ご購入プラン

最新アンチウィルスを手軽に使いたい方	プロの目でしっかり確認してほしい方	管理画面の操作や設定ミスが不安な方	プロの手に任せて安心したい方
月額 450円/1台	月額 530円/1台	月額 620円/1台	月額 700円/1台
年額 5,400円/1台	年額 6,360円/1台	年額 7,440円/1台	年額 8,400円/1台
基本ライセンス 月額 450円 /1台	基本ライセンス 月額 450円 /1台	基本ライセンス 月額 450円 /1台	基本ライセンス 月額 450円 /1台
	定期レポートOP 月額 80円 /1台	運用代行OP 月額 170円 /1台	定期レポートOP 月額 80円 /1台
			運用代行OP 月額 170円 /1台

・表示価格は、すべて税抜き価格です。
・ライセンスは管理対象のデバイス数分購入ください。最低5台から導入いただけます。
・月額プランの最低ご利用期間は6ヶ月です。
・年額プランもございます。詳細はお問い合わせください。
・オプションでCylanceOPTICSもご用意しています。詳細はお問い合わせください。
・LANSCOPE エンドポイントマネージャー クラウド版Freeが付属します。
・LANSCOPE エンドポイントマネージャーをお持ちの場合は連携機能の利用が可能です。
・CylancePROTECT®のディスコネクトモードは非対応です。
インターネット分離環境のマルウェア対策をご希望の場合にLANSCOPE エンドポイントマネージャー オンプレミス版の「マルウェア対策ライセンス」をご利用ください。

【台数無制限】AIアンチウイルス「CylancePROTECT®」無料体験版 お申し込み

CylancePROTECT®を1ヶ月無料で何台でも体験できます。
自社の環境でCylancePROTECT®の検知力の高さを体験でき、
体験後、ご希望の方にはマルウェア検知結果のサマリーレポートをプレゼント！
AIを活用した最新鋭のアンチウイルスを、この機会にご体験ください。

【お申込みはこちら】

キャンペーンコードをご入力の上
お申込みいただきますよう、お願いいたします。
https://www.lanscope.jp/cyber-protection/cylance/cylanceprotect/

キャンペーンコード
C-2020a

MOTEX エムオーテックス株式会社

本　　社：〒532-0011 大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル TEL:06-6308-8980
東京本部：〒108-0073 東京都港区三田3-5-19 住友不動産東京三田ガーデンタワー22F TEL:03-3455-1811
名古屋支店：〒460-0003 名古屋市中区錦1-11-11 名古屋インターシティ3F TEL:052-253-7346
九州営業所：〒812-0011 福岡市博多区博多駅前1-15-20 NMF博多駅前ビル2F TEL:092-419-2390

TEL:0120-968995 受付時間 9:30-12:00、13:00-17:30（下記休業日を除く）
（休業日：土・日・祝祭日および弊社の定める休日）
E-mail：sales@motex.co.jp　URL：www.motex.co.jp

●お問い合わせは当社へ

LANSCOPE
Cyber Protection

CylancePROTECT®

業界最高峰のAIアンチウイルスをお手軽にご利用いただけます！

マルウェア検知・隔離率
99%以上を実現※

※ 2023年3月 Tolly社のテスト結果より

月額450円/1台で
5台から導入でき、部分導入にも最適

※表示価格は、すべて税抜き価格です。

エムオーテックスは、BlackBerry Japanの
パートナーオブザイヤーを7年連続受賞

これまでのマルウェア対策における3つの常識。

検知率

従来型アンチウイルスでは
未知・亜種の
マルウェア感染は防げない

運用

マルウェア対策のためには
専門知識を持った
専任の運用担当者が必要である

コスト

多層防御には、
様々な製品が必要で、
対策コストが高い

「マルウェアは防げない」「専任の運用担当者が必要」「対策コストが高い」

その常識を覆します

CylancePROTECT®で
「アンチウイルスを入れておけば安心」の時代を取り戻す。

**AIを活用した
次世代型アンチウイルス**

CylancePROTECT

未知・亜種のマルウェアも
検知率99%以上

**世界の大手企業や
政府機関でも導入**

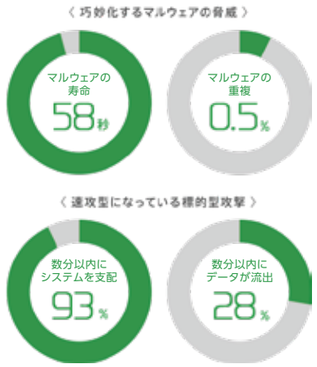
Fortune 500社のうち
87社がBlackBerryの
防御プラットフォームを採用

