

# 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

---

日本トラストテクノロジー協議会 運営委員長

2023.06.07

小川 博久 氏

# 目次

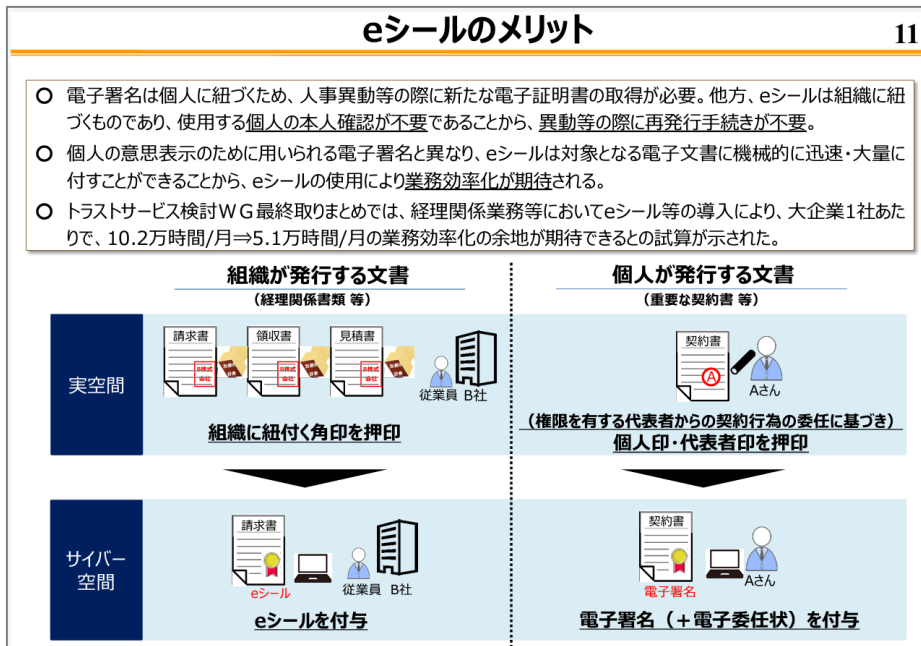
1. eシールとは	3
2. eシールの検討状況	4
総務省の検討 …… 「eシールに係る指針」など	
デジタル庁の検討 …… 「トラストを確保したDX推進サブワーキンググループ」	
デジタルトラスト協議会（JDTF） …… 「eシール解説」	
3. JT2Aの検討	9

# 1. eシールとは

## 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)



### eシールの分類

19

【参考】各ユースケースとeシールのレベルとの関係性の一例

	分類① 契約関係	分類② 組織が公開する情報	分類③ 組織が発出する証明書	分類④ 官民間のやりとり	分類⑤ 監査関係	分類⑥ その他
高			資格証明書 ・ (排他的独占業務とされている工業等) 等	法令上保存・義務のある書類 (国税関係等)		
レベル3		気象データ ・ IR関連資料	商工会議所が発行する貿易関係書類 ・ 健康診断結果証明書	国への各種申請書類等	監査の合格証明書 ・ 残高証明書	
	領収書 ・ 請求書 ・ 【契約書】 ・ 見積書 ・ 納品書 ・ 受領書	広報資料 ・ 【会社法に定める議事録】	生産者証明書 ・ 在学、卒業証明書 ・ 機器測定データ ・ 機器の保証書、ライセンス証書 ・ 加工証明書	請負、委託業務の成果物		
レベル2		デジタル名刺				
		企業間でやりとりされる一般的なデータ			企業文書	情報連携基盤・クラウド環境等でやり取りされるデータ
レベル1						
低						

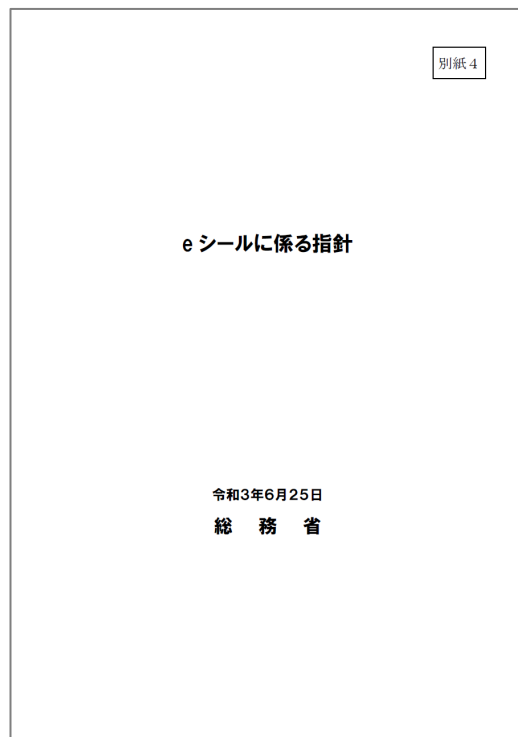
【】内は、本来、意思表示を目的とする“電子署名”が馴染むと考えられるユースケース 主に機械的に大量に発行するものにeシールの活用が期待

