

**TOSHIBA**

**令和3年度補正予算Trusted Web共同開発支援事業費  
「Trusted Webの実現に向けたユースケース実証事業」  
最終成果報告書概要版**

**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**

**代表機関名称 : 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**

**2023年3月24日**



# 目次

1. 背景・目的
2. 事業の概要
  - 2.1 事業概要及び実証の範囲
  - 2.2 社会・経済に与える価値・影響
  - 2.3 コンソーシアムの体制
  - 2.4 実証全体のスケジュール
1. 実証内容
  - 3.1 実証の実施事項、論点及び判断
  - 3.2 検証できる領域を拡大する仕組み
  - 3.3 6構成要素との対応
  - 3.4 本実証で企画・開発したシステムの概要
  - 3.5 実証を通じて得られた主な効果
  - 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）
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・ユーザーのメリット
  - 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
  - 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
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
  - 5.2 その他Trusted Webの課題と提言

# 01

背景·目的

## 1. 背景・目的

### 1.1 背景・目的

#### 背景

- a. 真正性を求められる文書を扱う企業の経理部門や官公庁などの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おり、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。
- b. 真正性が求められる文書を電子化し、その真正性を簡単に検証できるデータ流通システムが存在しない。
- c. この課題を従来のウェブの仕組みで解決する場合、デジタル複合機メーカーは、複合機の機体毎の暗号鍵管理、数十万台におよぶ機体のプロビジョニング、トランスポートごとのセキュリティ対応などの複雑なデータインフラ構築やコストの課題に直面する

#### 目的

本実証事業では、デジタル複合機と検証可能な電子化文書の流通システムをTrusted Web のアーキテクチャーを使って構築することで、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とともに、電子化文書の流通に貢献する。

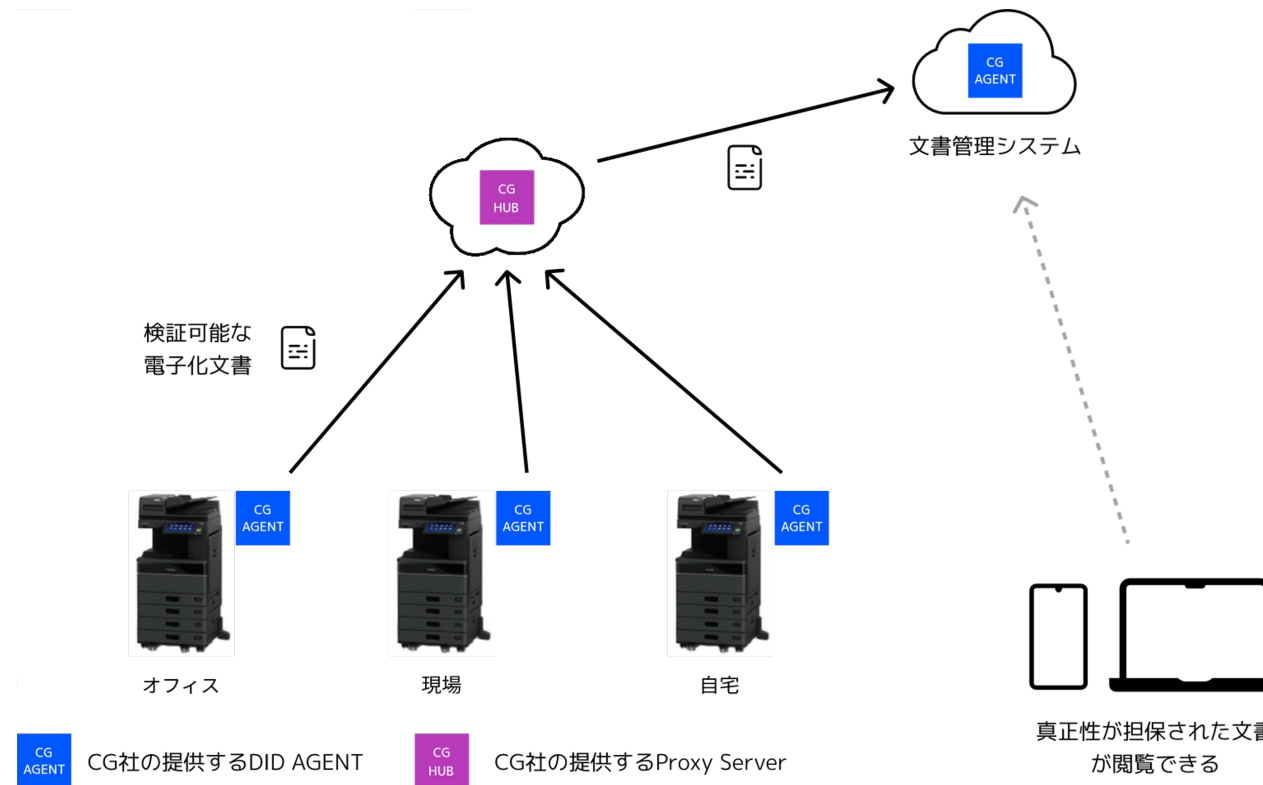
# 02

## 実証の概要

## 2. 事業の概要

### 2.1 実証概要及び実証の範囲

本実証事業では、分散型ID技術であるCollaboGate Japan 株式会社（以下、CG社）のE2Eセキュリティソリューションを活用し、東芝テック（以下TTEC）のデジタル複合機（MFP）でスキャンした画像データを、CG社製HUBを通じて検証可能な電子文書として文書管理システムに保存。分散型IDを活用することによって、監査証跡の必要な文書業務のデジタル化を推進するために、Trusted Webの要件を満たしたサービス提供の実現を検証する。



