令和 3 年度デジタル庁国家プロジェクト

Trusted Web の実現に向けたユースケース実証事業

成果報告書

ワークプレイスの信頼できる電子化文書の流通システム

2023 年 3 月 24 日

代表機関：東芝テック株式会社

コンソーシアム名称：Trusted Workplace Solution by TTEC and CG

Toshiba Tec Corporation

目次

1　背景と目的

ここ数年、新型コロナウイルス感染拡大の影響でテレワークが急速に拡大している。また、働き方改革の推進で時短勤務やフレックスタイム制など、多様な働き方が普及した。企業にとっては、従業員がどこにいても業務に支障が出ないような環境整備が急務となっている。

一方で、真正性を求められる文書を扱う経理部門や特定の業種業務では、未だ紙を基本としたアナログ業務が残っている。「電子帳簿保存法」（1998 年 7 月施行）、「e-文書法」（2005 年 4 月施行）にて、真正性が求められる電子化文書は、国税関連書類、会計帳簿、証憑書類（見積書・納品書・請求書・契約書など）、重要規約、設計図面、診察記録、行政文書など対象は多岐にわたり、特に金融・保険、会計監査、防衛システムの開発と製造に関する請負業者、医療関連企業、行政機関においては、真正性が求められる文書管理業務が発生しやすく、ワークプレイスをデジタル化する際のボトルネックになっている。

デジタル庁が創設され、ペーパーレスを含め行政の DX が推進されており、将来的には多くの文書が電子的になっていく方向になっており、実際電子文書を保存する文書管理システムは多数存在しているものの、真正性が求められる紙文書を信頼できるスキャナデバイスで電子化したうえで、簡単にその真正性を検証でき電子化文書を流通させるシステムがないことが原因の一つとして考えられる。

この課題を従来のウェブの仕組みで解決する場合、スキャン機能を搭載したデジタル複合機（以下 MFP）を利用して電子化した後、人の手で文書管理システムを利用する事が一般的であるが、電子化文書を MFP から直接文書管理システムに保存しようとすると、MFP の機器メーカーは、数十万台におよぶ MFP のプロビジョニング [1]、デバイスの識別子や暗号鍵の管理、特定システムへの依存度の高さ、トランスポートごとのセキュリティ対応などのデジタルインフラ構築の課題に直面する。

本実証では、Trusted Web のアーキテクチャー上に、MFP と検証可能な電子化文書の流通システムを構築することで、真正性を求められる紙文書を扱うワークプレイスのデジタル化を推進し、導入企業の効率的な業務運営と省力化を促進する。

2　事業の概要

2.1　事業概要及び実証の範囲

本実証では、分散型 ID 技術である CollaboGate Japan 株式会社の End-to-End（以下 E2E）セキュリティソリューションを活用し、MFP でスキャンする電子化文書の真正性を担保、簡単に改ざん検証可能なシステム構築を目指す。東芝テック株式会社の MFP でスキャンするデータを検証可能な電子文書として文書管理システムに保管する。本システムにより、監査証跡の必要な文書業務のデジタル化を推進し、導入企業の効率的な業務運営と省力化を促進するとともに、電子化文書の流通に貢献する。

[1] ネットワーク環境に合わせてセットアップすること

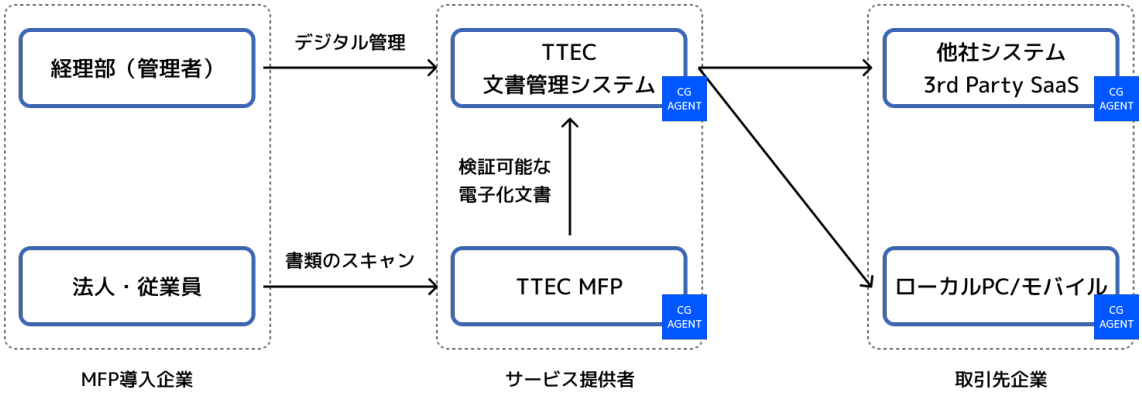


図 2.1-1 事業スキーム図

2.2 社会・経済に与える価値・影響

- 市場環境

2021 年国内メーカーの MFP における世界市場規模は 6,490 億円（前年比 99.1%）、年間出荷台数は 359 万台である [2]。

ペーパーレス化に伴い緩やかな市場縮小傾向にあるなか、主要国内メーカーは業務ワークフロー効率化を支援するトータル・ソリューションへと競争軸をシフトしている。本実証では、真正性を求められる紙文書の電子化と業務ワークフローの効率化を実現し、デジタル化の遅れる市場セグメントでのシェア獲得と月額料金の顧客単価向上を実現する。

- 市場規模（独自試算）

文書管理に特に高い真正性が求められる金融・保険、会計監査、防衛システムの開発と製造に関する請負業者、行政機関の 4 つのセグメントの合計を 2 千億円と推定。

- 日米で約 53,000 社が防衛省と直接取引、各社平均 2 事業所、平均 20 台の MFP 設置を仮定し、53 万台の導入余地
- 国内 90,000 の金融・保険業の事業所、平均 20 台の MFP 設置を仮定し、45 万台の導入余地
- 国内 26,000 の会計事務所、平均 20 台の MFP 設置を仮定し、13 万台の導入余地
- 国や地方公共団体の行政機関として、各省庁、都道府県庁・市区町村役場の数は約 2000 以

2 [1] JBMIA 集計: https://www.jbmia.or.jp/statistical_data/list.php?t=CMShipped

上あり、平均 20 台の MFP 設置を仮定し、10 万台の導入余地

4 つのセグメントで 120 万台の導入余地が存在。MFP の利用料に本システム利用料を加味することで、2400 億円程度の市場規模が見込まれる。

- サービス提供者が負担するコスト（独自試算）

また、サービス提供者として、プロビジョニング、インフラ構築、保守員用で下記のコストが発生しており、これらの削減が見込まれ、サービス提供者の収益改善やユーザ利用料の低減が期待される。

- プロビジョニングコスト：1 台当たり約 1,000 円のプロビジョニングコストがかかると仮定すると、10 万台を想定すると 1 億円のコストが発生
- インフラ構築コスト： Edge、ネットワーク、クラウドのインフラ構築を行う場合、300 人月の人件費かかると仮定すると、3 億円のコストが発生
- 保守運用コスト：インフラ保守費用、クラウド費、デバイス毎の人件費、その他のライセンス費として、月額 1000 万円のコストが発生

尚、本実証の取り組みは、ビジネス文書を扱う MFP だけでなく、決済情報を扱う POS システム、人流データを扱うネットワークカメラ、バイタルデータを扱う医療機器などのさまざまな IoT 機器に応用することができる。今後、サイバーとフィジカルとの融合が様々な分野で進展していく中で、デジタル社会を支える信頼できるデータ流通基盤の構築に大きく貢献することが考えられる。

2.3 コンソーシアムの体制

本コンソーシアムは、東芝テック株式会社（以下 TTEC 社）を代表機関として、CollaboGate Japan 株式会社（以下 CG 社）により構成される。TTEC 社は、プロジェクト全体の統括及びプロジェクトの推進運営管理、並びに、MFP の開発の役割を担う。 CG 社は、分散型 ID 技術を活用した E2E セキュリティソリューションを用いて、通信やデータの検証、監査証跡部分の実現を担当する。

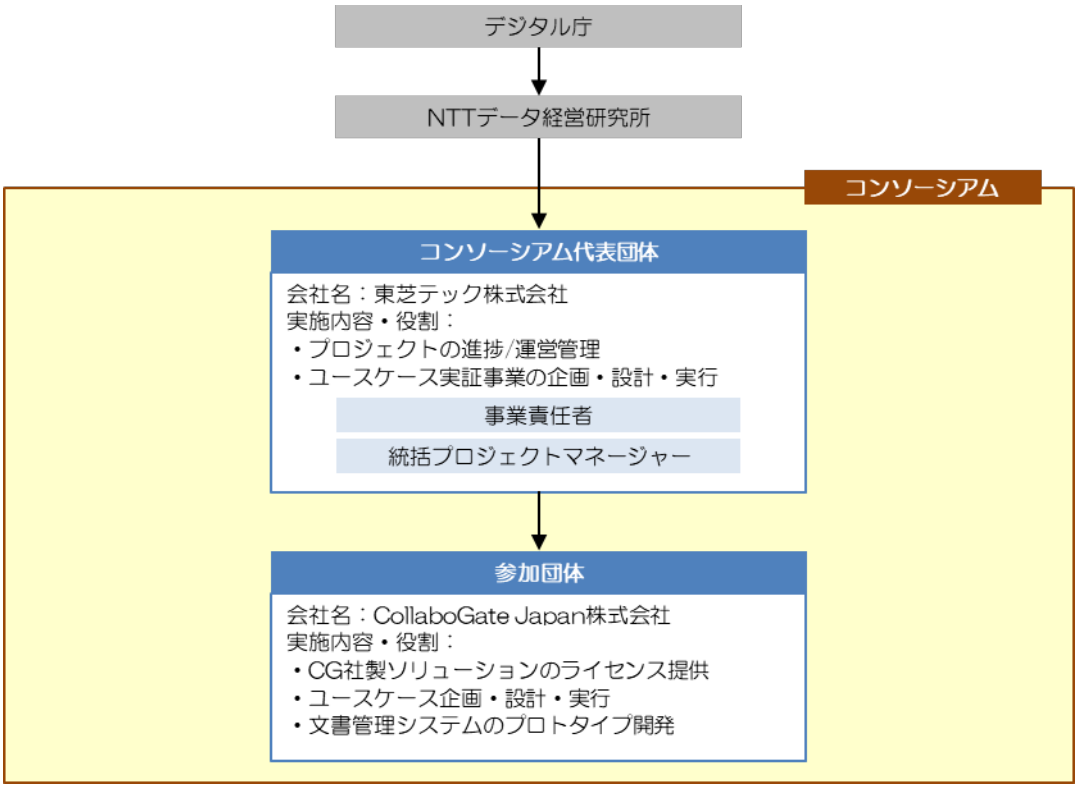


図 2.3-1 実施体制図

2.4 実証全体のスケジュール

以下の表 2.4-1 に本実証における全体スケジュールを示す。

実施事項				R4				R5		
大項目	小項目	担当	時期	9月	10月	11月	12月	1月	2月	3月
要件定義・基本設計										
	要件定義	TTEC	9/9-11/21							
	基本設計	TTEC,CG	10/19-11/30							
MFPへのCG EDGE組み込み										
	開発ボード送付	TTEC	10/26							
	カスタマイズ	TTEC,CG	10/31-12/13							
	組み込み	TTEC	12/13-1/13							
文書管理システム開発										
	プログラミング	CG	10/31-12/14							
	単体試験	CG	12/15-1/13							
スキャンアプリ開発										
	プログラミング	TTEC	10/31-12/21							
	単体試験	TTEC	12/21-1/13							
	結合試験	TTEC,CG	1/16-2/9							
デモ動画の制作										
	シナリオの作成	TTEC,CG	1/16-2/9							
	動画撮影	TTEC,CG	2/13-3/9							
報告書の作成・納品物準備										
	中間報告書作成	TTEC,CG	11/10-12/7							
	最終報告書作成	TTEC,CG	1/16-3/24							

図 2.4-1 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

3.1.1 プロトタイプの企画・開発

（１）要件定義

- TTEC 社と CG 社との打ち合わせを実施し、ワークプレイスにおける信頼できる電子化文書の流通システムに必要となる機能及び非機能（性能や可用性など）に関する制約事項について抽出した。論点となったのは、以下の 6 点。
  - A. デバイスのルートオブトラスト確立（暗号鍵管理）
  - B. プロビジョニングの自動化
  - C. IoT 向けの軽量メッセージングプロトコル
  - D. デバイスの高度な認証・認可
  - E. 検証可能なデータ流通
  - F. 他 IoT 機器への拡張性

- A.「デバイスのルートオブトラスト確立」について
  各種 CPU や OS がサポートするデバイスのルートオブトラストを確立するモジュール（例えば Arm TrustZone や TPM チップなど）を利用する。本実証では、CG 社の EDGE の RoT Extension 機能と、TTEC 社の MFP デバイスに搭載される TPM2.0 機能を活用し、CPU が生成する真正乱数から複数の暗号鍵ペアを生成し、秘密鍵を TPM2.0 で安全に保管する。
  CG 社 EDGE と TTEC 社 MFP TPM2.0 との統合が完了し、要件を達成できた。
- B.「プロビジョニングの自動化」について
  認証局から公開鍵証明書を取り寄せこれを各デバイスにインジェクションする方法と、分散台帳技術などで担保される DID Registry に識別子と公開鍵情報を登録する選択肢がある。大量デバイスを扱う IoT システムの場合、プロビジョニングを自動化することで効率化を図れる後者のアプローチがセキュリティとコストの観点において優れている。本実証では CG 社 EDGE の DID Method を活用し、Bitcoin 上に構築する Sidetree Node を経由して、DID Operation を実現する。これにより、従来手法と比べて大幅なコスト削減およびプロセスの脆弱性の排除を実現できる。具体的に、従来手法では、作業者がデバイスの外で鍵ペア・CSR を生成、認証局に CSR を送信、デバイスの公開鍵証明書を発行・取得し、これを各デバイスに手動もしくは 3rd Party のシステムを介してインジェクションする方法が一般的である。この作業にコストがかかり、また作業者（3rd Party）の信頼に依存するためプロセスに脆弱性が存在する。今回は、CG 社の EDGE と HUB の DID と Sidetree の仕組みを活用することで、デバイス内部で鍵ペア生成、sidetree node に公開鍵をハッシュ化したペイロードを送信、DID Document（公開鍵証明書に該当）を生成する。この仕組みを活用することで、プロビジョニング工程を自動化することができ、従来発生していたコストを削減、

