Microsoft

PKI & TRUST Days online 2021「デジタル社会におけるトラスト」
2021年4月15日（木）

プラットフォームで実装されるトラスト

Yurika Kakiuchi
Security Program Manager
Security Response Team
Microsoft Corporation
CISSP
@Eurekaberry

プラットフォームが「トラスト(信頼)」されるためには

© Copyright Microsoft Corporation. All rights reserved.

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。

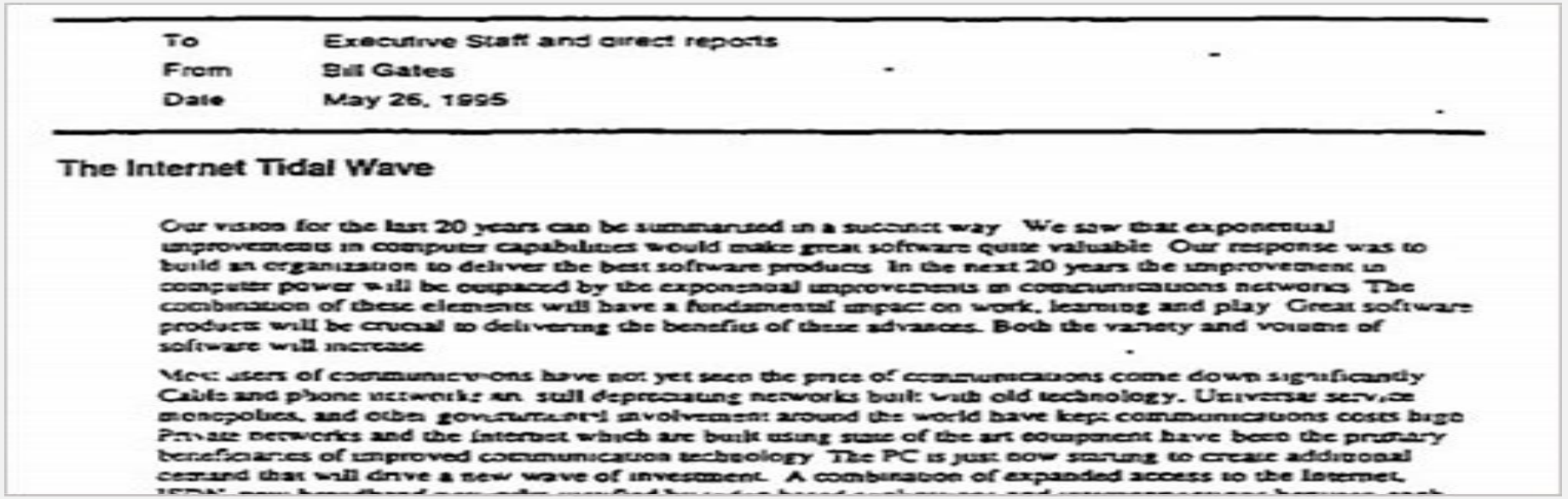
© Copyright Microsoft Corporation. All rights reserved.

「信頼」への旅路の始まり

Windows 95 そしてインターネット時代

© Copyright Microsoft Corporation. All rights reserved.

マイクロソフトが抱えた深刻な問題（2000年～2001年）



To Executive Staff and direct reports
From Bill Gates
Date May 26, 1995

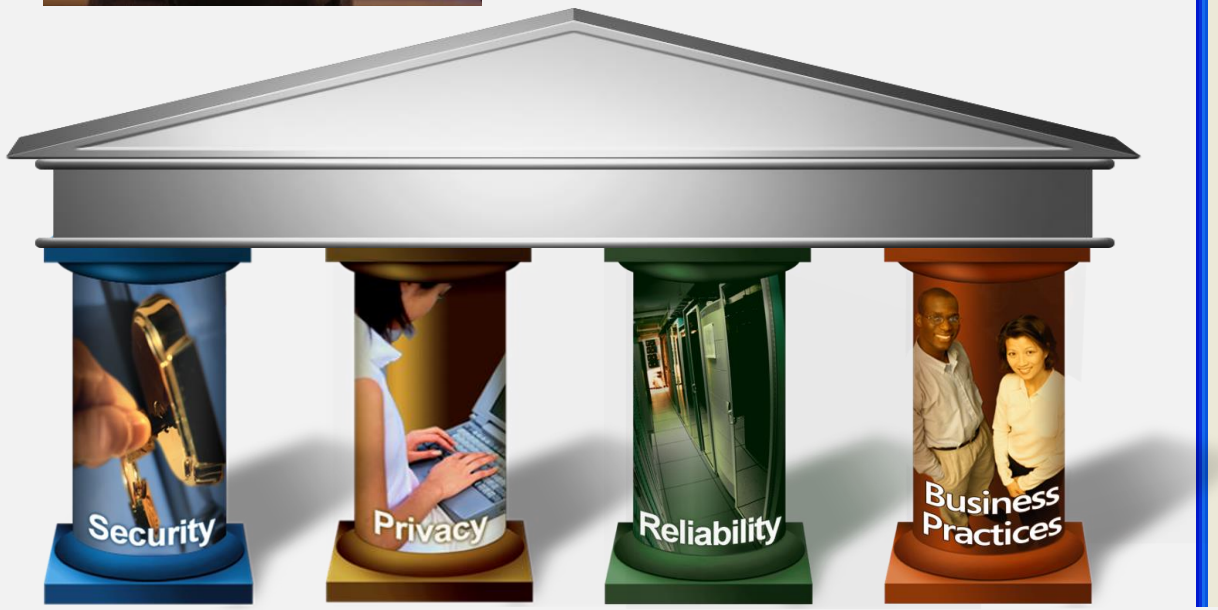
The Internet Tidal Wave

Our vision for the last 20 years can be summarized in a succinct way We saw that exponential improvements in computer capabilities would make great software quite valuable Our response was to build an organization to deliver the best software products In the next 20 years the improvement in computer power will be outpaced by the exponential improvements in communications networks The combination of these elements will have a fundamental impact on work, learning and play Great software products will be crucial to delivering the benefits of these advances. Both the variety and volume of software will increase

Most users of communications have not yet seen the price of communications come down significantly Cable and phone networks are still deploying networks built with old technology. Universal service monopolies, and other governmental involvement around the world have kept communications costs high Private networks and the Internet which are built using state of the art equipment have been the primary beneficiaries of improved communications technology The PC is just now starting to create additional demand that will drive a new wave of investment. A combination of expanded access to the Internet,

© Copyright Microsoft Corporation. All rights reserved.

信頼できるコンピューティング（2002年）



Trustworthy computing - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: Bill Gates Sent: Tue 1/15/2002 2:22 PM

To: Microsoft and Subsidiaries: All FTE

Cc:

Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

© Copyright Microsoft Corporation. All rights reserved.

「信頼できるコンピューティング」が目指したもの

技術： そもそも安全な製品づくり
- 安全なプラットフォームの開発（SDL）
- 多層的・統合的なセキュリティ技術

ガイダンス: 分かりやすい情報提供
- 啓発と教育コンテンツ
- 各製品の設定・具体的な構築手法のホワイトペーパー
- 信頼できるインシデント レスポンス

業界との連携： 業界全体でお客様を保護
- 政府機関、業界パートナーとの協業
- 脅威に関する技術情報の共有

© Copyright Microsoft Corporation. All rights reserved.

課題

“実際にユーザ環境で実行されているWindowsの環境”は「信頼」できるのか？

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.

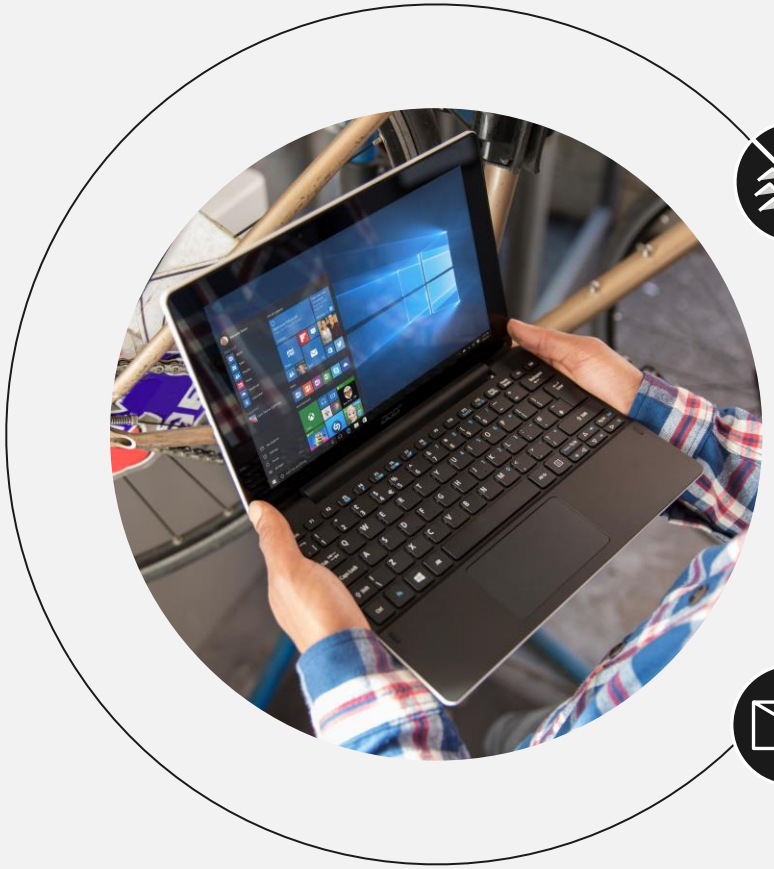
There is now a version 2, which is still as important as version 1 was. The 10 Laws are:

> 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

© Copyright Microsoft Corporation. All rights reserved.

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？

© Copyright Microsoft Corporation. All rights reserved.

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

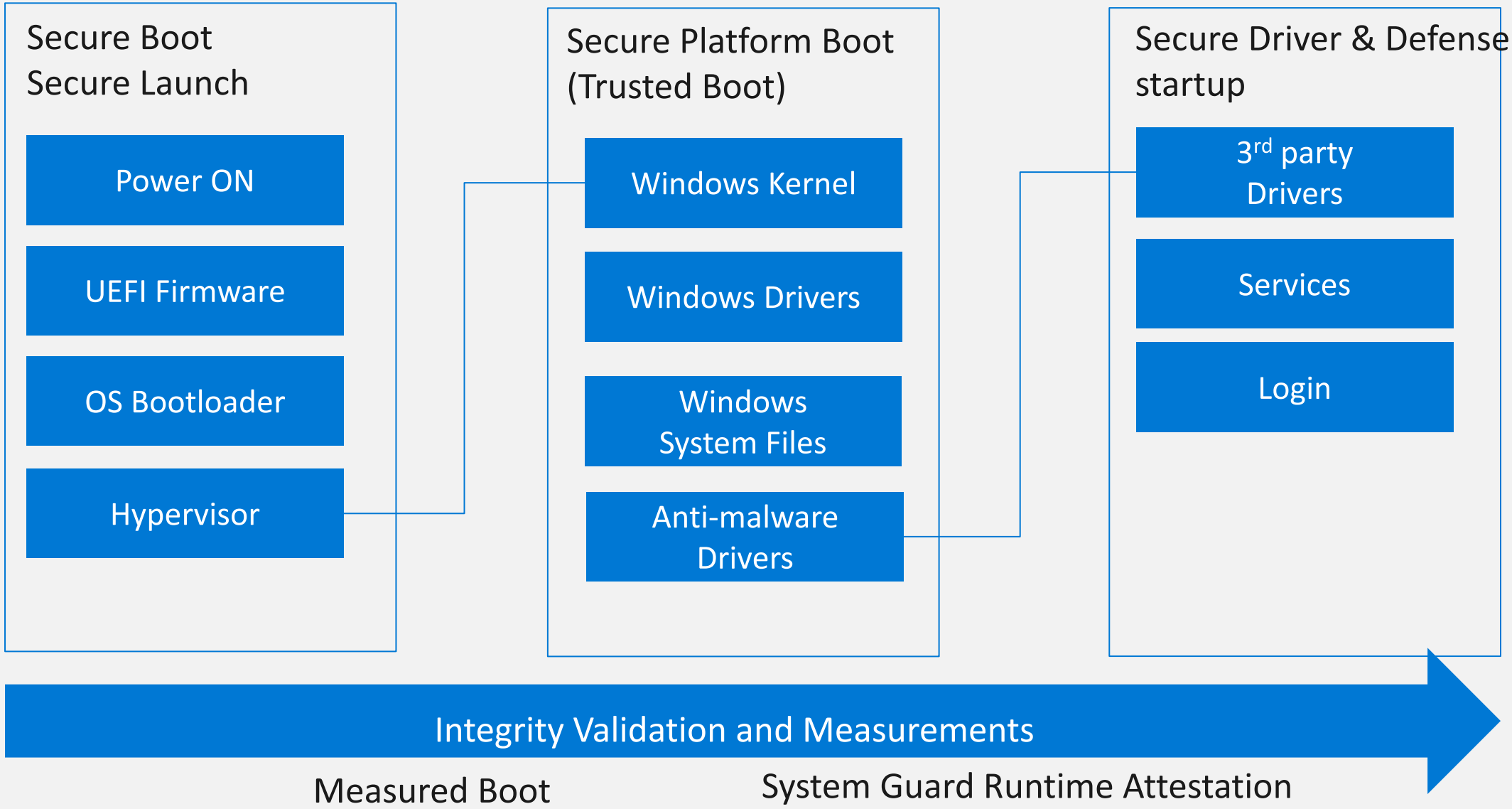
悪意のあるコードがデバイス上に留まらない

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

© Copyright Microsoft Corporation. All rights reserved.

ブート時の保護 in Windows 概要

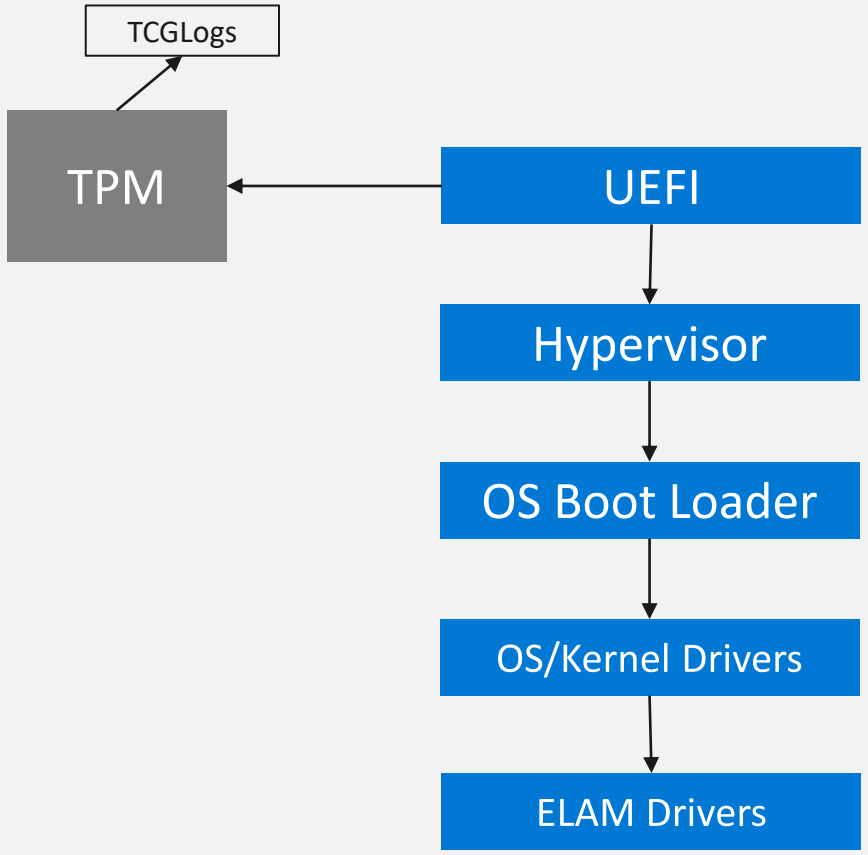


© Copyright Microsoft Corporation. All rights reserved.

