

リモート署名/eシールの現在と未来～商
業登記リモート署名・認定認証業務・ガ
イドライン～ アンケート



リモート署名/eシールガイドライン

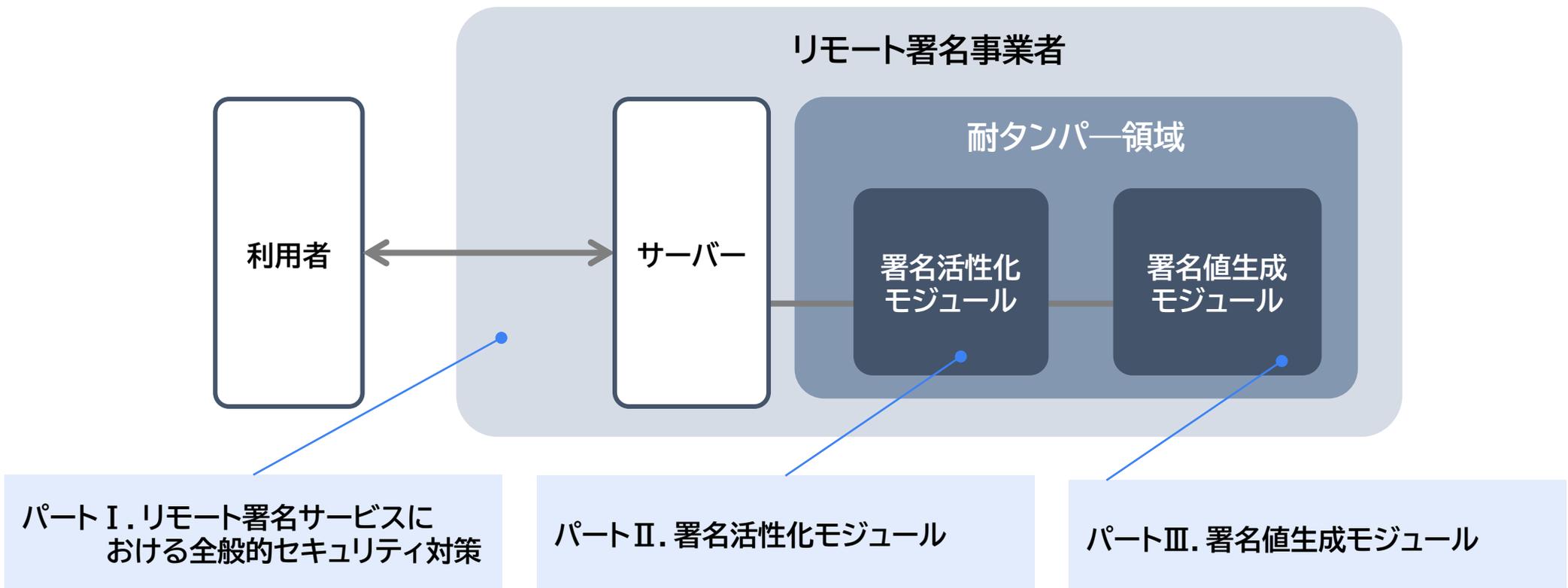
日本トラストテクノロジー協議会 運営委員長
株式会社三菱総合研究所
小川 博久

2026.02.19

