ーお客様導入事例ー

Networld

学校法人成城学園 成城大学

所在地：東京都世田谷区成城6-1-20
ＵＲＬ：https//www.seijo.ac.jp/

VMware Carbon Black Cloudを導入し 端末の可視化と的確な脅威対応を実現 学内のセキュリティ強化に貢献

[BEFORE]
- ◆ネットワーク内に侵入した脅威の存在や攻撃プロセスなどを明確に証明できない
- ◆テレワークで働く職員の情報セキュリティを確保する必要がある

[AFTER]
- ◆端末の挙動や操作をすべて可視化することで、的確な状況把握と脅威対応を実現
- ◆リモートからの調査・検索やマルウェア感染端末の遮断が可能に

キャンパス内に潜む 脅威の存在証明が課題に

学生一人ひとりの個性に主眼を置き、グローバル社会を生き抜く「独立独行」の人材を育成する成城大学。その教育の歴史は、実に100年以上前にまで遡る。また、長い伝統を有する一方で、時代を先取りした取り組みを積極的に推進しているのも同大学の大きな特長だ。

たとえば、8号館1階に設置された「Lounge #08（ラウンジナンバーエイト）」には、観葉植物が配されたカフェ風のスペースに、Wi-Fi6対応の高速な通信環境を整備。学生がいつでも気軽にPCやネットを利用できる環境を提供することで、ITに関するスキルやリテラシーを自然に身に着けられるようにしている。

ただし最近では、IT面で解決すべき課題も抱えていたとのこと。それは学内の情報セキュリティ強化だ。メディアネットワークセンター 課長 五十嵐 一浩氏「最大の問題は、ネットワーク内に脅威が存在しなかったという『悪魔の証明』をいかに成立させるかという点です。もちろん本学でもセキュリティには細心の注意を払っており、様々な製品を導入して対策を行っています。しかし、そこから上がってくるアラートやログなどをいくら積み上げても、情報漏えいなどの被害が本当に無かったと実証することが困難だったのです」と語る。

成城大学
メディアネットワークセンター
課長
五十嵐 一浩 氏

VMware Carbon Black Cloudで エンドポイント対策を強化

万一何らかのセキュリティ被害が生じた場合、それを証明するのは簡単である。なにしろ被害という実態が歴然と存在するのだ。しかし、「何も起きていなかった」ことを証明するのは相当な難題である。メディアネットワークセンター 大高 一真氏は「たとえばゲートウェイ製品から、怪しいサイトへのアクセスを示すログが見つかった場合、そこに大事な情報を入力したりしていないか調べるには、PCの操作履歴をチェックするしかありません。とはいえユーザーも、当時の操作を全部覚えてはいませんので、結局いろんなデータを突き合わせて『おそらく大丈夫だったはず』と結論付けるしかありませんでした」と振り返る。

