M³AAWG 技術サマリー

SPF (Sender Policy Framework)

2023 年 9 月

この文書の参考 URL https://www.m3aawg.org/ts_SPF

SPF とは：

SPF は、メール認証プロトコルであり、特定のドメインからメールを送信することが許可された IP アドレスを確認します。

SPF は何をするのか：

- ドメイン所有者は、認可された IP アドレスおよびドメインのリストを公開し、そのリストからメールを送信できるようにします。
- 受信サーバーは、送信サーバーの IP アドレスを、認証対象のドメインが公開した許可リストと照合します。
- IP アドレスが許可リストに含まれている場合、SPF=pass の結果が返されます。送信サーバーが認可されていない場合、認証クエリの結果は SPF=fail となります。認証クエリは SPF= neutral や SPF=soft fail などの他の結果も返すことがあります。

SPF は何をしないのか：

- SPF は、メッセージの内容の信憑性や品質を保証せず、メッセージが「良い」または「正当な」ものであることを証明するものではありません。
- SPF は、直接接続されたサーバーの IP アドレスを使用するため、SPF=pass はメーリングリストや卒業生アドレス転送などによる単純な配信や転送では持続しません。
- SPF の認証失敗が発生する原因には無害なものがいくつか存在するため、SPF=fail は悪意のある活動や悪い活動を意味するものではありません。

参考資料:

RFC 7208, “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email,

V1" RFC 5321, "Simple Mail Transfer Protocol" (SMTP)
"M3AAWG Email Authentication Recommended Best Practices"
"M3AAWG Best Practices for Managing SPF Records"

この文書の最新版は他の文書と同様、M3AAWG Web サイト(www.m3aawg.org) でご確認ください。