



医療分野におけるPKIの最新動向と JAHISにおける標準化活動

2017年5月22日

JAHIS 医療システム部会 セキュリティ委員会
委員長 茗原 秀幸

「はじめに」という名の今日のサマリ

- HPKIは国際標準ISO17090に準拠するCPを厚生労働省が策定している。
- HPKIはHPKI専門家会議の準拠性監査を受け、認められた事業者のみ発行可能。
- HPKIは厚生労働省をRootとして日本医師会、MEDIS-DC等が発行している。
- 署名用証明書、認証用証明書(人)、認証用証明書(組織)のCPが整備されている。
- 署名用は紹介状、診断書などに利用されている。電子処方箋への利用も期待されている。
- 認証用は日医がSAMLの認証サービスを実施しており、地域医療連携などで活用されている。
- JAHISでは厚生労働省のガイドラインやISO17090シリーズに準拠した業界標準を策定し、産業界として普及推進に協力している。

1. 署名用HPKIの推進状況

一つの証明書検証で、本人性と属性を一度に確認できること。

国家資格の確認: 診療情報提供書(紹介状)には医師の署名(もしくは記名押印)が必要。

医療機関の管理者の確認: 電子契約への応用の可能性を開く。電子レセプトにおける発行責任者であるかの確認を行うこと等も技術的には可能となる。

HPKIの国際規格(ISO IS17090)
との整合性を取りつつ
日本の社会インフラとして整備する

ネットワーク基盤検討会最終報告書

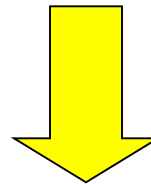
今後の医療情報ネットワーク基盤のあり方について
ネットワーク基盤検討会最終報告
(平成16年9月30日)

署名用証明書のための公開鍵基盤の整備
診断書や診療情報提供書の電子化を認める
外部保存の受託可能機関の拡大
e-文書法への対応に関する指針の提示

- 保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議設置（平成17年7月）
 - － 医療情報ネットワーク基盤検討会で策定された証明書ポリシーに準拠した各認証局の準拠性を公正に審査するための体制等について検討を実施。
 - － 当該会議の下に設置された専門作業班で準拠性監査基準を作成
 - － 同時に、証明書ポリシーのメンテナンス（改定、修正）を実施

ITによる医療の構造改革

- 医療の情報化のための共通基盤の整備 (以下演者が要約)
 - 個々のHPKI認証局が共通のHPKI証明書ポリシーに準拠していることを示す証明書を発行する認証局を2006年度までに構築し運用を開始する。(厚生労働省)



厚生労働省が協力を依頼している日本医師会のHPKI認証局と医療情報システム開発センター(MEDIS-DC)のHPKI認証局が厚生労働省の定める証明書ポリシーの準拠性監査に合格し、厚生労働省のRoot-CAを信頼点とするサブCAとなる(後に日本薬剤師会も合格)

医政発第0622010号 平成18年6月22日

厚生労働省医政局長

「書面に代えて電磁的記録により作成、縦覧等又は交付等を行うことができる医療分野に係る文書等について」

演者による要約: (正しい解釈は原文を参照願います)

医療分野における各種申請、請求などに関する手続きにおいて求められる医師などの証明書が必要と考えられる添付書類(診断書や証明書など)について電磁的記録により作成、交付および署名を認めることとする。

手続名と添付書類の例:(通知の別紙に記載されているものの抜粋)

健康保険疾病手当金請求書→疾病の状態に関する医師又は歯科医師の意見書

処方せんは当初は対象文書に含まれていなかったが、平成28年3月31日改正によって対象文書に処方せんが追加され、電子処方せんが制度上実施可能となった。

6.12 法令で定められた記名・押印を電子署名で行うことについて(抜粋)

- (1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと
 1. 保健医療福祉分野 PKI 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野PKI 認証局の発行する電子署名を活用するのが望ましい。ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。
- (2) 電子署名を含む文書全体にタイムスタンプを付与すること。
- (3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いること。

小野田医師会では「さんさんネット」を活用した主治医意見書の山陽小野田市とのオンライン化に取り組んで、全国で初めて実用化した。

主治医意見書オンライン化について

主治医意見書作成&送信



主治医意見書作成ソフト
電子署名ソフト
タイムスタンプ
事前申請：医師資格証
ICカードリーダー



主治医意見書受信



電子認証ソフト

主治医
意見書
印

引用元：http://www.yamaguchi.med.or.jp/sun2net/download/sun2net_Vol2.pdf

2. 認証用HPKIの推進状況

本人性の確認のみであれば、将来的にはマイナンバーカードなどのフレームワークが利用可能かもしれないが...

