e シール利用者ガイドライン

Ver1.0

2024 年 4 月

一般社団法人デジタルトラスト協議会（JDTF）

目次

１．はじめに

現代社会では、デジタル技術の発展により、いつでもどこでも瞬時に情報のやりとりができる環境が整備され、対面・書面による商習慣での取引は、業務効率の面で、だんだん支障が出てきています。

一方で、デジタルデータは、痕跡もなく変更ができ、容易に複製・発信ができてしまうことから、正しい情報かどうかの判断が難しく、信用のもと成立している取引では、そのまま疑うことなく利用するには課題があります。

デジタル化を促進し、業務改革や生産性向上のためには、組織などが発行するデータの信頼性を確保する仕組みの検討が必要であるとして、総務省において、令和２年（2020 年）から３年（2021 年）にかけて、「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」が開催され、「ｅシールに係る指針」[1]として令和３年（2021 年）６月にとりまとめられました。

この指針では、ｅシールは、「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」として定義されました。

その後、デジタル庁の「トラストを確保した DX 推進サブワーキンググループ」で議論がされ、デジタル社会の実現に向けた重点計画[2]（令和５年６月閣議決定）において、当面重点的に取り組むべき事項としてｅシールの信頼性を評価する基準策定及び適合性評価の実現が挙げられました。

これらの背景のもと、今般、令和５年（2023 年）９月より、総務省において、ｅシールに係る検討会[3]が開始され、制度化に向けて検討が進められました。

この検討会の最終とりまとめにて、ｅシールは転々流通する情報に付与されることから、「措置」ではなく「データ」として捉え、その要素として「origin（出所・起源）」と「integrity（完全性）」を盛り込むことが示されました。[4]

---

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

[2] 重点計画：
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

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

[4] 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

JDTF では、 e シールに係る指針を踏まえて 2022 年 9 月に、 e シールの技術的・運用上の観点から「 e シール解説〜実用化にむけて〜」[5]として整理し公開しました。

本書は、 e シールを利用する事業者側のガバナンス指針を具体的に示すガイドラインとして整理しています。デジタル時代の商習慣において、信頼のおけるデジタルデータをやりとりするため、 e シールの利活用を検討する一助となれば幸いです。

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

[5] 「 e シール解説〜実用化に向けて〜」: https://jdtf.or.jp/report/whitepaper/file/e シール解説%28 バージョン 1.0%29.pdf

２．本書の目的

本書は、デジタルデータの発行元の証明をするために、e シールの利用を検討する事業者向けのガイドラインです。e シールを利用する事業者の経営者、実務者およびシステム担当者を想定読者対象としています。

e シールに関わるサービスやシステムを提供する事業者や、e シールを利用してサービスを提供する e シール関連事業者は、「e シール解説～実用化に向けて～」[6]を参照ください。

図 2-1 に、本書のスコープを記載します。

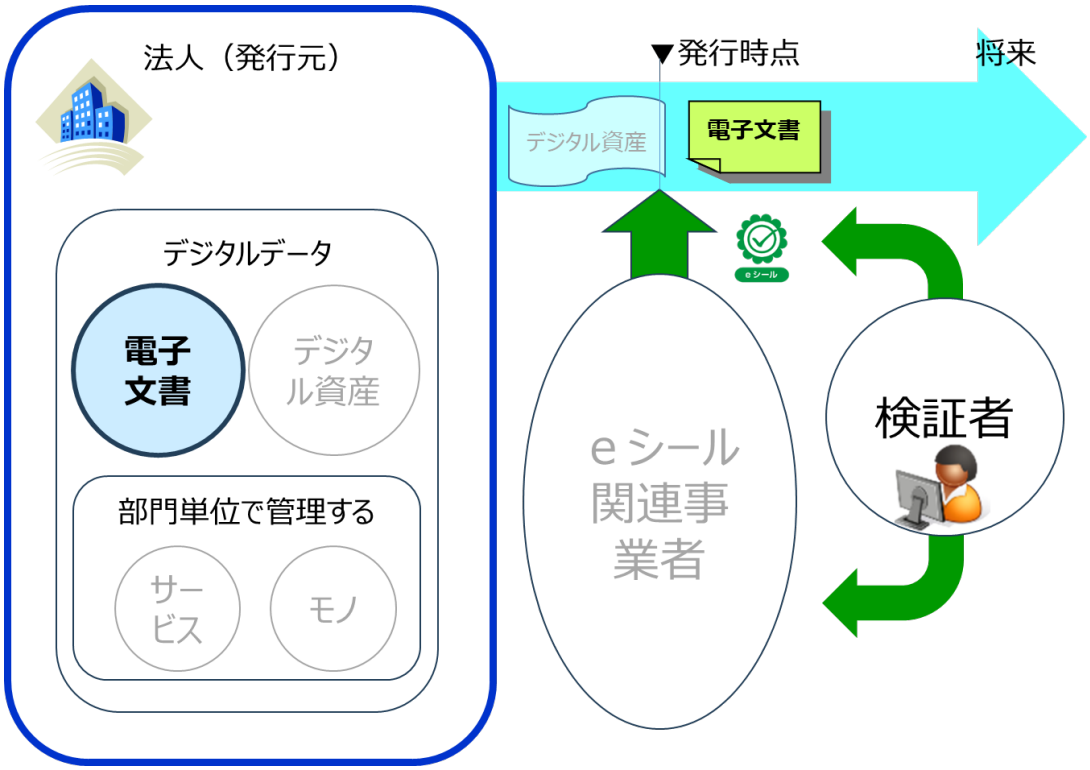


図 2-1　本書のスコープ

本書では、e シール付与対象をデジタルデータのうち電子文書とし、対象電子文書の発出元を確認・検証するステークホルダーが対象電子文書の入手時点のみならず、将来にわたって存在することを前提に、e シール関連の事業者を選択するうえでの判断ポイントを整理します。

---

[6] 「e シール解説～実用化に向けて～」：https://jdtf.or.jp/report/whitepaper/file/e シール解説%28 バージョン 1.0%29.pdf

３．用語

本章にて、本書で記載している用語を、利用者視点で整理して記載します。

公開鍵暗号方式基盤（PKI：Public Key infrastructure）

暗号鍵の生成時に、鍵のペア（秘密鍵と公開鍵）を生成し、一方の鍵で暗号化されたものは他方の鍵でのみ復号できる公開鍵暗号方式を利用した暗号基盤です。
第三者である認証局が、対象秘密鍵の管理者の実在を確認し、公開鍵を含む電子証明書を発行することで、当該電子証明書の検証により、秘密鍵の管理者を特定する仕組みです。

デジタル署名

公開鍵暗号方式基盤（PKI）を利用して、電子文書が信頼できることを証明する技術です。対象の電子文書を一方向関数で一定の数値にしたものを秘密鍵で暗号処理することで、なりすまし、改ざんを防止します。

電子署名

自然人が管理している秘密鍵によるデジタル署名措置です。
署名対象の文書について、自然人本人の意思表示が可能です。
電子署名法[7]にて、本人のみが付すことができることを適正に管理することで、対象文書の正当性を推定することが認められています。

e シール

組織が管理している秘密鍵によるデジタル署名データです。
署名対象の文書について、発行元を特定し、署名以降の改ざん検知が可能です。

e シール署名鍵

e シール生成時に対象データの暗号処理で使用する秘密鍵です。

e シール用電子証明書

第三者機関である認証局が、e シール署名鍵の管理組織の実在確認をして発行する、署名鍵のペアである公開鍵を含む電子証明書です。

---

[7] 電子署名法（正式名称「電子署名及び認証業務に関する法律」）：電子署名法及び関係法令については下記 URL を参照ください。
https://www.digital.go.jp/policies/digitalsign_law

タイムスタンプ

対象文書に、第三者であるタイムスタンプ局が管理する信頼のおける時刻を付与し、タイムスタンプ局の秘密鍵によってデジタル署名されたトークンです。
対象文書が、その時点に存在したことと、その時点以降の改ざん検知が可能です。

日本では、総務省告示によって適正な信頼性を確保した事業者を認定する制度[8]があり、安全・安心なタイムスタンプが提供されています。

トラストサービス[9]

オンライン環境における、電子取引の信頼を高めるためのサービスです。

電子署名、e シール、タイムスタンプ等の、対象文書の完全性を保証するサービスです。

ベースレジストリ

行政又は民間におけるサービスの共通基盤として利活用すべき又は利活用可能なデータ群であって、行政機関等が正当な権限に基づいて収集し、正確性や完全性の観点から信頼できる情報を基にした、最新性、標準適合性、可用性等の品質を満たすものです。

現在、法人番号公表サイトが指定されています。今後、より充実されることが期待されます。

---

[8] タイムスタンプについては、下記 URL を参照ください。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

[9] 国際連合国際商取引法委員会（UNCITRAL）にて策定されたモデル法では、下記のように定義されています。
“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;

４． ｅシールの有用性（企業におけるデジタル業務のリスクと対策）

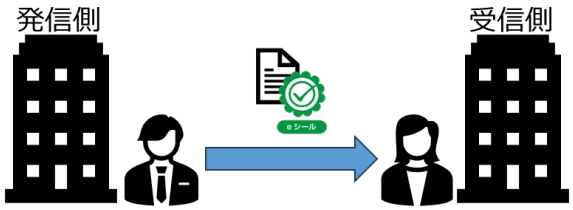
企業が発行する情報には、企業名であったり、企業内部門名やサービス名が記載されており、自然人個人を表すこともなく、発行元を明示することが通例となっています。
さらに、商取引における証票の場合には、より発行情報の信憑性を示すため、会社内ガバナンスの効いたフローを通すという意味から、ワークフロー管理や、その保証を対外的に目に見えるようにするため角印等の押印処理をしています。

これらは、書面によるビジネス慣習における偽造対応措置の商習慣として広く社会に浸透しているものです。しかし、作成者を特定できないデジタルデータで資料が作成され、発出元を特定する印影も、単なる画像のコピーであったり、元の印章そのものも、3D マシンで容易に生成できてしまう現代において、これまでの書面による取引における発出元の記載は、既に、形骸化されているのではないでしょうか。

容易になりすましや改ざんが可能なデジタルデータでは、その行為直接による被害のみならず、なりすましや改ざんが可能であることにより、事後に「相手方がデジタルデータを正しいと認めない、自分側も正しいと証明できない」という問題が生じる可能性があります。法人組織として、企業活動をより効率的に推進するために、これらのリスクを避けて発出元を特定するデジタル技術が、組織として情報の発出元を保証するｅシールです。

ｅシールを利用することで、発信側は、自社組織が正しく運用されたガバナンスの効いた組織として信用を高めることができます。受信側は受領したデジタルデータの発出元を特定できると共に、改ざんされていないことを確認できます。

さらにｅシール用電子証明書に記載されている識別子などから、信頼できる第三者データベースなどを利用して、その確からしさや属性を確実に確認できます。この仕組みを活用し、自動でスクリーニングすることが可能となり、デジタルデータの信頼性を手間なく確認でき、安心してデジタル社会でのビジネスを行うことができます。



自社組織が正しく運用されたガバナンスの効いた組織として信用を高めることができる	受領したデジタルデータの発出元を特定できると共に、改ざんされていないことを確認できる

図４　ｅシールの有用性

５． e シールの保証レベル（選択の仕方）

本書では、 e シールの保証レベルを「 e シール解説～実用化に向けて～」[10] 8.2 e シールの保証レベルの考え方に準拠し、第三者による実在確認がされることで、発出元の信頼性を一定程度の保証ができるレベル 2 以上の e シール用電子証明書を利用することを想定して記載します。

表 5-1　 e シールの保証レベルの考え方

	レベル１	レベル２	レベル３
レベル概要	発行元証明に必要とされる最低限の組織確認が行われるレベル。	国並びに国に準ずる機関又は中立・公正な機関が作成した基準に基づく適合性評価を受けたレベル。 日本国内において幅広く利用される。	国際相互承認の対象となる適合性評価を受けたレベル。 厳格な組織確認を必要とする。

