ご提供プラン

最新アンチウイ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 500円/1台	月額 580円/1台	月額 670円/1台	月額 750円/1台
年額 6,000円/1台	年額 6,960円/1台	年額 8,040円/1台	年額 9,000円/1台
基本ライセンス 月額 500円 /1台	基本ライセンス 月額 500円 /1台	基本ライセンス 月額 500円 /1台	基本ライセンス 月額 500円 /1台
	定期レポートオプション 月額 80円 /1台	運用代行オプション 月額 170円 /1台	定期レポートオプション 月額 80円 /1台
			運用代行オプション 月額 170円 /1台

・表示価格は、すべて税抜価格です。
・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カ月です。
・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Aurora Focus（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。
・統合エンドポイント管理「LANSCOPE エンドポイントマネージャー オンプレミス版／クラウド版」を別途ご契約中の場合は、連携機能のご利用が可能です。
・Aurora Protect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は、統合エンドポイントマネジメント「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。
・2024年11月から上記価格に改定しています。

次世代AIアンチウイルス「Aurora Protect」無料体験版 お申し込み

Aurora Protectを1カ月無料で100台まで体験できます。
自社の環境でAurora Protect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を活用した新しいアンチウイルスを、この機会にご体験ください。

【お申し込みはこちら】

「LANSCOPE サイバープロテクション powered by Aurora Protect」サービスサイトの「無料体験版」より、キャンペーンコードをご入力の上お申し込みください。

https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr

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
長崎 Innovation Lab：〒850-0862 長崎県長崎市出島町1-41 クレインハーバー長崎ビル3F

0120-968-995　受付時間　9:30-12:00, 13:00-17:30
営業日　月～金(祝祭除く)
※携帯電話からは 06-6308-8981 をご利用ください。

E-mail：sales@motex.co.jp　URL：https://www.lanscope.jp/

●お問い合わせは当社へ

●プロダクトの仕様・サービスの内容は予告なく変更させていただく場合があります。
●最新の情報は弊社 Web サイトをご確認ください。
●記載の会社名およびプロダクト名・サービス名は、各社の商標または登録商標です。
●MOTEX はエムオーテックス株式会社の略称です。
●本カタログに掲載の情報は、2025 年 7 月時点のものです。

© MOTEX Inc.

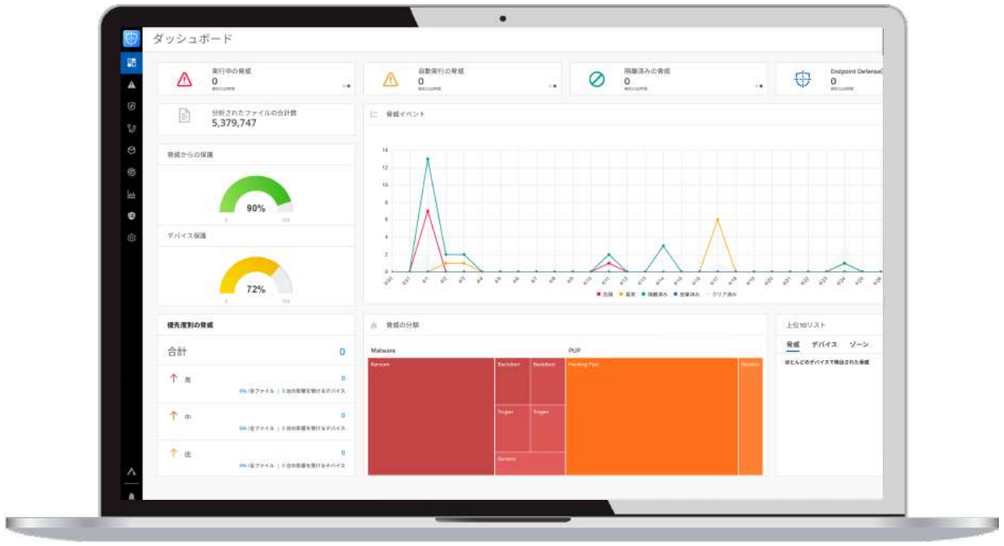
LANSCOPE
Cyber Protection

次世代AIアンチウイルス

Aurora Protect

AIを使用して99%※以上の高い検知率を実現

まだ見ぬウイルスも先回りしてブロック



※2024年5月 Tolly社のテスト結果より

MOTEX

Arctic Wolf Networks社によるBlackBerry社のCylance事業買収に伴い、
「CylancePROTECT」は「Aurora Protect」に、「CylanceOPTICS」は「Aurora Focus」に、
「CylanceMDR」は「Aurora Managed Endpoint Defense」に名称変更されました。

