製造業DX推進を阻害するボトルネックと解決アプローチ
製造現場のITインフラ改革で動き出す製造業DX

櫻井　望

CONTENTS

要　約

1　現在、大手企業の多くの工場では、制御系（OT系）ネットワークを情報系（IT系）ネットワークから分離した「閉じた工場」となっている。これは、高可用性を最重視するOT系を外部から守るための標準的なネットワーク構造といえるが、製造現場におけるDX（デジタルトランスフォーメーション）推進においては、この分離構造がDX推進のボトルネックとなっている。

2　OT系ネットワークの分離構造は、情報セキュリティ基準などのルールに基づいて運用されているが、長期にわたって見直しが入らず、閉じた工場構造を硬直化させる原因となっている。

3　製造業DX推進では、分析基盤へデータを送ることから始まるが、元データは分離された閉じた工場の中にある。加えて、高可用性重視のOT系では、システム停止の可能性となる脆弱性のスキャンや各種パッチ適用なども実施できないケースが多く、そもそも外部と安全にネットワーク接続できる素地がない。

4　「高可用性のためのOT系分離」と「DX推進のための接続」という相反する要件に対応するには、「ITインフラの構造改革」と「攻めの情報セキュリティ基準策定」が必要である。

5　加えて、DX活動を進めるために最初に動くべき組織は、従来の情報システム部門ではなく、新たにDX活動を推進・リードするために組織化されたDX推進中核部門である。

6　最後に、DX推進中核部門が果たすべき役割や、ITインフラ構造改革が動き出した場合に必要となる「攻めの情報セキュリティ基準策定」ならびに「ITインフラデザイン」の二面から具体的な実装ポイントを示す。

Ⅰ 製造業DX推進を阻害しているボトルネック

1 閉じた工場ネットワーク

製造業におけるITインフラ環境は、大きく2つに大別される。1つは、基幹システム・電子メール・ファイルサーバなどを利用するための情報IT系ネットワーク（Information Technology）である。もう1つは、工場内に構築され、生産設備の制御・監視、あるいは生産管理のシステムが配置される制御OT系ネットワーク（Operational Technology）である。

IT系ネットワークは、業務効率化や情報共有・データ分析などさまざまな目的のために利用される。働き方改革の流れから社外からのアクセスも求められ、クラウドの利活用も進むなど「広くつながるネットワーク」が求められる。

一方、OT系ネットワークは当該拠点の生産設備を正常に稼働させることが目的であり、高可用性が最重視される。このため、OT系のITインフラは極力変化を加えず、触らないことが基本である。結果、OSや各種ソフトウエアのバージョンアップ、そして端末のウイルススキャンすらリスクとされ、今なおサポート切れのOSが、ウイルス対策も十分施されずに運用されている。

IT系からの目線では、セキュリティ対策が不十分なOT系とのネットワーク接続はリスクであり、OT系からの目線では、IT系からの通信による生産設備への影響がリスクである。必然的にOT系とIT系の間にファイアウォールが設置され、あるいは物理的に隔離された「閉じた工場ネットワーク」が常識となった。ハードウエア型ファイアウォールの黎明期から20余年、自社で定めた情報セキュリティ基準などに基づき、多くの企業は今も閉じた工場ネットワークを守り続け、これを是としてきた。

米国、ドイツ、新興国などでは、デジタル技術の革新を背景とした環境の変化に対応する取り組みが進んでいる。わが国でもSociety5.0の実現に向け、「Connected Industries」というコンセプトが世界に向けて発信されているが、国内製造業は成長が伸び悩んでいる。国内製造業が他国と比べてあまり成長していない理由は、生産技術の向上を「閉じた工場ネットワーク」により限定的にしか享受できなかったという側面もあるだろう。

