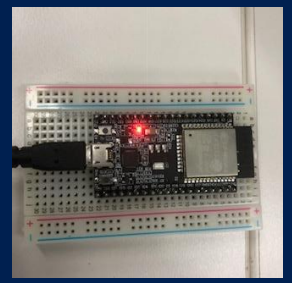
Microsoft

セキュアなIoTを構築する技術 -- Azure Sphere、対 Azure IoT Hubの場合

日本マイクロソフト株式会社
エバンジェリスト
太田　寛
Twitter:　@embedded_george

自己紹介

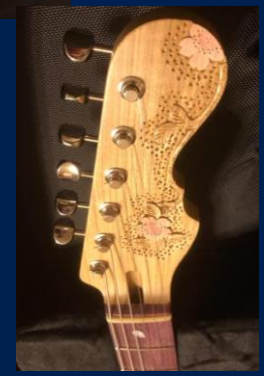




日本マイクロソフト株式会社
エバンジェリスト

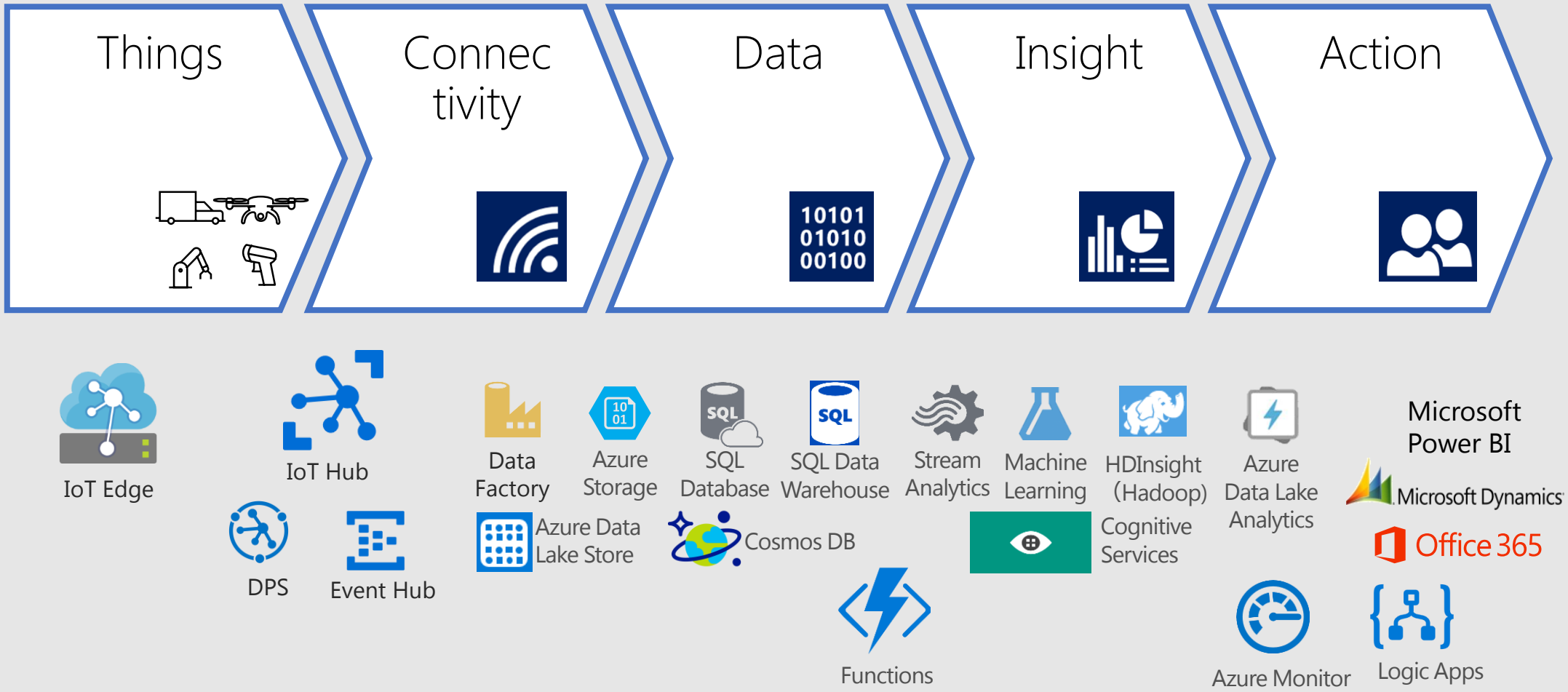
Twitter @embedded_george
前職は組込みSW技術者
Azure全般、特にIoTを普及啓発！
http://aka.ms/IoTKitHoLV4

