- AIアンチウイルス -

Protect Cat

プロテクトキャット Powered by Cylance

LanScope Cat

BlackBerry | CYLANCE

CYLANCE 2017 Japan Partner of the Year

国内導入実績 2年連続No.1

導入に必要な環境 ＊100台環境、標準パックの場合

統合マネージャー/サブマネージャー

- OS
  Windows Server 2008 R2、 Windows Server 2012、 Windows Server 2012 R2、
  Windows Server 2016
- CPU
  2.0GHz 相当
- メモリ
  4GB以上
- HDD空き容量
  200GB以上
- データベース
  SQL Server 2008、SQL Server 2008 R2、
  SQL Server 2012、SQL Server 2014
- Webコンソール（ブラウザー）
  Internet Explorer 11 以上
  Google Chrome 69 以上
  Mozilla Firefox 62 以上

エージェント

[Windows]

- OS
  Windows XP
  Windows Vista
  Windows 7
  Windows 8
  Windows 8.1
  Windows 10
  Windows Server 2003
  Windows Server 2003 R2
  Windows Server 2008
  Windows Server 2008 R2
  Windows Server 2012
  Windows Server 2012 R2
  Windows Server 2016

[Mac]

- OS
  Mac OS X Tiger v10.4.11 以降
  Mac OS X Snow Leopard
  OS X Lion
  OS X Mountain Lion
  OS X Mavericks
  OS X Yosemite
  OS X El Capitan
  macOS Sierra
  macOS High Sierra
  macOS Mojave

＊マネージャーのハードウェア環境は、クライアント数100台までの推奨環境です。
管理する台数や収集するログにより推奨環境が異なります。
＊マネージャーサーバーは、同一OS 内に他システムと共存させることも可能ですが、
専用ハードウェアをご用意いただくことを推奨しています。
共存させる場合、問題発生時の切り分けなど、サーバーの分離をお願いする場合があります。
＊データベースは本製品に付属の製品、もしくはお持ちのMicrosoft SQL Server ライセンスが利用できます。
＊500 台以上をクラウド環境で管理する場合、本製品に付属のSQL Server(Standard Edition) は利用できません。
＊Webコンソールの一部コンテンツの表示には、Silverlight5 以降のインストールが必要です。
＊エージェントの動作環境（CPU、メモリ、HDD 空き容量）はOS の推奨システム要件を満たしてください。
同居ソフトウェアの使用状況により必要となるシステム要件が変更になる場合があります。
＊クライアントエージェント（MR）は日本語／英語／中国語（簡体字）の海外OS に対応しています。
＊Mac OS X Mountain Lion以前の管理には、LanScope Cat Ver.9.0.0.0のクライアントエージェントを利用する必要があります。
＊Mac OSのCylancePROTECTサポートは、OS X Mavericks 以上が対象です。
＊対応OSについての詳細は、弊社Webサイト公開のOS対応表をご覧ください。

●開発／販売

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　〒108-0075　東京都港区港南1-2-70 品川シーズンテラス5F　TEL：03-5460-1371
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（月～金曜日）
※携帯電話／PHSからは06-6308-8981をご利用ください。

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

●お問い合わせは当社へ

2019.4 発行

MOTEX
Secure Productivity

BlackBerry | CYLANCE とは

サイランスはサイバーセキュリティをAIで実現する企業です。
AI (人工知能)、アルゴリズム技術、および機械学習を
サイバーセキュリティに応用することで、
未知・既知のマルウェアからお客様を守ります。

MOTEX × Cylance

MOTEXは、2016年5月11日にCylance社とのOEMパートナー契約の締結を発表しました。これにより、CylancePROTECT技術をLanScope Catに統合し、同製品の顧客に先進的な脅威対策モジュールとしての提供を実現しました。両社の共同ソリューションはサイバー攻撃を未然に防御し、どのアプリケーションや有害な可能性のあるプログラムがエンドポイントに存在しているのかを把握できるという、今までにない卓越した可視性を提供します。
LanScope Catは、Cylance社の人工知能を搭載した新機能プロテクトキャットにより、外部・内部に潜む企業のセキュリティ課題を解決します。

Stuart McClure氏(プレジデント兼創業者)からのコメント

“我々はMOTEXとともに、MOTEXの数千社に及ぶユーザー企業に、複雑なインシデント対応プロセスを必要としない革新的な脅威対策能力を提供できることを光栄に思います。Cylanceは情報セキュリティに対して最も効果を発揮する予防的アプローチを提供するためには、業界最高のツールを統合すべきだと考えています。この度の協業によって、日本企業は今、企業・組織とその情報を守る業界最高の製品を持つことになります。”

