KLI
Risk Management Journal

2026年
1月

発行日：令和8年1月5日
発行者：兼松ロジスティクスアンドインシュアランス株式会社　保険事業部
電話：03-4214-3951

1．アサヒビールを襲ったサイバー攻撃

2025年9月、アサヒグループホールディングスはランサムウェア「Qilin」による大規模なサイバー攻撃を受け、全国にある工場の出荷や受注システムが停止しました。その結果、ビール類の販売は前年同月比で約2割減少し、お歳暮商戦にも影響を及ぼしました。さらに、191万件以上の個人情報が流出した可能性が公表され、顧客や取引先の信頼を大きく損なう事態となりました。決算発表の延期やサプライチェーン全体への混乱など、経営全体にも甚大な打撃を与え、サイバー攻撃による損害が企業の収益だけでなく社会的信用や事業継続性にも深刻な影響を与えることを示しています。

2．アサヒビールにおけるサイバー攻撃対策

アサヒグループホールディングスは、従来からファイアウォールやウイルス対策ソフト、VPNを用いた外部接続管理などの通常、一般的とされるセキュリティ対策を行っていましたが、2025年9月のランサムウェア「Qilin」の攻撃に対しては、これらの対策だけでは十分に機能することができませんでした。

攻撃者はまず、事前に流出していたIDとパスワードを利用しVPN機器を通じてアサヒビールホールディングのシステムに侵入し、単要素認証しか導入していなかったために容易に突破され、さらに管理者権限を奪って内部システムへ深く侵入しました。バックアップは存在したものの、OSやアプリケーション構成を含む完全なシステムバックアップが不十分であり、復旧に大幅な時間を要しました。また、オンプレミス中心のシステム構造や権限管理の甘さにより、侵入後の被害拡大を防ぐ仕組みが十分ではなかったと考えられます。その結果、基本的な対策は高度化するサイバー攻撃には対応することができず、事業停止や情報漏洩といった深刻な被害へと繋がったと考えられます。

アサヒグループホールディングスにおいては、通常、一般的なセキュリティ対策は行っていましがたが、日々高度化するランサムウェア攻撃を完全には防ぐことはできませんでした。この事実が示すように、現時点で十分と思われる対策を講じていたとしても、「サイバー攻撃の方法は日々、高度化しておりどれだけサイバー対策を講じてたとしてもサイバー攻撃のリスクを完全にゼロにすることはできない」ことを理解することが大切だと考えます。

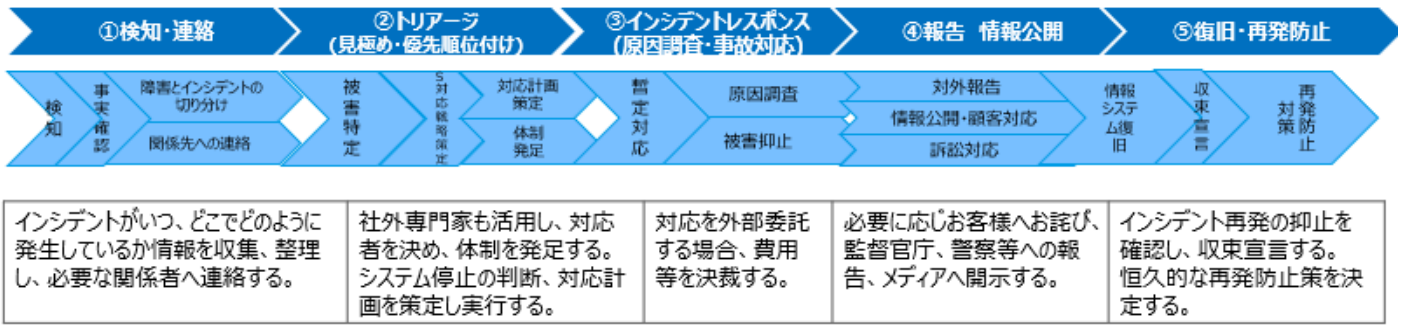
上記をふまえて、自社のサイバーリスク対策を策定する際は、サイバー攻撃を受けることを想定した対策が必要と考えます。次章では、サイバー攻撃時の企業の対応と発生する費用について解説します。

3．サイバー攻撃時の企業の対応と必要なコスト

サイバー攻撃を受けた場合、企業が対応すべきことは図 1 のとおり多岐にわたり、かつ、迅速な対応が求められます。具体的には、原因究明や被害範囲を特定するための専門調査、弁護士や外部コンサルタントへの相談などが必要となります。また、個人情報が漏洩した場合には、監督官庁への報告やコールセンター設置、社会的信用を回復するための広報なども必要となります。

また、これらの対応については、図 2 のとおり、通常のシステムの予算にはない高額な費用を臨時で支出する必要があります。

図1：インシデント発生時の対応



インシデントがいつ、どこでどのように発生しているか情報を収集、整理し、必要な関係者へ連絡する。	社外専門家も活用し、対応者を決め、体制を発足する。システム停止の判断、対応計画を策定し実行する。	対応を外部委託する場合、費用等を決裁する。	必要に応じお客様へお詫び、監督官庁、警察等への報告、メディアへ開示する。	インシデント再発の抑止を確認し、収束宣言する。恒久的な再発防止策を決定する。

図2：インシデント発生時の対応

💰 サイバー攻撃時の費用項目と概算

項目	内容	概算費用
初動対応費用	ネットワーク遮断、証跡保全、CSIRT連絡、フォレンジック業者手配	約 **500～800万円**
調査・フォレンジック費	原因究明、ログ解析、外部専門家レポート提出	数百万円規模
復旧費用	システム再構築、データ復旧、業務再開	約 **900～1,300万円**
通知・コールセンター費	顧客への郵送・メール通知、専用窓口運営	数百万円規模
顧客補償・賠償金	見舞金、損害賠償、クーポン発行など直接補償	数百万円～数千万円
弁護士・PR費用	法的助言、記者会見サポート、風評回復施策	数百万円規模
逸失利益	システム停止や休業による売上減少	数千万円～数億円
罰金・行政対応費	個人情報保護委員会や監督官庁への報告、行政指導対応	数百万円規模
再発防止策費用	ネットワーク再設計、機器入れ替え、従業員教育	約 **300～500万円**

４．サイバーリスク保険の必要性

企業はサイバーインシデントから企業経営を守るため、以下の内容について事前に対策を検討する必要があると考えます。

●サイバーインシデントが発生した際のインシデント対応のための組織、体制の構築。

●サイバーインシデント対応のための専門業者とのネットワークの構築。

●サイバーインシデント発生した際の対応コスト、資金の手当。

サイバーリスク保険は、インシデント対応に要する様々なコストを補償するとともに、保険会社のサイバーインシデント対応のエキスパートが専門業者と連携してインシデントの発生時から事態の収束までのワンストップでサポートする保険です。上記の事前対策について、「対策が十分ではない」または「検討されていない（これから検討する)」場合、サイバーリスク保険の加入をご検討されることをお勧めいたします。

以上、本稿についてご不明のことや、サイバーリスク保険についてお問い合わせがございましたら、お気軽にご連絡くださいますようよろしくお願い申し上げます。