健康で豊かな国民生活を保健医療福祉情報システムが支えます

電子処方箋署名共通モジュール仕様案について

2022年6月23日
2022年9月5日修正
JAHIS　セキュリティ委員会　HPKI電子署名規格作成WG

電子処方箋　署名共通モジュールの要件

- 参照すべき文書
  - 電子処方箋管理サービス記録条件仕様（処方編）
  - 電子処方箋管理サービス記録条件仕様（調剤編）
  - JAHIS標準 ID 18-006「JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格Ver.2.0」
- XAdESフォーマットのバージョンはISO 14533-2:2021で、XML名前空間は下記
  - https://www.iso.org/standard/79129.html
- ハッシュアルゴリズムはCRYPTREC暗号リストの電子政府推奨暗号リストに準ずる
  - 署名アルゴリズムは、rsa-sha256
  - ハッシュアルゴリズムは、SHA-256
- データの正規化方式は、Exclusive XML Canonicalization1.0のコメントなし版
- 本仕様に基づく署名以外の署名を付与してはならない
- 本仕様に基づく署名を複数付与してはならない
- 長期署名に対する要素は別表に示す。

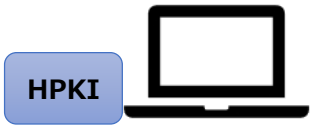
電子処方箋　署名共通モジュールの要件

＜対象システム構成例＞

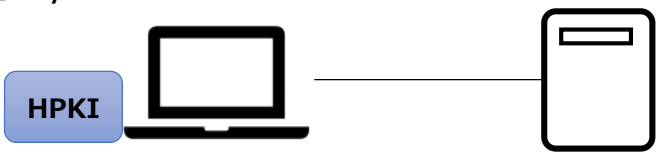
形態	OS	言語
①スタンドアロン	Windows	DLL/Java
②C/Sシステム	Windows（サーバ：Windows/Linux）	DLL/Java
③WEBシステム	Windows（サーバ：Windows/Linux）	DLL/Java/Js

