産業用コネクティビティとネットワーキングガイドブック101 初級編

理想的な産業用コネクティビティとネットワーキングソリューションを選定する頼れるエキスパートになれるヒントの提供

産業用Internet of Things (IIoT)または製造業におけるオートメーション化、データ化、コンピュータ化を目指す技術的コンセプトIndustry 4.0は、互いに独立して開発された技術のOT (Operational Technology) とIT (Information Technology) ネットワークとのコンバージェンス (収束) が急速に加速し、産業用コネクティビティとネットワーキングの新しい形の方向に進んでいます。これは、OTとITシステムの両方が産業用フィールドデバイスと接続する必要が生じため必要不可欠となりました。このように産業オートメーションがデジタル変革する中でIAエンジニア、ITエンジニア、OTまたはITシステムインテグレータ、プラントオーナー、システムオペレータのいずれであっても、このガイドブックが、IIoTプロジェクトに適した産業用コネクティビティまたはネットワーキングソリューションを選択することで、OTとITのギャップを埋めるヒントになれることを願っています。

Table of Content

産業用コネクティビティのニーズ – 現在と将来への対応

産業用ネットワーキングのニーズ – 現在と将来への対応

はじめに

ファクトリ現場の機器やデバイスを直接デジタルコントロールできるようになった初期の頃から産業オートメーション（IA）の状況は、大きく変化しています。従来、産業用コネクティビティを可能にするために使用されるOperational Technology（OT）の世界は、製造環境での物理的プロセスとマシナリー管理にのみに使われてきました。対照的にInformation Technology（IT）は、オフィスネットワーク上のデジタル情報の流れの管理にのみ使われてきました。

OTとITは、最初、互いに別々に開発されていましたがOTとITシステムの両方が産業用フィールドデバイスと接続する必要が生じため、広く受け入れられている“自動化の柱（pillar）”にこれら2つのテクノロジーが収束されてきました。コネクテッドワールドで競争力を維持するために以前、接続されていなかったOT資産は、産業用コネクティビティを必要とするだけでなく、産業の生産性、効率、およびスケーラビリティを改善するビジネスインテリジェンスを効果的に引き出すために企業などが情報システムのハードウェアを自社で保有し、自社の設備において運用する“オンプレミス”アプリケーションを超えるITまたはクラウド機能が要求されています。

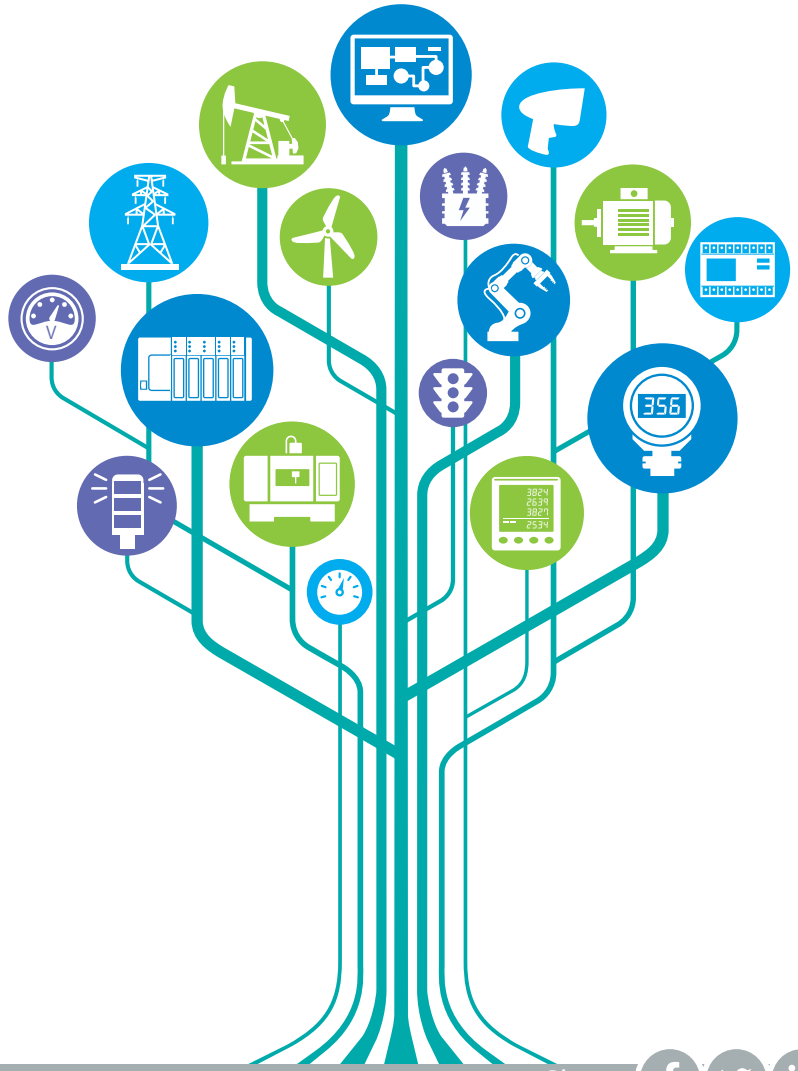
現在、産業用Internet of Things（IIoT）またはIndustry 4.0と呼ばれるOTとITネットワーク間のさらなるコンバージェンス（収束）に向けた傾向は、新しい形の産業用コネクティビティとネットワーキングへと進行しています。残念ながら、この統合されたランドスケープで適切な産業用コネクティビティとネットワーキングソリューションを選択する骨の折れるタスクは、OTプロトコルと自動化システムの経験に乏しいITエンジニアとエンタープライズITネットワーキングに精通していないOTエンジニアが頻繁に悩まされています。

Moxaは、産業用コネクティビティとネットワーキングの課題を克服するために支援を続けて30年以上の経験に基づき、産業用オートメーションアプリケーションに最も適したソリューションを選択するためのいくつかの重要な基準を特定しました。IAまたはITエンジニア、OTまたはITシステムインテグレータ、プラントオーナー、システムオペレータのいずれであってもIIoTプロジェクトに適切な産業用コネクティビティまたはネットワーキングソリューションを選択して、OTとIT間のギャップを埋めるために、このガイドブックがお役に立てば幸いです。

産業用コネクティビティのニーズ — 現在および将来への対応

IIoTアプリケーションを実現する最初のステップは、これまで接続されていなかった産業用フィールドデバイスと資産を接続することから始まります。このタスクを実行するには、接続する必要があるOT資産の種類と、OT資産をローカルネットワークまたはクラウドサーバに接続するなどの特定のコネクティビティ要件を理解する必要があります。産業用アプリケーションのOT資産は、主にシリアルまたはI/O通信インターフェースを使用しているため産業用コネクティビティを実現するには、適切なシリアルおよびI/Oコネクティビティソリューションの選定方法を理解することが不可欠です。さらに、OT資産をリモートサーバまたはクラウドサーバに接続するときに注意する必要がある追加の考慮事項があります。

このチャプタでは、シリアルコネクティビティ、リモートI/Oコネクティビティ、およびIIoTデバイスコネクティビティのソリューションを選択する方法を学びます。



シリアルコネクティビティ

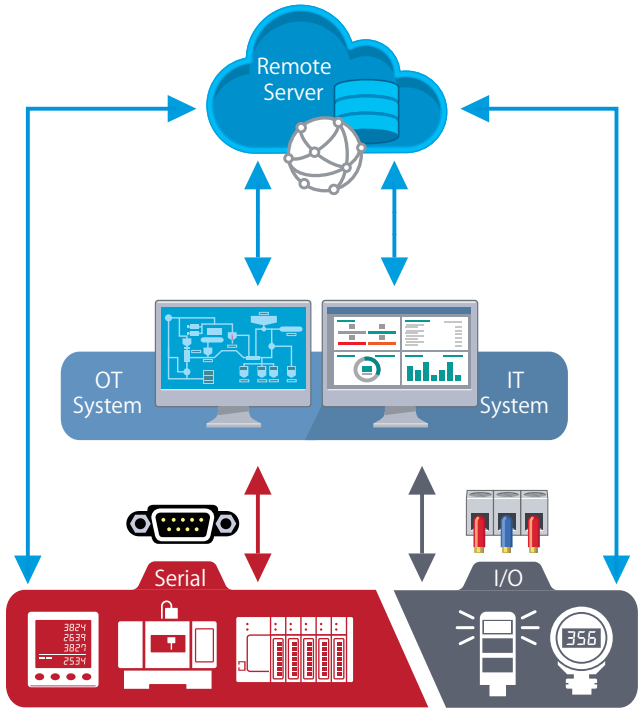
レガシーのマシン、機器、およびフィールドデバイスの大半は、様々な規格および独自のシリアル通信プロトコルを使用しているためレガシーシのリアルデバイスを標準のイーサネットコネクションを備えたシステムと通信するためには、シリアルデバイスサーバまたはプロトコルゲートウェイが必要となります。

リモートI/Oコネクティビティ

リモートI/Oコネクティビティの目的は、デジタルまたはアナログデータの収集と伝送に限定されません。OTシステムとITシステムの両方がI/Oデバイスからデータを収集する必要があるIIoTアプリケーションでは、リモートI/Oがアプリケーションシステムでデータを利用できるようにする上で重要な役割を果たします。

IIoTデバイスコネクティビティ

IIoTアプリケーションでフィールドデバイスを接続するために使用するコネクティビティデバイスは、独自の要件があります。例えば、コネクティビティデバイスは、ITシステムまたはクラウドサーバと通信するためにITプロトコルまたはクラウド機能を必要とします。すべてが接続されている場合、多くのコネクティビティデバイスの管理と安全なデータの伝送に関する問題にも対処する必要があります。



OT資産

実際、デバイスコネクティビティが実現されても、実績のあるレガシーデバイスおよびマシナリーを撤去する必要があるという意味ではありません。これまでのアンコネクテッドレガシーデバイスをインターネットに接続および異なるプロトコルおよびフォーマットからデータの収集およびトランフォーミングするための様々なソリューションを利用できます。IIoTアプリケーションが現在および予測可能な将来に向けて確実に成功するためにシリアルコネクティビティ、リモートI/Oコネクティビティ、およびIIoTデバイスコネクティビティソリューションを選択するための特定の要件についてのディスカッションを始めます。

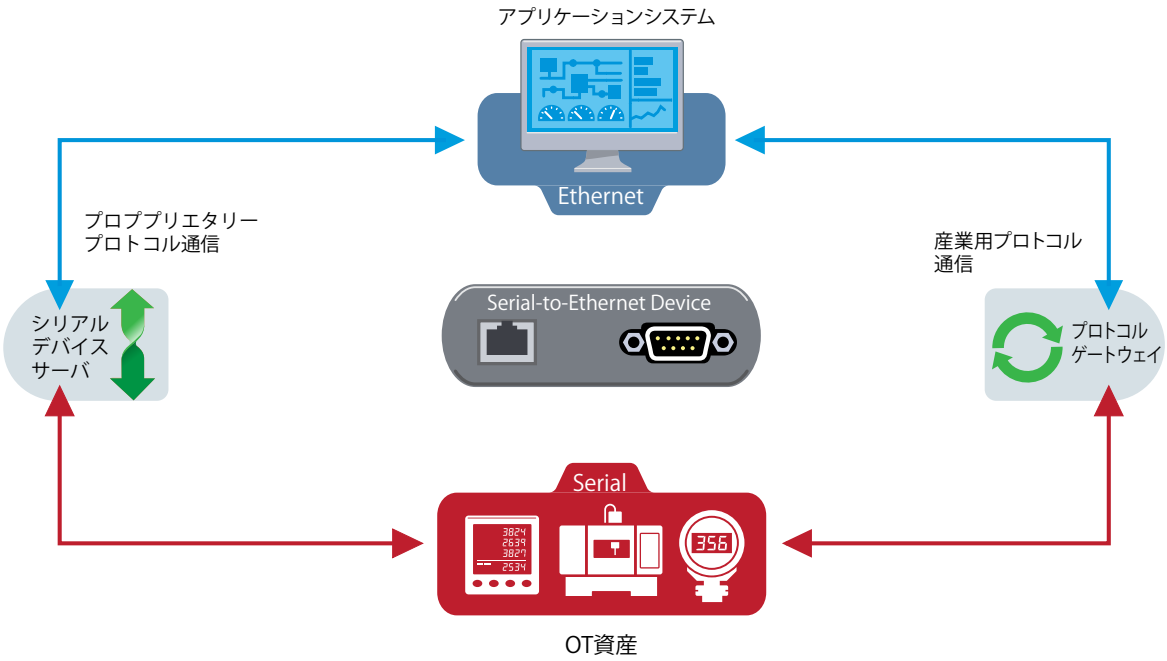
レガシーシリアルデバイスに新しい命を吹き込む

既存の産業オートメーションシステムを最新のIIoTアプリケーションに移行するために、今まで世話になったレガシーデバイスに別れを告げる必要はありません。産業用エッジシステムのレガシーデバイスは、現在使用されている多くのスマートフォン、ガラパゴスの携帯やNotePCに比べて古い歴史がありますが、時代の変化に見合った価値の高い目的を果たすために、この際、使用を諦めスクラップやリプレースしてしまいますか?しかし新たにシステムを導入するとなるとコストがかかりすぎます。

しかしながら、IIoTアプリケーションは、多くの場合、インターネットプロトコル（IP）を使用してイーサネットネットワーク経由で通信するSCADAシステムを利用します。一方、レガシーデバイスは、IP通信とは大きく異なるfieldbusプロトコルを使用したシリアルベースの通信を使用します。このような中で、例えばレガシーシリアルデバイスをイーサネットベースのSCADAシステムと接続しようとしても、当然互いに通信ができません。さて、どのような解決策があるのでしょうか？

すべてのレガシーシリアルデバイスを新しいイーサネットベースのデバイスにリプレースすると通信の問題は、明らかに解決します。しかし、すべての機器をアップグレードするとなると多大なコストがかかり、混乱を招きます。例えば、シリアルベースのCNCマシンをリプレースするには膨大な費用が発生し、多くの企業の予算を圧迫します。一方、シリアルデバイスには独自の利点があります。例えば、RS-485インターフェースの電力計は、マルチドロップ通信を実行できるため配線が簡単で効率的です。シリアルデバイスとIPベースのシステムの間にSerial-to-Ethernetソリューションを追加するとコストと作業が削減でき、シリアル通信のシンプルさとイーサネットの利点の両方を享受することができます。

スタートする前にシリアルデバイスを調べ、これらの古い友達と再会する必要があります。レガシーデバイスは、独自（プロププリエタリー）のプロトコルまたはModbusやPROFIBUSなどの標準Fieldbusプロトコルで通信するためIP通信を可能にする適切なシリアルデバイスサーバまたはプロトコルゲートウェイを選定する必要があります。

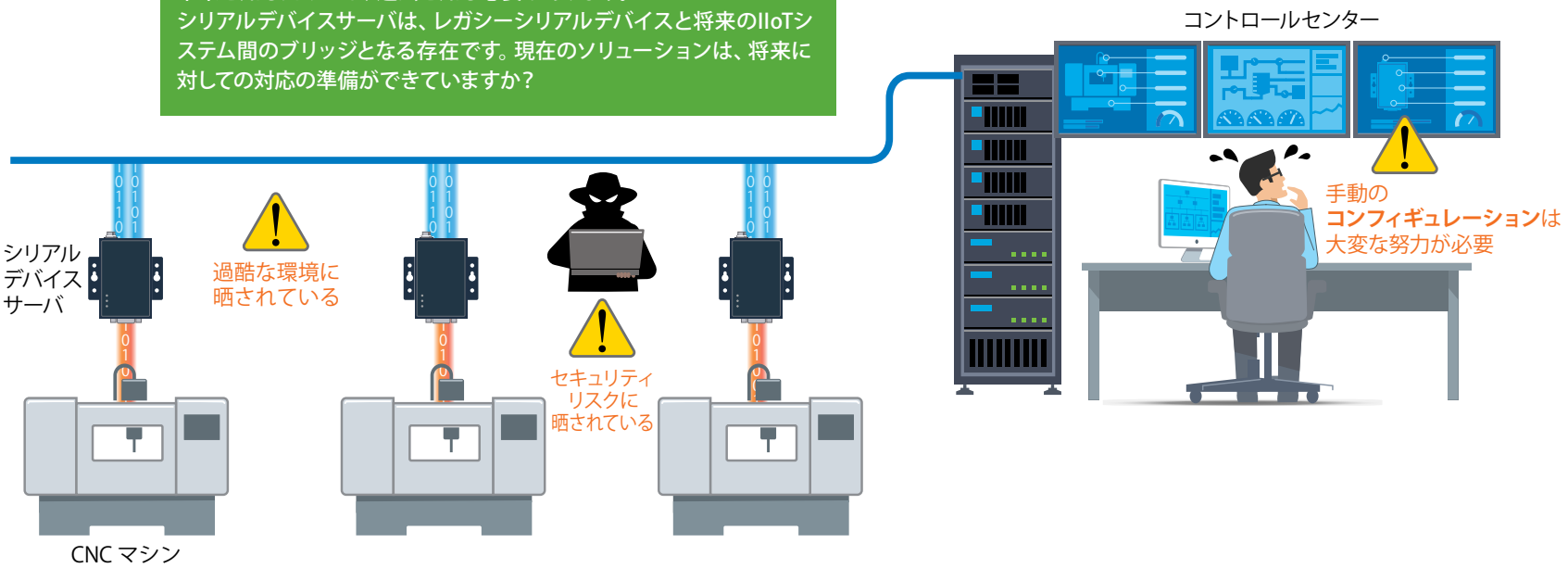


シリアルデバイスサーバを選定するための重要な基準

独自（プロプリエタリー）のプロトコルを使用するシリアルデバイスをIPネットワーク経由で接続する必要がある場合、シリアルデバイスサーバは、レガシーシリアルデバイスと最新の通信システムとの間のシンプルなブリッジを提供します。しかしながら、シリアルデバイスサーバの動作に関する十分な知識がないと、無駄な時間と労力を費やします。 シリアルデバイスサーバを選択するときに必要な3つの重要な基準を次に示します。

Key Question

未来を知るためには、過去を知る必要があります。
シリアルデバイスサーバは、レガシーシリアルデバイスと将来のIIoTシステム間のブリッジとなる存在です。現在のソリューションは、将来に対しての対応の準備ができていますか？