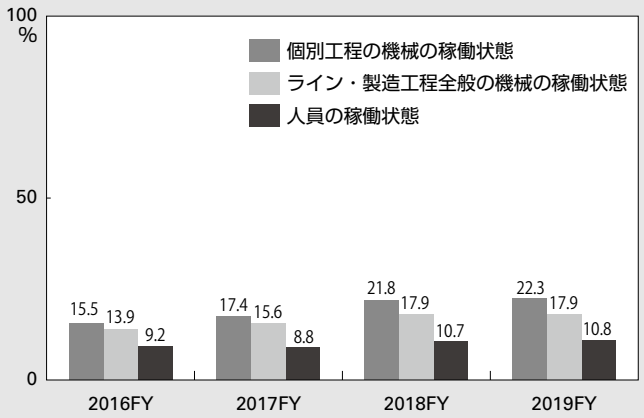
一方で、新興国は最新の生産技術を搭載した製造装置を導入して競争力を高め、欧米ではリアルタイムなOT活用によるビジネスモデルの変更で競争力そのものを変え、日本企業に対して競争を仕掛けてきている。その結果、DX（デジタルトランスフォーメーション）が進まない国内製造業は相対的に国際競争力を低下させていったと考えられる。

実際に、国内製造業のDXが足踏みしている状況を示すデータがある。経済産業省の「令和元年度ものづくり基盤技術の振興施策」によると、2019年度の国内製造業におけるセンサーやITを活用しての「見える化」を実施している企業数の割合は、①個別工程の機械：22.3％、②製造工程全般：17.9％、人員稼働状態：10.8％といずれも低く推移している（図1）。

2 変わらぬ情報セキュリティ基準

閉じた工場ネットワークの構造は、何に基

図1　国内製造業における「見える化」実施状況



づいて形作られているのか。多くの企業では、各社の情報セキュリティ基準やネットワーク構築のルールで定められており、場合によっては不文律ながらも脈々と「つながない」を受け継いでいるケースもあろう。従来の「閉じた工場ネットワーク」は組織に深く浸透しており、リモートアクセスやインターネット接続といった話を持ち出すこと自体がはばかられる。現場レベルで考えるさまざまな取り組みも、「どうせセキュリティ上、許可が出ない」と諦めの声に変わるケースを多く耳にしてきた。

昨今、DXが企業競争力をもたらすといわれ、データ利活用が必須となる中で、従来、是とされてきた「閉じた工場ネットワーク」そして「旧来からの情報セキュリティ基準」が、いかに製造業DX推進のボトルネックとなっているのかを、私たちは正しく理解する必要がある。

そこで、昨今の工場で非常に要望が多い「Webカメラを用いたリモート監視」の導入を例として挙げてみたい。筆者が知る限り、情報セキュリティ基準を適切に整備している大企業ほど、IT系ネットワークでは「会社指定端末以外は原則接続不可」というルールが多く、消去法的に「OT系もしくは専用ネットワークセグメントであれば、Webカメラを使用できるのでは」という発想に至る。

仮にOT系ネットワークにWebカメラを接続できたとすると、次に壁として立ちはだかるのが、「テレワーク環境からでも閲覧したい」というリクエストである。新型コロナウイルスの影響を受けて、生産管理部門のテレワーク要件が拡大しており、Webカメラの閲覧場所は工場内のみならず、テレワーク環境まで拡大している。つまり、工場とテレワーク環境の間を、会社のVPNあるいはインターネットを介した通信でつなぐことが求められることになる。

冒頭の製造業DXの源泉データ伝送にせよ、Webカメラの接続にせよ、もはや「閉じた工場ネットワーク」および「旧来からの情報セキュリティ基準」のままでは、どちらの要件も満たすことはできない。本来、企業のITインフラとは、事業を円滑・効率的に進めるための基盤ではなかったか。これらを放置すれば、ITインフラがその役割に反し、製造業DXや働き方改革を阻む壁となってしまうことはいうまでもない。

3　分離されたITインフラ管理部門

分離されたIT系ネットワークとOT系ネットワークのように、それぞれのITインフラ管理部門も分離されていることが多い。IT系ネットワークは全社の情報システム部門、OT系ネットワークは各工場の工場管理部門という具合である。そして、それぞれの管理部門が情報システム予算と管理権限を持ち、

