近畿大学医学部附属病院　治験事務局業務の電子化に関する標準業務手順書　変更対比表

項目	変更前（(第7版　平成29年9月5日）	変更後（第8版　平成30年6月4日）
表紙	作成日：平成28年 12月1日	作成日：平成30年 6月4日
p. 4 Ⅰ. 業務範囲	近畿大学医学部附属病院治験事務局(以下「治験事務局」という)業務に関して「サイボウズ社、デヂエ」を利用したシステムを使用する。 なお上記システムは、「近大臨床研究治験支援システム」KCTS（Kindai Clinical Trial Support　System）と命名した。治験依頼者(CRO を含む)の治験業務の効率化、迅速化、正確化を図ることを目的として「サイボウズ社、デヂエ」を利用したシステムとして運用、活用する。	近畿大学医学部附属病院治験事務局(以下「治験事務局」という)業務に関して「ファーマメディカルソリューション社製 治験・臨床研究支援システムCT-Portal」を利用したシステムを使用する。 なお上記システムは、「近大臨床研究治験支援システム」KCTS（Kindai Clinical Trial Support　System）と命名した。治験依頼者(CRO を含む)の治験業務の効率化、迅速化、正確化を図ることを目的として「ファーマメディカルソリューション社製 治験・臨床研究支援システムCT-Portal」を利用したシステムとして運用、活用する。
p. 5 Ⅱ. 近大臨床試験支援業務システムの運用に関する手順	7. KCTSのサーバは近大治験事務局内に設置したオンプレミスであり、サイボウズ社のリモートサーバを介してアクセスするが、外部にデータセンター及びクラウドサーバは使用しない。	7. KCTSのサーバは、データセンターに設置しており、すべてのユーザはインターネットを使用してアクセスするものとする。
p. 5～p. 9 Ⅲ.近大臨床研究治験支援システム KCTS	KCTS 安全対策の機能について記載する。 ・・・・・・・・・・ 12.　　利用可能時間	KCTS 安全対策の機能について記載する。 ・・・・・・・・・・ 12.　　利用可能時間

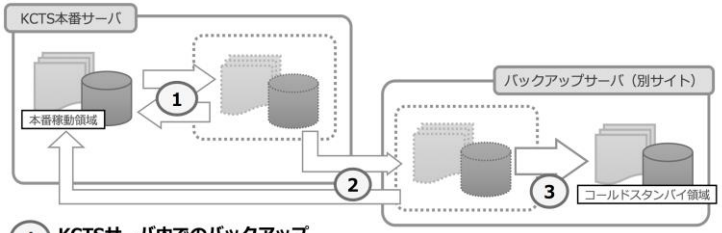
の安全対策に関する確認の手順	13.　システム監視	13.　システム監視 14.　システムの監査証跡
	1.通信経路の暗号化 128 bit SSLによりユーザが利用する PCと当該システムは、暗号化通信を行うため、情報を盗み取られることなく、安全に送受信することができる。	1.通信経路の暗号化 256 bit SSLによりユーザが利用する PCと当該システムは、暗号化通信を行うため、情報を盗み取られることなく、安全に送受信することができる。
	4.通信経路の制御 リモートサービスを利用するにあたり、各ユーザのPCにクライアント証明をインストールすることで、 システムにアクセス可能な端末もしくはネットワークを制御することができる。	4.通信経路の制御 各ユーザのPCにクライアント証明をインストールすることで、 システムにアクセス可能な端末もしくはネットワークを制御することができる。
	7. サーバ 当該システムは、近畿大学医学部附属病院内の施錠可能な場所に設置されており、当病院のみで占有されている。またデータはバックアップデータともに常に暗号化されている。	7.サーバ KCTSは、ISMS（ISO/IEC 27001）を取得したデータセンターに設置されている。
	10.データのバックアップ体制 利用者のデータは毎日バックアップを実施する。万が一、トラブルが発生した場合、速かにリカバ	10.データのバックアップ体制 KCTS本番サーバ内のデータ（データベースならびにPDF等の物理ファイル棟）は、以下に示す方法でバックアップおよ

	リーを実施する。 バックアップ装置はNAS によるRAID1 でのバックアップとする。バックアップの実施頻度は 週一回のフルバックアップ 月曜日から土曜日の01:00 から3 時間ごとの増分バックアップ 4 回の世代管理を実施 データの整合性はバックアップソフトのログにより確認することができる。 データのリストアについて バックアップソフトからの復元可能であり、復元前後での内容の整合性についてはバックアップソフトのログにより確認することができる。	びリカバリを行い、データを保全している。 ①KCTS本番サーバに直接接続されるバックアップ用ストレージおよび本番サーバを設置するデータセンターと物理的に離れたデータセンター（別サイト）に設置するバックアップサーバの２箇所にデータのバックアップを行っている。なお、バックアップは差分方式で３時間毎に自動で実行されている。（バックアップ・データの確認を定期的に目視で実施している。） ②システムの障害等でKCTS本番サーバにおいて、データのリカバリが必要な場合、上記２箇所のバックアップ・データを用いて、KCTS本番サーバのリカバリ（データのリストア）を行う。 ③災害・大規模な障害等の理由等で、KCTS本番サーバが長時間使用できない場合は、別サイトのバックアップサーバを稼働させることで、KCTSの利用を継続することができる。（ただし、バックアップサーバの稼働には、最短で２時間程度必要である。）
	13.システム監視 システム稼動状態の監視、ネットワークの監視等随時を行う。	13.システム監視 KCTSは、データセンターにおいて以下のシステム監視を行っている。

