［ハードウェアセキュリティの最新動向］

# ⑤ Trusted Execution Environment によるシステムの堅牢化

須崎有康 | TRASIO／産業技術総合研究所　　佐々木貴之 | NEC／横浜国立大学

## TEE が生まれた背景とコンセプト

過去の OS のセキュリティの歴史を振り返ると，脆弱性の発見とその修正が繰り返されてきた．このため，OS とは独立してクリティカルなプログラムを隔離実行するハードウェア機能 TEE：Trusted Execution Environment（例：Intel SGX, ARM Trust-Zone）が近年の CPU に付加されている．OS とは隔離実行する機能のみならば，今までもインテルアーキテクチャでは SMM（System Management Mode）や ME（Management Engine）があった．しかし，SMM や ME では BIOS のコードや特殊な管理コードに限定されており，第三者が使えるものではなかった．これらに対して TEE は任意のコードが実行できる点が大きく異なる．これにより，課金やコンテンツの DRM（Digital Rights Management）管理など，脆弱な OS からは隔離したいクリティカルな処理を外部のプロバイダが活用できるようになった．この自由度が増したセキュリティ環境を活用するために，研究ばかりでなくビジネスでも注目を集めるようになってきている．

## TEE の実装

残念ながら TEE は各 CPU で実装が大きく異なり，セキュリティレベルや適する活用領域が違う．この相違が TEE をバズワード化させており，正しい理解なしに使われて多くの誤解を招いている．以下では，代表的な TEE の実装について解説する．

### ARM TrustZone

ARM TrustZone はモバイルデバイス型の TEE を代表する CPU であり，CPU を Secure World と Normal World に分割して通常の OS と Trusted OS を起動する 2 ワールドビューモデルのアーキテクチャである．Normal World には通常のアプリケーションを配置し，Secure World には保護したいアプリケーションを配置することで，Normal World に脆弱性があったとしても，Secure World に配置されたアプリケーションの安全性を保証する．安全性を高めるため，Secure World のソフトウェアは検証が容易なように小さく作られる．

ARM の TrustZone の歴史は古く 2003 年の ARMv6K アーキテクチャから導入されているが，実際に使われるようになったのはスマートフォンで使われている Cortex-A アーキテクチャからである．本稿では Cortex-A を中心に TrustZone を説明する．

図 -1 に TrustZone の概念を示す．TrustZone が提供する基本機能は Secure World と Normal World の提供のみである．World を切り替えるのは SMC（Secure Monitor Call）命令であり，多くの機能はソフトウェアで実現されている．それぞれのワールドでは各 1 つ

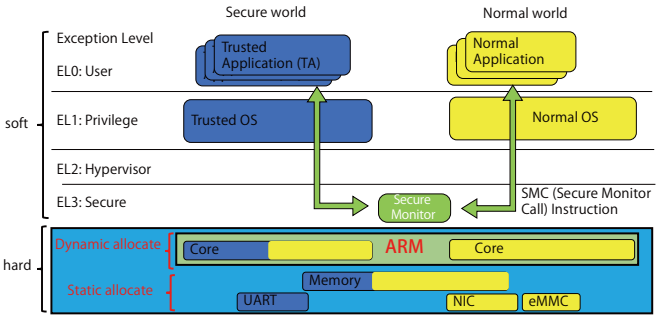


図 -1　ARM TrustZone の概念図（2 ワールドビューモデル）

の OS が実行される．Secure World が使うメモリやペリフェラルは基本的に起動時に設定され，Trusted OS の管理下になる．しかし，割り当てられるメモリは少なく，OS としての機能は限定されたものになる．多くの Trusted OS は TEE インタフェースを規定する団体である GlobalPlatform が定義する TEE Internal API を実装し，暗号やストレージや時間などクリティカルな処理に必要な API のみである．Secure world 内で実行される Trusted OS 上ではこの API を用いて複数の Trusted Application が実行される．

