ホワイトペーパー

モノのインターネットの戦略的活用

IoTのコンテキスト/データとビジネスの目的を関連付けて、戦略的目標を達成する

aruba
a Hewlett Packard Enterprise company

目次

教授ときこり

数年前、イェール大学のインダストリアルエンジニアリング学科の責任者は、「問題を解決するために1時間しかなかったら、1時間の3分の2は問題の定義に費やすでしょう」と述べました[1]。 同じように、あるきこりも、「ある木を伐採するのにわずか5分しかなければどうしますか」と尋ねられました。彼は「最初の2分半は斧を研ぐことに費やすでしょう」と答えました[2]。 業種や業務にかかわらず、慎重に目標を定義し、目標を達成するために必要なツールを選択し、準備することが肝要なのです。

残念なことに、この教訓はモノのインターネット（IoT）プロジェクトでは見過ごされていることが多くあります。IoTのコンセプトに魅力を感じている（あるいはよく理解していない）、競合他社に後れを取ることへの恐れ、新たな挑戦をしなければならないというプレッシャーなど、さまざまな理由から多くの企業がIoTプロジェクトに取り組むようになっていますが、目標、価値、そして適切なツールを明確に定義していないことが少なくありません。このため、IoTプロジェクトが失敗する確率が高くなり、企業の顧客はそのサービスに幻滅することになります[3]。

この問題の原因の一端は、モノのインターネットという言葉が独り歩きをしており、誤解を招いていることです。IoTは相互接続されたマシンのエコシステムの総称でしたが、その後、あらゆるデバイスをインターネットに接続する状態と捉えられるようになりました。IoTの最も重要な目的は、企業にあるすべてのデバイスをネットワーク化することではなく、ましてやあらゆるデバイスをインターネットに接続することでもありません。IoTデバイスはコンテキストとデータを乗せた船のようなものであり、関連性の高い情報（デバイス）を乗せた船だけを寄港させる必要があります。

では、関連性の高い情報かどうかをどのように判断できるのでしょうか。関連性の判断は、企業の戦略的な目標から、目標達成のために設計されたビジネス上の目標、お客様との関係において現状を一変させるような変革、リスク、機会をもたらすとガートナーが説明している「決定的な瞬間」までの流れ（チェーン）の中で確立されます[4]。「決定的な瞬間」とは、企業の戦略的な目標と関連するIoTコンテキストとデータ（図1）が1つになるポイントであり、この瞬間を活かすことができれば、お客様の行動、考え、さらには思いを大きく変えることができます。

「決定的な瞬間」は、お客様側からすると自然に発生するものですが、企業にとって慎重なオーケストレーションが求められます。このオーケストレーションが成功するかどうかは、目標とする「決定的な瞬間」のための情報にアクセスし伝達するIoTアーキテクチャーと、関連性のあるIoTコンテキストおよびデータをつなぐ第2のチェーンにかかっています。IoTアーキテクチャーが有用な情報を取り出すことができないなど、このチェーンが十分な機能を発揮しないと、何も成果を残すことなく決定的な瞬間が過ぎ去ってしまい、目標の達成に失敗したという否定的な感情を作り出してしまう恐れすらあります。

ここで教授ときこりの話をもう一度思い出してください。IoTプロジェクトで最初に実施するべきことは、達成すべき戦略的なビジネス目標を立てることです。それらは、決定的な瞬間を捉えるための具体的な目的につなげる必要があります。IoTアーキテクチャーは、関連性のあるIoTコンテキストとデータを抽出および活用することで、戦略的目標に沿ってお客様の行動や考え方を新しい方向へと向けるようにするためのツールです。

ビジネス目標をまず確立し、IoTアーキテクチャーおよび関連するデバイスにその目標を伝達するのであって、その逆ではありません。ビジュアル的なアピールや誇大広告によって選択されたIoTソリューションでは目標を達成することはできないでしょう。

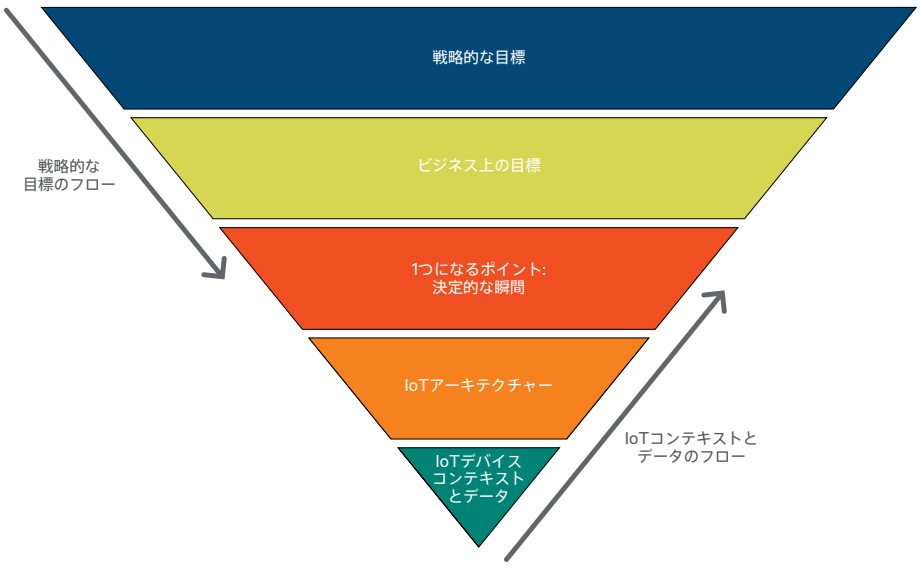


図1: IoTの戦略的階層構造

橋を架ける

ビジネス目標と目標を達成するために必要なIoTアーキテクチャーを適切にブリッジングするには、プロセスのガイド役となるフレームワークが必要となります。さまざまな事業部門の関係者は、各部門の指針よりも企業全体の目標を優先させることが求められる場合があります。マネジメント、製品、技術設計、IT、および運用組織の全体で、新しい次元のコラボレーションが必要になります[5]。さらに優れた選択肢のために、既存のプロジェクトやテクノロジーを撤廃しなければならないかもしれません。特定のベンダーと長期にわたる関係を構築していても、適切なソリューションを提供できる新しいサプライヤーとの新たな歩みを始めなければならないかもしれません。

IoTバリューサイクル（図2）は、可視性、セキュリティ、イノベーション、収益性の4つの主要な要素にビジネス目標を分解して、IoTを成功に導くためのフレームワークを提供します。最初の2つの要素は、ビジネス目標に関連するコンテキストとデータを抽出するためのIoTインフラストラクチャに関連しています。残りの2つは、これらのコンテキストとデータを利用する決定的な瞬間を定義します。関係者とともにこれらの4つの要素を定義し適切に実装することで、IoTソリューションは目標とする決定的な瞬間を成功に導き、そのビジネス目標を満たします。

可視化は「接続の状況は万全か」という質問に答え、あらゆるデバイス、マシン、および関連するプロセス、業務、および顧客関連のコンテキストとデータの他のソースとのインターフェイスを作り出すことで実現されます。この目的のために導入するインフラストラクチャは、アプリケーションによって異なります。自動車関連のアプリケーションでは移動型テレマティクスが、監視制御とデータ収集システムではLANとメッシュワイヤレスが必要な場合がありますが、オフショアの石油プラットフォームではClass 1 Division 1の要件に適合する防爆のWi-Fiインフラストラクチャが必要となる場合があります。

