"「日本版ｅシール」の社会実装に向けた実証実験"報告書

２０２５年３月

株式会社帝国データバンク
富士通株式会社

目次

1. 実証実験概要 4
1.1. 背景 4
1.2. 目的 6
1.3. 参加組織 7
1.4. 日本版ｅシール概要 9
1.4.1. ｅシール 9
1.4.2. 日本版ｅシール想定 11
1.4.3. 組織識別子 12
1.4.4. トラストサービス 13
1.4.5. 参照する公表資料 14
2. 実証実験（PoV　2022-2023 年度、PoC　2024 年度） 15
2.1. 実証環境 15
2.2. システム構成 16
3. 実証結果と課題（PoV　2022-2023 年度） 17
3.1. ローカルｅシール（2022 年-2023 年） 17
3.2. リモートｅシール（2022 年-2023 年） 19
3.3. ファイル送受信とｅシール検証（2022 年-2023 年） 24
3.4. タイムスタンプ（2022 年-2023 年） 26
3.5. ｅシールおよび適格請求書発行事業者登録番号検証と自動振分（プロトタイプ 2022 年-2023 年） 27
4. まとめと提言（PoV　2022-2023 年度） 34
4.1. ｅシールの有用性、ユーザビリティおよび普及させていくための検討事項 34
4.2. サービス連携 35
5. 実証結果と課題（PoC　2024 年度） 38
5.1. 実証目的と結果：外部 IdP を利用したリモートｅシール付与（2024 年度） 38
5.1.1. セイコーソリューションズ株式会社による実証実験 40
5.1.2. 株式会社スカイコムによる実証実験 52
5.1.3. 株式会社ハートビーツによる実証実験 58
5.2. 課題：外部 IdP を利用したトラストサービス連携（2024 年度） 62
6. 提言(2024 年度) 64
6.1.1. 基準に関する提言 64
6.1.2. 制度に関する提言 66
6.1.3. サービス連携に関する提言 68

改訂履歴

版	内容概略	公表日付
初版	日本版 e シールの社会実装に向けた価値実証実験(PoV)中間報告書として公表。	2022/11/09
第 2 版	日本版 e シールの社会実装に向けた価値実証実験(PoV)報告書として公表。	2023/06/30
第 3 版	日本版 e シールの社会実装に向けた実証実験(PoC)報告書として公表。 第 5 章　実証結果と課題（PoC　2024 年度）を追記 第 6 章　提言（2024 年度）を追記	2025/03/24

1. 実証実験概要

1.1. 背景

新型コロナウイルス感染症の数次にわたる流行拡大を機に、我が国でもテレワークが一定の定着を見ることができた。一方で押印手続だけのために出社を余儀なくされるなど、紙処理に関する課題も浮き彫りになり、インターネットを通じて官民や民間同士の様々なやり取り、特に企業においては取引により発生する納品書や請求書・領収書など、紙ベースで構築された処理の更なるペーパーレス化が必要とされている。

ペーパーレス化は徐々に浸透しているが、紙をデータに置換した際に必要となる「送信元のなりすましや電子データの改ざん、ねつ造等を防止する手段であるトラストサービス」が今後重要な役割を果たすと期待されている。

現在、デジタル文書の真正性証明として「電子署名」や「PDF パスワード」などにより、文書作成者の証明や文書自体の改ざん防止が行われている。当該方式では文書作成者個人の証明や改ざん防止は可能だが、一方で企業・組織が発行した文書であるという組織による真正性を証明するための裏付けや法的な枠組みがないという課題がある。

電子メールやファイル共有サービスにおいてファイルが共有される場合においても、受信時点では相手先が相応に確認できているとしても、一度電子メールや共有サービスから外れたデータは発行元が不明となる。データに発行元が記載されていても当該記載は証明されたものとは言えず、改ざんやなりすましが可能である。送信元が悪意の第三者である場合は、損害を被る可能性も否定できない。

電子データの発行元証明が重要であることは認識されている。デジタル庁「データ戦略推進ワーキンググループ[1]」のもとに設置された「トラストを確保した DX 推進サブワーキンググループ」で取り纏められた「トラストを確保した DX 推進サブワーキンググループ報告書[2]」にて以下が記載されている。

> 『トラストを確保した DX 推進サブワーキンググループ報告書』の「6.まとめ」から引用
> *例えば、「認定スキームの創設」については、実態調査や有識者ヒアリングから、オンライン取引・手続において、発行元に関する証明のニーズが高まると想定されることが示されたため、e シールの制度化が検討されることになった。*

業務における各種データ処理の「自動化・効率化・即時化」実現の観点から「トラストサービス」を援用し、データの真正性確認（発行元確認・改ざん有無確認）を「自動的・効率的・即時的」に

[1]デジタル社会推進会議令第 4 条の規定に基づき、デジタル社会の形成に資するデータ戦略を推進するため、データ戦略推進ワーキンググループを開催

[2]「トラストを確保した DX 推進サブワーキンググループ報告書」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf

実施可能であることの実証実験（PoV : Proof of Value、価値実証、以下 PoV）を 2023 年に実施した。

また、PoV 実施後の 2024 年度は「リモート e シール付与」の実証実験（PoC : Proof of Concept、以下 PoC）を実施した。

本報告書は、PoV および PoC 双方の内容を記載している。

1.2. 目的

デジタル文書の発行元に関する真正性を証明する「e シール」の社会実装に向けた実証実験を行う。本実証実験では富士通株式会社（以下、富士通）のデジタルトラスト技術と外部認証機関として株式会社帝国データバンク（以下、TDB）の企業の存在証明に関するナレッジを用い、トラストプラットフォームを構築し検証を実施する。

検証においては、2023 年では複数企業間での実業務を想定し「日本版 e シール」を付与したデジタル文書の受け渡しを実施する。具体的には、クラウドサービスやメールなどで受け渡しされるデジタル文書に、構築したトラストプラットフォームで「日本版 e シール」を付与し、その有用性を検証する。
また、2024 年からはリモート e シール実現に必要な IdP 連携を実施し、当該有用性を検証する。

検証結果として課題を抽出し検討を加えて、関係各社のみならず関係機関などに提言を行う予定である。

1.3. 参加組織

本実証実験は主体として実施する TDB と富士通が「電子データに対する e シールや電子署名の付与に関し、特定サービスに『閉じられた』環境とはせず、統一基準のもとで様々な事業者が連携・協業できる『開かれた』サービスを提供することが、より多くの利用者の利便性向上につながり、ビジネスシーンにおけるペーパーレス化を促進する」と考え、民間企業の協力先を募集[3][4]することとした。

募集にあたっては「表 1 募集要件」のとおり e シール電子証明書を発行する認証局機能のうち IA サービスを提供する社や、リモート署名サービスを提供する社など挙げている。

表 1 募集要件

募集要件（PoV） PoV 概要を理解し意義に賛同する、右記に記載するサービスを提供する企業	1) ファイル共有サービス 2) IA サービス[5] 3) リモート署名サービス[6] 4) タイムスタンプサービス 5) PDF ファイルへの電子署名・検証サービス 6) e シール用証明書発行業務に関する適合性評価を行うサービス
募集要件（PoC） PoC 概要を理解し、意義に賛同する、右記のサービスを提供する企業	1) e シールを利用した PDF ファイルへの署名・検証・ファイル共有サービス 2) IA サービス 3) リモート署名サービス

[3] “「日本版 e シール」の社会実装に向けた実証実験”参加企業募集(PoV)
https://www.tdb.co.jp/newsroom/news/dl4uo2jdf/

[4] 「リモート e シール付与」実証のお知らせ、および参加企業募集(PoC)
https://www.tdb.co.jp/newsroom/news/eimksqcoo5xz/

[5] Issuing Authority：認証局業務のうち、登録局からの指示に基づき電子証明書の発行・失効を実施

[6] 電子署名や e シールに必要な秘密鍵を外部サーバやクラウドに保管し、署名指示をリモートで実施可能な環境を提供するサービス。RSSP(Remote Signature/Seal Service Provider)

募集の結果、以下の企業が PoV または PoC へ参加することとなった。

表 2 PoV または PoC 参加組織

商号（社名 50 音順）	法人番号[7]	TDB 企業コード[8]
GMO グローバルサイン株式会社（※1）	1011001040181	981425556
株式会社スカイコム	5010501021588	986859998
セイコーソリューションズ株式会社	8040001079502	058008916
セコムトラストシステムズ株式会社	4011001040781	983278333
株式会社帝国データバンク（実施主体）	7010401018377	986700000
株式会社ハートビーツ（※2）	7011101047393	988929287
富士通株式会社（実施主体）	1020001071491	985732401

（※1）2022 年度-2023 年度の PoV 参画、（※2）2024 年の PoC から参画

なお上表に記載の他として、以下が協力を行った。

- 株式会社Ｂｏｘ　Ｊａｐａｎ（2022 年度-2023 年度）
  法人番号：9010401107327、TDB 企業コード：372010396
  協力内容：ファイル共有サービスおよびプロトタイプ開発支援
- 一般財団法人日本情報経済社会推進協会（2022 年度-2023 年度）
  法人番号：1010405009403、TDB 企業コード：981015511
  協力内容：e シール証明書の発行業務における組織確認レビュー
- 一般財団法人日本データ通信協会（2022 年度-2023 年度）
  法人番号：6013305001870、TDB 企業コード：986022411
  協力内容：e シール証明書の発行業務における組織確認レビュー
- 三菱電機インフォメーションネットワーク株式会社（2024 年度）
  法人番号：2010401059681、TDB 企業コード：200618166
  協力内容：IdP と e シールに関する検討協力

[7]法人番号は「国税庁法人番号公表サイト」で確認可能
https://www.houjin-bangou.nta.go.jp/

[8]TDB 企業コードは以下で確認可能
https://www.tdb.co.jp/service/u/1000.jsp

1.4. 日本版 e シール概要

1.4.1. e シール

総務省は 2020 年に e シールに関する検討を行うため「組織が発行するデータの信頼性を確保する制度に関する検討会[9]」を、2023 年には「e シールに係る検討会[10]」を実施した。一定基準に基づく民間認定制度の創設に向けてユースケースについて幅広く調査し、2021 年 6 月に「e シールに係る指針[11]」を、2024 年 4 月に「e シールに係る指針（第 2 版）[12]」（以下、第 2 版を「総務省指針」という）を公表した。総務省指針において、e シールは以下のとおり定義されている。

> ＜e シールの定義＞
> *「e シール」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録された情報（以下「電子データ」という。）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。*
> *一 当該情報の出所又は起源を示すためのものであること。*
> *二 当該情報について改変が行われていないかどうか確認することができるものであること。*

e シールと電子署名の違いは、総務省指針「1.2 e シールと電子署名の異同」において「e シールは発行元を証明する機能を果たす一方、電子署名は本人が電子文書を作成したこと、そして、当該電子文書に示された意思表示が当該本人によるものであることを証明する機能を果たすという点が異なる。」と言及されている。

なお総務省では 2024 年 6 月 3 日に「e シールに係る認定制度の関係規程策定のための有識者会議」の開催を公表[13]、同会議の結果を受けて 2025 年 1 月 27 日に「e シールに係る認定制度の関係規程策定のための有識者会議取りまとめ（案）」及び「e シールに係る認証業務の認定に関する規程（案）」に対する意見募集（パブリックコメント）を実施[14]した。

---

[9]総務省「組織が発行するデータの信頼性を確保する制度に関する検討会」
https://www.soumu.go.jp/main_sosiki/kenkyu/data_organization/index.html

[10]総務省「e シールに係る検討会」 https://www.soumu.go.jp/main_sosiki/kenkyu/e_seal/index.html

[11]総務省「e シールに係る指針」 https://www.soumu.go.jp/main_content/000756907.pdf

[12]総務省「e シールに係る指針(第 2 版)」 https://www.soumu.go.jp/main_content/000942602.pdf

[13]総務省「e シールに係る認定制度の関係規程策定のための有識者会議」の開催
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00212.html

[14]総務省「e シールに係る認定制度の関係規程策定のための有識者会議取りまとめ(案)」及び「e シールに係る認証業務の認定に関する規程(案)」に対する意見募集
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00232.html

なお EU では eIDAS 規則 2.0[15] Article3(25)にて、e シールが定義されている。

> *(25)'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity（「e シール」とは、データの起源と完全性を保証する為に電子データに付され又は論理的に関係している電子形式のデータをいう）。*

既に以下のような e シールの実利用も出てきている。

> ＜EU は食品類の輸入の際に適格 e シールを義務化＞
> https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=542277930
> 2022 年 3 月、欧州委員会は保健衛生・食の安全総局（DG SANTE）および欧州農業農村開発総局（DG AGRI）と共同で新しい協定に署名し、欧州連合に輸入されるすべての食品類(goods)に適格トラストサービスプロバイダー（QTSP）が発行する健康と安全のためのデジタルシーリング証明書（digital sealing certificates）を添付することを定めました。
> 欧州委員会が提供するオンラインプラットフォームである TRACES システムは、動物、動物製品、非動物由来の食品および飼料、植物の EU 域内への輸入、ならびに動物および特定の動物製品の EU 域内貿易、EU 域内輸出に必要な衛生および植物検疫証明に使用されています。
> これらの取引で適用される e シールの規格はすべて、eIDAS 規則とも呼ばれる規則（EU）No 910/2014 で定められた規格に適合しています。

一方で日本では、2025 年 3 月に総務省において日本国内での利用が想定されている e シールに係る認定制度の開始が予定されている。

[15] eIDAS 規則 2.0 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183

1.4.2. 日本版 e シール想定

総務省指針に記載された内容に基づき、特にリモート e シールに関して以下を想定した。
なおローカル e シールは EU 適格 e シールを利用しており、当該サービス提供側の仕様に基づく。

表 3 総務省指針に基づく日本版 e シール想定内容

「総務省指針」項目	本実証実験想定内容	
e シールの仕組み	公開鍵暗号基盤（PKI）を活用した方式	
e シールの方式	ローカル e シール/リモート e シール	
e シールの分類 （レベル）	レベル２：一定の技術基準を満たす e シール 技術的には発行元証明として十分機能することが確認できるもの。	
e シール用電子証明書の発行対象となる組織等の範囲	法人番号発番対象である法人。識別子として公的番号および民間番号から以下を採用（表 4 参照） ➢ 公的：法人番号 ➢ 民間：TDB 企業コード	
組織等の実在性・ 申請意思の確認の方法	実在性の確認 ●法的実在確認 ●物理的実在確認 ●組織の運営確認	第三者機関が管理するデータベース[16]
	代表者の意思の確認	申込書への代表者の押印
	代表者の在籍の確認	第三者機関が管理するデータベースと照合された電話番号を通じた代表者本人に対する当該申請の有無の確認
e シール用電子証明書の記載事項	・ フォーマットは ITU-T X.509 を使用 ・ 発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子、有効期間、公開鍵、署名アルゴリズム、e シール用電子証明書の発行者などを記載	
設備(PoV)	認証局側暗号装置	実証検証のため OpenSSL を使用
	利用者側 e シール生成装置	OSS の秘密鍵管理装置を利用
	認証局側暗号装置の管理	クラウド内で管理
	利用者側秘密鍵の管理	クラウド内で管理
設備(PoC)	参加組織であるセコムトラストシステムズの IA 及び RSSP 実証環境	
その他 （失効に係る事項）	報告書作成時点では未実装のため、詳細は省略	

[16] 総務省指針で「定期的に更新され、信頼できるデータソースとしてみなされる」と注釈

1.4.3. 組織識別子

e シールが組織の発行元証明を目的とすることから、当該組織を一意に識別可能とすることが重要である。

組織を識別する属性として商号が挙げられるが、類似商号もあり一意に特定することは難しい。そこで当該組織を一意に識別可能とする組織識別子を e シール電子証明書に格納することが考えられる。

総務省指針では、組織識別子として複数の候補が挙げられている。このうち、本実証実験では以下を利用する。

表 4 組織識別子の例

組織識別子と管理主体	概要	発番機関登録規格
法人番号[17] **管理主体** **：国税庁**	法人には、1 法人 1 つの法人番号（13 桁）が指定、個人番号（マイナンバー）と異なり、原則として公表され、自由に利用可能。 基本理念である、行政を効率化し、国民の利便性を高め、公平かつ公正な社会を実現する社会基盤としての役割と新たな価値の創出という目的がある。	両番号体系とも以下の発番機関登録規格を有する ・ UN/EDIFACT データエレメント 3055[18] ・ ISO/IEC 6523-2[19] ・ ISO/IEC 15459-2[20]
TDB 企業コード[21] **管理主体** **：株式会社帝国データバンク**	管理主体が独自に取材・収集した企業情報に加え、公的情報を基に 1 社＝1 コードとして厳格に設定した数字 9 桁の企業識別番号。	

[17]法人番号とは｜国税庁法人番号公表サイト　https://www.houjin-bangou.nta.go.jp/setsumei/index.html

[18]UN/EDIFACT　3055 Code list responsible agency code
https://unece.org/fileadmin/DAM/trade/untdid/d15a/tred/tred3055.htm

[19]ISO/IEC 6523-2:1998 Information technology - Structure for the identification of organizations and organization parts - Part 2: Registration of organization identification schemes
https://www.iso.org/standard/25774.html

[20]ISO/IEC 15459-2:2015 Information technology - Automatic identification and data capture techniques - Unique identification - Part 2: Registration procedures
https://www.iso.org/standard/54780.html

[21]TDB 企業コード　https://www.tdb.co.jp/lineup/code.html

1.4.4. トラストサービス

e シールを含めたトラストサービスは国内外で様々に定義されており、例として下表を挙げる。

	定義	出典
国内	インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み	プラットフォームサービスに関する研究会最終報告書 別紙「トラストサービス検討ワーキンググループ 最終取りまとめ」[22]
欧州	"trust service" means an electronic service normally provided for remuneration which consists of any of the following: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; (f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestation of attributes; (i) the creation of electronic timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger;	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework Article 3 Definitions[23] (16)
国際連合	(l) "Trust service" means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;	Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services[24] Chapter I. General provisions Article 1. Definitions
国際標準	"electronic service which enhances trust and confidence in electronic transactions"	ISO/IEC 27099 Information Technology - Public key infrastructure - Practices and policy framework[25]

[22]プラットフォームサービスに関する研究会最終報告書 別紙「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ最終取りまとめ」
https://www.soumu.go.jp/main_content/000668595.pdf

