

厚生労働省 HPKI 認証局の構築・運営事業について(案)

1. 趣旨

ネットワーク上の情報の改ざん、なりすまし等を防止するために、医師等の個人が電子署名を活用できるよう、公的資格等の確認機能を有する保健医療福祉分野の公開鍵基盤(ヘルスケア PKI: HPKI)が整備される必要がある。既に平成 17 年 3 月には「保健医療福祉分野 PKI 認証局証明書ポリシー(以下、共通ポリシー)」が策定され、HPKI の共通基盤の一部が整備された。平成 18 年度には、これらの基盤の一層の充実を目的として、個別認証局が共通ポリシーに準拠した形で電子署名を発行することが可能となるよう、厚生労働省に HPKI 認証局(仮称)を構築し、個別の HPKI 認証局に対して、共通ポリシーへの準拠を示す証明書を発行する事業を開始する。

2. 事業の概要

- ① 平成 18 年度に共通ポリシーに準拠した「厚生労働省 HPKI 認証局(以下、厚労省 HPKI CA)」を構築する。
- ② 「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(専門家会議)は本事業の実施にあたり専門的な見地から意見、助言を行う。
- ③ 厚労省 HPKI CA は共通ポリシーに準拠した個別認証局あるいはその中間認証局に対し、相互認証を可能とする仕組みを提供する。
- ④ その他に厚労省 HPKI CA は、自身の公開鍵証明書、CRL/ARL、CP/CPS 等の文書を公開する。

厚労省 HPKI CA を介して個別認証局が相互認証するにあたっては、あらかじめ共通ポリシーへの準拠について書面・実地調査等により確認する。当該調査は、専門家会議の要請に基づき、専門作業班が主体となって行う。専門家会議は専門作業班の報告に基づき、準拠性の確認を行い、厚生労働省ホームページに公表する。

3. 実施スケジュール

- ① 平成 18 年度は実証フェーズとし、個別認証局の共通ポリシー準拠性の審査手続及び厚労省 HPKI CA による認証業務についてのフィージビリティ検証を主な目標とする。
- ② 平成 18 年度前半に「共通ポリシー」「準拠性監査報告書様式」に基づく準拠性の審査手続を検証し、個別認証局に対する一般的な審査手続規則の策定を目指す。
- ③ 平成 18 年度後半に、厚労省 HPKI CA の個別認証局に対する認証業務について検証し、共通ポリシーへの準拠を示す証明書の発行が可能となることを目指す。
- ④ 平成 19 年度は運用フェーズとし、厚労省 HPKI CA 構築・運営事業に参画することを希望する個別認証局からの専門家会議に対する審査申請の受け付け開始を目指す。専門家会議により準拠性が確認された場合、HPKI 個別認証局として本事業に参画する。

4. 実施体制

平成 18 年度当初の実証フェーズにおける個別認証局として、日本医師会 CA、MEDIS CA への協力を依頼する。

5. 留意点

- ・本事業に参画する個別認証局は独自事業として認証局の運営を行うものとする。また電子署名法の定める認定認証事業者であることは要件としない。
- ・専門家会議による確認は、個別認証局が共通ポリシーに準拠し本事業に参画していることを表示する以外に、何らの権利義務等を生じせしめない。
- ・認証業務上の責任については、共通ポリシー「9.7 無保証」、「9.8 責任制限」、「9.9 補償」に従い、個別認証局が負う。
- ・厚労省 HPKI CA の CP/GPS を策定する際には、厚生労働省の法的な責任範囲等についても留意しつつ検討を進める。
- ・平成 18 年度の本事業に係る予算は、厚生労働省が担当する HPKI CA の構築及び専門家会議による個別認証局の準拠性審査に係る経費である。

厚生労働省医政局 平成18年度当初内示の概要(抜粋)

6. 医療のIT化の着実な推進

- 保健医療分野の公開鍵基盤(PKI)認証局の構築・運営(新規)

19百万円

安全かつ円滑な診療情報共有を実現するため、電子署名自体が医療従事者の公的資格の確認機能を有する、保健医療分野に適した公開鍵基盤の整備を行う。

「保健医療福祉分野 PKI 認証局 証明書ポリシー」について

◇ 証明書ポリシーとは

『証明書ポリシー (CP : Certificate Policy)』とは、電子証明書を発行する認証局に対して、「電子証明書の適用範囲」「審査の基準」「設備の基準」などの運用に係わる規則を定めるもの。

◇ 保健医療福祉分野 PKI 認証局 証明書ポリシーとは

様々な組織の認証局が存在する中で、保健医療福祉分野で PKI 認証局を運用しようとする組織が、共通に準拠すべき証明書ポリシー。(以下、「共通ポリシー」。)

