

脆弱性が狙われる!?

中小企業が最低限備えたい サイバー防衛策

どんな企業でもサイバー攻撃の被害に遭う可能性はありますが、「他人ごと」として捉えている中小企業が多いのではないのでしょうか。最低限、中小企業が備えておくべきセキュリティの知識を解説します。

株式会社CISO 代表取締役
セキュリティコンサルタント
那 須 慎 二



サイバー攻撃は 突然襲ってくる

サイバー攻撃はある日突然襲ってきますが、中堅・中小企業がサイバー攻撃に遭うと、何をどう対応すればよいのかわからないというケースが多々あります。

- ・ システムが破壊されて請求書や見積書の発行ができない
- ・ フォレンジック調査（不正アクセスや情報漏えい）が起きていないか、および原因の調査）が高額で、調査に踏み切れない
- ・ セキュリティを任せていたシステムベンダーへの不信任が募る
- ・ 業務を行えないことで社員が

疲弊する

など、さまざまな理由で身動きが取れなくなっているケースに遭遇します。

本稿では、近年のサイバー攻撃についての簡単な知識を解説するとともに、中小企業が知っておくべきセキュリティ対策の基本を紹介します。

進化する サイバー攻撃の仕組み

近年、ウイルス対策ソフトや、インターネットの出入り口に設置するセキュリティ装置であるUTM (Unified Threat Management)を導入したり、バックアップを保存するなどの対策はしていても、被害が甚大になるケースが増加してきています。いままでのセキュリティ対策では防げない攻撃が増えているためです。

ITリテラシーやセキュリティリテラシーが低い企業の場合は、自社がサイバー攻撃に遭うとは想像すらしていないため、ほとんど対策をしておらず、より被害が拡大してしまうのが実情です。

攻撃者は、ウイルス対策ソフトやUTMによるウイルスの検出、

バックアップによる保全を掻い潜って攻撃を仕掛けてきます。

(1) 中小企業を狙うランダム型攻撃とは

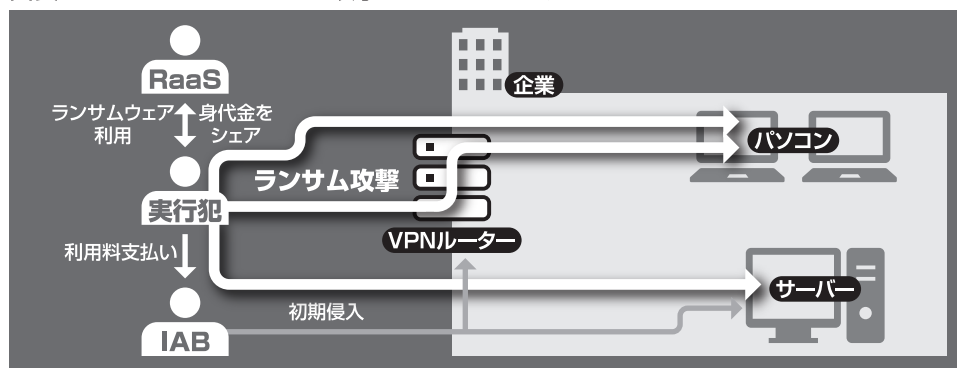
「標的型攻撃」は、攻撃者が入手したい情報を保有しているような企業（上場会社等）をターゲットとして、ピンポイントで攻撃を仕掛ける方法です。有名とはいえない企業が狙われることは多くありません。

しかし、「うちみたいな小さい会社をサイバー攻撃者が狙うわけではない」と考えていても、サイバー攻撃に遭う可能性があります。それが「ランダム型攻撃」です。

ランダム型攻撃は、インターネットにつながっている端末やネットワーク機器に対して、手当たり次第に攻撃を仕掛ける手法です。中堅企業・中小企業の場合は、ランダム型攻撃の流れ弾に当たって突然被害に遭遇するケースがほとんどです。

