



Azure Sphere: セキュアなIoTの 実現を目指して

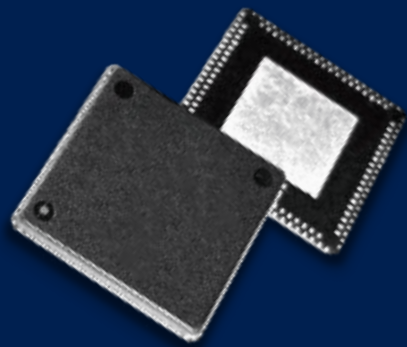
～ Securely unlocking IoT for your Enterprise～

日本マイクロソフト株式会社
IoTデバイス本部
テクニカルスペシャリスト
梅津 尚枝



マイクロコントローラ

安価, シングルチップコンピュータ



90億

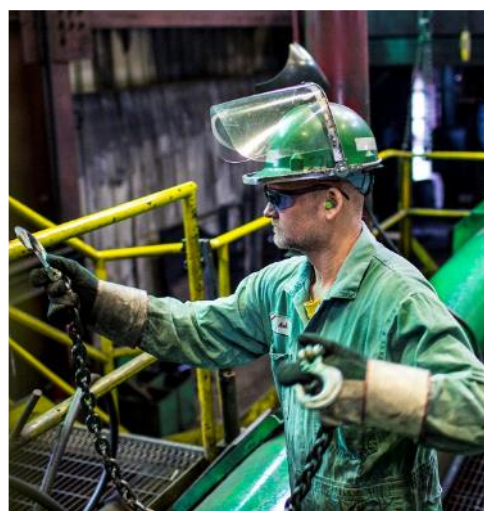
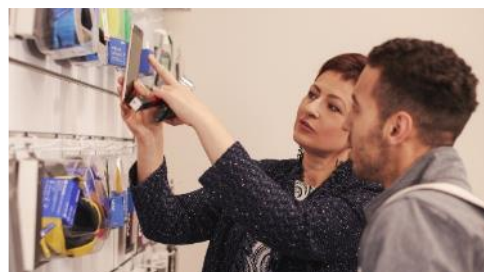
1 年間で誕生するMCUの数