## Intel SGX

SGX（Software Guard Execution）は 2015 年にリリースされた Intel Skylake マイクロアーキテクチャから追加されたセキュリティ機能である．SGX は enclave と呼ばれる隔離された実行環境を動的に提供するが，ここでの実行レベルはユーザレベルのみである．OS 相当の機能はハードウェアとして提供される．このため，ARM TrustZone のようは Trusted OS は存在しない．

Intel SDK に従えば，Enclave 内の処理は基本的にプロセス内のライブラリとしてプログラムされ，図 -2 に示すようにシングルアドレスモデルで処理される．Enclave が使うメモリは起動時に確保された最大 128MB の PRM（Processor Reserved Memory）のみを使う．各 Enclave は PRM 内のメモリを切り出した EPC（Enclave Page Cache）が使われる．この Enclave が使うメモリは暗号化されており，攻撃者がメモリに直接アクセスする攻撃（サイドチャネル）への耐性も施されている．

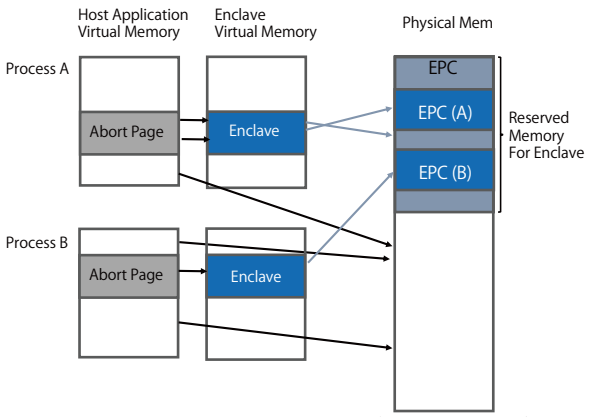


図 -2　SGX でのメモリの使われ方（シングルアドレスモデル）

SGX では実行するバイナリが正規にデバイス上で動作するかを確認する Remote Attestation の機能を提供している．Remote Attestation によりデバイス上の BIOS/UEFI が最新であるか，enclave 内で実行しようとしているバイナリが意図したものであるかを外部から確認することができる．

## RISC-V Keystone

RISC-V は命令セットの規格を公開するオープンソース CPU であり，その規格に基づいて各組織や個人が SoC（System-on-a-chip）[☆1] のプラットフォーム仕様や実装まで自ら公開しはじめ，多くの研究のベースに使われているようになっている．本稿では RISC-V で最も開発が活発な TEE である Keystone を取り上げる．

Keystone は ARM と同じ 2 ワールドビューを提供するが，Secure World である Enclave が，各 Trusted Application ごとに動的に作られる．各 Enclave には Trusted OS 相当の Runtime が実行される．このメモリ確保を図 -3 に示す．各 Encalve は RISC-V

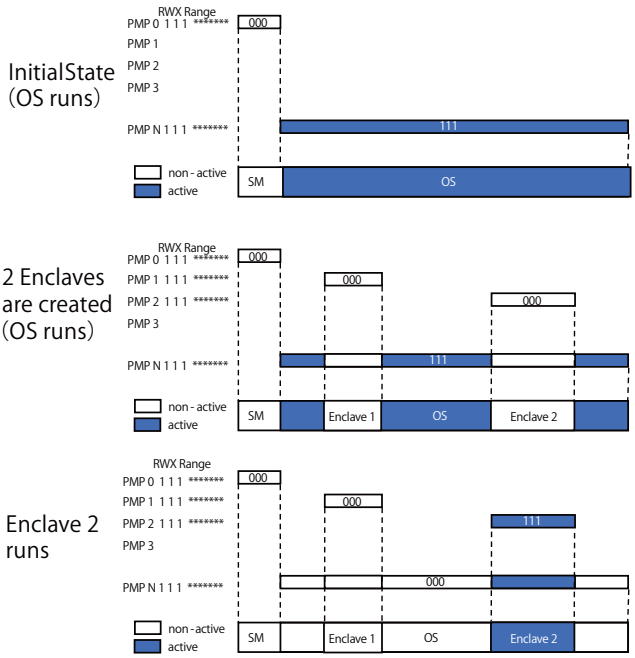


図 -3　RISC-V Keystone でのメモリの使われ方

☆1　CPU や入出力の機能などの周辺機能を 1 つにパッケージしたもの

が提供するメモリ保護機能である PMP（Physical Memory Protection）により，メモリ領域ごとに設定されたアクセス権限情報によって管理される．

