■一般ユーザ

項番	シナリオ	概要	確認内容	確認日	大阪大学	成育医療	東京女子大	慶応大学	医科研病院	京大IPS研	京大再生研	神戸理研
					判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）
1	ログイン	ログインする。	基盤システムのLDAPと連携してユーザ認証できることを確認する。	2014/3/18 2014/3/24	× ○	× ○	× ○	× ○	× ○	× ○	× ○	× ○
2	ノートの参照	ノート参照画面を開き、ノート（マスター）を参照する。	ノート（マスター）があることを確認する。 ノート（マスター）を参照できることを確認する。	2014/3/24	○	○	○	○	○	○	○	○
8	メモ登録及び検索した場合の新規グループ作成	ノートグループ作成画面を開き、ノート（マスター）にメモ「ST_3」を入力し、そのノートを検索して新規グループ（グループ4）を作成する。	ノートへのメモの登録、ノートの検索両方の機能が利用できることを確認する。 メモを登録したページを含むノート（グループ4）を作成できることを確認する。	2014/3/24	○	○	○	○	○	○	○	○
9	ノート（グループ）の参照	ノート参照画面を開き、ノート（グループ1）を参照する。	ノート参照画面で作成したノート（グループ1）を参照できることを確認する。	2014/3/24	○	○	○	○	○	○	○	○
13	ノート（グループ）編集 （メモ登録）	ノートグループ編集画面を開き、グループ5を表示して、メモを入力した後、登録する。 メモ登録後、グループを登録する（グループ6）。	ノートグループ編集画面でノート（グループ5）を編集できることを確認する。 ノートグループ編集画面でメモが登録できることを確認する。	2014/3/24	○	○	○	○	○	○	○	○
16	作成したノート（グループ）の削除	ノートグループ編集画面を開き、グループ1を選択して、ページをグループを削除する。	ノートグループ編集画面でノート（グループ7）を削除できることを確認する。	2014/3/24	○	○	○	○	○	○	○	○
17	ログアウト	ログアウトする。	ログアウトできることを確認する。	2014/3/24	○	○	○	○	○	○	○	○

■システム管理者

項番	シナリオ	概要	確認内容	確認日	大阪大学	成育医療	東京女子大	慶応大学	医科研病院	京大IPS研	京大再生研	神戸理研
					判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）
1	ログイン	ログインする。	基盤システムのLDAPと連携してユーザ認証できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
2	システム管理者のノートの参照	機能選択画面を開き、ユーザIDを選択せずにノート参照画面を開く。	システム管理者ユーザのノートがないことを確認する。 一般ユーザのノートがないことを確認する。	2014/3/23	○	○	○	○	○	○	○	○
3	一般ユーザのノートの参照	機能選択画面を開き、ユーザIDで一般ユーザを選択して、ノート参照画面を開く。 一般ユーザのノート（マスター）を参照する。	機能選択画面のユーザIDで選択した一般ユーザのノート（マスター）が参照できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
4	一般ユーザのノートの編集 （メモ登録）	機能選択画面を開き、ユーザIDで一般ユーザを選択して、ノート参照画面を開く。 一般ユーザのノート（マスター）にメモを入力して、登録する。	機能選択画面のユーザIDで選択した一般ユーザのノート（マスター）が参照できることを確認する。 一般ユーザののーと（マスター）にメモを登録できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
5	ログの表示	ログ参照画面を開き、ログを表示する。	ログが表示されることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
6	ログファイルの出力	ログ参照画面を開き、ログをダウンロードする。	ログファイルをダウンロードできることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
7	ログファイルの確認	ダウンロードしたログファイルを参照する。	ダウンロードしたログファイルを参照できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
9	バックアップファイルの出力	デジタルペンサーバにログインし、Dドライブにバックアップファイルがあることを確認する。	DBのバックアップファイルがデジタルペンサーバに出力されていることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
10	バックアップファイルの上書き確認	DB情報画面を開き、バックアップを取得する。 デジタルペンサーバにログインし、Dドライブのバックアップファイルが上書きされていることを確認する。	デジタルペンサーバのDBバックアップファイルが上書きされることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
11	バックアップファイルの移動の確認	デジタルペンサーバにログインし、バックアップファイルを別フォルダに移動する。	DBバックアップファイルが規定の格納場所から移動できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
12	ユーザの登録確認	ユーザー設定画面を開き、ユーザ情報を確認して、ユーザ情報を取り込む。	ユーザー設定画面で、ユーザ情報を登録できることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
13	ログアウト	ログアウトする。	ログアウトできることを確認する。	2014/3/23	○	○	○	○	○	○	○	○

