TOSHIBA

経済安全保障技術育成プログラム／ハイブリッドクラウド利用　基盤技術開発／〔１〕強固な鍵管理によるデータセキュリティ技術（HSMの技術開発）（中間評価）2023年～2027年　プロジェクト報告資料

株式会社東芝
HSM開発・拡販プロジェクトチーム
2025. 6. 2

１．評価項目１

＜評価項目１＞研究開発ビジョン及び研究開発構想の実現に向けた研究開発課題の達成目標や内容の妥当性

（１）研究開発課題の達成目標の妥当性
（２）知的財産・標準化戦略

（１）研究開発課題の達成目標の妥当性

他社主力製品のハードウェア、ソフトウェア機能のベンチマークを実施し、他社同等レベルで製品仕様を策定した。
裏付けを取るために、顧客ヒアリングを実施し、機能・処理性能等の要求妥当性を確認した。
ヒアリングの中から、既存製品の問題・課題、新たな要求を抽出し対応方法を検討した。
機能差異（ユーザ認証、マルチテナント）および抽出した問題の対応を差異化要素として取り込んでいく。
また、研究開発方法を変更し、システム設計以降、まず動くものを作る事に重点を置き、ハード、ソフトともフェーズ管理して進めることとし、方針変更した。
社会実装においては、まずは日本から展開という方針を立て、既存分野の置換えに着眼し、顧客ヒアリングを実施した。マーケット情報、ヒアリング情報を分析して、事業戦略に反映した。

（１）研究開発課題の達成目標の妥当性

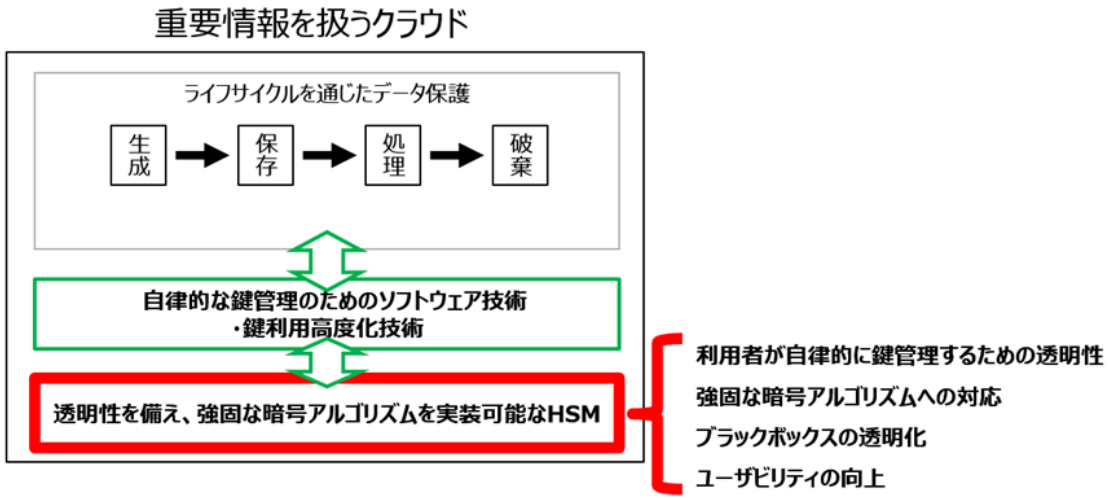
（１）－１　本事業の目的・概要

研究項目名：強固な鍵管理によるデータセキュリティ技術（HSMの技術開発）

＜事業の目的＞
現状のハードウェアセキュリティモジュール（HSM）は、**海外製しかなく、中身がブラックボックス化されている**という課題や、**現在の暗号アルゴリズムでは量子計算機によって現実的な時間で解読されうるというリスクが存在する**。

上記の課題を解決するため、利用者が自律的に暗号鍵を管理するための透明性を備え、強固な暗号アルゴリズムを実装可能なHSMの技術開発を行う。

＜事業イメージ＞



（１）研究開発課題の達成目標の妥当性

（１）－２　研究開発項目の必要性とその背景

HSMを使ったシステム構築を長年実施している経験を活かし、FIPS140-3認定を取得したHSMに係る
研究開発を実施する。

研究項目としては、要求されるHSMを実現するために必要な項目としている。
特に、“利用者が自律的に暗号鍵を管理するための透明性”を実現するために、ユーザ認証機能を具備して、
誰がいつ鍵操作をしたか、HSM内でロギングできる仕組みをつくる。この機能は、他社にはない機能であり、
今後各分野のセキュリティ規格上でロギングが必須になる可能性も見込まれる。
また、現行HSMでの課題を抽出、解決し、ユーザビリティの向上を目指す。

