TOPICS

法的リスクマネジメント講座 第87回

# 中小企業を狙い撃ちにする サイバー攻撃にどう備えたらよいか

長谷川俊明法律事務所
弁護士
**長谷川 俊明**

## はじめに

このところサプライチェーンにおける“弱点”とも言われる中小企業がサイバー攻撃に狙われるケースが増加しています。なかには、後述するランサムウェアでいわば狙い撃ちにされた事例も多くあります。

今年2月下旬には、トヨタ自動車に部品を納入する取引先のプレス会社がサイバー攻撃を受け、国内の14工場が稼働を休止する事件が起こりました。

サイバー攻撃は、パソコンやサーバーのネットワークに“侵入”して、電子機器の動作異常を発生させるために仕掛けられます。

ただ、誰が何を目的としてサイバー攻撃を仕掛けるかははっきりしない場合が多いのが実情です。

犯人とその動機は明らかではないのですが、日本企業を標的とするサイバー攻撃が増えているのは事実です。また、その“手口”は巧妙化、高度化しています。そこで、最近のサイバー攻撃の特徴を明らかにし、防御上の注意点を整理し、実例や予防策を考察します。

## サプライチェーンの拠点を狙うサイバー攻撃のケース

### 1.サプライチェーンとは

経済産業省の「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」(20.12.18)は、冒頭、次のような記載が有ります。

> 「2020 年に入ってから、新型コロナウイルスの感染拡大に伴い、テレワークの利用の急拡大など、サイバー空間を巡る環境が大きく変化している。また、サイバー攻撃の攻撃者による攻撃の痕跡の消去などサイバー攻撃の手法の高度化・巧妙化が進むとともに、中小企業等のサプライチェーン上の弱点を起点とする攻撃の拡大が見られる。」

サプライチェーンは、名称のとおり、いくつもの供給者(サプライヤー)をつなぐ“連鎖”です。そのなかにセキュリティが脆弱な企業が含まれていますと、これを攻撃の標的にする実態に基づき、この文書は警告しています。実際の事故例を検討しましょう。

サプライチェーンのいわばピラミッドの頂点に位置するのが自動車メーカーのような大企業であったとしても、原料、部品の供給者は中堅・中小企業であることがよくあります。

その場合、原料、部品の供給者は、最終製品につき製法など技術データを、部品の「仕様書」などを通じ、知らされているだけでなく、コンピュータ・ネットワークでつながっていることがよくあります。サプライチェーンを構成している「拠点」となる中堅・中小企業のセキュリティレベルは、完成品メーカーと比較して低い事が多く、そこを狙って、サイバー攻撃を仕掛け、ネットワークから侵入し、企業の秘密データを盗み出そうとしたりします。

### 2. 手口

“手口”としては、いわゆる不正アクセスによる攻撃が多く見られます。これは、本来アクセス権限をもたない者がサーバーや情報システムの内部へ侵入するものです。

たとえば、ある企業では、従業員が取引先を装ったメールの添付ファイルを開いたところ、社内のPCがウイルスに感染、そのPCに保存されていた過去のメール送受信歴が流出し、これに含まれるメールアドレスに対して、さらに同社社員を名乗る不審なメールが送付されました。

サプライチェーン拠点である中小企業の端末やメールアドレスなどが、取引先攻撃の起点になってしまい、攻撃先の標的企業がさらにウイルスに感染する悪循環に陥ってしまいました。

### 3. 対策

“敵”は巧妙に社員を装って、システムへの侵入を試みます。怪しげなメールは、とくに添付ファイルを開かないように社員間で徹底するのが第一です。

それだけでなく、あらゆる人物や端末を信用せず、データへのアクセスがあるたびに認証を必要とする、「ゼロトラスト」と称するセキュリティ対策なども有効とされています。

## ランサムウェアによるサイバー攻撃のケース

### 1.ランサムウェアとは

ランサムウェアとは、感染すると端末などに保存されているデータを暗号化して使えない状態にしたうえで、データを復元する対価として「身代金(ランサム)」を要求する不正プログラムです。

### 2. 手口

さらに近時は、データの暗号化のみならず、データを窃取したうえで、企業に対し「対価を支払わなければデータを公開する」などと二重恐喝(ダブルエクストーション)の手口も登場しています。

また、コロナ禍のなかで、テレワークを行う従業員個人の端末や病院など団体を標的とするなど、対象が広がっています。

### 3. 対策

対策としては、何よりも知り合いや日頃から知っている取引先からのメールに見えても、不用意に添付ファイルを開いたり、リンク先にアクセスしないことを徹底すべきです。「ゼロトラスト」ももちろん有効です。

ある日本企業の場合、社内ネットワークの構成や端末の設定を管理するサーバーに侵入され、グローバルネットワークに接続している複数拠点の複数のPCが暗号化される被害が発生しただけでなく、社内の情報システムが使えなくなり、一時操業停止状態に陥りました。

別の日本企業では、ランサムウェアによる感染で、データが窃取、削除されるとともに、システムの一部に障害が発生する事件が起こりました。犯行グループが、ネット上に犯行声明を掲載し、窃取した情報の公開停止と引き替えに身代金を要求しました。身代金の支払いを拒絶したところ、実際に情報の一部が公開されたとのことです。

ランサムウェアによる被害は、暗号化によってシステムが停止するだけでは済みません。やむをえず身代金を支払わされるケースが跡を絶ちません。最悪なのは、身代金を払ったにもかかわらず、犯行グループが暗号化の復旧を行わず、約束に反し、個人データを拡散させてしまうケースです。

## おわりに

日々高度化するサイバー攻撃への防御として、さまざまなセキュリティソリューションやガイドラインがつくられています。身近なところに気を配るだけでもサイバー攻撃を防ぐことができます。自社で利用する端末やソフトウェアの状態を調べ、古い基本ソフトなどが稼働し続けていないかをチェックし、脆弱な部分にはパッチを適用し、修正を心がけるなどを地道に行うことで情報流出の多くは予防できるとするセキュリティ専門家は少なくありません。


参考URL
1) 2020年12月18日　経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」
https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf
2) 2020年8月20日　独立行政法人情報処理推進機構セキュリティセンター「事業継続を脅かす新たなランサムウェア攻撃について」
https://www.ipa.go.jp/files/000084974.pdf