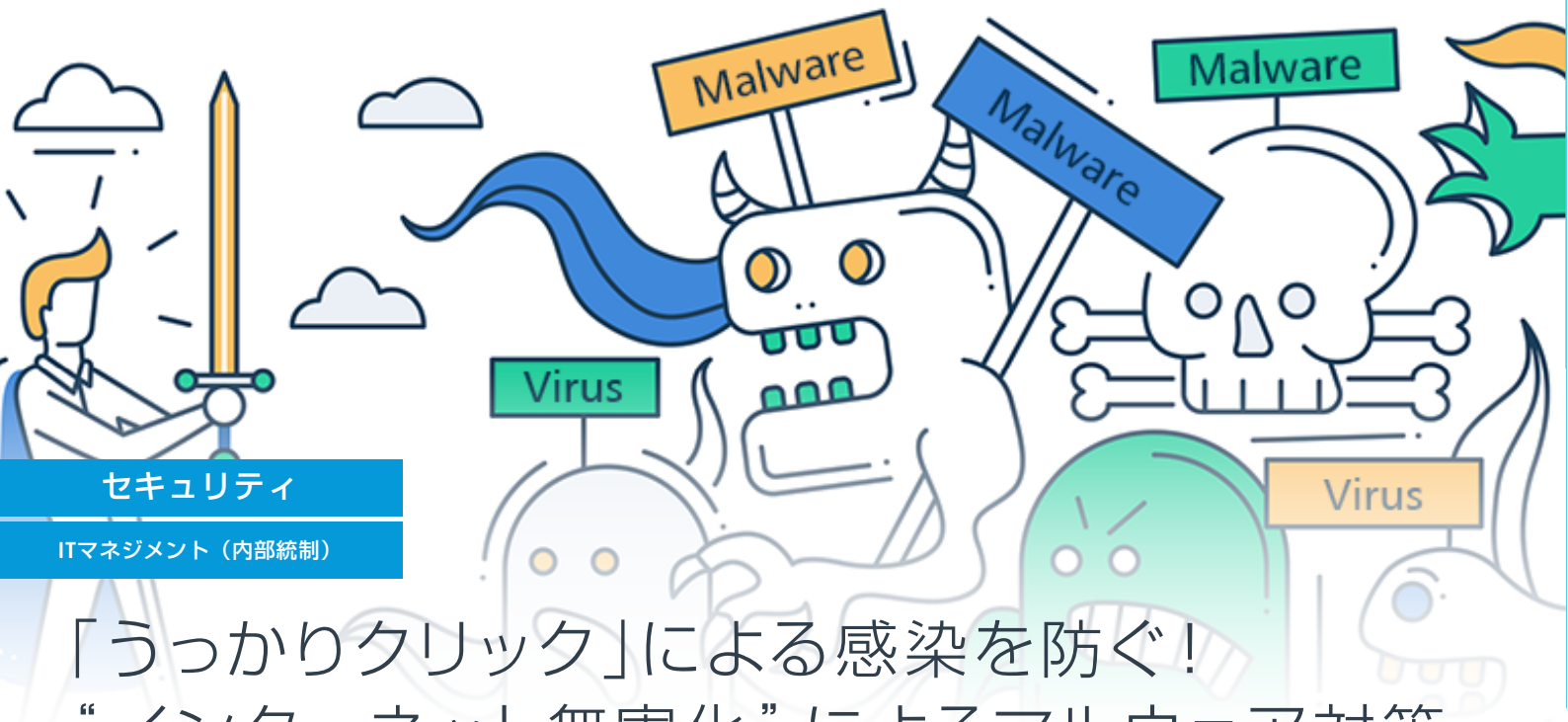


セキュリティ

ITマネジメント（内部統制）

「うっかりクリック」による感染を防ぐ！“インターネット無害化”によるマルウェア対策

Point

- 続々と登場する未知のマルウェアへの対策が必要
- マルウェアの検知を前提としない対策を実現する「Menlo Security」
- Menlo Securityなら、悪意のあるWebサイトに誘導するメールにも対処可能

マルウェア感染による情報漏えいや、重要ファイルを人質にした身代金の要求など、サイバー攻撃への対策に不備があると企業活動が大きな被害を受ける可能性があります。こうしたサイバー攻撃への新たな対策として、注目され始めているのが「インターネット無害化」と呼ばれる手法です。

従来のセキュリティ対策では、未知のマルウェアに対応できない

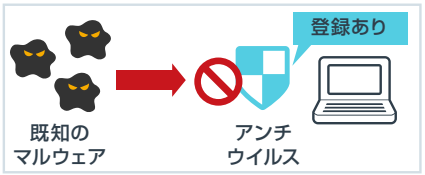
従来のセキュリティ対策は、マルウェアの検知と駆除に重点が置かれていました。仮に外部からマルウェアが送られてきても、インターネットと社内ネットワークの境界、あるいはサーバーやクライアントPC上で検知することができれば、被害を避けられるという考え方です。

