Cyber Security News

R8.10

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？

DMARCは、自社ドメインを悪用したなりすましメールから顧客・取引先・自社ブランドを守る仕組みです。

郵便局にたとえるDMARCの仕組み

① 住所・封蝋確認（SPF・DKIM認証）



郵便局員が、送り主の住所に紐付く氏名と封蝋（印）を確認。
（送信元IP・電子署名の検証）

② 名義の照合（アライメント確認）



送り主の氏名と、郵便局が持つ送り主リストを照合。
（送信元ドメインの検証）

③ 怪しい手紙に対応（ポリシー処理）



異常発見時は、定めたマニュアルに沿って厳正に対応。

③の対応（ポリシー設定）

① None（記録のみ）



記録し、宛先に送付
（＝顧客が受信）

② Quarantine（隔離）



不審物として保管
（＝顧客の迷惑フォルダへ）

③ Reject（拒否）



配達しない
（＝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（記録のみ）」のまま放置されていませんか？

- ☐ DMARCポリシーの設定（Noneのままか？）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。

神奈川県警察サイバーセキュリティ対策本部

警察庁 National Police Agency