



# Unbelievable Tour in Japan

未知の脅威は防げない。その概念を覆す瞬間をあなたは目撃する!!

Unbelievable Tour in Japan 開催レポート



本日は Unbelievable Tour in Japan にお越し頂きまことにありがとうございます。Unbelievable Tour は「本当に信じられない！」という言葉そのままタイトルにしたイベントです。これまでに全米 75 拠点で開催をしてきましたが、今回アジア初開催、そして全米を含めて最大規模での開催となります。是非最後までお楽しみください。

Cylance Japan 株式会社 代表取締役社長 金城 盛弘 氏



MOTEXはこれまで、IT資産管理・操作ログ管理といった機能で、内部脅威に対する対策ソリューションを提供してきました。しかし今回Cylanceの技術と出会ったことで、従来の機能に加えて外部脅威の検知から原因追跡までをトータルソリューションとして提供できるようになりました。CylanceのAIを使った革新的なアプローチにより、本日はセキュリティの世界が大きく変わっていく日になると思っています。是非それを皆様の目で確かめてください。

エムオーテックス株式会社 代表取締役社長 河之口 達也





# INDEX

04-05 Presentation by Cylance

## 世の中のすべてのエンドポイントを守る

- セキュリティ業界に突如現れた「Cylance」が今までの常識を覆す。 -

「Cylance は対前年度比 1,100%の成長をしている会社です」  
米国 Cylance 社 Nicholas Warner 氏の衝撃的なプレゼンから幕開けた Unbelievable Tour in Japan

登壇者：Cylance Inc. SVP, Worldwide Sales Nicholas Warner 氏

06-09 Presentation / Demonstration by Cylance

## AI(人工知能)を活用した予測脅威防御、 Cylance は 400 人の観客の目前で防御率 99%を実証！

「Unbelievable Tour in Japan」の目玉コンテンツ。全米 75 都市で実施された注目のイベント、アジア初開催となる今回は、米国よりセールスエンジニア Ryan William 氏が来日し、Cylance を含む 5 製品を並べた比較検証のデモンストレーションを実施

登壇者：Cylance Inc. Sales Engineer Ryan Williams 氏  
Cylance Japan セールスエンジニアリングマネージャー 井上 高範 氏

10-13 Presentation / Demonstration by MOTEX

## 残されたセキュリティの課題は「人」

- インシデント発生に起因したユーザー操作への対策で、再発を防止 -

2016.07.25 リリースの LanScope Cat 新機能「プロテクトキャット Powered by Cylance」  
「外部からの脅威」「内部による不正行為」対策と、次期バージョンロードマップを展開

登壇者：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 営業本部 執行役員 池田 淳

14-17 Unbelievable Tour Talk Session Round 1

## テクニカルセッション

### 「Cylance のココが知りたい」

OWASP Japan 代表の岡田氏、HASH コンサルティング代表の徳丸氏という業界でも大きな影響力を持つお二方が、Cylance に直撃質問を決定！ここでしか聞けないレアトークを展開！

登壇者：OWASP Japan 代表 / 株式会社アスタリスク・リサーチ 岡田 良太郎 氏  
HASH コンサルティング株式会社 代表取締役 徳丸 浩 氏  
Cylance Inc. SVP, Worldwide Sales Nicholas Warner 氏  
Cylance Japan 株式会社 セールスエンジニアリングマネージャー 井上 高範 氏

18-21 Unbelievable Tour Talk Session Round 2

## ガバナンスセッション

### 「2020 年に向けて日本のセキュリティはどうあるべきか」

第一線でセキュリティに携わっている 4 名が、企業におけるセキュリティの実情や、Cylance / プロテクトキャットの登場で、企業のセキュリティがどのように変わるのか、といった未来の話までを幅広くディスカッション

登壇者：OWASP Japan 代表 / 株式会社アスタリスク・リサーチ 岡田 良太郎 氏  
デロイトトーマツリスクサービス株式会社 代表取締役社長 丸山 満彦 氏  
株式会社ラック サイバーセキュリティ事業部 サイバー救急センター長 内田 法道 氏  
エムオーテックス株式会社 CISO 兼 執行役員 中本 琢也

# 世の中のすべてのエンドポイントを守る

- セキュリティ業界に突如現れた「Cylance」が今までの常識を覆す -

Presentation by Cylance



## 「Cylance は対前年度比 1,100%の成長をしている会社です」

Unbelievable Tour in Japanの幕開けは、米国Cylance社Nicholas氏の衝撃的なプレゼンテーションから始まりました。2012年の創業ながら、すでに米国では1,000社以上の導入実績があり、飛躍的な成長を遂げている同社。人工知能を使いこれまでとまったく違うアプローチでマルウェア対策を行う同社製品の脅威検知率は99%以上を誇り、セキュリティ業界に「未知の脅威は本当に防げないのか？」という疑問を投げかけます。Cylanceとは何者なのか、どのようにして誕生したのか。新進気鋭企業のSVP（シニア・バイス・プレジデント）登壇に、客席の注目が集まりました。



Cylance Inc. SVP, Worldwide Sales  
Nicholas Warner 氏

私たちは人工知能を使い、脅威を事前に予測・検知し、侵入を止めることが出来る製品を提供している企業です。既に1,000社を超える法人・政府機関のエンドポイントに導入されており、対前年度比は1,100%と大きく伸張しています。

Cylanceはインテルセキュリティ/マカフィーでCTOを勤めたCEOのステュアート、そして、同社でチーフサイエンティストを勤めたライアンによって、「世の中にある全てのエンドポイントを守る」というミッションで設立されました。Cylanceの事業は、製品、OEM、コンサルティングサービスの3つで構成されています。

おかげさまで、Cylanceは世界中で多くのお客様にご支持いただいております。グローバルな大企業から中堅企業、小売・金融・製造・医療といった多岐に渡る業種のユーザー様にご利用いただいております。製品リリースは2年前ですが、既に600万台に及ぶエンドポイントを保護しています。

PASSION  
PERSISTENCE  
DRIVE

Our mission is to protect every computer under the sun.



Cylance Inc. CEO/President and Founder  
Stuart McClure 氏



Cylance Inc. Founder and Chief Scientist  
Ryan Permech 氏

私たちは、膨大な被害を引き起こすサイバー脅威から組織を守るためにAI(人工知能)及び機械学習技術を活用して悪意の行動を事前に阻止します。

## サイバーセキュリティ関連企業の中で成長が著しい Cylance

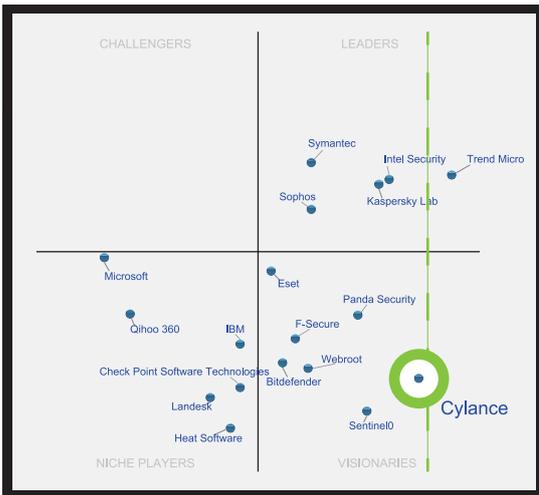
ガートナー社が出したエンドポイントセキュリティに関するマジッククアドラントにおいては、恐らく製品リリースの最初の年からビジョナリーリーダーのポジションに入った唯一の会社だと思います。縦軸は売上、横軸はビジョンを示しており、Cylance は（優れたビジョンを持つ）一番右側に位置していま

す。今後、売上げを増大させることによって上のリーダーの位置に上がっていくと確信しております。

Cylance が良いポジションに評価されているのは幾つかの理由があります。

一つ目は、脅威の予測防御ができる点。二つ目は、オンライン環境だけではなくオフライン

環境でも脅威を止められる点。三つ目は、製品のアップデートやシグネチャの更新をする必要がないという点。四つ目は、AI を駆使し、脅威を事前にブロックでき、被害をおこさないという点です。



### Gartner

#### マジック・クアドラント エンドポイント部門

- ビジョナリーリーダーと評価
- Cylance は、サイバーセキュリティ関連企業の中で最も成長が著しい企業
- Cylance の製品は、インターネット接続、シグニチャーを必要とせず、既知および未知のマルウェアからの保護が可能

Magic Quadrant - Figure 1: Magic Quadrant for Endpoint Protection Platforms -

## 他社にはないユニークなアプローチ

アンチウイルス製品の市場においては、以下のように分類することが可能です。

- シグネチャベース
- エクスプロイト防御
- ホワイトリスト、アプリケーション防御
- サンドボックス
- EDR (Endpoint Detection and Response)

