Microsoft Azure

信頼できる基盤を目指す Azure とその最新技術

日本マイクロソフト株式会社
Azure ビジネス本部
プロダクトマネージャー
佐藤 壮一

Azure

The world's computer

- Available regions
- Regions coming soon
- Edge zones
- Network PoPs
- WAN links
- Ground stations

65+ Azure regions

200+ datacenters worldwide

175k+ miles of fiber

190+ network PoPs

Network extends to space with Azure Orbital ground stations

データ保護の多層化

既存の暗号化手法

保存されたデータ

ブロブや DB 等に保存された
非利用中のデータの暗号化

通信中のデータ

信頼度の低いネットワークを介して
通信されるデータの暗号化

データ保護の多層化

既存の暗号化手法

保存されたデータ

ブロブや DB 等に保存された
非利用中のデータの暗号化

通信中のデータ

信頼度の低いネットワークを介して
通信されるデータの暗号化

Confidential computing

利用中のデータ

RAM 上や CPU で処理されているデータの暗号化・保護

BeeKeeperAI™

Customer:
BeeKeeperAI
Industry:
Healthcare
Size:
50 - 999 employees
Country:
United States

Products and services:
Azure
Azure Confidential Computing

Read full story here

Microsoft

"マイクロソフトは、Intel SGXとZero Trustインフラストラクチャによる最小のアタックサーフェスソリューションを提供し、セキュリティへの注力を実証した、ヘルスケア部門から信頼されるクラウドプラットフォームの完璧な組み合わせを提供しています。"

—Mary Beth Chalk, Cofounder and Chief Commercial Officer, BeeKeeperAI

Situation:

BeeKeeperAIは、ヘルスケア分野におけるAIの開発を加速させるために作られました。機密性の高い健康データと開発中のアルゴリズムの両方を覗き見されないようにする、ゼロトラストの機密コンピューティングプラットフォームを作成できる新しいセキュリティソリューションが必要でした。

Solution:

BeeKeeperAIはマイクロソフトと協力して、Azure Confidential Computingを通じてIntel SGX にアクセスし、高い安全性と HIPAA に準拠した堅牢な基盤を構築しました。

Impact:

BeeKeeperAIは、新生ヘルスケアAIの汎用化能力とFDA承認を達成するための新たなプロセスを構築しています。同社のシステムは、患者データへのユーザーによるアクセスを許可しないため、基準を満たすために必要なデータへのアクセスを18カ月も短縮しています。

Carbon Asset SOLUTIONS

Customer:
Carbon Asset Solutions

Industry:
Partner Professional Services

Size:
Small (1–49 employees)

Country:
Australia

Products and services:
Microsoft Azure
Microsoft Azure confidential computing
Microsoft Azure DevOps
Microsoft Azure Key Vault
.Net Framework

Read full story here

Microsoft

"私たちは、土壌炭素の測定・記録・検証のサプライチェーンにおいて、新興のボランタリーカーボン市場に参入する最大のプレーヤーになろうとしています。つまり、グローバルに効率よく拡張できるシステムが必要なのです。マイクロソフトには、私たちが必要とするツールがすべて揃っています。"

—Ian Jones, Chair and Cofounder, Carbon Asset Solutions

Situation:

カーボンアセットソリューションズ（CAS）は、農家が炭素を固定する持続可能な農法を実践し、CO2排出量を削減するプログラムを通じて、気候変動に挑みたいと考えている。この新しい分野で、CASのビジョンである「不変の炭素クレジット」を実現するための方法を欲していた。

Solution:

CASは、Microsoft Azure Confidential Computing とAzure の Confidential Ledger 技術を利用して、土壌炭素データと炭素クレジットを非公開かつ改ざんされにくいものにしています。これらの技術は、Azure.NET Framework、Azure DevOpsツールセットとシームレスに連動します。

Impact:

創業から3年、CASは市場に出ようとしています。炭素排出量を削減しながら、世界中の農村の生活と財政を改善するという共同設立者の夢は実現し、気候変動と戦う世界の未来を明るく照らし出そうとしています。

Confidential Computing の幅広い選択肢

Confidential VMs and AKS node pools

Confidential GPUs
Leverage GPUs for large AI/ML needs

SQL Server & AVD Conf VMs
Defense-in-depth on existing solutions

Confidential Containers

Azure Container Instances
Lift and shift apps to serverless containers

Intel SGX OSS + Partner solutions
Leverage ISVs to deploy containers in app enclaves
Https://aka.ms/ACC-Intel-Partner

