Trusted Web の実現に向けたユースケース実証事業

成果報告書

臨床試験及び医療現場における

信頼性及び応用可能性の高い情報流通システム

2023 年 3 月 20 日（提出日）

代表機関：シミック株式会社

ヘルスケア情報流通システム開発コンソーシアム

目次

1　背景と目的

1.1　事業の背景

臨床試験及び医療業界では、現在においても重要な情報及びプロセスが紙媒体に記録されていることが多い。これにより、紙での運用が前提となっているものが多数存在し、更新内容の把握・最新版の共有方法が煩雑になり、工数を要している事例が存在する。以下がその一例である。

＜臨床試験＞

治験薬管理表[1]、業務委任記録（Delegation Log）[2]、トレーニング記録（Training Log）[3]、ワークシート[4] など

＜実臨床現場＞

診療情報提供書　など

一方、既存の医療情報電子化システムを導入している場合にも、情報の信頼性、共有・流通の利便性及びコストベネフィットの観点で課題が顕在化している。以下がその一例である。

- 他人のアカウント情報を使用した医療従事者のなりすまし行為のリスクがあり、発生時にも技術的に検証困難
- システムの導入に際しては、ライセンス・構築・運用に多額のコストが必要になると共に、専門人材が必要（例：臨床試験でいえば EDC（Electronic Data Capture）[5]など）
- 医療情報は非常に機密性が高く、情報の共有・流通に際しては ID 管理や真正性、トレーサビリティ等が特に求められるが、既存のシステムは中央集権的で単一障害点を持つため機能的に必要十分ではない

加えて、近年、Wearable Device やオンラインコミュニケーションツールの普及に伴い治療の場も病院から生活の場に広がり、患者を中心としたケアを目指す方向性にシフトしており、臨床試験業界では分散型臨床試験（Decentralized Clinical Trial: DCT[6]）デザインの確立、医療業界では PHR

---

[1] 治験薬が管理され、治験依頼者より提供された「治験薬の管理に関する手順書」に従って、治験薬が管理され、被験者に適切に使用されたことを記録しておく文書。

[2] 治験のデータや被験者の安全に係るような重要な業務について、誰が何の業務を担当するかという「担当者とその責任範囲」を明確にするもの。

[3] 情報周知の証として残したトレーニング完了記録　（日付と実施者の署名等）。

[4] 臨床試験等において通常カルテに記録されない試験固有の検査結果や医師の所見及び評価を中心に、実施計画書（臨床試験等の実施に関する必要な事項を定めた文書。）で収集が規定されている試験データを記録する病院内で使用する様式のこと。

[5] インターネットを使い電子的に臨床データを収集すること、またはそのシステムを指す。電子的臨床検査情報収集ともいわれる。

[6] デジタル技術を活用し、病院に来院することなく患者の自宅など遠隔地で実施する臨床試験等のこと。

（Personal Health Record）[7]及び EHR（Electronic Health Record）[8]データの利活用が実現すべき大きな方向性として掲げられている[9]。これらの実現には、関係者間の信用を確保した上で情報の信頼性を担保する情報流通システムが必要不可欠である。

上記の現状及び将来的な方向性を鑑みて、相互に信用したユーザ/コミュニティ内で臨床試験及び医療に関する電子ファイルやデータをリーズナブル且つシンプルな UI/UX で共有・流通可能なシステムが必要であると考えた。その際、大前提として以下の要素について担保する必要があるが、大規模で中央集権型のシステムを構築するのではなく、Keychain Pte. Ltd.（以下、Keychain 社）の提供する Blockchain フレームワークである Keychain Core[10]の technical capability を活用し、応用可能性の高いコンセプトでの企画・開発に重点を置いた。

- ✧ 自己主権型デジタルアイデンティティ（SSI）
  ユーザーのデバイスによって制御されながら作成されるデジタルアイデンティティのことで、Keychain Core の場合は暗号キーペア
- ✧ データ真正性
  データのデジタル署名を検証する機能
- ✧ データセキュリティ
  静止時および飛行中のデータをエンドツーエンドで暗号化する機能
- ✧ 合意形成
  アプリケーションの状態（またはデータの受け入れ）について、2 者の間で合意に達することができる機能

なお、Keychain Core は上記に加えて以下の機能を提供する。

- ✧ キーマネジメント（暗号キーペアの管理）
- ✧ ネットワークグラフ
- ✧ キーロールオーバー

---

[7] 個人の健康・医療・介護に関する情報のこと。

[8] 医療機関が患者の既往歴、病態把握に必要な各種検査の結果（医用画像も含む）、医師の所見と診断を記録する診療録、処方箋（オーダー情報）などを電子的に記録・管理するしくみのこと。

[9] https://www.mhlw.go.jp/content/12601000/000976105.pdf
https://www.jpma.or.jp/information/evaluation/results/allotment/lofurc000000xnw9-att/lofurc000000xo2k.pptx
https://www.cas.go.jp/jp/seisaku/iryou_dx_suishin/pdf/siryou6.pdf
https://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/iryou_kaigo_kenkou.html
https://www.mhlw.go.jp/content/10904750/000546640.pdf
https://www.mhlw.go.jp/content/11909500/000741661.pdf

[10] Keychain Core は、Singapore Fintech Award など、多数の表彰を受けているアプリケーション開発フレームワーク。ブロックチェーン技術や分散台帳技術を一般的な開発チームでも実装できるような環境を提供し、自己主権的デジタルアイデンティティ、データセキュリティ、さまざまな端末や通信環境における合意コンセンサス・取引を実装可能。

- ✧ ID
- ✧ データ検証
- ✧ 任意のトランザクション

1.2 事業の目的

臨床試験及び医療現場における機密性の高い医療情報を関係者で共有する上で、旧来の紙運用及び臨床試験や医療機関個別の運用に部分最適化されたシステムに依存せず、リーズナブルで且つ情報の信頼性を担保するシステムを設計することで、関係者間で必要なときに必要な医療情報を共有できる環境の構築を目指す。

2 事業の概要

2.1 事業概要及び実証の範囲

臨床試験における「病院スタッフ」と「製薬会社/CRO（Contract Research Organization）[11] スタッフ」間、実臨床現場における異なる 2 つの病院（A 及び B）のスタッフ間における情報共有を想定した事業スキームを想定して開発を進める。

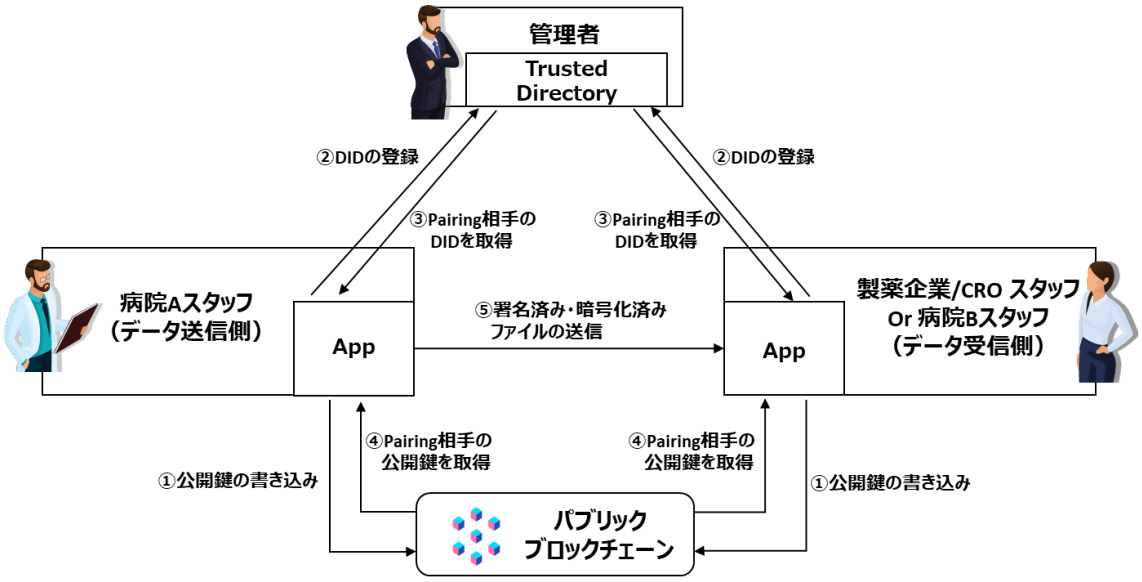


図 2.1-1 事業スキーム図

図 2.1-1 事業スキーム図について以下説明する。

【主体】

[11] 開発業務受託機関のこと。製薬会社から医薬品開発における臨床試験や製造販売後調査の業務を受託している企業。

・ 管理者
  - 本システムを利用する病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフを管理する。
  - ファイルの送受信ができるスタッフ同士の組み合わせを管理する。ファイルの送受信を行えるスタッフ同士の組み合わせ情報のことを「Contact List」と呼ぶ。つまり、管理者は Contact List を管理する。
・ 病院 A スタッフ（データ送信側）
  - 自分の PC でデータ受信側に送信したい臨床試験データや診療データ等を含むファイルを作成する。（ファイルの形式は問わない。例えば Microsoft word や Excel など）
  - 作成したファイルを、App を用いてデータ受信側のみが検証・復号化できる形で署名・暗号化し、データ受信側へ送信する。（復号化及び署名の検証を行える相手は Contact List で管理される。）
・ 製薬企業/CRO スタッフ or 病院 B スタッフ（データ受信側）
  - データ送信側から受領した暗号化ファイルを復号化・署名の検証を行う。
  - 復号化したファイルを閲覧する。

【構成】

・ Trusted Directory
  - Web アプリケーションで管理されるデータベースを指す。
  - 以下の 2 点の機能を有する。
    ① 本システムを利用する病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフ情報と、Contact List を格納する。
    ② 監査証跡（ファイルの暗号化及び復号化の履歴）を格納する。Web アプリケーションを介して暗号化と復号化の履歴が書き込まれ、また App に監査証跡を追加
  - 管理者は Web アプリケーションで上記の①を管理する。
・ App
  - 病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフが自分の PC にインストールして使用する Windows アプリケーションを指す。
  - デバイスに紐づく DID を生成し保持する。
  - 任意のファイルをデータ受信側のみが検証・復号化できる形で署名・暗号化し、データ受信側へ送信する。
  - 受信した暗号化ファイルを復号化及び署名の検証を行う。
・ パブリックブロックチェーン
  - DID の管理基盤として利用する。
  - App は生成した DID の公開鍵をパブリックブロックチェーンに書き込む。
  - App はパブリックブロックチェーンからデータの送受信を行う相手（Contact List）の DID の公開鍵を取得する。

なお、CMIC（株）が受託した臨床試験または臨床研究においては CMIC（株）が管理者となる。CMIC（株）が受託していない臨床試験または臨床研究で CMIC（株）が本システムのみを提供する場合においては、その臨床試験または臨床研究にて管理者を指名する形になる場合がある。

2.2　社会・経済に与える価値・影響

製薬/CRO 市場の市場規模、成長率及びその他関連情報は以下の通り。

＜製薬市場＞[12]

	売上 2021 年	成長率 2017-2021 年 CAGR	成長予測 2022-2026 年 CAGR
Global	約 192 兆円	5.1 %	3 ~ 6 %
Japan	約 11 兆 5,000 億円	-0.5 %	-2 ~ 1 %

CAGR：Compound Annual Growth Rate（年平均成長率）

- 世界の製薬市場は持続的成長が見込まれるが、本邦は市場が縮小し、売上・国際競争力低下の懸念あり。
- 世界の製薬市場は 2026 年までに CAGR 3 ～ 6% で成長し、約 243 兆円に達すると予想されている。

＜CRO 市場＞[13,14]

	売上 2021 年	成長率 2013-2021 年 CAGR	成長予測 2022-2029 年 CAGR
Global	約 8 兆 4,694 億円	–	12.1 %
Japan	約 2,255.6 億円 (前年より 20.8%増加)	1.71 %	–

- 世界の CRO 市場は持続的成長が見込まれる。その 1 つの要因として、欧米を中心にデジタル企業が本市場に進出したことで既存システムの技術革新及びプロセスイノベーションが進んでいることが挙げられる。加えて、規制当局も技術革新に合わせて柔軟且つ積極的にレギュレーションの

[12] The Global Use of Medicines 2022 Outlook to 2026; IQVIA Institute, Dec 2021

[13] The global CRO services market; FORTUNE BUSINESS INSIGHTS

[14] Japan CRO Association 2021 年年次業績報告

見直しを図っている。

- 一方、本邦における今後の成長性は未知数ではあるが、薬価制度の存在及びコスト高等により Global Pharma にとって本邦で臨床試験を行うことの魅力が低下している懸念があると共に、技術革新及びそれに伴うプロセスイノベーションの観点で欧米から遅れを取っていることは否定できない。

- 医薬品開発に要する期間と成功確率 [15]
  - 医薬品の開発には 10 年以上の時間と数百億～数千億円規模の費用が必要
  - 成功確率は年々低下（20 年前:0.0077%→現在:0.0044%）し、難易度が上昇
- 本邦における年間の臨床試験数（企業治験・医師主導治験・特定臨床研究）[16]
  以下、試験開始日が 2021 年中の試験の集計結果である。（小数点以下切り捨て）

	試験数	実施医療機関数/1 試験	被験者数/1 試験
企業治験	613	8.7	392
医師主導治験	71	5.4	47
特定臨床研究	389	9.6	125

- 本邦と欧米間のドラッグ・ラグ [17,18,19]
  - 日米間のドラッグ・ラグ：0.6 年
  - 2020 年までの直近 5 年間に欧米で承認された新薬 246 品目のうち、72%（176 品目）が日本では未承認。国内未承認薬の割合は、2016 年から 2020 年までの間で 16%上昇

医薬品開発、医療業界に身を置くものとして、当コンソーシアムはアナロジー思考でオペレーションをより最適化していく必要があると強く感じており、他産業で勃興した最新の技術・コンセプトを積極的に取り入れることで、本邦の医薬品開発、医療業界の国際競争力をより高めていく必要があると考えている。その点、欧米は技術革新に合わせて柔軟且つ積極的にレギュレーションを見直すなど、規制当局側が市場の革新・拡大を後押ししている。事実として、海外では Tokenization[20]を元にした情報流通の検討が既に進んでいる。本ユースケースは、臨床試験及び医療現場における情報共有の信頼性向上、検証領域の拡大及びコスト削減を実現しつつ、応用可能性の高いコンセプトとすることで、医薬品開発及び医療業界の国際競争力の向上に寄与する。

更には、本ユースケースを通して臨床試験及び医療現場における情報共有の新たなオペレーション

[15] 医薬品産業ビジョン 2021 資料編; 厚生労働省

[16] jRCT をもとに当社独自算出

[17] 海外で既に承認されている薬が日本国内で承認されるまでに、長い年月を要するという問題のこと。

[18] ドラッグ・ラグの試算; PMDA

[19] ドラッグ・ラグ：国内未承認薬の状況とその特徴; 製薬協

[20] 機密情報をトークンと呼ばれるランダムに生成された代理データに置き換えて保存・利用する技術のこと。

を提言することで、レギュレーションの見直しに向けた後押しにしたいと考えている。

また、今後の臨床試験及び医療現場はより分散型で情報を収集・共有・流通する必要性がある。その点、本ユースケースのコンセプトは「病院－患者間」の情報共有（例：患者の持つ Wearable Device 等）にも応用可能であり、既に検討を進めているが、本実証の範囲には含めない。

2.3　コンソーシアムの体制

本コンソーシアムは、シミック株式会社（以降 CMIC（株））を代表機関として、同社と参加団体である Keychain Pte. Ltd.により構成される。CMIC（株）は、実証全体の統括及びアプリケーション企画・開発等の役割を担う。Keychain Pte. Ltd.は Keychain Core SDK の提供及びアプリケーション企画・開発におけるサポート、コンサルティングの役割を担う。

