社会実装につながるSCUアプリケーションシステムの構築と実用化技術の実証

電子商取引安全技術研究組合（ECSEC組合）、横浜国立大学（YNU）、東京大学、神戸大学、
東北大学、奈良先端科学技術大学院大学（NAIST）、三菱電機、産業技術総合研究所（AIST）

適用領域

半導体・実装　IoT　製造　インフラ　ビル・スマートシティ

セキュア暗号ユニット「SCU®」がIoT末端ノードを守り、Society5.0時代のサイバー・フィジカル・システムの「信頼の基点（Root of Trust）」となります。

技術の特長

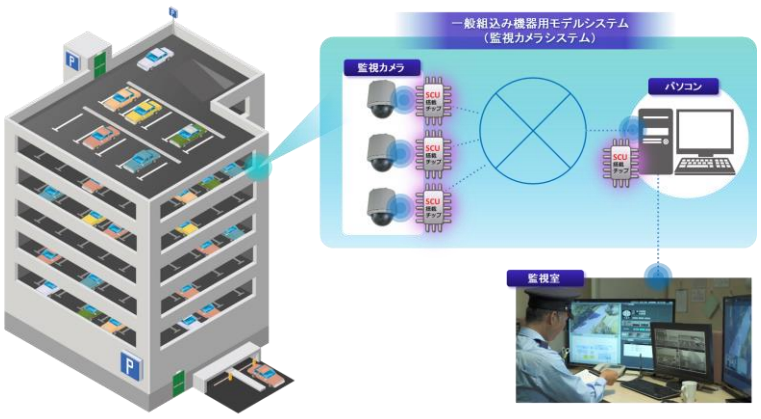
- **組込みスペース、電力供給、処理容量等の制約から現状では無防備に近いセンサー・アクチュエーター等のIoT末端ノード（機器）を守る、微小・微少消費電力のセキュリティチップ、それが「SCU®」です。**
  - ✓ 公開鍵暗号（世界最小、世界最少消費電力、世界最高速の個別記録を達成した楕円曲線暗号（ECC）エンジン）、共通鍵暗号、乱数発生器を搭載
  - ✓ 暗号エンジンへの不正アクセスを検出して阻止するアクセス制御機構を搭載

導入効果

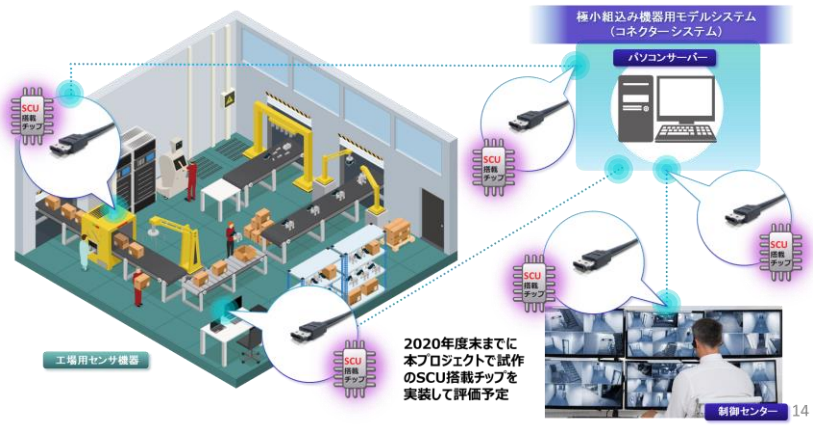
- 「ゼロトラスト」を踏まえた「エンドポイント・セキュリティ」の強化を実現します。
- 「SCU搭載コネクターシステム」なら、コネクター（アダプター）をIF部に装着するだけ、既存（レガシー）機器の入替えは不要です！