Big Data Stream系も今後力を入れていきます！
http://aka.ms/letsbegin - MS Learnもよろしく

歴オタ、御朱印集め、ギター好き

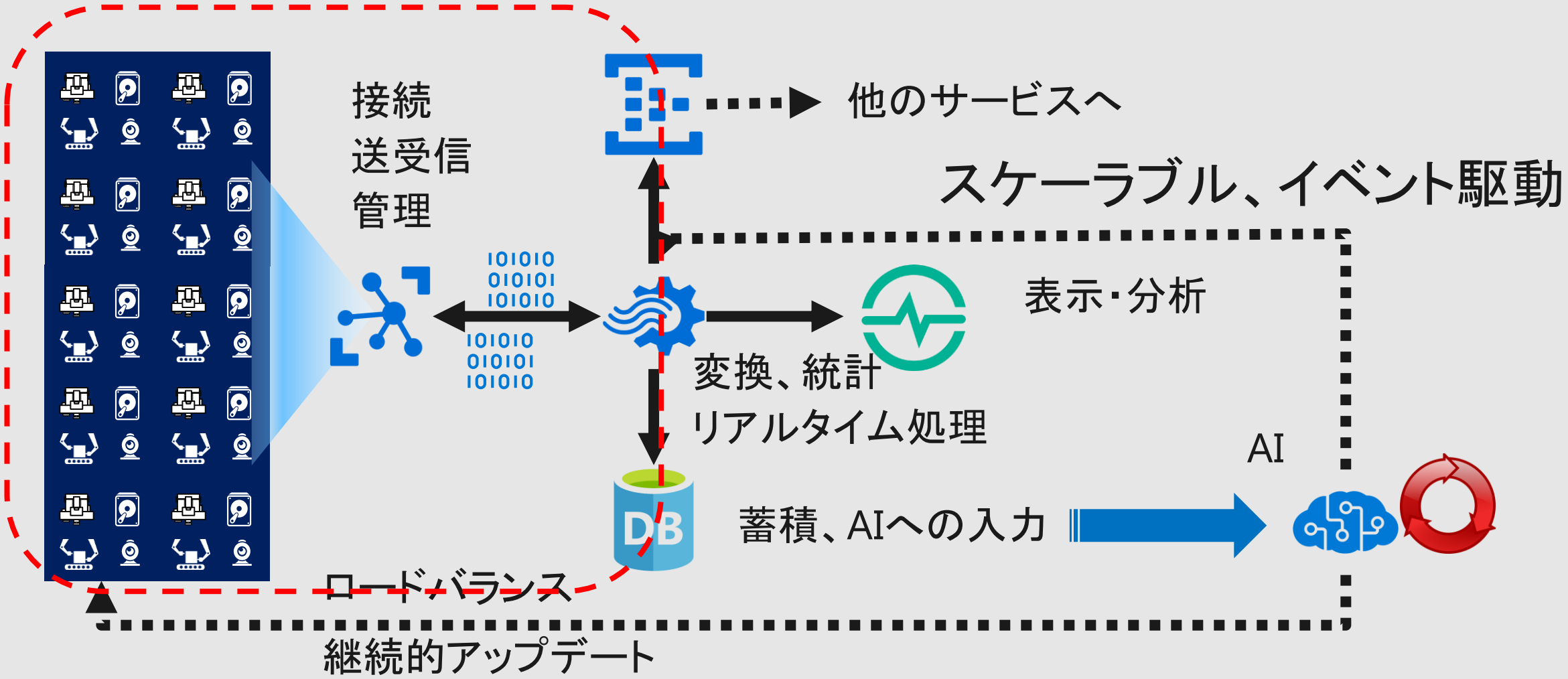
Azureで IoTを実現する



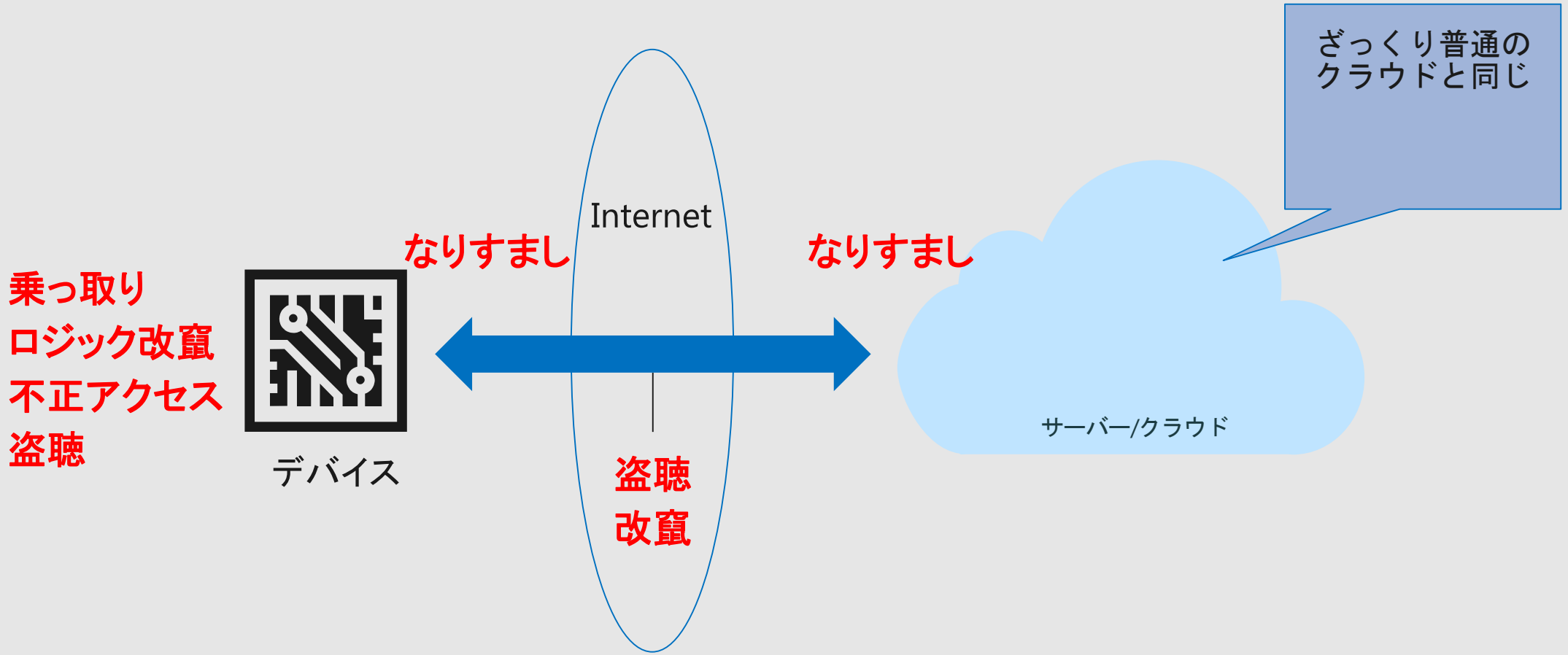
エンドツーエンドをカバーする、様々なサービス群

膨大なデバイスの接続・通信・管理とビッグデータ

- 多くの機器が同時に稼働&リアルタイムデータ処理システム

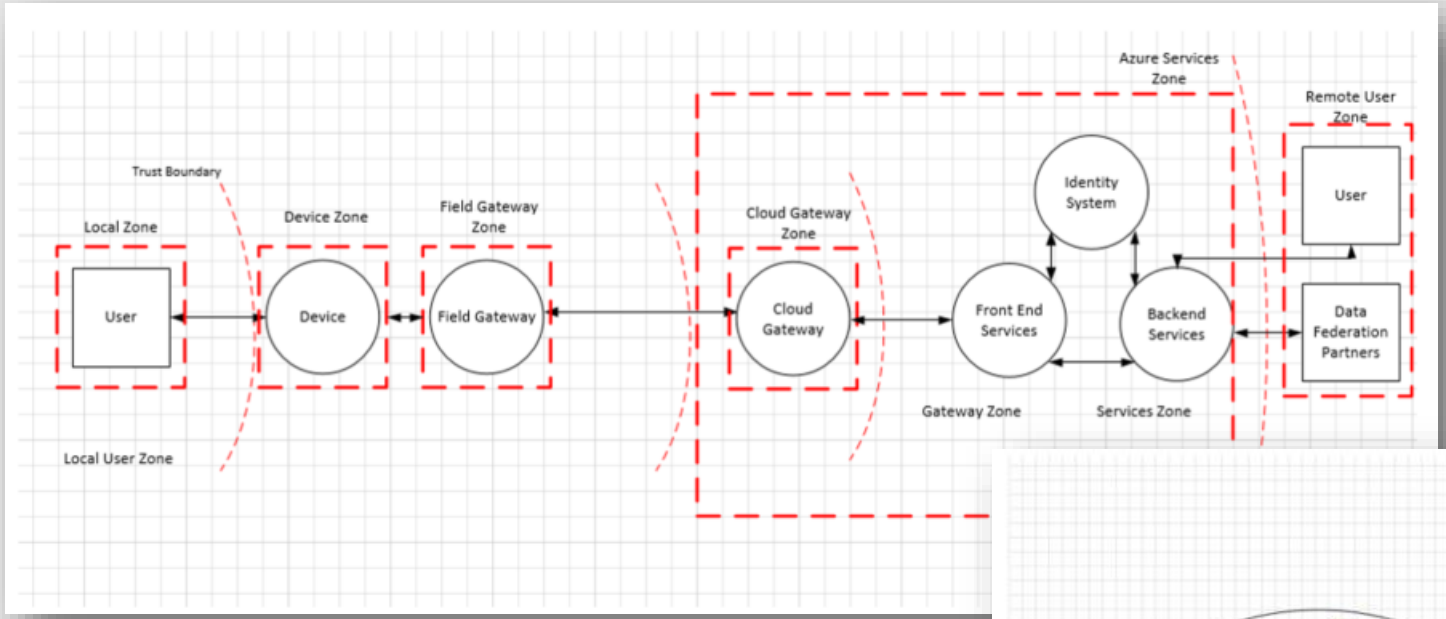


IoTにおける脅威


ざっくり普通の
クラウドと同じ
Internet
なりすまし
なりすまし
乗っ取り
ロジック改竄
不正アクセス
盗聴
デバイス
盗聴
改竄
サーバー/クラウド

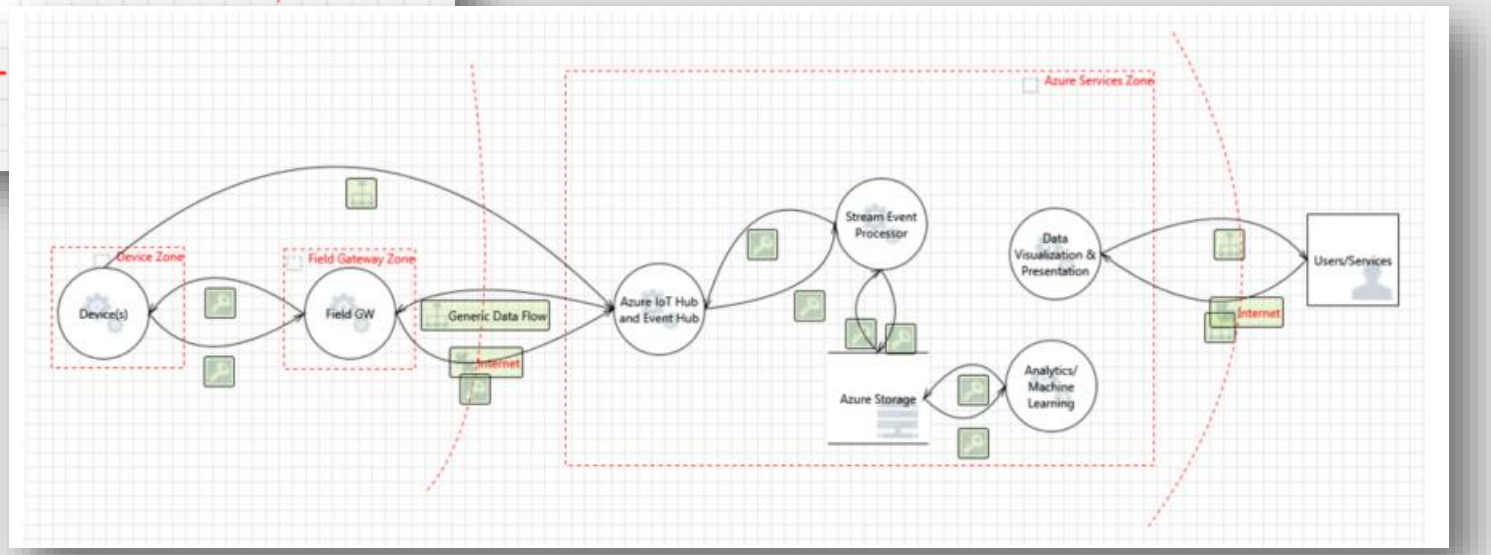
参考 – IoT Security Architecture

https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture



STRIDE model

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

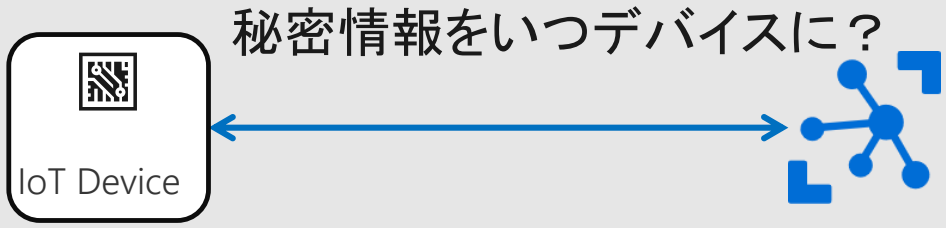


- Processes
- Communication
- Storage

参考- Microsoft Security Development Lifecycle https://www.microsoft.com/en-us/securityengineering/sdl/

セキュアなデバイス接続

デバイス毎のセキュアな接続
- デバイスIDと秘密鍵（SASToken)による接続
- デバイスIDとX509証明書による接続

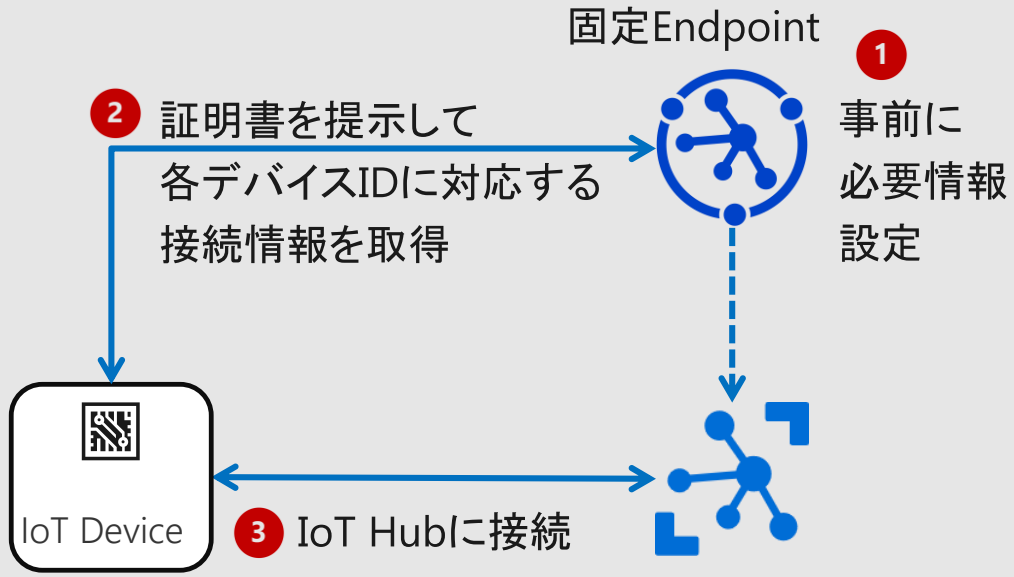


通信プロトコル
- HTTPS
- AMQPS
- MQTTS

SSL、TSLの層で暗号化

デバイスの登録
- ポータルで手動
- APIでプログラマブル
- 一括登録
- エクスポート/インポート
- 接続デバイスの Enable/Disable

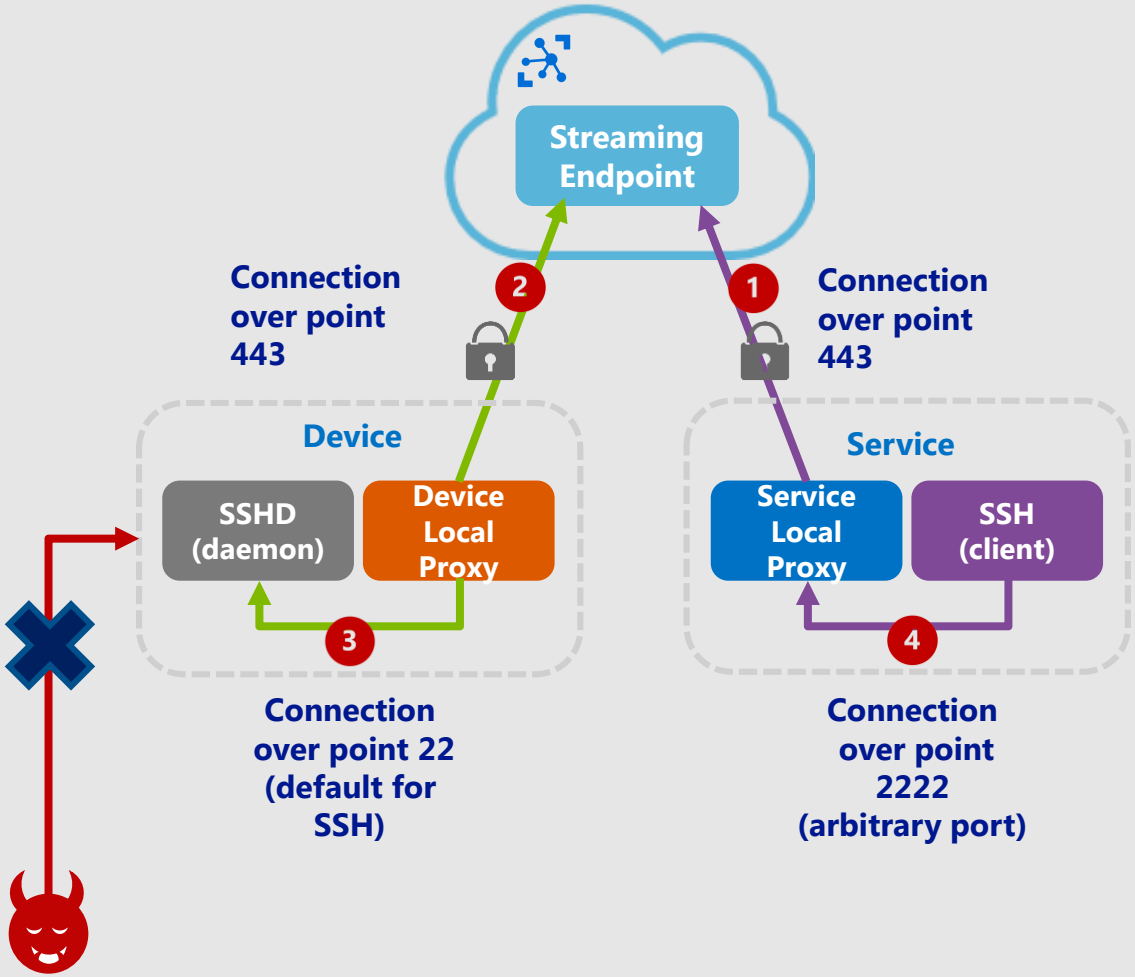
Device Provisioning Serviceを使った自動接続
- X509証明書による事前接続情報設定
- デバイス設置時のセキュアな接続情報取得



