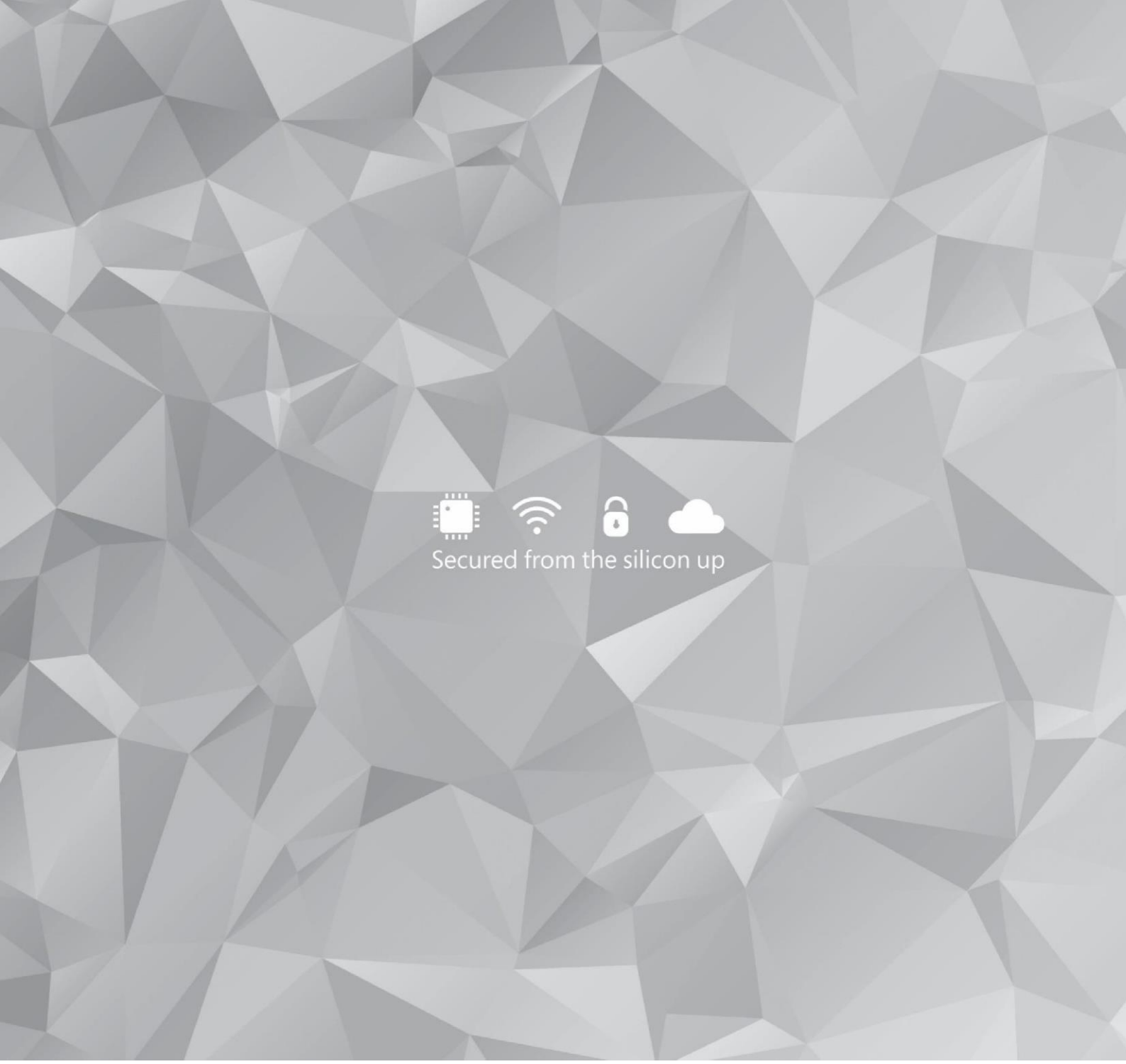


Azure Sphere

ソリューションの概要

バージョン 1.3 – 2018 年 4 月 27 日

目次

はじめに

Azure Sphere とは、相互接続されたデバイスに組み込みの通信およびセキュリティ機能を提供する、セキュリティ保護された高レベルのアプリケーション プラットフォームです。このドキュメントでは、Azure Sphere の機能、およびそれがどのようにモノのインターネット (IoT) に適合するかを含む、Azure Sphere の広範な技術的概要を提供します。この概要には、ファームウェアの技術者、セキュリティ専門家、技術的意思決定者のどなたにとっても、Azure Sphere プラットフォームの設計および操作環境の基本原理を理解するために必要な情報が含まれています。

Azure Sphere は進化中のプラットフォームであるため、ここに記載される情報の一部は、製品の一般提供後に変更される可能性があることに留意してください。この概要の目的は、重要な機能の要約を示し、プラットフォームの想定する稼働コンテキストについて紹介することです。可能な場合には、開発中であるが製品メーカーにはまだ提供されていない機能についても触れています。

Azure Sphere とは?

