CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会 活動報告 (2025年度～2026年度)

2026年7月31日

暗号技術評価委員会　委員長
高木 剛（東京大学、教授）

2025年度 暗号技術評価委員会の位置付け

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会

Advisory Board for Cryptographic Technology

事務局：デジタル庁、総務省、経済産業省

暗号技術評価委員会

Cryptographic Technology Evaluation Committee

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 新技術等に係る調査

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

Cryptographic Technology Promotion Committee

事務局：IPA、NICT

クラウド鍵管理ガイダンスWG
2025年7月～

2025年度 暗号技術評価委員会の委員構成

委員長　高木　剛	
委員　青木　和麻呂	委員　千田　浩司
委員　伊藤　忠彦	委員　花岡　悟一郎
委員　岩田　哲	委員　藤崎　英一郎
委員　上原　哲太郎	委員　本間　尚文
委員　大東　俊博	委員　松本　勉
委員　國廣　昇	委員　山村　明弘
委員　四方　順司	

敬称略

暗号技術評価委員会の活動目的

活動目的

■ CRYPTREC暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価

活動概要

■ 暗号技術の安全性及び実装に係る監視及び評価

① CRYPTREC暗号リストの監視

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格、運用監視暗号リストからの危殆化が進んだ暗号の削除に係る検討

③ CRYPTREC注意喚起レポートの発行

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加に係る検討

⑤ 新技術などに関する調査及び評価

■ 暗号技術の安全な利用方法に関する調査

①CRYPTREC暗号の監視

CRYPTREC暗号リスト掲載の暗号技術に関する研究動向の監視

■ CRYPTREC Report 2025 暗号技術評価委員会報告にて監視状況を報告*

電子政府推奨暗号リストの安全性に懸念を持たせるような事態は生じていない

■ 仕様参照先の変更

- 鍵共有方式ECDHの仕様書参照先の変更
- 共通鍵暗号Camellia, KCipher-2, MUGI, MULTI-S01、公開鍵暗号 PSEC-KEM、メッセージ認証コード PC-MAC-AESに関する連絡先・担当者の変更

