シリーズ

スマートマニュファクチュアリングの実践

ケース：工作機械を核とする加工プロセスの生産性向上

ロボット革命イニシアティブ協議会

IoT による製造ビジネス変革ＷＧ

産業機械サブ幹事会

平成２８年４月

目次

１．スマートマニュファクチュアリングの実践とは何か

２．工作機械を核とする加工プロセス生産性の向上

３．検討方法

４．対象とするサービスの概略と課題
（１）遠隔による予知保全・メンテナンス・操業支援サービス
（２）普及にあたり直面している課題

５．遠隔による予知保全・メンテナンス・操業支援サービスに係る情報モデル
（１）工作機械に関する情報モデルの整理
（２）各サービスに関する情報モデルの整理

６．情報モデルから抽出されるサービス展開のためのガイドライン試案
（１）工作機械の基本的な状態に関する定義と、状態に関する情報を取得する方法に関するガイドライン／インターフェースの整理
（２）工作機械をインターネットに接続するに当たっての情報セキュリティ対策に関する基本的な考え方
－技術的側面
－技術的接続方法の例示
－ユーザー及びサービスプロバイダーにおいて構築すべき情報管理体制・ルール
（３）工作機械から生成するデジタルデータに係るアクセス・コントロールに関するガイドライン

７．本サービスに係る情報モデルを活用したスマート工場の提案

１．スマートマニュファクチュアリングの実践とは何か

現在、IoT、ビッグデータ、人工知能等の新たな情報技術が、経済社会の様々な分野に大きな変化をもたらしており、製造業にも「第四次産業革命」とも呼ぶべき変革が訪れようとしている。

もとより、製造業においては、これまでも、情報化、知能化と呼ばれる生産プロセスの革新がなされてきた。中でも、加工プロセス（工作機械にワークをセットし、工場ライン内において、最終的に加工されるまでのプロセス）においては、高精度化、高効率化を追求する中で、デジタル制御技術を駆使した制御システムが高度に発展を遂げている。このような制御システムにおいては、加工対象であるワークの状態に関する情報、加工を担う工作機械の状態に関する情報などの多種大量のデータが生成・処理されている。

これらの情報は、第四次産業革命の文脈においては、加工プロセスの高精度化、高効率化という一義的な目的を超えて、他の異なるシステムから生まれる情報との相乗効果を伴いつつ、新たな価値創造の源泉になっていく。その点に、非連続的変化、「革命」と称しうる所以がある。すなわち、受注から製品出荷に至るサプライチェーンを管理する視点でみれば、加工プロセスの進捗状況や、工作機械等関連設備の稼働状況を示す情報となり、生産計画の全体最適化の実現へと連なっていく。また、工作機械等の正常な稼働を管理する視点でみれば、機械の稼働の健全性を検証し、また、故障等につながる予兆を捉える基礎に活用することができる。さらに、工作機械メーカーが、多様な使用状況に置かれる工作機械等の稼働時の情報を長期にわたり蓄積し、その大量のデータを分析・利用することができたならば、工作機械の開発に活かし性能向上に繋げられるほか、その機能を最大限発揮させるための操作ノウハウを洗練させることにも繋がり、そのようにして培われた操作のノウハウを提供し加工プロセスの高効率化、高精度化を支援するサービス事業へと展開することも可能となるだろう。スマート化された加工プロセスが、既存産業の競争力を高めることはもちろんのこと、新しい産業を創出することも想定できるであろう。

このように、今日、語られる革命的変化は、ものづくりを担う事業者もさることながら、ものづくりを支える産業機械を産み出す事業者にとっても、新しい付加価値を得ていくチャンスとなる。特に、新たな産業革命という動きの中では、情報技術がオープンソースで提供される場面も顕在化しており、進展著しい情報技術の活用は、競争力の確保という視点で欠かせないものになってきている。しかしながら、情報技術を活用し、高付加価値を生むサービスを実施していくために乗り越えるべき壁は低くない。これまで想定せず、むしろ、忌避してきた連携・結合が必要となるからである。経験のない連携・結合に伴う

予期しがたいリスクへの漠然とした不安、情報システムが連携・結合することで必然的に拡大する情報漏えいやセキュリティアタックに係るリスクへの懸念、そもそも連携・結合を想定していなかった情報システムの技術的課題（インターフェース、プロトコル等）などが典型的な壁である。

これらの壁を乗り越え、革命的変化の中で大きな果実を得ていくためには、困難な壁を乗り越えるだけの大きな付加価値を生み出し得る、スマートマニュファクチュアリングの具体例を見いだしてステークホルダー間で共有し、その実践を通じて、壁を乗り越えるための方法論を獲得していくことが有望なアプローチとなる。

ここで、スマートマニュファクチュアリングの特徴を指摘するならば、次の三点を挙げることができよう。

第一に、工場内にある機械の生産技術データを一元的に管理・集約させ、そこから得られるデータを情報処理し、機械の加工効率の改善、予知保全、現場のカイゼン等のために有用に加工されたデータとして、生産管理側である ERP、MES 等の上位システムに提供される仕組みが構築されていること。

第二に、情報処理された生産技術データを機械にフィードバックさせることにより、プロセスごとの部分最適を人が積み上げていくという従来の取組を超えて、人を介さずともライン全体が最適化される仕組みが構築されていること。

第三に、生産技術であるエンジニアリングチェーンと生産管理であるサプライチェーン（生産管理）の全体を可視化し、場合によっては人工知能を活用することにより、統合的に管理し、現場をサイバーフィジカルなシステムとして捉え、その全体最適につながるカイゼンを達成できる仕組みが構築されていること。

スマートマニュファクチュアリングの本質ともいえる連携・結合においては、全体最適化を行うコンダクターの指揮の下、複数の異なる主体の協働作業が必要である。他方、協働作業から生まれる新たな価値は、特定のプレイヤーのみに帰属するものではなく、連携し結合される多くのステークホルダーに幅広く行き渡る。このような構造を生み出し、win-win の関係を実現していく上でまずもって重要となることは、スマートマニュファクチュアリングの実践が、幅広いステークホルダーに共有できる形で提示され、メリットや、リスク、リスクを管理する手法等が正しく理解されて、幅広い主体が参加できるようにすることである。さらに何よりも、スマートマニュファクチュアリングを活用した事業者が、顧客に最高の製品、サービスなどのソリューションが提供できていることを実証し、その収益を多くのステークホルダーによって享受されることが重要である。

「シリーズ：スマートマニュファクチュアリングの実践」は、革命の担い手

を標榜する第一線の実務家が、このような考え方を共有して行う、世界に向けた日本からの発信である。

２．工作機械を核とする加工プロセス生産性の向上

スマートマニュファクチュアリングの実践に関する第一の取組として、工作機械を核とする加工プロセス生産性の向上に着目し、検討する。

製造業の高度化が、生産プロセスの機械化により実現されてきたという意味で、産業機械メーカーは製造業の進化に大きく貢献してきた。今後、製造業の高付加価値化を目指す新興国においても、先進国同様、高度な産業機械を実装し、高付加価値化を目指す動きが広がって行くものと考えられる。

生産プロセスの中でも特に加工プロセスは、工作機械の操縦の巧拙による差が大きく、段取り、保守点検などの要素を含めた総合的なノウハウによって、その生産性や付加価値が大きく左右される。したがって、加工プロセスを高度化する上では、とりわけ、工作機械メーカーの貢献できる余地が大きい。すなわち、工作機械メーカーには、工作機械を提供するとともに、その効果的な活用ノウハウ等を併せて提供する「マニュファクチュアリングサービスプロバイダー」として貢献するという、新たな市場が広がっているといえる。

そこで、IoT、AI といった最新の技術を活かすことを前提に、加工プロセスの生産性を向上させるための具体的なサービスを特定し、スマートマニュファクチュアリングの実践となるユースケースとして、広く共有できるものとして整理し提示することとする。

３．検討方法

実際のビジネスに即した実践とするべく、工作機械メーカーを中心に、ユーザーを含めた第一線の実務者メンバーが検討チームを組織し（36 ページ参照）、以下の手順で検討を進めた。

① 加工プロセスに関する顧客ニーズを踏まえ、参加メンバーが、スマートマニュファクチュアリングの実践として取り組む具体的なサービス内容を文書により整理。合議の上、対象とするサービス内容を特定。
② ①で特定したサービスに関し、参加メンバーが実施、又は実施に向けて検討している内容について、相互比較可能となるよう、共通の方式により、情報モデルとして記述（本ケースでは OMG の SysML を使用）。
③ 情報モデル化された参加メンバーのサービス内容を比較検討し、共通項を

抽出することで、当該サービスの基本構造を情報モデルとして確定。

④ ③で特定した情報モデルに基づき、当該サービスを実施する上で必要となる、他のシステムとの連携・結合のあり方等を検証し、インターフェース等共通化を要する部分や、セキュリティ、データのコントロール主体など、ルール化すべき部分を特定、整理。

4．対象とするサービスの概略と課題

（1） 遠隔による予知保全・メンテナンス・操業支援サービス

加工プロセスの生産性を向上させるためには、ワークの搬送や段取り換えを最小化するための工作機械の多機能化を進めるとともに（単一工作機械における制御軸数、利用工具数の増加等）、トラブルによる稼働率低下を極力なくすことが必要となる。

このうち、後者については、工作機械メーカー各社が 2000 年頃から注力しており、工作機械をネットワークに接続し、メーカーのサービス拠点から遠隔で稼働状況を把握・監視するなどのサービスが提供されてきている。

大手メーカーを中心に提供されている典型的な予知保全・メンテナンス等のサービスは、ユーザーが使用する工作機械を携帯電話網やインターネットを経由してメーカーのサービス拠点に接続し、メーカーが、当該工作機械のその時点の稼働状況や過去のログ情報等を遠隔で収集して、ユーザーに対する助言や遠隔からの改修を実施するものである。メーカーがユーザーからの連絡を受けてサービス拠点から現地に赴き状況確認を行う場合に比べ、トラブル原因等を迅速に特定し対処することができるほか、メーカー側で蓄積されている工作機械の挙動に関する各種データ等を活用することで、トラブルの予兆を察知して予防策を打つこともでき、従来よりもきめ細やかに対応することが可能となっている。これにより、ユーザーは、加工プロセス（機械単体）のダウンタイムを減少させ、生産性を向上させることができる。

また、工作機械の稼動状況がデータ化され、蓄積、分析できるようになるならば、トラブルへの対応を超えて、操業の巧拙が把握できるようになる。メーカーは、それに基づき、ユーザーに対し、より、高付加価値な加工プロセスとするための操業支援へとサービスを拡張することが可能となる。

加えて、工作機械の稼動状況に関するデータが、遠隔で把握可能な程度にまで収集・整理されているならば、当該データは、工場全体の生産管理や、それを含めたサプライチェーンの管理、最適化に活かすことも可能となる。

以上のような加工プロセスに係る生産性の向上のためのサービスを、遠隔による予知保全・メンテナンス・操業支援サービスとして整理する。

なお、予知保全・メンテナンス・操業支援サービスの実施形態については、一定の幅のあるものを想定することができる。

例えば、稼動状況のモニタリングの方式としては、稼働状況を示す多様なセンシングデータをリアルタイムに近い頻度で遠隔で取得する方法、対応策が必要となる異常停止等の定形事象発生のシグナルのみを自動的に遠隔で取得する方法、当該事象が発生した場合にその事実と併せて関連するセンシングデータのログ情報を自動的に遠隔で取得する方法、事象発生後に遠隔操作によって必要なデータをメーカーが探索し取得する方法などが想定される。