■システム

項番	シナリオ	概要	確認内容	確認日	大阪大学	成育医療	東京女子大	慶応大学	医科研病院	京大IPS研	京大再生研	神戸理研
					判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）	判定（○/×）
1	apacheのサービス確認	デジペンサーバにログインし、サービスを開き、apacheのサービスが自動で起動していることを確認する。	デジタルペンサーバにapacheのサービスが登録されていることを確認する。 Apacheのサービスが自動起動に設定されていることを確認する。	2014/3/20	○	○	○	○	○	○	○	○
2	MySQLのサービス確認	デジペンサーバにログインし、サービスを開き、MySQLのサービスが自動で起動していることを確認する。	デジタルペンサーバにMySQLのサービスが登録されていることを確認する。 MySQLのサービスが自動起動に設定されていることを確認する。	2014/3/20	○	○	○	○	○	○	○	○
3	環境変数の確認	デジペンサーバにログインし、環境変数にPHPのパスが設定されていることを確認する。	デジタルペンサーバの環境変数pathにPHPのインストールフォルダが登録されていることを確認する。	2014/3/20	○	○	○	○	○	○	○	○
4	タスクスケジューラの動作確認	デジペンサーバに「実験ノート取得用タスク」を設定し、起動することを確認する。	タスクが実行されることを確認する。	2014/3/23	○	○	○	○	○	○	○	○
5	LDAPの設定変更確認	基盤システムのLDAPにペンIDを登録できたことを確認する。	基盤システムのLDAPを確認して、localityname要素にペンIDを登録できることを確認する。	2014/3/20	○	○	○	○	○	○	○	○

８．セキュリティ対策資料

仕　様　書

「幹細胞関連情報の基盤システム」に係る

情報セキュリティポリシー構築支援業務

平成 25 年 10 月

東京大学医科学研究所

1. 件名　　「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ポリシー構築支援業務

2. 背景

「幹細胞関連情報の基盤システム」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」の参加者が互いに未発表の実験データ等を相互貢献の精神に基づき、その上で共有することによって、各自の研究の効率化をはかり、実験手法等の標準化を推進し、データマイニング等のIT技術によりデータを横断的に解析することで新たな発見を促進することを第一の目標とし、さらに、共有されたデータのうちで合意できたものを順次一般公開していくことで、参加者以外の研究者等にも便宜を与え、広くわが国における再生医療の臨床実用化を加速することを第二の目標として、導入しているものである。

3. 目的

「幹細胞関連情報の基盤システム」において、研究情報の漏えい、滅失、毀損を予防というセキュリティ強化が必要であると同時に、再生医療の臨床実用化の加速を実現するため、利用者の利便性と研究データの共有促進を確保できるセキュリティポリシーの策定が必要であり、セキュリティ対策の本格的運用に向けた準備を行う必要があるため、業務委託を行うものである。

4. 業務内容及び提案書について

以下は業務内容のリストである。提案書にはそれぞれの実現方法、手順、成果物、スケジュールについての記述を含めること。また全体の業務遂行体制、見積もり金額を記述すること。

(1) ヒアリング等による基盤システムの業務状況と既存運用ルールの把握。
(2) 現状の問題点、リスク、課題の把握・整理。
(3) 策定作業方針、進め方、ポリシーの全体像と構成検討、
(4) 文書体系の検討、記述レベルの調整・決定。
(5) ポリシー文書全体の策定
(6) 策定されたポリシーに基づいた運用開始と継続のプランの作成。
(7) 事故対応体制と行動指針の確立に向けたプランの作成。

5. 提案書及び見積書の提出期限　平成25年10月25日（金）

6. 業者選定方法について

5.の提出期限までに提出された提案書及び見積書を比較検討し、決定するものとする。

7. 実施期間　　平成25年11月1日～平成26年3月21日
なお、実施期間中は、東京大学医科学研究所機能解析イン・シリコ分野との連絡調整を行うこと、またセキュリティに関する質問への対応や問題への対処、およびポリシーに基づく運用の開始と継続のための支援を行うこと。