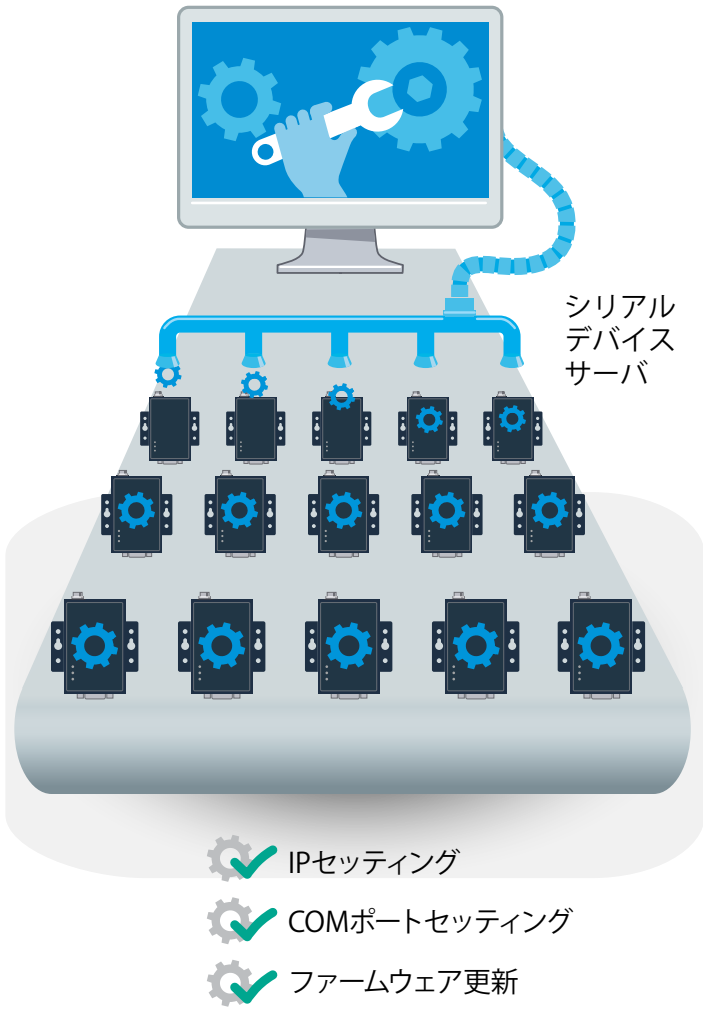
主要な基準 1

すべてのステップを考慮に入れる

すべての稼働中のレガシーデバイスを完全にリプレースすることと比較して、シリアルデバイスサーバの使用方法と導入方法を学習することは、さほど難しいことではありません。しかしながら、数10のシリアルデバイスサーバを機能させるには、多くの設定を手動で実行する必要があるため多大な時間と労力を費やします。シリアルデバイスサーバごとにIPアドレスを構成する場合でも、仮想シリアル（COM）ポートをセットアップする場合でも、またはシリアルおよびイーサネットパラメータを更新する場合でも、すべての手順に従って実行するための明確な指示やスマートユーティリティがないとシリアルデバイスサーバのコンフィギュレーションは容易ではありません。そのため数10のデバイスの管理またはメンテナンスを必要とする場合、多大な時間と労力を費やすことでフラストレーションが増大します。

シリアルデバイスサーバを選定するとき、コンフィギュレーションとマネージメントを簡素化できる使いやすいWebコンソールまたはユーティリティがあるかどうかを確認する必要があります。これは、ネットワークが成熟するにつれて接続する必要があるフィールドデバイスが増えるため、この機能を見過ごすことがないようにします。コンフィギュレーションプロセスを繰り返すとデバイスマネージメントの負担がますます増大します。

Serial-to-Ethernetテクノロジーを更に
学びたいですか？　詳細については、
Serial-to-Ethernetに関するQ&Aをご覧ください。
https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0447.html

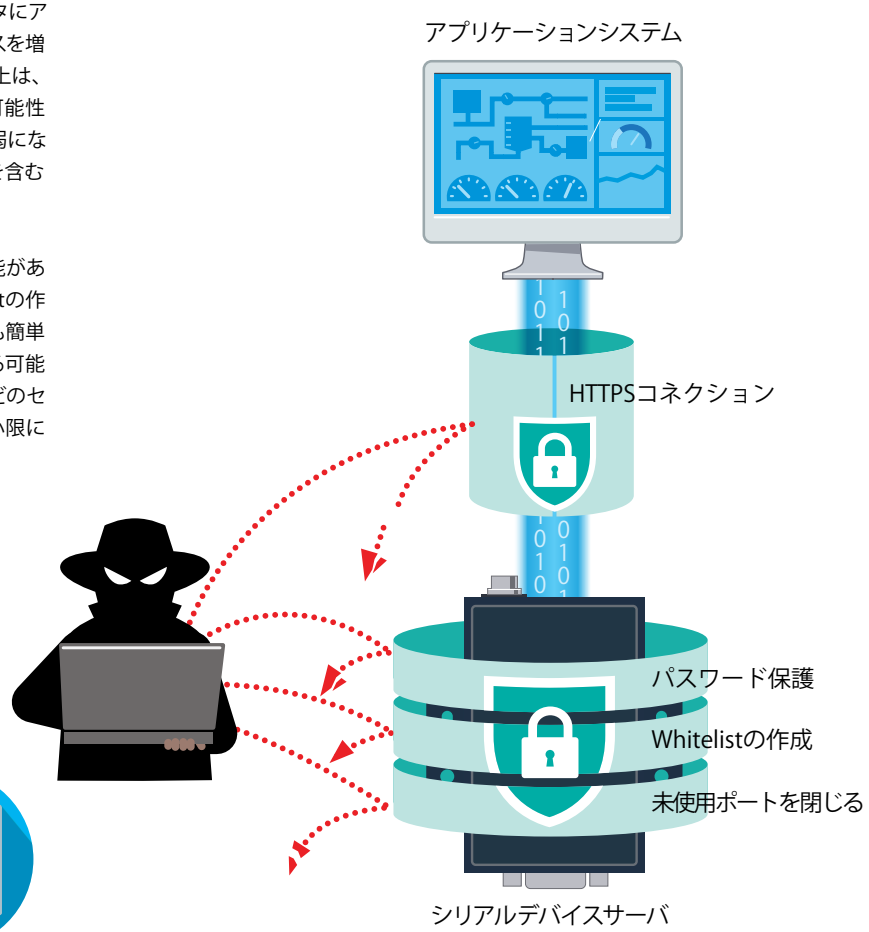


主要な基準 2

ネットワーク社会でのセキュリティ保護

これまで産業オートメーションは、小規模の独立したプライベートネットワーク内で、限られた数のフィールドデバイスを接続するだけで済みました。しかしながらIIoTの時代において産業用アプリケーションは、OTおよびITの両方のエンジニアがフィールドデータにアクセスすることができるパブリックネットワークを介して接続するフィールドデバイスを増やす必要に迫られています。外部世界のフィールドデバイスのアクセシビリティの向上は、多くの利点が得られる一方、ネットワークが新しいセキュリティリスクに晒される可能性が増大します。このため適切な保護を施さなければアプリケーションは、非常に脆弱になります。ネットワークが保護されているのであれば人々は、シリアルデバイスサーバを含む無数のエントリポイントを通じて安心してアプリケーションにアクセスできます。

選定するシリアルデバイスサーバがデータを保護するために十分なセキュリティ機能があることを確認する必要があります。強力なログインパスワードの使用またはwhitelistの作成は、シリアルデバイスサーバへのアクセスを許可された担当者だけに制限する最も簡単な方法です。シリアルデバイスサーバの未使用のポートを閉じることも、悪用される可能性のある不要な入り口をブロックする効率的な方法です。データ伝送中にHTTPSなどのセキュアなプロトコルを使用することは、フィールドデータへの不要なアクセスを最小限に抑えることができます。



コネクティビティをセキュアに保つ方法の詳細を知りたいですか？ そうであれば**デバイスセキュリティ**の記事を今すぐお読みください。

https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0712.html

主要な基準 3

“IIoT”の最初の“I”の重要性

現在、産業用アプリケーションで商用グレードのシリアルデバイスサーバを使用していませんか？商用グレードのシリアルデバイスサーバは、短期間の使用や、いくつかのフィールドデバイスを接続するだけの目的の場合には十分対応することができます。しかし、産業システムにおいて、多くのフィールドデバイスを接続し、重要なフィールドデータをオンタイムに転送する必要があるIIoTプロジェクトに関しては、再考する必要があります。商用グレードのデバイスサーバでは対応できない、極端な温度や激しい電磁干渉のある過酷な環境に耐えることができる耐久性のある産業グレードのシリアルデバイスサーバを選定することで、シリアルデバイスサーバのシャットダウンに起因するデータ損失を最小限に抑えることができます。

前述した3つの基準を使用してシリアルデバイスサーバを評価すると、産業用アプリケーションに適したソリューションを見つけることができます。その中でMoxaのNPortシリアルデバイスサーバ(https://www.ibsjapan.co.jp/products/moxa/5720/5910/)は、IIoTアプリケーションでフィールドデバイスを接続するために理想的かつ使いやすく、セキュアで信頼できる機能を備えて開発されています。

“信頼性に優れたデータ伝送を実現するためにIIoTコネクティビティをシンプルかつセキュアに保つことができる産業用シリアルデバイスサーバを使用することが大切です”

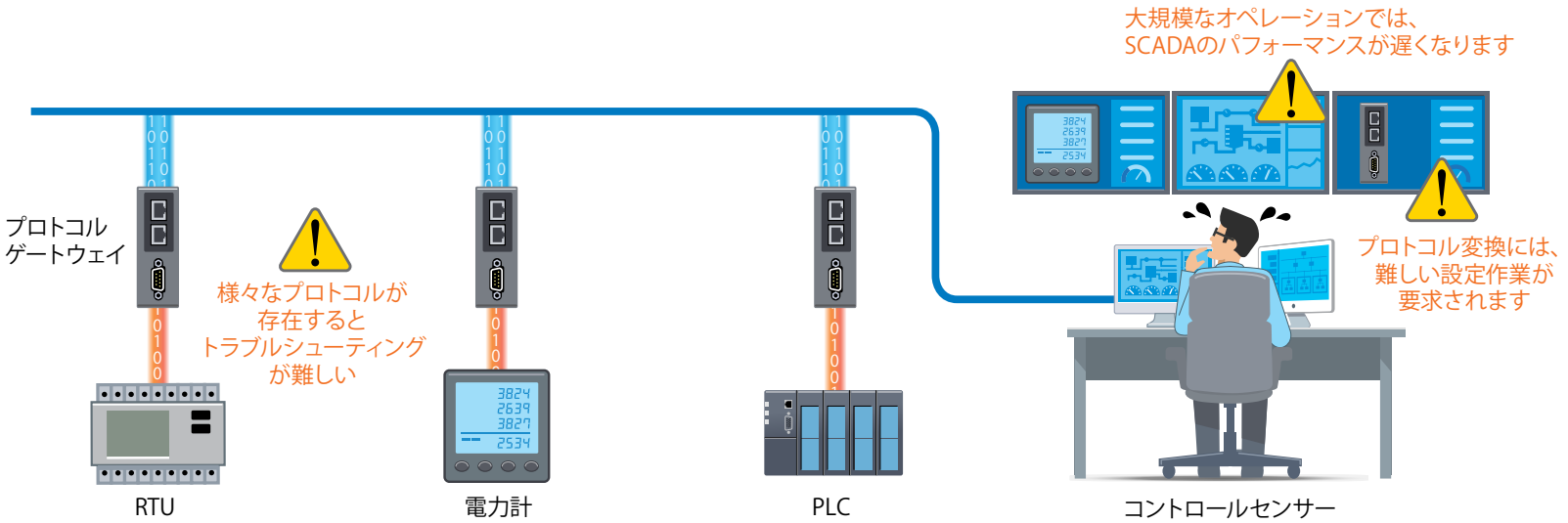
プロトコルゲートウェイを選定するための主な基準

以前のオートメーションシステムは、ITと異なりクローズされた世界で運用されるため**Modbus、EtherNet/IP、PROFINET**などの高度に専門化された独自のプロトコルセットが開発されました。これらのプロトコルは、産業用Fieldbusプロトコルとして知られ、異なるシステムアプリケーションの目的のためにユニークでありベネフィットがあります。今日、コネクテッドファクトリーへの移行により2つの主要な理由のためにプロトコル変換の需要が高まっています。　まず、レガシーデバイスでは、一般にシリアルベースの通信プロトコルを使用します、一方、産業用オートメーションにおいて最新のSCADAシステムは、イーサネット通信に依存しています。レガシーのシリアルデバイスとSCADAシステム間のスムーズなデータ通信を可能にするには、**Serial-to-Ethernetプロトコル変換**が必要です。次に、ファクトリには、いくつかの独立したコントロールシステムがあります。システム間の通信を可能にし、運用効率と可視性を向上させるには、システム間でデータを変換する方法が必要です。

プロトコルゲートウェイは、統合通信システムにおけるデータ通信をスムーズに実行する上で重要な役割を果たします。次の3つの基準は、プロトコルゲートウェイを選定するために必要なガイドラインです。

Key Question

レガシーデバイスと最新システム間のスムーズなデータ通信を実行するためには、プロトコル変換に依存します。そこで、すべての複雑な設定を管理し、データ通信を高速かつシンプルに保つためにプロトコルゲートウェイがあると便利でしょうね？



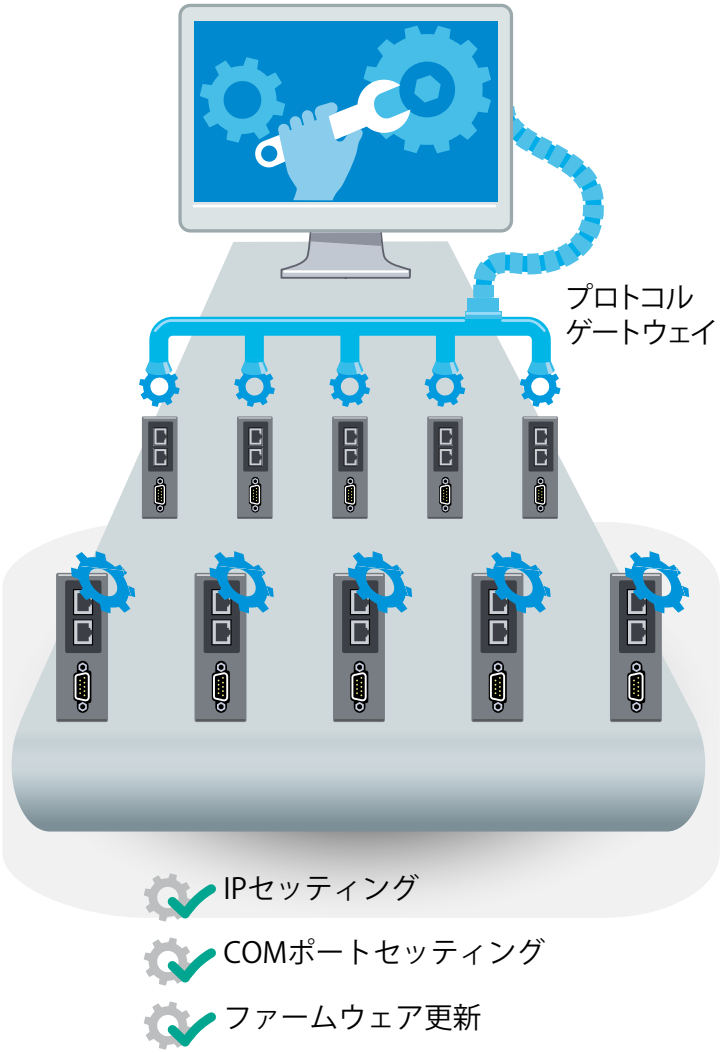
主要な基準 1

迅速なコンフィギュレーションによる力強い始まり

シリアルデバイスサーバのIPアドレスとCOMポート設定を手動で構成することが苦痛に感じた場合、産業用プロトコル変換設定が対処するまでお待ちください。産業用プロトコルの変換設定は、異なるデータフォーマットが関係しているため非常に複雑です。例え、経験が豊富なエンジニアでさえ苦労するかもしれません。優れたプロトコルゲートウェイは、異なるプロトコルを変換するだけではありません。プロトコルゲートウェイは、ノースバウンドおよびサウスバウンドの両方のプロトコルのビザンチンコンフィギュレーション（byzantine configuration）を簡素化するだけでなく、どのプロトコルの、どのデータを変換する必要があるかを適切にマッピングします。
これらの機能を直感的で使いやすい画面を提供するグラフィカルユーザインターフェースによりコンフィギュレーションプロセスのスピードアップを図ることができます。

百聞は一見に如かず。この ビデオにより プロトコル変換がいかに簡単であるかが、ご覧になれます(英語版)

https://www.youtube.com/watch?v=o_z8SHiS2Cw&feature=youtu.be&utm_source=ebook&utm_medium=organic&utm_campaign=202006-smb-cm-video

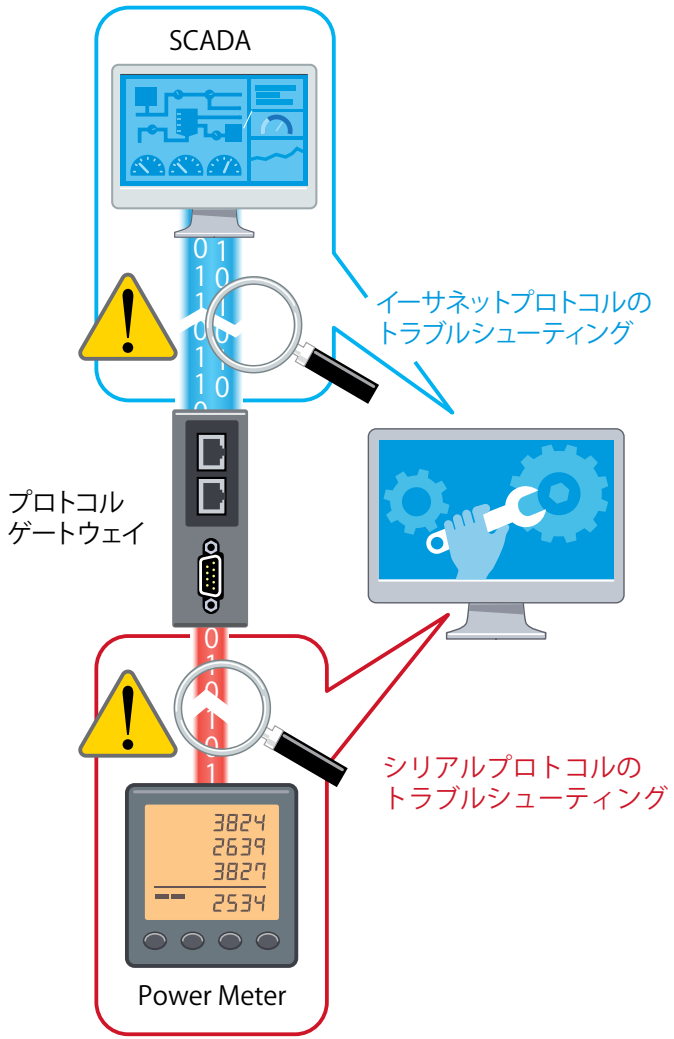


主要な基準 2

トラブルシューティングのトラブルを取り除く

システムがダウンすると時間と生産性が失われるだけでなく重要な利益まで失います。当然ながらエンジニアは、問題を迅速に処理したいと考えます。しかしながら、トラブルシューティングは必ずしも簡単ではありません。異なるプロトコルを使用する複数のデバイスが接続されている場合では、問題がイーサネット側で発生したのかシリアル側で発生したのかを判断する必要がありまた、通信問題の原因を特定することは、さらに難しくします。時間とエネルギーを使い、通信障害の根本原因を突き止めようとしても失敗することがよくあります。フラストレーションが増加するのは、根本的な原因をすばやく特定するための有用な診断ツールがないことです。

プロトコル変換の問題にかかわるトラブルシューティングには、ゲートウェイを通過するパケットを解析する方法が必要です。しかしながら、トラブルシューティングツールと機能は、セキュリティ上の問題（例えば、サードパーティのユーティリティがITポリシーで許可されない）やプラットフォームの制約（例えば、ユーティリティツールをPLCに直接インストールできない）のために制限される場合があります。従って、**便利なユーティリティツールまたは組み込みのトラブルシューティング機能**を備えたプロトコルゲートウェイがコネクションのステータス、タイムアウト頻度、無効な応答カウントを素早く特定することができます。ゲートウェイソリューションを選定する際には、トラブルシューティングに費やす費用と労力を忘れないことが必要です。



