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３１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（特定医薬品開発支援・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．日本医師会認証局　鍵更新結果の報告

２．暗号アルゴリズムの移行に関して

３．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．日本医師会認証局　鍵更新結果の報告

2．暗号アルゴリズムの移行に関して

3．連絡事項

日本医師会認証局　鍵更新結果の報告

日本医師会認証局サブCA鍵更新

- 2024年11月15日　　キーセレモニーを実施（立会）
- 2024年12月14日　　新鍵の切り替えを実施（立会）
- 2025年2月3日　　旧鍵の削除

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

１．日本医師会認証局　鍵更新結果の報告

２．暗号アルゴリズムの移行に関して

３．連絡事項

暗号アルゴリズムの移行に関して

2030年に向けて、移行を行う暗号アルゴリズムの方式を決定する必要がある

HPKIで使用している方式

ハッシュ：SHA-256（128ビットセキュリティ）　2050年まで

暗号：RSA2048（112ビットセキュリティ）　2030年まで

表 5　セキュリティ強度要件の基本設定方針

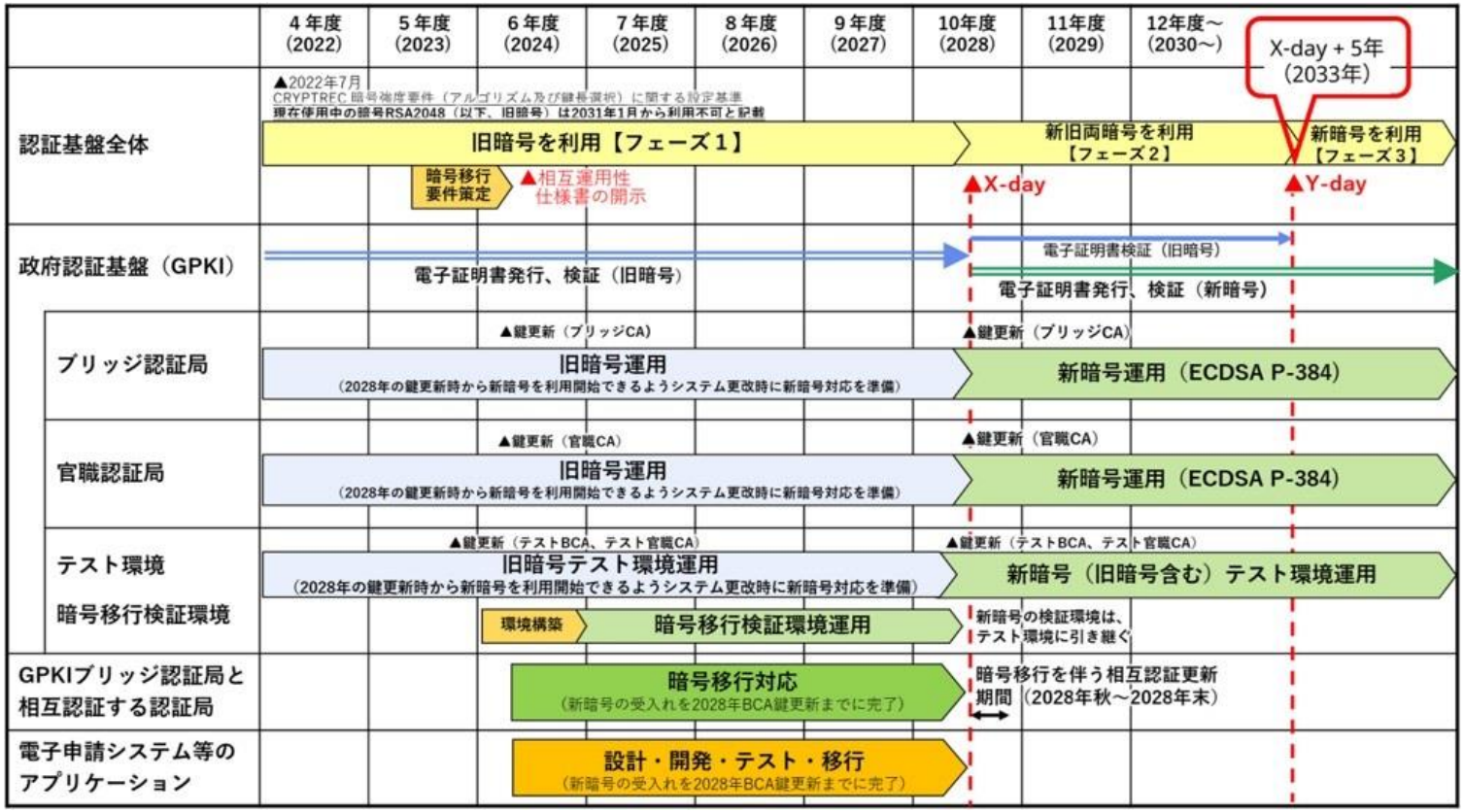
想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビット セキュリティ	新規生成 ((a)参照)	移行完遂期間 ((c)参照)	利用不可	利用不可	利用不可	利用不可
	処理 ((b)参照)		許容			
128 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	移行完遂期間 ((c)参照)	利用不可	利用不可
	処理 ((b)参照)				許容	
192 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					
256 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					