		①サーバの死活監視 ②サービスポートの状態監視 ③担当者による定期的なシステム確認 ④ネットワーク不正侵入検知 上記監視の報告により、喫緊の対応が必要な場合は、予め定められた手順に基づき、データセンターの担当者と連携し、適切かつ迅速な対応を行う。
	-	14.システムの監査証跡 KCTSは、システムの監査証跡として、以下のログを出力・保存している。 ①OSのシステムログ ②WEBサーバのアクセスログ ③データベースのアクセスログ ④アプリケーションのアクセスログ データの変更、削除に関して、すべての情報を履歴情報として保存しており、あらゆる使用状況において、データを上書きならびに削除が行えない仕様になっている。
p. 10	5. システム管理者は、近畿大学医学部附属病院にお	5. システム管理者は、近畿大学医学部附属病院における KCTS の

Ⅳ.システム管理者の任命・業務に関する手順	ける KCTS システムの実務責任者として、管理補助者へ直接業務の指示を行う。ただし、その範囲は「治験事務局支援業務委託契約書」による。	実務責任者として、管理補助者へ直接業務の指示を行う。
	6.システム管理者は、近畿大学医学部附属病院における KCTS システムの窓口として治験審査委員、治験依頼者（CRO を含む）等に対応する。	6.システム管理者は、近畿大学医学部附属病院における KCTS の窓口として治験審査委員、治験依頼者（CRO を含む）等に対応する。
p.11 Ⅴ.電磁記録の授受に関する手順	1.電磁記録受領手段について また、治験依頼者が DVD-R 等で電磁記録を提出した場合は、依頼者が作成した送付状に受領の旨記載し、FAX にて返信することで受領とする。	1.電磁記録受領手段について また、治験依頼者が DVD-R 等で電磁記録を提出した場合は、依頼者が作成した送付状に受領の旨記載し、FAX 等にて返信することで受領とする。
	2.電磁的手続きの責任者又は実務担当者について 電磁的記録の授受及び保管に関する責任者又は実務担当者は、以下の通りとする。 授受 （責任者：臨床研究センター長 実務 臨床試験センター研究管理者） 保管 （責任者：臨床研究センター長 実務 臨床試験センター研究管理者）	2.電磁的手続きの責任者又は実務担当者について 電磁的記録の授受及び保管に関する責任者又は実務担当者は、以下の通りとする。 授受 （責任者：臨床研究センター長 実務 臨床研究センター 治験管理部門管理者） 保管 （責任者：臨床研究センター長 実務 臨床研究センター 治験管理部門管理者）
	5. 保存中の機密性確保の対応について システムアクセスのためには ID、PW のみならず、デバイスにサイボウズ社が発行するクライアント	5.保存中の機密性確保の対応について システムアクセスのためには ID、PW のみならず、当該システム専用のクライアント証明をインストールする必要があり、また

	証明をインストールする必要があり、またユーザの権限設定により閲覧可能範囲を設定することで機密性を確保している。 治験依頼者が提出する DVD-R 等については治験依頼者が「電磁的記録のパスワード設定等による読み取り制限」を設定した上で提出し、受領・保存する。	ユーザの権限設定により閲覧可能範囲を設定することで機密性を確保している。 治験依頼者が提出する DVD-R 等については治験依頼者が「電磁的記録のパスワード設定等による読み取り制限」を設定した上で提出し、受領・保存する。
	7. 保存中の電磁的記録のリストアについて バックアップソフトからの復元可能であり、復元前後での内容の整合性についてはバックアップソフトのログにより確認を行う。	7. 保存中の電磁的記録のリストアについて バックアップソフトから復元可能であり、復元前後での内容の整合性についてはバックアップソフトのログにより確認を行う。
P. 13 VI. 資料の保存・管理に関する手順		3. 法的拘束力のある要求により、データの開示が求められた際には開示前に依頼者に連絡する。 4.KCTSで扱うデータの二次使用はしない。ただし契約内容に抵触しない範囲内で簡易的な治験実績を算出する目的でデータを使用することがある。
p. 16	-	《バックアップの仕組み》