参照)「 e シール解説～実用化に向けて～」表 8-1

なお、総務省の e シールに係る検討会では、「 e シールの保証レベル」として、その用途に応じ、①総務大臣による認定を受けた e シール用認証業務によって保証されてはいないが、より低コスト・簡易な手続きで大量発行される e シールに期待される保証レベル（ e シールの定義に合致するもの）と、②認定 e シール用認証業務によって保証され、 e シールが付された電子データの起源や改変が行われていないことについて高い信頼が期待される保証レベルの 2 段階まで整理され、国際相互承認を見据えた上位レベルであるレベル 3 は、中長期的に検討する課題として整理されました。

実際に、企業において、さまざまな用途で e シールが利用されることを考慮し、各用途に合わせ、保証レベルを選択され、そのレベルを保つため組織として守るべく運用等を第 9 章「各フェーズにおけるリスクと注意すべき点」に合わせて各フェーズにおけるリスクと注意点を認識して検討されることを推奨します。

[10] 「 e シール解説～実用化に向けて～」: https://jdtf.or.jp/report/whitepaper/file/e シール解説%28 バージョン 1.0%29.pdf

６． ｅシール用電子証明書の発行対象

ｅシール用電子証明書の発行対象は、総務省で実施している「ｅシールに係る検討会」（2024 年 3 月時点）において、

① 法人および権利能力無き社団・財団
② 法人に属する事業所・営業所・支店・部門等
③ 意思表示を伴わない担当者
④ 任意の団体
⑤ 個人事業主
⑥ 機器

を対象として整理されています。

発行対象として整理している上記①～⑥すべてにおいて、ｅシール用電子証明書は、認証局による実在確認のうえ発行されます。この中で公的な認定制度事業者によるｅシール用電子証明書は、「①法人および権利能力無き社団・財団」に対して発行される方針です。

その他②～⑥のうち、「②法人に属する事業所・営業所・支店・部門等」および「③意思表示を伴わない担当者」については、組織等の代表者の宣言結果を尊重し、発行対象である組織等が一義的な責任を負うことを前提として、ｅシール用電子証明書の拡張領域に記載することが可能とされています。

「⑤個人事業主」については、デジタル庁における「個人事業主の番号体系」の検討状況[11]を注視しながら、引き続きの検討となるとされています。

「⑥機器」ついては②や③と同様に整理されていますが、独立して稼働することから、その管理方法などの整備については一層の検討が求められることとなると思われます。

④～⑥についても、今後、公的な認定制度事業者によるｅシール用電子証明書の発行ができるように検討が進んでいくと考えられます。

なお、この整理では対象となっていませんが、組織が管理するシステムやアプリケーションが発行するデータについては、今後ｅシールの対象となることも想定されます。

ｅシール用証明書を発行する認証局は基本的に信頼できる情報源を参照し、確認できた

---

[11] デジタル社会の実現に向けた重点計画（2023年6月9日）６．AI 活用及びデータ戦略の推進（２）包括的データ戦略の推進と今後の取組、「個人事業主の番号体系について、本人確認や情報連携等の具体的なユースケースの整理を行った上で、制度的な対応を含めた検討を行い、2023 年（令和５年）内に具体的な結論を出す。」

情報を記載しています。情報源に登録されておらず、確認ができない情報については電子証明書への記載が難しく、申請者の宣言による担保をどのように確保するのかによります。また、記載する箇所も e シール用電子証明書の任意のフィールドである拡張領域に記載するなど認証局の発行対応が変わります。

JDTF では、「e シール解説～実用化に向けて～」[12] 8.3.2 組織や代表者等の確認方法にて、e シールの保証レベルに対して、組織や組織の下で構成される内部属性の確認レベルの案を提示しています。

[12] 「e シール解説～実用化に向けて～」：https://jdtf.or.jp/report/whitepaper/file/e シール解説%28 バージョン 1.0%29.pdf

７．発行対象の各利用部門での導入～運用

本章では実際の導入や運用について、ｅシール固有の検討ポイント等を含めて説明します。ｅシールは発行元証明であることから特にセキュリティ面には注意が必要です。

７-１　ｅシールの導入

ｅシール導入の一般的な流れは以下のようになります。導入の目的や規模等によって、様々な進め方が考えられますので、自社の状況に応じて柔軟に対応してください。

STEP1	プロジェクトの立上げ
STEP2	プロジェクトの遂行
STEP3	利用者・取引先への説明
STEP4	運用の開始

STEP 1 プロジェクトの立上げ

自社発行証明が有効な業務があり、ｅシールの導入を検討するフェーズです。

導入にあたっては、主管部門の他にも複数の関係部署や取引先も検討に含める場合があります。

プロジェクトの目的をはっきりさせ、明確なゴールを目指しましょう。

●検討事項

導入の目的	導入目的を明確にします。 ※ｅシールの活用用途は様々です、最初から広範囲を対象とすると、本来の目的を見失ってしまう恐れがあります。
スコープ （対象業務）	まずはどのような業務でｅシールを利用するのかスコープを決定します。複数の業務での利用を検討している場合は、フェーズを分けて対応するのもお勧めです。
体制	対象業務が決まれば、主管部門や利用部門が見えてきます。 早い段階で運用部門とも連携するように体制を組みましょう。 意思決定者を明確にしておくとスムーズに推進できます。
期間・予算	いつまでに達成したいのか、予算はどの程度が妥当かをプロジェクト立上げ時に明確にしておきます。

関係者間で上記の合意を取り、プロジェクトを開始します。

STEP 2 プロジェクトの遂行

実際にプロジェクトが開始されると、以下のようなタスクが必要となります。
関係部署と合意を取りながら進めましょう。

要件定義 ・5W2H の整理	「When（いつ)」「Where（どこで)」「Who（だれが)」「What（なにに)」「Why（なぜ)」「How（どのように)」「How Much（いくらで)」 e シールを付与するのか等整理します。 例）営業時間内に、自分のパソコン上で、営業員が、自社発行の請求書に、自社証明となる角印の代わりに、決裁システムを使って、一定の費用で e シールを付与できるようにする（出張先での利用も可とする)。e シール付与済の請求書は、取引先へメールで送付する。
・導入前フロー	現在の業務フローを洗い出します。
・導入後フロー	導入後の業務フローを検討します。
・セキュリティ	まず、通常のプロジェクトと同様に一般的なセキュリティを考慮します。 さらに付与権限者以外が勝手に e シールを付与したり、e シールを悪用されることのないよう厳重にリスク対策をしておきましょう。e シール固有のリスク[13]は第９章で詳しく説明しています。
製品・サービス選定	用途に合った製品やサービスを選定します。 どのような保証レベル[14]が望ましいか考慮しましょう。 e シール関連サービス提供者へ導入目的を説明し、目的に合致しているものを提案してもらうとよいでしょう。
導入	実際に製品・サービスを導入するフェーズです。 システムに組み込む場合は、設計や開発、テスト等も必要となるかもしれません。 厳格な動作検証を実施する場合は、テスト用電子証明書を使用した運用試験を行うこととなります。テスト用電子証明書は明らかにテスト用であることがわかるようにすることと、本番システム稼働時に本番用電子証明書への切り替えを忘れずに行いましょう。

[13] 「第９章 各フェーズにおけるリスクと注意すべき点」はチェックリストとしても有用です。必ず確認をお願いします。

[14] 保証レベルは「第５章 e シールの保証レベル」を参考にしてご検討ください。

ルール作り	ｅシールを利用する上での規約等を整備します。 ｅシールの契約や管理を行う主管部門、運用監視を行う情報システム部、実際にｅシールを利用する営業部門の役割と責任をまとめた社内規程[15]の作成等を実施します。
運用時の体制など	運用開始後の役割を明確にしましょう。 問い合わせ対応などの通常の役割の他に、ｅシールの更新、失効や廃棄等[16]を忘れないように責任者や担当者を決め、実施事項を整理しておきましょう。

STEP3 利用者・取引先への説明

せっかく策定したルールも利用者に理解され、遵守されなくては意味がありません。

ユーザ ID の管理がずさんで付与権限者以外がｅシールを付与できるような状況になったら、ｅシールの信頼性を損なうことにもつながります。

利用者への意識づけ	ｅシールは自社が発行したことを証明する重要な印です。 ｅシールを悪用されないよう利用者（付与権限者）への意識づけを行いましょう。説明会やマニュアル等も有効です。
取引先への説明	社内の利用者と同様に、取引先にも説明を実施しましょう。 特にｅシールが付与された書類を受け取った際には、ｅシールが正しいものかを確認する為、必ず「検証[17]」を行うよう依頼してください。 繰り返し確認できるように、説明資料を用意するとよいでしょう。

STEP4 運用開始

関係者の周知が終わったら、いよいよ運用開始です。

運用後もルールが徹底されるように気をつけてください。

また、運用実体や状況に応じて、改善する仕組みも検討することを推奨します。

---

[15] 社内規程のサンプルは「付録１：組織の内規テンプレート」にあります。

[16] ｅシールの更新や廃棄については「第８章　ｅシール用電子証明書の更新・失効およびｅシール署名鍵の廃棄」をご確認ください。

[17] 検証については「第 11 章　ｅシールの検証」に説明があります。

7-2 eシールの運用

業務部門と情報システム部門のいずれかが主管部門として、eシールの運用管理を行うと良いでしょう。運用開始後も、利用目的に合致した利用／運用ができているか定期的に確認が必要となります。

運用フェーズで必要な作業は以下です。

各作業の担当部門や作業フロー、ルールを決定してください。

通常運用	・ ログ監視 ・ 社内外からの問い合わせ対応 ・ eシールが付与されたドキュメントの管理 ・ 入社や異動、退職に伴うeシール利用権限の付与・剥奪 ・ eシール署名鍵の管理[18](※1) ・ 取引先への対応など
定期対応	・ 契約の見直し ・ eシール用電子証明書の更新[19] ・ 運用状況と課題の確認(※2)
異常時対応	・ トラブル時の原因調査、対応 ・ eシール署名鍵の危殆化時の対応 - 電子証明書の失効手続き[20] - 署名鍵の廃棄[21] ・トラブルの顧客通知
その他	・ 規程の施行、改訂 ・ 利用マニュアル、顧客向け説明資料の改訂 ・ eシール生成サーバーの起動(※3)

※1. 利用するeシールサービスによっては自社での管理が不要になる場合があります。

※2. 例えば以下を確認すると良いでしょう。

・ 発行事業者証明が必要なドキュメントにeシールを確実に付与出来ていること

・ 必要以上にeシールを付与していないこと

※3. 組織内にeシール生成サーバーを設置している場合に必要な作業になります。

常時稼働または自動起動にすることを推奨します。

---

[18] eシールを生成する為の署名鍵の管理は厳重に行う必要があります。「9-1 eシール署名鍵生成フェーズ」では鍵の生成から廃棄までのフローが記載されていますが、通常運用では特に「b.保管」や「c.生成」のポイントを注意しましょう。

[19] eシール用電子証明書の更新は「8-1 更新」に説明があります。

[20] eシール用電子証明書の失効手続きは「8-2 失効」に説明があります。

[21] eシール署名鍵の廃棄は「8-3 署名鍵の廃棄」に説明があります。

7-3　e シール導入例

e シールの導入例として、E 社のストーリーを紹介します。

お客様から「御社を名乗る怪しげな請求メールを受け取った。」との問い合わせがあり調査をしたところ、巧妙ななりすましであることが確認された。
E 社はお客様の安心のために、発行事業者証明である e シールの付与を決定した。
総務部の A 氏は情報システム部の B 氏とともに請求書に e シールを付与するプロジェクトを任された。

A 氏：今回のプロジェクトの目的ですが、「お客様に信頼できる請求書を送る」ことになります。

B 氏：分かりました。では、請求書以外は e シール付与の対象から一旦外しましょう。顧客に請求書を送るのは営業部のみですので、e シールの利用部門は営業部になりますよね。

