

2026年3月25日

株主の皆様へ

アサヒグループホールディングス株式会社

## 第102回定時株主総会 事前アンケート及びライブ配信でのご意見、ご質問に対するご回答

平素は格別のご高配を賜り、厚く御礼申し上げます。

当社第102回定時株主総会におきまして、事前アンケート及びライブ配信での多数のご意見、ご質問をお寄せいただきありがとうございました。

お寄せいただいたご意見、ご質問のうち、本総会の目的事項に沿った主なご意見、ご質問につきましては、総会当日に、

- ① 議長によるサイバー攻撃に関するご報告、
- ② 指名委員長による取締役選任議案の説明、
- ③ 会場での質疑応答における担当役員からの回答

でご回答しており、これらを含めた株主総会の模様は、[「株主総会事後配信掲載サイト」](#)よりご視聴いただけますので、ご参照いただきますよう、お願い申し上げます。

なお、上記「①議長によるサイバー攻撃に関するご報告」の内容は、以下のとおりとなります。

株主の皆様には、今後とも変わらぬご支援を賜りますよう、お願い申し上げます。

### 1. サイバー攻撃の概要

2025年9月29日、当社システムにおいて障害が発生し、調査を進める中で、暗号化されたファイルがあることを確認したことから、直ちに、被害を最小限にとどめるため、ネットワークを遮断し、データセンターの隔離措置を講じました。

その後の調査の結果、システム障害発生約10日前に、外部の攻撃者がアサヒグループ内の拠点にあるネットワーク機器を経由し、アサヒグループのネットワークに侵入したことが判明いたしました。当社の主要なデータセンターに入り込み、管理者権限を奪取し、そのアカウントを不正利用してネットワーク内部を探索し、複数のサーバーへの侵入と偵察を繰り返したとみられております。

そして、同9月29日、ランサムウェアが一斉に実行され、複数のサーバーやパソコン端末の一部のデータが暗号化されました。また、その後の調査により、従業員に貸与している一部のパソコン端末のデータが流出したことが判明いたしました。

一方、侵入されたデータセンターのサーバー内に保管されていた個人情報については、流出の可能性は否定できないものの、現時点、インターネット上に公開された事実は確認されておりません。

## 2. サイバー攻撃によるシステム障害の被害・対応

サイバー攻撃により、データセンターの複数のサーバー及び一部の従業員用パソコン端末が暗号化されました。また、従業員用パソコン端末の情報の一部が窃取されたことも確認されました。

このサイバー攻撃による被害の拡大を防止するための「封じ込めの対応」として、リモートアクセス VPN<sup>※1</sup>、拠点間ネットワーク、クラウド<sup>※2</sup>間接続の専用通信回線を全て遮断いたしました。さらに、他のシステムへの感染を防止するための緊急措置として、インターネット回線を遮断し、データセンターを完全隔離いたしました。

また、データセンターの全システムを停止させたことにより、業務システムが使用できないこととなりました。

※1 インターネット経由で社外から社内ネットワークへ接続するための技術で、自宅や外出先から社内システムやデータへのアクセスを可能にするもの。

※2 インターネット等を通じて利用する外部のコンピューター資源（サーバーやストレージ）を提供するサービスのこと。

## 3. システム障害の復旧状況

サイバー攻撃被害の拡大防止措置と隔離措置を行ったのち、システムの復旧に向け、複数の外部専門機関の協力も仰ぎ、安全性の高い復旧プロセスを策定し、安全性の確認されたバックアップデータからシステム復旧を行ってまいりました。

復旧のプロセスといたしましては、まず、影響を受けた全てのサーバーについて、健全性を確認するとともに、フォレンジック調査<sup>※</sup>の結果をもとに、必要な追加セキュリティ対策を実施いたしました。

