製造業IoT & AI導入の要諦は、「セキュリティ」「設備連携」「導入ステップ」にあり！

人気セミナーに、ものづくり現場におけるDX成功のための勘所を学ぶ

ものづくりの現場では、IoT & AI を導入する動きが活発化している。だが、さまざまな課題から壁に突き当たる企業も少なくない。DX を成功へと導くために必要なこととは何か。人気セミナーに製造業 IoT & AI の要諦を探った。

製造業に特有の課題を解決し AI & IoT 活用を促すポイント

経済産業省が DX レポートを公表して以降、業界を問わず IoT や AI の活用が進む。そうした中にあってもオンプレミスにこだわり、新技術の導入が遅々として進まなかった業界が製造業だったといえるだろう。

だが、これもコロナ禍を背景に状況は一変した。今や国内外に生産拠点が分散することも珍しくない事業環境にあって、移動自粛などの制約は生産性や運用、コスト面に大きく影響。これを解決すべく DX へと舵を切る企業が急増したわけだ。

しかし、IoT や AI を活用したいという製造業が増える一方、ものづくりの現場に特有の課題から「取り組み方が分からない」「導入に行き詰った」との声も漏れ聞こえてくる。こうした悩みに応えるべく、「生産・製造現場における効果的な AI ＆ IoT 活用セミナー」は開催された。

その要諦は、データ収集から利活用までステップを踏んで導入を進めていくこと。そして、製造業に特有の課題であるセキュリティや設備連携などの課題を解消することという。以下、三つの講演プログラムから重要なエッセンスを抜粋して、製造業の AI & IT 活用を成功させるポイントをひも解いていく。

プログラム① IoT セキュリティ、その課題と対策

まず、登壇したのは日本マイクロソフト・IoT & MR 営業本部・技術営業部の平井健裕氏。「IoT におけるセキュリティ対策の課題と対策方法」をテーマに、IoT を実現する上でのセキュリティの重要性と、製造業ならではの注意すべき事情について語った。

IoT にとってセキュリティとは何か。これを説明するために、提示されたのがビジネスバリューを生み出す IoT 活用のプロセスだ。モノを見ること（監視）に始まり、リアルタイムのインサイトにもとづく改善から、新たなビジネスチャンスと競争優位性を創出する変革へとつながっていく。セキュリティとは、これらプロセスの前段階に位置しており、価値と復元力を支える基盤であるとした。

さらに、セキュリティはビジネス価値に直結するものではないが、それを軽視すると以降の IoT 活用プロセスで生み出されるはずの価値を台無しにするとも。

実際、多くの企業が IoT 導入時の懸念事項としてセキュリティを挙げる。提示資料によると、その割合は 97%にも達している。では、IoT セキュリティを難しくしている要因は何か。平井氏は、「そもそもデバイスの信頼性や改ざんリスクからゲートウェイの安全性やデータアップロード後の管理まで、脅威は幅広く存在する」といい、「この解決には End-to-End でセキュリティを考えることが必須である」と断じる**（図 1）**。

加えて、製造業 IoT ではもう一つ考えねばならない階層があると指摘する。OT というレイヤーだ。

周知のように、IT と OT のセキュリティは異なる。安全性と可用性、固有のプロトコルやデバイス、サポート切れの古い OS への対応といった OT に特有のセキュリティが求められる。つまり、製造業の場合、IT と OT 双方のリスクがビジネスリスクに直結するため、IT に加えて OT や ICS（産業用制御システム）なども含めた IIoT（インダストリアル IoT）の視点から、統合的にセキュリ

図 1：IoT セキュリティはどこか 1 つのポイントを保護すればよいのではなく、デバイスからクラウドまで End-to-End での統合的な対策が求められる。

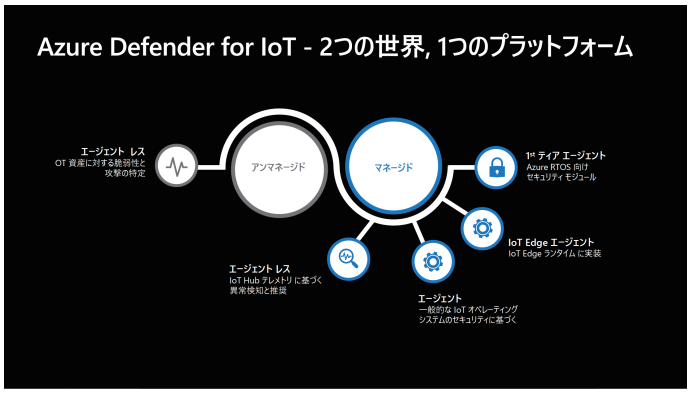

図 2：Azure Defender for IoT は、デバイス（資産）自動検出やセキュリティ・設備の異常検出、攻撃経路予測と対策支援など、さまざまな特長を持つ。