A 氏：はい。利用部門は営業部のみになります。情報システム部には導入後の運用監視をお願いしたいのですが。

B 氏：分かりました。体制含め、プロジェクトの概要を一度整理しましょう。

[プロジェクト概要]

目的		お客様に信頼できる請求書を送る
スコープ		営業員が発行する請求書
予算		1,000 万円
期間		6 か月
体制	主管部門	総務部
	運用部門	情報システム部
	利用部門	営業部（営業員）

〇プロジェクトのポイント
・導入目的を明確にすることでスコープの拡大を避けましょう。
・スモールスタートが望ましいです。

A 氏：問題ないと思います。次に、現状の業務フローを確認するべきですね。請求書を発行する際のフローを営業部長の C さんに確認してみます。

〇プロジェクトのポイント

ｅシール導入後の業務フローを決定する前に、まずは現状の業務フローを確認してください。

営業部長に問い合わせたところ、受発注管理システムで発行した請求書を営業員がメールで送付しているケースが大半であることが分かった。
ｅシール導入に対する営業部長の反応としては、信頼できる請求書を発行できるのは良いことだが、営業員の手間が増えるようなことはなるべく避けたいという要望があった。

A 氏：自社作成の受発注管理システムで発行した請求書を営業員がメールで送付しているケースが大半だそうです。受発注システムを改良すれば、業務フローを変えずにｅシールを導入することが可能ですか。

B 氏：はい。受発注管理システムにｅシールの付与サービスを組込み、営業員が請求書をダウンロードするタイミングで、ｅシールの付与された請求書がダウンロードされるようにしましょう。

A 氏：良いですね。ありがとうございます。
ところで、ｅシール導入にあたってセキュリティに関する対策も必要ですよね。わたしは技術的なことはさっぱりですので、B さんのセキュリティに関する知識を活かして対策を考えていただけますか。

B 氏：分かりました。セキュリティに関する事項も含め、一度要件を整理してみます。
[要件定義]

導入後の業務フロー	現状と同様
ｅシール付与タイミング	営業員が請求書をダウンロードするタイミング
ｅシール付与者条件	ｅシール付与権限を持つ利用者であること
ｅシールの方式	リモートｅシールサービス
利用単位	会社単位 (会社の角印相当として利用するため。)
保証レベル	レベル２
セキュリティ対策	・ ｅシール付与権限を持たない者が勝手に付与できないよう、受発注システムに利用者権限を設定する。 ・ 問題発生時の対応として、ｅシール用電子証明書の失効と、署名鍵の廃棄が確実にできる仕組みを作る。

A 氏：整理してくださり、ありがとうございます。リモート e シールサービスを利用する理由を教えていただけますか。

B 氏：今回はプロジェクトの期間が短いので、受発注管理システムの中から API 呼出しが可能なリモートサービスを利用するべきと判断しました。これによって社内でのシステム変更は最小限で済みます。

A 氏：なるほど。リモート e シールサービスを利用すれば署名鍵の管理もこちらでしなくて済みますし、総務部としても助かります。
セキュリティ対策としては、e シール付与 API を呼び出すことができる利用者を受発注システム内で制限するということですね。

B 氏：その通りです。

A 氏：ありがとうございます。では、これらの要件を満たす e シールサービスを探しましょう。また今回の利用目的を考えると保証レベル 2 の e シールが合っていそうですね。

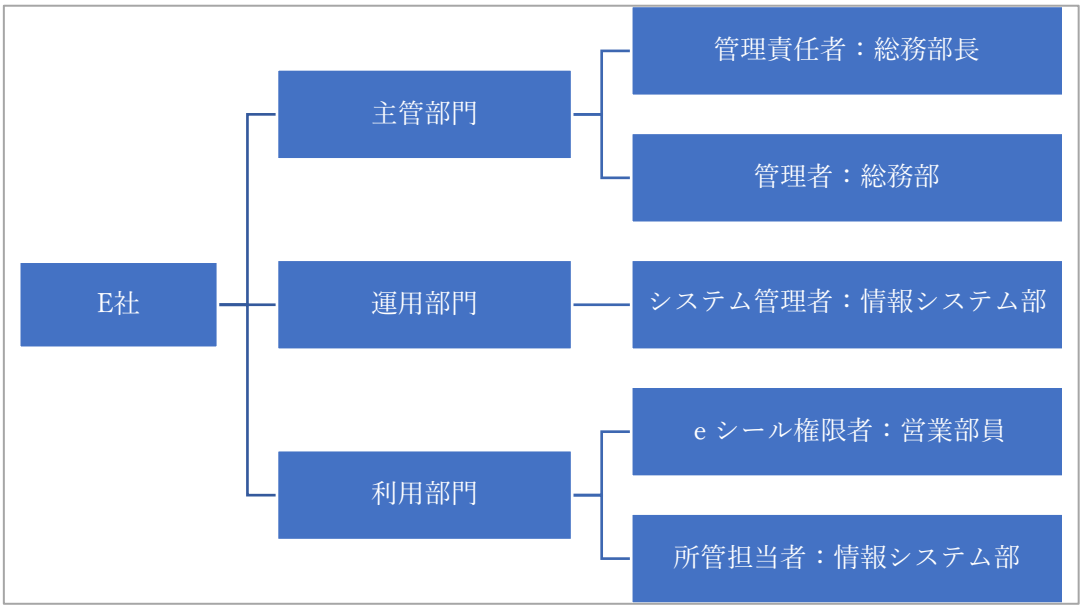
〇プロジェクトのポイント

- 今回の例では、リモート e シールサービスを利用しましたが、自社の目的に合った方式を選択してください。また、方式によって注意すべき点が異なります。第 9 章「各フェーズとリスク＆注意すべき点」を参考に注意点を洗い出してください。
- e シールの付与方法、付与タイミング、付与条件は、以下を考慮して決定してください。(詳細は「9-3. e シール生成フェーズ」を参考してください。)
  - e シールを悪用されないためのセキュリティ
  - 大量発行・自動発行のリスク

調査の結果、自社作成の受発注管理システムの中から API 呼出しが可能な X サービスと Y サービスが自社に合っていると考えた。社内でいくつかの判断基準を上げてこれらのサービスを比較し、X サービスと契約を行った。
当社の e シール用の電子証明書は、X サービスの預かりサービスを利用している。
情報システム部が受発注管理システム（開発機）に X サービスを組込み、テストを実施した所、問題なく発行されることが確認できた。

B 氏：無事テストが完了し、問題なく利用できることが確認できました。
A 氏：ありがとうございます。情報システム部が作業をしてくださっている間、私のほうで社内規程の草案を策定してみました。ｅシールに関わる各部門の役割と責任を定義しています。
※本資料の付録１にサンプルの社内規程を用意しましたので参考にご利用ください。

[社内規程]
○体制



○主管部門の役割

管理責任者	・ ｅシール利用に関する責任を負う。 ・ 適正な規程、体制、運用等の監督責任を負う。
管理者	・ ｅシールを利用するための仕組み(システム、規程など)を提供する。 ・ 利用者からの問い合わせやトラブル時の対応・周知を行う。 ・ ｅシール利用権限の付与・剥奪を行う。 ・ ｅシール関連事業者との契約更新を行う。 ・ ｅシール危殆化時の対応を行う。(事業者によるサポートを受ける)

○運用部門の役割

システム管理者	・ e シールを付与するシステムの運用監視を行う。 ・ トラブル時の調査・対応を行う。

○利用部門の役割

e シール権限者	e シールを付与する権利を持つ。今回の例では営業員。
所管担当者	e シールが付与されたドキュメントを適切に管理する。 今回の例では、ドキュメントは受発注システム内に保持される為、営業部ではなく受発注システムの主管部門である情報システム部が該当する。

B 氏：環境の準備やルール作りが完了し、いよいよ利用開始ですね。

A 氏：そうですね。利用開始にあたって、利用者と取引先に注意事項などを説明する必要があります。受発注システムのマニュアルの整備と、営業員への説明会をセッティングしましょう。

A 氏は受発注システムのマニュアルに e シール利用に関する注意事項を追記した。
また、説明会を実施し営業員への周知を図った。合わせて、顧客向けの説明資料を営業員へ配布し、今後は当社の e シールのない請求書についての注意喚起を促してもらうこととした。

e シール利用の周知が完了し、A 氏と B 氏はプロジェクト完了報告書を提出した。その後、 e シールの本格的な利用を開始した。

○プロジェクトのポイント

- 今回の例では、リモート e シールサービスを選択しましたが、選択した方式によって注意点が異なる為、第 9 章「各フェーズとリスク＆注意すべき点」を参考に注意点を洗い出してください。
- 正式に利用を開始する前に、一部の部門で試験的に利用して、利用規約やフロー等をまとめるのも有効です。

８．ｅシール用電子証明書の更新・失効およびｅシール署名鍵の廃棄

８-１　更新

ｅシール用電子証明書は、発行時に有効期間が設定されています。有効期限切れの後には、ｅシール用電子証明書は無効となります。このためｅシール用電子証明書を継続利用するためには、有効期限前に予め更新を行ってください。

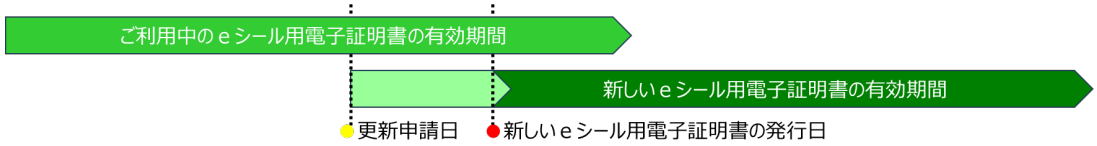


図 8-1　ｅシール用電子証明書の更新

通常、ｅシール用電子証明書を発行した事業者、もしくは提供サービスを通じて更新に関する案内が送付されます。案内に従い手続を行うことで更新を行ってください。

８-２　失効

ｅシール用電子証明書は、有効期限まで利用できますが、以下に挙げられる事象に該当する場合は利用者による失効手続きが必要です。

1. ｅシール用電子証明書の記載内容に変更が生じた場合
   (ア)商号や住所など（記載内容はｅシール用電子証明書を確認することで確認できます）
   (イ)法人番号など（法人などの合併・被合併などにより、当該番号が変わる場合）
2. ｅシール用電子証明書を今後利用しない場合
3. ｅシール用電子証明書の利用に必要な暗証番号などが盗難・破損により危殆化[22]した場合
4. ｅシール用電子証明書の利用に必要な暗証番号などが不明となり、再度手続が必要な場合
   (注)サービスによっては、暗証番号の変更手続が具備されている場合もあるので、提供事業者に確認してください。

失効に必要な手続はサービス毎に案内されているので、手続に従って申請を行います。
失効手続が完了すると、失効が完了した旨の通知が発送されますので、確認が可能です。

---

[22] 危殆化：電子証明書の有効性が攻撃の危険にさらされる事態となること。

また、失効は通常、利用者による申請に基づきますが、以下の事由で認証局による失効があります。

1. 認証局にてｅシール署名鍵の漏洩が発生、もしくは漏洩の疑いが生じた場合
2. 認証局にて使用している暗号の危殆化が発生、もしくは危殆化の疑いが生じた場合
3. 利用規約等で記載した義務を利用者が履行しない場合（例. 料金支払、受領書データ送信、などの未実施）
4. 利用規約等で記載した解除権に利用者が該当する場合（例. 清算、廃業など）

８-３　署名鍵の廃棄

失効の申請と共に、ｅシール署名鍵が安全に廃棄される必要があります。

署名鍵の廃棄は、ｅシール署名鍵の格納形態で対処が異なりますのでご注意ください。

1. 組織内管理で媒体に格納している場合

   廃棄後にｅシール署名鍵が不正利用されないよう、適切な廃棄処理を行う必要があります。廃棄処理は、物理的な破壊や論理的な完全消去が挙げられます。IC カードや USB トークンのような媒体に格納されている場合、破砕し処分することが可能ですが、HSM などの鍵管理装置の場合は、実装されている鍵消去機能を利用することで、署名鍵データの完全消去が確実に実施できます。
2. リモートｅシールサービスで管理されている場合