[23]REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183

[24]Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf

[25]「トラストを確保した DX 推進サブワーキンググループ報告書」2.2 トラストサービスの定義から引用
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf

1.4.5. 参照する公表資料

本実証、および本中間報告書作成にあたり、下表の資料を参照した。

表 5 本実証にあたり参照した資料

組織名称	資料名称
デジタル庁	データ戦略推進 WG 第４回 資料１ 「データ戦略の推進状況」[26]
総務省	プラットフォームサービスに関する研究会最終報告書 別紙 「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ最終取りまとめ」[27]
	e シールに係る指針(初版)[28] e シールに係る指針(第２版)[29]
一般社団法人デジタルトラスト協議会	e シール解説～実用化に向けて～[30] e シール利用者ガイドライン Ver1.0[31]
一般財団法人日本データ通信協会	e シール民間制度検討ワーキンググループ報告書[32]
日本トラストテクノロジー協議会	リモート署名ガイドライン[33]

[26]データ戦略推進 WG 第４回 資料１「データ戦略の推進状況」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/b565c818-75f4-4990-9125-dd43af8362ba/afe23c36/20220906_meeting_data_strategy_outline_01.pdf

[27]プラットフォームサービスに関する研究会最終報告書 別紙「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ最終取りまとめ」
https://www.soumu.go.jp/main_content/000668595.pdf

[28]e シールに係る指針(初版)
https://www.soumu.go.jp/main_content/000756907.pdf

[29]e シールに係る指針(第２版)
https://www.soumu.go.jp/main_content/000942602.pdf

[30]e シール解説～実用化に向けて～
https://jdtf.or.jp/report/whitepaper/file/e%E3%82%B7%E3%83%BC%E3%83%AB%E8%A7%A3%E8%AA%AC%28%E3%83%90%E3%83%BC%E3%82%B8%E3%83%A7%E3%83%B31.0%29.pdf

[31] e シール利用者ガイドライン
https://jdtf.or.jp/report/whitepaper/file/%EF%BD%85%E3%82%B7%E3%83%BC%E3%83%AB%E5%88%A9%E7%94%A8%E8%80%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_v1.pdf

[32]e シール民間制度検討ワーキンググループ報告書
https://www.dekyo.or.jp/digitaltrust/data/dekyo_e-sealwg_report202103.pdf

[33]リモート署名ガイドライン
https://www.jnsa.org/result/jt2a/2020/index.html

2. 実証実験（PoV　2022-2023 年度、PoC　2024 年度）

2.1.　実証環境

実証環境については大きな区分として以下が挙げられる。

・ ローカルｅシール

利用者の手元で秘密鍵を管理し、ローカル環境でｅシールを行う方式である。
具体的な方式は鍵ペア（秘密鍵と公開鍵）の生成される場所によって区別される。
本実証では以下の（ア）を利用した。

(ア) 認証局で生成した利用者の鍵ペア及び当該公開鍵に対して発行されたｅシール用電子証明書を利用者に送付するパターン

(イ) 利用者自身で利用者の鍵ペアを生成して証明書発行要求データなどを認証局へ送付、当該公開鍵に対して発行したｅシール用電子証明書を利用者に送付するパターン

・ リモートｅシール

利用者が、クラウド等のリモート環境にある利用者自身の秘密鍵にアクセスしてｅシールを行う方式。
具体的な方式としては、利用者はリモートｅシールサービスを提供する事業者（以下、「リモートｅシールサービス提供事業者」）が管理するクラウド等で管理されている秘密鍵にアクセスしてリモート環境でｅシールを行うといったことを想定。
リモートｅシールに関する具体的ユースケースについては、「1.4.5 参照する公表資料」で掲載した「eシール解説」が参考になり得る。

2.2. システム構成

2023 年 5 月までに実施したシステム構成としては以下のとおり。

- ローカル e シール

  以下のサービス・アプリケーションを利用した。

  - Qualified Certificates for Electronic Seals[34]
  - Adobe Acrobat[35]
  - SkyPDF Professional[36]
  - 日本データ通信協会認定タイムスタンプ（セイコーソリューションズ製品）[37]

- リモート e シール

  以下の構成にて実施を行った。（プロトタイプ環境を含む）

  - Fujitsu Computing as a Service Data e-TRUST[38]（以下 Data e-TRUST）
  - Box[39]および Box 連携アプリケーション（プロトタイプ環境）
  - TDB IdP（プロトタイプ環境）
  - eviDaemon on Cloud[40]
  - Adobe Acrobat[41]

2024 年度に実施した追加システム構成としては以下のとおり。

- RSSP(セコムトラストシステムズ実証環境)
- IA(セコムトラストシステムズ実証環境)
- サービス（スカイコム、セイコーソリューションズ、ハートビーツ実証環境）

---

[34]Qualified Certificates for Electronic Seals
https://www.globalsign.com/en/qualified-trust-services/qualified-certificate-for-electronic-seals

[35]Adobe Acrobat
https://www.adobe.com/jp/acrobat.html

[36]SkyPDF Professional
https://www.skycom.jp/product/skypdf/professional_7/

[37]セイコータイムスタンプサービス
https://www.seikotrust.jp/product/time-stamp/

[38]Fujitsu Computing as a Service Data e-TRUST
https://pr.fujitsu.com/jp/news/2022/10/17.html

[39]Box
https://www.box.com/ja-jp/home

[40]eviDaemon on Cloud
https://seiko-cybertime.app.box.com/app-center/evidaemon_on_cloud/app/B2Y2HTntmh

[41]Adobe Acrobat
https://www.adobe.com/jp/acrobat.html

3. 実証結果と課題（PoV　2022-2023 年度）

3.1. ローカル e シール（2022 年-2023 年）

本実証の協力社であるGMOグローバルサインが提供する EU 適格 e シール[42]、および Adobe Acrobat を用いてローカル環境で実施した。e シール付与後のローカル環境検証では、本実証の協力社であるスカイコムの SkyPDF Professional[43]、および Adobe Acrobat を用いた。

(1) Adobe Acrobat でGMOグローバルサインが提供する EU 適格 e シール、およびセイコーソリューションズのタイムスタンプを付与し、検証結果を表示した。

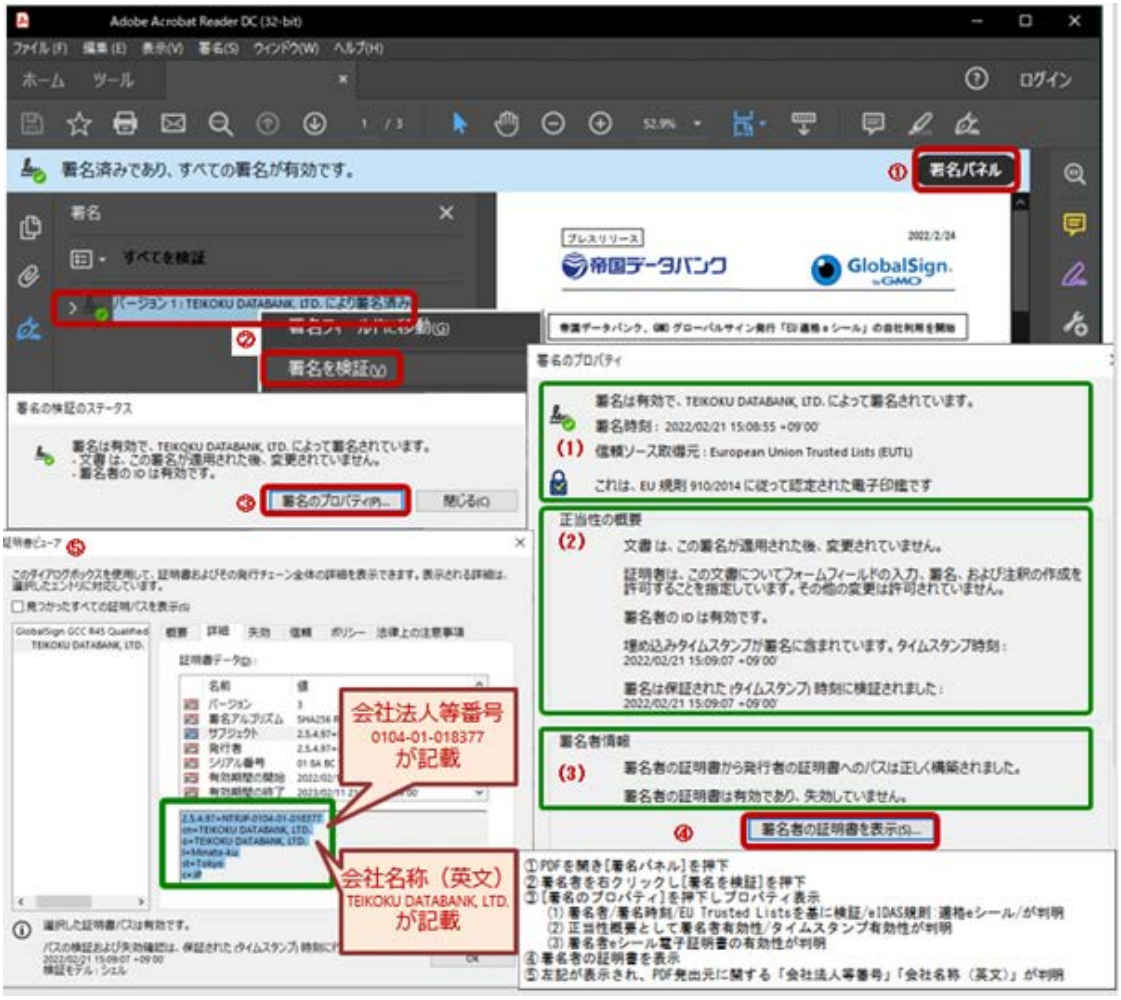

図 1 Adobe Acrobat で EU 適格 e シールを検証した結果

[42]「日本版 e シール」の実用化に向け、帝国データバンクが GMO グローバルサイン発行の適格 e シールの利用を開始
https://info-globalsign.com/press/20220224

[43]SkyPDF Professional
https://www.skycom.jp/product/skypdf/professional_7/

(2) EU 適格 e シールを付与した PDF ファイルについて、SkyPDF で検証結果を表示した。

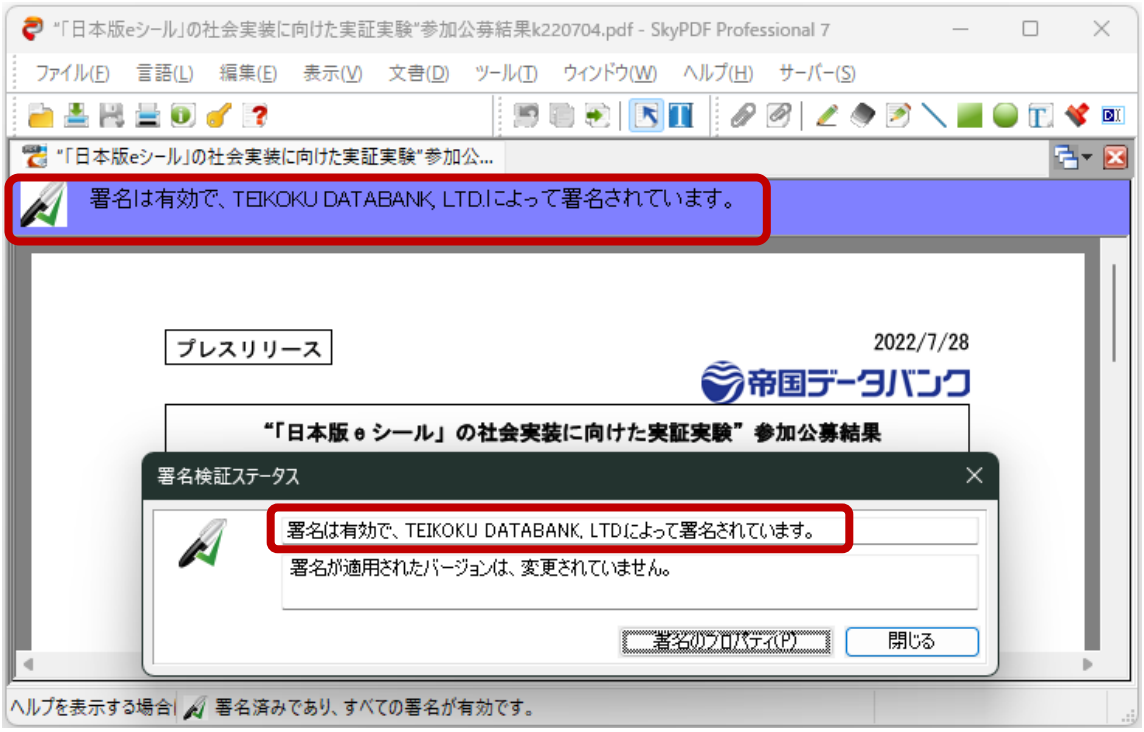

図 2 SkyPDF で検証した結果

3.2. リモート e シール（2022 年-2023 年）

TDB により認証され、発行された信頼できる法人アカウント、Data e-TRUST および Box を連携させて実施した。事前作業として以下が実施されていることを前提としている。

・TDB による法人認証および、信頼できる法人アカウントの発行
・Box アカウントの発行および連携アプリケーションの登録
・Data e-TRUST へのアカウント発行

なお、本実証実験で利用した環境はプロトタイプのため、制約事項ありきの状態での実施となる。以下に実際の実施結果を記載する。

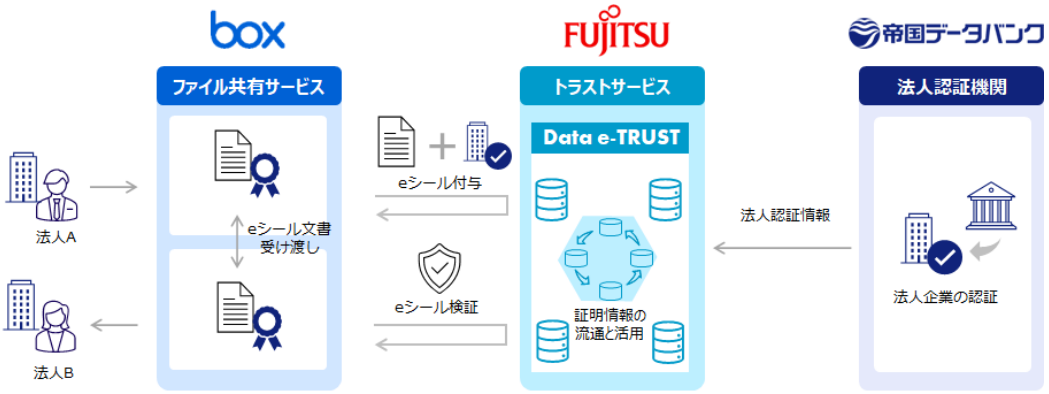

図 3 実証環境概念図

(1)Box 上で「証明書発行」操作を行うことで e シール用証明書の発行と、Data e-TRUST の連携を実施する。

図 4 Box 上での証明書発行と Data e-TRUST 連携

(2)Box 上で TDBIdP との連携が行われ、法人アカウントの認証画面が表示される。
なお、本来であればこのタイミングで多要素認証などの考慮も必要であるが、プロトタイプ環境のため、ID/PW のみの認証としている。

図 5 法人アカウント認証画面(プロトタイプ)

(3)認証が完了すると、アカウントに紐づいた法人情報から e シール用の証明書が発行される。
ここまでのオペレーションにより、Box から e シールを利用する準備が完了となる。

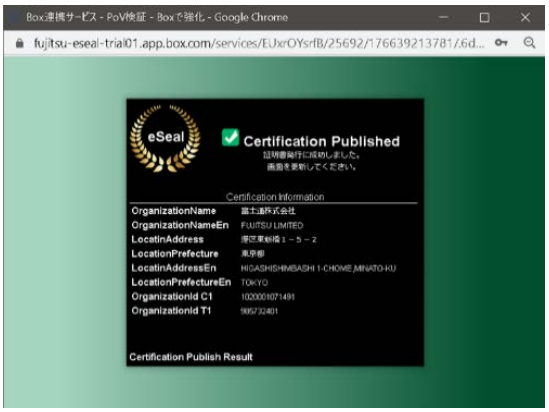

図 6 e シール利用準備完了画面

(4)Box にて e シール付与の準備を行う。本実験ではサンプルの見積書を Box に格納し、e シールを付与する操作を行った。すでに前オペレーションにて e シール発行の準備が完了しているため、画面上でファイルに対して「e シール付与」の操作を実施する。