データ分析

運用効率

新しいビジネスモデル

カスタマエクスペリエンス





ビジネスの可能性 | リスク

**“2018にはもっとランサム
ウェアがデバイスへの攻
撃を開始する”**

**“Huge IoT botnet may be
used for Ukraine attack”**

**“気付かないうちにスマート
機器を通して監視されるこ
とになるかもしれない”**

**“Industrial IoT to equip new era
of corporate intruders coming
in through devices”**

**“Security experts warn
of dangers of connected
home devices”**

**“子供のおもちゃのモニ
ターからは子供の遊び以
外の情報を取得している
かもしれない”**

**“Hackers infect 500,000
consumer routers all over
the world with malware”**

**“Your smart fridge may kill
you: The dark side of IoT”**

**“The Lurking Danger of
Medical Device Hackers”**

**“Why the KRACK Wi-Fi mess
will take decades to clean up**

**“Hacking critical infrastructure via a
vending machine? The IOT reality”**

**“家族を守るはずのセキュリティデ
バイスは、ハッカーの入り口かも
しれない”**

Mirai Botnet attack

デバイス経由で一日中インターネットへの攻撃を仕掛ける

対象は10万個のデバイス

弱点を悪用した攻撃

早期検出あつてのリモートアップデート



Hackers attack casino

カジノの魚の水槽タンクに侵入しカジノのデータベースへ

ネットに接続された温度計から侵入

一度侵入することで他の脆弱性を発見

その脆弱性からデータベースへ潜入

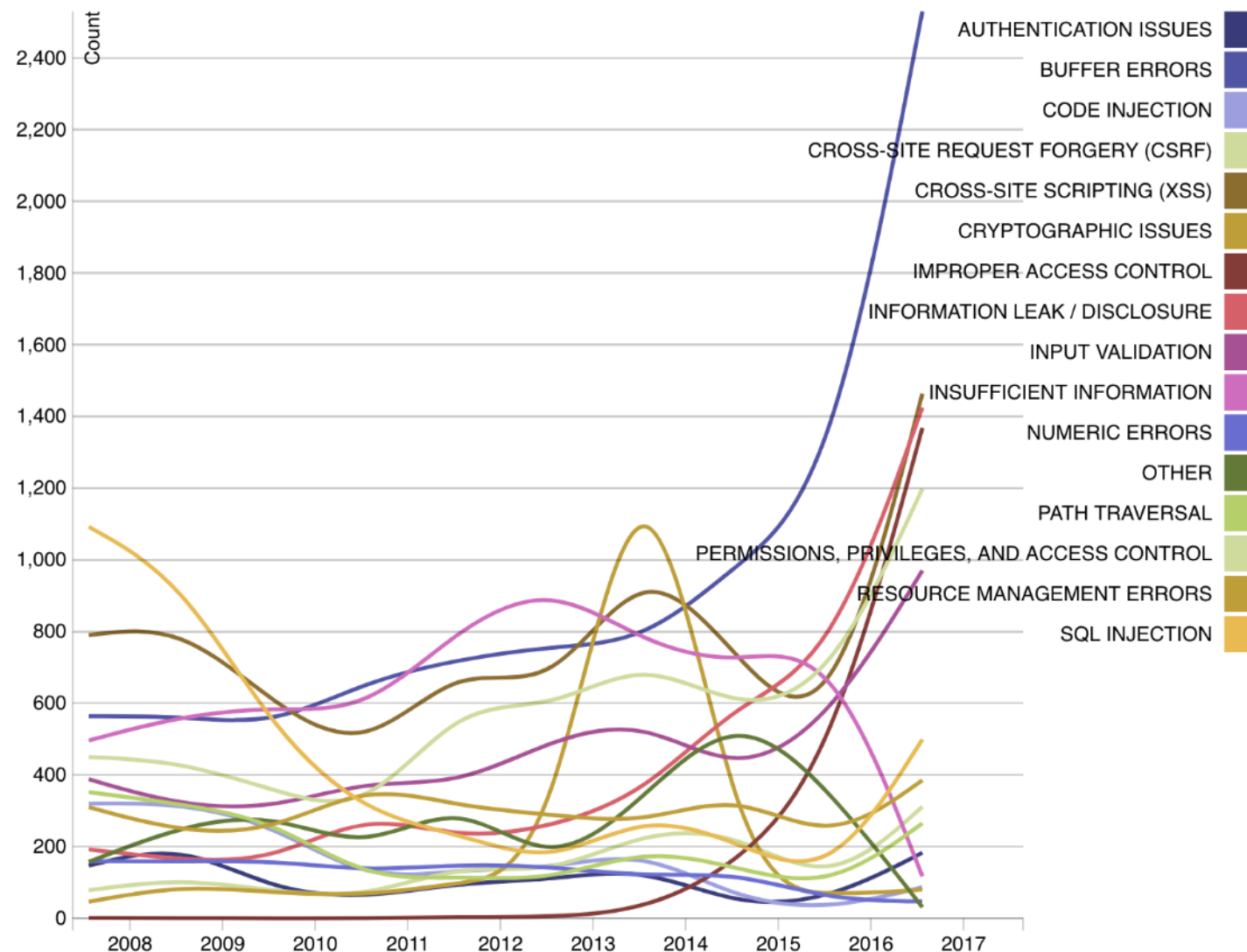


lessons & learned ...

