<<左より>> 株式会社シー・エル・シー
取締役　経営企画本部長 萩原　克彦氏
ビジネス推進部　部長　日向　修氏

ソフォスの販売代理店として、いち早くソフォス製品を自社導入しクラウド管理を行ったことで、Synchronized Securityによる容易でコスト効率に優れた運用管理を行えることを体感できた。

“ソフォスのEDR対応製品の導入により、インシデントがいつどのように発生し、データやシステムにどのような影響を与えたのかといったインシデント対応を高い水準で行えるようになったのが大きなメリットです。また、Synchronized Securityにより、ファイアウォールとエンドポイントをクラウドで一元管理できるようになったことで全体的な管理工数やコストを削減することができました”
株式会社シー・エル・シー 取締役　経営企画本部長 萩原　克彦氏、

CUSTOMER-AT-A-GLANCE

CLC corporation

株式会社シー・エル・シー
東京都港区虎ノ門1-21-19
東急虎ノ門ビル5階

社員数
30名強

Webサイト
www.clc.co.jp

ソフォスカスタマー
ソフォス製品導入年数：12年

ソフォスソリューション
Intercept X Advanced with EDR
Sophos Intercept X for Server with EDR
XG Firewall
Sophos Central

Synchronized　Securityにより、人手では決して対応できないミリ秒あるいは秒単位で訪れてくる攻撃を瞬時にかつ自動的に阻止、隔離したのを目の当たりにすることができました。仮に感染することがあっても、拡散することがないという確信を得ることができました。

株式会社シー・エル・シー
ビジネス推進部　部長　日向　修氏

株式会社シー・エル・シーは、1980年4月より主にメインフレームやストレージなどのハードウェア製品、米国で開発されたソフトウェア製品の輸入販売およびその導入サポートを手がけているIT専門商社で、2007年9月よりソフォス製品の販売代理店となる。同社はソフォス製品を販売する傍ら、自社でソフォスのネットワーク・セキュリティツールのSophos Firewall XG、EDR機能を搭載したエンドポイント・セキュリティツールのSophos Intercept X Advanced with EDR 、さらにそのサーバー版であるSophos Intercept X for Server with EDRを早期より導入し、Sophos Centralを介してクラウド上で運用を一元管理している。このように最新ソフォス製品を早期より導入し、最先端の方法での運用を実践するシー・エル・シー社に導入背景と効果、今後の展望等について伺ってみた。

導入の背景

シー・エル・シーでは当初、自社で利用するセキュリティ製品に関して、他社製品ウィルス・ワクチン製品を使用していたが、ソフォス製品の販売代理店になったのを契機に既存製品からソフォスのSophos Endpoint Protectionに移行。その後、ネットワーク・セキュリティ強化を目的に2018年12月にSophos XG Firewallを導入。さらに、2019年7月にはIntercept X Advanced with EDRおよびSophos Intercept X for Server with EDRを導入完了し、Sophos Centralを使ってクラウド上で運用を一元管理している。ネットワーク・セキュリティの強化を図った背景をシー・エル・シー社ビジネス推進部部長の日向修氏は次のように説明する。「それには主に二つの理由があります。一つは、ドアノック的な攻撃の頻度が増えてきたことで、セキュリティ製品を扱う会社として自らのセキュリティを一層強化しなければなりませんでした。もう一つの理由は、弊社の持株会社であるPCIホールディングス株式会社が

セキュリティ管理者のいない中小企業でもSophosLabsから提供されるアドバイスやレポートを活用しながらEDR機能のメリットを十分にコスト効率よく享受できます。

株式会社シー・エル・シー
取締役　経営企画本部長
萩原　克彦氏

弊社を含むグループ全体で導入していたエンドポイントプロテクション製品であるAppGuardを補完するためでした。AppGuardは、OSに近いレベルで動作するエンドポイント・セキュリティ製品ですが、不審なプログラムの検知は行っても駆除は行わないため、同ソフトを最終防衛ラインに据えて、その上位部分でネットワークとエンドポイントも防御する多層防御を行う必要があると判断しました。AppGuardとソフォス製品は機能的に相反することは全くなく、役割分担が完全になされています」