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

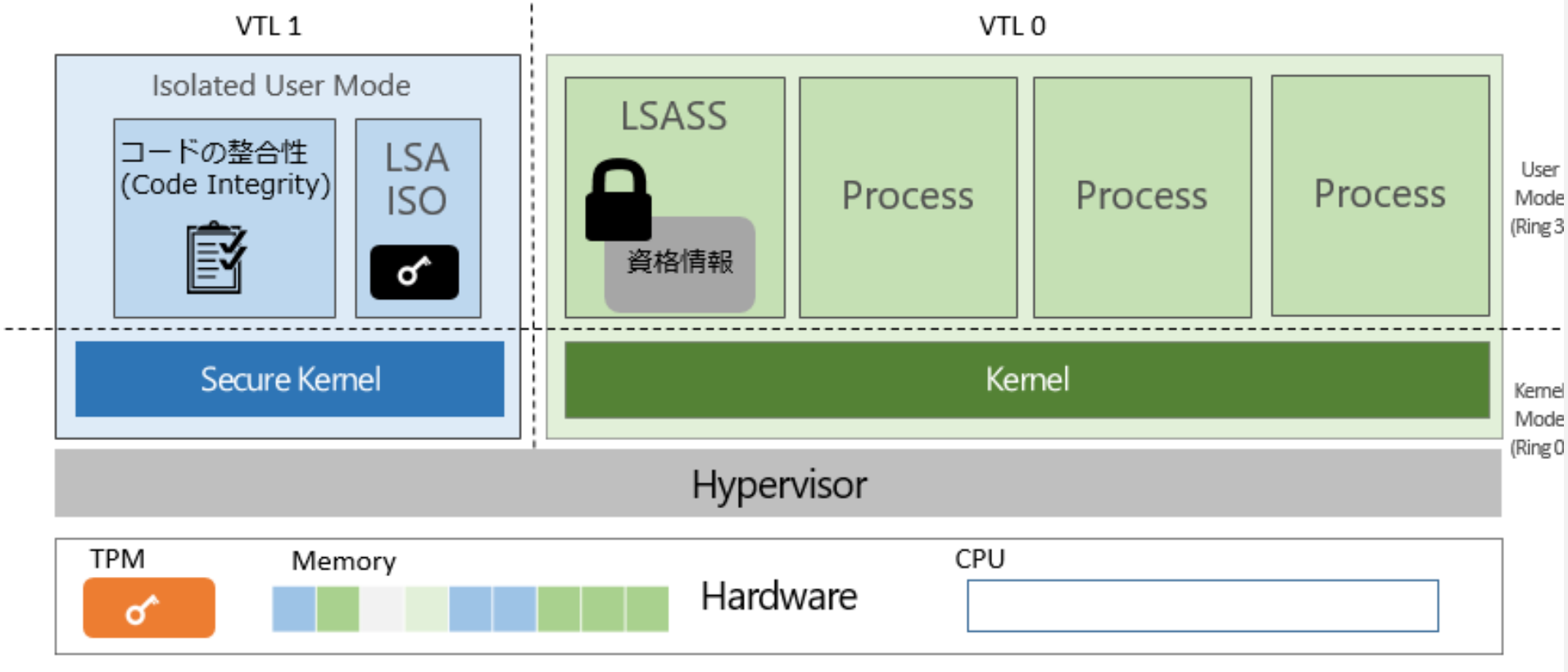
- UEFI ファームウェアへの信頼が低下
  - FEFI rootkit (Lojax) reported by ESET



© Copyright Microsoft Corporation. All rights reserved.

Virtualization-based security (VBS)

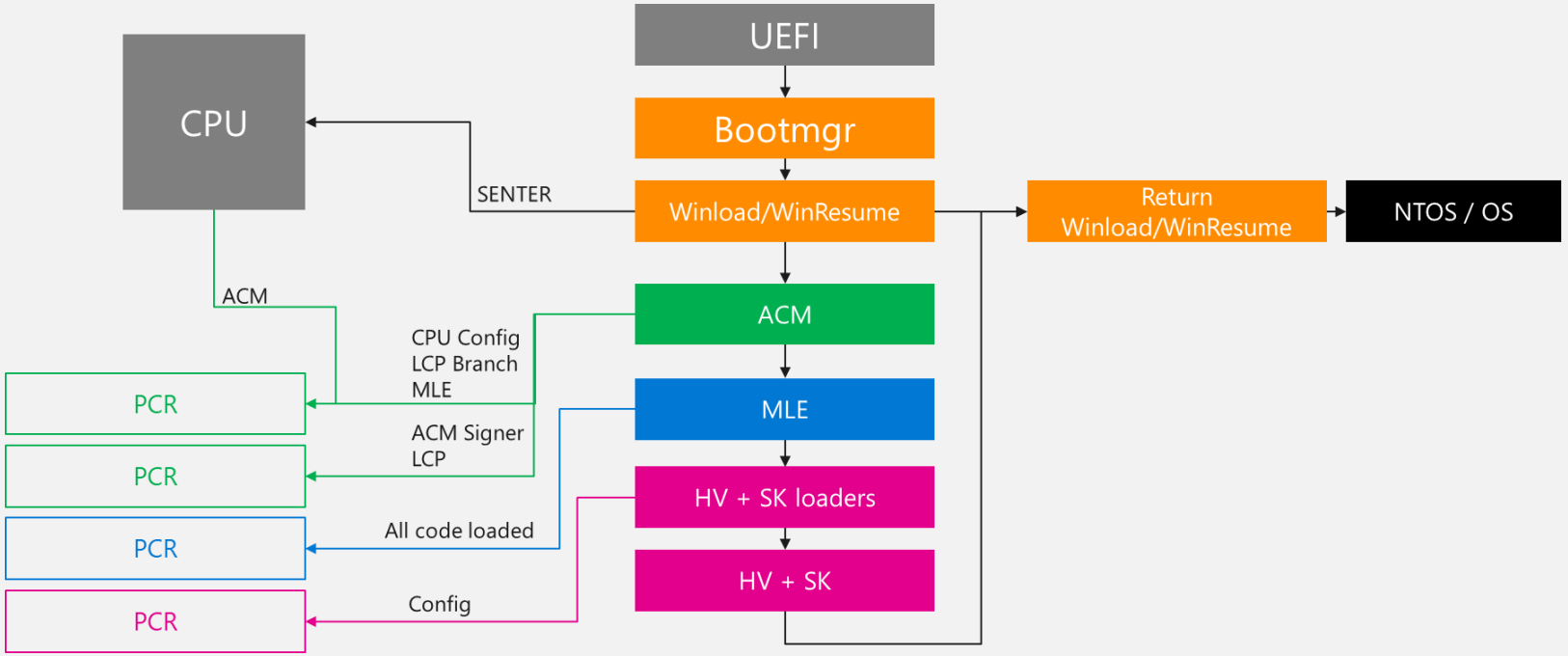
- Windows 10+ の多くのセキュリティ機能の基礎
- Hypervisor, SLAT, IOMMUをベースとした仮想化による保護技術



© Copyright Microsoft Corporation. All rights reserved.

