テクノロジーマップの整備に向けた調査研究

（アナログ規制の見直しに向けた技術実証等）における技術実証

技術実証報告書

実証類型番号 13：

情報の加工・流用防止技術等を活用した閲覧の実証

株式会社テクノロジックアート

2024 年 02 月 16 日

目次

1　技術実証の概要

1.1　目的

公的機関等の閲覧室等において、事前に閲覧許可を得た閲覧申請者が許可を得た文書の閲覧を可能とする制度があるが、閲覧申請者が文書を閲覧する際には、閲覧申請者に公的機関等が指定する場所への来所を求めた上、文書の改ざんや閲覧申請者以外の者による不正閲覧等が行われていないか、立会人（行政職員）が監視している。

当該閲覧について、情報の加工・流用防止技術やオンラインでの本人確認技術等を活用し、 オンラインで閲覧申請者本人のみに適切に情報開示が可能となるモデルを構築することで、立会人による監視を不要とするとともに閲覧者の利便性の向上を目指す。これらの方針を実現するために以下の事項を技術実証の目的とした。

① 閲覧申請者が任意の情報デバイスからインターネットを利用してシステムを利用できる環境を提供する。
② 閲覧申請者以外の第三者によるシステムの利用を回避し、閲覧申請者のみが安全に利用できる環境を提供する。
③ 閲覧申請者が閲覧している文書を複写及び保存することを防止する。
④ 閲覧申請者が閲覧している文書を第三者が覗き見することを防止する。
⑤ システムに保管されている文書の改ざんを防止する。
⑥ 改ざんされている文書を閲覧申請者に閲覧させない。

1.2　対象業務（法令）

公害紛争の処理手続等に関する規則第 64 条第 1 項等に基づく記録の閲覧及び、鉱業等に係る土地利用の調整手続等に関する法律第 39 条第 2 項に基づく調書の閲覧に関する業務を対象とする。

上記対象業務のうち、公害紛争の処理手続等に関する規則第 64 条の条文は次のとおりである。

> 第 64 条　当事者は、中央委員会の許可を得て、あつせん、調停又は仲裁に係る事件の記録を閲覧することができる。
> 2　当事者又は利害関係人は、中央委員会の許可を得て、裁定に係る事件の記録を閲覧又は謄写することができる。
> 3・4　（略）

現在、本対象業務では、閲覧者は公害等調整委員会が指定した場所に出向く必要があり、また、閲覧中には、文書の複写、改ざん、許可されていない第三者による閲覧が行われないように立会人による監視を必要としている。

1.3　全体像

本技術実証では、前述の目的の実現に向けて、次の実証事項（以下、実証事項）を満たす文書閲覧用のシステム（以下、実証システム）を開発し、当該システムを活用して、対象業務における立会人による監視を不要にできるかどうか、また、公的機関等が指定する場所に閲覧者が向かうコストを削減できるかどうかを実証した。

① 対象業務に基づく文書の閲覧を、任意の情報デバイスからインターネットを利用して行うシステムで、閲覧申請者から申請された文書のみを閲覧申請者本人のみに閲覧させ、デジタル化された文書を複写・改ざんさせないこと

② 任意の情報デバイスから閲覧が可能であり、情報の目的外利用や違法な第三者への提供を防止すること

以下に実証システムの全体像を示す（図 1）。また、実証システムを構成するサーバーやアプリケーションの機能・役割を表 1 に示す（詳細は、「2 技術実証内容の詳細」に記載）。

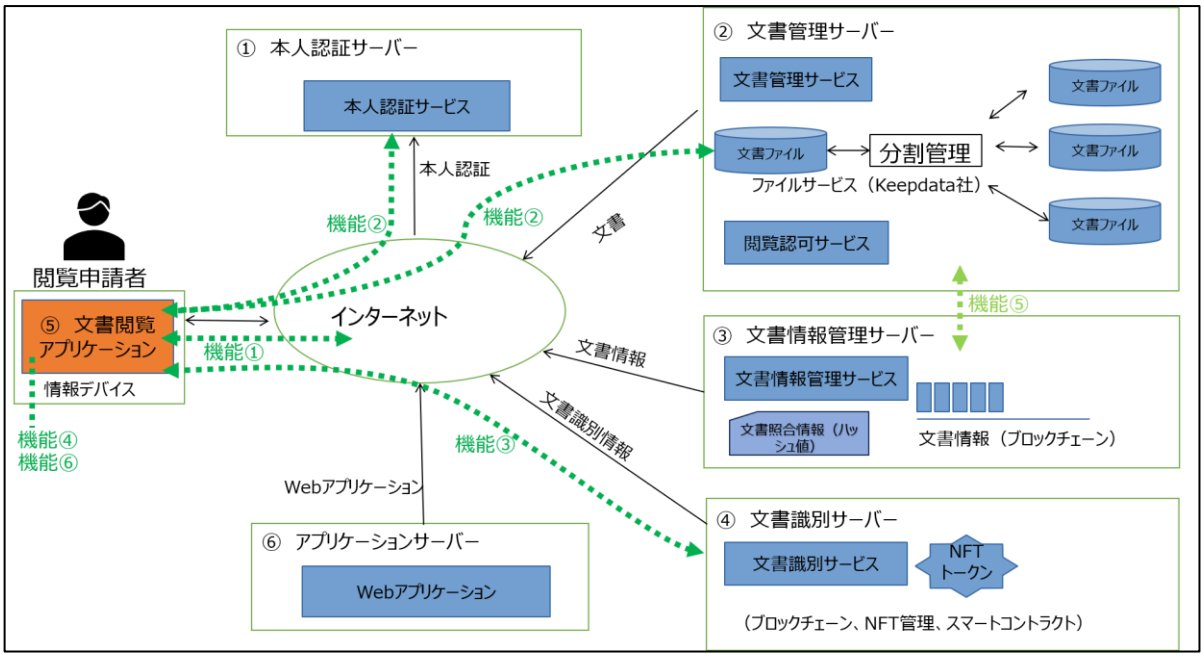

図 1：実証システム全体像

表 1：実証システムの各構成の役割と機能

構成システム名	機能・役割
① 本人認証サーバー	文書の閲覧を申請する者（以下、閲覧申請者）が本人であることを認証する。 ユーザー名とパスワード（以下、ID/PW）の入力、及び本人の所持する情報デバイスに送信したワンタイムパスワード（以下、OTP）の入力による多要素認証を行う。
② 文書管理サーバー	登録された閲覧対象文書を管理する。閲覧申請者が文書閲覧アプリケーションから送信した文書の閲覧の要求に対し、正当なものであれば文書の閲覧を認可し、文書を文書閲覧アプリケーションに送信する。文書のデータは暗号化され、複数のデータファイル上に分割管理される。
③ 文書情報管理サーバー	文書管理サーバーが管理する文書の文書名、文書属性、文書のハッシュ値をブロックチェーンのデータとして保持する。文書管理サーバーが文書から算出したハッシュ値と文書情報管理サーバーが保持する文書のハッシュ値を比較することにより文書の真正性を高めることが可能である。
④ 文書識別サーバー	閲覧申請者に文書の閲覧を許可する際に、文書情報管理サーバーが管理している文書情報、閲覧申請者の情報、及び閲覧を許可する期間の情報を NFT として生成する。この NFT により閲覧申請者が文書閲覧アプリケーションから閲覧できる文書を識別する。
⑤ 文書閲覧アプリケーション	閲覧申請者が使用する任意の情報デバイス上で稼働する文書閲覧用の Web アプリケーション。本人認証、閲覧が可能な文書のリスト表示、文書一覧から選択した文書の閲覧を行う。また、文書のコピー、印刷、改ざんを禁止し、画面キャプチャー、覗き見等による第三者への閲覧した文書の提供を防ぐ。
⑥ アプリケーションサーバー	Web アプリケーションのサーバー。文書閲覧アプリケーションの画面コードを保持し、情報閲覧者の所有する情報デバイスからの HTTP リクエストによりコンテンツとして送信する。

本技術実証では、1.1 の目的や実証事項を踏まえて、以下の各①～⑥の機能を実証システムに実装し、対象業務における実証システムの活用可能性を検証した。

① 閲覧申請者が任意の情報デバイスからインターネット経由で利用できる。
② 閲覧申請者のみに文書を閲覧させる。
③ 閲覧申請をした文書のみを閲覧申請者に閲覧させる。
④ システムに保管されている文書の複写を防止する。
⑤ システムに保管されている文書の改ざんを防止する。
⑥ 閲覧申請者が閲覧している文書について、第三者による覗き見等を防止する。

※図 1 の機能①～⑥の点線はこれらの機能の実証システム内での関連を表している。

上記の①～⑥の機能の実装方針の概要については、以下に示す。

- 「任意の情報デバイスからインターネットを利用」に関して、情報デバイス個別（iPhone、Windows PC など）のアプリケーションとして実装した場合、任意の情報デバイスに対応するアプリケーションではなくなるため、Web ブラウザー（Google Chrome など）対応のアプリケーション（以下、Web アプリケーション）として実装した。
- 「閲覧申請者から申請された文書のみを閲覧申請者本人のみに閲覧させ」に関して、閲覧申請者本人であることをより確かに認証する多要素認証を用いる。閲覧申請された文書のみの閲覧は、Keepdata 株式会社の共有ファイル管理システムを利用し、閲覧申請者が文書を閲覧する許可（以下、閲覧許可）の有無を確認して閲覧を制御することで実現した。
- 閲覧申請者の閲覧許可は、所管府省庁により文書の閲覧が許可された時に閲覧申請者の情報と文書の情報と閲覧の期間の情報から生成される NFT として実装した。NFT の生成と利用には、ラブロック株式会社のプライベートブロックチェーンとヒューマンズデータ株式会社の NFT に関する技術（スマートコントラクト）を使用した。本技術実証では、NFT の作成、及び付与等にスマートコントラクトを使用した。
- 「デジタル化された文書を複写・改ざんさせない」に関して、文書の複写防止は、個人の情報デバイスで閲覧している文書を情報デバイスに保存させない機能を実装することで、また、文書の改ざん防止は、文書の登録時にブロックチェーンに登録された文書情報と文書管理サーバーが保持している文書の文書情報を比較することで実現した。
- 「任意の情報デバイスから閲覧可能」について、及び「違法な第三者への提供を防止する」については、文書閲覧アプリケーションの保存防止機能と文書閲覧アプリケーションの覗き見防止機能により実現した。

