

令和 8 年 3 月 2 日

次期HPKI認証局の構成に係る提案

2026年3月2日

日本医師会電子認証センター

日本薬剤師会HPKI認証局

医療情報システム開発センター

提案趣旨

- HPKI認証局は、厚生労働省(厚労省)の定める「HPKI証明書ポリシー」に則り運営されるもの。
- その準拠性に関しては、HPKI専門家会議により選定される審査班により審査を受ける。
- このため、HPKI認証局になろうとする者は限定されている訳ではなく、希望すれば準拠性審査を受けてHPKI認証局を運営できる。
- ところが、実態としては、HPKI認証局を運営する者は、医師用電子証明書を発行する日本医師会(日医)、薬剤師用電子証明書を発行する日本薬剤師会(日薬)、27の医療国家資格の電子証明書を発行するMEDISの3者のみ。
- 更に、日医と日薬は発行局(IA)を共有していることから、実際のIAは日医とMEDISの2つ。
- この実態を踏まえて、**ルート・サブ認証局構成を廃し、厚労省ルート認証局に集約**。一方で、登録局(RA)業務は、準拠性審査により参入門戸を開きつつ、これまで通り、日医、日薬、MEDISが担う構成としてはどうか。

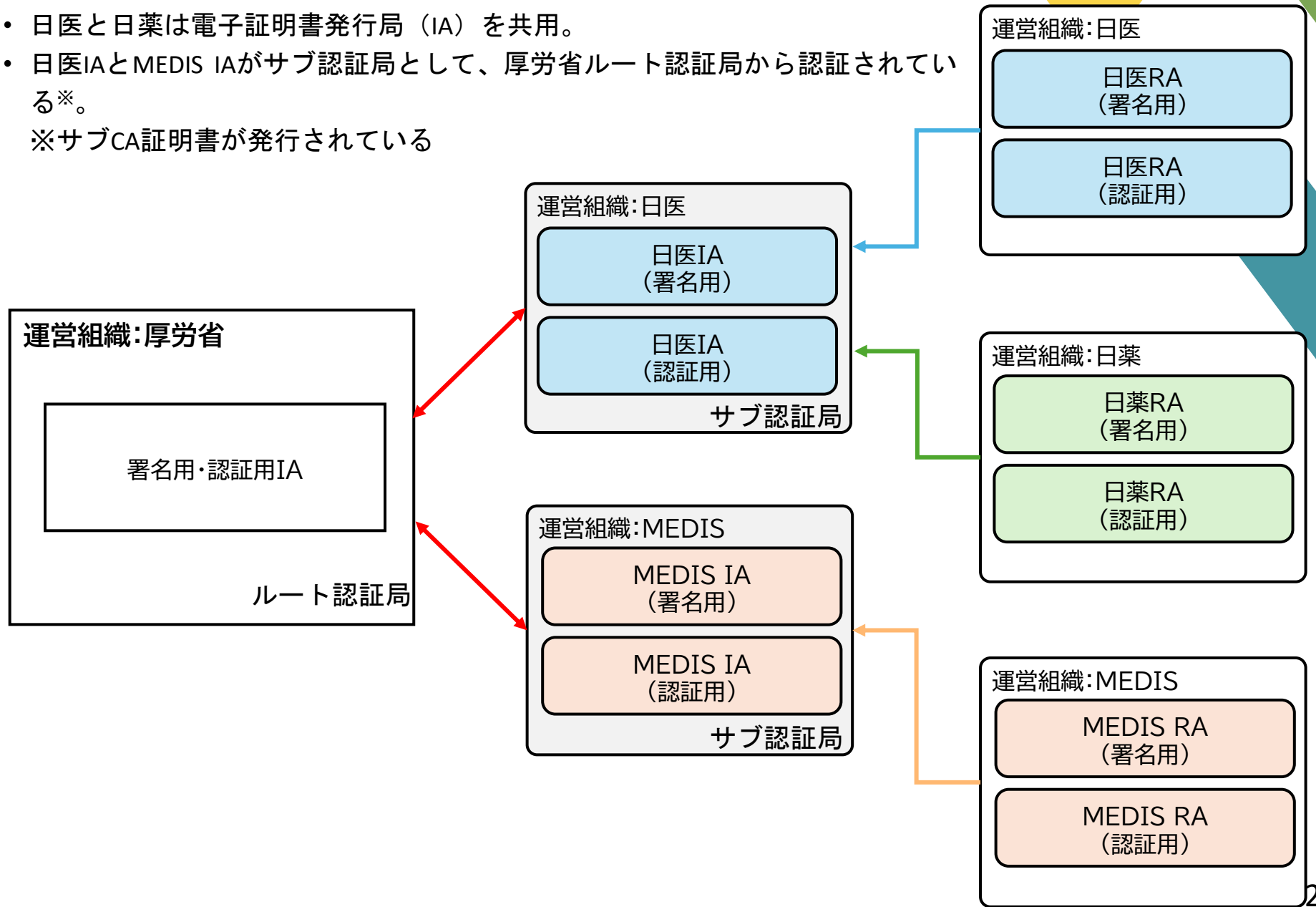
加えて、以下も提案する理由。

1. ルート・サブ認証局構成のため、サブCA中間証明書を各医療情報システムに設定する必要があるが、仕組みを理解していない医療情報システムベンダーも散見され、システム構築時のトラブルも見受けられる。
2. 先のサブCA鍵更新は、ルート・サブ認証局構成を取っていたがために、あまり前例がなく対応に苦慮することになり、一部医療情報システムベンダーが、署名検証に対応できない事態を招いた。
3. 政府系認証局との相互接続、特にJPKIとの相互接続もルート・サブCA認証局構成の場合、前例がないため実現可能性が低いが、ルート単独構成にすることでGPKIブリッジを通じて相互接続の実現可能性が高くなる。
4. これにより、HPKIの全体最適化を図り、HPKIに係るトータルコストを低減させ、政府全体の認証局との整合性も確保することが可能となる。
5. JPKIとHPKIの連携が図れれば、医療で大事な要素の一つである「本人であること」を患者・医療者双方で担保することができ、医療DXの安全・安心にも寄与する。

