CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2024年9月2日

暗号技術検討会 座長
産業技術総合研究所 フェロー
横浜国立大学 上席特別教授
松本 勉

目次

1.CRYPTRECの概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECとは

CRYPTography **R**esearch and **E**valuation **C**ommittees

CRYPTRECの概要

■ デジタル庁・総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価プロジェクト

■ 当プロジェクトは、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討すること等を通じて、セキュアなIT社会の実現を目指すもの

■ 暗号技術検討会並びに暗号技術検討会の下に設置される暗号技術評価委員会及び暗号技術活用委員会により運営

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC活動体制（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

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）
（2021年7月～ ）

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
（2021年6月～ ）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会構成員

座長	松本 勉	国立研究開発法人産業技術総合研究所 フェロー
		横浜国立大学 先端科学高等研究院 上席特別教授
構成員	阿部 正幸	日本電信電話株式会社 フェロー
	石井 義則	一般社団法人情報通信ネットワーク産業協会 常務理事
	上原 哲太郎	立命館大学 教授
	田村 裕子	日本銀行 金融研究所 企画役
	國廣 昇	筑波大学 教授
	高木 剛	東京大学 教授
	手塚 悟	慶應義塾大学 教授
	本間 尚文	東北大学 教授
	松井 充	三菱電機株式会社 開発本部 主席技監
	松浦 幹太	東京大学 教授
	松本 泰	日本ネットワークセキュリティ協会 フェロー
	向山 友也	一般社団法人テレコムサービス協会 技術・サービス委員会 副委員長
	吉田 博隆	国立研究開発法人産業技術総合研究所 研究チーム長
	渡邊 創	国立研究開発法人産業技術総合研究所 副研究センター長