LanScope Catはエンドポイントセキュリティに必要な機能を搭載

マルウェアの感染防御から内部漏えい対策までを実現する統合型エンドポイントマネジメント

● 検知率99%以上*のマルウェア防御

・未知・既知のマルウェアを実行前防御
・インターネット非接続環境にも対応

*2018 NSS Labs Advanced Endpoint Protection Test結果より

● 更新プログラム配布・脆弱性対策

・アプリ・OSの脆弱性確認、対策
・IT資産管理

● インシデント発生時の原因特定・内部漏えい対策

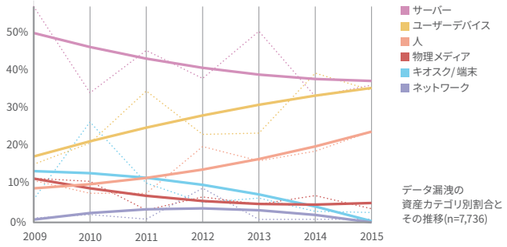
・マルウェアの流入経路追跡
・ログ管理による抑止効果

脅威の現状

企業や組織を狙うサイバー脅威の数は年々増加の一途を辿っており、その手口もさらなる進化を遂げています。サイバースパイ活動やサイバー犯罪を目的とした攻撃は、よりエンドポイント端末をターゲットとするように変化してきており、また攻撃で利用されるマルウェアも企業や組織間で使い回されることなく、ユニークなものが使われる傾向があります。

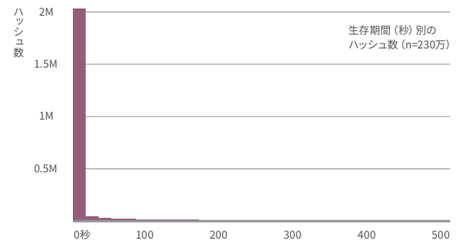
攻撃対象の変化

従来はサーバーをメインの標的としてきていましたがユーザーが使用するエンドポイントのデバイスに対象が移りつつあります。



ユニークなマルウェアの使用

攻撃者は既存のセキュリティ製品をすり抜けるために頻繁にマルウェアコードを変更しており、企業・組織間で同じものが使われるケースはほとんどなく、99%のマルウェアハッシュはわずか58秒間しか検出されていません。



出展元 : Verizon「2016年度データ漏洩/侵害調査報告書(DBIR)」

これまでの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ィ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

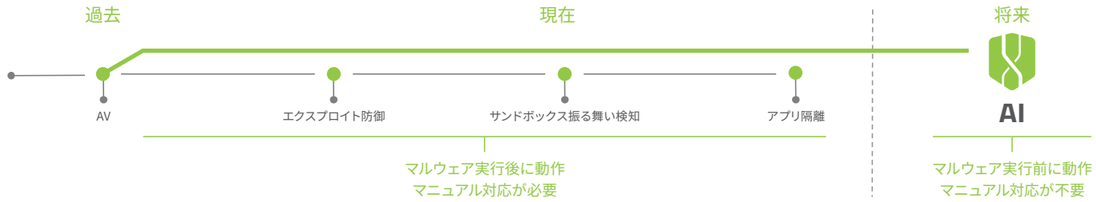
シグネチャベースで未知のマルウェアを止めることが出来ないのは構造的な問題。

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。

AIアンチウイルスというアプローチ

アンチウイルスだけで安心できた時代を取り戻す

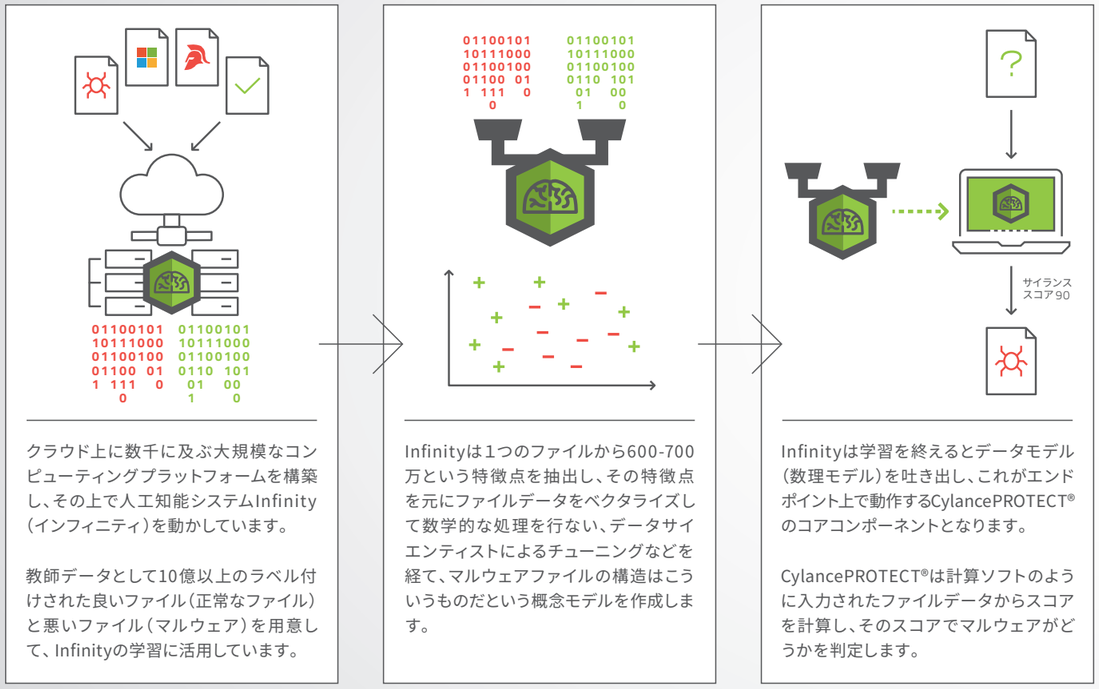
ほんの少し前までは「アンチウイルスを入れて最新のパターンファイルに更新しておく」ことがセキュリティ対策の定石となっていました。しかし、従来のアンチウイルスが脅威を止めることができなくなったために市場には数多くの新しいセキュリティ製品が溢れています。しかし、それらはいずれもマルウェアが動き出してから初めて検知できるという動的分析のアプローチになります。サイランスはAIの技術をアンチウイルスの静的分析に活用することで、マルウェアが実際に動き出して感染してしまう前に未然に防ぐことができます。また振る舞い検知のような動的分析では多くのアラートによって運用の負荷が高まる傾向がありますが、AIアンチウイルスでは精度の高い自動防御により、シンプルなセキュリティ運用を実現できます。AIアンチウイルスのCylancePROTECT®はアンチウイルスだけで安心できた時代を取り戻します。



