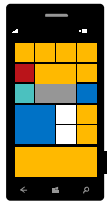
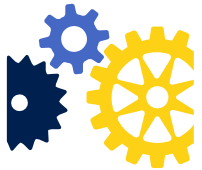
Microsoft

プラットフォームで実装されるトラスト

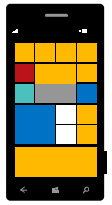
垣内 由梨香
Security Program Manager
Security Response Team
Microsoft Corporation
CISSP

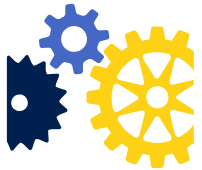
プラットフォームが「トラスト(信頼)」されるためには

プラットフォームが「トラスト(信頼)」されるためには

本セッションでは

マイクロソフトがプラットフォームを提供する立場として、
どのような問題を経験し、どのように解決しようとしてきたのか
を紹介することで、デジタルトラストに対応するコンピュータアーキテクチャの変化についての議論したい。

プラットフォームを「トラスト」するために求められていること








従来のセキュリティ境界の定義

Ten Immutable Laws Of Security (Version 2.0)

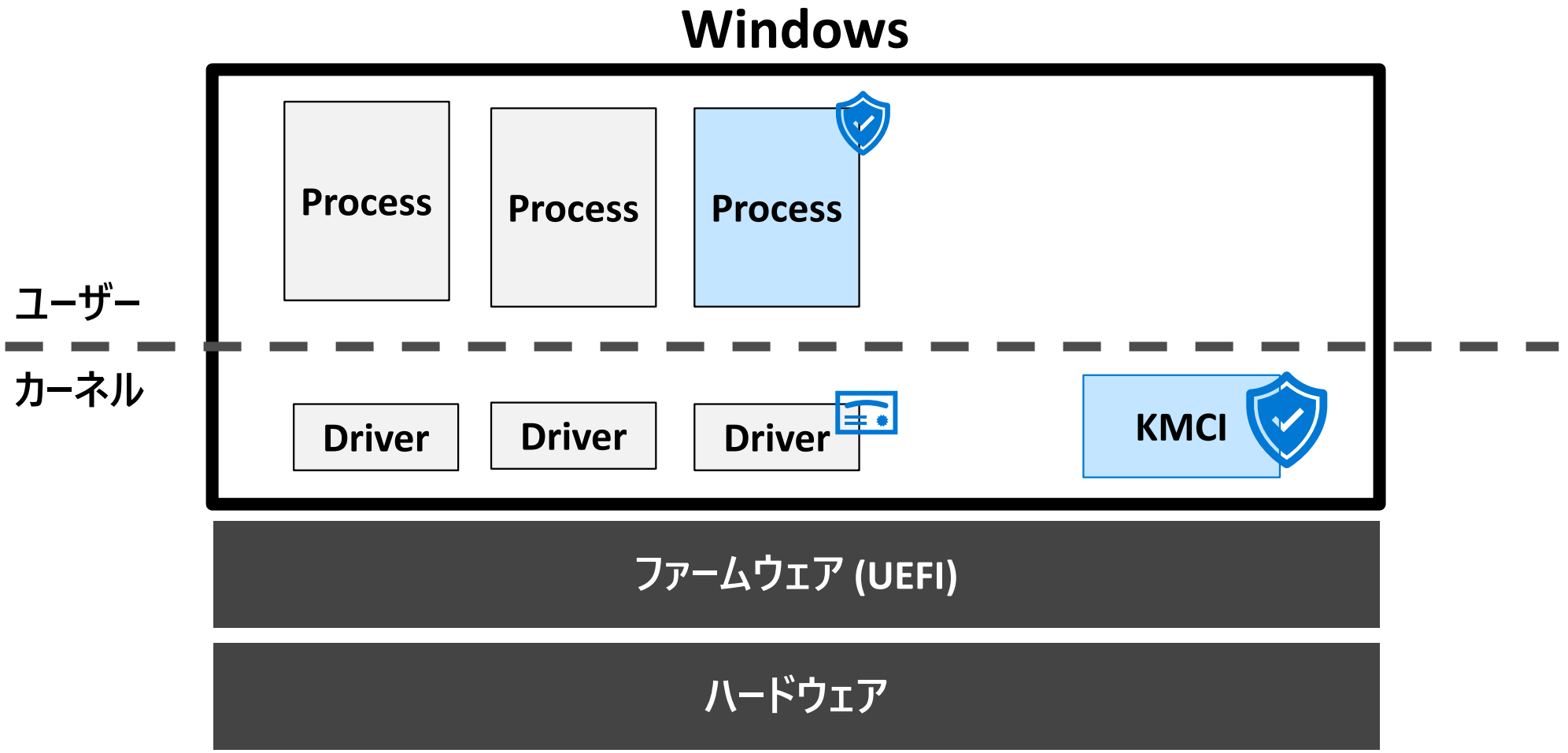
06/16/2011 • 2 minutes to read

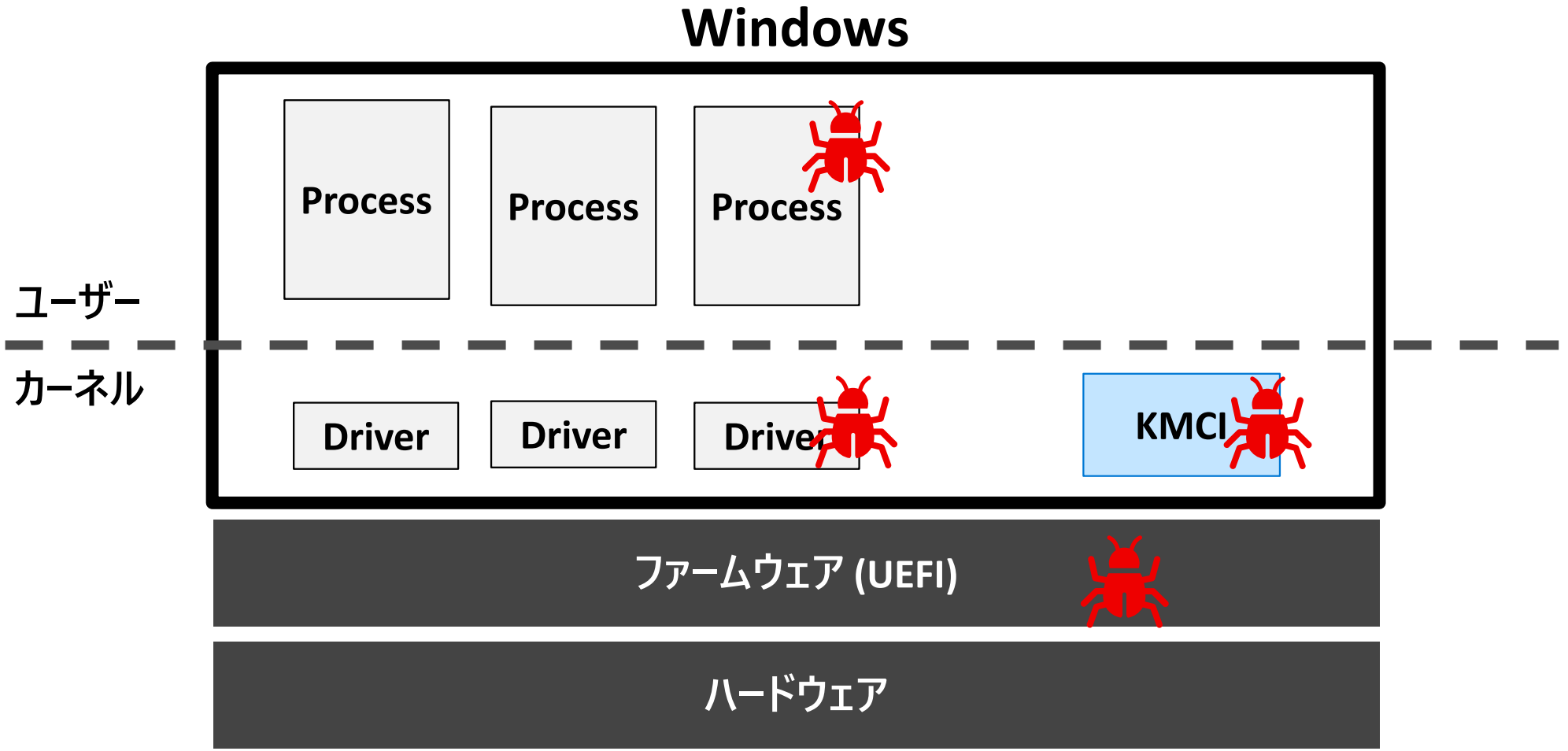
You might have known the 10 Immutable Laws Of Security since quite a while. It is kind of the "collected non-technical wisdom" of what we see in security respeonse being it in Microsoft Security Response Center or in our Security Product Support.

There is now a version 2, which is still as important as version 1 was. The 10 Laws are:

> Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
> Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.
> Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
> Law #4: If you allow a bad guy to run active content in your website, it's not your website any more.
> Law #5: Weak passwords trump strong security.
> Law #6: A computer is only as secure as the administrator is trustworthy.
> Law #7: Encrypted data is only as secure as its decryption key.
> Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all.
> Law #9: Absolute anonymity isn't practically achievable, online or offline.
> Law #10: Technology is not a panacea.

[Archive] Ten Immutable Laws Of Security (Version 2.0)
https://docs.microsoft.com/en-us/archive/blogs/rhalbheer/ten-immutable-laws-of-security-version-2-0





システム侵害の現実

5倍
過去4年間におけるファームウェアの脆弱性

36%
Hardware ベースのメモリプロテクションの利用。46% カーネルプロテクション利用

23%
フィッシングのメール開封率
(11% 添付クリック)

