

DMARCでフィッシングメール対策！

DMARCってなに？

DMARC※は、フィッシングメール（なりすましメール）の送信を防止するための認証技術の1つで、なりすましの可能性があるメールについて、なりすまされたドメインの本当の所有者が、その取扱いを指定することができる仕組みです。

DMARCを設定すると何ができるの？

DMARCを設定すると、フィッシングメール（なりすましメール）を

- ・ 受信者に届けない → reject
- ・ 迷惑メールとして取り扱う → quarantine

ように指定することができます。

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

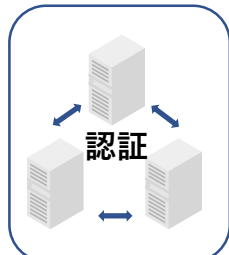
DMARCの動作概要

DMARCの動作概要（quarantineに設定した場合）は次のとおりです。

正規のメールの場合



A社
(送信者)



メールサーバ等

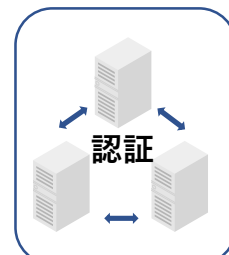


顧客
(受信者)

なりすましメールの場合



攻撃者
(A社のなりすまし)



メールサーバ等



顧客
(受信者)

迷惑メールフォルダに
自動で振分(quarantine)

(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>



北海道警察

YouTube動画
サイバ-セキュリティ講座
公開中です！



北海道警察公式HP
サイバ-セキュリティひろば