資料１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第２６回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・専門作業班合同会議

厚生労働省 医政局 参事官（特定医薬品開発支援・医療情報担当）付医療情報室

Ministry of Health, Labour and Welfare of Japan

Ministry of Health, Labour and Welfare of Japan

1．日本医師会認証局 サブCA鍵更新

審議：更新の再延期について

2．HPKIリモート署名サービスに関して

議論：リモート署名サービス評価基準の今後の進め方について

3．連絡：ポリシー類の保守計画について

4．連絡：次回（第２７回）の予定について

ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

1．日本医師会認証局 サブCA鍵更新

審議：更新の再延期について

2．HPKIリモート署名サービスに関して

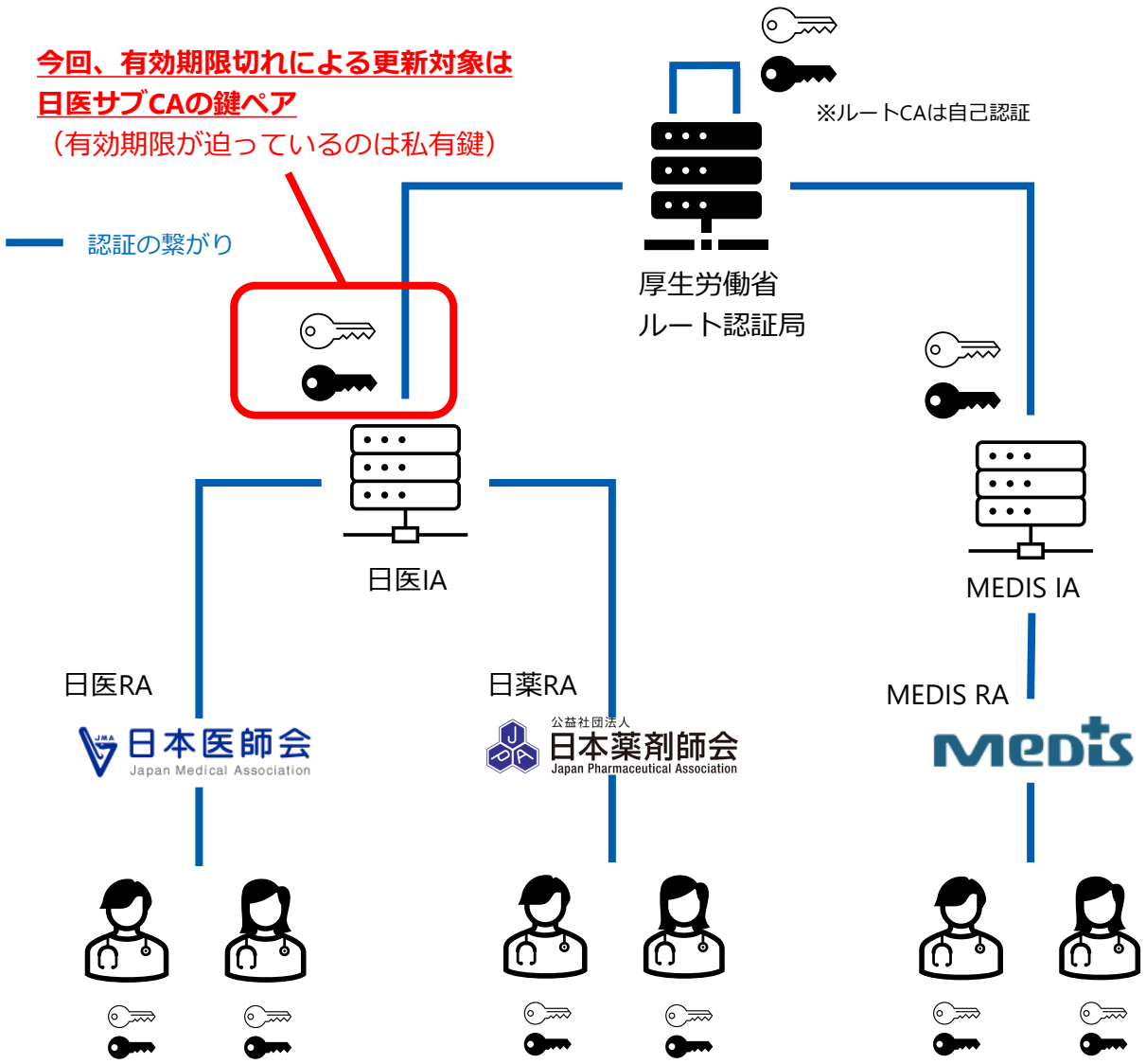
議論：リモート署名サービス評価基準の今後の進め方について

3．連絡：ポリシー類の保守計画について

4．連絡：次回（第２７回）の予定について

【前回資料再掲】鍵更新について

今回、有効期限切れによる更新対象は
日医サブCAの鍵ペア
（有効期限が迫っているのは私有鍵）



鍵ペアの有効期限

ルートCA

公開鍵証明書：30年

私有鍵：15年

サブCA

公開鍵証明書：20年

私有鍵：10年

エンドエンティティ

発行後5回目の誕生日まで

【参考】鍵ペアの有効期間（現状）

保健医療福祉分野PKI認証局署名用証明書ポリシ（令和５年１２月）での記載内容
※認証用（人）ポリシも同一の内容

> **6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間**
> CA公開鍵証明書の有効期間は20年を越えないものとし、その私有鍵の使用は10年を越えないものとする。ただし、10年の私有鍵の使用期間を延長する必要がある場合にはHPKI認証局専門家会議の承認を得て、最大1年の範囲において必要な期間に限り延長することができる。
