参考資料５

経済産業省
Ministry of Economy, Trade and Industry

クレジットカード会社等に対するフィッシング対策の強化を要請しました

2023年2月1日

同時発表：警察庁・総務省

▶安全・安心

経済産業省、警察庁及び総務省は、クレジットカード番号等の不正利用の原因となるフィッシング被害が増加していることに鑑み、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC*）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ました。

昨今、悪意のある第三者が、クレジットカード会社等を騙った電子メール等を利用者に送信し、利用者を当該電子メール等のリンクから偽サイトに誘導したうえで、利用者のクレジットカード番号等を詐取する攻撃（いわゆるフィッシング）が多発しています。

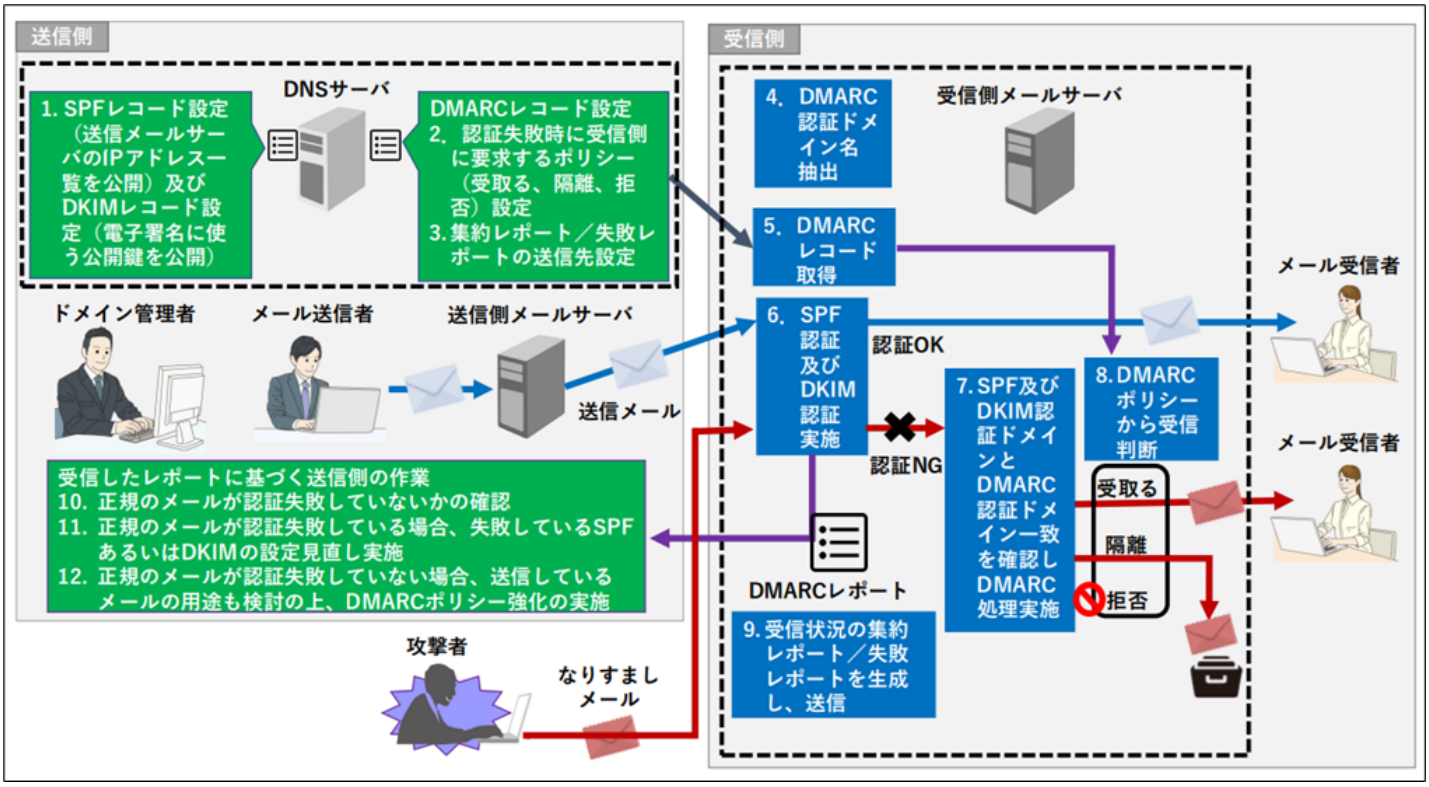
フィッシングによるクレジットカード番号等の詐取は、クレジットカード番号等の不正利用の一因となっており、利用者保護の観点から、クレジットカード会社等において適切な対応が取られることが求められます。とりわけ、フィッシングメールがドメイン名をなりすまして送信されることが多い点に鑑みると、送信ドメイン認証技術のうち、フィッシングメール対策に特に有効とされているDMARCを導入し、ドメイン名のなりすましを検出するとともに、自社を騙るフィッシングメールが利用者に届かなくなるよう利用者の受信を制限することが重要です。

経済産業省、警察庁及び総務省は、こうした状況を踏まえ、クレジットカード会社等に対してフィッシング対策の強化を要請しました。概要は以下のとおりです。

1．DMARCの導入によるなりすましメール対策

・利用者向けに公開する全てのドメイン名（メールの送信を行わないドメイン名を含む）について、DMARCを導入すること。

・DMARC導入にあたっては受信者側でなりすましメールの受信拒否を行うポリシーでの運用を行うこと。



図：DMARCの仕組み

出典：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」

*DMARC: Domain-based Message Authentication, Reporting, and Conformanceの略称。

2. その他のフィッシング対策

・フィッシング対策協議会が策定した「フィッシング対策ガイドライン」において、フィッシングに対して有効とされている対策を実施すること。

関連リンク

- 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第3版
- フィッシング対策協議会「フィッシング対策ガイドライン2022 年度版

担当

商務・サービスグループ商取引監督課長　刀禰
担当者： 松井、竹尾、小西

電話：03-3501-1511(内線　4191)
　　03-3501-2302（直通）
メール：bzl-shotorihiki-kantokuka★meti.go.jp
※[★]を[@]に置き換えてください。