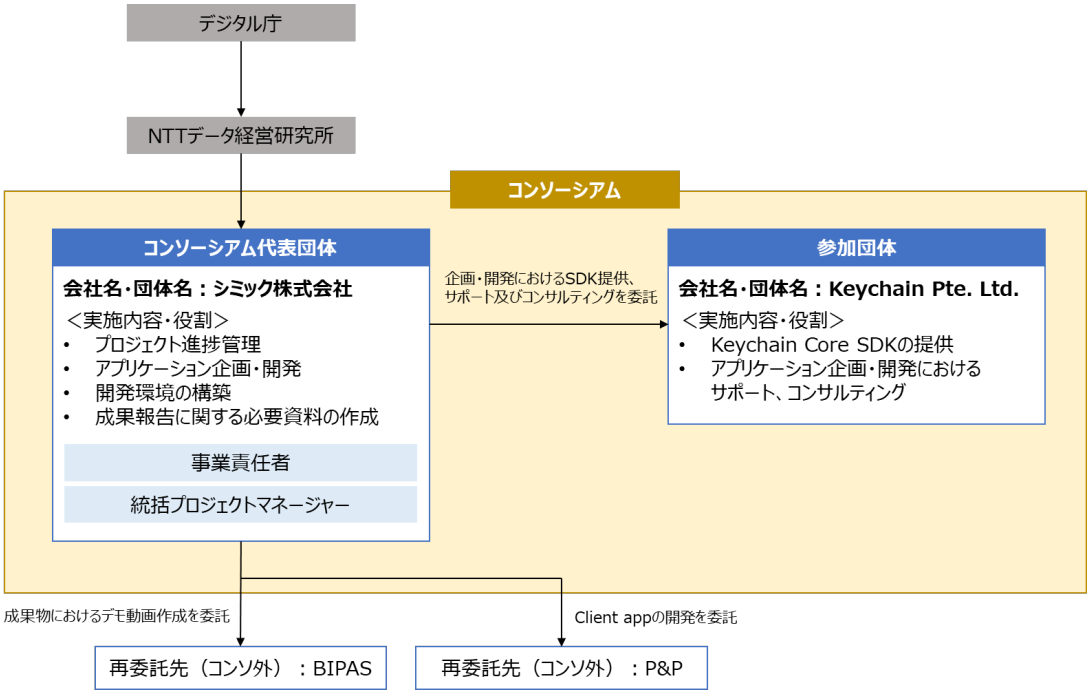


図 2.3 実施体制図

2.4　実証全体のスケジュール

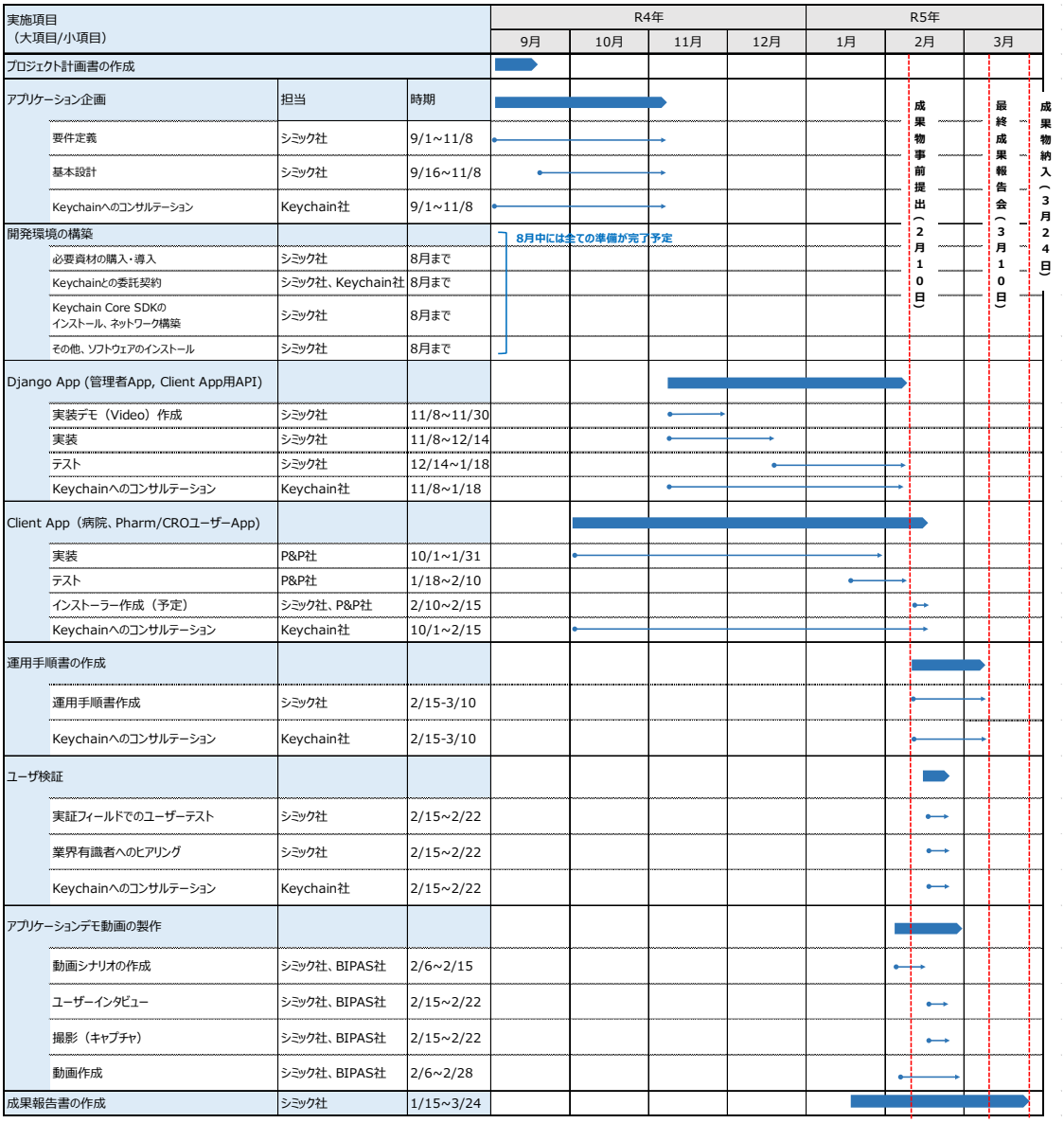


図 2.4 実証全体スケジュール

3　実証内容

3.1　実証の実施事項、論点及び判断

本実証事業の前提となる臨床試験におけるステークホルダーの関係図は以下の通りである。

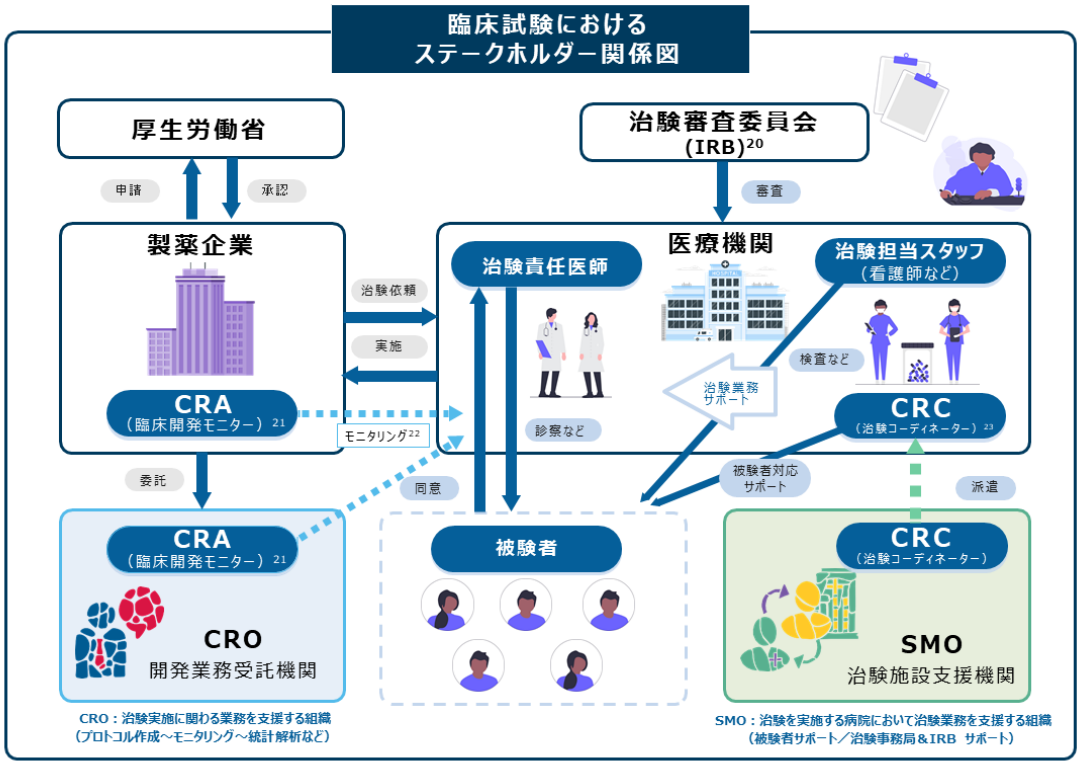


図 3.1.1　臨床試験等におけるステークホルダー相関図 [21,22,23,24]

---

[21] Institutional Review Board の略。治験開始前に医療機関で治験を正しく実施できるか、また治験が正しく実施されているか審査する委員会。

[22] Clinical Research Associate の略。臨床開発モニターともいう。医療機関で実施されている臨床試験が、GCP（Good Clinical Practice の略。日本においては「医薬品の臨床試験の実施の基準に関する省令」のこと）に準拠して実施されているかを調査・確認する職業。

[23] 医療機関で実施されている臨床試験が、GCP に準拠して実施されているかを調査・確認すること。

[24] Clinical Research Coordinator の略。治験コーディネーターともいう。 医療機関において、治験責任医師・分担医師（いずれも治験を担当する医師のこと）の指示のもとに、医学的判断を伴わない業務や、治験に係わる事務的業務、業務を行うチーム内の調整等、治験業務全般をサポートする職業。

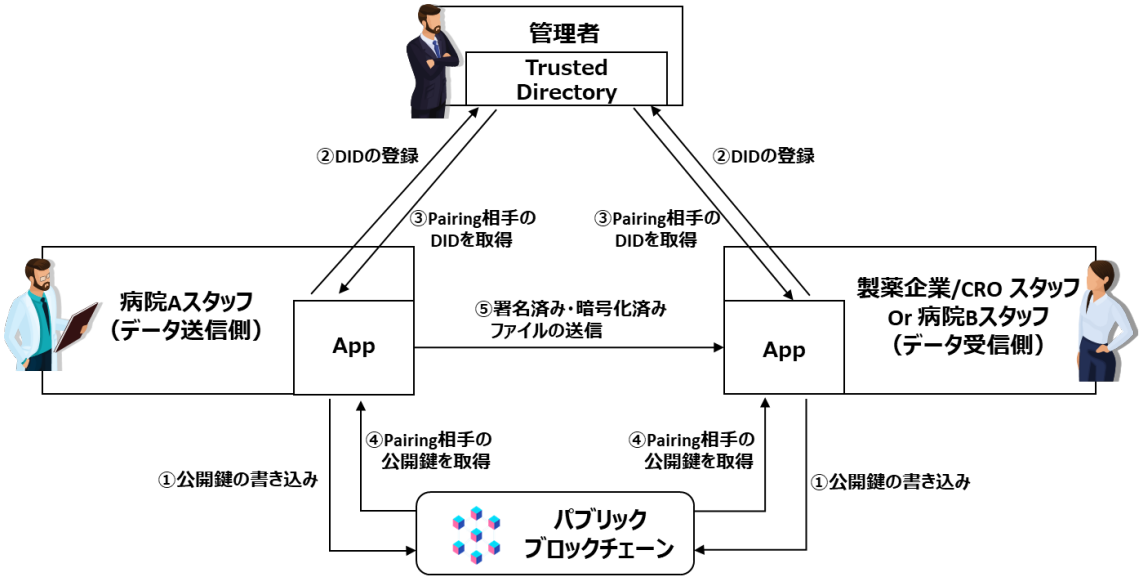


図 3.1.2 事業スキーム図（再掲）

図 3.1.1 の通り、臨床試験等においては多数のステークホルダーが関与する。ここで、臨床試験等を実施する病院（医療機関）と製薬企業/CRO の間では多数の情報のやり取りが実施される。当該情報は Clinical Data（所謂、症例報告書で収集される治験データ）と Operational Data（臨床試験が適切な管理下で遂行されていることを担保するため、GCP[25]（Good Clinical Practice）等の臨床試験関連の各種規制にて作成・記録が義務付けられている文書・データ）の 2 つに大きく分類されるがその内容は多岐に渡り、紙媒体やシステムへのデータ入力によりやり取りが行われる。加えて、当該情報に対して、被験者の人権と安全が保護され、最新の治験実施計画書および GCP を遵守して治験が実施され、記録、報告されていることを保証する業務として CRA によるモニタリングが実施される。

ここで、[1.1 事業の背景]に記載の通り、紙媒体及びシステム利用の如何に因らず多くの課題が山積していることに加え、情報の管理・記録・共有に多数の工数を要することでコスト増にも繋がっている。今回のユースケース事業においては、この点の課題解決を主要なスコープとした。

3.1.1 プロトタイプの企画・開発

（１） 要件定義

- 本事業における実証範囲

  本ユースケースは個人主権（被験者・生活者）でデータを管理した先に、個人との同意[26]形

[25] Good Clinical Practice の略。日本においては「医薬品の臨床試験の実施の基準に関する省令」のこと

[26] ヘルスケアまたは臨床試験及び臨床研究等の文脈で、患者又は生活者と医療従事者または臨床試験及び臨床研究棟の実施団体・実施者との間で形成される同意のことを本報告書では「同意」と呼ぶ。具体的には以下の通り。

・患者または生活者が臨床試験及び臨床研究等に参加することへの同意

・患者又は生活者が自身のヘルスケアに関する情報または臨床試験及び臨床研究等で収集される対象となる情報を、医療従事者または臨床試験及び臨床研究棟の実施団体・実施者へ提供することへの同意

成のもとで治験データを eSource（ePRO、Wearable Device、app など）から直接取得する世界感を目指しているが、現時点における現場の理解及びレギュレーションとの乖離が大きいためすぐに活用できるとは限らない。しかしながら、中長期的に実現すべきと考えるコンセプト及びアーキテクチャは前述の世界観であるため、今回の実証事業においてバックエンドはこの世界観を見据えて構築し、フロントエンド（クライアントアプリ）は病院-製薬会社/CRO の 2party 間における短期的且つ顕在的な課題解決をスコープとして開発することとした。

- Keychain 社の Keychain Core を採用した背景
  主に以下 4 点の理由から、Keychain Core は臨床試験及び医療現場において親和性があると判断した。
  1. Keychain Core の持つ DID のコンセプトと、臨床試験及び医療業界における情報の共有・流通に求められる要件には高い親和性があるものと考える。例えば臨床試験においては、その情報の機密性から病院の治験担当者と製薬会社/CRO の治験担当者間でのみ情報共有が必要であり、且つ治験担当者以外の不特定多数が情報を参照できない環境構築が不可欠となる。現在の多くの臨床試験では、この点を可能な限り担保するために多くのリソースを要した人的なオペレーションによる管理体制の構築や、既存システムの導入による管理を行っている。しかしながら、情報の信頼性やトレーサビリティ、セキュリティなどの観点において多くの顕在化した課題が存在する。
  2. 次世代ウェブ（Web3, Trusted Web）の構築に求められる構成要素とされる デジタル・アイデンティティ, データセキュリティ, ヴェリファブル・クレデンシャルなどは、技術的に開発難易度が高く、実現には多額の開発費用が必要となる。Keychain Core は、DID の作成と維持、データのエンドツーエンド暗号化、検証可能なクレデンシャル、鍵のロールオーバー、アプリケーションレベルのコンセンサスを提供可能である。
  3. Keychain Core の DID はデバイスに紐づける形で実装される。臨床試験では、試験に参画する病院スタッフ毎に業務の範囲が厳密に区分されており、その範囲を超えた業務を行っていないことを保証することが重要である。それは EDC などのシステムを用いた業務も同様であり、システムを利用する病院スタッフ毎に発行したアカウントによりシステム内での業務可能範囲をコントロールしている。しかし、既存のシステムは中央集権的でアカウントの認証には ID/Password を用いている場合が多く、ある病院スタッフが他のスタッフへ ID/Password を故意に渡すことで業務を不正に代行する形でなりすましが行われることがある。Keychain により DID をデバイスに紐づけてアカウントコントロールを行うことで、上記のように ID/Password を他のスタッフに渡すことによるなりすましを排除できる可能性がある。
  4. 1.、2.、3. にて記載した通り、Keychain によりデバイスに紐づく DID を実装できる。この DID により分散型のアーキテクチャを目指すことで単一障害点の回避を実現する。単一障害点の回避は PHR（Personal Healthcare Record）利用実現のための重要な要素である。なぜなら、医療・ヘルスケア分野においてスマホや各種ウェアラブル端末か

