2022 年 2 月 28 日

Venture Solution

コラム記事

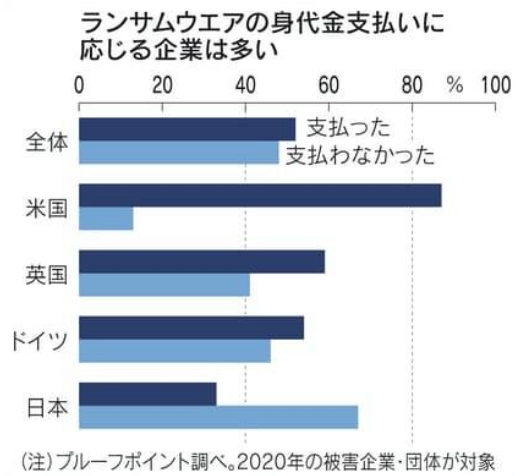
昨今のサイバー攻撃のトレンドとして、身代金を要求するランサムウエアの被害が世界で拡大しています。
機密情報の公開の代わりに金銭の支払いを要求され、金銭を支払えば情報流出を防止できるとの考えで支払うケースも数多く報告されています。
要求額は様々ですが、情報流出させない代わりに支払うのではなく、情報流出させないためにセキュリティ対策費として活用する企業様が多くなることを期待しています。
そこで、トレンドとされているランサムウエアによる身代金請求額についての記事が掲載されておりましたのでご紹介いたします。

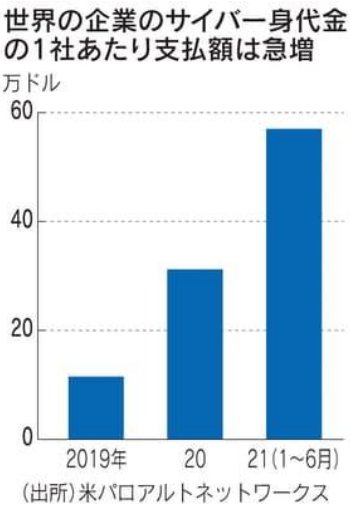
サイバー身代金、支払い 5 割　金額急増し攻撃に拍車

（日経電子版 2022/2/28(月) 05:00 配信より引用）

■サイバー身代金、支払い 5 割　金額急増し攻撃に拍車

企業にサイバー攻撃を加えて身代金を要求するランサムウエア被害が世界で拡大するなか、被害を受けた企業の過半が身代金の支払いに応じていることが分かった。取引先に被害が及ぶなど攻撃の悪質性が高まっていることが要因の一つだ。米ではサイバー保険による支払いが攻撃を助長しているとの指摘もある。**また、取引先のサイバー攻撃への防衛力を検証し、「落第点」なら取引停止を検討する例も出てきています。**





（日経電子版より引用）

身代金を払うか、払わないか――。首都圏の中小 IT（情報技術）企業の男性社長は悩んだ。ランサムウエア感染で端末が停止し、業務が続けられなくなった。パソコンには「機密情報を奪った。支払わなければ外部に公開する」とのメッセージが浮かんだ。結局、弁護士に相談したうえで数百万円相当を払い、半日以内に復旧したという。

米パイプライン運営会社コロニアル・パイプラインは 5 月に受けた攻撃で犯行グループに身代金を払ったことを認めた。「苦渋の選択だった」（ジョセフ・ブラウント最高経営責任者）。ブラジルの食肉大手 JBS も攻撃で 5 月に食肉処理場の操業が止まり、「データ流出を食い止めるため支払いを決めた」という。

米セキュリティ大手プルーフポイントが主要 7 カ国の 3600 の企業・団体（従業員 200 人以上）に実施した調査によると、**2020 年に約 2400 団体がランサム被害を受けたと回答。うち 52%（約 1200 団体）が身代金を払った**と答えた。国別では米国が 87%（約 410 団体）と最も多く、英国 59%（約 260 団体）、ドイツ 54%（約 220 団体）と続いた。**日本も 33%（約 50 団体）**あった。