また仲介者を排除することで、プロセスの脆弱性も低減することができる。
今回はこの仕組みを MFP デバイスにおいても確認することができた。

- C.「IoT 向けの軽量メッセージングプロトコル」について
  TCP/IP に TLS を実装し VC を送信する方法と、VC そのものを暗号化し送信する選択肢がある。IoT 機器の場合、デバイスが収集した IoT データを simplex に非同期に最終目的地に届けたいニーズが多く存在する。具体的に、デバイスがアクティブであることを確認するために、定期的に外部に向けて信号やパケットを送信する場合や、デバイスのセキュリティを更新するために、外部から大量のデバイスに向けて更新プログラムを配布する場合に、データを単一方向かつ非同期に送信したいニーズが存在する。また IoT システムには、複数の TCP Connection Hops を跨ぐことや、ノード間で利用される通信プロトコルが多岐にわたるなどの IoT 特有の特徴が存在する。したがって、IoT 機器で構成される分散システムにおいては、TCP/IP+TLS に頼らない、軽量でセキュアなプロトコルが求められている。本実証では、CG 社 EDGE の DIDComm メッセージングプロトコルと MQTT を組み合わせ、DID を持つ MFP デバイスとクラウド間でトランスポートに依存することない、検証可能な E2EE（End-to-End Encrypted）通信できることを確認した。また本実装では、暗号化データのルーティングを行う CG 社 HUB とデバイスがセキュアな相互認証チャネルを構築（HUB 側で DID と MQTT topic path とのテーブルを保有する）ことで、エッジデバイス側の Listening Port をインターネット上に露出しない構成を実現しており、IoT 機器が標的にされやすい Port Scanning Attack の脅威から防ぐことができる。
- D.「デバイスの高度な認証・認可」について
  デバイス側にユーザ名やパスワードなどを設定し、クラウド側でデバイスの認証・認可を行う手法と、公開鍵認証およびポリシーベースでのアクセス制御を行う選択肢が存在する。現在 IoT セキュリティに関する国際標準規格においても、IoT 機器のパスワード認証は推奨されていない。また IoT 機器の場合、攻撃サーフェイスが非常に広く、システム管理者の気が付かないところでデバイスへの不正アクセスやなりしましが発生しやすい状況にある。したがって、公開鍵認証によるデバイスの認証に加えて、デバイスの真正性を担保できる事前認証の仕組み、および Proxy Server でのポリシーによるアクセス制御を行い、不正な振る舞いやトラフィックを早期に検知、対応、復旧する仕組みが必要である。本実証では、CG 社 EDGE と HUB を活用し、デバイスの真正性を担保する事前認証と公開鍵認証によるデバイス認証の仕組み、およびポリシーによるアクセス制御できることを確認した。
- E.「検証可能なデータ流通」について
  DID エコシステムは、自由意志をもつ自然人や法人を主体とする Issuer-Holder-Verifier モデルで説明・理解されることが多いが、IoT 機器やバーチャルマシンやサーバーなどのマシンを主体とし、マシン間の検証可能なデータ流通モデルとしても捉えることができる。つまり、自然人や法人の属性証明書に限らず、IoT 機器でセンシングあるいは生成するデータの検証可能範囲を拡大し、信頼できるデータとして自由に流通させる仕組みだと捉えることができる。本実証の場合、MFP デバイスが財務書類などの紙文書を電子化しデジタル署名を施すことで、クラウドストレージ、SaaS、マイクロサービス、ローカル PC などのさまざまなマシンで検証可能な電子化文書として利用されるシナリオを

想定している。本実証では、文書管理システムをプロトタイプとして作成し、MFP デバイスから送信される署名付き電子化文書を検証することで、監査証跡を担保することができる。また本実証では範囲外となるが、MFP デバイスの認証高度を高めることで、MFP アプリから CG 社 EDGE に MFP デバイスを操作するユーザ名などのメタデータを渡し、「いつ・誰が・どのデバイスから」といったデータ検証が可能になる。

- F.「他 IoT 機器への拡張性」について
  CG 社 EDGE は、1) さまざまなハードウェアセキュリティモジュールと統合できるように汎用的な RoT Extensions が設計されている、2) オープンソースとして実装されている、3) Client App が操作できる汎用的な API が準備されている。従って、これまで述べた A~E の要件は MFP デバイスに限らず、リテール機器や医療機器などの IoT 機器についても同様に適用することができる。

（２）基本設計

以下の図 3.1.1-1 に本実証で構築するシステムの構成を示す。

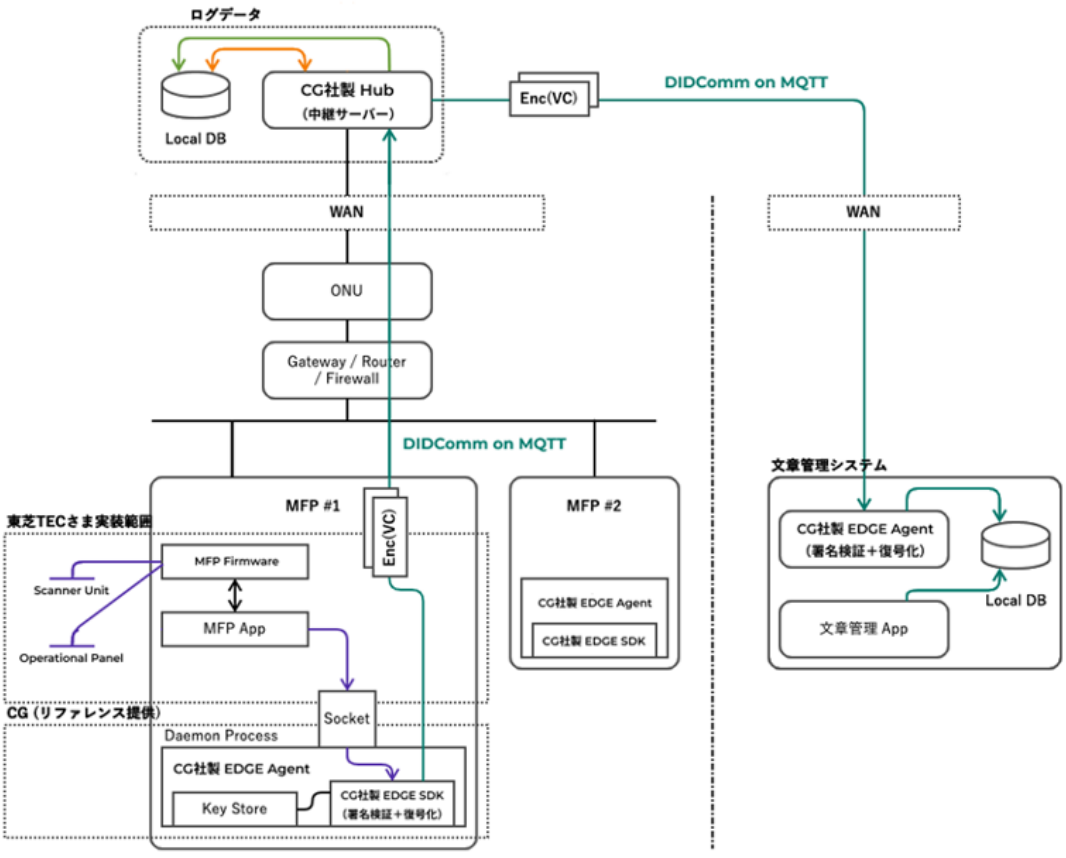


図 3.1.1-1 システム構成

本システムは MFP、MFP で動作するアプリケーション（以下、MFP アプリ）、CG 社 EDGE、CG 社

HUB、文書管理システムで成り立っている。MFP と文書管理システムには、CG 社 EDGE エージェントが搭載され、DID の生成や操作、DID 間での安全なコミュニケーションを実現している。 MFP アプリで電子化文書を生成し、CG 社 EDGE に送信し、EGDE 内部でデジタル署名および暗号化処理を行う。このデジタル署名付き暗号化データを CG 社 HUB を中継して、文書管理システムに統合された CG 社 EDGE で受け取り、復号化と署名検証を行い、データベースに保管する。

（３）システム開発

本実証の開発対象は以下になる。

- MFP アプリ（スキャンデータを CG 社 EDGE に API 経由で送信する）
- CG 社 EDGE と、MFP アプリと TPM2.0 との統合
- 文書管理システム

CG 社 HUB や MFP システムソフトは既存のものを利用するため、今回の開発対象からは外れる。業務フロー、データフロー、機能一覧、画面構成と遷移については、「基本設計書」を参照。

（４）ユーザテスト

本実証期間でユーザテストを実施しない

3.1.2 ヒアリングの実施

（１）ヒアリング概要と実施

- 2022 年 11 月中旬 地方自治体（S 市役所）IT 担当へ、行政文書の電子化の現状と課題についてヒアリング
- 2022 年 12 月下旬 TTEC MFP 国内営業部へ、監査証跡の担保ニーズについてヒアリング

（２）ヒアリング結果

S 市地方自治体：紙業務とデジタルのダブルスタンダードが大変。どの自治体にも文書保管室があり、大量の行政文書（紙）を管理。5 年単位で破棄するなど無駄な業務だらけ。一つの市庁の課（15 人前後）に MFP が一台設置、国家・地方公務員 330 万人、おおよそ 22 万台の導入ポテンシャルが存在。

TTEC MFP 国内営業部：大手から B2B 取引でのデジタルシフトは進んでいるが、SMB（Small to Medium Business）市場ではまだまだ紙業務が多く残っている。取引先などが紙業務、従業員が受け取る領収書の原本保管など、経理・財務系の紙文書の保管は継続して必要。営業目線では、監査証跡が担保できる機能で、普段の業務体験がどう変わるのかを伝えられるといい。

（３）ヒアリング結果の総括

地方自治体や中小企業を中心に、財務文書や行政文書などの原本管理が求められる紙文書管理

のデジタル化が進んでいない現状を確認できた。デジタルシフトの過渡期において、未だ根強く残る紙業務・過去文書管理に対し、誰でも簡単に利用できるデジタルソリューションが求められている。従って、本実証では、エンドユーザのこれまでの MFP 利用体験を大きく変えずに、誰もが簡単に使えるソリューションであることを訴求ポイントして意識してデモ動画を作成する。

参考）監査証跡が求められる文書一覧

- レンタルまたはリース契約
- 売買契約または資産購入契約
- 金銭消費貸借契約書
- 許可証
- 財務書類
- 保険関連書類
- 目論見書
- 賠償責任放棄書
- 医療関係書類
- 研究論文
- 製品保証書
- 秘密保持契約書
- オファーレター
- 機密保持契約書
- 独立請負人契約書
- 行政文書

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

表 3.2.1-1 に本実証システムのデータフローを示す。

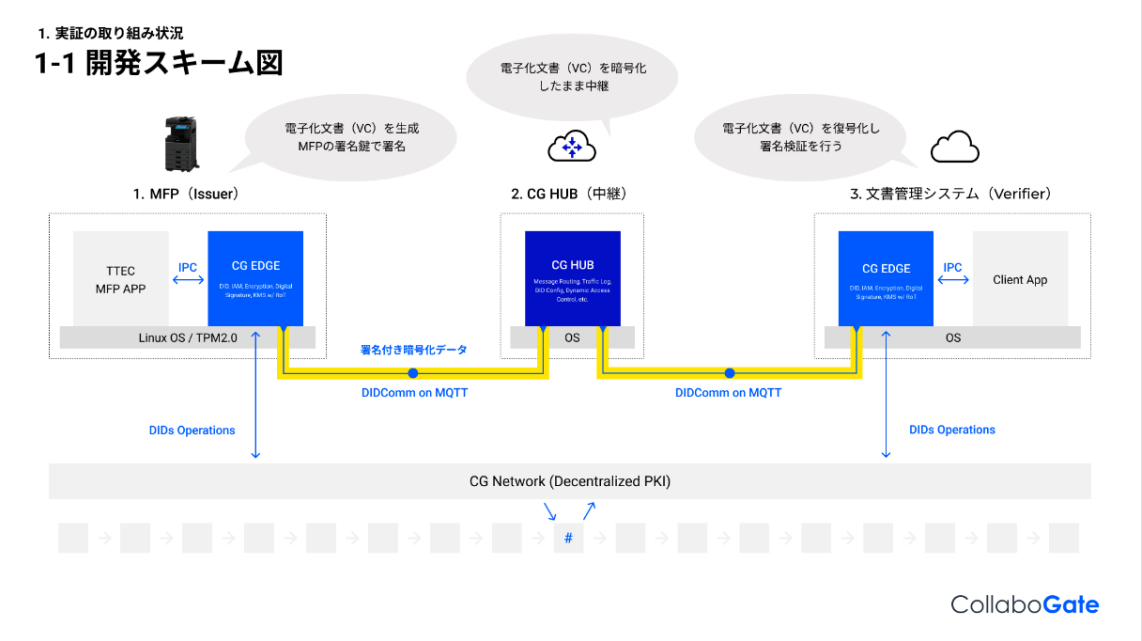


図 3.2.1-1　データフロー図

本実証では、図中の MFP デバイスが文書管理システムに署名付き暗号化データ（DIDComm Enc (VC)）を送信する。ユーザは、文書管理システムで受け取った署名付き暗号化データを復号・署名検証し、「どのデバイスから」スキャンしたデータなのかを確認することができる。また MFP アプリから、ユーザ名や設置場所やタイムスタンプなどのメタデータを渡し、署名付きメッセージに含めることで「いつ、誰が、どのデバイスから」スキャンしたデータなのかを検証可能にする。文書管理システムに保管する電子化文書には、一般的なユーザ名とパスワードによる認証・認可でアクセス制御する（本プロトタイプでは、必要最低限のユーザ認証を行う）。