デバイスは、攻撃者の手にさらされていないのか？

起動されたWindows は本物なのか？

正規のドライバが実行されているのか？

「管理者」ユーザーは、意図した本人なのか？

新たなセキュリテの境界の定義

すべてのコードは整合性を持って実行される

ユーザーのアイデンティティは、侵害、なりすし、盗難されない

簡易的な物理アクセスを持つ攻撃者は、デバイス上のデータやコードを変更できない

悪意のあるコードがデバイス上に留まらない

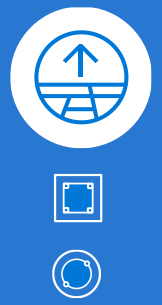
セキュリティ前提の違反が観測可能

すべてのアプリとシステムコンポーネントは最小権限を持つ

セキュアなデバイスに必要な 7 要素

Hardware Root of Trust

デバイスのIDとソフトウェアの完全性がハードウェアによってセキュリティ保護されているか？



Defense in Depth

セキュリティ メカニズムが破られてもデバイスは保護されるか？

Small Trusted Computing Base

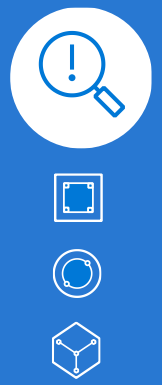
デバイスのTCBは他のコードのバグから保護されているか？

Dynamic Compartments

デバイスのセキュリティ保護をデプロイ後に改善できるか？

Certificate-Based Authentication

デバイスの認証にパスワードではなく、証明書を使用しているか？



Failure Reporting

デバイスは障害や異常を報告するか？

Renewable Security

デバイスのソフトウェアは自動的にアップデートされるか？

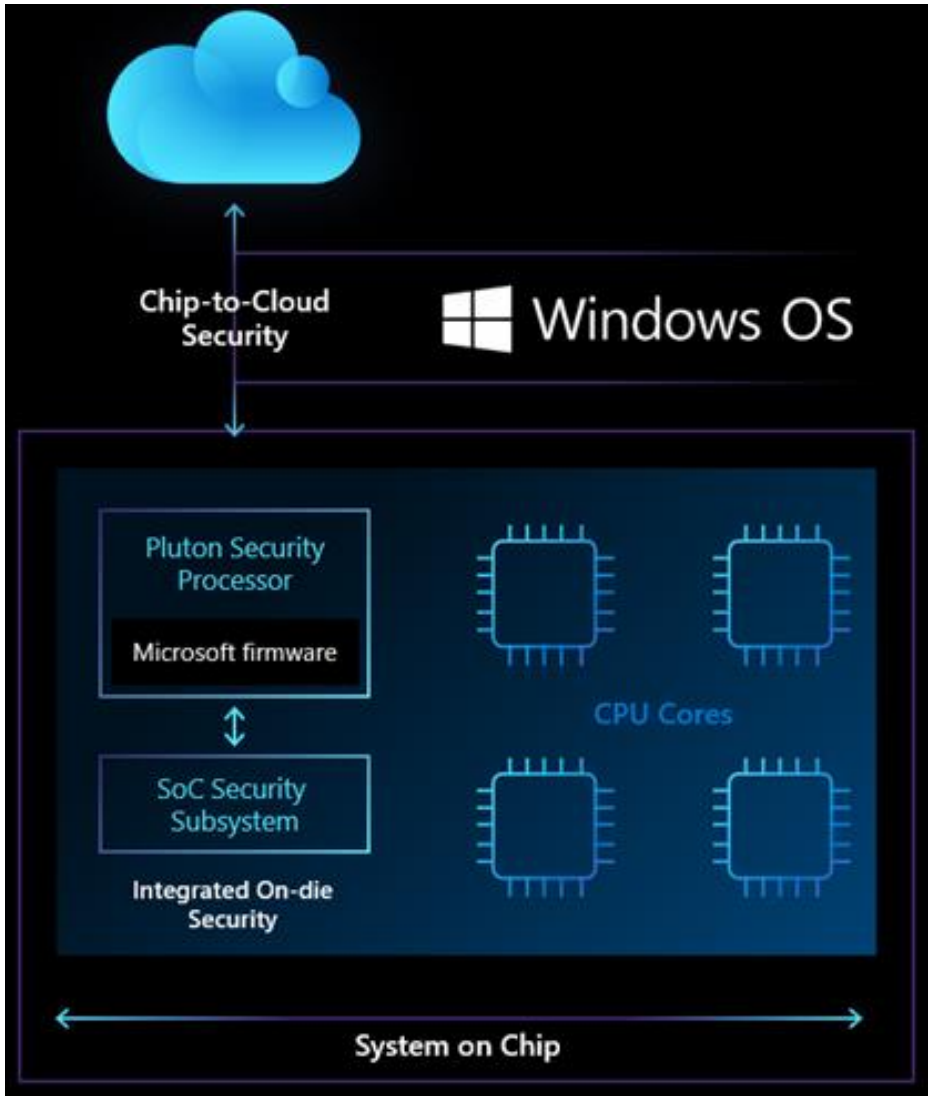
 = シリコンのサポートが必要  = OSのサポートが必要  = クラウド サービスのサポートが必要

チップからクラウドまで

内蔵されたセキュリティ、ハードウェアベースのアイソレーションで保護を強化と暗号化することで、攻撃者が隠れることが格段に難しくなります。

- ハードウェアルートオブトラストによる保護
- ファームウェアレベルの攻撃からの保護
- 検証されていないコードへのアクセスを防止
- 外部の脅威からのアイデンティティの保護
- Pluton support*

Microsoft Pluton on PCs

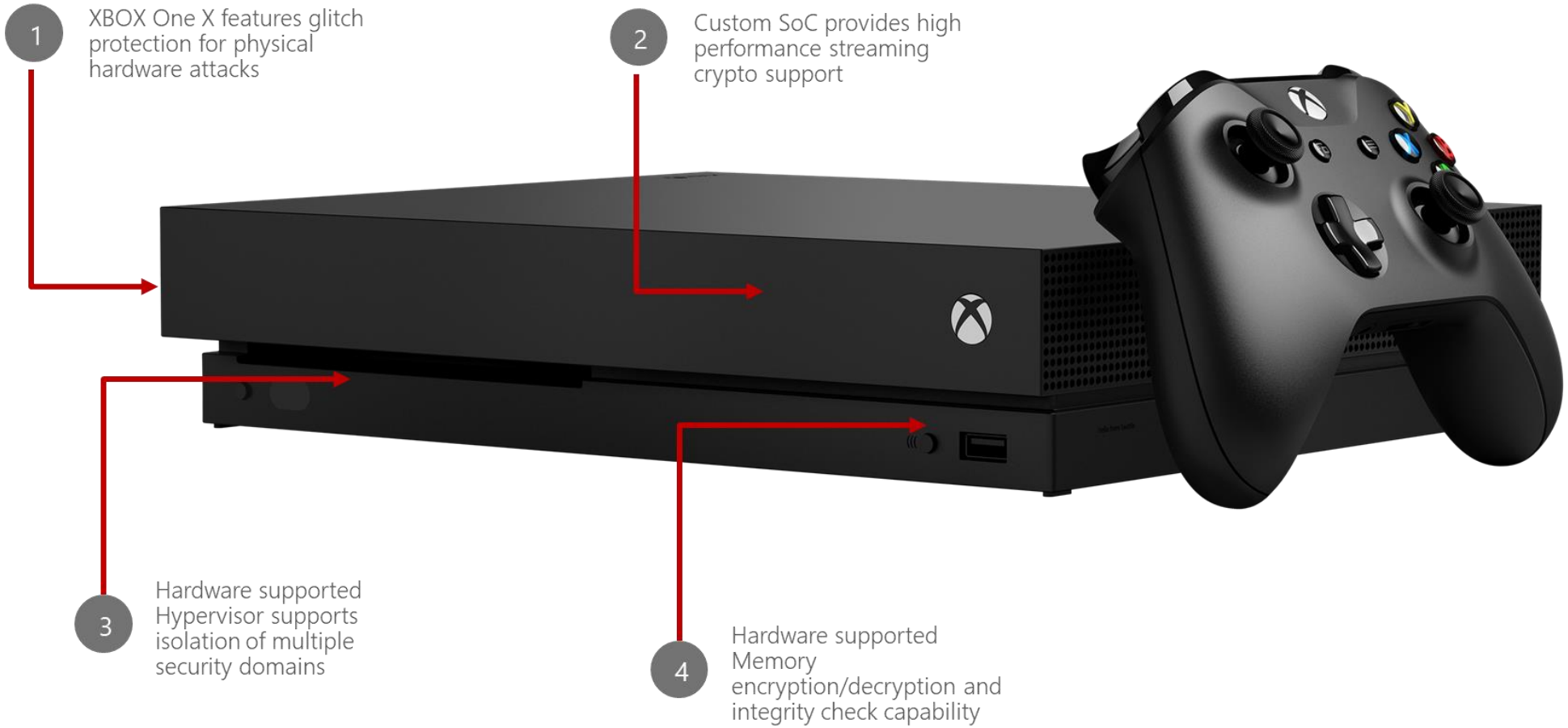


AMD、Intel、Qualcomm Technologies, Inc. という主要シリコンパートナーとの協力し

Plutonを搭載したPCの提供

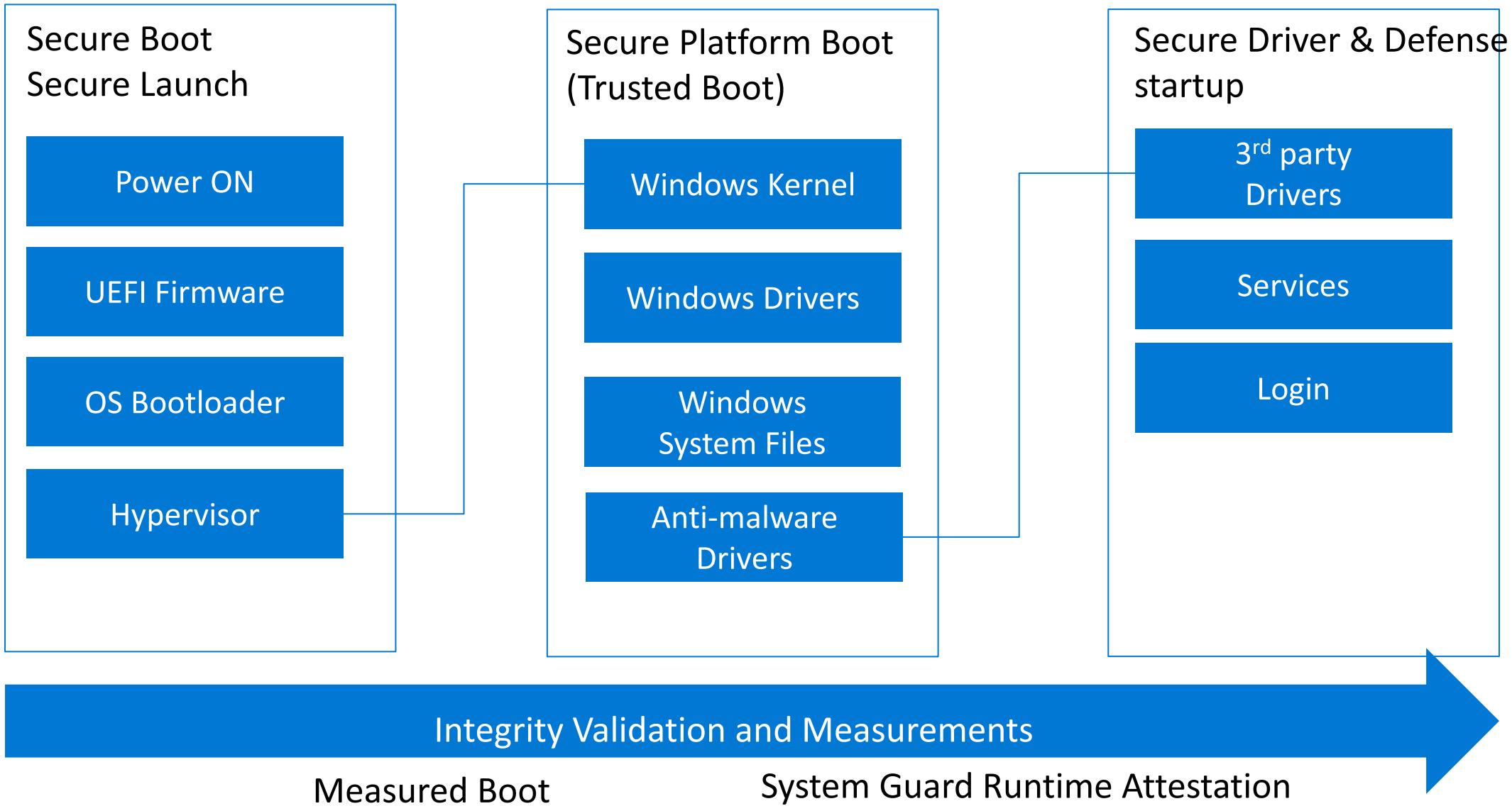
[Microsoft Pluton Processor のご紹介 – Windows PC の未来に向けて 設計されたセキュリティチップ]

