

意見公募要領

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 意見募集対象

「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）

4 意見の提出方法・提出先

意見の提出を装って不審メールが送付される事案を防ぐため、可能な限り(1)のe-Govによる提出をお願いいたします。(2)又は(3)の提出方法とする場合は、意見書（別紙様式）に氏名及び住所（法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地）、並びに連絡先（電話番号又は電子メールアドレス）を明記の上、意見提出期限までに御提出ください。

(1)から(3)までのいずれの場合も、提出意見は必ず日本語で御記入ください。

また、誤投稿防止のため、意見の提出に当たって必ず「意見募集要領（提出先を含む。）」及び「意見募集対象」の全部を御確認ください。

(1) e-Govを利用する場合

e-Gov（<https://public-comment.e-gov.go.jp/>）に掲載されている対象の意見募集案件の意見提出フォームに、郵便番号、氏名及び住所（法人又は団体の場合は、名称、

代表者の氏名及び主たる事務所の所在地）並びに連絡先（電話番号又は電子メールアドレス）を記載の上、意見提出期限までに御提出ください。

※e-Govから提出できる電子ファイルのサイズは4MBまでとなっています。

(2) 電子メールを利用する場合

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。

※メールに直接意見を書き込んでいただきますようお願いいたします。添付ファイルを送付する場合、ファイル形式は、テキストファイル又はマイクロソフト社Wordファイルにより御提出ください（他のファイル形式とする場合は、担当までお問合せください。）。

※電子メールアドレスの受取可能最大容量は、メール本文等を含めて20MBとなっています。

(3) 郵送する場合

〒100-8926 東京都千代田区霞が関2-1-2

総務省 サイバーセキュリティ統括官室 暗号トラストライン 宛て

※別途、意見の内容を保存した記録媒体を添えて提出いただくようお願いする場合があります。この場合、送付いただいた記録媒体は、返却できませんのであらかじめ御了承ください。

5 留意事項

- ・意見提出に当たっては、①ML-DSA・SLH-DSAに関する意見と②その他CRYPTREC暗号リストに関する意見を分けて記載願います。また、各意見には、意見公募対象の何ページのどの部分に対する意見であるのか明確に御記載ください。
- ・提出された意見は、e-Gov及び総務省ウェブサイト等に掲載するほか、連絡先窓口にて配布又は閲覧に供します。
- ・御記入いただいた氏名・連絡先については、提出意見の内容に不明な点があった場合等の連絡・確認のために利用します。なお、法人又は団体の場合は、提出された意見とともにその名称を公表する場合がありますので、匿名を希望される場合には、その旨を御記入ください。
- ・意見に対する個別の回答はいたしかねますので、あらかじめ御了承ください。
- ・意見提出期間の終了後に提出された意見、意見募集対象以外についての意見については、提出意見として取り扱わないことがありますので、あらかじめ御了承ください。
- ・提出された意見は、結果の公示の際、必要に応じ整理・要約したものを公示することがあります。その場合には、提出された意見を連絡先窓口へ備え付け、閲覧に供しますので、あらかじめ御了承ください。
- ・提出された意見を公示又は公にすることにより第三者の利益を害するおそれがあるとき、その他正当な理由があるときは、提出意見の全部又は一部を除いて公示又は公にすることがありますので、あらかじめ御了承ください。

<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。

意見書

令和 年 月 日

総務省・デジタル庁・経済産業省 宛

郵便番号

住所

氏名※

電話番号

メールアドレス

※法人又は団体にあつては、その名称及び代表者の氏名を記載すること。また、連絡担当者の氏名を記載すること。

CRYPTREC暗号リストの改定イメージに対して、次のとおり意見を提出します。

該当箇所	御意見
①ML-DSA・SLH-DSAに関する意見	
②その他CRYPTREC暗号リストに関する意見	