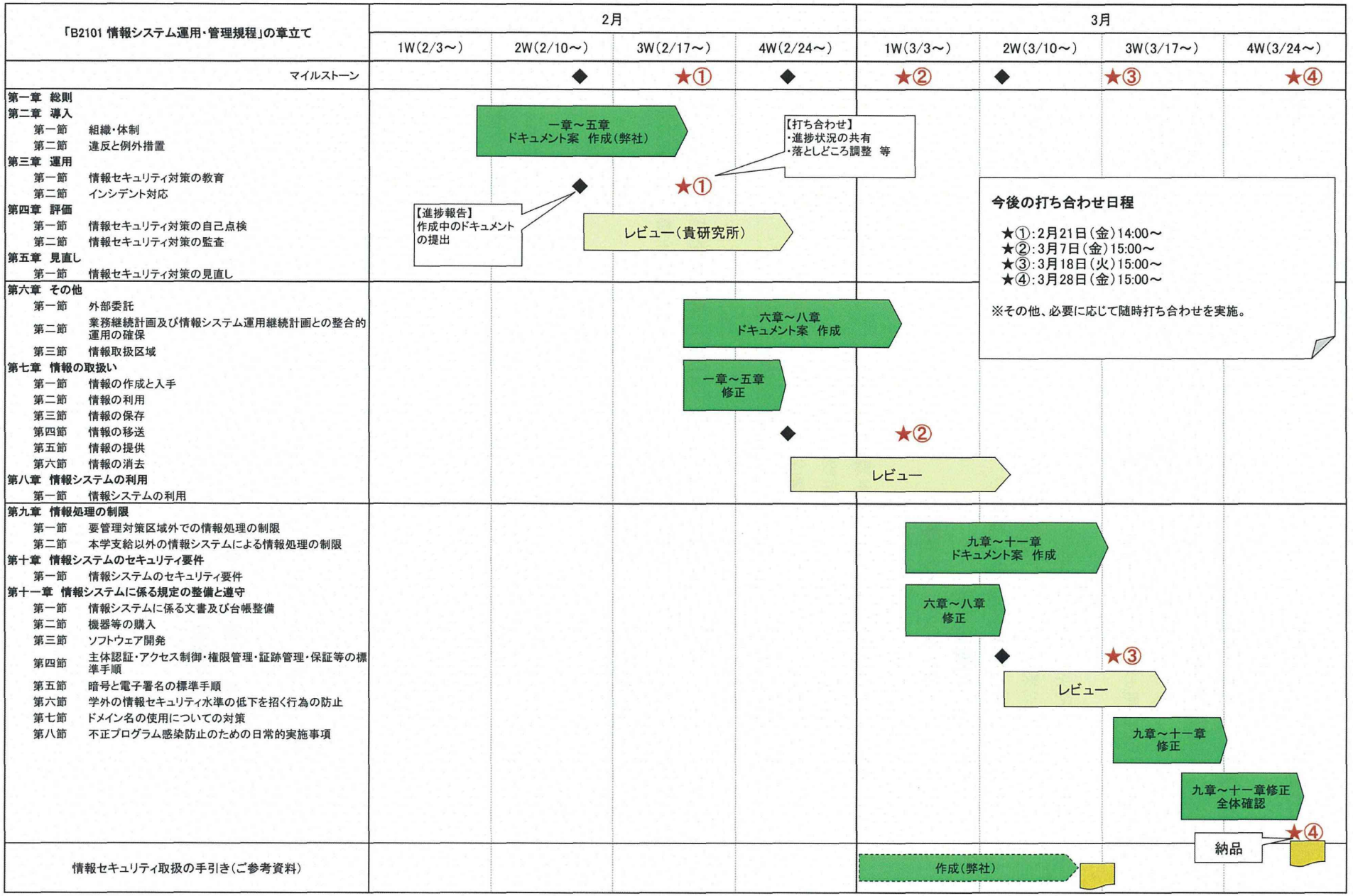
8. 成果物及び業務完了報告について
実施期間内に成果物として以下の資料を提出すること。
(1) 検討資料（契約後1ヶ月以内に提出のこと）
- 現状の課題/問題点一覧
- ポリシー整備プランニング資料

(2) 規定・基準、手順等（業務完了時）
- 基盤システム運用の基本方針と基本規程
- 基盤システム運用・管理規定（対策規程・基準）
（なお、基盤システムのシステム構成、アセット、アカウントの最新の状況を持続的に把握できるような仕組みの実現方法についても記述すること）

成果物について、受注者の検査を受けたうえで、業務完了報告書を提出すること。また、検査を受けた後、業務完了の翌月の5日までに、受注者は請求書を受注者に提出し、発注者は業務完了の翌月の25日に銀行振込を行う。

9. 特記事項
（1） 基盤システム上で行われるデータ共有方法に関しては『参考資料: 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』を参照のこと。
（2） 業務を実際の運用開始と継続の可能性に結びつく形で実行すること。
（3） 本業務に係わった全ての者は、本業務で知り得た事項について、守秘義務を負うこと。なお、必要であれば、協議のうえ、本契約とは別に秘密保持契約を締結することができる。
（4） 本事業に係る知的財産に係る業務が発生した場合には、発注者にすみやかに相談を行うこと。
（5） 本仕様書に記載のない事項について、定める必要がある場合には、発注者と受注者とが協議のうえ定めるものとする。

