



## SUCCESS STORY

# 2人でのセキュリティ運用を支えるTrendAI Vision One™ クラウド・オンプレミス環境のセキュリティを集約 効率良い運用を実現

株式会社ヤオコー <https://www.yaoko-net.com/>

埼玉県、日本 | 小売業 | 社員 4,347名(2024年3月末時点)

ソリューション: TrendAI Vision One™ Cyber Risk Exposure Management(CREM)、Cloud Risk Management、XDR for Endpoints、Endpoint Security、TrendAI™ Service One Complete

※Trend Vision One – Endpoint Security™、Trend Vision One – Attack Surface Risk Management™、Trend Vision One – Attack Surface Risk Management for Cloud™、XDR: Endpoint and Server、Trend Service One Completeは、それぞれTrendAI Vision One™ Endpoint Security、TrendAI Vision One™ Cyber Risk Exposure Management(CREM)、TrendAI Vision One™ Cloud Risk Management、TrendAI Vision One™ XDR for Endpoints、TrendAI™ Service One Completeに製品名が変更になりました。

## 導入の背景

首都圏に200店超の店舗を展開し、35期連続で増収増益を続けるヤオコー。スーパーマーケット業界の営業収益ランキングでも上位をキープし続けるヤオコーでは「IT施策はビジネスに直結する」(小笠原 氏)という考えから情報システム部門に相当するデジタル統括部は営業部門に属し、業績拡大につながる次の一手としてDXやCXを中心に積極的な取り組みを進めている。IT施策への注力と並行して「内部統制とコンプライアンス、そしてセキュリティはすべての企業にとって守らなくてはならない不変の柱と考えています」と語る藤森 氏を中心に2022年頃から既存のセキュリティをイチから見直す動きが加速した。

しかし、セキュリティに関するガイドラインやセキュリティインフラの整備、社員教育などを進めている最中にサイバー攻撃が発生。幸い大きな被害は発生しなかったものの、経営層を含めて改めてセキュリティの必要性を認識したことでEDRを含めた具体的な対処法についての検討が加速した。

## お客さまの課題

一度他社のEDR製品を導入したものの、運用にかけられるリソースが課題となった。EDRは日々検出されるアラートの確認や対処が必要不可欠だが、セキュリティ人材の不足が話題になる昨今、EDR運用に必要な知見を持った人材の確保は難しい。またシステムへの攻撃を防ぐEPPとシステム内に侵入した脅威をいち早く発見するEDRを別ベンダーの製品で実装すると、日々の運用や有事の際のお問い合わせ、調査などにかかる工数が、ベンダーを統一した場合と比べて大幅に増加する。

さらにヤオコーでは本部、店舗、クラウドと複数の環境を抱えているため環境ごとに導入するセキュリティ製品が変わるとさらに運用負荷が増加してしまう。ヤオコーではIT人材の採用を強化しているがセキュリティ運用だけに人員を割けるわけではないため、運用負荷を抑えつつ、セキュリティを強化できる方法を探していた。

## 導入効果:

- EDRをはじめセキュリティをTrendAI Vision One™ に集約することで日々のセキュリティ運用を効率化
- 本部や店舗のクライアントパソコンからクラウド上のサーバまで多様な環境のセキュリティを一元管理
- マネージドサービスの活用によってEDRのアラート確認にかかる時間を大幅に削減

## ソリューション

そんな時に提案を受けたのがトレンドマイクロのEndpoint Securityだった。Endpoint Securityはクライアントパソコンやサーバにセキュリティエージェントを導入することで、マルウェア対策や脆弱性対策をはじめとする複数の防御機能や、EDRを1つの製品で提供するエンドポイント向けセキュリティ製品だ。Endpoint Securityは保護対象から収集したデータをトレンドマイクロが運用するTrendAI Vision One™ というAIセキュリティプラットフォームに集約。トレンドマイクロの潤沢な知見で分析することで、脅威に対する迅速な発見・対処を支える。



