項番	発生日	分類	課題 ※課題本文＝太字	検討日	実証実験仕様（決定事項）	規格化検討課題（未決定事項）	備考・進捗状況
13	2015/2/20	ODM	**・ODMに関する知見の集約を図る必要がある。** 【ディスカッション】 ・厚労科研仕様案としてのスタンスの元、推奨案を決定する必要がある。 ・各ベンダが受付可能と思われるODM形式にしておく必要がある。 ・できるだけ各ベンダが対応しやすいように「知見」を明らかにしていく。 ・現時点では、EDCベンダのAPI仕様としては使えるタグ一覧のような情報は入手できているが、実際動いているプロトコルのタグの使われ方、作りこみ、決めの部分の情報がわからない。	2015/2/20	（実証範囲外）	（要検討） ・直接的に、EDCベンダーにデータ構造の詳細情報を頂くべきか？ 製薬協のメンバーに実例ODMを出して頂けないか？ （OIDのつけ方、エイリアスの定義など）	⇒製薬協に協力依頼、まずは利用状況について「アンケート」
14	2015/2/20	通信	**・通信でEDC側と行う「認証」方式とODMの中で書き込むことの可能な「ユーザー情報」や「署名情報」の使い分けを明確に行う必要がある。** 【ディスカッション】 ・代理送信の件、データ作成者の情報をODMに書き込む必要があるか。 ・トランスポート（たとえばHTTP）とメッセージ（たとえばSOAP）の中での認証。 ・署名の意味合い。 ・最初に送ったユーザーと修正ユーザーの管理をどうするか。 ・技術的な問題というよりか、運用の問題ではないか。 ・医者がはんこを押す前後のワークフローについて、複雑なトランザクション認証制御の設定（CRCあるいは医師らの権限をプロトコルごとに決めること）は難しいのではないか。	2015/2/20	実証実験の認証については最低限のHTTP Basic認証＋HTTPSとする	（要検討）	
15	2015/3/6	通信	**・データ送信時に試験（Study）の指定が可能と思われる箇所が複数あるため、記述方法を決定する必要がある。** 【ディスカッション】 SOAP Endpoint Addressの場合 例: http://www.hp-info.med.osaka-u.ac.jp/crit/TestStudy SOAP メソッド引数の場合 例: EnrollSubject(String studyOid, String subjectKey) ODM Study OIDの場合 例: <ODM ...>　　<Study OID="TestStudy">		（実証範囲外）	（要検討）	
16	2015/3/6	ODM	**・ODM上に責任医師を記述する場合、どこに記述すべきかを決める必要がある。** 【ディスカッション】 ODM AuditRecord 要素に記述　↓ODM Reference 3.1.4.1.2　AuditRecord An AuditRecord carries information pertaining to the creation, deletion, or modification of clinical data. This information includes who performed that action, and where, when, and why that action was performed. 複数の責任医師の場合が居る場合はどうするか。		（実証範囲外）	（要検討）	

項番	発生日	分類	課題 ※課題本文＝太字	検討日	実証実験仕様（決定事項）	規格化検討課題（未決定事項）	備考・進捗状況
17	2015/3/6	ODM	**・ODMの変更理由要素の使い方を検討する必要がある。** 【ディスカッション】 ODM ReasonForChange 要素の使い方 修正時の理由を記載する項目として使うか。 3.1.4.1.2.3　ReasonForChange Body: text Attributes: NONE Contained in: AuditRecord A user-supplied reason for a data change.			（要検討）	
18	2015/3/6	ODM	**・ODM Annotation 要素の使い方を検討する必要がある。** 【ディスカッション】 電子カルテからの自動引用データか、手入力データかの区別に使用できるのではないか。 2.6　Entities and Elements … An annotation is a comment applied to a subject, study event, form, item group, or item. Annotations can also be applied to pairs of entities.			（要検討）	
19	2015/3/6	ODM	**・ODM Archival 属性の使い方を検討する必要がある。** 【ディスカッション】 The Archival attribute is optional.　※Referenceから Archival=Yes states that this file (or collection of files) is intended to meet the requirements of an electronic record as defined in 21 CFR 11. More specifically, the file (or set of files) must clearly establish a complete and non-redundant set of insertions, updates, and deletions of data values with full auditing and signature information (if available).			（要検討）	

表2 OID番号体系の案

※ODM内で設定するOIDは下記ルールに従い決定する

タグ	属性	用途	OID命名規約	決定権	事前通知	決定内容伝	伝達方法	備考
ODM	FileOID	ODMファイルの特定	[スポンサーコード]-[プロトコルコード]-[施設コード]-[連番]	–	不要			
Study	OID	プロトコルの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
MeasurementUnit	OID	測定項目の単位(kg,cm等)の特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	測定項目の単位を標準化はODMの管轄外とする
MetadataVersion	OID	定義体のバージョン	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
StudyEventDef	OID	VISITの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
FormDef	OID	Formの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
ArchiveLayout	OID	Formのレイアウトイメージ(PDF)特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
ItemGroupDef	OID	ItemGroupの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
ItemDef	OID	Itemの特定	基本的にCDASHに準するが、存在しない場合は下記優先度で検討する。 CDASH ↓ SDTM ↓ 独自コードを検討	EDCシステム？	要	EDC→電カル	ODM(Study)	
CodeList	OID	CodeListの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
Presentation	OID	言語を表す Ex JP:Japanease En:English <Presentation OID="JP" xml:lang="Japanease">	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	使用目的が良くわからない。 また今後の開発用？？？
ConditionDef	OID	ロジカルチェックの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
MethodDef	OID	自由記述の特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Study)	
User	OID	Uesrの特定	ODMを生成する(または原データを生成する)システムに依存	ODMを生成する(または原データを生成する)システム	不要	電カル⇔EDC	ODM(Admin)	
Location	OID	Locationの特定	連携システム間で検討(EDCシステムで検討？)	EDCシステム？	要	EDC→電カル	ODM(Admin) or 文書等 ※施設毎に出力を制御する必要あり	対象実施施設の施設コードをそれぞれの施設に伝える
SignatureDef	OID	Signatureの特定	ODMを生成する(または原データを生成する)システムに依存	ODMを生成する(または原データを生成する)システム	不要	電カル⇔EDC	ODM(Admin)	