1.4　実施体制・期間

1.4.1　実施体制

表　2：実施体制

事業者名	実施業務・役割
株式会社テクノロジックアート	実証事業の運営、システム設計、システム開発
Keepdata 株式会社 （株式会社テクノロジックアートからの再委託先）	KeepData（ファイル管理システムの商品名） と Rablock（ブロックチェーンの商品名）の連携インターフェースの開発、文書管理サーバーの環境開発
ラブロック株式会社 （株式会社テクノロジックアートからの再委託先）	Rablock ブロックチェーン環境設定、技術実証時の稼働サポート 覗き見防止ソリューションのカスタマイズ
ヒューマンズデータ株式会社 （株式会社テクノロジックアートからの再委託先）	文書管理サーバー用 NFT×スマートコントラクトのカスタマイズ開発
pitdyne 株式会社 （株式会社テクノロジックアートからの再委託先）	マルチデバイスアプリケーション開発

1.4.2　実施期間

2023 年 10 月 2 日～2024 年 2 月 16 日

1.4.3　開発スケジュール

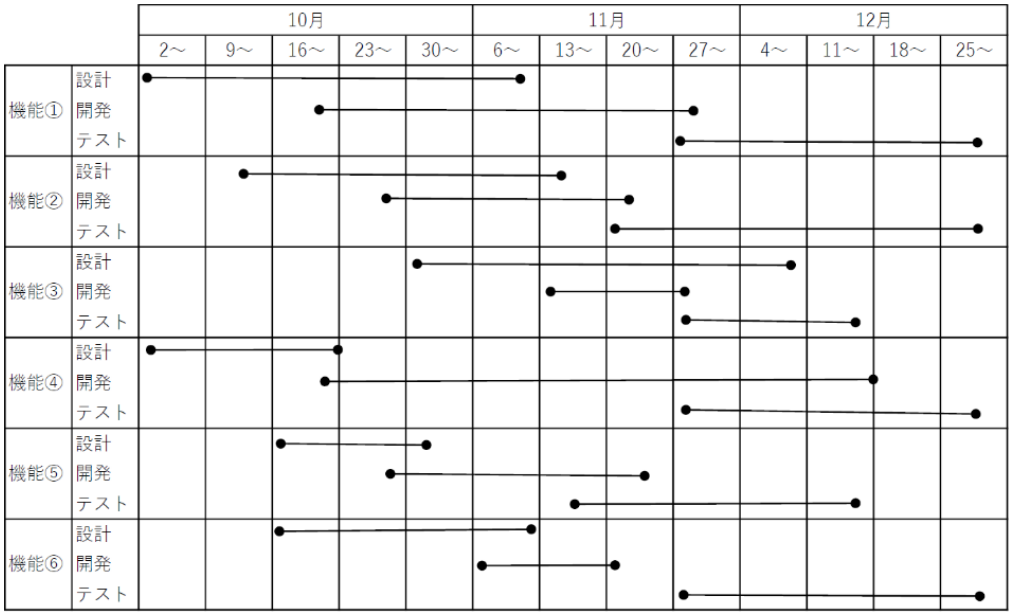

図　2：開発スケジュール

2　技術実証内容の詳細

2.1　技術実証の方法

1.3 の通り、実証事項の実現に必要となる機能①～⑥を実証システムに実装し、本技術実証の目的を達成できるかを確認した。具体的な各機能の実装方針や構築するシステム、活用する技術の詳細については、2.1.1 以下に示す。なお、実証システムを構成する文書管理サーバー、文書情報管理サーバー、文書識別サーバー、文書閲覧アプリケーションのアプリケーションサーバーは、すべて Amazon Web Services のクラウド上に配置した。

2.1.1　機能①（閲覧申請者が任意の情報デバイスからインターネット経由で利用できる）

[機能の実装方針]

インターネットに接続された任意の情報デバイスで文書閲覧アプリケーションを利用し、文書の閲覧が可能な仕様とする。

[構築するシステムの内容]

デバイスの種類、OS や Web ブラウザーで利用が著しく制限されないように、文書閲覧アプリケーションは、Web アプリケーションとして構築する。実証期間中に PC とタブレット端末、スマートフォンを準備し、文書閲覧アプリケーションが異なる情報デバイスであっても支障なく稼働することを検証している。検証対象の情報デバイスは、表 3 のものを想定していたが、取消線を引いた Android タブレット端末は、実証期間内に調達ができず稼働を検証していない。

表 3 ：実証対象の情報デバイス

情報デバイス種別	基本ソフトウェア(情報デバイスの本報告書内での呼称)		
PC	Windows (WindowsPC) 	macOS(MacPC) 	
タブレット端末	Windows	iOS(iPad) 	~~Android タブレット端末~~
スマートフォン		iOS(iPhone) 	Android スマートフォン 

2.1.2 機能②（閲覧申請者のみに文書を閲覧させる）

[機能の実装方針]

閲覧申請者の認証用の本人認証サーバーを使用し、インターネットに接続された PC やスマートフォン等の情報デバイスにおいて、ID/PW に加えて OTP により、多要素認証をしなければ文書を閲覧できないようにする。また、文書閲覧アプリケーションが継続して利用できることを確認することにより、認証情報を本人認証サーバーから取得できていることを確認できるようにする。

[要素技術]

- Keycloak
  OpenID Foundation が規定した身許認証のためのオープンな標準 OpenID Connect に準拠したオープンソースソフトウェア。認可機能や ID 管理機能を備える。
- Google Authenticator
  多要素認証の OTP の受信に用いるトークンソフトウェア。

[構築するシステムの内容]

文書閲覧アプリケーションから本人認証サーバーに対するリクエストには、本人認証サーバーに導入した Keycloak によって発行された有効なアクセストークンを必要とする。

Keycloak は、リクエストにアクセストークンが無い、もしくは有効期限切れのアクセストークンである場合に、ID/PW による認証を文書閲覧アプリケーションに要求する。ID/PW による認証を通過した後、Keycloak は外部の識別子プロバイダー（Google を使用）に OTP を閲覧申請者が登録している情報デバイスに送信するよう依頼する。文書閲覧申請者は、情報デバイスに導入されている Google Authenticator で OTP を確認し、文書閲覧アプリケーションに入力する。

ID/PW による認証と OTP による認証が通過した場合に Keycloak はアクセストークンを文書閲覧アプリケーションに送信する。

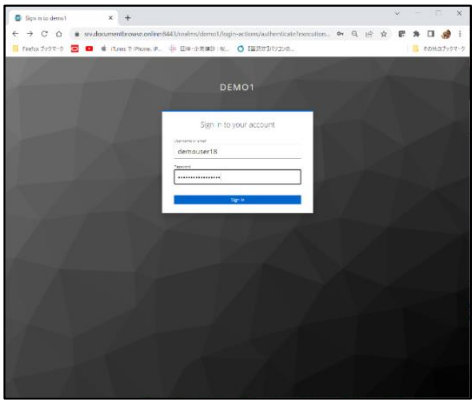

図 3：ID/PW による認証

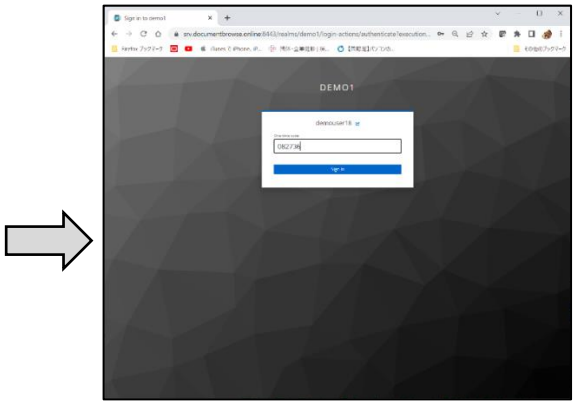

図 4：OTP による認証

2.1.3 機能③（閲覧申請をした文書のみを閲覧申請者に閲覧させる）

[機能の実装方針]

インターネットに接続された情報デバイスで文書閲覧アプリケーションにログインし、閲覧申請者に閲覧が許可されている文書のみを、文書一覧から選択して閲覧できるようにする。

[要素技術]

- Rablock
  NFT の管理用プライベートブロックチェーン

[構築するシステムの内容]

文書閲覧アプリケーションは、閲覧申請者のログイン後に閲覧が許可されている文書の一覧を文書識別サーバーにリクエストして取得する。文書一覧における文書データ（以下、文書情報）は、文書名、文書データのハッシュ値、その他属性（根拠法令、所管府省庁等）から構成されている。

閲覧申請者に文書の閲覧が許可された時点で、閲覧申請者、文書情報、閲覧開始日（閲覧が可能となる日）と閲覧終了日（閲覧が翌日からできなくなる日）からなる閲覧期間のデータを基に、文書閲覧の許可証となる NFT を作成し、文書識別サーバーのブロックチェーンに格納する。NFT は、唯一無二のデジタルデータであり、ブロックチェーンの改ざん防止性によって保護される。