規程作成スケジュール


「B2101 情報システム運用・管理規程」の章立て
2月
3月
1W(2/3～)
2W(2/10～)
3W(2/17～)
4W(2/24～)
1W(3/3～)
2W(3/10～)
3W(3/17～)
4W(3/24～)
マイルストーン
★①
★②
★③
★④
第一章 総則
第二章 導入
第一節 組織・体制
第二節 違反と例外措置
第三章 運用
第一節 情報セキュリティ対策の教育
第二節 インシデント対応
第四章 評価
第一節 情報セキュリティ対策の自己点検
第二節 情報セキュリティ対策の監査
第五章 見直し
第一節 情報セキュリティ対策の見直し
第六章 その他
第一節 外部委託
第二節 業務継続計画及び情報システム運用継続計画との整合的運用の確保
第三節 情報取扱区域
第七章 情報の取扱い
第一節 情報の作成と入手
第二節 情報の利用
第三節 情報の保存
第四節 情報の移送
第五節 情報の提供
第六節 情報の消去
第八章 情報システムの利用
第一節 情報システムの利用
第九章 情報処理の制限
第一節 要管理対策区域外での情報処理の制限
第二節 本学支給以外の情報システムによる情報処理の制限
第十章 情報システムのセキュリティ要件
第一節 情報システムのセキュリティ要件
第十一章 情報システムに係る規定の整備と遵守
第一節 情報システムに係る文書及び台帳整備
第二節 機器等の購入
第三節 ソフトウェア開発
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
第五節 暗号と電子署名の標準手順
第六節 学外の情報セキュリティ水準の低下を招く行為の防止
第七節 ドメイン名の使用についての対策
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
一章～五章
ドキュメント案 作成(弊社)
【打ち合わせ】
・進捗状況の共有
・落としどころ調整 等
【進捗報告】
作成中のドキュメントの提出
レビュー(貴研究所)
今後の打ち合わせ日程
★①:2月21日(金)14:00～
★②:3月7日(金)15:00～
★③:3月18日(火)15:00～
★④:3月28日(金)15:00～
※その他、必要に応じて随時打ち合わせを実施。
六章～八章
ドキュメント案 作成
一章～五章
修正
レビュー
九章～十一章
ドキュメント案 作成
六章～八章
修正
レビュー
九章～十一章
修正
九章～十一章修正
全体確認
納品
情報セキュリティ取扱の手引き(ご参考資料)
作成(弊社)

幹細胞関連情報の基盤システムの情報セキュリティに係わるヒアリング項目

●基盤システムの運用管理体制の確認（東京大学医科学研究所様へのヒアリングを想定）

組織体制	本研究の関係者の名称と役割
	各要員の人数
	各要員の登録・変更・削除手続き
	ELSI委員会の役割
データ	取り扱うデータの種類
	情報の分類（L1～L5）と取り扱うデータの紐付け
	分類ごとのデータの保管場所
	情報提供のプロセス、データ登録
	情報分類（共有レベル）の変更手続き
	情報分類（共有⇒公開）の変更手続き
セキュリティ	管理者アカウントの管理
	アカウントの登録・削除・管理
	全体ネットワーク構成
	専用端末の貸し出し管理、保守、返却
	ネットワーク機器、ケーブルの秘匿
	外部ネットワークへの接続

●基盤システム利用者のセキュリティ対策状況の確認（拠点担当者様へのヒアリングを想定）

組織体制	情報管理者、作業分担者の任命・罷免手続き
	宣誓書の取り扱い
情報管理者	アカウントの登録・削除・管理
	ID,パスワード管理
	アクセス権の登録・変更・削除
	二次利用者のルール違反時の手続き
データ提供者	情報提供のプロセス、データ登録
二次利用者	情報の利用手順、ダウンロード
	電子データの複製、保管、持ち出し、伝送、破棄
	紙ファイルの複製、保管、保管、持ち出し、送付、破棄
	利用する媒体（USBメモリーなどの記憶媒体、タブレット、デジタルペン、紙　等）
	外部ネットワークへの接続
セキュリティ	専用端末の設置状況
	クライアント端末の種類（ノートPC、デスクトップPC、タブレットPC…）
	クライアント端末へのアクセス制御
	クライアント端末のログの取得状況
	クライアント端末のバックアップ
	クライアント端末の脆弱性対応、パッチ適用
	クライアント端末のウイルス対策、
	保管データの暗号化
	ソフトウェアの導入ルール
	専用端末が設置された室への入退室管理
	機器の盗難対策、書類の施錠管理
	拠点のネットワーク構成
	機器の保守、廃棄・返却

●データセンターのセキュリティ対策状況の確認（日立様へのヒアリングを想定）

サーバ	サーバの種類
	バックアップの取得、冗長化構成
	サーバの保守、廃棄・返却
データセンターのスペック	サーバ設置区画への入退室管理
	電源、回線、空調、耐震、BCP、災害対策
	提供サービス（テープ交換、手順に基づいたオペレーション）
セキュリティ	データセンターのネットワーク構成
	ウイルス対策、脆弱性対応、IDS、IPS等セキュリティ対策
	監視、異常検出時の対応
	ネットワーク機器、ケーブルの秘匿

セキュリティポリシー構築にむけた現状報告

2013年 12月13日
セコムトラストシステムズ株式会社

1. 取り扱うデータの重要性

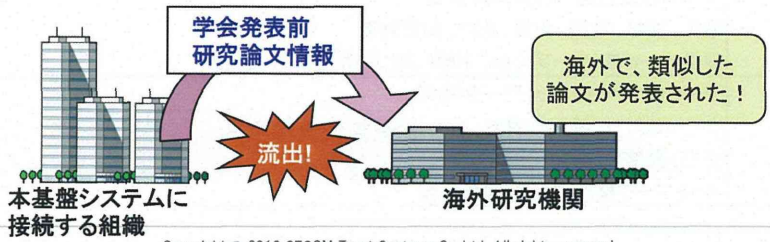
セキュリティポリシーの構築に当たって、本研究で提供される情報の重要性と取り扱いの要件について整理いたします。

