資料43－２－１

CRYPTRECの最近の取組

令和５年４月

サイバーセキュリティタスクフォース事務局

CRYPTRECの概要

- **CRYPTREC**（Cryptography Research and Evaluation Committees）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。

CRYPTRECの体制（2023年度）

暗号技術検討会（事務局：デジタル庁、総務省、経済産業省）

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース

暗号技術評価委員会（事務局：NICT、IPA）

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG（耐量子計算機暗号）

暗号技術活用委員会（事務局：IPA、NICT）

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

暗号鍵管理ガイダンスWG

最近の取組の紹介①～CRYPTREC暗号リストの改定～

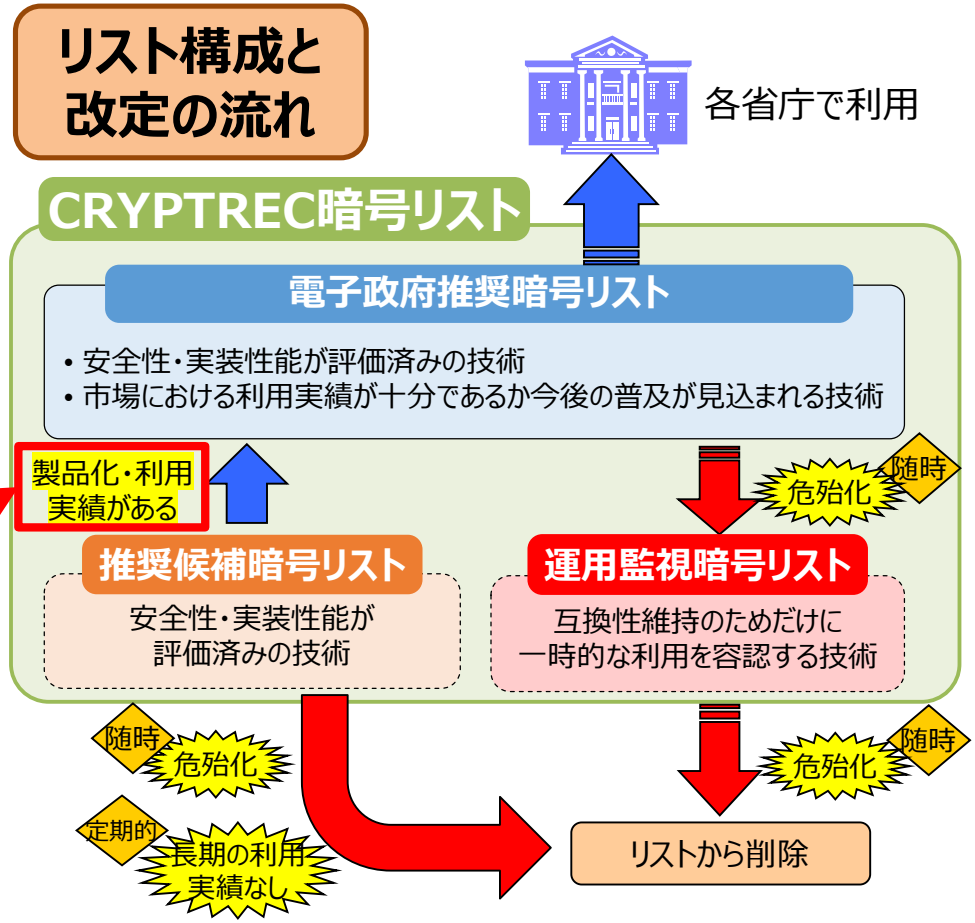
- **安全性・実装性能等が確認された暗号技術**について、平成15年２月に「電子政府推奨暗号リスト」を策定しており、**平成25年３月**にはこれを改定する形で、**電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）**を策定した。
- **令和５年３月**に、**10年ぶり**となる**CRYPTREC暗号リスト**の**大規模改定を実施**した。

10年ぶりの大規模改定

10年ぶりの大規模改定により、推奨候補暗号リストに掲載されている暗号の内、**「製品化・利用実績がある」**と認められた**暗号10件**が、**電子政府推奨暗号リストへ昇格**

今回昇格した暗号10件
EdDSA
ChaCha20-Poly1305
XTS
SHA-512/256
SHA3-256
SHA3-384
SHA3-512
SHAKE128
SHAKE256
ISO/IEC 9798-4

リスト構成と改定の流れ



最近の取組の紹介②～ガイドライン類の策定～

➢ 耐量子計算機暗号や高機能暗号の調査を行い、**令和５年３月**に、**耐量子計算機暗号ガイドライン**及び**高機能暗号ガイドライン**を策定した。

耐量子計算機暗号ガイドライン

量子コンピュータの実用化によって**公開鍵暗号方式の安全性が低下**することを踏まえ、**耐量子計算機暗号（以下PQC）に関する調査結果をまとめたもの。**

対象　**一般的な読者・暗号初学者～暗号技術に携わる研究者・技術者**

内容　PQCについて、**用途別の利用形態**や、**量子コンピュータの脅威・データ保護期間を踏まえた課題とその対策**について紹介。また、世界的に使用が見込まれる**代表的なPQCの方式について紹介**。

高機能暗号ガイドライン

高機能で高効率であり、**様々な用途での利用が期待されている高機能暗号**の利用を促進するために、**高機能暗号の方式及びユースケース等を調査した結果をまとめたもの。**

対象　**暗号技術を活用する技術者**

内容　高機能暗号について、**ユースケース**や従来の暗号方式と比較した際の**メリット**、運用時の**注意点等**を具体的に示す。

今後の取組予定（2023年度）

CRYPTREC暗号リストの改定

下記を踏まえて引き続き**小規模な改定を実施**する予定。

- ・暗号技術評価委員会における、暗号技術の安全性及び実装に係る監視及び評価
- ・暗号技術活用委員会における、暗号技術の利用状況に係る調査

CRYPTRECで公表しているガイドライン類の改定

策定年度	ガイドライン類
2022 （CRYPTREC公式Webサイトでの公表は5月を予定）	暗号鍵管理ガイダンス
2020	TLS暗号設定ガイドライン
2016	CRYPTREC 暗号技術ガイドライン (軽量暗号)

※その他、「素因数分解の困難性に関する計算量評価」の予測図及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新等の取組も実施予定。

（参考）
CRYPTRECで公表している
その他のガイドライン

策定・改定年度	ガイドライン類
2022	CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）
2022	CRYPTREC 暗号技術ガイドライン（高機能暗号）
2021	暗号鍵設定ガイダンス
2020	暗号鍵管理システム設計指針 (基本編)
2018	CRYPTREC 暗号技術ガイドライン (SHA-1) 改定版
2013	CRYPTREC 暗号技術ガイドライン(SSL/TLS における近年の攻撃への対応)

その他、技術報告書等をCRYPTREC公式Webサイトにて公表