プロトコル変換問題のトラブルシューティングの詳細については、White Paperをご覧ください。
https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0590.html

White Paper

主要な基準 3

データ収集のパフォーマンス問題

大規模なアプリケーションでプロトコル変換が必要な場合、コストとパフォーマンスのバランスをとることが主要な問題となります。数十または数百のデバイスがプロトコル変換を必要とする中でシングルのSCADAシステム内で通信する場合、システムパフォーマンスが期待どおりであることをどのように確認できますか？ フィールドデバイスごとに1ポートのプロトコルゲートウェイを使用してデータの変換と伝送を瞬時に行うことができますが、当然、規模が大きくなると共にコストの膨大とメンテナンスの労力が日常のオペレーションを圧倒する可能性が生じます。一方、高ポート密度のプロトコルゲートウェイは、効率的なインストレーションおよび容易なマネージメントを備えた費用対効果の優れたソリューションを提供できますが、パフォーマンスの問題がデータ処理を通して発生する可能性があります。多くのプロトコル通信は、ポーリングと応答の動作に基づいているため大量データのポーリングを処理するとゲートウェイに負荷がかかりSCADAシステムのパフォーマンスと応答時間に悪影響を及ぼします。

そこで1ポートと高ポート密度のプロトコルゲートウェイを組み合わせてネットワークを慎重に設計します。高ポート密度のプロトコルゲートウェイを選定する場合は、そのデータポーリングメカニズムが要件を満たしているかどうかを確認する必要があります。

使いやすいプロトコルゲートウェイは、システムのオペレーションを大幅に改善できます。上述の3つの主要な基準を確認し、適切なソリューションを選定します。例えば、**Moxa MGateプロトコルゲートウェイ**(https://www.ibsjapan.co.jp/tech/details/modbus-protocol-gateway/index.html)は、効率的なプロトコル変換を可能にし、スムーズなデータ通信によりシステムオペレーションを高速化することができます。

SCADAのパフォーマンスを最適化する方法については、White Paperをご覧ください。
https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0505.html

White Paper

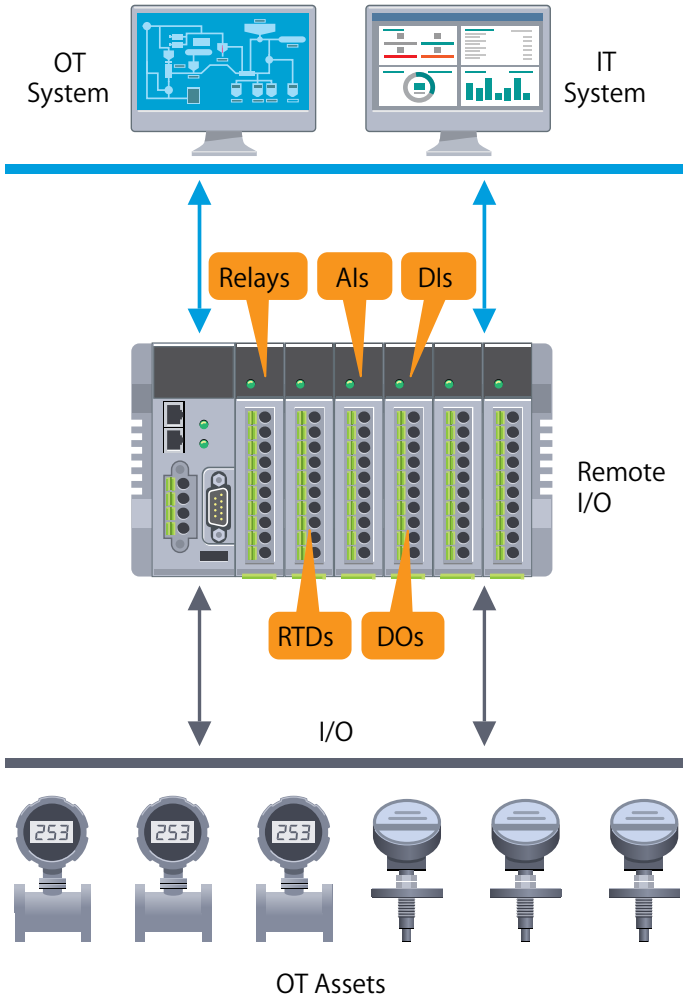
“プロトコルゲートウェイは、
オペレーションのいかなる場合でも、
いかなるサイズのアプリケーションの
プロトコル変換でも簡素化できる
必要があります”

リモートI/Oに対する大きな期待

データがなければ、産業用Internet of Things (IIoT)アプリケーションに対して実用的な洞察を引き出すことはできません。フィールドのセンサ、コントローラ、およびその他の機器間の入出力信号の送受信を司るリモートI/Oデバイスは、IIoTに直ちに関連付けられる"スマート"な自動化ロボットに似ていないかもしれませんが、これらのI/Oのワークホースがなければ 必要とするリモートI/Oデータは一切ありません。

リモートI/Oデバイスは、通常、遠隔地にあるコントロールセンタからのデータアクセスと環境監視を可能にするためにフィールドサイトに導入されます。I/Oデータの収集は、フィールドアプリケーションのスムーズな日常のオペレーションを保証するだけでなく生産性を最適化するために使用できる潜在的な洞察も提供します。

しかし、IIoTシステムおよびアプリケーションの複雑さが増すにつれて従来のデータ収集は、限界に達しています。モジュラーリモートI/Oデバイスは、リモートI/Oデバイス自体のI/Oモジュールをカスタマイズできるため明確な利点があります。別な言い方をすれば、使用したい特定のタイプのI/Oモジュール、柔軟な拡張を提供するモジュールの使用、および通信手段の選択に基づいたモジュールの使用など自由に選択ができます。モジュラーI/Oデバイスは、今日の市場における最新のソリューションではないかも知りませんが、それらを可能にする柔軟性により、すべてのノードからリモートデータを収集する方法に対する期待を高めています。

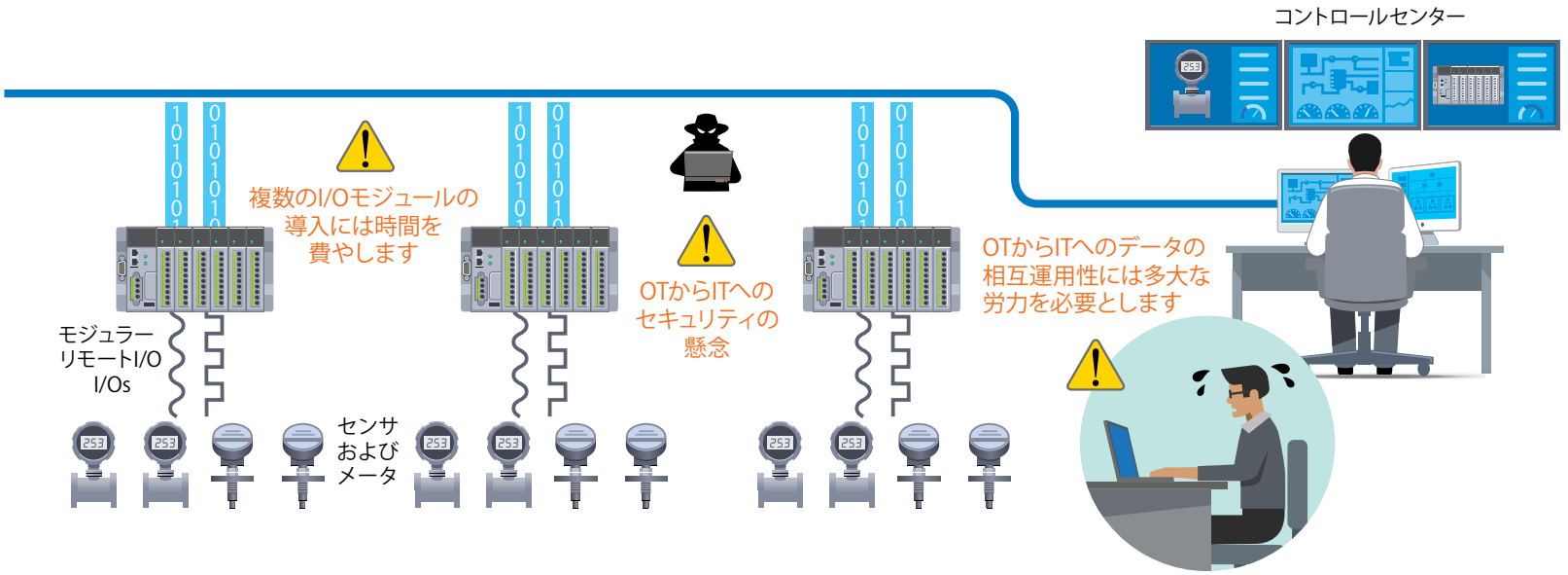


モジュラーリモートI/Oを選定するための主な基準

インストールからオペレーションおよびメンテナンスに至るまで収集したデータを最大限に活用することができるモジュラーリモートI/Oソリューションを選択することが重要です。同時に、OTシステムおよびITシステムの両方が収集したデータを使用できることを確認する必要があります。最後に重要なこととしてリモートI/Oソリューションには、慎重に収集したデータを保護するためのサイバーセキュリティ機能を含める必要があります。このセクションでは、これらの重要な考慮事項について詳しく説明します。

Key Question

I/Oデータを最大限に活用するには、リモートI/Oデバイスの役割を再考する必要があります。現在使用中のリモートI/Oソリューションは、IIoT時代の変化するコネクティビティ要件に対応することができますか？



主要な基準 1

ユーザビリティを犠牲にしない

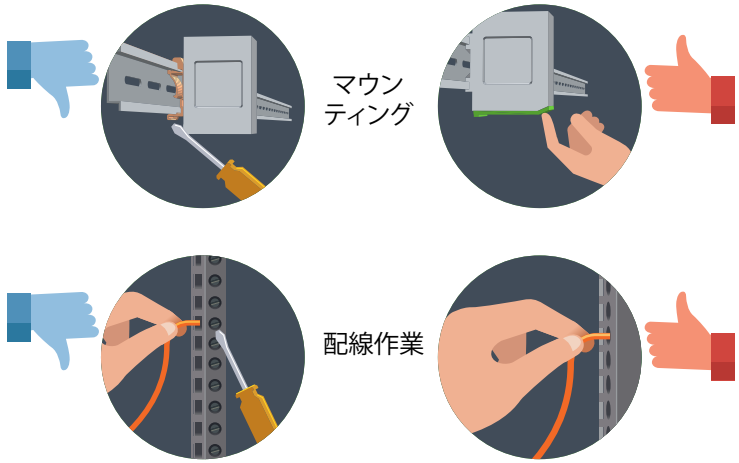
モジュラーリモートI/Oデバイスがもたらす柔軟性は、デバイスがどのようにフィールドアプリケーションに実装され、実際に使用されるかに注意を払わないと隠れたコストと追加の労力が伴う場合があります。柔軟性を高めるためにユーザビリティを犠牲にすることは、絶対に避けなければなりません。そうしないと、そもそもモジュール固有のメリットが打ち消され追加の労力が費やされることになります。ユーザビリティの落とし穴が発生する可能性があるのは、基本的に2つの段階に関係します。

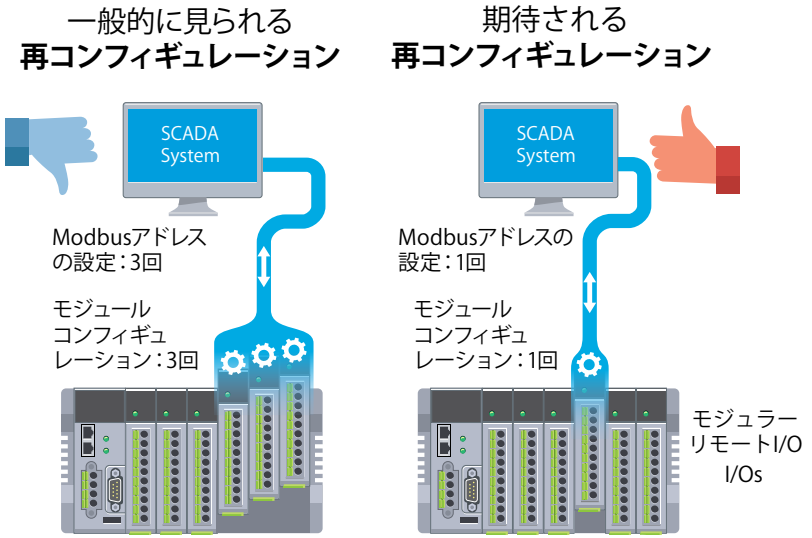
初期のインストレーション

モジュラーI/Oソリューションは、大量の異なるデータ収集ニーズを目的としたIIoTアプリケーションに最適です。従って、アプリケーションでモジュラーI/Oデバイスを必要とする場合は、間違いなく多くのI/Oモジュールが必要となります。絶えず注意を必要とする部品の移動や取り付けが多いことで稼働させるまでの時間を無駄にしたくありません。ユーザフレンドリーなインストレーション機能には、便利で標準化されたマウンティングオプション、および最適化された配線設計が含まれます。

オペレーションとメンテナンス

モジュラーI/Oデバイスは、データ収集アプリケーション規模の調整や拡張に便利に対応することができます。しかし、大規模システムでは、追加するI/Oモジュールをすべて構成するには、かなりの時間がかかります。システム内でシングルモジュールを変更する場合でも、変更しないモジュールもシーケンスの変更のためモジュールを再構成する必要の可能性があります。モジュールに加えて、無数のSCADAシステム設定がすべて最新であり、すべてのモジュール変更に対応していることを確認する必要もあります。　実際、ユーザフレンドリーなモジュラーI/Oソリューションは、不必要な労力を削減できるので見落としてはいけません。

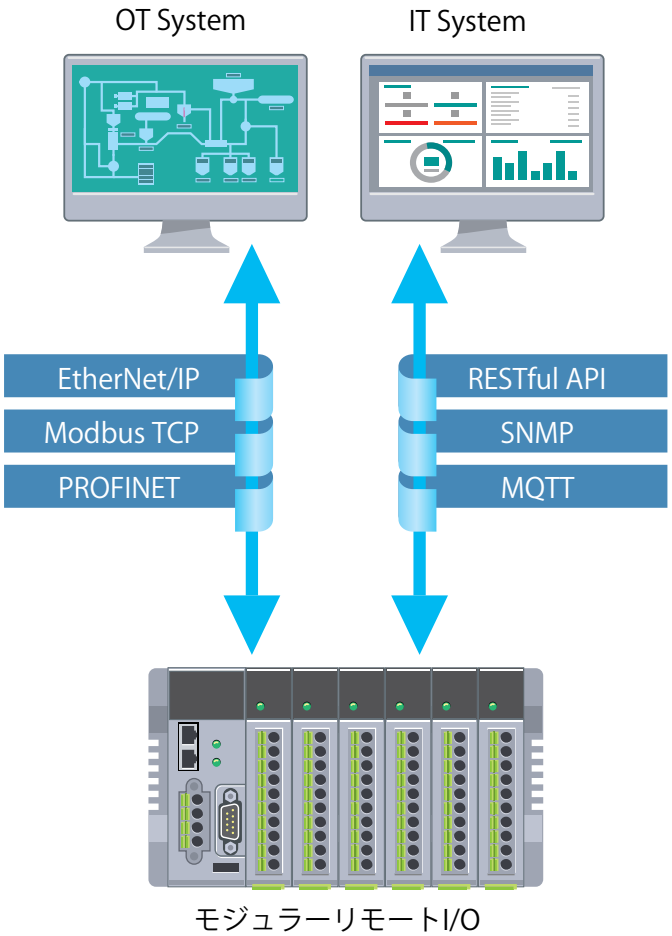




主要な基準 2

“I-Io-T”の中の“I/O”を選択する

前述したように、今日のIIoTアプリケーションにおけるITシステムとOTシステムの統合により、モジュラーI/Oソリューションを含む新しく拡張されたエッジデバイスの開発が促進されました。それにもかかわらず、OTおよびITシステムは、依然として本質的に異なる通信プロトコルに依存しています。ITとOTの両方に1つのサイズですべてに対応するリモートI/Oソリューションは必要ありませんが、IIoTアプリケーションのすべての部分を確実に適合させて連携させることが重要です。例えば、MQTT、SNMPv3、RESTful APIなどの新たに出現したITプロトコルを使用するとOTアプリケーションは、従来のITベースの解析ツールやサービスを活用できます。IIoTの時代には、IT/OTの準備が整っている将来を見据えたモジュラーリモートI/Oを選択することが不可欠です。



モジュラーリモートI/O

MQTTプロトコルを活用することができる方法の詳細は、White Paperをご覧ください。

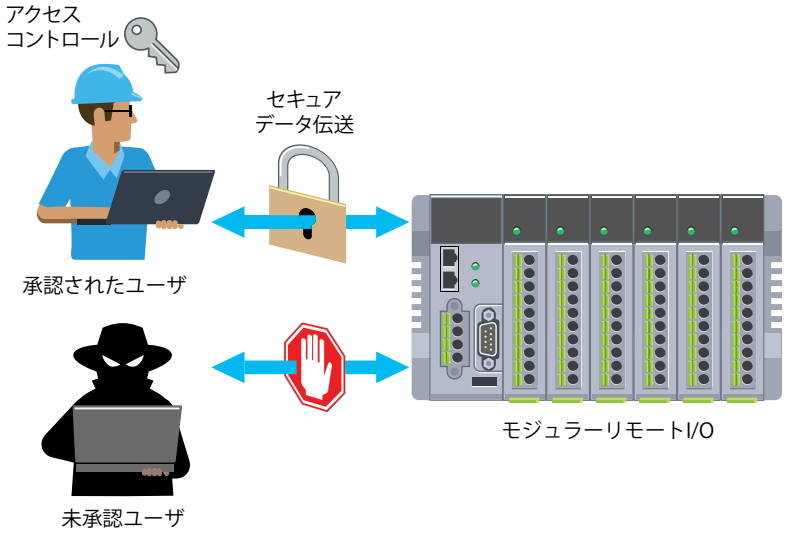
https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0681.html

White Paper

主要な基準 3

セキュリティを忘れてはなりません

IIoTアプリケーションのケースのようにデバイスがネットワークを介して接続される場合、いつでもサイバーセキュリティの懸念は、必然的に避けられません。リモートI/Oデバイスも同じです。ネットワーク上のデバイスのアクセシビリティおよびデータ機密性を慎重に管理する必要があります。企業内に適用されているセキュリティポリシーを確認することは、デバイスに必要なセキュリティ機能が装備されていることを確認することと同じくらい重要です。　デバイスは、不正アクセスをブロックし、許可されるトラフィックをコントロールする機能があることを確認します。さらに、ネットワーク上の機密データを通信するためのセキュアなデータ転送を可能にすることで貴重な情報を保護できます。モジュラーI/Oソリューションを選択する際、サイバーセキュリティは間違いなく考慮に入れたい事項です。



他の企業がI/Oデータをどのように保護しているか知りたいですか？詳細については、ケーススタディをご覧ください。
https://www.ibsjapan.co.jp/tech/details/case-studies/its/secure-modular-remote-i-o-increases-air-traffic-safety.html

