

## LanScope Cat Ver.9 新製品発表



PC・モバイルの一元管理とプロテクトキャットの登場で、エンドポイントを守るための対策はLanScope一つで実現する。Ver.9では、さらにその流れが加速。内部不正対策・外部脅威対策・働き方改革対策の機能強化を実施した。このVer.9にはお客様の声から生まれた機能も多く、その背景にはユーザー様で構成されているコミュニティである「LanScopeコンソーシアム」での意見も、より運用しやすい製品づくりに繋がった。今後も良い製品を送り出せるよう取り組みたいと思っている。

エムオーテックス株式会社 代表取締役副社長  
宮崎 吉朗



IT資産管理から始まったLanScope Catは、操作ログの取得により内部漏えい対策に効果があることを提案し続け、2016年には外部脅威対策も実現した。このLanScope Catの、エンドポイントで情報取得し制御できる「統合型エンドポイントマネジメント」を新たにメッセージしていく。そして今回、Ver.9で実現する価値を3つのポイントで紹介する。

- 1：内部不正対策
- 2：外部脅威対策
- 3：働き方改革対策

内部不正対策では、問題を「点」ではなく「線」で捉える新たな運用を可能にしている。単一のログで問題行動を捉えるのではなく、複数の行動を組み合わせるアラーム判定を行えるカスタムアラームを搭載した。日々のセキュリティチェックを実現可能とする、お客様と共に運用を考えた機能である。また、漏えい経路No.1である紙による漏えい対策として、印刷イメージ取得を新オプションとして搭載した。

外部脅威対策では、次世代FWで検出したインシデントの原因特定をLanScope Catで容易に行える仕組みを設けた。次世代FWのアラートで得られたIPアドレスとポート番号を元に、端末特定し、新機能のアプリ通信ログで問題の実行ファイルがわかるようになった。前後のログから端末使用者の行動が追うことができるので、専門知識を必要とせずにインシデントの原因特定が手軽にできるようになる。

働き方改革への対策としては、残業時間の抑制として端末の電源を強制的に落とす電源管理機能を強化した。制御前には端末使用者にメッセージを表示することも可能になり、会社の意図を伝え、従業員の意識を変える一助になれば幸いだ。

これからも、エンドポイントでログを取得し制御するLanScopeCatの強みを高めていく。

エムオーテックス株式会社 プロダクトマネージャ  
北村 和久

## LanScope 最新ロードマップ

**LanScope Cat Ver.9.0**  
**2017年12月13日リリース!**

- 新機能 1 カスタムアラーム機能
- 新機能 2 不審なプロセスを発見「アプリ通信ログ」
- 新機能 3 リアルタイムにすべてのログを一括確認
- 新機能 4 SIEM製品など、外部ツールとの連携
- 新機能 5 印刷内容をすべて保存「プリントイメージ」
- 新機能 6 検知/隔離したマルウェアの傾向を分析
- 新機能 7 電源管理強化で残業時間抑制

<https://www.lanscope.jp/cat/>

## 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:03-5460-1371 受付時間 9:00-18:00 (月~金曜日 祝祭日除く)  
 E-mail: sales@motex.co.jp  
 URL: www.motex.co.jp



# MOTEX DAYS 2017

LanScope Cat 最新バージョン発表 / 新種のマルウェア検知デモンストレーション

## 開催報告

2017年11月20日(月)~12月6日(水)  
東京/大阪/福岡/名古屋/金沢



## 多くのお客様に会場いただき、盛況のうちに無事終了しました



### 基調講演

AIのサイバーセキュリティへの応用、その未来

Cylance Japan株式会社  
最高技術責任者  
乙部 幸一朗 氏

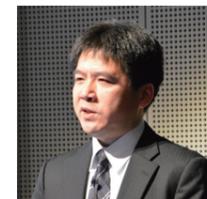


### LanScope Cat Ver.9 新製品発表

エムオーテックス株式会社  
代表取締役副社長  
宮崎 吉朗



エムオーテックス株式会社  
プロダクトマネージャ  
北村 和久



### 外部脅威セッション

セキュリティのプロだから語れる。  
「Cylance・プロテクトキャット」その凄まじさ!

