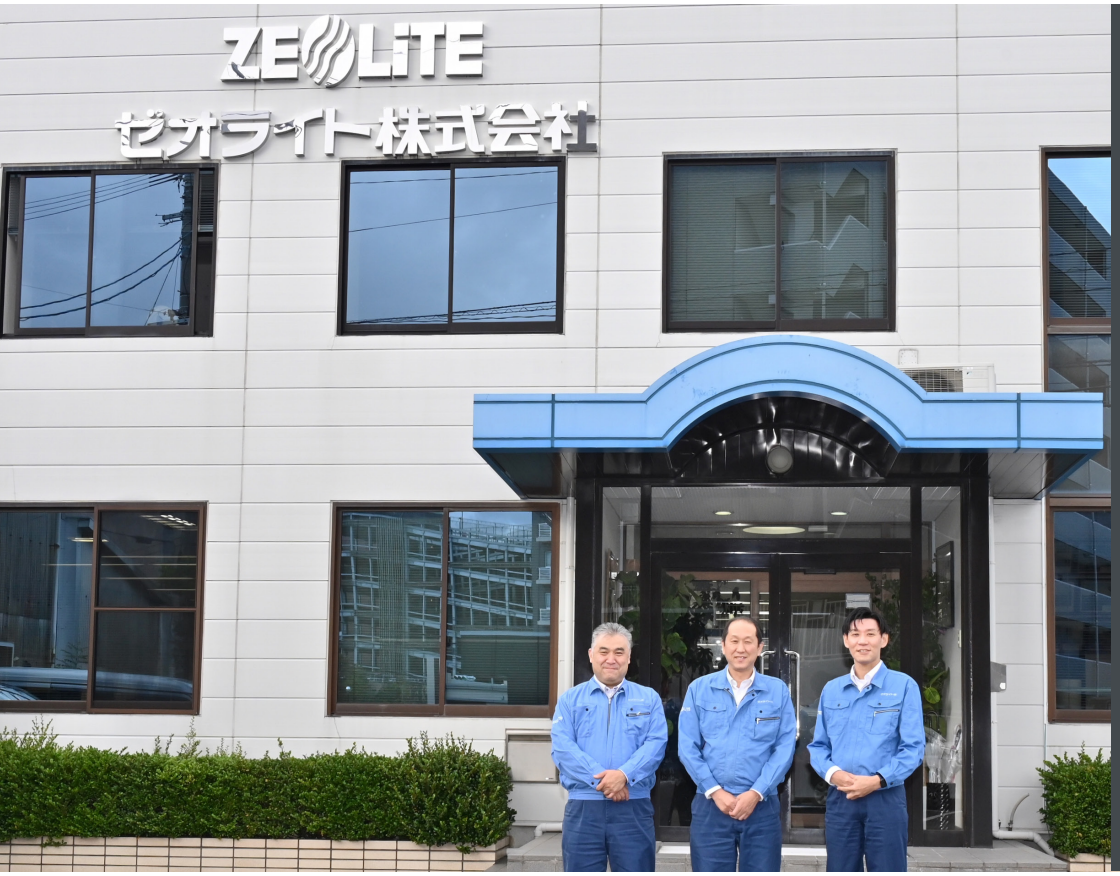


専用水道設備における逆浸透膜の導入実績で国内No.1を誇る水処理プラントのゼオライト株式会社。同社は、国内に1,300件以上の水処理プラントを導入し、自社のメンテナンス部門が導入設備の保守点検も担っている。同社の企画IT部では、水処理という重要なインフラ施設を担う事業を守るために、情報セキュリティ対策にも積極的に取り組んできた。そして、より強固で安全なIT機器の運用を実現するために、Sophos Managed Detection and Response（MDR）セキュリティサービスを契約した。

