# 暗号の危殆化等について

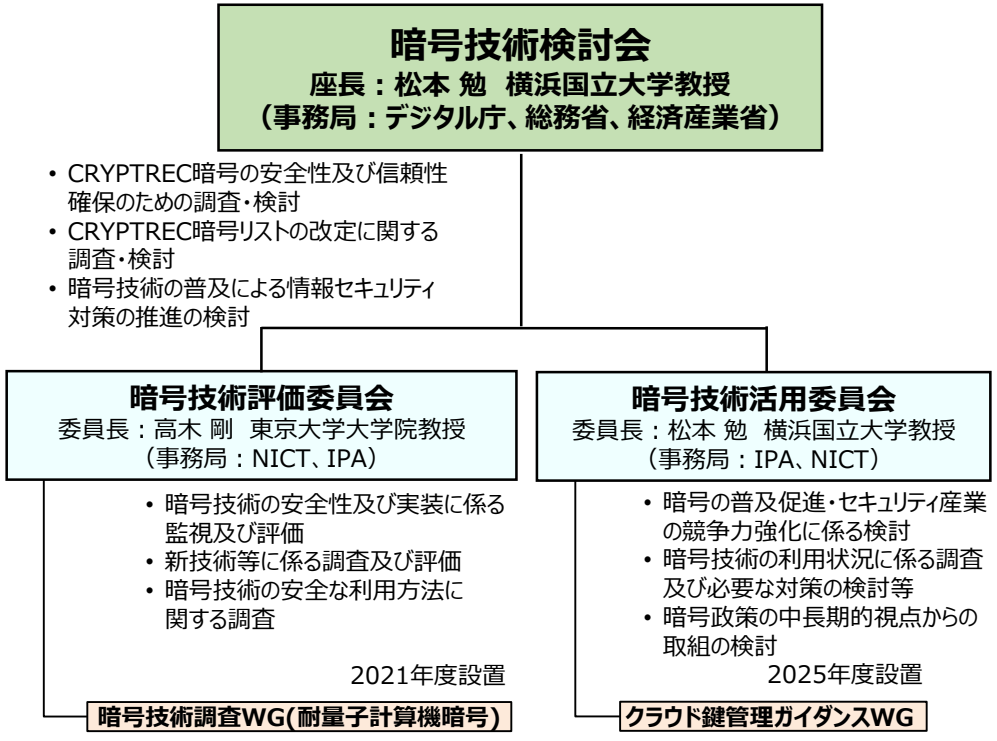
総務省
サイバーセキュリティ統括官室

# CRYPTREC（クリプトレック）

- **CRYPTREC**（**CRYPT**ography **R**esearch and **E**valuation **C**ommittees）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。
- デジタル庁・総務省・経済産業省が共同で運営する**暗号技術検討会**※と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する**暗号技術評価委員会**及び**暗号技術活用委員会**とで構成される。

※デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長の研究会として開催し、関係省庁がオブザーバとして参加している。

## CRYPTRECの体制




## 暗号技術検討会構成員

（敬称略）

| | | |
|---|---|---|
| 座長 | 松本 勉 | (国研)産業技術総合研究所 フェロー |
| 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 | (一社)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 |
| | 國廣 昇 | 筑波大学 教授 |
| | 黒田 真弓 | (一社) テレコムサービス協会 技術・サービス副委員長 |
| | 島岡 政基 | セコム株式会社 IS研究所 主幹研究員 |
| | 高木 剛 | 東京大学 教授 |
| | 田村 裕子 | 日本銀行 金融研究所 情報技術研究センター 企画役 |
| | 本間 尚文 | 東北大学 教授 |
| | 松井 充 | 三菱電機株式会社 研究開発本部　シニアフェロー |
| | 松浦 幹太 | 東京大学 教授 |
| | 松本 泰 | (NPO)日本ネットワークセキュリティ協会 フェロー |
| | 吉田 博隆 | (国研)産業技術総合研究所 研究チーム長 |
| | 渡邊 創 | (国研)産業技術総合研究所 研究部門長 |

オブザーバ

内閣官房(NCO)、個人情報保護委員会事務局、
警察庁、総務省(住民制度課)、法務省(民事局)、
外務省、財務省、文部科学省、厚生労働省、
経済産業省(国際電気標準課)、防衛省、
(国研)情報通信研究機構、(国研)産業技術総合研究所、
(独)情報処理推進機構、(一財)日本情報経済社会推進協会、
(公財)金融情報システムセンター

# CRYPTREC暗号リスト・移行ルール

- CRYPTRECでは「**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。
- **３つのリストにより構成**され、危殆化等における**移行ルールもCRYPTREC**において定められている。