Cryptrec 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準より抜粋

【参考情報】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　https://www.gpki.go.jp/session/index.html

【参考情報】GPKIにおける次期暗号アルゴリズム

8.3.3.1.　CA 鍵の署名アルゴリズムと鍵長

- BCA のCA鍵の鍵長は384 ビットのECDSA、署名アルゴリズムは ECDSAwithSHA384 を使用する。
- 官職 CA の CA 鍵の鍵長は 384 ビットの ECDSA、署名アルゴリズムは ECDSAwithSHA384 を使用する。
- 民間 CA の CA 鍵の鍵長は 384 ビットの ECDSA、署名アルゴリズムは ECDSAwithSHA384 を使用することが望ましい。（CA 鍵の鍵長 3072 ビットの RSA、 署名アルゴリズム sha256WithRSAEncryption 又は CA 鍵の鍵長 256 ビットの ECDSA、 署名アルゴリズム ECDSAwithSHA256 も許容する）

GPKI政府認証基盤相互運用性仕様書（移行完了編）より抜粋　https://www.gpki.go.jp/session/index.html

HPKIの暗号アルゴリズム移行に向けた議論

- JPKIについてもGPKIブリッジ認証局と相互認証を行っている関係上、GPKI同様の暗号アルゴリズムが使用される
- HPKIでは相互認証は行っていないが、同様に政府系のPKI認証局として問題なければ足並みを揃えられることが望ましい

