PKI Day 2019

午前の部

IoTのトラスト

IoTセキュリティ強化のための技術戦略解説

2019 年　4月　17日

河崎　俊平
SHコンサルティング（株）

発表内容

1. 自己紹介、会社紹介、社会的背景
2. IoTセキュリティ現状
3. オープンソース・セキュリティの技術課題
4. RISC-V紹介
5. オープンソースIoTセキュリティの実装
6. まとめ

1. 自己紹介、会社紹介、社会的背景

質の高いオープンなセキュリティ技術を供与することが必要である

I think what you are working on is important. I don't know of any open source high quality security solutions.

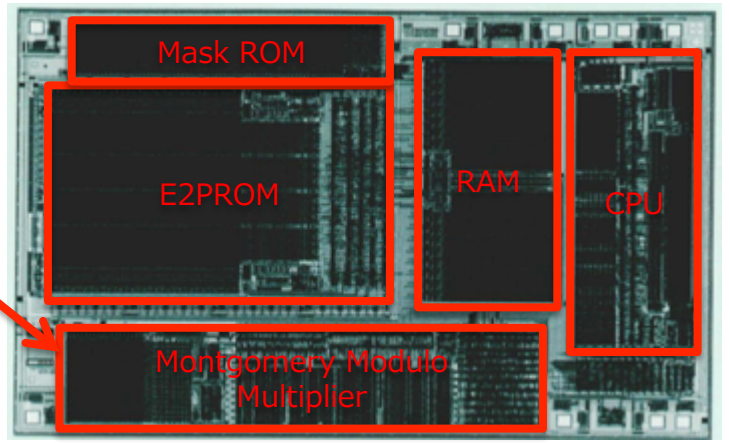
Andreas Olofsson, DARPA Microsystems Technology Office

発表者経歴

1980　モトローラ68K

1986　AIチップ、FPU

世界最初のPKI用チップ
日立製作所 H8/3111
1998



1987-1998 サターン用チップセット

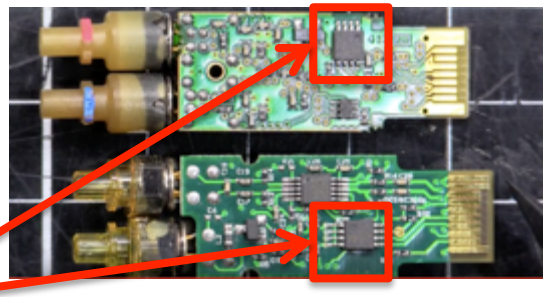
1998-2001 ドリキャス用チップセット

<低迷時代>

2001　米国駐在中に大手電機メーカ退社

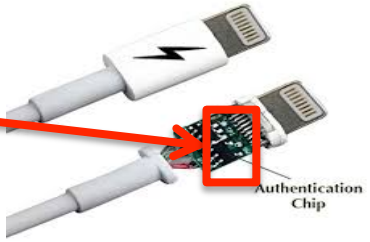
ローカル雇いになる。ソフトに転向。

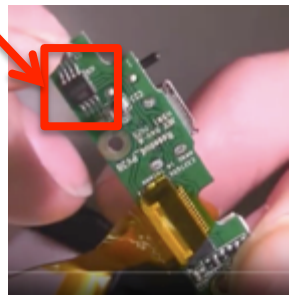
Java Card™ 自前開発



2003　ルータ真贋判定　C暗号ライブラリ開発

2007　北米スマホ大手用　セキュアOS開発





2010　FIPS140-2 Level 3取得

<低迷時代>

2013　大手半導体企業販社退社　SHC社設立

SHC製品

セキュアOS

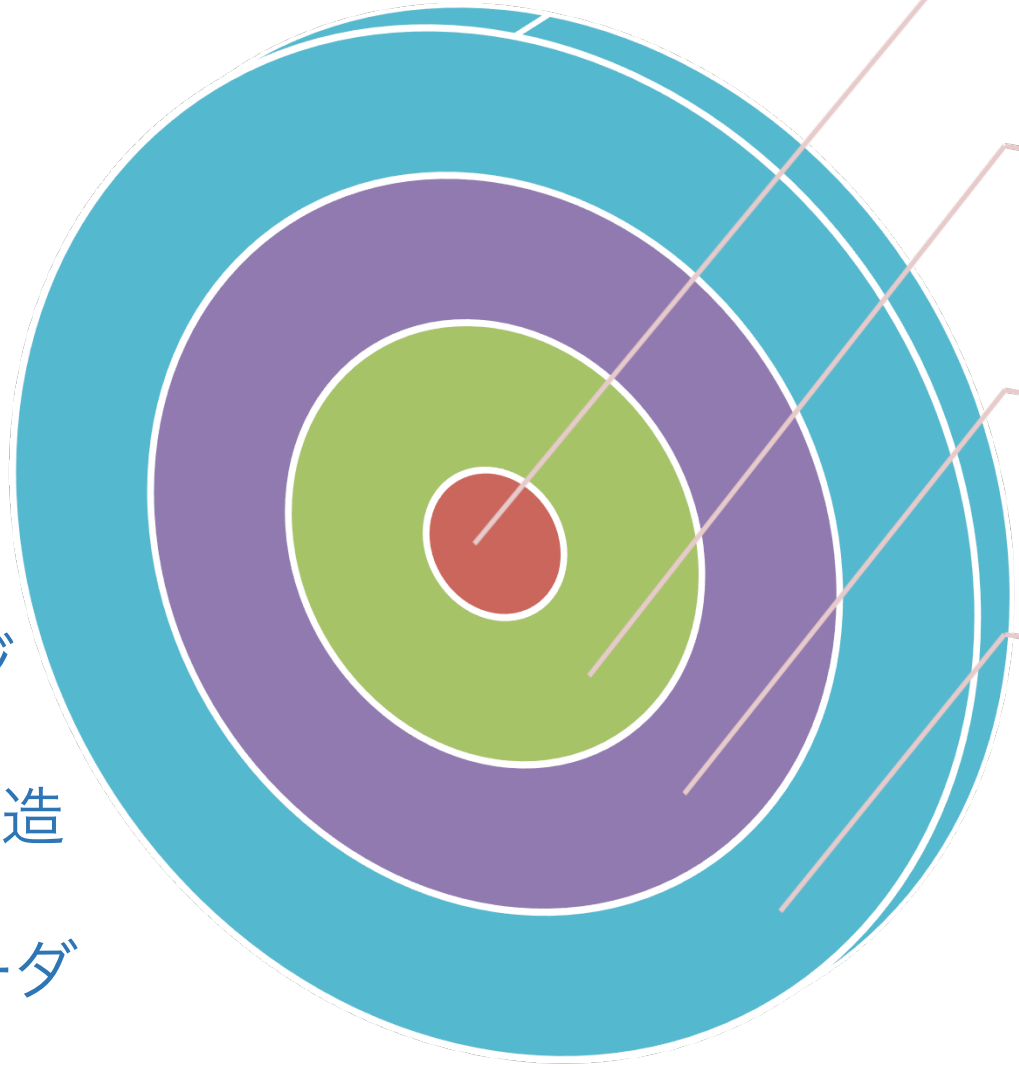
暗号API

無線
e.g. Lora,
BTLE

ボード
サポート
パッケージ

OS 内部構造

ブートローダ



セキュリティ

有線 例.
CANFD

パワーアナログ

32/64-bit
RISC

近代暗号の歴史とオープンソース暗号技術

1970年代には、米政府が暗号研究を発表禁止にする慣行があった。Diffie Whitfieldは、庶民がプライベート情報を護る技術としてDH共通鍵生成アルゴリズム開発を位置づけた。

Making Cryptography Available for the Masses!

というスローガンを掲げ、有名なIEEE論文「New Directions of Cryptography」などを発表、社会運動として宣伝した。

PKI技術を含む自主開発オープンソース暗号実装は、遠からず日本と周辺諸国にとって有用となる時がくると確信している。

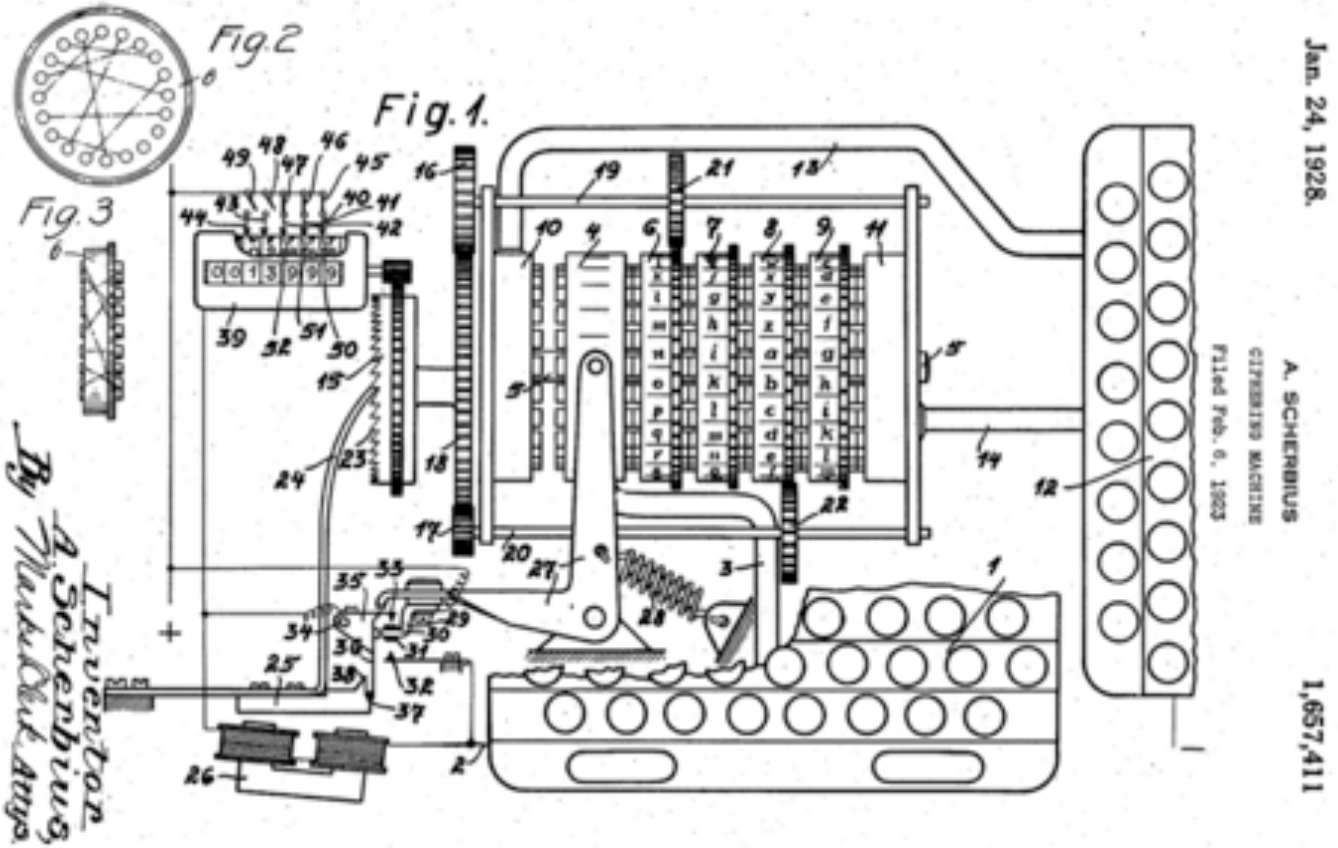
Galois　Turing　Diffie　Hellman　Scherbius　Kerckhoffs