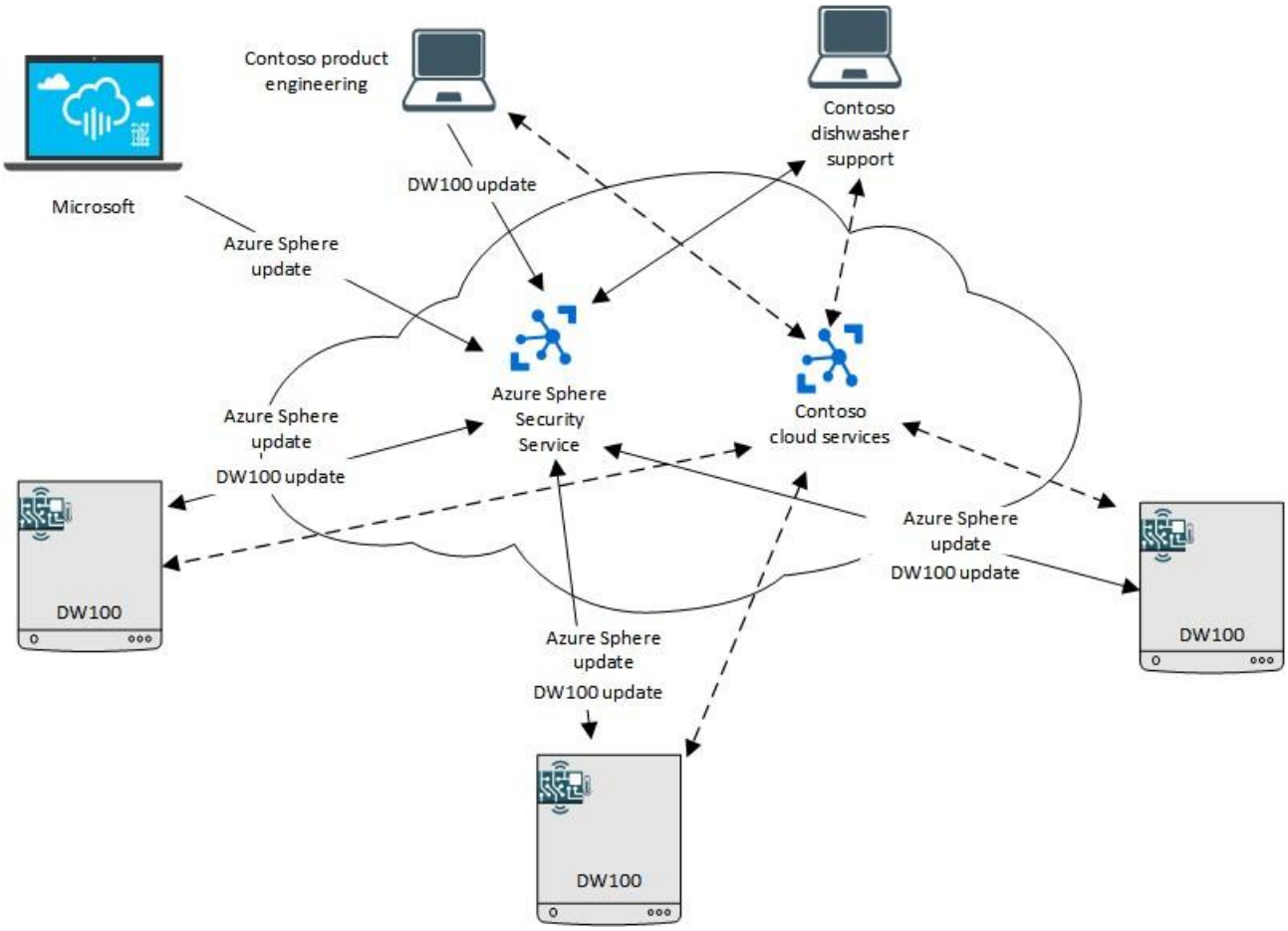
Azure Sphere は、セキュリティ保護された、新しいクロスオーバー クラスのマイクロコントローラー ユニット (MCU) を導入します。クロスオーバー MCU は、リアルタイムの処理能力と、高レベルのオペレーティング システムを実行する能力を統合します。そのような市場初の MCU である MediaTek MT3620 は、ARM Cortex-M クラスおよび Cortex-A クラス コアに Wi-Fi 接続性を搭載します。製品メーカーが Azure Sphere MCU を使用すれば、そのオペレーティング システムとアプリケーション プラットフォームとの連携により、アップデート/制御/監視/保守をリモート実行できる、セキュリティ保護されたインターネット接続デバイスの開発が可能になります。コネクテッド デバイスに MCU を埋め込んで、既存の MCU と併用または既存のものを置き換えることで、製品メーカーはセキュリティ、生産性、および機会を向上させることができます。以下にその例を示します。

