RISC-V Days Tokyo 2020

nVidia-ARM合併、ルネサスのRISC-V採用
その裏にある大きなオープンソースハードウェアの潮流

NVIDIA-ARM Merger, Renesas RISC-V Adoption, and Open Source Hardware Movement in Background

令和2年11月06日

河崎　俊平

RISC-V協会

SHコンサルティング（株）

@risc_v
@riscv_a

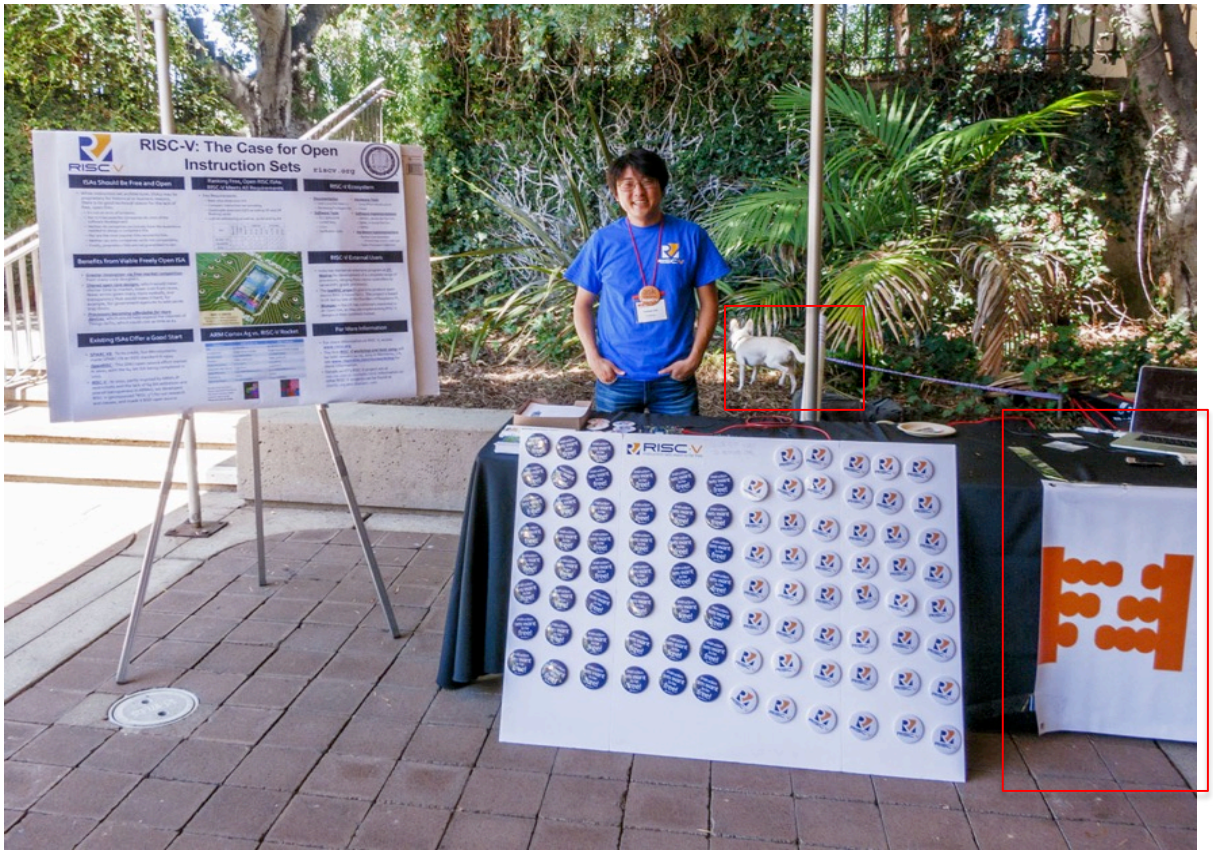
RISC-V® 協会
RISC-V Association

発表内容

1. 背景紹介
2. nVidia-ARM合併　と　RISC-Vへの影響
3. ルネサスのRISC-V採用
4. オープンソース　セキュリティ
5. RISC-Vからスタートしたオープンハードウエアの潮流
6. まとめ

