



神奈川県教育委員会

🌐 <https://www.pref.kanagawa.jp>

📍 神奈川県、日本

🏢 教育委員会

導入製品・ソリューション

- Trend Vision One
 - Trend Vision One Endpoint Security Essentials
 - Trend Vision One Email and Collaboration Security Essentials
 - Trend Vision One XDR Add-on: Email
 - Deep Discovery Inspector Virtual Appliance 1000 with XDR
- 教育委員会取りまとめ用 Trend Micro エディケーションパック
- Trend Service One Complete
 - Trend Service One Complete 基本サービス
 - Trend Service One Complete for MXDR Endpoints and Workloads
 - Trend Service One Complete for MXDR Messaging
 - Trend Service One Complete for MXDR Network 1Gbps

導入効果

- 本来ICT専任ではなく、教員である管理者の運用負担軽減、ヒトに依存しないセキュリティ運用体制の継続性も意識した構築
- クラウド利活用による「境界防御の穴」を、適所に配置した多層防御で保護
- 平時運用時の脅威を高い精度で検知することでインシデント発生時の迅速な対応を実現
- 単一のクラウドコンソールで情報の一元管理と相関分析による可視化で運用負担を低減

校務DX実現に向けたステップアップ型ゼロトラストの実現 「Trend Vision One」による校務&学習システム環境の保護と可視化と「Service One Complete」で強固な運用体制を実現

Before	After
<ul style="list-style-type: none"> ・校務ネットワークからのクラウド利用における、Microsoft 365のセキュリティオプションの防御力の物足りなさ ・システムおよびセキュリティ運用を現ITC担当教員の個人スキルに依存 ・導入済みネットワーク制御(SDN)の効果が低く、結果、属人化した運用が必要 ・各製品独自のセキュリティアラートを人手で繋ぎ合わせる煩雑さ 	<ul style="list-style-type: none"> → クラウド、サービス採用で、ITC担当者のスキル取得の負担を軽減 → Microsoft 365とのAPI連携で高度なメールセキュリティを提供するICES(*1)製品と教員端末の保護のための次世代EPP+EDR製品の連携による防御力強化 → 予防対策製品とXDR(*2)による検知を相関分析するTrend Vision Oneのアラートで、インシデントを迅速に把握 → 高度な脅威分析やインシデント対応が可能なセキュリティエキスパートによるお客様の負担軽減と安全性の維持

*1 Integrated Cloud Email Security
*2 Extended Detection and Response

導入の背景

神奈川県教育委員会は、県立高校全日制だけでも生徒数10万人以上、加えて教職員1万人以上を擁し、その校務や学習を支えるシステム運用、監視には多大なリソースがかかっていた。その一方でその運用は、自力でITCを学習した担当教員の個人スキルに依存し、少人数での対応を行ってきた。

その後クラウド利活用が求められ、Microsoft 365などを採用したが、「境界防御の穴」に対する防御力に問題を抱えていた。

更に令和5年3月、文部科学省から「GIGAスクール構想の下での校務DXについて」が公示され、現状は分離されている校務系ネットワークと学習系ネットワークの統合と、セキュリティ向上が求められることになり、より高度で複雑な業務運営に円滑に対応する必要に迫られていた。

お客様の課題

長期間神奈川県教育委員会配下のハードウェアやネットワーク、更にセキュリティなどを支えてきた担当者の定年退職も近付き、後継者の指名・育成が必要とされる中、オンプレミスシステムの運用のように、全てのスキルセットを担当が習得することは短期間では困難と考えていた。

また、セキュリティ強化のために、Microsoft 365には有償オプションであるAdvanced Threat Protection(現:Microsoft Defender for Office 365)を採用していたが、その防御力の物足りなさから重要な校務系のセキュリティ対策の穴に不安を感じていた。

