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

研究分担者：桑田成規（国立循環器病研究センター）

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が普及することを目指す。リモートSDVを実現するためのしくみとして、本研究では、①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、および②モニタリングに最低限必要な情報を医療機関の電子カルテからデータセンタ等のサーバに転送し閲覧させる方法を対象として具体的な検討を行い、システム要件をとりまとめたうえでシステム構成および運用方法について提案を行った。今後、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（上記①案）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業務手順書を作成する予定である。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する予定である。

分担研究者
山口光峰（医薬品医療機器総合機構）
研究協力者
中島唯善（日本製薬工業協会）
近藤充弘（日本製薬工業協会）
小宮山靖（日本製薬工業協会）

## A．研究目的

「臨床研究・治験活性化5か年計画2012」において、臨床研究におけるIT技術の更なる活用が課題として提示された。我が国では電子カルテシステムが大規模病院で普及しつつあり、電子カルテの基盤を利用することにより、より効果的な臨床研究の支援が期待される。研究代表者の元では、以下の４つの課題を取り上げ、一部は実験的にシステムを構築し実証を目的としている。

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

本研究分担者においては、「④リモートSDVによるモニター業務の効率化」のテーマのうち、具体的なシステム構築にかかる要件整理を中心に検討を行った。リモートモニタリングに関する法制度の観点からの留意事項の検討については、本研究の別の分担研究者（山口）によって検討が行われる。

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は、以下のとおり考えられる（参照：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、閲覧に供する方法。
[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、リモートモニタリングを支援するITシステムの普及を目標とする観点から、より多くの参加医療機関および利用者が見込まれる手法を研究対象にすることとし、今後の新たな手法として考えうる[3]および[4]に焦点をあてる。以下、表記を簡便化するために、[3]による手法、すなわち「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「Ａ方式」と呼び、[4]による手法、すなわち「モニタリングに最低限必要な情報を医療機関の電子カルテからデータセンタ等のサーバに転送し閲覧させる方法」を「Ｂ方式」と呼び分ける。以下では、両方式を対象として具体的なシステム構築の検討を行い、システム要件および運用方法案についてとりまとめを行った。

## C．研究結果

１）リモートSDVシステムのモデル（Ａ方式・Ｂ方式）

複数の医療機関Ｈと複数の製薬企業・C

ＲＯ等**P**が参加するシステムであり、**P**に所属する複数の利用者**U**が、Ａ方式またはＢ方式により、端末**T**からデータセンタ**D**を経由して**H**の被験者の電子化診療情報にアクセスし閲覧する（図１）。

Ａ方式では、複数の**U**が複数の**H**にアクセスする際の入り口となり、かつアクセス先を適切に制御し振り分ける「ハブ機能」を備えるサーバ$S_A$を**D**に配置し、**U**は**T**から$S_A$を経由し**H**の内部ネットワークに配置されている電子カルテシステム**E**に直接アクセスする。

Ｂ方式では、複数の**H**（の**E**）より転送された診療情報を保管し、かつ複数の**U**のアクセス権限を適切に管理するサーバ$S_B$を**D**に配置し、**U**は**T**から$S_B$にアクセスする。

いずれの方式においても、**D**は**P**および**H**とは独立したネットワーク上で運営されることを前提とし、**D**の運営主体となる組織を、以下では「事務局」と呼ぶ。**D**と**H**、および**D**と**U**の間の通信回線（インターネット回線、専用回線など）は別途準備されIP（Internet Protocol）による通信ができる環境が整備されているものとし、ここではその構成や設定について言及しない。なお、以下の記述においては、図１に用いられた略号を特に断りなく用いる。

２）共通の要件

リモートＳＤＶの対象となる電子化原資料は機密性の高い診療情報等であり、インターネット等の通信回線を経由してこれを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、医療機関が利用可能とな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－リスクバランスの取れたシステムの提案を行う。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する。

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、データセンタを運営する企業については、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]

2-1）利用者管理・利用者認証

本システムの総利用者数は、$\sum_{k=1}^{Np} N_{Uk}$であり（図１）、参加機関の増加に応じて相当数のアカウント管理が必要となると考えるべきである。また、１人の**U**が複数の**H**にアクセスする場合を考慮すると、仮に**H**側で個別に**U**のアカウント登録・管理をするならば、**U**は**H**ごとに異なるアカウントを保持する必要があり、**U**側の運用が煩雑になる。以上のことから、**D**側において効率的に利用者を集中管理するために、事務局側でアカウント管理ができる仕組みを有することが望ましい。利用者認証については、総当たり攻撃による不正侵入およ