## 2. 事業の概要

### 2.2 社会・経済に与える価値・影響

- 本件の取り組みは、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

#### 市場規模I（独自試算）

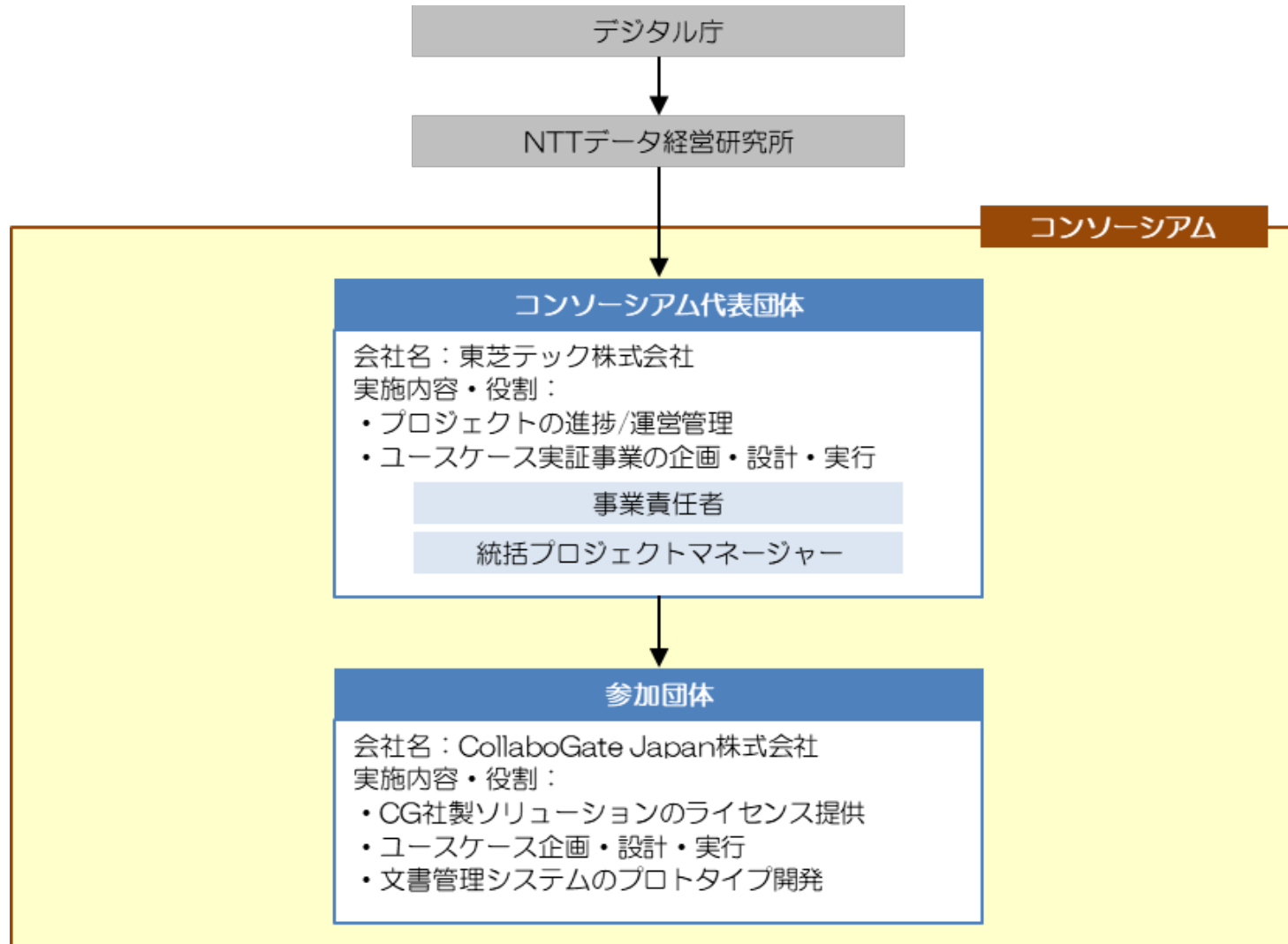
- 国内メーカーのMFPにおける世界市場規模は、2021年の統計で6,490億円（前年比99.1%）、年間出荷台数は359万台である
- ペーパーレス化に伴い緩やかな市場縮小傾向にあるなか、主要国内メーカーは業務ワークフロー効率化を支援するトータル・ソリューションへと競争軸をシフトしている
- 文書管理に特に高い真正性が求められる防衛省関係、金融・保険、会計事務所、行政機関の4つのセグメントの合計で、**120万台**の導入余地、**2400億円程度**の市場規模が見込まれる。
  - ✓ 日米で約53,000社が防衛省と直接取引、各社平均2事業所、平均20台のMFP設置を仮定し、53万台の導入余地
  - ✓ 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以上あり、平均20台のMFP設置を仮定し、10万台の導入余地

#### サービス提供者のコストI（独自試算）

- 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の削減が見込まれる
  - ✓ 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人月の人件費が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

