脱IT初心者「社長の疑問・用語解説」（第67回）

「踏み台」で危ない目に遭う！？

2023.07.19

理解しようと努めているが、難解な用語が多くて何回聞いても分からない。そんなIT初心者の社長にも、分かりやすく理解できるようにITキーワードを解説する本連載。今回は、対策を怠ると取引停止になりかねない「踏み台」だ。

「社長、同業のA社が踏み台にされて取引先から取引停止処分を受けたみたいです。うちも踏み台にされたら大変です」（総務兼IT担当者）

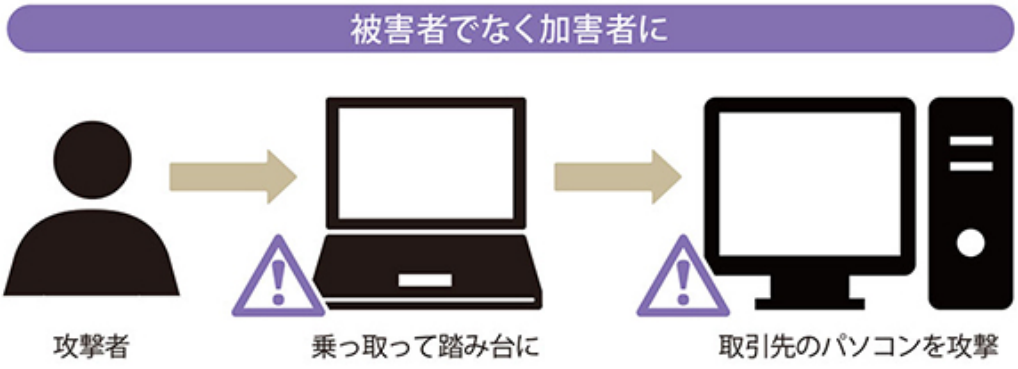
「踏み台だって。この前、家で片づけをしていて、踏み台から落ちて危ない目に遭ったばかりだ。何で君が知っているんだ」（社長）

「その踏み台ではありません。サイバー攻撃のことです。攻撃者が対策の甘い会社のパソコンを乗っ取って、そこを踏み台にして取引先のシステムに侵入するんです。A社は機密情報を盗まれ、取引先へ侵入する踏み台として利用されたようです」

「踏みにじられたってわけか。わが社も踏まれないようにすぐに対策しなさい」

攻撃の被害者でなく加害者に

踏み台とは、サイバー攻撃者が身元を知られないように第三者のパソコンやサーバーを乗っ取ること。セキュリティ対策がぜい弱なパソコンが乗っ取られる（踏み台にされる）と、取引先など重要な機密情報が盗まれる恐れがあります。踏み台にされた企業はサイバー攻撃の被害者でなく、意図せずに加害者になる場合もあります。セキュリティ対策をおろそかにしてはいけません。



Q 踏み台にされる企業にはどんな傾向がありますか

セキュリティ対策が手薄な中小企業が狙われやすいとされています。対策が弱い会社のパソコンやサーバーを踏み台に取引先企業のシステムを乗っ取って遠隔操作したり、機密情報を盗み取ったりします。近年はサプライチェーンを狙った攻撃もあり、踏み台になった企業は取引停止や損害賠償などで事業継続が困難になるリスクもあります。

Q 攻撃者の手口にはどんなものがありますか

攻撃者の目的の一つは、企業・組織の機密情報などを盗み取って換金したり、データを使えなくして金銭を要求したりすることです。踏み台にする企業のパソコンやサーバーを不正操作するために従業員のIDやパスワードを奪ったり、マルウエアに感染させたりする手口があります。

Q 踏み台にならないための対策は何ですか

攻撃者に悪用されないようにIDやパスワードの使い回しはやめる、ウイルス対策ソフトやOSは常に最新の状態にしておくなどの基本的な対策を徹底します。また、パソコンやサーバーの不正操作や社内ネットワークの不審な動きを検知するUTM（統合脅威管理）ツールも有効です。サプライチェーンに加わる中小企業に対し、取引先からセキュリティ対策の報告が求められるケースもあります。どのような対策が必要なのかを情報セキュリティの最新事情に詳しいITサービス事業者に相談するといいでしょう。

「社長、踏み台になるリスクについて、分かっていただけましたか。もう私の話を踏み外さないで聞いてくださいね」。（総務兼IT担当者）

「知らないうちに取引停止にでもなったら大変じゃ。ワシの社会的な立場も失いかねないな」（社長）

「そうなったらゴルフコンペに誘ってもらえなくなるかもしれません。セキュリティ対策を強化しましょう！」

「踏み台にされてじだんだを踏む羽目になったらゴルフどころじゃないな。対策を進めなさい」