"「日本版ｅシール」の社会実装に向けた実証実験"報告書

２０２３年６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

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出元が不明となる。データに発出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。

電子データの発出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（発出元確認・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）を行うこととした。

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、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。

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]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 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[4] 3) リモート署名サービス[5] 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

[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
https://www.tdb.co.jp/info/topics/k220701.html

[4]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

[5]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、以下の企業が参加することとなった[6]。

表 2 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	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
富士通株式会社（実施主体）	1020001071491	985732401

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
  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
  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に係る適合性評価を行うサービス
- 一般財団法人日本データ通信協会
  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に係る適合性評価を行うサービス

[6] “「日本版ｅシール」の社会実装に向けた実証実験”参加公募結果
https://www.tdb.co.jp/info/topics/k220704.html

[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]」を立上げた。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[10]」（以下、「総務省指針」）を公表した。同指針において以下のとおり定義されている。

> ＜e シールの定義＞
> *電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み*

以下は総務省指針「図 1 請求書への e シールの活用イメージ」から引用している。

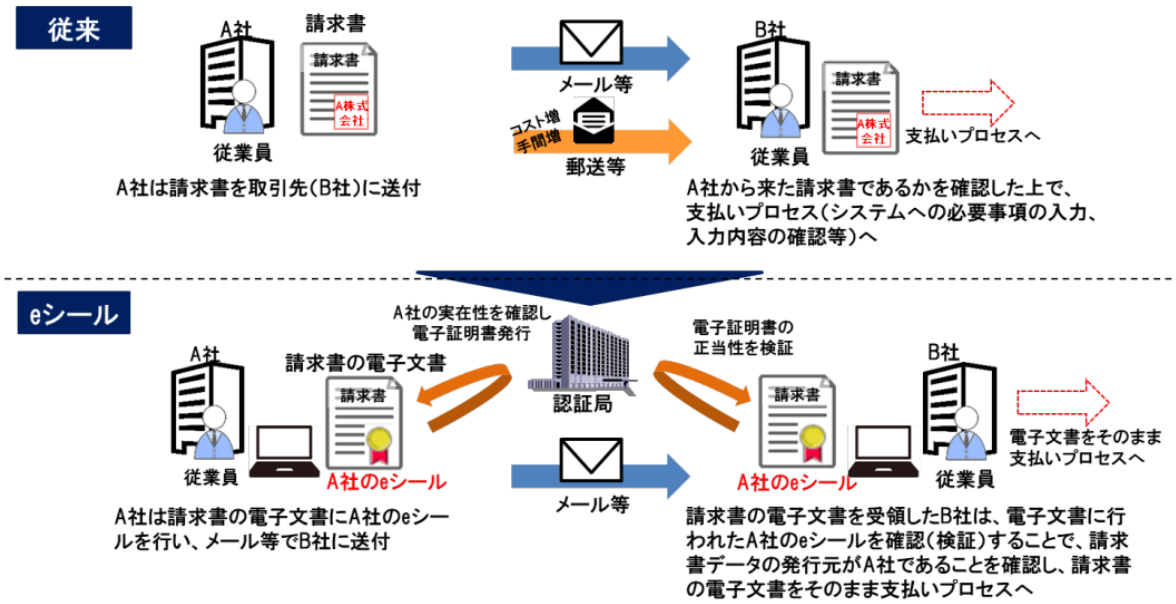

図 1 e シールの活用イメージ図（総務省「e シールに係る指針」より引用）

なお技術的には電子署名と同様であり、法人等の自然人以外を対象として発行された電子証明書に紐づく秘密鍵を用いて e シール対象データを暗号化する措置を指す。

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。

---

[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 シールに係る指針」 https://www.soumu.go.jp/main_content/000756907.pdf

なお EU では eIDAS 規則[11]においてトラストサービスが包括的に規定されている。
e シールについては当該規則の前文に、以下のように効果が記載されている。

> *(59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.（e シールは、電子文書が法人から発行されたことの証拠として、その文書の原本性及び完全性の確実性の確保を提供するものでなければならない。）*
> *(65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.（法人が発行したドキュメントの確認に加えて、e シールを使用して、ソフトウェアコードやサーバなど、法人のデジタル資産を確認できる。）*

また当該規則 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。

[11] eIDAS 規則
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

一方で日本では、2023 年 5 月の段階では公的にも民間においても e シールに関する制度は無い。不統一な規格の乱立や技術不足なサービス提供を未然に防ぐためにも、早期の制度設計に関する検討と整備、運用開始が望まれる。