図 7 Box 上 e シール付与操作画面

(5)Box より Data e-TRUST との連携が行われ、指定したファイルへの e シールの付与が完了する。

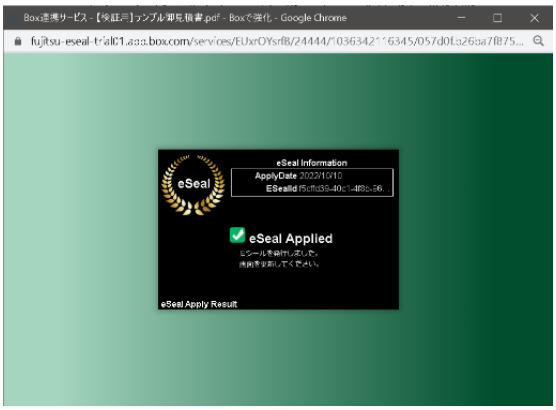

図 8 e シール付与完了画面

(6)e シールを付与したサンプル見積書に Box でタグを付与することで、e シール付与済であることを視認できる状態としている。

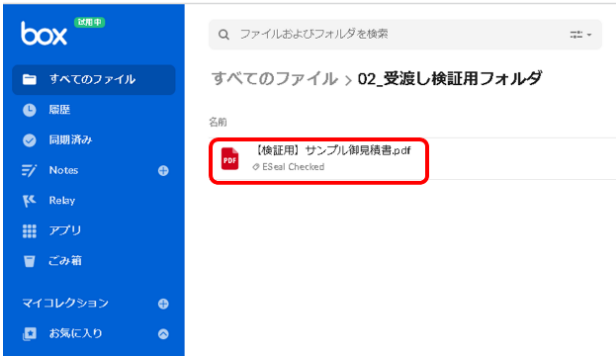

図 9 e シール付与済み確認

(7)e シールは Box の環境上から直接検証・確認を行うことができる。e シールを付与したファイルを指定し、「e シール検証・確認」の操作を実施する。

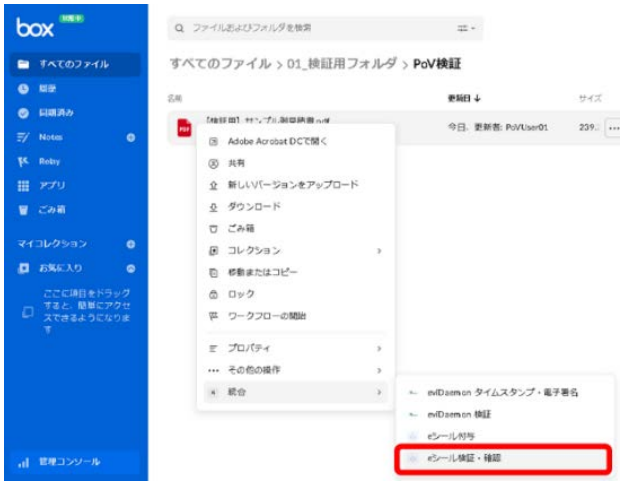

図 10 e シール検証操作画面

(8)e シールの検証結果及び表示されるプロファイルによりファイルの発行元情報を確認できた。

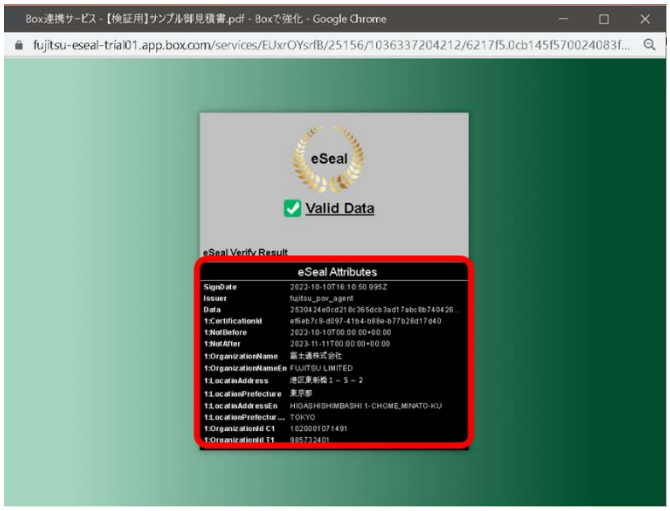

図 11 e シールプロファイル表示結果画面

(9)PDF ファイルを Adobe Acrobat で確認することで、PDF ファイルへの e シールが付与されていることも確認できた。

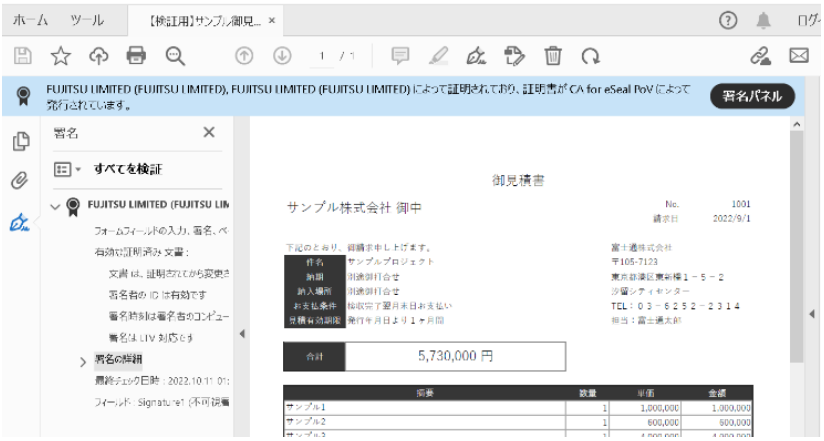

図 12 Adobe Acrobat での e シール付与確認画面

(10)Adobe Acrobat 上で、証明書のプロファイルも正しく設定されていることが確認できた。なお証明書プロファイルは、現在想定される暫定の内容を設定しているが、発行元の組織商号や法人番号など発行元証明情報を確認できた。

図 13 e シールプロファイルでの確認情報

3.3. ファイル送受信と e シール検証（2022 年-2023 年）

リモート e シール付与後に、実業務で想定される、企業間でのファイル受渡し業務を想定したオペレーションを実施した。

今回は、PoV 環境の中での実施となるため、Box コラボレーション機能を利用し、異なる企業が Box 上の別環境間でファイルを受渡す想定での実施とした。

今後は、他のサービス間でのファイル受渡しによる検証や、特定のサービスに依存しない形での検証についても検討していく必要がある。

以下に実際の実施結果を記載する。

(1)Box のコラボレーション機能を利用し、他社の Box 環境と直接ファイル授受を行える準備を行った。「02_受渡し検証用フォルダ」がコラボレーションフォルダであり、他社環境と共有することで、簡易にファイル授受を行うことできる環境である。

このフォルダに e シールを付与したサンプル見積書を格納することでファイルの受け渡しを実施した。

図 14 受渡し検証用フォルダ

(2)受取側の Box 環境から、ファイルの格納を確認することができた。受け渡されたファイルについて、受取側の環境で「e シール検証・確認」を実施した。

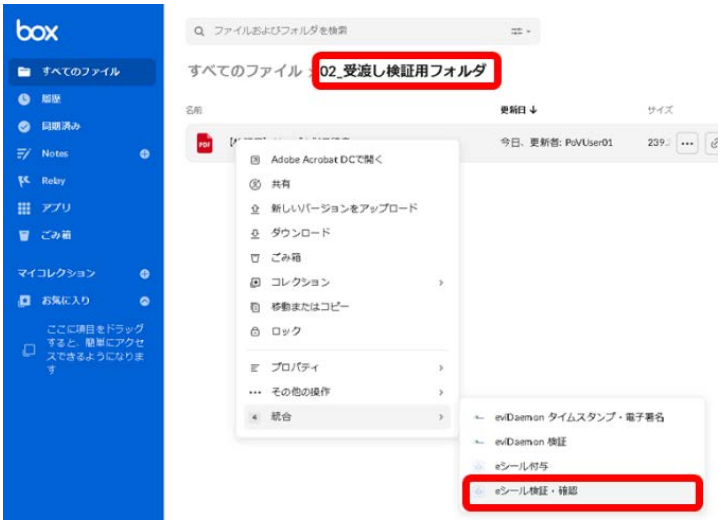

図 15 受取側環境での検証

(3)受取側の環境で受領したファイルの e シールおよび発行元の確認を実施することができた。

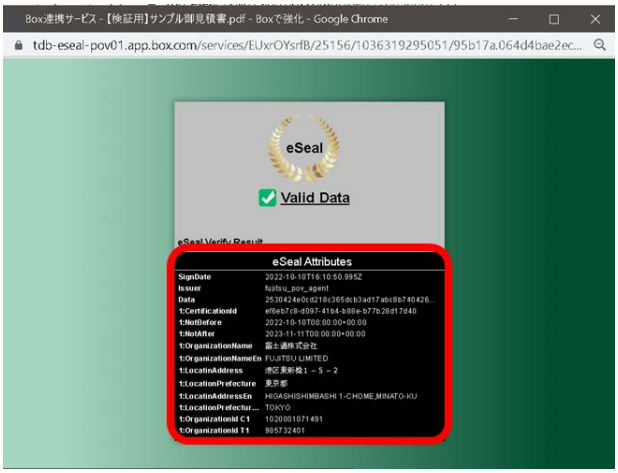

図 16 受取側環境での e シールおよび発行元確認

3.4. タイムスタンプ（2022 年-2023 年）

本実証実験では e シール付与の環境において、タイムスタンプ付与機能の実装までを行っていない。しかし、e シールの運用において、タイムスタンプの付与は必須と考えられ、本実験の協力社であるセイコーソリューションズの「eviDaemon on Cloud」を利用し、Box 上でドキュメントにタイムスタンプを付与した（2022 年-2023 年）。

なおユーザビリティを考慮すると本来であれば、一つのサービスおよび操作の中で e シールおよびタイムスタンプの付与が一度になされるべきであると考えられ、今後の課題として検討を行っていく必要がある。また、今回は民間認定（日本データ通信協会）のタイムスタンプを使用したが、今後は総務大臣認定のタイムスタンプの活用も考えられる。

本実験は事前作業として以下を実施していることを前提としている。

・Box アカウントの発行および eviDaemon アプリケーションの登録

・eviDaemon へのアカウント発行

以下に実際の実施結果を記載する。

(1)e シール付与と同様に画面上でファイルに対して「eviDaemon タイムスタンプ・電子署名」の操作を行う。

図 17 eviDaemon タイムスタンプ付与画面

(2)ファイルにタイムスタンプが付与されることが確認できた。

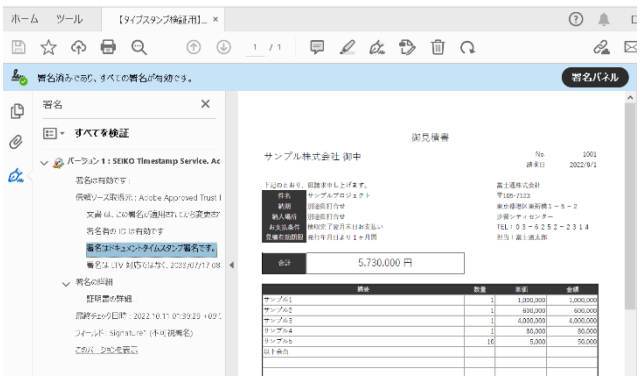

図 18 Adobe Acrobat でのタイムスタンプ確認画面

3.5. e シールおよび適格請求書発行事業者登録番号検証と自動振分(プロトタイプ 2022 年–2023 年)

本実証実験では、２つの観点がある。
・e シール付与と e シール検証(適格請求書発行事業者の登録番号の検証を含む)
・e シール付与したファイルの一括検証と自動振分け(適格請求書発行事業者の登録番号による振分けを含む)
令和 5 年 1 月 20 日から適格請求書発行事業者公表システム Web-API 機能（以下「インボイス Web-API」）の利用は、国税庁の承認が必要となった[44]。

本実証実験では、令和 5 年 1 月 20 日の前に実験した時はインボイス Web-API を利用していたが、令和 5 年 1 月 20 日以降実験した時は、インボイス Web-API を使用せずに、以前の実験の Web-API の結果データを利用した。

□ e シール付与と e シール検証(適格請求書発行事業者の登録番号の検証を含む)
(1)e シール付与対象ファイルをアップロードする。

図 19 e シール付与対象ファイルのアップロード

[44] 国税庁：適格請求書発行事業者公表サイト運営方針の改訂について
https://www.invoice-kohyo.nta.go.jp/news/r05/r05news01.html

(2)e シール付与を行う。

図 20 e シール付与実施(その 1)

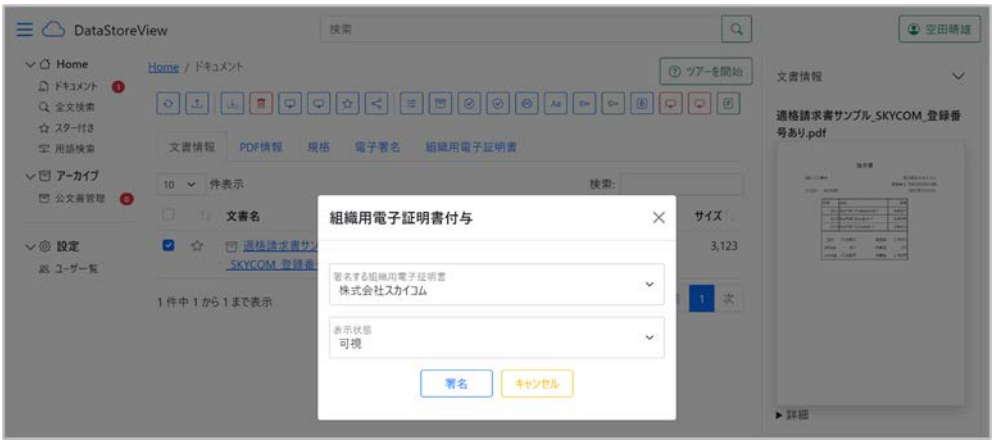

図 21 e シール付与実施(その 2)

(3)e シールの検証１。電子署名とタイムスタンプの検証を行う。

図 22 電子署名とタイムスタンプの検証

(4)e シールの検証２。 適格請求書発行事業者の登録番号の検証を行う。

図 23 適格請求書発行事業者登録番号の検証

国税庁のインボイス Web-API で適格請求書発行事業者の登録番号の検証を行い、PDF 内のテキストに適格請求書発行事業者の登録番号が存在しているかを検証する。

図 24 適格請求書発行事業者登録番号存在有無確認

□ e シールを付与したファイルの一括検証と自動振分け

(1)e シールを付与した対象ファイルをアップロードする。

図 25 e シール検証対象ファイルのアップロード

(2)一括検証を行う。

図 26 一括検証の実施

電子署名とタイムスタンプの検証を行い、国税庁のインボイス Web-API で適格請求書発行事業者の登録番号の検証を行い、PDF 内のテキストに適格請求書発行事業者の登録番号が存在しているかを検証する。

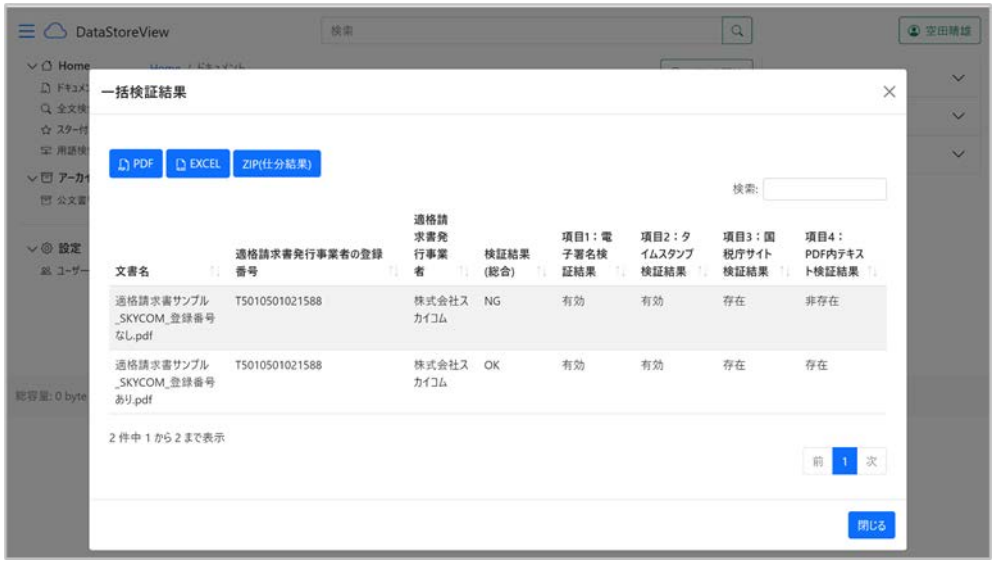

図 27 適格請求書発行事業者登録番号存在確認

(3)自動振分けを行う。

「ZIP(仕分結果)」ボタンをクリックして振分けた結果をダウンロードする。

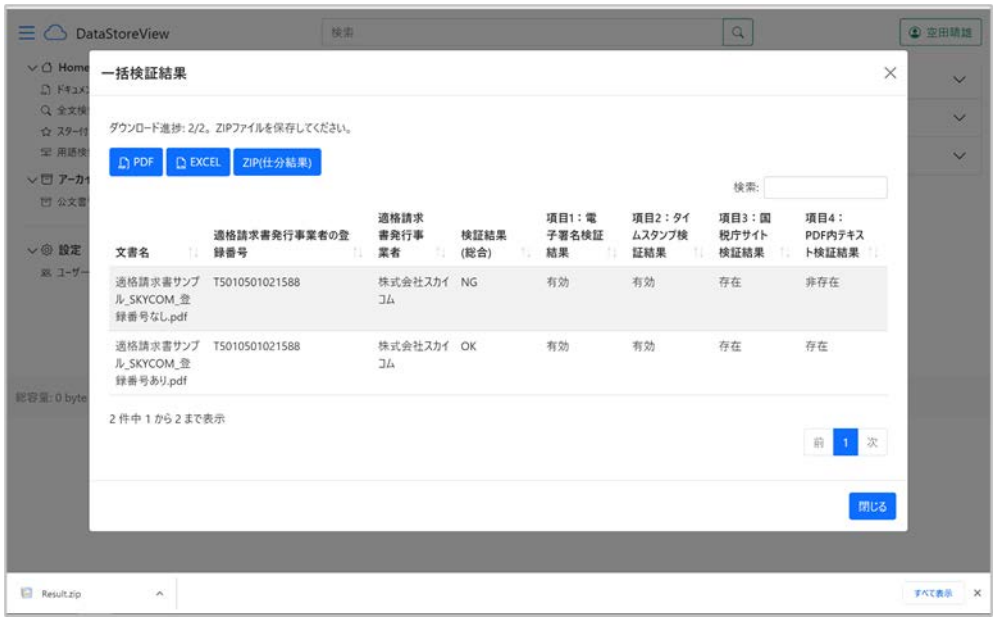

図 28 仕分結果ボタンの押下

ダウンロードしたファイルを展開して、中身を確認する。
適格請求書発行事業者の登録番号による振分けが行われた。

図 29 適格請求書発行事業者登録番号による振分け

下図のとおり、検証結果による振分けが行われたことを確認した。

図 30 適格請求書発行事業者登録番号検証結果による振分け結果

図 31 検証 OK 分の振分け

図 32 検証 NG 分の振分け

4. まとめと提言（PoV 2022-2023 年度）

4.1. e シールの有用性、ユーザビリティおよび普及させていくための検討事項

実業務における電子文書の授受は、メールによる伝送やクラウドサービスを利用するものなど、多様な方法がとられている。本実証では、Box を利用したファイル授受のユースケースを元に検証を行った。

(1)e シールの有用性

文書に e シールを付与し、検証の操作を行うことで、簡易に文書の真正性を確認することができた。現在、電話連絡や問合せ等による真正性確認業務において大幅な工数の削減が見込めるほか、従来真正性確認を実施してこなかった文書授受において新たに活用することで、不正文書取引の抑制やリスク回避も期待できる。

(2)ユーザビリティへの考慮

e シールを活用するうえで、既存の業務フローに影響を及ぼさない考慮が必要である。e シールによる真正性確認のために、既存業務とは異なるサービスやアプリケーションへのファイル転送、個別のオペレーションが必要になる場合、簡易な真正性確認ができる有用性が損なわれる。

e シールの検証において、証明書などの専門知識がない業務遂行者が Adobe Acrobat などを用いた一般的な証明書プロファイルを確認して、真正性確認を行うことは現実的ではなく、業務遂行者が正しく検証ができるユーザーインターフェースの考慮が必要と考えられる。

