【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の概要】

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 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
実証の全体像	**実証の方針** ● 任意のPC、タブレット端末、スマートフォン等の情報デバイスからインターネットを利用して、デジタル化された文書を閲覧申請者に対してのみ閲覧申請部分を閲覧させ、複写・改ざんさせない。 ● 任意の情報デバイスから閲覧可能とするが、閲覧情報の目的外利用や違法な第三者への提供を防止する。 **実証事項** 本技術実証のために開発した文書閲覧用のシステム（以下、実証システム）によって、指定した場所において立会人監視下で行われている記録等の閲覧業務（図2）に関して、以下の事項を実現できるか確認する。 ● 文書の閲覧を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からインターネットを利用して、閲覧申請者に閲覧を許可した文書だけを、閲覧申請者本人だけに閲覧させ、文書の複写や改ざんを防止する。 ● 文書閲覧アプリケーションで閲覧した文書の目的外利用や違法な第三者への提供を防止する。

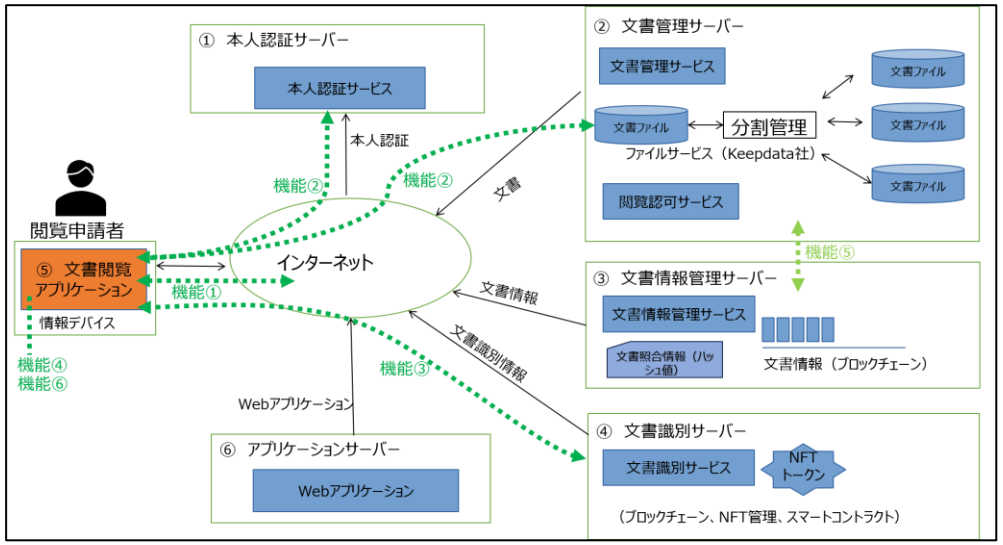


図1: 実証システム全体像

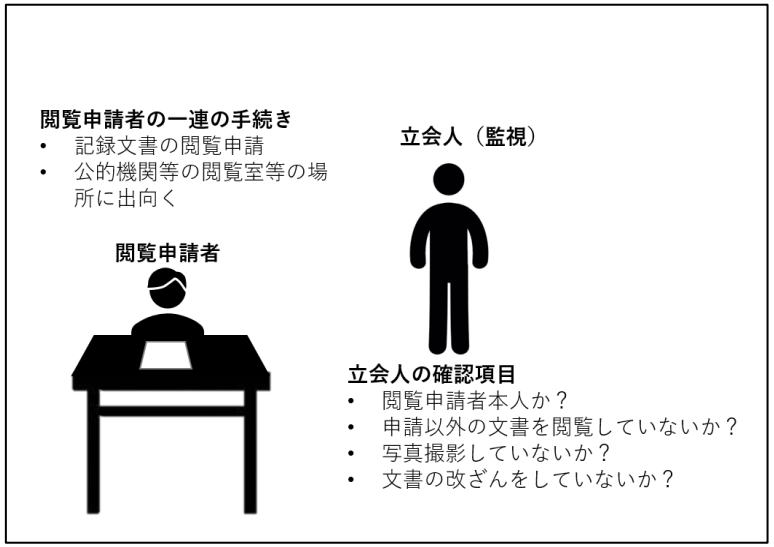


図2: 現状の業務

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の概要】

	事業者名	実施業務・役割
実施体制	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
実施期間	2023年10月2日～2024年2月16日	

※ **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のように繋ぎ、複数のサーバーで同一のコピーを分散保有する仕組みで、データの改ざん耐性が高いデータベース。

