明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

TEEの概要 RISC-V PMPを中心に
2023/12/18

情報セキュリティ大学院大学
須崎 有康 (Kuniyasu Suzaki)

簡単な自己紹介（Kuniyasu Suzaki,須崎有康）

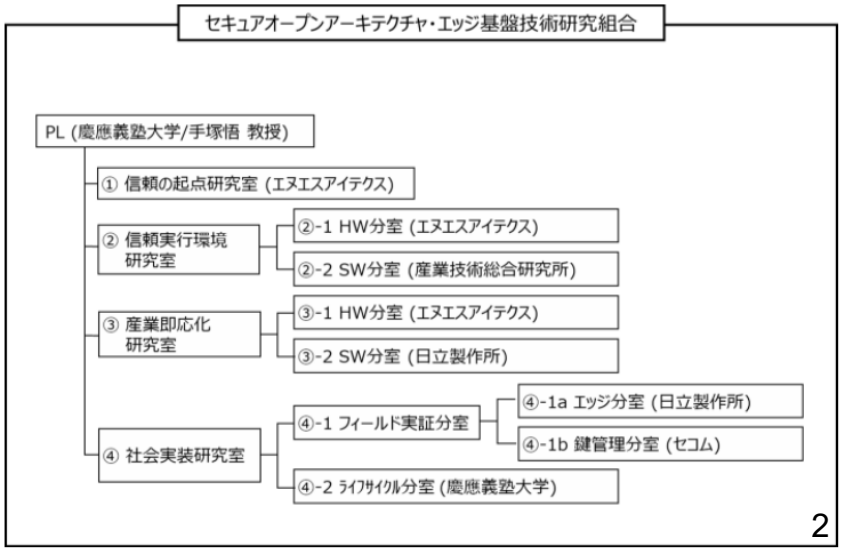
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 情報セキュリティ大学院大学に2022/9/1より奉職

- 前職：産業技術総合研究所サイバーフィジカルセキュリティ研究センター
  (2023/3までクロスアポイントメント)
- セキュアオープンアーキテクチャ・エッジ基盤技術研究組合(TRASIO)の
  研究員

◆NEDOプロジェクト「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 FY2018-2022」でRISC-VベースのTEE(Trusted Execution Environment)の研究

研究体制図



今までの研究経緯

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- TPM: Trusted Platform Module
  - 振興調整費「組込みシステム向け情報セキュリティ技術（研究代表者：柴山悦哉＠東大教授＆情セ大客員教授、2006-08）」
  - 日本IBMからの再委託(METI新世代情報セキュリティ研究開発事業、2007)

TPMによるRemote attestationを実現した。
TCGのInvited Expert (2019～)

- ARM TrustZone
  - JST日台研究交流「偽造困難なデバイスを用いたIoTセキュリティ管理システム」 (2015-17)

ACSAC2020論文
Reboot-Oriented IoTに結実

- RISC-V TEE
  - NEDOプロジェクト(2019-23)でRISC-V TEEのソフトウェア開発
    - ◆セキュアオープンアーキテクチャ・エッジ基盤技術研究組合 (TRASIO)が担当

IEEE TrustCom、RISC-V Forum Security、IEEE Access に結実

- 電通大、筑波大の学生。産総研リサーチアシスタント
  - Arm TrustZone, Intel SGXのRemote Attestation (Xeon DCAP)

⇦ **論文投稿中。中々通らない。**

- Zero-Trust IoT
  - JST CREST（2021-27 NII竹房教授, 京大 五十嵐教授, TID 松井教授)
  - TEE(Arm TrustZone)を活用したIoT

Reference 参考資料

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Trusted Execution Environmentによるシステムの堅牢化, 情報処理20/06
  - https://ci.nii.ac.jp/naid/40022255769
- Trusted Execution Environmentの実装とそれを支える技術,電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 2020/10 (無償公開)
  - https://www.jstage.jst.go.jp/article/essfr/14/2/14_107/_article/-char/ja/
- RISC-V におけるプロセッサセキュリティ機構とシステムアーキテクチャ—TEE (Trusted Execution Environment), Hardware Root of Trust, Remote Attestation,「システム／制御／情報」第67巻 第9号「オープンなプロセッサとドメイン最適化技術」特集号,システム制御情報学会, 2023/09 (無償公開予定)
- ResearchMapに公開資料があります。 https://researchmap.jp/kuniyasu-suzaki

これから

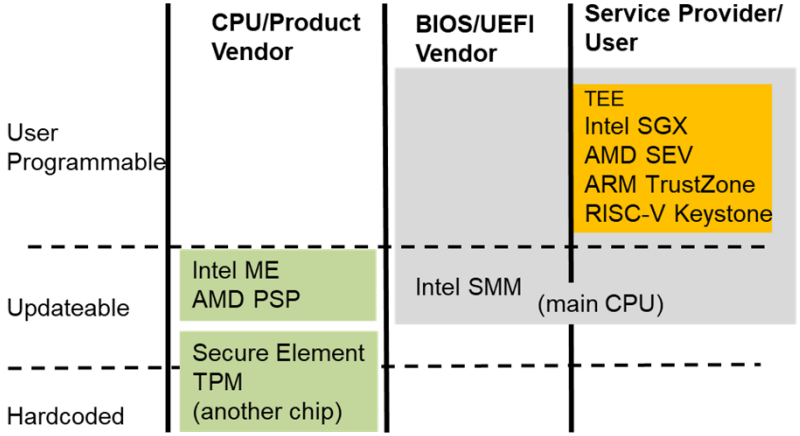
- IoTデバイスにおけるTEE(Trusted Execution Environment)の実装,システム制御情報学会, 出版予定 (無償公開予定)
- RISC-VにおけるTEE (Trusted Execution Environment)とCC (Confidential Computing) 、RISC-V Day Tokyo 2024 Winter 2024/1/1614:15-14:35
  - https://riscv.or.jp/risc-v-day-tokyo-2024-winter/

目次

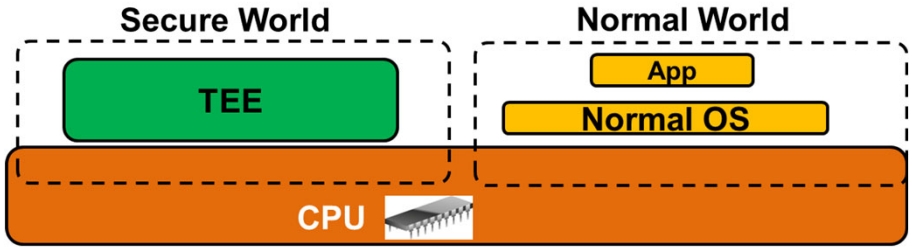
- TEEとは
- RISC-V PMP (Physical Memory Protection)
- RISC-V TEE
  - Keystone (PMPベース)
  - MultiZone (PMPベース)
  - AP-TEE (VMベース)
- 関係組織、規格、学会
  - GlobalPlatfrom, CCC, Arm PSA, IETF, etc
  - HOST, HASP, SysTex, etc

TEEとは（1/2）

- ハードウェアが提供する隔離実行環境HIEE(Hardware-assisted Isolated Execution Environments)の一つ
  - HIEEにはBIOSが使うSMMや別チップのIntel ME, TPMがある
  - TEEは第三者がプログラミング可能であることを特徴とする



- TEEはCPUの状態を二つに分ける
  - ノーマルワールド (i.e., REE: Rich Execution Environment)
    - ◆通常のOS(Linux, Windows)が実行される
  - セキュアワールド(i.e., TEE: Trusted Execution Environment)
    - ◆OSやハイパーバイザーなどの脆弱性とは無縁の環境
    - ◆クリティカルな処理を行う

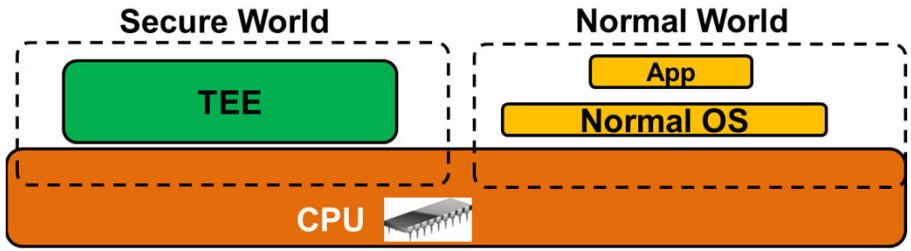


この図はあくまでTEEの一例

TEEとは（2/2）

■ 特徴：
- （極端に言えば）一時的に隔離実行されるのみ
- 長期的な鍵保存は別の手段が必要
  - ◆Root of Trustには安全に鍵・証明書を保存する耐タンパハードウェアが必要
  - ◆これを信頼の基点に外部からの健全性の検証（Remote Attestation）が行われる

■ 利用できるCPU
- ARM TrustZone （スマホ）
- Intel SGX (PC,サーバ), Intel TDX(サーバ)
- AMD SEV (サーバ)
- RISC-V は多くの実装あり



この図はあくまでTEEの一例
（Arm TrustZoneが一番近い）

■ その他の実装
- GPU (Nvidia H100)
- AWS Nitroはハイパーバイザー＋セキュアハード(Nitro Card, Nitro Security Chip)

TEEの応用

- 機密情報処理
  - 鍵管理
    - ◆AndroidのKeyMaster
  - DRM処理
    - ◆スマホのWidevine(Google)
    - ◆WindowsのUltra HD Blu-rayビューア
  - 個人情報管理
    - ◆指紋認証処理
    - ◆FIDO認証
    - ◆暗号資産ハードウェアウォレット
- コード・データの隠蔽
  - 機械学習の重み付けデータ
  - プライバシー保護
  - 遺伝子解析

スマホでTEEを普及させた
キラーアプリ

キラーアプリになれなかった

キラーアプリ候補？

- メモリ消費が少ない
- スマートフォン
- Arm TrustZone向き

- メモリ消費が大きい
- サーバ・クラウド
- Intel SGX、AMD SEV 向き
- **Confidential Computing**の
  ターゲットはこちら。

- RISC-V?

