革新的情報通信技術（Beyond 5G（6G））基金事業
電波有効利用研究開発プログラム
研究計画書

課題 096
移動体通信システムに実装する耐量子計算機暗号技術等に関する研究開発

2025年９月

国立研究開発法人
情報通信研究機構

１．研究開発課題

『移動体通信システムに実装する耐量子計算機暗号技術等に関する研究開発』

２．目的

「情報通信審議会最終答申　Beyond 5G に向けた情報通信技術戦略の在り方（令和６年６月 18 日）」において、「サイバー攻撃が巧妙化・多様化し、サイバーセキュリティ上の脅威が増大するとともに、2030 年代に向けて大規模量子コンピュータの実用化による現行暗号の危殆化リスクが高まる中、Beyond 5G において、耐量子計算機安全性等のより高度なセキュリティを確保することが重要となる。」とされているところ、Beyond5G における耐量子計算機安全性を確保することは急務となっている。また、「AI 社会を支える次世代情報通信基盤の実現に向けた戦略 -Beyond 5G 推進戦略 2.0-　具体的な戦略（令和６年８月 30 日）」では、「戦略分野として、周波数の国際的な開発・利用の動向等も踏まえつつ、今後のトラヒック需要の拡大に対応するための更なる周波数の確保や、AI を活用した RAN 制御による周波数利用効率の向上といった RAN の高度化等に向けて総合的な取組を推進することとする。」とされており、Beyond5G において、今後のトラヒック需要の拡大に対応するために周波数を確保することも重要である。以上を踏まえつつ、「ICT サイバーセキュリティ政策の中期重点方針（2024 年７月）」においては、「量子コンピュータの計算機能力向上に伴う現代暗号の危殆化リスクに対しては、各分野において適切にリスクを把握した上で、暗号移行には一定の期間を要することも考慮に入れつつ、耐量子計算機暗号（PQC：Post-Quantum Cryptography）等への移行に向けて必要な対応を進めることが重要である。これらの取組とあわせて、PQC 等への円滑な移行に向けて、PQC や鍵長を伸長した共通鍵暗号の性能向上技術やクリプト・アジリティ技術等の研究開発を推進することが求められる。」とされているところである。本課題は、大規模量子コンピュータの実用化による現代暗号の危殆化リスクの高まりに対し、効率的な次世代暗号技術や暗号移行支援技術等に関する研究開発を実施することで、耐量子計算機安全性を有した高度なセキュリティを確保した技術を社会実装するとともに、暗号データサイズ等の縮小による電波の有効利用に資することを目的とするものである。

現在広く実装されている従来型公開鍵暗号としては、RSA 暗号や楕円曲線暗号が挙げられる。RSA 暗号と楕円曲線暗号を安心して利用するためには、整数の素因数分解問題や楕円曲線上の離散対数問題が計算量的に困難である必要がある。これらの問題は現在普及しているコンピュータ（古典コンピュータ）では効率的に解くことはできないと考えられている。ただし、量子コンピュータの開発が十分に進むと Shor のアルゴリズムにより素因数分解や離散対数を高速に計算できるため，RSA 暗号と楕円曲線暗号の安全性は大きく低下する。近年、量子コンピュータの大規模化が急速に進展している。このため、大規模な古典コンピュータと量子コンピュータの双方を用いた攻撃に対しても安全性を確保でき、かつ古典コンピュータ上で効率的な実装が可能な公開鍵暗号方式として、PQC が必要とされている。また、現時点から暗号化された情報を収集しておき、将来的に大規模化した量子コンピュータを用いて高機密情報を解読する HNDL（Harvest Now, Decrypt Later）攻撃も指摘されており、可能な限り早期に PQC に移行させることが望ましい。

他方、現在提案されている PQC は、従来型公開鍵暗号に比べて鍵や暗号文サイズ等が大きい。例えば、128 ビット鍵の共通鍵暗号と同等の安全性を有する RSA 暗号の公開鍵・秘密鍵・暗号文サ

