令和７年度事後事業評価書

政策所管部局課室名：サイバーセキュリティ統括官室

評価年月：令和７年８月

１　政策（研究開発名称）

安全な無線通信サービスのための新世代暗号技術に関する研究開発

２　研究開発の概要等

（１）研究開発の概要

・実施期間

令和３年度～令和６年度（４か年）

・実施主体

民間企業、大学、国立研究開発法人

・総事業費

1,647 百万円

令和３年度	令和４年度	令和５年度	令和６年度	総　額
409 百万円	406 百万円	441 百万円	390 百万円	1,647 百万円

事業開始時点で、十億円以上の費用を要することが見込まれていなかったため、事前評価は実施していない。

・概　要

5G 等の無線通信の高度化においては、将来的に実用化が想定される大規模量子コンピュータに対応する必要がある。大規模量子コンピュータへの対策としては、共通鍵暗号方式[1]においては、鍵長の増加、公開鍵暗号方式[2]においては、耐量子計算機暗号（以下「PQC[3]」という。）への移行が挙げられる。一方、それらの技術を適用する際には、5G 等が求める超高速・大容量等の通信特性を損なわず、計算資源や通信リソースにも影響を与えないよう配慮する必要がある。

本研究開発では、5G 等の特性を損なわない形で、現状と同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応した共通鍵暗号方式を開発し、一般的な計算機環境において処理速度を 50Gbps にするとともに、暗号処理に要する時間を従来方式と比較して最大 50%程度削減することを目指す。また、5G 等の様々なユースケースに合わせた PQC への機能付加技術等を確立し、オーバーヘッド（暗号文サイズ、処理時間等）を最大８％以内に抑え、無線リソースのひっ迫を抑止することで電波の有効利用を図る。さらに、これらの実用化に向けて暗号アルゴリズムや PQC 活用ガイドラインの国際標準化に取り組む。

---

[1] 暗号化・復号の過程で、同じ鍵が用いられる暗号方式。

[2] 一対の異なる暗号鍵ペア（本人しか所有しない「秘密鍵」と一般に誰でも入手可能な「公開鍵」）が用いられており、一方の鍵で暗号化したものについては、それに対応するもう一方の鍵でしか復号できない暗号方式。

