

ESA はなぜ hardfail として DKIM 認証結果 permfail を処理していますか。

目次

[はじめに](#)

[ESA はなぜ hardfail として DKIM 認証結果 permfail を処理していますか。](#)

[関連情報](#)

概要

この資料は E メール セキュリティ アプライアンス (ESA) で処理する DKIM 認証結果についての詳細を記述したものです。

ESA が hardfail として DKIM 認証結果 permfail を処理する理由

イメージが下記の強調表示していると同時に ESA 内容フィルター条件 DKIM 認証に複数のオプション available があります。

DKIM Authentication

Is DKIM Authentication Passed?

DKIM Authentication Result:



状態 DKIM 認証結果が Hardfail で一致するために 設定されればメール ログファイルで permfail および下記の例に示すようにメッセージ トラッキングとして現れるメッセージが含まれています:

```
Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)
```

ESA は hardfail として permfail を考慮し、認証結果ヘッダに dkim=hardfail として結果を入れます。ESA の DKIM イベントおよび RFC6376 指名の指名間に相違点があります。認証結果ヘッダ (およびメッセージ トラッキングでコンテンツ フィルタは異なるイベント名前を使用するが) ESA は適切な RFC6376 スtringを示す必要があります。

RFC6376.PERMFAIL == ESA 内容フィルタ Hardfail のためのイベント マッピング

確認失敗の大半はシグニチャおよびメッセージ ボディ ハッシュ確認失敗が原因です。本文ハッシュ確認エラーはメッセージの本文がシグニチャのハッシュ (ダイジェスト) 値と同意しないことを示します。署名の検証エラーはシグニチャ値がメッセージの署名されたヘッダー フィールド

を (を含むシグニチャ自体) きちんと確認しないことを示します。これら二つのエラーのための複数の原因があります: メッセージは (多分メーリングリストかフォワーダによって) 送信中に修正されるかもしれませんが; シグニチャハッシュ値は署名者によって不正確に計算されるか、または適用されるかもしれませんが; 間違った公開キーの値は DNS で送達されるかもしれませんが; またはメッセージは必要とされるプライベートキーを所有してエンティティによって正しいシグニチャを計算するのにないスプーフィングされるかもしれません。原点 IP アドレスがスプーフィングの場合には有用な討論を提供するかもしれないがメッセージの分析によってこれらの原因を区別することは非常に困難です。ただし、なぜならプライバシー原因メッセージに自身アクセスできません、従ってそのよう分析は可能性のあるではないです。DNS で送達される公開キー (セレクタ) レコードの容易に避けられた Configuration エラーが理由でシグニチャが他の理由で確認しない頻繁にいくつかのメッセージ、そうなったものです。詳細については下記のリンクを参照して下さい。

関連情報

- [DKIM 確認失敗を引き起こすよくある エラーにより](#)