イズは、共に 384 バイトである。楕円曲線暗号の公開鍵・秘密鍵サイズは 32 バイト、暗号文サイズは 64 バイトである。一方で、米国で標準化された ML-KEM に関しては、公開鍵・秘密鍵・暗号文サイズはそれぞれ 800 バイト、1,632 バイト、768 バイトであり、RSA 暗号と比較し 2～4 倍、楕円曲線暗号と比較し 10 倍以上大きい。また、米国標準の第 4 ラウンドの候補である Classic McEliece に関しては、暗号文サイズは 96 バイトと小さいものの、秘密鍵サイズは 6,429 バイト、公開鍵サイズは 261,120 バイトと、ML-KEM と比べても更に大きい。処理速度に関しては、従来型公開鍵暗号と比べて速い PQC 方式と遅い PQC 方式がある。遅い PQC 方式を採用する場合は、利用者の待ち時間が増大し、利便性が低下する可能性がある。サーバなどにより同時に複数の TLS セッションを構築する必要がある場合や、省リソース環境では特に注意が必要となる。また依然として脆弱性の発見も続いている。例えば、米国標準の第 4 ラウンドの候補である SIKE に関しては、公開鍵サイズや暗号文サイズが小さいことから注目されていたものの、多項式時間で実行可能な攻撃手法が発見された。さらに、計算リソースが限定的な通信システム等においては、暗号処理により生じる遅延時間が通信速度のボトルネックとならないように、暗号処理の組み込み評価を実施することが重要である。

これらの課題の解決を前提として、PQC への移行を円滑かつ効率的に実現しなければならない。こうした状況を踏まえ、本施策では、次世代の移動体通信システムの特徴を十分に加味した上で、PQC 及び共通鍵暗号の高効率化・高機能化・安全性強化等のための技術を開発する。また、従来型公開鍵暗号から PQC への円滑かつ効率的な移行（クリプト・アジリティ）を実現するため、移行が必要な暗号を検出するための暗号インベントリ技術及び国産暗号実装技術を活用した次世代暗号モジュールを開発するとともに、ユースケースごとの最適化等のための技術を開発する。研究開発成果を活用し、量子コンピュータに対する安全性を確保するとともに、データ伝送のスループットの向上や伝送時間の短縮を実現し、通信サービス等においても周波数利用効率化を図る。なお、PQC の移行段階における異なる暗号方式間の相互接続性を必要に応じて確保するため、国際的な標準化活動への参画等も重要である。

本課題は、「革新的情報通信技術（Beyond 5G（6G））基金事業 基金運用方針」（令和６年７月４日改定・公表 総務省）における「３．本基金による事業内容」の「③電波有効利用研究開発プログラム」（p.６）として実施する。

３．内容

本委託研究では、以下の２つの研究開発項目に対し、研究開発を推進するものとする。

・研究開発項目１　量子コンピュータに対する安全性を確保した共通鍵暗号の移動体通信プロトコル等への導入に関する研究開発

量子コンピュータにより、共通鍵暗号の鍵の全数探索に必要な計算量が削減される。従来と同等の安全性を確保する場合、共通鍵暗号の鍵長を、移動体通信システムで主に実装されている 128 ビットから 256 ビットに伸長する必要があるが、それによって速度低下が生じる。その一方で、Beyond5G の通信速度は 100 Gbps 超に到達するとされている。モバイル通信システムでは、仮想化の進展、実装コスト削減、デバイスの汎用化等のため、専用ハードウェアに代わってソフトウ

ェアによる実装範囲が拡大しており、可能な限り汎用的な計算環境で実行できることが望ましい。256 ビットの鍵長を有することで量子コンピュータに対する安全性を有し Beyond5G の性能に対応可能な処理速度を両立する次世代の共通鍵暗号の実現が求められており、Rocca-S、HiAE などの Beyond5G 向けの新たな暗号方式が提案されている。そこで、以下を実施することで、これらの新たな共通鍵暗号の安全性を検証するとともに Beyond5G への導入における課題を明確化し、さらに課題を解決するプロトコル仕様、効率的な実装手法等を開発する。また、開発した技術の国際標準化を推進し、次世代の移動体通信規格等への導入やその他の通信サービスへの導入により、データ伝送の効率化及び安全性の確立を図る。

a）新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証

現在、Beyond5G 向けの高速な暗号方式が提案されている。これらの中には、暗号化とメッセージ認証コードの生成を一体化された処理として効率的に実行するよう設計された認証暗号も含まれる。一方で、移動体通信システムにおいては、共通鍵暗号が加入者認証、無線区間の通信における機密性・完全性の確保、派生鍵の導出、匿名 ID の生成など様々な機能に使用される。3GPP の現行技術仕様においては、機密性のための暗号化処理と完全性のためのメッセージ認証コードの生成処理は別個の処理として定義されている。そのため、認証暗号をそのまま導入すると処理が重複し、十分な性能を発揮できない可能性がある。また、現行仕様では複数の暗号方式を組み合わせて各機能を実現している。Beyond5G の超高速・大容量通信に対応した暗号方式を追加する場合は、実装・検証コストの増加も懸念される。単一の暗号方式で複数の機能を実現することにより、導入コストの削減も期待できる。