- DLLのシステム動作環境について、より多くの環境で幅広くサポートが必要
- 動作環境を明確化する必要がある

①スタンドアロンアプリ（クライアントで処理が完結するもの）



②C/Sシステム（サーバー側でも処理がなされるもの）

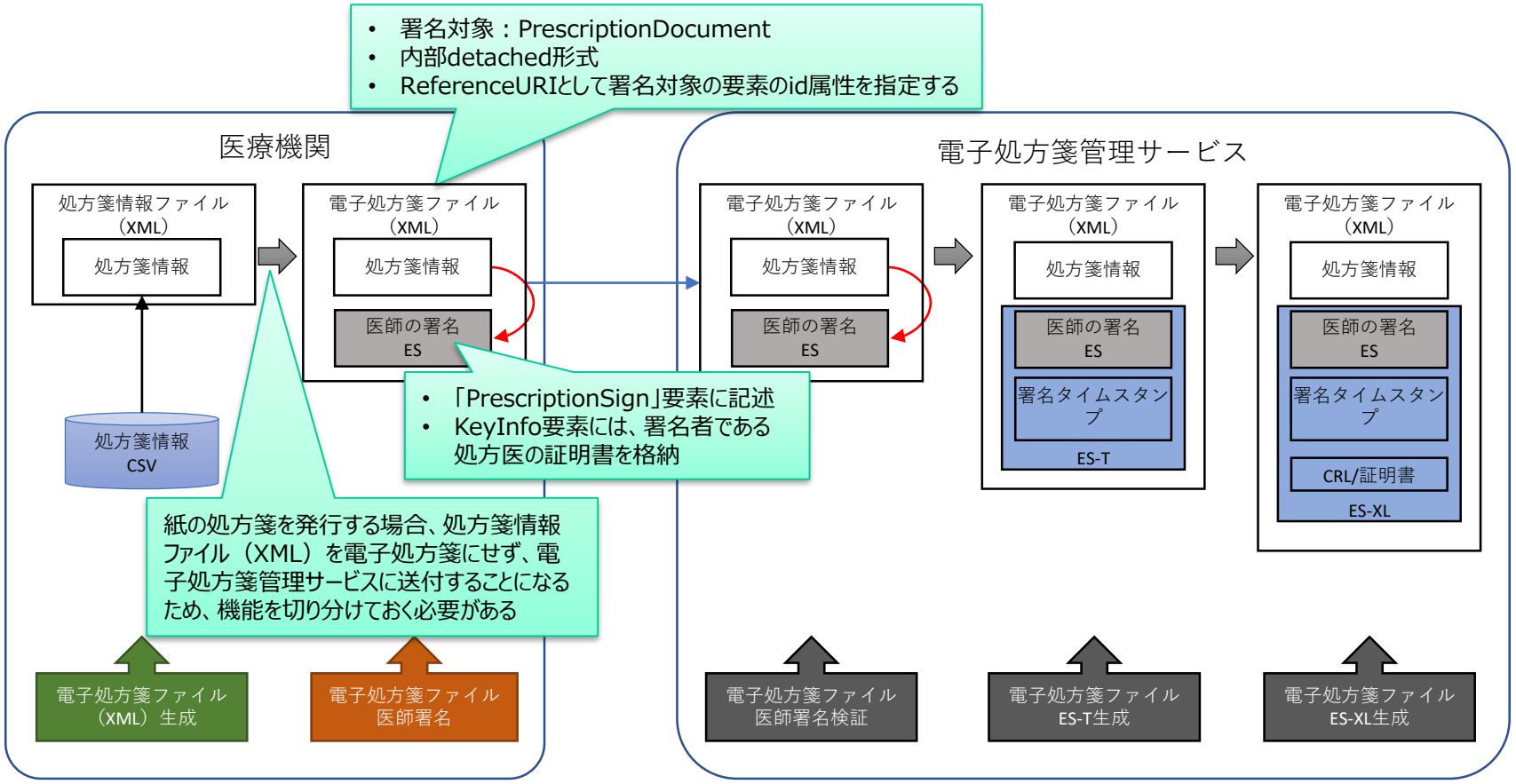