厚生労働科学研究費補助金(医療技術実用化総合研究事業（臨床研究・治験推進研究事業）)
分担研究報告書

リモートSDVによるモニター業務の効率化に関する研究

分担研究者：三原直樹　大阪大学医学部附属病院医療情報部　准教授
山口光峰　PMDA 安全第一部 医療情報データベース課　課長

研究要旨
臨床研究・治験活性化5か年計画2012において、具体的な目標と解決のための方策が定められ、IT技術の更なる活用が課題として提示された。我が国は、電子カルテシステムが大規模病院で着実に普及しつつあり、電子カルテの基盤を利用することにより、より効果的なITによる臨床研究の支援が実現できる可能性がある。本研究では、臨床研究・治験領域でITに期待される課題のうち、現在、少数施設においてのみ取り組みがなされているリモートSDVについて、システムの要件、具体的な運用手順、想定される運用体制を明らかにすることを目的とし、医療機関、製薬企業等の利害関係者がそれぞれのリスクを認識したうえでリモートSDVシステムを稼動させることができ、さらに多くの施設においてリモートSDVを普及させることを目指す。リモートSDVを実現するためのしくみとして、本研究では前年度、通信回線を使い医療機関の電子カルテを遠隔から閲覧させる方法を対象として、必要となるシステム要件および運用方法について検討を行った。今年度は、通信回線を使い医療機関の電子カルテを遠隔から閲覧させる方法についてシステムを試験的に構築し、医療機関でリモートSDVを実施する上での標準的な業務手順を検討した。さらに、複数の医療機関でリモートSDVシステムを運用するためのシステム構成、運用体制、運用手順を検討し、実装・運用を行った上で、システムの実現可能性を評価したので報告する。

研究協力者
真鍋　史朗（大阪大学大学院医学系研究科　医療情報学）

A．研究目的

我が国では、大規模病院を中心に電子カルテシステムの利用が普及しつつあり、電子カルテの基盤を利用することによるより効果的な臨床研究の支援の実現が期待されている。研究代表者の元では、電子カルテの基盤の利用に向け、以下の４つの課題を取り上げ、一部は既に実験的にシステムを構築し実証研究を開始している。

①患者数調査のためのデータベースの構築

②治験審査資料の電子化による治験審査の効率化

③病院情報システムとEDCの連動による症例報告書作成とデータ収集の支援

④リモートSDVによるモニター業務の効率化

本分担研究では、現在、少数施設においてのみ取り組みがなされているリモートSDVについて、システムの要件、具体的な運用手順、想定される運用体制を明らかにすることを目的とし、医療機関、製薬企業等の利害関係者がそれぞれのリスクを認識したうえでリモートSDVシステムを稼動

させることができ、さらに多くの施設においてリモートSDVが普及することを目指すものである。

B．研究方法

実施医療機関が臨床研究等のデータを遠隔地から閲覧させる方法として、以下のとおり考えられる（参照：前年度の分担研究者山口の報告書）。

[1] 同一医療法人の事務所等による閲覧：電子カルテシステム等が接続されている別の場所（法人事務所等）で閲覧に供する方式。

[2] 地域医療連携システムの外部閲覧機能を活用した閲覧：地域医療支援病院が支援病院に対し提供している電子カルテシステムの外部閲覧機能で閲覧に供する方式。

[3] ネットワーク設定の変更等による閲覧：実施医療機関内の電子カルテシステムに、VPN接続等で閲覧に供する方式。

[4] モニタリングサーバによる閲覧：電子カルテ内の被験者の情報（閲覧期間を限定した最低限の情報）をモニタリングサーバに転送・蓄積し、閲覧に供する方式。

[5] その他：電子カルテの内容を印刷出力したＰＤＦを一定の閲覧制限をあたえ閲覧に供するなどの方法。

これらのうち、[1][2][5]については、リモートSDVの先行導入施設で採用されているが、その適用範囲は少数であり限定的な条件あるいは用途下にて実現しうるものと考えられる。すわなち[1]は、同一法人内に複数のブランチを有する医療機関、[2]はすでに地域医療連携システムに一定の投資を行っている、または行う予定の医療機関、[5]は電子カルテデータのPDF化にかかる運用負荷に耐えうる人員が整備され、かつ比較的少数の利用者による閲覧が想定される医療機関でのみ運用が可能である。

本研究では、昨年度の検討結果を踏まえて[3]の手法（前年度報告の「通信回線を使い医療機関の電子カルテを遠隔から閲覧させる方法」「A方式」）で実験的にシステムを構築し、具体的な運用手順、想定される運用体制、問題点についての検証を行った。

C．研究結果

１）前提条件

治験や臨床研究においては、モニターが被験者の秘密が保全されることを条件に、診療録等を直接閲覧することで、治験データ等が正確かつ完全であることを原資料等の治験関連記録に照らして確認することが求められている。このため、本研究で開発したリモートSDVのシステムによる電子カルテ閲覧については、被験者から文書による同意が取得されている治験や臨床研究を対象に実施することを前提とする。

直接閲覧に興ずるための手順や閲覧場所を含め具体的な方法は、法令で定められているわけではなく、実施医療機関の責任において、個人情報の保護、電子カルテシステム等に対するセキュリティ等に留意しつつ、定めることができる（参照：前年度の分担研究者山口の報告書）。本研究においては、開発したリモートSDVのシステムを利用する場合の考え方をまとめているので、参考にされたい。

２）リモート SDV システム概要

本研究では、製薬企業やCROに属する複数の利用者（モニター）がPC端末を用いて、ハブセンターを経由して、複数の医療機関にある電子カルテ端末へ接続することが可能となるリモートSDVシステムを構築した（図１）。モニターは製薬企業やCRO内にあるPC端末からハブセンターのVPNルータを介して、アクセス先を適切に制御して振り分けるハブ機能を有するサーバ（コネクシ

ョンブローカ）に接続する。そして、コネクションブローカからVPN機能を有した仮想ハブを介して、各医療機関内にある電子カルテ端末へ接続する。ハブセンターには、他にモニターを管理する認証サーバとVPNルータへの接続に必要な電子証明書を発行するサーバがある。医療機関１には仮想デスクトップ上で動作する電子カルテ端末１を、医療機関２にはリモートデスクトップで動作する電子カルテ端末２を設置している。

なお、ハブセンターは製薬企業やCROおよび医療機関とは独立したネットワークを運営する組織として構築することを前提としているが、今回は、試行段階であるため、大阪大学医学部附属病院内に設置した。ハブセンターの運営主体となる組織を以下では「事務局」と呼ぶ。

ハブセンターと医療機関、およびハブセンターと製薬企業やCROの間の通信回線（インターネット回線、専用回線など）は、IP（Internet Protocol）による通信ができる環境を用意した。

３）システム構成要素

本研究で開発したリモートSDVシステムのシステム構成は以下のとおりである。

＜製薬企業やCRO内＞

・USBメモリ：モニターに配布し認証デバイスおよびPC端末の起動システムとして利用する。

・USBメモリ用OS：PC端末のUSB接続ドライブから起動可能なOS（Blubuntu）。

・コネクションブローカ接続用クライアントソフトウェア（Ericom AccessPad）：PC端末から、VPNルータを経由してコネクションブローカを利用するためのソフトウェア。モニター毎に利用可能な電子カルテ端末を選択可能にする。

・VPN接続用ソフトウェア（Cisco AnyConnect Mobile Client）：製薬企業やCRO内のPC端末とVPNルータの間で暗号化通信を確立するためのソフトウェア。

