

1. TEEとは何か？

Ao Sakurai

2026年度セキュリティキャンプ全国大会
L1 – 暗号・CVMビルド&スクラップゼミ

本セクションの目標



- Intel TDXに触れるにあたり、TDXもその一員であるTEE技術についてその背景や考え方、性質を押さえる
- TEEの有力な応用先の一つでもある秘密計算についてごく軽く触れ、関連する他の技術について知り比較を行う

自己紹介



- 名前：櫻井 碧（さくらい あお）
 - Twitter: @dd_clifford
- 所属/肩書：株式会社Acompany
CC Lab部シニア研究員、
未踏スーパークリエイター（2019）
seccamp全国大会講師（2023～）
IISEC特任研究員（2025～）
- 出身大学：早稲田大学（情報工学修士）
- 分野：TEE、暗号、プライバシーテック等
- 趣味：車、バイク、ゲーム、蒙古タンメン中本



「データを確実に保護しながら計算する」方法

現代のITインフラに蔓延する「偽の信頼」



- 「自らのデータを他人に預けて何らかの処理をしてもらう」ユースケースは、往々にして一定のニーズが存在する
 - オンラインショッピング
 - デジタル著作権管理（DRM）処理
 - クラウドコンピューティング
 - クラウドストレージ
 - etc...
- では何をもってしてその**他人**を「**信頼できる**」と見做している？

「人間を信用してはいけない」



- この世には、明らかに信用ならないのに世間に受け入れられてしまっているシステムが**多数存在する**
- この事実、特に**機密性の高いデータ**を扱う場合に**大きな問題**となる
 - 医療情報
 - 生体情報
 - 機微な個人情報
 - クレジットカード番号
 - etc.

ケース①：クラウドサービス（1/2）



- 現在普及しているクラウドサービスは、**クラウドプロバイダを信用する事が出来ない**
 - FW等で外界との境界にて防御はしている
 - 境界の内側のセキュリティは「**ブラックボックス**」
 - 「ハイパースケーラだから安心」は**根拠のない神話**



