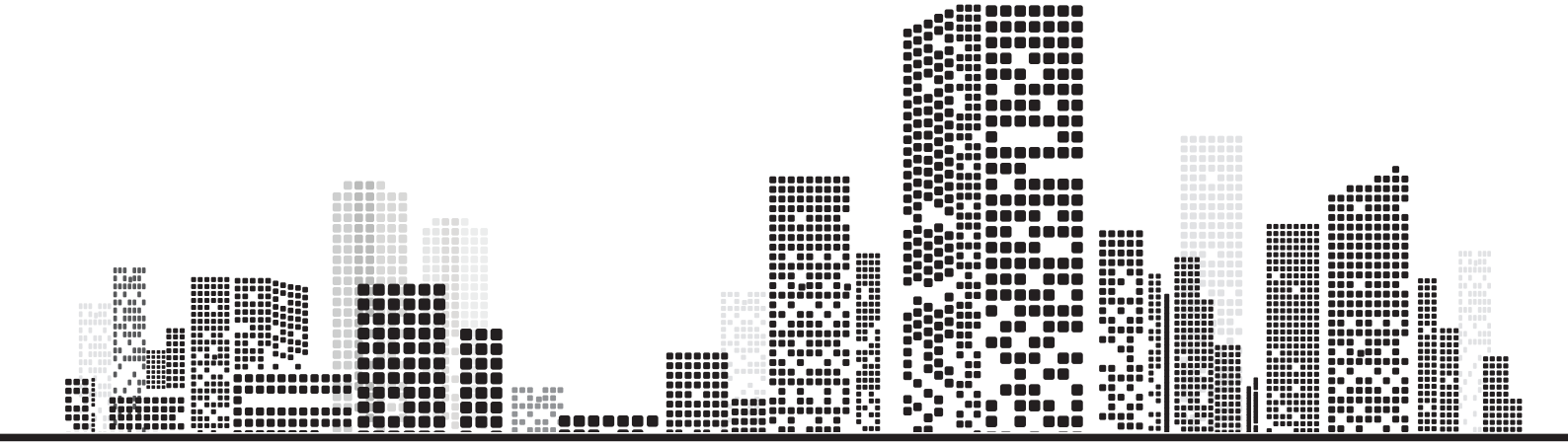
2017 | TOKYO NAGOYA OSAKA

MOTEX
Secure Productivity

Protect Cat Users Conference

LanScope Cat × CYLANCE



プロテクトキャットユーザー会について

2017 年も WannaCry をはじめとするランサムウェアが日本でも猛威を振るい、サイバー攻撃に対する対策の重要性はますます高まっています。数年前までは「アンチウイルスソフトをいれておけば大丈夫」というのが一般的でしたが、今や毎日 100 万個の新しいマルウェアが誕生しており、従来の対策だけではそれらを防ぐことは難しいと言われています。

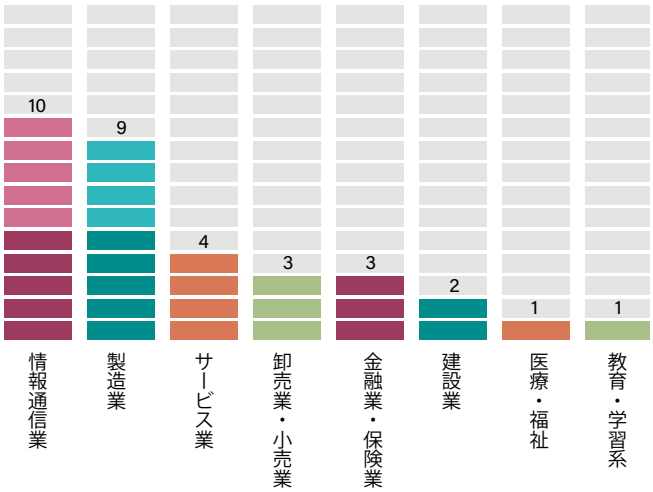
そんな中、MOTEX は 2016 年 7 月に未知のマルウェア検知率 99.7% ※を誇る次世代型アンチウイルス「CylancePROTECT®」を LanScope Cat に組み込み、新オプション「プロテクトキャット」をリリースしました。

現在プロテクトキャットは、リリースから1年で 100 社を超えるユーザー様に導入頂いております。今回はそのユーザー様（33 社 40 名）にお集まり頂き、東京・大阪・名古屋の3拠点で「プロテクトキャットユーザー会」を開催しました。当日は、Cylance Japan の基調講演をはじめ、ユーザー様による導入事例発表、また後半には普段のお悩みや課題、LanScope Cat の運用ノウハウを共有しあう情報交換会を実施し、チャタムハウスルールのもと、大変活発な意見交換が行われました。

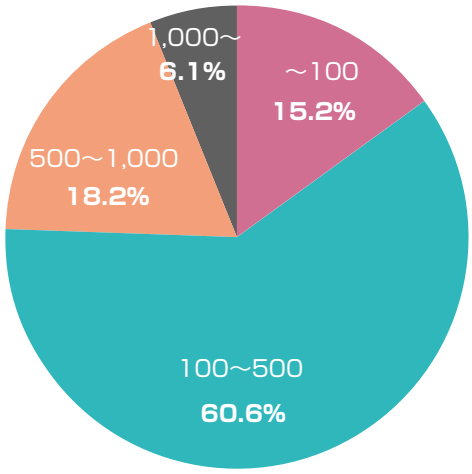
※：2016 年1 月　ドイツに拠点をおくセキュリティ製品の性能検証・比較検証を行う第三者機関「AV-TEST」にて評価