これまでのマルウェア対策における3つの常識

検知
パターンファイル型の
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
さまざまな製品が必要で
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

Aurora Protect(旧称: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

未知・亜種のマルウェアも
検知率99%以上※

※2024年5月 Tolly社のテスト結果より

大手企業や官公庁でも導入

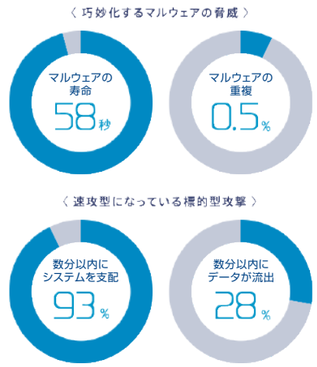
エムオーテックスでは2016年の
販売開始以来、
2,100社以上※に導入

※2025年3月時点

画期的な検知手法でさまざまな賞を受賞

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

マルウェアの脅威とは

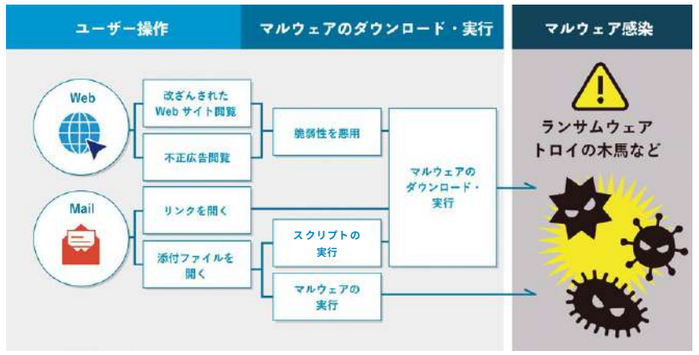


新しいマルウェアが作られる数 100万個／日

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。ベライゾン社の2016年度 データ漏洩/侵害調査報告書(DBIR)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、従来のパターンファイル型のアンチウイルス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% で「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分かります。

Web閲覧とメール開封によるマルウェア感染が主流に

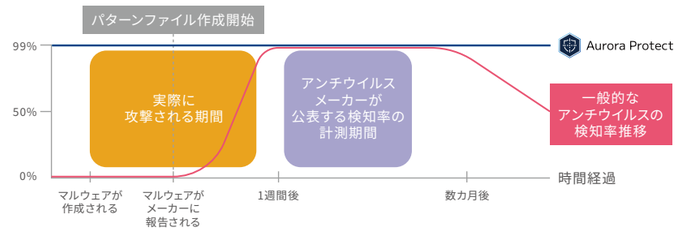


改ざんされたWebサイトの閲覧や、メールに添付されたファイルの開封など、人の行動における脆弱性を狙った攻撃が主流となっており、気づかない間にマルウェアに感染しているケースが多々あります。
テレワーク・在宅勤務が当たり前となった昨今、従業員がオフィス以外のネット環境で業務を行う場合、エンドポイントセキュリティが不十分なままだとマルウェア感染で重要情報が流出するリスクが高くなってしまいます。

パターンファイル型のアンチウイルスの限界

セキュリティ対策として広く使われている従来のパターンファイル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、結果的に昨今のマルウェアのほとんどがパターンファイル型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。