ら収集した PHR の利用を考慮すると、データの信頼性や帰属性等を担保するために各端末の認証が必要となるが、端末数は利用者・患者の数に応じて非常に膨大となることが想定されるからである。膨大な端末及びデータを扱う上で、セキュリティやプライバシーを十分に担保するためには、単一障害点を回避することが重要である。本実証ではスマホや各種ウェアラブル端末から収集した PHR の利用はスコープ外としているが、本実証において Keychain の DID 実装による単一障害点回避の実現することにより、PHR 利用実現に応用ができる可能性がある。

- Cloud storage を用いたデータの受け渡しについて
  Keychain の機能により、授受されるデータ自体が暗号化され、Pairing した相手のみが復号化できるため、授受の方法はセキュリティに影響しない。また、臨床試験ではデータの作成プロセス、つまり臨床試験データの事実経過の再現を可能とする記録（監査証跡）が求められるため、当該要件については更新前後のファイルの照合及びデータの授受の記録により担保することを想定し、授受されたすべてのファイルにおいてその順番を特定できる形で保管することとした。
  その方法として、以下の 2 つを検討した。
  ① 全ての授受されたファイルを送信者及び受信者の双方が自己のデバイス内で保管する
  メリット：完全な分散型。データのコントロールは当事者のみで実施可能。
  ② デメリット：双方のデバイスで管理されているデータの完全な同期を担保し、且つデバイスのスペックに依存しない動作を実現する設計が必要となり、実装コストが高い。また、デバイス紛失により情報漏洩のリスクがある。送信者及び受信者の双方がアクセス可能な Web 上のストレージに保管する
  メリット：①における同期の必要性がない。既存のストレージサービスから各種必要要件を満たすものを選択するだけであり実装が容易。
  デメリット：中央集権的になるため、保管データのセキュリティや保守性などがストレージ提供者に依存し、単一障害点を形成し得る
  →上記①②を勘案し、②のデメリットに挙げたセキュリティ面（非改竄性及び秘匿性）に対しては Keychain Core の機能により解決できることから②を採用した。
- Cloud storage として BOX を採用した背景
  CMIC グループの社内規定に基づいた Vendor Qualification を通してセキュリティ等の評価が社内的に完了しており、現時点においては CMIC グループ内で標準使用されているため BOX を採用することとした。

（2） 基本設計

- Trusted Directory（TD）の設計
  当初は TD の管理者という存在は想定しておらず、病院スタッフまたは製薬会社/CRO スタッフ自身が app 利用時に入力する病院及び試験情報をもとに TD 上にドメインが自動作成も

しくは参照する形で、自身の URI を当該にドメインに登録する仕様で考えていた。しかしながら、当該仕様における以下 2 点の課題が顕在化した。

1. 悪意を持った病院スタッフまたは製薬会社/CRO スタッフの故意により、本来登録されるべきではないドメインに自身の URI を登録することが可能となってしまう。これにより、意図的に担当外の試験の情報を入手可能となる。
2. 適切且つ共通のドメイン名（病院名と試験名の組み合わせ）を入力しないと、同一のドメインに登録されるべき URI が別ドメインに登録されてしまい、URI の交換が行われず Pairing が実行されない。
   例：病院スタッフ A 及び B は同一病院で同一試験を担当するスタッフ
   病院スタッフ A：「医療法人●●●会▲▲▲病院_ABC 試験」と入力
   病院スタッフ B：「▲▲▲病院_ABC 試験」と入力
   同一の病院及び試験名を意味するにも関わらず、異なる別のドメインが作成されてしまう。

上記課題の解決策として以下 2 つを検討した。

A) 同じドメイン上に登録されたすべての DID と自動的に Pairing するのではなく、Pairing するもの同士がリアルタイムで相手に間違いが無いことを確認した上で Pairing を行う。
B) TD 内で Pairing 可能な病院スタッフまたは製薬会社/CRO スタッフの組み合わせを管理する者（管理者）を置く。

A)は、システム利用者同士が自ら Pairing する相手を確認することができるメリットがあるが、臨床試験における情報のやり取りは基本的に非同期で行われ、また、Pairing すべきスタッフ（同じ試験-病院に参画するすべての病院スタッフと製薬会社/CRO スタッフ）は 10 名～数十名程度であるため、リアルタイムでお互いを確認することは現実的ではない。従って、非同期での Pairing が可能となる B）を採用することとした。Pairing 情報は集中管理を行う一方、アイデンティティ自体は病院スタッフまたは製薬会社/CRO スタッフ自身で管理可能であり、従来の集中管理によるアカウントコントロールと比較するとセキュリティが担保された。

- TD 上の病院スタッフ及び製薬会社/CRO スタッフ情報へのアクセス（ログイン）について
  上記 TD の設計変更により、部分的に集中管理されている病院スタッフまたは製薬会社/CRO スタッフ情報へのアクセスコントロールを行う必要が発生した。これは既存の方法（ID＆パスワードまたはワンタイムパスワード）を検討し、なりすましリスクがより低減できるワンタイムパスワードを本実証終了後に採用予定である。本機能は既存の機能であり、本実証事業内における検証の必要性は低いと判断し、ID によるログインのみを実装している。

（３） システム開発

- 要件定義、基本設計にて検討した事項を踏まえシステム開発を行った。要件定義及び基本

設計までに全ての検討が済んでいたため、システム開発の時点での検討事項は特になかった。。

（４） ユーザテスト

2023 年 2 月 21 日に医療法人相生会臨床研究部門の協力を得てユーザテストを実施し、プロトタイプシステムにおいて期待した挙動及び効果が確認できた。本件詳細については「3.1.2 ヒアリングの実施」にて記載する。

3.1.2 ヒアリングの実施

（1） ヒアリング概要

2 月 21 日：医療法人相生会臨床研究部門（以下、相生会）[27]にてユーザテスト及びヒアリングを実施

2 月中：社内外の有識者及びステークホルダーに対してヒアリングを実施

（２）ヒアリング結果

＜相生会担当者＞

- 病院やアカデミア主導で実施する臨床研究や疫学調査など、低コストでの計画及び実施が要求されるため現状ではデータインテグリティを担保できていない試験に対して導入したい。例えば、紙の CRF や Excel ファイルで研究データを収集している事例が挙げられる。
- 臨床試験や臨床研究等を実施する病院として、データの改竄やなりすまし行為を意図的に実施することは勿論あり得ないが、一方でシステム的にも運用的にも当該行為をやろうと思えば出来る環境にあることは間違いない。今回のプロトタイプシステム等を用いることで、当該行為が根本的に実施不可能な環境にすることができれば、医療機関だけでなく治験依頼者及び CRO の立場にとっても有用なシステムになると感じる。
- 今回のプロトタイプシステムのアーキテクチャ及び得られる効果は、今後のあるべき姿の一事例であるとも感じる。一方で、医療現場及び臨床試験業界における現時点で要求されているデータインテグリティの考え方と比較するとオーバースペックであるとも感じるため、今回のプロトタイプシステムのアーキテクチャ更には Trusted Web ホワイトペーパーで要求される技術要件について社会全体に浸透させていくような活動も必要だと感じる。

＜某大学の医療情報部門責任者・担当者＞

- 一般診療における医療情報を取り扱う上では HL7 FHIR への対応が必須である。また、PHR においても今後同様の標準規格化の動きがあるため、この動きに合わせたシステム設計が必要である。
- 現時点での所感としては、一般診療ではなく、臨床試験や臨床研究等の別規程下で運用管理される情報のやり取りという点では、一つの事例として可能性を感じる。

---

[27] https://souseikai-crd.com/
2023/3 時点で試験実施数：5,500、年間組み入れ被験者数：9,000、専門スタッフ：350

＜社内のデータマネジメント担当者＞

- 今回のプロトタイプシステムが現行の EDC とのリプレースを目的としたものではなく、あくまでも DCT への展開や臨床試験や臨床研究等における情報のやり取りにおける新しいコンセプトであると理解した上でのコメントとして、現行の EDC とだけ比較した場合にはこのシステムではログはファイル単位になる。EDC、CDMS[28]ではデータごとに監査証跡の形でログを残すが、このシステムではファイルを送るまでログが取れず、ファイルが暗号化されるまでのログが残せない。この点については、現行の EDC との相違点として社外への説明方法も含めて検討が必要と考える。一方で、臨床研究や疫学調査など、臨床試験と比較するとデータインテグリティの担保に対する要求度が高くない領域においては現行のプロトタイプシステムでも十分有用性がある。
- （以下、相生会担当者と同様の見解）
  今回のプロトタイプシステムのアーキテクチャ及び得られる効果は、今後のあるべき姿の一事例であるとも感じる。一方で、医療現場及び臨床試験業界における現時点で要求されているデータインテグリティの考え方と比較するとオーバースペックであるとも感じるため、今回のプロトタイプシステムのアーキテクチャ更には Trusted Web ホワイトペーパーで要求される技術要件について社会全体に浸透させていくような活動も必要だと感じる。

以上より、実施に対して多額のコストが掛かっている試験及び研究に対して、既存のプロセス自体に大きな変更を加えずにプロセス内での業務内容の簡素化を実現することで、Low cost model での実施可能性が示唆された。一方で、今回のプロトタイプシステムのアーキテクチャ更には Trusted Web ホワイトペーパーで要求される技術要件について、医療・製薬業界を含む社会全体に浸透させていくような活動も必要だと感じた。

3.1.3 国際的な関係規制の調査

調査内容臨床試験におけるデータマネジメント及びシステム設計に関する以下関連規制について調査を実施した。

【調査対象】

① 留意しなければならない国際的な関係規制の全般の特定

② ①の中でも特に臨床試験で使用するシステム設計における仕様検討等に影響を及ぼす関係規制の特定

【調査方法】

CMIC（株）データマネジメント担当者へのヒアリング

【調査結果】

[28] Clinical Data Management System の略。臨床試験等においてデータを管理するためのツールであり、病院（治験実施施設）で症例報告書に記載されて集められたデータは最終的に CDMS に格納・管理される。

① 留意しなければならない国際的な関係規制は以下の通りであることを確認した。

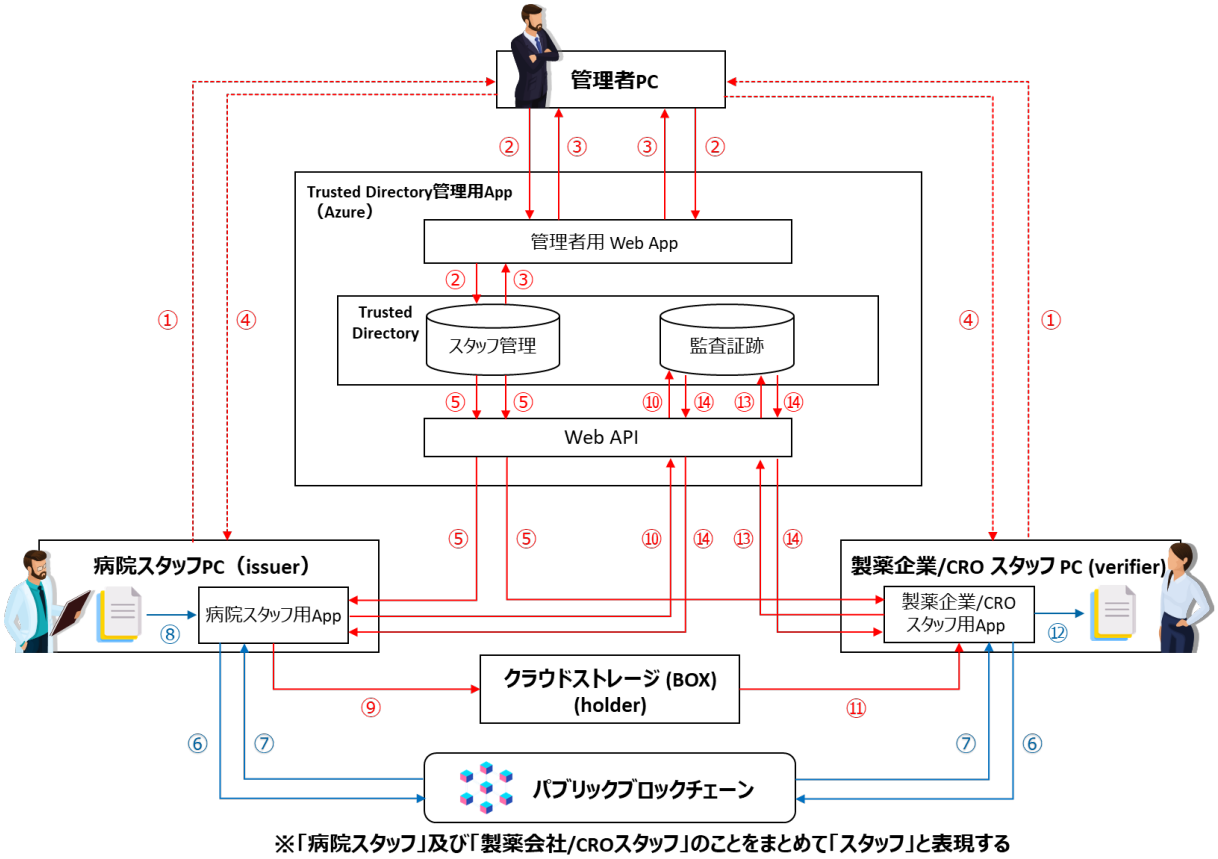
- GAMP（Good Automated Manufacturing Practice）[29]
- ICH-GCP（Good Clinical Practice）[30]
- 21 CFR part11[31]
- ER/ES 指針 [32]（Electronic Record/Electronic Signature）

② ①の中でも特に留意すべきところは GAMP にて要求される CSV 対応であることを確認した。

GAMP にて要求される CSV への対応については本実証事業終了後に CMIC（株）データマネジメント担当者と共同で着手することとした。

3.2 検証できる領域を拡大する仕組み

3.2.1 データフロー



① 利用申請、スタッフ情報の提供	⑧ 任意のファイルを暗号化

[29] https://ispe.org/initiatives/regulatory/what-gamp
[30] https://www.pmda.go.jp/int-activities/int-harmony/ich/0028.html
[31] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
[32] https://www.mhlw.go.jp/web/t_doc?dataId=00ta8216&dataType=1&pageNo=1

② スタッフ情報を TD に登録	⑨ 暗号化ファイルをクラウドストレージへ格納
③ スタッフ ID の発行	⑩ 暗号化履歴を TD に書き込み
④ スタッフ ID を用いてログイン	⑪ クラウドストレージから暗号化ファイルを取得
⑤ スタッフ情報と Contact List を TD から取得	⑫ ファイルを復号化し閲覧
⑥ スタッフ情報を用いて DID を作成し、 公開鍵をブロックチェーンへ書き込み	⑬ 復号化履歴を TD に書き込み
⑦ 送受信を行う相手のデバイスの DID の公開鍵を取得し Pairing	⑭ 監査証跡を TD から取得して閲覧

図 3.2.1 データフロー図

- データの保管場所
  - 臨床試験データはクラウドストレージ（BOX）に保管する。クラウドストレージは単にファイルの授受を行うために使用する物であり、データの送信先である特定の製薬会社/CRO スタッフしか復号化出来ない形で暗号化されたファイルを保管する。（暗号化前のファイルは病院スタッフがローカルで保持し、復号化後のファイルは製薬会社/CRO スタッフがローカルで保持するため、各スタッフ PC がデータの保有者であり保管場所であると捉えることも可能と考える）本システムでは以下の形で BOX のフォルダを構成する。

