JT2A 活動内容

JT2A activity details

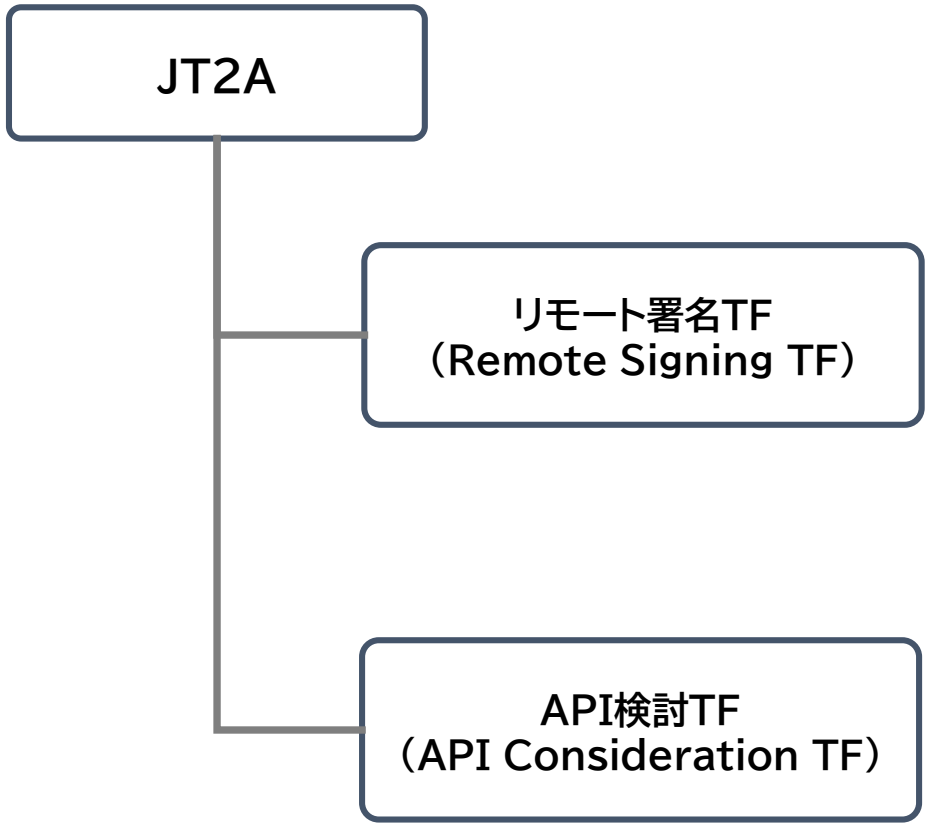
2023.11.15

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
Japan Trust Technology Association (Steering Committee Chairman)
Mitsubishi Research Institute, Ltd.

小川 博久
Hirohisa OGAWA

JT2Aは、2つのTFで検討している

- JT2Aは、リモート署名TFとAPI検討TFで活動
  JT2A works with remote signature TFs and API review TFs



リモート署名ガイドライン、リモートeシールガイドラインの作成・検討

Creation and consideration of remote signature guidelines and remote e-seal guidelines

リモート署名APIの検討、業界標準のCSCへの提案

Consideration of remote signature API and proposal for industry standard CSC*
*Cloud Signature Consortium

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/

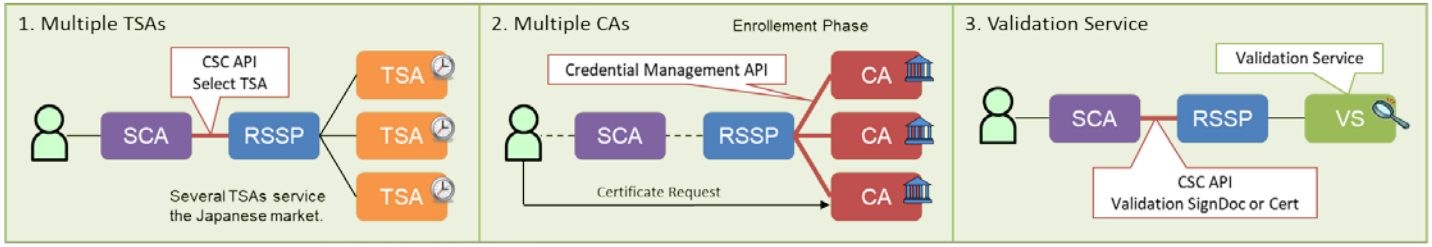
リモート署名APIの検討・提案

- 日本市場では単一RSSPが複数CAおよび複数TSAと連携する必要があるがCSCのAPIではこれらの仕様に対応していない。その為にCSC APIの拡張が必要となるのでAPI TFにて仕様を提案して行く。ベースとなる拡張APIは既に欧州と実証実験にて利用したものを利用している。
  In the Japanese market, a single RSSP needs to work with multiple CAs and multiple TSAs. However, the CSC API does not support these specifications. Therefore, the specification proposal for the extension of CSC API is examined in API TF. The base extension API is already using the one used in Europe and the demonstration.

