

IIJセキュアMXサービスにおけるお客様情報の漏えいについての お詫びとご報告

当社が法人向けに提供するメールセキュリティサービス「IIJ セキュア MX サービス」への不正アクセス事案について4月15日に公表いたしました(以下、第一報 ※)、その後の調査の結果についてお知らせいたします。

(※)2025年4月15日付報道発表資料「IIJセキュアMXサービスにおけるお客様情報の漏えいについて」
<https://www.ij.ad.jp/news/pressrelease/2025/0415.html>

お客様、および関係者の皆さまには多大なご迷惑をおかけしており誠に申し訳ございません。あらためて深くお詫び申し上げます。

■漏えい事実が確認されたお客様契約数

第一報で、情報が漏えいした可能性があるとお知らせしたIIJセキュアMXサービスの全ての契約のうち、情報が漏えいした事実が確認されたお客様契約数は以下の通りです。

当該サービスで作成された電子メールのアカウント・パスワードの漏えい

対象のお客様契約数：132 契約

※このうちの一部のお客様契約については電子メールアカウントのみ漏えい事実が確認されています。

※第一報で漏えいの可能性があるとした電子メールアカウント4,072,650件のうち、311,288件が該当します。

当該サービスを利用して送受信された電子メールの本文・ヘッダ情報の漏えい

対象のお客様契約数：6 契約

当該サービスと連携して動作するように設定されていた他社クラウドサービスの認証情報の漏えい

対象のお客様契約数：488 契約

なお、以上3項目の合計契約数から、重複するお客様を除外した契約数は586契約です。

■対象のお客様へのご案内について

現在当社とのご契約があるお客様には、当社担当者よりご案内しています。また、当該サービスの運用管理担当者の方は、「IIJ サービスオンライン」よりご案内を確認いただけます。

現在当社とのご契約がなく、過去に当該サービスをご利用されていたお客様におかれましては、ご不明な点がございましたら、以下のご相談フォームでご連絡をいただきますようお願いいたします。

ご相談フォーム

ご不明な点がございましたら、こちらのご相談フォームでお問い合わせください。

セキュリティ事故専用お客様フォーム

<https://biz.ij.jp/public/application/add/39186>

■不正アクセスの原因

本件の不正アクセスの原因は、IIJ セキュア MX サービスで利用していた第三者製のソフトウェアの脆弱性を悪用されたことによるものでした。この脆弱性は不正アクセス発生から発覚のタイミングでは未発見のものであり、今回の事案を通じて初めて明らかになったものです。その後、ソフトウェア製造元による改修が完了し、4月18日にJVN(※)において緊急度の高い脆弱性として情報が公開されております。

対象となった脆弱性

JVN#22348866:"Active! mail におけるスタックベースのバッファオーバーフローの脆弱性 緊急"

<https://jvn.jp/jp/JVN22348866/index.html>

(※)JVN(Japan Vulnerability Notes):日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト。脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基づいて、2004年7月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同で運営しています。

なお、IIJ セキュア MX サービスにおいて、当該ソフトウェアによるオプション機能は2025年2月をもって提供終了しており、現在、当該ソフトウェアは利用しておりません。

■今後の対応

現在、再発防止に向けて、セキュリティ対策および監視体制の強化について検討を進めております。また引き続き、関係機関と連携して対応を行っております。新たにお知らせすべき内容が判明した際は、速やかに情報を開示してまいります。

以上

報道関係お問い合わせ先

株式会社インターネットイニシアティブ 広報部

TEL : 03-5205-6310 FAX : 03-5205-6377

E-mail : press@ij.ad.jp URL: <https://www.ij.ad.jp/>

※本プレスリリースに記載されている社名、サービス名などは、各社の商標あるいは登録商標です。