FUJITSU

製造業における
セキュリティ最前線

～適材適所によるセキュリティ対策の
ベストプラクティス～

目次

1. 生産現場がなぜサイバー攻撃の対象になっているのか。

攻撃者の視点から狙われやすいポイントと実施しなければならないセキュリティがどの様なものなのか、セキュリティ実装が難しいと言われる要因やその中において有効性のある対策について解説します。

製造業を守るポイントとは何か。テレワークやリモートワークなどにより環境が変わってきている今だからこそ、変化した部分に対してしっかりと対策を打っていくことが重要です。

1.1　なぜ、サイバー攻撃は攻撃者優位であり続けるのか？

サイバー攻撃は攻撃者優位である、と聞かれたことがある方も多いかと思います。しかしなぜ、サイバー攻撃は攻撃者優位 なのでしょうか。ここではその根本的な原因に迫ります。

まず、コンピュータの歴史を深掘りしていきましょう。 まだ、マウスなどがなかった時代に遡ります。1970 年代は、コンピュータを操作する際には、呪文のような「コマンド」を打ち込まなければならない時代でした。1980 年代に入って GUI（グラフィカルユーザーインターフェース）が生まれ、マウスによる操作に変わりました。これにより直感的な操作が初めてコンピュータ上でできたのです。それから現在。時代はDX （ デジタルトランスフォーメーション）が注目されるようになり、現実世界がデジタルの中で拡張されるなど、デジタル技術を駆使して従来になかった革新的なビジネスモデルや価値を生み出し、企業が競争上の優位性を確立していく時代となりました。

コンピュータの進化は良いことですが、進化に伴った課題があります。それは、プログラム量の増大です。プログラム量の増大により、一定の確率でできる穴は無くならないものとなりました。それが、プログラムの欠陥による「脆弱性」に繋がっていったのです。こうした脆弱性は、プログラム量の増大に従って増えていく結果となりました。(図 1)

そして、攻撃者が先に穴を見つけると、誰も知らない脆弱性を突く攻撃が可能となり、防ぐことが難しくなっていったのです。こうしたことが原因となって、守る側としては先回りした対応が困難となっていきました。このような攻撃が、 Zero Day Attack と言われるものです。 こうしたコンピュータの進化の歴史に伴い、現在のサイバー情勢としては攻撃者優位、と言われるようになってしまったのです。つまり、サイバーセキュリティの難しさは、コンピュータの歴史上の課題そのもの、とも言うことができます。

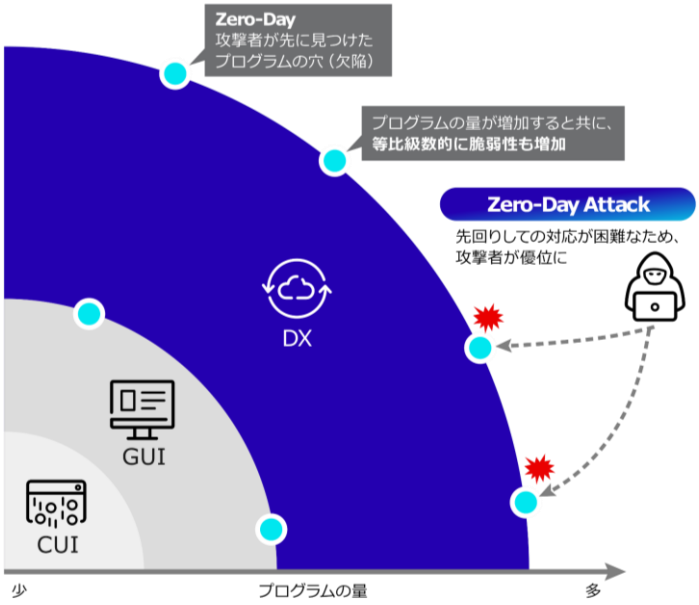

図１：サイバー攻撃が攻撃者優位な要因

1.2　攻撃者の実態

では、実際にはどのような人が、サイバー攻撃を行っているのでしょうか。これはとても様々ではあるのですが、最も多いと考えられている攻撃から考察していきたいと思います。