製品と脆弱性

セキュリティ脆弱性の原因に関する
NISTの調査レポート
(2008-2017年)

ハッカーは常に攻撃箇所を探しています



セキュリティリスクと価値の損失

どのようなことが発生するか？

- デバイスが使用不能
- 攻撃者によるデバイスの制御
- デバイスの機能を悪意目的で利用
- データ & プライバシーの侵害
- デバイスプラットフォームの保護無効
- 攻撃者によるデバイスのマルウェア感染

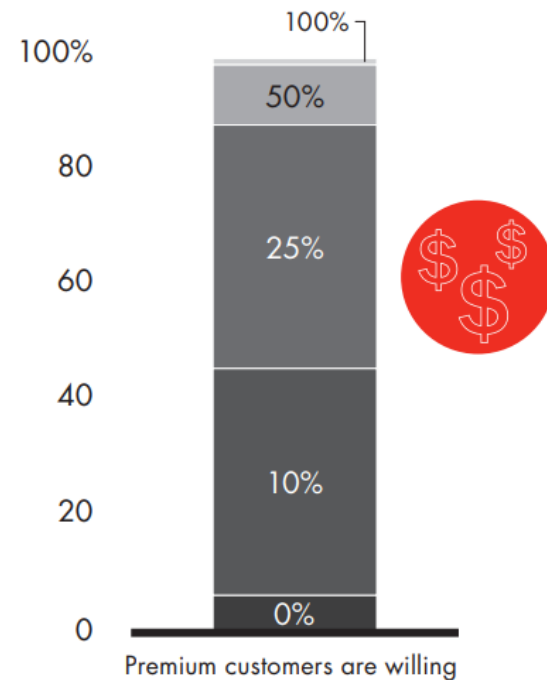
コストインパクト

- ブランドインパクト（信頼の喪失）
- 信頼回復にかかるコスト
- 法的責任
- ダウンタイム
- セキュリティフォレンジック

セキュリティについての企業の声

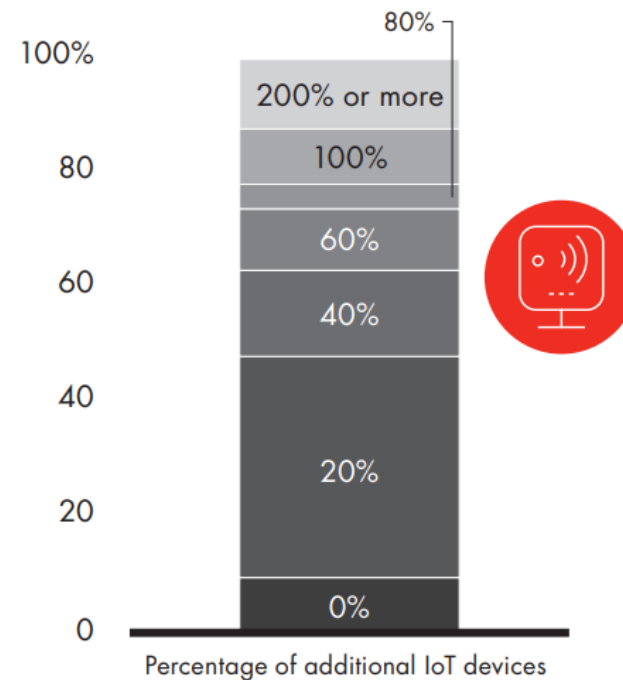
Customers would pay an average of 22% more for secure IoT devices ...