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>

## 2. eシールの検討状況

# 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。



### 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タンカー<sup>9</sup>によって信頼性が担保された eシール

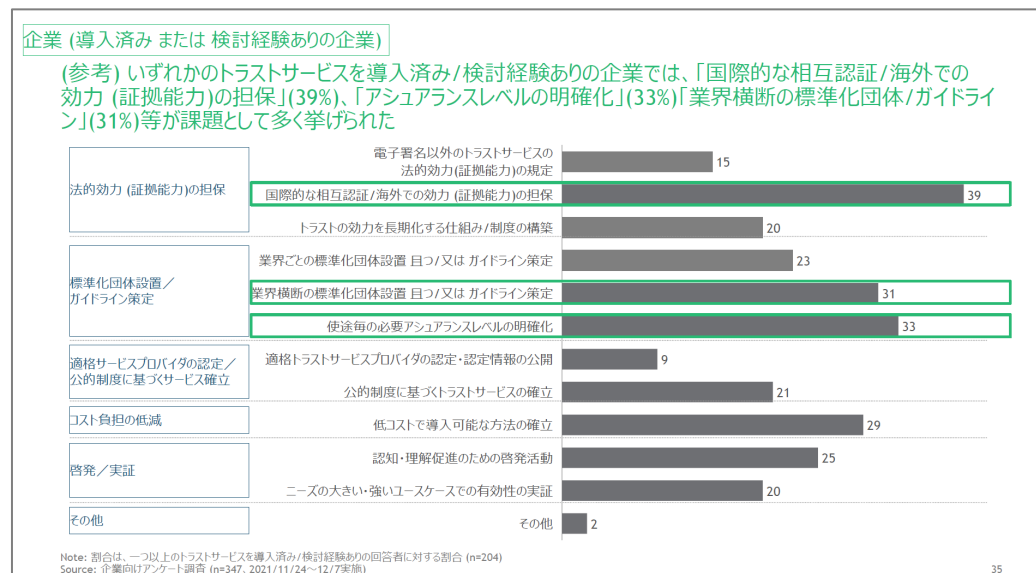
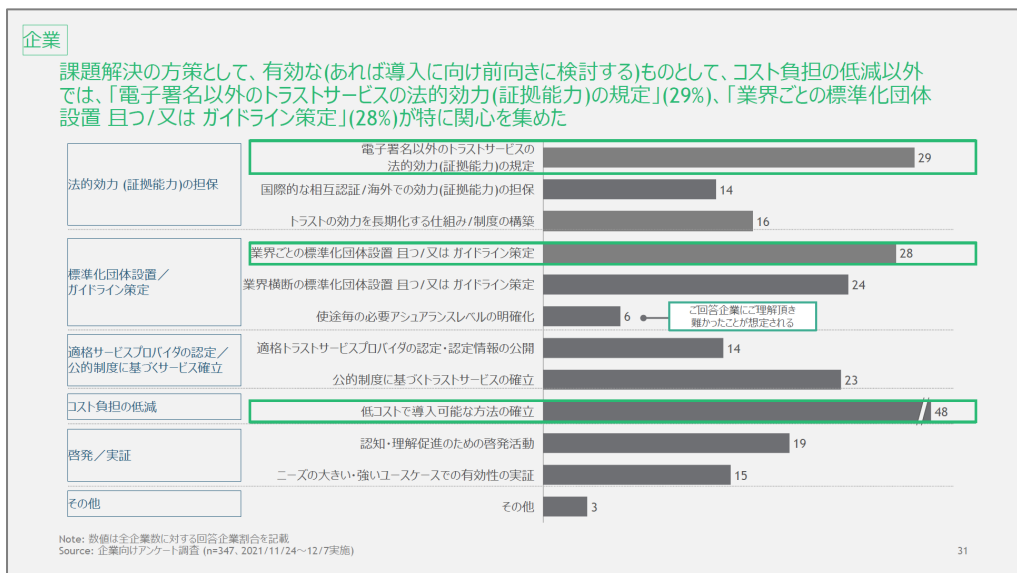
組織等の実在性の確認の方法や認証局における設備のセキュリティ要件等について、十分な水準を満たしたトラスタンカーによって信頼性が担保され、発行元証明として機能することに関し、第三者のお墨付き(将来的には国による認定制度等の要否を検討)があるもの。

