エッジ領域の
セキュリティ強化に貢献する
Menlo Security

各種接着剤の開発で培った樹脂合成技術をコアに事業領域を拡大させているアイカ工業株式会社では、オンプレミスで利用してきたプロキシが老朽化を迎え、エッジ領域におけるセキュリティ強化を図るべく、SSEを意識しつつSecure Web Gateway（SWG）など複数のソリューションの中から、Menlo Securityが提供するSWGやWebアイソレーション、検知回避型脅威対策に有効なHEAT Shieldを導入。その経緯について、アイカ工業 情報システム部 DX推進／情報セキュリティグループ 小倉 大樹氏にお話を伺った。

EDRが導入できない製造現場の制御端末など、セキュリティ対策の不備が不安感を生む

設立当初より培ってきた樹脂合成技術を核に、化学とデザインの融合から新たな価値を生み出し、活躍のフィールドを拡大し続けているアイカ工業株式会社。同社の製品は、住宅をはじめとした建築物、自動車、電子製品、化粧品、衣類、靴など様々な分野で活用されている。現在は、海外での売上が半数以上を占めており、世界14の国と地域に51社のグループ会社を展開中だ。

そんな同社では、過去に起こったホームページ改ざんというインシデントを契機にセキュリティ対策の強化を進めてきた経緯があり、エンドポイント対策となるNGAVやEDR、そしてメールセキュリティを含めた各種ソリューションを導入し、コストではなく将来の利益を守る投資としてセキュリティ対策を強力に推し進めている。そんなセキュリティ対策の1つとして運用してきたプロキシが老朽化を迎え、新たな環境整備が必要になったという。「オンプレミスで運用してきたプロキシのクラウド移行を進めながら、従来は十分でなかった対策が包括的に実施できるサービスへの切り替えを検討したのです」と小倉氏は当時を振り返る。

具体的には、多段型のセキュリティ対策を中心に外部との境界としてのエッジ領域強化を目的に、SWGやFirewall as a Service（FWaaS）といった各種コンポーネントを備えたSecurity Service Edge（以下、SSE）の概念を参考にセキュリティ対策を進めていくことに。「SSEを展開したいというよりも、バラバラの製品、ポリシーで運用していたものを統合していき、今の時代に適したポリシーに見直していくことでエッジ領域の強化を図っていこうと考えたのです」と小倉氏は説明する。

特にPCをはじめとしたOA機器であれば、EDRなどを導入することでマルウェアを経由して外部から攻撃をしかけるC&C通信などを検知することが可能だが、製造現場にある制御端末などEDRが展開できない機器の場合、脅威につながる通信が把握できていないなど、対策が十分でないことが懸念されていた。「EDRの導入で検知が進み、脅威につながる通信が発生していることが把握できました。具体的なインシデントは発生していませんが、いずれ何か起こってしまう可能性があるという不安感を持っていたのです」と小倉氏。

機能要件と最適なコストを満たしたMenlo Security、独特なWebアイソレーションに注目

新たな環境づくりに向けて、従来のプロキシが持つ機能とともに、既存ブラウザの活用やエージェントレスといった、現場に負担をかけないユーザビリティの観点を中心に、多段プロキシ構成でも通信元のローカルIPがきちんと特定できるなど技術的な要件を提示。複数のソリューションを候補に挙げるなか、Menlo Securityに注目したという。

「我々が提示した要件を満たせるソリューションは2社ほどに絞られましたが、信頼しているディストリビュータからお勧めされたのがMenlo Securityでした。特に少数精鋭で運用していることもあり、例えばログからのFQDN特定方法など細かな運用に負担がないかどうか気にしていました。運

社名：アイカ工業株式会社
業界：製造業
所在地：愛知県名古屋市中村区名駅1-1-1
JPタワー名古屋26F
URL：https://www.aica.co.jp/

1936年10月設立。以来、樹脂合成技術を核として、「化学」と「デザイン」のシナジーで社会の要請に応える製品を提供することで、着実な成長を続けてきた。日本初のユリア樹脂接着剤を開発するなど高い技術力を持ち、メラミン化粧板の分野では国内シェアNo.1を誇る。

ソリューション

- Secure Web Gateway
- Webアイソレーション
- HEAT Shield（検知回避型脅威対策）

課題

- オンプレミスのプロキシが老朽化を迎える
- EDRが展開できない製造現場の専用機器からの通信を制御したい
- SSEを中心に外部とのエッジ領域の強化を図りたい

効果

- クラウド型のSWG移行に成功、ユーザビリティを大きく変更せずに展開
- PCはもちろん、現場で使われる専用機器からの通信状況も把握可能に
- Webアイソレーションにてエッジ領域のセキュリティ強化を実現

アイカ工業株式会社
情報システム部
DX支援／
情報セキュリティ
グループ
小倉 大樹 氏

用の懸念点についてもディストリビュータがきちんと回答いただくことで安心できた点も大きい。我々が望んだ機能に見合ったコストだった点もMenlo Securityを評価したポイントの1つ」と小倉氏。

また、Menlo Securityが持つWebアイソレーションについては、検討当初は意識していなかったという。「VDIを軸にしたエンドポイントのシンクライアント化を検討していたことで、それに近しい機能があればという感覚でした。プロキシの更改案件で分離を求めていたわけではありませんが、WebアイソレーションやHEAT ShieldなどMenlo Securityが持つソリューションに関するデモを熱心に実施いただいたことで興味が高まっていったのです。今となっては絶対に必要な機能だと認識しています」と小倉氏は評価する。

