Microsoft

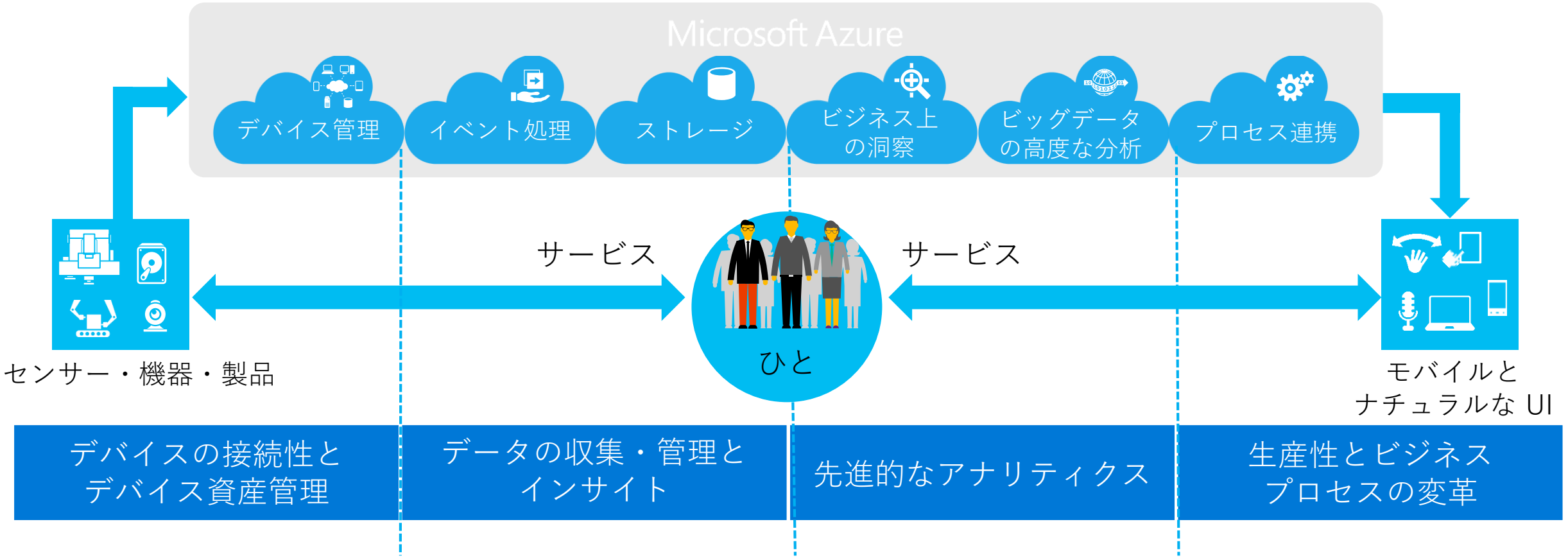
Network Security Forum 2019
IoT時代の「トラスト」は何か？

IoT プラットフォーム セキュリティ

垣内 由梨香
セキュリティ プログラム マネージャ
セキュリティ レスポンス チーム, Asia-Pasific
Microsoft Corporation
CISSP