Enclave-Aware Apps

Open Enclave SDK
Utilize HW-based TEEs with custom C++ code

Confidential Consortium Framework
OSS framework for secure multi-party compute/data

Built-for-purpose Services

Azure Key Vault Managed HSM
Microsoft Azure Attestation
Azure SQL Always Encrypted in secure enclaves
Azure Confidential Ledger
Managed CCF (Limited Preview)

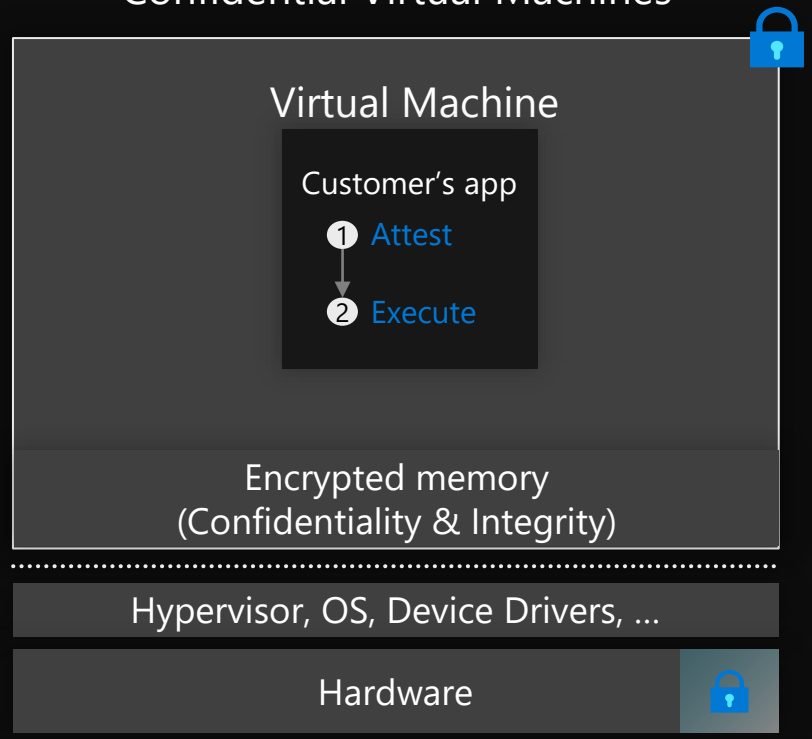
従来のアプリケーションを
そのまま容易に利用する

より細かく厳密なコントロールを
新たに実装する

CPU Trusted Execution Environments (TEEs) in Azure

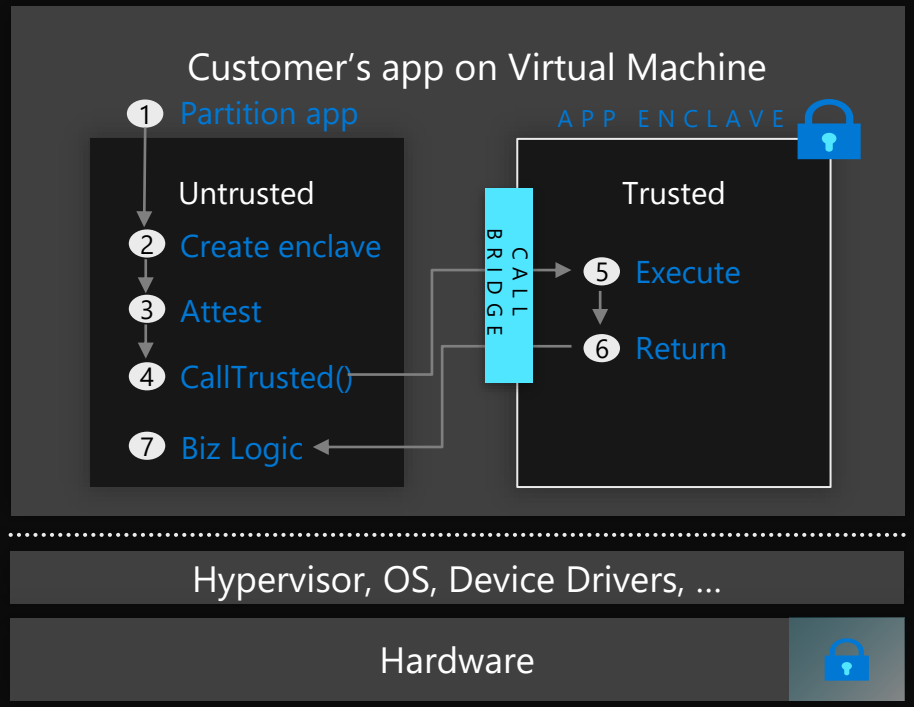
AMD

Confidential Virtual Machines



intel

VMs with App Enclaves



2段階の暗号化

RAM 上の VM のメモリ領域の暗号化+ OS ディスクの事前暗号化

- ハイパーバイザ、ホスト OS 、他 VM からの 分離
- 利用中のメモリ領域の暗号化
- OS 領域は Azure により事前暗号化可能
- OS ディスクの暗号化は 複数の鍵管理手法から選択可能