しかし、ウイルス対策ソフトにおけるマルウェアの検知率は低下し続けており、従来の考え方に沿ったセキュリティ対策では十分にリスクをコントロールすることができません。実際、主要製品で検知できない未知のマルウェアは90%を超えているという調査もあります。

そこでマルウェアの検知を前提としない、新たなセキュリティ対策として注目を集めているのが「インターネット無害化」と呼ばれる手法です。

既知の脅威

アンチウイルスソフトなどの
既存のルールで検知可
※新規マルウェア検知から登録まで通常一月



未知の脅威

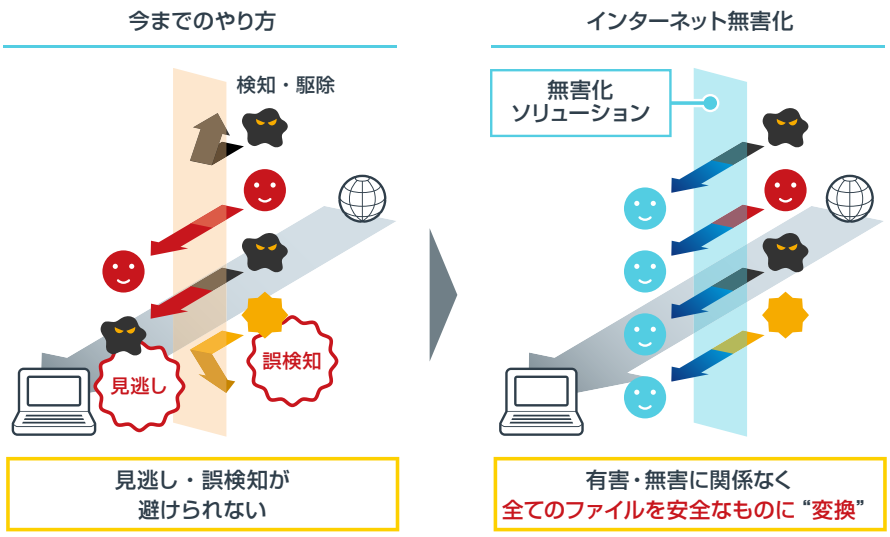
アンチウイルスソフトなどの
既存のルールで検知不可
→挙動などから判断しなければならない

マルウェアかどうかを判断せず、すべてのファイルを無害化

昨今のマルウェアの多くは、Webサイトやメールを感染経路として利用し、社内ネットワークに侵入します。「インターネット無害化」では、これらの通信で送受信されるすべてのコンテンツに対して無害化と呼ばれる処理を行うことで、マルウェアの侵入を防ぎます。

たとえばメールで頻繁にやり取りされる内容として、WordやExcel、PowerPointなどで作成したファイルが挙げられます。これらのアプリケーションには、ファイルの内容をプログラムで操作する「マクロ」と呼ばれる機能がありますが、これを悪用してパソコンに感染を試みるマルウェアは少なくありません。そこで、通信経路の途中でメールによって送受信されるファイルをチェックし、Officeアプリケーションのファイルであれば無条件でマクロを除去します。このような処理を無害化と呼び、ファイルの安全な利用を可能にします。

ポイントは、そのマクロに悪意があるのかどうかを判断せず、すべてのファイルを対象にマクロを除去する点です。判断を行おうとすれば、マルウェアの感染を目的としていないマクロを悪意があると誤って判断したり、あるいは悪意のあるマクロを含んだファイルを見逃してしまったりする可能性を排除できません。しかしすべてのファイルのマクロを除去すれば、このような誤検知や見逃しは起こらないというわけです。



マクロを除去することで業務に支障が生じないか、不安を覚えるかもしれません。しかしOfficeアプリケーションでファイルを作成する際、マクロが使われるケースは決して多くない上、マクロを除去しても閲覧には問題がないケースが大半です。