GPKIの参考情報も加味いただき、本日は下記内容について、ご議論お願いします。

「保健医療福祉分野やHPKIの運用上の特性を踏まえ、暗号アルゴリズムの選定に対する、課題、懸念事項はどのようなものが想定されるか」

なお、次回32回も暗号アルゴリズムの選定議論を継続し実施する見込みです。

1．日本医師会認証局　鍵更新結果の報告

2．暗号アルゴリズムの移行に関して

3．連絡事項

連絡事項

次回、第32回HPKI専門家会議について

2025年5月頃の開催を予定

議題案

- 暗号アルゴリズムの移行に関する議論
- MEDIS認証局鍵更新の報告

次回より、構成員を一名、追加させていただきます。

菊池　浩明	**明治大学　総合理工学部先端メディアサイエンス学科　教授**

連絡事項

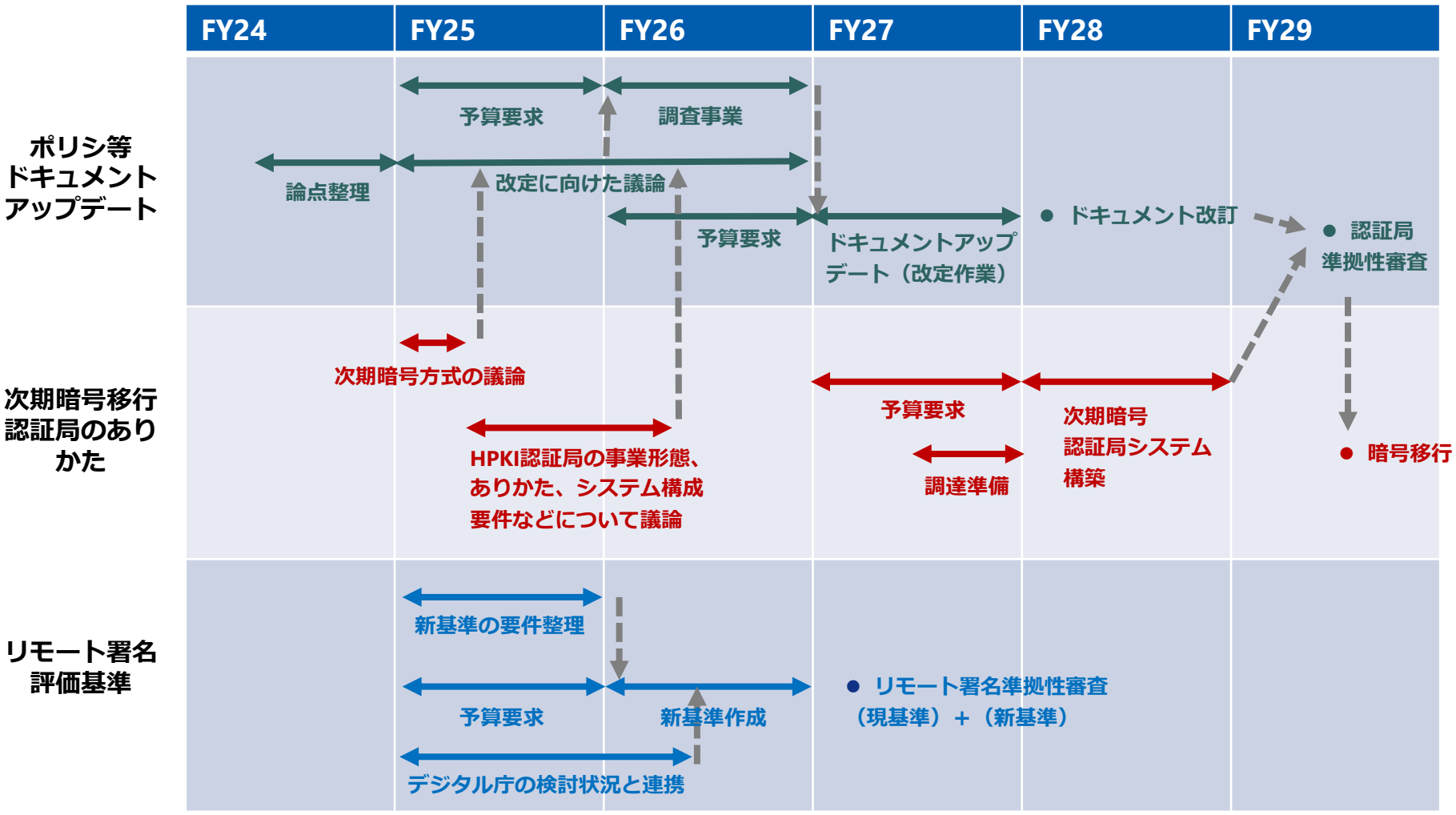
来年度以降の専門家会議体制について

2025年6月で現構成員の任期（２年）が終了するため、継続可否、交代希望について個別に確認をさせていただきます。
なお、７月以降の作業班につきましては、毎回の合同開催とせず専門家会議の状況に応じて招集させていただきますが、日本医師会認証局、日本薬剤師会認証局、MEDIS認証局はオブザーバーの形で継続参加をお願いいたします。

７月以降は下記の人員をHPKI専門家会議の追加構成員とさせていただきます。

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
宮崎　一哉	デジタルトラスト協議会 理事
ご相談中	JIPDECより選出いただく形でご相談中

HPKI専門家会議　オブザーバー参加

日本医師会認証局
日本薬剤師会認証局
MEDIS認証局

【参考】第２９回資料再掲
ロングレンジ　マイルストーン案