ウィルス感染対策とゼロトラスト

ゼロトラストが必要な理由

- ペリメタモデルのセキュリティ対策では、テレワークは無理
- 使用する場所や、時間帯を限定したくない
- 脅威は 100%排除することはできない
- 全ては信頼できないから、必ずチェックすべき
- 許可された人がアクセスしてきているのか？
- アクセスしてきたデバイスは許可されたものか？
- デバイスにマルウェアは感染していないか？
- OS やセキュリティソフトウェアは最新か？
- ログは取得できているか？

新型コロナウィルスに代表される感染症拡大防止のための考え方は、IT セキュリティ対策のゼロトラストに通じるものがあります。
季節や気温では終息しない新型コロナウィルスのような感染症は、残念ながら、多くの人々が抗体を持って集団免疫できる状態にならないと、流行を止めることができません。だからこそ、ワクチンの開発が熱望されているわけですが、ワクチンがない状態では、ロックダウンなどの強い介入によって一時的に感染者を極端に少なくできたとしても、いずれ第二、第三のアウトブレイクが起きてしまうと予想されています。よって、ある程度、感染者が増えることは、そのバランスをみながら容認しなければなりません。これにより、通常の生活を送るためには、自分が感染しているかもしれないことを前提に、三密を避け、マスクの着用、手洗いなどを習慣化して、他人にうつさないような行動が重要となります。
もちろん、誰もが新型コロナウィルスに感染したいとは思っていません。しかしながら、ずっと長い間全員が家から 1 歩も出ず仕事をしなかったら、経済活動は止まり、いずれ生活できなくなってしまいます。つまり、感染するかもしれないけど、被害を最小限に食い止めるという対策が必要となってきているのです。
これは、IT セキュリティ対策におけるゼロトラストの考え方と同じです。
現在、新型コロナの流行に乗じて、ハッキングなどのサイバー犯罪が増加していますが、もし、会社以外はセキュリティ上不安なのでテレワークはできない、という昔ながらの考え方に固執してしまったら、どの企業もリモートワークはできません。いわゆる、ペリメタモデル（perimeter-based）といわれる Firewall や、マルウェア対策ツールによって、守るべき境界線をつくり社内のネットワークは安全で、社外は危険と考えるネットワーク境界の防御を徹底する従来のセキュリティ対策では、働き方改革で効率化を目指す、時代の要請に答えられなくなってきています。
これに対し、ゼロトラストモデルでは、たとえばリモートワークで使用する PC はすでにマルウェアが潜んでいるかもしれないという観点で、どこからでも仕事ができるという利便性を残したまま、徹底した認証やアクセス管理、使用デバイスなどの管理を行い、ログも取得して必ずセキュリティのチェックをします。こうして、境界線の入口出口のチェックがメインだった方法とは違い、厳密なアクセス管理によって、インシデント発生時の被害も最小限にくいとめます。
感染症対策として流行ってきたテレワークですが、この機会にゼロトラストの考え方も徹底した方がよさそうです。