- セキュリティ保護されたアプリケーション環境、認証された接続、および周辺機器のオプトイン使用によって、スプーフィング、非承認のソフトウェア、またはサービス拒否攻撃などによるセキュリティ リスクを最小限に抑えます。
- ソフトウェア アップデートをすべてのコネクテッド デバイスに OTA (Over-The-Air) で自動的に展開して問題を解決し、新機能を提供し、新しい攻撃手法に対抗することで、サポート担当者の生産性を高めます。
- 製品の使用状況データをセキュリティ保護された接続を介してクラウドに報告し、問題の診断と新製品の設計に役立てることで、製品サービス、積極的なお客様とのやり取り、および将来の開発の機会を増加させます。

Azure Sphere Security Service は、Azure Sphere の不可欠な部分です。このサービスを使用して、Azure Sphere MCU は安全かつセキュリティ保護された方法でクラウドと Web に接続できます。このサービスにより、デバイスは承認された正規のソフトウェアの認可されたバージョンでのみ起動するようになります。さらに、マイクロソフトが現場で展開されたデバイスにオペレーティング システムのアップデートを自動的にダウンロード/インストールできる、セキュリティ保護されたチャネルを提供することで、セキュリティの問題を軽減します。メーカーまたはエンドユーザーの介入は必要ないため、一般的なセキュリティ ギャップを防止できます。

例: Azure Sphere シナリオ

Contoso, Ltd., は、Azure Sphere MCU を食洗器に搭載する白物家電メーカーです。DW100 食洗器では、MCU をいくつかのセンサーと、Azure Sphere MCU 上で動作するオンボード アプリケーションと組み合わせています。オンボード アプリケーションは Azure Sphere Security Service および Contoso 社のクラウド サービスと通信します。以下の図は、このシナリオを示しています。



Contoso 社のネットワークに接続された食洗器

左上から開始して時計回りに進みます。

- マイクロソフトは Azure Sphere Security Service を介して Azure Sphere デバイス ソフトウェアのアップデートをリリースします。
- Contoso 社の製品エンジニアリング部門は、Azure Sphere Security Service を通して DW100 アプリケーションにアップデートをリリースします。
- Azure Sphere Security Service は、アップデートされたマイクロソフト デバイス ソフトウェアと Contoso DW100 アプリケーション ソフトウェアを、エンドユーザーの場所にある食洗器にセキュリティ保護された方法で展開します。
- Contoso 社の食洗器サポート部門は、Azure Sphere Security Service と通信して、どのバージョンの Azure Sphere ソフトウェアと DW100 アプリケーション ソフトウェアを各エンドユーザー デバイスで実行する必要があるかを決定し、サービスに報告されたエラー レポート データを収集します。Contoso 社の食洗器サポート部門は Contoso 社のクラウド サービスとも通信して追加の情報を入手します。
- Contoso 社のクラウド サービスは、トラブルシューティング、データ分析、およびお客様とのやり取りのためのアプリケーションをサポートします。Contoso 社のクラウド サービスは、Microsoft Azure、別のベンダーのクラウド サービス、または Contoso 社独自のクラウドによってホストできます。

- エンドユーザーの場所にある Contoso DW100 モデルは、Azure Sphere Security Service への接続を介してアップデートされたソフトウェアをダウンロードします。これらのモデルは Contoso 社のクラウド サービス アプリケーションとも通信して、追加のデータを報告します。

たとえば、食洗器のセンサーは水温、乾燥温度、およびリンス剤のレベルを監視し、このデータを Contoso 社のクラウド サービスにアップロードして、クラウド サービスのアプリケーションによって潜在的問題を分析できるようにする場合があります。乾燥温度が異常に高いまたは低い場合、それによって故障部分が示される場合があり、Contoso 社はリモートで診断を実施して必要な修理についてお客様に通知します。食洗器が保証期間内の場合、クラウド サービスのアプリケーションでお客様の近くの修理店に修理部品があることを確認し、保守のための訪問や在庫の要件を削減することもできます。同様に、リンス剤が少なくなっている場合、食洗器はお客様にシグナルを表示して、メーカーから直接リンス剤を購入するよう促すこともできます。

すべての通信は、セキュリティ保護された、認証された接続を介して行われます。Contoso 社のサポートおよびエンジニアリング担当者は、Azure Sphere Security Service、Microsoft Azure 機能、または Contoso 社固有のクラウド サービス アプリケーションを使用することで、データを可視化できます。また、Contoso 社はお客様向けの Web およびモバイル アプリケーションを提供することもできます。食洗器の所有者はこれにより、サービスの要請、食洗器リソース使用状況の監視、同社とのやり取りが可能になります。

Azure Sphere 展開ツールを使用することで、Contoso 社は各アプリケーション ソフトウェアのアップデートの対象を適切な食洗器のモデルに絞ることができ、Azure Sphere Security Service はソフトウェア アップデートを適切なデバイスに配布します。署名され検証されたソフトウェア アップデートのみを食洗器にインストールできます。