参加ユーザー様属性（33 社）

◇業種



◇規模



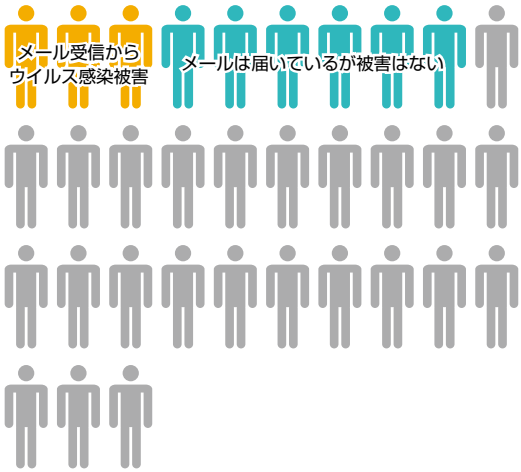
事前アンケートサマリー

Q：これまでに発生したセキュリティインシデント（ランサム感染について）

4 社に **1** 社がランサムウェア感染の被害経験あり

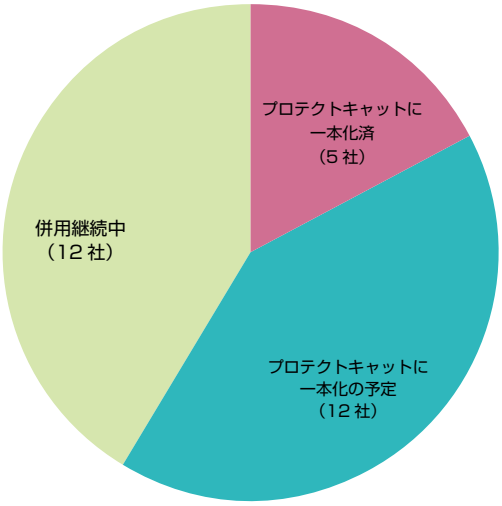
Q：これまでに発生したセキュリティインシデント（標的型攻撃メールについて）

11 社に **1** 社が標的型攻撃によるウイルス感染経験あり



Q：既存アンチウイルスソフトの運用について

6 割が「一本化」へ移行または検討 (NA=28)



Q：現在抱えているセキュリティ全般の課題

- 休眠 PC はパッチ適用されないため、リスクを抱えた状態で一時的に社内に接続される。**どこまでを対象に対策を施すか**、各社の判断基準を知りたい。
- **セキュリティ対策と利便性のバランス**のとり方
- **経営層の不理解への対応**（啓蒙）をどのように進めるべきなのか。
- 職員全体のセキュリティ意識の底上げ
- **製品ごとの操作方法**を覚えるのが大変
- **投資額の妥当性**をどのように判断するか。

チャタムハウスルール

会議の参加者に遵守が求められることがあるルールの一つ。チャタムハウスルールの下では、参加者は会議中に得た情報を外部で自由に引用・公開することができるが、その発言者を特定する情報は伏せなければならない。チャタムハウスルールには、会議参加者が自身の立場や役職に縛られることなく、自由な意見を述べることができる利点があるとされている。

サイバー脅威のトレンドと CylancePROTECT®の製品アップデート

Cylance Japan 株式会社 最高技術責任者　乙部 幸一朗氏

企業を狙ってくる脅威とその実態

CarbonView Research社が2017年5月に感染の実態や対応、製品選定等に関する調査（対象：米企業のセキュリティ担当者200名以上）によると、企業を狙った攻撃の数自体は増えているが、企業自体の対策が進んでおりマルウェア感染まで至らないケースも増えている一方、まだまだ被害にあう企業も多いようです。

次に、感染事象の実態としては、年間平均でおよそ4回発生。感染してしまった企業は決して対策を行っていなかった訳ではありません。90%がシグネチャベースの製品を利用、さらにその7割は設定及びシグネシャ更新を正しく行っていたことがわかっています。それでも被害が起こっており、43%がゼロデイマルウェアによる感染を経験しているということが分かっています。これまでの対策では脅威を防ぎきれないということです。

実際にマルウェアに感染すると、70%の確率でバックアップメージの再適用作業が必要となり、月平均でおよそ2台の感染PCをリストアしているという結果も出ています。

新たな脅威

攻撃側も常に進化しています。最近ではWannaCry、Petya、Bad　Rabbit…など色々なファミリーが出ており、さらに機能も拡充してきています。また、スピアフィッシングメール楽天、オリックスを語ったフィッシングメールなども増えて来ており、Zeusに続きアースニフなどの情報搾取型マルウェアでの感染が拡がっているのが最近の傾向です。

2017年5月に発生し、世界150カ国30万台以上に被害をもたらしたWannaCryは、感染をするとファイルを暗号化して、復元するためには金銭（ビットコイン）を要求するというもので、政府機関、病院、通信会社、自動車会社などで多くの被害を生むこととなりました。