金銭が目的であれば、より多くの企業に対してランダムに攻撃を仕掛け、いわば確率的に攻撃が成功するのを待てばよいわけです。中小企業の場合はこういった攻撃に引っかけたてしまい、被害

図表1 ランサムウェアによる攻撃のビジネスモデル



に遭います。
ランダム型攻撃では、脆弱性（セキュリティ上の穴）が狙われるケースが多く、アップデートなどがなされていないOSやソフトウェア、インターネットを経由して社内へアクセスするためのVP

N（インターネット経由で仮想的に専用回線を構築し、社内ネットワークのサーバー等を使うようにするしくみ）機器の脆弱性が狙われて、社内侵入を許してしまうのです。

(2) ビジネスモデルとして成立したランサムウェア攻撃

「ランサムウェア」は、システムのデータを暗号化して使用不能にし、復元のために身代金（ランサム）を要求するものです。ビットコインなどの暗号資産を要求する場合もあります。

ランサムウェアには、暗号化をする前にデータを盗み取り、金銭を支払わなければ盗んだ情報を公開すると脅す「二重強迫型」も存在します。

こうした最近のランサムウェアによる攻撃は、役割が分化され、ビジネスモデルとして成立しています（図表1）。

ランサムウェアを開発して利用料を入手するRaaS（Ransomware as a Service）、初期侵入を担当するIAB（Initial Access Broker）、そして、攻撃の実務を行なう実行犯がいます。

実行犯は、初期侵入が成功した

PC端末やVPN機器の利用料をIABに支払い、RaaSのランサムウェアを利用して攻撃をしかけます。身代金を獲得したら実行犯とRaaSが取り分をシェアするというビジネスモデルです。

利用料を支払った実行犯は、乗っ取りが成功している端末や、VPN機器を経由して社内ネットワーク内のPCやサーバーのデータを盗んだり、暗号化して身代金を要求したり、自分の代わりに他のPCを攻撃させる「踏み台」として利用するというように、あらゆることが可能になります。

中小企業のとるべきセキュリティ対策

突然襲ってくるサイバー攻撃から身を守るために、中小企業がとるべきセキュリティ対策の第一歩は「知ること」です。

自分が知らない・わからないことに対して行動を起こすことは極めて難しいものです。

特に中小企業の場合は、投資判断ができる社長が知らなければ、対策はできないといっても過言ではありません。

ここでは、実際に行動につなげ

られる対策方法を解説するので、勉強会に取り入れるなどして、セキュリティ対策の基礎を知ることから始めてみてください。

あわせて、会社のセキュリティ状況が現在どうなっているのかを知ることも重要です。以下の内容も参考に、システムベンダーに丸投げせずに、自社の現状を正しく知っておきましょう。

(1) OSやファームウェアのアップデート

アップデートは、セキュリティ対策のなかでも最も基本的なものです。一番の目的は「脆弱性を潰す」ことで、これはOSやファームウェアのアップデートによって定期的に改善されます。たとえばWindowsの場合は、月に1回、定期的にWindowsアップデートがありますので、手間を惜しまずにPCの電源を切るか再起動をして、アップデートを適用してください。

最近では、テレワーク等でノートPCを持ち出し、電源を切らずにバッテリーで利用しているケースも多いですが、これではアップデートが適切にできず、脆弱性が残ったままになります。

また、アップデートによって、構築したシステムの環境が崩れて不具合が生じる可能性があるという理由から、サーバーOSのアップデートがされていないケースもよく見かけます。脆弱性を潰すために、サーバーOSのアップデートは確実にこなしてください。

(2) セキュリティソフトの導入

ウイルス対策ソフトウェアの導入および最新化も重要です。前述のとおり、攻撃者はウイルス対策ソフトの検知を回避する技術を用いて攻撃してきますが、それでも既知のウイルスを防ぐためには必須です。