## 2. 事業の概要

### 2.2 コンソーシアムの体制





## 2. 事業の概要

### 2.4 実証全体のスケジュール

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				[Progress bar from Sep to Dec]						
	要件定義	TTEC	9/9-11/21	[Progress bar from Sep to Nov]						
	基本設計	TTEC,CG	10/19-11/30	[Progress bar from Oct to Dec]						
MFPへのCG EDGE組み込み				[Progress bar from Nov to Jan]						
	開発ボード送付	TTEC	10/26	[Progress bar in Oct]						
	カスタマイズ	TTEC,CG	10/31-12/13	[Progress bar from Nov to Dec]						
	組み込み	TTEC	12/13-1/13	[Progress bar from Dec to Jan]						
文書管理システム開発				[Progress bar from Nov to Jan]						
	プログラミング	CG	10/31-12/14	[Progress bar from Nov to Dec]						
	単体試験	CG	12/15-1/13	[Progress bar from Dec to Jan]						
スキャンアプリ開発				[Progress bar from Nov to Feb]						
	プログラミング	TTEC	10/31-12/21	[Progress bar from Nov to Dec]						
	単体試験	TTEC	12/21-1/13	[Progress bar from Dec to Jan]						
	結合試験	TTEC,CG	1/16-2/9	[Progress bar from Jan to Feb]						
デモ動画の制作				[Progress bar from Jan to Mar]						
	シナリオの作成	TTEC,CG	1/16-2/9	[Progress bar from Jan to Feb]						
	動画撮影	TTEC,CG	2/13-3/9	[Progress bar from Feb to Mar]						
報告書の作成・納品物準備				[Progress bar from Nov to Mar]						
	中間報告書作成	TTEC,CG	11/10-12/7	[Progress bar from Nov to Dec]						
	最終報告書作成	TTEC,CG	1/16-3/24	[Progress bar from Jan to Mar]						

# 03

## 実証内容

### 3. 実証内容

## 3.1 実証の実施事項、論点及び判断 (1/3)

プロトタイプシステムの企画・開発		
実施事項	論点	判断
要件定義	デバイスのルートオブトラスト確立 (暗号鍵管理)	CG社のEDGEとTTEC社のMFPデバイスに搭載されるTPM2.0機能を組み合わせ、ルートオブトラストを確立。
	プロビジョニングの自動化	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を行い、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を排除できることを確認。
	IoT向けの軽量メッセージングプロトコル	CG社EDGEのDIDCommメッセージングプロトコルとMQTTを活用し、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く検証可能なE2EE通信できることを確認。
	デバイスの高度な認証・認可	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。
	検証可能なデータ流通	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、「いつ・誰が・どのデバイスから」生成されたデータであるかを確認。
	他IoT機器への拡張性	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可能なめ、できる限り他IoT機器への拡張性を担保した設計と実装を目指す。
基本設計	MFPアプリケーション	スキャン機能は既存のMFPシステムソフトの機能をベースに実装する
	CG社EDGEと、MFPアプリとTPM2.0の統合	MFPアプリはCG社EDGEのAPIを呼び出すことで、DID Commに基づいた文書転送を行う。CG社EDGEからMFPシステムソフトのライブラリを組み込んでMFPのTPM2.0へアクセスする。
	文書管理システム	文書管理システムは、CG社Edgeを組み込むことで、DID Commに基づいた文書転送を行う。DIDやメタデータを表示することで、電子化文書の属性を確認できるようにする。
ユーザテスト	未実施	

### 3. 実証内容

## 3.1 実証の実施事項、論点及び判断（2/3）

### ヒアリングの実施

ヒアリングの目的	対象	ヒアリング結果
行政文書の電子化の現状と課題についてヒアリング	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
		自治体には「文書保管室」があり、大量の行政文書を紙ベースで管理している。5年単位で文書を破棄するなど非生産的な業務が多い。
		一つの支庁の課（15人前後）にMFPが一台設置されている。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あり。
紙文書のデジタル化ニーズ、監査証跡担保ニーズについてヒアリング	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よい。

