CRYPTREC
Cryptography Research and Evaluation Committees

# 暗号技術評価委員会 活動報告 (2024年度～2025年度)

2025年7月25日

暗号技術評価委員会　委員長
高木 剛（東京大学、教授）

# 2024年度 暗号技術評価委員会の位置付け

**暗号技術検討会**
（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**
（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）

# 2024年度 暗号技術評価委員会の委員構成

| | | | |
|---|---|---|---|
| 委員長 | 高木　剛 | 委員 | 手塚　悟 |
| 委員 | 青木　和麻呂 | 委員 | 花岡　悟一郎 |
| 委員 | 岩田　哲 | 委員 | 藤﨑　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 | 松本　泰 |
| 委員 | 四方　順司 | 委員 | 山村　明弘 |

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暗号等の監視

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 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

④ CRYPTREC注意喚起レポートの発行

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 2024 暗号技術評価委員会報告にて監視状況を報告*1

## 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

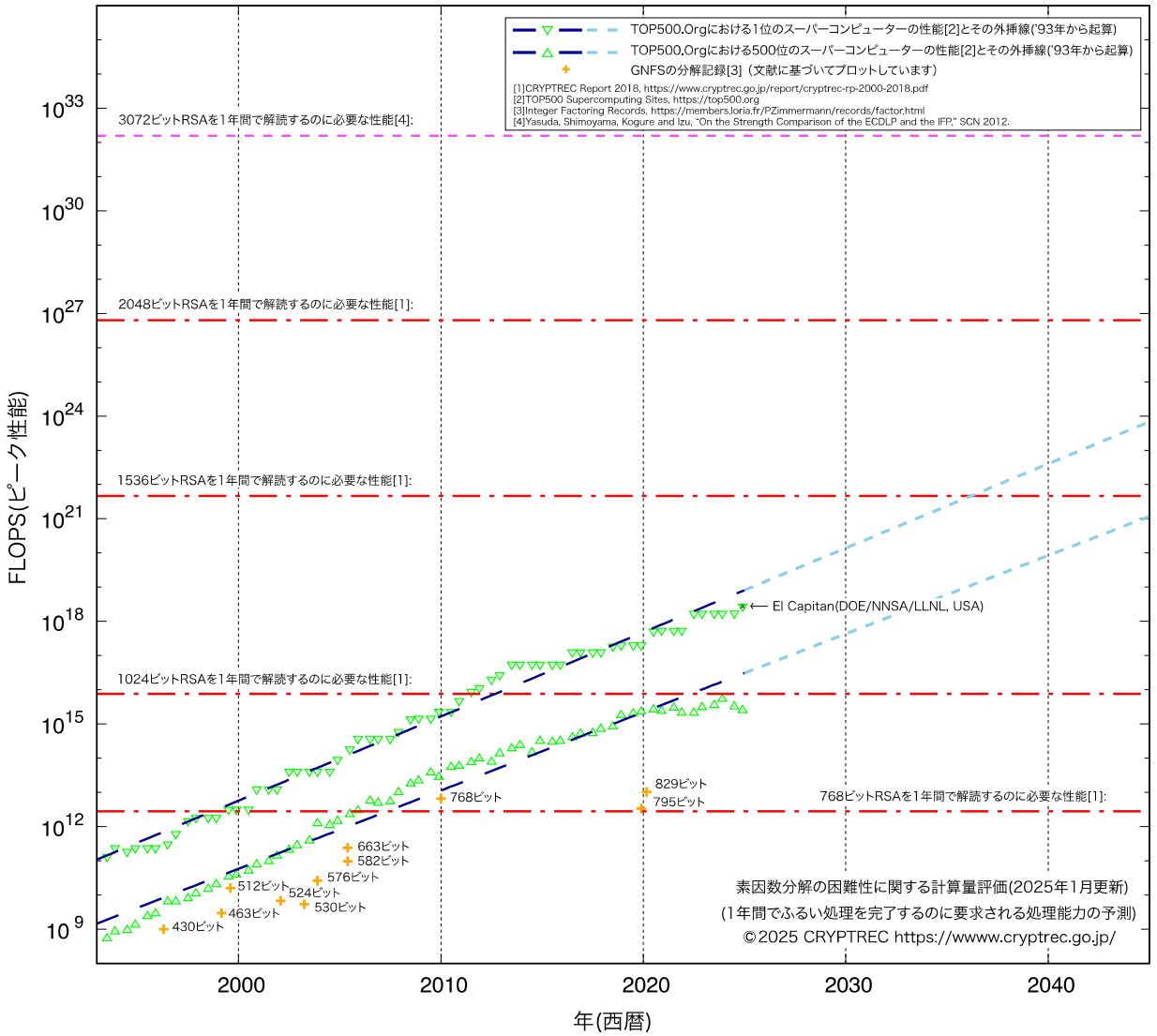
- ムーアの法則を仮定し、年度末から20年後までの外挿線を直線で引き、評価に大きな変動がない限り、安全側に配慮した評価として予測図を更新
- 公開鍵暗号のパラメータ選択に関する対応方針について、安全性以外にも相互接続性など、運用上の観点もあるため、関係各所などを含めて検討

