自社の“なりすましメール”をブロック！

「DMARC」でフィッシングメール対策！

「DMARC（※１）って何？　どんなことができるの？

　「送信ドメイン認証技術」の一つで、送信者側からメールサーバ等へ設定を行うことで、自社になりすましたメールを

　　　　受信者に届けない　または　迷惑メールとして扱う（※２）

ことができるようになる仕組みのことです。

メールの受信者を自社になりすましたメールから守ることができます。

※１ Domain-based Message Authentication,Reporting,and Conformanceの略

※２ 送信者側から「reject（届けない）」「quarantine（迷惑メールにする）のどちらかを

設定可能

「DMARC」動作概要のイメージ

DMARCの設定が無い場合

設定された情報が無いため、正規メールもなりすましメールも同じように受信者に到達

DMARCの設定（quarantine）を行った場合

設定された情報を基になりすましメールだけを迷惑メールフォルダに自動で振分

（参考）「送信ドメイン認証技術導入マニュアル」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**

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！