    ＜BOX のフォルダ構成＞

    本システム用のルートフォルダ

    ├試験 A-病院 A 専用フォルダ

    ├試験 A-病院 B 専用フォルダ

    ├試験 B-病院 A 専用フォルダ

    ├試験 B-病院 C 専用フォルダ …

    （試験とその試験に参画する病院の組み合わせの数だけフォルダを作成する。）
  - 監査証跡は Trusted Directory (TD)に保管する。TD は基本的には単なるデータベースであり、以下 2 つの機能を持つ。

    ① 病院スタッフ又は製薬会社/CRO スタッフ情報、試験情報、病院情報及びファイルの授受を行うことのできる病院スタッフ又は製薬会社/CRO スタッフ同士の組み合わせ情報が格納される。

    ② 監査証跡を保管する。

    管理者は管理者用 Web App を用いて①を管理する。

- データの格納場所へのアクセスコントロール

  クラウドストレージ（BOX）のアクセスコントロールは BOX が提供するアクセスコントロール機能を用いる。BOX ではユーザごとにアカウントを発行し各アカウントに対してフォルダ毎の権限管理を行える。病院スタッフまたは製薬会社/CRO スタッフはアカウントで Web アプリ等にログインしフォルダやファイ

ルの作成や編集を行う。また、BOX では API が提供されており、API を用いてファイルのアップロードやダウンロードなどが可能である。
ステークホルダーごとに発行するアカウントは以下のとおり。
＜ステークホルダーに発行するアカウントとその権限＞
管理者：
本システム用のルートフォルダ以下すべてのフォルダ/ファイルの作成、編集、削除の権限を与える。（ただし、暗号化済みのファイルの復号化は行うことはできないためファイルの閲覧、編集は不可）

病院スタッフ又は製薬会社/CRO スタッフ：
病院スタッフは病院スタッフ App、製薬会社/CRO スタッフは製薬会社/CRO スタッフ App を用いて暗号化ファイルのアップロードとダウンロードを行う。それぞれの App からの BOX へのアクセスは以下の通り実装する。

- 病院スタッフ App または製薬会社/CRO スタッフ App は BOX アカウントへアクセスするのに必要な情報を埋め込んで病院スタッフ又は製薬会社/CRO スタッフに配布される。当該アカウントは本システム用のルートフォルダ以下すべてのフォルダ/ファイルの作成、編集、削除の権限を持つ。
- 病院スタッフ App または製薬会社/CRO スタッフ App は当該アカウントを用い、BOX API を介して BOX にアクセスする。
- TD には各試験-病院専用フォルダの BOX ID が格納されている。病院スタッフ App または製薬会社/CRO スタッフ App は Contact List と共に当該 BOX ID を TD から取得する。
- 病院スタッフ App または製薬会社/CRO スタッフ App は取得した BOX ID に紐づいた試験-病院専用フォルダにファイルのアップロード/ダウンロードを行う。

なお、病院スタッフ App または製薬会社/CRO スタッフ App に組み込んだ BOX アカウント情報は、病院スタッフまたは製薬会社/CRO スタッフから見ることができない形で当該 App に組み込む。そのため病院スタッフまたは製薬会社/CRO スタッフは App を介してのみ本システムで用いる BOX フォルダにアクセスすることができる。つまり、ブラウザ等を用いてフォルダ/ファイルへのアクセスは行えない。BOX アカウントのなりすましリスクとしては上記の管理者用の BOX アカウント情報及び病院スタッフ App または製薬会社/CRO スタッフ App に組み込んだ BOX アカウント情報が流出する場合がある。BOX に格納されるファイルは全て暗号化ファイルである（下記「暗号化ファイルのアクセスコントロール（誰がファイルを閲覧できるか）」参照）ため、ファイル内容の流出や改竄の可能性は低い。一方、当該アカウントによりファイルが削除されるリスクがある。

- 暗号化ファイルのアクセスコントロール（誰がファイルを閲覧できるか）
  病院スタッフは病院スタッフ App を用いて任意のファイルを暗号化する。この際、病院スタッフ App は TD から「同じ試験-病院に参画している病院スタッフ又は製薬会社/CRO スタッフのリスト」

（Contact List）を受け取り、そのリストに記載されているスタッフのみが復号化できる形で暗号化を行う。その後、製薬会社/CRO スタッフは製薬会社/CRO スタッフ App を用いてファイルを復号化する。つまり、TD 上で「同じ試験-病院に参画している病院スタッフ又は製薬会社/CRO スタッフ」のみが製薬会社/CRO スタッフ App を用いてファイルを復号化し閲覧できる。

- TD のアクセスコントロール

  TD は Microsoft の Azure Server に構築したデータベースである。TD 上には大きく分けて 2 つの情報が格納される。

  ① 病院スタッフ又は製薬会社/CRO スタッフ情報、試験情報、病院情報、及びそれらの紐づけの情報

  ② 監査証跡（データ授受の記録）

  ①については管理者用 Web App にて編集が可能である。当該 App には管理者のみがアクセス可能であり、ID とパスワードを用いてアクセスコントロールを行う。

  ②については Django で構築する Web API と病院スタッフ App または製薬会社/CRO スタッフ App を介して監査証跡を管理する。病院スタッフ App または製薬会社/CRO スタッフ App にてファイルの暗号化、復号化を行った際にその履歴が TD 上に保存される。また、病院スタッフ App または製薬会社/CRO スタッフ App にて監査証跡を閲覧可能であり、当該病院スタッフまたは製薬会社/CRO スタッフが暗号化または復号化を行ったファイルのすべての履歴を閲覧可能である。（その他のファイルの履歴については閲覧不可）

3.2.2 データフローに登場する主体とその概要

- 管理者
  - 本システムを利用する病院スタッフまたは製薬会社/CRO スタッフを管理する。病院スタッフまたは製薬会社/CRO スタッフから試験情報、その試験に参画する病院情報、その試験に参画する病院スタッフまたは製薬会社/CRO スタッフの情報を受領し、TD 上に保存する。また、病院-試験-参画スタッフの紐づけ情報を TD 上に保存し、同じ試験-病院の組み合わせを担当している病院スタッフまたは製薬会社/CRO スタッフのリスト（Contact List）を作成する。
  - 病院スタッフまたは製薬会社/CRO スタッフに病院スタッフ App または製薬会社/CRO スタッフ App を配布する。
  - 管理者は臨床試験データのやり取りを行わない。アイデンティティも持たない。
- 病院スタッフ
  - DID を持つ。
  - 自分の PC で臨床試験データを含むファイルを作成し、TD からダウンロードした Contact List を参照して自分と同じ試験-病院を担当している病院スタッフまたは製薬会社/CRO スタッフのみが検証・復号化できる形で署名・暗号化し、BOX 上の試験-病院専用フォルダに暗号化ファイルを保存する。

- 暗号化した履歴は TD 上の監査証跡に保存する。また、監査証跡を TD からダウンロードし自分の担当している試験-病院のファイルの暗号化・復号化のすべての履歴を閲覧する。

- 製薬会社/CRO スタッフ
  - DID を持つ。
  - BOX 上の自分が担当している試験-病院専用フォルダから暗号化ファイルをダウンロードし、ファイルを復号化・署名の検証を行ってファイルを閲覧する。
  - 復号化した履歴は TD 上の監査証跡に保存する。また、監査証跡を TD からダウンロードし自分の担当している試験-病院のファイルの暗号化・復号化のすべての履歴を閲覧する。
- クラウドストレージ（BOX）事業者
  - 暗号化ファイルを保管する。ファイルは暗号化されており事業者による閲覧、修正は不可。

3.2.3 検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容

- データの改ざん
  - 背景
    - 臨床試験等において現在使用されているシステムは、ID・パスワードによるアカウントコントロールを行っている
    - 過去これまでに一定数の ID・パスワードの流用によるなりすまし行為が発生しており、結論としてはデータ改竄もしくは不適切な担当者によるデータ登録となり、臨床試験等のデータの信頼性に疑義が生じる重大の事案に繋がっている
    - 臨床試験では、手順書に記載された順番で業務を行いその業務を行った記録を紙媒体で記録することが多い。当該記録が適切なタイミングで作成されていない場合、その原因を記述した経緯記録の作成等で追加の業務が多く発生することや、当該業務の及ぼす影響によっては臨床試験中止等の重大な結果につながる可能性がある。そのため、業務実施の記録をバックデートして作成する、修正履歴を付さないで修正を行う等の不適切な事例が発生している。
    - 臨床試験において収集される個々のデータは臨床試験の結果を大きく左右することがあるため、常に改ざんのリスクにさらされているといえる。例えば、臨床試験実施を依頼する製薬会社としては、臨床試験の結果を操作するため臨床試験データを不正に書き換えることにより利益を得られる可能性がある。[33]既存のシステムは中央集権的なシステムであるため、不正アクセスによるデータ改ざんのリスクが高く、かつ、データを送信する側である病院スタッフは、そのデータの改ざんを知ることが難しい。
  - ペインポイント

[33] 製薬会社は臨床試験データを収集した後に、そのデータを解析する。データを収集時に改ざんするのではなく、解析時に改ざんすることによっても臨床試験の結果を操作することも可能であるが、本ユースケースでは、臨床試験データを収集するまでをスコープとしているおり、収集したデータを製薬会社がどのように扱うかについてはスコープ外とする。

- ID・パスワードによるアカウントコントロールの場合、運用及びシステム環境的になりすまし行為が可能な状態になっており、それによるデータ改竄も可能な状態になっている
- なりすまし行為及びそれに起因するデータ改竄発生時に技術的に検証困難
- 紙媒体で情報の授受を行う場合、バックデートを伴う記録の作成や必要な修正履歴が記載されない修正等が行われるケースがある
- 中央集権的なシステムでは不正アクセスによるデータ改ざんのリスクが高く、且つデータの改ざんを検知することが難しい

- 検証対象
  - ①送信データ（臨床試験データを含むファイルの内容）の真正性。
  - ②送信者、送信(暗号化)日時について改ざんされていない事。
- 検証方法
  - ①送信側のローカルで事前に特定した受信者のみが復号化及び署名の検証を行える形で署名及び暗号化し、受信側のローカルで送信者の署名を検証してから復号化する。
  - ②暗号化の監査証跡として、送信者及び暗号化日時を記録
- 検証者
  - 病院スタッフまたは製薬会社/CRO スタッフ
- データの保有者
  - クラウドストレージ事業者に移譲（ただし、あくまでも病院スタッフから製薬会社/CRO スタッフに対してデータを渡す際にクラウドサービスを経由することを選択しただけであり、クラウドストレージ事業者によるデータの中身のコントロールは不可能である。病院スタッフは暗号化前のファイルをローカルに保持しており、かつ製薬会社/CRO スタッフは復号化後のデータをローカルに保持するため、病院スタッフまたは製薬会社/CRO スタッフがデータの保有者であると捉えることもできると考える。）
- 発行者
  - 病院スタッフ
- データの置き場所
  - クラウドストレージ（BOX）
- アクセスコントロール
  - 病院スタッフまたは製薬会社/CRO スタッフのみアクセスでき、管理者及び患者は不可
- 成果・留意点
  - ①暗号化・復号化を Keychain Core の機能を利用して実装した。
  - ②監査証跡は Azure 上に構築したデータベース上に保管している。
  - ファイルが暗号化された状態で BOX 上に保管されていることにより、病院スタッフが送信したデータが改ざんされずに製薬会社/CRO スタッフに受信されることを担保することができた。また、ファイルの暗号化日時に誤りはなく、不適切なバックデート等が行われる余地がないことを担保することができた。あらゆるファイルのやり取りが可能なため、紙媒体で記録

していたデータも簡単にこのシステムでやり取りすることができる。なお、その製薬会社/CRO スタッフが受信したデータをどのように扱うかについては本事業においてはスコープ外である。

- ユーザのなりすまし
  - 背景
    - 臨床試験等において使用されているシステムは、ID・パスワードによるアカウントコントロールを行っている
    - 過去これまでに一定数の ID・パスワードの流用によるなりすまし行為が発生しており、結論としてはデータ改竄もしくは不適切な担当者によるデータ登録に該当し、臨床試験等のデータの信頼性に疑義が生じる重大の事案に繋がっている
  - ペインポイント
    - ID・パスワードによるアカウントコントロールの場合、運用及びシステム環境的になりすまし行為が可能な状態になっており、それによるデータ改竄も可能な状態になっている
    - なりすまし行為及びそれに起因するデータ改竄発生時に技術的に検証困難
  - 検証対象
    - ①TD に存在する病院スタッフまたは製薬会社/CRO スタッフ情報を本人が使用しているか。(ID は本人が利用しているか。第 3 者が利用していないか。)
    - ②本人が送信したデータであるか。
  - 検証方法
    - ①以下 2 つの方法で検証可能
      I. ワンタイムパスワードを実証終了後に実装予定。管理者用 Web App から TD 上に保存されたメールアドレスに対して、ワンタイムパスワードを送信する。
      II. DID はデバイスに紐づいており、あるデバイスで作成した DID を他のデバイスで使用することはできない。また、TD 上の 1 つの病院スタッフまたは製薬会社/CRO スタッフ情報から作成された DID が複数存在する場合、他のある DID が当該スタッフ情報由来の複数の DID のうち Pairing できるのは 1 つの DID のみである。例えば、図 3.2.3.1 の通り、病院スタッフまたは製薬会社/CRO スタッフ C（スタッフ C）が病院スタッフまたは製薬会社/CRO スタッフ A（スタッフ A）の DID A と Pairing を完了した後、病院スタッフまたは製薬会社/CRO スタッフ B（スタッフ B）がスタッフ A の ID でログインし、スタッフ A の情報を用いて DID A'を作成したとしても、スタッフ C は DID A'と Pairing することができない。

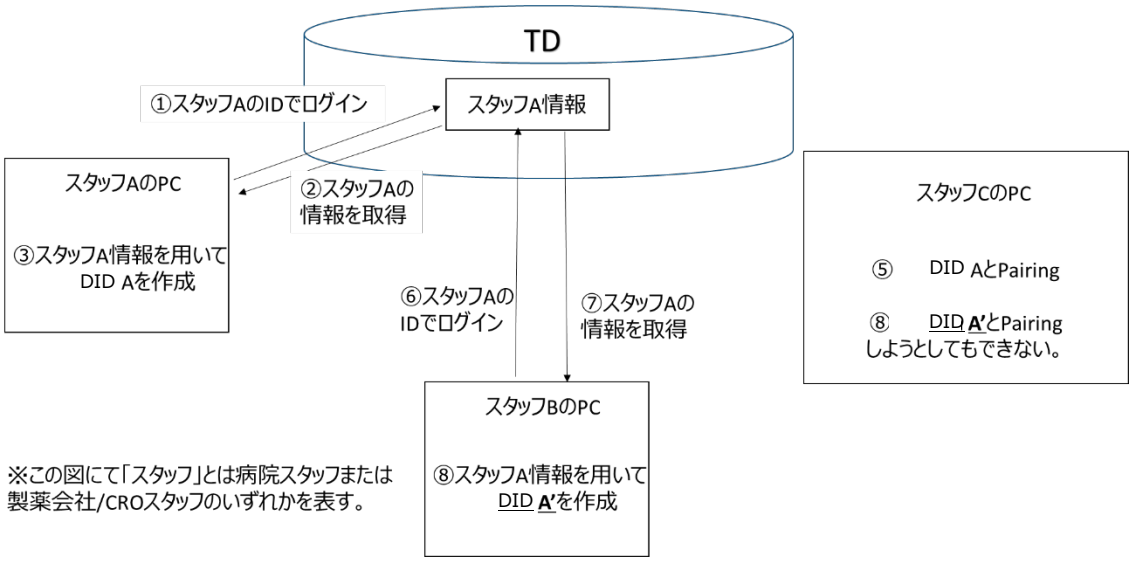


図 3.2.3.1 1 つのスタッフ情報から複数の DID を作成するスキーム図

・ ②電子署名

- 検証者
  - ・ ①-Ⅰ管理者用 Web App（病院スタッフ App または製薬会社/CRO スタッフ App から管理者用 Web App へ送信されるワンタイムパスワードが正しいことを管理者用 Web App が検証する。）
  - ・ ①-Ⅱ病院スタッフまたは製薬会社/CRO スタッフ
  - ・ ②製薬会社/CRO スタッフ
- データの保有者
  - ・ ①-Ⅰ管理者用 Web App（ワンタイムパスワードを生成し保持する。）
  - ・ ①-Ⅱ病院スタッフまたは製薬会社/CRO スタッフ
  - ・ ②クラウドストレージ事業者に移譲
- 発行者
  - ・ ①-Ⅰ管理者用 Web App（ワンタイムパスワードを発行）
  - ・ ①-Ⅱ病院スタッフまたは製薬会社/CRO スタッフ
  - ・ ②病院スタッフ
- データの置き場所
  - ・ ①-Ⅰ管理者用 Web App（ワンタイムパスワードを保持）
  - ・ ①-Ⅱ病院スタッフまたは製薬会社/CRO スタッフ PC
  - ・ ②BOX ストレージ
- アクセスコントロール
  - ・ 病院スタッフまたは製薬会社/CRO スタッフのみアクセスでき、管理者及び患者は不可
- 成果・留意点

