

「Yahoo!メール」アプリ、安全なメールの送信者アイコンに色が付く「ブランドカラー」機能を提供開始

～ メール送信元の認証情報（SPF、DKIM、DMARC）も確認可能になり、より安全で安心してメールが利用可能に ～

ヤフー株式会社（以下、Yahoo! JAPAN）が運営する「Yahoo!メール」アプリ（iOS版、Android版）は、メールによるなりすまし被害を防ぐため、なりすまし対策がされている安全なメールに色が付く「ブランドカラー」機能の提供を開始しました。



悪意のある第三者が、実在する企業や団体を装いメールを送信する「なりすましメール」は、ウイルスに感染するファイルの送信や、偽サイトへのアクセスにより個人情報を抜き取るフィッシング詐欺の要因の一つとして大きな社会問題になっています。フィッシング対策協議会が2021年2月3日に発表した月次報告書（※1）によると、2021年1月にフィッシング対策協議会に寄せられたフィッシング報告件数（海外含む）は43,972件であり、昨年比で6倍以上増加しています。

これらの問題を受け「Yahoo!メール」アプリを利用するユーザーが安全に安心してメールを閲覧できることを目的とし、「ブランドカラー」機能の提供を開始しました。

本機能は、「Yahoo!メール」が送信ドメイン認証を確認した一部のドメインから受信したメールの送信者アイコンに色が付く機能です。これにより、ユーザーは「ブランドカラー」に対応したドメインからのメールを安心して開封し、確認できます。送信者アイコンに色が付くのはSPF認証（※2）もしくはDKIM認証（※3）という、なりすましメール対策がされている約50の企業ドメインになり、順次拡大予定です。

また、ユーザーが受信したメールの、SPFやDKIM、DMARC（※4）の認証情報を簡単に確認

できる機能の提供も併せて開始します。本機能によりユーザーは受信したメールが正しく認証されたかどうかを確認（※5）できます。なお、正しい認証が確認できない場合、注意をうながすメッセージが表示されます。

これらの取り組みにより、ユーザーは安心して「Yahoo!メール」アプリを利用でき、また送信者アイコンに色が付くことでメール一覧画面での送信元の視認性が高まります。

「Yahoo!メール」は、なりすましメールやフィッシングメール対策として、2018年10月に「ブランドアイコン」（※6）を導入、2020年3月に「DMARC」（※7）を導入するなど継続的な取り組みを実施しています。一方で、SPFやDKIM、DMARCといった送信ドメイン認証技術は、メールの送信元が導入を行う必要があります。「Yahoo!メール」は「ブランドカラー」や「ブランドアイコン」を通じてメールの送信元へ認証技術の導入を推進し、より安全で安心な環境でユーザーにサービスを利用いただけるよう、機能追加や改善を行ってまいります。

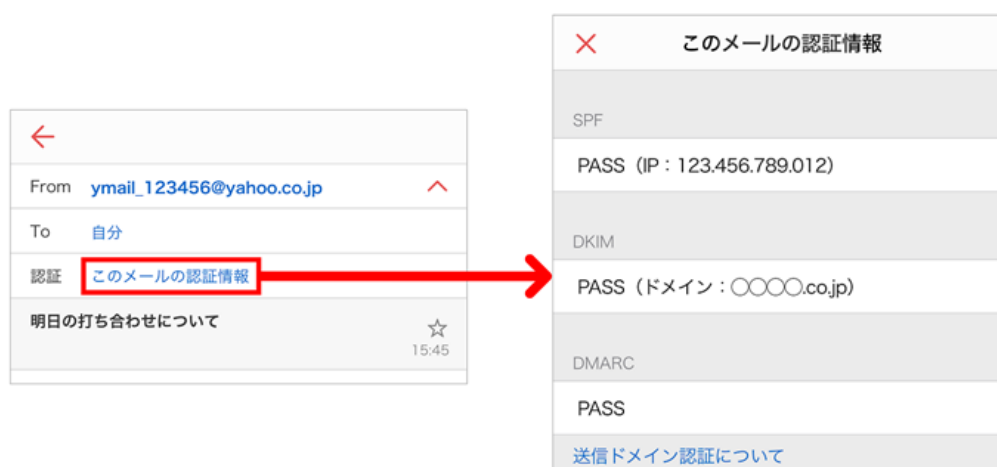
[「Yahoo!メール」アプリ（iOS）（外部リンク）](#)

[「Yahoo!メール」アプリ（Android）（外部リンク）](#)

■ ブランドカラー機能



■ 認証情報の確認画面



※1：[フィッシング対策協議会 フィッシング報告状況より](#)（外部リンク）

※2：SPF（Sender Policy Framework）：メールの送信元から、そのメールがなりすましであるかどうかを判断する技術。そのドメインからのメールを送信すると宣言されているサーバ

ーから送られているかを確認する。「Yahoo!メール」では2006年より導入。

※3：DKIM（DomainKeys Identified Mail）：送信元がメールに電子署名を付与し、受信者でそれを検証することで認証を行う技術。メールの改ざんがされていないかどうかを判断できる。「Yahoo!メール」では2012年より導入。

※4：DMARC（Domain-based Message Authentication, Reporting & Conformance）：送信事業者側がなりすまされたメールの扱いをあらかじめ設定し、受信事業者側がその扱いに準じたフィルタリングを実施する送信ドメイン認証技術

※5：2021年2月中旬以降に受信したメールから確認できます。

※6：Yahoo!メール、フィッシングメール対策として、企業などのブランドアイコンを表示する取り組みを開始

※7：Yahoo!メール、迷惑メール対策として、米国などグローバルで活用が進む送信ドメイン認証技術「DMARC」を3月より順次導入