

リック株式会社 様

オンプレミスのEPPからクラウドのApex One SaaS with XDRに移行
CEC SOCが24時間365日Apex One SaaS with XDR を運用・監視



Apex One SaaS with XDR & CEC SOC

事例



課題

- コロナ禍以降の出社制限と働き方改革によって、ノートPCの持ち出しを許可せざるを得なくなり、既存のセキュリティ対策では対応が不十分に
- 管理するPCの数が約600台と多いため、リソースが限られたシステムチームだけではセキュリティ対策が難しい
- 夜間に工事を行う現場が多数あるため、そういった現場で感染してしまうと、日中勤務のシステムチームでは対応が遅れてしまう

効果

- 外出先のノートPC、ネットワーク、Webアクセス、メールまで監視するクラウドのApex One SaaS with XDRによって強固なセキュリティを確保
- CEC SOCがApex One SaaS with XDRの運用と監視を担うことで、システムチームはセキュリティ業務の大部分から解放される
- 24時間365日監視し続けるCEC SOCが夜間のアラートにも素早く対応し、早期解決に導く

導入の背景と課題

ライフラインの構築を手掛ける会社

創業140年の歴史を持つリック株式会社は、道路および建物中におけるガスパイプラインの新設・移設・交換、上下水道工事、設備工事、土木・建設工事など、ガス工事をメインに電気、水道のライフラインを支える事業を展開している。同社の特徴は、工事を行ううえで安心・安全、そして品質のマネジメントを徹底していること。「現場を監督する従業員の常駐はもちろん、近年はWebカメラを設置し、現場の状況をリアルタイムに把握できるようにしています。これにより、安心・安全を脅かすような事態の際、すぐに対応することが可能です。」と常務取締役 管理本部長 木島 庸成氏は語る。

社外に対応するセキュリティ対策が必要

安心・安全を徹底している同社だけに、社内

の情報システム環境におけるセキュリティ対策にも気を配っている。サーバーをはじめ、共有PC、従業員に配布しているノートPCなど約600台に対し、2000年代前半からEPP (Endpoint Protection Platform) を導入。ウイルスやマルウェアなどの脅威からデータを守るセキュリティ対策を講じてきた。しかし、コロナ禍以降、より強固なセキュリティ対策を求められるようになったと、経理部 経理課 システムチームリーダー 大畑 肇氏は語る。

「コロナ禍以前は、ノートPCを持ち出すことはありませんでした。しかし、コロナ禍以降は出社制限のため、現場から会社に戻って行うオフィスワークは難しくなりました。社会からの働き方改革の要請も手伝って、ノートPCの持ち出しを許可せざるを得ない状況でした。そうになると、台数も多いため、マネジメントするのが非常に困難になります。加えて、オンプレミスで運用しているEPPの保守・メンテナンスやリプレースの手間とコストから逃れるため、クラウドでの運

用に切り替えたいという思いもありました。そこで、感染後も検知・駆除が可能なクラウドのEDR (Endpoint Detection and Response) 導入を検討することにしました。」(大畑氏)

製品の比較・検討

EDRに加えSOCを要件に

EDRを導入するにあたっては大きな要件を設けた。それは、EDRの運用・監視を継続的に、脅威の検知や対策、分析を行ってくれるSOC (Security Operation Center) を導入することだ。大畑氏いわく「リソースが限られている現状では、情報を集めるのがどうしても遅れていました。特に夜間に工事を行う現場が多数ありますから、例えば、そういった現場で感染してしまうと、対応できるのは早くても我々が出社する朝になってしまいます。そこで、我々に代わって24時間365日、EDRを運用・監視し続けてくれる

リック株式会社 様

オンプレミスのEPPからクラウドのApex One SaaS with XDRに移行
CEC SOCが24時間365日Apex One SaaS with XDR を運用・監視



Apex One SaaS with XDR & CEC SOC

事例

SOCのサービスを求めました。」とのことだ。

EDR製品の比較・検討は2021年から開始。数製品の候補の中から機能とコスト、そしてSOCに対応する3製品をピックアップした。最終的に選定したのは、トレンドマイクロ社のApex One SaaS with XDRと、同製品のSOCにおいて実績とノウハウが豊富なシーイーシーのCEC SOC。「もともとトレンドマイクロ社のEPPを利用していたこともあって、Apex One SaaS with XDRのインターフェースには慣れがありました。またXDRにしたのは、SOCの利用を前提とした場合、エンドポイントだけでなく、ネットワークやWebアクセス、メールなどさまざまなログを収集・分析できる製品の方が得策と判断したからです。また、CEC SOCは運用・監視に加え、脅威を発見したあとのサポートが充実。対策や駆除までサポートしてくれるとのこと、安心できると考えました。」と大畑氏は語る。

