SWGを含めたゼロトラスト環境を1つのプラットフォームで実現

半導体・電子部品メーカーとしてグローバルに事業を展開しているローム株式会社では、新型コロナウイルス感染症の影響で、従来の境界防御からVPNを含めたネットワークを開放して業務にアクセスできる環境づくりが必要に。NIST（米国国立標準技術研究所）が提示するサイバーセキュリティフレームワークなどに準拠しながら、ゼロトラスト環境に向けたソリューション展開を実施している。その基盤の1つとして、Menlo Securityが提供するWebやメールの脅威を無害化するアイソレーションおよびクラウドプロキシとしてのSWG（Secure Web Gateway）を選択している。その経緯について、IT統括本部 ITガバナンス室 室長 井上 正氏にお話を伺った。

新たな働き方への対応でネットワークを開放、セキュリティ対策の強化が急務に

1958年設立の半導体・電子部品メーカーとして、自動車や産業機器のほか、民生機器、通信機器など多様な市場に対して、品質と信頼性に優れたICやディスクリート、電子部品などをグローバルに提供しているローム株式会社。特にパワーやアナログ分野においては、SiC（シリコンカーバイド）をはじめとするパワーデバイスやそれらの性能を最大限に発揮するための駆動IC、またトランジスタ、ダイオード、抵抗器などの周辺部品を含め、システム全体を最適化するソリューション提案を強みとしている。現在は“MOVING FORWARD to 2025”という中期経営計画のもと、2025年度までの経営テーマを「“車載”“海外”での成長実現とさらなる成長に向けた基盤作り」と定めている。

そんな同社では、これまで社内からインターネットアクセスを厳格に制限するなど強固なセキュリティ対策を実施してきた経緯があるが、世界規模のパンデミックによって在宅勤務も含めた新たな働き方への対応が迫られたという。「一部が利用してきたVPN環境を全社員で利用するわけにもいかないため、新たな働き方へ柔軟に対応すべく、ネットワークの開放を進めてきました。同時に、グループ全体でNISTのサイバーセキュリティフレームワークに準拠する形でセキュリティ強化を行っています」と井上氏は説明する。

また社内におけるセキュリティ強化だけでなく、顧客や取引先を含めたサプライチェーン全体のセキュリティ対策も意識しており、日本自動車工業会が示す自動車産業サイバーセキュリティガイドラインやドイツ自動車工業会が策定したTISAXなども加味しながら、現在でもSASE（Secure Access Service Edge）を中心としたゼロトラスト環境の段階的整備を続けている状況にある。

1つのプラットフォームでゼロトラスト環境を強力に推進できるMenlo Security

そんなゼロトラスト環境の実現に向け、当初はネットワークが集中するVPN環境の課題を解消すべくZTNAソリューションを導入し、エンドポイント対策としてIT資産管理やEDRを展開した同社。そして、インターネットの入口対策やメール運用での脆弱性が危惧されるPPAP対策も含めて、総合的に検討するなかで複数のソリューションを候補に選定したという。「1つのベンダーで網羅的に対策できることが、運用やコストを考えると理想的です。しかし、たとえMicrosoftであっても、不足する機能はでてきてしまう。そこで複数のコンポーネントが利用できるプラットフォームを念頭に検討したのです」と井上氏。

そこで注目したのが、Menlo Securityが提供するMenlo Security Cloud Security Platformだった。Secure Web Gatewayを始め、安全なWebアクセスを可能にする Webアイソレーション、Emotetを含むメール経由の脅威を無害化するメールアイソレーションが1つのプラットフォームで統合でき、将来的にはCASBやDLP、そしてすでに導入済みのZTNAの置き換えも含めて活用

社名：ローム株式会社
業界：製造業
所在地：京都府京都市右京区西院溝崎町21
URL：https://www.rohm.co.jp/

1958年設立。半導体・電子部品メーカーとして、自動車や産業機器のほか、民生機器、通信機器など多様な市場に対し、グローバルに展開している開発・営業ネットワークを通じて、品質と信頼性に優れたICやディスクリート、電子部品を供給している。得意とするパワーとアナログ分野では、SiCをはじめとするパワーデバイスやそれらの性能を最大限に発揮するための駆動IC、またトランジスタ、ダイオード、抵抗器等の周辺部品を含め、システム全体を最適化するソリューション提案を強みとしている。

ソリューション

- Secure Web Gateway
- Webアイソレーション
- メールアイソレーション

課題

- 新たな働き方に対応する境界防御が限界に
- ゼロトラスト環境を軸に統合できるソリューションを希求
- Emotetなどのマルウェアに100%対処できない

効果

- ゼロトラスト環境の推進を実現
- 安全なWebアクセスとメール運用が可能に
- 従業員のセキュリティ意識の醸成に貢献

ローム株式会社
IT統括本部
ITガバナンス室
室長
井上 正氏

できる点を評価したという。

特にメールに関しては、標的型攻撃メールとして猛威をふるっていたマルウェアであるEmotetに対して有効な手段を検討していたが、実際にPoCを実施するなかでも100%の対策に至るソリューションは存在しなかった。一方でMenlo Securityであれば、クラウド上でメールの添付ファイルや感染リスクのあるサイトへ誘導するURLの無害化が可能となり、1つのソリューションで対策できると井上氏は考えたという。

