トピックス

サイバー攻撃対策について

～「ランサムウェア」の大規模な被害発生を契機として考える～

進和ビジネス株式会社
営業部次長兼サポートグループ課長
田　村　知　久

先ごろ世界同時多発的に発生した「ランサムウェア」によるサイバー攻撃は、世界各地で深刻な被害をおよぼしました。そこでサイバー攻撃対策等について、進和ビジネス株式会社・田村知久氏にまとめていただきました。ぜひともご参考ください。

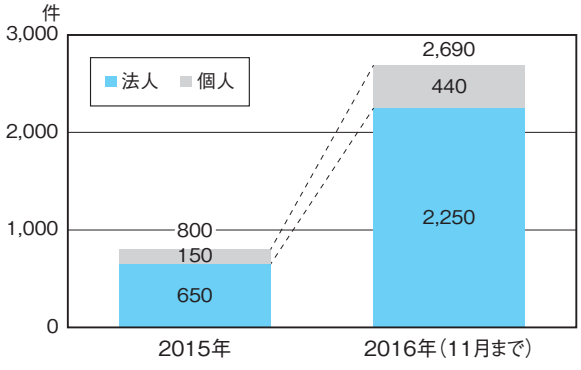
1.「ランサムウェア」などのサイバー攻撃について

去る５月12日、ランサムウェア（「Wanna Cryptor」などと呼ばれています）によるサイバー攻撃が発生、全世界のコンピュータシステムが大規模に感染しました。また、６月27日にも欧米やロシアなどを中心に再びランサムウェア被害が確認されました。５月発生の際は国内でも多くの攻撃が確認されましたが、弊社のお客様に限っては現在のところ感染被害がなく、ホッとひと安心したところです。

このランサムウェアに感染するとパソコンのデータが次々と暗号化され使用できなくなってしまいます。その後、脅迫文面が表示され「身代金（ランサム：ransom）」としてビットコインで300ドルを支払うように要求されたという例があります。ただし、たとえ身代金を支払ったとしても暗号化が解除される保証はありません。

メールを媒体とした一般的なウイルスとは違い、ファイル共有などの通信プロトコル（ネットワーク上での通信に関する取り決め）の脆弱性によって感染しますので、インターネットに直接接続されたパソコン、例えばダイヤルアップ接続している場合（近年では少なくなりましたが）や、自社にてホームページサーバ・メールサーバを立ち上げている企業などは大変危険です。もっとも、国内の一般的な中小企業においては、このような方法で接続されているケースは少なく、今

図１　国内のランサムウェア被害報告件数



トレンドマイクロ社「2016年国内サイバー犯罪動向」速報版

回のランサムウェアにおいては感染するケースは少ないと考えられますが、今後「亜種」（既存ウイルスのプログラムを一部修正し、ウイルス対策ソフトで検出できなくしたり、攻撃性をより高めたりしたコンピュータウイルス）が発生する懸念もあり、安心は出来ません。また、スマートフォンやタブレットなどモバイルコンピュータで通信機能を使用している場合や、公衆の Wi-Fi 接続（FREESPOT 等）する時もウイルスに感染するリスクがあり、そのコンピュータを社内に接続することで感染を拡大させる心配もあります。

また、インターネット閲覧中に突然、「Windows セキュリティやアンチウイルスで緊急事態が発生しています。今すぐここへ電話してください。」との警告画面が表示されて（同時に警告音が出るケースもあります）、指定された連絡先に電話するとパソコンが遠隔操作されソフト料金やサポート料金が請求される事例などが発生しています。一概には言えませんが、この攻撃手法はウイルス等ではなく、一般的な WEB 表示の画面に警告画像を表示しているだけなので、セキュリティソフトや WEB フィルター等では防げない場合があります。特に怪しいサイト等を閲覧していなくとも、バナー広告に紛れて表示してくるケースもあります。さらに、画面には Microsoft のロゴや Windows Defender の画面イメージも表示され、いかにも Microsoft の Windows 自体がエラー表示しているかのようにして不安感を煽ります（図２、３参照）。現実的に、あるお客様でセキュリティ対策が施されている環境の中、表示されたケースも数件発生しています。