そこで本研究開発項目では、移動体通信システムにおいて、単一の暗号方式により加入者認証、無線区間の通信における機密性・完全性の確保、派生鍵の導出、匿名 ID の生成など様々な機能を実現するため、量子コンピュータに対する安全性を備えた共通鍵暗号の利用モードを設計する。設計した利用モードは、移動体通信システムの各種機能に適用し、複数の端末や通信環境を用いた比較評価を実施する。これにより、Beyond5G において導入すべき暗号方式を明らかにするとともに、移動体通信システムの各種機能要件を満たす適切な利用モードを選定し、暗号方式の円滑な移行に資する利用モードも開発する。また、候補となる暗号方式や新たに設計した利用モードを対象に、従来の攻撃手法に対する安全性評価に加え、Grover の量子アルゴリズム等による一般的な鍵の総当たり攻撃及び暗号方式に特化した量子アルゴリズムを含む最新の攻撃手法の適用の可否を検証する。さらに、新たなセキュリティ要件に対する安全性評価を行い、その評価結果に応じて安全性を強化するための手法を検討する。以上によって得られた最適な暗号方式並びに利用モードを研究開発項目 1-b）に入力する。

b）移動体通信規格への組み込み手法の検証

次世代の新たな移動体通信規格やその他の通信サービスへの導入を推進するため、主要なプロトコルへの組み込み評価を実施する。また、プロトコルの改良及び実装の最適化により、暗号処理により生じる通信速度のボトルネックを解消し伝送時間を短縮することで、周波数利用の効率化を図る。

現行の 5G 等の移動体通信の標準規格においては、データ暗号化とメッセージ認証に異なる方式が用いられており、データ全体を暗号化した後、暗号化したデータ全体に対してメッセージ認証コードの生成が行われる。加えて、メッセージ認証コードが 32 ビットと短く、データの改ざんに対して十分な安全性を確保することも課題となる。そこで、これらの課題を解決するための次世代の移動体通信の標準規格を想定したプロトコルを設計し実装するとともに、現行のプロトコルに対して安全性、実装性、運用性の観点から比較評価を行う。また、Beyond5G の移動体通信システムにおける暗号関連プロトコルを模擬した評価環境にて、100Gbps 以上の暗号処理（暗号化及びメッセージ認証コード作成）を達成する。さらに、5G 等の移動体通信規格との後方互換性の検証を行う。加えて、3GPP、ISO/IEC、IETF 等の国際標準化団体の会合に参加し、最新の標準化動向を調査するとともに、検討した結果を標準化会合で入力し、国際標準化を推進する。

・研究開発項目２　PQC の高効率化・高機能化・安全性強化及び移行支援技術の研究開発

PQC は従来型公開鍵暗号方式に比べてデータサイズが大きい方式や処理時間が長い方式が存在するため、通信帯域の圧迫やサービスの遅延などのユーザビリティの低下が課題となる場合がある。そこで、以下を実施することで、PQC の高効率化を図り、暗号移行に起因するデータサイズや処理時間の緩和を図るとともに、PQC の安全性を強化するための技術の研究開発を実施する。また様々なユースケースにおける高効率・高機能 PQC 等の導入のため、研究開発項目１で開発する共通鍵暗号を含む次世代暗号モジュールを開発し、ユースケースに合わせた最適化手法を研究開発する。これらにより、研究開発項目１で開発した共通鍵暗号及び PQC の円滑な導入による安全性向上をもたらすとともに、最適なパラメータ設定による効率化を実現する。さらには、国産の暗号実装技術の競争力を強化し、様々なユースケースにおいてその普及を図る。加えて、従来型公開鍵暗号から PQC 及び従来型共通鍵暗号から次世代共通鍵暗号への円滑かつ効率的な移行を実現するための暗号インベントリ技術を開発する。

a）PQC の高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発

従来型公開鍵暗号から PQC に移行を行う際に、既存のインフラやシステム等に与える影響を最小化するため、PQC の安全性評価のための技術を開発し、PQC の安全性を向上するとともに、暗号文サイズ、署名サイズ及び鍵サイズの削減並びに処理性能の向上を行う。加えて、ユースケースを踏まえた PQC の高効率化及び高機能化にも取り組み、各ユースケースに最適な PQC を選択するための技術を開発する。