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（リモートｅシール）

「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 3 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[12]
	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	
設備の基準	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
その他（リモート方式）	レベル２リモート ｅ シールを想定し「利用認証と鍵認可を別々に行わなくてもよい」ものとした	
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	

[12] 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[13] **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[14] ・ ISO/IEC 6523-2[15] ・ ISO/IEC 15459-2[16]
TDB 企業コード[17] **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。	

[13] 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

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

[15] 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

[16] 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

[17] 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。なお、トラストサービスを利用した「トラストアプリケーションサービス」とは混同されるケースが散見されるが、区別して議論・定義・利用をすべきである。

	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」[18]
欧州	'trust service' means an electronic service normally provided for remuneration which consists of: (a)the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b)the creation, verification and validation of certificates for website authentication; or (c)the preservation of electronic signatures, seals or certificates related to those services;	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Article 3 Definitions[19] (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[20] 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[21]

[18]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

[19]REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

[20]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

[21]「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」[22]
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」[23]
	e シールに係る指針[24]
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～[25]
一般財団法人日本情報経済社会推進協会	トラストサービス評価事業 e シール用認証局の審査基準(案)0.1 版
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[26]
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[27]

[22]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

[23]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

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

[25]e シール解説～実用化に向けて～
https://jdtf.or.jp/activity/res/

[26]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

[27]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

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[28]
  - Adobe Acrobat[29]
  - SkyPDF Professional[30]
  - 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）[31]

- 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[32]（以下 Data e-TRUST）
  - Box[33]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[34]
  - Adobe Acrobat[35]

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

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

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

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

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

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

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

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

3. 実証結果と課題

3.1. ローカル e シール

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 [36]、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[37]、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。