次に、文書閲覧アプリケーションから文書一覧の取得を依頼された文書識別サーバーは、NFT を保持しているブロックチェーンから所有者のアカウント名が閲覧申請者名のアカウント名と同じものを検索し、文書一覧の取得依頼日時が閲覧期間の期間中であることを条件として絞り込みを行った結果セットを作成する。結果セットの NFT から文書情報を抽出し、文書一覧を作成し、文書閲覧アプリケーションに送信する。これにより、文書閲覧アプリケーションで表示される文書一覧は、閲覧申請者が閲覧を申請し許可された文書のみであることとなる。

文書閲覧アプリケーションは、上記の処理により、閲覧できる文書一覧が表示されるため、閲覧申請者に許可された文書のみを閲覧させることができるようになる。

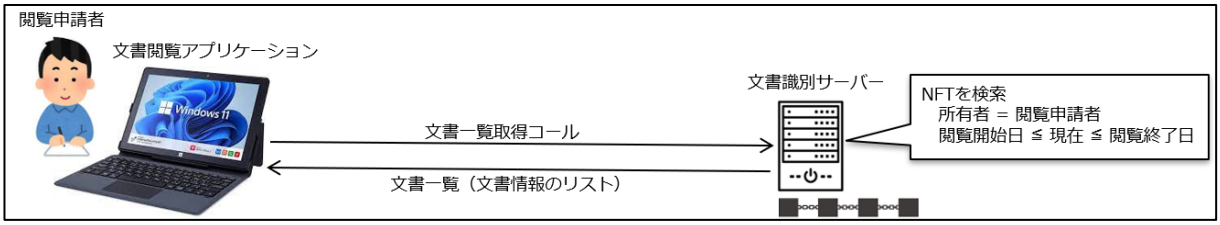

図 5：文書一覧の取得

2.1.4 機能④（システムに保管されている文書の複写を防止する）

[機能の実装方針]

文書閲覧アプリケーションの機能によって文書の保存等を制限し、閲覧申請者による複写（コピー、印刷）をさせない。

[構築するシステムの内容]

文書閲覧アプリケーションは、Web ブラウザーに表示されているコンテンツを Web ブラウザーの外に複写できないように制御するプログラムコードを記述している。この制御により Web ブラウザーのコンテキストメニューから表示している文書の印刷、及びファイルダウンロードは、図 8 のように 1 ページの白紙の文書として印刷・保存される。

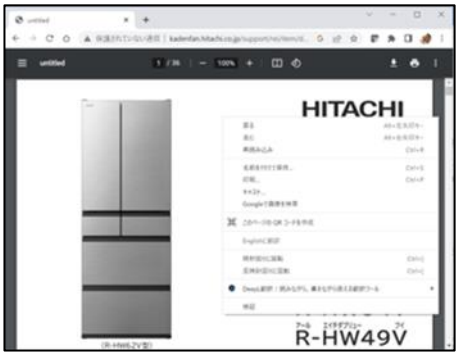

図 6：コンテキストメニュー

図 7：複写を制御していない場合

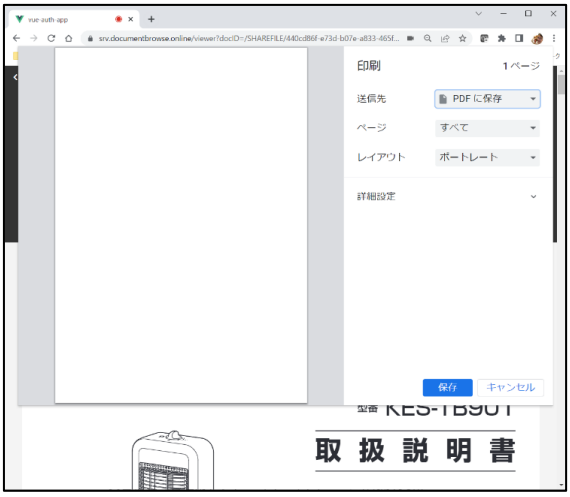

図 8：複写の制御を行っている場合

2.1.5 機能⑤（システムに保管されている文書の改ざんを防止する）

[機能の実装方針]

記録文書を管理する文書管理サーバーと、当該サーバー上で管理されている文書データ（ハッシュ値等）をブロックチェーンとして保持する文書情報管理サーバーを連携させ、文書の改ざんを検知する機能を構築する。具体的には、文書管理サーバーにおける文書情報と、文書情報管理サーバーに保管されている文書情報（ハッシュ値）を比較することで、文書の改ざん検知機能を実現する。

[要素技術]

- Rablock
  文書情報の管理用プライベートブロックチェーン
- ハッシュ値
  任意の長さのデータからハッシュ関数により生成される一定長のバイナリまたは文字列。
  文書管理サーバーに保管されている文書データが改ざんされているかを検知するために用いる。

[構築するシステムの内容]

文書管理サーバーに新規の文書を登録する際に、文書データのハッシュ値を計算し、文書名、所管府省庁などの文書の属性とあわせて文書情報を作成し、文書情報管理サーバーに保存する。

文書情報管理サーバーは、ブロックチェーンで文書情報を保管している。ブロックチェーンで保管されているデータは改ざんを防止することができるため、文書情報のハッシュ値は、新規に文書を登録した際に計算されたハッシュ値のままであり、信頼できるデータである。

文書管理サーバーは、文書ファイルの改ざんの検知のために保管している文書のハッシュ値を計算し、文書情報管理サーバーに保管されている文書のハッシュ値と比較する（図 9）。双方のハッシュ値が異なれば、文書管理サーバーの文書は改ざんされていることとなる。

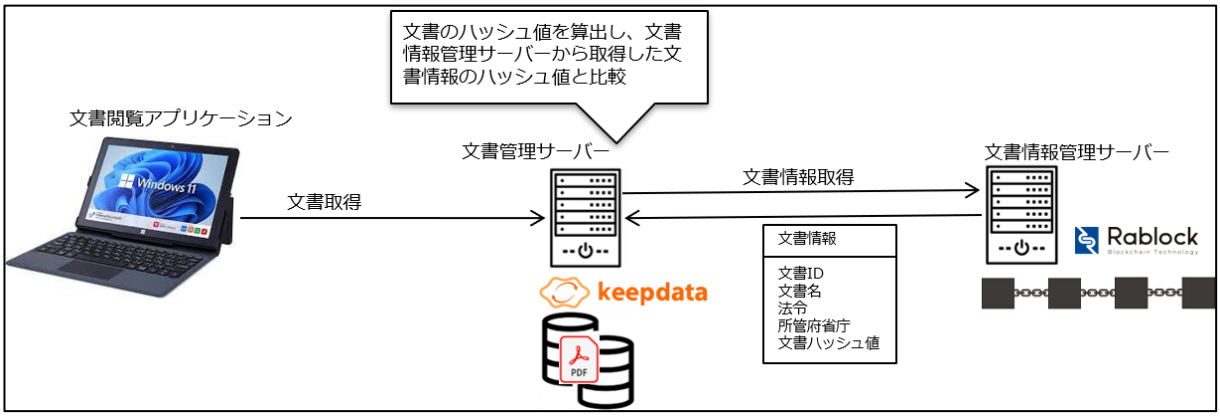

図 9：文書の改ざん検知

2.1.6 機能⑥（閲覧申請者が閲覧している文書について、第三者による覗き見等を防止する）

[機能の実装方針]

文書閲覧アプリケーションで閲覧中の文書を第三者が覗き見すること、また、閲覧申請者等による写真撮影や書き写しのような違法な第三者への情報提供の手段の防止対策を実装する。

[要素技術]

- 覗き見防止ソリューション（株式会社プラットフィールド）
  閲覧中の文書を覗き見する、写真撮影をする、書き写すといった違法な第三者への情報提供手法の防止対策。実装にあたっては ASP 形式で提供される覗き見防止ソリューションの一部機能を本技術実証で使用する Web アプリケーション用にカスタマイズし、iframe 形式で HTML 文書に埋め込めるようにした。

[構築するシステムの内容]

文書閲覧アプリケーションにおける覗き見防止機能は、接続している情報デバイスに組み込まれた Web カメラから入力データがあることを起動条件とし、情報デバイスの使用者の顔が Web カメラの画像の中心に写っている状態を認識して稼働する。

Web カメラの画像から次の 3 点を検知する。

- 閲覧申請者以外の第三者が写りこむと、覗き見として検知する。（図 10, 11）
- スマートフォンが写りこむと、画面撮影の可能性があることを検知する。（図 12, 13）
- 筆記具が写りこむと、謄写の可能性があることを検知する。

前ページの３つの行為が検知された場合、文書閲覧アプリケーションは、文書表示画面を検知画面に切り替えることで文書を見えなくする（図 11, 13）。検知画面は、閲覧申請者が「閉じる」ボタンを押すまで解除されない。

図 10：第三者による覗き見

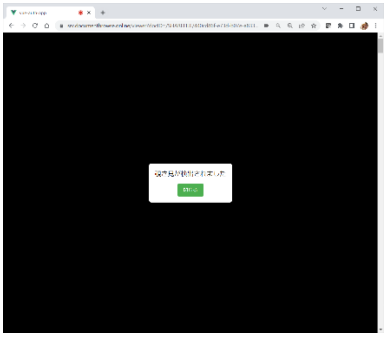

図 11：覗き見を検知

図 12：スマホで画面の撮影を試みる

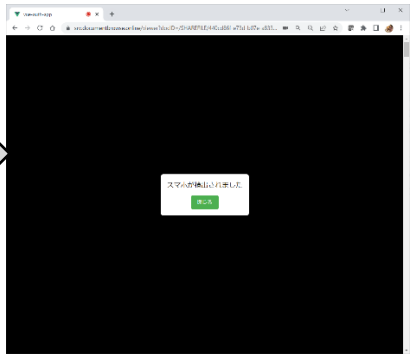

図 13：スマホを検知

2.2 実施場所等

実証システムは、Amazon Web Service クラウド上に構築しており、閲覧申請者を想定した実証事業者の社員の自宅等からインターネット環境がある場所であればどこでも技術実証が行える環境を構築した。

