戦略的イノベーション創造プログラム（SIP）

【電子商取引安全技術研究組合
ルネサスエレクトロニクス株式会社】

2－2　IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

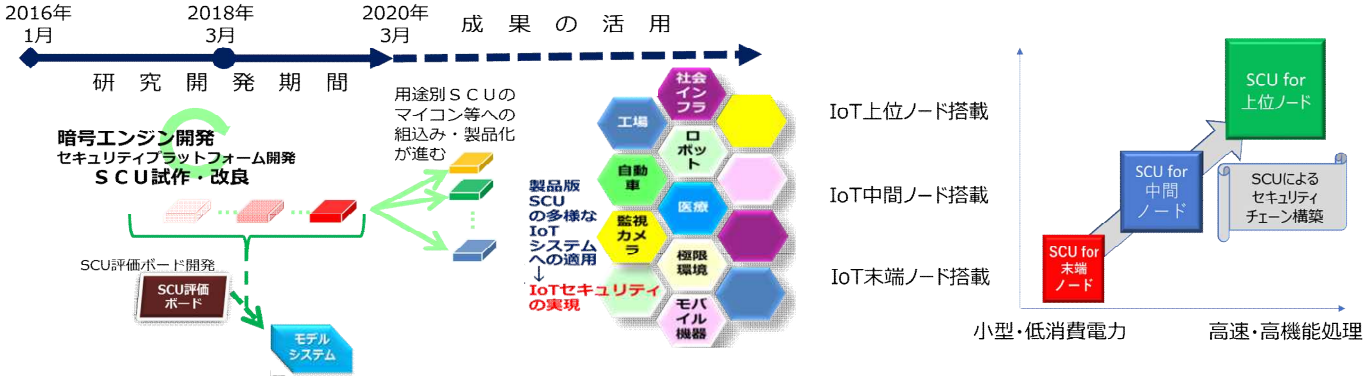
IoT向け対策技術

どこでも公開鍵暗号を！ Secure Cryptographic Unit

SCUのユーザメリットと普及に向けた方針

開発技術	ユーザメリット	普及に向けた方針
SCU	● すべての末端IoT機器に公開鍵暗号を耐タンパー性を確保して搭載可能 ● 末端ノードから中間ノード、上位サーバーまでスケーラブルな展開が容易 ● 既存のTPM製品等より、小型・低消費電力・高速化の点で有利。	● 認知度を高め、IoT市場での普及を加速するため、標準化モデル、ユースケースを研究 ● 先進ユーザ企業と連携し先導的な成功事例を蓄積 ● 多彩な分野／用途にアプリ展開。ガイド文書の充実。 →幅広い分野別ユースケースに対応したSCUモデル展開へ

研究成果による将来展望（イメージ）



SCUの普及イメージ（IoT用途別の広がりとIoTノード別の進化）

戦略的イノベーション創造プログラム（SIP）

【電子商取引安全技術研究組合
ルネサスエレクトロニクス株式会社】

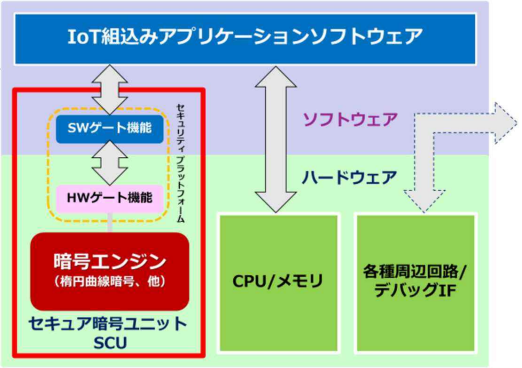
2－2　IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

IoT向け対策技術

どこでも公開鍵暗号を！ Secure Cryptographic Unit

セキュア暗号ユニット（SCU）

・SCUは、IoT機器をサイバー攻撃から守るICチップ内に組込む“軽い、速い、強い”モジュール。
・暗号エンジンとセキュリティプラットフォームから構成され、全ての繋がる機器に「最先端の公開鍵暗号機能」を内蔵させIoTのセキュリティを実現する。