3.2.2　データフローに登場する主体とその概要

- MFP デバイス
  - TTEC 社製 MFP（e-STUDIO シリーズ）に CG 社製 EDGE を搭載。MFP デバイスは自身の分散型 ID を管理し、電子化文書にデジタル署名・暗号化を施して文書管理システムに送信する。
- CG 社 HUB
  - HUB は、MFP デバイスから署名付き暗号化メッセージを受け取り、目的地である文書管理システムにメッセージを中継する。メッセージ Bus、高度なデバイス認証（公開鍵認証と事前認証の仕組みによるデバイスの真正性担保の仕組み）、ポシリーベースでのアクセス制御、トラフィックログ保管などの役割を担う。
- 文書管理システム
  - 文書管理システムは、受け取った電子化文書を復号・署名検証することで、「いつ、誰が、どの

デバイス」を確認し、これをシステムのデータベースに登録する。

- 導入法人・従業員
  - オフィスに設置された MFP で書類をスキャンして文書管理システムに送信する。紙業務をデジタル管理する主体。
- サービス提供者
  - MFP や文書管理システムを提供する主体。

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

- 従来と比べて拡大した検証可能領域
  - 従来、MFP デバイスでは当該範囲を検証することが困難であった（誰がいつどのデバイスで生成したものであるかを検証することが難しかった）。本実証事業では、MFP デバイスが電子化文書（VC）を作成し、文書管理システムに送信する。この電子化文書を検証することで、誰がいつどの MFP デバイスから生成した電子化文書であるかを確認することができる。ユーザはこれまでのスキャン作業と同じ体験でありながら、財務書類などの監査証跡の担保が求められる紙業務のデジタル化を実現することができる。
  - 本実証事業の対象からは外れるが、クラウドからエッジデバイスへのメッセージングも同様の仕組みで検証可能にすることができる。エッジデバイスのソフトウェアやセキュリティパラメーターの更新やデバイスの遠隔操作などを目的に、クラウドからエッジデバイスへのメッセージも必要とされる場合が多い。こうしたデバイスとクラウドとの双方向のメッセージの検証領域を拡大することは、IoT 機器を標的としたセキュリティ脅威に対して有効な対策となる。
- 検証の仕組み
  - 本プロトタイプでは、MFP デバイスに搭載された CG 社 EDGE が、電子化文書（VC）を生成し、文書管理システムに送信する。文書管理システム側に搭載された CG 社 EDGE が、受け取った電子化文書（VC）を復号化し、デジタル署名を検証する。
- トラストが向上したことで誰がどのような恩恵を受けるのか
  - 企業の経理業務や地方自治体の行政文書管理業務を行う従業員が、これまでのスキャン作業と同じ体験でありながら、財務書類などの監査証跡の担保が求められる紙業務のデジタル化を推進することができて、生産性の向上につながる。

（参考）新電子帳簿保存法では領収書、請求書、納品書などの紙書類には 7 年間の保管義務がある。電子化文書を正本として保管し、紙を捨ててよい状態にするためには、タイムスタンプが押されていることや改善防止の措置があることなどいくつか満たすべき要件がある。

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

今回のユースケースにおいては、MFP 機器の導入企業（管理者）とサービス提供者（東芝テック）

との間に、契約書という形でデータの取り扱いなどの合意を行うことになるが、これは Trusted Web の要件で期待されている内容とは異なるものと理解している。一般的にも IoT 機器とクラウドとの通信を考えると、Trusted Web 要件 3 と 4 にある自然人を前提としている合意という言葉をそのまま適用することが難しいのではないかと考える。

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

- MFP デバイスの識別子（DID）
- MFP デバイスの属性情報（シリアル番号、設置場所、ユーザ名など）
- スキャンした電子化文書

（2） 検証者

- 文書管理システム（CG 社 EDGE）

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

MFP デバイスと文書管理システム

（2） アイデンティティ管理システム

DID に基づく認証・認可システム、一般的なユーザ名とパスワードによる認証・認可（文書管理システム側）

(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

MFP デバイスのアイデンティティは、デバイスの DID、企業名・設置場所、ユーザ名、シリアル番号など属性情報で形成される（図 3.3.2-1）。

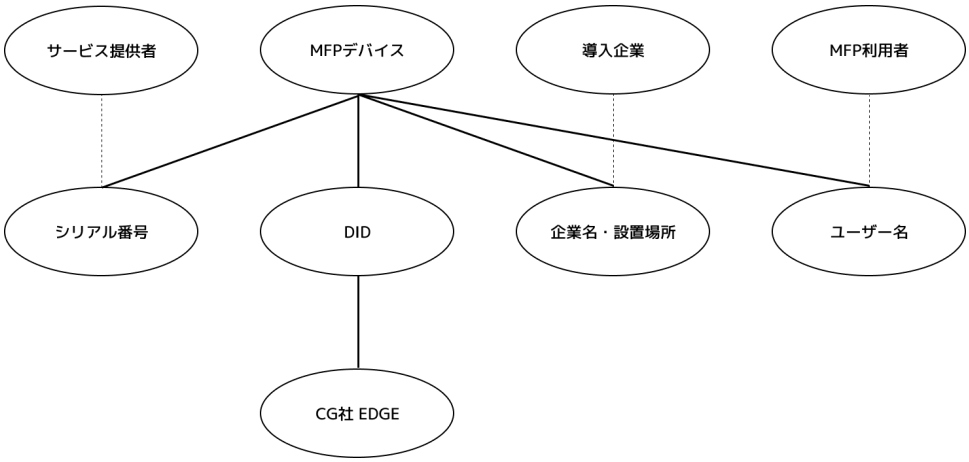


図 3.3.2-1　MFP デバイスのアイデンティティグラフ

上列からアイデンティティ、属性情報、ノードで構成されており、図中の実線はアイデンティティに紐づく属性情報の繋がり、点線は関係性のグラフを示す。

文書管理システムのアイデンティティは、システムの DID、企業名、サービス提供者、システム利用者などの属性情報で形成される（図 3.3.2-2）。

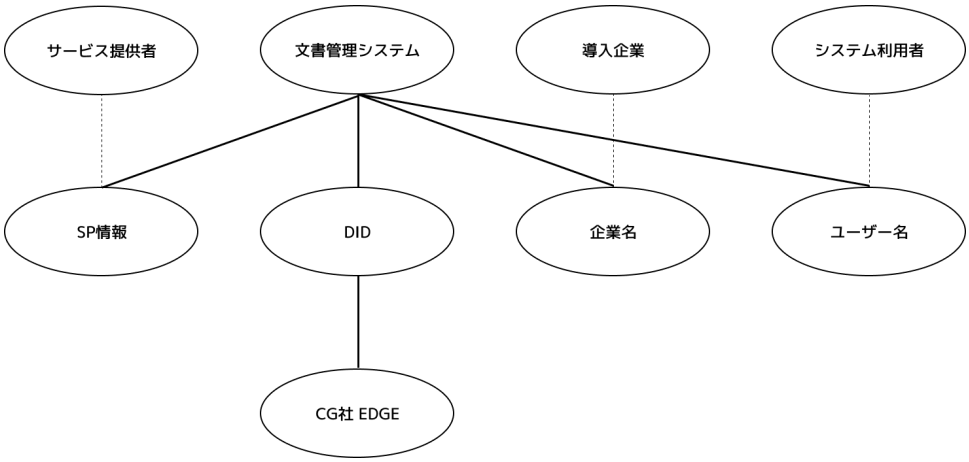
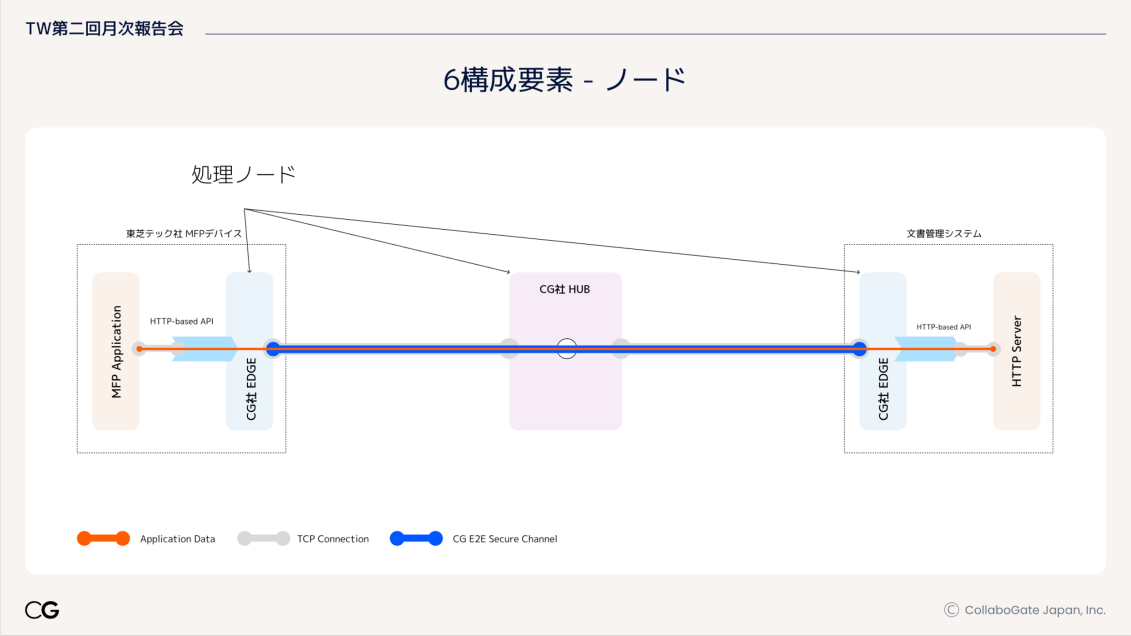


図 3.3.2-2 文書管理システムのアイデンティティグラフ

3.3.3 ノード

（1） Wallet の使用有無



3.3.3-1 6 構成要素-ノード

図 3.3.3-1 中の EDGE と HUB がそれぞれ識別子に紐づく秘密鍵を管理するノードになる。

（2） 合意形成がされているか、されている場合その手段

本ユースケースでは合意のプロセスを想定していない

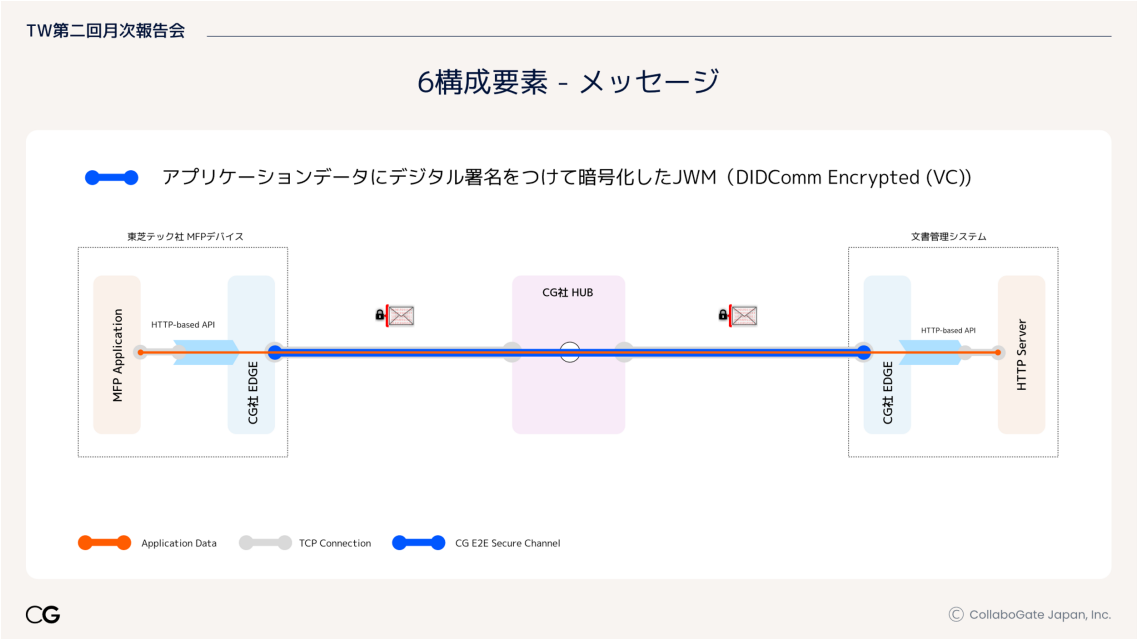
（3） データのやり取りの記録場所

HUB のトランザクションログ DB

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

本実証事業では、CG 社 EDGE が、HUB との間に相互認証コネクションを構築し、DIDComm Enc（署名付き暗号化メッセージ）を送信する（図 3.3.4-1）。



3.3.4-1　6 構成要素-メッセージ

以下に処理の順序について記載する。

1. CG 社 EDGE は、MFP アプリから受け取る電子化文書データを W3C – Verifiable Credential Data Model に従い VC として作成
2. 生成した VC から DIDComm Message Format[3]に従い、DIDComm Plaintext Message を生成
3. DIDComm Plaintext Message を暗号化し、DIDComm Encrypted Message を生成（暗号化した DIDComm Plaintext Message を “ciphertext” に格納。”ciphertext” は DIDComm Plaintext Message を共通鍵（ECDH-1PU+XC20PKW）で暗号化して格納する領域）
4. 受信側は、DIDComm Encrypted Message の ”protected” を bease64 で decode することで、送信元の DID を確認（”protected”は DIDComm encrypted message に含まれる鍵ラッピングの共通 header（JWE）。送信元の DID や暗号鍵情報を格納する領域）。
5. 送信元の DID Document から暗号用公開鍵を取得し、共通鍵を生成し、受け取った DIDComm Encrypted Message を復号する。
6. 最後に、送信元の DID から署名用公開鍵を取得し、復号した DIDComm Plaintext Message に含まれる VC の署名検証を行う

