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３４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 準拠性審査結果報告

2．暗号アルゴリズムの移行に関して

3．リモート署名サービスの活用に関して

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

Ministry of Health, Labour and Welfare of Japan

1．MEDIS 準拠性審査結果報告

2．暗号アルゴリズムの移行に関して

3．リモート署名サービスの活用に関して

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

MEDIS認証局 準拠性審査結果報告

審査対象認証局

一般財団法人 医療情報システム開発センター（MEDIS）

準拠性審査の対象項目

- 保健医療福祉分野 PKI 認証局 署名用証明書ポリシ 1.92 版
- 保健医療福祉分野 PKI 認証局 認証用（人）証明書ポリシ 1.82 版

申請区分

更新申請

実地審査日

2025年8月4日

審査班

丸山 満彦

六川 浩明

MEDIS認証局 準拠性審査結果報告

審査方法

書類審査及び実地調査

書類審査

- 認証管理規程
- 申請書
- 監査報告書（署名用）
- 監査報告書（認証用）
- 団体概要

実地調査

- 代表者インタビュー
- 認証局システム運用状況の確認（各種手順書、教育訓練等）
- 実地確認（人的・物理セキュリティの確認、保守状況等）

前回からの主な変更点、確認箇所

- マイナポータルからの届出対応に係る変更
- 厚労省の問い合わせ先変更に伴う記載の変更
- インシデント発生状況

MEDIS リモート署名サービス評価基準　準拠性審査結果報告

審査対象トラストサービスプロバイダー

一般財団法人 医療情報システム開発センター（MEDIS）

準拠性審査の対象項目

- 保健医療福祉分野における リモート署名サービスの評価基準 1.01 版（鍵管理（署名値生成）サービス）
- 保健医療福祉分野における リモート署名サービスの評価基準 1.01 版（デジタル署名サービス）

申請区分

更新申請

実地審査日

2025年8月4日

審査班

丸山 満彦

六川 浩明

MEDIS リモート署名サービス評価基準　準拠性審査結果報告

審査方法

書類審査及び実地調査

書類審査

- 運用規程
- 監査報告書（鍵管理（署名値生成）サービス）
- 監査報告書（デジタル署名生成サービス）
- 利用規約
- AWSから提出された文書（SOC等）

実地調査

- 代表者インタビュー
- システム運用状況の確認（各種手順書、教育訓練等）

前回からの主な変更点、確認箇所

- 利用規約を有償化ベースの記載に変更
- インシデント発生状況

MEDIS 準拠性審査結果報告

審査対象項目	審査結果
• 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	適合
• 保健医療福祉分野における リモート署名サービスの評価基準（鍵管理（署名値生成）サービス） • 保健医療福祉分野における リモート署名サービスの評価基準（デジタル署名サービス）	適合

準拠性審査　審査班用チェックリストについて

- 丸山構成員、六川構成員に審査班用チェックリストを用いて準拠性審査を実施いただいた。
- ポリシ等との齟齬は認められず、審査にあたり内容の見直しが必要な点はなかった。
- 今後のブラッシュアップなど、審査班用チェックリストの運用方法については引き続き検討する。

Ministry of Health, Labour and Welfare of Japan

1．MEDIS 準拠性審査結果報告

2．暗号アルゴリズムの移行に関して

3．リモート署名サービスの活用に関して

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

前回議論の振り返り

- **暗号アルゴリズムの移行について**
- 次期暗号移行に向けたスケジュール感や検討すべき事項に関して議論を行った。
- CRYPTREC 暗号強度要件を踏まえた次期暗号移行に向け、ECDSA※への移行を想定したスケジュール感や検討すべき事項に関して議論を行った。
- スケジュール感について、引き続き本専門家会議において議論を行うこととした。

※ECDSA：Elliptic Curve Digital Signature Algorithmの略称。楕円曲線暗号（ECC）を利用したデジタル署名アルゴリズムで、他の暗号方式に比べ短い鍵長で安全性を担保できる。

