

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郎、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。



# SPECIAL INTERVIEW

## 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

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せていただきます。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効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

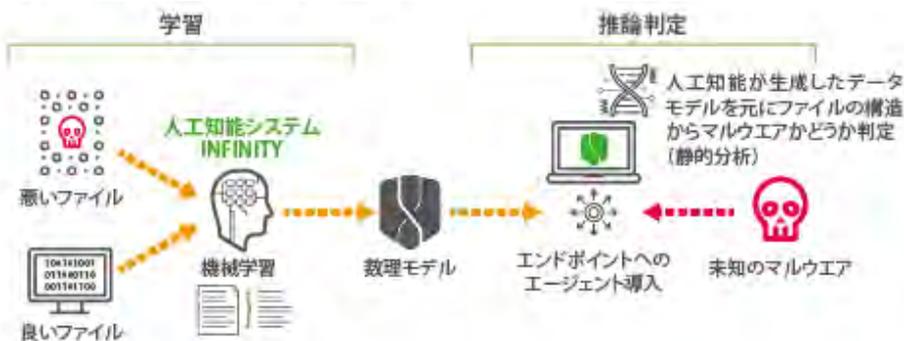
— CylancePROTECTを選ばれた理由は、AIを搭載した製品だからでしょうか。

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るの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。

### ▼CylancePROTECTの予測防御の仕組み



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。

## そのAIは本物か。「初見の」ウイルス検知率を検証して見破る

— 実際にCylancePROTECTの検証を実施されたとお聞きしました。その内容と結果について教えてください。

堂領 国内販売直後から17カ月間にわたる徹底した検証を実施しました。用いた540種類のウイルスのうち、500種類は過去に発生した既知のウイルスについて検証を行ったものです。CylancePROTECTは、これらを100%検知するという凄まじい結果を残しました。ところが、真に驚くべきは残り40種類のウイルスに対する検知率です。これらは全て「未知のウイルス」に該当します。このうち39種類ものウイルスが、この世に出現した瞬間に、瞬時に検知されたのです。衝撃的な出来事でした。

今日ではウイルスは、ほぼ“使い捨て”です。亜種や変異型が毎秒のように出現し、その流通時間は最短で数時間以下というほどに短命です。数時間後にウイルスを検出できたところで意味はありません。ランサムウェア被害ともなれば特にそうです。

今日のウイルス対策ソフトに求められている能力とは、世の中に未知のウイルスが出現した瞬間に「初見で」確実に検知ができる能力なのです。

従来型製品の各社は、いずれも「ウイルス検出率は100%である」と広報していますが、そこには「いつの時点をもって」という時間軸の情報が抜け落ちています。

ウイルスが出現してから、かなりの日数を経て実施される検出テストに意味はありません。さらに言えば、ウイルス検体を『VirusTotal』にアップロードして得られる「Cylance」項目の検知結果と、自身で CylancePROTECT を用いて行う実機検証では検知結果にも違いがあります。だからこそ、自身で検証を行うことがとても大切なのです。

**丸山** エムオーテックスでは、サイランスから OEM 供給を受け『LanScope Cat』のオプション機能『プロテクトキャット』として

お客様に提供しています。さらにこの製品の国内におけるファーストユーザー（2015年12月導入）であり、導入に際しては我々も独自の検証を行いました。

具体的には VirusTotal から出現後 3～5 日を経たウイルスの検体 100 個を入手。それから 100 個を難読化し、100 個の未知のウイルスを作成しました。

さらに、実際に弊社への攻撃で使われた検体 18 個、計 218 個のウイルスを用い、シグネチャ型のツールと CylancePROTECT の検知比較を行いました。

この時、シグネチャ型は最新のパターンファイルを適用したのに対し、



エムオーテックス株式会社  
経営企画本部 課長 MOTEX-CSIRT 丸山 悠介

#### ▼MOTEX が行った検証結果

(2015年11月時点：製品A～Dは最新バージョン、Cylanceは検証日から半年前のモデルで検証)

製品名	ウイルス検知率 (118種)	難読化ウイルス検知率 (110種)
製品A	95.8% (113/118)	15.0% (15/100)
製品B	96.6% (114/118)	6.0% (6/100)
製品C	97.5% (115/118)	7.0% (7/100)
製品D	100% (118/118)	11.0% (11/100)
製品E	11.9% (110/118)	95% (96/100)
製品F	97.5% (115/118)	33.0% (33/100)
<b>プロテクトキャット</b> <small>(CylancePROTECT)</small>	<b>100%</b> (118/118)	<b>100%</b> (100/100)

CylancePROTECT ではモデルの更新間隔が1年～半年程度だったため、あえて半年前のモデルを使用しました。

結果は、CylancePROTECT では218個すべてを検出したのに対し、シグネチャ型は既知のものに関して95%程度の検知率が得られたものの、亜種として作成した未知のウイルスについては最大でも30%程度の検知率にとどまりました。ベンダーがどのような内容をPRしようとするのを鵜呑みにせず、自ら検証してみることの重要性を痛感した結果でした。