Azure Sphere を使う理由

Azure Sphere プラットフォームは、価値の高いセキュリティを低価格で提供することで、価格重視のマイクロコントローラー搭載デバイスが、安全かつ信頼性の高い方法で IoT に接続できるようにすることを目指しています。ネットワークに接続された玩具、家電製品、およびその他の消費者デバイスがますます一般的になる中、セキュリティは最重要事項です。デバイスのハードウェアそのものがセキュリティ保護されるだけでなく、そのクラウドへの接続もセキュリティで保護される必要があります。操作環境のどこかにセキュリティの不備があると、製品全体を脅かし、その近くにあるモノや人を危険にさらす可能性があります。

インターネット セキュリティにおけるマイクロソフトの数十年にわたる経験に基づき、Azure Sphere チームは、強固にセキュリティ保護されたデバイスの 7 つの特性を特定しました。Azure Sphere プラットフォームは、以下に示すこれら 7 つの特性を中心に設計されています。

Hardware-based root of trust ハードウェアベースの信頼のルートにより、デバイスおよびその ID は分離されることがないため、デバイスの偽造またはスプーフィングを防止できます。すべての Azure Sphere MCU は、マイクロソフトが設計した Pluton セキュリティ サブシステム ハードウェアによって生成および保護される、偽造できない暗号化キーによって識別されます。これにより、改ざん防止機能を持つセキュリティで保護されたハードウェアベースの信頼のルートを工場からエンドユーザーに提供することができます。

Small trusted computing base デバイスのソフトウェアの大部分が Trusted Computing Base の外部にあるため、攻撃にさらされる領域を削減できます。マイクロソフトの提供する、セキュリティ保護された Security Monitor、Pluton ランタイム、および Pluton サブシステムのみが、Trusted Computing Base で実行されます。

Defense in depth 多層防御は、複数のセキュリティ層を提供することで、各脅威に対して複数の緩和策を実現します。Azure Sphere プラットフォームのソフトウェアの各層は、その上部にある層がセキュリティ保護されていることを検証します。

Compartmentalization コンパートメント化は、単一の障害の到達範囲を制限します。Azure Sphere MCU には、ハードウェアのファイアウォールを含むシリコンの対策が含まれ、あるコンポーネント内のセキュリティ侵害がその他のコンポーネントに伝播することを防ぎます。制約のある "サンドボックス" ランタイム環境により、アプリケーションがセキュリティ保護されたコードまたはデータを破損することを防止します。

Certificate-based authentication 偽造できない暗号化キーによって検証された、署名された証明書を使用することで、パスワードよりもさらに強力な認証が可能になります。Azure Sphere プラットフォームでは、あらゆるソフトウェア要素を署名することが要求されます。デバイスとクラウド間の通信には、さらに証明書ベースの認証が必要になります。

Renewable security　デバイスのソフトウェアは、既知の脆弱性またはセキュリティ侵害を修正するために自動的にアップデートされ、メーカーまたはエンドユーザーによる介入を必要としません。Azure Sphere Security Service は Azure Sphere OS および OEM アプリケーションを自動的にアップデートします。

Failure reporting　デバイスのソフトウェアまたはハードウェアの障害は、新しいセキュリティ攻撃において典型的です。デバイスの障害そのものが、サービス拒否攻撃を構成します。デバイスからクラウドへの通信では、潜在的な障害の早期警告を提供します。Azure Sphere デバイスは、運用データおよび障害をクラウドベースの分析システムに自動的に報告し、アップデートとサービシングはリモートで実行できます。

システムの概要

Azure Sphere ハードウェア、ソフトウェア、および Security Service は連携して、デバイスのメンテナンス、制御、およびセキュリティに対するユニークで統合されたアプローチを実現します。