- **耐量子計算機暗号（PQC）について**
- 政府機関等における耐量子計算機暗号（PQC）利用に係る検討状況に関して議論を行った。

本日の議論のポイント

● 本日の議論における到達目標について

- 第32回HPKI専門家会議にて整理した調査項目や検討すべき事項に関して、関係者への調査結果及び次期暗号移行に向けたスケジュール案について、事務局より説明いたします。
- 本日は、調査結果等を踏まえ、次期暗号化方式移行の決定や関連システムの対応内容、次期暗号移行に向けたスケジュール案について、議論頂きたいと考えています。
- 最後に、HPKIで採用する次期暗号化方式について承認頂きたいと考えています。

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	■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。 • 新暗号方式の検証環境が必要。 • 新暗号方式での証明書発行のパフォーマンス検証が必要。 • 電子証明書発行のための情報（発行要求のためのCSV等）の様式に変更があればシステム改修が必要。 ■鍵生成及び鍵管理への影響 • 新認証局を構築する方法であれば鍵生成や鍵管理に係る手順への影響はなし。 • 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。 • CC（Common Criteria）認証の新規取得要否は、HPKI専門家会議で議論する必要あり。 • HPKIで共通のカードとなることから、日薬様、MEDIS様とも協議が必要。 ■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 • 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。

※赤字箇所：他調査先とは共通しない、本調査先のみから頂いたご意見。

調査状況の報告

調査先等		調査項目	調査結果
認証局	日本薬剤師会	• 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	■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。

※赤字箇所：他調査先とは共通しない、本調査先のみから頂いたご意見。

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。

※赤字箇所：他調査先とは共通しない、本調査先のみから頂いたご意見。

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 • 特に懸念すべきシステム影響	■署名プロセスに係る影響 • 署名モジュールの更新・入れ替えが必要となる可能性がある。 • 署名モジュールが更新されることにより、次の影響が考えられる。 　• クライアントOS側の対応確認。 　• 証明書ストアの更新作業。 　• 電子カルテ側のプログラム改修。 　• ライブラリライセンス・機器・ソフトウェアに関する費用増加。 ■システムに係る影響 • 新暗号化方式への切り替えタイミングは病院側と調剤薬局側で合わせる必要あり。 • データ互換性の観点から、電子処方箋署名共通モジュールは旧方式と新方式の両方に対応できる必要がある。 • 新暗号化方式の移行に際して、H/Wリソースを増強する場合や電子処方箋署名共通モジュールを新開発する場合、システム価格に影響する。 • 異なるベンダーで作成された暗号システムで、どの組み合わせでも署名・検証が問題なく処理できるかの確認及び検証に時間を要する。 • 電子処方箋署名共通モジュールのAPIを変更する場合、システム改修規模が増大。 • システム稼働中に新方式に切り替える場合、運用中のアプリケーションや電子処方箋署名共通モジュールの入れ替えが発生。 • 署名プロセスと検証プロセスで同期をとって変更することが必要。 • 署名共通モジュールや署名フォーマットの、タイムスタンプも含めた次期暗号方式への対応可否は、HPKIリモート署名の対応方針や電子署名モジュールの仕様次第 • PQCについては現時点での対応が不可なベンダーも考えうる。

調査状況の報告

調査先等		調査項目	調査結果
検証者	JAHIS	• 医療情報システムへの影響や懸念点 • 特に懸念すべきシステム影響	■検証プロセスに係る影響 • 電子処方箋管理サービス・電子カルテ情報共有サービスにおいて、TSAの証明書に用いられる暗号方式を新暗号方式に対応させられるか懸念。 • TSA側の新旧証明書が混在する期間が発生することも想定され、新旧暗号を正しく判別して検証するための検証モジュールが必要。
		• システムの互換性	• HPKIを用いたシステムとして次期暗号方式への互換性のないシステムが存在する場合がある（リモート署名の対応方針や電子署名モジュールの仕様次第）。
		• ユーザーの業務プロセス変更	• ユーザーである署名者・検証者（医師・薬剤師等）にとって、業務プロセス上の変更は基本的に想定されていないが、リモート署名の対応方針や電子署名モジュールの仕様次第では変更の可能性あり。
	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。 • 現行システムでは、時刻認証局サービスでのタイムスタンプ付与の仕組みの中でRSA方式が利用されている。
	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。