また、メンテナンス等の実施方法としても、あくまでもユーザー等が工作機械等の実装されている現場において行う方法のほか、一般的な操作手順やパラメータの範囲内で対応できる場合であればメーカー等がインターネットを経由し遠隔で直接手当するという方法、プログラムレベルでの不具合を解消するために遠隔で改良プログラムを作成し送り込みシステムバージョンアップを行う方法なども想定される。

稼働状況のモニタリングと、メンテナンス等の実施方法との組み合わせだけでも、相当程度の多様な形態を想定することができる。このため、以下においては、可能な限り、このように幅のあるサービス形態を包摂する議論を目指しつつも、情報セキュリティ対策など、サービスの形態によって、大きな相違が生じる論点もあることから、メンテナンス等の実施方法としては、ユーザー等が工作機械等の実装されている現場において対応するという方法を原則として、議論を進めていくこととする。このような取扱とする理由は、目下、ユーザーが求めているメンテナンス等の実施方法に即したものであることにある。無論、今後の市場の広がりとしては、多様な形態があり得ることから、他の形態を検討対象から排除するものではなく、今後の検討課題とするものであることを付言する。

（２）　普及にあたり直面している課題

工作機械大手メーカー各社は、（１）に示したサービスの一部をそれぞれ提供しているが、現状において、必ずしも広くユーザーに受け入れられていない。これは、サービス提供を行おうとするメーカーのみならず、新たなサービスの活用により加工プロセスの高度化が図られるはずのユーザーにとっても、有用な機会を逸するものといえる。

普及に当たり直面している主たる課題として、以下を挙げることができる。

①　ネットワーク接続に起因するリスクの懸念

多くのユーザーは、加工プロセスで用いる工作機械等の情報システムが、自社外にまでつながるネットワークに接続されることにより、大きなリスクを呼び込むと認識している。例えば、悪意あるハッカーやコンピュータ・ウィルス感染によって、生産ラインの長時間に渡る停止、人命に関わる誤作動によるリスクが指摘される。また、加工プロセスで用いる工作機械等の稼動状況に関するデータは、加工プロセスの能力を端的に示すとして機密性の高いものと認識されており、情報漏洩によって大きな経済的損失が生じる可能性がしばしば懸念される。

第四次産業革命をもたらす最大の技術要素が情報ネットワーク技術であり、ネットワーク接続を前提にリスクを想定し適切に管理することが必要となるが、ネットワーク接続を前提としたサービスの構造についての理解や、リスク管理手法に関する定見が共有されていない結果、サービスの活用に逡巡するユーザーが多いものと想定される。IoT を活かしたサービスを展開するには、こうしたユーザーの不安を払拭できるような情報セキュリティ面での対応が必要となる。

② 異なるメーカーの機械を通じたサービス提供の困難性

ユーザーの生産現場（生産ライン）では、一般的に複数のメーカーの機械が導入されている。ネットワーク接続を前提としたサービスの利点を活かすならば、生産ラインを構成する様々なメーカー製の工作機械等の挙動を一括して把握できることが望ましい。メーカー毎に保守・予知保全メンテナンスサービスを受けることができたとしても、そのサービスの内容や、①で示したリスク管理のための処方に少なからぬ差があった場合、工場全体の最適化への効果には限界があり、ユーザーにとってのメリットが乏しいものとなる。

現状、各社メーカーが一体となってサービスを実施できるような連携体制が整っておらず、これを実現するためには、データの質・量やデータ連携の頻度、粒度、通信プロトコル等、各社の協調領域を定めることが必要となる。

③ データの蓄積・分析を基礎としたサービス展開の困難性

現在、メーカー各社が提供するサービスは、単一の工作機械等を対象に、トラブル対応などユーザーが求める問題解決に要する範囲で、断片的に稼働状況に関するデータやログデータ等を得て提供されるものとなっている。（１）で概略を示したとおり、スマートマニュファクチュアリングの実践として想定されるサービスの一つとして、ユーザーの元で稼動する機械の挙動について、より多くのデータを把握し深く分析することにより、ユーザーの加工プロセスを更に高度化するための操業支援を行うこととしている。

このようなサービスを具体化するためには、工作機械に関するデータの利用範囲に関する取決めや、データの蓄積・管理に関する責任関係の整理など、データを巡る考え方の整理を行い、広くステークホルダーが共通の認識をもって連携できることが必要であるが、現状、そのような整理ができていない。

④ 投資対効果におけるサービスメリットの不明確性

経営者（ユーザー）にとって、サービス導入により、どのようなサービスが実現できるか、それに伴いどのような効果が得られるか等、投資判断に結びつく効果の予測が難しい。この点、有効に活用できるサービスであることを明確に示し、経営判断の重要な参考材料によあるものとして周知していくことが必要である。また、スマートマニュファクチュアリングの実践を通じて、効果あるサービスの創造と提案を実施していくことが必要である。

⑤ ネットワーク、セキュリティに関する技術者の不足

これまで、工作機械メーカーやラインビルダーによって、機械、ロボット等のシステムインテグレートがなされてきたが、スマートマニュファクチュアリングの実践においては、これに加え、IT 機器やネットワークを加えたシステムインテグレーションが必要となる。しかしながら、工作機械メーカー内に、ネットワーク、セキュリティ関連の技術者が現状、不足しており、ソリューションを提案する際に、ユーザーのサービスへの理解度を高めセキュリティに関する不安を払拭させるまでの技術的なアドバイスを行うことが難しい状況にある。ネットワーク、セキュリティに関する技術者の育成や、システム連携のあり方やルール化すべき部分の特定を進めながらユーザーに分かりやすく提供できるようなガイドライン等が必要である。

（２）で示した課題に共通する点をまとめるならば、ネットワークとデータを駆使するサービスの基本的特性に関する共通認識の不在と、当該サービス特有のルールの未整備である。これらを検証し、解決策を見いだす作業の前提として、次の５．では、（１）のサービスの情報モデルを提示する。また、情報モデルを元に、他のシステムとの連携・結合のあり方等の検証、インターフェース等共通化を要する部分や、セキュリティ、データのコントロール主体など、ルール化すべき部分を特定、整理する。

５．遠隔による予知保全・メンテナンス・操業支援サービスに係る情報モデル

（１）工作機械に関する情報モデルの整理

遠隔保守、予知保全のサービスをユーザーの生産ラインに適用する場合、その生産ラインを構成する工作機械の状態をモニタリングする機能（見える化）は重要な要素となる。特に複数のメーカーの工作機械において共通の見える化を実現するためには、そのハードウェア構成や運用時に内部状態を明確化し、情報システムの設計、実装を行うための情報モデルが必要になる。現在の生産ラインを構成する工作機械には、加工主軸や工作テーブルの旋回軸数、設置場所、さらには各軸の駆動方式によって、様々な構造と動的振舞いが存在し、すべての機能を表す共通モデルを定義することは困難である。また、仮に現在の工作機械に関する共通モデルを定義し、それに基づいて工作機械を設計、製造することとしたならば、将来のすべての製品製造に対応する工作機械のモデルを決めてしまうこととなり、工作機械そのものの発展を損なうことになる。

しかしながら、複数の工作機械を用いて構成された生産ラインのユーザーにとっては、生産ライン全体を均一なレベルで「見える化」することが、生産管理の視点から重要であるのも事実である。そこで、対象となる工作機械をハードウェア構成、機械の動作状態を均一なレベルで認識できるレベルのモデル化を試みる。ここでは、工作機械メーカーのヒアリングをもとに切削加工機械のブロック定義図（静的構造）及び状態機械図（動的構造）のモデル化を行った。

【切削加工機械のブロック定義図】

切削加工機械のハードウェア構成は、加工装置の動作自由度、工具ユニットの数などにより様々な型が存在するが、基本的な構成としては、加工装置を制御する「CNC ユニット(図中「:NC」と表記する。)」、補助装置や内部センサーを制御する「PLC ユニット(図中「:PLC」と表記する。)」、ユーザインターフェース及びオフィスフロアとのネットワークインターフェースとなる「工業用 PC(図中「:IPC」と表記する。)」、および「加工ユニット」により構成されている。これらの構成要素の関係を SysML を用いてモデル化すると、図 5.1 のようなブロック定義図で表すことができる。

このように切削加工機械をブロック定義図でモデル化することによって、切削加工機械内のセンサー情報をインターネット(EtherNet)へ配信する場合は、ヒューマン・マシン・インターフェース(図中「:HMI」と表記する。)となる工業用 PC と、バス結合された PLC ユニットとを情報配信の起点とし

てインターネットへ情報が送信され、フィールド・ネットワーク（FA-Net）に接続された生産ラインの他の機器との連携動作は、PLC ユニットのみを介して実行されていることが明確になる。また生産ラインの稼働安全性の確保など共通の課題につき、インターネットに情報を配信する情報システムと、生産ラインを制御する制御システムを、どのように問題なく共存させるかという点についても、具体的な検討を行うことができる。このようなモデル化を行うことで、生産ラインを構成する各工作機械を運用する場合の制御情報、設計情報、センサー情報を取り扱う部分とその接続関係性・アクセス範囲が明確になり、機械の障害発生時の障害要因の特定、他の機械への影響の関係性、各種情報とインターフェースとの関連を取り扱う情報システムの設計に対し有効である。

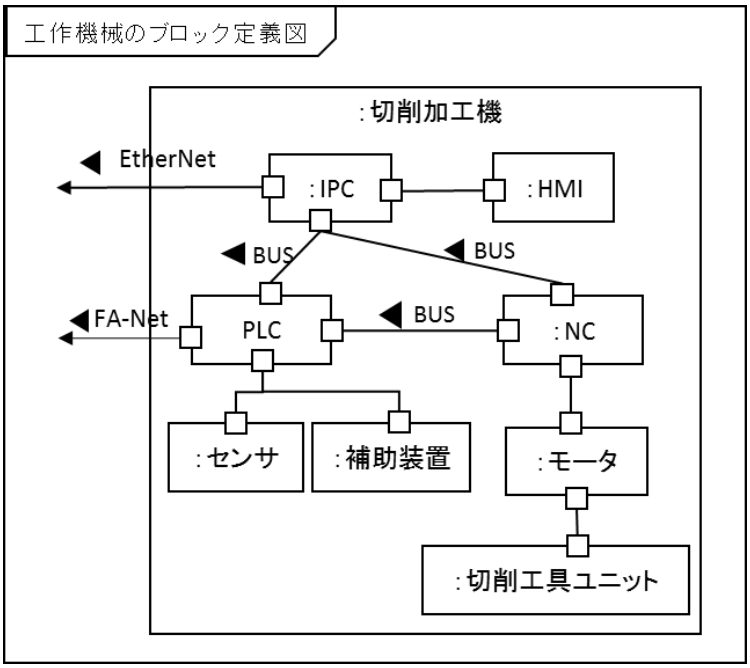

図 5.1　切削加工機械のブロック定義図

【切削加工機械の通常運転時の状態機械図】

前項で述べた切削加工機械のブロック定義図を用いることで、切削加工機械の内部ユニット、各種機能及び取り扱う情報の三者の関係性を記述することが可能になるが、切削加工機械の運用時の情報の発生とその流れが記述されていないため、切削加工機械の状態を「見える化」するための情報システムを開発するためには十分ではない。そのため、切削加工機械の通常運転時のおける状態機械図によりモデル化を行った。