構築から稼働後の評価

構築も運用もシーイーシーにお任せ

オンプレミスのEPPからの移行と、クラウドのApex One SaaS with XDR構築およびCEC SOCの体制づくりはシーイーシーが担当した。「当社は設定に必要な情報を提供した程度。実際に問題なく稼働するかどうか、固定のデスクトップで使うパターン、社内の無線LANにノートPCを接続するパターン、社外からVPN経由で接続するパターンの3つもテストしていただきました。こちらの手間はほとんどありませんでした。」(大畑氏)

大畑氏が語る通り、構築もテストも滞りなく



常務取締役 管理本部長 木島 庸成氏

進み、6月末にキックオフとなった。端末へのエージェント配布は大畑氏のシステムチーム側で行い、7月から本稼働が始まっている。

素早い対応で脅威を防御

導入して早くも効果があったと語る大畑氏。「怪しいメールはすぐに削除するように従業員には伝えていますが、昨今の脅威は非常に巧妙ですから、記載されている内容と自分がリンクする場合は誤ってクリックしてしまうことがあります。そのアラートを発見してくれたのがCEC SOCでした。すぐに連絡があり、まず、検出された端末をCEC SOC側でネットワークから隔離。次に端末を我々の手元に置き、CEC SOCの指示通りに処理を実施したところ、被害を未然に防ぐことができました。CEC SOCの対応が我々が思い描いていたとおりであったこと、また脅威への対応フローが分かったことに、とりあえず安堵しています。もちろん、さらなる安心・安全を得るには、従業員に対するセキュリティの教育が何より肝心だと実感しました。すぐに対策を考えていきたいと思っています。」(大畑氏)

その後、CEC SOCからの連絡は緊急性のない検知のメール通知のみ。業務に支障をきたすような大きなアラートは発生していない。月1回



経理部 経理課 システムチーム チームリーダー 大畑 肇氏

のレポートを見ても、憂慮するところはないと言う。先ほどの導入早々の対応もあり、同社にとってCEC SOCはコストに見合ったサービスという認識で、非常に満足しているとのことだ。

SDGsへの貢献

ガソリン代の大きな節約に

同社は社会貢献を標榜していることもあり、SDGsにも積極的に取り組んでいる。今回のセキュリティ対策がSDGsに関係してくるか伺ったところ、木島氏は「現場から会社に戻ってオフィスワークしていたコロナ禍前は、その分のガソリン代が発生していました。それがコロナ禍後は、働き方改革とセキュリティ強化が相まって、現場や車の中でのPC作業が可能に。さらに、直行直帰を推奨していることもあって、現場から会社に戻ってくる従業員はほぼ見かけなくなりました。日夜300台前後の車が稼働していることを考慮すると、その分のガソリン代を大きく節約することができました。そういう意味では、SDGsの『7 エネルギーをみんなにそしてクリーンに』『8 働きがいも経済成長も』に貢献していると考えています。」と自信を持って語ってくれた。

お客様プロフィール

リック株式会社 様

1882年の創業以来、ライフラインとして欠かせないガス・電気・水道を支え続けている工務会社。現在は都市ガスパイプラインのスペシャリストとして、安全を担保しつつ効率的な工事を実施している「パイプライン事業」、ガス設備、暖冷房・給湯設備、屋内外給排水、衛生設備、空調設備、電気工事などにおいて豊富な実績を有している「設備事業」、各種施設の建設から上下水道工事、道路・橋梁工事・河川整備工事など多様な「土木・建設事業」の3つを基幹事業として展開している。災害の復旧工事にも積極的に参加。東日本大震災の際には、宮城県気仙沼市にて、造成区画内における配水管布設に伴う減圧弁室の設置工事や、流水中の土砂などを取り除いて揚水施設のポンプの摩耗・損傷を防ぐ錫山沈砂池築造に携わる。現在、そしてこれからも、社会とSDGsに貢献する会社として研さんを重ねていく。



本 社 〒105-0014 東京都港区芝1-15-5
代表者 代表取締役社長 並木 一美
従業員数 429名 (2022年1月現在)
事業内容 パイプライン事業、設備事業、土木・建設事業
URL <https://ri-k.co.jp/>

お問い合わせ



〒150-0022 東京都渋谷区恵比寿南1-5-5 JR恵比寿ビル
TEL: 03-5789-2442 FAX: 03-5789-2585
Email: marketing@cec-ltd.co.jp
URL: <https://www.cec-ltd.co.jp/>

販売代理店

※カテゴリー内に記載されている会社名、製品名などは一般に各社の登録商標または商標です。なお本文中では、TM、Rマークは明記しておりません。
※上記事例に記載された社名・部署名などの情報は取材当時のもので、閲覧時点では変更されている可能性があることをご了承ください。

202301-004-014C1