1. リモート署名

リモート署名ガイドラインの発行

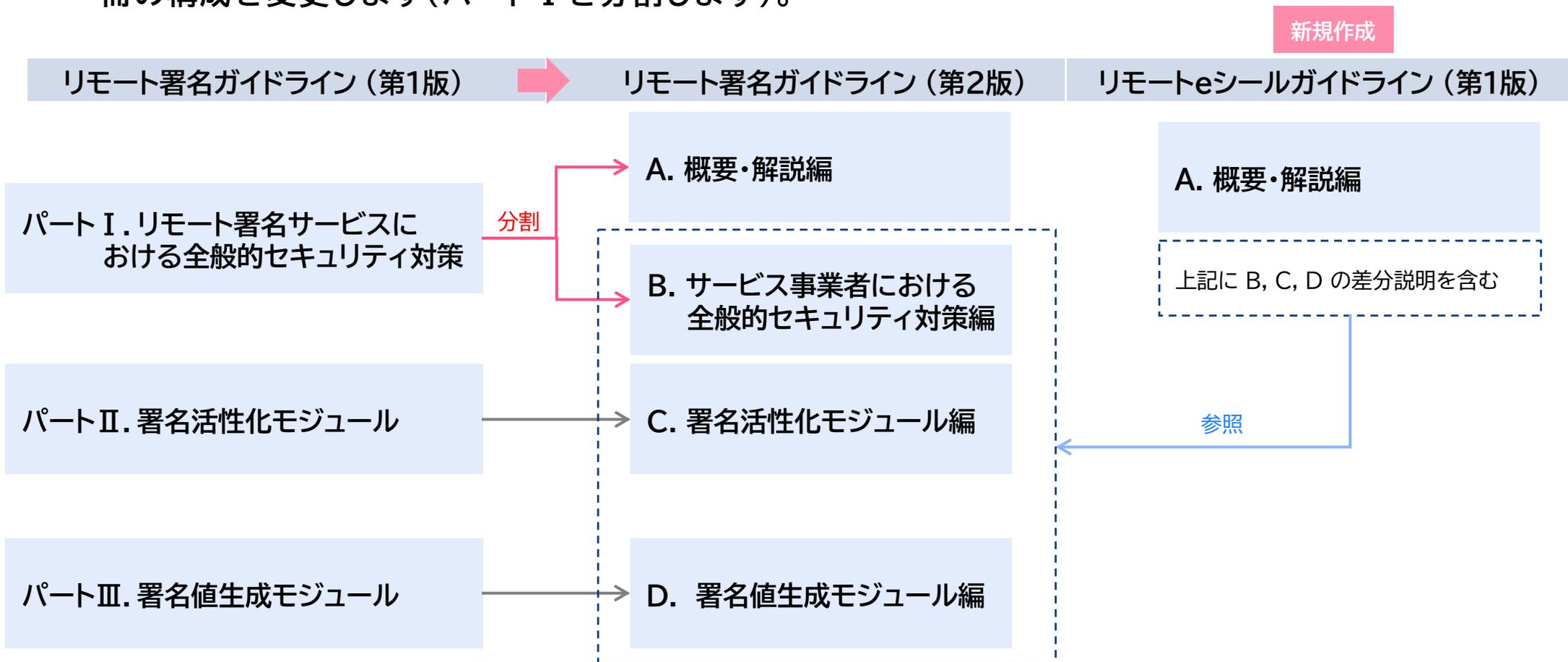
- JT2Aは、2020年に「リモート署名ガイドライン」を発行している。
- リモート署名事業者の「全般的セキュリティ対策」、「署名活性化モジュール」、「署名値生成モジュール」の3部構成。



