特集 狙われる個人情報

対応策１

ウイルス対策ソフトについて

今回、日本年金機構でウィルスメールによる不正アクセスが発生し、個人情報が流出するという事案が発生しました。

政府系機関でのパソコンには、当然ウイルス対策ソフトが付いており、通信の入り口には、UTM（Unified Threat Management：統合脅威管理：アンチウイルス、不正侵入防御、Webコンテンツフィルタリングといった複数のセキュリティ機能を統合的に管理）といった、セキュリティ装置も設定されていたにも関わらず、マルウェアの感染を防ぐことが出来なかったことについて、ウイルス対策ソフトの機能面から、説明してみたいと思います。

概要

＊2回に分けてお話します。

1 指数関数的に増加している新種のマルウェア

まずは（新種・亜種）マルウェア（ウィルスのこと）の数について、ウイルス対策企業では、定期的にマルウェアの検出数を発表しています が、ここ数年、マルウェア検出件数が指数関数的に増えていて、その対応に追われているのが現状です。

10年前ならば、ウイルス対策企業が対処する新種のマルウェアは1日にひと桁程度でした。これなら人手で解析し、対処することができましたが、現在は1日あたり数万ともされ、こうなると人手でこれ数十万ともされ、こうなるとしてもこれ対処するのは不可能。どうしてもほどまでに膨大な数のマルウェアが開発されるような状況になったのか？

これは、アンチウイルス製品の検知から逃れようとするマルウェア作成者側の「策略」？

なのかもしれません。

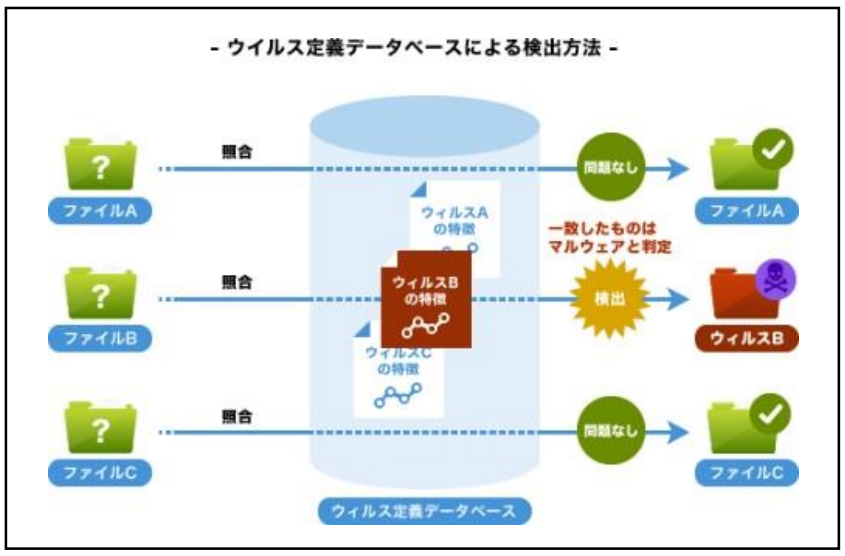
2 古典的なアンチウイルス製品は、「指名手配リスト」を使って検出する

古典的なアンチウイルス製品では、マルウェアを「ウイルス定義データベース」を利用して検出する。

ウイルス定義データベースとは、マルウェアの定義、つまり「どういうウイルスなのか」を記したデータベースで、いわば「指名手配リスト」です。ウイルス対策企業では「ウイルスパターンファイル」とも呼ばれています。

既知のマルウェアを「指名手配リスト」としてあらかじめ登録しておき、ファイルが「指名手配リスト」に該当するか否かを、セキュリティソフトがチェックしてマルウェアを見つけ出すという仕組みです。