CSC API Extensions by SIP JAPAN

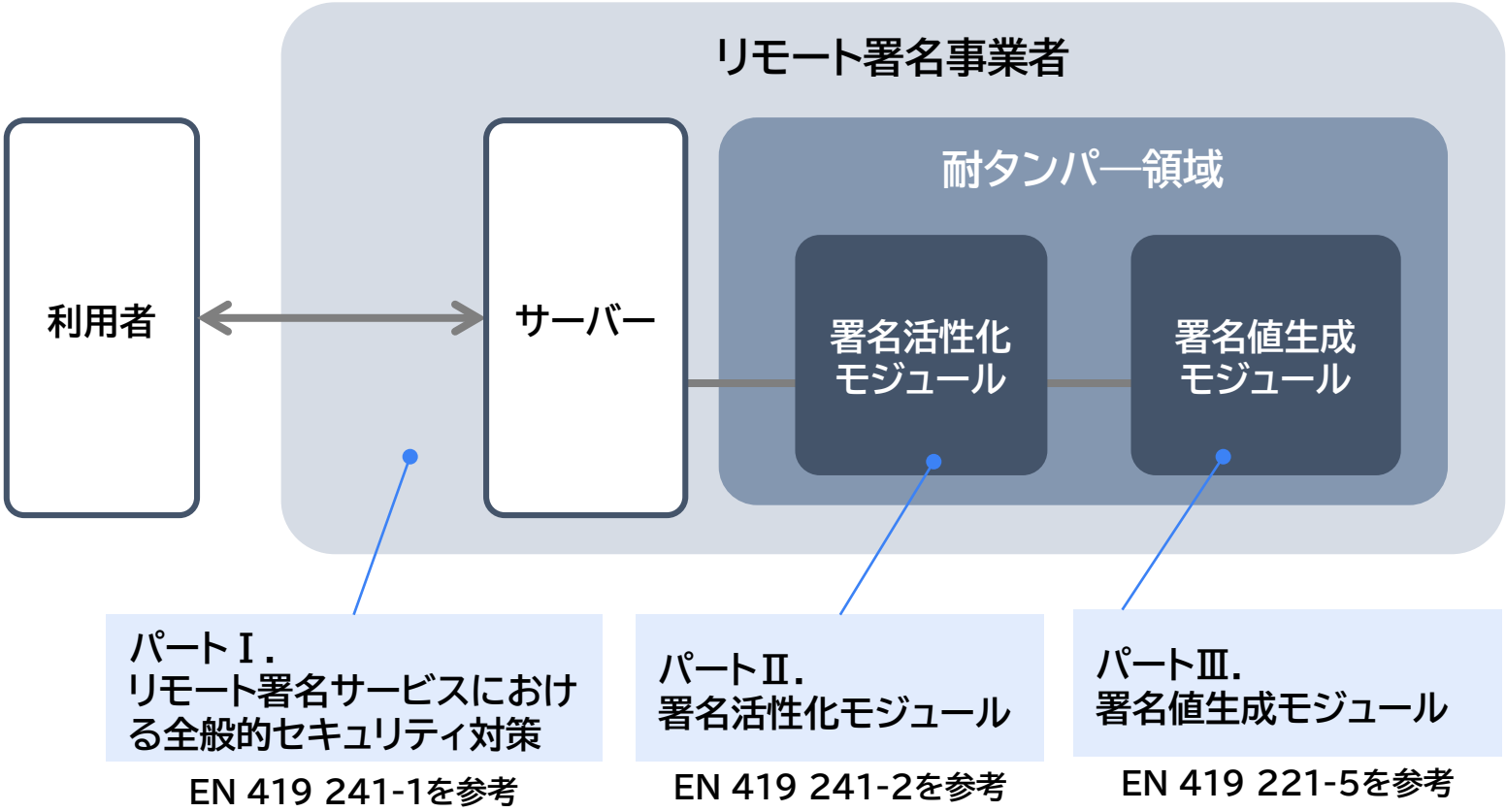
Define extended APIs required for Japanese trust services for CSC APIs.