ケルクホフス原理（出展：Wikipedia）

暗号方式は、秘密鍵以外の全てが公知になったとして、なお安全であるべきである。

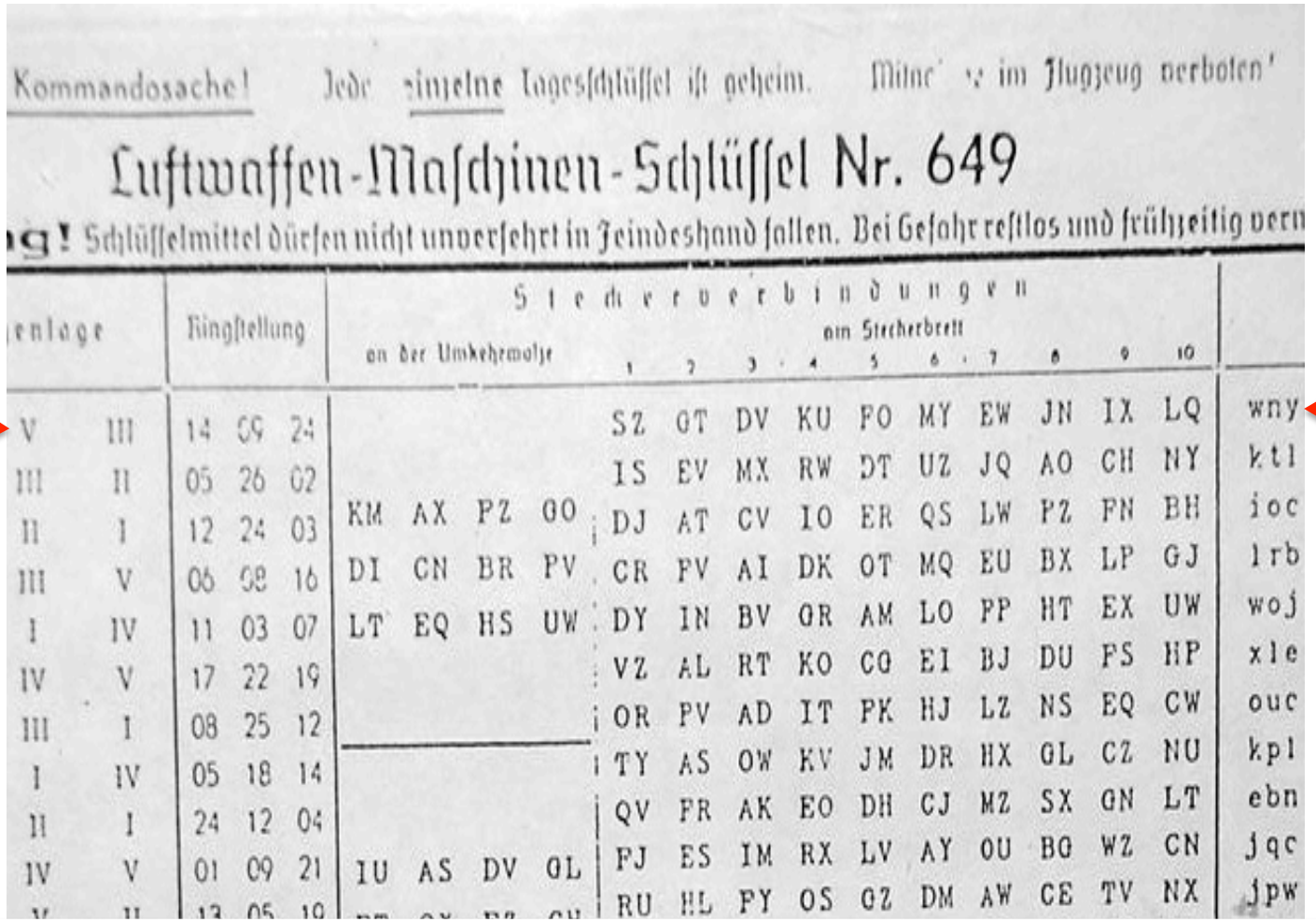
“エニグマ” 暗号方式

- 暗号方式は秘密にしようとしてもスパイによって設計書が盗み出されたり暗号装置ごと敵に捕獲されたりして、遅かれ早かれ敵に解析されてしまうという経験則に基づく。



Arthur
Scherbius 1918

エニグマ鍵管理表（ドイツ軍）



Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitne[illegible] im Flugzeug verboten!

Luftwaffen-Maschinen-Schlüssel Nr. 649

[illegible]g! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vern

Walzenlage		Ringstellung			Steckerverbindungen an der Umkehrwalze				Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	
V	III	14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny
III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl
II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc
III	V	06	08	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb
I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj
IV	V	17	22	19					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle
III	I	08	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc
I	IV	05	18	14					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl
II	I	24	12	04					QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn
IV	V	01	09	21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc
V	II	13	05	19					RU	HL	FY	OS	GZ	DM	AW	CE	TV	NX	jpw

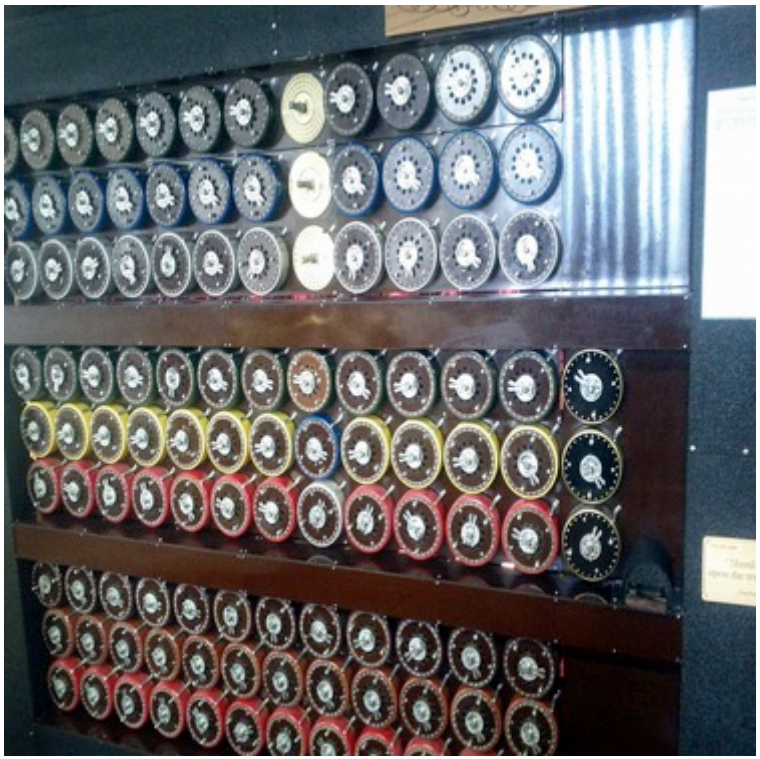
日にち →

← 設定

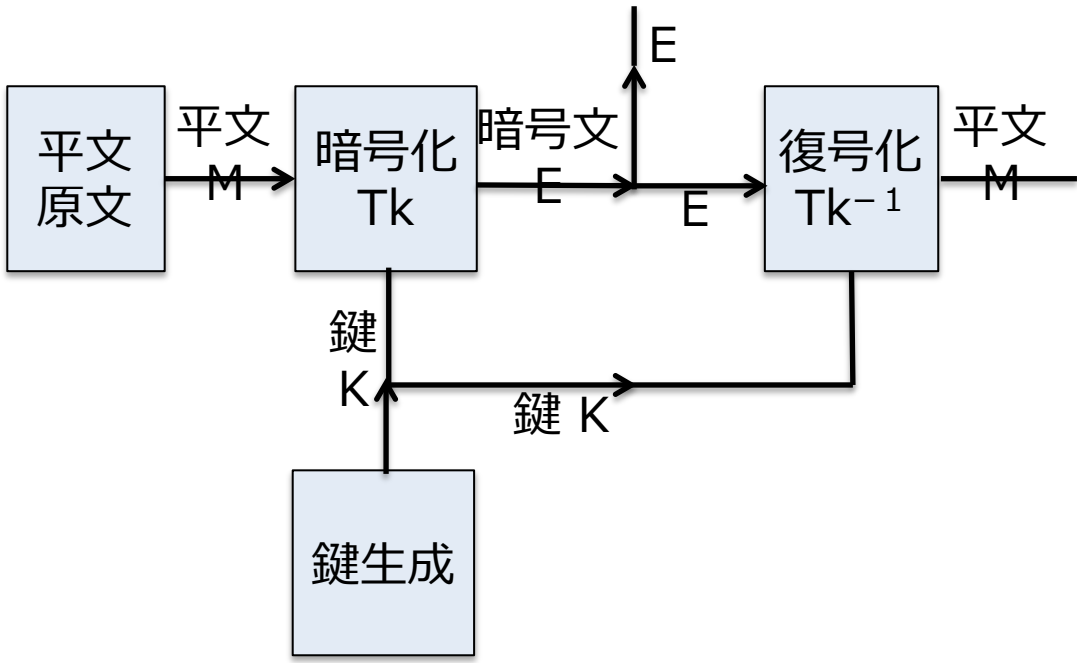
1月分の鍵管理表が配られた。飛行機に鍵管理表を持ち込んではならないとした。
船に持ち込む際は、敵に踏み込まれる前に破壊する決まりだった。

暗号解析マシン「ボンブ」 1941年

敵の暗号解読者



ボンブ



Alan Turing
1941

２。IoTセキュリティの現状

IOTデバイス用SOCデバイスが存在する。

スマートフォンのセキュリティとして存在する。

２０１８年にFIPS-140対応でメガOEMが技術を発表した。

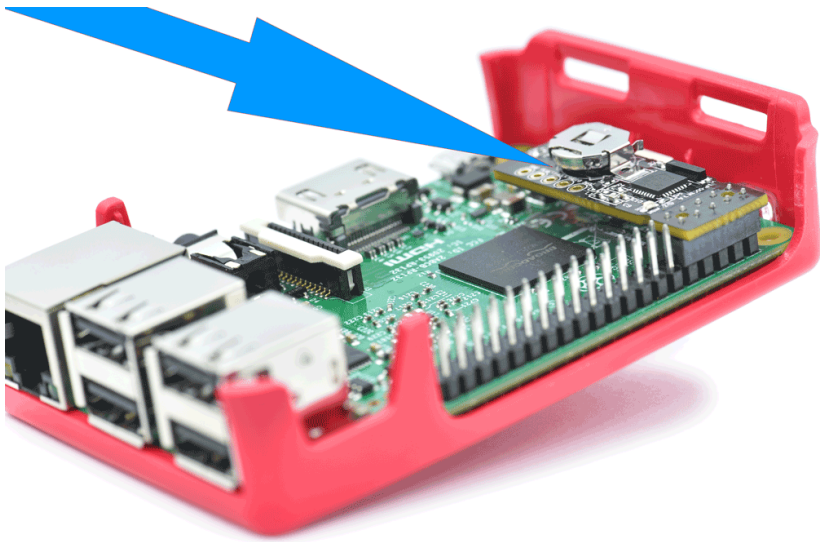
またメガOEMにより、有償OTAサービスの一環として
紐付けされて提供されている。

３つの例を調査してみる。

例１：IoTプラットフォームのセキュリティ

- Raspberry Pi3B
  - E-Fuseでブート手順を決め、ICE接続をディスエーブルする。
  - Raspberry Pi用のAuthentication Deviceが売られる。
- Arduino
  - Lock Fuse機能でFuseの読出書込み機能をディスエーブル
  - 読み書きディスエーブル方式は歴史的経緯から脆弱性も持つと思われ嫌われる。

ATECC608A
CryptoAuthentication™
Device



例2：アップル SEP (CoreCrypto) FIPS140-2 ARM用暗号モジュールv8.0

- SEP = Secure Enclave Processor：アプリプロセッサ（AP）とは完全に隔離された１つのコンピュータシステム。
  - セキュアブート評価（Secure Boot）
    - ブートレコード管理
  - バイオメトリックス情報（Touch ID、Face ID）
  - 電子マネー情報(Suica)

- 採用製品

製品	チップ
iMac	iBridge 2
Apple TV	AIDX Fusion
Apple Watch	SIP
iPad Air/Pro	A8X/A9X
iPhone 5S/6/6S/7/8/X	A7-A10, A11 Bionic