アンチウイルスにおける検知率の推移



パターンファイルで未知のマルウェアを止めることができないのは構造的な問題。

実際に攻撃に使われてい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。

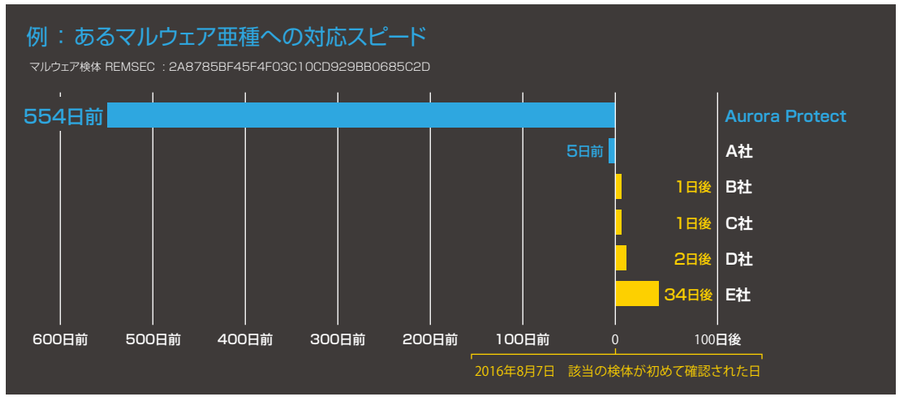
※Arctic Wolf Networks社調べ

Aurora Protectとは

未知のマルウェア検知率99%以上※を誇るAurora Protect

Aurora Protectの最も特長的なポイントは、まだ世の中に存在しない、全くの未知である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、一般的に新型マルウェア発見が公表されるよりも平均25カ月前のエンジンで検知できている実績があります。

※2024年5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

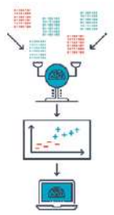
マシンラーニングの特許技術を活用した「予測脅威防御」

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

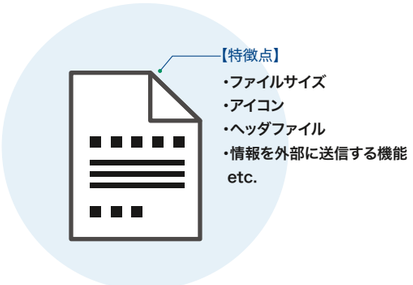
教師データの特徴点を抽出
（1ファイルあたり最大700万の特徴点）、
各ファイルのマルウェアらしさを数値化



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）

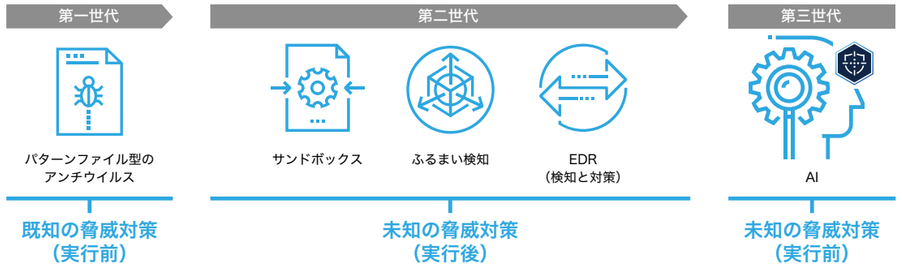
画像認識のマシンラーニングでキリンの特徴を学習し、キリンを判別できるようになるのと同様に、
ファイルにおけるマルウェアの特徴を学習し、未知・亜種のマルウェアも正しく判別します。



Aurora Protectの特長

AIエンジンを活用した第三世代のアンチウイルス

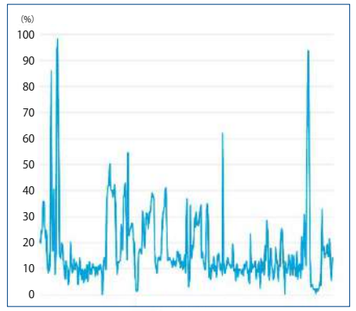
Aurora ProtectはAIエンジンを活用。ゼロデイ攻撃への対応が難しいパターンファイル型のアンチウイルスや、"マルウェア感染は止められない"ということを前提とするEDR製品のような事後対策とは別のアプローチで、未知の脅威でも実行前に検知し、防御することができます。