実は、旅路はここから始まっていた…



信頼のできるコンピューティングを起動する

ブート時の保護 in Windows 概要



Secure Boot

Windows 8 以降

SRTM

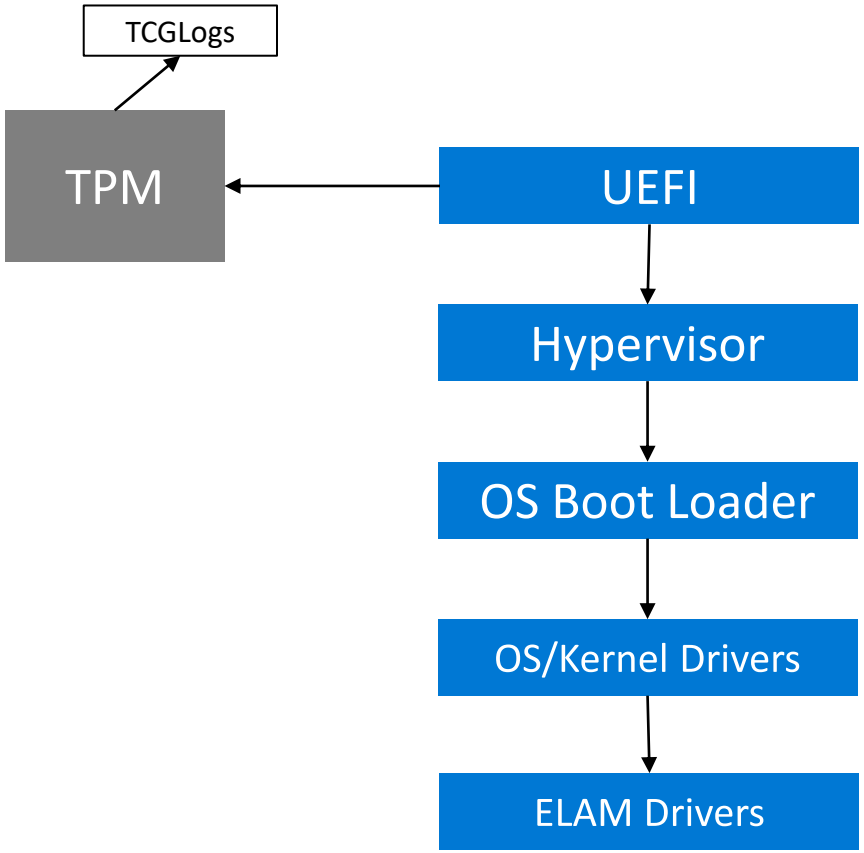
各ブートのコンポーネントを順次検証

OEMが製造時に NV-RAM に検証のためのデータを格納、signature database db, revoked signature database dbx, Key Enrollment database KEK, platform key (PK).

Microsoft KEK

UEFI ファームウェアへの信頼が低下

[FEFI rootkit (Lojax) reported by ESET]



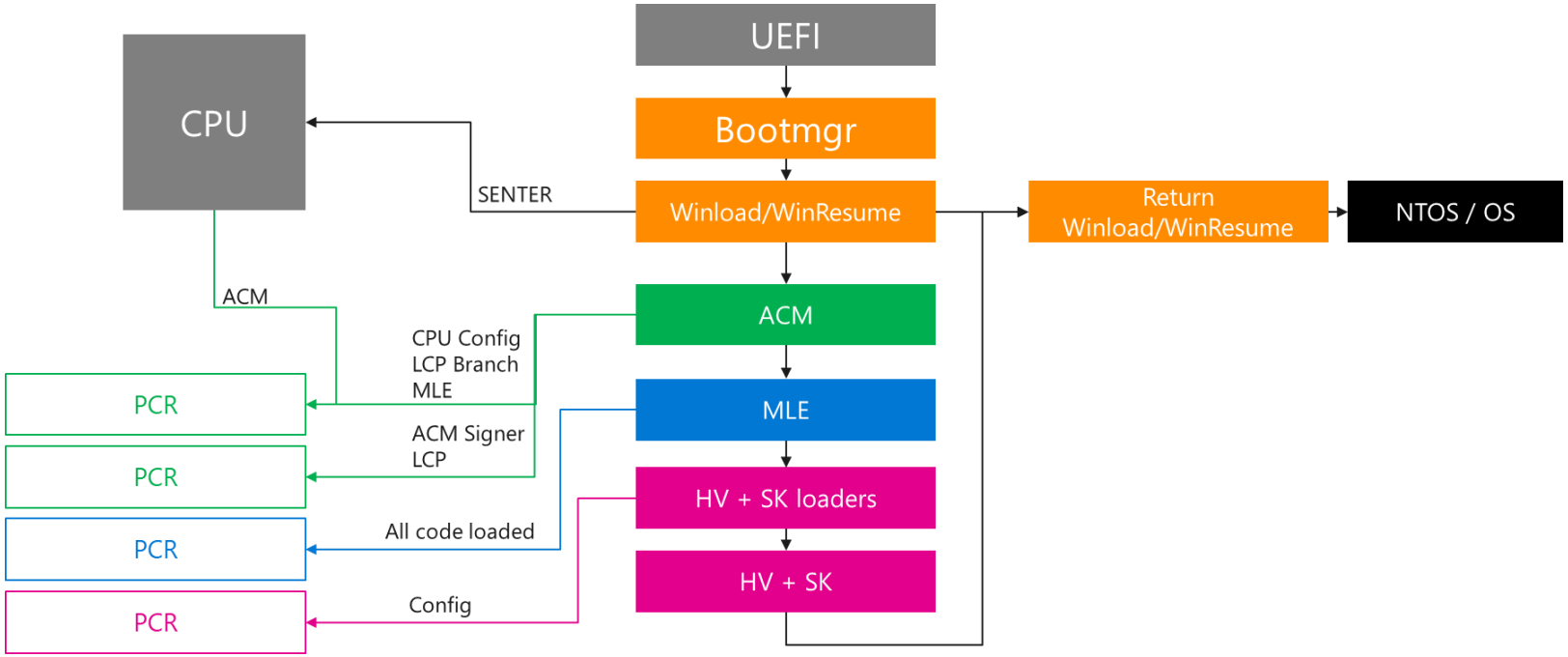
Secure Launch (Windows 10 1809+)

DRTM, (Intel TXT, AMD, Qualcomm)

UEFI への侵害を前提に、UEFIに依存しない安全なブート

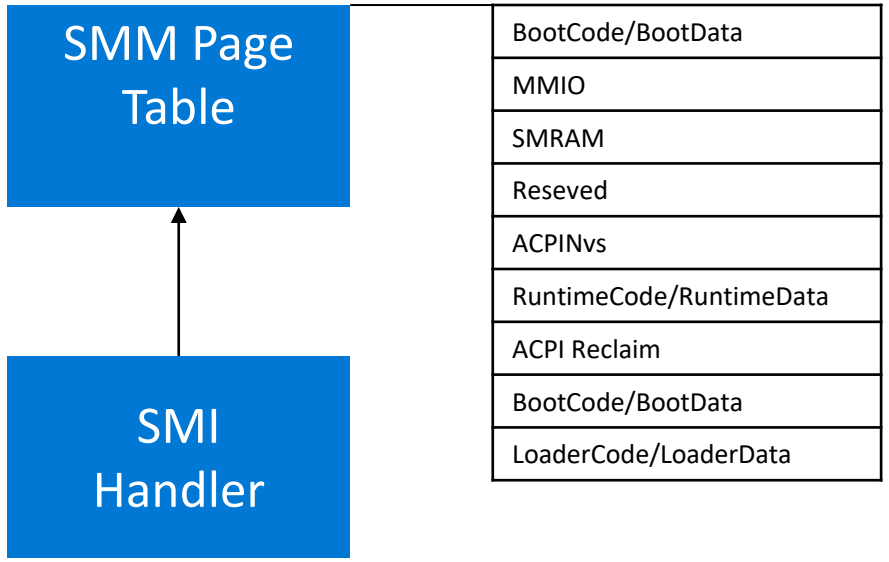
動的に Root of trust measurement を実行

Code integrity Policy, Hypervisor, kernel hashes, UEFI Vars, etc…



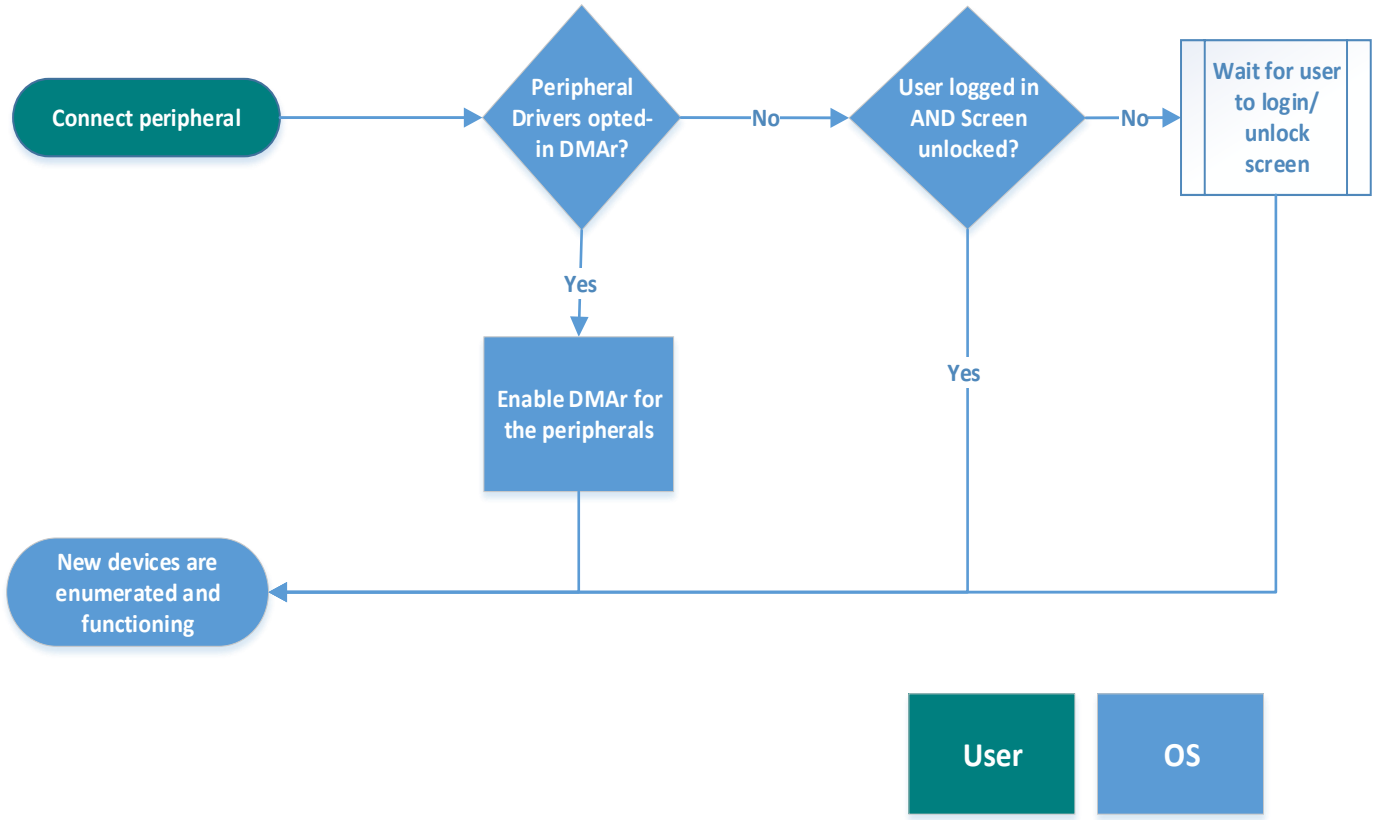
System Management Mode (SMM) protection

- SMMによるリスク
  - 高い特権 (ring-2) で実行され、OSには見えない
  - Secure Launch やVBS のバイパスのリスクがある
- Intel Runtime BIOS Resilience を活用した保護
  - Paging Protection
    - SMM エントリーポイント、メモリマップ、ページプロパティのロックダウン
    - OS/HV メモリへのアクセスを防止
  - SMM hardware supervision and attestation
- Microsoft SMM Paging Audit



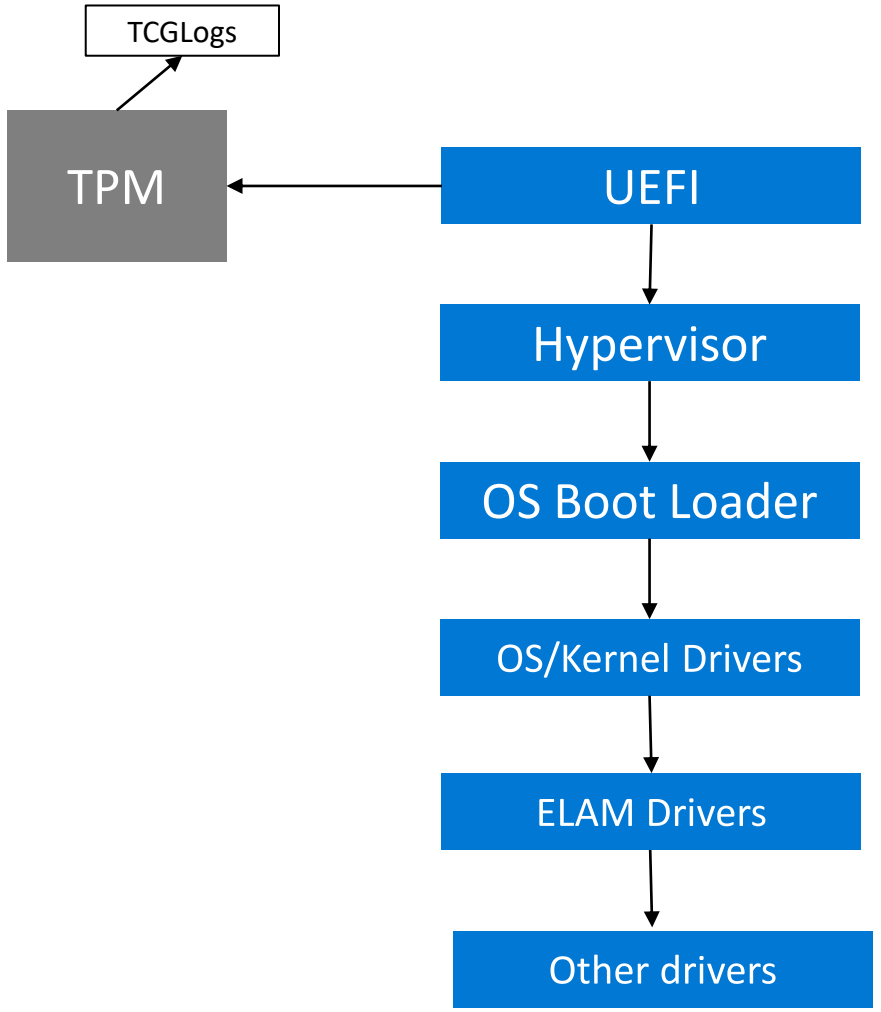
Windows DMA-r Attack Protection (Windows 1809+)

- DMAを介した攻撃からの防御
- IOMMU を利用
- 新たに接続された Thunderbolt™ 3 デバイスをユーザーがログインしロック解除するまで、ブロック
- ブート時のIOMMU (See Project Mu)



Early Launch Anti-Malware (ELAM)

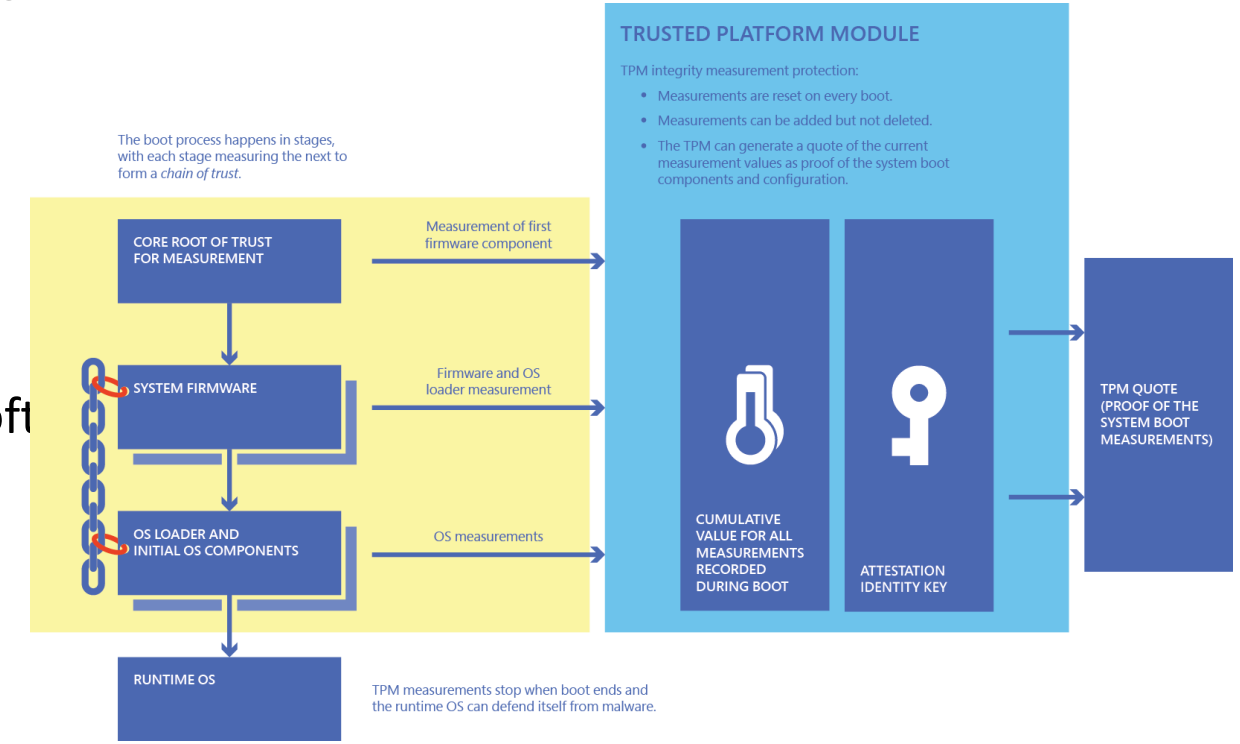
- マイクロソフトが認定する特定のAVドライバ
  - Microsoft Virus Initiative (MVI)
  - Windows Hardware Quality Lab (WHQL) signed
- 他の3rd Party カーネルドライバよりも先に起動
- ELAMが他のドライバを検証しカーネルがロード・初期化判断



Measured Boot

- UEFIを使ってファームウェアやブートローダ、ブートドライバなどのハッシュを記録
- そしてスタートアッププロセスの最後に、アテステーションサーバ（検証サーバ）でブートの正当性の検証を行う

- [TPM Platform Crypto-Provider Toolkit](#) from Microsoft Research
- Microsoft Enterprise Security MVP Dan Griffin's [Measured Boot Tool](#).