Percentage of respondents



... and would buy an average of 70% more IoT devices if they were secure

Percentage of respondents

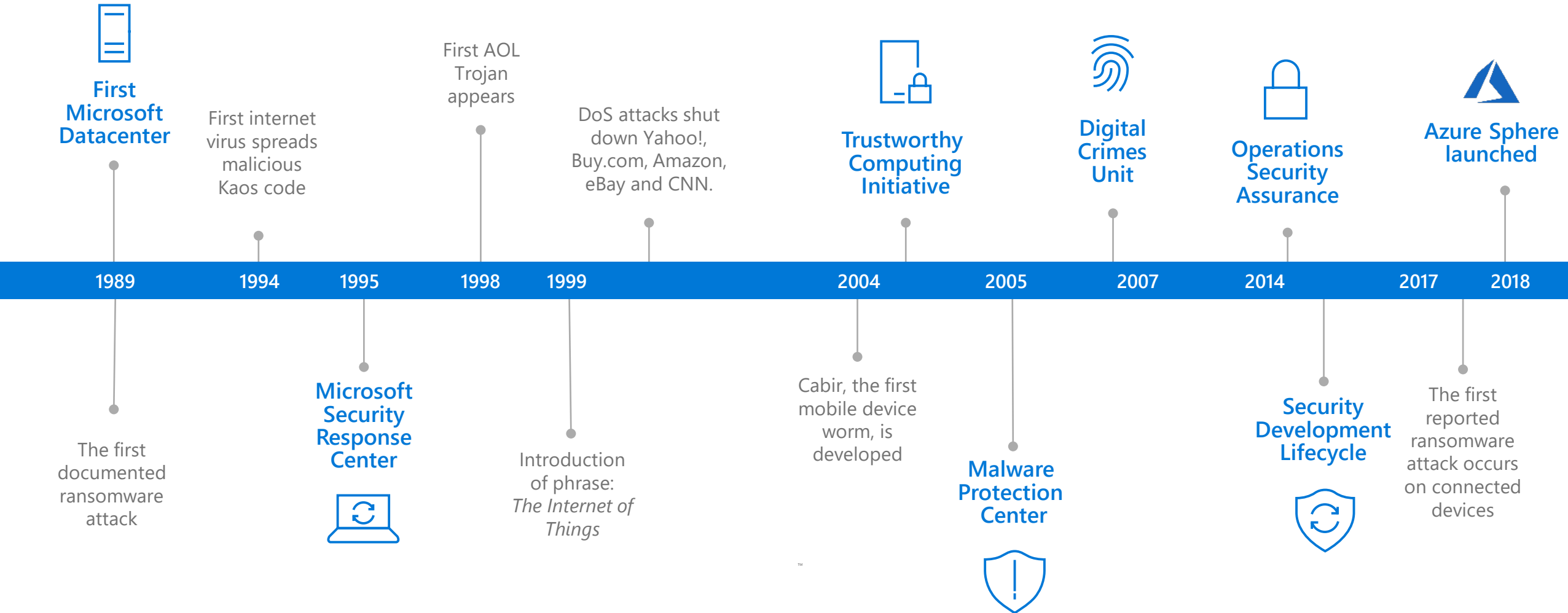


Premiums and greater sales would boost the IoT cybersecurity market by \$9 billion to \$11 billion in 2020