セキュア暗号ユニット（SCU）の特長

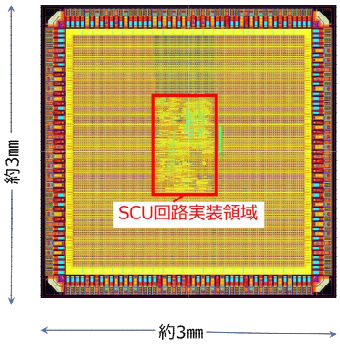
IoTシステムを構成する“末端ノード、中間ノード、上位ノードまでをスケーラブルに最先端の暗号技術・セキュリティ技術で守る。

1．IoT末端ノード向けに小型で超低電力の最先端の公開鍵暗号エンジンを搭載。
2．「信頼の起点」となる耐タンパー性の確保とライフサイクル管理の構築が可能。
3．ローエンドMCU (Micro Controller Unit) から高性能SOC (System On Chip)まで、スケーラブルに展開が可能。

ポイント1：「SCUプロトタイプチップ KM10 シリーズ」

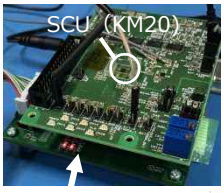
本研究では、プロトタイプチップを試作し、現実のIoTシステムにおけるSCUの応用を模したモデルシステムを開発している。

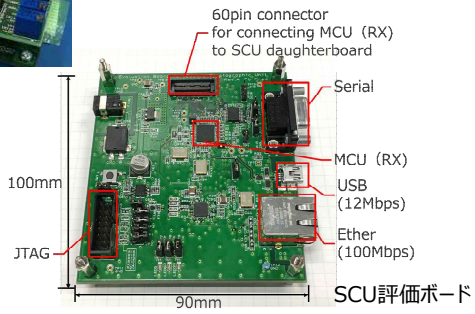
＜SCU“KM10シリーズ”の主な仕様＞
・暗号エンジン：ECC（楕円曲線暗号;256ビット素体), AES, SHA-256, ChaCha20-Poly1305, 物理乱数生成器
・セキュリティ制御：HWゲート、SWゲート



ポイント2：「SCU評価ボード」

SCU評価ボードは、SCUを搭載するIoT機器や応用システムの開発向けに提供される開発ツールで、SCUのセキュリティプラットフォームを利用してアプリ開発・評価を行うことが可能。





