TOPICS

法的リスクマネジメント講座 第88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（続編）

長谷川俊明法律事務所
弁護士
長谷川 俊明

はじめに

前号(本講座第87回)では、サプライチェーンの拠点を狙うサイバー攻撃及びランサムウェアによるサイバー攻撃への備えのあり方を探りました。今回は、サイバー攻撃全般に対象を広げます。中小企業としてかけられるコストの範囲内で実践が可能で、かつ有効な対策にはどのようなものがあるかを、さらに考えます。

中小企業を標的とするサイバー攻撃が増えている理由は、“備えが甘い”からです。なかには、しっかり対策をとっている中小企業があるのは承知しています。そうした企業でも、巨大メーカーへ部品を供給する、サプライチェーンの一員として、同メーカーの“備え”と比べますと、格段にレベルが落ちるのが普通です。

サイバー攻撃をする狙いはまちまちですが、巨大メーカーの技術データの盗み出しやそのシステムの誤作動を狙っての攻撃かもしれません。サプライチェーンの拠点のうち、“備えが甘い”企業から完成品メーカーのシステムへ侵入を謀るのがひとつの典型パターンになりました。

サイバー攻撃が怖いのは、企業だけでなく、国や公共団体の社会インフラ的システムを正常に稼働させなくし、個人データの大量ネット流出まで招きかねないからです。そうした事態のきっかけを作ったと言われないため、身近でできることから日頃の“備え”を怠らないことこそ肝要です。

サイバー攻撃を仕掛けられないためには、後述する「サイバーハイジーン※」を心がけるのがいちばんです。数ある標的候補のうち、防御が弱そうだと眼をつけられない、身近なやるべきことを当たり前のようにやっている、ある意味で“清潔で”目立たない企業であることが、コストパフォーマンス的にも最善の策です。

※サイバーハイジーンとは、一般の衛生管理と同じように IT 環境を健全な状態に保つ「サイバー空間の衛生管理の取り組み」を指します。

1. 実践的で役立つサイバーセキュリティのチェックリストに基づく対策検討

最善のサイバー攻撃対策は、サイバーハイジーンの考えに基づいたサイバーセキュリティ対策とわかっていても、何から手をつけたらよいか迷ってしまいます。

そこで、“対策チェックリスト”を作りました。今回は、その中から、身近でできる対策項目を２つ選び紹介します。

チェック項目１

社外ネットシステム接続時のセキュリティ対策に多要素認証を採用していますか。	Yes / No

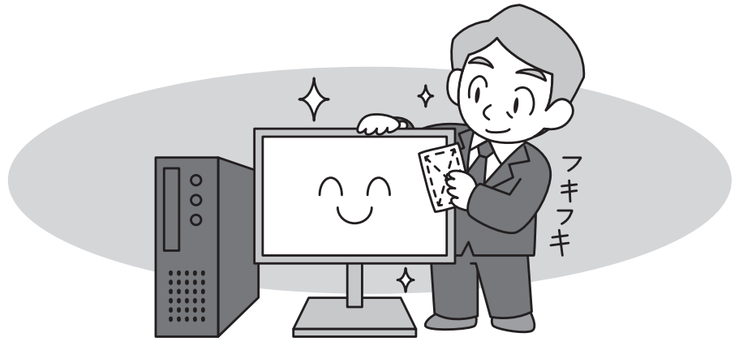
ポイント

22年９月上旬、ある会社が行った、サイバーセキュリティの防衛体制についての企業による自己評価の聞き取り調査結果が、新聞に載りました。調査は、21年7～12月、世界の3441社を対象になされ、日本は、サイバー攻撃の糸口となる脆弱性の修正についての項目で、世界の最低水準であることがわかったといいます。

ポイントは、脆弱性に気づいたら、放置することなく直ちに修正を施すなどの対策をとるかどうかです。調査によると、この対策をとった企業の割合が、他の国の場合と比較して目立って低かったのです。