医療分野におけるITの利用においては、医療の専門家であることを担保する仕組みが必要になる

医師でなければ作成できない記録などが存在する

業務アプリケーションに対するより厳密なアクセス制御をする場合には、属性認証が必要になる

従来は、各医療機関内や地域ドメイン内で
独自の属性認証の仕組みを個別に構築していた。
→施設間や地域間での互換性なし

検討課題：全国統一の属性を含む認証基盤の構築は必要か！？

HPKIであれば、一つの証明書検証で、HPKI認証局が信頼されていれば全国どの組織においても**本人性と属性(国家資格)を一度に確認できる**

本人性の確認:

本人性、実在性を認証用HPKIルート認証局が信頼点として保証することで、異なる組織間においても本人性が担保される。

国家資格の確認:

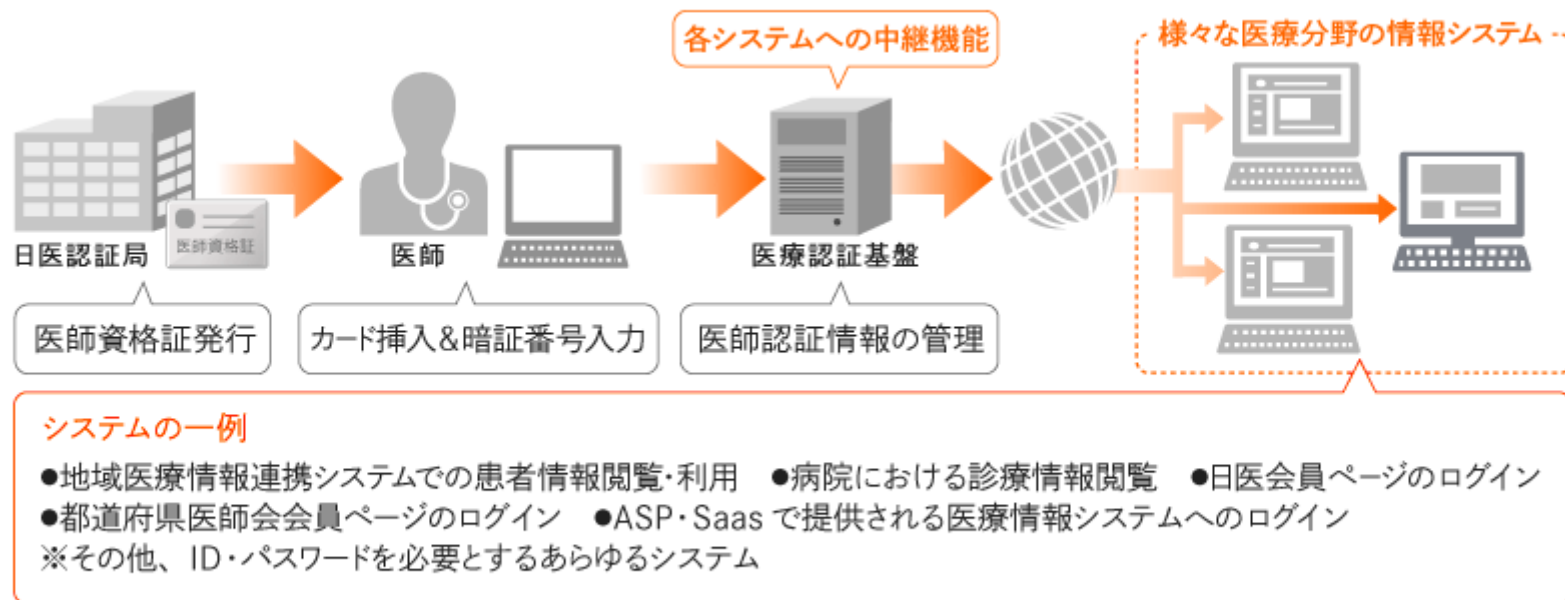
国家資格の保有についても、認証用HPKIルート認証局が信頼点として保証するため、異なる組織間において属性が担保される。

