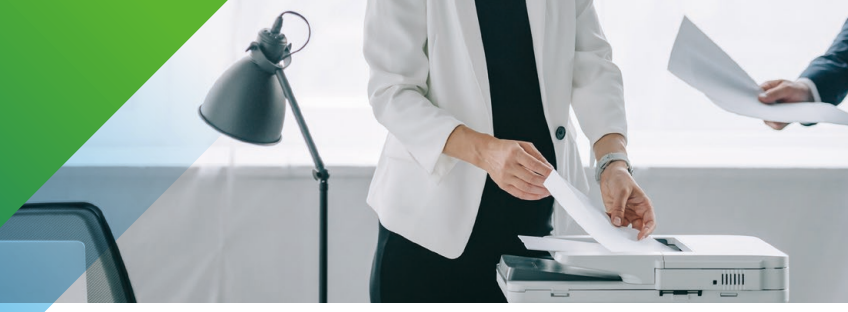
vmware®

CUSTOMER CASE STUDY



世界の拠点に配備された約50,000台のエンドポイントに次世代型アンチウイルスを導入。高度化が進む脅威に対抗するため、検知率と運用負荷を大きく改善

EPSON
EXCEED YOUR VISION

主力のプリンターやプロジェクターのほか、ウェアラブル機器やロボットの分野にも積極投資し、世界を舞台にビジネスを拡大するセイコーエプソン。日本を代表するものづくり企業として、情報セキュリティに対する取り組みもグローバル規模で力を入れており、全社的なセキュリティレベルの向上を図っている。今回同社では、国内外の事業所とグループ会社に配備された約50,000台にのぼるPCなどの端末に、カーボン・ブラックの次世代型アンチウイルス「CB Defense」を一斉導入する。多様化、高度化が進むサイバー脅威に打ち勝つため、エンドポイントセキュリティの本格的な強化に乗り出した。

導入前の課題

パターンマッチングによる
従来型アンチウイルスをすり抜ける
マルウェアが急増した

パターンファイルの容量や
更新頻度の増大で運用負荷の
軽減が急務となった

導入効果

未知のマルウェアや
非マルウェア攻撃の検知率と
運用負荷が大きく改善した

EDR機能によって
海外拠点などに対する
遠隔管理が容易になった

業界

MANUFACTURING

プロフィール

セイコーエプソンは、インクジェット技術に強みを持つプリンティングソリューションズ事業、液晶プロジェクターなどのビジュアルコミュニケーションズ事業、ウオッチなどのウェアラブル機器事業、産業用ロボットのロボティクスソリューションズ事業の4つを軸にビジネスを展開する国内屈指の情報機器・精密機器メーカー。1942年創業の同社は現在、国内16社、海外71社のグループ会社、76,000名超の従業員を抱える企業に発展し、その活躍の場は世界に広がっている。

「検知率の高さもさることながら、マルウェアの動きが詳細に示されるCB Defenseは、次の運用に生かせる有益な情報を数多く提供してくれます」

セイコーエプソン株式会社
征矢 隆志 氏

導入環境

- CB Defense（現VMware Carbon Black Cloud Endpoint Standard）

世界の拠点に配備された約50,000台のエンドポイントに
次世代型アンチウイルスを導入。高度化が進む脅威に
対抗するため、検知率と運用負荷を大きく改善

経営課題としてのセキュリティ強化の一環で エンドポイントセキュリティを刷新

セイコーエプソンは、インクジェット技術に強みを持つプリンティングソリューションズ事業、液晶プロジェクターなどのビジュアルコミュニケーションズ事業、ウオッチなどのウェアラブル機器事業、産業用ロボットのロボティクスソリューションズ事業の4つを軸にビジネスを展開する国内屈指の情報機器・精密機器メーカーだ。1942年創業の同社は現在、国内16社、海外71社のグループ会社、76,000名超の従業員を抱える企業に発展し、その活躍の場は世界に広がっている。

会社の成長とビジネス領域の拡大に伴い、セキュリティ対策の強化も継続的に進めてきた。2007年には「情報セキュリティー基本方針」を策定（2017年改訂）、個人情報保護や知的財産保護を優先的な経営課題の一つと位置付け、全社をあげてセキュリティ管理体制の整備と強固なセキュリティシステムの構築を推進している。