   リモートｅシールサービスを提供している事業者へ廃棄の申請を行います。上記失効を申請すると、併せてリモートｅシールサービス内で管理されている自社のｅシール署名鍵廃棄も同時に実施される場合もありますので、ご利用のサービス内容を確認することが推奨されます。

９. 各フェーズにおけるリスクと注意すべき点

本章では、「ｅシール解説～実用化に向けて～」[23] 7.3 にて記載のｅシール生成における各フェーズにおいて、リスクと利用者として注意すべき点を整理します。

９-１　ｅシール署名鍵生成フェーズ

ｅシールでは公開鍵暗号と呼ばれる暗号方式が利用されます。この技術はブラウザにおいて Web サーバーとのやり取りを行う際にもデータの暗号化やサーバーを認証するために用いられる一般的な技術的であり身近に利用されています。公開鍵暗号では 2 種類の鍵を利用し、検証に用いるために公開情報である公開鍵と、その対となる秘密鍵が存在します。秘密鍵は一般に公開してはならず、秘密裏に管理されていることが望まれます。過去には秘密鍵が漏洩したことで情報を搾取されたり、第三者によるなりすましが起きたりするなど金銭的な被害に及ぶ事件・事故が起きています。

ｅシールは公開鍵暗号の秘密鍵を利用者が安全に保管し第三者が利用できないようにすることによりｅシールの確からしさや信頼性を担保することができます。そのため利用者がｅシールを作成したことを保証するためにも秘密鍵を安全に管理する必要があります。

図 9-1-1 は代表的な鍵生成から破棄までのフローを示しています。図において青パートはｅシール生成時に利用するｅシール署名鍵（秘密鍵）のライフサイクル、黄色パートは電子証明書やｅシールのライフサイクルについて示しています。本節では青パートの４つのフェーズについて説明します.

[23] 「ｅシール解説～実用化に向けて～」：https://jdtf.or.jp/report/whitepaper/file/e シール解説%28 バージョン 1.0%29.pdf

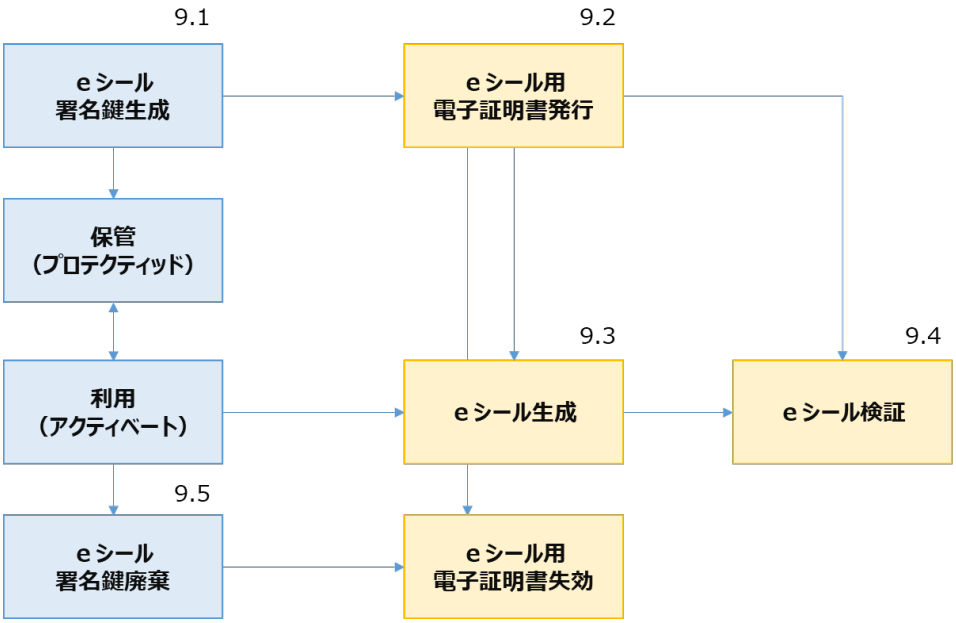


図 9-1-1　鍵生成から廃棄までのフロー

[青パート：署名鍵のライフサイクル]

a. 鍵生成

e シール署名鍵の生成を行います。

b. 保管（プロテクティッド）

e シール署名鍵が保護された状態です。

c. 利用（アクティベート）

保管から利用可能に移行した状態です。

d. 鍵廃棄

e シール署名鍵の利用を終えた状態です。

それぞれのフェーズにおけるリスクや考慮すべき点について以下列挙します。

・適切な暗号アルゴリズムと鍵長の設定[全体]：

e シールに利用される署名アルゴリズムや鍵長の選択を適切に行うことが必要です。CRYPTREC 暗号リスト [24]を活用して、広く利用され、かつ官民ともに利用実績の高いアル

[24] **CRYPTREC 暗号リスト**

デジタル庁、総務省および経済産業省で推進している、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト CRYPTREC（Cryptography Research and Evaluation Committees）で評価策定された暗号リストです。これまでに 2 回の改訂が行われています。これは経年変化により当時安全に

ゴリズムを選定する参考とすることができます。
本書では推奨アルゴリズムを提示しませんが、今後各種ガイドライン等が発行される可能性がありますので、その際には準拠されることを推奨します。

・鍵生成時の暗号学的リスク[a. 鍵生成]：
鍵の生成には乱数生成アルゴリズムが利用されています。ランダムに生成されていないと鍵に偏りが生じてしまい攻撃者により署名鍵を特定されてしまうリスクがあります。過去にも各種 OS やライブラリにおいて極端に小さい鍵空間（鍵の取りうる範囲）から鍵が選択されていたことにより暗号資産が流出するなどの事件もありました。

・鍵の共有とバックアップ[b. 保管]：
バックアップ目的であっても鍵を生データの状態で不用意にコピー・共有することは望ましくありません。このようなケースにおいては秘密分散などの技術を用いることで、適切な権限を設計し、必要な場合に署名鍵が利用できるための手順を確立しておくことが望まれます。
ハードウエア製品を用いることもできます。この場合、ハードウエアで生成された鍵を外部に抽出できない場合には、媒体の紛失や機器の故障に注意する必要があります。さらにコストに見合う製品であるかどうかも大切な選定技術ではありますが、FIPS140-3[25] などの第三者認証を取得しているかどうかなど十分に安全な機能を有する製品であるかどうかもポイントとなります。

・鍵の保管[c. 利用]：
鍵をそのままの状態で保管することは避けなければなりません。OS やシステムの問題だけでなく認証を回避するなどの外部からの攻撃によりデータの流出が起こりえます。USB ストレージなどの可搬性の高いデバイスに格納するケースにおいてはさらに強固な対策が

利用できていたにも関わらず暗号アルゴリズム自体が危殆化（安全に使えなくなる状態）する状況を鑑み、定期的に見直しを行った結果です。
https://www.cryptrec.go.jp/list.html

[25] FIPS140-3
米国国立標準技術研究所（NIST）が策定している、暗号モジュールのセキュリティ要件に関する米国連邦標準規格です。認証を受けた製品群のリストがありますので、これらの情報から利用を検討することができます。
https://csrc.nist.gov/projects/cryptographic-module-validation-program/fips-140-3-standards

必要とされています。そのためパスワードプロテクト（PKCS#5[26]などの利用）や鍵ファイルの暗号化などの施策が推奨されます。

・漏洩時の速やかな復旧[d. 鍵廃棄]：

漏洩・紛失が疑われる場合には速やかな復旧が望まれます。事前にどのような手順で鍵を無効化し，新しいｅシール署名鍵を生成するか事前に決めておくことが望まれます。

特に既存の署名データを延命させるための長期署名などの技術を利用するのか、ｅシール用電子証明書の失効や再発行の方針・設計についても留意する必要があります。

漏洩・紛失が疑われる場合の措置については、第 7 章、長期にわたって検証可能する手段については、第 10 章に記載します。

・監査と記録[全体]：

ｅシール署名鍵生成だけでなく各フェーズにおいては、適切な監査手順と各種操作の記録を取ることが望まれます。特に複数の鍵を生成した場合などは記録ログが混ざらないように仕組みづくりをしておく必要があります。また、ヒューマンミスを防ぐことを目的に、ログ記録を自動化するなどの施策も考えられます。

[26] PKCS#5

PKCS（Public Key Cryptography Standards）とは、公開鍵暗号に関連するプロトコル（通信規約）やデータ形式など各種の技術仕様を定めた規格群です。以下の RFC でパスワードから暗号化鍵を生成する実装に関する推奨事項が示されています。

RFC8018: PKCS #5: Password-Based Cryptography Specification Version 2.1

https://datatracker.ietf.org/doc/html/rfc8018

9-2　e シール用電子証明書発行フェーズ

e シール用電子証明書を発行するにあたり、e シール用電子証明書の保証レベルによって認証局での審査方法が異なります。レベル 3 が最も審査が厳格で、最も信頼性の高い e シール用電子証明書になります。実運用で最も利用が想定されるものとしてはレベル 2 が想定されます。

e シール用電子証明書の用途は発行元証明であるため、利用申込時に認証局が審査として、実在性及び申請意思の確認が行われることとなります。

確かに組織が存在していること（実在性）は、以下の 3 つの観点によって確認されます。

①　法的な存在：公的機関に登録されていること

②　物理的な存在：申請された住所が実在すること

③　運営的な存在：事業活動が行われていること

そして、なりすましではなく、確かにその組織の意思による申請であることの確認も行われます。

組織内における、事業所・営業所・支店・部門等の単位での発行は、組織等の代表者の宣言の結果が尊重され、発行対象である組織等が一義的な責任を負うことを前提として、認証局は利用申込の宣言に基づいて、e シール用電子証明書の中に、その内容を記載することとなります。

以下に、利用申込時、提出が必要な書類や手続きの例を記載していますが、実際の手続きは、認証局ごとに定められており、以下の例とは異なる可能性があります。

レベル 2（第三者による実在確認がされ、発出元の信頼性を一定程度保証できるレベル）
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、第三者機関が管理するデータベースで確認できる組織が対象となります。
利用申込方法の例として、以下の方法が考えられます。

＜A＞　商業登記電子証明書による電子署名が行われた利用申込。

＜B＞　代表者印が押印された利用申込書および印鑑証明書（法務局で発行）の提出。

＜C＞　代表者のマイナンバーカードの署名用電子証明書又は認定認証業務に係る電子証明書等による電子署名が行われた利用申込。

レベル 3（国際相互認証を想定した厳格なレベル）
法人番号を確認できる組織が対象となります。
紙での利用申込方法の例として、以下の＜A＞＜B＞＜C＞を全て実施する方法が考えられます。

＜A＞　代表者印が押印された利用申込書および印鑑証明書（法務局で発行）の提出。

＜B＞　2 点必要とし、最低でも A グループから 1 つが必要。写しの全てにおいて代表者等の本人氏名が確認できること。

【A グループ】

クレジットカードの明細書、デビットカードの明細書、住宅ローンの明細書、規制金融機関発行の銀行の明細書

【B グループ】（6 ヶ月以内に発行されたもの）

公共料金請求書、リース料支払の明細書、出生証明書(日本国内の場合は戸籍謄本もしくは戸籍抄本)、直近の課税年度の地方自治体税請求書

＜C＞　代表者等の写真付き身分証明書を持参のうえ、対面またはビデオによる対面審査

写真付き身分証明書の例：パスポート、運転免許証、マイナンバーカード

9-3　e シール生成フェーズ

e シールの生成では、対象の電子文書に対して e シールの付与を行います。e シールは、対象文書のハッシュ値[27]に対して、e シール署名鍵でデジタル署名することで生成されます。この e シールの生成概念を理解したうえで、適切に e シールの生成を行う必要があります。

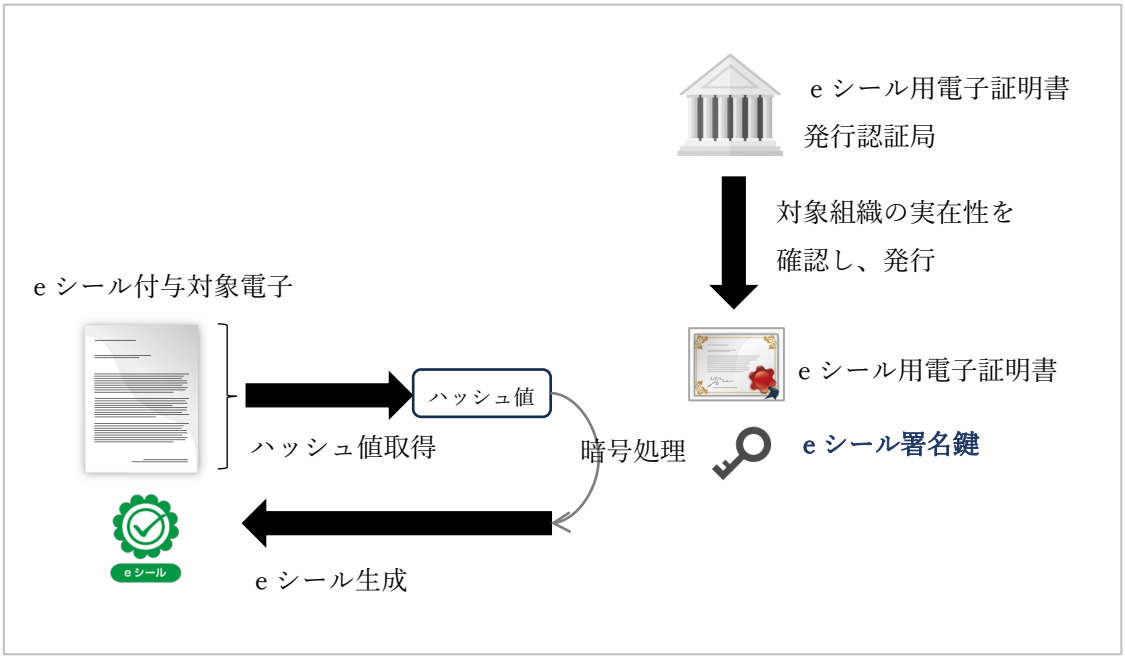


図 9-3-1　e シール生成の流れ

図 9-3-1 のように e シール付与電子文書には、e シール署名鍵によるマーキングであるデジタル署名と署名鍵のペアである公開鍵を含む電子文書の発行元組織を証明する e シール用電子証明書が[28]付与され、e シール付与電子文書が外部に提供されるため、以下の留意事項を考慮し e シールの生成を行う必要があります。

【e シール生成時の留意事項】

① 組織として責任のある情報の外部への発出であり、情報は単独で転々流通する事を理解してください。

② e シール付与電子文書は生成時のみだけでなく、将来にわたって利用される

[27] ハッシュ値：対象電子文書から特定のアルゴリズムで生成される短い固定長の文字列です。

[28] e シール用電子証明書に記載される事項については、「e シール解説～実用化に向けて～」を参照ください。

可能性があります。（e シール自体は、e シール用電子証明書の有効期間内のみ検証可能となります。e シール用電子証明書は、一般的には 1 年から 3 年の有効期間となります。有効期限寸前の e シール付与の場合、直後に検証ができなくなります。

③ 改ざん、なりすましによって誤情報となる e シール付与電子文書を公開した場合には信用失墜のリスクが存在します。

e シールの生成時には、e シール用電子証明書の管理している組織単位によって許可された特定の複数人のみ e シールの生成が可能な権限設定を適切に実施する必要があります。そのため、会社角印を付与する際の印章規程と同様に、e シール生成の運用に関する組織内でのルール設定が必要になります [29]。また利用権限を持つ人間の異動や退職など権限変更の必要がある際には、速やかに対応する必要があります。e シールは、組織として責任のある情報の外部への発出であり、情報は転々流通するものであるため、権限のない人間が不正に e シールを付与した場合には、信用失墜などのリスクが発生します。

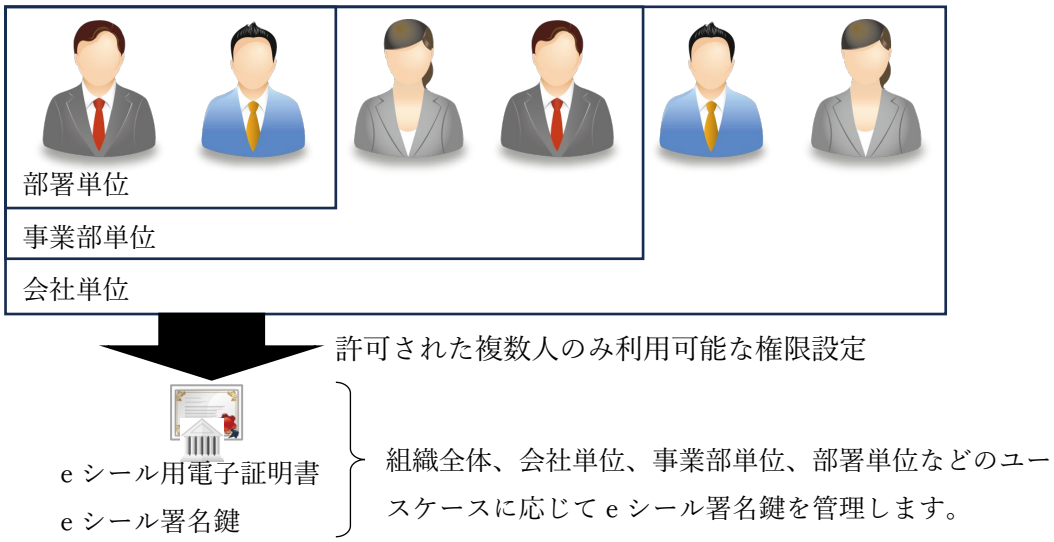


図 9-3-2　e シールの生成時権限設定

また、e シールでは大量の電子文書に対して、自動で e シールの生成を行うケースがあります。この大量発行・自動発行において、不正な電子文書に対して e シールを付与してしまった場合には、その特性上瞬時に誤った情報が広報され、その情報の訂正は相当困難になると考えられます。そのため、大量発行・自動発行においても、以下のようにリスクを回避する運用を検討することを推奨します。

・e シールを付与する電子文書について、事前に該当文書の正当性を確認する。システムに

[29] 本書の付録 1 に、組織の内規テンプレートのサンプルを用意しました。

よって自動で電子文書を生成する場合には、システム試験を正しく実施し不正な電子文書を生成しない事を担保する。

・処理実行前に正当な権限を持つ人間が処理開始の認証／認可を実施する。

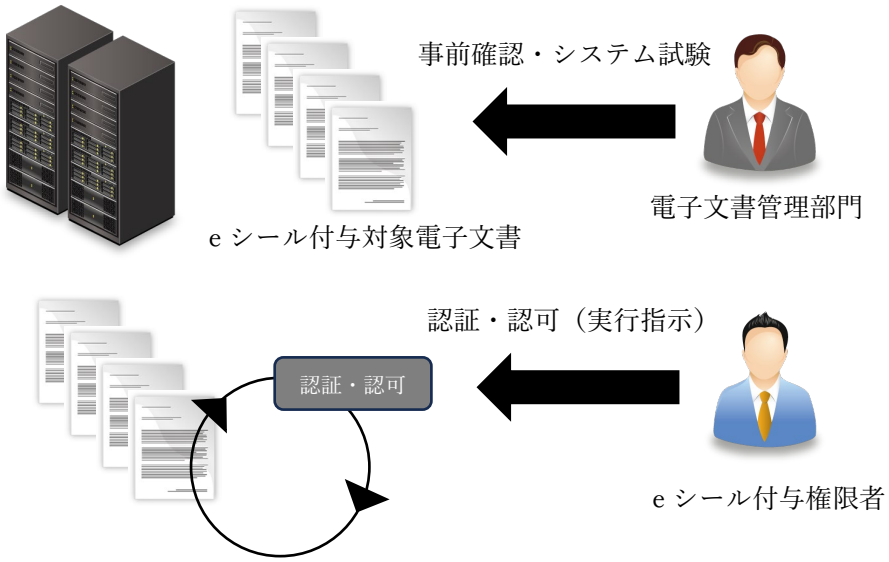


図 9-3-3 大量発行・自動発行時の対応

9-4　e シール検証フェーズ

本フェーズは、e シールを付与したデータを公開・配布したのちデータを受領した e シール検証者が真正性を検証するために、e シール利用者が運用上考慮すべき事項を示します。また本フェーズの記載事項は e シール利用者に焦点を当て、e シール検証者に関する記載事項は第 11 章に記載します。

以下、本フェーズの基本概念を示します。

図 9-4-1　e シール　検証概念図

eシールは付与するだけでなく、署名検証によってその価値が生じます。署名検証を通じてeシール利用者および検証者は、公開されたデータにおけるなりすまし等のデータ流通時のリスクを回避することが可能となり、より安全なデータ流通が可能になります。

以下は、eシールの検証により回避可能なリスクの代表例です。
・対象データの改ざんによる誤情報の利用
・データ発出元のなりすましによる誤情報の利用
・上記による誤情報を利用した情報発信による信用失墜

【eシール検証時の留意事項】
① eシール検証者がeシールの信頼性を確認できること
② eシール用電子証明書に組織を特定する情報が記載されていること
③ eシール検証者は不特定多数となりうること
④ eシールの検証は、いつ実施されるか特定できないこと

① eシール利用者は、eシールを発行する認証局およびその事業者から、以下の情報が公開されていることを確認してください。
- 認証局証明書ポリシー（CP）/認証局運用規程（CPS）
- 失効情報（OCSP/CRL）
- 認証局電子証明書 ※パブリック認証局の場合、信頼済みストアへ登録されていること

上記は、eシール検証者が確認可能な場所で公開されている必要があります。

② 署名検証と合わせてeシール用電子証明書の情報[30]をもとにベースレジストリより企業情報を参照すること可能ですが、あらかじめベースレジストリの記載情報と紐付く情報（組織識別子等）がeシール用電子証明書に記載されていることを確認してください。

[30] 総務省のeシールに係る検討会では、最終とりまとめで「認定に係るeシール用電子証明書には、公的機関が発行する番号体系を用いた組織識別子を少なくとも1つ記載することを要件とする」と整理されています。

③　e シール検証フェーズでは、一般的に「誰が」「いつ」「どのように」署名検証するかを想定して、運用を決定する必要があります。以下に e シールを付与したデータが検証されるパターンの例を示します。