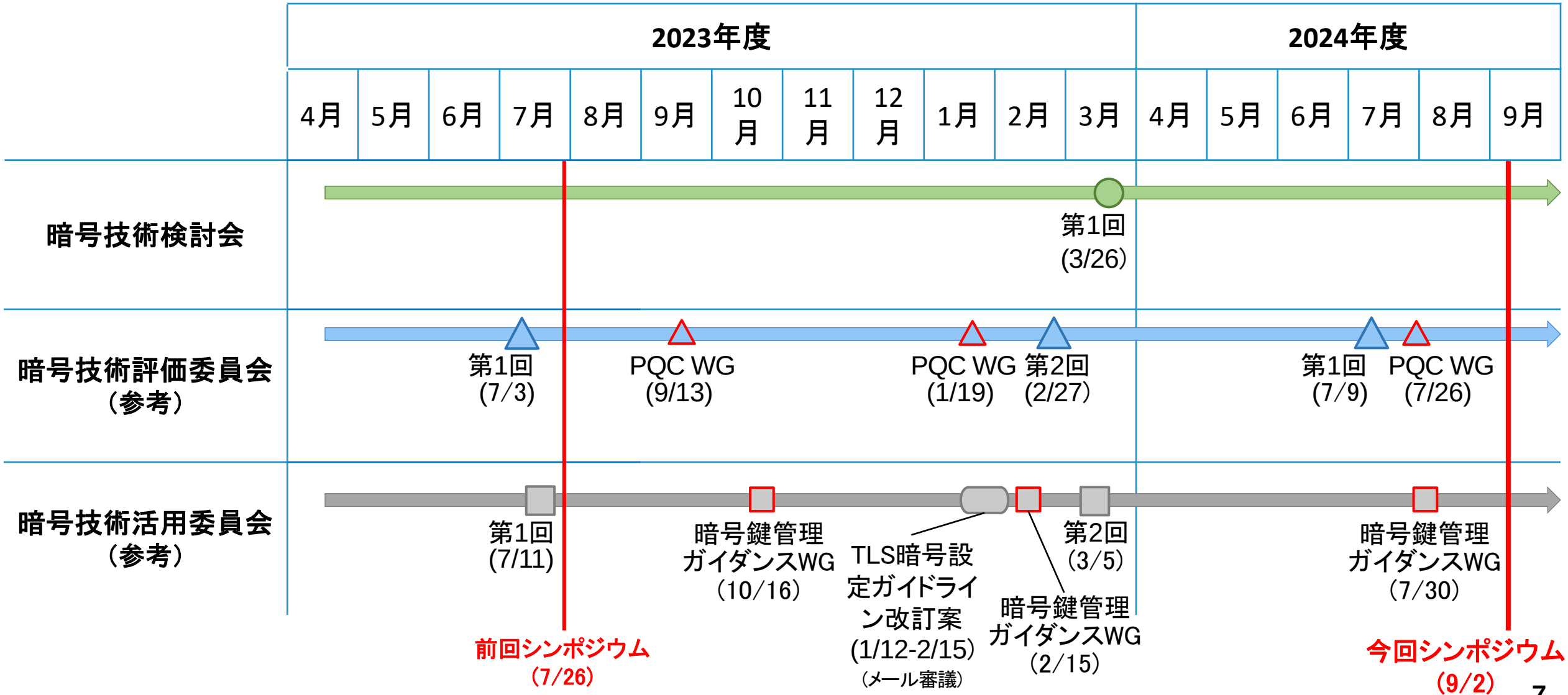
（五十音順、敬称略、所属は2024年8月末時点のもの）

オブザーバ：内閣サイバーセキュリティセンター、警察庁、個人情報保護委員会、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、防衛省、NICT、AIST、IPA、JIPDEC、FISC

事務局：デジタル庁、総務省、経済産業省

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会等の開催状況



2.暗号技術検討会の活動概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの概要

- CRYPTRECの活動を通して**安全性・実装性能等が確認された暗号技術**について、デジタル庁、総務省及び経済産業省において**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。
- CRYPTREC暗号リストは以下の**3リスト**により構成される。（注：現在の3リスト構成は2013年より）