こうした取り組みの一環として今回、さらなるセキュリティレベルの向上を目的に、エンドポイントセキュリティの強化を図ることになった。PCをはじめとする端末は、国内外の拠点に約50,000台。この膨大な数のエンドポイントをどうやって守るのか。個人情報や知的財産の保護における生命線であるエンドポイントセキュリティ対策の切り札として、カーボン・ブラックの次世代型アンチウイルス「CB Defense」が選ばれた。

マルウェアの急増と高度化で見えてきた パターンマッチングの限界

セイコーエプソンではこれまで10年以上の間、エンドポイントセキュリティ対策にパターンマッチングによる従来型アンチウイルスを利用してきた。マルウェアの数や種類が少なかった時代は、新しいマルウェアが出現するたびにパターンファイルを更新することで十分に対応できた。しかし、最近は新種のマルウェアがどんどん増えている。マルウェアが高度化・複雑化してくると、1件ずつ詳細な調査が必要になる。マルウェアの数は瞬く間に膨大になり、対応が間に合わなくなってきた。

エンドポイントセキュリティの見直しのきっかけの1つは、パターンファイルの更新の手間が増大したことだ。これについて、IT推進本部 IT基盤企画設計部 課長の征矢隆志氏は、「以前は1週間に1回程度パターンファイルを更新すればよかったものが、そのうち毎日に、そして1日に数回と増えていきました。マルウェアの数もさることながら、攻撃手法も多様化してパターンマッチングでは検知できないものが増え、従来型の方式に限界を感じるようになりました」と説明する。

もう1つは、マルウェアの増加によりパターンファイルが肥大化したことだ。パターンファイルの容量が急激に増え、サーバーのディスクが不足するという問題も起きた。パターンファイルが大きくなりすぎて、更新の際にネットワークがパンクするという事態も経験した。1日に何回も新しいパターンファイルに更新しているのにも関わらず、見つからないマルウェアは増える一方であった。こうした状況からの脱却を目指し、新しいアンチウイルス導入の検討が本格化する。

> 「検知率の高さもさることながら、マルウェアの動きが詳細に示されるCB Defenseは、次の運用に生かせる有益な情報を数多く提供してくれます」
>
> セイコーエプソン株式会社
> **征矢 隆志 氏**

検知率の高さと製品コンセプトが 評価されて選ばれた「CB Defense」

検討開始当初は、従来型アンチウイルスの枠組みの中で新たな製品を選定しようしていた。パターンファイルが少なくて済み、より性能と運用に優れた製品を探していたのである。しかし、パターンマッチング方式はすでに確立された技術であり、どの製品も性能に大きな差があるわけではない。既存のアンチウイルスを置き換えるだけの意味はあるのか。そうした懸念を持ちつつ検討を続けているタイミングで、パターンマッチングに頼らない新しいテクノロジーを基盤にした次世代型アンチウイルスが登場し始める。

そこで、従来型と次世代型あわせて5製品を評価・検証することになった。

従来型2製品、次世代型3製品を検証した結果、まず証明されたことは、次世代型アンチウイルスの検知率の高さだ。既存のサンドボックス製品で採取していたリアルな検体を使ったテストでは、従来型の各製品が30%ほどの検知率だったところを、次世代型は100%検知することができたのである。POC期間中には、ランサムウェアに繋がる最初のダウンローダーも検知された。こうした結果により、今後も増え続ける未知のマルウェアや非マルウェア攻撃に対抗するには、次世代型アンチウイルスの導入が不可欠との結論になった。

次世代型アンチウイルスの製品選定では、製品のコンセプトが重視され、カーボン・ブラックの「CB Defense」に決定される。最終的な選定理由について、IT推進本部 IT基盤企画設計部 シニアスタッフの北原健氏は次のように述べている。「CB Defenseでは、マルウェアを検知すると、そのマルウェアがどんな動きをして、なぜ見つけられた

