M³AAWG 技術サマリー

DKIM (Domain Keys Identified Mail)

2023 年 9 月

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

DKIM とは：

DKIM は、デジタル署名を使用してドメインと送信するメッセージとの関連性を確立するメール認証プロトコルです。同じドメイン名で署名された一連のメッセージは、そのドメイン名の所有者に関連する信頼性の高い情報を提供すると想定されており、この情報はドメインの評価に使用される可能性があります。

DKIM は何をするのか：

- DKIM は、DKIM-Signature ヘッダーでメッセージとドメイン名を関連付けます。DKIM-Signature ヘッダーでは複数の署名が許可されています。この関連付けは、メッセージの各部をカバーするデジタル署名を検証することで行われます。
- 受信サーバーはデジタル署名を使用して送信者の正当性を検証し、署名が作成されてからヘッダーや内容が変更されていないことを確認します。
- DKIM 署名が失敗しても、そのメッセージ評価には影響しません。署名の失敗は無視され、それ以上考慮されません。
- DKIM 署名の検証は、基本的なメール配送や、カバーされた部分が変更されていない転送では持続することがよくあります。メーリングリストは通常、DKIM 検証が失敗するような方法でメッセージを変更します。

DKIM は何をしないのか：

- DKIM は、メッセージの内容における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。
- DKIM の検証は、カバーされたヘッダーやメッセージ本体が変更されると維持されません。例えば、メーリングリストはメッセージの件名にプレフィ

ックスを追加したり、メッセージ本文にフッターを追加したりすることがあります。

- DKIM 検証の失敗は、必ずしも悪意のある活動や悪い活動を示すものではありません。

参考資料:

RFC 6376, “DomainKeys Identified Mail (DKIM) Signatures”
RFC 6377, “DomainKeys Identified Mail (DKIM) and Mailing Lists”
“M3AAWG Email Authentication Recommended Best Practices”
“M3AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability” “M3AAWG DKIM Key Rotation Best Common 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。