2021 年 10 月 29 日

各　位

株式会社 ムトウ
管理本部

当社サーバーへの不正アクセスについて

2021 年 8 月 31 日に発生いたしました当社サーバーへの不正アクセスにつきまして、外部の公的機関、及びセキュリティエンジニア企業等のご協力の下、本件への対応を進めてまいりましたので、その調査結果と今後の対策等についてご報告致します。

1. 経緯について

2021 年 8 月 31 日、早朝より外部から当社のシステムに不正なアクセスが行われていることを検知致しました。そこで、直ちに影響を受けたサーバーを洗い出し、稼働停止作業、ネットワークの遮断を行い、その後、安全確認を行った上で、復旧作業を進めてまいりました。また、同時に外部の専門家を含む対策チームを立ち上げ、原因究明や影響範囲の絞り込み、不正アクセスに関する様々な情報収集とその精査などを行ってまいりました。

2. 対応について

外部の公的機関やセキュリティエンジニア企業にもご協力いただき、次の作業を行いました。

・ＦW(ファイヤーウォール)のログ取得
・被害があったサーバーの抜線及び保全
・ＶＰＮのバージョンアップ及びパスワード変更
・ＶＰＮの利用制限
・サーバー/パソコンの正常性確認(ウィルススキャン)及びパスワード変更

3. 調査内容について

当社サーバーのログ内容を確認しましたところ、以下の事実が判明いたしました。

・不正なアクセスはＶＰＮ装置から行われた可能性が高い。
・複数台の Windows サーバーでランサムウエアが実行され暗号化された。

その後の確認・調査作業では、お客様の情報（個人情報を含む）の流出は確認されておりません。

4. 今後の対策について

今回発生しましたインシデントを踏まえ、外部の公的機関や専門家の意見も取り入れ、対策チームを中心に再発の防止に向けて、システムセキュリティ面の見直しはもちろんのこと、全社員へのシステム関連教育の強化などの取り組みを進めております。

改めまして、本件につき、お客様・お取引先様に対し、多大なるご迷惑及びご心配をおかけしている事を深くお詫び申し上げます。

以 上