③WEBシステム

ブラウザはChromium（Chrome、Edge）を想定

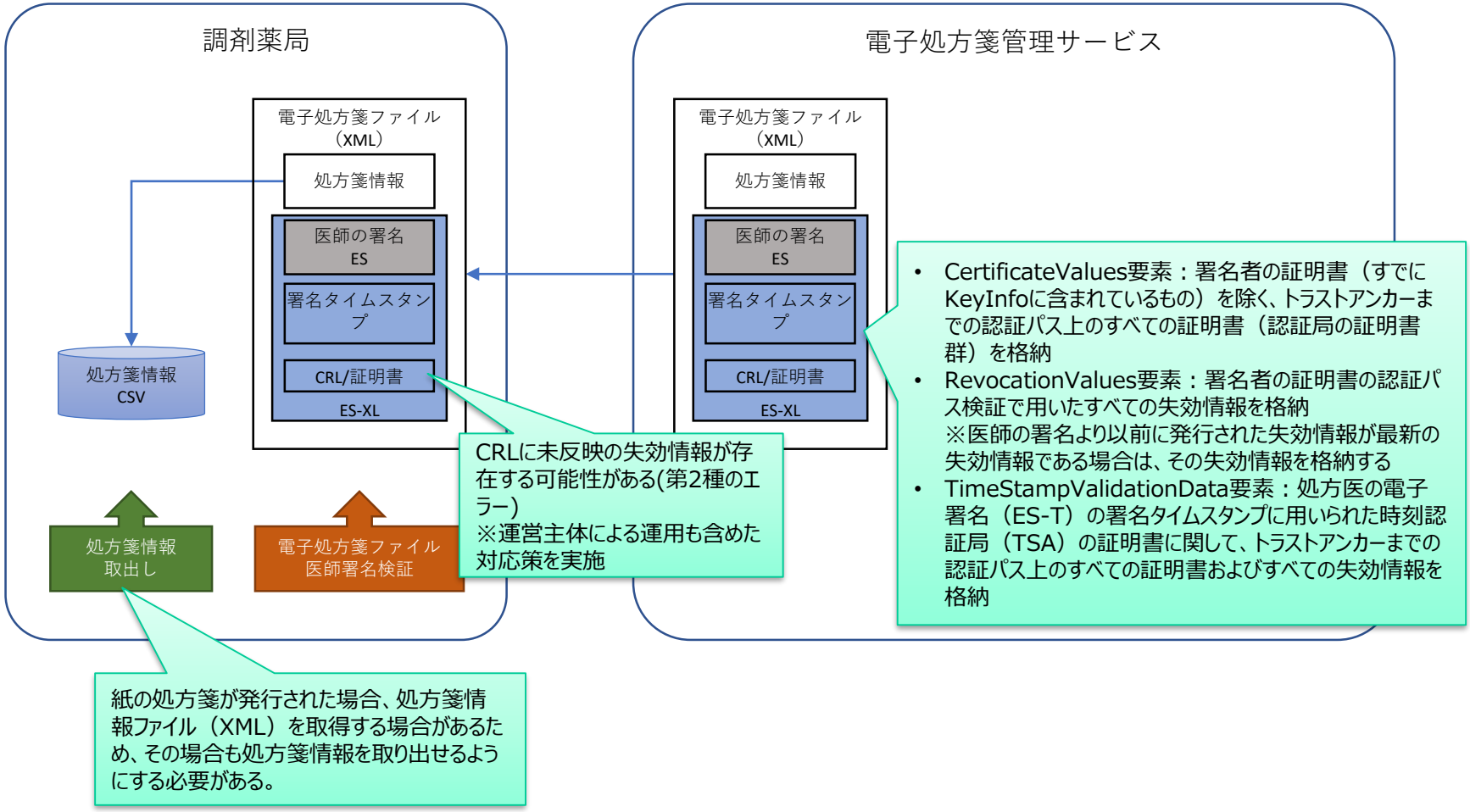
データ処理の流れ

（１）電子処方箋ファイルの発行



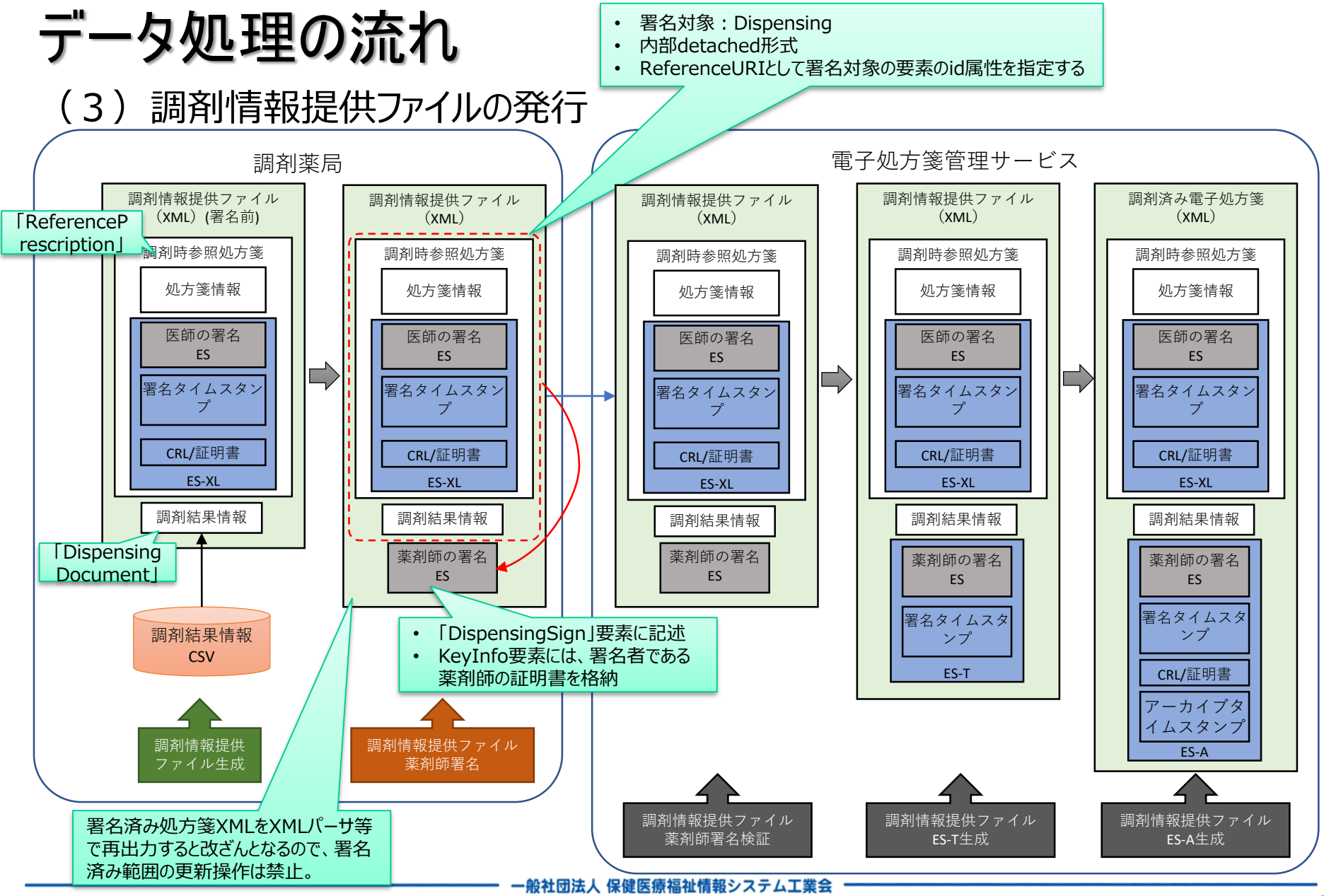
