マイクロセグメンテーション技術で社内ネットワークの通信状態を可視化―

東亞合成が見据える次世代のセキュリティ対策とは

デジタルテクノロジーの進化は、ビジネスの拡大に寄与する一方で、サイバー攻撃のリスクを増大させた。ランサムウェアをはじめ、高度化・巧妙化した攻撃が、業種や規模を問わずあらゆる企業を狙っており、セキュリティ対策の見直しは急務と言える。マルウェアの侵入を許すと、社内ネットワーク内のシステムに感染が拡大し、ビジネスの停止、企業信頼度の低下など甚大な被害を受けることになる。

基幹化学品事業を軸とし、ポリマー・オリゴマー、接着材料、高機能材料、樹脂加工製品の5つの事業を中心にビジネスを展開する東亞合成は、国内に18拠点、グループ会社10社、13のグローバル拠点を持つ化学メーカーだ。研究開発投資を成長の基軸と捉える同社では、新たな研究開発拠点(川崎フロンティエンスR&Dセンター)の立ち上げに伴い、従来技術にとらわれないセキュリティ強化、並びにセキュリティ運用の効率化に着手。本記事では、このプロジェクトについて担当者に話を聞いた。

新たな研究開発拠点の設置を機に、セキュリティ対策の見直しに着手

1944年に創立し、瞬間接着剤の代名詞ともいえる「アロンアルフア」シリーズなど、人々の暮らしや産業、社会に貢献するさまざまな製品を生み出してきた東亞合成株式会社。昨今では、半導体、電子材料、モビリティ、メディカルケア関連製品など高付加価値製品事業も拡大し、再生可能エネルギーなどカーボンニュートラルの実現を目指している。このようにESG/ SDGs の時代に向けた企業変革を推進し、スマートファクトリー化やAI活用といったDXの取り組みにも注力する同社では、川崎フロンティエンスR&Dセンターの設置に合わせて、課題を抱えていた特殊な運用の機器(実験用機器・製造管理システム)のセキュリティ対策の見直しを検討。従来のシステム、ネットワークに大きな変更を加えることなく、ネットワーク上のトラフィックを可視化・制御できるソリューションの選定を開始した。グループ経営管理本部 情報システム部 主事の尾原 徹哉 氏は、当時の状況について、こう語る。

「弊社では、基本的にUTM製品でネットワークの通信を制御しています。研究所で使われる実験機器や端末には、社内ネットワークへの接続に必要なセキュリティ要件を満たしていないものがあり、データのやり取りは、外部メディアに書き出すか、UTMで通信を制限して接続するといった方法で行っており、効率的なデータ連携とはいえませんでした。さらに実験機器や端末で新しい機能を使いたいとなった場合には、UTMの調整などを都度検討する必要があり、設定変更も現地に赴かねばならず、運用管理の負荷が課題となっていました。このため、川崎フロンティエンスR&Dセンターの立ち上げに合わせて、よりフレキシブルに通信制御や設定変更が行えるセキュリティ製品の導入を検討したというのが、今回のプロジェクトが発足した経緯となります。」(尾原氏)

同社では情報漏えいのリスクなどを考慮し、研究拠点のネットワークと情報系・基幹系のネットワークを分離させている。研究拠点の閉じたネットワーク内で運用される端末では、OSやアプリケーションのアップデートが難しく、そもそも実験機器との連動を担保するため古いOSのまま運用しているケースも少なくない。既存のセキュリティ製品が適用できない端末も多く、新たなセキュリティソリューション導入にあたっては、古いOSの端末に対応していることも重視したという。同社のインフラ、及びセキュリティ関連を担当するグループ経営管理本部 情報システム部 主事の隅 康弘 氏は、製品選定におけるポイントについてこう説明する。

「既存のUTMは物理端末のため、運用管理や更新作業にかかる工数も多く、さらにある程度専門的な知識も必要となります。IT人材の確保が困難な状況のなか、弊社の情報システム部においても専門的な知識を持つメンバーは少なく、より簡単かつ正確に通信を可視化できるソリューションを探していました。」(隅氏)

こうして製品選定に着手した同社は、以前よりセキュリティ対策で付き合いがあり、同社のシステムを理解するラック社から「Akamai Guardicore Segmentation(以下、AGS)」を紹介され、検討を開始。2つのUTM製品と比較検討した結果、最終的にAGSの導入を決めた。「これまでUTMを中心にセキュリティ体制を構築してきたので、エリアで守るのではなくホスト単位で守るというAGSの考え方は非常に画期的でした。UTMではローレベルの通信内容しか見えなかったのですが、AGSでは通信内容を高い解像度で可視化できることに驚きました。」と隅氏はAGSのファーストインプレッションを語る。

東亞合成株式会社
グループ経営管理本部
情報システム部 主事
尾原 徹哉 氏

東亞合成株式会社
グループ経営管理本部
情報システム部 主事
隅 康弘 氏

脆弱性診断や、その結果を受けたWAF(Web Application Firewall)の構築でラック社の支援を受けた尾原氏も「WAFの導入においても、ラック社には通信内容を細かく分析して制御内容を決定するという工程を支援していただき、弊社の環境に合わせて作り込んでもらえたので、今回のAGSに関しても安心してお任せできると考えました。」とラック社への信頼を口にする。