多くの技術がありますが、完全にお客様の環境を守ることは出来ていないのが現状です。最近では「検知して対応する」という、

新しい EDR というアプローチも出てきましたが、私どもはそういうアプローチではなく、「検知して即座に駆除する」ことを実現しています。Cylance は人工知能を使って実際に脅威を止められる唯一の企業です。非常にユニークなアプローチですが、導入いただけるお客様にとって、非常に大きなメリットを提供できると思っています。



このあと、実際のデモンストレーションも行いますので、是非ご自身の目で Cylance の凄さ確かめてください。



# AI(人工知能)を活用した予測脅威防御、Cylance は 400 人の観客の目前で防御率 99% を実証！

Presentation / Demonstration by Cylance

「Unbelievable Tour in Japan」の目玉コンテンツ。全米 75 都市で実施された注目のイベント、アジア初開催となる今回は、米国よりセールスエンジニア Ryan Williams 氏が来日し、Cylance を含むアンチウイルス 5 製品を並べた比較検証のデモンストレーションを実施。400 人の観客の前で繰り広げられた、「これまでの概念を覆す」結果に注目！また、前半は CylanceJapan セールスエンジニアリングマネージャー井上氏によるプレゼンテーションにて、「なぜ Cylance が防御率 99% を実現できるのか」その真髓を語っていただきました。



Cylance Inc.  
Sales Engineer  
Ryan Williams 氏



CylanceJapan  
セールスエンジニアリング  
マネージャー  
井上 高範 氏

## ■ マルウェアを実行前に止める。AI が実現可能にしたシンプルなコンセプト

これまでのエンドポイントセキュリティは、古いものであればシグネチャや、ふるまい検知（ビヘイビア）、最近ではサンドボックスや EDR（Endpoint Detection and Response）などを使ってエンドポイントを守ってきました。ただ、それで100%エンドポイントを守れていたのでしょうか。なかなかそうはならないですし、実は弊社も100%ではありません。しかし、限りなく100%に近いプロテクションをお客様に提供するために、CylanceはAI（人工知能）を利用した予測による脅威の阻止をご提案します。

これまでのエンドポイントセキュリティの歴史を見ていくと20年以上前のアンチウイルスソリューションから始まり、様々な高度な技術（例えば、脆弱性対策やサンドボックス、振る舞い検知、EDR）が出てきます。

しかし、これら全てに共通するのは、人の手を介すということ、またファイル実行後に対応することが常でした。これに対して、Cylanceが考えたものは、AIを使って人の対応をなるべく少なくし、マルウェアを実行前に止めることです。最終的には、人間に

裁量を委ねることをゼロに近づけることを目標にしています。

今年1月にドイツのAVテストという第三者のベンダーがテストした結果では、検知率 99.7%という非常に高い検出結果を出しています。



## Cylance はなぜ防御率 99%を実現できるのか、その特徴は？

Cylanceの特徴は3つです。1つ目はDNAレベルでのマルウェア解析をしていること。そして、2つ目はシグネチャの更新が不要ということ。（これは例えばネットワークから隔離されたクローズな環境、また逆にIoTなど常に通信を行うオープンな環境含め様々な環境で使うことができるということです。）そして、3つ目はインターネット接続が不要ということ。これらの特徴的な技術とユーザビリティを用い、予測と防御を徹底し、お客様のエンドポイントを安全に守っています。

ではCylanceが、どのように脅威を発見しているかについて解説します。単なる機械学習ではなく、ディープラーニングを行っていることが鍵です。CylanceはクラウドにAIを持っていて、そこでファイルを学習させています。このAIの中で2億5,000万個の良いファイルと、2億5,000万個の悪いファイルに対してそれらがどういう特徴を持っているのか、計5億個のファイル1つ1つを分析しています。1つのファイル解析において、約620万の特徴を抽出します。そこから

マルウェアなのか、正常なファイルなのか、はたまたPUPなどのツールなのか、VPNのようなソフトなのかを判断をしているのです。

ここでポイントなのは、5億のファイル进行分析し、その結果をAIのエンジンとして持っていること。そして、その結果をアルゴリズム化し、数理モデルという形でエンドポイントに導入していることです。新しいファイルや脅威を発見した際、エンドポイントに展開されているアルゴリズムが瞬時にその特異点を判定し、マッチングさせスコアをつけます。例えば、スコアが60点以上だと「悪いファイル」、59点以下だと「有害な可

能性あり」という風に、その疑わしさを、100万分の1秒という速さで判断していきます。

このAIエンジンは一度エンドポイントに入れていただくと、基本的に更新する必要はありません。ただし、Cylanceでは常に誤検知・過検知などの分析をしており改善を行っています。また継続的に人工智能に学習をさせ続けており、これらをアップデート版として約6ヶ月～10ヶ月ごとに提供しています。



## 実行前防御を実現する4つの機能

Cylanceの主な機能は4つです。今紹介したAIを使った「1：マルウェア実行制御」以外にも、メモリの悪用、脆弱性攻撃から防御する「2：メモリ保護」、マクロやスクリプトを使った侵入を制御する「3：スクリプト制御」、そしてクローズな環境である特定のアプリケーションだけを起動させることができる「4：アプリケーション制御」など、様々な機能を搭載し、マルウェアの実行前にエンドポイントを守っています。

最後にCylanceのメリットを2つ紹介します。1点目は、これまでで紹介してきた「脅威防御力」です。その実績は前述した通り99.7%という結果からも証明されています。2点目は「運用管理のしやすさ」です。CylanceはSaaSモデルなので、お客様の環境でSQLサーバーや管理サーバーを立てる

必要がありません。クラウドのCylanceにアクセスし、クラウド上で設定や管理をいただけます。またクラウドのメリットを利用し、特定のマルウェアがCylanceユーザー全体でどれだけ発見されているか？などの情報を共有することができます。

これにより、お客様の端末に対する無駄な投資を削減し、運用負荷を下げるができます。

ではここからは、実際の比較検証のデモンストレーションをご覧ください。

4つのプロテクション機能で99.7%の防御率を実現

マルウェア実行制御	メモリ保護	スクリプト制御	アプリケーション制御
<ul style="list-style-type: none"><li>AI(人工知能)で脅威を予測</li><li>マルウェアの実行を阻止</li><li>シグネチャ不要</li><li>毎日のスキャンが不要</li><li>ファイルシステム変更時にスキャン</li><li>潜在的に悪ましくないプログラムが環境に入るのを防止</li></ul>	<ul style="list-style-type: none"><li>メモリの悪用防御</li><li>脆弱性攻撃の防御</li><li>プロセスインジェクション防御</li><li>特権昇格の防御</li><li>シェルコード/ペイロード攻撃の防御</li></ul>	<ul style="list-style-type: none"><li>不正なパワーシェルとアクティブスクリプトの制御</li><li>危険なVBAマクロを制御</li><li>ファイルを残さない攻撃の阻止</li><li>危険なドキュメントファイルの制御</li></ul>	<ul style="list-style-type: none"><li>機器で利用する機能を限定して利用バイナリを制御</li><li>不正なバイナリの実行を阻止</li><li>任意のバイナリの変更を防止</li><li>Windowsの変更は許可</li></ul>

## 圧倒的な軽さと防御力で、人工知能がシグネチャの限界を突破 Cylance は他の追従を許さない防御率 99.5%を実証！ (211 / 212 個)

### Environment - 環境 -

#### 6つの仮想環境に Cylance を含む 5つのアンチウイルス製品をインストール

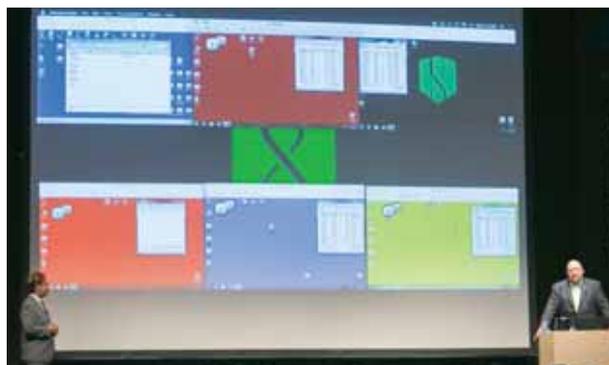
- Cylance は 8ヶ月前のバージョン (Ver.1370)、  
その他製品は最新バージョンを利用。
- それぞれのデスクトップは CPU とメモリが簡単に見れる  
ガジェットを用意。
- 最近だとシグネチャをクラウドへ見に行ったり、  
ハッシュデータを見に行ったりする製品も多いため、  
全ての環境はインターネットに接続。