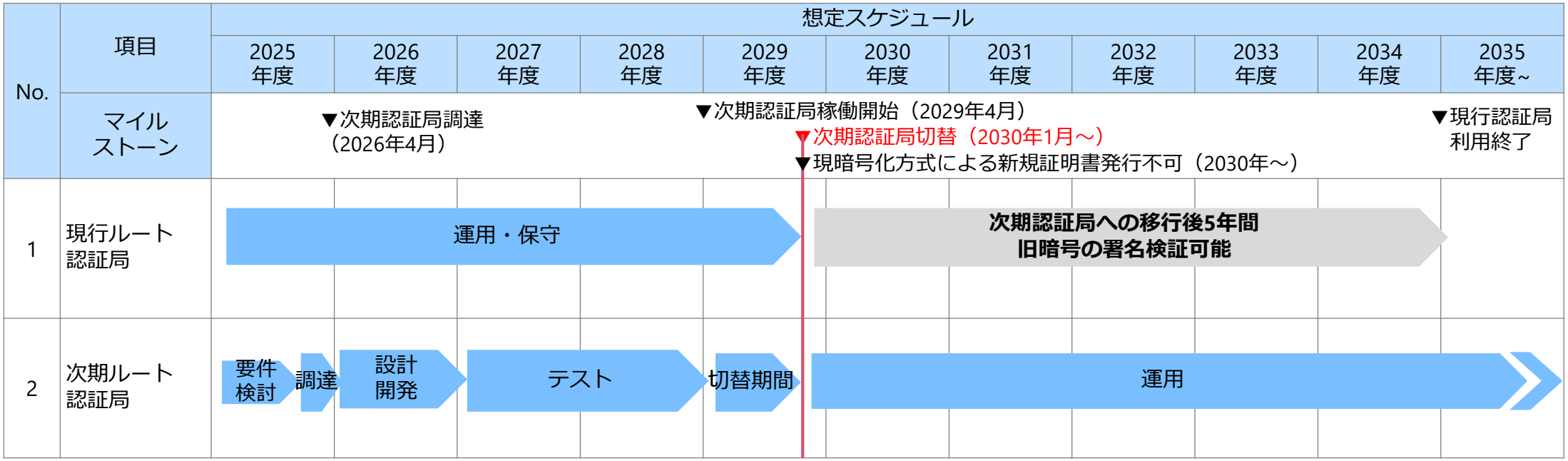
調査状況を踏まえた留意点の整理

カテゴリ		留意点
技術面	安全性等の検証	• 特にリモート署名サービスにおいて、ECDSAを用いることの安全性及び性能面を検証し、新暗号アルゴリズムに追従可能であることを確認する必要がある。
移行計画	検証環境の準備	• 次期暗号方式の移行による影響の詳細を把握するため、医療機関向けに新暗号方式の検証環境を準備する必要がある。検証環境を準備する主体や段取り、検証環境に求められる要件の具体化が必要。
	検証期間の考慮	• 医療機関による構築事前の検証期間も考慮し移行計画を策定する必要がある。 • 各ベンダーでの署名・検証の確認は時間を要することが見込まれるため、結合テストにおいては十分な期間を設ける必要がある。
	関係システムの開発期間の考慮	• HPKIカードやドライバの開発期間・納品期間を踏まえると、2026年度までには仕様を決定する必要があり、開発及び製造期間は2027年度～2029年度にわたること（開発：１～2年、製造1年）を見込んだ計画を策定する必要がある。 • 電子署名共通モジュールの新暗号方式対応について、開発ベンダーへ開発及びリリースに係る期間を確認のうえ、移行計画を策定する必要がある。
	切替後の旧証明書検証の考慮	• 移行後5年間は旧証明書の署名検証が可能な状態を維持できる移行計画を策定する必要がある。
	並行運用期間に係る考慮	• 新暗号化方式への切替タイミングは各医療機関で一致するように移行計画を策定する必要あり。 • 並行運用期間においては、技術的問い合わせ窓口の設置、データ出力機能の改修、登録局と発行局間での切り替えに係るテスト等の準備が必要。 • 新旧暗号方式両方で運用を行うため、ECDSA対応の認証局の準備や、新旧暗号に対応したCA証明書の作成やCRLの設定、利用者の環境要件を明確化し並行運用事前に周知する必要あり。
コスト面		• 新暗号方式への移行に際して、H/Wリソースの増強や電子処方箋署名共通モジュールの新開発によってシステム価格は現行より増大する可能性があり。