並行して、社会実装に向けた事業戦略策定を実施する。

本研究開発により、製品の安定供給に加えて、機器（HW・SW）の仕様・設計の透明性を担保し、
国内に技術力を確保できる。

（１）研究開発課題の達成目標の妥当性

（１）－３　実施項目についての概要説明

研究開発項目①：製品仕様定義
他社主要HSMのカタログ・取扱説明書でベンチマークを行い、対応暗号アルゴリズムや処理性能、適用外部規格（FIPS、安全規格等）を定義する。

研究開発項目②：利用者が自律的に鍵管理を可能とするためのアクセス権限/インタフェースの透明性の検討
HSM内に認証許可アクセス機能を具備することにより、利用者の識別を可能とし、HSMにアクセスしたユーザを識別し、アクセス制御するのと同時にロギングも行う。これにより、誰がという情報がロギングできる。

研究開発項目③：強固な暗号アルゴリズムへの対応
当社開発済みの暗号IP（ハードウェア回路）をHSM用にチューニングし、FPGAに搭載する。量子計算機対応として、耐量子計算機暗号（PQC：Post Quantum Cryptography）搭載の検討も実施する。

研究開発項目④：ブラックボックス化されている現行HSMの内部仕様透明化の実現
本事業において、ブラックボックスになっている部分を透明化することで、有事の際には、製品の何が問題なのか、部品単位・プログラム単位で詳細に解析できるようになり、どういった対策が必要なのかを説明し助言することを可能とする。

研究開発項目⑤：ユーザビリティの向上
利用者視点で使い勝手の良い製品を開発する。ユーザインタビューの中で得た既存HSMの課題を解決し、互換性も意識したものにする。

研究開発項目⑥：ハードウェア開発
FIPS140-3要件を満たす耐タンパ性を有したハードウェア開発を行う。また、他社製HSMと価格競争力のある製品開発を実施する。

研究開発項目⑦：FIPS認定
FIPS認定取得に向けて、セキュリティ評価ラボ（株式会社ECSEC Laboratory（以下ECSEC））と連携し、効率良く認定取得を実施する。

研究開発項目⑧：市場参入を見据えた具体的な事業戦略策定
市場参入を見据え、マーケット情報を調査し、各業界動向をヒアリングし、事業戦略を策定する。

（１）研究開発課題の達成目標の妥当性

（１）－４　開発の進め方

各研究項目で要件定義した結果を元に、システム設計を実施した。システム設計の結果、基本設計以降は、以下のようにフェーズ管理して進めることとした。

研究項目②、③、④、⑤に関しては、ソフトウェア機能として実装していき、以下のソフトウェアフェーズで進めていく。
研究項目③は、現状のIP（暗号ロジック）のチューニングを実施し、性能改善が完了した時点で順次入れ替えていく。
また、2025年度にPQC （ML-DSA：FIPS204、ML-KEM ：FIPS203 ）の実装を実施する。
研究項目⑥ハードウェアに関しても、以下の３回のプロトタイプを作成し、フィードバックを重ねていく。
研究項目⑦のFIPS認証に関しては、設計書含むドキュメント、および実機で事前レビューを随時実施し、FIPS本番評価（2026年度）前にフィードバックしていく。