国際規格 (IS17090) との整合性を取りつつ認証用においても日本の社会インフラとして整備する

- HPKI認証用証明書ポリシーは人用(医療専門職等向け)とその他用(施設やデバイス、アプリケーション向け)に分けて検討を実施。
- 人用ポリシーについては、署名用ポリシーをベースに認証用に向けての小改修を実施。→人認証用CPをリリース
 - PKIの用途はDigital SignatureとSSLに限定
 - 暗号用には利用できない(解読の機会を極小化するための措置)
- その他用ポリシーについては、保険医療機関等の施設認証を優先して検討。→施設認証用CPをリリース
 - 社会保障カード推進室によるオンライン保険証資格確認における認証用として検討
 - 制度化されることを念頭に置き、申請主義ではない発行パターンも検討
 - 保険医療機関等以外の認証については国としてのフレームワーク構築の可否も含めて検討
(必要性が見い出せないため当面は見送り)

JAHIS 日医のHPKI認証用証明書を利用したSSOサービス

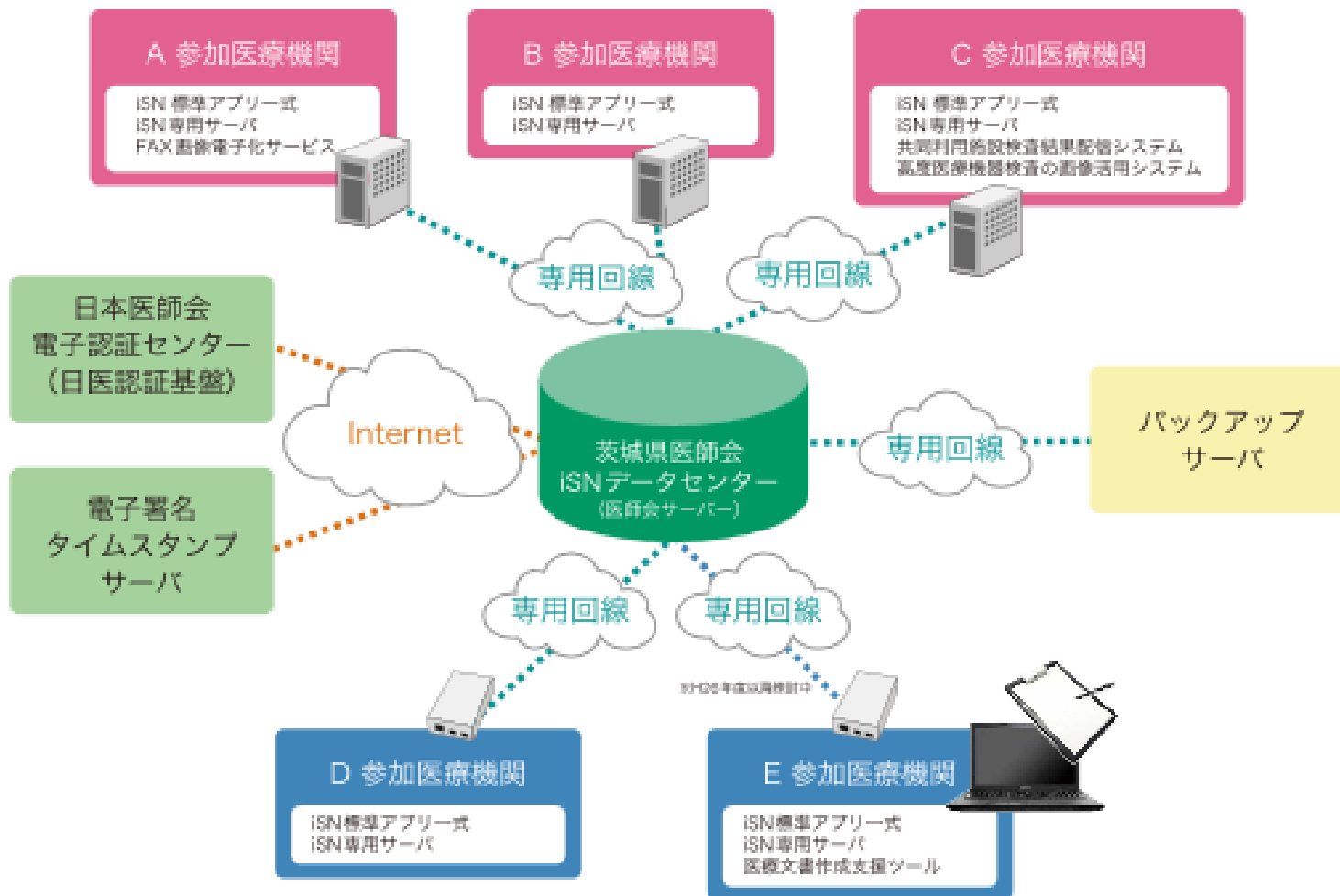
日本医師会では、日医認証局の運営と共に「医療認証基盤」というサービスも提供しています。この医療認証基盤は、情報へのアクセス時のシングル・サインオン（SSO: Single Sign-On）の機能を提供します。平成22年度に経済産業省が実施した「医療情報化促進事業」に「医療分野認証基盤整備コンソーシアム」として参画して、このシングル・サインオンを医療分野で使えるような仕組みを構築しました。