例2：アップルSecure Enclave Processor

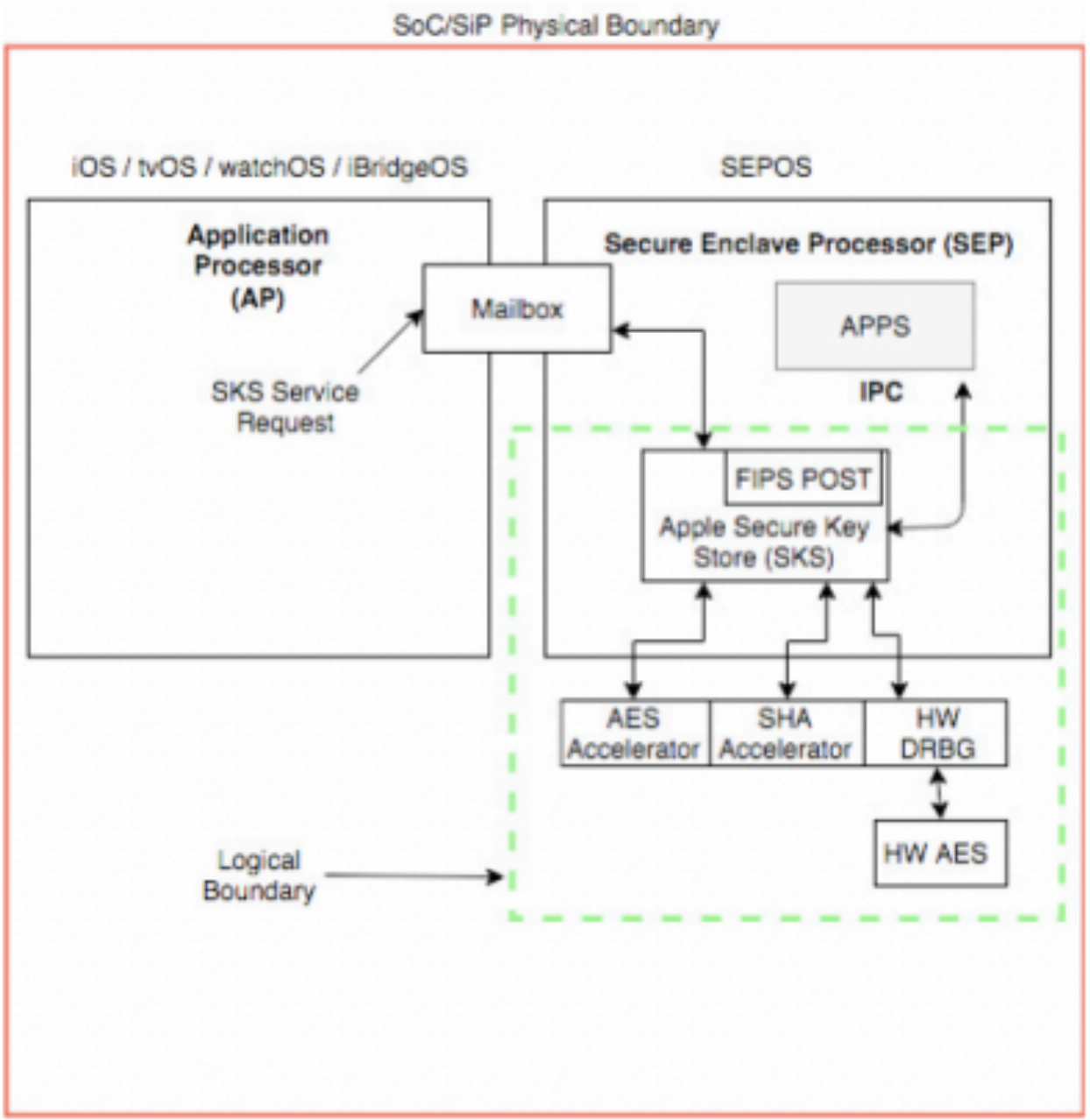
- SEPOS = SEP用OS
- FIPS140-2 Level 1
- 2004-2006年の間セキュアOSを開発。アップル社にライセンス。アップルは他社自社展開。

- 略語

POST = Power-On Self-Test

APPS = Applications

DRBG = Deterministic Random Bit Generator



例2:プロプリエタリ技術への対処方法

オープン実装では独自性保全を積極展開（公開特許調査＝２年）

- US8832465 “Security enclave processor for a system on a chip”
- US9043632B2 “Security enclave processor power control”
- 2012年出願、2014-15年成立。

オープン実装は先行例の複合解で構成。（特許期間=20年）

- 先行設計とは意図的に設計オブジェクティブを変える。
- プロプライエタリ技術とは２年ずらす。オープン実装のライフは長い。

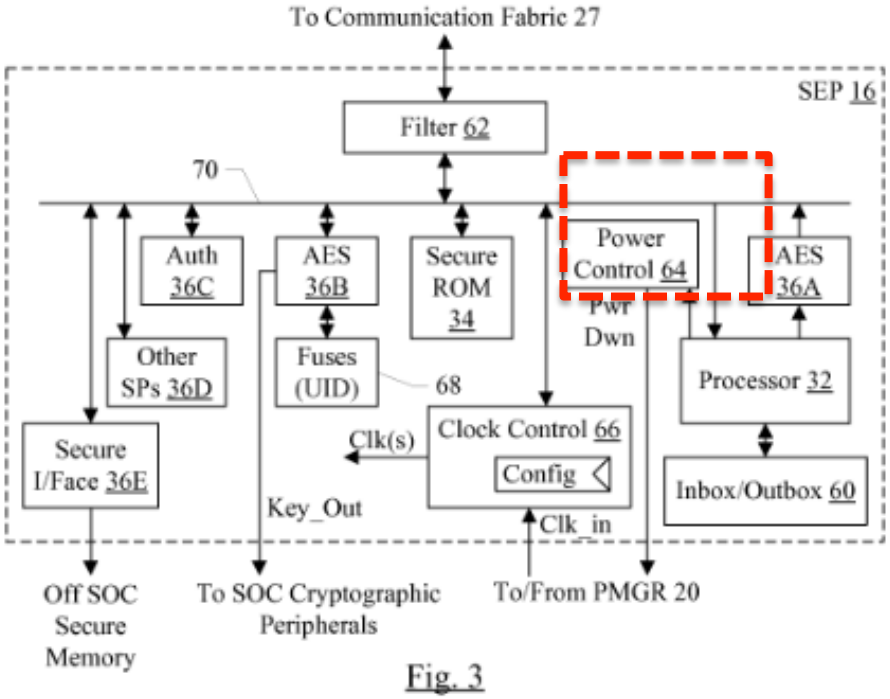


Fig. 3

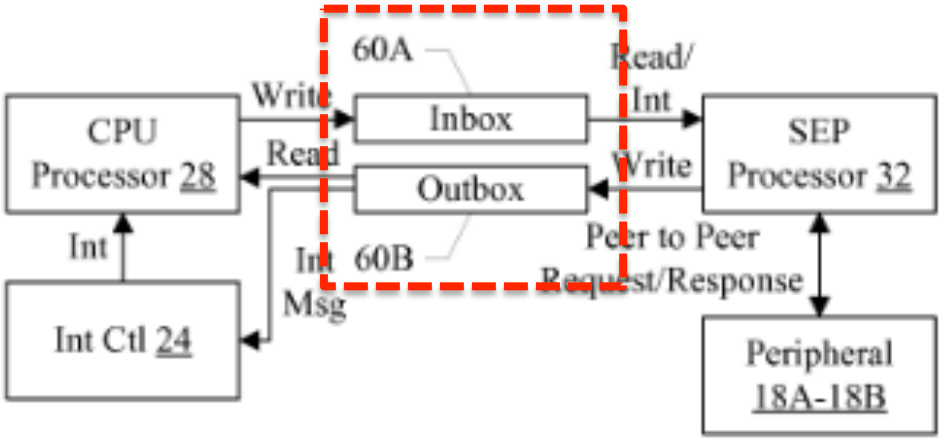
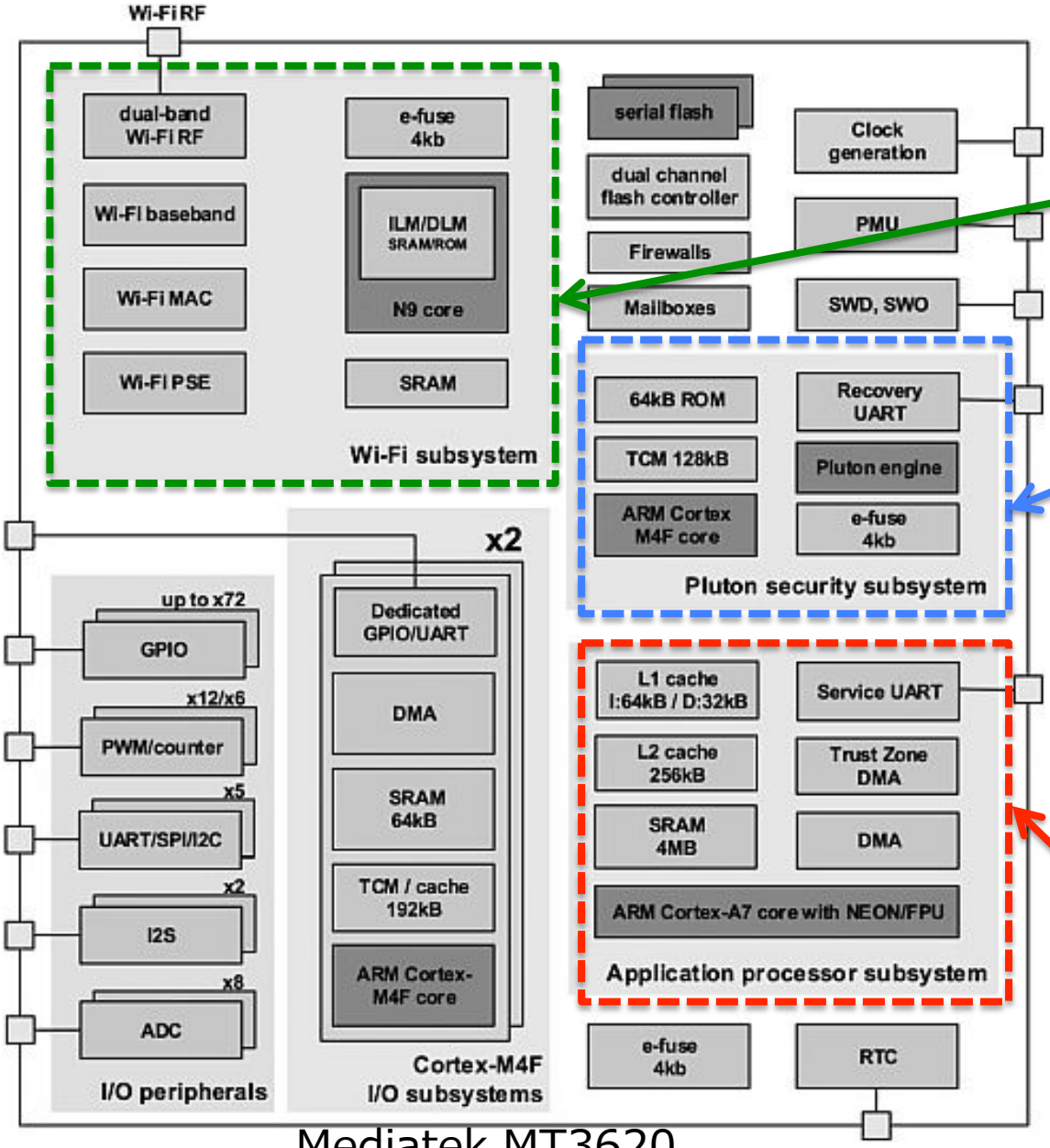