Protect Cat とは

プロテクトキャットは、CylancePROTECT®のOEM提供を受けMOTEXが開発した
LanScope Catの機能です。
人工知能アルゴリズムを活用しエンドポイント上でマルウェアが実行される前に攻撃を防御するだけでなく、流入経路の追跡から原因追求までの統合管理を実現しました。

AIによる予想脅威防御の仕組み How it Works



クラウド上に数千に及ぶ大規模なコンピューティングプラットフォームを構築し、その上で人工知能システムInfinity（インフィニティ）を動かしています。

教師データとして10億以上のラベル付けされた良いファイル（正常なファイル）と悪いファイル（マルウェア）を用意して、Infinityの学習に活用しています。

Infinityは1つのファイルから600-700万という特徴点を抽出し、その特徴点を元にファイルデータをベクタライズして数学的な処理を行ない、データサイエンティストによるチューニングなどを経て、マルウェアファイルの構造はこういうものだという概念モデルを作成します。

Infinityは学習を終えるとデータモデル（数理モデル）を吐き出し、これがエンドポイント上で動作するCylancePROTECT®のコアコンポーネントとなります。

CylancePROTECT®は計算ソフトのように入力されたファイルデータからスコアを計算し、そのスコアでマルウェアがどうかを判定します。

プロテクトキャット Powered by Cylanceの特長

- 1-2% CPU — 1〜2%CPU使用率
- 60 MB — メモリ消費 40〜60MB
- インターネットに接続しない オフラインでも判定可能
- 毎日の シグネチャ更新が不要
- Windows、Mac OS、Linuxに対応
- サーバ環境、仮想環境にも対応

プロテクトキャット Powered by Cylance

4つのプロテクション機能 Features

4つのプロテクション機能で99%以上*の防御率を実現

マルウェア防御

- AI（人工知能）で脅威を予測
- マルウェアを実行前に阻止
- シグネチャ不要
- シグネチャ更新に伴う定期スキャンが不要
- ファイルが実行される直前で判定
- 新しいファイルは最小のリソースで静かにバックグラウンドでスキャン

メモリ防御

- メモリの悪用防御
- 脆弱性攻撃の防御
- プロセスインジェクション防御
- 特権昇格の防御
- シェルコード/ペイロード攻撃の防御

スクリプト制御

- 不正なパワーシェルとアクティブスクリプトの制御
- 危険なVBAマクロを制御
- ファイルレス攻撃の阻止
- 危険なドキュメントファイルの制御

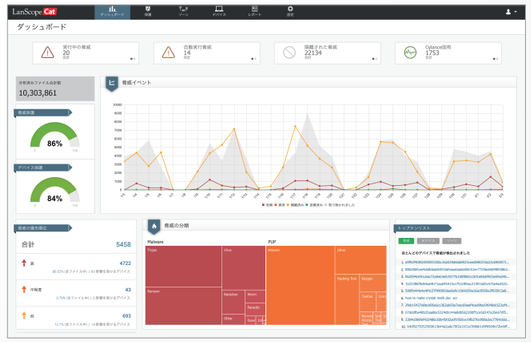
アプリケーション制御

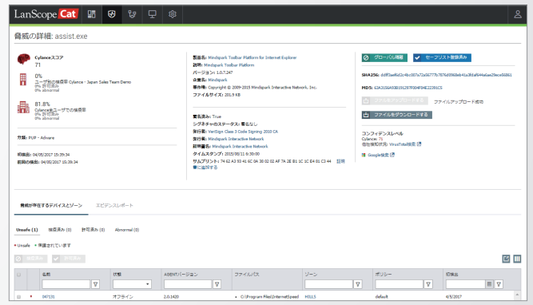
- 安全と判断されたバイナリだけに利用を制限
- 未確認または不正なバイナリの実行を阻止
- 任意のバイナリの変更を防止