最近のウイルス対策ソフトには、未知のウイルスだとしても「振る舞い」をみて検知する機能を有するものもあります。パターンファイル（不正プログラムの類型的な情報）が最新の状態になっているかどうか也必须確認するようにならしましょう。

(3) UTMの設置

通常、インターネットの出入り口にはルーターが設置されていますが、このルーターを置き換えて設置する、小型のセキュリティ機

器であるUTMも効果的です。

UTMには、外部からの侵入を防ぐファイアウォール機能が備わっているほか、アンチウイルス機能や危険性の高いサイトへの閲覧を防いでくれるURLフィルタリング機能、スパムメールの侵入に注意喚起を行なうアンチスパム機能等が付加されています。

ただし、UTMは万能ではないということに注意してください。

UTMの下に設置されている社内環境にあるPCやサーバーは保護されますが、外出先やテレワークで自宅に持ち帰ったノートPCは保護されません。

また、アンチスパム機能はウェブブラウザで閲覧する形式のメールには機能せず、通信の暗号化処理を施すSSL通信（URLがhttpsで始まるウェブサイトへの接続等）が行なわれる場合、通信データの中身までは監視できません。

リモートアクセスやリモートメンテナンス用にUTMのVPN機能をONにしている場合、これが入り口になって攻撃者の侵入を許してしまうことにも注意してください。継続的にUTM機器にインストールされているソフトウェア

（ファームウェア）をアップデートして、常に最新状況を保ってください。

(4) EDRの導入

最近のセキュリティ対策では、EDR（Endpoint Detection and Response）を導入するのも効果的です。

ウイルス対策ソフトは、既知のウイルスのパターンに該当した場合に、プログラムの隔離や駆除を行なうものです。一方、ウイルス対策ソフトでは検出されないような攻撃者の挙動、たとえばWindows標準で実装されているプログラムを使った攻撃は、ウイルス対策ソフトではウイルスとして検出できません。EDRは、これを検知し、「怪しい動きが起こっている」とリスクレベルに応じて注意喚起を促してくれる、PCやサーバーにインストールするソフトウェアです。

ウイルス対策ソフトをすり抜けるような攻撃が起こったとしても、危険性を発見してくれることや、テレワークなど外出先からPCを操作していたとしても、端末ごとに危険性を察知できることから、セキュリティ対策レベルが格

段に上がります。

EDRは怪しい動きを見つけて注意喚起をするものであり、SOC（Security Operation Center）における人的な監視をセットにしなければなりません。

SOCは、EDRが通知したアラート情報を専任の技術者が解析して、レポートとしてまとめたり、対応策を利用者（ユーザ側の情報システム部門など）に伝える機能を外部に委託するものなので、コストがかかる点には留意してください。

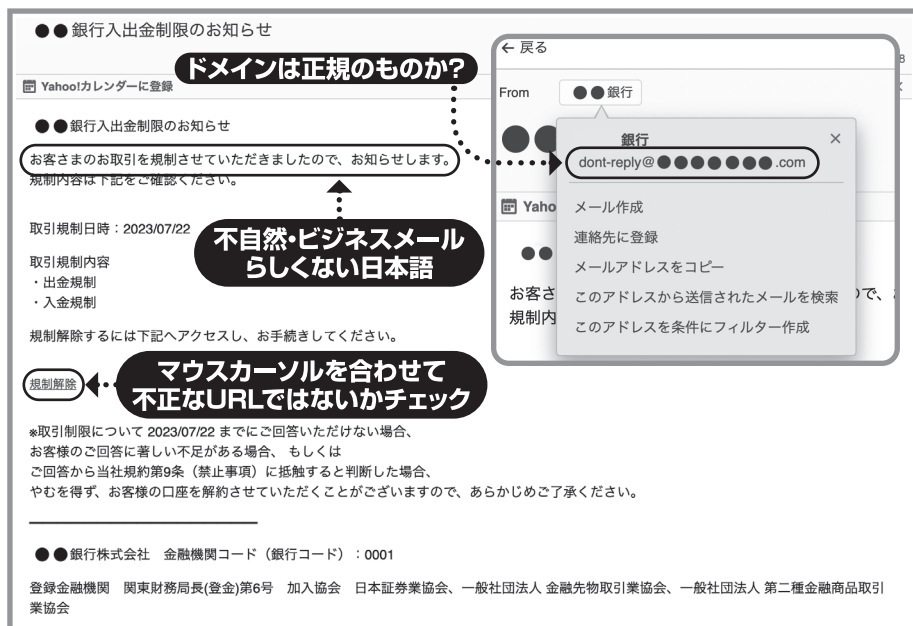
(5) バックアップ

バックアップも重要です。万が一データが破壊されたとしても、バックアップさえあれば通常業務に素早く復帰できます。

特に、ランサムウェアによる被害対策に効果的なバックアップ手法は、オフラインもしくはクラウドによるバックアップです。

オフラインのバックアップは、たとえばUSB接続の外部ストレージにバックアップを保存し、USBケーブルを引き抜いて物理的な通信ができないようにする方法があります。コストが最も安い方法ですが、人間がUSBケーブル

図表2 フィッシングメールの見分け方



手法です。

を抜くという動作が都度発生するので、人的ミスが生じやすくなります。

クラウドを利用したバックアップは、社内にデータを置かず、攻撃者の手の届かないクラウド上にデータを退避させる方法です。手間がかからないので、おすすめの

(6) フィッシングメール・偽サイトを見分ける

まずは送付元メールアドレスのドメイン（@***.co.jpなどの@以降の部分）を確認しましょう。特定の企業を騙っている

場合で、かつ正規のドメインではない場合は、フィッシングメールの可能性が高いと判断できます。

また、メール本文に添付されているURLリンクにマウスカーソルを当ててみて（クリックしてはいけません）、本文表記のURLリンクと異なるドメインがポップアップ表示されないかを確認して

みましょう。ドメインが異なる場合、攻撃者のサイトに誘導しようとしている可能性があります。URLリンクが短縮されている場合は、異なるドメインが表示されるため、正規のドメインかどうかを確認しましょう（図表2）。

偽サイトであるかどうかは、サイトで使われているURLが正規のものであるか、日本語表示に違和感がないか、文字化けを起こしている箇所がないかなどを確認してみてください。

IDやパスワードの入力を促したり、クレジットカード番号など金銭に絡む情報を入力させようとする場合は偽サイトを疑ってください。

そもそもメールを入り口にしたサイバー攻撃が多いことを念頭に置いて、「怪しくなくてもメールの添付ファイルの開封は疑ってかかる」「怪しくなくてもメールに貼付されているURLリンクのクリックはしない」といったルールを徹底しましょう。

メール以外でコミュニケーションが取れる方法（Slackなどのビジネスチャットツール）を利用することも効果的なセキュリティ対策になります。

いずれにせよ、フィッシングメールや偽サイト対策には、社員教育が重要になってきます。研修などを行ない、日々の業務におけるセキュリティリスクを認識してもらいましょう。

最新の情報に キャッチアップしよう

サイバー攻撃の手法は日々進化しており、新たな技術・機器が普及することによって、ますます多様化していきます。

たとえば、フィッシングメールは日本語に違和感があるものが多く、「怪しいメール」を開封しないことが、セキュリティ対策としていまのところ効果的です。

しかし、生成AIであるチャットGPTの登場によって、将来的には、日本語に違和感のないようなメールを、日本語話者でなくとも作成できるようになることも大いに考えられます。

まずは本稿を自社のセキュリティ対策の出発点として、常に最新の情報にキャッチアップしていく心構えで、自社のセキュリティの状況の把握と対策の導入に努めましょう。

なす しんじ インフラ系SE、大手経営コンサルティングファームを経て2018年に株式会社CIOを設立。著書に『小さな会社のIT担当者のためのセキュリティの常識』など。