サービスとデバイス間での接続情報をセキュアに交
- デバイスへの事前登録なし
- フレキシブルなデバイス設置を実現

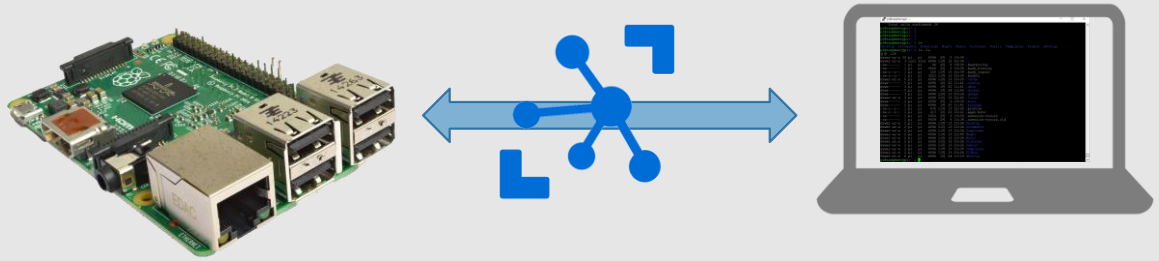
超セキュアに、デバイスのシェルに、リモートから接続

Device Stream

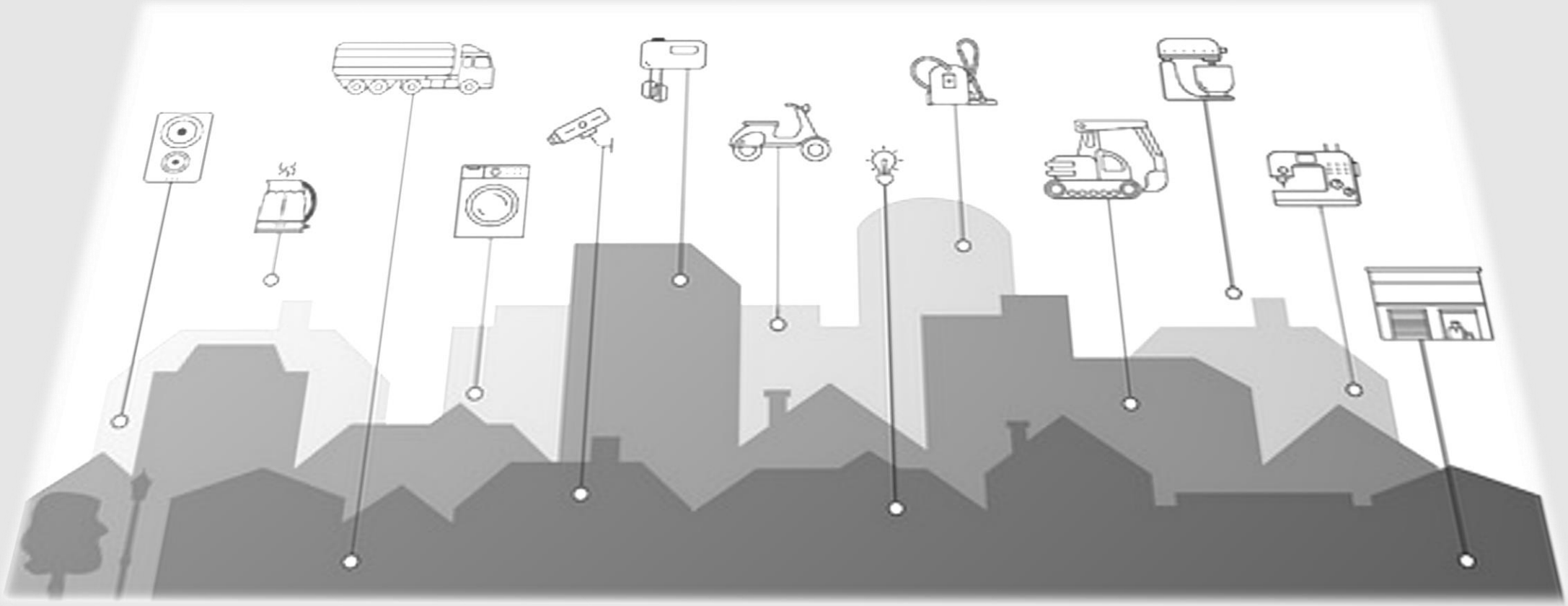


IoT Hubを介して、セキュアにSSH接続可能
セキュリティ情報の最小限化

その他のアクセスは拒否！



デバイス（ハードウェア）のセキュリティ ⇒ Azure Sphere



“Highly-secured connected devices”に要求される7つの特徴

Hardware Root of Trust

デバイスアイデンティティとソフトウェアの一貫性はハードウェアで保障されているか？

Defense in Depth

たとえセキュリティ機構が破られても、保護可能なままか？

Small Trusted Computing Base

デバイスのTCBは、アプリその他のコードのバグから守られているか？

Dynamic Compartments

デバイス導入後にセキュリティ保持機構を改善することが可能か？

Certificate-Based Authentication

デバイスは認証でパスワードの代わりに証明書を使うか？

Failure Reporting

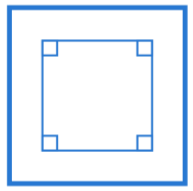
デバイスは障害や異常をレポートするか？

Renewable Security

デバイスは自動的にソフトウェアのアップデートを行うか？

= Silicon support required = OS support required = Cloud Service support required

幾つかの特徴は、ハードウェアでしか対処できない



Hardware Root of Trust

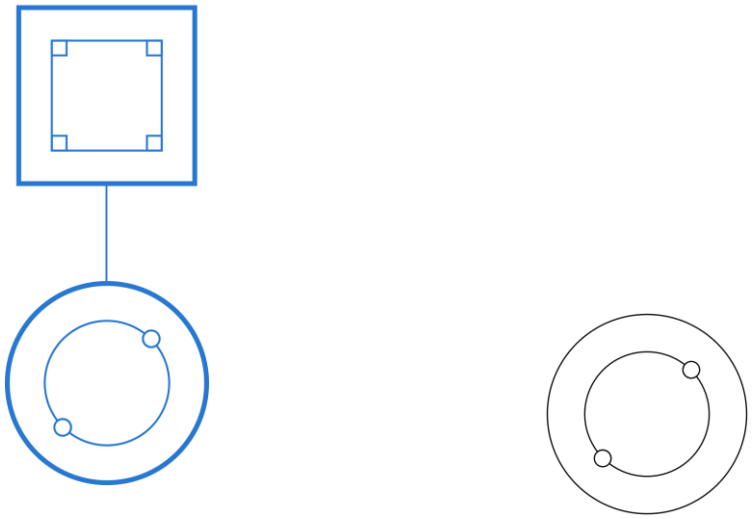
偽造暗号キーの生成防止は
ハードウェアで

デバイスのアイデンティティとソフトウェアの一貫性はハードウェアで確保されるか？

- ハードウェアが**デバイスアイデンティティを守る**
- ハードウェアが**セキュアブートを提供**
- ハードウェアが**システムの一貫性を証明**

© Microsoft Corporation

幾つかの特徴は、ハードウェア、ソフトウェア両方に依存



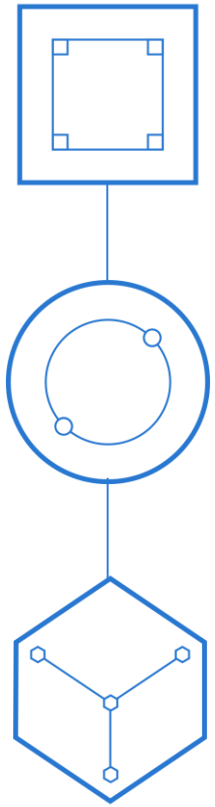
Dynamic Compartments

どんな障害の波及も内部バリアがブロックする

デバイスは配置後にセキュリティプロテクションを改善できるか？

- ハードウェアが<u>バリアを生成</u>
- ソフトウェアが<u>コンパートメントを生成</u>

© Microsoft Corporation



幾つかの特徴は、ハードウェア、ソフトウェアに加え、クラウドも必要

Renewable Security

デバイスセキュリティを、新たに出現した脅威やセキュリティ侵害に対して、
リニューアル

デバイスは自動的にソフトウェアアップデート可能か？

- クラウドが**アップデートを供給**
- ソフトウェアが**アップデートを適用**
- クラウドは**ロールバックを防ぐ**

© Microsoft Corporation

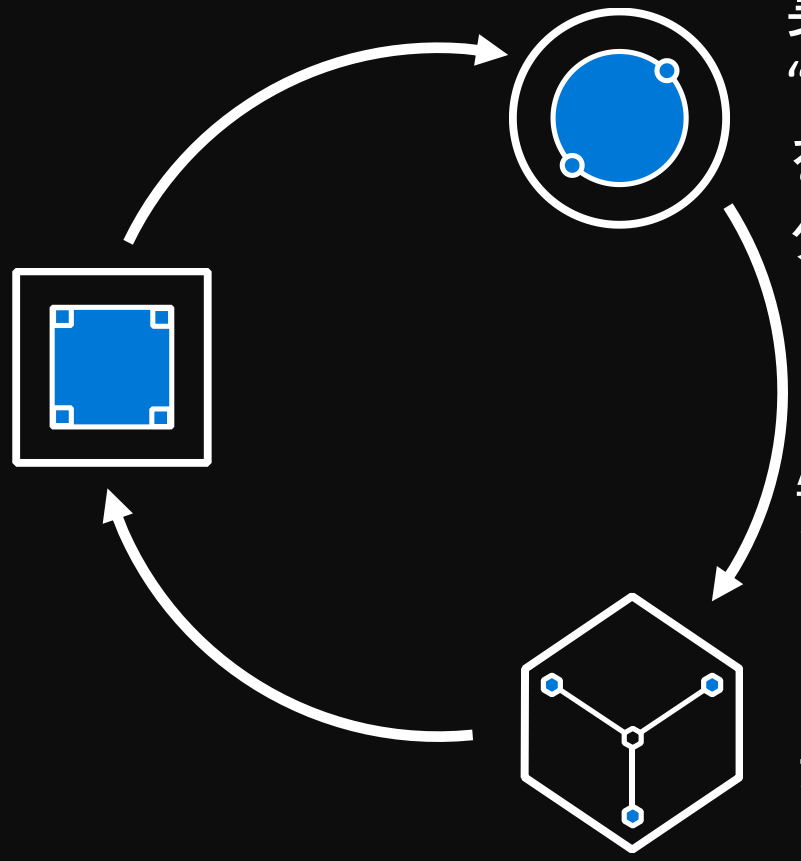
Microsoft
The Seven Properties of Highly Secure Devices

https://www.microsoft.com/en-us/research/publication/seven-properties-highly-secure-devices/

© Microsoft Corporation

Azure Sphere はエンドツーエンドのソリューション

Azure Sphere OS
新しいIoTエクスペリエンスを実現する
“信頼されたプラットフォーム”を作るために、10年間のライフタイムを提供する



Azure Sphere 対応 MCU
接続性と信頼された”Hardware Root of Trust” を提供するマイクロソフトのセキュリティテクノロジーが組み込まれた状態でシリコンパートナーから提供される

Azure Sphere Security Service
全てのAzure Sphereデバイスをガードする; D2D、D2C通信に対する信頼されたブローカー、新たな脅威の検知、デバイスセキュリティの更新を提供