- ①-Ⅰ今後解決すべき課題として特定した。本実証事業終了後に実装予定。
- ①-Ⅱ正しい病院スタッフまたは製薬会社/CRO スタッフが作成した DID と Pairing をすると、それ以降その Pairing 相手は異なるデバイスを使ってデータの授受を行うことはできない。このことにより Pairing 相手のなりすましを防ぐことができる。
- ②Keychain Core の機能を利用して電子署名機能及び電子署名を検証する機能を実装した。

- 提供範囲外へのデータの開示
  - 背景
    - 現状、臨床試験等で作成した電子ファイル及び紙書類の PDF は、メール添付やクラウドストレージサービスを使用してやり取りが行われている。
    - メールの誤送信や誤ったファイルの添付・格納により当該臨床試験等の担当者以外に機密情報が漏洩するケースが後を絶たない。
  - ペインポイント
    - 情報のやり取りの事前事後の両方にて、渡すべき人にだけ渡したい情報が渡っていることの検証が難しい。
  - 検証対象
    - 範囲外の病院スタッフまたは製薬会社/CRO スタッフに対してデータを送信していないか。（特定の試験、特定の病院を担当する病院スタッフまたは製薬会社/CRO スタッフのみに送信しているか）
    - 範囲外の病院スタッフまたは製薬会社/CRO スタッフから受信したデータでないか。（特定の病院で、特定の試験を担当する病院スタッフが送信したデータであるか）
  - 検証方法
    - TD にて送信相手（Contact List）を管理する。送信者または受信者は Contact List を確認してからデータを送信（暗号化）または受信（復号化）する。
  - 検証者
    - 製薬会社/CRO スタッフ及び病院スタッフ（暗号化/復号化時に Contact List を確認する）
  - データの保有者
    - 管理者（管理者用 Web App を用いて TD 上の Contact List を管理する）
  - 発行者
    - 管理者（管理者が管理する TD にて Contact List が作成される）
  - データの置き場所
    - TD
  - アクセスコントロール
    - 管理者が Contact List を管理する。（しかし、病院スタッフまたは製薬会社/CRO スタ

ッフは Contact List の内容を確認して問題が無い場合のみ暗号化、復号化を行う。つまり、病院スタッフまたは製薬会社/CRO スタッフは Contact List の内容に応じてデータを送信または受信するか否かの決定権を持つ。そのため、ある意味では病院スタッフまたは製薬会社/CRO スタッフがアクセスコントロールの最終的な権限を持つともいえる。）

- 成果・留意点
  - Keychain Core の機能を利用して実装した。

3.2.4 本システムで形成を目指す合意とその履行のトレースの内容

（１） データの管理（誰が誰のデータをどのように管理するのか）

【授受される臨床試験データ等を含むファイル】

データの流れは以下の通り。

- 病院スタッフがファイルを作成する
- 病院スタッフ App により暗号化され BOX にアップロードされる
- 製薬会社/CRO スタッフが製薬会社/CRO スタッフ App で受領したいファイルを選択する
- 製薬会社/CRO スタッフ App により暗号化ファイルが BOX からダウンロードされると共に復号化される

【病院スタッフまたは製薬会社/CRO スタッフ情報、試験情報、病院情報】

TD に保管される。その管理は管理者用 Web App をもちいて管理者が行う。

【監査証跡】

TD に保管される。病院スタッフまたは製薬会社/CRO スタッフが病院スタッフ App または製薬会社/CRO スタッフ App を介して記録と閲覧を行う。

（２） 合意事項（誰が誰と何について合意をするのか）

データの送信側（病院スタッフ）と受信側（製薬会社/CRO スタッフ）のデータ送受信者が互いに信頼しているということ及び信頼している間でのデータの授受

（３） 合意の条件（何を持って合意とするのか）

以下の流れでファイル授受が完了すること。

【ファイルの送信】

- 病院スタッフが臨床試験データを入力したファイルを作成する
- 病院スタッフ App で Contact List（当該ファイルを受領可能な病院スタッフまたは製薬会社/CRO スタッフ一覧）を確認
- ファイルを App にドラッグアンドドロップ
- 「暗号化」ボタンの押下

上記プロセスにより、送信するファイルとその相手を病院スタッフの意志で決定することが可能。

【ファイルの受信】

- 製薬会社/CRO スタッフが製薬会社/CRO スタッフ App で受領したいファイルを選択
- 製薬会社/CRO スタッフ App で Contact List を確認

- 「復号化」ボタンの押下
- 復号化されたファイルを閲覧

上記プロセスにより、どの病院スタッフが作成した何のファイルを受領するのかを製薬会社/CROスタッフの意志で決定することが可能。

上記送信と受信の完了を以って、ファイルの送受信について双方が合意したとみなす。

（４） トレースの方法（誰が・何を・どうやって）

- 病院スタッフと製薬会社/CRO スタッフが、自らが送受信に関与したデータ（暗号化又は復号化したデータ）の暗号化・復号化履歴及びその際の Contact List を監査証跡にて確認することでトレースすることが可能
- （３）で記載したファイル授受の流れにおいて、以下の内容が監査証跡に記録される
  - 暗号化/復号化が行われたこと。
  - 暗号化/復号化のタイムスタンプ
  - 暗号化/復号化を行った病院スタッフまたは製薬会社/CRO スタッフ名
  - 暗号化/復号化したファイル名
  - 暗号化/復号化した際の Contact List

この記録を確認することにより、（３）で記載したファイル授受の記録＝合意の記録を確認可能と考えている。

（５） 合意の取り消しの可否・方法

- BOX 上の暗号化ファイルを管理者が削除することにより合意の取り消しとする
- 合意の条件は（３）で示した通り特定のファイル授受が完了することにある
- そのため、暗号化ファイルを BOX から削除することにより、そのファイルの授受はできなくなる。具体的な流れとしては以下の通り。
  - （３）の合意の条件の流れでファイルの授受を行った後、送信側が「誤ったファイル送信してしまったこと」に気が付いたとする。
  - 送信側は管理者に、送信してしまったファイルの削除をメール等で依頼する。
  - 管理者は依頼を受けたファイルを BOX から削除する。
  - 以降、受信者は当該ファイルを受信することはできなくなる。
  - BOX から当該ファイルが削除される前にデータ受信側が受信及び復号化してしまった場合は、送信者から受信者へ復号化済みの当該ファイルを受信者の PC から削除するよう依頼する。

上記プロセスにより、合意が撤回されたとみなす。

3.3　6 構成要素との対応

3.3.1 検証可能なデータ

（１） 検証対象

① 送信データ（臨床試験データを含むファイルの内容）が改竄されていないこと、及び送信者及び送信（暗号化）日時が改竄されていないこと

② TD に存在する病院スタッフまたは製薬会社/CRO スタッフ情報を本人が使用しているか否か及び本人が送信したデータであるか

③ 範囲外の病院スタッフまたは製薬会社/CRO スタッフに対してデータを送信していないか。（特定の試験、特定の病院を担当する製薬会社/CRO スタッフのみに送信しているか）

（２） 検証者

製薬会社/CRO スタッフ

3.3.2 アイデンティティ

（１） アイデンティティとして想定されるもの

病院スタッフ PC、製薬会社/CRO スタッフ PC（Cloud Storage、管理者はアイデンティティを持たない）

（２） アイデンティティ管理システム

アイデンティティは、Keychain Core により実装される DID（各病院スタッフまたは製薬会社/CRO スタッフが各自の PC 等のノード上で作成する DID）にて実装する。アイデンティティ管理基盤としてパブリックブロックチェーンを用いている。なお、今回のユースケースでは何らかの証明（例：医師である証明など）を行うことはないため VC は未実装であるが、Keychain Core ではブロックチェーンを用いて VC の実装も可能である。）

（３） アイデンティティグラフとして想定されるものは何か

アイデンティティグラフとしては Pairing が該当する。Pairing とは 2 つの DID が互いに信頼している状態のことであり、Keychain Core により実装する。

- 2 つのアイデンティティそれぞれを識別する情報（アイデンティティ識別子等）
  DID の交換によって識別可能
- アイデンティティ間の関係を示すデータ
  Pairing はお互いが暗号化したデータを復号化可能であるという関係性を示す。

可視性については、各病院スタッフまたは製薬会社/CRO スタッフは Pairing 相手とのアイデンティティグラフのみが可視である。また、管理者はアイデンティティではないが、全てのアイデンティティグラフが可視である。

アイデンティティグラフの操作としては、Pairing する相手の取得及び Pairing の操作自体は各病院スタッフまたは製薬会社/CRO スタッフ（アイデンティティ）が行うが、一方で Pairing 対象を制御するのは全て管理者である。

本ユースケースでは、このアイデンティティグラフを担う Pairing が最も重要である。例えば製薬会

社 P が実施する試験 a 及び試験 b があり、その中で病院 A は試験 a と b の両方に参画しているとする。病院 A のスタッフの中には試験 a の担当スタッフ（便宜上 Hospital-Aa とする）と試験 b の担当スタッフ（Hospital-Ab）がいるとする。製薬会社 P には病院 A の試験 a のデータを受け取るスタッフ（Pharm-Aa)と病院 A の試験 b のデータを受け取るスタッフ（Pharm-Ab）がいるとする。

この時、Hospital-Aa が送信するデータは Pharm-Aa のみが受信し、Hospital-Ab が送信するデータは Pharm-Ab のみが受信する必要がある。もし Hospital-Aa が送信するデータを Pharm-Ab が受信してしまうと、重大な情報漏洩になる可能性がある。つまり、アイデンティティグラフに誤りがないことを送信者ー受信者の双方が確認してデータの送受信を行うことが重要である。

本プロトタイプシステムでは、Pairing している DID（病院スタッフまたは製薬会社/CRO スタッフ）同士のみでデータの送受信が可能である。Keychain Core の機能により、ファイルを暗号化する際に Pairing 相手のみが復号化できる形で暗号化が可能である。Pairing の組み合わせデータ（Contact List）は TD に保持し、Contact List は管理者が管理する。（TD 及び Contact List は Keychain Core に含まれる機能ではなく、本ユースケースにて新たに実装する機能である。）

また、病院スタッフと製薬会社/CRO スタッフは、データの暗号化及び復号化を実施する前に Contact List を確認可能であり、データの送受信を行う相手に問題がないことを確認可能である。（本ユースケースにて新たに実装する機能。）

3.3.3 ノード

（１） Wallet の使用有無

Wallet を使用している。病院スタッフ App 及び製薬会社/CRO スタッフ App では Keychain Core により DID を生成し当該 App 内で保存される。つまりエンティティである病院スタッフまたはが製薬会社/CRO スタッフがキーペアを自己主権的に保存する。

（２） 合意形成がされているか、されている場合その手段

DID 情報の交換による Pairing を実施した相手のみが復号化できる

（３） データのやり取りの記録場所

データの暗号化及び復号化の履歴は TD に記録する。TD は単なる DB であり、Azure 上に構築する。

3.3.4 メッセージ

（１） コネクションオリエンテッドかメッセージオリエンテッドか

通信自体はコネクションオリエンテッド（tcp/ip および HTTPS)である。なお、Trusted Web ホワイトペーパー2.0 では、トランザクションの説明の中で「コネクションオリエンテッドかメッセージオリエンテッドか」について言及されているが、本プロトタイプシステムでは、アイデンティティ間（病院ス

タッフと製薬会社/CRO スタッフのアイデンティティ間）のデータの送受信（＝暗号化ファイルの提供と復号化）はホワイトペーパーに定義されるトランザクションの形では実装しない。

3.3.5 トランザクション

（１） データのやり取りを記録するか

病院スタッフまたは製薬会社/CRO スタッフ自身が送受信に関与したデータ（暗号化又は復号化したデータ）及び全ての Pairing 履歴を残す。TD に暗号化と復号化の履歴を監査証跡として記録する。各ノードにおけるメッセージのやり取り履歴の保存は行わない。

（２） データのやり取りの検証はできるか

上記履歴を検証可能。一方でホワイトペーパーに記載される「検証（公開鍵暗号等を使った検証）」の意味では履歴データ自体を直接的に検証しない。なお、暗号化された全てのファイルは BOX に保存されるため BOX に存在する暗号化ファイルと暗号化履歴の記録を照合することにより、受信者は送信（暗号化）履歴の検証が可能ともいえる。