ケース①：クラウドサービス（2/2）



- 「流石に陰謀論すぎでは？」と多分思われると思うが、実際に**そのような事件が発生**している

全記事 ニュース

「Google従業員が、YouTubeを介して任天堂のゲーム発表動画を閲覧し事前にリークしていた」との報道。管理者権限で非公開動画を見る手口

By Hideaki Fujiwara - 2024-06-04 11:00



参照：<https://automaton-media.com/articles/newsjp/20240604-296067/>

ケース②：著作物配信



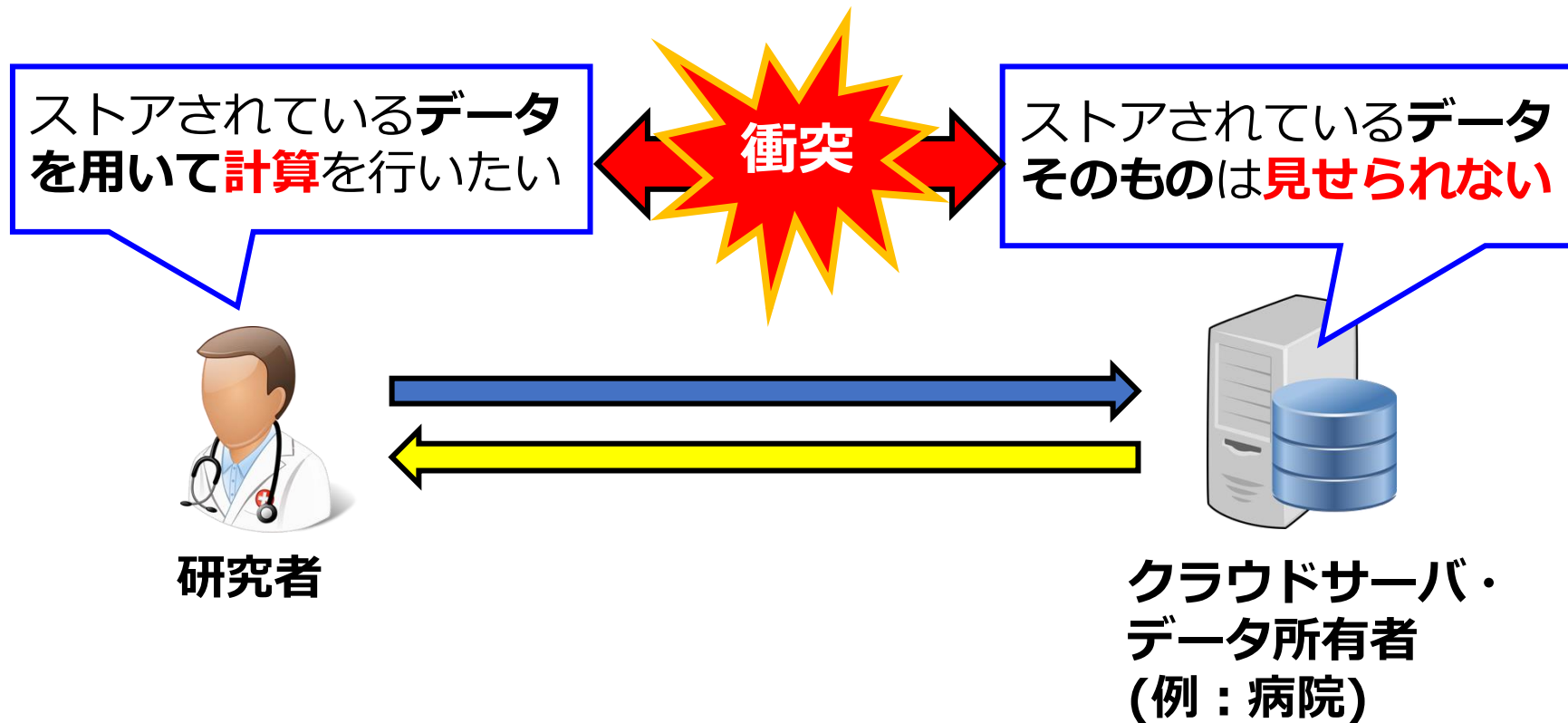
- ビデオや音楽のストリーミング配信等では、**デジタル著作権保護（DRM）**によって**コンテンツ**を保護する必要がある
 - いわゆる“**割れ厨**”ユーザ対策
- しかし、執念深いユーザは**DRMをバラバラ**にして解析し、鍵を取り出して**暗号を解き、コンテンツを抽出**してしまう
 - メモリは守られていないので根本的に無意味

データセキュリティに必要な根本的な思想



- 大原則は、「**人間の善意や人間自体の信頼性**には頼らず、**暗号的・数理的・構造的に絶対的な安全性**を保証する事」
- **データが保護**されていなければならない**全てのフェーズ**で、**絶対的にデータが保護された状態**で処理を進めれば良い

「秘密計算」という新しい概念



この衝突を解決するには、**データの中身を見ない**まま**計算**を行い、各データを**特定できない**形の結果を得る「**秘密計算**」技術が必要

準同型暗号を使う？



- 従来手法でこの要件を満たす技術として有名なのは「**準同型暗号**」
- **暗号文の状態**で**足し算**や**掛け算**が出来る種類の暗号

$$Enc(1) + Enc(4) = Enc(5)$$



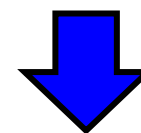
暗号化

1



暗号化

4



復号

5



- 結論から述べると、**現代のコンピュータは準同型暗号に追いついていない**
 - 必然的に**準同型暗号は現実的ではない**

メリット	デメリット
ハードウェアを信頼しなくて良い	極めて遅い
厳密な意味での 完全な保護	莫大なメモリ を 食い潰す
耐量子性 を持つ	精度に難がある

準同型暗号の致命的な欠点



- とにかく**非常に重く**、到底**実用に堪えない**

```
aos@Apollyon:~/cpp$ ./a.out
Result: 1000000000
Elapsed time: 113[ms]
```