関連するデバイスの物理的な設置場所にかかわらず、信頼できるソースの信頼できるデータのみを確実に参照して利用できるようにする必要があります。つまり、IoTデータは、そのライフサイクル全体において、移動中でも保管中であっても、適切に保護され管理される必要があります。デバイス、オペレーティングシステム、BIOS、およびインフラストラクチャは、外部からも社内からでも、改ざんから保護する必要があります。IoTソリューションとそのツールを導入して保守にあたるユーザーについても、安全に管理することが求められます。常時稼働を確実に実現するために、アプリケーションとシステムを保証する必要があり、データの利用方法についての適切なガバナンスを常に適用しなければなりません。サイバーセキュリティ環境は常に進化しており、信頼を常に得ることは決して容易ではありません。万全のセキュリティが確立されているかを繰り返し自問し、IoTプロジェクトのライフサイクルを通して最新の保護機能が常に適用されていることを確認する必要があります。

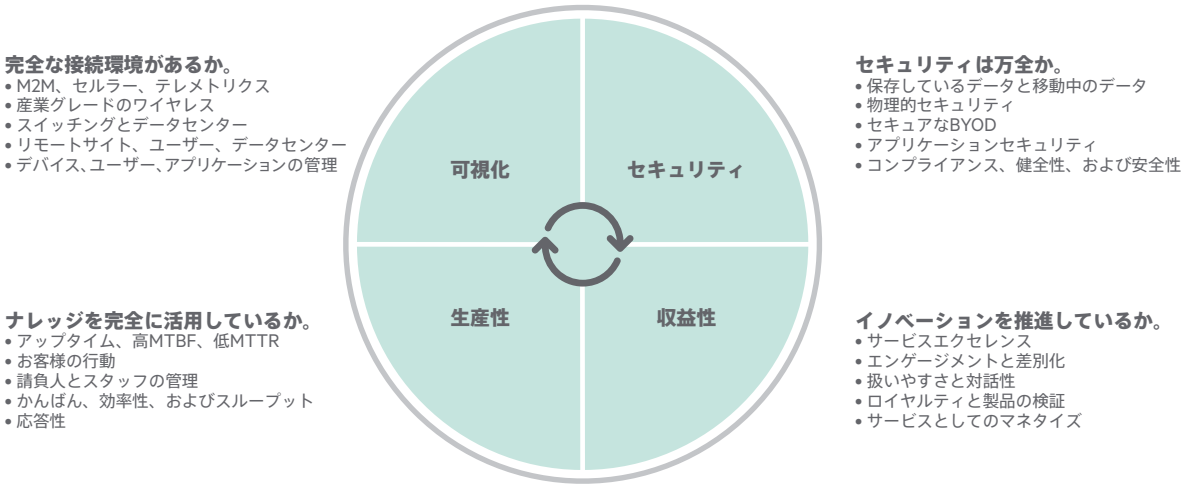


図2: モノのインターネットのバリューサイクル

IoTアーキテクチャーはセキュリティが確保された環境で、データソースにアクセスし、抽出された情報のライフサイクルを管理する必要があるため、その可視化とセキュリティが重要となります。そのため、可視化とセキュリティはIoTの戦略的な階層構造の第2レイヤーとして定義されます。

IoTの戦略的な階層構造の基盤となるこの場所で、IoTデバイス内に保管されているか、IoTデバイスによって生成される有用なコンテキストやデータと、アクセシビリティと信頼性（セキュリティ）との連携を図る必要があります。コンテキストやデータの関連性を考慮することなく、あらゆるデバイスを取り込んでしまうと、接続が追加されるときのデバイスコスト、可視性とセキュリティの強化による人件費や設備投資、抽出されたデータの処理と保存、有意な情報の選別に必要となるリソースなど、さまざまなコストが増大します。

関連性の高いデバイスを特定し、特定のIoTデバイスを対象とするためのガイドラインは、収益性と生産性の向上の要素に分類されます。収益性の向上は、お客様に対するサービスの向上、お客様の嗜好やニーズに合った優れた製品やサービスの提供、業務に対する行動や姿勢のポジティブな変化によって、収益を増大したりコストを削減したりして達成されます。「イノベーションに十分に取り組んでいるか」いう質問は、サービスエクセレンスを実現し、お客様との関わりを深め、競争力を高め、ビジネスのやりとりを簡略化し、ロイヤリティを強化し、製品の性能を検証し、サービスをマネタイズする方法の解決につながります。

生産性は、IoTバリューサイクルの第4かつ最後の要素であり、人と資産を可能な限り効率的に稼動させることにフォーカスしています。アップタイムを最大化し、ダウンタイムを最小限に抑え、セールスとサポートプロセスを合理化し、お客様とスタッフを効率的に管理し、資産の活用とプロセススループットを最適化し、要求や変更に対するレスポンス力を高めることで、生産性の向上が実現されます。「ナレッジを十分に活用できているか」という質問は、IoTのコンテキストとデータを活用して効率性を向上させる上で役立ちます。

可視化、セキュリティ、収益性、および生産性についての具体的な取り組みはお客様によってそれぞれ異なります。同じ業種であっても、あらゆる環境に適合する万能型のIoTソリューションは存在しません。企業の目標はそれぞれ若干異なっており、目標を達成するために必要ソリューションもそれぞれ異なります。競合他社の動向を把握することは有益です。しかし、自社の目標と決定的な瞬間が他社と一致していない限り、他社の解決策がそのまま自社に役立つとは限りません。先にIoTに取り組んでいる競合他社に追従しても、賢明な選択肢とはならないかもしれません。

IoTの戦略的階層構造（図3）をIoTのバリューサイクルと重ね合わせることで、目的とアーキテクチャーを適切に連携（ブリッジング）させることが可能になります。収益性と生産性の要素から適切なコンテキストとデータにつながるソースを特定し、可視化とセキュリティの要素からこれらのソースの情報を取り込むために必要なアーキテクチャーとインフラストラクチャを作り出します。

このブリッジングについて、事例を見ながら説明します。この後のセクションでは、小売などのさまざまな業界の状況について説明しますが、最初にセキュリティについて詳しく説明します。

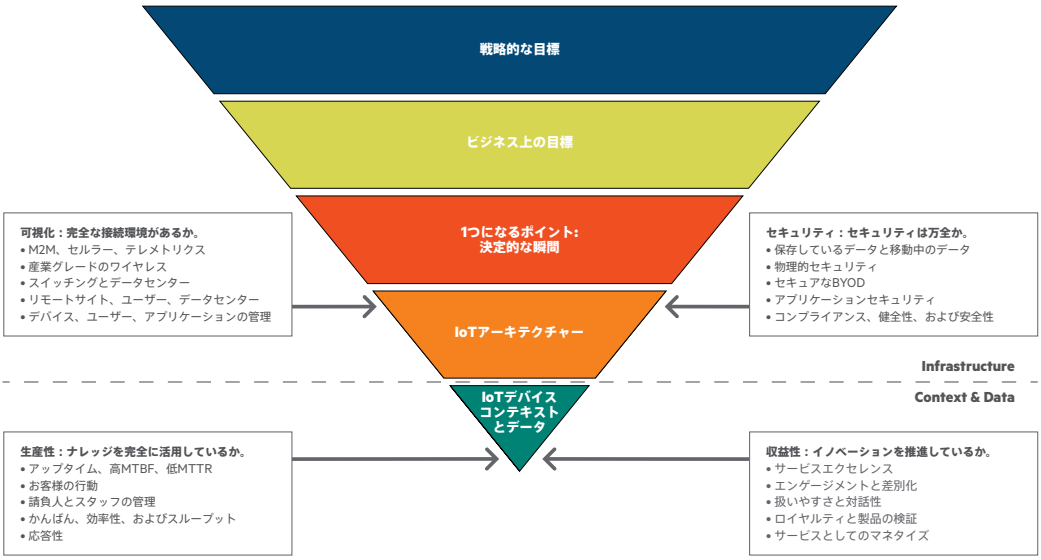


図3: ビジネスの目標とアーキテクチャーとIoTコンテキスト/データのブリッジング

外部からの攻撃と内部からの脅威の両方に対応するセキュリティ

IoTネットワークへの侵入とデータ侵害は、原子力、小売、ヘルスケア、コンシューマー業界などあらゆる業界において日常的に発生しています。その理由は極めて簡単です。ほとんどのIoTデバイスとその実装におけるセキュリティが貧弱または欠如しており、信頼できないためです。IoTデバイスを設計するエンジニアは、通常、プロセスの信頼性とアプリケーション固有のアーキテクチャーについてのトレーニングは受けています。これらのエンジニアが受けているトレーニングは、できるだけ長期間、製品を確実に稼動させることを目的とした運用テクノロジー（OT）の分野に該当します。一方で、サイバーセキュリティの専門性は、情報技術（IT）のエンジニアの担当になっています。OTとITがIoT製品とシステムの設計において緊密に連携されていないと、信頼できないソリューションになってしまう恐れがあります。

