「ハイブリッドクラウド利用基盤技術の開発」に関する研究開発構想
（個別研究型）

令和４年１２月
（令和５年３月改定）

内閣府
経済産業省

目次

１．事業の背景、目的、内容

（１）事業の目的

① 政策的な重要性

クラウドサービスの普及やサプライチェーンの多様化等に伴い、サイバー空間の複雑性が増し、クラウド等の複数の情報システムを組み合わせて利用する形態も増加している。あらゆる分野でデジタル技術の活用やデータ利活用の促進が求められる中、インシデントが発生した場合の経済社会活動への影響は、従来より広範に及ぶおそれがある。

政府の重要情報でもデジタル化が進む中、データ中心のセキュリティが重要となってきており、データの作成から使用、ひいては廃棄まで、ライフサイクル全体にわたってデータを安全に管理・制御する必要性が増してきている。一方、これまでのサイバーセキュリティの考え方は境界防御モデルを基本としてきた。境界防御モデルでは、信用する領域と信用しない領域に境界を設け、境界外部からの脅威を境界上で検証・防御するという考え方である。しかしながら、昨今のサイバー攻撃の深刻化等によりセキュリティインシデントも多発しており、境界防御モデルの信頼性に限界が指摘されている。これに対し、ゼロトラストモデルに立脚してセキュアなシステム構築を可能とするよう、オープンアーキテクチャで対抗することが重要な手段となると考えられる。

その際、ハードウェアのみならず、それを用いて構築されるクラウドを含むデジタル基盤もまた信頼に足るものである必要がある。今日のクラウドは、コストや利便性に優れ、AI をはじめとした最先端の機能を提供することからデジタル基盤として幅広く利用されている。その一方でクラウドの多くのサービスは、いわゆるマネージドサービスとしてブラックボックス化されており、十分に信頼性が確保されているとは言い難い。こうした課題を解決するためには、広く提供される最先端のクラウド技術を活用しつつ、内部構造や動作原理などが明らかになっているホワイトボックスクラウドで機密性の高いデータを取り扱うなど、それぞれのクラウドの長所を活かしたハイブリッドクラウドを構築することが有用であり、その利便性向上やセキュリティ面などの高度化に向けた技術開発を促進していくことが重要である。

サイバーセキュリティを確保しつつクラウドサービスの活用を進めていくため、「デジタル社会の実現に向けた重点計画」（令和 4 年 6 月 7 日閣議決定）においては、「政府が取り扱う情報の機密性等に応じてパブリッククラウ

ドとプライベートクラウドを組み合わせて利用する、いわゆるハイブリッドクラウドの利用を促進する。」こと、「また、政府として、クラウドサービスや関連する暗号化等の技術開発や実証を支援しつつ、その成果を政府調達に反映していく」ことを定めている。

また、クラウドを含むデジタル基盤を支えるシステム及びサービスに用いられる半導体及びそれに制御される電子機器等のハードウェアは必要なセキュリティ機能が実装されているなど、信頼に足るものである必要がある。他方、世界半導体会議は、2018 年 5 月に不正な半導体に関する白書を発行し、その背景や実態、危険性について述べるとともに、世界的に偽造半導体の流通が問題となっていることに注意喚起を行っており、製造・流通する半導体のハードウェアの信頼性が確保されているとは必ずしも言い難い。こうした課題を解決するためには、半導体・電子機器等のハードウェアに期待される機能以外の不正な機能が混入していないかを特定して排除するために必要な検証技術の開発を行うなどして、セキュリティ検証基盤を確立していくことが必要となる。

「サイバーセキュリティ戦略」（令和 3 年 9 月 28 日閣議決定）においても、「不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化を推進する。」旨が示されている。

経済安全保障重要技術育成プログラムの研究開発ビジョンにおいても、領域横断・サイバー空間領域で支援対象とする技術において、

- ハイブリッドクラウド利用基盤技術
- 不正機能検証技術（ハードウェア）

が上げられている。

以上を踏まえ、政府情報システムのセキュリティ強化に向け、様々なクラウドを連携して利用する際のデータ保護技術や、ハードウェアに対する不正機能混入を検証する技術等を開発することを本事業の目的とする。

② 我が国の状況

近年、様々な分野で個人情報や企業が持つ機密情報を活用し、新たな洞察を得ようとする動きが進む一方、他社へのデータ提供時における、情報漏洩や不正利用などへの懸念も高まっている。機密性の高い金融や医療でのデータ分析、プラントにおける稼働データの分析、マーケティング事業者や同業種・他業種の協業などによる組織横断型データ分析等を実現するため、大規模なデー

タを保護しながら活用可能にする秘匿化・分散処理技術の開発ニーズが存在している。

そうした中、NEDO「人工知能技術適用によるスマート社会の実現プロジェクト／データコラボレーション解析による生産性向上を目指した次世代人工知能技術の研究開発」（2018 年度～2022 年度）では、各機関・組織が保有するデータを一か所に集約させることなく人工知能が効果的にデータ解析を行う協調機械学習技術として、データコラボレーション解析技術の開発に取り組んでいる。

JST CREST「イノベーション創発に資する人工知能基盤技術の創出と統合化／プライバシー保護データ解析技術の社会実装」（2019 年度～2021 年度）では、入出力情報を秘密に保ったままデータ処理を実行可能なプライバシー保護データ解析技術の社会実装推進を目的として、広範な適用範囲に対して誰でも利用可能な汎用的データ処理秘匿化技術の開発と、金融データ解析を特に念頭においたプライバシー保護データ解析技術の開発及び実社会での実証などに取り組んでいる。