ウイルス対策企業では、新種のマルウェアが登場すると、そのマルウェアを解析し、ウイルス定義データベースへ情報を追加します。



3 爆発的に増える新種マルウェアに、指名手配リストだけで対抗するのは限界

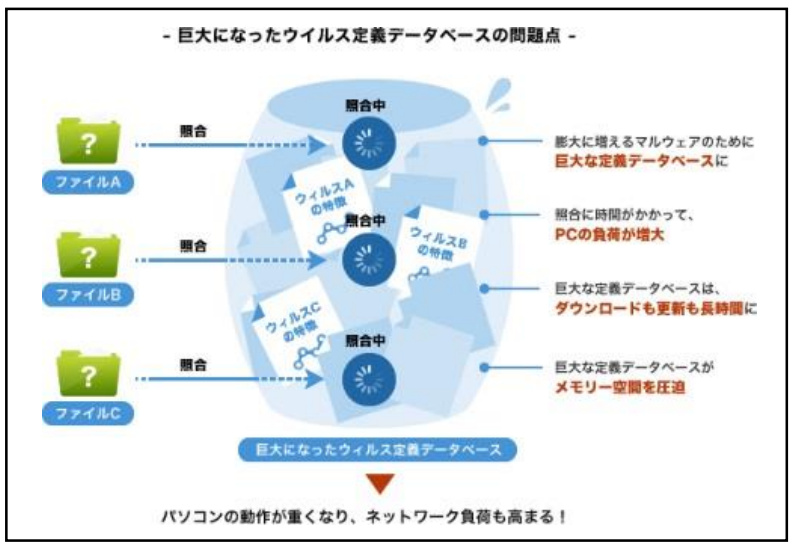
膨大な数のマルウェアが登場すれば、その分だけ「マルウェアの定義」を用意しなければなりません。ウイルス対策企業が検体（＝マルウェア本体）を入手し、解析してマルウェアと判断したのちに作成されるため、新種のマルウェアに対応するには、どうしても受け身にならざるを得ないのが現状です。

そのため、マルウェア作成者側は、ちょっとだけファイルの内容を変えた大量の亜種を作成し続けるのです。

最近は、同じURLからマルウェアをダウンロードしたとしても、毎回異なる亜種が配布されるなど、巧妙な攻撃もあり、新しい定義データベースが配布される前に、マルウェアを実行してしまえば、感染を予防できないのです。

つまり、事前に用意した「指名手配リスト」で対処するという「リアクティブ（事後対応）なウイルス対策」は、マルウェアを確実に判断できるというメリットがある反面、未知のマルウェアに弱い（今回の感染はまさにこのパターンです）側面があるのです。

しかも、マルウェアが増えれば、ウイルス定義データベースに情報を追加しなければならない。結果として巨大に膨らんだウイルス定義データベースは、パソコンの動作を重くし、オフィスのネットワーク負荷を高める要因にもなるのです。



（一部 ESET 出典）

では、どのような対策であれば、よりよいのかを次回お話致します。

次回内容

ソコロ通信7月号

発行日：2015.7.1
通算第43号

どんな人にもどんな時もどんな所にも
ソコロに出逢えた人にソコロのココロを届けます。

～ セミナーのお知らせ ～

ビジネスセミナー

ホームページ作成

create HoPe

クリエイトホープ

簡単・楽々・知識不要！

①ホームページを始めたい…でも難しそう…そもそも知識がない！と、お困りの方いらっしゃいませんか？

当講習会では、知識や経験は不要！ほとんどの操作はマウス操作で編集できる！クリエイトホープを使用します。

日時　7月　21日(火)　19:00～　場所：益田本社
　　7月　22日(水)　19:00～　場所：浜田営業所

※受講料は無料ですが、テキスト代が540円(税込)必要となります。

1時間程度の講習です

②Office365の概要　～Office365の基本設定と使い方～

日時　7月　8日(水)　16:00～17:00　チームで情報共有　その2
　　7月　22日(水)　16:00～17:00　オンラインで会議を行う

③仮想サーバーを作成してみよう　～Azure(アジュール)の概要と基本操作～

日時　7月　8日(水)　17:00～18:00　6回目
　　7月　22日(水)　17:00～18:00　7回目
　　8月　12日(水)　17:00～18:00　8回目