さらに文部科学省のガイドラインに従った今後の校務DXの推進では、更なるクラウドの利活用や、校務と学習ネットワークの統合が求められており、今以上のセキュリティ対策が必要とされ、本番環境で効果が薄く、人手による運用を必要としている導入済みのSDNとは異なり、運用者が稼働後に破綻しない、効率的かつ効果的なセキュリティ基盤を必要としていた。

選定理由

トレンドマイクロ社については、導入済みの**Deep Discovery Inspector**の検知・可視化による運用性の高さを実感。セキュリティ状況と重要度を直感的に把握でき、運用負荷軽減に効果が高い同社の**SaaS**製品の選択が、今後人に依存しない運用実現の前提と考えていた。また**Microsoft 365**の防御力、予防力を高めると同時に、重要な教職員の利用する**Windows**端末で「事後対策としての検知と対処ができる」ことは、今後見据えるゼロトラストに必要な要素と判断した。複数のセキュリティモジュールが連携して動作し、運用負荷を下げることも加点要素とした。

複雑化するセキュリティ運用は、組織内での対応が困難と予想、マネージドサービスも要求仕様を含め、公平な入札仕様を作成し公募したが、「この要求仕様を満たし入札できたのは、**Trend Vision One**を中心として連携されたセキュリティ製品と、自社で支援する**Service One Complete**を提供するトレンドマイクロ社だけでした」と担当者は語る。

ソリューション

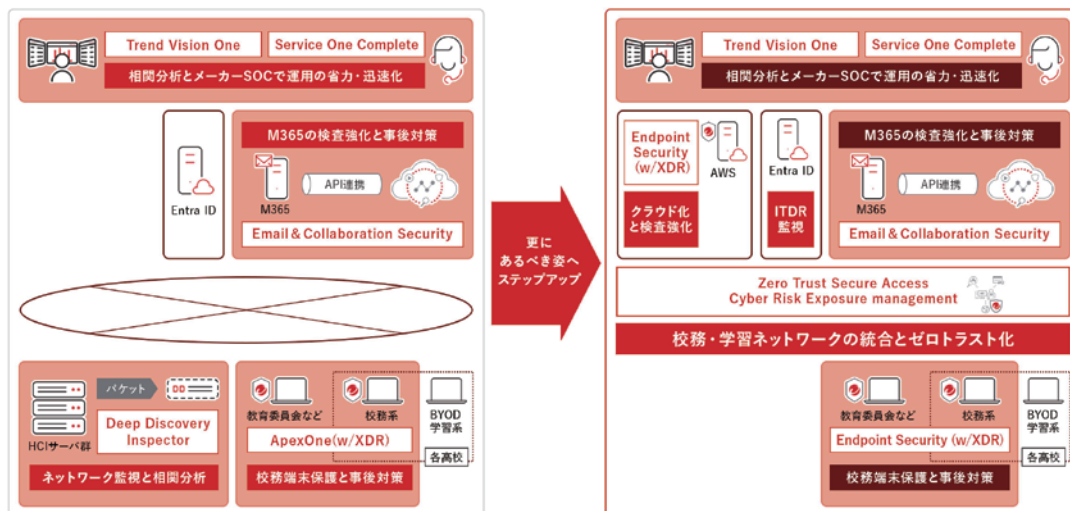
Trend Vision Oneは、セキュリティの統合コンソールとしてだけでなく、エンドポイント、メールなど複数レイヤーのデータ(テレメトリ)を一箇所に収集、相関分析、概要を可視化、必要に応じて詳細を確認可能。事後対策の検知と対処を含め、少人数で運用可能なセキュリティプラットフォームとしての大きな役割を担っている。**Trend Vision One Email and Collaboration Security**で**Microsoft 365**の防御力を向上するとともに、メールボックスやクラウドストレージ上の脅威を検知し対処。教職員が利用する端末やサーバに配置した**Trend Vision One Endpoint Security**と連携することで、「単なるデバイス向けのEDRではなく、複数のセンサーを繋ぎ合わせる**XDR**を実現し、分かり易いダッシュボードで表示してくれます」と評価する。更に、**Service One Complete**によるセキュリティサービスは、**Trend Vision One**を活用してトレンドマイクロのセキュリティエキスパートが**24時間365日**監視し、アラートの中から対処すべき優先度が高い攻撃や脅威の兆候を通知する。また、このサービスは一次対応だけでなく、脅威の侵入経路や方法、影響範囲を特定し、対処方法を指示。「管理者の異動時にも、個々人のスキルセットに左右されず安定した運用が実現できると考えています」と、サービスへの期待も高い。