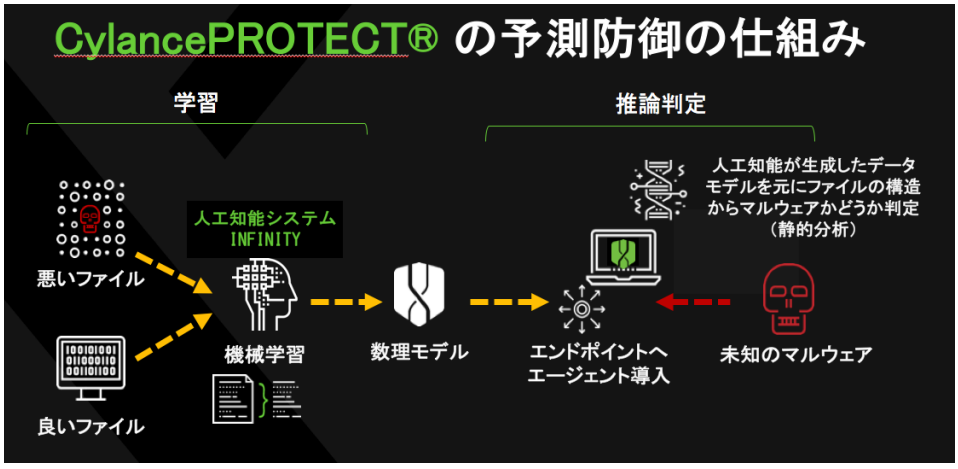
最近ではWannaCryの手法を真似た「Trickbot」は、2016年から金融機関を攻撃しており、先頃、英国と米国の多くの銀行を標的リストに追加したいう情報が出ています。Trickbotを使った攻撃は、件数こそ少ないものの、標的をピンポイントで狙うもので、同マルウェアは、国際的金融機関が送信したように偽装した電子メール経由で拡散し、その後、被害者を偽のログインページに誘導して、認証情報を盗むというものです。WannaCryが使っているEternalBlueというエクスプロイトを組み込んでワームのようなネットワーク拡散機能があることも確認されているので、日本でも注意が必要です。

なぜサイバーセキュリティに AI なのか

「Verizon DBIR 2015 & 2016」によると、サイバー攻撃のうち90%以上がマルウェアを活用されており、毎秒5件以上のマルウェアイベントが発生していると言われています。また、環境により異なりますが企業にやってくるマルウェアのうち70～90%がその組織にしか利用されてないユニークなもので、さらに、93%の攻撃においてシステムに侵入するまでに要した時間は1分以下という調査結果が出ています。

つまり、シグネシャ技術だけでは守ることはできず、今日の進化したマルウェアに対応するためには、よりスマートに対応できる新たな技術アプローチが必要ということなのです。

CylancePROTECT®は、ファイルのDNA（構造）をAIが学習し、構造から安全性を予測・判定するAIアンチウイルスです。その防御率は、既知・未知問わず99.7%を誇り、稼働実績はグローバルで1000万台以上です。



CylancePROTECT® の予測防御の仕組み

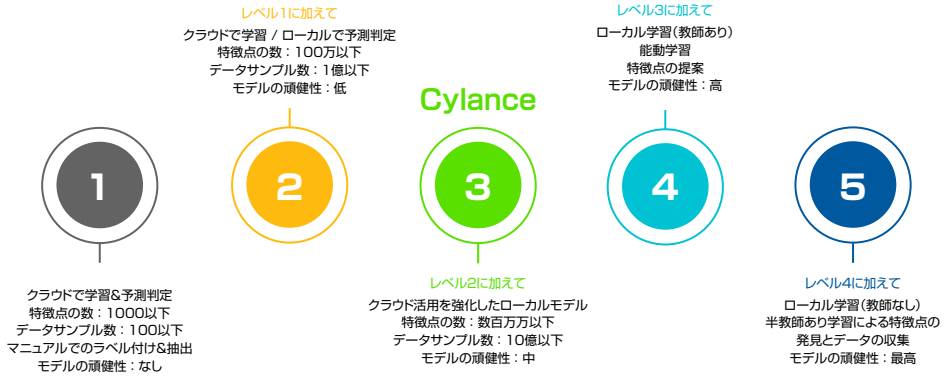
CylancePROTECT®は、人口知能システム（INFINITY）に10億個の良いファイルと悪いファイルを教師データとして学習させ、1ファイルから700万もの特徴点を抽出します。そして、そこから数理モデルを作成し、それをエンドポイントにエージェントとして導入することで、未知のマルウェアでも数理モデルを元にファイルの構造からマルウェアかどうかを判定します。バージョン1450から搭載している最新の第6世代データモデル（Dalek）では、検知率と

過検率の大幅な改善（40%以上）、スクリプトへの対応、新しいPackerなどへの対応（NSIS等）、新しいOSおよびファイルタイプへの対応（今後順次対応）を行なっています。また、来年年明けには新しいデータモデルを出す予定です。

AI だけでは不十分？

最近では、人工知能によるマルウェア防御だけでは不十分で、CylancePROTECT®はその機能が不足しているという指摘や、人工知能によるマルウェア防御は自社製品も対応していると公言する他のアンチウイルスベンダーも増えてきました。しかし、重要なのは機能の多さではなく「実際に脅威をブロックし、被害を防げるかどうか」ということです。従来のセキュリティ製品における機械学習の活用は、一部の作業を自動化・効率化するために使用していることが多く、検知技術についてはあくまでシグネシャがベースとなっているものがほとんどです。

ここにセキュリティ関連の研究や教育を行っている SANS Institute のInfoSec Reading Roomで2017年に公開されたNext-Generaiton Endpoint Security （次世代エンドポイントセキュリティ）製品テストの結果※1があります。
このテストでは、人工知能・機械学習対応を謳っている８つのメーカーの製品において、Sysinternals（Windowsプラットフォームで使うツール）とマルウェア、またそれらをパック化したものの検知力を比較したものです。結果は、下のグラフの通り、CylancePROTECT®亜種化されたものを含めマルウェアをほぼ検知できていますが、他社製品はそもそもマルウェアが検知できていないもの、また過検知をしているものもあります。そもそも、「AI対応」と謳っているセキュリティメーカーの95%は完全なマーケティングです。そして、残りの5%の企業もほとんどがレベル1に該当し、一部のメーカーはレベル2のアプローチを始めています。Cylance自身は現時点でレベル3と定義しており、このレベルに達してるのは我々だけです。ただし、私たちはここで終わらずに先のレベル5にむけて取り組んでいます。（各レベルの詳細は右上の図参照）

