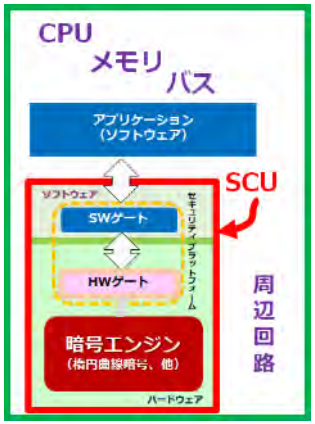
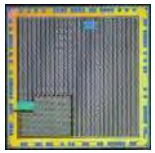
（3） 研究開発内容 （再掲）

IoTサプライチェーンの**信頼の基点**となる「軽く、速く、強い」セキュア暗号モジュールを開発

SIP1期の成果を継承
世界最小、世界最速の
楕円曲線暗号実装

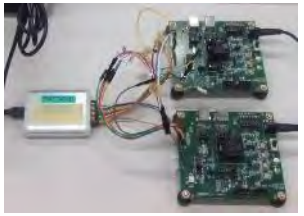


「軽く、速く、強い」セキュア暗号モジュール=SCUを搭載した半導体チップの試作開発



SC02チップ

SC02v.2チップ

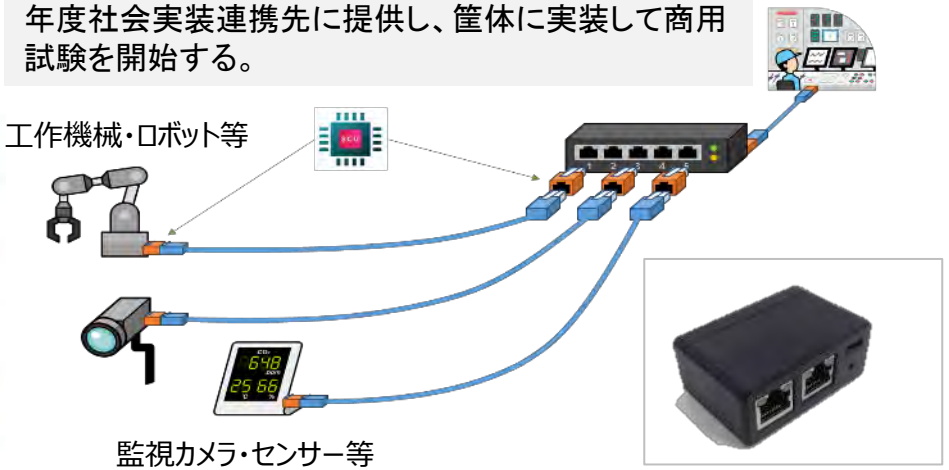


チップ評価完了

社会実装に向けて

レガシーシステムのIF部にアダプターを実装するだけで、システムのセキュリティを担保するコネクターシステムを開発

ネットワークケーブルの端末に**超小型のSCU機能を搭載**したチップを実装することで、システムのセキュリティを担保する**「セキュリティアダプター」**を開発。23年度社会実装連携先に提供し、筐体に実装して商用試験を開始する。



