企業向け

サイバーニュース
Cyber-News

R８年第１３号
奈良県警察本部
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？



DMARC（ディーマーク）でフィッシングメール対策しましょう

事業者は、自社のドメインの悪用を防止し、
顧客・取引先・自社ブランド
を守るため「送信ドメイン認証技術」の１つであるDMARCをご検討ください。



「DMARC」について
詳細は警察庁ＨＰをご参照ください

警察庁サイバー警察局
フィッシング対策（事業者における対策）
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

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

DMARCの仕組みを 郵便局 にたとえると・・・

① 住所・封蝋(印)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）

差出人リスト
〇〇株式会社 example1.co.jp
△△株式会社 example2.co.jp
□□株式会社 example3.co.jp



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（ポリシー設定状況により対応が異なります）

認証に失敗したメールの取扱いを送信側で指定できます

None（記録のみ）



記録し、宛先に送付
（＝顧客が受信）

Quarantine（隔離）



不審物として保管
（＝顧客の迷惑フォルダへ）

Reject（拒否）



配達しない
（＝顧客に届かない）



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のままではないか)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（隔離） 又は Reject（拒否） への移行を検討する。



奈良県警察
Nara Prefectural Police

警察庁
National Police Agency

奈良県警察のホームページでは、サイバーセキュリティ対策に関する情報を掲載しています。
是非ご覧ください！

奈良県警察HP