3.3.6 トランスポート

（１） トランスポートのプロトコル

BOX へのファイルアップロード及びダウンロード：HTTPS

Keychain Core：tcp/ip

3.4　本実証で企画・開発したシステムの概要

3.4.1　業務フロー

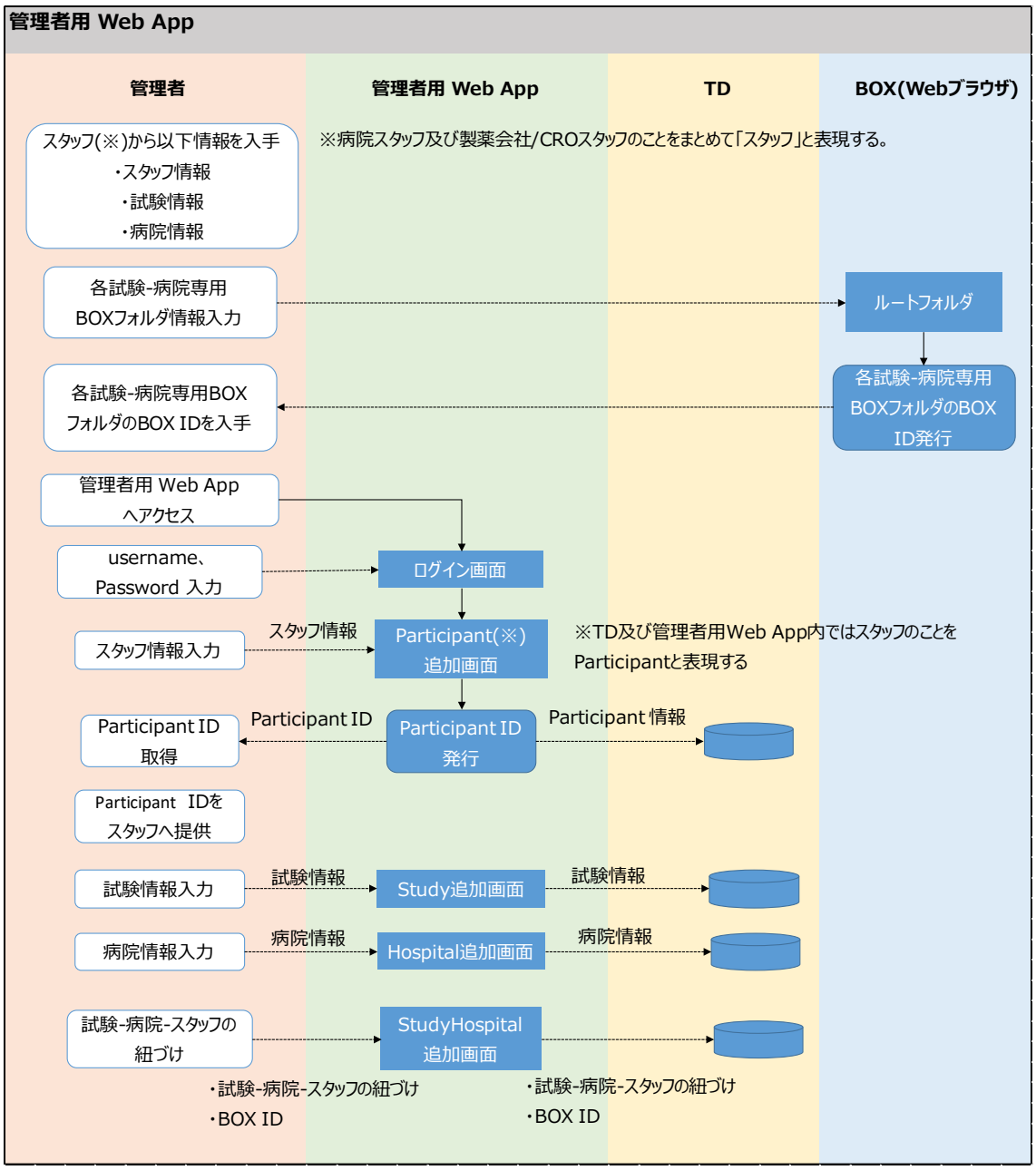


図 3.4.1.1 管理者業務フロー

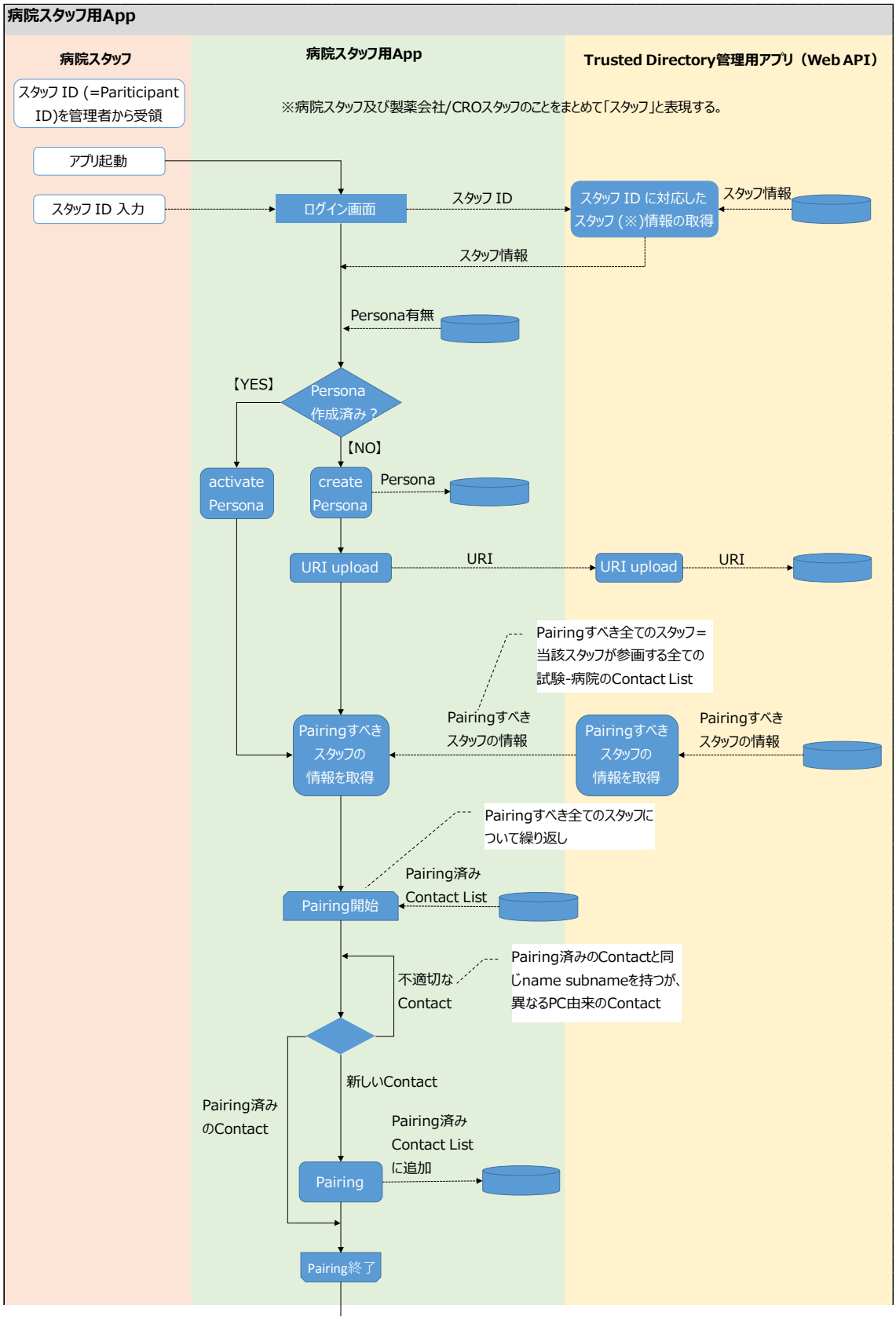


図 3.4.1.2-1 病院スタッフ業務フロー①

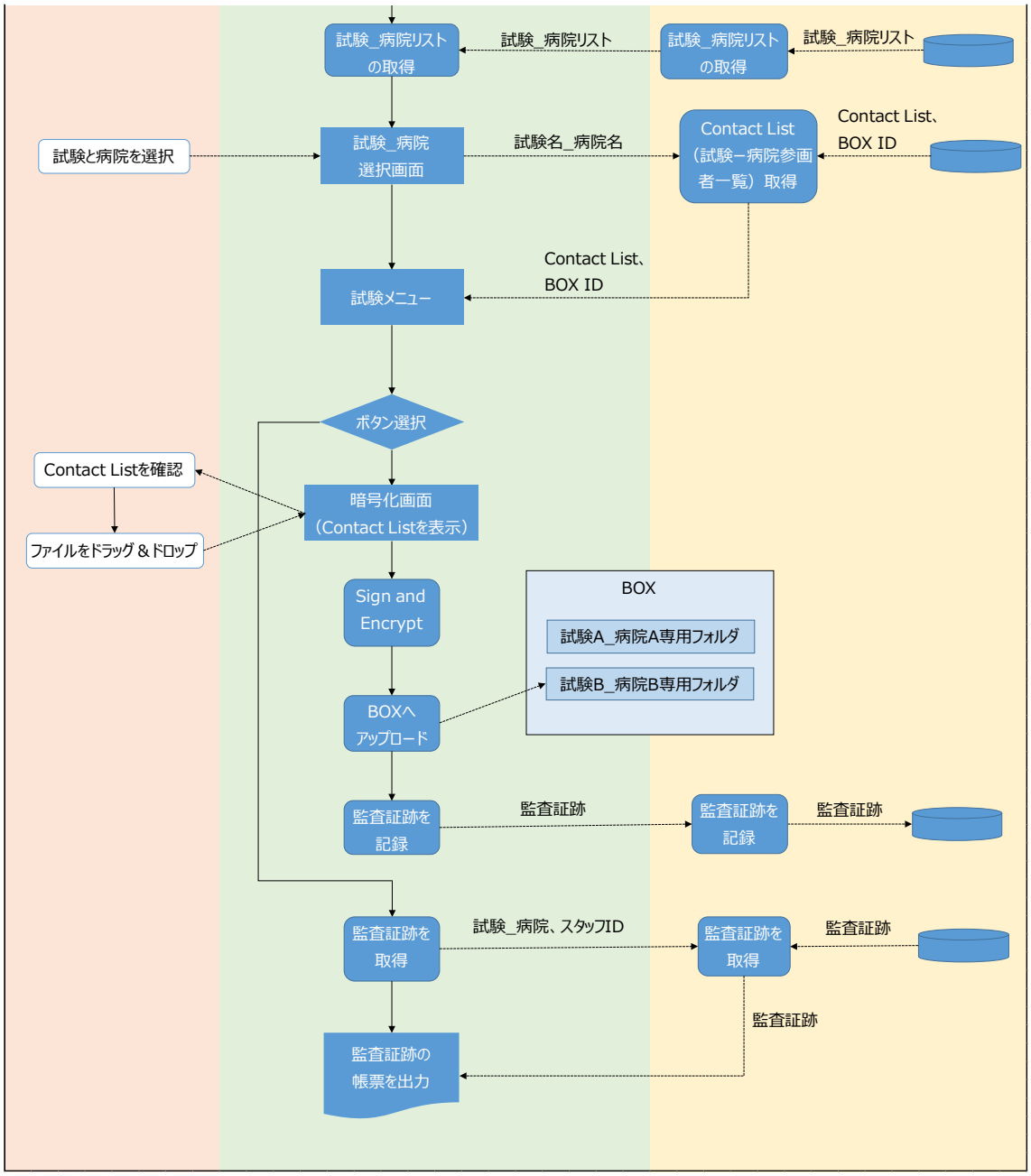


図 3.4.1.2-2 病院スタッフ業務フロー②

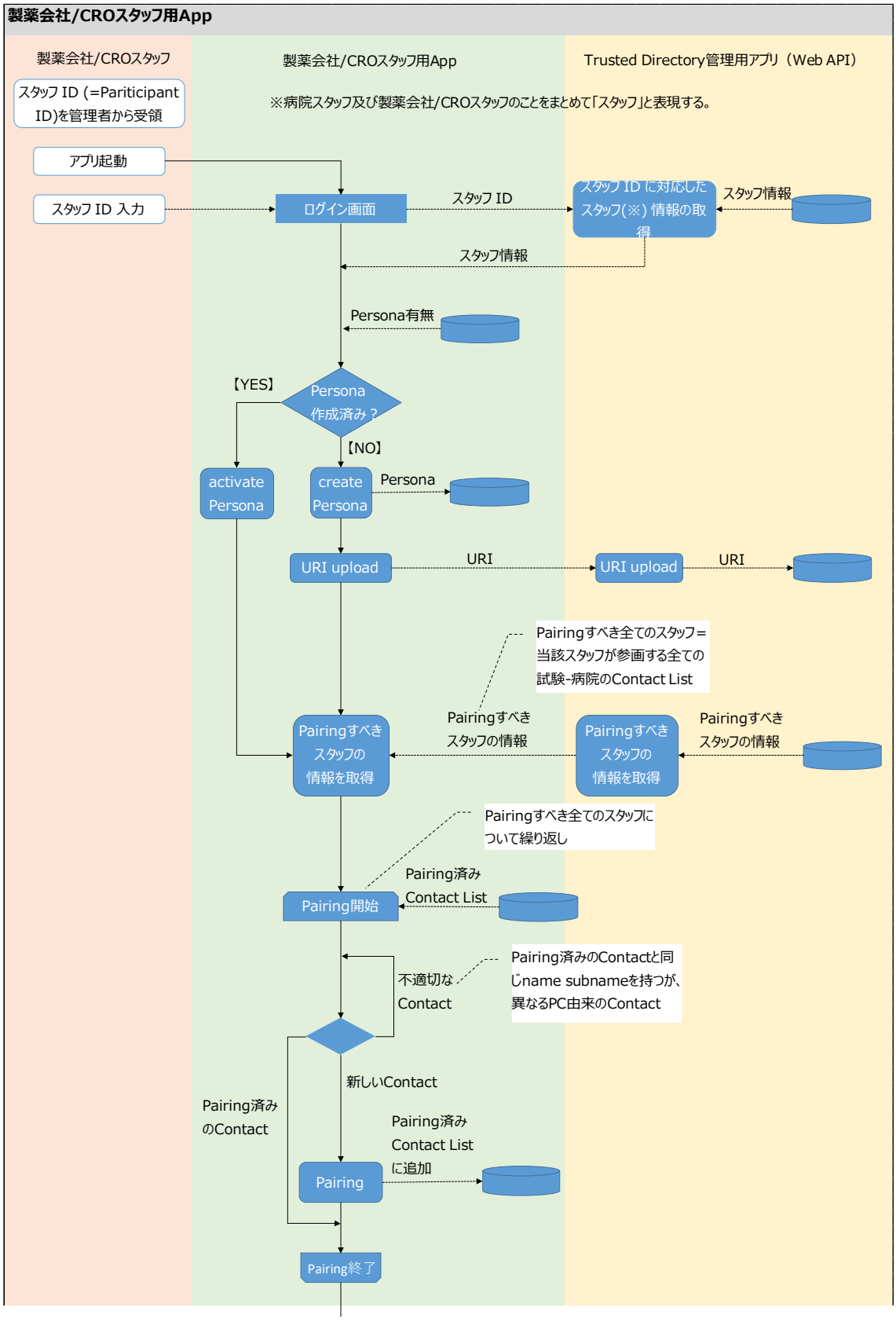


図 3.4.1.3-1 製薬会社/CRO スタッフ業務フロー①

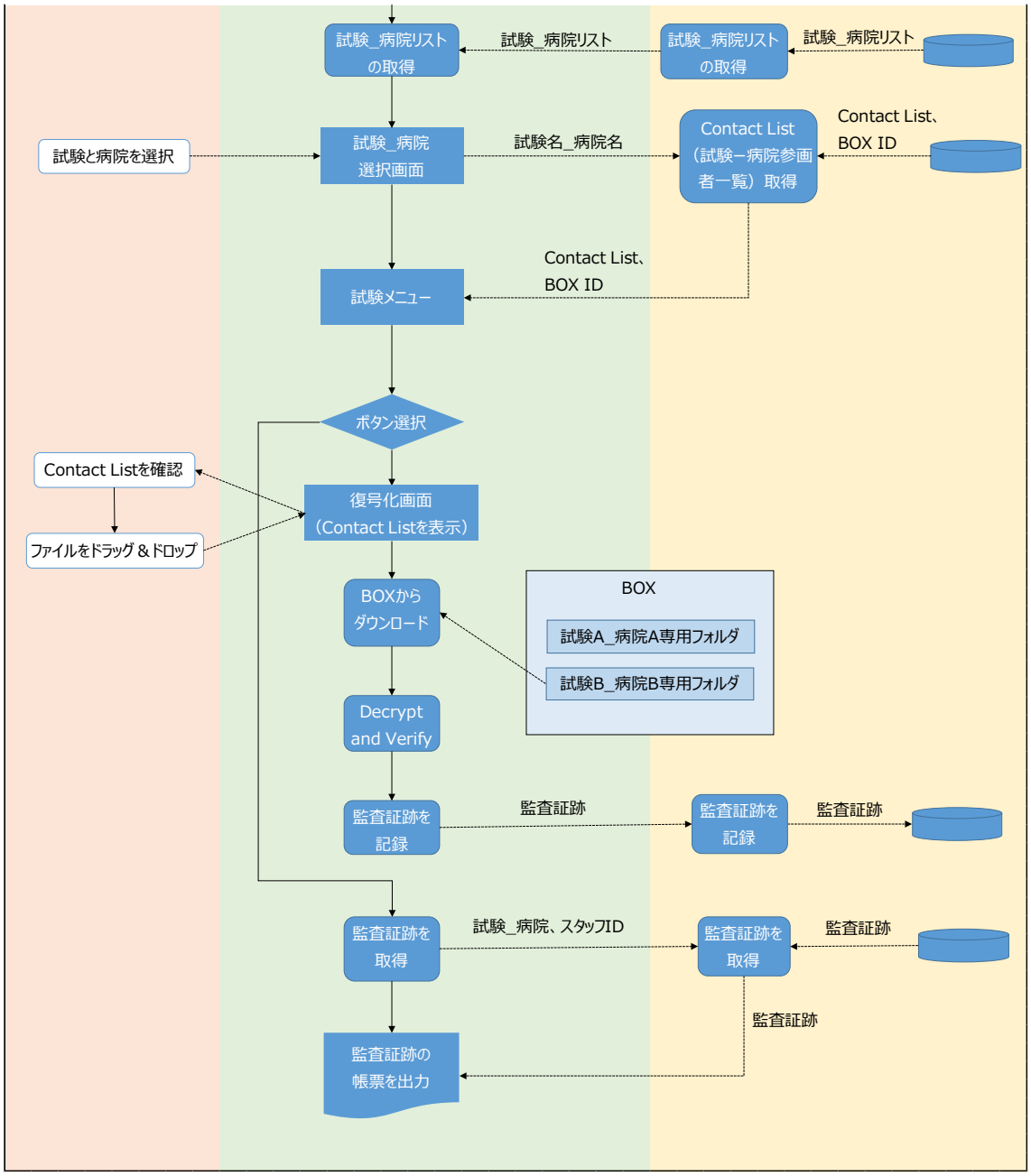


図 3.4.1.3-2 製薬会社/CRO スタッフ業務フロー②

3.4.2 ユースケース図

2.1-1 事業スキーム図を再掲する。臨床試験における「病院スタッフ」と「製薬会社/CRO（Contract Research Organization）スタッフ」間、実臨床現場における異なる 2 つの病院（A 及び B）のスタッフ間における情報共有を想定したユースケースである。

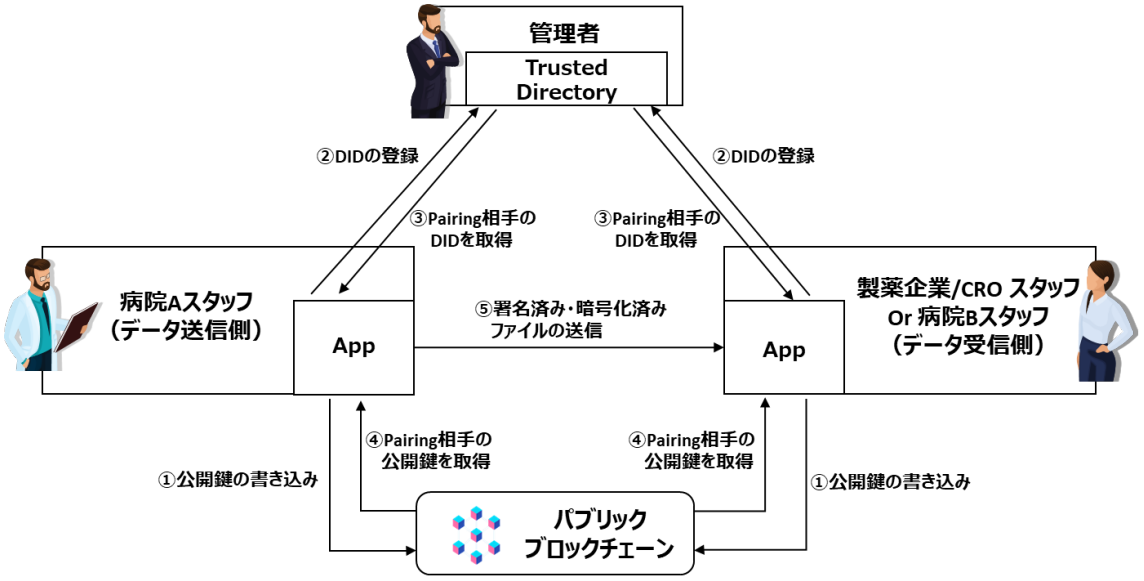


図 3.4.2.1 ユースケース図（再掲）

【主体】

- 管理者
  - 本システムを利用する病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフを管理する。
  - ファイルの送受信ができるスタッフ同士の組み合わせを管理する。ファイルの送受信を行えるスタッフ同士の組み合わせ情報のことを「Contact List」と呼ぶ。つまり、管理者は Contact List を管理する。
- 病院 A スタッフ（データ送信側）
  - 自分の PC でデータ受信側に送信したい臨床試験データや診療データ等を含むファイルを作成する。（ファイルの形式は問わない。例えば Microsoft word や Excel など）
  - 作成したファイルを、App を用いてデータ受信側のみが検証・復号化できる形で署名・暗号化し、データ受信側へ送信する。（復号化及び署名の検証を行える相手は Contact List で管理される。）
- 製薬企業/CRO スタッフ or 病院 B スタッフ（データ受信側）
  - データ送信側から受領した暗号化ファイルを復号化・署名の検証を行う。
  - 復号化したファイルを閲覧する。

【構成】

- Trusted Directory

- Web アプリケーションで管理されるデータベースを指す。
- 以下の 2 点を格納する。
  ① 本システムを利用する病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフ情報と、Contact List
  ② 監査証跡（ファイルの暗号化及び復号化の履歴）
- 管理者は Web アプリケーションで上記の①を管理する。

・ App
- 病院 A スタッフ及び製薬会社/CRO スタッフまたは病院 B スタッフが自分の PC にインストールして使用する Windows アプリケーションを指す。
- デバイスに紐づく DID を生成し保持する。
- 任意のファイルをデータ受信側のみが検証・復号化できる形で署名・暗号化し、データ受信側へ送信する。
- 受信した暗号化ファイルを復号化及び署名の検証を行う。

・ パブリックブロックチェーン
- DID の管理基盤として利用する。
- App は生成した DID の公開鍵をパブリックブロックチェーンに書き込む。
- App はパブリックブロックチェーンからデータの送受信を行う相手（Contact List）の DID の公開鍵を取得する。

なお、CMIC（株）が受託した臨床試験または臨床研究においては CMIC（株）が管理者となる。CMIC（株）が受託していない臨床試験または臨床研究で CMIC（株）が本システムのみを提供する場合においては、その臨床試験または臨床研究にて管理者を指名する形になる場合がある。

3.4.3 操作画面（UI）

操作画面については成果報告書概要版にて記載する。

3.4.4 機能一覧/非機能一覧

表 3.4.4.1 機能一覧

サブシステム	機能分類	機能	概要
TD 管理用 App: 管理者用 Web App	管理者の管理	ログイン	管理者が ID とパスワードでログイン
		管理者アカウントの編集	管理者アカウントの編集（ID, Password の変更）
		管理者アカウントの追加	管理者アカウントの追加

サブシステム	機能分類	機能	概要
		管理者アカウントの削除	管理者アカウントの削除
	システム利用スタッフ管理	システム利用スタッフ追加	システム利用スタッフの情報を入力し新規追加。ID を自動発行。
		システム利用スタッフ編集	システム利用スタッフの情報を編集
		システム利用スタッフ無効化	登録済みのシステム利用スタッフを削除
		システム利用スタッフ削除	登録済みのシステム利用スタッフの情報を無効化
	試験管理	試験追加	試験情報を入力し、本システムを利用する試験を追加
		試験編集	登録済みの試験情報を編集
		試験無効化	登録済みの試験情報を無効化
		試験削除	登録済みの試験情報を削除
	病院管理	病院追加	病院情報を入力し、本システムを利用する病院を追加
		病院編集	登録済みの病院情報を編集
		病院無効化	登録済みの病院情報を無効化
		病院削除	登録済みの病院情報を削除
	試験-病院紐づけ管理	試験-病院追加	試験-病院紐づけ情報を入力し、新規追加
		試験-病院編集	登録済みの試験-病院情報を編集
		試験-病院無効化	登録済みの試験-病院情報を無効化
		試験-病院削除	登録済みの試験-病院情報を削除
	試験-病院-システム利用スタッフの紐づけ管理	試験-病院-システム利用スタッフ追加	試験-病院に参画する（紐づく）システム利用スタッフ情報を入力し、新規追加
		試験-病院-システム利用スタッフ編集	登録済みの試験-病院に紐づくシステム利用スタッフ情報を編集
		試験-病院-システム利用スタッフ無効化	登録済みの試験-病院に紐づくシステム利用スタッフ情報を無効化
		試験-病院-システム利用スタッフ削除	登録済みの試験-病院に紐づくシステム利用スタッフ情報を削除
TD 管理用 App:Web API	TD とシステム利用スタッフ用 App の接続	システム利用スタッフ情報の送信	システム利用スタッフ用 App から当該スタッフの ID を受け取り、対応するシステム利用スタッフ情報を返却する
		URI を TD に保存	システム利用スタッフ用 App から DID を受け取り TD に保存する

サブシステム	機能分類	機能	概要
		試験-病院リストを送信	システム利用スタッフの参画している試験-病院リストをシステム利用スタッフ用 App に送信する
		Contact List を送信	Contact List をシステム利用スタッフ用 App に送信する
		監査証跡を記録	システム利用スタッフ用 App にて行われた暗号化/復号化の情報を TD に保存
		監査証跡を送信	監査証跡をシステム利用スタッフ用 App に送信
病院スタッフ用 App	ログイン	ログイン	ID を入力し、Web API 経由で TD からシステム利用スタッフ情報を取得
	DID の管理	DID 作成	DID を作成しデバイス内に保存。DID をブロックチェーンに書き込み URI を Web API 経由で TD に保存
		Activate DID	ログイン時点で DID が作成済みの時、既存の DID を起動
		Pairing	Pairing すべき全ての DID の情報（自分が参画する全ての試験-病院の Contact List）を Web API 経由で取得し、Pairing を行う。
	試験-病院リストの取得、選択	試験-病院リストの取得	Web API 経由で自分が参画する全ての試験-病院リストを取得
		試験-病院リストの選択	試験-病院リストから試験ー病院を一つ選択する
	試験メニュー	試験-病院のメニュー画面表示	選択した試験-病院のメニュー画面を表示。暗号化、復号化、監査証跡出力画面に遷移するボタンを表示
	暗号化	Contact List 表示	選択した試験-病院の Contact List を表示
		暗号化ファイルの登録	ドラッグアンドドロップで暗号化対象のファイルを登録
		暗号化実施	Contact List に記載されたシステム利用スタッフのみが署名の検証、復号化ができる形で暗号化
		BOX アップロード	暗号化済みファイルを試験-病院専用の BOX フォルダにアップロード
		監査証跡の記録	暗号化した履歴を Web API を介して TD に記録
	復号化	Contact List 表示	選択した試験-病院の Contact List を表示
		暗号化済みファイルの選択	試験-病院専用の BOX フォルダに保存された全てのファイルのリストを表示し、復号化するファイルを選択。
		復号化	選択したファイルをダウンロード後、署名の検証・復号化を行う。
		監査証跡の記録	

サブシステム	機能分類	機能	概要
	監査証跡取得	監査証跡取得	選択した試験-病院の全ての暗号化/復号化履歴を取得
製薬会社/CRO スタッフ用 App	-	-	病院スタッフ用 App の機能から暗号化の機能を除いたすべての機能を有する

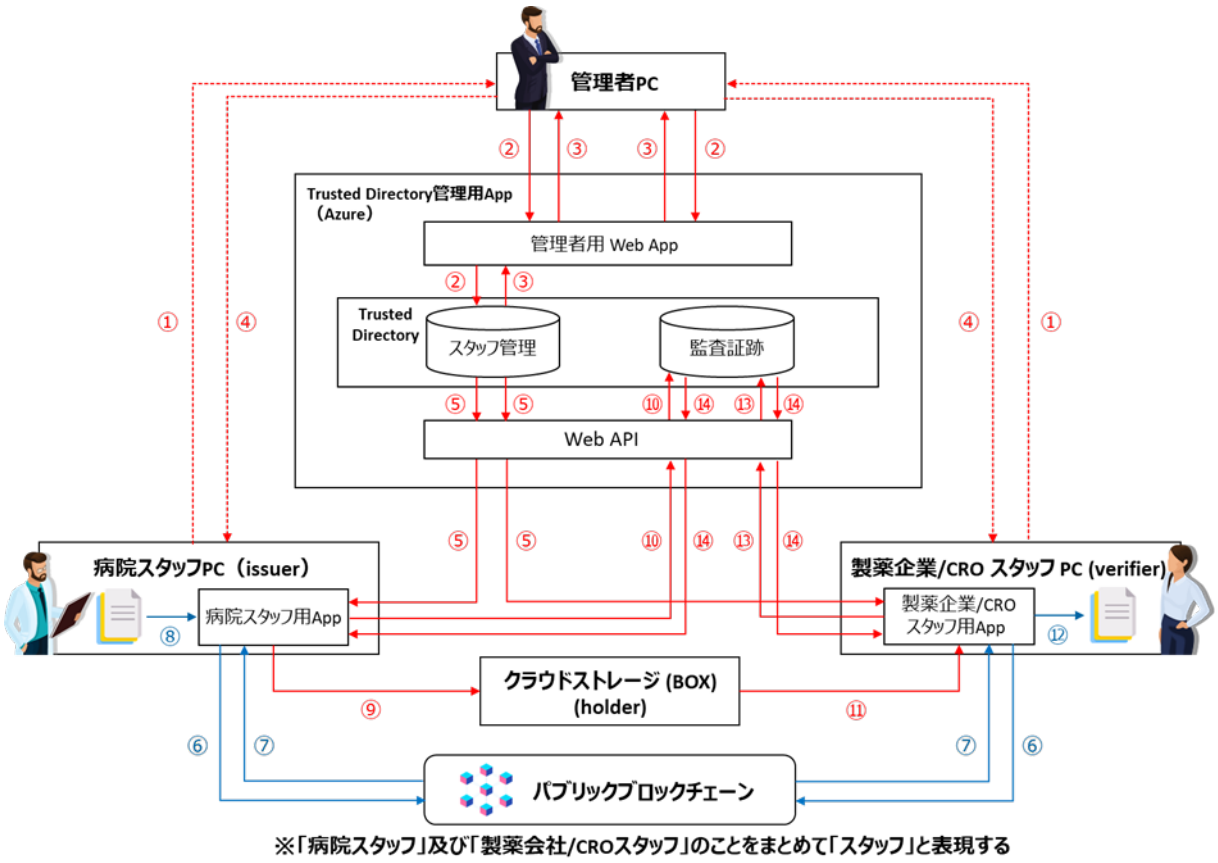
表 3.4.4.2 非機能一覧

機能名	機能概要
運用性	常時サービス提供が前提であり、24 時間 365 日の運用を行う。

3.4.5 データモデル定義(VC データモデルを採用する場合)

VC を採用していないため該当なし。

3.4.6 実験環境



① 利用申請、スタッフ情報の提供	⑧ 任意のファイルを暗号化
② スタッフ情報を TD に登録	⑨ 暗号化ファイルをクラウドストレージへ格納
③ スタッフ ID の発行	⑩ 暗号化履歴を TD に書き込み
④ スタッフ ID を用いてログイン	⑪ クラウドストレージから暗号化ファイルを取得
⑤ スタッフ情報と Contact List を TD から取得	⑫ ファイルを復号化し閲覧
⑥ スタッフ情報を用いて DID を作成し、 DID をブロックチェーンへ書き込み	⑬ 復号化履歴を TD に書き込み
⑦ Contact の公開鍵を取得し Pairing	⑭ 監査証跡を TD から取得して閲覧

図 3.4.6.1 実験環境（再掲）

3.4.7 システムの構成要素

表 3.4.7.1 主要な製品・ライブラリ一覧

コンポーネント名称	型式 （製品の場合）	OSS か否か	ライセンス
TD 管理用 App（新規開発）	－	CMIC（株）が権利を保有中	－
Django（既存）	－	OSS	新 BSD
PostgreSQL（既存）	－	OSS	PostgreSQL License
Microsoft Azure（既存）	－	OSS ではない	－
病院ユーザ App・製薬会社/CRO ユーザ App(新規開発)	－	CMIC（株）が権利を保有中	－
Keychain Core SDK（既存） （パブリックブロックチェーンとの接続部分を含む）	－	OSS ではない	CMIC（株）が購入しているライセンス
.NET Framework（既存）	－	OSS	MIT
Microsoft Visual Studio 2016（または 2019） （コンポーネントではないが、再現するために必須の IDE であるため記載） （既存）	－	OSS	CMIC（株）が購入しているライセンス
BouncyCastle（既存）	－	OSS	MIT

	BOX.V2（既存）	−	OSS	Apache-2.0
	CsvHelper（既存）	−	OSS	MS-PL or Apache-2.0
	Newtonsoft.Json（既存）	−	OSS	MIT
クラウドストレージ（BOX）（既存）		−	OSS でない	CMIC（株）が購入しているライセンス

3.5 実証を通じて得られた主な成果

3.5.1 システムの企画・開発に関する実証内容・得られた主な成果

フィールドテストは問題なく完了し、期待したシステムの挙動が確認できた。具体的には以下の通り。

- データの非改竄性
- ユーザのなりすまし防止
- 提供範囲外へのデータの非開示

特にユーザの「なりすまし防止」に関して、臨床試験等においては一定数 ID/Password の流用によるなりすまし及びデータ改竄が発生していることに加えて、それらの事象が発生したことが追跡不可能という現状がある。この点に対して、今回のプロトタイプシステムにおいては DID がデバイスに紐づいて生成・管理されるため、根本的に ID/Password の流用による諸問題も防止できる可能性が示唆された。この点、ヒアリング対象者である相生会担当者からも好評価を得た。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