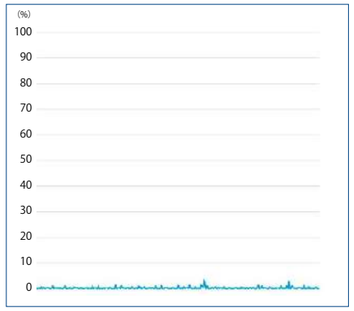
クライアント端末へのCPU平均負荷0.1%※、毎日のパターンファイル更新も不要

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、頻繁なパターンファイル更新も必要ありません。

※2023年7月 Arctic Wolf Networks社の検証結果より



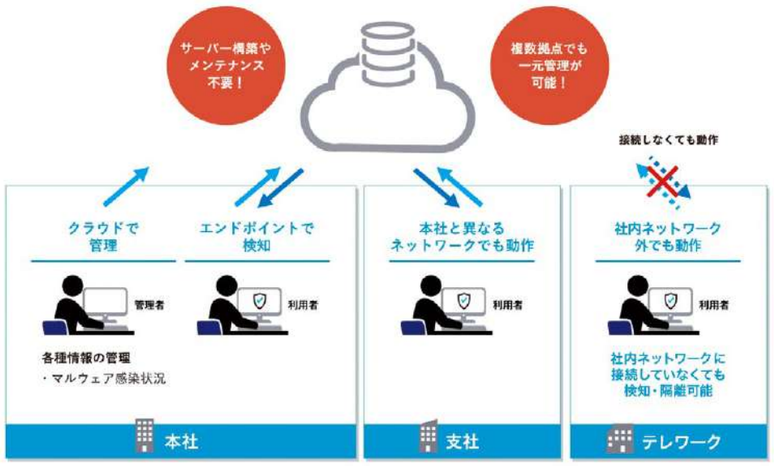
フルスキャン時のCPU利用率



フルスキャン後のCPU利用率

クラウド型製品のため、自社での環境構築・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なクラウド型製品であるため、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。



LANSCOPEが提供する新しいマルウェア対策とは

エムオーテックスが提供する“LANSCOPE サイバープロテクション”では、高性能な AIアンチウイルス「Aurora Protect」を、エムオーテックス独自の運用支援サービスとともにご利用いただけます。エムオーテックスのセキュリティエンジニアが直接お客様の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500円(税抜)/1台で、最低5台から導入できるため、部分導入もご検討いただけます。エムオーテックスのマネージドサービスにより、業界最高峰のAIアンチウイルスをお手軽にご導入いただけます。

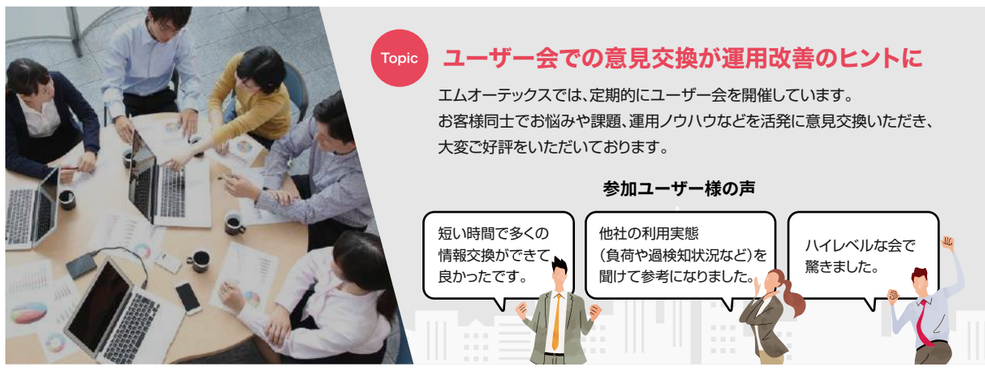
- 高性能のAIアンチウイルス「Aurora Protect」は
  マルウェア検知率 99%以上！※1
- セキュリティエンジニアによる運用代行・定期レポートサービス
  があるから、専任担当者不在でも安心！※2
- LANSCOPE エンドポイントマネージャーと連携すると、
  操作ログからマルウェアの侵入原因をカンタンに調査できる！※3

