M³AAWG 技術サマリー

メール認証 (Email Authentication)

2023 年 9 月

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

メール認証 とは：

メール認証とは、送受信システムが、メールが許可されたドメイン名サーバーから送信されたことを確認し、正しい形式で受信されたかどうかを検証するために使用する 1 つ以上の技術プロセスを指します。メール認証は、迷惑メールのフィルタリングやその他のメール処理に関する決定に役立つシグナルを生成し、場合によっては不正な送信者を特定することもあります。

広く使用されている 2 つのメール認証プロトコルは、Sender Policy Framework (SPF) と Domain Keys Identified Mail (DKIM) です。SPF と DKIM は、受信ドメインが、送信ドメインによってメッセージの送信が許可された送信者であるかどうかを確認するための情報を提供します。DKIM は、送信されたコンテンツが受信時に改ざんされていないかどうかも確認できます。

Domain-based Message, Reporting, and Conformance (DMARC)は、SPF と DKIM の上にレイヤー化されたプロトコルで、認証に失敗したメッセージをどのように処理するのが最善かを受信ドメインが判断するのに役立ちます。

メール認証が行うこと：

- メール認証は、メールメッセージにアイデンティティ（通常はドメイン名）を関連付け、そのアイデンティティがどのようにメッセージを処理したかを示す重要な情報を確認します。
- アイデンティティによって、メッセージがどのように処理されるかが決まります。例えば、ドメインの評判が悪い（頻繁にスパムに関連している）場

合、システムはそのメッセージをスパムとして分類することがあります。

- 1 つのメッセージには複数のアイデンティティが関連付けられ、それぞれが個別に認証され、メッセージ処理の指標として使用されることがあります。

メール認証が行わないこと：

- メール認証は、メッセージの内容の信頼性や質を保証したり、そのメッセージが「正当」であるかを証明したりするものではありません。
- メール認証は、メッセージを書いた実際の主体について何も言及しません。
- メール認証は、メールサーバーの設定ミスや構文エラーなど正当な理由で失敗することがあります。SPF や DKIM による認証失敗は、他の指標（DMARC など）がない限り、認証がない場合と同等であり、それ以上に悪いわけではありません。

参考資料:

RFC 6376, "DomainKeys Identified Mail (DKIM) Signatures"
RFC 7208, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1" RFC 7489, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)" "M³AAWG Email Authentication Recommended Best Practices"

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。