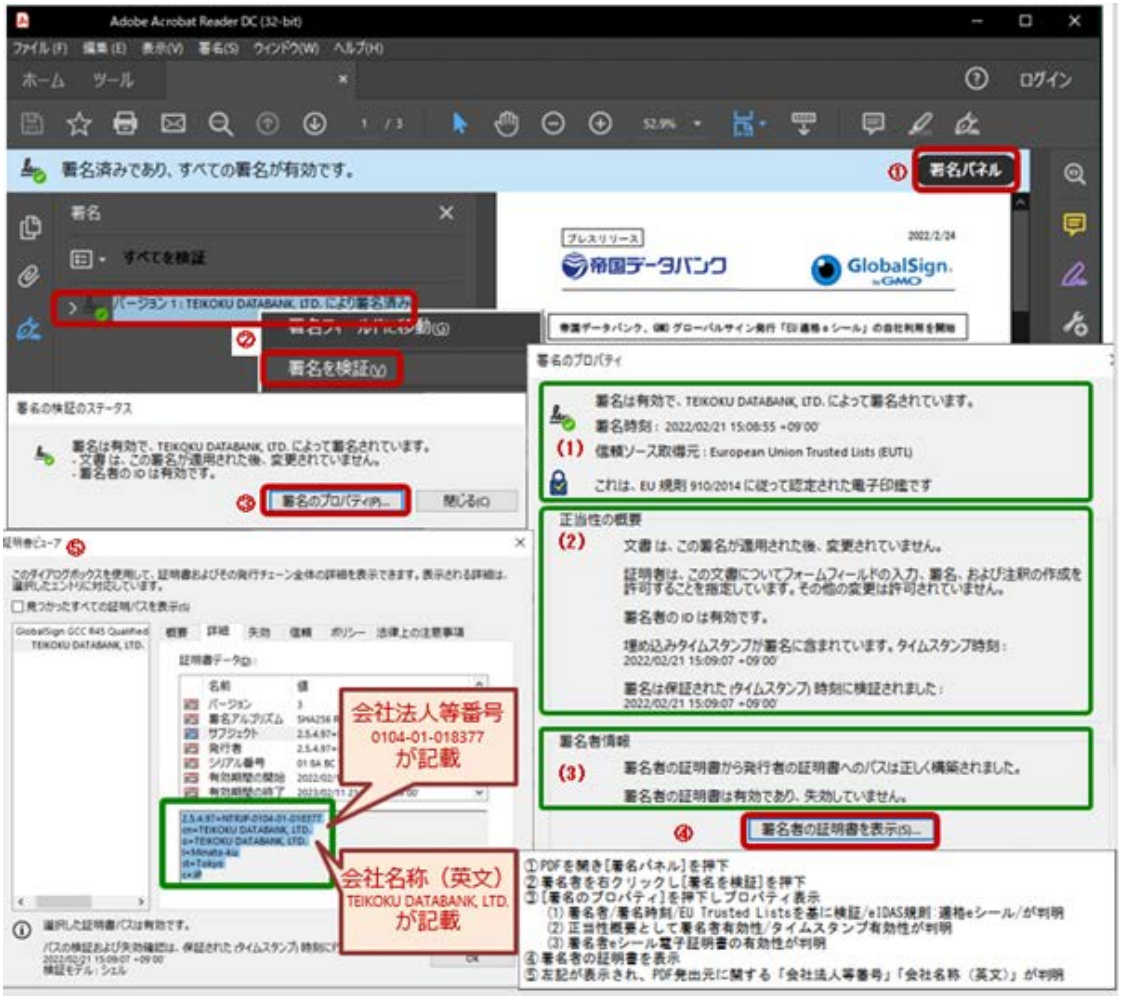

図 2 Adobe Acrobat で EU 適格 e シールを検証した結果

[36]「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

[37]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。

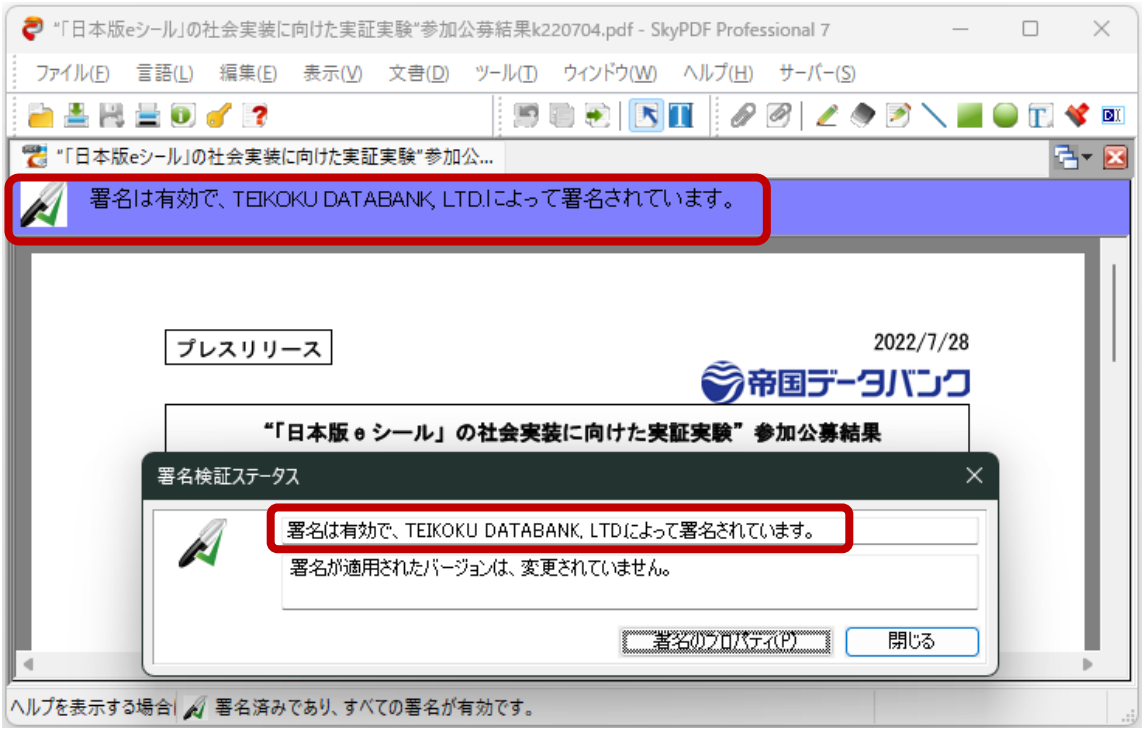

図 3 SkyPDF で検証した結果

3.2. リモート e シール

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。

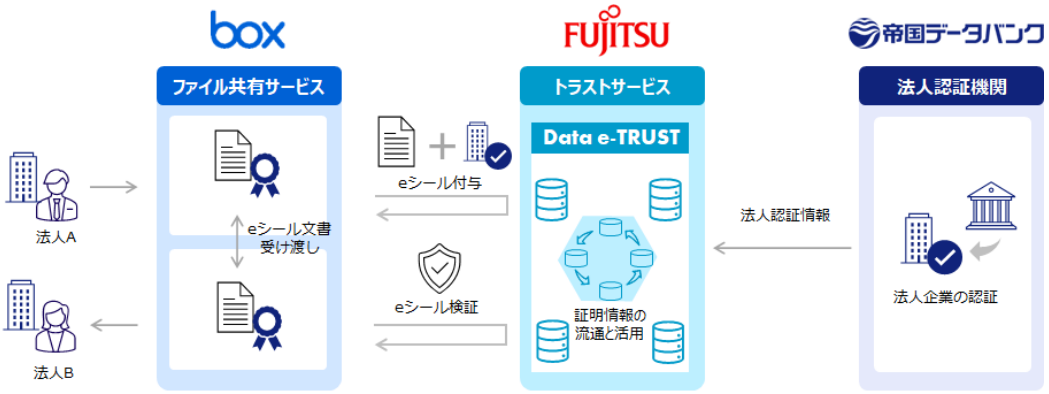

図 4 実証環境概念図

(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 5 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 6 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。