業務の中で e シールを活用していくうえでは、e シールが付与されていることを簡易に視認できる必要があると想定される。電子文書を開くことなく「当該ファイルの e シールあり・無しが視認可能であること」を実現することにより、更に業務効率の改善が図れると考えられる。

本実証では、以下によりユーザビリティへの考慮を行った。現状はプロトタイプでの確認のため、更なる検討を実施していく必要がある。

・Box 内で e シールの活用とファイル授受の業務を完結させた。
・検証結果のユーザーインターフェースを用意し、ファイルの真正性の確認を簡易化した。
・e シールの付与と共に Box タグを付与することで e シール付与の視認性を高めた。

(3)課題と検討要素

(ⅰ)サービスへ簡易に導入できる仕組みの検討

実業務でファイルの授受を行う場合、法人・組織の間で様々なサービスの利用が想定され、１対１の関係でなく多対多の関係で、様々なファイルが混在する。そうした環境下にいて、特定の証明機関とサービスに限定された e シールの利用では有用性の効果は低く、様々なサービスで簡易に導入可能な環境及び仕組みを検討していく必要がある。また、電子文書の特性として、特定のサービス外での運用も多々想定されるため、一般的な WEB サービスかつ、信頼できる形での検証手段も検討が必要と想定される。

（ⅱ）認証の仕組みにおける検討

サービスの利用と e シールの活用を合わせて検討していくうえで、認証の仕組みを検討する必要がある。e シールを利用するうえで、厳格な認証が必要になるものの、e シールの認証処理や認証インターフェースをサービス側で実装する場合、サービスに対する e シール導入の敷居が上がり、簡易な導入の阻害要因となりうる。

（ⅲ）e シール活用の拡張

e シールを活用していくうえで、単純な付与および検証だけではなく、その後の業務の自動化などを踏まえた検討が必要である。

一般的なファイル共有サービス等には、授受インターフェースやカスタマイズするための API が完備されており、e シールの発行元確認のみで振り分けの自動処理や e シール付与対象ファイル内の情報突合せ、および購買システムなどの情報とも連動が可能と考えられる。また、e シールが無いものは別途処理を促すことも検討可能と想定される。

本実証では、e シールに対する認証を TDBIdP が実施することで、Box に e シールのための認証の仕組みを持たせずに発行を可能とする仕組みとした。また認証機関、サービス、プラットフォームを連携させることで、複数の認証機関とのサービス連携を考慮したモデルのプロトタイプ作成を行った。同様の仕組みの更なる検討および横展開によって、認証情報を複数保持せずに、複数のサービス、複数の認証機関で同様の e シール活用モデルの構築が可能と想定される。

4.2. サービス連携

社内承認システムや購買システム等との自動サービス連携があれば、業務における各種データ処理の「自動化・効率化・即時化」が実現される。

実現にあたっては各サービス間での ID 連携も重要と考えられ、協力社であるセコムトラストシステムズ社などと共に 2022 年 10 月以降に検討を進めた。

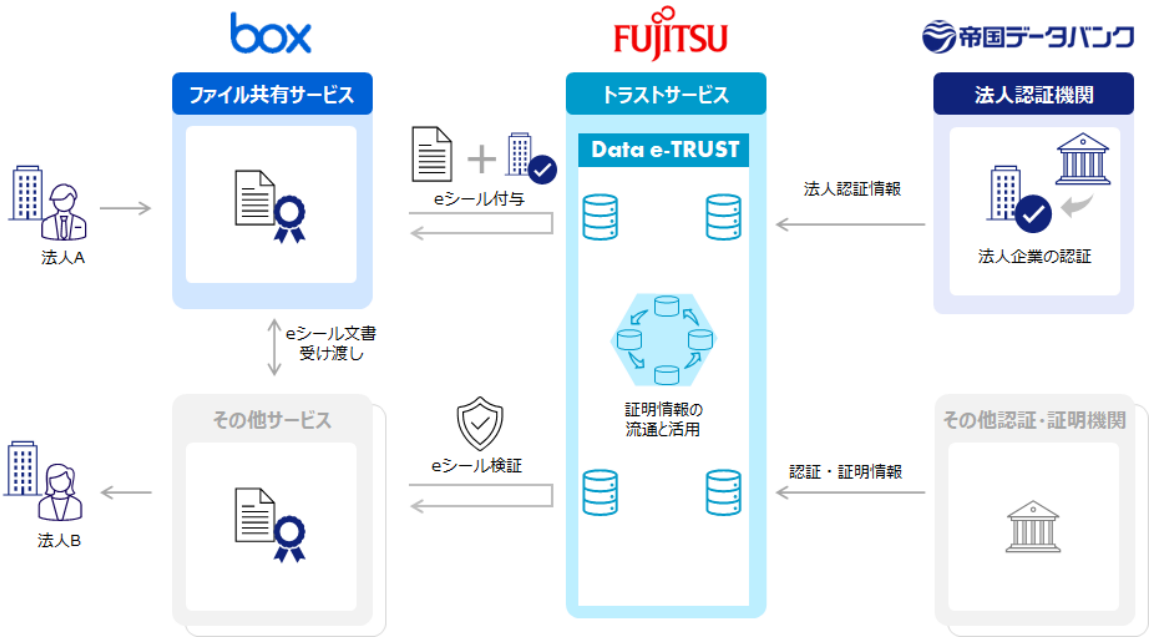

図 33 2022 年 10 月以降の検討概略

検討にあたり、以下をポイントとした。

1) 開かれたサービス

特定サービスに「閉じられた」環境とはせず、統一基準のもとで様々な事業者が連携・協業できる「開かれた」サービスを提供することが、より多くの利用者に対する利便性向上につながり、ビジネスシーンにおけるペーパーレス化を促進すると考えた。

2) 利用者に負担の無い簡易な利用

様々なサービス、各々で認証方法が異なると利用の大きな障壁となる。

なりすましを防止しながら利用者のセキュリティも確保し、操作が複雑でなく簡易であることが重要と想定した。

3) サービス提供事業者の負担軽減

利用者に対し様々なアプリケーションを提供するサービス提供事業者にとっても、トラストサービス毎にインターフェースが異なるようでは、選択肢が狭まる。またインターフェースに合わせて個別開発することは同事業者の負担となるため、その軽減が重要であると想定した。

検討した結果を以下に図示する。

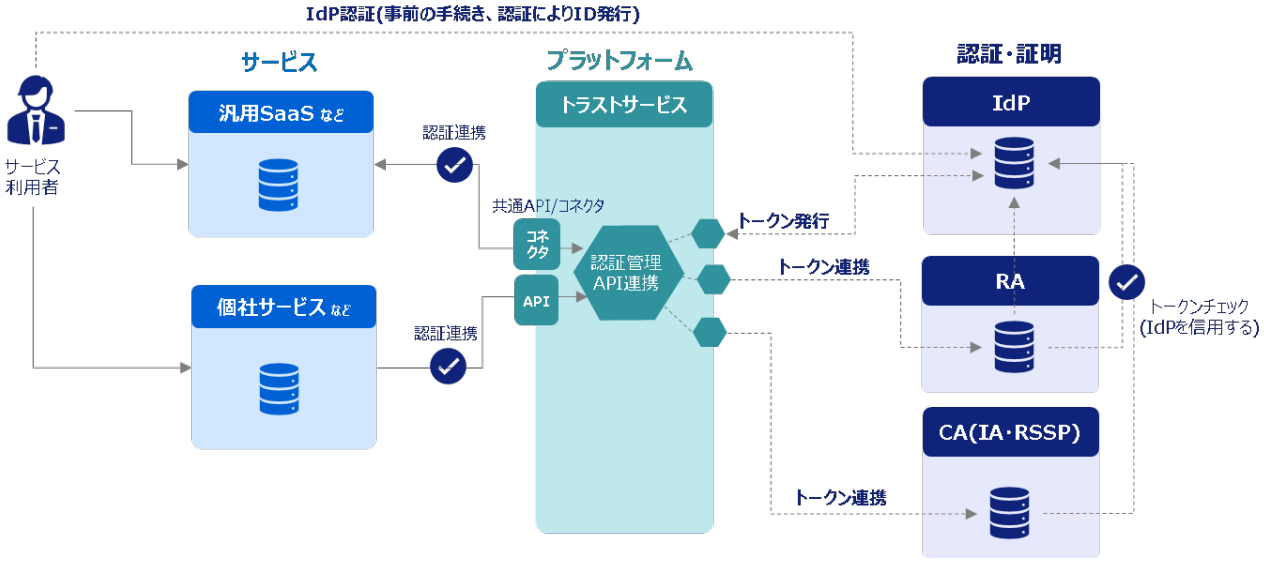

図 34 検討結果概要

1) 開かれたサービス

トラストサービスは複数のサービス提供事業者が存在している。個別の事情が無い限り、これらの連携（複数の電子契約サービス間での連携など）は有り得ない。この帰結として例えば、電子署名を利用した電子契約などを行う場合にはトラストサービス提供事業者によるベンダーロックインが想定される。利用者は電子契約を行う相手毎に、自身が利用しているものとは別のトラストサービスの利用を余儀なくされ、場合によっては別の端末を用意しなければならない状況にも陥る。上記の解決としては、利用者のサービスが異なっても共通にトラストサービスが可能となる仕組みづくりが挙げられる。

2) 利用者に負担の無い簡易な利用

利用者の観点からは（トラストサービス自体を意識することなく）簡易にサービスを利用できることが望ましい。サービス間の連携は、認証連携によってスムースに行われ、利用者のメインサービス内でトラストサービスが自然に活用できれば便利であり、サービスラインナップとして選択肢があれば、より良いサービスを自身で選択可能となる。また e シールは利用者のみが付与できることを担保する必要から、身元確認と当人認証は必須である。

3) サービス提供事業者への負担軽減

サービス提供事業者は、自身のサービス内でトラストサービスを利用する場合、トラストサービス提供社毎に用意された API などに対応しなければならない場合が多く、対応時間や費用が相応に必要となり負担となる。

上記 3 点を総合的に検討すると、適切な身元確認と当人認証を具備した外部 IdP を利用した認証連携、および同 IdP を援用したプラットフォームが望まれる。利用者には IdP を活用した認証連携によりスムースなサービス利用を享受でき、サービス提供側もトラストサービス毎の差異を吸収してくれるプラットフォームがあれば不要な対応時間・費用を圧縮できる。

5. 実証結果と課題（PoC 2024 年度）

5.1. 実証目的と結果：外部 IdP を利用したリモート e シール付与（2024 年度）

TDB により認証され、発行された信頼できる法人アカウントに紐づく組織内個人 ID、RSSP・IA（セコムトラストシステムズ）およびサービス事業者（スカイコム、セイコーソリューションズ、ハートビーツ）のサービスとの間を認証・連携プラットフォームにより連携させ実施を行った。

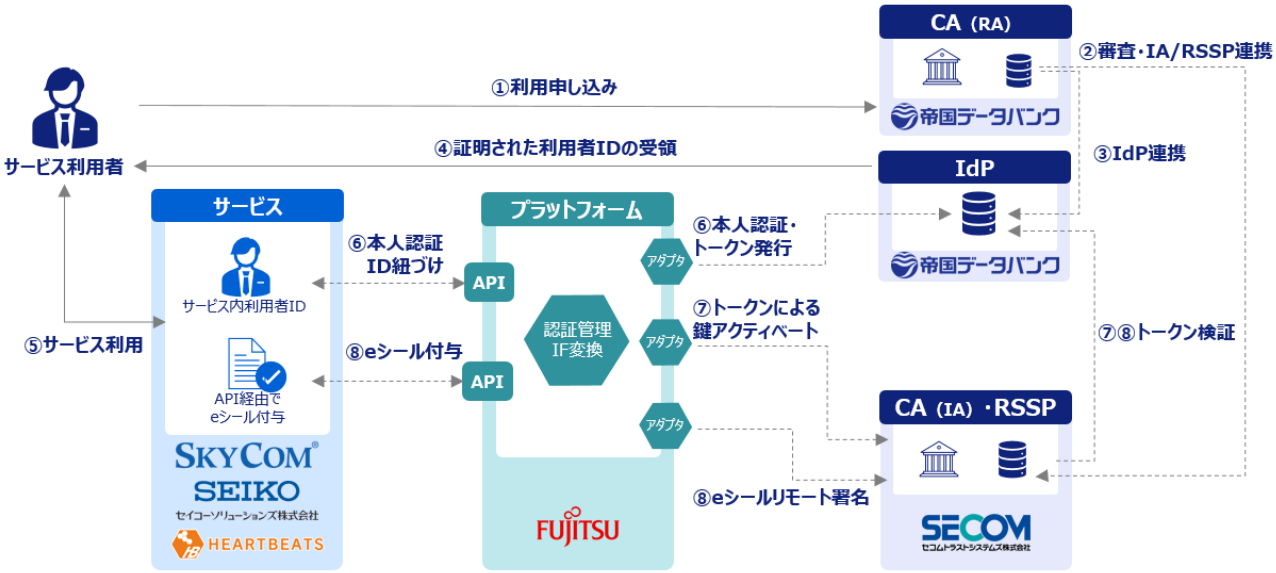

図 35　2024 年度実証実験概念図

手順：

①TDB の電子証明書（TDB 電子証明書 TypeA）を使用した利用申込

②TDB による書類審査および法人認証を経た e シール管理用 ID の発行、IA/RSSP 連携

③IdP 連携による利用者 ID の発行

④証明された IdP 利用者 ID の受領およびアカウントの初期設定（二要素認証の設定）

⑤サービス事業者サイトへのログイン、サービス利用

⑥本人認証およびトークン発行、IdP 利用者 ID との紐づけ

⑦発行されたトークンによる鍵のアクティベート

⑧PDF への e シール付与

2023 年 6 月に公表した報告書における 4.まとめ・提言の「4.1e シールの有用性、ユーザビリティおよび普及させていくための検討事項」および、「4.2.サービス連携」で考察したとおり、本 PoC では、以下を考慮した設計を行った。

本 PoC の目的：「開かれたサービス」「サービス提供事業者の負担軽減」

- e シールを運用するビジネスモデルの一つと想定される、各機関とサービスを連携させたリモート e シール付与の実証環境を構築し検証する。
- IdP による認証を行うことで発行されるトークンを元に各連携先の認証を一元管理し、e シールの付与が可能であることを確認する。サービス側では、トラストサービスに対する ID 認証

を行うのみで、当該 ID を利用したリモート e シール事業者のサービスおよび e シール署名までの ID 連携を実現する。

・ サービス側での認証管理や、個別モジュールの組込みなどを行わず、標準 API 連携のみでの e シール付与が可能であることを確認する。他のリモート e シール事業者等が今後参加された場合でも、リモート e シール事業者毎の API 連携はプラットフォームで実施するため、サービス提供事業者側でのシステム変更などの対応を不要としている。

本 PoC の狙い：「複数利用者によるリモート e シール付与」

e シールは、個人名義の電子証明書とは異なり、組織に所属する複数利用者による利用が想定されている。一つの e シールに対して、複数の利用者（ID）を設定することを可能とし、また一人の利用者（ID）に対して、複数の e シール証明書の利用権限の付与を実現する。

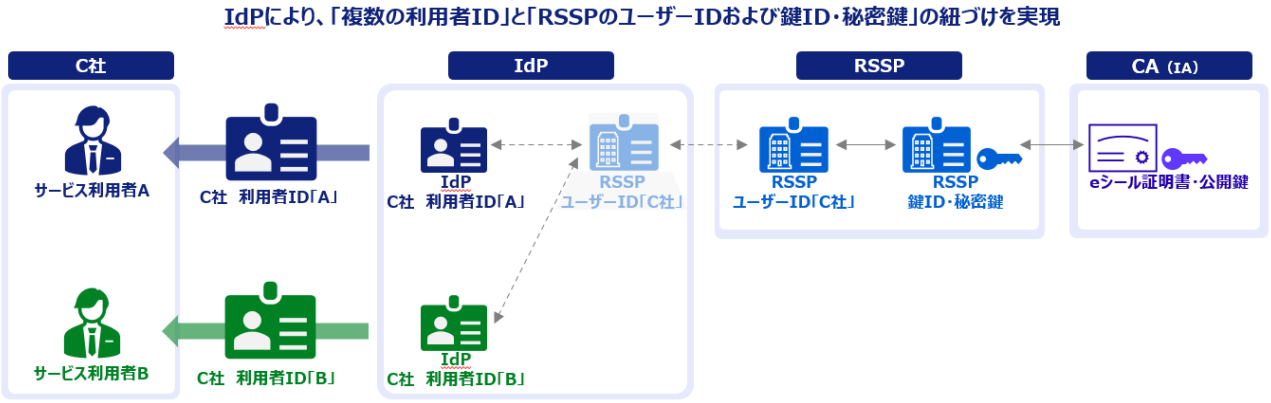

図 36　同一組織内複数利用者が e シールを利用可能とするイメージ

現状の RSSP の仕様では一つの鍵 ID を複数の利用者 ID が利用することは困難と想定される。しかしながら e シールの実運用においては、一つの鍵を「組織内における複数の利用者が使用するシーン」が想定される。

そのため、今回の PoC の仕組みでは、「RSSP のユーザーID」と「IdP 側で発行された利用者 ID」を IdP 側にて 1：N で紐づけることにより、同一鍵を複数の利用者で保持すること、および複数鍵を保持することを可能とした。

5.1.1. セイコーソリューションズ株式会社による実証実験

手順「⑤サービス事業者サイトへのログイン、サービス利用」から、Google Chrome ブラウザと Postman（API 実行ツール）を活用し、簡易的に API コールを行い、PoC 実施した。

(1) 事前準備

・Google Chrome ブラウザを PoC 用 PC へインストール
・Postman を PoC 用 PC へインストール
・Postman Interceptor 拡張機能を追加
・Postman へ Cookie の同期設定を実施

