INTRO FEATURE 01

IoTセキュリティの潮流

Trend of IoT Security

IoT技術の発展がもたらす「第4次産業革命」

IoT(Internet of things／モノのインターネット)の登場は人類史における産業の構造を大きく変化させようとしている。モノとモノがインターネットを介して有機的につながることで、機械が人の手を離れ、機械だけで材料の確保から製造までを行う産業の完全なオートメーション化が実現しようとしているのだ。IoT技術を用いた、この産業構造の抜本的な変革は「第4次産業革命」と呼ばれている。

第4次産業革命は、もともとドイツで提唱された概念である(ドイツ語では「Industry 4.0／インドゥストリー4.0」と呼ばれる)。

Appleに代表されるアメリカのグローバル企業が世界を席巻し、自国内のIT関連産業育成が不十分であることを認識したドイツでは、産学官が一体となって次世代的な生産体制の構築を目指しているのだ。その一環に、IoT技術を用いた生産体制そのものが変革を求められたかたちだ。

「知性の革命」、主役は「自ら集め、考え、生み出す工場」へ

IoT技術の活用による生産のオートメーション化。このプロセスを最大まで突き詰めた生産工場は「スマートファクトリー」と呼ばれる。これは「自ら集め、考え、生み出す工場」と言ったところだ。旧来的にコンピュータが得意とした情報の集積、そこにIoT技術が組み合わさることで、工場内の各セクションで集積したビッグデータを有機的に分析、活用することができるようになる。そうなれば、もはや生産ラインは不測の事態にも人の手を借りずに自ら考えて稼働し続けることができる。

それゆえ、イギリスで始まる第1次産業革命や19世紀後半の大量生産化の進展(第2次産業革命)が蒸気機関や電気の使用など「動力の革命」であったなら、20世紀後半に入って発展したIT技術の活用(第3次産業革命)や一歩進んだIoT技術による第4次産業革命は人類の生産史における「知性の革命」と呼べるものなのかもしれない。

欧米の企業はこぞってIoT技術の積極活用に取り組んでいる。自動車産業は代表的な例だが、それはイメージのしやすいGPSによる自動運転システムのようなコンテンツとしての活用だけではない。IoT技術によって、世界中で生産体制そのものが変わろうとしているのだ。

「つながる工場」とは？

「つながる工場」はIoT技術が押し進める第4次産業革命のキーコンセプトだ。文字通り工場に関わるすべてのモノ、事、人がつながることを表している。工場単位の機器類、設備、各セクションはもちろん、各工場間の連携、設備の調達先の技術者と工場の作業員、さらには生産者としての工場と消費者までのつながりといった工場にまつわるあらゆる「つながり」を包括する概念だ。

では「つながる工場」とは具体的に何をどう変化させるものなのだろうか？

生産体制とその先にある産業構造そのもの

工場内の設備や機器類がIoT化することで、種々の情報をクラウド上で集積、分析することができるようになるのはイメージしやすい。そうすることで生産はより効率化していくだろう。また、エンドユーザーとのつながりが、IoT技術により見える化することで需要と供給のバランスも把握しやすく、生産リスクの回避につながるかもしれない。「つながる工場」の実現によるこれら生産体制に関わる変化は大きい。しかし、「つながる工場」が産業に与えるインパクトはそれだけではない。

もっとも大きな変化は工場(企業)間の連携がより柔軟に変化することであると言えるだろう。これまで、サプライチェーンにおける企業間の関係は生産されたモノを介した売買が中心であった。しかし、「つながる工場」では生産プロセスそのものが取引の対象になり得る。部品だけのやり取りではなく、中間品のやりとりや最終的には製造のプロセスを別工場一部委託するという形での取引が実現するだろう。

これまでの生産構造は、素材を納品する中小企業、買い取る大手企業といった形での取引がメインであり、価格決定における買い手の権限が大きかった。しかし、製造プロセスそのものを一部委託することになれば、取引の柔軟性は増し、技術に長けた中小企業がサプライチェーン全体の中心となる可能性も高い。そうなれば、エンドユーザーが求める個別のニーズにもサプライチェーン全体で対応していくことが可能になる。