①電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト

②推奨候補暗号リスト

安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

③運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト。

CRYPTREC Cryptography Research and Evaluation Committees

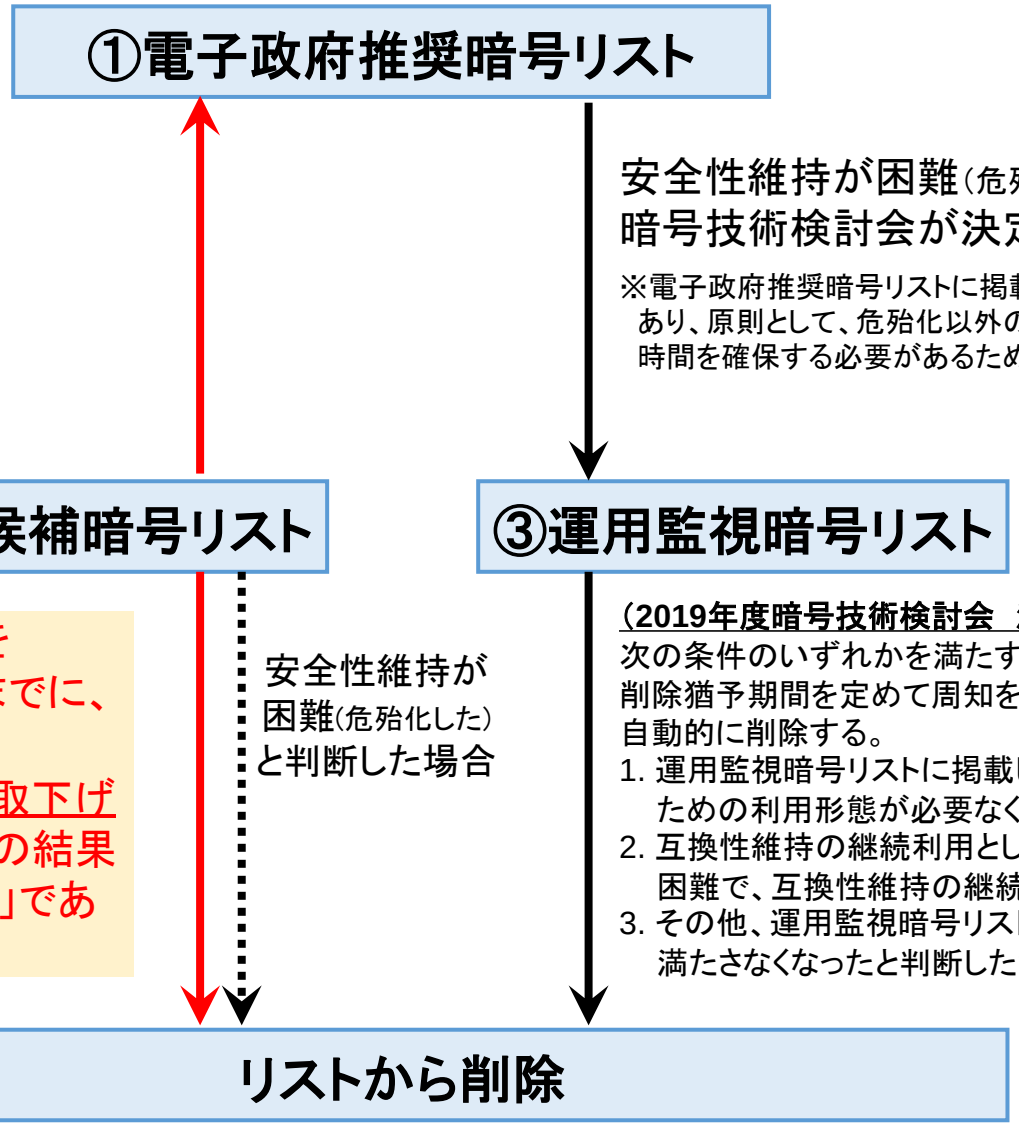
CRYPTREC暗号リスト移行ルール

次の条件のいずれかを満たすと暗号技術検討会が決定した場合
1. 5年ごとの利用実績調査により、複数の利用実績を確認した場合
2. その他、普及していることが明らか又は急速な普及が大いに見込まれる場合

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合（公募や事務局提案等）

- CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの
- 公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」であると判断されたもの

※利用実績調査の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。



CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの更新（2024年5月16日更新）

■ **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）に関して、次のとおり更新を実施。**

- DSAについて

  NIST FIPS PUB 186-4は2024年2月3日に廃止されたが、安全性・利用実績の状況に大きな変化がないため、**電子政府推奨暗号リストの「DSA」**について、注釈として「FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。」を追記した。

- Triple DESついて

  NIST SP 800-67 Revision 2は2023年12月31日に廃止されたが、暗号技術活用委員会からの回答を踏まえ、**運用監視暗号リストの「3-key Triple DES」**について、注釈として「SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。」を追記した。

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の策定（暗号技術評価委員会）

■ 耐量子計算機暗号ガイドライン（2024年度版）

- 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、耐量子計算機暗号に関する調査結果をまとめたもの。
- 耐量子計算機暗号に関する調査報告書と、調査報告書を簡略化したガイドライン（それぞれ2024年度版）を作成することが承認され、各章の大まかな更新内容を確認。
- 対象：
  - ➢ 調査報告書：暗号技術に携わる研究者・技術者　➢ ガイドライン：一般的な読者・暗号初学者

■ 軽量暗号ガイドライン（2023年版）

- 計算リソースの限られたデバイスにも実装可能な軽量暗号について、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的に作成したガイドライン。
- 2016年に発行した「軽量暗号ガイドライン（2016年版）」に対して、ガイドラインの更新方針及び2021年度から2023年度にかけて実施した外部評価に基づき更新し、外部有識者レビューを経て軽量暗号ガイドライン（2023年版）として公表。
- 対象：情報システムのセキュリティ機能の設計・開発・実装において暗号技術を活用する技術者

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の策定（暗号技術活用委員会）

■ TLS暗号設定ガイドラインの改訂

- TLS通信での安全性と相互接続性のバランスを踏まえたTLSサーバの設定方法を示すことを目的としたガイドライン。WebにTLSを利用するシステムが主な対象。
- 2020年に発行した「TLS 暗号設定ガイドライン（Ver3.0.1）」に対して、「鍵長」基準から「ビットセキュリティ」基準への変更、TLSでの利用を推奨／禁止する暗号アルゴリズムの改訂、「セキュリティ例外型」の取り扱い、DHEの強度設定について推奨要件の改訂要否などの観点で改訂しVer3.1として発行。
- 対象：TLSサーバを実際に構築するにあたって具体的な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びにTLSサーバの構築を発注するシステム担当者

■ 暗号鍵管理ガイダンスの拡充

- 暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計で明記する事項や考慮する点などを解説することを目的としたガイダンス。
- 2022年に発行した「暗号鍵管理ガイダンス」では記載を見送った、暗号鍵管理システムの設計原理と運用ポリシー、及び、暗号鍵管理デバイスへのセキュリティ対策について記載すべき内容を整理。
- 対象：暗号鍵管理機能を持つシステム設計者

https://www.cryptrec.go.jp/