本基盤システムにおいて取り扱う各種データは、相互貢献の精神に基づいて共有することにより研究の推進に寄与することが第一の目標。

とはいえ

研究データには、公開前データ（学会発表前研究論文関連情報、研究者関連情報）など、機密情報として扱うべき情報が多く含まれている。
研究が進むに従って、より高い機密性を確保すべき情報になる。

研究データは、**必要となる手続きなく外部に公開されないようセキュリティを確保すべき情報**として位置づける必要があります。

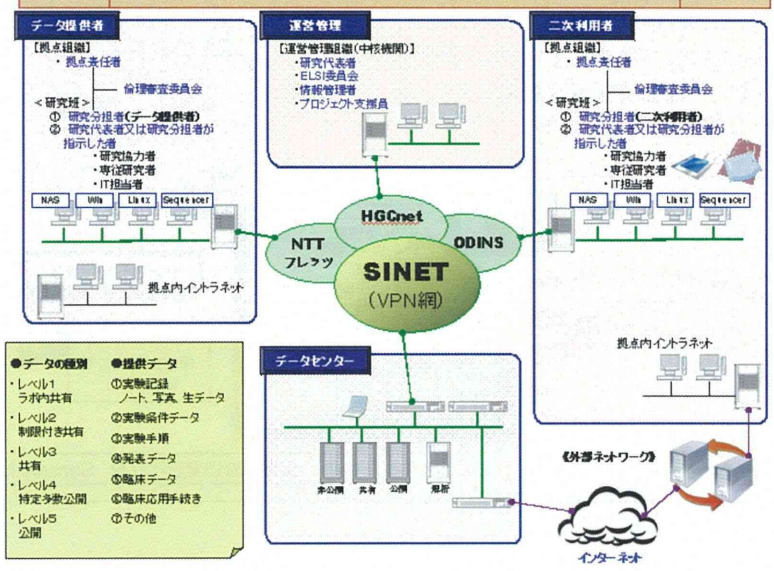


2. 本システムの基本的なセキュリティの考え方

取り扱うデータの重要性を踏まえ、研究データは次の3点を実現することが求められます。

① 基盤システム内でアクセスを制御（共有／限定）できること。
② 公開情報を除き、基盤システム内に限定して取り扱うこと。
③ 外部からのサイバー攻撃から防御できること。

システム基盤の概念図

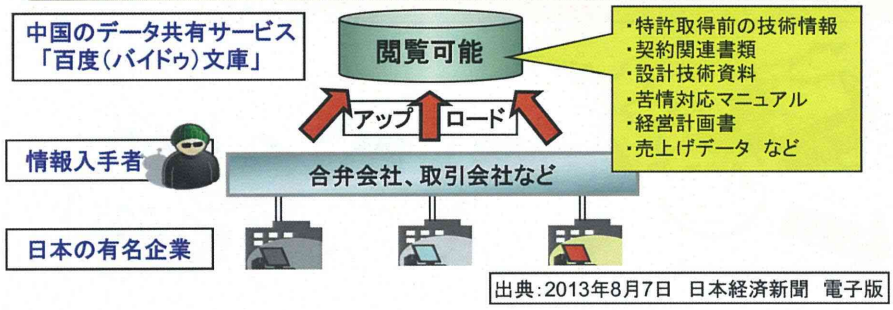


4. 事例研究①

日本企業の機密情報が大量に流出

大量の機密情報が閲覧可能に！

●日本の有名企業の重要機密が取引先を介して流出。
●流出した情報が中国のデータ共有サービスにアップロード。
●日本企業の機密情報がWEBで閲覧可能な状況に。



出典：2013年8月7日　日本経済新聞　電子版

4. 事例研究②

サイバー攻撃による情報の窃取

通信機器レンタル事業者
- ●WEBサーバに不正アクセス。
- ●データベースに保存されていたクレカ情報流出。
- ●クレジットカード会社からの指摘により、流出を認識。
- ●**約11万件の情報（名義、番号、セキュリティコード　等）が流出していた！**

この事例も、気付かぬうちに情報が流出。他社からの指摘で判明する事態に！

出典：2013年5月27日　Security NEXT

4. 事例研究③

海外への技術・品質の流出

海外で日本ブランドの模倣品（自動車、食品など）が横行
- ●日本の製品や技術が海外へ流出。
- ●模倣品による世界の**貿易被害額は年間25兆円！**
- ●模倣品は主に中国でつくられ、中近東を経て全世界に広がる。