普通のプログラム：**0.113秒**

```
m = 32109, p = 4999, phi(m) = 16560
ord(p)=690
normBnd=2.32723
polyNormBnd=58.2464
factors=[3 7 11 139]
generator 320 has order (== Z_m^*) of 6
generator 3893 has order (== Z_m^*) of 2
generator 14596 has order (== Z_m^*) of 2
T = [1 14596 3893 21407 320 14915 25618 11023 6073 20
668 9965 27479 16820 31415 10009 27523 20197 2683 24089
9494 9131 23726 2320 19834 ]

Security: 127.626
Creating secret key...
Generating key-switching matrices...
Number of slots: 24
Initial Ptxt1: [2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
2 2 2 2]
Initial Ptxt2: [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1]

Elapsed time for initialization: 9600[ms]

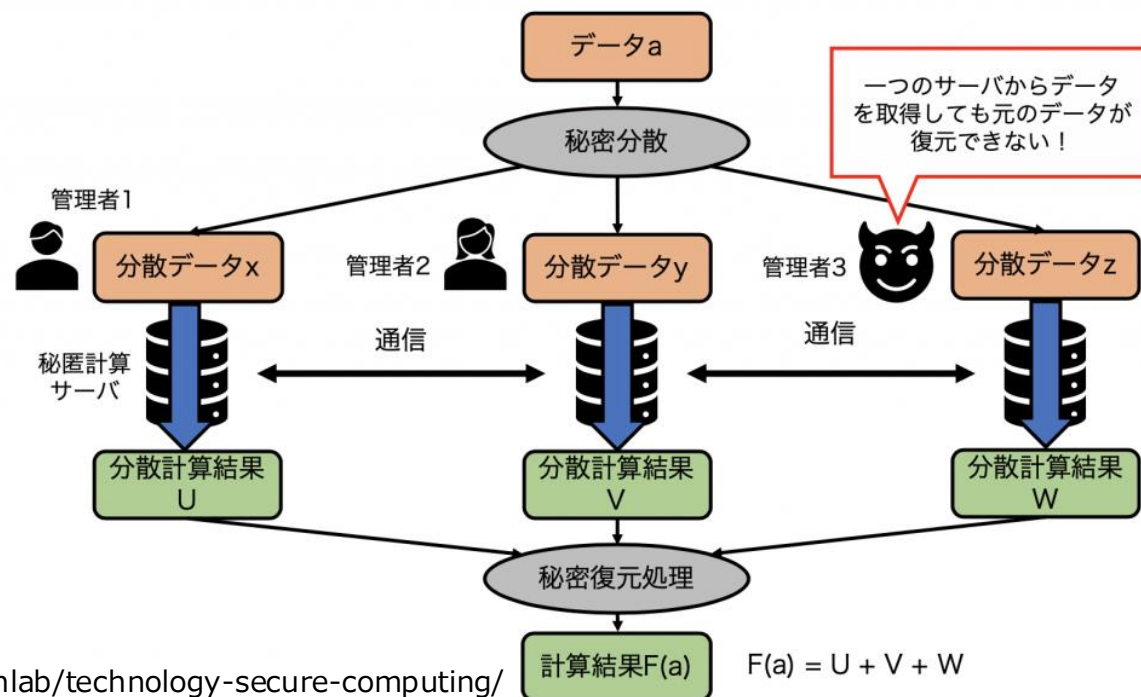
WARNING: decrypting with too much noise
Decrypted Ptxt: [4844 2247 319 4883 3790 2401 3966 1092
1438 2549 320 1139 3046 1921 3095 1123 832 1055 703 20
09 4243 2354 886 4665]

Elapsed time for calculation: 100825[ms]
```