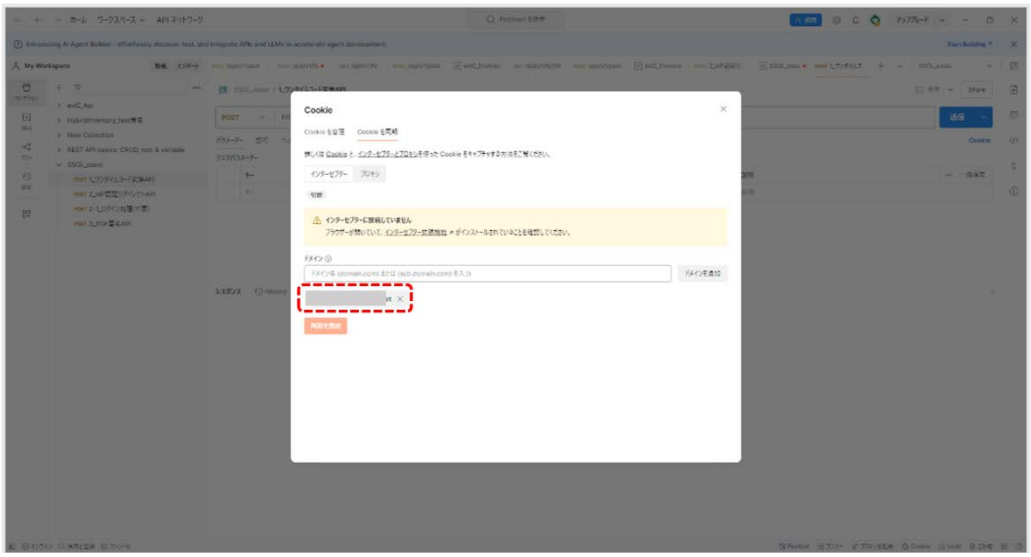

図 37　Postman へ Cookie の同期設定

・Postman へ以下の環境変数設定を実施

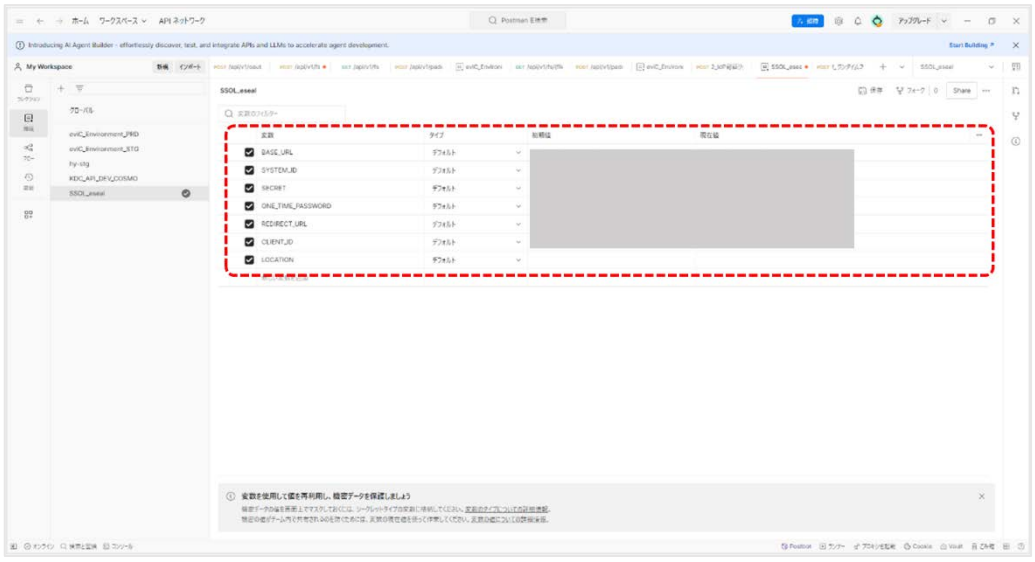

図 38　Postman への環境変数設定

(2) ワンタイムコード変換 API の実行

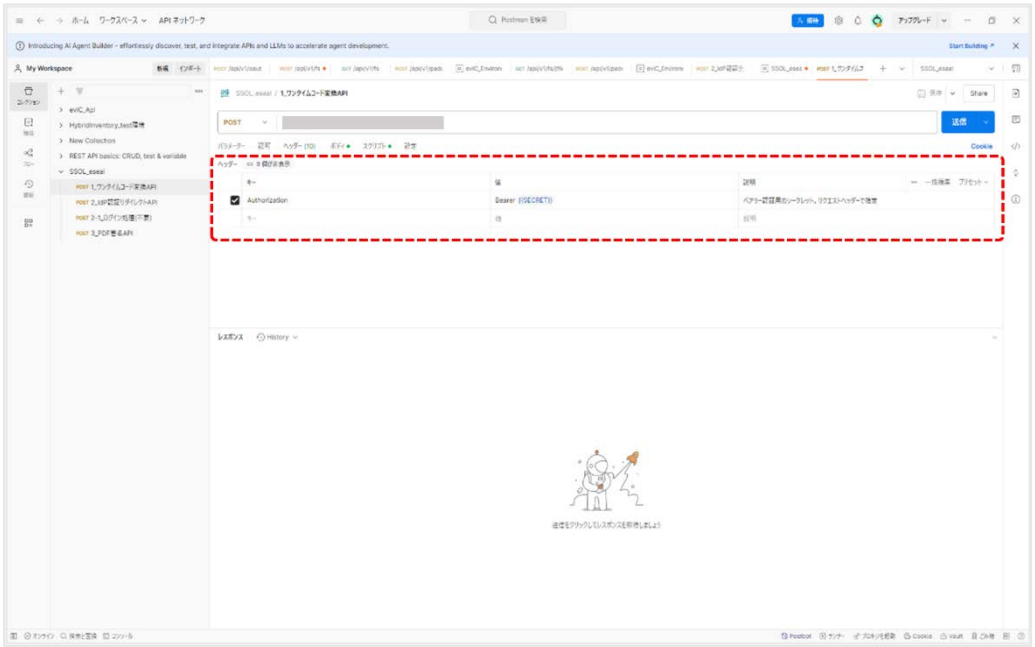

図 39　ワンタイムコード変換 : API コール - ヘッダー

＜API コール＞

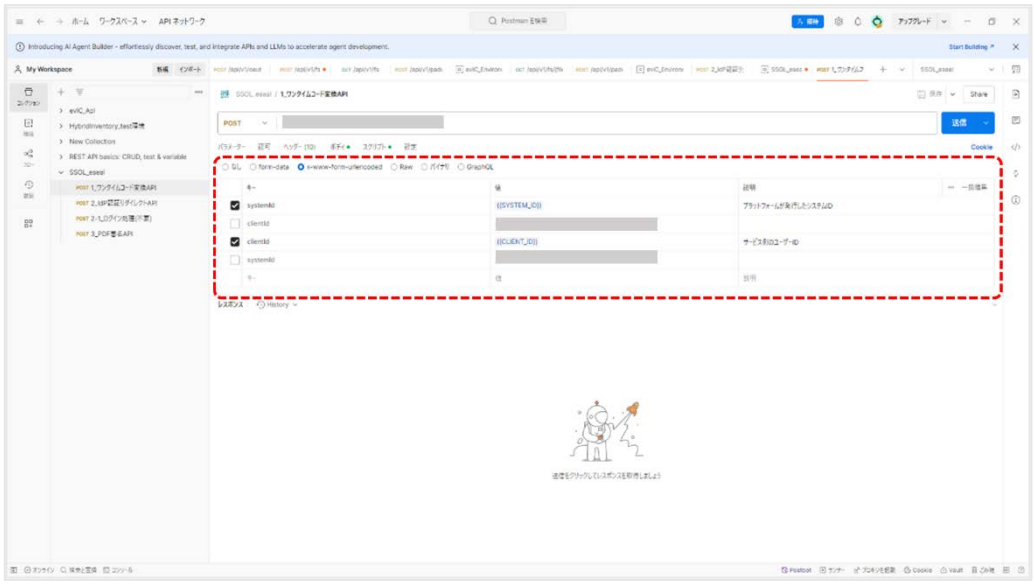

図 40　ワンタイムコード変換 : API コール - ボディ

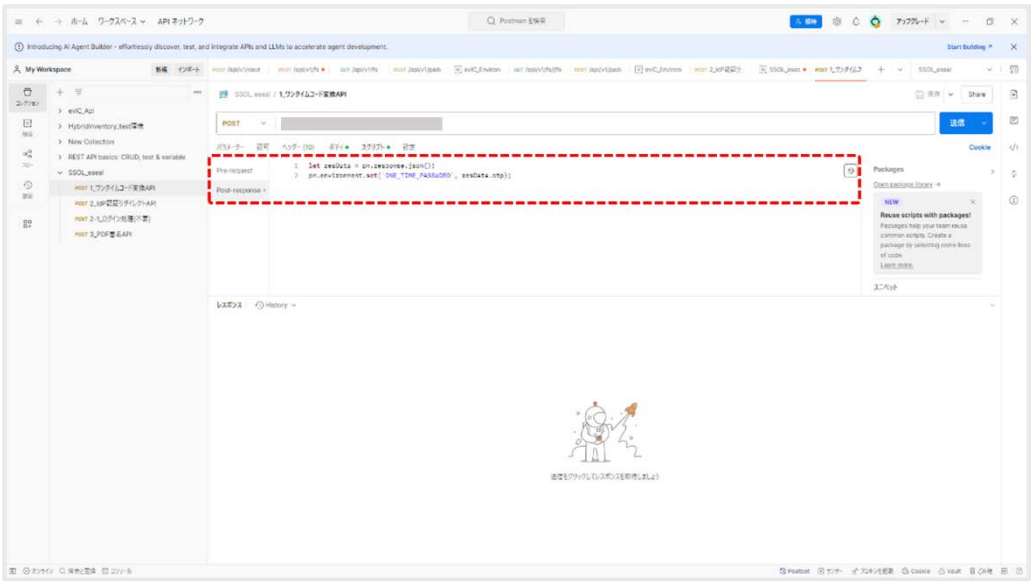

図 41　ワンタイムコード変換 : API コール - クリプト

＜API レスポンス＞

opt … ワンタイムコードの入手成功

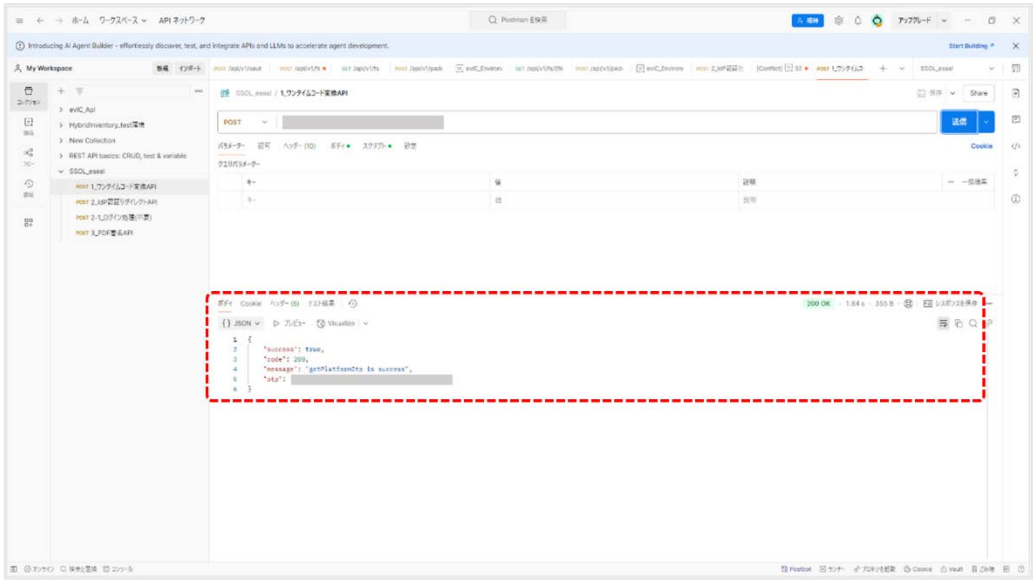

図 42　ワンタイムコード変換：API レスポンス

(3) IdP 認証リダイレクト API の実行

＜API コール＞

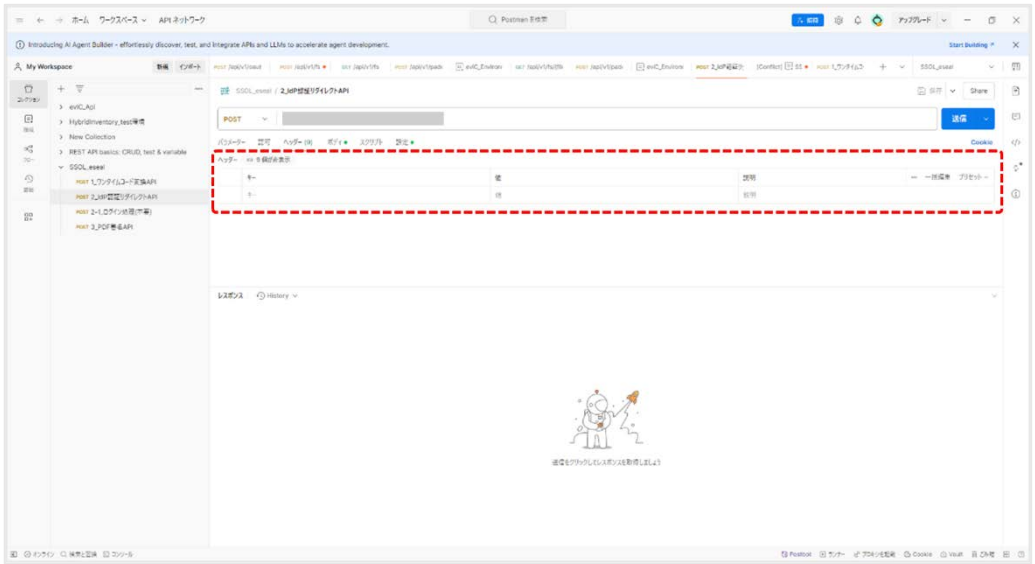

図 43　IdP 認証リダイレクト：API コール - ヘッダー

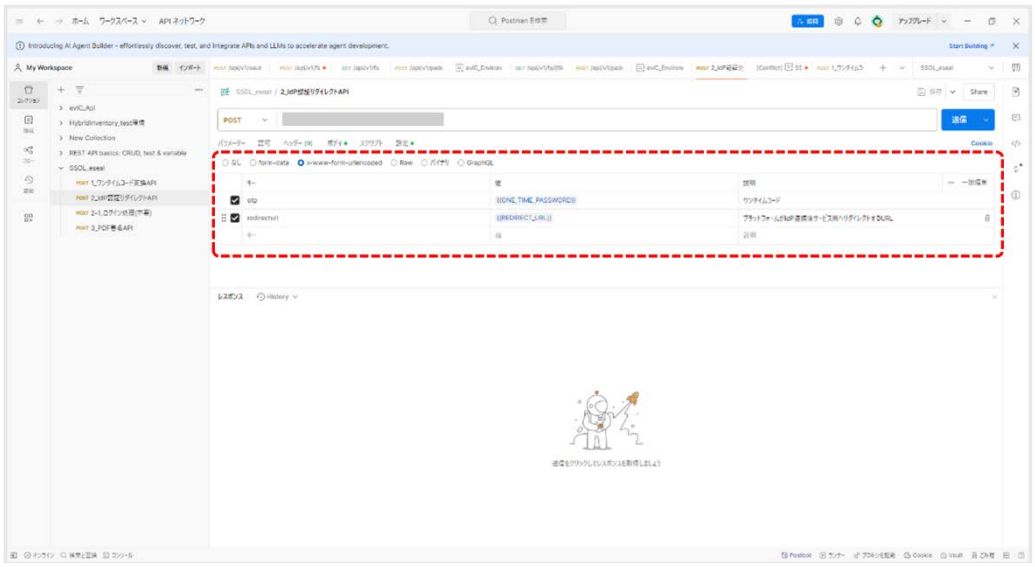

図 44　IdP 認証リダイレクト：API コール - ボディ

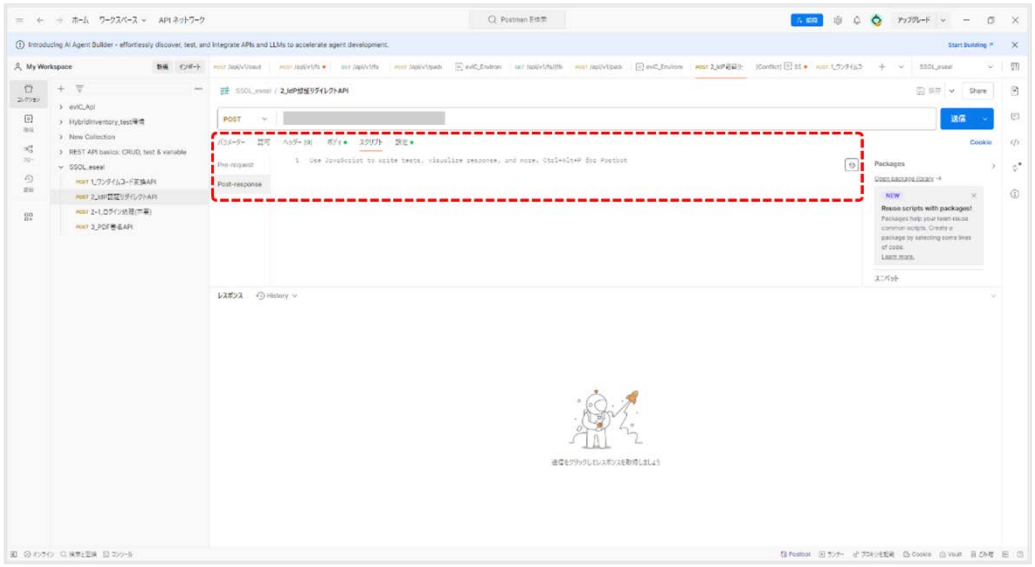

図 45　IdP 認証リダイレクト：API コール - スクリプト（無し）

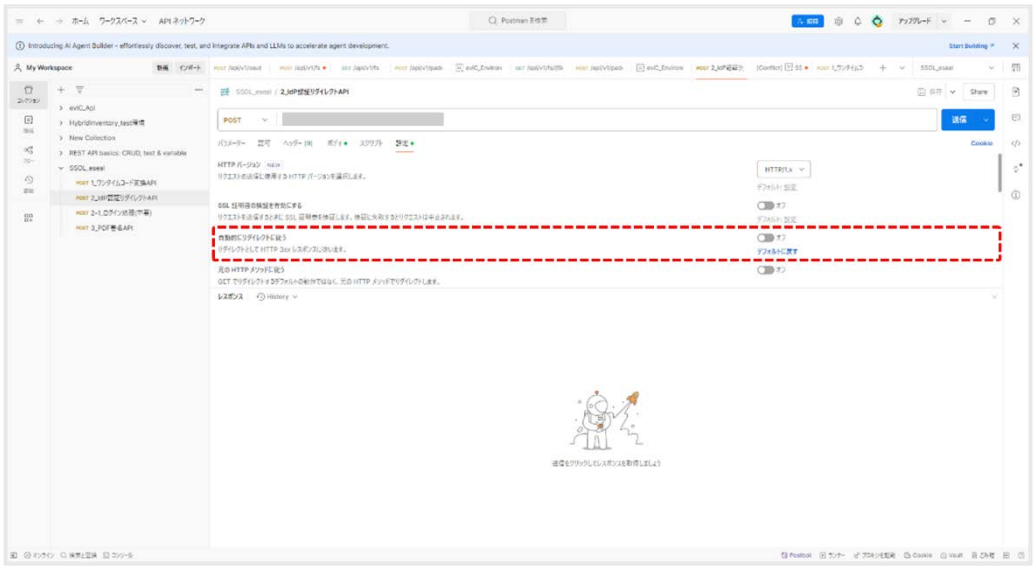

図 46　IdP 認証リダイレクト：API コール - 設定

＜API レスポンス＞

location…IdP ログイン URL の入手

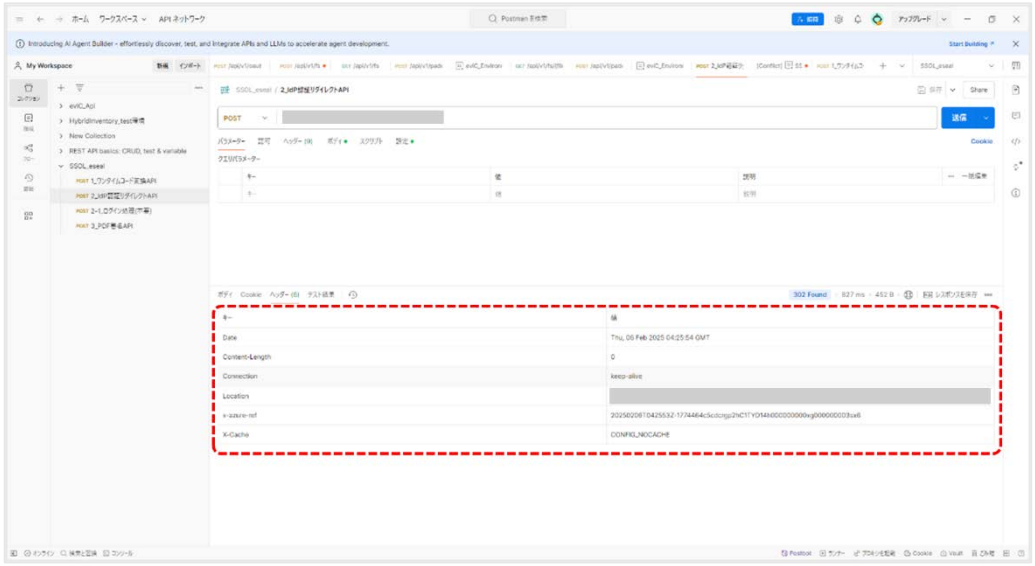

図 47　IdP 認証リダイレクト：API レスポンス

