南九州の酪農家の夢と願いで創業された南日本酪農協同株式会社のビジネスをITで支える情報システム部では、旧来のエンドポイント対策ソフトをCentral Intercept X Advanced with EDRとCentral Intercept X Advanced for Server with EDRに更新し、セキュリティ対策を大幅に強化した。

CUSTOMER-AT-A-GLANCE

ミルクでつなぐ明日の笑顔

南日本酪農協同株式会社

南日本酪農協同株式会社
宮崎県都城市姫城町32街区3号

社員数
501名［男405名、女96名］
（令和2年2月29日現在）

Webサイト
https://www.dairy-milk.co.jp

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

もっとも注目したのは、AIによる根本原因の解析機能でした。従来のエンドポイント対策では、感染しても原因までは解析できませんでした。解析のために、限られた情報システム部の人材を割くこともできませんでした。

南日本酪農協同株式会社
情報システム部
次長　長野 健氏

1960年に南九州の酪農家の夢と願いが集まって生まれた南日本酪農協同株式会社。創業以来、半世紀以上にわたって酪農家とともに牛乳・乳飲料をはじめとする乳製品を九州から全国に届けてきた。同社の事業をITで支えてきた情報システム部では、社内システムの開発や運用に保守、さらにはサポートまで担っている。現在は5名のスタッフが、現場から日々寄せられる要望をITで支援するために、パッケージ製品のカスタマイズや機器のメンテナンスなど広範囲に対応している。そして、2020年4月にセキュリティ対策を強化するために、Central Intercept X Advanced with EDR とCentral Intercept X Advanced for Server with EDRを導入した。

ビジネスチャレンジ

「エンドポイント更新のタイミングでタイムリーに提案を受ける」

グループ会社含め800名の職員が約470台のPCを利用している南日本酪農協同株式会社。同社では、以前からセキュリティ対策にパターンマッチング式のエンドポイント製品を利用していた。しかし、同製品の更新にあたり、情報システム部には大きな懸念があった。その問題について、同部の長野氏は次のように振り返る。

当社にとっては充分過ぎるくらいの機能が満載されていたので、これならば乗り換える価値があると判断したのです。以前に比べて、新しいマルウェアに対応しているという安心感は大きいものがあります。

南日本酪農協同株式会社
情報システム部 情報システム課
課長　長友 寛氏

「製品の更新を迎えたときに、依頼した見積もりの返事がないなど、対応に不安を感じました。加えて、従来型のパターンマッチングによるエンドポイントのセキュリティ対策を更新し続けていて、果たして社内システムを守りきれるだろうか、という不安もありました」

見積もり依頼に対する返答がないまま、販売代理店の対応で継続しようと検討していたときに、九州日立システムズからCentral Intercept X Advanced with EDR と Central Intercept X Advanced for Server with EDRの提案を受けた。長野氏は「紹介してもらったのは、まさにギリギリのタイミングでした。継続するのが難しそうだったら、他に国内で有名なベンダーの製品に切り替えようかと考えていたときでした。そこで、急いでCentral Intercept X Advanced with EDR とCentral Intercept X Advanced for Server with EDRの機能を調べたところ、当社にとっては充分過ぎるくらいのセキュリティ対策が満載されていたので、これならば乗り換える価値があると判断したのです」と話す。

テクノロジーソリューション

「AIによる解析とUSBメモリの保護などに期待」

導入において製品の評価を担当した長友氏は次のように説明する。

「もっとも注目したのは、AIによる根本原因の解析機能でした。従来のエンドポイント対策では、感染しても原因までは解析できませんでした。解析のために、限られた情報システム部の人材を割くこともできませんでした」

Sophos Threat Casesという根本原因解

析は、問題の発生したPCで何が起こったのかを、自動で解析し管理者の理解を支援する機能。Central Intercept X Advanced with EDRのユーザーは、脅威ケースの解析に加えて、問題の発生しているコンピュータの隔離や、ネットワーク上で脅威の他の例がないかを検索し、脅威のクリーンアップとブロック、さらには詳細な脅威解析情報も取得できる。一連の処理が自動化されているので、限られたIT人材で全社員のPCを安全に運用する情報システム部にとっては、セキュリティ強化の大きな支えとなる。

さらに長友氏は「運用面では、USBメモリの使用を管理できる機能にも注目しました」と補足する。USBメモリの管理について、長野氏は「以前からUSBメモリの利用はしっかり管理したいと考えていました。そこで、すでに導入していた資産管理パッケージのUSBメモリ管理オプションも検討してみました。しかし、追加のオプション代が高価だったので、導入は見送っていました。その問題と予算が、Central Intercept X Advanced with EDRで解決できたのです」と評価する。

導入の成果

「ソフォスのサポートで円滑なリモートインストールを実施」

少数精鋭で全社のITを管理する情報システム部門にとって、エンドポイント製品のリプレースも大きな業務課題となっていた。そこで長友氏は「すべてのPCへのCentral Intercept X Advanced with EDRのインストールと、旧製品のアンインストールは、資産管理ソフトのスクリプトを活用してリモートで実行する計画を立てました。そのときに懸念したのは、ネットワーク負荷でした。Central Intercept X Advanced with EDRは、インターネット経由でインストールするので、ネットワークの帯域が不足しないか心配したのです」と振り返る。情報システム部では、ソフォスの技術サポートのアドバイスを得て、Central Intercept X Advanced with EDRをインストールするPCを一日10~20台として、時間をずらすことでネットワークの負荷を軽減した。長友氏は「旧製品のアンインストールでも、少し苦労しましたが、ソフォスからのアドバイスによって、スクリプトで対応できるようになりました」と補足する。

導入から数ヶ月が経過して、Central Intercept X Advanced with EDR と Central Intercept X Advanced for Server with EDRによるセキュリティ対策は、適切な運用を続けている。

強化されたセキュリティ対策について長野氏は「以前に比べて、新しいマルウェアに対応しているという安心感は大きいものがあります。情報システム部で開発した新規のプログラムも、登録しておかないと検知の対象になるので、それだけしっかり機能していると確認できます」と話す。

今後の展望

「将来的にはSynchronized Securityも検討していく」

今後のセキュリティ対策について長野氏は「新型コロナウイルスの問題がなければ、UTMとL3スイッチの管理を外部に委託しようと計画していました。しかし、テレワーク対応などに追われ計画は止まっています。一段落したら計画を再開するか、あるいはSophos XG Firewallを組み合わせたSynchronized Securityを検討しようと考えています。まだ、予算などが見えていないので、はっきりとした計画は立てられませんが、情報システム部の運用管理の負担を軽減しつつ、より強固なセキュリティ対策の導入は、今後も必須になると受け止めています」と述べる。さらに、長野氏は「Central Intercept X Advanced with EDR と Central Intercept X Advanced for Server with EDRでセキュリティ対策は強化できたと考えていますが、攻撃者もより巧妙かつ悪質になっています。こからも、防御と攻撃のイタチごっこは続くでしょう。この問題を解決していくためには、とにかく新しい情報が重要だと受け止めています。地方では、情報が届くのが遅れがちです。それだけに、今後もソフォスやパートナー企業からのスピード感のある情報提供を期待しています」と希望を語った。

株式会社 九州日立システムズ
木下 明 様

SOPHOS