1. 背景紹介

2014
RISC-Vとの出会い



SHマイコン@Hot Chip 26

SHマイコン2013年廃止

- 囚われIP化
- 2545 ISA特許失効　　ISA使用権解放

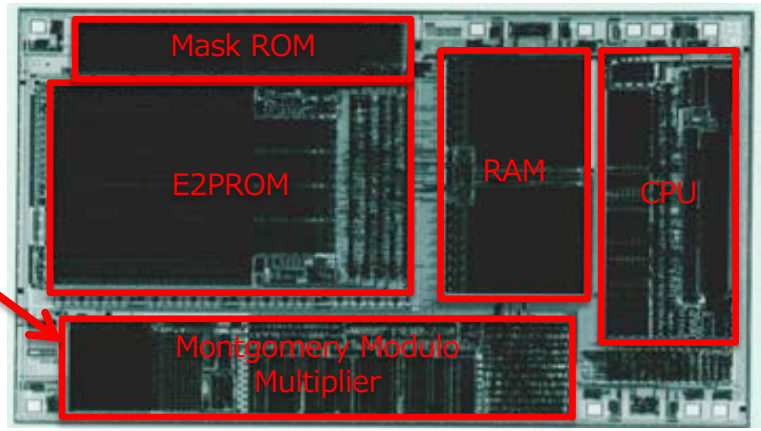
オープンソースSH-2

第２弾発表

- 2003 opencores.org
- 2014 0pf.org
- 2016~

発表者経歴

世界初のPKI用チップ
日立製作所 H8/3111 1998



1980-1986　68K、AIチップ

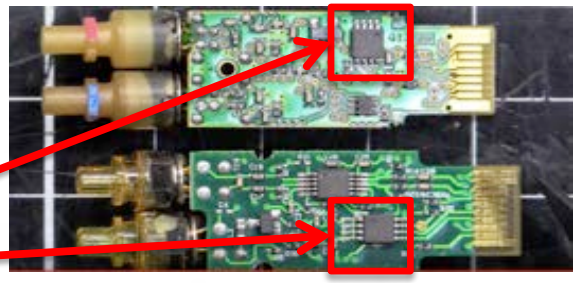
1986-2001 サターン、ドリキャスチップセット

<低迷>

2001　米国駐在中大手電機メーカ退社

ローカル雇いソフト転向

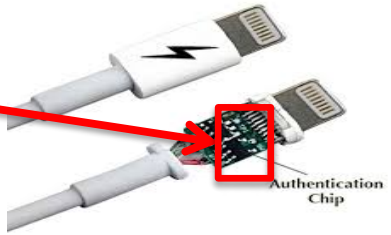
Java Card™ 、テレマ開発



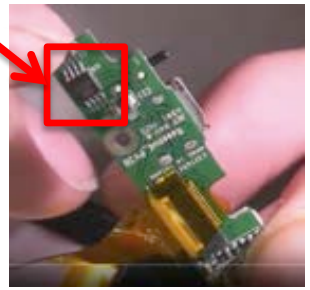
2003　ルータ真贋判定　C暗号ライブラリ

2007　北米スマホ大手用　セキュアOS

2010　FIPS140-2 Level 3取得作業



<低迷>



2013　大手半導体企業販社退社　SHC社設立

ソフトウエア、ハードウエア（FPGA）

2015
自由なISA と 解放されたISA連合

2004
OpenRISC
