

イスラエル発 産業サイバーセキュリティ ソリューションを提供する SCADAfence

垣貫 己代治

SCADAfence (Japan) 国内事業責任者



シリコンバレーに本社をおき、グローバルにエコシステムを提供するPlug and Play Japanより、同社の「Winter/Fall 2020 IoTプログラム」採択スタートアップである SCADAfence社をJOIに紹介いただきました。

近年、工場などの産業インフラに対するサイバー攻撃のリスク管理が叫ばれて久しい。2017年6月には、欧州を襲った大規模なサイバー攻撃が米国にも拡大、製薬大手メルクや、「オレオ」や「リッツ」で知られる菓子大手モンデリーズも被害を受けました。また、2018年には台湾の半導体大手TSMCもマルウェア感染により生産が一時停止、いずれも被害額は数百億円といわれています。

企業や個人の情報を狙ったサイバー攻撃にとどまらず、工場やインフラの制御システムへの攻撃リスクが高まる今、イスラエル発の産業サイバーセキュリティのソリューションサービスを提供するSCADAfence社の国内事業責任者である垣貫己代治氏に話を聞きました。

これまでの歩み、展開についてお聞かせください

2010年代前半から産業インフラを標的としたサイバー攻撃が増加し、その対策が急務となるなか、2014年にイスラエル国防軍の通称「8200部隊」と呼ばれるサイバーセキュリティ専門部隊出身のエンジニア2人によってSCADAfenceは創業されました。

主な導入実績

- VESTEL（欧州最大の家電メーカー）：17工場にある25000台超の生産設備を集中監視
- 三井不動産：スマートシティでの実証実験を経て他主要施設への展開
- タロ・ファーマシューティカル（大手製薬メーカー）：コンプライアンス対応（FDA）とリスク可視化
- CHS（米国最大規模の石油精製事業者）：稼働資産と工場ネットワークの可視化
- 欧州メーカー（世界販売台数トップ5の自動車OEMメーカー）：潜在的リスクの可視化、ITとOTの連携推進
- 欧州メーカー（世界最大規模の自動車用ガラスメーカー）：生産性の健全性向上と保全予知管理

SCADA（Supervisory Control and Data Acquisition）とは、産業インフラシステムの中心を担う監視制御の機能であり、SCADAfenceには、SCADAを含めた産業インフラ全体をサイバー攻撃から守る、という意味が込められています。

産業インフラの中でも製造業の生産拠点、オフィスビルや公共施設等で使われるビル管理システムなどを対象にしたセキュリティソフトウェアを開発し、2017年の欧州での事業展開を皮切りに、グローバル展開を開始しました。グローバルでは、製造業やビル管理事業、特に業界大手での採用が急速に進んでいます。また、これらの事例をもとに、近しい環境をもつエネルギーや交通インフラなど、社会インフラ関連企業での採用が始まっています。

2017年12月のグローバル・ブレインおよび三井不動産が運営するファンド「31 VENTURES Global Innovation Fund」からの出資をきっかけに、2018年9月に日本国内事業所を開設、2019年4月に日本版サービスを開始、日本市場における本格的な事業展開を始めました。製造業およびビル管理というセグメントに注力しているため、それらの成熟した市場をもつ日本を、グローバル展開の中でも最も優先順位の高い市場として位置づけています。

なぜSCADAfenceなのでしょう

サイバーセキュリティソリューションの導入を考えるときに、従来の対象であったITやOffice Automation（IT・OA）の領域と、今後急速に拡大される産業インフラ・制御技術のOperational Technology（OT）の領域とでは、その運用環境に幾つかの大きな違いがあります。そのなかでも大きなものとして、

- （1）OTでは対象のほとんどが稼働を止められない環境であるため、可用性の維持が最優先されること
- （2）ITでは通信技術を含め、ほぼすべての領域に標準化された技術が使用されているのに対し、OT

では稼働機器の技術のほとんどで、機器を製造するメーカーごとの独自仕様が使用されていることがあげられます。SCADAfenceのソリューションは、このOT分野の特異性を考慮し、

- (1) 「パッシブ型」と呼ばれる導入方法により、稼働機器への変更やエージェント等の追加を行うことなく導入できるため、生産プロセス等の可用性を担保しつつ、即効性の高い効果が期待できること
- (2) OT分野では使用される製品ごとに独自技術による開発・サポートが行われているが、独自仕様の機器・設備に対しても、深いレベルでの解析・分析を行うことを可能としています。