意図的に操作されるリスクのあるIoT情報とプロセスを利用することは、賢明ではありません。使用する情報の完全性と信頼性には万全を尽くす必要があり、IoTデバイスからそれらを利用するアプリケーションまで完全な信頼性が求められます。新しいIoTデバイスにセキュリティ機能を組み込み、レガシーデバイスを保護機能で包み込むことによって、デバイスやユーザーが認証されるまで信頼しない防御フレームワークを作り出すことで、これを達成できます。このフレームワークでは、多数のソースからのコンテキスト情報を活用して、接続前と接続後にユーザーとデバイスのセキュリティ状況を精査する必要があります。

ArubaのIoTセキュリティフレームワークはConnect-and-Protectと呼ばれ、次の保護機能が含まれています。

- ソース/データの送信先デバイスを認証し、センサーの入力およびバスを含むトラフィックパターンを監視。
- 商用および可能な場合には政府機関の暗号化標準を使用してデータパケットを暗号化。
- パケットをセキュアトンネルに入れて、目的の送信先にのみ転送。
- IoTデバイスが信頼できるか、不明なデバイスかどうかを判断し、アクセスおよびネットワークサービスを制御する適切なロールおよびコンテキストをベースとするポリシーを適用できるようにIoTデバイスにフィンガープリントを適用。
- アプリケーションファイアウォールとマルウェア検出システムを使用して、ノースサウストラフィックを監視し、動作を管理。
- エンタープライズモビリティ管理（EMM）、モバイルアプリケーション管理（MAM）、モバイルデバイス管理（MDM）システムを活用して、ポリシー違反が発生した場合に動作を監視し、他のデバイスを保護。

図4: IoTのセキュリティメカニズム「Connect-and-Protect」

特にArubaのClearPass Policy Managerは、IoTデバイスのプロファイリング、アイデンティティおよび動作管理において優れた効果を発揮します。フィンガープリントをプロファイリングし、接続するIoTデバイスを分類して、デバイスタイプを区別し、別のユーザーに悪意を持ってなりすましている攻撃者を検出します。アイデンティティによって、場所、時刻、曜日、現在適用されているセキュリティ対策など、いつ、どのように接続するのかを決定するロールがIoTデバイスに適用され、ロールベースの詳細なアクセス制御が可能となります。ここでは、既知の脆弱性、アクティブポート、オペレーティングシステムのバージョン、およびその他の機能におけるSNMPのセキュリティを判断するためのヘルスチェックがセキュリティ対策として実行されます。コンプライアンス対応を確実にするためにセキュリティ対策を定期的に検証する必要があり、セキュリティ対策が一定の基準に達していない場合、信頼されているデバイスであってもアクセスを拒否するようにできます。

ClearPassは、プロファイル、アイデンティティ、およびセキュリティ対策を活用しながら、IoTデバイスが信頼できるどうか、また、認識されているデバイスであるかどうかを判別し、その結果に応じて対策を講じます。デバイスが運用モードを変更したり、別のIoTデバイスのように偽装したりすると、プロファイリングデータにフラグが立てられ、ClearPassが自動的にデバイスの権限を変更します。たとえば、プログラマブルロジックコントローラーがWindows PCのように偽装されていると、ネットワークアクセスは直ちに中断されます。

ポリシーの効果は、ポリシーを構築するために使用される情報と、情報を保護するために利用するポリシー強制ツールによって決定されます。セキュリティに体系的なアプローチを適用することで、IoTの脅威のタイプを特定し、問題の修復に必要なセキュリティテクノロジーを特定できるようになります。

IoTのトランスフォーメションの終盤戦は、IoTデバイスの内部に埋もれている豊富なデータソースを活用してビジネストランスフォーメーションを実現することです。適切なセキュリティ対策をゼロから設計することで、IoTソリューション全体の信頼性を確保できます。信頼できるIoTアーキテクチャーを使用し、戦略的な目標をブリッジングすることに再び注力できます。ブリッジングのプロセスの仕組みを業界別のユースケースで見ていきましょう。