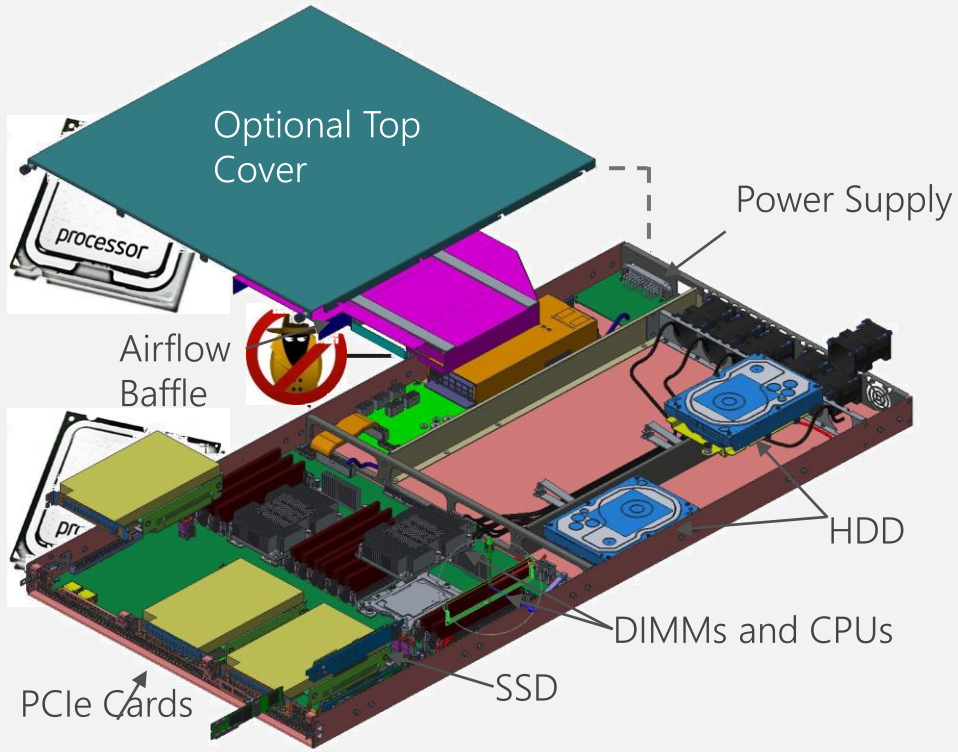
Secure Launch (Windows 10 1809+)

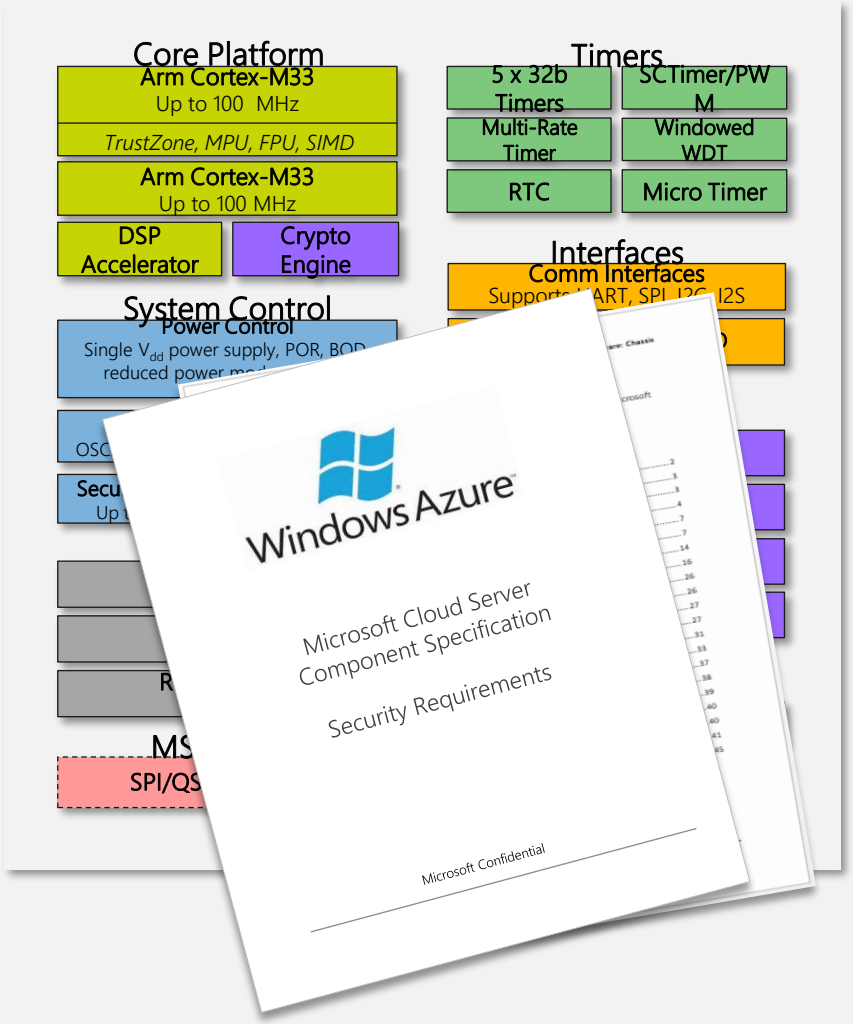
- DRTM, (Intel TXT, AMD, Qualcomm)
- UEFI への侵害を前提に、UEFIに依存しない安全なブート
- 動的に Root of trust measurement を実行
  - Code integrity Policy, Hypervisor, kernel hashes, UEFI Vars, etc…



© Copyright Microsoft Corporation. All rights reserved.

Project Olympus/Project Cerberus





© Copyright Microsoft Corporation. All rights reserved.

Microsoft Pluton 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

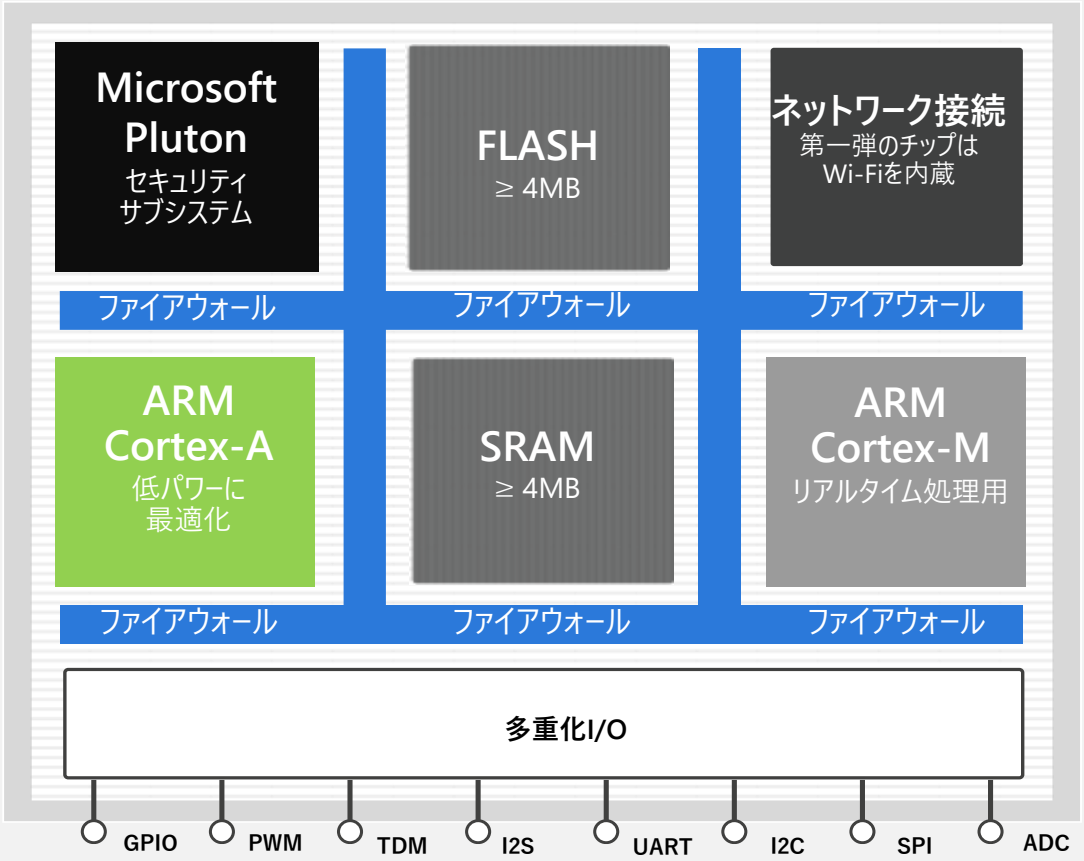
デバイスのソフトウェアは自動的にアップデートされるか？

= 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

© Copyright Microsoft Corporation. All rights reserved.

