CYLANCE™

沖縄銀行
導入事例

未知のマルウェアにも対抗する多層防御の中核を担う振る舞い検知とは異なる強固なマルウェア対策「CylancePROTECT®」

地域密着型金融機関として地域社会に貢献している株式会社沖縄銀行では、秘匿性の高い個人情報を数多く取り扱っている金融機関だからこそ堅持すべき、安全かつ信頼性の高いインフラ作りに長年取り組んできました。同行がさらなるセキュリティ強化策の1つとして取り組んだのが、未知のマルウェアへの対策でした。検証を重ねた結果、パターンマッチングのアプローチとは異なる、人工知能の技術を活用したAIアンチウイルス「CylancePROTECT®」を導入するに至りました。

課題

1. 金融庁指導によるサイバーセキュリティ管理体制の強化、未知のマルウェア対策の徹底
2. 従来アンチウイルス運用時のネットワーク全体における負荷

▼

効果

1. 未知のマルウェアを含む脅威に対する圧倒的な検知精度、DNA解析によるマルウェアの実行前防御が決め手となり採用
2. 日々のパターンファイルアップデートなどが不要なため、ネットワーク負荷の最小化を実現

沖縄銀行

住　所　沖縄県那覇市久茂地3-10-1
設　立　昭和31年6月21日
従業員数　1,099名（平成28年3月末）
事業内容　金融
http://www.okinawa-bank.co.jp/

業界　金融業界

●導入きっかけ
未知のマルウェアに対する対策

●ソリューション
CylancePROTECTを2200台の端末の一部に導入
段階的に全端末に導入予定

インタビュー

沖縄銀行
システム部
執行役員部長
髙良 茂 氏

沖縄銀行
システム部
システム企画管理グループ
上席調査役
上原 慶典 氏

株式会社おきぎんエス・ピー・オー
システム開発部
金融システム開発課
チーフ
上原 浩輝 氏

課題

ガイドラインで指摘された多層防御の重要性

「地域密着・地域貢献」を経営理念に掲げ、地域社会の発展に寄与することを使命に地域密着型の金融機関として多くの人に親しまれている株式会社沖縄銀行。長年にわたって築き上げてきた「お客さま目線」の姿勢を基本に業務革新に挑戦し、新たな価値創造を通じて県民に愛される「ピープルズバンク」として地域社会に貢献しています。この顧客第一主義を実現するため、同行では業務効率化に向けたシステム合理化に注力しており、さらに金融機関に求められるセキュアな環境づくりにも積極的に取り組んでいます。

金融機関を管理監督する金融庁では、信用秩序の維持や預金者保護の確保などを目的にした監督指針や業務ガイドラインとなる金融検査マニュアルなどによって、サイバーセキュリティに対する管理体制を強化するよう指導が行われています。近年では、大手の通信教育会社や旅行会社などで発生した情報漏えい事件などを背景に、より強固なセキュリティ対策が金融機関に求められているとシステム部 執行役員部長 髙良 茂氏は現状を振り返ります。「ガイドラインでは、万一の侵入に備えた多層防御の重要性が指摘されています。当行では、すでにさまざまな対策を実装しているものの、よりセキュアな環境づくりに着手する必要性があると考えたのです」。その過程で検討されたのが、エンドポイントセキュリティの更なる対策強化でした。

選定ポイント

未知のマルウェアでも実行前に検知できる仕組みとして注目

同行では、通信事業者が提供するゲートウェイ型メールセキュリティやPC上で動くアンチウイルスソフト、そして資産管理ツールによるUSB制御など、さま

ざまなセキュリティ対策をすでに実装しています。それでも、未知のマルウェア対策については十分でない部分もあったと語ります。「従来型のパターンマッチングのアンチウイルスソフトでは、既知のマルウェアにはある程度対処できても、未知のものには十分な対策とはなりません」と同部システム企画管理グループ 上席調査役 上原 慶典氏は語ります。ゲートウェイ側でどれだけ多層的に防御しても、マルウェアなどが暗号化されてすり抜けてくることも考えられ、最終的にはEXEファイルが動くPC側で対策する必要があったと語ります。