(4) 認証情報の入力

図 48　ユーザーID / パスワードの入力

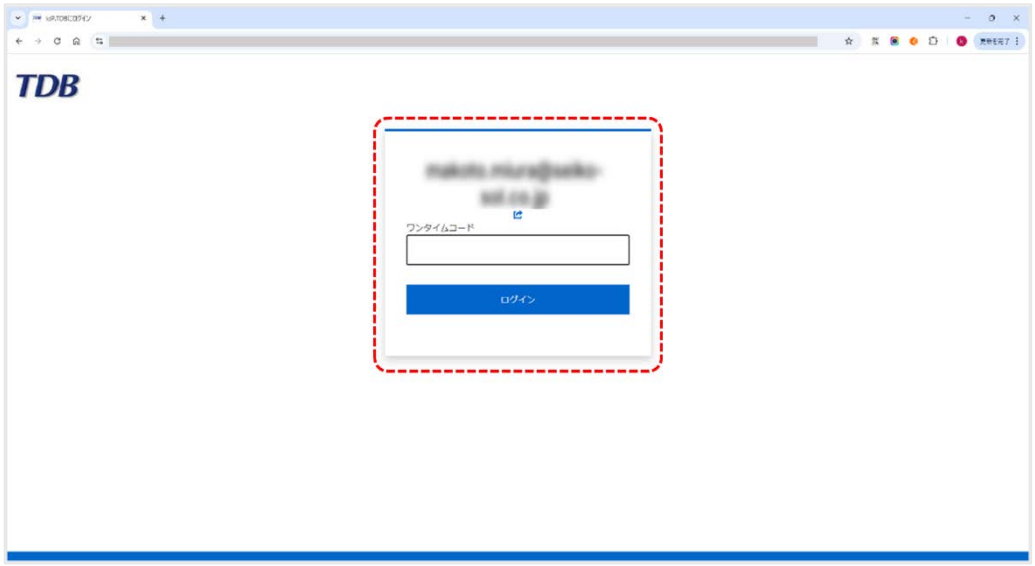

図 49　ワンタイムパスワードの入力

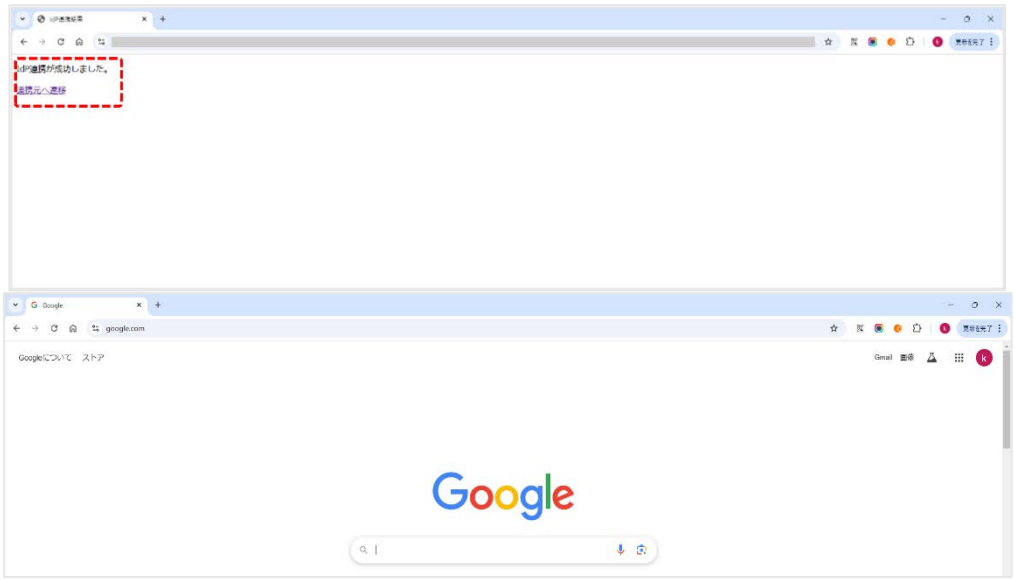

図 50　認証成功、遷移元（Google サイト）へ遷移

(5) PDF 署名 API の実行

＜API コール＞

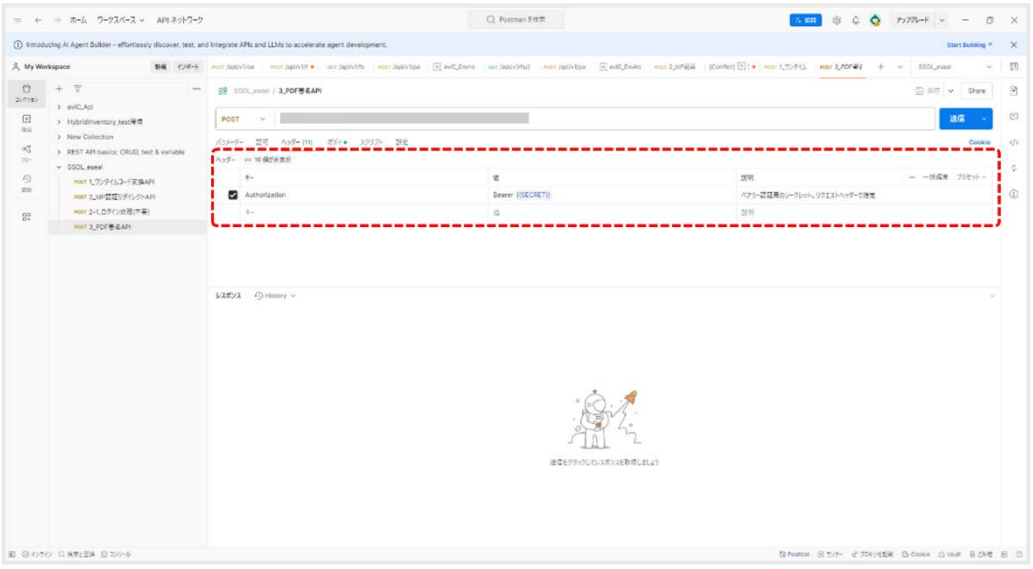

図 51　PDF 署名：API コール - ヘッダー

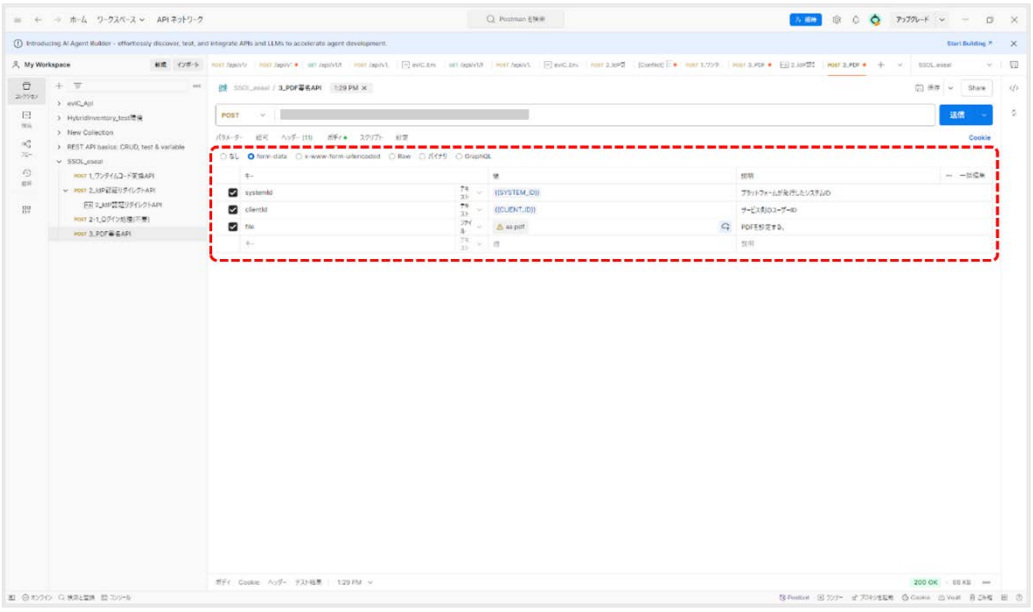

図 52　PDF 署名：API コール - ボディ（署名対象 PDF ファイルの指定）

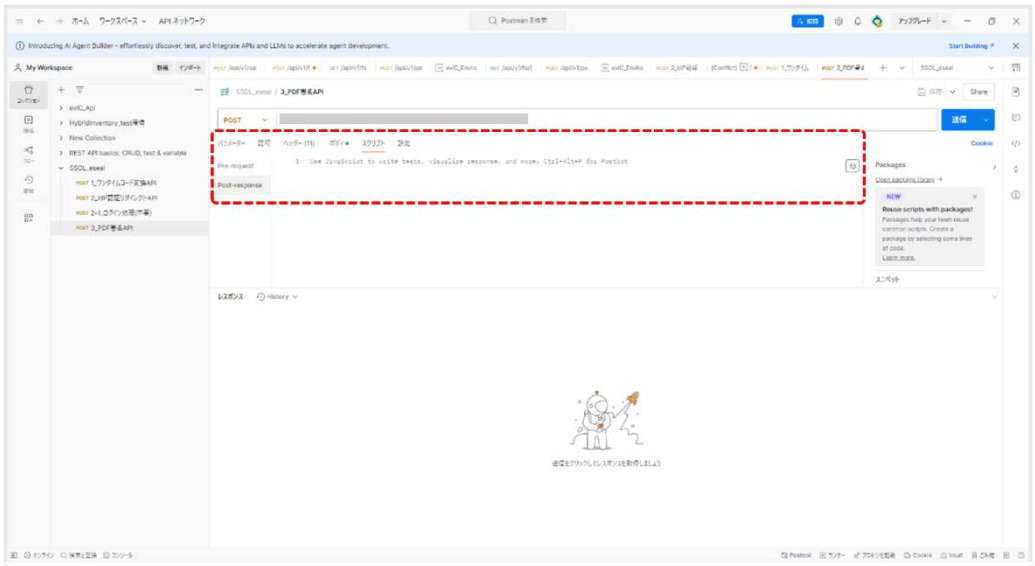

図 53　PDF 署名 : API コール - スクリプト（無し）

＜API レスポンス＞

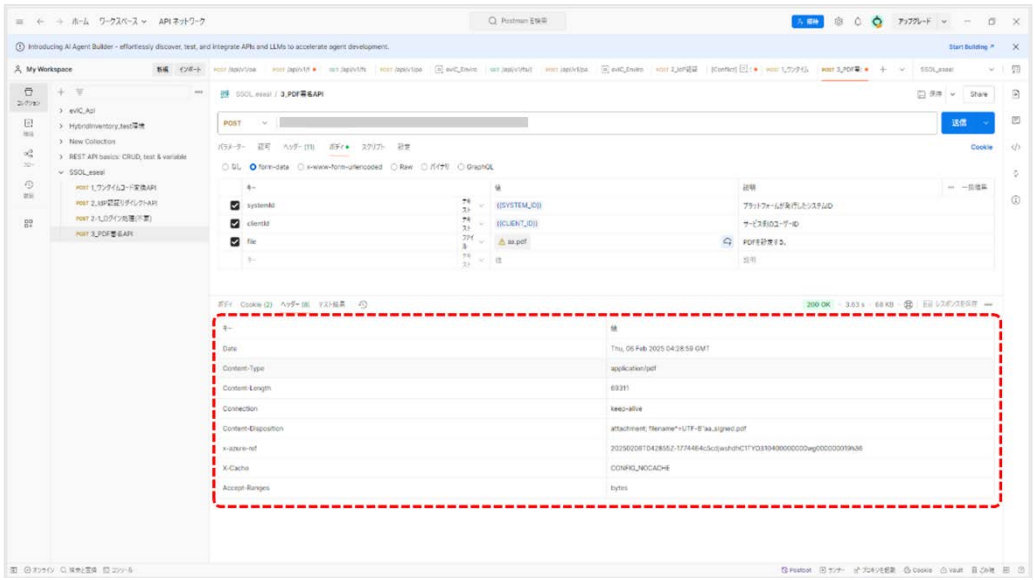

図 54　署名済み PDF ファイルの入手 : API レスポンス - ヘッダー

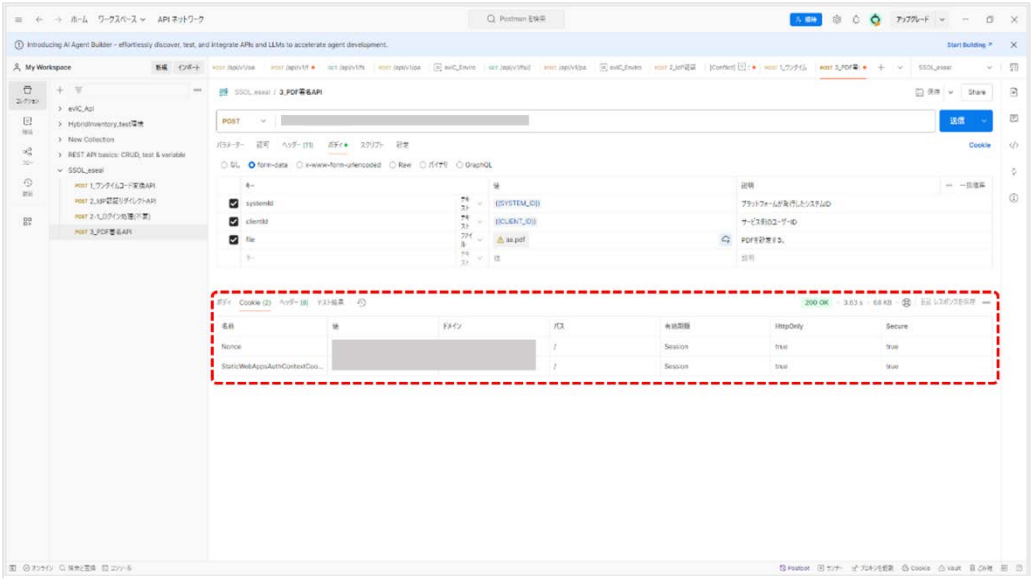

図 55　署名済み PDF ファイルの入手 : API レスポンス - Cookie

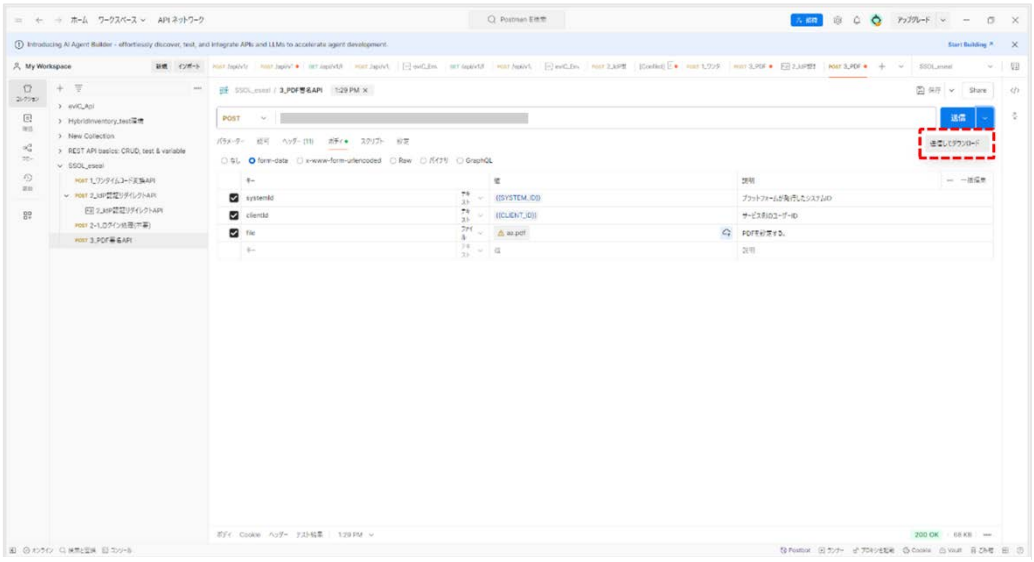

図 56　署名済み PDF ファイルの入手

(6) 署名済み PDF ファイル

※「少なくとも 1 つの署名に問題があります。」メッセージは、電子署名用証明書の信頼済み設定を行っていないため。

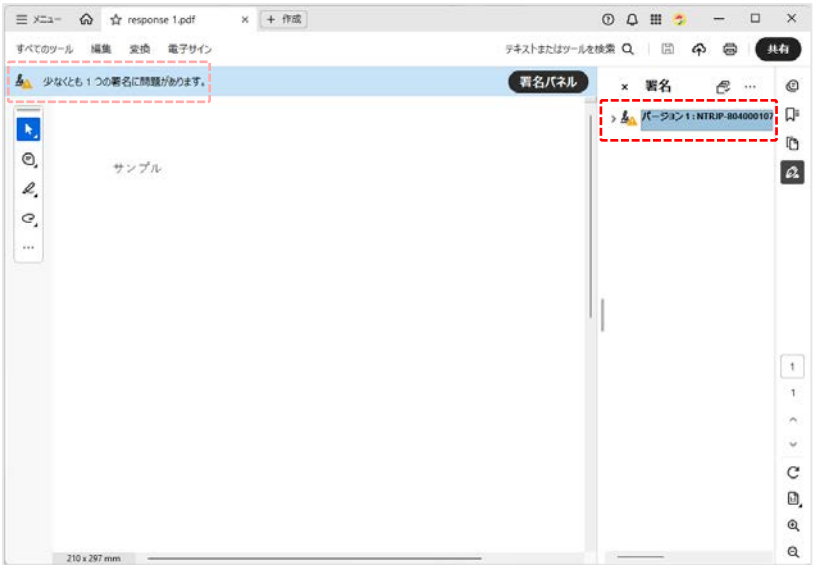

図 57　署名済み PDF ファイル : 展開

・PDF ファイルにおいて、以下の電子証明書による e シール付与が確認できる。

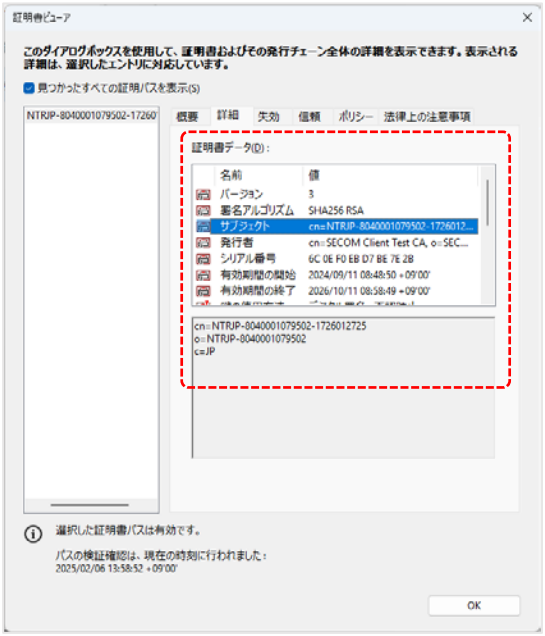

図 58　署名済み PDF ファイル : 証明書ビューア

5.1.2. 株式会社スカイコムによる実証実験

□ サービス事業者サイトへのログインおよび e シール付与操作