切削加工機械の運用時における状態機械図に関しても前述のブロック定義図と同様に各機械の機能、内部ユニットの構成によって詳細は異なっているが、メーカー企業へのヒアリングの結果、図 5.2 のような共通の状態機械図として記述可能であることが分かった。

ここで表現されている状態遷移は、切削加工機械を工場で動作、運用する場合の動作の流れと状態遷移のタイミングを表すものである。

切削加工機械では、加工運転時の事故の防止や製品（加工目標）の要求精度、そして加工機械の周辺装置、補助装置の準備のために、複数の加工準備状態を持っていることが多い。複数の工作機械により構成された工場、生産ライン、生産セルの継ぎ目のない「見える化」を実現するためには、全体を俯瞰するレベルの情報システムの設計、実装が必要であり、このような共通部分のモデル化は、この実現のために有益である。さらに、メーカー側から個別工作機械に対応した詳細モデル（個別モデル）が提供されるならば、共通モデルと個別モデルとを複合的に用いることで、様々なレベルの「見える化」を行い得る情報システムの設計、実装を容易にすることが可能になるであろう。また、このように各加工機械の動作を共通モデルとして表すことで、警告情報、障害情報を表すメーカー固有の ID の共通化を行うための重要な指針になり得る。

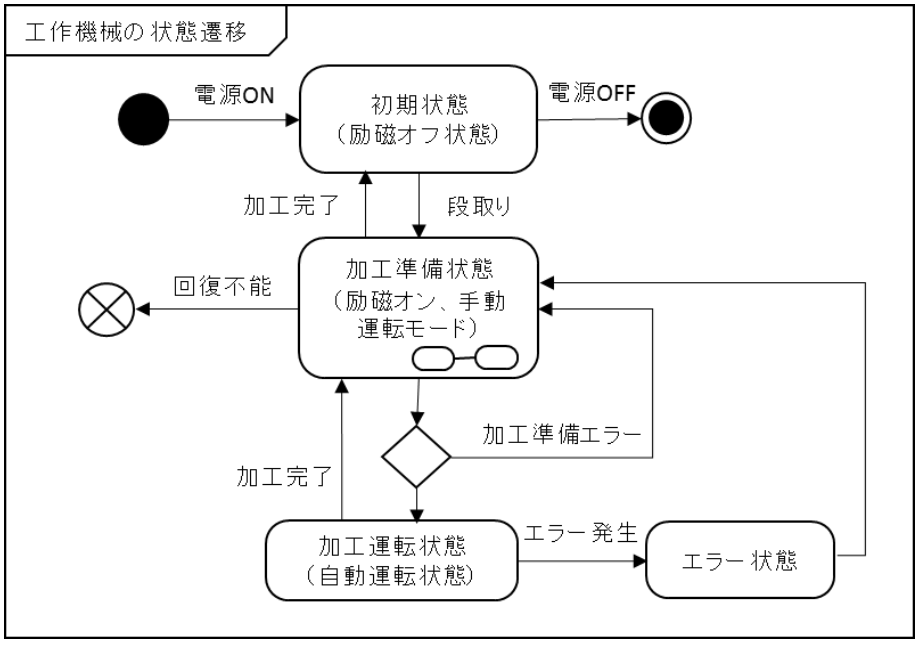

図 5.2 切削加工機械の運用時における状態機械図

（２）　各種サービスに関する情報モデルの整理

① 保守作業のモデル化

工作機械の IoT 化によって既存の生産技術の高度化を進め生産活動の高効率化を実現するには、既存の生産ラインの様々な障害によるダウンタイムの最小化や製造不良の発生などの「ムダ」をなくすことが重要なポイントとなる。生産ラインを構成する工作機械の保守作業の効率化、高度化は、この「ムダ」をなくすための重要な手法の一つである。

現在、多くの工場における生産ラインの保守作業は各工場によって様々な方法で実施されているが、保守作業の「カイゼン」については、現場の運用者（工場の生産技術者、現場管理者等）による暗黙知を利用した個別対応がほとんどである。このような暗黙知による個別対応を核とする生産活動の「カイゼン」においては、人的資源などがボトルネックとなって、早晩、限界を迎えることになる。また、IoT 化が進んだ工作機械、各種情報システム、人工知能（AI）等の技術の活用も難しい。

現在の生産現場における保守作業がこのような限界を克服し、IoT、AI を取り入れて進化し続けるためには、様々な保守作業に人間が介在せざるを得ない状況を転換することを目指し、まずは、保守作業に関する明確なモデル化を行うことが肝要である。そこで、メーカー企業およびユーザー企業からのヒアリングを通じて現在の生産現場における保守作業のモデル化を試みた。

保守作業に関するブロック定義図を図 5.3 に示す。このモデル化からわかることは、保守作業における予知保全及び遠隔保守に関しては、個々の技術の未発達による普及の遅れとそれらの保守作業と人（ユーザー、メーカー企業の各担当者等）との関係に曖昧な部分が存在しているということである。

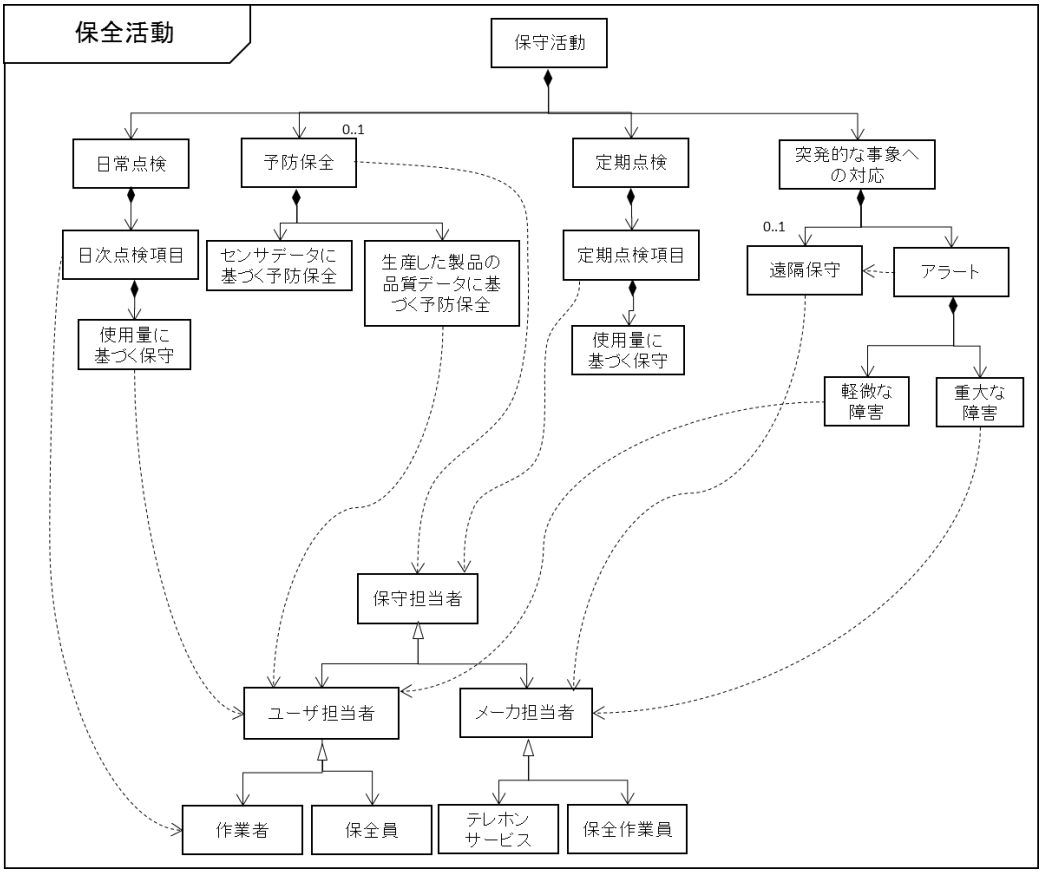

図 5.3 現在の工場における保守作業のブロック定義図

現在の生産ラインの保守作業は、製造する製品および生産体制によって、優先する項目が異なる。例えば、自動車産業における工場のように 24 時間体制で単品種大量生産/多品種少量生産を行う場合には、ゼロダウンタイムを実現するための保守作業を行っている。これに対し、大規模発電システムを構成するユニットのようなインフラ設備の生産ラインに見られる受注個別生産の場合には、生産時間内に生産ラインを停めない（計画保守時間のみ停める）ための保守作業を行っている。また、大企業の場合には、生産ラインを構成する工作機械であれば、どのメーカーの機械であっても、各メーカーの支援を得ずに、ほとんどの保守、修理がこなせる部署を有する工場が珍しくない。これに対し、中小の企業においては、そのような部署を有する余裕はない。

そこで、情報モデルで記述するに当たっては、「保守作業を行う部署の有無の視点」と「生産体制の視点（大量生産、多品種少量生産、受注生産等）」との二つの軸で分類し、さらに、保守作業の内容とその中で人が担う機能を明確に示すことに留意しながら、個別のモデルの作成と要求分析を行う必要があると考えられる。

② 遠隔保守と予知保全のモデル化

①で述べた、現状の保守作業を表す情報モデルを参照しながら、遠隔保守や予知保全として、現状、関係各社により実現されているシステムについて、情報モデルの作成を試みる。

【遠隔保守システム】

現在、工場では、情報セキュリティ対策が十分でないという理由で、有線又は無線LANによるインターネットへの接続はほとんど普及していない。そのため、遠隔保守に対応した工作機械の多くについては、データ通信専用の携帯電話網による公衆回線ネットワークを用いて保守サービスが実施されている。現在、工作機械メーカーにより実施されている遠隔保守システムの典型的なブロック定義図を図 5.4 に示す。

現在の遠隔保守サービスでは、通信回線の容量制限や通信コストの面で問題があるため、常時接続によるリアルタイムのデータ監視を行うことは困難である。このため、工作機械による加工プロセスにおける運転時間と、内部センサーから得られる情報は、あらかじめ工作機械内に設置されたハードディスク等の記憶装置に蓄積され、そのデータを、定期的に、メーカー企業で管理されているデータベースにアップロードするという構成がとられている。通常、不具合が発生しアラームが発報された時点で、そのアラーム種別等に関する情報がメーカーに自動送信される仕様となっており、メーカーは、定期的にアップロードしてきた動作履歴等のデータを用いて、アラーム種別に対応する不具合箇所の初期解析を行う。

この際、サーバーに定期的に蓄積されてきた動作履歴等のデータは、アラーム発生時の不具合箇所の初期解析にのみに利用制限されている場合が多い。これは、４．（２）でも言及した通り、ユーザーにとって、工作機械の動作履歴等の情報は、生産技術のノウハウそのものであるという認識があるためである。これにより、「様々なユーザーから収集したされた大量のデータを解析しこれを用いて付加価値の高い遠隔サービスを開発していく」という工作機械メーカーのサービス展開が阻害されている。しかしながら、実のところ、このモデル化によって明らかにされているように、蓄積される動作データは、工作機械の動きのみを取り扱っており、それのみでは加工プロセス全体を復元することは不可能である。遠隔保守のために取得されているデータが万が一漏洩したとしても、それが、ユーザーの生産技術の流出につながるリスクは低いということが分かる。