び「なりすまし」防止等の観点から、ID・パスワード認証だけでなくＩＣカード、トークン、クライアント証明書、生体認証を利用した複数要素による認証方式を採用すべきである。ただし、複数要素認証は、不正アクセスの発生リスクが高いU→Dへのアクセス部分に必要とするものであり、D内部、あるいはA方式におけるD→Hへのアクセス認証については必須ではない（A方式ではHは通信設定においてDからの接続のみ受け付けるよう設定可能であるため）。いずれにおいても、U側の認証に必要な操作が極端に煩雑にならないよう配慮が必要である。

2-2）アクセス権限制御

アクセス権限制御については、[1]U→Dへのアクセス、[2]D内部、あるいはA方式におけるD→Hへのアクセスを考える必要がある。

[1]については、ファイアーウォールやVPNルータ等による接続元・接続先IPアドレス制限を行うことが望ましい。具体的には、事前にUにTのグローバルIPアドレスを申請させてファイアーウォールで制限を行うことや、VPN接続時に利用者ごとのプロファイルによって接続先IPアドレスを限定することなどが考えられる。サイバー攻撃のリスクを考慮すれば、接続元を日本国内に限定する、あるいはDでWebアプリケーションを配置する場合はWAF（Web Application Firewall）を導入することも有効な対策である。[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、その管理責任は事務局が負うことが望ましい。

[2]については、Uごとにどの H（のデータ）へのアクセスを許可するかを制御する仕組みが必要である。このステップにおいて複数要素認証が行われないと想定するならば（前項参照）、Uの利用者間のなりすまし（たとえばUの業務に無関係なHにログインを試みてデータを閲覧する）のリスクを低減する対策が必要である。とりわけ、利用者数が増大した場合の運営状況を想定すると、H側から見て、自施設に無関係な多数のUの存在が脅威となりうる。この場合、Uの業務に無関係なHに対してはTからのネットワーク通信を遮断しておく方法が有効である。[2]は、各々H側においてUのアクセス権限設定（どのUに自施設へのアクセスを許可するか）の管理責任を負うことが望ましい。

2-3）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稼働している場合であっても、U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は残存する。これについては、Tでのコピー＆ペーストや印刷を禁止するしくみを導入すべきである。具体的には、デスクトップ仮想化技術やアプリケーション仮想化技術によって実現可能である。

３）A方式

3-1) 利用者管理・利用者認証

A方式では、UはTを使いH側のEの機能を直接利用してデータ閲覧を行う。このため、Hで考慮すべきは、[1]T→Hの通信開始および[2]Eの利用開始に付随する認証をどのように実装するかという点である。[1]について、2-2)で述べた「ネットワークレベルでのUのアクセス権限設定」が実施される場合は、Dを通過した段階ですでに「HにアクセスすべきでないU」は排除されている。したがって、H側で改めて利用者認証を行わず、次項で述べるネットワークレベルのアクセス権限制御を行い、利用者認証は[2]に委ねるのが現実的であろう。[2]については、HのEの利用者認証機能をそのまま利用するため、H

においては次項で述べるEのアクセス権限設定を適切に行う必要がある。

また、Eのシステム側でシングルサインオン（SSO：Single Sign-On）の機能が用意されていれば、本システムとの間で利用者認証情報を連携させることも条件（仮想化技術やE側の認証システムの組み合わせなど）が整えば技術的に可能であると思われる。Uが他者のアカウントを利用してEにログインすることを防止するために、可能であればE側でSSOを実装することが望ましい。とくに、UがHに所属する医療従事者のアカウントを悪用した場合にはきわめて重大なインシデントとなることに留意する。SSOを実装しない場合おいては、P－H間の契約においてアカウント悪用に対する厳しいペナルティを課すことにしたうえで、Uからのアクセスの都度、遅滞なくEのアクセスログ監査が実施可能な体制をH側で整備すべきである。

3-2) アクセス権限制御

まずネットワークレベルのアクセス制御について述べる。A方式においては、Tからの通信がHの内部ネットワークに配置されたEに到達する必要がある。このためには、H側ネットワークで$S_A$→E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。一般的に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は厳しく制限されているのが普通であり、H側ではD→H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。