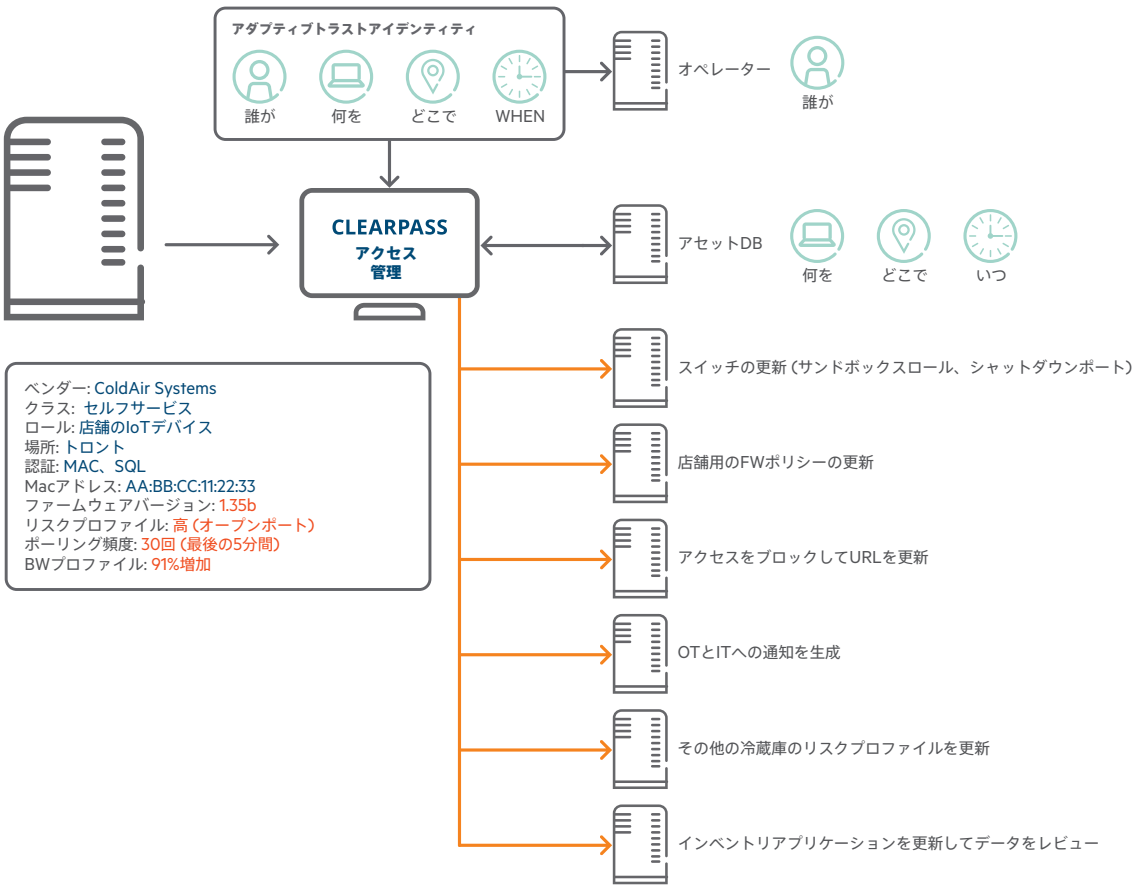


図5: ClearPassを利用したIoTデバイスのセキュリティ違反のワークフロー

各業界のユースケース: 小売

来年、ある国内の大規模小売業者は、バスケットのサイズを10％増加し、ストアの離脱率を半分にして、目標収入を達成する必要があります。これらの目標を達成するには、カスタマーエクスペリエンスの向上に取り組む必要があります。カスタマーエクスペリエンスを向上するために、いくつかの目標を設定します。最初に、購入範囲内の価格帯の関連商品をお客様に提示し、簡単に見つけることができるようにして、不満を抱いて店舗を後にすることがないようにします。第2に、商品を実際に店舗で見た後で、価格を確認した後にオンラインで購入する（ショールーミング）お客様は、店内で買い物をすることに価値を見いだしてもらうようにする必要があり、何らかの形でアクティブな対応が必要となります。最後に、必要な商品が見つからなかったお客様がお店を去ることがないように迅速な対応が必要となり、直接お客様に対応するスタッフの比率について慎重な管理が必要となります。

お客様、従業員、在庫は流動的であるため、バックエンドCRM、POS、在庫管理アプリケーションと連携するIoTロケーションベースのサービスは、最も有用なツールとなります。ロケーションサービスは、以下のような質問を解決します。

- 「自分がどこにいるか」
- 「お客様がどこにいるか」
- 「商品はどこにあるか」

この小売アプリケーションでは、次のビジネス目標を達成する必要があります。

- 店舗に来た既存の顧客を特定し、小売業者が過去の購入歴やWebでの活動を分析でき、今回店舗に来た目当ての商品をリアルタイムでオファーできるようにします。
- お客様がスマートフォンで在庫を検索でき、在庫にある商品または別の商品を購入するためのターンバイターン方式の指示を受けることができるようにし、バスケットサイズを増やすアップセル機会を最大化できるようにします。
- お客様がWebを自由に閲覧できるようにWi-Fiを提供し、お客様が使用しているアプリケーションや使用場所を確認できるようにします。たとえば、ショールーミングに対応するため、小売業者は電子看板の情報を更新し、インターネットとの価格マッチングに関するメッセージを送信します。この情報は、店舗関係者にも通知されるので、お客様に店舗で購入してもらうように働きかけることが可能になります。
- 店舗のあらゆる場所でサービスが行き届くように、お客様の場所と、スタッフが対応できるお客様の数の比率を監視します。

ビジネスの目標を確立したら、適切なIoTツールの選択を始めます。次のテーブルは、さまざまなArubaのIoTロケーションベースサービスオプションを示しています。適切なソリューションを決定するために、最初に概要的な質問への回答から開始し、最終的には特定のIoTツールを推奨して終了します。

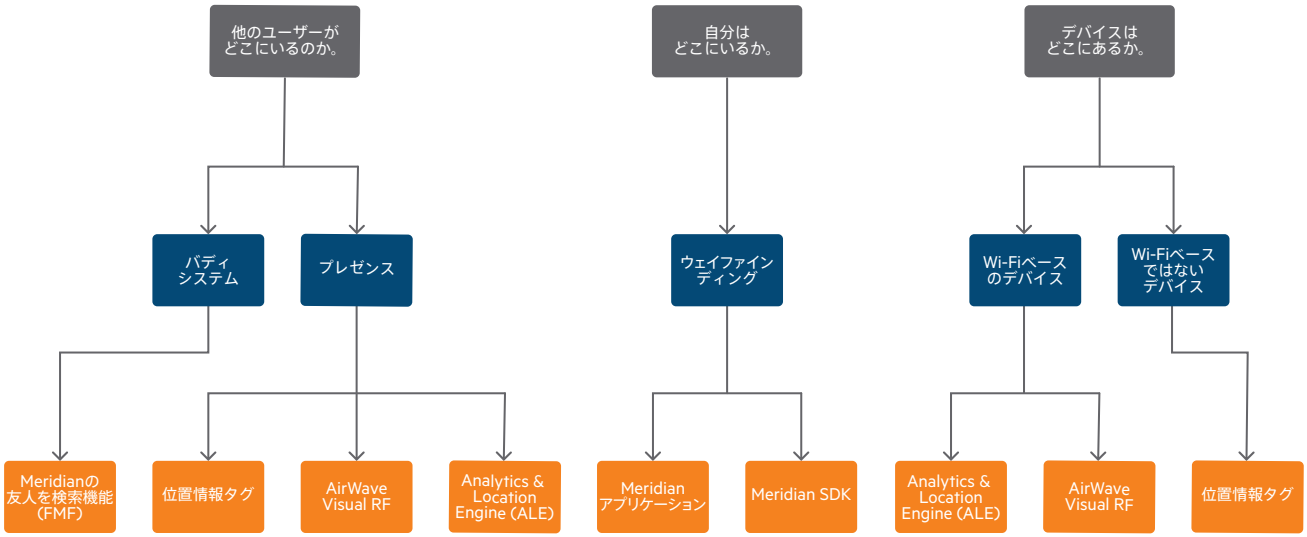


図6: ロケーションベースサービスのオプション

各企業がビジネス目標を達成するためにには、4つの異なるタイプのロケーションツールが必要です。

- ウェイファインディング (Wayfinding): 屋内版のGPSと考えることができるサービスであり、お客様がサイト内を自分でナビゲーションできるようにするアプリケーションです。たとえば、地理的な境界線を越えるとアラートしたり、お客様に直接メッセージをプッシュしたりできます。
- プレゼンス: いつ、どのようなお客様がいるのか、オンラインでどのような操作を行っているのか、そしていつジオフェンス境界から離れているのかを判断します。
- バディシステム (Buddy System): 店舗全体で従業員がどこにいるかを把握します。
- 非Wi-Fiベースの資産追跡: 資産、パレット、および商品の場所を識別します。

リアルタイムでお客様の行動を変える直接的なやり取りこそが、最も効果的なカスタマーエンゲージメントとなります。つまり、お客様のスマートフォンまたはタブレット上で実行され、ウェイファインディング、メッセージの配信、およびジオフェンスによってお客様に直接配信できるアプリケーションは高いエンゲージング効果を発揮します。ArubaのMeridianサービスは、1つのアプリで3つの重要なサービスをすべて提供します。このソリューションは屋内版GPSのようなウェイファインディング機能を提供し、ターンバイターン方式の指示とマップ上のリアルタイム位置をゲストに提供します。Meridianのフレンド検索 (Find A Friend) 機能により、店舗のマネージャーは店舗従業員が今どこにいるかを直接把握できます。ジオフェンスによって、お客様が店舗内にいるときにアクションやアプリケーションをトリガーさせることができるようになります。

Meridianは、複雑なブール条件処理を実装するビジネスルールエンジンだけでなく、顧客関係管理 (CRM)、POS (販売時点情報管理)、およびその他のバックエンドアプリケーションとも連携させることができます。メッセージプッシュ機能によって、即時のフィードバック、商品の紹介、およびアップデートが可能になります。小売業者が自社独自のアプリケーションを利用している場合で、Meridian SDKによってそのアプリケーションに代わる同等のサービスを提供できます。