また、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 4 3 号）に基づき、特定重要物資の安定供給確保のための個別施策として、情報処理の需要に応じて各計算資源を自動で拡張・縮小するための制御技術に係る基盤クラウドプログラム、共通化可能な機能を自動化・効率化することによりセキュリティを高度化するための基盤クラウドプログラムの開発等に関する取組に対する支援が検討されているところ、本事業と合わせて取り組んでいくこととする。

一方、半導体・電子機器等のハードウェアのセキュリティに関連する研究開発プロジェクトとして、戦略的イノベーション創造プログラム(SIP)における「重要インフラ等におけるサイバーセキュリティの確保」（2015 年度～2019 年度）において、半導体に対する外部からの侵襲性・非侵襲性攻撃技術の研究を行いそれらの攻撃に対する対策技術を開発したほか、「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（2018 年度～2022 年度）において機器の製造過程及び出荷後に機器を構成する基板上に実装される可能性のあるハードウェアトロージャンと呼ばれる IC チップや回路基板に密かに挿入された不正回路を検出し、信頼の基点となるハードウェアのセキュリティを確保するなどの研究開発が推進された。

また、半導体・電子機器等ハードウェアの消費電力や漏洩電磁波等から内部の秘密情報を取得する、サイドチャネル攻撃法が現実的な脅威となっている

が、これに関し IPA は、2021 年度の「フォトエミッション等のサイドチャネル攻撃に関する調査」事業において、半導体からの光子の放出、無線回線への情報漏洩、機械学習を利用した攻撃など、最新の攻撃方法について調査を行うと共に、同年の「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」事業において、無線回線への漏洩および機械学習を利用した攻撃について追試を行い、それらの攻撃の評価手順を明らかにした。

さらに、NEDO「AI エッジデバイスの横断的なセキュリティ評価に必要な基盤技術の研究開発」（2018 年度～2022 年度）において、AI エッジデバイスにおける入出力への脅威対策、内部保護、個体管理の各課題に取組み、AI エッジデバイス向け評価分析基盤の確立を目指している。特に、個体管理の課題では、正規の半導体・電子機器等のトレーサビリティを確保するために、物理的に複製困難なナノ人工物メトリクスの基礎技術を開発してその有効性を検証しているところである。

③ 世界の取組状況

クラウドについて、海外では、主に米国の最先端企業が高い技術力と市場競争力を持っている状況だが、国内の企業や研究機関も、秘密分散技術、データコラボレーション技術など一部の技術やシーズとなる技術を有している。また、単独のクラウド内でのデータ暗号化や機密 VM などセキュリティの高度化技術や、クラウド上のデータ基盤間の単純な連携を行う技術はそれぞれ存在するが、データの重要度に応じて適切に保護しつつ、安全・低コスト・自動で行う技術は存在しない状況にある。

また、米国では、IC チップを含むサプライチェーン・セキュリティについて、DARPA による研究開発プログラム(Supply Chain Hardware Integrity for Electronics Defense, SHIELD)が 2015 年～2019 年に実施されており、耐攻撃性を備えた半導体等の開発が進められている。欧州では、2021 年より ENISA 主導の下、あらたに EUCC セキュリティ評価認証制度の構築が開始され、IC チップのセキュリティ認証はその最初の対象とされて既にドキュメント等が整備されている。我が国においても、上述のとおり研究開発が進められてきたが、半導体等のハードウェアは機器・システムに不可欠な根幹であり、これらの信頼性を確保する検証技術は、我が国の戦略的自律性を確保していく観点から研究開発を行っていくことは重要である。

④ 本事業のねらい

本事業で研究開発を実施するハイブリッドクラウド利用基盤技術およびハードウェアの不正機能検証技術は、我が国が安全保障活動、社会経済活動を行う上で必須の基盤インフラ技術であり、他国に依存することなくこれを自律的に構築する能力を担保することをねらいとしている。

既存の事業では、データを一か所に集約させることなく効果的にデータ解析を行う技術や入出力情報を秘密に保ったままデータ処理を実行可能とする技術の開発に取り組まれてきたが、これらをクラウド上で扱う技術や現実的に利用可能な速度で処理する技術は存在していない。また、これまでの研究開発においてハードウェア・トロージャンフリーな IC 等の設計を保証する技術に関する基礎理論の構築や耐タンパー性や個体管理に関する基礎的な検討を行ってきたものの、半導体・電子機器に係るセキュリティ要求仕様の定義や実用化に向けた技術開発・実証は行われていない。

このため、本事業では、信頼性の高いクラウド基盤を構築可能とするため、異なるセキュリティ領域を接続し、利便性の向上やセキュリティの高度化に資する基盤的技術として、次世代のクラウド技術やソフトウェアスタックの技術を開発することを目的とする。また、クラウドを含む情報システムに用いられる半導体・電子機器等のハードウェアにおける不正機能排除が可能となるような検証技術の確立に向けて、半導体の設計時の IP コアに不要な機能が混入されていないか、仕様で定められていない部品が混入していないか、等の検証について、必要な要素技術の特定と技術開発を行うとともに、半導体の設計から組込みに至るまでのセキュリティ要求仕様の定義や標準化、検証のパイロット実証を行うことでハードウェアセキュリティ検証基盤を確立することを目的とする。

（2）事業の目標

① アウトプット目標

研究開発項目① 「ハイブリッドクラウド利用基盤技術の開発」

【中間目標】2026 年度まで

・ 異なるセキュリティレベルを有する複数のクラウドサービスを安全・安心かつ円滑に活用していくための基盤技術（ハードウェアセキュリティモジュールに関するものを除く）の確立および実サービスとしてのクラウド基盤の構築。

【最終目標】2028 年度まで

・ 異なるセキュリティレベルを有する複数のクラウドサービスを安全・安心かつ円滑に活用するための、鍵管理を厳格化するハードウェア技術を含めた各技術を実サービスとして実装したクラウド基盤の構築。

