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」

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

要件定義書

2023年3月20日

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

Copyright©2023 Toshiba Tec Corporation, All Rights Reserved.

Copyright©2023 CollaboGate Japan, Inc., All Rights Reserved.

目次

[1. 概要 4](#_Toc120518392)

[1.1. 目的 4](#_Toc120518393)

[1.2. 実証項目 4](#_Toc120518394)

[1.3. システム構成 5](#_Toc120518395)

[1.4. 用語集 6](#_Toc120518396)

[2. ユースケース 7](#_Toc120518397)

[2.1. Scan 7](#_Toc120518398)

[2.2. Send 7](#_Toc120518399)

[2.3. Routing 8](#_Toc120518400)

[2.4. Receive 8](#_Toc120518401)

[2.5. Save 8](#_Toc120518402)

[2.6. Browse 9](#_Toc120518403)

[2.7. Create DID 9](#_Toc120518404)

[2.8. Register DID 9](#_Toc120518405)

[2.10. Access Control 10](#_Toc120518406)

[2.11. Request Log 10](#_Toc120518407)

[2.12. Get Trace Log 11](#_Toc120518408)

[3. 機能要件 12](#_Toc120518409)

[3.1. MFP機能要件 12](#_Toc120518410)

[3.1.1. スキャン機能 12](#_Toc120518411)

[3.1.2. データ送信機能 12](#_Toc120518412)

[3.3.3 DID作成機能 12](#_Toc120518413)

[3.2. CG社製HUB機能要件 12](#_Toc120518414)

[3.3. 文書管理システム機能要件 13](#_Toc120518415)

[3.3.1. データ受信機能 13](#_Toc120518416)

[3.3.2. DID作成機能 13](#_Toc120518417)

[3.3.3. ファイル閲覧機能 13](#_Toc120518418)

[3.3.4. その他 14](#_Toc120518419)

[4. 非機能要件 15](#_Toc120518420)

# 概要

## 目的

Trusted Web の実現に向けたユースケース実証事業として、分散型ID技術であるE2Eセキュリティソリューションを活用し、デジタル複合機でスキャンする電子化文書の真正性を担保、改ざん検証可能なシステム構築を行う。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、導入企業のパフォーマンス向上と効率的な業務運用を実現するサービス提供を目指す。

## 実証項目

本システムを用いて、下記の項目を実証する。

A：特定のサービスに依存せず、デジタル複合機やクラウドサーバーがDIDsを発行し、DIDsに紐づく検証可能なデータを生成する。[Identifier 管理機能]

B：デジタル複合機の暗号鍵生成にはデバイス由来の真性乱数を活用し、生成した秘密鍵はTPM2.0のセキュア領域で保管することで、信頼のルートを保護する。[Identifier 管理機能]

C：デジタル複合機が生成する検証可能なデータを、生成者に都度直接参照することなく、検証可能な仕組みを構築する。[Trustable Communication 機能]

D：DIDsを持つデバイス（デジタル複合機、クラウドストレージ、社内サーバーなど）は、その経路や通信プロトコルに依存することなく、E2Eに検証可能なデータを交換できる仕組みを構築する。[Trustable Communication 機能]

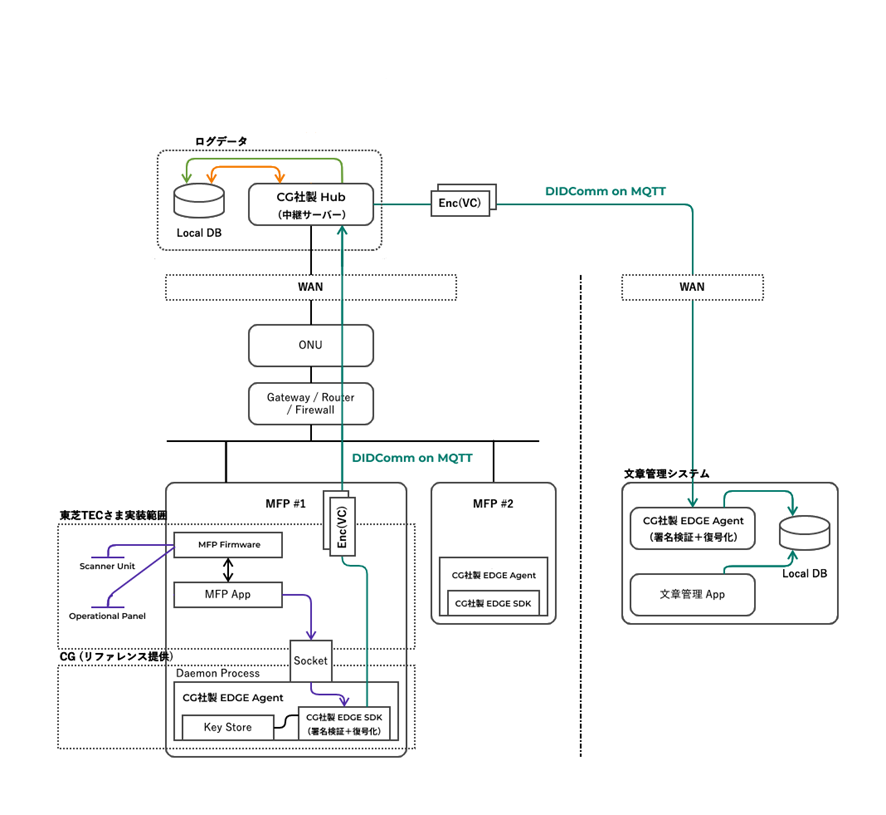
E：デバイス間のデータ通信をルーティングするコントロールプレーンは、やり取りするデータの中身を知ることができない。[Trustable Communication 機能]