### Target - 対象 -

- イベント当日の朝にダウンロードし入手した  
最新のマルウェア 100 個
- 上記 100 個のファイルをバック化 (亜種化) して  
作成した新しいマルウェア 100 個  
※一度検知されたものでもバック化 (亜種化) することで  
検知されなくなることもあり、攻撃者はバック化  
(亜種化) して、同じウイルスで何度も攻撃をすることが  
あります。
- 来場者より持ち込まれた検体 12 個

### Demo 手順

- 1 コントロールサーバーにあるフォルダに 100 個のサンプルをコピー  
※これにより、他 5 つの環境にも同様のファイルがコピーされます
- 2 コマンドを実行して 1 つ 1 つのファイルを起動
- 3 それぞれの環境で、実行状況・検知状況・  
CPU やメモリの状況を確認
- 4 100 個のファイルをバック化 (亜種化) し、  
新しいマルウェアを作成
- 5 再度 5 つの環境にコピーし、コマンドで実行
- 6 来場者より持ち込まれた検体 12 個を Cylance 環境で実行



## その場で作成した亜種のマルウェア 100 個含め Cylance は全てを防御

まずは A 社の環境でコマンドを実行開始。タスクマネージャーで複数のマルウェアが立ち上がっていることが確認できました。CPU は 100%、メモリは 37%になっています。進めていく中で WinGate など複数のプログラムが起動しデスクトップに表示されました。

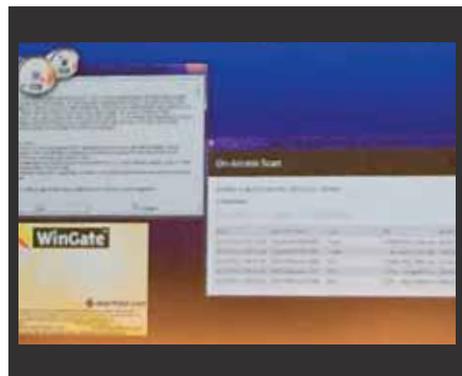
次に B 社の環境でコマンドを実行。A 社同様に複数のプログラムが実行されています。すぐに端末の操作が不可能になりました。「まだ 12 個しか検知していないですが、このコンピュータはすでに死んでしまったかもしれません。」(Ryan 氏)

C 社 D 社も同様にそれぞれの環境で実行。

それぞれの環境で複数のマルウェアが立ち上がっていることをタスクマネージャーで確認できました。そして、Cylance 環境でも同様にコマンドを実行。しかし全ての起動を拒否。タスクマネージャーでも動いてないことを確認。そして、あっという間に 100 個の隔離が完了しました。

その後、改めて他社製品の管理画面を確認。しかしまだ 1 つずつマルウェアをチェックしていて最後まで終わっていません。「他製品はクラウドでシグネチャを 1 つずつマッチングしたり、クラウドに確認したりするので時間がかかるのでしょう」(井上氏)

先ほど実行した 100 個のマルウェアをバック化 (亜種化) し新しいマルウェアを目の前で作成。「ある程度スクリプトを組んでいるということもありますが、実はこれだけ簡単



に新しいマルウェアを生成することができてしまうことは驚きです。」(Ryan 氏)

そして先ほど同様、コントロールサーバーからファイルをコピー、それぞれの環境で実行。Cylance の環境では、新しいマルウェアでも 1 つ 1 つ検知し 100 個全てのブロックが数十秒で完了。これに対し、他社製品は検知できず 0% となりました。



## ■ 来場者持込みマルウェアのうち 1 つがスルー!?

そして、最後に来場者から持込まれた 12 個の検体を Cylance の環境で実行。11 個は検知し、1 個は検知しないという結果になりました。検知漏れか!?!と思われる中、その 1 つの検体を実行してファイルの実態を確認しました。

このファイルは「Outlook を起動しメールを送付するプログラムで、現段階ではこれが良いファイルか、実際に害をもたらす悪いファイルかは、もう少し詳しくこのファイル自体の検証が必要でしょう。」(井上氏)

「このように検知できるものときないものがあり、100% ではありません。ただし 99% は防御しているのが実績です。そして、このように人工知能がマルウェアと判断しなかったものについては Cylance にフィードバック頂くことで、解析しその結果を改良

という形でまたお客様に提供いたします。」

(井上氏)

(後日談：持込まれた検体は、社内トレーニング向けに作られた擬似マルウェアで、実際の攻撃に使用されたマルウェアではなかったことを確認しています。)

最後に・・・「Cylance を含め、どのアンチウイルスベンダーも信じないでください。実際にマルウェアを使ってご自身で試した結果だけを信じて製品を採用してください。弊社では POC (※) という形でお客様に検証をおすすめします。」(Ryan 氏)

※POC(Proof-of-Concept)：導入前の評価



# R e s u l t 結 果

	製品バージョン	最新マルウェア 検知率	最新マルウェアの 亜種の検知率	持込み検体の 検知率
Cylance	8ヶ月前のバージョン (Ver.1.3.7.0)	<b>100%</b>	<b>100%</b>	<b>91%</b>
A社	最新バージョン	43%	0%	-
B社	最新バージョン	応答なし	0%	-
C社	最新バージョン	9%	0%	-
D社	最新バージョン	応答なし	0%	-

# 残されたセキュリティの課題は「人」

- インシデント発生に起因したユーザー操作への対策で、再発を防止 -

Presentation/Demonstration by MOTEX

## LanScope Cat 新機能 「プロテクトキャット Powered by Cylance」

外部攻撃の検知・隔離・追跡を 1 つのインターフェースで行うことができる「プロテクトキャット Powered by Cylance」。Cylance と LanScope Cat が組み合わせることで生まれる新たな価値について、エムオーテックス 代表取締役副社長 宮崎が説明しました。

また、セッションの後半ではエムオーテックス 執行役員 池田より、プロテクトキャットの画面を用いたデモンストレーションを実施。LanScope Cat の特徴的な管理画面である Web コンソールから、周辺操作ログをたどりウイルス流入時の原因を追跡する様子が紹介されました。



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  
営業本部 執行役員  
池田 淳

## IT 資産管理から始まった LanScope Cat が 新たに「外部脅威対策」の分野へ

まずは、LanScope Cat の代表的な機能を紹介したいと思います。1996 年にリリースした LanScope Cat。昨今では、セキュリティの第一歩は社内の IT 資産がどのような状況にあるのかを把握し、最適な状態に保つということが大切だということを改めて言われるようになってきていますが、Cat はこの資産管理機能からスタートしました。そして、次に Cat の特徴的な機能である操作ログ管理機能。これは「いつ・誰が・どの PC で・どんな操作をしているか」を把握することができるため、防犯カメラと同じように抑止環境をつくり、不正な操作をさせないというものです。そして 3 つ目が私物の USB を使わせないようにするデバイス制御機能や不正な

Web サイトを禁止する Web アクセス制御など、直接的に対策ができる情報漏えい対策機能です。これまでは、これらの機能をもとに「IT資産管理・内部情報漏えい対策ツール」として提供してきましたが、今回新たに

「外部脅威対策」としてリリースしたのがプロテクトキャットです。



## ■ セキュリティの最後の砦は「従業員のセキュリティ教育」

ここで、昨今のセキュリティ事故の実態を見ていきたいと思ひます。これまであったメール誤送信や盗難・紛失などに加え、「マルウェア感染」や「標的型メール攻撃」が上位に入ってきているのが最近のトレンドです。そして、それに対して企業が重視する対策として上位に上がっているのが、「従業員のセキュリティ教育」と「標的型攻撃に対するセキュリティ対策」です。「従業員のセキュリティ教育」が1位に上がってきているという点について非常に興味深いと感じます。なぜなら、従来からセキュリティの有識者が言われている「セキュリティの最後の砦は従業員教育だ」ということが、ようやく浸透してきたということが読み取れるからです。



## ■ 毎日 100 万個の新種マルウェアが誕生。日々、進化し続けるサイバー攻撃

さて、話しを標的型攻撃に戻すと・・・最近では毎日 100 万個以上の新しいマルウェアが誕生しているといわれており、既知のマルウェアを対策できる従来型の製品だけでは防ぎきれないというのは、先ほどの Cylance 社のデモを見ても明らかです。では皆さんどういふ対策をとられているかという、

例えば不正な通信をブロックするファイアウォールを導入されたり、IPS という侵入防止システム、あるいはサンドボックスなど、様々なツールを導入されてセキュリティを守ろうとしています。しかし、次々にこれらをすり抜けるマルウェアが誕生しており、エンドポイントまで入ってきているというのが現状です。

