資料１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第３２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

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

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

5．連絡事項

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

5．連絡事項

MEDIS認証局　鍵更新結果の報告

MEDIS認証局サブCA鍵更新

- 2025年2月14日　　キーセレモニーを実施（立会）
- 2025年3月17日　　新鍵の切り替えを実施（立会）

キーセレモニー、新鍵の切り替え時にHPKI専門家会議にて指定した立会人の元で作業実施
システムトラブル等なく、鍵更新完了
電子処方箋での運用においてもトラブル等の発生報告はあがっていない

立会人

チェックリストを使用し、立会を実施

丸山　満彦	**PwCコンサルティング合同会社　パートナー**
六川　浩明	**内幸町国際総合法律事務所　弁護士**

立会結果

全てのチェック項目に対し問題なく鍵更新作業完了を確認
参考資料２参照

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

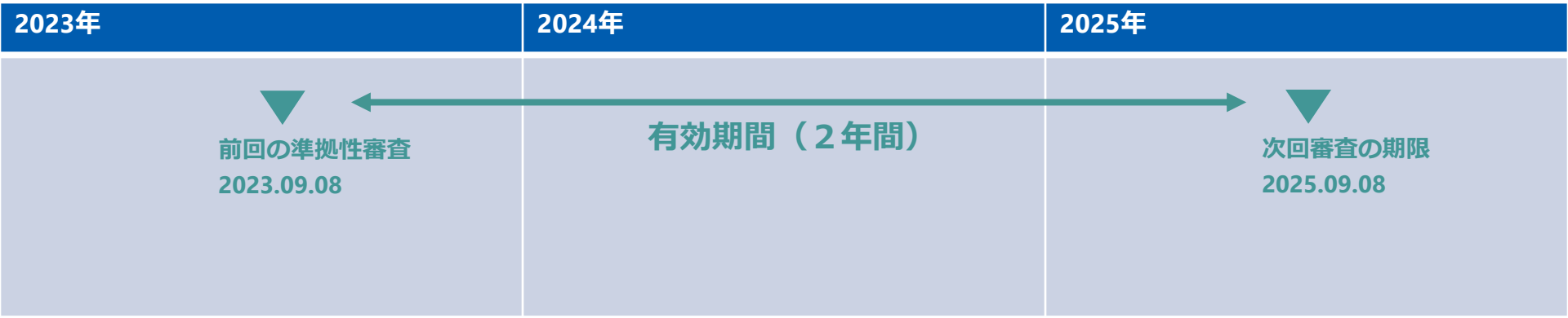
5．連絡事項

MEDIS認証局 準拠性審査班の指名

MEDIS認証局の有効期間は2025年9月

審査対象

- HPKIサブ認証局
- HPKIリモート署名サービス（鍵管理サービス）
- HPKIリモート署名サービス（デジタル署名生成サービス）



審査班の指名

審査班として下記２名にご対応を依頼させていただきたく審議お願い致します。

丸山　満彦	PwCコンサルティング合同会社　パートナー
六川　浩明	内幸町国際総合法律事務所　弁護士

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

5．連絡事項

厚生労働省組織名変更に伴うドキュメント改訂

厚生労働省組織名変更に伴い、以下のドキュメントを一律改訂させていただきます。

変更箇所

問い合わせ先記載

変更前：厚生労働省　医政局参事官（特定医薬品・医療情報担当）付医療情報室

変更後：厚生労働省　医政局参事官（医療情報担当）付医療情報室

改訂ドキュメント（資料2-1～2-6）

- 保健医療福祉分野PKI認証局署名用証明書ポリシ
- 保健医療福祉分野PKI認証局認証用（人）証明書ポリシ
- 保健医療福祉分野PKI認証局認証用（組織）証明書ポリシ
- 保健医療福祉分野PKI認証局署名用・人法要（人）証明書ポリシおよび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準拠性審査手続き規則
- 保健医療福祉分野PKI認証局署名用・認証用（人）証明書ポリシおよび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準拠性審査業務実施規則
- 厚生労働省HPKIルート認証局運用管理規定