IoT化の実現で変わるのは効率化といった産業の体制だけではない。「つながる工場」では産業構造そのものが変わろうとしているのだ。

INTRO FEATURE 02

IoTセキュリティの課題と将来

Challenges and Future of IoT security

IoTセキュリティの課題

これまで、IoT分野の技術開発に熱心だったのは物流の分野だった。しかし、第4次産業革命が銘打たれて後の世界的な潮流を見ると、その主たる利用者となるのは製造業だ。

製造の現場、工場はこれまで閉じた世界だった。工場内で作動する個々の器機が外部ネットワークとつながることはなかった。そのため、そもそも工場ではネットワークセキュリティの必要性がなかったのがこれまでだ。しかし、IoT化する中では、工場内で発生するあらゆるデータを本社系ネットワークやクラウド上で管理することになる。そうなると、工場はもはや閉ざされた空間ではなくなる。だからこそ、製造業の各現場は、IoTセキュリティに対する意識をしっかりと持っていなければならない。

工場がさらされる脅威

工場には多くのPLCが存在するが、もともとセクションごとに独立していたPLCも、IoT化で有機的につながっていくことになる。

そのつながりは工場内の横のつながりだけでなく、他工場や本社系ネットワークなどを介する外部ネットワークとのつながりも含むものになる。

そうなると、マルウェアが外部ネットワーク経由で侵入することで、末端にある工場内のリアルタイム系OSがハッキングされて、人命に関わる事故が発生したり工場の操業が停止したりといった可能性もあらわれ、工場が様々な脅威にさらされるため、会社全体で背負うリスクにもなる。

作動するOSの特殊性対策が難しいものが多い

ここで課題となるのは、工場で作動する組み込み系のOSは特殊な構造をしているということだ。中でもリアルタイム系のものはその構造がメーカー毎に独自で、メモリ容量も必要最小限になっている。また常に稼働し続けていなければならないという問題もある。そうなると、いざ脅威にさらされたときに、マルウェアを除去するためのセキュリティソフトを導入することが難しくなる。現実的な課題として、既存の組み込み系OSに外部からの脅威を除去するセキュリティソフトをウィルス感染後に導入することは不可能なのだ。IoTセキュリティの課題はまさにこの部分に存在することになる。

IoTセキュリティの将来像

IoTセキュリティの課題は導入する工場内で使用される組み込み系OSの特殊性にある。では、これにはどうやって対処してゆけばよいのか。IoTセキュリティの将来像となるのは、エッジサーバー内のセキュリティ強化だ。

そもそも工場の末端にある各組み込み系OSに対して個別にセキュリティ対策を施すことは現実的ではない。毎日かなりの種類が生み出されるウィルスにそれぞれ対策を講じていては時間もコストもかかる。そのため、工場におけるIoTセキュリティはネットワークの入り口になるエッジサーバーに強固な壁を築き、そこでマルウェアをシャットアウトすることが現実的になってくる。

エッジサーバーは工場のIoT化で欠かすことのできない場所で、本社系のネットワークやデータ管理のクラウドサービス等外部と結びつくだけでなく、工場内の組み込み系OS全体も同じように管理することになる。そうすることで、セクション毎のデータ取集、分析、管理が飛躍的に効率化する。

では、このエッジサーバー内のセキュリティにはどういった未来が待っているのだろうか。

エッジサーバー内で各OSを分離する

まず重要になるのは、エッジサーバー内に取り込んだ各OSの分離だ。AセクションのOS、BセクションのOSを一括で管理するわけだが、それだけではマルウェアの侵入に対して弱すぎる。1つが攻撃されれば、さらにほかのOSにも飛び火する可能性があるからだ。

そこで、エッジサーバー内の各OSを分離させる必要がある。特に本社系ネットワークとつながる場所は、外部からの侵入ルートになるため、他の組み込み系OSから完全に独立させることが大切だ。

さらに言えば、各OSは分離するだけではなく、完全に遮断してしまうことも必要になるだろう。そうすることで、より強固なセキュリティを築くことができる。

エッジサーバー内で各OSを分離し、遮断することで1つのOSへの攻撃をそこまでで食い止めることができるようになる。こういったOSの分離・遮断といった方法などにより、IoT化を実現しながら工場内の要である組み込み系のOSをしっかりと守ることができ、セキュリティ強化を果たした運営が可能になる。