### 3. 実証内容

## 3.1 実証の実施事項、論点及び判断 (3/3)

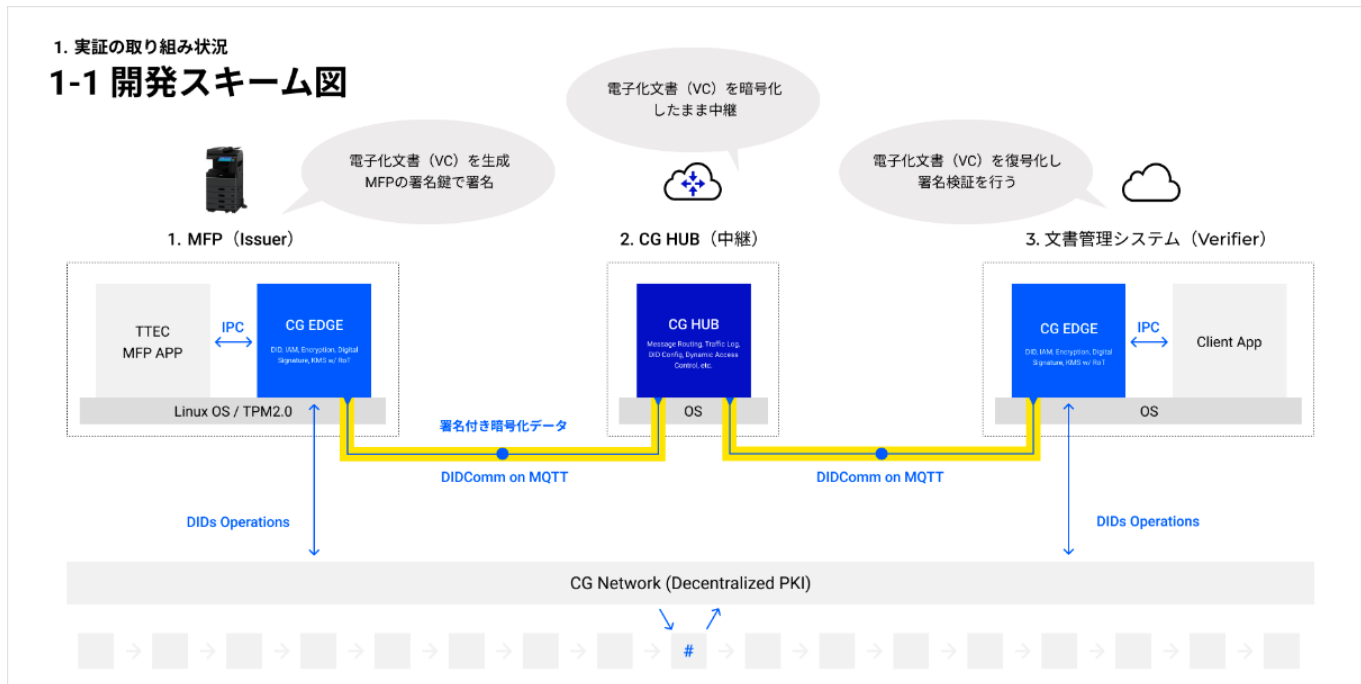
### 国際標準規格の調査

調査事項	調査対象機関	調査結果
DID/VC/DIDCommに関する標準化機関を対象に技術仕様について調査を実施	W3C	Decentralized Identifier, Verifiable Credential Data Model
	DIF	DIDComm v2

### 3. 実証内容

## 3.2 検証できる領域を拡大する仕組み (1/3)

### データスキーム図



### データへのアクセス

- 本システムでは、MFPでVCを生成し文書管理システムに送信
- 文書管理システムでVCを管理
- 文書管理システムにはユーザー名とパスワードで認証・認可を行う

### 登場する主体とその概要

主体	役割・設定
MFPデバイス	TTEC社製デジタル複合機 (e-STUDIOシリーズ)。MFPに統合されるCG社製EDGEで分散型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。
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、どのデバイスから」スキャンしたデータであるかを確認し、これをシステムのデータベースに登録する。
CG 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、ポリシ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。
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. 実証内容

## 3.2 検証できる領域を拡大する仕組み（2/3）

### 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

要検証の課題	検証対象	検証方法	検証者	保有者	発行者	データの置き場	アクセスコントロールの手法	成果・留意点
監査証跡の担保	電子化文書の作成元	電子化文書（VC）の署名検証	文書管理システム	-	MFPデバイス	文書管理システム	文書管理システムの認証機能を利用して関係者のみがアクセスできるように制御	いつ・誰が・どのデバイスからスキャンしたデータであるかを確認できた。

### 3. 実証内容

## 3.2 検証できる領域を拡大する仕組み（3/3）

### 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

合意の主体	合意の対象	合意の条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
導入法人とサービス提供者	MFPデバイスでスキャンした電子化文書の取り扱い	MFP導入時に契約書という形で電子化文書の取り扱いについて合意形成を行う。	履行された左記の合意	導入法人の管理者	文書管理システムおよびCG HUBのトラフィックログをサービス提供者に問い合わせることで確認できる。	可能