[3] Post-Quantum Cryptography の略。

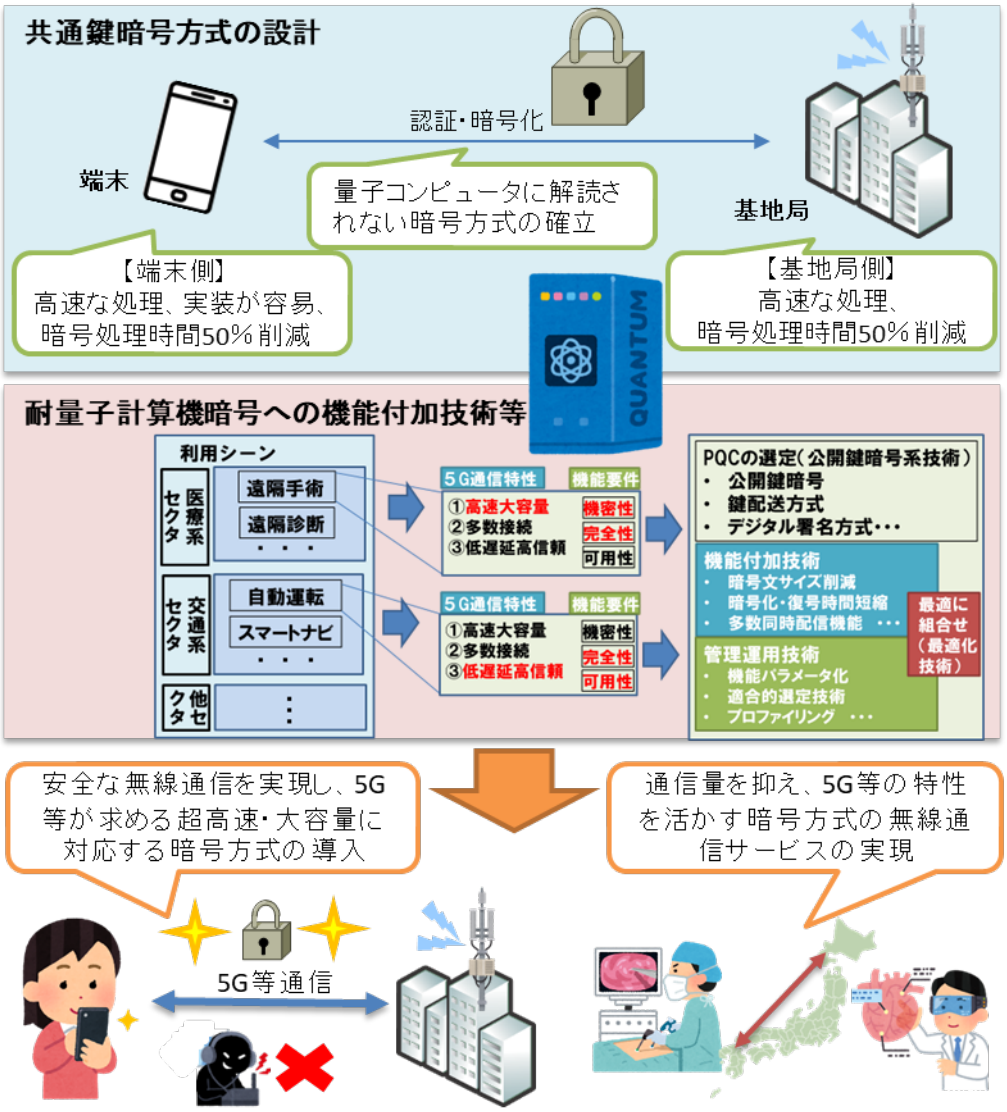


図 1：研究開発概要図

技術の種類	技術の概要
5G 等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）	5G 及びより高度な無線通信（端末と基地局の間の通信）においては、さらなる高速大容量化が図られると考えられ、既存の暗号方式よりも高速な共通鍵暗号方式が求められる。また、大規模量子コンピュータが実用化されると鍵の解読にかかる計算時間が削減されるため、現在利用されている鍵長（128bit）を２倍に伸ばし、鍵長 256bit の鍵を利用可能とする必要がある。一般に、速度と鍵長はトレードオフの関係にあり、既存の暗号方式で 256bit 鍵を使用した場合には、速度低下を引き起こすため、5G 等の無線通信に求められるようなさらなる高速化は実現できない。そのため、計算機リソースが限られた携帯端末にも実装が可能であり、大規模量子コンピュータへの安全性を確保しながら、5G 等に適した高速な共通鍵暗号方式の確立が必要となる。 また、暗号方式は、最新の解読手法等を考慮しても十分な安全性を保持することが求められるため、最新の攻撃手法を調査するとともに、将来想定される攻撃手法の改良に対しても検討を行う必要がある。併せて、暗号方式の実用性を評価するためには、実利用に近い環境において、その性能等を実証評価する必要がある。 したがって、大規模量子コンピュータに対する安全性を確保しつつ、暗号化処理に要する計算量や処理時間を低減させた高速共通鍵暗号方式の確立を目的として研究開発を行う。
5G 等のための耐量子計算機暗号への機能付加技術等（耐量子コ	5G 環境では、既に規格化された暗号化、認証、鍵管理技術が活用されているが、5G の高度化の一環として、将来の大規模量子コンピュータの実用化を見据え、5G の特性を損なわずに、PQC 技術を実装する必要がある。 将来の大規模量子コンピュータの実現を想定した 5G 等の無線環境において、PQC を利活

ンピュータセキュリティ技術）	用するためには、鍵長や暗号文サイズ、鍵生成・暗号化・復号の処理時間などをユースケース毎に適切に検討することによる、無線リソースを逼迫させないための PQC の選定及び当該方式におけるパラメータの選択等が重要となる。一例として、医療サービスにおける「遠隔手術」のユースケースを想定した場合、扱われる手術関連データの完全性、手術システムの可用性や低遅延性などが重要な特性と考えられ、これらの特性を加味した形で PQC の適用方法、実装方法の検討を進める必要がある。また、その際には、計算機リソースが限られた端末でも 5G の特性（低遅延等）を実現するため、物理層セキュリティについても検討を行うことが重要となる。 そこで、5G の様々なユースケースに応じてオーバーヘッドがより少なくなるように、複数の PQC への機能付加技術、管理運用技術、最適化技術（総称して「耐量子暗号系セキュリティ技術」という。）及び耐量子暗号系セキュリティ技術において計算機リソースをより効率的に利用するための物理層セキュリティ技術（耐量子暗号系セキュリティ技術と総称して耐量子コンピュータセキュリティ技術）を確立することを目的として研究開発を行う。