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

5．連絡事項

前回議論の振り返り

● **次期暗号方式について**

- GPKIと足並みを揃え、ECDSA（鍵長384ビット、192ビットセキュリティ）への移行を前提として、必要な調査等を実施していくこととした。

● **暗号アルゴリズム移行に向けた線表（計画）について**

- CPの改定時期、**認証局の構成、次回**鍵更新や検証側の状況やコスト等にも鑑みて、線表を検討していくこととした。

● **暗号アルゴリズム移行に係る今後の議論について**

- 次回の段階で調査が完了した部分について、厚労省より提示し、引き続き本専門家会議において議論を行うこととした。

検討、調査状況

GPKIにおけるECDSAの選定理由の確認

デジタル庁へ確認を行った結果、下記の理由によりECDSAを選定したとのこと

- デジタル庁において事業者及び民間認証局等へのヒアリングを実施し決定
- 128ビットセキュリティの場合、2041年～移行完遂期間となるため、利用出来る期間が短い
- このため、192ビットセキュリティのECDSA P-384を選択している
- 192ビットセキュリティのRSAの場合は鍵長が4096ビットより大きくなり、ICカードや対応しているシステム等が少ないこと、処理時間が増加することなどの懸念があったため未採用としている

今後の調査項目案

関係者等	暗号移行によるシステム影響等	調査項目案
認証局	**証明書発行プロセス等** • 発行局が証明書を発行する際に利用する証明書プロファイルの設定変更 • 移行期間における旧証明書との同時運用を考慮したプロセスの変更 **鍵生成及び鍵管理** • 鍵生成に係る手順 • 鍵バックアップに利用するユーティリティの変更及び鍵管理で利用されるHSMの更新 **HPKIカード** • 新証明書に対応したHPKIカードの発行及びCC認証（ISO/IEC 15408）の新規取得	• **暗号移行によるシステム上の変更等において支障となる点や懸念点** • これら以外に生じ得る影響とその懸念点等
署名者	**署名プロセスに係る影響** • システム内に実装された電子署名を行うためのアプリケーションや証明書を読み込むためのライブラリの導入又は変更 • HPKIカードでの署名実施の際に利用するカード読み取り機器やクライアントアプリケーションの導入又は改修 **システムに係る影響** • 署名生成に係る計算処理時間の長期化を考慮したシステムパフォーマンスの向上 • 新証明書への互換性が無いシステムの改修	• **暗号移行によるシステム上の変更等において支障となる点や懸念点** • **次期暗号方式への互換性がないシステム**の存在有無 • これら以外に生じ得る影響とその懸念点等

今後の調査項目案

関係者等	暗号移行によるシステム影響等	調査項目案
検証者	**検証プロセスに係る影響** • 署名検証に係るロジックの変更 • 検証時に利用する署名検証用ライブラリの導入又は変更 • 署名検証に係る計算処理時間の長期化を考慮したシステムパフォーマンスの向上	• **暗号移行によるシステム上の変更等において支障となる点や懸念点** • **次期暗号方式への互換性がないシステム**の存在有無 • これら以外に生じ得る影響とその懸念点等
関係するサービス等	**電子処方箋管理サービスや電子カルテ共有サービスへの影響** • 署名検証に係るロジック及び署名検証用ライブラリの導入又は変更 • 新証明書で署名された電子処方箋の保管に係る管理システムやデータベースの導入又は変更 • 署名生成又は署名検証に係る計算処理時間の長期化を考慮したシステムパフォーマンスの向上 **HPKIセカンド電子証明書** • 新証明書をクラウド保管するための設定変更	• **署名検証ロジックが実装されている場合のシステム内変更点や懸念点** • 次期暗号化方式へ移行した場合のシステム全体への**パフォーマンスに係る懸念点** • 左記以外に影響を受ける関連サービスや懸念点

調査方法

関係者等	想定される確認先
認証局	• 現ルート認証局委託先事業者、サブ認証局と確認
署名者	• JAHIS（保健医療福祉情報システム工業会）を通じ、医療情報システムベンダーと確認
検証者	• JAHIS （保健医療福祉情報システム工業会）を通じ、医療情報システムベンダーと確認
関係するサービス等	• 電子処方箋管理サービス、電子カルテ情報共有サービスの運営主体である社会保険診療報酬支払基金と確認

1．MEDIS認証局　鍵更新結果の報告

2．MEDIS認証局　準拠性監査審査班の指名

3．厚労省組織名変更に伴うドキュメント改訂

4．暗号アルゴリズムの移行に関して

5．連絡事項

連絡事項

次回、第33回HPKI専門家会議について

2025年7月頃の開催を予定
別途日程調整のご案内を致します。

今年度の専門家会議議題案

適宜、事務局より議題としてご提示いたします。

- 暗号アルゴリズムの移行について
- システムリプレイスに伴うルート認証局含む認証局体制の再編等検討
- CP等ドキュメントのアップデート
- 今後の準拠性審査及び認証局監査のあり方について
- リモート署名サービス評価基準の適用範囲拡大の検討