*2018 NSS Labs Advanced Endpoint Protection Test結果より

マルウェア解析結果をレポーティング

AIによるファイル解析結果のスコアや、ランサムウェア、トロイの木馬といった種別、どのような脅威があるのかなど、マルウェアの解析結果の詳細をレポーティングします。





[オプション] CylanceOPTICS™

CylanceOPTICSはプロテクトキャット導入ユーザー様向けオプション製品です。機械学習の技術を応用したCylanceOPTICSはEDR（Endpoint Detection and Response）機能として、プロテクトキャットと併用することであらゆる脅威への分析、検出そして対処を実現し、セキュリティ運用の効率と防御力を高めます。

より詳細な経路のフォレンジック調査

脅威がどのような侵入経路で来たのかを確認し、発見された攻撃の痕跡）情報に基づいてさらにオンデマンド検索での調査を実施。攻撃面を削減することで防御力を向上できます。

脅威ハンティング

ファイル、ネットワーク接続、プロセス、レジストリキーの攻撃の痕跡情報に基づき、隠れた脅威を検索。検索結果を多面的に確認することで、全社規模で端末上の状況を把握できます。

感染端末の封じ込め

攻撃の拡大をくい止める迅速なアクションを行い、端末の隔離やファイルの入手、自動隔離などを即座に実施できます。

端末挙動からの脅威検知と対処

端末上の疑わしい振る舞いをルールとして登録しておくことで、攻撃の予兆を未然に検知し、更に脅威に対する適切なアクションを自動化できます。

Protect Cat の特長

既知・未知のマルウェアを検知・隔離し、流入経路を追跡。
原因となるユーザー操作に対策することで再発を防ぎます。

マルウェアを検知し、トロイの木馬・ランサムウェアなどの種別やリスクの高さを判断します。検知前後の操作ログから特定のWebサイト閲覧・標的型メールの開封など、流入原因を確認し、Webサイトのフィルタ強化や社員教育により再発を防止できます。

インターネット非接続環境における
マルウェア検知・隔離状況の収集と把握を実現します。

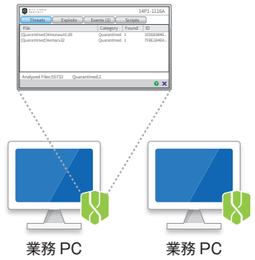
インターネットに繋がらない環境でもLanScope Catのマネージャーに全ての情報を集め、
レポートで検知状況の確認やアラートメールによる通知、またエージェントの配布やポリシーのアップデートが可能です。

インターネット非接続環境

CYLANCE PROTECT

● マルウェア検知・自動隔離（スタンドアロン）

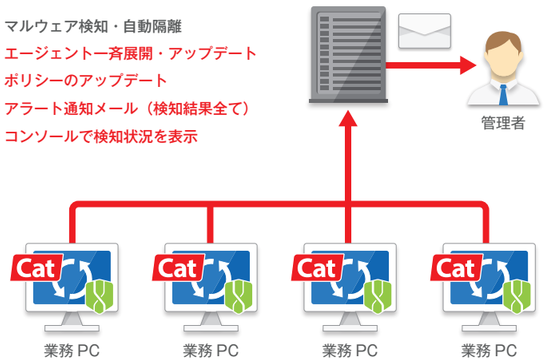
それぞれの PC上で
検知・隔離



業務 PC　業務 PC

プロテクトキャット Powered by Cylance

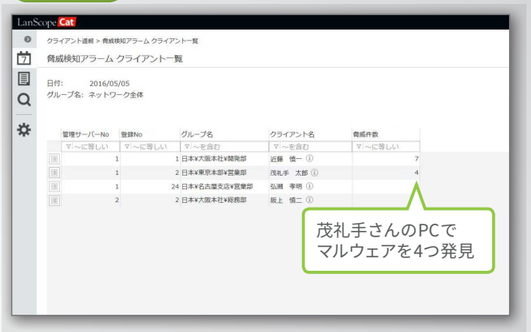
● マルウェア検知・自動隔離
● エージェント一斉展開・アップデート
● ポリシーのアップデート
● アラート通知メール（検知結果全て）
● コンソールで検知状況を表示