図 -3 上段は初期状態であり，ここでは Secure Monitor が PMP の最上位特権，OS（Linux）が最下位特権で割り当てられる．この後，通常のアプリケーションから Trusted Application の生成要求があると Secure Monitor が OS にメモリ開放を依頼し，解放されたメモリに Encalve を割り当てる．図 -3 中段では 2 つ Enclave が割り当てられて OS が走っている状態を表している．図 -3 下段は Encalve2 に制御が移った状態である．この後，Enclave の処理が終れば，メモリを開放・サニタイズして，OS に返却される．

## TEE の比較

表 -1 に上記で説明した 3 つの TEE の比較を行った．隔離実行の特徴，仮想化対応，ソフトウェア開発環境，既存の脆弱性などを参照されたい．

# TEE のユースケース

本章では，TEE が私たちの生活の中でどのように活用されるか，事例や研究動向を基にその展望について述べる．

## セキュリティ機能の保護

TEE の有力なユースケースとしてセキュリティ機能の保護が挙げられる．最近のサイバー攻撃にはセキュリティ機能を無効化した後に実際に被害を与えるような攻撃が観測されている．このような攻撃に対し，TEE を用いてセキュリティ機能を保護することで堅牢なシステムを構築可能である．

保護すべきセキュリティ機能として暗号に用いられる鍵の保護が挙げられる．たとえば TEE が使える Android OS では鍵を管理する keyMaster を TEE 内に実装している．加えて，TEE は，暗号化機能以外のセキュリティ機能を守るためにも用いることができる．たとえば，侵入検知システムを TEE を用いて実装した SGmonitor が挙げられる．

表 -1　TEE 比較表

| | ARM TrustZone | Intel SGX | RISC-V Keystone |
|---|---|---|---|
| 隔離実行の特徴 | 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．多くの機能をソフトに依存 | 複数の隔離実行環境を動的に作成．隔離実行環境からデバイスへはアクセスできない．多くの機能をハードで実装．変更不可 | 複数の隔離実行環境を動的に作成．隔離実行環境にデバイスを割り当てる仕様あり（未実装）．多くの機能をハード・ソフトで変更可能 |
| 特権レベル | すべての特権（TEE 内 OS 実装可能．1 つのみ） | 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．Enclave ごとに毎回作成） |
| 命令 | 1 命令（ワールド切替え）（SMC 命令） | 18 命令（環境設定など）（特権 13, ユーザ 5） | 1 命令（ワールド切替え）（ecall 命令） |
| メモリモデル<br>メモリ確保<br>メモリ暗号化 | 2 ワールドビューモデル<br>起動時時に固定．ワールド間で利用可能<br>なし（オプションでは追加可能） | シングルアドレスモデル<br>起動時時に固定（Intel SGXv1 で最大 128MB）<br>あり（起動時に乱数初期化） | 2 ワールドビューモデル<br>動的で可変．ワールド間で利用可能<br>なし（研究ロードマップにあり） |
| Secure Boot | オプション対応あり | 対応可能 | 現状ではない |
| サイドチャネル耐性 | オプション対応あり | あり | 現状ではない |
| 信頼の基点（Root of Trust） | 基本的になし．携帯は GlobalPlatform の Secure Element の利用例あり | Intel が提供した CPU 固有のもの．変更不可 | 研究段階 |
| Remote Attestation | 基本的にない | Intel が提供したものが使える．隔離実行のみも多い | ある．しかし，現状では信頼の基点がハードウェアではない |
| 仮想化対応 | 試験的に対応．KVM（TZVisor），Xen | Xen, KVM の VM およびコンテナから利用可．VMware は不可 | 仮想化自体が試験中 |
| ソフトウェア開発環境 | OP-TEE，QSEE，KNOX，Kinibi，Trusty | Intel SDK，SCONE，Asylo，OpenEnclave | Keystone SDK |
| 既知の脆弱性 | Boomerang[NDSS18],<br>API/ABI 脆弱性 [CCS19] | Prime+Probe[DIMVA17],<br>ForeShadow[USENIX Sec18],<br>API/ABI 脆弱性 [CCS19] | BOOM（Out-of-Order）Speculative Attacks[CARRV19],<br>API/ABI 脆弱性 [CCS19] |