## 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

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

- ✓ 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
- ✓ 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

**安全性維持が困難（危殆化した）**と暗号技術検討会が決定した場合

※ 電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

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）

## 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

安全性維持が困難（危殆化した）と判断した場合

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、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。

- ✓ 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
- ✓ 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
- ✓ その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

## リストから削除

※ 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暗号リストと鍵長要件

- CRYPTREC暗号リストに掲載されている多くの暗号技術では、一つのアルゴリズムで複数の鍵長が利用可能で、**利用する鍵長によってセキュリティ強度**と処理効率などが**変わる**。
- そのためCRYPTRECでは、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定した「**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**」を策定。
  ※利用する鍵長について、こ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。

## CRYPTREC暗号リスト(例)

| 技術分類 | | 暗号技術 | |
|---|---|---|---|
| 公開鍵暗号 | 署名 | DSA | 離散対数問題 |
| | | ECDSA | 楕円曲線離散対数問題 |
| | | EdDSA | 楕円曲線離散対数問題 |
| | | RSA-PSS | 素因数分解 |
| | | RSASSA-PKCS1-v1_5 | 素因数分解 |
| | 守秘 | RSA-OAEP | 素因数分解 |
| | 鍵共有 | DH | 離散対数問題 |
| | | ECDH | 楕円曲線離散対数問題 |
| 共通鍵暗号 | 64ビットブロック暗号 | 該当なし | |
| | 128ビットブロック暗号 | AES | |
| | | Camellia | |
| | ストリーム暗号 | KChipher-2 | |
| ハッシュ関数 | | SHA-256 | |
| | | SHA-384 | |
| | | SHA-512 | |
| | | SHA-512/256 | |
| | | SHA3-256 | |
| | | SHA3-384 | |
| | | SHA3-512 | |
| | | SHAKE128 | |
| | | SHAKE256 | |
| （略） | | （略） | |

## 暗号強度要件に関する設定基準(例)

### ＜公開鍵暗号の推定セキュリティ強度＞

| セキュリティ強度（ビットセキュリティ） | 素因数分解 | 離散対数問題 | 楕円曲線離散対数問題 |
|---|---|---|---|
| 112 | k=2048 | (L,N)=(2048,224) | P-224 等 |
| 128 | k=3072 | (L,N)=(3072,256) | P-256 等 |
| 192 | k=7680 | (L,N)=(7680,384) | P-384 等 |
| 256 | k=15360 | (L,N)=(15360,512) | P-512 等 |