> エンドエンティティの加入者の公開鍵証明書の有効期間は、発行の日後の加入者の5回目（加入者が発行を受けている署名用電子証明書の有効期間が満了する日の前に、CPSで定める更新の期間内に加入者が新たな署名用電子証明書の発行の申請をし、新たな署名用電子証明書の発行を受けるときにあっては6 回目）の誕生日とする。

CA名（SHA256)	開始日	公開鍵終了日	私有鍵終了日
厚労省ルートCA	2014年1月17日	2044年1月16日	2029年1月16日
日医署名サブCA	2014年1月17日	2034年1月16日	**2024年1月16日**
日医認証(人)サブCA	2014年1月17日	2034年1月16日	**2024年1月16日**
MEDIS署名サブCA	2015年4月20日	2035年4月19日	**2025年4月19日**
MEDIS認証(人)サブCA	2017年3月17日	2037年3月16日	**2027年3月16日**

（ルートCAは厚生労働省HPKIルート認証局運用管理規定で指定されており、有効期間は公開鍵30年、私有鍵15年）

日本医師会認証局
サブCA鍵更新の再延長について

第25回HPKI専門家会議（2023年12月）にてHPKI認証局ポリシ改定を審議いただき
「CA私有鍵の有効期間についてHPKI専門家会議の承認を経て最大１年まで延長できる」とし、
日本医師会サブCA私有鍵については**「半年間の延長」**をご承認いただきました。

延長承認後の経緯

【～2024年3月】
- 日本医師会において検証用のサブCAを構築。
- 日医認証局は、厚労省ルート認証局のサブCAであるため（RFC5280に従って）、リンク証明書は発行しない方式で構築。
- 鍵更新手順の検証・確認と共にシステムの検証用の証明書一式（CRL、EE証明書）を発行。
- ①リモート署名サービスを提供しているMEDIS、②（医薬局を通じて）電子処方の署名検証モジュールを作成している各ベンダーに検証用証明書を提供の上、検証を依頼。
- ①、②いずれも、現在のEE証明書による電子署名の検証が不可となった。
  ※①はApache/OpenSSL、②は各ベンダー毎の独自の実装

【2024年4月】
- 当初、発行しない予定であったリンク証明書（NEW with OLD、OLD with NEW）を発行して提供。
- この際、RFC4210を参照したが、サブCA鍵更新に関して明確な記載がないため、「ルート証明書鍵更新手順」を「サブCA鍵更新手順」と読み替えて発行
- 状況変わらず。