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。

## 2. eシールの検討状況

# 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」、「用途毎のアシユアランスレベル」に課題意識がある。

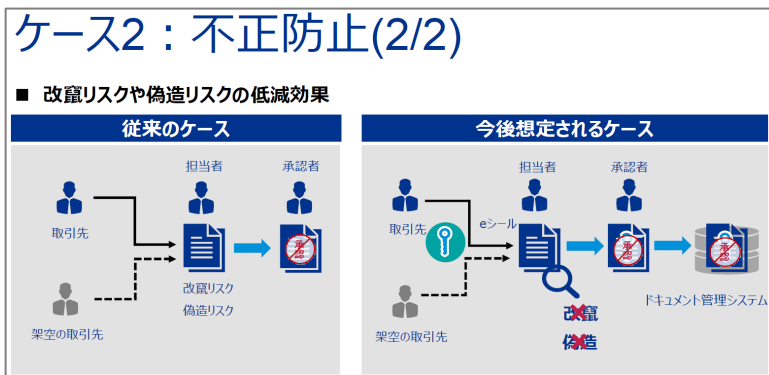


出所)トラストを確保したDX推進サブワーキンググループ報告書、令和4年(2022年)7月29日、デジタル庁  
[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729\\_meeting\\_trust\\_dx\\_report\\_01.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf)

## 2. eシールの検討状況

# 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、**鍵管理を考慮し、業務委託やクラウドサービスの活用**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	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
証明書の信頼性の確保	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

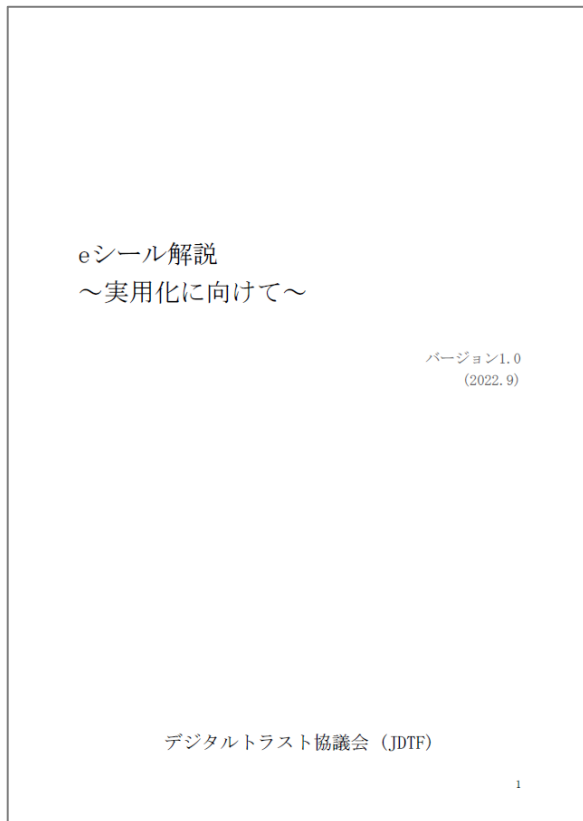
→集中管理のための専用設備の投資や鍵の管理方法を考慮すると、業務委託やクラウドサービスの活用は有益なものになると考えられる。



