RISC-V Days Tokyo 2021

RISC-V RTOSシステムのための セキュリティ開発

Security Development for for RISC-V RTOS Systems

令和3年11月17日
河崎　俊平
RISC-V協会
SHコンサルティング（株）

@risc_v
@riscv_a

発表内容

1. 背景紹介
2. Linux に対し RTOS　の利害特質
3. IoTデバイスセキュリティ
4. RTOS　デバイス認証、無線遠隔ソフトアップデート
5. オープンシリコンによるセキュアMCUチップ設計
6. まとめ

1. 背景紹介

発表者経歴

<MCU開発>

1980-1986　68K、AIチップ

1986-2001 サターン、ドリキャスチップセット

<セキュリティ開発>

2001　大手電機メーカ駐在員退社

　　ローカル雇い　インテグレータ転向

　　Java Card™ 、テレマ開発

2003　ルータ真贋判定　C暗号ライブラリ

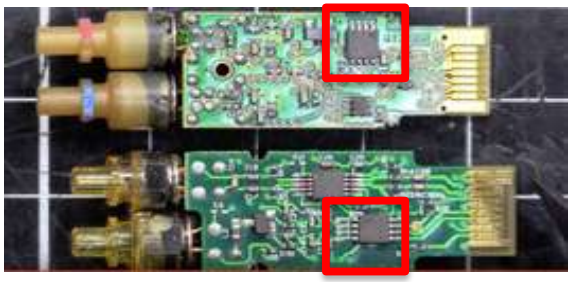
2007　北米スマホ用　セキュアOS

2010　FIPS140-2 Level 3　取得作業

<IoT開発>

2013　大手半導体会社退社　SHC社設立

　　マーモット 無線IoTボックス



RISC-Vとの出会い（2014）

SHマイコン@Hot Chip 26

SHマイコン2013年廃止

囚われIP からの 解放運動

2545 16-ビット固定長 ISA特許失効

オープンプロセサファウンデーション

2003 Verilog

2014 0pf.org

2016 System Verilog

軽量無線 IoTボックス Marmot（現行製品）

2016年よりレンタル開始

親機（ゲートウエイ）
　多様なアプリやフレームワークを活用できるLinuxプラットフォーム
　センサーモジュールとの通信
　クラウドへのデータアップロード
　PC、Androidスマホ・タブレットアプリ開発
　顧客要望の制御基板のカスタマイズ

子機（センサモジュール）
　業界最軽量小型、乾電池で長時間運転可能
　電池残量検出、外付けアンテナ/ワイアアンテナ選択、GPS標準装備、
　UART, I2C, SPI, A/D, GPIOなどのセンサ接続用端子とドライバを完備

スマートフォンデータ Viewer （ユーザインタフェース）
　PC、Androidスマホ・タブレット上の親機受信データ確認用GUI

軽量LoRaボックスはユニークな存在で、ドローン応用
建設現場等で多くの実績があります。
(注)　無線通信部は、技術適合認定取得済み。

全体システム構成例

親機接続Android
スマートフォン画面例
(グーグルマップ、
温度、湿度表示)

親機接続PCの操作画面例

軽量無線IoTボックス Marmot LoRa 通信性能評価

システム構成
　　親機：外付けアンテナ　子機：2種（外付けアンテナ：外付け、ワイヤアンテナ：ワイヤ）

自社実験
　　屋内 (1) 3LDK 84平米 室内（ワイアOK）
　　(2) マンション 30階 室内-2階ロビー (外付け OK, ワイヤ NG)
　　(3) マンション 30階 室内-25階エレベータホール (ワイヤ OK)
　　(4) 宇都宮マロニエプラザ展示場内 100m (36, 33, 43, 139, 54, 45–36, 33 ,47, 139, 54, 46)
　　多数展示ブース障害 (ワイヤ OK)、ガラスドア外 (ワイヤ NG)

　　街中　(1) マンション 30階 室内-広場 285m (外付け OK）、ビルの陰に入る （外付け OK)

　　山中　(1) 高尾山 ケーブルカー 清滝駅前広場 (35,37,52, 139,16,2 100m)-高尾山駅 周辺
　　(35,37,50, 139,15,22 450m) 1km (外付け OK, ワイヤ NG), ケーブルカー途中 (外付け OK)

　　トンネル　(1) 高尾山 ケーブルカー途中 約100m トンネル内 (外付け OK)

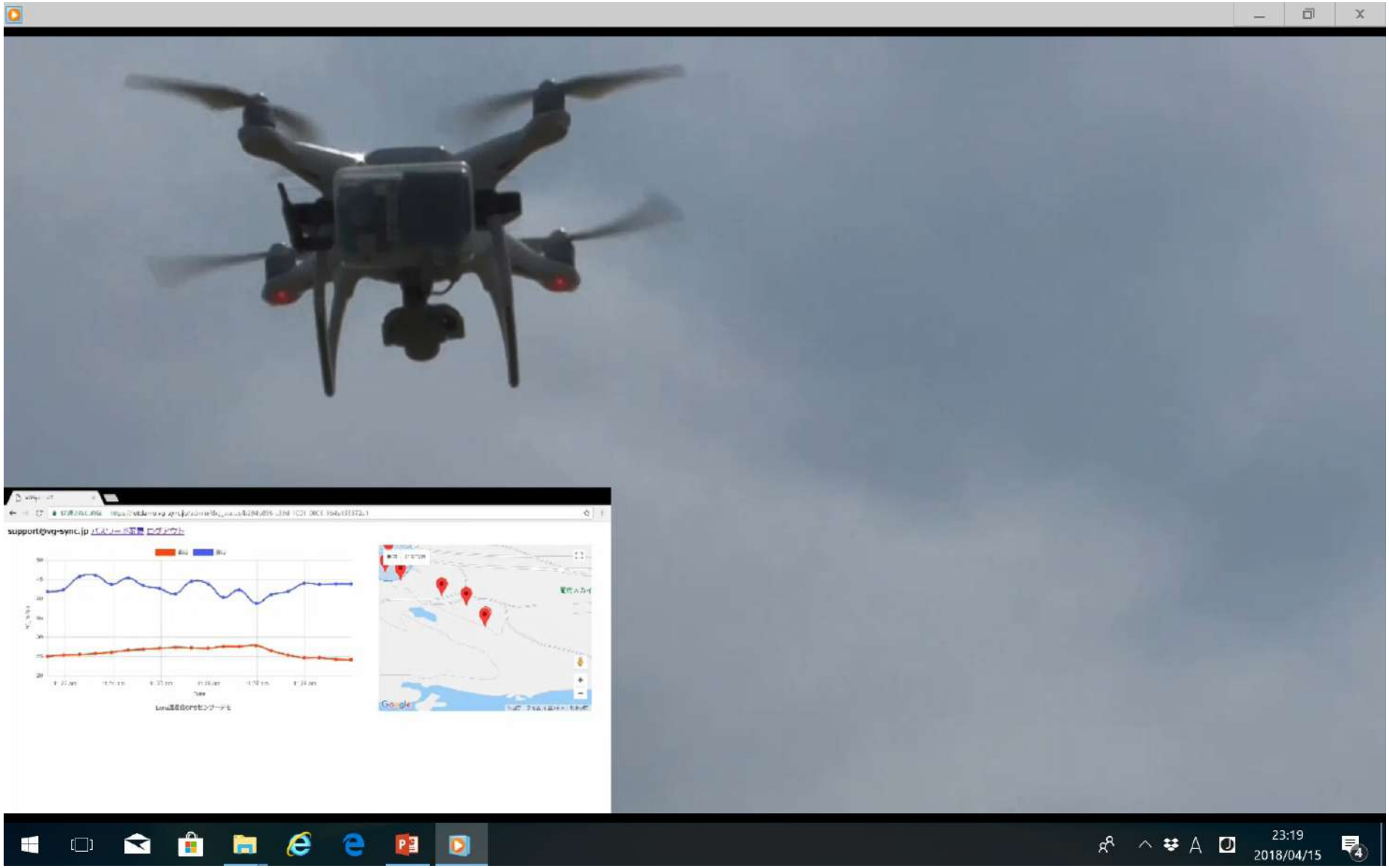
顧客実証実験　　（火山学会にて発表。弊社は、親機、子機カスタマイズを受注）
　　九州桜島　3Km-3.5Kmで伝送を確認
　　LoRa子機をドローンで、危険地域に設置
　　LoRa子機の圧力センサーで火山灰量検出を行い、親機へ伝送
　　親機から、指定のIoTクラウドにデータを送信

無線 IoT ボックス Marmot サービス

サービス対応	現行	将来
子機親機設置工事（レンタル）	軽量子機、親機レンタル	子機親機設置
子機応用対応	基本システムのセンサ変更☆ データ出力タイミング変更	ソフト開発サポート☆ 基本センサ活性化　新規センサ追加☆
親機操作用GUI	IoTクラウド出力 GUI仕様追加変更☆	RTOS上　ユーザアプリ開発☆
親機応用対応	親機接続、クラウド入出力、SDカードへデータ保存、その他	親機をLTEに接続、クラウドと入出力、クラウド中に、NORフラッシュ中データをセーブ
クラウド応用対応	クラウド IoTシステム貸出（月額料金） VB Sync IoT設置☆	クラウド機能貸出（月額料金） VB Sync IoT設置☆ AWS IoT コア、S3、ラムダ設置☆
セキュリティ含む IoT管理		ハードウエアルートオブトラストを使ったデバイス認証、OTAなど
IoTクラウドデータ可視化	Cloud Viewerのカスタマイズ☆	←
子機コンフィギュレーション	カスタマイズ☆	コンフィギュレータによるユーザ設置 OTAによるカスタマイズ☆

☆カスタマイズは受託開発。ご要望の仕様をお伺いし、工数検討の後、見積もりを発行します。
☆株式会社ソフトエージェンシー様のBG-Sync IoTサービスなどから選択できます。

ドローンによる大気状況検出実証実験
(GPS、温・湿度センサー)
工事現場の騒音・振動データ送信



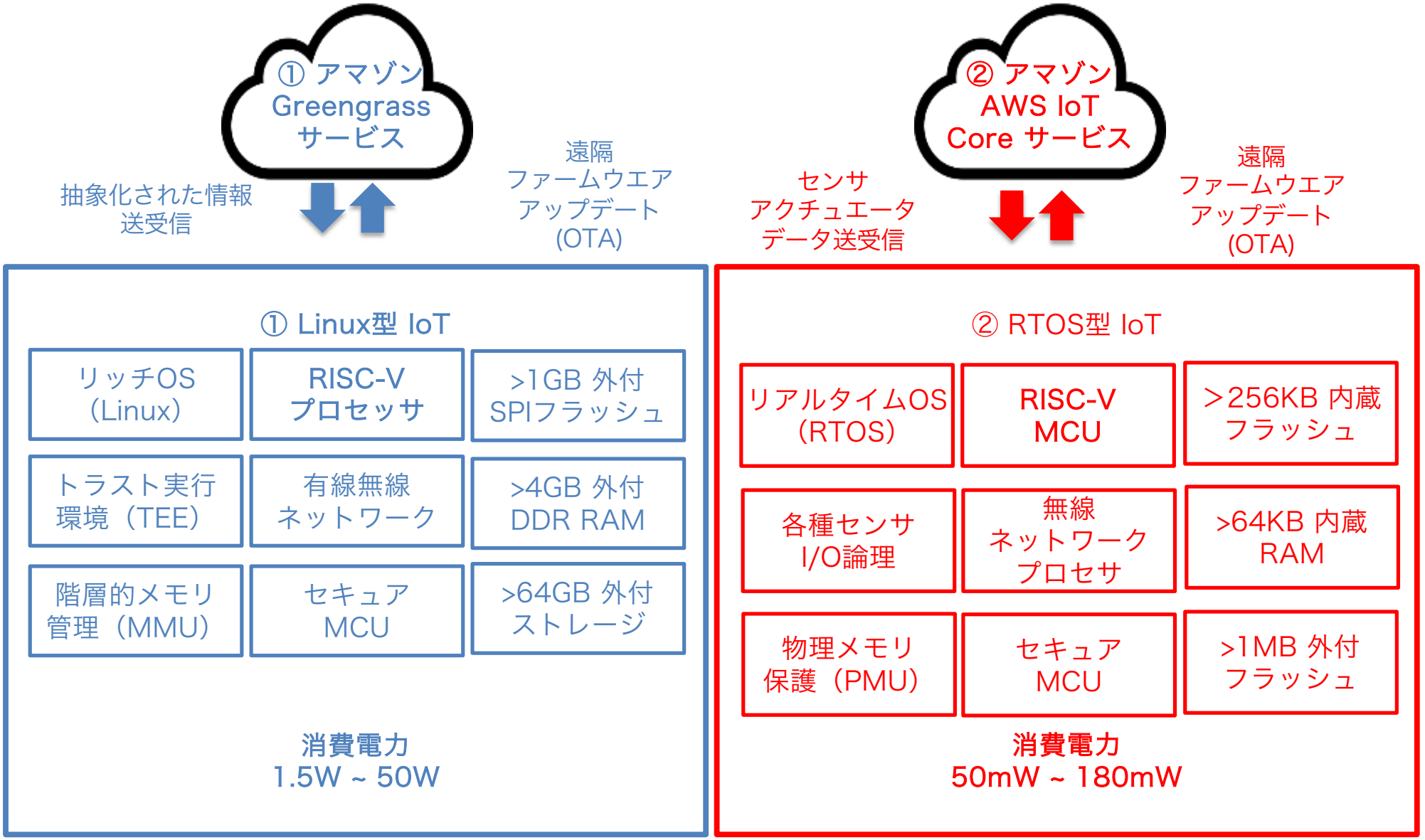
火山噴火時の降灰検出実証実験
(GPS, 圧力センサー, 温・湿度センサー)

