リモートeシールガイドの作成検討

eシールとは何なのか？
また、eシールが求められている用途や検討状況とJT2Aが検討しているガイドラインを説明します

2023.06.07

日本トラストテクノロジー協議会 運営委員長

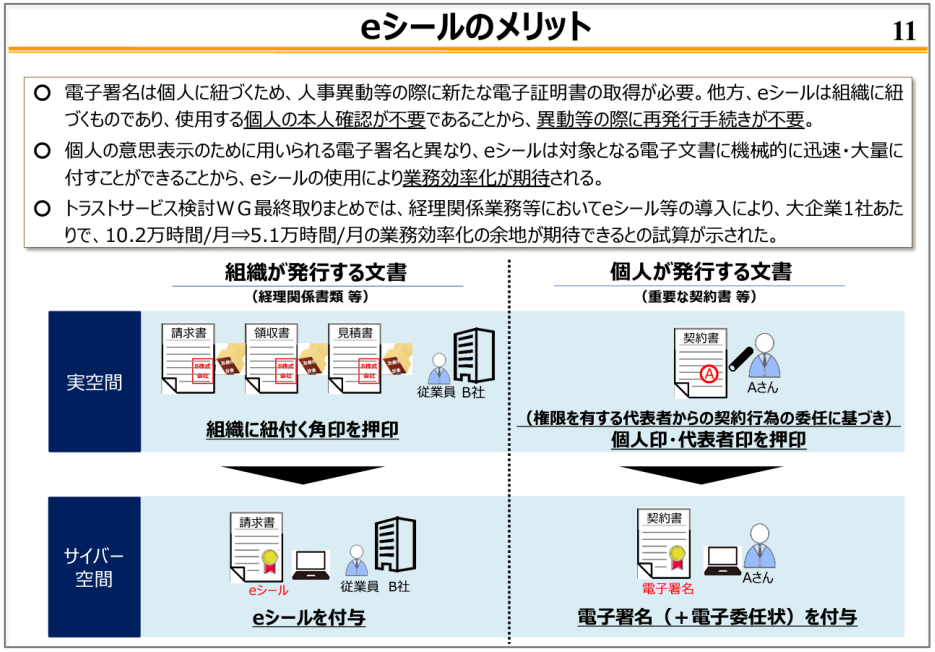
小川 博久 氏

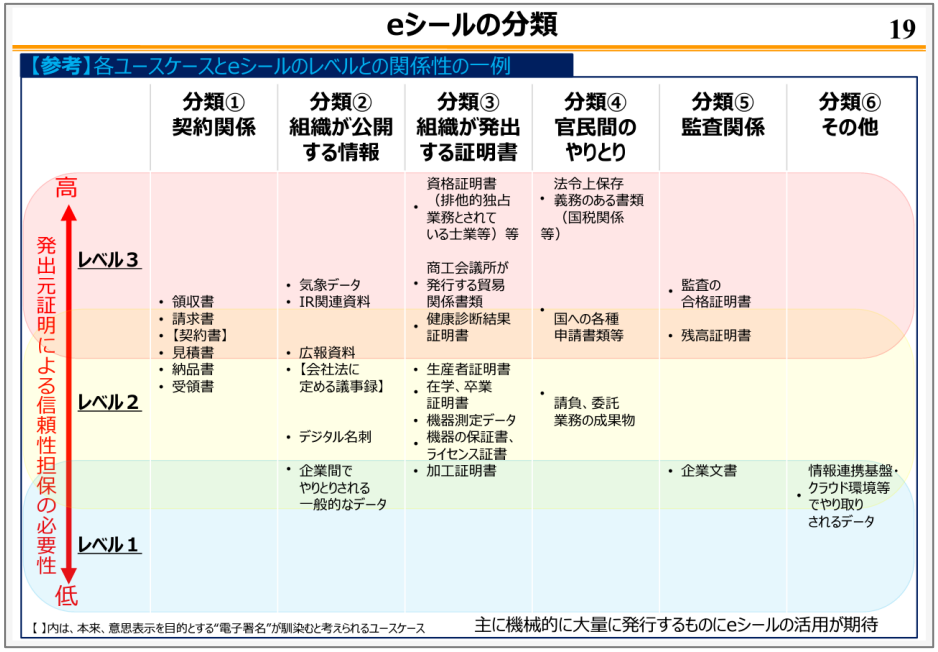
目次

eシールの定義と利用シーン

- eシールとは、電子文書等の発行元の組織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であって、発行元が個人に限らず組織となることもある。我が国においては、eシールに関する公的な仕組みは現状存在していないものの、一部の企業において、組織名の電子証明書としてe シールの導入が進んでいる。