次期暗号移行に向けたスケジュールについて

● **今後の暗号移行に向けたスケジュールについて**

- 早ければ年内中に入札公告を行い、令和8年度前半には契約し開発を開始する想定。
- 2029年度には次期認証局と現行認証局の並行運用を開始したいと考えています。
- 現時点では厚労省ルート認証局における想定スケジュールのみを記載しています。サブ認証局や関連システムの想定スケジュールについては、次期認証局の構成について議論を行った上で記載する予定です。
- なお、次期認証局の構成については、次回HPKI専門家会議においてご議論いただく予定です。



次期暗号方式の決定について

本日までの議論を踏まえて、HPKIの次期暗号化方式を以下で決定することについて、承認をお願い致します。

・HPKI　次期暗号化方式：ECDSA P-384 with SHA384

<u>選定理由</u>

- 「CRYPTREC 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に適合する暗号化方式に変更する必要がある。
- RSAで暗号移行を進めた場合、鍵長を長くする必要があり、ICチップの処理能力を踏まえると、署名時の処理時間等が伸び、運用に支障をきたすおそれがある。
- このため、ECDSA P-384 with SHA384 （192ビットセキュリティ）を採用することで、比較的短い鍵長でICカード等の処理性能・運用負荷を抑えつつ十分な暗号強度の確保が可能となる。
- 認証局・署名者・検証者・関連システムベンダー等への影響についての調査を通じ、ECDSA P-384 with SHA384への暗号移行を進めることが可能であることを確認済。
- 本暗号方式を採用することで、政府系のPKI基盤として、GPKIと足並みを揃えることが可能。
- なお、調査を通じて明らかとなった要検討事項については、HPKI専門家会議にて引き続き協議予定。

