

フィッシング対策の強化を!!

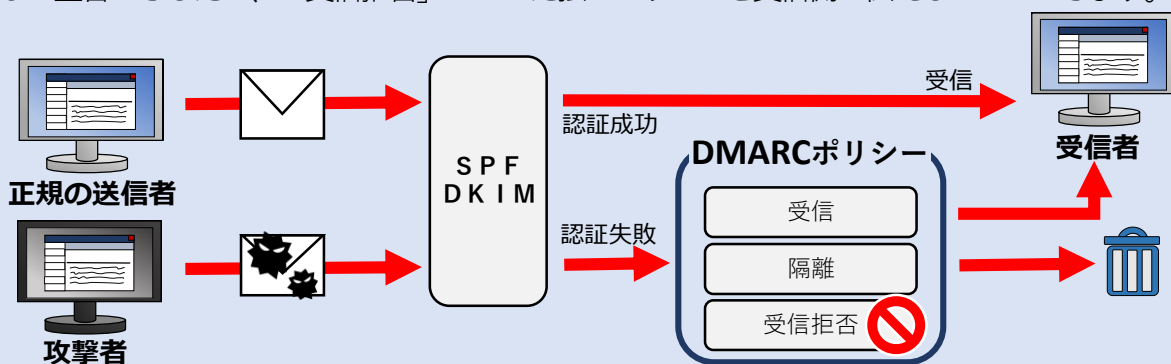
実在する金融機関、EC事業者、物流事業者等を騙ったフィッシングによる不正送金の被害が全国的に急増しています。

そこで、利用者保護のための取組として対策例を2つ紹介させていただきます。

対策例

1. DMARC ※1

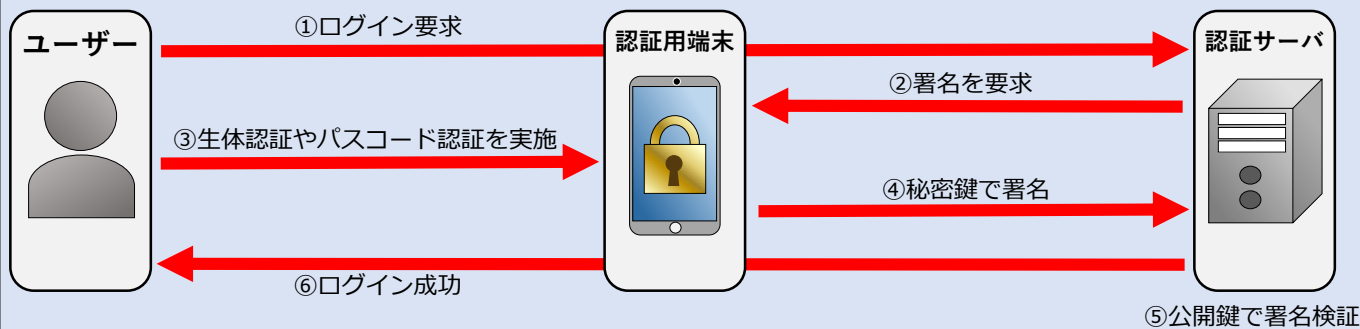
DMARCとは、SPF・DKIMの認証結果を利用し、総合的に送信ドメイン認証を行う技術です。ドメイン管理者は、なりすましメール（認証に失敗したメール）の取り扱いを送信側でDMARCポリシーとして宣言できるため、「受信拒否」といった強いポリシーを受信側に伝えることができます。



2. FIDO認証 ※2

FIDO認証とは、オンラインサービスを利用する際にパスワードを使わず、公開鍵暗号方式と生体認証等を組み合わせて認証を行う規格のことです。

ユーザー側と認証サーバ側で秘密の情報を共有しないため、情報窃取を目的とするフィッシングへの対策に有効とされています。



※1 DMARCの詳細についてはこちらをご確認ください。
迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル」
<https://www.dekyo.or.jp/soudan/asp/report.html>



※2 FIDO認証の詳細についてはこちらをご確認ください。
FIDO ALLIANCE
<https://fidoalliance.org>