※1:2024年5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

エムオーテックスは、BlackBerry Japanのパートナー・オブ・ザ・イヤーを8年連続受賞※

※BlackBerry社は現在、Arctic Wolf Networks社にCylance事業を売却しています。

※2025年3月末現在



Aurora Protect の提供サービス

標準サービス

▶ Aurora Protect ※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
・Aurora Protect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しており、
　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。

※1:オプションでAurora Focus(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:平日9:30-12:00, 13:00-17:30(祝祭除く)

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、
管理コンソール上で行う操作をエムオーテックスのエンジニアが代行します**

運用代行の例

■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、Aurora Protect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。

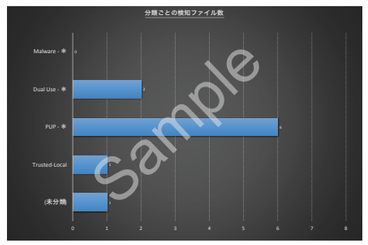
■クライアントプログラムのバージョンアップ
半年～1年に1回程度発生するクライアントプログラムの
バージョンアップ設定を行います。

Aurora Protectの管理コンソール

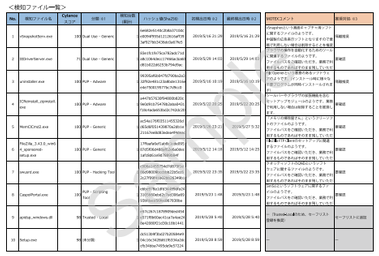
定期レポートオプション

エムオーテックスのエンジニアが検知状況を確認して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、
どのような種別のファイルが多かったかなどを分析し、
報告します。



【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。

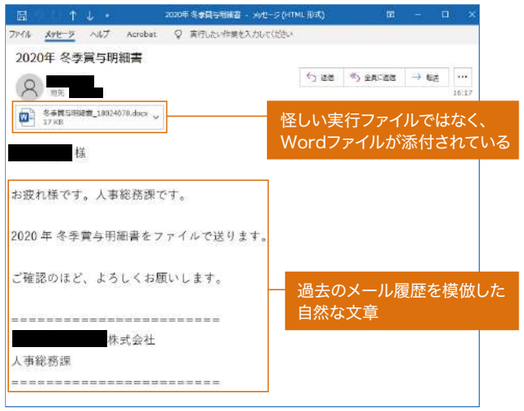


Emotetによる被害状況とAurora Protectによる検知

マルウェア「Emotet」について

近年、大きな被害をもたらしたマルウェアに「Emotet（エモテット）」があります。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、より危険なマルウェアに成長を遂げ、日本でも大きな被害を出しました。
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することが多く、情報を窃取する不正な動作が行われた後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は約9,000件と発表されています。
今後もマルウェアによる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、国内のマルウェア感染被害もより深刻化することが想定されます。

出典：JPCERT/CC（マルウェアEmotetの感染再拡大に関する注意喚起）



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。

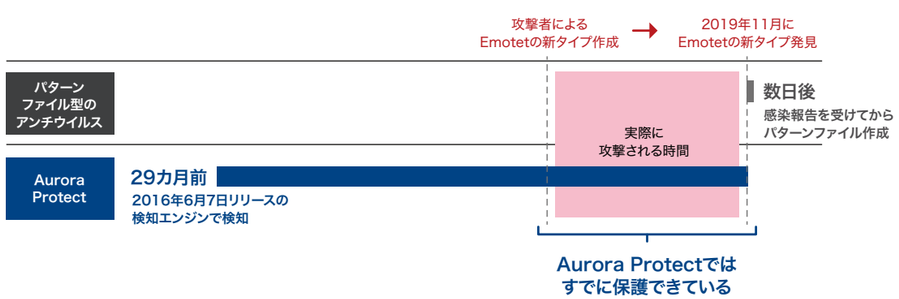
◀ばらまきメールの例
いくつかのバリエーションがあり、不信感を抱かせにくい工夫が施されています。

