可視化からはじめる製造現場のサイバーリスク対策

富士通株式会社
岡本　登

1．はじめに

いま、製造業は大きな変革を迫られている。ITを活用した新たなイノベーションを目指す一方で、新型コロナウイルスなどの感染症と経済打撃に立ち向かわなければならない。これまでにも国内経済は、オイルショック、バブル崩壊、リーマンショック、東日本大震災と幾度となく危機的な状況を乗り越えてきた。製造現場では、基本に立ち返り、やるべきことを徹底して行うための管理を中心に仕事の見直しが推し進められた。あらたな脅威が現れれば、愚直とも言えるほど改善を積み重ねて乗り越えていくことが日本の強みではないだろうか。

しかし、残念ながらサイバーリスクに対する取り組みはまだまだ低調だと感じる。ここ数年、多くの工場の実態を見てきたが、工場内のネットワークインフラ基盤は過去からあまり変化することなく、改善の余地がかなりあると言える。

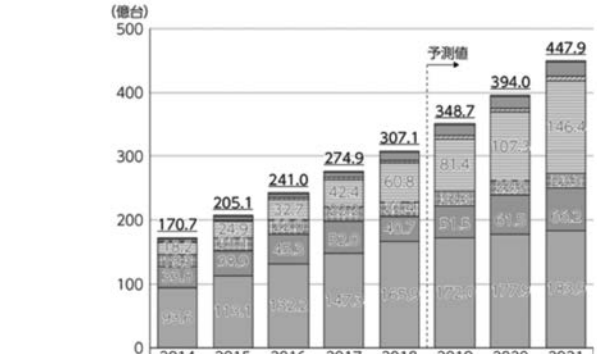
本稿がサイバーリスクは感染症と同じく、今、対策をしておかなければならないリスクであると認識をしていただくきっかけになれば幸いである。

2．10年以上遅れている実態

情報系環境（OA環境）におけるセキュリティ意識と対策はかなりのレベルまで成熟してきていると思われる。それでも、完璧な防御はあり得ないため、侵入後対策としてのレジリエンス強化が注目されている。一方、製造現場では、2005年に外部から持ち込まれたパソコンをネットワークに接続したことが原因で工場設備がウイルスに感染し、自動車製造工場（海外）が停止するという事故が発生しているが、2017年のWannaCry流行時には、これと同様の原因で工場が停止する被害が出ている。この実態から考えると、セキュリティ対策はここ10数年は進化していないと言える。

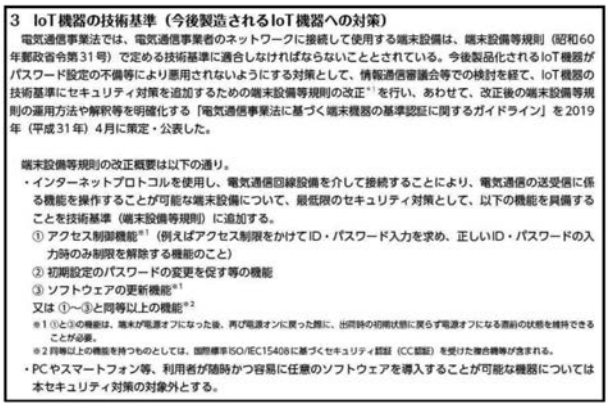
ウイルスやワームなどのサイバー脅威は技術的にも高度化され、より強力に変化している。しかし、これが理由で製造現場が被害を受けているわけではない。WannaCryの場合、感染後の動作は高度ではあるが、情報系環境であれば最初の感染は十分に防げるレベルだと思われる。また、仮に誰かの端末が感染したとしても他の端末が基本的な対策を施していれば拡散する可能性は低い。しかし、製造現場に感染したパソコンを持ち込まれたら、WindowsOSで動作している工場内の装置は無対策のため全滅する可能性が高い。実験によると、WannaCryは5、6秒で50台程度の端末に最初のアクションを起こすことが分かっている。