◇ 共通ポリシーの役割

様々な電子証明書を活用したサービスがあるが、当該共通ポリシーは、電子証明書による「電子署名」を対象。

※この共通ポリシーに則って発行された電子証明書は、コンピュータやホームページの会員ページへの入室などの「認証」及び「暗号化」の用途には利用不可。

また、当該共通ポリシーは、証明書を発行する際の厳密な本人確認や医療従事者としての資格確認、安全基準及び後述の hcRole を含む証明書の様式を定めており、これに準拠していることが示されれば、異なった認証局で発行された証明書でも同じ安全性のレベルが確保されている証明書として共通の信頼性のもとに運用することが可能。

◇ 共通ポリシーの特徴

共通ポリシーに則って発行された電子証明書内には、保健医療福祉分野の国家資格（医師、歯科医師等）と医療施設等の管理者の属性を格納できる。

通常の電子証明書では、そこから読み取れる情報は、氏名・住所・年齢等の個人に関する情報に限られているが、共通ポリシーでは資格専用の領域を確保して、そこに国家資格等の属性を格納するようにした。

この専用の領域を「hcRole」と呼び、国際標準化機構 (ISO : International Organization for Standardization) の技術委員会 (TC) 215/WG4 にて

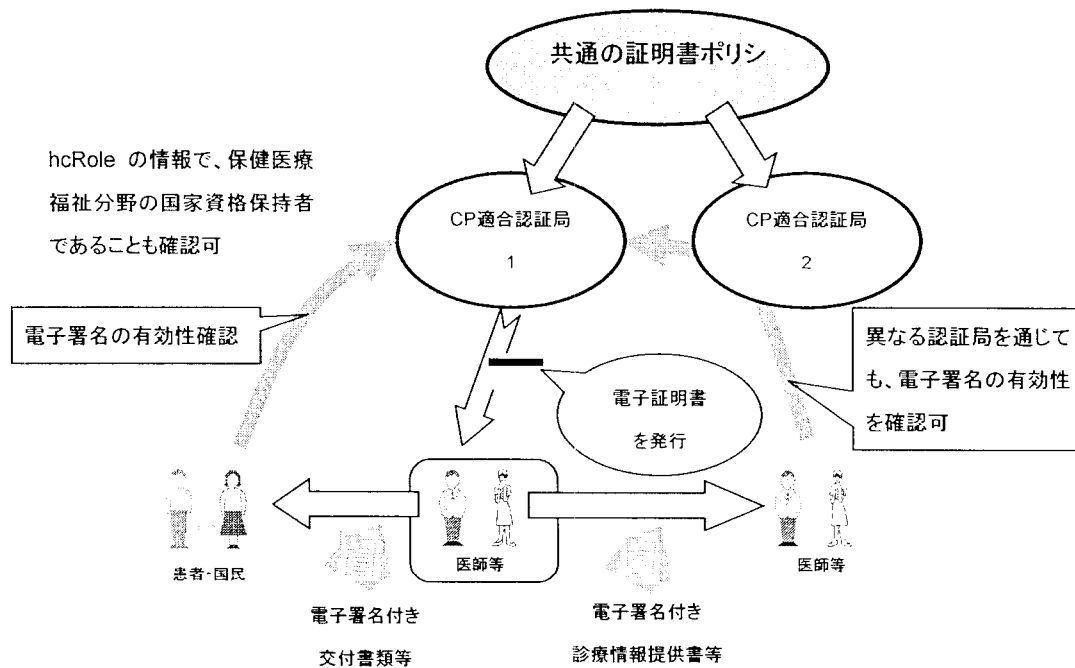
協議されており、hcRole を含む規格名「ISO TS 17090」は、2005 年中に正式な国際標準規格（IS）となる予定。

◇ 保健医療福祉分野 PKI 認証局として共通ポリシーを定めることの意義

共通ポリシーに準拠した認証局が発行した電子証明書による電子署名であれば、どの認証局が発行した電子証明書による電子署名であっても、その有効性を確認（検証という）することが可能。

このような基盤が整備された場合、医師等の作成する電子的な医療関係書類に署名が付されていれば、その書類を受け取った医療従事者や患者等は、日本全国で有効性の検証が可能。また、保健医療福祉分野の資格保持者が作成した書類であるということも直接確認できるようになる。

信頼できる電子情報を取り扱えることから、医療分野における電子紹介状や電子カルテなど様々な具体的な用途への展開が考えられる。



図：保健医療福祉分野共通の証明書ポリシーに準拠した認証局の運営（イメージ）