並列型セキュリティアダプターのイメージ

（4） 工程表

(A1) 信頼創出暗号モジュール

出口戦略・社会実装に向けて

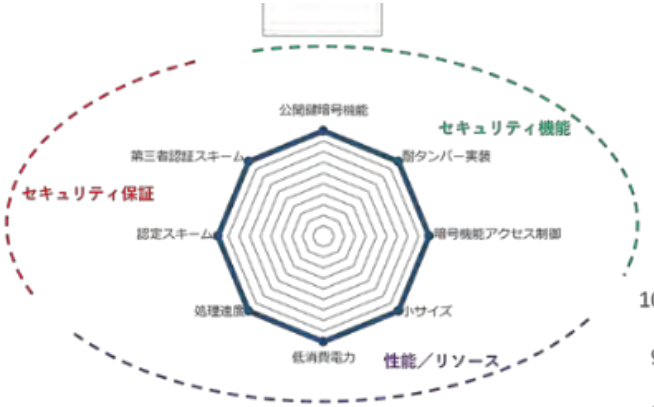
「IoT社会に対応したサイバー・フィジカル・セキュリティ」工程表

(A1) IoTサプライチェーンの信頼の創出技術

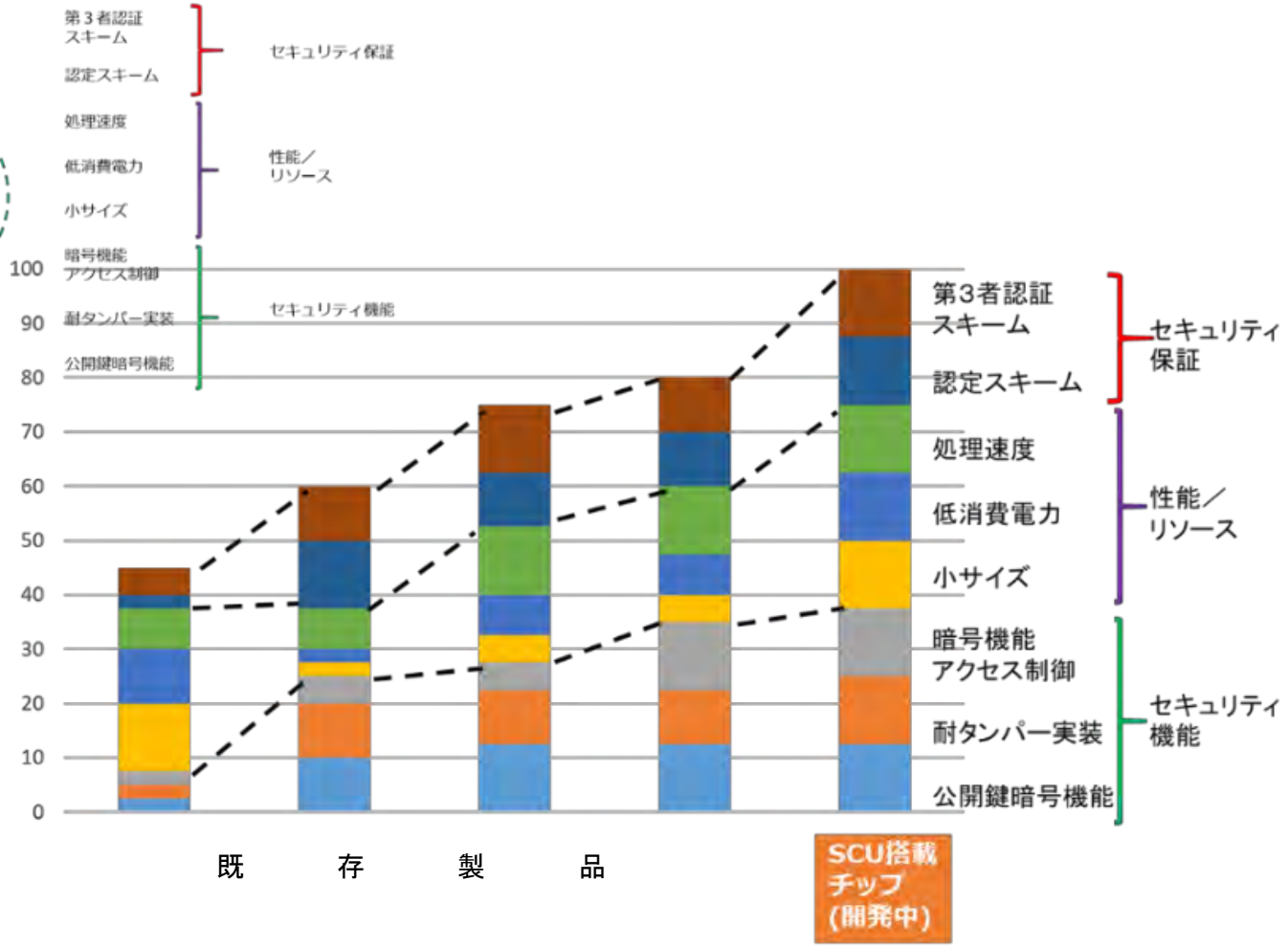
研究開発項目	2018年度実績	2019年度実績	2020年度実績	2021年度計画	2022年度計画	出口戦略	製品化
(A)「信頼の創出・証明」技術の研究開発							
(A1) IoTサプライチェーンの信頼の創出技術基盤の研究開発							
①IoT機器等に組込み可能な暗号モジュールをベースに、それを信頼の基点として活用するための基盤技術	• バランス型SCU(非ワンチップ)の一般組込み機器(監視カメラ)での実証実験 • ワンチップ化、鍵運用等検討 TRL2 → TRL4	• SCU搭載ワンチップ「α版」(SC01)完成 • コネクターシステム検討 TRL6	• SCU搭載ワンチップ「β版」(SC02)完成 • 工場・インフラ等向け「SCU搭載コネクターシステム」(鍵管理運用モデルを含む)の完成	• ECSEC組合組織変更 • 社会実装先開拓 • 事業資金調達 TRL7		● ECSEC組合の後継会社が、 ✓ 知財運用、 ✓ SCU搭載チップおよび活用システムの開発・販売、 ✓ 技術の標準化およびセキュリティ保証スキームの構築・運用 等、社会実装促進のための責務を担い、SCUを信頼の基点とする安全・安心なIoTシステム・サービスおよびサプライチェーンの確立を実現する。 ● SIP課題間連携	製品・サービス開発(2020～) 製品化・サービス化(2022～)
② 信頼の基点に対するサイバー攻撃とフィジカル攻撃の双方に対処するための技術等	• 耐タンパー技術／ボードレベルHT検知技術／HT形式検証技術の技術実証 TRL2 → TRL4			• 実用化開発(比類なき耐タンパー性の実現) TRL5			
③信頼の基点に対するセキュリティ保証スキームの整備／構築	• セキュリティ保証スキーム先例調査 TRL2	• SCU搭載組込み製品用チップの脆弱性DB公開 • SCU搭載チップのセキュリティ要求仕様策定 TRL4	• TCGへの加入 • 「SCUコンソーシアム」組成 • 技術標準化 • SCU認定方式の提案 • SCU組込み製品のセキュリティ保証スキームの具体化 TRL6				
実証実験等 (A,B,Cの各テーマ毎、およびテーマを横断して実施)	• 一般組込み機器(監視カメラ)での実証実験			• 製造・流通・ビル分野等での実証実験 • 関連機関と一体での実証実験			
	・普及活動 ・提言活動 ・海外動向 との摺合わせ						
	• 府省庁による制度設計						

