ＤＭＡＲＣ（ディーマーク）でフィッシングメール対策！

悪意のある第三者が、企業等になりすまして利用者にメールを送信し、偽サイトに誘導してID・パスワードを詐取する攻撃（フィッシング）が多発しています。
第三者にドメインを不正に利用されないよう、下記DMARCを導入しましょう。

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。

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

ＤＭＡＲＣを設定すると何ができるの？

DMARC を導入すると、フィッシングメール（なりすましメール）を

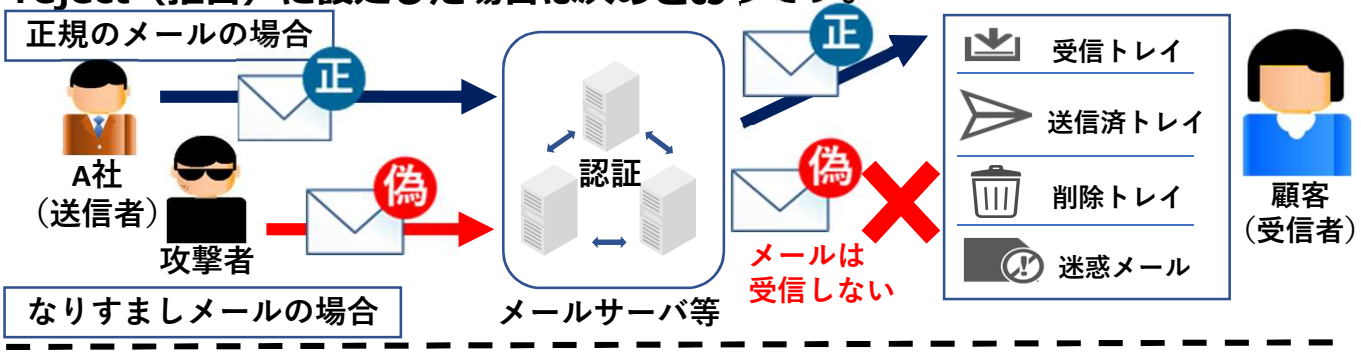
・ 受信者に届けない ⇒ reject（リジェクト）（拒否） ⇐「reject」設定が推奨！

・ 迷惑メールとして取り扱う ⇒ quarantine（クアランティン）（隔離）

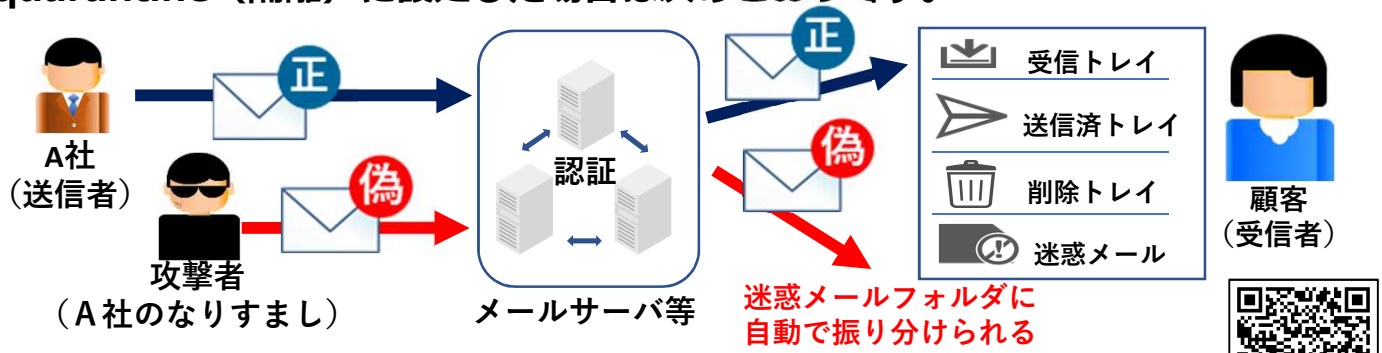
などのように設定することができます。

ＤＭＡＲＣの動作概要

reject（拒否）に設定した場合は次のとおりです。



quarantine（隔離）に設定した場合は次のとおりです。



（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

近年、なりすましメールを受信者に届けない「reject（拒否）」設定が特に推奨されています。

北海道警察

YouTube動画
ｻｲﾊﾞｰｾｷｭﾘﾃｨ講座
公開中です！

北海道警察公式HP
ｻｲﾊﾞｰｾｷｭﾘﾃｨひろば