ユースケース

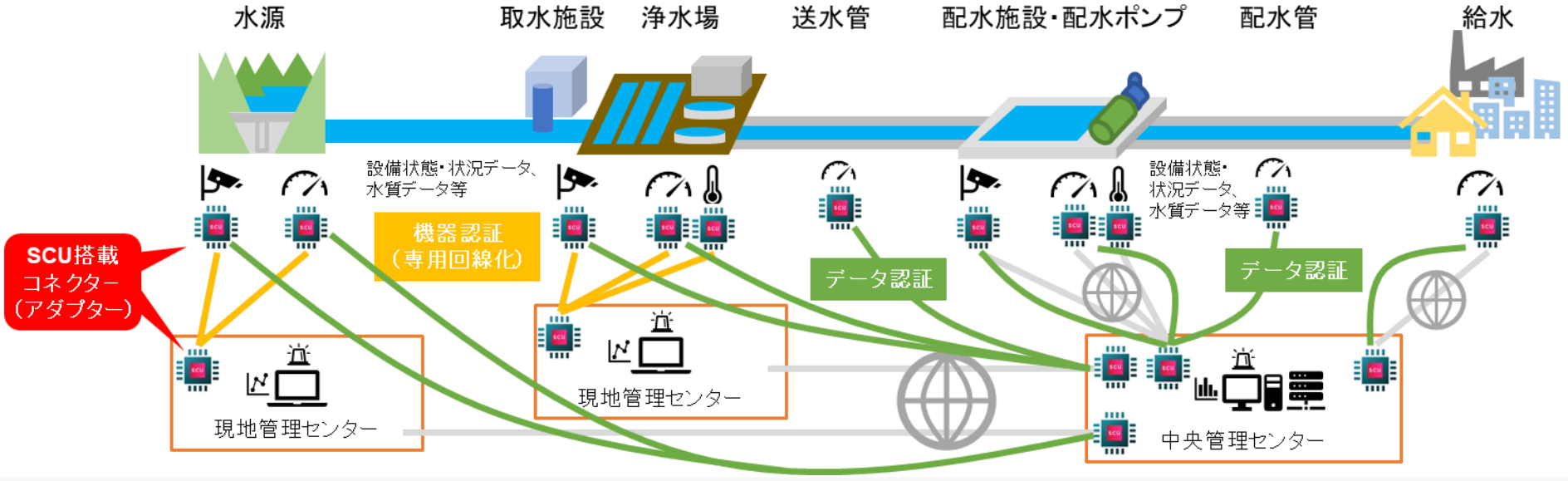
■ 一般組込み機器



■ 極小組込み機器



■ インフラ（上水道）における実装イメージ図



① 社会実装につながるSCUアプリケーションシステムの構築と実用化技術の実証

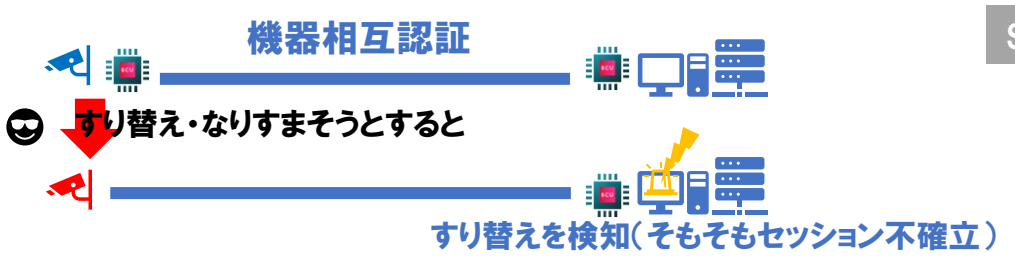
電子商取引安全技術研究組合(ECSEC組合)、横浜国立大学、東京大学、神戸大学、
東北大学、奈良先端科学技術大学院大学、三菱電機、産業技術総合研究所