	Extensions	About	APIs	APIs Overview
1	Multiple TSAs - Select TSA [from SCA to RSSP]	Specify timestampID at timestamp API and get TSAs list and info.	signatures/timestamp timestamps/list timestamps/info	[update] add new parameter 'timestampID' [new] returns the list of TSAs [new] retrieves the TSA info
2	Multiple CAs - Credential Management [from CA/RA to RSSP]	The credential management APIs specifications focus on the interface between RA/CA service and RSSP. Use for enrollment phase.	manages/login manages/generateKey manages/linkEid manages/linkCert manages/authorize manages/deleteKey	[new] obtain an manage access token [new] generate signing key-pair [new] links eID means references [new] links the certificates [new] used for sign a proof of possession [new] destroy signing key
3	Validation Service [from SCA to RSSP]	Validation signature document or certificate.	validates/validSign validates/validCert	[new] validate signed documents [new] validate certificates



リモート署名ガイドラインの発行

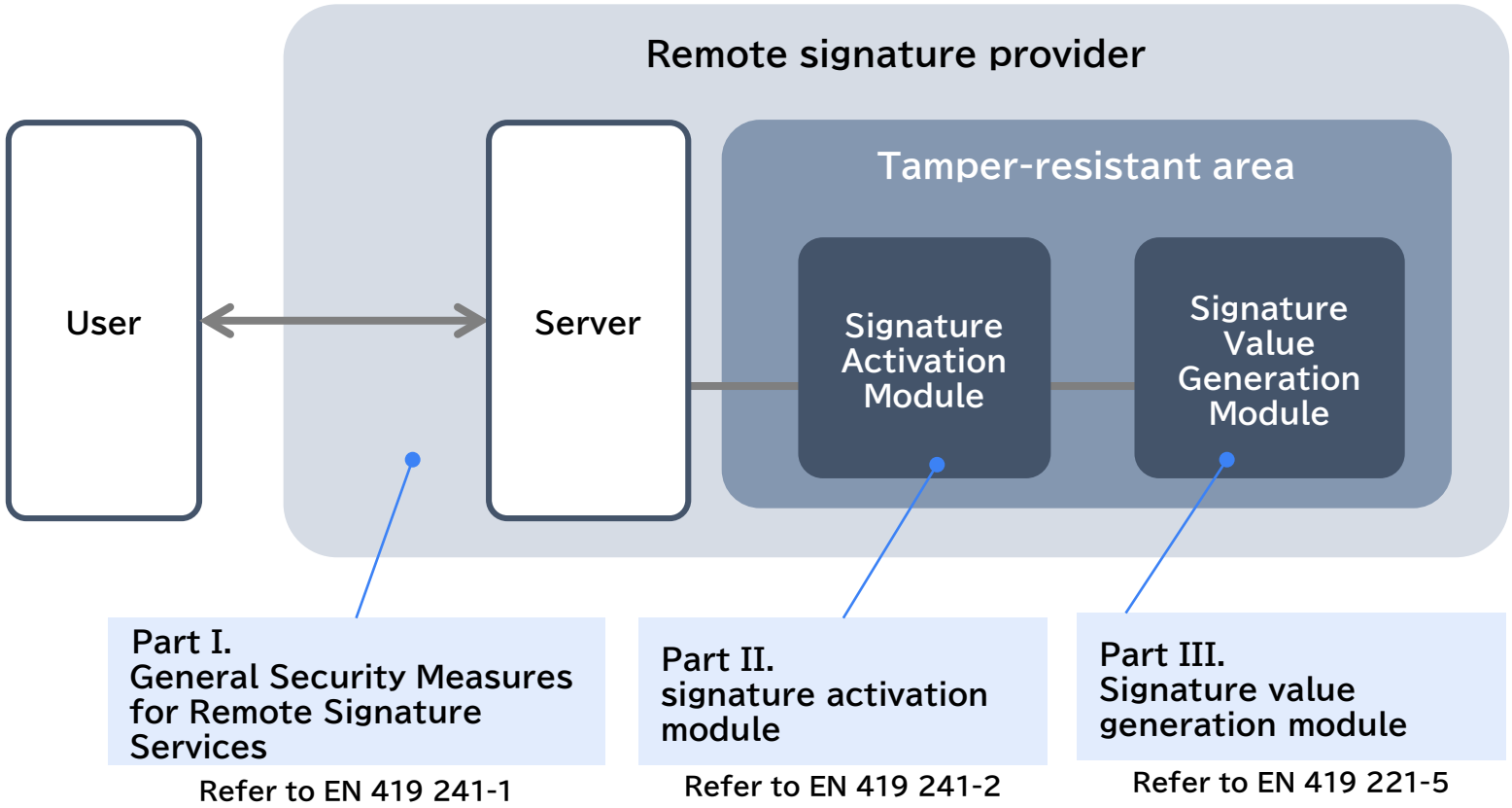
- JT2Aは、2020年に「リモート署名ガイドライン」を発行している。
- リモート署名事業者の「全般的セキュリティ対策」、「署名活性化モジュール」、「署名値生成モジュール」の3部構成。