© Microsoft Corporation

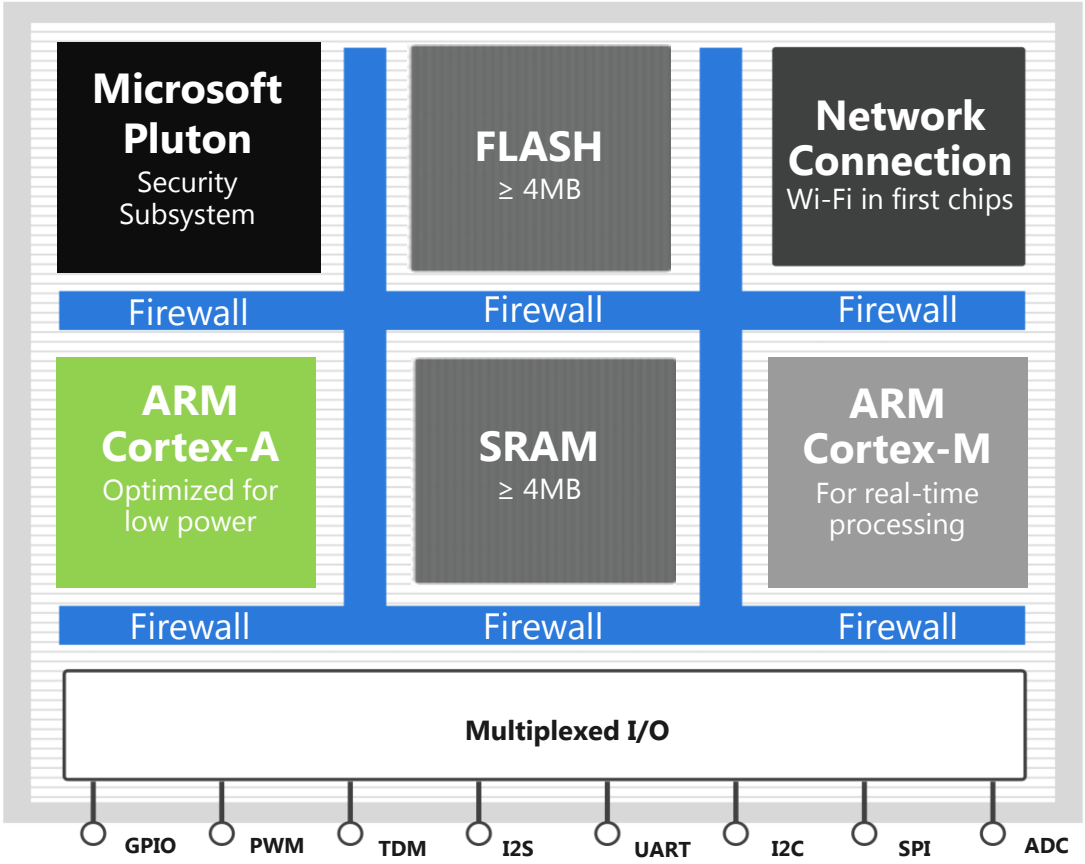
Azure Sphere MCU

Connected Intelligent Edgeに対し、”secured root of trust”を創出

コネクテッド
ビルトインされたネットワーク機能

セキュアード
ビルトインされたマイクロソフトのシリコンセキュリティ技術。Microsoft Pluton セキュリティサブシステムを内包

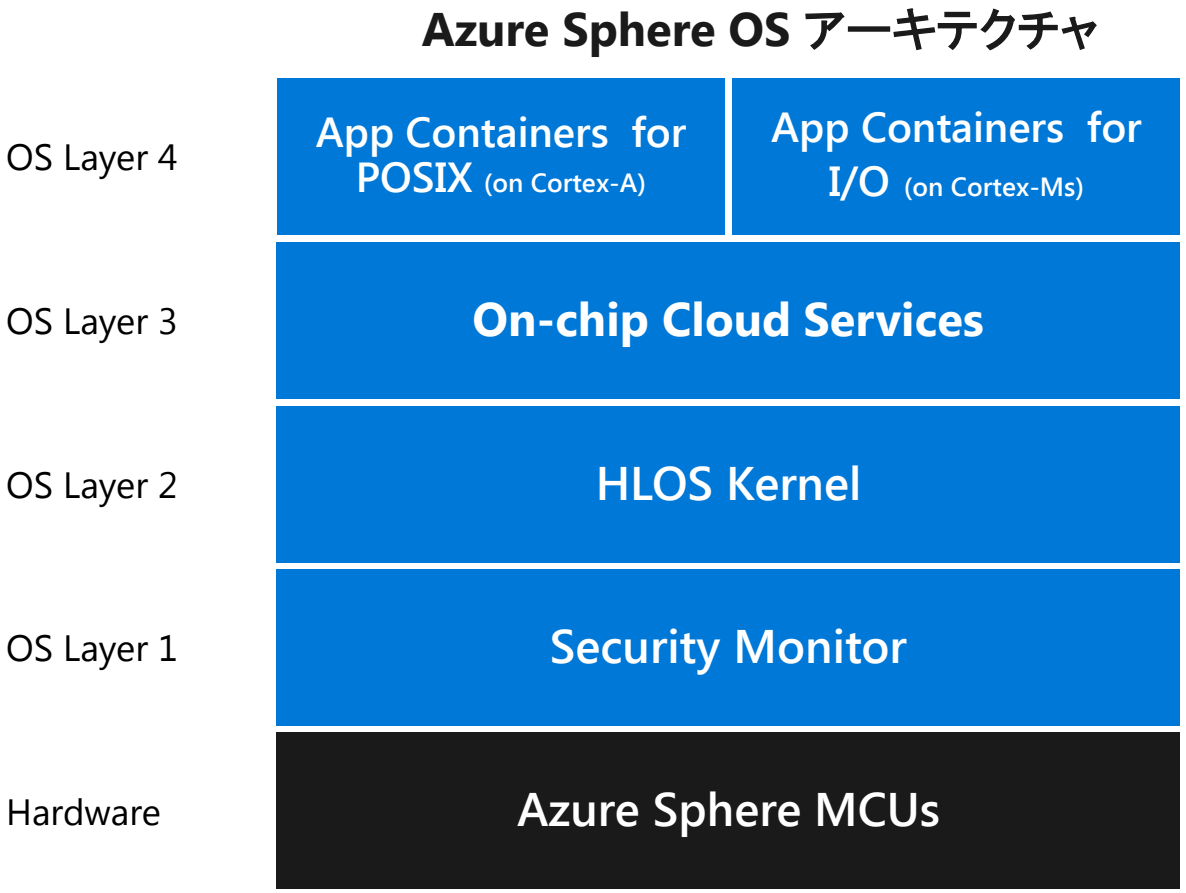
クロスオーバー
リアルタイム処理はCortex-M、アプリはCortex-Aで実行