PQC の安全性を向上するため、PQC の安全性評価に関しては、既存 PQC 等に対する最新の攻撃・安全性評価手法の調査を踏まえ、PQC を構成するプリミティブに対する構造解析を実施し、安全性評価手法を確立する。これにより、最良な PQC パラメータ設定を可能にする。また、移動体通信システム等への PQC の安全な実装のため、サイドチャネル攻撃や故障利用攻撃などの実装攻撃に対する安全性評価を実施し、これらの攻撃への対策技術を開発する。

PQC の処理時間又はデータサイズ削減については、PQC におけるデータ構造、計算手順及び実装を改良し、2024 年度時点における PQC のリファレンス実装を基準にして、10%のデータサイズ削減又は処理時間削減を図る。また、想定されるユースケースに適合する PQC の高効率化・高機

能化として多対多通信用 PQC や暗号化状態での情報処理機能等の実現を図り、2024 年度時点の高効率・高機能 PQC のリファレンス実装を基準にして、20%のデータサイズ削減又は処理時間削減を図るとともに、ITU-T、3GPP、ISO/IEC、IETF 等の国際標準化団体の会合に参加し、開発した要素技術の標準化提案を実施して国際標準化を推進する。

上記の成果を活用し、量子コンピュータに対して安全な暗号スイート（PQC 等による鍵共有、エンティティ認証、メッセージ暗号化、メッセージ認証等の暗号方式の組み合わせ）を含む通信システム向けの国産の次世代暗号モジュールを開発する。まず、当該暗号モジュールは、暗号処理により通常生じる通信速度の低下に対し、暗号実装を最適化することにより通信速度の低下を軽減し、電波の有効利用を図る。また、PQC は、方式ごとに鍵・データサイズや処理時間が異なる上に複数のパラメータが存在する。このため、当該暗号モジュールの設計においては、利用者が適切に PQC の方式及びパラメータを選択できるよう考慮する。さらに、従来の暗号モジュールからの次世代暗号モジュールへの移行時や次世代暗号モジュールにおける暗号方式の変更時に生じるシステムへの影響を事前調査し、これらの移行や変更時のテスト等における必要な工数が最小となるよう考慮した設計とする。

b）暗号インベントリ技術の開発

暗号は様々な用途で普及しているところ、これらの全ての暗号について、量子コンピュータに対して安全な暗号に移行するためには、膨大なコストを要する。また、暗号の用途によっては、その利用期間や生成されるデータの保護期間が短いものも存在し、量子コンピュータに対して安全な暗号に移行する優先度が低い場合もある。そこで、暗号移行を行う際には、移行優先度の高いものを洗い出し、その優先度に応じて対応を行うことが適切である。

そこで、研究開発項目 2-a）で開発する次世代暗号モジュールの円滑かつ効率的な導入を実現するため、システムにおいて移行が必要な暗号を検出するための「暗号インベントリ技術」を開発する。「暗号インベントリ技術」は、システムにおいて使われている暗号を検出するとともに、次世代暗号モジュールへの対応可否やその優先度及び次世代暗号モジュールの運用状況（適切なパラメータ設定がなされているか等）を確認するための技術である。

