

 **【緊急号】通信　i・ストリーム（法人版）VOL.43**

文：小川 康成

ﾌｧｲﾅﾝｼｬﾙ・ﾌﾟﾗﾝﾅｰ

　**「トヨタ自動車の取引先部品会社がサイバー攻撃」**と言うニュースが出ました。

今回の攻撃を受け、トヨタの国内工場をはじめ日野トラックの主力生産拠点工場、

ダイハツの一部の工場などが操業の停止となり、1日の停止で数百万台程度の減産となるそうです。セキュリティ専門家によると、最近はサイバー被害の相談が急増しているそうですので、各社再確認して下さい。大手企業は高度な対策を施して直接な攻撃は難しいので、取引先や関連企業を狙う手口が一般的となっています。中小企業者として、今までにないサイバーセキュリティを意識するべき時代に入ってきました。



◆ **会社のパソコンやサーバー等に保存されていた機密情報や個人情報が外部に流出**

**◆ Webサイトの内容が書き換えられたり、ウイルス等の設置**

**◆ 不正なプログラムの感染で、不正送金や迷惑メールの送信等、意図しない処理が行われる**

**◆ 外部からの大量アクセスで、システムダウンによりホームページの停止や停滞**

**◆ ランサムウエアにより、ファイルが暗号化され使用出来ない状態になり、身代金の要求**

**「サイバー攻撃」は企業規模に関係なく、攻撃されます。**

サイバー攻撃とは、会社のパソコンやネットワークに不正に侵入して、データ損壊や改ざん、情報の盗取、システムダウンによる障害等の損害を与える不正な行為です。手口や被害は様々ですが、年々高度化、巧妙化してきています。

**＜サイバー攻撃の例＞**



2019年に発表された神戸大学×大阪商工会議所×東京海上日動社の共同研究に

よると、商工会議所会員の中小企業の**１００％**でウイルス付メールや、不正なサイトへ

のリンクが添付されたメールも含め、悪意あるネット上の攻撃が確認されました。

また**約2割**の企業のパソコンから、**情報を見られたり、暗号化された情報が見られる状態**になっていた。外部からの遠隔操作が可能な状態になっている等、サイバー攻撃の被害にあっていた、もしくは遭う可能性が高い状態になっていたそうです。

同調査では、被害企業のうち約4分の1の企業から、メールを装ったウイルスメール攻撃などで、取引先の企業がサイバー攻撃を受け、それらが自社にも及んだそうです。



上記のような驚くべき実態調査が明らかになり、また年々攻撃の数は増えていて、一時期猛威を振るったコンピュータウイルス**「エモテッド」**と呼ばれる**マルウェア**(**※**)が再拡大しています。企業のパソコンが**感染すると、自社のメールを装い、取引先にもウイルスメールを勝手に送信し始めるので、気が付いた時には元請け企業など取引先企業にも多大なる迷惑をかけ、場合によっては以後の取引停止という事態も考えられる程の脅威です。**



* メール情報を盗み取るなどする悪意あるプログラムの一種

◆ **取引先とメールでのやり取りはしていませんか？**

◆ **社内のパソコンで外部のインターネットに自由に接続可能な状態になっていませんか？**

◆ **Wi-Fi（特にフリーWi-Fi等）を使用して、社用のパソコンを使用していませんか？**



**サイバー攻撃**

**動画**

**↑上記に一つでも当てはまるようであれば、注意が必要です。**



**個人情報とは？**

個人情報保護委員会の説明によれば、個人情報とは、「**生きている個人**に関する情報で

あって、その人が誰なのかわかる情報」をいいます。
　例えば、「氏名」や「その人が誰なのかわかる映像」などが個人情報です。また、「携帯電話番号」や「住所」だけでは「その人が誰なのかわかる」とは判断できませんが、「氏名と住所」など、**他の情報と組み合わせることで「その人が誰なのかわかる」ようであれば、個人情報**です。
　なお、公的な番号として1人に1つ異なる番号が割り当てられた「マイナンバー」、パスポート番号や、指紋など個人の生体情報をデータ化したものも、それだけで「その人が誰なのかわかる」ので、個人識別符号と呼ばれる個人情報です。また、会社が所有している社員の情報も大切な個人情報です。

本人への通知が義務付けられた事により、お詫びの対応が増える事が予測されます。

**漏えいの報告が義務化され、報告期限は30日以内**

**個人情報保護法　令和4年4月1日に改正施行（30日以内の対応が必須）**



**改正施行での変更点**

◆ 個人情報の漏えいが発覚した場合の**本人への通知が義務付け。**同様にへの報告も必要。

◆ 委員会の命令違反の罰則が従来の50万円以下の罰金から、**1億円以下の罰金**へ引き上げ

◆ 情報の利用停止・消去等の個人請求権が法令違反の場合に加えて、正当な権利や利益が侵害される場合の恐れも含めて、請求できるように要件を緩和。

* **個人情報保護委員会**

**原因究明費用は高額です。支払事例：PC10台の会社で、1,500万に！！**



**「サイバーセキュリティ保険」には必ず、加入をしておきましょう！**

・**ソフトウェアやウイルス対策ソフトは最新状態ですか？**

⇒ パソコンのOSやWebブラウザの修正プログラムやウイルス対策ソフトの

最新情報へ出来るだけ早い対応が必要です

**・IDやパスワードの管理は適切ですか？**

⇒ パソコンやシステムのIDやパスワードは、他人に推測されにくい設定と厳重の管理が必要です

**・標的型メール攻撃への心構えやルールは出来ていますか？**

⇒ 従業員がメールや添付ファイルを開いてし、ウイルス等が感染してしまわないように

日頃から訓練や不審点が無いかを確認する意識向上の学習会などが有効です

**・パソコンや外部記憶媒体の利用ルールは有りますか？**

⇒ Webサイトの閲覧や外部記録媒体の利用ルールの作成と徹底で、組織のネットワークにウイルス等

の進入や感染、重要な情報漏えいの防止になります

**～ 留意すべきポイント ～**







万一、サイバー攻撃被害に遭ってしまった場合は、**原因究明のためのPC点検などで、1台あたり1５0万円～200万円と多額の費用が掛かります。**ただ、どれだけ対策しても100％の防御は難しいので、ウイルス対策ソフトの導入と合わせ、**サイバー被害を受けた際に補償対象となる保険**などに加入して、緊急時の多額な費用を補う手配もしておきましょう。保険料は、意外とお安く5万円～加入可能です。また、日本政府の企業へのサイバー防衛を義務付ける動き同様、今後は大手企業よりサプライチェーン（供給網）の安全確保を目的に、発注先の下請け企業にも、サイバー対策や意識向上を求める動きが広がる事も考えられます。**大手企業や取引先などからサイバー対策についての義務付けや確認**が有った場合、きちんと回答出来るよう、自社の対策について考えてみる機会にして下さい。

****

**〒489-0976　瀬戸市井戸金町422-1**

**電話(0561) 83-8111　　FAX(0561) 83-8131**

**ﾎｰﾑﾍﾟｰｼﾞ http://istream-web.jp**

**E-Mail　 istream@istream-web.jp**