F：コントロールプレーンは、接続するエッジデバイスの属性情報に基づくアクセス制御を行う。[Dynamic Consent 機能（認可しないデバイスの接続をブロックできる）]

G：コントロールプレーンの管理者は、エッジデバイスのアクセスプロファイルを管理できる。[Dynamic Consent 機能（管理者はデバイスの通信相手のLocator（DIDs）を追加できる。任意のDIDsのみが復号できる暗号化通信が可能になる。）]

H：コントロールプレーンにて、トラフィックとプロファイル変更ログを確認することができる [Trace機能]

## システム構成



プロトタイプシステム概要図の各コンポーネントの説明

● MFP：e-STUDIOシリーズ

● MFP App： MFPの内蔵アプリケーション

● Socket：Unix Domain Socket

● CG社製 Edge：DIDの生成や暗号鍵管理を行うRustライブラリ/ミドルウェア

● CG社製 Hub：コントロールプレーン

● 文書管理システム(Document Management System, DMS)：クラウドストレージや社内ファイルサーバーのこと

● Enc(VC)：署名付き電子化文書を暗号化したデータのこと

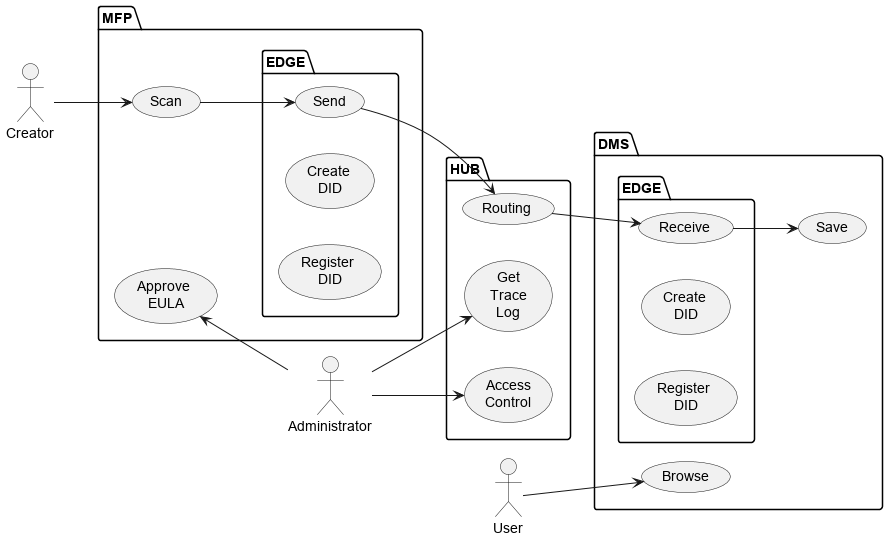
● DIDComm：DID間のE2Eメッセージングプロトコルのこと

## 用語集

|  |  |
| --- | --- |
| 用語 | 意味 |
| Trusted Web | インターネットを使ったデータのやり取りの信頼性を高めるための仕組み。​分散型でデータのやり取りの信頼性を高める。​  下記の機能を備える。  -Identifier管理機能　　​  -Trustable Communication機能​  -Dynamic Consent機能​  -Trace機能 |
| MFP | Multifunction Peripheral. コピー、スキャナ、プリンタなどの機能を搭載したデジタル複合機のこと |
| DID(s) | Decentralized IDentifier(s). 分散型識別子。  一元化された登録機関を必要とせず、多くの場合、暗号で生成または登録される、グローバルに一意の永続識別子  例: did:example:123456789abcdefghi |
| DID Document | DIDにリンクされた情報で、公開鍵などが記載されている。  例:  {  "id": "did:example:123456789abcdefghi",  "authentication": [{  "id": "did:example:123456789abcdefghi#keys-1",  "type": "Ed25519VerificationKey2018",  "controller": "did:example:123456789abcdefghi",  "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"  }]  } |