### ＜セキュリティ強度要件の基本設定方針＞

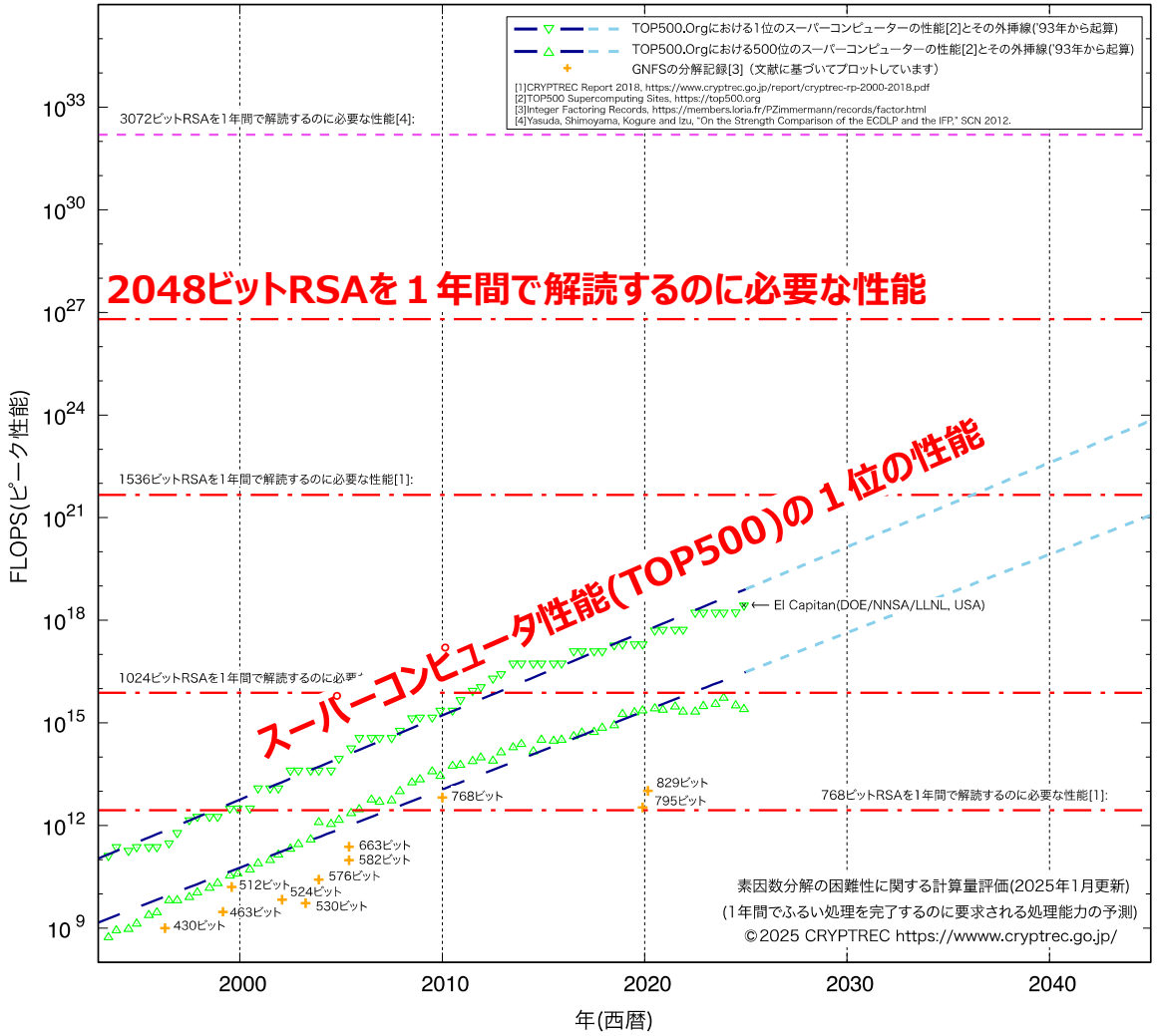
| 想定運用終了・廃棄年／利用期間 | | 2022～2030 | 2031～2040 | 2041～2050 | 2051～2060 | 2061～2070 |
|---|---|---|---|---|---|---|
| 112ビットセキュリティ | 新規生成 | 移行完遂期間 | 利用不可 | 利用不可 | 利用不可 | 利用不可 |
| | 処理 | | 許容 | | | |
| 128ビットセキュリティ | 新規生成 | 利用可 | 利用可 | 移行完遂期間 | 利用不可 | 利用不可 |
| | 処理 | | | | 許容 | |
| 192ビットセキュリティ | 新規生成 | 利用可 | 利用可 | 利用可 | 利用可 | 利用可 |
| | 処理 | | | | | |
| 256ビットセキュリティ | 新規生成 | 利用可 | 利用可 | 利用可 | 利用可 | 利用可 |
| | 処理 | | | | | |

→現状、**2048ビットRSA**は**セキュリティを確保するには必ずしも十分ではない**とされる。
(互換性・相互接続性維持のための利用に限定し、新規調達等は許容すべきでない。)
また、3072ビットRSA以上の強度を選択すべきとされている。
(2041年以降は更に高い強度の暗号を選択すべきとされている。)

# 古典コンピュータによる計算量評価予測

➢ **公開鍵暗号方式**は、**数学的な計算の困難さ**（素因数分解や離散対数計算）に基づいており、CRYPTRECでは、そうした計算の困難さの検討に関して**計算量評価の予測図**を更新・公表している。

## 素因数分解の困難性に関する計算量評価（2025年1月更新）




## 予測図の取扱い

いわゆる**ムーアの法則を仮定して外挿**線を年度末からプラス20年後まで従来通り直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として予測図を当面の間更新していく。

※予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

## 公開鍵暗号のパラメータ選択

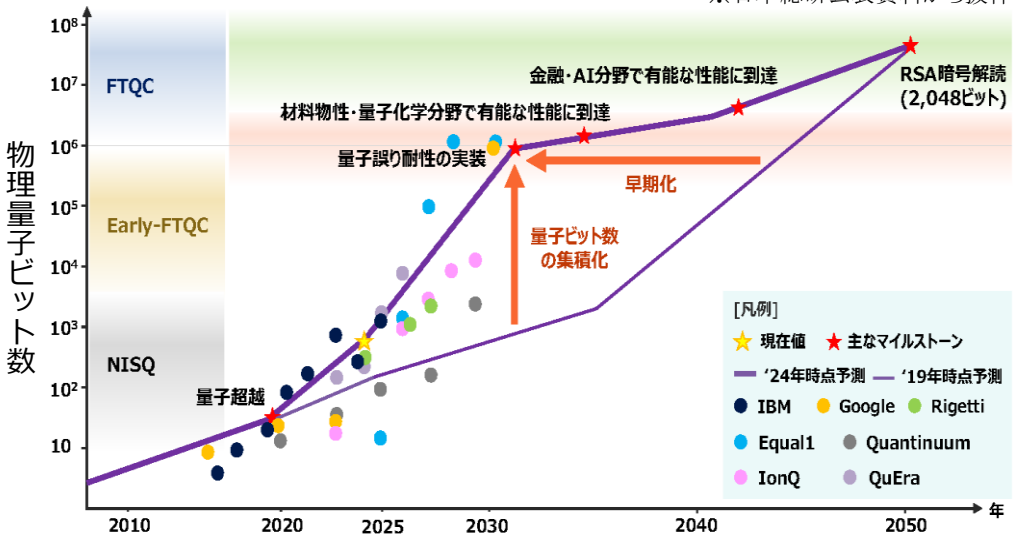
公開鍵暗号の**パラメータ選択**に関する対応方針については、**安全性以外にも相互接続性など、運用上の観点もある**ため、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討する。

