

Confidential Computing, TEE, TPM, Secure Elementが熱い！

須崎有康 (Kuniyasu Suzaki)



Confidential Computing, TEE(Trusted Execution Environment)はCPUが提供する一時的な隔離実行環境。OSやハイパーバイザからアクセスできず、機密処理が行える。ただし、長期の機密データは保存できず、耐タンパーハードのTPMやSE (Secure Element) に保存する。

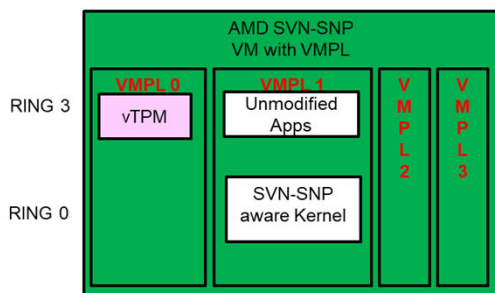
Confidential Computing, TEE対応CPUと活用状況

	組み込み	スマホ	ゲーム	PC	クラウド
Arm TrustZone (Cortex-M)	Raspberry Pi Pico				
Arm TrustZone (Cortex-A)	Raspberry Pi 3B+	Many	Nintendo Switch	???	
Arm CCA upcoming		upcoming	upcoming	upcoming	upcoming
Intel SGX (Core) deprecated				deprecated	
Intel SGX (Xeon Scalable)					Azure, GCP
Intel TDX (Xeon)					Azure, GCP
AMD PSP			Playstation5		
AMD SEV (EPYC)					Azure, AWC, GCP
Apple Secure Enclave		iPhone		Mac	

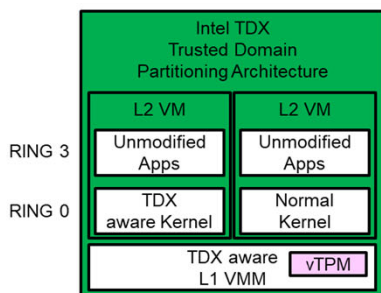
色の濃さは普及度合

Confidential ComputingではVMを基本とするため、**CPUベースのRemote Attestation**ではすべて検証できない。このためCPUベースのRemote Attestationでは初期ブートのみで、起動後は**TPMのRemote Attestation**を使う。しかし、VMを基本とするため、TPMも仮想化する。その仕組みは各CPUで異なる。下図参照

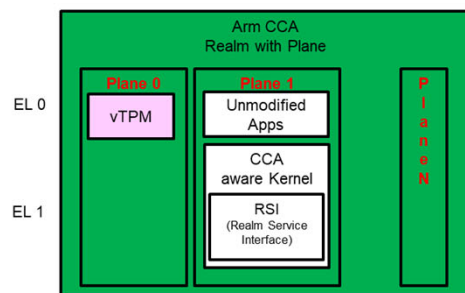
AMD SEV-SNP
VMPL (VM Privilege Level)



Intel TDX
TD Partitioning Architecture



Arm CCA
Plane



仮想化TPMもオープンソースの**coconatSVSM**やMicrosoftの**OpenHCL**などあるが、マイグレーション対応や鍵管理などまだまだ開発課題がある。

参考文献

- Remote attestation is necessary for CVM, IJ技術研究所セミナー 2025年5月
公開スライドPDF: <https://seminar-materials.iijlab.net/iijlab-seminar/iijlab-seminar-20250519-1.pdf>
公開ビデオ: <https://seminar-materials.iijlab.net/iijlab-seminar/iijlab-seminar-20250519.mp4>
- AI時代の安全なデータ処理「Confidential Computing」: 機密コンピューティングの技術的特徴〜低レイヤの開発課題とAI/機械学習等への適用が期待される新しい機能を解説〜, 須崎有康, 情報処理学会誌「情報処理」66(7) e8-e14 2025年6月 <https://ipsj.ixsq.nii.ac.jp/records/2002747>
- 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誌「システム/制御/情報」2024年5月
公開PDF: https://www.istage.ist.go.jp/article/isciesci/68/5/68_185/pdf-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, システム制御情報学会誌「システム/制御/情報」2023年9月
公開PDF: https://www.istage.ist.go.jp/article/isciesci/67/9/67_379/pdf-char/ja
- 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・境界サイエティ Fundamentals Review 2020年10月
公開PDF: https://www.istage.ist.go.jp/article/essfr/14/2/14_107/pdf-char/ja

修士、博士の学生募集中。共同研究も。(^_^)

毎週土曜にXでTEE論文のTweet (kunisuzaki)しています