東亞合成株式会社
グループ経営管理本部
情報システム部 主任
川島 佑希奈 氏

迅速かつ適切なラックのサポートを受け、社内ネットワークにおける通信の可視化を実現

隅氏と共にAGSの導入・運用に携わったグループ経営管理本部 情報システム部 主任の川島 佑希奈 氏は「2024年初頭から検討を開始し、ラック社、Akamai社の支援を受けて同年3月からPoCを実施。そこから構築を開始し、12月に構築を完了しています。」と、プロジェクトのタイムラインを解説。AGSの導入にあたり苦労したポイントを次のように語る。

「導入に先立って、現状の通信状態を把握する必要があり、その工程に時間を費やしました。私たちが把握していない通信もすべて可視化されるので、必要な通信とそうでない通信を一つ一つ精査し、判別していく作業に苦労しました。最初の2カ月でエージェントをインストールする対象となるサーバーを選定し、その後、どのような設計にしていくかを検討していきました。ただ、AGSには自動で制御内容を提案してくれる機能が搭載されており、それを参考にすることでイチから設計する手間が省けました。」(川島氏)

AGSはWindows XP/7といったレガシーOSから、最新のコンテナ環境まで幅広い環境に対応しており、懸念点であった古いOSの端末にも問題なく導入することができたという。ネットワーク構成の変更が不要で動作も軽く、業務への影響を最小限に抑えながら、通信の可視化とセキュリティの強化を実現できたと隅氏は語り、ラック社のサポートによりスムーズに導入できたことを喜ぶ。

「先ほどお話ししたように我々には専門的な知識がなく、サポートをお願いする際にも抽象的な表現になってしまうことが多いのですが、ラック社は抽象的な問い合わせの内容であっても、それを汲み取って具体的な解答をくださります。ポリシーに落とし込むところまでしっかり対応してくださり、本当にレベルの高いサポートだと感じました。レスポンスも早く、とても助かりました。」(隅氏)

尾原氏も「ポリシーの策定、ルール作りに関しても、我々の要望を理解したうえで適切な提案をしていただき、今後、AGSの利用範囲を拡大する際に、我々自身で設計や運用をするためのヒントをもらえたと感じています。」と所感を語り、ラック社の密接なサポートを高く評価する。

セキュリティ意識の向上や運用負荷の軽減など、AGS導入による効果は多岐にわたる

こうして川崎フロンティエンスR&Dセンターで AGSの運用が開始され、セキュリティ強化と運用負荷軽減の両面で効果が現れているという。

「運用管理の面では、体制としてはそこまで大きな変化はないのですが、通信状況が可視化されるため、疑わしい通信に対する初動が早くなりました。サーバー間での通信など、従来のファイアウォールに引っかからないものも可視化・制御できるようになり、より強固なセキュリティ対策が実現したと感じています。さらにUTMを入れずに済んだため、ハードウェアの運用負荷は大幅に軽減されています。」(川島氏)

尾原氏も「見えるポイントが増えたことで、あれ?と思ったときの確認工数はかなり減りました。」と話し、二つのポジティブな効果が現れていると話しを続ける。

「一つ目はシステム担当者の意識が変わったことです。新しいサーバーを立てる際に、AGSを入れるべきかなど、セキュリティについて考えるようになってきています。こうした変化はセキュリティの底上げにつながると考えています。二つ目は私が担当する領域となりますが、脆弱性診断でリスクがあると判定されたものへの対応が容易になったことです。これまでは改修にかかる費用と時間、システムへの影響度などの要因で迅速な対応が難しい面もあったのですが、AGSが導入されてから、各種通信の必要性を確認した上で該当通信を遮断するという、暫定手段を迅速に実施できます。この二つがセキュリティ強化という観点での導入効果と考えています。」(尾原氏)

実際、社内ネットワークの通信すべてを可視化・制御できるAGSは、ランサムウェアのように社内ネットワーク内のシステムに横展開(ラテラルムーブメント)するサイバー攻撃への対処も迅速化する。詳細な設定とメンテナンスが必要なUTMと比較すると、運用管理の手間も少なく、構築スパンも短くなると尾原氏は語る。

AGSの適用範囲を拡大し、新しい時代を見据えたセキュリティ体制の構築を目指す

本プロジェクトの成果を踏まえ、東亞合成ではAGSの導入を拡大していく予定だ。現状は最新の川崎フロンティエンスR&Dセンターや一部の重要なシステムへの導入にとどまっているが、未導入の重要システムへの展開をはじめ、AGSの導入に適した拠点やシステム、導入優先順を模索している段階と尾原氏は語る。

「情報システム部のリソースが限られ、専門知識を持つ人材の確保が困難な状況を鑑みると、AGSは非常に有効な選択肢となります。今回の取り組みで、サーバーにアクセスする経路の整理など、対処すべき課題が見えてきたので、その対応と併行してAGSの導入を進めていきたいと思います。コスト面の問題などもあり実現できるかわかりませんが、最終的にはすべての重要なシステムにAGSを適用できればと考えています。」(尾原氏)

マイクロセグメンテーション技術でネットワーク内のリスクに対処できるAGSの導入をフックに、運用負荷の軽減と、高度化するサイバー攻撃への対応を進める東亞合成とラックの取り組みは、社会インフラを担う化学業界はもちろん、事業継続性の向上とリスク軽減を目指すあらゆる企業に多大な“気付き”を与えてくれるはずだ。

本件に関するお問い合わせ先

株式会社ラック

URL https://www.lac.co.jp/contact.html