Case Study

リモートI/Oソリューションを選定するときに上述の基準の考慮事項を適用すると最終的にデータ収集が容易になり、日常のオペレーションがスムーズかつセキュアに保たれます。I/Oコネクティビティの新しい需要を見越してMoxaは、IIoTデータ収集のために少ない労力でより多くの価値を提供する将来性を見据えたモジュラーリモートI/OデバイスioThinx4510シリーズ(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0704.html)を開発しました。

“将来を見据えたモジュラー
リモートI/Oデバイスは、OTおよび
ITエンジニアの両方にとって
データ収集を容易かつ安全に
維持することができます”

IIoTデバイスコネクティビティの次は？

レガシーのシリアルデバイスとリモートI/Oシステムがネットワークコネクティビティを使い装備されたたことにより、すべてのフィールドデータは、即座に素晴らしいビジネス洞察にトランスフォームすることで生産性を向上させました。間違いありませんね？　しかし、そんなに早まらないでください！

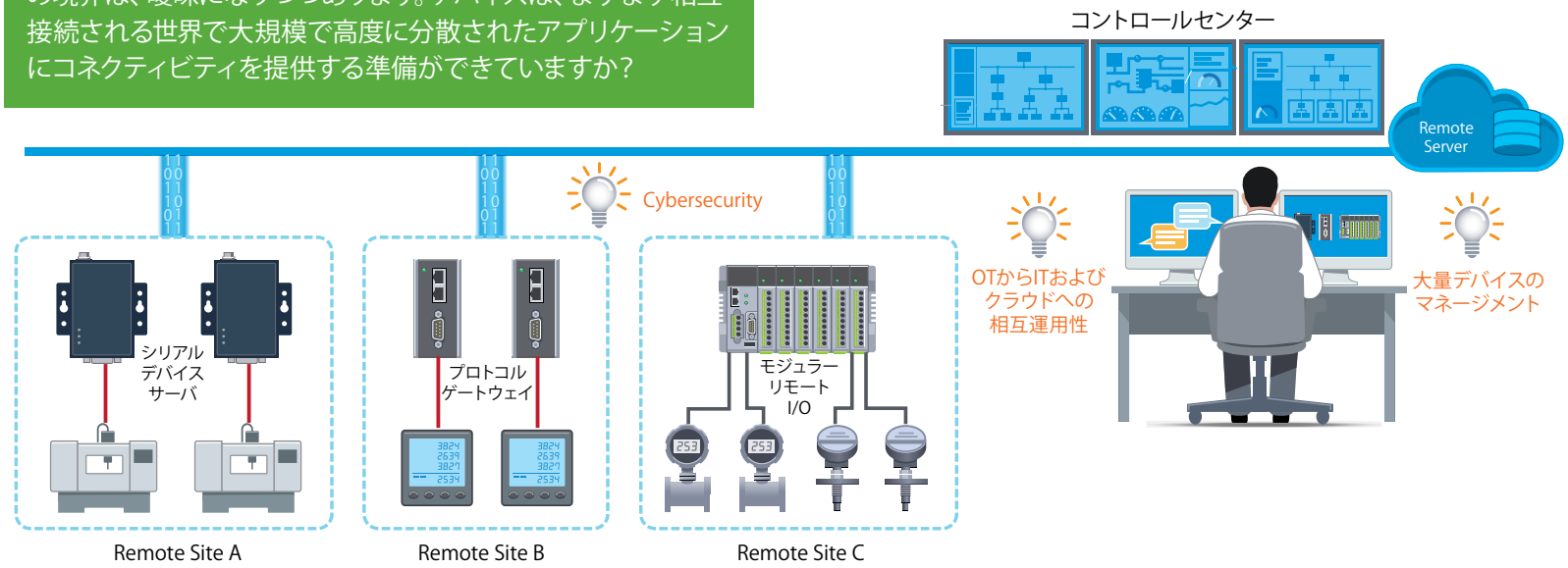
最適なデバイス サーバーまたはリモート I/O ソリューションを選択して導入することは、比較的単純な IIoT アプリケーションや小規模な IIoT アプリケーションに対して十分な場合があります。しかし、OTエンジニアおよびITエンジニアの両方がアクセスできるように異なる種類のデバイスを1つのネットワークに接続する必要がある場合では、どうなるのでしょうか？さらに、これらすべての異なるデバイスが世界中に分散している場合はどうでしょうか？

IIoTは、OTとIT間の境界を曖昧にするだけでなくフィールドデバイスが広い範囲に分散し、リモートサーバと直接通信する必要がある

大規模で高度に分散したアプリケーションの普及をもたらしました。つまり、データがどこに行き、どこから来るのか、異なるデバイスをどのように管理するのか、データの安全問題を以前よりも高く保つかがこれまで以上に重要であることを意味します。このセクションでは、コネクテッドワールドにおける大規模で高度に分散されたIIoTアプリケーションで要求される要件を満たすことができるデバイスコネクティビティソリューションを選択する際に留意すべき3つのヒントを提供します。

Key Question

IIoTの普及により産業オートメーションにおいて、OTとITの従来の境界は、曖昧になりつつあります。デバイスは、ますます相互接続される世界で大規模で高度に分散されたアプリケーションにコネクティビティを提供する準備ができていますか？



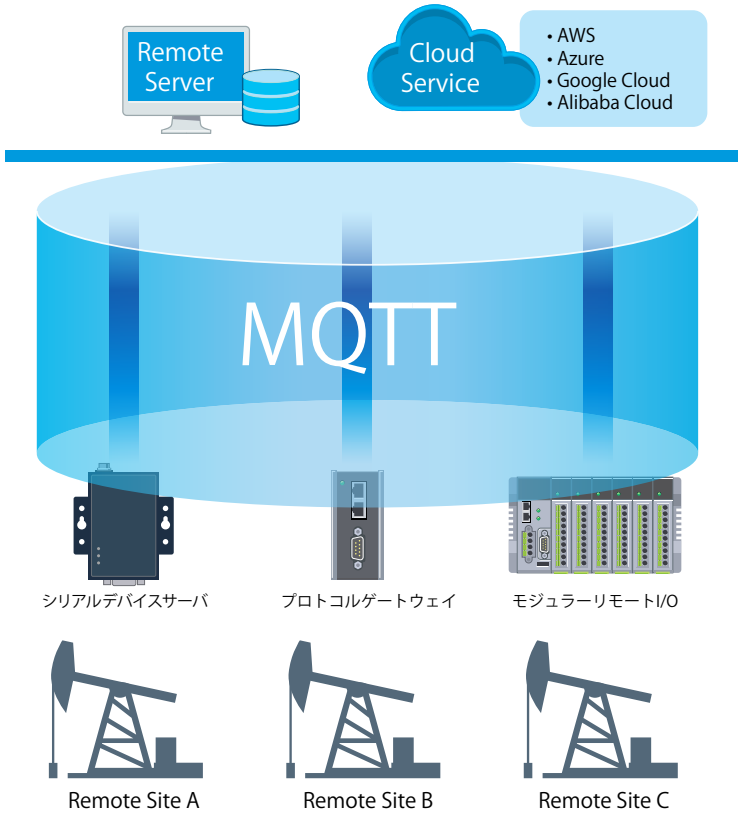
エキスパートのヒント 1

データの行き先を知る

大規模で高度に分散されたIIoTアプリケーションは、多くの異なるサイトからデータを収集する必要があります。例えば、広大な砂漠に展開される典型的な石油掘削アプリケーションのすべての掘削坑口を想像してみてください。各坑口からのすべてのデータが収集され、絶えず監視およびコントロールされる必要があるだけでなく、情報のすべてのデジタルビットを人間が読める洞察に変換するために伝送する必要があります。各フィールドサイトにエッジコンピュータを導入し、データの収集、ローカルでの前処理、リモートサーバへ伝送することで高度な解析を実行することができます。しかしながら、一部のアプリケーションでは、コネクティビティを可能にし、クラウドサーバでデータを十分に処理できる必要がある場合があります。

各IIoTフィールドサイトでコネクティビティデバイスを使用してOTデータをリモートサーバに伝送することは、不必要な時間、労力、コストを削減することができます。石油掘削などの多くの分散アプリケーションは、各フィールドサイトから比較的少量のデータを収集するだけなので複数の場所にエッジコンピュータを導入しては、関連するコストとプログラミングの労力をジャスティファイすることができません。その代わりにコネクティビティデバイスは、通常、そのトリックを実行することで費用対効果と効率が高くなります。

また、使用しているリモートサーバの種類も考慮する必要があります。プライベートサーバの場合、MQTTは、OTシステムとITシステムの間でデータをブリッジするために最も一般的に使用されるプロトコルの1つです。 Microsoft Azure、Amazon Web Services（AWS）、Google Cloudなどのパブリッククラウドサーバと同様に各サービスプロバイダには、データを収集するための独自の方法とプロトコルがあります。コネクティビティデバイスを選定する前に、アプリケーションがプライベートサーバまたはパブリックサーバのどちらを使用するかを把握または決定(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0712.html)し、関連するプロトコルまたはSDKをサポートするコネクティビティデバイスを見つけて、開発段階で時間と費用を削減する必要があります。

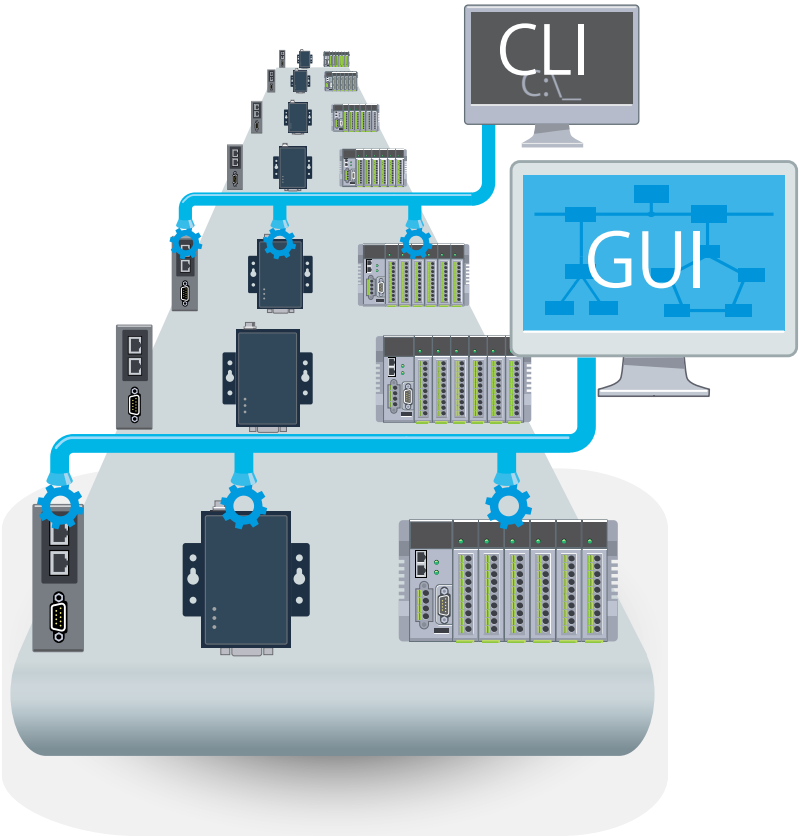


エキスパートのヒント 2

デバイスのマネージメントを完全に把握する

最終的に複数の通信インターフェースをフィールドデバイスとすべて接続すると、別に大きな疑問が生じます。数十または数百種類の異なるコネクティビティデバイスをどのように管理しますか？　日常のオペレーション中に、コネクティビティデバイスを監視して最新のファームウェアを最新の状態に保ち、すべてのユーザのデバイスログオン資格情報を更新することによって不正アクセスや潜在的な侵入を最小限に抑える必要があります。デバイスが少なく、コネクティビティデバイスが 1種類しかない場合、このようなタスクは問題とはなりません。しかしながら、IIoT アプリケーションで数十種類のコネクティビティデバイスを使用すると大きな負担になる可能性があります。

大量の異なる種類のコネクティビティデバイスを管理することができるソフトウェアツールまたはユーティリティを使用すると日常のオペレーションが大幅に楽になります。IIoT時代にITとOTワールド間の線引きが、ますます曖昧になる中、マネージメントツールは、両方のドメインのユーザにサービスを提供するために十分な柔軟性が必要となります。一括デバイスマネージメント機能に加えて、選択するコネクティビティデバイスには、IIoTシステムのメンテナンスを最適化するためにOTユーザのためのGUI(https://www.youtube.com/watch?v=2Im1TsfdUjo&feature=youtu.be&utm_source=ebook&utm_medium=organic&utm_campaign=20200 6-smb-cm-video)およびITユーザのためのCLI(https://www.youtube.com/watch?v=BuHvJgtmr14&feature=youtu.be&utm_source=ebook&utm_medium=organic&utm_campaign=20200 6-smb-cm-video)の両方が必要です。



エキスパートのヒント 3

いつものようにサイバーセキュリティは重要

サイバーセキュリティについて言及したのは、これが初めてではありません。そしてそれは最後ではありません！実際、産業用フィールドサイト、分散アーキテクチャ、およびレガシーシステムにおけるエンドデバイスの多様性は、IIoTアプリケーションのセキュリティリスクを増大させます。これは、これらのデバイスのほとんどがサイバーセキュリティを考慮して設計されていないためです。そのため、エンドデバイスの前に配置する組み込みのセキュリティ機能を備えたコネクティビティソリューションを選択することが不可欠です。しかし、異なるエッジデバイスの通信需要を満たすために非常に多くのコネクティビティソリューションが市場に存在している中で、フィールドデータを適切に保護するにはどうすればよいでしょうか?
IEC62443規格(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0561.html)の技法を使います。これは、選択したデバイスが最新のサイバーセキュリティ規格に確実に準拠するためにデバイスマニファクチュアラーが従うべき特定のセキュリティ要件をリストした一連のグローバルセキュリティガイドラインです。

コネクティビティデバイスを選択するときは、下記のチェックリストを使用してデバイスが十分なセキュリティ機能をサポートしていることを確認し、IIoT アプリケーションへのユーザアクセスを定義および管理ができるようにします。

- ☑ デバイスにログオンできるユーザを特定して管理する
- ☑ アクセスコントロールを強化するためにパスワードの複雑さを増す
- ☑ デバイスがネットワークにアクセスして他のデバイスと通信する前に許可されたデバイスを確認する
- ☑ ネットワーク上の機密シリアルインターフェースデータを暗号化してデータの完全性を確保する
- ☑ コンフィギュレーションデータを暗号化して機密性を高める
- ☑ 報告された脆弱性に迅速に対応して修正するデバイス ベンダを選定する

上述の 3つのヒントを念頭に置くことでIIoT アプリケーションが簡単、よりセキュアで効率的にできるデバイスコネクティビティを可能にします。このためにMoxaは、フィールドデータをプライベートサーバまたはパブリックサーバにセキュアかつ効率的に接続できるシリアルデバイスサーバ、プロトコルゲートウェイ(https://www.ibsjapan.co.jp/products/MGate_5105-MB-EIP.html)およびリモートI/Oデバイス(https://www.ibsjapan.co.jp/products/ioThinx_4510.html)の一連のデバイスコネクティビティソリューションを開発しました。

“接続が進む世界で大規模または高度に分散されたIIoTアプリケーションにデバイス接続を可能にするには、OTとITシステム間の円滑な通信、強力なデバイス管理性、および妥協のないサイバーセキュリティが必要です。

産業ネットワークのニーズ — 現在および将来への対応

前のチャプタでは、IIoTアプリケーションと従来、接続されていないOT資産をデータ収集、データトランスフォーメーション、およびデータ解析の恩恵を受けられるように産業用フィールドデバイスのコネクティビティを実現する方法について説明しました。しかしながら、これらすべてのフィールドデバイスを接続するには、複数の相互接続されたデバイス、システム、さらにはリモートサイト間の情報フローをサポートできるネットワークを構築する必要があります。

従って、以下の要素を産業用ネットワークインフラストラクチャに組み込むことを考慮する必要があります。

イーサネット ネットワークノード

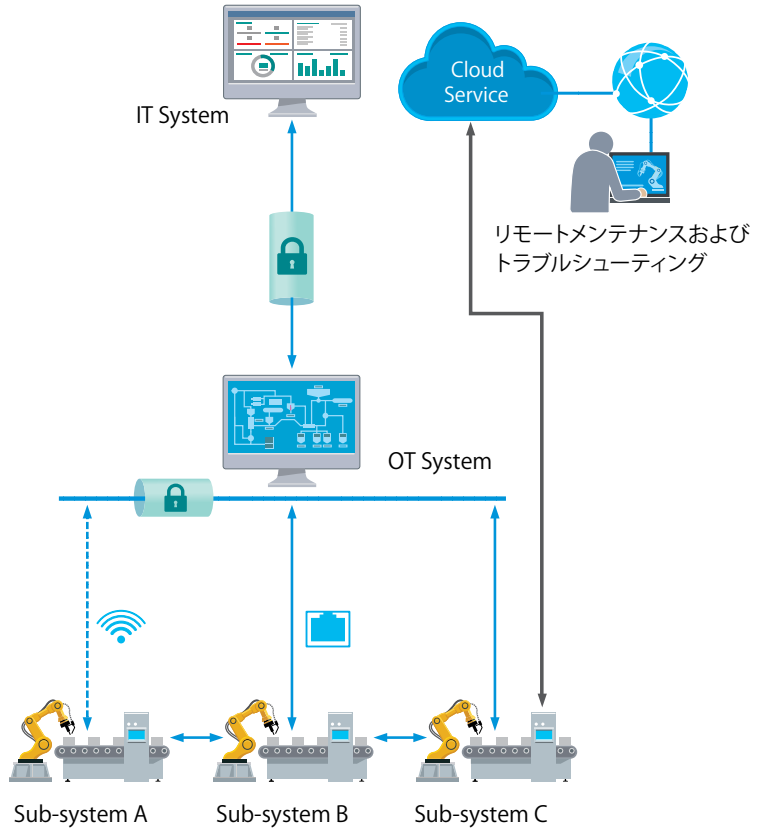
LANのイーサネット基盤の構築、リモートエッジシステムの統合、ネットワーク全体の接続には、様々なマネージドまたはアンマネージドイーサネットスイッチを利用できます。

ワイヤレスネット ワークノード

ケーブル配線が困難なアプリケーションまたは優れたモビリティを実現するために必要なアプリケーションの場合、ワイヤレス LANテクノロジーが有線イーサネットネットワークに代わる費用対効果に優れた柔軟なオプションを提供できます。

ネットワーク ゲートキーパー

フィールドデバイスおよびOT資産をインターネットに接続するとネットワークが新しいサイバーセキュリティリスクにさらされます。そのためセキュアなルータおよびファイアウォールが優れた防御の最前線を提供します。