研究開発項目② 「半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立」

【中間目標】2025 年度まで

・ 半導体・電子機器等のハードウェアのライフサイクルの各フェーズにおける不正機能検出に必要な検証技術の開発や検証手法の構築。

【最終目標】2028 年度まで

・ 検証技術の最適化と検証体制の構築。

詳細な技術目標については、（３）項の事業の内容に記載する。

② アウトカム目標

・ 本事業で開発したクラウド基盤技術が実装されたサービスを通じて、政府や重要インフラ事業者等が機密性の高い情報等を扱うことができる、高い利便性やセキュリティを有する信頼性の高いクラウド基盤を構築可能とする。
・ 本事業で開発した検証技術により「サイバーセキュリティ戦略」で謳われている「不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化を推進する。」に貢献し、その結果、クラウドを含むデジタル基盤を支えるシステム及びサービスの信頼性の根幹となる半導体・電子機器等のハードウェアのセキュリティが確保され、当該システム及びサービスの利活用が促進される。

（３）事業の内容

本事業で研究開発を実施する両技術は、我が国が安全保障活動、社会経済活動を行う上で必須の基盤インフラ技術であるが、世界的にも本技術は確立されてい

ない。また、本事業の成果においては民生利用のみならず公的利用につなげていくことが前提となっているため、以下の研究開発項目は全て委託で実施するものとする。

研究開発項目①「ハイブリッドクラウド利用基盤技術の開発」

ア．研究開発の必要性

サイバーセキュリティを確保しつつクラウドサービスの活用を進めていくためには、内部構造や動作原理などが明らかになっている「ホワイトボックスクラウド」で機密性の高いデータを取り扱いつつ、必要に応じて最先端のクラウド（ホワイトボックスクラウドとの対比で「ブラックボックスクラウド」という）を活用するなど、それぞれのクラウドの長所を活かしたハイブリッドクラウドを構築することが有用である。こうした異なるセキュリティレベルを有するクラウドを連携させてハイブリッドクラウドとして利用するためには、利便性の向上やセキュリティの高度化に資する基盤的技術として、次世代のクラウド技術やソフトウェアスタックの技術開発を行うことが必要である。併せて、更なるセキュリティの高度化を実現するために、次世代のクラウド技術と組み合わせてセキュリティを高めるハードウェアセキュリティモジュール（以下「HSM」という。）の技術開発にも取り組むことが重要である。

イ．具体的研究内容

セキュリティレベルの異なるクラウドを利用した利便性の向上やセキュリティの高度化を実現するには、各クラウドでの厳格なデータセキュリティを実現する技術、データ流通の自動化技術及びデータ流通の基盤となるネットワークの高度化技術を一連の基盤技術として確立していく必要がある。

具体的な要素技術については、以下の通り。

〔1〕強固な鍵管理によるデータセキュリティ技術

データセキュリティとはデータをそのライフサイクル全体を通じて不正アクセスや破損、窃盗等から保護することをいい、特にデータの暗号化に用いる暗号鍵の管理はデータセキュリティの根幹をなす。その一方で、クラウドでは一般に暗号鍵管理機能自体がマネージドサービスとして提供されブラックボック

ス化されており、このため利用者にとってはその安全性を確認する手段がないといった問題がある。

こうした課題を解決するため、鍵管理をブラックボックスクラウドから分離し、ホワイトボックスクラウドで利用者が自律的に鍵管理を行うためのソフトウェア技術を開発する。また、開発した技術を用いて、ホワイトボックスクラウドのみならずブラックボックスクラウドでも利用者がデータの保存/転送/使用時の完全な制御を可能にする鍵利用高度化技術を開発する。

加えて、更に利用者が自律的に鍵管理を行うためには、鍵管理を行うための HSM の開発も重要。現状の HSM においては、中身がブラックボックス化されているという課題や、暗号化の根幹である暗号アルゴリズムに関しても現在の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リスクが存在する。

こうした課題を解決するため、利用者が自律的に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。

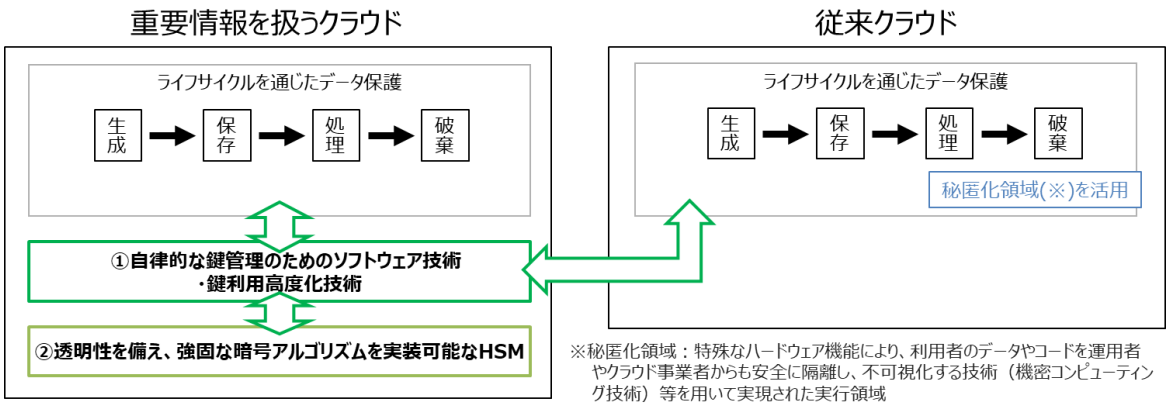

図１　強固な鍵管理によるデータセキュリティ技術の概念図

〔２〕データの保護と流通の自動化技術

あらゆる分野でデータ利活用の促進が求められる中、複数のデータ提供者とデータ利用者の間でデータの重要度に応じて、安全にデータ流通を行うニーズがある。その一方で、厳格なルールに基づきデータの安全性を確保しつつ、大量のデータ処理を円滑に実行させる処理性能を確保することが課題となっている。

安全性の確保にあたっては、データ提供者がデータへのアクセス管理ルールを作成する必要があるが、その作業を属人的に手作業で行うため、ルールの設定漏れや設定誤りが発生しやすい状況にある。さらに、そのルールに基づきデータへのアクセス管理が運用されているか、データが改竄されていないかをデータ提供者やデータ利用者自らが正確に把握するための手段が十分ではない。特に、サービスの運用者がシステムの管理者権限を有している場合にはデータへのアクセス履歴等の証跡自体を書き換えることができるため正確な把握が困難である。加えて、上述したデータの安全性に対する課題を解決しつつ、複数利用者の要求によって生じる大量のデータ処理の拡張性も同時に確保するような制御技術が十分に実現されていない状況にもある。

こうした課題を解決するため、本研究開発項目では、複数のデータ提供者とデータ利用者の間でデータの保護と流通を自動化する技術を開発する。さらに、クラウド事業者間での仕様差異をなくし、サービス利用者にとっての導入・運用の煩雑さ解消を目的として開発したインターフェース仕様の標準化を検討する。

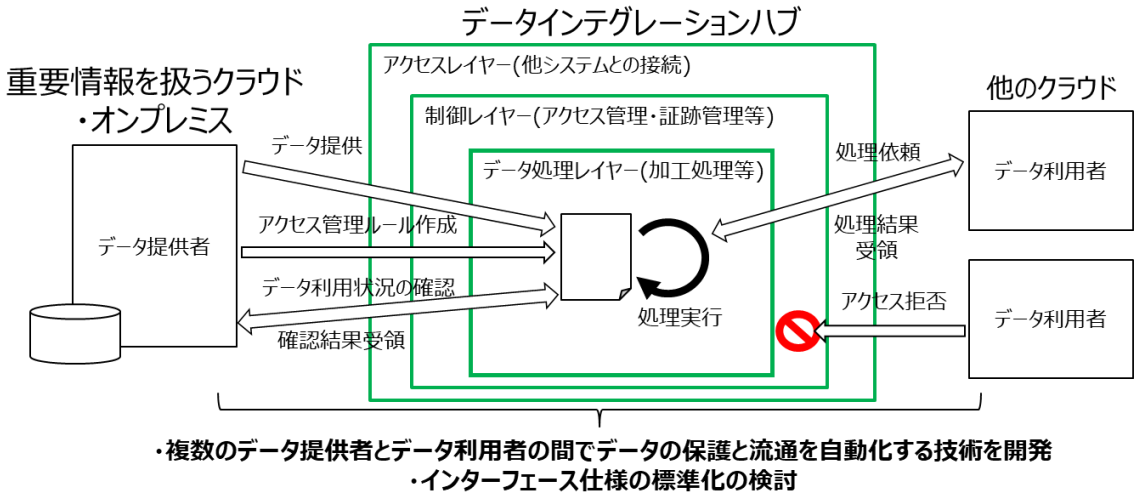

図２　データの保護と流通の自動化技術の概念図

〔３〕経路特性保証型のクラウドネットワーク技術

重要データのデーターセンター間広域通信においては、経路上での盗聴などによるデータ漏洩を防ぐため通信路の暗号化が行われる一方、より高機密なデータやそうしたデータの暗号化に用いる鍵データなどの通信では、通信路の暗

号化だけではなく、使用される経路の独立性など通信路が備える経路特性[1]の保証も必要となる。

他方、先行するクラウドセキュリティプロバイダーは、IaC（Infrastructure as Code）で管理・運用されるクラウドインフラ全体に対して、設定ミスや意図しない設定変更の防止やアラートの発出といった高度なセキュリティ機能を提供し始めている。今後高機密データを取り扱うクラウドインフラを、こうしたソリューションを通じて安全に運用・管理していくには、経路特性の指定・制御に加えて、経路特性の意図しないデグレードなどの設定変更の検出・防止を可能とする技術も不可欠となる。

こうした課題を解決するため、本研究開発項目では、経路特性の指定・制御を可能にし自動化する技術、ならびに経路特性変更等の検出・防止を可能にする技術を開発し、経路特性保証型のクラウド間接続を実現するネットワーク運用技術を確立する。

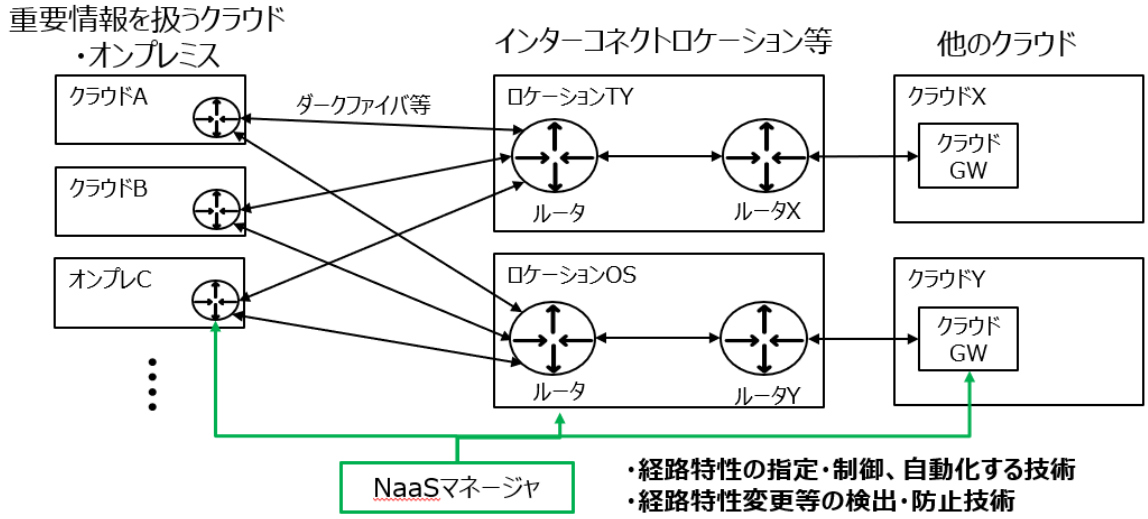

図３　経路特性保証型のクラウドネットワーク技術の概念図

ウ．達成目標

【中間目標】　2026 年度まで（〔１〕のうち、HSM の技術開発に関しては 2025 年度までの中間目標とする）

〔１〕強固な鍵管理によるデータセキュリティ技術

[1] ※ここでいう経路特性とは、帯域幅や多重度など性能や耐障害性に関わる性質のみならず、経路の論理的・物理的な独立性の有無や、将来的には量子暗号通信による情報理論的安全性の有無など、データの機密度等に応じて通信路が備えるべき性質を指す。

自律的な鍵管理のためのソフトウェア技術及び鍵利用高度化技術（以下「鍵管理ソフトウェア技術」という。）を開発するとともに、開発した技術を用いたクラウド基盤をプロトタイプ実証する。

また、HSM に関しては国際的なセキュリティ基準（FIPS 等）を参照した要求仕様の策定や設計を行うとともに、評価手法を構築する。

〔2〕データの保護と流通の自動化技術

データの保護と流通の自動化技術を開発するとともに、開発したインターフェース仕様等の標準化に着手する。

〔3〕経路特性保証型のクラウドネットワーク技術

経路特性保証型のクラウド間接続を実現する技術を開発するとともに、開発したインターフェース仕様等の標準化に着手する。

【最終目標】　2028 年度まで

〔1〕強固な鍵管理によるデータセキュリティ技術

利用者が自律的に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 の技術開発を行うとともに、2026 年度までに開発された鍵管理ソフトウェア技術を用いて構築されたクラウド基盤に、開発した HSM を組み込んでプロトタイプ実証する。

なお、これら〔1〕から〔3〕の技術開発の実施に当たっては、相互の開発テーマとも整合を図りつつ、一体性をもって取り組む。

エ．その他

クラウドサービスに係る技術進展が急速に変化していることを考慮し、国内外の技術開発動向や各国の政府系クラウドの導入状況等について情報収集・調査研究を並行して実施し、その結果は、必要に応じ、各研究開発課題の見直し等に活用されることとする。

研究開発項目②「半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立」

ア．研究開発の必要性

ソフトウェアレベルでホワイトボックスなクラウドを構築できたとしても、ハードウェアにおいてもホワイトボックス化が必要となる。例えば、クラウドに用いられる半導体・電子機器等のハードウェアについて、サプライチェーンの複雑化に伴い、粗悪品や偽造品が混入する危険性が生じているため、不正品を排除するための要素検証技術の特定と技術開発を実施することが必要である。

イ．具体的研究内容

半導体・電子機器のライフサイクルは、〔１〕半導体設計、〔２〕半導体製造、〔３〕ソフトウェア印加、〔４〕電子機器設計・製造・運用（廃棄・リユースを含む）の４つのフェーズ（段階）に大別できる。半導体・電子機器への不正機能や不正部品の混入を防ぎ信頼のおける半導体・電子機器のサプライチェーンを築くためには、これらの４つのフェーズのすべてにおいて必要な技術を開発し適用することが求められる。フェーズ毎にわが国において最低限強化すべき技術について研究開発を実施する。

〔１〕半導体設計フェーズにおける検証

半導体のチップは複雑なシステムであり、通常、半導体設計者は自らが一から開発した回路（設計 IP）に加えて外部から調達した回路（設計 IP）を活用してチップ全体の設計を行う。また、最先端の攻撃に対抗する技術とその評価を踏まえ、セキュリティ上の要求をチップ設計に課す。したがって、不正機能の混入を防ぐためには、〔１－１〕設計 IP の検証、〔１－２〕チップ設計の検証、〔１－３〕チップ設計に組込む最先端攻撃対抗技術の検証、〔１－４〕セキュリティ仕様への適合性検証を行うことが必須である。

〔１－１〕半導体 IP 検証

半導体設計者が、調達を予定する第三者設計 IP に対して必要十分な機能要求の仕様を所定の形式言語で記述して示し、第三者から購入する半導体設計 IP に当該仕様外の機能が混入されていないかを検証するための技術の開発を行う。

〔１－２〕チップ設計検証

デジタル・アナログ・メモリなどの多様な機能を搭載する大規模な半導体チップに対して、要求外の機能が混入されていないことを、半導体開発に利用される半導体設計ツールを用いて計算機上で検証する技術を確立する。

〔１－３〕最先端攻撃・攻撃対抗技術

半導体に対する最先端の論理攻撃、物理攻撃、サイドチャネル攻撃、エミッション攻撃等に対する耐タンパー性検証技術を開発し、前記攻撃に対抗する半導体実装技術を開発評価する。

〔１－４〕セキュリティ仕様への適合性検証

半導体チップに必要不可欠である最低限のセキュリティ機能について、セキュリティ要求仕様を策定し、当該仕様を満たすことを検証するための脆弱性検証技術を開発する。

〔２〕半導体製造フェーズにおける検証

半導体製造のすべての工程にわたって設計データが適切に管理されることが必要である。また、製造された半導体チップ等の機能が仕様どおりか否かを検査できることが必要である。