特に国内のグループ会社は同社のネットワーク傘下に入ってくる構成となっているため、EDRも含めてグループ会社に展開はしているものの、拠点全ての端末がきちんと展開できるとは限らない。「アイソレーションがあれば、リスクがある状況でもとりあえず大丈夫という感覚になれると考えたのです」と小倉氏。

結果として、オンプレミスのプロキシの更改に向けて、新たにMenlo Securityを採用することになったのだ。

Menlo Securityがもたらした安心感、現場に意識させずにセキュリティレベルの向上を実現

当初は情報システム部を中心に、各部署やグループ会社のキーマンおよそ200名に対して検証をスタートさせ、最終的には4つのグループ会社を含めた1800名ほどがMenlo Securityが提供するSWGを経由してインターネットにアクセスし、Webアイソレーションによるインターネット分離を行っている。また、ITだけでなく工場側のOTネットワークに接続する専用機器もSWGを経由したアクセスとなっており、従来できなかった通信の可視化を実現している。「工場は創業からの歴史が積み重なっており、把握できていない機器もゼロではありません。過去の遺物を100%把握することは難しい状況でしたが、これまで把握できていなかった環境が可視化でき、かつ安全性も担保できるようになりました。資産の把握という意味でも有効です」と小倉氏。

ネットワーク構成的には、同社だけでなくグループ会社も含めて同社のネットワーク網を経由してインターネットアクセスを行っており、各社で運用する複数のIDPに適した、SAML認証によるSSOやID/PWといった複数の認証方式を採用。また、会社や組織、役割によってWebサイトへのアクセス可否を制御しているため、50ほどのポリシーでMenlo Securityを運用している。「検知を回避する脅威に対しても、HEAT Shieldがきちんと機能しています。本来はEDRで検知すべきものがすり抜けたことが半年間の運用で1度だけありましたが、その際にも脅威をしっかり検知してブロックできました。それだけでも効果があるソリューションだと実感しました」と小倉氏は評価する。

ちなみに通信の振り分けについては、以前から設置していたADC装置にて行っており、必要な通信のみをSWGに振り分けて運用している。

稼働時には、専用機器がうまく通信できないなど、いくつか課題が顕在化する場面もあったが、回避策も含めて十分に学んでいたことで、業務に大きく影響するようなトラブルもなく移行に成功している。「何の問題もなく稼働できるとは考えていなかったですし、初期に発生した課題は想定の範囲内でした。ディストリビュータの支援もいただいたおかげで、大きな問題もなく運用できています」と小倉氏。現在でも利用者からの問い合わせがあるものの、マルウェアの検知によってダウンロードできないといった、ある意味で正当な問い合わせが主なものだという。

> “これまで可視化できていなかった機器の把握と制御が可能になり、さらにWebアイソレーションによって無条件で安心できる環境が実現できたことが大きな利点だと感じています”
>
> アイカ工業株式会社
> 情報システム部
> DX 支援／情報セキュリティグループ
> **小倉 大樹 氏**

Menlo Securityを導入したことで、安心感が得られたことが大きな効果の1つだと小倉氏は力説する。「これまで見えなかったものが把握でき、人手をかけるなど頑張れば運用でリスクを回避していくことも可能です。それでも、今は無条件で安心できる環境というのは大きい」。利用者に対しては、特に意識することなく新たな環境に移行できたことが大きなポイントだ。「ユーザビリティを優先したこともあり、何も変わっていないのにセキュリティレベルが上がっているという評価を得たかった。結果としてそのような理想に近い形で運用できています」と小倉氏。また、SWGに通信が集まることで活動履歴のログが蓄積され、情報システム部としての活用だけでなく、他部門から求められた場合でも活用できるデータが取得できるようになったことも大きな効果の1つだと説明する。

Menlo Securityに対しては、通信を止める理由が明確に提示されることがありがたいという。「何かしらプロキシ側で通信を止めた場合、ユーザーからの問い合わせに確証を持って回答する必要があります。以前は私がいろいろ調べていくことが必要で、プロキシ側で内容を解析してくれるわけではありませんでした。Menlo Securityであれば、きちんと専門家としての判断基準が提示され、ファイルの何が問題なのかもきちんと通知してくれます。早急に回答できますし、調査手法の属人化も防いでくれるため、個人的にとても重宝しています」と評価する。

FWaaSや内部不正対策など、さらなるセキュリティ強化に向けた取り組みを加速させたい

今後について小倉氏はSSEのコンポーネントの1つであるFWaaSをはじめとした新たな対策への投資を進めながら、社用携帯からの通信経路についてもエッジ領域で統合管理できるような環境を整備していくことで、運用負担のさらなる軽減を図っていきたいと意気込む。「すでにCASBやDLPなどの取り組みは他のソリューションで実現していますが、現在は統合された単一の環境にはなっていません。できれば統合したコンソールで集約していければと考えています」。

また、現在はグローバルについては情報システム部にて方針を決定するものの、実際の対策そのものは現地法人など各現場で行われている。グループ全体のセキュリティ対策をさらに強化していくためにも、いずれは情報システム部が主導的な形でソリューション展開できるような活動につなげていきたいと小倉氏は今後の展望を語った。