・クライアント証明書：VPNルータに対するPC端末を特定してアクセスを許可し、「なりすまし」を防止するために利用する。

＜ハブセンター内＞

・VPNルータ/FW（ファイアーウォール）：PC端末とハブセンターの間で暗号化通信を確立する。また、電子カルテ端末とハブセンターの間の通信制御を行う。

・コネクションブローカ（Ericom Power Term WebConnect）：モニターの権限を確認し、モニター毎に利用可能な電子カルテ端末を選択可能とさせ、特定の電子カルテ端末が選択された際に仮想HUB/VPNサーバに対して電子カルテ端末への接続要求を振り分け、必要なソフトウェアを提供する。仮想環境（Xen Desktop）で動作する電子カルテ端末１に対しては、仮想環境を操作するソフトウェア（Citrix Receiver）を、リモートデスクトップで動作する電子カルテ端末２に対してはリモートデスクトップ用アプリケーションをそれぞれ提供する。

・認証サーバ（ADサーバ）：コネクションブローカサーバにおけるモニターの認証情報を一元的に管理する。

・Windows証明書サーバ：PC端末が使用するクライアント証明書を発行・管理する。

・仮想HUB/VPNサーバ（SoftEther PacketiX VPN）：ハブセンターと各医療機関の電子カルテ端末間でVPN接続を行い、暗号化通信を行うためのサーバ。仮想L2スイッチとして作動し、医療機関毎に仮想HUBを作成する。

＜医療機関内＞

・仮想デスクトップ上電子カルテ端末（Xen

Desktop）（電子カルテ端末１）：仮想環境で動作する電子カルテ端末。病院端末にアクセスするための仮想端末として機能。データ漏洩防止機能を有する。
・リモートデスクトップで動作する電子カルテ端末（電子カルテ端末２）：本実証実験では実際の電子カルテ端末ではなく、電子カルテを想定した Windows端末を用いた。
・仮想HUB/VPN接続用ソフトウェア（PacketiX Client）：電子カルテ端末と仮想HUB/VPNサーバの間で暗号化通信を確立するためのソフトウェア。

４）システム運用上の仕様

リモートSDVで閲覧対象となる情報は機密性の高い診療情報等である。これらの情報をインターネット等の通信回線を経由して製薬企業等に閲覧させることは、医療機関にとって一定のリスクを伴う。これまでリモートSDVが少数の医療機関でのみ実施されてきた理由の一つは、診療情報等の漏洩リスクを低減させるためのセキュリティ技術にかかるコストが非常に高い、あるいは見積困難と考えられてきたことにある。本研究では、将来的に多数の製薬企業、CRO、医療機関が参加できるシステムモデルの確立を目的とし、実用的な観点に立ち、多数の参加機関にて実現可能かつ運用可能と考えられる、コストーリスクバランスの取れたシステムの提案を目指した。

なお、医療機関側では、①電子カルテシステムが稼働しており、下記の関連ガイドラインに準拠したシステム構築および運用がなされていること、および②契約書や申し合わせ書等により、製薬企業・CRO側の行為に対して適切な制約条件が課されていることを前提として開発を行った。製薬企業・CRO側に求める制約条件については、本格稼働を開始するまでに、必要に応じて、関係団体の意見を聴取しながら、医療機関側で定めることとし、本研究で言及しない。

①医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン[厚生労働省]
②医療情報システムの安全管理に関するガイドライン[厚生労働省]

また、ハブセンターを運営する企業は、下記の関連ガイドラインに準拠したシステム構築および運用がなされていることを前提とする。

③ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン[総務省]
④医療情報を受託管理する情報処理事業者向けガイドライン[経済産業省]

4-1）ネットワーク構築の考え方と利用者管理・利用者認証

ネットワーク構築の際、総数MのPC端末と総数Nの医療機関を直接、接続する方式を採用すると、M×Nのネットワーク敷設が必要となり、非現実的である。そのため、ハブセンター内にHUB Centerの機能を持たせ、ここを起点として総数MのPC端末と総数Nの医療機関を接続させて管理する方式を採用することが望ましい。この方式を採用すると、M＋Nのネットワーク敷設で済む（図２、図３）。

本システムでは、昨年度の検討を踏まえて、モニターをハブセンターで集中管理して各医療機関の電子カルテ端末を閲覧可能とする方式を用いた。利用者認証は、USBメモリという物理媒体の利用と、ログイン時のID/パスワードの入力という複数要素による認証方式を採用している。

3-2）ネットワークレベルでのアクセス権限制御

ネットワークレベルでのアクセス権限制御については、①モニターーハブセンターー間のアクセス、②ハブセンターー医療機関間のアクセスについて考慮する必要がある。

①について、本システムではクライアント証明書を使用したSSL-VPNルータによるVPN接続を行った。

製薬企業やCROが固定IPアドレスを有したネットワーク回線を用意し、VPNルータにおいて接続元IPアドレスの制限を行うことで、より強固なセキュリティを確保することが可能になる。なお、①の権限設定はシステム全体のセキュリティレベルに大きく関わるため、事務局がその管理責任を負う。

②については、医療機関側から仮想HUB/VPNサーバへ暗号化通信を行うこと、コネクションブローカにおいてモニター毎に仮想HUB/VPNサーバへの接続の可否を設定することで、ネットワークレベルでのアクセス制御を実現している。医療機関側で本システムによる閲覧を不許可にする場合は、仮想HUB/VPNサーバへの接続を遮断することで処理する。

利用者が増大した場合の運営状況を想定すると、医療機関に無関係なモニターが多数存在することとなり、これは医療機関においてセキュリティ上のリスクとなる。その場合、モニター毎に無関係な医療機関（電子カルテ端末）への接続を拒否するような仕組みが必要となる。ここでは、コネクションブローカにおける設定でその処理を行う。基本的に、モニターが医療機関へ接続可能かどうかの設定は医療機関が行うべきであると考えられるが、その設定作業を全て医療機関で行うことは作業量などを勘案すると困難である。そのため、設定は各医療機関と連携しながら作業は事務局で行うこととしている。

ネットワークレベルのアクセス制御においては、モニター側端末からの通信が病院の内部ネットワークに配置された病院情報システムに到達する必要がある。このためには、病院側ネットワークでハブセンター→病院情報システム方向のインバウンド（内向き）の通信を許容しなければならない。電子カルテシステムは外部ネットワークと接続されていないか、接続されていてもインバウンドの通信が厳しく制限されているのが普通であり、病院側ではハブセンター → 病院の通信について運用ポリシーを明確にしたうえで運用管理責任を負う必要がある。

今回は実験環境ということで病院ーハブセンター間の通信の安全性は、暗号化機能を有するVPNソフトウェア（PacketiX）を用いて担保した。しかし、セキュリティ保持の観点からは、本来は病院とハブセンター間で接続元IPアドレスを限定したIPsec-VPNなどの拠点間VPNを構成し、VPN内のネットワーク上にFWを設置してハブセンター→病院情報システム方向の通信制御を行うことが求められる。