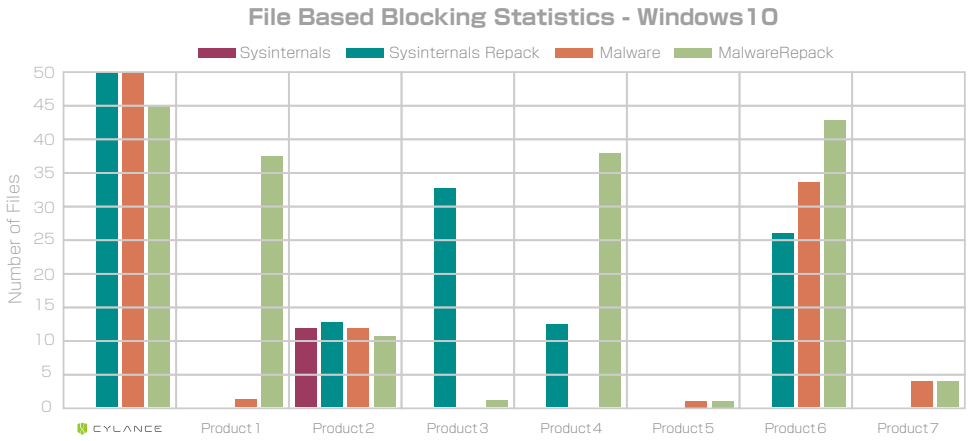


サイランスは誤検知が多い？

「サイランスは過検知・誤検知が多い」と言われることがありますが、実際のお客様環境において購入前評価（PoC）で確認していただいたデータ※2によると、過検知率は0.002%程度という結果が出ています。また先ほどの次世代エンドポイントセキュリティ製品テストの結果でも、Sysinternalsと呼ばれるWindowsの正規アプリケーションやツールは過検知していないことが分かります。
先ほどもご説明した通り、CylancePROTECT®では、教師データとして悪いファイルだけ出なく良いファイルも学習させているため、誤検知・過検知は少ないのです。

サイランスはマクロ型やファイルレスマルウェアに弱い？

これもよく言われることが多いのですが、これは事実ではありません。なぜなら、スクリプト型やマクロ型と呼ばれるマルウェアは99%がダウンローダーと呼ばれるもので、別のマルウェア本体(ペイロード)をダウンロードして実行しています。最近ではPowershellを使って動作するものが増えていますが、Cylanceはこの本体を他社よりも圧倒的に高い精度で検知します。
たしかに、スクリプト完結型のマルウェアも稀には存在しますが、これらに対してはスクリプト制御が有効です。例えば、Javascriptだけで書かれたランサムウェアなども過去に数件報告されていますが、これらはJavascriptからWSHを呼び出しています。
他社製品がスクリプト型やマクロ型に強い訳ではなく、どのようなファイル種別のマルウェアであろうが、他社のアンチウィルス製品では未知マルウェアを検知できないという事実は変わらないのです。
ここまでご紹介した通り、Cylanceはマルウェアの問題解決に対する全く新しい考え方を持っています。そして、それは世界中ですでに多くの企業に受け入れられており、成長率は前年比490%と急成長を遂げています。次から次に出現する新たな脅威に対して、「未知の脅威は防げない」という考え方が一般化してきていますが、Cylanceはこの現状を打破し再びアンチウイルスだけで安心できた時代を取り戻したいと考えているのです。



※1：レポートはこちらから入手できます。http://prevent.cylance.com/FydOzOOCzODOu2vzOOOMcz5

※2：エムオーテックスが実施した購入前検証（PoC）のサンプリングデータ

あすか製薬株式会社 様

業　　種：製造業
従業員数：連結 862 名（2017年3月現在）

ウイルス実行前後の操作ログを追跡し、サイバーレジリエンスを実現！

経営企画部システム課　IoT Manager 石川氏

あすか製薬株式会社は、1920年6月創立、医薬品、動物用医薬品、医薬部外品／食品および医療機器等の製造、販売、輸出入を事業とする3つのグループ会社で構成されており、内科・産婦人科・泌尿器科領域に注力する製薬会社である。
田町の本社をはじめ、川崎研究所、いわき工場、そのほか全国に20の営業所を持ち、全体で約1200台（デスクトップ50台、ラップトップ600台、モバイル500台）のPCを管理しています。

情報システムの現状

私は前職から、ウイルス対策全般やセキュリティゲートウェイの導入など、セキュリティ対策を専門としていました。サーバーシステムを担当するということであすか製薬株式会社に入社しましたが、PC担当メンバーの入れ替えや定年退職があり、現在はPCとサーバーを含むシステム全体を担当しています。また、現在はERP導入推進のための専門チームの形成も相まって、現場のシステム課は4人体制と非常に少ない状態です。
すでにPC対策、サーバー対策、ネットワーク対策、サンドボックス対策などバランス良く配置されていて、及第点のセキュリティ対策は実施できていました。ただし、四半期に一回程度は事故が起こってしまうのが現状で、より対策を強化すべきという課題は認識されていましたので、既存導入セキュリティ対策を精査するところからスタートしました。