攻撃者は、何かを欲しくて攻撃する、ということが多いのです。もちろん、政治的な理由による攻撃もありますが、圧倒的に前者の目的における攻撃が多いと目されています。では、攻撃してまで欲しいものとは何なのでしょうか。サイバーの世界では、個人情報などが取り沙汰されることが多いものですが、本当に欲しいものは得たくてもなかなか得られない情報です。では、そうした情報とは一体何なのでしょうか。それは、長い間、研究開発されてきたデータです。つまり、開発データや研究データなのです。研究開発データさえあれば技術的に、時間的に、コスト的に一足飛びできるため、欲しい人にとっては喉から手が出るほど欲しい情報です。

このように考えた時、「開発するより攻撃した方が楽だ」と思った瞬間に攻撃に転じる人が出てくることになる訳です。こうしたことが、製造業が狙われてしまう理由でもあり、その攻撃は海外から行われるものが多く存在します。さらに、脆弱性を自ら見つけるよりも、裏の組織から、つまりダークウェブなどから購入した方が容易なのです。また、誰も知らない脆弱性を探すよりも、既に知られた脆弱性を持つ対象を探し、攻撃することの方が容易なのです。これは、とある元攻撃者からの話ですが、いくつか

攻撃すると成功するものがあるので、あえて難しい攻撃をする必要はない、ということです。そして、最近はマルウェアを自分で作るよりも買った方が楽、というように製作者と攻撃者が分業化されていっています。そして、そもそもマルウェアを使って攻撃するよりも、弱いパスワードを狙う方が楽でもありますので、認証については特に気を付けた方が良い、ということです。

1.3　弱点部分のチェック

このように、攻撃者は楽な方、楽な方に流れていますので、容易に見つかるような弱点を作らない、残さないことがセキュリティにおいては重要です。弱点になりやすいところを、ロケーションごとにチェックしていくということも分かりやすい対策手法の一つです。(図２)

では、ロケーションごとに弱点がないかを考えていきましょう。特に最近はテレワークが普及した関係もあり、自宅におけるセキュリティに弱点があることがあります。また、クラウド化が進むことによって、それぞれのクラウドサービスとその認証部分が弱点となり易くなっています。つまり、端末とクラウドの両方が組織のネットワークの外に移動しているため、ゼロトラストの考え方を活用することも必要となってきているのです。そして、様々な環境の変化に伴い工場などにおいては、実施しなければならない新たな接続への対応も必要となってきています。

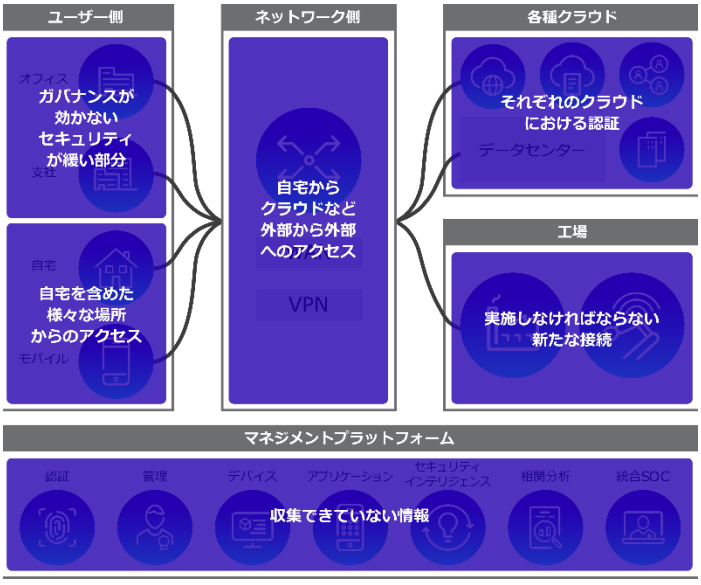

図２：ロケーションごとの弱点

今回のポイント

特に最近は、テレワークなどの影響もありユーザー側におけるエンドポイントの対策状況を今一度見直すこと、それから生産現場などにおいても追加すべきセキュリティがないか、この２点を中心にお伝えしていきます。(図３)