© Microsoft Corporation

The Azure Sphere OS

IoT、セキュリティ、MCUアジリティ向けに最適化



セキュアアプリケーションコンテナー
コードを、アジリティ、ロバストネス、セキュリティ向けにコンパートメント化

オンチップクラウドサービス
アップデート、認証、接続機能を提供

カスタム Linux カーネル
シリコンの進化への最適化とコードの再利用

セキュリティモニター
一貫性と保持とクリティカルリソースへのアクセスをガード

© Microsoft Corporation

Azure Sphere Security Service

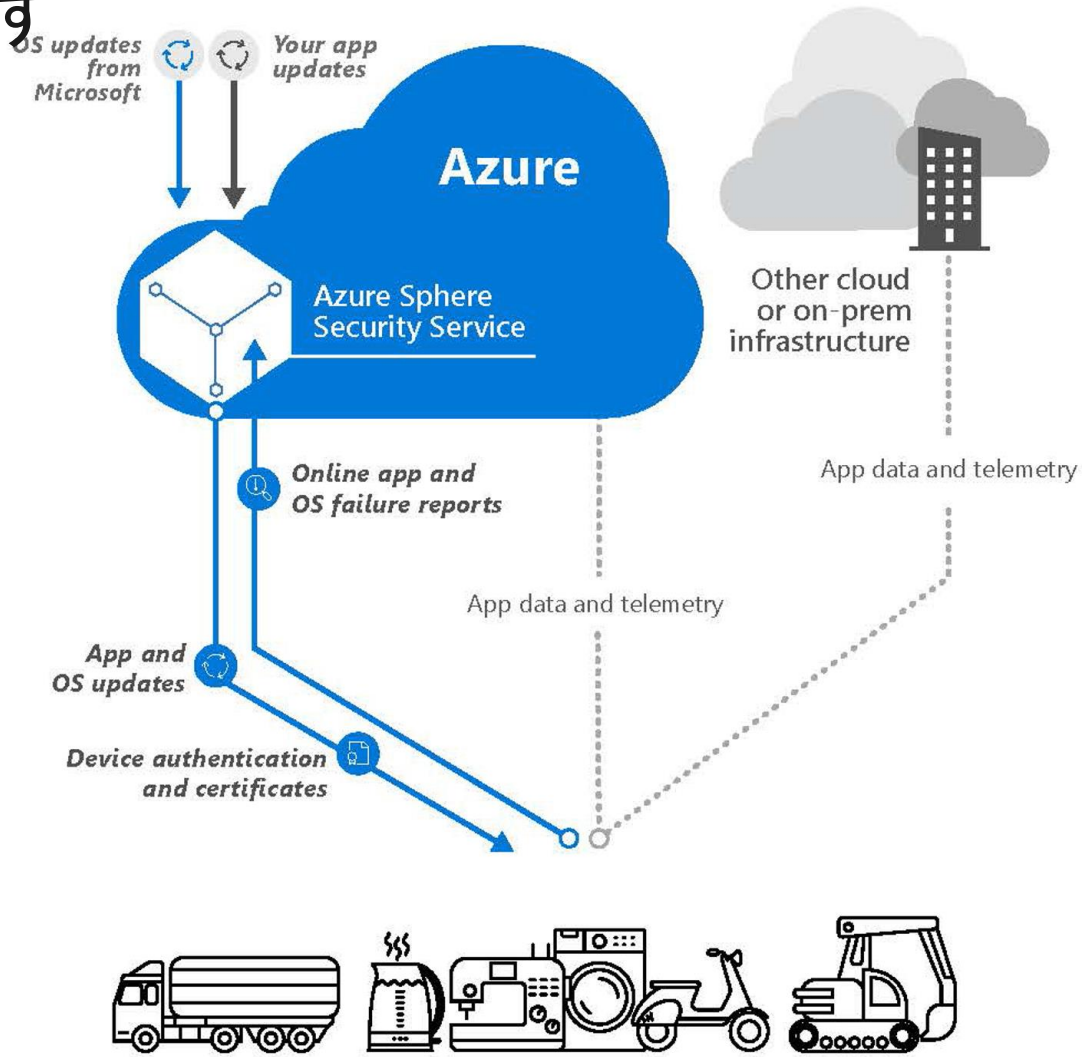
全ての Azure Sphereデバイスを接続・保護する

保護する
デバイスと顧客を、全ての通信に対する証明書ベースの認証で保護する

検知する
新たに出現したセキュリティへの脅威を、デバイス上の障害を自動化されたプロセスで検知する

対応する
完全に自動化されたデバイス上のOSアップデート機能で脅威に対応する

許可する
Azure Sphere で強化されたデバイスへの、ソフトウェアの容易なアップデートを許可する



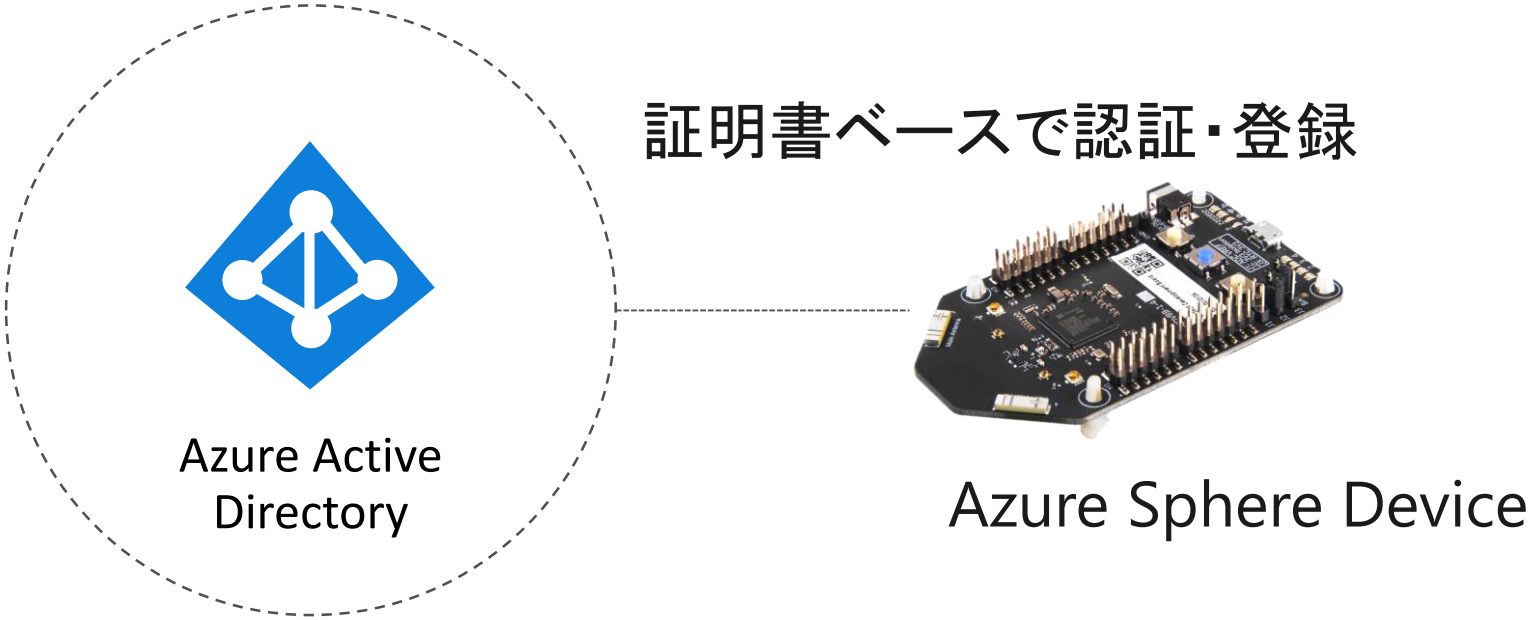
© Microsoft Corporation

Pluton セキュリティ概要

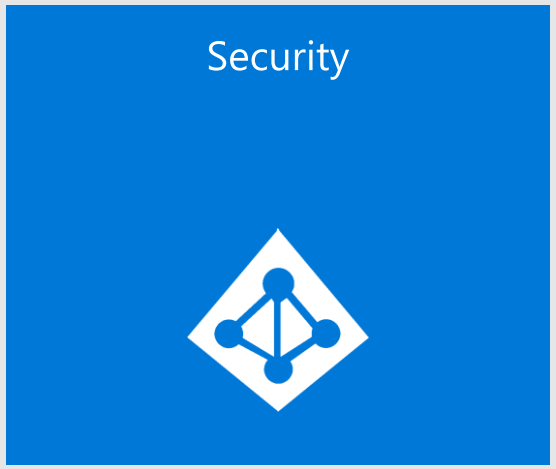
- https://azure.microsoft.com/en-us/blog/anatomy-of-a-secured-mcu/
- Pluton キーマネージメント
  - 暗号キーは製造時に書き込まれる
  - ソフトウェアから暗号キーは見えない
- セキュアブート
  - Azure Sphere上で実行される全てのソフトウェアはマイクロソフトによるデジタルサインが必要
- リモート構成証明の活用（Leveraging remote attestation）
  - AS3（Azure Sphere Security Service）とPlutonの連携により、デバイスとサービス間の認証を担保
- セキュリティ機能の追加・改良
  - ロイヤリティフリーでチップベンダーにシリコンセキュリティ技術を提供