[3] https://identity.foundation/didcomm-messaging/spec/#didcomm-plaintext-messages

Verifiable Credential (電子化文書)


```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1"
    ],
    "credentialSubject": {
        "container": [
            {
                "base64_data": "JVBERi0xLjMNCiXi48X…",
                "filename": "FILENAME0000",
                "media_type": "application/pdf"
            }
        ]
    },
    "issuanceDate": "2023-02-23T08:53:49.943249+00:00",
    "issuer": {
        "id": "did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg"
    },
    "proof": {
        "challenge": null,
        "controller": null,
        "created": "2023-02-23T08:53:49.943419+00:00",
        "domain": null,
        "jws":
"eyJhbGciOiJFUzI1NksiLCJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdfQ..AvGSbU5lH7IR6MIgefmFbqBMRhdr
ncfCZnlaJMMpH2JllUQUwgcIYYlw7WjQbSsOPXQmCr-eXq8uOUneJ3ySxQ",
        "proofPurpose": "authentication",
        "type": "EcdsaSecp256k1Signature2019",
        "verificationMethod":
"did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg#signingKey"
    },
    "type": [
        "VerifiableCredential"
    ]
}
```

DIDComm Plaintext Message


```
{
    "id": "543db1d5-e921-4538-9c58-41a4782e03aa",
    "type": "JWM",
    "from": "did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg",
    "to": [ "did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg" ],
    "typ": "application/didcomm-plain+json",
    "body": {
        "@context": [
            "https://www.w3.org/2018/credentials/v1"
        ],
        "credentialSubject": {
            "container": [
                {
                    "base64_data": "JVBERi0xLjMNCiXi48...",
                    "filename": "FILENAME0000",
                    "media_type": "application/pdf"
                }
            ]
        },
        "issuanceDate": "2023-02-23T08:53:49.943249+00:00",
        "issuer": {
            "id": "did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg"
        },
        "proof": {
            "challenge": null,
            "controller": null,
            "created": "2023-02-23T08:53:49.943419+00:00",
            "domain": null,
            "jws": "eyJhbGciOiJFUzI1NkQ...",
            "proofPurpose": "authentication",
            "type": "EcdsaSecp256k1Signature2019",
            "verificationMethod":
"did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg#signingKey"
        },
```

```
            "type": [ "VerifiableCredential" ]
        },
        "attachments": [
            {
                "data": {
                    "json":
"{¥"location¥":¥"Jupiter¥",¥"mfp_serial¥":¥"SERIAL0000¥",¥"user¥":¥"USER0000¥"}",
                    "links": [ "https://did.getunid.io" ]
                },
                "format": "metadata",
                "id": "clegvat4u0000ehq3d78bh2md",
                "lastmod_time": "2023-02-23 08:53:49.950270 UTC"
            }
        ]
}
```


DIDComm Enc Message

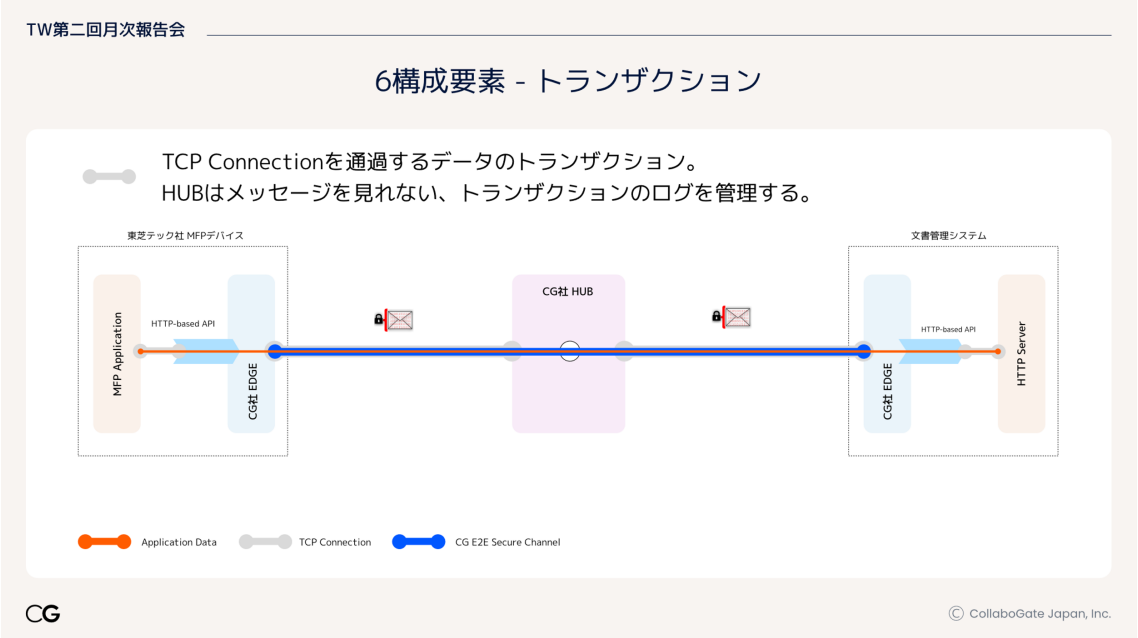

```
{
    "ciphertext": "1USvve5YjPqM...",
    "iv": "QXtoOcsCfTn408epoKXzuZrJ4saKaAGr",
    "protected": "eyJ0eXAiOiJhcHBsaWNhdGlv...",
    "recipients": [
        {
            "encrypted_key": "ehgyo813uvz4iRq50BLdESxiLQl0ak2tlpSwazajhsQ",
            "header": {
                "alg": "ECDH-1PU+XC20PKW",
                "epk": {
                    "crv": "X25519",
                    "kty": "OKP",
                    "x": "-KUZm2DJNvSD5I-gSE_z6l1jmYefW70jNHjYg3Bum2Y"
                },
                "iv": "NnmvFYJ3ravTjFNcLD7HSLZOTnns8Ojf",
                "key_ops": [],
                "kid": "did:unid:test:EiCYAhLIt9pfzz9pR7bUolzJVqYWfkq_dH9_ox1vfpKQTg",
                "tag": "uDN-lHOT8zZMvyzaxSKE1w"
            }
```

```
        }
    ],
    "tag": "6IbsAW9CenSDIZBWaeF2xw"
}
```


3.3.5 トランザクション

（1）　データのやり取りの記録・検証はできるか

HUB 側のトランザクションログ DB で、すべてのトランザクションログを管理する（図 3.3.5-1）。

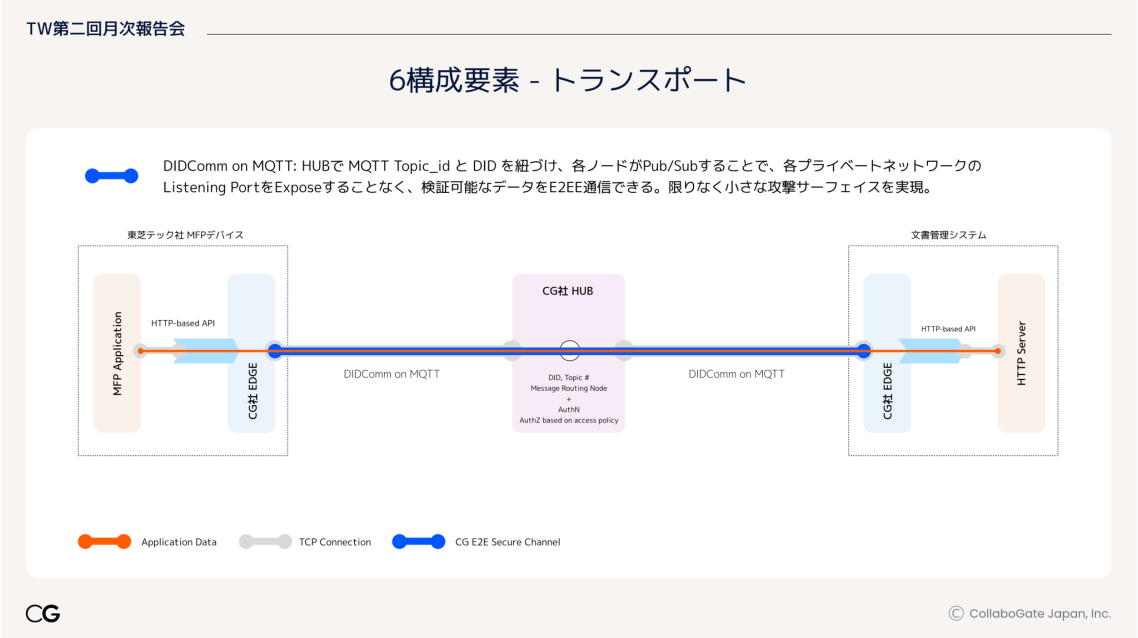


3.3.5-1　6 構成要素-トランザクション

3.3.6 トランスポート

（1）　トランスポートのプロトコル

HUB 側で MQTT Topic と DID を紐づけるテーブルを保有することで、MFP デバイスや文書管理デバイスの Listening Port を露出することなく、ノード間で DIDComm Enc（署名付き暗号化メッセージ）を送信する（図 3.3.6-1）。



3.3.6-1　6 構成要素-トランスポート

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

（１）文書のスキャンと文書管理システムへの保存

文書をスキャンし、文書管理システムに保存するフローを示す（図 3.4.1-1）。MFP、文書管理システムの DID は生成済み、HUB に登録済みとする。文書作成者は文書管理システムの DID を知っていることとする。

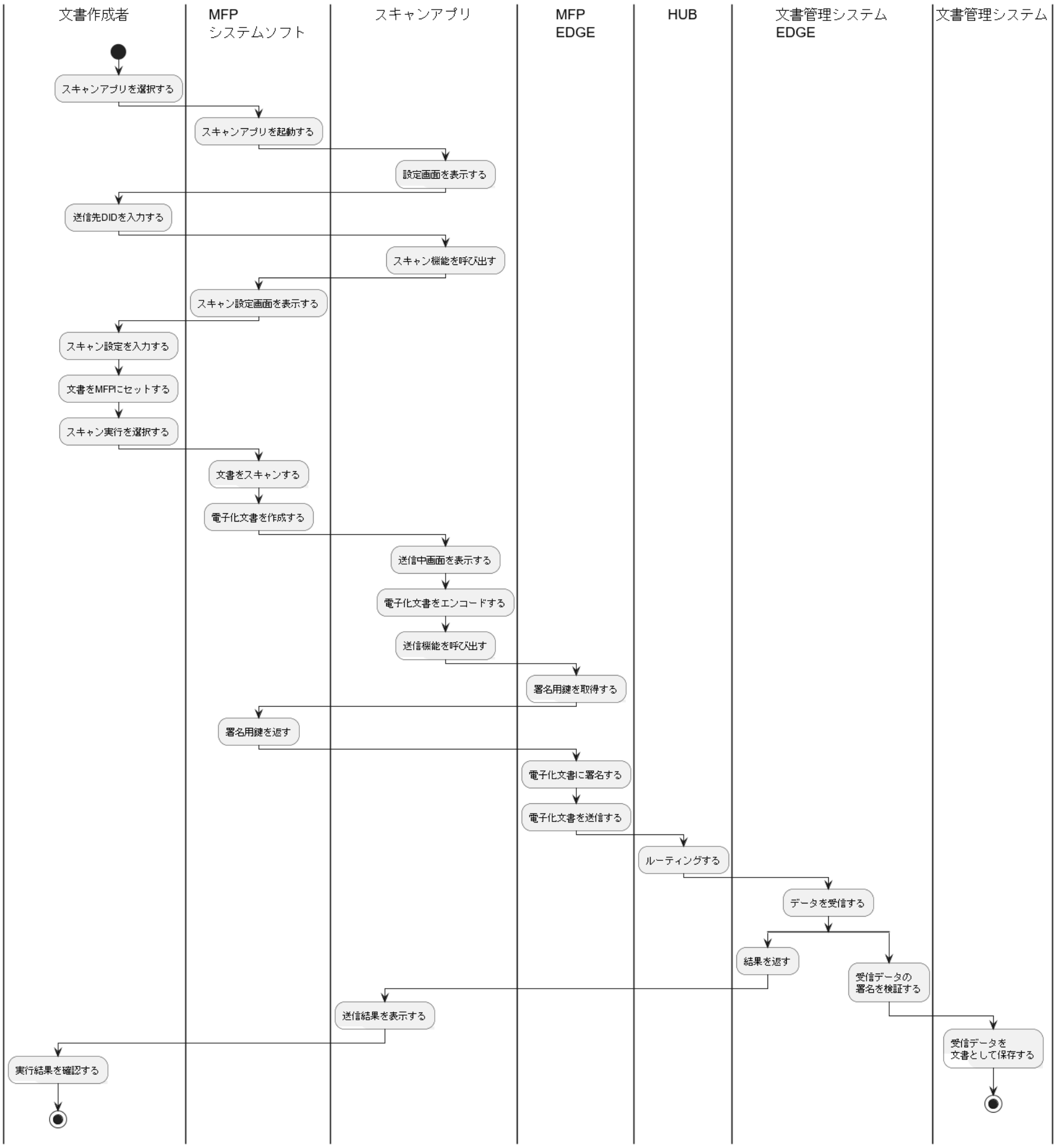


図 3.4.1-1 業務フロー図- 文書のスキャンと文書管理システムへの保存

1. 文書作成者は ID/Password または物理カードを使った MFP に設定された認証方式に従ってログインする
2. 文書作成者は MFP のパネルからスキャンアプリを選択する
3. MFP システムソフトはスキャンアプリを起動する
4. スキャンアプリは起動後に設定画面を表示する
5. 文書作成者は送信先となる DID を入力し、次の画面へ遷移するボタンを選択する
6. スキャンアプリはスキャン機能を呼び出す
7. MFP システムソフトはスキャン設定画面を表示する
8. 文書作成者はスキャン設定を入力し、文書をセットする
9. 文書作成者はスキャン実行ボタンを選択する
10. MFP システムソフトは文書をスキャンし、電子化文書を作成する
11. スキャンアプリは送信中画面を表示し、電子化文書をエンコードする
12. スキャンアプリは MFP EDGE インタフェースの送信機能を呼び出す
13. MFP EDGE インタフェースは MFP システムソフトの署名用鍵の取得機能を呼び出す
14. MFP システムソフトは署名用鍵を取り出し、MFP EDGE インタフェースに渡す
15. MFP EDGE インタフェースは電子化文書に署名し、電子化文書の送信処理を行う
16. HUB は宛先 DID を元にルーティングを行う
17. 文書管理システムの EDGE インタフェースはデータを受信すると、送信元に応答を返す
18. スキャンアプリは送信結果を受け取ると、送信結果を表示する
19. 文書作成者はスキャン実行結果を確認する
20. 17.と並行して、文書管理システムの EDGE インタフェースは送信元 DID の公開鍵を Sidetree から取得する
21. 文書管理システムの EDGE インタフェースは受信データの署名を検証する
22. 文書管理システムは受信データを文書として保存する

（２）MFP の DID 生成と登録について

MFP の DID 生成と登録に係るフローを以下に示す（図 3.4.1-2）

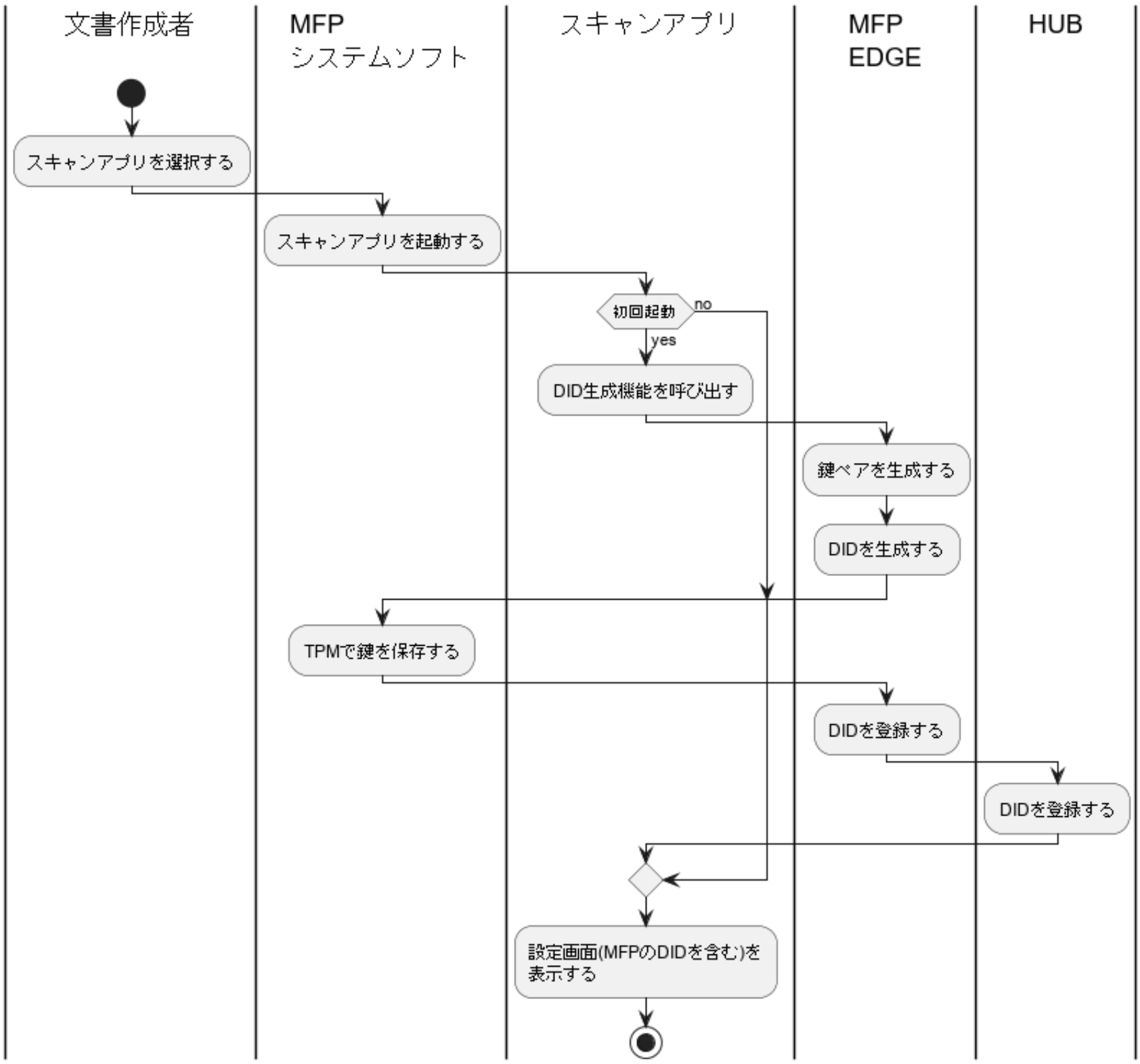


図 3.4.1-2 業務フロー図- MFP の DID 生成と登録

1. 文書作成者は MFP のパネルからスキャンアプリを選択する
2. MFP システムソフトはスキャンアプリを起動する
3. スキャンアプリは初回起動かどうか判定を行い、初回起動時にのみ DID 生成と登録を行う
4. スキャンアプリは EDGE インタフェースの DID 生成機能を呼び出す
5. MFP EDGE インタフェースは鍵ペアを生成し、DID Document を作成する
6. MFP EDGE インタフェースは作成した DID Document を Sidetree に送信する
7. Sidetree 側では DID Document を受信すると、DID を登録し、それを返却する
8. MFP EDGE インタフェースは DID を受信すると、MFP システムソフトのインタフェースを通して、MFP 内の TPM に鍵を保存する
9. MFP EDGE インタフェースは鍵を保存後、DID を保存し、呼び出し元に戻る
10. スキャンアプリは起動後に設定画面を表示する

（３）文書管理システムの文書を閲覧する

文書閲覧のフローを示す（図 3.4.1-3）。

文書一覧を表示後に閲覧者は文書を削除することもできる。

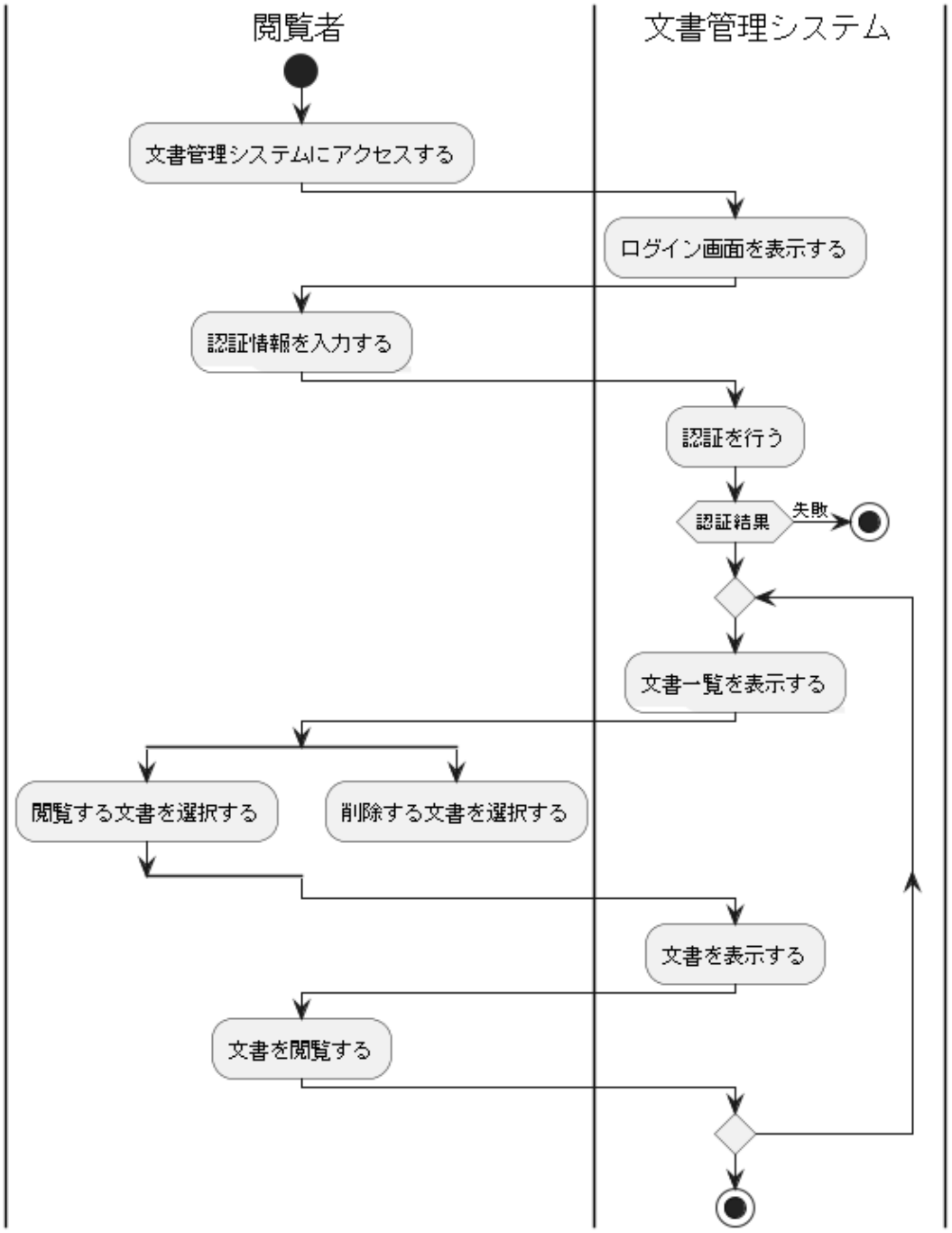


図 3.4.1-3 業務フロー図- 文書管理システムの文書閲覧

1. 閲覧者はブラウザを利用して文書管理システムにアクセスする
2. 文書管理システムはログイン画面を表示する
3. 閲覧者は認証情報を入力する
4. 文書管理システムは認証を行う。成功した場合、文書一覧を表示する
5. 閲覧者は文書一覧から、閲覧する文書を選択する閲覧者が閲覧する文書を選択した場合、文書管理システムは選択された文書を表示する
6. 閲覧者は文書を閲覧する

（４）文書管理システムの文書を削除する

文書一覧を表示後に文書を削除するフローを示す（図 3.4.1-4）。

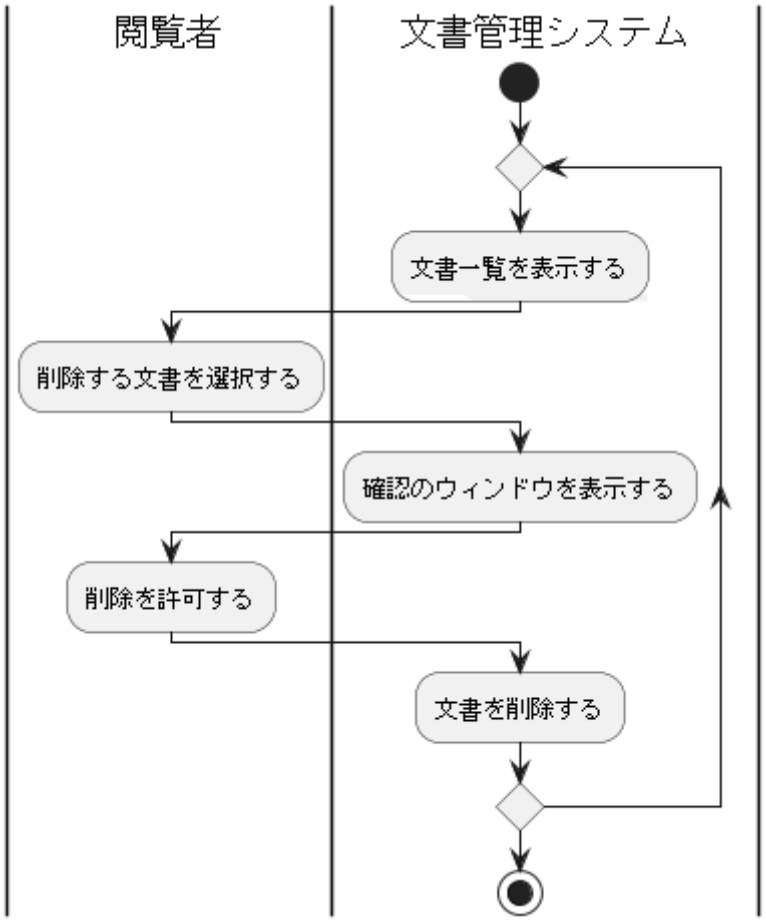


図 3.4.1-4 業務フロー図-文書管理システムの文書削除

1. 文書管理システムは文書一覧を表示する
2. 閲覧者は削除する文書を選択する
3. 文書管理システムは削除するか確認のウィンドウを表示する
4. 閲覧者は削除を許可する
5. 文書管理システムは文書を削除し、削除後の文書一覧を表示する