絶妙な距離感とともに、お互いがそれぞれの領域や権限に踏み込まない運用を成立させてきた。

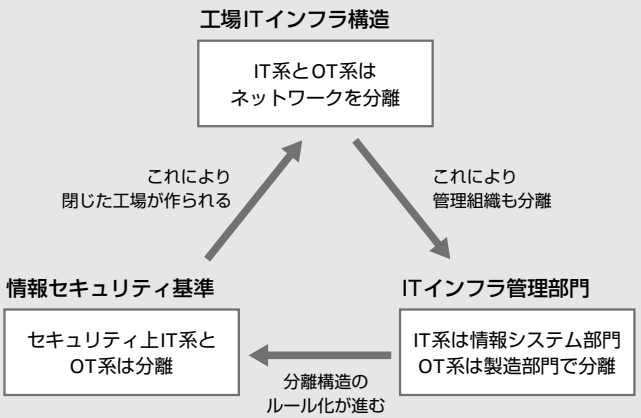
では、製造業DXの阻害要因として挙げた「旧来からの情報セキュリティ基準」は、どこが管轄しているのか。これは全社共通ルールであるため、本社の情報システム部門やセキュリティ部門が担っていることが多い。結果、工場側での新たな取り組みや接続要件は、本社部門への「情報セキュリティアセスメント申請」という形で届けられ、本社部門は「旧来からの情報セキュリティ基準」に基づいて、要件を満たさないケースであれば正しく却下する。分離された情報システム部門と工場管理部門の温度差や、「旧来からの情報セキュリティ基準」に縛られている組織もまた、製造業DXの阻害要因の一つといえるであろう。

4　製造業DX推進阻害要因の三すくみ構造

これまでに述べた「閉じた工場ネットワーク」「旧来からの情報セキュリティ基準」、そして「分離されたITインフラ管理部門」の三要素は、どこかを動かそうとすると他方に抵触してしまう、いわば「三すくみ構造」に陥っており、どこからも手が付け難い状況となっている（図2）。

それでは、三すくみ構造のどこからメスを入れればよいのか。まず着手すべきは、「閉じた」を「つながる」に変革させるための「情報セキュリティ基準の見直し」となる。本社情報システム部門・セキュリティ部門が長らく堅持してきた基準を見直すためには、彼らが行動を起こすためのトリガー・理由が必要である。そして、そのトリガーとなり得るのが、「工場DX推進を妨げているITインフラ問題」の正しい認知と、その影響・事の重大性の理解である。

図2　工場ITインフラの硬直化を生む三すくみ構造



とはいえ、本社側の情報システム部門は工場管理部門の領域には踏み込まないため、工場側の実情を把握することが難しい。そこで双方の組織をつなぎ合わせる「第三の組織」が必要となる。

Ⅱ　ITインフラ改革を呼び起こす第三の組織

1　DX推進中核部門

製造業のDX推進においては、先に述べた本社側の情報システム部門と工場側の工場管理部門に加え、第三の組織ともいえる「DX推進中核部門」が最も重要なカギを握っている。ここでは、その役割について述べたい。

経営戦略でDX推進を掲げる企業では、DX推進をリードするための専門組織を立ち上げるケースが少なくない。製造業では、生産技術や生産戦略部門、あるいは製造現場に

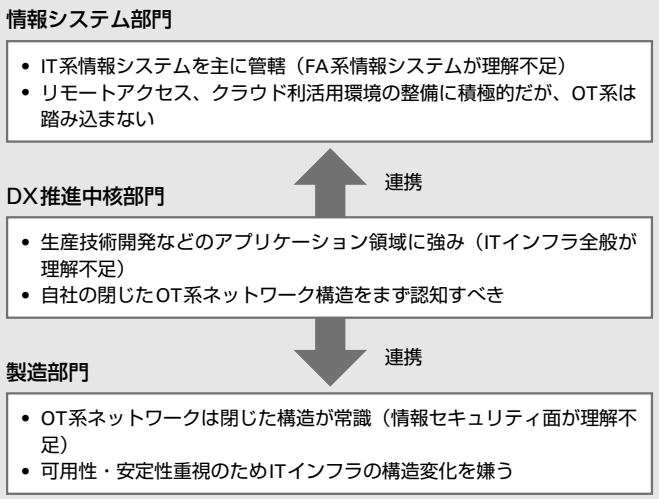
近い組織からDX推進人材が集められることが多いのではないだろうか。製造業DXを推進する上では製造部門と情報システム部門の中間に位置し、それぞれと連携・つなぎ合わせる役割を担う（図3）。

DX推進中核部門は、傾向的にアプリケーション領域に強い人材に偏ることが多く、ITインフラ領域の知見者の割合が低い。長らく閉じた工場ネットワークを是とし、ITインフラ構造に極力変更を加えずに維持してきた結果、自社のITインフラ構造を理解するためのさまざまな機会が奪われた側面を反映しているといえる。

ITインフラ領域の知見者が含まれないチームがPoC（Proof of Concept：概念実証）を始めると、「個別環境」でのトライアルまでは進めることができるが、閉じた工場ネットワークの中にある実データを分析基盤へ送り届けようとした途端に、ITインフラ構造・セキュリティ基準に阻まれる。自社のITインフラ環境の実情を知らぬまま進めてしまうためである。

一方、自社のITインフラ環境を理解している担当者がプロジェクト体制に組み込まれているケースでは、あらかじめ自社のITインフラ事情も織り込むことができる。この場合、PoC推進と並行して、ITインフラの整備についても検討が進むため、本格展開の段階でITインフラ整備の必要性に気が付くという時間的ロスを小さくすることができる。

図3　DX推進中核部門の立ち位置



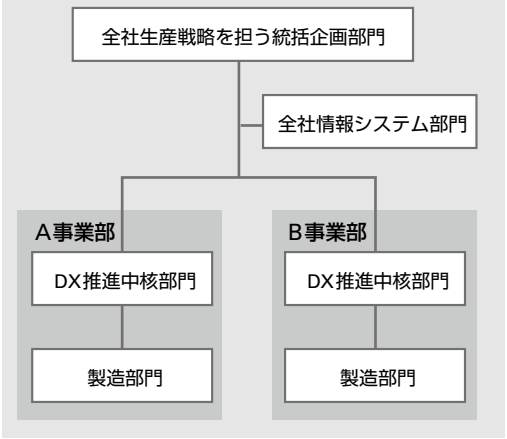
2　ITインフラ改革に向けた口火

情報システム部門はOT系を管轄していないことが多く、工場側DX推進の足踏み状況やITインフラ構造の問題を把握することが難しい。そこで、情報システム部門に対し「閉じた工場ネットワーク」の警鐘を鳴らす役割を担うのが、DX推進中核部門である。この組織は各事業のDX推進において生じている各種問題を吸い上げる役割があり、事業部単位で必要となる。また、ITインフラ領域の問題も取り扱う担当が含まれている必要がある。

なお、どの事業部のDX推進中核部門がITインフラに関する問題を掘り起こしても、「閉じた工場ネットワーク」という共通的な問題に行き着く。よって、先行したDX推進中核部門のITインフラに関する問題分析結果は、他事業部門にも横展開することができる。事業部門別での個別検討・個別最適にならないようにするために、ITインフラ改革のプロジェクト体制には「全社生産戦略を担う統括企画部門」が体制のトップに入ることが望ましい（図4）。

とはいえ、DX推進中核部門はITインフラの理解度が不足気味である。そこで登場するのが、日頃からITインフラ全般を構築・運用し、その実態を最も掌握しているITイン

図4　ITインフラ改革推進体制モデル



フラベンダーである。ユーザー系IT子会社は最もこれに近い立場にある。日頃から現場の声に耳を傾け、DX推進におけるITインフラにかかわる問題を収集・整理し、現場がどれだけ新しい取り組みに難儀しているのか、DX推進中核部門へありのままを伝えてもらいたい。DX推進中核部門が「ITインフラ改革が必要であること」を認知できれば、そこからITインフラ改革は大きく動き出す。

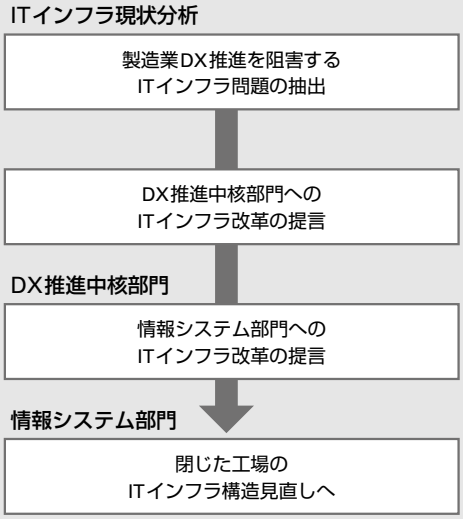
本社側情報システム部門、情報セキュリティ部門、製造現場を巻き込んでのITインフラ改革に向け、問題分析からアクションプラン策定、そして「つながる」を前提とした情報セキュリティ基準の見直し、それに基づくITインフラ構造の再構築といった大きな流れにつながる。

実際、筆者がDX推進中核部門に提言するために行った事前情報収集では、あるメーカーのグループ企業の現場レベルで横断的にヒアリングを実施した。その際、DX推進のボトルネックとして、ITインフラ構造・情報セキュリティ基準の制約、管理組織の分離に伴う個別最適といった共通的な問題があることを整理し、これらをステークホルダーとの共通認識へ引き上げるまでに1年以上を要した。その後、DX推進中核部門へのプレゼンテーションの機会を得て、ITインフラ改革がDX推進に向けて必要不可欠であることを広く理解してもらった。

当時の顧客は行動が早く、翌月には関係部門を集め、「閉じた工場構造」の見直しに必要なプロジェクト体制が議論された。さらにグループ各社へヒアリングを行い、「閉じた工場構造」がDX推進における共通のボトルネックとなっていることも再認識された。しばらくして、全社生産戦略を担う統轄企画部門をトップに、DX推進中核部門、情報システム部門、セキュリティ担当、そして問題提起を行ったNRIシステムテクノでITインフラ改革に向けたプロジェクト体制が組まれることとなった。

図5は、製造業DXにおける阻害要因の三すくみ構造にメスを入れ、ITインフラ改革に導くためのステップである。起点となる活動は、自社の現状を最もよく理解しているITインフラ運用を担うITインフラベンダー

図5　ITインフラ改革のステップ



やユーザー系IT子会社がふさわしいが、コンサルティングなどによるDX推進の阻害要因分析アプローチも考えられる。

Ⅲ 攻めの情報セキュリティ基準・ITインフラ実装に向けた実践ポイント

1 つながるリスクを極小化するために

2017年３月に経済産業省が提唱した「Connected Industries」を、工場のOT系ネットワークに当てはめた場合、何が求められるのか。これは、OT系ネットワークが外部と自由に、双方向に通信できる環境を目指すという話ではない。

OT系ネットワークをデザインする上で、最も重要なのは可用性の担保である。21年５月、米石油パイプライン大手であるコロニアル・パイプラインがサイバー攻撃を受け、全米への石油移送が一時停止となった報道などもあり、OT系ネットワークの「高可用性のための分離」と「DX推進のための接続」という相反する要件を満たすことがいかに難しいかをあらためて感じさせられた。製造業DXに適したITインフラ構造を考える上では、サイバー攻撃がどこから来るのかを想定した上で、製造業DX推進で必要となる通信の方向性・通信先・プロトコルなどを洗い出し、現実解を導き出す必要がある。

OT系ネットワークの特徴として、高可用性担保のために、端末のウイルススキャンや各種パッチの適用なども受け入れられない状況を先に述べた。さらに現場担当者の心理として「外部と接続していないので、OT系は攻撃を受ける心配がない」という勘違いをされているケースも非常に多い。メンテナンス端末やUSBメモリーなどでOTネットワーク内部に持ち込まれるウイルスに対しては、無防備であることを理解しておくべきだ。

OT系ネットワーク特有の問題ともいえる「OS・アプリケーションなどの脆弱性の存在」を織り込んだ上で、製造業DXでデータ利活用を実現するにはどうしたらよいか。ここからは実装ポイントを述べる。

2 まずは分析基盤への「データアップロード」の実現を目指す

製造業DXでまず必要となるのは、クラウドなどにある分析基盤への「データアップロード」の実現である。

もし、「旧来からの情報セキュリティ基準」に抵触するようであれば、ここからの見直しが必要となる。従来なかった業務要件として、「工場内の各種データを分析基盤へ送る」を大前提に置き、これに対応した情報セキュリティ基準策定が必要である。

ITインフラ構造の観点では、高可用性を重視するOT系ネットワークにインターネット接続点が存在しないことが一般的である。仮にクラウドへのデータアップロードを考えた場合、その経路として「IT系のLAN・WAN・Webプロキシなどの流用」を思い浮かべるかもしれない。しかし、２点の理由からIT系のITインフラ管理者との折り合いがつかないことが予想される。