マルウェア検知前後の“人の操作”を把握。
クリックしていくだけで、原因を特定できます。

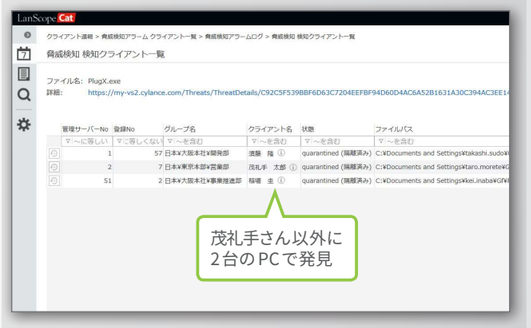
Step1 カレンダーで脅威の有無を確認。

Step2 どのPCで何件の脅威があったか確認。

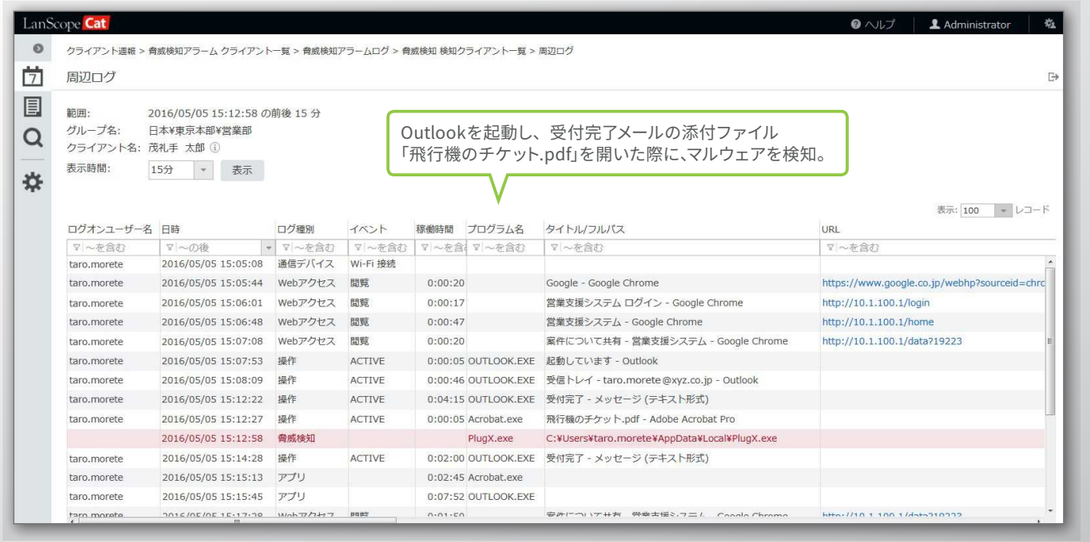


Step3 どんなマルウェアを検知したか確認。

Step4 同じマルウェアを検知した PCの確認。



Step5 マルウェアの流入原因となるユーザー操作を追跡・確認し、再発を防止。



※流入経路の追跡は、別途ログキャット（操作ログ管理）の購入が必要です。

ランサムウェア WannaCry 事例（2017 年 5 月）

概要

2017年5月12日、スペインのコンピュータ緊急レスポンスチームであるCCN-CERTがスペイン国内の大手通信会社に対してランサムウェアの攻撃が急速に広がっていることを警告しました。またその後、英国のNational Health Service（NHS）からも国内のいくつかの組織に対する攻撃についての注意喚起が公開されました。この「WannaCry（泣きたくなる）」という名が付けられたランサムウェアによる攻撃は、欧州だけでなく世界100カ国以上に感染を拡大し、政府機関、病院、通信会社、自動車会社などで実際に被害が確認され、世界で20万台以上が感染したとテレビやメディアなどでも大きく報道されることになりました。

WannaCryについて

この攻撃では、WannaCry または WannaCrypt などと呼ばれるランサムウェアが使われており、感染すると端末内部の Office データや動画、画像、など 166 種類のファイルを暗号化し、身代金（ランサム）を要求します。暗号化されたファイルのファイル名には「.WNCRY」という文字列が付与され、暗号化が完了した後にボリュームシャドーコピーを削除するため復元が阻止されてしまいます。身代金は仮想通貨ビットコインでの支払いが要求され、最初の要求額は $300 - $600 ですが、3 日以内に支払いがなければ要求金額が倍になるような脅しを用いています。

これまでの一般的なランサムウェアは、感染後に表示される脅迫画面のメッセージが英語でしたが、今回の WannaCry については、下記のように日本語化された画面が表示される点が特徴です。これは世界の中で日本もターゲットにされているということがいえます。

WannaCry は、2017 年 3 月にマイクロソフト社がパッチを公開した、Windows の SMB（Server Massage Block）の脆弱性（MS17-010）をついて感染行動を行います。