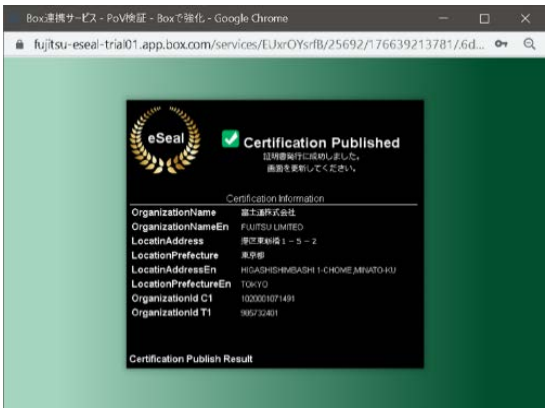

図 7 e シール利用準備完了画面

(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 8 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。

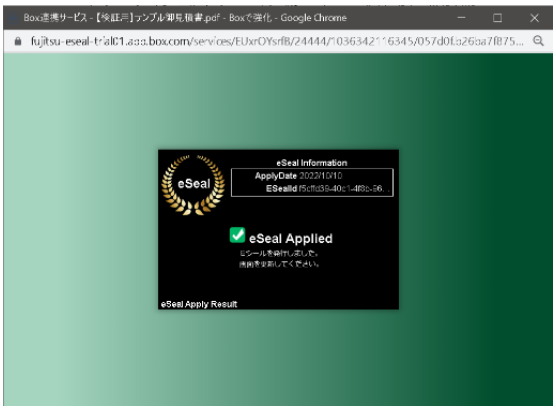

図 9 e シール付与完了画面

(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。

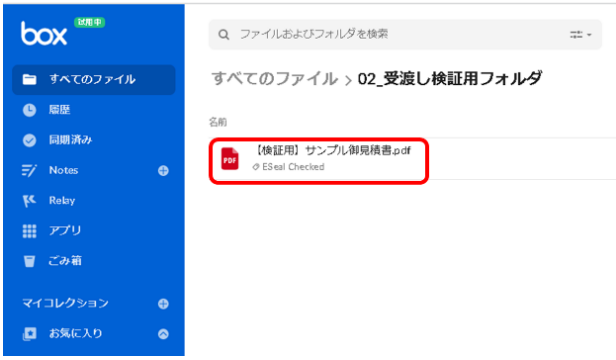

図 10 e シール付与済み確認

(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 11 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出元情報を確認できた。