サーバでのキラーアプリ候補？

TEE CPU比較

	ARM TrustZone	Intel SGX (Coreアーキ中心)	AMD SEV	RISC-V Keystone
特徴	1つの隔離実行環境を起動時に作成。 隔離実行環境でのみ使えるデバイスが設定可能。	プロセス内のライブラリを隔離実行する。動的に作成。。 多くの機能をマイクロコードで実装。	仮想化をTEEに拡張。各VMが1つのTEEとして扱える。	複数の隔離実行環境を動的に作成。 隔離実行環境でのみ使えるデバイスを設定可能な仕様あり。未実装。
TEEの数	1つだがTEE内OSが複数プロセスを管理。	制限なしだがメモリ量からの制約あり。	第一世代EPYCで15 第二世代EPYCで509	14
メモリサイズ・割り当て、暗号、完全性	数メガ程度を起動時に確保。暗号・完全性は無し。	起動時に128-256MB確保。 暗号、完全性あり。 Xeon Scalableでは最大1TBで暗号のみ	サイズの制限なし。暗号化はある。	サイズの制限なし。Linuxから切り出して動的に割り当て。暗号・完全性は無し。
TEEのみデバイス	○ 可能	基本的に不可能だが拡張の研究はある(Graviton[OSDI 18]など)。	基本的に不可能	○ 拡張仕様あり(IOPMP)。
Root of Trust	× 基本的になし。携帯はSecure Elementの利用例あり	CPU固有のもの。Intel ME (CSME)	CPU固有のもの。Platform Security Processor(PSP)	オプションで拡張。
Remote Attestation	基本的にない。	Intelが提供したもの(EPID)などが使える。隔離実行のみも多い。	あり。	テスト版。信頼の起点がハードウェアではない。
特権レベル	すべての特権 (TEE内OS実装可能)	ユーザ(ring 3)のみ (TEE内OSの実装不可)	すべての特権 (TEE内OS実装可能)	すべての特権 (TEE内OS実装可能)
VMからの利用	試験的に対応。KVM(TZVisor), Xen	Xen,KVMのVMおよびDockerコンテナから利用可。VMwareは不可だった	TEE自体がVM	仮想化自体が試験中。

TEE CPU比較

	ARM TrustZone	Intel SGX (Coreアーキ中心)	AMD SEV	RISC-V Keystone
特徴	1つの隔離実行環境を起動時に作成。 隔離実行環境でのみ使えるデバイスが設定可能。	プロセス内のライブラリを隔離実行する。動的に作成。。 多くの機能をマイクロコードで実装。	仮想化をTEEに拡張。各VMが1つのTEEとして扱える。	複数の隔離実行環境を動的に作成。 隔離実行環境でのみ使えるデバイスを設定可能な仕様あり。未実装。
TEEの数	1つだがTEE内OSが複数プロセスを管理。	制限なしだがメモリ量からの制約あり。	第一世代EPYCで15 第二世代EPYCで509	14（PMPレジスタに依存。最上位と最下位は予約済み）
メモリサイズ・割り当て、暗号、完全性	数メガ程度を起動時に確保。暗号・完全性は無し。	起動時に128-256MB確保。 暗号、完全性あり。 Xeon Scalableでは最大1TBで暗号のみ	サイズの制限なし。暗号化はある。	サイズの制限なし。Linuxから切り出して動的に割り当て。暗号・完全性は無し。
TEEのみデバイス	○ 可能	基本的に不可能だが拡張の研究はある(Graviton[OSDI 18]など)。	基本的に不可能	○ 拡張仕様あり(IOPMP)。
Root of Trust	× 基本的になし。携帯はSecure Elementの利用例あり	CPU固有のもの。Intel ME (CSME)	CPU固有のもの。Platform Security Processor(PSP)	オプションで拡張。
Remote Attestation	基本的にない。	Intelが提供したもの(EPID)などが使える。隔離実行のみも多い。	あり。	テスト版。信頼の起点がハードウェアではない。
特権レベル	すべての特権 (TEE内OS実装可能)	ユーザ(ring 3)のみ (TEE内OSの実装不可)	すべての特権 (TEE内OS実装可能)	すべての特権 (TEE内OS実装可能)
VMからの利用	試験的に対応。KVM(TZVisor), Xen	Xen,KVMのVMおよびDockerコンテナから利用可。VMwareは不可だった	TEE自体がVM	仮想化自体が試験中。

TEE比較

- Towards A Secure Joint Cloud With Confidential Computing, 2022 IEEE International Conference on Joint Cloud Computing (JCC), 上海交通大学

TABLE I
COMPARISON OF EXISTING CONFIDENTIAL COMPUTING SOLUTIONS

	SGXv1	Scalable SGXv2	SEV-SNP	TDX	TrustZone	Realm	Nitro	Penglai	Keystone	H100
Architecture	x86-64	x86-64	x86-64	x86-64	Arm	Arm	x86-64	RISC-V	RISC-V	GPU
Abstraction	enclave	enclave	VM	VM	PM	VM	VM	enclave	PM	vGPU
Instances	unlimited	unlimited	509	unlimited	1	unlimited	unlimited	unlimited	16	7
Encryption	●	●	●	●	○	●	○	●	○	●
Integrity	●	◐	◐	◐	○	◐	○	●	○	●
Freshness	●	○	○	○	○	○	○	●	○	○
Attestation	●	●	●	●	○	●	●	◐	◐	●

* PM stands for the physical machine abstraction. Integrity means this CC can resist both hardware and software tampering; ◐ for integrity means this CC can detect software tampering. H100 has full integrity against hardware attacks because it uses on-chip High Bandwidth Memory (HBM). AMD EPYC (Rome) processors currently support 509 keys for SEV VMs. Nitro uses TPM for remote attestation. Penglai and Keystone currently only support local attestation, but can also achieve remote attestation using TPM or other methods alike.

RISC-Vとは

- RISC-V International が管理するOpen ISA(Instruction Set Architecture)
  - 仕様自体がフリーなため、多くの実装あり (Chisel, Verilog, SystemVerilog, VHDL)

Academia
- ◆ETH: PULP(Parallel Ultra Low Power)(Swiss)
- ◆MIT: Sanctum, MI-6,Carbon Nano-Tube RISC-V
- ◆IIT-Madras: SHAKTI (India)
- ◆U-Tokyo: RSD (32-bit Out-of-Order, superscalar) (Japan)
- ◆UC Berkeley/SiFive: Rocket(In order)/Boom(Out of Order)

発祥元。リファレンスとして多く使われる

Industry
- ◆Esperanto: ET-Maxion, ET-Minion
- ◆**Western Digital**: SweRV (Controller of SSD&HDD)

自社製品で活用

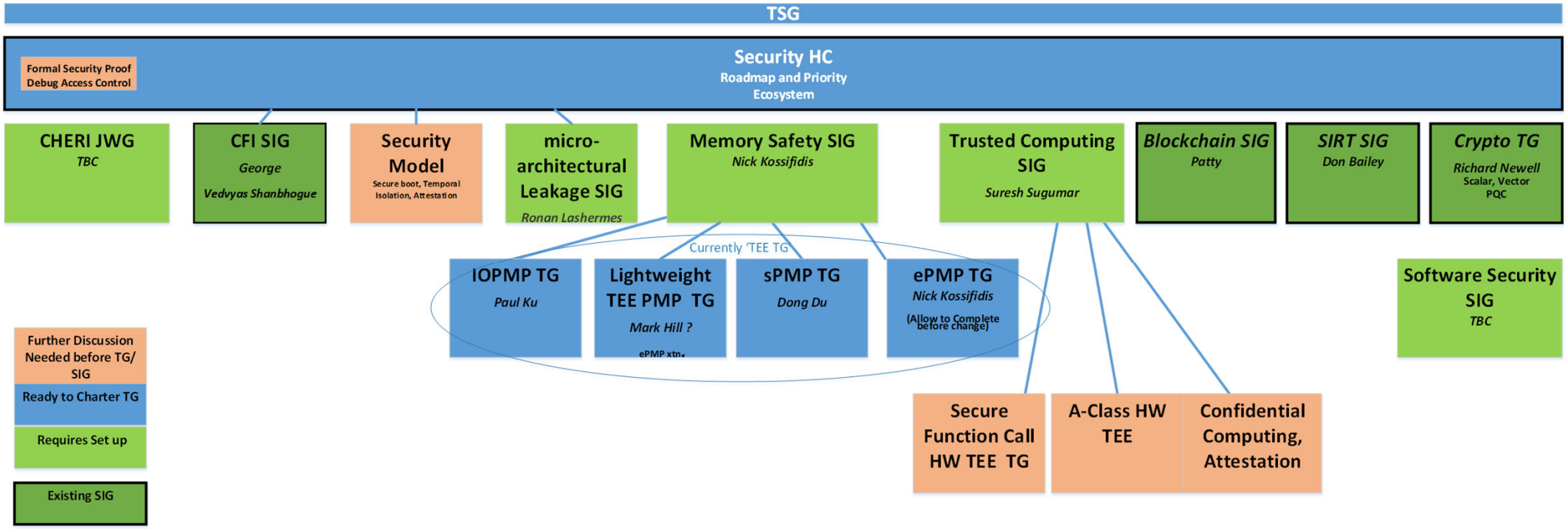
- ◆**NVIDIA**: NVRISCV
- ◆Andes: AndesCore (Taiwan)
- ◆Alibaba(Pingtouge):XuanTie 910 (2.5GHz 16 Core) (China)
- ◆SyntaCore: SCR Family (Russia)
- ◆CloudBare: BM, BR, BI Series (Russia)

幾つかはOpen Source

RISC-V Securityのスコープ

■ Security HCより

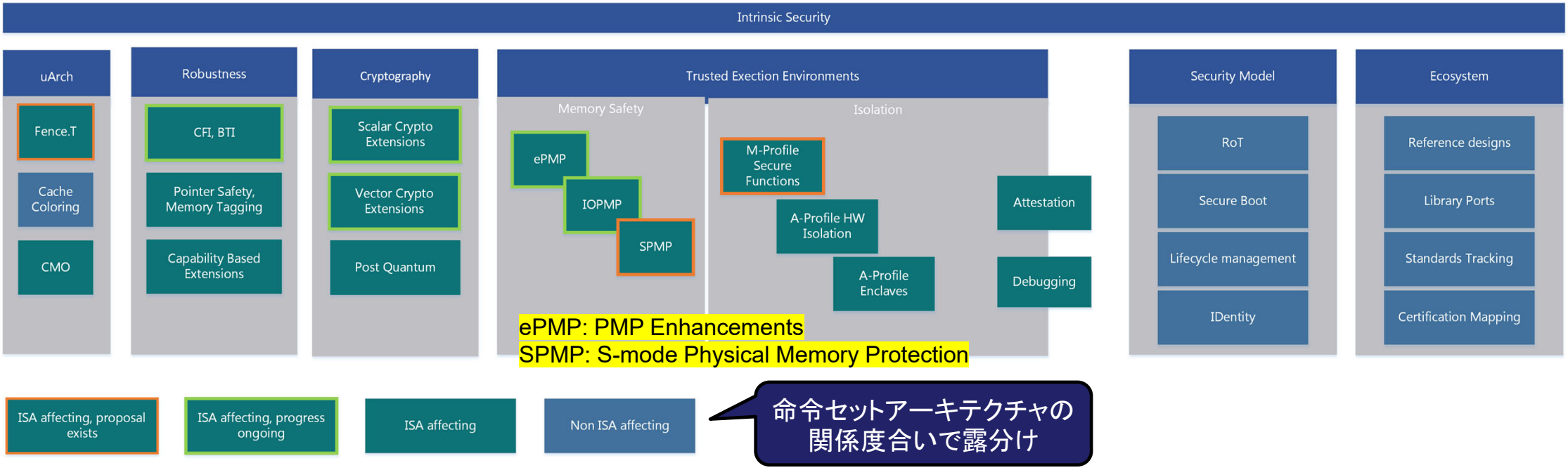
- https://github.com/riscv-admin/security/blob/main/topics/RiscV%20security%20direction%20Nov%202021.pptx



RISC-V Securityのスコープ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Security HCより
  - https://github.com/riscv-admin/security/blob/main/topics/RiscV%20security%20direction%20Nov%202021.pptx
  - RISC-V Summit2021のArchitecture Design for Security: Do's and Don'ts が詳しい。
    - https://www.youtube.com/watch?v=sQyrxvswY38&ab_channel=RISC-VInternational



RISC-V TEE

■ RISC-VでのTEE 実装

Academia
- Sanctum [MIT,USENIX Sec'16]
- TIMBER-V [グラーツ工科大学, NDSS'19]
- MI6 [MIT,MICRO'19]
- **Keystone** [UC Berkeley, EuroSys'20]　システム制御情報学会誌で解説　23/09
- HECTOR-V [グラーツ工科大学, arXiv'21]
- uTango [arXiv'21, ミーニョ大学]
- Cure [ダルムシュタット工科大学,USENIX Sec'21]
- CHERI-TrEE [ケンブリッジ大学, IEEE S&P'23]
- HPMP (Hybrid Physical Memory Protection) [上海交通大学, MICRO'23]