このように、システムのモデル化は、遠隔保守のような新しいサービスによる障害可能性の部分を明確化し、さらに、新しい技術の導入の際のリ

スクアセスメントにおいて有効である。したがって、今後、IoT 機器の普及や工場内のインターネット環境整備がなされる中で、遠隔保守システムの構成図を活用し、ネットワーク周辺の構成の変化に適切に対応したものへと調整することによって、必要十分なセキュリティ対策を伴ったサービス拡張が可能であると考えられる。

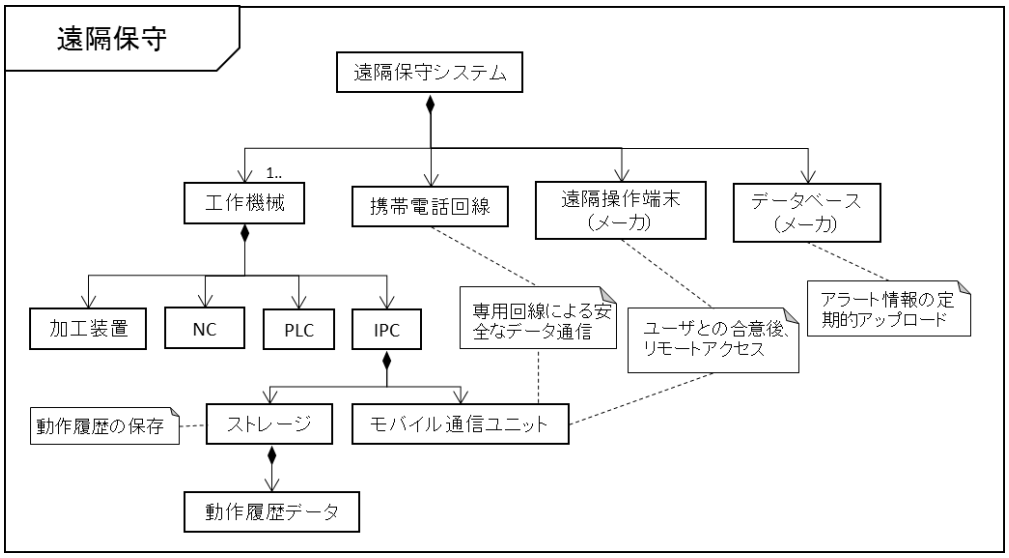

図 5.4 遠隔保守システムのブロック定義図

【予知保全システム】

予知保全とは、生産ラインのダウンタイムの主な原因となる工作機械の動作不良、障害等を極力なくすことを目指し、機械又は周辺環境に設置された様々なセンサーから得られる情報を収集・解析することにより、その不具合発生の時期を予知し、未然に防止措置を行うことで生産ラインの効率的な運用を実現する保全活動であるということができる。現状では、このような予知保全に関わるセンサーデータと不具合との相関を計測する技術が発展途上であり、工作機械の予知保全サービスの対象は極一部分の機能ユニットに限られている。本項では、現在、各メーカーが取り組んでいる予知保全システムに関して、ヒアリングの結果を基に、複数の工作機械を想定し、システム構成のブロック定義図（図 5.5）によるモデル化を試みた。

図 5.5 は、複数の工作機械から構成される生産ラインにおける予知保全システムの構成を表しており、外部の環境センサー等で生産ラインに係る周囲状況を計測可能な工場のモデルである。予知保全の場合には、工作機械単体のセンサーのみならず工作機械を利用している環境についてのデー

タを活用することにより、より高精度の予兆検出が可能であると考えられる。予兆検出においては、工作機械の取り付け位置や、加工対象となったワークの形状・素材等を表すデータが有益である場合もあり、このようなデータを含めた生産ラインに係る蓄積データは、ユーザー固有の生産技術又はノウハウになり得るものである。このため、遠隔保守と比較した場合、より情報セキュリティのリスクを考慮したシステム構成をする必要性があると考えられる。なお、ここで示したモデルでは、生産現場のデータベースとクラウドシステムとを利用することを想定しているが、クラウドシステムへアップロードするべき情報の種類等の分類・重要度付けを行うことが、情報セキュリティに関するリスクアセスメントにおいて有効であることが分かる。

このように、予知保全システムに関しても、外部システムを含めた工場全体をモデル化することで、サービス提供側とユーザー側とで、今後創出するサービスに関するリスクとその対策を事前に協議し、共通認識を持つことを容易にすることが可能になる。

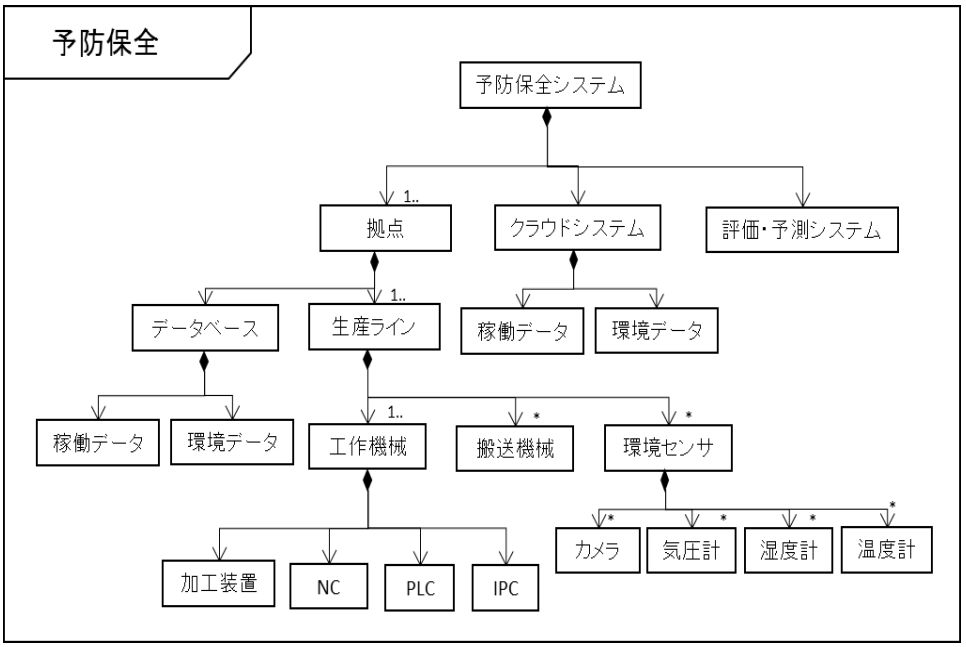

図 5.5 予知保全システムのブロック定義図

６．情報モデルから抽出されるサービス展開のためのガイドライン試案

（１）　工作機械の基本的な状態に関する定義と、状態に関する情報を取得する方法に関するガイドライン／インターフェースの整理

前述の５．（１）①において、工作機械の情報モデルについて述べた。図 5.2 の状態機械図は、生産ラインを運用するユーザーに対し生産ラインあるいは工場全体の稼働状態を俯瞰し、生産ラインの不具合箇所を検出し、保全活動を行うために十分な状態定義であると考えられる。そこで、工作機械の基本的な状態として、下記の 4 つの状態を定義可能であると考える。

① 初期状態

この状態は、工作機械の電源を投入した直後に移行する状態であり、加工終了後に安全に機械を停止する前の状態である。エラーやその他の不具合等による電源の停止は、工作機械に何らかの障害を発生させる恐れがあるため、正常な電源停止のためには、この状態に戻る必要がある。

② 加工準備状態

加工準備状態は、加工運転状態へ移行するための準備状態であり、工作機械の構成によっては、加工精度維持のために工作治具の交換時のウォームアップ状態や工作治具の自動交換などの自動化された段取りのための準備状態など複数の状態に細分化することが可能な状態である。加工運転時に生じたアラームにより移行したエラー状態から正常に復帰する場合にも必ずこの状態へ移行するものと定義する。また、この状態から正常状態（加工可能な状態）に復帰できなかった場合には、回復不能として機械を停止させ保守が必要なモード移行を行うようにする。

③ 加工運転状態

段取りが正常に終了したのちにワークを加工している状態であり、加工準備状態から移行する。工作機械運転時に、アラームが発生した場合にはエラー状態に移行する。

④ エラー状態

加工運転時に発生した警告・不具合のアラーム発生を契機に加工運転状態から移行する。作業員の確認後、電源の停止又は加工状態に復帰させたい場合には、必ず加工準備状態に移行するようにする。

ここで定義した工作機械の基本状態は、工場全体又は生産ラインの稼働状態の「見える化」を行い、生産管理の効率化を図ることを目的とする状態定義であるから、内部の IPC を介して生産管理を司る情報システムに通知されるようにする必要がある。現在、工作機械を構成する NC および PLC における情報取得の仕様がメーカーごとに異なるため、工作機械の状態に関する情報を取得するためには、一旦、NC および PLC のメーカーに応じたインターフェース（API: Application Program Interface）を通じて、IPC が生産ライン上の機械の状態を取得し、その上で、外部の情報システムが、当該 IPC を通じて、各機械等の状態に関する情報を取得するように設計されている。工作機械メーカーごとに独自のインターフェースが定義され、それに応じて生産ライン管理システムを構築する必要があるため、将来、生産設備を更新した場合には、その都度、生産ライン管理システムの再実装を余儀なくされる可能性がある。サプライチェーンおよびエンジニアリングチェーン全体の最適化を目指した「スマート工場」を実現し、効率的なプラットフォームの構築や、様々な工作機械自体の生産の効率化を進めるためには、メーカーの相違に伴う調整コストを低下させるべく、可能な限り、オープンなプラットフォーム技術を適用して必要な情報が取得できるようにすることが期待される。

このような考え方に立ち、工作機械の状態やその他の情報取得に関して下記の 2 つのインターフェースについて、共通化を進めることとする。

【NC および PLC と IPC 間のインターフェース】

工作機械の加工治具、周辺補助装置の制御を司る NC および PLC からの情報取得には、従来、メーカー固有の API による実装が用いられてきた。これでは、工作機械を製造するメーカー側に開発負荷がかかることになり、結果的に工作機械のユーザーの利便性も欠く可能性がある。そのため、共有モデルで表現された構成を満たす情報取得に関しては、原則として、オープンで標準的な仕様を採用することとする。具体的には、デファクトとなりつつある MT-Connect 標準又は ORiN 等のデジュール標準に準拠したインターフェースを用いることを推奨する。

【IPC と外部情報システム間のインターフェース】

工作機械のユーザーにとって、管理すべき対象は、個々の工作機械ではなく製品製造のための生産ラインである。この生産ラインの稼働状態をオフィスフロアや外部拠点からも監視することで更なる生産効率向上を図るという取組が進みつつあり、個々の工作機械の挙動を含めた生産ラインの状態を掌握する情報システムと、生産管理を行うための外部情報システムとを連結させるインタ

ーフェースは重要である。現状では、工作機械の状態に関するデータを取得するためには、各メーカー独自の API を実装する必要があり、設備の更新などが行われる都度、大きな改修を必要とする場合がある。このため、MES や ERP との連携機能部分も想定した、共通インターフェースを用いることを推奨する。この共通インターフェースとしては、今後の世界的なオープン戦略として ISO20242 等の国際標準に準拠したミドルウェア等を利用すべきであると考えられる。