お客様がオンラインショッピングサービス（Amazonなど）をチェックするタイミングを知る必要があるため、ウェイファインディングからショールーミング検出に移行することは容易ではありません。ArubaのAnalytics & Location Engine (ALE) は、サービスを利用することを明確に同意してもらったお客様のWi-Fiデバイスを使用し、店舗内の全員のx/y位置を計算し、Wi-Fiネットワーク上で実行されたURLサーフィンを監視します。ALEはバックエンド分析エンジンと連携させることができ、小売店がお客様がショールーミングを行っているかどうかを識別して、店頭でのセールスにつなげる多くの機会を提供できるようになります。

ALEのx/y位置の監視機能は、バックエンドまたはクラウドアプリケーションとともに使用して、従業員が対応できるお客様に関する比率を監視することもできます。この比率が最小許容レベルを下回ると、従業員と店舗のマネージャーの両方に通知できます。ALEのロケーションプロセスには、通りがかりのユーザーと入店者のトラフィックを監視し、店舗に入るユーザーの割合を小売業者が把握できる利点もあります。

図7は、小売業者の戦略的な目標を決定的な瞬間にどのように結び付け、その決定的な瞬間がIoTインフラストラクチャとそのタスク向けのデバイスデータによってどのように処理されるかを示しています。この例では、ハイレベルの目標を、決定的な瞬間を成功させるための特定のIoTツールに落とし込む方法を示しています。

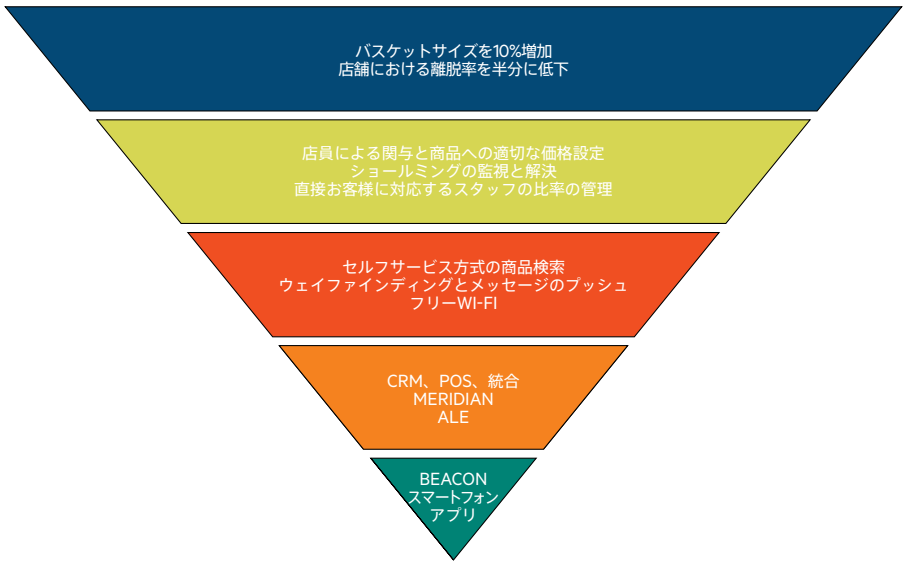


図7: IoTインフラストラクチャと小売業者の戦略的な目標との整合性の確保

目標とツールの整合が取れていない場合、IoTプロジェクトは思わぬ方向へ逸れてしまうことがあります。たとえば、プレゼンス分析によって受動的にお客様のロケーションを追跡すると、お客様の行動を一部把握でき、お客様がどこにいるかは分かりますが、お客様の購入行動をリアルタイムに変えることはできません。既存のWi-Fiインフラストラクチャに簡単に追加して導入できるという理由から、多くのプレゼンス分析プロジェクトが開始されていますが、プレゼンス分析の結果をセールスの向上につなげる方法がなかったために、その後、多くのプロジェクトが頓挫することになっています。IoTプロジェクトに着手する前に、IoTソリューションとビジネス目標を緊密に連携させるという明確な教訓が得られたのです。

各業界のユースケース: ヘルスケア

ヘルスケア業界でも、小売業界の例でも見られたロケーションサービスの一部が活用されています。その例を見てみましょう。来年度に向けて、多くの病院や診療所を有するマネージドケア組織は、拠点の設置面積、雇用者数、残業コストなどを増加させることなく、請求可能な来院数を10%増やしたいと考えています。患者と病院スタッフに対して実施された満足度調査では、患者が医師の診断を受ける時間がすでに許容されるレベルぎりぎりまで短くなっているため、予約される診察時間をこれ以上短縮することが難しいことが示されています。同じアンケートでは、予約している時間が守られないことについて患者と病院スタッフ両方の不満が示されています。大規模な病院施設では目的地に到達することが容易ではなく、英語以外を母国語とする来院者や高齢者はサイトマップを簡単に理解できない場合があります。利用できる診療室は当日に変更されることがありますが、診察予約のリマインダーは更新されない場合もあります。患者の遅刻や無断キャンセルなどによって午前の診察予定をこなすことができずに病院のスタッフと医師は苛立つことになり、午後の診察予約は現在のシフトが終わってから組み込むことになるため、この患者（怒っているかもしれません）を別の日に来院するように再度スケジュールすることが求められる場合もあります。

この組織の目標を達成するには、すべての診察予約が時間通りに実行され一日の終わりにバックアップが必要となることがないように、英語または英語以外を母国語とする患者が病院施設をスムーズに移動できるようにする効率的な方法が必要となります。ロケーションサービスを使用すると、「私はどこにいるか」、「患者はどこにいるか」、「診療施設はどこになるか」 という問題を解決でき、次のような目標を達成できるようになります。

- 各患者が診療所に到着した時に、予定の診療時刻と正確なオフィス番号を、患者が設定する言語でメッセージをプッシュします。
- 予定の場所や時間に変更があった場合は、更新したメッセージをプッシュします。
- 患者が来院するときに使用する入口や駐車場を考慮しながら、次の診察予約のためのターンバイターン方式の指示と到着時間を提供します。
- 外部や臨時の医師や病院スタッフにも同じメッセージプッシュとウェイファインディング機能を提供し、次の診察予定の場所に簡単に移動できるようにします。
- 病院スタッフは、患者が院内を移動しているときにその位置を追跡して、患者が診察に遅れた場合に電話で連絡できるようになります。

これらの目標を達成するには、3つの異なる領域のツールが必要です。

- 患者、職員、医師が自分が選択した言語でサイトを自分で移動できるようにするウェイファインディングアプリケーション。
- 患者が来院したときに、診察予約のスケジューリングシステムと通信し、挨拶のメッセージをユーザーの次の診察の場所と時間と共に送信するジオフェンシング機能。
- 病院スタッフが診察予定に遅れている患者や外部医師を見つけることができるようにするユーザー追跡機能。