完全準同型暗号 (HElib):
合計**110秒**、しかも解が破損

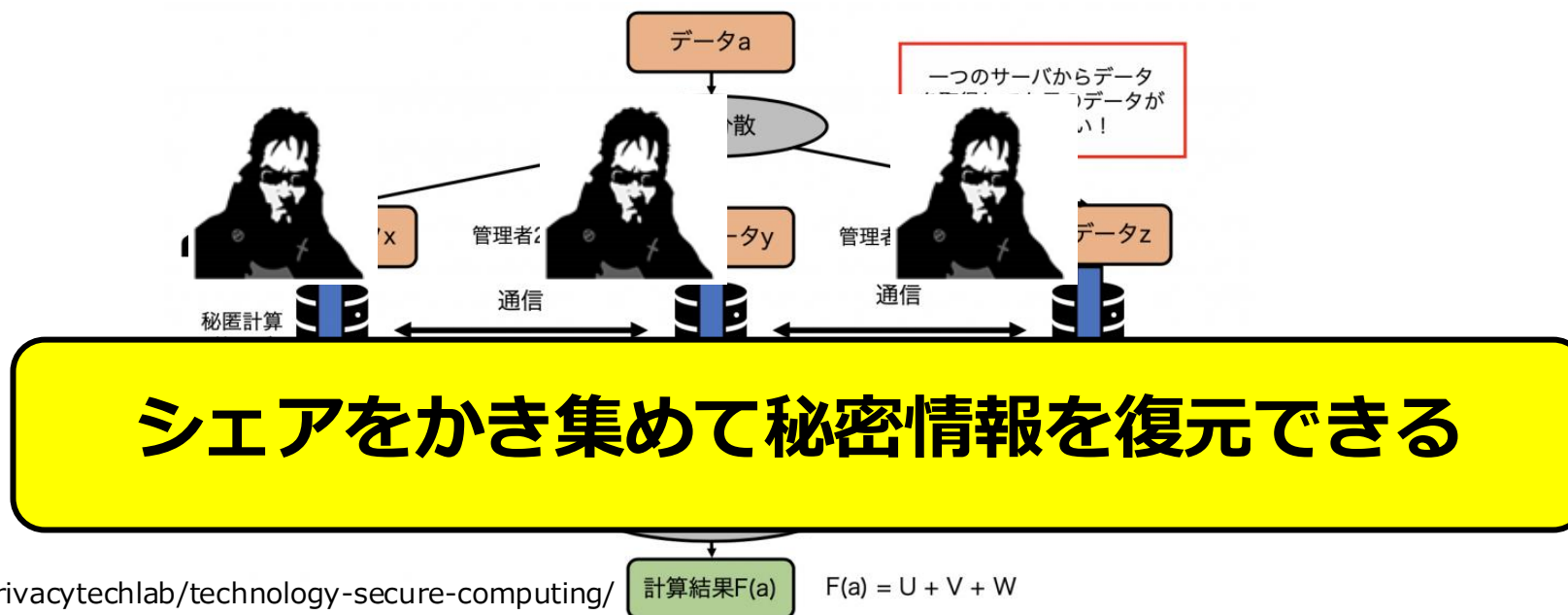
秘密分散を使う？

- 秘密計算手法でよく使われる他の手法に「**秘密分散**」がある
- 「シェア」という無意味化された断片に分割して計算を行う、**情報理論的安全性**を保証できる技術
 - シェアを全て揃えない限りはどう足掻いても秘密を解読できない



秘密分散は「陰謀論」に弱い

- 逆に言えば、分散先のサーバが**全て危殆化**している場合、**一瞬で秘密情報が解読されてしまう**
 - 全サーバが同一事業者のクラウドだったら、事業者は攻撃できるのでは？
 - 外部の攻撃者が全サーバを侵害していたらどうするのか？
⇒**限りなく陰謀論だが言い返せない（信頼の仮定が広すぎる）**
- 処理速度も決して速くはない（通信のオーバーヘッドが顕著）



秘密計算界のダークホース



- そんな中、比較的最近登場した技術が**TEE**
(**Trusted Execution Environment**; 信頼可能な実行環境)
- ハードウェアの力を借りる事で、秘密情報を保護したまま計算に使用できる保護領域を実現できる技術
 - 秘密計算に使えるそう

