HITACHI
Inspire the Next

導入事例

因幡電機産業株式会社 様

CylancePROTECT®

比較検証でAIベースのエンジンの圧倒的なマルウェア検知率を確認
パターンファイルベースのマルウェア対策製品からリプレース

電設資材の卸売専門商社として
創業80年以上の歴史を持つ因幡電機産業では、
セキュリティ対策としてファイアウォールとパターンファイルベースの
マルウェア対策製品を導入していました。
しかし、パターンマッチングに頼った防御では、
未知のマルウェアによる攻撃は防ぎ切れないことを実感し、
既存のマルウェア対策製品と置き換える形で次世代マルウェア対策製品
「CylancePROTECT」を全社導入、セキュリティの強化を実現しました。

BlackBerry
CYLANCE
×
INABA
因幡電機産業株式会社

課題

- パターンファイルベースのマルウェア対策製品によるPCの動作遅延や、インストール可能なソフトウェアの一覧作成・確認など、運用に負荷がかかっていた
- 従来のセキュリティ対策では、マルウェアを防げているのか漠然とした不安があり、セキュリティを強化したかった

効果

- PCの動作も軽くなり、脅威の自動隔離も可能となったため、ユーザー・システム部門両方にとって利用しやすい環境を実現
- AIベースの検出エンジンによって、マルウェアなどを高精度で検知できるようになりセキュリティの強化を実現

背景と課題

パターンファイルベースのマルウェア対策に感じていた不安

因幡電機産業は、創業80年以上の歴史を持つ電設資材の卸売専門商社です。公共物件の入札案件もあり、上層部からは「情報漏洩が起きないように」と念を押されていました。そのため、ファイアウォールを設置し、エンドポイントセキュリティ対策としてパターンファイルベースのマルウェア対策製品を導入することで、要請に応えていました。

マルウェア感染などのトラブルも特にありませんでしたが、導入したマルウェア対策製品には物足りなさを感じていました。

「特にこれと言ったトラブルがあったわけではないのですが、漠然と『脆弱かもしれない』とは思っていました」（藤幹氏）

「怪しいメールが届いたという警告が出て、フルスキャンしてみても、何も見つからないので『本当に大丈夫なのだろうか』という意識はありました」（林氏）

また、運用面では、課題も感じていました。フリーのソフトウェアのインストールについてはホワイトリストやブラックリストを作って対応していましたが、追いつかないこともあるなど、運用負荷が高いものとなっていました。さらに、マルウェア対策製品のフルスキャンには時間もPCへの負荷もかかるため、その間業務が進まなくなります。フルスキャンを頻繁にすることは難しく、リアルタイムスキャンで対応していましたが、本当にマルウェアの侵入を防ぐことができているのか、不安はぬぐい切れませんでした。

「外部からの侵入を100%防ぐことはできないという前提に立ってEDR（Endpoint Detection and Response）製品や、従来のマルウェア対策製品ではなくAIを活用したマルウェア対策製品の情報を収集していました」（藤幹氏）

既知のマルウェアとのパターンマッチングによって検知するマルウェア対策製品では未知のマルウェアには対応できないと感じていた藤幹氏は、ベンダーのセミナーや勉強会にも積極的に参加し、情報を収集していました。

Interview

因幡電機産業株式会社
管理本部
情報システム部
システム企画課長
藤幹 昌宏 氏

因幡電機産業株式会社
管理本部
情報システム部
システム企画課　主事
林 孝一 氏

株式会社 日立ソリューションズ

選定と導入

比較検証で証明された次世代マルウェア対策の力

2019年3月に、情報収集活動を行っていた藤幹氏のもとに、セキュリティセミナーの案内が届きます。そこで紹介されていたのがAIベースの検知エンジンを搭載した次世代マルウェア対策製品「CylancePROTECT」でした。

「以前から製品名は知っていましたが、メーカーの担当者から改めて『パターンファイルベースのマルウェア対策製品は後追いになるが、『CylancePROTECT』なら先手を打つことができる』と聞いて、前向きに検討しようと考えました」（藤幹氏）