2段階のメモリ暗号化

RAM 上の VM のメモリ領域の暗号化+ アプリの特定処理における EPC メモリ

- アプリケーションによる特定モジュールの 分離の実現
- 利用中のメモリ領域の暗号化
- 鍵により自動で 通常のメモリ領域を暗号化
- 既存コンテナアプリの ISV と OSS エコシステム によるデプロイ

Availability: Now

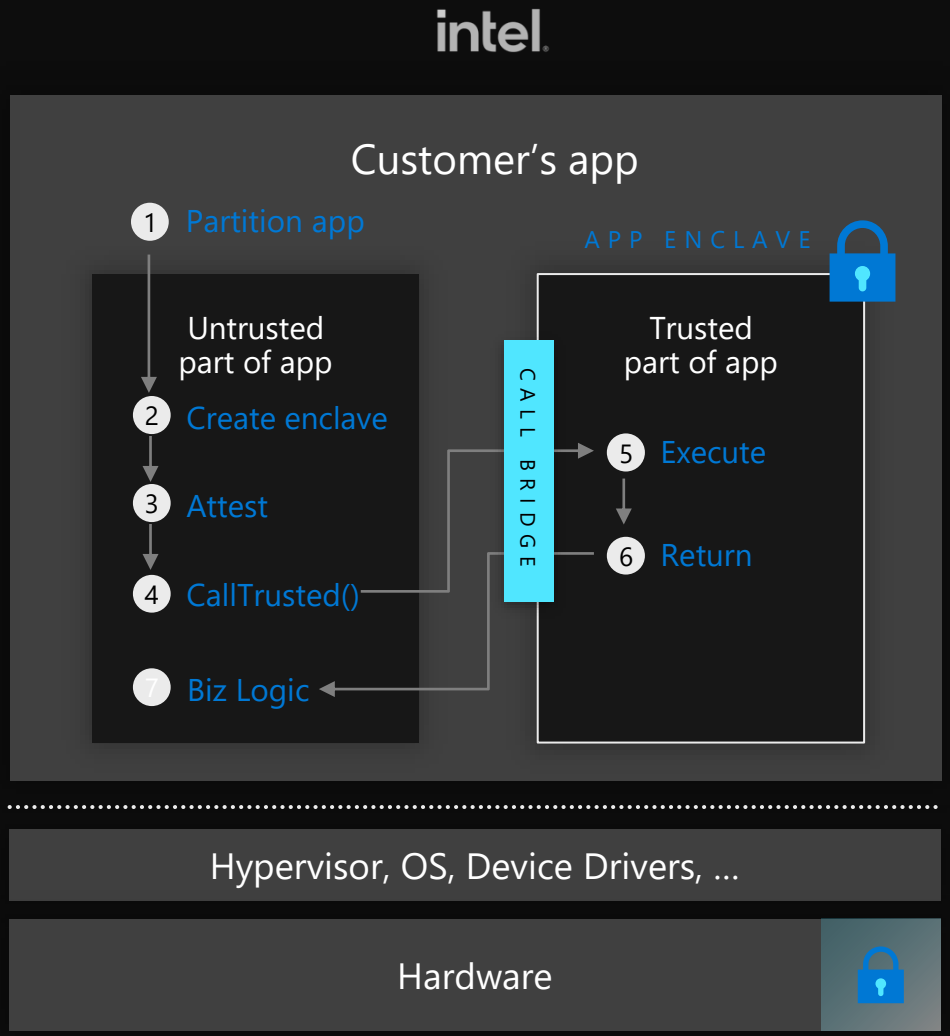
App Enclaves with Intel SGX

データのプライバシーと制御を、アプリケーションのコード一行単位で可能とする、最高レベルの堅牢さ

DCsv2, DCsv3 series

アプリ単位でのデータ保護の実現	Intel SGX と TME-MK によるメモリ暗号化	以前のバージョンから 1500 倍に増えた EPC メモリ

3rd Generation Intel® Xeon Scalable confidential processors



Availability: Limited Preview

Azure Managed Confidential Consortium Framework (CCF)