- 相生会担当者からのコメントとして、医療機関やアカデミア主導で実施する臨床研究や疫学調査など、低コストでの計画及び実施が要求されるため現状ではデータインテグリティを担保できていない試験に対して導入したいとのこと。
- 実施に対して多額のコストが掛かっている試験及び研究に対して、既存のプロセス自体に大きな変更を加えずにプロセス内での業務内容の簡素化を実現することで、Low cost model での実施可能性が示唆された。
- 今回のプロトタイプシステムのアーキテクチャ及び得られる効果は、今後のあるべき姿の一事例であるとも感じる。一方で、医療現場及び臨床試験業界における現時点で要求されているデータインテグリティの考え方と比較するとオーバースペックであるとも感じる。今回のプロトタイプシステムではデバイスに紐づく DID の実装により、なりすまし及びそれに付随したデータ改竄がより発生しにくい仕組みを実現し、この点において既存のシステムよりも高いデータの真正性及びセキュリティを担保することを実現した。一方で、既存のシステムでは ID・パスワードを利用したアクセスコントロールが前提となっており、利用者の視点では当該運用が内包するリスクに対する危機意識が十分とはいえず、システムの視点ではID・パスワードの流用等によるなりすましの防止までは要求されていない。そのため、今回のプロトタイプシステムのコンセプト及び効果について医療現場の理解を得ることは容易ではなく、

当該システムのアーキテクチャ更には Trusted Web ホワイトペーパーで要求される技術要件について社会全体に浸透させていくような活動も必要だと感じる。

3.6 本実証で開発したシステムの第三者による再現可能性（A 類型のみ）

本実証事業で開発したシステムは Keychain 社製の Keychain Core SDK、BOX を組み込んで実装しており、同製品のライセンスを利用することで第三者による再現が可能になる。また、C#で開発したクライアントアプリについては IDE として Visual Studio（2015 または 2019 など）を用いた。

4　実証終了後の社会実装に向けた見通し

4.1　社会実装時に想定しているビジネスモデル・ユーザのメリット

想定しているビジネスモデルでは、CMIC（株）がサービス提供者となり、臨床試験及び臨床研究等の実施団体・実施者より 1 つの試験・研究毎にサービス利用料を徴収することでマネタイズを図り、当該試験・研究における実施団体・実施者側の担当スタッフ（CRO 含む）及び病院側のスタッフがエンドユーザとなる。各ステークホルダーが享受するベネフィット及び想定利用料は表 3.1.1 の通りである。本ビジネスモデル自体は既存の臨床試験及び臨床研究等で使用されるシステムと相違はない。サービス提供に要する CMIC（株）側のコストは年間約 2,500 万円を想定している。単純な比較は困難であるものの、一例として既存の EDC のサービス利用料（セットアップ及び運用・管理）と比較すると、10 分の 1 から 5 分の 1 となることが期待できる。また、将来的には DCT デザインの臨床試験において Wearable Device や ePRO 等への実装を想定しており、その場合には CMIC（株）が当該システムと連携しているデバイスリストを作成・公開し、臨床試験及び臨床研究等の実施団体・実施者が利用したいデバイス等を選択して利用する形を想定している。その場合、臨床試験及び臨床研究等全体のコスト削減が図れると共に、本システムの利用料についてもデバイス毎且つ被験者数に依存する従量課金制で請求することを想定している。

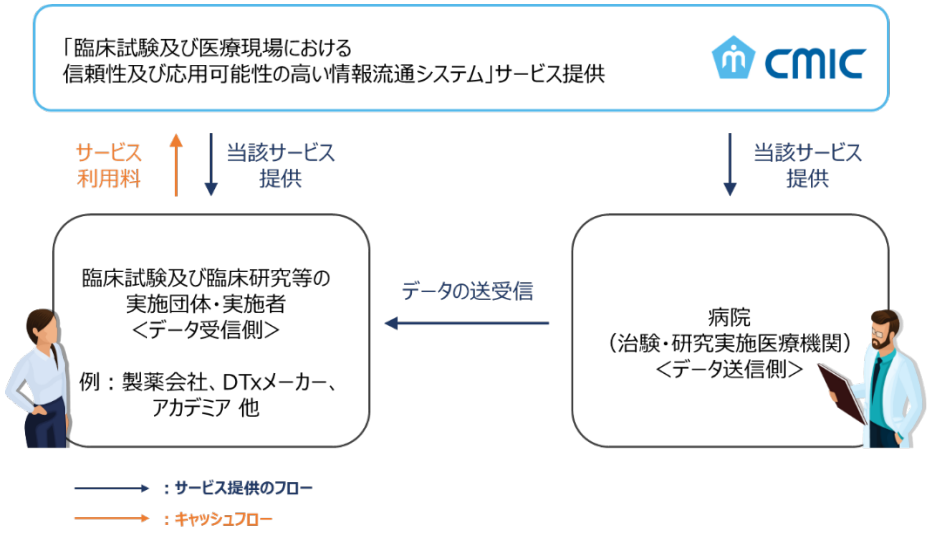


図 4.1.1 ビジネスモデル

表 4.1.1　各ステークホルダーの主なベネフィット及び想定している利用料

ステークホルダー	主なベネフィット	負担するコスト
臨床試験及び 臨床研究等の	・　なりすまし、データ改竄が困難な環境構築による Clinical data	月額 10～15 万円/1 試験

ステークホルダー	主なベネフィット	負担するコスト
実施団体・実施者	及び Operational data 双方の信頼性の向上 ・ 既存システムと比較した場合でのコスト削減効果	（Wearable Device や ePRO に実装した場合には、被験者数に依存した従量課金制を想定）
病院（治験・研究実施医療機関）	・ なりすまし、データ改竄が困難な環境構築による試験・研究実施医療機関としての信頼性の向上 ・ システム毎の煩雑な ID/パスワード管理からの解放による、スタッフの心理的負担の軽減 ・ 各種文書を電子ファイルの形でデータの真正性、セキュリティ及び追跡可能性（Contact List、監査証跡）を担保した上で遠隔て提供可能となることによる、製薬企業/CRO スタッフによるオンサイトでのモニタリングに対する対応工数の削減	NA （製薬企業等の臨床試験及び臨床研究等の実施団体・実施者から委託され試験・研究を実施する立場であるため、システムのサービス利用料も当該実施団体・実施者が負担の上で CMIC（株）よりシステム提供を受ける）

4.2　実証を通じて判明したユースケースの課題とその解決方針

- 課題①

  本実証内では試験-施設専用の BOX フォルダの作成は管理者がブラウザで BOX のアプリケーションにアクセスし、フォルダ名等を手入力して対応している。試験数と病院数はそれぞれ 10～数十以上となることが見込まれるが、管理者が全て手入力でフォルダを作成することは現実的ではない。実証後に自動でフォルダを作成できるよう開発を進める。

- 課題②

  期間に関するアクセスコントロールについて、本実証内では暗号化したファイルを復号化することができる期間は設定していない。実証後その期間設定の要否も含めて検討を行う。

- 課題③

  病院スタッフ App または製薬会社/CRO スタッフ App の UI について、復号化画面では各病院スタッフまたは製薬会社/CRO スタッフの参画している試験-病院の BOX に格納されているすべての暗号化ファイル名を確認できる。しかし、各暗号化ファイルを病院スタッフまたは製薬会社/CRO スタッフが復号化できるか否かは復号化するボタンを押下しエラー文が出るまでわからない。例えば、ある

試験-病院に途中から参画した病院スタッフまたは製薬会社/CRO スタッフは、自分が Pairing する前に暗号化されたファイルを復号化することはできないが、現状の UI ではどのファイルが自分が復号化でき、どのファイルが復号化できないのかを確認することができない。実証後、各暗号化ファイルを復号化をできる病院スタッフまたは製薬会社/CRO スタッフを確認できるような UI に変更予定。

- 課題④

  BOX のフォルダ構成について、本実証では施設-病院用のフォルダ直下に当該施設-病院で作成された全ての暗号化ファイルを格納する。一つのフォルダに臨床試験データのファイルや各種ログのファイルなど様々なファイルを保存する形となるため病院スタッフまたは製薬会社/CRO スタッフは復号化するべきファイルを探したり格納すべき暗号化ファイルが格納されていることを確認したりしにくい UI/UX となっている。実証後に UI/UX を検討する。

- 課題⑤

  相生会で実施したフィールドテスト等にて、「今回のプロトタイプシステムのアーキテクチャ及び得られる効果は今後のあるべき姿の一事例であるとも感じる。一方で、医療現場及び臨床試験業界における現時点で要求されているデータインテグリティの考え方と比較するとオーバースペックであるとも感じるため、今回のプロトタイプシステムのアーキテクチャ更には Trusted Web ホワイトペーパーで要求される技術要件について社会全体に浸透させていくような活動も必要だと感じる。」とのコメントを得ている。本件に関して、2023 年 6 月以降に相生会内で実施される臨床研究で更なる POC（実装及び効果検証）を行い、得られた成果を学会などで相生会と共同で対外発表することを検討中である。

4.3　本ユースケースの社会実装に向けたマイルストーン

今年度の実証で明らかになった課題を、令和 5 年度前半に解消し、令和 5 年度後半には臨床試験分野（主に臨床研究）におけるサービス提供を目指す。また、同時に Wearable Device データの情報共有・活用に向けた企画・開発に着手する。病院間における社会実装に関しては、同法人内もしくは地域包括ケアシステムを念頭に特定のエリアにおける複数病院への導入を想定している。

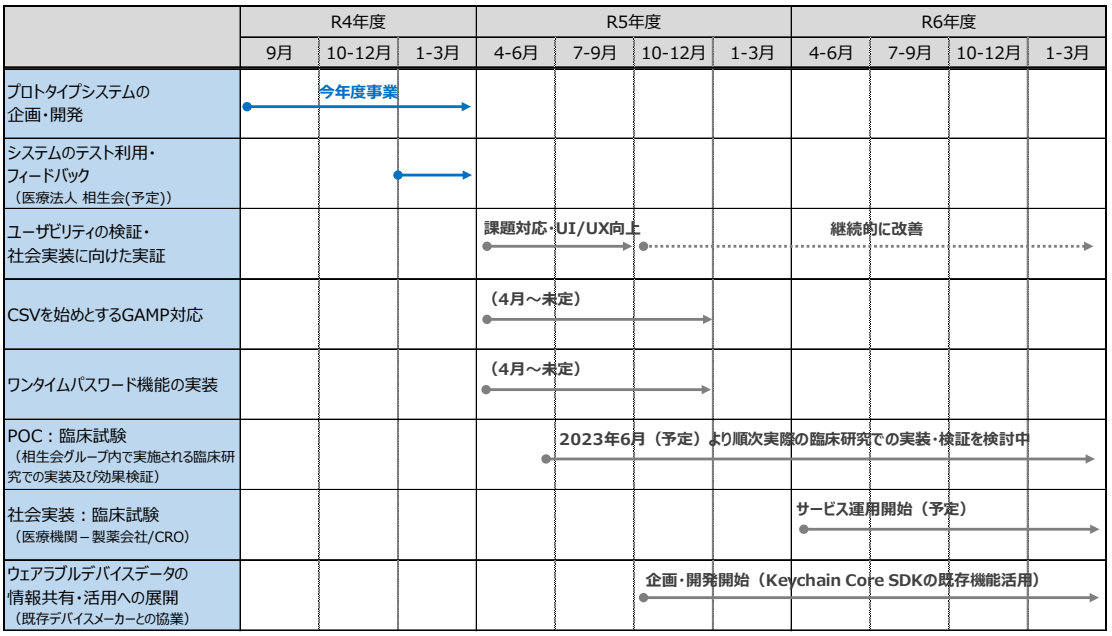


図 4.3.1　社会実装に向けたマイルストーン

5　Trusted Web に関する考察

5.1　Trusted Web のアーキテクチャに関する課題と提言

・　私たちとしては、今回のユースケース事業にて開発したプロトタイプシステムは臨床試験や臨床研究等での使用に限定しておらず、アーキテクチャ自体は患者・生活者が分散型で取得した自らのヘルスケアデータ、例えば PHR などを信頼できる人に・信頼できる仕組みで共有可能な Trusted Health Care Data Network の実現を見据えている。つまりは、患者・生活者が自己主権的に自らのヘルスケアデータを管理し、適切な同意制御の下で信頼できる相手にのみ同意の範囲でデータを共有するという世界観である。Trusted Web のアーキテクチャの意義という観点においては上記の世界観更には DCT デザインの臨床試験を実現するにあたっては必要なアーキテクチャであると考えている。

・　現在の TW ホワイトペーパーでは、希望者は誰でも利用可能なシステムの開発を前提としている。一方で、医療現場/臨床試験の領域においては一部の許可されたユーザ同士によって形成される動的なコミュニティが存在し、その中での Trust なデータのやり取りを実現する必要がある。このように動的なコミュニティ内でのデータのやり取りにおける必要な技術及びコンセプトの整備も必要ではないか。

例えば、本ユースケースにて主に取り上げた臨床試験における情報の授受については、臨床試験毎に特定の製薬会社/CRO スタッフと医療機関スタッフの間でのみデータが授受される。企業治験を例にすると治験の開始時に製薬会社/CRO が治験実施医療機関及び治験責任医師を選定する。治験責任医師は治験に関する業務の一部を適切な実施医療機関スタッフに委任する。また治験審査委員会は治験実施計画書と共に院内での実施体制（治験責任医師と業務を委任された治験分担医師・治験協力者など）について審査し承認する。

このように製薬会社/CRO 及び治験審査委員会によって特定された医療機関スタッフが委任された範囲で治験業務を行うことができる。当該医療機関を担当する製薬会社/CRO スタッフは、治験実施中を通して特定された医療機関スタッフのみが治験責任医師に委任された業務の範囲内において治験業務を行っていることを確認する。この治験業務には患者から取得した治験データの収集など情報の取り扱いを含む。また、治験では患者や医療機関における個人情報や医療情報などの機密性の高い情報が取り扱われるため、製薬会社/CRO のスタッフのうち当該医療機関を担当するスタッフのみに情報を開示する。すなわち、治験（その他の臨床試験においても同様）では医療機関、製薬会社/CRO スタッフのうちお互いに事前に特定したスタッフ同士のみで情報の授受がされることが重要であり、試験-病院の組み合わせ毎に情報の授受を行うコミュニティを形成している。2.2. 社会・経済に与える価値・影響の <その他の関連情報> に記載の通り本邦にて年間 1000 を超える臨床試験が実施されている。その試験毎に 1～数十の医療機関が参画するため、試験-病院毎に形成されるコミュニティ数は年間で万単位となる。本ユースケースでは多数のコミュニティの効率的な管理を実現するために Keychain Core の技術と TD を採用した。Keychain Core によりデバイスに紐づく DID の導入とコミュニティ内での信頼できるやりとりを行い、さらに TD によりコミュニティ

参加者の管理を可能とした。この事例が動的で多数なコミュニティ内でのデータのやり取りに真に有用であるか否かも含めて検討頂きたい。その上で、このようなパーミッションドな場合における Trusted Web 実現のモデル、具体的に必要な技術及び規格について示していただきたい。

5.2 その他 Trusted Web の課題と提言

- 本事業を進める中で、TW ホワイトペーパーに存在しない表現や語彙を用いた確認事項が多々あった。（例：ウォレット、Ownership など）当該表現や語彙の定義及び出典が不明な状態で検討してため、今回開発したプロトタイプシステムのアーキテクチャが TW の思想に沿うものとなっているか判然としない部分もある。今回のユースケース事業は各事業者からの TW ホワイトペーパーへの提言を収集することも目的の 1 つであったと認識しているが、今後より広く社会全体に理解を促していくためには用語集の整備や理解を醸成するための啓発活動が必要であると考える。
- TW ホワイトペーパーにおける各種表現や語彙の定義や詳細説明が少なく、初心者にはわかりづらい。仮に、IT ベンダー以外の各産業における企業に対しても周知していくのであれば、可能な限り詳細かつ平易な表現がなされた方が良いものと考える。
- 初心者にとってホワイトペーパーは分かりづらく、特に IT ベンダー以外のユーザ企業にメリットを PR する分かりやすいコンテンツ制作が必要ではないか。また、政府の文書としては、様々なトラストに関する技術のメリットデメリットを中立的に整理すると、ユーザ企業との合意・調整がしやすくなると考える。