■ 素因数分解・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を予測した図の更新

- ムーアの法則を仮定し、年度末から20年後までの外挿線を直線で引き、評価に大きな変動がない限り、安全側に配慮した評価として予測図を更新

*CRYPTRECのWebページ（https://www.cryptrec.go.jp/）で確認可能

仕様参照先の変更

CRYPTREC Cryptography Research and Evaluation Committees

■ 鍵共有方式ECDHの仕様書参照先の変更

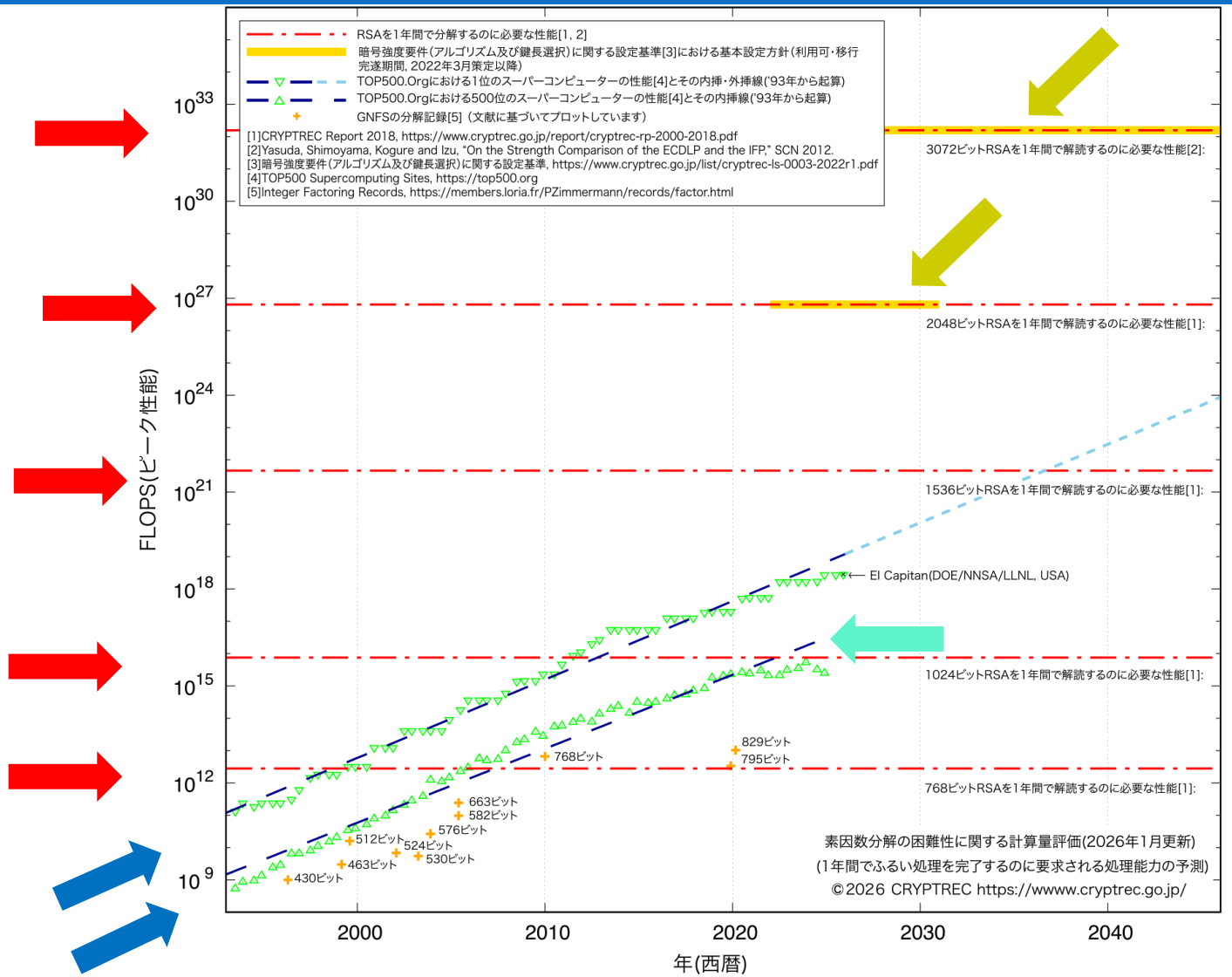
- 旧参照先

SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0)
参照先https://www.secg.org/SEC1-Ver-1.0.pdf
または
NIST SP 800-56A Revision 2 (May 2013) において、C(2e, 0s, ECC CDH) として規定されたもの
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

- 新参照先

SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0)
参照先https://www.secg.org/SEC1-Ver-1.0.pdf
または
NIST SP 800-56A Revision 3 (April 2018) において、C(2e, 0s, ECC CDH) として規定されたもの
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
※使用するメッセージ認証コードはHMAC またはAES-CMAC に限る。