・スケジュール

技術の種類	令和３年度	令和４年度	令和５年度	令和６年度
5G 等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）	安全性・機能性評価指針の検討	アルゴリズムの設計	アルゴリズムの安全性評価・実装評価	無線通信環境での実証評価
5G 等のための耐量子計算機暗号への機能付加技術等（耐量子コンピュータセキュリティ技術）	PQC の機能評価	耐量子暗号系セキュリティ技術の構築	技術の改良・特定ユースケースでの評価	無線通信環境での実証評価

（２）達成目標

5G 等において、将来的に実用化が想定される大規模量子コンピュータによって既存の暗号技術は危殆化するおそれがある。そこで、本研究開発では、大規模量子コンピュータへの耐性を持ちながら、無線通信リソースの効率的な利用環境を提供できる暗号技術を開発することで、無線リソースのひっ迫を抑止し電波の有効利用を図る。さらに、開発した暗号技術については、国際標準化に向けた取組を推進する。

（5G 等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号））

共通鍵暗号として、大規模量子コンピュータにおいても、現実的な計算時間で解読できない方式、かつ計算機リソースが限られた携帯端末にも実装が可能な設計を行う。さらに、一般的に入手可能な既存の計算機環境における暗号処理のスループットとして 50Gbps を達成すること及び暗号処理に要する時間を従来方式と比較して最大 50%程度削減する。

（5G 等のための耐量子計算機暗号の機能付加技術等（耐量子コンピュータセキュリティ技術））

通信事業者が提供する 5G 基盤サービスや各種ユースケースにおける 5G サービスにおいて、その特性を損なわない耐量子コンピュータセキュリティ技術を構築し、技術付与前と比較してそのオーバーヘッド（暗号文サイズ、処理時間等）を最大８％以内に抑える。また、PQC の活用の視点から、計算機リソースが限られた携帯端末等でも実装が可能な技術開発も行う。

○政府の基本方針（閣議決定等）、上位計画・全体計画等

名称（年月日）	記載内容（抜粋）
統合イノベーション戦略 2020（令和２年７月 17 日）	第Ⅲ部 第１章 知の源泉 （２）信頼性のある自由なデータ流通の実現及びデータ駆動型社会の社会実装

	②目標に向けた施策・対応策 ＜サイバーセキュリティ統合知的基盤の構築＞ ○5G に対応したセキュリティ検証技術、IoT 機器や通信機器等のコネクテッドデバイスのセキュリティ検証技術のほか、データのセキュリティやプライバシーを確保し、安全なデータ流通と利活用を促進する技術の創出を行うとともに、暗号技術の安全性評価や耐量子計算機暗号などの新たな暗号技術の開発により、量子計算機時代に安全に利用できる暗号基盤技術を確立する。
サイバーセキュリティ研究・技術開発取組方針(令和元年５月17日)	４．今後の取組強化の方向性 ④　暗号等の基礎研究の促進 ＜具体的取組＞ 　既存の暗号システムの危殆化につながる量子コンピュータ等の国際動向を把握しつつ、耐量子計算機暗号や量子暗号等の安全なセキュリティ技術の研究・技術開発に取り組む。

（３）目標の達成状況

４年間の研究開発を通じて、目標を達成することができた。

「5G 等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号)」については、大規模量子コンピュータへの耐性のある高速共通鍵暗号の暗号アルゴリズムを設計し、現在利用されている共通鍵暗号方式の鍵長（128bit）を２倍にした 256bit の共通鍵において、当初目標 50Gbps に対し、世界最速の 530.7Gbps[4]の処理速度を達成した。さらに、暗号処理に係る時間については、最大 50%削減という当初目標に対し、従来方式（AES）と比較して約 84%の削減を実現した。