こうして、健全性が保証されたシステムから段階的に再開し、現在、事業活動に必要な主要システムは復旧しております。

※コンピューターやネットワークで起きた不正アクセス・ウイルス感染などの原因や経路を突き止めるための鑑識調査のこと。

## 4. サイバー攻撃による事業への影響と復旧状況

システム障害発生により、お客様への商品供給に直接関係する、受注及び出荷に関するシステムにつきましては、停止を余儀なくされました。

これにより、約2ヶ月強の間、手作業での対応を行ってまいりましたが、従業員及び協力会社の皆様による懸命な復旧作業により、2025年12月上旬より、「電子受発注システム」による受注を再開いたしました。

また、通常よりお時間をいただいております商品配送のリードタイムにつきましても、2026年2月までに通常化したことで、物流業務全体が正常化しております。

本システム障害の影響による商品の販売、売上への影響につきましては、2025年10月から12月までの売上は、前年比で、アサヒビール株式会社が8割台前半、アサヒ飲料株

式会社が7割程度、アサヒグループ食品株式会社が9割程度となりました。

また、依然として、取扱品目数も以前の水準に戻っていないこともあり、2026年2月の状況は、アサヒビール株式会社のビール類売上金額は前年比91%、アサヒ飲料株式会社の販売数量は前年比91%、アサヒグループ食品株式会社の売上金額は前年比90%となっております。

国内事業の状況につきましては、経営の最優先課題として、一日も早い売上の回復に全社一丸となって取り組んでまいります。

## 5. 個人情報漏えいについて

データセンターに不正にアクセスされたことにより、サーバー内に保管されていた個人情報につきましては、これまで漏えいの事実は確認されていないものの、漏えいの可能性が否定できない状況となっております。

漏洩のおそれがある個人情報<sup>※1</sup>は、

国内グループ各社のお客さま相談室にお問い合わせをいただいた方、  
祝電や弔電などの慶弔対応を実施した社外の関係先の方、  
当社グループの従業員及び退職者、並びにその家族の方、  
の氏名、生年月日、性別、住所、電話番号、メールアドレスなど、合計約191万件<sup>※2</sup>の漏えいのおそれがあることが確認されました。

また、従業員に貸与していた一部のパソコン端末への不正アクセスにより、当社グループの従業員及び退職者<sup>※3</sup>の氏名、生年月日、性別、住所、電話番号、メールアドレスなどのほか、お取引先の代表者名などの氏名、電話番号など、合計11万5千513件<sup>※4</sup>の情報の漏えいが確認されております。

これらの個人情報の漏えい及び漏えいの可能性への対応につきましては、個人情報保護委員会に届け出を行うとともに、個人情報保護法に基づき、公表及び対象者へのご通知等、必要な対応を進めておりますが、対象の皆様におかれましては、ご心配とご迷惑をおかけいたしましたことにつきまして、心よりお詫び申し上げます。

個人情報の漏えい及びその可能性に関しましては、多数のご心配の声を頂戴しております。

これまでに個人情報漏えいによる被害は確認されておりませんが、今後とも、誠意をもって対応してまいります。

※1 個人情報の中にクレジットカード情報は含まれておりません。

※2 一件ごとに氏名、生年月日、性別、住所、電話番号、メールアドレスなどの全ての情報が含まれているわけではございません。

※3 当社グループの従業員及び退職者の件数は、漏えいのおそれがある個人情報の数にも含まれております。

※4 一件ごとに氏名、生年月日、性別、住所、電話番号、メールアドレスなどの全ての情報が含まれているわけではございません。

## 6. 今後の対策

当社は、サイバー攻撃のリスクを、「アサヒグループエンタープライズリスクマネジメント」※<sup>1</sup>において、経営上の最重要リスクの一つと位置付け、その対応計画を策定し、実行及びモニタリングを行っております。

この一環として、グループ全体で遵守すべき「グローバルサイバーセキュリティ基準」を制定し、運用の徹底を図るとともに、本基準により国内・海外グループ会社のサイバー攻撃対策状況を評価し、セキュリティ体制の維持・向上を図るとともに、そのリスクが顕在化しないよう、セキュリティの改善などに努めてまいりました。