（５）トラフィックログを確認する

トラフィックログを確認するフローを示す（図 3.4.1-5）。このフローは、HUB のみが関連するため開発対象に含まれないが、実証項目として動作確認を実施する。

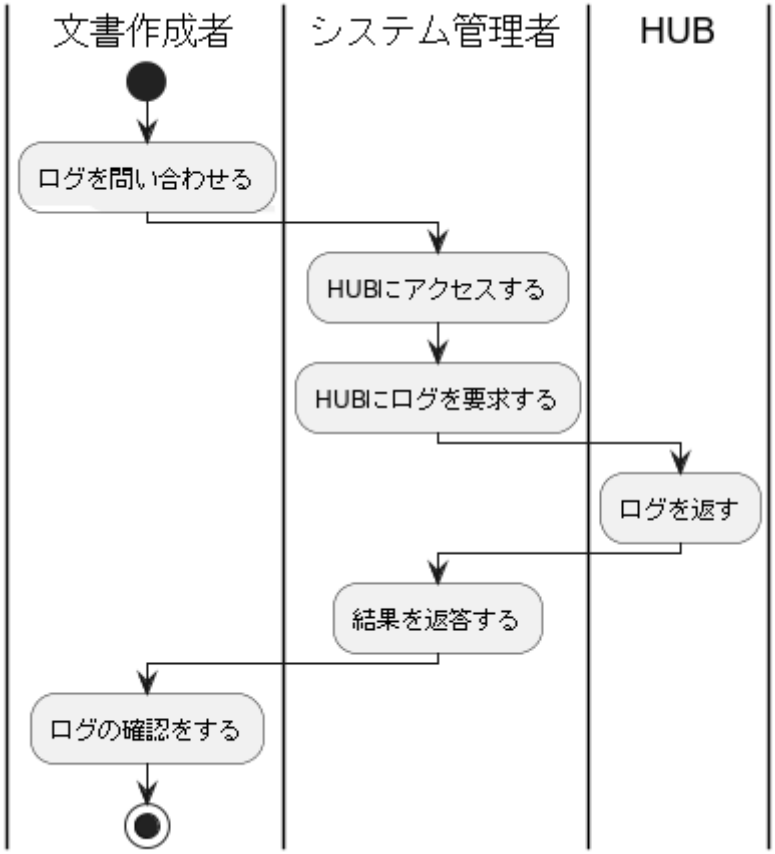


図 3.4.1-5 業務フロー図-ログ確認

1. 文書作成者はトラフィックログを HUB のシステム管理者に問い合わせる
2. システム管理者は HUB にアクセスし、トラフィックログの取得を行う
3. システム管理者は取得したトラフィックログを文書作成者に返答する
4. 文書作成者はログを見ることで、いつどのデバイス（識別子）からどの宛先にデータが送られたのかを確認する

3.4.2 ユースケース図

ユースケース図を以下の図 3.4.2-1 に示す。

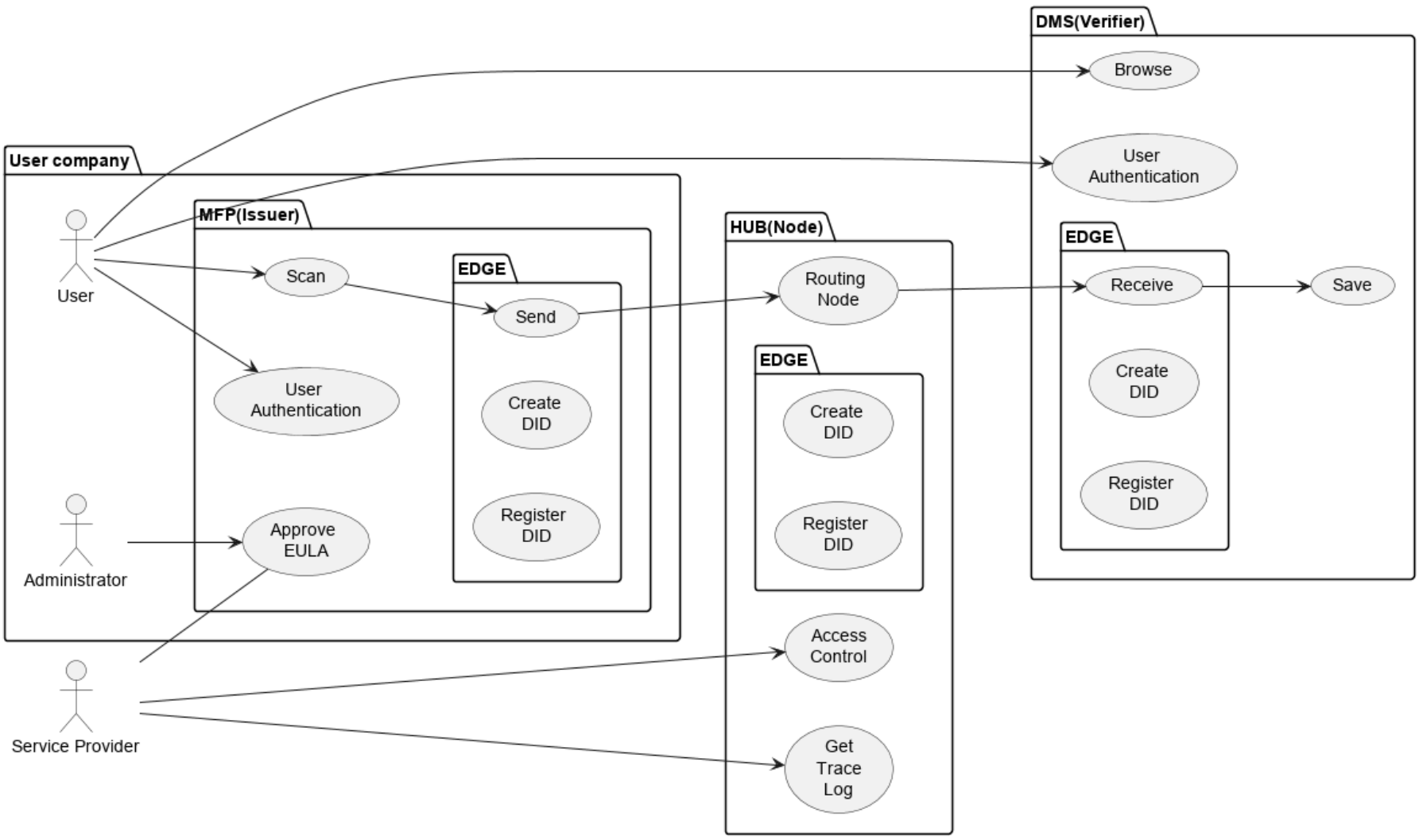


図 3.4.2-1 ユースケース図

Actor:

User: 利用者。文書の作成、閲覧を行う。

Administrator: 企業内のシステム管理者

Service Provider: サービス提供者。スキャンアプリ作成、HUB 管理を行う。

Use Case:

Scan: 紙をスキャンして電子化文書にする

User Authentication: 正当な利用者であることを認証する

Approve EULA: EULA(End-User License Agreement)を許諾する

Send: 電子化文書に署名を行い宛先 DID に送信する

Create DID: DID Document を生成する

Register DID: DID Document を Sidetree に登録する

Routing Node: 対象の DID を持つデバイスへの通信をルーティングする

Access Control: アクセスポリシーを変更し、認可しない EDGE デバイスからのアクセスを禁止する

Get Trace Log: トラフィックログを取得する

Browse: 電子化文書を閲覧する

Receive: 電子化文書を受信する

Save: 電子化文書を保存する

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。

機能一覧/非機能一覧

表 3.4.3-1 機能/非機能一覧

機能/非機能	機能名	搭載箇所	機能概要
機能	Scan	MFP	紙をスキャンして電子化文書を作成する
機能	Send	EDGE	電子化文書を宛先 DID のストレージに送信する
機能	Routing	HUB	対象の DID を持つ EDGE デバイスへの通信をルーティングする
機能	Receive	文書管理システム	自 DID に送付された電子化文書を受信する
機能	Save	文書管理システム	受信した電子化文書を保存する
機能	Browse	文書管理システム	ストレージに保存された電子化文書を閲覧する
機能	Create DID	EDGE	DID Document を作成する
機能	Register DID	EDGE	DID Document を Sidetree に登録する
機能	Access Control (HUB)	HUB	アクセスポリシーを変更し、認可しない EDGE デバイスからのアクセスを禁止する。
機能	Get Trace Log	HUB	トラフィックログを取得する
非機能	Access Control (DMS)	文書管理システム	文書管理システムに特定ユーザのみアクセスできるようアクセス制御を行う
非機能	Remote Operation	文書管理システム	文書管理システムはネットワークを通してリモート操作を行う

MFP に搭載する Scan 機能は、紙をスキャンして電子化文書を作成する。

EDGE に搭載する Send 機能は、電子化文書を宛先 DID のストレージに送信する。 Create DID 機能は DID Document を生成する。 Register DID 機能は DID Document を Sidetree に登録する。

HUB に搭載する、Routing Node 機能は対象の DID を持つ EDGE デバイスへの通信をルーティングする。Access Control(HUB)機能はアクセスポリシーを変更し、認可しない EDGE デバイスからのアクセスを禁止する。Get Trace Log 機能はトラフィックログを取得する。

文書管理システムに搭載する、Browse 機能では利用者は電子化文書を閲覧することができる。Receive 機能では自 DID に送信された電子化文書を受信する。Save 機能では受信した電子化文書を保存する。 Access Control(DMS)機能によって特定のユーザのみ利用できる。 Remote Operation 機能によって、遠隔地から文書管理システムを利用することができる。

3.4.4 データモデル定義

3.3.4 のメッセージで整理される各種メッセージごとのデータモデルは、それぞれ W3C - Verifiable Credential Data Model, DIDComm Message Format に準拠する。上から VC, DIDComm Plaintext Message, DIDComm Encrypted Message の順番で、各種データモデルを整理している。

表 3.4.4-1 データモデル定義-VC

属性値	属性取得元	属性値（VC 内）
電子化文書	MFP デバイス	credentialSubject.container[number].base64_data
ファイル名	MFP デバイス	credentialSubject.container[number].filename
MIME タイプ	MFP デバイス	credentialSubject.container[number].media_type
発行元	MFP デバイス	issuer.id
発行日	MFP デバイス	issuanceDate

表 3.4.4-2 データモデル定義-DIDComm Plain (DCPM)

属性値	属性取得元	属性値（DIDComm Plain (DCPM) 内）
ユーザ名	MFP デバイス	attachments[number].data.json.user
MFP 設置場所	MFP デバイス	attachments[number].data.json.location
MFP シリアル番号	MFP デバイス	attachments[number].data.json.mfp_serial

表 3.4.4-3 データモデル定義- DIDComm Enc (ECEM)

属性値	属性取得元	属性値（DIDComm Enc (ECEM) 内）
送信先 DID	MFP デバイス（HUB から更新可能）	recipients.header.kid

3.4.5 実験環境

実験環境図を図 3.4.5-1 に示す。

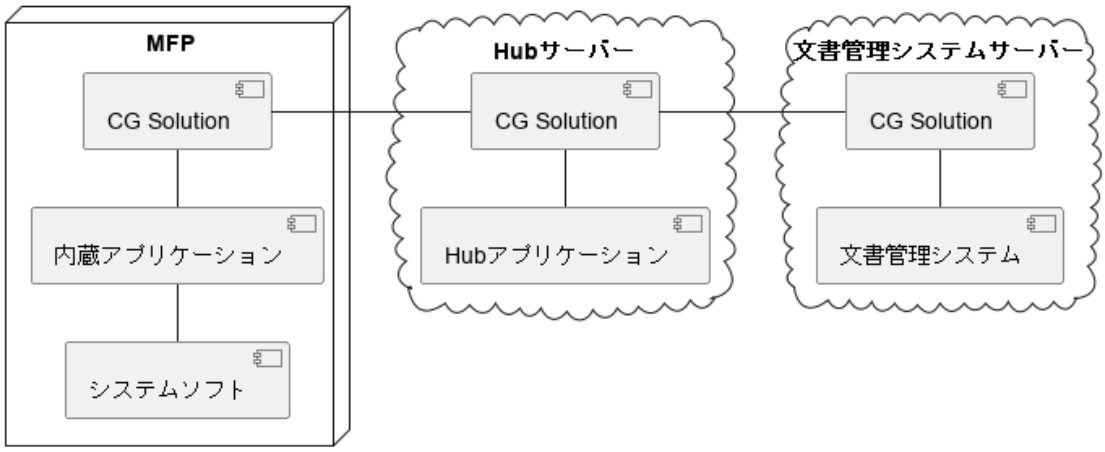


図 3.4.5-1 実証環境図

実験環境には MFP、Hub サーバー、文書管理システムサーバーが必要となる。MFP には MFP システムソフトの他に、内蔵アプリケーション、CG 社 EDGE を備える。Hub サーバーには Hub アプリケーションと CG 社 EDGE を備える。文書管理システムサーバーには文書管理システムのと CG 社 EDGE を備える。

3.4.6 システムの構成要素

システム構成要素を表 3.4.6-1 に示す。

表 3.4.6-1 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	参照している国際標準
TTEC 社 MFP	E-STUDIO5525AC Series e-STUDIO5528A Series	-	-	
TTEC 社 MFP システムソフト	-	-	-	
TTEC 社 MFP アプリケーション	-	-	-	
CG 社 EDGE	V1.0.0	OSS	Apatch2.0	DID, VC
CG 社 HUB	V1.0.0	-		DID, VC,

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	参照している国際標準
				DIDComm
文書管理システム	prototype	-	-	DID, VC

システム構成要素としては、MFP、MFP システムソフト、MFP アプリケーション、EDGE,HUB、文書管理システムがある。MFP は東芝テック社製 MFP を利用する。型式は e-STUDIO5525AC Series/e-STUDIO5528A Series に対応している。上記 MFP に対応した MFP システムソフトが必要となる。また、今回の事業のための MFP アプリケーションを開発した。DID を取り扱う EDGE クライアントとして CollaboGate Japan 社製 EDGE を利用している。OSS であり、ライセンスは Apatch2.0 となっている。DID の HUB として CollaboGate Japan 社製 HUB を利用している。プロプライエタリソフトウェアである。文書管理システムは今回の用途のために開発したものとなる。

