NEWS RELEASE

2026 年 2 月 18 日
アサヒグループホールディングス株式会社

サイバー攻撃被害の再発防止策とガバナンス体制の強化について

アサヒグループホールディングス株式会社（本社 東京、社長 勝木敦志）は、2025 年 9 月 29 日に発生したサイバー攻撃によるシステム障害の経緯、原因の特定、情報漏えいの可能性について調査を進めてまいりました。2026 年 2 月 18 日時点で調査が完了した内容や範囲およびガバナンス体制の強化を含む再発防止策は以下の通りです。

1. 事案の概要
   - 2025 年 9 月 29 日午前 7 時ごろ、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いたしました。
   - 同午前 11 時ごろ、被害を最小限にとどめるために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、具体的な日時は特定できないものの、システム障害発生の約 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、パスワードの脆弱性をついて管理者権限を奪取した後、奪取したアカウントを不正利用してネットワーク内部を探索し、主に業務時間外に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。
   - 同 9 月 29 日、ランサムウエアが一斉に実行され、ネットワークに接続する範囲で起動中の複数のサーバーや一部のパソコン端末のデータが暗号化されました。
   - 攻撃を受けたシステムを中心に影響する範囲や内容の調査を進めている中で、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。
   - データセンターにあるサーバー内に保管されていた個人情報については、流出の可能性がございますが、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。
   - 今回の攻撃の影響は、日本で管理しているシステムに限られております。

2. サイバー攻撃によるシステム障害の被害・対応

■システムの被害
   - 複数のサーバーおよびゼロトラストモデル※への移行前の一部の従業員用パソコン端末が暗号化されました。
   - ゼロトラストモデルへの移行前のパソコン端末の情報の一部が窃取されたことを確認しております。

※「何も信用しない」を原則とするセキュリティモデルで、社内外を問わず全てのユーザー、デバイス、ネットワーク接続に対して、情報資産へのアクセスごとに厳格な認証と認可を求めるセキュリティのこと。

■封じ込めの対応（被害拡大防止策）
   - リモートアクセス VPN※1・拠点間ネットワーク(約 300 拠点)・クラウド※2間接続の専用通信回線を全て遮断いたしました。

・　さらに、攻撃の横展開（他システムへの感染）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。

※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。

■封じ込め対応によるシステムへの影響

・　データセンターの全システムを停止させたことにより、業務システムへのアクセスが不可となりました。

・　バックアップデータの健全性を保持するため、バックアップシステムを一時停止いたしました。

■フォレンジック調査※

・　外部専門機関によるフォレンジック調査を実施し、システムごとの健全性を検証するとともに、侵害の有無や影響範囲を精査いたしました。

※ 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。

3.　システム障害の復旧状況

■復旧対応

・　複数の外部専門機関と協力し、安全性の高い復旧プロセスを構築いたしました。

・　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いました。

・　影響を受けた全てのサーバーについて再構築後に健全性を確認いたしました。

・　フォレンジック調査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。

・　健全性が保証されたシステムから段階的に再開しております。

■外部との安全なデータ授受および外部システム連携の再開

・　健全性確認済みのシステムから順次、外部システムとのデータ連携を再開いたしました。

・　ウイルス検知・駆除機能を備えたクラウドストレージ経由でのファイル授受を再開いたしました。

・　メール経路を再構築し、健全性を確認したうえで送受信を再開いたしました。

4.　事業への影響と復旧状況

・　お客様への商品供給に直接関係する、受注および出荷に関するシステムにつきましては、システム障害発生以降、停止を余儀なくされ、手作業による対応を続けてまいりました。

・　これらの物流関連のシステムによる受注・出荷業務は、アサヒビール株式会社およびアサヒ飲料株式会社では、EOS（電子受発注システム）による受注を 2025 年 12 月 3 日から、アサヒグループ食品株式会社では同 12 月 2 日から再開しております。
また、制限が残っていた配送のリードタイムについても、2026 年 2 月までに通常化したことで物流業務全体は正常化いたしました。

・　出荷可能な商品の品目数については、順次拡大していく予定でおります。

	アサヒビール 株式会社	アサヒ飲料 株式会社	アサヒグループ食品 株式会社
2025 年 10-12 月 累計売上金額前年比	8 割台前半	7 割程度	9 割程度
2025 年 12 月時点 取り扱い品目数	107 品目 （売上構成比 83%）	350 品目 （売上構成比 95%）	944 品目 （売上構成比 98%）

5.　個人情報の漏えいについて

・ サイバー攻撃発生翌日の 2025 年 9 月 30 日、個人情報保護委員会へ速報を提出いたしました。
・ 同 10 月 8 日、当社から流出した疑いのある情報がインターネット上で確認されたことを個人情報保護委員会へ続報として報告いたしました。
・ 同 11 月 26 日、情報漏えいのおそれがあるとして、個人情報保護委員会に確報として報告いたしました。
・ 同 12 月 10 日、新たに当社から流出した疑いのある情報がインターネット上で確認されたことを個人情報保護委員会へ追加報告いたしました。
・ 情報漏えいが確認された方および情報漏えいのおそれがある方には、順次お知らせしております。