TEE（信頼可能な実行環境）（1/6）

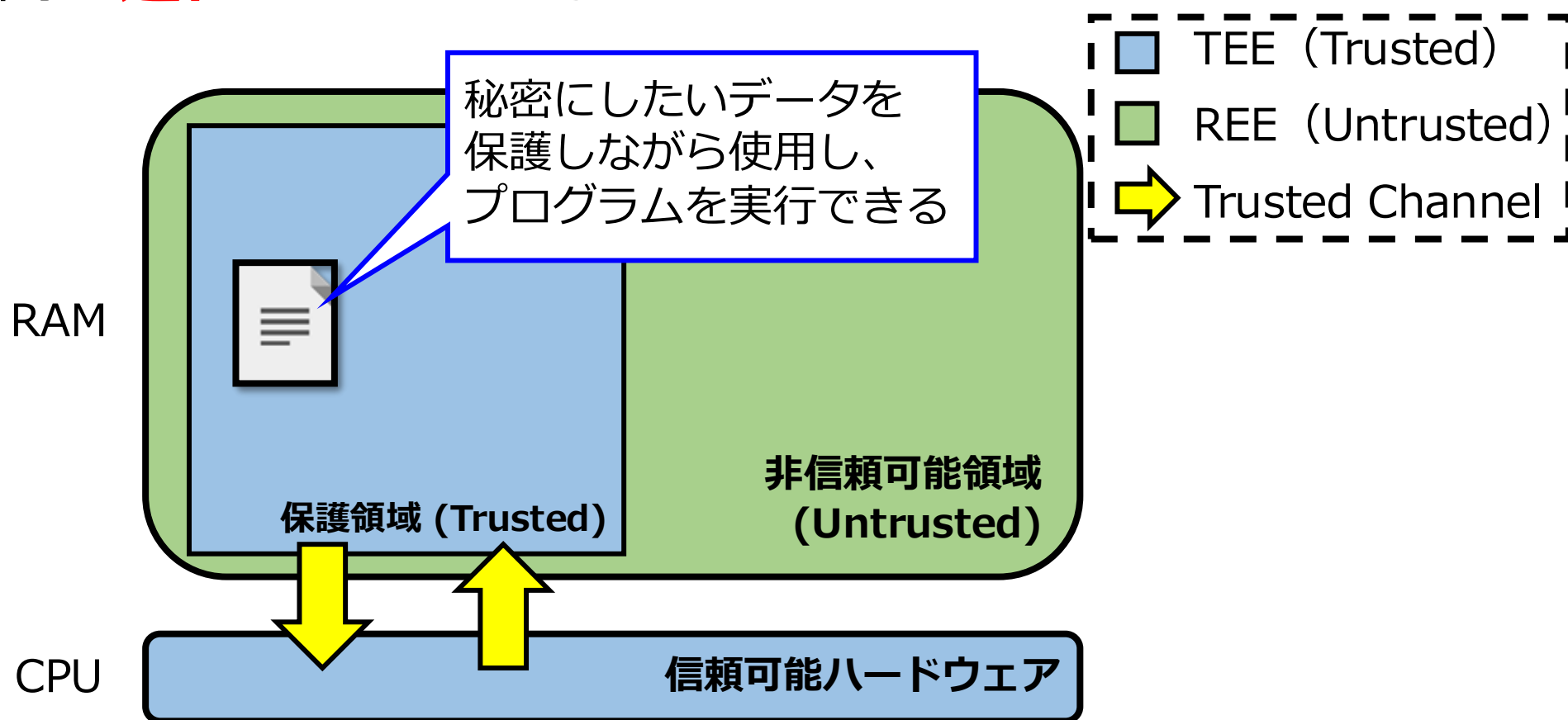


- **TEEの思想**：コンピュータリソースを、**信頼可能な領域**と**信頼できない領域**に分ける
 - 信頼可能領域でデータを扱う事で、データを保護しながらのプログラム実行を可能とする
- **信頼可能な領域**：**信頼可能なハードウェア**及びそれによりメモリ上に生成された**保護領域**
- **信頼できない領域**：**それ以外のすべて**
 - 脅威モデル次第では、OSやVMMすら非信頼領域として扱う

TEE（信頼可能な実行環境）（2/6）



- より具体的な事例に落とし込むと、**信頼可能領域**は**CPU内**、CPUによって生成された**RAM上の保護領域**及びその間の**通信路**がTEEとなる





- CPU等の**信頼可能なHW**が、メモリ上の**隔離領域の絶対的な隔離処理を行う点**は**原則全てのCPU型のTEEで共通**
- 隔離領域には、**予め定義された厳格なインタフェース**に対し、**専用の手続き（特殊なCPU命令等）を経る事でのみ進入**できる
- それに加え、大部分のTEEでは、メモリ上の**隔離領域を暗号化する鍵**も、その**信頼可能なHWが有し暗号処理も実施**する