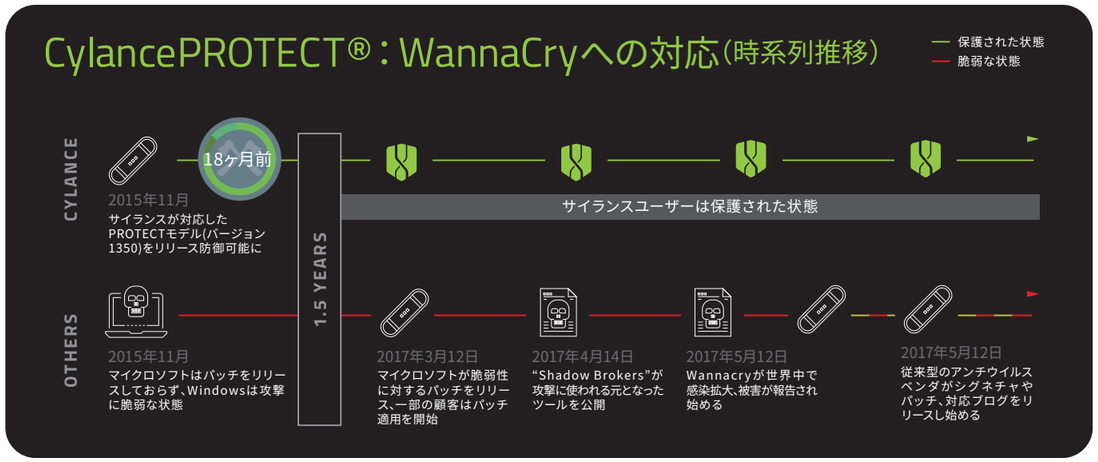
このランサムウェアの厄介な点は、1 台の端末の感染で終わるのではなく、感染した端末が他の社内・社外端末に対して、同じ脆弱性を持つ端末のスキャンを行い、該当の端末を発見次第感染拡大させていく点にあります。

この結果、最初はたった 1 台の感染にもかかわらず、社内のファイルサーバーや基幹システムまでもがランサムウェアに感染し重大な問題を引き起こす可能性を秘めています。

▲ WannaCry によって表示される日本語の身代金要求の画面

AIによる予測防御

CylancePROTECT®では一連の攻撃が報告される前から既にWannaCryランサムウェアに対応していました。CylancePROTECT®は従来製品のようにパターンファイルを利用せず、機械学習の技術を活用してデータモデルを作成した上で、そのモデルに基づく予測判定によって未知のマルウェアを検出します。サイランスではこれまでにIn-the-Wildで報告されているWannaCryのサンプルファイルを入手して試験を行い、CylancePROTECT®で検知・ブロックできることを確認しています。WannaCryを検知できるCylancePROTECT®のデータモデルは2015年11月にリリースされていますので、弊社製品をご利用のお客様は既に1年半以上も前から今回の攻撃を防ぐことができる状態になっていたと言えます。



SPECIAL INTERVIEW

セキュリティ対策の “ 常識 ” が変わる

ウイルスは防ぐ時代へ、攻撃防御のプロが認めた「半世紀に 1 度の製品」とは

今日、サイバー攻撃リスクへの対策が企業には切実な課題として突きつけられている。一方で、多種多様な対策製品・ソリューションの中からどのようなアプローチが最善なのか見極めに苦慮している企業も多い。警察組織でサイバーテロ対策やサイバー攻撃対策に従事した経歴を持ち、20 年以上にわたりサイバー攻撃防御の第一線で活躍を続ける九電ビジネスソリューションズ株式会社の堂領輝昌氏と、最新鋭のウイルス対策ソフトを提供する Cylance Japan 株式会社の乙部幸一朗氏、さらに Cylance OEM パートナー兼ユーザーでもあるエムオーテックス株式会社の丸山悠介が、今日の日本企業におけるサイバーセキュリティ対策の「誤った常識」について鋭い意見を交わした。

▲ 左から、Cylance 乙部氏・QBS 堂領氏・MOTEX 丸山

従来製品を超越する、歴史的かつ革命的な製品

― サイバーセキュリティ対策を巡る現在の状況をどのように捉えていますか。

堂領　あまりにも大きな「誤った常識」に満ちています。それは「ウイルス対策ソフトではウイルスは防げない」という常識です。勘違いをしないでいただきたいのは、多層防御やウイルス侵入後の事後対策を否定する意図は一切ないということ。お伝えしたいのは、多層防御における構成要素の要であるウイルス対策ソフトについて、「まだ 20 年前のアーキテクチャである従来型製品を使い続けているのですか？」という問題提起です。

国内企業の多くは、現在凄まじいスピードで販売実績を伸ばしつつある、最新鋭のウイルス対策ソフトの情報を見逃しています。セキュリティ業界の歴史が始まって以来の革命的な製品が出現している事実を知っていただきたい。私はベンダー側の人間ではありません。国内のセキュリティ被害を抑えたいと願うユーザーの立場であるからこそ、垣根を越えた真実を発信できると信じています。