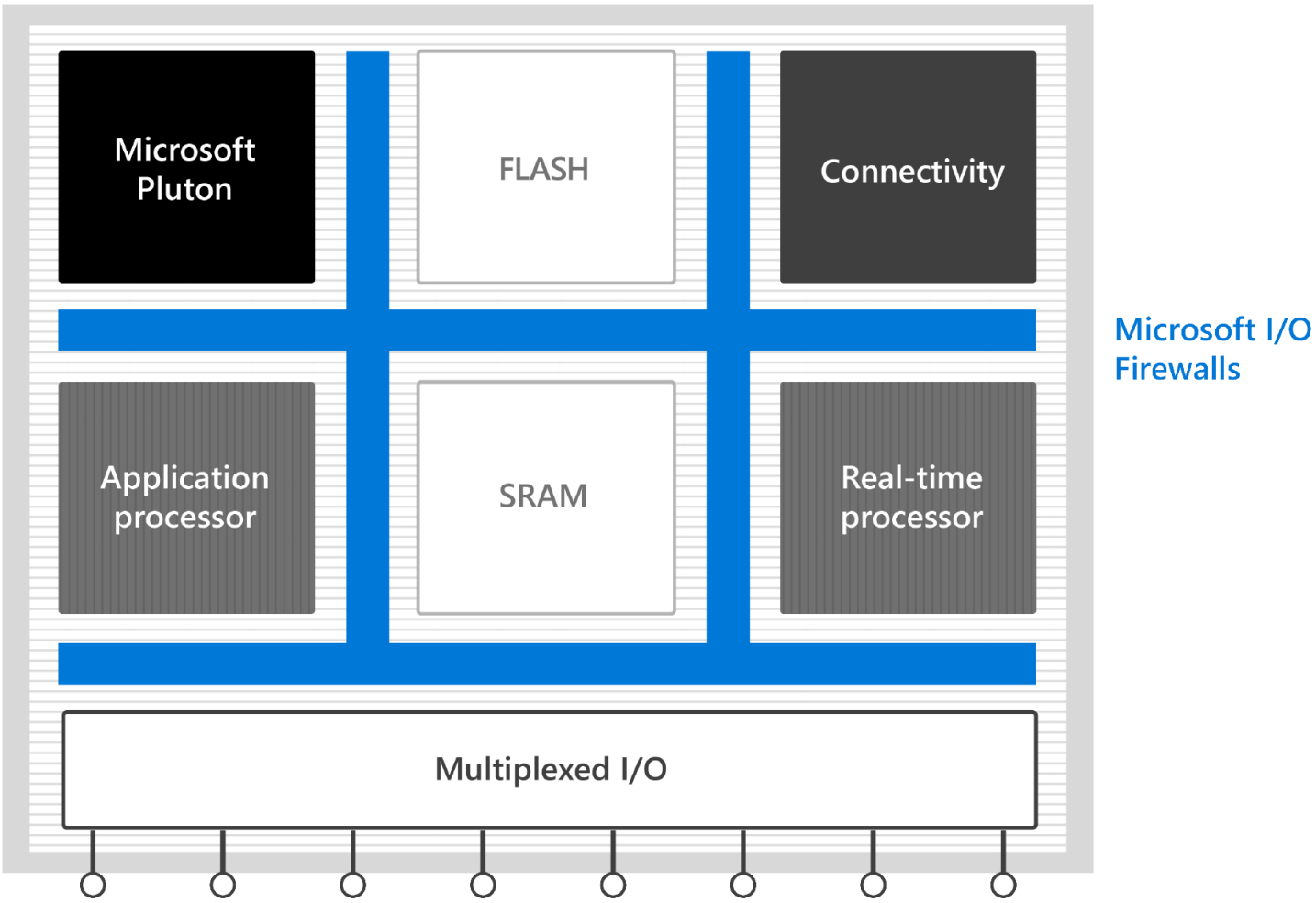
ハードウェア アーキテクチャが、IoT 上のデバイスに根本的にセキュリティ保護されたコンピューティング ベースを提供するため、製品メーカーは自分たちの専門分野、つまり製品固有の機能や強化に集中できます。

同様に、ソフトウェア アーキテクチャも、マイクロソフトの開発した Security Monitor 上で実行されるセキュリティ保護されたカスタム OS カーネルを備えているため、メーカー側は、顧客や株主にメリットをもたらす付加価値の高い IoT 機能に絞ってソフトウェア開発に取り組めるようになります。

Azure Sphere Security Service は、セキュリティ保護されたクラウド - デバイス間チャネルを介した認証、ソフトウェア アップデート、および障害報告をサポートするため、メーカーはセキュリティ保護された通信インフラストラクチャを信頼でき、製品が最新の Azure Sphere OS を実行していることを確信できます。

ハードウェア アーキテクチャ

Azure Sphere クロスオーバー MCU は、以下の図に示すように、単一のダイ上の複数のコアで構成されます。



Azure Sphere MCU ハードウェア アーキテクチャ

各コアと、それに関連付けられたサブシステムは、異なる信頼ドメイン内に存在します。信頼のルートは Pluton セキュリティ サブシステム内に存在します。アーキテクチャの各層は、その上にある層が侵害される可能性があると想定します。各層内で、リソースの分離とコンパートメント化によって、さらなるセキュリティが実現します。

マイクロソフトの Pluton セキュリティ サブシステム

Pluton セキュリティ サブシステムは、Azure Sphere のための、ハードウェアベースの (つまりシリコン内の) セキュリティ保護された信頼のルートです。それには、セキュリティ プロセッサ コア、暗号化エンジン、ハードウェア乱数生成器、公開/秘密鍵の生成、非対称暗号化と対称暗号化、セキュア ブートの楕円曲線 DSA (ECDSA) 検証のサポート、およびクラウド サービスでのリモート認証をサポートするためのシリコン内のメジャー ブートと共に、エントロピー検出ユニットを含むさまざまな改ざん対策が含まれます。

セキュア ブート プロセスの一部として、Pluton サブシステムはさまざまなソフトウェア コンポーネントを起動します。また、ランタイム サービスを提供し、デバイスのその他のコンポーネントからのリクエストを処理し、デバイスのその他の部分の重要なコンポーネントを管理します。

