トラストを確立する技術の概要

どのような技術がなぜ作られてきたのか

セコム株式会社IS研究所
宮澤慎一

PKI and Trust Days 2021
2021年4月15日

Disclaimer

- 本日の講演は文献やインターネット上の情報をもとに歴史を考察したものです。
- 細心の注意を払って調査しましたが事実と異なる点もあるかもしれませんが、ご了承ください。
- 社名や製品名も出てきますので、もし問題がありましたら後日修正いたしますので、ご指摘いただければと思います。

本講演の目的

- この後に続く講演のための
  - 基礎知識
  - 歴史背景
  - を知っていただきたい
- 温故知新の技術にもっと光を当てたい
  - 聴衆の皆様の中には、今日紹介する技術の中の人（中だった人）がいるかと思います。
  - 間違い、補足、批判がある場合は、Twitter等でつぶやいて頂くと幸いです。
- 今回のPKI & Trust Days2021で紹介される技術がもっとSNSで話題になると嬉しいです。

年表

1960 1970 1980 1990

60s 70s 80s

Tamper Proof (Smart Card)

IC/IDカードの発明
(1967、ドイツ)

ICカードの発明
(1975, フランス)

開発競争(1977 -)
BullCP8
SGS Thomson
Shlumberger
Motorola

開発競争(日本)
大日本印刷(1981-)
凸版印刷(1983-)
東芝(1984-)
日立(1985-)

uAbyss(1987)

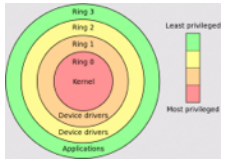
Integrity (Trusted Computing)

New directions in cryptography (1976)

Trusted Computer system Evaluation Criteria (1983)
Trusted Computing Base (TCB)の考え

Distributed System Security Architecture (1989)

Isolation



Multics (1964-1969)
プロセス間の分離、privilegeによる分離
RING protection

Intel 286(1982)
Protected mode

Intel 386(1985)
Protected mode

年表

1990 2000 2010 2020

90s 00s 10s

Tamper Proof (Smart Card)

Integrity (Trusted Computing)

Isolation

Multos(1990)
英国ナショナルウエストミンスター銀行
モンデックス

Felica(1994)

Visa Open Platform (1997)

NFC(2003)

Java Card (1996)
ICカード上でJavaアプリが動く試作機
Integrity Arts(Gemplus子会社)は
ICカード上の共通アプリ開発環境

GlobalPlatform (1998)

sim card(1991)

eSIM (2016)

Apple Secure Enclave (2013)
Iphone5s touchid

Trusted Computing Platform Alliance (1999)
AMD, Hewlett-Packard, IBM, Intel and Microsoft.

TPM内蔵 ThinkPad(2002)

Intel LaGrande(2003)

Intel TXT (2007)

Chromebook(2011)

Titan(2018)

NitroChip2018)

Titan-m(2018)

Cerberus(2018)

IBM4751(2001)

AEGIS(1997)
Secure Boot

Trusted Computing Group (2003)
AMD, Hewlett-Packard, IBM, Intel and Microsoft.

TPMチップ

Intel PTT (2013)

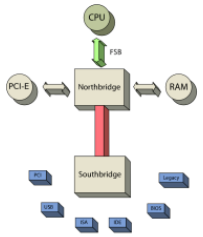
DICE(2015)

TPM2.0(2014)

ATECC608A+GCP(2018)

Intel EPID (2008)

Apple Secure Enclave (2013)
Iphone5s touchid



ARM TrustZone (2003)

Intel ME (2007)

Intel CSME (2015)

ARC

Quark

Microsoft NGSCB(2003)

Intel Haswell(2013)

Intel SGX(2013,2015)

Apple T1(2016)

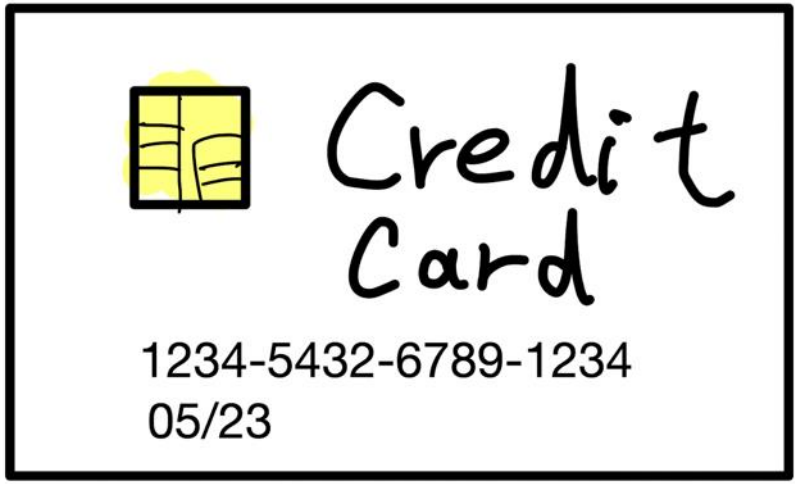
Apple T2(2018)

Southbridge (1991) , ICH

Intel Mac SMC(2006)

ICカード (Smart Card)

- ICカードの概要
- クレジットカード、Suica、携帯電話やスマホのSIM
- Secure Element
- 秘密鍵や公開鍵も埋め込まれる
- **耐タンパ性**という特性が大変重要



耐タンパ性とは

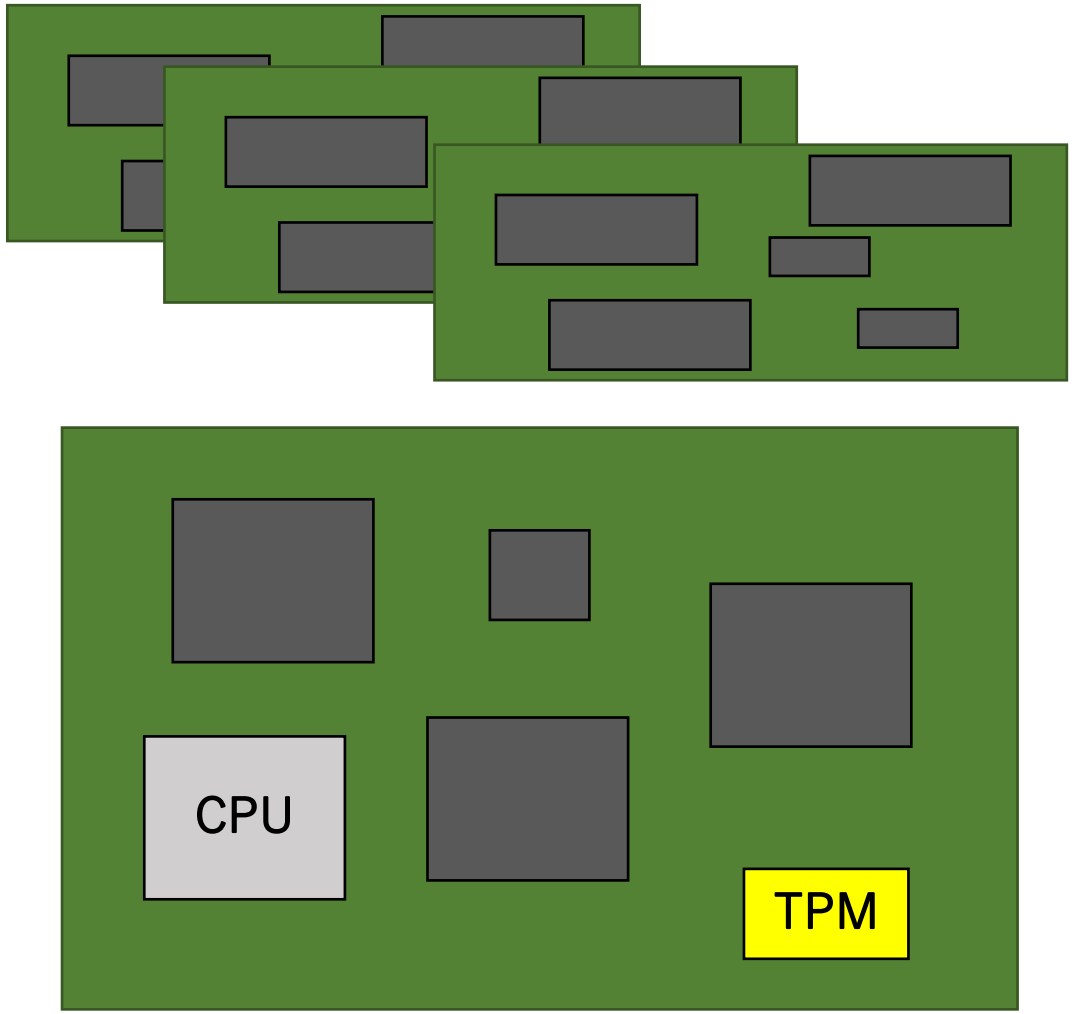
- Tamper
  - （許可なく勝手に）変更する
- Tamper Proof Tape
  - 貼った後、剥がされた跡がわかるテープ
- Anti-Tamper
- Tamper Proof
- Tamper Resilient
- Tamper Detection
- 半導体回路を製造する物理的な技術
- チップ内部について、
  - 後から変更できない
  - 中身がどうなってるかわからない