将来を見据えた 産業用ネットワーク

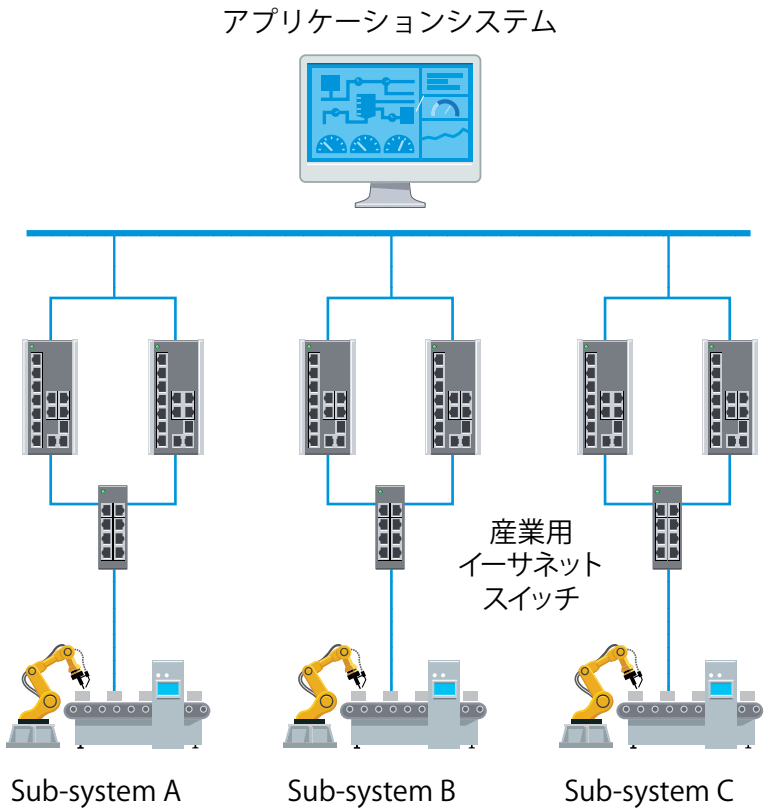
多くのIIoTアプリケーションは、ビジネスチャンスを提供するだけでなく、既存のネットワークインフラストラクチャから、より多くのものを必要とします。この長期にわたる戦いを勝ち抜くためには、産業ネットワークが将来の課題と機会に確実に対応できることが不可欠です。

次のチャプタでは、現在および将来の産業用ネットワークのニーズに対応するイーサネットスイッチ、ワイヤレスデバイス、セキュアルータ、セキュアリモートアクセス、およびネットワークマネージメントを導入する際に事前の計画に必要な重要な考慮事項について説明します。

エッジネットワークにイーサネットスイッチを導入

多くの数の機器を1つのシステムに接続することは、容易ではありません。単一の自動化された生産ラインの場合、コネクティビティを可能にするためにイーサネットネットワークノードは、1つまたは2つだけなのでコントロールセンタのオペレータによりシステムのステータス監視とインシデントに対応することができます。ここで、増え続けるデバイスを複数のシステムから単一のネットワークに接続するという頭痛の種を想像してみてください。すべての問題と課題が掛け算のように大きく増大します。これは、複数の自動化生産ラインを異なるファクトリに統合する産業オートメーションエンジニアが直面する現実です。これらのデバイスとイーサネットノードがすべて接続された後、オペレータが継続的なオペレーションを維持するために必要な重要なデータを受信するには、どうすればよいでしょうか。

1つのソリューションは、マネージドのイーサネットスイッチを導入することでネットワーク伝送を管理し、必要に応じて関連するパラメータを設定することができます。マネージドイーサネットスイッチは、優れた管理を提供しますが、複数のマネージドスイッチを維持するには、多くの時間と労力を要します。さらに、マネージャブルなネットワークノード数を増やすと、コンフィギュレーションおよびメンテナンス作業が増える可能性があります。実際、ネットワークの早い成長を考慮して慎重なネットワーク計画と設計が不可欠です。一方、一部のネットワークノードでアンマネージドスイッチを使用するとネットワーク全体の効率が向上すると共にメンテナンス作業を軽減することができます。

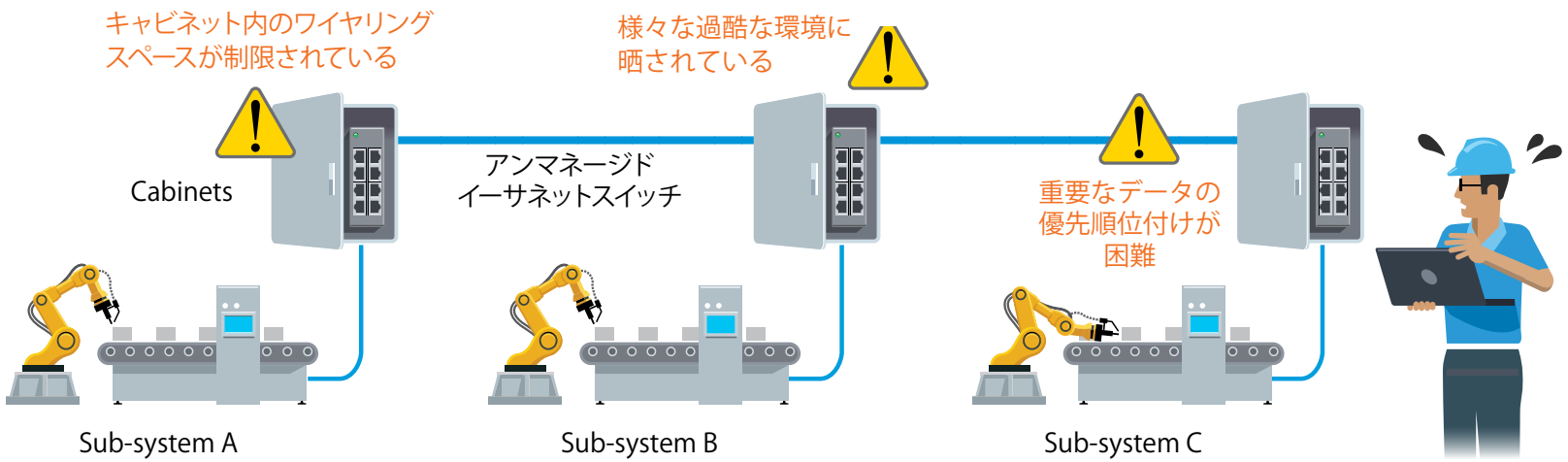


アンマネージドイーサネットスイッチを選定するための重要な基準

産業オペレータは、アンマネージドイーサネットスイッチがフィールドデータをIPネットワークに接続するためのシンプルなネットワークhubと見なすことがよくあります。産業オペレーションを運用中、オペレータは、ネットワーク上にアンマネージドイーサネットスイッチが存在していることすら忘れていることがあります。しかし、ビジネスの洞察を生成するために接続するデバイスが増大することで、予期せぬネットワークの不安定さにより産業オペレータが脅かされる可能性が生じます。そのため増大する複雑なネットワーク要件を満たすためには、アンマネージドイーサネットスイッチに追加機能が必要となります。ここでは、IIoTアプリケーションに最適なアンマネージドスイッチを選定することができる、いくつかの重要な基準について説明します。

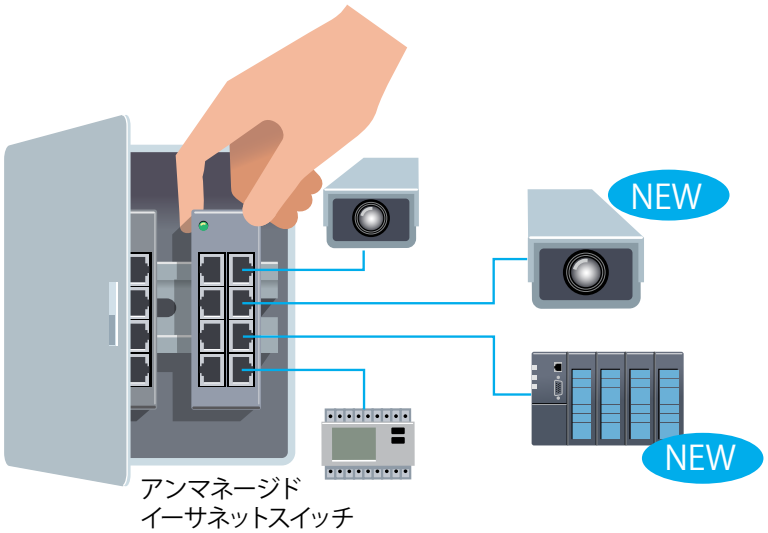
Key Question

既に複数の産業用デバイスがフルに収納されているスペース制限のあるコントロールキャビネットにアンマネージドイーサネットスイッチを押しこみ、またオペレーション中やメンテナンス中にエンジニアがデバイスとネットワークのステータスを容易にチェックするには、どうすればよいでしょうか？



主要な基準 1
拡張の計画

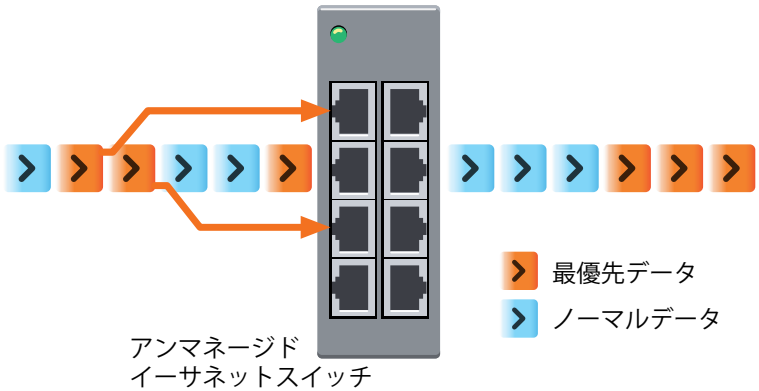
ネットワークで増大するコネクテッドデバイスの数を確実にサポートすることができる基本的な要件は、ポート数と大容量のデータボリュームに対し十分な帯域幅を備えたアンマネージドスイッチを使用することです。アンマネージドスイッチは、通常、スペース制限のあるキャビネットにインストールされるためコンパクトで高密度ポートソリューションを使用することで将来の拡張が懸念される問題を削減できます。もう一つの大きな考慮事項は、ネットワークのスピードと伝送距離です。今日では、ビデオストリーミングといった帯域幅を大量に使用する全体的な伝送スピードに影響を与える様々な種類のデータが存在します。ギガビットポートまたはファイバーポートを備えたアンマネージドスイッチは、現在および将来を見据えたデータアップリンクに必要な十分なネットワークスピードと伝送距離を確保できます。



主要な基準 2
各ノードでのパケットの優先順位付け

サービス品質（QoS）は、重要なデータを常に高い優先度で伝送するために使用される一般的な機能です。QoSを使用しないとネットワークが混雑している場合、重要なデータが伝送中に遅延する可能性があります。QoSは、通常、マネージドスイッチまたはPLCデバイスなどの特定のコントロール機器によりサポートされていますがアンマネージドスイッチではめったに見られません。現在、ネットワークノードでフィールドサイトから複数のデータの種類を伝送する需要が高まっていることから、アンマネージドスイッチでもこの機能を使用して、すべてのノードにマネージドスイッチを導入するような必要な余分な労力と高額な投資を行うことなく、重要なデータを時間内に伝送できるようになりました。

アンマネージドスイッチを選定する場合、重要なデータのコントロールを優先できるQoSまたは同様の機能が搭載されていることが確認できたならネットワークをシンプルに保つことできるので敢えてマネージドスイッチを使うために多くの時間と労力をかける必要がなくなりました。



主要な基準 3

あらゆる環境の信頼性を検証

特定のアプリケーション要件に対して、産業認証を受けたアンマネージドスイッチを選定することが信頼性を確認する最も簡単な方法です。しかしながら、すべての産業用アプリケーションが認証を必要とするわけではありません。それでも注意すべき点として、一般的な環境条件として極端な温度と高い電磁干渉の2つがあります。産業用アンマネージドスイッチは、ワイド動作温度と冗長電源入力のサポートにより過酷なネットワーク環境下で信頼性の高い動作を続けることが保証されます。

オペレーション中に電源またはポート障害などの緊急事態が発生した場合、アンマネジメントスイッチは、オペレータに警報を送ることでオペレータが直ぐに応答できることが必要です。

信頼できるオペレーションを実現した成功例を紹介します。詳細は、アプリケーションノートをご覧ください。

https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0697.html

前述の3つの基準を使用してオプションを評価すると産業用アプリケーションに適したアンマネージドスイッチを見つけることができます。急速に拡大する産業用ネットワークのニーズに対応するためにMoxaは、超スモールフォームファクタ、信頼性に優れ、導入が容易で、優れた柔軟性を提供する様々な産業用アプリケーションに適したEDS-2000-ELシリーズおよびEDS-2000-MLシリーズの新しい一連の産業用アンマネージドイーサネットスイッチを開発しました。

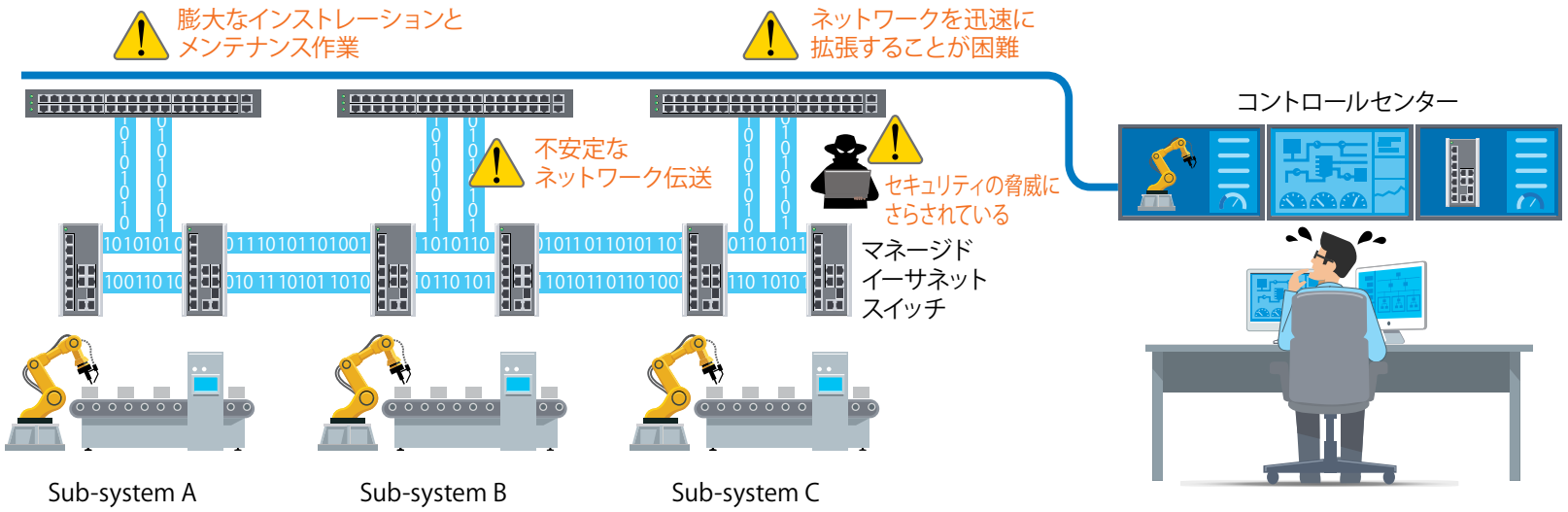
“超スモールフォームファクタでありながら重要なデータを常に高い優先度で伝送するサービス品質(QoS)をサポートするアンマネージドスイッチは、より最適化されたデータ伝送を必要とするファクトリオートメーションに最適です”

マネージドイーサネットスイッチを選択するための主な基準

コネクテッドシステムを実現するためのネットワークノードへの需要の高まりは、Industry4.0およびIIoTの変革が本格化する傾向に伴い避けられなくなっています。一部のネットワークノードは、基本的な管理機能を備えたアンマネージドスイッチを使用してネットワークの複雑さと管理の労力を最小限に抑えることができますが、他の状況では、大規模な統合ネットワークで引き続き重要な役割を果たすマネージドスイッチが必要となります。マネージドスイッチは、新しい変更に適応し、適切な場所に適切なタイミングでデータを確実に配信するために以前に比べてスマートで汎用性が高い必要があります。ここでは、最新の自動化に適したマネージドスイッチを特定するために役立つ3つの主要な基準を見てみましょう。

Key Question

デジタルトランスフォーメーションは、信頼性の高いネットワークを使用してシステムの稼働時間を維持し、リスクとエラーを削減します。現在使用中のマネージドスイッチは、この状況に十分耐えることができますか?



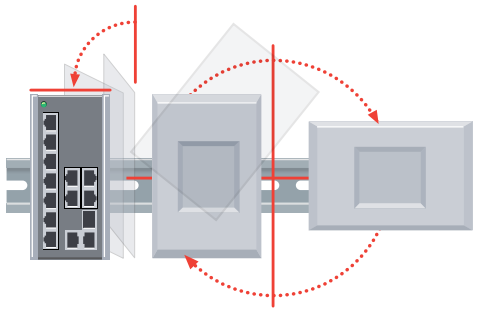
主要な基準 1

使いやすく、オペレーションが簡単

優れたユーザビリティは、あらゆるネットワーキングソリューションにとって不可欠です。産業オートメーションに、これまで以上に必要なものは、単一の産業ネットワーク上に多数のネットワークノードが接続されることです。インストレーションから日常のオペレーションおよびメンテナンスに至るまで、下記のマネージドスイッチ機能を使用することで管理性を容易に保つことができます。

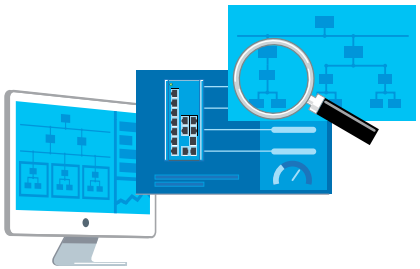
様々なマウンティングオプションを使いシンプルにインストレーション

各ノードは、どこにそれをインストールするかに応じて異なる要件があります。様々なマウンティングオプションによりインストレーションが容易になります。



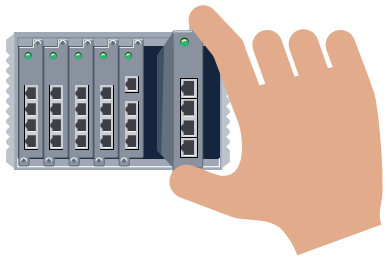
ネットワークステータスを一目で

エンジニアが対応を必要とする数百のタスクの1つとしてネットワークノードのステータスの追跡があります。ユーザフレンドリーなインターフェースをもつマネージドスイッチを選定することによりステータスをすばやくチェックし、変更を実行することができます。



ホットスワップ設計により メンテナンスを容易にする

デバイスのメンテナンスは、避けられません。モジュラーマネージメントスイッチを選定することで全体的なオペレーションに影響を与えることなくメンテナンス中に電源モジュールまたはラインモジュールをホットスワップすることが可能です。



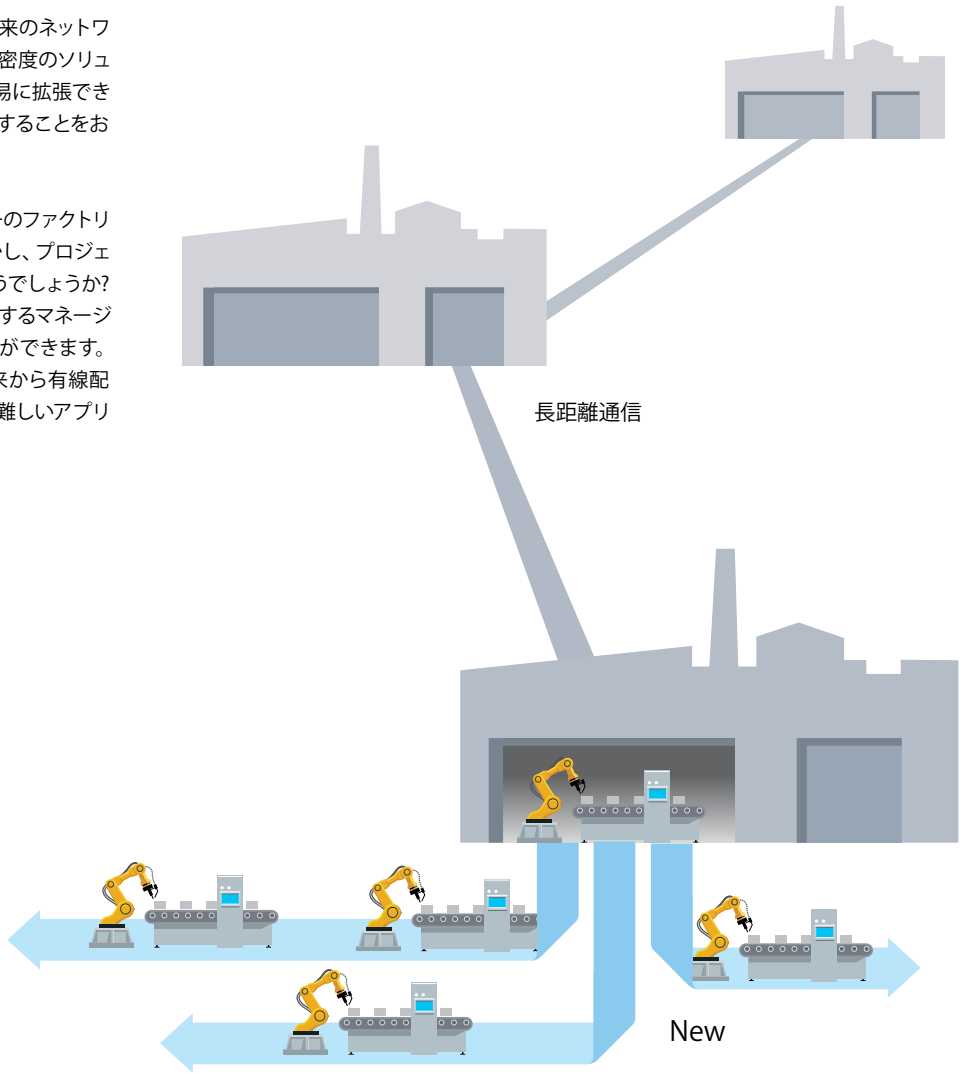
主要な基準 2

使いやすく、オペレーションが容易

アンマネージドスイッチと同様にマネージドスイッチを選定する場合は、将来のネットワーク拡張を考慮する必要があります。しかしながら、コンパクトで高ポート密度のソリューションを探す代わりに、必要に応じてモジュールを追加し、システムを容易に拡張できる共に、そのインストール時間が低減できるモジュラー設計の製品を選定することをお勧めします。

もう 1つの考慮する事項は、コネクテッドシステムの場所です。これは、単一のファクトリ内でコネクテッドシステムを可能にする場合には問題とはなりません。しかし、プロジェクトが異なる場所にある複数のファクトリや施設が含まれている場合はどうでしょうか?