素因数分解の困難性に関する計算量評価



修正①

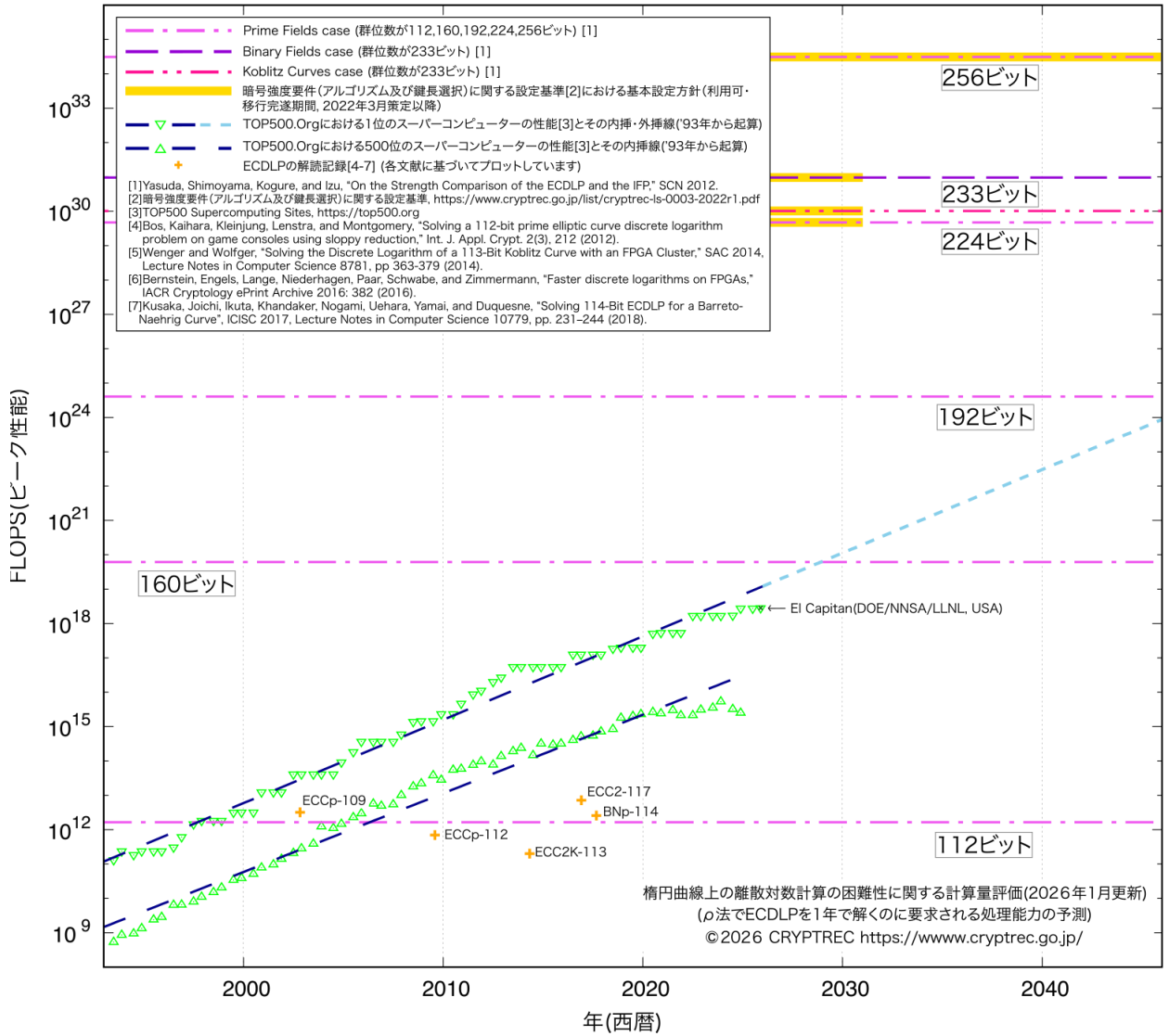
暗号強度要件(アルゴリズム及び鍵長)に関する設定基準における基本設定方針(利用可・移行完遂期間、2022 年3 月策定以降)に対応するパラメータの領域を黄色の太線で示す

修正②

上位500位の内挿線は2024年度までとする
(以降の外挿線は削除)

図:素因数分解の困難性に関する計算量評価(2026年1月更新)

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



修正③

群位数が233ビットのBinary Fields及びKoblitz Curvesに対応する計算量（112ビットセキュリティ相当）を追記

図：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(2026年1月更新)

耐量子計算機暗号ML-KEMの安全性・実装性能評価

■ 背景

CRYPTREC暗号リストへの掲載に向けたPQCの技術的検討として、耐量子計算機暗号ML-KEMの評価を行う

- 過去の事例に従い、安全性評価２件、実装性能評価１件

■ 2025年度外部評価①（立教大学理学部　安田 雅哉 教授）

- ML-KEMの安全性について、Module構造などML-KEMに特化したものを含めて公開されている解析手法とそれらの影響を調査

■ 2025年度外部評価②（PQShield社）

- ML-KEMの安全性について、サイドチャネル攻撃などを含め公開されている解析手法とそれらの影響を調査
- ML-KEMの実装性能について調査、ECDH等既存の鍵共有方式との比較を行う

耐量子計算機暗号ML-KEMの安全性・実装性能評価

調査結果の概要（安全性）

- ML-KEMのIND-CCA2安全性はROM、QROMのもとでModule-LWE問題へと帰着される安全性証明が与えられている
- サイドチャネル攻撃に対してはマスキングおよびハイディングが有効
- 計算量見積りは以下の通りであり、各安全性レベルの要求を満たしている
  - いくつかの解析モデルではアルゴリズムが攻撃者に有利な形で単純化されており、ゲートコストが過小評価となり要求を下回るものの、実際にはマージンがあると判断