2. Linux と RTOSの利害特質

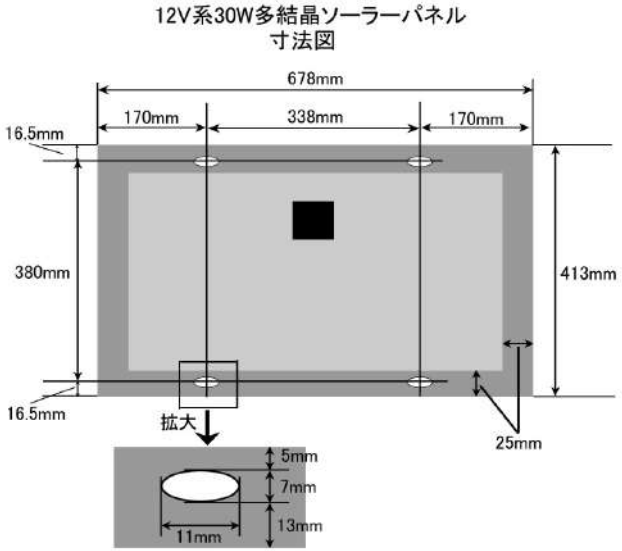
RISC-V　セキュリティ

技術	定義	製品例	応用例
TEE	Linux IoTエッジ 「コンピューティング プラットフォーム」	AWS Greengrass Azure IoT Edge	大手 IoT事業 インフラ等
RTOS Security	RTOS 組込MCU 「オペレーティング システム」	aws Amazon FreeRTOS	中堅 IoT事業 家電 医療介護等

Linux 対　RTOS



Linuxシステム用 ソーラパネル例　30W



定格出力：　30W

開放電圧：約21.6V

短絡電流：約1.83A

最大動作電圧：17.28V

最大動作電流：1.74A

寸法：41.3cm x 67.8 cm x 2.6cm

重量：約3.4Kg

表面のガラス：強化ガラス

機体寿命：25年

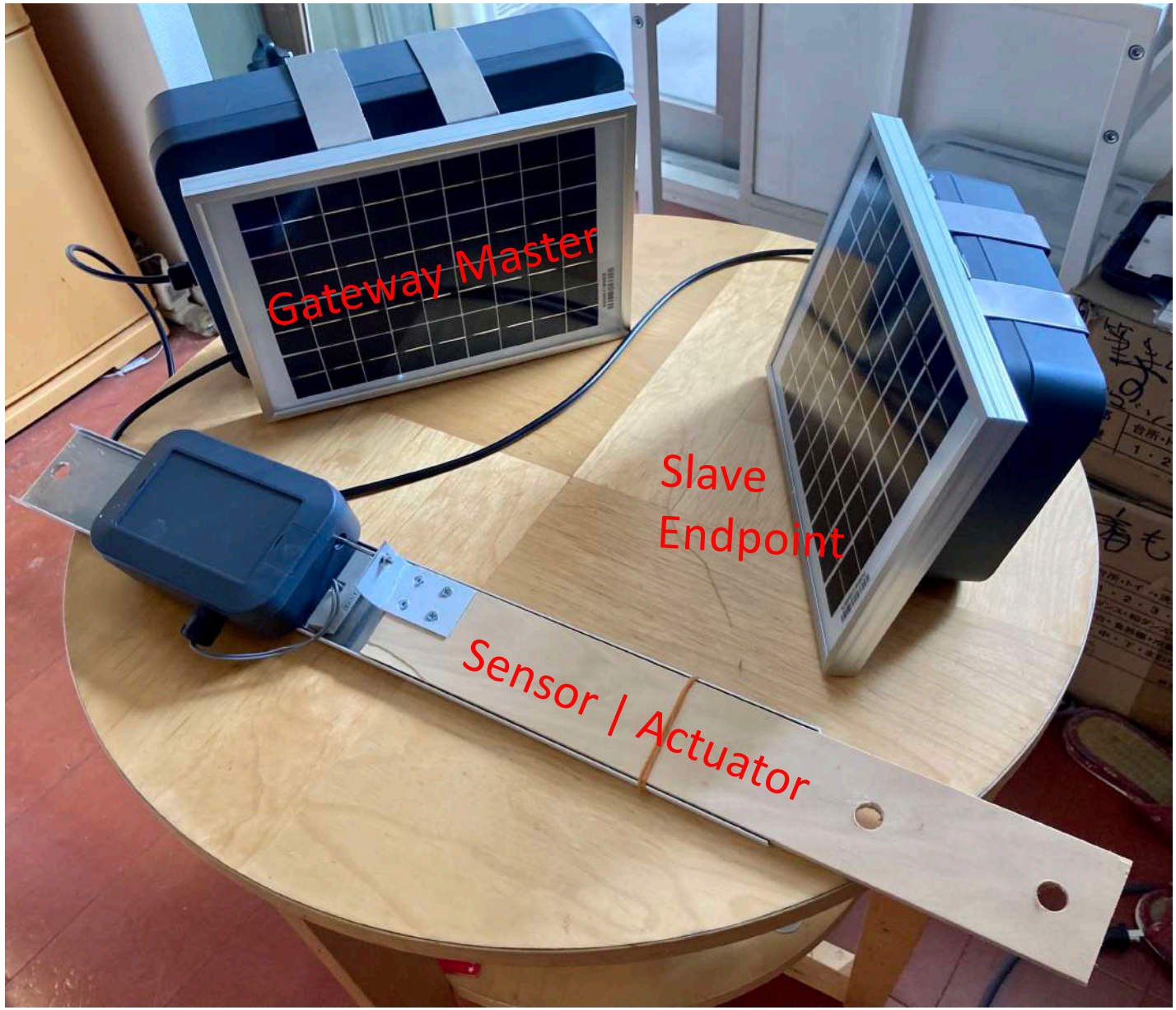
高品質セル使用

12Vバッテリー対応

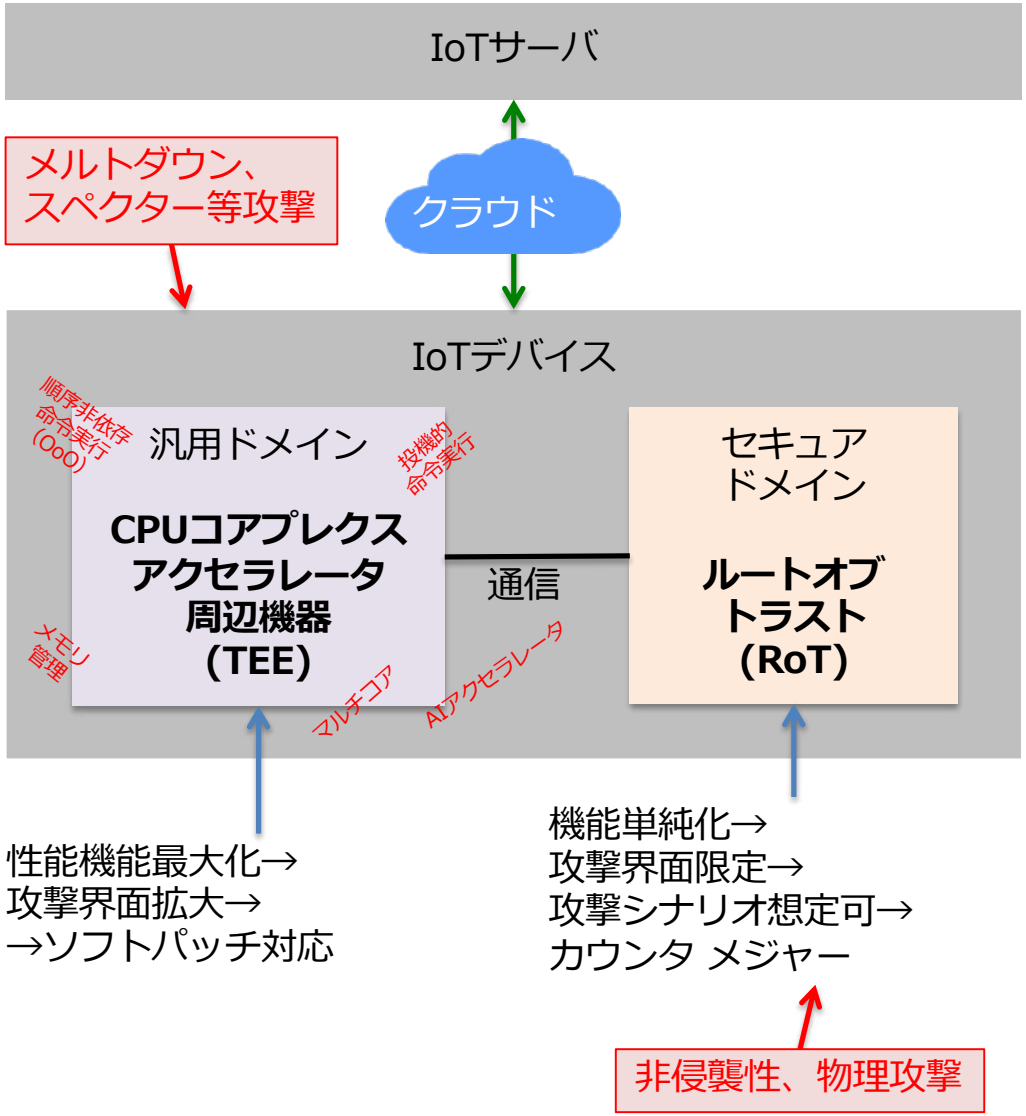
ロングケーブル搭載（約8m）

YMT ENERGY (YMT. net Limited company)				
30Watt Poly-Crystalline Solar Module				
Model:	MS-P-30W			CE
Serial No:				
Pmax	Vmp	Imp	Voc	Isc
30W	17.28V	1.74A	21.60V	1.83A
Max System Volt		1000V DC		
Dimension:		L:413mm; W:678mm; T:26mm		
Frame:		Aluminum		
Standard Test Conditions: AM1.5 100mW/cm2 25°C				

RTOSシステム用一体型ソーラ リチウム



信頼基点モジュールを分離独立



- 汎用処理CPUは複雑。複雑さゆえに守る方法がキャッチアップしない。
- 信頼起点を分離。単純なシステムを多様な方法で守る。
- 各攻撃法を網羅的に分析し、防衛方法を構築し各個撃破する。

3. IoTデバイスセキュリティ

RISC-Vにおける信頼の基点（Root of Trust）

- 信頼の基点 = 軽量なコプロセサ
- 鍵管理、鍵生成、乱数生成の機能を持つ
- 公的空間、自然空間、屋外空間に置かれるIoT脅威を分析すると物理攻撃を排除できない。
- 分解剥離等による物理攻撃、電流解析などのサイドチャンネル攻撃に対する耐タンパ技術を適用したセキュア格納領域を持つ。

RISC-V IoT セキュリティ

- IoTセキュリティを実現するセキュアチップのファーム、IoTシステムのソフト、クラウドのソフト作り込みが必要である。調査するとセキュアチップ側に１０万行、システム、クラウド側に１０万行程度、新規開発ステップ数があることがわかった。