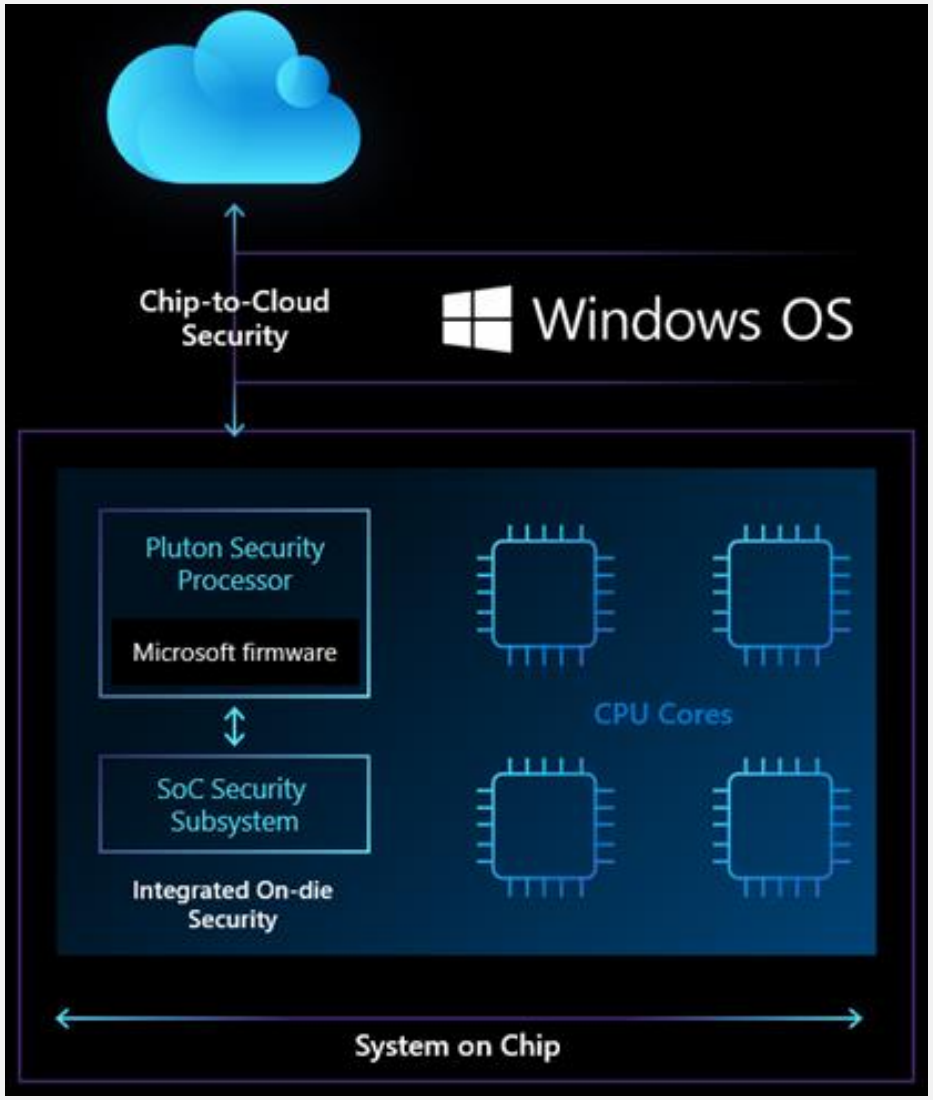
Azure Sphere MCU

- Pluton Security Subsystemを含むMicrosoft シリコン セキュリティ テクノロジーによる保護
  - 組み込み済みのネットワーキングによる接続
  - Pluton Security Subsystemを含む組み込み済みMicrosoftシリコン セキュリティ テクノロジーによるセキュリティ保護
  - クロスオーバーCortex-Aの処理能力を初めてMCUで実現



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Pluton on PCs



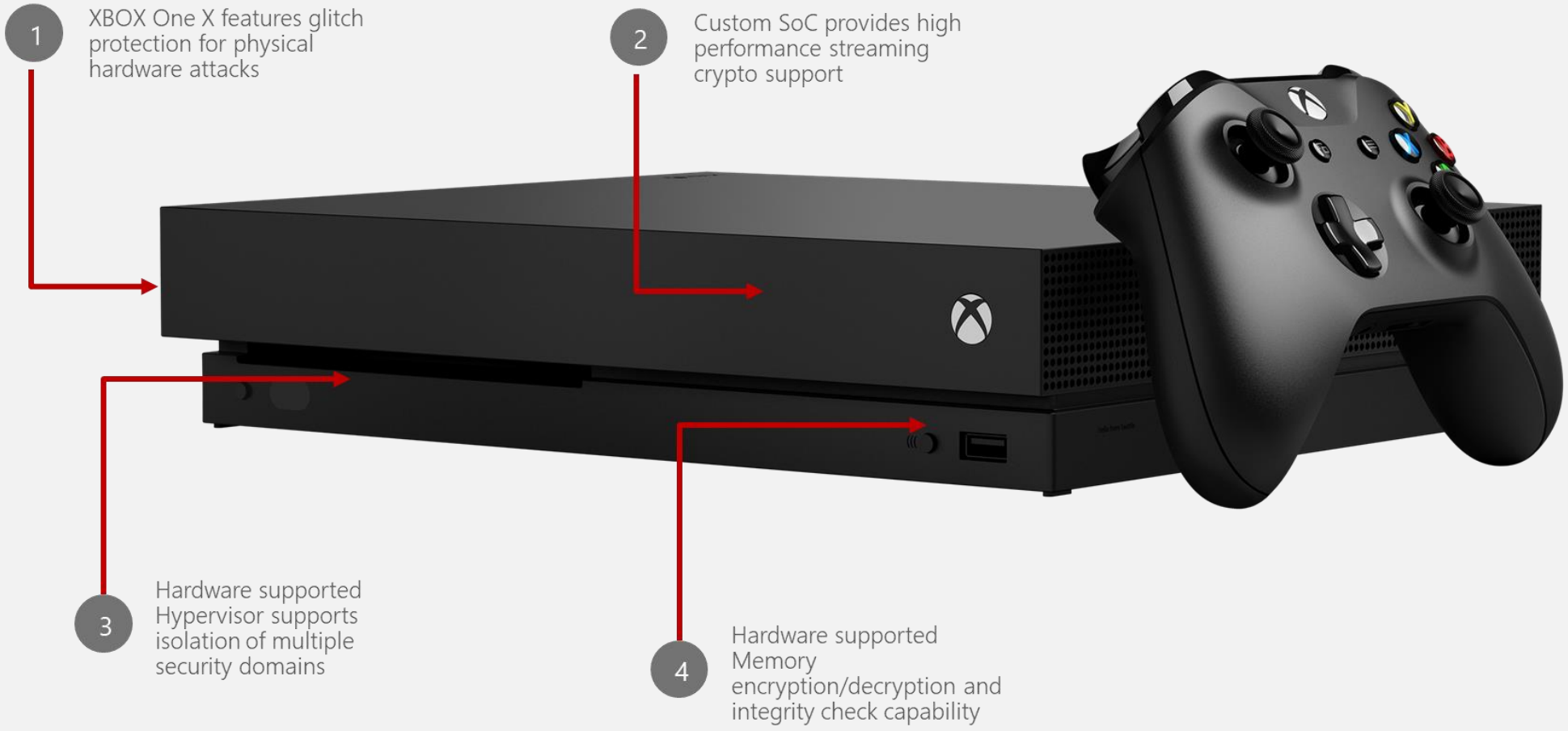
AMD、Intel、Qualcomm Technologies, Inc. という主要シリコンパートナーとの協力し

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]

© Copyright Microsoft Corporation. All rights reserved.