※ **NFT**
　Non-Fungible Tokenの略称で、代替不可能な唯一無二の「一点物」の価値を表すデータのトークン。
　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。

※ **スマートコントラクト**
　ブロックチェーンに保存されたプログラムであり、所定の条件が満たされた場合に実行される。
　本技術実証では、NFTの作成、及び付与等に使用している。

※ **マルチデバイスアプリケーション**
　複数のコンピュータ、タブレット端末、スマートフォンなどの情報端末に対応するように作成されたアプリケーションプログラム。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の詳細】

<table>
<tr><td rowspan="7">技術実証の方法</td><td colspan="2">技術実証の実証事項を以下の6つの機能に分割し、機能ごとの評価方法に機能性、信頼性、セキュリティ、互換性の観点から複数の評価項目を設定して実証を実施した。
※P1の図1の機能①～⑥の点線は、これらの機能が実証システムのどのサーバーと関連しているかを表している。</td></tr>
<tr><th>実証機能</th><th>実証内容</th></tr>
<tr><td>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）</td><td>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。</td></tr>
<tr><td>機能②（閲覧申請者のみに文書を閲覧させる）</td><td>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、ユーザー名とパスワード（以下、ID/PW）、及びワンタイムパスワード（以下、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。</td></tr>
<tr><td>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）</td><td>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。</td></tr>
<tr><td>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）</td><td>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、及び保存を制限し、文書の複写を防止できることを確認する。</td></tr>
<tr><td>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）</td><td>文書管理サーバーがKeepdataから取得した文書から算出した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。</td></tr>
<tr><td>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）</td><td>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。</td></tr>
</table>

※多要素認証：
複数の要素により行う認証方法。要素には、ID/PWのような知識情報、OTPやICチップなどの所持情報、指紋や顔などの生体情報がある。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の詳細】

実証場所①	実証事業者社員による遠隔場所

実証システムを Amazon Web Services クラウド上に構築し、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。

- 実施した技術実証項目：全ての技術実証機能
- タイムスケジュール：12月1日～12月27日

実証場所②	公害等調整委員会事務局の会議室

Amazon Web Services クラウド上に構築された実証システムを使用し、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。

- 実施した技術実証項目：全ての技術実証機能に関して、実証システムで確認できるもの。
- タイムスケジュール：12月5日 10:00～11:30

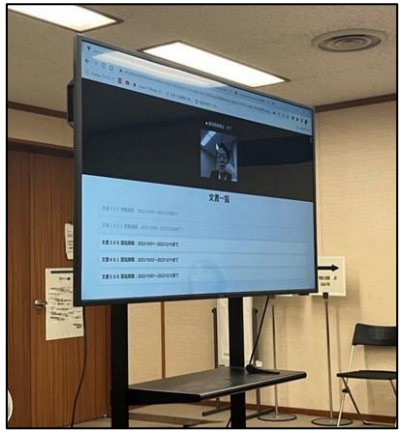


図3:公害等調整委員会事務局でのデモ

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】

評価の観点	**観点**	**観点内容**
	機能性	● 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。
	信頼性	● 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。
	セキュリティ	● 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。
	互換性	● 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。
評価のポイント・方法	技術実証を次の6つの機能に分割し、機能ごとの評価方法の設定ポイントと複数の評価項目を設定して実証を実施した。 技術実証の機能①～⑥の6つの機能の評価方法の設定ポイント、及び評価項目は次ページ以降に順に掲載する。	

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　1/2

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。	
評価項目	**番号**	**評価項目**
	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。
	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。
	①-3	WindowsPC で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。
	①-4	①-1～①-3の評価項目をMacPCで行う。
	①-5	①-1～①-3の評価項目をiPadで行う。
	①-6	①-1～①-3の評価項目をiPhoneで行う。
	①-7	①-1～①-3の評価項目をAndroidスマートフォンで行う。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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） 2/2

実証の実施結果	評価項目の評価結果
	すべての評価項目の確認ができた。
	実証結果
	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が確認できた。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 機能②（閲覧申請者のみに文書を閲覧させる） 1/2

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。	
評価項目	**番号**	**評価項目**
	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。
	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。
	②-3	間違ったOTPでOTP認証されないことを確認する
	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。
	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。
	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。
	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。
	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。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 機能②（閲覧申請者のみに文書を閲覧させる） 2/2

実証の実施結果

評価項目の評価結果

評価項目②-8（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）のみ確認できなかった。

実証結果

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可能であることを確認できた。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が確認できた。