製造現場での活用が期待されているIoT機器に関しては、その脆弱性が話題になることも多く、最近の情報通信白書でもIoT機器のセキュリティ対策が取り上げられている。



	2014	2015	2016	2017	2018	2019	2020	2021
	170.7	205.1	241.0	274.9	307.1	348.7	394.0	447.9
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.03	0.04	0.05	0
自動車	3.8	4.7	6.0	7.5	13.5	16.6	19.1	22.0
医療	2.0	2.3	2.8	3.4	3.9	4.8	5.9	7.1
産業用途	18.2	24.9	32.7	42.4	60.8	81.4	107.3	146.4
コンピュータ	19.3	21.1	22.0	22.2	22.4	22.3	22.3	22.3
コンシューマ	33.8	38.9	45.3	52.0	40.7	51.5	61.5	66.2
通信	93.6	113.1	132.2	147.3	165.9	172.0	177.9	183.9

図1．世界のIoTデバイス数の推移及び予測
（総務省　令和元年版　情報通信白書より）



3　IoT機器の技術基準（今後製造されるIoT機器への対策）

電気通信事業法では、電気通信事業者のネットワークに接続して使用する端末設備は、端末設備等規則（昭和60年郵政省令第31号）で定める技術基準に適合しなければならないこととされている。今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、情報通信審議会等での検討を経て、IoT機器の技術基準にセキュリティ対策を追加するための端末設備等規則の改正*1を行い、あわせて、改正後の端末設備等規則の運用方法や解釈等を明確化する「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」を2019年（平成31年）4月に策定・公表した。

端末設備等規則の改正概要は以下の通り。

・インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

① アクセス制御機能*1（例えばアクセス制限をかけてID・パスワード入力を求め、正しいID・パスワードの入力時のみ制限を解除する機能のこと）

② 初期設定のパスワードの変更を促す等の機能

③ ソフトウェアの更新機能*1

又は①～③と同等以上の機能*2

※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。

※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証（CC認証）を受けた複合機等が含まれる。

・PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

図2．IoTセキュリティ対策の推進
（総務省　令和元年版　情報通信白書より）

一方、工場内の既存装置は使用年数も長く、現在もなお、数多くのWindowsXPが動いている実態にも目を向けるべきではないだろうか。

3．脅威に負けないために必要なこと

サイバーセキュリティ対策のリファレンスとして国内でも活用する企業が増えてきたNIST サイバーセキュリティフレームワーク(CSF)では、リスク管理を識別、防御、検知、対応、復旧の5つの機能で定義している。CSFに関する解説は別の機会に譲るとして、ここでは、この5つの管理機能に沿って、製造現場の課題とサイバーセキュリティ対策を考察してみる。

①識別

工場内のネットワークに接続されている端末や装置は確実に把握できているだろうか?これまで多くの工場を見てきた経験から、資産管理が非常に弱いと感じている。リスト化された機器一覧は最新化されず、実態調査を行ってみると管理者も知らない端末が見つかることもある。また、工場内ネットワークの管理もかなり怪しい。セグメント化されずに数珠つなぎで延長されたLANが工場内に張り巡らされている状態では、端末や装置がどこに繋がっているのかを人手で的確に把握し、維持管理することはきわめて難しい。

従って、考慮すべき対策としては、やはり資産管理の徹底ということになるのだが、これを属人化あるいは形骸化させないためには人手を介さずにすべてを自動で行えることが重要である。このような機能を持つ製品も数多くあるが、工場内ではネットワークアドレス部が想定外なIPアドレスを持つ端末が存在するケースもあり、漏れなくすべてを拾い集めて可視化できることがポイントになる。

②防御

工場内への脅威の侵入口はそれほど多くはない。情報系環境のように、個人の端末からのメールの送受信やWEBサイトを閲覧するようなことはないため、外部ネットワークとの接続がない場合に想定される侵入口は、工場LANへの直接接続か工場内機器へのUSBメモリー挿入に絞られる。しかし、これらを規制することは工場運営上かなり難しい。また、保守用ネットワークや情報系ネットワークなどの外部ネットワーク接続がある場合でも、意図しない工場の稼働停止を避けるなどの理由から、その境界にFWなどが導入されていないか、設置されていても工場を脅威から守るための防御設定が適切ではないことが多い。

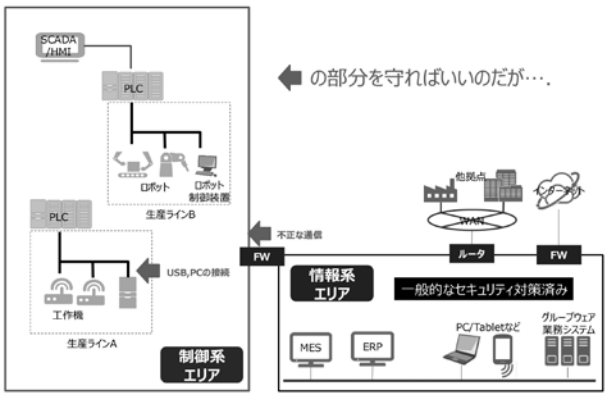


図3．工場セキュリティの防御ポイント

パッチ適用やアンチウイルス対策などのエンドポイントセキュリティ対策が導入できない事情も併せて考えると、残念ながら既存ネットワークに大きく手を加えることなく適用できる有効な防御策は少ない。それでも何

らかの製品導入を検討する際は、考え得るリスクシナリオをしっかりと検証することが重要である。

③検知

工場内に侵入したサイバー脅威を検知する仕組みはほとんど導入されていない。工場内通信は情報系環境のようなクライアントとサーバーもしくはクラウドとの通信のように垂直的で経路が集約されるようなものよりは、装置間などの水平的な通信の方が多いため、ネットワーク上の検知機能を効率的に配置することが難しい。また、工場内装置が何らかのマルウェアに感染したとしても、工場の操業に直接的な影響を与えない場合もあり、表面的な事象として認識できないこともある。実際に、情報持ち出しの機能を持つワームに感染した工場を調査する機会があったが、時々トラフィックが増大する程度で操業にはほとんど影響が見られなかった。(増大量によってはチョコ停が発生する可能性はある)

検知対策として最も単純な方法は、工場内LAN通信をすべてキャプチャし、リアルタイムに分析することである。一般的にはリピータハブにキャプチャー装置を繋ぐ方法とスイッチのミラーリング機能を使う方法があるが、工場に導入されているネットワーク装置の多くはミラーリング機能を持たない単機能なスイッチであり、両者とも対応できない。また仮にミラーリング機能を持つスイッチが導入されていたとしても、すべてのキャプチャデータを採取するには、データ量やキャプチャ装置の配置に課題が残る。そこでもう少しハードルを下げた別の方法を以下に示す。

工場内通信は比較的パターン化されているので、このパターンの崩れを可視化することができれば、ワームの拡散活動の検知などに有効であることが実験的に分かっている。スイッチにはポートを流れたデータをカウントする機能を有するものもあり、これを短い時間間隔で採取し、前日、前週、前月などのデータと比較すれば、特異点を見つけることができる。さらに通信フローデータを分析できれば、より精度の高い異常検知が可能になる。ただし、この場合でも、ネットワークの構成は変わらないが、インテリジェントスイッチへのリプレースは必要となる。