アプリケーション プロセッサ

アプリケーション プロセッサは、完全なメモリ管理ユニット (MMU) を持つ ARM Cortex-A サブシステムを搭載しています。これは Trust Zone 機能を使用することでハードウェアベースのコンパートメント化を実現し、オペレーティング システム、アプリケーション、およびサービスの実行を担っています。次の 2 つの操作環境がサポートされます。ユーザー モードとスーパーバイザー モードの両方でコードを実行する Normal World (NW) と、マイクロソフトが提供する Security Monitor のみを実行する Secure World (SW) です。お客様の開発したアプリケーションは、アプリケーション プロセッサの NW ユーザー モードで実行します。

リアルタイム プロセッサ

リアルタイム プロセッサは、ベアメタル コードまたはリアルタイム オペレーティング システム (RTOS) のどちらかを使用する ARM Cortex-M I/O サブシステムを搭載します。Azure Sphere が成熟するにつれ、お客様がカスタムの A7 アプリケーションを補足できるよう I/O サブシステムのためのアプリケーションを開発できるようにする予定です。

接続性と通信

すべての Azure Sphere MCU にはワイヤレス通信サブシステムが搭載されており、それによってインターネット サービスに接続できます。最初の Azure Sphere MCU では、2.4GHz と 5GHz の両方で、802.11 b/g/n Wi-Fi 無線運用を提供します。お客様のアプリケーションでは、ワイヤレス通信サブシステムを構成、使用、クエリできますが、それを直接プログラムすることはできません。

現在、Azure Sphere では Wi-Fi ステーション モードがサポートされます。アクセス ポイント (AP) モードは計画中です。

多重化 I/O

Azure Sphere プラットフォームは、さまざまな I/O 機能をサポートするため、メーカーは組み込みデバイスを市場要件に合わせて設定できます。I/O 周辺機器は ARM Cortex-A または ARM Cortex-M I/O コアのどちらかにマップできます。

Microsoft Firewall

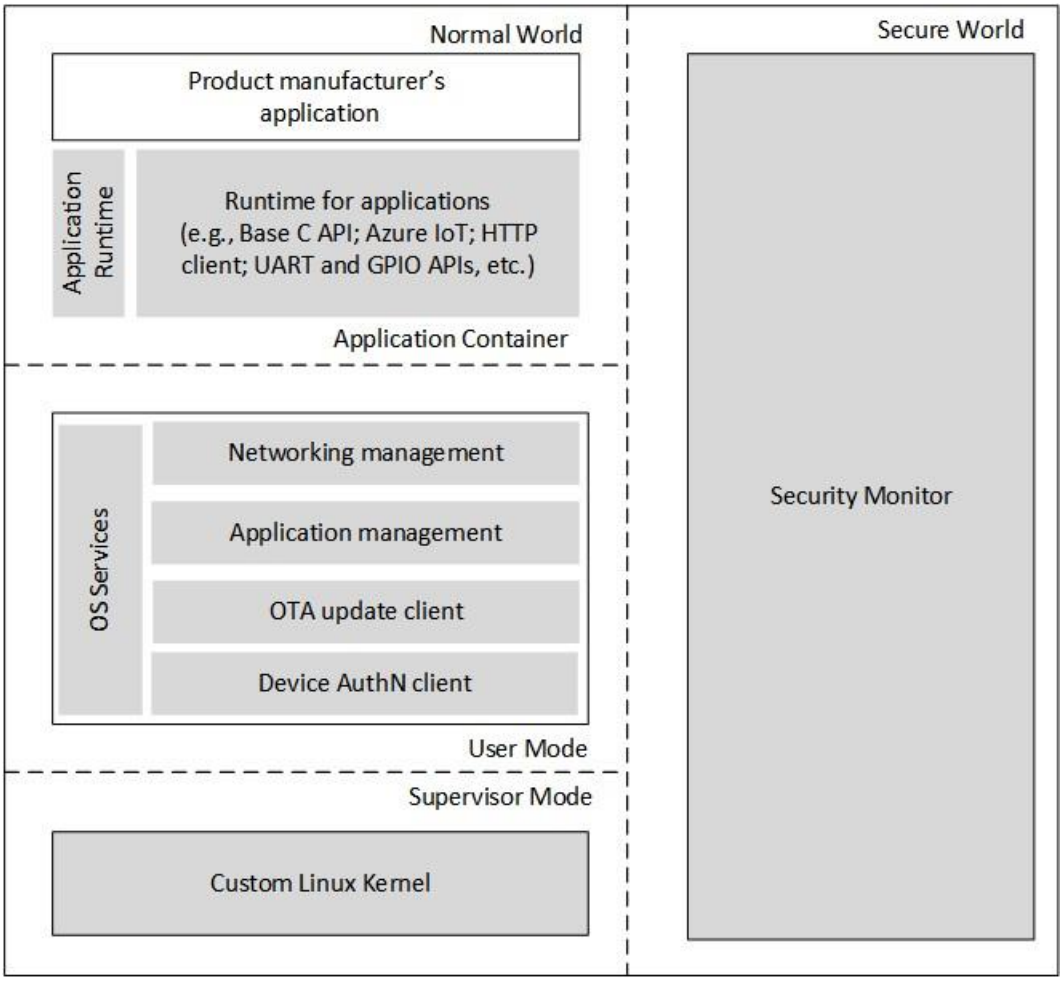
ハードウェア ファイアウォールは、"サンドボックス" 保護を提供して I/O 周辺機器がマップされたコアにのみアクセスできるようにする、シリコンの対策です。ファイアウォールではコンパートメント化が強制されるため、A7 コアにローカライズされたセキュリティの脅威が、I/O M4 コアの周辺機器へのアクセスに影響することを防止できます。

