

製品オプションを識別する

100 XP

5 分

IoT を使用すると、データ分析のためにデバイスで情報を収集して中継することができます。スマート デバイスには、データを収集するセンサーが搭載されています。物理的な世界の属性を測定する一般的なセンサーには次のようなものがあります。

- 温度と湿度のレベルをキャプチャする環境センサー。
- バーコード、QR コード、または光学式文字認識 (OCR) のスキャナー。
- geo ロケーションと近接のセンサー。
- 光、色、赤外線センサー。
- 音と超音波のセンサー。
- モーションとタッチのセンサー。
- 加速度計と傾きのセンサー。
- 煙、気体、アルコールのセンサー。
- デバイスに問題がある場合を検出するエラー センサー。
- 異常または変形を検出する機械センサー。
- 気体および液体を測定するための流量、レベル、圧力のセンサー。

Azure IoT サービスを使用することで、これらの種類のセンサーを搭載し、インターネットに接続できるデバイスでは、メッセージを介して Azure の特定のエンドポイントにセンサーの読み取り値を送信できます。この後、メッセージのデータは、収集および集約され、レポートやアラートに変換することができます。また、Azure IoT サービスから各デバイスにソフトウェア更新プログラムを送信することで、すべてのデバイスを新しいファームウェアで更新して問題を修正したり、新しい機能を追加したりすることもできます。

たとえば、会社がスマート冷蔵自動販売機を製造し、稼働させているとします。どのような種類の情報を監視しますか。次の点を保証することが必要になる可能性があります。

- 各マシンがエラーなしで動作している。
- マシンが侵害されていない。
- マシンの冷却システムでは、内容物が一定の温度範囲内で保管されている。
- マシンに補充できるように、製品が特定の在庫レベルに達すると通知される。

自動販売機のハードウェアで、この情報を収集し、それを標準メッセージで送信できれば、各マシンから送信されたメッセージを、Azure IoT サービスを使用して受信、保存、整理、表示ができます。

これらのデバイスから収集されたデータは、Azure AI サービスと組み合わせることで、次の予測を行うのに役立てることができます。

- マシンでプロアクティブ メンテナンスが必要な時期。
- 在庫を補充し、新しい製品をベンダーに注文する必要がある時期。

Azure で IoT 向けのエンドツーエンド ソリューションを支援および促進できるサービスは数多くあります。

Azure IoT Hub

Azure IoT Hub はクラウドでホストされるマネージド サービスであり、IoT アプリケーションとそれが管理するデバイス間の双方向通信のための中央メッセージ ハブとして機能します。 Azure IoT Hub を使用すると、数百万台の IoT デバイスと、クラウドでホストされるソリューション バックエンドとの間で信頼性が高く安全な通信を行うことができる IoT ソリューションを構築できます。ほとんどすべてのデバイスを IoT ハブに接続できます。

IoT Hub サービスを使用すると、デバイスからクラウドと、クラウドからデバイスの両方向の通信がサポートされます。 また、デバイスからクラウドへのテレメトリ、デバイスからのファイルのアップロード、クラウドからデバイスを制御するための要求/応答メソッドなど、複数のメッセージ パターンもサポートされます。 IoT ハブでデバイスからメッセージが受信されると、それを他の Azure サービスにルーティングすることができます。