Aurora ProtectによるAIを活用した予測防御

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。パターンファイル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、感染を防ぐことが難しい状況です。

Aurora Protectは、2019年11月に確認された当時の最新タイプであった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（Arctic Wolf Networks社調べ）。つまり、Aurora Protect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



24時間365日、専門家が脅威を監視「Aurora Managed Endpoint Defense」

世界トップレベルのセキュリティ専門家による監視代行サービス
AIアンチウイルス（EPP）・EDR・運用支援・MDRをオールインワンでご提供

Aurora Managed
Endpoint Defense

Aurora Protect	Aurora Focus	MDR	
		個社ごとの導入設計	脅威監視の代行
99%以上※1 の検知率で マルウェア感染を未然に防御	EDRでマルウェアの侵入経路 を特定。再発防止策の検討に	Aurora Protect・ Aurora Focus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

※1：2024年5月 Tolly社のテスト結果より

Aurora Managed Endpoint Defense 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Arctic Wolf Networks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：Arctic Wolf Networks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%以上 ※1 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。

エムオーテックスによるAurora Protect導入事例

※CL数：クライアント端末数
＊掲載の事例はいずれも取材当時の内容です。ただし、Arctic Wolf Networks社によるBlackBerry社のCylance事業買収に伴い、「CylancePROTECT」は「Aurora Protect」に、「CylanceOPTICS」は「Aurora Focus」に名称変更されています。

山梨県庁 様（CL数：約4,200）

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買い替えのタイミングに合わせて、セキュリティ運用の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を利用する次世代型アンチウイルス「Aurora Protect」だった。

「パターンファイル型のアンチウイルスの場合、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た。その過程で数理モデルを用いたAurora Protectの先進的な技術を知り、興味を持った」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だったが、Aurora Protectで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なかったが、その部分の負担が減ることを期待する」と担当者は語った。
また、「これまでグレーな検知結果が出た際の判定で悩ましい場面もあったが、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などのエムオーテックスからの説明も迅速で十分満足のいくものが得られている。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る」とエムオーテックスの対応も評価した。

株式会社沖縄銀行 様（CL数：2,432）

システム部 執行役員部長　髙良 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。
「パターンファイル型のアンチウイルスでは、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にならない」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、最終的には実行ファイルが動く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、Aurora Protect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ない。しかしAurora Protectであれば、ファイルの特徴を解析して判断するため、実行前に検知できる」と評価する。 Aurora Protectの能力を確かめるべく、導入前に試用した結果、その検知率の高さを改めて実感することができたとのことだ。
「こんなに良い製品があるのかと驚いた。試行フェーズでは未知のマルウェアを実行してみた上で、しっかり検知できることを確認した。」

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年よりパターンファイル型のアンチウイルスを利用してきたが、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、Aurora Protectの検討を開始した。
「Aurora Protect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だった。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、検知した際に、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「Aurora Focus」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支援するもので「Aurora Protect」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際には、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
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、「パターンファイル型のアンチウイルスでは、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の見直しのために、Aurora Protectの評価検証が行われた。パターンファイル型のアンチウイルスでは検知できなかったファイルがAurora Protect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、Aurora Protect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、Aurora Protect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カ月に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」と従業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、これまでパターンファイル型のアンチウイルスを利用していたが、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。
それまで利用していたアンチウイルス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アンチウイルスである「Aurora Protect」の導入が検討された。

複数製品と比較しつつ、 Aurora Protectのトライアルを実施。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、パターンファイル型のアンチウイルス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。「以前利用していたパターンファイル型のアンチウイルスでは、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、Aurora Protect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パートナー企業の従業員が利用する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、最終的に次世代型アンチウイルス「Aurora Protect」と、EDRである「Aurora Focus」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、「パターンファイル型の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を用いた次世代型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。Aurora Protectのマネージドサービスである「LANSCOPE サイバープロテクション」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」と評価した。