統合 RAM およびフラッシュ

Azure Sphere MCU には、最小 4MB の統合 RAM と、16MB の統合フラッシュ メモリが含まれます。

Cortex-A ソフトウェア アーキテクチャ

ARM Cortex-A (A7) アプリケーション プラットフォームは、最初の Azure Sphere MCU で利用可能になるお客様によるプログラムが可能な初のコアです。以下の図は、このプラットフォームの要素を示しています。マイクロソフトが提供する要素はグレーで表示され、製品メーカーが提供する要素は白色で表示されています。



Cortex-A ソフトウェア プラットフォーム

マイクロソフトは、製品メーカーのアプリケーション以外のすべての Cortex-A ソフトウェアを提供および保守します。デバイス上で実行されるアプリケーションを含むすべてのソフトウェアは、マイクロソフトの証明書機関 (CA) によって署名されます。アプリケーションのアップデートは信頼されるマイクロソフトのパイプラインから提供され、各アップデートと Azure Sphere デバイス ハードウェアとの互換性は、インストール前に検証されます。

A7 アプリケーション

製品メーカーは、NW ユーザー モードで実行されるカスタムの A7 アプリケーションを開発します。そのようなアプリケーションでは、次のことを実行できます。

- 汎用 I/O (GPIO) ピン、汎用非同期送受信回路 (UART)、およびその他のインターフェイスを含む、Azure Sphere MCU に統合された周辺機器の構成および対話
- Azure IoT ハブまたはその他のクラウドベースのサービスとの通信
- 証明書ベースの認証を介したその他のデバイスおよびサービスとの信頼関係の仲介

- 基幹業務 (LOB) サービスとの通信

製品メーカーのアプリケーションは、A7 コアのアプリケーション コンテナー内で実行されます。それは、マイクロソフトが提供するライブラリおよびランタイム サービスにのみアクセスできます。さらに、コンパートメント化されたセキュリティの一環として、アプリケーションでは必要な外部サービスとインターフェイスを指定する必要があります。たとえば、未承認のまたは予期しない使用を防止するため、I/O およびネットワーク要件を指定します。外部のソフトウェアまたは悪意のあるデータによる破損を防ぐため、A7 アプリケーションでは汎用ファイル I/O またはプロセス間通信 (IPC) を実行できません。ただし、認証後、クラウド サービスと対話したり、または Azure Sphere ソフトウェア開発キット (SDK) で提供される http および https ライブラリを使用して、その他のインターネット サービスと対話したりできます。

デバイス上では一度に 1 つの A7 アプリケーションのみを実行できます。A7 アプリケーションは、継続して実行するよう想定されており、停止または障害発生時には自動的に再起動されます。

非承認のソフトウェアのインストールを防止するため、アプリケーションは次の 2 つの方法でのみロードできます。

- ソフトウェア開発およびテストのためのサイドローディング。サイドローディングにはデバイスへの直接のアクセスと、Azure Sphere Security Service による認証が必要です。
- OTA アップデート。これは Azure Sphere Security Service によってのみ実行できます。

すべての展開は署名され、デバイスに対して信頼性が証明されます。

アプリケーション ランタイム

マイクロソフトが提供するアプリケーション ランタイムは、POSIX 標準のサブセットに基づいています。それは、NW ユーザー モードで実行されるライブラリおよびランタイム サービスで構成されます。この環境は、A7 アプリケーションと Azure Sphere Security Service をサポートします。

アプリケーション ライブラリにはいくつかの制約がありますが、特に汎用ファイルの直接の I/O、IPC、またはシェル アクセスはサポートされていません。これらの制限により、プラットフォームはセキュリティ保護された状態を維持し、マイクロソフトはセキュリティおよび保守のアップデートを提供できます。さらに、制約付きライブラリは、長期間安定した API サーフェイスを提供するため、お客様のアプリケーションとのバイナリ互換性を維持しつつ、システムのソフトウェアをアップデートしてセキュリティを強化できます。

OS サービス

OS サービスはアプリケーション コンテナーをホストし、Azure Sphere Security Service との通信を担当します。これらのサービスはすべての送信トラフィックに対して WiFi 認証とネットワーク ファイアウォールを管理します。アプリケーション開発時には、OS サービスは接続された PC とデバッグ中のアプリケーションとも通信を行います。

