プレスリリース 2020.01.29

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

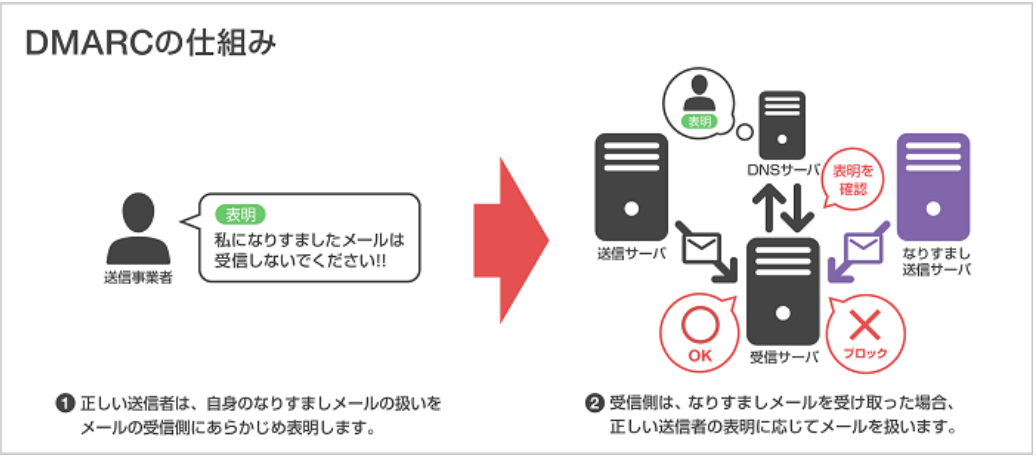
～ 送信事業者とヤフーとの連携により、なりすましメールを削減
ユーザーにより安全で安心なメール環境を提供 ～

「DMARC」説明ページ

ヤフー株式会社（以下、ヤフー）は、運営するメールサービス「Yahoo!メール」において、セキュリティ強化を目的に、なりすましメール対策として送信ドメイン認証技術「DMARC（Domain-based Message Authentication, Reporting & Conformance）」を2020年3月より順次導入します。

企業や銀行などを装ったメール（なりすましメール）から偽サイトに誘導し、ユーザーのクレジットカード番号などの個人情報を盗みとるフィッシング詐欺は、社会における大きな問題となっています。
「Yahoo!メール」ではメール対策技術として、送信元のドメインを認証するSPF（※1）やDKIM（※2）を導入しています。SPFやDKIMが受信事業者側（「Yahoo!メール」側など）でなりすましを判断する技術であるのに対して、DMARCは送信事業者側がなりすまされたメールの扱い（ブロックする、迷惑メールフォルダに振り分けるなど）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ことで、なりすましメールを届きにくくする技術です。

DMARCの導入により、なりすましメールを排除する効果が高まるため、より安全で安心な環境で「Yahoo!メール」をお使いいただけます。



米国においては、政府機関から送信するメールにはDMARCの設定が義務付けられるなど、グローバルでDMARCの活用が推進されています。国内においては、2017年7月に総務省がDMARCの導入留意点を定め（※3）、ヤフーはそれにのっとってDMARCを導入します。月間約2,300万人が利用（※4）している「Yahoo!メール」がDMARCを導入することによって、送信事業者においてもDMARCの導入が進む契機になることを期待しています。
また政府では、重点的かつ効果的にサイバーセキュリティに対する取り組みを推進するため、毎年2月1日から3月18日までを「サイバーセキュリティ月間」（※5）と定め、サイバーセキュリティに関する普及啓発強化を図っています。当社は同活動に協力するとともに、「Yahoo!メール」においては、今後もユーザーが安全で安心にメールを利用できる環境を提供するため、機能追加や改修を行ってまいります。

※1：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。
※2：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。
※3：総務省「送信ドメイン認証技術等の導入に関する法的解釈について」（外部リンク）
※4：1か月に1回以上「Yahoo!メール」にログインした利用者数の年間平均値。1つのYahoo! JAPAN IDにつき1人の利用者とした場合（2019年3月現在）
※5：内閣サイバーセキュリティセンター「サイバーセキュリティ月間」（外部リンク）

■参考）セキュリティ強化に伴うヤフーの最近の取り組み
・2020年1月8日発表：長期間ご利用がないYahoo! JAPAN IDに対し利用停止措置を実施
・2019年5月9日発表：Yahoo!ショッピングのiOS版アプリ上の再認証に生体認証を導入
・2018年10月30日発表：Yahoo!メール、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
・2018年10月23日発表：Androidスマートフォンのウェブブラウザー上でのログインが指紋認証などの生体認証に対応