(5)グローバルベンチマーク ① 国際競争力

グローバルベンチマーク8項目を設定。
いずれの項目においても、プロジェクト終了時に、競争品に対して優位を確立することを目標とする。
SCU搭載チップは、とくにセンサノード等の超小型末端機器への活用において優位性がある。



IoT末端機器向けセキュリティチップの要件



次の項目は、プロジェクト終了後も継続。

【第3者認証スキーム】

(評価・)認証母体、技術WGの体制確立と(SCU搭載)実認証製品を普及するためのエコシステム構築

【認定スキーム】

SCU搭載製品の開発と評価の効率化のためのツール開発と評価認定手順に関する文書の保守

（6） ② 研究成果で期待される波及効果

(A1) 信頼創出暗号モジュール

開発されたSCU搭載チップは極小のIoT機器に搭載可能であることから、あらゆるサプライチェーンの末端までセキュリティ機能を届けることが可能であり、セキュアなSociety5.0に必須の技術である。

この成果によりIoT末端機器分野におけるセキュリティ市場の創出・活性化にとどまらず、製品に関わる多くのステークホルダーへのセキュリティ意識の向上、セキュリティ確保によるIoTシステムの総コストの低減が見込まれる。

また、同時に開発した耐タンパー機能はSCU搭載チップに留まらず多くの集積回路に展開可能な技術であり、セキュリティ対策技術へ貢献し安全安心の社会を実現する。

＜新技術・市場の創出＞	
新製品・新機能への展開	公開鍵暗号を装備したIoT用極小組込機器が可能 高機能暗号実装にもチャレンジ
科学技術の進展や新技術の確立	裏面配線パッケージングによる新しいセキュリティ対策技術の確立
新たな市場創出の可能性	IoT末端機器分野におけるセキュリティ市場の創出
生産性向上への貢献	末端機器分野のセキュリティが確保されることによるIoTシステム総コストの低減
海外展開への可能性	末端機器用のセキュリティカーネルの市場は未形成で、IoTの普及とともに地球規模で有望な分野
＜社会貢献＞	
IoT社会の安全安心	末端のリソースに乏しい組込みデバイスに「軽く、速く、強い」「信頼の基点」を実装できるようになり、Society5.0におけるセキュリティの実現に大きく貢献した。
経済安全保障上の貢献	宇宙分野等新たな情報セキュリティが必要とされる分野への活用の道を拓いた。 我が国半導体産業の復興に不可欠のHWセキュリティ技術のコアを確立した。

（7）研究目標の達成状況・見込み　③ 達成度（1）

(A1) 信頼創出暗号モジュール

主な目標である、「SCU搭載チップSC01～SC02ver.2の開発」、「モデルシステムによる技術実証（監視カメラ、コネクターシステム等）の実施」をはじめとして、技術的目標は全て達成した。

研究開発項目		研究開発目標	達成予定時期	備考
1.1 社会実装につながるSCUアプリケーションモデルシステムの構築と実用化技術の実証	1.1.1　一般組込み機器用SCUアプリケーションモデルシステム	SCUを用いたアプリケーションシステムの技術実証	2021年度	監視カメラシステムにて技術実証完了。
	1.1.2　極小組込み機器用SCUアプリケーションモデルシステム	SCUを用いたアプリケーションシステムの技術実証	2022年度	SCU搭載チップSC01・SC02・SC02ver.2の開発・評価完了。 実用コネクターシステムの技術実証完了。
	1.1.3　高機能暗号のSCU搭載に関する検討	1.1.4、1.1.5のフィジビリティ検証	2020年度	高機能暗号のSCU搭載仕様案を策定。 1.1.5に移行。
	1.1.4　秘匿検索用SCUアプリケーションモデルシステム	SCUを用いたアプリケーションシステムの技術実証	選択集中により中止	2021年実施計画変更：研究対象から削除。
	1.1.5　集約署名用SCUアプリケーションモデルシステム	SCUを用いたアプリケーションシステムの技術実証	2022年度	追跡機能付き集約署名アルゴリズムをFPGA実装した試作品の開発・実証完了。
	1.1.6　IoT向け公開鍵暗号運用システム	SCUを用いたアプリケーションシステム運用のための社会基盤技術実証	2021年度	2021年度までにコネクターシステムへの実装を想定した鍵管理運用システムの開発を完了。
	1.1.7　IoT向け高機能暗号運用システム	SCUを用いたアプリケーションシステム運用のための社会基盤技術実証	2022年度	高機能暗号鍵管理システム開発完了。
2.1 セキュリティ対策技術研究	2.1.1　SCUへの脅威と対策	SCUのセキュリティ対策実装	2022年度	裏面配線対策技術を対象としたサイドチャネル、レーザーフォールト等の攻撃の実験・評価完了。
	2.1.2　SCUの国際標準化と事業化、知財運用	SCUの認定基準の公開	2022年度	3.1.3と連携し、標準化戦略を完成。 ECSEC組合の事業会社（株）SCUへの移行完了（2022年8月）。
2.2 ハードウェアトロージャン(HT)対策技術	2.2.1　ボード上のHT検知技術	トロージャンセンシング技術の実現	2022年度	技術実証用のチップ開発・デモシステム開発完了。
	2.2.2　LSI設計IPのHT形式検証技術	形式検証による対HT技術基礎理論の構築	2020年度	外部発表完了。
3.1 SCUのセキュリティ保証スキーム	3.1.1　組込製品用チップの脆弱性分析技術の集約	脆弱性リストの公開とメンテナンス体制の構築、維持	2021年度	脆弱性リスト最終版リリース。
	3.1.2　SCUアプリケーション分野別セキュリティ要求のまとめ	セキュリティ要求仕様公開	2021年度	SCU搭載組込機器用ワンチップのPPのISO/IEC15408認証取得。
	3.1.3　セキュリティ保証スキーム運用の技術的支援とSCU認定	セキュリティ保証スキーム運用 SCU認定スキーム運用	2022年度	セキュリティ保証スキーム、SCU認定スキームのための仕様設計完了。