opencores.org
東欧ウエブ

OpenCores
www.opencores.org

2015
RISC-V
カリフォルニア非営利

RISC-V

2003
Aquarius **SH-2**
Verilog opencores.org
東欧ウエブ

OpenCores
www.opencores.org

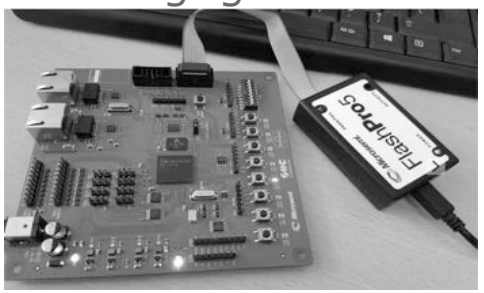
2014
特許失効

2014
J201 **SH-2**
VHDL 0pf.org
カリフォルニア非営利

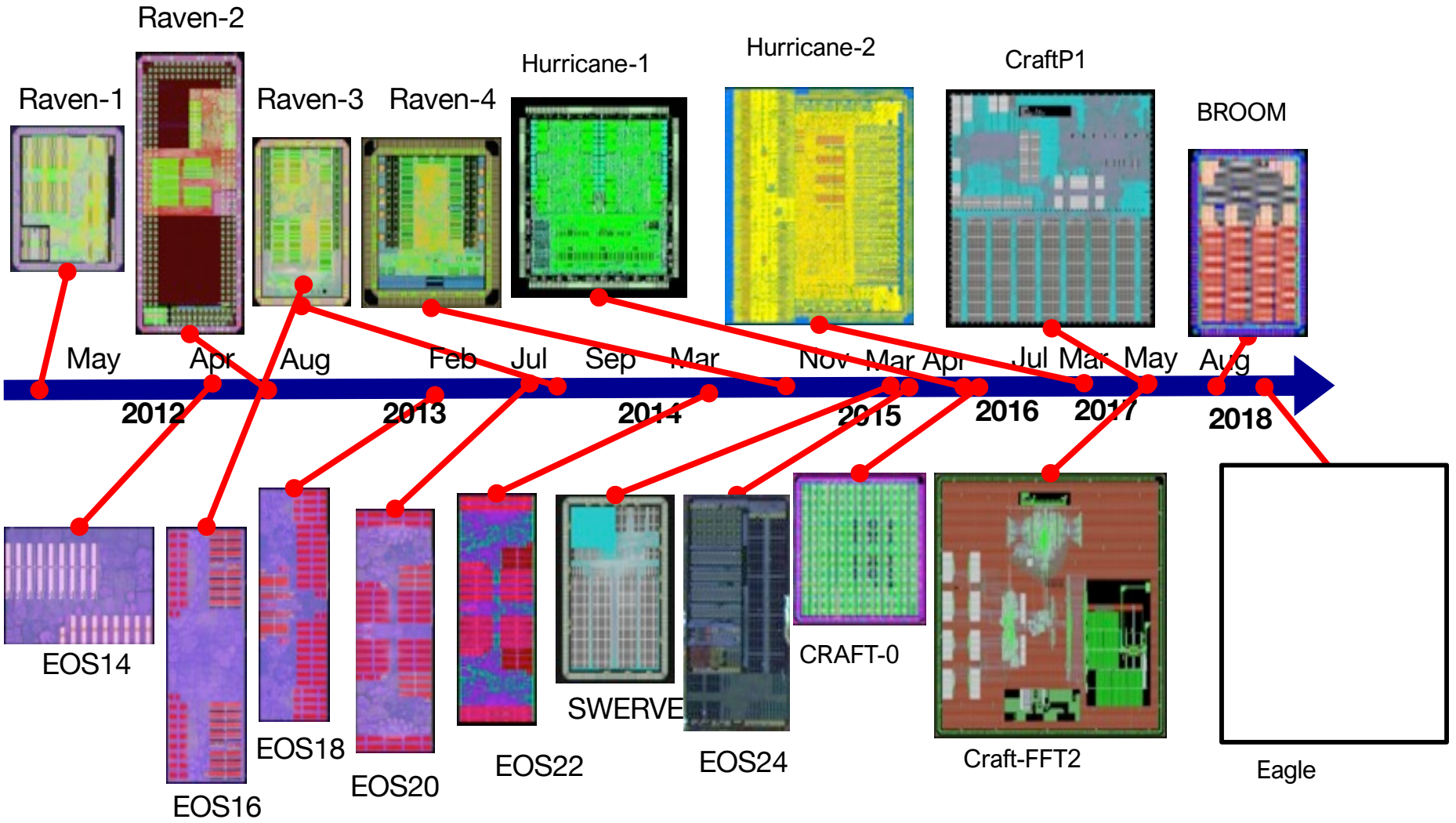
Open Processor Foundation

2016
クリーン
ルーム
開発

2019
J202 **SH-2**
Sverilog Igloo2 FPGA



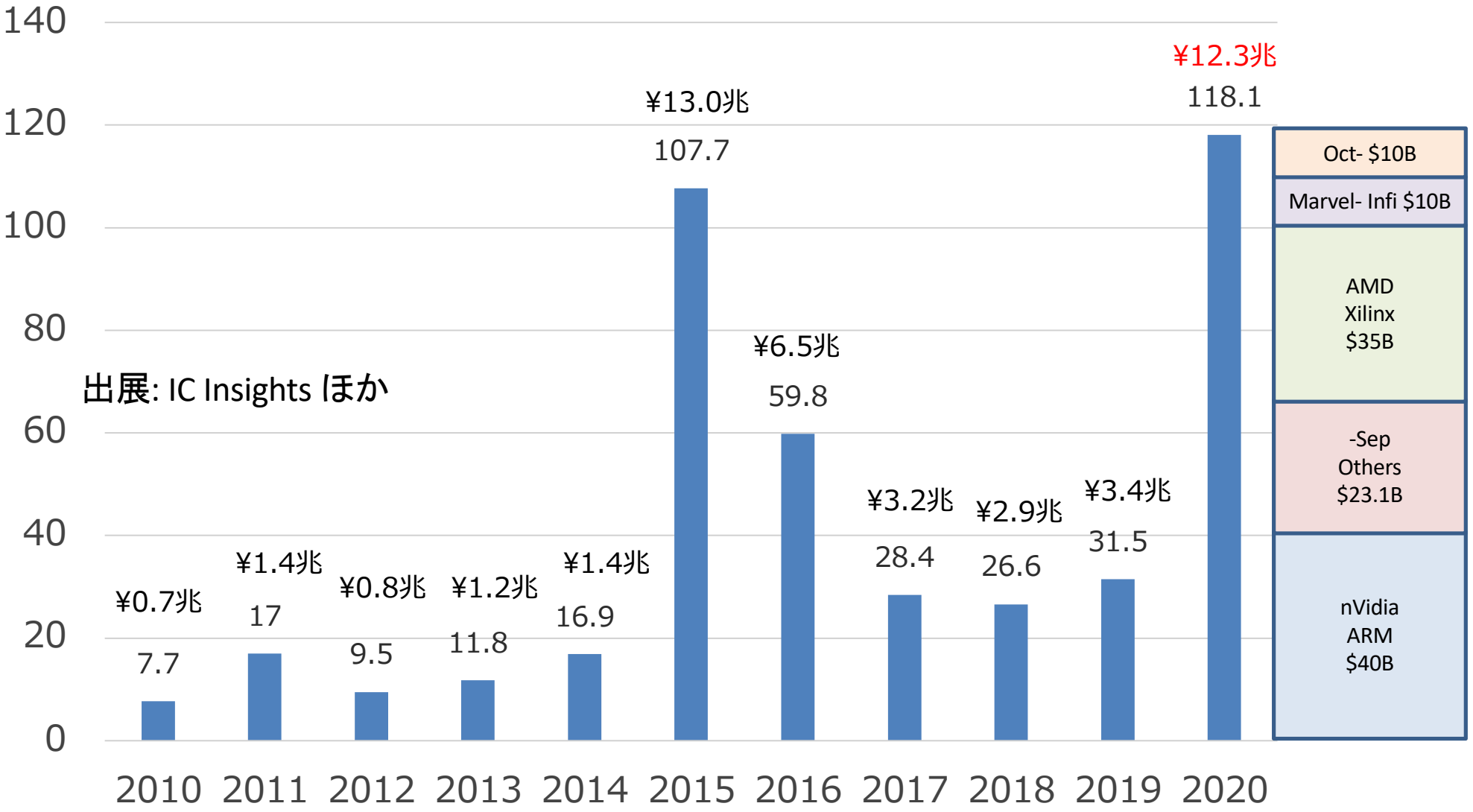
RISC-V: チップ実装、ソフト実装で裏付けアーキテクチャリリース



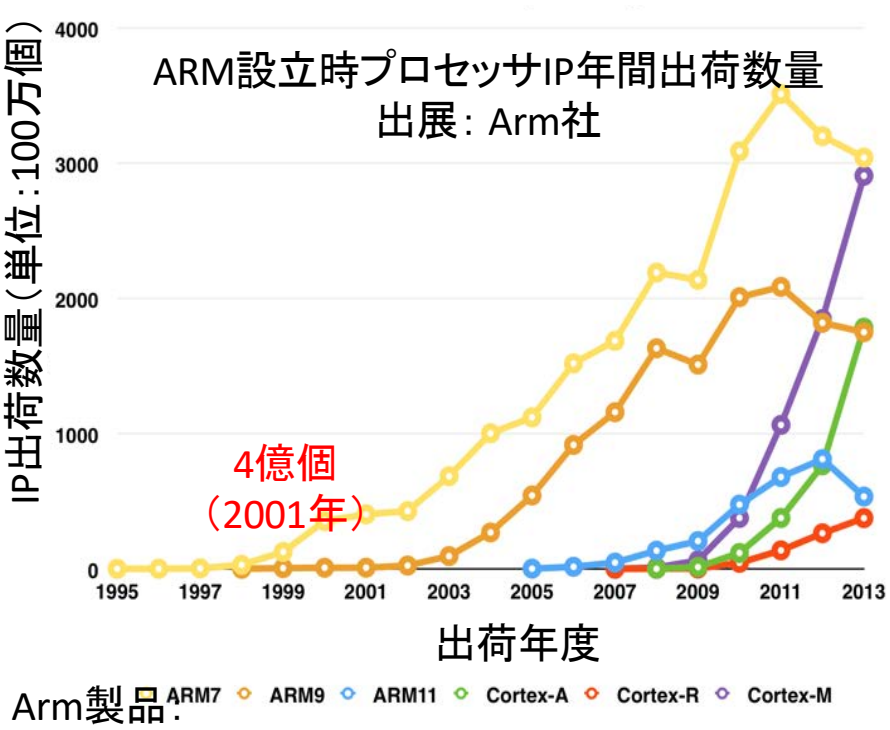
IBM 45nm, ST 28nm FDOI, TSMC 28nm and 16nm FF, GF 14nmで設計

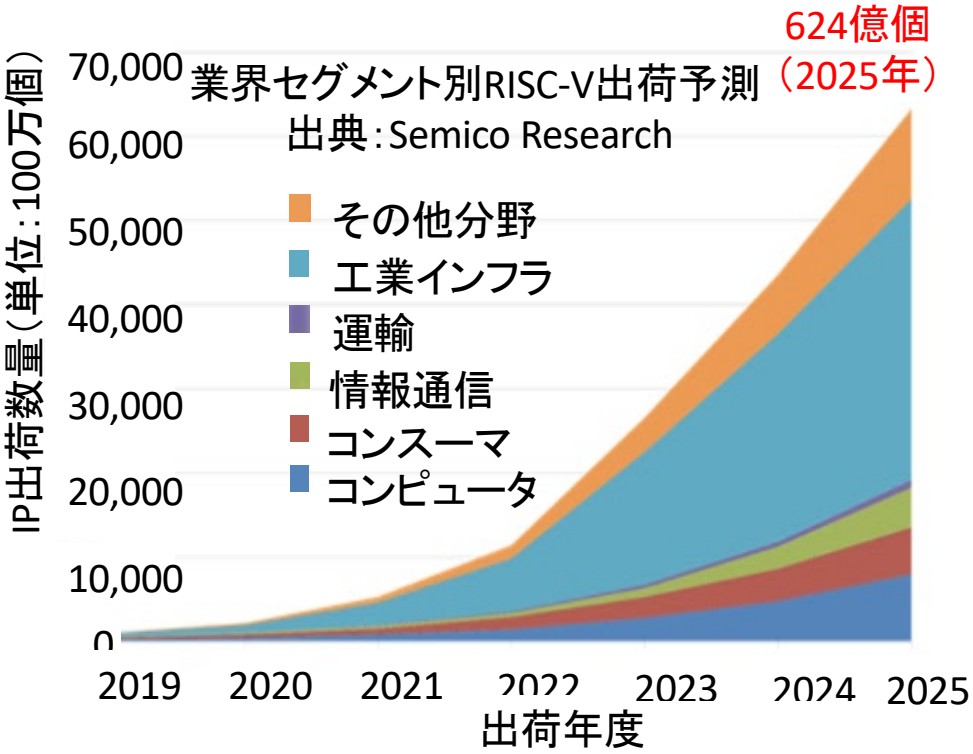
2. エヌビディアによるARM買収

半導体M&A 世界市場合計 ($B = 10億ドル)