実証事業者の社員は、自宅から文書閲覧アプリケーションを操作し、また必要に応じて実証システムの各サーバーにログインし、各機能が出力しているログを確認し、検証を行った。図 14 は、本人認証サーバーが文書閲覧アプリケーションからリクエストされた本人認証の処理を行ったログの例となる。

```
2023-12-20 13:51:52,758 DEBUG [org.keycloak.events] (executor-thread-1) type=LOGIN,
realmId=6dc4846f-4a47-483d-b002-3e06c40ffccb, clientId=democlient2, userId=75b56a7a-f73e-
4ee3-8233-168d969e0c8d, ipAddress=133.200.170.65, auth_method=openid-connect,
auth_type=code, selected_credential_id=f1f6c4dd-224b-49d4-9a3f-d43ad93ba724,
response_type=code, redirect_uri=https://srv.documentbrowse.online/,
consent=no_consent_required, code_id=e45ba252-daf7-4541-ba4d-1045560e984a,
username=demouser17, response_mode=fragment, authSessionParentId=e45ba252-daf7-4541-
ba4d-1045560e984a, authSessionTabId=y0dnB6OHF9s
2023-12-20 13:51:53,079 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (executor-
thread-1) new JtaTransactionWrapper

        中略

2023-12-20 13:51:53,093 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (executor-
thread-1) JtaTransactionWrapper   commit
2023-12-20 13:51:53,093 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (executor-
thread-1) JtaTransactionWrapper end
2023-12-20 13:51:53,093 DEBUG [org.keycloak.events] (executor-thread-1)
type=CODE_TO_TOKEN, realmId=6dc4846f-4a47-483d-b002-3e06c40ffccb, clientId=democlient2,
userId=75b56a7a-f73e-4ee3-8233-168d969e0c8d, ipAddress=133.200.170.65, token_id=dcdad020-
5dbc-48f3-869e-c4431adf6c07, grant_type=authorization_code, refresh_token_type=Refresh,
scope='openid email profile', refresh_token_id=4fd8f8ae-ecce-4e6c-a8f6-eaf0db2282ac,
code_id=e45ba252-daf7-4541-ba4d-1045560e984a, client_auth_method=client-secret
2023-12-20 13:51:56,303 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (Timer-0) new
JtaTransactionWrapper
2023-12-20 13:51:56,303 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (Timer-0) was
existing? false
2023-12-20 13:51:56,303 DEBUG [org.keycloak.services.scheduled.ScheduledTaskRunner] (Timer-0)
Executed scheduled task
AbstractLastSessionRefreshStoreFactory$$Lambda$1623/0x00007f14bbc12ad8
2023-12-20 13:51:56,303 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (Timer-0)
JtaTransactionWrapper   commit
2023-12-20 13:51:56,303 DEBUG [org.keycloak.transaction.JtaTransactionWrapper] (Timer-0)
JtaTransactionWrapper end
```

図 14：ログの確認例（本人認証サーバー）

また、総務省公害等調整委員会事務局の会議室において、公害等調整委員会事務局メンバーに対して実証システムを理解していただくために、実証システムに関するプレゼンテーション、及びデモンストレーションを実施した。

プレゼンテーションでは、実証システムの各サーバー、及び文書閲覧アプリケーションの機能の説明を行った。デモンストレーションでは、文書閲覧アプリケーションの画面をモニターに表示し、多要素認証によるログイン、文書の一覧表示、文書の閲覧、複写防止機能、第三者による覗き見の防止機能（外部からの撮影防止機能を含む）の動作を実演して説明した。

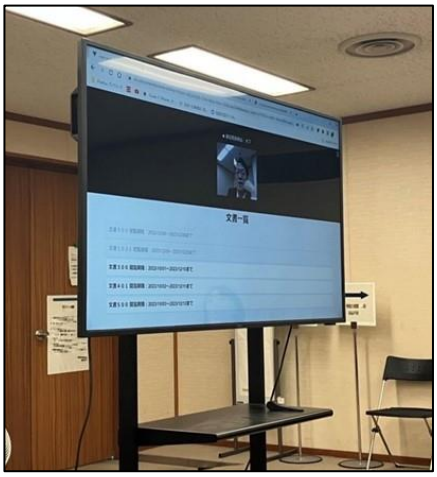

図 15：公害等調整委員会事務局の会議室におけるデモンストレーションの様子

3　技術実証の結果

3.1　結果の評価ポイント・方法

本技術実証（実証システム）の評価は、ソフトウェア品質に関する包括的なフレームワークである SQuaRE(Software Product Quality Requirements and Evaluation)の考え等も踏まえて整理した以下の表 4 に基づき、機能①～⑥それぞれについて行う（具体的な評価方法等の詳細は 3.2 以下を参照）。

各機能①～⑥の評価に際して、どの評価観点・ポイントに基づいて評価したかは、3.2.1 以下の[評価方法・評価観点]において表 4 記載の記号により示している。

表　4 ：評価の観点

観点	観点内容	記号
機能性 (Functionability)	ソフトウェアが正確に動作し、仕様に準拠しているかどうか。 ソフトウェアがユーザーの期待や要件を満たしているかどうか。	F
信頼性 (Reliability)	長時間実行されてもクラッシュやエラーが発生しないか。 予期せぬ事態に対する回復力や復旧力があるか。	R
セキュリティ (Security)	データが適切に保護され、機密情報が漏れないか。 アクセス制御が適切に機能しているか。	S
互換性 (Compatibility)	ソフトウェアが対象となるハードウェアやオペレーティングシステムで正しく動作するか。	C

前提として、各実証項目を実現する機能が方針通りに動作すること（機能性）が最も重要な評価観点である。また、実運用の観点から非機能要件の評価観点も必要である。任意の情報デバイスで稼働することに対しては互換性の、文書を含むデータの漏洩、改ざんを防ぐことに対してはセキュリティ及び信頼性の評価観点が必要である。

3.2　結果及び評価・分析

3.2.1 機能①（閲覧申請者が任意の情報デバイスからインターネット経由で利用できる）

[実証内容]

「閲覧申請者が任意の情報デバイスからインターネット経由で利用できる」機能について、インターネットに接続された任意の情報デバイスで稼働する文書閲覧アプリケーションから文書の閲覧が可能なことを確認する。

[評価方法の設定ポイント]

- WindowsPC 上で稼働する文書閲覧アプリケーションのインターネットへの接続は一般的なインフラから行える。
- WindowsPC 上で稼働する文書閲覧アプリケーションのインターネットへの接続が一般的なインフラから行えた場合、WindowsPC 以外の任意の情報デバイス上で稼働する文書閲覧アプリケーションにおいてもインターネットへの接続は一般的なインフラから行える。

[評価方法、評価観点]

表　5 ：機能①の評価方法

No.	評価方法	評価観点
①-1	WindowsPC で社内 LAN の Wi-Fi 経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F
①-2	WindowsPC で社外の公衆 Wi-Fi 経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F
①-3	WindowsPC を用いてモバイル回線経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F
①-4	①-1～①-3 を MacPC で行う。	C
①-5	①-1～①-3 を iPad で行う。	C
①-6	①-1～①-3 を iPhone で行う。	C
①-7	①-1～①-3 を Android スマートフォンで行う。	C

[評価結果]

表 6 : 機能①の評価結果

No.	評価方法	評価観点	評価結果
①-1	WindowsPC で社内 LAN の Wi-Fi 経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F	○
①-2	WindowsPC で社外の公衆 Wi-Fi 経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F	○
①-3	WindowsPC を用いてモバイル回線経由で文書閲覧アプリケーションから実証システムにログインし、文書を閲覧する。	F	○
①-4	①-1～①-3 を MacPC で行う。	C	
	①-1		○
	①-2		○
	①-3		○
①-5	①-1～①-3 を iPad で行う。	C	
	①-1		○
	①-2		○
	①-3		○
①-6	①-1～①-3 を iPhone で行う。	C	
	①-1		○
	①-2		○
	①-3		○
①-7	①-1～①-3 を Android スマートフォンで行う。	C	
	①-1		○
	①-2		○
	①-3		○

①-1，①-2，①-3 の結果、文書閲覧アプリケーションは情報デバイスが一般的なインターネット環境に接続できていれば、どこからでも使用できることが確認できた。

①-4，①-5，①-6，①-7 の結果、任意の情報デバイスで同等に使用することが確認できた。

[結果分析]

文書閲覧アプリケーションは、Web ブラウザー上で稼働するため、任意の情報デバイスでインターネットを利用して文書の閲覧をすることは問題がないことがわかる。

本技術実証の評価ポイントではないが、文書閲覧アプリケーションは、情報デバイスのカメラを使用するため低速な回線でインターネットに接続している場合に、動作に遅延が発生することが考えられるが、文書閲覧アプリケーション自体の挙動に問題はない。

情報デバイスのインターネット接続は、高速なインターネットに接続しているルーター(Wi-Fi 含む)を使用することが望ましい。モバイル端末では、4G 以上の公衆回線に接続し、3G 以下の場合はなるべく使用しないことが考えられる。

3.2.2 機能②（閲覧申請者のみに文書を閲覧させる）

[実証内容]