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

- ルートオブトラストの確立
  - MFP デバイスの TPM2.0 と CG 社 EDGE の RoT Extension 機能を活用し、真性乱数から暗号鍵ペアを生成し、秘密鍵を安全に管理する仕組みを確認できた。
- IoT 向けの軽量メッセージングプロトコル（DIDComm on MQTT）
  - CG 社 EDGE と HUB を活用し、MFP デバイス側と文書管理システム側の、各プライベートネットワークの Listening Port を露出することなく、NAT/Firewall を超えた署名付き E2EE 通信ができる仕組みを確認した。IoT システムにおける 1:N, 非同期, Simplex なメッセージ通信などの要求を満たし、TCP/IP+TLS に頼らない、軽量でセキュアな通信プロトコルが本システムにおいて動作することを確認した。
- デバイスの高度な認証・認可
  - CG 社 EDGE と HUB を利用することで、MFP デバイスと文書管理システム間で、DID に基づく公開鍵認証、事前のメッセージ認証（EDGE と HUB で事前に共有された秘密情報から HMAC 値を計算し、EDGE から HUB の初回通信時に HMAC 値を含める。HUB 側でこの HMAC 値を検証することで、サービス提供者がアクセス許可を与えたデバイスの識別子（DID）であるかどうかを判断する。）によるデバイスの真正性担保、アクセスポリシーに基づくアクセス制御ができる。本プロトタイプでは、MFP デバイスと文書管理システムにおいて、デバイスの高度な認証・認可ができることを確認した。
- プロビジョニングの自動化
  - CG 社の EDGE は DID と Sidetree を活用し、プロビジョニング工程における脆弱性とコストの課題を解決できる。従来の手法では、作業者の人件費、バックグラウンドチェック、セキュリテ

ィルームなどの設備費、認証局を利用するコスト、PKI インフラコストなどが発生する。またデバイスの外部で暗号鍵管理を行うことにはセキュリティ面で大きな問題がある。本実証では、CG 社 EDGE を活用し、MFP デバイスのプロビジョニング作業を自動化することで、これまで一台当たり 600~1,200 円のコストが発生していたプロビジョニングのコストをゼロに近づける。またデバイス内部で鍵生成を行い、公開鍵証明書（DID Document）の生成を自動化することで、プロセスに存在していた脆弱性を排除する。

- 監査証跡を担保した電子化文書の流通
  - TTEC 社の MFP と CG 社の EDGE と HUB を組み合わせることで、経理文書や行政文書などの監査証跡が必要な紙文書のデジタル保管をシームレスに実現できた。利用者がこれまで通りの業務フローのままで、簡単に紙文書のデジタル管理ができることを確認した。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

- 得られたビジネスの成果
  - 該当業務で発生する紙業務のデジタル化を実現し、利用者がシームレスに本システムを利用できることが確認できた。地方自治体職員および TTEC 社営業部のヒアリングベースになるが、未だ特定業界や業務では紙文書で管理されていることが多く、ペーパーレス化の過渡期において本システムのニーズがあることを確認できた。
- 得られたシステムの成果
  - CG 社の EDGE と TTEC 社 MFP TPM2.0 との統合が完了し、TTEC の MFP デバイスにおいてルートオブトラストの確立を達成できた。
  - CG 社の EDGE の DID Method を活用し、Bitcoin 上に構築する Sidetree Node を経由して、DID Operation を実現する。これにより、MFP デバイスにおいても、従来手法と比べて大幅なコスト削減およびプロセスの脆弱性の排除ができることを確認した。
  - 本実証では、CG 社 EDGE と HUB が持つ DIDComm メッセージングプロトコルと MQTT を組み合わせ、MFP デバイスとクラウド間での検証可能な E2EE 通信をトランスポートに依存することなく実現できることを確認した。また CG 社の EDGE と HUB を活用することで、MFP デバイスと文書管理システムのプライベートネットワークにおいても、Listening Port を露出させない仕組みにより、Port Scanning Attack などのセキュリティ脅威のリスクを低減できることを確認した。
  - CG 社 EDGE と HUB を活用することで、MFP デバイスにおいても、デバイスの高度な認証、およびポリシーによるアクセス制御が実現できることを確認した。
  - 本実証では、文書管理システムをプロトタイプとして作成し、MFP デバイスから送信される署名付き電子化文書を検証することで、監査証跡を担保する。また MFP アプリから CG 社 EDGE に MFP デバイスを操作するユーザ名などのメタデータを渡すことで、「いつ・誰が・どのデバイスから」といったデータを検証できることを確認した。
  - 本システムの成果は、MFP デバイスに限らず、リテール機器や医療機器などの IoT 機器とクラ

ウドで構成されるシステムにも同様に適用することが期待できる。

- マネタイズ手法
  - 以下の二つのマネタイズ手法を検討した。
    - MFP 本体販売時にアプリケーションのライセンスをオプションとして提供し、MFP 導入タイミングで売り切るライセンス提供モデル（図 3.5.2-1）

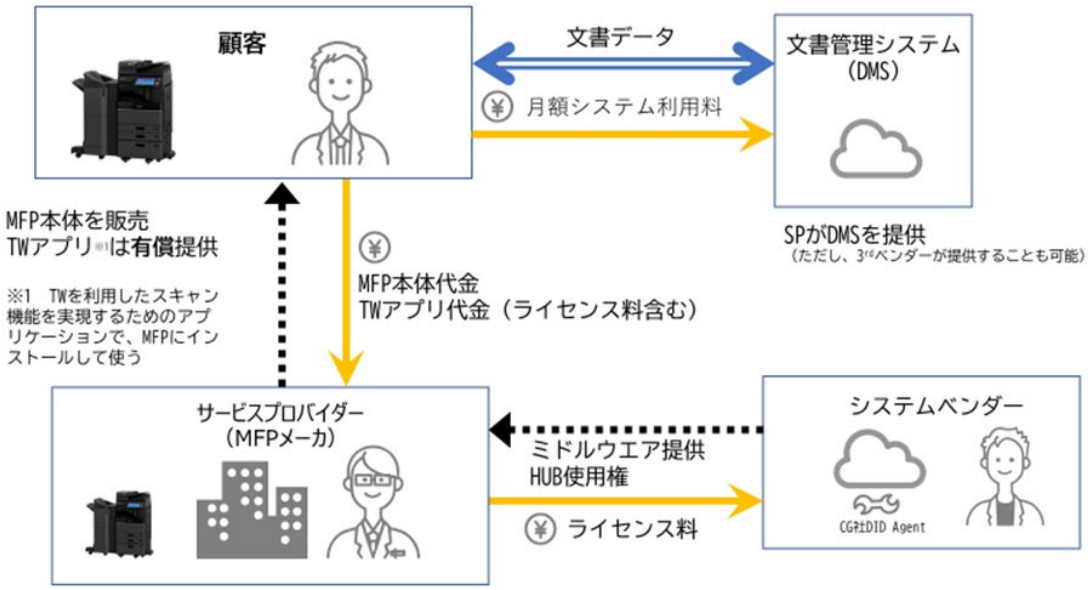


図 3.5.2-1　導入タイミングで売り切るライセンス提供モデルのビジネスモデル

    - MFP アプリケーションは標準機能として提供し、利用に応じて課金するサブスクリプションモデル（図 3.5.2-2）

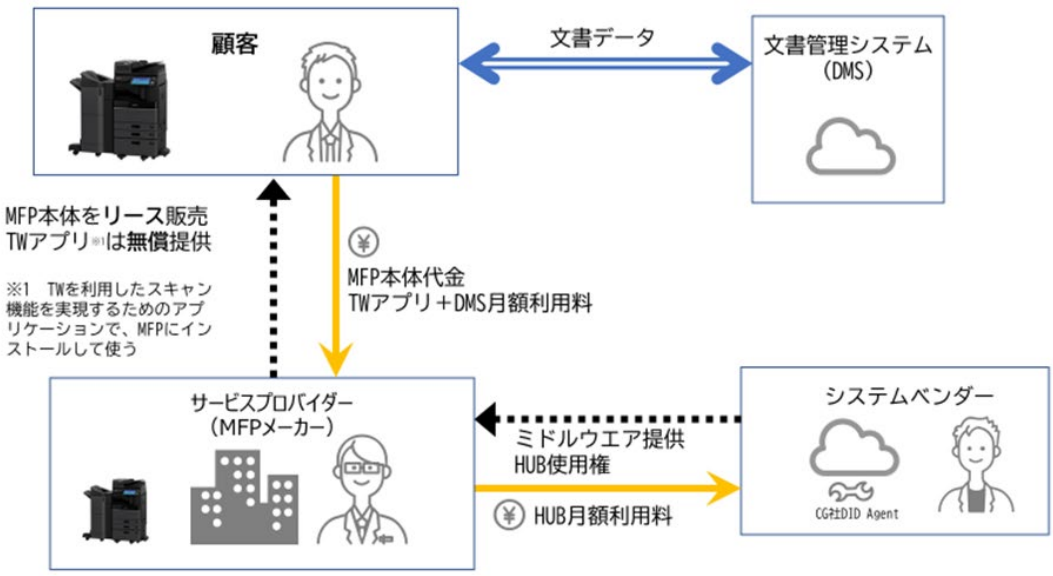


図 3.5.2-2 利用に応じて課金するサブスクリプションモデルのビジネスモデル

- 現状のオペレーションでは、システムオプション（ソフトウェア的なオプション追加機能）でユーザがライセンスを購入して機能をアクティベートすると言う提供方法を行っている。この現状オペレーションに合わせると前者のライセンスモデルのほうが現実的である。一方で、MFP アプリ、データインフラ、文書管理システムを継続的に保守・メンテしていくコストを考えると、サブスクリプションモデルのほうがビジネスモデルとして適合していると考えられる

- 今後の検討課題
  - データの保管方法は、各社によりさまざまであることから、文書管理システム（データ保管場所）と 3rd party のクラウドストレージサービス（google drive や box など）との API 連携を将来的に検討していく

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）

本実証実験で開発した範囲と既存のソフトウェアを活用した範囲を以下の図 3.6-1 に示す。図中の**青枠**が既存ソフトウェアで、**赤枠**が今回開発した部分を示している。

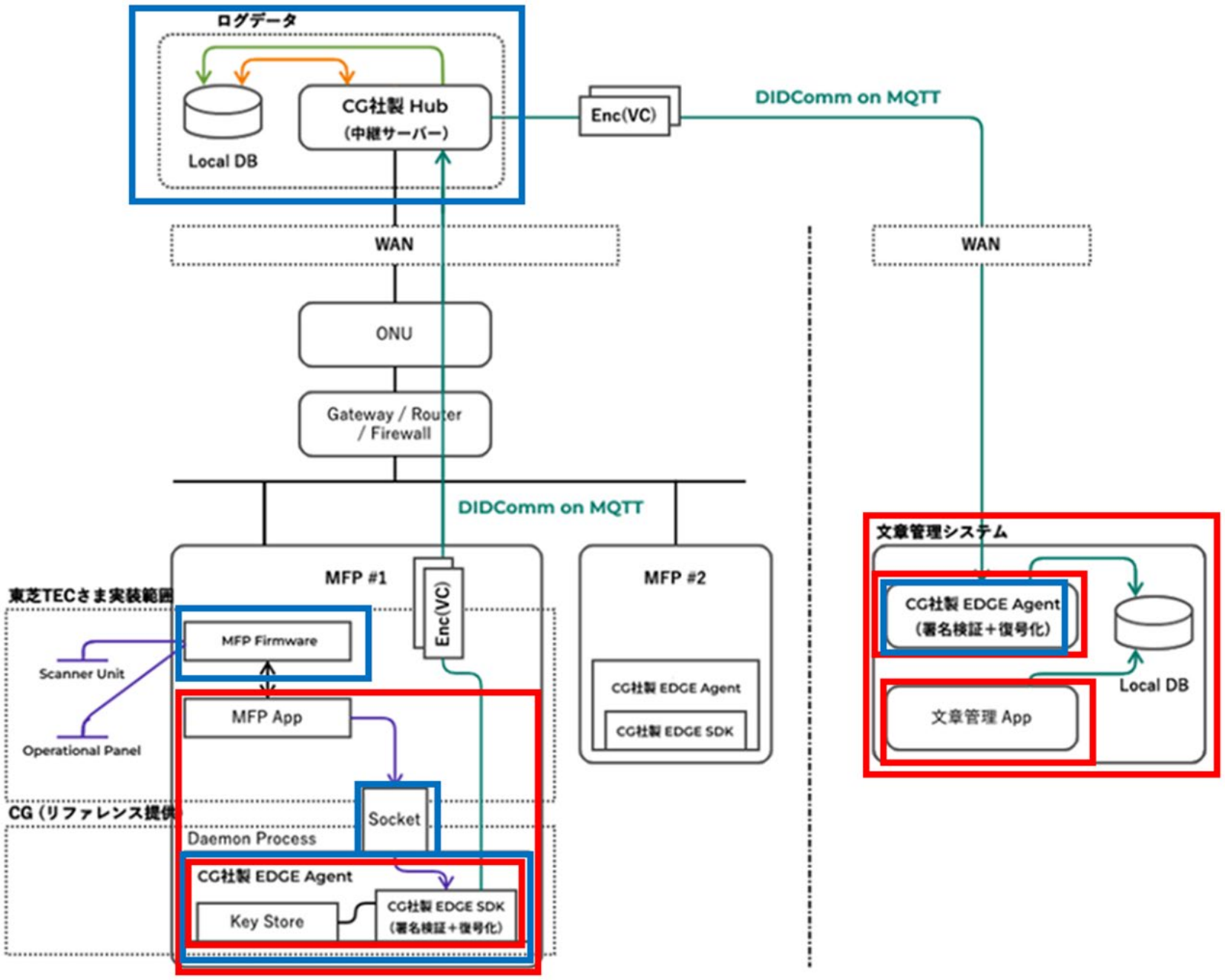


図 3.6-1 システム構成

- 今回新規開発した部分・ MFP アプリケーション（MFP App）
  - ✓ 文書管理システム
- 既存部分を活用し改変した部分
  - ✓ CG 社製 Edge
- 既存部分
  - ✓ CG 社製 HUB
  - ✓ MFP Firmware