- TEEは、**信頼可能なHWまたはTEE的に信頼可能とされるSWが侵害不可能な形で有する秘密鍵**（≠メモリ暗号化鍵）により、その**身元の真正性を保証**できる（事が多い）
 - 例えば、**CPUベンダが製造時に焼き付けた鍵**、CPUベンダとの特殊な手続きの末**信頼可能SWにプロビジョニングされた鍵**を保持する
- この鍵は、その鍵を**発行した権威**（CPUベンダ等）の**ルート証明書により検証可能**な、そのTEEの**トラストチェーンの頂点**として機能する（**トラストアンカー**）
- 専門用語では、このようにトラストアンカー鍵を耐タンパ的に保持するHW/SWコンポーネントを**信頼の基点（Root-of-Trust ; RoT）**と言う



- 同時に、大抵のTEEにおいては、そのTEEの**セキュリティバージョン**や**測定値**（Measurement）等を格納した**身元証明書**を、**改竄不可能な形で発行**する機能が提供されている
- この身元証明書に、先述の**RoT鍵によって署名して利用者に渡す**事で、利用者は相手をしようとしているTEEが、本当に**自分の期待する通りの信頼可能なものか**を確かめられる
 - ベンダのルート証明書で検証する事で、ベンダのお墨付きが得られる
- この手続きを**Remote Attestation**といい、TEEが備えるべき重要な機能として位置づけられている[4]
 - 本ゼミの中盤で解説予定



- 大分類としては、TEEは**HIEE**（Hardware-Assisted Isolated Execution Environment）と呼ばれる技術に分類される
- 他のHIEE技術（TPM等）と比較した場合のTEEの明確な特徴は、**保護領域内での動作をユーザが定義**できるという点
 - 今回のセキュリティキャンプでのコード実装の大部分はこれ



- この**TEEの特長・機能**により、使用中のデータ（data-in-use）を保護しながらの計算（つまりは**秘密計算**）を行う事を**機密コンピューティング（Confidential Computing）**と呼ぶ



Confidential Computing JP

メジャーなTEE技術



Intel SGX



ARM TrustZone



ARM CCA



Keystone

RISC-V Keystone



AMD SEV



Intel TDX

2タイプのTEE



- **部分隔離型**

- 例：SGX、TrustZone、KeyStone
- メモリの**特定の区画を保護**する、**本来の文脈でのTEE**
- 保護領域内の動作定義の実装に**独特のスキルが必要**
- **OSやVMMすら信頼しないモデルが多い**

- **Confidential VM (CVM) 型**

- 例：SEV、TDX、CCA
- メモリ（あるいはVM）を**丸ごと保護**する、**TEEとしては割と異端**
- TEE実行を想定していないプログラムも**そのまま実行可能（OS含む）**
- **デプロイモデルによっては、ゲストOSやクラウドベンダを信頼**する必要がある（脅威モデルが弱い）
- **Attestationの適切な設計が極めて難しい**



- 保護領域が**暗号化**されるかは**TEEの技術次第**
- 例えば、TrustZoneやKeyStoneは、**超特権ソフトウェア**による極めて強力な**アクセス制御**により保護領域が守られる
 - 超特権ソフトウェアの名前は前者では「Secure Monitor」、後者では「Security Monitor」
 - ここで**専用のCPU命令**により保護領域内外の切り替えが発生する
- 暗号化されていない場合、**コールドブート攻撃**等には**無力**
 - 大体は暗号化プラグインが用意されている



- また、NVIDIAはHopperアーキテクチャより**GPUのTEE機能を提供**し始めた
 - NVIDIA Confidential Computing (**NCC**)、H100のTEE等と呼ぶと多分通りが良い
- 主に**CVM型TEEとセキュアチャネルを確立**してデータの送受信を行い、そのデータを用いて**安全なモードでGPU処理を行う**事で、**TEEの範囲をGPUにまで拡張**できる革新的な技術
 - これにより、LLM等の極めて重いワークロードをTEEで行う活路が拓けた事になる



- GPU TEEにおいては**GPUメモリは暗号化されないが**、これはGPUメモリが極めて精巧な造りとなっているため、**物理アクセス攻撃でも中身を盗聴できない事を前提**としている
 - 通常のDRAMのようなPCB上の銅ベースの配線と異なり、シリコンインターポーザ等の極めて複雑な構造をしている
 - メモリ暗号化機能を持つ**CPU型TEE**も、直接の盗聴が不可能であると考えられている**CPUパッケージ内は暗号化しない**
- 上記の考え方は、2018年に発表されたGPU TEE構想についての論文である**Graviton**[5]の系譜を継ぐものである（と思われる）
 - Graviton論文の著者はMicrosoftの研究者