# 量子コンピュータ時代における現代暗号

- **量子コンピュータ**を利用して現代暗号を**効率的に解読**する方法が存在（Shorアルゴリズム;1994年考案）
- 量子コンピュータの研究が加速しており、**将来的**に、**実用的で大規模な量子コンピュータ**の実現が想定
  → 現在広く利用されている**公開鍵暗号の安全性低下（危殆化）**のおそれ
  ※「公開鍵暗号方式」は、事前に暗号鍵を送受信先で設定する必要が無いため、ネットワーク利用等で広く利用
  事前に暗号鍵を共有する「共通鍵暗号方式」については、暗号鍵の長さを増やすことで、量子コンピュータによる影響を限定することが可能。
- データを保存しておき、量子コンピュータでの暗号解読が可能となった後に解読を行う**HNDL**※**攻撃**も懸念
  ※Harvest Now, Decrypt Later

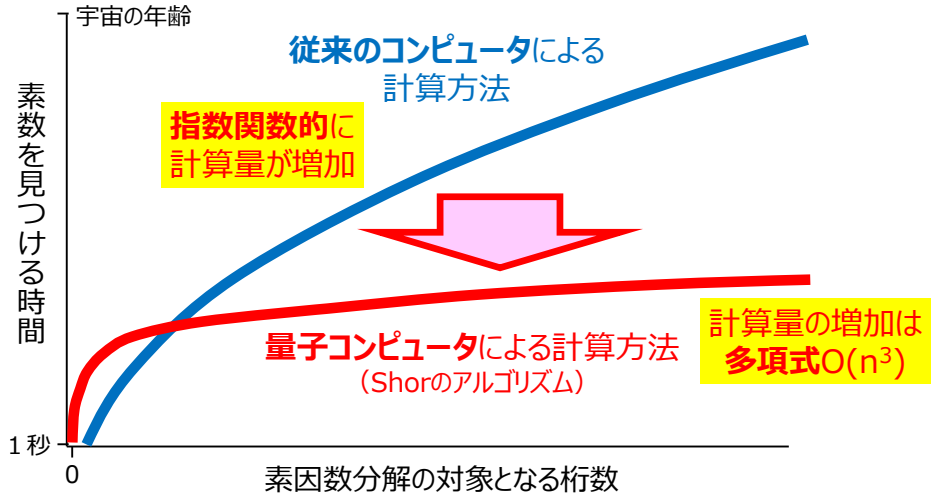
## 量子コンピュータの進展予想
例：民間事業者によるロードマップ

※日本総研公表資料から抜粋




## 実用的な量子コンピュータによる影響
例：RSA暗号の安全性評価

※Quantum Computing (Stolze and Suter)により作成



# 暗号強度要件に関する設定基準におけるPQC等の扱い

➢ **「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」**に※おいて、
※「CRYPTREC暗号リスト」及び「政府機関等の対策基準策定のためのガイドライン」において参照

- 量子コンピュータに必要な性能は、現状は大きく乖離し、**公開鍵暗号の危殆化時期の予測は困難**としている。
- また、PQCは鍵長のサイズが大きくことなる※ため、**移行に当たってアプリケーション等の大幅な変更が必要**になることや、**PQCと現代暗号との併用**も視野に入れることとしている。
※現在使用している暗号は数十～数百バイトだが、PQCではキロバイト単位／暗号方式によっては暗号文のサイズも増加

