RISC-Vの狙いと、IoT、AIエッジセキュリティの実現

河崎 俊平
SHコンサルティング株

範公可
電気通信大学

概要

1. 背景、自己紹介、会社紹介

2. RISC-Vアーキテクチャは、米国国防省国防高等研究計画局 （DARPA）の支援でカリフォルニア大学バークレー校が開発しました。知財モデル、ビジネスモデルの変革をもたらす破壊的イノベーションと呼んでいます。

3. 日本でも、官民学でRISC-Vのコミュニティ貢献を組織化する動きがあります。

4. セキュリティ機能をオープンRISC-Vプラットフォームとして供与し、安全に繋がるAIチップ、IoT等を実現します。セキュリティモデルを変革し少額電子マネー応用も視野に入れます。

5. 今後の計画

1. 背景、自己紹介、会社紹介

発表者経歴

1980　モトローラ68K

1986　AIチップ

1987-1998 サターン, ドリキャス用チップセット

<低迷>

2001　米国駐在中に大手電機メーカ退社

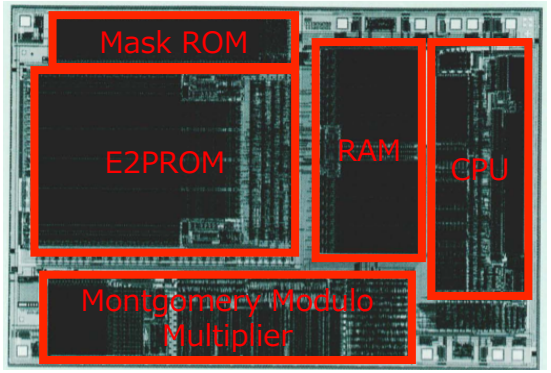
　　ソフト転身　Java Card™ 自前開発

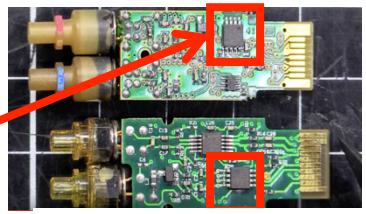
2003　ルータ真贋判定　C暗号ライブラリ開発

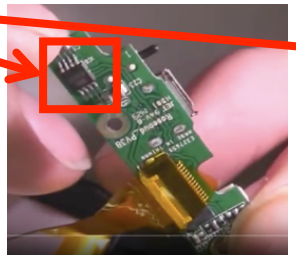
2007　大手スマホ　セキュアOS開発

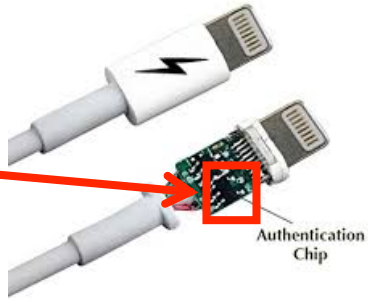
<低迷>

2013　大手半導体米国販社退社、SHC社設立









SHC製品

セキュアOS

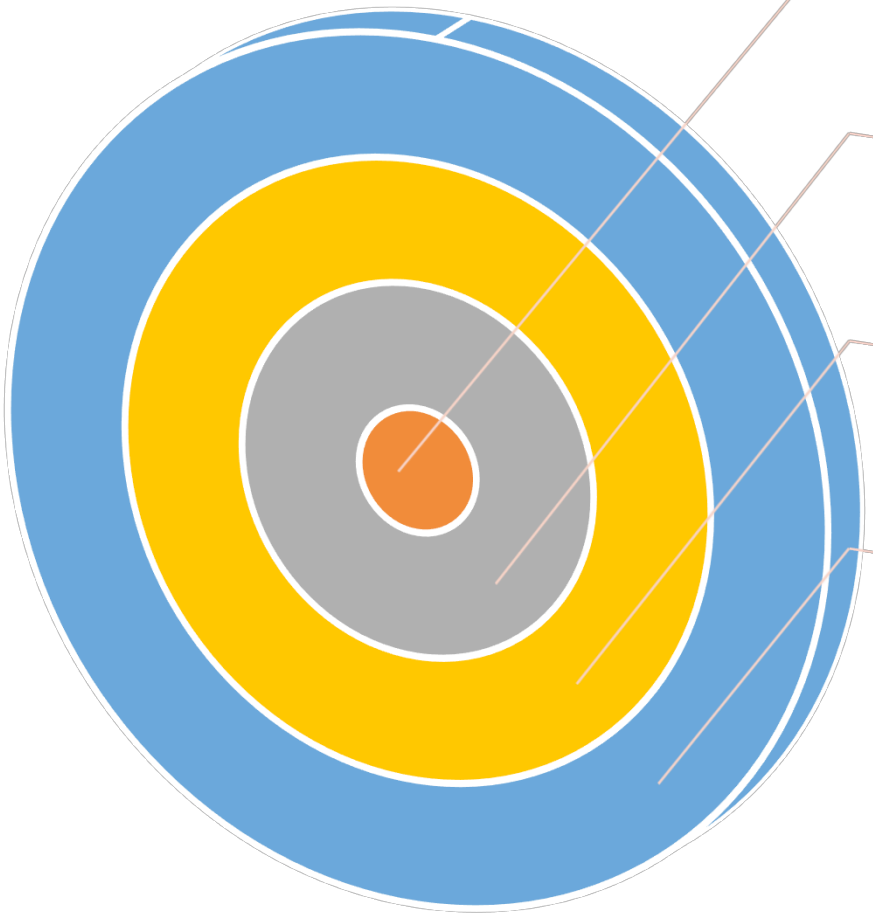
暗号APIライブラリ

無線
e.g. Lora, BTLE

ボードサポート

コンパイラ

OS 内部構造

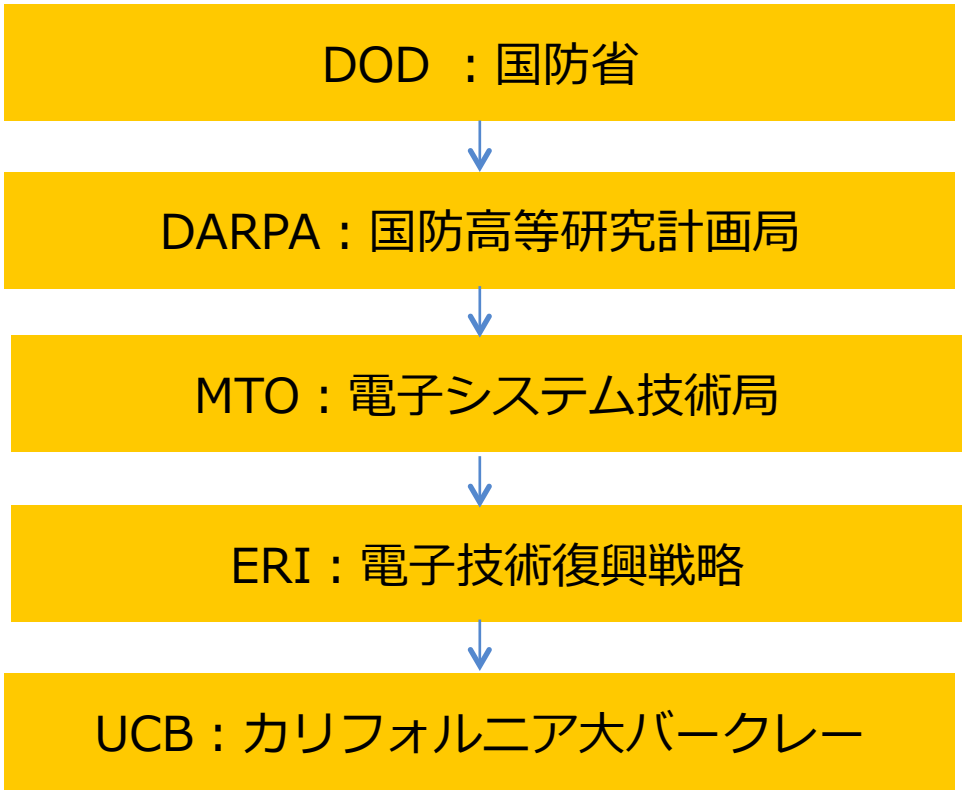


2. RISC-V

RISC-V沿革

- 研究目的でカリフォルニア大学バークレー校（UCB）で命令セット(ISA)を新規開発することとした。
  - X86とARMが選択肢だった。
  - X86はとても複雑。ARMは複雑。知財権も難しい。
- 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より0PF.ORG(SH CPUコアNPO)に協力依頼あり。
  - SHCはワークショップに全て参加。
  - 2015年に、0PF.ORGを参考にRISC-V基金がNPOとして誕生。

RISC-V開発支援



- 2010年より左の体制でアーキテクチャ開発開始
- 2014年よりデモ開始
- 2015年にRISC-V Foundation結成。
- UCB スピンアウト会社SiFiveの結成
- インテルスピンアウトEsperantoの参加
- Google, Western Digital, Qualcomm等の大手企業が参加

RISC-V基金

- 基金目的:
  - 世界中の全ての計算機RISC-VのISAを無償に使用できる。
  - 規格化、保護、 プロモートし、このハード、ソフトのエコシステムを発展させる。
- オープン命令セット利点:
  - フリーマーケット>イノベーション。
  - ソフトは50年 以上末永く使える。
- オープンソースコアをシェア：
  - プロセサを安くする。IoT用の$1以下のデバイス。
  - アーキテクチャ研究と学習をより現実的にする。
  - DARPAのセキュリティ研究は、RISC-Vを必須条件としている。

RISC-VのIPへのスタンス

- 命令セットライセンスはフリー
- オープンソースとプロプライエタリ実装を両方尊重
  - オープンソース：
  - プロプライエタリ：
- 互換性テストは公開しダウンロード可能
- RISC-Vトレードマークは 互換性テストを通すことが必要。
  - RISC-V会員のみ使える。

RISC-V基金の機能

- 教宣活動:

  ①RISC-Vの公式の情報源、②ドキュメントのリポジトリ、③ウエブ管理、④イベント企画、⑤RISC-V関連のプロモーションをするための出版物を編集し販売する。

- ISA管理:

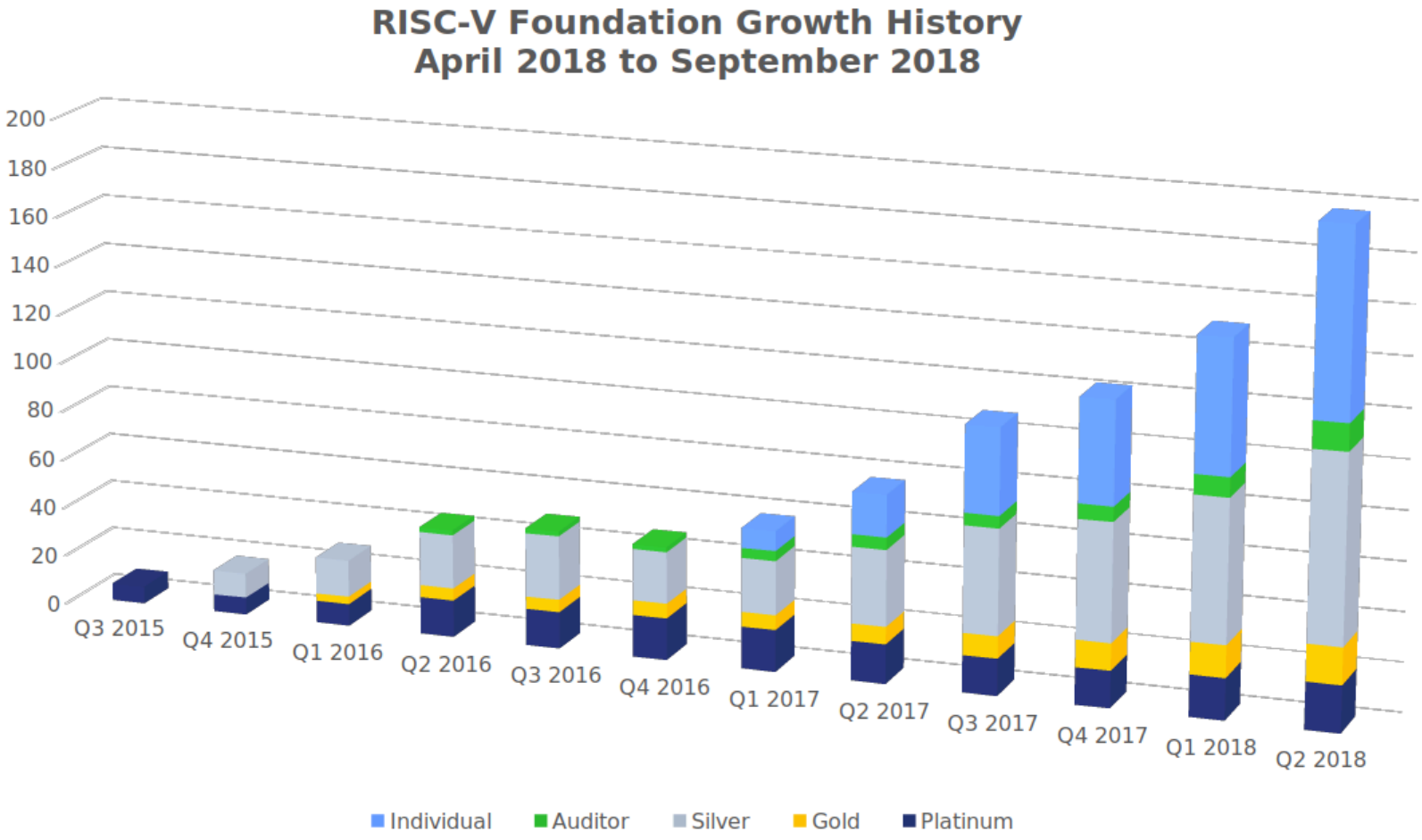
  ユーザコミュニティのニーズと依頼に従いISAと ハードとソフトのエコシステムを①維持②進化させ、③ライセンスさせる。

- トレードマーク管理:
  - どの製品がRISC-Vトレードマークを使 えるかを決定する。
  - パブリックドメインのISAを維持する。
  - 出版と失効した特許を使う

RISC-V基金組織

- 取締役は7名以上により構成される。補充は選挙により行われる。
  - 取締役会はミッションステートメントを充足できるか否かについ て最終的な責任を負う。
  - 取締役会は、2/3の評決で内規を改正できる。
  - 取締役会は、アドホック委員会を任命する権限を持ち、アドホック委員会の最終承認権限を持つ。
  - 委員会の全メンバはRISC-V基金の会員である必要がある。
- 委員長は取締役会にレポートし、委員会のメンバは取締役会が委員会の仕事が進んでいないと判断した場合に解任できる。
  - 取締役会は、RISC-Vを各地域でプロモートするために、地域委 員会長を任命する。

RISC-V Foundation: ~ 200 Members

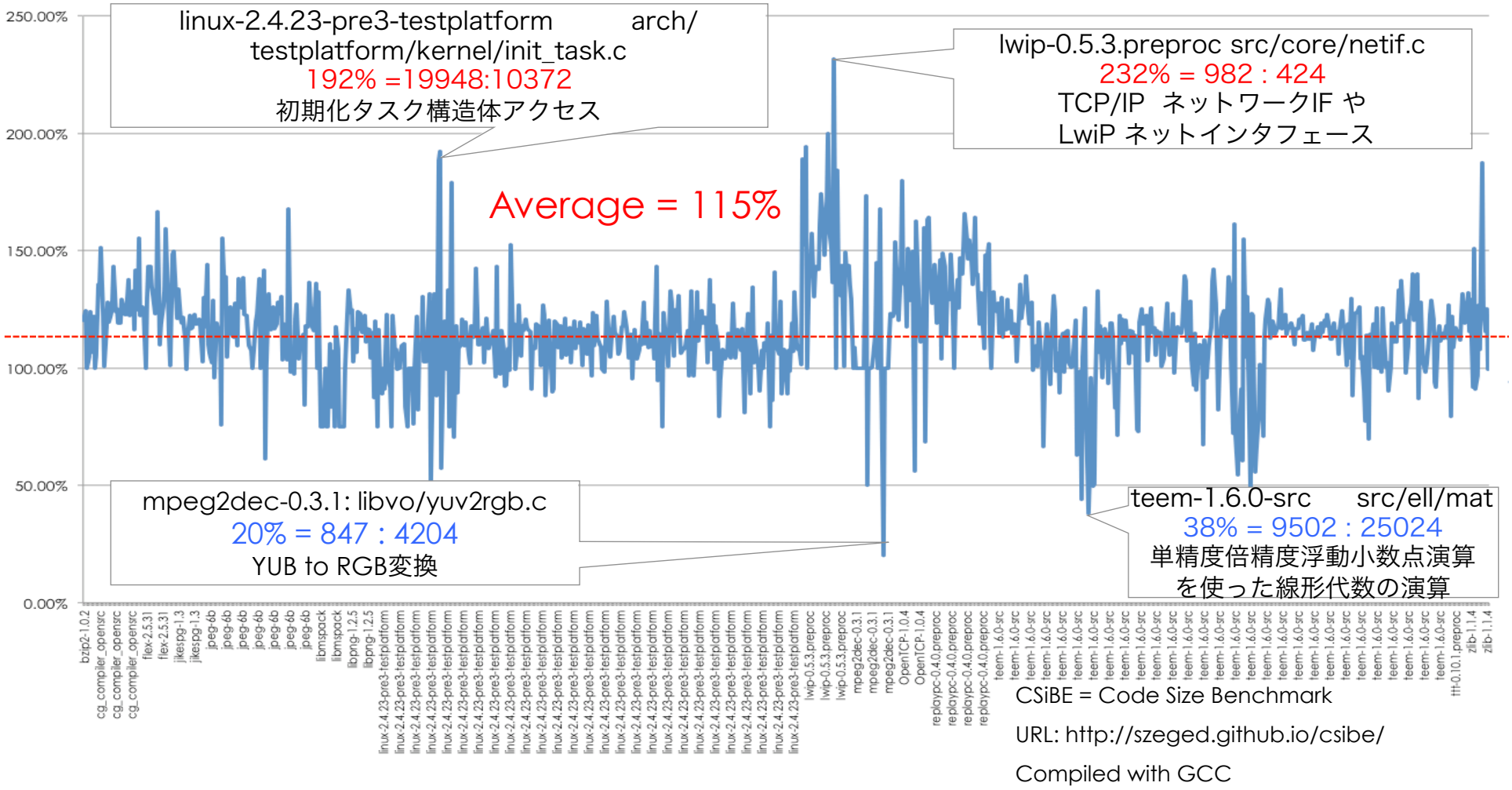

RISC-V Foundation Growth History
April 2018 to September 2018
200
180
160
140
120
100
80
60
40
20
0
Q3 2015
Q4 2015
Q1 2016
Q2 2016
Q3 2016
Q4 2016
Q1 2017
Q2 2017
Q3 2017
Q4 2017
Q1 2018
Q2 2018
Individual
Auditor
Silver
Gold
Platinum

RISC-V ISA 特徴

- レジスタ、メモリ、データフォーマット
  - リトルエンディアン。
  - レジスタのビット幅は任意。
  - ビット幅はXLEN命令で取得できる。
  - 汎用レジスタはx1-x31の31本。
  - x0はゼロレジスタ。それとプログラムカウンタのみ。
  - 条件フラグや特殊なレジスタはない。
  - キャリー/ボローはない。
  - メモリコンシステンシはRelax Ordering。ロードやストアが入れ替わっても良い。
  - メモリに対するアトミック命令としてLR/SC命令とCAS命令がある。
  - ロード/ストア命令はアライメントをまたいでも例外は発生しない。遅くなるだけ。
- 命令体型、フォーマット
  - 32bitを基本とした可変長命令。頻度の高い命令は16bit長。
  - プレフィックス指定でVLIW向けの命令グルーピングも考慮してある。
  - 整数基本命令I、乗除算命令M、アトミック操作命令A、単精度浮動小数点演算命令F、倍精度浮動小数点命令Dと分類してある。実装によりIMA、IMAFD(=G)と呼んでいる。
  - Q(四倍精度浮動小数点)、L(BCD浮動小数点)が定義してある。
  - C(圧縮)、B(ビット操作)、T(トランザクショナルメモリ)、P(Packed-SIMD)も定義。
  - これらを基本に必要な命令を拡張しやすくしてある。
  - 除算命令と剰余命令を連続させ１命令の様に扱うと実装により性能向上。
  - アセンブラのニーモニックはMIPSに似ている。
- 分岐命令
  - ディレイド分岐命令はない。
  - 静的分岐予測のヒントはない。
  - 分岐命令は比較を合わせたCompare&Branch命令。
  - 1命令で2レジスタを比較して飛ぶ。
- 例外処理
  - 乗除算命令のオーバーフローなどでトラップは発生しないが、結果で判断できる。

