

## コラム記事

多く投資家にとってサイバーセキュリティ対策への取り組みは、投資先企業を決定する上で重要な指標となっております。2022年からは個人情報保護法の改正にともない、情報漏えい等の報告が義務化されているため、いつ・どの企業で・どのような情報が漏えいしたのかすぐに知ることが出来る環境へ変化しています。企業の信頼度にもつながる「個人情報管理対策」を万全に取ることで、大切な顧客情報を守りましょう。そこで、個人情報の流出と株価の関連性について、記事が掲載されておりましたのでご紹介いたします。



### 個人情報漏洩を公表した上場企業の約8割が公表直後に株価が下落

(Gunosy 2022/2/22(火) 11:01 配信 より引用)

#### ■サイバーセキュリティクラウド「個人情報漏洩被害公表と株価の変化に関する調査レポート」

近年、サイバー攻撃数の増加や攻撃手法の巧妙化によって、企業におけるサイバーセキュリティ上の脅威が高まっており、直近では、ソフトウェアやシステムの脆弱性を悪用した攻撃や標的型メールなどを通じてランサムウェアに感染させられるなどの被害が多数発生している。

このようなサイバー攻撃を受け個人情報が漏れると、企業のブランドイメージの毀損だけでなく、株価の下落や損害賠償費用の負担など、経済的に大きな損失を被る恐れがある。

そうした中、サイバーセキュリティクラウドは、2021年1月1日から2021年12月31日までに公表された、漏洩件数1,000件以上の主なサイバー攻撃に関する個人情報漏洩事案に基づき、『個人情報漏洩被害公表と株価の変化に関する調査レポート』を発表した。電子カルテシステムが被害に遭った病院では、オンラインで接続していたバックアップも含めて感染した事例もあり、復旧が長期化している。調査では、98%の病院でバックアップを取得していたが、ネットワークから遮断したオフラインで保管していたのは47%にとどまった。

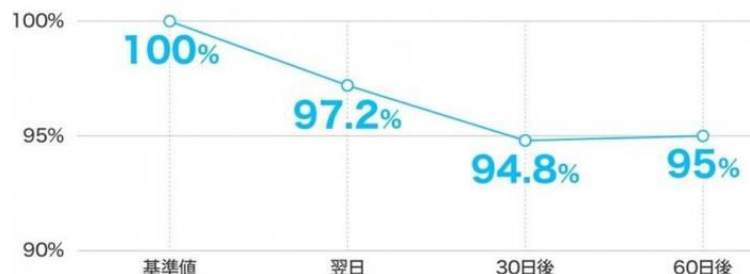
厚生労働省も1月下旬から、全国の病院に脆弱性が指摘された機器の使用状況や、バックアップの取り方に関する調査を実施している。調査結果を踏まえ、各病院に個別に改善を促す。

#### ■個人情報漏洩を公表した上場企業のうち、約8割が公表直後に株価が下落



[個人情報漏洩被害の公表後の株価の変化]

(Gunosy より引用)



調査対象とした110件の個人情報漏洩事案のうち、約2割となる24件が上場企業で発生しており、さらにそのうちの18件がサイバー攻撃に関する個人情報漏洩事案であることがわかった。

さらに、上記の被害にあった上場企業において、**情報漏洩に関する適時開示の前日と、適時開示の翌日の株価終値を比較したところ、約8割となる14社の株価が下落。14社のうち、最大下落率は21.6%、平均下落率は2.8%**となった。同様に、14社の情

報漏洩に関する適時開示前日と適時開示を行なった 30 日後、60 日後をそれぞれ比較すると、**平均下落率が 5.2%、5.0%となり、30 日後まで下落幅が拡大し続ける**ことがわかった。

#### ■サイバーセキュリティクラウド 代表取締役 CTO 渡辺洋司氏のコメント

今回の調査で、情報漏洩事案のうち 2 割以上もの事案が、セキュリティ体制を強固に整備しておかなければならない上場企業において発生しており、またサイバー攻撃によって個人情報を外部へ漏洩すると、その企業の株価にとって、事案を公表した直後だけでなく、長期的にマイナスの影響を与え続けることがわかりました。

近年では、こうした影響の他に企業が身代金を要求され、大きな損害を負うケースも目立ってきています。そうした中、多くの投資家にとって、投資先企業のサイバーセキュリティ対策への取組み方が投資判断の重要なファクターになりつつあると考えられます。サイバーセキュリティ対策は、積極的に対策を進める一部の先進企業や IT 企業だけでなく、国内の企業全体が当事者となって取り組むべき課題になっております。

特に上場企業では定期的に自社のサイバーセキュリティを見直すなどの対策が重要視されるほか、定期的に自社の Web サイトの脆弱性を確認したり、素早く攻撃に気付いたりするような社内体制の構築が一層重要になっていくと考えられます。



株価は企業信頼度を図る上で、重要な位置づけであると認識しています。

对企业だけではなく、对个人でも言えることですが、信頼を落とすことよりも信頼度を作り上げ、高めていくことはとても難しく時間のかかることだと思います。

セキュリティ対策をしっかりと行うことは、企業信頼度を上げ安定した企業運営に結び付くと考えています。