## 2. eシールの検討状況

# 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~

1. はじめに	4
2. 本書目的	4
3. 用語定義	5
4. eシールの定義	6
5. 本書が扱うeシールのスコープ	7
6. eシールのユースケース例	8
7. eシールのシステムモデル	9
7.1 本章の概要	9
7.2 eシール用証明書の発行対象のバリエーション	9
7.3 システム構成例の分類	10
7.4 組織内運用	12
7.4.1 媒体管理型	12
7.4.2 サーバー管理型	13
7.4.3 システム組込み型	14
7.5 リモートeシールサービス	15
7.6 機器組込み	16
8. eシールを実用化するための課題	18
8.1 本章の概要	18
8.2 eシールの保証レベルの考え方	19
8.3 eシール用証明書の発行に関する課題と対応案	20
8.3.1 本節について	20
8.3.2 組織や代表者等の確認方法	21
8.3.3 証明書の記載事項に関する論点	25
8.3.3.1 証明書の記載事項を検討する際の留意点	31
8.3.3.2 QStatementsの運用方法について	33
8.3.4 eシール用証明書等の受け渡し方法に関する論点	33
8.4 eシール署名鍵の管理について	34
8.4.1 eシール署名鍵生成	34
8.4.2 eシール署名鍵管理における運用上の課題	36
8.4.2.1 eシール署名鍵管理の考え方	36
8.4.2.2 eシール署名鍵の管理や利用について	36
8.4.2.3 eシール用証明書の失効とeシール署名鍵の廃棄について	38
8.5 eシールの国際相互承認	38
8.5.1 本節について	38
8.5.2 国際相互承認の必要性	38
8.5.3 国際相互承認のために必要な項目	41
8.5.4 国際的な相互運用への配慮	43
8.6 eシールの実用化に向けた制度等の全般に関わる課題	43
9. おわりに	45
付録A: 印におけるeシール用証明書の記載項目に関する特記事項	46
A.1 QStatements拡張の要素	46

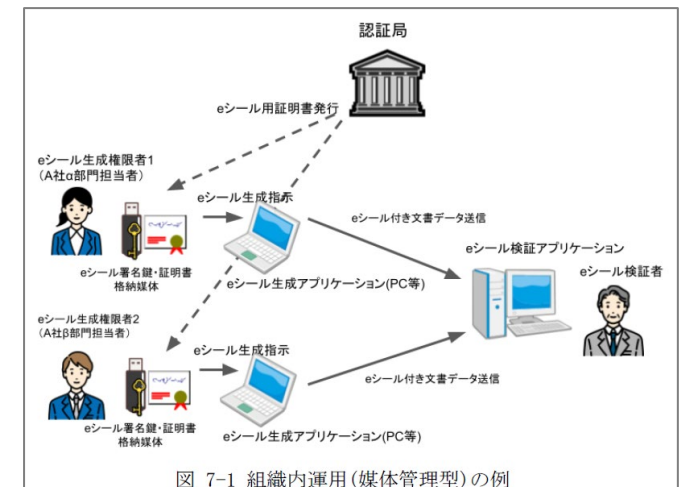


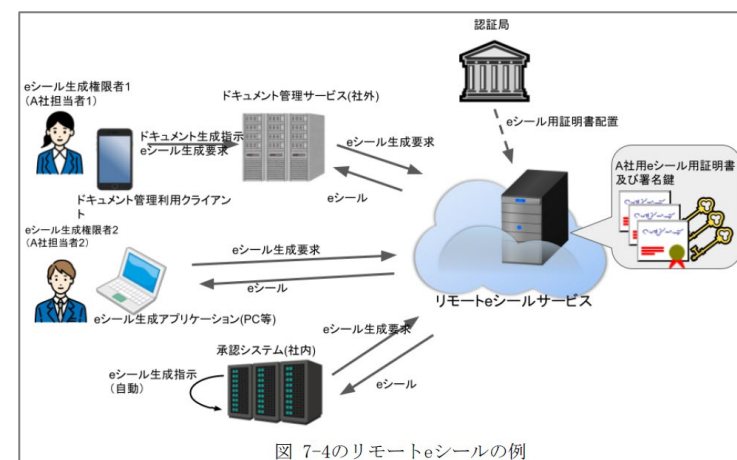
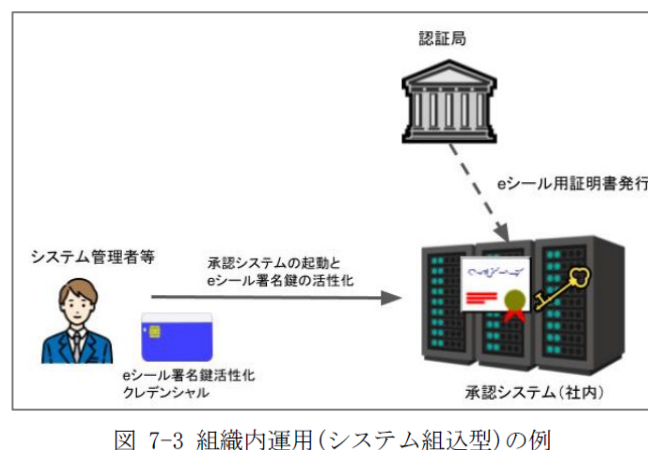
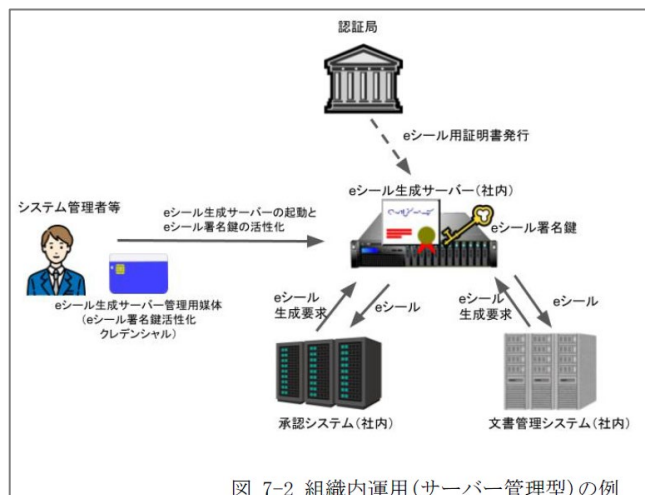
図 7-1 組織内運用(媒体管理型)の例