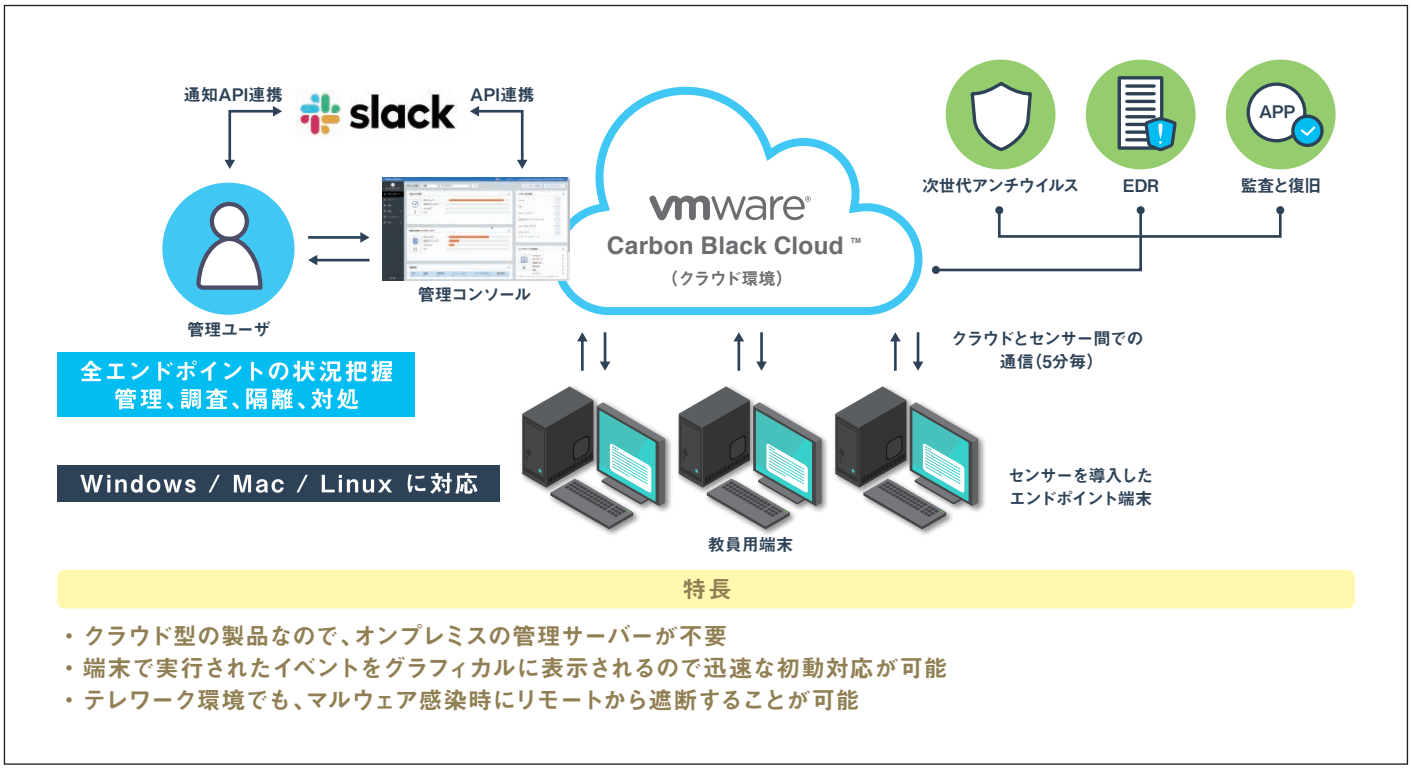
成城大学
メディアネットワークセンター
大高 一真 氏

このような課題を解決するものとして、近年注目を集めているのが、いわゆる「EDR（End-point Detection & Response）」製品である。脅威の侵入を防ぐことを目的とするアンチウイルス製品に対し、EDRは内部に侵入した脅威の検知とその後の対処を目的とする。実は同大学でも早くからエンドポイント対策の有用性に着目し、あるベンダーのEDR製品を既に導入していた。しかし、データの収集や分析に時間が掛かる、使い勝手が良くないなど問題が多く、なかなか思うような成果を上げられなかったという。

そこで同大学では、新たなEDR製品の導入を検討。ここで白羽の矢が立てられたのが、ネットワールドが提供する「VMware Carbon Black Cloud」だ。五十嵐氏は「私自身、VMware User Groupでリーダーを務めていることもあり、VMwareの旧Carbon Black社買収には強い関心を持ちました。クラウド型の製品ですから、オンプレミスの管理サーバーを自前で運用する必要もありませんし、大量ログの保管場所にも悩まされずに済みます。また、物理／仮想両方の環境を監視できる点や、エージェントだけで使える手軽さなども評価し、採用を決めました」と語る。

