資料　２

平成２５年５月１６日

「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」における検討事項ついて

○ 厚生労働省 HPKI 認証局の構築・運営事業について

↓

厚生労働省 HPKI 認証局における認証機能の追加

従来より、厚生労働省 HPKI 認証局においては、電子署名による基盤が構築されているが、今年度、新たに電子認証の機能を追加し、推奨される暗号技術（SHA-256）に対応した認証局を構築する。

そのため、本専門家会議において以下について審議を行う。

①暗号技術の進展に対応した認証用の HPKI 認証局証明書ポリシの改定

②署名用の HPKI 認証局証明書ポリシについても、暗号技術の進展に対応した改定

③構築した認証局が HPKI 認証局証明書ポリシに準拠していることを確認

電子署名…そのデータを作成・記録した利用者が誰で、どういう資格を持つか、その後の書き換えがないかを確認できます。**→改ざんの防止・否認の防止**

電子認証…そのシステムにアクセスしようとしている利用者は誰で、どういう資格（医療関連の国家資格）を持つかを確認できます。**→なりすましの防止**

証明書ポリシ…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です。

認証局…電子証明書を発行する機関であり、その電子証明書が本人のものであると証明する機関です。

HPKI 認証局証明書ポリシ…様々な認証局が存在する中で、保健医療福祉分野で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です。

HPKI 認証局証明書ポリシの特徴…通常の証明書ポリシに則って発行された電子証明書では、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、HPKI 認証局証明書ポリシに則って発行された電子証明書では、保健医療福祉分野の国家資格（医師、歯科医師等）を確認できます。

暗号技術（SHA-1）…認証やデジタル署名などに使われる技術のひとつです。通信途中で原文が改ざんされていないかを検出することができますが、コンピュータの処理能力と暗号解読技術の向上により、安全性の低下が指摘されています。

暗号技術（SHA-256）…SHA-1 を踏襲し開発された技術です。SHA-1 よりも安全性が高いとされています。電子政府推奨暗号のひとつとされています（平成 25 年 3 月時点）。