実は、旅路はここから始まっていた…



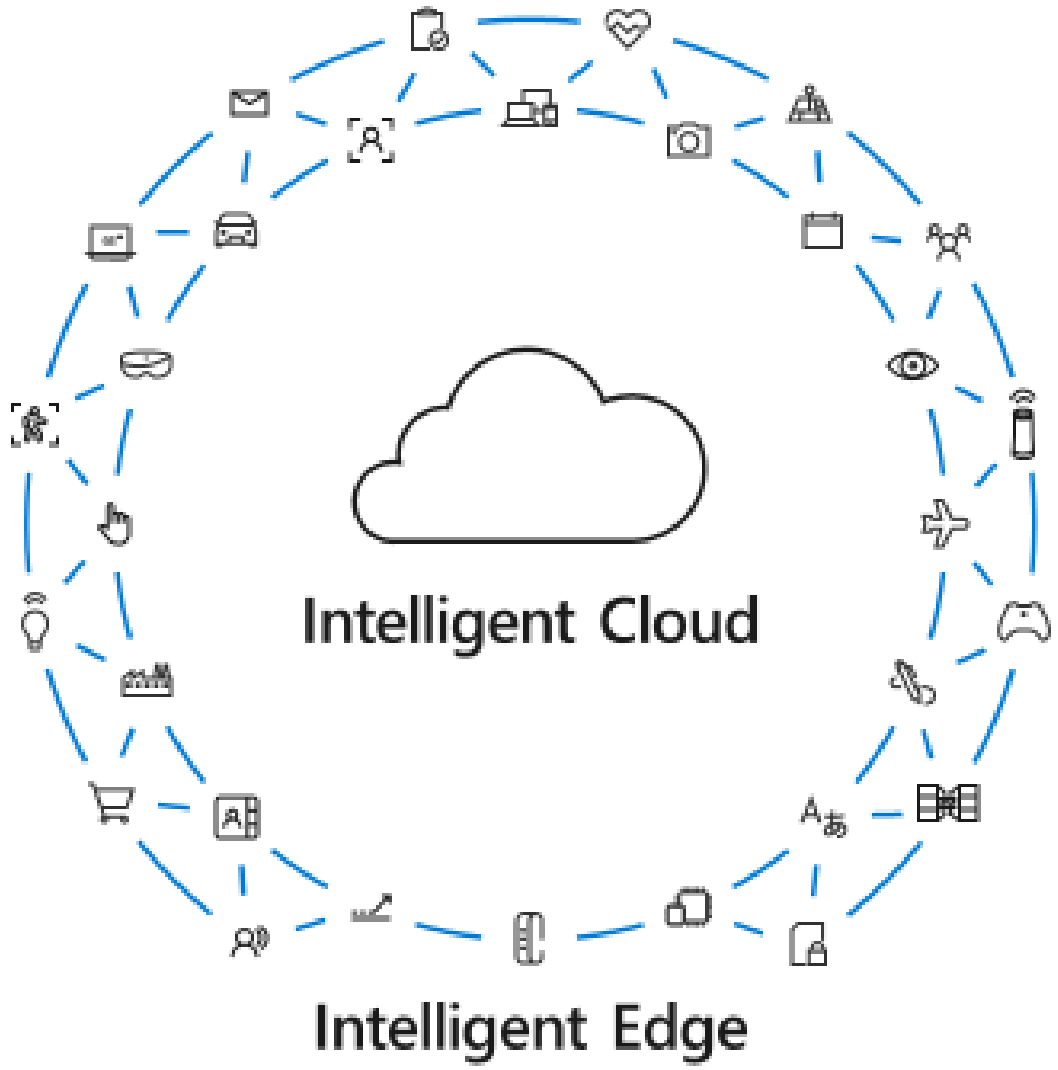
© Copyright Microsoft Corporation. All rights reserved.

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

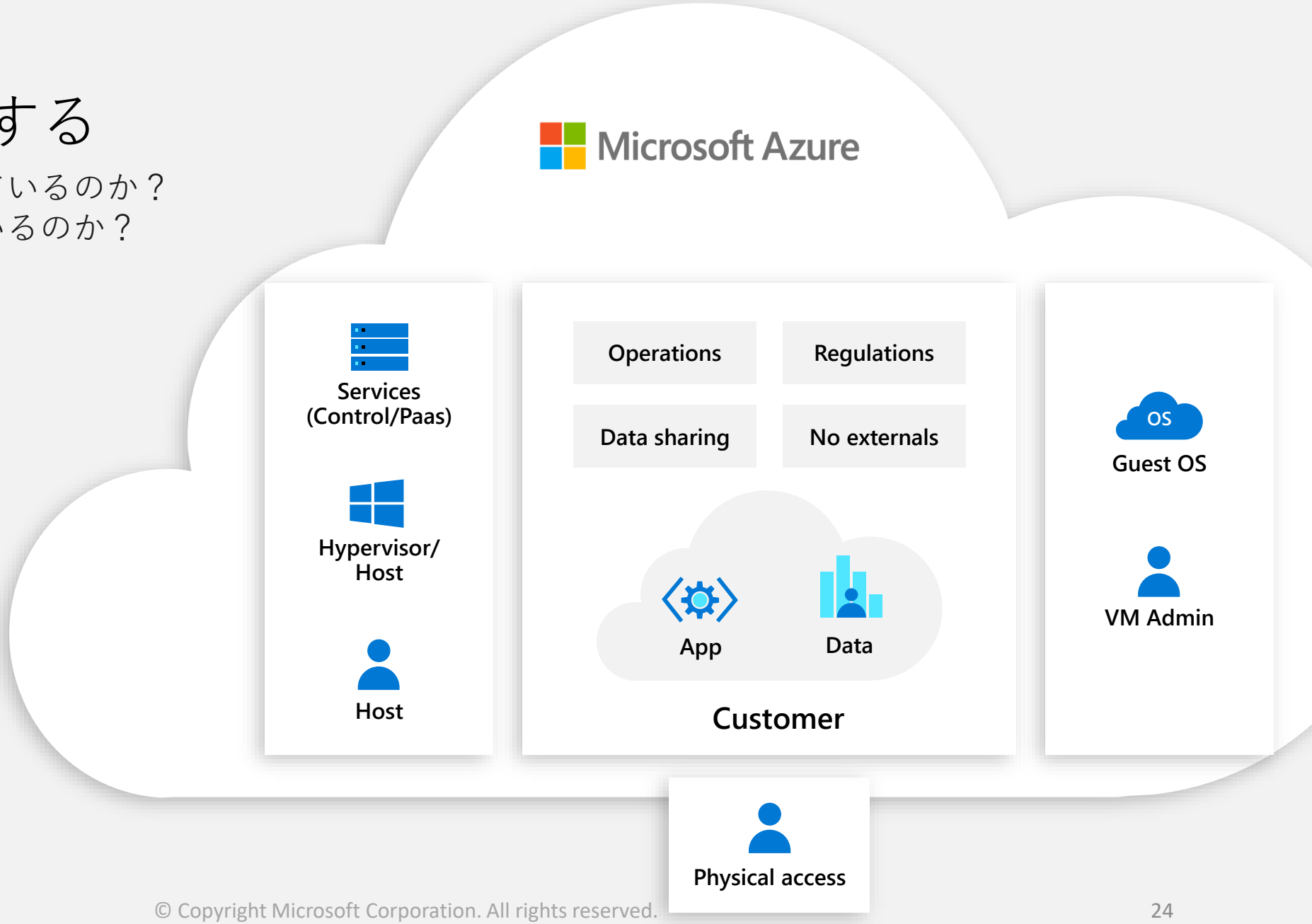


Microsoft Azure | Microsoft 365

© Copyright Microsoft Corporation. All rights reserved.

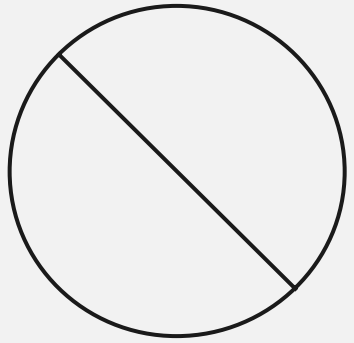
クラウドを信頼する

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？

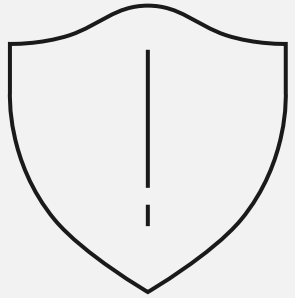


© Copyright Microsoft Corporation. All rights reserved.