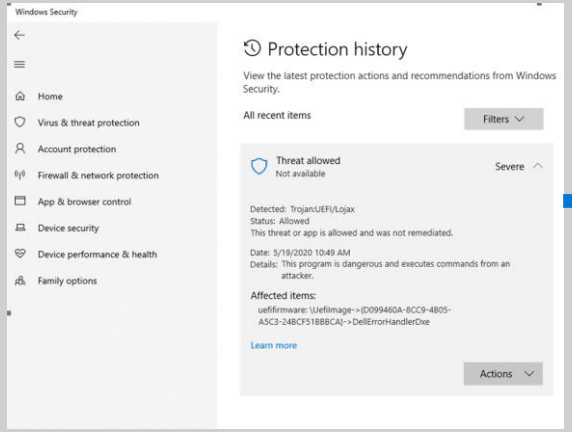
UEFI Scanner

- SPI Flash のファームウェアを読み出し、スキャンする
- EPP Scanner:
  - 悪意のあるマルウェアの検出
  - 例: **Lojax DXE driver**
- EDR Anomaly detector
  - EDR にテレメトリを提供する
  - アノマリ検出を実行しMDATP ポータルにアラートを出す

- Chipset Configuration Assessment
  - Chipsetの構成をチェック

EPP Scanner

EPP detection



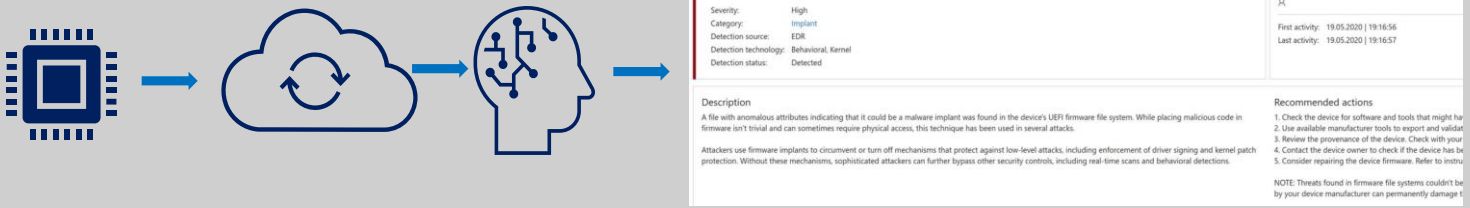
alert

EDR – Anomaly detector

Telemetry sent to EDR backend

ML model

alert

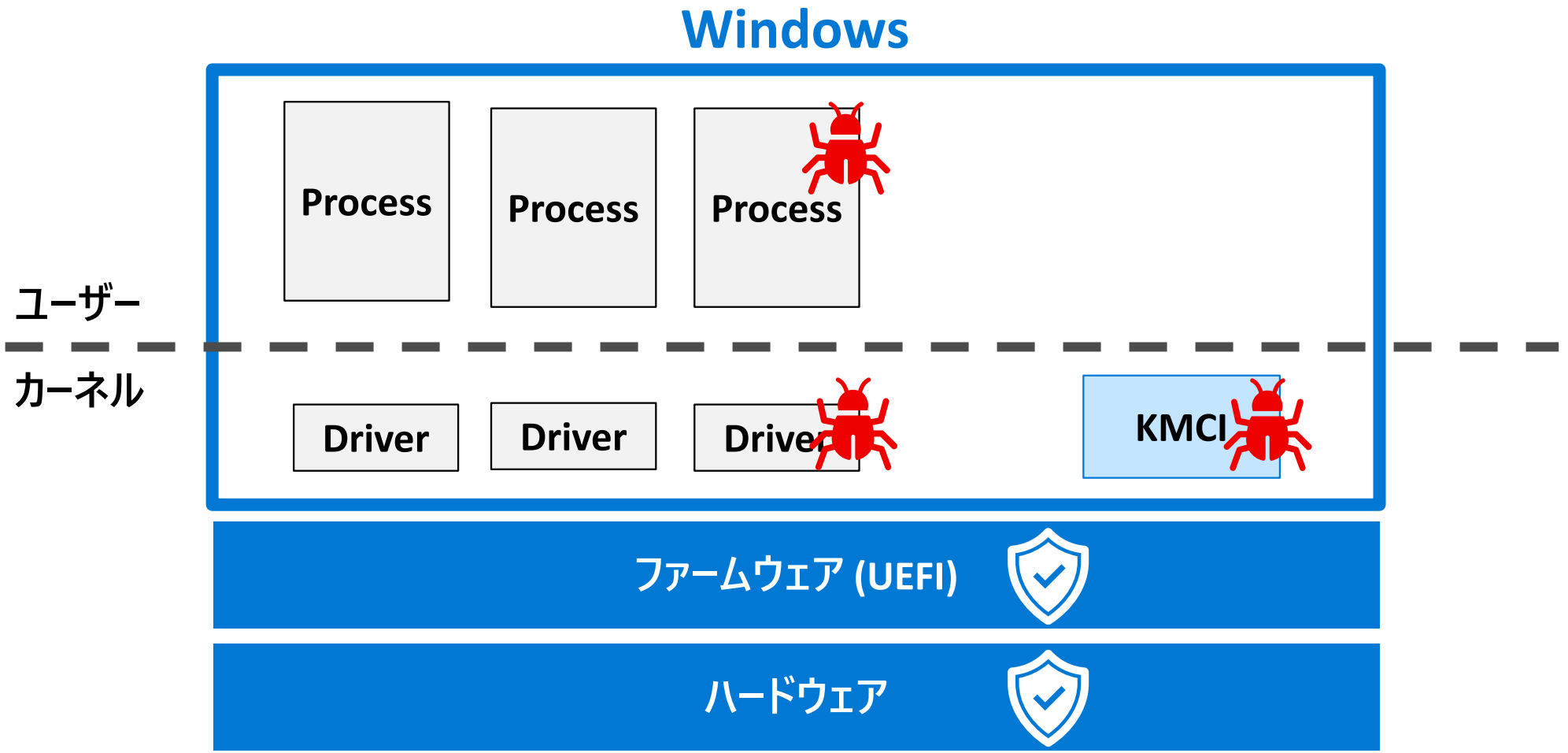


信頼のできる
実行環境を提供する



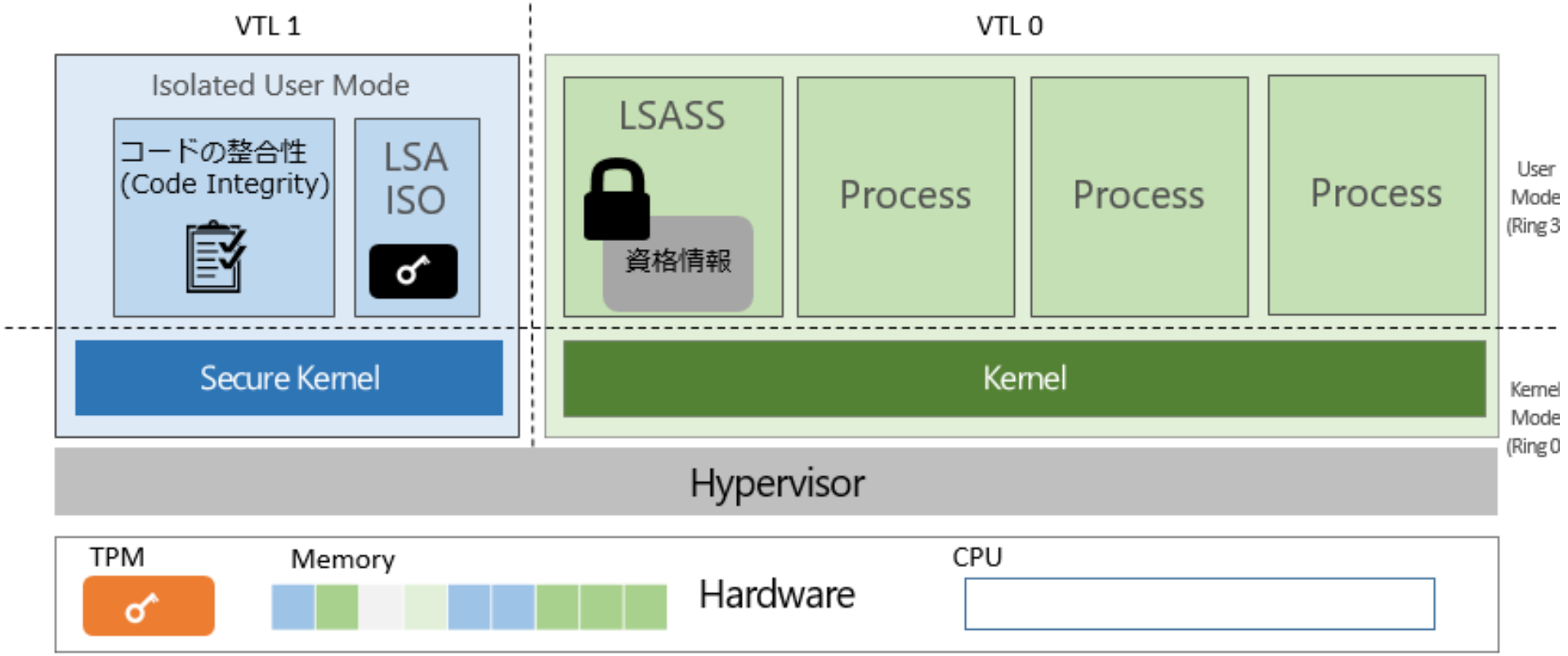




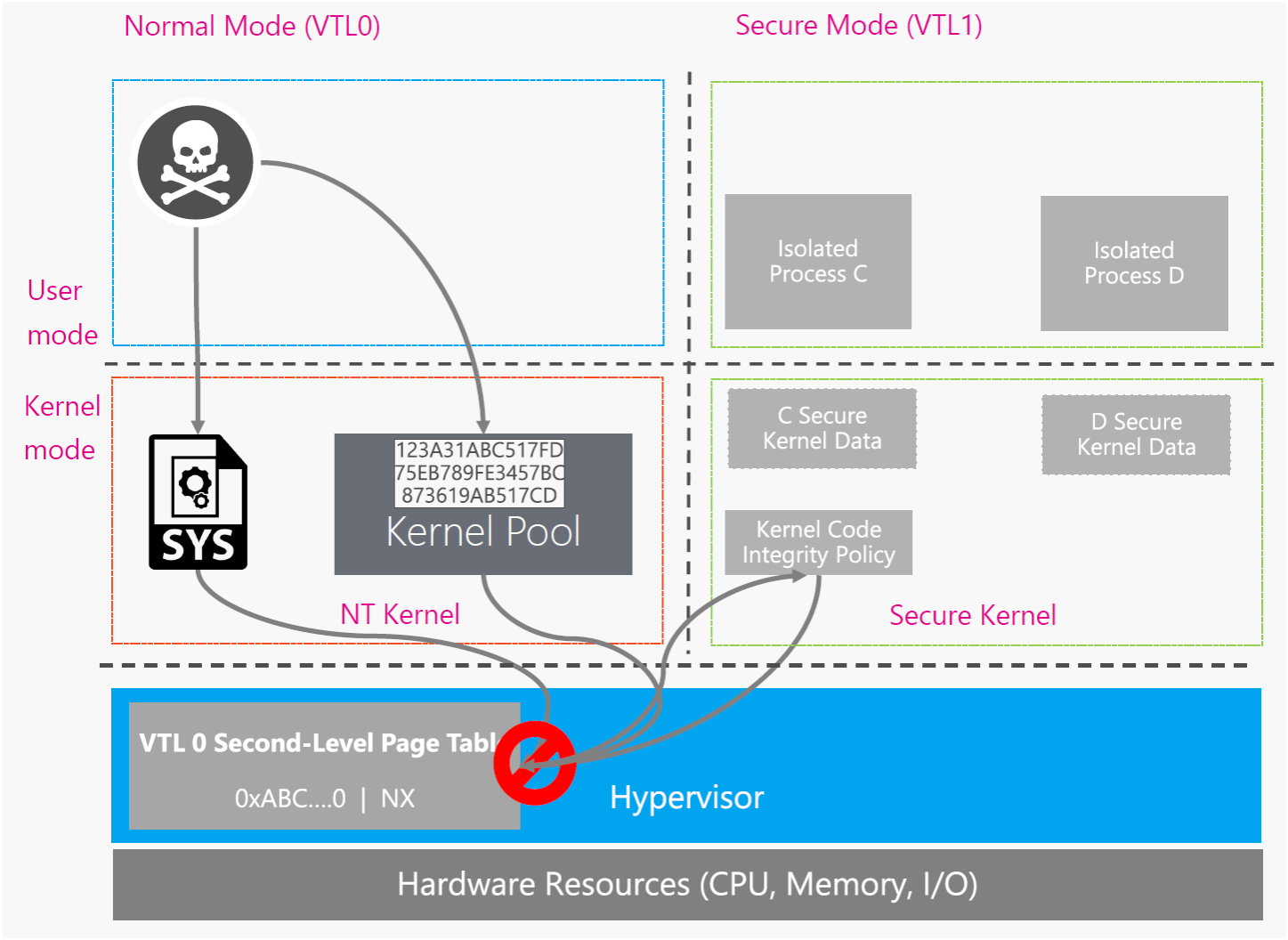
Virtualization-based security (VBS)