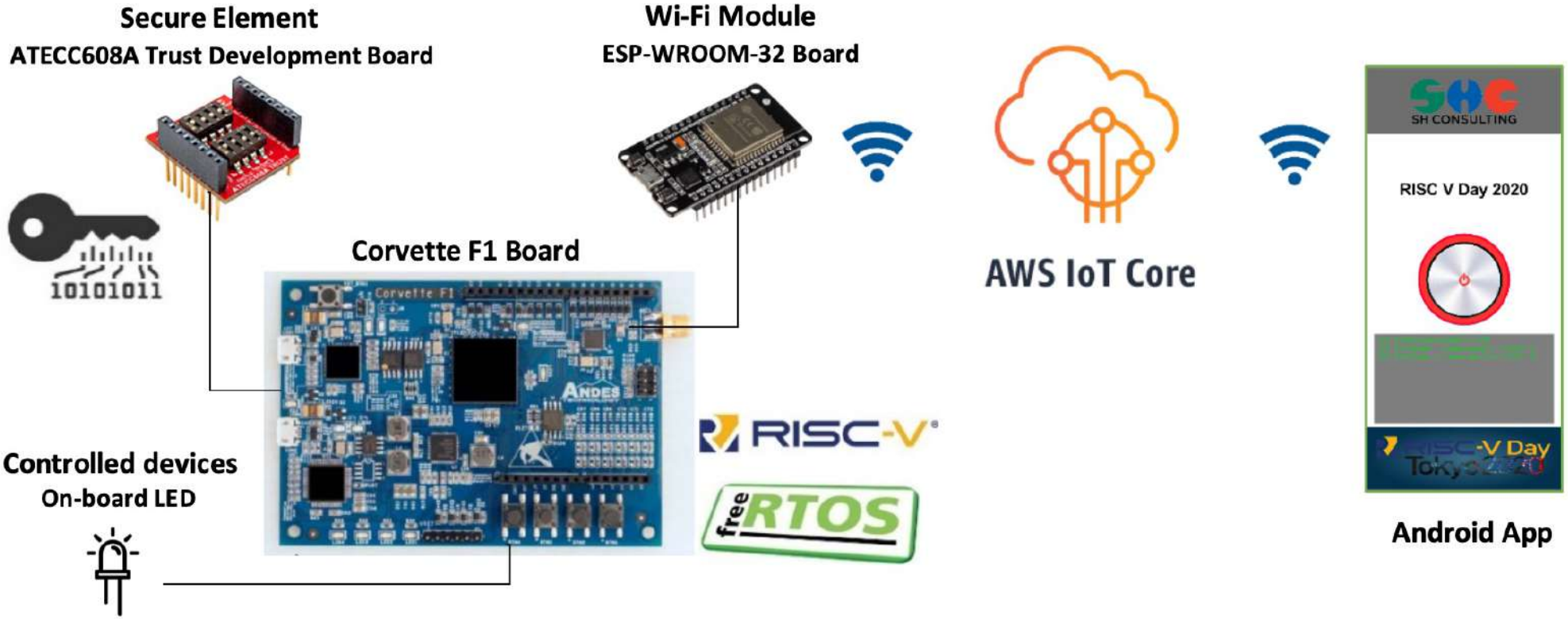
- 日本企業やドイツ企業からハードウエアルートオブトラストを購入しようとした。断られた（２０１３年）。セキュアチップを作ろうと考えた（２０１８年）。米国のベンダから部品が提供された（２０２０年）。

- ２０１９年にFreeRTOSがアマゾンに買収された。アマゾンは、FreeRTOSに必要なネットとセキュリティのソフトを載せた。２０２１年になるとIoTのフルセキュリティシステムが提案された。

4. RTOS IoTによるデバイス認証と遠隔無線ソフトウエアアップデート（OTA)

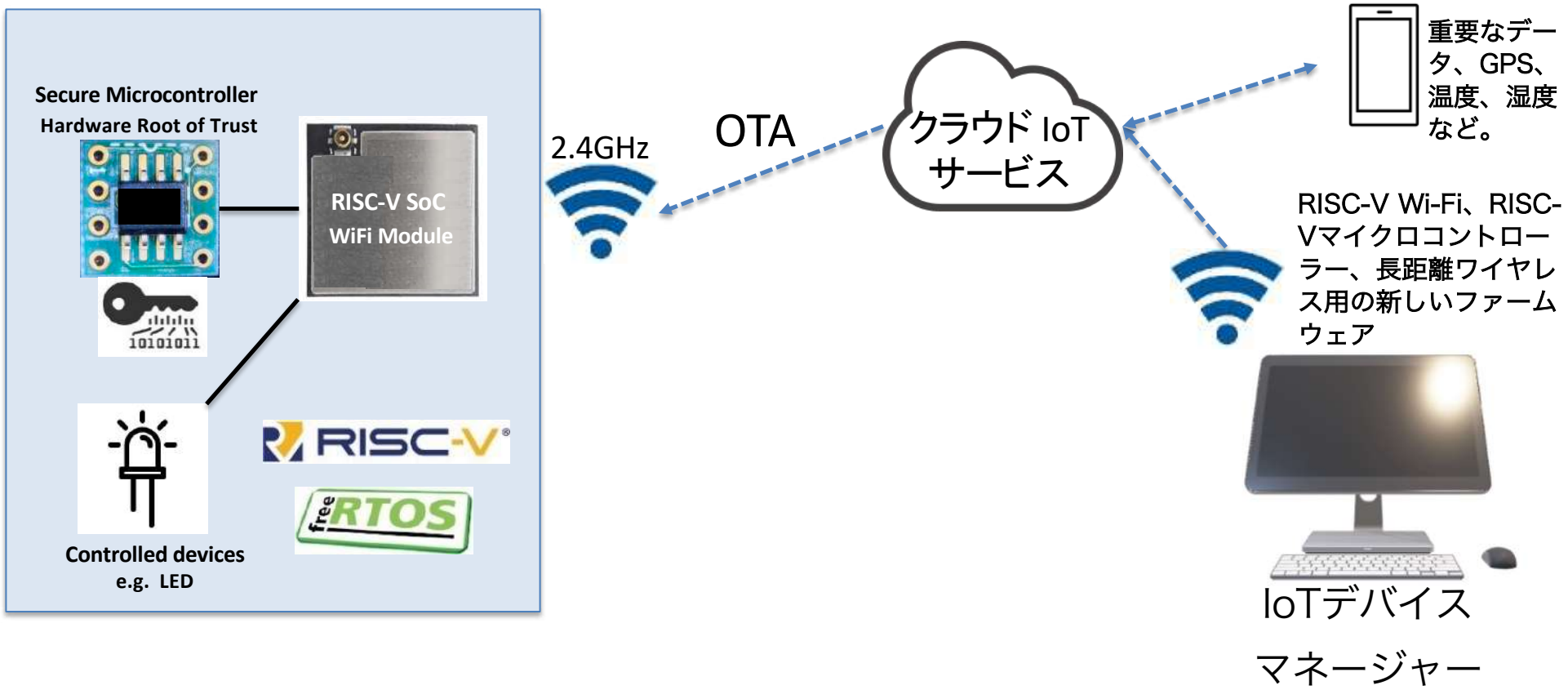
SHC RISC-V AWS IoT Core デモ（2019, 2020）

2019年、RISC-Vツールの使用しSHCはFreeRTOS　をRISC-Vに移植し、Amazonネットワークに接続しました。2020年には、FreeRTOSにルートオブトラストチップを集積し、BYOC（自前公開鍵証明書をAWS IoTにプロビジョニングする技術）を行いました。