（総務省の検討資料抜粋）

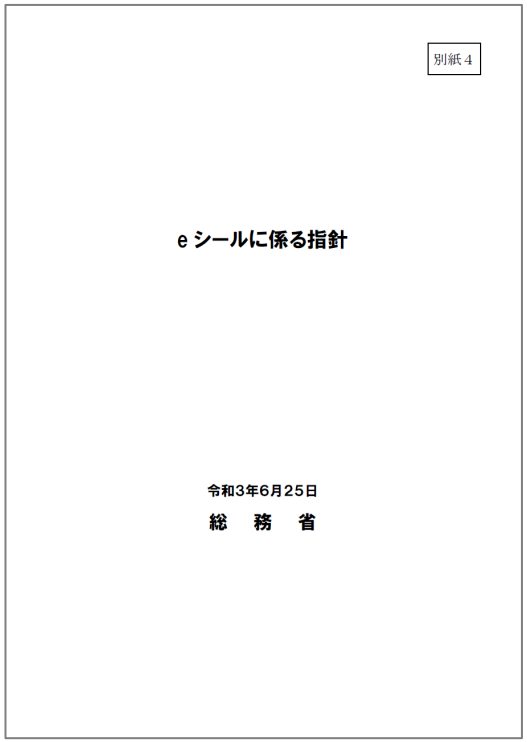




出所）eシールに関する総務省の取組と期待、令和５年３月８日、総務省サイバーセキュリティ統括官室
https://jdtf.or.jp/news/2023/file/【230308+講演資料】eシールに関する総務省の取組と期待+vf.pdf

総務省から指針を発行している

- 令和3年に総務省から発行された「eシールに係る指針」では、「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」での議論を踏まえ、eシールを3つに分類している。