Reference: http://keisanki.at.webry.info/201408/article_2.html

64b RISC-V コードサイズベンチマーク(RV64GC vs. ARM Cortex M0)



CSiBE = Code Size Benchmark

URL: http://szeged.github.io/csibe/

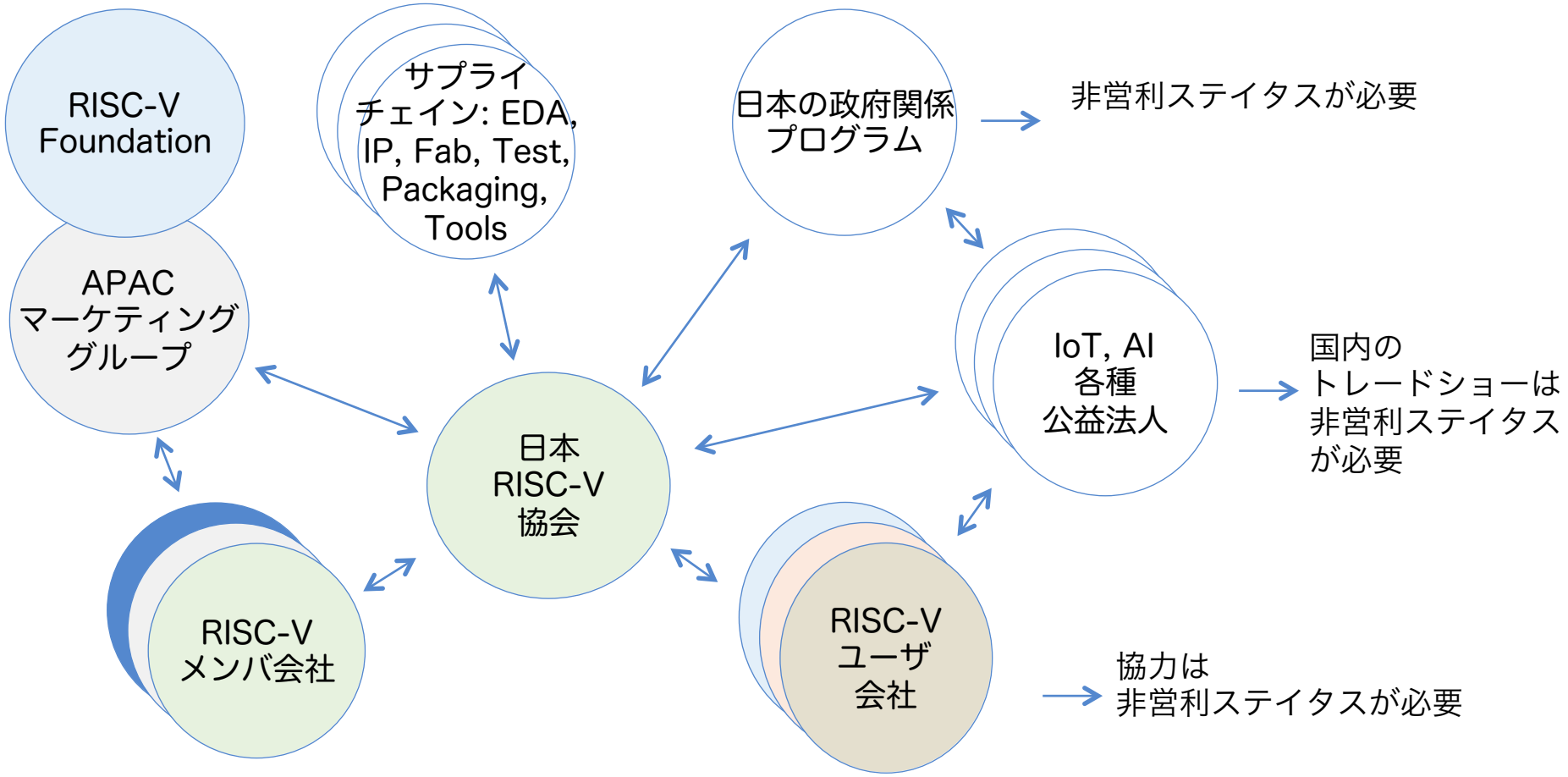
Compiled with GCC

3. 日本でのRISC-V活動

RISC-Vの日本の状況　2017 - 2018

- 会員：
  - SHコンサルティング株式会社（2016）、TechAnalye（2017）、株式会社日立製作所（2018）
- 辻岡直美氏がアジア太平洋（APAC）マーケティング議長に選出。
  - 日本RISC-V協会の設立を考えることとなった。
- 本とドキュメント
  - 日経BP社からのRISC-V READER日本語訳、LaTex言語の実施。
  - TEEとセキュリティ作業部会の参加。
- ハードウエア
  - 電気通信大学180nm実験用チップ
  - 共同プラットフォーム作成の概念化

日本RISC-V協会（JRVA）の必要性



RISC-V原典　連続アマゾンベストセラー

David Patterson
デイビッド・パターソン

リカ合衆国の計算機科学者で、1977 年からカリフォ
ア大学バークレー校 (UCB) の計算機科学教授を務め
る。RISC と RAID の基礎を築いた 1 人であり、
という用語の生みの親である。バークレー RISC(英
) プロジェクトを指揮した [2]。ジョン・ヘネシーと
ンピュータ・アーキテクチャに関する共著は教科書
て広く採用されている。アメリカ科学振興協会フェ
。

Andrew Waterman
アンドリュー・ウォーターマン

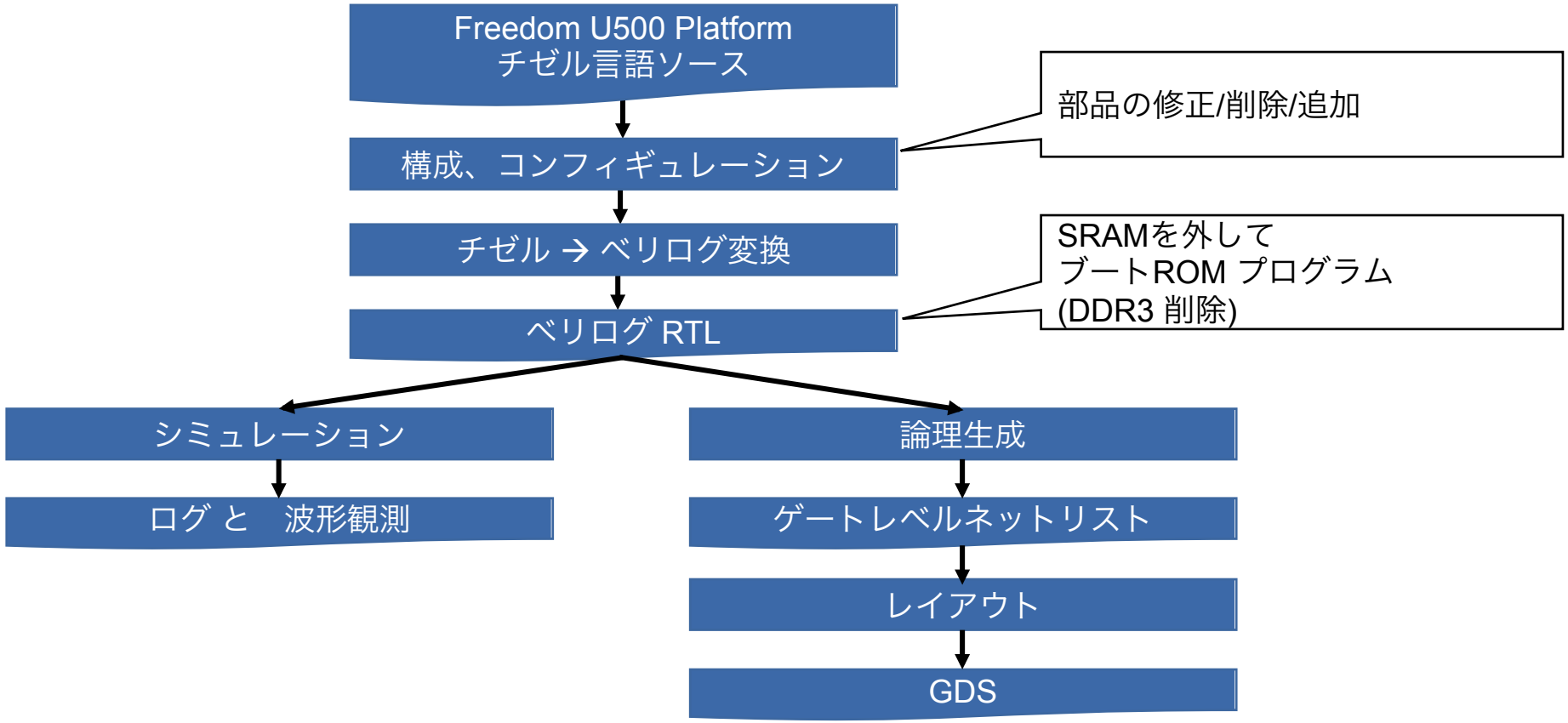
リカ合衆国の計算機科学者で、1977 年からカリフォ
ア大学バークレー校 (UCB) の計算機科学教授を務め
る。RISC と RAID の基礎を築いた 1 人であり、
という用語の生みの親である。バークレー RISC(英
) プロジェクトを指揮した [2]。ジョン・ヘネシーと
ンピュータ・アーキテクチャに関する共著は教科書
て広く採用されている。アメリカ科学振興協会フェ
。

日経 BP の関連書籍

コンピュータの構成と設計 第 5 版 <上>
ジョン・L ヘネシー (著)
デイビッド・A. パターソン (著)
成田 光彰 (翻訳)
定価 4,200 円+税

コンピュータの構成と設計 第 5 版 <下>
ジョン・L ヘネシー (著)
デイビッド・A. パターソン (著)
成田 光彰 (翻訳)
定価 4,200 円+税

電通大RISC-Vチップの設計フロー(チゼル言語)