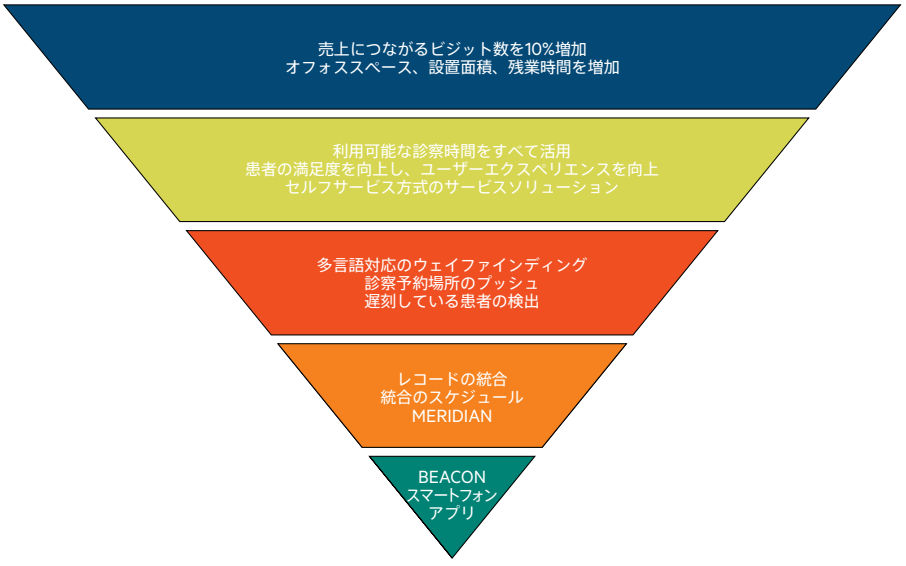


図8: IoTインフラストラクチャとヘルスケア組織の戦略的な目標との整合性の確保

前述のAruba Meridianサービスは、セルラー方式とWi-Fiの両方で動作しますので、携帯の通信網やWi-Fiのいずれかの対応範囲から外れているガレージや屋外などの場所でもサービスを配信できます。MeridianはWi-Fiネットワークに依存しておらず、ArubaやAruba以外のWi-Fiシステムの両方で動作します。

このソリューションを利用するには、患者記録、経理、および職員の人事システムと統合する必要があります。導入時の負荷は高くなりますが、導入が完了すれば、職員の時間およびアクティビティ管理の最適化、サイトの不動産管理の最適化、駐車場の空き状況の通知など、上記以外の付加価値サービスも提供できるプラットフォームとして活用できます。

一方、目標を確立しておかないと、最適ではないソリューションがベンダーから提供される恐れがあります。たとえば、ロケーションサービスを使用して電子メールやテキストメッセージを送信する場合、タイムリーに患者が受信しない恐れがあり、リアルタイムのウェイファインディングアプリケーションと比べて効果が低くなります。多言語マップをサポートする場合、多くの初期設定が必要となるかもしれませんが、患者や患者を支援するスタッフが最適な言語を選択できるようになります。また、病院のスタッフ情報をリアルタイムで更新できるため、無駄な労力を最小限に抑えながら、スケジュールを調整したり、扱いが難しい患者に適切な対応を行うことができるようになります。

各業界のユースケース: 石油 & ガス

ロケーションサービスとエッジ分析の両方を活用しているある業界のIoTの例を紹介しましょう。来年度に、25,000機のポンプジャックと15,000名の請負人を有する石油ガス会社が、ポンプのダウンタイムを10％削減し、産出量を減らすことなく請負人のコストを10％削減し、生産性を維持しながらスペアパーツを25％削減したいと考えています。この企業は、理論的なポンプの故障率からポンプ稼動のスケジュールを立てようとしましたが、その試みは失敗に終わっています。その結果、ポンプの停止が頻発し、結果的に生産収益が減少しました。さらに、ポンプのスペアパーツやパイプの紛失、誤配置、盗難によってコストが増大し、機器を適宜修理することが難しくなっています。在庫を移動しているのは誰か、また盗難や適正に記録されていないことが原因であるかどうかも分からないままになっていました。最後に、請負人のサービスの請求書を現場の実際の作業時間と手動で照合することも難題となっています。請負人があまりにも多く、会計の担当者が不足しているのです。

この企業の目標を達成するには、ポンプをリアルタイムで監視し、異常な動作を観察することで障害を予測するための仕組みが必要です。ポンプにはセンサーとアクチュエーターが装備され、ローカルの閉ループ制御に利用されていますが、閉ループ制御の目的以外に、これらのデータが分析されてインテリジェンスとして活用されていませんでした。稼動中のポンプ数が非常に多く、広域対応のセルラーネットワークの費用は変動するため、リモート解析のためにすべてのポンプデータを転送する場合、コストが高くなります。その代わりに、ポンプジャックでローカルに分析を実行し、異常な動作が検出された場合にのみ監視センターに通知すると、はるかに経済的となります。監視センターは、ポンプがあるサイトにデータが保管されていれば、必要に応じて追加のセンサーデータを要求することができます センターはまた、ポンプメーカーのデータベースと照合し過去の稼動データを分析して、異常な動作への最良の対応方法を判別できます。

請負人がポンプジャックやロジスティクス拠点に到着するタイミングを追跡し、そのデータを企業の会計アプリケーションと共有することで、請求された時間と現場での実際の作業時間を直接比較できるようになります。このソリューションは、レポート作成の自動化を要求することになり、手動の作業による追加の人件費が発生しません。また、すべての請負人がサービスに対する対価の支払を希望される場合に、請負人がこのシステムに完全に参加することを義務付ける契約上の変更も要求します。

ポンプサイトで請負人を監視するために使用するのと同じ追跡ソリューションは、ロジスティクス拠点でも使用できます。アクセスコントロールとCCTV（閉回路テレビシステム）とロケーションデータを共有することで、請負人のアイデンティティをサイトのビジットとリンクさせることが可能となり、在庫の紛失時には容疑者を容易に特定できるようになります。

石油ガス会社には、次のようなビジネス目標があります。

- ポンプジャック制御システムによって生成されたアナログおよびデジタルデータを処理できるようにし、異常を報告すること。
- 広域データ収集システムを管理するリモート監視センターの導入、ポンプデータのメタ分析、過去の障害データを活用した予測分析アプリケーションと連携させること。
- すべての請負人に、ポンプサイトまたはロジスティクス拠点での到着出発を報告するロケーションサービスアプリケーションをインストールすることの強制。これらの請負人は独立したエージェントであるため、プライバシー上の理由から、石油会社の施設の到着と出発によってのみアプリケーションを起動する必要があり、常時接続してGPSをトラッキングすることは許可されていません。

これらの目標を達成するには、いくつかの異なる領域のツールが必要です。

- ジャックポンプのセンサーとアクチュエーターのデータを取得し、データを処理する分析アプリケーションを実行し、その結果をリモート監視センターに通信するための広域ネットワークを提供して伝えるゲートウェイ。
- 広域ネットワークを管理し、集約されたデータに対して独自の分析を実行し、稼働状況の履歴やメーカーのデータベースなどの他のデータリポジトリと通信できるリモート監視システム。
- 請負人のスマートフォンやタブレットがポンプやロジスティクス拠点に出入りする際にアプリケーションを起動するジオフェンス機能。
- 請負人がサイトに出入りするときに毎回、アクセスコントロールおよびビデオ監視アプリケーションにアクセスし、請負人のアイデンティティデータと日時を記録できるインターフェイス。請負人がサイトにアクセスする権限がない場合、アクセス制御システムによって、アクセスが拒否されます。

ハイレベルな予測障害検出機能を実現するには、インテリジェントIoTデバイス、アクセスデバイス、通信メディア、IoTコントローラー、IoTビジネスおよびアナリティクスアプリケーション、およびシステム管理ツールなどの、さまざまな実装要件について複合的に対応できるいくつかの基盤が必要となります。

