CyberNews
サイバー犯罪対策課
広　報　用　資　料
令　和　７　年　第　１　０　号
サ　イ　バ　ー　犯　罪　対　策　課

〔企業・団体向け対策のご紹介〕
御社になりすましたフィッシングメールへの対策

送信ドメイン認証技術「DMARC※」導入のご検討を！

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

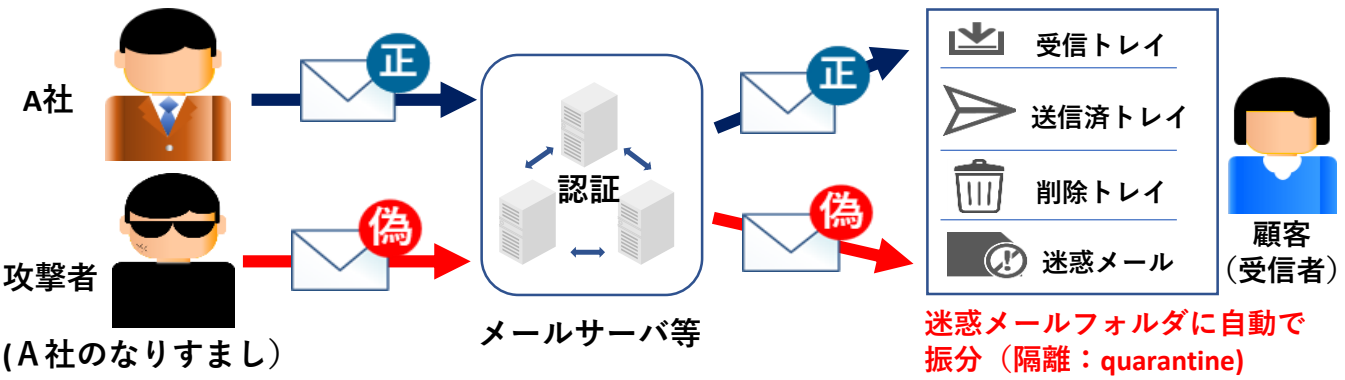
「ＤＭＡＲＣ」とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン名単位で確認する技術です。

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
- 迷惑メールとして取り扱う（**隔離**：quarantine）
- 受信者に届けない（**拒否**：reject）

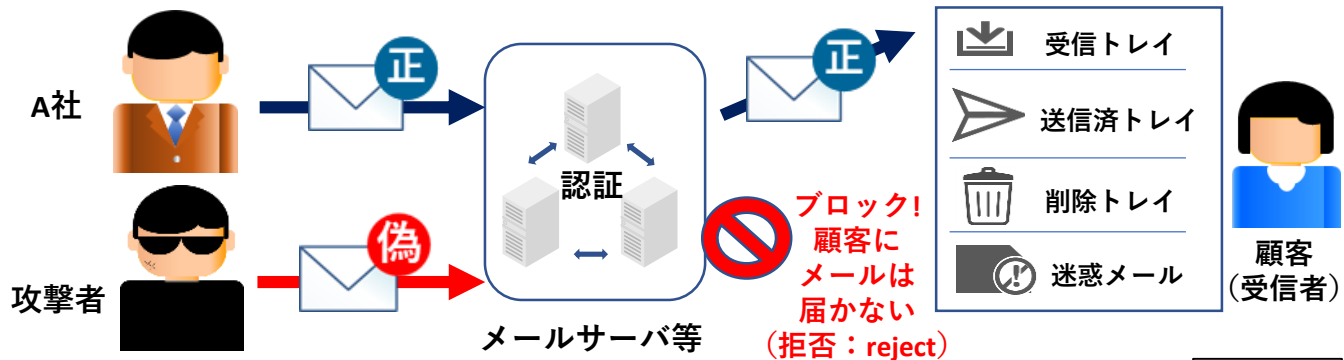
ことができます。

ＤＭＡＲＣの動作概要

隔離：quarantineに設定した場合



拒否：rejectに設定した場合



（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

佐賀県警察
(https://www.police.pref.saga.jp/kurashi/cyber.html)