- Windows 10+ の多くのセキュリティ機能の基礎
- Hypervisor, SLAT, IOMMUをベースとした仮想化による保護技術



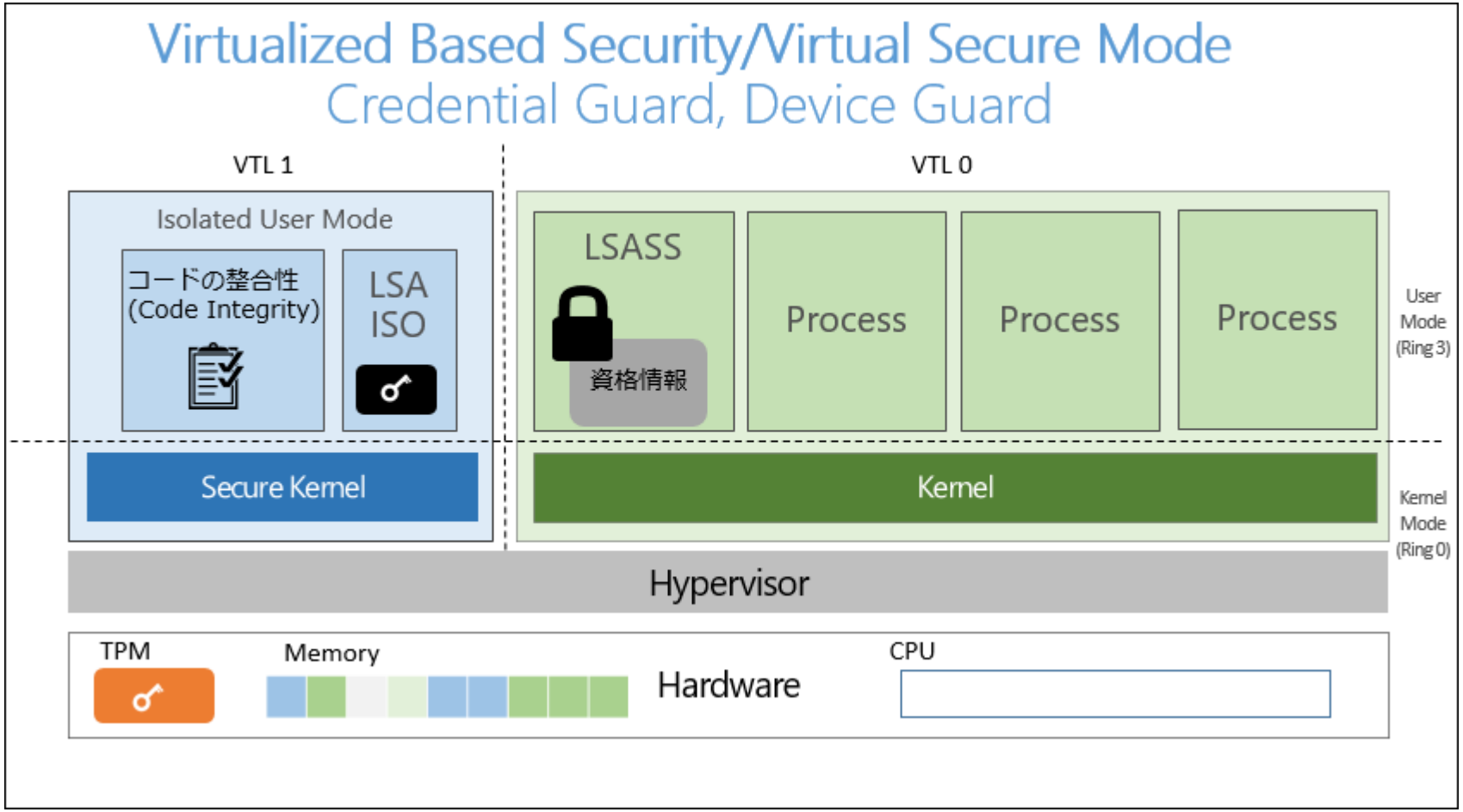
Hypervisor-protected Code Integrity (HVCI)

- Virtualization based Security を利用したカーネルドライバのコード整合性
  - SLAT を利用したメモリ管理
  - 整合性チェックをVTL1で実行
  - アサインされたメモリはRX only
- Mode-Based Execute (MBE) control
  - Extended Page Tables (EPT)
  - XU for user pages
  - XS for supervisor pages
  - KMS and UMX hardware bits
- Windows 10 1803以降既定で有効
  (MBEC/Kaby Lake+)



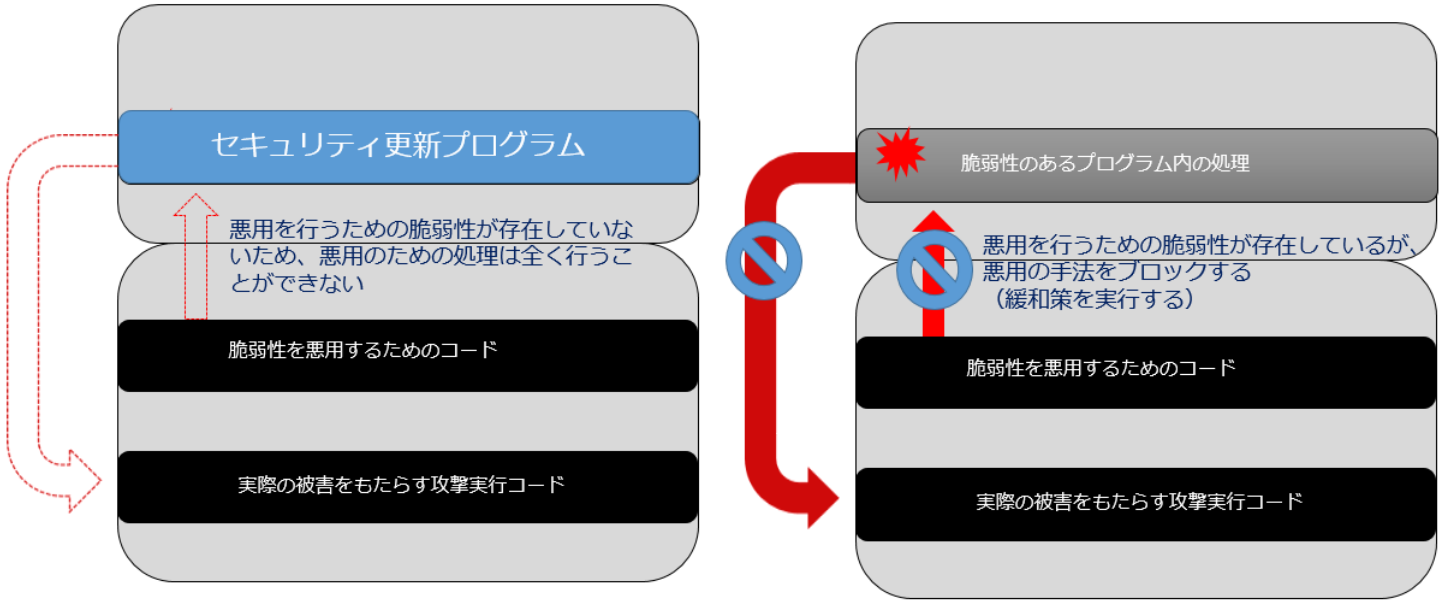
Windows Defender Device Guard

- デバイスのロックダウン機能
  - KMCI
  - UMCI
  - +VBS = HVCI
- Windows Defender Application Control (WDAC)



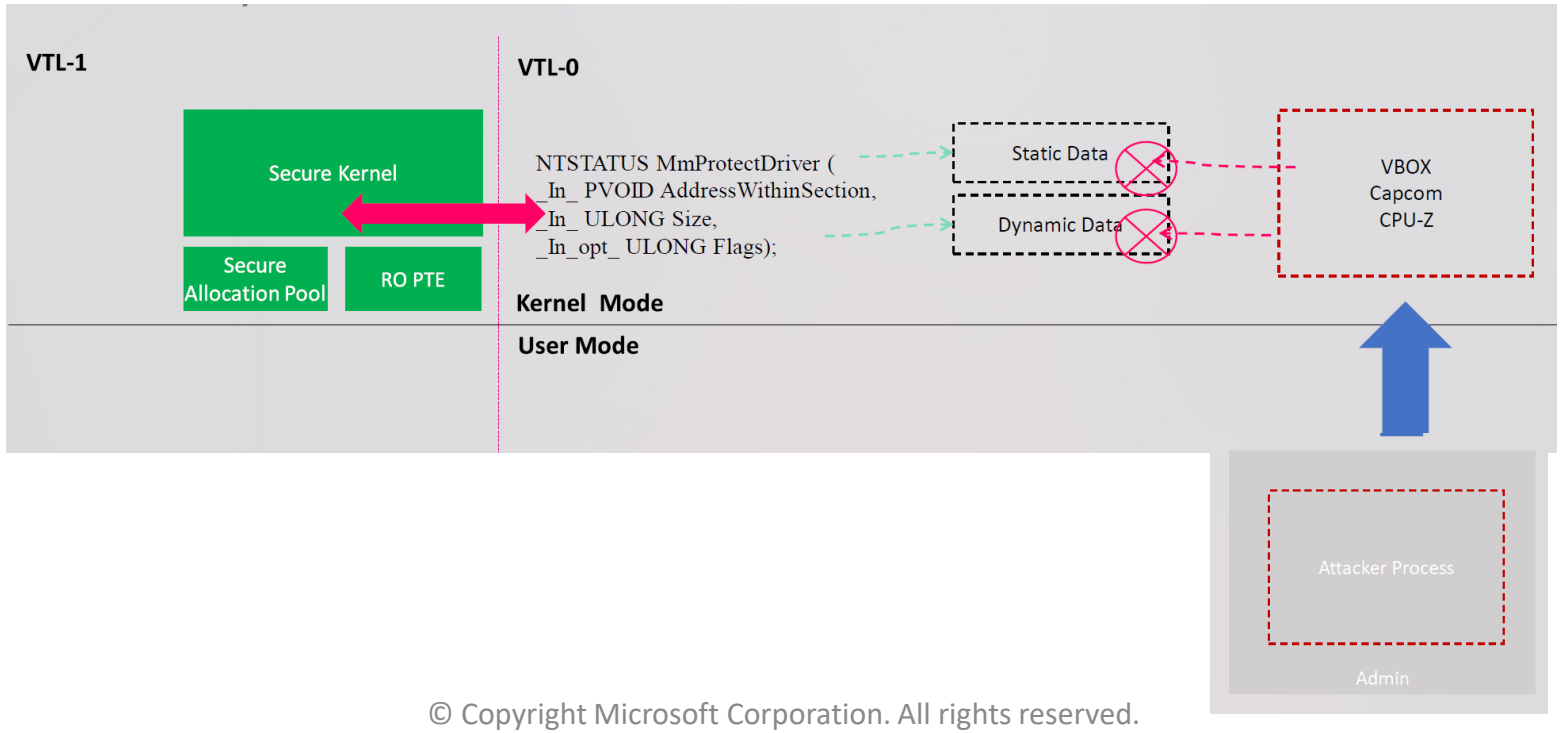
Windows Defender Exploit Guard

- エクスプロイトを緩和し、Attack Surfaceを減少させる技術
  - Attack Surface Reduction
  - Exploit mitigations
  - Protected Folders
- Windows 8以前は、追加のツール　Enhanced Mitigation Experience Toolkit (EMET) として提供