ティを検討することが欠かせない。統合的なアプローチにより、個別にセキュリティ実装を検討する負担から解放されると共に、IoT 活用が生み出すビジネスバリューの最大化に集中できるようになる。そして、こうした統合環境を実現するソリューションとして、マイクロソフトが手掛ける「Azure Defender for IoT」などが紹介された。

Azure Defender for IoT は、元イスラエル国防軍のセキュリティエキスパートにより開発されたもの。IT 資産を対象としたマネージド領域と、OT 資産向けのアンマネージド領域という 2 つの異なる世界を 1 つのプラットフォームでカバーする製品だ**（図 2）**。行動分析アルゴリズムと ICS 固有の脅威インテリジェンスにより、IoT や OT 資産を検出し全トラフィックを管理。包括的なリスク把握と継続的な脅威に対する監視の実現を可能とする。

「IoT セキュリティはビジネスバリューを実現する基盤であり、これを支援するべくマイクロソフトは最高レベルのソリューションを幅広く提供している」と平井氏。「新規インフラだけでなく、既存インフラのセキュリティも担保できることが特長だ」とした。

プログラム②
接続性課題の解決と導入コスト最小化

製造業が IoT 活用を進める上で、大きな妨げとなっている課題の一つが生産設備からいかにデータを収集するかである。この解決策について、たけびし・技術本部・システムソリューション開発部・オリジナル商品開発部の黄波戸信治氏が語った。

同氏が強調したのは、「IoT や AI は企業にとって競争力の源泉であり、ものづくりの現場はその活用に必要なデータの宝庫だ」ということ。確かに、電流・電圧や温度、振動、PLC 経由の実績データや工作機械から得られる加工データ、さらには人の位置や移動、手書きレポートといった具合に生産性現場では膨大なデータが発生している。

せっかくの豊富なデータとはいえ、取得できなければ意味がない。そこで課題となるのが、接続性やシステムの連携性である。データの収集経路はさまざまであり、すべてがセンサーを接続してネットワーク経由で済むわけではない。旧型設備ともなれば、シリアル通信や USB のプログラミングポートを使わざるを得ないケースもある。こうした新旧設備やメーカーの混在、深く根付いた紙文化といった複雑な環境から簡単かつ低コストでデータ収集が可能な解決策が求められる。

これを開発コンセプトに、同社が用意したソリューションが「Device Gateway」や「Dxp SERVER」などである。Device Gateway は IoT ゲートウェイ、Dxp SERVER は Windows 向け通信ドライバだ。

その特長は、「メーカー専用やオープンなプロトコル通信はもちろん、USB 接続や PCI ボードを用いたコントローラーネットワーク、Bluetooth の無線通信やビーコンなどをサポートしていること」と黄波戸氏。「幅広い機器へ一元的に対応でき、従来は収集を断念していたデータを取得できる可能性を持つ」という**（図 3）**。

また、実装作業を不要とするプログラムレスであることも特長であり、設定だけで導入が可能だ。GUI で統一さ

れたユーザーインターフェイスはアイコンやウィザード形式による直感的な操作を実現し、ロジック登録や複数のイベント定義にも対応している。

こうした柔軟な仕組みは大幅な工数の削減につながることから、導入にかかるコストを最小化する。データは、シンプルで軽量なMQTTプロトコルによりAzureなどのクラウドと連携する。収集データはAzureにアップロードされて可視化や分析を実行。あるいはフィードバックにより、ゲートウェイを介して遠隔地からPLCに値を書き込み、生産設備などを制御することも可能だ。