Ministry of Health, Labour and Welfare of Japan

1．MEDIS 準拠性審査結果報告

2．暗号アルゴリズムの移行に関して

3．リモート署名サービスの活用に関して

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

Ministry of Health, Labour and Welfare of Japan

1．MEDIS 準拠性審査結果報告

2．暗号アルゴリズムの移行に関して

3．リモート署名サービスの活用に関して

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

連絡事項

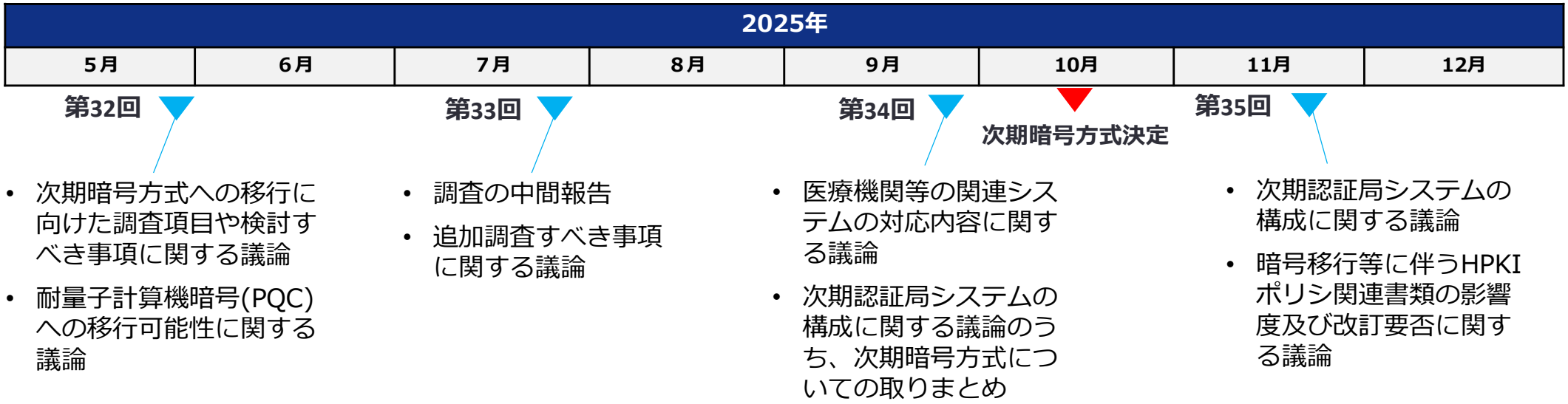
次回、第35回HPKI専門家会議について

2025年11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。

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

●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

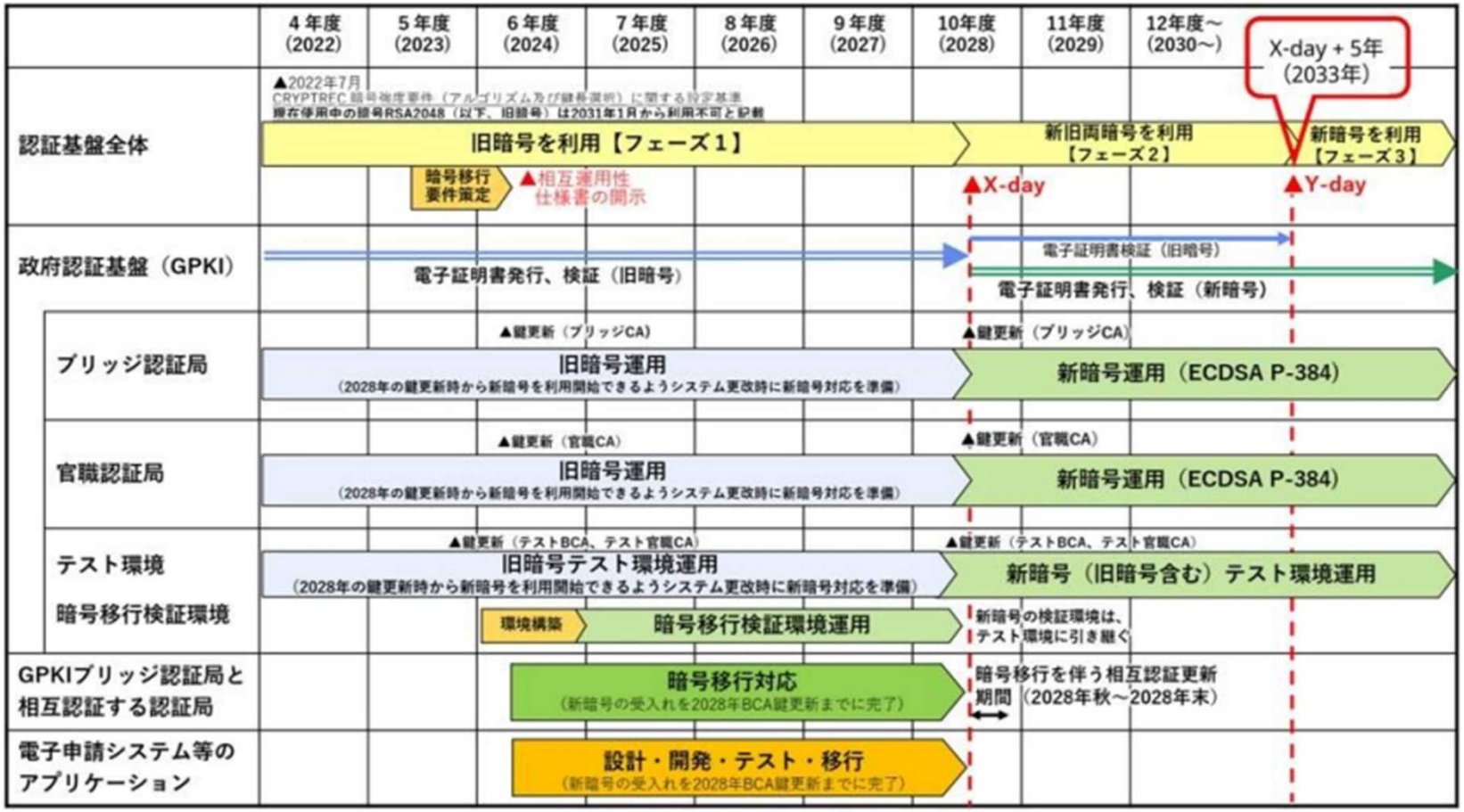
- 年内には次期暗号方式を決定したいと考えています。
- 次期暗号方式の決定に向けた本専門家会議における議論のスケジュール（予定）は次のとおりです。



【参考】第３１回資料再掲
GPKI認証局の対応状況

政府系のPKI認証局であるGPKI認証局については昨年１０月に暗号アルゴリズム移行時の相互運用性仕様書が示されており、既に仕様が確定している。

GPKIの暗号アルゴリズム移行スケジュール



GPKIホームページより抜粋　相互運用性仕様書