22% 「サイバーセキュリティに対して支払いをいとわない」
70% 「セキュアが保証されればデバイスを購入する」

Microsoftのトラストコンピューティングヒストリー

Microsoft は 25 年以上前からお客様とデバイスを守り続けてきました



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？



 = 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

<https://aka.ms/7properties>

セキュアなデバイスに必要な 7 要素 : 7 Properties

ハードウェア 信頼性の根源



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？



深層防衛



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？



スモールトラステッド コンピューティング ベース



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？



ダイナミック コンパートメント



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？



証明書ベース認証



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？



障害・異常の レポーティング



デバイスは障害や異常を報告するか？



リニューアブル セキュリティ



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？



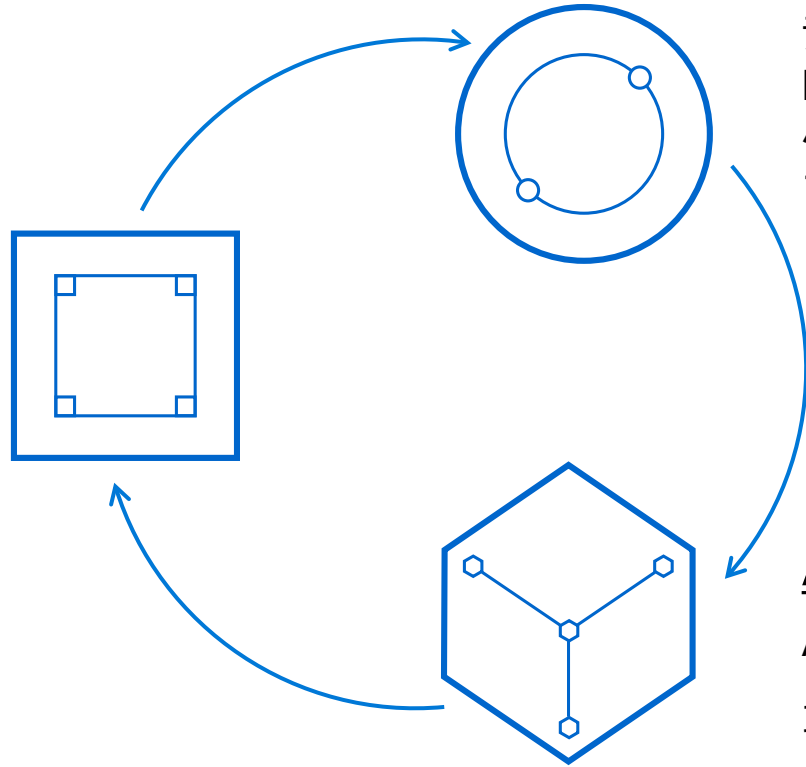
 = シリコンのサポートが必要  = OSのサポートが必要  = クラウドサービスのサポートが必要

<https://aka.ms/7properties>

Azure Sphere を構成する3要素

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ェ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

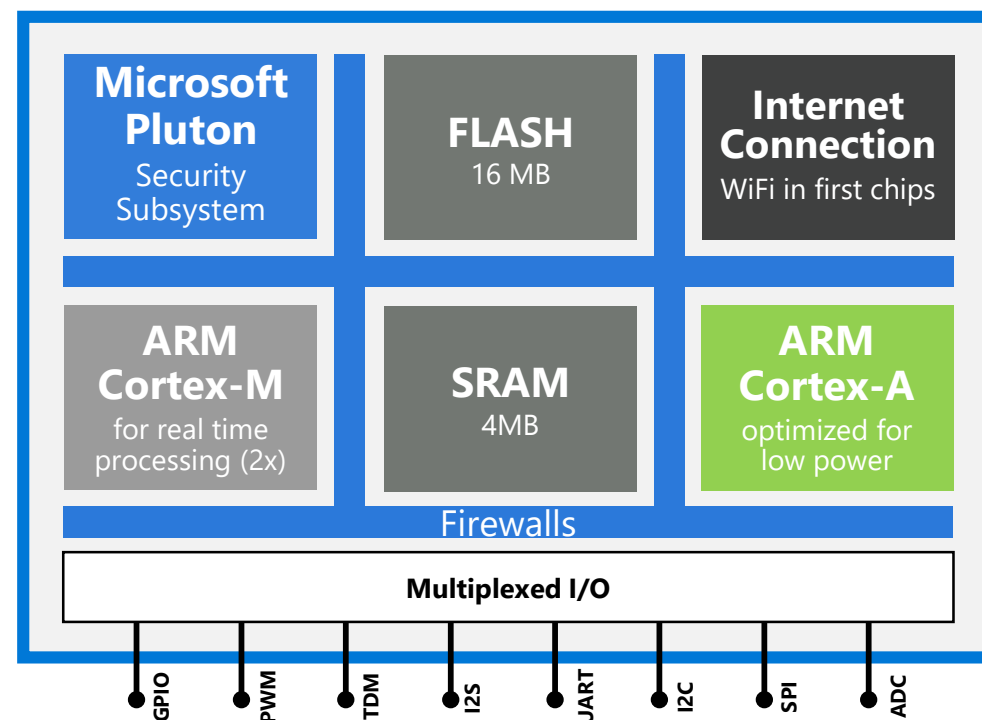
Azure Sphere OS のアップデートを行い、またOS上で稼働するPOSIXアプリのデプロイを行うことができる。もしハードウェアレベルでの脅威が発見された場合、動作を遠隔で止める