（8）出口戦略　④ 達成度（2）

ア．社会実装に向けた具体的な計画

2022年8月、技術研究組合法　第7章第1節（組織変更）を適用しECSEC組合を改組、株式会社化。当該法人（株）SCUが責任を持って社会実装を推進する。

当初のもくろみでは、当該法人のビジネスは、研究成果知財のハンドリングが主であったが、その後の市場分析とフィジビリティスタディーの結果、「IPビジネス」、「SoCビジネス」、「システムインテグレーション・コンサルティングビジネス」を並行して行うこととした。

SCU搭載チップを普及させる企業グループを組織。
株式会社SCUが**ターンキービジネスの中核**となる。

IPビジネス
本研究開発の成果をIPとしてベンダー等に販売する事業

SoCビジネス
SCU搭載チップをグループで開発し、組込機器ベンダーに販売する事業

システムインテグレーション・コンサルティングビジネス
成果普及、社会実装を早めるために組込ベンダーとコネクターシステムを共同開発、これをユーザーに実装するためのサービス事業

（8）出口戦略　④ 達成度（2）

イ. 社会実装に向けた計画進捗状況

すでに、民間投資もふまえて社会実装に着手しているものが4件。

連携先	対象	技術実証の狙い	時期	状況
組込機器ベンダー ハイテクインター	コネクターシステム	コネクターシステムのキーデバイスであるセキュリティーアダプター（共同開発）の実証	2021年　SC01ボード 2022年5月　SC02ボード 2022年12月 SC02ver.2ボード試作開始	合意済み 実験開始
大手メーカ NDAにより社名秘匿	工場用ロボット	ロボット制御にコネクターシステムを実装、アクチュエーターのセキュリティを実証（データファイル形式の定まった署名検証）	2022年5月頃 SC02ボードによる実験開始 2022年12月頃 SC02ver.2による実験へ移行	実証実験中
CPSテーマA2 窓口 NTT（社会情報研究所）	真贋判定システム	A2真贋判定システムにSCU搭載チップを実装	2022年8月 SC02ボードを先方へ提供、A2側で接続仕様検討中	実証実験中
SIP2フィジカル空間デジタルデータ処理基盤 窓口 モバイルテクノ	工場オートメーションシステム（一般）	先方の工場内無線（秘密分散）通信システムと当方の有線コネクターシステムの連携による汎用的な工場制御セキュリティシステムの実証	2022年4月 SC01ボードにて接続成功 2022年10月 監視カメラシステムを用いた接続実験を完了	実証実験中

（8）出口戦略

⑤知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

＜知財戦略＞

本プロジェクトの成果をECSEC組合の後継会社（株）SCUがIPとして普及させる。
（株）SCUは、従来予定のIPビジネスだけではなく、いわゆるターンキービジネス（SCU搭載ワンチップの製品販売）も視野に入れる。2022年8月新会社発足。

＜国際標準化戦略＞

ISO/IEC15408に準拠した設計開発過程を踏むことにより、セキュリティ保証面からの国際標準化を図る。
SCUのセキュリティ保証スキーム構築を研究。ICSS-JC/SWG11（Low resource chip分科会）との連携。
同分科会をセキュリティ保証スキームの母体として活用することも検討中。

