ペット専門店のコジマ、マイクロセグメンテーション導入で万一の侵害に備えた対策を強化

通信のリアルタイム可視化と柔軟な運用ポリシー変更により今後のサイバー攻撃の変化にも迅速に対応

ソリューション　Illumio Segmentation

株式会社 コジマ
https://pets-kojima.com/company/

業界：ペット専門店
本店所在地：東京都江東区
事業：
ペットショップの経営、動物病院の経営、ペット用品の通信販売、ペット用品の輸入・販売

ソリューション
Illumio Segmentationを用いてマイクロセグメンテーションを実装することで、社内ネットワークが万一侵害された際にも被害の範囲を最小限に抑える。

導入前の課題
データセンターとクラウドに全社データを集約した一元管理とともに、UTMやSASE、EDRなどによる多層防御を固めてきたが、現在の高度化したサイバー攻撃を完全に防ぐことは不可能に近い。万一侵害された際の対策強化が必須課題であった。

導入後の効果
各サーバーの通信状況のリアルタイムな可視化とセグメント分割による侵害拡大防止を図り、事業継続リスクを最小化した。

お客様の課題

段階的な多層防御の強化を図ってきたがラテラルムーブメント対策は不十分

ペットの専門店として、ペット用品販売、トリミング、ペットホテル、動物病院など幅広いサービスを提供しているコジマ。「ペットの総合ライフサポート」を特徴とし、販売から医療までワンストップで対応できる点が強みです。近年はオンラインショップの強化や、子犬・子猫を専用施設で一定期間管理し、健康管理の強化にも努めています。

一方、事業の多角化・高度化とともに強化が求められるのがセキュリティ対策です。同社は顧客の個人情報やペットの健康データなどを扱う業務の特性を考慮し、データセンターとクラウドにデータを集約した一元管理とともに、UTMやSASE、EDRなどによる多層防御を固めてきましたが、それでも万全な体制とは言えない状態だったといいます。

同社 情報システム部 部長の森下 万優氏は「現在のサイバー攻撃を完全に防ぐのはほぼ不可能であり、万が一にも侵害された際の備えを欠かすことができません。具体的には社内ネットワーク内を横移動しながら侵害範囲を拡大していく、ラテラルムーブメント（水平展開）への対策が手薄な状態にありました」と振り返ります。

Illumioの選定ポイント

マイクロセグメンテーションを導入し運用ポリシーを動的に変更できる点を重視

課題解決に向けて同社が注目したのが、マイクロセグメンテーションです。

「当初は、ネットワーク検知・対応が可能なNDR（Network Detection and Response）も検討しましたが、通信制御と脅威封じ込めを強化するためには、やはりマイクロセグメンテーションが有利と判断しました。通信の可視化とセグメント分割による侵害拡大防止を図り、事業継続リスクを最小化したいと考えました」（森下氏）

そして情報収集のために訪れたITリーダー向けイベントにてIllumioと出会い、同社は導入の検討を開始しました。

「Illumioに魅力を感じたのは、通信のリアルタイムな可視化に加え、運用ポリシーを動的かつ容易に変更できる点です。従来型の固定ルールに基づく運用とは一線を画し、変化する状況に応じてポリシーを適宜修正し、適用できる仕組みを重視しました」（森下氏）

さらに同社が高く評価したのが、イルミオジャパンのサポート体制です。

「対面やメール、電話で気兼ねなく相談できるカスタマーサクセスおよび

お客様にとっての価値

社内ネットワークのセキュリティ強化

全社の約70拠点をVPNで接続し、店舗、病院システムと本部システムを連携させるネットワークにマイクロセグメンテーションを導入。万一サイバー攻撃による侵害があった場合でもラテラルムーブメントを防ぎます。

業務実態に合わせたマイクロセグメンテーションの運用

Illumioによって一元的に可視化されたデータフローを把握・分析することで、業務実態にあった最適なマイクロセグメンテーションを実現します。

取引先から高い評価を獲得

マイクロセグメンテーションの導入は、大手メーカーを中心とした取引先からも高く評価されています。今後予想されるセキュリティガイドラインの規制強化も見据えた対策を導入することができました。