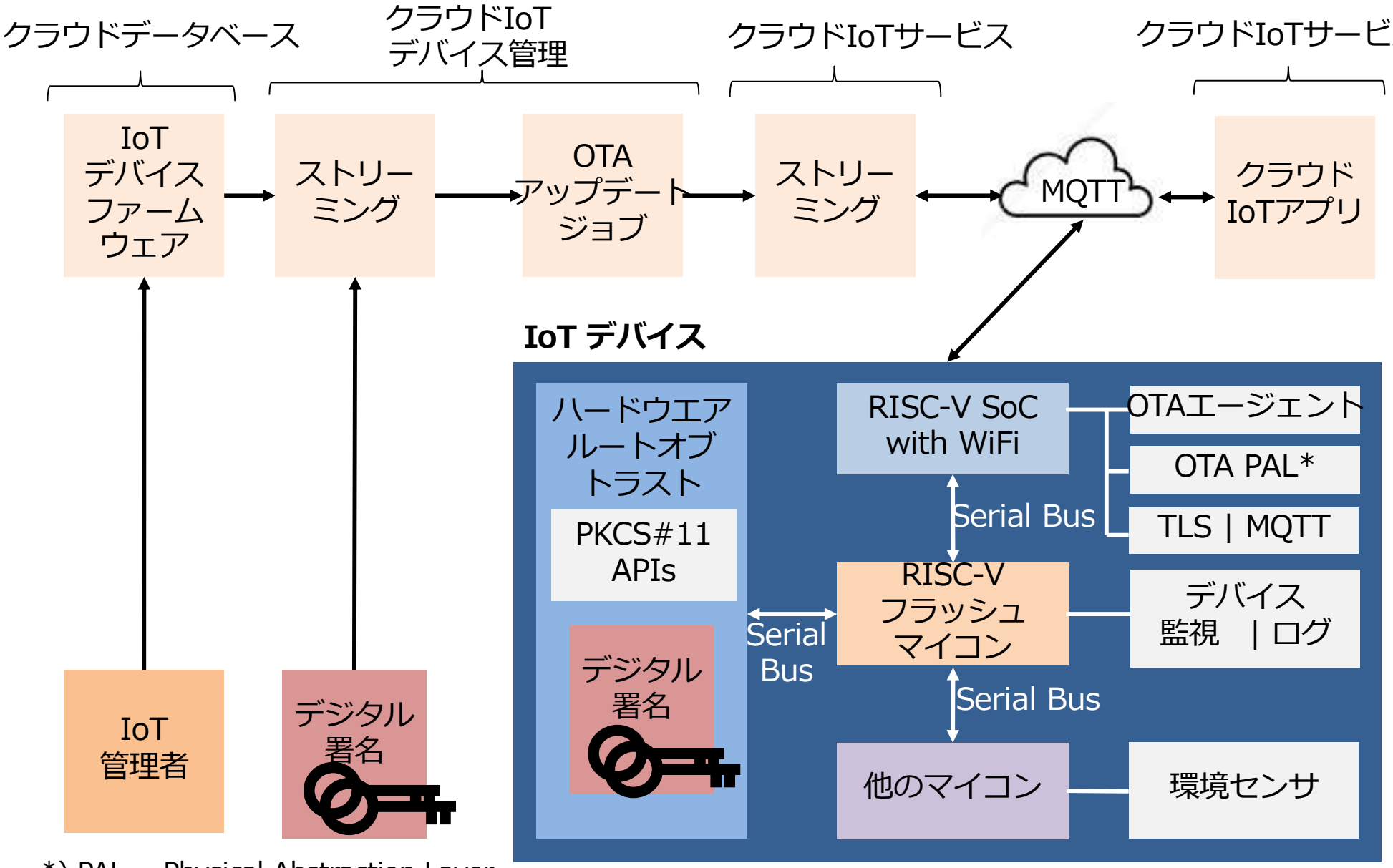


オンライン　RISC-V パビリオン デモ（２０２１）

RTOSを実行するRISC-V IoT

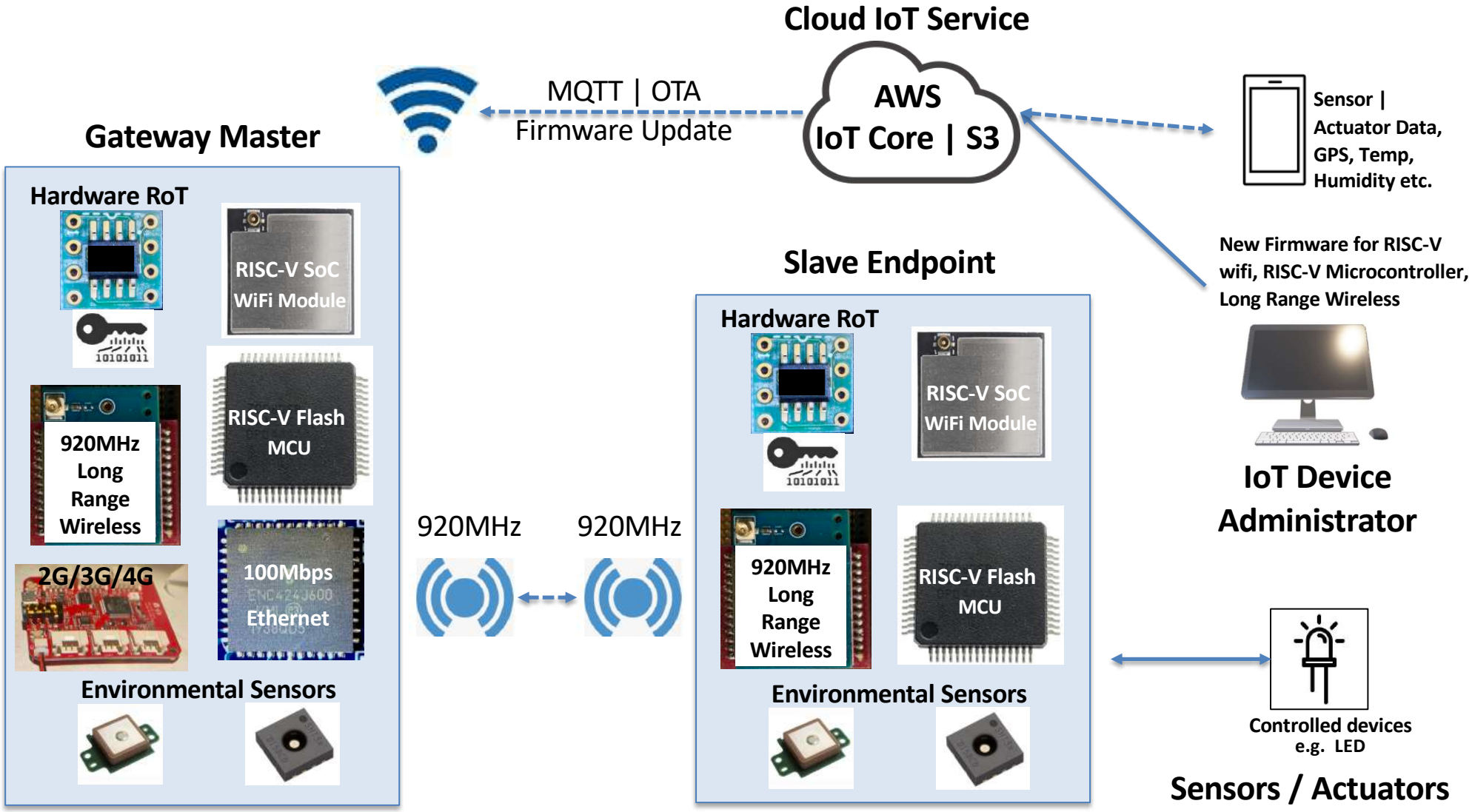


アマゾン FreeRTOS　でのOTA方式

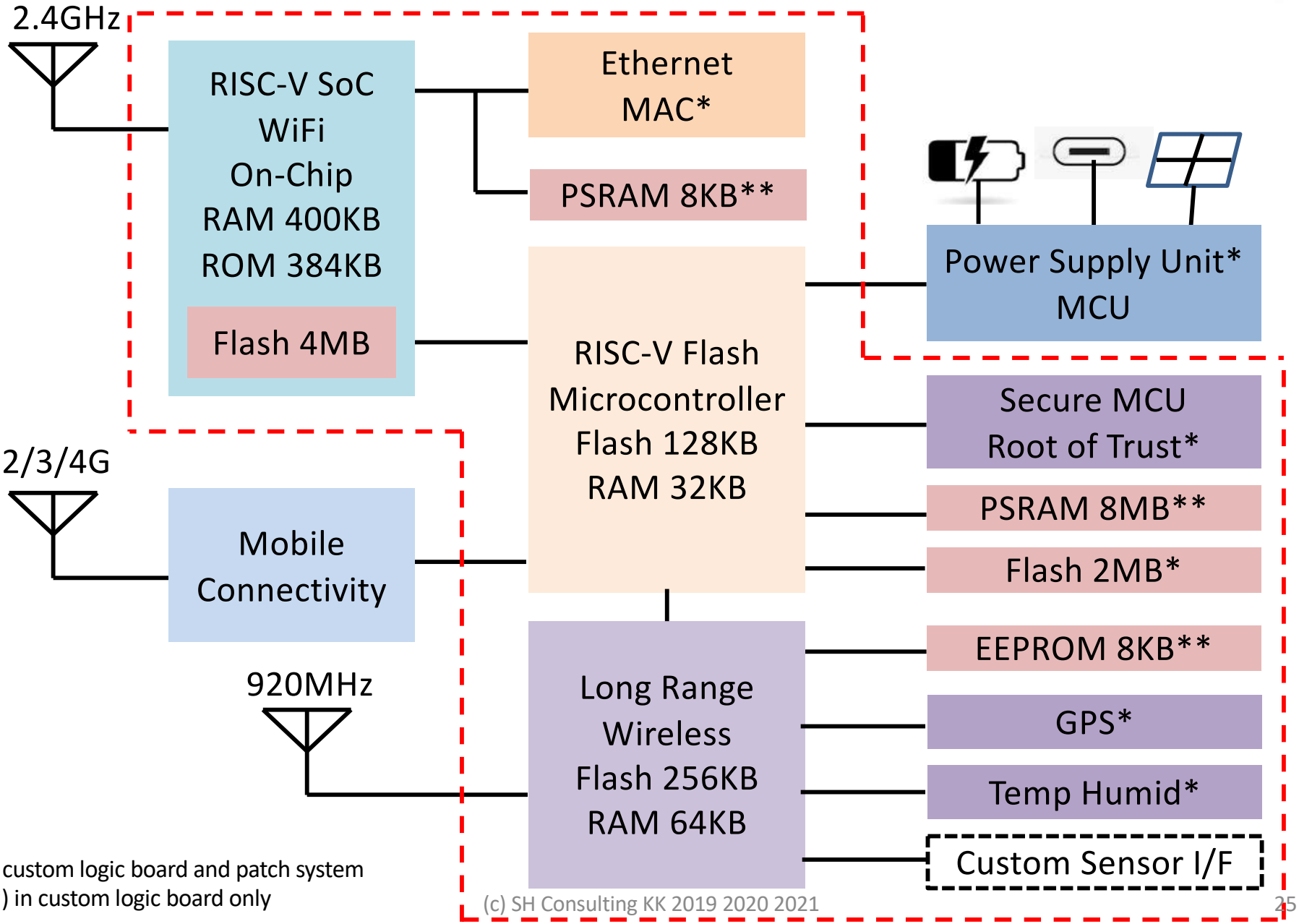


*) PAL = Physical Abstraction Layer

Marmot　システム



RISC-V RTOS IoT マーモットシステム



*) custom logic board and patch system
**) in custom logic board only

2019年提案に対して出現した技術

アマゾンBYOC方式を使い認証サーバを立てることはできる。

アマゾン AWS IoT コア｜ラムダ ｜S3 活用

RISC-V SoC ツール活用

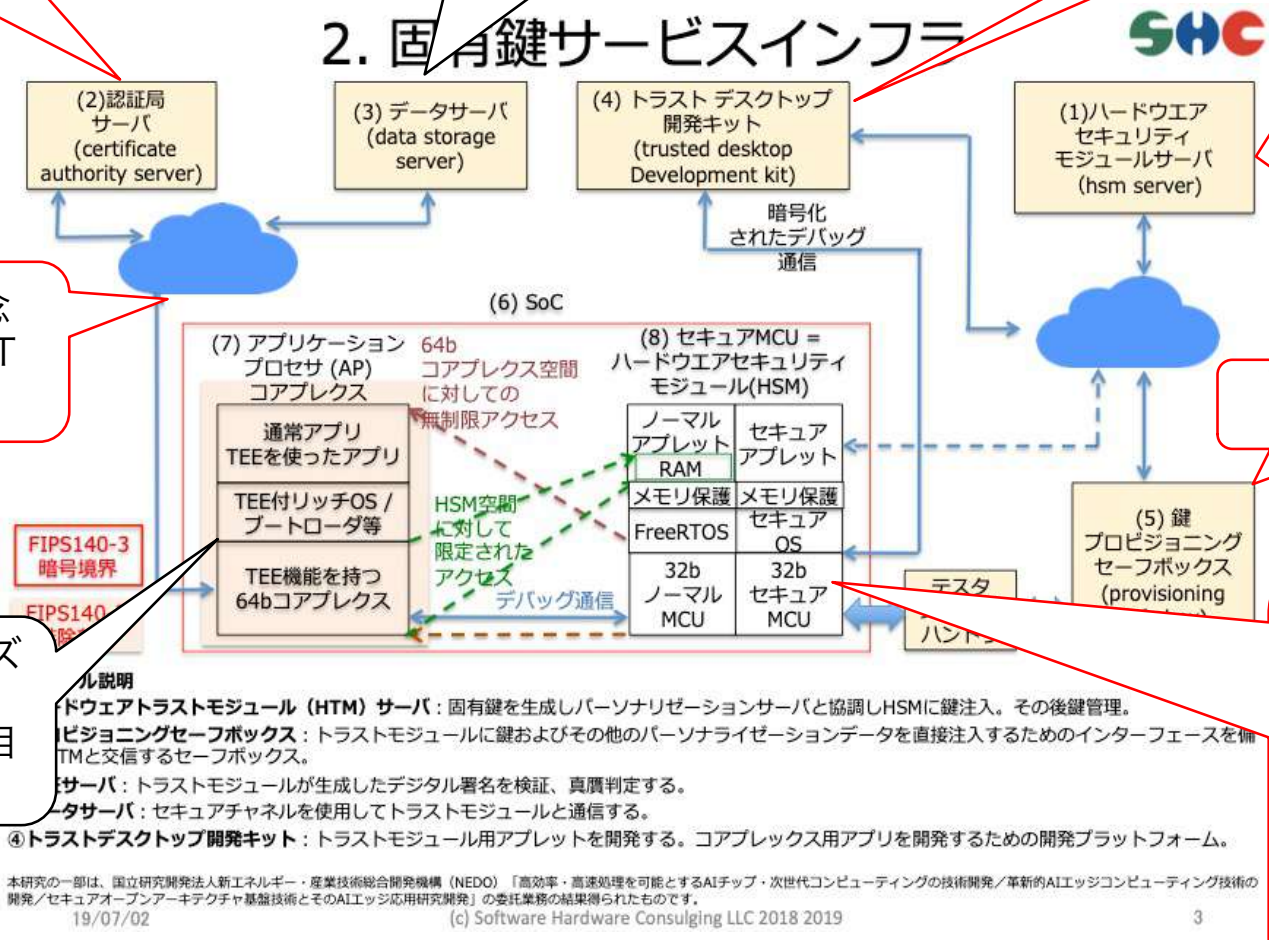
市販セキュアMCUチップが提供するIoT、HSM管理サーバ活用

SoC開発断念 →RISC-V IoT ボード開発

市販セキュアMCUが解決

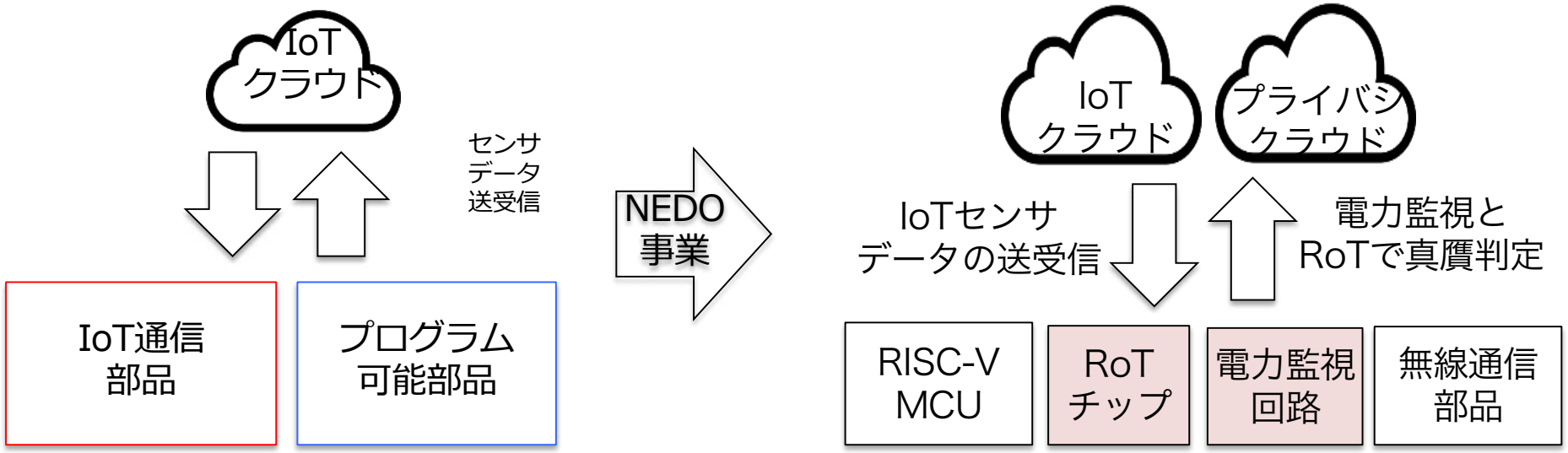
国内商用ニーズにフォーカス →RTOSにも目を向けた

安価な市販セキュアMCUチップ供給開始（2020年）→ セキュアMCUチップ、セキュアOS開発 → eFablessのChipIgniteなどでチップ試作を検討中。