〔２－１〕半導体設計データ管理

半導体製造工程における設計データの改竄を排除するための品質管理技術を確立する。

〔２－２〕半導体解析による検証

半導体のディレイヤリング（パッケージ開封、研磨等）と高分解能観測により設計データを抽出する解析技術を確立し、要求外の機能の混入あるいは設計データの改竄が無いことを確認する手法を構築する。

〔３〕ソフトウェア印加フェーズにおける検証

半導体・電子機器に外部からソフトウェアを印加するフェーズにおける検証技術を開発する。

〔３－１〕ソフトウェア組込み段階でのセキュリティ要求仕様と検証技術

セキュアにソフトウェアを印加するために必要なセキュリティ機能について、セキュアにソフトウェアを印加するための要求仕様を策定し、当該仕様が満たされていることを検証するための脆弱性検証技術を開発する。

〔4〕電子機器設計・製造・運用フェーズにおける検証

電子機器の設計・製造・運用（廃棄・リユースを含む）に係るフェーズにおいては、不正部品混入を検知できること、また、半導体・電子機器の模倣品・非正規品を検知できるようにする必要がある。

〔4－1〕不正部品混入検知

半導体が制御する電子機器の使用フェーズにおいて、不正な部品等が混入していることを検知する技術、当該の検知技術を正常に実装していることを検証する技術を開発する。

〔4－2〕個体 ID 管理

半導体・電子機器個体に ID を付与し、市場流通後に半導体・電子機器から ID を取得してデータ基盤（クラウド）に参照することにより、半導体・電子機器個体の属性（真正性を含む）を検証できる技術を開発する。

ウ．達成目標

【中間目標】2025 年度まで

〔1〕半導体設計フェーズにおける検証

〔1－1〕半導体設計 IP 検証

・ 用いる形式言語の統一や、モデル化された要求仕様と第三者設計 IP 間における形式的検証手法の開発、代表的ないくつかの第三者 IP に対する要求仕様の策定とモデル化、形式検証ツールの開発、形式検証実験による不要な機能の定義を行う。

〔1－2〕チップ設計検証

・ 多様な半導体機能が搭載されている大規模なチップについて、設計データに要求外の機能が混入していないことを、一般性の高い半導体設計ツールを用いて計算機上で検証する手法を構築する。

・ フルチップの機能を網羅的に検証するため、チップのデジタル機能について形式的/論理的及び物理的な検証手法、またチップのアナログ機能及びメモリ機能について回路レベル及び物理的な検証手法を構築する。

〔１－３〕最先端攻撃・攻撃対抗技術

・ 論理攻撃、物理攻撃、サイドチャネル攻撃、エミッション攻撃等に関し、評価法が確立していない最先端の具体的な攻撃について攻撃の有効性を計測する手順等を構築する。

〔１－４〕セキュリティ仕様への適合性検証

・ 組込み電子機器向け半導体チップへの必要最小限のセキュリティ要求仕様を構築し、当該要求の評価手法を開発する。

〔2〕半導体製造フェーズにおける検証

〔２－１〕半導体設計データ管理

・ 半導体製造工程において設計データの改竄を排除する品質管理技術を構築する。

〔２－２〕半導体解析による検証

・ 半導体チップのパッケージング開封、半導体チップの表面研磨、集束イオンビームによる研磨、電子ビームやＸ線による立体撮像、等の半導体・電子機器の解析に必要な基盤技術を構築する。また、当該技術により設計データを抽出するとともに、要求外の機能の混入あるいは設計データの改竄が無いことを確認する手法を構築する。
・ 半導体・電子機器事業者より提供される実製品について、要求外の機能の混入あるいは設計データの改竄が無いことを確認し、事例集等を構築する。

〔3〕ソフトウェア印加フェーズにおける検証

〔３－１〕ソフトウェア組込み段階でのセキュリティ要求仕様と検証技術

・ ソフトウェア印加に係るセキュリティ要求仕様を策定し、当該仕様が実現されていることを確認する評価手法を開発する。

〔4〕電子機器設計・製造・運用フェーズにおける検証

〔４－１〕不正部品混入検知

・ 半導体が制御する電子機器の使用フェーズにおいて不正な部品等が混入していることを検知する技術を確立する。
・ 事前に設計工程や製造工程を検証した事業者による半導体・電子機器について、その電気的及び電磁的な特性についてのゴールデンデータを確立する。
・ 電子機器の使用フェーズにおける特性と比較することにより、不正な改竄を検知する手法を開発する。
・ 半導体・電子機器に検知機能を搭載するためのチップに、セキュアな暗号モジュールを実装するなどのセキュアパッケージングの手法を開発する。

〔4 － 2〕個体 ID 管理
・ 半導体・電子機器の個体の人工物メトリクス等による ID を付与し、その ID と紐づけて当該半導体・電子機器個体に関する情報を記録したデータ基盤に照会できる技術を開発する。
・ 半導体・電子機器の属性の照会・検証においてはデータ主権と機密性保持の両立を図るために高機能暗号を活用した技術を開発する。

【最終目標】　2028 年度まで
検証技術の最適化と検証体制の構築

〔1〕半導体設計フェーズにおける検証
〔1 － 1〕半導体設計 IP 検証
・ 検証に用いる形式言語と形式検証手法の標準化を行う。
・ 第三者設計 IP に対する、形式言語で記述されモデル化された機能要求仕様例について、半導体・電子機器設計者への提供を行うことも念頭に、半導体・電子機器設計者がセキュリティ検証を行うための形式検証ツール等を開発するとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔1 － 2〕チップ設計検証
・ 多様な半導体機能が搭載されている大規模なチップの開発工程において、設計データに要求外の機能が混入していないこと検証する手法が適切に導入・運用されていることを半導体事業者が宣言する方法及び第三者が確認する方法について標準化を行うとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔１－３〕最先端攻撃・攻撃対抗技術