3-3）病院情報システムのアクセス権限制御

各々の病院において、以下のような点について適切に病院情報システムの利用者マスタメンテナンスを実施する必要がある。

①モニターにデータの閲覧権限のみを付与する。

②病院情報システムの機能で、利用者あるいは職種・グループなどの単位で閲覧可能なデータ種を制限できる場合は、モニター側に必要最小限のデータのみの閲覧権限を付与する。

③モニターが当該治験対象患者の診療情報のみにアクセス可能となるよう制限す

る。

上記のうち、③については、マスタメンテナンスのみで対応できない実装がなされている製品も存在するので、とくに以下のような点について病院情報システム側で機能改修が必要となる場合があることに留意する。

①患者検索機能を無効にする。

②患者リスト、たとえば入院患者一覧や血縁関連患者一覧の表示を無効にする。

③SSOを実装している場合は、その機能により病院情報システムの認証情報入力画面（ログイン画面）の表示を抑止する。

SSOを用いることができれば、モニターが電子カルテ端末の認証を行う際に別人のユーザIDを用いるリスクが軽減できるが、今回の実験ではここまでの実証は行っていない。

3-4）情報保護

ユーザ認証とアクセス権限制御が適切に設定され、実行された場合であっても、モニターが本システムで閲覧したデータを外部に漏洩するリスクが残存する。そのため、本システムではUSBメモリから起動するOSを用いることで、PC端末において他システムへの情報のコピー&ペーストや印刷ができないように制御している。

3-5）システム運用方法

本研究の実証実験で構築したシステムにおいて想定した運用フローを以下に示す。

① ハブセンターを管理する事務局は、製薬企業やCROより申請を受け、モニターに対してシステムの使用方法等に関する教育訓練を実施する。また、モニターの認証情報を認証サーバであるADサーバに登録する。

② 事務局は、同時に、モニターに配布するUSBメモリを準備する。USBメモリの内容は、USB接続ドライブから起動可能なOS（Blubuntu）、コネクションブローカ接続用クライアントソフトウェア（Ericom AccessPad）、VPN接続用ソフトウェア（Cisco AnyConnect Mobile Client）、VPN接続の際になりすましを防ぐクライアント証明書で構成される。

③ 事務局は、製薬企業との契約のもと、モニターに対してUSBメモリを配布し、認証ID・パスワードを通知する。

④ 事務局は、病院との契約のもと、仮想HUB/VPNサーバ内に各病院用の仮想HUBを作成する。病院は、自院のモニター用電子カルテ端末に、仮想HUB/VPNクライアントソフトウェアをインストールし、ハブセンターの仮想HUB/VPNサーバとの接続を行う。（なお、今回の実証実験において大阪大学医学部附属病院の電子カルテを閲覧できる仮想デスクトップサーバは、ハブセンターと同一施設内にあるため、仮想HUBを介さず、直接コネクションブローカに接続している。）

⑤ 病院は、製薬企業との契約のもと、自院の電子カルテ端末を利用可能なモニターを事務局に伝える。事務局はコネクションブローカに対して、病院毎に接続可能なモニターを登録する。

⑥ モニターは、インターネット経由でハブセンターに接続可能な状態になっている端末に対して、USBメモリを端末に挿入した状態でUSBメモリ内部のOS（Blubuntu）を起動する。続いてVPN接続用クライアントを起動する（AnyConnect）。

⑦ モニターは、VPN接続用クライアントでVPNルータに接続し、IDとパスワードを入力する。なお、接続に際し、USBに含まれるクライアント証明書による認証

も行われるため、VPN接続確立のため2要素認証が行われることになる。

⑧ VPNルータとの接続完了後、モニター端末のコネクションブローカ用ソフトウェアが起動するので、IDとパスワードを入力する。認証が行われると、モニター毎に利用（接続）可能な医療機関の選択肢が表示される。

⑨ モニターが、選択肢から利用したい病院を選択すると、コネクションブローカを経由して該当病院の端末への接続認証画面が表示されるので、必要な情報を入力する。接続先の環境（仮想デスクトップもしくはリモートデスクトップ）によって、それぞれ画面構成は異なる。

⑩ 認証が成功すると、画面上に電子カルテ端末のログイン画面が表示される。モニターは病院から配布されている認証情報を用いると、電子カルテの閲覧が可能となる。

⑪ 病院は本システムを全モニターに対して利用させない場合は、仮想HUB/VPNクライアントソフトウェアを用いて仮想HUB/VPNサーバへの接続を遮断する。モニター単位で利用を禁止させる場合は、事務局へ連絡してコネクションブローカの設定を変更してもらう。

3-6）システムの特徴・留意事項

本システムの特徴は、以下の通りである。

・USBメモリの利用によりクライアント認証とID・パスワードの複数要素認証を実現している。

・コネクションブローカの導入により、モニター毎に利用可能な病院が選択可能になる。また、モニターが入力した認証情報を各病院の電子カルテ端末環境に引き渡すことが出来る。病院側で認証情報を受け取ることが可能な場合、多段認証によるモニターの運用負荷を軽減することが可能になる。

・病院側で自院の仮想HUBの管理を行うため、ハブセンターから病院へのネットワークレベルでのアクセス権限を病院側が主体的に制御することが可能となる。

・病院側は電子カルテ端末に対してリモートデスクトップの利用を可能にするだけで、多くの場合病院情報システムの改修等を実施せずに容易に実現できる。

ただし、以下の点には留意が必要である。

・モニターは、病院情報システムを直接操作するため、病院情報システムの瑕疵・脆弱性によって、病院が意図せずモニターの知るべきでない診療情報を与えてしまう可能性がある。この点については製薬企業・CRO側に求める制約条件を定めておく必要がある。

・モニターは病院に所属しないため病院情報システムを利用することに関して、OSやソフトウェアのライセンスが別途必要になる場合がある。これは病院のライセンス契約状況に依存するため、事前に関連企業に確認が必要である。

4）リモートSDV実施時に必要となるマイクロソフト製品ライセンスの考え方

本研究においてシステムを構築する際、Windows製品のライセンスに対する考え方を整理する必要があった。これにあたって日本マイクロソフト株式会社の協力により情報提供を受けることが出来たのでここに報告する。以下は2015年4月現在でのマイクロソフトのライセンス条件を元に作成した（「製品使用権説明書および製品表」
http://www.microsoft.com/ja-jp/licensing/aboutlicensing/
product-licensing.aspx）。

また、病院側でのライセンスプログラム

締結状況、契約条件などが異なるため、個別の要件についてはマイクロソフト営業もしくはライセンス問い合わせ窓口（VLCC）に確認をすることを日本マイクロソフト株式会社は推奨している。

