

令和8年10月27日

総務省
デジタル庁
経済産業省

「電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)」の改定(PQC対応)に対する意見募集

総務省、デジタル庁及び経済産業省では、CRYPTRECにおいて、量子コンピュータ（量子計算機）の進展を踏まえた「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」の改定について検討を進めています。

今般、CRYPTRECの「耐量子計算機暗号（PQC）リスト検討タスクフォース」における検討を踏まえ、耐量子計算機暗号（PQC）の対応に係るCRYPTREC暗号リストの改定に関する資料を作成したので、本日から令和8年11月11日（水）までの間、意見を募集します。

1 背景・概要

総務省、デジタル庁及び経済産業省では、CRYPTREC※の活動を通じて、電子政府で利用される暗号技術の安全性、実装性能及び利用実績の評価・検討等を行い、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」を策定しています。

また、近年、量子コンピュータ（量子計算機）の研究開発が進展する中、将来的に従来の暗号技術の安全性が低下することが懸念されており、耐量子計算機暗号（PQC）への移行に向けた取組が重要となっています。

こうした状況を踏まえ、令和8年3月には、CRYPTREC暗号リストの「電子政府推奨暗号リスト」に、新たに「耐量子計算機暗号（PQC）リスト」を追加する改定を行いました。その際、更なる検討が必要な一部の暗号技術等の取扱いについては保留し、継続して検討することとしました。これらの課題について、安全性評価の観点に加え、暗号技術の利活用・普及促進の観点も含めて横断的な検討を行うため、CRYPTRECに「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設置し、検討を進めてきました（別添1参照）。

今般、同タスクフォースにおける検討を踏まえ、暗号技術の利用状況等も考慮しつつ、今後のCRYPTREC暗号リストの改定に向けて幅広い観点から検討を行うため、耐量子計算機暗号（PQC）の対応に係るCRYPTREC暗号リストの改定について、意見を募集します。

※ CRYPTREC（Cryptography Research and Evaluation Committees）とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトです。

2 意見募集内容

「CRYPTREC暗号リストの改定イメージ」（別添2）について、意見を募集します。

特に、ML-DSA及びSLH-DSAのCategory 1・2（ML-DSA-44及びSLH-DSA-[SHA2/SHAKE]-128[s/f]）について、利用状況や将来的な利用見込み等も踏まえたCRYPTREC暗号リストにおける取扱い（掲載に関する考え方及びその理由）について、意見を募集します。

なお、改定イメージの考え方については、別添3を御参照ください。また、ML-DSA及びSLH-DSAについては、CRYPTRECにおいて安全性評価等が完了していない段階であり、改定内容が確定したものではありませんので御留意ください。

3 意見募集期間等

令和8年10月27日（火）14時から同年11月11日（水）24時まで
（郵送の場合は期間内必着）

意見提出の詳細については、意見公募要領（別添4）をご覧ください。

4 今後の予定

提出された意見を踏まえて、改めてCRYPTRECにおいて検討を行う予定です。また、当該検討の結果及び別途CRYPTRECで実施している安全性評価等の結果を踏まえて、CRYPTREC暗号リストの改定を行う予定です。

5 資料の入手方法

資料は、総務省サイバーセキュリティ統括官室において閲覧に供するとともに配布します。また、e-Gov（<https://www.e-gov.go.jp/>）の「パブリック・コメント」欄に掲載します。

<連絡先>

総務省

サイバーセキュリティ統括官室

担当：梅城企画官、遠藤補佐、太田専門職、梶川官

電話：03-5253-5431

デジタル庁

デジタル社会共通機能グループ トラスト班

担当：盛岡参事官補佐、宇都木主査、池田係員

電話：03-6891-2720

経済産業省

商務情報政策局サイバーセキュリティ課

担当：橋本企画官、石坂課長補佐

電話：03-3501-1253

共通（電子メールアドレス）

cryptrec2026iken_atmark_ml.soumu.go.jp

※迷惑メール防止のため、@を「_atmark_」と表示しています。