## 2. eシールの検討状況

# 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

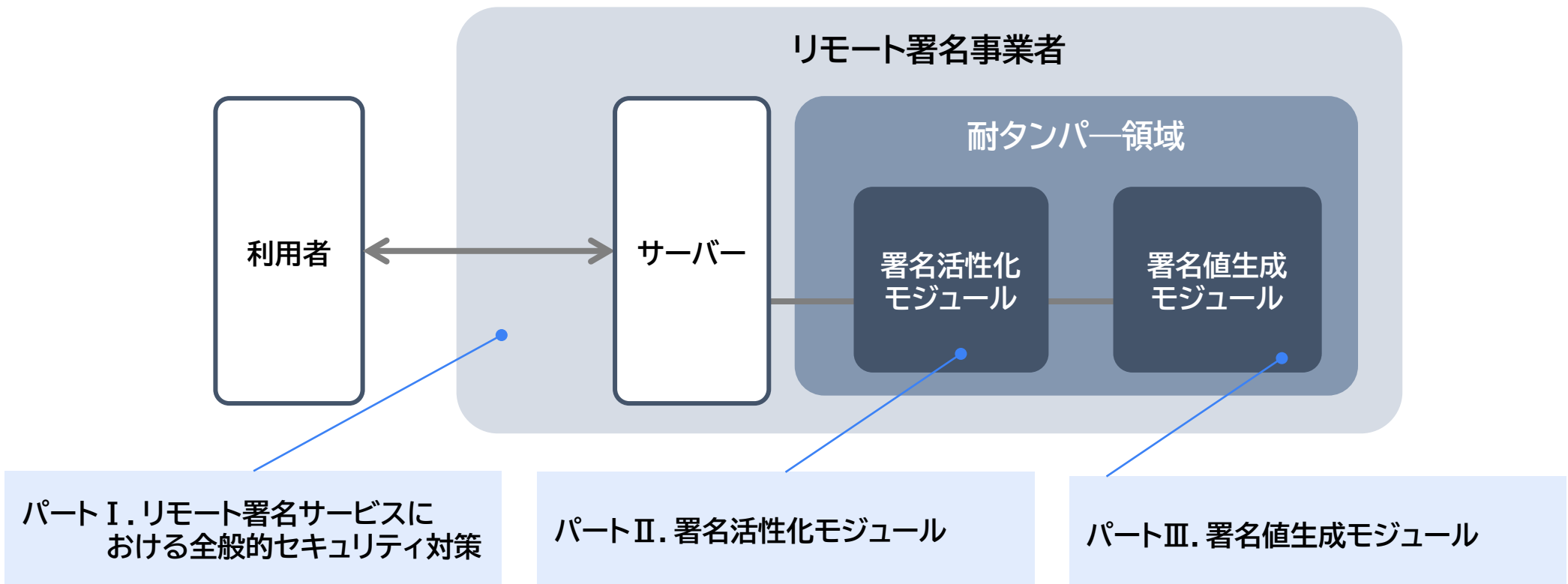




### 3. JT2Aの検討

## 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。



## 3. JT2Aの検討

## 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)。