・ 論理攻撃、物理攻撃、サイドチャネル攻撃、エミッション攻撃等に関し、評価法が確立していない最先端の具体的な攻撃について攻撃の有効性を計測する評価体系や攻撃に対抗する半導体実装技術等を構築するとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔１－４〕セキュリティ仕様への適合性検証

・ 組込み電子機器向け半導体チップへの必要最小限のセキュリティ要求仕様の認証を取得し、評価手法の標準化を行うとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔2〕半導体製造フェーズにおける検証

〔２－１〕半導体設計データ管理

・ 設計データに要求外の機能が混入されていないことを検証済みの設計データと半導体製造工程に用いられるマスクデータの等価性を計算機上で検証する手法を構築するほか、マスクの作製および半導体製造の各工程において改竄を排除する管理手法を構築するとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔２－２〕半導体解析による検証

・ 半導体・電子機器の微細化・大規模集積化・大面積化に対応するため最先端の解析装置を用いた解析手法を構築するとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔3〕ソフトウェア印加フェーズにおける検証

〔３－１〕ソフトウェア組込み段階でのセキュリティ要求仕様と検証技術

・ セキュリティ要求仕様の認証を取得し、評価手法の標準化を行うとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔4〕電子機器設計・製造・運用フェーズにおける検証

〔４－１〕不正部品混入検知

・ 半導体・電子機器の電気的及び電磁的な特性を記録・比較して不正な改竄を検知する機能を具備する検知チップを開発するほか、セキュリティ向け暗号

コアのサイドチャネル漏洩を電気的および電磁的な特性量とし、その場で計測・記録・評価する仕組みについて、半導体集積回路コアの機能・仕様を構築し、セキュアパッケージングによる半導体・電子機器のモデルシステムを構築するとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。

〔4 － 2〕個体 ID 管理

・ 半導体・電子機器の個体における人工物メトリクス等による ID 付与の方法や照会の手順の標準化を行うとともに、運用の方向性を示すことを目的としたパイロット実証を実施する。
・ ID 付与サービスおよび照会サービスを運用するために必要なシステムを開発し、パイロット実証を実施する。

2．実施方法、実施期間、評価、社会実装に向けた取組

（1）事業の実施・体制

本事業は、内閣官房、内閣府、文部科学省、経済産業省を含む関係府省が設置したプログラム会議が定める「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき事業を実施する。

研究推進法人（Funding Agency: FA）は、国から示された研究開発ビジョン及び研究開発構想に基づき、公募により研究開発課題を採択するとともに、その進捗管理・評価等の責務を担う。本事業の FA は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）である。

研究開発課題の実施責任者（以下「研究代表者」という。）の所属する機関は、国内に研究開発拠点を有し、日本の法律に基づく法人格を有している機関とする（以下「研究代表機関」という）。また、研究代表者及び主たる研究分担者は日本の居住者であることとする。（ここで言う居住者とは外為法の居住者（特定類型該当者を除く）であること。）

本事業の公募では、研究開発項目①〔1〕、〔2〕、〔3〕及び②はそれぞれ別に事業を実施するものとする。また、〔1〕の鍵管理ソフトウェア技術と HSM の技術開発に関する事項についても別に事業を実施するものとする。

なお、１（３）①エに掲げる情報収集・調査研究については、NEDO が PO と相談の上、別途実施するものとする。

（２）事業の実施期間

本研究開発構想に基づく、本事業は、2028 年度にかけての 5 年間（ただし、研究開発項目①〔１〕の鍵管理ソフトウェア技術、〔２〕及び〔３〕の技術開発は、2026 年度までの 3 年間）とする。また、研究開発項目①〔１〕の HSM の技術開発に関する事項および研究開発項目②については、ステージゲート方式を採用し、以下のスケジュールで実施するものとする。

