SUCCESS STORY

# EDR導入による事後対策の強化と将来的なXDR導入の道筋を整備

**高砂香料工業株式会社 https://www.takasago.com/ja**
**東京都、日本 | 香料製造業 | 3,913名(2023年3月31日現在)**
**ソリューション: TrendAI Vision One™ Agentic SIEM、TrendAI Vision One™ - Endpoint Security**
※XDR Data Retention 365 daysは、TrendAI Vision One™ Agentic SIEM に製品名が変更になりました。

## 導入の背景

高砂香料工業株式会社(以下、高砂香料工業)は、日本最大の香料メーカーとして国内はもとより、28の国と地域で飲料や食品、香水、日用品など多彩な分野に香りの価値を提供するとともに、独自の技術力を生かした医薬品向けのファインケミカル事業なども展開している。

2020年に創立100周年を迎えた同社は、国内屈指の歴史を誇る老舗企業であると同時に、先端ICT技術を駆使して常に新たなチャレンジに挑む先進企業としての顔も持つ。同社の情報システム部では国内の事務系システムのみならず、工場システム、さらには海外拠点のシステムまでも一手に管理し、グループ全体でしっかりとガバナンスを効かせながらIT活用を推進している。

同社情報システム部 部長 武田 久美子 氏によれば、情報セキュリティ対策に関しても現在、全社的な取り組みを強化しているところだという。

「NISTのサイバーセキュリティフレームワークに則ったセキュリティ対策を段階的に導入する『10カ年計画』を立案し、現在は、アクセス権限の棚卸の年2回実施をはじめ、対策マニュアルの整備や防御力と検知力の強化を推進しています。経営陣のITやセキュリティに対する理解も深く、グローバルで事業リスクを減らすためにもセキュリティ対策強化を進めています」

「海外拠点からサポート窓口に直接問い合わせできるよう調整いただいたおかげで、グローバルでのセキュリティ対策を大幅に強化できました」
武田 久美子 氏
情報システム部 部長

「営業担当の方にはいつも親身になって対応いただいており、さまざまな情報もご提供いただいており大変助かっています」
星野 智和 氏
情報システム部 副部長

**導入効果:**

- EDRの導入により社内環境に潜む脅威を迅速に検知·排除
- 誤検知の低減によりセキュリティ対策業務を効率化
- 管理コンソールの統合でより容易かつ迅速にセキュリティ状況を把握

## お客さまの課題

そんな同社は2022年、PCをはじめとするエンドポイント端末のセキュリティ対策を大幅に見直すことになった。きっかけとなったのは、5年に一度訪れるシステム基盤の更改だ。同社は大手SIパートナーが運営するデータセンターで自社システムを構築·運用しており、ハードウェア機器の老朽化や保守期限満了に伴うインフラ刷新を5年間隔で実施している。

2024年に実施予定の次期刷新に向けて新たなインフラ基盤を検討するにあたり、「同時にエンドポイントセキュリティ対策も強化できないか」という声が上がった。その背景について、同社情報システム部 須藤 伸一 氏は次のように述べる。

「以前のエンドポイントセキュリティ製品はマルウェアの侵入を防御する機能に特化していました。しかし近年のサイバー攻撃は極めて巧妙で、既存の防御技術を巧みにすり抜けてきます。そのため、万が一防御を突破されて侵入を許してしまった際に備えて、脅威を検知·排除する必要性を強く感じていました」

また同社情報システム部 副部長 星野 智和 氏は、別の観点からも既存のエンドポイントセキュリティ製品に課題を感じていたと語る。

「既存のエンドポイントセキュリティ製品では、正規のファイルであるにも関わらずマルウェアとして誤って検知してしまう『誤検知』が頻繁に発生しており、その正誤を調査するのに多大な手間を強いられていました。そのためより検知精度が高く、誤検知の少ない製品を模索していました」