引用元: 日本医師会電子認証センター <http://www.jmaca.med.or.jp/hpki/role/sso.html>

電子認証活用事例 (SSO)

いばらき安心ネットでは医師のLOGIN時にHPKIカードを用いた日本医師会電子認証センターによる第三者認証を行っている。(電子紹介状による電子署名も実装している)



引用元: <http://www.ibaraki.med.or.jp/isn/html/about.html>

3. ISO/TC215における HPKIの規格化の状況と対応

- ISO/TC215WG4エキスパートとして日本からメンバーを派遣
 - 東工大 大山教授 JAMI、JAHIS、JIRA他がメンバー
 - 茗原がWG4 vice convener に就任

- ISO/TC215国内対策委員会WG4作業部会にて対応を検討
 - 作業部会長 東工大 大山教授 副部会長 茗原
 - ISOの国際会議前に対処方針などを確認、決定する

- JAHISセキュリティ委員会(委員長 茗原)における対応
 - 各規格の対応を検討、投票コメントの検討などを実施。さらに詳細検討が必要な場合は担当WGにて具体的な翻訳作業、詳細仕様検討などを実施。
 - JIRAセキュリティ委員会と積極的に意見交換を実施し、産業界としての統一見解の取りまとめを実施。
 - JAHIS標準類のISO規格への組み込みを積極的に実施。
 - 制定済みISO規格のJAHIS標準への反映を実施。

規格名称: Health informatics – Public key infrastructure (IS17090)

IS17090はヘルスケア部門向けのPKI(HPKI)に関するISです。Part1ーPart4はISとして出版されています。Part5は現在策定中です。

本規格は日本の厚生労働省の認証局ポリシーと整合性が取られています。

Part1 Framework and overview:

Part1では、HPKIのフレームワーク及び概要を記載されています。発行対象の種類(自然人、アプリケーション等)、役割の種別などが規定されています。

Part2 Certificate profile:

Part2では、HPKIの証明書に記載される内容について記載されています。PKIとしての標準的な箇所の定義とヘルスケア独特のhroleの定義がなされています。

Part3 Policy management of certification authority:

Part3では、認証局における認証ポリシー作成のためのガイドラインが記載されています。

Part4 Digital Signatures for healthcare documents:

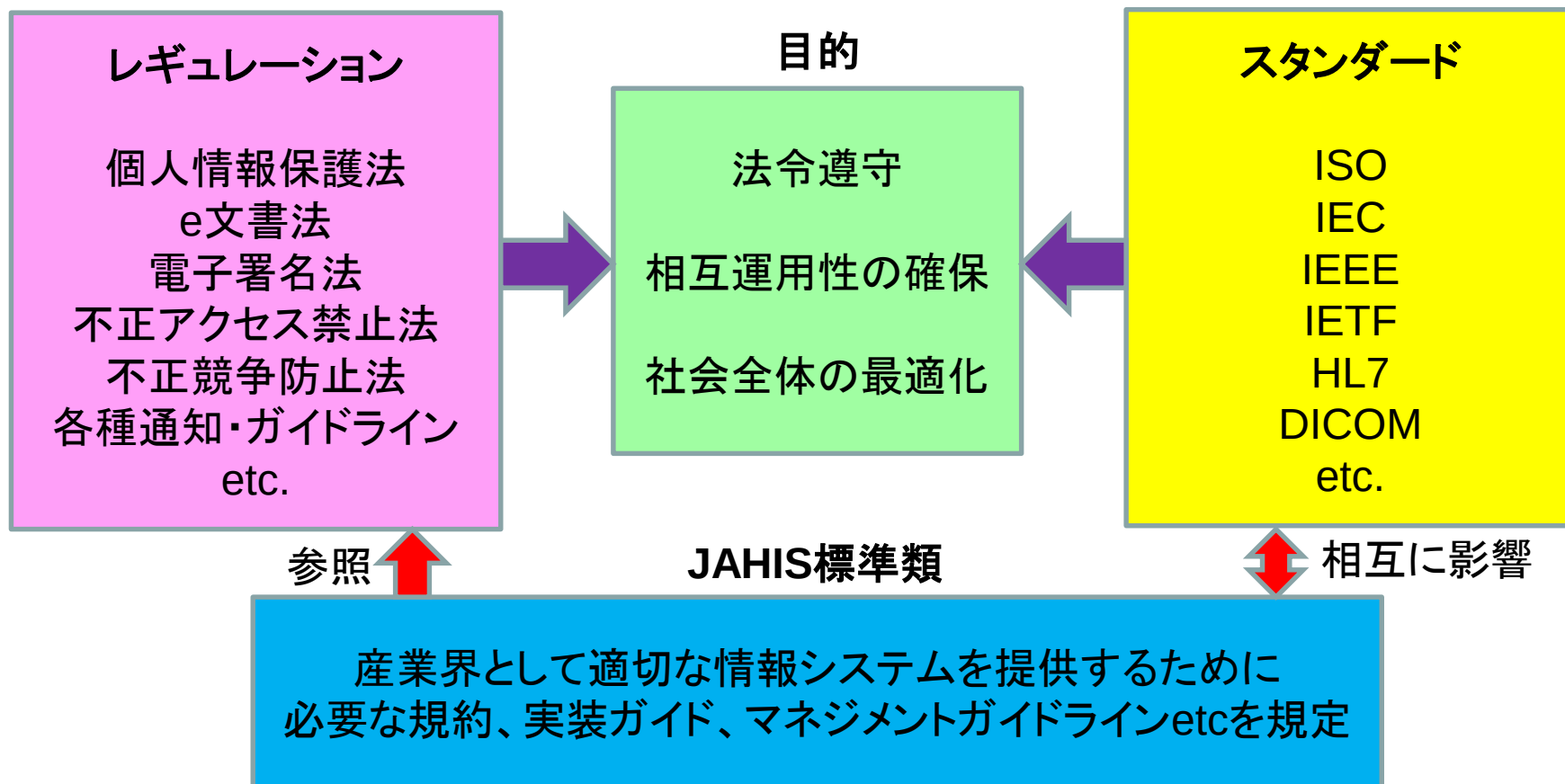
Part4は**日本のJAHIS標準の電子署名規格をそのままISOに提案したものです。**日本主導で規格化を行い、ISとして成立しました。

Part5 Authentication using Healthcare PKI credentials:

Part5は**日本のJAHIS標準を参考にクルデンシャルの検証ルールを規定するものです。**現在FDIS投票に入ることが承認されました。

4.JAHIS標準類の位置づけ

ヘルスケアセキュリティ分野における レギュレーションとスタンダード



セキュリティ委員会のJAHIS標準類策定における考え方

レギュレーションにおいては、
厚生労働省の「医療情報システムの
安全管理に関するガイドライン」を遵
守することを念頭に置いた規約、ガ
イドラインを制定する

スタンダードにおいては、
ISOとの整合性を確保するため、
JAHIS標準類のISOへの提案や、
ISO規格のJAHIS標準類への取り
込みを実施する

工業会組織であるため、視点はあくまでベンダーの視点であり、医療サービ
サーや情報システムサービサーの視点ではない。

最近の課題

情報システムサービサーとしての、クラウドに関する
問い合わせや、標準化の要請が増えつつある。

15-001 保存が義務付けられた診療録等の電子保存ガイドライン

電子保存・外部保存システムにおける技術的対策としてベンダーが整備すべきものを規定

13-009 ヘルスケア分野における監査証跡のメッセージ標準規約

医療情報システムにおける監査証跡としての監査LOGのメッセージを規定

14-008 製造業者による医療情報セキュリティ開示書ガイド

医療情報システムの技術的対策の実装内容をベンダーが自ら説明するフォーマットを規定

16-003 リモートサービスセキュリティガイドライン

リモート保守などのリモートサービスを実施する際のサービスラーとして考慮すべき事項を規定

8-002、10-002 HPKI対応ICカードガイドライン

HPKI証明書をICカードに格納した場合のHPKIへのアクセスメソッドを規定

12-007 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

HPKIを利用して否認防止のための電子署名を行う際の手続きを規定

14-005 HPKI電子認証ガイドライン

HPKIを利用して本人確認などの認証を行う際の考慮すべき事項を規定

16-002 シングルサインオンにおけるセキュリティガイドライン

病院内の複数システムにおいてシングルサインオンを実現するための要求事項とリスクアセスメントの考え方を記載

16-103 セキュアトークン
実装ガイド機器認証編

医療機関内における無線接続機器の機器認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載

14-103 セキュアトークン
実装ガイド

医療機関内、施設間などにおけるノード認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載

安全管理GLとJAHIS標準の関係

15-001 保存が義務付けられた診療録等の電子保存ガイドライン

安全管理ガイドラインの技術的対策として要求されているC項、D項を網羅的に記載

13-009 ヘルスケア分野における監査証跡のメッセージ標準規約

安全管理ガイドラインの6. 5章C6.の要求事項を満たすように規定されている

14-008 製造業者による医療情報セキュリティ開示書ガイド

安全管理ガイドラインの技術的対策として要求されているC項への対応状況を記載可能

16-003 リモートサービスセキュリティガイドライン

安全管理ガイドラインの6. 5章、6. 8章、6. 11章の要求事項を踏まえた記載となっている

8-002、10-002 HPKI対応ICカードガイドライン

安全管理ガイドラインの6. 5章に対応しているが直接の関係はない

12-007 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

安全管理ガイドラインの6. 12章の要求事項を踏まえた記載となっている

14-005 HPKI電子認証ガイドライン

安全管理ガイドラインの6. 5章の認証をHPKIで行う際の要件を記載している

13-009 ヘルスケア分野における監査証跡のメッセージ標準規約

RFC3881,DICOM3.0Part15を参照標準とし、ISO27789のベースの規格となった。
ISO27789出版を受け完全に整合するよう改訂。

16-003 リモートサービスセキュリティガイドライン

SPC White Paperを参考にJIRAが立案し、JAHISと合同でメンテナンスを実施している。
ISO/TR11633のベースの規格となった。
ISO/TR11633出版を受け整合するよう改訂。