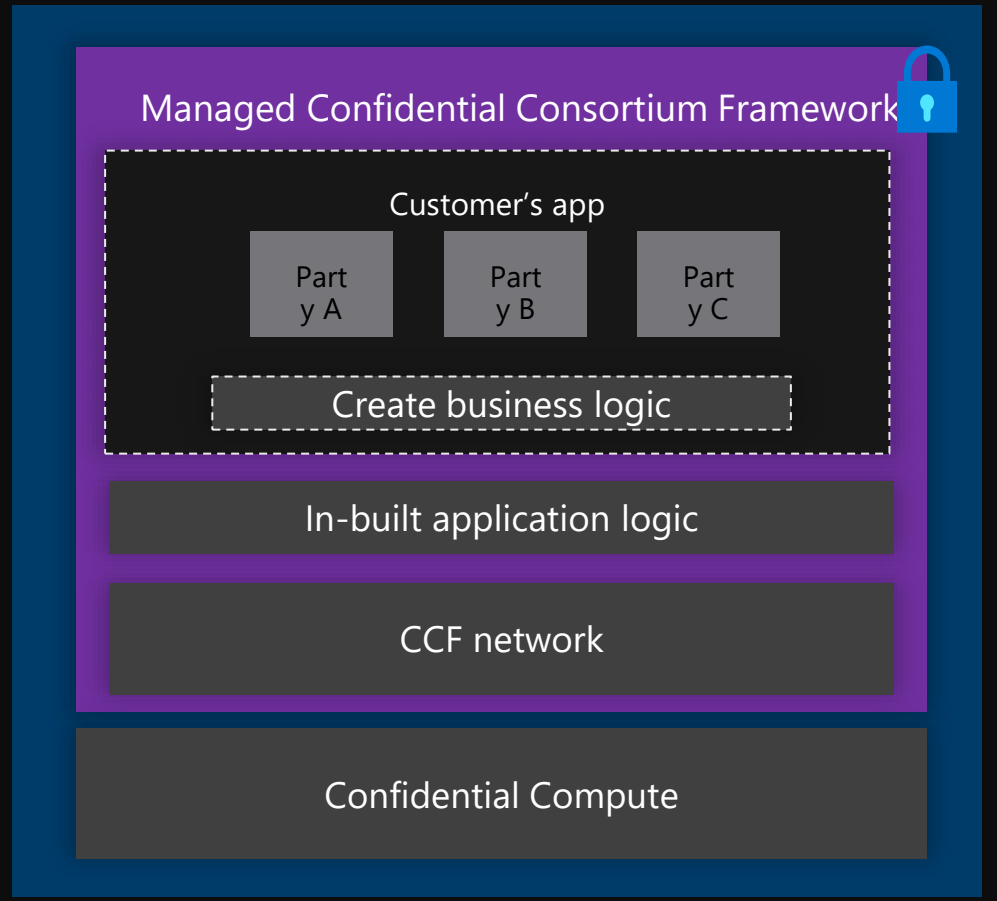
秘密計算ベースのステートフルサービスを迅速に構築するための
マネージドフレームワーク環境

分散処理のための集約された機能、プログラマブルな秘匿性

依存関係の低減により、
市場提供速度を向上

検証可能ネットワーク上に CCF
対応のアプリケーションをデプロイ

複数パーティでの利用のための
コンソーシアム形式のガバナンス



Confidential Computing の幅広い選択肢

Confidential VMs and AKS node pools

Confidential GPUs
Leverage GPUs for large AI/ML needs

SQL Server & AVD Conf VMs
Defense-in-depth on existing solutions

Confidential Containers

Azure Container Instances
Lift and shift apps to serverless containers

Intel SGX OSS + Partner solutions
Leverage ISVs to deploy containers in app enclaves
Https://aka.ms/ACC-Intel-Partner

Enclave-Aware Apps

Open Enclave SDK
Utilize HW-based TEEs with custom C++ code

Confidential Consortium Framework
OSS framework for secure multi-party compute/data

Built-for-purpose Services

Azure Key Vault Managed HSM
Microsoft Azure Attestation
Azure SQL Always Encrypted in secure enclaves
Azure Confidential Ledger
Managed CCF (Limited Preview)

従来のアプリケーションを
そのまま容易に利用する

より細かく厳密なコントロールを
新たに実装する

Microsoft