弊社システムへの不正アクセスについて（第三報）

2024 年 5 月 16 日
TMT マシナリー株式会社

2024 年 3 月 18 日に発生した不正アクセス被害については、3 月 26 日付けの第一報、4 月 9 日付けの第二報でお知らせしてきたところですが、今後の復旧及び調査の見通しおよび新たに判明した事項につきまして、下記の通りお知らせいたします。

お客様をはじめ、関係者の皆様にご迷惑およびご心配をおかけする事態となっておりますこと、深くお詫び申し上げます。

記

1.　概要

2024 年 3 月 18 日に、当社は、外部の第三者からランサムウェアを使用した攻撃を受け、当社の業務用システム上の個人情報を含むデータが暗号化されました。なお、その際、個人情報を含む一部のデータが窃取された可能性がありますが、後記の調査の結果、これに伴う二次被害のおそれは確認されておりません。

また、当社から窃取されたと思われるデータの一部のキャプチャ画像が、ダークウェブ（一般的なウェブブラウザを用いた通常の方法ではアクセスできず、専用のツールと技術を用いることでアクセスできるインターネット上の領域）に掲載されたことを確認しておりますが、この中に個人情報は含まれておりません。当該キャプチャ画像以外のデータの公開はされておらず、また、ダウンロード等もできない状況であることを確認しております。

なお、第三者からは、身代金の支払いを要求するメッセージを受領しておりますが、当社は、これに応じておりません。

2.　対応状況

当社は、不正アクセスを認識した後、システムの保守運用を委託しているベンダーと連携し、業務の復旧及び調査を開始するとともに、大阪府警察及び個人情報保護委員会に報告及び相談を行いました。その後、専門の分析調査会社に依頼して専門的な調査を開始するとともに、情報セキュリティを専門とする弁護士の助言の下、復旧及び調査を進めてまいりました。

この度、分析調査会社から調査結果を受領したことから、当社内部における調査結果と合わせて検討した上、再発防止策を策定いたしました。

3.　調査結果

(1)　原因

第三者は、何らかの方法で当社のネットワークに侵入し、ランサムウェア（システム及びデータを暗号化し、使用できないようにするマルウェア）を実行したものと考えられますが、侵入経路については、フォレンジック調査によっても判明しませんでした。

(2)　漏えい等の可能性がある個人情報

漏えい等の可能性がある個人情報は、以下のとおりです。対象となるお客様には、可能な限り個別にご連絡させていただいております。

お客様ならびに取引先様にかかる情報（担当者氏名、電話番号、メールアドレス、会社名、部署名など）

従業員・派遣社員・退職者・採用応募者にかかる情報（氏名、生年月日、住所、電話番号、メールアドレス、学歴、職歴など）

なお、本項に関するご質問がありましたら「５．お問い合わせ先」までご連絡お願いいたします。

4.　今後の見通し及び再発防止策について

現在、システムの保守運用を委託しているベンダーと連携し、業務システムを再構築しております。業務システムの完全復旧には時間を要する見込みですが、それまでの間につきましては、手元情報をもとに手作業にて対応を行い、業務への影響が最小限に留まるよう努めて参ります。なお、今後、納期等に影響が出るおそれがあるお取引先様には、事前に、個別のご説明をさせていただきます。

復旧にあたっては、当社は、PC を全台入れ替え、ネットワークを新規に構築し、新たなウイルス対策を実施するなど、十分なセキュリティ措置を取っております。また、今後、従業員に対する教育・訓練、内部監査の強化等を含め、弊社全体としてセキュリティ水準を高められるよう、一丸となって努力してまいります。

5.　お問い合わせ先

本件に関するお問い合わせは、営業担当者又は以下の連絡先までお願いいたします。

連絡先

https://www.tmt-mc.jp/contactus/

お客様をはじめ、関係者の皆様にご迷惑およびご心配をおかけする事態となりましたこと、改めて深くお詫び申し上げます。

以上