う。）

是正処置	□ 要　　■ 不要
改善処置	□ 要　　■ 不要

【説明】
メジャー　：重大な不適合
マイナー　：軽微な不適合
オブザベーション　：不適合ではないが是正した方が良い

監査実施者	監査責任者	被監査部門責任者	総括責任者
田辺 2015.3.17	2015.3.20	2015.3.23	2015.3.24

内部監査報告書（パイロット版）

作成日	2015年3月17日
作成者	田辺　裕也

※敬称略

管理No.1	
被監査部門	東京大学医科学研究所　ゲノム解析センター　機能解析イン・シリコ分野（本プロジェクト中核拠点） （監査対応者：池田　恵美）
監査実施日時	2015年3月17日　15:30～17:00
監査人名	監査チーム1　　田辺　裕也（セコムトラストシステムズ（株））
監査責任者	黒澤　隆
監査テーマ	(1)内部監査のパイロット運用を目的に実施する。 (2)運用基本方針、運用基本規程、運用管理規程に定めた運用が行われているかを確認する。
監査内容	(1)ルールの浸透度 (2)基本的な運用の状況

指摘事項	□ メジャー（0件）　□ マイナー（0件）　■オブザベーション（1件）
監査結果	本プロジェクトのシステム管理、セキュリティ推進部門として、大きな問題は発見されなかったが、以下の点については対応の検討が望まれる。 オブザベーション1： PCソフトの脆弱性が報告された場合、技術責任者が各拠点のIT担当者にセキュリティパッチの適用を要請しているが、対象となるPCすべてに適用されたかどうかの確認までは行われていない。 その他： 以下の対策導入が計画されていることを確認した。早期の導入、運用開始が望まれる。 ・システムログの管理強化 セキュリティ管理強化のため、サーバのシステムログ、特権ID等の操作ログなど、ログの集中管理及びログ解析の仕組みを構築中であった。 ・サーバルームの入退管理強化 サーバルームの入退管理強化のため、顔認証による入退管理システムの導入準備を進めていた。

是正処置	□ 要　　■ 不要
改善処置	■ 要　　□ 不要　　※改善の検討対象事項として取り上げます。
	オブザベーション1：ソフトウェアの脆弱性が放置された場合、不正プログラム等の侵入によってデータの漏えいやPCの乗っ取りなどの事案に繋がる可能性がある。技術責任者は、脆弱性が発見された場合には、速やかにセキュリティパッチの適用を利用者等に要請するとともに、すべてのPCに適用が完了するまで追跡管理を行うことが望まれる。 運用例： 追跡管理については、システム化によって確認できることが望ましいが、システム化による追跡管理が困難な場合は、各拠点のIT担当者に拠点内全PCへのパッチ適用の要請※を行うとともに、適用完了報告を求める運用を検討する。また、技術責任者は全拠点から適用完了報告が行われるまで、セキュリティパッチの適用状況を管理し、基幹システム内のすべてのPCにセキュリティパッチの適用が完了したことを確認する。 ※セキュリティパッチ適用の要請の際には、適用期限及び報告期限を指定して要請を行う。

【説明】
メジャー　：重大な不適合
マイナー　：軽微な不適合
オブザベーション　：不適合ではないが是正した方が良い

監査実施者	監査責任者	被監査部門責任者	総括責任者
田辺 2015.3.17	黒澤 2015.3.20	2015.3.24	2015.3.24

８．倫理申請手続　資料

1）　基盤システム上の統合データベース利用に関する倫理申請手続きフローチャート

2）　倫理審査関連手続き　事例（2種　7件）

3）　基盤システム上の統合データベース利用及び複数拠点からなる共同研究遂行に関する倫理申請手続きの短縮化