ハイブリッドクラウド利用基盤技術の開発

（51億円を超えない範囲／5年）

背景

- クラウドサービスの普及やサプライチェーンの複雑化等に伴い、サイバー空間内やサイバーとフィジカルの垣根を越えた主体間の「相互連関・連鎖性」が一層深化。さらに、産業分野でのIoT機器の利用拡大や、AI技術の様々なシステムへの活用などにより、**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、より広範に、多様な主体・場面に及ぶおそれ**。
- こうした中、サイバーセキュリティや機器の信頼性を確保しつつ、クラウドサービスの活用を進めていくため、**政府情報システム**の分野においては、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促進**がうたわれているところ。
- 各主体が構築する情報システムにおいて、利便性の高いパブリッククラウド利用と、我が国における自律性の確保の観点等も念頭にしたプライベートクラウド利用、オンプレミス・システム利用という、**セキュリティポリシーの異なる領域を、必要に応じてデータを行き来させて処理や利活用を可能とするような、データ中心のセキュリティを確保**していくことが重要。

想定される利用ニーズ

- 官民において、クラウドサービスの利用が急速に拡大しており、今後は、組織の基幹システムや社会インフラなどの領域にも拡大することが見込まれている。こうしたクラウドサービスの利用に当たっては、**利便性が高く、新しい技術の導入も早い、主に海外で開発されるクラウドを積極的に利用**していく一方で、**機密性の面など高い信頼性が求められるデータを扱う場合には、自律性を確保したクラウドを利用**するニーズが存在している。
- こうした様々なニーズをすべて満たす１つのクラウドサービスは存在しない中、**本事業で開発する技術は、異なるセキュリティポリシーの複数のクラウドサービスを利用していくための重要な技術**。
- この技術により、迅速なデータ利活用と安全・安心を両立させたデータドリブン社会の実現に貢献していく。

研究開発の内容※

※　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、研究開発課題の見直し等に活用される予定

①強固な鍵管理によるデータセキュリティ技術

- データ保存時の暗号化とその鍵管理の厳格化は、データのライフサイクル全体を通じた保護の手段として期待される一方、暗号鍵管理機能のブラックボックス化など、課題が多い。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とともに、本技術を用いて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。更に利用者が自律的に鍵管理を行うためには、鍵管理用のHSMも重要。現状においては、中身がブラックボックス化されている等の課題が存在するため、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。

②データの保護と流通の自動化技術

- 複数クラウド間でのデータ連携においては、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することが課題。そのため、データの重要度やアクセス制御情報に基づく処理の最適化、漏洩や改ざんの防止、匿名化加工、証跡管理等、データの保護と流通の自動化技術を開発する。

③経路特性保証型のクラウドネットワーク技術

- 高機密なデータや暗号化に用いる鍵データなどの通信では、通信路の暗号化に加え、使用される経路の独立性など通信路が備える経路特性の保証も必要。そのため、経路特性の指定・制御を可能にし自動化する技術、及び経路特性変更等の検出・防止を可能にする技術を開発する。

想定スケジュール

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

（34億円を超えない範囲／5年）

背景

- サイバー空間を構成する電子機器・システムのサプライチェーンの複雑化やグローバル化、OSS (Open Source Software) の普及など、サイバー分野におけるサプライチェーンを取り巻く環境は一層複雑化し、**サプライチェーンの過程で不正機能等が埋め込まれるリスクなど、サプライチェーン・リスクが顕在化**している。
- 中でも半導体等のハードウェアについては、世界半導体会議が、2018年5月に不正な半導体に関する白書を発行し、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いるなど、**半導体等のハードウェアの信頼性確保に課題が生じている状態**。
- 半導体等のハードウェアの信頼性が損なわれれば、半導体等のハードウェアを基盤とする**クラウド等のデジタルインフラやデジタル産業の信頼性が損なわれることにも繋がるおそれ**がある。
- 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ことにより、**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。

想定される利用ニーズ

- IoT機器は全世界で2021年の約290億台から2024年には約400億台に増加するとの予測があり、現に**IoT機器を狙った攻撃は2020年には2017年と比較し約3.3倍**になっている。**本技術はこうしたIoT機器に用いられる半導体等のハードウェアの信頼性確保に資する**。さらに、特に**重要インフラをはじめとした経済安全保障上重要な機器・システムに用いられる半導体等のハードウェア検証**に用いられることも期待される。
- また、政府が用いるクラウド等、政府調達品に用いられる半導体等のハードウェアの検証に用いられることも期待される。
- このように、安全保障上重要な機器・システムの信頼性が向上することで、サイバーセキュリティに強靭な社会構造となることに寄与する。

研究開発の内容

- クラウドを含む情報システムに用いられる半導体等のハードウェアにおける不正機能排除が可能となるための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**

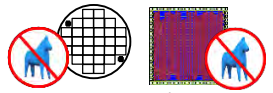
  等の検証について、必要な要素技術の特定と技術開発を行う。
- また、半導体の設計から組込みに至るまでの**セキュリティ要求仕様の定義や標準化**、検証のパイロット実証を行うことでハードウェアセキュリティ検証基盤を確立する。

フェーズ1：半導体設計

半導体回路資産
（ソフトIP、ハードIP、半導体チップ）

半導体IP・チップ設計検証技術、最先端攻撃・攻撃対抗技術、セキュリティ要求仕様への適合性検証

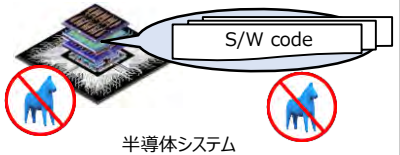
フェーズ2：半導体製造



半導体チップ
（ウェハ、チップレット）

半導体の製造フェーズにおけるデータ管理・検証技術、半導体解析による検証技術

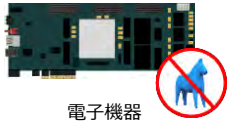
フェーズ3：アプリケーション・ソフトの印加



半導体システム
（パッケージング、ファームウェア）

半導体へのソフトウェア組込みフェーズにおけるセキュリティ要求仕様と検証技術

フェーズ4：組込み機器の設計・製造・流通・運用・廃棄（再利用を含む）



電子機器
（システム実装、プリント基板）

半導体・電子機器への不正部品混入検知技術、個体ID管理技術

想定スケジュール