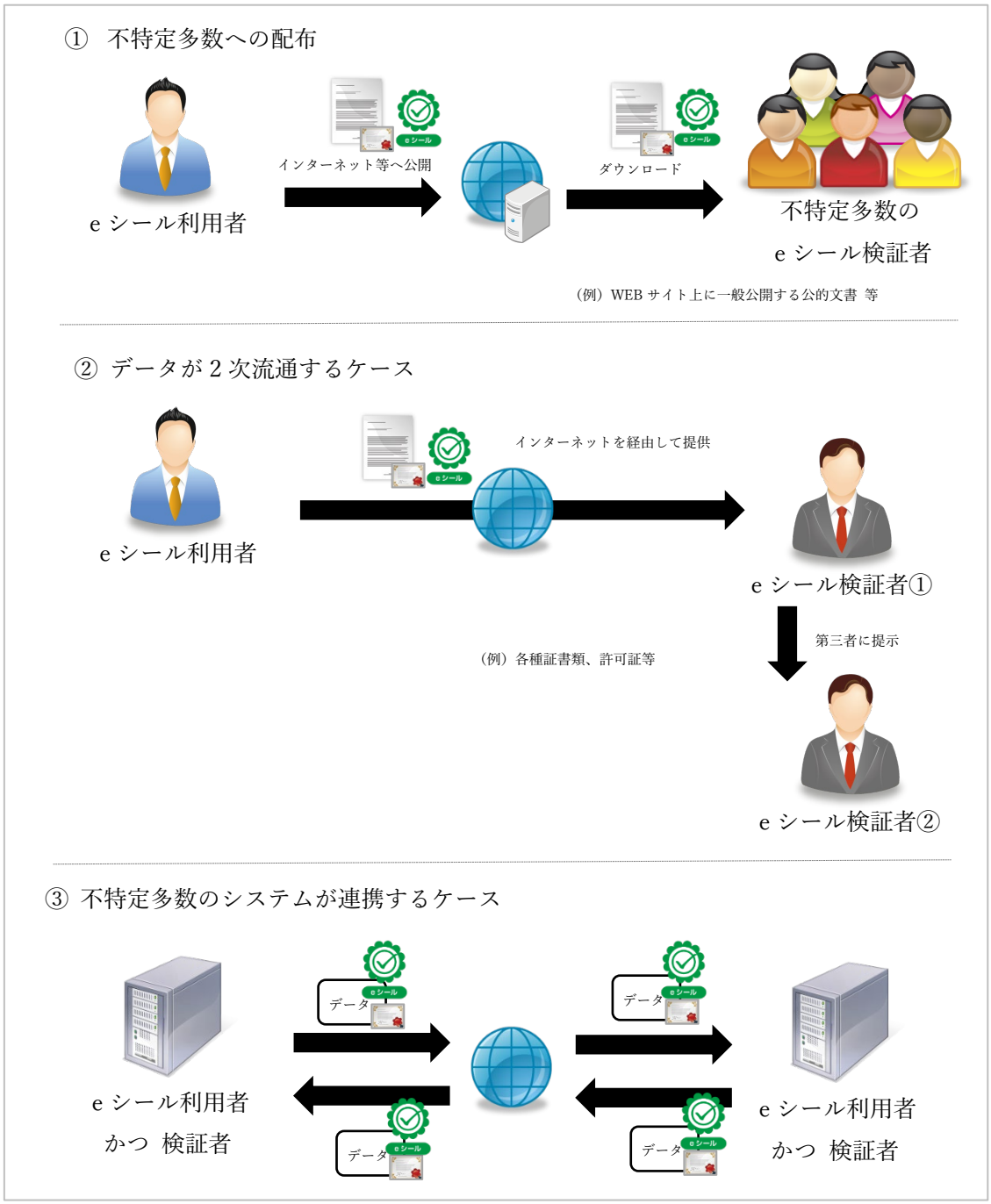


図 9-4-2　e シール検証者の想定されるケース

データ流通の範囲は、ユースケースによって異なりますが不特定多数に配布されるケースやより厳密な発出元の証明が必要なケースが存在することに注意が必要です。

いずれのケースにおいても、e シール利用者は容易に検証可能な署名形式を採用する必要があります。

不特定多数の e シール検証者により検証される場合には、e シール検証者が検証機能を有したソフトウェア、デバイス、システム、第三者機関による検証サービス等を容易に取得でき、利用可能である必要があります。検証に利用されるツールは、一般的なツール（例：PDF ファイルであれば Adobe 社の Acrobat Reader 等）を利用するケースと専用ツール（例：システム間連携等における署名ライブラリやアプリ等）を配布する方法が想定されます。

④ 署名検証はデータが流通する期間において発生し、いつ検証するかを制御することは困難です。したがって、e シール利用者は対象のデータが流通もしくは保管される最大期間にわたって検証が可能となるように署名形式（長期署名形式等）を検討してください。e シール用電子証明書の有効期間を超えて検証が求められる場合は、長期署名が有効です。長期署名については、第 10 章をご覧ください。

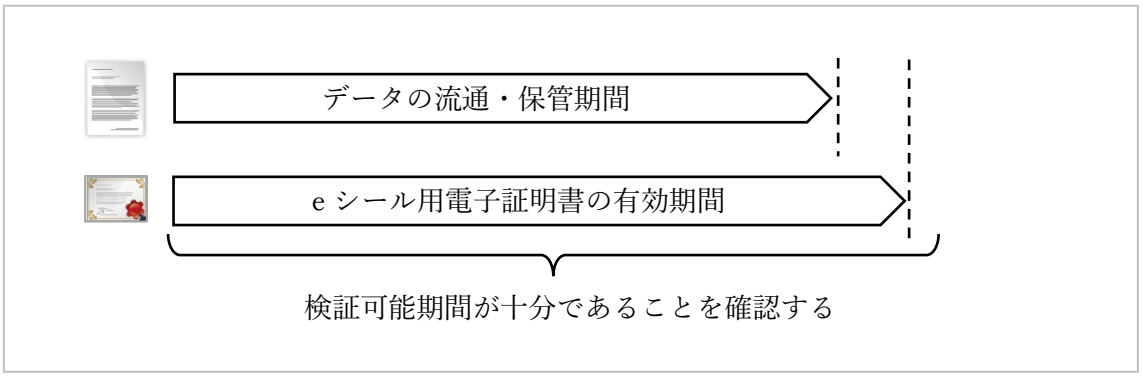


図 9-4-3　e シールの検証可能期間

【e シールの検証によって提供される価値】

① 第三者機関による認証

e シールは、第三者機関である認証局によって認証を得た e シール用電子証明書を利用しています。これらの認証局は、認証局運用規程（CPS）やパブリックストアへの登録など運用状況を公開しており第三者の認証よって組織が存在することを証明します。また e シール用電子証明書が信頼されるものであることで、データの完全性と発出元が保証されます。e シールが不特定多数により検証される場合には、認証局はパブリック認証局（WebTrust[31]制度等により監査を受けている認証局や Adobe Approved Trust List[32]に登録されている認証局）を利用することが好ましく、信頼された証明書ストアによって検証が可能です。

---

[31] **WebTrust**

米国公認会計士協会（AICPA）とカナダ公認会計士協会（CPA Canada）によって共同開発された国際的な電子商取引認証局監査プログラムです。

認証局のための WebTrust 原則と規準にもとづいて、電子認証局（CA）の内部統制（①運営方式の開示、②サービスの完全性、③情報の保護等）のデザインの適切性、運用の有効性を評価し、監査法人等の第三者機関より監査レポートが提供され、WebTrust Seal プログラムを採用している認証局においては、監査レポートをインターネットから確認することができます。

[32] **AATL**：Adobe Approved Trust List

PDF 文書の安全性を確認するため、Adobe 社において、署名鍵の電子証明書を認証するプログラムです。

この基準を満たした電子証明書が、Acrobat® または Reader® に登録リストとして定期的にダウンロードされます。署名された PDF 文書は、その秘密鍵が、信頼された鍵であるかを常に確認することができます。

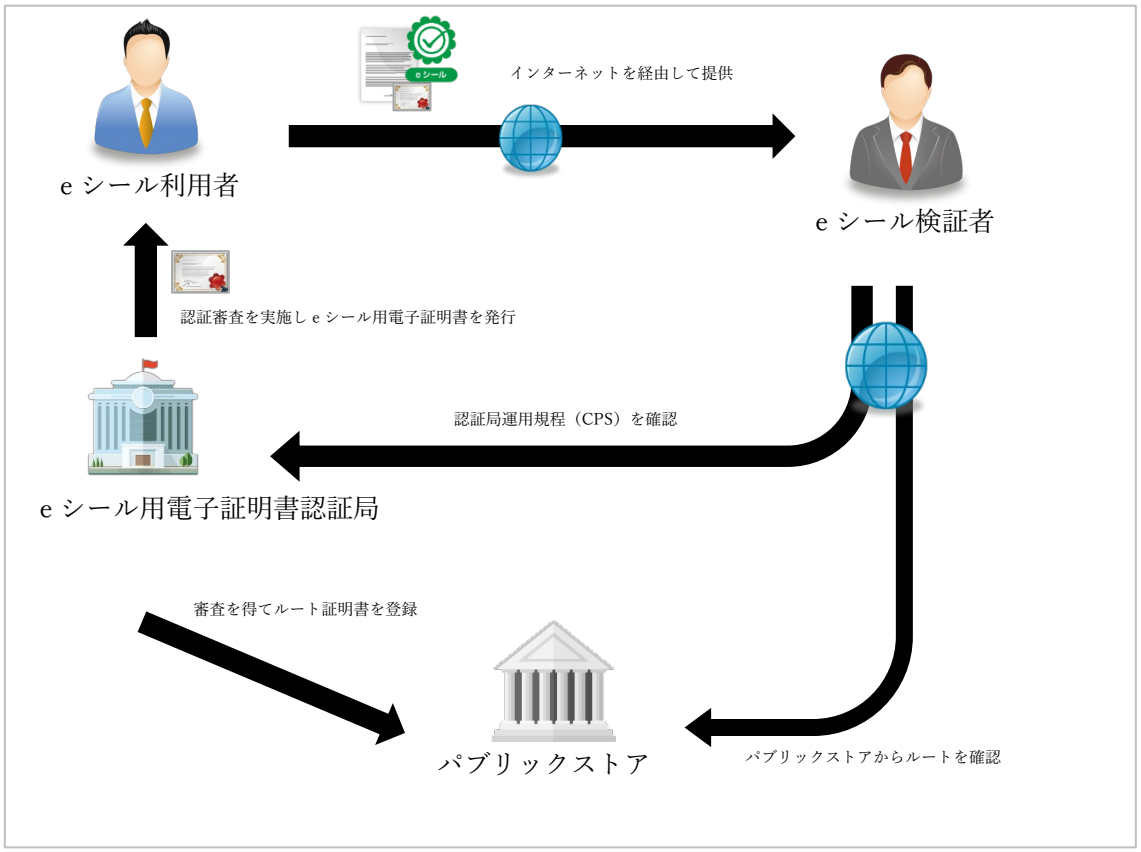


図 9-4-4 第三者機関による認証局とパブリックストアの関係

② ベースレジストリとの紐付け

e シール用電子証明書に記載されている事項は、認証機関によって審査された情報であり、そのため正確な情報が記載されます。企業識別番号などの一部の情報は、ベースレジストリなどに公開されている情報と関連しており、これらを紐づけることで、確実に対象の企業であるかを確認することが可能です。また、これらの情報をシステム的に処理することも可能です。

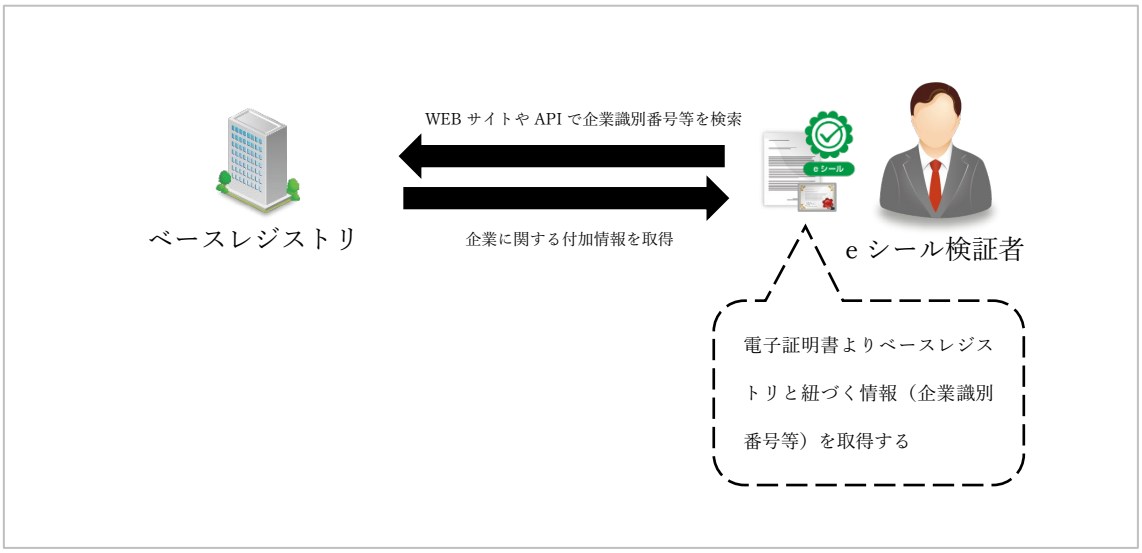


図 9-4-5　e シールとベースレジストリの連携

③ 必要情報を正確に簡便に保持できる

e シール用電子証明書に含まれる企業情報は、認証局を運営する第三者機関によって審査されて記載されています。組織名称や番号の真実性は認証局によって保証され、改ざん防止とともに担保されています。検証者は、該当の情報が自身の想定しうる企業であるかを確認するとともに、デジタルデータとして、必要な情報を簡便に保持できます。