必要ライセンス算出のための前提条件は以下の通りである。

・リモートSDVを実施する際のシステム構成例をパターン１～４に分け、必要となるマイクロソフトソフトウェアライセンスを提示する。

・リモートSDVを実施する病院は、ソフトウェアライセンスをボリュームライセンスプログラムにて手配することを前提とする（プリインストール製品は個人利用を想定しているため）

・電子カルテ（Windows Serverベース）参照にはMS Officeを利用することを想定する。

・必要となるライセンスは基本的には病院側にて接続用の環境として手配することを想定する。

・製薬企業は外部ユーザとして病院の所有するライセンスに含まれる（ライセンス保有者のための業務を行うという考え方：例として、システム保守のための管理会社などと同等との理解）

下記に示すそれぞれパターンごとのシステム構成に応じた具体的な必要ライセンスに関する内容については、図４－９に示す。

＜パターン1-1＞

病院外部よりリモートデスクトップ接続により電子カルテを直接閲覧する場合で、アクセスする端末がWindows OS端末の場合

＜パターン1-2＞

病院外部よりリモートデスクトップ接続し、かつ病院外からアクセスする端末が非Windows OS端末である場合

＜パターン2-1＞

病院内部でSBCシステムあるいは仮想デスクトップを構築している場合で、外部からWindows OS端末にてアクセスする場合

＜パターン2-2＞

病院内部でSBCシステムあるいは仮想デスクトップを構築し、外部から非Windows OS端末にてアクセスする場合

＜パターン3＞

クラウド型SBCの仕組みを採用する場合

＜パターン4＞

クラウド型サーバVDIを採用する場合

それぞれの参考資料として下記を列挙する。

・製品使用権説明書および製品表

http://www.microsoft.com/ja-jp/licensing/aboutlicensing/product-licensing.aspx

・デスクトップ仮想化ライセンスガイド

http://download.microsoft.com/download/F/8/1/F8199620-6205-4E27-86F5-2F24CAEFFDC0/SA_Customer_Virtual_Desktop_Brochure_JP.pdf

・Windows Server 2012 R2 リモートデスクトップサービスおよびRDS を使用したMicrosoft デスクトップアプリケーションのライセンス

http://download.microsoft.com/download/C/B/0/CB0931B5-5B44-4A6A-AFB7-BEFB81AE409F/Licensing-Windows-Server-2012-R2-RDS-and-Desktop-Apps-for-RDS-JP.PDF

５）リモートSDVによるモニタリングにおける留意点

リモートSDVによるモニタリングであっても、治験依頼者により指名されたモニターが、治験の進行状況を調査し、治験が治験実施計画書、標準業務手順書、薬事法14

条第3項および第80条の2に規定する基準並びに各病院がそれぞれ定める基準に従って実施、記録および報告されていることを保証しなければならないことは、通常のモニタリングにおける要件と何ら変わりは無い。

実際にリモートSDVを行うにあたっていくつか追加すべき留意点があるので、以下に記載する。

《依頼者側の留意点》

依頼者側では、管理責任者の設置、接続USBの受け渡しの手順、USB管理のルール、依頼者側の端末環境の整備、実際にモニター業務を行うユーザの管理、ハブセンターのヘルプデスクや病院の病院情報システム管理者への申請手続き、終了通知手続きなどをStudy毎に行う必要がある。

《病院側の留意点》

モニターが病院情報システムを利用する際、データ登録が出来ない専用の権限を付与し、担当患者に限定した閲覧が出来る様にする設定を行う必要がある。また閲覧される端末の操作ログなどの監視も行うなど、運用を徹底する必要がある。

《ハブセンターの留意点》

ヘルプデスクにより申請を受けて接続設定サービスを行える体制が必要である。また各Studyの終了を確実に捉えたり、不適切なアクセスがないかどうか見張り業務を行ったりすることが必要。さらに契約時には、依頼者組織の環境、病院の病院情報システムネットワーク環境を確認し、セキュリティホールがないことの確認も行った上で、必要な設定作業を行う運用が可能な体制整備が必要である。

6）リモートSDVを実施させる際の教育訓練

本研究で構築したシステムを利用するためには、モニターに対し一定の教育訓練を実施しなければならない。

教育の内容については、ハブセンター及び病院で効率的に実施することを前提に、本格稼働までに決定することとするが、基本的には以下を実施することが望ましい。

①ハブセンターにおける教育訓練

ハブセンターにおいては、以下、共通事項に関する教育訓練を中心に実施する必要がある。

・リモートSDVシステムを利用する際の留意事項について
・リモートSDVシステムのセキュリティについて
・ID、パスワード及びUSBデバイスの管理方法について
・リモートSDVシステムの利用方法について

②病院における教育訓練

病院においては、以下、病院特有な事項を中心に実施する必要がある。

・病院システムを利用する際の留意事項について
・製薬企業・CRO側に求める制約条件について
・利用申請について
・ID、パスワードの配布、管理について
・病院システムの利用方法について

D．考察

リモートSDVによるモニター業務の効率化を推進するために、具体的なシステム構築に係る要件整理を行った。また具体的なシステムを構築し、現在、少数施設においてのみ取り組みがなされているリモートSDVについて、システムの要件、具体的な運用手順、想定される運用体制を明らかにすることを検討した。医療機関、製薬企業等の利害関係者がそれぞれのリスクを認識したうえでリモートSDVシステムを稼動させることができ、さらに多くの施設にお

いてリモートSDVを普及させることは実現可能であると考えられる。

E．結論

本研究では、通信回線を使い医療機関の電子カルテを遠隔から閲覧させる方式についてシステムを構築し、実証実験を行った。実証実験においては、リモートSDVを実施する上での標準的な業務手順の提示、および複数の医療機関でシステムを運用するためのより効率的なシステム構成、運用体制、運用手順などを検討し、システムの実装・運用を行った上で、コストおよび利便性などの観点からシステムの実現可能性を示すことができたと考える。