### 3. 実証内容

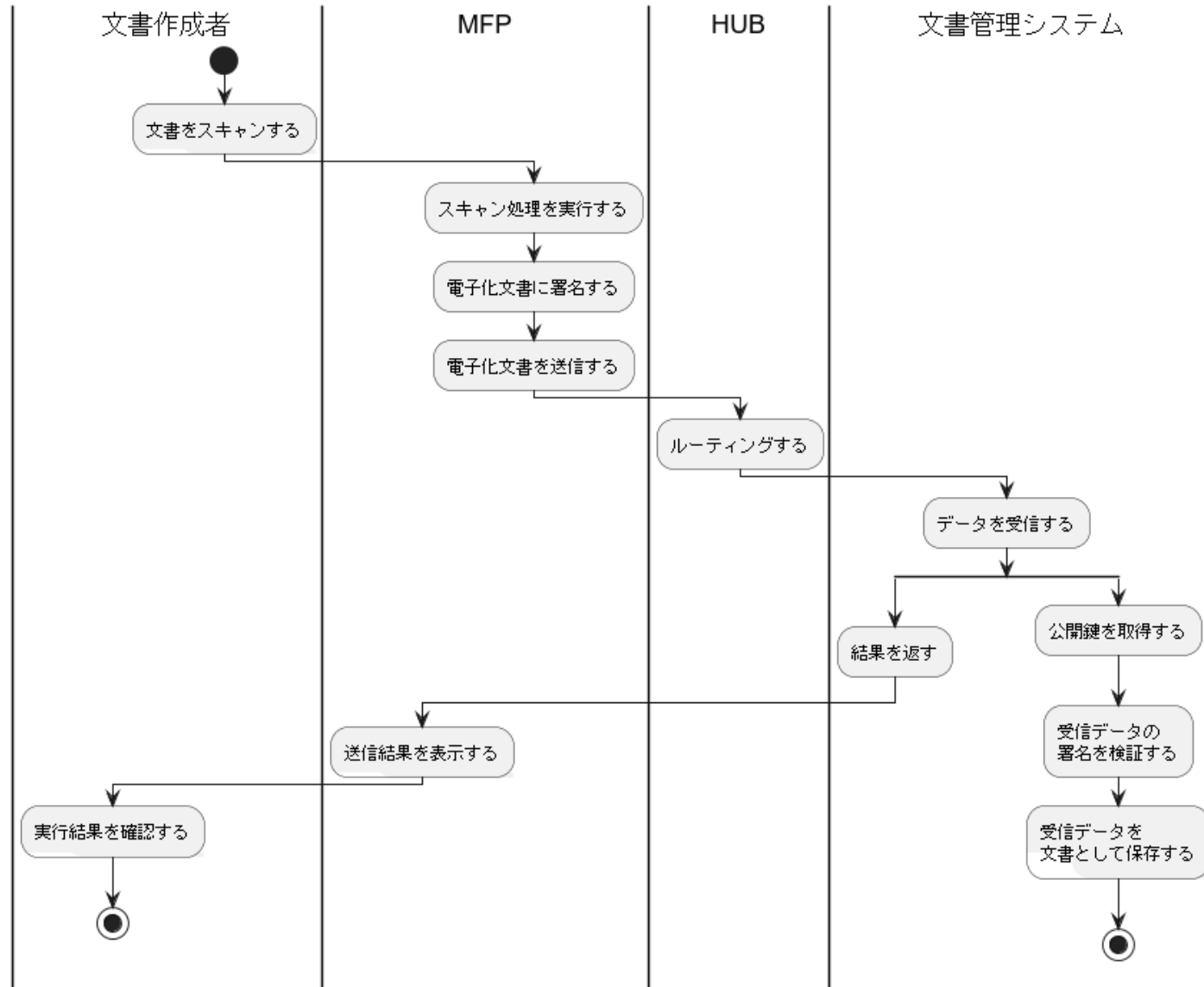
## 3.3 6構成要素との対応

6構成要素	6構成要素との当てはめ	
検証可能なデータ	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、ユーザー名など）、MFPデバイスでスキャンした電子化文書
	署名者	MFPデバイス（統合されたCG社EDGE）
アイデンティティ	アイデンティティとして想定されるものは何か	MFPデバイスと文書管理システム
	アイデンティティ管理システム（外部）は何を利用しているか（例：OIDC for VC, DID）	MFPデバイスとCG社HUBとのDIDに基づく公開鍵認証、文書管理システムのユーザー認証（ユーザー名とパスワードによる認証）
	アイデンティティグラフとして想定されるのはなにか	MFPデバイスとサービス提供者（シリアル番号）、導入企業（設置場所）、ユーザー名（MFP利用者）とのグラフ。文書管理システムとサービス提供者、導入企業、システム利用者（ログイン情報）とのグラフ。
ノード	Walletか否か	MFPデバイスと文書管理システムに統合されたCG社EGDEとCG社HUBがVCを処理するノードになる（いずれもWalletではないと判断）。
	合意形成がされているか、されているならその手段	MFPデバイスに統合されたCG社EDGEが宛先を指定、宛先以外は復号することができないVCを送信する。
	データのやりとりをどこに記録するか	CG社HUBにトラフィックの送信元と宛先のDID、時間などのトラフィックログを記録して保管。
メッセージ	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	メッセージオリエンテッド
トランザクション	データのやり取りを記録するか	CG社HUBにトラフィックの送信元と宛先のDIDや時間などのトラフィックログ、デバイスのアクセスプロファイル変更ログを保管。電子化文書の監査証跡は文書管理システムで確認できる。
	データのやり取りの検証はできるか	CG社HUBを運用するサービス提供者に問い合わせることで、トラフィックログを確認できる。電子化文書の監査証跡は、発行者に都度直接参照することなく検証できる。
トランスポート	トランスポートのプロトコルは何か	DIDComm on MQTT

### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (1/6)

