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

資料３－１

HPKI暗号アルゴリズムの移行について

第35回公開鍵基盤認証局の整備と運営に関する専門家会議　2026（令和８）年３月２日(月)

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

暗号アルゴリズムの移行について

次期暗号方式移行に係るご指摘事項の対応状況

- 第34回HPKI専門家会議にて、次期暗号方式として「ECDSA P-384 with SHA-384」への移行を、リモート署名サービスの構築方法が明確化されることを前提として条件付き承認された。
- 同会議にて「リモート署名が使用できない場合、HPKI自体が今後実際に使用されない事態が生じる可能性があるため、リモート署名サービスの実装方式を明確にした上で、最終的な決断を下すことが望ましい」との意見を頂いた。
- 今般、リモート署名サービスのトラストサービスプロバイダーであるMEDISにて、ECDSA方式に対応したリモート署名サービスの実装方式を検討した結果、クラウドHSMを用いた鍵管理方式を採用する旨の報告を頂いた。その中で、当該方式においてECDSA方式でのリモート署名サービスが実装可能であることを検証頂いている。
- 今般のECDSA方式でのリモート署名サービスの鍵管理方式は、クラウドサービスプロバイダーが提供するFIPS認証取得済みのクラウドHSMを利用して実装されており、リモート署名サービスに預託される鍵の管理について、HPKIポリシに準拠していると考える。

本日議論頂きたい内容

- 本日は、ECDSA方式に対応したリモート署名サービスの実装方式について、許容可能なものであるかを議論頂き、前回の専門家会議にて次期暗号アルゴリズムへの移行を条件付き承認としていたが、「ECDSA P-384 with SHA-384」への暗号移行を進めることについて、正式に承認をお願いしたい。

次期暗号方式移行に係る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のご報告

- CRYPTRECの暗号強度要件に関する設定基準において、2031年以降112ビットセキュリティによる署名生成を認めていない。
- 一方で、次期暗号アルゴリズムに対応したHPKIカードのICチップの開発及びドライバの開発等に２～３年を要する見込みであり、関連システムの改修期間、現行暗号で発行したHPKIも考慮すると、2031年以降も一定期間、旧暗号による署名生成を許容する必要があると考える。（次ページのスケジュール参照）
- その場合のリスクとしては、時間の経過とともにコンピュータの解読計算能力が向上することにより、秘密鍵が解析され、不正な署名が発行されることで、電子処方箋の不正発行や医療記録の改ざんが行われるといった可能性が考えられる。
- CRYPTRECによれば、量子コンピュータの将来性能や暗号解読に関する予測には不確実性があるものの、2048ビットRSAが近い将来に危殆化する可能性は低いとされている*。また、不正な署名を発行するためには、高度な技術的知識、さらには認証局システムを模倣するための多大なリソースが必要である。
- したがって、事務局としては、次期暗号アルゴリズムへの移行完了までの限定的な期間において、2031年以降に旧暗号による署名生成の利用することは、一定許容されるのではないかと考える。
- なお、 2031年以降に旧暗号による署名生成を利用する場合には、政府機関等のサイバーセキュリティ対策のための統一基準及び厚生労働省情報セキュリティポリシーで定められた「電子政府推奨暗号リスト」に準拠しないこととなるため、事務局において今後関係部局との調整を行う予定。

*出典：政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議幹事会（第１回）
資料３　暗号の危殆化等について（総務省提出資料）

次期暗号方式移行に係るスケジュールについて

次期暗号方式移行に係るスケジュール案

No.	項目	想定スケジュール										
		2025年度	2026年度	2027年度	2028年度	2029年度	2030年度	2031年度	2032年度	2033年度	2034年度	2035年度～
	マイルストーン		▼次期認証局調達（2026年4月）			▼次期認証局稼働開始（2029年4月）	▼次期認証局切替（2030年1月～）					▼現行認証局利用終了
1	現行ルート認証局						**次期認証局への移行後 最大5年間 旧暗号による署名生成・署名検証可能**					
							運用・保守					
2	次期ルート認証局	要件検討	調達	設計開発		テスト	切替期間	運用				
3	現行サブ認証局						**次期認証局への移行後 最大5年間 旧暗号による署名生成・署名検証可能**					
							運用・保守					
4	次期サブ認証局				次期サブ認証局開発期間		運用					
							新HPKIカード運用					