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/

Publication of Remote Signing Guidelines

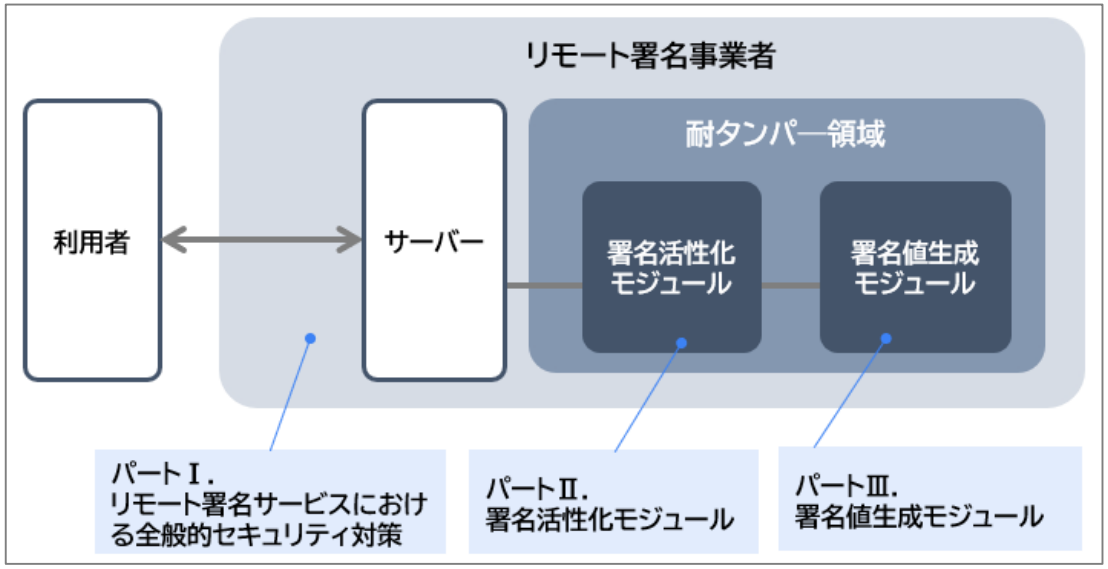
- JT2A issued the ”Remote Signing Guidelines” in 2020.
- It consists of 3 parts: ”general security measures,” ”signature activation module,” and ”signature value generation module” of the remote signature provider.

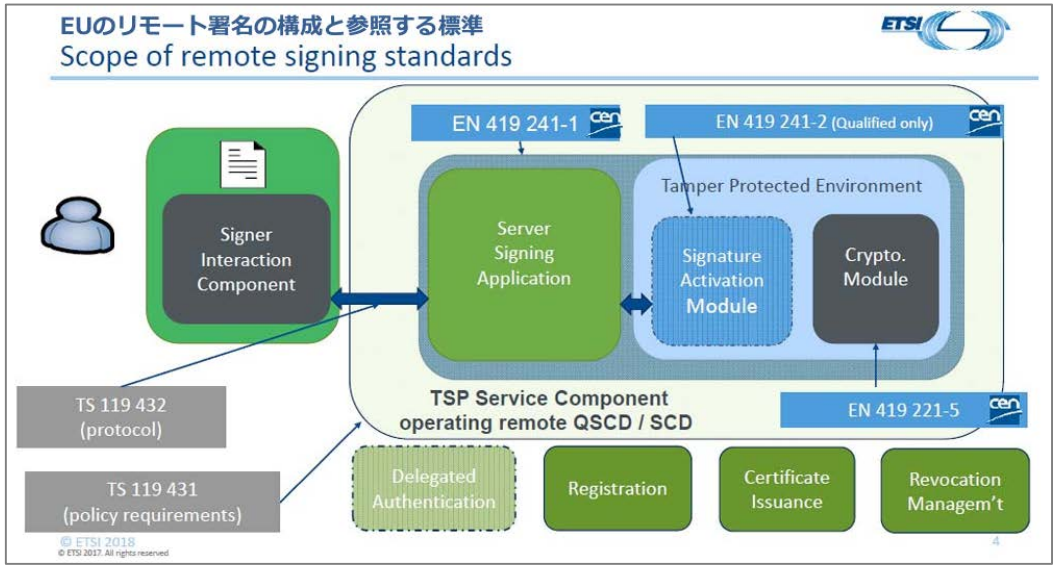


Source: NPO Japan Network Security Association Report and Public Materials Remote Signing Guidelines, Japan Trust Technology Council (JT2A)
https://www.jnsa.org/result/jt2a/2020/

