

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  
議事概要

○ 日時：令和 6 年 5 月 20 日（月）10：00～12：00

○ 場所：AP 虎ノ門 B ルーム

○ 議題

- (1) 日本医師会認証局サブ CA 鍵更新
- (2) HPKI リモート署名サービスに関して

○ 議事概要

事務局より資料 1 に沿って各議題の概要を説明し、各構成員による自由討議が行われた。

・ 日本医師会認証局サブ CA 鍵更新について

日本医師会認証局の鍵更新準備において署名検証が行えないケースがあること、改めてサブ CA における鍵更新方法について現状の想定内容が事務局より報告され、専門作業班構成員より参考資料 1 を用いて「鍵交換時の処理について」具体的な解説がされた。

○ 鍵更新方法についてはリンク証明書の有無や IETF RFC5280 に準拠した実装について議論がされ、HPKI としてはサブ CA における鍵更新においてリンク証明書を使用しないことが決定された。

○ その他の内容については本日時点で判断がつかないため、早急に次回会議を開催し議論を継続することとした。

・ HPKI リモート署名サービス評価基準について

事務局より昨年度制定した、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、継続した保守を行っていくことが説明され、今年度も継続して議論を行い、改定に向けた検討作業を行うことが承認された。なお、具体的な進め方やスケジュールについては次回以降の会議で議論することとし持ち越しとなった。