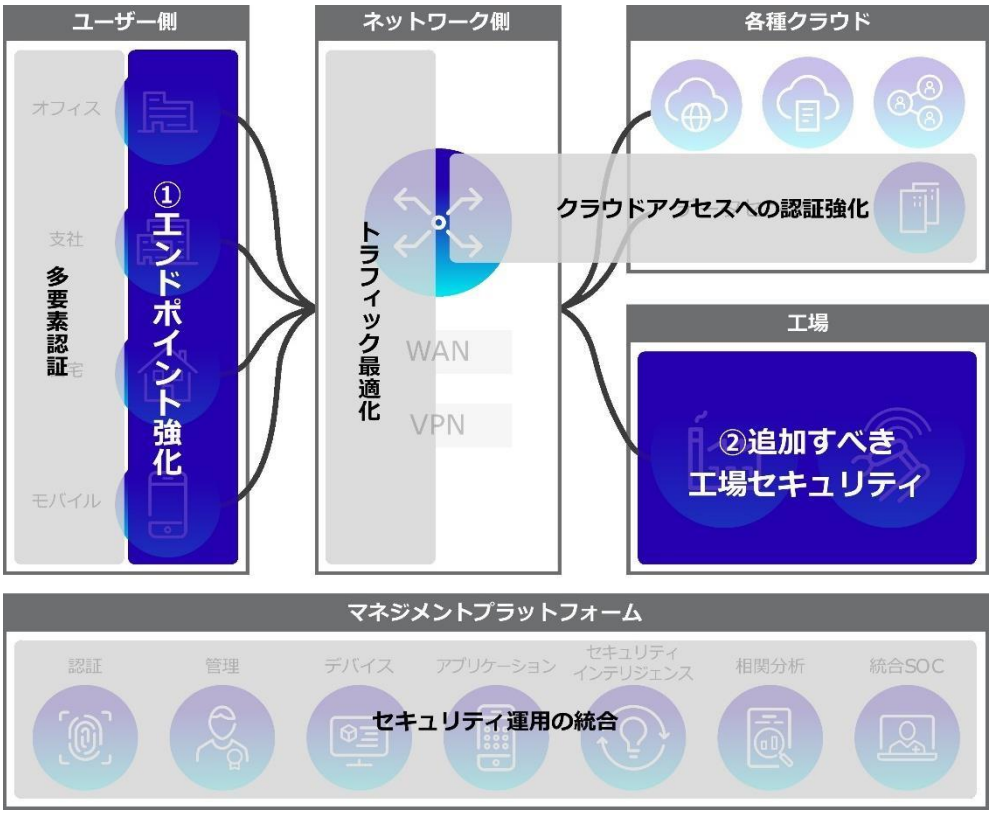

図３：ロケーションごとのセキュリティ

① エンドポイントセキュリティ

エンドポイントに対するセキュリティ強化としては、サプライチェーンやガバナンスが効きにくいところを含めて取り組むことが重要であり、早期にサイバー攻撃を見つけることができる EDR（Endpoint Detection and Response）の導入が必要です。

これを富士通では、お客様の環境・状況に合うものを適切に提供できるようにソリューションをご用意しています。
1つ目は、ファイアウォールや振る舞い検知として有用なパロアルト社の製品と連携することができる**XDRソリューション**で、こちらは既にパロアルト製品を導入や検討しているお客様にお勧めです。
また、富士通の**EDRソリューション**は運用を含めてしっかりと EDR 対策を行いたいお客様にお勧めです。