（２）　工作機械をインターネットに接続するに当たっての情報セキュリティ対策に関する基本的な考え方

ー技術的背景

これまで、工場におけるネットワークの安全性については、外部との接続を是としない閉域のネットワークを前提にシステムが設計されてきた。その結果、工場内の多くの機器は、現在のインターネットに接続するサーバー等と比較して、セキュリティ対策が大きく遅れている状況になっており、PLC などにも多数の脆弱性が指摘されている。しかも、閉域ネットワークでありながら実際には様々な侵入の実例が生じており、主に制御システム（インフラなど）の分野では、機器破壊や工場での暴走・爆発事件に繋がるなど、具体的な脅威となっている。このような状況の中で、IoT の考え方を生産現場に持ち込み、生産機器の情報をインターネット経由のビッグデータとして活用することには、大きな困難と解決すべき問題が多数存在する。

一般的な制御システムにおいては、多段のファイヤウォールなどによる制御系ネットワークと情報系ネットワーク・外部インターネットとの分離などは既に行われている（図 6.1)。一方で、このような構成においても各層間では情報の流通が必要となるため、2 つ以上のネットワークにまたがる機器が存在することは避けられない。また、情報ネットワークから制御系ネットワークに設計図などの情報を流通させるために、USB 記憶媒体などが安易に使われる傾向もあり、これら記憶媒体も、広義の意味で、「2 つ以上のネットワークに接続する機器」ととらえるべきである。このような 2 つ以上のネットワークにまたがる機器がウィルスなどのマルウェアに感染した場合、制御系のネットワークに侵入され、アップデートの行われていない PC などが多数存在する制御系ネットワークは深刻な事態に陥ることになる(図 6.2)。

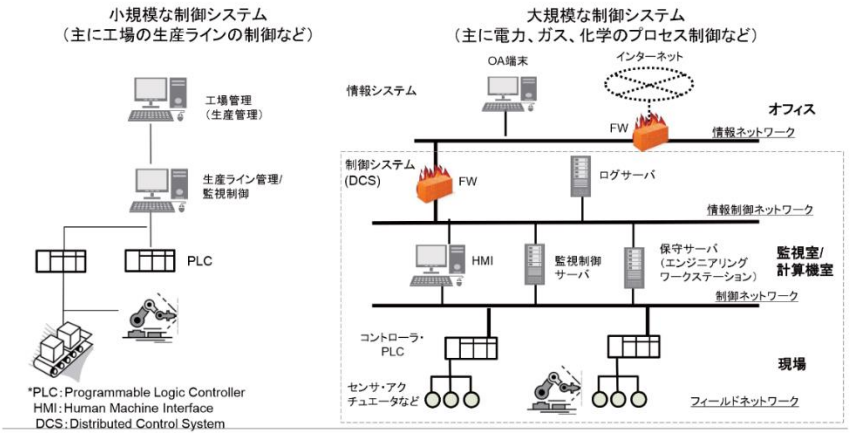

図 6.1 工場を含む制御システムの概念的な構成例
（引用元: IPA「重大な経営課題となる制御システムのセキュリティリスク」P15）

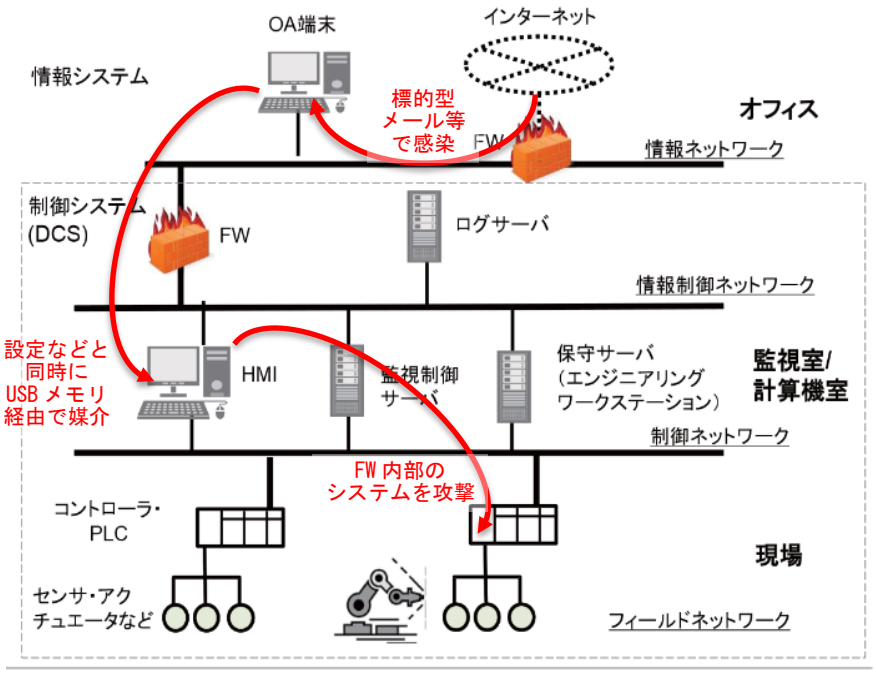

図 6.2 ファイヤウォールを超えたマルウェアの感染ルート例
（IPA「重大な経営課題となる制御システムのセキュリティリスク」P15 の図をもとに修正）

他方、現在の一般的な工場を念頭におく場合、第四次産業革命と呼ばれる技術を適用するために、わざわざ、新たなネットワーク環境を準備することは現実的ではない。そこで、既設の制御系ネットワークの閉鎖的な環境に、外部向けとなる遠隔保守のための通信を通過させることが不適当であると

判断されるなどの事情から、携帯電話網などの無線通信により、制御機器をIP（インターネット・プロトコル）の専用接続経由でメーカー等の監視設備に接続することが広く行われている（図 6.3）。このような接続は、それ単体であれば（セキュリティを一義的にメーカーに委ねることになることを除けば）現在の安価な無線通信環境においては現実的であるが、近い将来に工場内においても機器間連携の IP 接続が設備されることになると、このような機器の全てが上に述べた「2 つ以上のネットワークにまたがる機器」になり（図 6.4）、セキュリティ上の脆弱なポイントになることが危惧される。特に、管理者の異なる複数の外部接続ルートがネットワーク内に存在することは、問題の把握・管理・対処の全てにおいて、大きな問題である。もし仮に、機器が必然的に構内 LAN への接続と外部通信を両立しなければならない状況なのであれば、このような接続点はきちんと一括して工場側のファイヤウォールなどによって管理・掌握されるべきであり、安易に接続点を増やすことは厳に避けるべきである。

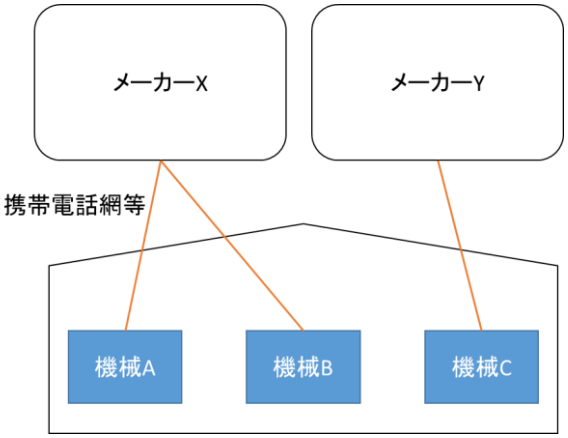

図 6.3 携帯電話網等による直接接続

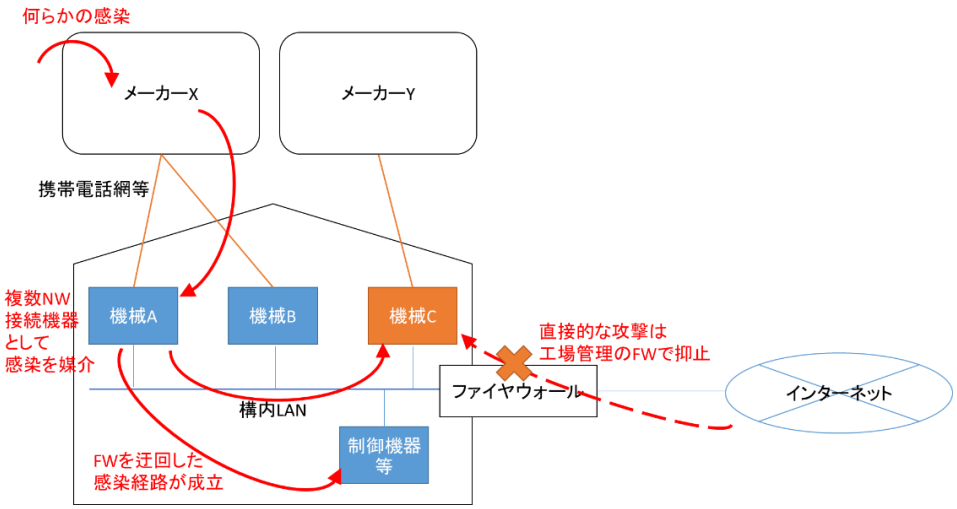

図 6.4 携帯電話網と構内 LAN の 2 重接続による侵入リスク

上記のような観点を踏まえるならば、当面、多くの工作機械メーカーがサービスの展開を進めようとしている遠隔保守システムを構築する上では、現状の通信モジュールの利用形態を踏まえつつ、構内における機器間連携が想定されるか否かの観点から、セキュリティモデルを大きく 2 つに分けて考えるべきである。

まず、構内における機器間連携が想定されない場合に限り、携帯電話網などの専用接続を利用し、工作機器をメーカー側のネットワークに論理的に直結できる可能性を残す。この場合当該の機器は、実際の所有権や設置箇所とは無関係に、情報セキュリティの観点では、メーカー側のネットワークに所属する機器と考えてセキュリティを設計する。本節では、このような場合に対応して、接続方式として「単独機器接続方式」と「VPN による簡易な接続方式」を例示する。

一方、構内における機器間連携などにより構内 LAN の構築が必要な場合、適切に管理された構内ネットワークに一本化させていく方向で、技術の検討を進めていく必要があると考えられる。本節では、「構内 LAN 方式」として要件を整理し、それぞれの場合に特有の安全上の対策要件を検討する。

いずれの場合においても、ウィルス等の攻撃に対する防護は現在では閉鎖環境においても必須と考えられており、単独の機器としてのセキュリティ防護の機能は、どのような接続形態を取る前提においても必要である。接続形態によらない安全上の対策については、情報管理体制として別途整理する。

ー 技術的接続方法の例示

【単独機器接続方式】

構内で LAN および USB メモリ等での情報系システムとの情報交換がなく、かつメーカー側システムからのセキュリティ侵犯リスクが無視できる（工場側の判断としてメーカー側に安全性確保を一任できる）状況においては、単独機器をそれぞれ、携帯電話網や商用広域 VPN サービスなどを用いた専用通信サービスを用いてメーカー側のネットワークに直接接続する方式（以下、「単独機器接続方式」という。）（図 6.3）は有効である。この場合には、メーカー側システムと接続する生産機器は、ネットワーク・セキュリティの観点からは、メーカー側のネットワークに収容され所属する機器として考える必要がある。具体的には、機器設置工場側においては下記のような点を確認することが、セキュリティ上重要である。

① 直接接続方式によりメーカー側システムと接続する生産機器は、原則として構内 LAN に接続しないこと（図 6.4）。

② 当該の生産機器と USB 記憶媒体等でデータを交換する際は、工場外部の機器とみなした情報セキュリティ上の取扱い（コンピュータ・ウィルス等のチェック）をすること。

