

なりすましメール対策！

送信ドメイン認証技術「DMARC (ディーマーク)」

◆「送信ドメイン認証技術」

送信ドメイン認証技術とは、なりすましメール対策として、メールを送信する側がメールを受信する側に対して、正規のメールとなりすましメールを見分ける方法を提供するための仕組みです。

DMARC?



◆「DMARC」

DMARC (Domain-based Message Authentication, Reporting, and Conformance) とは、メールを送信する側が、「検証の結果、なりすましメールと判定されたメールを受信する側でどう扱ってほしいか。」を宣言する技術です。

送信する側で宣言できるポリシーは、

- メールをそのまま受信させる。
- なりすましメールとして隔離する。
- メールを受信拒否する。

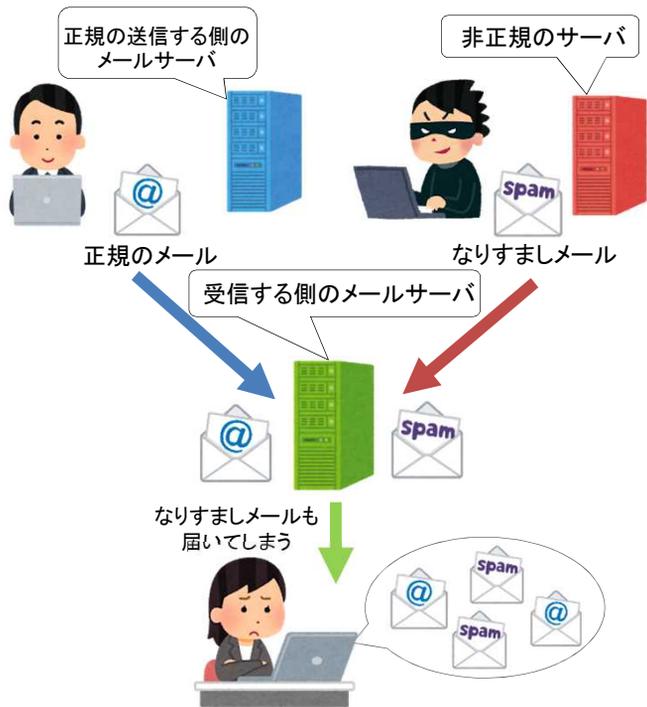


なんと！
そんな技術があったのか〜

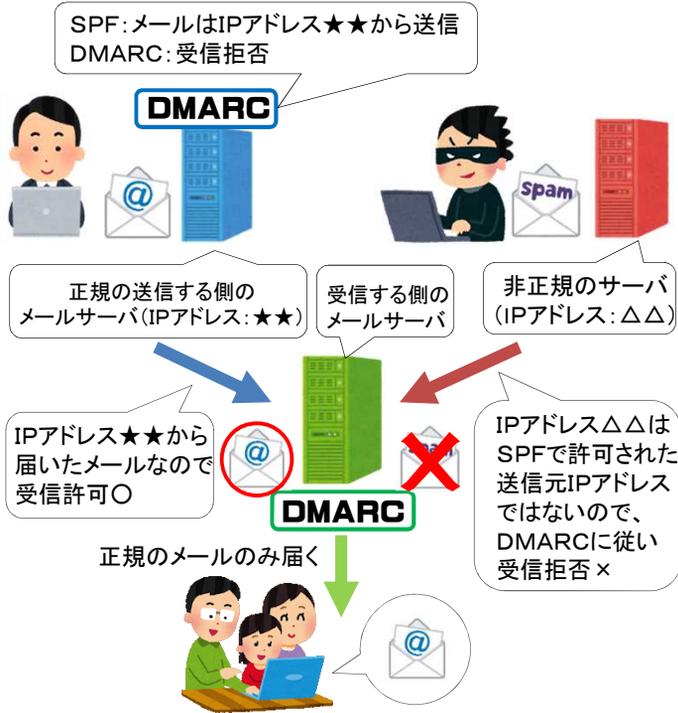
の3種類があります。

送信する側でなりすましメールを隔離や受信拒否するよう宣言し、受信する側がそのポリシーに従い、なりすましメールを隔離や受信拒否することで、なりすましメールが利用者まで届かず、フィッシングによる被害を抑止することができるのです！

《対策をしていない場合》



《DMARCによる対策を行っている場合》



DMARCは、送信する側のメールサーバ・受信する側のメールサーバ
双方に導入することで効果を発揮する技術です！