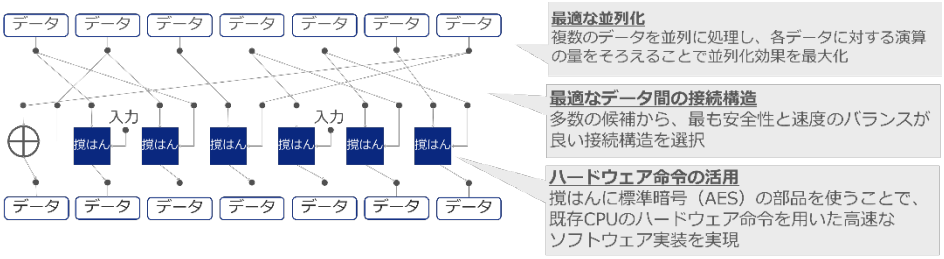
「5G 等のための耐量子計算機暗号の機能付加技術等（耐量子コンピュータセキュリティ技術)」について、高速大容量通信、低遅延高信頼通信、多数接続通信が必要とされるユースケースを考慮し、PQC に対する機能付加技術、管理運用技術及び最適化技術等を確立した。特に、オーバーヘッドを最大８％以内に抑えるという当初目標に対しては、制限付き ID ベース暗号技術[5]とプロキシ再暗号化技術[6]において、暗号文長のオーバーヘッド０％（暗号文の冗長なし）を達成した。

本研究開発において設計した暗号技術については、大規模量子コンピュータへの耐性を有しており、将来的に無線通信システムの標準仕様に採用されることによって、5G 等の特性を保ちながら、安全性を有する無線通信サービスを実現でき、周波数の有効利用の一層の向上が期待される。

また、本研究開発で開発した高速共通鍵暗号については、3GPP、ISO/IEC、IETF に標準化規格として提案活動を実施するとともに、PQC を基盤とした高機能暗号の活用に関する技術ガイダンス文書については、ITU-T の国際標準規格に提案しており、国際標準化にも貢献している。

技術の種類	目標の達成状況
5G 等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）	・高速共通鍵暗号の暗号アルゴリズムの図２のとおり設計を完了。 ・設計したアルゴリズムについては、インドの大学及びフランスの大学の独立した専門家による第三者安全性評価を実施し、安全性が確保されていることを確認。 ・ソフトウェア実装の暗号処理性能として、当初目標 50Gbps であるところ、PC では世界最速の 530.7Gbps、スマートフォンでは 173.0Gbps を達成し、大幅に目標値を超えた。 ・ソフトウェア実装の暗号処理時間に関し、当初目標 50%削減であるところ、従来方式である AES と比較して、暗号処理に要する時間を最大 84%削減され、暗号処理時間の観点でも大幅に目標値を超えた。 ・ハードウェア実装に関し、特定用途向けの集積回路である ASIC によるシミュレーション評価において、処理性能が世界最速の 2.02Tbps を達成。FPGA 実装においては、102.4Gbps を達成。 ・高いセキュリティ実装を実現するため、サイドチャネル攻撃に利用可能な電磁波による情報漏洩がないことを確認し、十分な安全性を有することを確認。 ・256bit 共通鍵暗号として、AES-256 と開発した高速共通鍵暗号を導入し、3.7GHz 帯の無

[4] 他研究の実績においては、352.3Gbps が最速であった。
[5] メールアドレス等の任意の値を公開鍵に設定可能な公開鍵暗号。
[6] 暗号化されているデータを復号することなく、再び暗号化する