このような背景の下、ソフォス製品の導入を決定したのは“Synchronized Security”というキーワードが大きく影響したようだ。ソフォス製品が実現するネットワークおよびエンドポイント間のSynchronized Securityの効果について、日向部長は次のように振り返る。「検証段階において、Synchronized　Securityの導入により、人手では決して対応できないミリ秒あるいは秒単位で訪れてくる攻撃を瞬時にかつ自動的に阻止、隔離したのを目の当たりにすることができました。仮に感染することがあっても、拡散することがないという確信を得ることができました。このような体験を得られたことで、お客様にソフォス製品を売り込む際にアピールしやすかったのも良かった点の一つです」

導入後のメリット

検証時点で期待通りのパフォーマンスを見せたソフォス製品であったが、導入後にはどのような効果が表れたのであろうか。「Intercept Xについては、元々オンプレミス型のIntercept X Advancedを使用していたので、クラウド運用に移行した後でもそのまま安定使用できました。XG Firewallについては、制御設定を行う際に何をブロックするのかがカテゴライズされており、容易に設定が行えます。実際に一番効果が顕著だったのは、ニュースサイトや検索結果画面上に表示されるフィッシング目的の広告バナーやリンクに社員がアクセスしないよう予めブロックすることができたため、そのような設定を行ってからは社員からの問い合わせが一切なくなりました」と日向部長は当時を振り返る。

また、シー・エル・シー社 取締役 経営企画本部長で同社の情報管理担当役員を務める萩原克彦氏は、「弊社ではISMS認証を取っており、厳密なセキュリティ運用が求められているのですが、ソフォスのEDR対応製品の導入により、インシデントがいつどのように発生し、データやシステムにどのような影響を与えたのかといったインシデント対応を高い水準で行えるようになったのが大きなメリットです。またSynchronized Securityにより、ファイアウォールとエンドポイントをクラウドで一元管理できるようになったことで全体的な管理工数やコストを削減できたほか、AppGuardとの明確なすみ分けができたことも大変良かったと評価しております」と語った。

中小企業に対するEDRの訴求

高度化し続ける脅威に対して、さまざまなIT/セキュリティ・メディアでもEDRの特集が組まれ、その重要性が唱えられているが、その一方でEDRの導入はセキュリティ管理者のいない中小企業では導入コストが高く運用も困難であるため、導入が難しいのではという意見も少なくないのではないかと水を向けてみると、「他社のEDR製品ですと導入費用も高く、設定や管理も複雑で中小企業には敷居が高くなるかもしれませんが、ソフォスのEDR対応製品はEDR機能がライセンス内に含まれており、セキュリティ管理者のいない中小企業でもSophosLabsから提供されるアドバイスやレポートを活用しながらEDR機能のメリットを十分にコスト効率よく享受できます」と、日向部長は自らの経験を基に太鼓判を押す。

今後の展望

メインフレームを販売していることで何万人もの従業員を持つ金融機関などの大手企業から、何百何千名単位の従業員を持つ中小・中堅企業まで幅広い規模の顧客を持つシー・エル・シー社は、自らのソフォス製品の導入運用経験を今後、販売戦略にどのように生かしていくのであろうか。「やはりお客様には最低限Interecpt X Advancedを導入していただき、Synchronized Securitiyを軸としたセキュリティの自動化のメリットを訴求していきたいと考えております。また、PCIグループ全体でAppGuardの補完ソリューションとして導入してもらえるよう働きかけてもいきたいと考えております」と日向部長は今後の展望を明かしてくれた。

SOPHOS

弊社を含むグループ全体で導入中のエンドポイントプロテクション製品であるAppGuardとソフォス製品は、機能的に相反することは全くなく、役割分担が完全になされています。

株式会社シー・エル・シー
ビジネス推進部　部長
日向　修氏

その他の導入事例は**こちら**