特集

サイバーセキュリティの新局面

コロナに便乗するサイバー攻撃

今年6月、ホンダの複数の工場が操業を停止し、出荷を一時停止する事態に陥りました。原因はコロナショックによるサプライチェーンの混乱……ではなく、サイバー攻撃でした。

ランサムウエア（身代金要求型ウイルス）が社内ネットワークに入り込んだことによりシステムがダウン。従業員が使うすべてのパソコンを初期化して回復するのに1週間程度の時間を要したとされます。システム内のデータの一部は失われたとみられ、株主総会を目前に控えて多大な影響が全社に及びました。

ホンダに対する攻撃には、時間をかけて周到に仕組まれたマルウエア（悪意を持ったプログラム）が使用されていたとされるので、コロナショックと直接関係するわけではありません。しかし、新型コロナウイルス感染拡大の裏で、サイバー攻撃は確実に厳しさを増しています。

いまに始まったことではないとはいえ、働き方改革やテレワーク導入のためにシステムの見直しを急ぐあまりあちこちに生じたセキュリティの「穴」を、攻撃者側は見逃しません。急激なIT環境の変化がリスクを拡大させていることは確かです。

新型コロナウイルスの感染拡大にともなう具体的な手口としては、PCR検査やクラスター、マスクといった関連するキーワードを用いて、厚生労働省や保健所を装って偽メールを送りつけるものがあります。人々の関心が高い情報を提供すると見せかけて、ウェブサイトに誘導したり、添付ファイルを開かせたりするものです。

ただし、こうしたサイバー攻撃は目新しいものではなく、過去に何度も世の中のホットワードに便乗して行われてきました。たとえば、オリンピックです。本来ならば2020年の夏は、東京2020オリンピックで日本中が沸いていたはずでしたが、こうした大規模イベントは攻撃者が最も好むものの1つです。

広い意味での営利目的や、特定の思想に基づいて行動するハクティビスト（ハッカーとアクティビストを合わせた造語）、さらには単なる嫌がらせと動機はさまざまですが、国家レベルの祭典がサイバー攻撃によって大きなダメージを受ければ、国の威信を揺るがしかねません。

2014年のロンドンオリンピックでは、23億5000件のセキュリティイベントが発生。メインスタジアムへの電力供給システムもターゲットになるなど、大混乱を引き起こしかねない脅威にさらされました。物理的に人が集まるところや世間の注目度が高いと

ころは、攻撃者にとって、最小限の攻撃で最大の戦果を得る効率の良い攻めどころでしかないのです。

来年、無事に東京でオリンピックが開催された場合も、世界中の攻撃者が日本をターゲットにしてくることはまず間違いないでしょう。国や東京都はもちろん、オリンピックに直接関係しない民間企業も巻き込まれる可能性は十二分にあります。

戦い方を変える時がきた

世の中の変化や人々のわずかな隙をついて攻撃をしかけてくるサイバー攻撃に対して、企業はどのようなセキュリティ対策を取れるのでしょうか。いま注目されている新たなコンセプトが、「ゼロトラスト」です。直訳すれば、何も信用しないということになります。

ゼロトラストが注目される背景には、社内のネットワーク環境は安全と考えて、外から攻め入ろうとする敵に対して、ファイアウォールやＩＰＳ（侵入防御）、ＩＤＳ（侵入検知）などで内を守ろうとする従来のセキュリティ対策の限界があります。攻撃者側がこうした境界型のセキュリティ対策を悪用することを考えついて、利用するようになったからです。

ホンダのケースでも、社内ネットワーク内部だけで感染を広げるマルウエアが攻撃に用いられたとされます。何らかの方法で境界の内側に入り込み、その中にいることが確認できた場合にのみマルウエアは活動する。こうなるとネットワーク内は安全だと考える従来型のセキュリティ対策では被害の拡大を止められません。

これに対してゼロトラストでは攻撃されることを前提に、境界の内外に関係なく、社内システムへのアクセスなどに対して常に安全かどうかチェックを行います。

本特集の「ゼロトラストという新たな戦術」ではこの注目のセキュリティモデルを、確実に広がりつつあるテレワークとの関係も踏まえて解説します。筆者の門林雄基・奈良先端科学技術大学院大学教授によれば、新型コロナウイルス感染症対策としてのテレワークは、バイオリスクがサイバーリスクを上回るという認識のもとで採用されるといいます。突き詰めて言えば、サイバー攻撃による損害をある程度受容してでも、従業員塔の感染による損害を回避したい場合にテレワークが選択されるということになるでしょう。テレワーク時代において、サイバーセキュリティにおけるこの新しい戦い方をどのように取り入れるべきなのか。論考では、各社各様の答えを導き出すためのアプローチが示されます。

中小企業のセキュリティ対策は、さらに問題が山積しています。サプライチェーン上の弱点となる中小企業を足がかりに、大企業や官公庁への攻撃をしかけるケースは数え切れないほど報告されていますが、対策はいっこうに進んでいません。「中小企業の課題と望まれるセキュリティ対策のあり方」では、実情をよく知るＳＯＭＰＯリスクマネジメントの永塚純一氏が、経営資源が圧倒的に不足する中での現実解を示します。

へこたれず、しなやかに回復する

問題は、何をどこまでやってもゼロリスクはあり得ないということでしょう。３密を避け、マスクと手洗いを励行したとしても、社会生活を営む以上、感染リスクをゼロにすることはできないのと同じです。こうした現実に対峙するうえで有効なのが、自然災害などにも適用される「減災」という考え方です。

国立情報学研究所の高倉弘喜教授は、『求められる「サイバー攻撃減災」の発想』の中で、サイバー攻撃を受けてもへこたれずに業務を継続する強さをもつという考え方を提示しています。サイバー攻撃による被害が発生したからといって直ちにすべてのシステムを遮断して業務を中断するのではなく、監視を強化して延焼を防ぎながら、継続できる業務は継続するというものです。

そのうえで、マネジメント層が判断し、準備しなければならない問題は多いとも指摘します。事業の社会的影響も含む重要度を見据えたうえで、場合によってはＩＣＴに頼らない人の手による事業継続に備えておくこともその１つです。

さらに緊急時には、経営層自身も真価を問われることになります。担当者から、不完全な情報を、初めて耳にする専門用語を並べて説明されることで疑心暗鬼になり、ミスリードをしたり現場に過度な負担をかけてしまうエリートパニックに陥るトップは珍しくありません。実際、東日本大震災の原発事故では、さまざまなところでこうしたケースがみられました。コミュニケーション力に優れた技術陣との間で、日ごろから信頼関係を築いておくことが不可欠になるでしょう。

どの論考も、むずかしい技術用語やカタカナをできるだけ避けて、わかりやすく書かれています。「サイバーセキュリティ？興味ないな」という方にも、ぜひ読んでいただきたいと思います。ここに書かれているのはサイバー空間（だけ）のことでなく、私たちが生きる実世界、フィジカル空間の話であり、経営そのものの課題でもあるからです。