“隙間のない”セキュリティ環境を構築する重要性とは。真の意味での「無害化」を実現 | OPSWAT × FileZen S

目次

IPA（情報処理推進機構）が公表した「情報セキュリティ10大脅威 2023」を見てみると、ランサムウェアや標的型攻撃、サプライチェーンの弱点を悪用した攻撃が、2022年に続き、ますます脅威になると指摘されています。実際、企業や団体におけるランサムウェアの被害件数は増加傾向にあり（※）、情報資産を守るために多方面でのセキュリティ対策が求められています。

※参照：警視庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

そんな中、創業以来グローバルなセキュリティ市場をリードし続けてきたOPSWAT, Inc.（以下、OPSWAT）は、高品質なセキュリティソリューションを展開し、世界各国の企業やインフラを守っています。

今回は、同社の日本法人であるOPSWAT JAPANのチャネルセールス ディレクター 皆川文哉氏にお話を伺い、企業がセキュリティで抱えている課題、OPSWATのソリューションによって期待できる効果、そしてソリトンシステムズが提供するソリューションとの関わりについてご紹介します。

どんなセキュリティにも隙間が？企業が抱える課題の本質とは

デジタル化が進行し、働き方も多様化してきた現代の企業にとって、情報セキュリティ対策の重要性はますます高まっています。ランサムウェア、サプライチェーン攻撃といった脅威の高まりから、社内LANだけでなくリモートアクセスやクラウド環境を含めて対策する必要がある中で、日々セキュリティの“継ぎ足し”を迫られているのではないでしょうか。

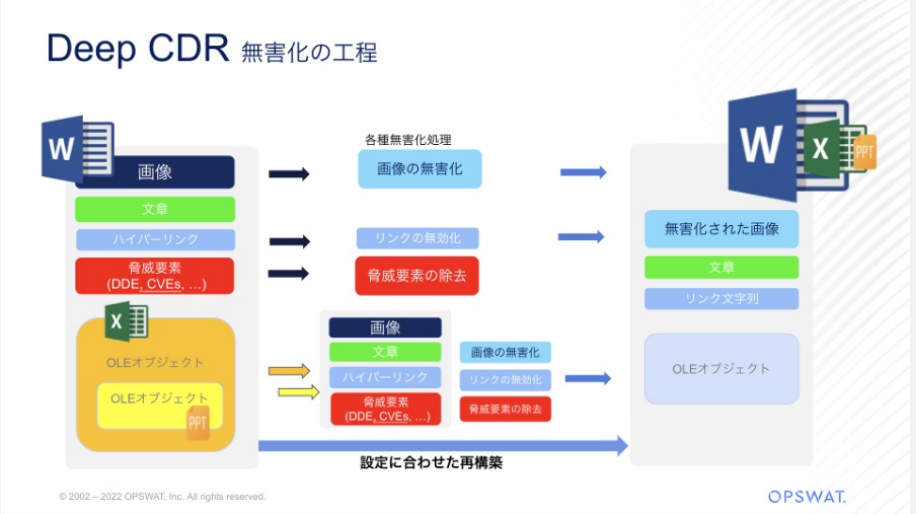
企業には、目的や場所ごとにたくさんのセキュリティソリューションが導入されていますが、ひとつひとつが連携しておらず、ばらばらに動作していることが多くあります。その原因はセキュリティ製品を個別に購入し、異なるベンダーから入手していることにありますが、これは企業が抱える大きな課題のひとつです。

たとえば、ある製品は特定の脅威を検出することができ、別の製品は同じ脅威を検出できない場合、情報が連携されなければ侵入経路次第で攻撃が通ってしまいます。製品同士の連携が不十分な環境で最新のソリューションを個別に導入し続けても、全体的なセキュリティの強度はあまり高まっていきません。

このような状況について、皆川氏は次のように警鐘を鳴らします。

“我々の調査によると、1企業当たり60～70のセキュリティソリューションが導入されていますが、それぞれのソリューション同士が連動していないケースが少なくありません。そのため、その繋ぎ目の部分や隙間が空いている部分に、さまざまな脅威が入ってきてしまう可能性があります。”