図4:多要素認証

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。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　1/2

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。	
評価項目	**番号**	**評価項目**
	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を検索し、検索結果の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。
	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。
	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。
	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。
	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対して送信した文書情報の真正性を確認し、改ざんされていないことを確認しているか文書識別サーバー、及び文書情報管理サーバーのログから確認する。
	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。
	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。
	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。

【技術実証の結果】 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）　2/2

実証の実施結果	評価項目の評価結果
	すべての評価項目の確認ができた。
	実証結果
	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を確認し、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と確認できた。

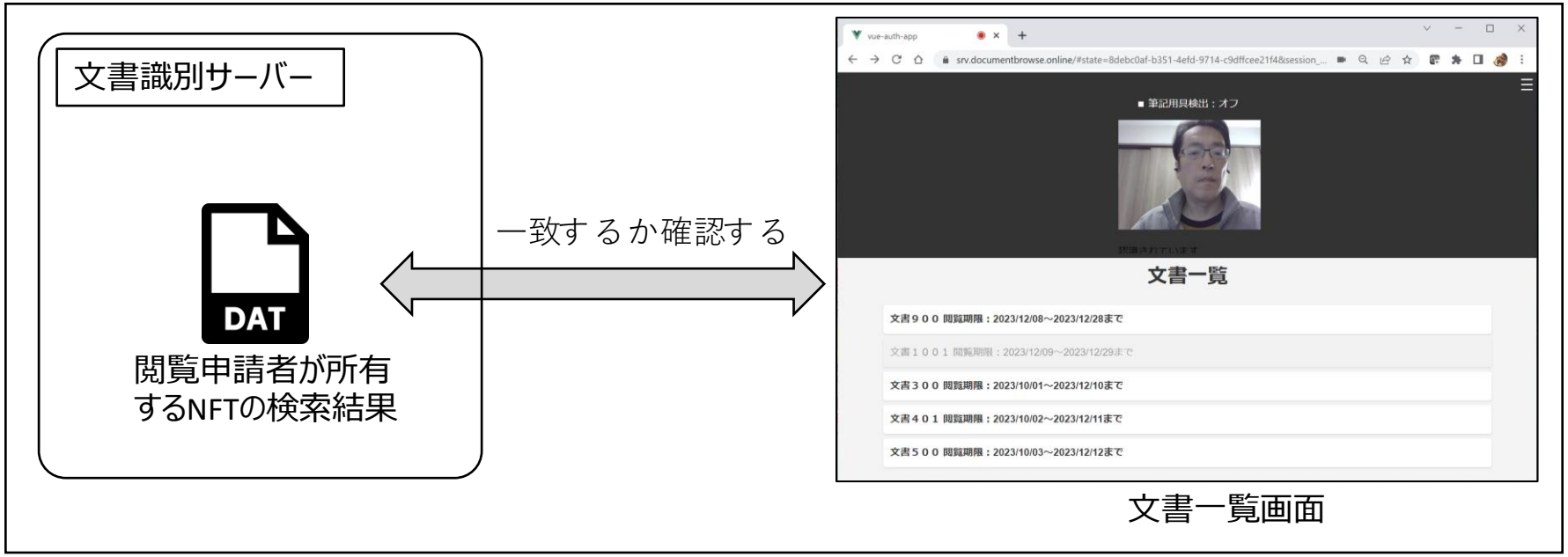


図5:NFTと文書一覧画面の内容確認

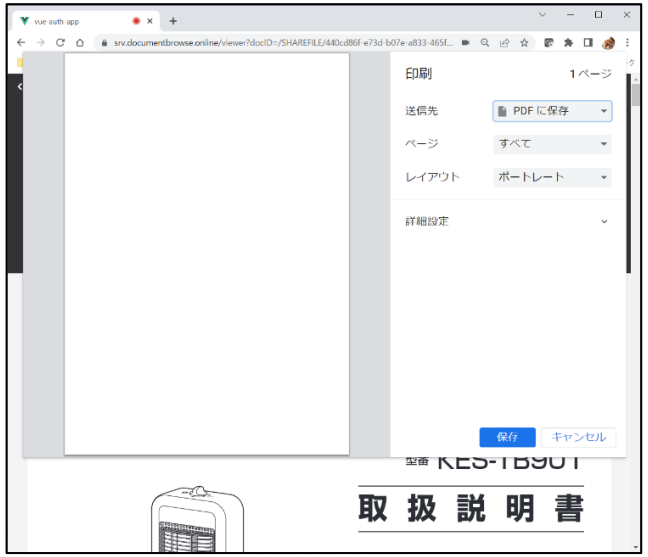
【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　1/2