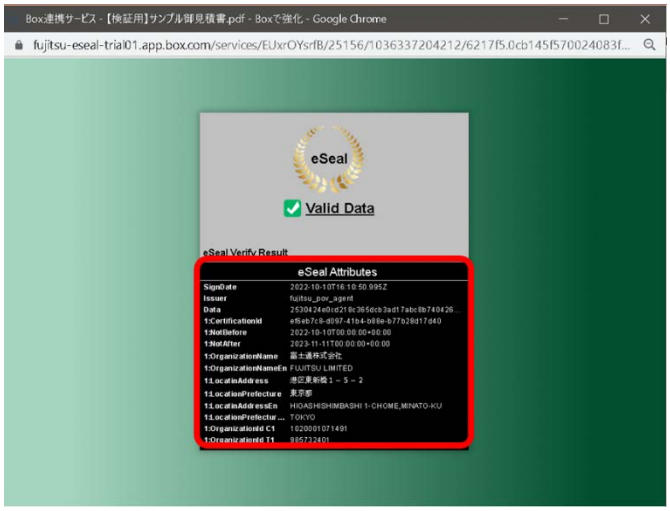

図 12 e シールプロファイル表示結果画面

(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。

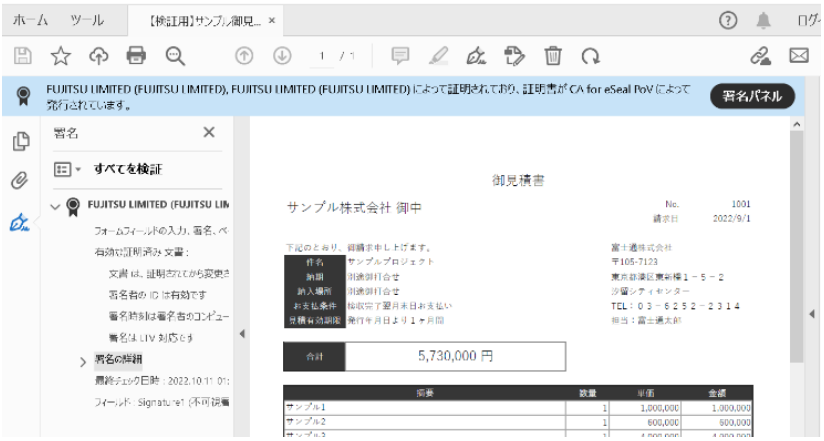

図 13 Adobe Acrobat での e シール付与確認画面

(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出元証明情報を確認できた。

図 14 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

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 15 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。

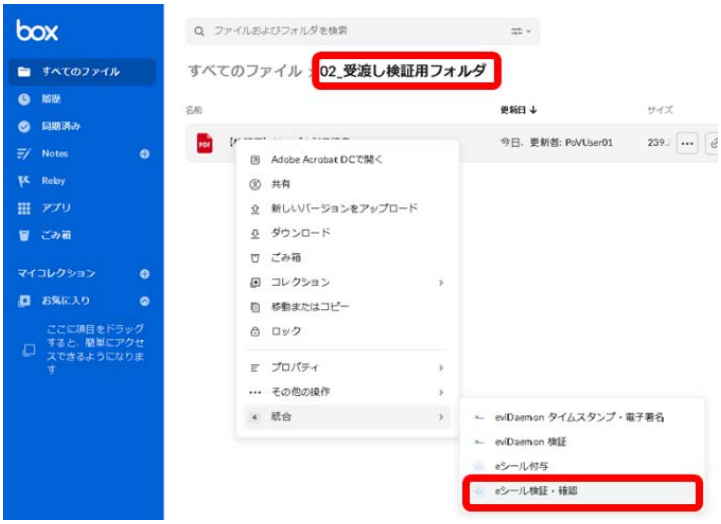

図 16 受取側環境での検証

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

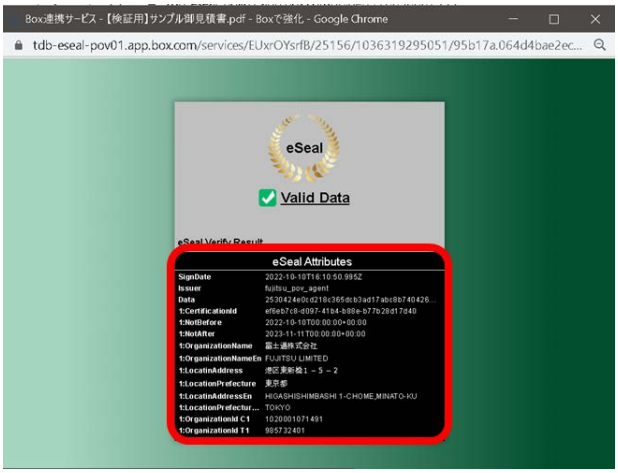

図 17 受取側環境でのｅシールおよび発出元確認

3.4. タイムスタンプ

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。

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 18 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。

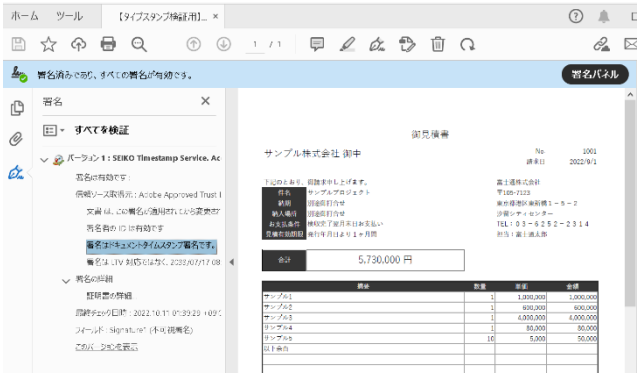

図 19 Adobe Acrobat でのタイムスタンプ確認画面

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

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[38]。

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 シール付与の対象ファイルをアップロードする。

図 20 e シール付与対象ファイルのアップロード

[38] 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 21 e シール付与実施(その 1)

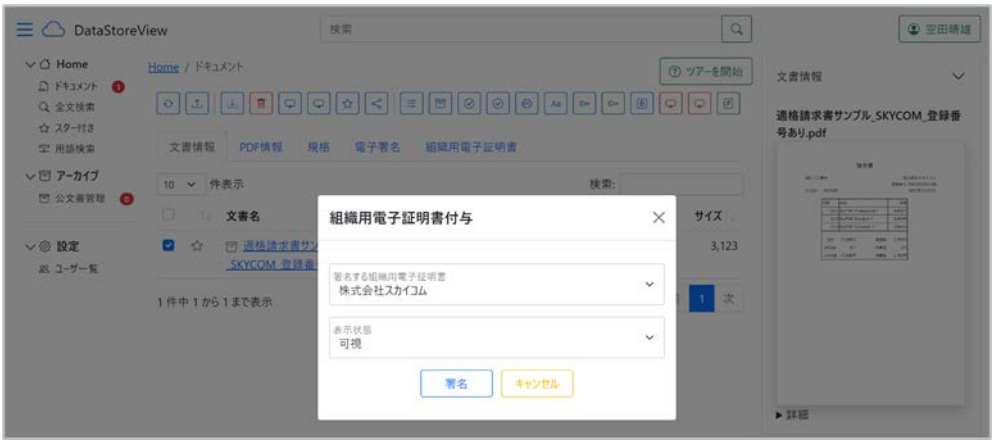

図 22 e シール付与実施(その 2)

(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 23 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 24 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

図 25 適格請求書発行事業者登録番号存在有無確認

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。

□ e シール付与したファイルの一括検証と自動振分け

(1)e シール付与した対象ファイルをアップロードする。

図 26 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 27 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

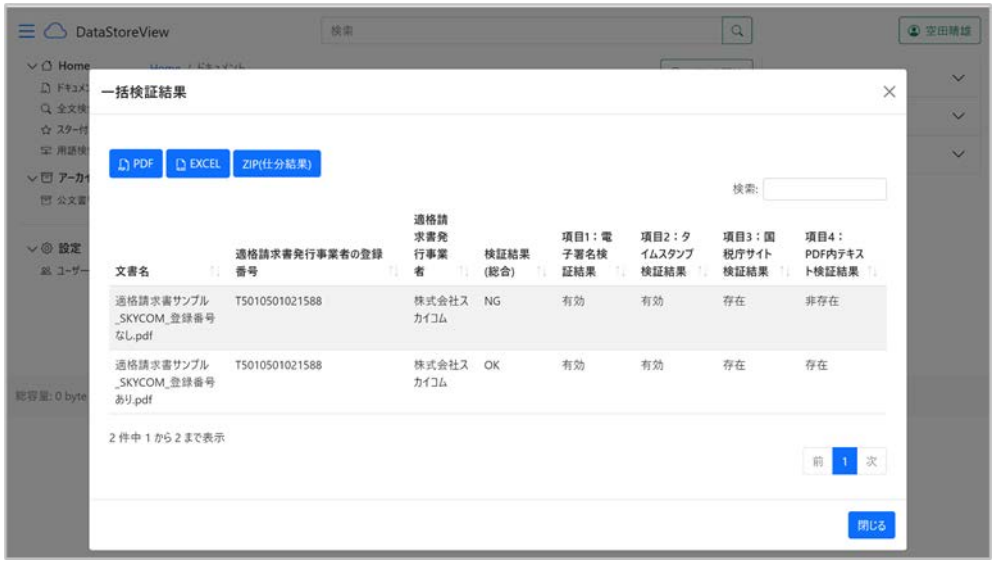

図 28 適格請求書発行事業者登録番号存在確認

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。

(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。

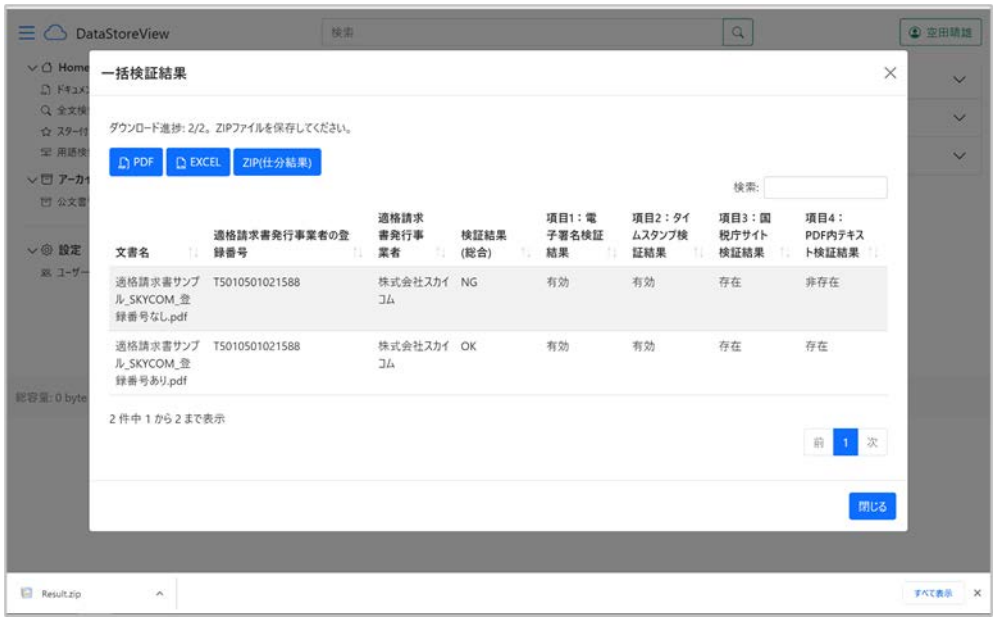

図 29 仕分結果ボタンの押下

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 30 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 31 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 32 検証 OK 分の振分け

図 33 検証 NG 分の振分け

4. まとめと提言

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、サービスへの e シール導入への敷居が上がり、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 シールの発出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。

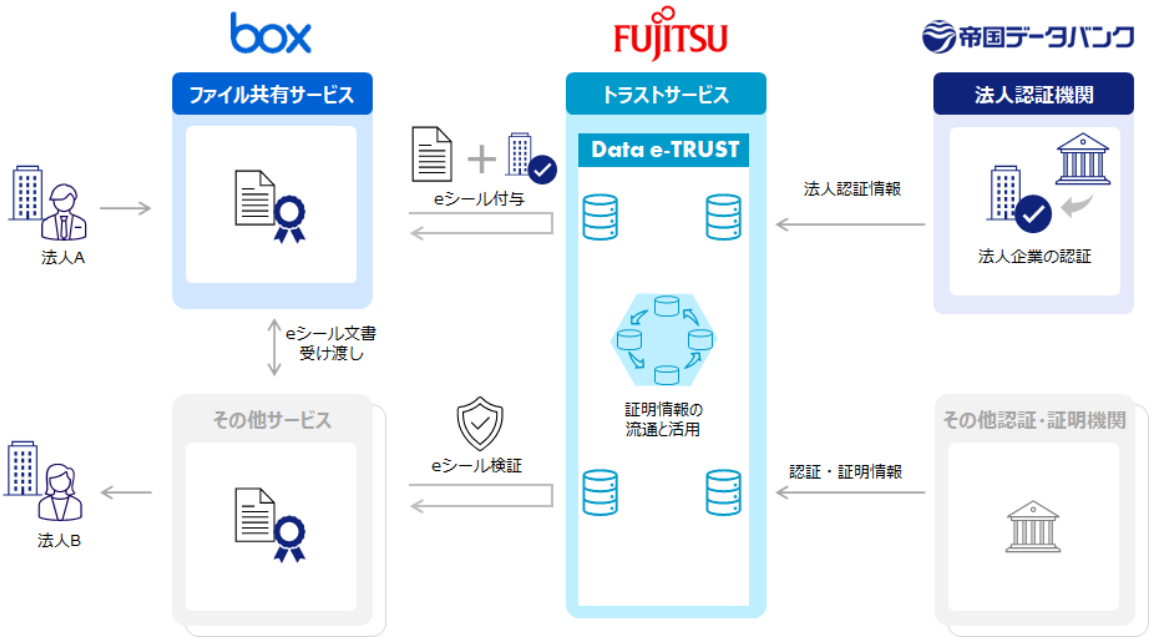

図 34 2022 年 10 月以降の検討概略

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。

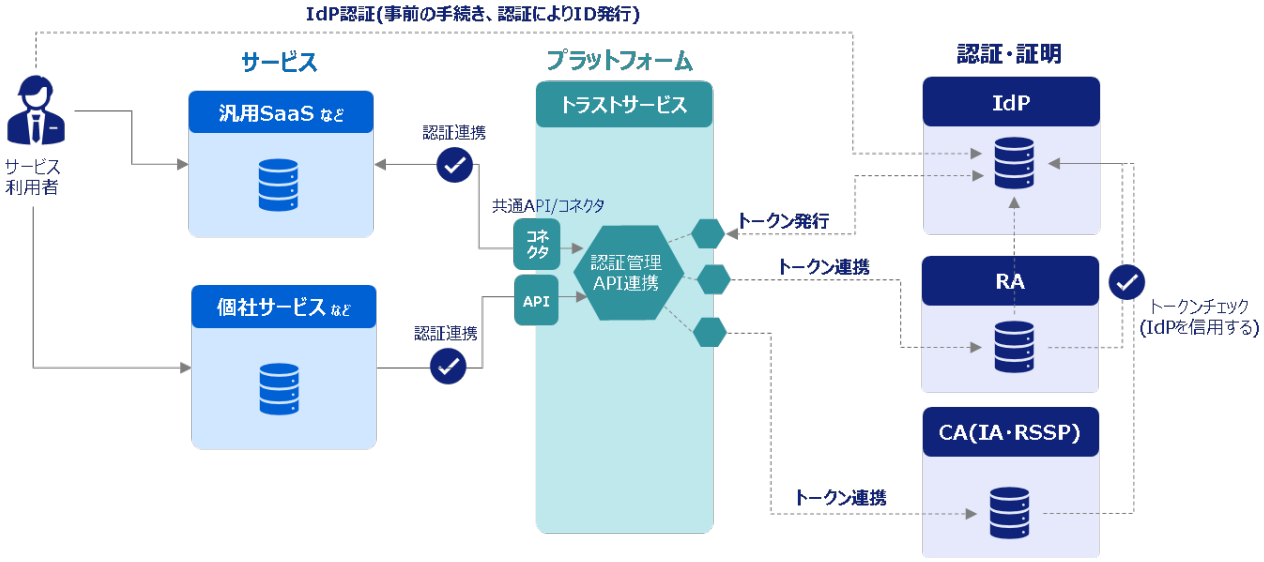

図 35 検討結果概要

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。ユーザー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、ユーザー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。

4.3. 提言

4.3.1. 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

電子署名に限れば、日本国内では「電子署名及び認証業務に関する法律[39]（平成 12 年法律第 102 号)」や同法施行規則[40]、同法指針[41]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。一方で、e シールを発行する電子認証局に関する基準は存在しない。

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も作成されないと、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り、最終的に利用者にとって不利益となることが容易に想定される。極力早期の基準作成が必要である。

デジタル庁「データ戦略推進ワーキンググループ（第 4 回）[42]」の資料 1「データ戦略の推進状況[43]」において「総務省は、デジタル庁による取組の下、タイムスタンプに係る制度運用、e シールに係る制度整備の検討等の取組を行う。」と記載され、同取組に期待するものである。

(2) e シール用電子証明書プロファイルに関する基準

発出元証明を行う e シールの電子証明書プロファイルには「1.4.3 組織識別子」で記載のとおり、組織を一意に識別可能な識別子を格納することが必要である。

当該識別子の番号体系候補としては、複数の候補が存在する（本実証では法人番号と TDB 企業コードを利用)。

organizationIdentifier に格納する際のプレフィックスを日本国内で統一的に決定し周知しておくことで、検証側（様々なシステム）において機械可読が実現できる。

さらに国際的な相互運用を考えた場合、他の国から簡単に参照可能であることが望ましい。

e シールの業界横断的な活用や国際的な相互運用を想定し、organizationIdentifier のプレフィックス管理は、国の基準として決めることが望ましいと考えられる。上記(1)で引用したとおり総務省の取組において検討・確定されることが望ましい。

---

[39]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

[40]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

[41]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

[42]デジタル庁「データ戦略推進ワーキンググループ（第 4 回)」
https://www.digital.go.jp/councils/b565c818-75f4-4990-9125-dd43af8362ba/

[43]デジタル庁「データ戦略推進ワーキンググループ（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

また国際的な利用において関連する内容としては、法人名の英語表記が挙げられる。
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に英文による名称や組織情報が登録され、当該登録情報が参照可能となることが望ましい。
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) 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[44]するものの、リモート e シールサービスに関するものは 2023 年 5 月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。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「4.3.3 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、今後基準づくりにおいては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。

[44]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

4.3.2. 制度に関する提言

(1) 国内の制度

上記「4.3.1 基準に関する提言」で基準が作成された後には、当該基準を満たしたことを適合性評価機関が確認し、確認結果をもとに公表する制度が必要である。サービス実施者が自身で証明するよりも透明性が確保可能であり、利用者は当該制度に基づき必要なサービスを選択できる。

(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。

- EU eIDAS および同技術基準
- CA/Browser Forum の様々なガイドライン
- ISO/IEC の標準化ドキュメント

(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 シールは発出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、世の中のサービスが大きな負荷なく 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。デジタル化、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。

4.3.3. 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 シールの発出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、ユーザー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。

ユーザーに対しては、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。

以上