② 工場におけるセキュリティ対策

工場セキュリティは、セキュリティ実装が難しいところがあります。例えば、セキュリティパッチなどは容易に適用できません。制御ソフトとの相性でパッチの適用や VerUP が困難ということもあり、サポート切れ OS を継続して使用せざるを得ないこともあります。また、アンチウイルスソフトも容易に導入することができません。それは、工場設備の動作連係上において導入不可であったり、そもそもアンチウイルスソフトが対応していなかったりします。

このように簡単にセキュリティ対策を付加しにくいという反面で、リモートで接続が必要になってきているということもあるため、追加の対策を検討することは必要です。 従来の対策は出来る範囲内で実施した上で、新たな対策の検討が必要となってきます。よって、既存の機器、品質に影響を与えない対策と、実施した対策の有効性確認が必要であるところです。そこで、工場セキュリティとしては、２点挙げられます。

まず１つ目はホワイトリスト対策です。ホワイトリスト型で制御を行うことでシステムの負荷を上げない対策が可能となり、現行機器に対し極力、影響を与えず対策を行うことができます。

工場セキュリティの２つ目としては、可視化です。工場内の機器に影響を与えずにセキュリティ強化を行うためには、ネットワークにおける可視化が有効な手段となります。 最近は高度な攻撃も増えてきていることから、このように常に可視化を行い、いつもと何か変わったことがないかを比較することにより、異常を検知していくということが大切です。富士通では、いつもの状態と違う「異常」を検知することにより、**OT ネットワークを監視するサービス**を提供しています。 (図４)