4．アウトプット目標・アウトカム目標

・研究開発項目１　量子コンピュータに対する安全性を確保した共通鍵暗号の移動体通信プロトコル等への導入に関する研究開発

2028 年度末におけるアウトプット目標 （最終目標）

a）新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証

- Beyond5G において導入すべき暗号方式の選定と移動体通信システムの各種機能要件を満たす実装の評価完了。

b）移動体通信規格への組み込み手法の検証

- 移動体通信規格への組み込み・後方互換性の検証完了。
- Beyond5G の移動体通信システムにおける暗号関連プロトコルを模擬した評価環境に

て、100Gbps 以上の暗号処理（暗号化及びメッセージ認証コード生成）を達成。

2025 年度末におけるアウトプット目標

a）新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証

- 候補となる暗号方式に対する最新の攻撃・安全性評価手法の調査完了。

b）移動体通信規格への組み込み手法の検証

- 移動体通信規格における利用実績の調査完了。

2026 年度末におけるアウトプット目標

a）新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証

- 候補となる暗号方式に対する量子アルゴリズム及び新規セキュリティ要件に対する安全性評価完了。

b）移動体通信規格への組み込み手法の検証

- 移動体通信規格への導入方法の設計完了。

2027 年度末におけるアウトプット目標

a）新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証

- 移動体通信システムの各種機能要件を満たす実装手法の設計完了。

b）移動体通信規格への組み込み手法の検証

- 移動体通信規格の後方互換性確保手法設計完了。

アウトカム目標

2025～2026 年　3GPP、ISO/IEC、IETF 等の標準化団体における仲間づくりを完了
2026～2028 年　3GPP 等の標準化団体において、次世代の移動体通信規格等における性能要件に合意
2027～2029 年　国産暗号技術の導入に関する標準化提案を実施
2028～2030 年　国際標準への採用決定
2030～2035 年　既存方式からの置き換えが進み、国際標準において必須技術となる
2035 年～　国際標準における必須技術として全世界に普及

・研究開発項目２　PQC の高効率化・高機能化・安全性強化及び移行支援技術の研究開発

2028 年度末におけるアウトプット目標　（最終目標）

a）PQC の高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発

- 2024 年度時点の PQC に対して、パラメータの脆弱性又は十分性の究明を完了。
- 2024 年度時点の PQC のリファレンス実装を基準にして、10%のデータサイズ削減又

は処理時間削減。
- 2024 年度時点の高効率 PQC のリファレンス実装を基準にして、20%のデータサイズ削減又は処理時間削減。
- ユースケースを考慮した試験環境における統合評価の完了。
- 次世代暗号モジュールの検証・改良の完了。

b）暗号インベントリ技術の開発
- 通信システムを考慮した試験環境での暗号インベントリ技術の検証完了。

2025 年度末におけるアウトプット目標

a）PQC の高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発
- 既存 PQC 等に対する最新の攻撃・安全性評価手法の調査完了。
- 高効率・高機能 PQC 等に対する基本設計の完了。
- 主要なライブラリ・通信プロトコル等における PQC 等の実装状況の調査完了。
- 通信システムにおける暗号活用状況の調査の完了。

b）暗号インベントリ技術の開発
- 暗号インベントリ技術に関する研究動向の調査完了。

2026 年度末におけるアウトプット目標

a）PQC の高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発
- 高効率・高機能 PQC 等の方式・パラメータ設計完了。
- 高効率・高機能 PQC 等の性能評価指針の設計完了。
- PQC に対する実装攻撃に関する安全性評価の完了。
- 通信システムを想定した試験環境の設計。
- 次世代暗号モジュールの基本設計、PQC 等の選択方式・パラメータの選定完了。

b）暗号インベントリ技術の開発
- 暗号インベントリ技術の設計完了。

2027 年度末におけるアウトプット目標

a）PQC の高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発
- 高効率・高機能 PQC 等の性能評価完了。
- 高効率・高機能 PQC 等の方式・パラメータ改良完了。
- PQC に対する実装攻撃への対策技術の設計完了。
- 次世代暗号モジュールの開発完了。
- 主要なライブラリ・通信プロトコル等やユースケースを考慮した最適化設計完了。

b）暗号インベントリ技術の開発

- 暗号インベントリ技術の評価・改良完了。

アウトカム目標

2033 年　通信事業者、サービス提供者及びシステム運用者等が、システムにおいて、PQC 移行の対応が必要な暗号をリストアップするツールとして活用し、PQC の普及を促進。（オープンソース化も想定。）

2035 年～　想定したユースケースにおいて、暗号モジュールとして活用し国産暗号実装技術を商用化。（本プロジェクトの成果は、通信サービス・製品へのライブラリとしての提供を想定。）

5. 採択件数、研究開発期間及び研究開発予算等

採択件数　：１件

研究開発期間：契約締結日から 2028 年度（2026 年度後半に実施するステージゲート評価を踏まえ、継続の必要性等が認められた場合には、最長で 2028 年度まで継続予定。認められなかった場合当該年度末で終了。）