次世代無線IoTボックス ：RISC-Vによるセキュリティ実現

マルウエア　から　システムを守る



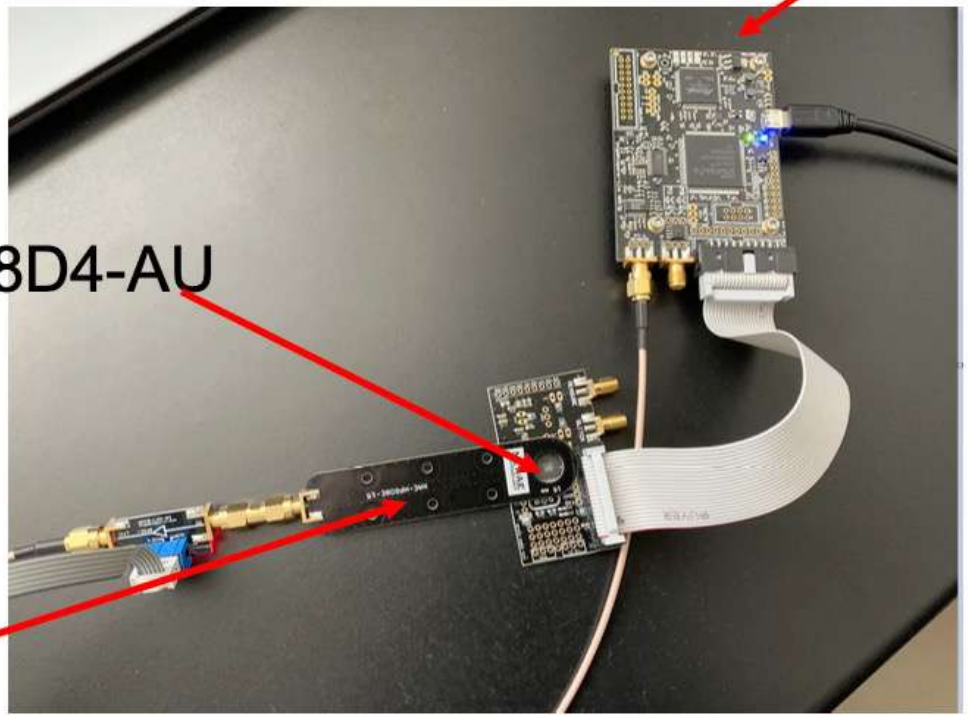
NEDO助成により研究実施中
米国特許申請済

次世代無線IoTボックス　：背景技術

マルウエア　から　システムを守る

ChipWhisperer-Lite

電源波形、電磁波系をアナログ信号をデジタル信号に変え連続データとしてRAMに格納



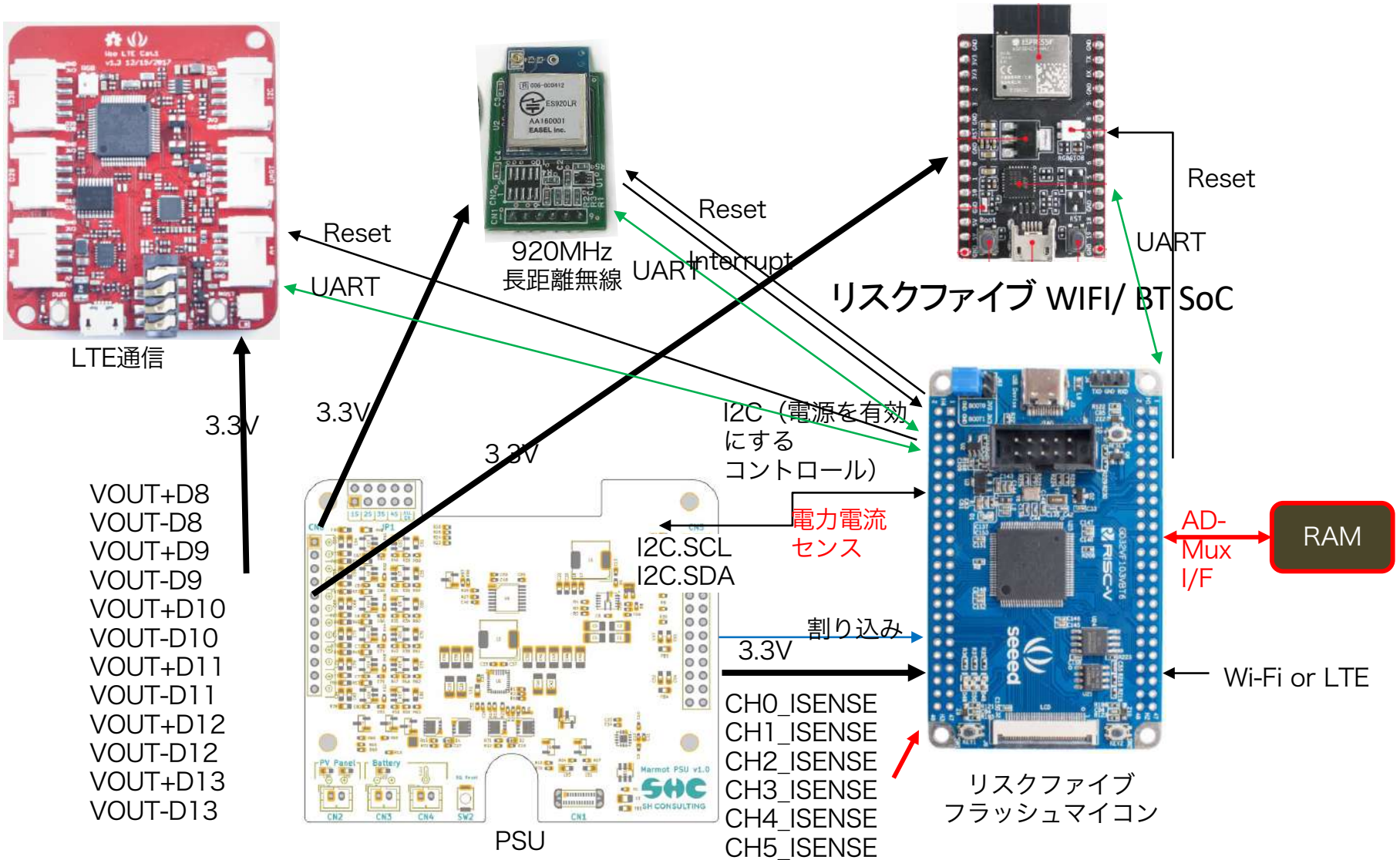
ATXmega128D4-AU

測定対象のマイコン

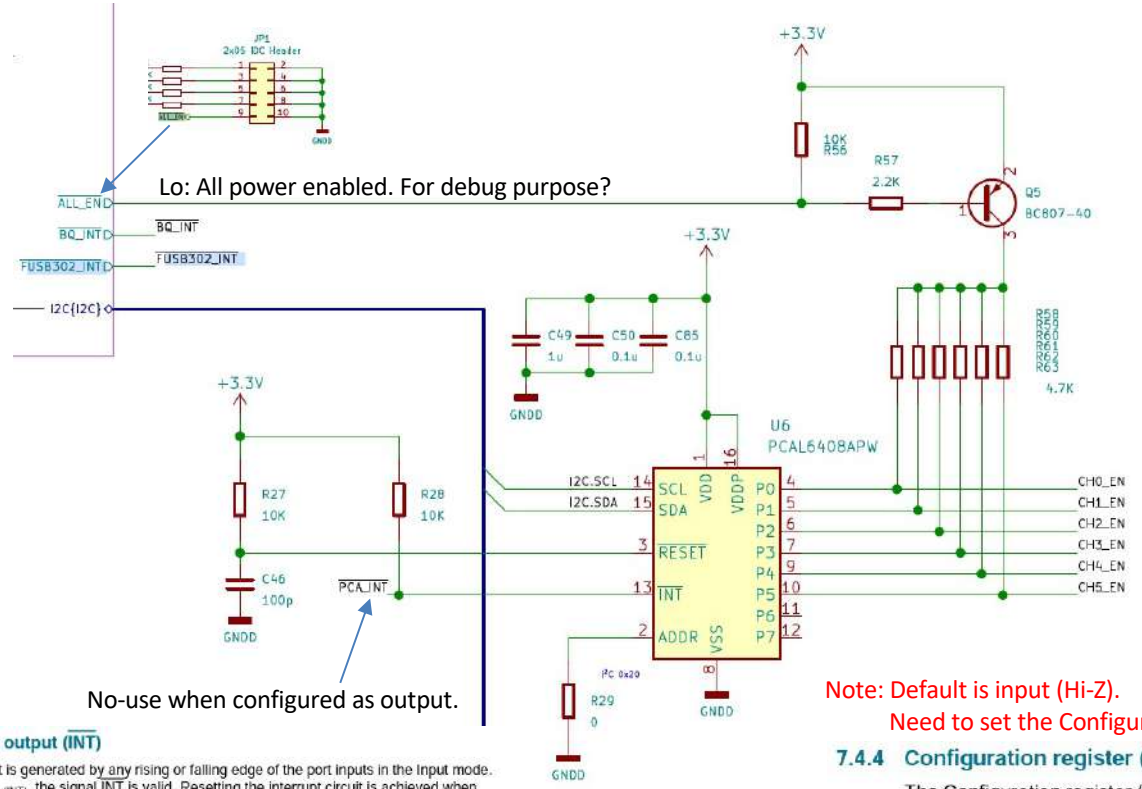
H-Field probe

電磁プローブ

フラッシュマイコンによる電源分離管理



PSU Board (1/x): PCAL6408A (Power enable control)



Power enable (Hi:On, Lo:Off)

Note: Default is input (Hi-Z).
Need to set the Configuration register to change to output.

7.8 Interrupt output ($\overline{INT}$)

An interrupt is generated by any rising or falling edge of the port inputs in the input mode. After time $t_{v(INT)}$, the signal $\overline{INT}$ is valid. Resetting the interrupt circuit is achieved when data on the port is changed to the original setting or when data is read from the port that generated the interrupt (see Figure 14). Resetting occurs in the Read mode at the acknowledge (ACK) or not acknowledge (NACK) bit after the rising edge of the SCL signal. Interrupts that occur during the ACK or NACK clock pulse can be lost (or be very short) due to the resetting of the interrupt during this pulse. Each change of the I/Os after resetting is detected and is transmitted as $\overline{INT}$.

A pin configured as an output cannot cause an interrupt. Changing an I/O from an output to an input may cause a false interrupt to occur, if the state of the pin does not match the contents of the Input port register.

7.4.4 Configuration register (03h)

The Configuration register (register 3) configures the direction of the I/O pins. If a bit in this register is set to 1, the corresponding port pin is enabled as a high-impedance input. If a bit in this register is cleared to 0, the corresponding port pin is enabled as an output.