## 仕様参照先の変更

- 仕様書の更新を確認した場合、旧バージョンとの差分を調査した上で参照先を更新*1

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

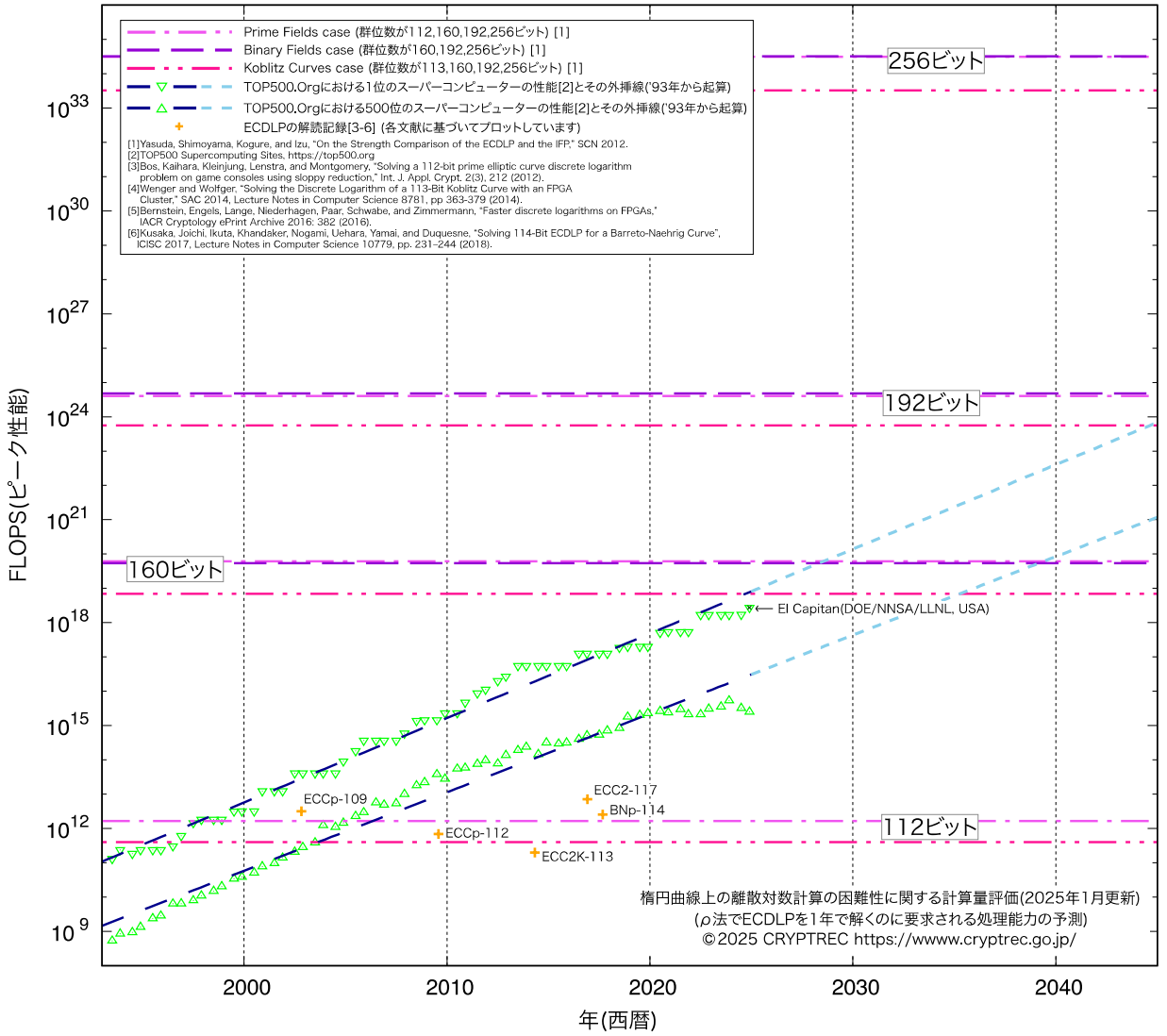
# 素因数分解の困難性に関する計算量評価




**図：素因数分解の困難性に関する計算量評価(2025年1月更新)**

CRYPTREC
Cryptography Research and Evaluation Committees

# 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




**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(2025年1月更新)**

CRYPTREC Cryptography Research and Evaluation Committees

# 仕様参照先の変更

CRYPTREC暗号の仕様書参照先をCRYPTRECのWebサイトに掲載

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

## ECDSAとAESの仕様参照先の変更を実施

■ アルゴリズム部分に変更がないことを確認済み

| 暗号技術名 | 旧参照先 | 新参照先 |
|---|---|---|
| ECDSA | ANS X9.62-2005(*1)<br>(*1) 仕様書は、一般財団法人日本規格協会で購入が可能です。 | ANS X9.142-2020(*1)<br>(*1) 仕様書は、https://www.x9.org/ で購入が可能です。 |
| AES | NIST FIPS PUB 197<br>https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf | NIST FIPS PUB 197<br>https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf |

# ⑤新技術等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2024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

2024年度外部評価

■ 量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版

CRYPTREC
Cryptography Research and Evaluation Committees

