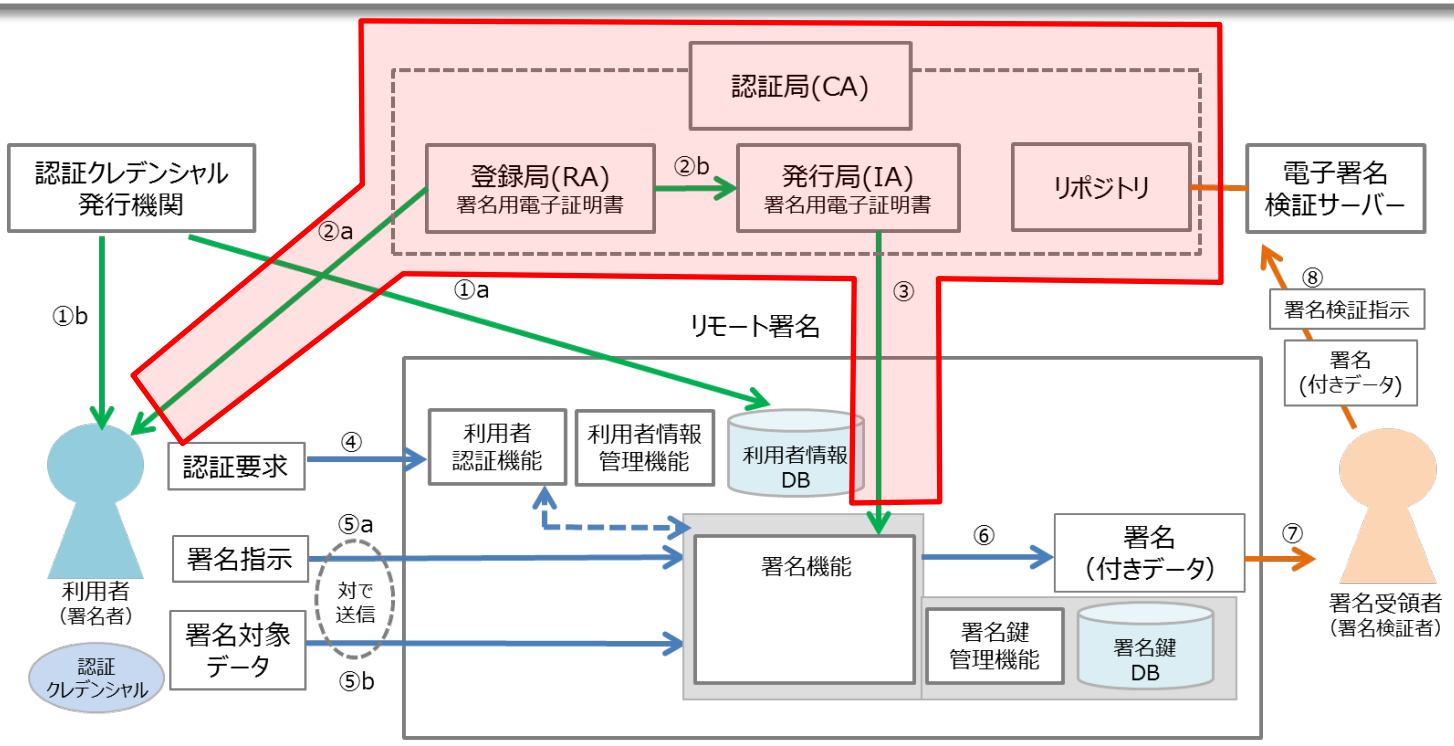
資料４

リモート署名概要と
昨年度の検討結果

1.リモート署名の概要

リモート署名の定義

事業者のサーバに利用者（エンドエンティティ）の署名鍵を設置・保管し、利用者がサーバにリモートでログインし、自らの署名鍵で事業者のサーバ上で電子署名を行うこと。



※上図の赤枠は、特定認証業務の範囲

緑線は登録フェーズに関するもの
青線は署名生成フェーズに関するもの
橙線は署名検証フェーズに関するもの

2.昨年度の検討結果（一覧）

区分	検討項目	昨年度の検討結果概要
Ⅰプレイヤ・役割	1 リモート署名のプレイヤ・役割の整理	昨年は機能の検討に特化した。引き続き調査し検討を要する。
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	同上
	3 署名の利用用途に応じたレベルの検討	同上
	4 リモート署名の構成・設置環境の検討	同上
Ⅲリモート署名を行う際に必要な機能	5 署名機能要件　（機能③）	アルゴリズム及び鍵長等は、CRYPTREC資料を参照。
	6 署名検証機能の有無	必要機能ではあるが、リモート署名の必須機能ではない。
	7 署名鍵のバックアップ機能の有無　（機能⑥）	必須機能として定義（詳細化はしていない状況）
	8 署名生成ログ機能の有無　（機能④）	署名生成に関する一連の処理のログ生成等は必須。
	9 署名付きデータの送信機能の有無	必要機能ではあるが、必須機能ではない。
Ⅳ登録フェーズ	10 利用者登録方法	電子署名・認証ガイドを参照し、レベル3及びレベル4とした。
	11 利用者の署名鍵の設置	現行法制度上、HSMで鍵生成は問題ない。鍵のインポートを認めるかは、引き続き検討を要する。
	12 利用者の署名鍵の保護対策　（機能⑤）	HSMは問題ない。SSMは今後の動向を踏まえて要検討。
Ⅴ署名フェーズ	13 署名指示の要件	指示とDTBSを対でTLSを使用する程度の記述
	14 利用者認証方法　（機能①）	電子署名・認証ガイドを参照し、レベル3及びレベル4とした。
	15 利用者情報と署名鍵情報の保護対策　（機能②）	利用者IDと署名鍵IDの関連付け（紐づけ）のDBの保護→一般的には、アクセス制御を厳重に設定することを求める内容。
Ⅵその他	16 利用者環境での分散署名処理	モバイルは今後の検討材料とする。
	17 利用者による署名対象データの確認	昨年はサーバーの機能の検討に特化した。利用者環境については引き続き調査し検討を要する。
	18 長期署名の適用	長期署名の適用は今後検の検討材料とする。
	19 電子署名法との関連	①利用者の署名鍵の保管状態、②上記1～4に関するガイドライン等は引き続き調査し、検討を要する。

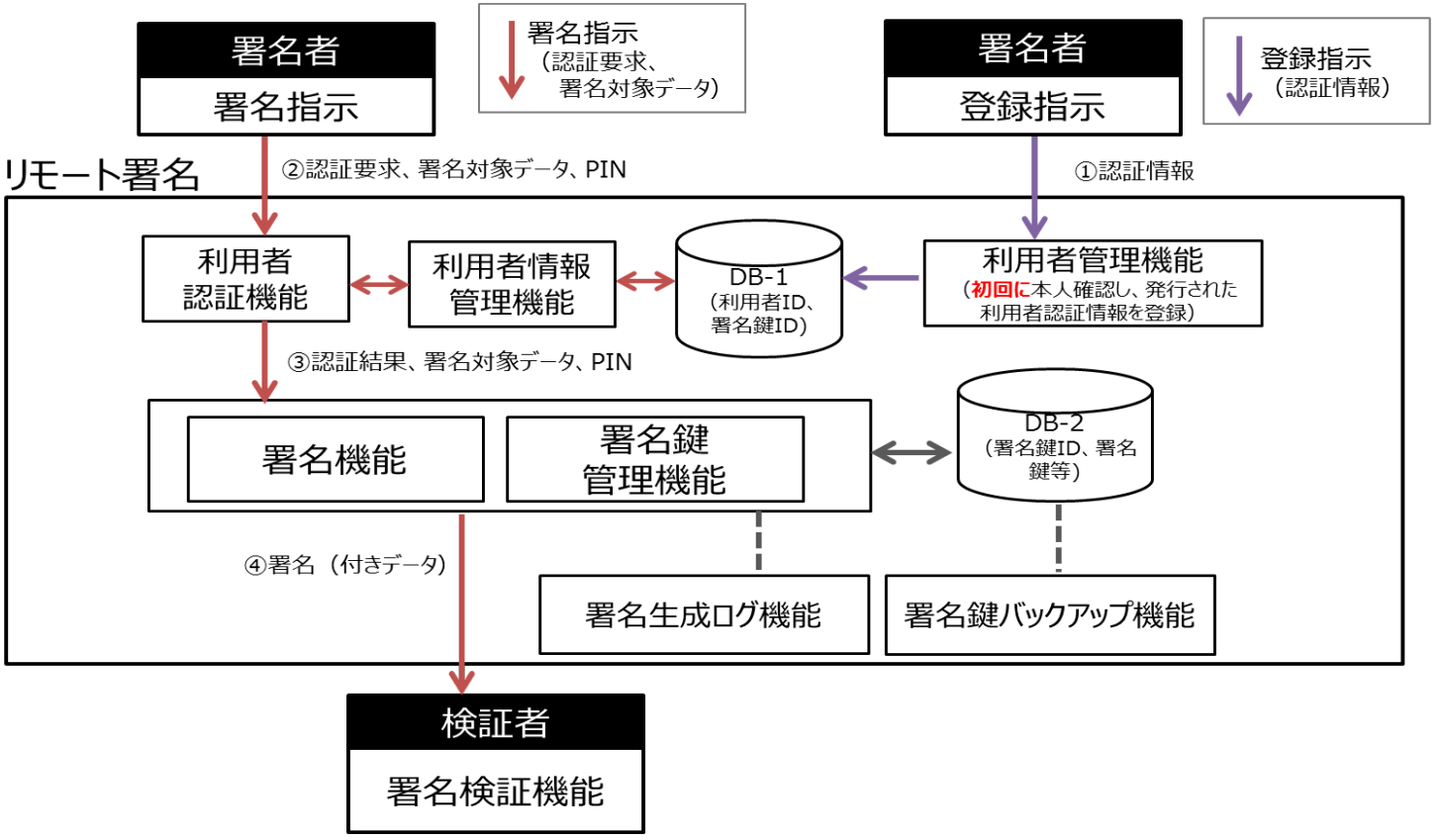
・・・必須ではない機能。　・・・引き続き検討を要する項目。

DTBS：Data to be Signed（署名対象データ）、HSM：Hardware Security Module、SSM：Software Security Module、TLS：Transport Layer Security