導入の背景

その中で、エンドポイント対策の強化をすることになり、複数製品を検証。実は2016年の上期の時点で　プロテクトキャット導入の提案をしたのですが、価格面で却下されてしまいました。
しかし、その後2016年下期に、社員が英語のメールの添付ファイルを実行してしまったことが原因で、ランサムウェアの被害にあいました。
実行後すぐに社員から報告があったのですが、このランサムウェア「Locky」の場合、実行から3時間の潜伏期間があるため、実際に暗号化の動作が始まった時にはすでに遅く、止めることができなかったのです。
既存のウイルス対策によって検知はできていたのですが、原因となったアラームを見逃してしまい被害に繋がってしまいました。
さらに、その社員のPCは、ファイルサーバーへのアクセス可能な範囲が広かったがため、ファイルの暗号化の範囲も大きく、一部サーバーとファイルサーバーを前日時点まで戻すこととなり、脅迫の文面がPCにポツンと出たまま、復旧に数日を要するというかたちになってしまいました。
最終的に、想定で数千万円くらいの被害があったという計算になり、それがプロテクトキャット導入の後押しとなって、最初に躓いた価格の問題は簡単にクリアすることができました。加えて、担当部長がウイルス対策と操作ログ統合の有用性を大プッシュしてくれたこと、またPCのWindows10リプレースのタイミングもあり、資産管理ツールの見直しを絡める事ができ、最初はCylancePROTECT単体で検討していたのですが、結果的にはプロテクトキャット（LanScope　Cat）を導入することになりました。

検知率の高さ、使いやすい UI、操作ログとの連携が決め手

選定の決め手はなんといっても検知率の高さ。未知や亜種のウイルスも止められることが高評価でした。また、管理UIが使いやすいのもポイントです。複雑すぎると後任への引き継ぎが難しくなってきます。そこで簡単でシンプルで操作しやすいUIが必要でした。
そして、操作ログとウイルス検知ログの連携により、ウイルス実行前後の操作ログが確認できるという点です。ウイルスをブロックするだけでなく、なぜ流入したのかを特定できることで初めて再発防止の対策を打つことが可能となります。私は「簡易レジリエンス」という位置づけで捉えていますが、非常に費用対効果が高いと感じました。また、管理サーバーがクラウド上にあるので、グループ会社の管理が統合できます。以上4つの理由で、導入を決めました。

導入の効果

プロテクトキャット導入後は、大きな問題は発生していません。ただ、管理PCのWindows10への移行がまだ十分にできておらず、現状は60%くらいの配布率です。配布率が100%になって効果を十分に発揮できるのが楽しみです。

株式会社洸陽電機 様

業　　種：エネルギー . 電力・電気
従業員数：連結 159 名（2017年９月現在）

AIがアルゴリズムで脅威を判断する新技術を取り入れ、変化に対応するだけではなく、変化をリードする

洸陽電機は「未来の子供のために、より良い地球環境を残します。」を経営理念とし、未来のエネルギーいわゆる再生可能エネルギー、クリーンエネルギーを扱う水力発電、太陽光発電、バイオマス発電といった発電の事業を行っている。また、新電力の事業者として電力の公認や節電のソリューションも提供し、未来のエネルギーのかたちを創造し、安価で持続的なクリーンエネルギーを賢く使う社会の実現を目指しています。

General Energy System
Genesys
洸陽電機

導入の背景

「働き方改革」推進の一貫で、生産性の向上に全社で取り組んでおり、また、新電力事業において自給の予測を行うために、ワトソンやMyAnalyticsを業務に取り入れる検討をしていましたので、背景として人工知能やAIの活用に非常に興味を持っていました。
そんな中非常に恥ずかしいことですが、2016年に標的型メール、ランサムウェア「Locky」の被害にあっていたこともあり、人的ミスへの対応をどのように行うか、ということを課題にあげていました。
また会社として、「変化に対応するだけではなく、変化をリードする」という方針がありますので、IT業界の最新の技術を業務に取り入れ、効率化に繋げることはできないかと考えていました。

生産性の向上と未知の脅威への対応を同時に実現

決め手は、パターンファイルや振る舞い検知では無く、AIがアルゴリズムで脅威を判定する、という他社製品とは異なる特長です。
また、課題であった人的ミスについては、人的ミスは防ぎきれないという考え方の元、万が一人的ミスがあったとしても、被害を最小にするか、もしくは起こさないかを考えて選定していました。
会社では、既にアンチウイルス製品を導入していたのですが、PCの動作が重くなること、最新のパターンファイルを適用するのにインターネット環境が必要である点を改善したいと思っていました。弊社では、発電所などをつくるにあたって、山の中などに通信環境の悪い場所に1年単位で作業に行く社員もいます。メンテナンスが行き届いていないパソコンでも軽く、さらにオフラインの環境でいかに動作させるかが選定の大きなポイントでした。

導入の効果

実は、導入後に標的型メールの添付ファイルを開いてしまった社員も何人かいましたが、問題なく隔離できていました。
管理側の視点としては、日々のメンテナンス、パターンファイルの更新やクライアントへの適用を意識する必要が無いところが嬉しいです。
ホワイトリストの登録も、POCでの準備期間を長く取っていたこともあり、その期間でホワイトリストへの登録ができたので、現状はほとんど登録の必要がありません。社内で作るアプリケーションのようなイレギュラーのもののみ、必要に応じて日々登録している状況です。この作業により、業務影響なく自動的に悪意を持ったプログラムのみが隔離されるので、利便性を損なわずにセキュリティが高められていると実感しています。