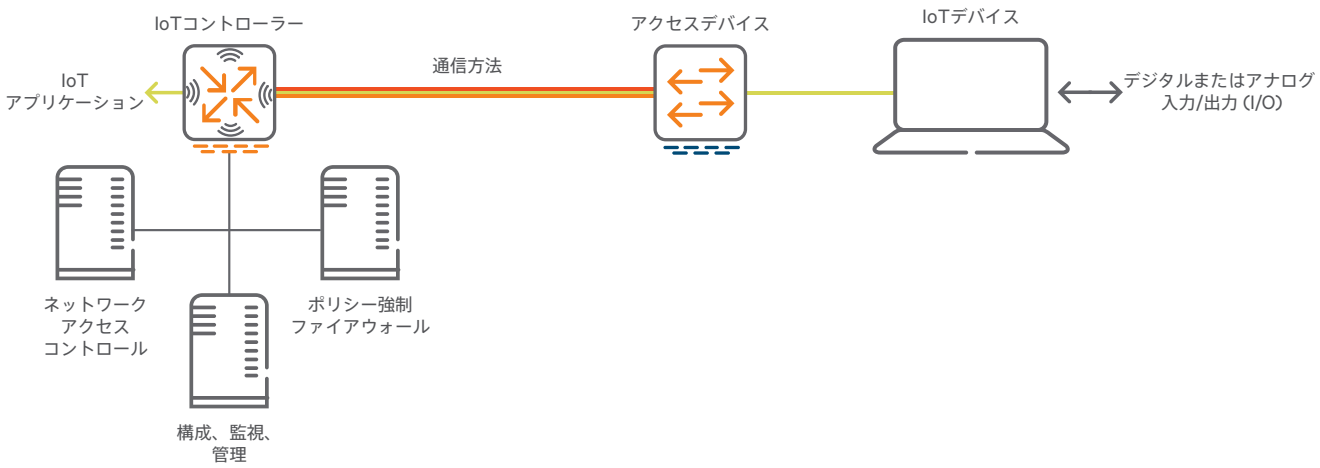


図9: 予測的な障害監視の構成要素

インテリジェントIoTデバイスは、企業が可視化したいと考えているアナログ、デジタル、または制御ネットワークのデータを生成するマシンを意味します（この場合はポンプジャック）。アクセスデバイスは、IoTデバイスと連携してデータを取り込み、次に、ローカルでアクションを実行するか、リモート監視サイトのIoTコントローラーにデータを送信します。

アクセスデバイスには、ゲートウェイおよびコンバージドIoTシステムの2つの形式があります。ゲートウェイは、IoTデバイスからのデータストリームを、利用しているネットワークと互換性のある安全な形式に変換します。IoTデバイスがネットワーク（LAN、セルラー、Wi-Fi）と安全に通信する機能を備えていない、セキュアなリモートアクセスのためのローカルVPNクライアントを実行できない、また、広域ネットワークと互換性がないシリアル、アナログ、または独自仕様の入出力（I/O）がある場合に、ゲートウェイは使用されます。

図10: Aruba Edgelineゲートウェイアクセスデバイス

コンバージドIoTデバイスにはI/Oインターフェイスがあり、IoTデバイスのデータをローカルで処理するコンピューティングパワーがあります。このソリューションは、プロセスのレイテンシの短縮、広域データ通信トラフィックの量とコストの削減、ローカルIoTアクティビティの処理と保存、およびローカルIoTアクティビティのサマリデータのリモートデータセンターへの送信に使用されます。コンバージドIoTデバイスは、機械学習とデータ分析エンジンをローカルで実行することでこれらのタスクを達成します。これらのデバイスには強力なコンピューティングエンジン、アナログ/デジタルセンサーのデータとコントロールバストラフィックの処理機能、およびリモート管理機能という特長があります。

図11: ArubaコンバージドIoTシステムアクセスデバイス

石油ガス会社の場合、広域ネットワークの費用をできる限り抑えるためにローカルインサイトが必要となるため、コンバージドIoTシステムが最適なアクセスデバイスとなります。セルラー方式は、ある通信電波塔で障害が発生した場合でも耐障害性に優れているため、このシステムでは通信方法として携帯電話ネットワークを使用して、展開にかかる時間を短縮します。

セルラー方式の費用は、ヒューレット・パッカード エンタープライズの仮想移動体通信事業者 (MVNO) 向けサービスを使用して決定されますが、この費用は、マシン監視アプリケーションなどの低帯域幅のIoTアプリケーションに対して事前に交渉されています。分析ソフトウェアを備えたコンバージドIoTシステムを使用してオンサイトでIoTデータを前処理すると、セルラー通信の量とコストが大幅に削減されます。

ArubaのVIA VPNは、ポンプジャックと監視センター間でデータを暗号化してトンネリングします。VIAは、AES 256ビットの暗号化鍵をサポートし、ネットワークレベルのピア認証、データ発信元認証、データ整合性、リプレイプロテクションを提供します。政府のIoTアプリケーションの場合、VIAはSuite B規格の楕円曲線暗号を使用して、最高レベルのTop Secretに分類される情報を保護できます。

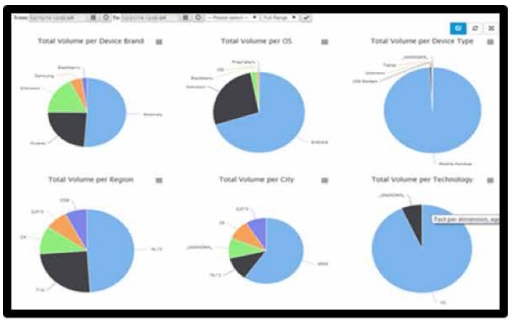
VIA VPNの終着点は、石油ガス会社のデータセンターにあるIoTコントローラーです。コントローラーは、ネットワークの暗号化と認証を管理し、ファイアウォール、ネットワークアクセスコントロール、およびアプリケーションレイヤーセキュリティ、パケットの優先順位決定、アクセスルールを適用するポリシー管理アプリケーションとのインターフェイスとして動作します。コントローラーソフトウェアのインスタンスは、プライベートおよびパブリッククラウドアプリケーション向けのハードウェアコントローラーの代わりに使用できます。

図12: Arubaコントローラー

分析アプリケーションは、コンバージドIoTシステムと監視システムの両方で動作します。分析アプリケーションは、IoTデータを利用し、数学および統計的手法、機械学習、および予測モデルを使用して異常な動作にフラグを立て、ポンプのメーカー、内部のサービスレコード、さらには他の企業サイトのデータプールをマイニングすることで、障害を予測します。HPE Vertica、SAP HANA、GE Predix、Schneider Wonderwareなどのアプリケーションを利用できます。

ポンプジャックのサイトは、HPEのユニバーサルIoTプラットフォーム (UIoT) アプリケーションを使用して監視されます。UIoTは、IoTデバイスを監視するためのさまざまな専門サービスが含まれる強力なアプリケーションスイートです。提供されるサービスは、次のとおりです。

- クライアントアプリケーションがデータを利用できるようにするAPI。
- 新しいアプリケーション、マイクロサービス、およびアルゴリズムを迅速に導入できるようにするデジタルサービス。
- Arubaのゲートウェイおよびコンバージドプラットフォームからのデータ収集、オープンソースのメッセージブローカリングによるIoTプロトコル。
- セルラーインフラストラクチャの管理
- 構築済みのアルゴリズムとすぐに使用できるテンプレートを利用できる堅牢な予測分析。
- oneM2Mまたは同等のデータ構造標準の遵守。一般的に使用される制御プロトコル用の組み込みプロトコルライブラリ。
- デバイスとサブスクリプション管理の両方を含むオープンスタンダードのメッセージングバスを介するメッセージキューイング。



FEATURES	CORE BASELINE	OPTION	MODULE
Managing devices and services	Yes		DSM
Uplink and downlink data acquisition	Yes		NIP
Data acquisition and validation	Yes		DAV
APIs exposure	Yes		SGF PRM
Advanced dashboard	Yes		Console
Relational database	Yes		EDB
Dashboard designer		Yes	Console designer
Analytic columnar database		Yes	Vertica
Alarms handling and correlation		Yes	TeMIP/UCA
Micro service design and execution		Yes	SIS