# 2. ユースケース

本システムのユースケース図は以下の通りである



## 2.1. Scan

|  |  |
| --- | --- |
| 目的 | 電子化文書を作成する |
| アクター | 文書作成者 |
| 事前条件 | 文書作成者は原稿を用意している |
| 主シナリオ | 1. 文書作成者はMFPに原稿をセットする 2. 文書作成者はスキャン実行ボタンを押下する 3. MFPは電子化文書を作成する |
| 事後条件 | 原稿を電子化した文書が作成される |
| 関連情報 | - |

## 2.2. Send

|  |  |
| --- | --- |
| 目的 | 電子化文書を宛先のDIDへ送信する |
| アクター | - |
| 事前条件 | 電子化文書が作成されている  宛先のDIDが指定されている  MFPのDIDが作成されている |
| 主シナリオ | 1. CG社製EDGEはMFPの鍵ペアを使って電子化文書に署名/暗号化を行う 2. CG社製EDGEは宛先のDIDへ電子化文書を送信する |
| 事後条件 | 電子化文書が宛先のDIDへ送信されている |
| 関連情報 | - |

## 2.3. Routing

|  |  |
| --- | --- |
| 目的 | 対象のDIDを持つデバイスへの通信をルーティングする |
| アクター | - |
| 事前条件 | あるDIDへの通信指示を受けている |
| 主シナリオ | 1. CG社製HUBは指定されたDIDへの通信をルーティングする |
| 事後条件 | 指定されたDIDを持つデバイスへの通信が行われている |
| 関連情報 | - |

## 2.4. Receive

|  |  |
| --- | --- |
| 目的 | 電子化文書を受信する |
| アクター | - |
| 事前条件 | 自デバイスのDID宛に暗号化文書が送信されている |
| 主シナリオ | 1. CG社製EDGEは自デバイスのDID宛に送信されてきた暗号化文書を受信する 2. CG社製EDGEは暗号化文書の復号を行い、署名を検証する |
| 事後条件 | 送信されてきた暗号化文書が復号されている |
| 関連情報 | - |

## 2.5. Save

|  |  |
| --- | --- |
| 目的 | 電子化文書を保存する |
| アクター | - |
| 事前条件 | 送信されてきた暗号化文書が復号されている |
| 主シナリオ | 1. 文書管理システムは復号された電子化文書を保存する |
| 事後条件 | 文書管理システムに電子化文書が保存されている |
| 関連情報 | - |

## 2.6. Browse

|  |  |
| --- | --- |
| 目的 | 電子化文書を閲覧する |
| アクター | 文書利用者 |
| 事前条件 | 文書管理システムに電子化文書が保存されている |
| 主シナリオ | 1. 利用者は文書管理システムに保存した電子化文書を閲覧する |
| 事後条件 | なし |
| 関連情報 | - |

## 2.7. Create DID

|  |  |
| --- | --- |
| 目的 | DIDを作成する |
| アクター | - |
| 事前条件 | 自デバイスのDIDが作成されていない |
| 主シナリオ | 1. CG社製EDGEは自デバイスのDIDを作成する 2. CG社製EDGEはCG社製HUBに自デバイスのDIDを登録する |
| 事後条件 | 自デバイスのDIDが作成されている  CG社製HUBに自デバイスのDID登録が行われている |
| 関連情報 | - |

## 2.8. Register DID

|  |  |
| --- | --- |
| 目的 | DIDを登録する |
| アクター | - |
| 事前条件 | デバイスのDID登録要求を受けている |
| 主シナリオ | 1. CG社製EDGEは自デバイスのDIDをDPKIに登録する |
| 事後条件 | 登録要求を送ったデバイスのDIDが登録されている |
| 関連情報 | - |

## 2.10. Access Control

|  |  |
| --- | --- |
| 目的 | CG社製HUBは、MFPデバイスやクラウドサービスの属性（データ）をフィルタリングすることで、悪意を持つ相手をブロックすることができる |
| アクター | HUBのシステム管理者 |
| 事前条件 |  |
| 主シナリオ | 1. HUBのシステム管理者は、HUBの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。 |
| 事後条件 | なし |
| 関連情報 | - |

## 2.11. Get Trace Log

|  |  |
| --- | --- |
| 目的 | HUBのシステム管理者は合意形成の条件に関するログを取得する |
| アクター | HUBのシステム管理者 |
| 事前条件 | HUBが合意形成の条件に関するログデータを管理している |
| 主シナリオ | 1. システム管理者はHUBのログデータを抽出し、文書作成者の合意形成の条件が履行されていることを確認する |
| 事後条件 | なし |
| 関連情報 | - |