（図１）



それではどのような対策を行えばいいのでしょうか。解決策のひとつとして提案できるのが、OPSWATが提供するソリューションです。

必要なセキュリティ対策を一気通貫で提供し、データに含まれるあらゆる脅威を排除する

OPSWATは、接続してくるものを常に信用せず、すべてのファイルやデバイスを検証する「ゼロトラストセキュリティ」の理念のもと、長らく世界中の企業・重要インフラをサイバー攻撃から守ってきました。ITだけでなく、近年ではOT（オペレーショナルテクノロジー）ネットワークにおいてもOPSWAT製品の導入が進んでおり、官民問わず高い評価を受けています。

OPSWAT製品が全世界で評価を得ているのには理由があります。まず挙げられるのが、組織内のセキュリティ環境を整える際に必要なソリューションを、一気通貫で提供できる点です。マルウェア検知から無害化、DLP（Data Loss Prevention）、サンドボックス、脅威インテリジェンスなど、包括的にセキュリティソリューションを自社提供しており、それぞれが密に連携されているため、攻撃の侵入を許すような“隙間”や“抜け道”がありません。これは、同社が自社製品の開発だけでなく、M&Aを行った企業のソリューションを再開発して自社製品群に組み込み、機能を拡張し続けたことによって得た独自の強みと言えます。

OPSWATのソリューション群の中心となるテクノロジーが、「MetaDefender Core」です。OPSWATが提供するほとんどすべてのセキュリティエンジンがこの「MetaDefender Core」に詰まっており、世界各国の企業やインフラの安全を支えています。

「MetaDefenderCore」は、具体的には以下のような機能を提供しています。

- **Multiscanning（マルチスキャン機能）**

「MetaDefender Core」に搭載されている最大“32種類”の商用マルウェア対策エンジンを使って、脅威を検知する機能です。マルチスキャンの特徴について皆川氏は以下のように話します。

“「MetaDefender Core」は32種類ものマルウェア対策エンジンの同時稼働により、1日何万と生まれてくるマルウェア攻撃にも、ほぼ100%の検知率を実現しています。それぞれのエンジンは、開発国や使用国によって脅威の特性や種類が異なるため、基本のアルゴリズムにも違いがあります。そのような世界中で作られた商用エンジンを複数使用し、何層ものスキャンを実施することで、1つや2つの特定のエンジンだけでは不可能な、持続的で高い検知率を実現しています。”

- **DeepCDR（ファイル無害化機能）**

従来のファイル脅威対策では、なんらかの方法でグレーと判断された時点で、そのファイルが重要なものであっても開くことはできず隔離となったり、ユーザーによっては脅威を無視して開いてしまったりという状況が起こっていました。

しかし、同社の「DeepCDR」は根本的に異なると皆川氏は言います。

“当社の無害化処理は、ファイルに脅威があるかないかにかかわらず、ファイルを完全に分解し、脅威の要素となり得る部分を排除し、ユーザビリティを維持したまま再構成します。たとえばワードファイルであれば、画像、文章、リンクなどさまざまな要素で成り立っています。その細かい成分を一つ一つ分解し、脅威要素だけを抽出して削除。その後、ファイルを再構築します。そうすることで、ユーザビリティを維持したまま、安全なファイルとしてオリジナルファイルと変わらず利用できるのです。今まで捨てざるを得なかったファイルも、安全なファイルに変換できる革命的な技術です。画像ファイルのメタデータなども残せるので、写真の撮影日や位置情報もそのまま利用することができます（図1）。”

また、設定画面でユーザーごとのカスタマイズも容易にできると皆川氏は話します。

“企業・団体によっては、「複数の操作をまとめて呼び起こす“マクロ”機能は分解しないでほしい」という声があります。当社の製品は、そのようなユーザー様のご要望にも応え、たとえばエクセルのマクロだけは外して無害化するなど、こと細かにカスタマイズできます。カスタマイズは、アプリケーションごとに詳細に行うことが可能です。”

さらに驚くべきことに、「MetaDefenderCore」の無害化は一般的なファイル形式に留まらず、140種類以上の形式に対応しています。日本では、特に慎重に取り扱わなければならない個人データをやり取りするヘルスケア領域などで、同社の無害化技術が多く採用されています。

- **DLP（Data Loss Prevention）**

OPSWATのDLPでは、ファイルデータに含まれるマイナンバーやクレジットカード番号などのセンシティブな情報を検知して、塗りつぶすなどの処理を施すことができます。普段のやり取りの中で起こりがちな機密情報の漏えいから組織・企業を守りつつ、業務を継続させることが可能です。