Industry
- **MultiZone** [HexFive]　システム制御情報学会誌で解説予定
- SiFive Shield / World Guard [SiFive]
- **AP-TEE**（Application Processor –TEE) [RISC-V International TEE WG]　システム制御情報学会誌23/09
- CoVE (Confidential Virtual Machine for RISC-V) [Rivos Inc., arXiv'23]

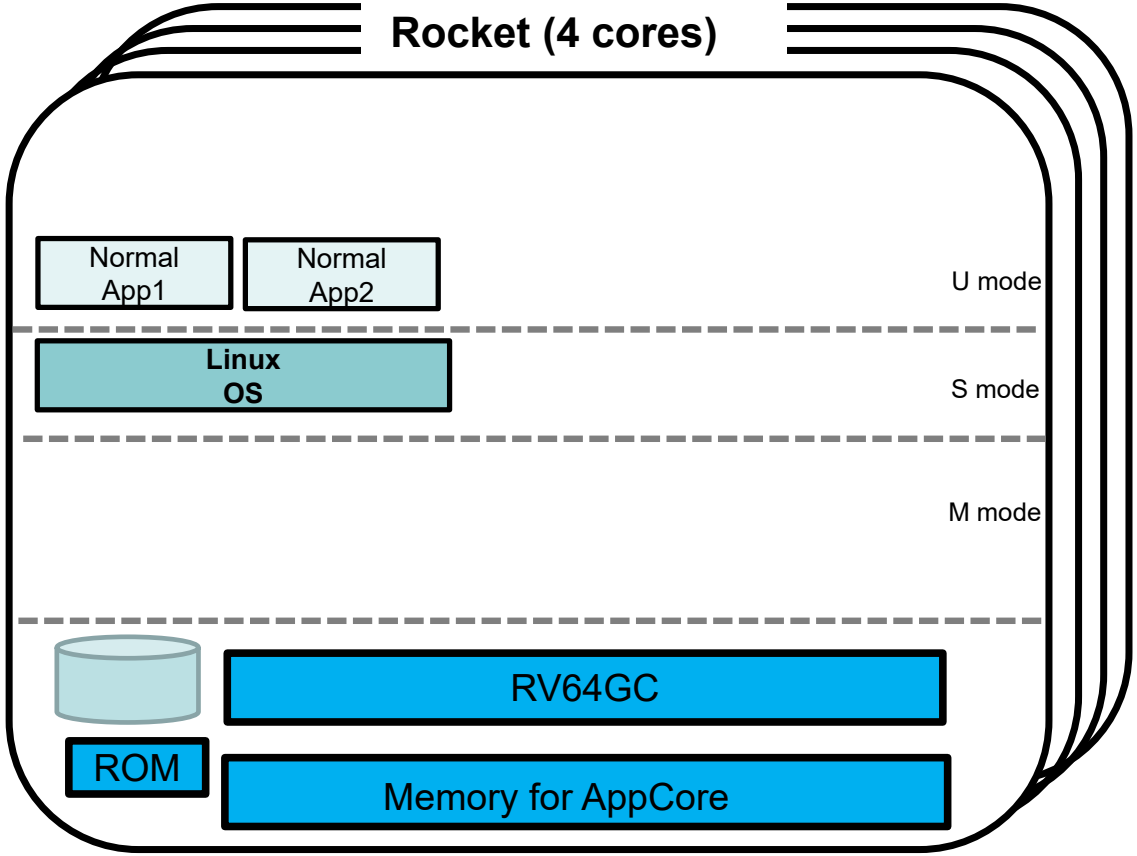
多くはハードウェアの拡張を伴う。KeystoneとMultiZoneはRISC-Vが標準仕様にあるPMP (Physical Memory Protection)を使い、ハードウェア拡張なし。

RISC-V TEE "Keystone"

- UC Berkeleyで開発しているTEE
  - RISC-Vの開発メンバーが率いている (Krste Asanović先生）
  - RISC-Vの特権命令仕様書で定義のある　PMP(Physical Memory Protection)を活用
  - CCC: Confidential Computing Consortiumでも注目されている

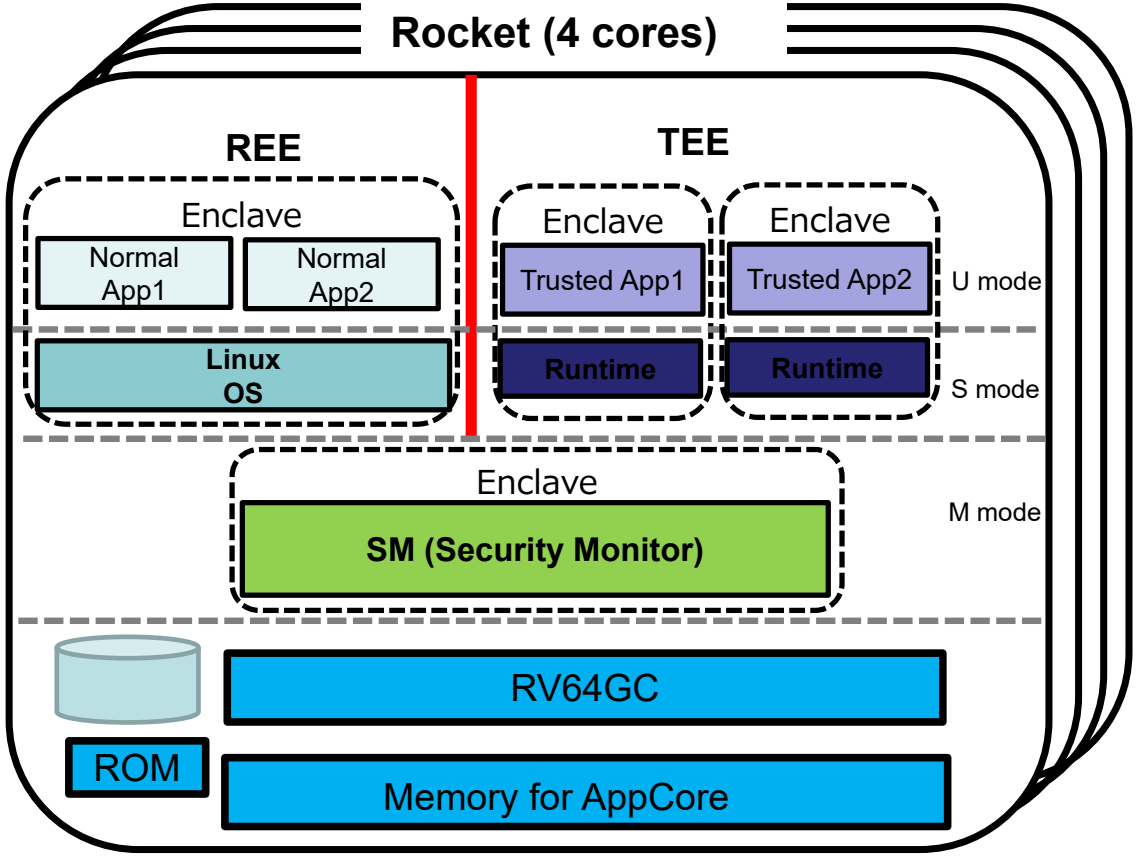
CONFIDENTIAL COMPUTING CONSORTIUM

通常のRISC-V



- Rocket コアでLinuxの実行を想定
  - 正確には割り込みがM modeに落ちるので対処が必要だが省略。

通常のRISC-VでのKeystone



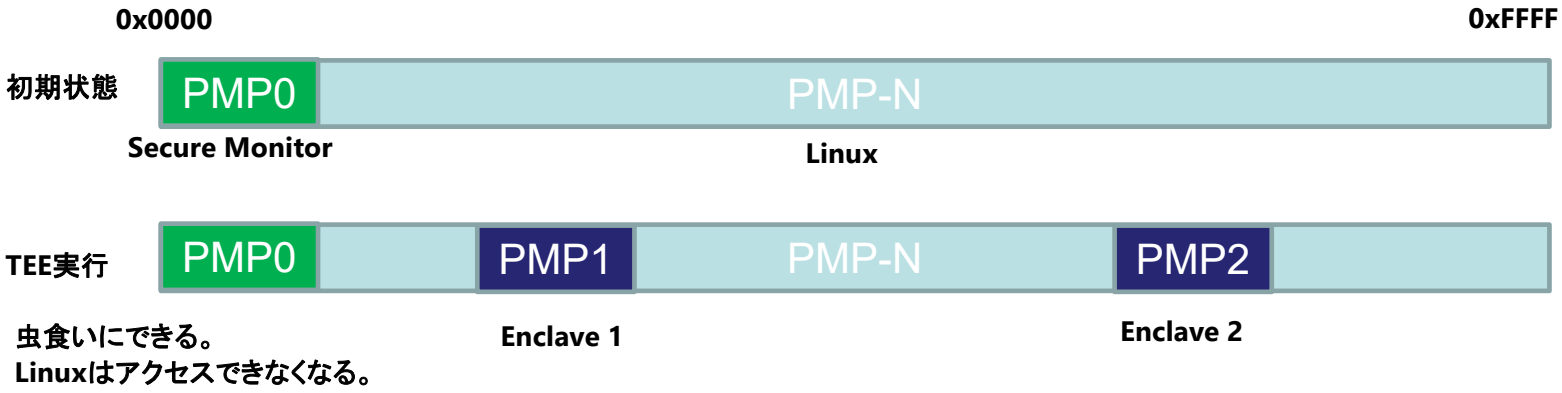
- ハードウェアの変更はない
- PMPによるメモリ保護
  - 1つ(最高特権)はSecure MonitorがM modeで利用。
  - 1つ(最下位特権)はREEが使い、Linuxが起動
  - 図中では2つのTEE (Enclave)が実行

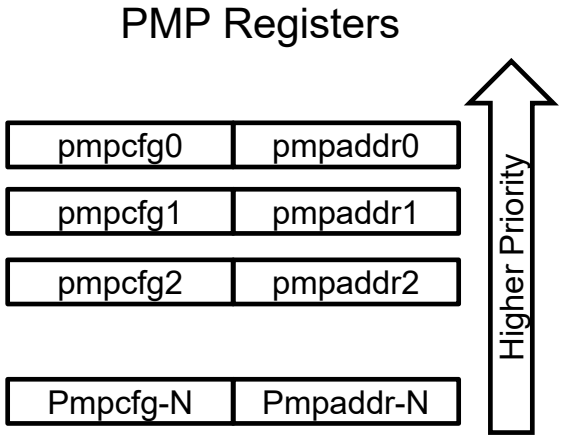
RISC-VのPMP (Physical Memory Protection)

■ 物理メモリにアクセス制限を掛ける仕組み

- 領域を区切って権限があるもののみアクセスできる。動的に指定できる。
- U mode, S modeなどの権限に直行した制御。PMPの領域に対して各modeのソフトが作られる。

- RISC-V CPU 内に制御レジスタが最大N＝16(最新のPriv1.12仕様では64) 本あり、メモリの範囲とそれに対するアクセス制限を定義する
  - 番号で優先度がある。0:highest 、N:lowest
  - 0 (highest) はSecure Monitor、N (lowest) は Linux、残りがTEE(Enclave)に使われる。





pmpcfgレジスタとpmpaddrレジスタ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- pmpcfgレジスタ
  - コンフィグ指定
- pmpaddrレジス
  - レンジ指定

Mode
Lock, Unlock
pmpaddlのコンフィグ(4byte単位、他)

Permission
eXecute, Write, Read
(1:Allow, 2: Deny)

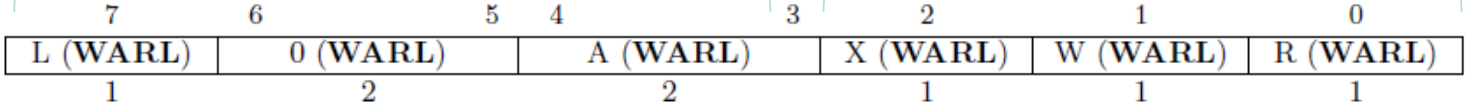


Figure 3.35: PMP configuration register format.