●今回の導入:

ハイブリッド構成を元に**SaaS**アプリの安全性と運用容易性の強化

●あるべき姿へ:

オールクラウド化にも対応可能なゼロトラストと更なる運用統合



導入製品・ソリューション

詳細については、下記にアクセスしてください。

- **Trend Vision Cloud One - Workload Security™**
www.go-tm.jp/c1ws
- **Trend Service One™ Complete**
www.go-tm.jp/sl
- **Trend Micro Managed XDR™**
www.go-tm.jp/mxdr1
- **Trend Vision One™**
www.go-tm.jp/v1

トレンドマイクロ株式会社

www.trendmicro.com

TREND MICRO、TREND MICRO、およびASRMは、トレンドマイクロ株式会社の登録商標です。記載内容は2024年11月現在のものです。内容は予告なく変更になる場合がございます。
※製品・サービスの導入効果は、ご利用企業・組織の方の声に基づくものであり、お客様のご利用状況により効果は異なります。
Copyright © 2024 Trend Micro Incorporated. All rights reserved.
[BR-CASE-282]

東京本社 〒160-0022 東京都新宿区新宿4-1-6 JR新宿ミライナタワー
TEL.03-4330-7601 (法人お問い合わせ窓口)
名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内3-22-24 名古屋桜通ビル7階
TEL.052-955-1221
大阪営業所 〒532-0003 大阪府大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル13階
TEL.06-6350-0330 (代表)
福岡営業所 〒812-0011 福岡県福岡市博多区博多駅前2-3-7 シティ21ビル7階
TEL.092-471-0562

1年以上の運用を経て、各セキュリティ製品の防御力、加えてアラートとその監視による効果を実感。「より詳細な情報と合わせて、今対応が必要な重要度の高いイベントが把握できるため、得られた情報を高度なセキュリティ対策に容易に活用できている。また**Trend Vision One**のコンソールだけですべての情報を一元的に把握できるようになったので、個々のコンソールを行き来する様な以前の運用負荷とは雲泥の差です」
また、「トレンドマイクロの監視サービスや支援サービスを受けられるようになり、われわれの環境や実現したいことを理解した専任のエンジニアがアサインされているので、何か相談したいことがあった際には迅速に対応してもらえること、また定期的な面談により、最適な運用の実現や脅威動向などの勉強会も実施され、組織のセキュリティの意識が高まり、とても助かっています」

今後の展望

神奈川県教育委員会では、数年後に迫った次回のネットワーク更改で、校務系と学習系のネットワークの統合とセキュリティの両立を行うために、単なる認証ではなくゼロトラストアーキテクチャへのステップアップを考えている。

今回の調達においてゼロトラストの基礎となる部分をトレンドマイクロの**Trend Vision One**で構築しているため、現在の構成にゼロトラストネットワークアクセス(ZTNA)やセキュアWebゲートウェイ(SWG)、CASB(Cloud Secure Access Broker)を提供する「**Trend Vision One Zero Trust Secure Access**」を追加することで、実現できると想定している。更に有事の際の対応であるXDRだけでなく、平時のリスクの予兆検知や、攻撃対象領域の把握による予防措置につながるアタックサーフェイス管理(ASM)として同社の「**Cyber Risk Exposure Management**」なども合わせて検討し、ゼロトラストの概念である「いつでも、どこでも、同じセキュリティレベル」に近づいていくことを考えている。