	線信号を送受信する環境を構築。当該環境において暗号処理時間が 68%削減されることを確認。 ・上記より、暗号処理のスループット及び暗号処理に要する時間に係る目標値については、計画を超えた成果を達成。これにより、5G 等の特性を保ちながら、安全性を有する無線通信サービスを実現でき、周波数の有効利用の一層の向上に寄与できると期待される。 ・また、IETF、3GPP、ISO/IEC の国際標準規格に提案しており、国際標準化にも貢献。 ・さらに、高速共通鍵暗号のソフトウェア実装をオープンソース化するとともに、暗号化通信に利用できる主要なオープンソースライブラリにも組み込み公開することで、本研究開発で設計した暗号技術の普及活動も実施。  **図 2：設計した高速共通鍵暗号の概念図**
5G 等のための耐量子計算機暗号への機能付加技術等（耐量子コンピュータセキュリティ技術）	・実用的な高機能 PQC として、暗号文長のオーバーヘッドが０%の制限付き ID ベース暗号技術及びプロキシ再暗号化技術等を開発。これにより、暗号文サイズ等のオーバーヘッドを最大８%以内に抑える当初目標を達成。 ・さらに、効率的な高機能 PQC として、ID ベース暗号の拡張方式を開発し、従来方式と比較して復号鍵サイズが約 1/72 のサイズ、暗号文サイズが約 1/7 を実現。また、ID ベース署名については、従来方式と比較して鍵サイズが約 1/20 のサイズ、署名サイズが約 1/250 のサイズを実現。これら幅広い PQC の機能付加技術を開発。 ・その他、新たな鍵共有方式やデジタル署名の高速化を開発するとともに、多変数連立方程式の求解を競う暗号解読コンテストにおいて２回の世界記録更新を達成。 ・PQC の管理運用技術については、5G 等の多様なユースケースと高機能暗号のアクセス構造に対応した PQC の管理フレームワークの設計を実施。 ・ユースケースごとの機能要件に基づき最適な暗号方式を選択する技術を開発し、本研究開発で開発した高速共通鍵暗号及び集約署名を併せた統合評価を実施（図３）。端末が少ない場合は通常の署名方式を使用し、端末が多い場合は集約署名を適用することで、通信量の削減が可能であることを実証。 ・物理層セキュリティ技術として、PQC を利用できない環境において、無線通信路の特性を活用して秘密鍵を共有する技術や PQC の実装に対するサイドチャネル対策技術について検討を実施。 ・上記より、暗号文長のオーバーヘッドに係る目標値については達成。これにより、5G 等の特性を保ちながら、安全性を有する無線通信サービスを実現でき、周波数の有効利用の一層の向上に寄与できると期待される。 ・また、PQC を基盤とした高機能暗号の活用に関する技術ガイダンス文書の ITU-T 規格化に向け、「Guidance on use of advanced cryptography based on PQC (TR.ac-pqc)」を提案しており、国際標準化にも貢献。  **図 3：統合評価系**

３　政策効果の把握の手法

研究開発の評価については、各要素技術における目標の達成状況、論文数や特許出願件数などの指標が用いられ、これらを基に専門家の意見を交えながら、必要性・効率性・有効性等を総合的に評価するという手法が多く用いられている。この観点に基づき、「電波利用料による研究開発等の評価に関する会合」（令和７年６月 20 日）において、目標の達成状況等に関して外部評価を実施し、政策効果の把握に活用した。

また、外部発表や特許出願件数、国際標準提案件数等も調査し、必要性・有効性等を分析した。

４　政策評価の観点・分析等

○研究開発による特許・論文・研究発表・国際標準の実績からの分析

・論文や研究発表の実績の観点では、下表に示すとおり、査読付き誌上発表論文 51 件、査読付き口頭発表論文 55 件、その他の誌上発表 21 件、口頭発表 136 件を実施した。受託期間４年間にて、研究成果についてタイムリーにアピールに努めていた。これらの発表の中には、暗号技術のトップカンファレンスである Eurocrypt（２件）や Asiacrypt（２件）への採択も含まれる。また、本研究に係る一連の成果により、文部科学大臣表彰 若手科学者賞、末松安晴賞、船井学術賞など、数々の権威ある賞を受賞した。これらの内容は、研究成果のアピールを積極的に行っているとともに、本研究開発の必要性、有効性等が外部から認められた証左と考える。

・特許の観点では、下表に示すとおり、受託期間４年間で 28 件（うち国際特許出願は２件）を実施した。本研究開発は、大規模量子コンピュータの実用化後においても、無線通信システムに導入可能な暗号技術に関わるものであり、権利化後の有効性は高い。今後も関連する特許出願が見込まれ、本研究開発の必要性、有効性が認められる。

・国際標準化の観点では、下表に示すとおり、受託期間４年間で 37 件の寄書を実施。IETF、3GPP、ISO/IEC 及び ITU-T に提案活動を実施しており、議論が継続中である。国際標準化により移動体通信の基地局や端末等への導入が進むことが期待され、本研究開発の必要性、有効性が認められる。

主な指標	令和３年度	令和４年度	令和５年度	令和６年度	合計
査読付き誌上発表論文数	１件（１件）	18 件（18 件）	14 件（14 件）	18 件（18 件）	51 件（51 件）
査読付き口頭発表論文数（印刷物を含む）	１件（１件）	10 件（10 件）	24 件（24 件）	20 件（20 件）	55 件（55 件）
その他の誌上発表数	４件（４件）	７件（３件）	４件（３件）	６件（３件）	21 件（13 件）
口頭発表数	18 件（０件）	37 件（１件）	47 件（１件）	34 件（３件）	136 件（５件）
特許出願数	１件（０件）	８件（０件）	９件（２件）	10 件（０件）	28 件（２件）
特許取得数	０件（０件）	０件（０件）	０件（０件）	０件（０件）	０件（０件）
国際標準提案数	０件（０件）	５件（５件）	11 件（11 件）	21 件（21 件）	37 件（37 件）
国際標準獲得数	０件（０件）	０件（０件）	０件（０件）	０件（０件）	０件（０件）
受賞数	０件（０件）	２件（０件）	７件（１件）	８件（１件）	17 件（２件）
報道発表数	１件（０件）	０件（０件）	２件（０件）	０件（０件）	３件（０件）
報道掲載数	１件（０件）	２件（０件）	０件（０件）	０件（０件）	３件（０件）