高度に分散されたネットワークにおいては、光ファイバー伝送をサポートするマネージドスイッチが膨大な距離を通して信頼性の高いデータ伝送を実現することができます。実際、環境の制限によりネットワークの接続が困難な場合があります。従来から有線配線は、依然としてそれなりのメリットがありますが、有線に接続することが難しいアプリケーションでは、ワイヤレスネットワークを検討する必要があります。



主要な基準 3

可用性とセキュリティがすべて

産業用システムを相互に接続するとネットワークの複雑さが大幅に増大し日常のオペレーションに影響を与える可能性があります。 1つの要素でシステム全体を停止する単一障害点は、ネットワークのダウンタイムを引き起こし、重要なデータが失う可能性があります。ネットワークノードの障害を回避するには、マネージドスイッチに冗長メカニズムとセキュリティ機能が必要となります。

冗長メカニズム

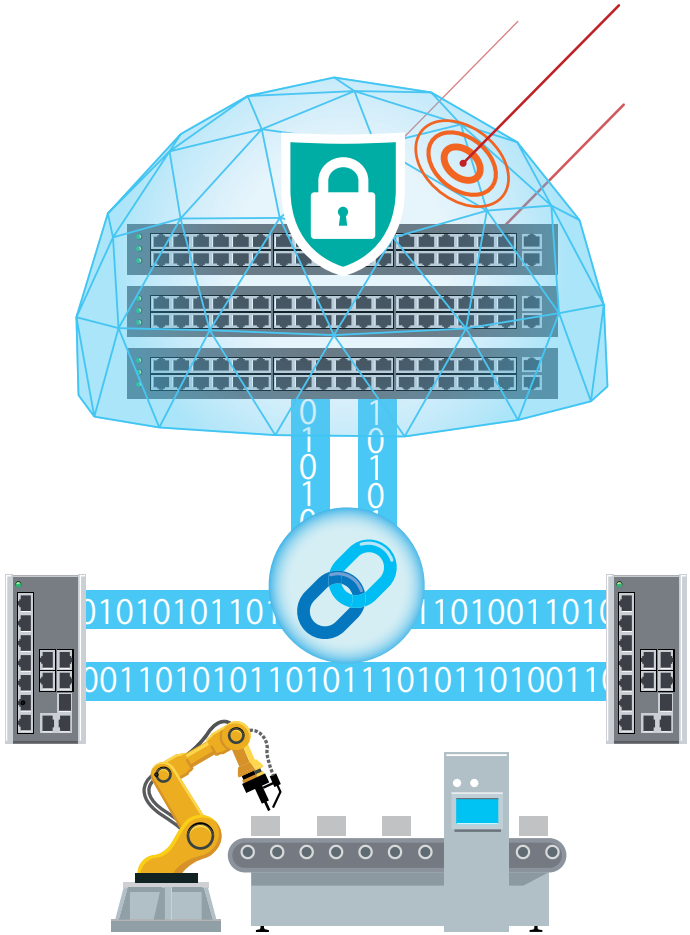
ネットワークの冗長性(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0632.html)は、マネージドスイッチで見られる高度な機能です。この考え方は、ネットワークノードに障害が発生した場合に重要なデータが失われることを防ぐことです。冗長バックアップパスを有効にして障害が発生したノードをバイパスし、数秒未満またはさらに高速にデータ転送をリカバーできます。

セキュリティ機能

ネットワークノード数とコネクティビティを増やすことによるもう1つの潜在的なリスクは、不正アクセスや脆弱性にさらされる危険性が高くなる点です。セキュリティ上の懸念事項を見逃さないためにIEC62443規格（https://www.ibsjapan.co.jp/tech/moxa-a/moxa-tech-0561.html）に基づくセキュリティ機能を備えたネットワークデバイスを選定してネットワークノードを不要なアクセスから保護することが必要です。さらに安心してネットワークデバイスを脆弱性から保護するために独自のサイバーセキュリティ対応チームを有するベンダを選定することも必要です。

上述の3つの主要な基準を使用してマネージドスイッチのオプションを評価することで産業用ネットワークの自動化に最適なソリューションを見つけることができます。急速に変化するネットワーク要件に対応してMoxaは、様々な産業アプリケーションに対して費用対効果に優れたユーザビリティ、セキュリティ、ネットワーク可用性を提供するスケーラブルなモジュラー設計による新しいシリーズの産業用マネージドイーサネットスイッチMDS-G4000シリーズを開発しました。

https://www.ibsjapan.co.jp/products/MDS-G4012_series.html
https://www.ibsjapan.co.jp/products/MDS-G4020_series.html



“信頼性の高いネットワークを開発する鍵は、スケーラブルで使いやすく、データ転送を正確でセキュアに保つことができるパワーフルなマネージドイーサネットスイッチを使用することにあります”

ワイヤー配線を使わないで多くの可能性を実現する

すべての産業アプリケーションでは、従来のように有線を利用することが常に可能であるとは限りません。新しく産業用オペレーションを実現するために新たに電力線の敷設、LAN配線などを含めた設備を再構成に関わる大きな投資に要し、インストールも困難で時間がかかるような場合、産業用ワイヤレスLAN(WLAN)が従来の有線イーサネットLANに代わる理想的な選択肢を提供します。近年、ワイヤレステクノロジーの進歩は、自動車、物流、交通輸送システムなどなど様々なアプリケーションにおいて一般的なソリューションとして産業WLANに浸透しています。これらの産業用アプリケーションは、通常、絶えず移動を必要とし、各種配線が困難な自動化された機器に適用するために必要とします。適切な産業用WLANを導入することで運用効率を向上させることも可能となります。

従来の有線から解放のされる可能性が非常に高くなりつつある近年、産業WLANアプリケーションの人気が急速に高まっています。例えば、WLANテクノロジーを使用してスマート倉庫や自動搬送システム、AGVを導入して効率と生産性を向上させ、限られた人材を最大限に活用することができます。

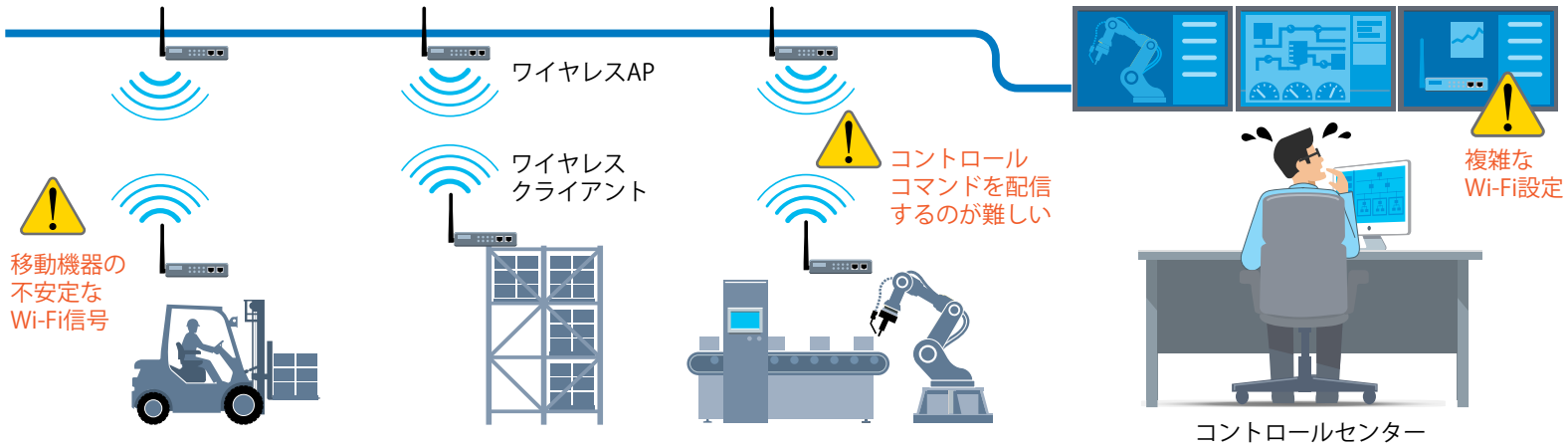
可能性は、無限であるとしてもワイヤレスに使用することが必ずしも明確な選択とは限りません。ワイヤレスLANを決定した場合、産業要件に適したソリューションをどのように選択しますか？ そこで以下の基準を考慮する必要があります。

産業用Wi-Fiデバイスを選定するための主な基準

間違いなく産業用ワイヤレスLANは、従来の物理的な制限や境界を超えてコネクティビティを拡張し、新しい可能性へと進んでいます。しかしながら、産業用ワイヤレスLANには、様々なハードルが存在するため産業エンジニアは、ワイヤレスアプリケーションの導入に躊躇する場合があります。有線と違い電波が見えないワイヤレスコネクション中でネットワークが実際に接続されていることをどのように確認したらいいのでしょうか？これらの見えないコネクションがダウンした場合、どのようにトラブルシューティング(https://www.ibsjapan.co.jp/news/04/newProducts-0471.html)をしたらいいのでしょうか？　IIoTアプリケーションでは、システムを1つの統合ネットワークに接続する必要があるため、このような懸念はこれまで以上に必要となります。単一障害点は、ネットワーク全体にとって致命的となる場合も考えられます。産業用ワイヤレスネットワークの設計(https://www.ibsjapan.co.jp/downloads/gview/kataban:Expert_Tips_for_Optimizing_Industrial_Wireless_Networks)を計画することに加えて、産業用WLANデバイスを選定するためのいくつかの重要な基準と一般的な問題に対処する方法について説明します。

Key Question

WLANテクノロジーを利用する場合、WLANデバイスがWi-Fiネットワークを介してデータ転送を保証し、期待に応えることができますか？



主要な基準 1

Wi-Fiの可用性はファーストプライオリティ

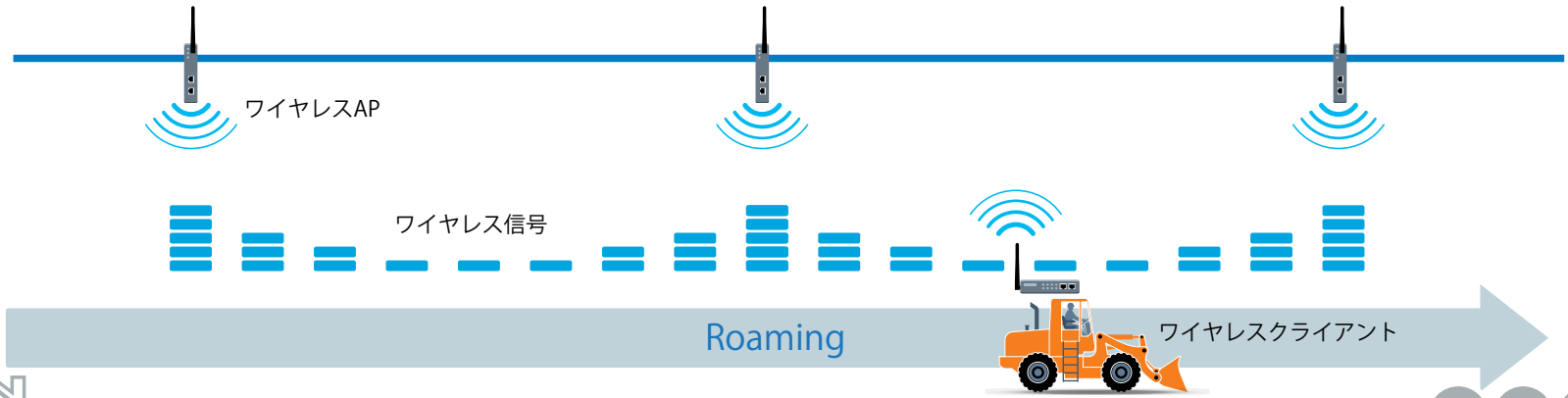
産業用WLANデバイスには、信頼性の高いワイヤレスネットワークを確立し、保証するための特殊なテクノロジーが要求されます。その理由は、ワイヤレスコネクションの品質は、無線周波数（RF）、産業環境での各種干渉、チャンネルの電波干渉、不適切なアンテナのコンフィギュレーション、長距離をサポートする信号強度など、様々な問題の影響を受けます。このような問題を回避するためにシステムを適切に設計しないと、不安定な通信、モータ駆動の際のサージ発生によるデバイスへの損傷、強いてはシステムの完全なシャットダウンに繋がります。

さらに、ワイヤレスクライアントAPを搭載し、絶えず移動するビークルは、ローミング要件に特別な注意を払う必要があります。例えば、A点のワイヤレスAPからクライアントが強力なワイヤレス信号を受信できても、別の場所B点のAPに移動するまでの間に信号強度が減衰して受信ができなくなる前にB点のAPからの信号を高速に受信する高速なローミングが必要となります。ローミングが遅いまたはローミングを失敗したコネクションは、産業環境では絶対に受け入れられません。高度なワイヤレスローミングテクノロジーは、ミリ秒レベルの高速ローミングにより信頼性の高いワイヤレスコネクションを実現できます。

特にAR/RS(自動倉庫)システムでの走行するビークルに搭載するワイヤレスデバイスを使用するワイヤレスネットワークの設計については、注意が必要です。詳細についてはWhite Paperをご覧ください

https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0479.html

White Paper



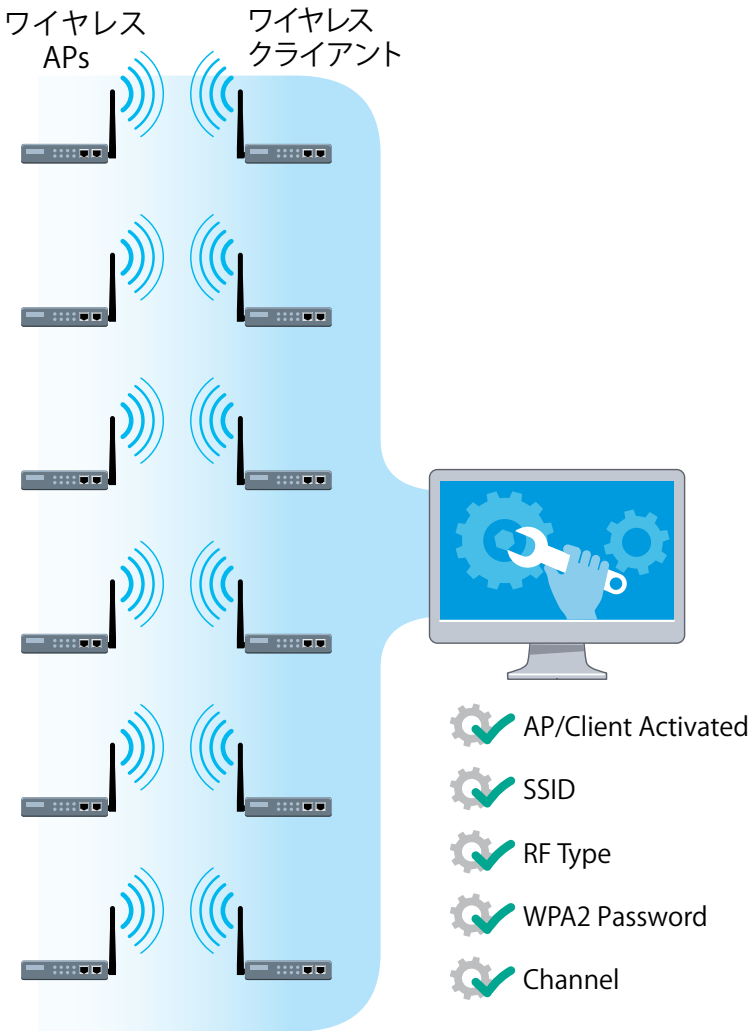
主要な基準 2

Wi-Fi設定の作業努力を最小限に

初めてワイヤレスネットワークを実装する場合でも、既に多くのWLANの導入を経験している場合でも、使いやすいソリューションを常に選択する必要があります。ワイヤレスコネクションは、ネットワークインフラストラクチャの構築をより便利にしますが、ネットワークのセットアップと長期にわたるメンテナンスがユーザエクスペリエンスに大きな影響を与えます。ネットワークを導入または維持するための初期セットアップ段階での基本的なデバイスコンフィギュレーションに関しては、パワーフルなソフトウェアツールを使用すると時間と作業を大幅に低減できます。または、サイトサーベイツールEkahau(https://www.ibsjapan.co.jp/products/Ekahau_Pro_10.html)を使用することができます。ネットワークがアップしたら、すべてのデバイスを簡単に構成し、マウスをクリックするだけで環境に対応した最適なWi-Fiチャンネルを見つけることができるソフトウェアツールAeroMag Technology(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0585.html)を使用してワイヤレスコネクションを安定させ、ネットワーク管理による頭痛の種を取り除くことができます。