Kernel Data Protection

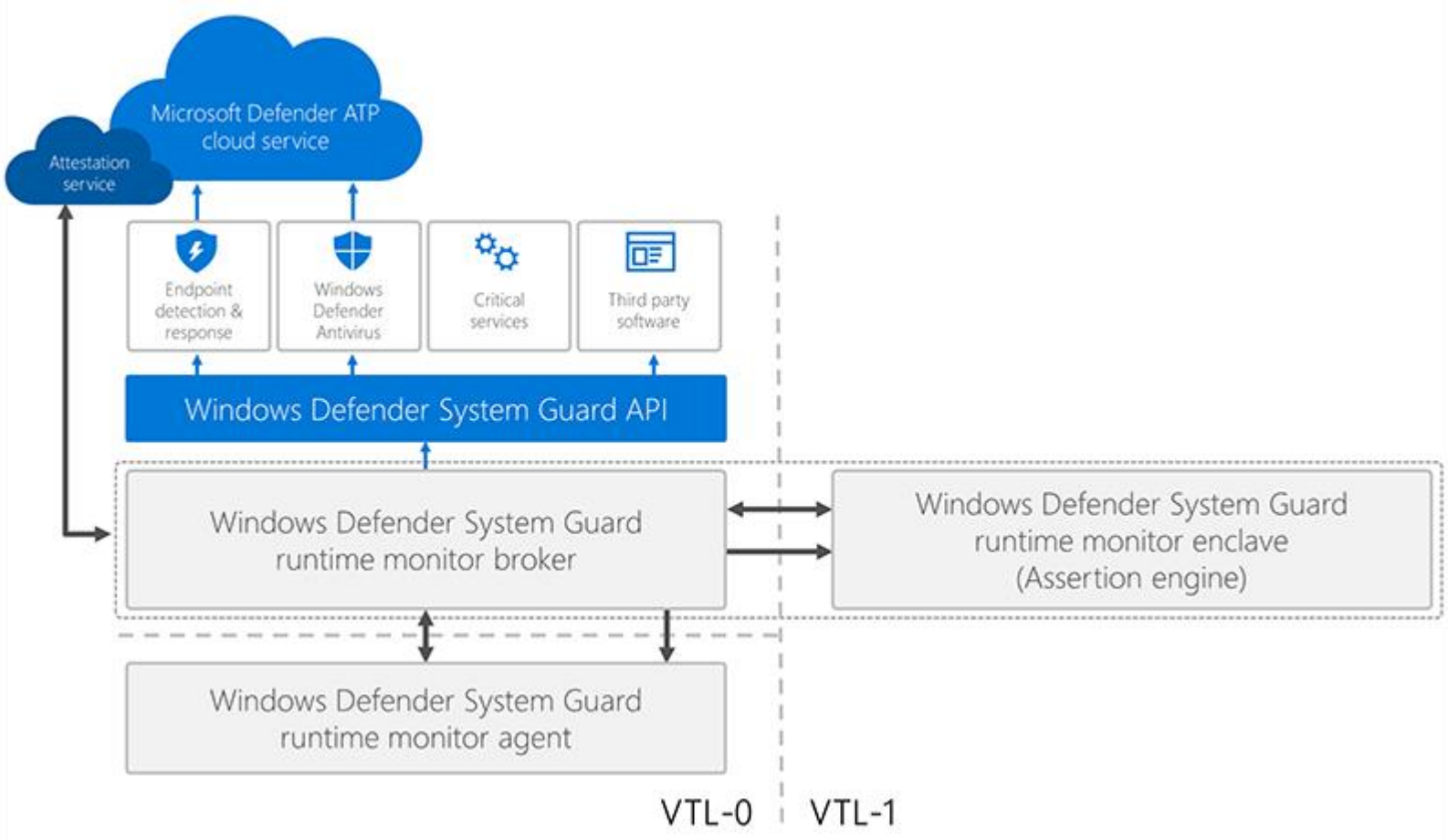
- Virtualization Based Security (VBS) を利用したKernel Data Corruption からの保護
  - カーネルのエクスプロイトの多くが System Structure Corruption
  - エクスプロイトに利用されやすい data structures を対象
- Static KDP: Static Data 保護
- Dynamic KDP：Read-Only Pool Allocation



Windows Defender System Guard Runtime Attestation

- Windows 実行中に実施するデバイスのコード整合性の検証

- Runtime report by WDSG RA
  - Boot State, Measured boot log
  - VBS Enclave内で生成された鍵ペアのプライベート鍵で署名
  - パブリック鍵は ASで署名されセッション証明書 (Microsoft CA)
- Session report by AS
  - デバイスの状態レポート



