



Customer-at-a-Glance

ポーライト株式会社
〒331-0823
埼玉県さいたま市北区日進町 2-121

業種

製造業
(粉末冶金製品 軸受け&機械部品の製造・販売)

社員数

約400名 (グループ 約4600名)

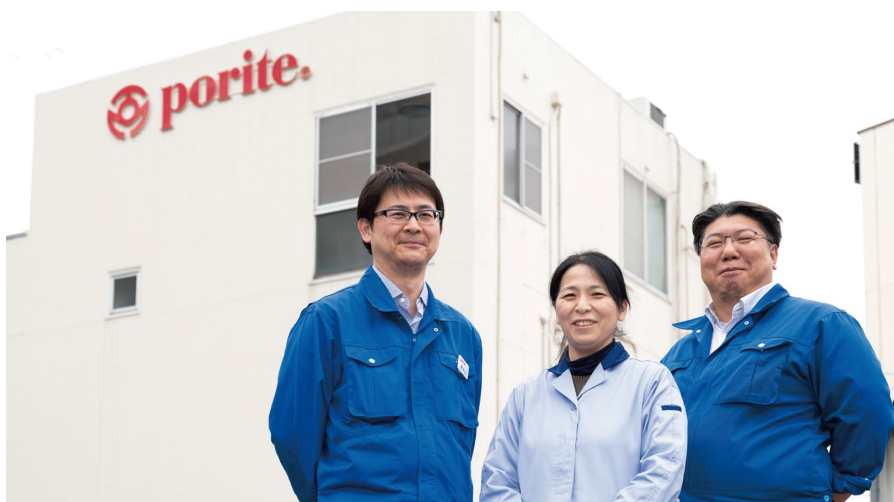
Webサイト

<http://www.porite.co.jp/>

ソフォスソリューション

Sophos XG Firewall

モーター用軸受け部品で世界的に大きなシェアを誇るポーライトが、IoT 技術を駆使したスマートファクトリーを新設した。この新工場を構築する際に、最新のセキュリティ対策としてソフォスのソリューションを採用。
新工場のコンセプトである「工場最適化サイクル」を具現化することができた。



“当社に限らずに製造事業者の間では、最新のクラウド技術を導入して生産設備を高度化する動きが世界的に加速しています。このため、サイバー攻撃に対する防御が極めて重要な課題として急浮上してきました”

喜多山 孝氏 (写真左)

経営改善室 情報システム課 副課長



“セキュリティ対策から直接的な付加価値が生まれてくるわけではないので、当社のような規模の企業では専門家を育成することは難しいのが現実です。その観点で考えると、運用担当者の作業を大きく省力化できるソフォスの製品が当社に適したソリューションだと考えています”

鴨田 香南子 氏

取締役 経営改善室 室長

1952年にオイルレスベアリングの製造・販売事業者として埼玉県与野市（現さいたま市）で創業したポーライトは現在、米国、中国、シンガポール、マレーシア、インド、米国に生産拠点を、香港、フランス、米国に営業拠点を設置して、グローバルなビジネスを展開している。小型モーター用軸受けでは世界トップシェア、DVDやCDなどの光ディスク駆動モーター用軸受けでも圧倒的なシェアを誇り、グループ全体の売上高の約8割が海外からの受注で占められているという。

そんな同社が2018年9月に、最新のデジタルテクノロジーを駆使したスマートファクトリーを埼玉県熊谷市に新設した。IoT（インターネット・オブ・シングス）技術を活用して、生産ラインを可視化できるようにしたことが大きな特徴だ。ライン上に取り付けた各種のセンサーから、リアルタイムでデータを収集する仕組みである。

ビジネスチャレンジ

「工場最適化サイクル」というコンセプトを掲げたスマートファクトリーについて、取締役で経営改善室長を務める鴨田香南子氏は次のように説明する。

「不良率を少なくするといったように何らかの仮説を立案した際に、即座に検証できるような環境を目指しました。リアルタイムに近い形でラインを可視化することで仮説検証のサイクルが飛躍的に短くなり、継続的な改善、すなわち工場の最適化が実現できると考えました」

ただし、これを実現するためには大きな課題があった。データの機密性と可用性をどのように担保するかである。IoT技術を導入する新工場では、膨大な数のデバイスをIPプロトコルのネットワークに接続しなければならない。サーバーやPCなどで稼働するソフトウェアであれば、提供元がセキュリティに十分に配慮しているので脆弱性が放置されたままであるケースは少ない。しかし、センサーやカメラなどのIoT関連デバイスでは、脆弱性を突かれて攻撃者に乗っ取られたといったことも報道されている。さらに、最近の生産設備はIPネットワークに接続できるようになっているにもかかわらず、セキュリティ対策のための機能を新たに搭載することはできない。つまり、脆弱性が残るデバイスを工場内のネットワークに参加させることを容認しなければならないのだ。万が一、ネットワークにサイバー攻撃者が侵入すれば、情報を盗まれるだけでなく、工場全体の操業が止まる恐れもある。