データ処理の流れ

（２）電子処方箋ファイルの受領



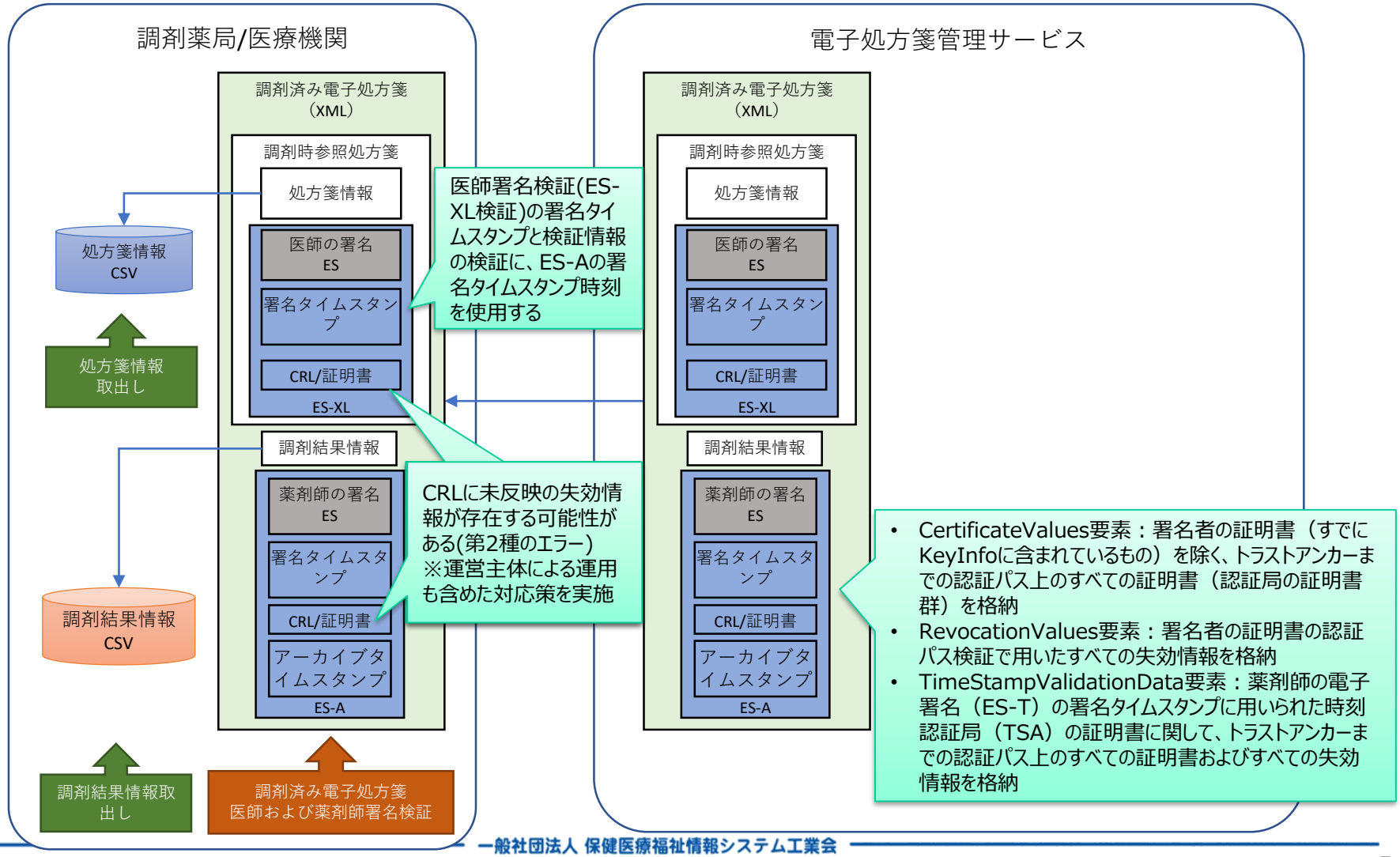
データ処理の流れ

（３）調剤情報提供ファイルの発行



データ処理の流れ

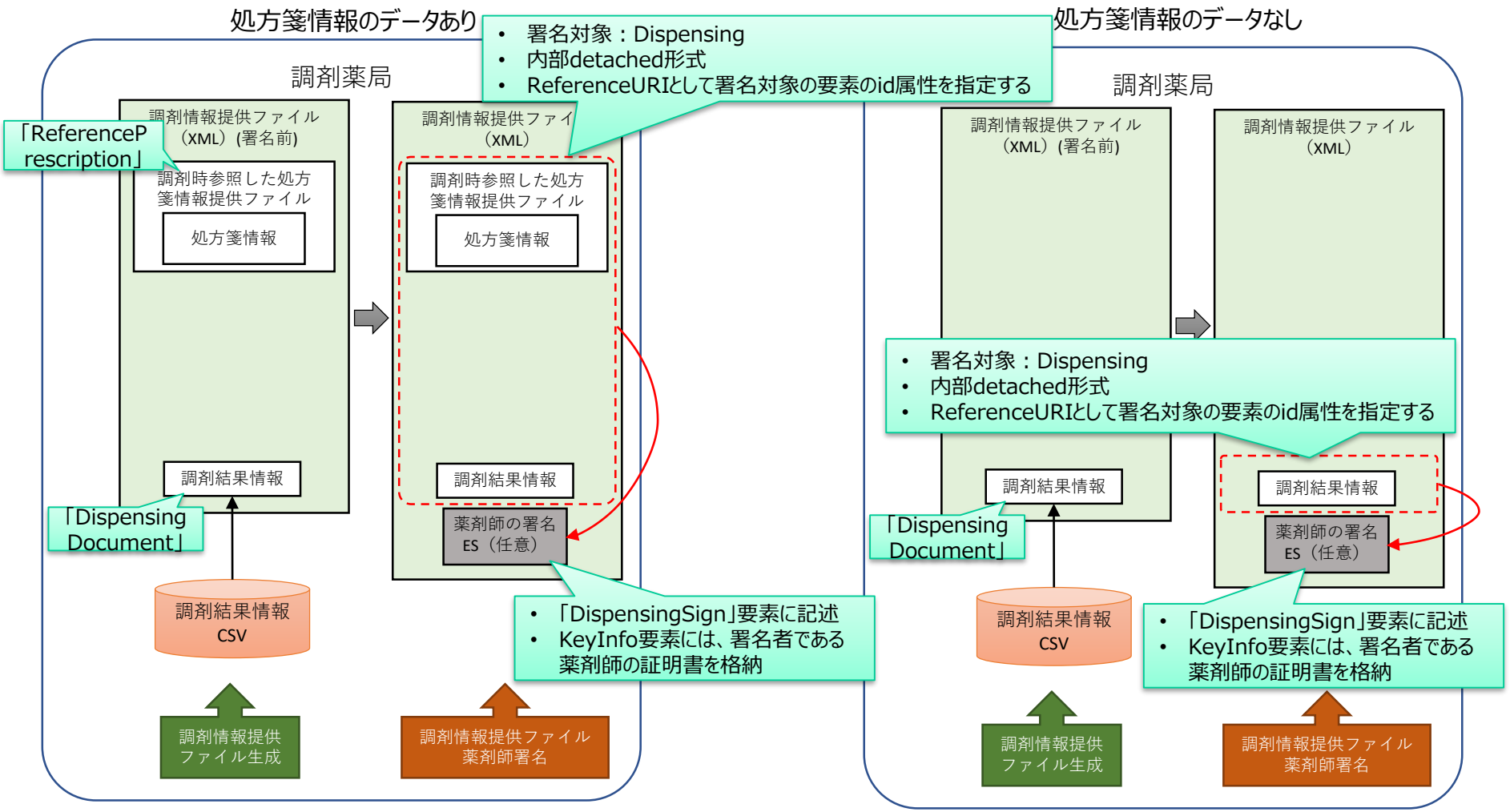
（４）調剤済み電子処方箋の受領