IoT 基盤

モノと人をデジタルにつなぎ、クラウドの力でスケーラブルなサービスとして素早く展開する



セキュアなデバイスに必要な7要素：7 Properties

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

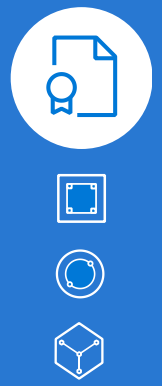
セキュリティ メカニズムが破られてもデバイスは保護されるか？

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？

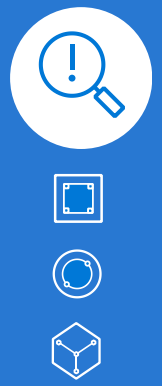
Dynamic Compartments

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？

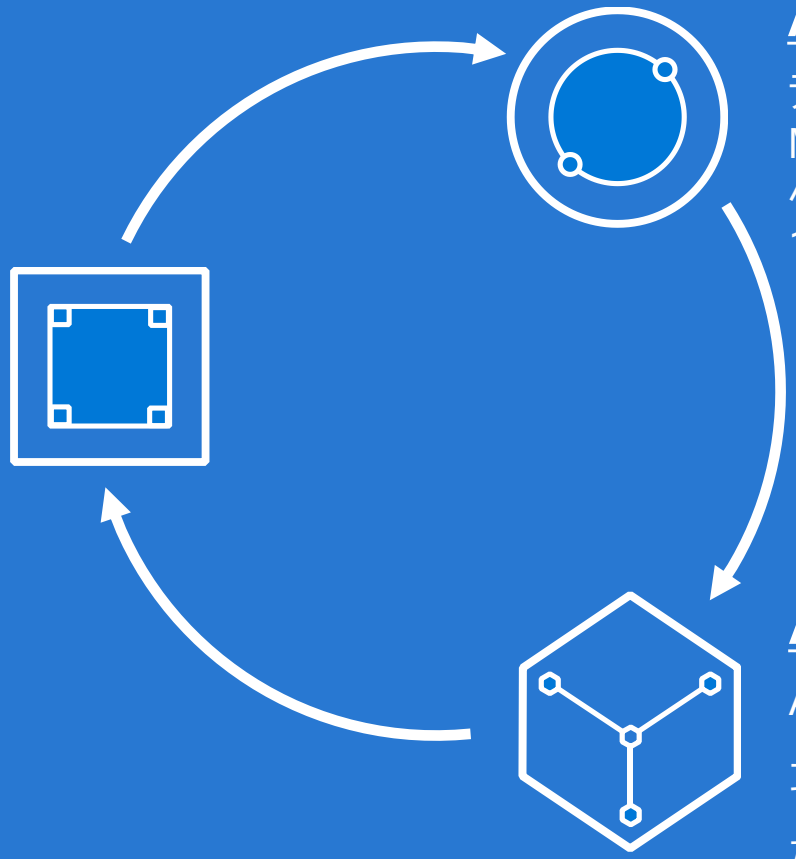
Renewable Security

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？

Azure Sphere

Azure Sphere Certified MCU

Microsoftのシリコンパートナーが製造するマイクロコントローラで、Microsoft Researchが提唱するハードウエアセキュリティ基準に準拠しているかどうかをMicrosoftが認定している



Azure Sphere OS

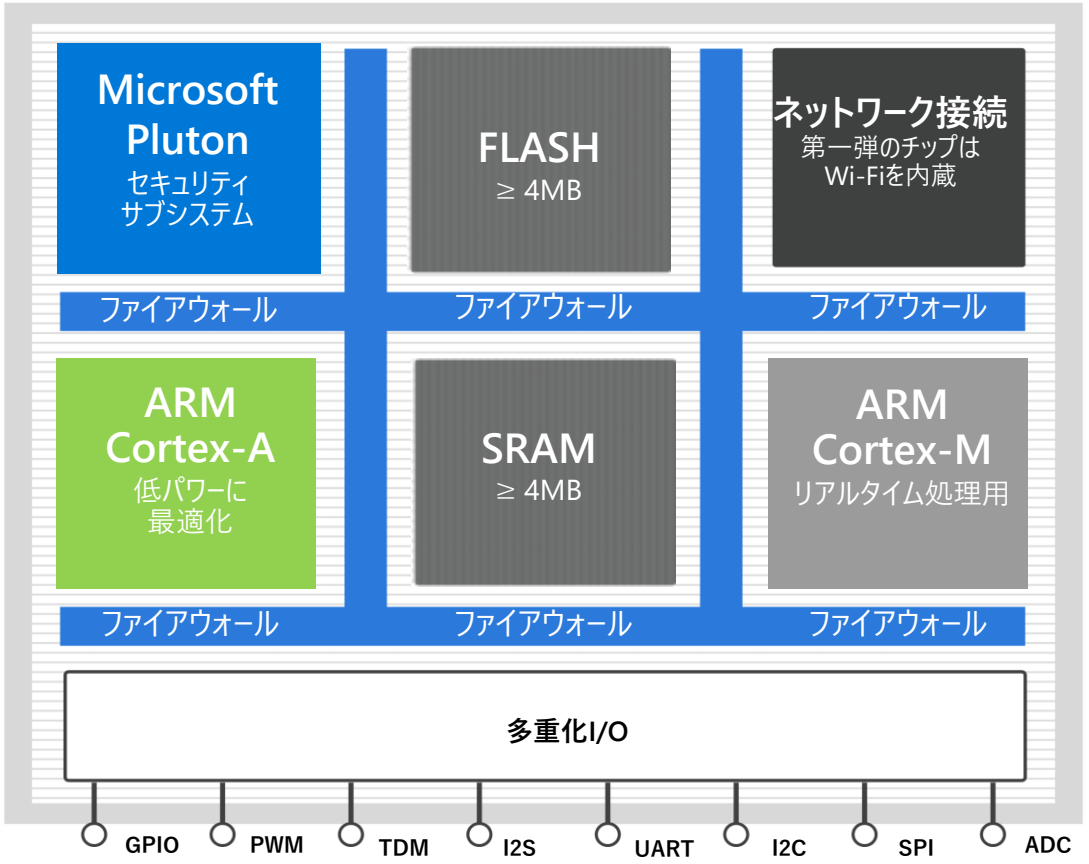
デバイスの10年間の耐用年数に渡ってMicrosoftがセキュリティ保護するLinuxベースの新しいOS. クラウドサービス経由で10年間のOSアップデートが保証される

Azure Sphere Security Service

Azure Sphere OS のアップデートを行い、またOS上で稼働するPOSIXアプリのデプロイを行うことができる。もしハードウエアレベルでの脅威が発見された場合、動作を遠隔で止める

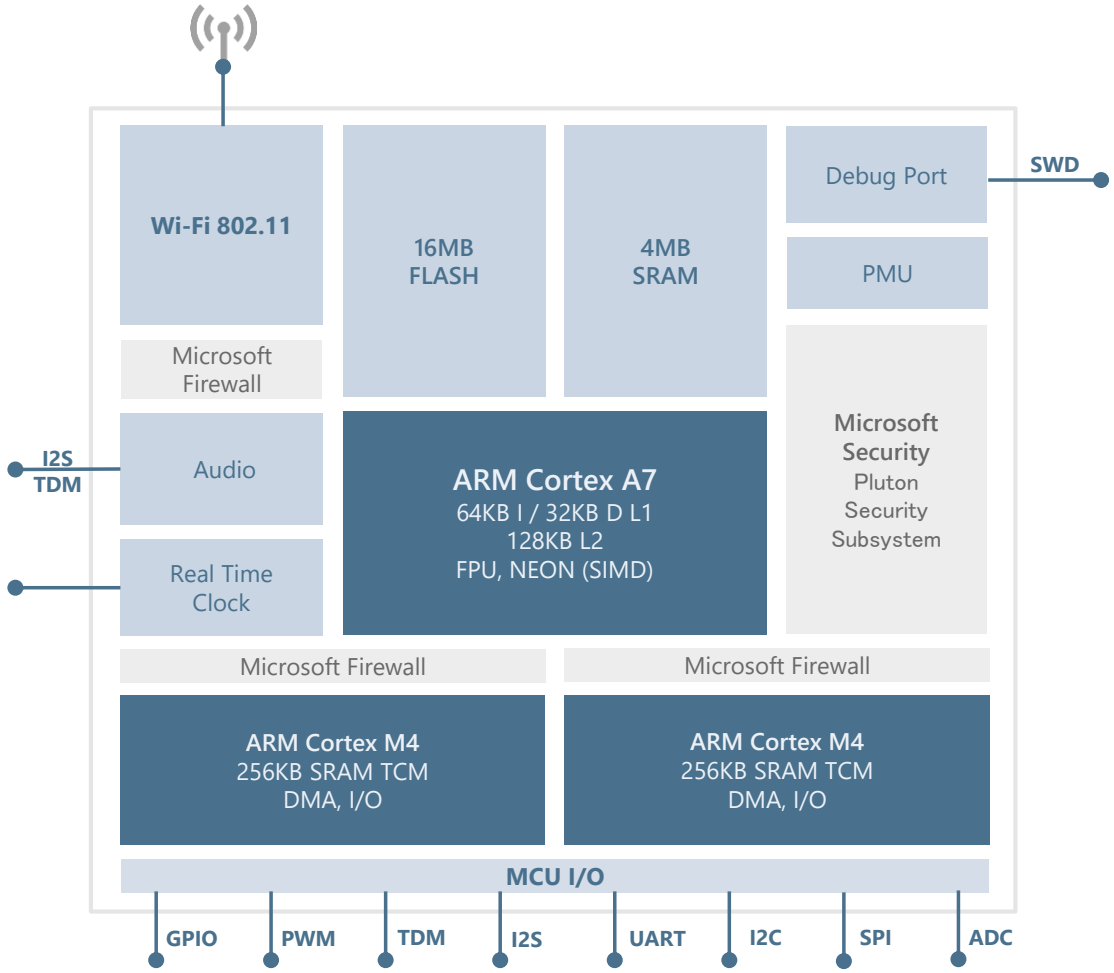
Azure Sphere MCU

- 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



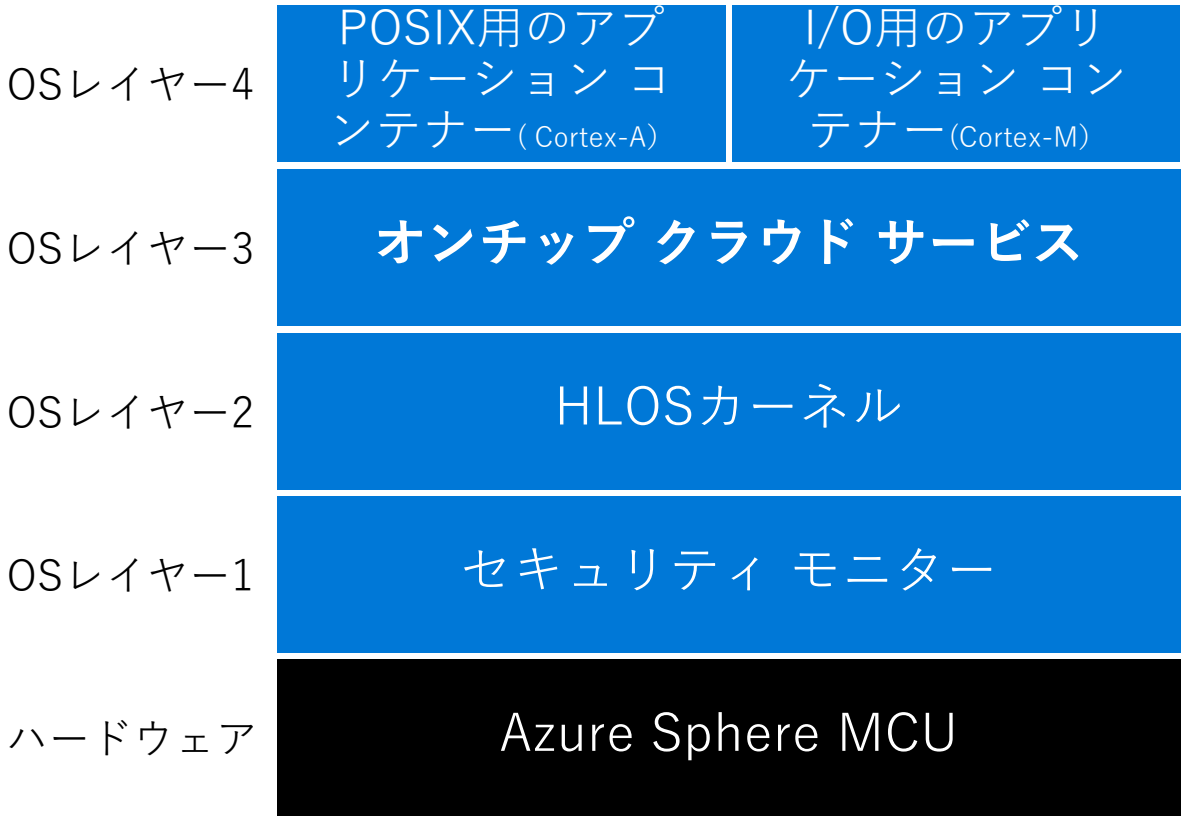
Azure Sphere MCU : MediaTek MT3620

CPUs		**ARM Cortex A7 (500MHz) + 2 x Cortex M4 (192MHz)**
RAM		4MB
Flash		16MB (8MB Runtime Firmware + 8MB Backup Firmware)
Connectivity		WiFi 802.11 b/g/n, dual band: 2.4GHz, 5GHz
Microsoft Security		Firewalls, Crypto Accelerator: AES-256, SHA-2, ECC, RSA2K, e-Fused private and public keys, attestation, …
I/O	GPIO	24, 4 configurable as PWM
	SPI	6 configurable
	I2C	
	UART	
	ADC	8 Channels, 12bit SAR, 2M sample/sec
I2S/TDM		I2S (2 interfaces) or TDM (4 channels)
Package		DR-QFN 164
Target Price		



Azure Sphere OS

Azure Sphere OSアーキテクチャ



安全なアプリケーション コンテナー
アジリティ、安定性、セキュリティを確保するためにコンパートメント化されたコード

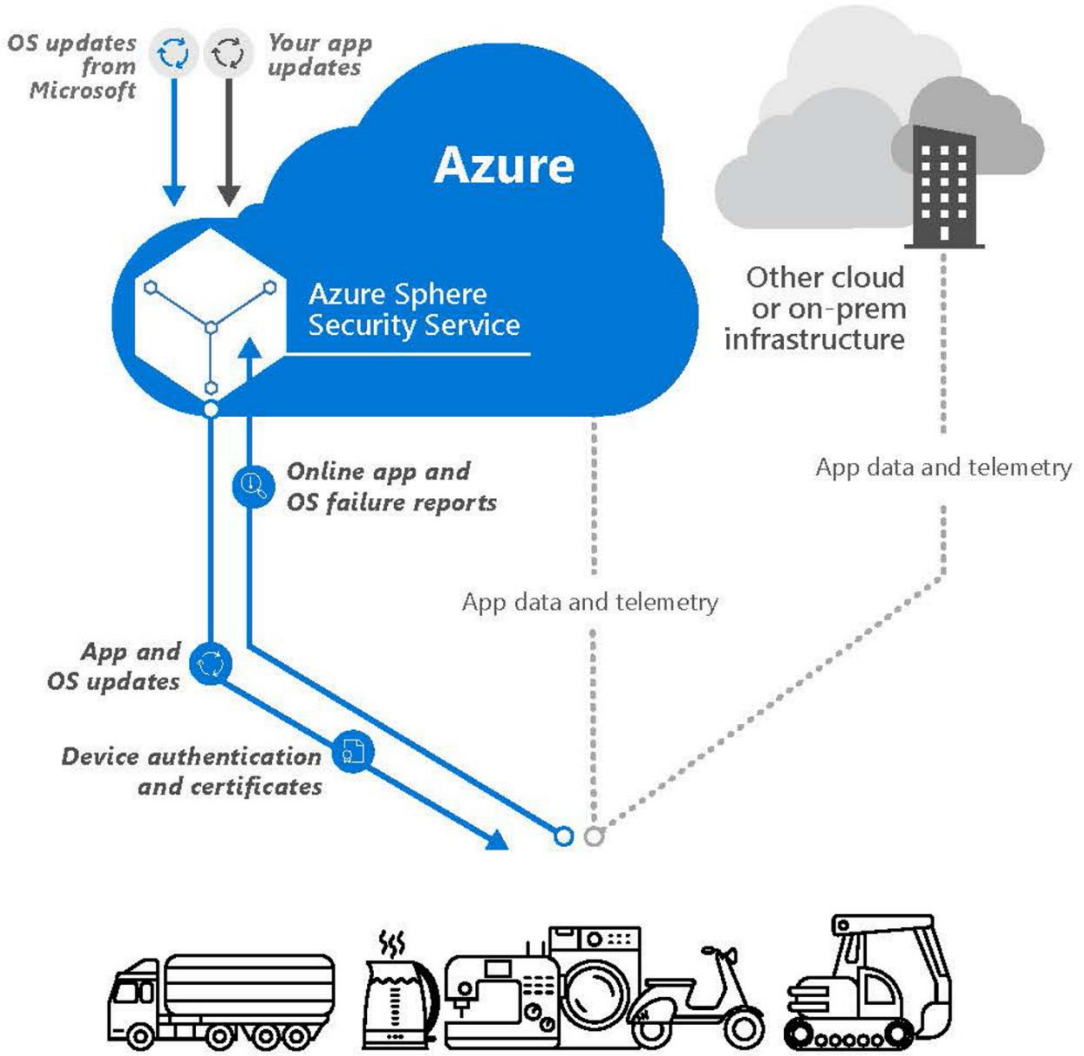
オンチップ クラウド サービス
アップデート、認証、接続性を提供

カスタムLinuxカーネル
アジャイルなシリコンの進化とコードの再利用を実現

セキュリティ モニター
重要なリソースの完全性とアクセスを保護

Azure Sphere Security Service

- すべての通信の証明書ベースの認証でデバイスと顧客を**保護**
- オンデバイス障害の自動処理を通じて新しいセキュリティ脅威を**検知**
- OSの完全に自動化されたオンデバイスアップデートで脅威に**対応**
- Azure Sphere搭載デバイスへのソフトウェア アップデートのデプロイが可能



Let’s secure the future.

SECURED FROM THE SILICON UP

Microsoft

© Copyright Microsoft Corporation. All rights reserved.