2023 年 11 月 28 日
マツダ株式会社

不正アクセス発生による個人情報流出可能性について（第 2 報）

2023 年 9 月 15 日付「不正アクセス発生による個人情報流出可能性のお知らせとお詫び」（以下、「第 1 報」といいます。）にて公表した弊社サーバーへの不正アクセス（以下、「本件事象」といいます。）について、今般、第三者機関（以下、「外部セキュリティ専門家」といいます。）による本件事象に関する調査が完了しましたので、その概要及び今後の取り組みについてご報告いたします。

なお、第 1 報でお知らせしたとおり、不正アクセスを受けたサーバーにはお客様の個人情報は保管しておらず流出しておりません。当該サーバーにおいては、弊社及びグループ会社の社員、協力会社社員、お取引先様ご担当者のアカウント情報等を保管しており、一部が外部へ流出した可能性があることが判明しています。

また、現時点では確認されていませんが、今後、これらの個人情報を悪用し、フィッシングメールやスパムメール等が送付される可能性があります。不審なメールを受け取られた場合は慎重にご対応下さいます様よろしくお願いいたします。

関係者の皆様には多大なるご迷惑とご心配をおかけしましたこと、重ねて深くお詫び申し上げます。

【調査結果と対応】

弊社のサーバー及びネットワーク装置について、外部セキュリティ専門家による調査を実施しました。その結果、弊社ネットワークに設置されていたサーバーの脆弱性が悪用され、これが弊社内への不正アクセスの経路となり、アカウント情報（弊社などの社員のユーザーID、パスワード等）を管理するサーバー（以下、「アカウント管理サーバー」といいます。）に対して、第三者による不正操作が行われたことを確認しました。

そこで、本件事象を確認後、アカウント管理サーバーへの不正アクセスの経路となったサーバーを停止いたしました。

また、これらのサーバーの調査を進めた結果、アカウント管理サーバー及び不正アクセスの経路となったサーバー以外への不正アクセスは確認されませんでしたが、アカウント管理サーバーに不正操作の履歴が確認されていたことから、被害拡大を防ぐために、全てのユーザーID のパスワード変更を行うとともに、不正操作の履歴があったアカウント管理サーバーの監視強化を実施するなど、さらなる被害を防ぐための措置を講じました。その後、不正アクセスは確認されていません。

【今後の対応】

弊社では、今回の事象を重大な経営課題と捉え、再発防止に取り組んでまいります。

具体的には、脆弱性を悪用した不正アクセス対策として、外部から不正なアクセスを受けた場合の検知能力を高めるために、ASM（Attack Surface Management）（※1）を導入し、インシデント対応プ

ロセスの改善を図ります。また、OS やソフトウェアのバージョン情報を管理するプロセスを強化することで、これらを最新の状態に保ち、継続的に脆弱性を解消することに努めます。

更に、多要素認証(※2)の実装を加速するとともに、ユーザーID を悪用したネットワーク内部不正アクセスや不正行為を検知し、迅速に対応するためのシステムを導入してまいります。

これらの対策を継続的に実施することで、安心してご利用いただける弊社システムサービスへ改善してまいります。

この度は皆様に多大なご迷惑ご心配をお掛けしましたこと、改めて深くお詫び申し上げます。

＜本件に関わるお問い合わせ先＞

本件に関するお問い合わせは、下記にて承ります。

お問合せフォーム：https://mag.mazda.jp/enq/pub/common/svaccinq

以　上

※1)組織の外部（インターネット）からアクセス可能な IT 資産を発見し、これらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスをいいます。

引用：経済産業省　商務情報政策局　サイバーセキュリティ―課
「ASM（Attack Surface Management）導入ガイダンス　外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する」（2023 年 5 月 29 日）
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

※2）サービスやアプリケーションにログインする時、パスワードや電話番号など、複数の種類の情報を使って本人認証を行う方法をいいます。