Azure Sphere セキュアチップ

- 組み込み済みのネットワーキング接続
- Pluton Security Subsystem
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
リッチなプロセッサMCUで実現

First chip: MediaTek MT3620

Highly-Secured & Connected



The Azure Sphere Security Service

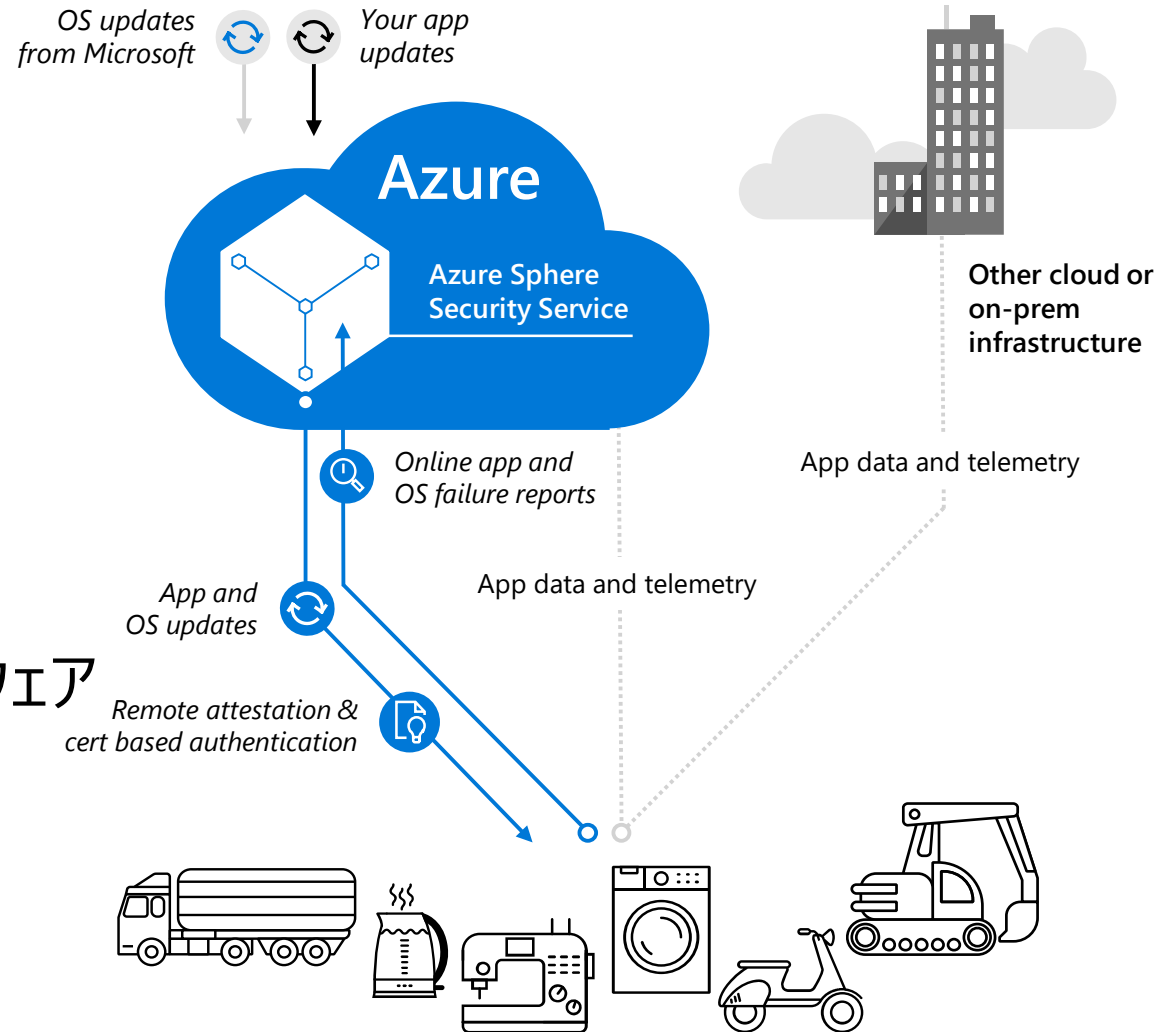
Azure Sphereがネットワークに接続したデバイスを保護

証明書ベースの認証でデバイスを**保護**

オンデバイス障害の自動処理により
新しい脅威を**検知**

自動化されたオンデバイスアップデートで
脅威に素早く**対処**

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**



Azure Sphere: Best-in-Class Support for 7 Properties

	Component	\$\$	Hardware Root of Trust	Small TCB	Defense in Depth	Compartmentalization	Certificate-based Auth.	Renewable Security	Failure Reporting
Traditional MCU	Espressif ESP32	\$							
	RealTek RTL8710	\$							
	Marvell 88MW300/2	\$							
	Qualcomm QM 4010	\$							
	MediaTek MT7687	\$							
	ARM mBed CMv8+CryptoCell	\$							
	BCM 43907	\$							
	TI CC3220	\$							
4X 4	Azure Sphere MT3620	\$\$							
SoCs	Allwinner GR8	\$\$\$							
	Qualcomm QCM8016	\$\$\$							