技術や品質を確保する知的財産の保護が急務です！

出典：2013年11月18日　日本経済新聞　朝刊

4. 事例研究④

標的型進化、官公庁狙う、サイトに仕掛ける「水飲み場型」

官公庁に対する攻撃
- **複数の中央省庁**が新種のサイバー攻撃に狙われていた。
- 利用しそうなWebサイトにウイルスを仕掛けられている。
- 閲覧者のパソコンを感染させ、**遠隔で情報を抜き取られる**ようにしていた。

・標的組織のIPアドレスからの閲覧者だけが感染する工夫

・攻撃が露見するのを避け、対策を遅らせる。

出典:2013年10月10日　日経産業新聞

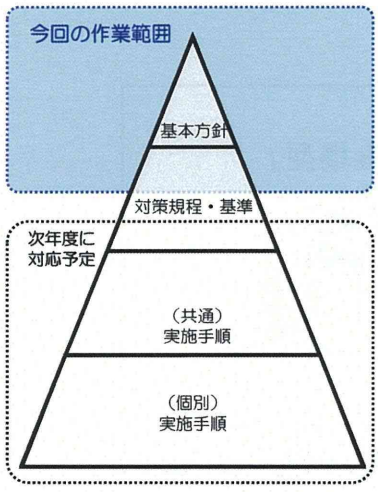
5. 情報セキュリティポリシーの策定に向けて

本研究の利便性とセキュリティの実現のトレードオフ。今後、最適なルールを検討いたします。

下表は、ルールを検討する際の考え方の一例です。

セキュリティ強度	提供データの取り扱い	課題	対応例	責任の所在
強	基盤システム内限定（システムで制御）	・制御するための仕組みの構築 ・利便性の阻害	・私有端末、媒体、外部NW接続の禁止 ・無線の利用停止・物理セキュリティの強化	基盤運営
	基盤システム内限定（一部ルールで制御）	・利便性の阻害 ・運用ルールの策定 ・ルールの遵守状況のチェック	・インターネット接続の制限 ・メールの検査 ・定期的な運用チェック・改善 ・NW接続時の審査基準の策定 ・審査の実施	基盤運営（ルール違反は、拠点側）
	基盤システム外への媒体による持ち出し	・拠点側のデータのセキュリティ確保 ・拠点側運用ルールの策定 ・ルールの遵守状況のチェック ・拠点側のセキュリティ教育 ・データ持ち出しの追跡	・持ち出し申請、審査 ・持ち出した情報の管理、切り分け ・ログの取得、採取、解析	持ち出した情報は拠点側
弱	基盤システム外へのNW接続による持ち出し		・WAF、IDS、IPSの導入・管理	持ち出した情報は拠点側（影響が大きいため例外措置）

6. 作業範囲と今後の予定



① 本ご提案の作業対象範囲として左図の青色部分を想定し、ポリシーの整備を実施します。

② ①で整備した規程に関わる共通手順の整備作業を展開します。個別手順については、必要に応じて整備を検討することとなります。

③ ①で整備を保留または内容を絞った規程、基準の整備作業を展開すると共に、①で整備済み規程、基準の対策レベルの向上を図ります。

④ 上流規程、基準の再整備に合わせて、手順の再整備作業及び新規手順の整備作業を展開します。

～2014年3月

2014年4月～

★ 以下のガイドライン・基準を考慮し、ポリシーの策定を行います。

・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
・NBDCヒトデータ各種ガイドライン
　＜共有ガイドライン、取扱いデータセキュリティガイドライン（利用者向け、データ提供者向け、データベースセンター向け）＞
・大学における情報セキュリティポリシーの考え方
・高等教育機関の情報セキュリティポリシーの策定について
・政府機関統一基準

End

ELSI1000　ヒト幹細胞関連情報の基盤システム運用基本方針

（情報システムの目的）

第一条　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。）の理念である、ヒト等の幹細胞を用いた再生医療技術の早期実用化に向け、再生医療に関わる我が国の研究機関が情報共有を図ることによって、All JAPAN体制で研究を加速させるための情報基盤の構築を目的とし、本プロジェクトに係るすべての研究活動及び運営の基盤として設置され、運用されるものである。

（運用の基本方針）

第二条　前条の目的を達するため、本基盤システムは、本プロジェクトで取り扱うヒト幹細胞の研究に関する情報を円滑で効果的な活用を図るために、以下の各号の定めを運用の基本方針とし、別に定める運用基本規程により、優れた秩序と安全性をもって安定的かつ効率的に運用され、本基盤システムを利用する者や運用に携わる者すべてに供用される。

一　取り扱う情報資産の重要性、機密性に鑑み、情報漏えい対策、不正アクセス対策、ウイルス対策、信頼性対策など、情報保護に対するセキュリティ対策を実施する。

二　情報セキュリティに関連する法令、国が定める規範又は契約上の義務ならびにセキュリティ上の要求事項に適合するための規則を策定し実行する。

三　本基盤システムにおける情報セキュリティ総括責任者を定め、情報セキュリティの維持、向上に取り組む。また、これらの取り組みを定期的に監査し、改善に努める体制を整備する。