注１：各々の件数は国内分と海外分の合計値を記入。（括弧）内は、その内海外分のみを再掲。

注２：「査読付き誌上発表論文数」には、定期的に刊行される論文誌や学会誌等、査読（peer-review（論文投稿先の学会等で選出された当該分野の専門家である査読員により、当該論文の採録又は入選等の可否が新規性、信頼性、論理性等の観点より判定されたもの））のある出版物に掲載された論文等（Nature、Science、IEEE Transactions、電子情報通信学会論文誌等および査読のある小論文、研究速報、レター等を含む）を計上する。

注 3：「査読付き口頭発表論文数（印刷物を含む）」には、学会の大会や研究会、国際会議等における口頭発表あるいはポスター発表のための査読のある資料集(電子媒体含む)に掲載された論文等(ICC、ECOC、OFC など、Conference、Workshop、Symposium 等での proceedings に掲載された論文形式のものなどとする。ただし、発表用のスライドなどは含まない。）を計上する。なお、口頭発表あるいはポスター発表のための査読のない資料集に掲載された論文等（電子情報通信学会技術研究報告など）は、「口頭発表数」に分類する。

注 4：「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等（査読の有無に関わらず企業、公的研究機関及び大学等における紀要論文や技報を含む）を計上する。

注 5：PCT（特許協力条約）国際出願については出願を行った時点で、海外分１件として記入。(何カ国への出願でも１件として計上)。また、国内段階に移行した時点で、移行した国数分を計上。

注 6：同一の論文等は複数項目に計上しない。例えば、同一の論文等を「査読付き口頭発表論文数（印刷物を含む)」および「口頭発表数」のそれぞれに計上しない。ただし、学会の大会や研究会、国際会議等で口頭発表を行ったのち、当該学会より推奨を受ける等により、改めて査読が行われて論文等に掲載された場合は除く。

○各観点からの分析

観点	分析
必要性	5G 等の無線通信システムにおいても、送信者と受信者で共通の鍵を使って暗号化・復号化を行う共通鍵暗号方式と、暗号化と復号化で公開鍵・秘密鍵という別の鍵を使う公開鍵暗号方式が広く利用されている。これらの暗号方式は計算困難性に基づいて利用されているが、大規模量子コンピュータが実用化されると、従来の公開鍵暗号方式が危殆化するおそれがあるため、PQC に移行する必要がある。PQC として様々な暗号技術が開発・提案されているが、移行する PQC の方式によっては、暗号文データが膨大となり、無線通信における帯域をひっ迫する可能性がある。また、共通鍵暗号方式についても、大規模量子コンピュータへの耐性を持つには、一般に鍵長を２倍程度増やす必要があるとされているが、鍵長が増えると暗号化に要する計算量等が増え、単位時間あたりに処理可能なデータ量が減少する。つまり、5G 等の高速・大容量といった特性を踏まえると、大規模量子コンピュータに耐性のある暗号技術の暗号化処理に係る時間がボトルネックとなることが想定される。 統合イノベーション戦略 2020（令和２年７月 17 日）においては、暗号技術の安全性評価や耐量子計算機暗号などの新たな暗号技術の開発による、量子計算機時代に安全に利用できる暗号基盤技術についての研究開発の重要性が指摘されているところ、本研究開発は、5G 等が求める超高速・大容量に対応した暗号アルゴリズムを開発するとともに、ユースケースに合わせた PQC の機能付加技術等を開発することで、5G 等におけるセキュリティの確保を通じて安全・安心な社会インフラの実現に資することから、研究開発すべき課題である。 また、高速共通鍵暗号や公開鍵暗号に基づく PQC への機能付加技術等の開発により、暗号処理性能の向上や暗号データ量の削減等が実現されることは、国民の財産である電波資源の有効利用及び国民の生活インフラである ICT の安全・安心の確保に資するものであり、国が実施すべき研究開発として推進する必要がある。 よって、本研究開発には必要性があったと認められる。
効率性	実施期間中も受託者の研究代表者・実務者の定期的会合において各々の進捗状況や課題が調整・共有され、さらに外部の有識者と受託者から構成される委員会や、外部有識者による継続評価において、研究進捗や進め方等について助言を受けるなど、効率的な実施のため情報交換が積極的に行われた。 また、暗号技術に関する専門的知識や研究開発遂行能力を有する企業・大学・国立研究開発法人、研究者等のノウハウを積極的に活用することにより、各々がそれぞれ得意な分野を担当し、効率的に研究開発が進められた。 委託経費の執行に当たっては、予算要求段階、公募実施の前段階、提案された研究開発提案を採択する段階、研究開発の実施段階及び研究開発の終了後における、実施内容、実施体制及び予算額等について、外部専門家・外部有識者から構成される評価会において評価を行い、効率的に実施した。 よって、本研究開発には効率性があったと認められる。
有効性	本研究開発においては、将来実用化が想定される大規模量子コンピュータにも安全性を有する高速共通鍵暗号の設計完了・実装技術を完成するとともに、5G 等のユースケースに応じて、PQC の機能付加技術等を開発した。超高速・低遅延な共通鍵暗号方式や効率的な高機能 PQC の開発により、5G 等の高速・大容量という特性を活かしながら、安全性を有する暗号技術を導入することができ、大規模量子コンピュータ実用化後においても安全性を有する無線通信サービスが提供できる。これらの研究成果