**画期的な検知手法で
様々な賞を受賞**

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

RSA 2020
「セキュリティカンパニー」及び
「サイバーセキュリティAI」を受賞

マルウェアの脅威とは

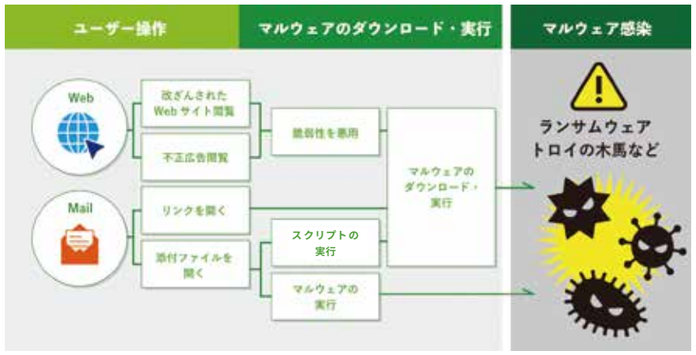


新しいマルウェアが作られる数 100万個／日

世界中で新しいマルウェアは毎日100万個作られていると言われています。
最近では誰でも数千円支払えば簡単にマルウェアを作ることができます。
VERIZON DBIR（データ漏洩/侵害調査報告書）2016の調査によると、99%のマルウェアは寿命が58秒以下でした。また、複数の組織で発見されたマルウェアはわずか0.5%でした。

これらの結果は、同じマルウェアが使われないことを示しており、パターンファイル型の製品ではすぐに検知することが難しいと言えます。
さらに、企業に侵入したマルウェアの93%は「数分以内にシステムを支配」し、28%が「数分以内にデータが流出」したというデータからも、標的型攻撃が「巧妙化」し、さらに「速攻型」になっていることがわかります。

Web閲覧とメール開封によるマルウェア感染が主流に

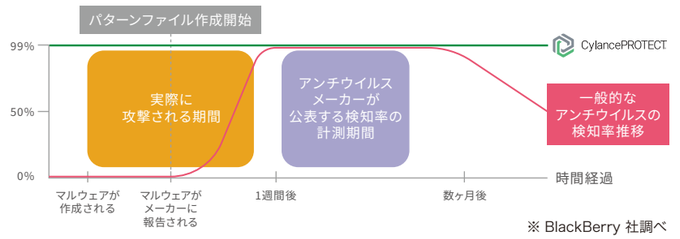


改ざんされたWebサイトの閲覧や、メールに添付されたファイルの開封など、人の行動における脆弱性を狙った攻撃が主流となり、気づかない間にマルウェアに感染しているケースが多々あります。
テレワーク・在宅勤務が注目を集める昨今、社員が自宅のネット環境で業務を行う際、エンドポイントセキュリティが不十分なままだとマルウェア感染で重要情報が流出するリスクが高くなってしまいます。

従来型アンチウイルスの限界

セキュリティ対策として最も広く使われている従来型のアンチウイルスは、日々発見されるマルウェアをブラックリスト化してパターンファイルを更新しています。このアプローチの構造的な問題はゼロデイと呼ばれる未知のマルウェアを止めることができないという点です。また仮にマルウェアが発見されたとしても、メーカーがそのファイルを入手し、パターンファイルを作成し、エンドポイントに配信されるまでにはタイムラグがあります。攻撃者はこの構造的な欠陥を突くために頻繁にマルウェアコードを変更するようになり、結果的に最近のマルウェアのほとんどが従来のアンチウイルスをすり抜けるようになってしまいました。