＜ソフトウェア　フェーズ＞

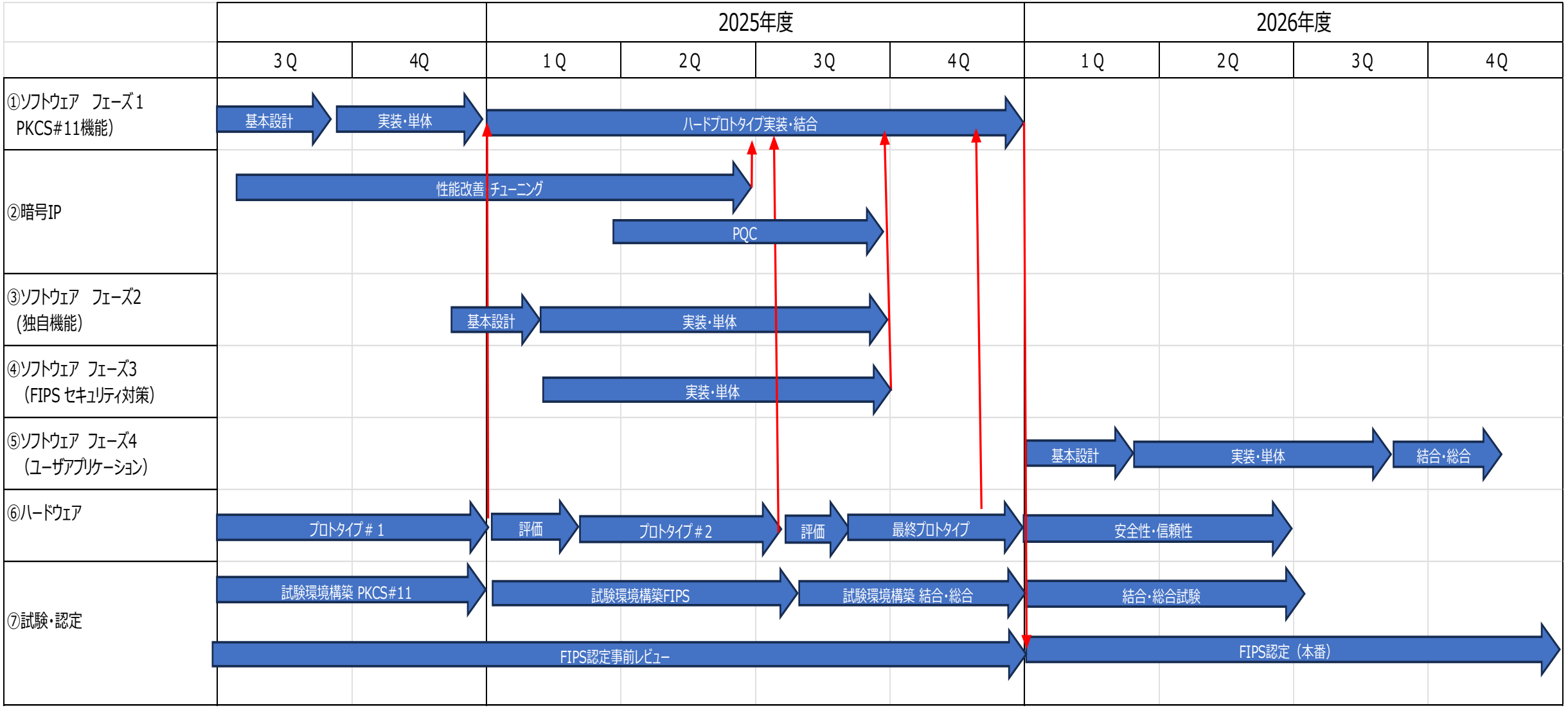
工程	時期	内容
フェーズ１ （PKCS#１１機能）	2024年度	HSMの標準I/FとなるPKCS#１１を先行して開発し、システムのベースを立ち上げる。本機能を先行開発することにより、データクラウドとの接続確認を早期に実現できる。
フェーズ2 （独自機能）	2025年度	PKCS#１１で定義されていない固有機能を開発し、結合していく。 （ユーザビリティ向上のためのユーティリティ、Wrapper） 2024年度　ユーザインタビューで現行HSMの課題も抽出して取り込む。
フェーズ３ （FIPS対応）	2025年度	FIPS認証に必要な、セキュリティ対策を実施する。
フェーズ4 ユーザアプリケーション （SAM）搭載機能	2026年度	HSM内で動作するアプリケーションを実装する機能。 （FIPS認定対象外）

＜ハードウェア　プロトタイプ＞

工程	時期	内容
プロトタイプ試作(＃1)	2024年度 (ソフト搭載の評価は、2025年度)	・少量を試作し、製品の基本的な機能や性能を確認することを目的とする。 ・FIPS要求と海外安全規格適合に向けた設計妥当性検証を行い、改善点を洗い出すことを目的とする。
プロトタイプ試作(＃２)	2025年度	・プロトタイプ試作(＃1)の改善点取り込みを行うことを目的とする。 ・台数を多く製造することで判明する製造性・信頼性の課題(製造ばらつき等)と改良点を抽出することを目的とする。 ・FIPS及び海外安全規格に対して、合格レベルに引き上げることを目的とする。
最終プロトタイプ試作機	2025年度	・プロトタイプ試作機＃２の改善点取り込みを行うことを目的とする。 ・金型製作／大量生産で安定した製造プロセスを確立することを目的とする。 （採用する部品、材料、製造条件を確立し、信頼性としてばらつきのない試作に作り上げる） ・製品同等の最終試作機を用いて、FIPS試験と海外安全規格試験を行う。 また、ハードウェア信頼性試験、ソフトウェア/ハードウェア含めた 総合試験を実施する。

（１）研究開発課題の達成目標の妥当性

（１）－５　各項目と基本設計以降のスケジュール



（2）知的財産・標準化戦略

Kプロ知財方針に基づき実施中。

２．評価項目２

＜評価項目２＞研究開発課題の達成目標に向けた進捗状況

（1）研究開発課題の達成目標に向けた進捗状況（国内外との比較を含む）
（2） 今後の見通し（多様な分野における実現可能性含む）

（１）研究開発の進捗状況・成果

（１）－１　開発の進捗状況

基本設計以降、主にソフト機能、ハード機能に研究項目を振り分けて、開発方法をフェーズ管理で実施することにし、目標を再設定した。
スケジュールも変更して開発を進め、モノ作りに関して順調に進捗しており、2024年度の目標を達成している。
事業計画に関しては、市場状況、顧客ヒアリングをもとに分析を実施、新規分野との連携協議も実施して事業計画を策定した。