	により、周波数の有効利用の一層の向上に寄与することができる。 さらに、5G やその後継技術となる無線通信の保護に利用できる。本研究開発において設計した高速共通鍵暗号方式や PQC の機能付加技術等については、国際標準化規格への提案活動を実施しており、これらの移動通信システムの標準仕様に採用されることで、基地局、端末、センサデバイス、スマートカード等への実装が進み、本暗号技術の普及が急速に進むことが期待できる。ソーシャルメディア、ネット動画視聴サービス、ネットショッピング等のオンラインサービスにおいては、通信の暗号化に共通鍵暗号方式、認証・鍵共有に公開鍵暗号方式を利用することが一般的であり、国際競争力のある高速共通鍵暗号方式の設計や PQC の機能付加技術の開発に成功したことで、さまざまなサービスに導入されることが期待できる。また、これらの技術開発により知的財産を確保するとともに、この知的財産を我が国の製造事業者やサービス事業者にライセンシングする体制を築き上げることにも寄与するものである。このことにより、研究成果の実用化・商用化を促進するとともに、我が国の製品開発能力の引き上げを図る。 よって、本研究開発には有効性があったと認められる。
公平性	本研究開発の成果は、国民の財産である電波資源の有効利用に資するものであり、無線通信サービスの利用者の利益となる。また、本件研究開発は情報セキュリティの基盤である暗号技術に関するものであり、国民の生活インフラである ICT の安全・安心の確保に資するものである。 本研究開発の実施に当たっては、開示する基本計画に基づき広く提案公募を行い、提案者と利害関係を有しない複数の有識者により審査・選定した。 よって、本研究開発には公平性があったと認められる。
優先性	5G 等の無線通信システムにおいては、将来的に実用化が想定される大規模量子コンピュータに耐え得る安全性を担保する必要がある。加えて、十分な安全性評価や標準化活動を行う期間がそれぞれ必要となるため、社会において新たな暗号方式を導入し普及させるためには 10 年以上を要する。 以上から、本研究開発の成果を社会実装し、周波数の有効利用を図りつつ、安全・安心に 5G 等の無線通信システムを活用できる社会を実現するため、本研究開発を優先的に実施する必要がある。 また、サイバーセキュリティ研究・技術開発取組方針（令和元年５月 17 日）においても、「既存の暗号システムの危殆化につながる量子コンピュータ等の国際動向を把握しつつ、耐量子計算機暗号や量子暗号等の安全なセキュリティ技術の研究・技術開発に取り組む」とされており、大規模量子コンピュータに耐性のある暗号技術の研究開発は早急に実施する必要があった。 よって、本研究開発には、優先性があったと認められる。

