

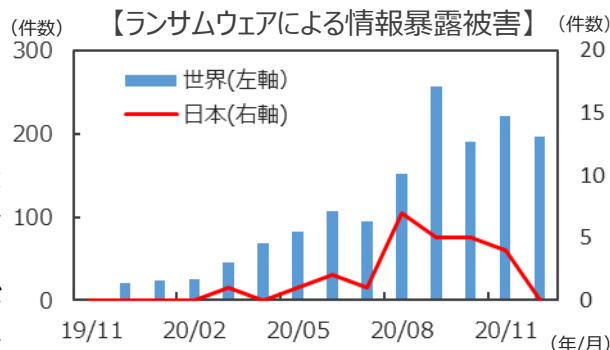


## 今日のキーワード DX時代のジョーカー、企業を狙う『サイバー攻撃』

デジタルトランスフォーメーション（DX）時代の到来で私たちの生活はますます便利になり、ビジネスも飛躍的に効率化しています。その一方で、コンピューターウイルス「ランサムウェア」を使って企業を脅迫する『サイバー攻撃』が世界で頻発しています。コロナ禍によるリモートワークの普及や社外サーバーを活用するクラウドコンピューティングの浸透が、こうした『サイバー攻撃』への防御を難しくしている面もあり注意が必要です。

### ポイント1 猛威を振るう『サイバー攻撃』

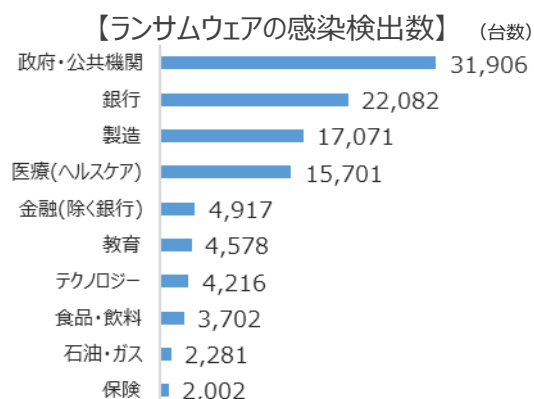
- 企業を狙う『サイバー攻撃』が世界で猛威を振るっています。米国では大動脈の東海岸沿いの石油パイプラインが止まり、一時ガソリン価格が急騰しました。オーストラリアでは世界最大規模の食肉加工場が操業停止に追い込まれ、またアイルランドではほぼ全域で病院のシステムがダウンしました。
- 深刻な事態を受けて、先のG7では米国のバイデン大統領がこうした企業を狙う『サイバー攻撃』に共同で対処するよう呼び掛けるなど、参加各国でも危機感が高まっています。



Copyright (C) 2021 Trend Micro Incorporated. All rights reserved.  
(注) データは2019年11月～2020年12月。  
(出所) トレンドマイクロ社のデータを基に三井住友DSアセットマネジメント作成

### ポイント2 悪質かつ卑劣な「ランサムウェア」

- 近年特に被害が大きいのが「ランサム（Ransom、英語で身代金）ウェア」を使った『サイバー攻撃』です。
- 「ランサムウェア」を使った『サイバー攻撃』では、まず社員に成りすましたハッカーがターゲットとなる企業のネットワークに侵入、「ランサムウェア」をばらまき企業のデータを暗号化して使用不能の状態にします。そしてこの暗号化されたデータを人質に身代金を要求、更に身代金の支払いを拒否した場合は搾取した情報を一般に公開すると脅す、2重の脅迫となっている点が特徴です。



Copyright (C) 2021 Trend Micro Incorporated. All rights reserved.  
(注) データは2020年。  
(出所) トレンドマイクロ社のデータを基に三井住友DSアセットマネジメント作成

### 今後の展開 今後は日本でも被害拡大が

- これまでは言葉の壁もあり、日本企業が狙われるケースはあまり多くありませんでした。今後は中国系ハッカーの活動活発化もあり、被害の増加が懸念されています。こうした『サイバー攻撃』を受けた企業では、事業継続が困難になるだけでなく機密情報の流出リスクに見舞われるため、その被害は甚大です。
- 更に、公益や通信といった社会インフラを担う企業が狙われた場合、その影響は社会全般に及ぶため、大規模災害時のように金融市場全体が動揺するような事態にもなりかねず、注意が必要です。

ここもチェック! 2021年3月31日 AI活用などにより、『美容家電』への参入が相次ぐ  
2021年1月28日 PPAPは危険? 高まる情報セキュリティの重要性

■当資料は、情報提供を目的として、三井住友DSアセットマネジメントが作成したものです。特定の投資信託、生命保険、株式、債券等の売買を推奨・勧誘するものではありません。■当資料に基づいて取られた投資行動の結果については、当社は責任を負いません。■当資料の内容は作成基準日現在のものであり、将来予告なく変更されることがあります。■当資料に市場環境等についてのデータ・分析等が含まれる場合、それらは過去の実績及び将来の予想であり、今後の市場環境等を保証するものではありません。■当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。■当資料にインデックス・統計資料等が記載される場合、それらの知的所有権その他の一切の権利は、その発行者および許諾者に帰属します。■当資料に掲載されている写真がある場合、写真はイメージであり、本文とは関係ない場合があります。