(1)サイトにログインして、e シール付与の対象ファイルをアップロードする。

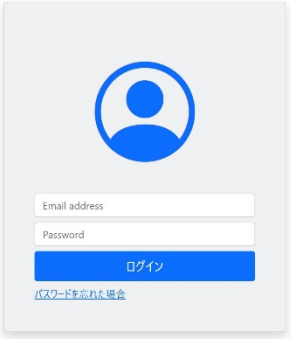

図 59　サイトへのログイン

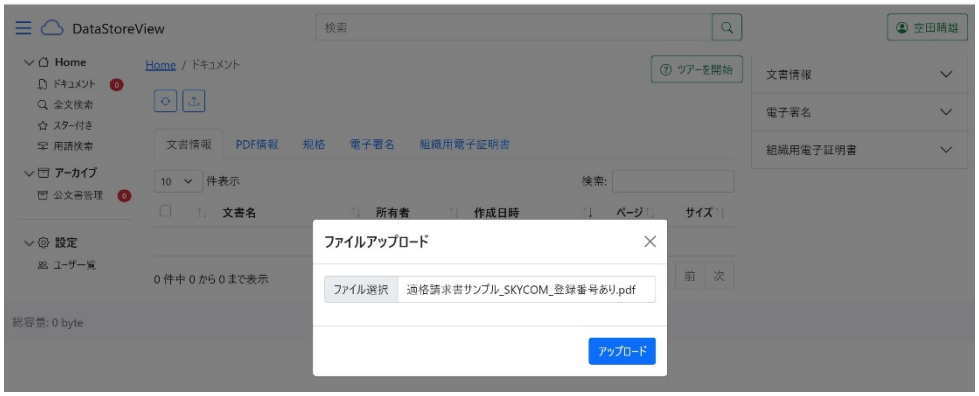

図 60　e シール付与対象ファイルのアップロード

(2)e シール付与を行う。

図 61　e シール付与実施(その 1)

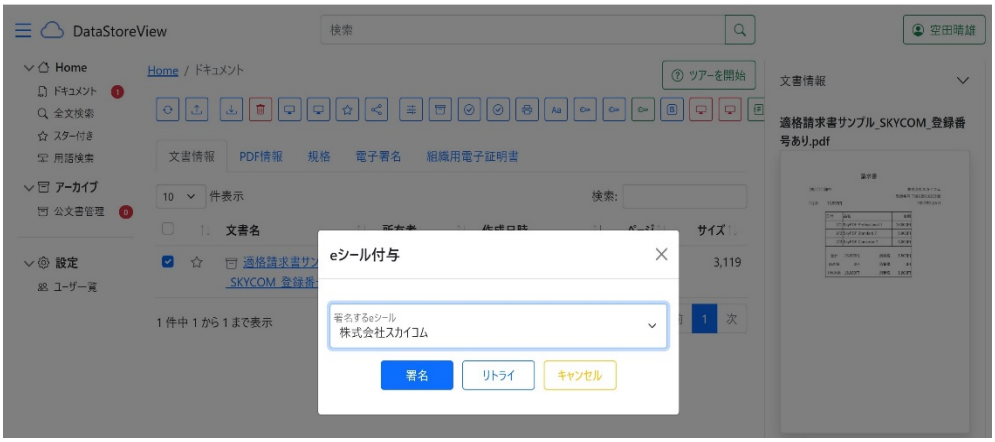

図 62　e シール付与実施(その 2)

e シール付与を実施する際の TDB 認証を行う。

図 63　e シール付与実施(その 3)

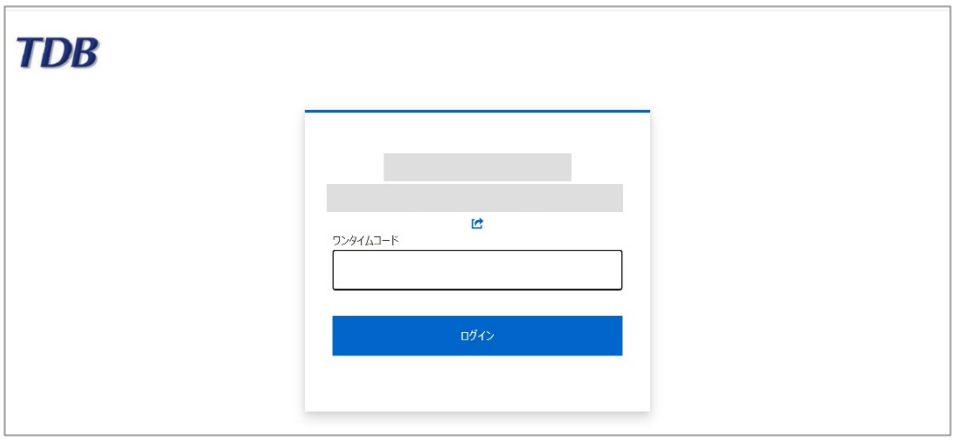

図 64　e シール付与実施(その 4)

図 65　e シール付与実施(その 5)

図 66　e シール付与実施(その 6)

TDB 認証後、継続して処理を行う。

図 67　e シール付与実施(その 7)

(3)e シールの検証。電子署名とタイムスタンプの検証を行う。

図 68　電子署名とタイムスタンプの検証

□ e シール付与済み PDF ファイルの検証

(1) サービス事業者サイトでの検証は、前記の内容をご参照ください。

(2) クライアントソフトでの検証

・ SkyPDF Professional 8 を利用する場合

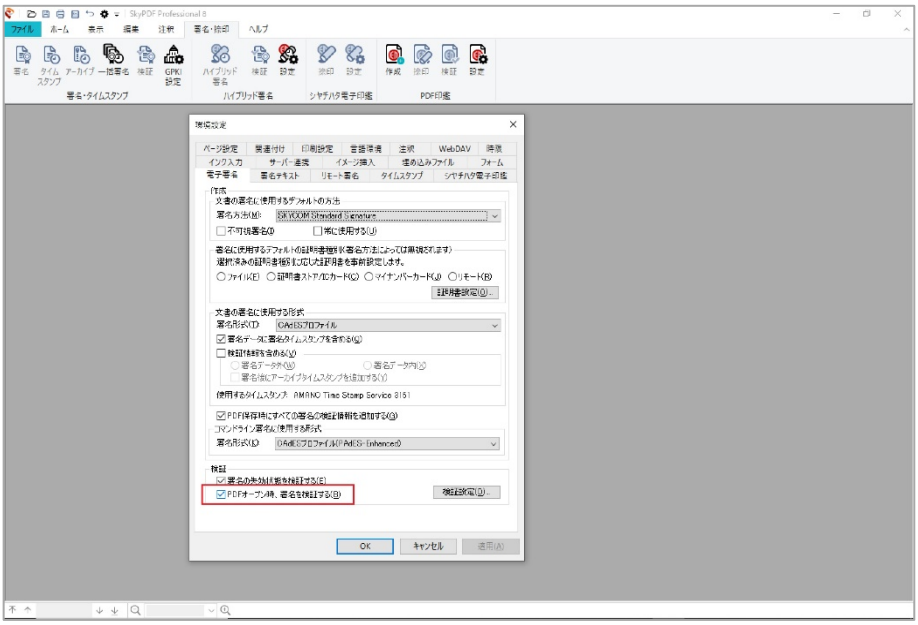

図 69　オープン時の検証設定

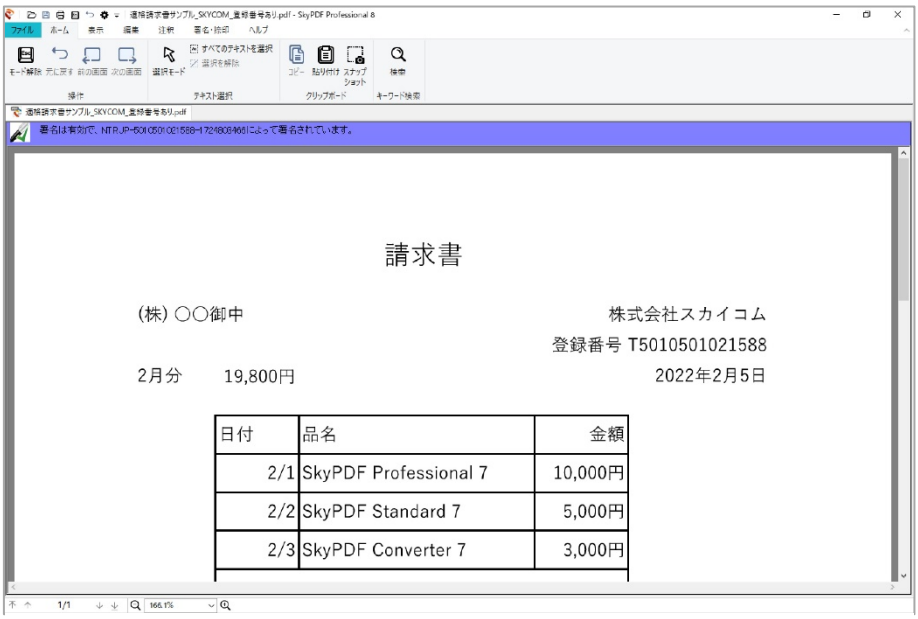

図 70　開いた後

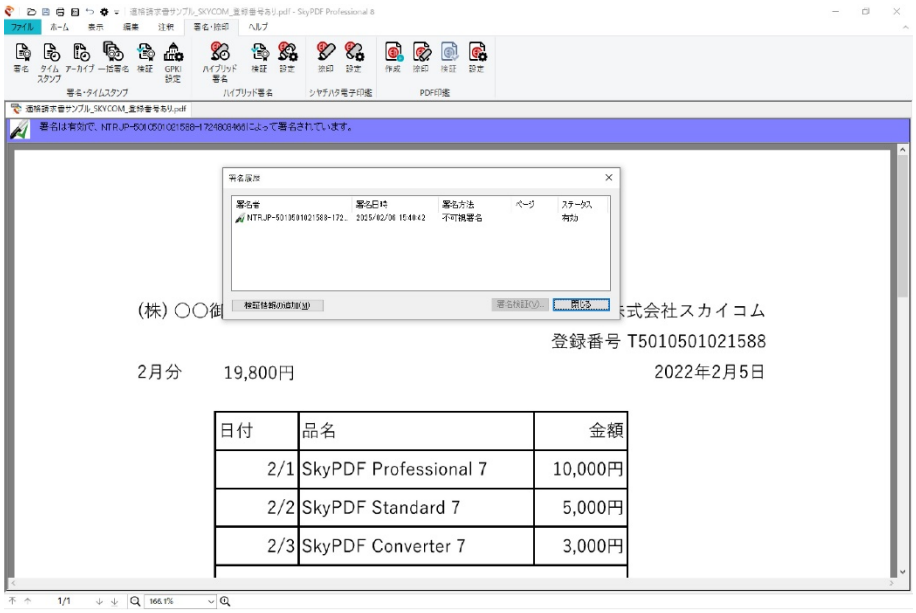

図 71　電子署名とタイムスタンプの検証の詳細(その 1)

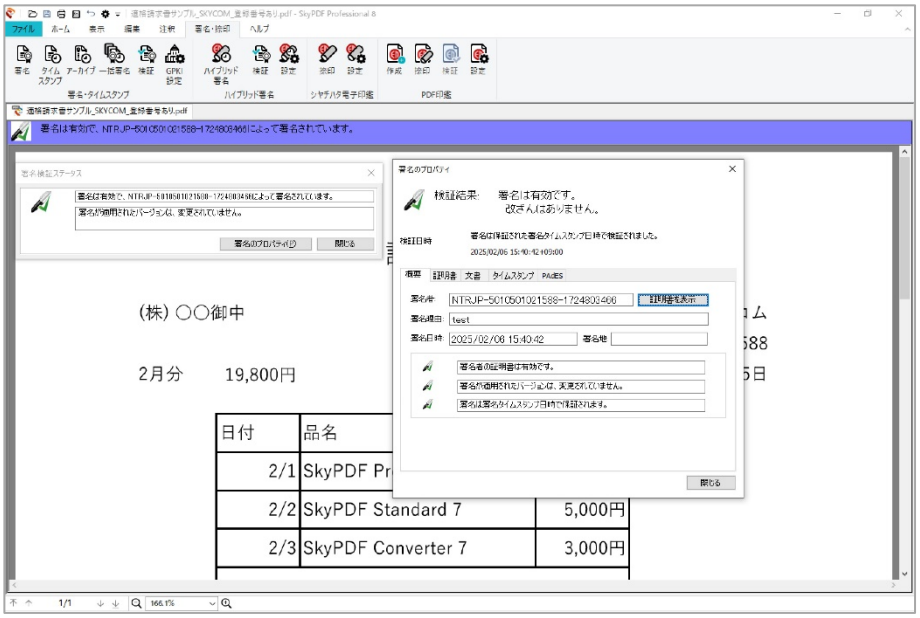

図 72　電子署名とタイムスタンプの検証の詳細(その 2)

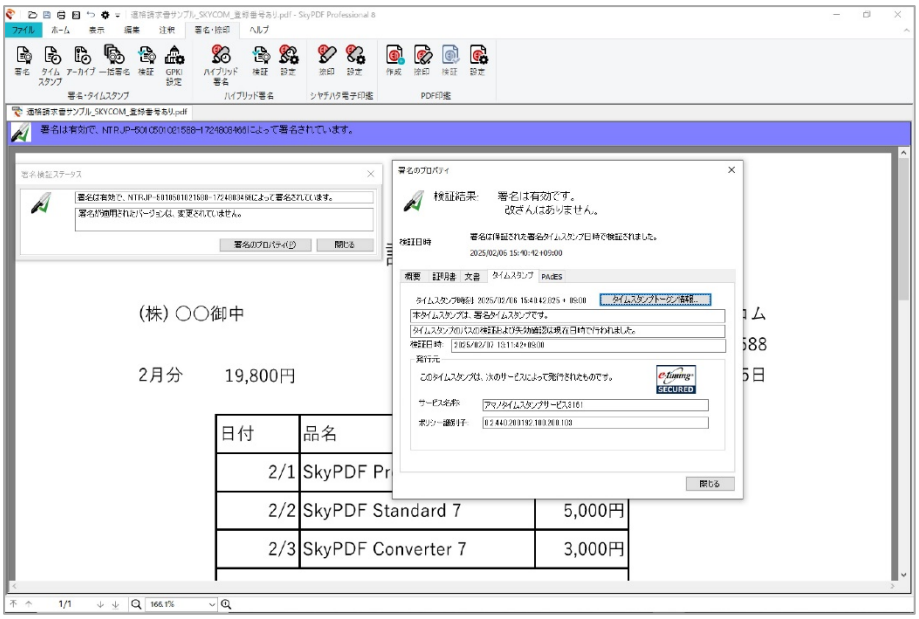

図 73　電子署名とタイムスタンプの検証の詳細(その 3)