Azure Sphereを使う

最初に行う事は…



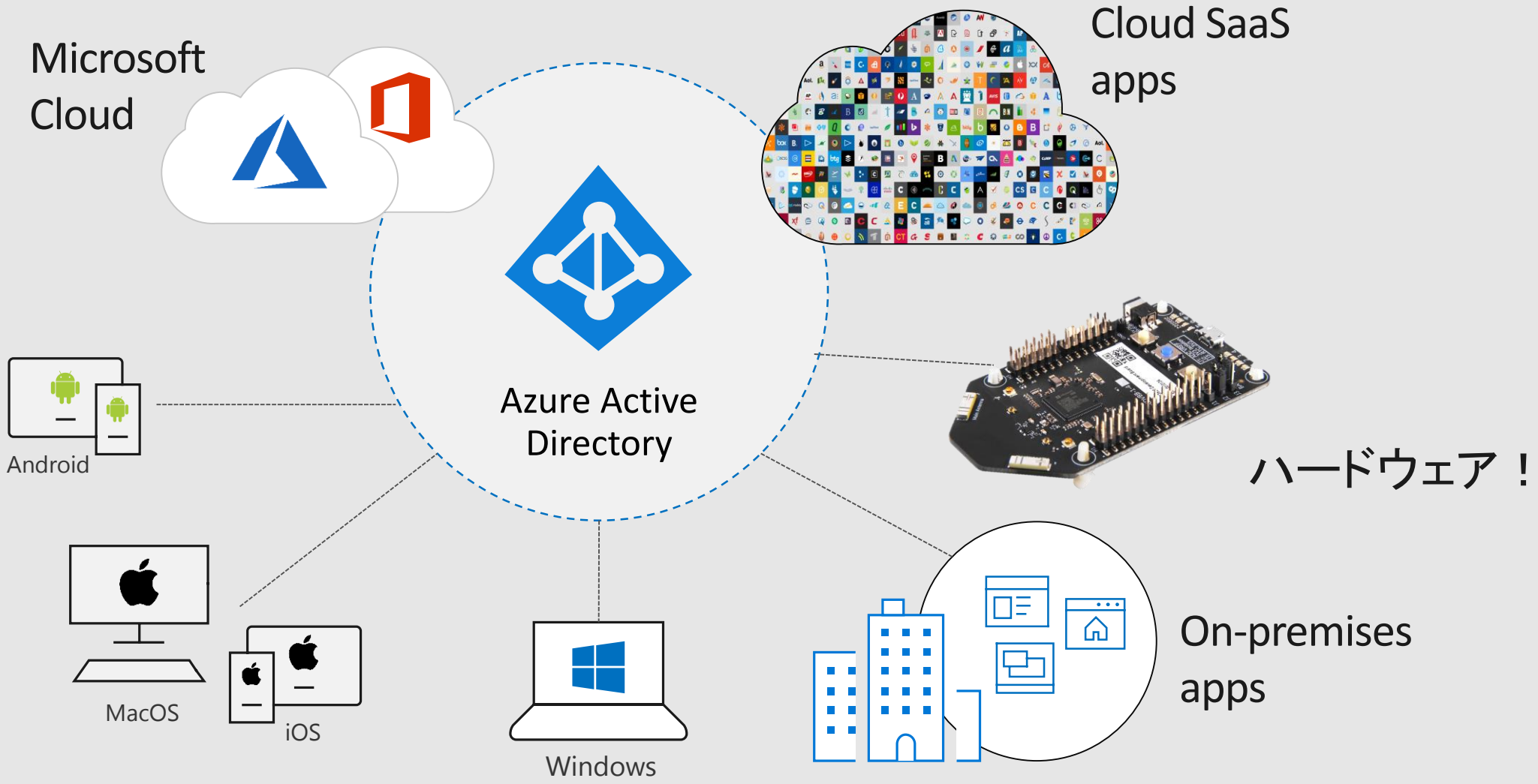
IoT セキュリティの基盤



- 正当なユーザー
- 正当なアプリケーション/サービス
- 正当なデバイス

Identity、Identity、Identity

Active Directory

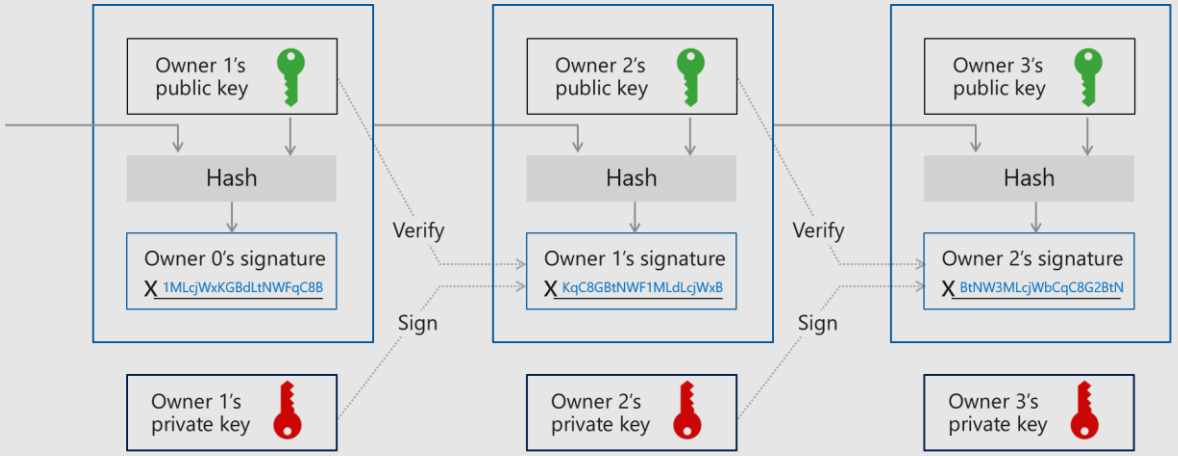


認証されたユーザー、アプリ・サービス、組織を支える基盤


その先へ…

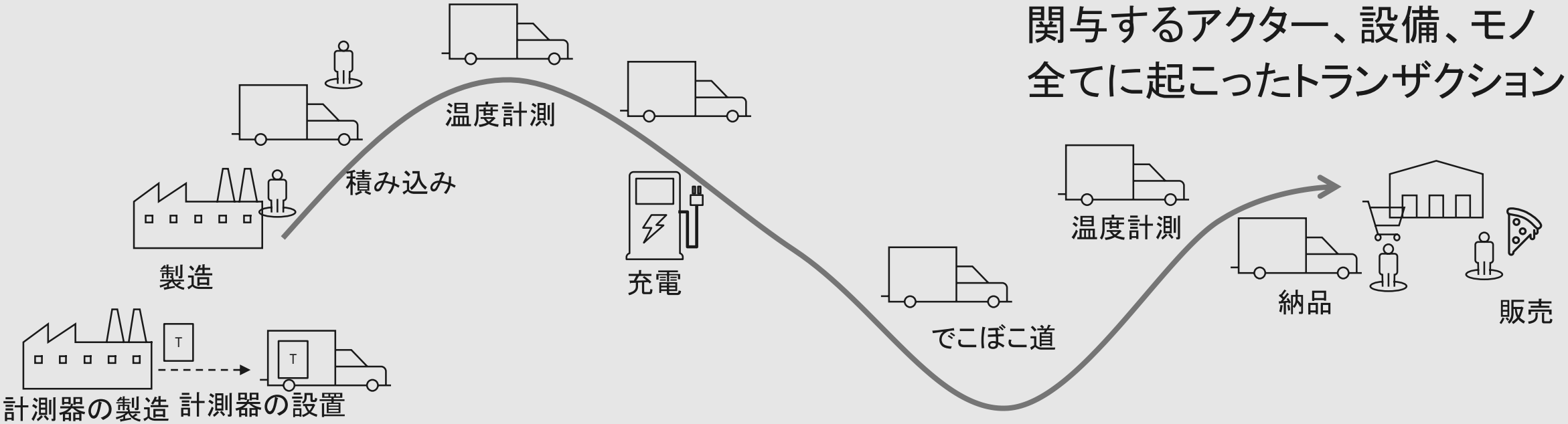
一連の作業の流れの正当性を保証する

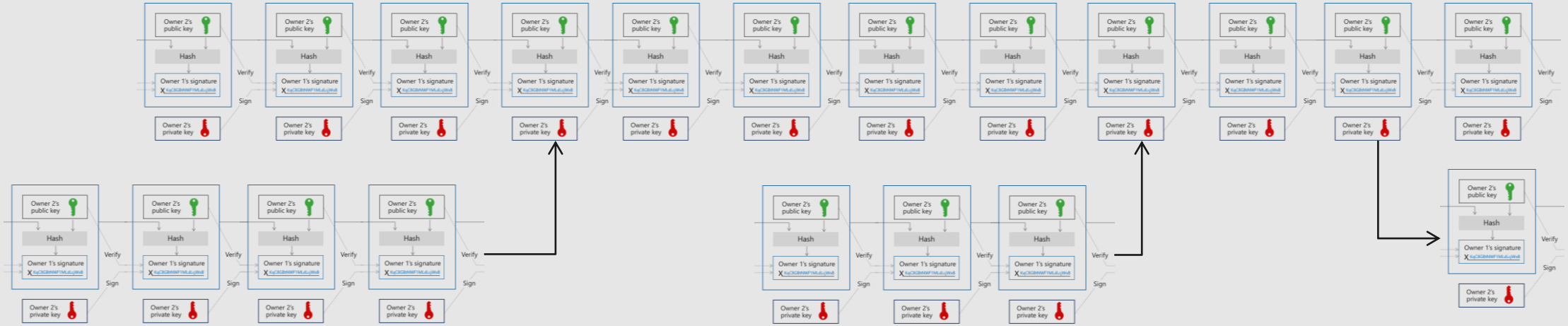
- Blockchainの活用
  - 信頼されたハンコが押された、チェーンでつながった記録台帳
  - かつ、記録台帳は複数の場所で記録され、改竄が非常に困難



連なるトランザクションチェーンで正当性を保持

関与するアクター、設備、モノ
全てに起こったトランザクションの記録





最後に

まとめの列挙

自分のペースで学べるサイト

有料サービスも無料で学べる

https://docs.microsoft.com/ja-jp/learn/

https://www.microsoft.com/handsonlabs

de:code 2019開催！

http://aka.ms/decode からお申込みを！

4/24まで早期割引！

EXPO展示・セッションに参加可能な無料枠もあり！

今日、ReButtonもらった人は、ブログとかでアイデアを！

https://seeedjp.github.io/ReButton/

http://matsujirushi.hatenablog.jp/entry/2019/01/23/171257

※“Seeed ReButton”で検索