

DKIM では、どのような条件でどのような認証結果になりますか。

目次

[はじめに](#)

[結果](#)

[関連情報](#)

概要

この資料は DKIM のためのある特定の認証結果を生む条件を記述したものです。

結果

DomainKeys はドメインからの着信メールがそのドメインの管理者によって承認されることを確認するためにメール エクスチェンジャを受け取ることを割り当てるようにメール (DKIM) をですメールをスプーフィングすることを検出するようにメカニズムの提供によって設計されているメール 検証システム識別しました。

Cisco E メール セキュリティ アプライアンス (ESA) はオン/オフ DKIM 署名の結果および確認の後で生成できます:

DKIM シグニチャ (端を送信します)	DKIM 確認 (受電端)	結果
オン	オン	パス/Permerror/Temperror/Hardfail
オン	オフ	なし
オフ	オフ	なし
オフ	オン	中立

- 渡して下さい。メッセージは認証テストに合格しました。
- 中立。認証は実行された。
- Temperror。回復可能誤りは発生しました。
- Permerror。回復不能誤りは発生しました。
- Hardfail。失敗する認証テスト。
- ありません。メッセージは署名しませんでした。

DKIM の確認が受電端にメール フロー ポリシーの OFF である場合、DKIM 結果はメール ログで表示されません。ただし、「どれも」の結果はコンテンツ フィルターで一致することができません。

関連情報

- [AsyncOS for Email ユーザ ガイド](#)
- [GLO サポート連絡先情報](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)