CRYPTREC の活動について

國廣昇

2026 年 2 月 27 日

筑波大学システム情報系

自己紹介

氏名：國廣 昇 （くにひろ のぼる）

経歴

- 1996 年 4 月〜2002 年 6 月 NTT 研究所研究員
- 2002 年 7 月〜2008 年 2 月 電気通信大学
- 2008 年 3 月〜2019 年 4 月 東京大学
- 2019 年 5 月〜 筑波大学

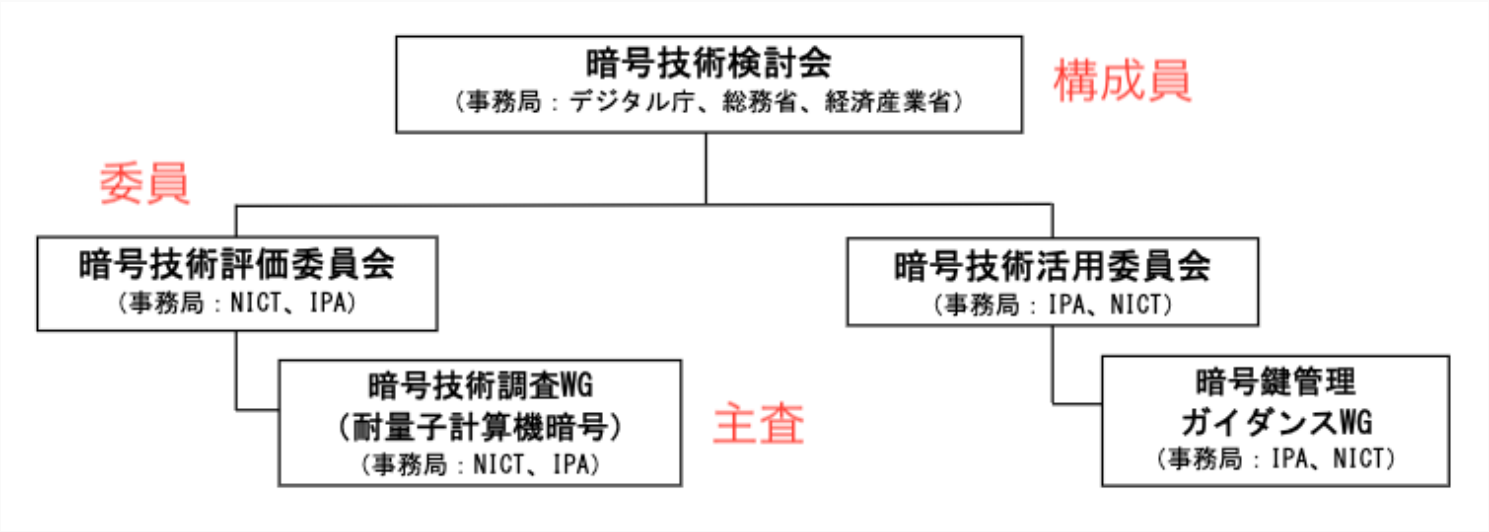
研究テーマ

暗号理論，特に，公開鍵暗号の安全性評価に関する研究

社会的貢献

CRYPTREC (Cryptography Research and Evaluation Committees)

- 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
- 「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)」を公開



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 構成員（2019 年度，2020 年度）

日本銀行金融研究所

- 国内客員研究員（2024 年 4 月〜2026 年 3 月）
  - 金融研究所ディスカッション・ペーパー「量子コンピュータによる暗号解読アルゴリズム：隠れ部分群問題から見た素因数分解問題と離散対数問題」を出版（2026-01-27）.

量子計算機

1994 年：Shor の量子素因数分解，離散対数問題アルゴリズムの提案．現在広く使われている暗号は，理論的には，量子計算機により解読される．

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）

令和5年3月30日
デジタル庁・総務省・経済産業省
（最終更新：令和6年5月16日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、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ると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA(注18)
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH

NIST による PQC 標準化

耐量子計算機暗号（Post-Quantum Cryptography, PQC）の募集

- 2015 年 8 月：NSA（米国家安全保障局）が，PQC への移行を表明
- 2016 年 2 月：NIST（米国立標準技術研究所）が，PQC の標準化計画を公表（量子計算機の実現に備えて，素因数分解，離散対数問題の困難さに依存しない暗号の募集）

レベル	基準となる解読困難性	ビットセキュリティ
I	AES-128（≈RSA-3072）と同等以上	128 bit
III	AES-192 と同等以上	192 bit
V	AES-256 と同等以上	256 bit

- 2017 年 11 月 30 日：締め切り（69 個が応募）
- 2019 年 1 月 30 日： Round 2 Candidate Algorithms 26 個を公表（鍵交換・暗号化：17 個，デジタル署名 9 個）
- 2020 年 7 月 22 日：Round 3 Candidate Algorithm Finalist 7 個，Alternate 8 個（合計 15 個）を公開

2022 年 7 月 5 日最終候補 4 件が決定

最終候補（4 件）

鍵交換・暗号化（1 件）

- CRYSTALS-KYBER（格子暗号）

デジタル署名（3 件）

- CRYSTALS-DILITHIUM（格子暗号）
- FALCON（格子暗号）
- SPHINCS+（ハッシュ関数署名）（Alternate Candidate から）