【2024年5月】
- そもそも、サブCA鍵更新の場合は、リンク証明書を発行しないという指摘あり（参考資料１参照）。
- OpenSSL自体が鍵更新に対応していないことが判明。
- 改めて、RFC5280に基づいてリンク証明書を用いない検証をOpenSSL外で実施する仕組みを構築したところ検証成功。
- ②の電子処方箋の署名検証モジュールについては、各ベンダーが独自実装しているため、RFC5280に基づいてコーディングされているか不明。
- 従って、医薬局（電子処方箋実施機関）主催の元、保健医療福祉情報システム工業会（JAHIS）の協力も得て、モジュールの実装方法に係る補足説明をする説明会を開催予定（5/20 14時から）（参考資料2参照）

日本医師会認証局
サブCA鍵更新の再延長について

ご依頼内容

経緯の通り、日本医師会サブCAの鍵更新にあたり、電子処方箋の署名検証モジュールを中心に事前の検証作業を進めたところ、更新後の新CAのCRL（失効リスト）では旧CAで発行された証明書が失効確認できないものが存在することが判明しました。ただし、その範囲が一部のモジュールなのか、多くのモジュールに及ぶものか不明です。
※原因と対応については次ページ以降に記載

サブCA鍵更新そのものは、手順に従い準備を進めてきましたが、このまま鍵更新を実施した場合、利用者の認証（電子処方箋の運営）に支障をきたすことから、モジュールベンダーに対する確認と対応のために**「再度の延長」**をご審議いただきたくお願いいたします。

審議事項

1. **日本医師会サブCA　鍵更新の再延長可否**
2. **鍵更新方法に関わる認証局ポリシの改定（リンク証明書の扱いについて）（資料2-1、資料2-2、参考資料1）**

確認依頼

1. **日本医師会サブCA更新時の運用方法と実装について（参考資料１）**

審議①：日本医師会サブCA私有鍵期限の延長案

2024年1月16日（当初期限）　⇒　2024年7月16日（延長期限）　⇒　2025年1月16日（再延長期限、最大の場合）
昨年改定したポリシの範囲内にて再延長を実施、具体的な延長期間は範囲内において最短となるべく、ベンダー各社の対応日程が確定次第、ご承認いただきたくお願いいたします。
（万が一ポリシを超える延長が必要となることが判明した場合は、再度、専門家会議にお諮りさせていただきます。）

日本医師会認証局
サブCA鍵更新の再延長について

審議事項②：鍵更新に関わる認証局ポリシの改定（リンク証明書の扱いについて）

HPKIにおける鍵更新の運用は下記の通りとし、ポリシの改定を実施する

- ルート認証局が鍵更新を行う場合は「リンク証明書」を使用する。
- サブ認証局（中間CA）が鍵更新を行う場合は「リンク証明書」を使用しない。

リンク証明書　（認証局ポリシ　定義と略語より抜粋）

CA鍵を更新する際に、新しい自己署名証明書（NewWithNew）と古い世代のCA鍵と新しい世代のCA鍵を紐付けるために発行される電子証明書。リンク証明書によって、世代の異なるCAから電子証明書を発行された加入者間での証明書検証が可能となる。リンク証明書には、新しい公開鍵に古い私有鍵で署名した証明書（NewWithOld）と、古い公開鍵に新しい私有鍵で署名した証明書（OldWithNew）がある。

以下、認証局ポリシ修正箇所案

2.2　証明書情報の公開

＜検証者に公開する事項＞に**「リンク証明書（ルートCAのみ対象）」**を追加

5.5.1　アーカイブ記録の種類

認証局がアーカイブする情報に**「リンク証明書（ルートCAのみ対象）」**を追加

5.6　鍵の切替

「ルートCA私有鍵の更新時にはリンク証明書を発行し、公開する。（サブCA私有鍵の更新時は不要）」の文言を追加

表1.2におけるOIDについて

ポリシで定めるリンク証明書では独自OIDの設定とせず「2.5.29.32.0(any-policy)」とし、「1.2 文書の名前と識別」における表1.2に追記は行わない形で進める