Permanent tamper evident numbered label showing the label applied to the surface, the label voiding and the permanent void message left on the surface of the container.

TamperTechTeam

TPM

- ICカードは、一つのチップを保護すればよかった
- PCの世界は？
  - マザーボードや拡張ボードにはチップやファームウェアがたくさん
  - これらの完全性を満たす方法は？
- 耐タンパ性のあるチップを一つ利用して、基盤全体（プラットフォーム）のハードウェアとファームウェアの完全性を実現



TPMフロー詳細

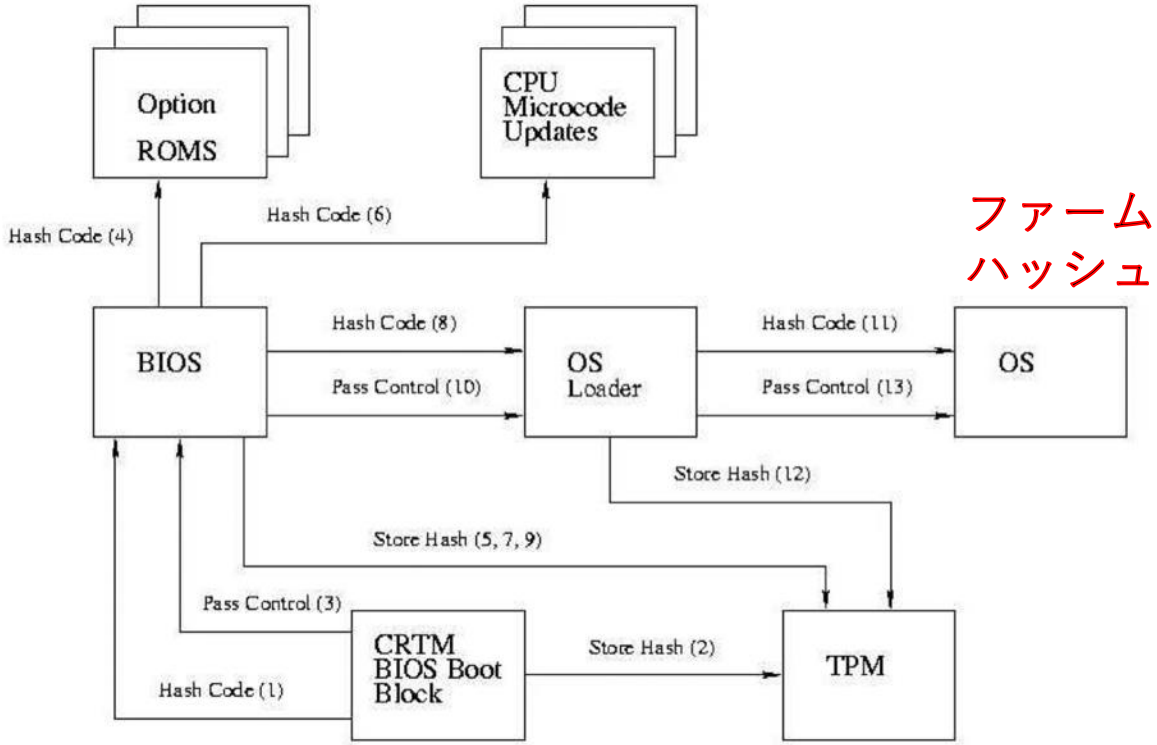
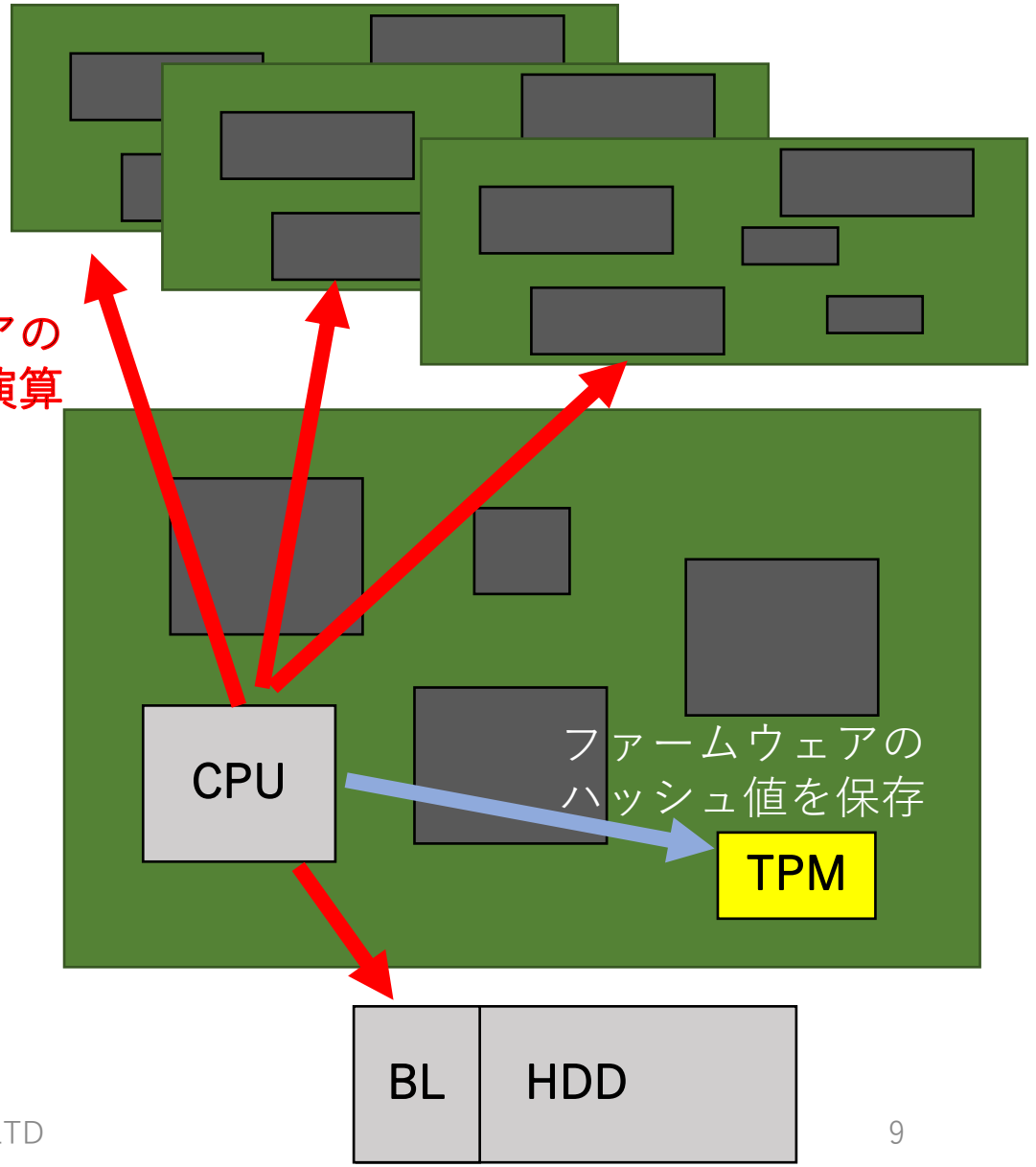
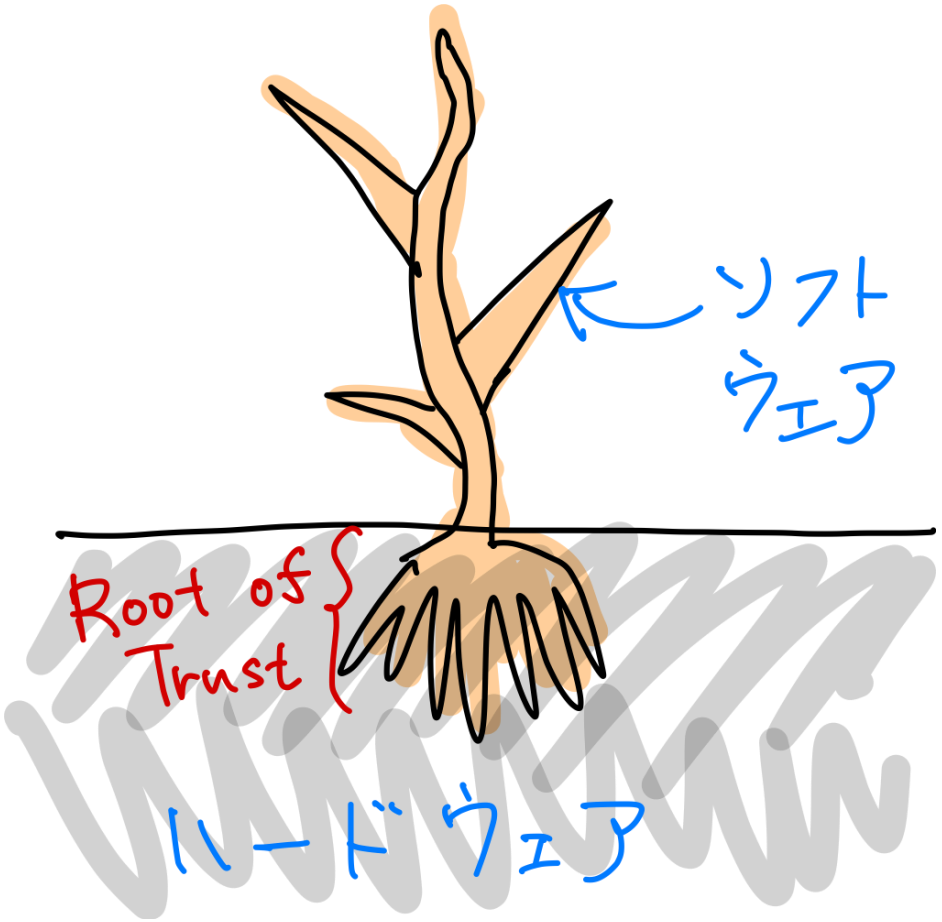


Figure 2 TCG Integrity Protected Boot Sequence

Reid, J., & Caelli, W. (2005). DRM, trusted computing and operating system architecture. In ACSW Frontiers 2005:



Root Of Trust



- Root Of Trust for Measurement
  - **完全性**を実現する計測プログラム
  - BIOSのROMやCPUのマイクロコード
- Root Of Trust for Report
  - **機器認証**できる形での**完全性報告**のための証明書
  - TPM
- Root Of Trust for Storage
  - 外部ストレージへ**暗号化保存**する暗号鍵
  - TPM
- ソフトウェアの木を成長させる
  - Chain Of Trust

本来は「信頼の根幹」という意味。

Core Root of Trust for Measurement

- 起動後、もっとも最初に読み込まれ実行されるRoot of Trust
- 保存メディア
  - Fuse, ROM, Flash
- 保存されているソフトウェアの状態
  - 昔BIOS、今Microcode
  - BIOSはROMというよりも今はFlash（書き換え可能）
  - Microcodeも書き換え可能

- Static-CRTM (TPMベース。起動時に一度だけ計測する）
- Dynamic-CRTM（Microcode等。起動後にも計測できる）

Secure Boot/Trusted Boot/xxx Boot

- Secure Boot
  - ブート時にソフトウェアをチェック
  - ブート時に想定外のファームウェア・ソフトウェアがあった場合起動を止める
- Trusted Boot
  - ブート時にソフトウェアをチェック (Root Of Trust for Reportに保存)
  - ブートを最後までやり遂げる。
  - ブート時のチェック結果をまとめ、TPM内部の鍵で署名をつける。
  - 第３者にブート時のチェック結果を送信し判断を仰ぐ(Remote Attestation)
  - 受信者は「どの機器」で「想定したハッシュ値のソフトウェアが動作しているか」が判定できる。
- その他ブート(xxxBoot)の呼び名、機能や会社
  - Authenticate Boot
  - Verified Boot
  - Measured Boot