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 様

今年の「MOTEX Days 2017」は導入ユーザー様、ご検討中のお客様ならびにパートナー様を対象に、東京(11/20)を皮切りに、大阪(11/22)、福岡(12/4)、名古屋(12/5)、金沢(12/6)のキャラバンを実施しました。今年度は基調講演として、Cylance Japan株式会社 最高技術責任者 乙部幸一朗 氏を迎え、AIアンチウイルスに関してご講演頂くとともに、各テーマごとの事例発表やLanScope Cat Ver.9のリリース内容をお伝えしました。

また、導入ユーザー様の事例セッションとして九電ビジネスソリューションズ株式会社 堂領輝昌様をお招きし「外部脅威」に関しての具体的な事例をご講演いただきました。

今年は例年にも増して、導入ユーザー様及びご検討中のお客様に多数ご来場いただきました。過去最多のご来場数を記録し、大盛況のうちに閉会しました。



## ご挨拶



「MOTEX Days 2017」は、弊社 河之口より、ご来場された皆様への御礼と挨拶から始まった。（以下引用）  
私たちのビジョンは「Secure Productivity（安全と生産性の追求）」です。市場ではサイバー脅威の拡がりに対抗するために多層防御が進んでいますが、その運用性、利便性の低下が大きな課題となっています。LanScopeCatは1996年の発売以来、IT資産管理から始まり、内部不正対策の分野で多くのお客様にご導入を頂いてまいりました。そして昨年、外部脅威対策の機能を加え、「統合型エンドポイントマネジメント」へ自らのポジションを再定義しました。そして、この取り組みは、メーカーの一時的な製品開発だけでなく、お客様とお客様、また、パートナー様とのコミュニティ作りをコアに据えた活動が必要と考えています。MOTEXは統合型エンドポイントマネジメントで安全性を高めると同時に、コスト及びリソースを劇的に削減し、本来企業が集中すべき事業活動に専念できるための環境の創造を目指します。

エムオーテックス株式会社 代表取締役社長  
河之口 達也

## TOPICS 1

### 基調講演『AIのサイバーセキュリティへの応用、その未来』

Cylance Japan株式会社 最高技術責任者  
乙部 幸一朗 氏



#### 世界に存在する事象のすべてはそれぞれ1つの数式で理解できる

ある映画の一節を例にとりあげ、世の中の人工物・自然物は数値（数式）で表現することができる。と数学的な話で始まった乙部氏の講演。乙部氏によれば数式の良いところは、その数式さえ導き出せば結果の予測ができる点だという。例えば我々は $1+1=2$ という文字を丸暗記している訳ではない。加算の数式（ルール）を理解しているが故、どんな数字がきても解けるだろう。Cylanceは、この数式の「未知の入力に対して予測ができる」という点を応用し、マルウェアに対して予測検知を行うという新たなアプローチを行っている。

Cylanceはファイルの構造を人工知能に学習させており、その学習の過程でマルウェアの特徴点から数式を導きだす。ここで作られた数式を元にスコアリングし、スコアで正常なファイルか悪意あるファイルかで判断する。検知率は99.7%と非常に高く、かつ「予測検知率」であり、他メーカーの手法（パターンマッチング方式）とは一線を画す。明日、1か月後、1年後にでてくるものも99.7%止めるのがCylanceだ。

その検知率の高さは仕組みにある。Cylanceは人工知能システム「インフィニティ」に大量のファイルを覚えさせる。その数約10億個、そのファイルデータの特徴を学習することで、数理モデル（数式の集合体）を掃出し、それを使ってエンドポイントで判定するという仕組みだ。一般的に学習するには時間がかかる。例えば、人間でも幼少期は犬猫の判断すらつかないが、大人になるまでに多くの犬を見て学習することで、大人は瞬時に犬かどうかを答える事が可能である。この様に、学習には時間がかかるが、その判定は瞬時に行える。Cylanceがマルウェア検知技術にAIを活用した理由は4点だ。既存の技術はブラックリスト検知が主流だがゼロデイに対応できないため、予測検知が必要だった点。扱うデータ量が非常に多く、リアルタイム性を鑑みると人の手で対応することが難しい点。慢性的に人材不足であり、自動化の必要性がある点。そして何よりもサイバーセキュリティ空間には機械学習のレベルを決める多くのデータが存在している点である。

#### WannaCryは1年半前のモデルで検知に成功

実際に予測検知の実証として、2017年春に猛威を振るった「WannaCry」が挙げられる。Windowsの脆弱性を突いて感染を広げるワーム型だが、アンチウイルスベンダーは感染発覚後パターンファイル配信を開始、亜種化ごとにパターンファイルを順次作るという対応をしているが、それに対しCylanceはすでに1年半前の数理モデルで予測検知に成功している。10年ほど前まではパターンファイルでも十分にマルウェアを止める事ができていたが、すり抜けるものが増えてきたため現在、様々な技術（ふるまい型・サンドボックス）=実行後の動的解析が登場している。Cylanceはそれらとは異なり、元来のファイルを実行前に止めるという静的解析（予測型検知）にフォーカスした製品である。

今やAIは自動運転技術などでより私達の身近な存在となりつつある。近い将来、犯罪者側でもAIを用いて攻撃してくる事も想定される。AIに対抗できるのはAIでしかなく、サイバーセキュリティにおけるAIはもはや必須である。