研究開発予算：研究開発項目 1 及び研究開発項目２を合わせて総額で 2,000 百万円（税込）を上限とし、最初の２年間での累計額上限を 1,000 百万円（税込）とする。（提案の予算額の調整を行った上で採択する提案を決定する場合がある。ステージゲート評価や革新的情報通信技術（Beyond 5G（6G））基金事業の後年度予算の状況等により、各年度の研究開発予算を変更する場合がある。）。

研究開発体制：単独の提案も可能であるが、産学官連携等による複数の実施主体からなる体制とすることを推奨する。その際、社会実装を考慮した体制とすること。

6. 提案に当たっての留意点

- 研究開発項目１、研究開発項目２の研究開発項目を一つの提案書にまとめて提案すること。
- 提案書には、ステージゲート評価後 2028 年度まで実施することを仮定して、2028 年度までの計画を記載すること。
- 具体的目標に関しては、2026 年度後半のステージゲート評価を受ける際の中間目標と、当該評価で継続が認められた場合の各年度の目標について、定量的に提案書に記載すること。
- 本委託研究で研究開発する技術について、具体的に Beyond 5G の実現に当たりいつ頃どのような分野のどのような知的財産の取得が期待できるのか、何件程度の特許出願を目指すのか、また、知的財産の取得とともに標準化活動の推進も重要であることから、いつ頃どのような分野のどのような標準の策定が期待できるのか、どのような標準化活動を推進するのか等について提案書に記載すること。
- 外国の民間企業や大学等との連携体制が構築できている又は計画している場合には、具

体的な連携の方法について提案書に記載すること。

- 実施体制については、本研究開発の目的に則した実施体制を構築することとし、それぞれの役割を明記すること。
- 研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言をいただくとともに、実際の研究開発の進め方について適宜指導をいただくため、国立研究開発法人情報通信研究機構（以下「機構」という。）の研究者、学識経験者、有識者等を含んだ研究開発運営委員会等を開催すること。
- 本研究開発成果の社会実装に向けて、到達目標の項目に記載されたマイルストーンを意識しつつ、具体的な時期（目標）、体制、評価方策等を記載すること。その際、本研究開発が対象としているシステムのデモンストレーションや、それら成果を用いたより高度な研究開発活動あるいは通信事業が、持続的に発展するためのライフサイクル計画等についても記載すること。
- 研究開発成果の情報発信を積極的に行うこと。

7. 運営管理

- 複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の運営管理を行い、受託者間調整会議を定期的に開催すること。
- 機構と受託者の連携を図るため、代表提案者は、機構の指示に基づき研究開発の進捗状況などについて報告すること。また、我が国の PQC に関する研究を俯瞰しての取組となるよう、可能な場合には機構との間で共同研究その他の連携をすること。なお、PQC の移行段階における異なる暗号方式間の相互接続性を必要に応じて確保するための国際的な標準化への参画等の際には、我が国での PQC に関する研究の状況を踏まえたうえで、総務省の政策に沿う取組とするため、機構における関連研究と連携を図ることか望ましい。
- 社会情勢や研究環境の変化等、必要に応じて、機構が研究計画書を変更する場合があるので、留意すること。

8. 評価

- 2026 年度後半に評価委員会による評価（ステージゲート評価）を実施し、継続の必要性等が認められた場合には、最長で 2028 年度まで研究開発を継続する。なお、ステージゲート評価の結果を踏まえ、委託研究の中止、縮小、実施体制の変更等を判断する場合がある。
- 機構は、研究開発終了時に終了評価を実施する。
- 機構は、本委託研究終了後に成果展開等状況調査を行い、追跡評価を行う場合がある。
- 機構は、上記以外にも本委託研究の進捗状況等を踏まえて、臨時にヒアリングを実施することがある。

9. 成果の社会実装等に向けた取組

- Beyond 5G の実現を支える技術として、知的財産戦略及び標準化戦略、さらには社会実装

と海外市場への展開戦略を記載すること。

- 社会実装・海外展開に向けた事業計画を明確とすること（委託研究後の事業化等に向けた取組を明確にする）。
- 上記の社会実装・海外展開を実現するため、提案に先立ち、事業計画を練り、その実現に向けた研究開発提案を検討すること。また、必要に応じて、成果発表やそれに留まらずコミュニティ先導のための国際ワークショップや国内セッション開催、展示、標準化等を行うこと。