ARM と RISC-V 出荷数量の伸び率比較





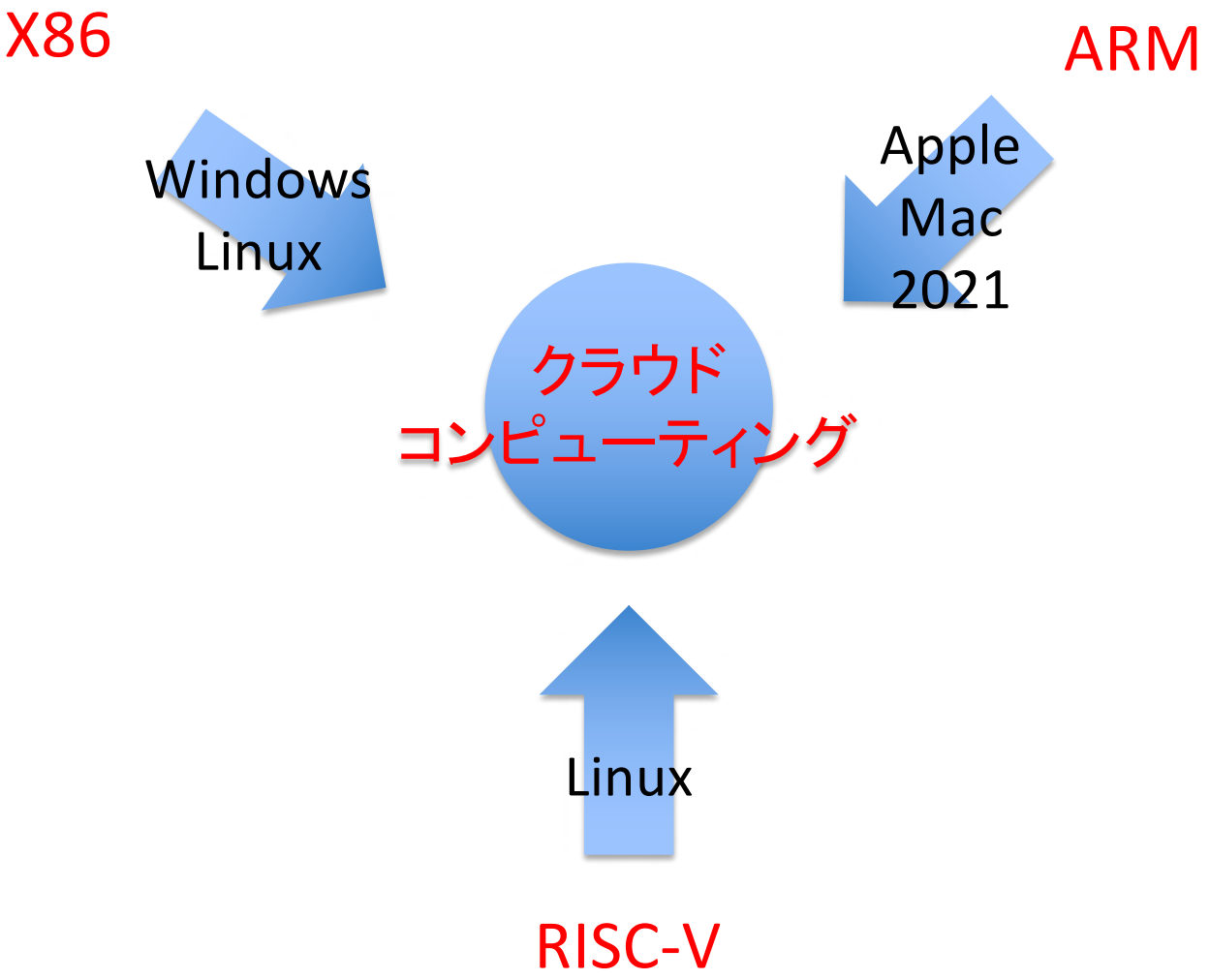
RISC-V PC と クラウド応用
RISC-V PC and Cloud Applications

RISC-V PC

「クラウド」では、命令セットが重要ではないと考える人もいます。それはでたらめです。と、トーバルズ氏はフォーラムの投稿で述べています。x86で開発する場合は、レジデント環境で開発し、クラウドにデプロイします。X86では、「レジデント環境」で実行できるため、「レジデント環境」でテストしたものを、クラウドにデプロイできます。 つまり、文字通りあなたの家にいるという意味ではなく、あなたの職場環境にいるという意味です。
リーナス トラボルド

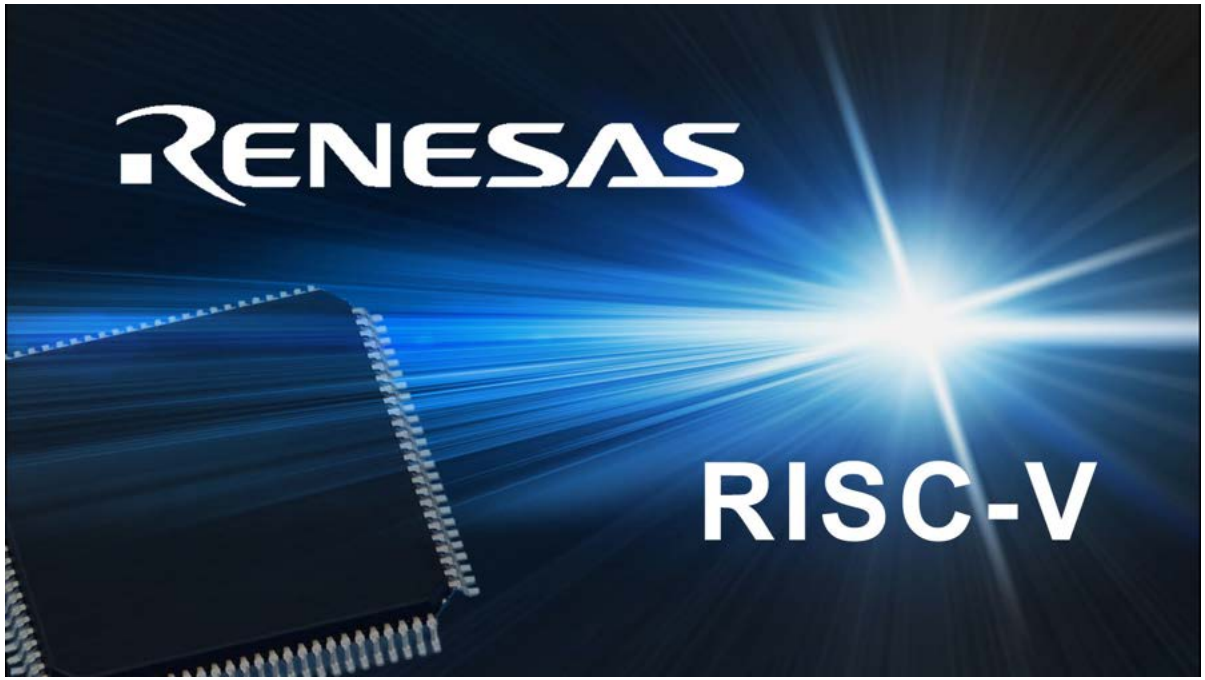
"Some people think that 'the cloud' means that the instruction set doesn't matter," Torvalds said in a forum post. "Develop at home, deploy in the cloud. That's bullshit. If you develop on x86, then you're going to want to deploy on x86, because you'll be able to run what you test 'at home' (and by 'at home' I don't mean literally in your home, but in your work environment)."
Sat 23 Feb 2019 https://www.theregister.com/2019/02/23/linus_torvalds_arm_x86_servers/

レジデントPC開発環境 → クラウドプログラミング
PC → cloud computing



3.ルネサスのRISC-V採用

ルネサス　と　RISC-V



4. オープンソースセキュリティ

高い質のセキュリティ技術を
オープンソースで提供する

… I think what you are working on is important. I don‘t know of any open source high quality security solutions…

Andreas Olofsson, DARPA MTO

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。

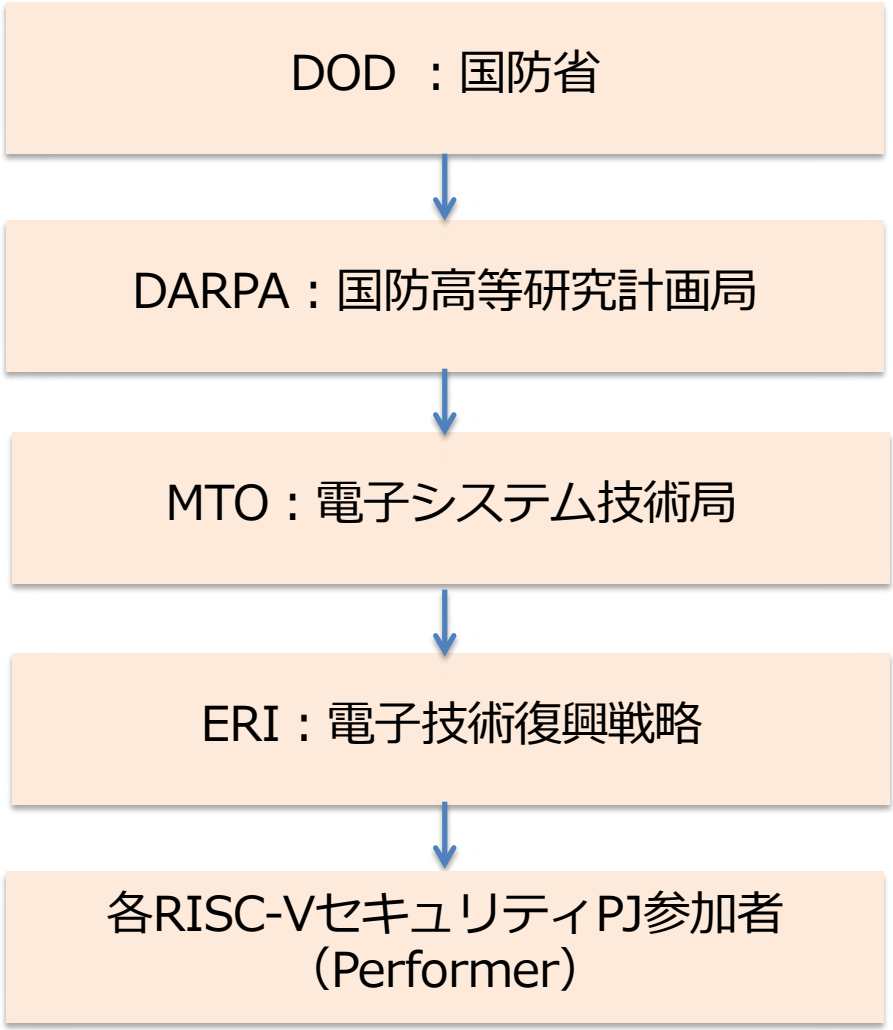
暗号技術において、ケルクホフスの原理とは、19世紀にアウグスト・ケルクホフスによって提案された原理である：

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。

信頼基点商品（チップ、IP）の多くでは、実装を一般公開してない。

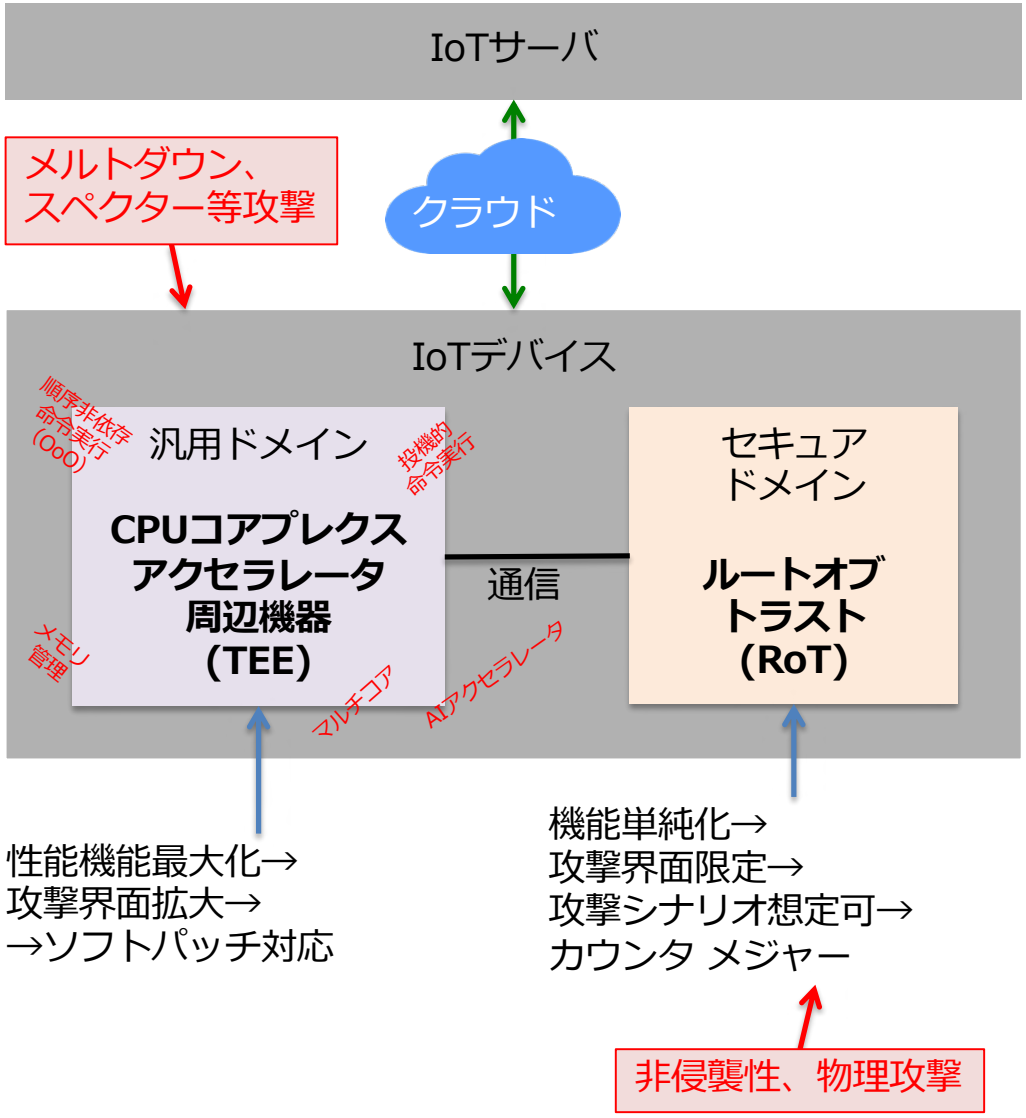
実装の構成方法を公開しても、秘密鍵を守る工夫をすれば、安全な実装は可能なはずである。

RISC-Vセキュリティ とDARPA



- 2017年に米国DARPAはセキュリティ研究にはRISC-VをCPUとして使うことをファンディング条件として義務付けた。
- DARPAは2018年12月にRISC-V用LLVMコンパイラのファンディングを始めた。

信頼基点モジュールを分離独立



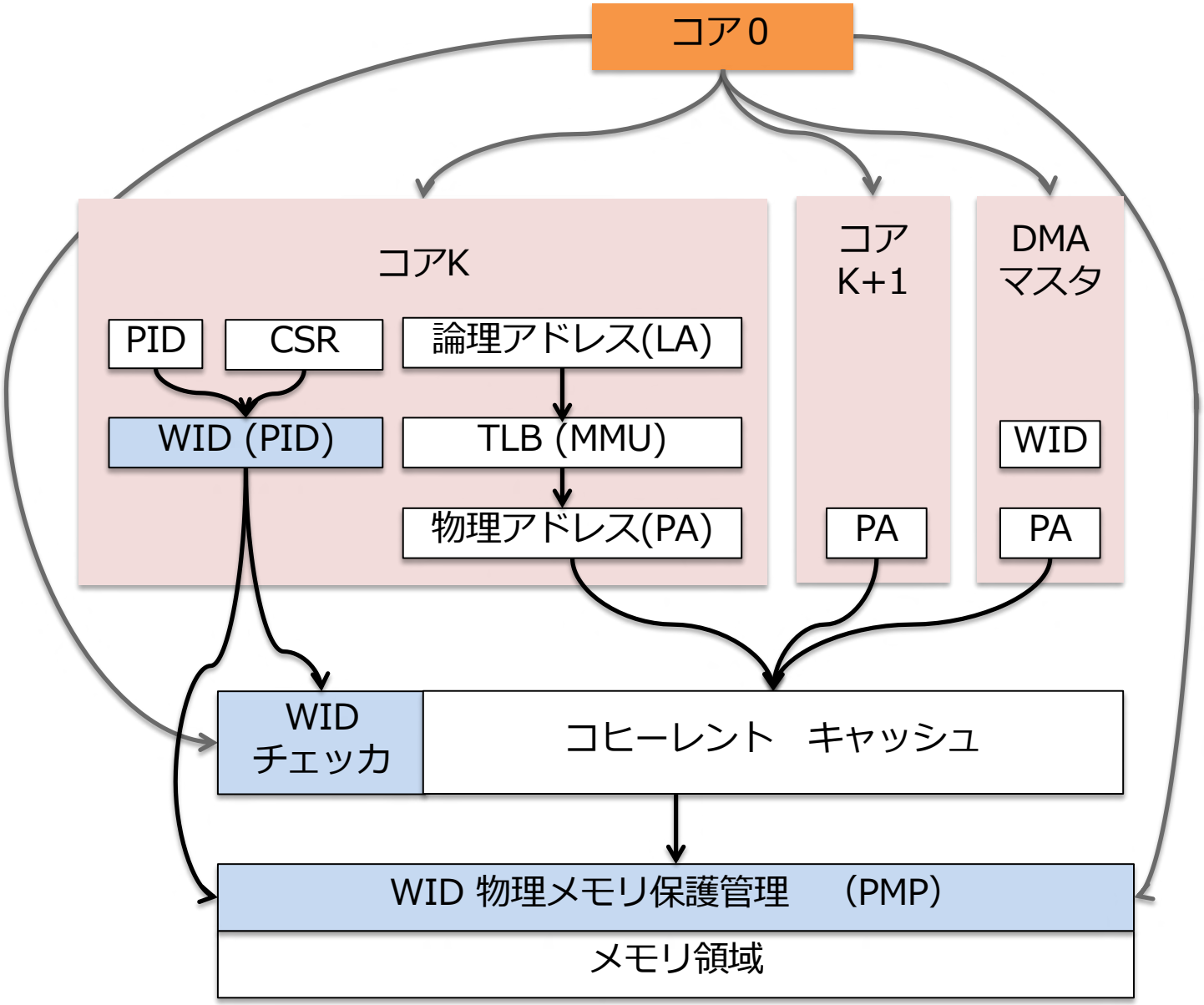
- 汎用処理CPUは複雑。複雑さゆえに守る方法がキャッチアップしない。
- 信頼起点を分離。単純なシステムを多様な方法で守る。
- 各攻撃法を網羅的に分析し、防衛方法を構築し各個撃破する。

SiFive 「シールド」比較表

10/23/2019発表

機能	シールドのセキュリティ	競合他社セキュリティ
複数ワールドのサポート	無制限の数をサポート可	部分サポート
マルチ コア サポート	有	部分サポート
ソフトウエア複雑性	低	非常に高い
コンパイルし直しの必要性	リコンパイルなし	完全リコンパイル必要
ユーザモードでの 割り込みサービスルーチン	有 RISC-V基本アーキテクチャに内蔵	無
プロセサIDごとの隔離	有	無
DMA転送の保護	有	有
メモリと周辺のフィルタ	有	有
独自暗号エンジン	有 オープンソース	有
鍵プロビジョニング	SIFive サービス（独自サービスも可）	サードパーティ
オープンソースのセキュアブート	有	有

ワールドID動作原理



複数セキュア隔離（WIDで実現）と特権モードの関わり合い方がTrustZone異なり2002年特許群を回避している。本方式は68000が当初標榜していた先行方式とほぼ同一。

68000 FC
先行技術例

ファンクションコードと参照の分類[6]

FC2	FC1	FC0	参照の分類
0	0	0	未定義
0	0	1	ユーザ・データ
0	1	0	ユーザ・プログラム
0	1	1	未定義
1	0	0	未定義
1	0	1	スーパーバイザ・データ
1	1	0	スーパーバイザ・プログラム
1	1	1	割り込み応答

Open Titan RISC-V ルートオブトラスト

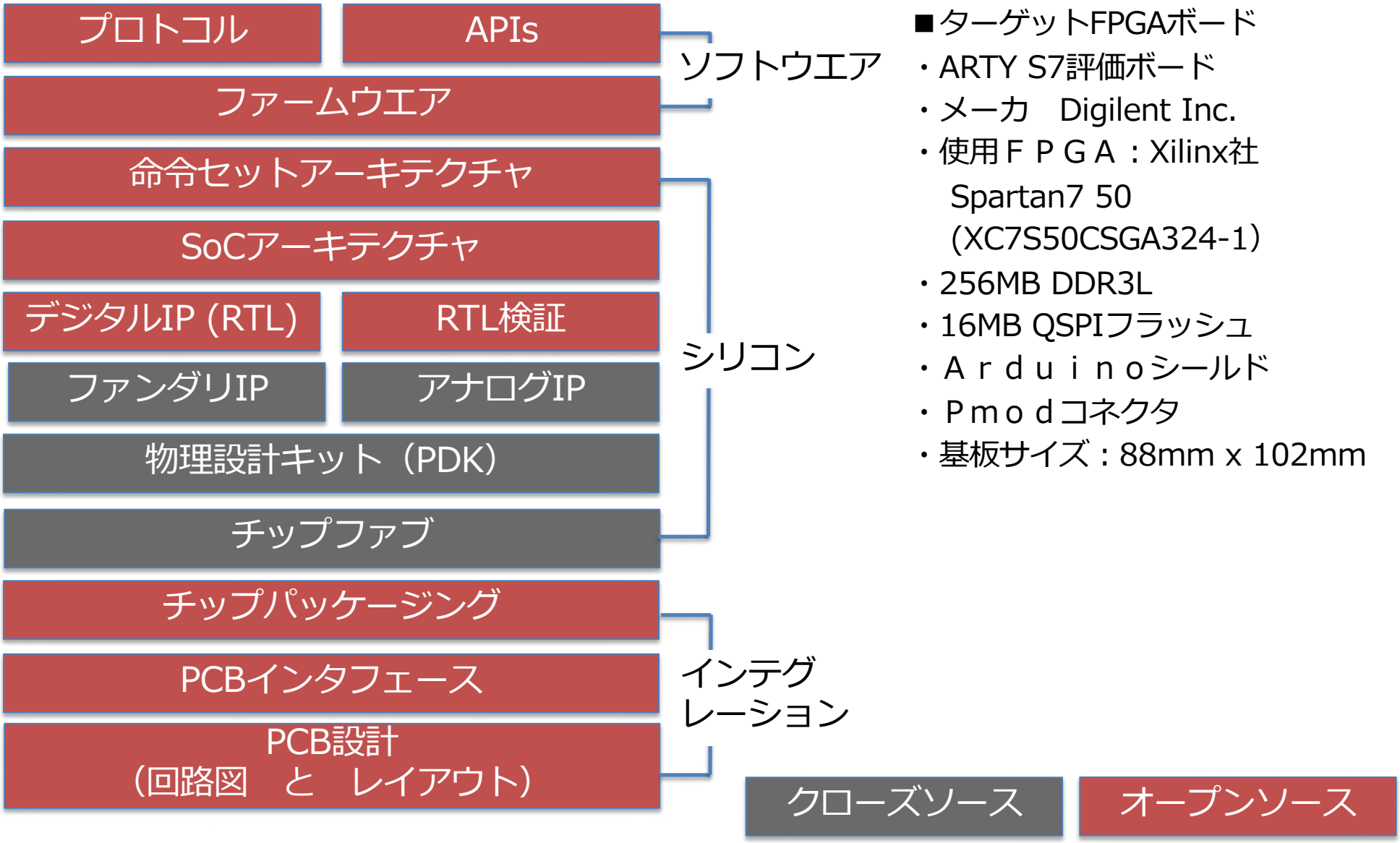
2019/10/14発表

- ハードウェア非営利のlowRISC CICがオープンソース管理。

- 「透明性とセキュリティは密接に関係しており、全てはオープンソースのルートオブトラストの構築につながります。ベンダのチップは不透明で、何が起こっているのか不明な要素が入ります。オペレーティングシステムからチップと会話ができますが、その下の要素とアーキテクチャは見えません。」- lowRISC CIC

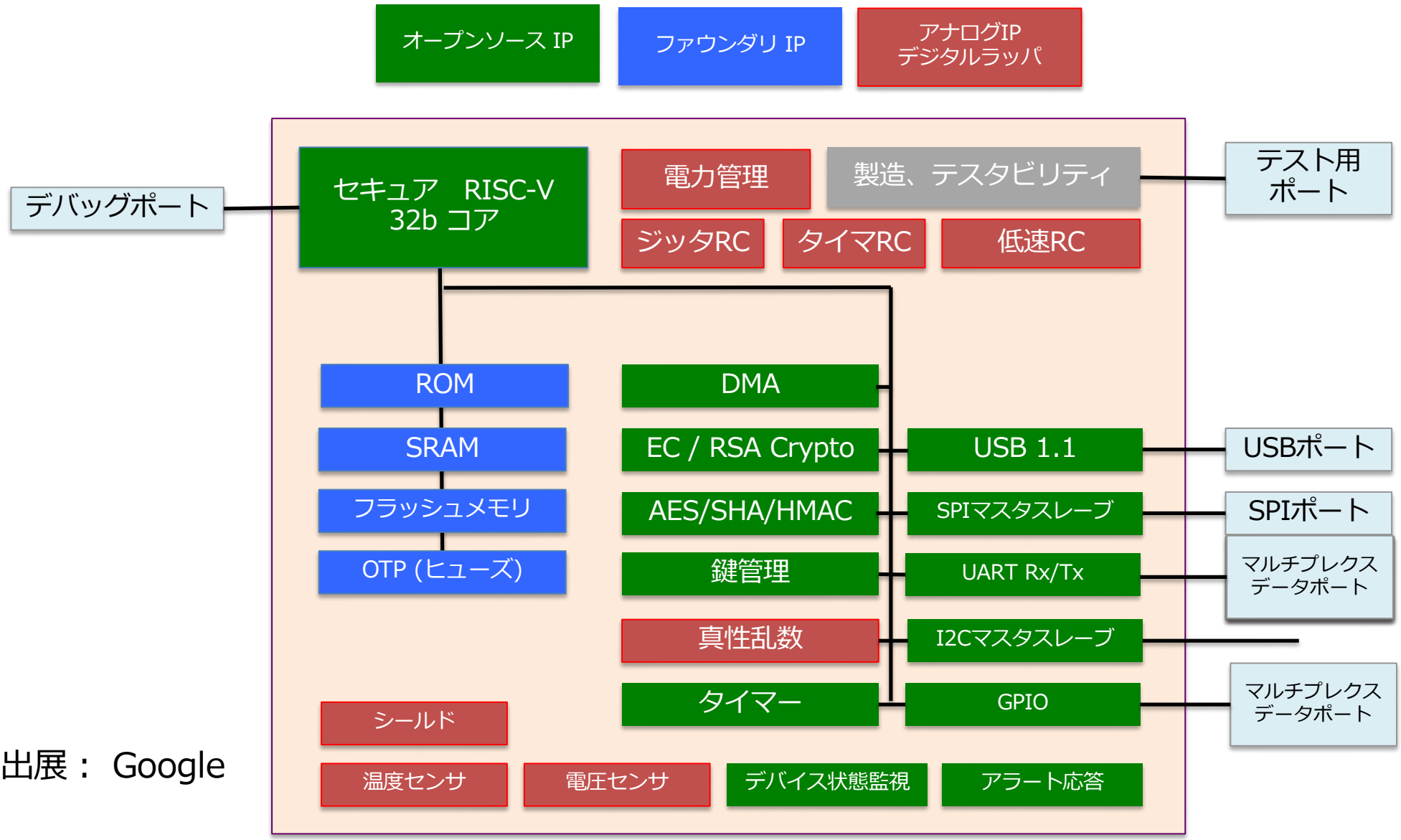
- OpenTitanは、Google携帯電話用Pixel3/4の独自ルートオブトラストチップの技術に流用されます。 OpenTitanは独自のチップアーキテクチャで、ETH Zurich、G+D Mobile Security、Nuvoton Technology、Western Digital、Googleのと共にlowRISCのエンジニアが開発した回路です。- Google

OpenTitan目的



■ターゲットFPGAボード
- ARTY S7評価ボード
- メーカ　Digilent Inc.
- 使用ＦＰＧＡ：Xilinx社
  Spartan7 50
  (XC7S50CSGA324-1)
- 256MB DDR3L
- 16MB QSPIフラッシュ
- Ａｒｄｕｉｎｏシールド
- Ｐｍｏｄコネクタ
- 基板サイズ：88mm x 102mm