Table 10. Configuration register (address 03h)

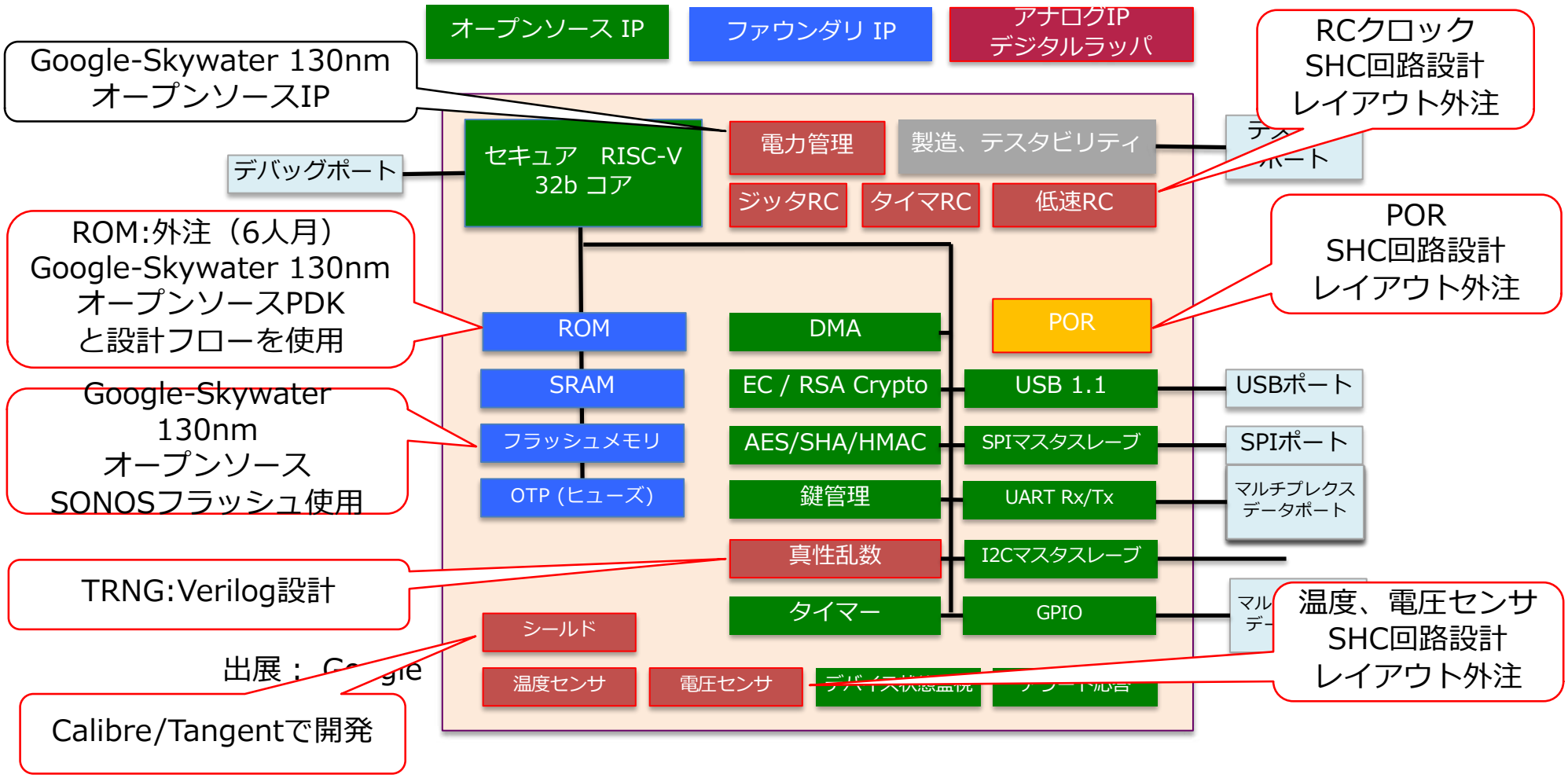
Bit	7	6	5	4	3	2	1	0
Symbol	C7	C6	C5	C4	C3	C2	C1	C0
Default	1	1	1	1	1	1	1	1

Considerations

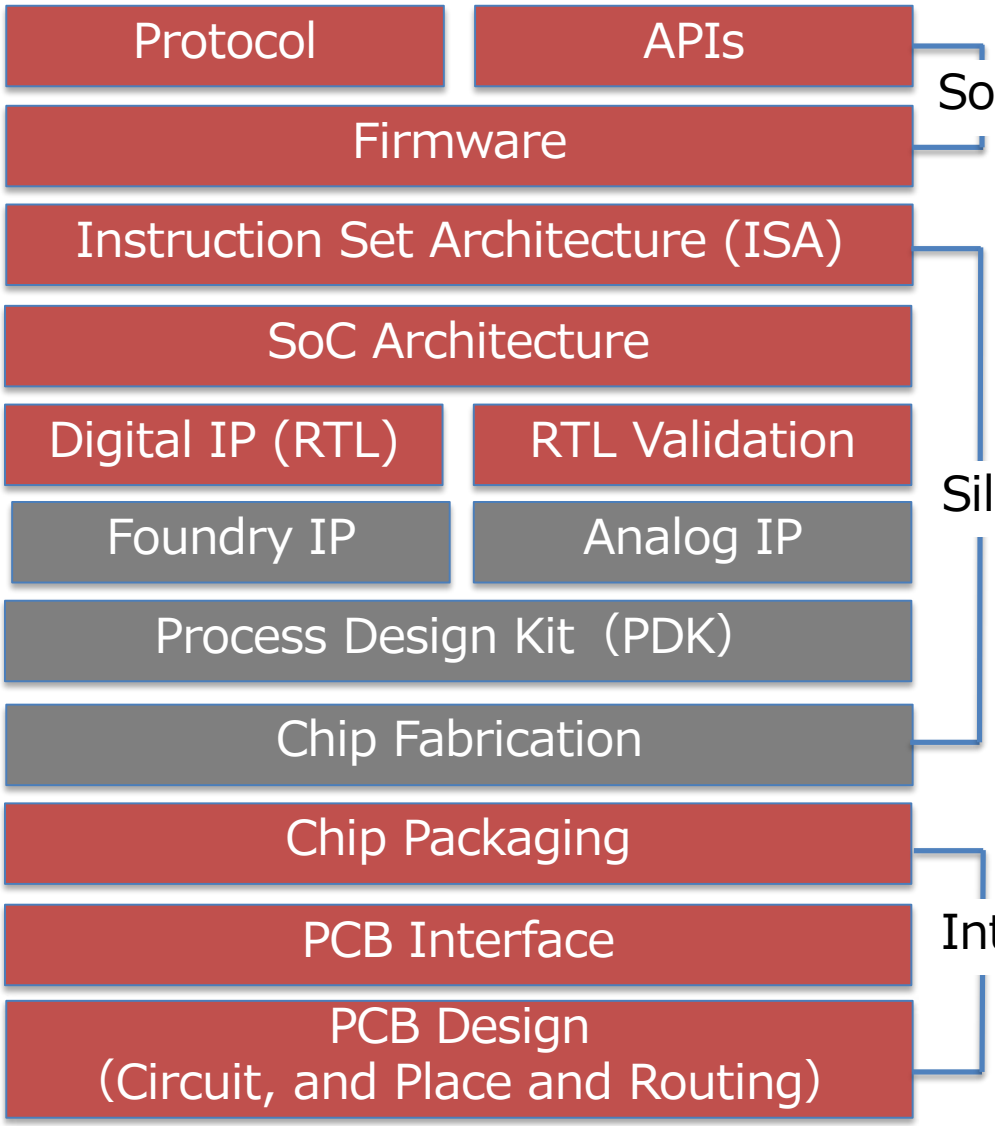
- PSUからの電流センス(CH#_ISENSE)をサンプリングするMCU?
  - GD32V: ADC 12bit, 1Msps
  - ESP32: ADC 12bit, 100Ksps
  - 参考: ChipWhisperer は105Msps
    - https://forum.newae.com/t/cwlite-sampling-question/1424/3
    - Target 25MHz: AES break needs 120 traces
    - Target 100MHz: AES break needs 400 traces
  - 各ボードのCPU動作周波数？上記ADCの性能で足りる？
    - GD32V (RISC-V ~108MHz)
    - ESP32 (RISC-V ~160MHz)
    - Wio LTE (STM32F412RG, CM4 ~100MHz)
    - LoRa (MKL16Z128(NXP), CM0+ ~48MHz)

5. オープンシリコンによる セキュアMCUチップ設計

オープンタイタン実装はチャレンジ



Google's OpenTitan



■Target FPGA board
- ARTY S7 evaluation board
- Manufacturer Digilent Inc.
- FPGA used: Xilinx
  Spartan7 50
  (XC7S50CSGA324-1)
- 256MB DDR3L
- 16MB QSPI flash
- Arduino shield
- Pmod connector

-Board size: 88mm x 102mm

Closed Source

Open Source

新チップ設計技術OpenROADの試用

１）SKY130プロセス（130ナノメータ）に対して、Googleオープンソース PDKを開発。プロセスライブラリ、セルライブラリ、I/O、メモリコンパイラ、（ノンボラ）をオープンソースで提供し無償で使える。

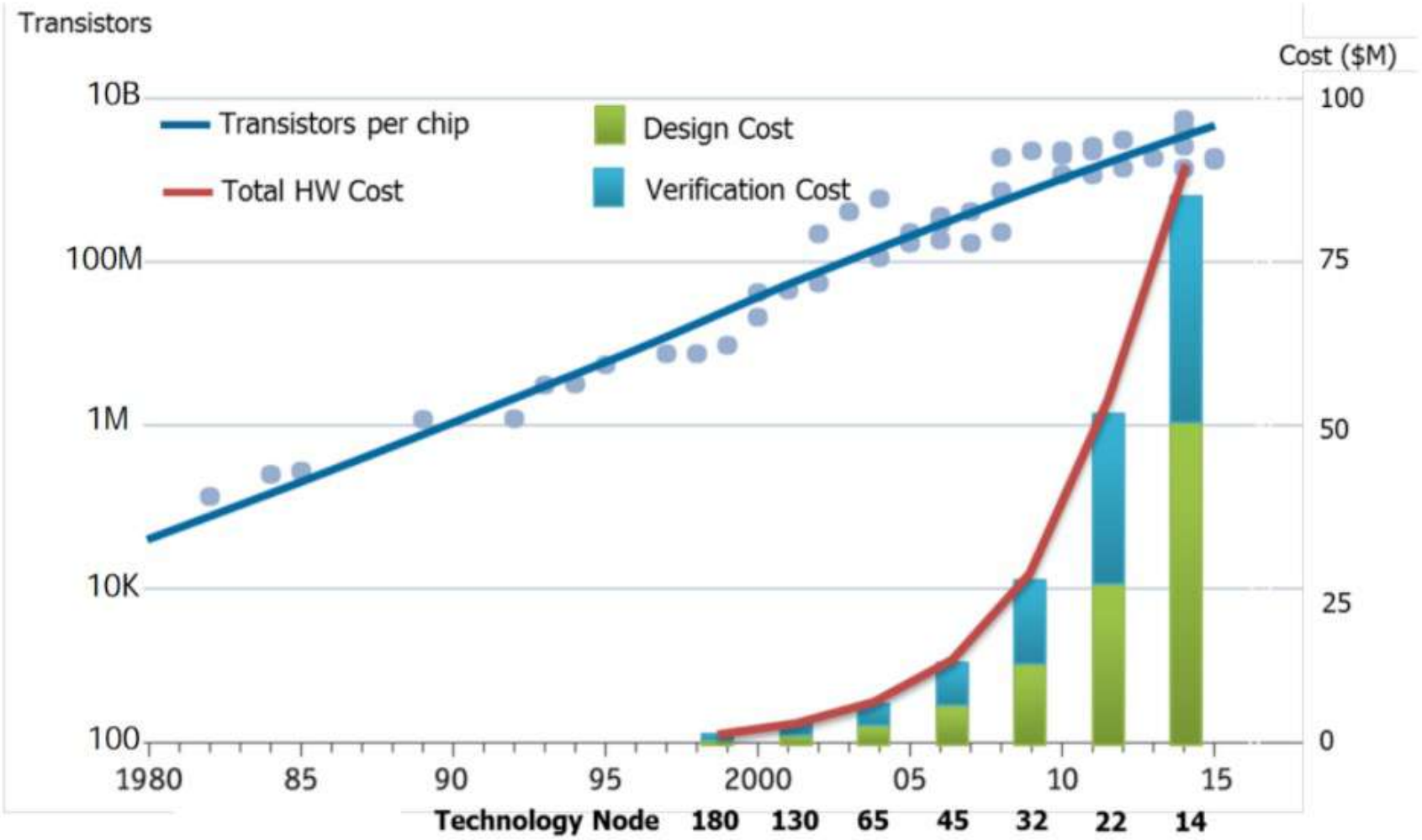
２）DARPAが推進するOpenROADプログラムでは、デジタル設計のためのオープンソースEDAツール（無償）を開発すみである。

３）OpenROAD　EDAツールをデジタル部開発に使用する。原開発者にコンサルティング料を支払いサポートを受けつつ、自助努力でEDAツールを立ち上げる。

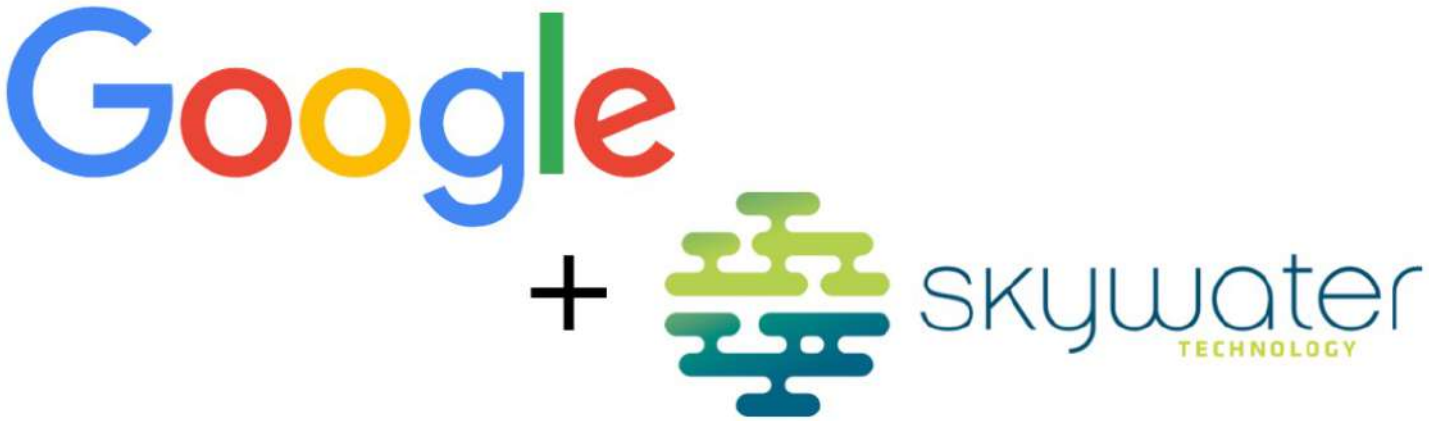
４）アナログIP開発が不要なシステム構成を考えている。

電子システム復興運動（ERI）の背景

DARPA Has EDA failed to keep up with Moore's Law?