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、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、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、保存を防止することができる。	
評価項目	**番号**	**評価項目**
	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。
	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。
	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。
	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。
	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。
	④-6	④-1～④-5の評価項目を、MacPCで行う。
	④-7	④-1～④-5の評価項目を、iPadで行う。
	④-8	④-1～④-5の評価項目を、iPhoneで行う。
	④-9	④-1～④-5の評価項目を、Androidスマートフォンで行う。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　2/2

実証の実施結果	評価項目の評価結果
	評価項目④-1～④-4までと、これらの評価項目に対応する他の情報デバイスの評価項目④-6、④-7、④-8、④-9は確認ができた。 評価項目④-5と、この評価項目に対応する他の情報デバイスの評価項目④-6、④-7、④-8、④-9は確認できなかった。
	実証結果
	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、及び保存を制限し、文書の複写を防止できることが確認できた。  図6:文書の印刷防止による文書の白紙化 文書は閲覧できるが、印刷をすると文書は白紙として印刷された。 また、文書を保存しても内容が空白の文書として保存された。 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。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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） 1/2

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。	
評価項目	**番号**	**評価項目**
	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。
	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。
	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。
	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。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　2/2

実証の実施結果	評価項目の評価結果
	すべての評価項目の確認ができた。
	実証結果
	文書管理サーバーがKeepdataから取得した文書から算出した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が確認できた。

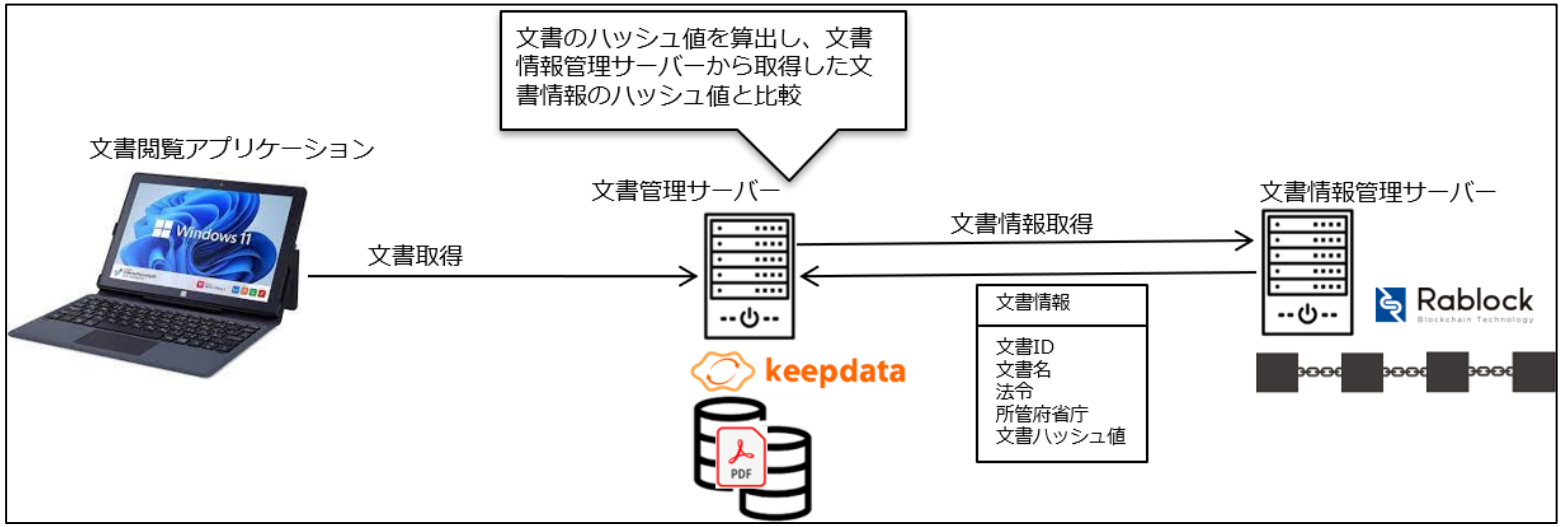


図7: 文書の改ざん検知

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　1/2

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。	
評価項目	**番号**	**評価項目**
	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。
	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。
	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。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果】 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）　2/2