「閲覧申請者のみに文書を閲覧させる」機能について、本人認証サーバーを使用し、インターネットに接続された情報デバイスのある場所で、ID/PW、及び OTP による多要素認証ができるかどうかを確認する。また、文書閲覧アプリケーションが継続して利用できることを確認することにより、認証情報を本人認証サーバーから取得できていることを確認する。

[評価方法の設定ポイント]

- 閲覧申請者の本人確認が ID/PW の確認で行え、また OTP を利用することでより正確な本人確認ができる。
- 文書一覧は閲覧認証者に閲覧が許可されている文書だけである。
- 閲覧申請者以外の第三者による文書の閲覧を防ぐ仕組みが機能している。

[評価方法、評価観点]

表 7：機能②の評価方法

No.	評価方法	評価観点
②-1	間違ったパスワードで ID/PW 認証されないことを確認する。	S
②-2	ID/PW 認証後、OTP 受信用に登録した情報デバイスで OTP の受信を確認する。	S, F
②-3	間違った OTP で OTP 認証されないことを確認する	S
②-4	OTP 認証が通過し、実証システムにログインし、文書一覧画面に遷移したことを確認する。	F
②-5	文書一覧から文書を選択し、文書閲覧が可能であることで文書閲覧アプリケーションが継続的に使用できることを確認する。	F
②-6	文書閲覧アプリケーションのログアウトを操作し、文書閲覧アプリケーションからログアウトし、ID/PW 認証画面に遷移したことを確認する。	S, F
②-7	同一の ID を使用して複数箇所で同時に起動している文書閲覧アプリケーションから実証システムにログインできないことを確認する。	S
②-8	文書閲覧アプリケーションにログイン後、操作の時間がシステム側で設定したタイムアウト時間を経過した後、継続して文書閲覧アプリケーションが使用できないことを確認する。	S

[評価結果]

表 8：機能②の評価結果

No.	評価方法	評価観点	評価結果
②-1	間違ったパスワードで ID/PW 認証されないことを確認する。	S	○
②-2	ID/PW 認証後、OTP 受信用に登録した情報デバイスで OTP の受信を確認する。	S, F	○
②-3	間違った OTP で OTP 認証されないことを確認する	S	○
②-4	OTP 認証が通過し、実証システムにログインし、文書一覧画面に遷移したことを確認する。	F	○
②-5	文書一覧から文書を選択し、文書閲覧が可能であることで文書閲覧アプリケーションが継続的に使用できることを確認する。	F	○
②-6	文書アプリケーションのログアウトを操作し、文書閲覧アプリケーションからログアウトし、ID/PW 認証画面に遷移したことを確認する。	S, F	○
②-7	同一の ID を使用して複数箇所で同時に起動している文書閲覧アプリケーションから実証システムにログインできないことを確認する。	S	○
②-8	文書閲覧アプリケーションにログイン後、操作の時間がシステム側で設定したタイムアウト時間を経過した後、継続して文書閲覧アプリケーションが使用できないことを確認する。	S	×

②-1，②-2，②-3，②-5，②-6 の評価結果のとおり、本人認証を ID/PW 認証と OTP 認証の 2 段階かつ多要素で認証が可能であり、閲覧申請者が本人である可能性が高いことを認証することができた。

②-4、②-6 の結果、文書閲覧アプリケーションは、本人認証後に文書一覧を表示し、ログアウト操作後にはログイン画面に遷移し、共に正常に稼働した。

②-7 については、閲覧申請者が複数の情報デバイスから実証システムにアクセスすることを防止し、複数の同一な閲覧申請者による不正な文書の閲覧を防ぐことができた。

②-8 については、文書閲覧アプリケーションは、ログイン後にログアウトを明示的に行う必要があり、ログインしたままの状態の情報デバイスを第三者に手渡したり放置したりした場合には、第三者による不正な閲覧を防ぐことが困難であった。本人認証に使用している Keycloak の設定ではタイムアウト処理ができないことが事後調査で判明した。このため、文書閲覧アプリケーションにタイムアウト処理を入れることが必要である。文書閲覧アプリケーションにタイムアウト処理を実装する場合、設計、開発、テストを含めて 2 人日ほどで可能と見積もられる。タイムアウト機能を実装しない場合は、閲覧使用者が情報デバイスから離れる場合に必ず文書閲覧アプリケーシ

ョンのログアウトを実行するよう注意喚起する運用となる。

[結果分析]

対象業務の記録の閲覧では、閲覧する人が閲覧申請者本人であることを認証する必要があるが、本技術実証で利用した ID/PW と OTP による 2 段階かつ 2 要素の認証は、本人の知識ベースである ID/PW だけでなく、本人の所有物ベースである OTP を受け取る手段の認証であるため本人認証の精度は高い。より精度の高い本人認証が必要な場合には、ID/PW と OTP の 2 要素の認証に顔認証や指紋認証などの生体認証を加えて 3 要素の認証とすることも可能である。

②-7，②-8 は閲覧申請者以外の第三者による不正閲覧を防ぐことを課題としているが、②-7 は、同時に複数の情報デバイスからログインしなくとも、ログイン後の情報デバイスを第三者に手渡すことで不正閲覧を防ぐことはできない。②-8 は文書閲覧アプリケーションの仕様の問題であり、アイドルタイムアウトを設ける、文書アクセス時に再度 OTP を求めるなど要件が明確であれば問題は解決する。

3.2.3 機能③（閲覧申請をした文書のみを閲覧申請者に閲覧させる）

[実証内容]

「閲覧申請をした文書のみを閲覧申請者に閲覧させる」機能について、インターネットに接続された情報デバイスの文書閲覧アプリケーションにより、文書識別サーバーが閲覧申請者の所有する NFT を基に作成した文書一覧の文書のみ閲覧できることから、閲覧申請をした文書のみを閲覧申請者に閲覧させることが可能であることを確認する。

[評価方法の設定ポイント]

- 文書識別サーバーが閲覧申請者に閲覧が許可され、期限内である NFT を検索し、正しい文書一覧を作成している。
- 文書識別サーバーが文書閲覧アプリケーションから送信された文書情報の真正性を確認し、NFT を返信している。
- 文書管理サーバーが文書閲覧アプリケーションから送信された NFT の真正性を確認し、文書を返信している。

[実証の評価方法、評価観点]

表 9 ：機能③の評価方法

No.	評価方法	評価観点
③-1	文書識別サーバーのブロックチェーンで管理されている NFT で文書閲覧アプリケーションのログインアカウントが所有する NFT を検索する。 検索結果における NFT の文書情報が文書閲覧アプリケーションの文書一覧にあることを確認する。	F
③-2	文書一覧に所有者が異なる NFT の文書情報が無いことを確認する。	S, F
③-3	文書一覧の文書で閲覧許可期間から外れている文書が閲覧できないようになっていることを確認する。	F
③-4	文書一覧の文書で閲覧許可期間中の文書が閲覧できることを確認する。	F
③-5	文書閲覧アプリケーションが文書を閲覧する際に、文書識別サーバーに送信した文書情報に改ざんがないことを確認する処理を文書識別サーバー、及び文書情報管理サーバーのログから確認する。	S, F
③-6	文書識別サーバーが文書情報の真正性を確認した後に、その文書情報の NFT を文書閲覧アプリケーションに送信していることを情報識別サーバーのログから確認する。	S, F
③-7	文書閲覧アプリケーションが文書取得時に文書管理サーバーに送信した NFT の真正性確認を文書管理サーバーが文書識別サーバーにリクエストしているかを文書管理サーバー、及び文書識別サーバーのログから確認する。	S, F

③-8	③-7 の NFT の真正性が確認できた後に、文書管理サーバーが文書の閲覧を認可し、文書を文書閲覧アプリケーションに送信したことを文書管理サーバーのログから確認する。	S, F

[評価結果]

表 １０：機能③の評価結果

No.	評価方法	評価観点	評価結果
③-1	文書識別サーバーのブロックチェーンで管理されている NFT で文書閲覧アプリケーションのログインアカウントが所有する NFT を検索する。 検索結果における NFT の文書情報が文書閲覧アプリケーションの文書一覧にあることを確認する。	F	○
③-2	文書一覧に所有者が異なる NFT の文書情報が無いことを確認する。	S, F	○
③-3	文書一覧の文書で閲覧許可期間から外れている文書が閲覧できないようになっていることを確認する。	F	○
③-4	文書一覧の文書で閲覧許可期間中の文書が閲覧できることを確認する。	F	○
③-5	文書閲覧アプリケーションが文書を閲覧する際に、文書識別サーバーに送信した文書情報に改ざんがないことを確認する処理を文書識別サーバー、及び文書情報管理サーバーのログから確認する。	S, F	○
③-6	文書識別サーバーが文書情報の真正性を確認した後に、その文書情報の NFT を文書閲覧アプリケーションに送信していることを情報識別サーバーのログから確認する。	S, F	○
③-7	文書閲覧アプリケーションが文書取得時に文書管理サーバーに送信した NFT の真正性確認を文書管理サーバーが文書識別サーバーにリクエストしているかを文書管理サーバー、及び文書識別サーバーのログから確認する。	S, F	○
③-8	③-7 の NFT の真正性が確認できた後に、文書管理サーバーが文書の閲覧を認可し、文書を文書閲覧アプリケーションに送信したことを文書管理サーバーのログから確認する。	S, F	○

③-1，③-2 の結果、文書識別サーバーが管理する NFT は、閲覧申請者の情報、その閲覧申請者に閲覧が許可された文書の情報、及び閲覧が許可された期間を示す情報を基に作

成された、唯一無二の閲覧許可証として活用することが可能であることを確認できた。

③-3，③-4 の結果、文書閲覧アプリケーションが文書一覧を常時保持しているのではなく、ログインと同時に文書識別サーバーが作成しているため、文書識別サーバーが管理している情報と一致した結果を反映させていることが確認できた。