※表1.2のOIDは証明書の「certificatePolicies」項に記載される

表1.2　本CPで定めるOID

名称	オブジェクト識別子
HPKI署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1
HPKI認証用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.3.1
HPKI認証用（組織）証明書ポリシ	1.2.392.100495.1.5.1.3.3.1
HPKI署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1
HPKI認証テスト用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.0.1
HPKI認証テスト用（組織）証明書ポリシ	1.2.392.100495.1.5.1.3.0.1

日本医師会認証局
サブCA鍵更新の再延長について

発生事象

① 「リモート署名サービスのHPKI-KAGURAにおけるHPKIカードを用いた認証」
② 「電子処方箋における一部ベンダーの署名共通モジュール」
において更新後の新CAのCRL（失効リスト）では旧CAで発行された証明書が失効確認できない。ただし、①HPKI-KAGURAについては対策を施して事象を解消予定。

確認依頼：日本医師会サブCA更新時の運用方法と実装について

②の対応について、電子処方箋では下記の形での実装を想定していることに対して、ご意見をいただきたい

- 鍵更新における運用において**「新たなサブCAを立てることは行わない」**
- RFC5280の解釈として**「issuer nameをチェックする実装を行う」**

※詳細は参考資料１にて説明

参考 RFC5280 6.1.1 Inputs　（抜粋）

(d) trust anchor information, describing a CA that serves as a trust anchor for the certification path. The trust anchor information includes:
(1) the trusted issuer name,
(2) the trusted public key algorithm,
(3) the trusted public key, and
(4) optionally, the trusted public key parameters associated with the public key.

The trust anchor information may be provided to the path processing procedure in the form of a self-signed certificate. When the trust anchor information is provided in the form of a certificate, the name in the subject field is used as the trusted issuer name and the contents of the subjectPublicKeyInfo field is used as the source of the trusted public key algorithm and the trusted public key. The trust anchor information is trusted because it was delivered to the path processing procedure by some trustworthy out-of-band procedure. If the trusted public key algorithm requires parameters, then the parameters are provided along with the trusted public key.

(d) トラストアンカー情報。認証パスのトラストアンカーとして機能するCAを記述します。トラストアンカー情報は次のとおりです。
(1)信頼される発行者名、
(2)信頼される公開鍵アルゴリズム、
(3)信頼される公開鍵、および
(4)オプションとして、公開鍵に関連付けられた信頼される公開鍵パラメータ。
トラストアンカー情報は、自己署名証明書の形でパス処理手順に提供することができます。トラストアンカー情報が証明書の形式で提供される場合、主体者名フィールドの名前が信頼される発行者名として使用され、subjectPublicKeyInfoフィールドの内容が信頼される公開鍵アルゴリズムと信頼される公開鍵のソースとして使用されます。トラストアンカー情報は、信頼できるアウトオブバンドの手順を通じてパス処理手順に配信されるため、信頼されているものとします。信頼される公開鍵アルゴリズムにパラメータが必要な場合、パラメータを信頼される公開鍵とともに提供します。

日本医師会認証局
サブCA鍵更新の再延長について

参考 RFC5280 6.3.3 CRL Processing　（抜粋）

This algorithm begins by assuming that the certificate is not revoked. The algorithm checks one or more CRLs until either the certificate status is determined to be revoked or sufficient CRLs have been checked to cover all reason codes.

(b) Verify the issuer and scope of the complete CRL as follows:
(1) If the DP includes cRLIssuer, then verify that the issuer field in the complete CRL matches cRLIssuer in the DP and that the complete CRL contains an issuing distribution point extension with the indirectCRL boolean asserted. Otherwise, verify that the CRL issuer matches the certificate issuer.

(f) Obtain and validate the certification path for the issuer of the complete CRL. The trust anchor for the certification path MUST be the same as the trust anchor used to validate the target certificate. If a key usage extension is present in the CRL issuer's certificate, verify that the cRLSign bit is set.