戦略的イノベーション創造プログラム（SIP）

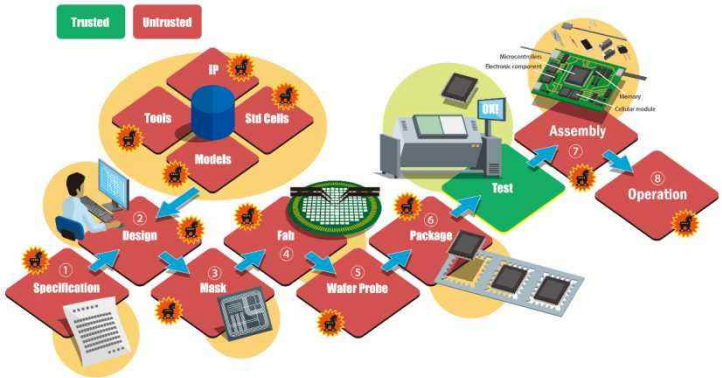
【電子商取引安全技術研究組合
ルネサスエレクトロニクス株式会社】

2－2 IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

IoT向け対策技術

ハードウェアトロージャンに対抗する技術の開発

ハードウェアトロージャン（HT）の脅威



信頼できないサプライチェーンにおいてICチップ、基板、接続線路などに意図的な電気的改変が行われる

安価に実装できるHTの出現により民生品にも脅威が拡大

攻撃タイミング・想定される攻撃・前提・コスト

	攻撃タイミング	想定される攻撃	攻撃の前提	攻撃コスト	攻撃者
システムLSIの設計製造工程	①要求仕様	ベンダによる悪意ある製品	サプライチェーンへの介入・ICへの物理アクセスによる攻撃の実行	コスト大	Bespoke, Professional
	②システムLSI設計	悪意ある設計者による設計			
	③マスク製造	製造過程におけるマスクの改ざん・すり替え			
	④チップ製造	下請けベンダの介入による設計改ざん			
	⑤チップ検査	下請けによる配線・回路改ざん			
	⑥パッケージ				
組込機器の製造工程	⑦制御部の組込	電子部品の挿入	機器への物理アクセスによる攻撃の実行	「コスト大」よりは大幅に少ないコスト	Bespoke, Professional, Hobbyist
	⑦機器の組み立て				
出荷後	⑧機器の運用	電子部品の挿入・マルウェアの書き込み・装置の挿入		上記に比べ少ないコスト	Bespoke, Professional, Hobbyist

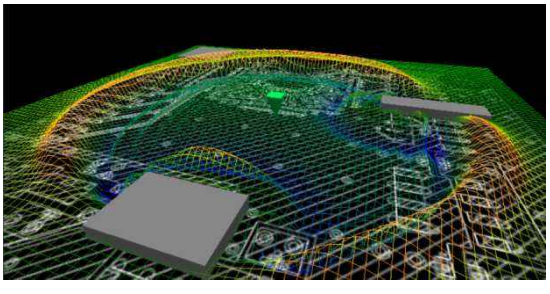
課題1： マイコンなどの制御部品にハードウェアトロイが仕掛けられないようにする仕組の構築（ 制御部品の設計製造工程におけるトロイの検出、発動の抑止）

課題2： マイコンなどの制御部品にはハードウェアトロイはないという前提で、安全な制御部品を利用してハードウェアトロイが仕掛けられないようにする仕組みの構築（ 組込機器の製造工程におけるトロイの検出、発動の抑止）

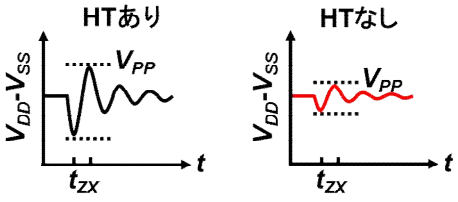
課題3： ライフサイクルにおいてトロイが発動した場合の対処法に関する検討

課題2の解決技術を展示

IC及びその周辺に仕掛けられたHTを検出する技術の開発

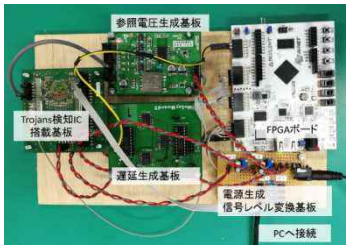


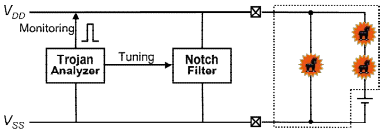
真正性が保証されているICから周囲IC及び電気素子をセンシング



センサーから発せられるインパルスを用いた回路応答からHTの有無を検出

HT検出試験環境





IoT向け対策技術

戦略的イノベーション創造プログラム（SIP）

【電子商取引安全技術研究組合、ルネサスエレクトロニクス株式会社】

2－2 IoTのセキュリティを実現する超低電力公開鍵暗号実装技術【研究開発全体像】

セキュリティプラットフォーム技術

ルネサスエレクトロニクス

セキュア暗号ユニット（SCU）のSWゲート/HWゲートの設計仕様開発と設計試作、SCU暗号エンジン部分への外部からのセキュアなアクセス制御を実現。

デジタル回路設計・暗号実装

横浜国立大学、東京大学、電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）の暗号エンジン部分の設計仕様開発とデジタル回路設計及び試作、楕円曲線暗号（ECDSA)の超効率的なハードウェア実装を通じて、「軽く、速い」公開鍵暗号エンジンを実現。

アナログ回路設計・構造

神戸大学、産業技術総合研究所、電子商取引安全技術研究組合

セキュア暗号ユニットを搭載するシステムLSI全体のアナログ実装技術の新規開発、2.5次元実装等を通じて、システムLSIの性能向上とセキュリティの双方を実現。

耐タンパー技術

東北大学、横浜国立大学、神戸大学、奈良先端科学技術大学院大学、電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）の耐タンパー性を確保する技術の開発と実装、評価。「強い」公開鍵暗号エンジンの実現。

HWトロージャン対抗技術

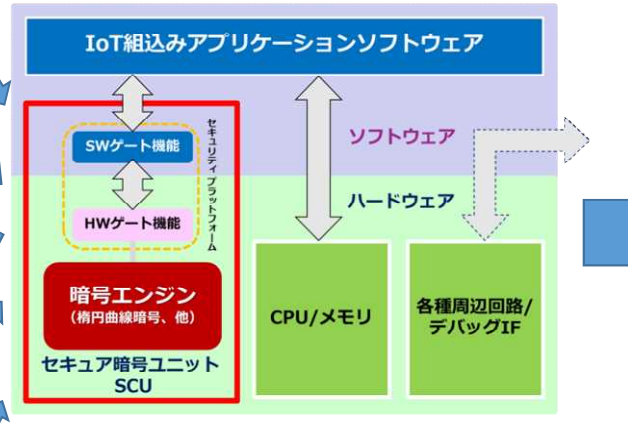
電気通信大学、奈良先端科学技術大学院大学、神戸大学、横浜国立大学、電子商取引安全技術研究組合

組込み機器へのHWトロージャン攻撃の事例整理と各製品レイヤーでの攻撃技術の分析、ポイントを絞った対抗技術の開発。

研究開発成果をセキュア暗号ユニット（SCU）として結実

各研究機関の共同研究の成果を結集して、システムLSIチップに搭載されるセキュア暗号ユニット（SCU）に集約。将来SCU部分をシステムLSIの設計IPとして、チップベンダに供給することを目指す。
（アナログ構造、耐タンパー技術、HWトロージャン対抗技術等はSCU以外の分野にも応用可能。）

セキュア暗号ユニットSCU内蔵マイクロコントローラの例

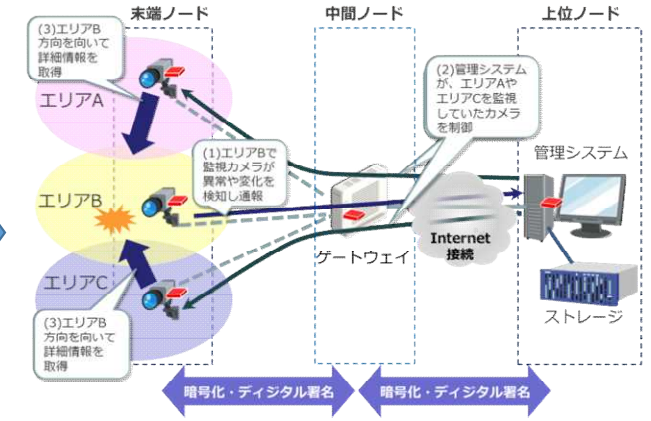


モデルシステムとして監視カメラシステムを構築

電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）を搭載したシステムLSIチップのIoTシステムへのアプリケーション実証例の一つとして監視カメラシステムを構築し、検証。但し、SCUの応用範囲は、広く産業用機器制御、交通・医療機器、ロボット等IoT全般。

セキュア暗号ユニット適用例：監視カメラシステム



社会実装に向けて

【導入分析】　セコム

自動車や医療機器のような、１つのシステムがマルチベンダの部品やモジュールによって構成され、さらに他システムと相互接続されることが見込まれるものや、人命等の重要資産にクリティカルに影響する分野で、広く社会アプリケーションで活用する可能性を検討し、可能なアプリケーション・システムのモデルを複数提案する。

【知財戦略ほか】　電子商取引安全技術研究組合

SIP終了後も研究開発成果を一体として知財運用するため、プロジェクト参加者の一つである電子商取引安全技術研究組合を会社化し、事業後継法人としてSCUの知財運用と普及に努める。
既に、本研究開発期間の中途から、IoTユーザより中間成果を利用したいとの引合いがあり、SCUは、今後IoTシステムのセキュリティを向上させるコア技術として、広く産業用機器制御、交通・医療機器、ロボット等、IoT全般での利用が期待される。

実用化へ

研究開発スケジュールと活用の展望