## 量子コンピュータの影響について

**【重要な注意】**
大規模な量子コンピュータが利用可能になった場合、Shorのアルゴリズムにより多項式時間で素因数分解問題や（楕円）離散対数問題が解けることが知られており、とりわけCRYPTREC暗号リストの公開鍵暗号（守秘、署名、鍵共有）に掲載されている全てのアルゴリズムにとって理論的には大きな脅威になっている。
しかし、2021年3月時点のCRYPTREC調査では、35（＝5×7）の素因数分解が成功しなかったという研究発表などを踏まえ、「現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であると考える。」と結論付けている。このことは、**現時点で実現されている量子コンピュータと実際の暗号解読を行うのに必要とされる量子コンピュータの性能に関しては依然として大きな乖離がある**ことを意味している。加えて、量子コンピュータの性能を測る上での指標（量子ビット数、量子誤りの大きさ、演算可能回数など）や量子コンピュータの開発状況を考慮すると、2022年6月時点において**量子コンピュータによる公開鍵暗号の危殆化時期を予測することは困難**である。

## 量子コンピュータの実現リスクへの対応

現在のCRYPTREC暗号リストに掲載されているアルゴリズムの鍵長と**PQCの鍵長とでは大きくサイズが異なる**ため、**移行にあたってアプリケーションやインタフェース、データフォーマット、プロトコルなどに大幅な変更が必要となる可能性が高い。**その場合、移行のための準備や開発コスト、実際の移行に必要な期間などが従来以上に大きく膨らむ可能性があることに留意されたい。加えて、現在主流の暗号技術とは違い、PQCに特化した暗号解読手法や安全性評価の蓄積、実装脆弱性を回避するためのPQCを実装する際のセキュリティ対策（例えば、サイドチャネル攻撃対策）の蓄積といったものが十分に進んでいるとはいえない状況である点も考慮しておく必要がある。
したがって、**PQCへの移行については、ガイドライン等を参考に、移行の必要性や方法などについても予め十分に検討し、移行計画を慎重に策定したうえで実施すべき**である。利用環境によっては、**PQCへの完全な移行ではなく、PQCと現在主流の暗号技術との併用を視野に入れることも考えられる。**

# 量子コンピュータによる暗号技術の安全性への影響

- 2020年に量子コンピュータによる「量子超越」を実現したとの発表があり、現代暗号が危殆化することが懸念。
- CRYPTREC 暗号技術評価委員会から、**暗号解読には量子コンピュータの規模の拡大だけでなく量子誤り訂正などの実現が必要**であり、**暗号技術が近い将来に危殆化する可能性は低い**との考えを発表している。
  「現在の量子コンピュータによる暗号技術の安全性への影響（2020年2月17日）」

CRYPTREC ER-0001-2019

現在の量子コンピュータによる暗号技術の安全性への影響

2020年(令和2年)2月17日
CRYPTREC 暗号技術評価委員会

今般、ゲート型の量子コンピュータが量子超越を実現したと主張する論文がNature誌に発表されました。この論文では、ランダム量子回路からのサンプリング問題を、古典計算機を用いた場合には1万年かかるところ、量子コンピュータを用いると200秒で完了すると主張しています。この主張は、ランダム量子回路からのサンプリング問題を、量子コンピュータが古典計算機よりも高速に解くことを示しています。これにより、現在広く使用されている公開鍵暗号であるRSA暗号及び楕円曲線暗号などの安全性が大きく低下することが一部で懸念されています。その理由としては、それらの暗号技術が安全性の根拠として利用している素因数分解問題と離散対数問題が、大規模な量子コンピュータとShorのアルゴリズムを使用することで高速に解読されることが知られているためです。

現在、CRYPTREC暗号リストの電子政府推奨暗号リストに記載されているRSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEPは素因数分解問題を、DSA、ECDSA、DH、ECDHなどは離散対数問題を安全性の根拠にしています。CRYPTRECでは、以前よりRSA合成数の素因数分解などにおける安全なパラメータサイズについて、通常の計算機だけでなく、量子コンピュータによる影響に関しても評価を行っておりますが、今までの評価結果をふまえると、CRYPTRECとしては、近い将来にCRYPTREC暗号リスト記載の暗号技術が危殆化する可能性は低いと考えています。

論文で使用されている**量子コンピュータは53量子ビットであり、計算は合計1543回のゲート演算**で構成されています。このとき、1回当たりの計算時間は、1マイクロ秒程度であると見積もられています。なお、ターゲットとする問題の性質上、量子誤り訂正は組み込まれていません。

その一方で、例えば、量子コンピュータを用いて**2048ビットRSA合成数の素因数分解を行う場合には、量子誤りが一切ないという理想的な環境下でも、4098量子ビットが必要であり、$10^{12}$～$10^{13}$回のゲート演算が必要**であると見積もられています。また、量子誤りがあるという現実的な環境下では、2000万量子ビットが必要であるという見積もりもあります。