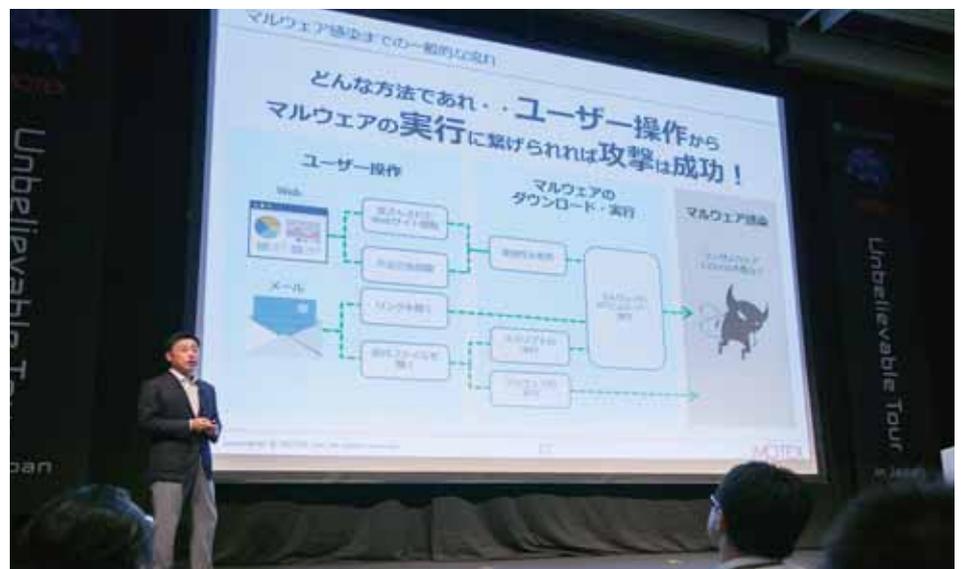
ここに対して、エンドポイントで防ぐことができるのが、先ほどご覧いただいた Cylance 製品を LanScope Cat の新機能として組み込んだ「プロテクトキャット Powered by Cylance」です。

## ■ Cylance × LanScope Cat で、マルウェア検知時に流入原因となったユーザー操作を追跡

Cylance で未知の脅威を実行前に検知し止めることができるということは、先ほどのデモで存分にご理解いただけたと思いますが、では「プロテクトキャット Powered by Cylance」でさらに何が出来るのか。まずは、こちらのデータをご覧ください。これは、弊社で行った「現状の情報セキュリティに関する課題」のアンケートですが、「感染原因の特定に時間がかかる」「感染原因が特定できず応急対応が多い」という結果が半数以上を占めています。つまり、ここから読み取れるのは「未知の脅威を止めたとしても、原因特定ができない」ということです。原因特定ができなければ、根本的な対策を施すことは出来ません。この課題を解決できるのが、冒頭にも紹介した LanScope Cat の特徴である操作ログです。感染するということは、なんらかの人の操作、例えばメールの添付を開いたり

リンクをクリックしたり、改ざんされた Web サイトを閲覧するなどの操作が行われます。つまり、操作ログを分析することで、マルウェアがどのように進入してきたかということ特定でき、また、エンドポイ

ントで止めるだけでなく、その上流である感染源を見つけ対策につなげることができるという点が、プロテクトキャット最大の特徴であり価値となります。



# RoadMap of LanScope Cat The Next Version.

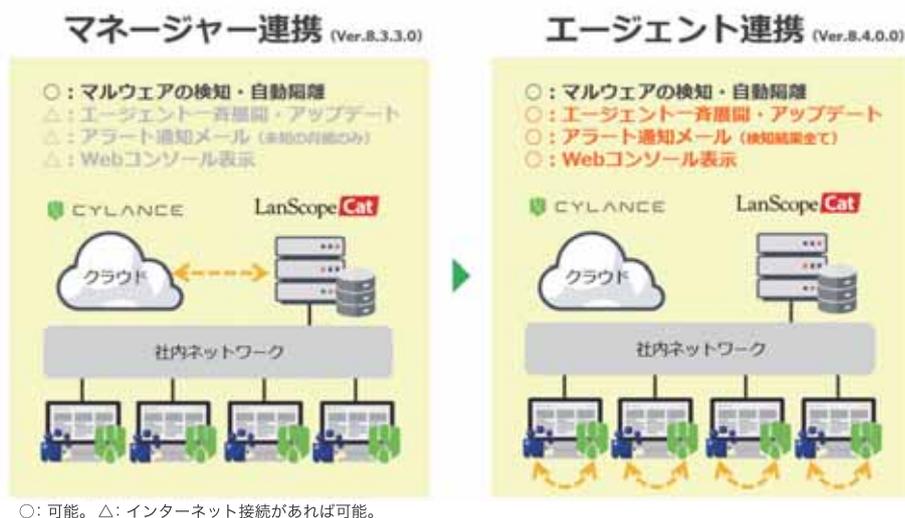
## ■ 次期バージョンで、プロテクトキャットのオンプレミス運用を実現

現在のプロテクトキャットは、クラウドにある Cylance と LanScope Cat のマネージャをつなぐことで、情報を連携しています。しかし、最近では金融業や自治体などは強靱化対策としてネットワークに繋がらない環境が増えてきています。もちろん、これらの環境でも Cylance は利用することができるので、感染を防ぐことが出来ます。しかし、何が起きているのかということは管理者には分かりません。

そこで、LanScope Cat の次期バージョンでは、お互いのエージェント同士を連携させることで、外部ネットワークに繋がらない環境でも LanScope Cat のマネージャに全ての情報を集め、レポートでの検知の状況確認やアラート通知メール機能、

エージェントの配布・アップデートを可能にします。インターネットに接続できない環境においても、オンプレミスでより高度な運用を実現できるようになることが、

次に提供できる新しい価値となります。是非ご期待ください。



## Demonstration

## ■ Web コンソールで、インシデント発生時の原因特定をわずか3クリックで実現

LanScope Cat は取得したログを自動で分析し、アイコンでルール違反の有無を把握し、クリックするだけで詳細をみることができる「Web コンソール」という運用コンソールがあります。プロテクトキャットもこの Web コンソールで運用が出来ます。

Web コンソールの TOP 画面は、このようなカレンダー画面になっており、縦軸に管理グループ、横軸が曜日になっています。その中に様々な種類のアイコンがあると思いますが、これはアラーム違反をカテゴリ別に表しています。つまり、このカレンダーを見れば、膨大なログがあったとしても、いつ・どのグループで、どんな違反操作があったのかを一目で把握することができます。今回プロテクトキャットについては、新たに「脅威」というアイコンが追加されました。カレンダーを見ると、26日に4台で脅威が発生していたということがわかります。では次に、この4台がどの端末なのかを確認してみます。「脅威」アイコンをクリックして見て

みると、大阪本社 - 開発の近藤さん、東京本部 - 営業の内田さんといった風に具体的に把握することができます。また、それらの端末で何件の脅威があったのかということも同時にわかります。

端末がわかると、次にそれらがどんなマルウェアなのか気がになります。その場合は脅威発生件数の数値をクリックします。すると、どんなファイル名でいつ検知したもののなのか、どの

フォルダパスに存在しているか、また、すでに自動隔離されていて感染はしていない（隔離モードに設定している場合）といった状態、人工知能エンジンがスコアリングしたスコア、またそれがハッキングツールなのかアドウェアなのといった種別など、マルウェアの詳細を確認することができます。

脅威リスクが4台で発生している！

グループ	8/22 (月)	8/23 (火)	8/24 (水)	8/25 (木)	8/26 (金)	8/27 (土)	8/28 (日)
ネットワーク全体	Web 1						
所属グループ							
大阪本社	Web 1						
東京本部	Web 1						
名古屋	Web 1						
札幌	Web 1						

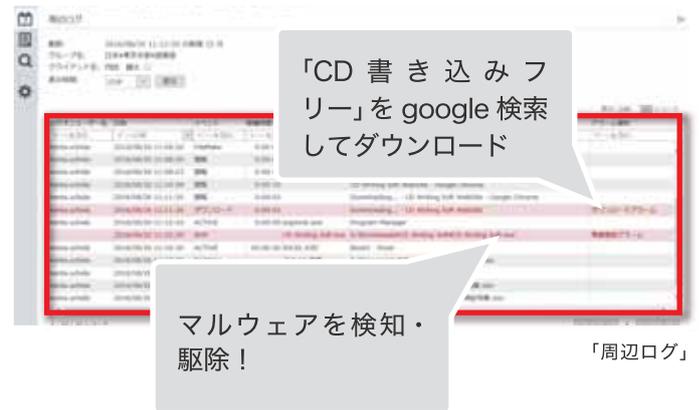
- アプリ禁止 2
- 実行 4
- Web 3
- 通信デバイス 1
- メール 1
- 脅威 4

