日本のリモート署名の検討

JNSA
電子署名WG サブリーダー
リモート署名TF リーダー

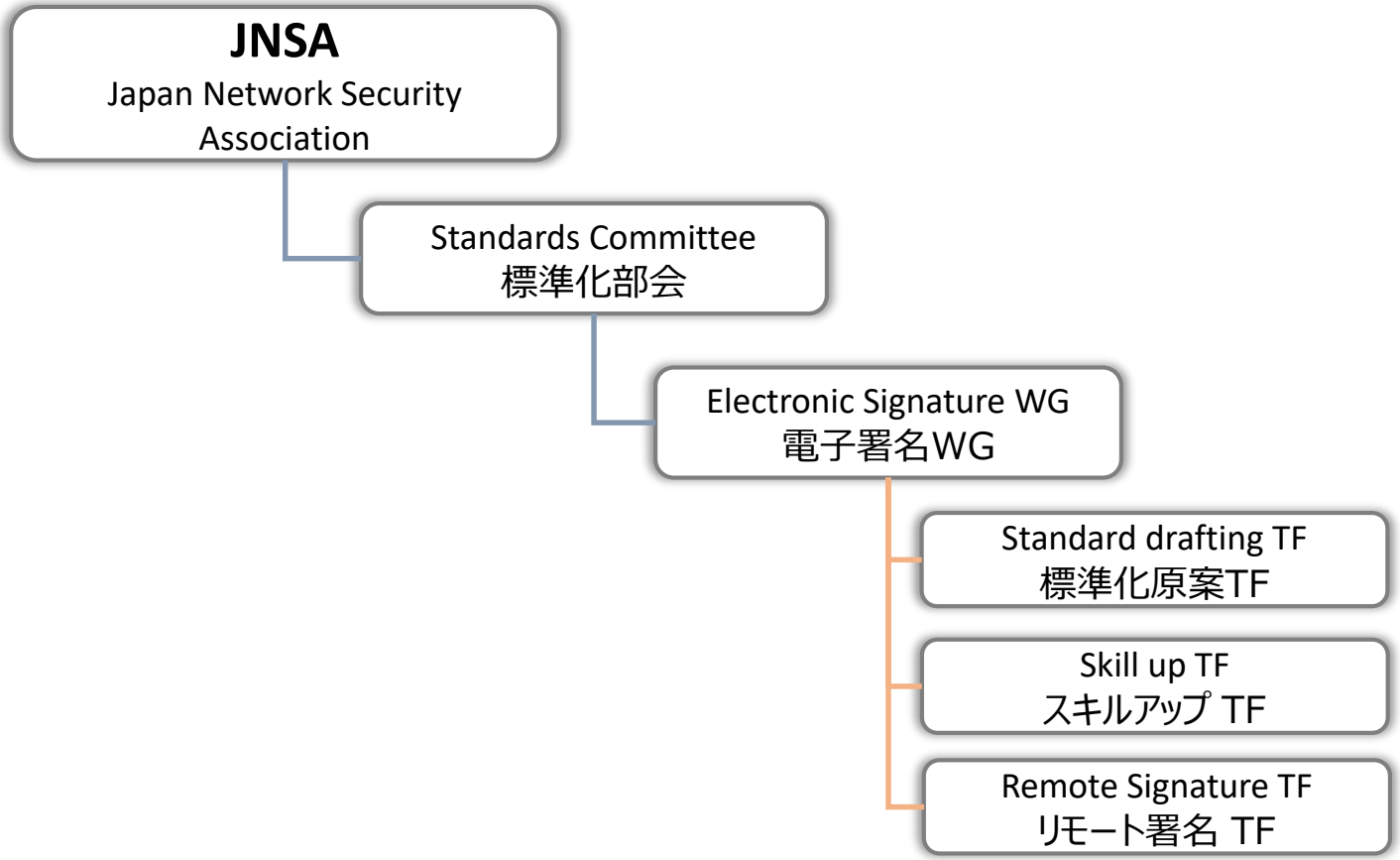
みずほ情報総研
経営・ITコンサルティング部

小川 博久

内容

- JNSAと電子署名WGの概要
- リモート署名TFと経済産業省の事業
- リモート署名の検討

JNSA・電子署名WG・リモート署名TF



電子署名WGの関連団体・組織

ETSI/TC ESI

Associate Member

JNSA
Electronic Signature
Work Group

JAHIS

Technical cooperation
ex) Electronic Prescription

TBF

Partner
ex) Timestamp, Trust List

ISO/TC154

Expert

International Organization for Standardization
ex) PAdES Profile

ISO/TC171

Expert

Document management applications
ex) PDF signature

ISO/SC34
Technical committee

Liaison

Document description and processing languages
ex) Long-term signature of XML

ETSI/TC ESI #42 meetings in Austria

JAHIS : Japanese Association of Healthcare Information Systems Industry
TBF : Time Business Forum in Japan Data Communications Association

経済産業省とJNSAの活動

■国際標準化プロジェクト

- 標準原案作成 TFが実施
  - ISO 14533-3:2017, Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)

■リモート署名プロジェクト

- リモート署名 TFが実施
  - 日本では電子署名法があり、電子署名法研究会ではリモート署名を検討。
  - 2016年の調査では、リモート署名の基本機能とセキュリティ要件を検討。

METI : Ministry of Economy, Trade and Industry

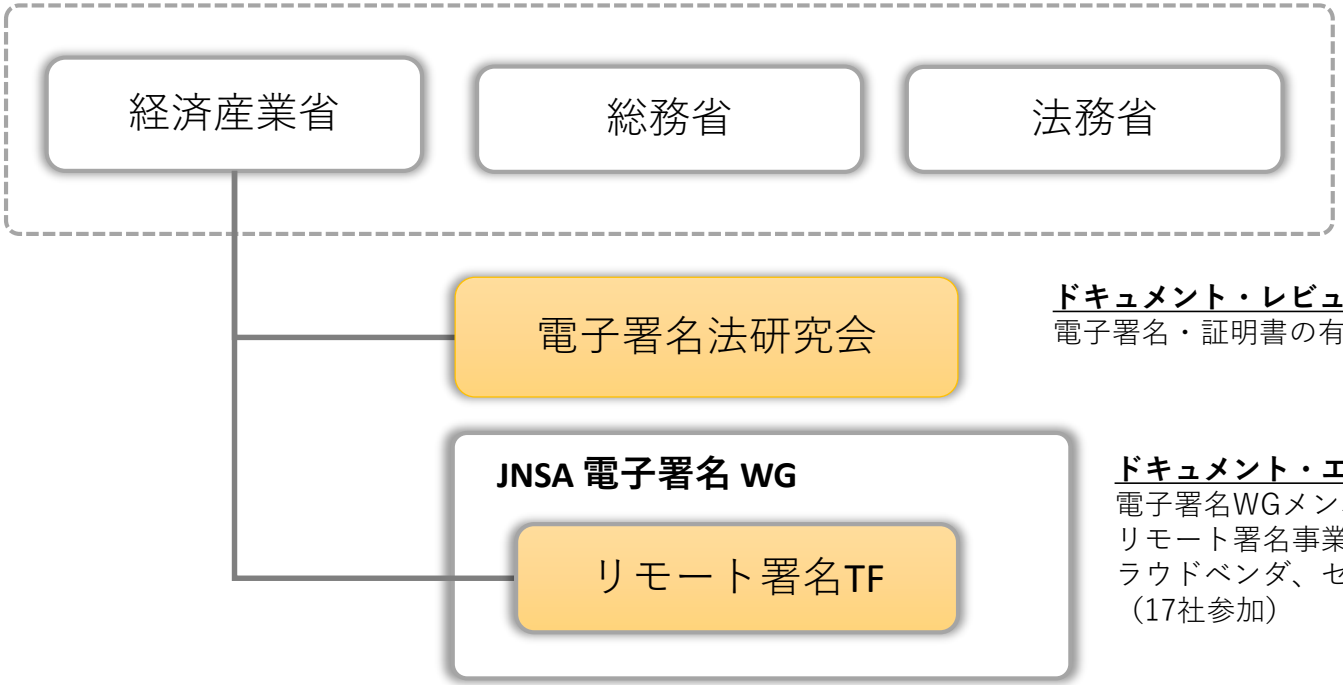
日本の電子署名法

電子署名及び認証業務に関する法律
（平成十二年五月三十一日法律第百二号）
最終改正：平成二六年六月一三日法律第六九号

第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

電子署名法研究会

- 電子署名法に関する研究会を毎年開催。
- 2015年度、2016年度は、リモート署名を検討。
- 2016年度の検討体制（下記）

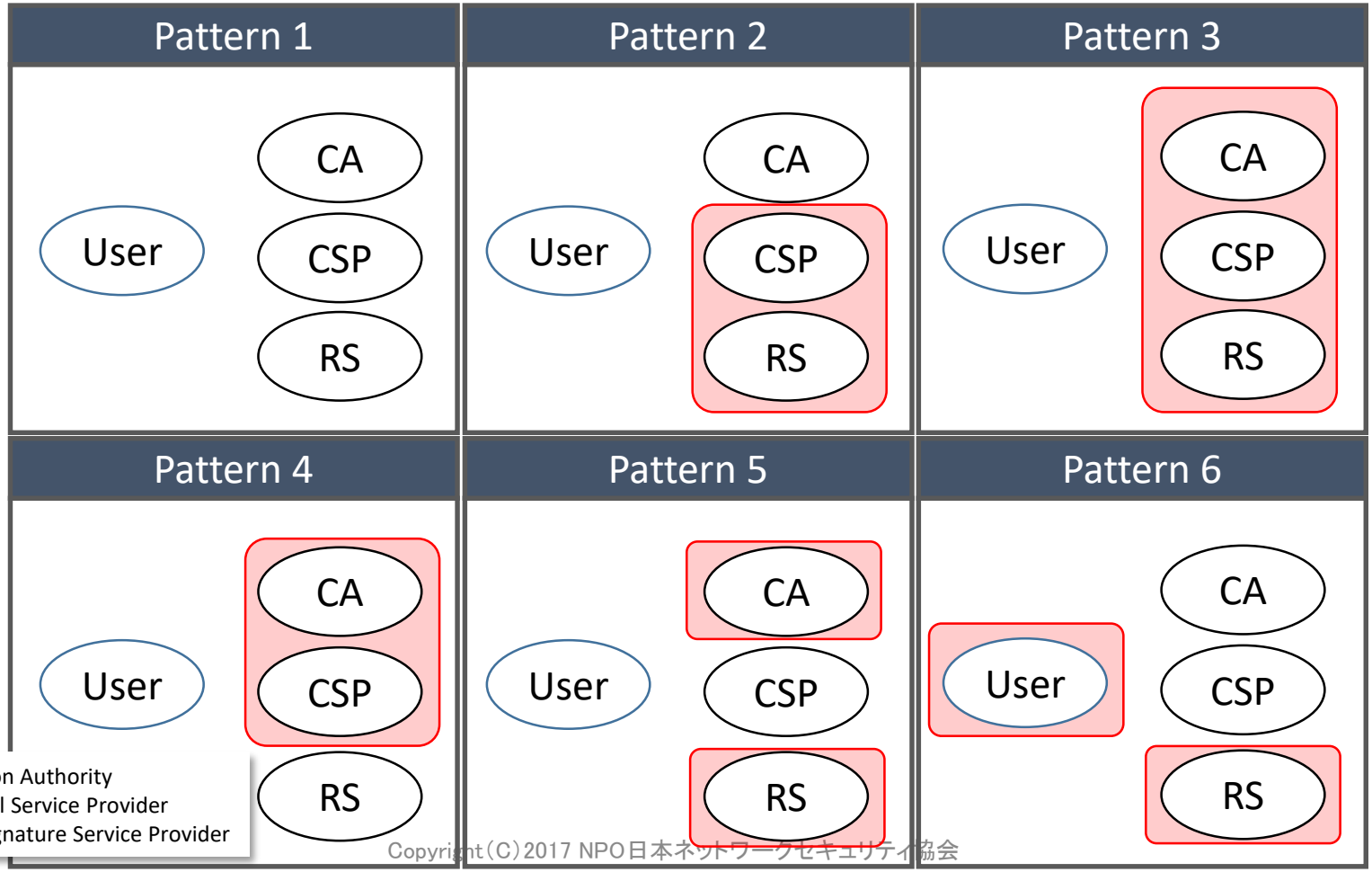


20の検討項目

Ⅰプレイヤ・役割	1	リモート署名のプレイヤ・役割の整理
Ⅱリモート署名・提供者	2	リモート署名提供者の要件・保証レベル
	3	署名の利用用途に応じたレベル
	4	リモート署名の設置環境
	5	リモート署名の構成
Ⅳ登録フェーズ	6	利用者登録方法
	7	利用者の署名鍵の設置（※署名鍵の生成とインポート）
	8	利用者の署名鍵の保護対策 （機能の詳細化）
	9	署名鍵のバックアップ機能
Ⅴ署名フェーズ	10	署名指示の要件
	11	利用者認証方法
	12	利用者情報と署名鍵情報の保護（対策）
	13	署名機能要件
	14	署名付きデータの送信機能
	15	署名生成ログ機能
	16	署名検証機能
	17	利用者による署名対象データの確認
Ⅵその他	18	利用者環境での分散署名処理
	19	長期署名の適用
	20	電子署名法との関連

1. リモート署名のプレイヤと役割

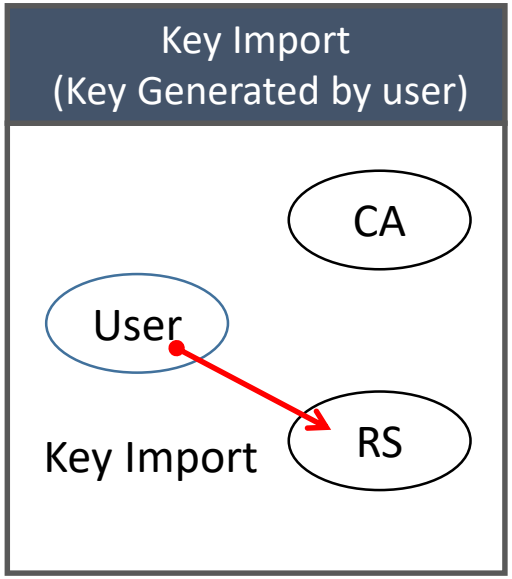
- 想定されるリモート署名の実施パターン（具体例を含む）
- 赤枠が単一のプレイヤを意味する。
- 単一のプレイヤが複数の役割を担うことで、利用者登録情報の共有による効率化が期待でき、利用者はワンストップが可能。一方で、プレイヤのガバナンスが必要になる。

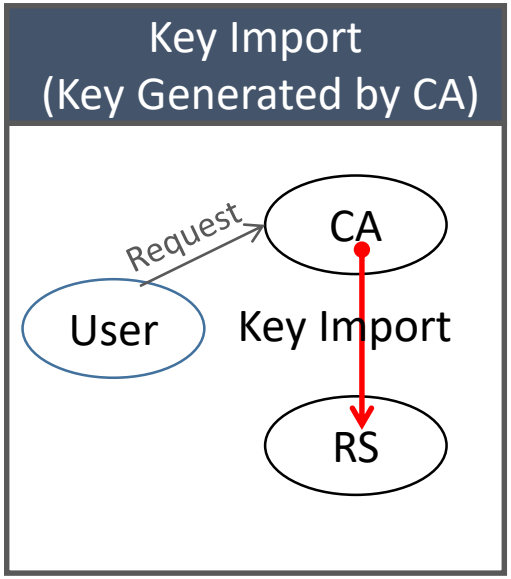


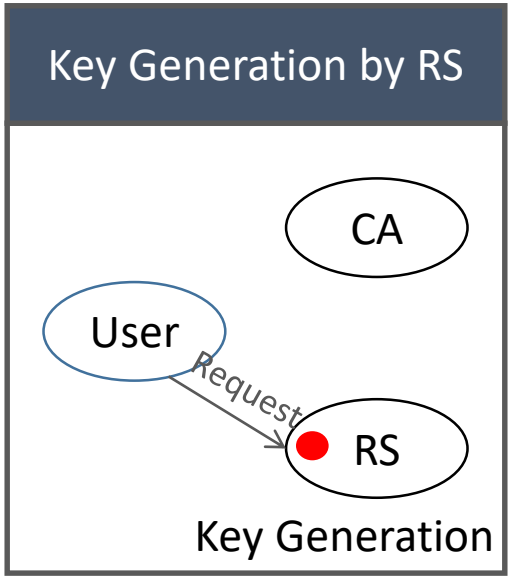
CA : Certification Authority
CSP : Credential Service Provider
RS : Remote Signature Service Provider

7. 署名鍵の設置

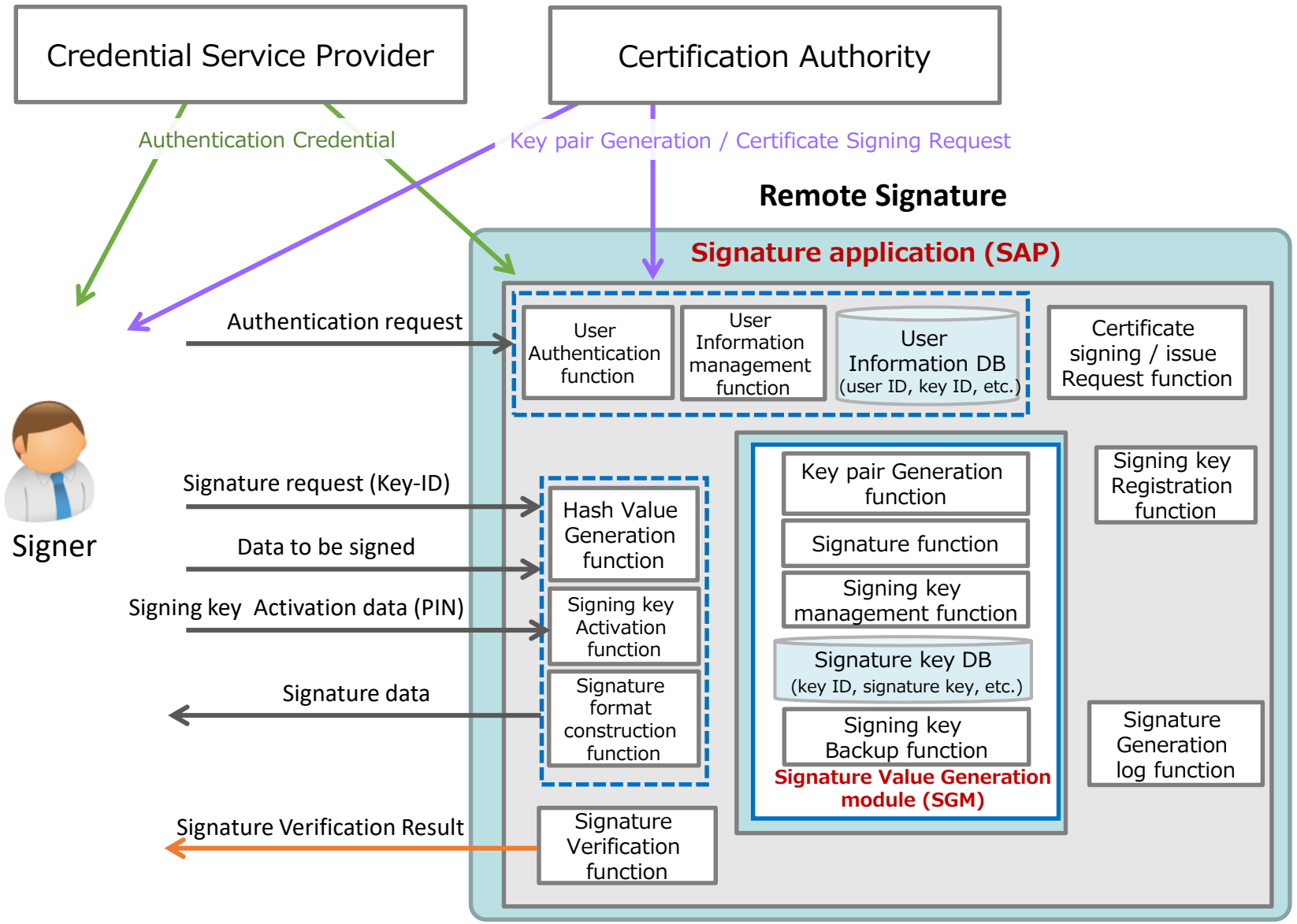
- 想定される署名鍵の設置パターン（具体例を含む）
- 鍵ペア生成は、User／CA／RSが行う。







5. 基本的な機能構成


Credential Service Provider
Certification Authority
Authentication Credential
Key pair Generation / Certificate Signing Request
Remote Signature
Signature application (SAP)
Authentication request
User Authentication function
User Information management function
User Information DB (user ID, key ID, etc.)
Certificate signing / issue Request function
Signer
Signature request (Key-ID)
Hash Value Generation function
Key pair Generation function
Signing key Registration function
Data to be signed
Signature function
Signing key Activation function
Signing key management function
Signing key Activation data (PIN)
Signature key DB (key ID, signature key, etc.)
Signature format construction function
Signing key Backup function
Signature data
Signature Value Generation module (SGM)
Signature Generation log function
Signature Verification function
Signature Verification Result

5. 基本的な機能構成（簡略化）

- SAP : Signature Application
- SGM : Signature value Generation Module

利用者
（署名者）

Signature Application (SAP)

署名鍵登録機能
証明書署名/発行要求機能

利用者認証機能
利用者情報管理機能
利用者情報DB (user ID, key ID, etc.)

Hash値生成機能
署名鍵活性化機能
署名フォーマット構築機能

署名検証機能

署名生成ログ機能

Signature value generation module (SGM)

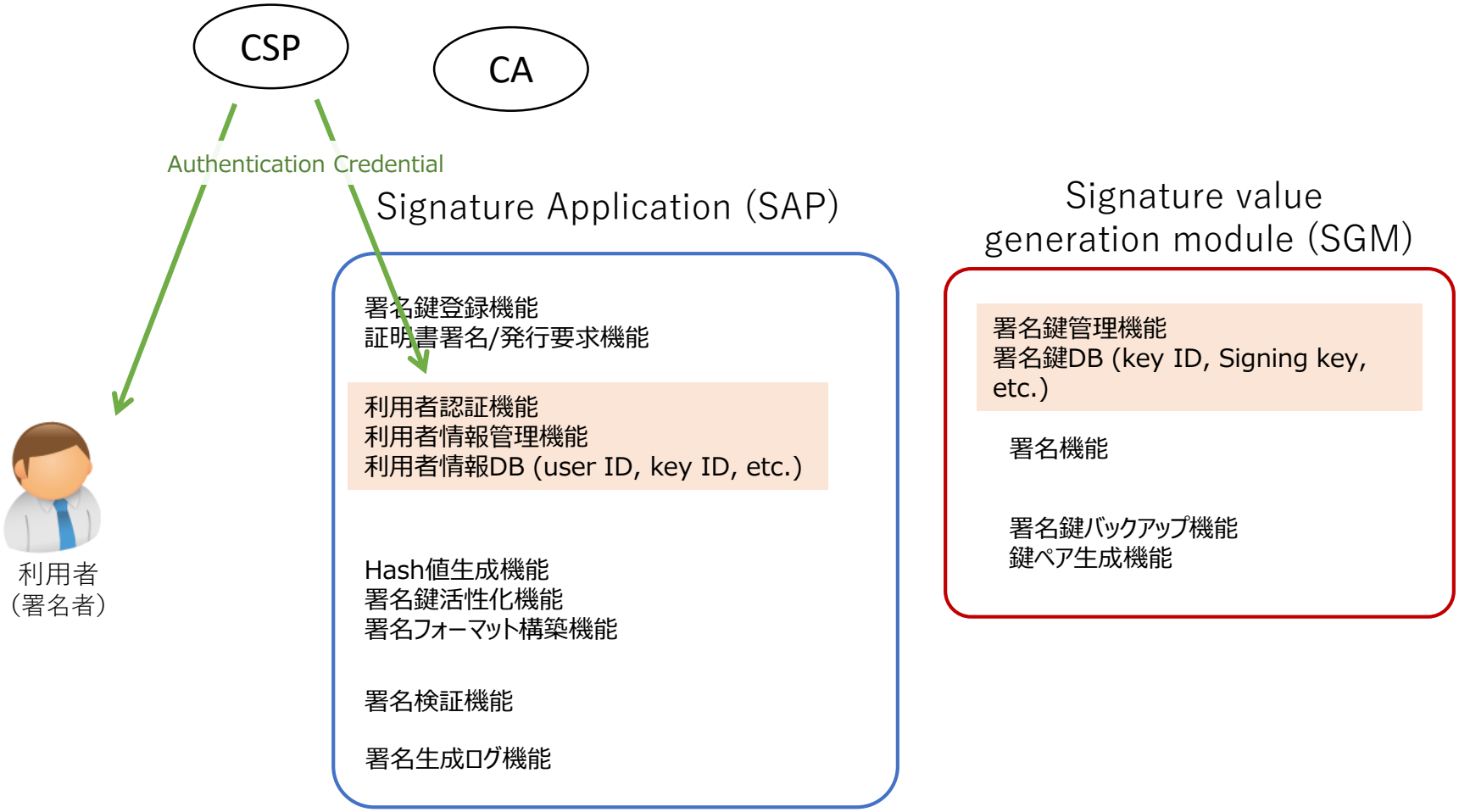
署名鍵管理機能
署名鍵DB (key ID, Signing key, etc.)

署名機能

署名鍵バックアップ機能
鍵ペア生成機能

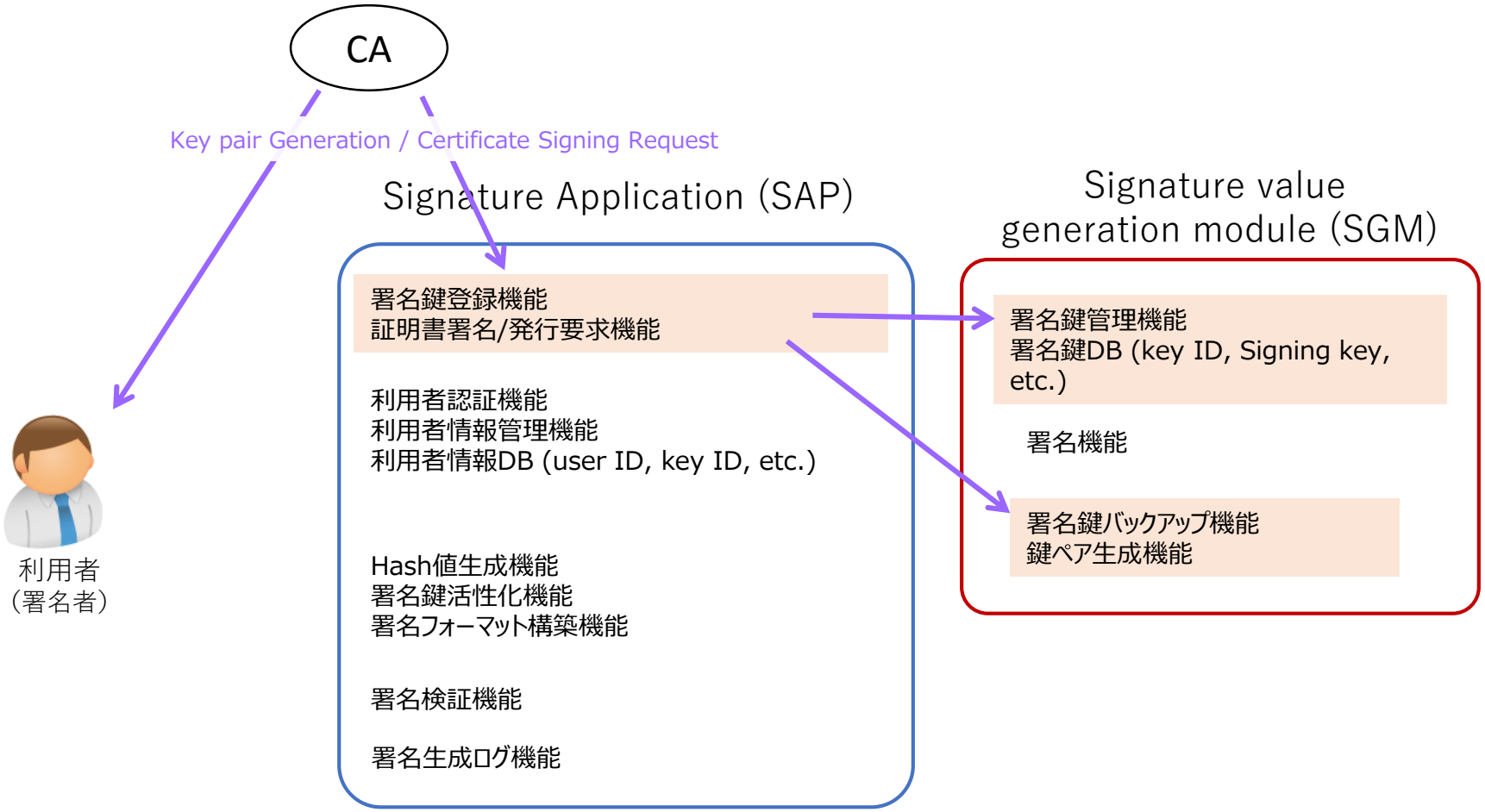
5. 基本的な機能構成

■ 登録フェーズ（認証クレデンシャル）



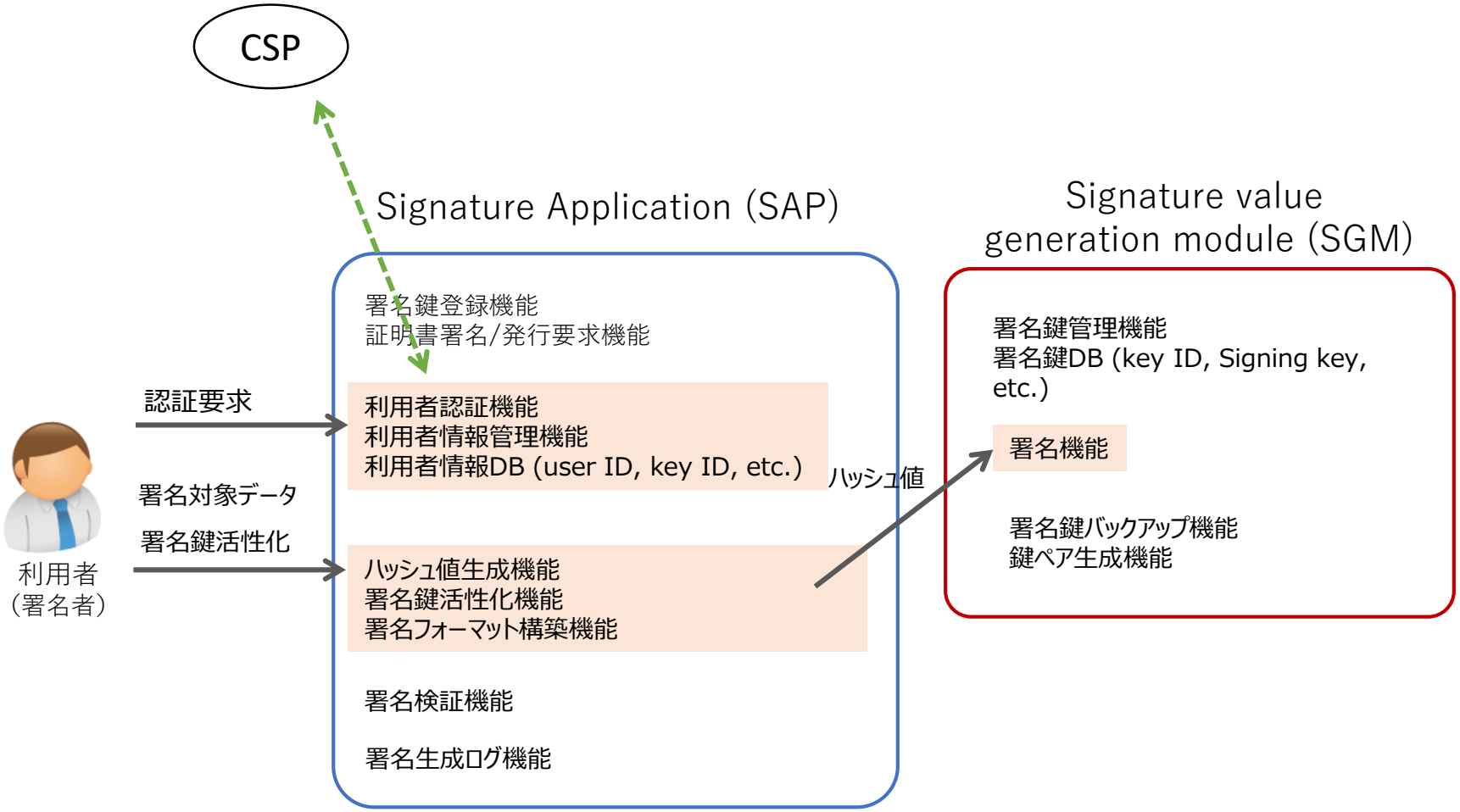
5. 基本的な機能構成

■ 登録フェーズ（署名鍵の生成 or インポート）



5. 基本的な機能構成

■署名フェーズ