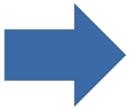


電通大RISC-V実験チップの設計パラメータ(チゼル言語)

ベースIP: SiFive's Freedom U500 Platform
https://github.com/sifive/freedom (@89059e7)

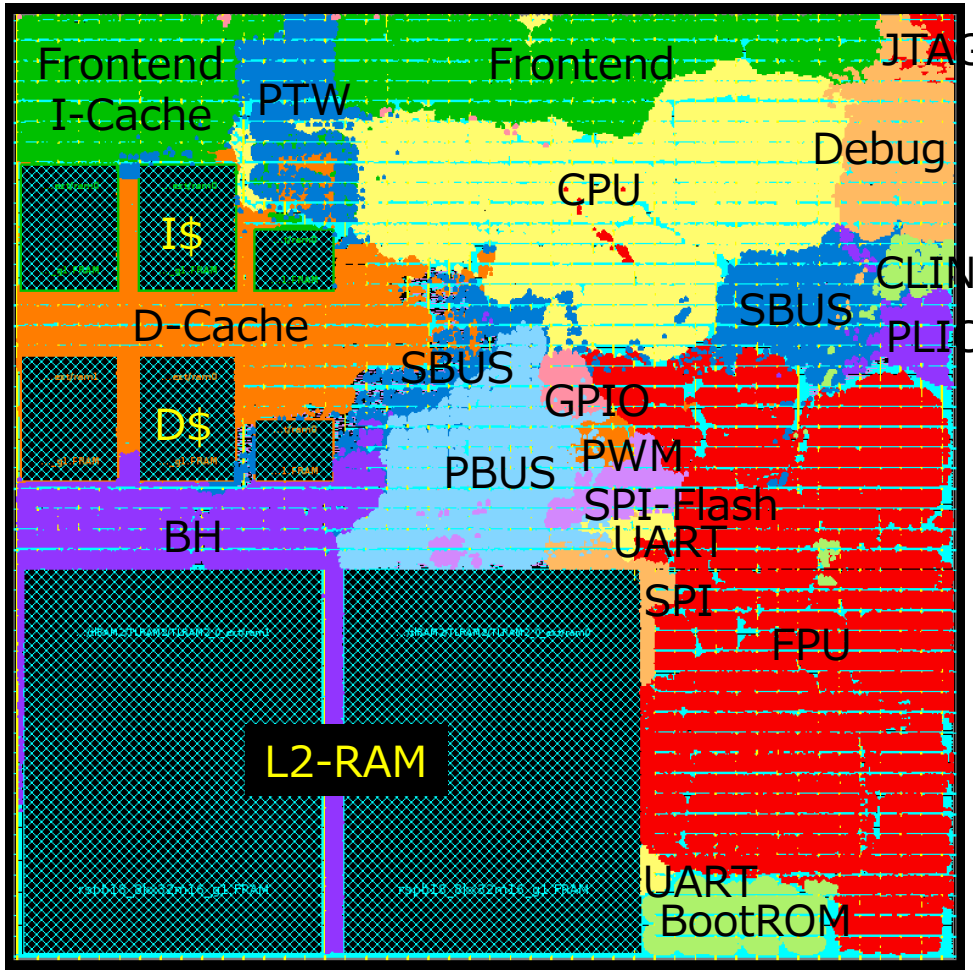
Github内容
(U500VC707DevKitConfig)

- 4 Cores (w/ 4way $)
- UART
- SPI (w/o Flash controller)
- GPIO (4bit)
- Boot ROM (sdboot)
- Debug & JTAG
- PCIe (Xilinx IP)
- DDR3 (Xilinx IP)



電通大設計内容

- 1 Core (w/ 1way $)
- UART
- SPI (w/o Flash controller)
- GPIO (16bit)
- Boot ROM (kzload)
- Debug & JTAG
- ~~PCIe (Xilinx IP)~~
- ~~DDR3 (Xilinx IP)~~
- L2-RAM (64KiB)
- SPI-Flash
- PWM

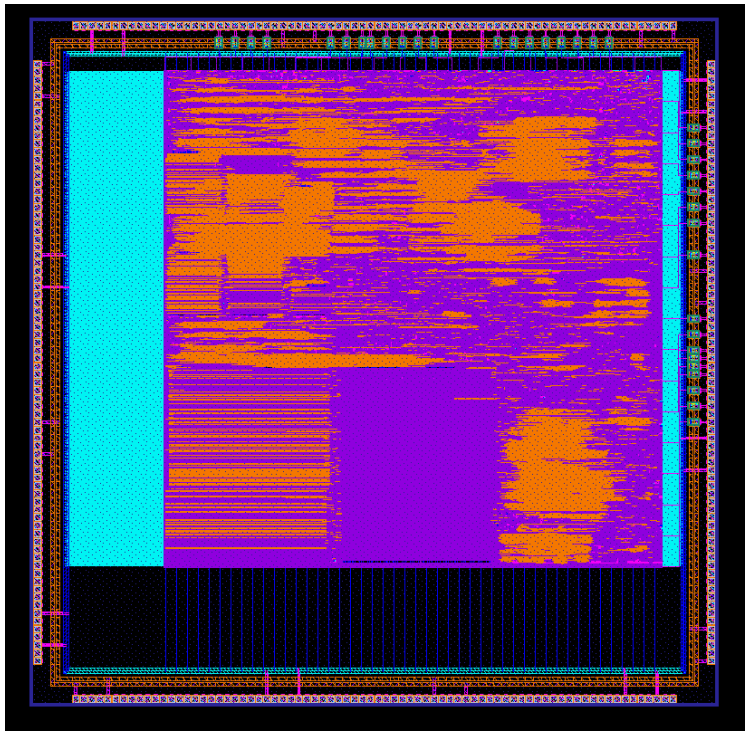


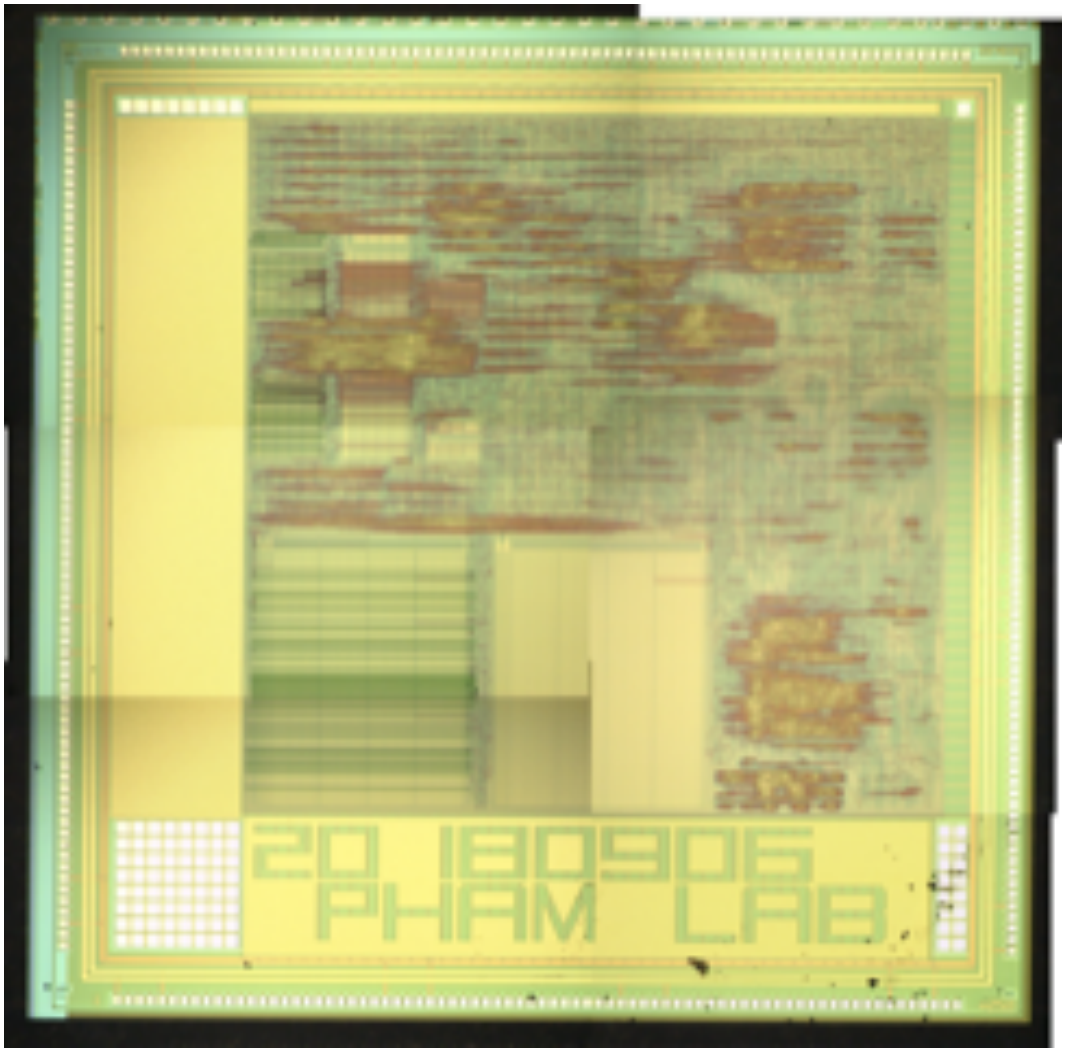
電通大64b RISC-V実験チップ設計 レイアウト結果

プロセス:
　ROHM 0.18um
面積:
　3.75mm x 3.75mm
SRAM:
　I$ + D$: 4KiB + 4KiB
　L2-RAM: 64KiB
スタンダードセル:
　302KG
　(Utilization: 53%)
周波数:
　80MHz @typ
　(最適化せず)

