かわら版

2020年12月 NO.12
合同会社ＩアンドＳ
福岡市中央区大名2-10-1Ａ1208
TEL092-791-1498 Fax092-791-1641

暴露ウイルス　1000社被害

盗んだ情報をさらして相手を脅す「暴露型ウイルス」と呼ばれる新型サイバー攻撃の被害企業が2020年1月～10月に世界で1千社を超えることがわかった。企業から盗み取った機密情報を暗号化し、元に戻すための身代金を求める。要求に応じないと情報を暴露する。情報流出は社会的な信用も傷つけるだけに、企業は対策が急務。

～対策Ｑ＆Ａ～

問１Ｑ．暴露ウイルスの被害にあった時はどうしたら？
　　Ａ．業務システムの復旧手順を熟知するＩＴ企業などへ相談する

問２Ｑ．身代金要求されたらどうしたらよいか？
　　Ａ．支払うべきではない（犯罪組織への活動資金となる為）

問３Ｑ．被害状況の公表はするべきか？
　　Ａ．顧客、取引先に速やかに情報公開するべき（二次被害を防ぐ）

問４Ｑ．盗まれたデータは取りもどせる？
　　Ａ．取り戻せないと考えるべき。

問５Ｑ．予防策は？
　　Ａ．ＵＳＢ端子で接続するハードディスクに保管する
　　（社内ネットワークからは　　切り離し保管できるようにする）
　　ファイルを暗号化し、パスワード設定し保管する事も効果がある。

デンマークでコロナ変異種

北欧のデンマークでは、毛皮を採取するための家畜のミンクから変異した新型コロナウイルスが見つかり、人への感染が確認されたとして、政府は国内の農場で飼育されるミンク、最大で1700万匹を殺処分にする方針を明らかにした。

デンマーク政府は、毛皮を採取するための家畜のミンクの農場で、変異した新型コロナウイルスがみつかり、ミンクから感染したとみられる12人からも確認されたことを明らかにした。

フレデリクセン首相は、変異したコロナウイルスは、将来、開発されるワクチンの有効性を弱める可能性があると指摘し、国内の農場で飼育されるミンクをすべて殺処分にする方針を明らかにした。

首都コペンハーゲン近郊にある農場では、殺処分が始まり、この農場の男性は、「うちには感染したミンクはいないが、なるべく早く処分しなくてはならない。すべてのミンクを失うのは大きな打撃だ」と話していた。

デンマークは世界でも有数のミンク毛皮の生産国として知られていて、国内で飼育されているミンクは最大で1700万匹にのぼる。

ミンクをめぐっては、これまでにオランダやスペインでも、殺処分が行われた。

ＤＤｏＳ恐喝　相次ぐ

「カネを出さなければウェブサイトをパンクさせるぞ。」こんな恐喝めいたサイバー攻撃が国内で相次いで確認された。「はったりではない」と示すかのように、実際に短時間、大量のデータを送りつけてくるのが特徴だ。慌てて脅しに乗らないためには攻撃を想定した備えが重要となる。

コンピューターウイルスで乗っ取った機器などを使ってサイトに大量のデータを送りつけ、過剰な負荷をかけてパンクさせる手口は「DDoS（分散型サービス妨害）攻撃」と呼ばれる。

民間団体JPCERTコーディネーションセンターによると、8月以降、国内の通信事業者などに対しDDoS攻撃を予告し、暗号資産（仮想通貨）を要求するメールが断続的に複数確認された。脅迫メールが届いた後、実際に30分から1時間程度のDDoS攻撃があり、支払いに応じなければさらに攻撃を仕掛けると脅してくる。

これまで把握している範囲では支払いに応じた例はなく、応じなかったために本格的な攻撃を受けたケースも確認していないという。

海外でも同様の脅迫は相次いでおり、金融業や小売業など幅広い業種が対象となっている。8月にはニュージーランド証券取引所に脅迫メールが届いた後、DDoS攻撃が仕掛けられた。攻撃は執拗に続けられたもようで、取引所は4日間連続で取引の一時中断に追い込まれた。

DDoS攻撃自体は新しい攻撃手法ではない。トレンドマイクロなどによると、パソコンを遠隔操作ウイルスに感染させ、攻撃の「踏み台」として使う手法は2004年ごろに登場した。

あらゆるモノがネットにつながる「IoT」機器が普及するなか、16年にはIoT機器に感染する「Mirai（ミライ）」と呼ばれるウイルスが世界中で拡散。パソコンやサーバーだけでなく、ウェブカメラやスマート家電も踏み台に使われるようになった。

情報通信研究機構（NICT）によると、ミライに感染してDDoS攻撃の踏み台となる機器は20年5月に世界で約20万台観測された。感染を防ぐ対策ソフトなどは普及してきたが「ウイルスも進化を続けながら感染先を常に探している状況だ」（Ｋ上席研究技術員）という。

トレンドマイクロのＯセキュリティエバンジェリストは「闇市場では、依頼に応じてIoT機器をミライに感染させるサービスも販売されている。以前より容易に大規模なDDoS攻撃を仕掛けられるようになっている」と指摘する。

DDoS攻撃への対策としては▽サイトへのアクセスを分散する▽不審な通信を検知、遮断する。など、セキュリティー会社や通信事業者がシステムやサービスを提供している。

JPCERTの脅威アナリスト、Ｋ氏は「DDoS攻撃を受けてシステムが止まるのは一時的な被害にとどまることが多い。事前に対応を想定しておき、脅迫を受けても慌てて支払いに応じないことが重要」と話している。

コロナ禍ですが、良いお年を
お迎えください