## ■ 標的型メールの添付ファイル実行、

## フリーウェアのダウンロードなど、マルウェア流入原因をログで把握。

さらにここからは、なぜこの端末はマルウェアの流入に至ったのかを周辺操作ログから見ていきましょう。

周辺操作ログのアイコンをクリックすると、今回はまず google で「CD 書き込みフリー」を検索し、そして CD ライティングソフトの Web サイトにいき、ダウンロードしています。その結果、フリーの CD ライティングソフトの EXE がマルウェアとして検知されているということがしっかりと記録に残っていることが分ります。ここまで分ればサイトをフィルタリングして見せないような対策や、従業員教育を行うことで、他の人がこのサイトから感染するということを防ぐことができます。



## ■ 人工知能によるファイル要素解析で、マルウェアの要素とそのリスクを確認。

では次に、この発見したフリーの CD ライティングソフトがなぜマルウェアとして判断されたのか、その解析結果を確認したいと思います。

ここで、マルウェア情報の「詳細」をクリックするとマルウェア解析結果のページを表示できます。まず、画面左のフィールドに Cylance スコアが 77 と出ていますが、これは人工知能がマルウェアらしさをスコアリングした結果でファイル要素としては 77 点だということが分かります。

次に 100% が二つ続いています。これは自社内の端末で隔離や許可を設定した割合、もうひとつは、Cylance ユーザー全体の中で隔離や許可を設定した割合を表示し、他のユーザーの判断を共有できるようになっています。完全に未知のものは 0% となりますが、今回は 100% のユーザーが隔離設定にしているという判断を参考にすることができます。

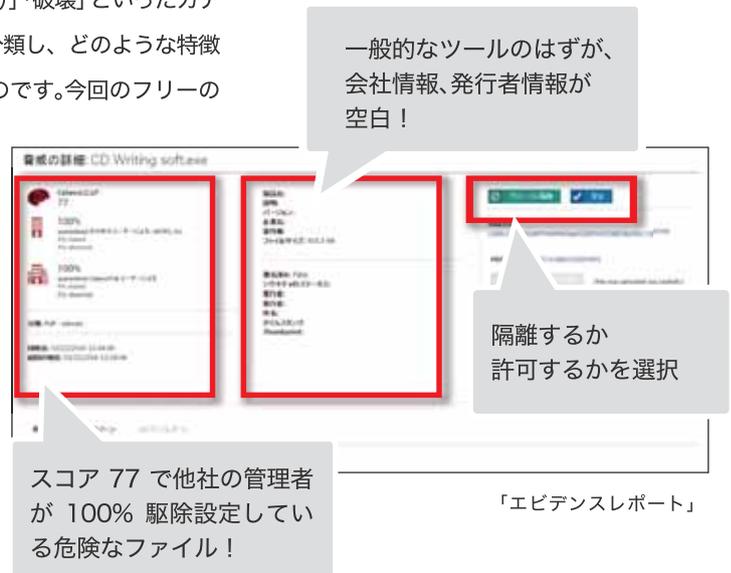
次に、画面真ん中のフィールドでは、ファイルの情報が記載されています。ファイル名やバージョン、企業名、ファイルサイズ、デジタル署名の有無や発行元などです。例えば商用ソフトに

もかかわらず企業名が記載されていない等から、怪しいファイルかどうかを判断します。

では、人工知能がこのファイルに対しどのような解析をしたのか、その詳細を確認しましょう。画面下にあるエビデンスレポートをクリックしファイルの詳細を表示します。

このレポートは、ファイルの要素を解析した結果からどのようなマルウェアらしい要素をふくんでおり、どのようなリスクがあるかを説明してくれます。「異常」「コレクション」「データ損失」「デセプション (偽装)」「破壊」といったカテゴリにファイル要素を分類し、どのような特徴があるか教えてくれるのです。今回のフリーの

CD ライティングソフトは CD ライティングソフトのようですが、「デセプション (偽装)」の分類では、プログラムの中に他のプログラムを含んでいる点と、隠れてバックグラウンドで動作しようとしている点、また「破壊」の分類では、他のマルウェアをダウンロードする危険性を指摘しています。このように、何気なく使っているフリーウェアや未知のマルウェアを、自動的に隔離すると同時に、そのリスクをしっかりと把握することができるのです。



## ■ 最も重要なのは、マルウェアの流入を食い止め、実行前に防御すること。

「プロテクトキャット Powered by Cylance」の効果是非皆さんの目でご確認ください。マルウェアの感染は人の操作に起因して始まるため、エンドポイントで検知し止めるだけでは、リスクをゼロにすることはなかなか難しいのが現状です。だからこそ、エンドポイントでの対策に加えて、より上流工程で対策を打つしかありません。今回の Cylance との連携は、その要素解析の技術とログによる原因特定～対策が実現したことで、これまでにないマルウェア対策がみなさんにご提供できるようになりました。ご興味のある方は是非 POC を実施していただき、その効果を体感頂ければと思います。



# テクニカルセッション Cylance のココが知りたい

Unbelievable Tour Talk Session Round 1

## Unbelievable Tour in Japan

### Talk Session Round 1

OWASP Japan 代表 / 株式会社アスタリスク・リサーチの岡田氏、HASH コンサルティング代表の徳丸氏という業界でも大きな影響力を持つお二方が、Cylance に直撃インタビューを決定！「Cylance の AI はいったい何を学習しているの?」「Cylance を入れたら Windows XP でも安全に使えるの?」と、突っ込んだ質問も飛び出し、ここでしか聞けないレアトークが展開されました。



### Speakers - 登壇者紹介 -



OWASP Japan 代表 /  
株式会社アスタリスク・リサーチ  
岡田 良太郎 氏



HASH コンサルティング株式会社  
代表取締役  
徳丸 浩 氏



Cylance inc.  
SVP, Worldwide Sales  
Nicholas Warner 氏



Cylance Japan 株式会社  
セールスエンジニアリング  
マネージャー  
井上 高範 氏

## ■ 岡田氏・徳丸氏が Cylance へ直撃！

岡田：なんでも質問していいコーナーということなので。最初は和やかに、マイクテストもかねて自己紹介をしていききたいと思います。私は岡田 良太郎と申します。どうぞよろしくをお願いします。

そして、私の隣におりますのは旧知の友でありまして、業界の中でも有名で、今日はこの方を見に来られたという方も多いのではないかと思います。徳丸さん、では自己紹介をお願いします。

徳丸：HASH コンサルティングの徳丸でございます。どうぞよろしくお願いたします。

岡田：そして引き続き、ニコラスさんと井上さんにもお越しいただきました。何か一言ありますでしょうか？

井上：先ほどのデモでは Cylance の(ソフトウェアの)軽さと(スキャンの)速さを見ていただけたかと思います。ここでは色々な質問が来るかと思しますので、そこでまた Cylance のことを知っていただけたらと思います。

岡田：ニコラスさんいかがですか？

Nicholas：本日はこのようなエキスパートの皆さんと登壇でき、大変光栄に思っております。

岡田：さてさて、なんと徳丸さんと僕で Cylance について聞きたいことをどんどん聞いていこうというセッションです。では徳丸さん、ちょっと優しめの質問からお願いできますか？

徳丸：そうですね、最初の質問は今日の Cylance デモンストレーションで、一部ダメダメだった既存のアンチウイルスソフトと共存することを Cylance は薦めているのか、あるいは共存することができるのかについてお伺いしたいと思います。

岡田：なるほど・・・確かにだいたい今の PC にはアンチウイルスソフトが入っていますからね。そういう環境で使う場合、どのように考えたらよいのでしょうか。

井上：Cylance で実際に評価していただく時には、既存のソフトと同居している環境で

評価することができます。既存のアンチウイルスソフトと Cylance を一緒に動かすことで、既存ソフトですり抜けてしまったものを Cylance で止めることができます。ですので、既存ソフトと一緒に使いたいというお客様もいらっしゃる。ただ、実際に使っていただく場合、例えば既知のウイルス対策用・未知のウイルス対策用と入れてしまうのであれば、Cylance にまとめてしまう方が運用コストや導入コストも削減できるのではないかと考えております。

岡田：なるほど。ちょっとアグレッシブにきましたね。

## Cylance を入れればサポート切れの Windows XP でも安全!?

岡田：では、次の質問へ。

徳丸：はい、今でも Windows XP を使い続けているお客様が結構おられると聞いているのですが、Cylance を入れたら、Windows XP でも安全に使えたりするのでしょうか。

