おいしい毎日がやってくる！
デリクックちくま

【注意喚起】弊社を装った「なりすましメール」にご注意下さい

2024.3.25

平素より当ホームページを閲覧していただき、誠にありがとうございます。

弊社では「まりすましメール対策」として送信元メールサーバーにセキュリティ対策として SPF、DKIM、DMARC の設定を行っています。

※こちらは弊社利用中のサーバーによる対策となります。

SPF とは送信元メールサーバの IP アドレスを送信側の DNS に SPF レコードとして事前に登録し、受信者はメール受信時に送信側の SPF レコードと照合し認証されたメールのみ受け取る仕組みです。

DKIM とは送信メールに電子署名を付与し送信側 DNS に公開鍵情報を登録、受信者は送信側 DNS 上の公開鍵情報と受信メールの電子署名を照合し認証されたメールのみ受け取る仕組みです。

DMARC とは送信者側が受信側の受信メールが SPF や DKIM の認証に失敗したときの推奨アクションを DNS サーバーに「DMARC ポリシー」として宣言しておくことです。受信側は認証失敗時にこの DMARC ポリシーを参照して、受信メールをどう扱うか（受信する、隔離する、拒否する）を判断します。

DMRC ポリシーに「拒否する」と定義されていれば受信メールを棄却します。

DMRC ポリシーに「隔離する」と定義されていれば受信メールを隔離します。

DMRC ポリシーに「何もしない」と定義されていれば受信メールを受信し、受信者に判断を委ねます。

これは正しいメールでありながら、認証されなかったメールを救出する方法となります。