場所にとらわれない
「信頼できる場」へ



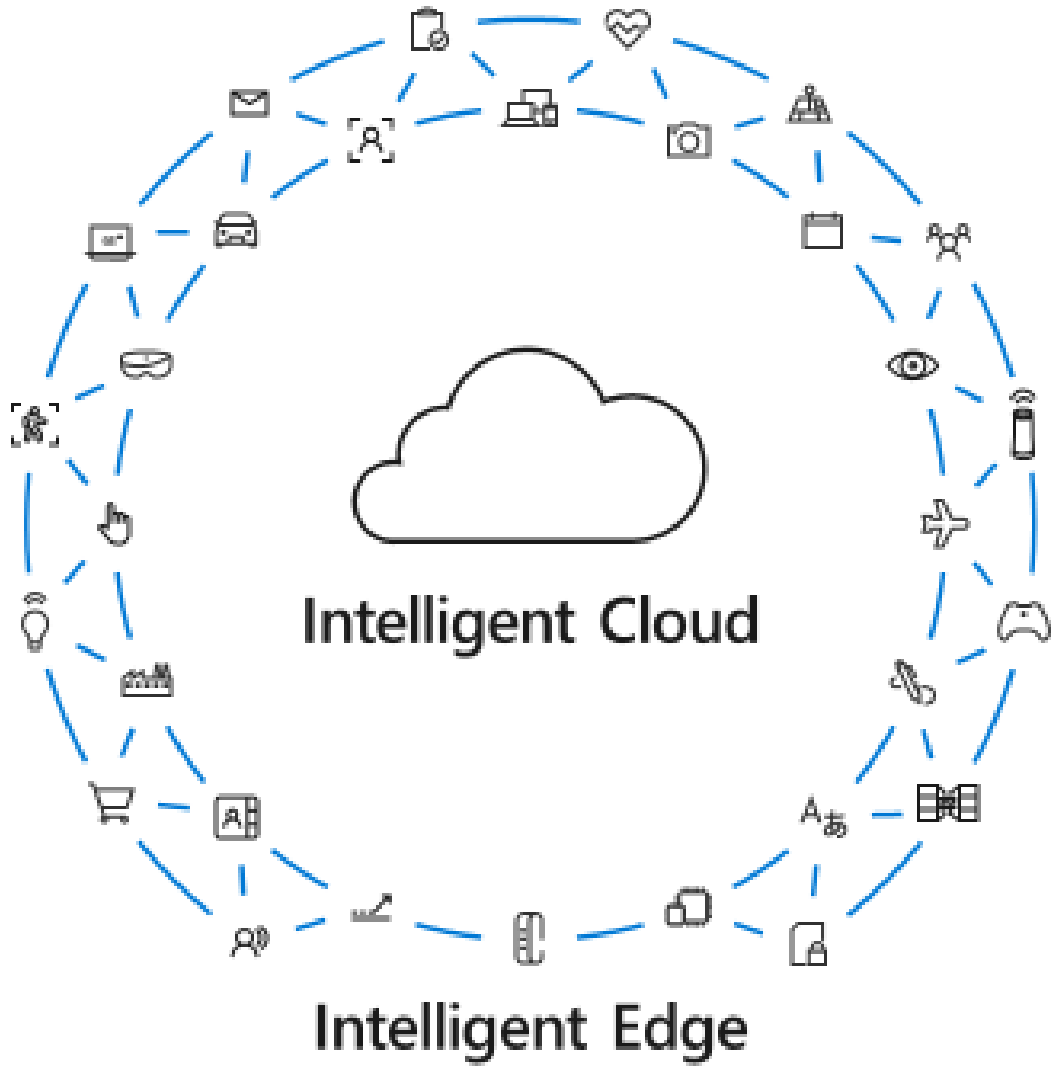





Ubiquitous computing

Artificial Intelligence

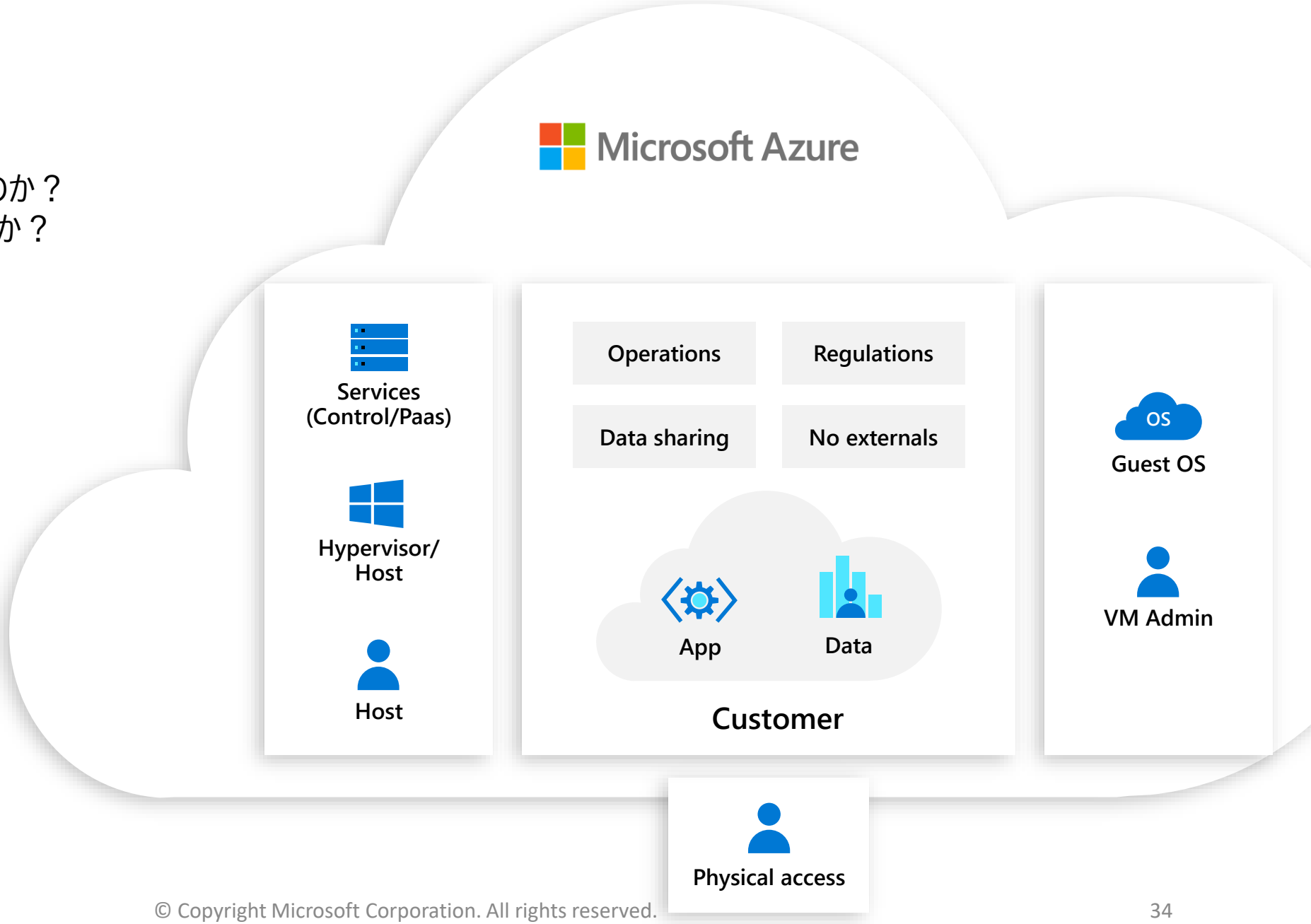
Multi-sense, multi-device experiences



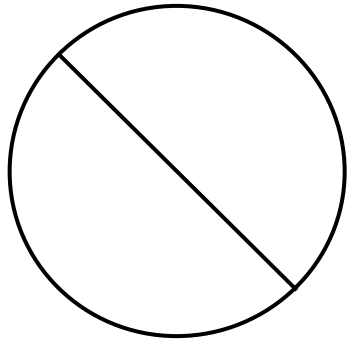
Microsoft Azure | Microsoft 365

クラウドを信頼する

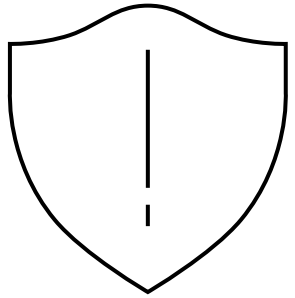
意図したコードが実行されているのか？
データの機密性は保たれているのか？



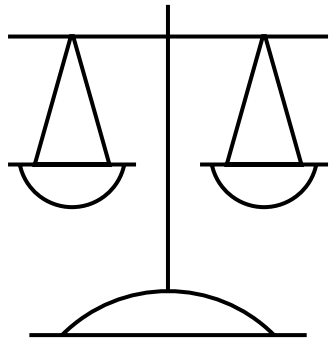
信頼への懸念



クラウドファブリックの
Hypervisor/OSのバグを
悪用するハッカーたち



悪意のある特権的な管
理者やインサイダー

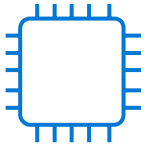


お客様の同意なく第三者がア
クセスすること

クラウドプラットフォームに求められていること

主要なデータ漏えいの脅威を軽減すること

ユーザーのデータに対する完全なコントロール (データ主権)



実行されるコードの検証が可能

データとコードはクラウドプラットフォームから見えない

クラウドプラットフォームに求められていること

主要なデータ漏えいの脅威を軽減すること

ユーザーのデータに対する完全なコントロール(データ主権)

実行されるコードの検証が可能

データとコードはクラウドプラットフォームから見えない

センシティブな処理に対する**最小限の**ハードウェア、ソフトウェア、そしてTCB (Trusted Computing Base)

ポリシーではなく、**技術的な策**

保証、残留リスク、軽減策に対する**透明性**

透明性のあるコンピューティングから秘匿性のあるコンピューティングへ

1

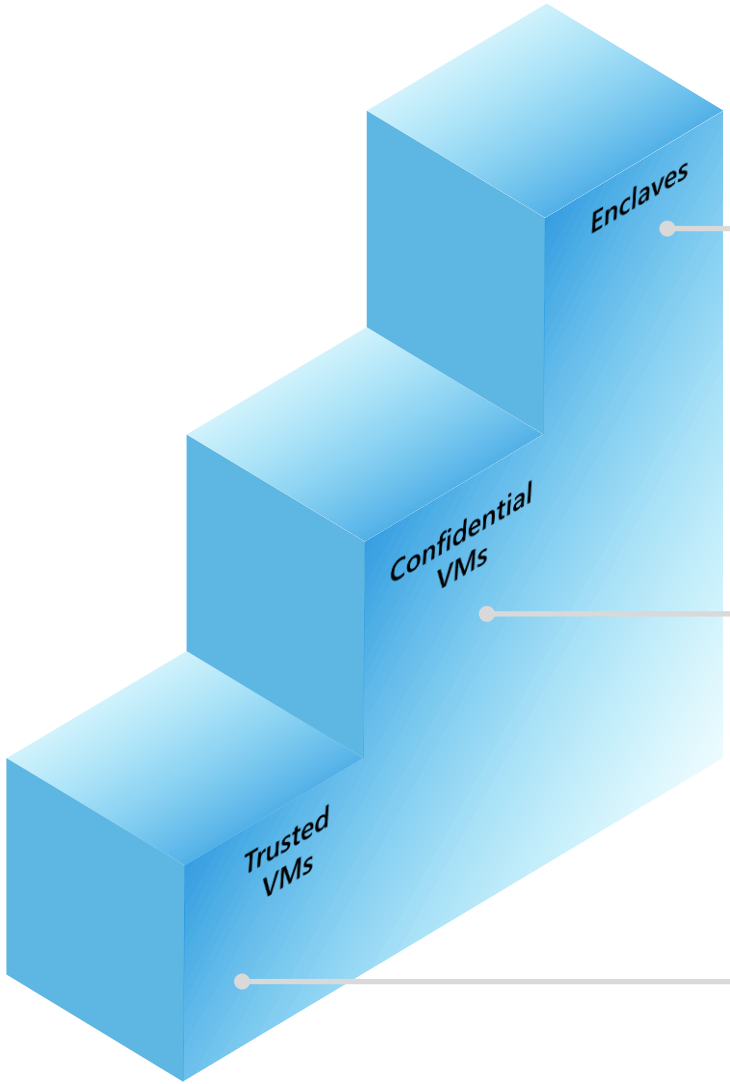
秘匿性の高いコンピューティングVMとOpen Enclave SDKを活用して、アプリケーションの安全性を高める

2

顧客のワークロード、機密ブロックチェーン,機密の保存と処理、アナリティクス、MLのトレーニングと推論、データストア、IoT

3

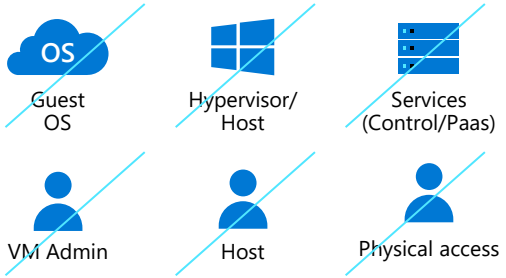
マルチパーティのデータセット分析と機械学習により、組織全体のプライバシーとセンシティブな顧客データを保護



Hardware Enclaves with Intel SGX

Technology: Attestation, Secure Key Release, Cloud sealing

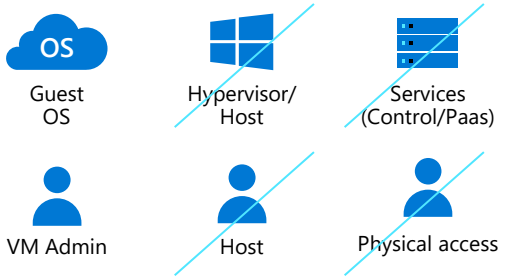
"私は自分のアプリコードとチップを信じています。"



Hardware Confidential VMs with AMD Milan, Intel TDX

Technology: (Trusted VM), Secure Key Release, Blind Hypervisor

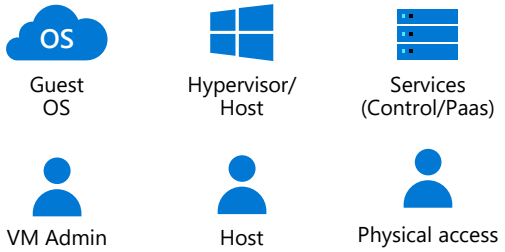
"マイクロソフトは私のVMにあるものには手を出せない"



Trusted VMs

Technology: (Host/Overlake Integrity) + VM Attestation, VM Secure Boot, vTPM, Virtualization-Based Security

"信頼できる既知のコードのみが私のVM上で実行されている"



TRUST

Confidential Computing at Microsoft

Unlocking new cloud possibilities


Internal Tools

SaaS Offerings


ISV Partners


Finance


Governments


Healthcare

Developer tools, deployment, and data management


VS Studio/Code


WinDbg


CCF SDK


Open enclave SDK


Open LibOS


Containerization


Azure Data Share

Confidential-enabled Azure platform products


Azure Machine Learning


Azure Key Vault


Azure Confidential Ledger


Microsoft Azure Attestation


Azure Kubernetes Service (AKS)


Microsoft Azure IoT

Suite of cloud and edge offerings tailored to security needs


Enclave VMs


Confidential VMs


Trusted VMs


IoT Edge Device

Innovative new hardware

Industry leadership and standardization

まとめ








信頼されるプラットフォームに求められること

- より信頼される場の提供へ
  - トラストに対するさらなる**選択肢**と**コントロール**をユーザーに提供する
  - **最小限**のトラストのコンポーネント
  - 保証、残留リスク、軽減策に対する**透明性**

- 普及に向けた課題
  - 互換性,ハードウェアの選択肢、パートナーのサポート






Microsoft

Let’s secure the future.

SECURED FROM THE SILICON UP