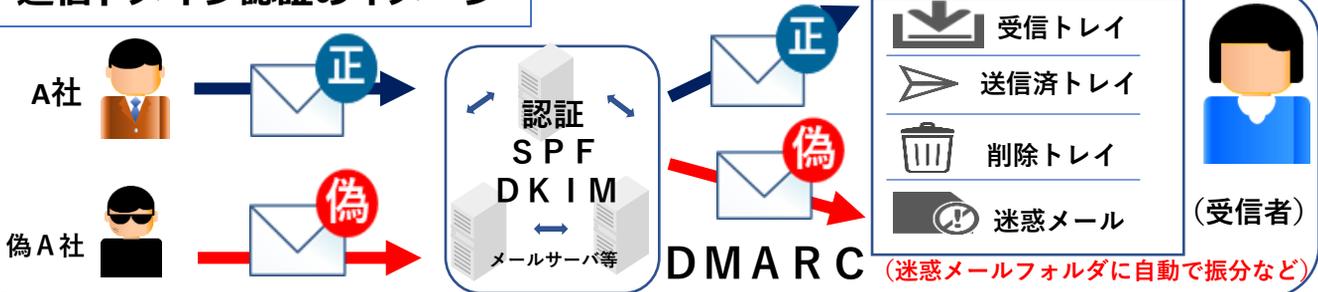


## なりすまし被害防止！

# 送信ドメイン認証技術を導入しよう！

- ◆ フィッシングによる被害を防止するためには、**DMARC**などの**送信ドメイン認証技術**を活用し、**なりすましメールを受け付けない**ようにすることが有効です。
- ◆ フィッシングメールやビジネスメール詐欺などのなりすましによる被害を防止するために、送信ドメイン認証技術を導入しましょう！

### 送信ドメイン認証のイメージ



### 認証が失敗したときの事前対処マニュアル～DMARC

SPF・DKIMによる認証が失敗した場合の対応を事前に決めることで、受信をしない「拒否」や迷惑メールに「隔離」するなど、自動で対処できる技術

### 送信元情報を事前登録する～SPF

事前に送信元のIPアドレスを登録し、送信元がなりすましのアドレスか識別できるよう確認する技術。

### 電子署名をメールに付与する～DKIM

電子署名が正しいものか検証し、なりすましかどうかを識別する技術

(参考) 「送信ドメイン認証技術導入マニュアル」  
迷惑メール対策推進協議会から公表されています。

<https://www.dekyo.or.jp/soudan/aspc/report.html>