アンチウイルス製品における検知率の推移



※ BlackBerry 社調べ

パターンファイルで未知のマルウェアを止めることが出来ないのは構造的な問題。

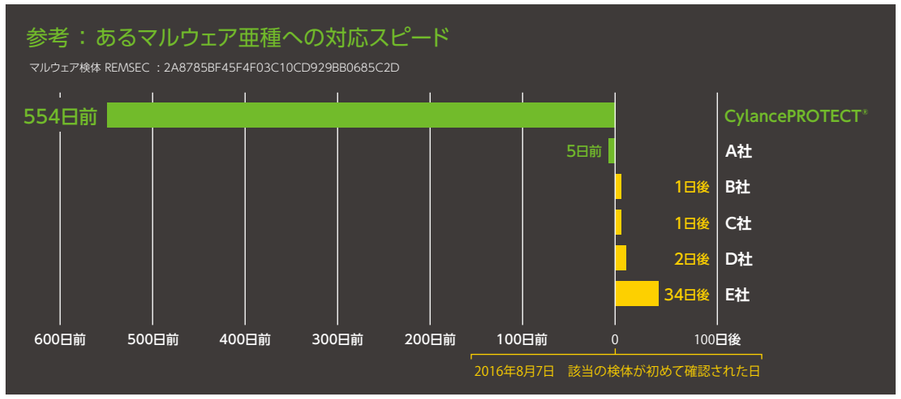
実際に攻撃に使われてる期間にマルウェアから防御できるかどうかが一番のポイントです。

CylancePROTECT®とは

CylancePROTECT®は未知のマルウェア検知率99%以上※

CylancePROTECT®のもっとも特徴的なポイントは、まだ世の中に存在しない、全く未知のマルウェアに対しても、予測をして防御できるという点です。実際に「WannaCry（ワナクライ）」や「Emotet（エモテット）」のような、全世界で大きな被害をもたらした危険なマルウェアに対して、世界で最初に発見されるよりも平均で25か月前のエンジンで検知できている実績があります。

※2023年3月 Tolly社のテスト結果より

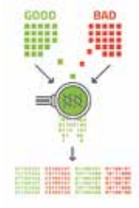


優れたAIを使った次世代型アンチウイルス製品

マシンラーニングの特許技術を活用した「予測脅威防御」

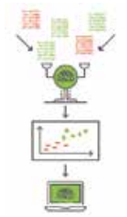
収集と学習

正常なファイルとマルウェアを
10億以上収集し、クラウド上の
AIに教師データとして学習させる



特徴抽出・数値化

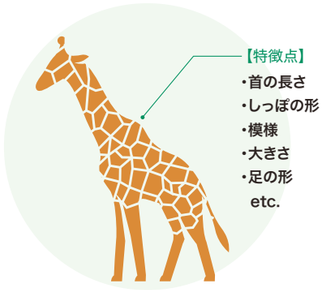
教師データの特徴点を抽出
（1ファイルあたり最大700万の特徴点）、
各ファイルのマルウェアらしさを数値化

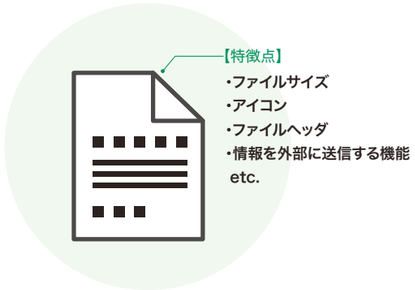


数理モデル作成

数学者やアナリストのチューニング後、
膨大なノウハウを反映した数理モデルを作成。
端末上は数理モデルのみ稼動

画像認識のマシンラーニングでキリンの特徴を学習し、キリンを判別できるようになるのと同様に、
ファイルにおけるマルウェアの特徴を学習し、未知・亜種のマルウェアも正しく判別します。