プロセスデベロップメントキット



FOSS 130nm Production PDK

github.com/google/skywater-pdk

OpenTitan論理規模 → 16mm2 @ SKY130

１）米国ミシガン州に存在するSkywaterファブの130nmプロセスSKY130を使う。

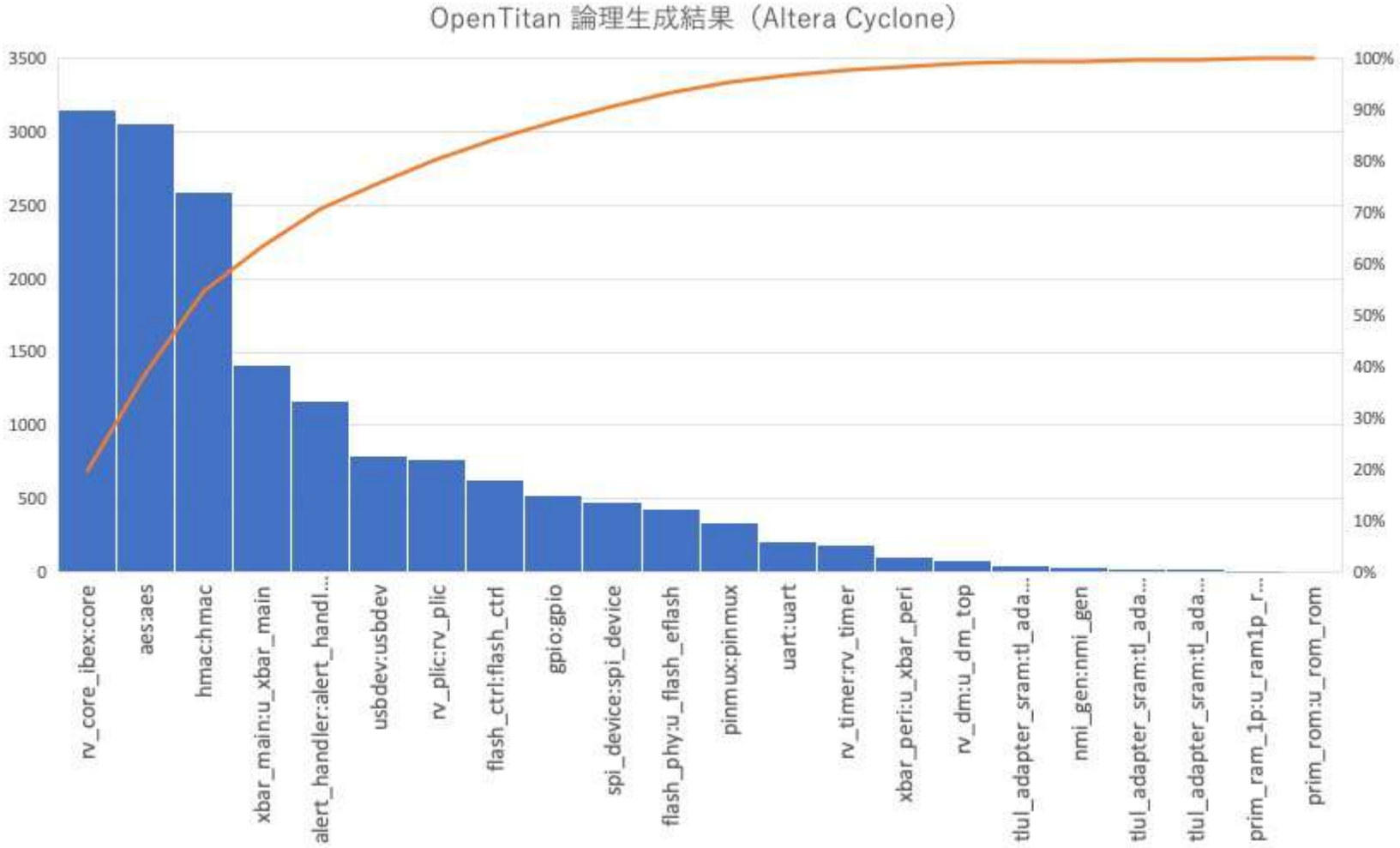
２）OpenTitan論理規模を論理生成しFPGA（Altera）上で動作機能評価した。

３）論理ブロック＋メモリのみで9mm2+（180nmデータから）。

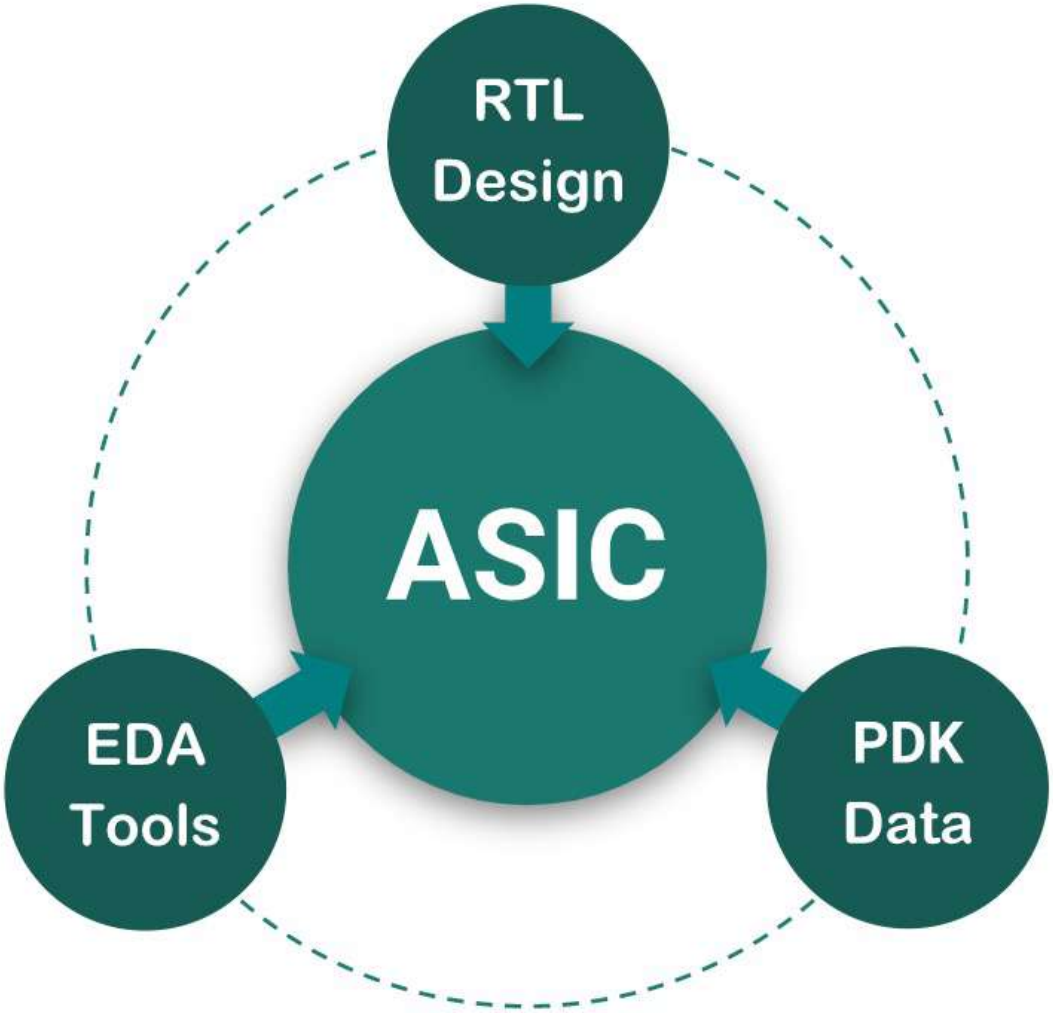
４）TEG、I/O、アナログを入れて16mm2（4mmx4mm）ダイにフィットさせる。

