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３３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

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

Ministry of Health, Labour and Welfare of Japan

1．MEDIS認証局 準拠性審査の実施について

2．暗号アルゴリズムの移行に関して

3．耐量子計算機暗号（PQC)について

4．連絡事項

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

1．MEDIS認証局 準拠性審査の実施について

2．暗号アルゴリズムの移行に関して

3．耐量子計算機暗号（PQC)について

4．連絡事項

MEDIS認証局 準拠性審査の実施について

審査スケジュール

2025年8月4日

審査班

下記２名に決定

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**

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）

審査方法

書類審査及び実地調査により審査いただく。
今回の審査からチェックリストを用いて書類審査及び実地調査を実施する予定。

本日の協議事項

今回の審査からチェックリスト案（資料2-1~2-2）を利用することについて、ご審議をお願い致します。

1．MEDIS認証局 準拠性審査の実施について

2．暗号アルゴリズムの移行に関して

3．耐量子計算機暗号（PQC)について

4．連絡事項

前回議論の振り返り

●次期暗号方式について

- 次期暗号方式への移行に向けた調査項目や検討すべき事項に関して議論を行った。
- 耐量子計算機暗号(PQC)への移行可能性に関して議論を行った。

●暗号アルゴリズム移行に係る今後の議論について

- 次期認証局構築の要件検討にあたり、関係者への調査を実施し、対策方針の検討を進める必要がある。
- 調査が完了した部分から順次結果を提示し、引き続き本専門家会議において議論を行うこととした。

※PQCに関する議論は、次議題にて協議予定

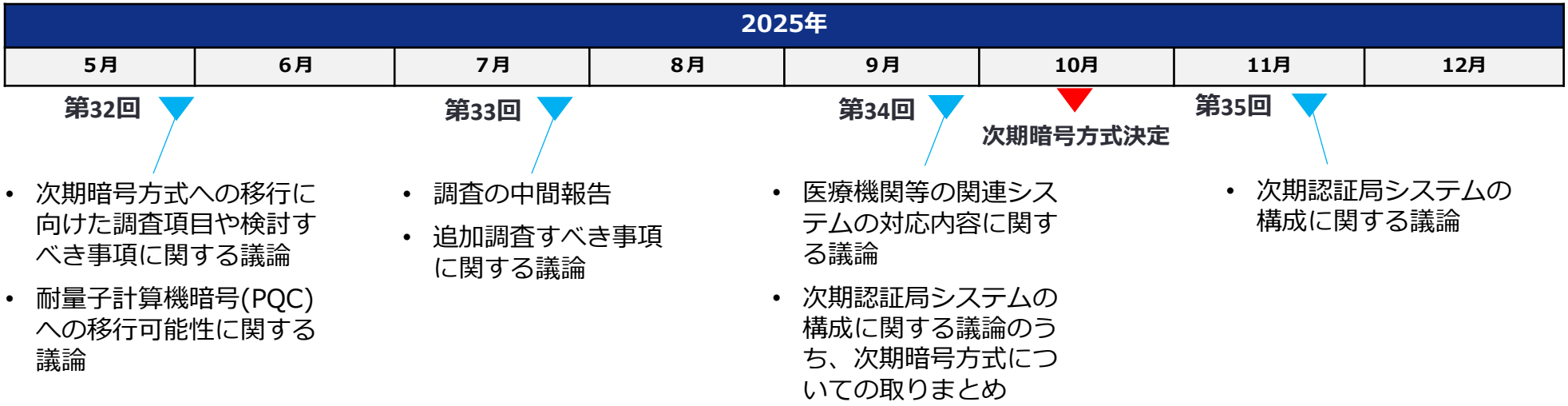
本日の議論に向けたポイント

●本日の議論における到達目標について

- 前回整理した調査項目や検討すべき事項に関して、関係者への調査を進めており、本日は調査の中間報告を行います。
- 本日は中間報告を踏まえて、追加調査すべき点があるか等について議論頂きたいと考えています。
- 追加調査が必要な場合は、要点を整理のうえ、事務局で持ち帰ったうえで、次回目処で報告する予定です。

●今後の本専門家会議における議論のスケジュールについて

- 年内には次期暗号方式を決定したいと考えています。
- 次期暗号方式の決定に向けた本専門家会議における議論のスケジュール（予定）は次のとおりです。



調査状況の報告

調査先等		調査項目	調査結果
認証局	日本医師会	• サブ認証局への影響や懸念点 • 旧暗号方式と新暗号方式の並行運用期間中における問題発生リスク • 特に懸念すべきシステム影響	ヒアリング中
	日本薬剤師会		■HPKIカードへの影響 • 暗号方式およびチップ内の仕様が決定されて初めて、カードの開発、ICチップの調達、カード製造の工程が始まる。 • カード開発には1-2年みる必要あり。また、認証局としては、発行局（IA)において、カードの書込/印刷を行うプリンターの調達、ICチップへの書き込みを行うツールの開発、HPKIカードドライバの開発等の対応が必要。 • ICカード製造は、1年近くかかる可能性あり。 • これら開発期間・納品期間を踏まえ、仕様決定から暗号方式切り替えまでのスケジュールを組むことが必要。 ■旧暗号方式と新暗号方式の並行運用期間に係る考慮事項 • ドライバに関して新旧暗号方式に対応するようベンダーへ周知することが必要。 • 新暗号方式への対応にかかる技術的問合せ対応窓口の設置及びベンダーへの周知が必要。 • 発行データの出力内容に変更がある場合、データ出力機能の改修が必要。 • 登録局と発行局間での切り替えにかかるテスト、切り替え実施も連携して実施することが必要。