Remote Attestation

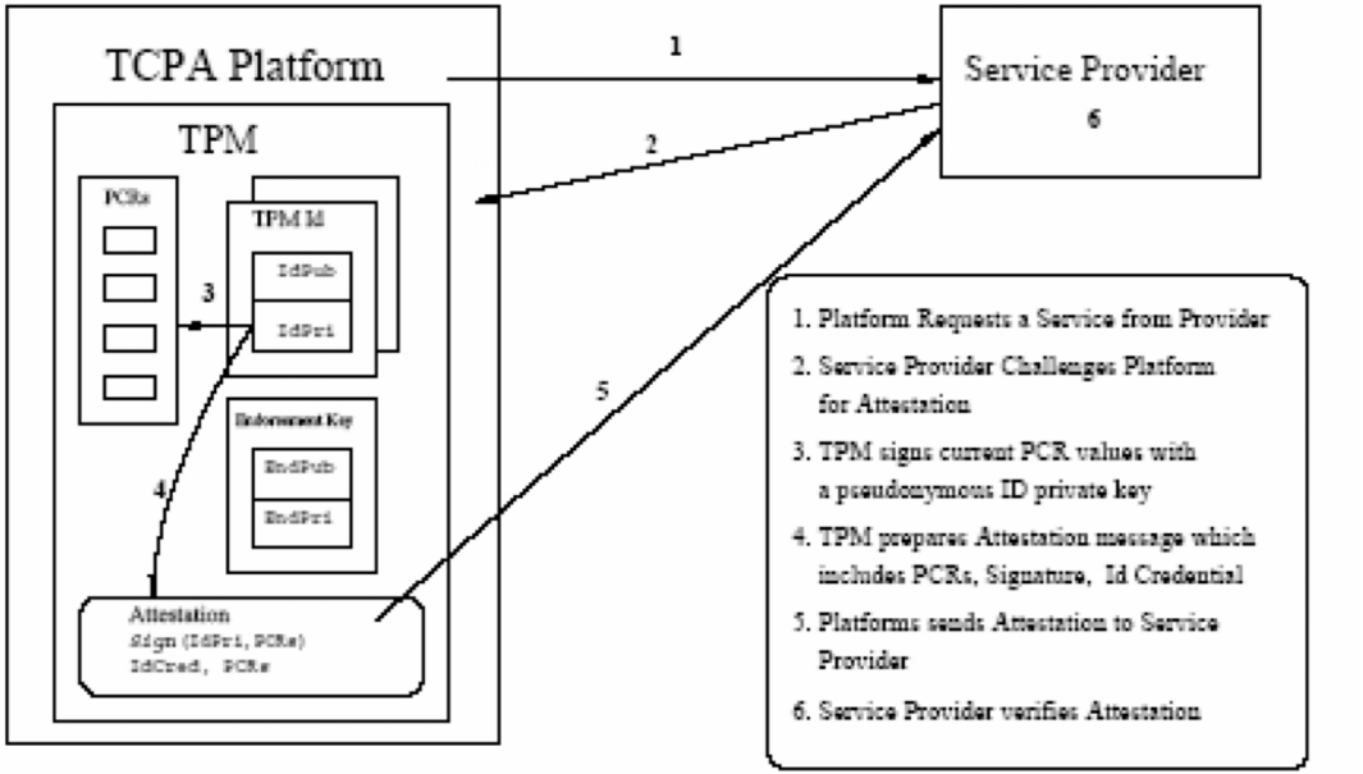


Figure 3 TCG Remote Attestation Protocol

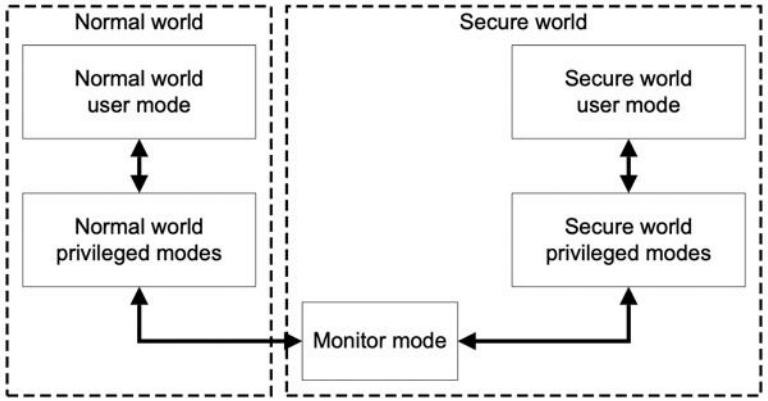
Reid, J., & Caelli, W. (2005). DRM, trusted computing and operating system architecture. In ACSW Frontiers 2005:

Trusted Computing BaseとRoot of Trust

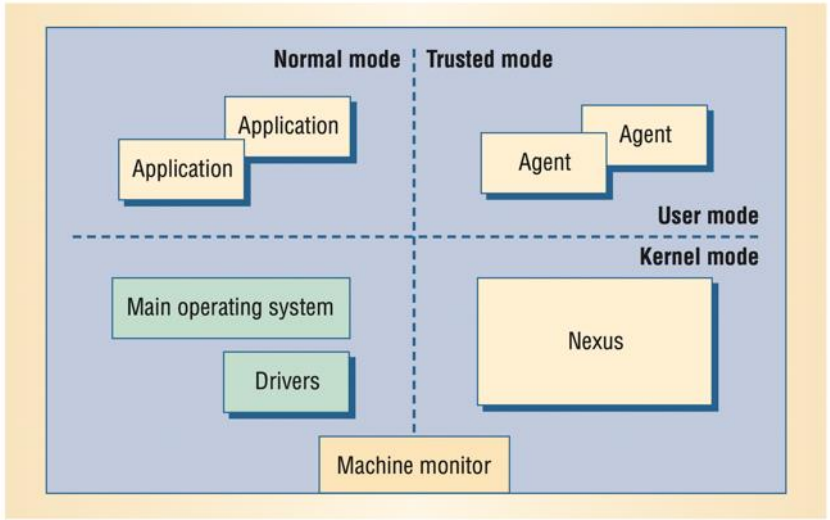
- Trusted Computing Base（TCB）
  - あるシステムのセキュリティを実現する基礎部分（１モジュールというわけではない）
  - TCBは、それ自体でセキュリティの機能を保護できる必要がある
  - TCBのセキュリティが破綻すればシステムのセキュリティも破綻してしまう

- Root Of Trust
  - TCBのソフトウェアを実現するための（完全性、認証、暗号化）の根幹となるモジュール
  - セキュリティが破られないという想定するモジュール。

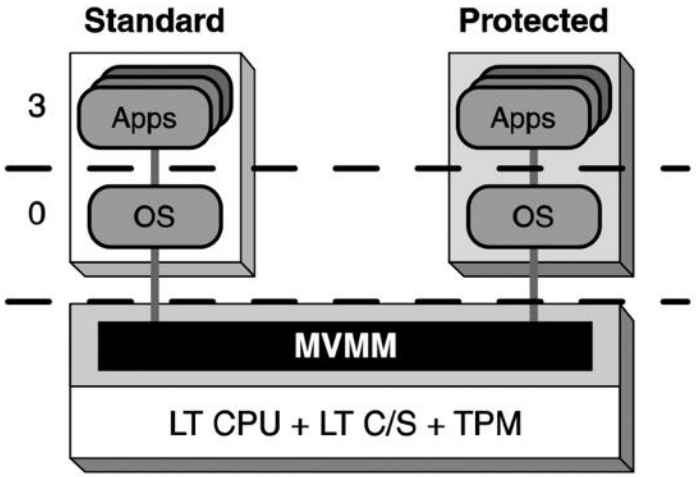
ベンダーのための完全な実行環境と
ユーザーのための自由な実行環境の両立の夢



ARM TrustZone (2003)[1]



Microsoft NGSCB(2002)[2]



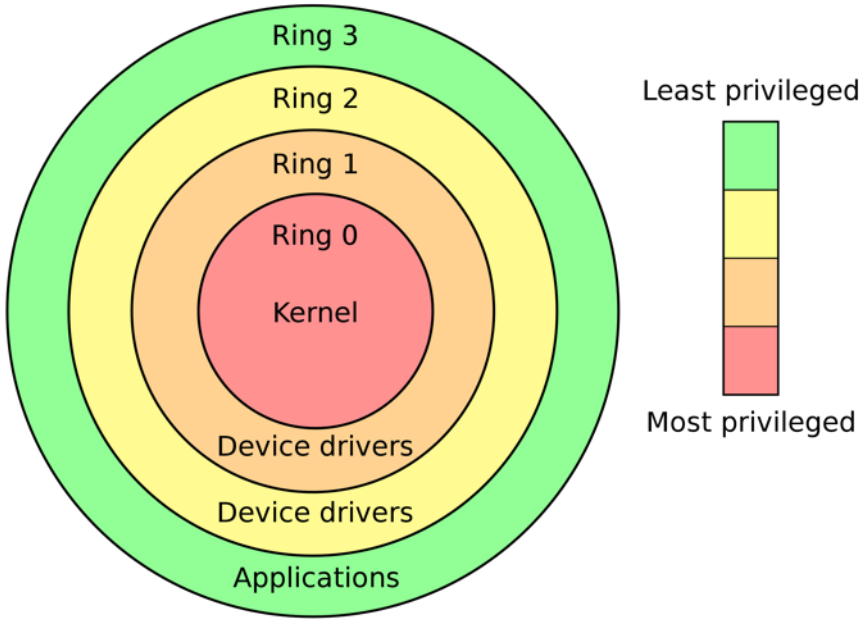
Intel LaGrande(2002)[3]

ベンダーのための完全な実行環境：出荷時からガチガチに完全性を保証できる実行環境
ユーザーのための自由な実行環境：どのようなOSでもアプリでもユーザーが好きなものを実行できる環境

[1] Holdings, A. R. M. (2009). ARM Security Technology: Building a Secure System using TrustZone Technology.
[2] England, P., Lampson, B., Manferdelli, J., & Willman, B. (2003). A trusted open platform. *Computer*, *36*(7), 55-62.
[3] Grawrock, D. (2005). The Intel Safer Computing Initiative.