③-5，③-6 の結果、管理できない外部の情報デバイスで稼働している文書閲覧アプリケーションから文書識別サーバーに送信されたデータを信用せずに真正性を確認し、改ざんがされていなければ NFT を文書閲覧アプリケーションに送信していることが確認できた。

③-7 の結果、管理できない外部の情報デバイスで稼働している文書閲覧アプリケーションから文書管理サーバーに送信された文書取得リクエストに添付された NFT を信用せずに真正性を確認して、NFT が改ざんされていない場合に文書データを送信していることが確認できた。

③-8 の結果、文書管理サーバーが文書閲覧アプリケーションに文書データを送信する前に、文書データの真正性を確認するために文書情報管理サーバーと通信し改ざんが検知されなかった場合のみ文書を送信していることが確認できた。

以上から、実証システムは、閲覧申請者に申請された文書のみを閲覧させることをより確実に行うよう機能していることが確認できた。

[結果分析]

対象業務の文書の閲覧では、閲覧申請者が本人であっても、管理できていない情報デバイスの安全性を信用せずに、送信されたデータの真正性を確認すること、また閲覧申請者が閲覧する文書は改ざんされていない文書であることを要件とした。

１つ目の要件は、文書を閲覧するために必要な NFT を取得するための送信データと文書を取得するための送信データの真正性を確認することで外部の情報デバイスから送られてきたデータが改ざんされていないことを保証することができている。

２つ目の要件は、実証システムに文書を登録する際に文書情報管理サーバーに保存した文書情報のハッシュ値を確認することで文書データが改ざんされていないことを保証することができている。

3.2.4 機能④（システムに保管されている文書の複写を防止する）

[実証内容]

「システムに保管されている文書の複写を防止する」機能について、文書閲覧アプリケーションの機能により文書のコピー、印刷、保存を制限し、文書の複写を防止できることを確認する。

[評価方法の設定ポイント]

- WindowsPC 上で稼働する文書閲覧アプリケーションに閲覧中の文書のコピー、印刷、保存を防止する機能がある。
- WindowsPC 上で稼働する文書閲覧アプリケーションの閲覧中の文書のコピー、印刷、保存を防止する機能が有効であった場合、WindowsPC 以外の任意の情報デバイスで稼働する文書閲覧アプリケーションにおいても閲覧中の文書のコピー、印刷、保存を防止することができる。

[実証の評価方法、評価観点]

表 １１：機能④の評価方法

No.	評価方法	評価観点
④-1	WindowsPC で文書閲覧アプリケーションが閲覧中の文書をクリップボードにコピーし、他のアプリケーション(ノートパッド等）にペーストできないことを確認する。	F
④-2	WindowsPC で文書閲覧アプリケーションでは印刷、保存などのコンテキストメニューが動作しないことを確認する。	F
④-3	WindowsPC で文書閲覧アプリケーションが閲覧中の文書を Web ブラウザーの印刷機能で印刷しても白紙 1 枚しか印刷しないことを確認する。	F
④-4	WindowsPC で文書閲覧アプリケーションが閲覧中の文書を Web ブラウザーの保存機能で保存しても白紙 1 枚の PDF として保存されることを確認する。	F
④-5	WindowsPC で文書閲覧アプリケーションの機能により画面キャプチャ―が行えないように制御できることを確認する。	F
④-6	④-1 ～ ④-5 の確認を、MacPC で行う。	C
④-7	④-1 ～ ④-5 の確認を、iPad で行う。	C
④-8	④-1 ～ ④-5 の確認を、iPhone で行う。	C
④-9	④-1 ～ ④-5 の確認を、Android スマートフォンで行う。	C

[評価結果]

表 １２：機能④の評価結果

No.	評価方法	評価観点	評価結果
④-1	WindowsPC で文書閲覧アプリケーションが閲覧中の文書をクリップボードにコピーし、他のアプリケーション(ノートパッド等）にペーストできないことを確認する。	F	○
④-2	WindowsPC で文書閲覧アプリケーションでは印刷、保存などのコンテキストメニューが動作しないことを確認する。	F	○
④-3	WindowsPC で文書閲覧アプリケーションが閲覧中の文書を Web ブラウザーの印刷機能で印刷しても白紙 1 枚しか印刷しないことを確認する。	F	○
④-4	WindowsPC で文書閲覧アプリケーションが閲覧中の文書を Web ブラウザーの保存機能で保存しても白紙 1 枚の PDF として保存されることを確認する。	F	○
④-5	WindowsPC において文書閲覧アプリケーションの機能により画面キャプチャーが行えないように制御できることを確認する。	F	×
④- 6	④-1 ～ ④-5 の確認を、MacPC で行う。	C	
	④-1		○
	④-2		○
	④-3		○
	④-4		○
	④-5		×
④- 7	④-1 ～ ④-5 の確認を、iPad で行う。	C	
	④-1		○
	④-2		○
	④-3		○
	④-4		○
	④-5		×
④- 8	④-1 ～ ④-5 の確認を、iPhone で行う。	C	
	④-1		○
	④-2		○
	④-3		○
	④-4		○
	④-5		×

④-9　④-1 ～ ④-5 の確認を、Android スマートフォン　C で行う。

④-1	○
④-2	○
④-3	○
④-4	○
④-5	×

④-1，④-2，④-3，④-4 の結果、文書閲覧アプリケーションからクリップボードへの文書のデータコピー、情報デバイスへの文書のデータコピー、情報デバイスからの文書の印刷ができないことが確認できた。

④-5 については、ハードウェアレベルの制御が必要となるため、Web アプリケーションでは画面キャプチャー機能を行えないように制御することはできなかった。

④-6，④-7，④-8，④-9 の結果、文書閲覧アプリケーションがマルチデバイス対応の Web アプリケーションかつ同等の機能を各種情報デバイスに提供できることが確認できた。

実証システムは、「システムに保管されている文書の複写を防止する」に対して画面キャプチャーが行えないように制御することを除いて機能していることが確認できた。

[結果分析]

対象業務の記録の閲覧は、閲覧申請者によって使用する情報デバイスが異なるが、どの情報デバイスであってもクリップボードへのデータコピー、情報デバイスへのデータコピー、情報デバイスからの印刷ができないことを実現できた。

ただし、情報デバイスが持つ画面キャプチャーはハードウェアレベルの制御が必要なため Web アプリケーションからは制御できていない。対応策として、ハードウェアレベルの画面印刷機能を制御するためには、文書閲覧アプリケーションを情報デバイスの基本ソフト上で稼働するアプリケーションとして開発することが考えられる。ただし、Web アプリケーションではなくなるため、情報デバイスごとにアプリケーションを開発・保守しなければならなくなる。

3.2.5 機能⑤（システムに保管されている文書の改ざんを防止する）

[実証内容]

「システムに保管されている文書の改ざんを防止する」機能について、文書管理サーバーが保管している文書のハッシュ値と文書情報管理サーバーに保管されている文書情報のハッシュ値が同一であるかどうかによって文書改ざん検知が可能であり、文書の改ざんを防止できることを確認する。

[評価方法の設定ポイント]

- 文書管理サーバーが管理している文書の真正性を確認できる。
- 改ざんされた文書を閲覧申請者に閲覧させない。
- 改ざんされた文書を改ざんされていない元の文書で上書きすれば閲覧申請者は文書を閲覧できる。

[実証の評価方法、評価観点]

表 １３：機能⑤の評価方法

No.	評価方法	評価観点
⑤-1	文書管理サーバーは文書閲覧アプリケーションに文書ファイルを送信する前に文書ファイルの真正性の確認処理（※）を行っていることを文書管理サーバーのログから確認する。 ※文書ファイルの真正性の確認処理は、対象となる文書ファイルのハッシュ値を算出し、情報管理サーバーが管理している文書情報のハッシュ値と比較する処理。	F, S, R
⑤-2	⑤-1 において、文書管理サーバーは文書情報管理サーバーが管理している文書情報（ハッシュ値含む）を都度、取得していることを文書管理サーバー、及び文書情報管理サーバーのログから確認する。	F, R
⑤-3	文書管理サーバー上の文書を意図的に改ざんする。 文書が改ざんされている場合、文書閲覧アプリケーションで、その改ざんされた文書を閲覧しようとしても、表示されないことを確認する。 また、文書管理サーバーが改ざんを検知したことを文書管理サーバーのログから確認する。	F, R
⑤-4	文書管理サーバー上の改ざんされた文書を改ざん前の元の文書で上書きした後、文書管理サーバーで文書の改ざんを検知する処理を行う。 文書が改ざんされていなければ、閲覧申請者が文書を閲覧することができることを確認する。	F, R

[評価結果]

表 １４：機能⑤の評価結果

No.	評価方法	評価観点	評価結果
⑤-1	文書管理サーバーは文書閲覧アプリケーションに文書ファイルを送信する前に文書ファイルの真正性の確認処理（※）を行っていることを文書管理サーバーのログから確認する。 ※文書ファイルの真正性の確認処理は、対象となる文書ファイルのハッシュ値を算出し、情報管理サーバーが管理している文書情報のハッシュ値と比較する処理。	F, S, R	○
⑤-2	⑤-1 において、文書管理サーバーは文書情報管理サーバーが管理している文書情報（ハッシュ値含む）を都度、取得していることを文書管理サーバー、及び文書情報管理サーバーのログから確認する。	F, R	○
⑤-3	文書管理サーバー上の文書を意図的に改ざんする。 文書閲覧アプリケーションで、その改ざんされた文書を閲覧しようとしても、文書が改ざんされているので表示されないことを確認する。 また、文書管理サーバーが改ざんを検知したことを文書管理サーバーのログから確認する。	F, R	○
⑤-4	文書管理サーバー上の改ざんされた文書を改ざん前の元の文書で上書きした後、文書管理サーバーで文書の改ざんを検知する処理を行う。 文書が改ざんされていなければ、閲覧申請者が文書を閲覧することができることを確認する。	F, R	○