CUSTOMER-AT-A-GLANCE

ZEOLITE
ゼオライト株式会社

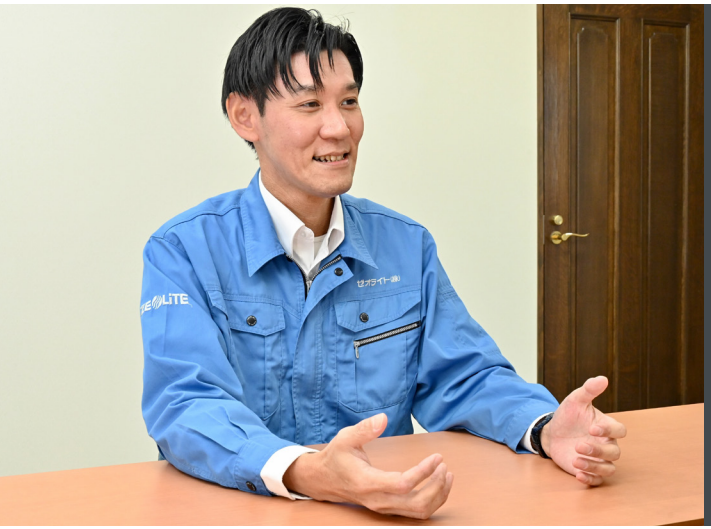
ゼオライト株式会社

所　在　地　〒812-0893
福岡県福岡市博多区那珂5丁目1-11

従 業 員 数　106名（令和3年2月現在）

WEBサイト　https://www.zeolite.co.jp

ソフォスソリューションズ　Sophos Managed Detection and Response（MDR）



決めたことしか通知してくれないSOCサービスに比べて、Sophos MDRセキュリティサービスは、セキュリティの改善提案もしてくれます。

ゼオライト株式会社
企画IT部
境 啓志氏

「良い水創り、人財（ひと）創り」を経営理念に掲げるゼオライト株式会社。逆浸透膜装置を用いた水処理プラントで多くの実績を誇る同社では、常に技術革新を推進し、顧客の課題を解決する提案力を強化してきた。同社の企画ＩＴ部では、水処理プラントの設置や保守を担う人材をITで支えている。そして、情報セキュリティ対策を強化するために、従来の守りを固める防御ではなく、より積極的に脅威を未然に防ぐSophos Managed Detection and Response（MDR）セキュリティサービスを契約し、プロアクティブな防御を実現した。

ビジネスチャレンジ

「Sophos Intercept X Advanced with XDRをきっかけにSophos Centralの管理性能を実感」

ゼオライト株式会社がSophos Managed Detection and Response（MDR）セキュリティサービスを採用した背景について、企画IT部　境啓志氏は、次のように振り返ります。

「最初のきっかけは、旧世代のエンドポイントセキュリティ対策ソフトから次世代型への更新でした。旧ソフトは、社内のネットワークにPCを接続しておかないと、パターンファイルが更新されないため、全国で1,300箇所を超える水処理プラントに出張している社員のPCを100%守りきれない、という心配がありました。また、数年前から日本でもランサムウェアの被害に遭う事件が増えていたので、当社も対策をより強化する必要があると感じていました。そこで、2021年の春頃から次世代型ソフトの選定を開始しました」。

複数の次世代型ソフトが検討された中で、Sophos Intercept X Advanced with XDRが選定された理由について、境氏は「3社の製品を比較検討した結果、導入

をサポートしてくれる販売会社とSophos社の対応を評価しました。導入した後もしっかりしたサポートが受けられる点に安心しました。特に、他社がSOC（Security Operation Center）の利用を提案してきたときに、2022年から日本でもサービスが開始されると聞いたSophos社の日本語のManaged Detection and Response（MDR）セキュリティサービスに魅力を感じました」と話す。

テクノロジーソリューション

「SOCを超えるプロアクティブな対応を評価してMDRセキュリティサービスを採用」

Sophos Intercept X Advanced with XDRへの更新は、2021年9月からスタートし、同年11月には全社員が利用するPCとサーバーへの導入が完了した。その経緯について、境氏は「当社の社員はITスキルが高いので、システム部門が作成した導入手順書を配布するだけで、各自がSophos Intercept X Advanced with XDRへの移行をスムーズに推進しました。円滑な導入を推進できたもうひとつの理由は、Sophos Centralの管理コンソールの優秀さでした。Sophos Centralから、端末の管理状態を統合的に監視できるので、インストールが完了したPCを正確に把握できました」と説明する。