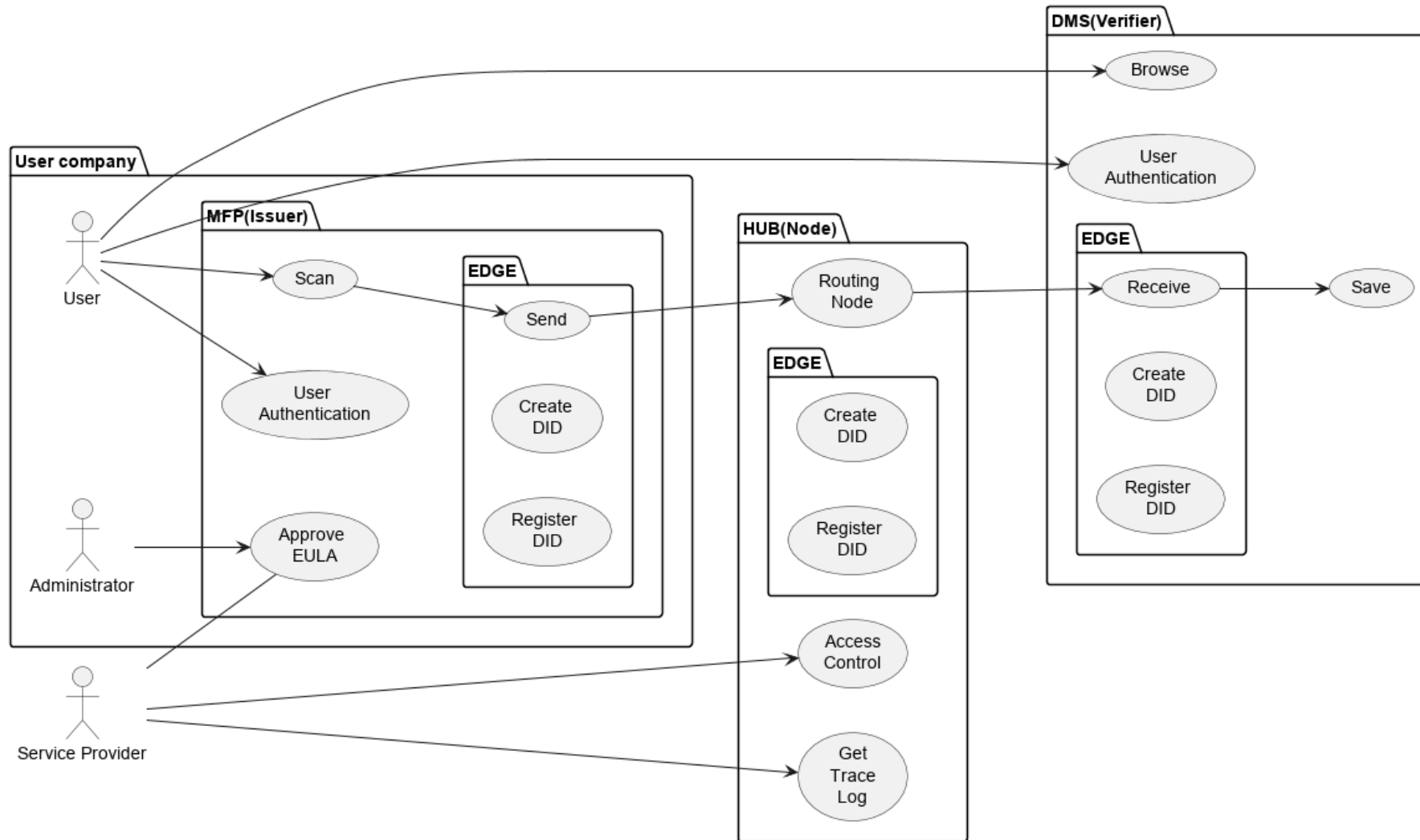
### 業務フロー



### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (2/6)

### ユースケース図

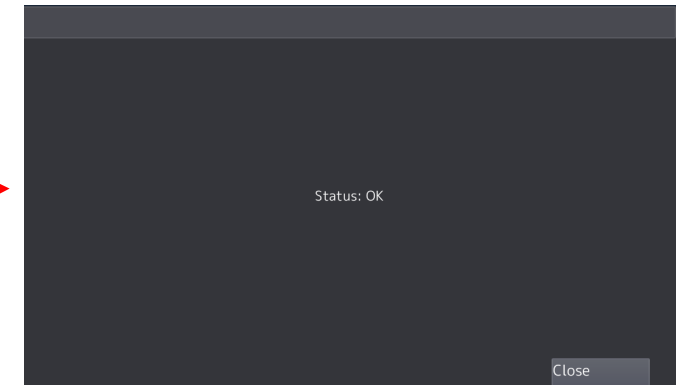
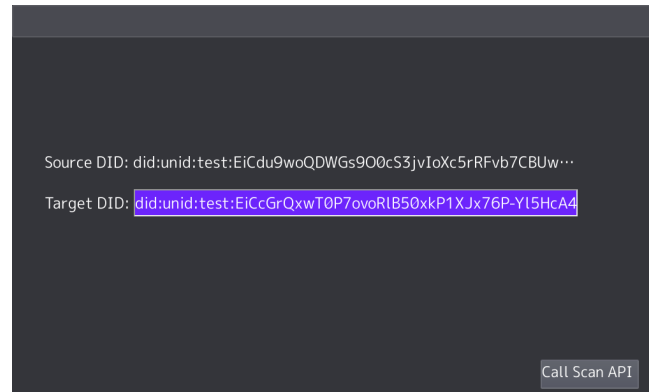
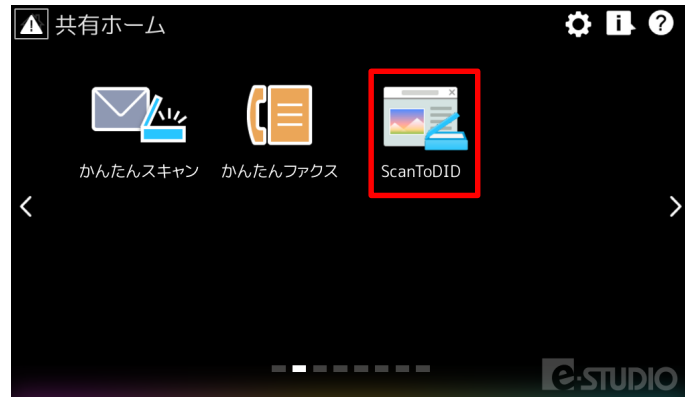


### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (3/6)

### 操作画面 (MFP 操作パネル)

#### MFP



### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (3/6)

### 操作画面 (文書管理システム)

The image displays three screenshots of a document management system. The first screenshot shows a login page with a scenic background image of a river and mountains. It includes a 'ログイン' (Login) button and input fields for 'メールアドレス' (Email address) and 'パスワード' (Password). The second screenshot shows the main dashboard with a '文書管理システム' header, a 'ログアウト' button, and a table of documents. The third screenshot shows a detailed view of a document, including a '検証ステータス' (Verification status) section with a green checkmark and a 'スキャンデータ' (Scan data) section displaying a scanned invoice.

**ログイン画面**

ログイン  
メールアドレス  
admin@example.com  
パスワード  
.....  
ログイン

**文書管理システム**

ログアウト

文書管理 > 文書管理  
スキャンされたデータを番積・データに紐づくメタデータを確認することができます。

文書 ID	設置場所	ファイル名	スキャン日時
<input type="checkbox"/> cle86rsgv00003zossyzlgdac	10fs/r	DOC230217160409-MFP14193307.pdf	2023年02月17日 16:04:23
<input type="checkbox"/> cle86g7sr00003z9tu8ipz5qs	10fs/r	DOC230217155445-MFP14193307.pdf	2023年02月17日 15:55:33
<input type="checkbox"/> cle73xw6e00003z9neo2jmbfg	1b3f nwチーム	DOC230216215640-MFP13970461.pdf	2023年02月17日 14:56:52
<input type="checkbox"/> cle6yfus600003z13k2giqgwy	1b3f nwチーム	DOC230216192155-MFP13970461.pdf	2023年02月17日 12:22:19
<input type="checkbox"/> cle6y4aoz00003zo40g7azq20	1b3f nwチーム	DOC230216191306-MFP13970461.pdf	2023年02月17日 12:13:21
<input type="checkbox"/> cle5dgo1y00003z1q5lvvgtj9	1b3f nwチーム	DOC230215164830-MFP13970461.pdf	2023年02月16日 09:48:47

**文書管理システム**

ログアウト

文書管理 > cle86rsgv00003zossyzlgdac

**文書詳細**  
スキャンされたデータに紐づくメタデータとスキャンデータを確認することができます。

**検証ステータス**

この文書は 2023年02月17日 16:04:23 に「10fs/r」が所有する MFP デバイス (did:unid:test:EiDmrczZhf2BTWAUPByUDMg\_tf5Z7AOD1OoxE8SFevhteg) で test がスキャンしました。

**スキャンデータ**

**請求書**

年 月 日

様 (会社名)

〒 (住所)

下記のとおりご請求いたします。

(振込先)  
〇〇銀行 〇〇支店  
種別: 普通  
口座番号: 1234567  
口座名義: 〇〇株式会社

TEL.  
FAX.

御請求金額 ¥32,400- (消費税込み)

品名	数量	単価	金額	備考
洗面台ハイソ付機	1	21,000	21,000	マシン1台

### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (4/6)

機能/非機能一覧		
機能/非機能	機能名	機能概要
機能	Scan	紙をスキャンして電子化文書を作成する
機能	Send	電子化文書を宛先DIDのストレージに送信する
機能	Routing	対象のDIDを持つデバイスへの通信をルーティングする
機能	Receive	自DIDに送付された電子化文書を受信する
機能	Save	受信した電子化文書を保存する
機能	Browse	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	DID Documentを作成する
機能	Register DID	DID DocumentをDPKIに登録する
機能	Access Control (HUB)	アクセスポリシーを変更し、認可しないデバイスからのアクセスを禁止する。
機能	Get Trace Log	合意形成の条件に関するログを取得する
非機能	Access Control (DMS)	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にアクセス制御を行う
非機能	Remote Operation	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

### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (5/6)

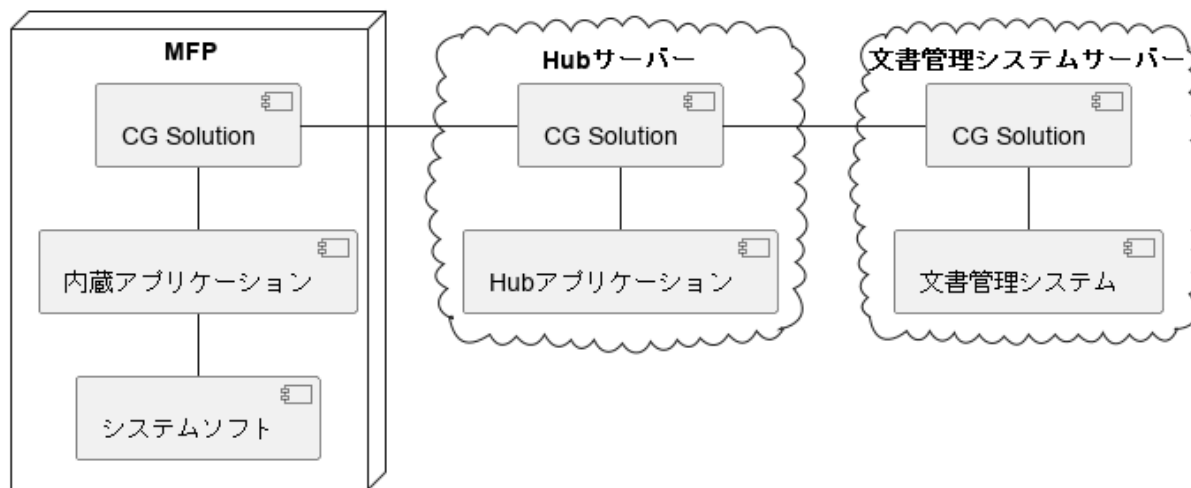
### データモデル定義

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
ユーザー名	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
送信先	MFPデバイス	recipients.header.kid

### 3. 実証内容

## 3.4 本実証で企画・開発したシステムの概要 (6/6)

### 実験環境



### システムの構成要素

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	-	-	-	
内蔵アプリケーション	-	-	-	
CG社EDGE	V1.0.0	OSS	Apatch2.0	DID, VC
CG社HUB	V1.0.0	-		DID, VC, DIDComm
文書管理システム	prototype	-	-	DID, VC



### 3. 実証内容

## 3.5 実証を通じて得られた主な成果

### システムの企画・開発に関する成果

- **デバイスの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**
  - 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とHUBでは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する。本プロトタイプでは、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、これまでのサービス提供者あるいは利用者が負担していたコストを軽減できることを確認できた。
- **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、簡単に紙文書のデジタル管理ができることを確認した。

### ビジネスモデルに関する成果

- **特定業務における紙業務のデジタル化ニーズを確認**
  - 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した。
- **マネタイズ手法の検討**
  - ①MFP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、②MFP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の二つのマネタイズ手法を検討した。
- **データインフラの構築コストの削減**
  - CG社EDGEとHUBを利用することで、データインフラ構築、プロビジョニング、インフラ運用に関するコストを削減できることを確認した。
- **より安全で信頼可能なデータ流通**
  - CG社EDGEとHUBを利用することで、デバイスのRoTの確立、なりすましやポートスキャン攻撃からの保護、データの真正性を担保した双方向でのデータ流通など、IoTセキュリティに関する国際標準規格に求められるセキュリティ機能要件を満たしながら、検証可能な電子化文書の流通ができることを確認した。
- **多様なデバイスへの応用**
  - CG社EDGEとHUBは、MFPだけではなく、オフィス機器やリテール機器など、異なる産業や用途のIoTデバイスにも適応することができる。

### 3. 実証内容

## 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

### ● 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できるようになる。

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。

### ● 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。

### ● 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<sup>[1]</sup>、Verifiable Credentials Data Model<sup>[2]</sup>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。

また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。

[1] DID Method Syntax: <https://www.w3.org/TR/did-core/#method-syntax>

[2] Verifiable Credentials Data Model: <https://www.w3.org/TR/vc-data-model/>

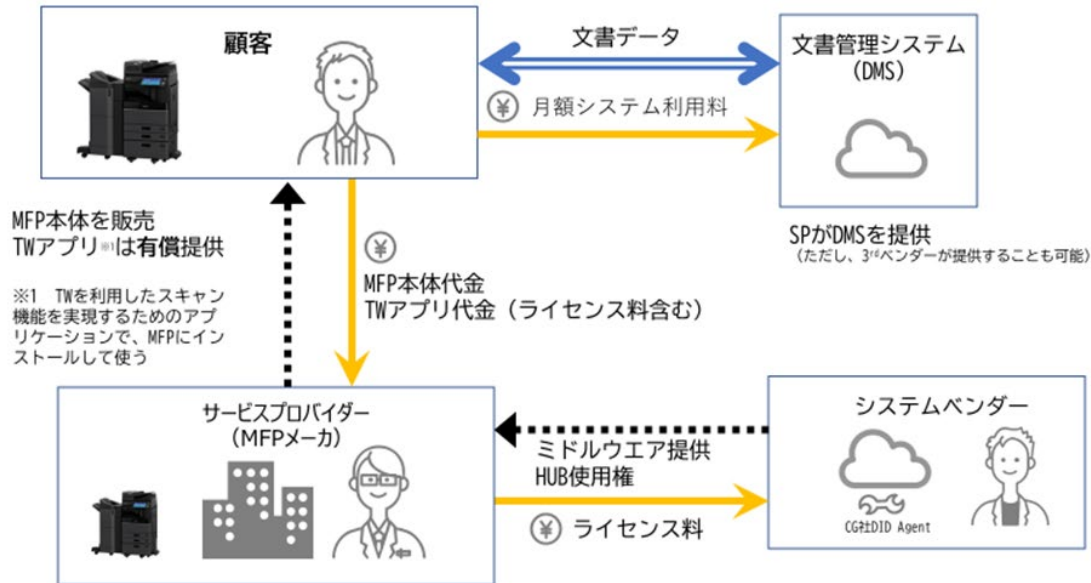
# 04

**実証終了後の社会実装に向けた見通し**

## 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・ユーザーのメリット

#### ビジネスモデル



#### ユーザーのベネフィット

ステークホルダ	ベネフィット	負担するコスト
サービスプロバイダー (MFPデバイス+文書管理システム)	<ul style="list-style-type: none"> <li>①文書管理ソリューションを顧客に提供し、MFP本体代金に加えてソリューション提供によるマネタイズが期待できる。</li> <li>②TWデータ流通インフラを多様なデバイスで容易に構築・運用できる。</li> </ul>	システムベンダーへのライセンス料金
顧客	<ul style="list-style-type: none"> <li>①紙業務のデジタル管理に係る煩雑な手続きの簡略化</li> <li>②従業員の生産性を高め、バックオフィス業務の負担を軽減する。</li> </ul>	MFP本体代金 + TWアプリ代金
システムベンダー	CG社EGDEとHUBなどのデータインフラをSaaSモデルで提供する。	

## 4. 実証終了後の社会実装に向けた見直し

### 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 通信プロトコル（MQTTのメッセージサイズ）

- 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、あるいはHTTPを活用するなどの対応が考えられる。
- 実証終了後に、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アプリのユーザーインターフェイス

- 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、ユーザーは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。
- 市場投入後にMFPデバイスに送信先を追加する場合、CG社HUBからEDGEのアクセスプロファイル（送信先のDID情報）を更新することになるが、複数のDIDをリスト表示しても、ユーザーはそれらの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アプリ側でユーザーがサービス（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 MFPデバイスの属性情報の定義

- MFPデバイス进行操作するユーザー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。
- 実施検証を通じて、電子化文書（VC）の流通範囲や、署名検証で得たい検証範囲をより具体的に特定することで、該当情報をどちらに含めるのか判断する予定。

#### 4. 実証終了後の社会実装に向けた見通し

### 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年度以降に商用化検討を実施、R8年度以降に商用化を想定
- 課題①については、令和5年度と令和6年度に仕様検討を行い、令和7年度以降に商用化検討を実施することを予定
- 課題② ③については、令和5年度に仕様検討を行い、令和6年度にPoCを実施、令和7年度以降に商用化検討を実施
- 弊社はMFP事業以外にも様々な事業を展開しており、様々なデータ、商材、ソリューションでTrusted Webの成果を活用を目指していく

	R5年度	R6年度	R7年度	R8年度
社会実装に向けたスケジュール	継続的な実証		商用化検討	
課題① 通信プロトコル (MQTTのデータサイズ)	仕様検討		商用化検討	
課題② MFPアプリのユーザーインターフェイス	仕様検討	PoC実施	商用化検討	
課題③ MFPデバイスの属性情報の定義	仕様検討	PoC実施	商用化検討	

# 05

## Trusted Webに関する考察

## 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ます。
- 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. Trusted Webに関する考察

### 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デバイス进行操作するユーザー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ー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、内部に統合されるエージェントを処理ノードとして整理するアプローチが有効であると考え。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。

# THANK YOU