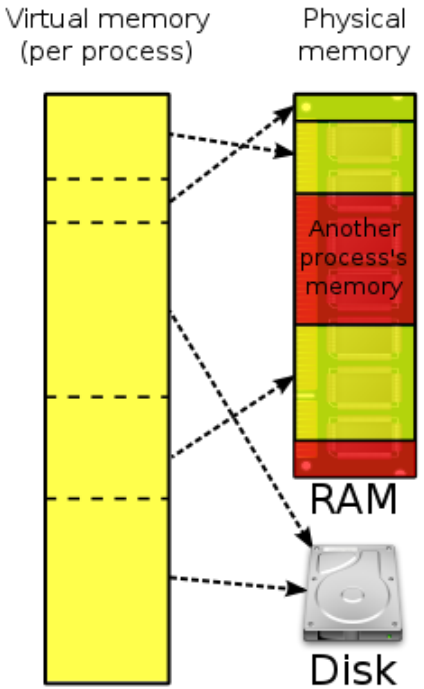
予備知識：CPUに備えるべき2大セキュリティ機構

- リングプロテクション（特権レベル、特権モード）



https://en.wikipedia.org/wiki/Protection_ring

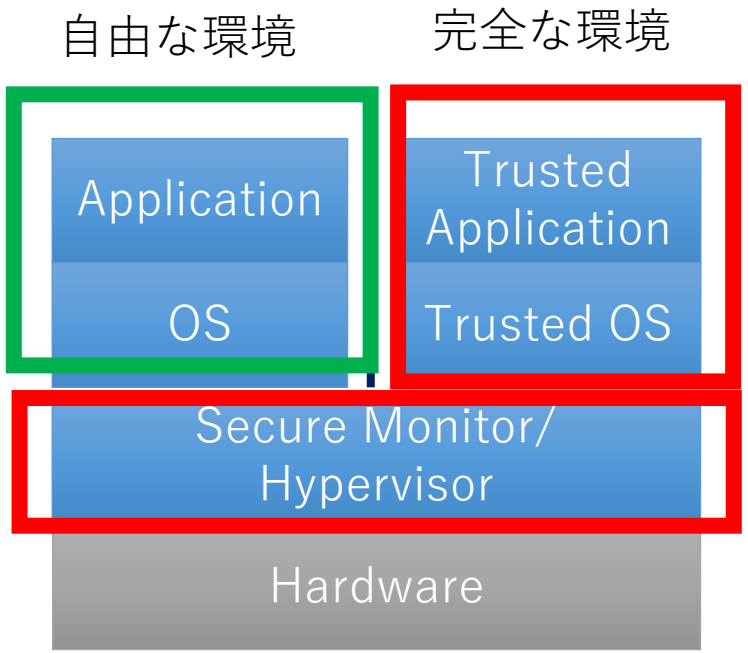
- メモリ保護機構（MMU/MPU/IOMMU）

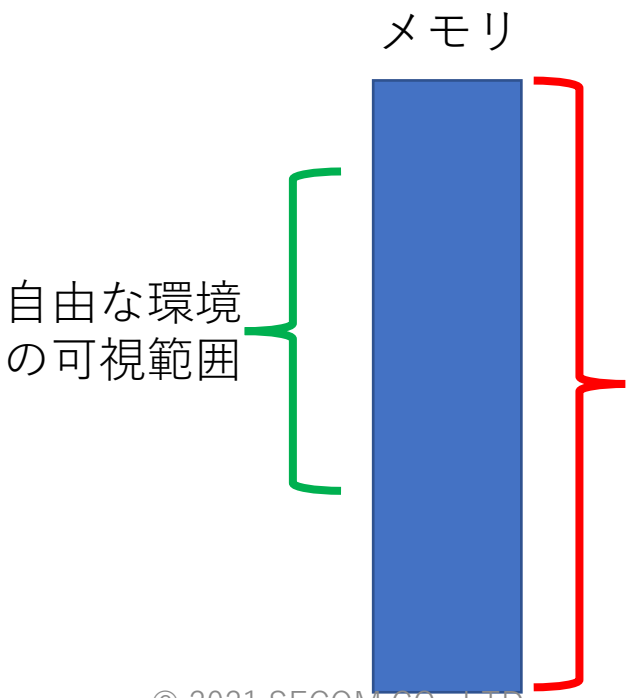


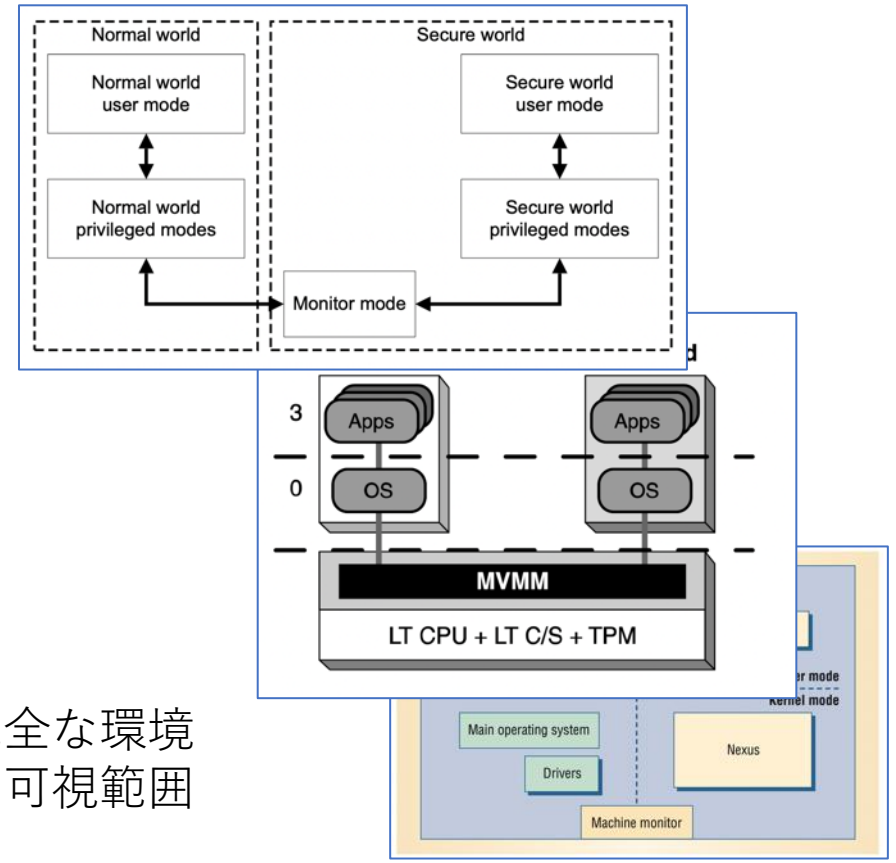
https://en.wikipedia.org/wiki/Virtual_memory

