2025 年 10 月 22 日

アクリーティブ株式会社
代表取締役社長 菅原 猛

当社ネットワークへの不正アクセスによるシステム障害について（調査結果のご報告）

このたびの当社ネットワークへの不正アクセスによるシステム障害について、2025 年 8 月 25 日および同月 29 日付でお知らせいたしましたが、その後の外部専門会社による調査結果等について下記のとおりご報告いたします。

お取引様、関係先の皆様には、多大なるご心配とご迷惑おかけいたしましたことを、深くお詫び申し上げます。

記

1. 概要

2025 年 8 月 25 日に当社のサーバに対する第三者による不正アクセスがあり、当社サーバの一部が暗号化され閲覧不能な状態となりました。既報にてご案内の通り、不正アクセスが確認されたサーバは、発覚後ただちに外部からのアクセスを遮断する措置を講じております。

その後、当社にて対策本部を設置のうえ、専門家の助言の下で、被害状況の把握、原因究明と復旧・再発防止対策の実施等を進めてまいりました。

2. 調査結果

(1)フォレンジック調査

2025 年 8 月 25 日から同年 9 月 12 日にかけて、外部のセキュリティ専門会社によるフォレンジック調査を実施いたしました。当該調査では、データセンター内のサーバやファイアウォールなどの個別機器内に保存されているドキュメント、およびネットワーク上の流通経路において、ファイルデータが外部に持ち出された形跡が無いかの調査を実施いたしました。

2025 年 9 月 29 日にセキュリティ専門会社より最終報告を受領した結果、外部へのデータ流出の痕跡は確認されませんでした。

また、調査の過程で不審なアクセスが確認された機器等につきましては、速やかに交換作業を実施しております。

(2)ダークウェブ監視

2025年9月5日より、ダークウェブ上（一般的な方法ではアクセスが困難なインターネット領域）での情報流出有無の監視を行っております。（不正アクセスの発生日に遡り、情報流出の有無を調査しております）引き続き監視を継続したうえで、専門機関から結果の報告を受ける予定です。

現時点でダークウェブ上でのデータ流出は確認されておりませんが、万が一、ダークウェブの監視期間中、流出が確認された場合、改めてご報告をさせていただきます。

３．本件の原因

2025年8月24日に実施した当社ネットワークにおけるファイアウォールの入替作業において、システムベンダーの事前の設定ミスにより、ファイアウォールの一部の機能が停止した状態のまま機器が設置された結果、外部からのサイバー攻撃が行われ、サーバへの不正アクセスが発生したものと考えられます。

４．再発防止策

本件の原因がネットワーク機器の入替時に発生した設定ミスに起因していると考えられることから、再発防止策として、以下を実施いたします。

・システムベンダーに対し、セキュリティ体制の抜本的強化と再発防止策の策定を要請し、その内容を定期的に評価・確認を実施。
・セキュリティリスクを伴う作業を行う際は、当社による作業確認に加えて第三者検証機関による検証を実施。

改めまして、この度はご迷惑とご心配をおかけし、深くお詫び申し上げますとともに、今後とも変わらぬご愛顧を賜りますようよろしくお願い申し上げます。

以上

【本件に関する問い合わせ先】
アクリーティブ株式会社　社長室
連絡先　03-6261-4920
E-mail：acr_pr@accretive.jp