

令和5年6月に発覚した個人情報の漏洩の恐れに関する事案の
経緯及び講じた対策の詳細についてご報告（最終報）

2024年8月7日

令和5年6月に発生しました当研究所のスパムファイアウォールに対する不正アクセスについて、以下のとおり当研究所ホームページで掲載してまいりました。まず、令和5年7月にはインシデント発生速報を行い、令和6年6月には約1年間の調査を踏まえ、メールアドレス等の個人情報が漏えいした可能性を排除できない方に対して個別にメールで通知させていただいた旨、注意喚起をさせていただきました。

不正アクセス発生時より有識者及び関係機関の指導の下、委託業者が調査を行った結果、不正アクセスは当該機器の脆弱性を原因とするゼロデイ攻撃※¹によるものであり、当研究所が令和5年5月から令和5年6月までの間にインターネット経由で受信した個人情報を含むメールアドレスの一部が外部に漏えいした可能性があることが判明いたしました。

不正アクセス発見後、被害を特定するため個人情報漏洩の可能性のあるデータを含むすべてのデータを対象に被害内容の解析作業を実施し、その結果から漏洩の恐れのあるメールアドレス等の特定作業を進めました。併せて、システムの脆弱性対策については、セキュリティを強化したスパムファイアウォールへの設備更新を実施いたしました。

インシデントの発見、調査、漏洩の恐れのある情報特定・通知及びセキュリティ対策が全て完了しましたので最終報告をさせていただきます。

スパムファイアウォールの脆弱性の把握から現時点までの詳細な経緯及び当研究所が講じてきた措置は以下のとおりです。

- ・令和5年6月8日 スпамファイアウォール（当時）のファームウェアバージョンに脆弱性があると判明したため、通信ログ調査を開始
- ・令和5年6月13日 通信ログ調査を実施した結果、不正通信ログを確認したため、スパムファイアウォールに保存されている不正通信データの解析、外部に流出した可能性のあるメールアドレスすべての抽出作業を開始
- ・令和5年6月16日 個人情報保護法第68条第1項に基づき、個人情報保護委員会へ個人情報漏洩の恐れがあることを報告
- ・令和5年6月28日 スпамファイアウォールの代替機器への交換を実施
- ・令和5年7月3日 個人情報保護法第68条第2項に基づき、土研HPにて不正アクセスが発生したことを報告（第一報：速報）するとともに警察へ報告

- ・令和5年12月20日 外部に流出した可能性のあるメールデータすべての抽出が完了し、個人情報が含まれるメールの特定作業を開始
- ・令和6年3月25日 スпамファイアウォールの設備更新を実施
- ・令和6年5月15日 有識者等の指導の下、個人情報が含まれるメールアドレスを特定
- ・令和6年6月3日 個人情報保護法第68条第2項に基づき、漏洩の恐れについて、特定したメールアドレスに対してメールを配信。また情報提供として、当研究所HPに掲載（第二報：注意喚起）
- ・令和6年8月7日 HP掲載の第2報までを含め、詳細な経緯及び講じた措置を取りまとめたので当研究所HPに掲載（第三報：最終報告）

現時点で、個人情報の悪用等の被害は確認されておりませんが、今後当研究所を装った不審なメールが送付される等の可能性は否定できませんので、ご注意※²ください。

本事案を踏まえ、関係機関等とも連携し、より迅速に対処していくため体制強化を進めて参ります。

関係者の皆様には、ご迷惑をおかけすることになり、重ねてお詫び申し上げます。

（問合せ先）

国立研究開発法人 土木研究所 情報セキュリティ委員会事務局（企画部 業務課）

電話：029-879-6754（平日 9:30～17:00）

メールアドレス：pwri-security (a)pwri.go.jp

※お問合せの際は、(a)を@に変換して送信してください

※1：ゼロデイ攻撃とは、システムの脆弱性に対して、修正が行われる前にそれを悪用するサイバー攻撃を指します。

※2：【参考情報】不信メールの注意点

独立行政法人情報処理推進機構（IPA）

「メールの見かけ上の送信元情報を安易に信じないで」

<https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210921.html>