電通大64b RISC-V実験チップ（RV64GC/Sv39） ローム社180nm

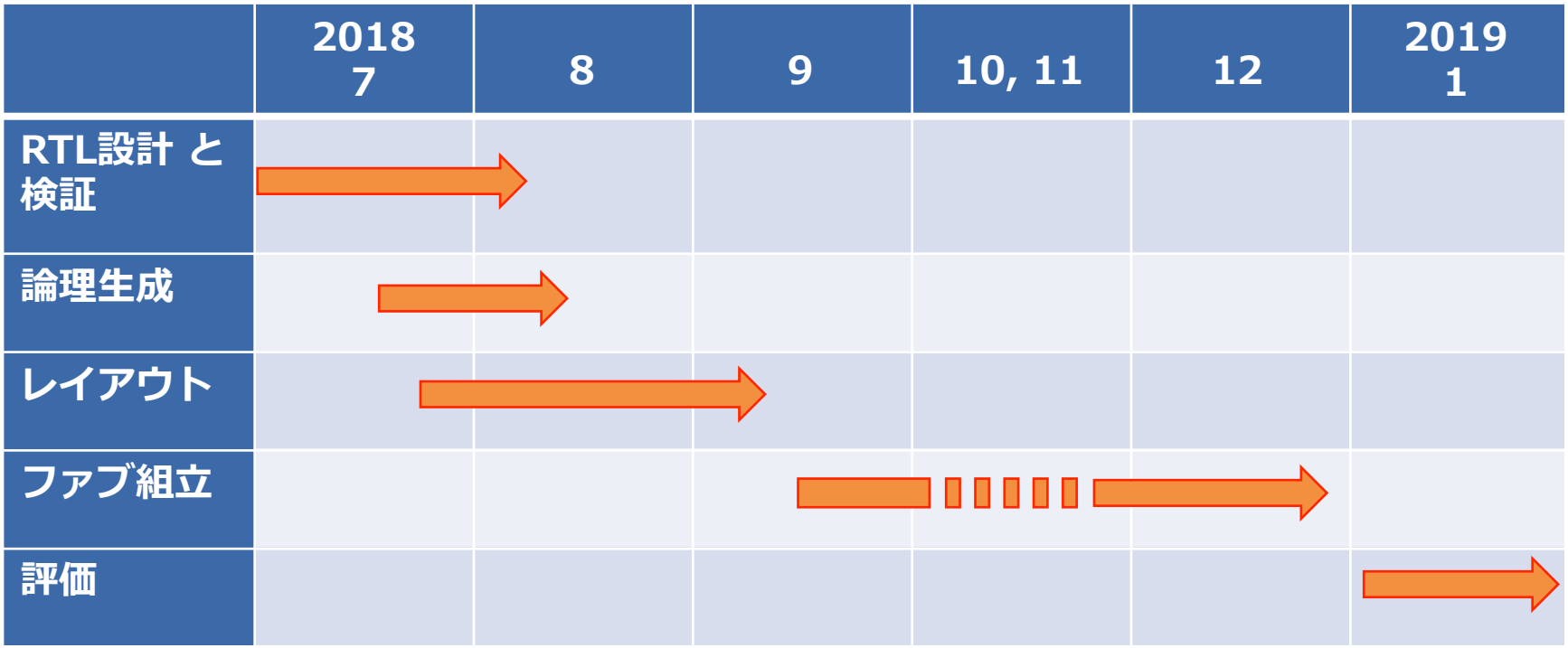
5mm x 5mmチップサイズ（パッド含む）





電通大
64b RISC-V実験チップ
（2018年12月）
チップ写真

電通大 64b RISC-V実験チップ設計スケジュール



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。

NEDO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

- 経済産業省とNEDOが、RISC-Vベースのオープンセキュリティシステムレベルのプラットフォームを開発プロジェクトを立ち上げようとしている。
- 課題は、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。
- RISC-Vハードウェア（TEE機能追加）、ソフトウェア（OP-TEE）とセキュアMCUを集積することを目的としている。
- 内閣府主導のSociety 5.0の産業アプリケーションに重点を置く。産業向けアーキテクチャを実現する。
- 構成メンバは、産総研、日立、セコム、慶應義塾大学、東京大学、SHC。今後これをさらに拡大予定。

Keio University 1858 CALAMVS GLADIO FORTIOR

UEC TOKYO

SHC

東京大学 THE UNIVERSITY OF TOKYO

NEDO

HITACHI

SECOM

AIST NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY (AIST)

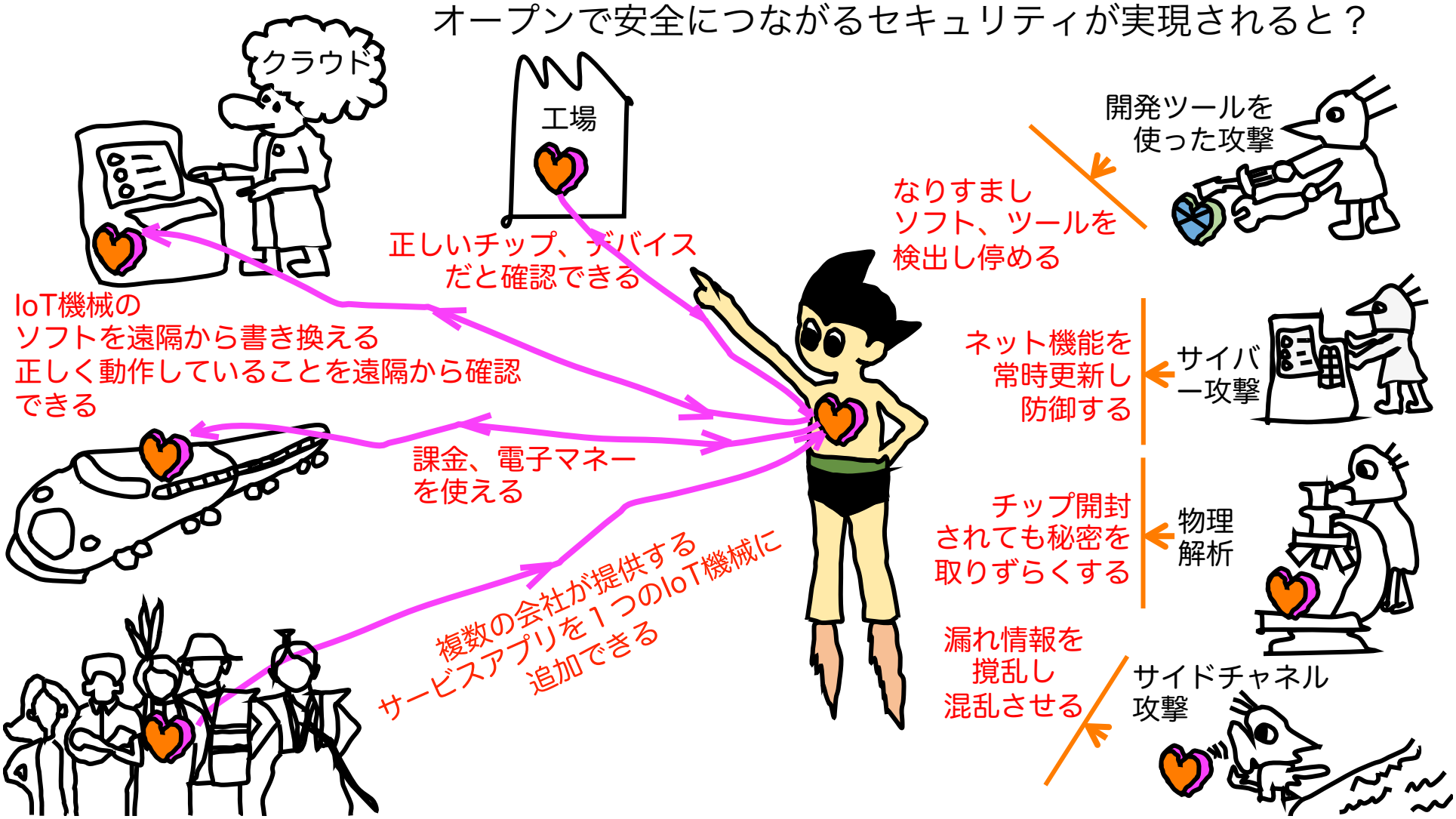
METI Ministry of Economy, Trade and Industry

RISC-V 日本の活動予定2019

- 2019年7月RISC-Vデイ2019日本
  - 2017年12月、2018年10月
  - 幅広いAPACインバウンド参加
- ブックプログラム
  - 定量6 / e日本語翻訳
  - デザインメソドロジブック出版
- 日本の企業会員が増える
  - 日立製作所他の加入
  - 見本市へのRISC-V常時参加
  - 日本RISC-V協会設立2018年10月
- 相乗りRISC-Vプラットフォームプロジェクト実現