## 選定理由

そこで同社は、データセンターを運営するSIパートナーに新たなエンドポイントセキュリティ製品の提案を依頼。同時に自社でも複数のエンドポイントセキュリティ製品をピックアップし、それぞれの機能や性能、コストなどの比較検討を行った。その結果、最終的に同社が選んだのが、トレンドマイクロが提供するクラウド型のエンドポイントセキュリティ製品「TrendAI Vision One™ - Endpoint Security」(以下、Endpoint Security)だった。

同製品を選んだ理由について、武田 氏は「もともとトレンドマイクロのメールセキュリティ製品を国内外で利用していたのですが、海外拠点からもサポート窓口に直接問い合わせできるようになるなど柔軟な対応をしていただき、ベンダーとして高い信頼を寄せていました」と、トレンドマイクロのセキュリティベンダーとしての高い信頼性や柔軟な対応力を挙げる。

また同社では、スキャン機能やログ監視など複数のセキュリティ機能を1製品で提供するサーバ環境向けの総合セキュリティ製品、「TrendAI™ Deep Security™」を数年前に導入していた。これに加えてエンドポイントセキュリティ製品もトレンドマイクロ製品に統一するメリットについて、須藤 氏は次のように期待を述べる。

「サーバのログとエンドポイントのログを別々の製品で収集・管理するのは運用効率が悪いため、可能であれば単一のコンソールで一元的に管理できればと考えていました。その点トレンドマイクロは現在、XDR機能のあるTrendAI Vision One™ 上で一元管理できるようアップデートさせているため、弊社の方針とも合致していると考えました」

## ソリューション

まずは国内で利用されているPC約2000台に対して TrendAI Vision One™ - Endpoint Security を導入し、エンドポイントセキュリティ対策を強化することにした。現時点では導入に向けた準備を行っており、導入が完了した暁にはEndpoint Securityが備えるEDR(Endpoint Detection and Response)機能を活用することで、これまで手薄だった「侵入を許した脅威の検知・排除」を大幅に強化できるものと期待しているという。

またEndpoint Securityのログ(PC上のアクティビティデータ)は、標準では30日間分をクラウド環境上に保管するが、高砂香料工業ではこれを1年間保管できるオプション契約を締結している。その理由について武田 氏は「弊社のセキュリティポリシーでは、万が一インシデントが発生した際にその原因や影響範囲を正確に調査できるよう、ログを1年間分保管するよう定めています。確かにログの長期保管にはコストが掛かりますが、インシデントの全体像を迅速かつ正確に分析できる安心・安全にはかえられません」と説明する。

さらには、以前に利用していたエンドポイントセキュリティ製品と比べ誤検知率が低いという評価もあり、ホワイトリストを使って誤検知を低減する設定をコンソール上で行うことができる点など、誤検知の減少による運用効率の向上も期待しているという。

「トレンドマイクロのXDRの機能を使えばサーバやエンドポイントの状況を一元的に把握でき、効率的かつ迅速な対応が可能になるのではと期待しています」

須藤 伸一 氏
情報システム部

## 今後の展望

将来的に、さまざまなセキュリティ製品を一元的に管理することで、セキュリティ対策業務のさらなる効率化を図っていきたいとしている。トレンドマイクロのAIセキュリティプラットフォーム「TrendAI Vision One™」はエンドポイント、サーバだけでなく、幅広いレイヤーのセキュリティ対策や製品ライセンスといった情報を共通の管理コンソールで一元管理できるため、星野 氏は「将来的にはぜひ活用の幅を広げて行きたい」と大きな期待を寄せる。

「管理コンソールの統合は大いに楽しみにしています。その他の面においてもトレンドマイクロのソリューションの進化に期待しています。製品面だけでなく、技術的なサポートの面でも本当に親身になって支援いただいていますので、引き続き弊社にとって価値の高い提案をぜひお願いできればと思います」

## サイバーセキュリティの取り組みを一歩先へ

**高砂香料工業株式会社のような組織が、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