なお、本分担研究は、著者の個人的見解に基づくものであり、独立行政法人医薬品医療機器総合機構の公式見解を示すものではない。

F．健康危険情報

特になし

G．研究発表

1．論文発表

なし

2．学会発表

なし

H．知的財産権の出願・登録状況

なし

■ リモートSDV システム構成図

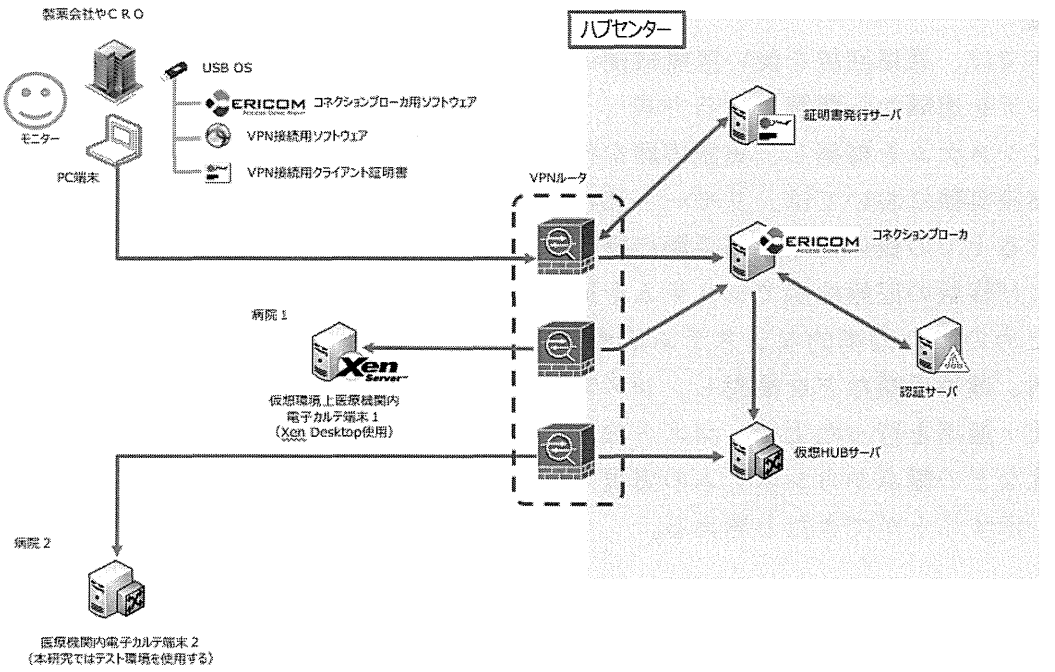
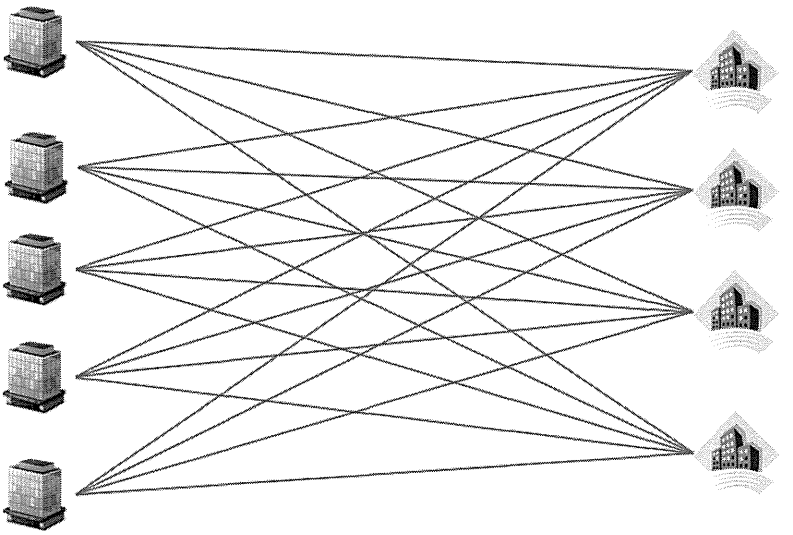