これにより多彩なユースケース**（図4）**が実現されるといい、「BIによるKPI管理・横断管理」や「BACnet通信によるビル設備の監視」、「AI連携による競争力強化」などを例示した。例えば、Azure Machine Learningといったサービスと連携し、学習用のデータ収集やAIへの推論指示、コントローラーへのフィードバックをDevice Gatewayが提供することで、設備や製品に新しい価値を付加できるという。

黄波戸氏は、「データはやみ雲に収集していても活用できない。クラウドやAIの活用により本当に必要なデータが見えてくるので、新たなセンサーの追加や集めるデータの見直しなどが必要。このサイクルを効率的に回していくには、豊富な接続性やプログラミングレスで柔軟に変更できる要件が求められる」と指摘。「分析サイクルは新たな気づきを生み、企業の競争力が高まっていくと確信している」と言葉をつないだ。

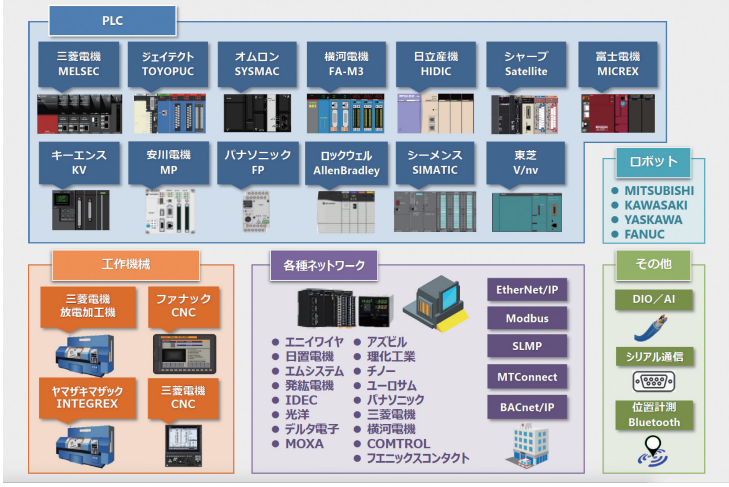

図3：Device GatewayとDxp SERVERがサポートする機器の一部。70ベンダー/200シリーズ以上の制御機器に対応する豊富な接続性を備える。

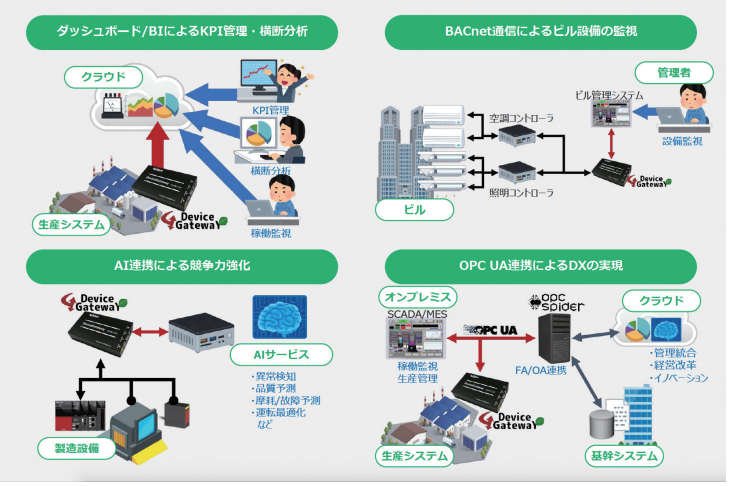

図4：たけびしでは、Device GatewayやDxp SERVERの他にもOPC UA対応ツールなども用意。さまざまなユースケースの実現を可能とする。

プログラム③ 製造業IoT & AIの導入方法と活用事例

セミナーを総括する形で最後に登壇したのは、SBテクノロジー・法人公共事業統括法人第1本部・DXサービス部の杉井雄汰氏。「製造業におけるIoT & AIの導入方法と活用事例」について語った。

同氏がIoTやAI活用の要諦として掲げたのは、「データの収集に始まり、蓄積から可視化、利活用へと進んでいく4つのステップ**（図5）**」。これらを順次、確実にたどっていくことが重要であり、過去の経験からそうした企業には成功事例が多いという。各ステップのポイントについては、以下のように解説している。

データ収集の問題点として、国内製造業における設備の長期使用を挙げた。高品質な製品を安定して供給できる強みだが、IoTや新技術の導入では足かせになっていると指摘。これは、たけびし製品などにより解決できるとした。