また、以前のアンチウイルスソフトに比べてPCの動作が軽いことで、社内からの評判も非常に良いです。以前のアンチウイルス製品では端末に負荷がかかる毎日のウィルススキャン必要でしたが、プロテクトキャットに一本化することで、それが必要なくなったのです。
管理側も日々の運用や保守の手間が大きく削減され、またユーザー側はPC動作環境が改善できました。この二つの効果は、もともとプロテクトキャットを検討していた時点では期待していなかったのですが、実際に導入して運用してみて、初めて分かった嬉しい効果です。

今後の取り組み

プロテクトキャットそのものの機能というより、UIに気になる部分があります。一つは、全体的に日本語のローカライズが甘く、ホワイトリストや隔離リストの備考に2バイト文字で登録すると文字化けしてしまう現象です。実際に各リストを登録した後に、「これなんだっけ？」となることも多いので、社内でルールを作って文言を入れて工夫しているのですが、是非改善してほしい点です。
管理側の視点からですと、ホワイトリストや隔離リストをメンテナンスするにあたり、どこで何のメンテナンスを行うことができるのかが分かりにくいなと感じる部分があります。また、現状は、隔離したことは分かっても、何を隔離したのかが分からないので、ユーザー側に表示される通知内容や表示内容をカスタマイズできるようにできれば良いなと思っています。

社会福祉法人 静岡市社会福祉協議会 様

業　　種：医療・福祉
従業員数：1,155 名（平成 29 年 11 月現在）

二度のウイルス感染から見えてきたこと、プロテクトキャットは「最後の砦」

総務部　部長　朝比奈氏

静岡市社会福祉協議会は、地域福祉の推進を目的として社会福祉法に基づき設立された。歴史としては、戦後まもなくに発足した社会福祉法人であるが、行政合併により設立は平成15年4月1日と登記されている。地域で生活する住民と地域にある住民組織、ボランティア団体、社会福祉施設などの関係者と協力して、誰もが安心して暮らすことのできる「福祉のまちづくり」を目指している。民間の社会福祉法人として、様々な福祉問題への取り組みや、介護保険事業など、地域に根差した活動を続けている。

情報システムの現状

以前はＩＴに精通した職員の力量に頼っていたため、結果として属人化した管理になっていましたが、組織化すべきということで、平成27年に情報システム委員会を設置しました。委員会は各部門から選出したメンバーで構成され、法人内全体のシステムの管理やハード面／ソフト面について協議を行いながら運営しています。

導入の背景

実は、平成28年に二度のウイルス感染が発生しました。一度目は8月にスパムメールのZipファイルを開けたことでウイルスに感染。ウイルスは亜種であったために当時利用していた既存アンチウイルスソフトでは検知することはできず、ネットワーク監視を委託している運用会社から「不正な通信が行われている」という連絡をもらい発覚しました。その際は、ログを解析してウイルスを発見し手動で削除するという対応を行いました。

この一件があり、社内にはフリーメールの利用やスパムメールについて注意喚起を行いましたが、残念ながら10月に職員宛て届いたスパムメールのZipファイルを開封したことで再びウイルス感染が発生。こちらも亜種であったために、既存の製品では検知することができませんでした。
幸いにして情報流出などの被害は認められませんでしたが、この二度の感染を受けて、改めて職員のモラルの重要性と、何らかのシステムで対策をしていくことが必要だということを痛感しました。特に、亜種ウイルスにどのように対応していけばいいのかが大きな課題でした。

そんな中、Cylanceのセミナーに参加する機会がありました。そのセミナーでは、「自社で感染したウイルスを検体として持ってきて来てください」とのことだったので、保存していた亜種ウイルスを持ち込むことにしました。すると、Cylanceではすぐに検知。検知率の高さ、また亜種ウイルスにも対応していることから導入を検討することになりました。

決め手は資産管理機能との連携

当時は別の資産管理ソフトを導入していましたが、ウイルス対策と資産管理ソフトが連携することで、効果的な運用ができるのではないかということで、資産管理機能を有するプロテクトキャット（LanScope　Cat）を導入することに決めました。

導入の効果

8月にプロテクトキャットを導入してまだ間もないのですが、すでに効果はかなり出ていると感じます。
まずは、既存製品から置き換えたことで、いままで使用していたアンチウイルスソフトでは検知されなかったウイルスを検知することができたことです。これには情報システム担当者たちも非常に驚いていました。
また、業務では様々なソフトやシステムを利用していますが、利用実態までは把握することができていませんでした。しかし、LanScope Catの資産管理機能（アプリ稼働管理）を活用することで、これまで見えていなかったそれらの利用実態を見える化することができました。これは導入前に想定していませんでしたが、今は大きな効果だと実感しています。

今後の課題

情報管理に対する職員の意識には、特有の組織風土等により、まだ「緩さ・甘さ」があると認識しています。急速に変化する環境に対して、どのように向き合っていけばいいのかは常に課題です。
特に、事業外のことに対してはどうしても消極的な面がありますが、情報システムとしては「積極的な防衛が必要」だと考え、今回プロテクトキャットを導入することを決めました。
プロテクトキャットを導入し、最後の砦を構築することができたことで、より本業に対して新たな向き合い方ができてきているのではないかと感じています。ただし、プロテクトキャットの安心感を誤った形で捉えている職員がいることもわかってきたので、その誤解が新たなリスクともならないよう、そこは慎重に対応していきたいと考えています。

株式会社エスケイエム 様

業　　種：サービス業
従業員数：900 名（2017 年 12 月現在）

毎日Webコンソールで検知状況を確認、検知した場合はすぐに原因を特定！

経営管理部　IT企画推進室　鈴木氏

豊田自動織機グループの株式会社エスケイエムは、建物のトータルマネジメントという視点で、顧客の生産性を高める環境づくりと資産価値の管理・保全に貢献しています。清掃・設備メンテナンス・施設警備を主とした建物管理業務を中心に、不動産管理・仲介、建築・営繕にいたるまで高品質なサービスをご提供し、信頼いただけるパートナーを目指しています。

