送信ドメイン認証(SPF/DKIM/DMARC)の導入について

OTNet 2025/3/4

SPF/DKIM/DMARCによる送信ドメイン認証を行うことにより、なりすましメールを識別し、被害を未然防止に役立ちます。

また、認証結果をメールのヘッダーに追加することにより、送信元アドレスの正当性を確認する事ができます。

- ※ SPF: 受信メールの送信元メールサーバのIPアドレスを確認 DKIM: 受信メールの電子署名を検証 DMARC:認証失敗時の対応策を定義
- ※ 他ISPからii-okinawaへメール**転送を行っている場合**等、正しく判定されない場合があります。
- ※ 送信ドメイン認証を行うには**迷惑メール判定サービスを有効**にする必要があります。

概要図 ISP-A 問い合わせ SPF/DKIM/DMARC pass ISP-Aのユーザ (送信元認証OK) ii-okinawa メールサーバ 認証 ii-okinawaのユーザ メールサーバ ISP-Aと偽る 迷惑メール 迷惑メール fail等 配信者等 (送信元詐称の疑いがあります)

ヘッダ例と認証結果

お客様の受信メールのヘッダに「Authentication-Results」 に続いて、認証結果が記載されます。 l) spf=認証結果 dkim=認証結果 dmarc=認証結果

認証結果	意味	解説
Pass	成功	送信ドメインの正当性が認証された正しい送 信元から送信されたメールである。
Fail	失敗	送信ドメインは詐称されている。
Soft Fail	失敗	送信ドメインは詐称されている可能性がある。
Permanent Error Temporary Error	不可能	認証処理が失敗している。
None	存在 しない	送信ドメインの認証情報が公開されていない ため、認証ができない。