8-002、10-002 HPKI対応ICカードガイドライン

ISO/IEC7816-4,8,15を参照標準とし、日本医師会のHPKI対応ICカード発行時のベースの規格となった。

12-007 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

ISOのCAAdES、XAdES規格(14533)を参照標準とし、ISO17090-4策定の際のベースの規格となった。

14-005 HPKI電子認証ガイドライン

電子認証の要求事項をまとめるためJAHISが立案し、ISO17090-5として国際標準策定作業中(現在はFDIS)。

JAHIS技術文書 JAHIS電子処方せん実装ガイドVer.1.0を策定

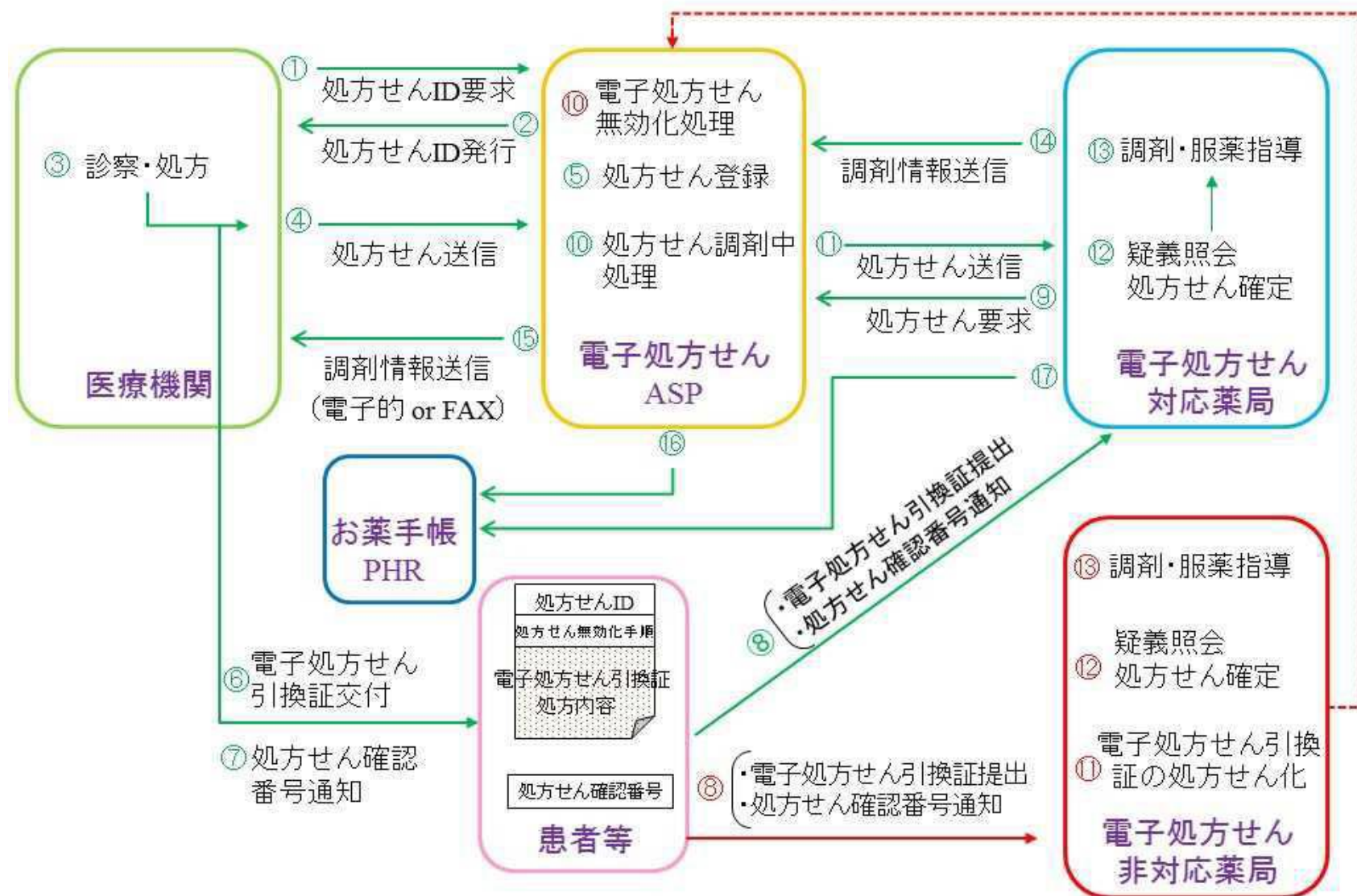
JAHIS電子処方せん実装ガイドVer.1.0は、2016年3月に厚生労働省から公開された「**電子処方せんの運用ガイドライン**」を実現するために、関係する医療機関、薬局、ASPサーバの各アクタの情報システムで必要となる機能の**具体的な実装仕様を取りまとめたもの**である。

電子処方せんやその調剤結果の情報を記述する際の**データフォーマット**については、2016年4月に東京大学から公開された「電子化した処方箋の標準化様式の整備と運用に関する研究 平成27年度総括報告書」に含まれている「**電子的処方指示・調剤実施情報提供書 CDA 記述仕様(案)**」に基づいて整理を行った。

- 「電子処方せん」と「調剤情報」のCDA(**XML文書**)に対して電子署名ルールを規定
- 調剤情報では処方箋の医師の署名と調剤した薬剤師の署名をいずれも長期署名として検証可能な実装仕様を規定(**ES-XLフォーマットの活用**)
- ネットへの**接続状況によって**タイムスタンプの利用方法を**場合わけ**して規定
- 電子処方せんの**実装上の課題について明確化**を実施

厚生労働省による課題解決のための更なる検討が進むことを期待

⑨ 電子処方せん無効化要求



JAHIS 多重署名のワークフロー

医療機関:

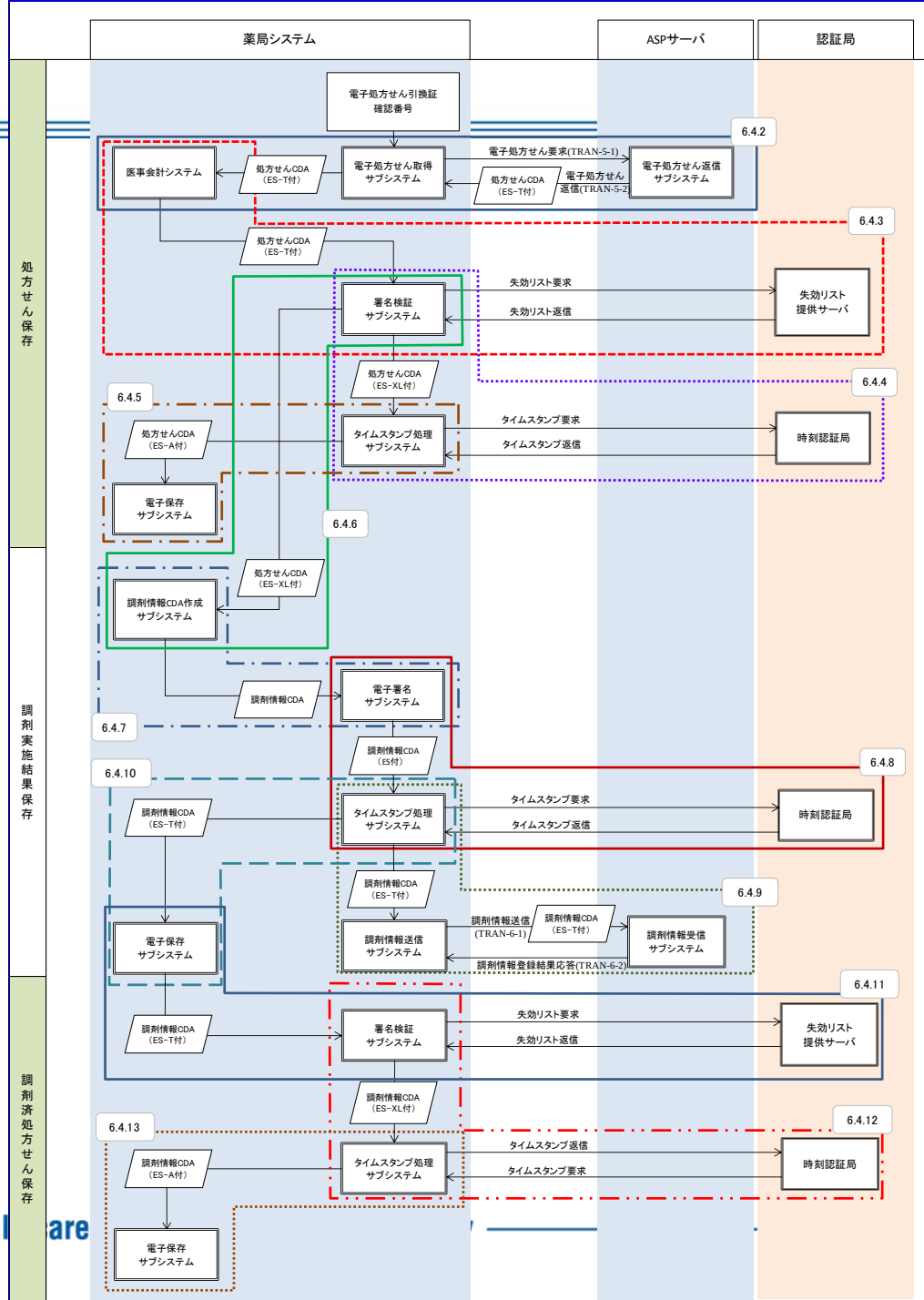
電子処方せんCDAに対して医師が電子署名を行い、タイムスタンプを取得してES-TとしてASPサーバに送信する。

薬局:

医師のES-T付の電子処方せんCDAを取り込み、医師の電子署名をES-XL化し、調剤情報CDAに組み込む。
薬剤師は調剤情報CDAに電子署名を行い、タイムスタンプを取得してES-Tとして、ASPサーバに返す。
(右の詳細ワークフローの部分)

医療機関:

薬剤師のES-T付の調剤情報CDAを取り込み必要に応じて薬剤師の電子署名にES-Aを付与する。その結果、医師のES-XLも改ざん防止が行われ、二つの署名の長期真正性担保が行われる。



- 日本は厚生労働省が中心となり国際標準17090シリーズに準拠したHPKI環境が整いつつある。
- HPKI電子署名の利用が始まっている。
ユースケースは紹介状や主治医意見書となっている。
- 電子認証の利用も始まっている。
ユースケースは地域医療連携システムのSSOとなっている。
- 電子処方せんへの適用に向けた検討が進んでいる。
ようやくJAHISとして実装ガイド策定にこぎつけた。
- 今後、電子処方せんの実装に向けた課題解決のためのアプローチが行われることを期待する。

ご清聴ありがとうございました。