FSH-57C-1128
2025 年 12 月 12 日
ウエットマスター株式会社

弊社へのランサムウェア攻撃の対応経過および今後の見通しについてのご報告

弊社では本年８月末にランサムウェアによる攻撃を受けてシステム障害が発生し、お客様、お取引先および関係者の皆様には多大なるご迷惑とご心配をおかけしておりますこと、深くお詫び申し上げます。

本書により、経緯および主な経過、現時点で判明している情報流出の可能性、システム復旧に向けた今後の見通しについてご報告申し上げます。

記

1. 経緯および主な経過

2025 年 8 月 25 日	弊社社内業務システムの不調が発生し、調査したところランサムウェアによる攻撃を受けたことが判明いたしました。感染拡大を防止するため、直ちにネットワークの遮断を実施いたしました。また、個人情報保護委員会、所轄警察署に対して感染の報告を行うとともに、外部専門会社との調査を開始いたしました。
同 8 月 29 日	弊社ホームページ上にて「ランサムウェア攻撃に関するご報告と対応措置」を公表いたしました。
同 9 月 19 日	続報として弊社ホームページ上に「弊社業務状況に関しまして」を掲載し、仮復旧に向けた取り組みにより、通常業務の継続をご報告いたしました。
同 10 月 2 日	外部専門会社より、サイバー攻撃の侵入経路の報告を受け、海外からクラウドサーバーにリモートデスクトップで接続され、侵入したことが判明いたしました。
同 10 月 15 日	基幹業務システムの仮運用を再開いたしました。
同 11 月 25 日	外部専門会社より、ダークウェブ上に流出した認証情報・重要情報があるかないかについて報告を受けました。
同 12 月 12 日	対応経過および復旧状況、今後の見通しについてのご報告を実施いたしました。

2. 情報流出について

・外部専門会社の調査（フォレンジック調査）により、社内サーバーおよび一部 PC に保管されていた社内外文書（データ）の一部が、社外に流出した可能性があることが確認されました。流出した可能性のある情報には、製品・部品のお送り先等、一部現場名・納入情報（住所・ご担当者名）が含まれます。

・お取引情報で流出の可能性がある件数は、約 9 千件を数えました。

・11 月 30 日時点で、本件に起因すると思われる流出情報、漏洩情報の不正利用等、二次被害についての報告は受けておりません。

・ダークウェブ上に流出した認証情報・重要情報があるかないかについて、当社では把握できないため、専門会社による調査を行いましたが、11 月 25 日時点で流出は確認されておりません。なお、今後も専門会社による調査を継続してまいります。

3. システム復旧の対応および対策について

・サーバーについては、全台の初期化・バックアップからの復元作業を実施しております。

・PC については、全台の初期化・OS の再インストールを実施しております。

・社内ネットワークについては、再構築のうえ、復旧が完了したサーバー・PC から順次復帰させています。

・今後のセキュリティ強化対策として、マルウェア対策の強化を図り、全社員を対象としたセキュリティ教育の強化と検証を実施し、機器の脆弱性強化と管理体制の見直しに取り組んでおります。

4. 今後の見通し

・現時点において、本件の影響による事業計画・業績見込みの修正はございません。今後の調査継続により開示すべき事項が明らかになりましたら、速やかに公表いたします。

・業務管理システムの復旧は徐々に進んでおり、2026 年 1 月以降順次、攻撃前の状況に復旧の予定です。

・お客様、お取引先および関係者の皆様には多大なるご迷惑とご心配をおかけしておりますこと、あらためて深くお詫び申し上げます。

・本件に関しまして、多大なご配慮を賜りましたことに深く感謝申し上げます。

以　上