四　業務を外部に委託する際には、セキュリティの面からも適格性を十分に審査したうえで委託先を選定し、セキュリティレベルを確保する。また、委託先のセキュリティレベルの状況を定期的に確認するとともに管理レベルの維持のための改善活動を推進する。

五　情報セキュリティインシデントの発生予防に努めるとともに、万一、事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じる。

六　本基盤システムを利用する者や管理に携わる者に対し、定期的な情報セキュリティに関する情報発信を行い、情報セキュリティの重要性、情報の適切な取り扱いに関し、周知・徹底を図る。

七　研究環境の変化、社会環境や法規制の変化、情報関連技術の最新動向および新たに発見されたリスクに照らし合わせて、本基本方針の適宜見直しを行い、継続的な改善を行う。

八　偶発的に発生する災害・故障・過失及び意図的に発生する情報資産の悪用などによる本基盤システムが提供するサービスの中断を可能な限り抑える。

（利用者の義務）

第三条　本基盤システムを利用する者や運用の業務に携わる者は、本方針及び運用基本規程に沿って利用し、別に定める運用と利用に関する実施規程を遵守しなければならない。

（利用の制限）

第四条　本方針に基づく規程等に違反した場合の利用の制限は、それぞれの規程に定めることができる。

附　則

本規程は、平成 XX 年 xx 月 xx 日から施行する。

ELSI1001　ヒト幹細胞関連情報の基盤システム運用基本規程

（目的）

第一条　本規程は、「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。）におけるヒト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。）の運用及び管理について必要な事項を定め、もって本プロジェクトの情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

（適用範囲）

第二条　本規程は、基盤システム利用者、並びに臨時利用者、運用管理に携わるすべての者に適用する。

（定義）

第三条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　基盤システム

以下に定める基幹システムと拠点追加機器をいう。

二　基幹システム

本プロジェクトにより、所有又は管理されているもので、データセンターおよび本プロジェクトが各拠点用に配置した機器及びネットワークをいう

三　拠点追加機器

各拠点機関で本プロジェクト遂行上必要とされ、導入された機器。

四　情報

本プロジェクトにおいて、情報は主にヒト幹細胞の研究に関する情報及びそれに付帯する情報を指すが、基盤システムに関する各種の設計書、定義情報、運用記録等もその対象とする。情報には次のものを含む。

(1)　基幹システム内部に記録された情報

(2)　基幹システム内部から外部の電磁的記録媒体にコピーされた情報

(3)　基幹システムに関係がある書面に記載された情報

(4)　基盤システム内部に記録された情報で、基幹システムの維持、運用に係る情報

五　ポリシー

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」及び「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。

六　実施規程

ポリシーに基づいて策定される規程及び、基準、計画をいう。

七　手順

実施規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

八　利用者

本プロジェクトが提供する基盤システムを利用する許可を受けた者または組織をいう。本プロジェクトの「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

一タ共有・公開に関するルールにおいて定義された研究代表者、研究分担者、中核機関、拠点機関、参加者、データ提供者、二次利用者を指す。

九　臨時利用者

外部委託事業者の要員など、基盤システムを臨時に利用する許可を受けて利用するものをいう。

十　情報セキュリティ

情報の機密性、完全性及び可用性を維持することをいう。

十一　電磁的記録

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で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

十二　障害

基盤システムの装置や回線、ソフトウエアなどに不具合が生じ、正常な稼働状態を維持できなくなること、およびその原因となった不具合をいう。

十三　インシデント

前号に定める障害及び情報セキュリティに関し意図的または偶発的に生じる、本プロジェクトの定める規程または法律に反する事故あるいは事件をいう。

（情報セキュリティ総括責任者）

第四条　基幹システムの運用に責任を持つ者として、本プロジェクトに情報セキュリティ総括責任者（以下「総括責任者」という。）を置く。本プロジェクトにおける研究代表者がその任を負う。

2　総括責任者は、ポリシー及びそれに基づく規程の決定や基幹システム上での各種問題に対する処置を行う。

3　総括責任者は、基幹システムの運用業務に携わる者及び利用者向け教育を推進する。

4　総括責任者は、総括責任者があらかじめ指名する者に、職務の一部を代行させることが出来る。

5　総括責任者に事故があるときは、総括責任者があらかじめ指名する者が、その職務を代行する。

6　総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くことができる。

（システム運用に係る審議及び実施）

第五条　基盤システムの円滑な運用のため、総括責任者は、次の各号に定める要員の参加のもと、システム運用に係る協議を行う。

一　実施責任者

二　技術責任者

三　情報セキュリティアドバイザーなど、総括責任者によって協議への参加を要請された者

2　総括責任者は、基盤システム運用に係る審議を経て、以下を実施する。

一　基盤システム運用リスクの管理、並びにその実施状況の把握

二　情報セキュリティ監査に係る規程の制定及び改廃、並びにその実施

三　基幹システム非常時の行動計画の制定及び改廃、並びにその実施
四　インシデントや障害の未然防止策および再発防止策の検討ならびにその実施
五　インシデントや障害発生時の対応指示の検討ならびにその実施
六　基幹システムの整備および運用に係る事案の承認
七　追加拠点機器の利用及び運用に係る事案の承認
八　その他、基盤システムの運用に必要となる規程、ガイドライン、計画の制定及び改廃、並びにその実施状況の把握