図１　リモート SDV 接続構成図

■リモートSDVのためのネットワーク

製薬企業：M　　病院：N

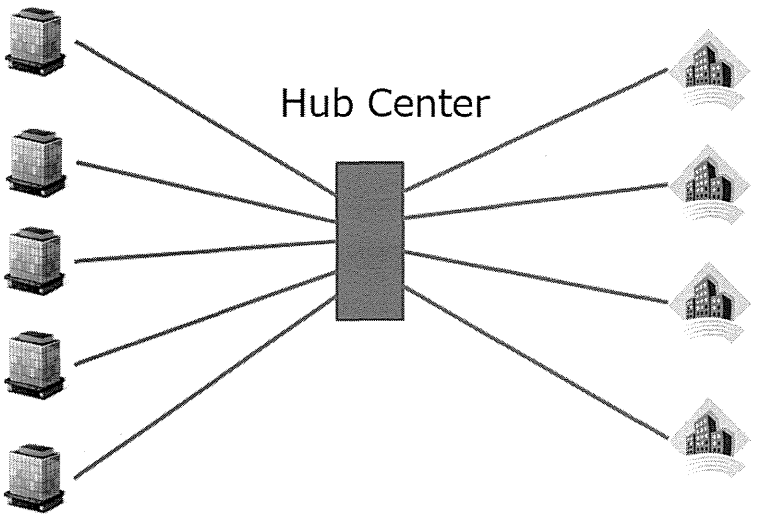


M x N のネットワークの設置

図２　　M×N ネットワーク配置イメージ

■リモートSDVのためのネットワーク

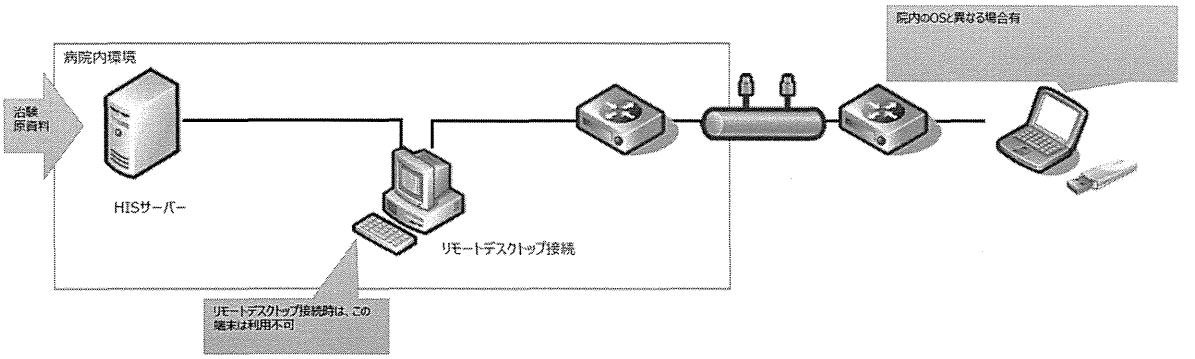
製薬企業：M　　病院：N



M ＋ N のネットワークの設置

図３　M+N ネットワーク配置イメージ

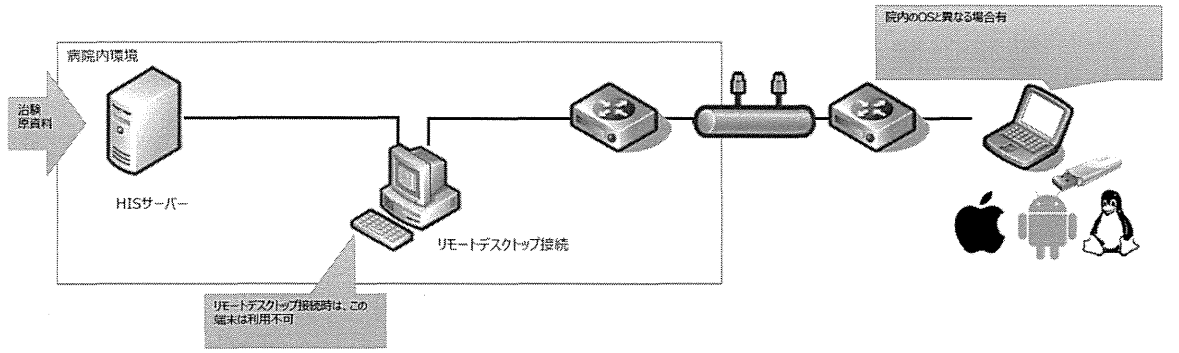
パターン1-1



	病院側端末	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	要	
Windows Pro もしくはEnterprise	–	（要）	院内のOSと異なる場合
Windows SA	–	–	WTG利用の場合は必要
VDA	–	–	
Office	–	要	Viewerで代替可能な場合も。
Office SA	（要）	–	SA適用により病院に属する職員がローミング権で外部から接続することも可能
Windows Server CAL	–	要	院内HISサーバーへのExternal Connecter License適用で代替可能
Windows Server RDS CAL	–	–	

図４　リモート SDV に必要なライセンス

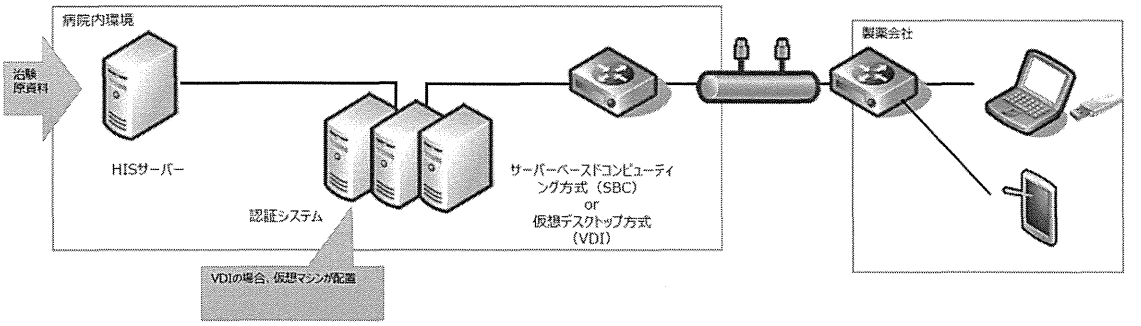
パターン1-2　端末が非Windows



	病院側端末	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	–	
Windows Pro もしくはEnterprise	–	–	
Windows SA	–	–	
VDA	–	要	
Office	–	要	Viewerで代替可能な場合も。
Office SA	（要）	–	SA適用により病院に属する職員がローミング権で外部から接続することも可能
Windows Server CAL	–	要	院内HISサーバーへのExternal Connecter License適用で代替可能
Windows Server RDS CAL	–	–	

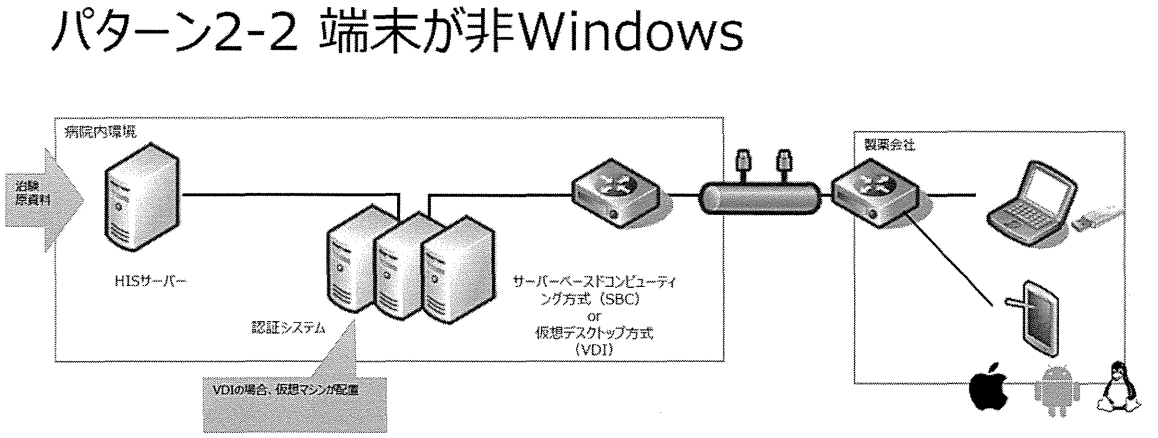
図５　リモート SDV に必要なライセンス（非 Windows OS によるアクセスの場合）

パターン2-1



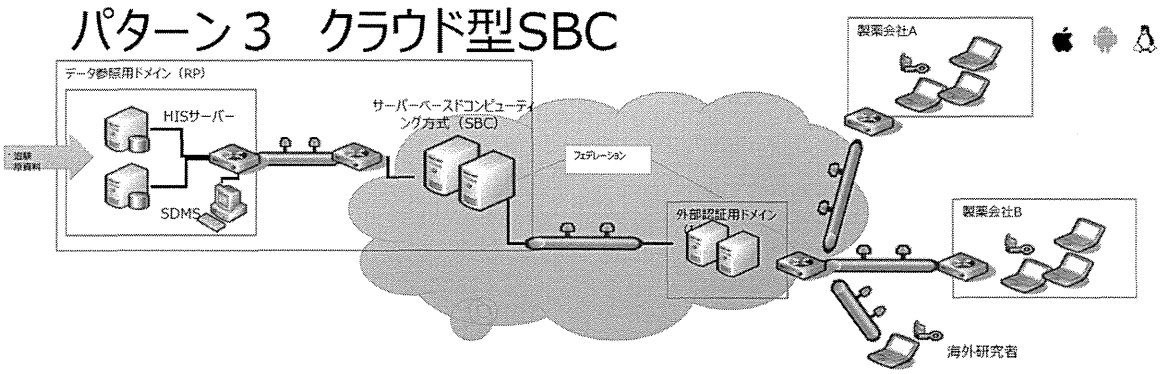
	病院側端末	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	要	
Windows Enterprise	–	（要）	VDI利用の場合
Windows SA	–	（要）	VDI利用の場合
VDA	–	–	
Office	–	要	Viewerで代替可能な場合も。
Office SA	（要）	–	SA適用により病院に属する職員がローミング権で外部から接続することも可能
Windows Server CAL	–	要	院内HISサーバーへのExternal Connecter License適用で代替可能
Windows Server RDS CAL	–	（要）	SBC利用の場合

図６　VDI 利用の場合



	病院側端末	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	–	
Windows Enterprise	–	–	
Windows SA	–	–	
VDA	–	（要）	VDI利用の場合
Office	–	要	Viewerで代替可能な場合も。
Office SA	（要）	–	SA適用により病院に属する職員がローミング権で外部から接続することも可能
Windows Server CAL	–	要	院内HISサーバーへのExternal Connecter License適用で代替可能
Windows Server RDS CAL	–	（要）	SBC利用の場合