また、このような機器を収容する接続網（通信網サービス）ならびにメーカー側ネットワークについては、下記の点を満たしていることを確認することが重要である。

（ア）接続網は IP レベルでインターネットから切り離されており、相互に通信が不可能であること。
（イ）接続網のメーカー側接続点は、インターネットに接続を持たないか、工場に準ずる厳格な管理で安全性が保護されていること。
（ウ）同一の接続網により複数の機器を収容するネットワーク（通信網を含む）においては、少なくとも他工場の機器間および、同一工場でも異なる箇所・ライン等に設置され相互の連携をしない機器間について、機器間の直接通信が不可能であること。
（エ）異なる工場の機器を接続するネットワークは、論理層（Layer 2）以下で分離すること。必要であれば、仮想ネットワーク（VLAN）等を用いること。
（オ）十分な暗号化又は盗聴・通信改変に対する防護・分離機能が、通信網の機能として実現されていること。又は、機器レベルで対策をする場合には、十分に普及し検証された汎用の技術を用いた暗号化と、機器とシステムの相互認証を機器メーカー側で実装する事。

なお、携帯電話網などを利用する場合でも、通信の制御・分離機能を持たない公衆網サービスなどを用いて制御機器を接続することは、セキュリティ上好ましくない。どうしても行う場合には、ファイヤウォールなどの十分な安全対策をした上で、公衆回線を次の「構内 LAN 簡易接続方式」として考える。

【VPN による簡易的な接続方式】

上記図 6.1 のような本格的な工場内制御システムネットワークが整備されていない場合において、次項で述べる本格的な構内 LAN 接続方式などのような万全の対策を実現するコストが難しく、かつ安全性に対する要求が低い小規模な応用に対しては、工場内において機器間連携が無い場合に限って、幾分管理を簡略化した方法を考えることができる。現状ではこの方式は、単

独機器接続方式に対して煩雑な分セキュリティ上の管理項目が増えることになるが、一方で将来的な本格的な制御ネットワーク経由の情報流通の仕組みの段階的導入ととらえることも可能である。

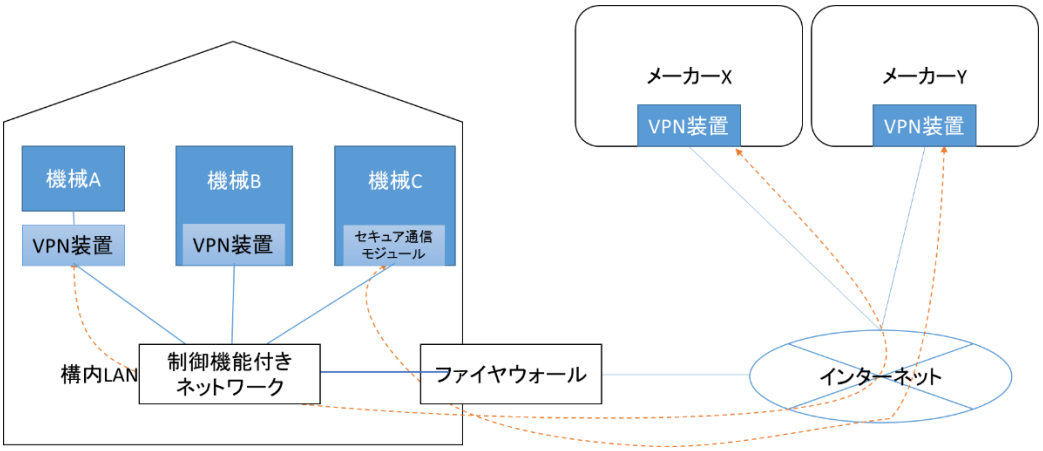

図 6.5 VPN と通信制御スイッチの併用による通信制御

具体的には、図 6.5 のような形で仮想専用ネットワーク（VPN）装置を用いることにより、公衆網上で専用ネットワークとほぼ同等の機能を実現することが可能である。この場合、構内 LAN は実質的にインターネットと同等の「危険性」とみなして、安全性を確保していることになる。この場合、各機器における注意点は個別接続方式の場合とほぼ同等となる。ただし、VPN 装置そのものも比較的セキュリティ脆弱性および攻撃被害を受けるリスクの高い装置であることから、その管理には十分な注意が必要である。VPN 装置が攻撃された際のリスクを緩和するため、ネットワークおよびファイヤウォールにおいて、追加的な通信制御を行うこととする。

この場合、工場側装置の VPN 装置（図の機械 A）については、メーカー側の VPN 装置と一体的に運用する必要があることや、中小企業などの想定利用者が（イ）（ウ）のメンテナンスを行うことは困難であろうことから、メーカー側の保守管理範囲とし、提供サービスの 1 つとすることが相当と考えられる。装置の通信モジュールの一部とし、機器と一体化すること（機械 B）も 1 つの考え方といえる。さらにこの場合、通信規格は必ずしも完全な仮想ネットワーク規格でなく、安全な暗号通信手段であればよく（機械 C）、将来的な構内 LAN 方式への移行を想定した設計とすることもできる。一方、構内 LAN およびファイヤウォールについては、工場側で管理し自己防御の手段とすることが望ましい。

具体的には生産機器に対する単独機器接続方式での留意点に加え、VPN 装

置とネットワーク装置に関し、次のような設定を行う。

（ア） 双方の VPN 装置は、それぞれの内部からの全ての通信を仮想ネットワーク向けとして扱い、構内 LAN に透過させない設定とする（企業内アクセス用の VPN クライアント装置は、一般のインターネット向け通信を透過させる機能を持つ場合がある）。また、仮想ネットワークの通信以外は一切通過させない設定とする。仮想ネットワーク以外の専用通信を用いる場合もこれに準ずる。

（イ） VPN 装置等の相互認証鍵等については厳格な管理を行う。

（ウ） VPN 装置等の脆弱性等についても、直ちにメンテナンス・対策が可能な体制を、必要な場合にはメーカー又は第三者のサービス等を用いて確保する。

（エ） ネットワークスイッチにおいて、各 VPN 装置とファイヤウォールの間の通信のみを許可し、VPN 装置相互間の通信を破棄する設定を行う（図 6.6）。

（オ） ファイヤウォールについては、構内 LAN からインターネット方向の通信のみを行う設定とし、インターネット側からの通信は構内 LAN からの通信に対する応答を除き破棄する（図 6.6）。VPN 接続は構内 LAN 側から確立するものとする。可能であれば、VPN 装置ごとにメーカー側 VPN 装置への個別の通信許可のルール設定を行い、その他の想定されない通信を破棄する。

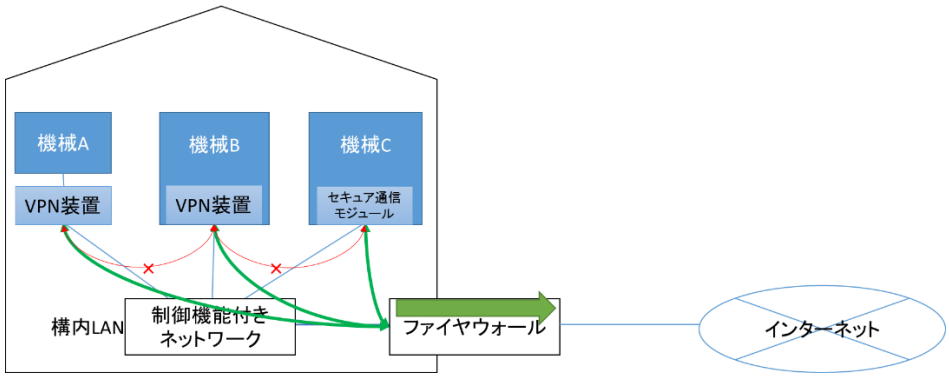

図 6.6 通信制御スイッチ等の通信可否の設定

このような制御をするスイッチ機器については、共同住宅の LAN における顧客間分離などに用いるために設計された経緯があり、市販の製品に機能として組み込まれているものがある。また、無線 LAN（インフラストラクチャモードのもの）においても、多くの機器がこのような分離機能を備えている。

【構内 LAN 接続方式】

一方で、本格的な機器間の連携を工場内で行う場合、セキュリティ上の設計の原則上、情報の流れを集中して構内ネットワークで管理することとなる。これは、機器間連携を行うために構内 LAN で機器間の相互接続がある前提で、外部から工場内機器に対する侵入経路を 1 つに限定し集中的に把握できるようにするためには、必然的に図 6.1 のような構成となり構内ネットワークがこの唯一の経路とならざるを得ないことによる。このような設計を達成するためには、必然的に工場内機器からの情報の出るルートも、構内 LAN 経由となることになる。

構内 LAN を用いて機器を外部と接続する場合においては、特定の機器が侵入されることにより、内部の他の機器に広範な影響を及ぼすことや、外部接続のための通信許可設定を悪用され情報を盗み出されることが、大きなリスクになる。このようなリスクを排除・軽減するためには、できるだけ機器間の接続を分離し、できるだけ詳細なレベルで通信の可否を制御できるようにすることが望ましい。一方で、VLAN などのネットワークの複雑な運用は、そのための専門技術者を確保しない限り、現状においてはコストと運用ミスのリスクが大きい。このような問題を解決するためには、下記のような対策を検討することが望まれる。ここで上げている対策は現時点では高コストで実現が難しいものもあり、運用コストを低減し導入を現実的にするための技術・製品開発などを行う事も必要であると考えられる。

（ア） 構内の機器相互間において、その機器がどの接続ポートに接続され、どの IP アドレスを用いて通信するかについて、物理レベル又は論理レベルで管理を行い、なりすましを防止すること。この方法については、例えば無線 LAN においては個別暗号鍵の設定又は WPA2-エンタープライズなどの利用、有線 LAN においては IP アドレスの固定設定を物理ポート単位の ARP および IP のフィルタ設定と併用することなどが考えられる（Layer 2 構成）。また、各機器を L3 スイッチと仮想 LAN（VLAN）などを用いて個別の論理ネットワークに格納すること（Layer 3 構成）によっても実現できる。

（イ） 構内の機器相互間および各機器・インターネット間の通信について、個別に通信の種別ごとの可否を管理し制御すること。このような制御については、((ア）の対策を取った前提で、）Layer 2 構成ではスイッチでのパケットフィルタリングにより、Layer 3 構成では L3 スイッチやルータの IP フィルタ設定によることなどが考えられる。

（ウ）上記の設定について、工場又はラインなどの単位で、設定の一元管理を行い、工場・ラインの情報管理者が全機器の状況を俯瞰できる体制を整えること。

（エ）（イ）において許可されない通信の状況を監視し、ルールの更新又は異常動作する機器の切り離し等をおこなえる体制を確保すること。

（オ）少なくともインターネットにかかる通信については、十分に普及し検証された汎用の技術を用いて暗号化等の対策を行う事。また、技術的に確実な方法を用いて機器とシステムの相互認証を行う事。例えば、TLS のサーバー証明書およびクライアント証明書を用いた認証などによることや、個別に L2TP 等の VPN 通信を確立することが考えられる。暗号化は基本的には end-to-end で行われることが望ましく、工場内に管理・中継システムを置く場合も、機器～中継システム間・中継システム～メーカー側システム間のそれぞれで end-to-end の暗号化がなされるべきである。末端の機器側で暗号化がされない場合には（ア）および（イ）などにより、通信が IP ネットワーク上で暗号化前に改変されないよう対策すること。

機器メーカーごとに LAN や外部接続を分離すること（仮想 LAN などによるものを含む）などにより、セキュリティリスクの波及の可能性を幾分抑えることは可能であるが、部分的にでも論理ネットワークを共有する、又は 2 つ以上の論理ネットワークにまたがる機器を持つ限りは、上記のような対策は多かれ少なかれ必要になるものと考えられる。