(g) Validate the signature on the complete CRL using the public key validated in step (f).

If the revocation status has not been determined, repeat the process above with any available CRLs not specified in a distribution point but issued by the certificate issuer. For the processing of such a CRL, assume a DP with both the reasons and the cRLIssuer fields omitted and a distribution point name of the certificate issuer. That is, the sequence of names in fullName is generated from the certificate issuer field as well as the certificate issuerAltName extension. After processing such CRLs, if the revocation status has still not been determined, then return the cert_status UNDETERMINED.

このアルゴリズムは、証明書が取り消されていないと想定することから始まります。アルゴリズムは、証明書のステータスが取り消されたと判断されるか、すべての理由コードをカバーするのに十分なCRLが確認されるまで、1つ以上のCRLを確認します。

(b)次のように、完全なCRLの発行者と範囲を確認します。
(1)DPにcRLIssuerが含まれる場合、完全なCRLの発行者フィールドがDPのcRLIssuerと一致し、完全なCRLに、indirectCRLブール値がアサートされた発行配布ポイント拡張が含まれていることを確認します。それ以外の場合は、CRL発行者が証明書発行者と一致することを確認します。

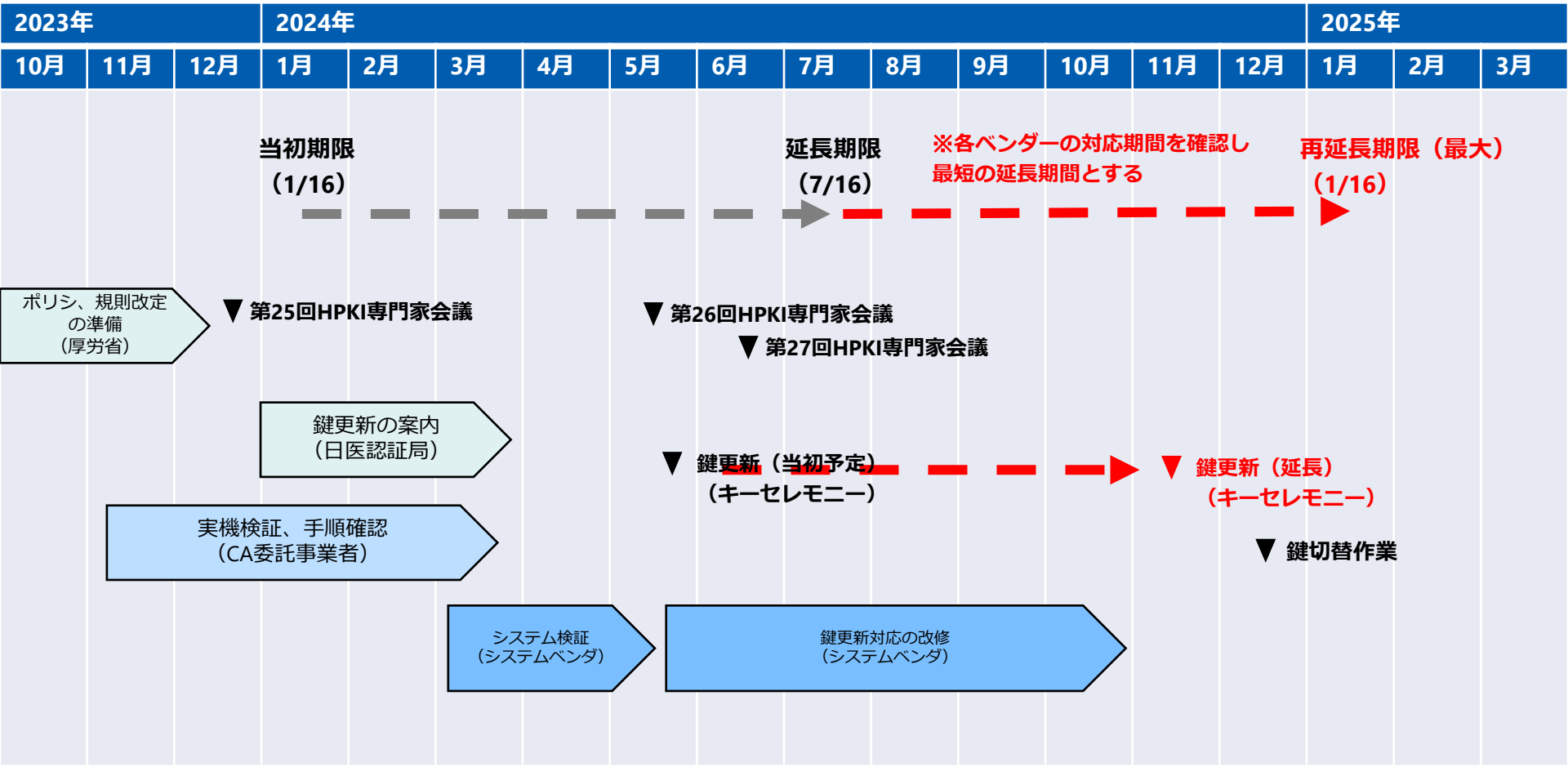
(f)完全なCRLの発行者の認定パスを取得して検証します。証明書パスのトラストアンカーは、ターゲット証明書の検証に使用されるトラストアンカーと同じである必要があります。鍵使用目的拡張がCRL発行者の証明書に存在する場合は、cRLSignビットが設定されていることを確認します。