参考情報： 昨年度の検討概要（リモート署名の機能）

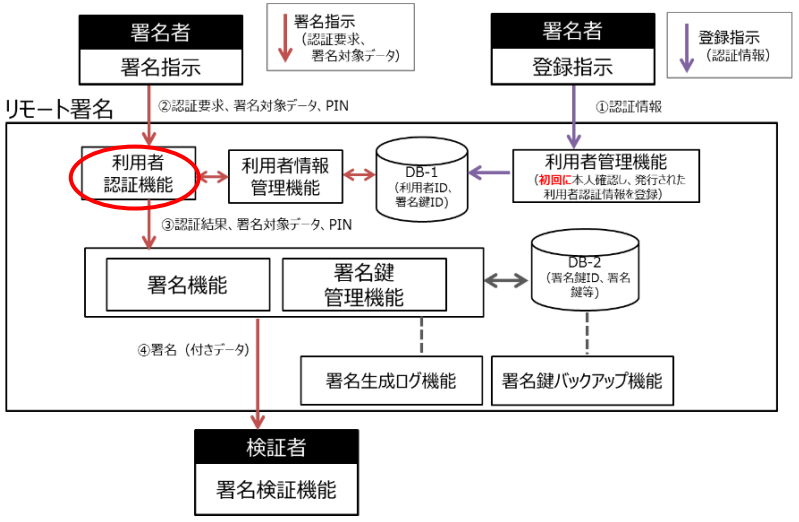
リモート署名の構成

①利用者認証機能、②利用者管理機能、③署名機能、④署名生成ログ機能、⑤署名鍵管理機能、⑥署名鍵バックアップ機能から構成される。



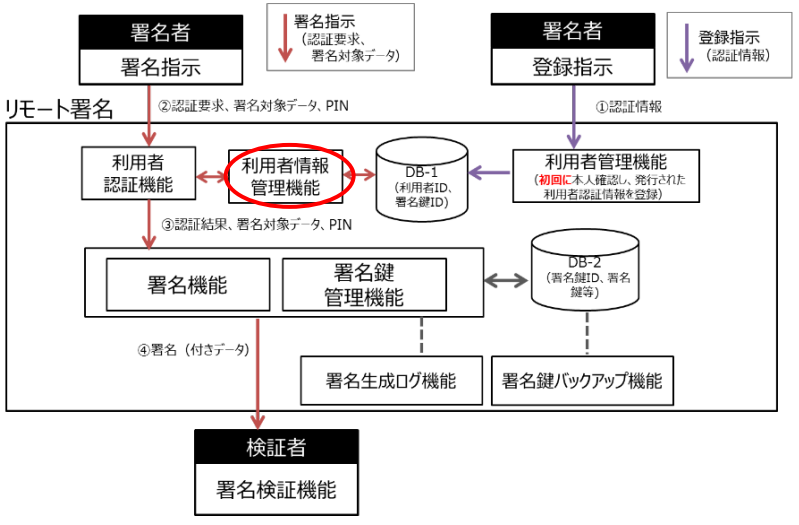
参考情報： 昨年度の検討概要（リモート署名の機能①利用者認証機能）

- 機能
  - 利用者認証機能は、利用者の署名指示を受け、利用者の認証を行う。
- 動作
  - 利用者認証の結果に応じて、利用者IDに対応した「署名鍵ID」、及び利用者から受信した「PINと署名対象データ」を署名機能に送信する。
- 利用者認証プロトコル
  - 認証プロトコルは、オンライン上の推測、リプレイ攻撃、盗聴、セッション・ハイジャック、中間者攻撃、フィッシング／ファーミングについて対策する必要がある。
  - さらに、署名指示と署名対象データは、すり替えによるリプレイアタック等についても対策する必要がある。



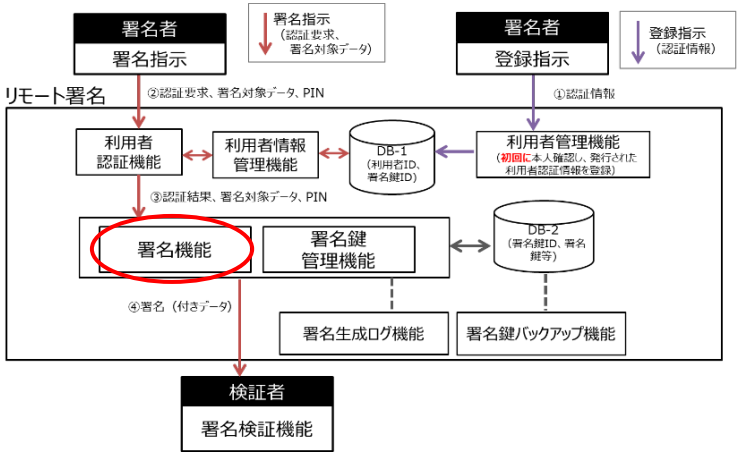
参考情報： 昨年度の検討概要（リモート署名の機能②利用者管理機能）

- 機能
  - 利用者管理機能は、利用者ID等の利用者認証情報と署名鍵IDを管理する。
  - 利用者IDと署名鍵IDを格納しているDB-1を制御する。
  - 認証情報等の管理には、登録、変更、削除、更新/再発行、失効を含む。
- 動作
  - 利用者認証機能の要求に基づき、DB-1に格納した利用者認証情報及び署名鍵IDを利用者認証機能へ送信する。
- 初回の認証情報登録
  - 初回の認証情報登録では、登録指示を受け、利用者本人の確認結果を基に、利用者認証情報と署名鍵IDをDB-1に登録する。



