CyberNews
サイバー犯罪対策課

広　報　用　資　料
令　和　８　年　１　９　号
サイバー犯罪対策課

あなたの会社のメール、「誰でも名乗れる状態」になっていませんか？

送信元メールアドレスのドメイン（@より右の部分）は簡単に偽装することができます。

DMARCは、あなたの会社のドメインを悪用したなりすましメールから顧客・取引先や会社の信用を守る仕組みです。

※　DMARCは送信側（会社側）が設定する必要があります！

導入方法はこちらのサイトをご確認ください。

https://www.dekyo.or.jp/soudan/aspc/report.html

DMARCの仕組み

① SPF・DKIMによる認証

メールを受け取った受信サーバーでは、送信元のIPアドレスや電子署名を検証

② ドメインとの整合性を確認

送信元メールアドレスのドメインと、①の検証に使用されたドメインが一致しているかを確認

③ 不審なメールに対応

検証結果から不審が認められた場合は、ドメイン管理者が定めた方針（ポリシー）に沿ってメールを処理

ドメイン管理者の設定（ポリシー設定）による処理方法の違い

①　None（未設定）

検知結果を記録し、通常のメールと同様に宛先に送付（＝顧客に不審メールであることが伝わらない）

②　Quarantine（隔離）

不審なメールとして迷惑フォルダに隔離（＝顧客が不審メールであることが分かる）

③　Reject（拒否）

受信サーバーで不審メールを破棄（＝不審メールが顧客に届かない）

DMARC導入の主なメリット

顧客・取引先の保護

なりすましによる詐欺や情報漏えいを防止

ブランド・信頼の維持

自社ドメインの悪用を防ぎ、企業イメージを守る

メール到達性の向上

迷惑メール判定を減らし、自社メールを届きやすく

今すぐチェック！

設定が「None（未設定）」のまま放置されていませんか？

- ☐ DMARCポリシーの設定を確認する。
- ☐ レポートを確認し、自社ドメインを名乗るメールを把握する。
- ☐ 把握できたら、Quarantine又はRejectへの移行を検討する。

警察庁 National Police Agency

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