

[ホーム](#) > [サステナビリティ](#) > [ガバナンス](#) > [情報セキュリティ](#) > [プロダクトセキュリティ](#) > [脆弱性ごとの情報リスト](#) > 脆弱性情報

「リコー製Web Image Monitorを実装している複数のレーザープリンタおよび複合機（MFP）におけるオープンリダイレクトの脆弱性」によるリコー製品への影響について

公開日時: 2026年04月30日 3時00分 (2026-04-30T12:00:00+09:00)
株式会社リコー

日頃は弊社製品をご愛用いただきまして、誠にありがとうございます。
当社が開発、製造し、日本国内で販売する製品・サービスに対し、「リコー製Web Image Monitorを実装

脆弱性情報ID	: ricoh-2026-000004
バージョン	: 1.00J
CVE ID(CWE ID)	: CVE-2026-41226 (CVE-601)
JVN登録番号	: JVN#65118274
CVSSv3スコア (基本値)	: 4.7 MEDIUM

している複数のレーザープリンタおよび複合機（MFP）におけるオープンリダイレクトの脆弱性」による影響が確認されました。

より強固なセキュリティを確保するため、以下(表1)に記載の製品・サービスをご利用のお客様におかれましては、表中のリンク先ページに記載の対処を頂けますようお願いいたします。

[脆弱性概要]

細工されたURLにアクセスした場合に、弊社複合機/プリンタを介して第三者が指定した外部サイトへ遷移してしまう可能性があります。

この脆弱性が悪用された場合、正規サービスを装ったURLから不正なサイトへ

誘導される可能性があります。送信元や内容に心当たりのないメールやメッセージに記載されたURLはクリックしないようご注意ください。

表1.脆弱性への対処が必要なリコー製品・サービス

製品・サービス	詳細情報ページ
RICOH Pro 8420S/8410S/8400S	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000263-2026-000004
RICOH MP C306	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000053-2026-000004
RICOH MP CW1201/CW2201	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000050-2026-000004
RICOH Pro 8420Y/8420HT/ 8410Y/8410HT	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000264-2026-000004
RICOH P C6010/C6010M	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000259-2026-000004

製品・サービス	詳細情報ページ
RICOH IP C6020/C6020M	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000154-2026-000004
RICOH P 6520/6520M/65 10/6510M/6500	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000260-2026-000004
RICOH IP 6530/6530M	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000155-2026-000004
RICOH P 501/501M/500/ 500M	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000113-2026-000004
RICOH SP 8400/8400M/84 00a1/8400M a1	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000114-2026-000004
RICOH P C375/C375M	影響あり。詳細はこちらを参照ください。 > https://jp.ricoh.com/security/products/vulnerabilities/adv?id=ricoh-prod000267-2026-000004

本件に関するお問合せ先

リコーテクニカルコールセンター

Tel: 0120-892-111

※ 対応時間：祝日を除く月～金 9:00～17:00

謝辞:

本脆弱性をご報告いただいたSIXGEN社のTony Kirkland様に感謝いたします。

更新履歴:

2026-04-30T12:00:00+09:00 : 1.00J 新規公開

本ページのURL:

<https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2026-000004>

このURLリンク先と内容の異なる、あるいはURLを省略した、このドキュメントのテキストのコピーは、重要な情報の欠落や誤りの可能性がありますのでご注意ください。

[ホーム](#) > [サステナビリティ](#) > [ガバナンス](#) > [情報セキュリティ](#) > [プロダクトセキュリティ](#) > [脆弱性ごとの情報リスト](#) > [脆弱性情報](#)

リコーについて	株主・投資家情報	サステナビリティ	技術	ニュース
ビジョン	IRニュース	環境	技術開発について	ニュースリリース
会社概要	経営方針説明会	社会	リコーの技術一覧	お知らせ
関連会社	事業説明会/ESG説明会	ガバナンス	リコーテクニカルレポート	重要なお知らせ
統合報告	決算説明会	情報セキュリティ	リコーデザイン	ストーリーズ
DX・働き方変革	決算短信	製品・サービス	採用	
コミュニケーション活動	有価証券報告書	☞		

事業報告書(招集
通知/株主通信)

新卒・キャリア採
用

株主総会

障がい者採用

株式基本情報

インターンシップ

株主還元

関連会社の採用

個人投資家の皆様
へ

リコーについて



株主・投資家情報



サステナビリティ



製品・サービス



技術



採用



ニュース



[一覧へ](#)

[Page Top](#)

[個人情報保護について](#) [ご利用条件](#) [商標について](#) [アクセシビリティ](#) [サイトマップ](#) [お問い合わせ](#) [Cookie設定](#)

© Ricoh