データ処理の流れ

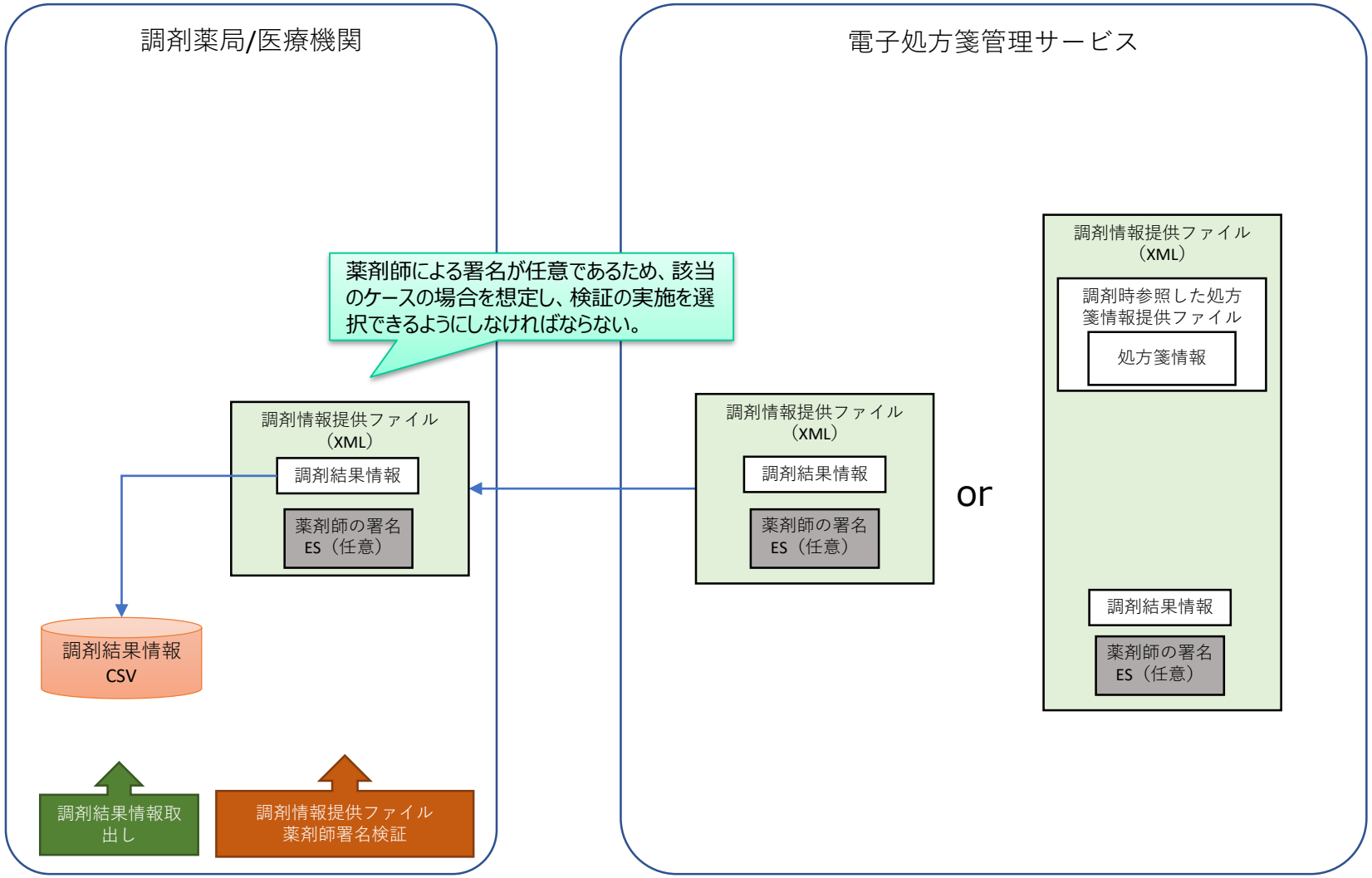
薬剤師による署名が任意であるため、該当のケースの場合に、署名を実施することを選択できるようなモジュールにする必要がある。

（５）紙処方箋等の場合の調剤情報提供ファイルの発行(薬剤師署名(任意))