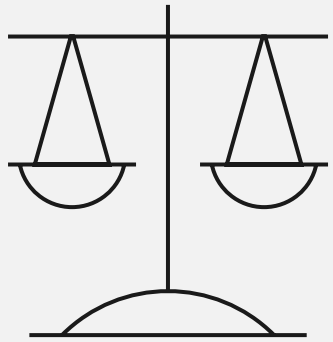
信頼への懸念



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



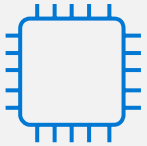
お客様の同意なく第三者
がアクセスすること

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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**

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

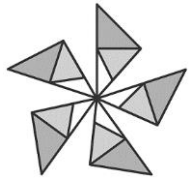
オープンソースへの投資

MOST CONTROL

Open Enclave SDK

MACHINE LEARNING

Confidential Inference ONNX Runtime



FOUNDING MEMBER

Confidential Computing Consortium

LIFT AND SHIFT ON SGX

Mystikos Library OS

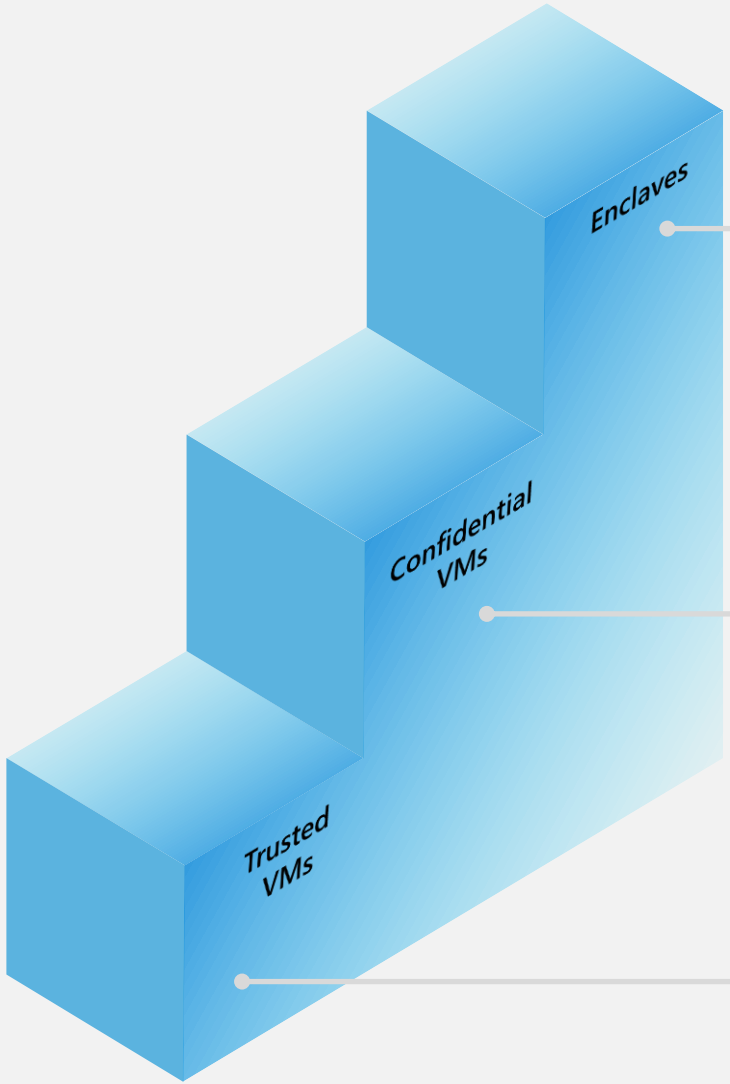
SECURE BLOCKCHAIN/LEDGER

Confidential Consortium Framework (CCF)

PRIVATE PREVIEW

Azure Confidential Ledger

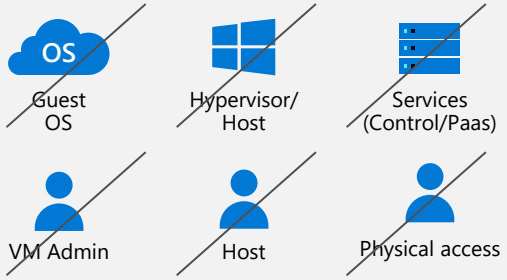
© Copyright Microsoft Corporation. All rights reserved.



Hardware Enclaves with Intel SGX

Technology: Attestation, Secure Key Release, Cloud sealing

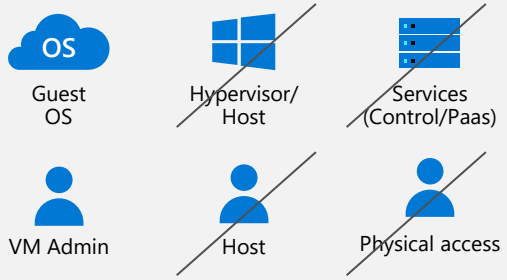
"私は自分のアプリコードとチップを信じています。"



Hardware Confidential VMs with AMD Milan, Intel TDX

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

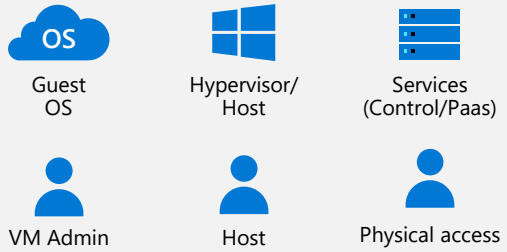
"マイクロソフトは私のVMにあるものには手を出せない."



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

© Copyright Microsoft Corporation. All rights reserved.

Confidential Azure services

PUBLIC PREVIEW

Azure Kubernetes Confidential Computing Nodes

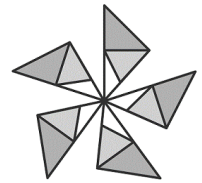
COMING SOON

Azure SQL

Always Encrypted with secure enclaves

BETA RELASE

Confidential Inference ONNX Runtime



PUBLIC PREVIEW

Microsoft Azure Attestation

PUBLIC PREVIEW

Azure Key Vault

Managed HSM

COMING SOON

Azure Confidential Ledger

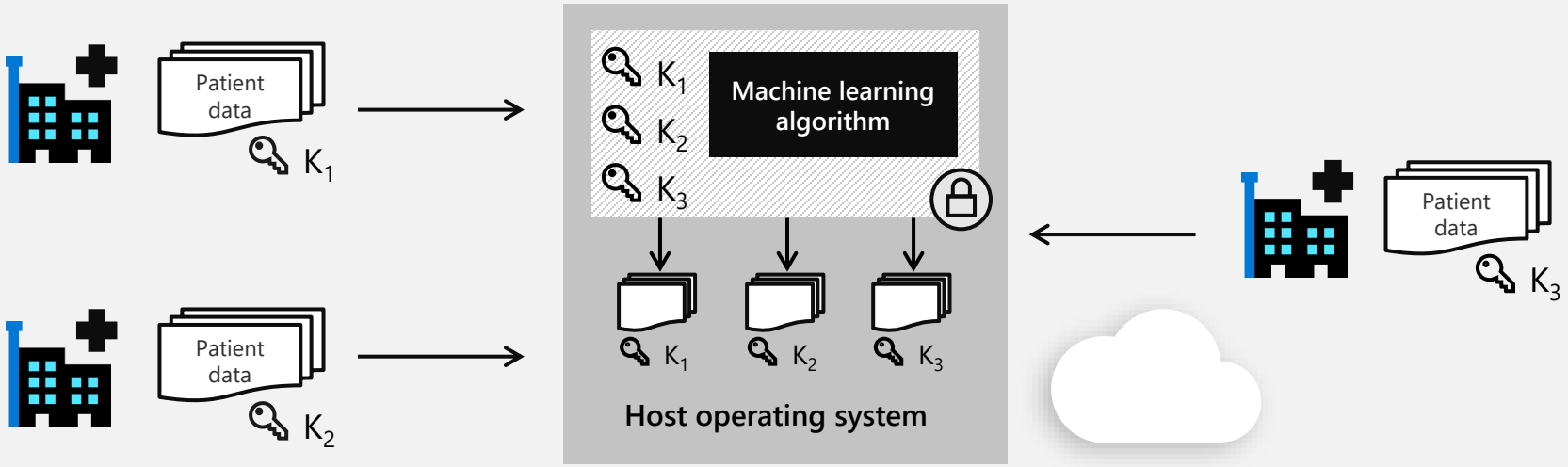
https://aka.ms/acc-getintouch

マルチパーティデータ共有
ヘルスケアにおける新薬開発

提携している医療機関が個人の患者の健康データセットを提供し、MLモデルを学習する

各施設はそれぞれのデータセットのみを見ることができ、クラウド提供者も含め、誰も全てのデータや必要に応じて学習したモデルを見ることはできない

学習したモデルを使用することで、すべてのパーティが利益を得る



利用シナリオ

政府組織

- 不正・浪費・虐待防止
- デジタルアイデンティティ
- 重要インフラ
- 腐敗防止
- テロ対策
- サイバー犯罪防止
- 司法手続きとケースマネジメント
- 記録と証拠の管理
- インテリジェンス分析
- グローバルな兵器システムとロジスティクス管理
- 配備されたオペレーションと切断されたオペレーション
- 保護・弱者保護（児童搾取、人身売買などを含む

ファイナンシャル分野

- マネーロンダリング対策
- デジタル通貨
- ブロックチェーン
- 詐欺防止
- トランザクション処理
- カスタマーアナリティクス
- 独自のアナリティクス/アルゴリズム

ヘルスケア分野

- 疾病診断
- 保険金詐欺防止
- 医薬品開発
- コンタクトトレーシング

© Copyright Microsoft Corporation. All rights reserved.