Nicholas：はい、私どもは Windows XP の Service Pack3 以降のものについては、きちんと互換性を担保しています。Cylance のプログラムそのものは非常に軽量となっていますので、古いマシンであってもまったく問題なく動作します。

岡田：それはすごいですね。

徳丸：なんかちょっと聞いてみたけど、聞かなかったほうが良かったような気も立場上いたします。

岡田：うーん。なんか Windows XP を使っているだけでも、ほとんどマルウェアそのものなんじゃないかっていう…はい、すいません。

井上：補足すると、XP を使われているお客様というのは、IoT 環境や工場などが多いですね。そこで Cylance を使っていただくメリットは、「軽い」という点、「XP をサポートしている」点、後は「アプリケーション制御」機能で、限定されたアプリケーションだけ起動するといったことができることです。

ですから、例えば IoT の環境は多数のアプリを使うことがないので、ある特定の限定されたアプリと Cylance を使うことによって、既知のウイルスも未知のウイルスもブロックしたうえでアプリケーションも安全に動かすといったことが可能になります。

岡田：なるほどね、そういうことなんですね。



## 「99%の検知率」に誤検知は発生しないのか？

岡田：すごく高い検知率だということを、今日のデモンストレーションで実証されましたね。後ろの方で見ていて「なんで今拍手が起らないんだ」と思っていました。今度1000個でやってみたらどうなるのか・・・つまり何が言いたいのかというと、検体の数が多くなると、これまたいろいろなブレみたいなものが出るような気がして。どうですか、徳丸さん。その辺り気になりませんか？

徳丸：そうですね、今日はウイルスを止めるということにフォーカスしたデモだったので、ウイルスでないものが止まってしまうというのも困るわけですね。

やらないといけない人たちは、どうやってそれを救済したらいいんだろうという、もう少し実務よりの質問だとしたらどうですか？

Nicholas：まずここで、基本的な概念をご説明します。これまでアンチウイルスのソフトウェアというのは、次の2つのいずれかをやってきたと思います。まず、すでに悪いと分かっている既知のものに関しては、それをブロックする。あるいは、良いものをホワイトリストとして定義付ける。ホワイトリストの場合、「これは良いものである」という想定するわけです。そして、良いものかどうかはわかっていない、となると

どちらかの判断を出していく。こういった仕組みになっているわけです。

次に、より具体的にお答えしていきたいと思いますが、万が一、擬陽性(過検知)が発生した際には、それを許可する、あるいはホワイトリスト化するというプロセスを組み込んでいます。そして、そこには我々が開発した、セントロイドという非常に興味深い概念が存在します。これは考え方としては、いわゆるDNAでファイル家族のラベル付けをするというもの。つまり、擬陽性(過検知)向けにセントロイドを構築すること



その辺はどう考えておられますか？そういうことはないのでしょうか。

井上：今の話というのは、例えば過検知の話と、すり抜けの話だと思うのですが、弊社の製品もやはり100%ではないです。ただし、他のものと比べると非常に過検知が少ないですし、すり抜けも少ないです。一つ例をあげると、すり抜けの確率は0.00002%というのが弊社の値になっています。

岡田：いや、すり抜けてしまう可能性が0になるということを期待しているというよりは、例えば使いたいと思っているソフトウェアがCylanceでとめられてしまった。多少ダサいソフトと分かっているけど、使いたい場合に、企業の情報システム部門や、ガバナンスを

「それは悪いものだ」とやはり想定をしていくわけです。このモデルには両方とも欠点があると思います。それは、どちらも「想定する」ということが発生しているからです。

一方でCylanceのAIは、良いものも悪いものも、同等に特定するという仕組みを持っています。何億という良いアプリケーションに対して、どんどんトレーニングを重ねていきます。同様に、悪い、つまりウイルスとかマルウェアといったものについても何億回といったトレーニングを続けています。そうすることによって、CylanceのAIプラットフォームは「想定」を立てず、ファイルの要素から常に「良い」か「悪い」か

です。擬陽性(過検知)に近い、親類のようなファイル、これらをDNAによって許可をすることができるといえます。つまりハッシュ値の分だけのホワイトリストよりも優秀だということになります。

## ■ Cylance の AI エンジンが『何を』学習しているのか？

岡田：そうするとですね、もう少し突っ込んだ質問をしたくなるのですが… AI は何を学習しているのかということに非常に興味がありますね。今日のデモンストレーションで見たとおり、マルウェアを実行させる前にその実行を止めるということは、実行する前のバイナリを解析していると、簡単にいえばそういうことになりますよね。一体どういう部分を学習して AI エンジンでトレーニングしているのかを、ここだけの話ということで聞かせていただきたいなと。

Nicholas：Cylance では、ファイルそのものを解析します。ファイルを動作させるのではなく、静的な状態でのファイルを学習します。ファイルは、マルウェアだけを学習するのではなく、良いファイル、悪いファイル、PUP ファイルなど5億のファイルを学習させます。ファイルの学習では、機械学習の技術を利用して個々のファイルの特徴を学習します。例えば、ファイルタイプ、ファイルのアイコン、ファイルのサイズといったものになります。特徴の数としては、多いファイルでは 600 万を超え

るものがあったり、少ないものでは数十万しかないものもあります。ファイルの多くの側面を見るということと、あまり見過ぎないという、そのバランスをとっていくことがとても重要になります。弊社では、ディープラーニングの技術を使い、ファイルの特徴から最終的にこのファイルがマルウェアなのか、正常なファイルなのか、または PUP なのかという分析を数理的に実施します。この結果の集合体のアルゴリズムをクライアント側にインストールします。クライアント側は新しい脅威が侵入してきた時に特徴点をこのアルゴリズムを利用して数理的に瞬時に分析し、ファイルが正常か、マルウェアか、PUP かを判断します。数理的に判断することで非常に早く処理することが可能になります。

徳丸：ちょっとまだ狐につままれたような気分です…例えば非常に巨大なマルウェアもあるわけですが、そういうものも特徴を逃さず見つけられたりするのでしょうか。

井上：そうですね、Cylance の中には先ほど申し上げたように、だいたい5億のサンプル

があり、2億5000万が良いもの、2億50000万がそうじゃないものとなっているわけです。もちろん、中には大きいもの・小さいものがあります。これらのファイルの特徴を見つけていく。弊社ではそれを DNA と呼んでいます。つまり、ファイルの DNA を勉強して、それが AI でクライアントの方に反映される、という形です。ここが大きなポイントかなと思います。



## ■ アップデートは半年に1回。それはどうして？

岡田：だんだん数学的になってきたな、という気がします。では、半年に1回とアップデートのスパンが長いですが、それだけ長いと新たな脅威やまさかの発想によるウイルスが出てくることもありえると思うのですが、

その辺りはいかがでしょう？

Nicholas：そのようなマルウェアが出てくる可能性はあります。そのためすり抜けた場合には、ブラックリストで登録してマルウェアをブロックすることが一つの対策になります。すり抜けたマルウェアを Cylance 社にフィードバックして頂くことにより、現状の数理モデルに個別数理モデルのセントロイドで登録することですり抜けたマルウェアやそのマルウェアに近いファイルをブロックするなどの対処が可能です。次の数理モデルではすり抜けが発生しないアップデートを行います。また、すり抜けたマルウェアを調査するという点では、本日のパートナーである MOTEX の LanScope Cat を利用することで

脅威に感染する前後のログを把握したり、すり抜けてしまった感染の行動などを調査して分析することも可能です。

岡田：なるほど・・・聞けば聞くほどさらにいるんな質問をしたくなるのですが、時間がきたようですのでこのセッションは一旦ここで終了したいとおもいます。徳丸さん、そしてニコラスさん、井上さん、ありがとうございました。





# ガバナンスセッション 2020年に向けて日本のセキュリティは どうあるべきか

Unbelievable Tour Talk Session Round 2

## Unbelievable Tour in Japan

### Talk Session Round 2

Round2 では、第一線でセキュリティに携わっている 4 名が登場。企業におけるセキュリティの実情や、Cylance / プロテクトキャットの登場で企業のセキュリティがどのように変わるのか、といった未来の話まで幅広くディスカッションいただきました。



### Speakers - 登壇者紹介 -



OWASP Japan 代表 /  
株式会社アスタリスク・リサーチ  
岡田 良太郎 氏



デロイトトーマツ  
リスクサービス株式会社  
代表取締役社長  
丸山 満彦 氏



株式会社ラック  
サイバーセキュリティ事業部  
サイバー救急センター長  
内田 法道 氏



エムオーテックス株式会社  
CISO 兼執行役員  
中本 琢也

## ■ 増加するサイバー攻撃 被害の状況とその傾向とは？



岡田：丸山さん、温めておきましたよ。

丸山：先ほどのトークセッションを聞いていて、人工知能の続きを話したくなってきましたよ。ちょっとだけ人工知能の話しをさせてもらおうと、たぶん、Cylance の人工知能を打ち破るコンテストみたいなものができるんですよ。「人工知能に人間が勝とうぜ！」みたいな。そういうプロジェクトがハッカー達の中で走る、そんな感じがしてきましたね。でも後半はガバナンスの話しをしるということですよ。ね・・・。