Fig. 4

例３：Azure Sphere用多層防御



Mediatek MT3620

WiFiサブシステム

Pluton
セキュアMCU：
セキュリティモニタ機密をAPからの不法アクセスから保護。

TrustZone
トラスト実行環境
Azure Sphere OS：OS。カスタムLinux

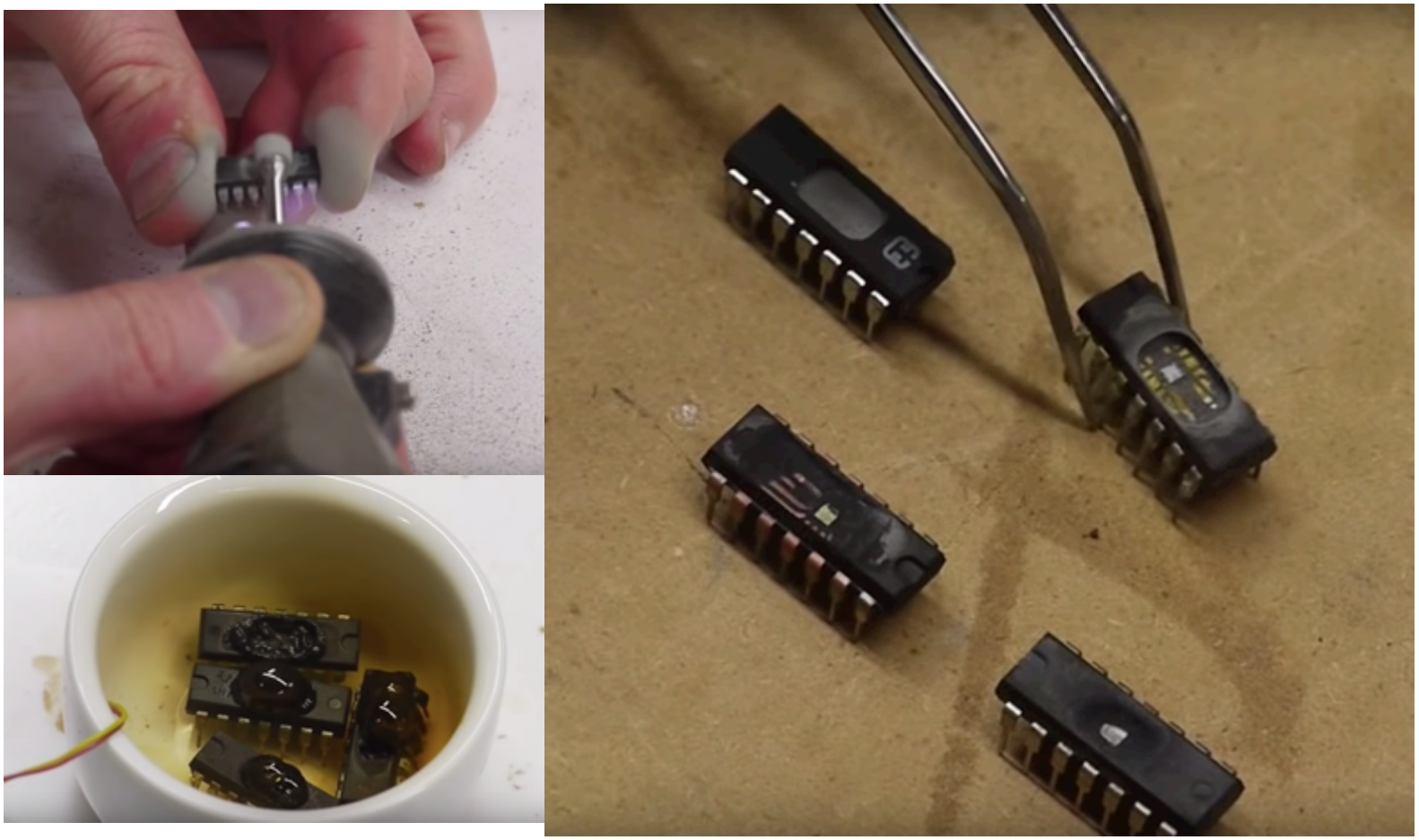
3. セキュリティのオープンソース化に伴う技術課題

実製品や実システムにおいては、ソースコード等を全て公開してしまうと安全性を保証するのが原理的にできない場合や、少なくとも公開しない方が安全性が高いと考える自然人や法人や任意団体等は2018年11月現在の所、まだ多数あり、そのような顧客に対しケルクホフスの原理について解説するのではなく、ケルクホフスの原理に基づかない商品（製品やサービス）を提供するといったような、方式の詳細は未公開な製品やシステムも多い。

出展：WIKIPEDIA

チップ開封テクニック

- チップ開封の処方箋はYoutubeに

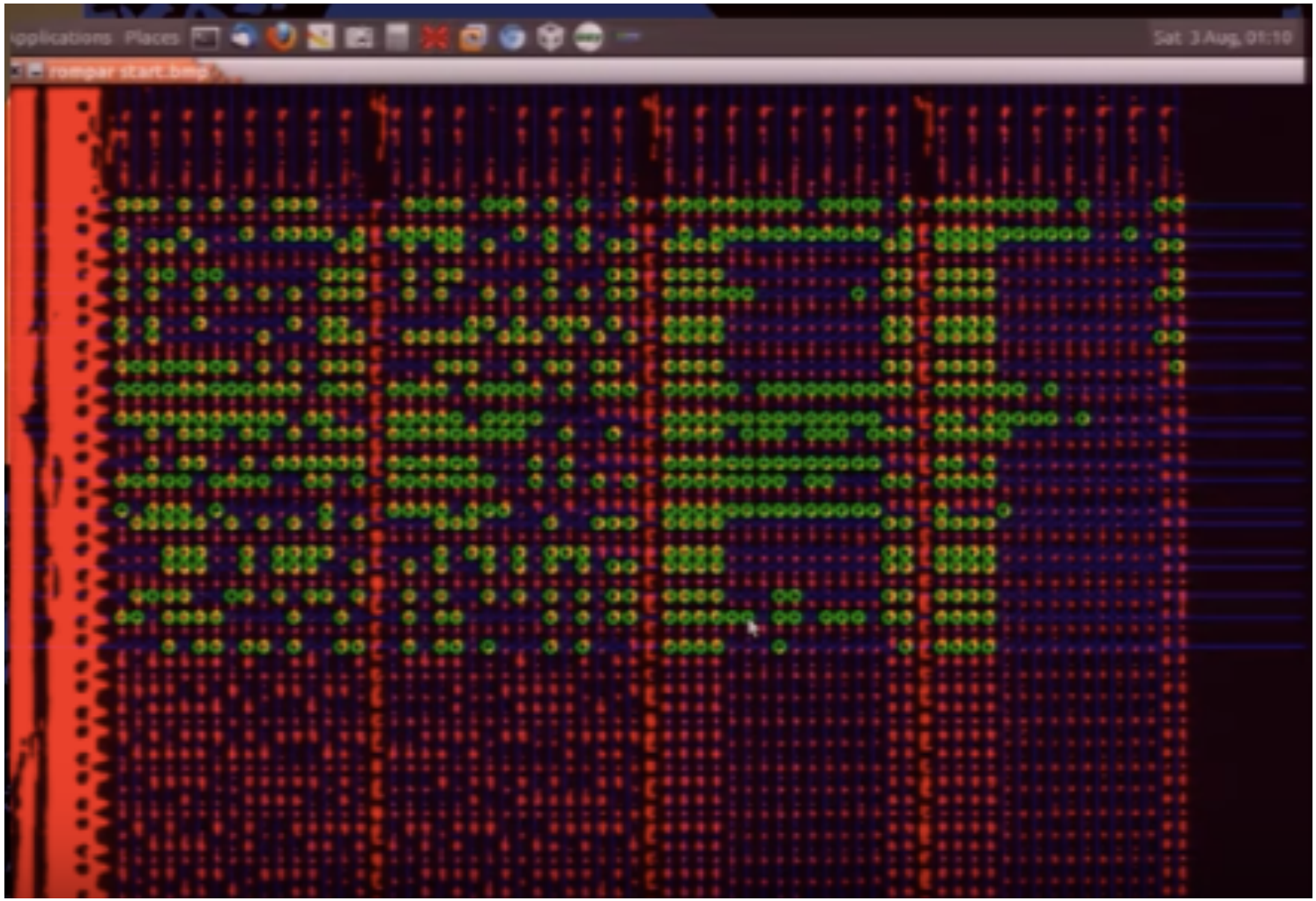


出展：　https://youtu.be/mT1FStxAVz4

マスクROM読み出し

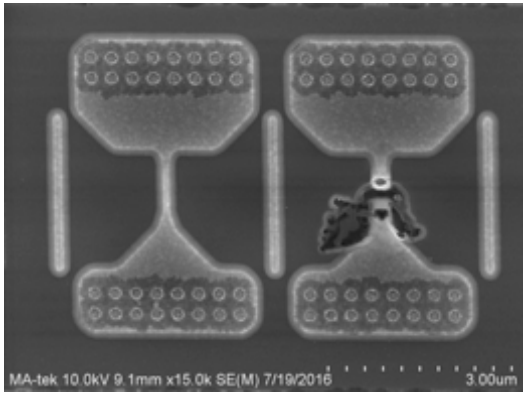
- オープンソースツールも存在。

出展：https://github.com/ApertureLabsLtd/rompar

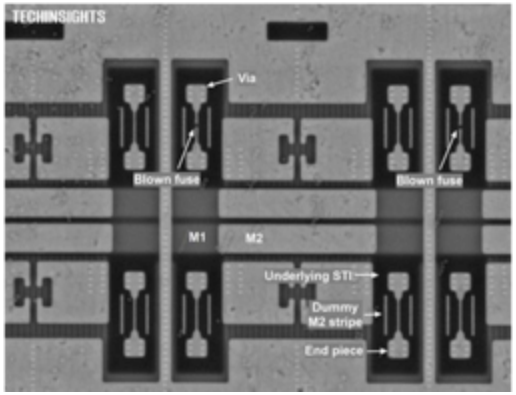


OTP読出し、ヒューズ復元

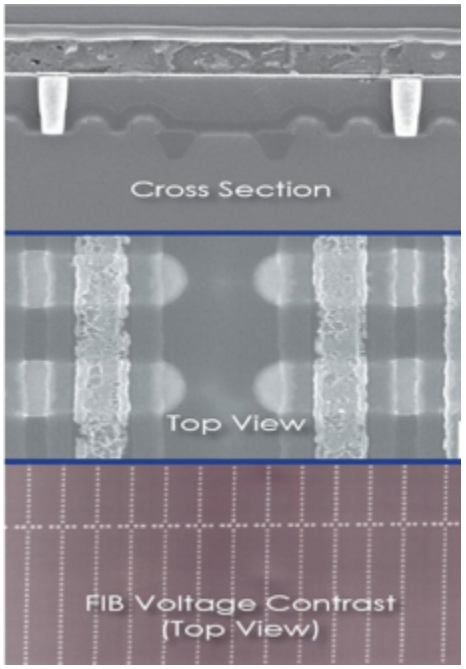
- 高性能SoCに使うOne-Time-Program ROMは、eFuseタイプのもの①②は顕微鏡で読める。③アンチフューズ方式なので顕微鏡では読めないのでより安全。



①



②

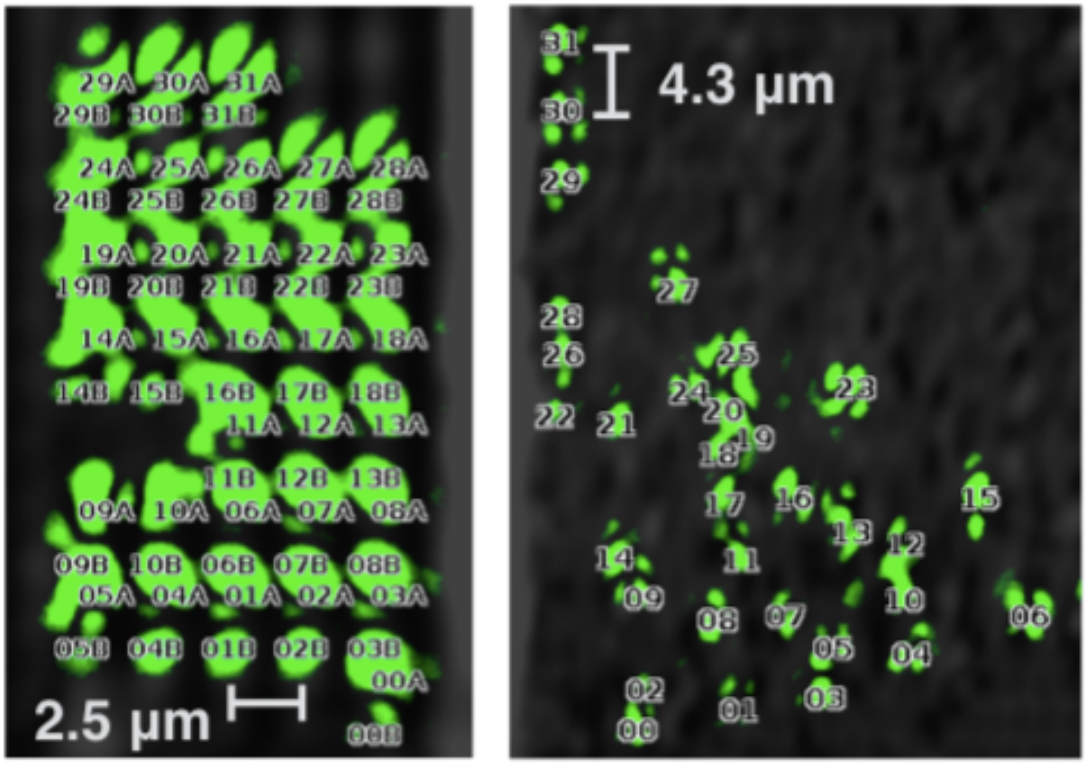


③

- 出展：https://semiengineering.com/the-benefits-of-antifuse-otp/

光学的非接触型プローブ
Optical Contactless Proberによる電圧解析

- HamamatsuPHEMOS-1000故障解析顕微鏡、プロービング光源（Hamamatsu C13193）、光学プロービングプリアンプ（Hamamatsu C12323）を使用。