「セキュリティの強化は重要ですが、DXやCXのスピードを阻害しないということも重要なポイントです」

小笠原 暁史 氏  
株式会社ヤオコー デジタル統括部長 兼  
プロダクト開発担当部長



「セキュリティは一社で取り組みば充分というものではないと考えています。業界、ひいては日本の企業全体で対策をしていく必要があると考えています」

藤森 秀雄 氏  
株式会社ヤオコー デジタル統括部 IT基盤  
ネットワーク/セキュリティ マネージャー



「TrendAI Vision One™ はUIが直感的にわかりやすく、導入後に操作に困ることが少なかった点も良いポイントでした」

内田 晶子 氏  
株式会社ヤオコー デジタル統括部 IT基盤担当

## 選定理由

ヤオコーがEndpoint Securityの導入を決定した理由は大きく3つある。1つはトレンドマイクロ自身がTrendAI™ Service One CompleteというEDRのマネージドサービスを提供していること。24時間365日のEDR監視と有事の際の調査や対処の支援をトレンドマイクロに一任できるマネージドサービスのメリットは大きかった。2つ目の理由はオンプレミスとクラウドを1つの製品で管理できること。Endpoint Securityはオンプレミス上のクライアントパソコンもクラウド上のサーバもまとめて保護できる。管理コンソールの統合や保護対象の一元管理、ベンダーの一本化によって日々の運用工数の圧縮が期待できた。そして3つ目はTrendAI Vision One™ の拡張性。TrendAI Vision One™ はEndpoint Security以外に、ネットワークやメール、モバイル端末向けのセキュリティ製品、EASM(External Attack Surface Management)やCSPM(Cloud Security Posture Management)、ITDR(Identity Threat Detection and Response)といったASM機能を提供しており、それらの管理・運用もTrendAI Vision One™ に集約できる。

※EASMやITDR機能はCyber Risk Exposure Management(以下、CREM)、CSPM機能はCloud Risk Managementで提供

2023年に公開された総務省のASM導入ガイダンスを受けてASMの必要性も感じていたヤオコーにとって、エンドポイント領域以外のセキュリティ運用までTrendAI Vision One™ に統合できるのは非常に魅力的だった。「限られた人数でヤオコー規模の会社を守っていくのは正直厳しい部分もあり、セキュリティを統合的に監視する方法が必要だと考えていました。TrendAI Vision One™ の話を聞き、「これだ」と思いました」(藤森 氏)

## 今後の展望

ヤオコーでは、本部・店舗・クラウドをつなぐネットワークや本部や店舗で活用が進むモバイル端末のセキュリティについてもTrendAI Vision One™ への集約を前提に検討を進めていく予定だ。「今後サイバー攻撃がますます巧妙化する中で、組織の体制を含めてセキュリティを強化していく必要があると考えています。トレンドマイクロにはAIをはじめ新しい技術に対しても感度の高い伴走パートナーとして継続して支援をお願いしたい」と小笠原氏は語る。

## 導入効果

他社EDR利用時にはアラート内容の確認や対処に1件あたり30分～2時間ほどかかっていたため、複数件のアラートが上がった場合は1日対応に追われることもあった。

それがエンドポイント領域のセキュリティをTrendAI Vision One™ に集約して、アラートの一次確認をトレンドマイクロのマネージドサービスが対応、対処が必要なもののみヤオコーにエスカレーションする運用に変更したことで、アラートへの対処時間を大幅に削減できた。また、CSPM機能を提供するCloud Risk Managementを導入したことで「従来は、クラウド環境ごとに管理コンソールを開いて設定状況を確認する必要のあった設定不備がTrendAI Vision One™ の画面でまとめて確認できるようになり、効率よくリスクの把握と対処ができています」(内田 氏)

## サイバーセキュリティの取り組みを 一歩先へ

株式会社ヤオコーのような組織が、TrendAI Vision One™ を活用して、どのように「リアクティブ」から「プロアクティブ」なセキュリティへと進化を加速しているのかをご紹介します。

### 詳細はこちらから

<https://trendaisecurity.com/ja>

## TrendAI™ について

TrendAI™ は、トレンドマイクロのエンタープライズ向け事業部門であり、AIセキュリティのグローバルリーダーです。AIの包括的な可視化と統合セキュリティの提供を通じて、組織に確かな信頼をもたらし、イノベーションを推進するとともに、リスクを最小化します。

現在、世界185か国において大手企業や政府機関に採用され、アイデンティティ、インフラ、データに至るまで、組織全体を横断したセキュリティを提供しています。AI Fearlessly.

<https://trendaisecurity.com/ja>