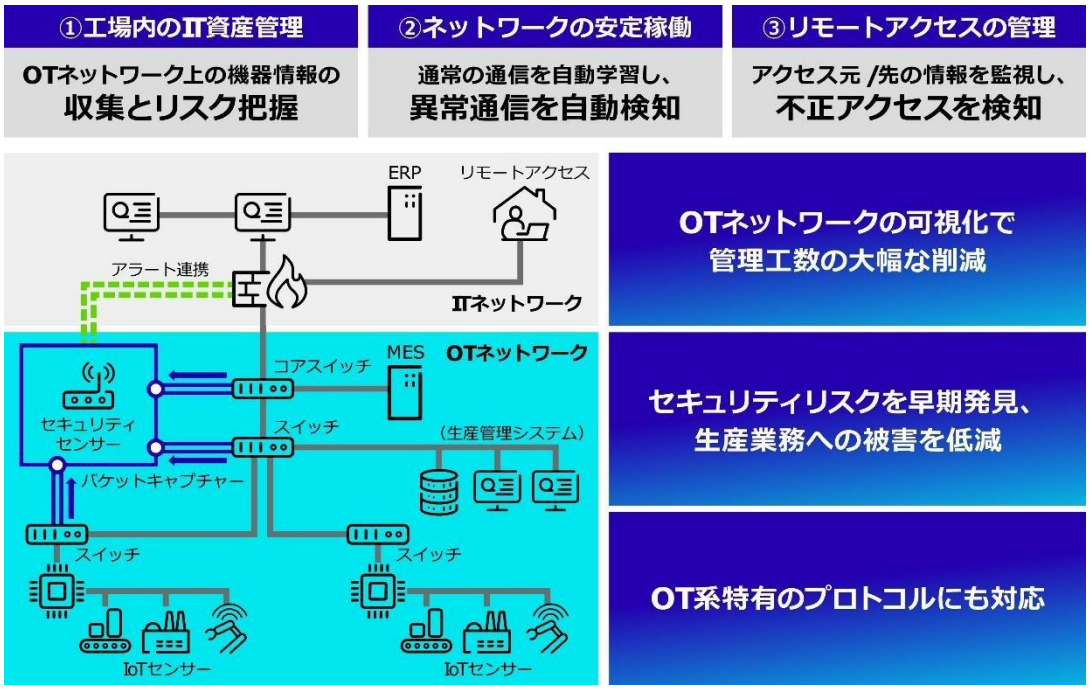

図 4：OT ネットワークの可視化

2. 製造業を守るポイント

まず、全体を俯瞰して必要な対策を打っていくことです。ロケーションごとに整理するなどで分類し、どこに弱点があるのかを洗い出すことも有効です。(図５) テレワークやリモートワークなどにより環境が変わってきている今だからこそ、再点検が必要なのです。次に、そうした中で無理なくできる対策を実施していくことが重要です。一つの対策に予算やリソースを掛け過ぎてしまうと他の対策が出来なくなってしまい、本末転倒ということにもなりかねません。
アフターコロナを見据えた対策をしていくことが大切です。コロナ禍が明ければ以前の通り、という訳にはいきません。変化を的確に受け入れ、その変化した部分についての対策をしっかりと打っていくことが重要なのです。

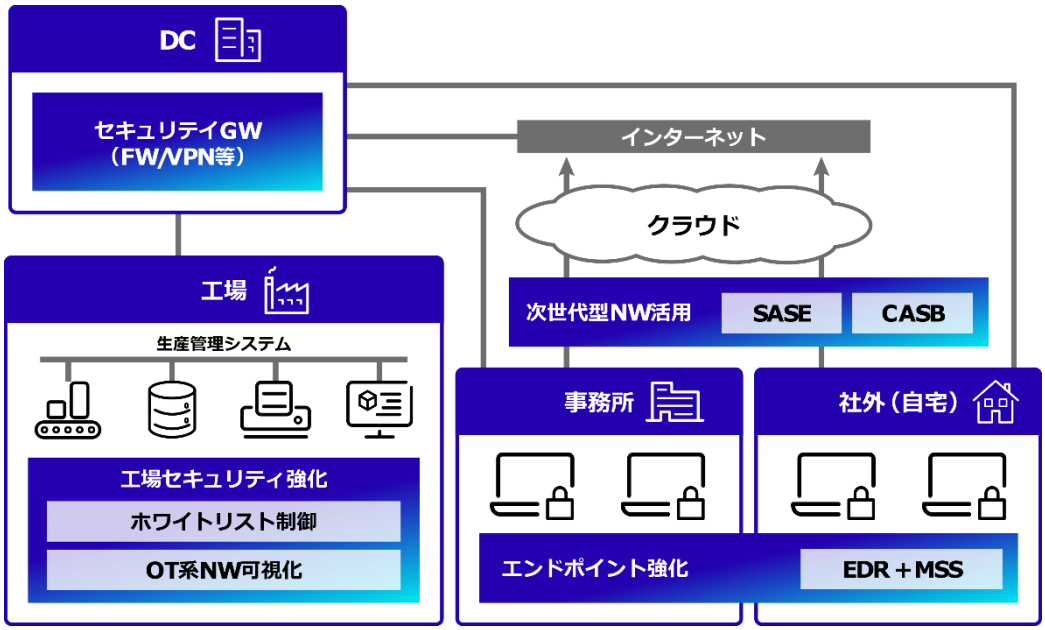

図５：製造業 IT マップ

さいごに

製造業をサイバー攻撃から守っていくためには、全体を俯瞰してそれぞれの特性に応じた適材適所によるセキュリティが必要です。そして、総合的に何をどこから行っていくべきなのか、検討していく必要があります。製造業のセキュリティはこうした対応ができる富士通に、ご相談ください。

[2023年掲載]
本記事中に記載の数値や固有名詞等は掲載日現在のものであり、このページの閲覧時には変更されている可能性があることをご了承ください。

【ご参考】

- ✓ サイバー攻撃から生産現場を守る 早期検知と迅速対応で事業継続を実現
- ✓ リアルタイムでサイバー攻撃の兆候を検知・防御し侵入後の対応も迅速に実現するEDRソリューション
- ✓ 端末やネットワークの挙動から不正な兆候を検知し、高度なセキュリティ運用を実現するXDRソリューション

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中4-1-1

【発行元】富士通株式会社
〒211-8588　神奈川県川崎市中原区上小田中4-1-1