第27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6月11日（火）18：00～20：00

○場所：TKP 新橋 ホール 16A

○議題

（1）CA 鍵更新に関して

○議事概要

事務局より資料1に沿って第26回の議論の振り返りとサブCA鍵更新に対する複数の案が示された。その後、専門作業班構成員よりサブCA鍵更新に関する専門的な解説がされ、これを受けて各構成員による自由討議が行われた。なお、議事内容に係るものとして、臨時専門作業班構成員として新井聡構成員、JAHISより新垣淑仁オブザーバーが本会議へ参加した。

・HPKIにおけるサブCA鍵更新について

サブCA鍵更新の方法が議論され、下記の通り進めることが決定された。

○鍵更新方法としては資料1のC案として進める。HPKIとしては運用上で鍵の切替を行うA案はポリシ上問題ない。サブCAシステムを新規構築し並行運用するB案は現行ポリシでは運用できないため、対応可能となるようにポリシ改定等の議論を継続して行う。

○A案の場合は個別のベンダーが対応する必要があるため、実装ガイドの周知など、配慮の必要がある。

○将来的な暗号移行の対応も想定し、B案に近い運用についてもHPKIとして可能とできるように認証局ポリシだけでなくルート認証局CP/CPSの改定も進めること。本改定に対する、CP/CPS含めドキュメント改定の検討は、必要な対応の確認後に改めて事務局より連絡を行うこととする。

○HPKI認証局における発行者（Issuer）やトラスアンカー、リンク証明書のあり方、暗号移行における実施方法など、運用における定義や規定については継続した議論を行い、取りまとめを行っていく。

・日本医師会認証局のサブCA鍵更新について

上記の議論を受けて、下記のとおり進めることとなった。

○日本医師会認証局のサブ CA 鍵更新は、2025 年 1 月 16 日まで期限を延長することが承認された。

○日本医師会認証局より、今回のサブ CA 鍵更新は A 案の形で進めることが、連絡された。