暗号パラメータセット	ML-KEM-512	ML-KEM-768	ML-KEM-1024
NIST安全性レベル	レベル1	レベル3	レベル5
要求されるゲートコスト（ビット）	143	207	272
攻撃に必要なゲートコスト（ビット）	151.5	215.1	287.3
Primal攻撃のゲートコスト（ビット）	140.2	201.0	270.7
Dual攻撃のゲートコスト（ビット）	149.9	214.3	288.5
Hybrid攻撃のゲートコスト（ビット）	139.7	196.4	262.3

BKZシミュレーションとd4fに基づくprimal攻撃モデル

幾何級数仮定を用いたMATZOV計算量モデル

耐量子計算機暗号ML-KEMの安全性・実装性能評価

調査結果の概要（実装性能）

■ ECDHとML−KEMのソフトウェア実装における計算時間の比較（ミリ秒）

鍵共有アルゴリズム		安全性レベル	KeyGen	Encap	Decap
古典	EC X25519	1†	0.027	0.058	0.029
	EC P-256	1†	0.008	0.058	0.047
	EC P-384	3†	0.088	0.327	0.229
	EC P-521	5†	0.098	0.341	0.226
量子	ML-KEM-512	1	0.020	0.014	0.023
	ML-KEM-768	3	0.031	0.020	0.032
	ML-KEM-1024	5	0.047	0.028	0.043
ハイブリッド	X25519 + ML-KEM-768	1† + 3	0.061	0.076	0.060
	P−256 + ML-KEM-768	1† + 3	0.044	0.076	0.076
	P−384 + ML-KEM-1024	3† + 5	0.143	0.344	0.256

ML-KEMはECDHと同等以上の処理性能

1†、3†、5†は古典安全性レベルを表しており、耐量子安全性は考慮していない。

耐量子計算機暗号ML-KEMの安全性・実装性能評価

■ 暗号技術評価委員会としての見解

- ML-KEMは、全てのパラメータセット（ML-KEM-512/768/1024）において、米国NIST が規定する安全性レベル1/3/5 を満たしている。
- ML-KEMは、従来方式と比較して高速である一方、鍵長および暗号文長が増加するが、メモリ制約が厳しいデバイスを除き、実用上問題なく利用できる。
- ML-KEMは、サイドチャネル攻撃対策が不十分な場合に脆弱性が生じる可能性があるものの、適切な対策の実装を前提とすれば、電子政府システムを含む多様なシステムへの広範な展開が可能である。

⑤新技術などに関する調査及び評価

■ 耐量子計算機暗号に関するガイドライン・調査報告書の2026年度版を作成

- ●暗号技術調査ワーキンググループ（耐量子計算可能）活動報告にて概要を報告

■ 耐量子計算機暗号への移行に関する技術動向調査

- PQCへの移行に関する技術動向を調査、公開情報を基にまとめた外部評価報告書として出版

耐量子計算機暗号への移行に関する技術動向調査

■ 背景

- ●世界各国の機関からPQCへの移行に関する情報が公表されている
- ●PQCへの移行に向けた技術的課題の検討が必要

■ 2025年度外部評価③ （株式会社日立製作所）

- ●暗号技術ガイドライン（耐量子計算機暗号）2024年度版第2章「PQCの活用方法」における技術的な部分を掘り下げて体系的に整理
- ●2020年度に公開した「ハイブリッドモードに関する技術動向調査」を踏まえ、ハイブリッドモードに関する技術動向を再整理