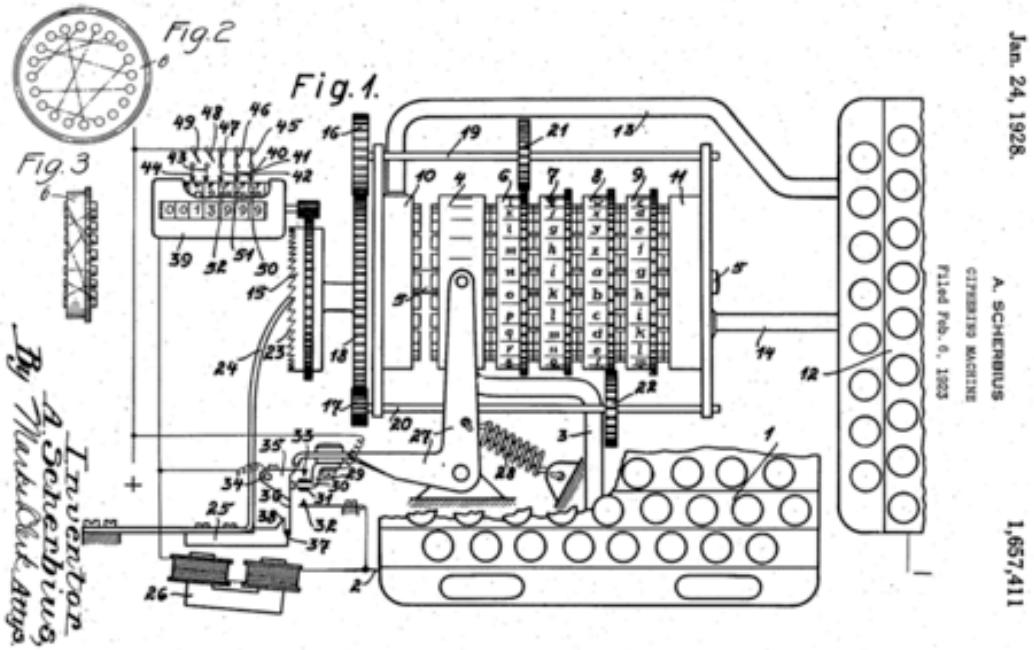
4. RISC-Vセキュリティ

オープンで安全につながるセキュリティが実現されると？



ケルクホフス　«軍用暗号» 1883年

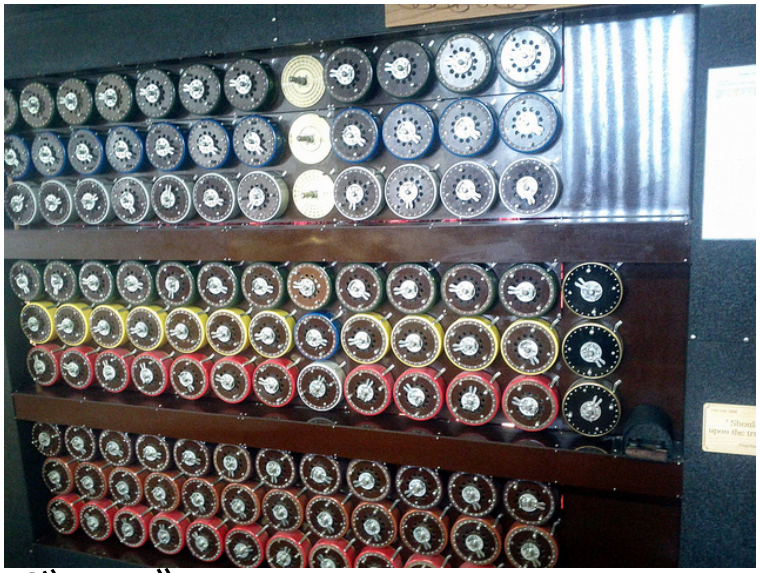
1. 暗号方式は、現実的に（数学的にではなく）逆変換不能であること
2. 暗号方式は、秘密であることを必要としてはならず、敵の手に落ちても不都合が無いようにする
3. 鍵は伝達可能で、文書を見なくても維持ができ、通信員が変更できる
4. 携帯可能で電気通信に適したものであるあり、利用動作に大勢の人を必要としない
5. 利用状況を考え、精神的緊張や長い取扱書の通読を不要とし取扱い易い



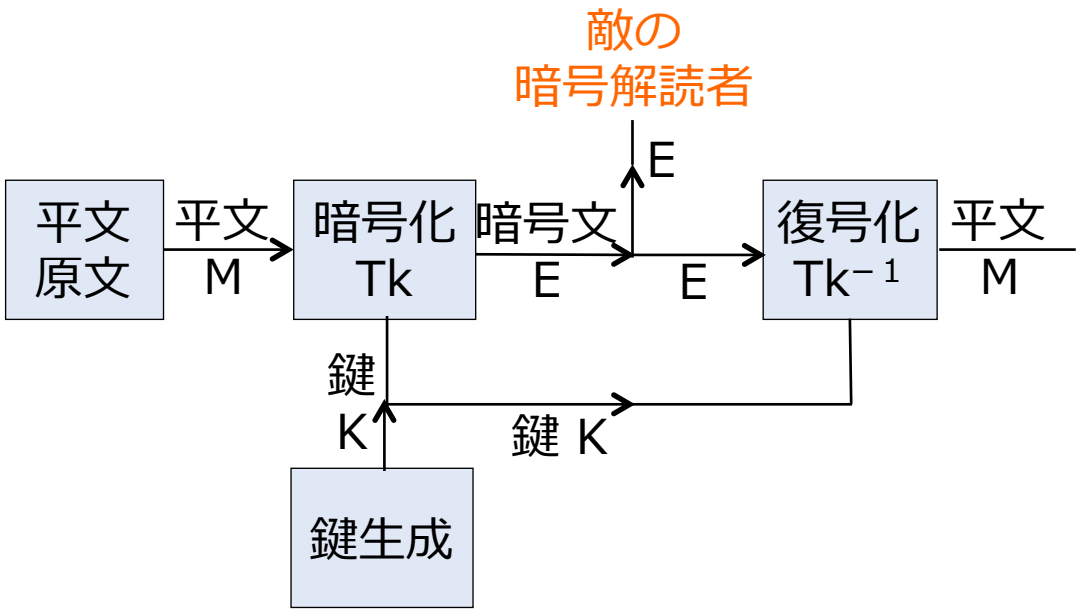
“エニグマ” by Arthur Scherbius 1918

“ボンブ” by Alan Turing

暗号解析マシン「ボンブ」 1941年
と
シャノン «機密システムの通信理論» 1949年



ボンブ by Alan Turing 1941



ドイツ軍のエニグマ鍵管理表

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

Luftwaffen-Maschinen-Schlüssel Nr. 649

[G]eheim! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vern[ichten]

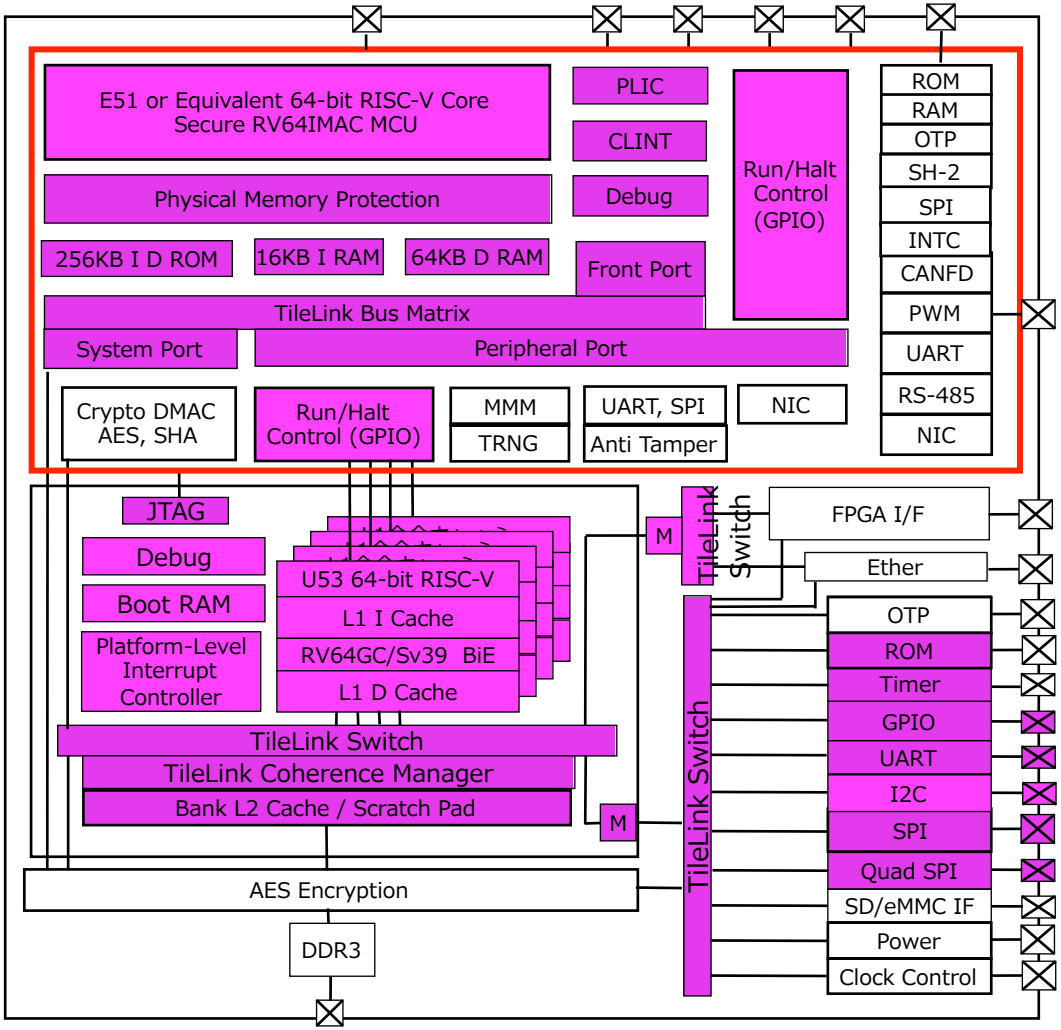
Walzenlage		Ringstellung			Steckerverbindungen an der Umkehrwalze				Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	
V	III	14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny
III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl
II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc
III	V	06	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。

ケルクホフスの原理（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。
- 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。
- しかし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。