技術内容

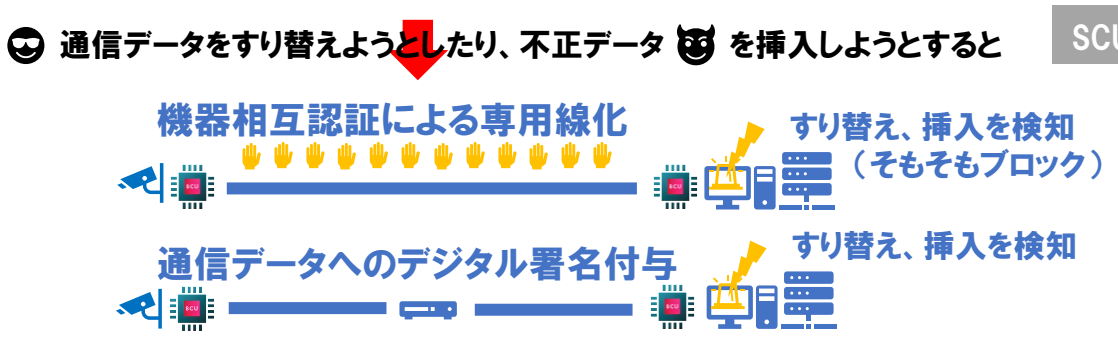
■ IoT時代の信頼の基点としてのセキュア暗号ユニット(SCU)

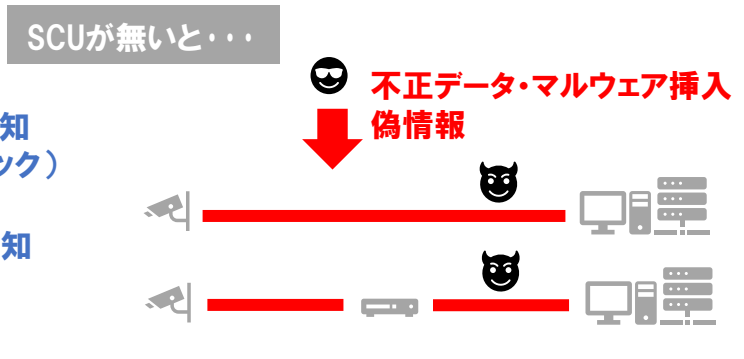
➢ 「SCU®」により、Society5.0時代のCPSの信頼の基点を守る、次の事が実現します。

● IoT機器・末端ノードのすり替え・なりすまし防止



● IoT機器・末端ノードからの通信データのすり替え防止、不正データ挿入防止





● IoT機器・末端ノード(から)の感染・乗っ取り防止

● IoT機器・末端ノードからの通信暗号化(公開鍵方式)

■ 技術の優位性

➢ ECDSA(楕円曲線暗号)の処理において、世界最小、世界最少消費電力、世界最速の個別記録を、複数試作品でそれぞれ達成。これにより、すでに国際的に流通しているセキュリティカーネルと比較し決定的に小サイズの暗号ユニットを製造することが可能な技術を得ました。

➢ IoT用の小さな組込みデバイスにも、公開鍵暗号を実装することを可能としました。

Lowest power ever reported

Smallest ever reported

Fastest ever reported

	Platform	#Gate [kG]	Area [mm²]	#Clk	Vdd [V]	Freq [MHz]	Tsg [ms]	Pow. [mW]	E [μJ]
SCU KM14	65nm	13	0.03	19.4M	0.45		800	0.092	74
					0.75	77	279	0.58	161
					1.2		141	3.2	448
SCU KM15	65nm	1,580	5.64	6.9k-7.5k	0.45	35.7	0.21	15.6	3.28
					0.75	98.7	0.076	123	9.32
					1.4	240	0.0313	1,227	38.7
(1)	Stratix II (90nm)	9,177ALM +96DSP	--	107k	--	157	0.32	--	--
(2)	90nm	540	2.72	22.3k	--	131	0.17	--	--
(3)	65nm	1,370	1.92	34.7k	0.25		11	0.15	1.68
					0.3		2.3	0.69	1.68
					1.1		0.33	42.9	13.9
(4)	65nm	2,500	--	15k	--	236	0.06	--	--
(5)	AMD EPYC7601 (14nm)	NA (64-thread)	NA	157.4		2.2-3.2GHz	0.072	180,000	12,900

問い合わせ先

電子商取引安全技術研究組合(ECSEC組合)
Tel: 03-5259-8077　Email: researchers@ecsec.org

内閣府 Cabinet Office　NEDO　SIP 戦略的イノベーション創造プログラム