耐量子計算機暗号への移行に関する技術動向調査

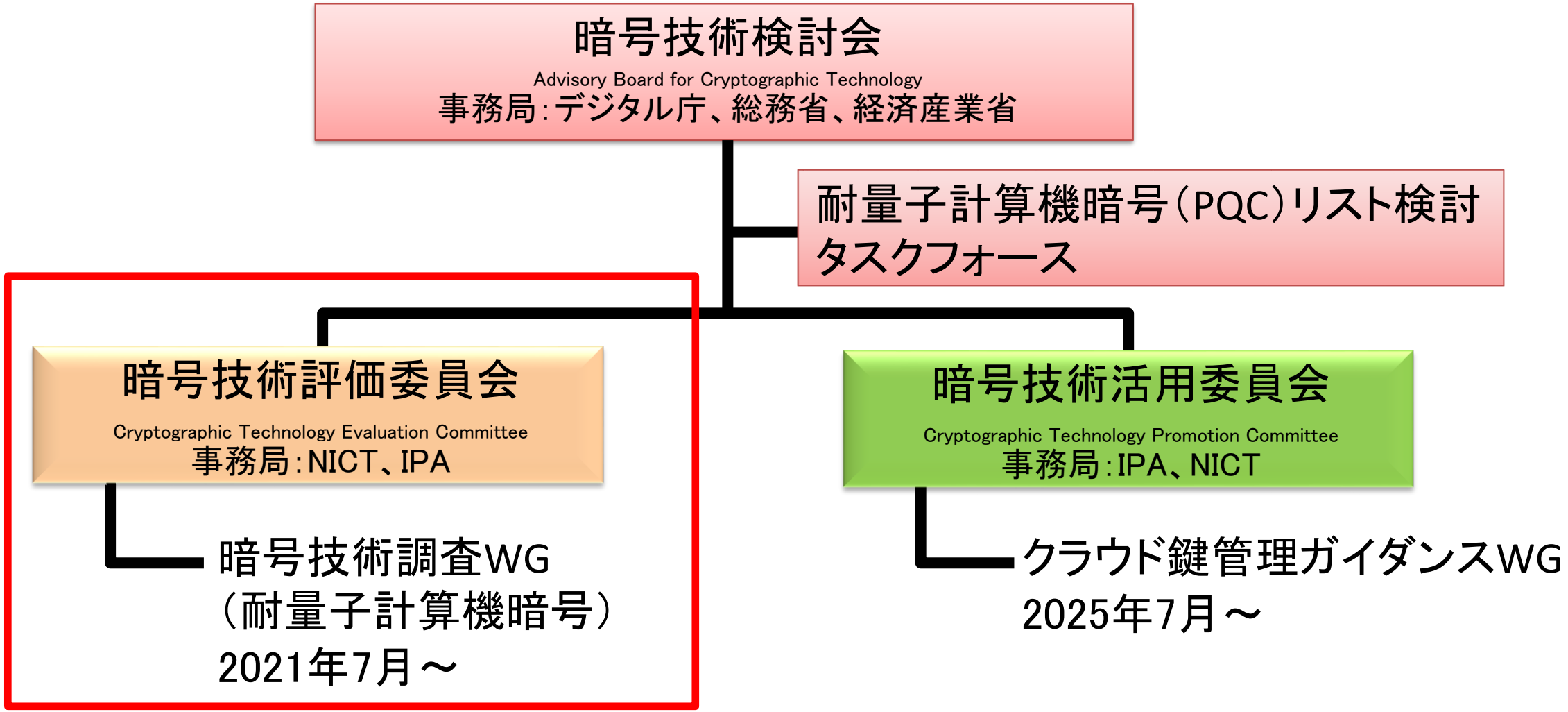
■ 調査結果の概要

- PQC移行、導入時の技術的課題、アプローチについて署名、守秘、鍵共有の用途別に整理
- ハイブリッド構成を目的と運用主体のレイヤーから体系的に整理
- ハイブリッド構成の安全性、実装、運用、標準化動向に関する事例を含めた解説
  - 2020年外部評価の時点ではハイブリッド構成は概念レベルであり、標準化活動も議論が始まったばかりであったのに対し、2026年1月時点では主要な標準化機関で技術仕様として確立されている

■ 暗号技術評価委員会としての見解

提出された外部評価報告書は、2025 年度の調査対象である耐量子計算機暗号への移行に関する技術動向調査として十分な内容を含んでいると考えられることから、本報告書をCRYPTRECの技術調査報告書とすることが承認された。

2026年度 暗号技術評価委員会の位置付け



2026年度 暗号技術評価委員会の委員構成

委員長　高木　剛	
委員　青木　和麻呂	委員　千田　浩司
委員　伊藤　忠彦	委員　花岡　悟一郎
委員　岩田　哲	委員　藤崎　英一郎
委員　上原　哲太郎	委員　本間　尚文
委員　大東　俊博	委員　松本　勉
委員　國廣　昇	委員　山村　明弘
委員　四方　順司	

2026年度 暗号技術評価委員会の活動計画

■ 暗号技術の安全性及び実装に係る監視及び評価

① CRYPTREC暗号リストの監視

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格、運用監視暗号リストからの危殆化が進んだ暗号の削除に係る検討