調査状況の報告

調査先等		調査項目	調査結果
認証局	MEDIS	• サブ認証局への影響や懸念点 • 旧暗号方式と新暗号方式の並行運用期間中における問題発生リスク • 特に懸念すべきシステム影響	■証明書発行プロセス等への影響 • 証明書プロファイルの設定変更が必要。 • 構築事前の新暗号方式の検証環境が必要。 ■鍵生成及び鍵管理への影響 • 現行のHSM（PCIe3）で、ECDSA P-384に対応可能。 • セカンド電子証明書を格納するHPKI-KAGURAにも影響する可能性あり。 ■HPKIカードへの影響 • 新証明書に対応したHPKIカードの発行が必要（HPKIカード開発に1-2年、HPKIカードドライバ開発に2年かかる見込み。 ■旧暗号方式と新暗号方式の並行運用期間に係る考慮事項 • ECDSA対応の厚労ルート認証局ならびにサブ認証局をどのように準備するか検討が必要（手段としては次の2通り）。 ① 現行の認証局とは分けて新しい認証局を構築する ② 現行の認証局の鍵更新を実施する • 誤作業防止や電子証明書のキー値（例.電子証明書のシリアル番号）の重複防止の観点から、審査システムを認証局ごとに分ける対応等が必要。 • 新旧暗号両方に対応したCA証明書類やCRLの設定が必要。 • 新暗号証明書発行開始や旧暗号証明書の有効期限等、イベントを意識した準備や関係者への漏れなき連絡・対応依頼は必須。 • 利用者の環境要件の明確化が必要。 ※暗号アルゴリズム自体の移行は今回が初であり、利用者（証明書検証）への影響が大きいと思われる。

調査状況の報告

調査先等		調査項目	調査結果
署名者	JAHIS	• 医療情報システムへの影響や懸念点 • システムの互換性 • 特に懸念すべきシステム影響 • ユーザーの業務プロセス変更	ヒアリング中
検証者	JAHIS	• 医療情報システムへの影響や懸念点 • システムの互換性 • 特に懸念すべきシステム影響 • ユーザーの業務プロセス変更	
	弁護士	• 検証者としてのケース（医療訴訟における署名の開示等）や暗号アルゴリズムの移行に係る影響等の確認	• 裁判所等が検証することは通常はないとしても、いざというときには、訴訟手続き上の検証により、有効性を確認できるべき。従って、裁判所等が署名検証をすることを可能にしておくべき、というご意見をいただいた。

調査状況の報告

調査先等		調査項目	調査結果
関連サービス	支払基金	• 電子処方箋サービス・電子カルテ共有サービスへの影響や懸念点	• 保存調剤情報の保存義務期間を考慮し、移行後5年間は旧証明書の署名検証が可能な状態とする必要がある。 • 署名検証ライブラリの更新と、新旧証明書併存期間におけるCRL発行方法及び形態を考慮する必要がある。 • 構築事前の新暗号方式の検証に係る環境や資材提供を求められている。 • ドキュメントに記載のハッシュアルゴリズム選定理由を修正する必要がある。
		• システム全体のパフォーマンスに係る懸念点	• 一般にRSAよりECDSAのほうが高速だが、実際のパフォーマンスは検証する必要がある。
		• 接続しているシステムへの影響	• 接続システムは、署名データ部分を使用していなければ影響なし（対向システムに要確認）。
		• タイムスタンプシステムへの影響	• ECDSAで署名された電子データへのタイムスタンプ付与は、論理的には可能だが、検証は必要。
	総務省	• タイムスタンプ制度との整合性・懸念点	• 時刻認証業務のデジタル署名で用いられる署名アルゴリズムは、総務省が発行している「タイムビジネスに係る指針」及び「時刻認証業務の認定に関する実施要領」に記載の要件に準拠する必要がある。 ✓ CRYPTRECの「電子政府推奨暗号リスト」に記載されている暗号技術であること ✓ 各事業者で次期暗号化方式への対応が技術的に可能であること ✓ 高い強度・安全性が見込まれること

調査状況の報告

調査先等		調査項目	調査結果
関連サービス	MEDIS	• リモート署名システムへの影響や懸念点 • システム全体のパフォーマンスに係る懸念点	• 現在の分散鍵による署名はRSAのみ対応しており、ECDSAでの実装方式や安全性・性能等の評価は検討段階。 • 新証明書発行に伴い証明書の発行者情報に変更がある場合、新旧を含めて区分処理を行える対応が必要。 ※セカンド電子証明書を格納するHPKI-KAGURA上では、証明書の発行者情報に基づく区分管理（日医、日薬、MEDIS）を実施している。 • 並行運用期間中は、RSAとECDSAの鍵が混在する形となるが、DB上では鍵の保管と証明書の保管を別途実施している。そのため、署名時に使用する鍵がRSAのものであるかECDSAのものであるかは不明であるため、ユーザの証明書を確認をしたうえで署名アルゴリズムを指定するロジックの追加が必要。 • 署名アルゴリズム指定ロジックの追加による処理負荷が増えるためパフォーマンスに影響を及ぼすリスクあり。

1．MEDIS認証局 準拠性審査の実施について

2．暗号アルゴリズムの移行に関して

3．耐量子計算機暗号（PQC)について

4．連絡事項

- 資料3をご確認ください

1．MEDIS認証局 準拠性審査の実施について

2．暗号アルゴリズムの移行に関して

3．対量子計算機暗号（PQC)について

4．連絡事項

連絡事項

次回、第34回HPKI専門家会議について

2025年9月頃の開催を予定しております。別途日程調整のご案内を致します。