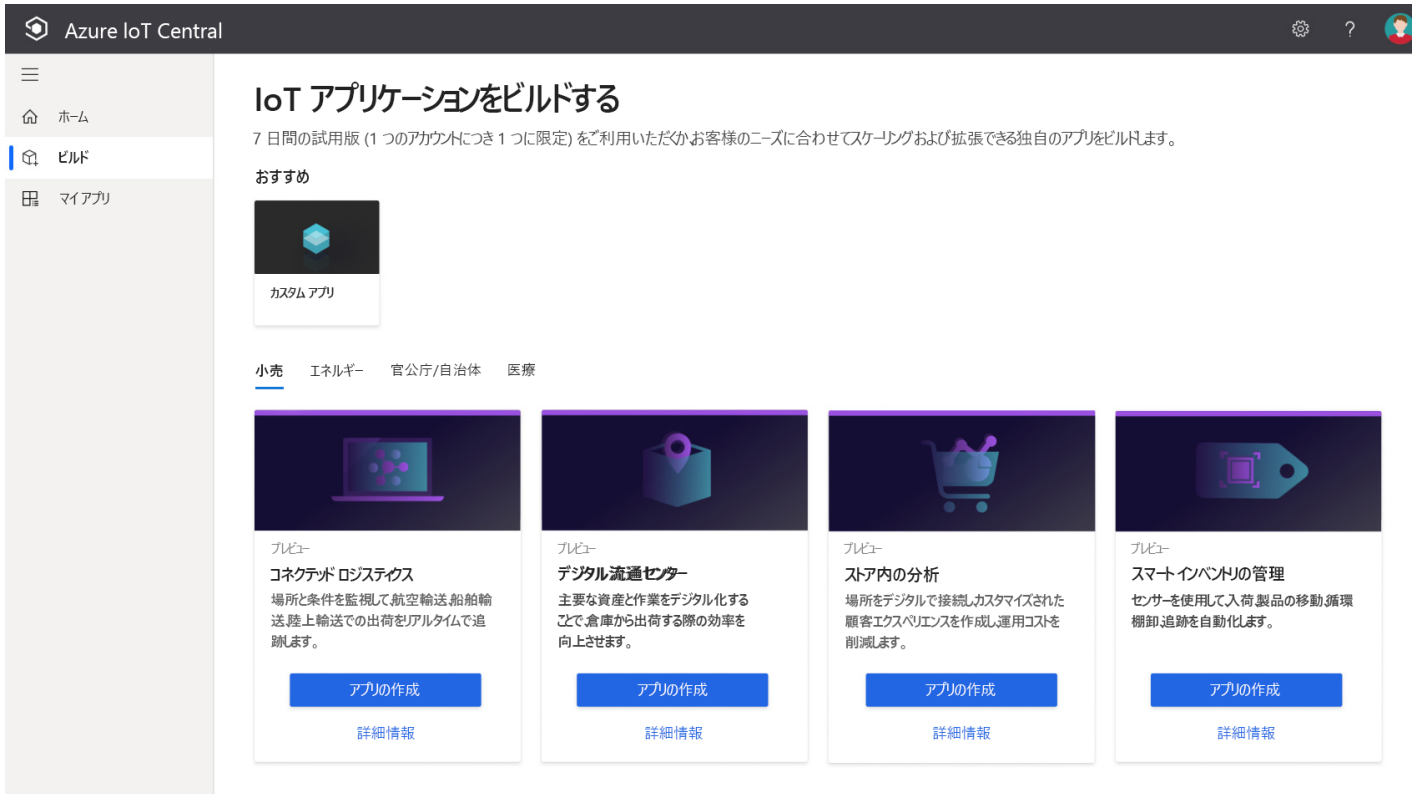
クラウドからデバイスへは、IoT Hub を使用して、"命令と制御" を行うことができます。つまり、接続されたデバイスを手動でまたは自動的にリモート制御できるため、バルブの開放、目標温度の設定、スタックしているデバイスの再起動などをデバイスに指示することができます。

IoT Hub の監視は、デバイスの作成、デバイスの障害、デバイスの接続などのイベントを追跡することにより、ソリューションの正常性を維持するのに役立ちます。

Azure IoT Central

Azure IoT Central は、IoT デバイスの接続、監視、管理を可能にするダッシュボードを追加することで、IoT Hub 上に構築されています。 ビジュアル ユーザー インターフェイス (UI) を使用すると、簡単に新しいデバイスを接続し、テレメトリやエラー メッセージの送信開始時を監視することができます。 すべてのデバイスにわたってパフォーマンス全体を総合的に監視することができます。また、特定のデバイスでメンテナンスが必要になったときに通知を送信するようにアラートを設定することができます。最後に、ファームウェア更新プログラムをデバイスにプッシュすることができます。