③ CRYPTREC注意喚起レポートの発行

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加に係る検討

- FIPS204(ML-DSA)、205(SLH-DSA)に関する安全性評価・実装性能評価に関する活動を継続

⑤ 新技術などに関する調査及び評価

- 暗号技術調査WG（耐量子計算機暗号）を通じてPQCに関する最新動向を把握、調査報告書およびガイドラインの公表

■ 暗号技術の安全な利用方法に関する調査

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術調査ワーキンググループ（耐量子計算機暗号）活動報告

2026年7月31日

ワーキンググループ　主査
國廣 昇（筑波大学、教授）

2025-2026年度耐量子計算機暗号WG委員

主査　國廣　昇	
委員　青木　和麻呂	委員　成定　真太郎
委員　伊藤　忠彦	委員　廣瀬　勝一
委員　下山　武司	委員　安田　貴徳
委員　高木　剛	委員　安田　雅哉
委員　高島　克幸	

敬称略

耐量子計算機暗号WGの活動目的

■ 背景

- ●量子コンピュータが実用化されても安全性を保てると期待される暗号（耐量子計算機暗号:PQC）の研究開発、標準化、移行などが各国で進められている
- ●国内においても耐量子計算機暗号についての議論が進められている
- ●2022年度、2024年度に耐量子計算機暗号の調査報告書・ガイドラインを作成、公表

■ WGの活動目的

- ●2026年9月末までの耐量子計算機暗号に関する情報を網羅的に調査
- ●2026年度までに、耐量子計算機暗号の新たな調査報告書・ガイドラインを作成する

耐量子計算機暗号WGの活動概要（技術動向調査）

- 「耐量子計算機暗号の研究動向調査報告書」（2018年度）「耐量子計算機暗号の研究動向調査報告書」（2022年度、2024年度）を基に技術動向調査を行う
- 2026年9月末までの耐量子計算機暗号に関する情報を網羅的に調査
  - 国際会議Crypto、Eurocrypt、Asiacrypt、PQCrypto
- 2024年度の報告書において速報としていた内容の拡充
  - 韓国KpqC最終方式決定
  - NIST PQC第4ラウンド終了、符号ベースKEM HQCのNIST FIPS207標準化決定

2026年度版調査報告書・ガイドラインに向けた調査活動

■ 各章とも調査報告書は網羅的な情報、ガイドラインはその抜粋としている

1章（はじめに）

2章（PQCの活用方法）

3章（格子に基づく暗号技術）

4章（符号に基づく暗号技術）

5章（多変数多項式に基づく暗号技術）

6章（同種写像に基づく暗号技術）

7章（ハッシュ関数に基づく署名技術）

1章　はじめに

■ 量子コンピュータの開発と暗号解読の現状

- 素因数分解問題、離散対数問題、PQCに関わる計算問題での実験を中心に、量子コンピュータによる暗号解読に関わる文献を調査
- 2026年7月の時点で、現実的な大きさのパラメータを持つ暗号が解かれたという報告は調査範囲では存在しない

■ PQC の研究及び標準化等に関する動向

- PQCに関する国際会議・イベントの開催状況
- NIST PQCなどの標準化、世界各国の標準暗号・推奨暗号選定の動向
  - ➢ 推奨暗号・許容暗号リストを公開している世界13か国の状況調査