⑤-1，⑤-2 の結果、文書の真正性を確認するために、文書と文書情報を別々に管理し、文書は改ざんされているかもしれないデータとして管理し、文書情報は信頼すべきデータとして改ざんが現実的に不可能なブロックチェーンにて管理する方式は正しく機能していた。

⑤-3 の結果、閲覧申請は、改ざんされた信頼性のない文書を閲覧することはないことが確認できた。

⑤-4 の結果、改ざんが検知された文書を元の改ざんされていない文書で上書きすれば、元の改ざんされていない文書を閲覧することができた。

[結果分析]

対象業務の記録の閲覧は、閲覧申請者が真正性のある文書を閲覧していることが重要であるが、本技術実証で実装した文書と文書情報を別々に管理し、改ざん検知を行う方式により、閲覧申請者は常に真正性のある文書を閲覧できることが実証できた。

3.2.6 機能⑥（閲覧申請者が閲覧している文書について、第三者による覗き見等を防止する）

[実証内容]

「閲覧申請者が閲覧している文書について、第三者による覗き見等を防止する」機能については、文書閲覧アプリケーションで閲覧中の文書を覗き見する、写真撮影をする、書き写そうとする違法な第三者への情報提供の防止対策が機能するか確認する。

[評価方法の設定ポイント]

文書閲覧アプリケーションの覗き見防止機能により、スマートフォンなどのカメラでの画面撮影、筆記具による文書の謄写、第三者による文書の覗き見を情報デバイスのカメラ画像から検知する。

[実証の評価方法、評価観点]

表 １５：機能⑥の評価方法

No.	評価方法	評価観点
⑥-1	文書閲覧が可能である状態で、覗き見されているかどうかを、カメラ画像を AI 解析により確認する。	F
⑥-2	文書閲覧が可能である状態で、スマホ等のカメラで撮影されているかどうかを、カメラ画像を AI 解析により確認する。	F
⑥-3	文書閲覧が可能である状態で、ペンで書写しを行っているかどうかを、カメラ画像を AI 解析により確認する。	F

[評価結果]

表 １６：機能⑥の評価結果

No.	評価ポイント、評価方法	評価観点	評価結果
⑥-1	文書閲覧が可能である状態で、覗き見されているかどうかを、カメラ画像を AI 解析により確認する。	F	○
⑥-2	文書閲覧が可能である状態で、スマホ等のカメラで撮影されているかどうかを、カメラ画像を AI 解析により確認する。	F	○
⑥-3	文書閲覧が可能である状態で、ペンで書写しを行っているかどうかを、カメラ画像を AI 解析により確認する。	F	△

⑥-1 の結果、文書閲覧アプリケーションの画面を第三者が覗き見していることを検知できた。

⑥-2 の結果、文書閲覧アプリケーションの画面に表示されている文書を閲覧申請者が写真撮影する行為を検知できた。

⑥-3 の結果、文書閲覧アプリケーションの画面に表示されている文書を閲覧申請者が筆記具にて書き写す行為は、検知精度が低くカメラにペンを写しても無反応な場合が多かった。

[結果分析]

⑥-1,⑥-2 の評価結果から情報デバイスのカメラの画像データを AI 解析することで、文書閲覧アプリケーションに表示されている文書の覗き見、写真撮影を防止することで違法な第三者への情報提供を防止することができることが確認できた。

⑥-3 の評価結果から、実証システムの現時点での AI による画像解析では筆記具の検知精度が低く、違法な第三者への情報提供を防止することは困難であった。

実証の結果、情報デバイスのカメラを使用する監視方法には、表 17 のような問題を認識することができた。

表 １７：情報デバイスのカメラによる監視方法の問題

No.	問題点	内容	解決案
1	外部モニター出力	情報デバイスの画面が別のモニターなどに出力されている場合、そのモニターを見ている人物は検知不可能である。	360 度カメラを使用するという制約を設けられるのであれば、同室の外部モニターは検知できるが、別室であれば検知できないので有効度は下がる。 外部モニターに繋がるケーブルの検知も考えられるが、ワイヤレス接続の場合は検知できない。 360 度カメラの接続検知はハードウェアであるため難しいが、送られてくる画像データを解析することで 360 度カメラであるどうかは判別可能と考えられる。
2	筆記具の検知	技術実証時では筆記具の検知精度が低く、カメラにペンを写しても無反応な場合が多い。	AI の学習により解決可能と考えられる。 学習に必要なデータ量は、AI に画像内に筆記具があるかどうかを識別させ、識別結果がシステム要件で許容されるまで繰り返すため未定である。
3	筆記具の位置	筆記具などは手元にあることが多く、情報デバイスのカメラの範囲外で写らないことが多いと考えられる。	360 度カメラを使用するという制約を設けられるのであれば手元でも検知可能である。
4	メモ書き	筆記具の使用が書き写しであるのか、メモ書きなのかの判断が難しい。	AI の学習により、書き写しかメモ書きかを判断ができると考えられる。 AI による人の行動分析では、次のようなものがある。 ● 物体検出とトラッキング：ペンやノートなどの物体を検出し、その位置や動きを追跡することで、何に注意を払っているかを判断する。 ● 行動のパターン認識：特定の行動パターンを学習し、メモを取るときの特有の動作や手順を検出し、文書を書く行為とメモを取る行為を区別する。
5	閲覧申請者の真正性	カメラに写っている人物が閲覧申請者本人であるかが不明である。 2 名以上であれば覗き見と検知するが、1 名であれば判断していない。	本人の顔認証をする必要がある。 閲覧申請時に顔写真もしくは顔写真データを取得し、ユーザー情報とすることで対応可能と考えられる。

3.2.7 まとめ

機能①～⑥の評価結果は、以下のとおり整理できる。いくつかの機能については課題がある。実際に、実証システムのようなシステムを活用して、オンラインで閲覧申請者本人のみに適切に情報開示が可能となるシステムを構築し、対象業務における立会人による監視を不要にした場合には、閲覧申請者が使用する情報デバイスが所管省庁の管理下になく、またソフトウェアでは制御不可能な情報デバイスのハードウェア機能、及び任意の周辺機器との接続が可能であるため、第三者に情報が利用される可能性がある点には留意すべきである。

文書の閲覧に使用する情報デバイスには、任意の周辺機器を接続しないこと、画面キャプチャーを行わないことを閲覧申請者に承諾させた上、文書の閲覧を許可する必要がある。

機能	評価結果	課題と対応策
機能①（閲覧申請者が任意の情報デバイスからインターネット経由で利用できる）	○	特になし
機能②（閲覧申請者のみに文書を閲覧させる）	△	文書閲覧アプリケーションの最後の操作から無操作状態が続く場合、一定時間で実証システムのサーバーとの接続が切断されるように設定したが、検証時には切断されず文書閲覧アプリケーションを使い続けることができた。 実証後の調査で本人認証サーバーの設定では正しく動作しないことが判明した。よって、文書閲覧アプリケーションの機能として実装することで問題は解決できると判断した。
機能③（閲覧申請をした文書のみを閲覧申請者に閲覧させる）	○	特になし
機能④（システムに保管されている文書の複写を防止する）	△	ハードウェア制御による画面キャプチャー機能による複写は、管理下にない情報端末では防ぐことができない。

機能⑤（システムに保管されている文書の改ざんを防止する）	○	特になし
機能⑥（閲覧申請者が閲覧している文書について、第三者による覗き見等を防止する）	△	筆記具が Web カメラの死角にある場合や、情報デバイスに接続された外部モニター等がある場合に、それらを認識することができないため、第三者による覗き見等を完全に防止することはできない。

3.3　実証システムの活用に関する所見

3.3.1デジタル代替の可能性

技術実証の対象業務のデジタル代替には、次に挙げる４つの機能が必要である。

- デジタル化された文書の改ざんを防止する機能
- 閲覧申請者に許可した文書だけを閲覧申請者本人に閲覧させる機能
- 閲覧申請者による文書の複製を防止する機能
- 違法な第三者への情報提供、及び情報漏洩を防止する機能

デジタル化された文書の改ざんを防止する機能に関しては、文書管理サーバーが使用している KeepData が文書データを暗号化し、複数のファイルシステムに分割管理することで文書本体を安全に保管する技術、並びに文書情報管理サーバーが文書データの改ざんを検知するための文書のハッシュ値を改ざん不可能なブロックチェーンに保管する技術は、本技術実証で有効であったことからデジタル代替は可能である。

閲覧申請者に許可した文書だけを閲覧申請者本人に閲覧させる機能に関しては、文書識別サーバーが閲覧申請者に対する閲覧の許可を唯一無二の許可証として NFT を発行し、改ざん不可能なブロックチェーンに保管する技術、並びに閲覧申請者の本人認証が行われた文書閲覧アプリケーションから閲覧申請者の所有する NFT を使用した文書のリクエストに対して文書を表示する技術が本技術実証で有効であったことからデジタル代替は可能である。

閲覧申請者による文書の複製を防止する機能に関しては、文書閲覧アプリケーションでは文書データの保存を防止する機能、文書の印刷を防止する機能を実装しており有効であるが、文書閲覧アプリケーションの画面に表示されている画像データのコピー機能（画面キャプチャー）は、情報デバイスの OS レベルで組み込まれており、アプリケーションから完全に制御することはできない。よって、文書の複製を防止することは、閲覧申請者が任意の情報デバイスを使用する状況ではデジタル代替の可能性は確定的ではない。

