2022 年 3 月 1 日

Venture Solution

## コラム記事

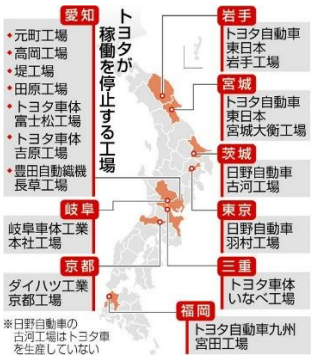
サイバー攻撃は自社のシステムや営業を停止するだけではなく、取引先へも被害を拡大させてしまう恐れがあるため
復旧についても時間を要する場合が多くあります。
サイバー攻撃を受けた場合の対策をたてるのではなく、サイバー攻撃を未然に防ぐための対策をたてることが重要であると考えています。
そんな中、サイバー攻撃被害が取引先へ影響したとの記事が掲載されておりましたのでご紹介いたします。

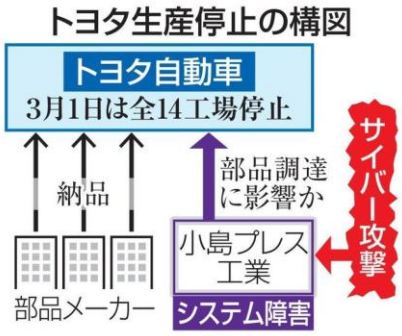
## トヨタ工場停止、部品会社がランサムウエア被害と発表

2022/3/1(火) 10:01 配信

日本経済新聞 電子版

**■トヨタ工場停止、部品会社がランサムウエア被害と発表**



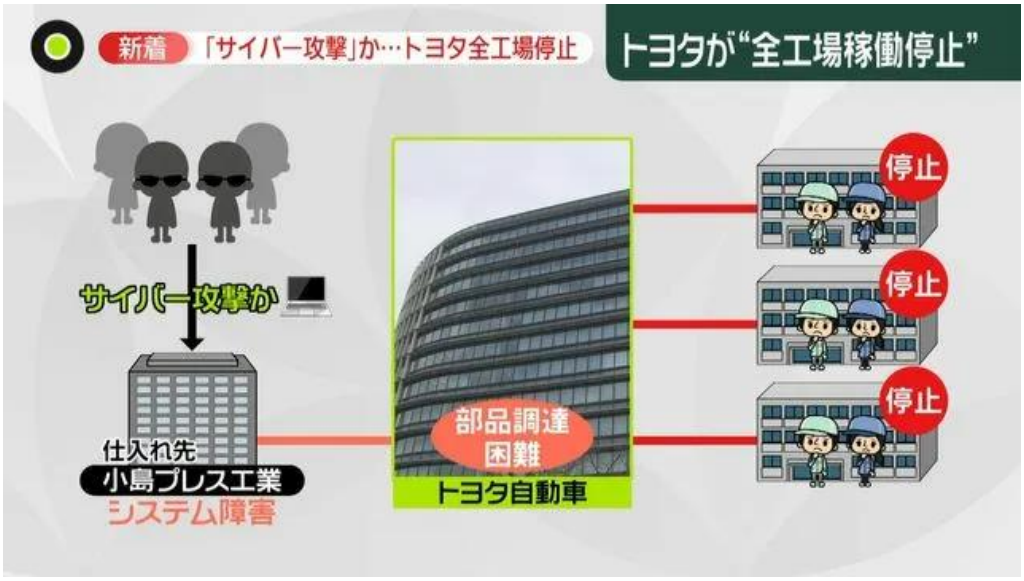

サイバー攻撃を受けた小島プレス工業（1 日、愛知県豊田市）（日経電子版より引用）

**トヨタ自動車は 1 日、部品会社へのサイバー攻撃を受けて国内全工場（14 工場 28 ライン）の稼働を止めた。トヨタ車の部品をつくるサプライヤーがサイバー攻撃を受け、部品供給を管理するトヨタのシステムを止めた。「ランサムウエア（身代金要求型ウイルス）」による攻撃を受けた。**詳細は専門家を交えて調査を進める。

サイバー攻撃を受けたのはトヨタの主要なサプライヤーの 1 社で、樹脂部品を手掛ける小島プレス工業（愛知県豊田市）。同社は 1 日、ウイルス感染を確認し、脅迫メッセージを受け取ったと発表した。小島プレスは「サイバー攻撃とみられるきっかけでシステム障害が生じたのは事実」としていた。2 日以降に通常稼働に戻せるかどうかは精査している。

2 月 26 日夜にウイルス感染を確認、27 日にウイルスの感染拡大を予防するため、外部とのネットワークを遮断した。攻撃の発信元やウイルス感染の具体的な被害状況については「調査中」としている。

トヨタは高岡工場（愛知県豊田市）で「カローラ」などを、田原工場（愛知県田原市）で高級車「レクサス」を生産している。このほか多くの車種が影響を受ける見込みだ。**国内全工場を 1 日に止める影響は、トヨタの国内の月間生産台数の 4～5%にあたる約 1 万 3 千台に上る**。日野自動車とダイハツ工業も同じ理由で同日、国内工場を一部止めた。




（日経電子版より引用）

被害に合わないようなセキュリティー対策を取り、守ることが出来るのは自社だけではありません。
取引先企業や関連企業を守るためにも、サイバー攻撃を受けないような対策を講じる必要があると感じています。
まずは自社を守る、そのためには侵入されてから撃退するセキュリティー対策でいいのか、侵入前にブロックしてしまう対策が良いのか、検討していくべきだと考えています。