また、万一、インシデントが発生した際の報告ルールを明確化し、グループ全体でインシデント情報を集約するとともに、リスク対応を強化するなど、体制整備に取り組んでまいりました。

こうした取り組みを行ってまいりましたが、今般のサイバー攻撃を踏まえ、これまでの取り組みをさらに強化し、継続的な監視と改善を前提とした体制へと移行し、万一の事態が発生した場合でも影響を最小限に抑える仕組みの強化を進めてまいります。

また、安全性と信頼性を重視したシステム運用のもと、環境や脅威の変化に応じた継続的な取り組みを行い、再発防止に努めてまいります。

今回のサイバー攻撃を踏まえ、必要な対策に既に取り組んでおり、現段階で安全性は十分に確保されております。今後はさらに、ネットワーク機器をはじめとする、サーバーやパソコン端末などのIT資産の管理徹底、EDR※<sup>2</sup>を含めた、セキュリティツールの最新化・高度化、全従業員への情報管理規程の周知徹底などに努めるほか、ガバナンス体制の強化により、情報管理・セキュリティ管理をより高度化してまいります。

※1 当社は中長期経営方針を遂行する上で、あるいは目標達成を阻害しうる重大リスクを低減しつつリスク総量をコントロールした上で適切なリスクテイクを図るため、エンタープライズリスクマネジメントを導入しております。あわせて「リスクアペタイト」を制定し、「とるべきリスク」と「回避すべきリスク」を明確にしております。

※2 EDR：Endpoint Detection and Response の略。エンドポイント（パソコン端末やサーバー等）で発生する不審な挙動を常時監視し、攻撃の兆候を検知した際に、影響の拡大を防ぐため自動的又は迅速に対処を行う仕組みのこと。

## 7. 国内事業の回復戦略

サイバー攻撃によるシステム障害により国内の酒類、飲料、食品事業は、大きな影響を受けました。

一方で、このような中、お客様からは、多くの励ましのお言葉や応援のお手紙を頂戴いたしました。また、お取引先をはじめとした関係先の皆様には、大変なご不便をおかけしているにも関わらず、商品の供給に関係する通常とは異なる対応にご理解いただき、多大なるご協力とご支援を賜りました。全てのお客様、関係先の皆様に、この場をお借りしまして、深く感謝申し上げます。

このように当社をご支援いただいた皆さまへの感謝の気持ちをお届けするため、2026年2月20日に全社一丸となった、「THANKS ACTION」活動を開始いたしました。本活

動を皮切りに、国内事業各社においては、売上の回復に向けた取り組みを開始しております。

酒類事業においては、2026年10月に予定されている酒税改正でビール類の酒税が一本化されることから、ビールの需要喚起につながるチャンスと捉え、『アサヒスーパードライ』の「冷え」を訴求した取り組みの強化や、麦芽100%の『アサヒゴールド』を発売するなど、当社の強みであるビールに注力することで、売上の回復だけでなく、拡大を目指してまいります。

飲料事業においては、重点ブランドを軸とした事業基盤の拡充に加え、社会課題の解決につながる『未来のBLACK』、『未来のLATTE』や、これまでにない体験価値を提供する『泡 MATCHA』といった、新価値創造商品の展開をさらに強化し、売上の早期回復を図ってまいります。

食品事業においては、和光堂ブランド誕生120周年、「MINTIA」発売30周年といった節目の年を契機としたプロモーション活動により、日本での強固なブランド力を活用した事業成長を目指すとともに、酵母・乳酸菌などの海外における事業成長を両立させ、売上の拡大を図ってまいります。

こうした取り組みにより、お客様、お取引先の信頼を回復し、サイバー攻撃により影響を受けた国内事業の一刻も早い回復に、全社一丸となって取り組んでまいります。

今後は、セキュリティ体制の強化などの再発防止策を速やかに実行し、経営陣一同、信頼の回復とともに、国内事業の一刻も早い回復に向けて全力で取り組んでまいりますので、株主の皆様におかれましては、今後とも何卒ご支援賜りますよう、よろしくお願い申し上げます。

以 上