カスタムの Linux カーネル

カスタムの Linux カーネルは、ブート ローダーと共にスーパーバイザー モードで実行されます。カーネルは Azure Sphere MCU のフラッシュおよび RAM のフットプリントに応じて慎重に微調整されています。それは別個の仮想アドレス領域におけるユーザー領域のプロセスの割り込み可能な実行のためのサーフェイスを提供します。ドライバー モデルは MCU 周辺機器を OS サービスとアプリケーションに公開します。Azure Sphere ドライバーには、Wi-Fi (TCP/IP ネットワーキング スタックを含む)、UART、および GPIO などが含まれます。

Security Monitor

マイクロソフトの提供する Security Monitor は SW で実行されます。これは、メモリ、フラッシュ、およびその他の共有 MCU リソースといったセキュリティ重視のハードウェアを保護し、これらのリソースへの限定的アクセスを安全に公開する役割を持っています。Security Monitor は Pluton セキュリティ サブシステムおよびハードウェアの信頼のルートへのアクセスを仲介および制御し、NW 環境の監視人のような働きをします。ブート ローダーの開始、ランタイム サービスの NW への公開、ハードウェア ファイアウォールと NW にアクセスできないその他のシリコン コンポーネントの管理を行います。

ソフトウェア開発エクスペリエンス

Azure Sphere は、Microsoft Visual Studio に基づいたリッチな開発エクスペリエンスを提供します。Visual Studio Tools for Azure Sphere では、IntelliSense と PC からのブレークポイントベースのデバッグと共に、Azure IoT Hub を使用するためのウィザードがサポートされます。サンプル アプリケーションとプロジェクト テンプレートも付属しています。

Azure Sphere Security Service

Azure Sphere Security Service は、証明書ベースの認証、アップデート、および障害レポートの 3 つのコンポーネントで構成されます。

- **証明書ベースの認証。**認証コンポーネントは、リモート認証と証明書ベースの認証を提供します。リモート認証サービスは、Pluton サブシステム上のメジャー ブート機能を使用するチャレンジ/応答プロトコルを介して接続します。それによって、デバイスがブートされたのが適切なソフトウェアであることだけでなく、そのソフトウェアの適切なバージョンであることも保証されます。リモート認証が成功すると、認証サービスが引き継ぎます。認証サービスはセキュリティ保護された TLS 接続経由で通信を行い、デバイスが Microsoft Azure などの Web サービスに提出できる証明書を発行します。Web サービスは証明書チェーンを検証し、デバイスが正規であり、ソフトウェアが最新で、マイクロソフトがその提供者であることを確認します。その後デバイスはオンライン サービスに安全に、かつセキュリティで保護された方法で接続できます。
- **アップデート。**アップデート サービスはマイクロソフトが提供するすべての Azure Sphere OS および OEM ソフトウェアに自動アップデートを配布します。アップデート サービスは Azure Sphere SDK のクラウドおよびデバイス ユーティリティと連携して、継続した運用を確保し、メーカーが自社のアプリケーション ソフトウェアをリモートでアップデートおよびサービシングすることを可能にします。
- **障害報告。**計画された障害報告サービスは、展開されたソフトウェアのシンプルなクラッシュ報告を提供します。より詳細なデータを入手するには、メーカーは自分の Microsoft Azure サブスクリプションに含まれるレポートおよび分析機能を使用できます。

一般的には、Azure Sphere アプリケーションでは、設計者は必要に応じてどれほどの Microsoft Azure 機能を使用するかを選択できます。シンプルなアプリケーションでは、クラウド関連のコードは必要ありません。より一般的なアプリケーションでは、デバイスの運用を監視してデータを Azure IoT Hub、メーカーのクラウド サービス アプリケーション、またはメーカーのセキュリティ保護された Web サイトに報告する場合があります。

詳細情報

Azure Sphere の詳細については、以下の参考資料を参照してください。

- Azure Sphere の一般的な概要については、Azure Sphere Web サイトを参照してください。
- Azure Sphere 設計のセキュリティ原則の説明については、「The Seven Properties of Highly Secure Devices」を参照してください。
- 特定の Azure Sphere MCU のハードウェア機能と設計の考慮事項の詳細については、その MCU のデータ シート、ユーザー ガイド、およびアプリケーション ノートを参照してください。これらのドキュメントは、Azure Sphere MCU 製品を製造するシリコン ベンダーから入手できます。場合によっては、この情報を入手するために関連するシリコン ベンダーとの秘密保持契約に同意する必要があることがあります。
- ソフトウェア プラットフォーム、開発エクスペリエンス、および潜在的なアプリケーション機能に関する情報については、SDK と共にインストールされる Azure Sphere 技術文書を参照してください。『作業の開始』は、セットアップとサンプル コードについて順を追って説明します。『アプリケーション開発ガイド』は、A7 アプリケーションの開発者のための概念および運用に関するドキュメントです。『デプロイメント ガイド』は、Azure Sphere アプリケーションの展開とアップデートについて説明しています。『コマンドライン ユーティリティ リファレンス』は、コマンドライン ツールの参照情報を提供します。最後に、『API リファレンス』は、お客様の A7 アプリケーションにアクセス可能なアプリケーション プログラミング インターフェイス (API) に関する詳細情報を提供しています。