リモート署名ガイドラインの発行

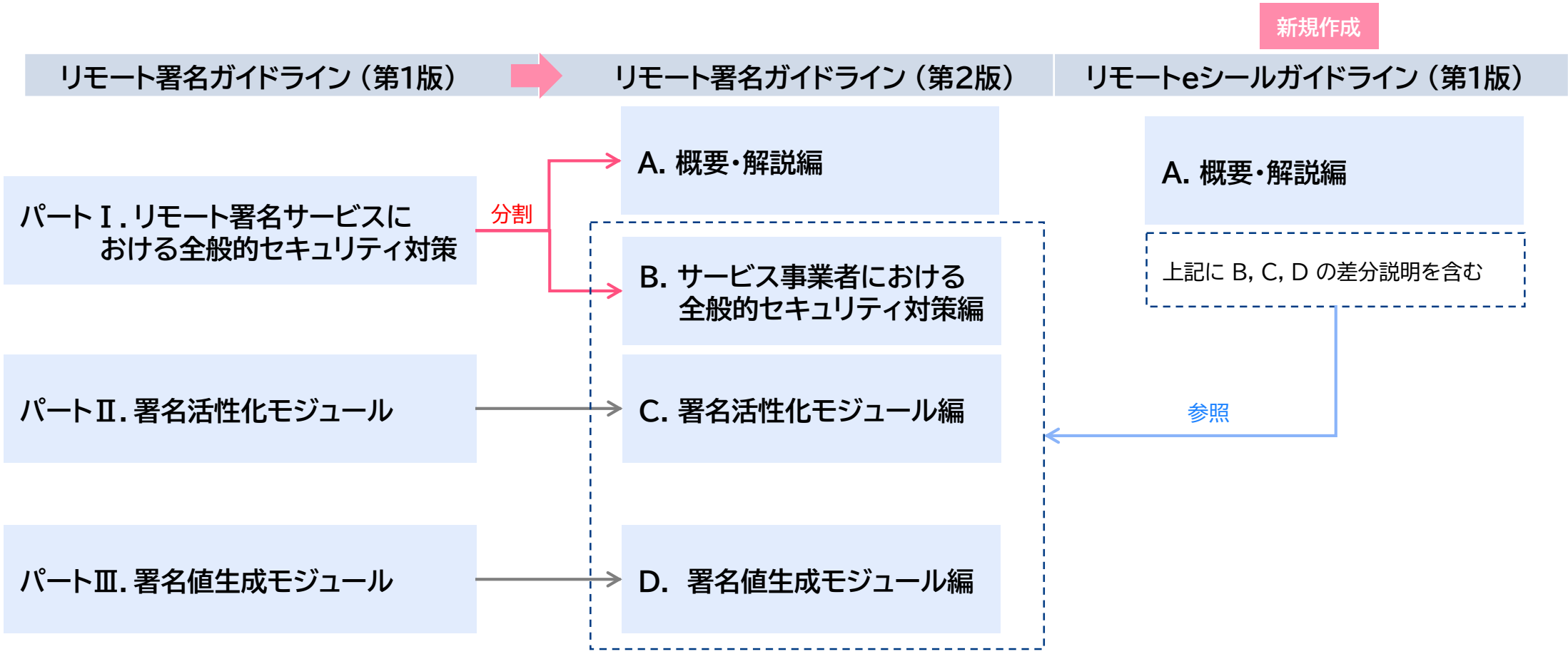
- **参照している規格**
  - EN 419 241-1:Security Requirements for Trustworthy Systems Supporting Server Signing（サーバ署名に関わるセキュリティ要件）
  - EN 419 241-2:Trustworthy Systems Supporting Server Signing -Part 2: Protection profile for QSCD for Server Signing(サーバ署名における適格署名値成デバイスのPP)
  - EN 419 221-5:Protection profiles for Trust Service Providers（TSP）Cryptographic modules -Part 5 - Cryptographic Module for Trust Services -（トラストサービスに対する暗号モジュール(リモート署名を含む)のPP）





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）。



Developing remote e-seal guidelines

- The basic security requirements of the remote e-seal service are (1) general security measures, (2) a signature activation module, and (3) a signature value generation module, similar to those of remote signatures.
- Change the structure of the Remote Signature Guidelines (Part I will be divided) according to the timing of the new issue of the Remote e-seal overview and explanation.