蓄積については、IoTで取得したデータは「資源」であるとし、幅広い用途で活用できるため、どのような目的で活用するかを想定することが重要とのこと。

続く、可視化では「誰に見せたいか」を定義することが大事だという。担当者や部署により必要なデータの形は異なるもの。特定部門でしか使えないようでは可視化の意味がなく、役割や立場に応じて必要なデー

タを提供することが求められる。

最後のステップであるデータ利活用については、工場内の機器や設備に対して、IoT から取得した電流値や振動量などを解析することで異常検知を行いラインの停止をできるだけ避ける取り組みが可能になる。また、検査工程を AI 解析によって効率化、生産計画に対して現在の生産数を将来値予測することで、計画と実績値のギャップを早期に把握して対応策を図ることも期待できる。装置周りのインフラについても、データの傾向を読み取ることで、定期的な検査工程の作業効率化や、適切なアラート通知が行え、より迅速化した工場内の運用保守が実現できるようになると解説した。

この 4 つのステップを実現するためには、「常に現場とのコミュニケーションを通じて、望まれている情報は何か、他部署でも活用できるかといったことに意識を向ける

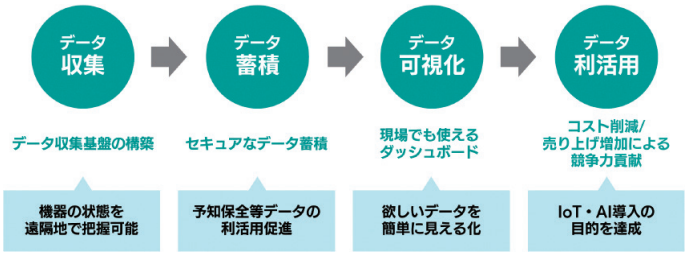

図 5：SB テクノロジーが積み重ねてきた知見に基づいて提示した、「IoT & AI 導入に必要な 4 つのステップ」。製造業にとっても、活用を成功へと導く大きなポイントといえる。

図 6：AI を用いたデータ利活用の代表例である時系列予測と異常検知。それぞれ、SB テクノロジーの「ML Connect Forecast」と「ML Connect Anomaly Detection」により実現される。

ことが必要」と杉井氏。これが「IoT や AI の導入価値の最大化につながる」と話す。

具体例として、SB テクノロジーの IoT プラットフォーム「IoT Core Connect」や AI サービスなどを活用したワンストップソリューションにより、同社が手掛けた事例やデモが多数紹介された。

とりわけ注目を集めたのは、IoT で収集したデータを AI により分析する「時系列予測」と「異常検知」である **(図 6)**。時系列予測は、過去のデータ推移から将来の値を予測して最適な運用・管理やコスト低減を実現するもの。同社の AI サービス「ML Connect Forecast」の活用例として、空調設備の最適運転化を提示。機械学習開発の工数を 10 分の 1 に削減すると共に、予測精度の向上により電力コストを削減した活用例を示した。クラウド AI の活用は、データや AI モデルの集約化を行うことができるため、複数拠点への展開やモデル構築にかかる開発コストを大きく削減することも期待できる。

異常検知は、過去の設備稼働データをもとに各製品の稼働状況を分析して異常検知を行い、不良品発生率やダウンタイムの低下に貢献するもの。同社の異常検知 AI サービス「ML Connect Anomaly Detection」を用いて、注目度の高い CBM（状態基準保全）の活用例をデモとして紹介した。こうした機器の状態に合わせたメンテンスを実現（TBM から CBM）することで、熟練工の経験と勘に頼らず判断基準の属人化回避や、メンテンス中に発生する機器の停止時間、部品交換にかかるコストなどを極小化することが期待できる。

杉井氏は、「製造業が最新技術を活用していくとなると、社内ハードルが高く技術的知見も必要とするなど、難しいという話を聞く」といい、その解決には「ベンダーと共にビジョンを描きながら取り組むことが大事。気軽に相談してほしい」と語り、セミナーを締めくくった。

株式会社たけびし

〒615-8501　京都府京都市右京区西京極豆田町29
お問い合わせ　TEL. 075-325-2261　FAX 075-325-2273　E-mail. fa-support@takebishi.co.jp
https://www.faweb.net/