このため、実現されている量子コンピュータと素因数分解を行うのに必要とされる量子コンピュータの性能に関しては、依然として大きな乖離があります。これは離散対数問題を利用する暗号についても同様です。**量子コンピュータの性能を測る上での指標（量子ビット数、量子誤りの大きさ、演算可能回数など）や、量子コンピュータの開発状況もあわせて考慮にいれると、近い将来に、2048ビットの素因数分解や256ビットの楕円曲線上の離散対数問題が解かれる可能性は低い**と考えます。

しかしながら、**革新的な技術の発展**などにより、量子コンピュータで暗号解読を実現する**可能性は否定できません**。このため、CRYPTRECでは、量子コンピュータによる暗号技術に対する影響、及び量子コンピュータ実現後にも安全な暗号技術（耐量子計算機暗号）に関する監視評価活動を継続していきます。

# 耐量子計算機暗号ガイドライン（2024年度版）

- CRYPTRECにおいて、量子コンピュータの実用化により一部の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「**耐量子計算機暗号ガイドライン（2024年度版）**」を作成。
- ガイドラインは一般的な読者・暗号初学者を対象としており、**PQCに関する技術的事項や活用方法**のほか、**PQCを取り巻く現状等**についてもとりまとめている。

## 量子コンピュータの開発状況

✓ **現在の量子コンピュータはNISQ**（Noisy Intermediate-Scale Quantum）で**実行時のノイズが大きい**が、暗号解読には、**ノイズ等の影響を低減し大規模・長時間の計算を可能としたFTQC**（Fault-Tolerant Quantum Computation）**が必要**と考えられている。
※量子回路型計算において数年前までは誤り訂正処理を行うことで逆にノイズが蓄積しエラーレートが悪化する状態だったものが、誤り訂正後のエラーレートが下回るという結果が報告されており、FTQCに向けた論理量子ビットの構築が進んでいる。（日本のムーンショット目標6では、2050年までのFTQC実現を目指している。）

✓ **量子ビット数の増加のみではなく**、ゲート操作の忠実度の向上、コヒーレント時間の向上などの課題を克服し、量子誤り訂正、量子ランダムアクセスメモリ等の2025年**現在では完全には実用化されていない技術を用いる必要**。
→それらの開発スピードの予測困難性が、**量子コンピュータが暗号に与える影響の将来予測を困難**なものとしている。

## 現代暗号の危殆化予測

✓ 量子コンピュータによる**RSA-2048の危殆化時期に関して、様々な予測**が存在。**今後数十年で暗号解読を可能**とする規模の量子計算を実行可能な**量子コンピュータが開発されうる**。
※定量的な予測では、「2039年以降」や「2050年前後」と少なくとも20年程度は実現に時間がかかるとされている。多くの専門家へのアンケートを集計した結果(Global Risk InstituteによるQuantum Threat Timeline)では、解読可能な量子コンピュータが15年以内に出現する可能性が33%～54%程度であると分析。

✓ 暗号方式の提案から社会的な普及までは**RSA暗号・楕円曲線暗号で20年ほどの期間が必要**とされたことから、PQCの場合でも同程度の期間が必要と想定されるため、**長期間の移行スケジュールを策定し、準備を行う必要**。
※RSA-2048については、古典コンピュータの性能の伸びにより長期的には危殆化すると考えられており、移行準備は量子コンピュータに関わらず進めていく必要。

## 量子コンピュータによる素因数分解・離散対数問題計算の現状

✓ 量子回路型コンピュータ実機を用いた実験は、**「15」・「21」・「35」の素因数分解、「$2^z \equiv 1 \pmod 3$」の離散対数計算**のみ。
※量子アニーリングでは23ビット（8219999=32749×251）の実験が2023年に行われている。
※実験では入力インスタンスに合わせ簡略化した量子回路を使っているが、暗号解読には汎用の剰余加算・乗算回路と最低でも数万ゲートの操作が必要。

✓ **Shorのアルゴリズムが量子ノイズに弱い**事の理論的な証明が与えられており、**量子ノイズの影響を下げる必要**。

# 耐量子計算機暗号ガイドライン（2024年度版）＜続き＞

## 米国NIST（米国国立標準技術研究所）による標準化動向

- ✓2016年12月に**Call for Proposals**が正式公開され、2017年11月の公募締切までに82方式が提案され、公募条件を満たした**69方式が第１ラウンド候補**として公開（5方式は公開後に取り下げ）。
- ✓2019年1月に、**第2ラウンドへ進む26方式**が発表。
- ✓2020年7月に、**第3ラウンドへ進む15方式**（Finalistsの7方式とAlternate Candidatesの8方式）が発表。
- ✓2022年7月に、**標準化方式として4方式**が発表。
- ✓2024年8月に、**3方式が標準化**(FIPS 203～205)し、今後**１方式が標準化予定**(FIPS 206)。

| | | | |
|---|---|---|---|
| **・FIPS 203(ML-KEM)** | (改称前 CRYSTALS-Kyber) | 格子暗号ベース | 暗号化・鍵交換用途 |
| **・FIPS 204(ML-DSA)** | (改称前 CRYSTALS-Dilithium) | 格子暗号ベース | 署名用途 |
| **・FIPS 205(SLH-DSA)** | (改称前 SPHINCS+) | ハッシュ関数ベース | 署名用途 |
| **・FIPS 206(FN-DSA)** | (改称前 FALCON) | 格子暗号ベース | 署名用途 |