そこで注目したのが、Cylance Japan株式会社が提供しているAIアンチウイルス「CylancePROTECT」でした。「マルウェアの振る舞いを検知して防御する仕組みも検討したのですが、その場合はマルウェアが実行された後にしか検知できません。しかしCylancePROTECTであれば、ファイルのDNAを解析して判断するため、実行前に検知できます」と評価するのは、同行のシステム開発から運用までを手掛ける株式会社おきぎんエス・ピー・オー（以下、おきぎんSPO）システム開発部 金融システム開発課 チーフ 上原 浩輝氏です。CylancePROTECTの能力を確かめるべく、導入前に自社で試用してみた髙良氏は、その検知率の高さを改めて実感することができたと評価します。「こんなにいい製品があるのかと驚きました。試行フェーズでは自分たちで未知のマルウェアを実行してみたうえで、しっかり検知できることを確認しました」。

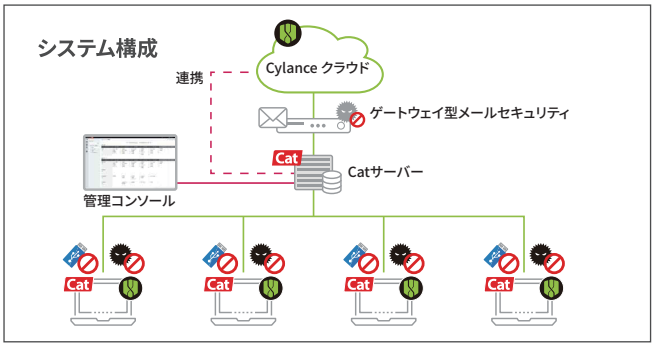
人工知能の技術については、それぞれ最初に受けた印象が異なっています。「未知のマルウェアに対処するためには、自己学習していくような仕組みでなければ厳しい時代。実はFinTechなどのソリューションの中にはAI技術を活用したのもあり、経営陣を説得するには良いタイミングだった」と髙良氏はとらえる一方で、上原氏は「他の業務でAIの話題は聞いたことがありますが、セキュリティ製品では初めてだったことで衝撃を受けた」と振り返ります。運用管理を行うおきぎんSPO上原氏も当初は半信半疑だったものの、実際のデモで検知する様を目の前で確認し、しかもネットワークに繋げることなく検知できたことに驚きを隠せなかったと当時を振り返ります。

CylancePROTECTの場合、日々のパターンファイルアップデートや頻繁なバージョンアップを必要としないため、ネットワークにおけるパフォーマンスの影響を最小限に抑えられます。おきぎんSPO上原氏は、この点についても選定ポイントの1つであったと語ります。「従来のものはウイルス検索エンジンが変わるタイミングなどでプログラム自体を配信しなおす必要があり、ネットワーク全体に負荷を与えることも少なくありません。そういった煩雑さがないのはありがたいです」。

また、「既存のアンチウイルスソフトは毎日昼休みに、フルスキャンするといった運用上の工夫を行っていますが、どうしてもPCは重くなりがち。パターンファイルを使用しないCylancePROTECTであれば、PCへの負担は軽い」と髙良氏は評価しています。以前パターンファイルアップデートに起因するエラーが発生し、すべてのエンドポイントで誤検知が発生してしまったこともありました。「1つのミスが大きく影響するのもエンドポイントならでは。パターンファイルアップデートの配信がなくなったことで、ミスが発生しにくい環境になっているのは大きい」と上原氏。