さらに、Sophos Centralの効果について「クラウドサービスとして提供されるSophos Centralは、管理サーバーも不要なので、メンテナンスの手間もなくなり、運用管理も簡素化されました。また、社内だけではなく社外からインターネット経由で社員の利用するPCも管理できるようになりました」と評し、「旧世代のエンドポイントセキュリティと比較して、Sophos Intercept X Advanced with XDRは検知力が向上していると思います。その一方で、すべてのアラートへの対処に、企画IT部としての限界を感じるようになっていました」と境氏は情報セキュリティ対策への人的な課題に触れる。

同社の企画IT部は、IT構築からすべて内製で行っていた為、情報セキュリティ対策に注力できる人員には限りがあった。Sophos Centralを活用した監視やアラート対応は、境氏が担っていたため「移行から数ヶ月が経過して、アラートへの対応が後手になるケースが出てきました。重大なインシデントを発生させないようにするためには、より安心できるセキュリティサービスを活用するべきだと考えるようになりました」という課題が持ち上がった。そこで、「導入時に比較検討したSOCサービスを超えるプロアクティブな対応をしてくれるSophos MDRセキュリティサービスが、2022年から提供が開始されるのを知って導入を決めました」と境氏はサービス採用の理由を話す。

ビジネスインパクト

「脆弱性を未然に防ぐ改善提案で情報セキュリティ対策の強化を実現」

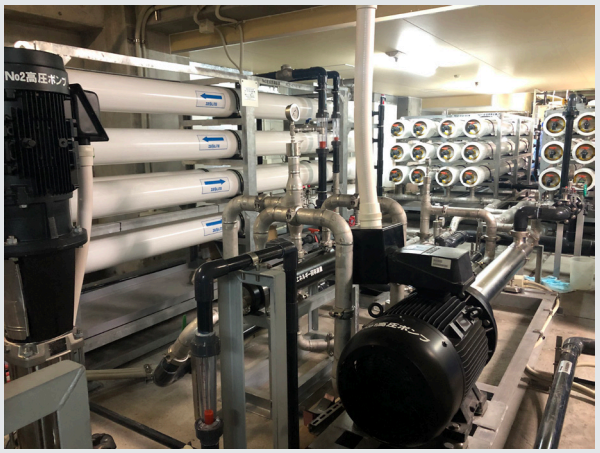
Sophos MDRセキュリティサービスは、機械学習と専門家の分析を融合させ、

24時間年中無休で脅威ハンティングと検出を行い、プロアクティブな防御を実現する。境氏は「決めたことしか通知してくれないSOCサービスに比べて、Sophos MDRセキュリティサービスは、セキュリティの改善提案もしてくれます。高度な知識を持つスペシャリストが、Sophos Intercept X Advancedから得られる情報をもとに、安全に守られているかどうかだけではなく、脆弱性が疑われるポイントも指摘してくれるので、これまで以上に安全な運用が可能になりました」と話し、「Sophos MDRセキュリティサービスの採用により、私自身もセキュリティ対応の業務から開放され、企画IT部門としての本業である新たな企画やシステム開発など、生産的な業務に注力できるようになりました。こうした効果は、当社の経営陣からも高く評価されています」と導入の成果を語る。

フューチャービジョン

「Sophos Firewallの検討も含めてネットワークの保護も推進」

今後に向けた取り組みについて、境氏は「Sophos Intercept X AdvancedとSophos MDRセキュリティサービスで、PCとサーバーの安全性は大きく向上したと思います。次の課題は、ネットワークです。まだ、ネットワークの部分がSophos Centralで監視できないので、Sophos UTMの導入を検討しています。将来的には、端末からネットワークまでSophos Centralによる統合管理を実現し、Sophos MDRセキュリティサービスで情報セキュリティ対策を強化していきます」と展望を話す。



SOPHOS