(a) (b)

出展： https://youtu.be/uAINV-VXuq0
https://eprint.iacr.org/2017/822.pdf

４。RISC-Vの紹介

研究目的でカリフォルニア大学バークレー校（UCB）が
命令セット(ISA)を新規開発した。

2010年より無償で使えるクリーンスレートISAを開発開始。

2014年にRISC-V基金がNPOとして誕生。

RISC-Vはモジュラ方式で32/64/128ビットで全応用領域をカバー

モジュラーアーキテクチャ使用例

Linuxを実行できるマシンとするには、
①レジスタ長（XLEN)＝64ビット。
②命令群としてG(汎用命令群）＝
Ｉ（整数）+M（乗算）+A（アトミック）
+F（単精度浮動小数点）
+D（倍精度浮動小数点）
＋ C（圧縮命令）を選択。
④特権モード構成は、
３レベル（３）を選択。
M（マシンレベル）
S（スーパバイザレベル）
U（ユーザレベル）
をサポートする。

MXL	XLEN
1	32
2	64
3	128

①レジスタ長の指定

Table 3.1: Encoding of MXL field in `misa`

Level	Encoding	Name	Abbreviation
0	00	User/Application	U
1	01	Supervisor	S
2	10	*Reserved*	
3	11	Machine	M

特権モード定義

Table 1.1: RISC-V privilege levels.

Number of levels	Supported Modes	Intended Usage
1	M	Simple embedded systems
2	M, U	Secure embedded systems
3	M, S, U	Systems running Unix-like operating systems

④特権モード構成の指定

Table 1.2: Supported combinations of privilege modes.

Subset	Name
Standard General-Purpose ISA	
Integer	I
Integer Multiplication and Division	M
Atomics	A
Single-Precision Floating-Point	F
Double-Precision Floating-Point	D
General	G = IMAFD
Standard User-Level Extensions	
Quad-Precision Floating-Point	Q
Decimal Floating-Point	L
16-bit Compressed Instructions	C
Bit Manipulation	B
Dynamic Languages	J
Transactional Memory	T
Packed-SIMD Extensions	P
Vector Extensions	V
User-Level Interrupts	N
Non-Standard User-Level Extensions	
Non-standard extension “abc”	Xabc
Standard Supervisor-Level ISA	
Supervisor extension “def”	Sdef
Non-Standard Supervisor-Level Extensions	
Supervisor extension “ghi”	SXghi

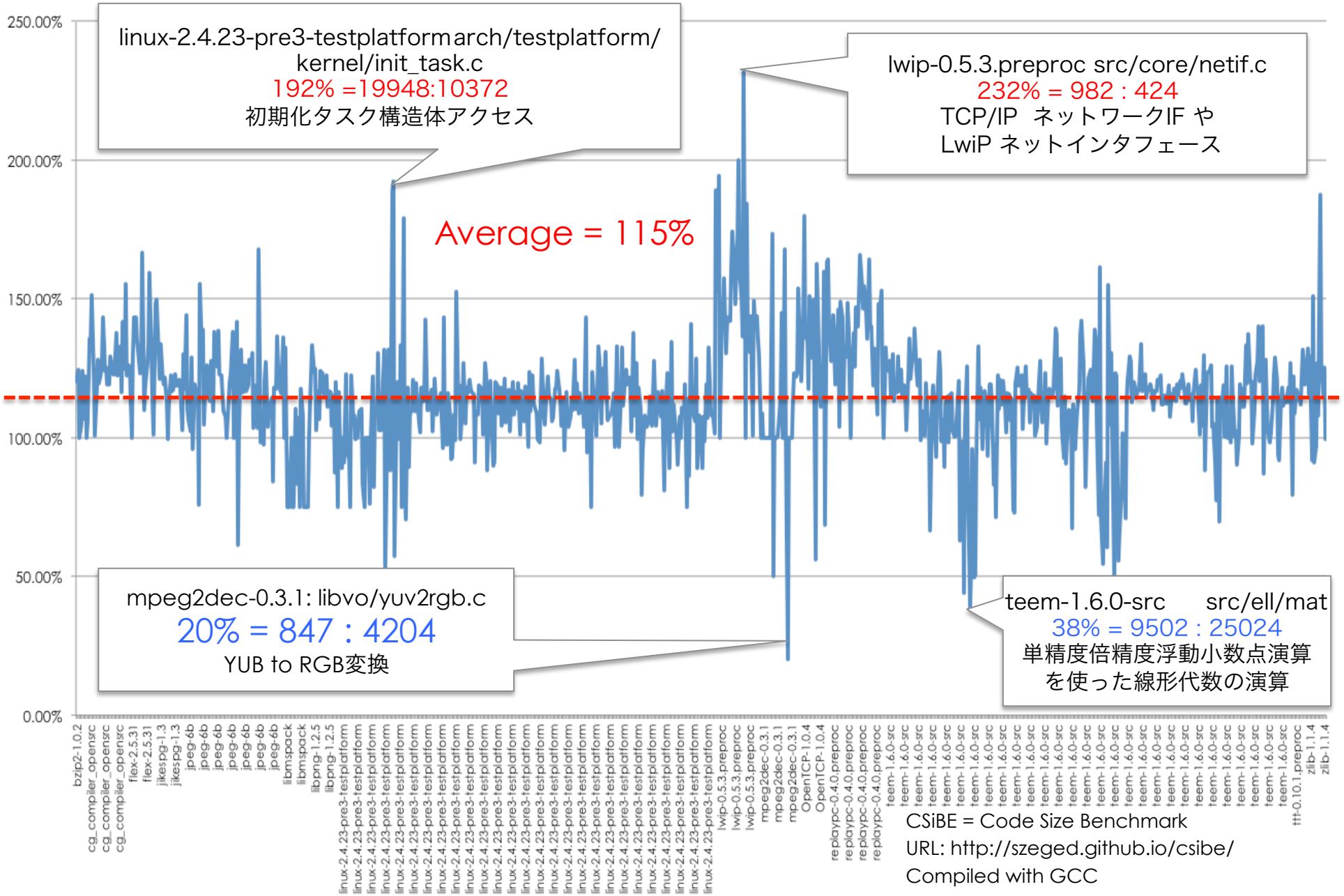
汎用命令群G

圧縮命令C

②命令群の指定

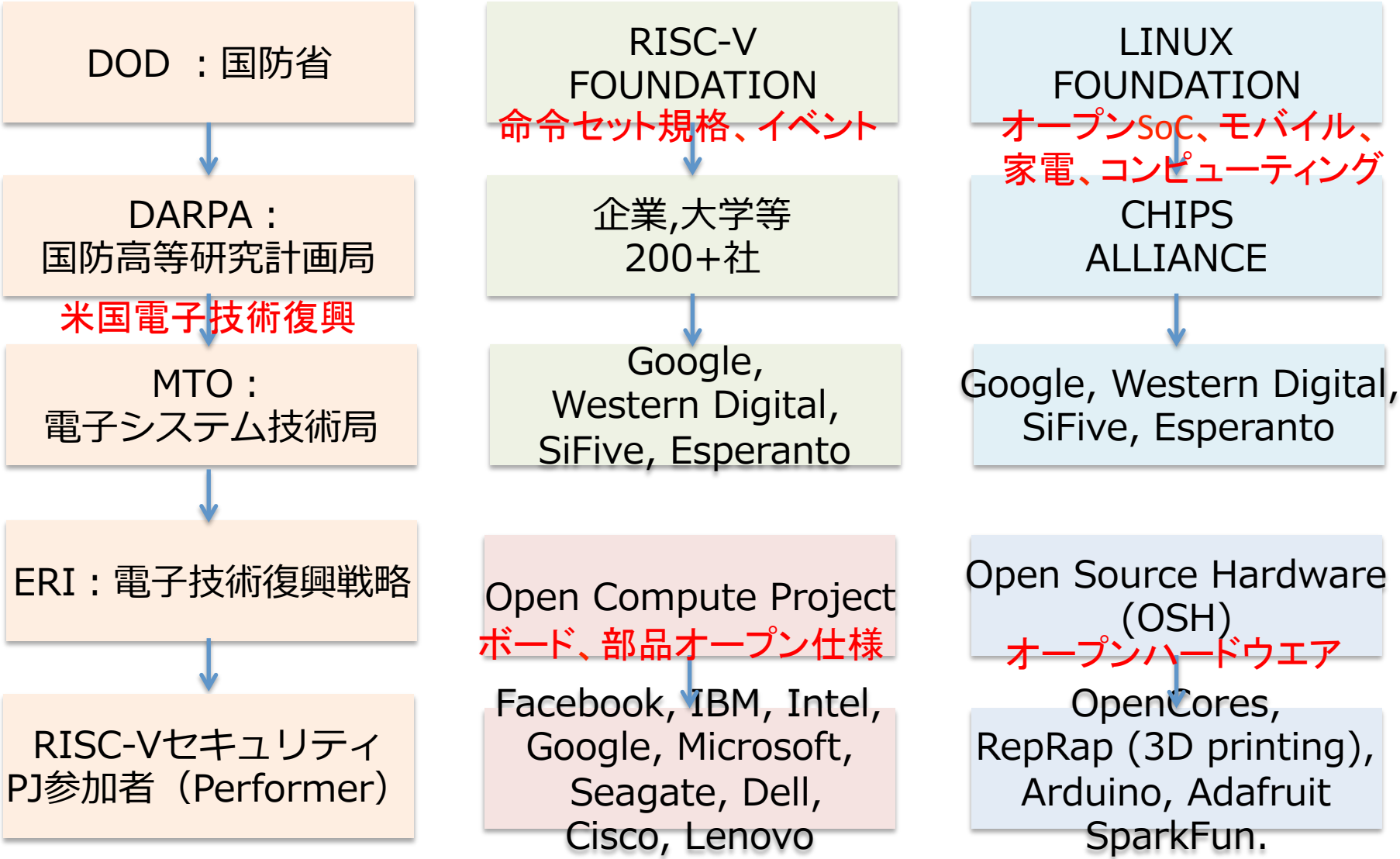
Table 22.1: Standard ISA subset names.

RISC-V コード密度（RV64GC vs. ARM M0）

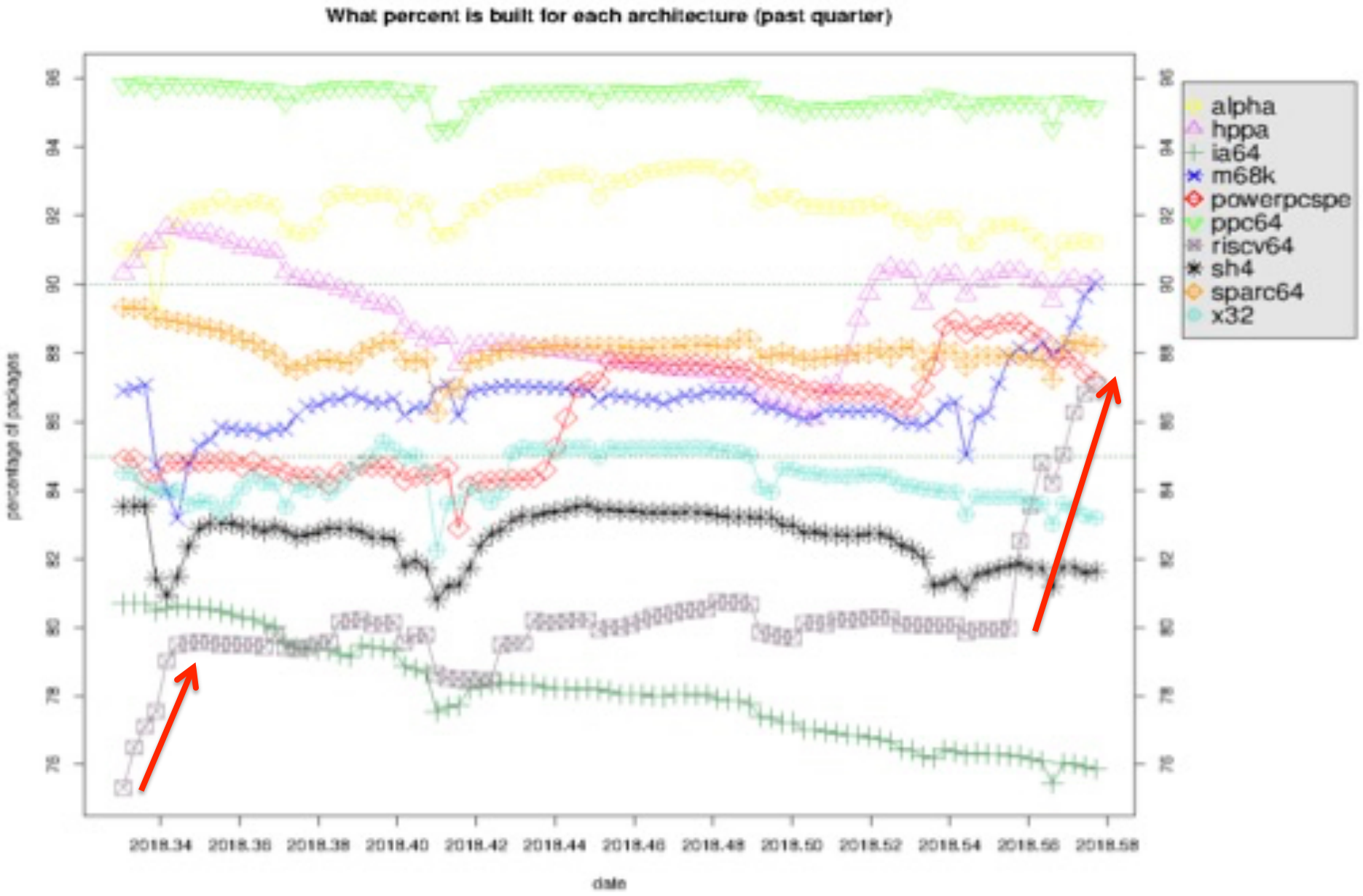


CSiBE = Code Size Benchmark
URL: http://szeged.github.io/csibe/
Compiled with GCC

RISC-Vと関連組織


DOD ：国防省
DARPA：
国防高等研究計画局
米国電子技術復興
MTO：
電子システム技術局
ERI：電子技術復興戦略
RISC-Vセキュリティ
PJ参加者（Performer）
RISC-V
FOUNDATION
命令セット規格、イベント
企業,大学等
200+社
Google,
Western Digital,
SiFive, Esperanto
Open Compute Project
ボード、部品オープン仕様
Facebook, IBM, Intel,
Google, Microsoft,
Seagate, Dell,
Cisco, Lenovo
LINUX
FOUNDATION
オープンSoC、モバイル、
家電、コンピューティング
CHIPS
ALLIANCE
Google, Western Digital,
SiFive, Esperanto
Open Source Hardware
(OSH)
オープンハードウエア
OpenCores,
RepRap (3D printing),
Arduino, Adafruit
SparkFun.

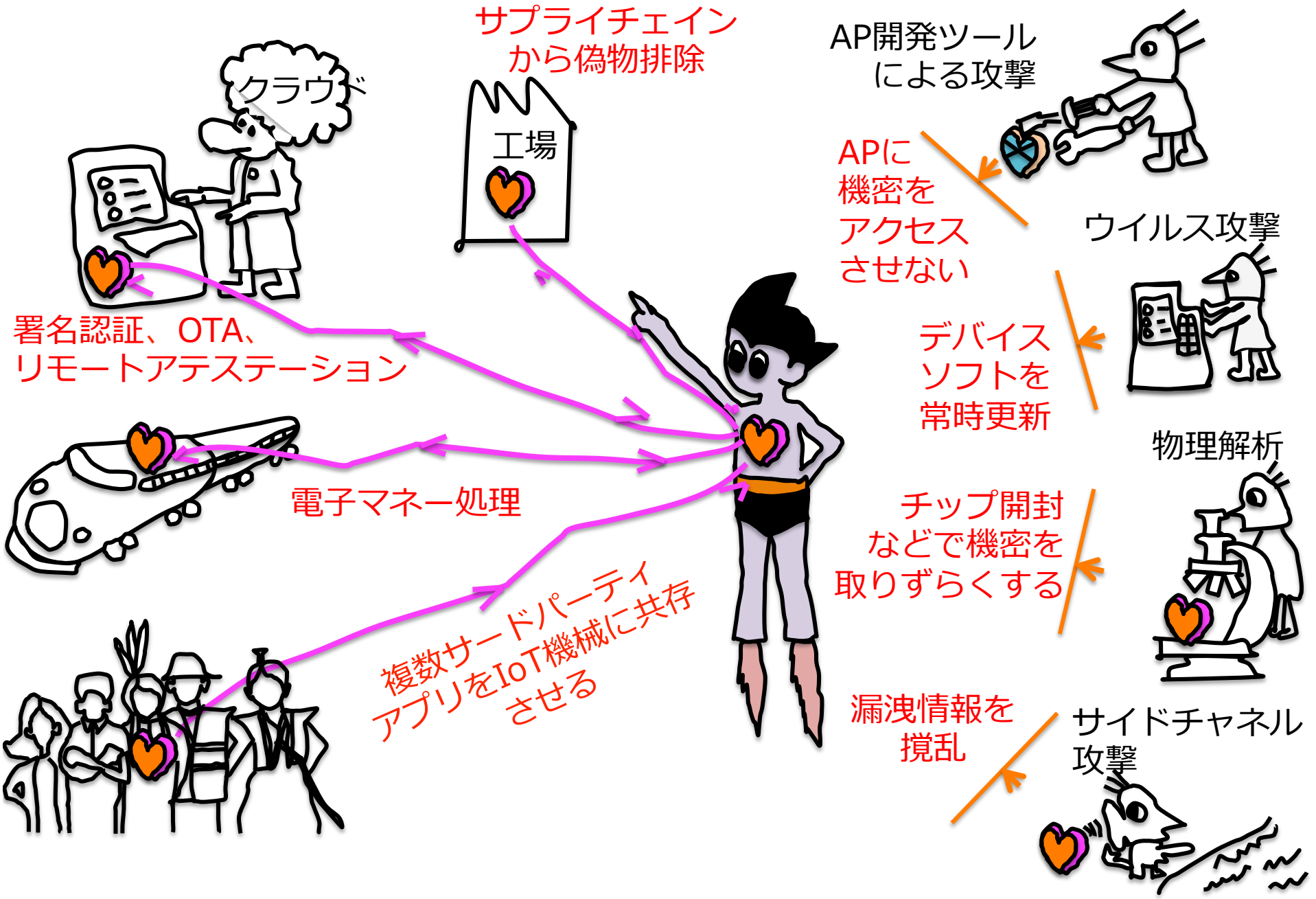
RISC-VのLinuxパッケージビルド成功率改善



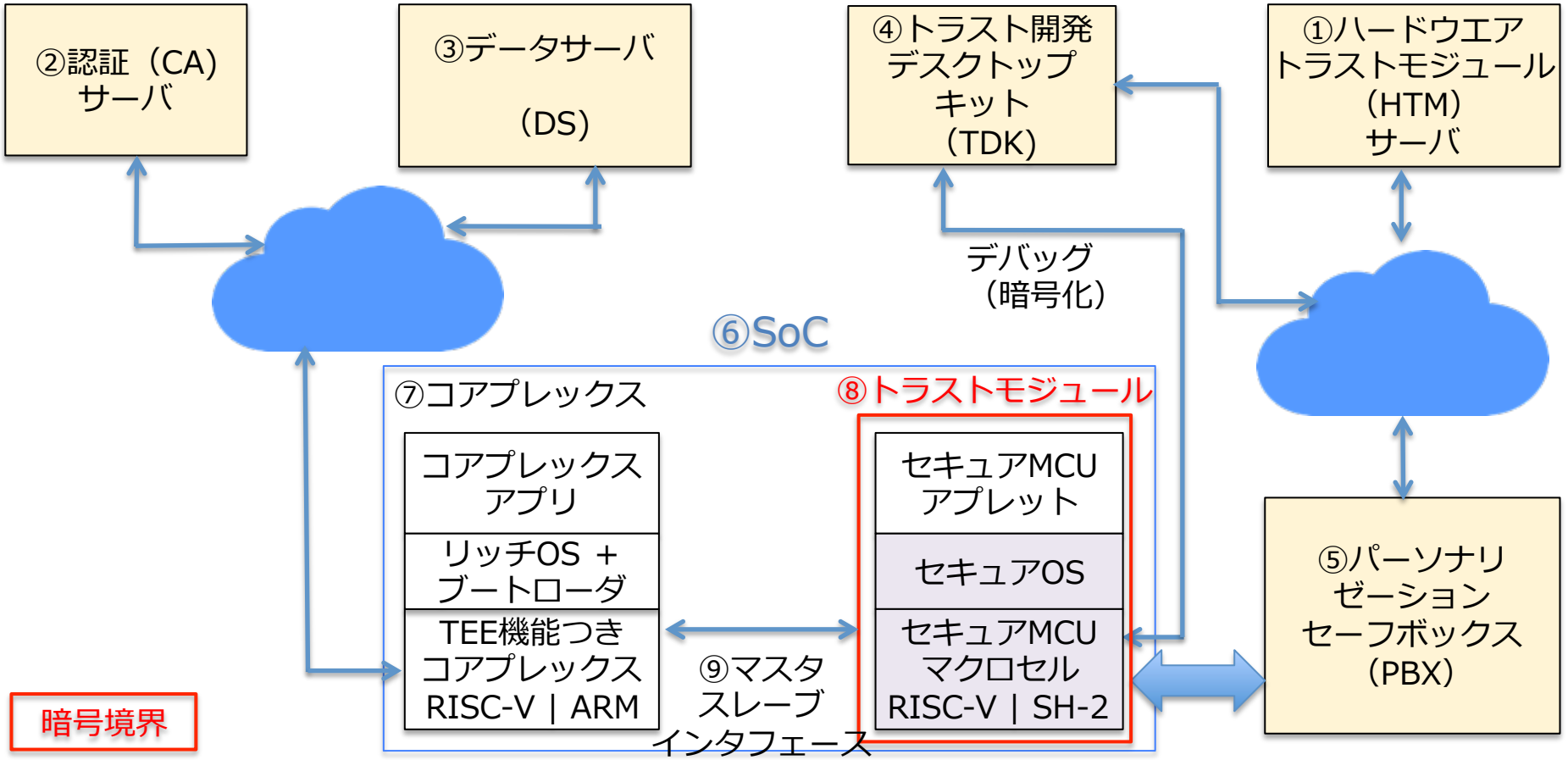
5。オープンセキュリティ

ホワイトボックスとオープンソースの違い
ホワイトボックスはソフトウェアに埋め込まれた機密情報（A暗号鍵等）を暗号化して強力に保護する。攻撃者が動的解析をして、ソフトウェアの中身をみたとしても、機密情報を見ることのできないように、ソフトウェアをソースコードレベルで変換します。動作速度は低下するが、機密情報は隠ぺいされる。どんなタイミングで、メモリ空間のどこを見ても、機密情報を見ることはできない。

IoTセキュリティのビジョン



トラストモジュールサービス環境



モジュール説明

①ハードウェアトラストモジュール（HTM）サーバ：固有鍵を生成しパーソナリゼーションサーバと共に家具注入する。

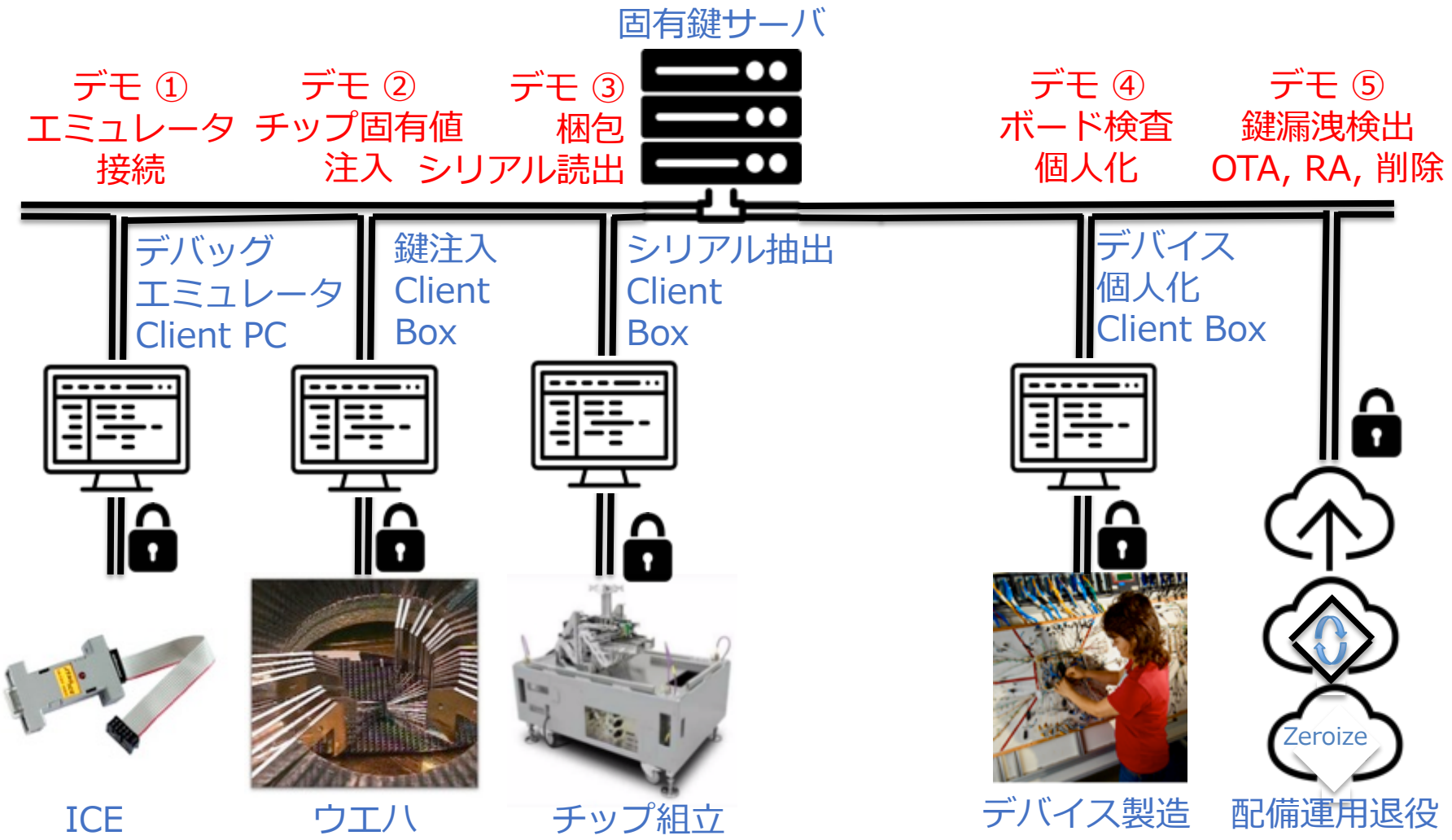
⑤パーソナリゼーションボックス：トラストモジュールに鍵およびその他のパーソナライゼーションデータを直接注入するためのインターフェースを備え、HTMと交信するセーフボックス。

②認証サーバ：トラストモジュールが生成したデジタル署名を検証、真贋判定する。

③データサーバ：セキュアチャネルを使用してトラストモジュールと通信する。

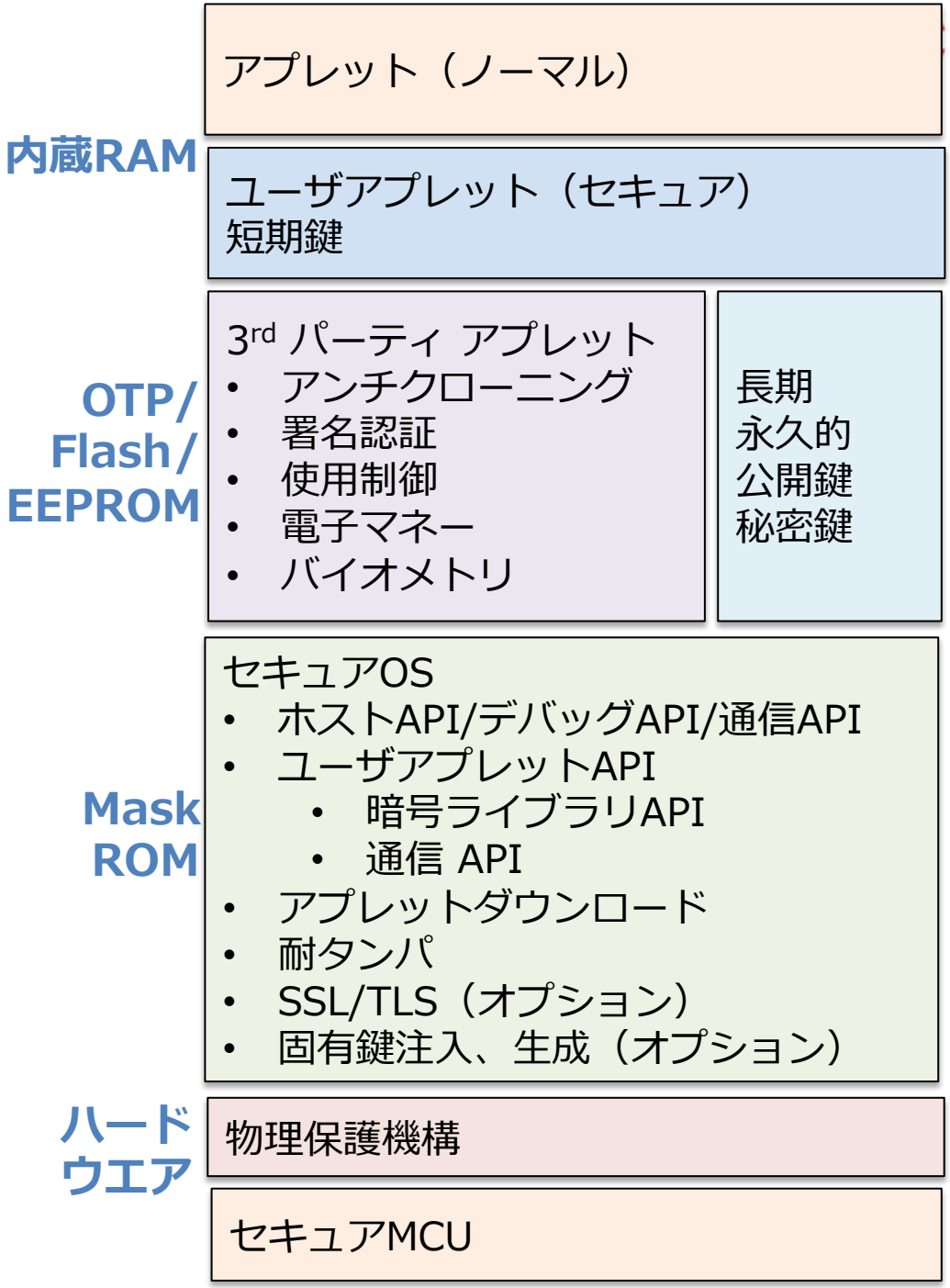
④トラストデスクトップ開発システム：トラストモジュール用アプレットを開発する。コアプレックス用アプリを開発するための開発プラットフォーム。

チップサプライチェーンと固有鍵インフラ

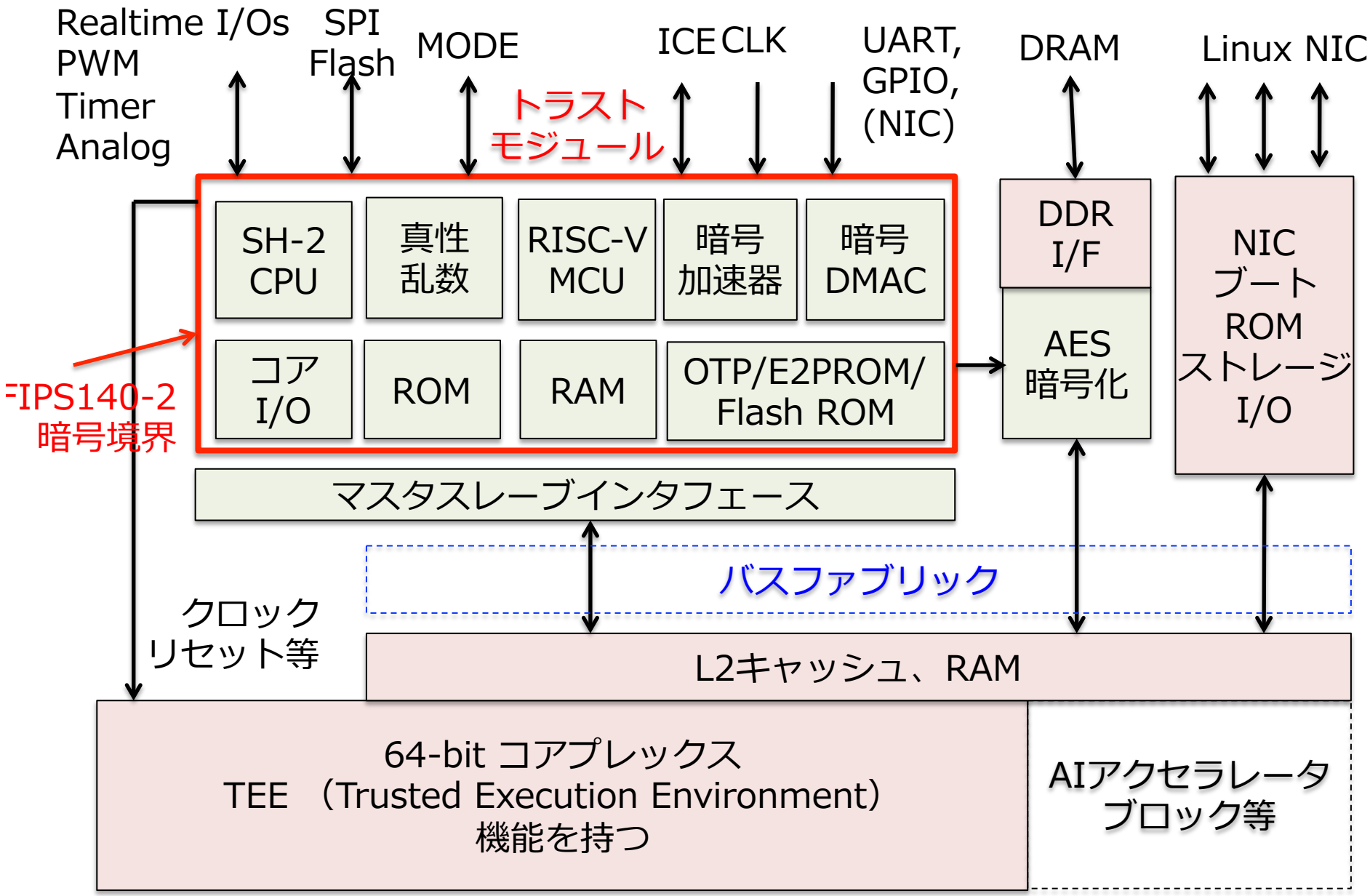


セキュアOS

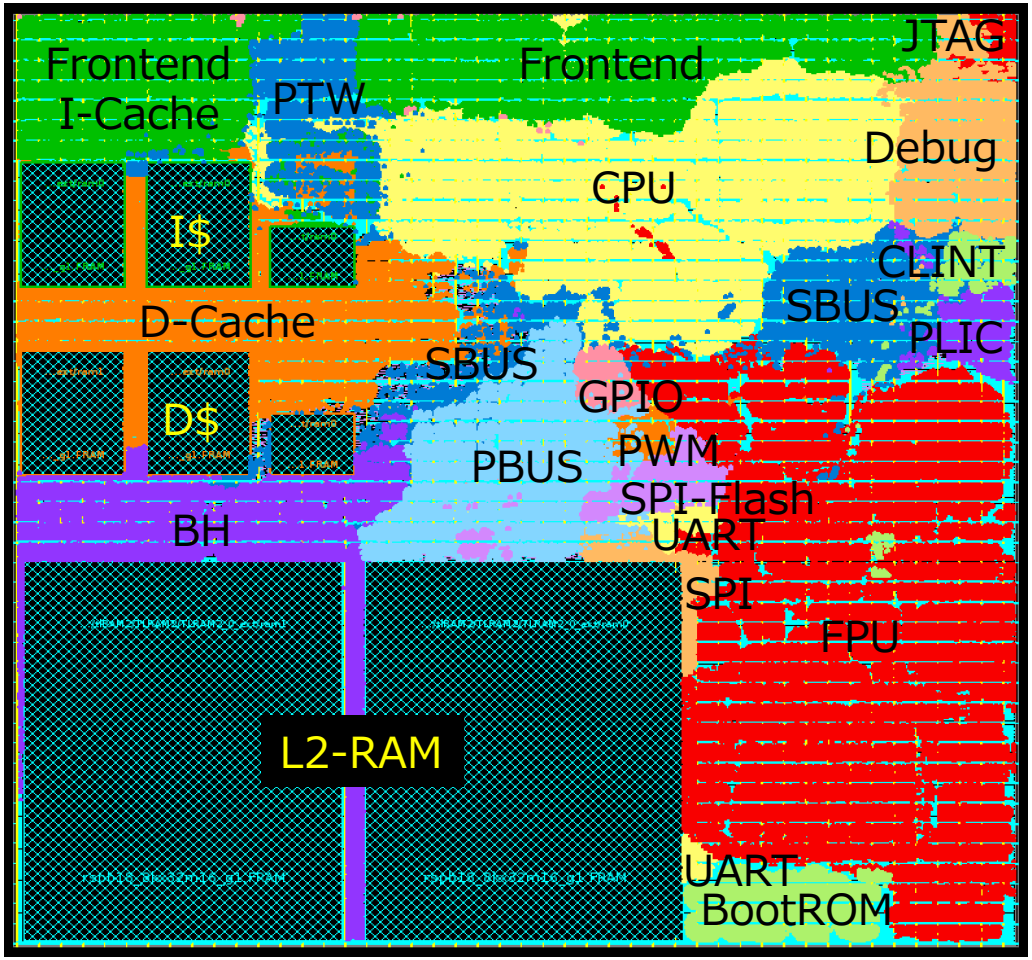
- APのOSから隔離された「独立した コンピュータシステム」 。
- 秘密情報 ストレージ：
  内蔵ノンボラと外付ノンボラ（暗号化）格納。
- EEPROM/Flash/OTP 長期鍵格納 (e.g. RSA/DSA/ECDSA)
- ユーザ鍵　(e.g. 3DES/AES/HMAC)
- RAM 短期鍵格納　(e.g. TLS セッション鍵　(e.g. 3DES/AES/HMAC)。
- コールバック, インテグリティチェック, 呼出アドレスリスト。



RISC-V IoT用SoCブロック図



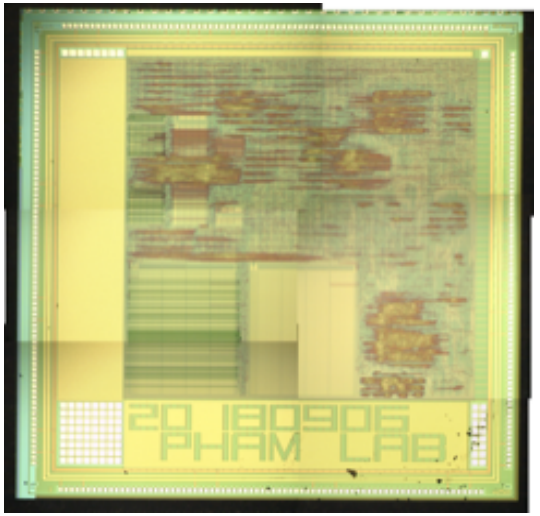
64-bit RISC-V Coreplex実験チップ



出展：電通大、東大VDEC

備考: 設計は週の夜、ウイークエンドに実施。
実質設計は１月未満。

チップ完：2018年12月
プロセス: ローム社180nm
面積: 3.75mm x 3.75mm
SRAM:
　I$ + D$: 4KiB + 4KiB
　L2-RAM: 64KiB
論理規模: 302KG (使用率: 53%)
周波数: 80MHz @typ
(最適化せず)



5mm x 5mm（パッド含む）

セキュアMCU実装実験

技術調査
- 仕様書
- QEMUエミュレータ
- FPGA実装
- チップ実装
- コンパイラ

が同時進行。

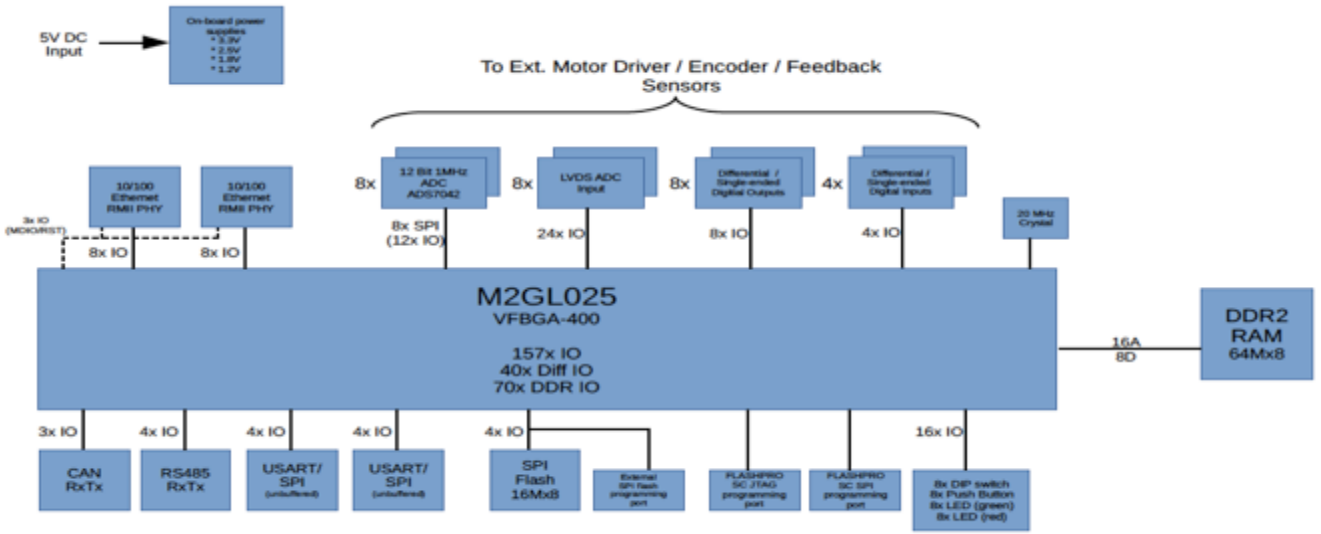
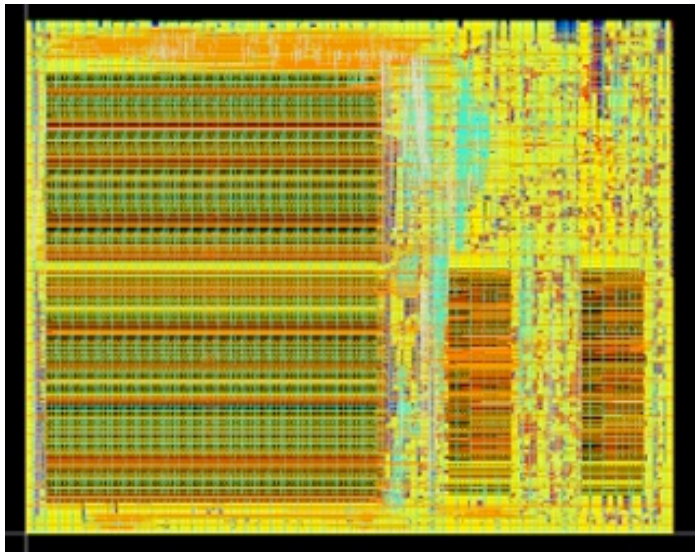


Illustration 1: Board Block Diagram

Igloo2 25KG FPGAボード



セキュアMCU試験レイアウト

FIPS140-2セキュリティ脆弱性評価

FIPS140-2 暗号脆弱性評価の11項目と作業に必要となるDUT物件リスト

	評価項目	システム仕様書	ハード仕様書	ソフト仕様書	RTL	OS ソース	CM＊	回路	GDS-II	チップ	実装ボード	テスタ装置
1	暗号モジュール仕様	✓	✓	✓	✓	✓	✓		✓			
2	暗号モジュールのポートとインタフェース	✓	✓	✓	✓				✓			
3	役割、サービス、認証操作	✓	✓	✓								
4	有限状態モデル	✓	✓	✓	✓	✓	✓					
5	物理的セキュリティ		✓	✓	✓	✓	✓	✓	✓	✓	✓	
6	運用環境	✓	✓	✓		✓						
7	暗号鍵管理	✓	✓	✓	✓	✓				✓	✓	✓
8	電磁放射/電磁両立性	✓	✓	✓						✓	✓	
9	セルフテスト		✓	✓		✓						
10	デザイン保証	✓	✓	✓	✓	✓	✓					
11	その他攻撃への対策	✓		✓						✓	✓	✓

出展： SHC

参考文献：NIST, “SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES” May 25, 2001"

＊) CM = コンフィギュレーションマネージメント（Configuration Management）

NEDOプロジェクト

「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発/革新的AIエッジコンピューティング技術の開発/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」

【概要】

・サプライチェーン全体でAIエッジデバイスのセキュリティを担保する基盤技術を開発する。

・オープンソースCPUであるRISC-Vをベースに、トラスト実行環境（TEE）にAPI準拠したセキュリティ機能を実装する。

・RISC-V-TEEの産業用途即応化技術、チップ固有鍵の実装方式、サービス活用時の鍵管理技術を合せて検討し、これら技術を活用したAIエッジの社会実装PoCを実施する。

【実施研究機関】

日立製作所 、慶應義塾大学、産業技術総合研究所、SHコンサルティング 、セコム 、電気通信大学 、東京大学

まとめ

- スマホでは、AP上のアプリがセキュリティを担保するトラスト実行環境(TEE）とこれから隔離され耐タンパ性を持つトラストモジュールの2段構えで守る構成が確立。
- セキュリティは社会通念であるため、貨幣、銀行、証券取引などの分野と同じく、実績と慣行が先行。マルチメディア、個人情報、電子マネー、バイオメトリクスの管財人、消費者は保守的で新技術を嫌うことが確認されている。
- IoTセキュリティは、Raspberry PiやArduinoの電子ヒューズ方式に退化はしない。スマホのセキュリティと固有鍵管理方式を踏襲すると予測される。メガOEMが公開したIoTシステムもそうした構成である。
- オープンソースセキュリティは、スマホに見られる2段構え方式を採用し、米国政府セキュリティ購買基準FIPS140-2等に準拠することをベースライン仕様とする。

2019年９月30日にRISC-V DAY TOKYO 2019を東京国分寺の
日立馬場記念ホールにて開催いたします。