5.1.3. 株式会社ハートビーツによる実証実験

□ サービス概要と今回の実証実験参加の目的

重要ファイル転送サービス「Kozutumi」は、ファイルの送受信における信頼性向上と効率アップを実現するファイル転送サービスです。ファイル送受信が手軽に行えるだけでなく、ウイルススキャン、タイムスタンプで送信したファイルの 10 年間の内容証明、サイバーリスク保険自動付帯などの特徴があります。

日本版 e シール実証実験では、タイムスタンプ機能に、さらに e シール機能を加え、これまでの利便性を維持しながら企業や団体などの組織としての正当性を証明することで、さらに信頼性の高いファイル転送サービスを提供してまいります。

□ ファイル送信時の画面遷移

Kozutumi では、PDF ファイルを送信する際に、PDF ファイルに e シールを自動付与し、送信先に届くように実装しています。

(1) メール本文を書き、ファイルをアップロードする。

図 74　メール本文の記載とファイルのアップロード

(2) アップロード後、ウイルスチェックを行った後、PDF ファイルの場合は自動で e シールの付与を行う。

図 75　ウイルスチェック後に e シールを付与

(3) e シールを付与したファイルのタイムスタンプを作成し、宛先へ受信用メールを送信する。

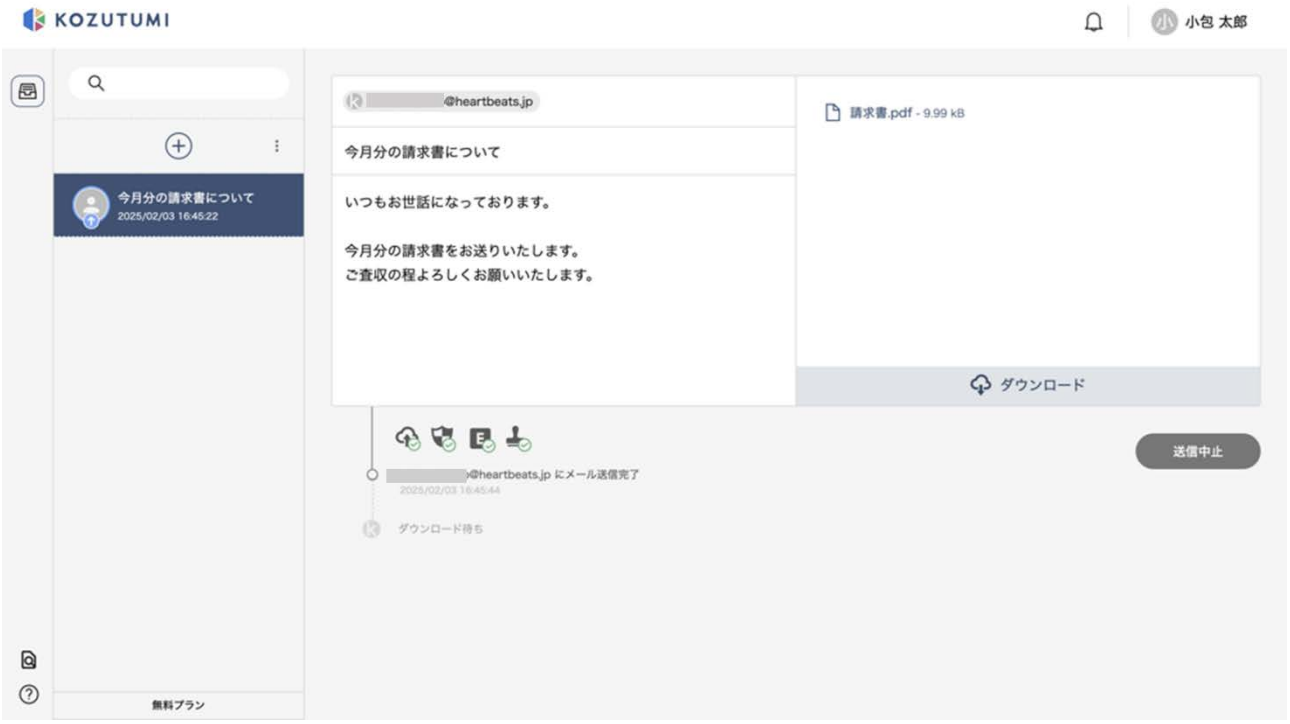

図 76　タイムスタンプを付与後にメール送信

(4) 受信用メールにある受信リンクより、受信者は e シールが付与された PDF ファイルをダウンロードできた。

図 77　受信者による e シールが付与された PDF ファイルのダウンロード

(5) 受信したファイルは、Kozutumi 上の検証画面にアップロードすることで、送信者側のファイルとダウンロードしたファイルが同一かタイムスタンプを用いて検証が可能。

図 78　受信したファイルのタイムスタンプによる正当性の検証

(6) PDF ファイルを Adobe Acrobat で確認することで、PDF ファイルへの e シールが付与されていることも確認できた。

図 79　受信した PDF ファイルの e シール付与確認

5.2. 課題：外部 IdP を利用したトラストサービス連携（2024 年度）

現状ではシンプルな業務運用パターンでの検証のみ実施しており、実運用に合わせた利用方法に合わせて、仕組みの検討や機能の充足が必要になる。

以下は、今後検討していく検討課題の一部である。

■実際の業務に即した ID 管理体系の検討

本実証においては、必要最低限の ID 管理のみ（ID 利用権の付与、利用停止、利用再開）を実施した。ID 管理は、当該組織のみが管理可能なサイトからのみ実施可能とし、各利用者組織内の管理者による管理を前提としている。社員の入退社、組織内の異動等を想定し適切な ID 管理方法を検討し、モデル全体の ID 管理の在り方の再検討が必要である。

※e シール利用者と、ファイル送信サービス等の既存サービスの利用者とは組織毎に権限を付与する社員が異なることが想定されるため、e シール用 ID の付与権限・停止権限は「管理者」のみに付与する仕組みとした。

■利便性及び導入の簡易性

①サービサーの提供するサービスとのシングルサインオンの実現

②サービサー目線での利便性の向上、実装しやすさ、導入しやすさの向上

・e シール付与対象データ：

現状、e シールの付与にあたっては元データ全体をプラットフォームに送信しなければならない。元データが大きくなればなるほどデータ転送量や応答速度が課題となる。元データではなくハッシュ値のみを送信する仕組みとすることも検討課題である。

・課金方法の検討：

e シールと SaaS と連携する際の利用料金の支払いから発行までの自動連係の在り方の検討が必要である。例として、SaaS 側の ID と外部 IdP サービス利用者が TDB で e シール利用を登録し、SaaS 側で課金した場合に自動発行する仕組みがあれば利便性が向上する。

■仕組みおよびシステム観点でのブラッシュアップ、機能充足

③複数鍵を運用した際の鍵の新規作成、利用者の追加、利用者削除、廃棄などライフサイクルに合わせたフローの検討が必要である。

④業務イベント（社員の入退社、所属変更、権限変更など）に伴う運用フローの検討、モデルのブラッシュアップが必要である。

⑤e シール付与時の再認証（トークン有効期間の適切な長さ、リフレッシュトークンの有効期限）

セキュリティ面への考慮から、e シール操作時の当人認証には二要素認証を必須としている。一方で e シールではユースケースとして請求書等の大量の PDF に対する一括処理のように機械による自動付与も想定され、当該ユースケースの場合の在り方は別途検討が必要である。

また、実際の運用を考慮した個々人の e シール署名を許可するための適切なトークンの有効期間を検討しなければならない。例として用途ごとに適切なトークン有効期間設定も可能とすべきか否か、API キー等での認証連携を容易化する仕組みについても検討が必要である。

⑥仕組み全体のセキュリティ向上、監査や証跡に対応したログの運用やトレーサビリティの確保

現状では、e シール付与にあたりプラットフォームに対して元データを送信するため、データの取り扱いについて e シールシステムの信頼性が確保されることが重要となる。プラットフォーム側の堅牢なセキュリティの担保は必須であるが、元データではなくハッシュ値のみを送信する仕組みとする等の検討も必要である。

6. 提言 (2024 年度)

6.1.1. 基準に関する提言

(1) e シール用電子証明書を発行する電子認証局に関する基準

日本国内では「電子署名及び認証業務に関する法律[45]（平成 12 年法律第 102 号)」や同法施行規則[46]、同法指針[47]等で電子署名用電子証明書を発行する電子認証局に関する基準が存在する。

総務省においては 2025 年 1 月 27 日に「e シールに係る認定制度の関係規程策定のための有識者会議取りまとめ（案)」及び「e シールに係る認証業務の認定に関する規程（案)」に対する意見募集（パブリックコメント）が実施された。「本取りまとめ及び本規程に寄せられた意見を踏まえ、速やかに取りまとめ、公表する予定」とのことから、以下 3 点が整備されることになる。

・e シールに係る認証業務の認定に関する規程
・e シール用認証業務の認定に関する実施要項
・e シール用認証業務の認定に関するガイドライン

このため、以上 3 点の整備後に想定されている指定調査機関の早期認定も併せて期待される。

(2) e シール用電子証明書プロファイルに関する基準

前述の e シール用認証業務の認定に関する実施要項(案)により、発行元証明を行う e シールの電子証明書に記載すべきプロファイルの内容が示された。

後述する「共通証明書ポリシーOID」や組織識別子のプレフィクス管理は制度の信頼性観点からも重要であり、関係省庁間での連携を十分に実施いただきたい。

併せて、e シール以外のトラストサービス（例. 電子署名）に対する共通証明書ポリシーOID 設定も、関係省庁と調整いただきたい。

また、国際的な利用において関連する内容として「法人名の英語表記に関する課題」が挙げられる。海外における e シール活用には法人名の英語表記が必要不可欠と容易に想定されるが、現行商業登記制度では法人の和文名称しか確認できない。e シールの検証者や検証処理を行うプログラムが e シール用証明書に記載されている英名表記の確認を行うことを考えた場合、商業登記等のベース・レジストリ[48]に英文名称が登録され、参照可能となることが望ましい。

---

[45]電子署名及び認証業務に関する法律
https://elaws.e-gov.go.jp/document?lawid=412AC0000000102

[46]電子署名及び認証業務に関する法律施行規則
https://elaws.e-gov.go.jp/document?lawid=413M60000418002

[47]電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針
https://www.moj.go.jp/content/001300889.pdf

[48]ベース・レジストリ（デジタル庁)
https://www.digital.go.jp/policies/base_registry

なお、個人事業主の屋号を e シール用証明書の記載対象として扱うべきかに関しても、同様に検討が必要であると考える。

(3) e シール用「共通証明書ポリシーOID」

既に利用されている電子署名と e シールに関する混同を電子証明書プロファイルでも明確に、且つ機械可読で区別可能とするような仕組みが必要であり、共通証明書ポリシーOID が関係省庁において公表され、継続的に維持管理されることが望まれる。

(4) リモート e シールサービス提供に関する基準

リモート署名に関する民間ガイドラインは存在[49]するものの、リモート e シールサービスに関するものは 2025 年 2 月末時点では存在していない。リモート e シールサービスについても上記(1)(2)と同様で「基準が無ければレベル感やセキュリティ基準が不統一な基準群が乱立する可能性がある」ことから、上記(1)および(2)と同様に総務省、もしくは民間での取組が期待される。

なお、以下「6.1.3 サービス連携に関する提言」の①適切な身元確認と当人認証を具備した外部 IdP で必要となるのが「外部 IdP を活用したリモート e シールに関する基準」であり、今後の同基準づくりにおいて想定されるユースケースとしてスコープ内とすることが必要である。

[49]以下が挙げられる。

日本トラストテクノロジー協議会（JT2A）「リモート署名ガイドライン」
https://www.jnsa.org/result/jt2a/2020/index.html

厚生労働省「保健医療福祉分野におけるリモート署名サービス評価基準等について」
https://www.mhlw.go.jp/stf/shingi/000071128_00008.html

デジタル庁「令和５年度電子委任状の普及及びリモート電子署名基準等に関する調査研究業務 最終報告書（詳細版） リモート電子署名基準の検討（案）」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/82a1ea56-128f-4cf6-bbd5-9ef6d4b7bafc/3a91a5bb/20240527_policies_budget_entrustment_deliverables_report_01.pdf

6.1.2. 制度に関する提言

(1) e シールを含む国内のトラストサービスに関する統一的制度

総務省において「e シールに係る認証業務の認定に関する規程」が施行された後においても、現行トラストサービス群では制度上不統一な状況にある。

例えば電子署名は「電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第 3 条」において「法律上の効果が規定」されているが、タイムスタンプや e シールは規定されていない状況にある。

2024 年には民間において以下の提言がなされている。特に国際的な事業を展開する組織だけのみならず流通・サプライチェーン観点から「国境を越えてデータを安全・安心に転々流通・共有できることが必要不可欠」と考えられる。そのためにもトラストサービス全体の共通整備および相互運用性の確保が不可欠且つ喫緊の課題と考えられる。

- 産業データスペースの構築に向けて[50]（2024 年 10 月 15 日）
- 共同提言「データガバナンス戦略の推進」[51]（2024 年 10 月 17 日）
- 共同声明「データスペース等に関する国際標準化の必要性」[52]（2025 年 3 月 6 日）

(2) 国際的な相互運用への配慮

国際的なデータの相互運用や DFFT を想定する場合、e シールのユースケースに応じて、国際的な相互運用性を意識してプロファイルや運用方法を検討することが求められる。国際的な標準化の動向についても注視する必要がある。例えば以下が挙げられる。

- 国際連合
  (Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services)
- ISO/IEC の標準化ドキュメント
  (例.ISO/IEC 27099 Information Technology - Public key infrastructure - Practices and policy framework)
- EU eIDAS および同技術基準
- CA/Browser Forum の様々なガイドライン

---

[50]一般社団法人 日本経済団体連合会「産業データスペースの構築に向けて」
https://www.keidanren.or.jp/policy/2024/073.html

[51]DPFJ、DSA、JDTF 共同提言「データガバナンス戦略の推進」を発表
https://prtimes.jp/main/html/rd/p/000000009.000131931.html
DPFJ(デジタル政策フォーラム、代表幹事：谷脇康彦)
DSA(一般社団法人データ社会推進協議会、代表理事：奥井規晶)
JDTF(一般社団法人デジタルトラスト協議会、理事長：手塚悟)

[52]DPFJ、DSA、JDTF 共同声明「データスペース等に関する国際標準化の必要性」
https://jdtf.or.jp/news/2025/pdf/0306-01.pdf

(3) 共通利用が可能な環境への配慮

デジタル 3 原則（デジタルファースト、ワンスオンリー、コネクテッド・ワンストップ）は、国のみならず民間でも同一であり、e シールは発行元証明を行うツールとして利活用が期待される。e シールの仕組みを社会実装するためには、世の中のサービスで大きな負荷なく e シールを活用できる仕組みや制度が必要になると考えられる。特定のサービスの中だけで成立する仕組みや、e シールを活用することを目的とするサービスの展開は利用の促進には繋がらない。単純なデジタル化のみではなく、業務効率改善を目的とした社会導入への官民を挙げた後押しが必要である。例えば、データスペース等における共通的なトラストサービスの活用などが挙げられる。

(4) 機械可読可能な検証の仕組みの具備

企業等が発行する電子データが増大する中、業務効率化や生産性向上の観点から電子データの発行元を証明可能な e シールの活用が期待されるが、e シールを受け取った検証側にとっては、認定を取得していることを検証・証明できるような「トラストアンカー」の確認手段が重要となる。

トラストアンカーは、データの信頼性を確認するための「信頼の基点」である。電子署名を例にとると、電子署名および認証業務に関する法律に基づいて認定を取得した認定認証業務は政府認証基盤（GPKI）との相互認証を行うことが可能であり、ブリッジ認証局を介して検証者が信頼するトラストアンカーとの間に認証パスを構築することで検証が実施される。

欧州においては、トラストアンカーの開示手段としてトラステッドリストが利用されており、人が介在することなく、機械的に検証することが可能となるような仕組みとなっている。
トラステッドリストは現時点のみならず過去のトラストサービスについても履歴として検証ができるメリットがあり、e シールにおいても早期の取り組みが必要である。

6.1.3. サービス連携に関する提言

前述「4.2 サービス連携」に記載のとおり、利用者が簡便に様々なトラストサービスを利用できる、且つ、活用されるサービスが簡易に様々なトラストサービスと負担無く連携できるようにするためには、以下が必要と想定される。

① 適切な身元確認と当人認証を具備した外部 IdP

e シールの活用方法としてはリモート e シールが想定される。

リモート e シールは、利用者と e シール秘密鍵（および e シール公開鍵証明書）の紐づけが重要であり、利用者の身元確認（e シールの発行元証明という観点から組織内個人が対象と想定）、および当人認証（適切な身元確認が実施された本人に対する適切なクレデンシャルの提供方法、および当人認証のセキュリティレベルなどを含む）が適切に実施される必要がある。

また、複数のサービス間で連携を行う想定がある以上、身元確認、当人認証ともに相当程度のレベルが求められる。

以上からリモート e シールのサービス化にあたっては、関係者における身元確認レベルおよび当人認証レベルの合意が必要であると考えられる。

② 複数サービス・複数トラストサービスを連携可能とするプラットフォーム

e シールの社会実装を促進するためには、利用者およびサービス事業者に対して、e シール活用の負担を下げる仕組みをつくる必要がある。

利用者に対しては、複数のサービスやトラストサービスに対して、別々のアカウント管理や業務オペレーションごとの認証などによる管理や操作の煩雑化を避け、現状業務と同様程度のオペレーションで利用可能なものであるべきと考えられる。

サービス事業者に対しては、各種トラストサービスとのシステム連携インターフェースやシステム間認証の仕組みの開発を、極力簡易にするべきであると考えられる。

一方で、トラストサービスとの連携に対しては、セキュリティ面の考慮やトレーサビリティの担保を行う必要がある。

これらを実現するためには、各サービス事業者と各トラストサービス間でのシステム仕様の調整だけでは限界があるため、連携を安全かつ簡易に実施可能とするプラットフォームが必要になると考えられる。

2024 年度の PoC においてプラットフォームを介した連携を実現した。今後は、サービス事業社のみならず、実際に使用する利用者の意見も取り入れながら、実運用に即したさらなる利便性の向上が必要であると考える。

以上