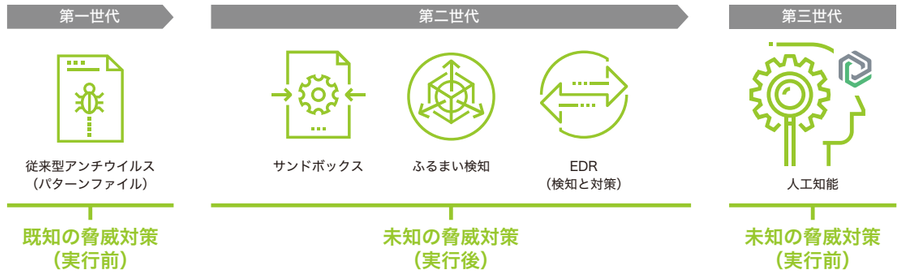




CylancePROTECT®の特徴

AIエンジンを活用した第三世代のアンチウイルス

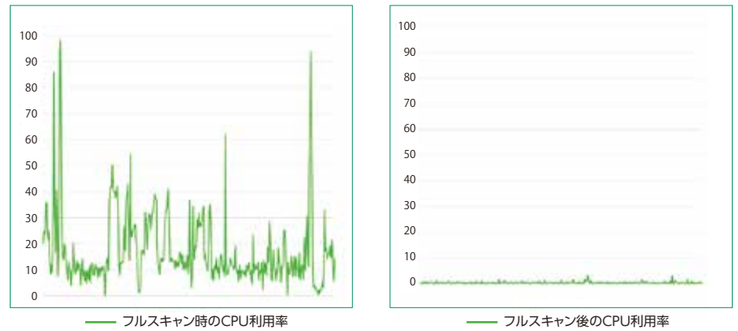
CylancePROTECT®はAIエンジンを活用。ゼロデイ攻撃に対応できない従来型アンチウイルスや、EDRのように止められないことが前提の事後対策ではなく、未知の脅威でも実行前に検知し防御することができます。



クライアント端末へのCPU平均負荷0.1%※、毎日のパターンファイル更新も不要

インストール時にフルスキャンを行った後は、新しいファイルが作成／ダウンロードされた際やプログラム実行時にマルウェアか否かを瞬時に判断します。検知時のCPU負荷も非常に軽く、毎日のパターンファイル更新も必要ありません。

※2023年7月 BlackBerry社の検証結果より



クラウド型のため、自社での構築・メンテナンスが不要

自社でのサーバー構築・メンテナンスが不要のため、すぐに運用をスタートできます。マルウェア検知状況は管理コンソール上で確認できるため、複数拠点がある場合でも管理者による一元管理が可能です。

エムオーテックスが提案する新しいマルウェア対策とは

CylancePROTECT®のマルウェア検知・隔離機能に加えて、エムオーテックス独自の運用支援サービスをご提供します。セキュリティメーカーの技術者が直接運用をサポートしますので、サイバーセキュリティ対策について専任担当者が不在の場合でも、無理なく運用が可能です。さらに月額450円/台で、最低5台から導入できるため、部分導入にも最適です。サポートサービスの提供により、更に手軽に CylancePROTECT®をご導入いただけます。

超高精度のAIアンチウイルス「CylancePROTECT®」だから、
マルウェア感染を99%以上防げる! ※1

セキュリティメーカーによる運用代行・定期レポートサービス
があるから、専任担当者不在でも大丈夫! ※2

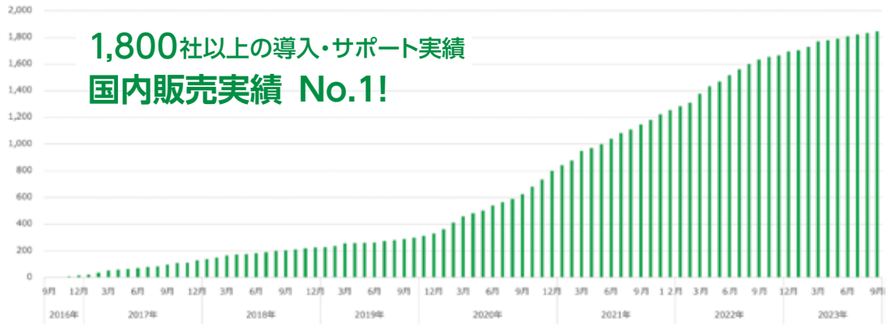
LANSCOPE エンドポイントマネージャーと連携すると、
操作ログからマルウェアの侵入原因をカンタンに調査できる! ※3

付属のMDM機能でモバイル端末のセキュリティをさらに強固にできる
リモートワイプ機能つきだから、リモートワークでの利用に最適! ※4

※1：2023年3月 Tolly社のテスト結果より
※2：有償オプションサービスです
※3:別途LANSCOPE エンドポイントマネージャーの導入が必要です
※4：リモートワイプにはLANSCOPE エンドポイントマネージャー クラウド版Freeを利用します