別紙４

eシールに係る指針

令和3年6月25日

総　務　省

2．1　eシールの分類

我が国における e シールは、発行元証明の信頼性を担保するための措置の水準に応じて、以下のとおりレベル分けを行う。

・　**レベル1：　eシール**

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）に合致するもの。

・　**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。

・　**レベル3：　レベル2に加えて、十分な水準を満たしたトラストアンカー[9]によって信頼性が担保されたeシール**

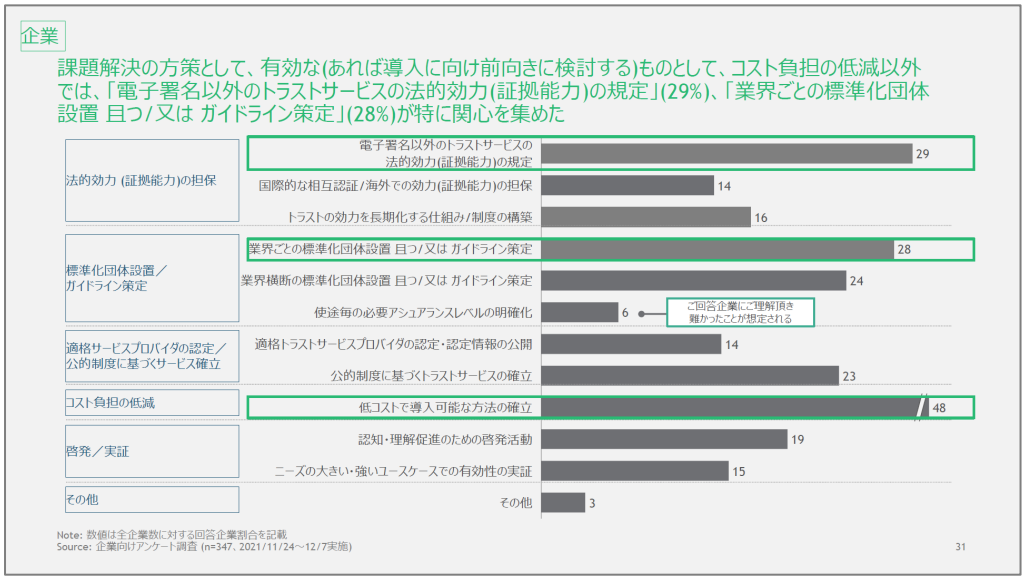
組織等の実在性の確認の方法や認証局における設備のセキュリティ要件等について、十分な水準を満たしたトラストアンカーによって信頼性が担保され、発行元証明として機能することに関し、第三者のお墨付き（将来的には国による認定制度等の要否を検討）があるもの。

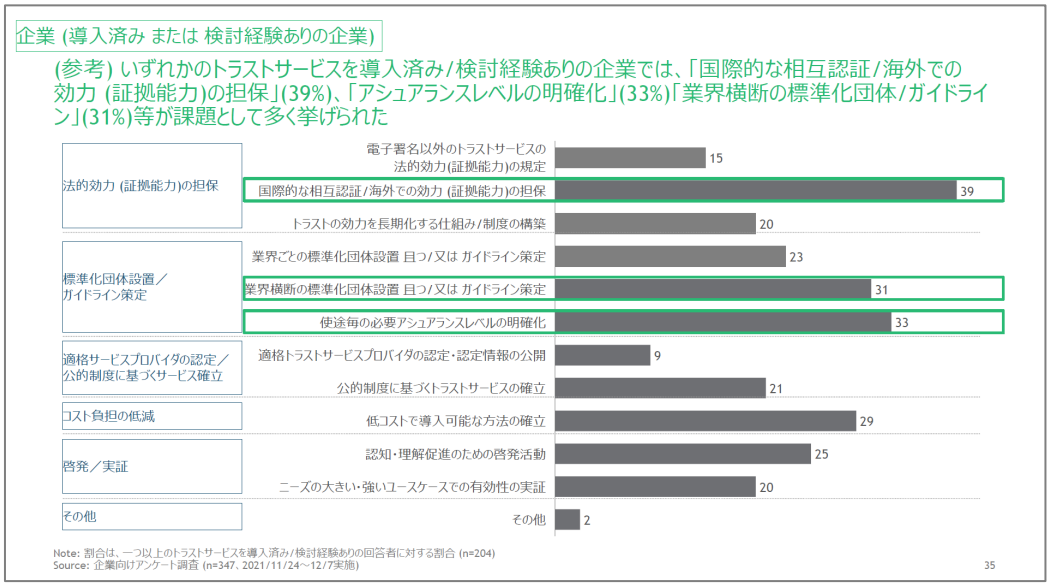
なお、レベル1～3の eシールを判別するための呼称については将来決定することが必要となる。

出所）総務省｜タイムスタンプ・eシール　eシールに係る指針
https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html

デジタル庁｜トラストを確保したDX推進サブワーキンググループの検討

- 企業は、「法的効力」、「業界ごとのガイドライン」、「低コストで導入可能」に課題意識がある。
- 導入済・検討経験のある企業は、「国際的な相互認証/海外での効力」、「業界横断のガイドライン」、「用途毎のアシュアランスレベル」に課題意識がある。

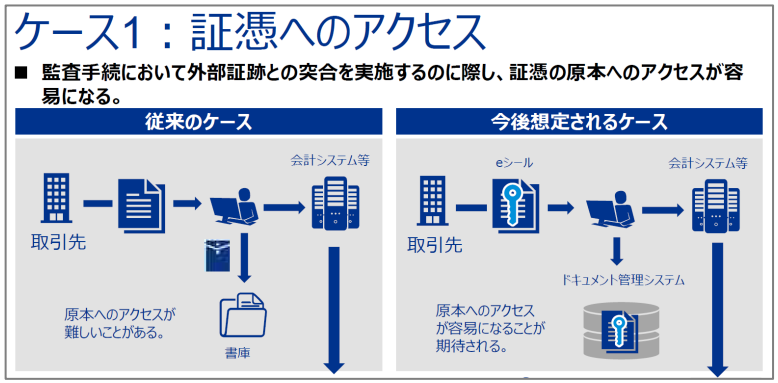




出所)トラストを確保したDX推進サブワーキンググループ報告書、令和4年(2022年)7月29日、デジタル庁
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf

デジタル庁｜トラストを確保したDX推進サブワーキンググループの検討

- 検討会で議論した内容として、監査分野での事例を示している。
- また、<u>鍵管理を考慮し、業務委託やクラウドサービスの活用</u>も示唆している。



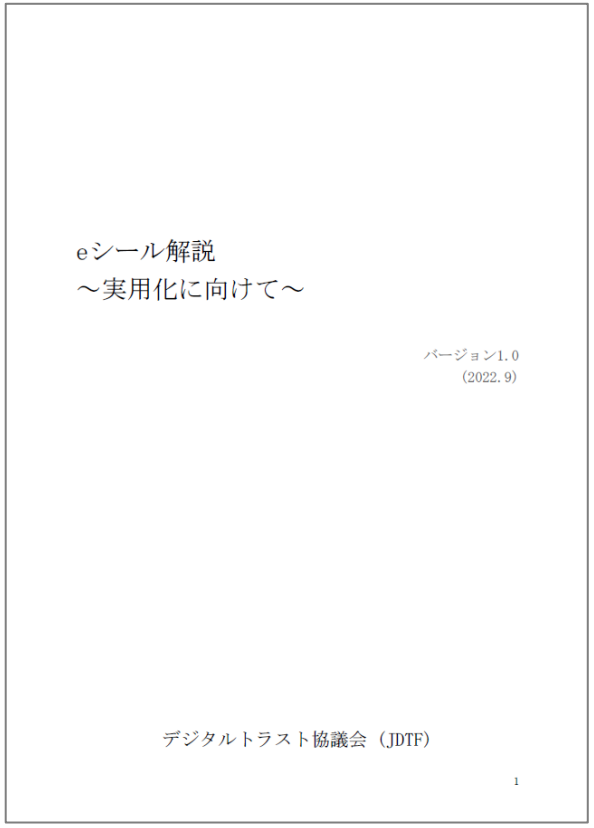
制度推進に際しての課題(2/3)

項目	課題	参考
暗号鍵の管理、承認手続	• 暗号鍵が不正に流出しないように管理を徹底する必要がある。 • 企業側の利用者権限ルールの明確化、厳格な運用が必要になると考えられる。 • 幅広い証憑において利用可能となるが、物理的な社印と管理方法が異なるため、従来のルールで良いか検討が必要と考えられる。	• 暗号鍵を各利用者の個別管理に委ねる対応は、不正利用のリスクが高まる要因となるため、（組織規模によるが）集中管理が望ましい。 • USBやPCに保存する場合は、耐タンパー性の考慮は必須になるが、PC交換が難しい場合やUSBなどの物理管理を避けたい場合も想定される。 →集中管理のための専用設備の投資や鍵の管理方法を考慮すると、業務委託やクラウドサービスの活用は有益なものになると考えられる。
証明書の信頼性の確保	• 認証局のセキュリティの確保、証明書のインテグリティの確保のための制度作りが必要 • 外部委託やクラウドサービスを活用する場合は、その委託先やクラウドベンダーのセキュリティや処理のインテグリティの確保も必要	• 認証局のセキュリティや証明書のインテグリティに関する評価制度は、既存の他の制度が存在するため、それらが参考になる。規制やガイドラインが重複しないような調整が望まれる。 • eシールの活用も踏まえて請求書発行プロセスを外部に委託する場合は、財務報告の主要なプロセスであることから、SOC1/SOC2などの外部評価があることが望ましい。

出所）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、令和4年（2022年）7月29日、デジタル庁
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

デジタルトラスト協議会（JDTF）はeシール解説を発行

- JDTFのeシール解説では、ユースケース例、システムモデル、実用化するための課題を記載している。
- eシールのシステムモデル例は、4つの具体的な例を示している。

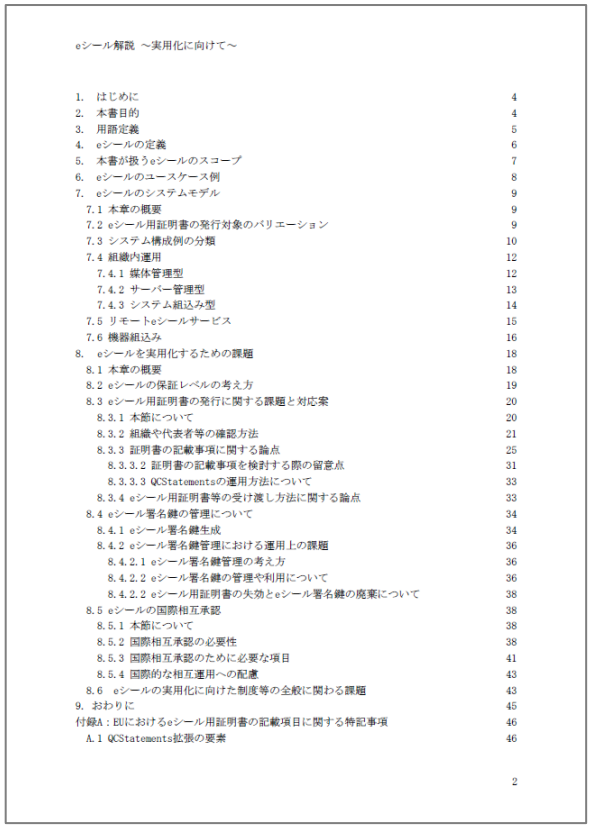


eシール解説
～実用化に向けて～

バージョン1.0
(2022.9)

デジタルトラスト協議会（JDTF）

1



eシール解説 ～実用化に向けて～

2

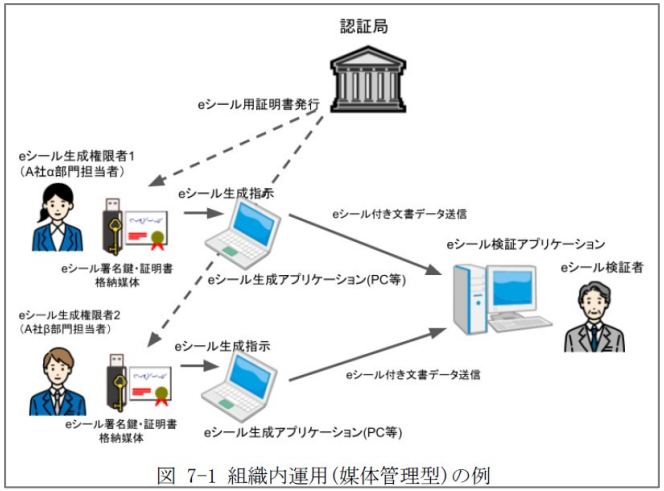


図 7-1 組織内運用（媒体管理型）の例

出所）eシール解説 ～実用化に向けて～ バージョン1.0（2022.9）デジタルトラスト協議会（JDTF）
https://jdtf.or.jp/report/whitepaper/file/eシール解説(バージョン1.0).pdf