セミナーでは、既に導入し運用している企業の講演もあり、「CylancePROTECT」はPCの動作が重くなることもなく、また、怪しいファイルは自動で隔離されるため、調査や報告の作業も軽減でき、運用が容易になったという話がありました。「実際に使っているシステム担当者の『運用が楽になった』という感想は印象に残りました」（藤幹氏）

導入を検討していた藤幹氏のもとに、10月に代理店担当者から「現在使用しているマルウェア対策製品との違いを一度検証してみてはどうでしょうか」という申し出があり、検証を実施することになりました。

比較検証では、仮想サーバー上に従来のマルウェア対策製品の環境と「CylancePROTECT」の環境をそれぞれ用意して、300種のマルウェアの検体を入れて検知する様子をリアルタイムで確認しました。

「結果は衝撃的でした。元々使用していたマルウェア対策製品では、すべてとはいかなくとも、7～8割はブロックできていると思っていましたが、検知できたのはたったの2割程度。一方、『CylancePROTECT』はほぼブロックしました。早く手を打たなければ危険だと思いました」（藤幹氏）

早速、社内向けに提案書をまとめて、「12月には社内システムとの相性を確かめるために10台のPCへ導入し、システム部門内で技術的な検証を行いました。検証でトラブルがないことを確認し、年内に導入を決定しました」（藤幹氏）

実際に「CylancePROTECT」を全社展開したのは翌年の2月です。使用していたマルウェア対策製品の契約更新のタイミングで約2,000ライセンスを購入しました。インストールは、資産管理ツールの配布機能を利用したため、ユーザー側での作業は不要で簡単に導入できました。

「『CylancePROTECT』は既存のマルウェア対策製品と共存させることができて、マルウェア対策製品を後から削除すればよかったので、スムーズに移行できました」（林氏）

成果と今後

防御は「CylancePROTECT」に任せることで、システム部門、ユーザー両方の負荷を軽減

「今回のリプレースでは、比較検証が重要な契機となりました。結果に目を見張りましたが、未知や亜種のマルウェア検知が難しいことや、古いマルウェアがパターンファイルから抜け落ちていることなど、パターンマッチングによるマルウェア対策の限界がよく分かりました」（藤幹氏）

現在、同社では「CylancePROTECT」の検知機能だけを使って怪しいファイルなどを隔離。検知状況を1日1回確認しながら運用しています。「CylancePROTECT」のダッシュボードから、検知したファイルがどれだけマルウェアに近い構造かといったスコアや、他社で検知されたマルウェアの情報なども確認できるため、対応要否の判断も簡単です。

「システム担当者として運用が楽になっただけでなく、ユーザーの自由度を高めることができたのがよかったと思います。『CylancePROTECT』が守ってくれているので、これまでフリーのソフトウェアのインストール時に作っていたホワイトリストやブラックリストの作成も不要になり、ユーザー側もリストの確認が不要になりました。システム部門にとってもユーザーにとってもよい状況です。PCへの負荷がかかっていたスキャンも軽量になり、業務への影響も削減することができました」（林氏）

「これまで180くらいのファイルが隔離されていますが、マルウェアだけでなく、スパイウェアやアドウェアも隔離してくれており、セキュリティが強化できたと感じています。そろそろ隔離だけでなく、排除の自動化も検討したいと思っています」（藤幹氏）

今後は、全社のマルウェア対策を「CylancePROTECT」に一本化していく計画を立てています。

「『CylancePROTECT』は問題なく運用できています。しかし、セキュリティの世界は変化の激しい世界です。次々と新たな手法のサイバー攻撃が行われてきます。今後も引き続き『CylancePROTECT』が優位性を維持してくれることを期待するとともに、日立ソリューションズには、幅広い情報提供を期待しています」（藤幹氏）

日立ソリューションズはマルウェア対策を含め、これからも先進的なセキュリティソリューションを提供していきます。

Company Profile

因幡電機産業株式会社

本社所在地	大阪本社／大阪市西区立売堀4丁目11-14 東京本社／東京都港区港南4丁目1-8 リバージュ品川
設立	1949年5月
従業員数	連結：2,572人（2020年3月31日現在）
事業内容	電設資材事業、産業機器事業および自社製品事業

https://www.inaba.co.jp

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cylance/case14/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cylance/sp/

J20K-04-00　2020.09