- 有識者や政府関係者による再現
  - TTEC 社製 MFP に本実証で開発したアプリケーション（システム構成図にある MFP App）をインストールすることで、MFP でスキャンした電子化文書を文書管理システムに保存することが出るようになる
  - 文書管理システムは、文書管理システムにアカウント登録することで利用可能となる。また CG 社製「HUB」は CG 社の開発ライセンスを利用することで、アクセスすることが可能となる

（TTEC 社製 MFP を事務局に貸し出し、もしくは、弊社のオフィスまで足を運んでいただき、別途作成する再現手順書に従って再現していただくことを想定している。）

- 他社の機器との相互互換性
  - CG 社製「EDGE」はオープンソースとして公開されており、他社の機器にも組み込むことが可能である。また、CG 社製「HUB」は CG 社の開発ライセンスを利用することで、アクセスすることが可能になる
  - 以上により、他社の機器が CG 社製「EDGE」「HUB」を利用することで、機器とクラウドとの信頼できるデータ流通を実現することが可能と考える

- 他社のサービスとの相互互換性
  - CG 社製「EDGE」は W3C 国際標準規格の DID Method Syntax[1]、Verifiable Credentials Data Model[2]に準拠している。また、CG 社製「EDGE」を組み込んだデバイスで生成される Verifiable Credentials は、異なる DID Method で動作するシステムにおいても、（DID Method が W3C 国際標準規格に準拠する限りにおいて）同様に検証可能である
  - CG 社製「EDGE」が組み込まれたデバイスから、他社のクラウドサービスに署名付き電子化文書を送信する場合、他社のクラウドサービスに CG 社製「EDGE」を組み込むことで、機器とクラウドの信頼できるデータ流通を実現することが可能である
  - CG 社製「EDGE」が組み込まれたデバイスから、一度「EDGE」が組み込まれたクラウドサービスに署名付き電子化文書を送信し、そこから他社のクラウドサービスにデータを送信する場合、その他社のクラウドサービスに実装される DID Method が W3C 国際標準規格に準拠する限りにおいて、同様に検証すること可能である
  - 相互互換性を担保するという観点では、CG 社製「EDGE」の DID Method Syntax[4]、Verifiable Credential Data Model[5]の技術仕様・ソースコードが公開されることで必要十分であると考える。

[4] https://www.w3.org/TR/did-core/#method-syntax

[5] https://www.w3.org/TR/vc-data-model/

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、TTEC 社がサービサーとなり MFP を提供し、紙文書を扱っていてこれを電子データ化したい利用者に対して、MFP のオプションとして販売する。（サブスクリプション形式で月額利用料を徴収し、サブスクリプションで申し込みを行うと、MFP のアプリケーション、および HUB が利用可能となる。）これによって、MFP の利用者は、紙文書を安全に電子化し、文書管理システムにおいて電子化文書を管理することが出来るようになる。（表 4.1-1）

表 4.1-1　各ステークホルダのベネフィット及び想定している利用料

ステークホルダ	ベネフィット	負担するコスト
利用者	紙文書を安全に電子化でき、再利用することが出来るようになる	MFP アプリケーションと CG 社 HUB の月額使用料 1,000 円 文書管理システムの使用料は容量によって変動する
TTEC 社 （サービサー）	TTEC 社製 MFP を販売	システムベンダーへのライセンス料金

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
  - MQTT の最大メッセージサイズは 256 MB であるので、これよりも大きなサイズのスキャンデータを送る場合は、複数のスレッドに分割して送信することになる。DIDComm では Threading を活用して、これを実現する手段が用意されており、設計レベルでは解決が可能であることを確認している。[6]
    また MFP デバイスから電子化文書を送る場合には、DIDComm on HTTP を活用するなどの対応も考えられる。双方の実装パターンにおける実装コストや周辺コンポーネントへの影響などを検証した上で、最終的な実装方法を決定する予定。

- 課題②
  - MFP アプリのユーザインターフェイスに関して。本システムでは、送信先となる文書管理システムの DID を EDGE のアクセスプロファイルに事前設定している。そのため、ユーザは MFP アプリ画面から、DID を意識することなく「文書管理システムに保存する」操作を実行することができる。一方、市場投入後に送信先を追加する場合、HUB から EDGE のアクセスプロファイル（送信

[6] https://identity.foundation/didcomm-messaging/spec/#threading

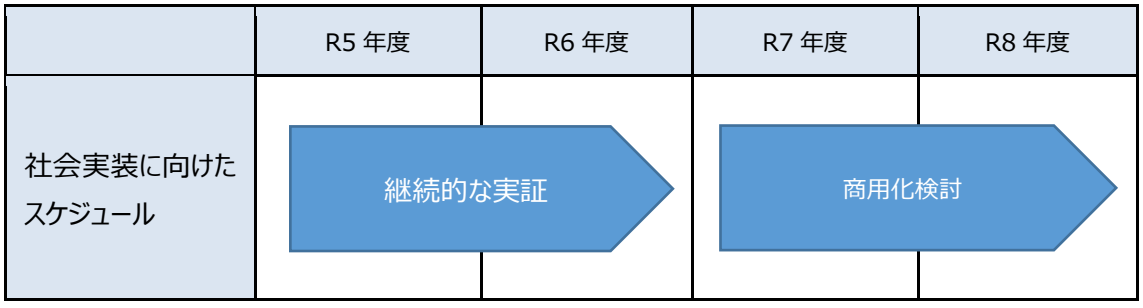
先の DID 情報）を更新することになる。本システムの実装では、複数の DID（例：did:unid:test:1234567 のような識別子）をリスト表示することになり、ユーザはそれらの DID がどのサービスに紐付いているかを判断することが困難。送信先の DID に紐付くサービス名やアイコン画像などのメタデータを含めてアクセスプロファイルを更新する方法、または MFP アプリ側でユーザがサービス（送信先）に対応する識別子を入力してセットアップする方法などが考えられる。今後、実地検証を行い、商用プロダクトのユースケースが確定した後に解決する予定。

- 課題③
  - 本実証において、MFP デバイスを操作するユーザ名や導入する設置場所（所有する法人情報）を、MFPデバイスの属性情報として扱うか、電子化文書に付随するメタデータとして扱うかで議論が分かれた。該当情報を MFP デバイスの属性情報として扱う場合、該当情報を VC の credential subject に含める。該当情報を電子化文書に付随するメタデータとして扱う場合、該当情報を DIDComm Plaintext Message の Attachments に含める。本実証における実装では、該当情報を電子化文書に付随するメタデータとして扱い、DIDComm Plaintext Message の Attachments に格納している。送信先である文書管理システムから、3rd Party のシステムあるいはローカル PC などに電子化文書（VC）が流通し、その電子化文書が「いつ・誰が・どのデバイスから」スキャンされたデータであるかを検証したい場合は、該当情報を VC に含める方が適切であると考える。この点は実地検証を通じて実際にユーザがどのように電子化文書を利用するかを確認し、現実的なシステム構成が見えたタイミングで判断していくことになると考える。

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

本ビジネスモデルの社会実装については、令和 6 年度まで継続的な実証を行い、令和 7 年度以降の商用化を想定している。

前述の課題①については、令和 5 年度に仕様の検討を行い、対応方針を決定することを予定している。前述の課題②③については、令和 5 年度に仕様検討、令和 6 年度に PoC を行い、対応方針を決定することを予定している。令和 7 年度のサービス開始当初は、ワークプレース市場への展開を想定しているが、令和 7 年度以降は、リテール事業をターゲットにマーケティングを行い、市場の拡大を目指す。



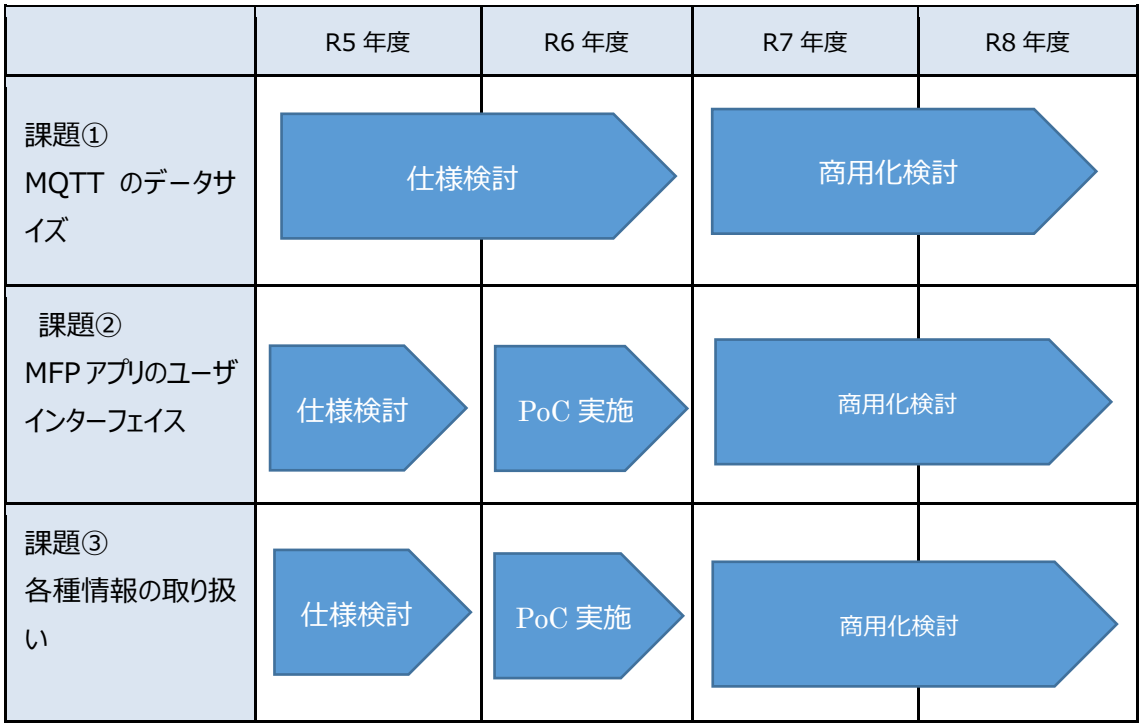


図 4.3-1　社会実装に向けたマイルストーン

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

- 自然人ではなくIoT 機器を主体とする場合、現在の Trusted Web 要件 3 ”Dynamic Consent” と要件 4”Trace 機能” をそのまま適用することが困難である。「技術」「ガバナンス」の両面でのセキュリティやプライバシー懸念に対し、達成すべき要件を具体化することで適用範囲が広がると考える。例えば、DID や署名値が Super Cookie になるプライバシーリスク（Correlation Risks）に対して、Pairwise DID やその他の技術的なアプローチについて検討することは IoT デバイスにも適応できる要件である。
- Trusted Web ホワイトペーパー全体に対する提言になるが、主体となるエンティティに自然人や法人を前提にすることや、VP Request のようにリクエスト・レスポンスモデルを前提にすることで、アーキテクチャーの適用範囲を狭めていると感じている。本ホワイトペーパーの目的は、ユースケース実装を通じて信頼できる自由なデータ流通を支えるデータ・プラットフォームレイヤーのアーキテクチャーについて検討することであるため、こうしたユースケースレベルでの前提を排除し、6 構成要素のようなプリミティブな構造設計に基づいた形で議論することが重要であると考える。
- 技術とガバナンスによってカバーされる領域を明確に分離して議論することが望ましいと考える。例えば、合意形成や合意条件の実行トレースなどは非常に重要な観点であるが、ガバナンスとして担保される領域が多いため、これらを技術要件と混合して記述すると、実装者が混乱する。要件 3 と 4 に該当する具体的な技術要件が書き出せる場合は、そのようにした方がわかりやすい（例：ノード間のトランザクションを記録して検証できるシステム、Selective Disclosure や秘密計算を活用した開示範囲の制御システムの実装など）。

5.2 その他 Trusted Web の課題と提言

- 本ユースケースでは Linux OS TPM2.0 モジュールを用いて信頼の起点となるデバイスの暗号鍵管理を実装した。暗号鍵管理は、設計・開発段階から、あらかじめ IoT 機器の公開鍵情報を安全に更新する仕組みを考慮しておかないと、市場投入後に対応することが難しく、一旦社会に実装されると回収することが困難なポイントとなる。このため、デバイスで暗号鍵ペアを安全に保護する方法、秘密鍵の回復方法、DID Document の更新・失効プロセスに関する一定のガイドライン（本件における TPM2.0 を活用した暗号鍵保護 p5 記載）を示すことが重要だと考える。
- 国際連携先の機関として、DID, VC, DIDComm などの各要素技術の仕様策定や OSS 開発を推進する DIF(Decentralized Identity Foundation)が良いのではないかと考える。
- 本実証において、MFP デバイスを操作するユーザ名や導入する設置場所（所有する法人情報）を、MFP デバイスの属性情報として扱うか、電子化文書に付随するメタデータとして扱うかで議論が分かれた。最終成果報告会のブレイクアウトセッションを通じて、MFP デバイスを（6 構成要素における）エンティティ、CG 社 EDGE を処理ノードとして分離し、MFP デバイスのアイデンティティにユーザ名や法人名などを含む構成のほうが、システム全体をうまく説明できることがわかった。IoT システ

ムを考える場合、自然人ではない IoT 機器をエンティティとし、内部に統合されるエージェントを処理ノードして整理するアプローチが有効であると考える。この場合、IoT 機器の認証機能や IoT 機器導入時の契約書（法的ガバナンス）がアイデンティティグラフを定義することになる。