(g)ステップ(f)で検証された公開鍵を使用して、完全なCRLの署名を検証します。

失効ステータスが決定されていない場合は、配布ポイントで指定されていないが証明書発行者によって発行された使用可能なCRLを使用して、上記のプロセスを繰り返します。このようなCRLの処理については、理由とcRLIssuerフィールドの両方が省略されたDP、および証明書発行者の配布ポイント名を想定します。つまり、fullName内の名前のシーケンスは、証明書発行者フィールドと証明書発行者AltName拡張から生成されます。そのようなCRLの処理後、失効ステータスがまだ決定されていない場合は、cert_status UNDETERMINEDを返します。

日本医師会認証局
サブCA鍵更新の再延長について

延長スケジュール案（最大）



1．日本医師会認証局 サブCA鍵更新

審議：更新の再延期について

2．HPKIリモート署名サービスに関して

議論：リモート署名サービス評価基準の今後の進め方について

3．連絡：ポリシー類の保守計画について

4．連絡：次回（第２７回）の予定について

HPKIリモート署名サービスについて

昨年度９月に公表させていただいた
「保健医療福祉分野におけるリモート署名サービス評価基準」について、
公表後も専門作業班にて文言等の細かな部分の修正作業を継続しております。

次回のMEDIS認証局準拠性審査前に改定を行うにあたり
昨年度からの環境変化、デジタル庁での調査研究事業の成果も踏まえ
本年度、専門作業班にて追加の改定作業、検討作業が必要かどうかご議論お願いします。