豊富な国内導入実績の経験をもとにサービスを提供

エムオーテックスは、BlackBerry Japanの
パートナーオブザイヤーを7年連続受賞



Topics **ユーザー会での意見公開が、運用改善のヒントに**

エムオーテックスでは、CylancePROTECT®のユーザー会を定期的に開催しています。ご担当者様同士でお悩みや課題、運用ノウハウなど活発な意見交換が行われ、大変ご好評をいただいています。

参加ユーザー様の声

- 短い時間で多くの情報交換ができて良かったです。
- 他社の利用実態（負荷や過検知状況など）を聞けて参考になりました。
- ハイレベルな会でおどろきました。

LANSCOPE サイバープロテクションの提供サービス

標準サービス

▶ CylancePROTECT® ※1
AI を活用した高精度のマルウェア検知・隔離機能をご提供します。

▶初期運用サポート
・CylancePROTECT®の製品概要や導入手順などをご説明します。
・ユーザー様向けの専用サイトをご用意。
利用ガイドや説明動画などをご提供しています。

▶ヘルプデスクサポート ※2
ご利用中に発生した疑問や質問に対して、電話やメールによるサポートサービスをご提供します。

▶リモートワイプサービス
紛失時に遠隔で、デバイスに対してリモートワイプを実施できます※3。

※1 オプションでCylanceOPTICS（EDR機能）もご用意しています。詳細はお問い合わせください。
※2 受付時間：月～金 9:30～12:00 / 13:00～17:30（土日祝日および当社規定の休日を除く）
※3 OSによって、条件・挙動が異なります。詳細はお問い合わせ下さい。

ユーザー様向け専用サイトイメージ

運用代行オプション

Webフォームからの依頼に応じて、
CylancePROTECTのコンソール上で行う操作をエムオーテックスの技術者が代行します

運用代行内容（一例）

■ポリシー変更
検知モードから隔離モードへの変更や、スクリプト制御の有効・無効など、CylancePROTECT®の運用ルールの変更作業を行います。

■セーフリスト登録
検知・隔離されてしまった業務上必要なファイルについて、セーフリストへの登録作業を行います。

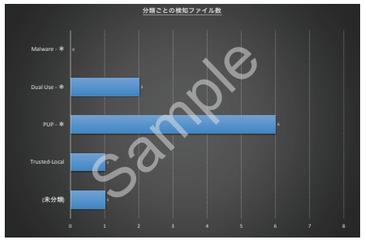
■クライアントプログラムのバージョンアップ
半年～1年に1度程度発生する、クライアントプログラムのバージョンアップ設定を行います。

CylancePROTECTコンソール

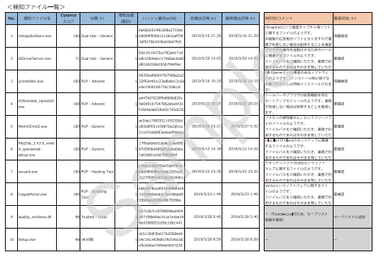
定期レポートオプション

エムオーテックスの技術者が検知状況を確認し解析した結果をレポーティングします（年4回）

【検知状況】
検知されたファイルのうち、
どの種別のファイルが多かったかを分析し、
報告します。（CylancePROTECTコンソール上の
未対応のファイルを対象とします）



【検知ファイル一覧】
「マルウェア」と判定されたすべてのファイルと、
その他のスコアが高い不審なファイル
（10個程度）について解析結果をご報告します。



24時間365日、専門家が脅威を監視「CylanceGUARD®」

世界トップレベルのセキュリティ専門家によるMDRサービス
AIアンチウイルス・EDR・導入支援・MDRをオールインワンでご提供

CylanceGUARD

CylancePROTECT®	CylanceOPTICS® EDR	ThreatZERO 導入支援	MDR 24/365の監視
			
高性能AIにより 99%※1 マルウェアを防御	マルウェアの侵入経路を特定 再発防止策の検討に	PROTECT・OPTICSの 有効な使い方をレクチャー	セキュリティ専門家が 24時間365日監視