2. リモートeシール

リモートeシールのガイドラインを作成中

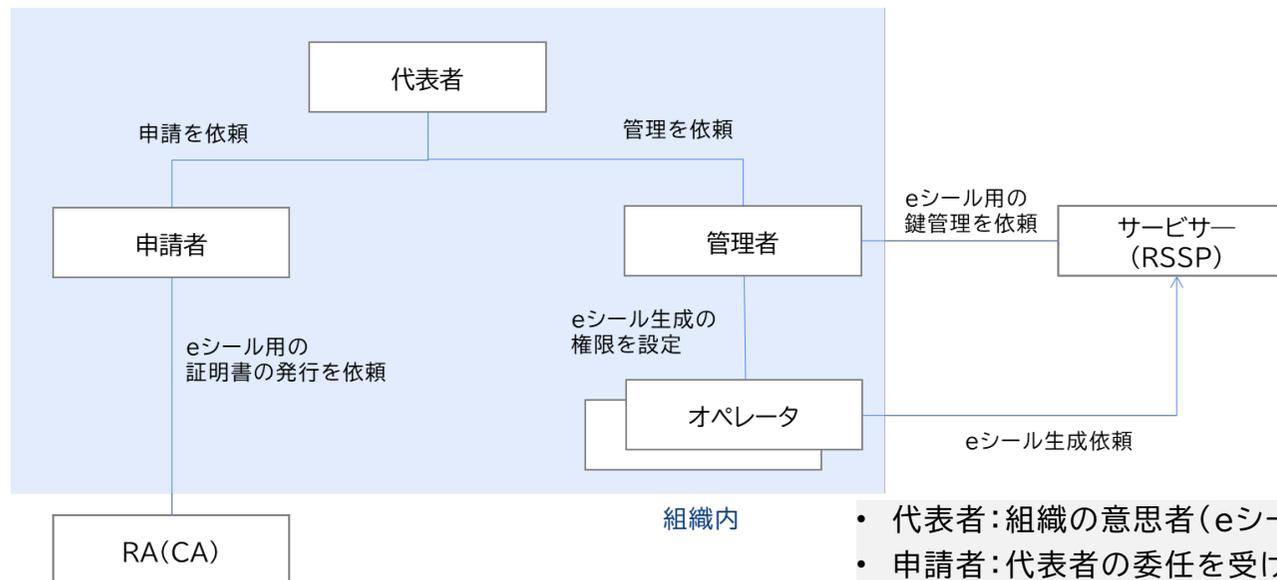
- リモートeシールサービスの基本的なセキュリティ要件である①全般セキュリティ対策、②署名活性化モジュール、③署名値生成モジュールはリモート署名と同様。
- リモートeシールの概要・解説を新たに発行するタイミングに合わせ、リモート署名ガイドラインの分冊の構成を変更します(パート I を分割します)。



3. リモートeシールの検討

リモートeシールの検討

- リモートeシールでは、リモート(遠隔)で生成するため、人が行っているのか、システムが行っているのかが不明確。
- さらに、権限を持った人物か、単に操作を行っているのか(オペレーターなのか不明確)も不明です。
- 結果として、リモートeシールを受け取って検証できたとしても、それが正しいかどうか。ユースケースからパターンを考え、議論した内容をまとめました。