セキュアな RISC-Vシステム

FIPS-140-2 Cryptographic Boundary

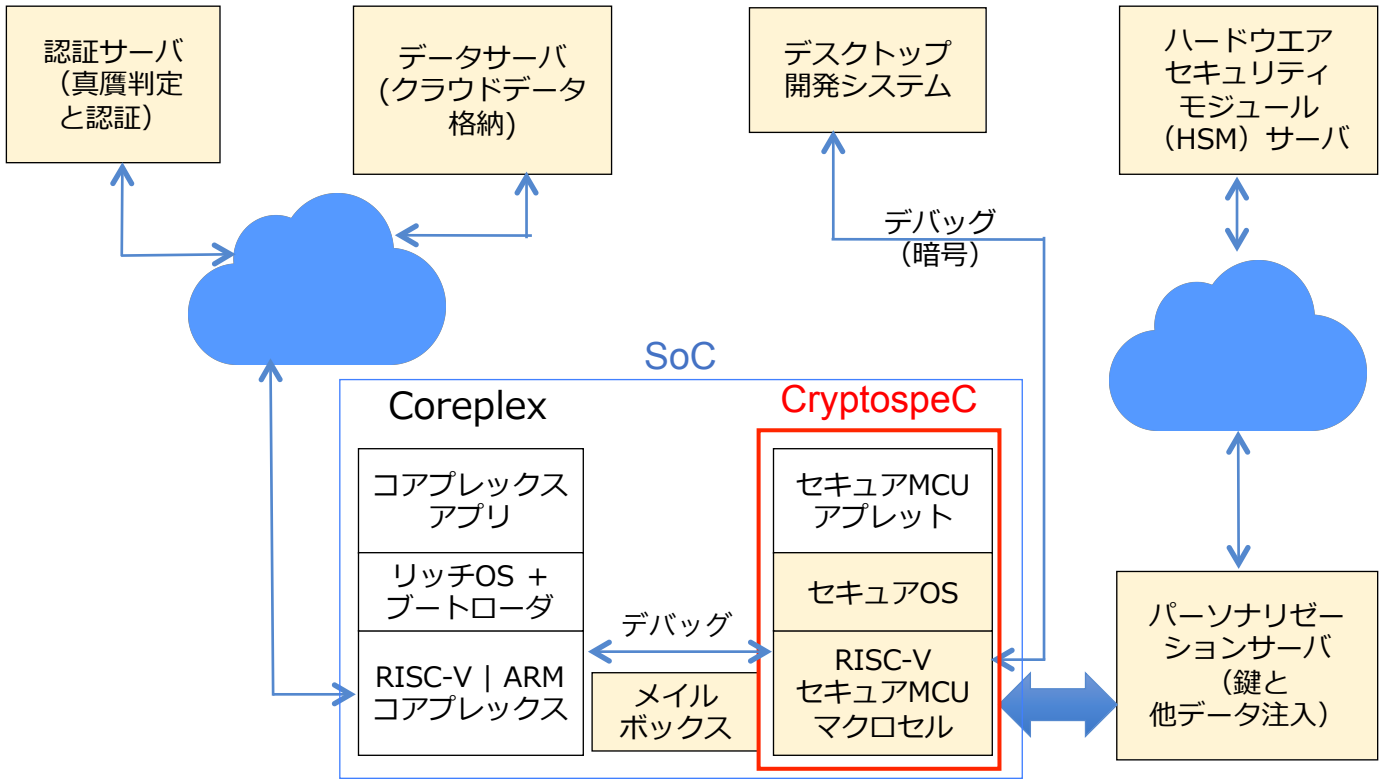
RISC-V Core Complex

- TEE導入活動は並行して進行中。
- 赤い四角はFIPS140-2暗号化境界、評価対象（TOE）の論理的および物理的境界を示す。
- 主流ベンダと同構成と同周辺機器を利用することで、主流のRV64GC / Sv39システムからのフラグメントを最小限に抑えることを試みている。
- 暗号化のコストは高い。したがって、安全であると指定された唯一のページはDDRで暗号化されていると想定する。

クリプトスペック（CryptospeC）

- CryptospeC ：メインCPUコアプレクスのトラストとユーザ秘密を不法アクセスから保護するマクロセルIP。セキュアMCU部とセキュアOS部からなる。基本部をオープンソースとしシステム理解も促進。
- CryptospeCは、ARM | RISC-V等のメインCPUの深い部位に集積。システムが繋がるために必要な通信を秘匿化する。不法プログラム実行をハードで阻止する。
  - メインCPUが、システム管理者の意図と異なるプログラムソフトを実行することを阻止する。過去記録、命令、データを解析し、プログラム信頼度を評価し、実行許可をGo-No-Goベースで出す。
- 自身のTLSソフトウエアをオプションで持ち、サーバとマクロセルでセキュアチャネルを持ち交信できる。

CryptospeC アーキテクチャ



モジュールの説明

ハードウェアセキュアモジュール（HSM）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。

パーソナリゼーションサーバ：Cryptospecモジュールにキーおよびその他のパーソナライゼーションデータを注入するためにCryptospeCモジュールとインターフェースする。

認証サーバ：CryptospeCモジュールが生成したデジタル署名を検証および検証する。

データサーバ：セキュアチャネルを使用してCryptospeCモジュールと通信する。

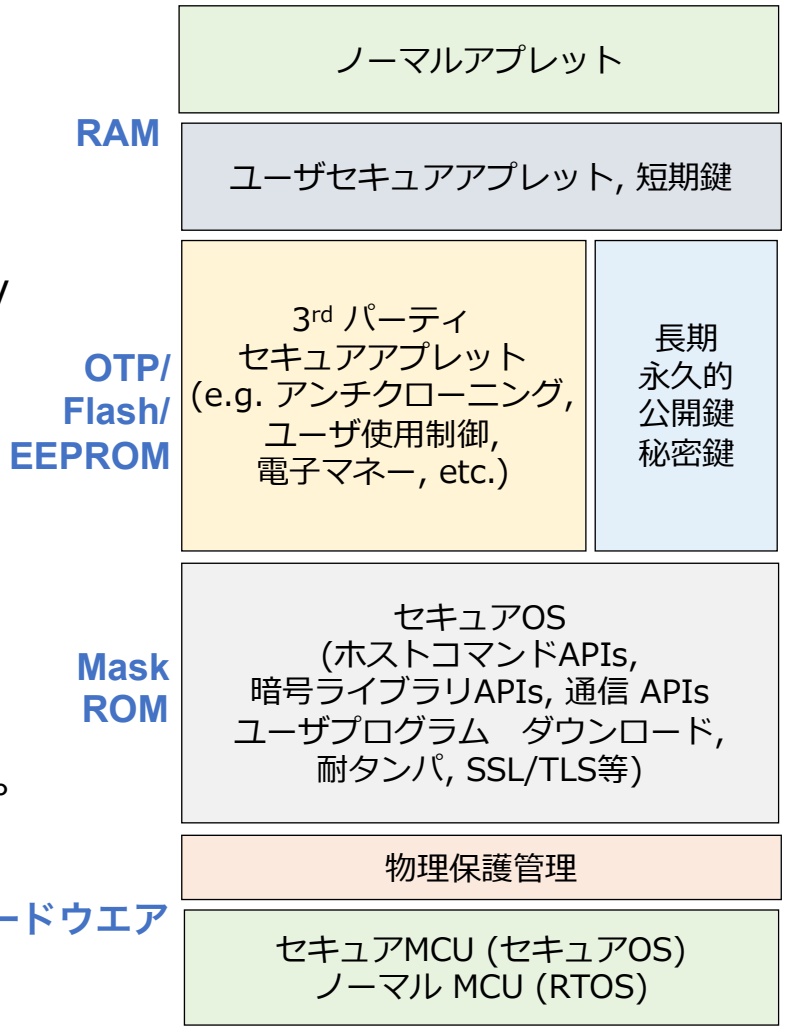
デスクトップ開発システム：CryptospeC用アプレットを開発する。RISC-V Coreplexアプリを開発する。このための開発プラットフォーム。

デモ内容

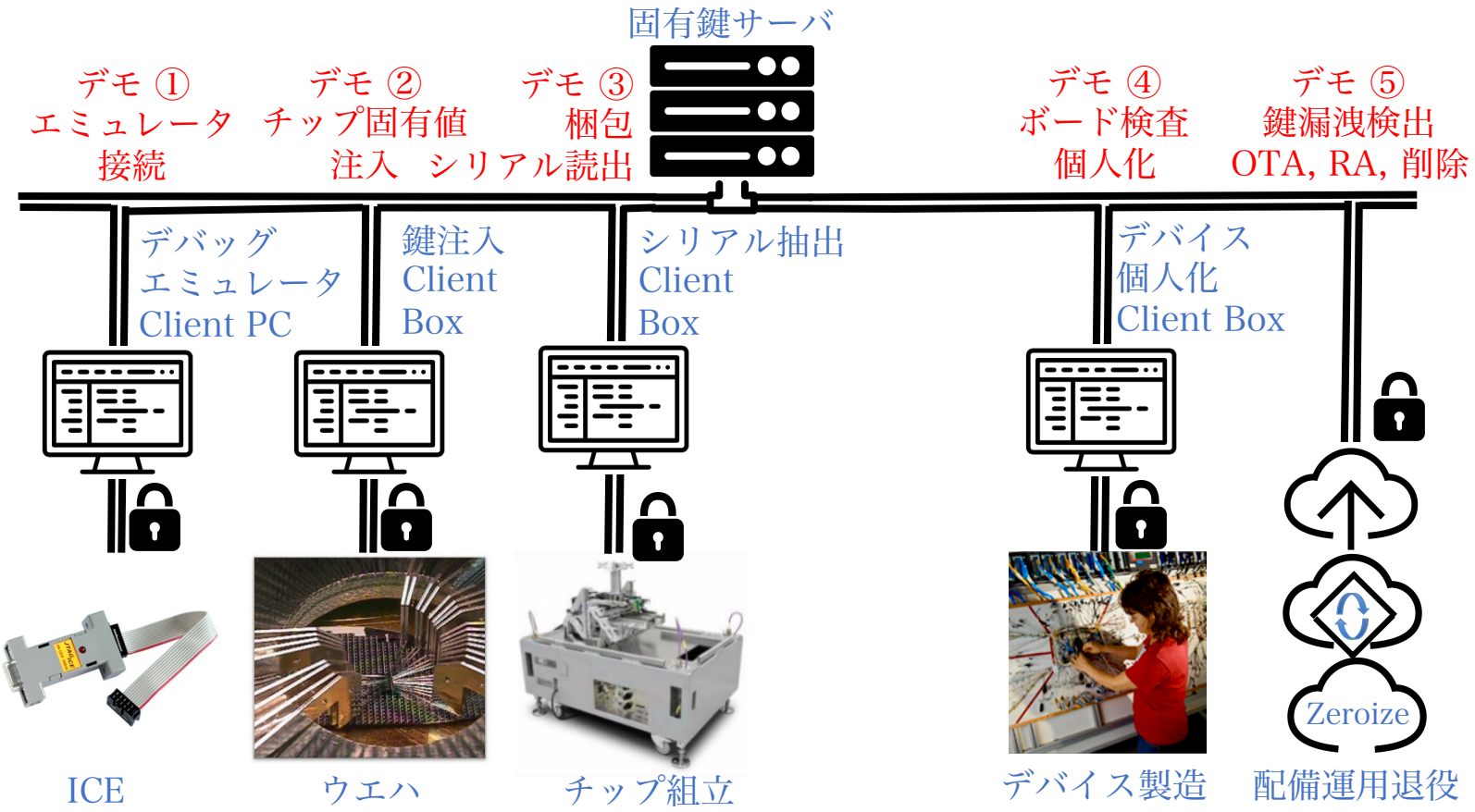
- 開発システムは、ツールチェーン、Cryptospecモジュール、およびCoreplexプロセッサ用のアプリケーションを開発するためのデバッガコンポーネントで構成されます。
- 認証サーバコンポーネントは、認証と識別を目的としたCryptospecモジュールの使用方法をデモします。
- データサーバコンポーネントは、クラウド内のデータストレージにCryptospecモジュールを使用し、暗号化を使用して機密データを転送するためにCryptospecモジュールと安全に通信することをデモします。
- パーソナリゼーションモジュールとHSMコンポーネントは、Cryptospecモジュールの使用とエンドユーザーアプリケーションでのさらなる使用のためのそのパーソナライゼーションをデモします。