2023 年 8 月 24 日

- NIST FIPS の first draft 公開

2024 年 8 月 13 日

- FIPS 203(ML-KEM), 204 (ML-DSA), 205 (SLH-DSA)が公開
- CRYSTALS-KYBER, CRYSTALS-DILITHIUM, SPHINCS+に対応

多様性の確保（第 4 ラウンドと追加署名）

第 4 ラウンド (2022 年 7 月 5 日開始)

多様性を確保するために，鍵交換・暗号化に対して，格子暗号以外の方式を対象として，第 4 ラウンドが開始

- Classic McEliece（符号暗号）　（Finalist から）
- BIKE（符号暗号）（Alternate Candidates から）
- HQC（符号暗号）（Alternate Candidates から）
- SIKE（同種写像暗号）（Alternate Candidates から）

2025 年 3 月 8 日

- HQC が標準化候補として選定

追加署名の募集

- 2022 年 9 月 6 日：構造化格子以外の署名方式の公募開始
- 2023 年 6 月 1 日：締め切り（40 件）
- 2024 年 10 月 24 日：Round 2 進出の 14 件が決定

NIST PQC の状況の整理

鍵共有，暗号化：(2 方式)

- 標準化済：ML-KEM (FIPS 203)
- 標準化作業中：HQC-KEM (FIPS 207)

署名（3 方式+ 1 方式？）

- 標準化済：ML-DSA (FIPS 204)，SLH-DSA (FIPS 205)
- 標準化作業中：FN-DSA(FIPS206)
- 選定中：14 方式から選定中

CRYPTREC 暗号技術検討会での議論

2025 年 3 月 25 日に開催された「CRYPTREC 暗号技術検討会」の資料中「耐量子計算機暗号（PQC）への対応について」の抜粋

- 2020 年度に「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」で CRYPTREC 暗号リストへの PQC 掲載を見据えて検討したが、「PQC は、多数の方式が提案され安全性を検討している段階で、利用実績等に言及できる段階ではない」ことから、CRYPTREC 暗号リストに組み込まず、別途ガイドラインを作成することとした。
- 上記の検討から約４年が経過。政策的な観点（各国取組との調和性、国内における議論の高まりなど）を踏まえれば、上記の方針を見直すべき時期にあるのではないか。

- 今後、安全性等が確認された PQC を推奨候補リストに順次掲載できるよう準備を始めてはどうか。
  - 米欧をはじめ、複数の国において PQC への移行に関する方針や推奨アルゴリズムに関する情報が発出されている。我が国政府における PQC 移行の旗振り・総合調整役は定まっておらず、移行方針もないが、 CRYPTREC リスト掲載に向けた PQC の技術的検討は、移行方針の検討と両輪で進めるべきもの。サイバー空間における経済安全保障の観点からも、PQC のリスト掲載を遅滞なく行うことが CRYPTREC に求められている。
  - 機動的なスケジュールを前提とすれば、まずは諸外国において多くの専門家による検証を経て決定された方式（例えば FIPS 203 (ML-KEM)、FIPS204（ML-DSA)、FIPS 205（SLH-DSA)など）の安全性評価・実装性能評価を先行し、その後、国産 PQC を含めた他のアルゴリズムの取扱を順次検討し、追加の評価を実施してはどうか。

例年，暗号技術検討会は，3 月下旬に開催されています．

政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）（2025 年 11 月 20 日公表）の抜粋

米国での標準化動向とその波及効果

- PQC の国際的な標準化動向については、米国の NIST が FIPS として複数の暗号方式の標準化を進めている.
- 今後、標準化済みの FIPS の暗号方式を多くの国が用いることが想定される。

CRYPTREC での動き

- CRYPTREC において、CRYPTREC 暗号リストの更新が可能となるよう、耐量子計算機暗号（PQC）の安全性評価・実装性能評価に関する活動を開始している。
- 具体的には、2024 年 8 月に NIST 標準として公開された FIPS 203(ML-KEM)、FIPS 204(ML-DSA)、FIPS 205(SLH-DSA) を対象として、順次、安全性評価・実装性能評価を実施中である。

我が国での移行の時期

- こうした諸外国に比べて我が国における PQC への移行が遅れることになれば、諸外国との間で、安定的なネットワークの構築やサイバーセキュリティの確保、防衛や外交といった安全保障上重要な情報のやり取りに支障が出ることも想定される。
- サイバー空間は、国際的なネットワークであるところ、 国際連携等を鑑みれば、我が国も 2035 年を目標として PQC への移行を進めていくことが考えられる。
- 2035 年までの移行を目指し，政府機関等における暗号技術の利用状況等も踏まえ，関係府省庁の連携の下，2026 年度に工程表（ロードマップ）を策定し，我が国における円滑な移行を推進していく．

技術的な詳細は，

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

を御覧ください．

今後の動向については，

- CRYPTREC 暗号技術検討会資料，
- CRYPTREC シンポジウム（例年７月に開催），

などを御覧ください．