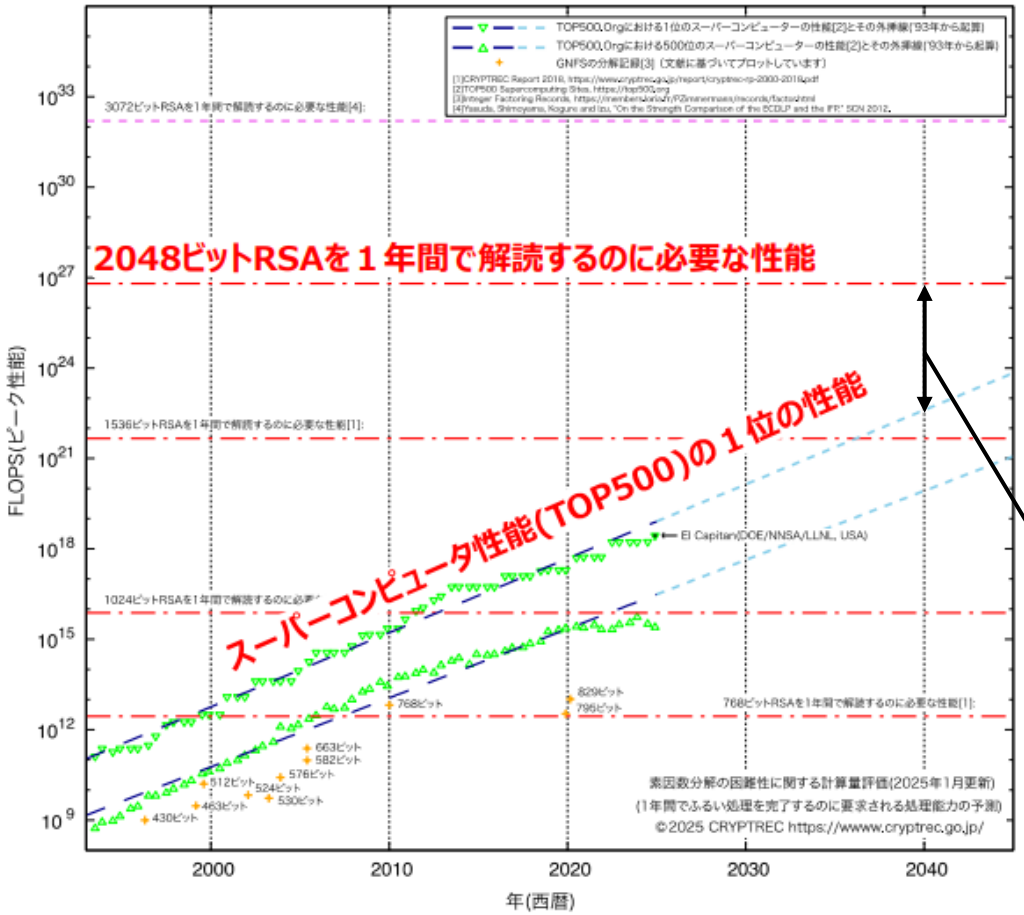
本日承認頂きたい内容

- 本日は、次期暗号アルゴリズム移行のスケジュールに関し、次期サブ認証局の運用開始後においても、現行のサブ認証局で発行された電子証明書による署名生成を、電子証明書の有効期間内に限り許容することについて、承認いただきたい。

【参考】政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議幹事会報告　素因数分解の困難性に関する計算量評価

➢ **公開鍵暗号方式**は、**数学的な計算の困難さ**（素因数分解や離散対数計算）に基づいており、CRYPTRECでは、そうした計算の困難さの検討に関して**計算量評価の予測図**を更新・公表している。

素因数分解の困難性に関する計算量評価（2025年1月更新）



予測図の取扱い

いわゆる**ムーアの法則を仮定して外挿**線を年度末からプラス20年後まで従来通り直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として予測図を当面の間更新していく。

※予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

ムーアの法則※より、2040年時点のスーパーコンピュータの予測性能は、2048ビットRSA暗号を1年間で解読するために必要な性能に到達しないことを示している。

※ムーアの法則：コンピュータに使われる半導体チップ（集積回路）に載るトランジスタの数は、約2年ごとに2倍になるという経験則。トランジスタ数が増加することでチップが同時に処理できる回路や機能が増えるため、計算処理能力が向上する。

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議幹事会（第１回）
資料３　暗号の危殆化等について（総務省提出資料）より抜粋

【参考】　第３４回資料再掲
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。