この機能について、皆川氏は以下のように説明します。

“指定された文字コードを発見するとそこだけ塗りつぶしたり、その文字コードが含まれる場合にはファイルの送信を止めたり、アラートを鳴らしたりすることができます。Officeファイルに限らず、画像やPDFファイルにも対応しています。”

これらに加え、脆弱性評価や脅威インテリジェンスといった機能も備える「MetaDefender Core」は、“単体で多層防御を実現”しています。マルウェアにとっては、入ってきてから出ていくまでにあらゆる検査が行われ、“逃げ場がないセキュリティソリューション“であるといえるでしょう。

連携ソリューション「FileZen S」にファイル受け渡しを集約し、検知・無害化をより確実に

MetaDefender Core」のマルチスキャンや無害化処理の機能は、ソリトンが提供する「FileZen S」のエンジンに組み込まれています。MetaDefender Core」のマルチスキャンや無害化処理の機能は、ソリトンが提供する「FileZen S」のエンジンに組み込まれています。「FileZen S」はネットワーク分離環境において、承認フローや証跡を残しながらファイルの受け渡しを安全に行えるソリューションです。OPSWATと連携することで、ファイルに潜む脅威を確実に排除することが可能になり、安心してファイルを受け渡すことができます。

皆川氏はOPSWATと「FileZen S」が連携する意義について、次のように話します。

“現在のセキュリティ技術は、すでにネットワークに侵入したマルウェアを検知する後追いのものが多いです。そうではなく、そもそもマルウェアを組織内のネットワークに入れないことが、被害を防ぐために重要な考え方なのです。その点で、社外やインターネット等からのファイルの受け渡しは「FileZen S」に任せ、OPSWATの技術で確実にそのファイルを安全なものにするというこのソリューションは、非常に意義のあるものになっています。“

現在、OPSWAT JAPANとソリトンは、「FileZen S」の展開に注力しており、すでに官公庁や地方自治体などを中心に導入が進んでいます。導入が進んでいる理由について、ローカライズがうまくいっている点もあると皆川氏は話します。

“OPSWATが無害化処理できるファイルは140種類以上ありますが、国内で販売されているワープロソフトで作成されたファイルや、ローカルなCADファイルなどにも対応しています。
さらに品質向上のために、何万という日本語ページの処理結果を解析する専用プログラムも開発し、品質を確保しています。OPSWAT製品は日本でさらに使いやすくなっていきます。”

最後に、皆川氏は今後の展開について以下のように力を込めます。

“OPSWATの特筆すべき強みは、無害化機能です。一般的な製品による無害化は特定のデータだけをただ削除する方式で、図表等の埋め込みデータは削除され、元ファイルと情報が異なってしまうだけではなく、すべての構成要素から脅威を取り除いてはいません。当社の「無害化処理」であれば、ファイル構成要素を認識して解析し、脅威要素の完全削除・そして再構築を行うため、ファイルの見た目や中身は無害化の前後で変わらず、完全に安全なファイルとなります。「FileZen S」には、当社のそうした特徴的な技術が搭載されています。今後は病院や金融など、デジタルファイルの受け渡しなどをビジネス上で頻繁に行うような民間のお客様にも有効活用していただきたいと思っていますので、訴求活動をソリトンさんとともに積極的に行っていこうと考えています。”

謝辞

OPSWAT JAPAN様、インタビューにご協力いただき誠にありがとうございました。

OPSWAT JAPAN様と連携することで、お客様の希望を叶えるソリューションをご提供することができました。ソリトンは、FileZen Sをはじめとしたネットワーク分離環境向けソリューションなど、お客様の「困った」を解決するセキュリティソリューションをこれからも提供していきます。

ネットアテスト

「ネットアテスト」は、企業ネットワークに関わる全ての方のためのサイトです。安心・安全な環境を実現したい情報システム担当者様、確かなシステムを提案されたいインテグレータ様に向けて、運用の効率化やセキュリティ強化の方法などをお届けしていきます。

サイトはこちら

OPSWAT JAPAN 様

OPSWATは、重要インフラを保護しています。私たちの目標は、マルウェアとゼロデイ攻撃を排除することです。私たちは、すべてのファイルとすべてのデバイスが、脅威をもたらすと考えています。脅威は、入口、出口、内部のすべての場所で対処する必要があります。「脅威の防御」と、「安全なデータ転送とデバイスアクセスのプロセス構築」に、焦点を合わせている当社の製品により、侵害されるリスクを最小限に抑える、生産的なシステムが実現します。

お問い合わせはこちら