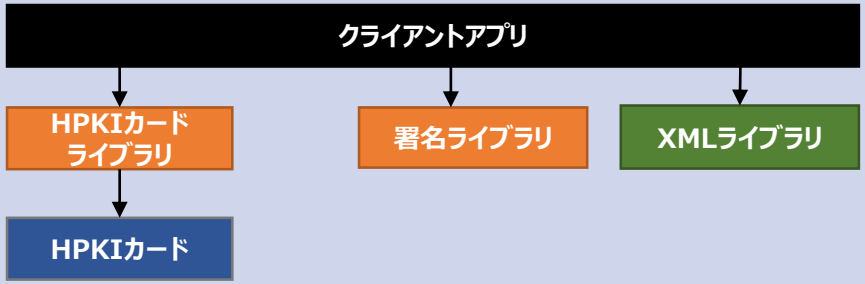
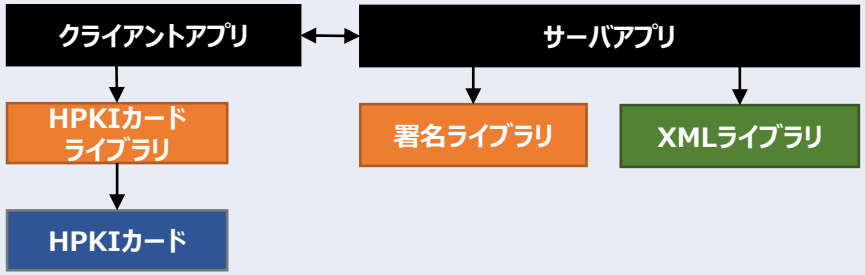
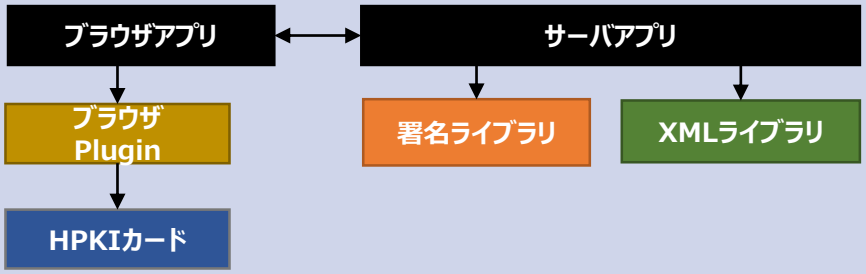
データ処理の流れ

（６）調剤情報提供ファイルの受領



ライブラリ構成

ライブラリ構成の例示を行う

形態	HPKIカード署名
①スタンドアローン	
②C/Sシステム	
③WEBシステム	

署名共通モジュールが有すべき機能の概要（1／2）

XMLライブラリ（形態に依らない）

共通モジュール	機能概要	対象
処方箋情報ファイル（XML）生成	処方箋情報(CSV)を入力し、処方箋情報ファイル（XML）を生成する。	医療機関
処方箋情報(CSV)取出し	電子処方箋ファイル(XML)または調剤済み電子処方箋(XML)から処方箋情報(CSV)を取り出す	医療機関 調剤薬局
調剤情報提供ファイル(XML)生成	電子処方箋ファイル(XML)と調剤結果情報(CSV)を入力し、調剤情報提供ファイル(XML)を生成する。	調剤薬局
調剤結果情報(CSV)取出し	調剤済み電子処方箋(XML)または調剤情報提供ファイル(XML)から調剤結果情報(CSV)を取り出す	医療機関 調剤薬局

署名ライブラリ（形態に依らない）

※概形要件であるため、必ずこの通りモジュール分割しなければならないものではない

共通モジュール	機能概要	対象
処方箋情報署名ハッシュ値生成	医師の署名が必要な電子処方箋の要素であるPrescriptionDocument要素を含む署名対象範囲（※）のハッシュを計算し、返す。	医療機関
電子処方箋ファイル(XML)の署名XML生成	医師のHPKIカードにより取得した署名値を入力し、処方箋情報ファイル（XML）に医師の署名を生成する。	医療機関
調剤結果情報署名ハッシュ値生成	薬剤師の署名が必要な調剤結果の要素であるDispensing要素を含む署名対象範囲（※）のハッシュを計算し、返す。	調剤薬局
調剤情報提供ファイル(XML)の署名XML生成	薬剤師のHPKIカードにより取得した署名値を入力し、調剤情報提供ファイル(XML)(署名前)に薬剤師の署名を生成する。	調剤薬局
電子処方箋ファイル(XML)の検証	電子処方箋ファイル(XML)（ES-XL(医師の署名)）の署名検証を行う。	調剤薬局
調剤済み電子処方箋(XML)の検証	調剤済み電子処方箋(XML)（ES-XL(医師の署名)/ES-A(薬剤師の署名)）の署名検証を行う。	医療機関 調剤薬局
調剤情報提供ファイル(XML)の検証	調剤情報提供ファイル(XML)の(ES(薬剤師の署名))署名検証を行う	医療機関 調剤薬局

（※）XML署名で必要な対象範囲を指す（詳細は規格書参照）

署名共通モジュールが有すべき機能の概要（2／2）

HPKIライブラリ　（形態①、②の場合）　※概形要件であるため、必ずこの通りモジュール分割しなければならないものではない

共通モジュール	機能概要	対象
署名者証明書取得	クライアントアプリにて HPKIカードを用いて、署名者証明書を取得する。	医療機関 調剤薬局
署名値生成	クライアントアプリにて HPKIカードを用いて、事前に取得したハッシュとHPKIカードの PINを入力して署名値演算を行う。	医療機関 調剤薬局

ブラウザ Plugin（形態③の場合）　※概形要件であるため、必ずこの通りモジュール分割しなければならないものではない

共通モジュール	機能概要	対象
署名者証明書取得	WEBブラウザにて HPKIカードを用いて、署名者証明書を取得する。	医療機関 調剤薬局
署名値生成	WEBブラウザにて HPKIカードを用いて、事前に取得したハッシュとHPKIカードの PINを入力して署名値演算を行う。	医療機関 調剤薬局