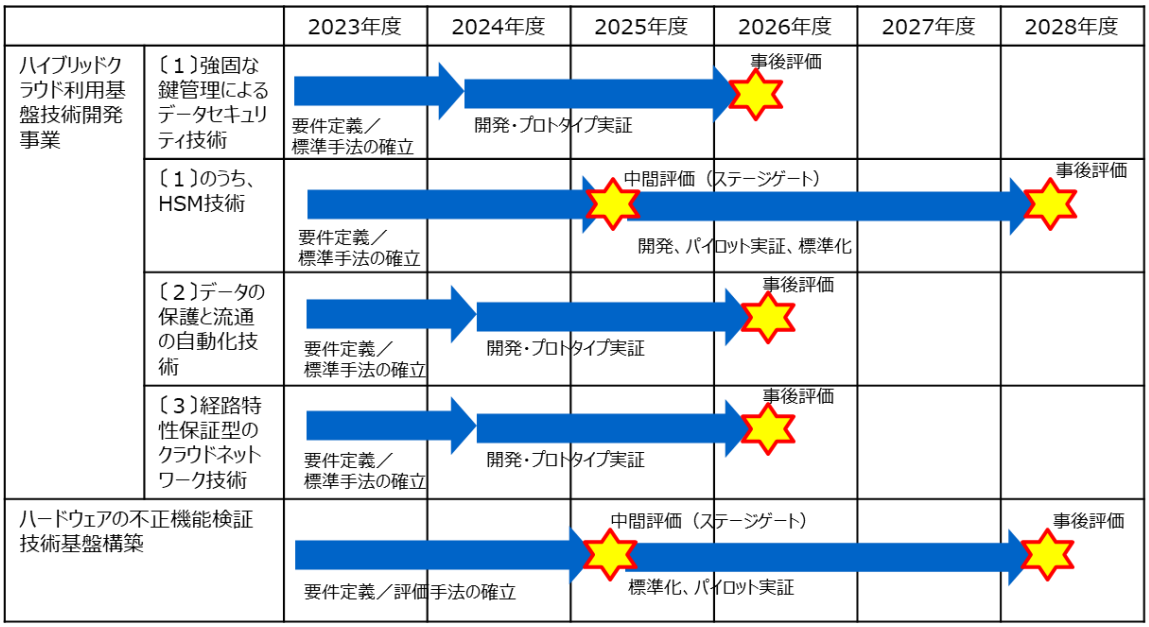

図４　研究開発のスケジュール

（３）評価に関する事項

本事業は、「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき、評価を実施する。研究代表者は自己評価を毎年実施し、PO に報告する。

NEDO は外部評価として、研究開発項目①について、〔１〕の鍵管理ソフトウェア技術、〔２〕及び〔３〕については事後評価を 2026 年度（当該テーマの事業終了年度）に、〔１〕の HSM については、中間評価を 2025 年度（事業開始から 3 年目）、事後評価を 2028 年度（事業終了年度）に実施し、事業の進捗等に応じて評価時期を早める場合は、PO 及び所管省庁と連携して、あらかじめ適切な実施時期を定める。

研究開発項目②について、評価の時期は中間評価を 2025 年度（事業開始から 3 年目)、事後評価を 2028 年度（事業終了年度）に実施することし、事業の進捗等に応じて評価時期を早める場合は、PO 及び所管省庁と連携して、あらかじめ適切な実施時期を定める。

（4）社会実装に向けた取組

本事業は、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 4 3 号）に基づく指定基金協議会を設置した上で推進していく。これにより、本事業によって生み出される研究成果等を活用し、民生及び公的な利用を促進するとともに社会実装につなげていくことを目指し、その実現に向け、潜在的な社会実装の担い手として想定される関係行政機関や民間企業等による伴走支援を可能とするとともに、参加者間で機微な情報も含む有用な情報の交換や協議を安心かつ円滑に行うことのできるパートナーシップを確立していく。

具体的には、本事業により開発を行うハイブリッドクラウド利用基盤技術は、政府や重要インフラ事業者によるデータ利活用と安心安全を両立したクラウド利用に資することが想定される。このため、このような利活用を行う場合の将来的に想定される具体的なユースケースやビジネスモデル、その実現のために必要な制度・標準・機能等や普及の在り方、求められるセキュリティの強度、世界の市場動向等の情報を共有しつつ研究開発を進めることは、研究開発成果を将来の社会実装に円滑につなげていく上で、大きな意義がある。

本事業に係る協議会については、研究開発課題の採択後に、関係行政機関、PO、研究代表者等の協議会への参画者における十分な相談を行いつつ、運営していく。なお、協議会の詳細は別に示す。

（5）予算

本事業の予算は、研究開発項目①については 51 億円を超えない範囲とし、研究開発項目②については 34 億円を超えない範囲とする。各研究開発項目、フェーズ毎の配分については、必要に応じて、経済産業省からの指導に基づき目安を示す。これを変更する場合も同様とする。

（６）経済産業省の担当課室

本事業の運営に係る経済産業省の担当課室は、研究開発項目①については商務情報政策局ソフトウェア・情報サービス戦略室、研究開発項目②についてはサイバーセキュリティ課とする。

３．その他重要事項

（１）研究開発成果の取扱い

① 共通基盤技術の形成に資する成果の普及

研究開発課題実施者は、研究成果を広範に普及するよう努めるものとする。経済産業省及び NEDO は、経済安全保障の観点を留意しつつ、研究開発課題実施者による研究成果の広範な普及を促進する。

経済安全保障の観点から、経済産業省は必要に応じて NEDO に対して助言を行い、NEDO は本助言を踏まえて、成果の普及について検討することとする。

② 標準化施策等との連携

研究開発実施者は、安全性検証手法等に関する研究開発成果の着実な実用化のため、本研究開発の終了後に実施すべき取組のあり方や検証・認証機関の構築及びビジネスモデルについて立案する。また、経済産業省、NEDO 及び研究開発課題実施者は、安全性基準等の国際標準化を戦略的に推進する仕組みを構築する。

③ 知的財産権の帰属、管理等の取扱い

研究開発成果を民生利用のみならず公的利用につなげていくことを指向し、社会実装や市場の誘導につなげていく視点を重視するという本プログラムの趣旨に則り、研究代表機関、研究代表者は、PO 及び研究分担者との協議の上、知的財産権の利活用方針を定めることとする。その際には、研究開発途中及び終了後を含め、知的財産権の利活用を円滑に進めることができるように努めることとする。

なお、研究開発成果の利活用にあたりその成果にバックグラウンド知的財産権が含まれる場合には、その利活用についても同様に努めること。

（２）「研究開発構想」の見直し

経済産業省は、NEDO、PO 及び関連省庁と連携して、当該研究開発の進捗状況及びその評価結果、社会・経済的状況、国内外の研究開発動向、政策動向、研究開発費の確保状況等、事業内外の情勢変化を総合的に勘案し、必要に応じて、達成目標、実施期間等、本研究開発構想の見直しを行う。

（３）研究開発の対象経費

「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき、運用する。大学・研究開発法人等以外に関する間接経費の額の設定については、事業の性質に応じて経済産業省の担当課室から別に示す場合を除き、業務委託契約標準契約書に基づくものとする。

４．研究開発構想の改定履歴

（１）令和４年１２月、制定。
（２）令和５年３月、改定。