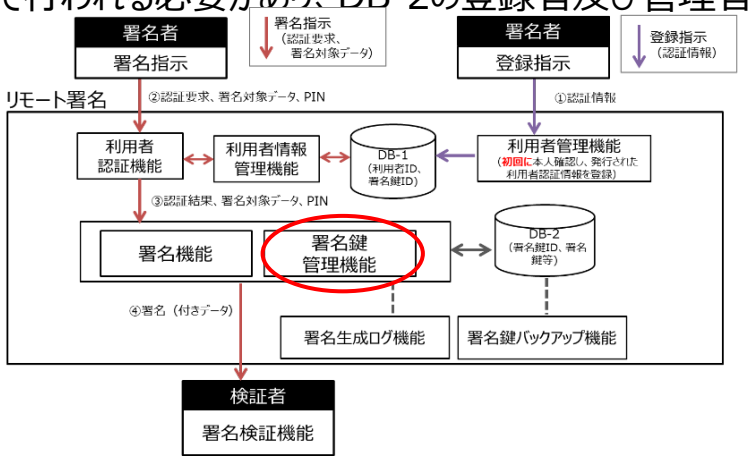
参考情報： 昨年度の検討概要（リモート署名の機能③署名機能）

- 機能
  - 署名機能は、利用者認証機能の認証結果を受け、利用者の署名鍵を用いて署名を行う。
  - 署名鍵をリモート署名サーバ内で生成する場合には、署名鍵の生成及び消去を行う。
  - 署名鍵が暗号化されている場合は、暗号化された署名鍵を復号する。
- 動作
  - 利用者認証機能から受信した「認証結果」及び「署名対象データ」と署名鍵管理機能から受信した「署名鍵」を用いて署名し、署名結果（署名付き署名対象データ）を出力する。
- アルゴリズム・鍵長
  - 署名アルゴリズム及び鍵長は、電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)に記載された安全な署名アルゴリズム及び鍵長のみに限定し、第三者試験・認証制度の認定取得モジュールや製品を利用することが望まれる。



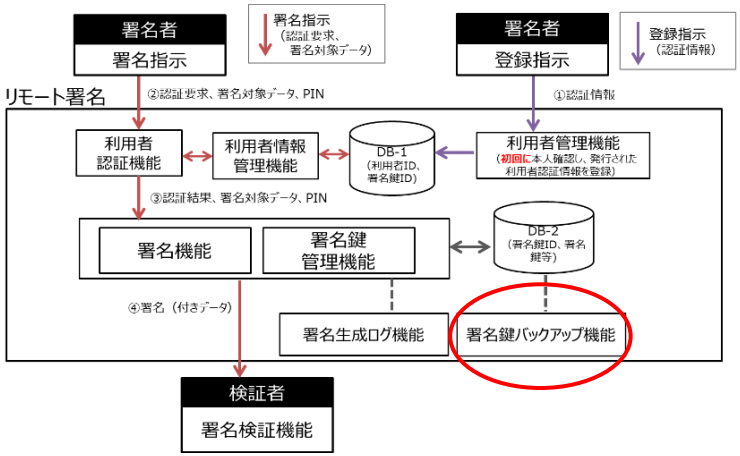
参考情報： 昨年度の検討概要（リモート署名の機能⑤署名鍵管理機能）

- 機能
  - 署名鍵管理機能は、署名鍵IDと署名鍵を管理する。
  - 署名鍵管理機能は、署名鍵IDに対応した署名鍵を格納しているDB-2を制御する。
  - 署名鍵等の管理には、登録、更新/再発行、失効を含む。
- 動作
  - 署名機能の要求に応じて、署名鍵IDに対応した署名鍵を署名機能に送信する。（署名鍵は暗号化された署名鍵の場合もある）
- 初回の署名鍵登録
  - 初回の署名鍵登録では、登録指示を受け、利用者本人の確認結果を基に、署名鍵IDと対応した署名鍵を登録する。（送信された署名鍵を登録する場合と生成した署名鍵を登録する場合がある）
- DB-2（利用者ごとの「署名鍵ID」と「署名鍵」の対を格納するデータベース）
  - 利用者の署名鍵IDの関連付け情報を格納しているDB-2は保護する必要があり、アクセスを限定する必要がある。
  - DB-2へのアクセスは必ず署名鍵管理機能を介して行われる必要があり、DB-2の登録者及び管理者に限定される。