5. 基本的な機能構成

■署名結果確認フェーズ

利用者
（署名者）

署名結果

Signature Application (SAP)

署名鍵登録機能
証明書署名/発行要求機能

利用者認証機能
利用者情報管理機能
利用者情報DB (user ID, key ID, etc.)

Hash値生成機能
署名鍵活性化機能
署名フォーマット構築機能

署名検証機能

署名生成ログ機能

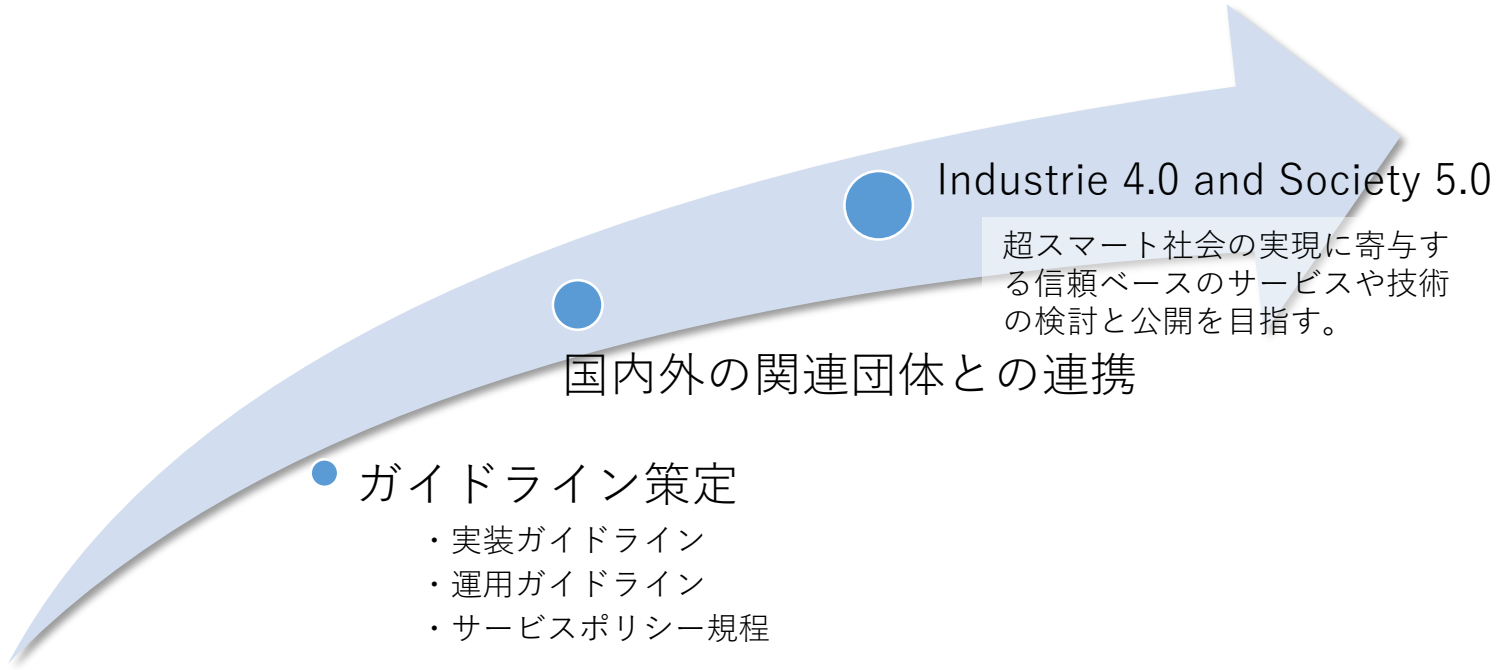
Signature value generation module (SGM)

署名鍵管理機能
署名鍵DB (key ID, Signing key, etc.)

署名機能

署名鍵バックアップ機能
鍵ペア生成機能

今後の活動



コンソーシアムの構築

JTSC
Japan Trusted Signature-service Consortium（仮称）