また、同行は、エムオーテックス株式会社が提供する資産管理ツール「LanScope Cat」で取得しているPCの操作ログで、マルウェア流入の前後操作が確認できる点も大きな選定ポイントに上げています。「LanScope Catの操作ログを確認することで、どこからマルウェアが侵入したのか、どのタイミングで入ってきたのかなどの履歴を追いかけることができます。侵入経路やその方法を分析しやすいこともCylancePROTECTを選択した理由です。例えば、マルウェアを検知した場合、以前は現場の人にヒアリングし、Webサイトを見ていたのであればWebサーバーのログを取得し、そこから調査していくというプロセスを踏む必要がありました。今はLanScope Catのレポート画面を確認しながらクリックをするだけでマルウェアの感染経路が簡単に解析できるため、負担軽減につながっています。」と上原氏は評価しています。

コスト面では、一度の情報漏えい事件で億単位の損害賠償につながりかねないという意識から、しっかり予算をかけてセキュリティが担保できるソリューションを導入するべきだという理解が経営陣から得られていました。そこで、「CylancePROTECT」が同社のエンドポイントセキュリティの要として選択されることになりました。



導入効果

未知のマルウェアへの対策が可能なCylancePROTECTの導入は周囲からの反響大

現在はおよそ2200台あるエンドポイントの中で、電子メールなど外部とのやり取りが発生する営業部門や融資部門などの一部からCylancePROTECTの展開を進めています。マルウェアについては検知モードが基本であり、ファイルを起動するたびにポップアップでアラート表示させる運用です。「セキュリティ意識を高めてもらう意味でも、現場へ通知することが重要」と髙良氏。何かあればユーザー自身でアラートは解除できますが、全体に導入が進んだ段階でマルウェアをブロックする自動隔離モードへの移行も視野に入れています。

マルウェアの検知については、初期インストール時に実施されるスキャンの段階では、マルウェアだけでなくフリーソフトやプリンタドライバなどさまざまなものがリスクとして検知の対象になりました。しかし、そのことがかえって検知率の高さを裏付ける結果になったと髙良氏は評価します。

クラウド上で管理できるメリットについても髙良氏は言及します。「ダッシュボード画面で自社の状況を可視化しやすく、日本語にローカライズされているためわかりやすい。PCのログがクラウド上で管理されているだけなので、情報漏えいの心配もありません。最近はFinTechの影響もありクラウドを活用する機会も増え、クラウド自体が導入の障壁になることはありません」。また、おきぎんSPO上原氏は運用管理面でもメリットが大きいと語ります。「サーバー本体の維持管理を行う必要がないだけでなく、CylancePROTECTを利用している他社が、発見された脅威をどの様に対応しているのか知ることが出来るのはクラウド利用の大きなメリット」と指摘。CylancePROTECTの管理者が無償で使用できる、テナントサーバーはクラウド上で提供されており、特定のマルウェアについて他社がどう対処しているのか、そのナレッジが共有できるようになっている。そのため、検索エンジンなどでマルウェア情報を探すという行為自体がなくなったと高く評価しています。

未知のマルウェアへの対策が可能になったCylancePROTECTを導入したことで、周囲からの反響も大きいと髙良氏は語ります。「金融機関同士で行われる情報交換会などで話をすると、CylancePROTECTが持つ検知率の高さに“嘘でしょ?”と皆さん驚かれます」。

今後

すべてのエンドポイントへの展開を計画

今後について髙良氏は、「すべてのエンドポイントへの展開を2017年春以降、順次行っていきたい」と意欲的です。現状は既存のアンチウイルスソフトと重複して稼働させていますが、最終的にはCylancePROTECTの1本に絞っていきたい考えです。

また強固なセキュリティが求められる金融機関だけに、同社では多層防御を実現するためにさまざまなセキュリティソリューションを実装しています。「現状は多層防御が基本となっていますが、いずれはコスト削減という話題も出てくることでしょう。機能として重複しているものがあれば、提案いただいたうえで外していくことも考えなければいけない場面も。そのための情報提供にも期待しています」と髙良氏に今後について語っていただきました。

Cylance Japan株式会社
〒100-6510 東京都千代田区丸の内1-5-1 新丸の内ビルディング10F
www.cylance.com/jp
03-6386-0061 (代表)

CYLANCE™

201704-CS002