- Q1. TEEは準同型暗号や秘密分散より速い？
 - **YES**。CPU内での演算は**平文を用いた普通の処理**であり、秘密分散に顕著な多量の通信も発生しないため、関連技術の中では**極めて速い**
- Q2. TEEは本当に誰も信頼しなくていいのか？
 - **NO**。明らかにそのCPUの**ハードウェアベンダ**（SGXならIntel）を**無条件に信頼する必要がある**
 - 何ならハードウェアベンダによるTEEの実装に不具合があると致命的な脆弱性になり得る ⇒**本ゼミの攻撃実践パートで説明**
 - さらに言えばCVM型（SEV、TDX等）に関しては、現在のクラウド環境だと**ゲストOSやそれを用意したクラウドベンダすら信頼する前提**となっている（例：悪性のOSによる悪さを覆い隠すつもりか？）

その他TEEについての議論 (1/3)



- TEEの保護機能としては、**サイドチャネル攻撃の対策は行われない**
 - **サイドチャネル攻撃**：直接秘密情報を解読・取得するのではなく、周辺の情報（例：実行時間）から秘密情報を推測する攻撃
 - **TEEが特異的にサイドチャネル攻撃に弱いわけではない**。他でもサイドチャネル攻撃に弱いワークロードはTEEで動かしても弱い
 - よって、サイドチャネル攻撃の対策を意識しての実装を行う事が望ましい
- 量子コンピュータ耐性は**現時点の推定では恐らく当面は十分**
 - AES 256bit相当以上であればまず間違いなく当面は大丈夫そう
 - TDXの保護領域はAES 128bit相当であるが、最近のNISTの見解[3]によれば128bitも同様に当面は安全そうであるため、こちらも当面は問題ないと考えられる

その他TEEについての議論 (2/3)



- マシンに**物理的にアクセス**し、メモリ等に直接物理的に行うような攻撃には、**現在のTEEは耐性を持たない**（持たなくて良い）という**暗黙の合意**が生まれつつある[6]



サーバ室に侵入し
物理アクセスで
攻撃を仕掛けようとする例
([画像出典](#))

その他TEEについての議論 (3/3)



- メモリ暗号化機能を持つTEEの場合は機密性の観点では保護できるが、**物理完全性攻撃**からの**完全な保護は現状困難**
- 物理完全性攻撃にも唯一対応していたTEEが、**Coreシリーズ等に搭載されていた版のIntel SGX**であるが、**現在では廃止**されている
 - 現行のSGX (Scalable-SGX) では物理完全性保護機能は持たない

本ゼミでやる内容



- CVM型TEEの主要な実装例の1つである**Intel TDX**に着目し、その**基本知識**や**応用的な議論**を解説する
- TDXを用いて**秘密情報を安全に取り扱いながら処理を行う**アプリケーションを開発し、**TEEの恩恵**を体感する
- TDX、ひいてはTEEにおける**様々な抜け穴や攻撃**について詳細に解説し、その一端を**実践的に体験**する



- [1] “【技術】 TEE (Trusted Execution Environment) とは？”, 自己引用,
<https://acompany.tech/privacytechlab/trusted-execution-environment/>
- [2] “TEE (Trusted Execution Environment)は第二の仮想化技術になるか?” by Kuniyasu Suzuki, <http://www.ipsj.or.jp/sig/os/index.php?plugin=attach&refer=ComSys2020&openfile=ComSys2020-Suzaki.pdf>
- [3] “Post-Quantum Cryptography”, NIST, 2023/7/27閲覧, [https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-\(evaluation-criteria\)](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria))
- [4] “A Technical Analysis of Confidential Computing”, Confidential Computing Consortium,
https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf
- [5] “Graviton: Trusted Execution Environments on GPUs”, Stavros Volos et al.,
<https://www.usenix.org/conference/osdi18/presentation/volos>
- [6] “Nimble: Rollback Protection for Confidential Cloud Services (extended version)”, Sebastian Angel et al.,
<https://eprint.iacr.org/2023/761.pdf>