	Samsung ARTIK 530	\$\$\$							
	Intel Atom x5-E3930	\$\$\$							
Xbox	Xbox	\$\$\$							
	Xbox 360	\$\$\$							
	Xbox One	\$\$\$							

processes. Certificate-based Authentication: AAD-equivalent w/ isolated keys.
Renewable Security: Rollback-protected update. Failure Reporting: WER-equivalent

Two types of implementations

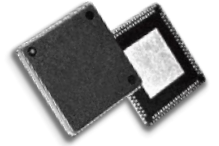


Our growing ecosystem of HW partners

MEDIATEK

Azure Sphere certified MCUs

Our silicon foundation delivered through a growing ecosystem of chip manufacturers



AVNET

Development kits

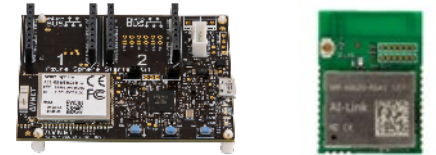
Help organizations prototype quickly



seeed studio

Modules

Speed up time to market for device makers

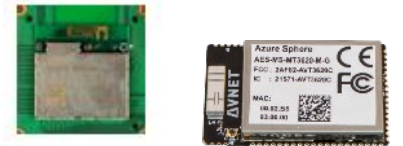


AI-Link

USI

Guardian Modules

Enable secure brownfield IoT



innodisk

InnoAGE™ SSD For AIoT Devices

The World's 1st hybrid SSD with Azure Sphere inside



Guardian Module embedded by Japan Partners



COWBELL ENGINEERING CO., LTD.

