フィッシング被害を防げ！クレカ会社などにDMARC導入を要請

経産省と総務省、警察庁がフィッシングメール対策で要請

経済産業省と総務省、警察庁は2月1日、クレジットカード会社などに対し、DMARC（ディーマーク）の導入をはじめとするフィッシング対策の強化を要請した。「なりすまし」メールなどを検出し、クレジットカード番号などの搾取を狙う迷惑メールが利用者に届かなくなるようにする環境の整備を急ぐ。

なりすまし・フィッシング詐欺を防止する「DMARC」とは

DMARC（Domain-based Message Authentication, Reporting and Conformance）とは、電子メール認証プロトコルの1つで、正当な組織から送信されたように装った「なりすまし」のメールを検知し、送信先に届く前にブロックする仕組みのこと。SPF（Sender Policy Framework、送信者のドメインを利用したなりすましメッセージを阻止する技術）やDKIM（DomainKeys Identified Mail、第三者が電子メール内のデータを改ざんしていないことを確認する技術）など単体の技術を組み合わせることで、「なりすまし」と判断した迷惑メールの取り扱いを正規のメール送信者が指定することができる。

民間のメールシステム会社が2022年5月に実施した調査によると、日経平均株価の選定銘柄である225社のうちDMARCを導入している企業は約半数（49.8%）だった。

Amazonを騙るフィッシング報告が半数超に

フィッシング対策協議会によると、2022年12月のフィッシング報告件数は前月比4730件減の6万5474件。前月比は3カ月連続のマイナスとなったが、Amazonを名乗るフィッシング報告が前月に続いて急増し、報告数全体の51.7%に上っている。月に1000件以上の大量のフィッシング報告が寄せられたブランドも9つあり、全体の89.9%を占めた。

同協議会の調査用メールアドレス宛に12月に届いたフィッシングメールの85.7%は、実在するサービスのメールアドレス（ドメイン）になりすましていた。フィッシングサイトのURLをQRコードにしてメールに埋め込む手法が増加。キャッシュレス決済の正規サービスに誘導し、送金させるケースも報告されている。

認証外メール受信拒否のポリシー運用も求める

同協議会によると、DMARCで排除できるフィッシングメールは63.0%だが、報告の多くは受信時にDMARCポリシーに従ってメールをフィルターしていないサービスの利用者から届いている。このため、オンラインサービスを提供している事業者には、DMARCなどによるドメイン保護を呼び掛けている。

経産省などの要請は、こうした状況を踏まえた措置。クレジット会社などに対しては、利用者向けに公開する全てのドメイン名（メール送信をしないドメイン名を含む）についてDMARCを導入するよう促した。導入に当たっては、受信者が「なりすまし」メールの受信を拒否するポリシーの運用も求めている。

文：M&A Online編集部