INTERVIEW

IoTセキュリティの世界で勝負する

アドソル日進株式会社
セキュリティ・ソリューション推進部 部長
山西　正則

顧客の厳しいニーズに答えることができる製品

2016年9月に東証第一部に上場を果たしたアドソル日進。工場内のシステムに関するIoTソリューションを得意とする同社は、アメリカLynx社との提携で、国内向けにIoTセキュリティ対策プラットフォーム「LynxSECURE」の販売を始める。成長を続けるIoT界の老舗は、IoTセキュリティに対してどういった考え方を持っているのだろうか。

今回、アドソル日進が日本市場での独占販売権を得た「LynxSECURE」ですが、その特徴はどういったものでしょうか。

セキュリティ商品と言われているものは、ウィルスを検知して駆除するのが一般的なイメージかと思います。ただ、その方法はIoT化を考えたときにはすでに限界が来ています。それを踏まえて、LynxSECUREの特徴は、旧来型の対処療法的なアプローチではなく、システムの基盤に直接セキュリティを入れるところにあります。

アメリカではすでにその価値が認められているそうですが、その理由はどういった部分にあるのでしょうか。

まずはアメリカ国内のIoTセキュリティに対する関心の高さがあると思います。その上で、「LynxSECURE」の製品としての評価は、アメリカ国防総省で採用されている事実からもわかるように、「顧客の厳しいニーズに答えることができる製品である」という点にあるかと思います。

高度なセキュリティであるがゆえに、販売にあたって顧客のOSに適合させることが難しい場合があったりしないのでしょうか。

もちろんあります。工場を例にとると、工場の難しいところは、組み込み系、制御系OSが存在することです。これらはすごく特殊な構造だったり、メモリ容量が小さかったりする場合が多い。ただ、我々(――アドソル日進)はもともとそういったOSの開発、販売を行っていました。知識や経験、そして長年その業務に携わってきた優秀な技術者がいます。さらに、Lynx社とは以前から長期的な協業関係にあるので、システムやOSの中身までソースコードからすべて権利はもらっています。ですから、国内企業のあらゆるシステムの中に製品とのギャップを埋めて導入することができます。

IoTセキュリティの世界でビジネスを行っていく上で一番重要だと考えているのはどういったことになりますか。

IoTの世界は工場に限らず今までつながっていなかったものがつながっていくことになります。そうなるとIoT化を実現するための技術を持ったソリューションベンダーにも、多種多様なプレイヤーが必要になってきます。ITベンダーだけでなく、IoTから派生するあらゆることに対応できるような。だからIoTセキュリティという世界でのビジネスですが、そこでは多様な業種の人たちとつながっていかなくてはいけません。我々が大切にしているのはその部分です。具体的には、IoT化するということは工場内の各設備やセクションだけでなく、本社系ネットワークや分析網とも工場がつながらなければならない。そうなるとその分野(工場外のネットワーク)ではその分野に強いパートナーと強調してやっていく必要があるかと思います。

IoTセキュリティの世界でビジネスを行っていく

なるほど。ベンダー同士もつながっていかないといけない。

そうです。これまで日本のビジネスでは下請けに丸投げするといった階層構造がありました。そういった旧態依然としたビジネスの形はIoT開発には向きません。IoT業界ではものすごいはやさで様々なコンポーネントが登場しています。それを一つの企業だけでキャッチし、市場に出すことは大変難しいことです。だから、様々な分野で個性的な強みを持った小ぶりな企業が横につながって、強みを持ち寄ってやっていくことが非常に重要になります。

今後IoT化する社会で特にセキュリティの問題が重要になってくると予想される分野はどういったところがあるでしょうか。

間違いなく医療分野でしょう。直接人命にかかわる分野でもあるし、個人情報の観点からも大切になります。

具体的にはどういった形のIoT化が進むのでしょうか。

IoTの本質はビッグデータの活用をより効率化することにあります。そうなると、医療の現場で得られたデータの場合は最終的に患者さん個人のカルテとも結びつくことになります。現場で使われる機器を有効に結びつける先に個人情報がある形ですね。だから、これまで以上にセキュリティに対するソリューションが必要になるのではないでしょうか。