※1：2023年3月 Tolly社のテスト結果より

CylanceGUARD® が選ばれる4つの理由

01 世界トップクラスの高品質なサービス

全員がサイバーセキュリティの修士号を持ち、世界的なSOC※2 コンテスト※3
優勝経験もあるBlackBerry社の専門家が24時間365日監視します。

※2：Security Operation Center　※3：DEFCON29 (2021) OpenSOC 優勝

02 EDR 特有の “無意味なアラート”から解放

お客様環境に合わせた最適なチューニングと独自の検知ルールにより、
お客様の確認が必要なアラートを月7件※4 にまで絞り込みます。

※4：BlackBerry社サンプル事例より、1万台規模の月平均の件数

03 応答時間は平均9分※5！ 緊急時にも即対応

MDR メンバーが24時間365日、お客様環境を監視します。
また、MDRメンバーに直接問い合わせが可能で、すばやく回答を得ることができます。

※5：2023年6月時点の平均応答時間（MTTR）。なお、SLO（サービスレベル目標値）は60分。

04 調査・封じ込め・復旧の一連に対処する 充実したEDR機能

99%※6 のマルウェア検知率でエンドポイントを最大限保護。脅威の発見後に必要な、
原因の調査・封じ込め・復旧までの一連の対応に対処できるEDR機能がすべて備わっています。

※6：2023年3月Tolly社のテスト結果より

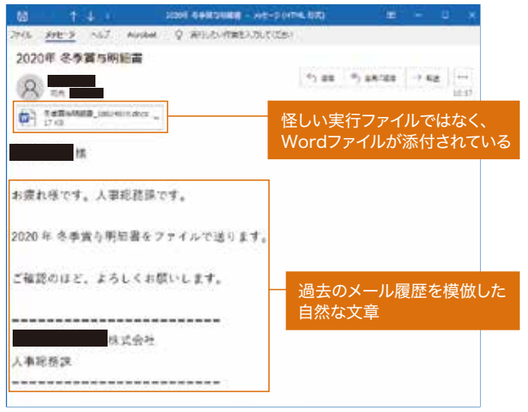
Emotetによる被害状況とCylancePROTECT® による検知

■概要

近年「Emotet（エモテット）」というマルウェアの感染被害が増加しています。2019年11月末ごろにメディアで取り上げられ一気に知名度を上げたこのマルウェアですが、2014年から欧州では被害が発生しており、その後何度もバージョンアップを繰り返しながら、さらに危険なマルウェアに成長を遂げています。
現在のEmotetは他のマルウェアを感染させるプラットフォームとして動作し、情報を窃取する不正な動作が行われたのちにランサムウェアが実行され、攻撃の痕跡自体を消し去ってしまいます。2022年は3月に大規模なEmotetのばらまき型攻撃が観測されており、JPCERTコーディネーションセンターによると、Emotetに感染したことで窃取されたメールアドレス数は約9,000件と発表されています。

出典：JPCERT/CC：マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

今後もサイバー攻撃はさらに増えていくことが確実視されておりEmotetの国内被害もさらに深刻化することが想定されます。



■ばらまきメールの例
いくつかのバリエーションがあり、
不信感を抱かせにくい工夫が施されています。

■Emotetについて

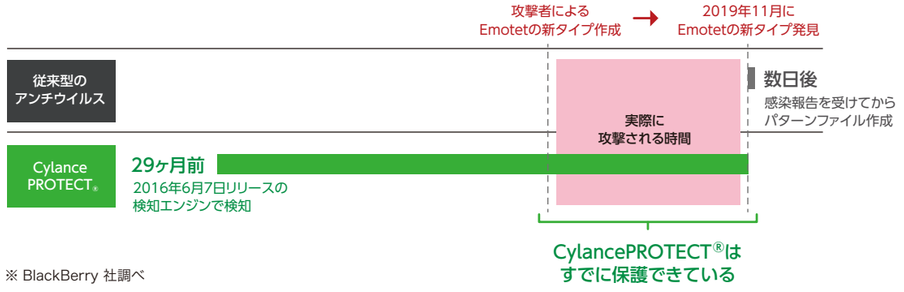
Emotetの特徴は、感染するとメール情報が窃取され、取引先を装うなどより本物のメールらしい、巧妙なばらまきメールが作成されることにあります。このようなばらまきメールにはいくつかのバリエーションがあり、いずれも不信感を抱かせにくい工夫が施されています。
また、年末には賞与、2020年1月には「新型コロナウイルス」を題材にした手口が確認されるなど、社会的な関心事に便乗する傾向がある点も巧妙です。