領域　　先頭アドレス

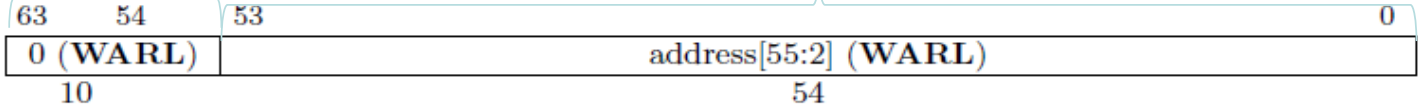


Figure 3.34: PMP address register format, RV64.

The RISC-V Instruction Set Manual
Volume II: Privileged Architecture
Document Version 20211203 より

RISC-V PMPと類似技術

■ Arm MPU: Memory Protection Unit

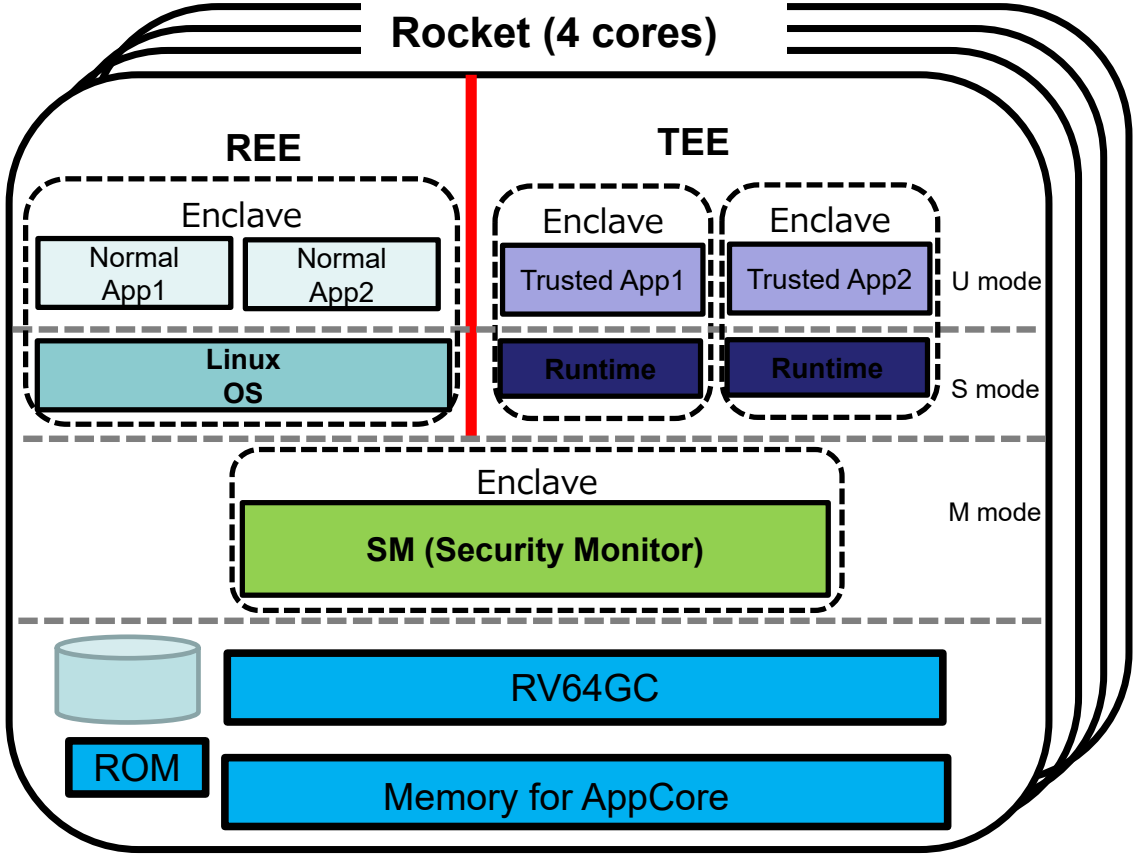
- A Survey on RISC-V Security: Hardware and Architecture [arXiv21] https://arxiv.org/abs/2107.04175 より

Table 2. Comparison of RISC-V PMP and ARM MPU Main Features.

	RISC-V PMP	ARM MPU
The smallest region size	4 Bytes	32 Bytes
The maximum size of a region	32 GB (if XLEN = 32)	4 GB
Region granularity	Configurable (2^{G+2} Bytes, $G \geq 0$)	32 Bytes
Privileged and unprivileged settings	Hybrid (If PMP configuration register L bit is set, the setting also applies to M-mode)	Independent (Explicitly indicated by the MPU_RBAR AP field)
Supported memory attributes	R/W/X	R/W/X
Maximum number of supported memory regions	16 (All for unprivileged, some also applies to privileged if L bit is set)	16 (8 for privileged, 8 for unprivileged)

- RISC-Vでは32/64でPMPががあるが、ArmはCortex-Mのみ？

通常のRISC-VでのKeystone

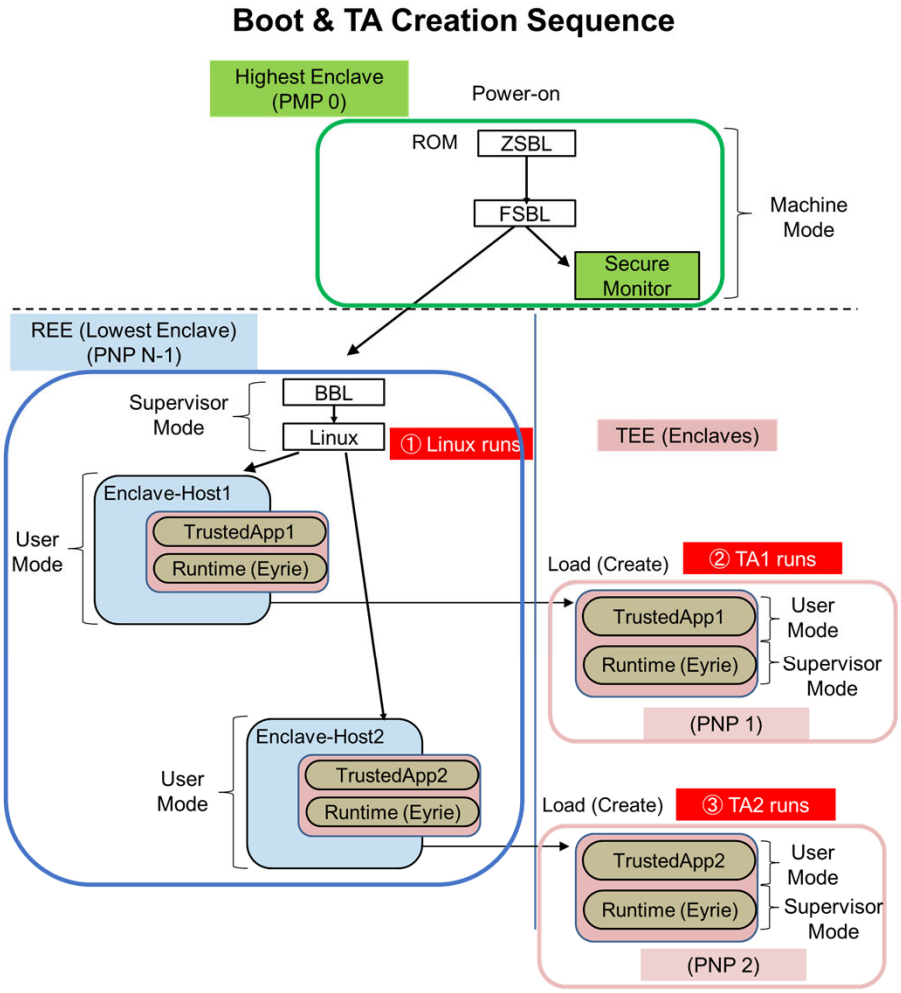


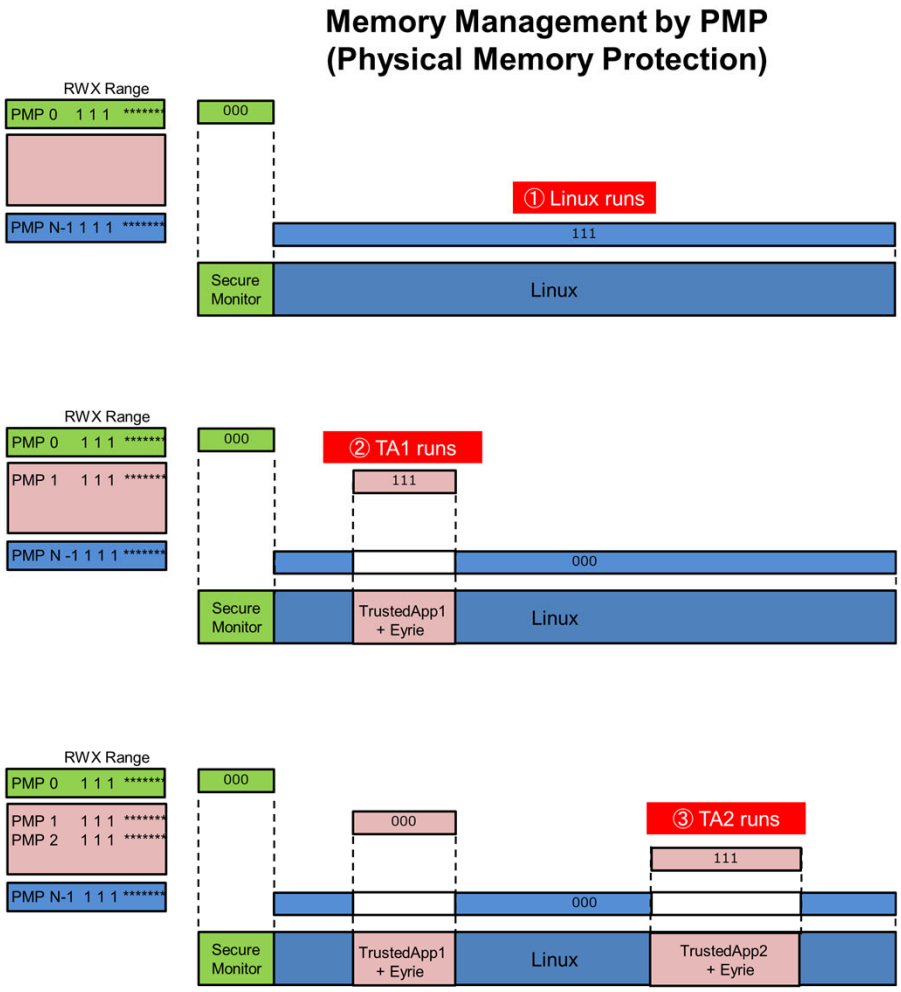
- ハードウェアの変更はない
- PMPによるメモリ保護
  - 1つ(最高特権)はSecure MonitorがM modeで利用。
  - 1つ(最下位特権)はREEが使い、Linuxが起動
  - 図中では2つのTEE (Enclave)が実行