＊マイクロソフトアカウントを使用します
＊3回完結コースとなります。

場所　ソコロ益田本社　受講料：無料

お問合せ　お申込み　について　■各セミナー　ソコロ益田本社へ　☎ 0856-22-5172　皆様のご参加心よりお待ちしております。

地元企業紹介

ほけんフレンド

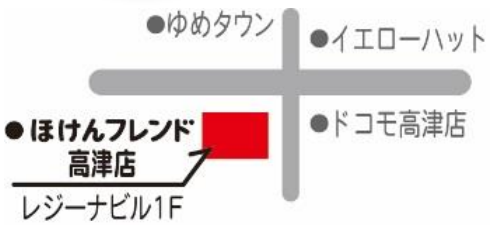
６月３日より、㈱メイワの高津店として、保険相談「ほけんフレンド」　がオープンしました!!

総合的な保険相談窓口として、ご希望やご要望にあわせて、複数の保険会社からお客様にあわせた最適な保障をご案内致します。

土曜日・日曜日も営業していますので、ご家族でお気軽にご来店ください。
お待ちしています。

営業時間:10:00～18:00（受付 17:30）
定 休 日:水曜日、祝祭日

益田市高津5丁目34-13 ﾚｼﾞｰﾅﾋﾞﾙ101
フリーダイヤル　0120-939-640



企業情報を守れ！

企業セキュリティの要！

UTM(統合脅威管理システム)　①

■企業セキュリティ問題

一面でもご紹介しておりますが、本年度のマイナンバー制度の施行に伴い、企業では個人情報の保護が義務付けられます。その様な中起こった『日本年金機構』の情報漏洩事件も踏まえ、今、企業内の様々な情報管理体制の整備が急務となってきています。

そこで登場するのが UTM(統合脅威管理)と呼ばれるシステムです。

■UTM の特徴とメリット

インターネットと社内ネットの境界（通称：ゲートウェイ）に設置し、内部で行われる通信の内容をセキュリティ上のさまざまな視点でチェックし、社内⇔社外ネットワークの接続制御を行うシステムです。

また、ウイルス対策、スパムメール、Web 閲覧フィルタなど個々で対策していくより、UTM1 台導入する方が遥かに低コストである点も大きな特徴であり、メリットです。

●設置イメージ

編集長のつぶやき。

仕事柄、提案書等を作成する際にIT用語をカタカナで記載することがあります。その中でいつも悩んでしまうのが、『communication』という単語。『コミュニケーション』が正解なのか、それとも『コミニュケーション』が正解なのか。

この記事を書いている最中にも、訳が分からなくなる始末・・・

口に出して話すときは何となくごまかしているので気にはなりませんが、イザ活字にしてみると、違和感が満載です。

しょうもないことで悩むと思われるかもしれませんが、何分コミュニケーションが苦手なものですから・・・

今月の名言

コミュニケーションで一番大切なことは、相手が口にしていない言葉を、聞き分ける力である。

ピーター・ドラッガー（アメリカの経営学者）

私たちソコロは
「コンピューターやネットワークで元気になるビジネスを創っていく」をモットーに、企業様や個人様が求める様々な IT 技術を提供・サポートしております。

■ トラブル対応・診断料
■ 個人講習(1時間/内容要相談)

￥3,240～(税込)

まずはご相談を！

【お問合せ・お申込み先】株式会社　ソコロシステム　FAX　0856-22-5165（本社・営業所共通）

■益田本社　益田市三宅町 1-19　電話 0856-22-5172
http://www.socorro.co.jp/

■浜田営業所　浜田市相生町 3905　電話 0855-28-7767
http://socorrohamada.createhope.jp/