※FIPS(Federal Information Processing Standards)：米国連邦政府が採用する情報処理に関する公式な標準規格で、NISTが策定。

- ✓2022年７月の際、第3ラウンド候補から**第4ラウンドへ進む4方式**(暗号化・鍵共有用途)が発表（1方式はその後取り下げ）。
  ※BIKE、Classic McEliece、HQC、SIKE(取り下げ)／いずれも格子暗号ベース以外の方式による暗号
- ✓第4ラウンド発表と並行して、2022年9月から正式に**追加（Additional Digital Signature Schemes）の募集**を開始。締切の2023年6月までに50方式の応募があり、翌7月に公募条件を満たした**40方式が発表**。
- ✓2024年10月に、**追加募集第2ラウンドの候補となる14方式**が発表。
  ※ CROSS、FAEST、HAWK、LESS、MAYO、Mirath (merger of MIRA/MiRitH)、MQOM、PERK、QR-UOV、RYDE、SDitH、SNOVA、SQIsign、UOV

## 米国以外での動向

- ✓多くの国が、NIST PQCの標準化方式を用いるが、FrodoKEMのようにNIST PQC標準化プロジェクトの選考に漏れた方式や、Classic McElieceのように第4ラウンド選考中の状態で選ばれた例も存在。
- ✓多くの機関が、NIST標準方式の**単独利用ではなく**、古典的安全性がよく知られている**RSAやECDSAとのハイブリッドを推奨**。

# 量子コンピュータの共通鍵暗号等の安全性

- **共通鍵暗号**や**ハッシュ関数**については、公開鍵暗号のように量子コンピュータを用いた効率的なアルゴリズム（Shorアルゴリズムにより多項式時間での計算）は見つかっていないが、Groverアルゴリズム及びBHTアルゴリズムにより、**計算において一定の効率化は可能**。
- 現在128ビット相当が主に用いられているが、共通鍵暗号は192ビット・256ビットに、ハッシュ関数の出力長は384ビット・512ビットなど、**高い強度のものへの変更検討が必要**。

※「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）」より

## 量子コンピュータの共通鍵暗号に関する安全性

CRYPTRECの電子政府推奨暗号リストにあるハッシュ関数以外の共通鍵暗号技術に量子コンピュータが与える影響は**Groverのアルゴリズムを用いるとkビット鍵の全数探索が時間$O(2^{k/2})$で実行**できるため、長期的に保護したいデータには鍵長が**192ビットや256ビットの暗号技術を使用した方が賢明**であるという以上のものは現状では無いと考えられる。しかし、安全性へ現実的な影響を直接及ぼしうる攻撃が今後発見される可能性もあるため、研究の動向には今後も注意を払っておく必要がある.

## 量子コンピュータのハッシュ関数に関する安全性

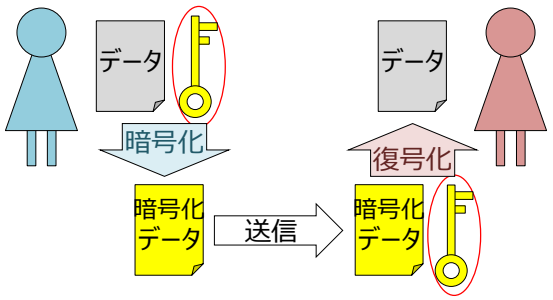
汎用的な攻撃のうち主に考慮に入れるべきものは、（量子計算の有無に関わらず）原像探索と衝突探索である。原像探索については、Groverのアルゴリズムを用いればnビット出力ハッシュ関数の原像を発見するのに要する時間が古典の$O(2^n)$から$O(2^{n/2})$にまで高速化される。また衝突探索については、**BHTのアルゴリズムを用いれば衝突を発見するのに要する時間が古典の$O(2^{n/2})$から量子の$O(2^{n/3})$まで高速化**される。