■AIによる予測防御

Emotetは2014年に発生して以降、何度もバージョンアップを繰り返し、初期とは異なる機能を備えたマルウェアに進化しています。
従来型のアンチウイルスの場合、タイプが変わるたびにパターンファイルの作成が必要となり、感染を防ぐことは不可能です。

CylancePROTECT®は、2019年11月に確認された当時最新タイプのEmotetに対して、2016年6月7日にリリースした検知エンジンで検知できたことを確認しています。
つまり、CylancePROTECT®のAIは3年半もの間更新されなくてもEmotetの最新タイプに対応できたことになります。

■当時最新のEmotet発見から起算した最新時期



※ BlackBerry 社調べ

エムオーテックスによるCylancePROTECT®導入事例

山梨県庁 様（CL数：約4,200台）

総務部 情報政策課 課長補佐　矢崎 孝 氏

パターンファイル脱却で運用負荷軽減！
エムオーテックスの迅速なサポートで運用の精度も向上

PC更改のタイミングに合わせて、セキュリティに関する運用負荷軽減につながる新たな環境を検討する中で注目したのが、AIを利用する次世代マルウェア対策製品CylancePROTECT®だった。

「パターンファイルの場合、定時スキャンがなかなか終わらないという課題もあり、新たな対策に向けての情報収集を行っていました。その過程で数理モデルを用いたCylancePROTECT®の先進的な技術を知り、興味を持ったことがきっかけです」と選定ポイントを説明する。

導入後の効果について「新たなマルウェアに対する定義がいつのパターンファイルで配信されるか分からないため、これまでは定時スキャンが必須でしたが、今回は端末を配る前にフルスキャンを実行し、あとはリアルタイム保護を実施するのみ。
以前は定時スキャンのタイミングも業務に影響がないよう調整が欠かせませんでしたが、その部分の負担が減ることを期待しています」と担当者は語った。
また、「これまでグレーな検知を行った際の判定で悩ましい場面もありましたが、導入準備段階ではあるものの、検知したファイルや検知理由等の説明も迅速で十分満足のいくものが得られています。理屈を知ることで我々も運用の精度を高めていくことができます」とエムオーテックスの対応を評価する。

株式会社沖縄銀行 様（CL数：2,432台）

システム部 執行役員部長 高良 茂 氏

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

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た。
「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」と担当者は説明する。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る。

そこで注目したのが、CylancePROTECT®だ。「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。CylancePROTECT®の能力を確かめるべく、導入前に自社で試用した結果、その検知率の高さを改めて実感することができたと語る。
「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」

四国中央市役所 様（CL数：1,610）

政策部 情報政策課　係長　篠原 大輔 氏

EDRとの連携によって、インシデント対応時間は
最大で80%削減を見込む

2008年よりアンチウイルス製品を利用してきたが、未知のウイルスに対して防御できるのか不安を感じていた。そこで、アンチウイルスの入れ替えのタイミングで、より検知精度の高いエンドポイント製品を検討することになり、CylancePROTECT®の検討を開始した。
「CylancePROTECT®は、AIによるマルウェア検知精度の高さによって、未知の脅威にも対応できる点が魅力的でした。さらに、LANSCOPE エンドポイントマネージャー オンプレミス版と連携することで、攻撃を検知したときに、誰が、どの端末で、どんな操作を行っていたか、ログの追跡が容易に行えるため、さらなるセキュリティ強化につながると考えた」

また、EDR製品である「CylanceOPTICS®」は、AIを活用し、エンドポイントの脅威分析や、検出および対応の自動化を実現するもので「CylancePROTECT®」と統合・連携できる。これにより、インシデント発生時の対応時間・工数削減効果が期待された。
「これまでのエンドポイント製品では、マルウェア検知などのセキュリティインシデントが発生したときに、インシデント対応に平均で8時間程度かかっていました。それが、両製品の導入による連携効果によって、最大で80%程度削減されることが期待される」