■漏えいのおそれがある個人情報（2025 年 11 月 26 日時点）

対象者	内容	件数
アサヒビール株式会社、アサヒ飲料株式会社およびアサヒグループ食品株式会社各社のお客様相談室にお問い合わせをいただいた方	氏名、性別、住所、電話番号、メールアドレス	152.5 万件
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	氏名、住所、電話番号	11.4 万件
従業員（退職者を含む）	氏名、生年月日、性別、住所、電話番号、メールアドレスなど	10.7 万件
従業員（退職者を含む）の家族	氏名、生年月日、性別	16.8 万件

（注）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「内容」に記載の全ての情報が含まれているわけではございません。

■漏えいが確認された個人情報（2026 年 2 月 18 日時点）

対象者	内容	件数
従業員（退職者を含む）	氏名、性別、住所、電話番号、メールアドレスなど	5,117 件
取引先の役員および従業員の方、並びに取引先個人事業主およびその従業員の方など	氏名、電話番号など	110,396 件

（注）1．「従業員（退職者を含む）」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。
2．一件ごとに「内容」に記載の全ての情報が含まれているわけではございません。

6.　再発防止策とガバナンス体制の強化

当社はサイバー攻撃のリスクについて、「アサヒグループエンタープライズリスクマネジメント」※1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、実行およ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「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、当該基準により国内・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・向上および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、当該基準において、インシデント発生時の報告ルールを明示し、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の体制整備に取り組んでまいりました。

今後は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。

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。主な対策として、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（エンドポイント検知・対応）※2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、さらには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。

具体的な取り組みの概要は次のとおりです。

※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 とは 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または迅速に対処を行う仕組みのこと。

■攻撃経路の特定と再発防止

- ネットワーク機器からの再侵入を防ぐためのリモートアクセス VPN 装置の全面廃止
- 不正アクセスされる可能性がある古い通信経路を排除するための通信経路の再構築
- 攻撃経路の特定によって明らかとなった、外部侵入リスクを抱えるデバイスの全面廃止
- パソコン端末からのデータ窃取リスク低減に向けたクラウド保管への一本化およびクラウド保管データ利用時のキャッシュ非残存対策の実施

■パソコン端末・ネットワーク・システム構成の再設計

- 攻撃された場合の他のパソコン端末への拡大を防止するための、より安全な仕組みに対応した専用のパソコン端末（ゼロトラストモデル対応のパソコン端末）への完全移行
- 不要な通信を遮断し外部との接続を分離するための、安全なネットワークエリアの新設
- 攻撃の拡大を防止するための、全システムでのネットワークの分離・接続の制限
- パソコン端末での不審な動きを検知・遮断するための、全パソコン端末の EDR の設定強化
- インターネット接続を行うクラウド環境での EDR による監視強化
- 安全性を客観的に確認するためのペネトレーションテスト（第三者によるインターネットからの侵入を試行するテスト）の実施
- 安全性の維持・向上を図るため、ペネトレーションテストおよびスレットハンティング（脅威調査）を継続的に実施

■監視・検知・初動対応の高度化

- セキュリティルールと運用体制の見直しによる、異常を検知した際の初動の迅速化
- サイバー攻撃や異常を素早く検知・対処し、被害を最小化するための、ログ分析システムやセキュリティの監視・遮断の自動化

■権限管理・アカウントセキュリティの強化

- 全システムにおけるパスワード変更および認証・権限管理の強化
- 人的作業ミスや削除漏れを防ぐためのアカウント作成・変更・削除の自動化

■インフラおよびクラウド環境のセキュリティ強化
・　ネットワークの接続制限の更なる強化、攻撃の広がりを防止するインフラ構成への改善
・　クラウドのセキュリティ状況の継続的チェック・問題是正の自動化

■復旧性・耐障害性の強化
・　システム復元の更なる迅速化の実現に向けた、バックアップの仕組みの更なる強化
・　迅速な復旧に向けた、復旧手順の定期的な見直し・訓練の実施
・　システム・データの整理・統合による、システム構成のスリム化

■人的対策の継続的強化
・　従業員向けセキュリティ教育の強化・継続
・　最新の攻撃手法に備えた実践的なセキュリティ訓練の継続

■ガバナンス体制の強化
・　情報セキュリティを管轄する独立した組織および専任の担当役員の設置
・　情報セキュリティ委員会を設置し、情報セキュリティリスクを可視化するとともに、対応策の計画・実行が行われていることをモニタリング
・　「情報管理・情報セキュリティ規程」の改定および遵守・徹底の監視・監査の強化
・　「取締役会スキルマトリックス」の見直し、および取締役会と情報セキュリティ委員会、内部監査機能、外部専門家などとの連携による、取締役会によるサイバーセキュリティに関する監視・監督機能の強化

【関連リリース】
2025 年 9 月 29 日「サイバー攻撃によるシステム障害発生について」
2025 年 10 月 3 日「サイバー攻撃によるシステム障害発生について（第 2 報）」
2025 年 10 月 8 日「サイバー攻撃によるシステム障害発生について（第 3 報）」
2025 年 10 月 14 日「サイバー攻撃によるシステム障害発生について（第 4 報）」
2025 年 11 月 27 日「サイバー攻撃による情報漏えいに関する調査結果と今後の対応について」

<本件に関するお問い合わせ先>
アサヒグループホールディングス株式会社　コーポレート・コミュニケーション部門　電話:03-5608-5126