例外テーブルは ESA でどのように動作しますか。

目次

概要

このドキュメントでは、E メール セキュリティ アプライアンス (ESA) の例外テーブルの仕組みについて説明します。

例外テーブルは ESA でどのように動作しますか。

例外テーブルは、一部または全部のメールアドレスと 許可または拒否の 2 種類の動作を表にしたものです。 メール フロー ポリシーでは、[Use Sender Verification Exception Table] のオプションを選択する必要があります。そうしない場合は、例外テーブルは照合されません。

許可

例外テーブルで許可となっている場合、送信者の DNS 検証を省きます。 エンベロープ送信者のドメインやメールアドレスが例外テーブルに記載されている場合、エンベロープ送信者のメールアドレスのドメインネームが解決できるかにかかわらず、送信者は ESA にメールを送信できます。 **これは、送信者の DNS 検証が有効に設定され、ドメインが解決できない場合に役立ちます** (たとえば、検証できない内部ドメインやテストドメインからのメールを可能とします) 。

使用中のメールフローポリシーで送信者の DNS 検証が有効であり、エンベロープ送信者のドメインネームが解決できない (存在しない、解決できない、正しい形式でない) ときは、メッセージは拒否されます。 ここに SMTP 応答の例を示します。

```
SMTP code: 553
Message: #5.1.8 Domain of sender address <$EnvelopeSender> does not exist
```

エンベロープ送信者のメールアドレスまたはドメインが例外テーブルに許可と記載されている場合には、送信者はメッセージの残りの部分 (RCPT TO、DATA など) を続けて送ることができ、通常のメッセージの処理が進められます (メッセージ フィルタ、アンチスパム スキャンなど) 。 これにより送信者のドメインネームが検証できないメッセージをアプライアンス内で受信することが可能となります。 たとえば、次の状況では、送信者は拒否されます。

これは、拒否された送信者のログ エントリです。

```
553 #5.1.8 Domain of sender address <user@example.com> does not exist
```

@example.com を「許可」リストに追加すると、送信者は許可され、ログには以下のエントリが残されます。

```
mail from:<user@example.com>
250 sender <user@example.com> ok
```

拒否

エンベロープ送信者が例外テーブルの拒否リストに記載されている場合は、メッセージは拒否されます。 デフォルトでは、SMTP の応答は次のようになります。

```
SMTP code: 553
Message: Envelope sender <$EnvelopeSender> rejected
```

「拒否」動作のリストに user@example.com が記載されていれば、エンベロープ送信者が「user@example.com」である一切のメールは拒否されます。

```
mail from:<user@example.com>
553 Envelope sender <user@example.com> rejected
```