以上のとおり近年、ソフトウエアの脆弱性に対する攻撃や虚偽の警告などを表示し不安を煽り、金銭の振込やソフト購入を強制するケースが多数発生しており、企業活動を脅かす攻撃も数多くあります。コンピュータセキュリティ対策に関する情報収集やソフトウエアのアップデート更新はなくてはならないものになっております。

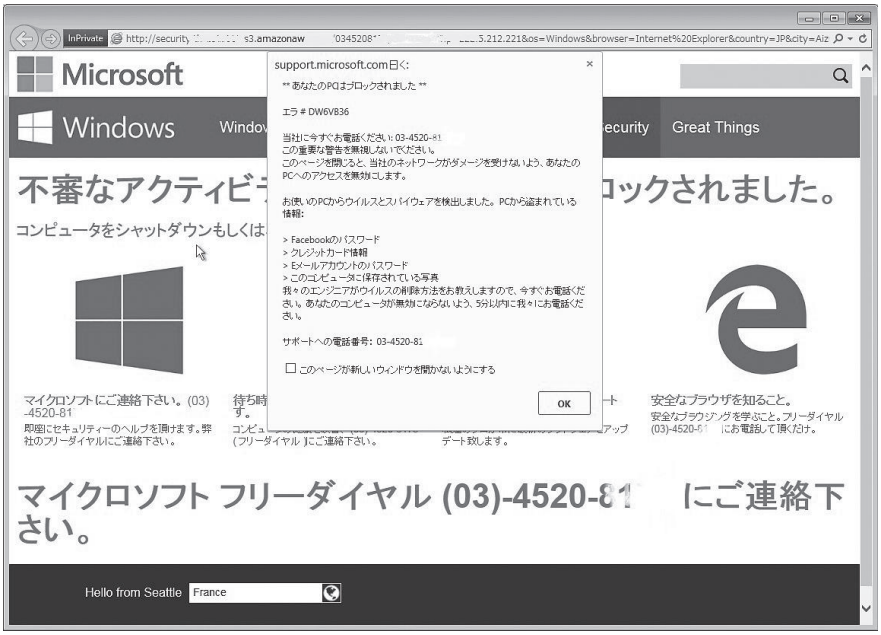
２．主な対応策について

残念ながら、サイバー攻撃に対して「これをやっておけば絶対安全！」というものはありませんが、ウイルス感染を防ぐシステムの環境整備を行うことが重要です。

(1) パソコンのウイルス対策ソフト（エンドポイントセキュリティ）の導入と常に最新状態に更新すること。

(2) プロバイダ側によるメール送受信のウイルス駆除・スパム検査等、セキュリティサービスを利用すること。

図２　Microsoft や Windows の警告画像を表示した例（一部画面を加工しています）



(3)　インターネット接続に使用するルータ機器のセキュリティ対策を実施すること（ゲートウェイセキュリティ）

※　UTM（統合脅威管理）・ファイアウォールなどの機器導入によりインターネット通信のセキュリティを強化すること。アンチウイルス対策及びインターネット WEB フィルターの機能が有する機器を選択すること。

(4)　USB メモリーからのウイルス感染を予防すること（使用制限も含む）

※　使用する場合はウイルスチェック機能が搭載されたものを使用すること。さらに、紛失時のデータ漏洩事故を防ぐため、ハードウエア暗号化が可能なものを推奨します。

＜セキュリティ対策のまとめ＞

- パソコンにウイルス対策ソフトを導入することは必要最低限の対策です。ウイルス対策ソフトで頻繁にウイルスが検知されている場合、セキュリティを通過し社内ネットワークに入ってから検知している状態なので、安心はできません。コンピュータに検知される前の対策をしなければ感染するリスクは十分ありと言えます。前述のセキュリティ対策を参考に安全策を考えましょう。
- 最近のサイバー攻撃はメール経由の場合が多いのですが、リンク URL のみを送り付けるなど、コンピュータの対策ソフトでは検知できないケースも多くあります。その場合、URL を制限する等のインターネット WEB フィルター（UTM など）を導入することが重要です。
- ゲートウェイセキュリティの UTM について、中小企業においては未導入の企業が多いと思いますが、最近では手ごろな商品もあります。導入する場合は、不正侵入検知・防御機能はもちろん、重要なのは WEB フィルター機能です。カテゴリー（不正サイト・ギャンブル・アダルト・薬物などが代表例）で閲覧制限が可能なものが便利です。さらに、コンピュータのウイルス対策ソフトとは別メーカーのものでウイルスを検知する機能があるものを推奨します。なぜなら、別メーカーのものを使用し対策することで各社独自のセキュリティ機能をあわせて利用できることになり、防御力がさらに上がるからです。