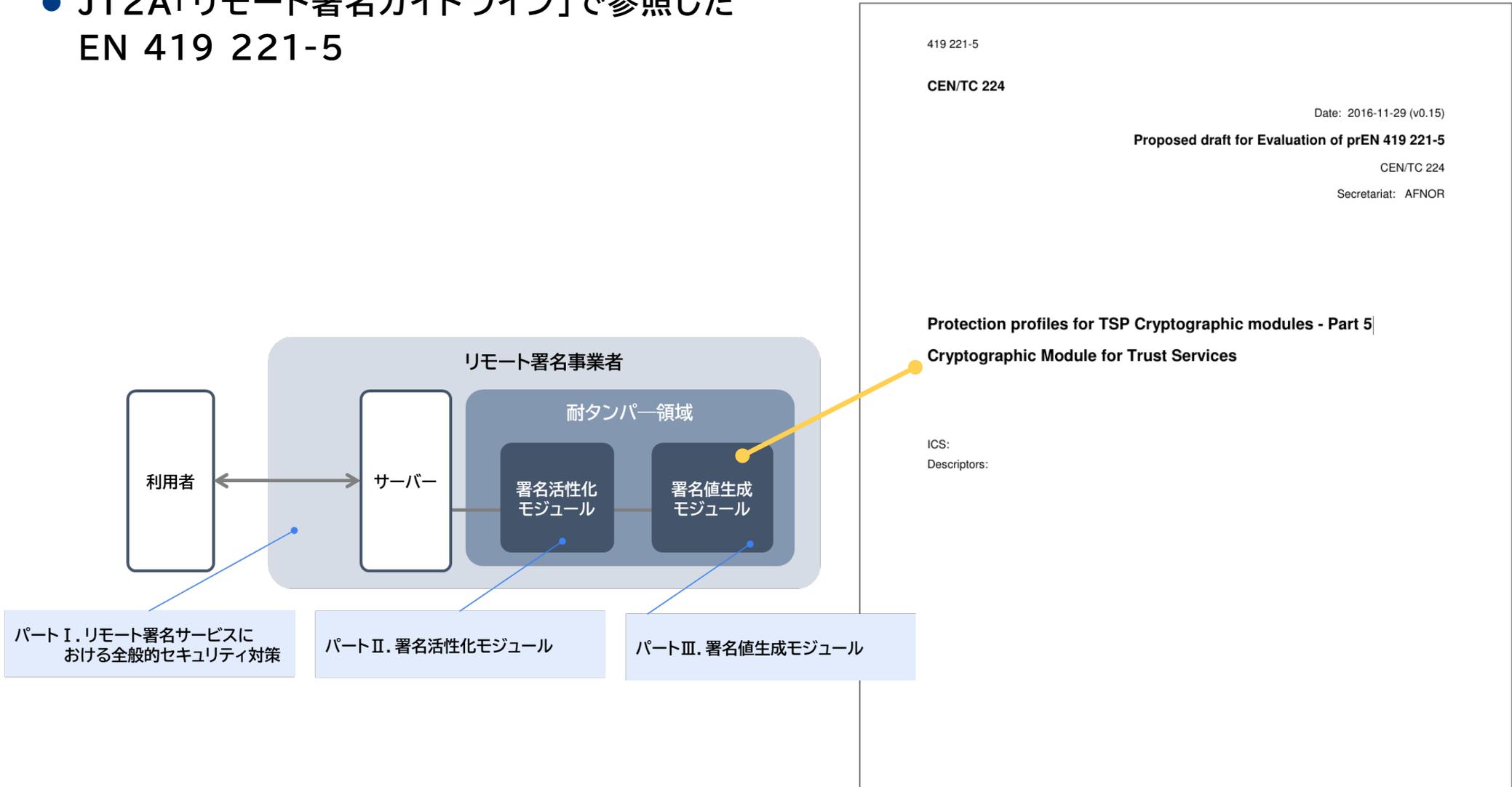


- 代表者: 組織の意思者 (eシール発行組織の代表)
- 申請者: 代表者の委任を受けて、eシール用証明書の発行を申請する者
- RA(CA): 外部の認証局・身元資格確認者
- 管理者: 代表者の委任を受けて、eシール生成とオペレータ(の利用)を管理する者
- オペレータ: eシール生成を操作する者・システム(者の場合、複数もある)
- サービス: eシール用の鍵を管理する外部の事業者

3. リモートeシールの検討

参照規格のアップデート (EN 419 221-5)

- JT2A「リモート署名ガイドライン」で参照した EN 419 221-5



3. リモートeシールの検討

参照規格のアップデート (EN 419 221-5)

1. EN 419 221-5

- 欧州規格(CEN)で定められた、「トラストサービス向け暗号モジュール(HSM)」のための保護プロファイル(PP)。
- eIDAS規則に基づき、リモート署名などで使用される「適格署名作成デバイス(QSCD)」として認められるための要件を定義。

2. EAL4+ (Evaluation Assurance Level 4+)

コモンクライテリア(ISO/IEC 15408)における評価保証レベル。

- **EAL4:** 既存の製品ラインに対して、設計・開発段階からの厳格な検証が行われていることを示す。
- **「+」(Augmented):** 標準のEAL4のパッケージに、追加の保証要件(今回のようなVAN.5など)を意味する。

3. AVA_VAN.5 (Vulnerability Analysis)

「高度な攻撃耐性」を検証する項目です。攻撃者が高度な専門知識やリソース(資金、時間、機材)を持っていると想定し、それに対抗できるかをテストする。HSMのような高いセキュリティが求められる製品では、EAL4にこのVAN.5を組み合わせるのが一般的。

4. ALC_FLC.2 (Flaw Remediation)

「欠陥修正の手順」に関する項目。製品のリリース後に脆弱性や欠陥が見つかった際、ベンダーがそれをどのように追跡し、修正し、ユーザーにパッチを配布するかという「運用プロセス」を保証する。

ALC_FLC.2 のみ削除されている。

CC(コモンクライテリア)のバージョンアップやPPの改訂に伴い、ライフサイクルサポート(ALCクラス)の中
の他の項目(ALC_CMSなど)で十分な管理がカバーされていると判断された場合、FLC.2を独立した「追加要件(+）」として明示しない構成が取られないことも考えられる。