Open Titan 構成

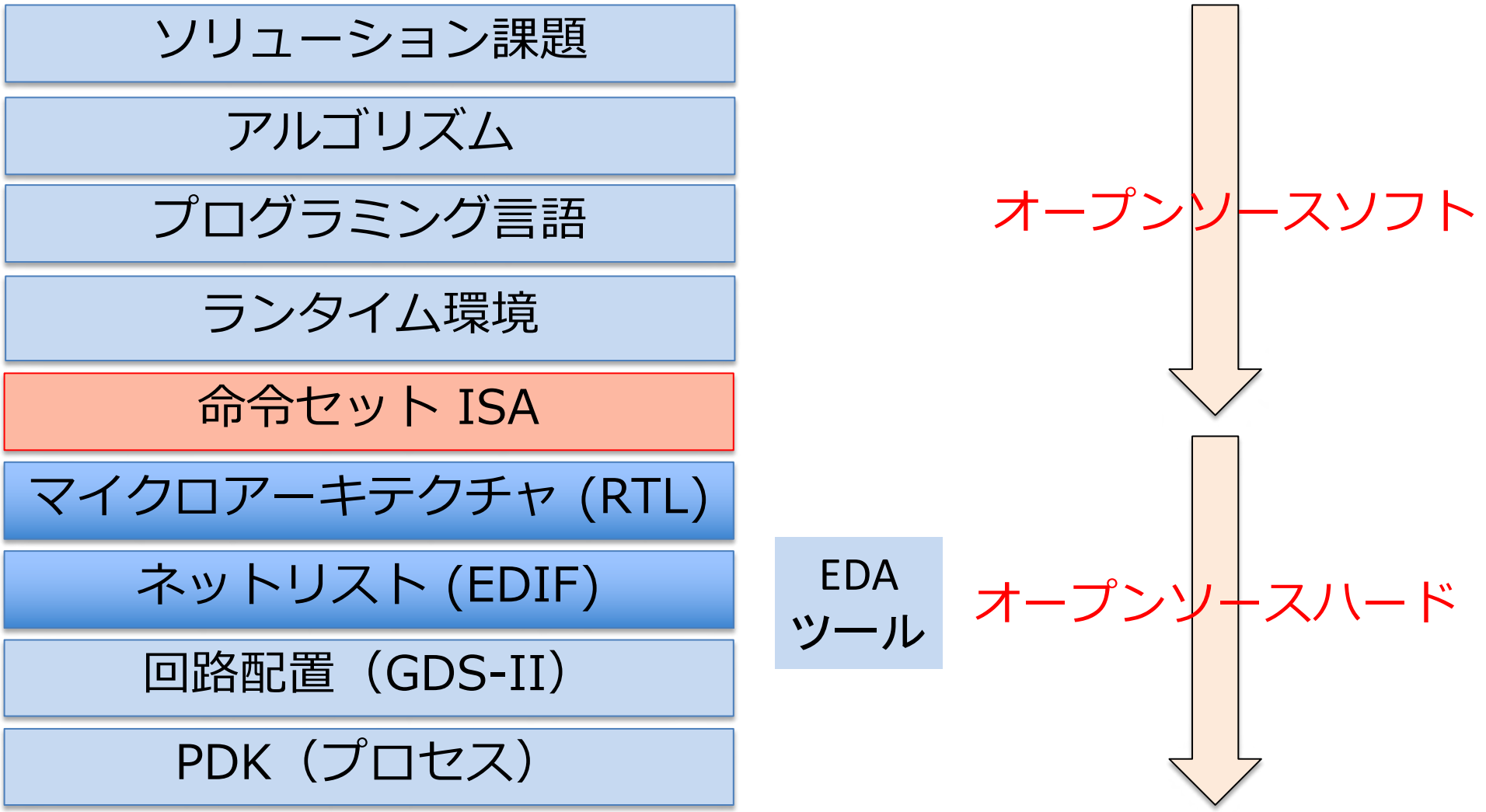


出展： Google

5.　RISC-Vからスタートした オープンハードウエアの潮流

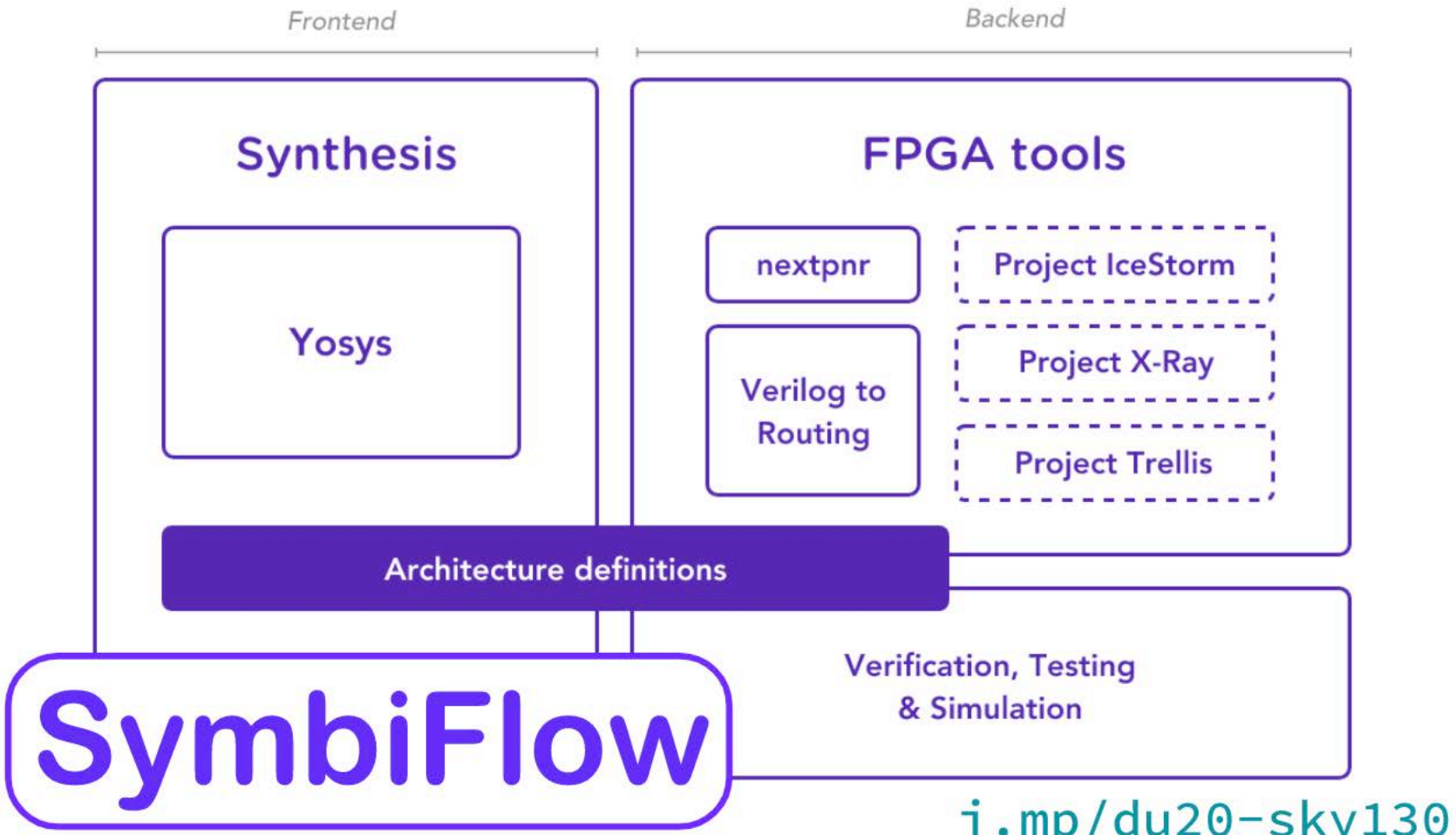
オープンソース
EDAツール PDK
（プロセスデベロップメントキット）

命令セットアーキテクチャ(ISA)の位置付け



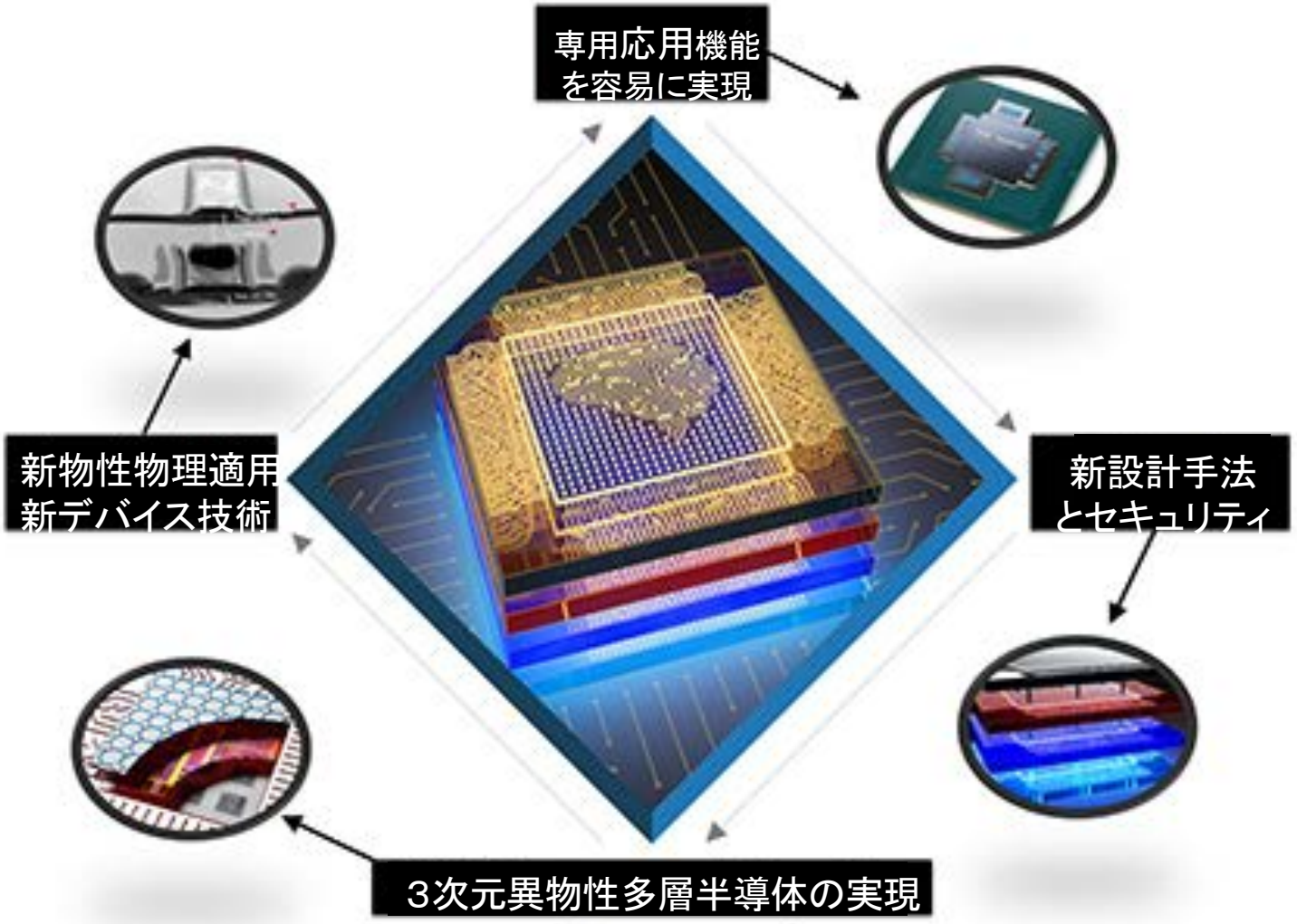
FPGAオープンソースツール

FPGAにはRTLのものをそのまま作ることができる。
機能検証をソフトと一緒、システムと一緒にできる



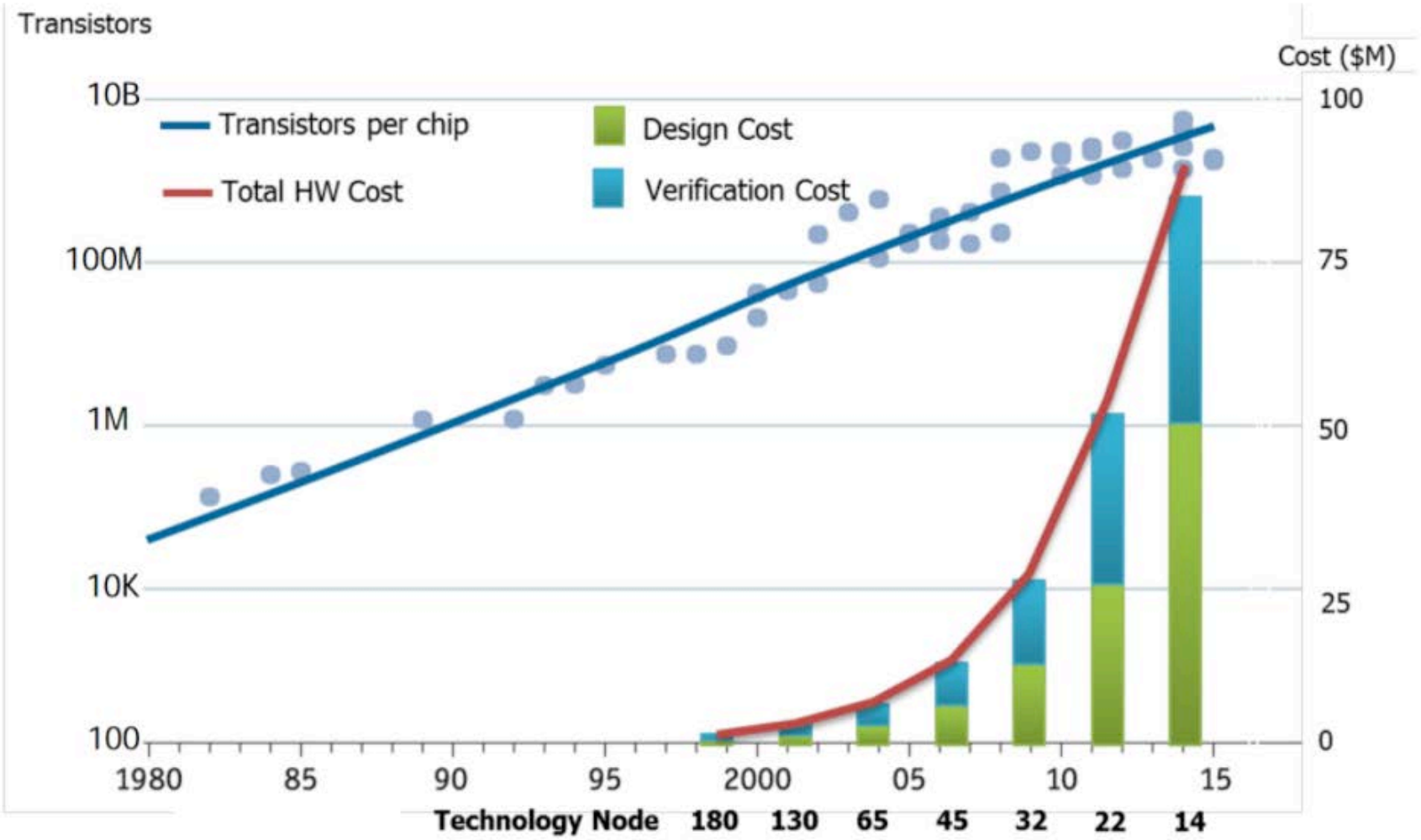
j.mp/du20-sky130

米国国防省　DARPA の 電子システム復興運動（ERI）
US Defense Department DARPA's Electronics Resurgence Initiative