端末の挙動を明確に可視化 初動対応もスピーディに

具体的な監視対象としては、大学の事務業務で利用されるPC約160台を選定。実際の導入作業も非常にスムーズに進んだという。「今



回のような取り組みでは、複数のセキュリティ製品同士が競合してうまく動作しないケースも多い。その点、VMware Carbon Black CloudはNGAV（次世代アンチウイルス）とEDRの両方の機能を備えた製品でありながら、すんなりと既存環境に導入できました」と五十嵐氏。大高氏も「端末へのエージェント配布なども、手持ちの資産管理ソフトを利用することで20～30分程度で完了しました。あまりにも簡単に終わったので、本当に導入できたか逆に不安になったくらいです」と続ける。

この結果、VMware Carbon Black Cloudは2021年4月より本番稼働を開始。これにより、同大学のセキュリティ運用にも大きな改善効果が生まれている。まず一点目は、課題であった端末の操作や挙動を可視化できた点だ。VMware Carbon Black Cloudには独自のストリーミング分析機能が備わっており、PCで実行されるイベントをすべて記録／タグ付けして相関分析する。このため、いつ・どのように実行されたアクションがインシデントの原因なのかを突き止めることが可能だ。

成城大学
メディアネットワークセンター
ITコンサルタント
田村 忠才 氏

メディアネットワークセンター 田村 忠才氏は「さらに大きいのが、それぞれのイベントのつながりをグラフィカルに表示してくれる点です。これなら高度な専門知識を持たないメンバーでも、素早く正確な判断を下せます。このことは、初動対応のスピードを上げていく上で非常に大きなメリットとなります」と語る。

さらに五十嵐氏も「ファイルサーバーからデータを持ち出す際に、端末側からメディアにコピーされたらゲートウェイでは検知できません。その点、VMware Carbon Black Cloudがあれば、このような行為もエージェントで確実にキャッチできます。懸案であった『悪魔の証明』は、ほぼ実現できたと言えるでしょう」と力強く語る。

テレワークの安全確保に寄与
リモートからの端末制御も可能に

加えて、もう一つ見逃せないのが、安全なテレワークの実現にも役立っている点だ。五十嵐氏は「本学でも緊急事態宣言下ではテレワークを実施していますので、自宅などで働く職員向けに、VMware Carbon Black Cloudのエージェントを導入した貸出端末を用意しました。各端末の状況把握はもちろん、マルウェア感染時の遮断などもリモートから行えますので、学外でも安心して働くことができます」と五十嵐氏は語る。

ネットワールドのサービス・サポートも、今回の取り組みに大きく貢献。大高氏は「PoCの段階では低レベルの脅威もすべて通知する設定で運用を開始したため、軽微なアラートが大量に発生しました。こうしたものどこまで無視して良いのか、ユーザーだけで判断するのは非常に難しい面があります。その点、経験豊富なネットワールドから様々な運用ノウハウを提供してもらえますので、大変助かっています。EDR製品は長く使い続けるものですから、経験豊富なパートナーの力が非常に重要ですね」と満足げに語る。

このように大きな成果を収めた同大学だが、今後も学内のセキュリティ強化に努めていく考えだ。五十嵐氏は「我々が目指す『ゼロトラスト』の実現に向け、今後も環境改善を続けていきたい。ネットワールドの提案にも、大いに期待しています」と述べた。

お問い合わせ

株式会社ネットワールド
https://www.networld.co.jp/
vmware-info@networld.co.jp

本　　社　〒101-0051 東京都千代田区神田神保町2-11-15
住友商事神保町ビル
TEL：03-5210-5020,5031,5095

関 西 支 店　〒530-0001 大阪市北区梅田3-3-20
明治安田生命大阪梅田ビル 24F
TEL：06-7777-4174

中 部 支 店　〒450-0003 名古屋市中村区名駅南1-17-23
ニッタビル 10F
TEL：052-588-7611

九 州 支 店　〒812-0013 福岡市博多区博多駅東2-6-1
九勧筑紫通ビル 3F
TEL：092-461-7815