④ 発出元側の否認防止

e シールの署名検証により、対象データ発出時点での発出元を証明可能となり、受領側もしくは、途中段階で、情報が書き換えられる余地があることを根拠に発出側に否認されることを回避できます。

9-5　eシール署名鍵廃棄フェーズ

組織においてeシール署名鍵が有効期限切れ以前に、eシール用電子証明書の記載内容の変更やeシール署名鍵の漏洩の疑いが生じた等の理由により、使用を終える場合には、eシール用電子証明書の失効手続きを行い、eシール署名鍵を廃棄する必要があります。

失効手続きを怠ると、誤った情報の拡散や第三者による不正利用のリスクがあります。eシール署名鍵を組織内で管理している場合、リモートeシールサービスを利用している場合、それぞれで失効および廃棄が適切に行われたことを確認する必要があります。いずれも不足の事態に備えて、予め手順化しておくことが重要です。また、失効時の手続きが明確になっていることもサービス事業者の選定ポイントとなります。

失効、廃棄に至る事由および手続きについては、第8章「eシール用電子証明書の更新・失効およびeシール署名鍵の廃棄」をご覧ください。

１０．ｅシールを長期にわたって検証可能とする手段「長期署名」

ｅシールが付与された文書は、ｅシールと電子証明書を検証することで、発出元の保証と、付与された時点からの改ざん検知が可能となります。

電子証明書は、署名鍵の管理がご利用いただく組織に委ねられていることや、署名に係る暗号処理の安全性がコンピュータの能力に依存することから、一般的に 1 年から 3 年程度の有効期間として認証局が発行します。

長期にわたる検証に関する留意事項１：電子証明書の有効期限 電子証明書の有効期間が３年であっても、電子証明書が発行された時点からの期間になるため、利用してから短期間で検証ができなくなることに注意が必要です。 ｅシール付与時点で、有効期間内であっても、翌日にはその有効期限を迎える可能性があり、有効期限を超えた証明書は効力が無くなり、検証ができなくなる恐れがあります。

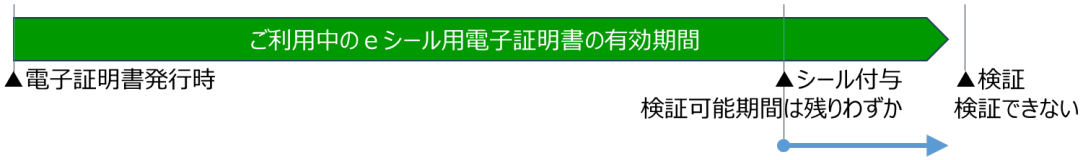


図 10-1　ｅシール用電子証明書の有効期間と検証の可否

ｅシールの検証可能期間は、電子証明書の有効期間になります。

この検証期間を延長する手段が、タイムスタンプを利用し、シール付与時点の有効性を保持する「長期署名」です。

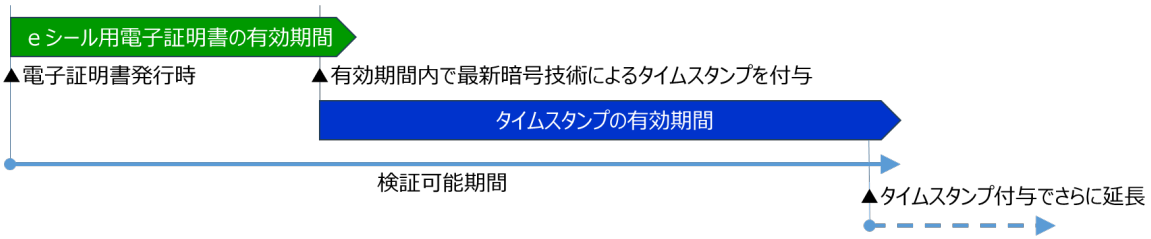


図 10-2　タイムスタンプで検証期間を延長する手段

長期にわたる検証に関する留意事項２：国際標準準拠 ｅシールが付与された文書の確からしさを確認する時点に備えて、将来にわたってｅシールが付与された文書の信頼性を担保することを可能とする国際標準に準拠して処理しておくことを推奨します。 国際標準は、タイムスタンプを利用する長期署名のプロファイルが、ISO14533 にて規定

されています。
検証は、いつ、だれによって実施されるか、そのタイミングや対象データのステークホルダーは特定ができません。国際的に通用する標準に準拠したフォーマットを利用することが有効です。

ここで、国際標準である長期署名プロファイル（ISO14533）の仕組みについて、図 10-3 にて説明します。

まず、①ｅシールでデジタル署名します（ES)。署名時点を後日確認できるように、②署名タイムスタンプ（STS）を付与します（ES-T)。そして③ｅシール用電子証明書に係る情報を収集し、そのｅシールが署名時点で有効であったことを後日証明するために格納します（ES-XL)。④これらの情報をタイムスタンプ（ATS）で包みます（ES-A)。さらに⑤ATS の有効期限以前に、さらに ATS で包むことを繰り返すことで、ES の信頼性を保証するフォーマットです。

ATS は、付与時点で強力な暗号技術を利用することで、暗号技術の進化にも追従し将来にわたって ES の信頼性を証明することが可能となります。

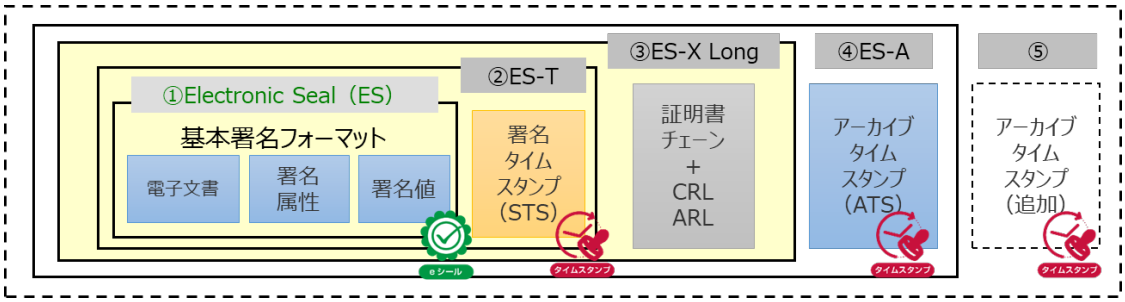


図 10-3　長期署名フォーマット ISO14533

１１．ｅシールの検証

ｅシールの検証時に先ず重要となるのがデジタル署名の検証ですが、デジタル署名方式のｅシールと電子署名は技術的には同様の実装であるため、この部分において電子署名とｅシールに実質的な違いはありません。（デジタル署名の検証については、日本ネットワークセキュリティ協会から発行されているデジタル署名検証ガイドライン[33]を参照ください。）その為、本章では、デジタル署名の検証以外の観点について解説します。

１１-１　ｅシールの検証例

ｅシールの提供する信頼性が、検証者が求める信頼性のレベルに達しているかを判断する為には、デジタル署名の検証後、ｅシールの保証レベルを確認することが重要となります。

ｅシールのレベルについては、総務省の「ｅシールに係る検討会」において示され、その認定制度化及び検証基盤について検討されている段階（2024 年 3 月時点）です。将来的には、認定されたサービスに基づくｅシール用電子証明書について、検証可能な基盤が整備されることが期待されますが、本書では現時点で可能な検証例について紹介します。

現在、ｅシール用電子証明書を発行する認証局について一定の基準に基づく第三者評価を実施することで信頼性の保証を実現している枠組みがいくつかあります。

Adobe 社の AATL（Adobe Approved Trust List）

Adobe 社は、AATL Technical Requirement を充足している認証局を AATL で公開しており、AATL に掲載されている認証局の証明書は、Adobe 社の製品群においてデフォルトで信頼されています。従って、Adobe Acrobat 等で信頼できる署名として表示されるｅシールについては、一定の信頼性があると言えます。

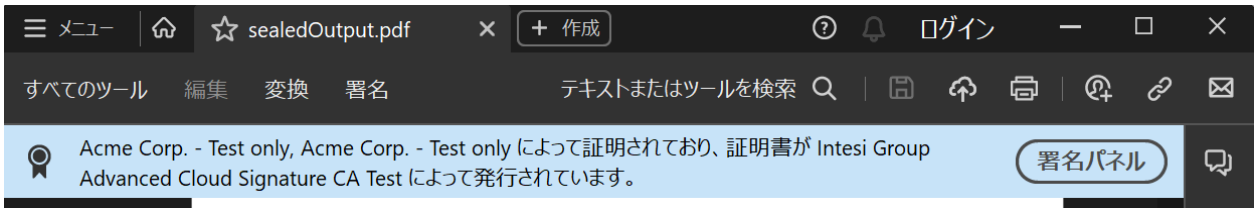


図 11-1　AATL の表示例

[33] デジタル署名検証ガイドライン：
https://www.jnsa.org/result/e-signature/2023/index.html

JIPDEC トラステッド・サービス登録

一般財団法人日本情報経済社会推進協会（JIPDEC）の JIPDEC トラステッド・サービス登録では、公開された基準（JIPDEC トラステッド・サービス登録（認証局）登録基準）に基づいた認証局の審査を実施しており、基準に適合した認証局とその証明書のフィンガープリントのリストを公開しています。検証者が手動で、e シール用電子証明書とリストを比較して検証する必要があるものの、一定の信頼性があると言えます。

欧州 eIDAS 規則

欧州域内において、法的効力（データの起源と完全性）が推定されるレベルの e シールとして、適格 e シールがあります。適格 e シール用電子証明書は日本国内でも入手可能であり、Adobe 社の製品群においては自動的に信頼できる署名として表示されます。また、適格 e シール用証明書を発行する事業者の一覧は、トラステッドリストと呼ばれる XML 形式のリストで公開されています。[34]

図 11-2　eIDAS 規則の適格 e シールの Acrobat での表示例

日本の e シール認定制度

前述の通り、日本における e シールの認定制度は現在総務省主催の検討会において検討された段階です。その最終取りまとめでは、e シールの保証レベルについて、次の 2 段階を想定しています。

① *総務大臣による認定を受けた e シール用認証業務によって保証されてはいないが、より低コスト・簡易な手続で大量発行される e シールに期待される保証レベル（例：企業間で日常的にやり取りされる電子データ等に活用）*

② *総務大臣による認定を受けた e シール用認証業務によって保証され、e シールが付された電子データの出所・起源や完全性について高い信頼が期待されるレベル（例：排他的独占業務とされている士業等の資格証明書等に活用）*