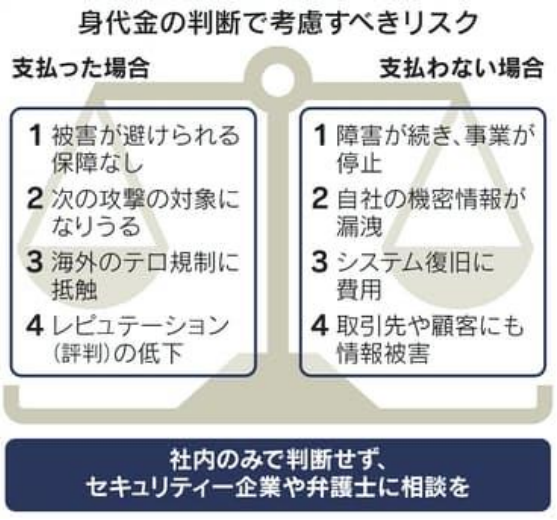
身代金を払ったことを公表した日本企業はまだない。EY 新日本監査法人の加藤信彦パートナーは「経営に重要な影響を及ぼす金額なら開示義務が生じるが、少額なら営業外費用などとして処理され、外部からは分からない」と話す。「非上場の中小・零細企業の支払いも多いのではないか」（日本サイバーセキュリティ・イノベーション委員会の上杉謙二主任研究員）との指摘もある。

ランサムウエア事案を多く手がける弁護士によると、被害企業はまずセキュリティ会社や弁護士に相談し、自力復旧に加え脅迫元との接触を探る。「相手の素性調査、支払いによる復旧の見通し、身代金額の交渉など複数のプロセスを踏む。そのうえで企業は支払うかどうか判断する」という。多くは警察にも捜査を求めるが、中小・零細企業の中には最初から届け出ない企業もある。

身代金の支払額は年々増えている。米サイバー大手のパロアルトネットワークスによると、**世界の企業 1 社あたりの支払額は 20 年に 31.2 万ドル（約 3400 万円）と 19 年比 3 倍に急増**。21 年 1～6 月は約 57 万ドルと拡大が続く。

標的がインフラや生活産業、大手サプライチェーンなどに広がり、個人情報や機密データを奪うなど悪質な攻撃が急増している。急ぎ対応しなければ顧客や取引先にも被害が及びかねない。企業は自社の信用低下を避けようと被害隠蔽を図り、支払いに応じてしまう。

サイバー犯罪者がサイバー保険に加入する米国企業を調べて狙っている可能性があるとの指摘も聞かれる。英ソフォスが 26 カ国の企業・官公庁の IT 管理者 5000 人を対象に実施した 20 年調査では、ランサムウエアに対応したサイバー保険への加入割合は米国が 75%と世界平均（64%）を上回る。



（日経電子版より引用）

増える身代金を問題視し、米政府は支払いに制限をかけ始めた。米財務省の外国資産管理局（OFAC）は 20 年 10 月、ロシアや北朝鮮、シリアなどとの関係が疑われる組織への支払いが制裁対象になり得ると表明した。とりわけロシアやその周辺国とみられる集団による攻撃が急増しており、何らかの追加措置が取られる可能性がある。

日本も経済産業省が 20 年 12 月に発行した経営者向けの文書で、ランサムウエアについて「金銭の支払いは厳に慎むべきだ」とした。

サイバー犯罪者の脅迫行為は違法となる一方、被害企業側の支払いを禁じる法律はない。企業の身代金支払いをすべて禁じるのは容易ではない。米連邦捜査局（FBI）は「ビジネスが機能障害に陥った場合、経営陣があらゆる選択肢を評価することは理解する」と指摘する。

そのなかで、企業は専門家に相談するなど慎重な判断が必要となる。サイバー法制に詳しい山岡裕明弁護士は「被害規模や支払わずに復旧できる可能性を確認しないまま払えば、経営陣が善管注意義務違反を問われる可能性もある」と話す。

安易な支払いは脅迫行為を勢いづかせ、サイバーテロの温床となりかねない。自社のサイバー防衛を最新の状態にしたうえで、被害を受けたらいち早く捜査機関に通報したり、業界団体と情報共有したりする適切な対応が求められる。

（サイバーセキュリティーエディター　岩沢明信、渡辺直樹、島津忠承）

以前までは身代金要求の対象となるのは「人」でしたが、いまは「情報」の時代へ変化しているように感じています。
要求される金額が支払える金額であれば、お金と引き換えに情報を取り戻せるのであれば、支払う企業があることは頷けると思います。
ただし、その支払う金額をセキュリティ対策費として利用できていれば、社会的信用度を落とすことも、それに伴う事業縮小もあり得なかったかもしれない…と後悔するのであれば、そんな心配をしないように対策を講じる必要があると考えています。