情報システムの現状

現在IT部門は4名体制で、システム導入／運用・管理、クライアントPCやネットワークのセキュリティ管理など、社内IT全般を一手に担っています。

導入の経緯と決め手

当時、既存アンチウイルスソフトを利用していましたが、昨今のセキュリティ事情を鑑みてこれだけではウイルス感染をおさえることはできないと考え、プロテクトキャット含めた数製品の検討を始めることにしました。

まず性能面については、3つの観点で次世代型アンチウイルス製品の比較を行いました（標的型攻撃メールの対策、ランサムウェアの対策、未知の脅威対策）。この点についてはどの製品も申し分なく、それぞれの強みがありました。

次に費用面について、CylancePROTECT®はクラウド製品ということで、年間ライセンスのみだったのに対し、他社製品はオンプレミスだったので、ライセンス費用以外にサーバーなどのハード調達、保守費用が必要だったため高いという印象でした。

導入の容易さについては、こちらもクラウド製品であるCylancePROTECT®はエージェント展開のみのため、短期での導入が可能でした。他社製品はサーバーの調達・構築などを含めると数か月かかるものもありました。

ここまでですでにCylancePROTECT®が第一候補となっていたのですが、これらの点に加え導入の決め手になったのが、LanScope　Catとの連携でした。すでにLanScope　Catを導入していたので、使いなれたWebコンソールでまとめて管理・運用できること、また、LanScope　Catのログで原因追跡が容易にできることが非常に魅力的だったため、プロテクトキャット（CylancePROTECT®）を導入することに決めました。

導入検証（POC）の実施

導入が決まった後は、MOTEXさんとCylanceさんに協力いただき、操作説明を受けたうえで、エージェント展開を行いました。最初は「自動隔離モード」にはせず、各PCの検知結果の確認し、怪しいものかどうかを随時判断し手動で隔離していく運用を行いました。
すべてのPCでスキャンが完了した後は、「自動隔離モード」に切り替え、現在もこれで運用していますが、特に業務に影響が出ていることはありません。

導入の効果

日々の運用はLanScope CatのWebコンソールで検知結果を確認し、検知した場合はログ解析を行い、どこから流入したのかを調べています。
流入経路がわかると・・・例えばWebダウンロードが原因であれば、LanScope　CatのWebアクセス管理機能で制御をおこなったり、ファイアウォール側での制御を実施するなどの対策を行なっています。流入を止めるだけでなく、原因まですぐに特定できるところが良いですね。
効果は大きく、おかげで検知事例も最近は皆無です。また同時に、全社に対してこういった検知があったということを共有し、再発防止のための教育・啓発を実施し周知徹底を図っています。

今後の取り組み

現在、PCインフラの集中化を目的に、シンクライアント化を進めています。各PCを本社に一括集中し、管理しやすい体制にすることで、OSなどを常に最新の状態に保てる環境を作る予定です。また、アライドテレシス社製のSDNも導入していますが、こちらもLanScope Catと連携ができるので、不正なアクセスがあった場合には自動で遮断するといったことが実現できています。
こういったものを活用しながら、トータルでセキュリティリスクの低減化を図っていきたいと考えています。

情報交換会

Information Share Meeting

Q. プロテクトキャット導入のきっかけはなんですか?

・既存アンチウイルスソフトをインストールしていましたが、ランサムウェアに感染してしまいました。事故があったため、稟議が通りやすかったです。

・事故があったので即決でした。社内の役員会で標的型攻撃のサンプルを見せて「このメール、開かない自信ありますか?」という風に見せることで承認を得ることができました。

・既存アンチウイルスソフトをインストールしていましたが、不安がありました。本当に何も感染していないかどうかを確認したかったこともあり、POCを実施してプロテクトキャットを運用してみると、怪しいマルウェアが見つかりました。その結果があったことで稟議はすんなり通りました。

・親会社のセキュリティポリシー上、親会社指定の既存アンチウイルスソフトを導入しないといけないのですが、何度かウイルス感染をしてしまったことがあり、それだけでは防ぎきれないと思い、プロテクトキャットの導入を決めました。現在は、既存アンチウイルスと同居させています。

・既存アンチウイルスソフトをインストールしていましたが、ランサム被害にあい、他にもっと良い製品が無いかを検討している中で、Cylanceを知りました。検知性能や負荷が軽いことが決め手となり、導入に至りました。

・セキュリティ事業をやっているので、何かあったときのことを考えると費用よりも穴をうめる方を優先しました。また、すでに導入していたLanScope Catのログと連携できることが強みであることをアピールした結果、承認を得ることができました。

・既存アンチウイルスソフトは2年で4,000円/台でしたが、セキュリティ事故が起って業務をとめた場合、どれだけの損害があるかを算出し説得しました。

Q. POCの結果、また現在はどのような運用をしていますか?

・100台でPOCを実施しました。初期で検知した数はそんなに多くなかったですね。今は毎日90個程度検知しています。その中で登録が必要なものは多くて2個程度、時間にして数分程度の作業です。
メモリ保護の推奨設定も行っています。Unix環境をWindowsで動かすソフトが必ず検知されるので、パスの一部を例外登録する運用をしています。スクリプトは本当はやりたいけど全部警告が出るので今はやってないですね。