RISC-V Keystone

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

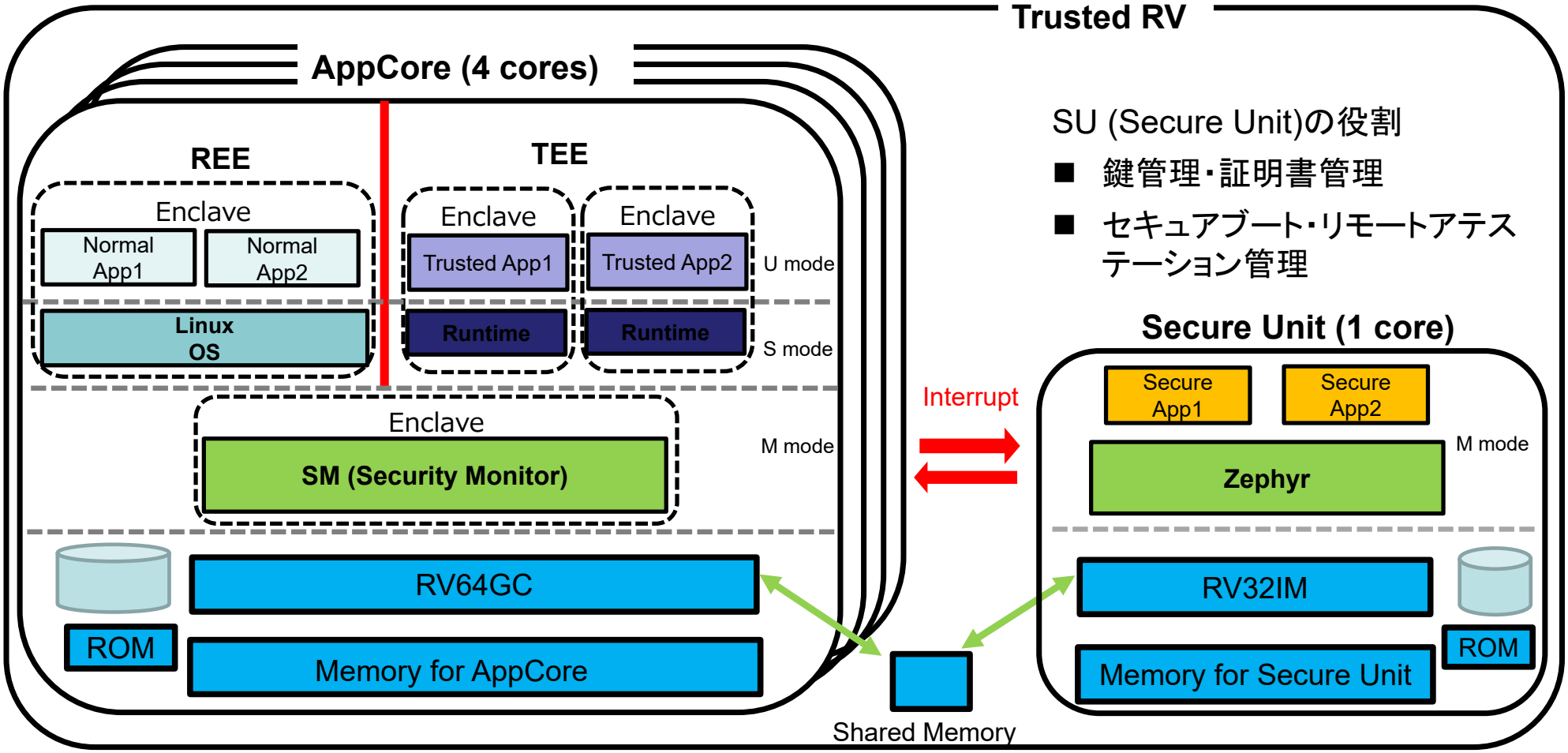
■ Keystoneを有効にした場合の起動とPMPの動作



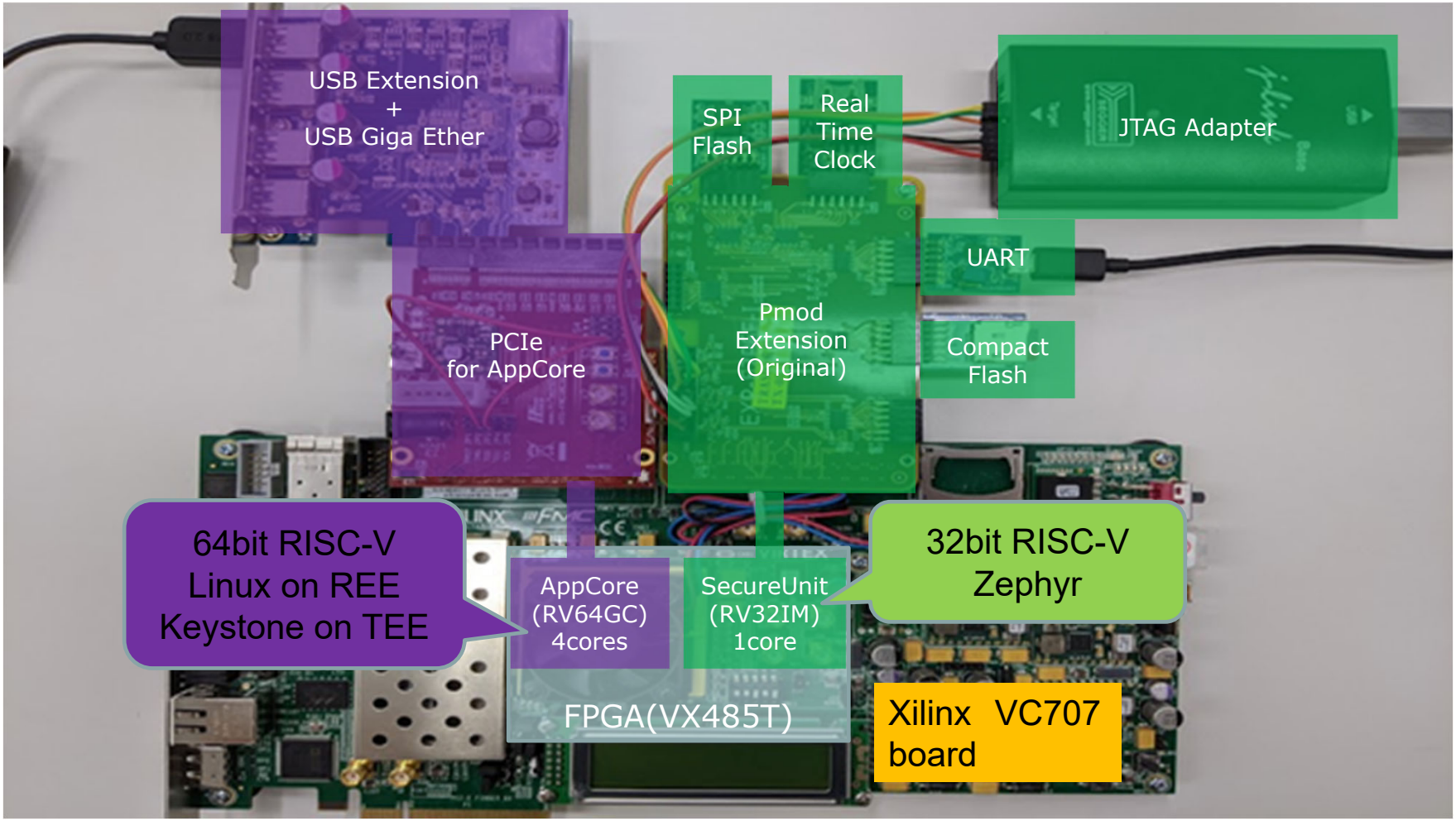


TRV（Trusted RISC-V）でのKeystone

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

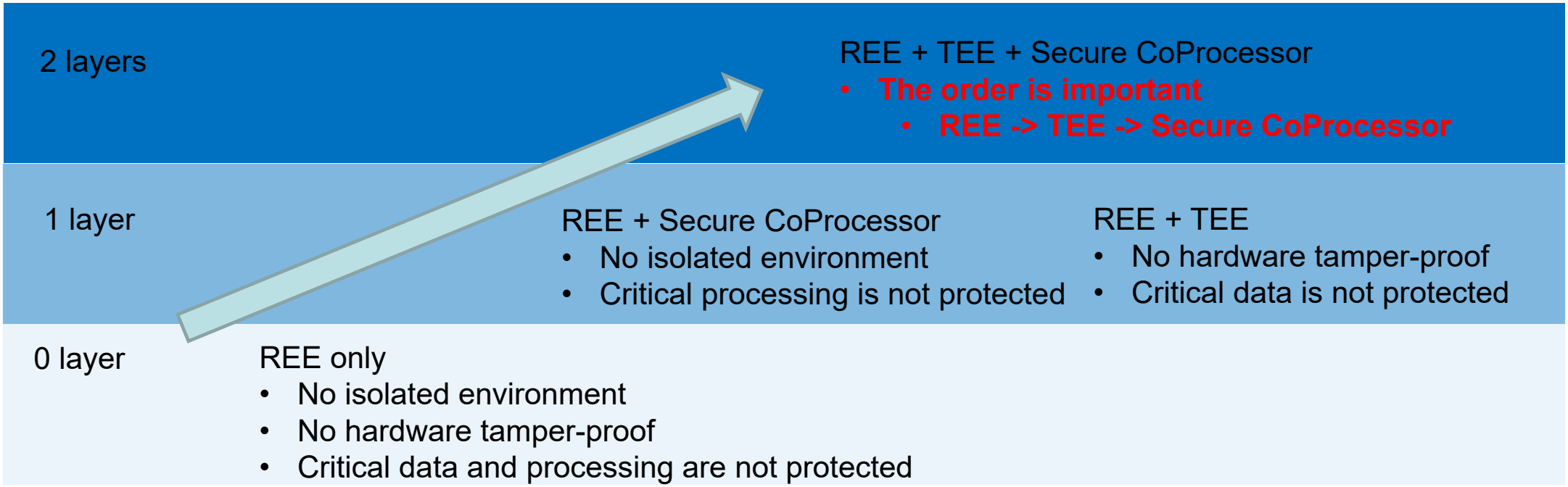


TRASIOのTRV実装



TEEとSecure CoProcessorのレイヤー構成（セキュリティレベル）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



- 同様のレイヤー構成がArm TrustZoneでも提案されている。
- Intel SGXではこの構成が取れない。(Ring3のみで直接デバイスにアクセスできないため)

TEEとRoot of Trustの構成例 (FIDO Authenticator)