－ ユーザー及びサービスプロバイダーにおいて構築すべき情報管理体制・ルール

こういった工場で必要となる基本的な情報管理体制については、基本的にはこれまでの制御システム向けの管理体制（例えば、IEC 62443-2-1 CSMS for IACS）の延長にあると考えられるが、特に外部との情報交換が必須になる本応用においては、セキュリティ上の侵犯の影響が大きくなることから、脆弱性および侵入事案への対応体制については、これまで以上の体制整備が求められる。加えて、価値のある情報を生み出し流通させる仕組みとして、情報システムとしてのマネジメントも同時に大切になる。

本節の前半の整理で述べたとおり、実際の情報管理体制の運用については、ネットワークの構成によりその管理すべき主体が大きく分かれる。

直接接続方式においては、メーカーが直接的に機器との通信を一次管理することから、制御システムとしてのセキュリティマネージメントについても、

その一次的管理の任務はメーカー側によらざるを得ない。この場合、メーカー側の終端装置は、いわば「工場から伸びてきた複数の工場内ネットワークの延長」に当たることから、メーカー側のネットワークは概念的には（複数の顧客に対応した）複数の独立したラインを持つ仮想工場のネットワークのような位置づけとなり、各種ガイドラインを類推適用できると考えられる。一方で、実際の機械の利用者と情報上の管理者が異なることから、セキュリティ上のリスクや対策については、顧客との十分な情報共有が必要と考えられる。VPN 方式についても、（中間的な形態も取りうるが）現段階では基本的には直接接続と同様の位置づけとなる。

一方、「構内 LAN 方式」では、メーカー側の遠隔監視機能への情報の流れ、構内 LAN から外部への情報提供と位置づけられ、一次的な情報管理は工場側の任務となる。この場合、特に機器監視のための外部接続にかかる通信について、慎重な管理が求められることになる。

いずれの方式においても、メーカーと利用者側との間では、発生する通信の内容やセキュリティ上のリスクについて、十分な情報共有が取られることが、何よりも重要であると考えられる。工場側でリスクの確実な管理を行えるようにするため、以下の情報についてはメーカーから整理し、必要に応じて工場側に提供できることが望ましい。

- 各機器毎に、その機器が情報機器として正常に動作するために必要な通信に関する情報。例えば、正常生産時における通信先や通信量の概要、機器異常時に発信されるアラートに関する通信先や通信量の概要、ソフトウェアアップデートなどを正常動作させるために必要な通信先と通信量などが挙げられる。このような情報が無いと、不必要に許容的な通信ルールの設定によりマルウェアの自由な侵入活動を許したり、逆に生産異常時のアラートの送出が、平常と異なる通信として妨害されたりする恐れがある。
- 機器に使用している自社開発以外のソフトウェア基盤（OS 等）のメンテナンス期間と、セキュリティ対策更新の手順、メーカーとしてセキュリティ脆弱性等の対策に対応する期間。現在の OS はほぼ全てがメンテナンスなしではセキュリティ上安全に動作できないことを踏まえ、アップデートに対応できる期間およびコストをきちんと顧客と情報共有し、「古い機器がメンテなしに使われ続けないようにする」こと、言い換えれば「古い機器が使えなくなることを相互理解すること」が、強く求められる。

（３）工作機械から生成するデジタルデータに係るアクセス・コントロールに関するガイドライン

（２）で示した情報セキュリティに関する措置は、いわば、当事者にとって予期せぬ事態にならないようにするための措置である。（３）で示そうとする、デジタルデータに係るアクセス・コントロールに関するガイドラインは、情報セキュリティとの対比でいえば、当事者にとって「予期している（すべき）状態」が何であるかについての整理といえる。

例えば、遠隔による工作機械の保守等のサービスを利用する際に、工作機器に関する情報がサービスプロバイダー側に一定程度流れるということについては、工作機械ユーザーにとっても想像に難くない。しかしながら「どのデジタルデータが誰の管理の下でどのように利用されているか」、「当面の目的を終えた後に関連のデジタルデータがどのように処理されているのか」など、デジタルデータの利用や管理に関する状態について、ユーザーとサービスプロバイダーとの間で、共通認識が定着しているケースは多くない。インターネットに接続された環境の下でのデジタルデータの共有に関し、とりわけ工作機械等のユーザーが慎重になる背景には、このような、デジタルデータの管理の側面に着目し、アクセス・コントロールという観点から、当事者の共通認識醸成を促すための指針を整理する、

その際、今回想定している保守管理等のサービスに限定したとしても、その内容は、プロバイダーの創意工夫の結果、多様であり、いわゆる競争領域としての性格が大きいという点に注意が必要である。サービスの内容によって、デジタルデータの活用のあり方も異なることから、デジタルデータに係るアクセス・コントロールに関する共通了解事項をガイドラインとして整理するに当たっては、このような多様な有り様を許容し、イノベーションを育みうるものとする必要がある。

このような問題意識に基づき、当面の考え方の整理を、以下のとおり行う。

① 原則

ア）取り扱うデジタルデータに関し、以下の観点について、当事者間で明確な共通認識を持つこと

- 取り扱うデジタルデータの範囲
- 取り扱うデジタルデータの利用目的
- 取り扱うデジタルデータの収集、保存、処理、廃棄の方法
- 取り扱うデジタルデータの収集、保存、処理、廃棄のできる者の範囲
- 取り扱うデジタルデータにアクセスできる者の範囲

イ）取り扱うデジタルデータは、利用目的に照らし必要十分な範囲で収集等を行うこと

ウ）取り扱うデジタルデータの処理等に伴い得られる新たな知見については、処理等を担う者に帰属することを原則としつつ、当事者間で事前に方針の明確化を図ること

② 遠隔保守・予知保全サービスにおける原則的整理

①の原則に掲げた内容については、個別のサービスに照らし必要な範囲で、契約等とすることによって、当事者間における一定の規律を保持することが望ましい。

最終的には当事者間の合意により多様な取扱が許容されるべきであるが、インターネットのような開かれたネットワークの利用を前提としたサービスが主流になる場合には、サービスを提供する側、受ける側の双方において、当事者の範囲が広くなり、あらかじめ関係者を事前に特定することができない場合も生じ得る。このため、典型的なサービス類型については、可能な範囲で、原則的な考え方を整理し、個別のサービスに関する円滑な合意形成のための活用していることとする。

【遠隔保守サービスに関するデジタルデータの取扱】

遠隔保守サービスは、図 5.3 で示した保守作業のブロック定義図からわかるように遠隔保守は、突発的な事象への対応の一つであると考えられる。現在の遠隔保守では、工作機械の不具合発生時に稼働履歴を参照することで、不具合発生の原因の特定と交換する保守パーツの特定が主なサービス内容であり、デジタルデータの取扱は、図 5.4 に示した遠隔保守システムのブロック定義図により下記のように整理することができる。

- 取り扱うデジタルデータの範囲：
  - 不具合発生までの一定時間の工作機械の稼働情報（工作機械内部に設置したセンサー情報及びアラーム情報等。ただし、ユーザーの製品製造に係る製造プログラム、ワークに関する情報は含まない）
  - 作業員の操作履歴（電源・運転スイッチの操作、補助装置の操作等）
  - 一定期間の過去の保守作業記録

- 取り扱うデジタルデータの利用目的：

  工作機械の不具合を解消し、通常運転可能な状態への復帰および不

具合と保守部品との関連性の特定を行うため

- 取り扱うデジタルデータの収集、保存、処理、廃棄の方法：
  工作機械の稼働情報および作業員の操作履歴は、機械内部に設置されたセンサーから収集し、ユーザーとメーカー間の遠隔保守契約に基づき、工作機械内部又はメーカーが保守するサーバーに保存する。過去の保守作業記録は、原則としてメーカーの行った保守作業であるが、ユーザーが独自に保守作業を実施した場合には遠隔保守契約に基づき収集しメーカーが保守するサーバーに保存する。
  上記のデジタルデータは、十分な情報セキュリティ対策を施した計算機上のみで処理し、不具合の解消、不具合の原因と稼働履歴との関連性を明確化できた時点、又は遠隔保守契約に基づき廃棄する。

- 取り扱うデジタルデータの収集、保存、処理、廃棄のできる者の範囲：
  各デジタルデータの取り扱いのできる者は、ユーザー側の生産管理者およびメーカー側の保守担当者およびその責任者等、遠隔保守契約に記された者に限定する。

- 取り扱うデジタルデータにアクセスできる者の範囲：
  各デジタルデータへのアクセスは、原則として、収集、保存、処理、廃棄できる者とする。

【予知保全サービスに関するデジタルデータの取扱】

図 5.3 で示した保守作業のブロック定義図から、予知保全サービスは、定期点検や日常点検と同様に一定周期で検査し、補修すべき箇所を事前に通知するサービスであり、現状では、長時間の生産ラインの停止（アラーム停止）を誘発する部品の不具合に対する予兆検出となっており、取り扱うデジタルデータのアクセス･コントロールは、下記のように整理できる。

- 取り扱うデジタルデータの範囲：
  - アラームを誘発する部品の保守・交換の記録
  - 運転時の稼働情報（絶縁抵抗、スポット溶接の加圧力、チップ摩耗度、アーク溶接の電圧・電流等）
  - アラーム停止を誘発する予兆推論モデル

- 取り扱うデジタルデータの利用目的：

工作機械のアラーム停止する前の異常を検出する。

- 取り扱うデジタルデータの収集、保存、処理、廃棄の方法：
  工作機械の運転時の稼働情報は、機械内部に設置されたセンサーから収集し、ユーザー又はメーカーが保守するサーバーに保存する。過去の保守作業記録（部品の交換記録）は、予知保全契約に基づきユーザーの保守記録から収集し、稼働情報と同じサーバーに保存する。予兆推論モデルは、予知保全サービスを提供するメーカーによって生成・管理されるものであり、予兆検出を行うサーバーに保存する。各デジタルデータは、予兆検出を行うサーバーへ送信、処理され、廃棄される。

- 取り扱うデジタルデータの収集、保存、処理、廃棄のできる者の範囲：
  各デジタルデータの取り扱いのできる者は、ユーザー側の生産管理者およびメーカー側の保守担当者およびその責任者等、予知保全契約に記された者に限定する。

- 取り扱うデジタルデータにアクセスできる者の範囲：
  各デジタルデータへのアクセスは、原則として、収集、保存、処理、廃棄できる者とする。

以上、予知保全サービスのデジタルデータの取り扱いについて整理を行ったが、現在の予知保全サービスでは、工作機械の様々な不具合の予兆をすべて検出するまでに至っておらず、これからの様々な技術開発を必要とすべき分野であると考えられる。特に、アラーム停止を誘発する予兆推論モデルとそのデータ処理に関する技術は、予知保全サービスの根幹となる技術であり、発展途上の技術である。したがって、このような技術の研究開発を促進させるためには、上記のデジタルデータを、守秘義務契約等を交わした第三者へのアクセスを可能にすることも考慮すべきであろう。

７．本サービスに係る情報モデルを活用した、スマート工場の提案

５．で整理した情報モデルは、工作機械の挙動を総合的に把握し状態を記述するものであるから、４．（１）で触れたとおり、工場全体の生産管理や、それを含めたサプライチェーンの管理に活かすことも可能となる。また、近年進歩の目覚ましい人工知能を、工場における生産性の向上に活かす上で、工作機械から生成されるデジタルデータが、高度に利用可能な状態で整理蓄積される環境は、有用である。

スマート工場で目標とされるマスカスタマイゼーション（カスタマイズされた製品を大量生産品と同程度のコストと価格で製造し、価値を生み出す戦略）を遂行する上でのカギは、システムを制御する周期と全体最適である。

生産管理において、日単位のデータであれば、人の判断で対応が可能であるが、時間、分単位のデータでは、人の判断において最適な生産指示は困難である。また、機械の短時間の停止相当のトラブルでも、硬直化した生産指示では対応できず、これらへの柔軟な取組みが重要となってくる。ここで、生産現場の設備、工作機械、様々な工程の状況を繋いでリアルタイムな掌握、分析、対策を行うため、それを支援する様々なソフトウェアツールが必要となるが、多様な分野の製品群であり容易に接続することが出来ない。従って、工場を構築する顧客では、この仕組みを構築することは困難である。

そして、日本の強みは現場力、現場のカイゼン力にあり、この強みの維持・強化策は重要である。今までの日本のカイゼンは部分最適になりやすい。現場のカイゼン活動は、人が主体となり、目の届く範囲、手の届く範囲が多く、設備と設備、設備と作業者、設備と部品、部品と部品、といった狭い範囲の問題を扱う場合には効果を発揮するが、ライン全体、工場全体、製品全体を取り扱うことは得意としていない。部分最適を積み重ねても、全体最適にたどりつけない。そこで、国内の優位性を確保しながら、スマート工場を実現するには以下のポイントが挙げられる。

（１）サイバーフィジカルなカイゼン現場

同じ工場であっても離れた作業エリアに対するカイゼンや、海外工場に対するカイゼンを遠隔地で可能とするリモートカイゼン、カイゼンの生産性革新を行う。

IoT の情報収集能力を活用して人の目に見えない範囲であっても可視化し、あたかも手元にあるようなバーチャルな環境をつくりあげ、そこで予測的な手法を交えた PDCA を回すサイバーフィジカルなカイゼン現場、俊敏な PDCA のカイゼン現場を構築する。

（２）日本の強みを生かす創発型インフラの提供

こうした日本版のサイバーフィジカルなカイゼン現場からは、新たなものづくりコンセプト、サービス、方法論への組み換えが始まる。

日本には、工作機械、生産設備、周辺装置、さらにはMES、SCADAに関わるソフトベンダー、インテグレータが存在するが、こうした日本のものづくりノウハウを柔軟に融合出来るインフラを構築する。

ここで、重要なことは、生産技術サイドでのカイゼン結果を生産管理側へフィードバックする流れを持つサイバーフィジカルな工場を構築することである。生産管理での活用、人工知能による分析を行う際、工作機械からリアルタイムで生成される全てのデータが、全てそのまま利用されることに合理性があるとは限らない。情報処理と通信の速度を左右する技術進歩の動向にもよるが、少なくとも、当面想定される技術進歩のトレンドを前提とするならば、生成される情報を取捨選択しながら、効果的に利用していくメカニズムを指向することが合理的である。これによって、製造計画のみならず、工程設計のカイゼンも可能となる。

すなわち、高度なリアルタイム制御を要する工作機械、ＦＡ、ロボット等をどのように駆使して高品質で高効率な生産を実現するかを決めるエンジニアリングチェーン（生産技術）といつまでに、どこで、いくつ作るかを決めるサプライチェーン（生産管理）とを情報レベルでどのように連携させるかについて、各々がIoT等の新たな技術の成果を活かしそれぞれ高機能化していく際に必要な情報の質・量の違いを重視して、具体的な連携の方策を、インターフェース（情報の内容、粒度、頻度、手段、通信プロトコル等）として整理することが有意義である。

以下に、５．で整理した情報モデルを活用しつつ、あり得るスマート工場の構造を提示する。また、インターフェース試案の骨子を併せて提示する。インターフェースについては、第一次案を2016年中に公表する。

- 下図のNCに代表される工作機械の中のデータ（Ａ）は、生産管理、生産技術の領域に活用され、具体的には以下のデータの流れにより、幅広いサービスを提供することが可能となる。なお、これまでの稼働状況の見える化等のサービスは各工作機械から直接、生産管理データに集約されていたが（Ｂ）、今回提示するスマート工場では、生産技術データとして集約し、情報処理を実行した上で上位システムである生産管理データに提供する仕組みを想定する。
- （Ａ）の中の稼働状態を秒、分、時間、日の単位で示す様々なデータは、生産現場の中で生産技術データとして集約、格納され（Ｃ）、稼働状況等のよ

り詳細な現場の見える化等を推進し、現場のカイゼン活動により生産性向上に活用される。

- （Ａ）の中の稼働状態をμｓ、ｍｓレベルでの時間単位で示す様々なデータは、生産現場の中で生産技術データとして集約、格納され（Ｃ）、機械の加工条件の改善などに活用される。
- 生産技術データ（Ｃ）は、機械の生産現場に実装される知的判断モジュール（Ｄ）で一義的に処理（遠隔、クラウド等、システム構築の選択肢の幅あり）され、（Ａ）にフィードバックし、加工効率改善等のサービスに活用されていく。
- 生産技術サイドでのカイゼンを推進する知的判断モジュール（Ｄ）の成果を、生産管理側へフィードバックする流れを作れば、全体最適のカイゼンシナリオを持つサイバーフィジカルな工場を構築することができる。

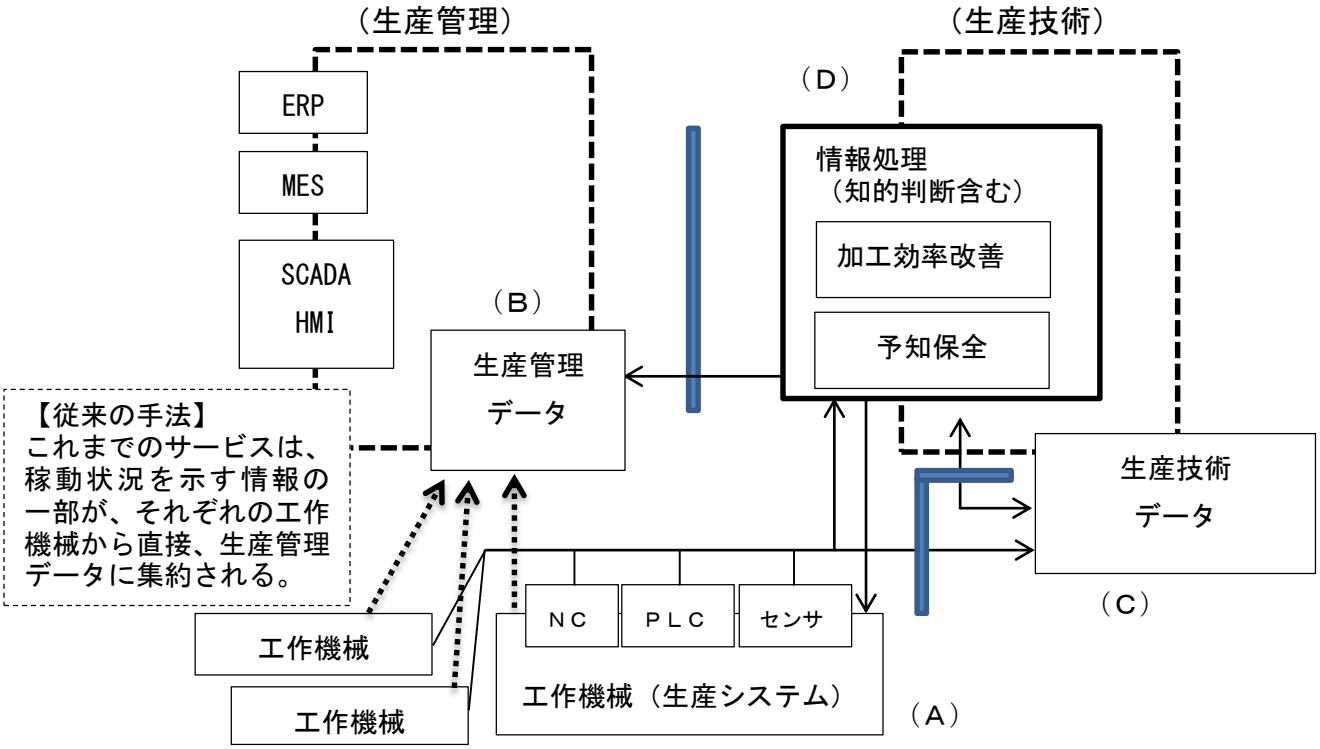

図 7.1 スマート工場概念図

日本の生産技術の強みを生かすために、前述の各サービスにおけるカイゼンサイクルを想定したデータの流れをモデル化して、データを流す上で共通化すべきインターフェースを提供していくことが肝要である。

【インターフェース骨子】

本システムを検討するにあたり、工作機械やＣＮＣ、ＰＬＣ、センサー等これに繋がる（Ａ）の構成要素は様々であり、かつメーカーも様々であるため、インターフェースの共通化は重要である。

現時点では、そのインターフェースとして必要な種類のデータの例を列挙する。今後の取り組みで更に追加を行うと共に、具体的なデータの意味を共通化することが必要である。

■（Ａ）と（Ｃ）、（Ｄ）との間のインターフェース

・工作機械の状態信号（初期、加工準備、加工、アラーム、通信切断等）
・工作機械の加工状態（加工プログラム、加工モード、加工開始、停止）
・工作機械の運動状態（位置、速度、加速度等）
・工作機械の主軸・送りモータの状態（位置、速度、加速度、トルク、温度等）
・工作機械のアラーム状態（アラーム種類、関連する情報）
・工作機械の機械状態（稼動管理、予知保全に必要な状態量）
・センサーからの情報

■（Ｄ）と（Ｂ）の間のインターフェース

・加工セルの機械の稼動状況（初期、加工準備、加工、アラーム、通信切断等）
・加工セルの機械の加工状況（加工部品種類、加工数、加工時間、停止時間等）
・加工セルの機械の消費電力
・加工セルの機械のアラーム状態とその推定原因
・加工セルの機械のワーニング状態と予知保全対象部品
・加工セルの部品の品質に関する情報（精度、面品位等）

（別添）

検討メンバー

（主査）	早稲田大学	教授	可部 明克
（副主査）	産業技術総合研究所　情報技術研究部門		
	サイバーフィジカルウェア研究グループ長		大岩　寛

【五十音順】

オークマ	常務取締役　技術本部　本部長	家城　淳
ジェイテクト	取締役副社長　工作機械・メカトロ事業本部長	井坂　雅一
	シニアフェロー	中野　史郎
DMG 森精機	専務執行役員 製造・開発本部電装・制御担当	藤嶋　誠
日立製作所	モノづくり戦略本部　生産技術強化推進部　主管技師	浜岡　昭夫
ファナック	専務取締役　研究統括本部長	松原　俊介
富士通	産業・流通営業グループプリンシパル・コンサルタント	熊谷　博之
三菱電機	FA システム事業本部 産業メカトロニクス事業部 技師長	安井　公治
ヤマザキマザック	常務執行役員　生産本部　副本部長	大野　寧彦
	経営本部　BEST 推進部　執行役員　部長	稲鶴　勇
産業技術総合研究所	ロボットイノベーション研究センター	
	ロボットソフトウエア研究ラボ　ラボ長	原　功

（ＷＧ１主査）

日立製作所	電力・インフラシステムグループ 経営企画本部	
	事業開発渉外部 部長	水上　潔