・POCで予想以上のアドウェアを検出したことに驚きました。ひっかかったものはユーザーに削除依頼をしました。他には、TrustedLocalはセーフリストに追加しました。うちは設計を行うような部署もあり、インストーラがよく引っかかっているので、この辺りは注意しながら運用しています。

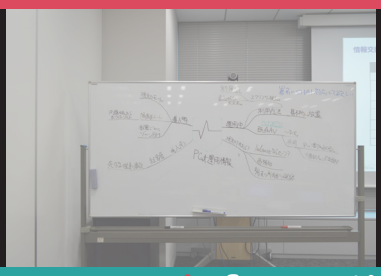
・アドウェアを検知するので検知数は既存AVと比較すると結構多いなという印象です。

・現在は既存アンチウイルスソフトとプロテクトキャットを併用しています。脅威ファイルが別の端末に入っていないかを確認する為に、Cylanceが発見した脅威ファイルを他のアンチウイルスメーカーに調査依頼し、既存アンチウイルスソフトのシグネチャに反映してもらっています。「Cylanceで検知しました」というと対応が早いです。笑

・運用開始して1年ぐらい経つが、自社内で検知されると困る内製のソフトがあるため、過検知が低いとはいえまだ検知モードで運用しています。
開発途中のファイル、特に署名が無ければ検知されることがあるので、何処かで思い切って切り替えるのもありかと検討しているところです。

・業務上ゲームをPCにいれることもあるが、Cylanceはカテゴリとしてゲームも検知するので、デジタル署名を登録して回避するようにしました。ホワイトリストにも入れたいが、SHA256だけでSHA1に対応してないので、対応してもらえるよう要望を出しています。

・自社でインストールを制限していないところもあるので、フリーソフトが結構な数が検知されてしまい管理が大変でしたが、ログを活用すると調査に役立つので助かってます。



Q. プロテクトキャット以外の外部脅威対策を行なっていますか?

・ゲートウェイ製品を中心に、次世代ファイアウォール、UTM、メールフィルター、など多数導入しています。

・エンドポイント製品をしっかり固めていれば、他は不要と考えています。費用対効果に見合うものがあれば検討したいですが。

・ネットワークUTMサービスを利用。そこでWebのウィルスチェック、アクセス制御を実施しています。またSDNコントローラを使っており、LanScope Catとの連携設定を実施しています。

・ゲートウェイ製品や既存アンチウイルスソフトの保守が切れるタイミングで、プロテクトキャットに一本化しました。ユーザーからは「ヤマト運輸などを偽装したメールを開きそうになった」という話をよく聞きますが、その都度社内ポータル掲示板で情報共有として「こんなメールが来てるので注意してください」と注意喚起しています。

・既存アンチウイルスソフトとプロテクトキャットを併用していますが、先に発見できるのはプロテクトキャットであって、既存アンチウイルスソフトではないので意味がなくなってきてると感じます。Windows Defenderに変更し、プロテクトキャットで発見された脅威ファイルをMicrosoftに提供し、反映してもらうという運用でいいと考えています。

・感染があったこともあり、経営陣の意識が変わり、セキュリティに投資しなさいという状況に変化しました。

・閉鎖網とWebフィルタリングを利用。業務上、使ってもいいものもあるため、期間を定めて開放したりしている状態です。

・入り口対策としてインターネット閲覧を外部委託しています。他には、メールサーバー、プロキシサーバー、次世代ファイアウォールという構成をとっています。また添付ファイルが暗号化されてるかどうかチェックするため、専任チェック者を1名設けています。
内部対策はまだあまりできていませんが、ファイルアップロードは使えないようにしています。出口対策はWebフィルタリングを利用しているが、こちらはほぼ見れていません。

・営業など外勤メンバーにはDaaSがよいのではないかと検討しています。もともとは暗号化製品を使っていましたが、Windows10のアップデートに追いつかないため、Windows BitLockerに変えました。しかし、ユーザーで有効・無効の操作ができてしまうため、ツールを使ってコントロールしています。

・入り口対策はUTMです。週次でアラートをだしてくれ、安価ですがいい性能で満足しています。他にはインターネット分離、内部漏えいはファイル暗号化ツールで対策しています。

・DaaSを使っています。パスワードを間違えたら消去する運用です。

・データセンターを経由してインターネットに出るようにしています。(閉域網) 他には、Webフィルタリングで制御しています。

・工場は分かれていますが、閉域網を使っています。メールは社外送信は全て暗号化しています。BCP対策も必要だと考え、何かあっても北海道にとっているデータからすぐに戻せるようにしています。

Q. セキュリティ全般の課題はなんですか?

・Pマークを取得しており、従業員教育を定期的に実施。標的型メール訓練もしていますが、それでも開いてしまう人がいます。

・権限のある責任者に対してセキュリティの報告や、そもそも関心があまりない上層部に対してどう興味を持ってもらうかが課題です。

・セキュリティ教育をした直後にインシデントが発生したこともあるので、監査のための教育になっており、実態が追いついていません。MOTEXさんからセキュリティの本をもらったので、これを使ってみたいと思います。

・eラーニングを実施しているがやってくれないこともある。漫画やクイズ、脱出ゲームなどでやるなど工夫していますが、年配の方が多いとeラーニングを2択だけにしても80点いかないこともあります。

・空気感も大事だと思ってます。セキュリティをやっている空気があるとみんなやってくれたりします。そういう意味では物理的な対策も重要ですが、社員のセキュリティモラルをいかにあげていくかが課題です。

・取引先のガイドラインが厳しいところもあります。ガイドラインが追加されるとそこに合わせていかないといけないので、大変です。

MOTEX
Secure Productivity
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：052-253-7364
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

2 版：2018 年 2 月発行