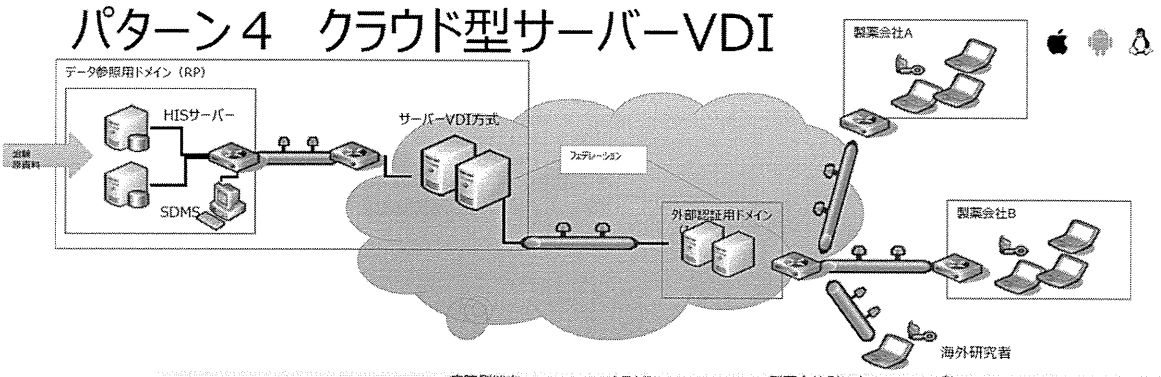
図７　VDI 利用の場合（非 Windows OS によるアクセスの場合）



	病院側端末	クラウド	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	–	–	
Windows Enterprise	–	–	–	
Windows SA	–	–	–	
VDA	–	–	–	クライアントVDI利用は不可
Office 365 ProPlus	–	–	要	Viewerで代替可能な場合も。 Azure以外の場合はSPLAでの手配
Windows Server CAL	–	（要）	要	院内HISサーバー、クラウド上のサーバーへのExternal Connecter License適用で端末側のCAL代替可能
Windows Server RDS CAL	–	–	要	ユーザー数でカウント
Windows Server RDS CAL SA	–	–	要	ユーザー数でカウント

※Office 365 ProPlusのクラウド上での利用は、Microsoft Azureもしくは物理的にお客様専用の物理ハードウェア サーバー（ハウジングなど）であること
※クラウド利用料は別途必要

図８　クラウド型 SBC の場合



	病院側端末	クラウド	製薬会社側端末	備考
Windowsクライアント OS（OEM）	–	–	–	
Windows Enterprise	–	–	–	
Windows SA	–	–	–	
VDA	–	–	–	クライアントVDI利用は不可
Office 365 ProPlus	–	–	要	Viewerで代替可能な場合も。 Azure以外の場合はSPLAでの手配
Windows Server CAL	–	（要）	要	院内HISサーバー、クラウド上のサーバーへの External Connecter License適用で端末側 のCAL代替可能
Windows Server RDS CAL	–	–	（要）	利用する技術により選択 ユーザー数でカウント
Windows Server RDS CAL SA	–	–	（要）	利用する技術により選択 ユーザー数でカウント

※Office 365 ProPlusのクラウド上での利用は、Microsoft Azureもしくは物理的にお客様専用の物理ハードウェア サーバー（ハウジングなど）であること
※クラウド利用料は別途必要

図９　クラウド型サーバ VDI の場合

研究成果の刊行に関する一覧表

書籍

なし

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
Matsumura Y, Hattori A, Manabe S, Takeda T, Takahashi D, Yamamoto Y, Murata T, Mihara N.	Interconnection of Electronic Medical Record with Clinical Data Management System by CDISC ODM.	Stud Health Technol Inform	2014;205	868-72.	2015
武田 理宏、三原 直樹、真鍋 史朗、松村 泰志	レセプトデータを活用した患者病名の推定	医療情報学	vol.34 (Suppl.)	312-315	2014
青柳 吉博、千葉 吉輝、岡田 昌史、赤堀 澄子、溝渕 真名武、横井 英人	病院情報システムを治験データとして活用することへの展望と課題	医療情報学	vol.34 (Suppl.)	178-180	2014

e-Health – For Continuity of Care
C. Lovis et al. (Eds.)

doi:10.3233/978-1-61499-432-9-868

Interconnection of Electronic Medical Record with Clinical Data Management System by CDISC ODM

Yasushi MATSUMURA[ab], Atsushi HATTORi[b], Shiro MANABE[ab], Toshihiro TAKEDA [a], Daiyo TAKAHASHI[b], Yuichiro YAMAMOTO[ab], Taizo MURATA[c], Naoki MIHARA[a]

[a] *Medical Informatics, Osaka University Graduate School of Medicine, Osaka, Japan*
[b] *MKS ltd, Osaka, Japan*
[c] *Division of Medical Informatics, Osaka University Hospital, Osaka, Japan*

Abstract. EDC system has been used in the field of clinical research. The current EDC system does not connect with electronic medical record system (EMR), thus a medical staff has to transcribe the data in EMR to EDC system manually. This redundant process causes not only inefficiency but also human error. We developed an EDC system cooperating with EMR, in which the data required for a clinical research form (CRF) is transcribed automatically from EMR to electronic CRF (eCRF) and is sent via network. We call this system as "eCRF reporter". The interface module of eCRF reporter can retrieves the data in EMR database including patient biography data, laboratory test data, prescription data and data entered by template in progress notes. The eCRF reporter also enables users to enter data directly to eCRF. The eCRF reporter generates CDISC ODM file and PDF which is a translated form of Clinical data in ODM. After storing eCRF in EMR, it is transferred via VPN to a clinical data management system (CDMS) which can receive the eCRF files and parse ODM. We started some clinical research by using this system. This system is expected to promote clinical research efficiency and strictness.

Keywords. Medical Records Systems, Computerized Clinical Research, CDISC, ODM, eCRF

Introduction

With the growth of importance of evidence based medicine, efficient clinical data collection method is desired for clinical research. These days, EDC has been used in the data collection process for clinical research, where a CRC transcribes data in a medical record to an EDC terminal. EDC has a merit of making instant remote monitoring possible. In addition, it improves data accuracy by checking system on the timing of data entry and streamlines data management process.

In Japan, more than 50% of hospitals with more than 400 beds implement EMR system. Despite this, a CRC transcribes data shown on an EMR terminal screen to an EDC terminal manually. It is desired that necessary data for CRF which is recorded in EMR can be transcribed to electronic CRF (eCRF) automatically. This vision was already proposed by Clinical Data Interchange Standards Consortium (CDISC). CDISC developed Operational Data Model (ODM) as standard eCRF[1)]. However,