OSよりも強力な層を用意し、仮想化により2つの実行環境に分離する

弱 → 強
強
権限の強さ
（権限：命令数、メモリの可視範囲）

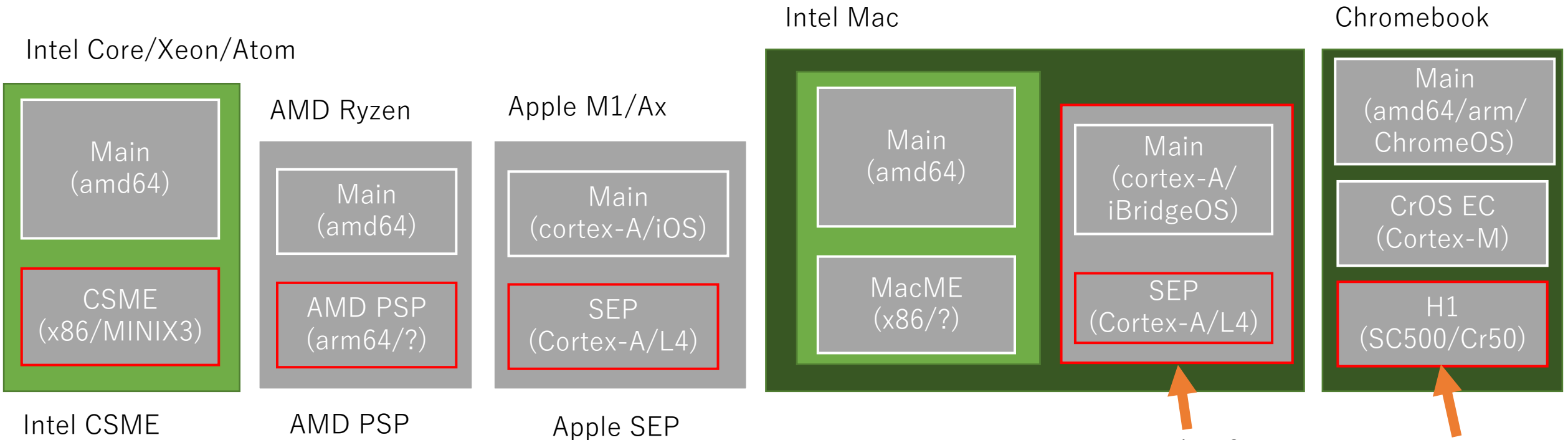






ARM:TrustZoneで実現
Wintel: Virtual Secure Modeで実現

メインCPUとは別のCPUを用意し独立した2つの実行環境に分離する



Intel CSME

Converged Security Management Engine

AMD PSP

Platform Security Processor

Apple SEP

Secure Enclave Processor

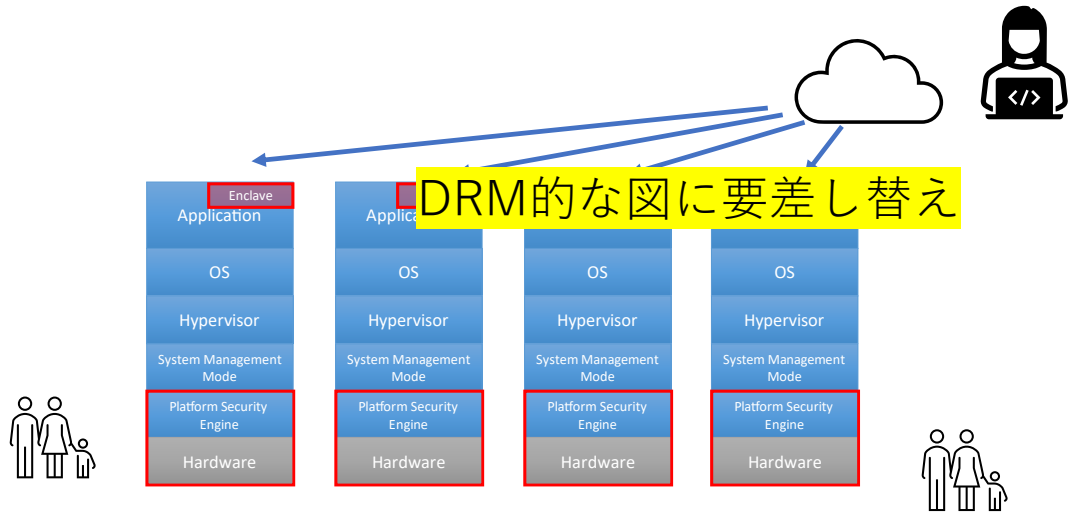
Apple T2

Touch?
Trust?

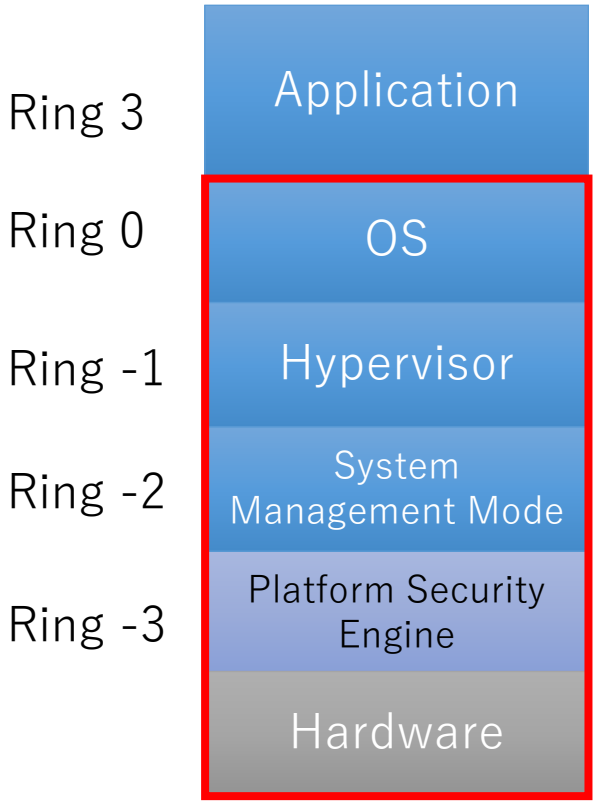
Google H1
後のTitan-m

なぜこのような技術に力が入れられてきたのか？

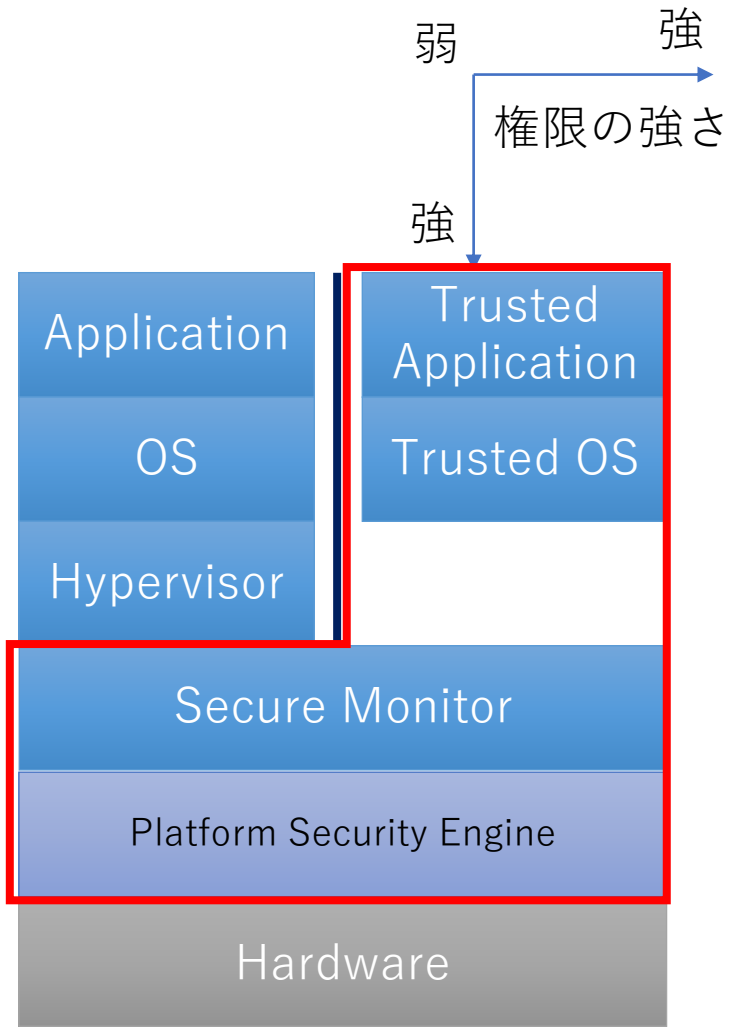
- **「私が作ったバイナリ」が「他人のPC」に入った時でも正当に使われたい要求**
- 1990年代半ばからのインターネットの爆発的な一般普及
  - データを世界へ拡散するコストの低下
  - メリット
    - 音楽、映画、アプリケーションのインターネット経由販売
  - デメリット
    - 違法コピーの氾濫
- 対策
  - PC出荷時から、ユーザーがチートできない（変更できない）エリアを作り分離。
  - チートのされていない、お金を払った人の機器であるのか確認してから再生できる仕組みを埋め込む（Remote Attestation）