CryptospeC セキュアOS

- EEPROM/Flash/OTP 長期鍵格納 (e.g. RSA/DSA/ECDSA) and 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)。
- 秘密情報 はオンチップフラッシュとか外付けフラッシュに暗号化されて格納。
- Linux SSL/TLSから隔離された自身の SSL/TLS。
- 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。



安心に繋がるデバイスのサプライチェーンとチップ固有鍵管理インフラ



FIPS140-2 認証

- 米国政府購買基準：
- 技術内容
  - 不正開封防止コーティングまたはシール。
  - ゼロ化
  - 系統的にテストされチェックされた設計保証
  - 入力：セキュリティアーキテクチャ、機能テスト、開発者テスト、構成テスト、開発者手順。
  - 脆弱性分析と独立テスト
- FIPS140-2レベル3認証に関する経験を生かす。

5. 直近の計画

セキュアMCUボード　2018年12月

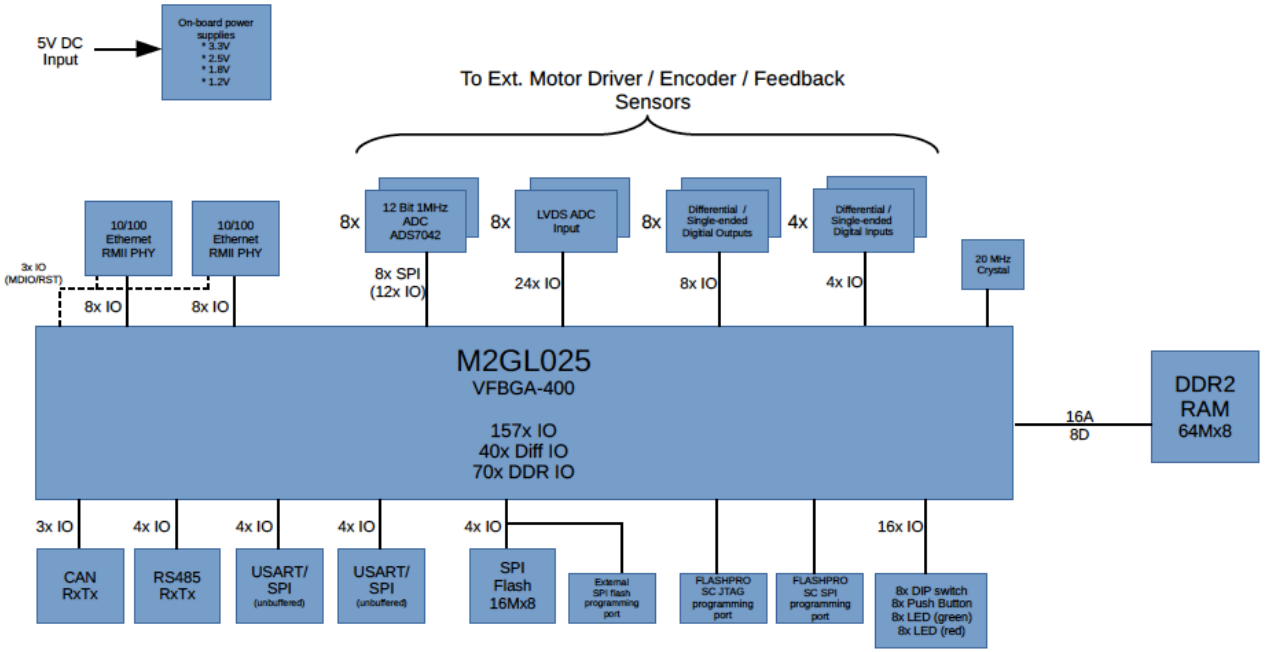
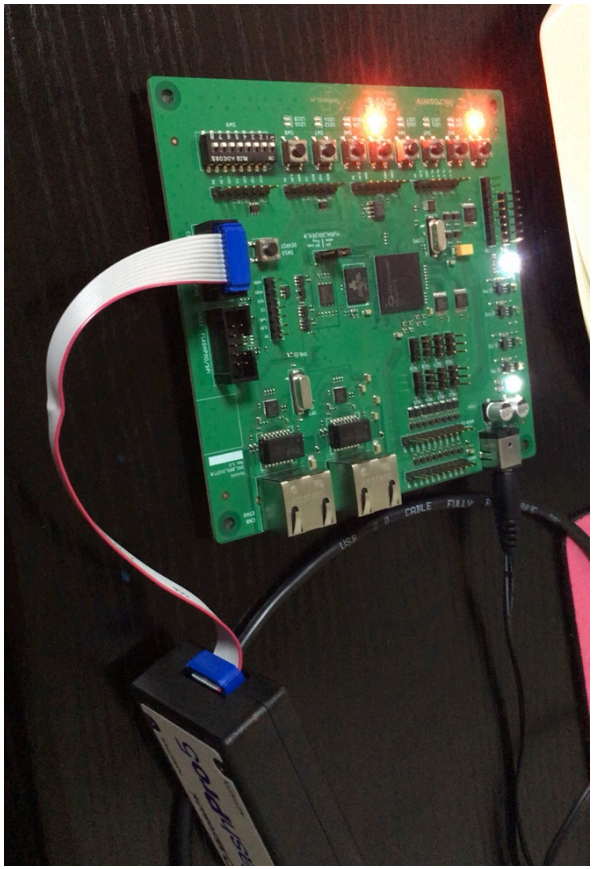
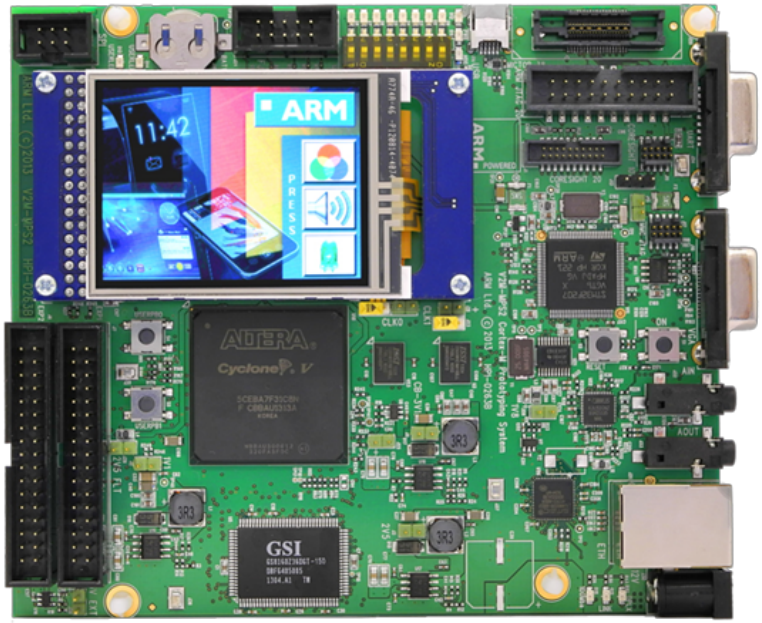


Illustration 1: Board Block Diagram



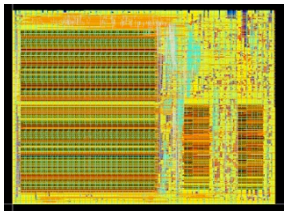
ARM M23/33 MPS2+ へのクリプトスペック集積

- M23やM33の正式ライセンスは高価。ARM社のMPS2+ FPGA Prototyping Boardが存在する。上記ARMソフトコアをFPGAに乗せたキットを価格13万円で販売。
- FPGAはアルテラの標準300K LE。コア内部は暗号化されている。動かすだけならコンフィグバイナリが付いている。TOPレベル記述も自分で書ける。AMBAに自分の周辺を接続できる。開発環境を繋げてソフトを開発できる。



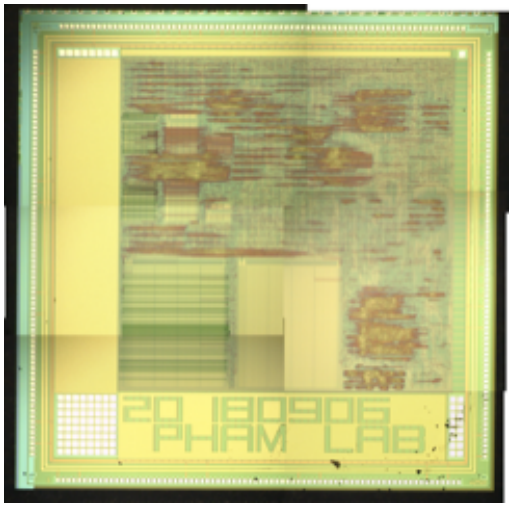
開発キット

オープンなセキュアMCU
Igloo2 25KG FPGA



＋

オープンRISC-Vコア

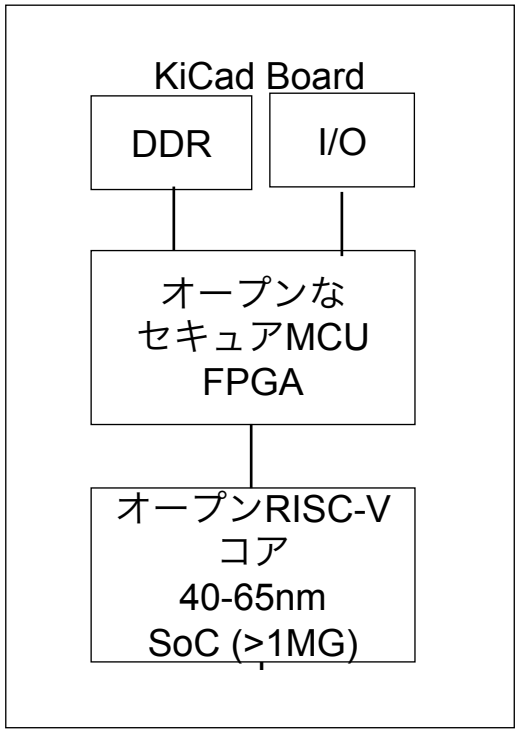


開発ボード　Kicad

＋

オープンな開発環境
OP-TEE移植 = トラスト環境
（Trusted Execution Environment）

POCボード



ありがとうございました。