不正行為の検知

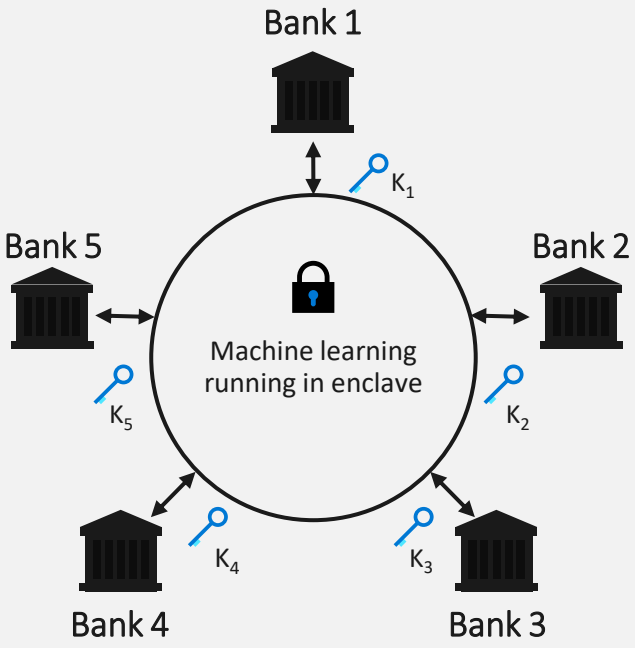
信頼された実行環境は、機密性を維持しつつ、複数人による解析を可能に

コンフィデンシャル・コンピューティングは

機密性の高いデータセットを組み合わせて、合意した分析を実行することができます。

アクセス権を与えずに洞察することができる。

機密保持の要件を満たすことができます。



Create a complete picture of movement of funds using enclaves

結果

検知率の向上

誤認識の低減

反復学習。

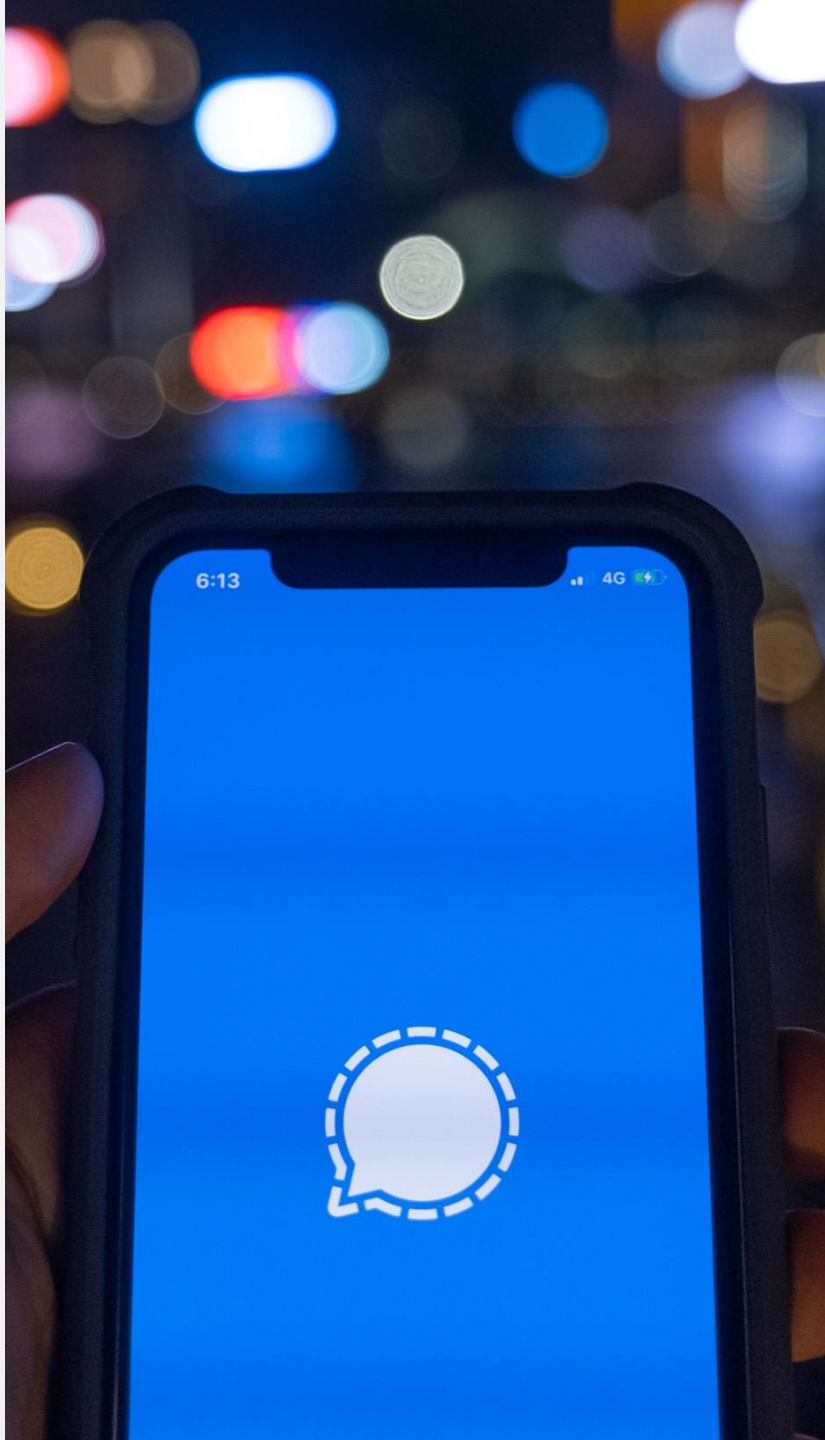
© Copyright Microsoft Corporation. All rights reserved.

Signal

多くのメッセージング・アプリは、広告の収益化や政府への提供を目的として、ユーザー・データを保存、販売、共有しています。
Signalは、プライバシーを保護するメッセージング・プラットフォームを提供し、ユーザー・アカウントは機密のコンピューティング・インフラストラクチャ内で処理されるため、ユーザーは自分のデータが販売または共有されないことを信頼できます。

“To meet the security and privacy expectations of millions of people every day, we utilize Azure Confidential Computing to provide scalable, secure environments for our services. Signal puts users first, and Azure helps us stay at the forefront of data protection with confidential computing.”

Jim O'Leary
VP of Engineering, Signal



© Copyright Microsoft Corporation. All rights reserved.

まとめ

© Copyright Microsoft Corporation. All rights reserved.

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
  - TEE, Enclave を利用した、最小限のトラスト
  - 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






© Copyright Microsoft Corporation. All rights reserved.

Microsoft

Let’s secure the future.

SECURED FROM THE SILICON UP

© Copyright Microsoft Corporation. All rights reserved.

Appendix

Resources

- Azure Confidential Computing
  - Learn more—http://aka.ms/AzureCC
  - Deploy—http://aka.ms/ACCMarketplace
  - Develop—http://aka.ms/OESDKGitHubRepo
- New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats - Microsoft Security