プロフェッショナルサービスの体制が整っており、Illumio を選定して良かったと感じています。他ベンダーの一般的なサポート窓口と違い、顔の見えるアドバイザーが寄り添ってくれることに、非常に大きな安心感がありました」（森下氏）

森下 万優 氏
情報システム部
部長

Illumioに大きな魅力を感じたのは、通信のリアルタイムな可視化に加え、運用ポリシーを動的かつ容易に変更できる点です。変化するネットワークの利用形態とサイバー攻撃の動向にあわせた運用の見直しを、柔軟に行うことができます。

導入の期待効果

各サーバーの通信状況の可視化により先手で次のアクションを打つ“ 攻め”のセキュリティ体制を構築

Illumioの導入プロジェクトは2025年8月にキックオフし、同年11月に稼働を開始しました。この3ヶ月半という短期導入を成功させた背景にあったのが、先にも述べたイルミオジャパンの手厚いサポートです。

「特にありがたかったのが、ポリシー設定に関するアドバイスです。『ネットワークセグメントの設定内容がデフォルト設定と重複している』『拠点のポリシーと全社ポリシーを統合した方がよい』など、レビューを通じて細かい指摘をいただいたことで、初期ポリシーの設定が順調に進みました」（森下氏）

結果、通信の可視化機能の効果も即座に表れました。

「可視化機能は本番稼働前から利用可能な状態になっており、各サーバーがどのポートを使って通信しているのか、一目瞭然となりました。これまではシステム設計書を見ながら、一つひとつ紐解かなければならなかったことが、Illumioの画面を見るだけですぐに確認できます。さらに現時点の正確なネットワークトポロジー（構成図）の “逆起こし”も可能となりました」（森下氏）

また、取引先が同社を見る目も大きく変わりました。マイクロセグメンテーションの戦略的な導入に対して、「そこまでセキュリティ対策を徹底しているのか」と高く評価される機会が増えています。

「ペットフード、用品を仕入れている取引先は大手メーカーが大半を占めており、今後予想されるEDI（電子データ交換）に関するセキュリティガイドラインの規制強化なども見据えた対策を、先手を打って説明できることが重要なのです。『Illumioのマイクロセグメンテーション製品を導入しました』と伝えるだけで、相手方の反応が良くなりました」（森下氏）

今後の展望

人依存からの脱却と迅速な判断を目的にAI導入を積極的に検討

Illumioの導入によって同社のセキュリティレベルは大きく向上しましたが、それでも100%安心ということはありません。セキュリティ対策にゴールはないのです。

そうした中で同社が注視しているのは、生成AIを悪用してより巧妙な手口で侵入を仕掛けてくるサイバー攻撃が多発している昨今の動向です。これに対抗するためには、防御側でもAI技術を駆使することが必須となっています。

「セキュリティの攻防が『AI vs AI』の構図となった時代に合わせた取り組みを、私たちも強化していかなければなりません。例えばIllumioの導入によって可能となった動的な運用ポリシーの見直しについても、人間系に依存していたのでは攻撃側の後手を踏んでしまうおそれがあります。そこにAI技術を導入することで、より迅速な状況判断と的確な変更を行える体制を確立したいと考えています」（森下氏）

同社は引き続きイルミオジャパンのカスタマーサクセスアドバイザーと緊密に連携しながら、継続的なセキュリティ対策の強化を進めていく方針です。

Illumio（イルミオ）について

Illumioは、ランサムウェアや侵害の封じ込めにおける先駆者として、企業や組織のサイバー攻撃の封じ込めやオペレーショナルレジリエンスを向上させるアプローチを再定義しています。Illumioのプラットフォームは、AIセキュリティグラフ（AI駆動のセキュリティグラフ）を搭載し、ハイブリッド環境およびマルチクラウド環境全体で脅威を特定して封じ込めを行い、甚大な被害に発展する前に攻撃の拡大を阻止します。Illumioは、Forrester Wave™のマイクロセグメンテーション部門でリーダーとして認定されており、ゼロトラスト、インフラストラクチャやシステムにおけるサイバーレジリエンスの強化を通じて企業や組織を支えています。

イルミオジャパン合同会社
〒104-0028 東京都中央区八重洲2-2-1
東京ミッドタウン八重洲 八重洲セントラルタワー 7F
https://www.illumio.com/ja