５）チップ実装をする場合には、OpenTitan FPGAを　再調整を行う。

OpenTitan 主要論理ブロック FPGA 規模 単位：ALM換算



オープンソース運動の実態



Google-eFabless Open Silicon

efabless.com

HOW-TO CONTACT MARKETPLACE LOGIN REGISTRATION

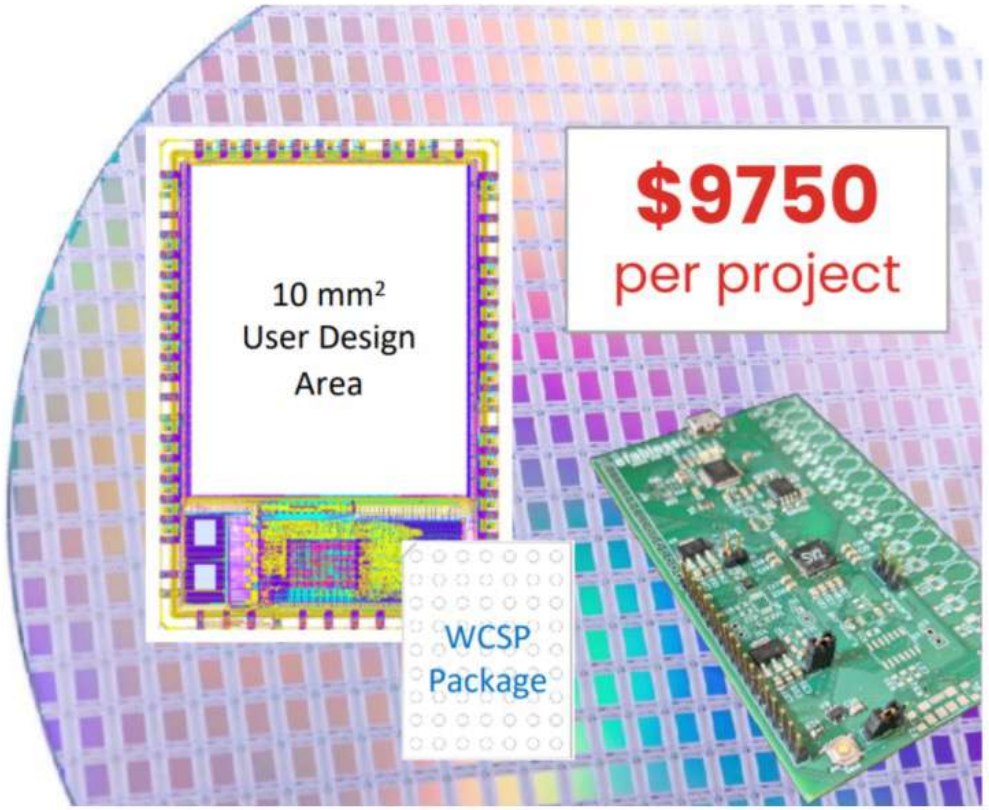
chipIgnite

Rapid IC Creation

Shuttle 2106Q

19 of 40 project slots reserved

Tapeout: June 18
Delivery: Oct 6



マルチプロジェクト ウエハ2乗

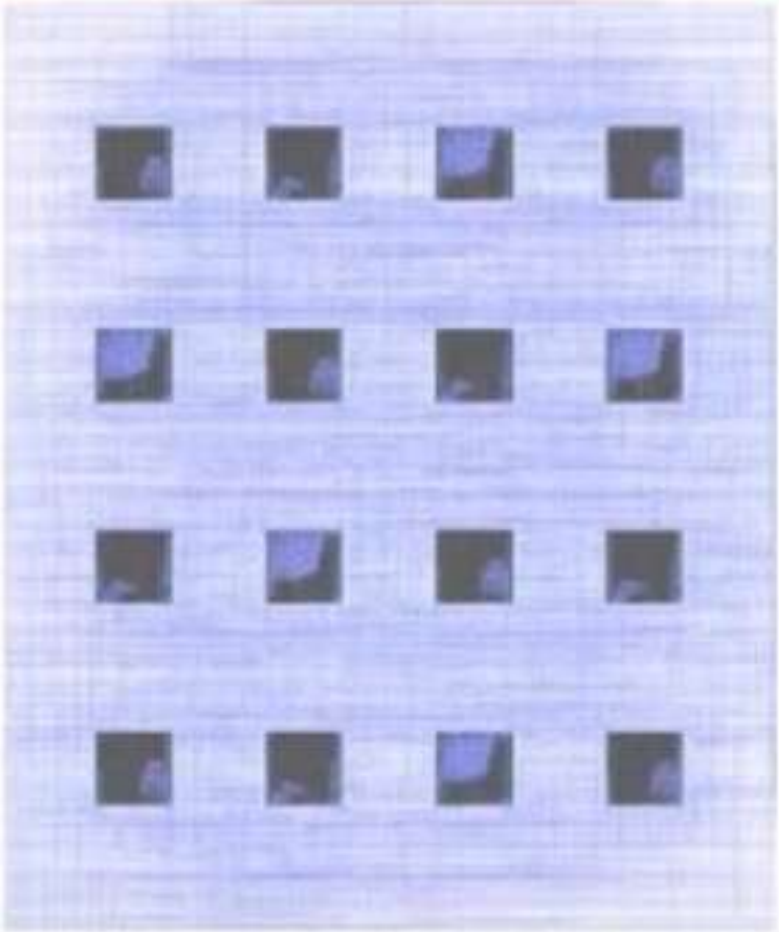
MPW²

github.com/mattvenn/
multi_project_tools

Compatible with
Open MPW *or* chipIgnite
Programs

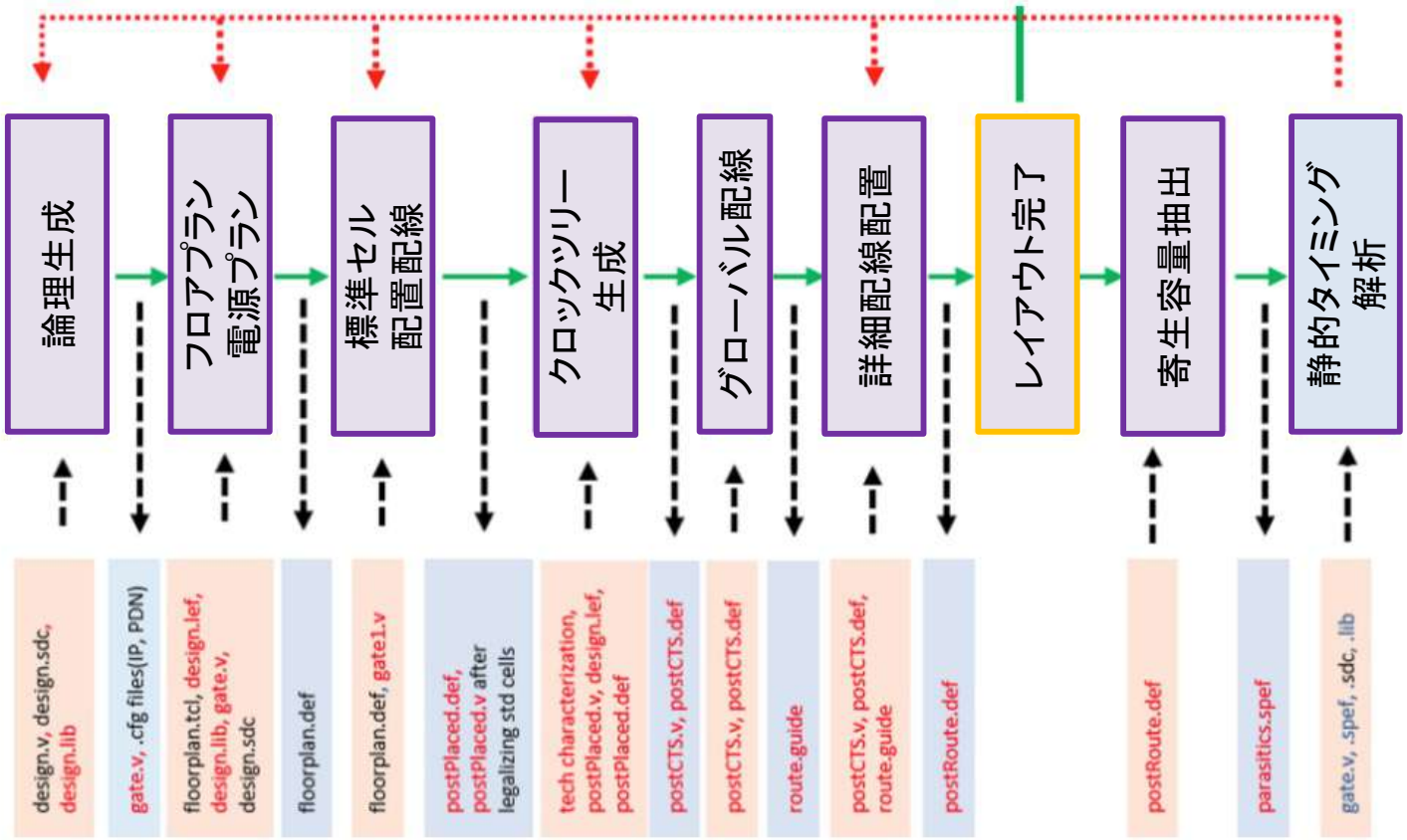
16 projects in one slot

100 ICs ÷ 16 = ~5 ICs each
$9,750 ÷ 16 = ~$610 USD



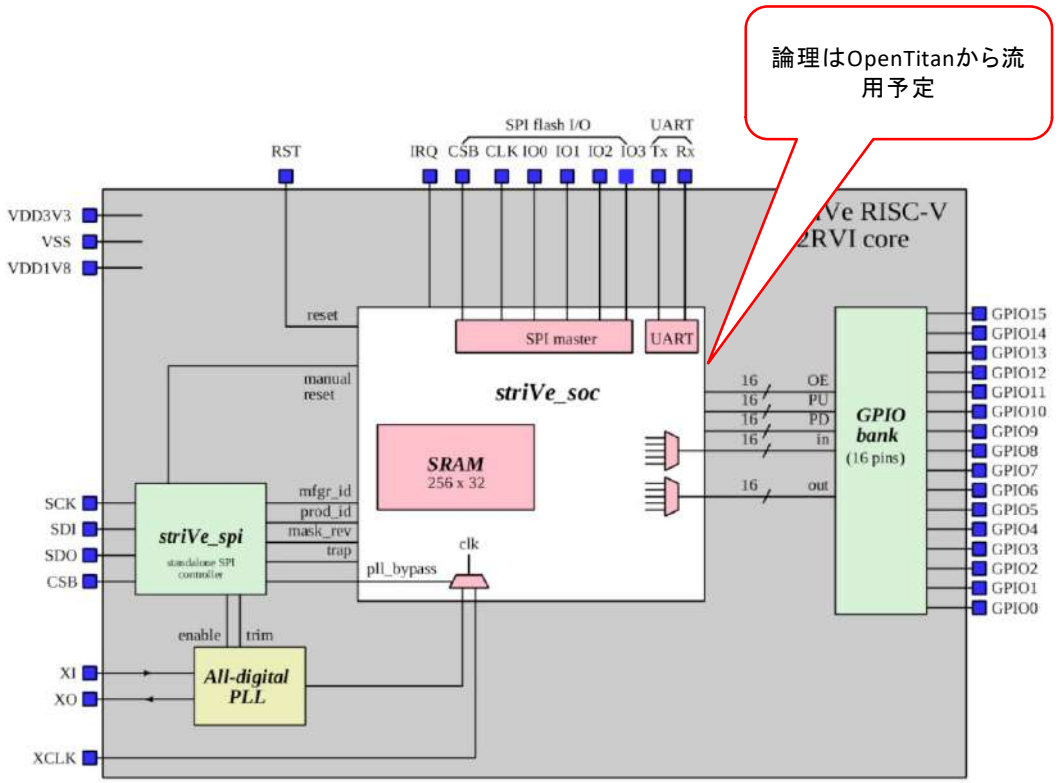
j.mp/oto21-sky130

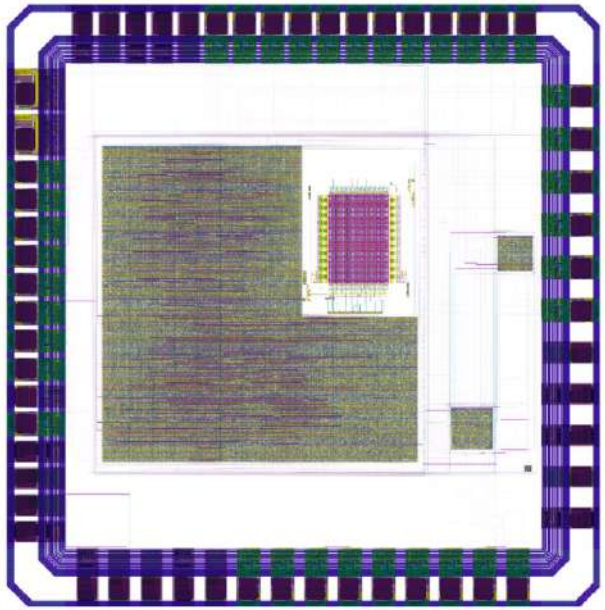
OpenROADによるデジタル設計フロー



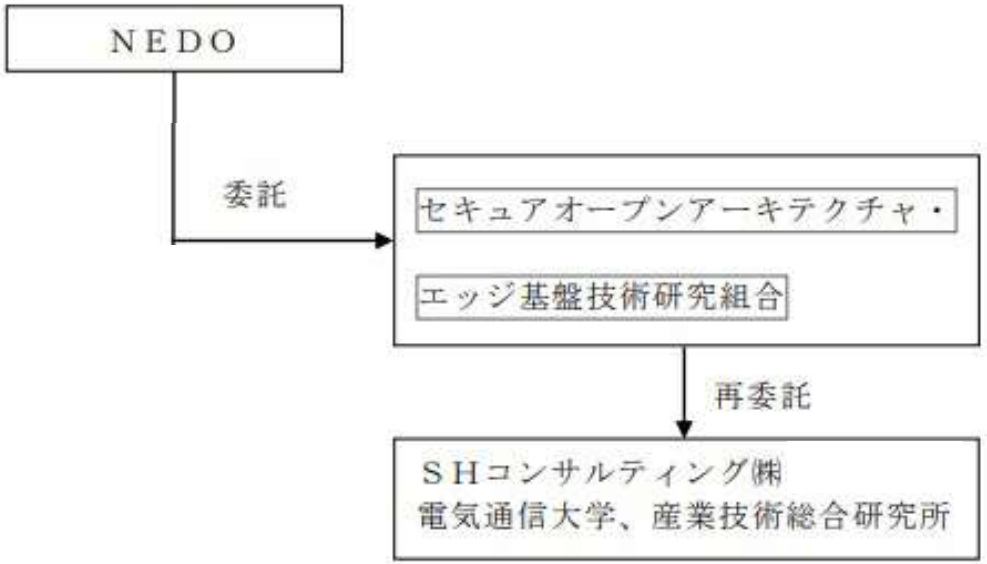
j.mp/du20-sky130

Google-Skywater SKY130プロセスで　オープンソースPDKで作成した　チップ例





実行組織



6. まとめ

1. Linux に対し RTOSは、消費電力が少ないためソーラ、リチウムなどでの電力供給ができる。
2. IoT デバイスセキュリティには、ルートオブトラストチップを集積している。
3. チップ電流測定によるマルウエア検出の可能性を調査している。

4. RTOS　デバイス認証、無線遠隔ソフトアップデート を実現中である。

5. オープンシリコンによるセキュアMCUチップ設計を計画している。

謝辞 この成果は，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)の委託業務(JPNP16007)「セキュ アオープンアーキテクチャ基盤技術とその AI エッジ応用研究開発」の結果得られたものです