ConverloT Guardian Module



Cactasphere Guardian Module

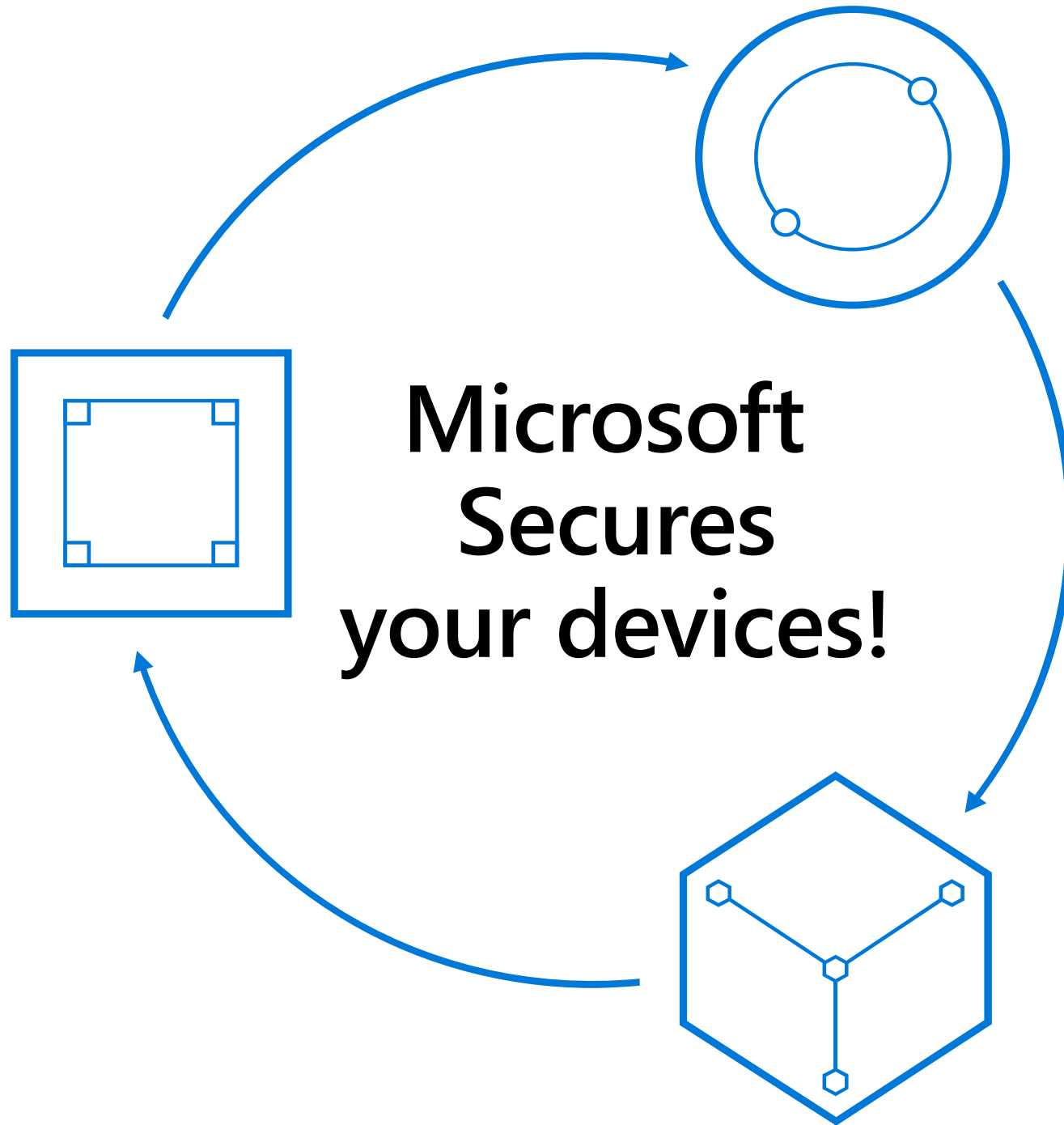




STARBUCKS

StarbucksはAzure Sphereを活用することで
ビジネスの戦略を迅速に実現しています

- ・コストセーブ：
マシンのメンテナンスを必要な時に提供
- ・顧客満足：
日々完成度の高いコーヒーを提供
- ・新しいサービスの提供：
シーズンに沿ったレシピをエスプレッソマシンに配信



Thank you !

Using our Pluton security subsystem royalty **free for use** in any chip*
You are free to innovate with our GPL'd OSS Linux kernel code base
You are free to connect to Azure or any other cloud, proprietary or public for application data