# 量子コンピュータが共通鍵暗号の安全性に及ぼす影響

## 背景

- 2019年度外部評価「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」の実施から約5年が経過
- 耐量子計算機暗号に関するガイドライン・調査報告書では、共通鍵暗号の耐量子安全性に関する内容が対象外

## 実施概要

- 依頼先：細山田 光倫 様（NTT株式会社）
- 主な依頼内容
  - 公開されている解析手法やその影響範囲
  - CRYPTREC暗号リストやCRYPTREC暗号技術ガイドライン（軽量暗号）2023年度版に含まれる主要な共通鍵暗号方式などに及ぼす影響の考察
  - 2019年度外部評価の結果に最新の情報を反映させ、2024年度版として報告書を作成

CRYPTREC Cryptography Research and Evaluation Committees

# 量子コンピュータが共通鍵暗号の安全性に及ぼす影響

## 調査結果の概要

- 攻撃種別を、Q2モデル（量子クエリ攻撃モデル）での攻撃、Q1モデル（古典クエリ攻撃モデル）での攻撃、ハッシュ関数への攻撃の3種類に分類
- CRYPTREC暗号やNIST標準軽量暗号Asconの安全性への影響範囲を確認

| | |
|---|---|
| Q2モデルでの攻撃 | 影響なし |
| Q1モデルでの攻撃 | Groverのアルゴリズムの影響を考慮<br>➢ $k$ビット鍵の全数探索が$O\left(2^{k/2}\right)$で実行可能*1 |
| ハッシュ関数への攻撃 | 汎用量子衝突攻撃（特に、BHTのアルゴリズム）の影響を考慮<br>➢ ハッシュ関数が$c$ビットのキャパシティ*2、$h$ビットの出力長である場合、量子衝突探索が$\min\left(2^{c/3}, 2^{h/3}\right)$で実行可能*3 |

*1 $k$ビット鍵の全数探索に係る古典計算量：$O\left(2^{k}\right)$

*2 スポンジ構造型ハッシュ関数のパラメータ

*3 $c$ビットキャパシティ、$h$ビット出力のハッシュ関数の衝突探索に係る古典計算量：$\min\left(2^{c/2}, 2^{h/2}\right)$

CRYPTREC
Cryptography Research and Evaluation Committees

# 量子コンピュータが共通鍵暗号の安全性に及ぼす影響

## 2019年度外部評価時における結論との差異

■ ハッシュ関数に関する技術動向の変化

| 2019年度外部評価時 | 現在 |
|---|---|
| 古典的に128ビット安全なハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい。 | 重要な用途に供するハッシュ関数の出力長BHTのアルゴリズムの計算量を基準とし、ビット長384ビット、もしくは512ビットのハッシュ関数を用いた方が無難である。 |