Menlo Securityに対しては、その実績も高く評価したポイントの1つ。官公庁をはじめ、社会インフラを担う大規模な導入が実績としてあったことも背中を押す要因になったという。統合的に利用可能なことでコストパフォーマンスが高い点も評価し、同社が進めるゼロトラスト環境のコンポーネントとして、Menlo SecurityのSWGおよびWeb・メールアイソレーションの導入を決断したという。

Web・メールの無害化が ガバナンス強化に大きく貢献

現在は、日本国内および海外の関係会社も含めて1万名以上がMenlo Securityを活用しており、半年ほどかけて部門ごとに担当者を決めてチューニングする期間を設けたうえで、統一されたポリシーを軸にインターネットアクセスおよびメールセキュリティの強化を行っている。現在でも業務上必要なWebサイトにアクセスできない場合があれば、その都度チューニングを実施しながら業務に支障が出ないような運用を行っている。

基本的に業務端末はインターネットアクセスを許可していないが、Microsoft 365をはじめ、ホワイトリストとして登録された業務システムにはアクセス可能で、SWG側で正規カテゴリーに位置づけられるものはアイソレーションを行わず、加えてブラックリスト登録されたものがブロックされる。未分類およびリスクのあるカテゴリーについてはアイソレーションを実施することで安全なWebアクセスを実現している。メール経由のファイルも同様にアイソレーションが実施され、クラウド上で安全にファイルの中身を閲覧した上で、必要に応じてダウンロードできる運用が可能だ。

メールアイソレーションについては、一部システムからのアラートなど自動化されたスクリプトで動くものは、Fromとなるシステム側のIPを固定することで柔軟に対応している。「システムからの通知を個人のメール宛に送っているケースが発覚するなど、ガバナンス上不適切な使い方の可視化にも役立っています」と井上氏は説明する。

新たにMenlo Securityを導入したことで、必要な環境にのみ安全にアクセスさせる運用が可能になり、セキュアな環境によってガバナンス強化に大きく貢献していると井上氏は評価する。実際にEmotetをはじめとしたマルウェア感染による被害は発生しておらず、攻撃者が設置しているC&Cサーバへの情報のやり取りも防げているなど、高度化する脅威への対策も十分実施できているという。「世の中でEmotetの被害が多くなった時期もありましたが、Menlo Securityのおかげで安心して運用できました」と井上氏。また、監視環境が強化されたことで、従業員に対するセキュリティの意識づけが可能になるなど、抑止効果としての効果も見逃せないという。

> メールの中身を分別できるソリューションは他にもありますが、基本的にマルウェアのリスクがゼロにならない。ならば無害化できるアイソレーションの仕組みを持つ Menlo Security が有効だという結論でした ”
>
> ローム株式会社
> IT 統括本部
> IT ガバナンス室
> 室長
> **井上　正 氏**

システム管理者の立場としては、従業員に安心して業務が推進できる環境が整備できたことが何よりも大きいという。「私自身利用者の立場でもありますが、危険と思しきURLのリンクがあっても無害化したうえで確認できます。安心してアクセスできるツールとして高く評価しています」と井上氏は力説する。セキュリティに理解のあるボードメンバーが多い同社だけに、経営層からもMenlo Securityがもたらす価値に対する評価は高い状況にある。

メンロ・セキュリティ・ジャパン株式会社に対しては、場面に応じてレクチャー時間を確保してもらうなど、手厚い支援を高く評価する。「日本特有のサイトにアクセスできない場面では、当初はホワイトリストで回避しましたが、本国にエスカレーションいただいて数か月後にはきちんと対処いただいたことも。課題の切り分けも含めて真摯に対応いただけています」と支援体制についての評価も高い。

ログの相関分析とともに SASEに必要なコンポーネントの整備を進めたい

現在も継続してセキュアな環境づくりに取り組んでいる同社だが、外部脅威への対策とともに、内部不正への対処や不要なサイト閲覧の抑制による業務の効率化など、さまざまな取り組みを加速させていくことで、ガバナンス強化に向けたアプローチを推進していきたいと井上氏は意欲的だ。

また、ゼロトラスト環境の整備に向けてさまざまなソリューションを導入しているが、蓄積されたログを活用した相関分析などはまだこれからの課題となっている。「Menlo Securityのログも活用しながら、統合監視できるような環境づくりを検討していきたい」と井上氏。ログ活用が進むことで、少数精鋭でも脅威の検知から対処までが自動化できるSOARのようなアプローチにも活かしていくことが期待されている。

さらに、DLPやCASBなどSASEを構成する他のコンポーネントも導入検討しながら、さらなるセキュアな環境整備を進めていくことで、ログ活用の精度を高め、新たな気づきにつなげていくことが期待されている。「個別に対策するのではなく、できれば1つのベンダーに寄せていくことで、監視する画面も減り、個別の相関分析の仕組みを入れずともソリューション内でできるケースも増えてきます。Menlo Securityでカバーできる範囲が増えれば、セキュリティがより強化できるはず。今後も期待しています」すでに導入済みのZTNAも将来的な統合へ向けて検討を進めていきたいと今後について井上氏に語っていただいた。