セキュリティ保持の観点からは、H側ファイアーウォール等で接続元（D側）IPアドレスの制限を行ったうえで、IPSecなどの技術によりD－H間で拠点間VPNを構成することが望ましい。この際、VPN 装置あるいはVPNソフトウェア間の認証に証明書を利用することで第三者による「なりすまし」を防止する。VPN通信の起点をD側とする場合は、通信の必要があるときのみ（オンデマンドで）VPNを構成することが可能である。H側で固定的なグローバルIPアドレスを保有していない場合は、VPN通信の起点をH側とし、D－H間で常時VPNを構成することになる。VPN内での$S_A$→E方向の通信制御はH側のVPNルータあるいはL3スイッチ等で行う。

つぎに、Eのアクセス権限設定について述べる。各々のHにおいて、以下のような点について適切にEの利用者マスタメンテナンスを実施する必要がある。

①Uにデータの閲覧権限のみを付与する。
②E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、Uに必要最小限のデータのみの閲覧権限を付与する。
③U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、最終項目については、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E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、Eの認証情報入力画面（ログイン画面）の表示を抑止する。

3-3）情報保護

A方式においては、UはEの画面を直接操作することになるため、データ漏洩を防止するために、H側でデスクトップ仮想化技術やアプリケーション仮想化技術を実装することが望ましい。

3-4）システム構成例

A方式によるリモートSDVシステムのシステム構成例を図２上に示す。以下では、主たる構成要素と、具体的な想定される製品名について述べる。

＜P側＞

・USBメモリ:利用者に配布し認証デバイスとして利用する。
・USBメモリ用OS（Microsoft Windows To Go):USB接続ドライブから起動可能なOS。
・仮想化クライアントソフトウェア（Ericom PowerTerm WebConnect）：Tから、DのVPNゲートウェイ、コネクションブローカを経由してHの仮想化デスクトップ環境に接続するためのソフトウェア。

＜D側＞

・VPNゲートウェイ（Ericom SecureGateway):Tと暗号化通信を行う。
・コネクションブローカ（Ericom PowerTerm WebConnect)：Uの権限を確認し、TからHへの接続要求を適切に振り分ける。
・仮想HUB（SoftEther Pakcetix VPN)：Hごとに割り当てられるD内部のL2スイッチ。H側の管理によりUによるEへのアクセス制御設定を行う。
・認証サーバ（Microsoft ActiveDirectory)：Uの認証情報を一元的に管理する。

＜H側＞

・仮想化デスクトップ（Microsoft RDP Server):Eにアクセスするための仮想端末として機能し、データ漏洩防止機能を有する。

3-5）システム運用方法

本システム構成における運用フローを以下に述べる。

①事務局は、Uの認証情報を認証サーバに登録する。認証情報のうち、認証ID、およびUがTを利用して$S_A$に接続した際に割り当てられるDの内部IPアドレスをHに通知する。
②事務局は、Uに配布するUSBメモリを準備する。USBメモリの内容はUごとに固有の認証情報が埋め込まれ、容易に書き換えができないように設定を施す。
③事務局は、Pとの契約のもとでU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。
④Hは、Pとの契約のもとで、自院に割り当てられた仮想HUBに対してUの認証IDと内部IPアドレスを許可登録する。またUがEにログインし対象患者のデータ閲覧ができるよう設定を行う。
⑤UはUSBメモリを挿入した状態でTを起動する。TはUSBメモリ内部のOSから起動する。起動時にUはOS起動のためのPINの入力を求められる。
⑥TのOS起動が完了すると、自動的にVPNゲートウェイに接続する。接続の際に、Uは認証IDとパスワードの入力を求められる。
⑦VPNゲートウェイとの接続完了後、Tはコネクションブローカに接続し、参加医療機関Hの選択肢を表示する。
⑧UはHのうち一つを選択し接続する。UがHに対する接続権限を与えられている場合は、Hの仮想HUBにおいて通信許可が与えられている（④）ため接続は成功する。そうでない場合は、Tから、Hに対応するEにはネットワーク通信ができないため接続は失敗する。
⑨接続に成功した場合、TはHの仮想化デスクトップ環境にアクセスできる。UがVPNゲートウェイで入力した認証情報は、コネクションブローカを経由してHの仮想化デスクトップ環境に引き渡される。EがSSOに対応している場合は、当該認証情報を利用してTはEに自動的にログインする。そうでない場合はEのログイン画面を表示し、Uが手動でEにログイ

ン操作を行う。

3-6）システムの特徴・留意事項

本システムの特徴は、以下のとおりである。

・USBメモリの利用により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、H側の仮想環境に対して直接的に接続を振り分けることができる。これによりD側で本来配置すべきポータルサイトなどの中間的なしくみを削減できる。またUが入力した認証情報をHの仮想環境に引き渡すことができ、多段認証環境におけるUの運用負荷を軽減することができる。
・H側で自院の仮想HUBの管理を行うため、DからHへのネットワークレベルでのアクセス権限をHが主体的に制御することができる。
・H側では仮想化デスクトップ環境を準備するだけで、多くの場合E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。

・UはDからのインバウンドアクセスを許可しておく必要があるため、ファイアーウォールなどの外部ネットワーク接続機器の設定には十分な配慮と注意が必要である。
・UはEを直接操作するため、Eの瑕疵・脆弱性によって、Hが意図せずU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PとH間の契約で対応を定めておく必要がある。
・Hに所属しない部外者UがE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H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となる。

4）B方式

4-1）Hからのデータ転送・データ閲覧

B方式では、Hから転送された診療情報を蓄積し、Uの閲覧に供するためのモニタリングサーバ（以下、サーバ）を設置する。サーバに転送するデータを抽出するために、Eより対象患者の情報（閲覧期間を限定した最低限の情報）を抽出するプログラム（以下、抽出プログラム）を開発する必要がある。抽出する情報の範囲と条件は、以下を想定している（参照：分担研究者山口の報告書）。

・抽出期間：同意取得日（または同意取得前1ケ月程度）～最終来院日（または追跡期間終了日）
・抽出する診療科情報：治験を担当した診療科及びその他の診療科
・抽出する情報：被験者ID（電子カルテシステムの患者IDを変換させることを想定）
・来院等情報（受診日・入院日・退院日・死亡日）
・傷病情報（病院オーダーや退院サマリの情報）
・処方・注射情報
・検体検査情報・生理検査情報・薬物血中濃度検査情報
・細菌検査
・カルテ記事
・治験の記録（テンプレートに入力された情報）

以下では、上記の情報をSS-MIX2標準化ストレージから抽出し、原則としてフォーマット変換を行わず（SS-MIX2形式のままで）サーバに転送する場合を想定する。これらの情報のうち標準化ストレージで対応できないデータ種（カルテ記事、治験の記録、監査証跡、タイムスタンプ）については、別途E側で拡張ストレージを用意し、それぞれに独自フォーマットを定義し格納することになる。

抽出プログラムは、日次などの一定間隔のバッチ処理にて抽出と転送を実施する。

4-2）アクセス権限制御

サーバはD内部に設置する。サーバを１台に集約するのが最も効率的ではあるが、2-2)で述べた「ネットワークレベルでのUのアクセス権限設定」の要件を考慮するのであれば、Hごとにサーバを設置することになる。Hごとにサーバを設置する場合は、サーバのファイルシステムにおいてUごとにフォルダを用意し、当該フォルダに対して閲覧権限を付与したうえで、Uの閲覧可能な患者データをそこに格納すればよい。U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ためには、抽出プログラム側でUと対象患者のひもづけ情報を管理しておく必要がある。

4-3）システム構成例

Ｂ方式によるリモートSDVシステムのシステム構成例を図２下に示す。

4-4）システム運用方法

本システム構成における運用フローを以下に述べる。①～⑦まではＡ方式と同じであるため記載を省略する。

⑧UはHのうち一つを選択し接続する。UがHに対する接続権限を与えられている場合は、Hの仮想HUBにおいて通信許可が与えられている（④）ため接続は成功する。そうでない場合は、Tから、Hに対応するモニタリングサーバにはネットワーク通信ができないため接続は失敗する。

⑨接続に成功した場合、Tはモニタリングサーバに接続するための仮想化デスクトップ環境にアクセスできる。UがVPNゲートウェイで入力した認証情報は、コネクションブローカを経由して仮想化デスクトップ環境に引き渡される。Uはデータ閲覧ソフトウェアを利用してUに割り当てられたフォルダ内のデータファイルを参照する。

4-5）システムの特徴・留意事項

本システムの特徴は、以下のとおりである。

・USBメモリの利用により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、H側の仮想環境に対して直接的に接続を振り分けることができる。これによりD側で本来配置すべきポータルサイトなどの中間的なしくみを削減できる。またUが入力した認証情報をHの仮想環境に引き渡すことができ、多段認証環境におけるUの運用負荷を軽減することができる。
・H側で自院の仮想HUBの管理を行うため、DからHへのネットワークレベルでのアクセス権限をHが主体的に制御することができる。
・UはDからのインバウンドアクセスを許可する必要がなく、内部ネットワークに対する脅威が少なく、サイバー攻撃などの影響を受けにくい。

ただし、以下の点には留意が必要である。

・診療情報を限定して抽出しているため、電子化原資料のすべてを確認できるわけではない。また情報の正確性は抽出プログラムの精度に依存するので、抽出プログラム本体に対するバリデーション等の手続きが必要となる可能性がある。
・現時点では、最低限の診療情報に限定したとしても、SS-MIX2標準化ストレージの対象外のデータ種が存在する。このため、Hごとに抽出プログラムのカスタマイズが必要となる可能性が高い。またデータ閲覧ソフトウェア（SS-MIX2ビューワ）についても別途追加開発が必要になるものと思われる。この点については、SS-MIX2拡張ストレージの活用について十分なコンセンサスを得て開発を進める必要があると考えられる。

## D．考察

A方式とB方式を比較すると、コスト面ではA方式が優位である。これは、抽出プログラムとデータ閲覧ソフトウェアにかかる開発コストの差である。医療機関ごとの個別カスタマイズをできるだけ少なくするためにはSS-MIX2標準化ストレージを利用することが最も望ましいが、これが導入されていない医療機関においては別途導入費用がかかることになる。また拡張ストレージの取扱いについても議論が必要である。

一方、医療機関の内部ネットワークに対する安全性については、B方式が優位である。医療機関によっては、外部から電子カルテネットワークにアクセスさせないというポリシーを強固に守る可能性があり、このような場合はB方式によるリモートモニタリングが有効であろう。

## 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（A方式)、およびモニタリングに最低限必要な情報を医療機関の電子カルテからデータセンタ等のサーバに転送し閲覧させる方法（B方式）について、必要となる要件の検討を行い、システム構成および運用方法について提案を行った。その結果、一定のセキュリティを保持しつつ、利用者および医療機関の実運用を踏まえた実現可能性の高いシステムの構成モデルが提示できたと考える。

本研究においては、今後、多施設での展開を考慮して、まずはコスト面で優位であるA方式についてシステムを試験的に構築し、複数の医療機関で実証実験にとりかかる予定である。実証実験においては、リモートSDVを実施する上での標準業務手順書の作成、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評価する予定である。

一方、B方式におけるコストの問題を解決するためには､SS-MIX2のさらなる活用を目指しつつ、対象外となる診療情報の取り扱いについて、別途検討の場が必要であると考える。