＜特許出願＞

8件（三菱電機（株）×4、（株）SCU（発明は神戸大学）×4）

(8)出口戦略

⑥ 成果の対外的発信

プレス/アウトリーチ活動など:7件
(SIP-CPSシンポジウム×4(2019-2022)、産総研Website、SCU技術発表会(2022/1)、SCU事業発表会(2022/11))

論文受理/学会採択、講演など:44件
(e.g.国際論文誌で発表:Tsutomu MATSUMOTO, Makoto IKEDA, Makoto NAGATA, Yasuyoshi UEMURA, "Secure Cryptographic Unit as Root-of-Trust for IoT Era," IEICE Transactions on Electronics, Vol. E104.C, No. 7. pp. 262-271, 2021.)

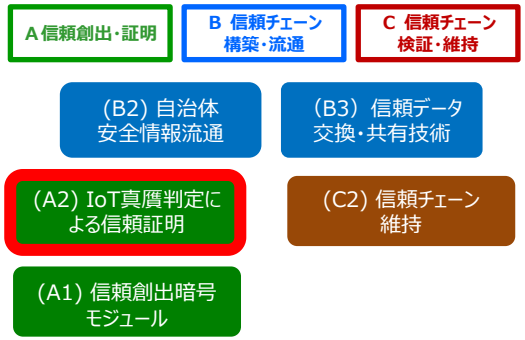
⑦ 国際的な取組・情報発信

ISO/IEC15408 (コモンクライテリアCC) に準拠した設計開発過程を踏むことにより、セキュリティ保証面からの国際標準化を図る。本研究開発においてはSCU搭載シングルチップマイクロコントローラのセキュリティ要求仕様(PP)を作成した。本PPは、日本においてCCに基づく「ITセキュリティ評価及び認証制度 (JISEC) 」を運営する独立行政法人情報処理推進機より、認証を取得している (JISEC-C0764)。この認証は、国際的承認アレンジメント (CCRA) 加盟国でも通用する。SCU搭載組込み機器向けマイコンが ISO/IEC 15408 に基づく認証を取得する際には、このPPが要求するセキュリティ仕様を満たすことを示せば良いこと、またそれにより取得した認証が国際的にも通用することから、本PPの認証取得は、今後の国内マイコンベンダーの国際市場競争力の確保の点においても大変意義のあるものである。

なお、2021年4月よりTCG(Trusted Computing Group)に加入し、TCGの一員として技術情報の収集を開始すると共に、現在TCG内部で検討中のIoT版TPM規格と、本研究成果SCUとの接点がないかを検討中。

また、2020年度より、Arm社の主導する、ARM-PCI規格を調査、その提供するAPIと本研究成果SCUのAPIとの共通化の可能性を検討中。

（A2）IoT機器等向け真贋判定による信頼の証明技術〔NTT, NEC　他〕



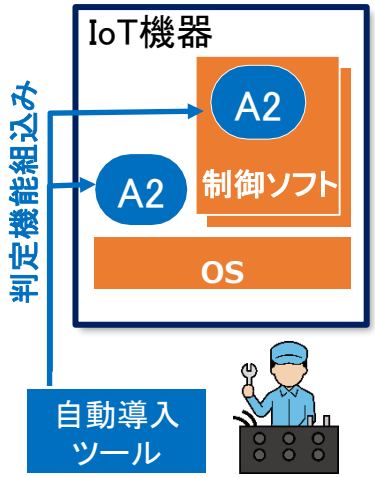
（1） 研究開発概要

Society 5.0 実現に向けて、従来技術では対応できないサイバー・フィジカルシステムを構成するIoT機器のライフサイクル全体にわたって、改造やすり替えといったサプライチェーンセキュリティリスクが懸念されていた。

当初の上記懸念が現実化し、各国政府も対策に動き始める中、本テーマにおける先行的な研究開発が功を奏し、この動向にいち早く対応した技術を創出することができている。

具体的には、上記対策において米国政府等を中心に活用が進むSBOM(Software Bill of Materials)フォーマットに対応した、① IoT機器のサプライチェーン全体及び大規模IoTシステムに対する真贋を判定する技術、及び② IoT機器において稼働中のソフトウェアに対しても精密に真贋を判定する技術を確立している。