実証の実施結果

評価項目の評価結果

評価項目⑥-1、⑥-2の確認ができた。
評価項目⑥-3で、筆記具の検知精度が低く、検知できない場合が多かった。

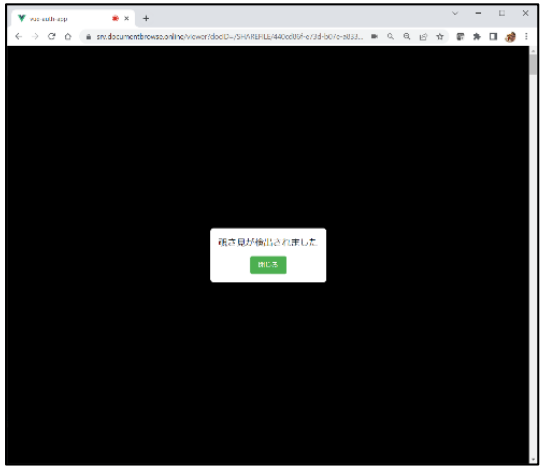
実証結果

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は概ね確認できたが、違法な第三者への情報提供の防止対策に対して十分ではなかった。

文書閲覧画面

覗き見を検知

実証では、概ね1秒以内に文書閲覧画面を遮断した。



文書閲覧画面を遮断

図8：覗き見を検知した場合

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の評価結果】

実証の評価結果	技術実証機能	評価結果
	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）	文書閲覧アプリケーションは任意の情報デバイスで稼働し、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。
	機能②（閲覧申請者のみに文書を閲覧させる）	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。 評価項目②-8（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）が機能せず確認できなかったが、事後調査で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ず、文書閲覧アプリケーションにタイムアウト処理を追加実装することで解決できることが判明した。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。
	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）	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。
	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）	アプリケーションの制御によりシステムに保管されている文書の複写を防止することができた。
	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）	文書の改ざん検知機能は有効に機能した。
	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）	情報デバイスに付属しているカメラから画面を第三者による覗き見、閲覧申請者による画面の写真撮影する行為や筆記具にて書き写す行為を検知することができ、第三者への情報提供を防止する対策として有効であることが確認できた。

※KeyCloak：
Cloud Native Computing Foundationが公開しているID管理やアクセス管理を実現するオープンソースソフトウェア

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果分析】 1/2

実証の結果分析

実証結果から合計39個の評価項目のうち、36個が有効に機能しており、本技術実証で使用した技術が対象業務をデジタル化するために十分に有効であると判断できた。
機能①～⑥の結果分析を以下のように要約した。

技術実証機能	分析	分析結果内容
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）	○	情報デバイスのOSに依存せず、Webブラウザーに依存して稼働しているアプリケーションにより、任意の情報デバイスでインターネットを利用した文書の閲覧を可能としている。 文書を閲覧する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、正常に動作しなくなるわけではない。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。
機能②（閲覧申請者のみに文書を閲覧させる）	△	ID/PWとOTPによる2要素で認証精度は高いと考えられる。より精度の高い本人認証が必要な場合には、顔認証や指紋認証などの生体認証を追加することも可能である。 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）	○	管理できない情報デバイスを信用せず、送信されてきたデータの真正性を確認することで閲覧申請者に許可された文書を閲覧申請者にだけ閲覧させることができている。

【類型13 株式会社テクノロジックアート】技術実証　最終報告サマリー

【技術実証の結果分析】2/2

実証の結果分析	技術実証機能	分析	分析結果内容
	機能④：実証システムに保管されている文書の複写防止機能	△	情報デバイスが異なっていても、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が、情報デバイスが持つ画面印刷機能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。
	機能⑤：実証システムに保管されている文書の改ざん防止機能	○	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り、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だけを閲覧できる。
	機能⑥：第三者による覗き見等の防止機能	△	情報デバイスのカメラ画像をAIにより解析することで、文書の覗き見、写真撮影、書き写しの検知をおこなうことで、違法な第三者への情報提供を防止する機能は概ね有効であったが、筆記具の識別精度が低く、書き写しを防止することにはあまり有効ではなかった。また、カメラの死角となる場所の行為は判断できない点に問題があると認識できた。 **物体検知ミスの対応策**として、AIの学習により筆記具の検知精度を上げることは可能と考えられるが、学習に必要なデータ量は、AIに画像内の物体が何であるかを識別させ、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。 **死角の対応策**として、死角への対応は文書閲覧アプリケーションの稼働要件に360度カメラが接続されている情報デバイスであることを加えることが考えられる。