## 暗号技術評価委員会としての見解

■ CRYPTREC暗号やNIST標準軽量暗号Asconの安全性に量子コンピュータが及ぼす影響は、汎用量子アルゴリズム（特に、Groverのアルゴリズムと BHTのアルゴリズム）のみを考慮すれば十分である。

# 2025年度 暗号技術評価委員会の位置付け

**暗号技術検討会**
（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**
（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）

# 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 | 四方　順司 |
| 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 | 藤﨑　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 |

敬称略

# 2025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暗号等の監視

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 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

④ CRYPTREC注意喚起レポートの発行

⑤ 新技術などに関する調査及び評価

- 継続して、暗号技術調査WG（耐量子計算機暗号）を設置し、PQCに関する最新動向を把握
- NIST標準のFIPS 203, 204, 205に関する安全性評価・実装性能評価に関する活動を開始
- ハイブリッドモードを含む、PQCへの移行を踏まえた技術動向調査を開始

## 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

2025年7月25日

ワーキンググループ　主査
國廣 昇（筑波大学、教授）

# 2023-2024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 | |

# 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
- CRYPTRECは2022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し公開した

## ■ WGの活動目的

- 2024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
- 2024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）を基に調査
- 2024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
- それ以降でも大きな話題があれば取り上げた
  - 韓国KpqC 第2ラウンド終了、4方式の選定
  - NIST PQC 追加署名公募 第2ラウンド終了、14方式の選定
  - NIST PQC 第4ラウンド終了、HQCの選定

## ■ 調査報告書およびガイドラインの公開

- 耐量子計算機暗号の研究動向調査報告書2024年度版
- CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）2024年度版

# 2024年度版　耐量子計算機暗号の研究動向調査報告書

■技術者や専門家が対象
■PQCとして署名・守秘・鍵共有を扱う
　（CRYPTREC暗号リストの中で「公開鍵暗号」として分類されている技術）
■安全性の根拠となる計算問題の種類ごとに技術を分類

**暗号技術関連の調査報告** https://www.cryptrec.go.jp/tech_reports.html

| 年度 | 報告書名 | 文書番号 |
|---|---|---|
| 2024 | 「耐量子計算機暗号の研究動向調査報告書」 | CRYPTREC TR-2001-2024 |
| 2022 | 「耐量子計算機暗号の研究動向調査報告書」 | CRYPTREC TR-2001-2022 |
| 2018 | 「耐量子計算機暗号の研究動向調査報告書」 | CRYPTREC TR-2001-2018 |

NIST FIPSの解説
活用方法の章を追加

ハッシュベース署名の
章を追加

格子、符号、多変数
同種写像について調査

# 2024年度版　暗号技術ガイドライン（耐量子計算機暗号）

■調査報告書の抜粋
■暗号初学者が代表的なPQC方式を把握するために最小限の内容のみ

**暗号技術ガイドライン**　https://www.cryptrec.go.jp/tech_guidelines.html

| 年度 | ガイドライン名 | 文書番号 |
|---|---|---|
| 2024 | 「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024年度版」 | CRYPTREC GL-2007-2024 |
| 2023 | 「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023年度版」 | CRYPTREC GL-2006-2023 |
| 2022 | 「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」 | CRYPTREC GL-2004-2022 |
| | 「CRYPTREC 暗号技術ガイドライン（高機能暗号）」 | CRYPTREC GL-2005-2022 |

世界の動向に合わせて内容の更新

PQCの利用指針を示すために作成

# 1章　はじめに

- 暗号技術調査ワーキンググループ(耐量子計算機暗号)の活動概要
- 報告書内でのPQCの範囲の明確化
  - 古典アルゴリズムの組み合わせにより定式化され，かつ耐量子計算機性を持つことを技術的に判断できる暗号方式
  - 特に公開鍵暗号の下位分類としての公開鍵暗号方式、署名方式、鍵共有について取り扱う
- 量子コンピュータの開発と暗号解読の現状
  - 様々な種類の量子コンピュータの開発が進んでいるが、調査の範囲では全てNISQ
  - 素因数分解問題を中心に、暗号解読実験の文献を調査
  - 2024年9月末の時点で、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存在しない