JDTFのeシールのシステムモデル例

- 以下、4つのシステムモデル例を掲載している。
- ①組織内運用（媒体管理型）、②組織内運用（サーバー管理型）、③組織内運用（システム組込型）、④リモートeシール　＊①は前頁に掲載

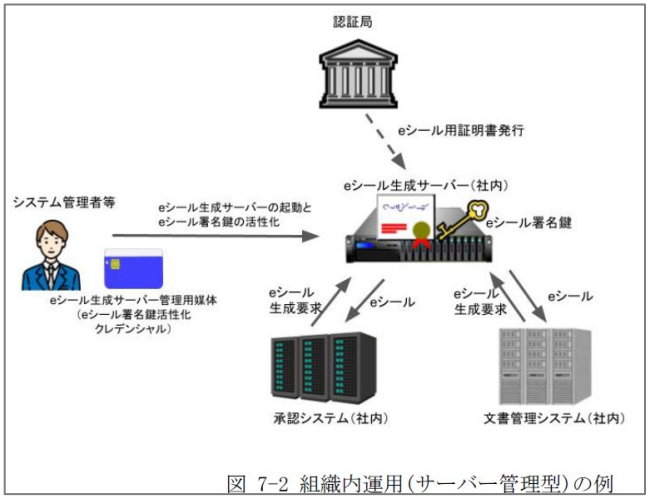


図 7-2 組織内運用（サーバー管理型）の例

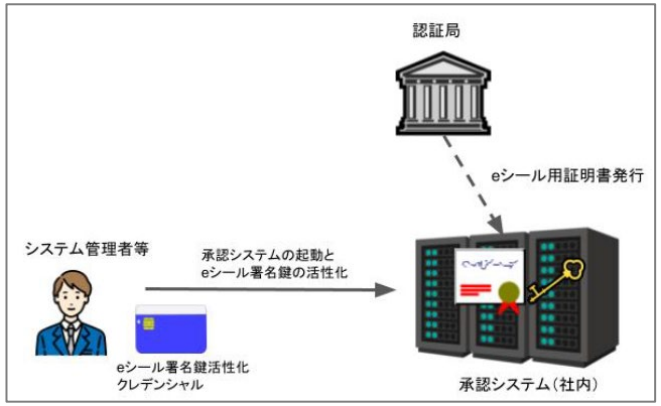


図 7-3 組織内運用（システム組込型）の例

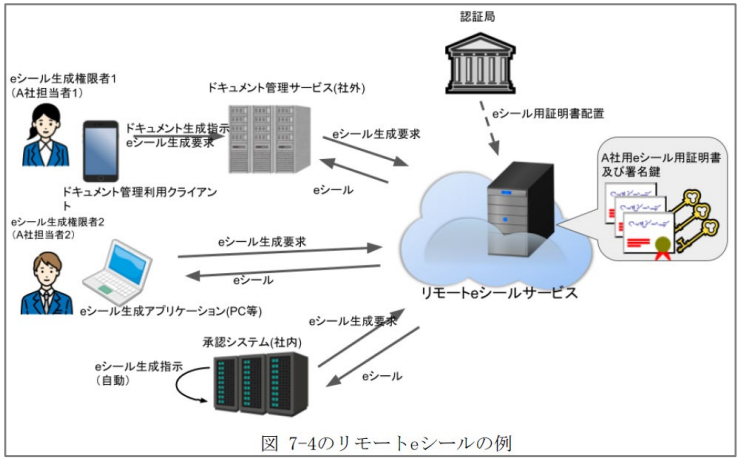
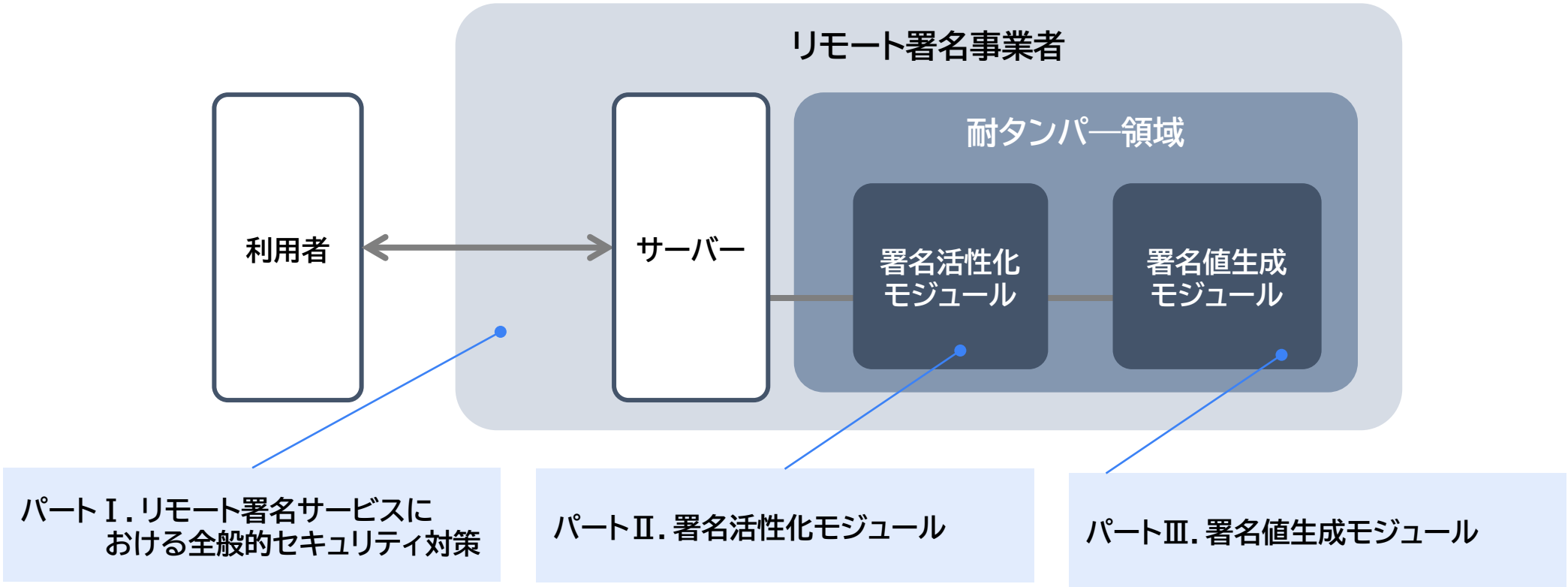


図 7-4のリモートeシールの例

出所）eシール解説　～実用化に向けて～　バージョン1.0（2022.9）デジタルトラスト協議会（JDTF）
https://jdtf.or.jp/report/whitepaper/file/eシール解説(バージョン1.0).pdf

リモート署名ガイドラインの発行

- JT2Aは、2020年に「リモート署名ガイドライン」を発行している。
- リモート署名事業者の「全般的セキュリティ対策」、「署名活性化モジュール」、「署名値生成モジュール」の3部構成。



出所）NPO日本ネットワークセキュリティ協会　報告書・公開資料　リモート署名ガイドライン、日本トラストテクノロジー協議会（JT2A）
https://www.jnsa.org/result/jt2a/2020/

リモートeシールのガイドラインを作成中

- リモートeシールサービスの基本的なセキュリティ要件である①全般セキュリティ対策、②署名活性化モジュール、③署名値生成モジュールはリモート署名と同様。
- リモートeシールの概要・解説を新たに発行するタイミングに合わせ、リモート署名ガイドラインの分冊の構成を変更します（パートⅠを分割します）。