機器内部に真贋判定技術を搭載



（2） 技術的目標

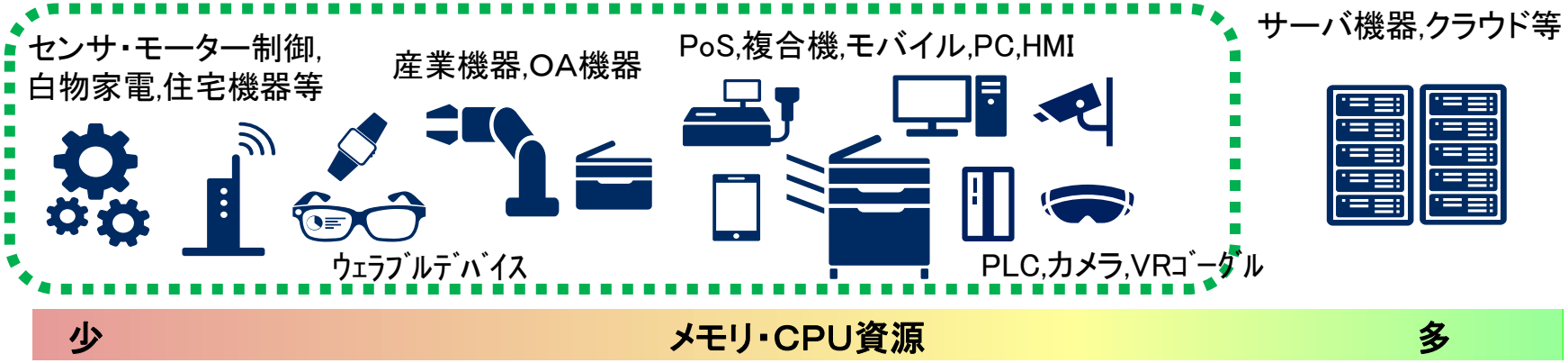
① 真贋判定技術は サプライチェーン上（多対多）での柔軟な開発活動を阻害することなく、高精度な構成保証が可能になるために、IoT機器の本来機能に影響を与えない軽量性（リソース使用率、判定効率）による常時監視を実現する。

② 稼働中の機器についても動作可能とするとともに、低機能機器（OSレス）への搭載、低い検査オーバヘッドを実現する。

（3） 研究開発内容

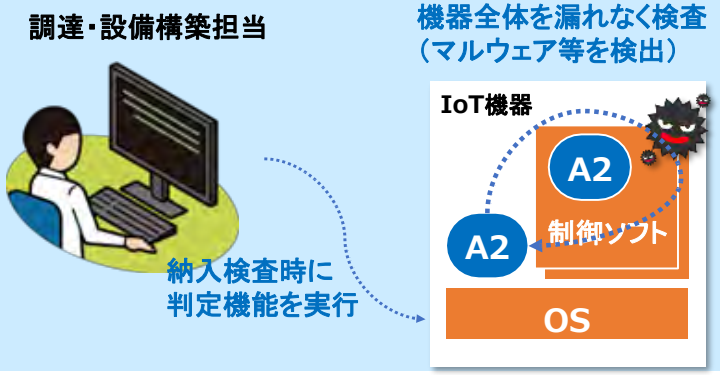
(A2) IoT真贋判定による信頼証明

ターゲットはメモリ・CPU資源の少ない「**中～低レベル機器**」であり、リソース制限等によって、従来は対策が困難であった多様なIoT機器の**構成を確認・証明**できる。



サプライチェーン上でIoT機器に不正な構成要素（マルウェア等）が混入する脅威、および運用中に遠隔制御や保守作業を介して汚染される脅威に対処できる

【効果①】
納入時に不正な構成要素を発見できる



【効果②】
本来動作に影響を与えず稼働中に判定できる