５　政策評価の結果（総合評価）

5G 等の無線通信システムにおいて、将来実用化が想定される大規模量子コンピュータにより、従来使用してきた暗号技術が危殆化するおそれがあるため、高速・大容量といった 5G 等の特性を損なわず、大規模量子コンピュータにも耐性のある暗号技術を利用する必要がある。本研究開発においては、5G 等の特性を保つことを前提に、超高速・低遅延な共通鍵暗号方式を開発するとともに、5G 等のユースケースに応じて、PQC の機能付加技術等を開発した。なお、本研究開発で開発した暗号技術については、当初設定した目標を大幅に超えて達成することができた。

また、本研究開発において設計した高速共通鍵暗号方式や PQC の機能付加技術等が、今後移動通信システムの標準仕様に採用されることで、基地局、端末、センサデバイス、スマートカード等への実装が進み、本暗号技術の普及が急速に進むことが期待できるため、大規模量子コンピュータの実用化後においても安全性だけでなく効率的な無線通信サービスの提供に貢献し、周波数の有効利用の一層の向上も貢献できる。

よって、本研究開発には有効性、効率性等があると認められた。

＜今後の課題及び取組の方向性＞

上述のとおり、本研究開発の目標は達成することができたが、研究成果の社会実装を目指し、国際標準化活動に係る取組を実施する必要がある。

本研究開発で開発した高速共通鍵暗号については、3GPP、ISO/IEC 及び IETF での標準化を目指す。3GPP については、標準化されることによって我が国を含む様々な国の移動体通信の基地局や端

末等への導入が進むことが期待される。ISO/IEC の標準化については、汎用共通鍵暗号アルゴリズムとして幅広い普及が見込まれる。IETF の標準化については、インターネットにおける暗号化通信のデファクトスタンダードである TLS（Transport Layer Security）を規定しており、当該高速共通鍵暗号を暗号スイートに追加することで、インターネットでの通信における幅広い活用が期待される。

また、本研究開発では、PQC を基盤とした高機能暗号の活用に関する技術ガイダンス文書の ITU-T 規格化にも取り組む必要があり、サービス設計者・開発者に向けた参考指針となることが期待される。

上記の取組を通して、本研究開発の成果を社会に還元し、電波の有効利用に貢献していく。

６　学識経験を有する者の知見の活用

「電波利用料による研究開発等の評価に関する会合」（令和７年６月 20 日）において、目標の達成状況や得られた成果等、実施体制の妥当性及び経済的効率性、実用化等の目途等について外部評価を実施し、外部有識者から以下の御意見等を頂いたため、本研究開発の評価に活用した。

・高速共通鍵暗号に関しては、アルゴリズムの設計を完了し、ソフトウェア実装により、PC では 530.7Gbps（世界最速）、スマートフォン（iPhone 16）では 173.0Gbps の処理性能を達成し、AES-256 と比較し暗号処理時間を最大 84%削減している。また、高速共通鍵暗号を無線通信プロトコルに組込み、暗号の処理時間を約 68%削減している。耐量子計算機暗号（PQC）に関しては、同種写像問題に基づく新たな鍵共有方式、格子問題に基づくデジタル署名の高速化、効率的、実用的な PQC ベース高機能暗号の開発と評価を行っている。査読あり論文 51 件、査読あり口頭発表 55 件、特許申請 28 件、受賞 17 件と顕著な研究成果をあげており、高く評価できる。予算は効率的に使用されたと思われる。標準必須特許への採用を目指した特許出願 17 件、外国出願２件を含め、28 件の特許出願がなされている。高速共通鍵暗号に関しては、3GPP において 256bit 暗号の導入に合意し、技術文書を発行し、また、ISO/IEC において認証暗号規格 ISO/IEC 19772 の改定に向けた作業項目を主導している。耐量子計算機暗号の機能付加技術に関しては、2025 年度に ITU-T 勧告(TR)として完成させ、承認の取得を目指している。よって、総合的に見て有益であったと思われる。

７　評価に使用した資料等

○統合イノベーション戦略 2020（令和２年７月 17 日）
https://www8.cao.go.jp/cstp/togo2020_honbun.pdf

○サイバーセキュリティ研究・技術開発取組方針（令和元年５月 17 日）
https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/kenkyu_torikumi.pdf

○電波利用料による研究開発等の評価に関する会合 ＜電波利用料＞
https://www.tele.soumu.go.jp/j/sys/fees/purpose/kenkyu/index.htm

○基本計画書　安全な無線通信サービスのための新世代暗号技術に関する研究開発
https://www.tele.soumu.go.jp/resource/j/fees/purpose/pdf/210126_keikakusho_RD.pdf