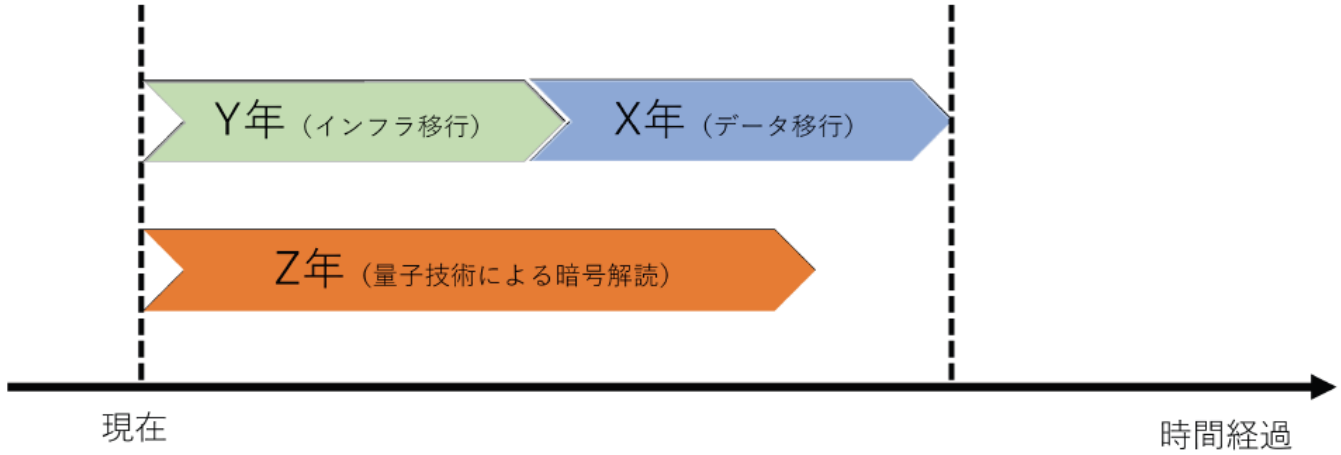
■ 調査対象としたPQCの種類

- 格子、符号、多変数多項式、同種写像、ハッシュ関数に基づく暗号方式を調査

※色付きは2024年度版報告書と比較して大きな差分を予定している箇所

2章　PQC の活用方法

- PQCの実社会での活用方法
  - IETFにおけるPQC標準化、ハイブリッドの動向
- 公開鍵暗号の用途を署名、守秘、鍵共有に分類
- 利用形態ごとの利用方法
- 利用形態ごとのPQC移行にかかわる課題
  - クリプト・インベントリの構築
  - クリプトグラフィック・アジリティの確保



3～7章　暗号技術の解説（各章で共通した内容）

格子、符号、多変数多項式、同種写像、ハッシュ関数に基づく暗号技術を
各章で取り上げる

■ 安全性の根拠となる計算問題の紹介
- 代表的な解法アルゴリズム、計算量
- 最新の攻撃状況（公開チャレンジの動向）

■ 暗号方式の基本設計の紹介
- 教科書的な基本の暗号方式、構成のフレームワーク

■ 実用的な暗号方式の設計
- 標準化方式など、世界的に使用が見込まれる方式
- アルゴリズムの疑似コード、基本的な暗号方式との関係
- 実装パラメータ（暗号文長、署名長、鍵長）および実装性能の記述

3～7章　暗号技術の解説（個別の章ごとの内容）

- 格子に基づく暗号技術
  - ML-DSAのCRYPTREC外部評価報告書に合わせた内容の更新
- 符号に基づく暗号技術
  - HQCの最新仕様書に合わせた内容の更新
  - 近年の新たな安全性仮定およびそれらに基づく署名方式の調査報告
- 多変数多項式に基づく暗号技術
  - NIST PQC追加署名方式（UOV型、MPC-in-the-Head型）の調査報告
- 同種写像に基づく暗号技術
  - 最近の安全性証明技術の進展、SQISign署名方式に関する議論の進展
- ハッシュ関数に基づく署名技術
  - 署名回数の上限が小さい用途に向けた追加パラメータの議論

2026年度 PQCWGの活動計画

耐量子計算機暗号の技術動向調査を行い、
2026年度中に新たな調査報告書・ガイドラインを公表する

■ NIST PQCを中心に大きな動きが続いている

- 追加署名第3ラウンドが開始、9件の暗号方式が候補として残っている
- 標準化された方式に関しても追加パラメータの議論が行われている

■ 調査の方針

- 2026年9月末までの耐量子計算機暗号に関する情報を網羅的に調査
- それ以降でも大きな話題があれば掲載
- 過去の報告書・ガイドラインで取り上げた分類以外の暗号技術でも、必要があれば取り上げて紹介

おわりに

委員会活動・外部評価・ガイドラインの公開

CRYPTREC Report 2025 暗号技術評価委員会報告

■ 検索： CRYPTREC 暗号技術評価委員会

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

外部評価報告書

■ 検索： CRYPTREC 外部評価

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

健全なサイバー空間の実現・維持に向けて

今後も暗号技術評価委員会では、

- 暗号技術の安全性及び実装に係る監視及び評価
- 新技術等に係る調査
- 暗号技術の安全な利用方法に関する調査

など、健全なサイバー空間の実現・維持につなげるべく、
暗号技術の安全性という観点から必要とされる活動を展開していく所存です。

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