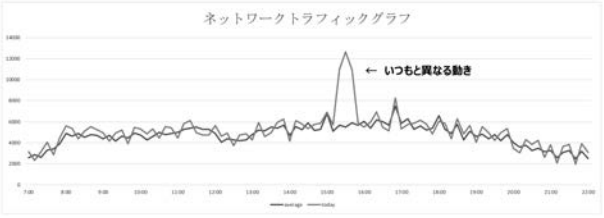


図4．トラフィック変化の可視化

④対応

リスク低減のために拡大を防ぎ、影響を緩和し、インシデントを解決に導くためには、早期対応が重要である。もちろん対応のためには検知できることが前提となるが、ここではその前提をクリアしたとして話を進める。

情報系環境では、端末のマルウェア感染が検知されると、直ぐにネットワークから切り離すことが推奨されている。しかし、工場系環境では、感染装置の特定そのものが難しいことに加え、仮に特定できたとしてもネットワークから切り離す判断は容易ではない。なぜなら、この1台を停止させるとライン全体が止まってしまう可能性もあるからだ。稼働に影響がなければ動かし続けたいと考える工場関係者も多い。

そこで検知情報を元に的確に対応するためには、あらかじめサイバーリスクに合わせたBCPを検討し、手順を可視化しておく必要がある。中でもWannaCryのようなワームは、無防備な工場内装置に対して短時間のうちに感染を広げるため、被害を最小限に抑えるためには素早い行動が求められる。この場合、BCPに従って人が判断し対応するスピードでは間に合わない可能性もあるため、人に代わってネットワークシステムとして自動的に遮断するような仕組みの検討も必要である。

⑤復旧

早期復旧のためには、被害範囲が特定でき、BCPなどで復旧プロセスが明確になっている必要があるが、そもそも現在のBCPは自然災害や火災などを想定したものであり、サイバーリスクを考慮したものではない。ワーム感染によって工場が全停止に至った場合、復旧後に1台でも対応漏れが残っていると、数時間後には再度同じことが起こるということを考慮しなけれ

ばならない。従って、作業効率的な手順だけでは復旧はできない。

工場内の装置はパソコンのようにマルウェアチェックを行うことが難しく、簡単に感染の有無を識別することはできない。一方で全装置を初期化あるいは入れ替えるという方法では大きなコストが発生する。感染範囲を絞り込むには、資産管理情報の装置OS種別を活用する方法や通信パターンの崩れから被害エリアを推測する方法などが考えられる。しかし確実ではないため、ブロック毎に高機能なスイッチを仮置きしながらキャプチャデータで状況を可視化し、徐々に復旧範囲を広げるなど慎重に進めて行く必要がある。なお、先の検知、対応が適切に機能していれば、被害範囲が最小限に抑えられることは言うまでもない。

4．製造業の未来のために

一つの製品の生産には多くの企業が関係している。今後、サプライチェーンのすべてでスマート化が進めば、製造現場の効率化やデータ活用は飛躍的に高まることになるが、一方で相互の依存度も高くなる。従って、製造現場のリスクマネジメントはひとつの工場だけの問題ではない。サプライチェーンのどこかで問題が発生すれば、その影響は全体に大きく波及する。例えば、先般の大雨による一部地域の浸水被害は多くのIT機器製造に影響を及ぼした。

日本の製造業はもちろん大企業だけではない。多くの中小企業や町工場に支えられていることを考えると、彼らを巻き込んだ形でリスクマネジメントを進めて行かなければならない。

ここまで製造現場の現状とサイバーリスク対策について述べてきたが、自然災害と違いサイバー脅威は弱者を襲う。新型コロナの影響などにより経済環境が厳しくなるなか、対策に大きな投資は難しいが、今できることから始めないと日本の製造業の未来は危ういのではないだろうか。

セキュリティ視点において、情報系環境との10年のギャップは簡単には埋まらない。しかし製造現場の情報化はどんどん進んでいく。高度化された工場が砂上の楼閣とならないようにすぐにでも行動を起こすべきである。

＊執筆者プロフィール

富士通株式会社
岡本　登（おかもと のぼる）
ネットワークサービス事業本部
シニアマネージャー
okamoto.noboru@fujitsu.com