岡田：ということで凄い切り口を持ってやってこられました。デロイトトーマツリスクサービスの丸山さんです。そして、内田さん。

内田：ラック サイバーセキュリティ救急センターの内田です。サンドボックス対策が進んできましたが、アンチ AI もこれから進むのではないかと考えて前半聞いていました。

岡田：またキレイな感じでやってこられました。ラックの内田さんです。宜しくお願いします。そして、これは私からお願いして出ているのが、MOTEX のなんと CISO、中本さんです。

中本：MOTEX CISO の中本と申します。10年間開発を担当しておりまして、その後、2年ほど情報シスをしておりまして。今年から CISO という立場で活動していますので宜しくお願いします。

岡田：宜しくお願いします。それでは早速本題ですが、内田さんに資料をご用意いただきました。そもそも企業がどういう戦いを強いられているのかということがまとまっていますね。やはりマルウェアが多い状態ですね。

内田：そうですね。駆け込み寺的にお電話いただきますが、最近ではやはり 5 割ぐらいは

マルウェア絡みです。その中でも年金機構だったり今年おきた大きな情報漏えい事故の件で出てきた APT だったり、最近ばら撒かれている不正送金、ランサムなど色々なお問い合わせを頂いている状況ですね。

岡田：なるほど。これは今日の文脈でいくと、例えばマルウェアディテクションみたいなことを考えた時に、APT・不正送金・ランサムとかが半分以上を占めていますね。そして、41% でその他とありますが、その他というのは具体的にどういうものなのでしょうか？

内田：アドウェアといったものや結果的に種類が特定できなかったというのも含んでいます。岡田：なるほど。ノンカテゴリーといったものもあるんですね。

内田：そうですね。結局は何か開いてしまったけれども、アンチウイルスソフトが反応しないので調べてもらいたいという問い合わせは

その他に入っている状況ですね。

岡田：なるほど。世間を賑わせているニュースもマルウェアきっかけで見つかることが多いですが・・・そこで丸山さん、侵入されるバリエーションは増えてきていますか？

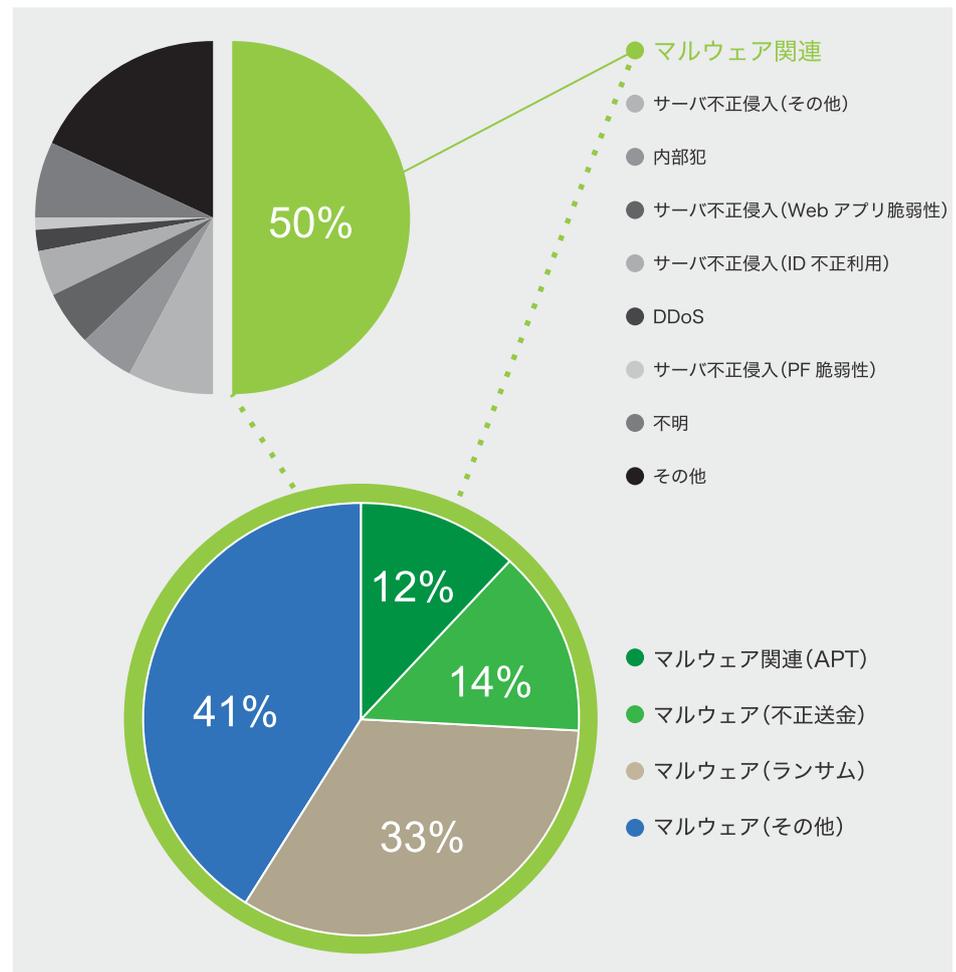
丸山：そうですね。我々のなかでも、問い合わせがあって調べてみると、色んな入り口から入ってきているケースがありますが、やはり Web 経由が多いですよ。

岡田：Web 経由？

丸山：はい、実際は経路が分からないというのも結構ありますが、それはログとっていない時で、しっかりとログとっている会社は分かりますよね。

### LAC サイバー救急センター 出勤実績ベース

対象期間：2015.4～2016.8



岡田：フリーソフトや Web サイトでも安全なんだけど、時々凶悪なアドウェアがやってきて、突然感染みたいな・・・

丸山：ありますね。広告の中に仕込まれているから、そこをクリックしてしまうと勝手にダウンロードしてしまう。だから URL だけで判別するのはなかなか難しいですね。

岡田：そうなんですよね。その場合、リスクに対する対応って定石的にはどんな感じなんですか？

丸山：セキュリティ対策の定石は予防です。でも、予防では防ぎきれない、発見・対応のところに力をいれる会社が最近多いですね。

岡田：業界によって投資額は変わってくるのではないかなと思いますが、内田さんの APT 事案の業種別割合の資料を見ると、IT はやや多いですが、結構幅広いですよ？

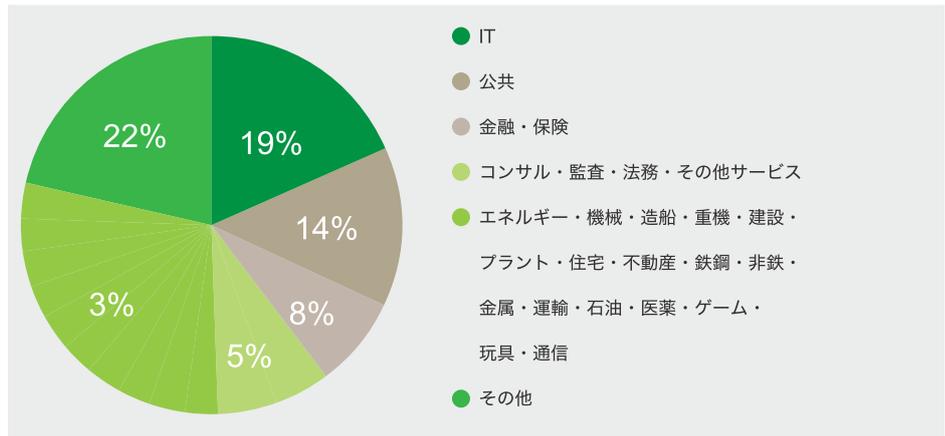
内田：IT 系が多い理由としては、大きな会社の SI や子会社さんからの問い合わせがあったりするので母体はどこかの業種といった

ケースであったり、エンドユーザーを抱えている SI さんから「お客様先で事故がおこっちゃったんだけど」ということでお問い合わせをいただくケースが多い状況です。金融・公共は何かあると事故報告しなくてはいけない業界ですので、色々お問い合わせいただくケースが多いのかなと思っています。その他、

エネルギー・造船・機械・鉄鋼・運輸・石油・医薬・ゲーム・通信などのインフラ周りや、技術情報をもっている会社さんが狙われているのが APT に限って取ったときに出る特徴ではないかなと思っています。