<table>
<tr><td>別紙①</td><td></td><td> 

① KCTSサーバ内でのバックアップ
本番サーバでは、 3時間おきにローカルに設けたバックアップ領域へデータのコピーを行ないます。
本番サーバ稼動中の領域でデータの喪失があった場合は、コピーされたデータからの復旧を試みます。

② 別サイトのバックアップサーバへのデータ転送
本番サーバのバックアップデータは、3時間ごとに別サイトに設置したバックアップサーバへ差分を転送し、内容が同期された状態を保ちます。①のローカルデータから復旧が見込めない場合は、このバックアップ用データを本番サーバに転送してデータのリストアを試みます。

③ 別サイトのバックアップサーバの稼働（コールドスタンバイ機構）
別サイトには、バックアップシステムとして本番システムと同等レベルでサービス提供が可能なシステム環境（コールドスタンバイ）を保有しています。本番サーバもしくはネットワーク機器等の関連設備に障害が発生し、長時間に渡り本番環境の復旧が見込めない場合は、バックアップサーバを始動させることにより、サービスの提供を継続することが可能です。</td></tr>
<tr><td></td><td>－</td><td>《データセンターの概要》

KCTSは、「情報セキュリティマネジメントシステム(ISMS)」を取得した
安全な国内データセンターで、365日24時間有人監視の下、運用しております。

<table><tr><th>設備</th><th>内容</th></tr><tr><td>電源</td><td>・24時間365日安定供給
・無瞬断2回線ループ受電方式
・予備電源回線を更に装備
・停電時2台の非常用発電機によるバックアップ</td></tr><tr><td>セキュリティ</td><td>データセンター及びサーバールーム入館、入室時のIDカードを利用した二重チェック</td></tr><tr><td>耐震/防火/空調設備</td><td>・ビル全体が耐震構造
・IDCフロア耐震用フレーム構造
・消火用ハロゲンボンベ設置
・室内温度22（±2）度、湿度30（±5）%に常時設定</td></tr></table>
ISMSとは
財団法人日本情報処理開発協会（JIPDEC）が運営する適合評価制度の基準で、ISO（国際標準化機構）とIEC（国際電気標準会議）により策定された「情報セキュリティマネジメントシステム(ISMS)」の国際規格であり、情報セキュリティ対策のみならず、組織全体に渡ってセキュリティ管理体制を構築・監視し、リスクマネジメントを実施することで、企業が保護すべき情報資産の「機密性」「可用性」「完全性」をバランスよく維持し改善していくことを要求するものです。</td></tr>
<tr><td>p. 17</td><td>－</td><td>《セキュリティ対策》</td></tr>
</table>

<table>
<tr><td rowspan="2">別紙②</td><td></td><td>
<table>
<tr><th>想定される脅威</th><th>対策</th><th>対策内容</th></tr>
<tr><td>①サーバへの物理的な侵入</td><td>データセンターの設備</td><td>データセンターにおいて、非接触ICカードによる二重の入退室管理、監視カメラによる監視等、サーバ室内へ部外者が侵入できない対策を行っております。</td></tr>
<tr><td>②ネットワーク侵入</td><td>ファイアウォールの設置</td><td>ファイアウォールにより、ネットワークからの不正侵入を防いでおります。</td></tr>
<tr><td>③コンピュータ・ウィルス</td><td>ウィルス対策ソフトの導入</td><td>ウィルス対策ソフトを導入し、ウィルスによる脅威を防いでいます。ウィルスのパターンは、定期的にアップデートし、最新のウィルスに備えております。</td></tr>
<tr><td>④脆弱性攻撃</td><td>アプリケーションの脆弱性対策</td><td>次に代表されるようなアプリケーションの脆弱性対策を行い、脆弱性を狙った攻撃を防いでおります。
・SQLインジェクション、コマンドおよびHTTPヘッダインジェクションへの対応、
・ディレクトリトラバーサルへの対応
・データベースへの不正アクセスの対応
・セッション管理に関する対応
加えて、定期的にOSならびにミドルウェアの更新を行い、セキュリティホール対策を行います。</td></tr>
<tr><td>⑤盗聴</td><td>SSLによる暗号化通信</td><td>通信経路を暗号化することで、データの盗聴を防いでおります。</td></tr>
<tr><td>⑥不正ログイン</td><td>ログイン認証</td><td>ログイン時にユーザIDとパスワードによる認証を行います。パスワードを５回連続間違えた場合は、ログインができなくなります。</td></tr>
<tr><td>⑦他の試験情報の閲覧</td><td>研究毎のアクセス権限</td><td>アクセス権限のない試験情報（グループ）へアクセスできない環境を構築し、情報の秘匿性を担保しています。</td></tr>
</table>
</td></tr>
<tr><td>－</td><td>《脆弱性攻撃に対する対応》

■SQLインジェクション、コマンドおよびHTTPヘッダインジェクションへの対応
プログラム内の共通ライブラリで、データのサニタイジングを行なう処理を行なっております。
外部から入力されたデータにつきましては、いかなる場合もこの処理を通過するように作成しています。