SCADAfenceのソリューションは、産業インフラの中でも特に規模が大きく、かつ業務の中で構成変更が多く発生するセグメントで、その強みを活かすことができると思います。その理由として、

- (1) 規模が大きく、大量のデータを処理する必要がある場合でも遅延なく、また機能を担保するための独自かつ高速AI+マシンラーニング技術を投入していること
- (2) 振る舞い検知の仕組みの中で使用されるベースラインの構築手法に独自技術を投入し、通常業務内での変更と、サイバー攻撃もしくは人為的なミスによる変更を正しく判別し、誤検知を抑制することなどがあげられます。よって具体的には、製造業の大規模な生産設備・工場、大型オフィスビル・商業施設などが活きる領域といえるでしょう。

SCADAについて、日本の状況は他国と比較してどうでしょうか。また、コロナ危機が産業界に与える影響をどうお考えですか

産業インフラシステムの成熟度という観点であれば、日本は大きく進んでいる国であるといえます。また、その産業インフラシステムの最適化（たとえばIoT）についても、その取り組みはほかの先進国と比較しても活発であるといえるでしょう。ただ「システム」という側面で見ると、従来はIT向けとOT向けで分断して運用・管理されていたシステムを、欧米では一元的に運用・管理しているという大きな流れがあり、日本は少し遅れをとっているかもしれません。急速に拡大するDX（デジタルトランスフォーメーション）を進めていくうえでも、ITとOTの融合は必須であり、日本でも期待されるところです。

コロナ危機によって、SCADAfenceが注力する市場、なかでも製造業においては、その事業継続性の考え方

に大きな変化を強いられ、たとえばサプライチェーンの再構築などに発展していく可能性は非常に高いと思います。これは当然のことながら痛みを伴う改革になるであろうことは容易に想像できますが、DX 推進という観点からは強い追い風になることも想定できます。過去の設備投資や、稼働が止められない環境が足枷となっている製造業においても、さまざまな角度からの最適化が急速に進んでいくでしょう。SCADAfenceは単なるサイバーセキュリティソリューションではなく、「生産プロセスの健全性・可用性を最大化」させるソリューションであるといえます。今後大きく進んでいく製造業でのDX 推進の中で大きな役割を担えるものと確信しております。

SCADAfence社の魅力やビジョンをお聞かせください

多くのスタートアップに比べることかもしれませんが、スピード感および透明性の高い組織であることです。また、イスラエルという国は、ご存知のように世界一のスタートアップ大国として、従来のサイバーセキュリティや自動運転の領域以外の、たとえば医療分野などでも常に最新の技術が生まれています。こういったイノベティブな環境の中で、お互い切磋琢磨し合いながら成長を加速させていくという文化にも非常に魅力を感じています。

SCADAfenceにとって、日本は最も戦略的な市場のひとつであり、イスラエル本社も日本のお客様からのご要望に対して強いアテンションをもちています。こういった環境の中で、強いモノづくり国家日本の復活に少しでもお役に立てればと思っております。

お問い合わせ

SCADAfence (Japan) 国内事業責任者 垣貴 己代治
TEL: 03-4588-5432
E-Mail: info-jp@scadafence.com
URL: <https://www.scadafence.com/ja/>

SCADAfenceの導入には、既存の環境への変更・追加等は必要ないため、ほかのサイバーセキュリティソリューションと比較しても容易に導入を進められます。システムエンジニアリング、コンサルティングのサポートが必要な企業様については、パートナー契約を締結したセキュリティコンサルティング、ネットワークインテグレーション、製造業向けシステムインテグレーションの国内トッププレイヤー各社からも支援します。また、導入後の運用の最適化を目的とした運用監視業務を請け負うサービスなども、パートナー企業からの展開が始まっています。

足下の情勢下、新型コロナ拡散防止のために、SCADAfenceが注力する市場の中で、特に事業・生産活動の重要性や必然性が高まっている医療、食品、飲料、消耗品、エネルギーなどの分野に対する支援策として、4月2日よりソリューションの無償提供を開始しています。ぜひこちらをご参照いただければ幸いです。
<https://prtimes.jp/main/html/rd/p/000000009.000038333.html>