3．その他のリスクの回避策について

(1)　自己のホームページを持っている方は、ホームページにメールアドレスを表示することを中止しましょう。「問い合わせ先」などとして、

図３　Windows Defender の画像を表示した例（一部画面を加工しています）

メールアドレスを公開しているケースがあると思いますが、攻撃者はこのメールアドレスに対して攻撃してきます。ホームページ上にメールアドレスを公開するのではなく「問い合わせフォーム」を利用する方法に変更してください。自分で問い合わせフォームを作成するツールもありますが、不安な方はホームページ作成ノウハウがあるところに相談してみてください。ただし、問い合わせフォーム利用をしてもサイバー攻撃を受ける可能性はありますので、問い合わせメールの送受信は通常業務用のパソコンとは別のパソコンを使用することをお勧めします。

(2) ネットバンキングや商取引などの電子決済が使用できない場合に備えての対応

インターネットバンキング等に使用しているパソコンが故障などにより使用できなくなるリスクがありますので、最低限２台以上を使用できるよう準備しましょう。また、インターネット回線が使用できないリスクもありますので、通常回線の他にモバイル Wi-Fi やスマートフォンなどにて通信を確保することも考慮しましょう。さらに、金融機関側でインターネットバンキングが利用できないリスク発生も少なからず考慮したほうが良いでしょう。一度、ATM での振込手順や振込用紙による手順を確認しましょう。取引先との商取引にインターネットを利用しているケースも多いと思いますが、上記のとおりインターネットが利用できない場合に備えて、FAX や電話などによる取引が可能か確認しましょう。

前にも述べましたが、公衆 Wi-Fi 接続（FREE SPOT 等）にはリスクがあります。通信費用を節減する目的や LTE 通信が利用できない場合に公衆 Wi-Fi 接続を利用するケースもあると思いますが、悪意ある第三者がダミーのアクセスポイントを設置して通信を傍受、ログイン情報やセキュリティ情報が盗まれてしまうリスクがあります。もちろん、公衆 Wi-Fi に接続するとすぐ危険にさらされるということではありませんが、悪意を持った者が傍受しようとする可能性があることを忘れてはいけません。このような環境で安易にメール確認や ID パスワード入力が必要なサイトを利用してしまうと、入力した情報や通信内容が傍受されてしまいます。攻撃者は、この情報をもとに通販サイト・ネットバンキング・Facebook・プロバイダのメールなどにログインしようと試みます。ログインできた場合は悪用されてしまいます。さらに「使いまわしパスワード」（同一のパスワードを複数のインターネットサービスで登録すること）を使用していれば被害はさらに広がることになるでしょう。

４．最後に

現代社会において、パソコンやインターネットはなくてはならないものとなっています。しかしながらパソコン利用における問題はサイバー攻撃だけではありません。本年５月に施行された改正個人情報保護法への対応という課題もあります。改正前は5,000件以上の個人情報を扱う事業者のみが法適用の対象でしたが、改正後は5,000件以下の事業者も対象となります。つまり、ほぼ全ての事業者が適用対象となります。システムに保管されているデータ以外に紙で保存されたものも該当します。さらに、データ漏洩対策も求められています。万が一、個人情報を漏洩してしまった場合「６ヶ月以下の懲役または30万円以下の罰金」の刑事罰が課せられますが、賠償責任や信用損失による取引停止など、刑事罰以外の大きなダメージを負うことも考えられます。

ここまで、なるべくわかりやすいように述べたつもりですが、どうしても専門用語を使わざるを得ない部分もあり、十分にご理解いただけたかどうか不安です。しかしながら、これらのリスクについて回避対策を確実に行うことは、会社を存続させる上で必要不可欠の投資であり重要なものであると考えます。サイバー攻撃対策をはじめとした企業経営におけるリスク軽減のアドバイスや、業務効率化・経費節減等の提案・対応策について、いちど専門知識を有するコンサルティング会社にご相談されてみてはいかがでしょうか。もちろん、当社でも各種ご相談や対応策のご提案に応じております。ぜひお気軽にご相談ください。