１点目はOT系トラフィックのアップロードによる、IT系WANのトラフィック逼迫懸念である。将来的なOT系のトラフィック流

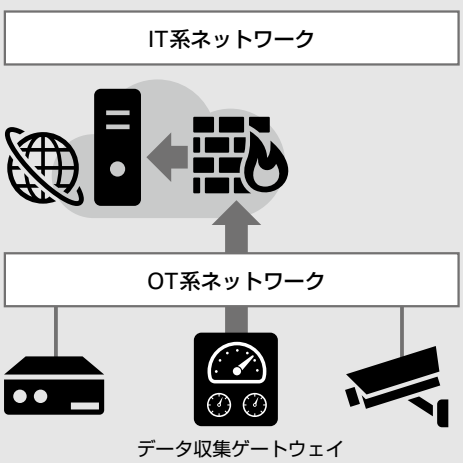
量は予測が難しく、IT系のITインフラ管理者としては「基幹システム・IT系サービス」保護の観点からOT系のトラフィックは受け入れ難い要素となる。

２点目はOT系が求める可用性を、IT系ネットワーク環境で担保することが難しい点である。IT系では計画的にネットワーク機器の老朽化対応を行う。ここでは「ネットワーク停止」も伴う機器交換や増強作業が実施される。一般的にIT系の利用者に配慮し、休日・夜間作業として計画が組まれる。ところが、OT系の通信要件が休日・夜間でも停止できない要件だとすれば、IT系ネットワークのメンテナンス調整が難しくなり、IT系のITインフラ管理者としては、OT系の通信を受け入れることが難しくなる。先述の通り、IT系とOT系でITインフラの管理組織・管理区分・予算・責任などが分離しており、２点の理由でも示した通り、「IT系のLAN・WAN・Webプロキシなどの流用」は難しい。

そこで、OT系データの分析基盤へのアップロードの実現に向けては「OT系専用の分析基盤向けネットワークの整備」が考えられる。図６に示した通り、まずはIT系ネットワークに依存しないOT系専用の単独インターネット接続点（光回線やモバイル回線）を設ける。

会社で認められたクラウド上の分析基盤にデータをアップロードする場合は、VPNや認証機構など、適切な情報セキュリティ対策を組み合わせ、OT系の専用ゲートウエイからのデータ送信は許可する。工場のデータをクラウド上の分析基盤へ送り届けるための要件を、情報セキュリティ基準に重要な業務要件として織り込むことができれば、ITインフラ設計や情報セキュリティ対策の具体的な検討へ進むことができる。

図6　分析基盤に向けたOT系専用通信経路（例）



3　サイバー攻撃から守るために

過去のIoTデバイスなどの情報セキュリティインシデントの傾向を見ると、当該機材がインターネットから直接アクセスできる環境に配置され、かつ初期パスワード、あるいは容易に推定できるパスワードによって侵入されるケースが多い。図６で示した構成例では、データ収集ゲートウエイがインターネットから直接アクセスされることがないように、ファイアウォールの内側に配置されている。従来の「閉じた工場ネットワーク」の常識を捨て、OT系に配置したデータ収集ゲートウエイから分析基盤などへのアップロードの限定的許可といったデザインは難しい話ではない。なお、インターネットを含む外部ネットワークからの接続要求は、遮断が大原則である。

ここからは、OT系ネットワークの内部構造について述べる。OT系LANは単一セグメ

ントで構成されている企業も多いと思われる。元来、OT系ネットワークは外部ネットワークと分離してきたため、情報セキュリティ観点でOT系ネットワーク内をさらに分割する必要性がなかった。ところが、昨今のOT系では単一セグメント構造によるリスクが高まってきている。OT系でもWindowsなどの汎用OSの利用が拡大傾向にあり、ウイルス対策を施せないというOT系特有の問題も拡大傾向にある。これが単一セグメント環境下に収容された場合、容易にOT系ネットワーク内部でウイルスを拡散することができる。「OT系は閉じた工場ネットワークなので安全である」という認識は過去の工場セキュリティインシデント事例が語る通り、誤りである。製造業DX推進に向けたITインフラ改革を検討される際は、OT系内部で相互に通信要件の端末については、ネットワークを分割（ゾーニング）するなども併せて検討されたい。