すぐに使用を開始し、実行できるように、IoT Central には、小売、エネルギー、医療、政府などのさまざまな業界にわたって、一般的なシナリオのスターター テンプレートが用意されています。次に、既存のテーマから選択したり、独自のカスタム テーマを作成し、ロゴを設定したりするなどして、UI でデザイン スターター テンプレートを直接カスタマイズします。 IoT Central を使用すると、デバイスから送信される特定のデータ、表示するレポート、送信するアラートに合わせて、スターター テンプレートを調整できます。



UI を使用して、デバイスをリモートで制御できます。この機能を使って、ソフトウェア更新プログラムをプッシュすることや、デバイスのプロパティを変更することができます。IoT Central 内から直接、1 台またはすべての冷蔵自動販売機の目的の温度を調整することができます。

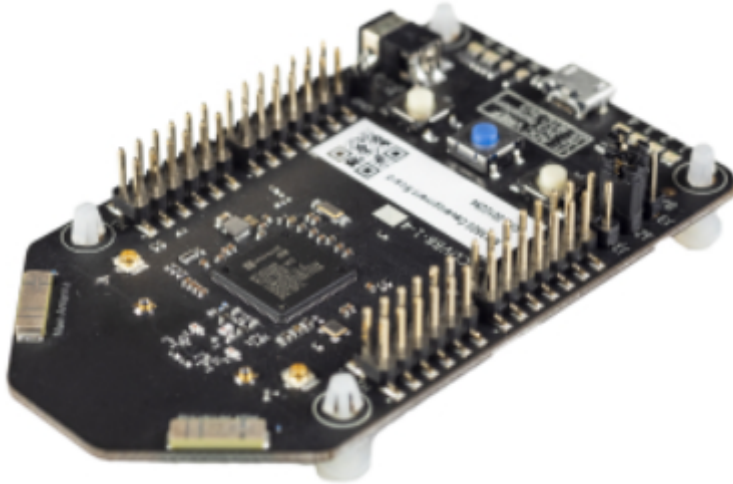
IoT Central の重要な部分は、デバイス テンプレートの使用です。デバイス テンプレートを使用すると、サービス側でコーディングすることなくデバイスを接続できます。IoT Central では、テンプレートを使用してダッシュボードやアラートなどが構築されます。デバイス開発者は、デバイス上で実行するコードを作成する必要があります。また、そのコードはデバイス テンプレートの仕様と一致する必要があります。

Azure Sphere

Azure Sphere では、お客様向けのエンドツーエンドの安全性の高い IoT ソリューションを作成します。これには、デバイス上のハードウェアやオペレーティング システムから、メッセージをデバイスからメッセージ ハブに送信する安全な方法まで、あらゆるものが含まれています。Azure Sphere には、インターネットに接続されたデバイス用の通信とセキュリティの機能が組み込まれています。

Azure Sphere は次の 3 つの部分で構成されます。

- 最初の部分は Azure Sphere マイクロコントローラー ユニット (MCU) で、オペレーティング システムと、接続されたセンサーからの信号の処理について責任を負います。次の画像は、Azure Sphere アプリケーションのプロトタイプ作成と開発に使用できるさまざまなスターター キットの 1 つである Seeed Azure Sphere MT3620 Development Kit MCU を示しています。



- 2つ目の部分は、セキュリティ サービスとの通信を処理し、ベンダーのソフトウェアを実行できる、カスタマイズされた Linux オペレーティング システム (OS) です。
- 3つ目の部分は、AS3 と呼ばれる Azure Sphere Security Service です。その役割は、デバイスが悪意を持って侵害されていないことを確認することです。デバイスでは、Azure に接続を試みる場合、最初に、(デバイスごとに) 証明書ベースの認証を使用して自身を認証する必要があります。認証に成功すると、AS3 によって、デバイスが改ざんされていないことを保証するためのチェックが行われます。セキュリティで保護された通信チャネルが確立されると、AS3 によって、OS、または顧客によって開発された承認済みのソフトウェアの更新プログラムがデバイスにプッシュされます。

Azure Sphere システムによってデバイスの信頼性が検証され、認証されると、デバイスでは、テレメトリやエラー情報を送信して、他の Azure IoT サービスと対話できるようになります。