■ディレクトリトラバーサルへの対応
ファイルなどの参照につきましては、フレームワークを介してドキュメントルート配下ではない場所にあるファイルにアクセスしております。パスを直接指定してのアクセスは一切行なっておりません。

■データベースへの不正アクセスの対応
データベースサーバについては、ローカル内のWebアプリケーションからのみアクセス出来る権限を持たせたアカウントで運用しています。メンテナンス等についても、一度セキュアなリモートアクセス手段（SSH）で接続した上で行なうようにし、外部からの直接アクセスは遮断しております。

■セッション管理に関する対応
セッションIDはアクセスの都度異なるものを発行するようにし、外部への漏洩についてもアプリケーション側にて対策を施してあります。

■リモートからのアクセスに関する対応
遠隔作業については、SSHのみを用いるようにし、アクセス用TCPポートもデフォルト値から変更し、サーバ側で発行した証明書をインストールしたPCからのみアクセスできるようにしております。</td></tr>
<tr><td>作成年月日</td><td>2017 年 9 月 5 日</td><td>2018 年 6 月 4 日</td></tr>
</table>

近畿大学医学部附属病院

治験事務局業務の電子化に関する
標準業務手順書

第8版　　平成30年6月４日

目　次

略語一覧

CRO（Contract Research Organization）	開発業務受託機関
ID（Identification）	身分証
IRB（Institutional Review Board）	治験審査委員会
KCTS（Kindai Clinical Trial Support System）	近大臨床研究治験支援システム
NAS(Network Attached Strage)	ネットワークに直接接続して使用するファイルサーバ
PC（Personal Computer）	パーソナルコンピューター、パソコン
PW（Password）	パスワード
RAID1(Redundant Arrays of Inexpensive Disks 1)	同じデータを２本のハードディスクに書き込みすることで耐障害性を高めた構成
SOP（Standard Operating Procedure）SMO（Site Management Organization）	標準業務手順書治験施設支援機関
SSL（Secure Socket Layer）SOP（Standard Operating Procedure）	Internet上で情報を暗号化して送受信する通信規約標準業務手順書
URL（Uniform Resource Locator）SSL（Secure Socket Layer）	Internet上に存在する情報資源の場所を示す記述方式Internet上で情報を暗号化して送受信する通信規約
アクセスログ(LOG)URL（Uniform Resource Locator）	コンピュータの利用状況やデータ通信の記録をとること。またその記録Internet上に存在する情報資源の場所を示す記述方式
ユーザアカウント（User Account）アクセスログ(LOG)	利用者の口座（取引き）コンピュータの利用状況やデータ通信の記録をとること。またその記録
ユーザアカウント（User Account）	利用者の口座（取引き）

Ⅰ. 業務範囲

近畿大学医学部附属病院治験事務局(以下「治験事務局」という)業務に関して「ファーマメディカルソリューション社製 治験・臨床研究支援システムCT-Portal」を利用したシステムを使用する。

なお上記システムは、「近大臨床研究治験支援システム」KCTS（Kindai Clinical Trial Support System）と命名した。治験依頼者（CRO を含む）の治験業務の効率化、迅速化、正確化を図ることを目的として「ファーマメディカルソリューション社製 治験・臨床研究支援システムCT-Portal」を利用したシステムとして運用、活用する。

Ⅱ.近大臨床試験支援業務システムの運用に関する手順

1. 原資料は紙媒体であり、KCTSは治験事務の運用を効率化と円滑にするためのシステムである。

2. システム管理者は、システム管理者を補助する者（以下「管理補助者」という）と協力して治験事務局を支援する。

3. 治験依頼者（CROも含む）の担当者は、「治験支援システム利用許可申請書（以下「許可申請書」という）」に必要事項を記載のうえシステム管理者に提出する。治験事務局および管理補助者は、当該治験が近畿大学医学部附属病院のIRBで審議され、承認を得たことを確認する。

4. システム管理者は治験依頼者（CROも含む）のシステム利用者に対しユーザアカウントの払い出しを行う。なおシステム利用者は、１試験に対し１ユーザアカウントを原則とする。

5. システム管理者は、治験依頼者（CROも含む）の担当者にID、PW、およびシステムのHPアドレスをそれぞれ別々にメール配信する。

6. ２者間（近畿大学医学部附属病院長、治験依頼者）で、「治験支援業務におけるシステム利用に関する覚書」また、必要に応じて３者間（近畿大学医学部附属病院長、治験依頼者、CRO）で「治験支援業務におけるシステム利用に関する覚書」を取り交わす。治験依頼者は上記様式を臨床研究センターのHPより入手する。

7. KCTSのサーバは、データセンターに設置しており、すべてのユーザはインターネットを使用してアクセスするものとする。

Ⅲ.近大臨床研究治験支援システム KCTS（Kindai Clinical Trial Support System）の安全対策に関する確認の手順

近畿大学医学部附属病院（治験事務局）が臨床研究治験支援システム（以下「KCTS」という）を

導入し、治験依頼者（CROも含む）がそれを利用する際、最も考慮しなければならない問題として、情報の安全対策が挙げられる。この点に関してシステム管理者は以下のセキュリティ対策をすべての関係者に対して安全対策を徹底する様、あらゆる機会を通じて指導する。

なおセキュリティ対策について、システム管理者は必要に応じて追加・変更を行い、より安全性の高い KCTS とすべく努める。またセキュリティ対策について、追加・変更があった場合は、逐次関係者に 連絡するとともに、必要に応じて説明会を企画・実施し、その周知徹底を図る。

KCTS 安全対策の機能について記載する。

1. 通信経路の暗号化
2. クライアント証明およびユーザIDとPWによるユーザ認証
3. アクセス権限の設定
4. 通信経路の制御
5. アクセスログ検索
6. メール通知
7. サーバ
8. リソースの多重化
9. コンピュータウィルス対策
10. データのバックアップ体制
11. メンテナンス
12. 利用可能時間
13. システム監視
14. システムの監査証跡

（詳細は以下に記載）

1. 通信経路の暗号化

256 bit SSLによりユーザが利用するPCと当該システムは、暗号化通信を行うため、情報を盗み取られることなく、安全に送受信することができる。

2. クライアント証明およびユーザIDとPWによるユーザ認証

利用者が当該システムを利用するためには、システム管理者よりクライアント証明の発行を受け、ユーザIDとPWの提供を受ける必要がある。利用者はユーザのPCにクライアント証明をインストールし、ユーザ IDと PWによるユーザ認証をおこなうことにより、当該システムを利用することができる。

（ア） 利用者は、「治験支援システム利用許可申請書」を作成のうえ、システム管理者にユーザIDとPW の発行を依頼する。

（イ） システム管理者は、内容を確認のうえ利用者にクライアント証明およびユーザIDとPWをメールで送る。なおクライアント証明およびユーザIDと PWは、セキュリティの観点から、別々にメールする。

（ウ） 利用者は、クライアント証明をインストールしたPCでブラウザを起動し、ユーザIDと PWを入力して当該システムにログインする。

3. アクセス権限の設定

各ユーザIDには、利用者の役割・立場に則したアクセス権限の設定を行うことができる。アクセス権限は、以下のとおりに大別される。

① 「プロトコール単位による制御（プロトコールにアクセスできるか否か）」

② 「各機能単位による制御（当該機能が利用できるか否か）」

に大別される。

この２つの権限を組み合わせることにより、利用者に対して、きめ細かいアクセスコントロールを行うことができる。

4. 通信経路の制御

各ユーザのPCにクライアント証明をインストールすることで、 システムにアクセス可能な端末もしくはネットワークを制御することができる。

5. アクセスログ検索

当該システムは、利用者のシステム上での登録・変更・削除・参照等をアクセスログ検索として記録する。システム管理者は、検索によりアクセスログを確認することができる。

6. メール通知

当該システムは、電子メールを利用し、システム上の情報更新を関係者に通知する機能（システムにより電子メールが発信される）が搭載されている。通知メールの本文には、当該情報にアクセスするための URL が搭載され、利用者はユーザ認証を行った上で、必要な情報にアクセスすることが可能となる。

（電子メールは暗号化されていない平文でインターネット上を流れるため、情報漏えいのリスクが高いため、この方法を採用している。）

7. サーバ

KCTSは、ISMS（ISO/IEC 27001）を取得したデータセンターに設置されている。

8. リソースの多重化

当該システムに使用するサーバ機器、ネットワーク機器、回線、電源等はすべて多重化しており、障害に強いシステム構造をしている。加えて使用する機材は、製造メーカと保守契約を締結し、万が一のトラブルにも迅速に対応できる体制を整えている。

9. コンピュータウィルス対策

電子ファイルの入出力を行うサーバには、ファイヤーウォール及びコンピュータウィルス駆除ソフトを導入している。

ウィルスの定義ファイルの自動更新、週一回のフルスキャンを実行している。

10. データのバックアップ体制

KCTS本番サーバ内のデータ（データベースならびにPDF等の物理ファイル棟）は、以下に示す方法でバックアップおよびリカバリを行い、データを保全している。

①KCTS本番サーバに直接接続されるバックアップ用ストレージおよび本番サーバを設置するデータセンターと物理的に離れたデータセンター（別サイト）に設置するバックアップサーバの２箇所にデータのバックアップを行っている。なお、バックアップは差分方式で３時間毎に自動で実行されている。　（バックアップ・データの確認を定期的に目視で実施している。）

②システムの障害等でKCTS本番サーバにおいて、データのリカバリが必要な場合、上記２箇所のバックアップ・データを用いて、KCTS本番サーバのリカバリ（データのリストア）を行う。