BXゆとりフォーム株式会社 様（CL数：550）

管理統括部 係長　高杉 実 氏

Emotet被害を“ゼロ”に抑えた防御力
そして管理者の工数も1/20に激減

同社ではランサムウェアによって従業員のPCが暗号化される事案が発生しており、「従来のパターンマッチング型のアンチウイルスソフトでは、日々変化する未知のマルウェアを検知できないことが不安だった」と振り返る。
そこからアンチウイルスソフトの見直しのために、CylancePROTECT®の評価検証が行われた。パターンマッチング型のアンチウイルスでは検知できなかったファイルがCylancePROTECT®で検出されたため、検知力の高さを実感。猛威を振るったマルウェア「Emotet」に対しても防御できていたため、「導入してから感染してしまったことは1回もなく、弊社にもなりすましメールが飛んできたことがあるものの、CylancePROTECT®が検知し、動作前に止められたので実害はなかった」と話した。

運用の負荷については、「これまでは週に1回程度、定期的に管理コンソールを開いて検知状況や、パッチ適用の有無を確認していたが、CylancePROTECT®導入後は、気になったことがあるタイミングで確認すればよく、管理者の負荷は軽減されている」と話す。これは、実際の対応時間にして「1回1時間で月4～5時間相当だったものが、1ヵ月に10分～15分程度に減っている」とのことだ。パターンファイルの更新を確認する作業も不要になるので、管理者としては大きな工数削減になったという。加えて、ユーザー視点からクライアントPCの動作が軽くなった点も導入効果だという。日中のスキャンがないことで「動作が遅い」と社員から問い合わせや相談が来ることもなくなったということだ。

株式会社テラバイト 様（CL数：80）

総務部　諏佐 喜与志 氏

運用状況が可視化され、ひとり情シスでも大きな安心感が得られた

同社では、エンドポイントセキュリティ対策として、これまで従来型のアンチウイルスソフトを利用していたが、メーカーの販売形態が変わり、契約を更新することとなったため、この機会に導入製品を見直すことになった。
これまで利用していたアンチウイルスソフトは運用方法が難しいなど、さまざまな課題があり、専任のシステム担当者を設けることができない「ひとり情シス」の体制の中、今後も現状の運用体制が維持できるかが不透明な状態であった。このような状況を打開するために、可能な限り少ない工数で管理ができ、AIによって未知の脅威にも対応できる次世代型のアンチウイルス製品である「CylancePROTECT®」の導入が検討された。
複数製品と比較しつつ、CylancePROTECT®のトライアルを実施した。使用感については「提供されたマニュアルに記載された内容を確認しながら使用環境の構築を行うことができた。管理担当者として、従来型のアンチウイルスソフトに比べて、運用の難易度は低いと感じた」と話す。
現在は、約80台のPC端末を諏佐氏が1人で管理・運用している。「以前利用していた従来型のアンチウイルスソフトでは、何が起きているか、私たちが分かりやすい可視化がなされなかったが、CylancePROTECT®導入後は検知アラートに沿って、何が起きているかを把握できるようになり、大きな安心感につながっている」

サッポロ不動産開発株式会社 様（CL数：30）

経営企画部 山内 健次郎 氏

小規模事業者でもコストパフォーマンスに優れ
手厚いサポートを利用できる点が決め手に

施設の運営を委託する外部のパートナー企業の社員が利用するPCの入れ替えを機に、エンドポイント対策の強化を検討していた。当時、複製製品を比較していたが、最終的に次世代型AIアンチウイルス「CylancePROTECT®」と、EDRである「CylanceOPTICS®」を採用した。

選定の要件として、「PC入れ替えのタイミングである4年間の総額コストとあわせ、機能面を比較検討した」と山内氏は述べた。機能面については、「従来のパターンマッチング型アンチウイルスでは、未知の脅威（ゼロデイ攻撃）に対して脆弱である」という理由で、AIを用いた次世代アンチウイルスが選定対象となった。万が一のインシデント時に、どこからマルウェアが侵入し、どのプログラムが要因となったのかを可視化するEDRの機能を重視したと振り返る。

しかし、「管理対象のPCが20台という小規模のユースケースに対応したサービスが基本的に少ない」という、小規模事業者ならではの課題があった。セキュリティの脅威は企業規模に関わらず存在するものだが、大手のセキュリティベンダーのサービスは、基本的に大企業向けのものが中心となっている。CylancePROTECT®のマネージドサービスは「小規模事業者でもコストパフォーマンスが高く、手厚いサービスを利用できる内容」と評価し、「それに対し、LANSCOPE サイバープロテクションが最も優れている」と語った。