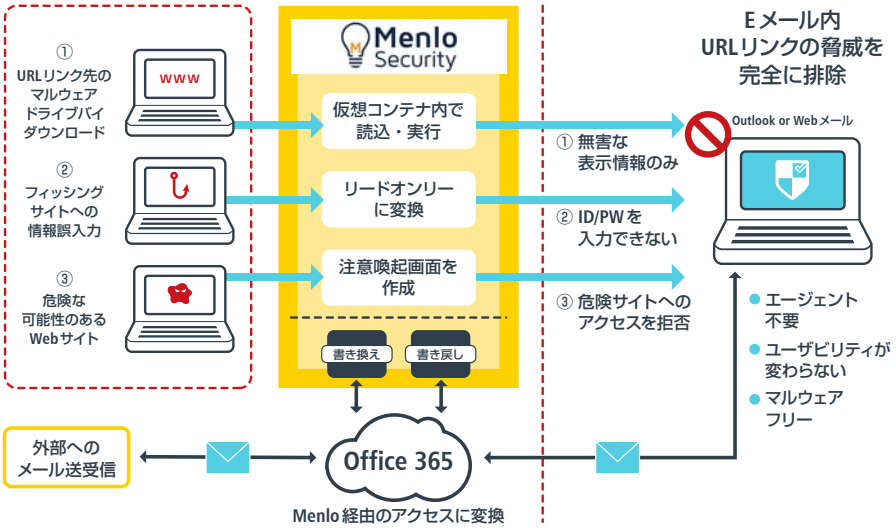
また無害化を実現するソリューションには、オリジナルファイルは別途保存する仕組みがあるため、どうしてもマクロを実行する必要があり、なおかつファイルが安全だと判断することができれば、オリジナルのファイルをダウンロードして利用することも可能になっています。

添付ファイルだけでなく、URLを使った攻撃も防げるMenlo Security

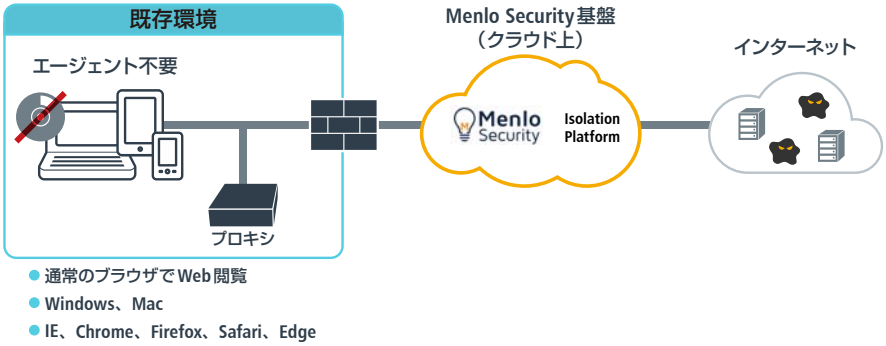
このようなインターネット無害化を実現するソリューションの1つを提供しているのがMenlo Securityです。このサービスでは、前述した添付ファイルにおけるマクロの除去などを実現するだけでなく、メール本文に記載されたURLも無害化の対象となります。またOffice 365にも対応し、Exchange Onlineで受信したメールに無害化を施すこともできます。

フィッシングサイトに誘導して個人情報を盗み取る詐欺行為、あるいはWebサイトにアクセスしただけでマルウェアに感染してしまうドライブバイダウンロード攻撃では、悪性サイトに誘導するための手段としてメールが使われることが少なくありません。URLを記載したメールを送信し、言葉巧みにURLをクリックさせるという手口です。

このような攻撃への対策として、URLから危険性を判断してユーザーに通知する仕組みなどが広まっていますが、マルウェアの検知と同様に誤検知や見逃しの可能性が残ります。しかしMenlo Securityのサービスでは、メール内のURLをクリックしてWebサイトにアクセスした際、Webサイトのコンテンツに含まれるスクリプトなどを除去し、無害な情報だけを表示したり、あるいは参照のみが可能でIDやパスワードの入力ができない状態に変換するなどして、フィッシング詐欺やドライブバイダウンロード攻撃の脅威を排除します。また危険な可能性があるWebサイトであれば、注意喚起画面でユーザーに警告するといった機能もあります。



Menlo Securityのサービスはクラウド上で提供されているため、迅速に導入できるほか、ハードウェアを維持管理する手間もありません。ライセンス単位での課金のため、スモールスタートが可能なこともメリットです。



まとめ

いずれにしても、サイバー攻撃はさまざまな形で企業のシステムを狙ってくるのは間違いありません。それを防ぐことを考えた際、Webサイトやメール経由で侵入を試みるマルウェアの阻止は極めて有効です。もしウイルス検知を前提とした従来のセキュリティ対策しか講じていないのであれば、Menlo Securityのようなインターネット無害化ソリューションを活用して早急に手を打つことをおすすめします。

関連サービス

Menlo Security Web Isolation Service

お客さま端末とインターネット上のWebサーバーの間の通信を代理サーバーで中継しつつ、インターネット側から送られてきたコンテンツに代理サーバーが無害化処理を施し、お客さま端末に転送する仕組みです。これにより、インターネット経由でのマルウェア感染のリスクを低減することが可能になります。