図13: UIoT IoTデバイス監視システム

UIoTは、oneM2Mの業界標準を遵守しながらIoTデバイスをサポートしており、各種のIoTアプリケーションおよびプロセスをサポートします。同じプライベートまたはハイブリッドクラウドプラットフォームで、デバイスの検出、構成、およびIoTトラフィックの制御（従来の音声およびデータトラフィックとは別に）などの新しいアプリケーションのインスタンスを大規模に素早く作成できます。

Meridianプラットフォームと同様に、UIoTは、企業の現在の戦略目標を達成するために必要なサービスの他にもさまざまな価値を提供するサービスの基盤として活用できます。UIoTは、地上のモバイルテレマティクスアプリケーション、LoRaおよびSigfox長距離無線システムとのインターフェイスとして稼働し、他の監視、レポート、および監査アプリケーションとやりとりするためのさまざまなAPIを備えています。

請負人のロケーションサービスは、ArubaのMeridianジオフェンスとメッセージプッシュサービスによって提供されます。ポンプジャックおよびロジスティクス拠点にAruba BLE Beaconが導入されると、ポンプサービスおよび保管場所の境界にジオフェンスが確立されます。ジオフェンスのサイズは、場所に合わせて調整されます。請負人のスマートフォンやタブレットがジオフェンスに出入りするときに、ジオフェンスが起動し、そのユーザーのアイデンティティ、時刻、位置が記録されて、アカウンティングアプリケーションに通知がプッシュされます。Meridianがアクティビティを正しく記録していることを確認するメッセージを請負人にプッシュすることもできます。提供されたサービスの対価を支払うために請負業者がMeridianアプリケーションを使用していると主張することで、石油ガス会社は高いレベルのコンプライアンスを保証できます。

Meridianには、アカウンティング、アクセスコントロール、ビデオ監視ワークフローなど、他のアプリケーションとロケーション関連データを共有できるAPIが含まれています。この機能により、同じビーコンとアプリケーションをポンプジャックで使用したり、ロジスティクス施設のセキュリティシステムを起動させたりすることができるため、集荷や配送をカードアクセスやビデオ監視データと関連付けることも可能になります。在庫が減少しており、請負者の関わりがある場合、セキュリティレコードからその請負者を識別できるようになります。

この例では、石油ガス会社が、ポンプの稼動時間、請負者のコスト管理、および在庫のセキュリティなどの高レベルの目標を達成するために、どのようなIoTツールを選択し、これらの目標の達成に役立つ分析、レポート、およびロケーションベースのサービスを利用していくかを説明しました。

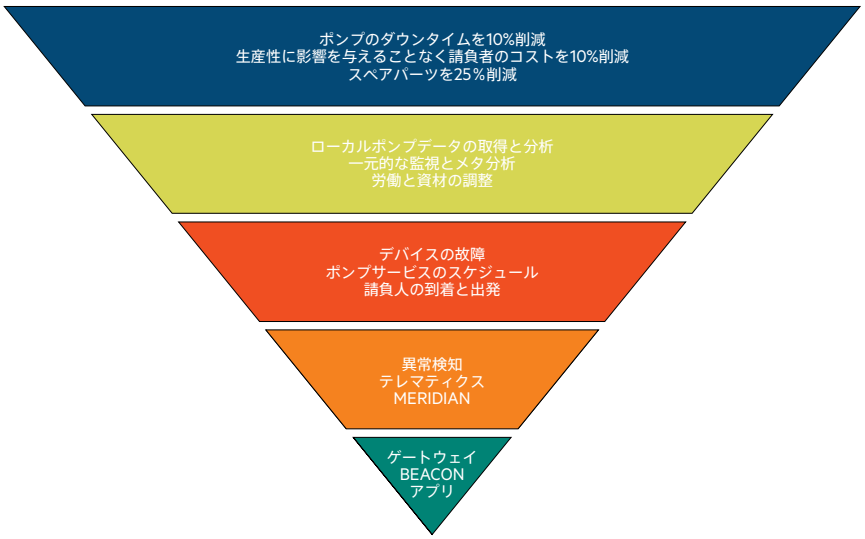


図14: IoTインフラストラクチャと石油ガス会社の戦略的な目標との整合性の確保

IoTのトランスフォーメーション推進のための最初のステップ

IoTツールは拡張性に優れ、将来的なビジネス目標にも対応できるプラットフォームであることが求められます。上記の3つのユースケースすべてにおいて見られるように、ArubaとUIoTのソリューションは、拡張性に極めて優れており、広範なユースケースに対応できます。

ビジネス目標とIoTアーキテクチャーのブリッジングに関する技術的な課題は、企業内での調整を行うために必要となる政治的なハードルと比べると、容易に克服できます。既存の問題や進行中のプロジェクトがあると、戦略的な目標やビジネス目標に影響を与え、異なる解釈をもたらし、その新しい解釈に合わせるように他のグループに要求することにつながることがあります。異なる事業部門の関係者は、プロジェクトや問題の管理をめぐって争うことがあり、特定のビジョンが明確になっていないと、支援や資金の確保が難しくなる場合もあります。

管理、製品、エンジニアリング、IT、および運用組織全体の関与が必要となる新しいレベルのコラボレーションを実現するには、中立的な第三者の介入が必要になることがあります。この目的のために、HPEのテクニカルサービスコンサルティング組織は、IoTプロジェクトについて統一されたビジョンを定義し、主要な関係者との連携を図り、戦略的な目標を設定し迅速に価値を創出できるようにするIoTワークショップを立ち上げています。詳細については、https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-7269ENW.pdfをご覧ください。

結論

IoTの最も重要な目的は、関連性の高いIoTのコンテキストとデータと企業の戦略的な目標を1つに収束させて、決定的な瞬間を成功に導くことです。決定的な瞬間を成功させるためには、お客様と関わることができる一瞬の機会を動的に活用しなければなりません。IoTのコンテキストとデータは、お客様の行動、態度、または企業に対する考えをプラスに変えることができる重要な役割を果たします。

IoTアーキテクチャーを介して広がる関係性の高いIoTコンテキストおよびデータのチェーンは、すべての部分が正しく実行されなければなりません。このホワイトペーパーでは、IoTの階層構造の要素に橋を架けて、IoTデバイスから関連するコンテキストとデータを抽出して利用するための適切なアーキテクチャーを実装する方法について説明しました。企業の目標に沿って、慎重に準備し、客観的な定義を用いて、適切なツールを選択すると、大きな効果を得ることができます。これを実現できれば、最も困難なビジネスの目標であっても達成することができます。

参考資料

1. William H. Markle氏、『The Manufacturing Manager's Skills』、『*The Manufacturing Man and His Job*』Robert E. Finley氏およびHenry R. Ziobro氏、American Management Association, Inc., New York 1966年
2. C. R. Jaccard氏、『Objectives and Philosophy of Public Affairs Education』、『*Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation*』、Chicago、Illinois 1956年
3. Alfonso Velosa氏、W. Roy Schulte氏、Benoit J. Lheureux氏、『*Hype Cycle for the Internet of Things*』、2016年、Gartner、2016年7月14日
4. 決定的な瞬間とは、人、企業、モノが一定のコンテキストの下で相互に関わり合い、特定の結果を生み出す瞬間であり、場所、時刻、CRMデータに基づいて小売業者がパーソナライズし対象を絞り込んだオファーとは異なります。Frank Buytendijk氏、『*Digital Connectivism Tenet 4: We Do Not Differentiate Between People and Things*』、Gartner、2016年11月1日
5. Dale Kutnick氏およびSaul Brand氏、『*Exploit Enterprise Architecture to Guide IoT Deployments at Scale*』、Gartner、2016年12月15日

a Hewlett Packard Enterprise company

3333 Scott Blvd | Santa Clara, CA 95054
1.844.473.2782 | 電話 : 1.408.227.4500 | ファクス : 1.408.227.4550 | info@arubanetworks.com

www.arubanetworks.com