同社で情報システムの企画・構築・運用を担う喜多山孝氏は「サイバー攻撃の脅威は理解していますが、当社のような規模の企業では十分な人的リソースを配備することが難しいのが現実です」と語る。確かにサイバー攻撃は複雑化の一途をたどっており、最新の技術や手口に追隨して

いくには、セキュリティに管理する高度な知識やスキルを備えた人材が専任で研究・分析していく体制が必要だろう。

テクノロジーソリューション

こうした課題を解決するために、同社はネットワークの構築・運用で取引があったジャパンコンピューターサービス（JCS）に相談を持ちかける。JCSと共同で新工場におけるネットワークの要件を立案したのだ。

JCSは、データの発生から保管までを新工場内で完結するネットワーク形態を提案した。既に稼働中の第2工場で発生したデータは、社内光ファイバーを経由し第1工場内のサーバーにデータを集約していた。新工場で発生する大量のデータにより、ネットワーク遅延の可能性が高まるため、新工場内では屋内でデータサイクルを完結させる構成にした。この構成であれば、送信の遅延や喪失もなくなるので、データの可用性も高まる。

さらに、業務用ネットワークと設備機器用ネットワークを分離。ネットワーク間には、ソフォスのファイアウォール製品「Sophos XG」を導入した。これを選定した理由は、高度な検疫機能を実装しているからだ。ほかの製品も選択肢に挙がっていたが、TCO（総所有コスト）の観点で、Sophos XGが圧倒的に優位だったという。

Sophos XGは、隠れたリスクや脅威を顕在化する機能を備えていることが大きな特徴である。リスクが高いユーザーや不明なアプリ、高度な脅威、不審なペイロードなど、ネットワークに潜むあらゆるリスクを可視化することが可能だ。包括的なオンボックスレポートを標準搭載しているほか、複数のファイアウォールの統合レポートを提供する「Sophos iView」もオプションで追加できる。

ランサムウェアや高度な脅威からネットワークを保護するための最新のテクノロジーも提供する。具体的には、トップクラスの評価を獲得しているIPS（侵入防止システム）やATP（Advanced Threat Protection）、クラウドサンドボックス機能、デュアルAV、Web・アプリ制御、メール保護、フル機能のWAF（Webアプリケーションファイアウォール）などが含まれている。

ポーライトのネットワークを構築したJCSでも、自社のセキュリティ対策として2018年からソフォスのソリューションを導入している。脆弱性を解消する手段が見つかっていないゼロデイ攻撃や、長期間にわたってターゲットを分析するAPT攻撃（持続的標的型攻撃）といった高度なサイバー攻撃に備えるために選定したのがソフォス製品だったという。



“高度化・複雑化するサイバー攻撃を
防御するためにソフォスの
ソリューションを採用、導入しました。”

黒崎 直樹 氏

経営改善室 情報システム課
インフラ担当エンジニア

導入した結果

現在、ポーライトではネットワークの運用も JCS に委託中だ。JCS の技術者 3 人が同社に常駐し、ネットワークやセキュリティに関するハードウェアやソフトウェアの設定や日常の運用を担う体制である。常駐している技術者の 1 人である黒崎直樹氏は、現在のポーライトのネットワーク環境について次のように評する。

「JCS で導入・運用した経験から『これなら安心・安全』だと、ポーライト様に自信を持ってソフォス製品をお勧めしました。最初にきちんと設定さえ行えば、レポートの出力をはじめとして数多くの作業が自動化できるので、日常的な運用を担う私たちの仕事も生産性が高くなっていると感じています」

ポーライトの鴨田氏は「現状の運用体制が当社にとって最適な形態」だと前置きした上で次のように語る。

「サイバー攻撃への備えは重要な課題だと認識しています。ただし、そこへの投資から当社のビジネスにとっての付加価値が生まれてくるわけではありません。ですので、社内で専門家を育成するよりも外部のプロフェッショナルに任せの方が、投資対効果が大きくなると判断しました」

同社では今後、新工場で導入した IoT 技術を進化させていく予定だ。喜多山氏は「将来は、生産ラインの全てを仮想空間上にリアルタイムで再現するサイバー・フィジカル・システムに発展させたいと考えています」と展望を語る。



ソフォス株式会社 営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp