熊本県警察本部サイバー犯罪対策課

サイバーセキュリティニュース

事業者におけるフィッシング対策

フィッシングサイトへは、企業の本物のメールアドレスになりすましたメールで誘導するケースも確認されています。事業者にあっては、自社のドメインの悪用を防止する観点で、「送信ドメイン認証技術」の導入をご検討ください。

主な「送信ドメイン認証技術」

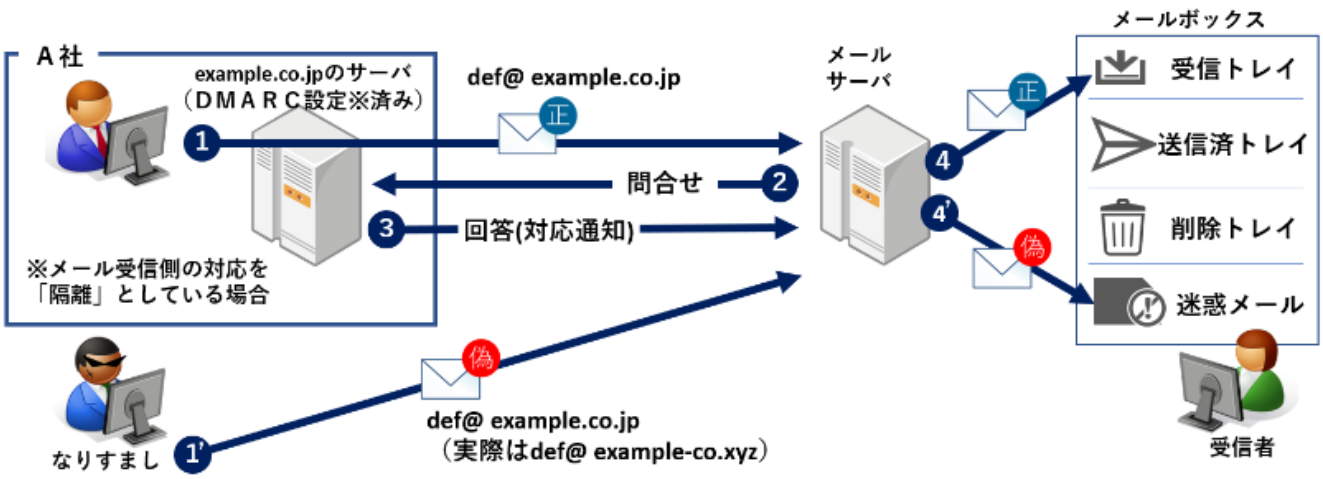
- SPF（ネットワーク方式）：メール送信元IPアドレスの妥当性を認証するもの
- DKIM（電子署名方式）：電子署名を検証することで認証するもの
- DMARC：ネットワーク方式と電子署名形式を組み合わせたもの

特に、DMARCは認証に失敗したメールの取扱いを送信側で宣言できます。

これにより、なりすまされているメールは受け取らない、といった強いポリシーを受信側に伝えることができるようになります。

ＤＭＡＲＣの仕組みの概要

DMARCを導入することにより、なりすましメールを迷惑メールフォルダに隔離（quarantine）したり、メールボックスに到達させない（reject）ようにすることができます。
下図は、隔離の際の仕組みの概要について説明しています。



正規メール の場合
1. 正規のメール を送信
2. A社のサーバに問合せ
3. A社のサーバが回答
4. は受信トレイに

なりすましメール の場合
1'. なりすましメール を送信
2. A社のサーバに問合せ
3. A社のサーバが回答
4'. は迷惑メールフォルダに（隔離）

DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、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

【出典】警察庁　フィッシング対策

https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html