結論を言います。あらゆるセキュリティ対策製品の検証に優先して『CylancePROTECT®』の検証及び導入をされてください。それが 20 年間にわたりサイバー攻撃防御の最前線に立ち、幾多の製品を検証してきた私の答えです。未知のウイルスが世に出現した “ 瞬間 ” に、それこそ検知率が 100% に迫るほどの圧倒的な数字でウイルスを次々と検知する凄まじさを目にした時、私は言葉を失いました。「半世紀に 1 度しか出現しない究極の製品」と断言する理由はここにあります。

ウイルス対策ソフトが無力とされた時代は終わりを告げました。CylancePROTECT® が現れた今、過去の常識は完全に覆ったのです。

加熱する AI ブーム。だが、AI ありきの製品選定は誤りを生む

― CylancePROTECT® を選ばれた理由は、AI を搭載した製品だからでしょうか。

堂領　違います。ウイルス対策ソフトの性能とは、ウイルスの検知力のみが唯一の指標です。いたずらに AI という言葉に振り回されていては目的も手段も見誤ってしまいます。今回の検証では、結果的に「AI 搭載」を宣伝する複数の著名製品を比較しましたが、真の AI たる圧倒的な実力を示した製品は、CylancePROTECT® だけです。

乙部　我々の製品のアプローチにおいては、AI の使い方に大きな特色があります。一般的なウイルス対策ソフトにおける AI 活用は、シグネチャ（ウイルス検知パターン）の生成において機械学習を用いるというものですが CylancePROTECT® にはシグネチャそのものが存在しません。それに替わる「モデル」を提供しており、AI の機械学習エンジンに対して「ウイルスのファイル」および「ウイルスでないファイル」を教師データとして大量に読み込ませて学習させることでモデルを構築しています。我々が収集した数十億というあらゆるファイル構造にかかわる特徴を、AI が精密に分析して導き出したものがモデルであり「あるファイルにウイルスの特徴があるか否か」の判断を極めて高い精度で高速に行えます。（続く）

インタビューの全文は、Web からダウンロードいただけます。　Cat　資料　検 索

九電ビジネスソリューションズ株式会社
上級セキュリティプロフェッショナル
課長　堂領 輝昌 氏

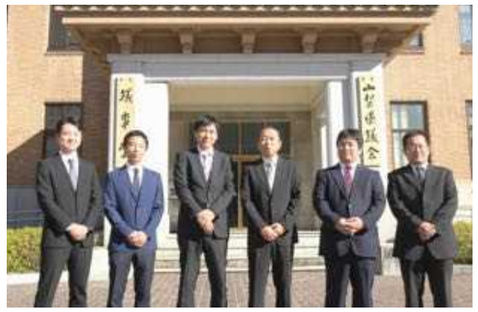
90 年代からサイバー攻撃防御の分野に 20 年以上従事。過去に警察組織でサイバーテロ対策及びサイバー攻撃対策業務に従事し、セキュリティシステム開発で警察庁長官賞を 2 度受賞。現職で情報セキュリティ対策の全般を担当。制御系システムに対する情報セキュリティ監査を 2007 年度から 10 年以上にわたり展開、国内有数の監査実績を持つ。経済産業省認定システム監査技術者、IT ストラテジスト、システムアーキテクト、IT サービスマネージャ、情報セキュリティスペシャリスト、ネットワークスペシャリスト、平成 29 年度 春期 情報処理安全確保支援士試験合格。公認情報セキュリティ主任監査人。CISSP - 国際公認情報システムセキュリティプロフェッショナル。

プロテクトキャット導入事例

山梨県庁

http://www.pref.yamanashi.jp/

職 員 数：約3,600名
構　　成：Cat 4,200CL



パターンファイル脱却と操作ログとの統合で運用負担を軽減！

ネットワーク分離など自治体特有の環境に
対応できるプロテクトキャット

インターネットと庁内LANを分離させるネットワーク分離にいち早く取り組むなど、総務省の方針に沿った対応を確実に行っている山梨県庁。
ネットワーク分離により顕在化した課題の解消と、マルウェア対策にかかるログ追跡のコストを軽減すべく、プロテクトキャットを導入。

「2年前に実施したネットワーク分離により、インターネット経由でのパターンファイル更新が簡単にできなくなってしまいました」と担当者は語る。またアンチウイルスとふるまい検知についても、検知されたものが問題あるか否か、影響範囲がどの程度かを判断するために必要な通信ログや操作ログの追跡に多くの時間と手間がかかり、機能の集約と管理効率向上が課題だったという。
プロテクトキャットの導入によって、以前はログ解析まで含めた原因特定に30分～1時間程度は必要だったものが、数クリックで必要な情報にたどり着くことができるようになった。
パターンファイル脱却についても「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」と担当者は語る。