### “Test for Yourself” をキャッチフレーズに検証を支援



Cylance Japan 株式会社  
最高技術責任者 乙部 幸一郎

— ユーザー企業自らの検証が重要とのことですが、一般の企業においては、やや敷居が高いとも思われます。

**乙部** サイランスでは、“Test for Yourself” というメッセージを発信しており、お客様における検証実施の支援も行っています。ウイルス対策ソフトの検証テストを実施するためのガイドブックを配布し、その中で検証環境の構築の仕方から、チェックすべきポイントを詳述しています（Webより入手可能）。

**丸山** 検証を通じて運用管理面の感触をつかむことも重要です。現在は多層防御がトレンドですが、ツールは導入するだけで効果を発

揮せず、機能理解に始まり、運用に人的工数とスキルの問題が発生します。そのため、製品の選定に当たっては、機能だけでなく効果を発揮させるためのマンパワー・スキルなどの要素も総合的に捉える必要があります。CylancePROTECT は、より少ない労力で最大限の効果を発揮し得るソリューションであると考えています。また、当社の提供する IT 資産管理・内部不正対策ツール『LanScope Cat』を併用くだされば、CylancePROTECT が検知したファイルが、従業員のどの操作によって侵入したかといったことも明らかにできるなど、運用管理上の付加価値を高めていただけます。

— CylancePROTECT は、現時点でスクリプト系やマクロ系のウイルス検知に対応していません。どのようにお考えですか。

**堂領** 主に電子メールに添付される形で攻撃に用いられるスクリプトやマクロは、多くが「ダウンロード」と呼ばれるものです。ダウンロードは、実際に攻撃を担当する「ウイルス本体」をインターネット上から入手する役割を担います。検証結果を明かせば、従来型製品の多くはダウンロードもウイルス本体も初見時において、ほぼ検知ができませんでした。重要なのは、ダウンロードが落ちてくるウイルス本体を初見で即座に検知できるかどうか。CylancePROTECT は、それが可能な製品です。

**乙部** サイランスでも、スクリプト系、マクロ系の攻撃にもモデルベースで対応していけるよう、現在準備を進めています。攻撃に対する素早い対応で、さらなる安心をお客様に

提供していきたいと考えています。

— いわゆるファイルレス攻撃についてはいかがでしょうか。

**堂領** CylancePROTECT にはメモリ領域の保護機能やスクリプト制御機能があり、ファイルとしての実体を持たない特殊な攻撃に対しても効力を発揮します。適用を検討されても良いでしょう。

— EDR 製品については、どのようにお考えですか。

**堂領** 従来型ウイルス対策ソフトの弱さを補完する目的でクライアントに導入する製品であり、ウイルス駆除の機能を持たない製品が大半です。CylancePROTECT の導入を先に行い、その後が必要であると判断すれば、『CylanceOPTICS』という EDR 機能を追加導入すれば良いでしょう。

— 最後に一言お願いします。

**堂領** セキュリティ人材が不足している状況は、簡単には改善しません。だからこそ圧倒的な性能を持つ製品を導入し、不足する防御力を強化する対策が必要です。一騎当千のセキュリティ対策製品とは、業界の歴史を見ても滅多に出現しない稀有なものです。ぜひ一度、無料で CylancePROTECT を体験されてください。

今、目の前には、世界中のセキュリティ技術者が渴望した（※1）、半世紀に1度しか出現しない最高峰の性能を持つ製品があるのです。製品を検証し、選ぶ権利は皆さんにあります。ぜひ自らの熱意をもって手を伸ばされ、組織に安全と安心を導いてください。

※1:CylancePROTECT は SANS コミュニティが選出した「2016 年度 エンドポイント防御製品部門」で大賞を受賞している。

[ 関連リンク ]

- ・ Test For Yourself 自分の手でテストをするという意味 : [https://www.cylance.com/ja\\_jp/blog/jp-time-to-test-for-yourself.html](https://www.cylance.com/ja_jp/blog/jp-time-to-test-for-yourself.html)
- ・ 読めばわかる！次世代マルウェア対策のテスト : [https://pages.cylance.com/ja\\_jp-testing-for-dummies-eb.html](https://pages.cylance.com/ja_jp-testing-for-dummies-eb.html)
- ・ プロテクトキャット導入ユーザー様の声を集めたレポート : <https://go.pardot.com/l/320351/2018-01-11/8w99m>

エムオーテックスは、国内唯一の Cylance OEM パートナーです。LanScope Cat は CylancePROTECT を新機能『プロテクトキャット』として統合したことで、外部・内部に潜む企業のセキュリティ課題を解決します。詳細は Web をご覧ください。

[プロテクトキャット](#)

[ 問い合わせ先 ]

■Cylance Japan 株式会社

TEL : 03-6386-0061

E-mail : [infojapan@cylance.com](mailto:infojapan@cylance.com)

URL : [www.cylance.co.jp](http://www.cylance.co.jp)

■エムオーテックス株式会社

TEL : 0120-968-995

E-mail : [sales@motex.co.jp](mailto:sales@motex.co.jp)

URL : [www.lanscope.jp/cat/special/protectcat/](http://www.lanscope.jp/cat/special/protectcat/)