③災害・大規模な障害等の理由等で、KCTS本番サーバが長時間使用できない場合は、 別サイトのバックアップサーバを稼働させることで、KCTSの利用を継続するこ

とができる。（ただし、バックアップサーバの稼働には、最短で２時間程度必要である。）

11. メンテナンス

メンテナンスを行うことで、安定運用を図る。メンテナンスでは、ソフトウエアのセキュリティパッチ適応、バグ修正、ハードウエア交換等を実施する。メンテナンス日は、７日前に通知する。

なおシステムの安全性上、重大な問題が発生した際は、利用者へ通知した上で、不定期のメンテナンスを実施する。システムに蓄積される情報の機密性、インターネット経由でアクセスするシステムの特性を考慮して安全最優先で運用する。

12. 利用可能時間

利用者のインターネットによるシステムへのアクセスは24時間可能とするが、 治験事務局の受付は平日の09:00から17:00までとし、それ以後のアクセスによる申請事項については翌日の取扱いとする。 また土日、祝祭日、年末年始にアクセスした情報の受付は休み明けの取扱いとする。

13. システム監視

KCTSは、データセンターにおいて以下のシステム監視を行っている。

①サーバの死活監視

②サービスポートの状態監視

③担当者による定期的なシステム確認

④ネットワーク不正侵入検知

上記監視の報告により、喫緊の対応が必要な場合は、予め定められた手順に基づき、データセンターの担当者と連携し、適切かつ迅速な対応を行う。

14. システムの監査証跡

KCTSは、システムの監査証跡として、以下のログを出力・保存している。

①OSのシステムログ

②WEBサーバのアクセスログ

③データベースのアクセスログ

④アプリケーションのアクセスログ

データの変更、削除に関して、すべての情報を履歴情報として保存しており、あらゆる使用状況において、データを上書きならびに削除が行えない仕様になっている。

Ⅳ.システム管理者の任命・業務に関する手順

１．　システム管理者は、管理補助者に運用の補佐をさせる。

２．　システム管理者は、管理補助者と適宜連絡を取りKCTSの安全性対策および利便性向上について検討する。

３．　システム管理者はKCTSの支援内容の検討・見直しを逐次行う。

４．　システム管理者は、ユーザアカウントの割り当てを実施する。

５．　システム管理者は、近畿大学医学部附属病院におけるKCTSの実務責任者として、管理補助者へ直接業務の指示を行う。

６．　システム管理者は、近畿大学医学部附属病院における KCTSの窓口として治験審査委員、治験依頼者（CRO を含む）等に対応する。

７．　システム障害が発生した場合、システム管理者は急ぎ復旧作業を行う。

８．　利用したデータ等の保管および所有権は、すべて近畿大学医学部附属病院に帰属する。

Ⅴ．電磁記録の授受に関する手順

KCTS では、法令上で署名又は記名捺印等が求められる文書（契約書、合意書、Financial disclosure 等）ではない治験関連文書を運用する。

1. 電磁記録受領手段について

安全性情報においては、治験依頼者が KCTS の該当する試験データにアクセスし、安全性情報を登録することで、受領した旨の通知が KCTS より治験依頼者にメールされる。この一連の工程が終了した時点で受領が完成する。登録情報はシステムログに記録される。

また、治験依頼者が DVD-R 等で電磁記録を提出した場合は、依頼者が作成した送付状に受領の旨記載し、FAX 等にて返信することで受領とする。

2. 電磁的手続きの責任者又は実務担当者について

電磁的記録の授受及び保管に関する責任者又は実務担当者は、以下の通りとする。

授受　（責任者：臨床研究センター長　実務　臨床研究センター 治験管理部門管理者）

保管　（責任者：臨床研究センター長　実務　臨床研究センター 治験管理部門管理者）

3. 電磁的記録の取り扱いに関する教育について

各ユーザに対し、書面での案内または実地指導を行った場合には、日時、対象者名、内容を記載した記録を保存する。

4. 医療機関が電磁的記録を交付する際について

KCTS は、閲覧のみの運用であり電磁的記録の交付は行わない。

5. 保存中の機密性確保の対応について

システムアクセスのためには ID、PW のみならず、当該システム専用のクライアント証明をインストールする必要があり、またユーザの権限設定により閲覧可能範囲を設定することで機密性を確保している。

治験依頼者が提出する DVD-R 等については治験依頼者が「電磁的記録のパスワード設定等による読み取り制限」を設定した上で提出し、受領・保存する。

6. 保存中の電磁的記録を消去した際の事実検証について

システムによるログ記録にて検証する。

7. 保存中の電磁的記録のリストアについて

バックアップソフトから復元可能であり、復元前後での内容の整合性についてはバッ

クアップソフトのログにより確認を行う。

8. 電磁的記録を再現不可能な方法で破棄する対応の有無について

サーバ破棄、データの削除等の運用は病院システム運用管理規程に準拠する。

電磁的記録が保存された DVD-R 等を破棄する場合、その媒体はシュレッダーにて破棄処理する。

メールで受領した場合、メール自体の削除は行っていない。

KCTS に登録されたデータは、試験終了報告書の提出の一ヶ月後よりデータの閲覧不可とする処理を行っているが、データの削除については将来の当局調査での質問に対応する必要性を考慮し、サーバより削除することは現時点では実施していない。