脆弱性の修正についての項目でレベルも低いと評価されていたのは気になるところですが、救いは日本企業に共通の弱点とされている点については、身近なところで改善できる余地がありそうなことです。

とくに、社内システムに容易に侵入されないよう、“認証システムの高度化”を図るべきです。具体的には、「多要素認証」を採用するのが有効です。これは、ID・パスワードなどの「知識情報」、「所持情報」、および「生体情報」の３要素の中から、２つ以上の認証要素を用いて認証する方法を指します。



なぜ、こうした二重、三重の防御体制が必要になるかといいますと、もしパスワードを推測されてしまったとしても、他の要素が揃わないかぎりログインできないようにするためです。

日本では、主要企業でさえも、社員が設定するパスワードの多くが“脆弱”だといわれています。実際に漏洩したパスワード約２万５千件について新聞社が調査したところ、64%が推測されやすい設定で、「12345」や「password」のようなものが、利用数の１位と２位を占めていたそうです。ちなみに、これらは、“プロ”の手にかかると瞬時に解読されてしまうといいます。

こうした“単純”パスワードを“複雑”に変えるのは、コストも掛けず容易にできます。ただ、複雑なパスワードを嫌ったり、変えたパスワードの内容を忘れてしまう社員が出てくるのが難点です。そのため、各社員に任せるのではなく、企業が音頭を取って、組織全体で多要素認証を採用するのが良いでしょう。

生体認証と組み合わせるところまでやれなくても、メールの都度送るワンタイムパスワードを活用するだけでも、相当程度のリスクを軽減できます。しかも身近で簡易な２要素認証は、中規模以下の企業のほうが徹底しやすいとも考えられます。

チェック項目２

コンピュータ・ウイルスに感染しないよう、サイバー環境の衛生状態を“清潔”に保つよう努めていますか。	Yes / No

ポイント

サイバー攻撃の手口は、日々高度化していますが、典型的なのは、コンピュータ・ウイルスに感染させて、システムからデータを盗み出すというものです。

この手口のサイバー攻撃対策は、単純です。何よりもウイルスに感染しないよう、しっかり“予防する”ことに尽きるからです。

ウイルスといえば、2020年春以来、日本でも猛威をふるった新型コロナウイルスへの感染防止の決め手は、ワクチンです。ワクチンと並び、より身近でだれでも簡単にできる予防策が、うがい、手洗い、マスク着用、“密”を避けるなどの励行です。

自然界のウイルスになぞらえて、コンピュータ・ウイルスとこれへの感染、予防のためのワクチンというように、同じ用語を用います。共通して、ワクチン以上に有効なのが、身の回りの“衛生環境”改善です

新型コロナウイルス対策としての、手洗いやマスクについては、かなり社会で浸透していますが、サイバー空間では、何をどうすればよいでしょうか。

それには、「サイバーハイジーン」の徹底が最善の策とする考えが有力になっています。もともと英語のhygieneは「衛生」を表しますから、サイバーハイジーン（CH）は、「サイバー衛生管理」と訳されます。

CHは、身の回りの基本的な対策を重視します。企業が使う端末やPCの状況を把握し、認識した脆弱性を修正するパッチを適用する、認証とアクセス制御による最小権限の原則を適用する、などを着実に実践していけば、最も有効にサイバー攻撃を防げるとの考えに基づくからです。

おわりに

サイバー攻撃への備えは、中小企業にとって、最新のワクチン導入もさることながら、身の回りのサイバー衛生向上を優先させるべき場面が多いといえます。

日本だけでなく世界中で、企業が使うサーバーや基幹パソコンの約半数が古いまま放置されているといいます。

とくにメーカーのサポート期限切れの古い基本ソフト（OS）を搭載したサーバーを使い続けていると、サイバー攻撃のリスクは格段に増大します。

古い基本ソフトの更新は、デジタル化(DX)を進めるなかでいずれ必要になります。サイバー攻撃への備えとして、上述したチェックポイントに示した対策を複合的に実施し、少しでもリスクを減らしておくのが良いでしょう。