◎くにまもりの提言65◎

# ランサムウェアは経営を止める
## アサヒ事例の衝撃

八尋 滋（やひろ しげる）
（しがく総合研究所）

２０２５年９月、国内ビール市場で圧倒的なシェアを持つアサヒグループホールディングス（アサヒＧＨＤ）が、大規模なランサムウェア攻撃に見舞われた。工場の稼働こそ一部維持されたものの、物流や受発注システムが完全に麻痺し、完全復旧までには４ヶ月以上がかかり、業績への下押し影響も大きいとみられる。

本事例からもわかるように、サイバー攻撃は単なるＩＴ関連の問題にとどまらず、重大な経営課題となっている。本コラムでは、アサヒＧＨＤのサイバー攻撃被害を一事例として紐解きながら、現在のセキュリティの在り方と企業が直面する課題について解説する。

### アサヒＧＨＤへのランサムウェア攻撃の被害は甚大

アサヒＧＨＤへの攻撃は、ロシア語圏を拠点とするランサムウェアグループによって引き起こされたとみられる。





この攻撃による被害の大きさは、定量的に見るとよくわかる。まず、個人情報の流出については、アサヒＧＨＤなどのお客様相談室に問い合わせた顧客の情報が約１５２万５００件、従業員やその家族、外部関係者の情報を含め、漏えいのおそれがある個人情報は約１９１万４０００件にのぼる。別途、漏えいが確認された情報もある。

業績への影響をみると、２０２５年10月の酒類売上は前年同月比約10％減、同年11月には20％超減となった。また、一部の市場関係者からは、２０２５年12月期の連結営業利益はアサヒＧＨＤが示している予想を10％以上下回る水準になったのではないか、との見方も示されている。こうした売り上げの減少は、自動受発注システムが停止し、電話やＦＡＸなどによる手作業対応を余儀なくされた結果、２０２５年10月に出荷量が通常時の10％程度に激減したことが要因である。そして、長期間にわたる事業の混乱も起き、２０２５年９月29日の障害発生から、システムの完全な正常化・復旧は２０２６年２月と、実に４ヶ月以上もの期間を要した。

### アサヒＧＨＤが受けた「サプライチェーン攻撃」

この事件は、現代の企業が抱える、情報システムをめぐる構造的な弱点を浮き彫りにした。攻撃の最初の入り口となったのは、アサヒグループの中枢であるデータセンターなどではなく、グループ内拠点に設置されていたネットワーク機器であった。

近年、ＤＸ（デジタルトランスフォーメーション）の推進やクラウドサービスの普及により、企業のネットワークは関連会社や取引先、外部ベンダーなどと密接に結びつくよう

になった。これにより、セキュリティ対策が強固な大企業本体を直接狙うのではなく、対策が相対的に手薄なサプライチェーンの末端企業や拠点を踏み台にして中枢へ侵入する「サプライチェーン攻撃」が急増している。アサヒＧＨＤの事例は、まさにこの弱点を突かれた形だ。

## 「バックアップを取れば大丈夫」は誤り

アサヒＧＨＤは攻撃者からの身代金要求を拒否し、自力での復旧を選択した。日本経済新聞によるインタビューでアサヒＧＨＤの勝木敦志社長は「（身代金を）支払ったところで完全復旧できる保証もなければ、支払う行為自体が反社会的勢力の助長にもつながる」と判断の背景について説明している。一方、安全性の検証やシステムの再構築に膨大な手間がかかり、数ヶ月に及ぶ業務の停滞を余儀なくされ、先述した大きな被害を受けた。

かつてＩＴの世界では「バックアップさえ取っておけば、有事の際も元に戻せる」という認識が一般的だった。しかし、近年のランサムウェアは暗号化を実行する前に長期間ネットワーク内に潜伏し、バックアップファイル自体を探し出して破壊・暗号化する手口が主流となっている。そのため、ネットワークから物理的・論理的に切り離された「改ざん不可なバックアップ」の確保が急務となっている。また、ＩＴシステムが全停止した状態でも最低限の出荷を続けられるよう、今回のアサヒＧＨＤの「手作業による業務継続」のように、実効性のあるＢＣＰ（事業継続計画）の策定が強く求められるようになっている。





## システム障害はＩＴ部門の技術的課題ではなく、経営課題である

アサヒＧＨＤは決して対策を怠っていたわけではなく、不審な挙動を検知するＥＤＲという最新セキュリティツールを導入していた。それでも今回の事態が起きたことは、最新の技術やツールを導入しただけで「即安全だ」とはならないことを示している。また、かつては高度なプログラミングスキルを必要としたマルウェアの作成だが、生成ＡＩを悪用することで、専門的な知識を持たない個人でも容易に攻撃コードを生成できるようになっている。さらにＡＩは、既存のセキュリティソフトの検知をすり抜けるために、マルウェアのコードを微妙に書き換えることも可能にする。

サイバーセキュリティはもはや「ＩＴ部門の技術的課題」ではなく、組織の社会的責任や事業継続に直結する「経営課題」である。それだけに、今求められているのは、技術だけでなく、運用の領域までセキュリティを担保する経営だ。トップは「いつか侵入される」というリスクと向き合い、十分な予算と人材の確保やゼロトラスト化への投資検討、そして有事における事業継続の基本方針を自らの責任で明確に示す必要がある。さらに、技術を活かすための24時間体制の監視運用や、インシデント発生時に迅速に対応できる組織的な体制整備も不可欠である。

最新の脅威トレンドを的確に押さえ、技術の導入にとどまらず組織全体を巻き込んでレジリエンスを高める、強力なトップのリーダーシップこそが現代の組織防衛における最大の要となるだろう。