しかしながら、終了した試験はシステム管理者以外閲覧不可にして守秘義務に配慮している。

9. 治験審査委員会審査時に電磁的記録を利用する場合の機密性確保について

治験審査委員会審査時において、電磁的記録は利用しない。

電子メール、DVD-R、閲覧デバイスでの配布は行わない。

審査時はシステムを利用せず、事前の審査資料を確認する場合に於いてはシステムの権限設定による利用範囲とすることで機密性を確保する。

10. 原データを含む文書（書式 8、12−１、12−2）における作成者の見解確認について

システムのログにより作成責任者の見解を確認する。

11. スキャンについて

紙原本が原資料となるデータにおいては､スキャン文書はあくまでも補助データとする。

Ⅵ. 資料の保存・管理に関する手順

１．KCTS業務に関連する契約書・覚書等（以下「記録等」という）は、適切な条件の下に保存する。

２．記録等の保存期間は、①又は②のうちいずれか遅い日までの期間とする。ただし、治験依頼者がこれより長期間の保存を必要とする場合には、保存期間及び保存方法について協議決定する。

① 被験薬に係る医薬品製造販売承認日（GCP省令第24条第３項の規定により通知を受けたときは、通知を受けた日後３年を経過した日。）

② 治験の中止若しくは終了の後３年を経過した日

なお、製造販売後臨床試験については、再審査・再評価が終了する日までとする。

３．法的拘束力のある要求により、データの開示が求められた際には開示前に依頼者に連絡する。

４．KCTSで扱うデータの二次使用はしない。ただし契約内容に抵触しない範囲内で簡易的な治験実績を算出する目的でデータを使用することがある。

Ⅶ. SOP改訂に関する手順

本標準業務手順書（SOP）改訂に関しては以下の手順に従って行う。

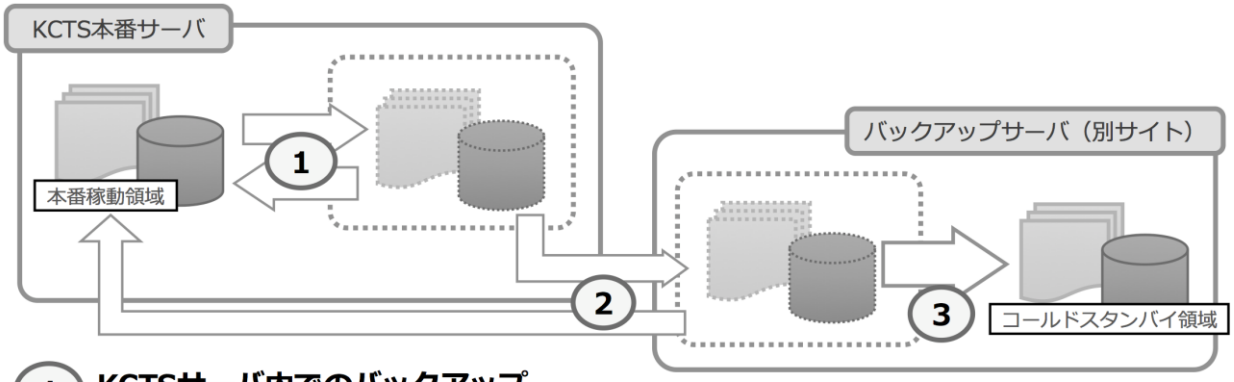
1. SOPは現状に照らし合わせ必要時に随時改訂をする。
2. SOP改訂項目に関する内容の変更は、近畿大学医学部附属病院およびシステム管理者が案を作成する。
3. 近畿大学医学部附属病院治験事務局が、SOP改訂について内容確認を行う。
4. 上記の改訂 SOPは、近畿大学医学部附属病院治験審査委員会の承認日を持って採用・ 実行される。

以上

附記　1）平成22年11月29日、治験審査委員会に於いて手順書として定めることを決定した。
2）平成23年4月1日改訂
3）平成23年6月1日改訂
4）平成26年11月25日改訂
5）平成28年4月1日改訂
6）平成28年12月1日改訂
7）平成29年9月5日改訂
8）平成30年6月4日改訂

本手順書の内容は臨床研究センター長が責任を負う。

【別紙①】
《バックアップの仕組み》



1 KCTSサーバ内でのバックアップ

本番サーバでは、 3時間おきにローカルに設けたバックアップ領域へデータのコピーを行ないます。
本番サーバ稼動中の領域でデータの喪失があった場合は、コピーされたデータからの復旧を試みます。