違法な第三者への情報提供、及び情報漏洩を防止する機能に関しては、文書閲覧アプリケーションは、情報デバイスに付随するカメラから入力される画像データを AI で解析し、閲覧申請者による文書表示画面のカメラ撮影、筆記具による文書の書き写し、及び第三者による覗き見を検知し、文書表示画面を遮断する機能は有効であるが、筆記具による書き写しはカメラの死角で行われることも多く、また画像に入っていてもそれがメモ書き程度であるのか、その程度を判断するのは困難であり、360 度カメラを必須として死角をなくすことや、筆記具で書いている内容の解析などが必要となってくる。さらに、情報デバイスに複数のモニターを接続していて画面を複製表示している場合、そのモニターを見ている第三者への情報提供を防止することができない。よって、違法な第三者への情報提供、及び情報漏洩を防止することは、閲覧申請者が任意の場所で任意の情報デバイスを使用する状況では、デジタル代替することは難しい。

結論として、対象業務をデジタル代替することは、閲覧申請者が任意の場所から任意のデバイスを使用して行うことからセキュリティの観点で難しいが、地方自治体等の公共施設内に設置した 360 度カメラを接続した情報デバイスで文書の閲覧を行う等であれば可能である。

3.3.2費用対効果

対象業務による文書の閲覧申請数が 1 年間に多くても数件であり、閲覧申請者の移動にかかる時間と費用、公害等調整委員会の立会人がその立会いに要する時間、及びシステム構築費用・運用・保守費用から、対象業務のデジタル化は、デジタル化による利便性から閲覧申請件数が増加したとしても費用対効果は低いと考えられる。

システムの運用・保守で運用時間を平日の日中のみに制限すれば、2 人態勢で年間合計 12 人月程度であるが 365 日 24 時間稼働であれば 7 人態勢で年間 24 人月程度となる。

3.3.3他の法令や規制への活用の可能性

対象業務は文書の閲覧に申請とその許可が必要であり、指定された場所で文書の閲覧をするものであるが、同様に法令により文書に申請と許可が必要なアナログ業務は多数ある。 令和 6 年 2 月現在の e-Gov 法令検索において、「閲覧」で検索した結果、1,227 件がヒットし、「調書」で検索した結果、396 件がヒットした。また、「記録の閲覧」もしくは「記録を閲覧」で検索すると合計 85 件ヒットし、「調書の閲覧」もしくは「調書を閲覧」で検索すると合計 54 件ヒットした。ヒットした全ての法令や規制を確認していないが、記録の閲覧申請、指定された場所と時間で閲覧する法令がいくつか確認でき、それらの法令に本技術実証において検証した技術を活用することは可能ではないかと考えられる。

また、本技術実証で使用した技術では、デジタルデータの改ざん検知の方式、NFT による許可証のデジタルデータ化などは他の法令や規制に活用可能な技術である。

例えば、機能②（閲覧申請者のみに文書を閲覧させる）では、本技術実証で使用した本人認証機能は、現在の一般的な業界標準的技術を採用しており、他の法令、規制において本人認証が必要なシステムでは、スマートフォンなどの認証の対象となる人物が所有する身近な情報デバイスを用いた本人認証が簡易な方法で高精度に行えるため有用だと考えられる。

また、機能⑤（システムに保管されている文書の改ざん防止）で使用している公開するデータのハッシュ値を公開データとは物理的に別の場所に保管し、それらをデータの利用時に突合させることでデータの改ざんを検知する技術は、データの真正性の確認が必要な業務に関して、汎用的に多くの法令や規制に対して活用可能である。

用語集

用語	定義・解説
AI 解析	AI 解析は、人工知能がデータを分析し、パターンを抽出して情報を生成するプロセスである。 本技術実証では、情報デバイスのカメラで取得した画像を AI 解析を使用し、画面の覗き見とスマートフォンの写り込みを判断している。
Amazon Web Services	Amazon 社が提供するクラウドサービス。
ASP 形式	ASP は、Application Service Provider の略称で、ASP 形式は、ASP によってインターネットを経由して提供されるソフトウェアサービスもしくはソフトウェア稼働環境。
Google Authenticator	Google 社が提供する多要素認証アプリケーション。
HTTP リクエスト	Web ブラウザや Web アプリケーションが Web サイトに情報をリクエストする際に Web サイトのサーバーに送るメッセージ。
ID/PW 認証	固定の ID と PW を使用したユーザー認証。
iframe	Web ページを構成する HTML のタグの一つ。 Web ページの中に別の Web ページを埋め込み、表示させるために使用する。
Keycloak	オープンソースの Red Hat が提供しているアクセス管理のためのプラットフォームで、ユーザーの認証、認可、シングルサインオン、多要素認証などを統合管理するために使用する。
NFT	NFT（Non-Fungible Token）とは、代替不可能なトークンのことである。代替不可能なトークンとは、唯一無二の「一点物」の価値を生み出せるトークンという意味である。 また、デジタルデータに唯一性を与えることができる NFT は、ゲーム以外にも会員権や不動産の所有の証明、著作権やアートなどさまざまな分野で実用化が進んでいる。 本技術実証では、閲覧申請者に付与される文書の閲覧許可として使用している。
OpenID Foundation	オープンで標準化されたアイデンティティ管理プロトコルを推進する非営利組織。主なプロトコルには OpenID Connect や OAuth が含まれる。

OTP	One Time Password の略で、一度だけ使用できるパスワードで指す。セキュリティの向上や認証プロセスの強化のために使用される。ユーザーがログインやトランザクションを行う際に、都度異なるパスワードが生成され、これにより不正アクセスやパスワードの漏洩のリスクを低減する。OTP はさまざまな形態で提供され、テキストメッセージ、ハードウェアトークン、ソフトウェアアプリケーション、電子メール、及び他の手段を使用して生成されることがある。 本技術実証では、Google が生成した OTP を Google Authenticator で受信している。
OTP 認証	OTP を使用したユーザー認証。
Web アプリケーション	Web ブラウザーを介してアクセスし、ユーザーに様々な機能やサービスを提供するソフトウェア。データの入出力や処理はサーバー上で行い、ユーザーはブラウザーを通じて直感的な画面を利用して情報にアクセスし、操作する。 本技術実証の文書閲覧アプリケーションは Web アプリケーションとして開発した。
Web ブラウザー	インターネット上の Web ページを閲覧するためのソフトウェア。ユーザーが URL を入力、もしくはリンクをクリックし、Web ページを表示し、テキスト、画像、動画などのコンテンツを表示する。Web ブラウザーは HTML や CSS などの言語を解釈し、ユーザーが直感的に操作できる画面を提供する。主なブラウザーには Google Chrome、Mozilla Firefox、Microsoft Edge などがある。
アイドルタイムアウト	デバイスやアプリケーションが一定期間活動していない場合に、自動的にセッションを終了する仕組み。
アクセストークン	ユーザーがアプリケーションやウェブサービスにアクセスする際の認証情報で、一時的に発行されるトークン。このトークンは、ユーザーが認証を通過したことを示し、アプリケーションがユーザーのデータやサービスにアクセスするために使用される。
アプリケーションサーバー	クラウド上のコンピュータで稼働するアプリケーションの実行や処理を行うサーバーソフトウェア。クライアントソフトウェアのリクエストを受け、それに応じて動的なコンテンツを生成する。また、一般的な機能としてデータベースへのアクセス、セッション管理、セキュリティ機能なども含む。
インターフェース	システムやデバイス同士、あるいはユーザーとシステム間で情報や操作が交換される接点、もしくは手段である。インターフェースは、相互に異なるもの同士が効果的に連携できるように設計され、相互作用を可能とする。

オペレーティングシステム	コンピュータを動作させる基盤のソフトウェア。 本技術実証で使用する情報デバイスもコンピュータである。
識別子プロバイダー	Keycloak が利用する多要素認証のプロバイダー。本技術実証では、Google を使用している。
真正性	物事や情報が本物であり、その信頼性と信用性があること。 例えば、デジタル署名や認証手段を使用して、データやメッセージの真正性を保証することがある。真正性は、信頼できる情報や製品の提供、セキュリティの確保に重要な役割を果たす。
スマートコントラクト	ある契約・取引について「特定の条件が満たされた場合に、決められた処理が自動的に実行される」といった、契約履行管理の自動化を指す。
多要素認証	複数の手法（パスワード、デバイス、生体情報）を組み合わせてアクセスを許可。これにより、単一認証の弱点を補い、不正アクセスやデータ漏洩リスクを低減。オンラインサービスや企業で広く導入されている。
ハッシュ値	任意の長さのデータからハッシュ関数により生成される一定長のバイナリまたは文字列。異なるデータに対して固有で、逆引きが難しく、主にセキュリティやデータ整合性の確認に利用される。
プライベートブロックチェーン	一般に公開されておらず、限定された人しかアクセスできないブロックチェーンでブロックチェーンを管理する組織もしくは人により設けられる。
ブロックチェーン	データを保持するブロックをチェーンで繋ぎ、複数のサーバーで同一のコピーを分散して保有する仕組み。 ブロックのハッシュ値を次のブロックのデータの一部として持ち繋いでいくため、データの改ざんが極めて難しく、さらに分散されたサーバー間でブロックの真正性を確認するため、一つのサーバーのデータの改ざんに成功しても、改ざんされたサーバーの信頼性は失われる。
文書情報	本技術実証において、文書情報は、文書番号、文書名、法令、所管府省庁、文書のハッシュ値から構成されるデータである。 文書管理システムでは、文書番号、文書名、法令、所管府省庁、文書ファイル名を属性として持っているが、文書情報管理システムでは、文書ファイル名以外の属性及び文書のハッシュ値を文書情報としてブロックチェーンに格納している。