## LAC サイバー救急センター 出勤実績ベース

対象期間：2015.4~2016.8



## リスクが下がると工数は上がる!? 嬉しい悲鳴は CSIRT から

岡田：こういったものの防御や、あるいは何かあった時の対応は今後どう変わっていくのかなという視点で今日は楽しませてもらっています

が・・・では、プロテクトキャットによって企業の CSIRT (Computer Security Incident Response Team) は楽になるのでしょうか？

中本：そうですね、今回 LanScope Cat が Cylance と連携をしましたが、実はその前から「マルウェアに感染してしまった」「ランサムにかかりました」となった時に、Cat のログを見ると、ランサムウェアのロッキーが暗号化している履歴がずらっとログに残っているんですよ。

岡田：その様子をつぶさに見ているわけですね？

中本：リアルタイムには見ていないですけど、ログを遡るとその前にはブラウザを開いて、このサイトを見て感染して広がっていったということが分かるので、対策を取る前の原因特定に Cat は使われていたという背景があります。今回の連携で、マルウェアの侵入を事前に止め、

さらにどこからログを見れば良いのかというポイントが Cat だけで分かりますので、より活用しやすくなるのではないかなと思っています。

岡田：どうですか丸山さん、この信憑性は？

丸山：逆だと思いますよ。プロテクトキャットがあると CSIRT が忙しくなりますよ。それは・・・今まで見つけてないから！今まではマルウェアが入ってきてても何も見てないから（気づいてないから）暇なんですよ。でも、プロテクトキャットを入れるとどんどん見つけてくるじゃないですか、見つけてきたら調べなくちゃいけないでしょ、調べたら「こういうことがありました・・・」って報告書を社内向けに作らないといけないでしょ・・・もう忙しくなりますよ。これはまずいかもしれない！！

岡田：今、会場の皆さんは結構シンパシー感じていますよ。でも反対に内田さんのところに電話がかかってくる率は下がりそうですね。

内田：私の電話が鳴る機会が減るという意味で

は嬉しいことですね。皆さんで原因を調べられて、初動の判断ができるという意味であれば、いわゆる町のお医者レベルの病気なら皆さんのところで対応いただいて、大手術が必要な APT とかは私たちが対応する。分業制みたいなことができる、非常に世の中うまくまわっていく可能性はあるかなと思いましたね。

岡田：検知率が上がると、検知できるかっていうことが論点じゃなくなってきましたよね。そうするとその後、どう捌いていくのが正しいプロセスなのかなど、それこそ丸山さんがおっしゃるように報告書を書くことそのものも AI でやっていかないといけないのではないかなと思いますね。

丸山：それ、MOTEX にとって次のビジネスのヒントですよ。次の製品に入るとすごく良いと思いますね。

## 進化する LanScope Cat

### 重要なのは操作ログの活用と報告しやすい環境づくり

中本：実は Cat のログをもっと活用できるのではないかと話しが話題になっていて、今まさにお客様 5 社と共にログをどうやって活用していくかという基準を作っています。セキュリティインシデント対応レベル表と申しまして、例えば、何かあった時の事後対策としてログを取っているだけではレベル 1、定期的な運用チェックやプロセスに管理部門や役職者、経営者含めて事前対策の対応が整っている場合はレベル 2、といったものを作り上げている段階です。

岡田：ここに Cylance のディテクションみたいなものが出てくると、更にその後のアクションをどうするのかといったところを発展させていけないといけません。

中本：そうですね。ここまでは第一期で、今は第二期を進めています。実用でどうやってレベルを上げていくのかといったところをこれからの第二期としてお客様と追及していきたいと考えています。

岡田：こういう基準は非常に重要ですが、具体的に企業の CISO、あるいは CSIRT チーム

というのはどういうアクティビティを大事にしていく必要があると思いますか？

中本：実は私も最初は勘違いをしていましたが、「感染した＝悪い」というのがありました。でも、そしたら隠してしまいますよね。その後、一週間や一ヶ月後に発覚する。そしたらもう原因も分からないですし、他にかかる人が増えてしまうかもしれない。発見したことを報告することは良いということにして、「あなたを守るためだよ」という文化・風土を作っていくことが重要だと思いますね。

## 2020 年以降 AI と人との上手な付き合い方

岡田：ちょっとここだけの話のコーナーとして、なにか会話のヒントをいただければ思うのですが・・・。

丸山：本題からは逸れているかもしれませんが、景気について話したいですね。

岡田：景気？

丸山：僕らセキュリティ業界というのは広告業界以上に不要不急かもしれないと思います。だから景気が悪くなると経営が傾くのではというのが常にあって、2020 年まで景気もつか、2020 年以降大丈夫かという問題が気になりますね。

岡田：この問題を真剣に考えている人は少ないかもしれませんね。

丸山：今後のキーワードとして出てくるのが AI ですよ。もしかしたら、攻撃者側が AI を使って、見つからないようなマルウェアを作ってくるとか、そんなこともあると思います。なので、そういうところに対して人間対人工知能の戦いではないですが、いかに人工知能を人間がうまく活用するか、対決姿勢というのをうまく活用していくのが僕の考えているなかでは重要なポイントかなと思います。

岡田：内田さんいかがですか？

内田：AI に棋士も負けつつありますが、AI に対して違う打ち方をすると過去に学習して

なかったので対応できないということもあるわけですよ。それは Cylance の AI でも同じことがあるかなと思ってます。今は 99%ですけど攻撃者側が学習して検知されないマルウェアを生み出す。その時に、エンドポイントが 2020 年までにどう進化しているのかが重要になってきますね。次世代型と言われる製品もリリースから 2～3 年程度で普及してしまうので、次世代型をリリースした直後に次々世代型を検討しなくてはならない状況になっているのではないかと想像しています。

岡田：人間の中にあるクリエイティビティみたいなものが益々必要になってきますし、パターン化されているものはどんどん AI になっていくと感じますね。中本さんいかがですか？

中本：AI の流れで、他で話した事が無いことだけの話ですが、Cat のログを AI にかけて解析をするということ、実は 2 年前から進めています。もう少しお時間いただきますが、いち早く皆様にログと機械学習によるセキュリティの価値を提供できればと思っています。コンセプトは、「人が判断すべきところに集中できるように」です。AI × ログというところはメーカーとしては目指すべきところですし、自分自身も使ってみたいなと思っています。

岡田：多くの場合、リスクはパッと特定できた



らいいですし、リスクのあるような動きを見つけたら降りかかってこないようにプロアクティブなコントロールというものに反映させる仕事をするというのは AI で非常に重要なポイントだと思います。端的に言えばブロックするとか、特定時間ブロックするとか、そういった事柄を手動ではなく自動でやっていくことです。今後、LanScope Cat がやらないといけないことがどんどん増えていってる感じでも楽しみですね。期待しています。またあつという間に時間がきてしまいました。丸山さん、内田さん、中本さん、ありがとうございました。



## アンビリーバブルツアーの反応 - Twitter #UBTJ より抜粋 -

- #UBTJ Cylance motex すごいね！ Protect Cat アンビリーバブルだよ。オフラインでも使用できてシグネチャーではなく AI で予測検知！デモも他社は感染しているのに全て検知削除。入れたいなあ
- プロテクトキャット（サイランスの OEM）見てたら、アンチウイルスも UTM も今のままでは気休めにしかになってないのではと本気で思った。セキュリティインシデントは起きてしまう前提で考えるべきだし、そう考えると導入すれば更に良くなるものではなく、導入する必要のあるものだな。#UBTJ
- #UBTJ Cylance は、スクリプトも対応しているとのこと。サンドボックスやホワイトリストでは対応しにくいものなので、ちょっと驚き。
- Funny malware is still malware.@cylanceinc&@MOTEXPR won' t let the joke be on you #UBTJ
- サイランス凄ってなりましたわ～。#UBTJ

#UBTJ



## プロテクトキャットの反応 - アンケートコメントより抜粋 -

- 検知の速さに驚いた。
- 組み合わせにより**完全に他社より強い製品**になったと感じた。
- **ロードマップ**も聞いたのは非常に有意義だった。
- **マルウェア感染時（防御時）の操作記録**はありがたい。
- LanScope Cat と組み合わせることで**両者の良いところがより強化**されている。
- **他社との比較デモ**が大変分かり易かった。
- **オンプレミスに期待**している。
- 実際に目の前でマルウェアを動かして検知させるという方法はユニークで面白かった。大変実感がわいた。
- **デモが大変分かりやすく如何に優れているか実感**できた。
- **大変興味深い内容**だった。
- AI の活用は**気になる**。

VOICE