技術的な整理



普通のPC



スマホ等
Arm TrustZone

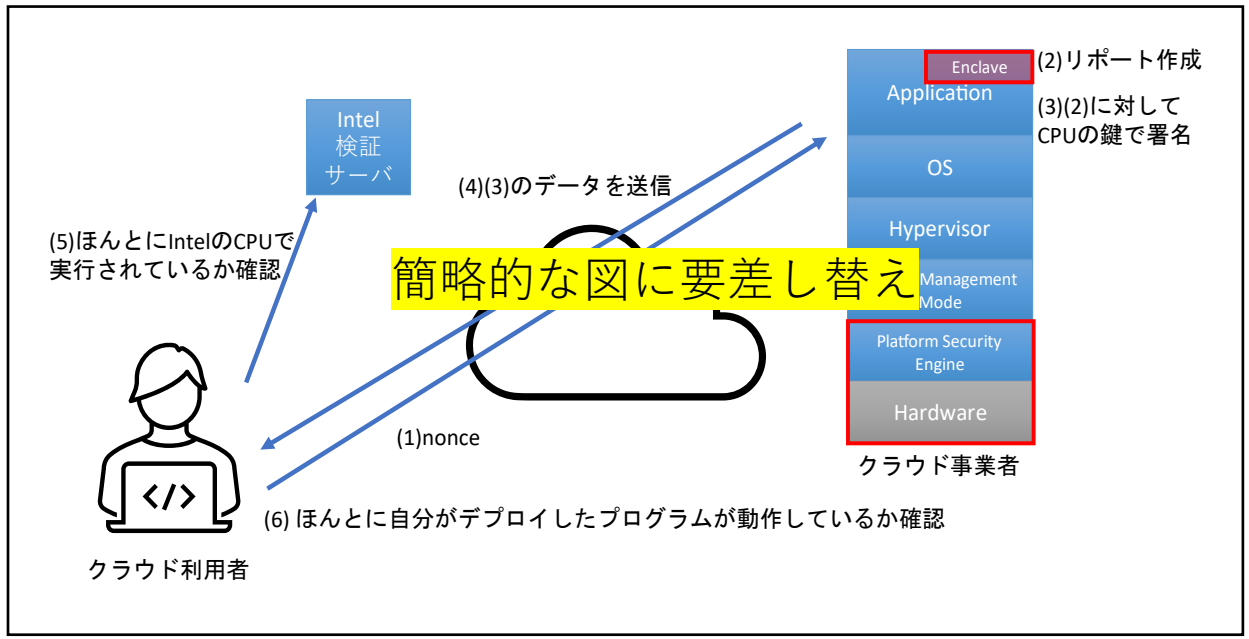
なぜこのような技術に力が入れられてきたのか？

- **「私が作ったバイナリ」が「他人のPC」に入った時でも正当に使われたい要求**
- ２０００年代後半からクラウドが注目される

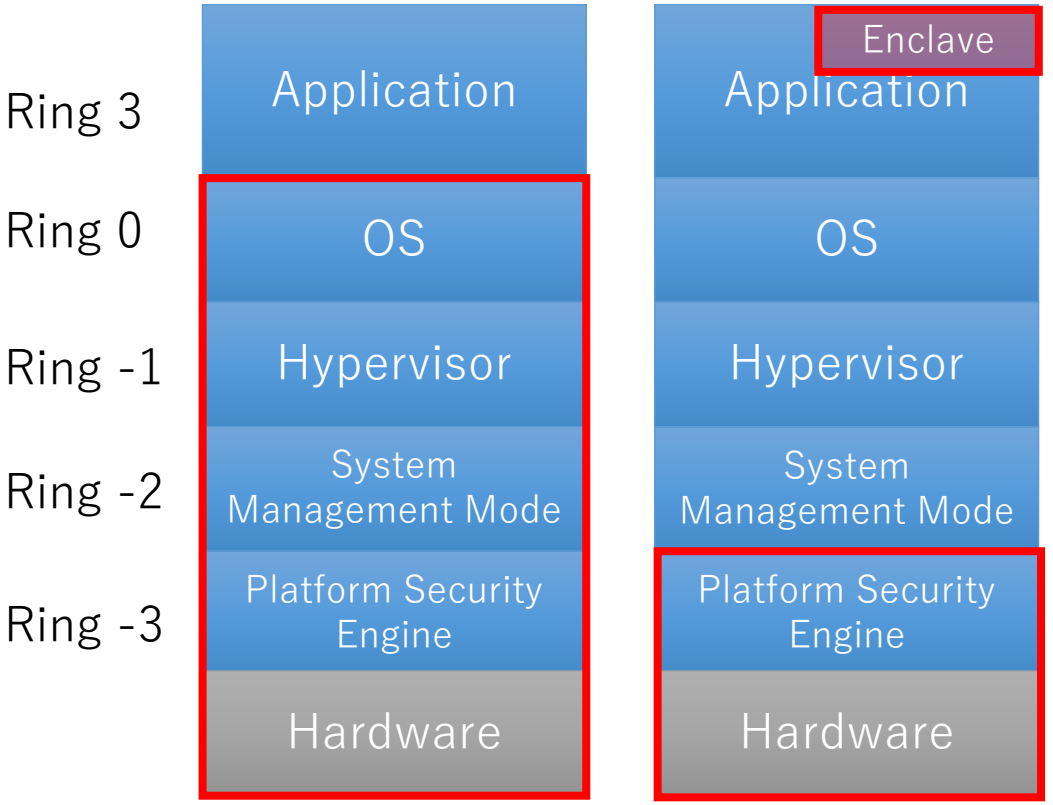
- 「クラウド利用者（WEBサービス開発者）が作ったWEBアプリケーション」が「クラウド」に入った時でも正当に使われたい要求