BHTのアルゴリズムは非常に大きな量子メモリを必要とし、古典衝突探索アルゴリズムや他の単純な衝突探索アルゴリズムと比べて真に効率的か否かについては様々な議論がある。しかし、SHA-256やSHA-512、SHA3-256を含むハッシュ関数の攻撃可能段数が古典より伸びることがここ数年で判明していることも考慮すると、重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）はBHTのアルゴリズムの計算量を基準にして**384ビットや512ビットのものを用いた方が無難**であると考えられる。

# （参考）量子コンピュータ時代の暗号関係技術

## 共通鍵暗号

**同一の暗号鍵**を事前に双方で共有

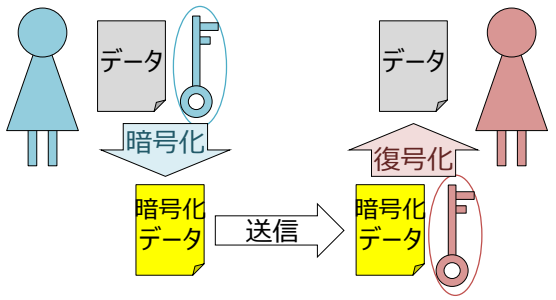



N人が通信する際、**N(N-1)/2個の鍵**が必要

ネット利用の進展に伴い鍵の共有が煩雑化

## 公開鍵暗号

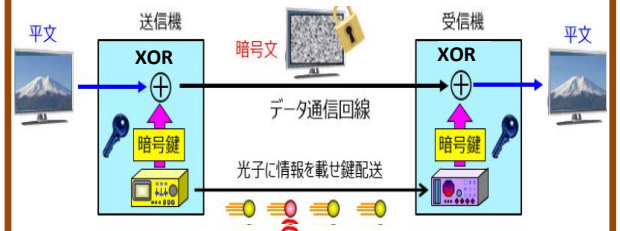
**公開鍵**を公開し、**秘密鍵**は自身で保有




N人が通信する際、**N組の鍵**で足りる

鍵の共有(運搬)がセキュリティリスクになりうる

量子力学の原理（物理法則）に基づき、盗聴が不可能な方法により鍵共有が可能




**量子鍵配送(量子暗号)**
**Q**uantum **K**ey **D**istribution

## <公開鍵暗号の代表例：RSA暗号>

<イメージ>

素因数分解

$$n = \underbrace{p \times q}_{\text{秘密鍵}}$$

合成数　素数　素数

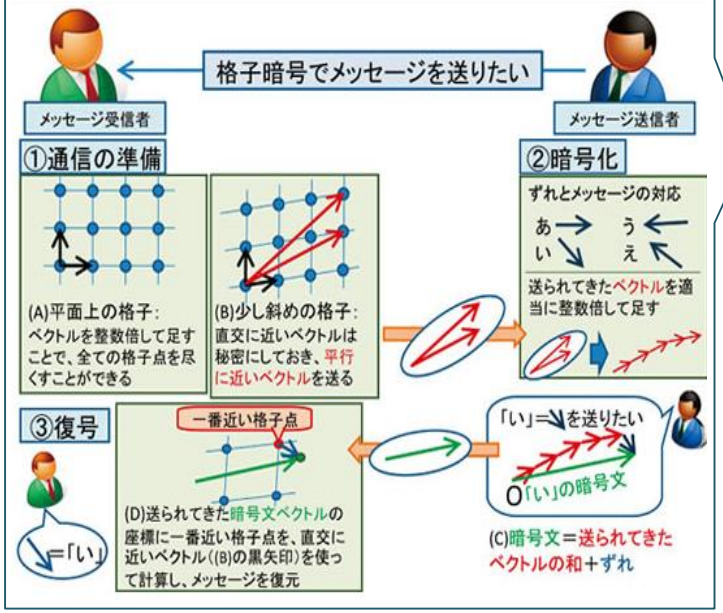
公開鍵

例：公開鍵＝23449／秘密鍵＝131、179
（実際には数百桁程度の数を使用）

**古典コンピュータ**　解読は実質不能
スーパーコンピュータでも解析困難な計算量

**量子コンピュータ**　解読の可能性
量子コンピュータを使うことで計算時間を減らす方法が発見

## <格子に基づく耐量子計算機暗号の例>




## 量子コンピュータに耐えうる暗号の必要性

量子コンピュータでも効率的な計算方法が発見されていない数学的計算問題を活用した暗号方式が各種提案

- ✓格子に基づく暗号技術
  （CRYSTALS-KYBER、FrodoKEM、LAC、NewHope、NTRU、NTRU Prime、Round5、SABER等）
- ✓符号に基づく暗号技術
  （BIKE、Classic McEliece、HQC、LEDAcrypt、NTS-KEM、ROLLO、RQC等）
- ✓その他
  （SIKE、Three Bears等）

**耐量子計算機暗号**
**P**ost-**Q**uantum **C**ryptography