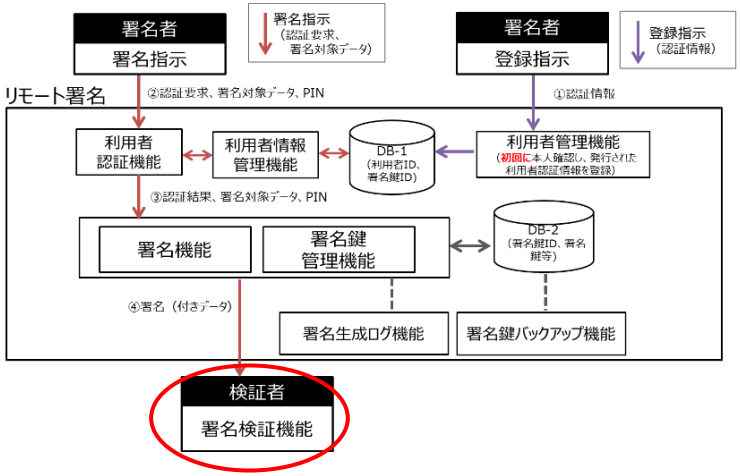
参考情報： 昨年度の検討概要（リモート署名の機能⑥署名鍵バックアップ機能）

- 機能
  - 署名鍵バックアップ機能は、署名鍵のバックアップを行う。
- バックアップ対象
  - バックアップする署名鍵は、暗号化するなどの対策を施し、署名者（利用者）以外が利用できない状態でバックアップする必要がある。
- 留意事項
  - なお、バックアップ期間や具体的な方式及び運用上の対策については、利用目的や取扱う情報の重要度に応じて別途検討する必要がある。



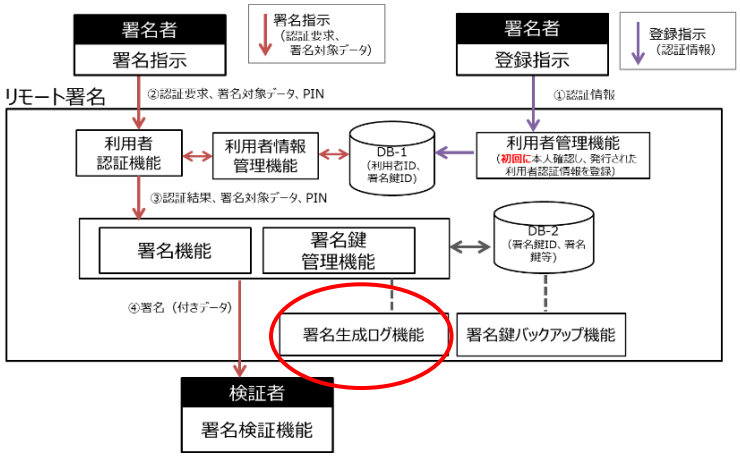
参考情報： 昨年度の検討概要（リモート署名の機能→×署名検証機能）

- 機能
  - 署名検証機能は、署名付き署名対象データと署名検証鍵を基に署名検証し、検証結果を出力する。
- なお、リモート署名で得られた電子署名は、改ざん検知や否認防止のために署名検証を行う必要がある。一方で、署名検証は、署名者の環境で検証する場合や他のサーバや署名検証サーバ等で行うことも想定され、リモート署名に必須機能とは言い難い。
  そのため、リモート署名の構成として必須の機能ではない。



参考情報： 昨年度の検討概要（リモート署名の機能④署名生成ログ機能）

- 機能
  - 署名生成ログ機能は、署名生成処理に関する一連の処理のログを出力する。署名生成ログは、改ざんされたことを検知できる必要がある。
- 留意事項
  - なお、ログを生成する具体的な内容やログの保存期間及び改ざん検知の技術的な方式、運用上の対策については、利用目的や取扱う情報の重要度に応じて別途検討する必要がある。



参考情報： 昨年度の検討概要（リモート署名の運用・管理に関する配慮事項）

- 昨年度の報告書8章では、リモート署名で必要となる機能を示したものであり、リモート署名提供者の以下の検討は、対象外である。

  ①提供者の人的・組織的な管理
  ②サーバの構成
  ③サーバの設置環境
  ④物理的な対策

- 上記等の運用面や管理面については、リモート署名の利用目的や取扱う情報の重要度に応じて別途検討する必要がある。