- クラウド事業者に処理内容を秘密にしつつ、計算資源だけ借用したい。

クラウド時代になり、同じ要求が注目される



信頼の階層を打ち壊した Intel SGX



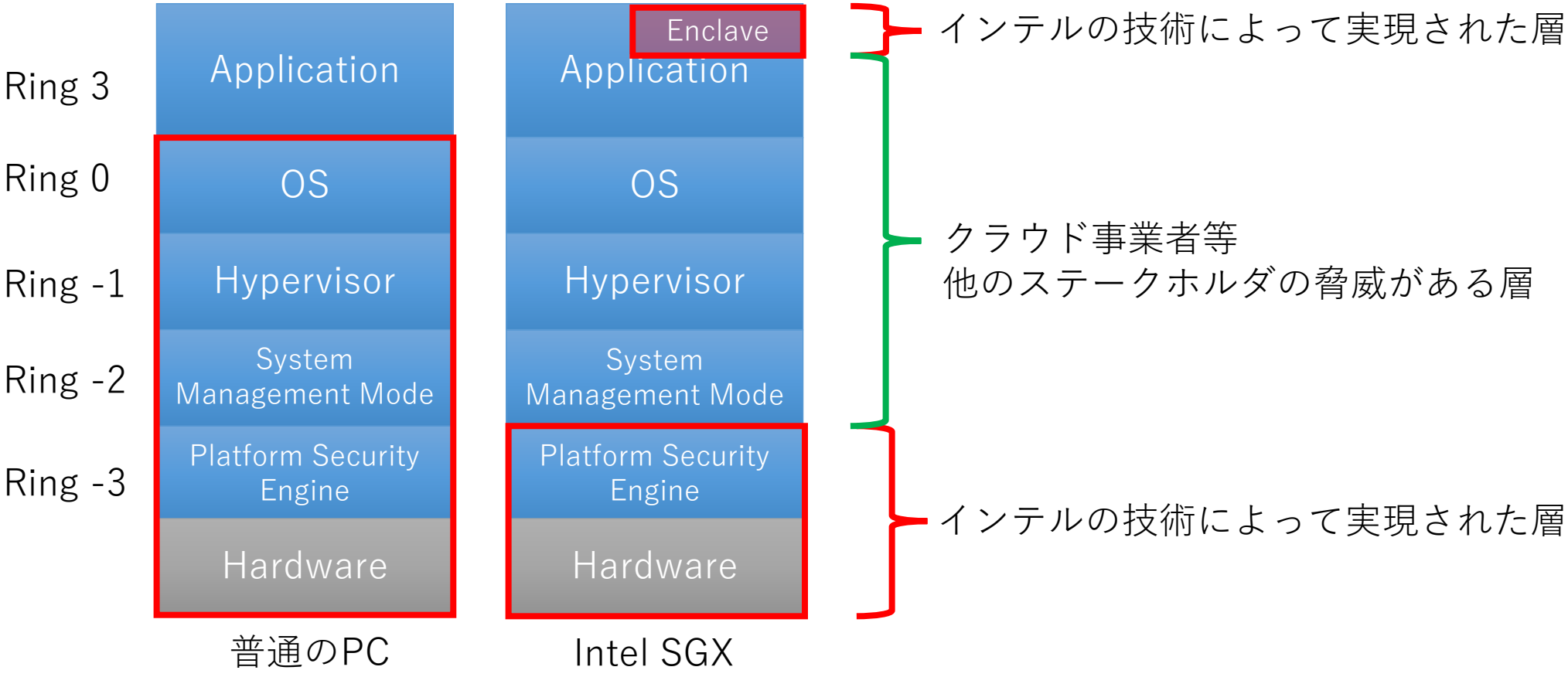
普通のPC　　Intel SGX

※赤枠はTCB

Enclave (飛び地)

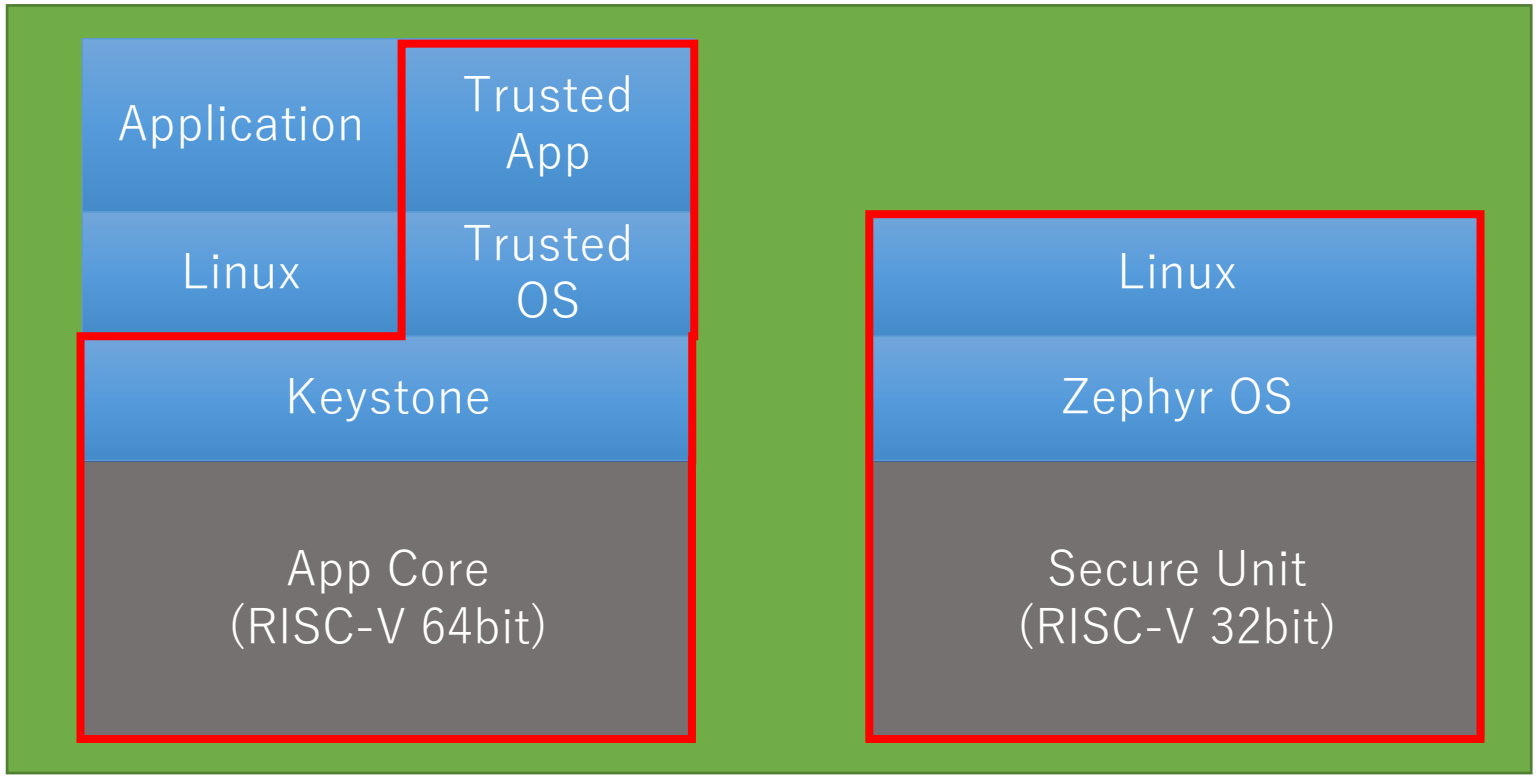
"Locator map of municipalities of East Timor"© J. Patrick Fischer (Licensed under CC BY 4.0)

信頼の階層構造を打ち壊した Intel SGX



※赤枠はTCB

宣伝：
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



まとめ

- ICカードなど古くからセキュアなチップの実現に研究開発されてきた
- チップ単体だけでなく、PC（基盤全体のハードウェアファームウェア、HDDに格納された基盤上で動くソフトウェア）についても完全性を実現するための技術が研究されてきた。
- 完全な状態を実現するだけでなく、遠隔から確認できることが重要
  - DRMの文脈：コンテンツ提供者が、適切なコンテンツ再生環境なのか確認してから、再生許可したい。復号処理をみられたくない。
  - クラウドの文脈：WEBアプリ開発者が、適切なクラウド実行環境なのか確認してから、実行許可したい。実行処理をみられたくない。