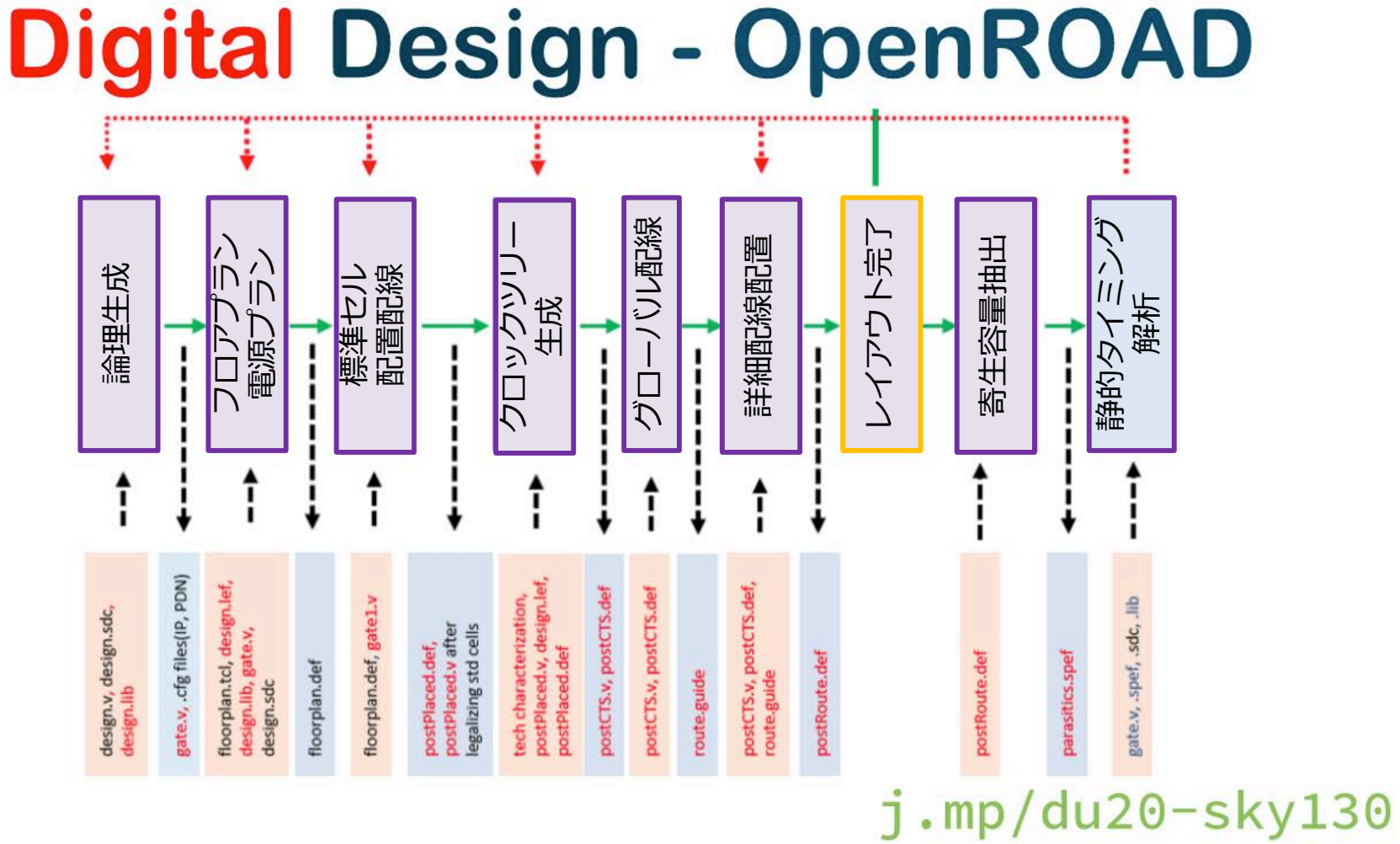


電子システム復興運動（ERI）の背景

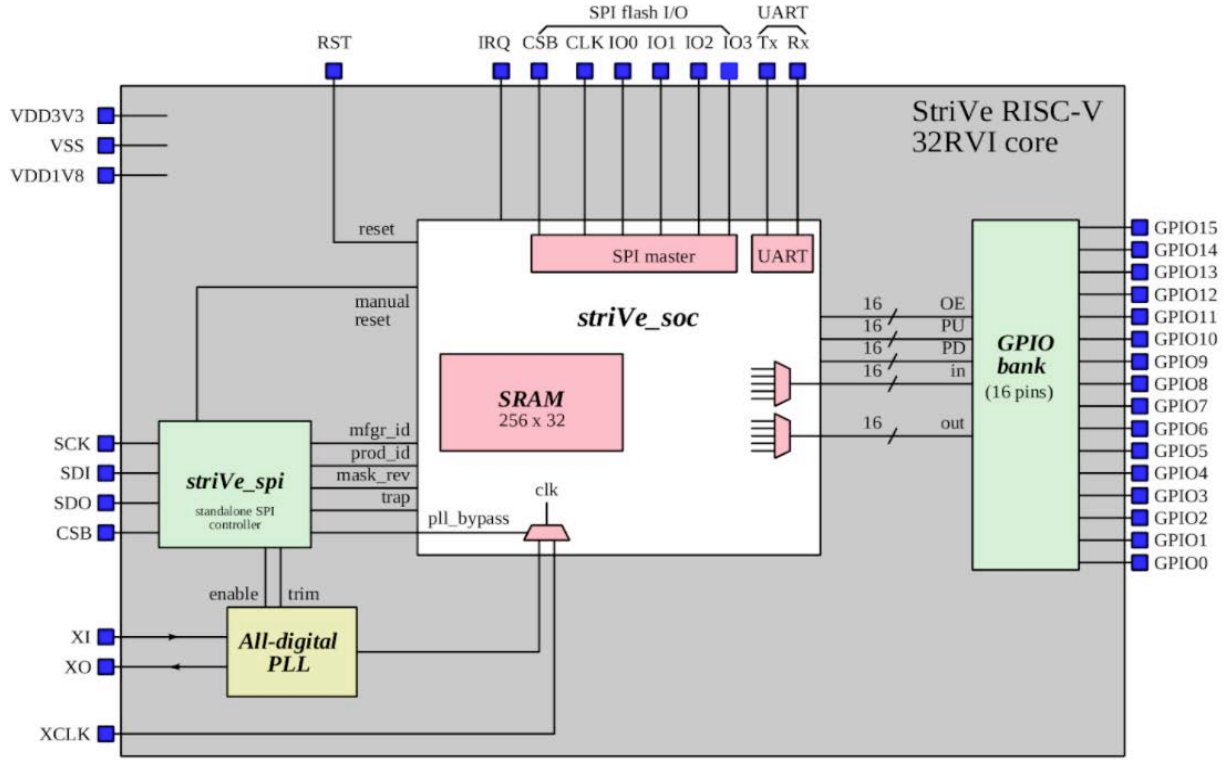
DARPA Has EDA failed to keep up with Moore's Law?

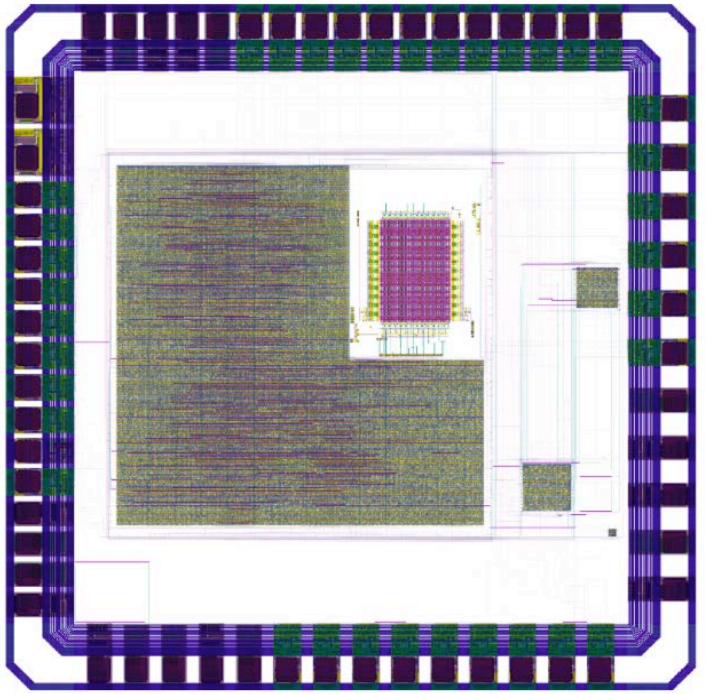


OpenROADによるデジタル設計フロー
Digital design flow with OpenROAD

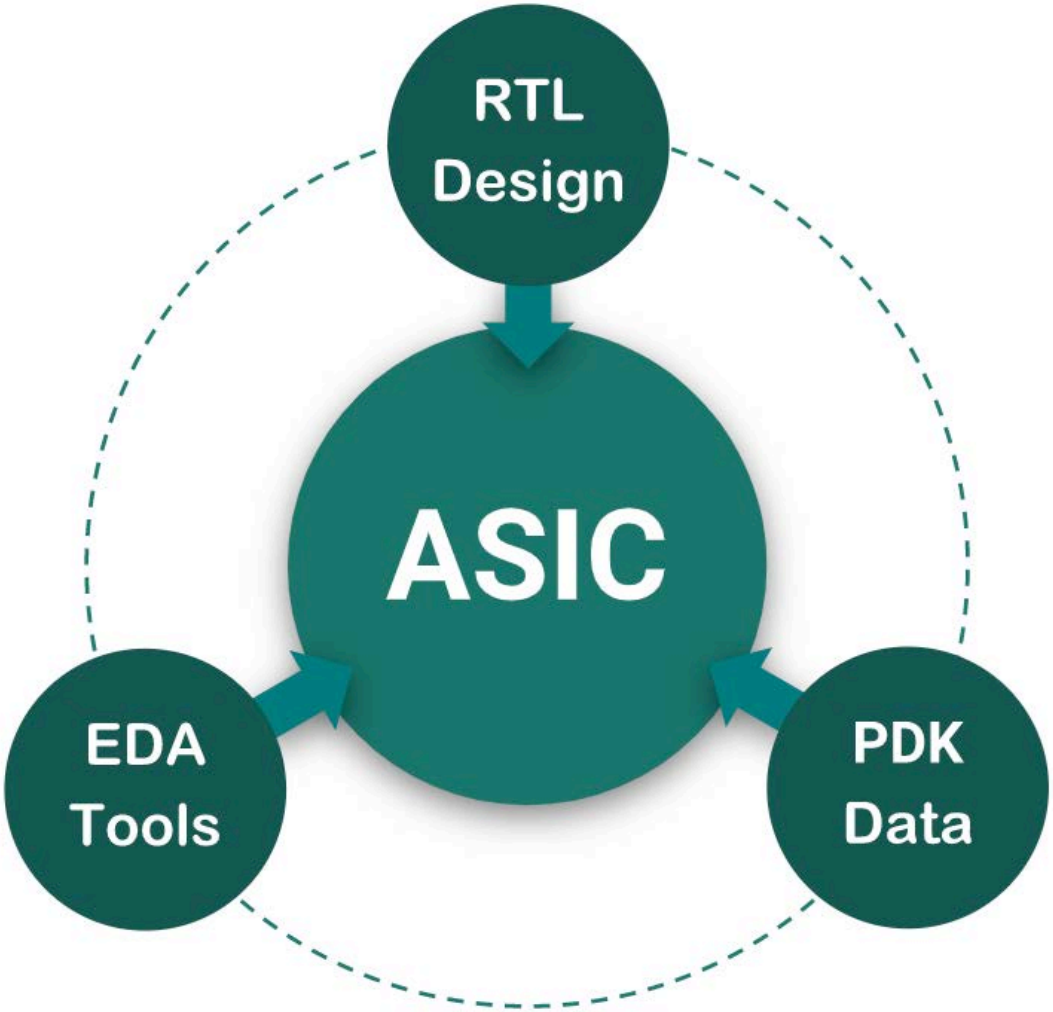


Google等による開発例

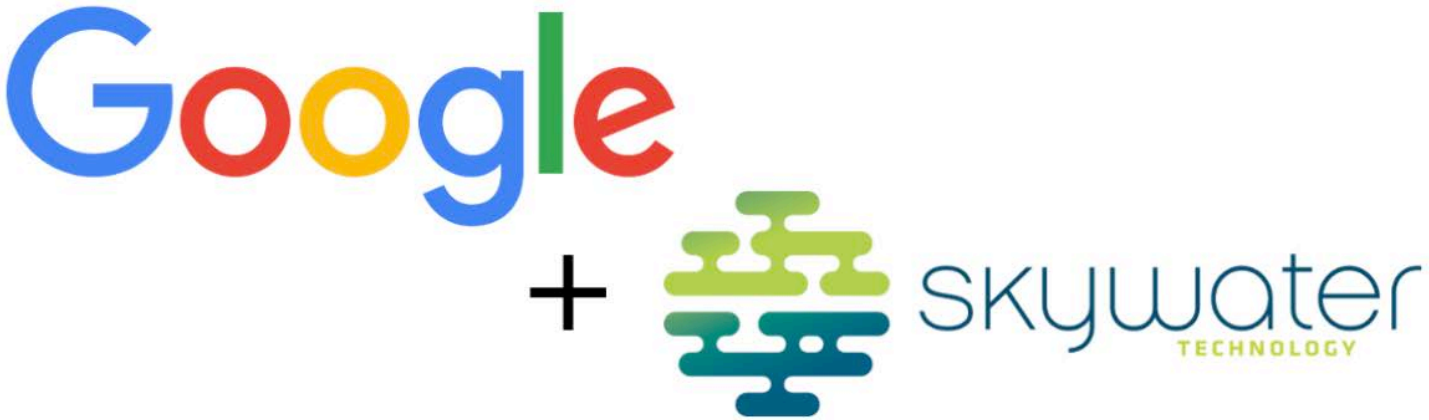




オープンソース運動の実態



プロセスデベロップメントキット



FOSS 130nm Production PDK

github.com/google/skywater-pdk

6. まとめ

- RISC-Vは、ハードウエア　オープンソースの潮流を作った
- そのオープンソースの潮流はハード抽象レイヤ全域に渡った
- RISC-Vはソフトの面でもクラウドコンピューティングの地盤を作りつつある。