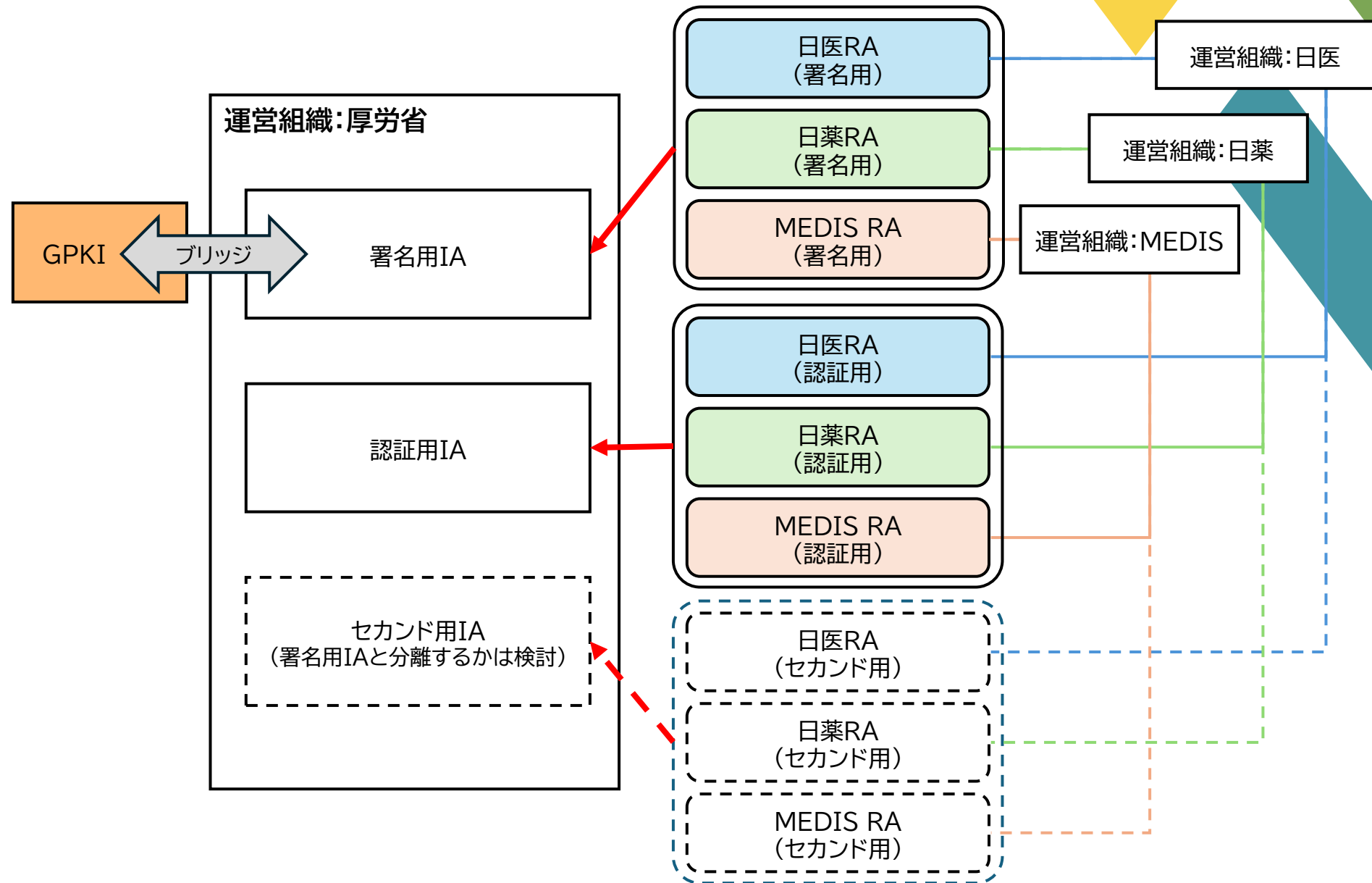
現在のHPKI認証局の構成

- 日医と日薬は電子証明書発行局（IA）を共用。
- 日医IAとMEDIS IAがサブ認証局として、厚労省ルート認証局から認証されている※。

※サブCA証明書が発行されている



HPKIルート単独構成案(機能別)



【ルート単独構成時の変更点】

- 厚労省は一つのルート認証局(IA)を保持していたところ、少なくとも署名用・認証用の2つのIAを保持することになる。
- RAは、申請者(医師等)からの申請を受けて、IAに電子証明書発行要求をするだけのため、これまでと大きな変更なし。

【課題】

- IAが発行要求を受けて電子証明書を発行する処理をどうするか？
(案1)厚労省が自ら人員・予算をかけて発行する(当然、実際は外注)
(案2)各運営組織(日医・日薬・MEDIS)への委託という形を取り、IAの利用権限を付与して、実作業を各運営組織が実施する。
(案3)RAからの発行依頼を受けて、自動で電子証明書を発行できる仕組みを構築する。
- 案1を除けば、厚労省IAは電子証明書を生成だけすればよく、ICカードへの書き込みやクラウド基盤(KAGURA)への格納などの処理は、これまでと変わることなく各運営組織が予算を組み実施する形が取れば課題解決は可能。
- また、各運営組織もIAを抱えずに済むため、経費の削減が見込め、その分、新たな投資(支出)もできるようになる。

【GPKIブリッジについて】

- GPKIとのブリッジは署名のみ。
- ブリッジすることにより、JPKIとの連携、JPKIの活用がより容易になる。

【参考】HPKIルート単独構成案(組織別)