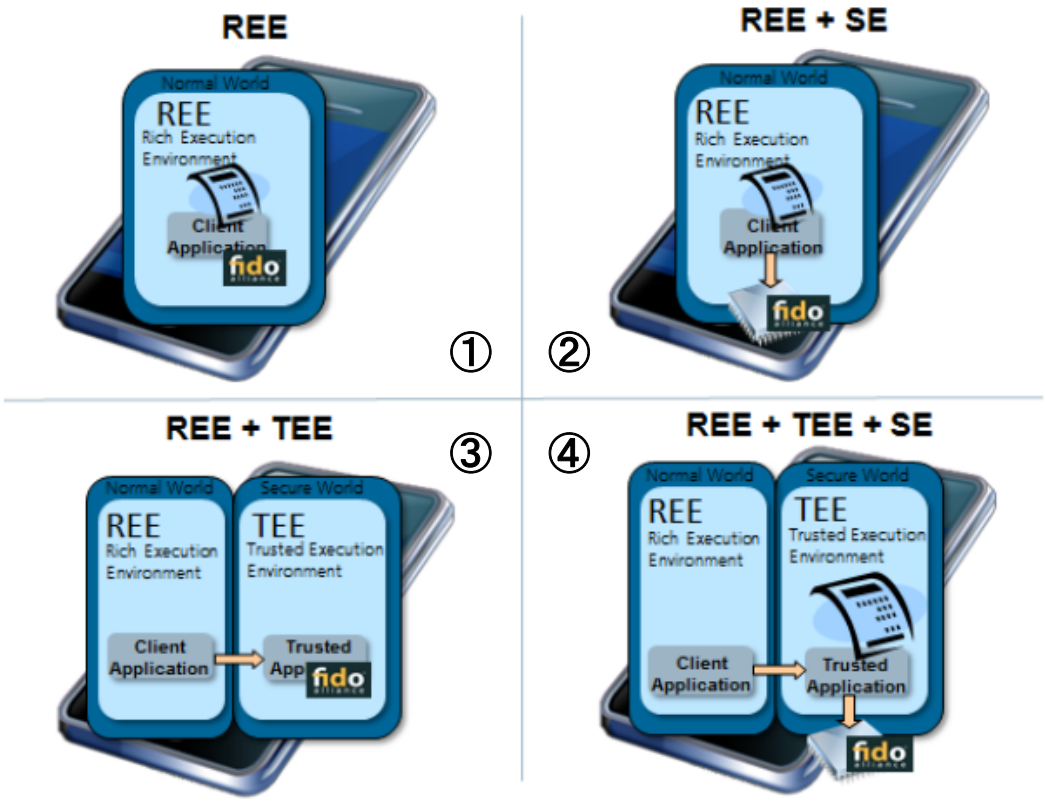
- Realizing FIDO Authentication Solutions with GlobalPlatform Technologies, 2018
  - https://globalplatform.org/wp-content/uploads/2018/04/White-Paper-Technical-FIDO-Auth-using-GlobalPlatform-Jan2018.pdf
  - FIDO Authenticatorの実装パターン
    - ① REE直接
    - ② REE+SE(RoT)
    - ③ REE+TEE
    - ④ REE+TEE+SE

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Practical Considerations: Technical Overview

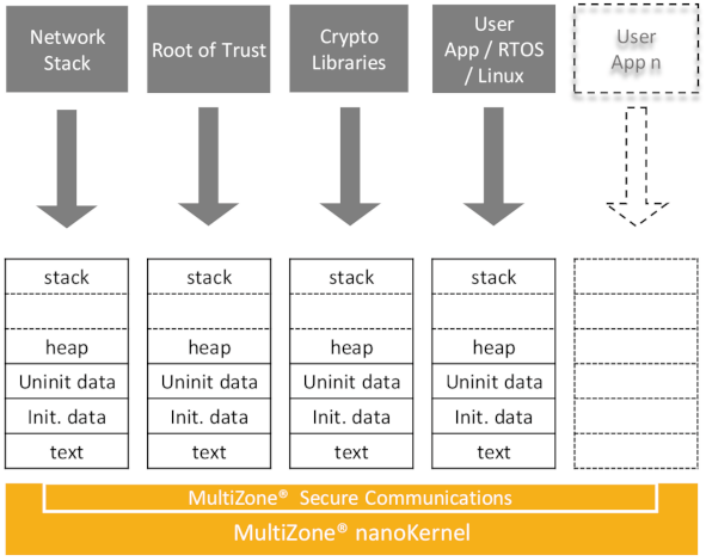
Realizing FIDO Authentication Solutions with GlobalPlatform Technologies

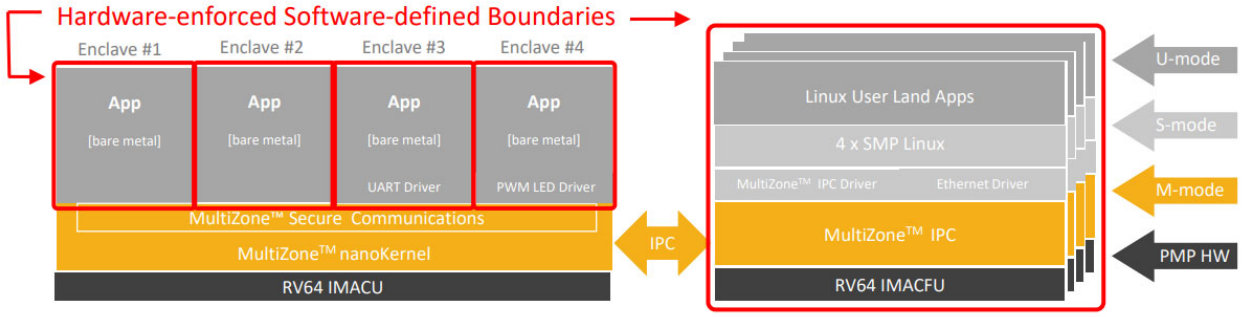
White Paper Companion
High Level Technical Guide
January 2018



MultiZone https://hex-five.com/multizone-security-tee-riscv/

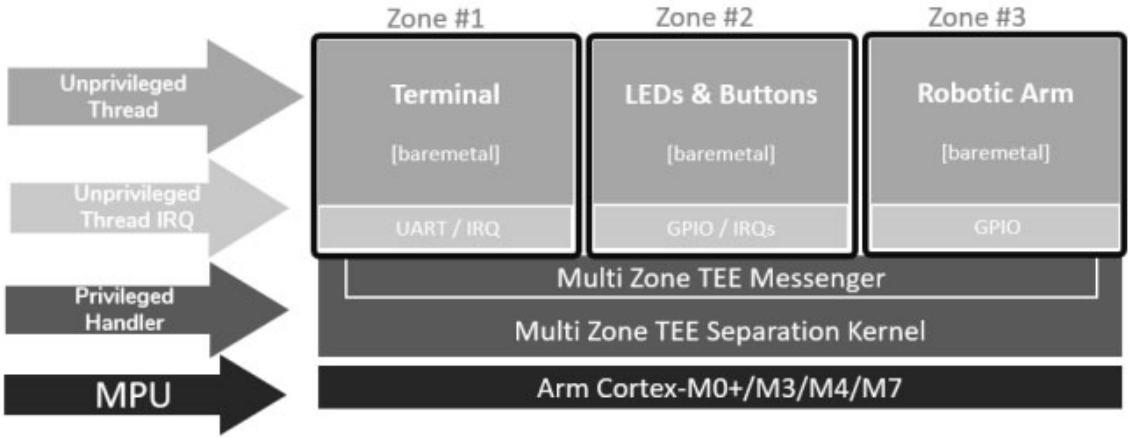
- 個々のEnclave（PMP)で信頼できるOSやTAを動かすのではなく、単純にアプリを動かし、そのアプリが他に影響を与えないようにする(Hardware enforced Software defined Boundaries)
  - Arm　Cortex-MのMPUを使った実装もあり。次スライド
- 構成
  - MultiZone NanoKernel　隔離設定
  - MultiZone Secure Communications　アプリ間の通信





MutiZone on Arm Cortex-M

- Multi Zone Security for Arm Cortex-M Devices [Embedded World 2022] より
  - Arm MPU (Memory Protection Unit)を使って隔離
  - Cortex-MのTrustZoneは使っていない!



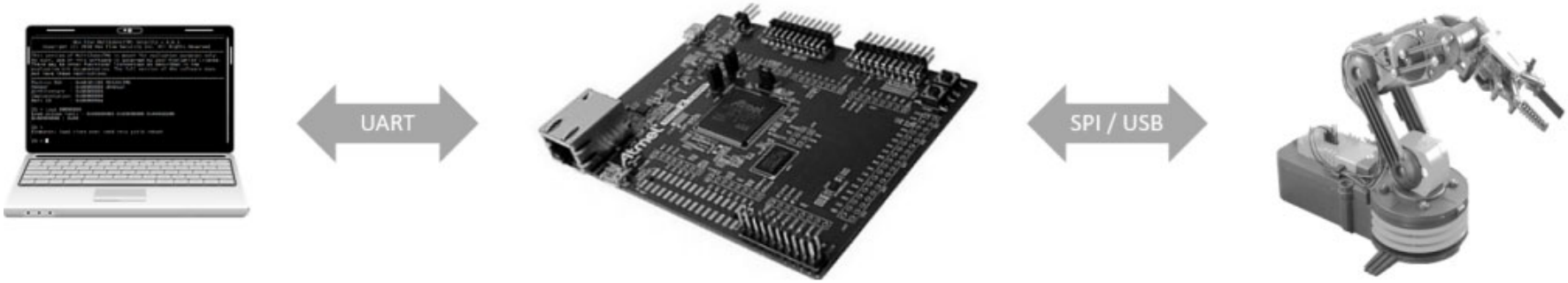
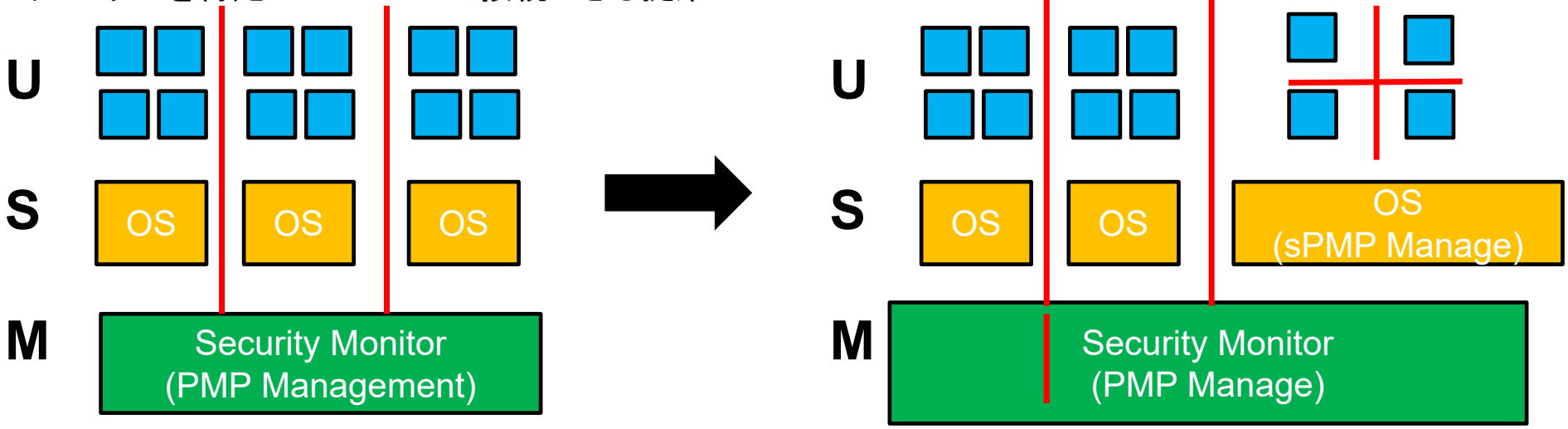


Fig. 3 - Multi Zone Trusted Execution Environment - Reference Implementation Architecture.

PMPの開発方向

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- PMP (Physical Memory Protection)の拡張　(済み)
  - PMPレジスタとセキュリティ設定機能を拡張する。(Priv仕様1.12でレジスタが16から64に拡張)
  - RISC-Vの特権命令仕様にもかかわるのでその提案。
- sPMP（S Mode PMP)の提案
  - 既存のPMPはマシンモードでS+U modeを分割したが、S modeのOSがプロセス単位のTEEができるようになる拡張
- ePMP (PMP Enhancements)の提案
  - 既存のPMPはマシンモード(M Mode)を分割できないが、M Modeも分割できる提案
- IOPMP
  - ペリフェラルを特定のPMPにのみ接続できる提案



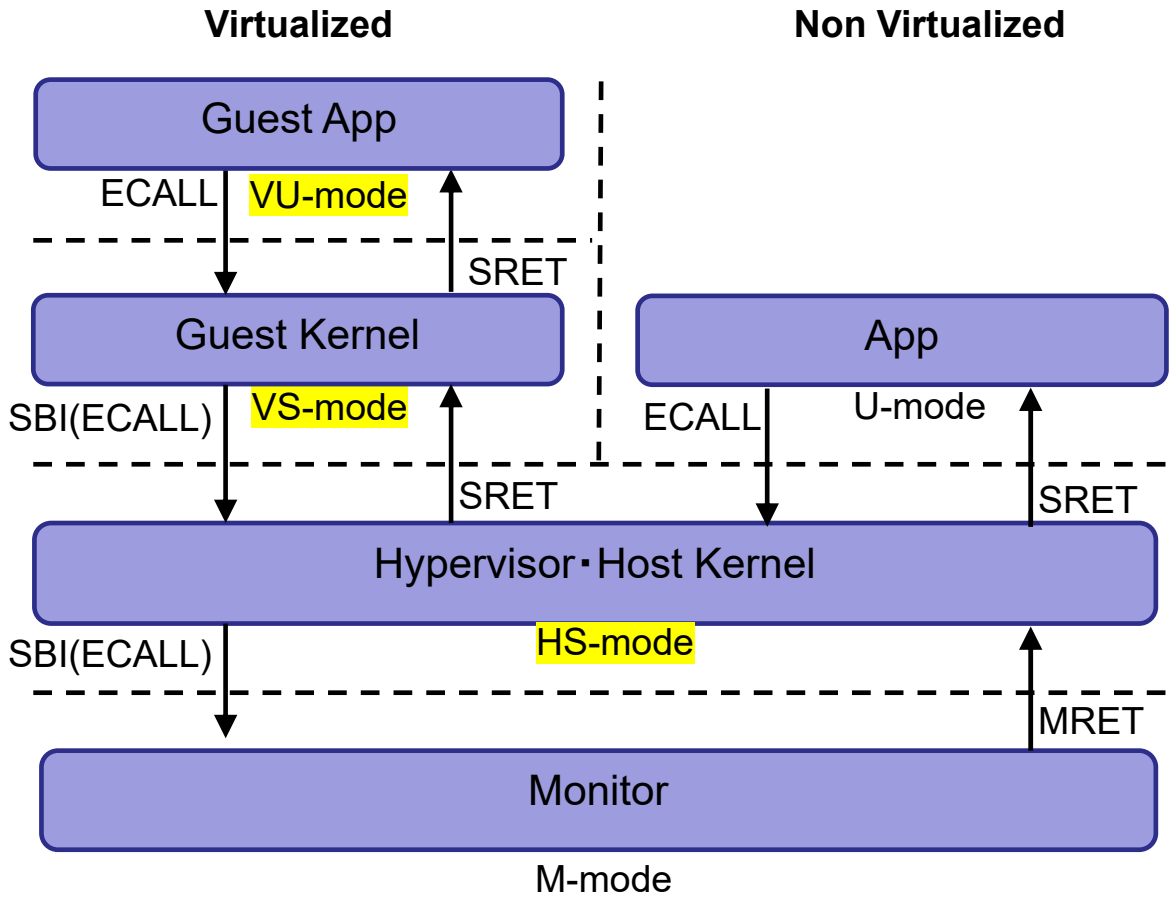
AP-TEE

- Application Platform-Trusted Execution Environment

- RivosでCoVE: Confidential VM Environment と同じ

仮想マシンのTEE化　RISC-V AP-TEE

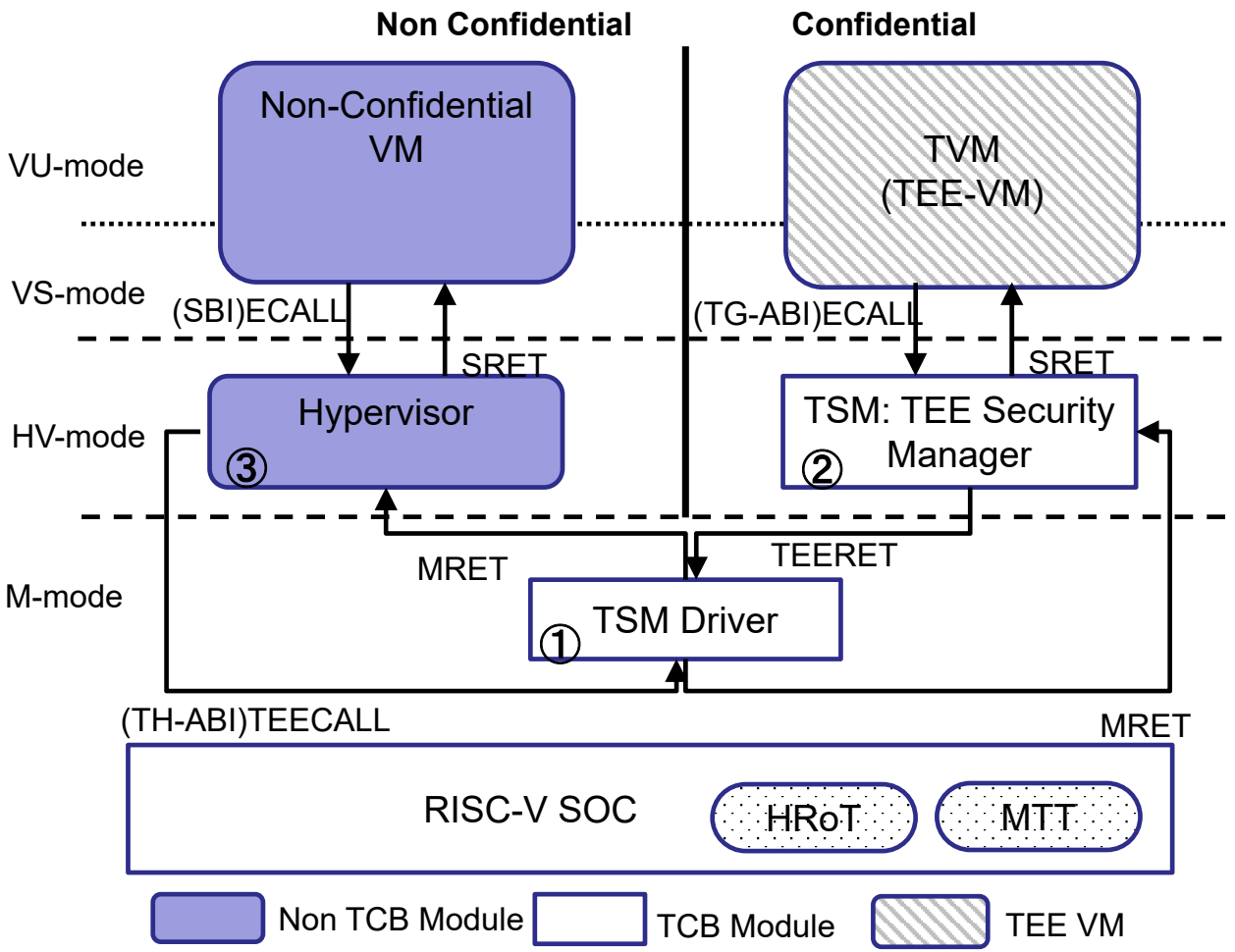
- RISC-V InternationalのWGで仕様策定が進んでいるAP-TEE(Application Platform-Trusted Execution Environment)
- RISC-Vの仮想化を拡張
  - 右図は仮想化の仕組み
    - ◆仮想化拡張によりVU (Virtualized User), VS (Virtualized Supervisor), HS (Hypervisor-extended Supervisor) のModeが導入された



仮想マシンのTEE化　RISC-V AP-TEE

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Confidentialな空間でTSMが軽量Hypervisorとして動く。
  - TEE-VMとHypervisorからの要求に応えるPassiveなコンポーネント
    - ◆TG(Trusted Guest)-ABI
    - ◆TH(TEE-Host)-ABI
- Hypervisorがスケジューリングやメモリ提供を行う。
- メモリはMTT(Memory Tracking Table)がページを識別して暗号化
- ①、②、③はブート順
  - HRoT(Hardware Root of Trust)がRemote Attestationのためのログを取る



TEE CPU比較　全ての要件を満たすものはない

	ARM TrustZone	Intel SGX（Coreアーキ中心）	AMD SEV	RISC-V Keystone
特徴	1つの隔離実行環境を起動時に作成。 隔離実行環境でのみ使えるデバイスが設定可能。	プロセス内のライブラリを隔離実行する。動的に作成。。 多くの機能をマイクロコードで実装。	仮想化をTEEに拡張。各VMが1つのTEEとして扱える。	複数の隔離実行環境を動的に作成。 隔離実行環境でのみ使えるデバイスを設定可能な仕様あり。未実装。
TEEの数	1つだがTEE内OSが複数プロセスを管理。	制限なしだがメモリ量からの制約あり。	第一世代EPYCで15 第二世代EPYCで509	14
メモリサイズ・割り当て、暗号、完全性	数メガ程度を起動時に確保。暗号・完全性は無し。	起動時に128-256MB確保。 暗号、完全性あり。 Xeon Scalableでは最大1TBで暗号のみ	サイズの制限なし。暗号化はある。	サイズの制限なし。Linuxから切り出して動的に割り当て。暗号・完全性は無し。
TEEのみデバイス	○ 可能	基本的に不可能だが拡張の研究はある(Graviton[OSDI 18]など)。	基本的に不可能	○ 拡張仕様あり(IOPMP)。
Root of Trust	× 基本的になし。携帯はSecure Elementの利用例あり	CPU固有のもの。Intel ME（CSME）	CPU固有のもの。Platform Security Processor（PSP）	オプションで拡張。
Remote Attestation	基本的にない。	Intelが提供したもの(EPID)などが使える。隔離実行のみも多い。	あり。	テスト版。信頼の起点がハードウェアではない。
特権レベル	すべての特権 (TEE内OS実装可能)	ユーザ(ring 3)のみ (TEE内OSの実装不可)	すべての特権 (TEE内OS実装可能)	すべての特権 (TEE内OS実装可能)
VMからの利用	試験的に対応。KVM(TZVisor), Xen	Xen,KVMのVMおよびDockerコンテナから利用可。VMwareは不可だった。	TEE自体がVM	仮想化自体が試験中。

Confidential Computing on Cloud

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

	Service Name	TEE implement ation	CPU	Root of Trust	Remote Attestation	Hypervisor	Migration	Accelerator (GPU)	Scaling (manage & mem limit) Load balancer
MS Azure	Confidential Computing	Hardware TEE	Intel SGX, Intel TDX, AMD SEV	Intel ME, AMD PSP	yes	Hyper-V (VMware)			
Google	Confidential Computing	Hardware TEE	AMD SEV	AMD PSP	yes	KVM (VMware)			
Amazon AWS	**Nitro**	**Nitro** Hype rvisor	**CPU independent** Intel, AMD, Arm (Graviton)	**Nitro** Securi ty Chip	yes	Xen/KVM (VMware)		**Nitro** Card (?)	
IBM	**Cloud Data Shield Cloud Hyper Protect**	Hardware TEE	Intel SGX IBM z15	Intel ME	yes				
Alibara	**Inclave** **ACK-TEE** Container Service for Kubernetes	Hardware TEE	Intel SGX	Intel ME	Yes Intel DCAP base				

Confidential Computing on Cloud

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

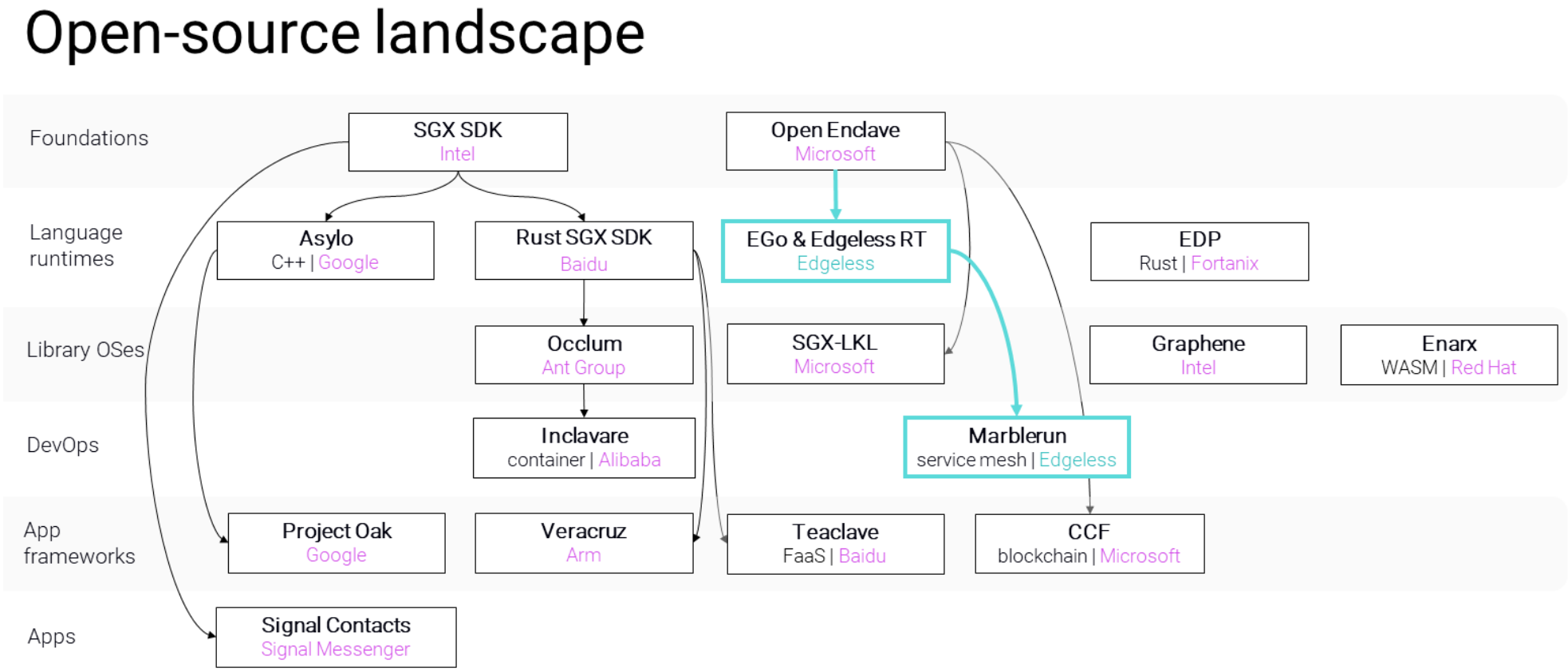
	Service Name	TEE implementation	CPU	Root of Trust	Remote Attestation	Hypervisor	Migration	Accelerator (GPU)	Scaling (manage & mem limit) Load balancer
MS Azure	Confidential Computing	Hardware TEE	Intel SGX, Intel TDX, AMD SEV	Intel ME, AMD PSP	yes	Hyper-V (VMware)			
Google	Confidential Computing	Hardware TEE	AMD SEV	AMD PSP	yes	KVM (VMware)			
Amazon AWS	**Nitro**	**Nitro** Hypervisor	**CPU independent** Intel, AMD, Arm (Graviton)	**Nitro** Security Chip	yes	Xen/KVM (VMware)		**Nitro** Card (?)	
IBM	**Cloud Data Shield Cloud Hyper Protect**	Hardware TEE	Intel SGX IBM z15	Intel ME	yes				
Alibara	**Inclave** **ACK-TEE** Container Service for Kubernetes	Hardware TEE	Intel SGX	Intel ME	Yes Intel DCAP base				

Next Battle Filed

今後の方向性予想（Confidential Computing のプロジェクト）

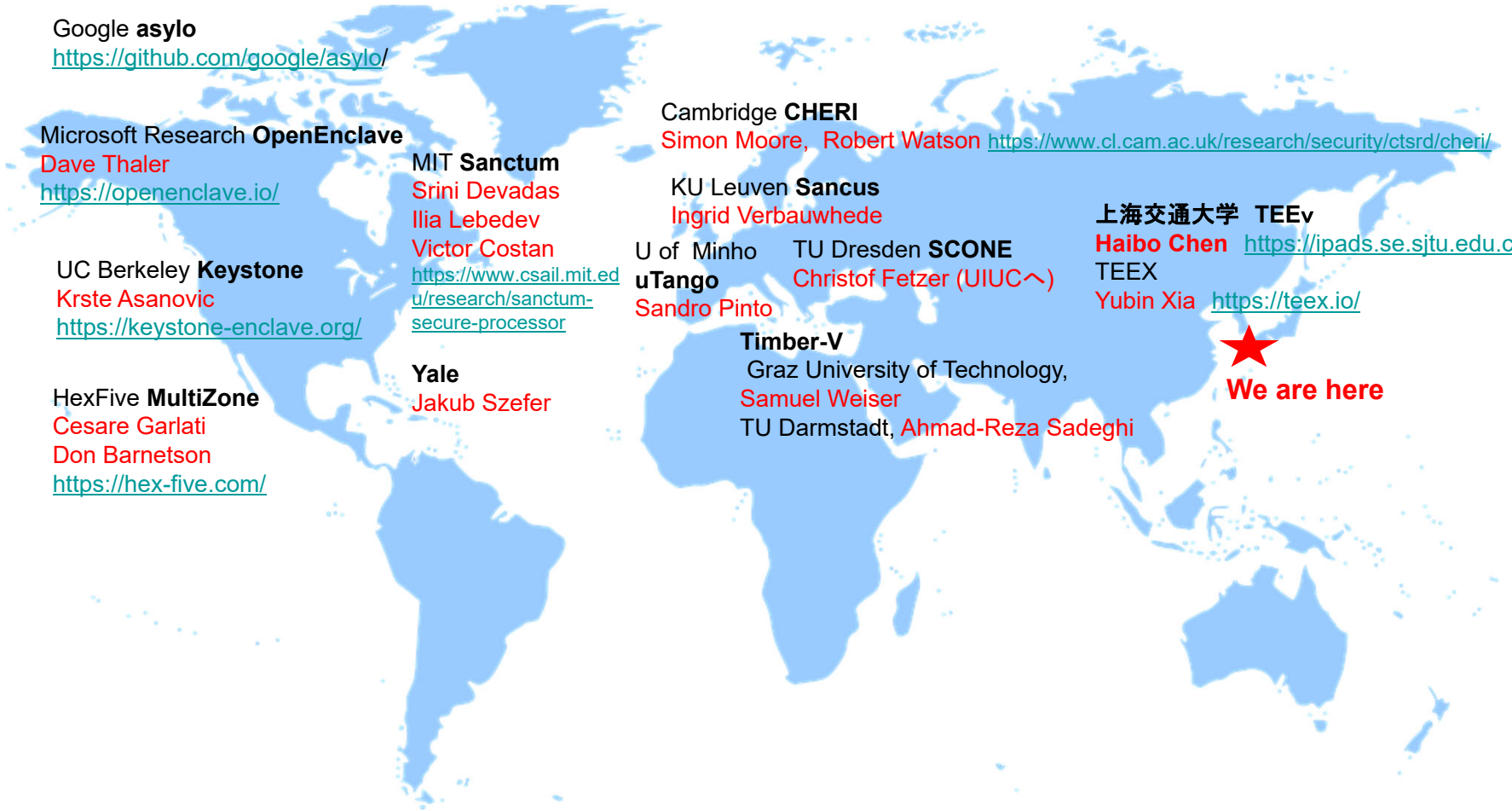
■ The open-source landscape of confidential computing in 2021より

- https://medium.com/edgelesssystems/the-open-source-landscape-of-confidential-computing-in-2021-7f847ebfc0a9



私から見たTEE Research Map

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



TEE関連組織・規格

- GlobalPlatform
  - TEE関係のAPI規格。スマートフォンで採用が多い。
  - SESIP: Security Evaluation Standard for IoT Platforms
- TCG: Trusted Computing Group
  - TPMの仕様を作成している組織。
- Arm PSA(Platform Security Architecture) Certificate
- IETF Protocol
  - TEEP: Trusted Execution Environment Provisioning
  - RATS: Remote Attestation Procedures
- CCC: Confidential Computing Consortium
  - Linux Foundationプロジェクト

- 規格争い
- 主導権争い

関連学会（Academic & Community）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- https://github.com/kunisuzaki/misc/wiki/TEE-conference-%28Academic-and-Community%29/_edit
- **Academic Conference**
  - IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (2024/May/6-9)
  - Asian Hardware Oriented Security and Trust Symposium (AsianHOST) (2023/Dec/13-15) 来年は神戸
  - IEEE International Symposium on Secure and Private Execution Environment Design (SEED) 2024, January 29-30
  - Hardware and Architectural Support for Security and Privacy (HASP) with MICRO 2023, October 29
  - 6th Workshop on System Software for Trusted Execution (SysTEX) with EuroSys 2023 (2023/May/8)
  - Zero Trust Hardware Architectures Workshop (ZTHA) 2023 (2023/November/2) In person workshop
  - 3rd Program Analysis and Verification on Trusted Platforms (PAVeTrust) Workshop with ACSAC 2023
  - IEEE Secure Development Conference 2023
- **Community Conference**
  - Confidential Computing Summit (2023/June/9)
  - FOSDEM2023 Confidential Computing devroom (2024/Feb/3,4)
  - OC3: Open Confidential Computing Conference (2024/March/13)
- 国内だとIEICEのハードウエアセキュリティ研究専門委員会 (HWS)

まとめ

- TEEとは“一時的な”隔離実行環境
  - 実装や制約条件は様々
- RISC-VのTEEは研究を含めて多くある
  - PMPベースのKeystone, Multizone や仮想化ベースのAP-TEE
- PMPも拡張あり
  - sPMP, ePMP, IOPMP
  - Armには
- TRASIOではTEE + Hardware Root of Trustを開発していた
- 関係団体も多くあり
  - CCC, GlobalPlatform, IETF

- おまけ　毎週Google Scholarで上がるTEE関連の論文をつぶやいています。
  - Github Wiki にも上げています。https://github.com/kunisuzaki/misc/wiki/Papers