## F．健康危険情報

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

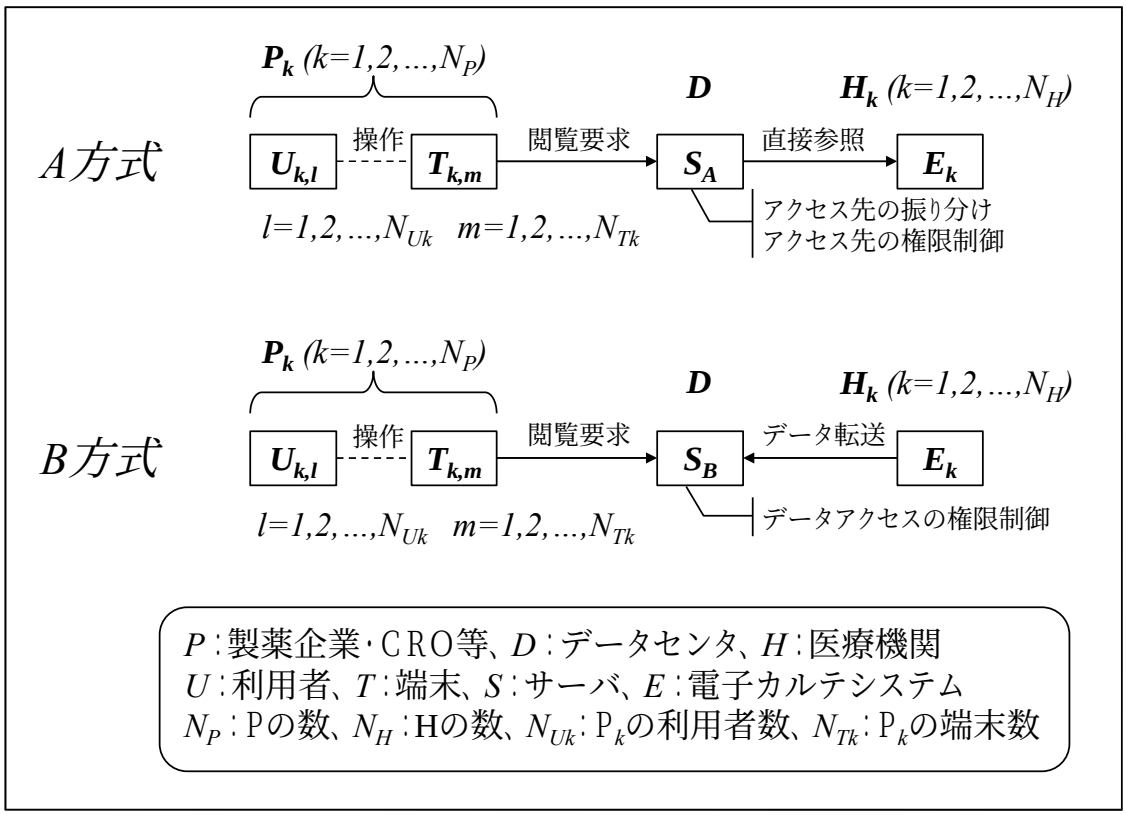


**図１．本研究におけるリモートＳＤＶシステムのモデル（Ａ方式・Ｂ方式）**

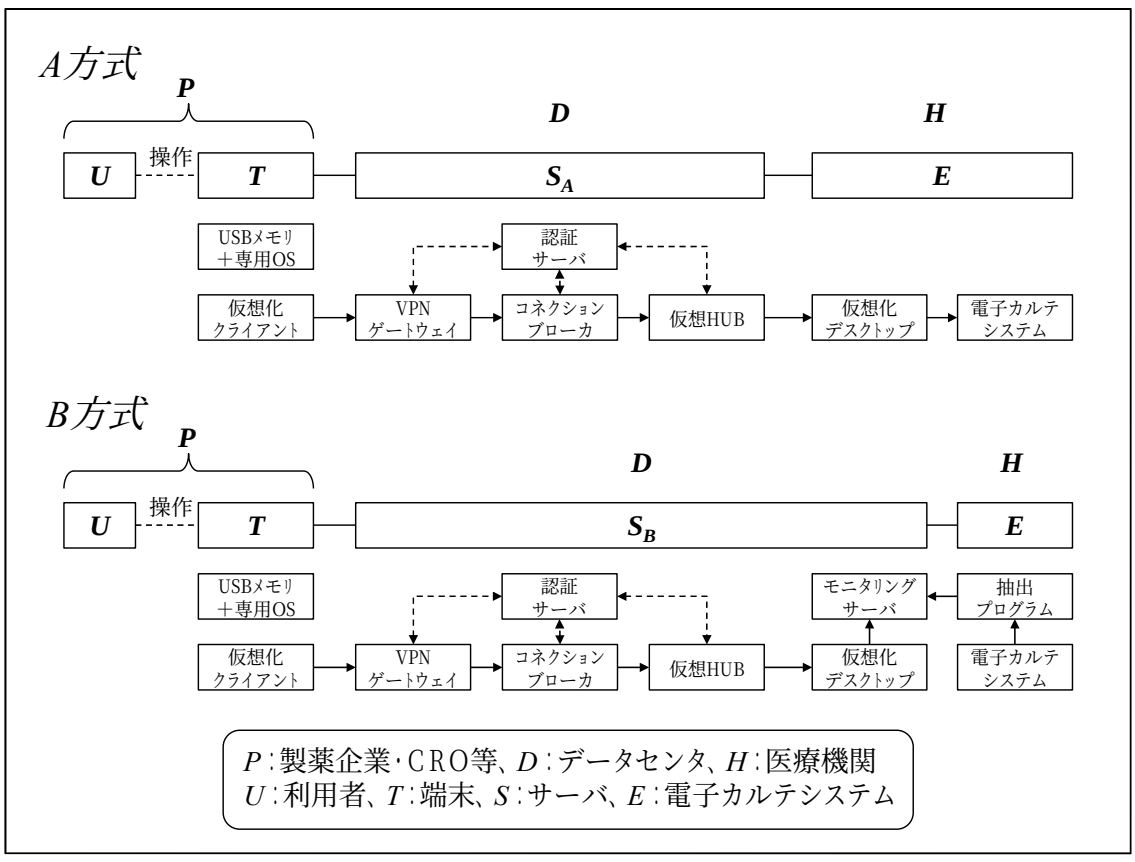


**図２．リモートSDVシステムの構成例（Ａ方式・Ｂ方式）**