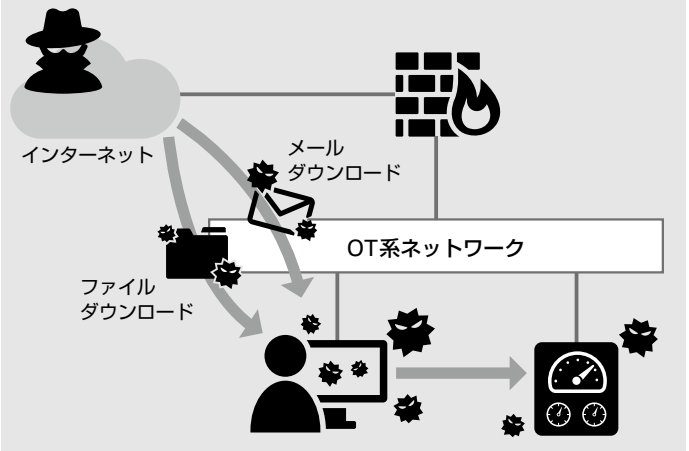
4　ミスオペレーションによるマルウエアを呼び込まないために

独立行政法人情報処理推進機構（IPA）の「情報セキュリティ10大脅威 2021」によると、「組織」向け脅威の第1位が「ランサムウエアによる被害」、第2位が「標的型攻撃による機密情報の搾取」となっている。これらの攻撃の手口としては、社内の関係者にウイルス付きのメールを開封させて当該端末を感染させる、あるいは標的組織が頻繁に利用するサイトを調査の上で改ざんし、不正なサイトに誘導することで当該PCがマルウエアに感染させられる。いずれも人を油断させ、マルウエアを「呼び込む」ように仕掛けられている。そして今も、インターネットアクセス可能な環境と意図しない人のオペレーションの組み合わせにより、ランサムウエアの被害はとどまることを知らない。

先に製造業DX推進に向けてインターネット接続点を専用に設けることについて触れたが、汎用OS端末によるブラウジングや電子メールを受信する環境を、OT系ネットワーク内に構築してはならない（図7）。

業務メールのごとく巧妙に仕掛けられた添付ファイルにマルウエアが入っている可能性を考えれば、脆弱性を消すことができないOT系ネットワーク内において、マルウエアを呼び込む可能性がある端末環境を用意してはならないのはいうまでもない。「便利だから」といった感情に流されないためにも、情報セキュリティ基準でこういった事項も明示しておくべきである。

図7　OT系に入れてはいけないメール・ブラウジング環境



5　製造業DX推進のためのITインフラ改革に向けて

本論考では、高可用性を求めるOT系ネットワーク固有の事情から、OT系ネットワーク・管理部門が分離され、情報セキュリティ基準も含めた三すくみ構造が製造業DXの大

きな阻害要因であることを述べた。もし、あなたが自社工場のDXが遅々として進まないと感じているならば、DX推進中核部門へこの質問を投げかけてほしい。

「工場の各種データをクラウドに送信できるか」

もし、「NO」もしくは「分からない」が返ってきたならば、従来の「閉じた工場ネットワークの常識」にとらわれている可能性が高い。経営戦略上でDX推進が必要不可欠と感じているならば、まずは足元のITインフラ構造見直しの狼煙を上げてほしい。ITインフラ改革に踏み込み、分析に必要なデータがクラウド上の分析基盤に到達できるようになれば、生産技術・生産戦略担当が本来求めていた、クラウド環境でのデータ解析などが動き出す。製造業DXの推進により、先進的な製造プロセスなどが生み出され、人に依存せず効率的・高品質な生産が実現するだろう。

参考文献

1　経済産業省「令和元年度ものづくり基盤技術の振興施策　第201回国会（常会）提出」
https://www.meti.go.jp/report/whitepaper/mono/2020/honbun_pdf/pdf/all.pdf

2　独立行政法人情報処理推進機構セキュリティセンター「情報セキュリティ10大脅威 2021」
https://www.ipa.go.jp/files/000088835.pdf

著者

櫻井　望（さくらいのぞむ）
NRIシステムテクノ 基盤システム事業部統轄
専門は製造業DX推進支援、ITインフラセキュリティ診断など