これにより，侵入検知システムへの攻撃や侵入検知システムが扱う情報を保護することができる．

### ライセンス管理やペイメント機構の保護

有料のコンテンツをユーザに配信する際には，コンテンツにアクセスする権利のあるユーザのみがコンテンツを利用できるように制御する必要がある．この際，デバイスの持ち主が悪意のあるユーザであったとしても，権限のないコンテンツの閲覧や不正な再配付が行われないように，コンテンツが保護されなければならない．この問題は，TEE の中にライセンス管理機能を配置し，悪意のあるユーザからライセンス管理機構を保護することによって解決することができる．

また，近年は，スマートフォンを用いたペイメントが普及している．安全なペイメントを実現するためには，マルウェアなどによるペイメントの情報の漏洩や，ペイメントのソフトウェアへの攻撃を防ぐ必要がある．TEE によって，スマートフォンのペイメントの機構を保護することが検討されている．

### プライバシ情報の保護

TEE の中に格納されている情報は TEE の外から見えないという機密性から，プライバシ情報の保護に用いるユースケースが検討されている．たとえば近年は顔や指紋がスマートフォンの認証に用いられており，生体情報がスマートフォンに保存されている．認証機能や生体情報を TEE の中に配置することで生体データを守ることが可能になる．

### クラウドの保護

クラウド環境では，利用者はクラウド事業者のリソースを借りて，それを利用する．もし，クラウド事業者が 100% 信用できなければどうなるだろうか．クラウド事業者が利用者のデータを盗み見たり，改ざんしたりするかもしれない．TEE を用いることで，この懸念を払しょくすることができる．具体的には，Intel SGX のデバイスの持ち主であっても，TEE で保護された領域にアクセスできないという特徴を利用して，クラウドの利用者のみが TEE で保護されたデータにアクセスできるようにすることができる．Microsoft Azure や IBM のクラウドが，TEE に対応した仮想マシンの払い出しに対応している．

### AI の保護

近年の AI に用いられる機械学習は，学習データや学習プロセス，学習の結果を攻撃者に改ざんされてしまうと，誤った判断を引き起こし，AI が用いられているシステムが正常に動作しなくなる恐れがある．そのため，AI の保護に TEE を活用する研究が進められている．具体的には，機械学習の基盤である TensorFlow を Intel SGX によって保護する TensorSCONE や，分散処理基盤である MapReduce を SGX によって保護する研究が進められている．

## 今後の展望

TEE は，情報化社会の安全性を担保するための重要な技術であり，使いやすい実装や活用法の研究開発が活発に進められている．インターネットのプロトコルを定義する IETF においても TEE を活用する TEEP（Trusted Execution Environment Provisioning）などの策定が進んでおり，社会に浸透していく技術である．

（2020 年 4 月 3 日受付）

**謝辞**　本成果の一部は，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「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」の結果得られたものです．

**須崎有康（正会員）**　k.suzaki@aist.go.jp
1990 年東京農工大大学院中退．その後，電子技術総合研究所を経て，国立研究開発法人産業技術総合研究所／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．情報理工学博士（東大，2009 年）．本会シニア会員．

**佐々木貴之（正会員）**　tsasaki@nec.com
2004 年東北大・工卒業．2006 年東大・理・物理学専攻修士課程修了．同年日本電気（株）入社．以来，クラウドセキュリティや，ネットワークセキュリティ，IoT セキュリティの研究開発に従事．現在，同社セキュリティ研究所主任研究員．