署名共通モジュールの入力、出力等に関する仕様（1／4）

医療機関での電子処方箋ファイル発行

※実装する際に最低限必要となるであろう項目を挙げているもの

機能	処方箋XMLの生成から医師署名までの流れ				
	処方箋情報ファイル（XML）生成	（※基本的には一連の流れとして以下の機能が実施される（実装上は必ずしも分割すべきものではない））			
		署名者証明書取得	処方箋情報(CSV)署名ハッシュ値生成	署名値生成	電子処方箋ファイル(XML)の署名XML生成
	XMLライブラリ	HPKIライブラリ／ブラウザPlugin	署名ライブラリ	HPKIライブラリ／ブラウザPlugin	署名ライブラリ
入力データ	・処方箋情報(CSV)ファイルパス ・処方箋情報ファイル（XML）ファイルパス	－	・処方箋情報ファイル（XML）ファイルパス ・署名者証明書	・Hash値 ・HPKIカードのPIN	・署名値 ・電子処方箋ファイル(XML)ファイルパス
処理内容	処方箋情報(CSV)をBase64エンコードして処方箋情報ファイル（XML）を生成する。	HPKIカードから署名者証明書を取得する。	処方箋情報ファイル（XML）の署名対象範囲を識別して、そのデータを含む署名対象データのHash値を生成する。	Hash値に対してHPKIカードで署名値を生成する。	署名値を格納した電子処方箋ファイル(XML)を生成する。
出力データ	・処方箋情報ファイル（XML）	・署名者証明書	・Hash値	・署名値	・電子処方箋ファイル(XML)（ES）
エラーコード	・処方箋情報(CSV) が存在しない ・指定パスに処方箋情報ファイル（XML）が出力できない	・RWにカードなし ・HPKIカード異常	・指定の処方箋情報ファイル（XML）が存在しない ・処方箋情報ファイル（XML）でない ・Hash値計算不能	・RWにカードなし ・PIN異常 ・PIN閉塞 ・HPKIカード異常	・処方箋情報ファイル（XML）が存在しない ・指定パスに電子処方箋ファイル(XML)が出力できない
備考				WEBブラウザではブラウザPlugin 使用	

署名共通モジュールの入力、出力等に関する仕様（2／4）

調剤薬局での調剤情報提供ファイル発行

※実装する際に最低限必要となるであろう項目を挙げているもの

機能	調剤結果XMLの生成から薬剤師署名までの流れ				
	調剤情報提供ファイル(XML)生成	（※基本的には一連の流れとして以下の機能が実施される（実装上は必ずしも分割すべきものではない））			
		署名者証明書取得	調剤結果情報(CSV)署名ハッシュ値生成	署名値生成	調剤情報提供ファイル(XML)の署名XML生成
	XMLライブラリ	HPKIライブラリ／ブラウザPlugin	署名ライブラリ	HPKIライブラリ／ブラウザ Plugin	署名ライブラリ
入力データ	・調剤結果情報(CSV)ファイルパス ・電子処方箋ファイル(XML)ファイルパス（ただし、紙の処方箋等の場合は存在しなくともよい） ・調剤情報提供ファイル(XML)(署名前)ファイルパス	－	・調剤情報提供ファイル(XML)(署名前)ファイルパス ・署名者証明書	・Hash値 ・HPKIカードのPIN	・署名値 ・調剤情報提供ファイル(XML)ファイルパス
処理内容	調剤結果情報(CSV)をBase64エンコードして調剤情報提供ファイル(XML)(署名前)を生成し、指定があれば電子処方箋ファイル(XML)を組み込む。	HPKIカードから署名者証明書を取得する。	調剤情報提供ファイル(XML)(署名前)の署名対象範囲を識別して、そのデータを含む署名対象データのHash値を生成する。	Hash値に対してHPKIカードで署名値を生成する。	署名値を格納した調剤情報提供ファイル(XML)を生成する。
出力データ	・調剤情報提供ファイル(XML)	・署名者証明書	・Hash値	・署名値	・調剤情報提供ファイル(XML)（ES）
エラーコード	・調剤結果情報(CSV) が存在しない ・指定の電子処方箋ファイル(XML) が存在しない ・指定パスに調剤情報提供ファイル(XML)(署名前) が出力できない	・RWにカードなし ・HPKIカード異常	・指定の調剤情報提供ファイル(XML)(署名前)が存在しない ・調剤情報提供ファイル(XML)(署名前)でない ・Hash値計算不能	・RWにカードなし ・PIN異常 ・PIN閉塞 ・HPKIカード異常	・調剤情報提供ファイル(XML)(署名前)が存在しない ・指定パスに調剤情報提供ファイル(XML)がファイル出力できない
備考	XMLパーサ等で電子処方箋ファイル(XML)（ES-XL）部分を再生成しない事（改ざんとなるため）。			WEBブラウザではブラウザ Plugin 使用	

署名共通モジュールの入力、出力等に関する仕様（3／4）

調剤薬局での電子処方箋ファイルの受領

※実装する際に最低限必要となるであろう項目を挙げているもの

機能	処方箋XML 医師署名の検証	処方箋情報(CSV)取出し
	署名ライブラリ	XMLライブラリ
入力データ	・電子処方箋ファイル(XML)ファイルパス	・電子処方箋ファイル(XML)ファイルパス もしくは処方箋情報ファイル（XML）ファイルパス ・処方箋情報(CSV)ファイルパス
検証に必要な外部情報	・厚労ルート証明書 ・タイムスタンプCA証明書	－
処理内容	医師署名検証 （ES-XL検証）	電子処方箋ファイル(XML)もしくは処方箋情報ファイル（XML）から処方箋情報(CSV)を取り出す
出力データ	検証結果（正常/検証NG）	処方箋情報(CSV)
エラーコード	・指定の電子処方箋ファイル(XML)が存在しない ・電子処方箋ファイル(XML)でない ・検証不能（証明書なし） ・検証不能（証明書期限切れ）	・電子処方箋ファイル(XML)もしくは処方箋情報ファイル（XML）が存在しない ・指定パスに処方箋情報(CSV)がファイル出力できない
備考	CRLに未反映の失効情報が存在する可能性がある(第2種のエラー) ※運営主体による運用も含めた対応策を実施	