株式会社沖縄銀行

http://www.okinawa-bank.co.jp/

設　　立：昭和31年6月21日　　従業員数：1,099名（平成28年3月末時点）
構　　成：Cat 2,432CL

未知のマルウェアにも対抗する多層防御の中核を担う

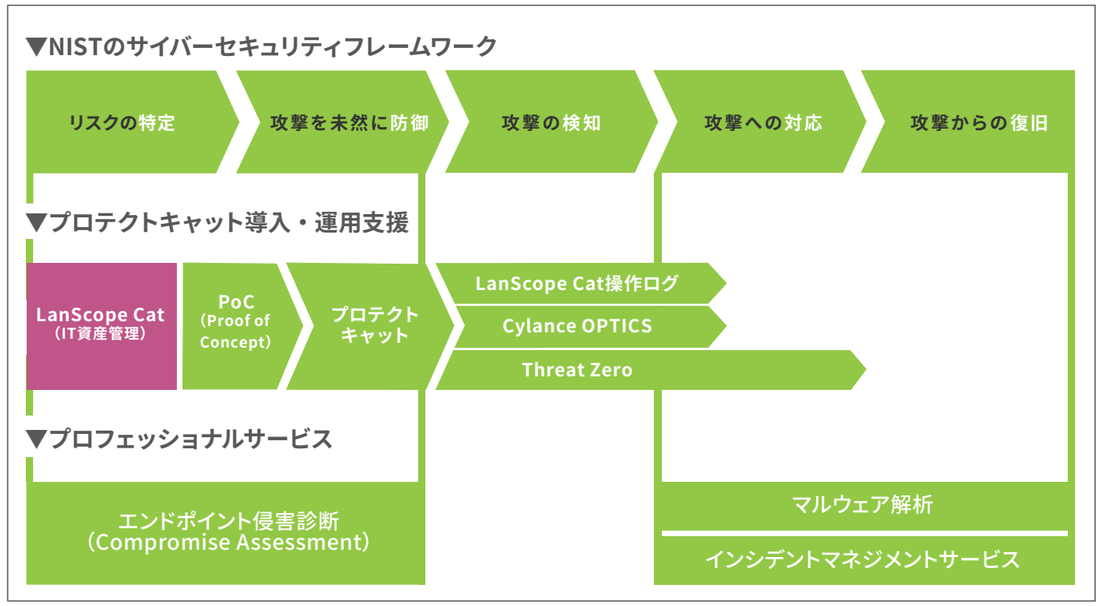
振る舞い検知とは異なる強固なマルウェア対策
「プロテクトキャット Powered by Cylance」

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が、長年取り組んできた安全かつ信頼性の高いインフラ作りに加え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。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「プロテクトキャット」を導入。

導入前の検証では、当初は半信半疑だったものの、実際のデモで未知の脅威を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いう。
また、同行は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る。
「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プロテクトキャット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侵入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。」と担当者は語る。

導入・運用支援 / プロフェッショナルサービス（有償）

MOTEXでは、サイランス社と連携し、お客様の運用シーンに合わせた支援体制をご用意しています。
アメリカ国立標準技術研究所（NIST）が定義する、サイバーセキュリティフレームワークの“5つの備え”に対応したそれぞれのシーンで、プロテクトキャットを、より効果的にご活用いただくための導入・運用支援から、エンドポイント対策のプロフェッショナルが提供する、各種プロフェッショナルサービスで、お客様のセキュリティをより強固に守ります。



サービス詳細

	サービス名	目的	対象
導入・運用支援	PoC （Proof of Concept）	導入前の製品検証を行う事で、製品に対する理解を深めていただきます。	ご検討ユーザー様
	Threat Zero	導入いただいたプロテクトキャットの運用を支援します。 検知したファイルの対処方法や分析の支援を行い導入環境下の脅威をゼロにすることで、強固なセキュリティの土台を作ります。 最終的に環境のレポートを提供します。	プロテクトキャット ユーザー様
	CylanceOPTICS	人工知能を活用し、いち早くインシデントを検出し、被害の拡大を防止するEDRオプション機能です。	プロテクトキャット ユーザー様
プロフェッショナルサービス	エンドポイント侵害診断 （Compromise Assessment）	**インシデント発生時**にサイランス社のプロフェッショナルチームと協力しインシデントの調査を実施します。 **平常時**では自社のエンドポイントが気づかない間に侵害されていないか、診断を行い結果のレポートを提供します。	すべての方
	マルウェア解析	**24時間以内**に、怪しいプログラムをサイランス社の解析官が解析して結果を報告します。 ＊プロテクトキャット以外で発見された検体も解析可能です。 ＊サイランス社の検体受取通知送信時から開始します。	すべての方

連携サービス

提携会社	サービス名	目的	対象
株式会社ラック	インシデント マネジメントサービス	セキュリティ緊急対応で培ったノウハウを有する株式会社ラックが、プロテクトキャットで検知したインシデントを、「LanScope Cat」で収集した情報をもとに、速やかに解析し、リスクをご報告します。	プロテクトキャット ユーザー様