2025 年 9 月 26 日

藤倉コンポジット株式会社

当社メールサーバーへの不正アクセスについて

このたび、当社が管理するメールサーバー（Microsoft Exchange Online）を利用するメールアカウントに対し、第三者による不正アクセスが確認されました。この不正アクセスにより、情報が漏えいした可能性があります。

漏えいの可能性がある情報は以下のとおりです。

・過去 5 年間に送受信されたメールの From、To、Cc に記載されたメールアドレス
・過去 5 年間に送受信されたメール本文および添付ファイル
※添付ファイルには個人情報が含まれているものもありました。

関係者の皆様には多大なるご迷惑とご心配をおかけすることとなり、深くお詫び申し上げます。本件につきましては、すでに個人情報保護委員会へ必要な報告を行っており、外部のセキュリティ専門会社の協力を得ながら、事実確認および必要な対応を進めております。

現在も調査および対応を継続しておりますが、一定の進捗が得られましたので、現時点で判明している事実および当社の対応について、以下のとおりご報告いたします。

1. 本件の概要

2025 年 8 月 25 日 15 時頃、当社ベトナム子会社の従業員より、同子会社に出向中の当社社員のメールアドレスから不審なメールが送信されてきたとの第一報がありました。

現地 IT 担当者が確認したところ、以下の特徴があるフィッシングメールであることが判明しました。

・差出人（From）と送信先（To）の名前が同一
・日本語の文章が不自然
・添付ファイルに見せかけた不審なリンクが含まれている

同子会社の IT 担当者は、当社システム部門に連絡し、システム部門からは、発信元と思われる PC および送信先の PC に対してウイルス対策ソフトによるフルスキャンを指示しました。

その後、当社システム部門がメール送信記録を確認した結果、約 300 件の不審なメールの送信記録が確認されました。この記録は、発信元のメールアカウントの「送信済み」情報には記録がなく、アカウントの利用者からは確認ができなくなっていました。

ウイルスチェックの結果、PC に問題は見られなかったため、原因は PC ではなくメールサーバーへの不正アクセスであると判断し、現地 IT 担当者に対して該当メールアドレスのパスワード変更を依頼しました。

翌日（8 月 26 日）、メールサーバー等へのサインインログを確認したところ、利用者が在席しないはずの米国の IP アドレスから該当のメールアドレスへのサインインが行われていたことが判明しました。これを不正アクセスと判断し、追跡した結果、パスワード変更後はアクセスが失敗し、2025 年 9 月 26 日現在まで新たなアクセスは発生しておりません。

2. 原因と対策

原因は、メールアカウント（Microsoft アカウント）のパスワード漏えいによるものと推定されますが、明確な漏えいの原因は特定されていません。

対応として、以下の対策を実施しました。

・他のアカウントでもパスワード漏えいの可能性を考慮し、当社メールシステム利用者全員にパスワード変更を指示
・ベトナム子会社においては、当社のメールシステム利用者に対して二段階認証を導入

2025 年 9 月 26 日

藤倉コンポジット株式会社

・不正アクセス検知のため、定期的なサインインログの監査

3. 漏えいの可能性がある個人情報

不正アクセスが確認されたのは、ベトナム子会社に出向中の当社社員 1 名のメールアカウントのみです。

メールサーバー内に添付ファイルとして保存されていた従業員 64 名分の個人情報には、氏名、生年月日、住所、電話番号、世帯主情報が含まれていました。なお、マイナンバー、銀行口座、クレジットカード番号等は含まれておりません。

取引先情報については、過去のメール送受信に使用されたメールアドレスの一部が不審なメールの宛先に使用されていたことから、Exchange Online に保管されているすべてのメール内に記載されたメールアドレスが漏えいした可能性があります。

これらのメールは、2020 年に Exchange Online へ移行して以降、継続的に保管されているものであり、それ以前のメールは PC にバックアップとして保存されているため、今回の対象外となります。

4. 今後の対応

現在、Microsoft 365 のシステムにおいて SOC（Security Operation Center）サービスもしくは監視システムを調査中です。今回の不正アクセスの対象は、ベトナムからでも利用できる Exchange Online だけでしたが、同一のアカウントとパスワードを使用する、M365 ファミリー（Teams、Share Point 等）においても、同様な危険性が存在するため、早急な SOC サービスもしくは監視システムの導入を行います。

また、メールへの添付による情報交換を全社的に見直し、クラウドストレージの利用も視野にコミュニケーションツールの活用について再検討を行います。

５. 二次被害又はそのおそれの有無及びその内容

現時点で、当社から流出したデータがインターネット上で公開されたなどの事実は確認されておらず、その不正利用などの二次被害も確認されておりません。もし、不審なメールを受け取られたなど、本件による被害が疑われる事例がございましたら、下記問い合わせ先までご連絡をいただきたくよろしくお願いいたします。

６. 当社生産活動への影響等

本件による当社生産活動への影響はございません。また、現時点において、流出が問題となるような業務上の秘密の流出も確認されておりません。当社では、今回の事態を真摯に受け止め、委託先との協働体制の強化を含め、情報セキュリティの一層の強化及び再発防止に全力で取り組んでまいります。

＜本件に関するお問い合わせ先＞

personal_info@fc.fujikura.co.jp