署名共通モジュールの入力、出力等に関する仕様（4／4）

医療機関／調剤薬局での調剤情報の取得

※実装する際に最低限必要となるであろう項目を挙げているもの

機能	調剤済み電子処方箋(XML) 薬剤師署名の検証	調剤情報提供ファイル(XML)の検証	調剤結果情報(CSV)取出し
	署名ライブラリ	署名ライブラリ	XMLライブラリ
入力データ	・調剤済み電子処方箋(XML)ファイルパス	・調剤情報提供ファイル(XML)ファイルパス	・調剤済み電子処方箋(XML)ファイルパスもしくは調剤情報提供ファイル(XML)ファイルパス ・調剤結果情報(CSV)ファイルパス
検証に必要な外部情報	・厚労ルート証明書 ・タイムスタンプCA証明書 ・タイムスタンプCRL	・厚労ルート証明書	－
処理内容	①薬剤師署名検証（ES-A検証） ②医師署名検証（ES-XL検証）	薬剤師署名検証(ES検証)	調剤済み電子処方箋(XML)もしくは調剤情報提供ファイル(XML)ファイルパスから調剤結果情報(CSV)を取り出す
出力データ	検証結果（正常/検証NG）	検証結果（正常/検証NG/署名無し）	調剤結果情報(CSV)
エラーコード	・指定の調剤済み電子処方箋(XML)ファイルが存在しない ・調剤済み電子処方箋(XML)でない ・検証不能（証明書なし） ・検証不能（証明書期限切れ） ・検証不能（CRL不適（※））	・調剤情報提供ファイル(XML)が存在しない ・調剤情報提供ファイル(XML)でない ・検証不能（証明書なし） ・検証不能（証明書期限切れ）	・調剤済み電子処方箋(XML)もしくは調剤情報提供ファイル(XML)ファイルパスが存在しない ・指定パスに調剤結果情報(CSV)がファイル出力できない
備考	CRLに未反映の失効情報が存在する可能性がある(第2種のエラー) ※運営主体による運用も含めた対応策を実施	薬剤師の署名が任意であるため、署名が存在しない可能性がある	

薬剤師署名検証（ES-A検証）が正常に検証できる場合、医師署名検証(ES-XL検証)の署名タイムスタンプと検証情報の検証に、ES-Aの署名タイムスタンプ時刻を使用する

調剤情報提供ファイル(XML)の場合は、薬剤師の署名が任意であるため、署名が存在しない可能性があることに留意する必要がある

（※）
- CRLのnextUpdateが署名タイムスタンプ時刻より前
- 署名用証明書のnotAfterが署名タイムスタンプ時刻よりも前
- CRLのthisUpdateが署名者証明書のnotAfterよりも後

等

JAHISからの電子処方箋での署名共通モジュールに対する要望

- 前頁までの仕様案の実現にあたり、電子処方箋での署名共通モジュールへの要望を以下に示す。
  - 本仕様案で示した事項は概形の要件であるため、複数の電子署名モジュール実装事業者が想定される場合は、HISベンダの開発負荷を極小化するために、外部インターフェース（関数名、引数、戻り値、処理内容、エラーコード等）について共通化し、より詳細な仕様を電子署名モジュール実装事業者に対し示す必要がある。
  - 電子処方箋での署名共通モジュールを、ソリューション／サービスに組み込むベンダーによって開発言語は様々であるため、DLLで提供しソリューション等に組み込んでもらう際は、システム動作環境について、より多くの環境で幅広くサポートを行うと共に、動作環境を明確化する必要がある。
    - DLLの対応環境について幅広くサポートを行うことができないならば、EXEでの提供も候補となるが、EXEの実行速度が遅くなることで、動作速度のボトルネックにならないようにすべき。
  - 医療機関等内の既存システムとして、ユーザー認証のために独自のICカードを利用することがあるため、独自のICカードを利用した状態でも、HPKIカードによる電子署名を実現可能とする必要がある。
  - 紙処方箋で交付された場合の、調剤情報提供ファイルにおいて、参照した処方箋情報提供ファイルには医師の電子署名が付与されないこと、参照した処方箋情報提供ファイルそのものがないこと、薬剤師の電子署名が任意であることを踏まえた仕様を示す必要がある。
  - 処方箋に対するES-XL形式とする際に、CRLに未反映の失効情報が存在する可能性があるため、想定しているエラーに対して運用も含めた対応策をきちんと行い、各関係者でリスクを受容できるよう調整されることを願う。
  - 署名共通モジュールを組み込んだHPKIカードによる署名を行う際に、「JAHIS電子処方箋実装ガイド Ver.1.2」で「医師が入力したPINをアプリケーション内でキャッシュすることにより１回のPIN入力で済ますことは許容される。」(5.4.3.3 電子署名付与)と記載しているため、本人性の担保が取れる場合においてPINキャッシュについても容認していただけるように願う。