MEDIS認証局審査予定（リモート署名含む）：２０２５年３月予定

1.00版からの修正作業で対応済みのもの

- 昨年９月時点で反映しきれなかった指摘内容（誤記や表記揺れ等）
- その他の誤訳、表現の統一など

ご議論いただきたい点

- 議論を進める上での論点整理
- 昨年度作成した基準で不十分な点や議論を行うべき点はあるか
- 議論の進め方（例：ワーキンググループを作成して議論等）

１．日本医師会医認証局 サブCA鍵更新

審議：更新の再延期について

２．HPKIリモート署名サービスに関して

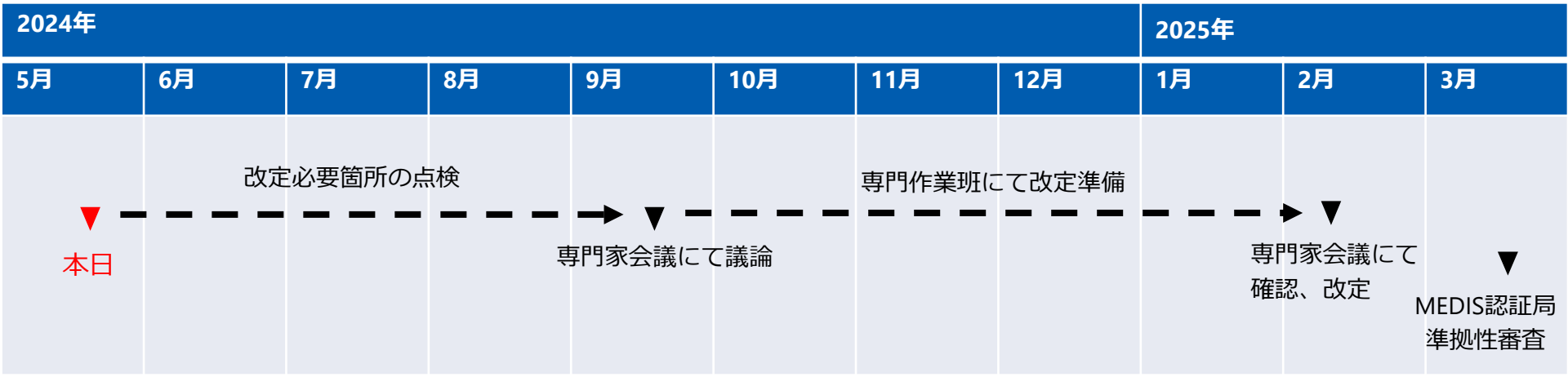
議論：リモート署名サービス評価基準の今後の進め方について

３．連絡：ポリシー類の保守計画について

４．連絡：次回（第２７回）の予定について

今年度のポリシー類保守計画について

昨年度の第25回専門家会議にて、リモート署名の状況も加味し、ポリシー類の見直しのご指摘をいただいております。
本年度に改定に向けた議論を下記のスケジュールで進めさせていただきたく、構成員の先生方にはポリシを確認いただき、ご意見の提出をお願いします。（ご意見取りまとめシートを追って配布いたします。）



<u>点検対象のドキュメント</u>

HPKI認証局証明書ポリシ（CP）

- 保健医療福祉分野PKI認証局署名用証明補ポリシ
- 保健医療福祉分野PKI認証局認証用（人）証明書ポリシ
- 保健医療福祉分野PKI認証局認証用（組織）証明書ポリシ

厚生労働省HPKIルート認証局運用管理規定（CP/CPS）

- 厚生労働省HPKIルート認証局運用管理規定

HPKI認証局証明書ポリシ準拠性審査手続規則・実施規則

- 保健医療福祉分野PKI認証局署名用・認証用（人）証明書ポリシおよび保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査手続規則
- 保健医療福祉分野PKI認証局署名用・認証用（人）証明書ポリシおよび保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査業務実施規則

前回いただいていたご意見（参考）

● **2nd鍵預かりについて、6.1.2 加入者への私有鍵の送付の項も修正を行った方がよいのではないか**

※鍵の預託については6.2.3項で記載

6.1.2　加入者への私有鍵の送付

エンドエンティティの加入者の私有鍵が認証局で生成される場合は、IETF RFC 4210「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、加入者に引き渡されるものとする。認証局はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする。

● **鍵の更新という表現ではなく、鍵の切り替え等の表現のほうが適切ではないか**

（民法では、更新とは、「従前の賃貸借と同一の条件で更に賃貸借をしたもの」）

１．日本医師会認証局 サブCA鍵更新

審議：更新の再延期について

２．HPKIリモート署名サービスに関して

議論：リモート署名サービス評価基準の今後の進め方について

３．連絡：ポリシー類の保守計画について

４．連絡：次回（第２７回）の予定について

第２７回HPKI専門家会議　予定

開催日時：６月２０日（木）　１０：００～１２：００
場所：AP虎ノ門　Bルーム　（オンライン同時開催）

<u>議題予定</u>

- ルート認証局　準拠性審査結果報告
- 日本医師会認証局　準拠性審査結果報告
- 日本薬剤師会認証局　準拠性審査結果報告
- HPKIリモート署名サービスの利用用途限定の扱いについて