[34] EU/EEA Trusted List Browser　https://webgate.ec.europa.eu/tl-browser/

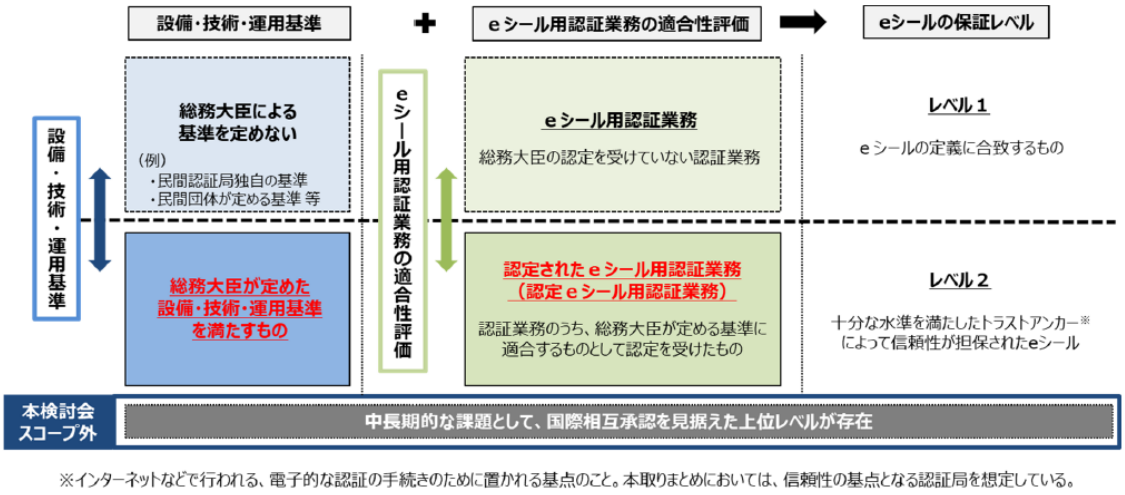


図 11-2　ｅシールの保証レベル [35]

図 11-2 中レベル２のｅシールについては、トラステッドリストや、国によるルート認証局の運営等による検証基盤の整備が期待されます。

１１-２　データの発出元（ｅシールの利用者）の信頼性

多くの場合においてｅシールが提供する信頼性は、データの完全性と、その発出元が商業登記等のベースレジストリに記載のある実在の組織であることの保証であり、発出元組織に対する特定のアプリケーション、ドメインにおける完全な信頼性が保証されるわけではないことに留意が必要です。従って、データの発出元の信頼性については、特定のアプリケーション、ドメインで必要な属性情報の確認を追加で検証することが求められる場合も情報の保証レベルによっては求められることもあります。例えば、発出元組織が特定の ISMS やプライバシーマーク等の特定のセキュリティ要件を充足しているかについて、ｅシールの検証とは別に確認することなどが考えられます。

[35] 総務省「ｅシールに係る検討会」最終とりまとめ　図６

１２．本書の改廃

本書は、デジタルによる業務効率向上のため、流通するデジタルデータの発出元を明確にするｅシールの利用促進を図るうえで、利用者が注意すべき内容を整理し作成したものです。今後、法令や国際的な環境の動向にあわせて随時改訂を行ってまいります。

さらに、ご利用される事業者・組織における実情や課題を適時集約し、ｅシールの最適なご利用方法を盛り込む予定です。

本書に関するご意見・ご要望がございましたら、一般社団法人デジタルトラスト協議会（JDTF）[36]までご連絡ください。

[36] https://jdtf.or.jp/

付録１：組織の内規テンプレート

【サンプル】ｅシール運用規程

目次

第１章 総則

（目的）

第１条 本規程は、印章管理規程に則り社印（角印）の交付を受け、当社から発行する文書・書類に社印（角印）を捺印することによって対象となる文書・書類の発行元を明らかにする行為（以下「本行為」という）に代わり、電磁的に作成された文書・書類に対して、本行為を実現するためにｅシールを付与する際の、適法性の確保および業務内容を明確化することを目的とし、ｅシール用電子証明書、ｅシールを付与した電磁的文書・書類の保管および管理に関する事項を定める。

（定義）

第２条 本規程における用語を以下のとおり定義する。

（１）「ｅシール」とは、電磁的記録に付与された電子データをいう。
ｅシールは、電子認証局により適切な審査を経た上で組織に対して発行された電子証明書を使用し、ｅシールが付与された電磁的文書・書類の発出先を特定し、付与された時点での完全性を証明するために用いるものとし、契約行為などの意思表明には利用をしないものとする。

（２）「管理責任者」とは、本規程に関するすべての管理責任を負う者をいう。

（３）「ｅシール権限者」とは、電子文書にｅシールを付与することができる権限者をいう。

（４）「所管担当者」とは、ｅシールを付与した電子文書の保管および管理の手続きを行う者をいう。

（主管部署）

第３条 本規程に関する主管部署（以下「主管部署」という）は、〇〇〇部とする。

（管理責任者）

第４条 管理責任者は、主管部署の担当役員とする。

第２章 ｅシール、ｅシール付与済み電子文書の保管および管理

（原則）

第５条 プレスリリースなど社外に公開する文書の発行及び、取引関連書類（見積書・請求書など）の発行を電磁的に作成する方法により行う場合は、原則、本規程に定めるｅシールを付与する。

（ｅシール）

第６条 本規程の対象となる文書・書類に対してｅシールを付与するｅシール権限者は、主

管部署に所属し、主管部署責任者に指名された者とする。ただし、主管部署以外の部署に所属する者であっても、印章管理規程に則り本目的のために印章の交付を受けた押印所管部署に所属し、ｅシール権限者の代わりにｅシールを付与する権限の承認を主管部署責任者より受けた者はｅシール権限者としてｅシールを付与することができる。

（ｅシールの手続き）
第７条　ｅシールの手続きは、主管部署が別途作成するマニュアルに定めるものとする。また、ｅシールを付与するために必要な決裁の取得については、社印（角印）を付与する際の押印手続きに関する規程に準ずるものとする。

（ｅシール用電子証明書の発行、管理等）
第８条　ｅシール付与に必要となる電子証明書の発行、管理等については電子認証局より提供される規約や運用規程に準ずるものとする。

（情報管理）
第９条　ｅシール権限者は、ｅシールを付与する際に必要となるID及びパスワードや暗証コードなどを厳正・的確に管理するものとし、漏洩、紛失、盗難等が発生した際には、管理責任者に速やかに報告するものとする。また、報告を受けた管理責任者は電子認証局に対して、当該ｅシール用電子証明書の失効手続きを行うものとする。

（管理責任）
第10条 管理責任者は、本規程に関するすべての管理責任を負う。

（ｅシール付与済み電子文書の保管および管理）
第11条　ｅシールを付与した電子文書の保管および管理は、所管担当者が行う。
２．所管担当者は、主管部署に所属する者とする。

（ｅシールに関連する事故）
第12条　ｅシールに関連する事故が発生した場合、管理責任者は自らの責任のもと、適切に対処を行う。

第３章 その他
（改廃）
第13条 本規程は、主管部署の担当役員の承認により、改廃する。

附 則

本規程は、YYYY年MM月DD日から施行する。
規程制定日：YYYY 年 MM 月 DD 日

改訂履歴
YYYY 年 MM 月 DD 日　第 1 版発行

付録２：Q&A

Ｑ１：ｅシールとは何ですか？

Ａ１：ｅシールは、デジタルデータの発出元の組織を特定するために付与されるデータです。総務省の「ｅシールに係る検討会」では、最終とりまとめにて、以下のように定義されています。

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。

Ｑ２：ｅシールのメリットは？

Ａ２：ｅシールは、発行組織、受信側それぞれに、以下のメリットがあります。

発行組織

・対象デジタルデータの完全性を担保して発信ができます。

・組織内の複数の担当者が利用できます。

・システムから発信ができるので、効率良く大量に発信ができます。

・デジタルデータの状態で、組織の信用を高めることができます。

受信側

・対象情報の発信元を電子的に検証ができるので、情報を効率良くスクリーニングが可能です。

・デジタルデータの状態で発行元を特定する記録として保管できます。

・安心して対象のデジタルデータを利用できます。

Ｑ３：電子署名とｅシールの違いは？

Ａ３：電子署名もｅシールも対象デジタルデータの完全性と発出元を保証しますが、電子署名は自然人を特定し、ｅシールは組織を特定します。

電子署名では、付与した本人による意思表示まで証明することが可能ですが、ｅシールでは、意思表示はありません。

また、電子署名は、自然人個人を特定することとなるため、署名者は本人に限られます。

ｅシールは組織を特定することが目的なので、組織によって利用者権限を付与された複数人および組織によって管理されているシステムによる利用が可能となります。

Q４：ｅシールには有効期限がありますか？
Ａ４：ｅシールは、暗号処理の安全性がコンピュータの能力に依存することから、その検証には有効期限があります。詳しくは、第 10 章を確認ください。

Q５：ｅシールとタイムスタンプの違いは？
Ａ５：ｅシールとタイムスタンプは、どちらも対象データの完全性を保証するものですが、その証明対象が異なります。ｅシールは、付与対象データの発出元を特定するデータであり、タイムスタンプは、対象データに信頼のおける時刻を付与することで、その事象がその時点に存在していたことを証明するデータです。
併用することで、対象データの発出元とその内容が存在していた時刻を証明することが可能となります。

Q６：ｅシールとタイムスタンプの付与順は？
Ａ６：タイムスタンプは、事象の時刻を証明するものなので、ｅシールを付与したのちにタイムスタンプを付与することでシール時刻を特定することとなります。

Q７：当社がｅシールを使い始めると、取引先に余計な仕事を増やすことにはならないでしょうか？
Ａ７：取引先では、ｅシールがあることで特に業務の発生はありません。
必要に応じて、付与されているｅシールの検証を実施し、受領した電子文書が正当なものであることの判断が容易に可能になります。検証の詳細は、第 11 章を確認ください。

Q８：電子契約の際に電子署名に替えてｅシールは使えますか？
Ａ８：電子契約における意思表示を示す手段としてｅシールは利用できません。
ｅシールは、組織の発出元を特定する手段であります。組織には、自然人と異なり意思がありませんので、契約行為に対しての意思表示はできません。
しかし、対象情報に関して、組織が関与していることを特定することは可能であり、
例えば、電子取引（取引に関して受領し又は交付する注文書、契約書、送り状、領収書、見積書その他これらに準ずる書類に通常記載される事項（電子帳簿保存法第二条５号））において、これらの情報の発出元を特定し、完全性を保証することは可能です。

Q９：電子署名とｅシールの手続き上の留意点の違いは？
Ａ９：電子署名の場合、利用権限を持つ人間の異動や退職など権限変更の必要がある際には、電子証明書の失効や署名鍵の廃棄の処理と、新たに任命された責任者の署名鍵および電子証明書の発行手続きが必要になります。

一方で、e シール用電子証明書は組織に対して発行されるので、認証局への手続きは法人格の変更など以外は、不要です。

eシール利用者ガイドライン TF 委員名簿（所属名・氏名の 50 音順、敬称略）

須賀 祐治	株式会社インターネットイニシアティブ
大槻 文彦	一般社団法人 XBRL Japan
濱口 総志	株式会社コスモス・コーポレイション
板倉 忠文	ＪＦＥシステムズ株式会社
猪俣 智子	ＪＦＥシステムズ株式会社
伊藤 健太郎	GMO グローバルサイン株式会社
佐藤 拓巳	サイバートラスト株式会社
渡邉 弘幸	サイバートラスト株式会社
木村 正光	株式会社スカイコム
柴田 孝一	セイコーソリューションズ株式会社
大野 文彰	セコムトラストシステムズ株式会社
相良 直彦	セコムトラストシステムズ株式会社
小田嶋 昭浩	株式会社帝国データバンク
丸山 修平	東京海上日動火災保険株式会社
坂本 浩基	日本電気株式会社
関 行秀	日本電気株式会社
林 亮平	日本電気株式会社
石川 智也	株式会社 日立製作所
渋谷 秀人	富士通株式会社

一般社団法人　デジタルトラスト協議会
ビジネスプロセス with トラスト委員会　e シール利用者ガイドラインタスクフォース

以上