# 1章　はじめに

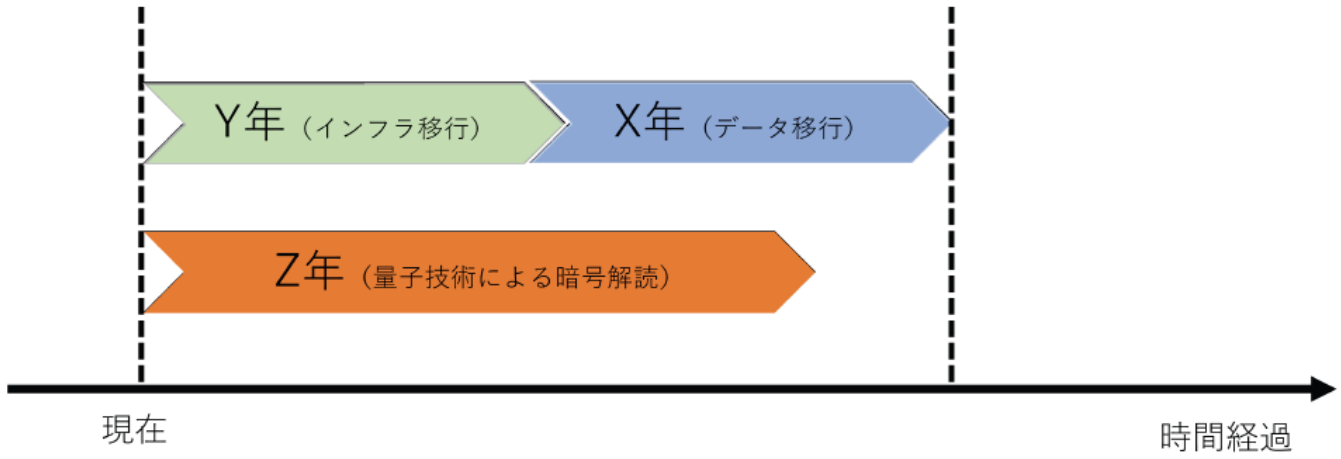
■ PQC の研究及び標準化等に関する動向
- PQCに関する国際会議
- NIST PQCなどの標準化、世界各国の標準暗号・推奨暗号選定の動向

■ 調査対象としたPQCの種類
- 格子に基づく暗号技術
- 符号に基づく暗号技術
- 多変数多項式に基づく暗号技術
- 同種写像に基づく暗号技術
- ハッシュ関数に基づく署名技術

■ 執筆者リスト

# 2章　PQC の活用方法

- PQCの実社会での活用方法
- 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

- 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）
- 代表的な暗号方式の紹介
  - 教科書的な基本の暗号方式、構成のフレームワーク
- 主要な暗号方式の紹介
  - 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

# 主要な暗号方式として取り上げたものの一覧表

| ベースとなる問題の種類 | 暗号化・鍵交換 | 署名 |
|---|---|---|
| 格子 | FIPS 203 (ML-KEM), CRYSTALS-Kyber, FrodoKEM, NewHope, NTRU, SABER | FIPS 204 (ML-DSA), CRYSTALS-Dilithium, FALCON |
| 符号 | Classic McEliece, BIKE, HQC | |
| 多変数 | | UOV, QR-UOV, MAYO, MQOM, MiRitH |
| 同種写像 | | SQISign, SQISign2D |
| ハッシュ | | LMS, XMSS, FIPS 205 (SLH-DSA) |

（赤字：暗号化・鍵交換、青字：署名、下線：ガイドライン掲載）

# 今後の予定

■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）を2025～2026年度にかけて設置、引き続き耐量子計算機暗号の技術調査を行う

- NIST PQC標準化方式に関して、新たなパラメータセットが議論されている
- NIST PQC追加署名の選定が続いており、攻撃の改良、暗号方式の修正が続いている

■ 調査の方針は2024年度版と同様

- 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追加

# おわりに

# 委員会活動・外部評価・ガイドラインの公開

## CRYPTREC Report 2024 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

## 暗号技術ガイドライン（耐量子計算機暗号）2024年度版

■ 検索： CRYPTREC ガイドライン

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

# おわりに

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
- 新世代暗号に係る調査
- 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/