（１）研究開発の進捗状況･成果

（１）－２　主な成果と進捗状況

実施項目	実施状況	これまでの主な成果
①ソフトウェア　フェーズ１ （PKCS#11機能）	順調	システム設計、基本設計完了。評価ボードを使って機能試作実装完了。 プロトタイプボード#１にポーティング実施中。PKCS#11 基本機能のポーティングと一部結合確認完了（70%）。 結合確認完了は、８月予定。
②暗号IP	少し遅れ	処理性能改善は、処理並列化、コア128bit化の実装とシミュレーションでの動作評価が完了した。改善の結果、目標処理時間を達成することが確認できた。128bit化の改善の途中で予想以上にリソース容量（ロジック量）が増加することが解り、再チューニング（最適化）が必要になったため、少し遅れが出た。 但し、本部分は共通部分であり、他の改善は並列で進めているため、全体スケジュールの影響はない。
③ソフトウェア　フェーズ2 （独自機能）	順調	Wrapper　：基本設計完了し、Linux実装開始。Windows含めて９月単体完了予定。 独自コマンド：基本設計が70%進んでおり、7月に完了予定。 Wrapper、独自コマンド含めて、結合は、12月完了予定。
④ソフトウェア　フェーズ3 （セキュリティ対策）	順調	2025年度実施予定。
⑤ソフトウェア　フェーズ4	順調	2026年度実施予定。
⑥ハードウェア	順調	プロトタイプ#１（PCI型）：試作ボードが完成し、安全性評価、物理セキュリティ事前評価（FIPS）を実施中。 プロトタイプ#１（LAN型）：組み立て完了。安全性評価実施中。
⑦試験	順調	PKCS#11機能の試験環境を完成。品質維持のための追加項目は、継続して追加中。 CAVP、結合、総合試験環境構築中。
⑧事業計画	順調	マーケット情報、ヒアリング結果をもとに、事業戦略を策定した。

（２）今後の見通し

モノ作りに関しては、フェーズ管理した新スケジュールに従い、開発を進めていく。
社会実装に向けて、ハイブリットクラウドの上流にあたるベンダと早期に接続確認を実施し、動作検証を実施していく。また、その他既存HSMユーザとのPoCを早期実施し、フィードバックや業務連携を進めていく。

（２）今後の見通し

（２）－１　今後の進め方

＜ソフトウェア＞

スケジュールに従い、開発を実施していく。

＜暗号IP＞

スケジュールに従い、チューニング作業を実施していく。

＜ハードウェア＞

プロトタイプのそれぞれの目的、実施内容に従い、開発を実施していく。

＜事業戦略＞

関係ベンダとの先行PoC等を実施して、早期に置換えの確認を実施する。

３．評価項目３

＜評価項目３＞マネジメント

（1）実施体制
（2）研究資金の効果的、効率的な活用
（3）国民との科学・技術対話に関する取組

（１）実施体制

2024年8月に専門組織として、HSM開発・拡販プロジェクトチームを新設し、マネジメントの強化を図った。
進捗管理方法に関しても、以下のように実施している。
ソフトウェアに関しては、開発の状況、問題点などを見える化するツールを使用して、週1回開発リーダが進捗確認を行っている。ハード等も週1回開発リーダが打合せにより進捗確認を実施している。
また、ソフト、ハードの全体進捗を責任者含む全メンバで確認共有して進めており、問題点の早期把握や調整を実施して、進捗遅れの無いように進めている。

（２）研究資金の効果的、効率的な活用

NEDO委託業務　事務処理手続き、経費計上の手引きに従い適切に計上をしている。
年度初めに予算計画を実施して、毎月管理している。
また、その他経費、機械設備費等　検収毎に、エビデンスをまとめ、毎月社内経理部門の確認を実施している。
その他、社内の国プロコンプライアンス規定に従い、年に１度自主監査を実施している。

2023年度中間検査（中間）、（年度末）、2024年度中間検査（中間）を受けて、経費が正しく計上されていることをNEDOに監査していただき、合格している。

（３）国民との科学・技術対話に関する取組

展示会の出展、講演、デジマコンテンツによる紹介、東芝レビュー（東芝グループの先端技術開発の取り組みや技術成果を紹介する技術論文誌）による投稿を予定しています。