

次期認証局の構成について

第35回公開鍵基盤認証局の整備と運営に関する専門家会議 2026（令和8）年3月2日(月)

厚生労働省 医政局

参事官（医療情報担当）付医療情報室

Ministry of Health, Labour and Welfare of Japan

次期認証局の構成について

次期HPKI認証局の構成の検討に係る背景

- HPKI暗号アルゴリズムの移行期間にさしかかり、CRYPTRECの電子政府推奨暗号リストを踏まえ、現行の112bitセキュリティ強度暗号からの移行を2030年内に確実に完了し、安定稼働することが必要である。
- これを受け、HPKI専門家会議では次期暗号アルゴリズム移行に係る議論を行っているところ、次期暗号アルゴリズムに対応したHPKI認証局のシステム構築が必要である。
- 次期暗号アルゴリズムに対応したHPKIカードのICチップの開発及びHPKIカードドライバの開発等に2～3年を要する見込みであり、関連する後続システムである電子処方箋管理サービスや医療機関等システムの改修期間も一定必要となることから、次期HPKI認証局の構成を早期に決定する必要がある。

本日議論頂きたい内容

本日は、次期HPKI認証局の構成について、日本医師会・日本薬剤師会・MEDIS案および事務局案を踏まえ、ご議論いただきたい。

次期認証局の構成に対する事務局案

- これまでHPKI専門家会議での議論では、「現行のルート認証局・サブ認証局という構成からルート認証局単独構成とするのは如何か」とのご意見を頂戴し、本日も、日本医師会、日本薬剤師会、MEDISから具体的な提案をいただいた。
- より効率的・安定的な運用のあり方を検討し、対応することは、事務局としても重要な課題と認識している。
- 一方で、現在のルート認証局が担っているサブ認証局に証明書を発行する役割から、サブ認証局が現行担っているエンドエンティティ向けの証明書も発行することになれば、HPKIの制度的位置づけや公共性に関する整理、その場合のRA業務の取扱いの整理等を行い、その上で、必要な法制面の取扱いも含めた対応、費用負担のあり方等についても整理・調整することが必要となり、相応の期間を要する可能性がある。
- 電子処方箋など医療DXの各種サービスが順次実装されていくなか、HPKIの継続性と安定稼働は必須であり、まずは確実に暗号移行する必要があるが、認証局構成の検討にこうした時間を要することになれば、今後、ルート・サブの認証局対応だけでなく、医療機関等でのシステム改修等も必要になる中、暗号移行のスケジュールが切迫し、移行遅延のリスクを高めるおそれがある。
- 現行構成は、サブ認証局が医師等ユーザの審査・証明書発行等を担うことで、ルート認証局をオフライン環境で運用することができ、HPKIの信頼の起点であるルート認証局の安全性を確保している。
- また、HPKI証明書ポリシーに基づく各認証局のCPSが整備されていることによる制度面の信頼性に加え、運用実績や定期的な準拠性審査によって運用面の信頼性・安定性も担保されている。

【事務局提案】

- 次期HPKI認証局の構成については、国がルート認証局を担い、サブ認証局が医師等ユーザの審査・証明書発行等を担う現行構成を維持し、来年度早期から移行に向けて準備を開始するのが妥当と考えている。
- 一方で、現行構成は社会的コストが大きいことも事実であることから、医療DX全体の施策や技術動向も踏まえながら、ルート認証局単独構成についても将来的なあり方としては引き続き検討を行うこととしたい。