## TOPICS 2

### 【外部脅威セッション】セキュリティのプロだから語れる。『Cylance・プロテクトキャット』その凄まじさ！

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 様

#### 従来製品を超越する、歴史的かつ革命的な製品

セミナー後半の『外部脅威セッション』では、九電ビジネスソリューションズ株式会社の堂領 輝昌様にご講演をいただいた。

ご自身の警察組織におけるサイバー犯罪対策等のご経歴や現在の業務経験を踏まえつつ、最新のクライアント導入型ウイルス対策ソフトが切り拓いた「新たな常識」を説く。「セキュリティ技術者は公平中正であるべきとの信念を越えてまで、お伝えしたい製品があります。既存の製品群のレベルをはるかに上回る革命的な製品が出ておりますので、強く推薦を差し上げたいと考え、この場に立たせていただきました。」と切り出し、まず結論から話し出した。

「今回お伝えする『Cylance・プロテクトキャット』は、セキュリティ業界の歴史上、いや、人類の歴史上における最強のウイルス駆除製品です。半世紀にひとつ出るか出ないかという凄まじいウイルス駆除能力を誇る製品であり、私の20年間に及びセキュリティ対策業務においても、このような製品には出会ったことがありません。誰もが今すぐに導入を検討しなければならない製品といえます。究極の製品をご紹介できる機会に感謝します。」と、本製品の圧倒的なウイルス駆除能力を力強く宣言した。



#### なぜ驚異的なウイルス駆除能力を誇るのか

『Cylance・プロテクトキャット』の持つウイルス駆除能力については、前述の乙部氏同様、ご自身が自ら実施した検証結果を公表した。その内容は、未知のものを含む540種類の実際のウイルスを用いた駆除率が99.8パーセントに達したという驚くべきデータであった。「自身で検証を行うことで、公称値の99.7パーセントが間違いのない数字であることを客観的に証明しました。これまでの常識では考えられないウイルスの駆除率です。セキュリティ業界の歴史を塗り替える、最強の製品が出現した事実を確認した瞬間でした。」

そして、なぜ歴史上において最強なのかを、分かりやすさを優先させながら説明した。「過去に出現した数億というあらゆるウイルスの特徴を、数理モデルを駆使した人工知能が精密に分析し、データベース的な要素として持つためです。侵入したウイルスは人工知能が速やかに判定し、即座に駆除します。この方式の強みは、ウイルスのプログラムを改変した亜種や変異型に対して圧倒的な駆除能力を誇ること。世の中に流通するウイルスは、その大部分が亜種や変異型です。従来型の製品は亜種や変異型にきわめて無力でしたが、『Cylance・プロテクトキャット』はあらゆる亜種や変異型を見つけ出せるという、従来製品とは真逆の特性を持っています。つまり完全新作のウイルスでないかぎり、ほぼ全てを駆除できるということ。これこそが凄まじいウイルス駆除能力の秘密なのです。」と、その優れた設計理念について力説した。

気になる競合製品に関する言及も忘れない。「人工知能を用いたウイルス検出については他社も猛追を図るでしょうが、本製品はウイルスの特徴抽出に関する特許を数多く取得済みです。その優位性は続くでしょう。」「世の中の“人工知能を搭載”とする製品の大部分は、本製品の足元にも及ばないレベルにあります。いわゆる“人工無能”です。売り手の宣伝に踊らされずに製品を自ら“目利き”することが大切。ぜひ本製品と比較検証されてください。」

#### 今こそ本気で、組織における最良の製品選択を

さらに、本製品の強みとして、制御系や基幹系システムにおける導入例を挙げた。インターネットへの接続を不要としながら高いウイルス駆除能力を維持する特性が制御系などに最適であること、データダイオードと『プロテクトキャット』を組み合わせることで、制御系内のウイルス検知を制御系の外部に対して安全にメール通知できる点などをピックアップ。「今こそ本気で、組織における最良の製品を選びましょう。近い将来に必ず“あ”のときに決断しておいて良かった”と思える時が来ます。」「やがて攻撃者側が人工知能を駆使して、人々を翻弄する時代が来ます。人工知能に対抗できるのは人工知能だけです。混乱の時代が来る前に、必ず対策を実施してください。」「ウイルス対策ソフトが無効とされた時代は終わりを告げました。『Cylance・プロテクトキャット』が現れた今、過去の常識は完全に覆ったのです。」

最後に、ご自身が大好きであるというミュージカル『キャッツ』を引き合いに出し、「キャッツでは、深夜に集う猫たちが名乗りをあげ、選ばれし一匹の猫を見つけるというストーリーが展開します。今、皆さま方の目の前には『プロテクトキャット』という、まさに猫の名前を冠した選ばれし製品があるので、ぜひ、今こそ『最も優れた猫』に手を伸ばして、自らの組織に安全と安心を導いてください。本日はありがとうございました。」とユーモアを交えながら締めくくった。