素早くかつ簡単にWi-Fiネットワークの導入を実現できる"AeroMag Technology"を使用した実践的なビデオ（英語版）をご覧ください。

https://www.youtube.com/watch?v=R2Xyryov1ll&feature=youtu.be&utm_source=ebook&utm_medium=organic&utm_campaign=202006-smb-cm-video



主要な基準 3

プロトコル互換性の問題が原因で足かせにならないために

多くのWLANデバイスは、無人搬送車（AGV）や物流システムのフォークリフト(https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0661.html)など、様々な産業用アプリケーションに導入されています。

これらのシステムでは、移動するビークルの位置を特定するためにセンサやPLCなどの高度なデバイスが必要です。また、安全上の理由からPLCとコントロールセンタ間のシームレスな通信を確保することが不可欠です。PLCなどの産業用機器をワイヤレスクライアントに接続する場合に考えられる一般的な問題は、ワイヤレスクライアントデバイスがPROFINETなどの特定の産業用プロトコルをサポートできるかどうかです。シームレスな産業用プロトコル通信を確保するためには、次の要件を考慮する必要があります：

1.WLAN上を通してLayer 2の透過性
2.アプリケーションを満たす通信レイテンシー要件

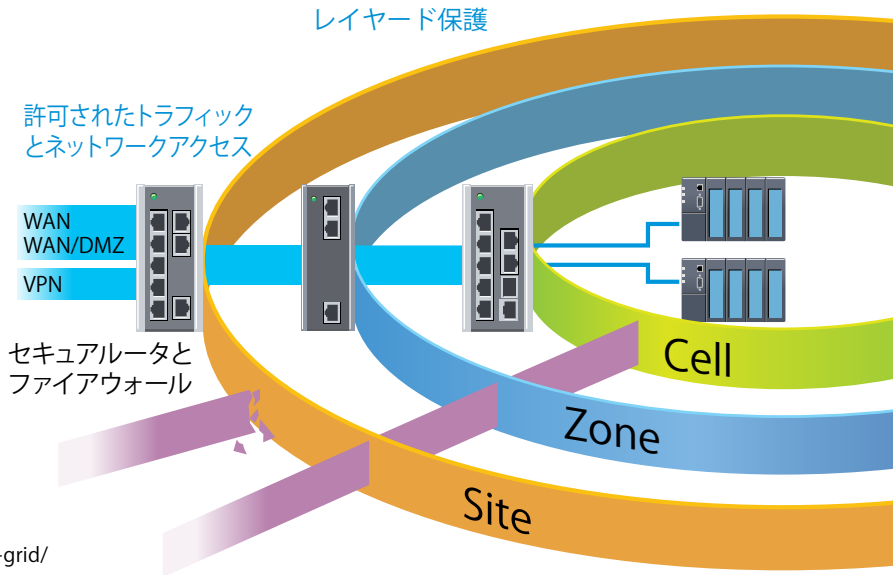
上述した3つの重要な基準は、世界中のカスタマのために産業用コネクティビティを可能にする長年の経験から抽出されたものです。産業用アプリケーションの課題を克服するために特別に設計された産業用IEEE 802.11nワイヤレスAPブリッジ/クライアントの詳細については、Webサイト(https://www.ibsjapan.co.jp/products/moxa/5760/)をご覧ください。

“信頼性の高いワイヤレスネットワークには、コネクションのアベイラビリティ、通信の相互運用性、オペレーションのあらゆる段階での使いやすさを保証できる産業用WLANソリューションが必要です”

ネットワーク防御の最前線

何十万人もの人々が電気を失いました1。グローバルサプライチェーンが急停止2。これらは、近年の重要なインフラストラクチャと製造に対するサイバー攻撃による壊滅的な影響のほんの一例です。実際、過去10年間で、産業用コントロールシステムに関連するサイバーセキュリティインシデントがかつてないほど多く発生しています3。これらのインシデントのいくつかは、Stuxnetといった標的型攻撃でありイランの核計画に対しても障害を与えました。一方、ネットワークコンピュータに感染してマルウェアが産業用コントロールシステムに拡散する非標的型のインシデントもあります。

IIoT時代では、より多くの洞察を得て生産性を向上させるために、かって従来接続されていなかったシステムがプライベートネットワークまたはパブリックネットワークを介して接続されるようになりました。より大きなコネクティビティの欠点は、産業ネットワークがもはやサイバー脅威に対して免疫がなくなっているということです。グッドニュースとしては、エキスパートが口をそろえ、産業ネットワークに対するサイバーセキュリティの強化を訴えています。一般的に、産業サイバーセキュリティを実装する方法には、2つあります。1つは、ネットワークインフラストラクチャの基盤をセキュリティで保護し、許可されたトラフィックのみが適切な場所に流れるようにすることです。もう1つは、重要な資産を特定し、階層化された保護を適用することです。産業用セキュアルータとファイアウォールは、産業用ネットワークへの不正アクセスおよびトラフィックを防ぐために最前線に導入されるため、これらの方法の両方が不可欠です。



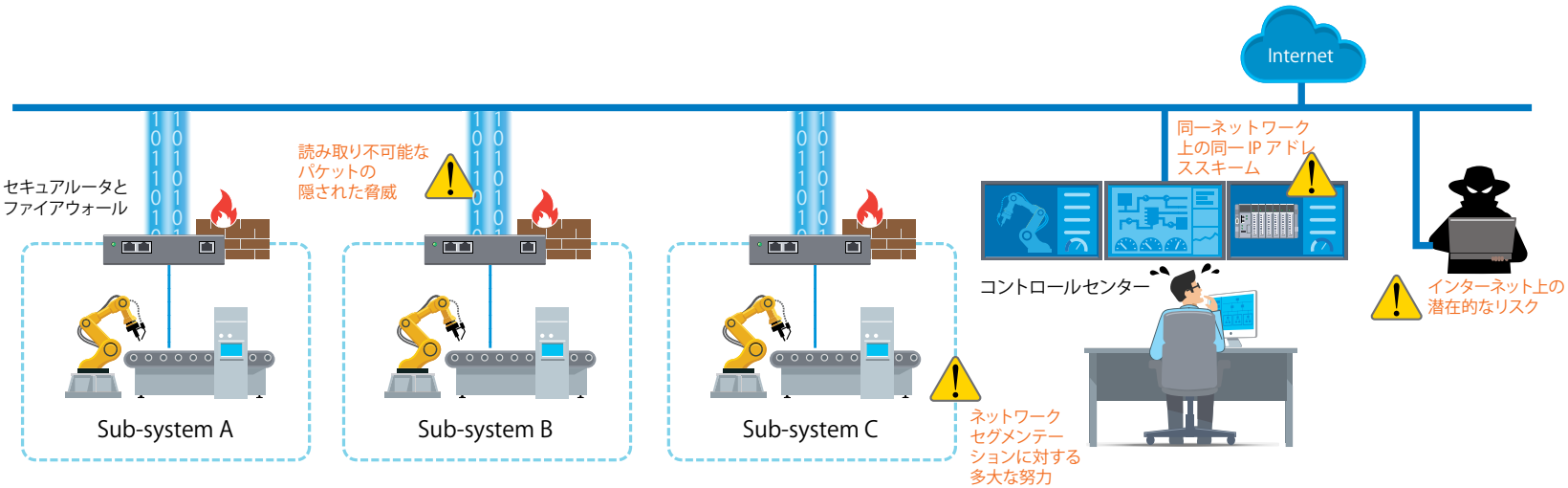
1. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
2. https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-march-26/
3. According to ICS-CERT Advisories from the United States Cybersecurity and Infrastructure Security Agency (CISA). https://www.us-cert.gov/

産業用セキュアルータとファイアウォールを選定するための主な基準

産業用コントロールシステムは、重要な機器を保護し、オートメーションネットワーク上の様々な場所、デバイスCell、ファンクションZone、ファクトリSiteを保護するために"多層防御"（defense-in-depth）アプローチを適用できます。多層防御サイバーセキュリティには、物理的、テクニカル、管理の3つのタイプのコントロールが含まれます。まず、ネットワークをセグメント化し、各セグメント間に境界を作成することにより物理的なコントロールを実装します。次に、ネットワークトラフィックの保護またはデータパケットのフィルタリングによりテクニカルなコントロールを適用します。最後に、IPアドレスの管理、強力なセキュリティポリシーを採用することにより管理セキュリティを強化します。セキュアルータおよびファイアウォールは、ネットワークで多層防御のサイバーセキュリティを実現する優れた方法を提供しますが、産業用アプリケーションに適したルータまたはファイアウォールをどのように選定したらいいのでしょうか？　そこで以下の基準を考慮する必要があります。

Key Question

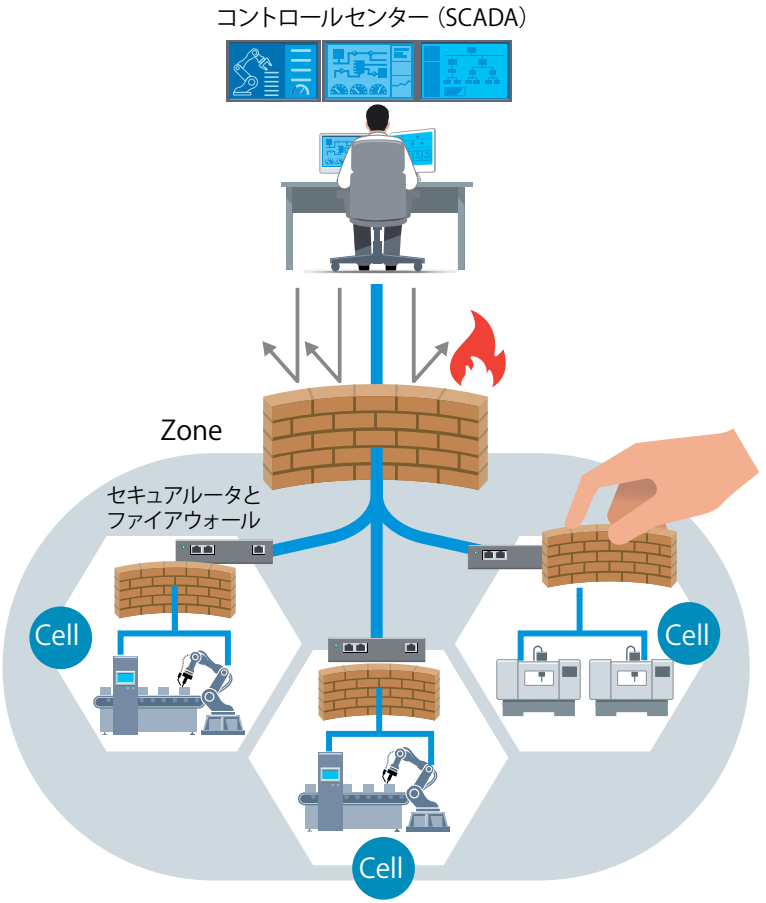
産業用オートメーションネットワークのセキュリティを強化することは、もはや選択の余地がありません。それは必須です。産業オペレーションを維持しながらサイバー脅威からビジネスと資産をどのように保護したらいいのでしょうか?



主要な基準 1

ネットワークを変更せずにファイアウォールを追加する

ネットワークのセグメンテーションは、産業用ファイアウォールを使用してネットワークを物理ゾーンまたはロジカルゾーンに分割します。ファイアウォールは、IPパケットを調べ、事前に構成されたポリシールールとパケットを比較し、パケットに対して許可、拒否、またはその他のアクションを実行するかどうかを決定するアクセスコントロールデバイスです。 一般的に言えば、ファイアウォールは、"ルーティング"または"透過"のいずれかであり、必要なのはアプリケーションの要件によって異なります。ルーティングファイアウォールとは異なり透過型ファイアウォールでは同じサブネットを維持できるため既存のネットワークにファイアウォールを簡単に追加できます。透過型ファイアウォールを使用するとネットワークトポロジを変更する必要もありません。透過型ファイアウォールは、ネットワークトラフィックが単一のサブネット内で交換されるコントロールネットワーク内の重要なデバイスまたは機器の保護に適しています。さらに透過型ファイアウォールは、ルーティングプロセスに参加しないためIPサブネットを再構成する必要はありません。



適切な産業用ファイアウォールの選定方法の詳細については、White Paperをご覧ください

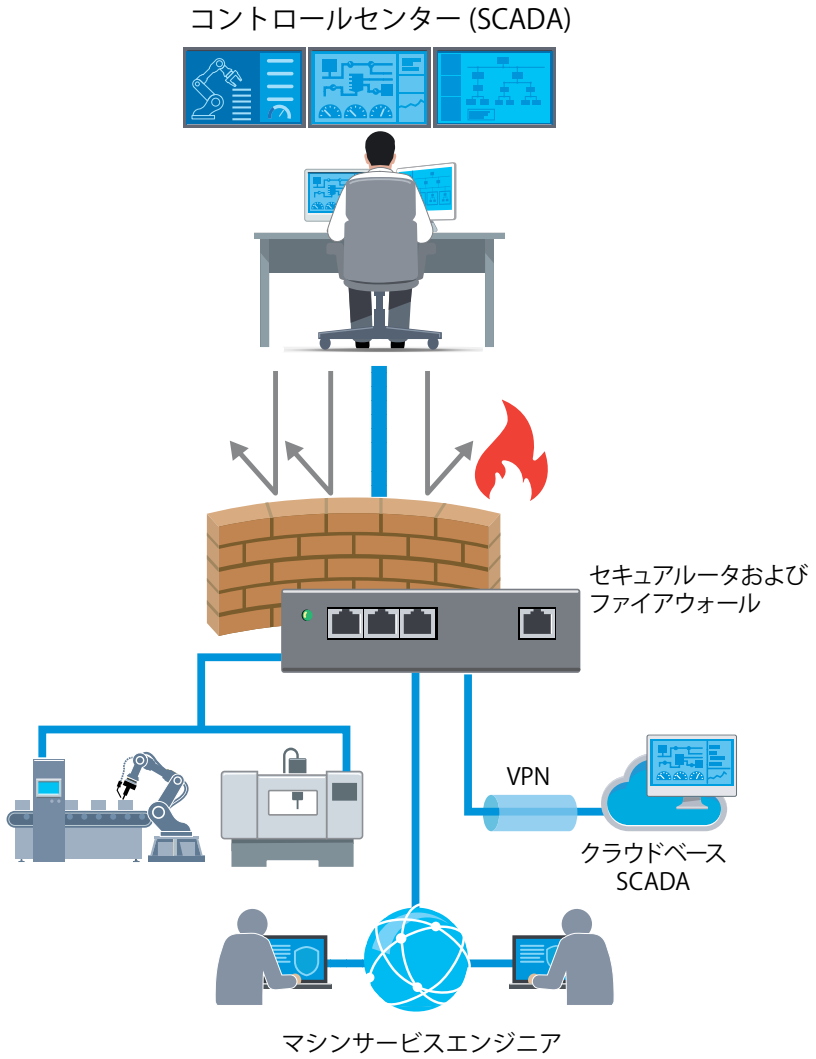
https://www.ibsjapan.co.jp/downloads/gview/kataban:How_to_Choose_the_Right_Industrial_Firewall

White Paper

主要な基準 2

脅威を検出して重要なデータを保護

ファイアウォールは、ゲートキーパーに似ています。残念ながら、意思を持った侵入者がセグメント化されたネットワークのゲートを通過できる可能性があります。そのため、ゲートを通過するトラフィックを常にチェックする必要があります。これを実現するための1つの方法は、必要なときや製造中に安全状態を脅かすとき、産業プロセスを損なう可能性がある書込みコマンドまたはconfigコマンドなどの不要なコマンドをフィルタリングすることです。従って、より詳細なホワイトリスト管理に必要な産業用セキュアルータおよびファイアウォールは、コマンドレベル(読み取り、書き込みなど)で産業プロトコルのフィルタリングをサポートすることが重要です。機密データのセキュアな伝送を実行する場合、サイト間通信のためのセキュアトンネルの構築を検討することもできます。いくつかのシナリオでは、パブリックネットワークまたは信頼がおけないネットワークを介した通信では、セキュアな暗号化されたデータ伝送が必ず必要になります。このような状況下では、産業用セキュアルータおよびファイアウォールを選定するときにVPN機能を検討することができます。



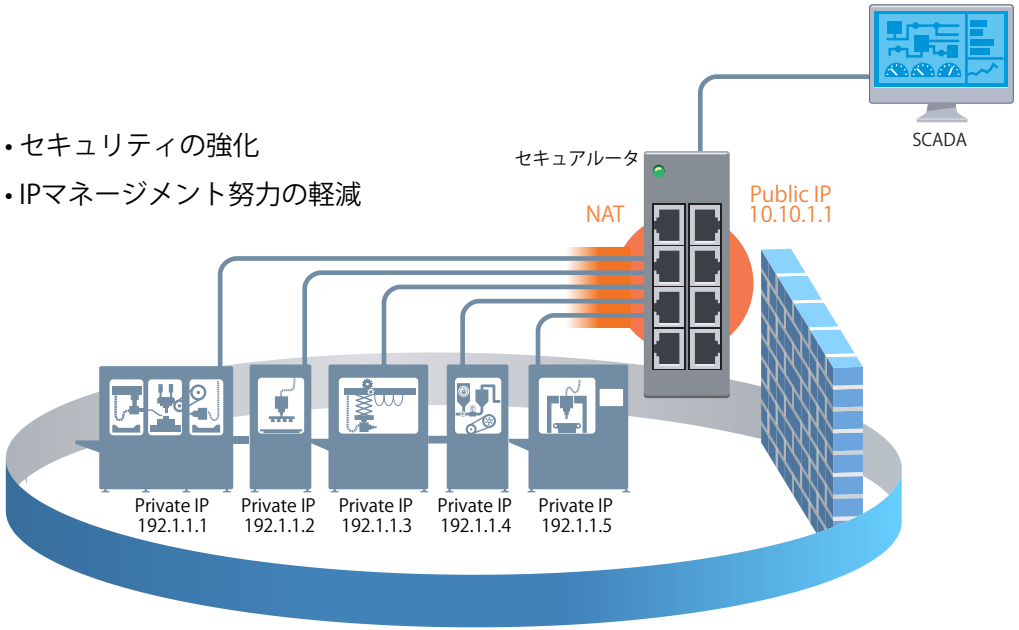
主要な基準 3

ファイアウォールおよびネットワークの管理

産業用アプリケーションにおいて、データトラフィックの管理およびフィールド機器を悪意のある攻撃から保護するために数百または数千のファイアウォールがインストールされます。ネットワーク上には、さらに多くのIPアドレスが存在します。ネットワークが拡大し続けるにつれて、すべてのデバイス、ファイアウォールルール、およびIPアドレスの管理が複雑になります。従って、Network Address Translation (NAT)は、産業用セキュアルータおよびファイアウォールを導入するときに非常に重要な機能を提供します。NATを使用すると同じネットワーク上でマシンのIPアドレススキームを再利用し、少ないIPアドレスを使用して複数なデバイスをインターネットに接続できます。これによりメンテナンス作業と管理のオーバーヘッドが大幅に削減されるだけでなくシンプルなネットワークセグメンテーションも提供します。さらに、内部アドレス指定を外部ネットワークから非公開に保つことによりプライベートネットワークのセキュリティを強化します。

アプリケーションに適したセキュアルータまたはファイアウォールを見つけることは、産業用ネットワークのセキュリティの強化を半分、無事に乗り切ったと言えます。これら3つの基準を使用して選択をすると、当てずっぽうのいくつかを取り除くことができます。例えば、Moxa　EDR-810シリーズなどの、ファイアウォール/NAT/VPNをサポートするマネージドLayer　2スイッチ機能を備えた高度に統合された産業用マルチポートセキュアルータは、必要とする、すべてを提供することができます。それにもかかわらず、最終的に選択するソリューションは、すべて特定のアプリケーション要件に適合する必要があります。

- セキュリティの強化
- IPマネージメント努力の軽減



“ネットワークセグメンテーションおよびトラフィックフィルタリングは、セキュアな産業用ネットワークを構築するための基本です“

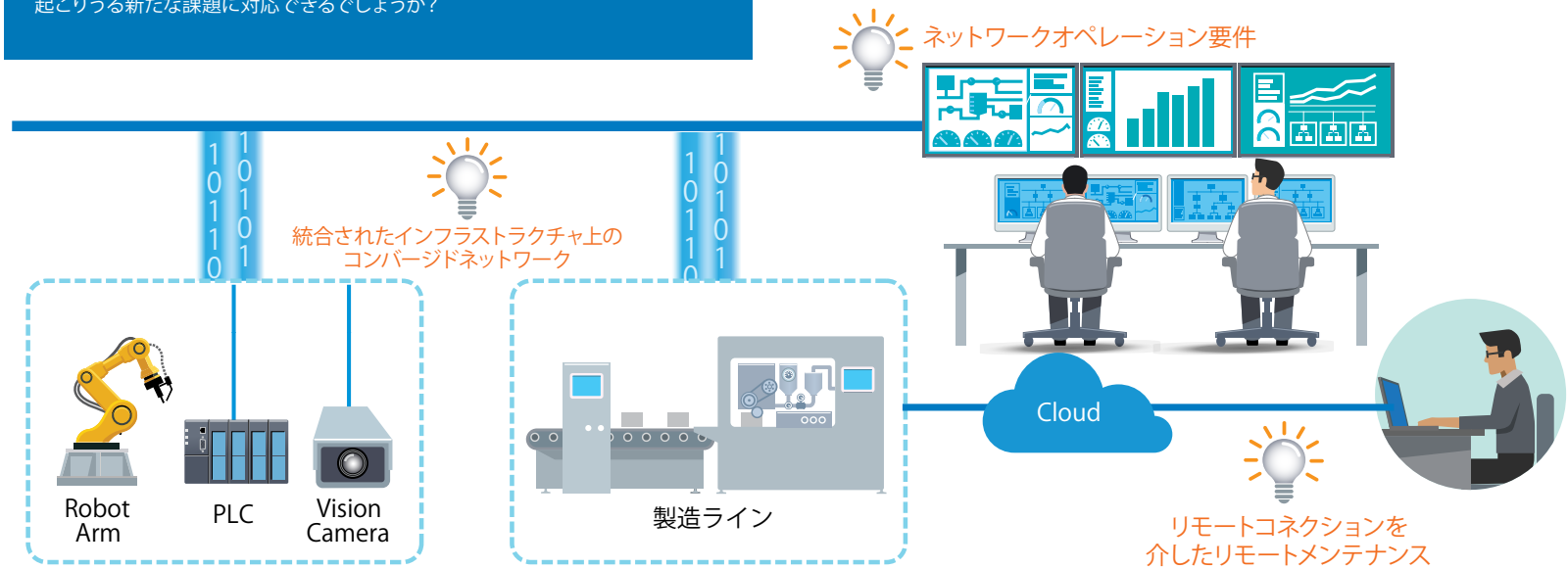
将来の予期せぬ事態を見据えたネットワークの構築

IIoTネットワークを構築し稼働させれば、その成功に満足してしまい、それ以上の変化を考えなくなります。人生も同じです。安定した人生を変化させたくありません。これは、産業用ネットワークの世界も例外ではありません。現在のIIoTネットワークは、現在のニーズに対して十分であるかもしれませんが、今後数年間において予測可能なアプリケーション要件に対応できる可能性もあります。しかし、今後の10年間は、どうでしょうか。それは、COVID-19パンデミックが、そのすべてを変化させてしまったことから証明できます。事前の準備を怠ると予期せぬ事態が発生することにより致命的な結果を生み出します。

Key Question

新しい要求に遭遇しても機敏性に対応することは、絶えず変化する世界で競争上の優位性を維持するための重要な基準になります。 IIoTネットワークは、将来起こりうる新たな課題に対応できるでしょうか？

産業オートメーションの初期の頃からマニファクチュアラーは、高度に専門化された産業用コントロールアプリケーションのために現在の標準のイーサネット技術ではない、様々な目的で作成された専用のプロトコルとシステムを導入してきました。しかしながら、IIoT市場は、当初、2023年までに24.0% 1のCAGRで成長すると予想されるため（コロナの影響により予想が異なる可能性があります）、将来の産業用ネットワークは、相互接続されたデバイス間で大量のデータの伝送やリモートデバイスからデータを収集する機能が必要になるでしょう。また、予期せぬ需要の高まりにより産業用ネットワーキングの将来を見据えて、どれだけの準備ができているかにより、新しい課題への取り組みに対する成功が決定されるかもしれません。このセクションでは、IIoT対応の産業用ネットワークを将来に向けて準備する際に必要とする3つの考慮事項について説明します。



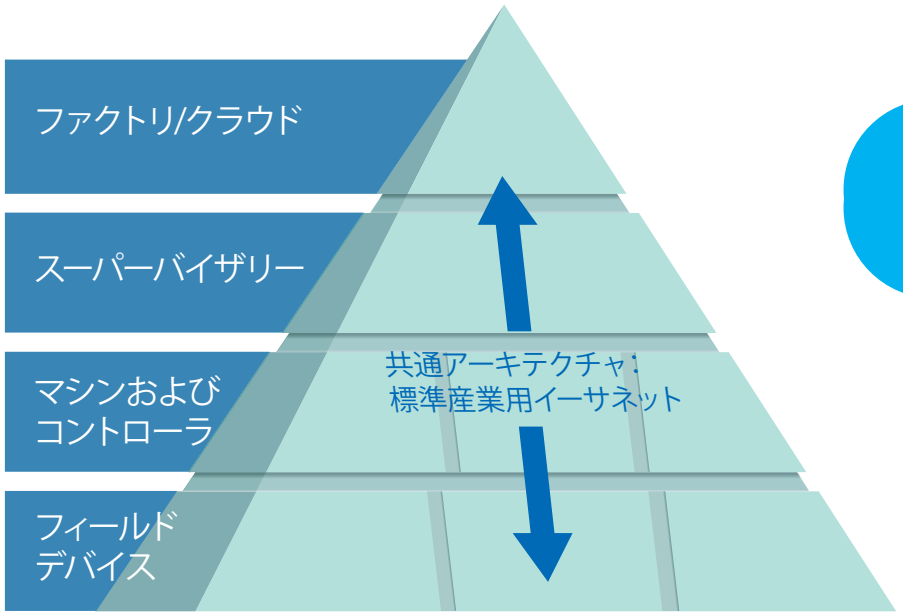
1. The Industrial Internet of Things Market Forecast, MarketWatch, March 2019

じっくり考えること 1

統合されたインフラストラクチャとのより優れた統合を実現

長年にわたり、異なる産業プロトコルを使用する様々なデバイスが産業ネットワークに導入され、多様なサービスを提供してきました。このような状況下でネットワーク統合は、通常、予想以上にコストがかかると共に実現が難しくなります。マニファクチュアラーは、現状を選択するか、つまり、過去の専用の多数のプロトコルを使用して既存の分離されたオートメーションネットワークを維持するか、または、deterministic（時間確定性）サービスを提供して産業用通信プロトコル、ネットワーク技術、システムが相互に通信できない、これらの"islands of automation"「自動化のアイランド」を統合するためのソリューションを模索することができます。

目標が将来的にIIoTネットワークへの高まる需要に備える準備ができている場合、選択すべきことは、明らかに「自動化のアイランド」を統合するためのソリューションである後者です。大ざっぱなやり方であるrule of thumbは、潜在的な産業プロトコルを考慮に入れ市場で新しい需要が発生した場合に備えてネットワークを再設計できるようにします。標準のイーサネットを拡張し産業用ネットワークとITネットワークをシームレスに統合するネットワークテクノロジーであるTime-sensitive networking（TSN）は、IEEE 802.1 TSN Task Groupによって高度なツールボックスとして導入された新しい規格です。TSNを使用すると将来の柔軟性を確保する標準のイーサネットテクノロジーを使用してオープンな統合ネットワークを構築できます。さらに、この新しいテクノロジーを支持する主要なプレーヤがTSNプラグフェストに積極的に参加してエコシステムを完成させ、異なるベンダ間の互換性を確保するためソリューションを選択することが考えられます。



"Time-Sensitive Networking（TSN）が
産業オートメーションに革命をもたらす"
と題するWhite Paperをご覧ください。
https://www.ibsjapan.co.jp/downloads/
gview/kataban:how-time-sensitive-networking
-is-revolutionizing-industrial-automation-white-paper

White Paper

じっくり考えること 2

簡単なクラウドサービスでリモートマシンにどこからでもアクセス

クラウドベースのリモートアクセスは、メンテナンスエンジニアを複数のリモートサイトに派遣するために要する移動時間と経費の削減などIIoTカスタマに多くの利点を提供します。さらに、クラウドベースのセキュアリモートアクセスは、柔軟でスケーラブルなコネクションを提供し、将来の動的で変化する要件を満たすことができます。しかし、例えば、上下水道処理プラント、マシンマニファクチュアラー、およびその他のIIoTカスタマのOTエンジニアにとって、新しいサービスとアプリケーションを提供するために独自のクラウドサーバのセットアップおよび維持が煩雑となります。確かに、例えクラウド内であっても新しいインフラストラクチャのセットアップにはかなりの労力が必要となります。幸いなことに、現在、OEMおよびマシンビルダは、独自のクラウドサーバを維持する必要がなくセキュアなクラウドベースのサービスとリモートアクセスをカスタマに提供できるようになりました。

間違いなく精査すべき重要な問題の1つは、クラウドサーバライセンススキームがあります。多くの場合、初期費用は、限られたサーバホストでは低く見えるかもしれません。しかしながら、サーバホストのこれらの明らかなコスト削減は、コネクションの規模が限られているため、実際にはプロジェクトを不経済にする可能性があります。次に、将来的にリモートコネクションを柔軟に拡張するために集中マネージメント機能を検討する必要があります。　これを踏まえて、産業用ネットワークへのセキュアなリモートアクセスを組み込むことへのコストと利点を慎重に比較検討します。言及されている煩雑さを解消し、カスタマにより多くの価値とベネフィットを提供することに集中できるソリューションを常に選択する必要があります。

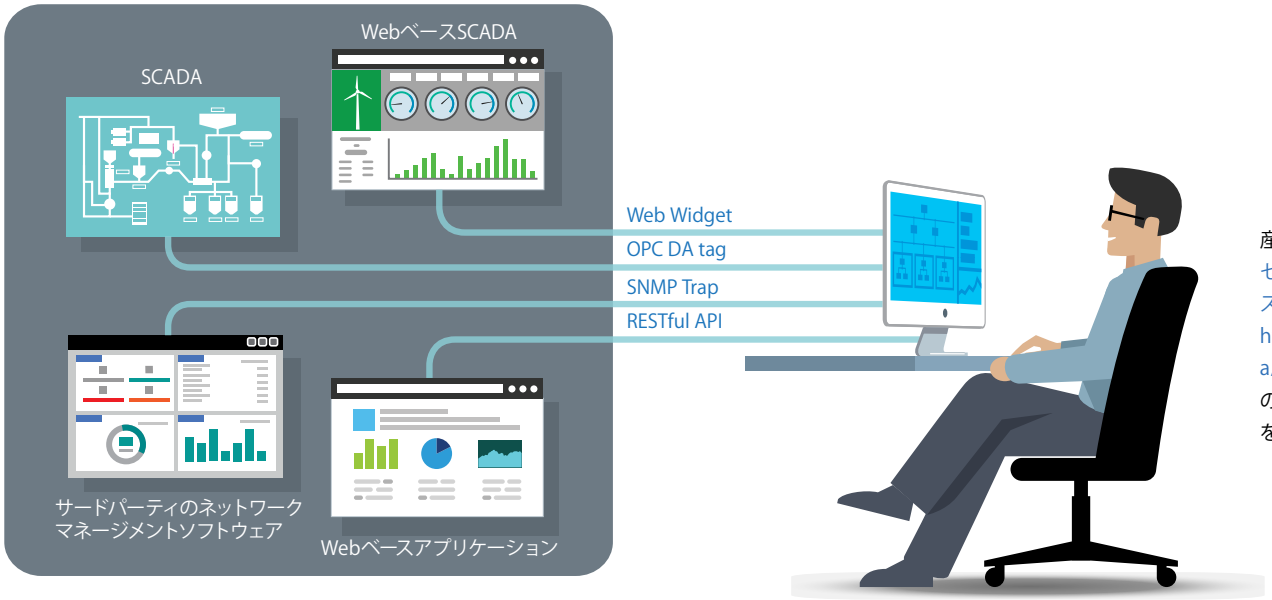
詳細は、こちらのWebサイト“リモートマシンへの容易なアクセスを実現”をご覧ください。
https://www.ibsjapan.co.jp/tech/moxa/moxa-tech-0710.html

じっくり考えること 3

OT と IT プロフェッショナルの両方のネットワークステータスを見える化する

テレビの報道特集などで鉄道運用システムのコントロールルームを見たことがあると思いますが、コントロールルームは、列車の運行を集中的に監視し、運行状況の的確な把握と迅速で確実な指令業務を実現します。オペレータは、現在のステータスを迅速に判断し、コントロールルームのスクリーンに集約された情報に従ってアクションを実行します。このような見える化により、すべてが管理しやすくなります。産業用ネットワークのコネクティビティが増大し、複雑さが増すと、問題の根本原因を特定し、十分なネットワークの見えるかを維持することが非常に困難になります。コントロールエンジニアは、システムを通常の状態に戻すために試行錯誤を繰り返す必要があり、これは時間と煩雑さが増します。

このため成長する産業用ネットワークの促進および管理をするためにネットワークオペレータは、ネットワークの導入、メンテナンス、診断全体を通じてより多くの情報に基づいた意思決定を行うための統合ネットワークマネージメントソフトウェアを必要とします。さらに、システムが成長し続けるにつれて、ネットワーク統合に関する多くの問題に注意を払う必要があります。まず、特に既存のシステムを新しいシステムと統合する必要がある場合、ローカルコントロールセンタで産業用ネットワークを管理するだけでは、3～5年後に実現が困難になる可能性があります。従って、SCADAシステム統合のためのOPC DAタグや外部Webサービスのための RESTful APIといった統合インターフェースを備えたネットワークマネージメントソフトウェアを使用することが重要です。さらに、サードパーティソフトウェアの統合を容易にするインターフェースも、将来の柔軟性を確保するための重要な基準となります。



産業ネットワークの先駆者としてMoxaは、セキュアなクラウドベースのリモートアクセスやネットワークマネージメントツール（https://www.ibsjapan.co.jp/tech/mox-a/moxa-tech-0665.html）といった、多くの革新的なテクノロジーとソリューションを提供しています。

“将来を見据えたIIoTネットワークには、統一されたネットワークインフラストラクチャ、多くのリモートアクセスアプリケーションを処理する機能、使いやすいパワーフルなマネージメントツールが必要です”

結論

IIoTは、多くの業界における機会と同じくらい多くの課題を提示します。それにもかかわらず、従来のOTとITサイロが収束する産業オートメーションにおけるこの未知のフロンティアは、明らかに未来の考え方と言えます。IIoT アプリケーションの導入を成功させるには、この新たな考え方を歩み始めた瞬間から細部まで慎重な計画と注意が必要です。デバイスのコネクティビティを実現することから、現在および将来のネットワーキングのニーズが満たすまで、このガイドブックでディスカスされた重要な要素が、IIoTトランスフォーメーションへの道を歩み始める際に勇気づけられることを願っています。結局のところコネクティングワールドは、私たちのDNAの一部であるのです。

業界で30年以上の経験を有するMoxaは、シリアルコネクティビティ、リモートI/Oコネクティビティ、IIoTデバイスコネクティビティを提供する数多くのソリューションを提供し、信頼できるレガシーデバイスとマシナリーのデバイスコネクティビティを実現してきました。また、マネージドスイッチおよびアンマネージドイーサネットスイッチ、ワイヤレス LAN テクノロジー、セキュアルータとファイアウォール、将来を見据えたネットワーキングソリューションを幅広く提供し、すべての新しいコネクテッドOT資産のための複数の相互接続されたデバイス、システム、さらにはリモートサイト間の情報フローをサポートします。Moxaは、IIoTアプリケーションのどんな迷路が存在するにしても、それがどこに繋がるにしても、あらゆる段階ですべてカスタマをサポートすることができます。

Your Trusted Partner in Automation

Moxa は産業オートメーション構築のための信頼できるパートナーです

IIoTは、多くの業界における機会と同じくらい多くの課題を提示します。それにもかかわらず、従来のOTとITサイロが収束する産業オートメーションにおけるこの未知のフロンティアは、明らかに未来の考え方と言えます。IIoT アプリケーションの導入を成功させるには、この新たな考え方を歩み始めた瞬間から細部まで慎重な計画と注意が必要です。デバイスのコネクティビティを実現することから、現在および将来のネットワーキングのニーズが満たすまで、このガイドブックでディスカスされた重要な要素が、IIoTトランスフォーメーションへの道を歩み始める際に勇気づけられることを願っています。 結局のところコネクティングワールドは、私たちのDNAの一部であるのです。

業界で30年以上の経験を有するMoxaは、シリアルコネクティビティ、リモートI/Oコネクティビティ、IIoTデバイスコネクティビティを提供する数多くのソリューションを提供し、信頼できるレガシーデバイスとマシナリーのデバイスコネクティビティを実現してきました。また、マネージドスイッチおよびアンマネージドイーサネットスイッチ、ワイヤレス LAN テクノロジー、セキュアルータとファイアウォール、将来を見据えたネットワーキングソリューションを幅広く提供し、すべての新しいコネクテッドOT資産のための複数の相互接続されたデバイス、システム、さらにはリモートサイト間の情報フローをサポートします。Moxaは、IIoTアプリケーションのどんな迷路が存在するにしても、それがどこに繋がるにしても、あらゆる段階ですべてカスタマをサポートすることができます。

■ アイ・ビー・エス・ジャパン株式会社はMoxaの日本正規代理店です。
■ カタログ・資料請求・お問い合わせは info@ibsjapan.co.jp まで。

IBS Japan
アイ・ビー・エス・ジャパン株式会社

https://www.ibsjapan.co.jp/
E-mail：info@ibsjapan.co.jp
営業時間（土日・祝日を除く）9:00～17:30

■ 厚木センター
〒243-0432　神奈川県海老名市中央2-9-50 海老名プライムタワー12F
TEL 046-234-9200　FAX 046-234-7861

■ 東京システムセンター
〒151-0053　東京都渋谷区代々木2-4-9 NMF新宿南口ビル2F
TEL 03-5308-1177　FAX 03-5308-1188

■ 大阪営業所
〒532-0003　大阪府大阪市淀川区宮原1-2-6 新大阪橋本ビル4F
TEL 06-7176-9191　FAX 06-7176-9192

IBS-202008Moxa