# 機能要件

## MFP機能要件

### スキャン機能

- MFPの既存機能を利用して文書をスキャン、電子化できる

-出力フォーマットはPDFとする

### データ送信機能

-自デバイスのDIDに紐づいた鍵ペアを利用して送信データに署名を行う

-指定したDIDを宛先とし、DIDCommプロトコルに従って、暗号化した電子化文書を送信できる

-添付ファイルはbase64エンコードされる

### DID作成機能

-デバイスのDIDが作成されていない場合、DIDを作成する

-作成したDIDをDPKIに登録する

-MFPのUIで自デバイスのDIDを確認できる

-MFPの暗号鍵生成にはデバイス由来の真性乱数を利用する。生成した秘密鍵はTPM2.0を使ってセキュアに保存する。

## CG社製HUB機能要件

-デバイス間のデータ通信をルーティングする

-接続するエッジデバイスの属性情報に基づくアクセス制御を行う

認可しないデバイスの接続をブロックできる

-CG社製HUBの管理者は、エッジデバイスのアクセスプロファイルを管理できる

管理者はデバイスの通信相手のLocator（DIDs）を追加できる

任意のDIDsのみが復号できる暗号化通信が可能になる

-トラフィックとプロファイル変更ログを確認することができる

## 文書管理システム機能要件

### データ受信機能

-自デバイスのDIDに送信されたデータを受信できる

-受信したデータが改ざんされていないことを、生成者に都度直接参照することなく検証できる

-検証した結果を表示する

- DIDCommプロトコルに従ってデータを受信できる

-受信したデータをファイルとして保存できる

-添付ファイルをbase64デコードできる

### DID作成機能

-デバイスのDIDが作成されていない場合、DIDを作成する

-作成したDIDをDPKIに登録する

-文書管理システムのUIで自デバイスのDIDを確認できる

### ファイル閲覧機能

-保存した文書ファイルの中身を閲覧できる

-対応ファイルフォーマットはPDFとする

### その他

-保存された文書データを削除できる (テスト用)

# 非機能要件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **大項目** | **中項目** | **小項目** | **小項目説明** | **メトリクス (指標)** | **要件** | |
| **選択** | **補足** |
| 性能・拡張性 | 業務処理量 | 通常時の業務量 | 性能・拡張性に影響を与える業務量。 該当システムの稼働時を想定し、合意する。 それぞれのメトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。 | ユーザ数 | 特定ユーザのみ | 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 |
| 同時アクセス数 | 特定利用者の限られたアクセスのみ |  |
| データ量 | 主要なデータ量のみが明確である | スキャン文書数件分のデータを転送、保存できればよい |
| 業務機能数 | 業務機能が整理されている | ユースケースを参照すること |
| 性能目標値 | オンラインレスポンス | オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など） | 通常時レスポンス順守率 | 順守率を定めない | 実験用途のため、性能目標を定めない |
| 運用・保守性 | 通常運用 | 運用時間 | システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。 | 運用時間（通常） | 規定無し | 実験用途のため、継続運用を行わない |
| 運用環境 | 開発用環境の設置 | ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。 | 開発用環境の設置有無 | システムの開発環境を設置しない | 本番環境上で開発を行い、そのまま本番運用に使用する。 |
| 試験用環境の設置 | ユーザがシステムの動作を試験する目的で導入する環境についての項目。 | 試験用環境の設置有無 | システムの試験環境を設置しない | 試験用環境を用意しない。 |
| リモートオペレーション | システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。 | リモート監視地点 | 遠隔地でリモート監視を行う | 文書管理システムはネットワークを通して監視する |
| リモート操作の範囲 | 任意のリモート操作を行う | 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 |
| セキュリティ | 前提条件・制約条件 | 情報セキュリティに関するコンプライアンス | 順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール | 順守すべき社内規程、ルール、法令、ガイドライン等の有無 | 有り | 知財管理、輸出管理 |
| データの秘匿 | データ暗号化 | 機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。 | 伝送データの暗号化の有無 | 重要情報を暗号化 | 機能要件として記述 |
| 鍵管理 | 耐タンパデバイスによる鍵管理 | 機能要件として記述 |
| システム環境・エコロジー | システム特性 | クライアント数 | システムで使用され、管理しなければいけないクライアントの数。 | クライアント数 | 特定クライアントのみ | アクセスするMFPは2-3台のみ |
| 特定製品指定 | ユーザの指定によるオープンソース製品や第三者製品(ISV/IHV)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。 | 特定製品の採用有無 | 一部に特定製品の指定がある | CG社製EDGE, HUBを利用する |
| 複数言語対応 | システム構築の上で使用が必要、またはサービスとして提供しなければならない言語。扱わなければならない言語の数や各言語スキル保持者へのアクセシビリティを考慮。 | 言語数 | 1 | 日本語のみ対応 |