（実施責任者）
第六条　本プロジェクトの中核機関に実施責任者を置く。
2　実施責任者は、総括責任者が指名する。
3　実施責任者は、システム運用に係る協議に参加し、総括責任者を補佐する。
4　実施責任者は、総括責任者の指示により、基幹システムの整備と運用に関し、ポリシー及びそれに基づく規程並びに手順等の実施を行う。
5　実施責任者は、基幹システムの運用に携わる者及び利用者に対して、基幹システムの運用並びに利用及び基幹システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。
6　実施責任者は、追加拠点機器の利用及び運用に係る事案に関して、基幹システムの整備、運用及び本プロジェクトへの影響を確認する。
7　実施責任者は、基幹システムのセキュリティ、インシデント、障害に関する連絡と通報において基幹システムを代表する。

（技術責任者）
第七条　技術責任者は総括責任者が指名する。
2　技術責任者は、システム運用に係る協議に参加し、実施責任者および総括責任者を補佐する。
3　技術責任者は、総括責任者の指示により、基幹システムに係る技術的及び運用的実務を担当し、利用を支援する。
4．技術責任者は、追加拠点機器の利用及び運用に係る事案に関して、技術的及び運用的側面から評価し、追加拠点機器の利用を支援する。
5　技術責任者は、基幹システムに係るセキュリティ、インシデント、障害に関する連絡と通報を行う。

（情報セキュリティ監査責任者）
第八条 総括責任者は、情報セキュリティ監査責任者を置く。
2　情報セキュリティ監査責任者（以下「監査責任者」という）は、総括責任者の要請に基づき、監査に関する事務を統括する。

（プロジェクト支援チーム）←管理運営部局
第九条　総括責任者は、第五条に定める事項を円滑に運用するためにプロジェクト支援チームを定めることが出来る。
2　プロジェクト支援チームは、総括責任者がプロジェクト支援員として指名した者で構成する。

（プロジェクト支援チームが行う事務）
第十条　プロジェクト支援チームは、総括責任者の指示により、以下の各号に定める事務を行う。
一　基盤システムの運用と利用におけるポリシーの実施状況の取りまとめ
二　リスク管理及び非常時行動計画等の実施状況の取りまとめ
三　第五条の各号に関する規程、計画、手順等の素案及び懸案事項に係る改善案などの検討、策定
四　本プロジェクトに参加する組織との調整

（基盤システム利用の責任者）
第十一条 本プロジェクトに参加し、基盤システムを利用する各拠点は、その組織内に基盤システム利用の責任者（以下「利用の責任者」という）を置く。原則、拠点機関の研究分担者がその任を負う。

2　利用の責任者は、総括責任書の要請に基づき、拠点における基盤システムの利用に関し、ポリシー及びそれに基づく規程並びに手順等の実施を行い、権限に基づいた各種の申請、届出等を承認する。
3　利用の責任者は、ポリシー及びそれに基づく規程並びに手順等の遵守を自組織の利用者に対して指導する。
4　利用の責任者は、基盤システムのセキュリティ、インシデント、障害に関する連絡と通報において組織を代表する。

（役割の分離）
第十二条 情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
一　承認又は許可事案の申請者とその承認又は許可を行う者
二　監査を受ける者とその監査を実施する者

（情報の格付け）
第十三条 基盤システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備すること。

（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）
第十四条 総括責任者は、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。
2　基盤システムを運用・管理する者、並びに利用者は、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を講ずる。

（基盤システム運用の外部委託管理）
第十五条 総括責任者は、基盤システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講ずる。

（情報セキュリティ監査）

第十六条 情報セキュリティ監査責任者は、基盤システムのセキュリティ対策がポリシー（xxxx運用基本方針及び本規程）に基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める情報セキュリティ監査に係る規程等に従う。

（例外処理）

第　　条　本ポリシーに基づき定められる実施規程の適用が、本プロジェクト及び基盤システムの運用業務の適正な遂行を著しく妨げる等の理由により、実施規程とは異なる代替の方法を採用すること又は規程を実施しないことを認めざるを得ない場合の取り扱いについては、別途、例外処置に係る手順等に定める。

（見直し）

第二十三条　本ポリシー、実施規程及び手順は、見直しを行う必要性の有無を定期的または適時検討され、必要があると認められ場合にはその見直しが行われる。

２　基盤システムを運用・管理する者、並びにプロジェクトへの参加組織及びその利用者は、利用している基盤システムに対して自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

附　則

本規程は、平成 XX 年 xx 月 xx 日から施行する。