2 別サイトのバックアップサーバへのデータ転送

本番サーバのバックアップデータは、３時間ごとに別サイトに設置したバックアップサーバへ差分を転送し、内容が同期された状態を保ちます。①のローカルデータから復旧が見込めない場合は、このバックアップ用データを本番サーバに転送してデータのリストアを試みます。

3 別サイトのバックアップサーバの稼働（コールドスタンバイ機構）

別サイトには、バックアップシステムとして本番システムと同等レベルでサービス提供が可能なシステム環境（コールドスタンバイ）を保有しています。本番サーバもしくはネットワーク機器等の関連設備に障害が発生し、長時間に渡り本番環境の復旧が見込めない場合は、バックアップサーバを始動させることにより、サービスの提供を継続することが可能です。

《データセンターの概要》

KCTSは、「情報セキュリティマネジメントシステム(ISMS)」を取得した安全な国内データセンターで、365日24時間有人監視の下、運用しております。

設備	内容
電源	・24時間365日安定供給 ・無瞬断2回線ループ受電方式 ・予備電源回線を更に装備 ・停電時2台の非常用発電機によるバックアップ
セキュリティ	データセンター及びサーバールーム入館、入室時のIDカードを利用した二重チェック
耐震/防火/空調設備	・ビル全体が耐震構造 ・IDCフロア耐震用フレーム構造 ・消火用ハロゲンボンベ設置 ・室内温度22（±2）度、湿度30（±5）%に常時設定

ISMSとは

財団法人日本情報処理開発協会（JIPDEC）が運営する適合評価制度の基準で、ISO（国際標準化機構）とIEC（国際電気標準会議）により策定された「情報セキュリティマネジメントシステム(ISMS)」の国際規格であり、情報セキュリティ対策のみならず、組織全体に渡ってセキュリティ管理体制を構築・監視し、リスクマネジメントを実施することで、企業が保護すべき情報資産の「機密性」「可用性」「完全性」をバランスよく維持し改善していくことを要求するものです。

【別紙②】
《セキュリティ対策》

想定される脅威	対策	対策内容
①サーバへの物理的な侵入	データセンターの設備	データセンターにおいて、非接触ICカードによる二重の入退室管理、監視カメラによる監視等、サーバ室内へ部外者が侵入できない対策を行っております。
②ネットワーク侵入	ファイアウォールの設置	ファイアウォールにより、ネットワークからの不正侵入を防いでおります。
③コンピュータ・ウィルス	ウィルス対策ソフトの導入	ウィルス対策ソフトを導入し、ウィルスによる脅威を防いでいます。ウィルスのパターンは、定期的にアップデートし、最新のウィルスに備えております。
④脆弱性攻撃	アプリケーションの脆弱性対策	次に代表されるようなアプリケーションの脆弱性対策を行い、脆弱性を狙った攻撃を防いでおります。 ・SQLインジェクション、コマンドおよびHTTPヘッダインジェクションへの対応、 ・ディレクトリトラバーサルへの対応 ・データベースへの不正アクセスの対応 ・セッション管理に関する対応 加えて、定期的にOSならびにミドルウェアの更新を行い、セキュリティホール対策を行います。
⑤盗聴	SSLによる暗号化通信	通信経路を暗号化することで、データの盗聴を防いでおります。
⑥不正ログイン	ログイン認証	ログイン時にユーザIDとパスワードによる認証を行います。パスワードを５回連続間違えた場合は、ログインができなくなります。
⑦他の試験情報の閲覧	研究毎のアクセス権限	アクセス権限のない試験情報（グループ）へアクセスできない環境を構築し、情報の秘匿性を担保しています。

《脆弱性攻撃に対する対応》

■SQLインジェクション、コマンドおよびHTTPヘッダインジェクションへの対応
プログラム内の共通ライブラリで、データのサニタイジングを行なう処理を行なっております。
外部から入力されたデータにつきましては、いかなる場合もこの処理を通過するように作成しています。

■ディレクトリトラバーサルへの対応
ファイルなどの参照につきましては、フレームワークを介してドキュメントルート配下ではない場所にあるファイルにアクセスしております。パスを直接指定してのアクセスは一切行なっておりません。

■データベースへの不正アクセスの対応
データベースサーバについては、ローカル内のWebアプリケーションからのみアクセス出来る権限を持たせたアカウントで運用しています。メンテナンス等についても、一度セキュアなリモートアクセス手段（SSH）で接続した上で行なうようにし、外部からの直接アクセスは遮断しております。

■セッション管理に関する対応
セッションIDはアクセスの都度異なるものを発行するようにし、外部への漏洩についてもアプリケーション側にて対策を施してあります。

■リモートからのアクセスに関する対応
遠隔作業については、SSHのみを用いるようにし、アクセス用TCPポートもデフォルト値から変更し、サーバ側で発行した証明書をインストールしたPCからのみアクセスできるようにしております。