世界の拠点に配備された約50,000台のエンドポイントに
次世代型アンチウイルスを導入。高度化が進む脅威に
対抗するため、検知率と運用負荷を大きく改善

（写真右）
IT推進本部
IT基盤企画設計部
課長
征矢 隆志 氏
（写真左）
IT推進本部
IT基盤企画設計部
シニアスタッフ
北原 健 氏

のか、といった情報が詳しく示されます。一方、他の製品ではなぜ検知されたかの情報が提供されないものもあります。検知したという情報だけでは不十分ですし、納得できません。我々は検知・ブロックしたから終わりではなく、必ず次に生かす運用を心がけています。CB Defenseは我々の運用方針に合致する製品だと確信しました」

なお、セイコーエプソンのプロジェクトメンバーは、製品の検討期間中に米国マサチューセッツ州ボストンにあるカーボン・ブラック本社を訪問している。カーボン・ブラックの多くのスタッフと会話し、その企業風土に共感したという。「顧客の声を大事にして、要望を伝えると真摯にくみ取ってくれる姿勢や、ユーザーコミュニティが充実していることも大きな評価ポイントになりました」（北原氏）。

今回の次世代アンチウイルス導入は海外拠点を含めた大規模な展開だったが、検討の初期段階から海外拠点の担当者を意識的に巻き込むことで、その後の社内調整がうまくいったという。エンドポイントの入れ替え検討は2年前から始まったが、次世代型を具体的に検討し始めたのは後半の1年。検討、準備に3か月、POCに3か月、結果の精査、製品選定に3か月かかった。

重大なマルウェアの検知と運用負荷が大きく改善
今後はEDRの効果にも期待

CB Defenseはまず、国内外の拠点にある約47,000台のエンドポイントに展開された。北原氏は、「CB Defenseは展開が非常に簡単なので、3か月という短期間でこれだけの台数を完了させることができました。以前は各国にサーバーが必要だったので、現地に構築手順から指示するなど手間がかかりましたが、CB Defenseはクラウドベースなので展開がスピーディでした。途上国など回線の細い拠点においても問題なく展開できました」と話している。海外含めて同じテナントに同居して運用するのは今回が初めてのことで、残りの約3,000台はヨーロッパを中心に近日中に展開される予定だ。

すでに導入効果も出ている。以前は見つからなかったマルウェアも検知され始めているという。運用面についても、「CB Defenseを自社で運用していますが、マルウェアを自動で止めてくれることが多いので、管理コンソールに張り付いている必要がありません。ポリシーも柔軟にカスタマイズでき、自社環境に合ったポリシーが作れるのも利点です。CB Defenseは、製品として尖った良さを持っています」と北原氏は評価する。

CB DefenseのEDR（Endpoint Detection & Response）機能にも大きな期待が寄せられている。これまでサンドボックスで検知したマルウェアが海外拠点などの遠隔地だと、初動調査に半日から1日かかっていたが、調査完了まで何も対処ができなかった。しかし、CB Defenseを使えば、感染PCの特定、ネットワークからの隔離、ファイルの削除などが遠隔から即座にできるので安心感があるという。また、以前はインシデントの調査と対応においては、ウイルスの横展開を調べるのにログ収集などで2週間も費やしていた。これについては、CB Defenseを使うことで横展開の様子が把握でき、ハッシュを検索して削除すれば調査と対応が2日で完了するという試算も出ている。

今後は、別系統のシステムとなっている工場のエンドポイントセキュリティの強化にも取り組む予定だ。今後の計画について、征矢氏は次のように語った。「工場はネットワークを分離して運用しているので、別の対策を講じなければなりません。具体的にはホワイトリスティングを用いたアプリケーション制御の導入を見据えて、カーボン・ブラックの「CB Protection」を含め幅広い製品を比較・検証している最中です。カーボン・ブラックにはこれからも、ユーザーの声を開発に生かす姿勢を持ち続けていただきたい。その上でタイミングよく魅力的な製品をリリースしてくれることを期待しています」

※本内容は2018年当時の取材に基づいて記載しています。

vmware®

ヴイエムウェア株式会社　〒105-0013 東京都港区浜松町1-30-5 浜松町スクエア13F　URL：www.vmware.com/jp
Copyright © 2020 VMware, Inc. All rights reserved. Protected by U.S. and international copyright and intellectual property laws.
VMwareおよびVMwareロゴはVMware, Inc.の商標です。他のすべての社名および製品名はそれぞれの企業の商標です。 Item No. CS_Epson_JPQ220