# 目次



# 概要

このマニュアルでは、Cisco 電子メール セキュリティ アプライアンス（ESA）での Sender Policy Framework（SPF）を使用したさまざまなシナリオを示します。

# 前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ESA
- AsyncOS のすべてのバージョン

# SPF とは何ですか。

Sender Policy Framework（SPF）は、受信側のメール エクスチェンジャで、あるドメインからの着信メールがそのドメイン管理者が承認したホストから送信されたことをチェックできるメカニズムを提供することで、電子メールのスプーフィングを検出するように設計された単純な電子メール検証システムです。 ドメインの承認済み送信元ホストのリストは特別な形式の TXT レコードの形でドメインのドメイン ネーム システム（DNS）レコードで公開されます。 電子メールのスパムおよびフィッシングは偽造した送信者アドレスを使用することが多いため、SPF レコードの公開とチェックは、アンチスパム技術と見なすことができます。

## ESA のパフォーマンスに対する多大な影響はありますか。

CPU の視点からすると、パフォーマンスへの大きな影響はありません。 ただし、SPF 検証をイネーブルにすると、DNS クエリーの数および DNS トラフィックが増加します。 ESA ではメッセージごとに 1 ~ 3 個の SPF DNS クエリーを開始しなければならない場合があり、これが DNS キャッシュの有効期限切れを早めることになります。 したがって、ESA では他のプロセス用にも、より多くのクエリーを生成することになります。

さらに、SPF レコードは通常の DNS レコードと比べて大きいと思われる .TXT レコードになり、追加の DNS トラフィックが発生する可能性があります。

## SPF はどのようにイネーブルにしますか。

次の手順の出典は、『Advance User Guide』の SPF 検証の設定に関する記述です。

デフォルト メールフロー ポリシーで SPF/System Independent Data Format（SIDF）をイネーブルにするには、次の手順に従います。

1. [Mail Policies] > [Mail Flow Policies] をクリックします。
2. [Default Policy Parameters] をクリックします。
3. デフォルトのポリシー パラメータで、[Security Features] セクションを表示します。
4. [SPF/SIDF Verification] セクションで、[Yes] をクリックします。
5. 準拠のレベルを設定します（デフォルトは SIDF 互換）。 このオプションを使用して、使用する SPF または SIDF 検証の規格を判別できます。 SIDF 準拠に加えて、SPF と SIDF を組み合わせた SIDF 互換を選択できます。
6. 準拠レベルで SIDF 互換を選択した場合は、Resent-Sender: または Resent-From: ヘッダーがメッセージにある場合に、PRA ID の結果 **Pass** を **None** に ダウングレードする かどうかを設定します。 このオプションはセキュリティを目的として選択できます。
7. SPF の準拠レベルを選択した場合は、HELO ID に対してテストを実行するかどうかを設定します。 このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。 これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。 アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

SPF 検証結果を処理するには、コンテンツ フィルタを追加してください。

1. SPF/SIDF 検証のタイプごとに spf-status コンテンツ フィルタを作成します。 命名規則を使用して、検証のタイプを示します。 たとえば、SPF/SIDF 検証に合格したメッセージには **SPF-Passed** を使用し、検証中の一時的エラーのために合格しなかったメッセージには、

SPF-TempErr を使用します。 spf-status コンテンツ フィルタの作成については、GUI の spf-status コンテンツ フィルタ ルールを参照してください。

2. 多数の SPF/SIDF 検証済みメッセージの処理後、[Monitor] > [Content Filters] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

## 「HELO テスト」のオン/オフにはどのような意味がありますか。 特定のドメインで HELO テストが失敗するとどうなりますか。

SPF の準拠レベルを選択した場合は、HELO ID に対してテストを実行するかどうかを設定します。 このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。 これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。 アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

### 有効な SPF レコード

SPF HELO チェックに合格するには、各送信側 MTA に ( ドメインとは別に ) SPF レコードを含めます。 このレコードを含めないと、HELO チェックは HELO ID に None 判定を下す可能性があります。 ドメインへの SPF 送信者が大量の None 判定を返した場合、これらの送信者は各送信側 MTA に SPF レコードを含めていない可能性があります。

このメッセージは、メッセージ フィルタまたはコンテンツ フィルタが設定されていない場合に出力されます。 同じく、すべての SPF/SIDF 判定用にメッセージ フィルタまたはコンテンツ フィルタを使用して特定のアクションを実行できます。

## 単一の外部ドメインに対してのみイネーブルにするにはどのような方法が最適ですか。

特定のドメインに対して SPF をイネーブルにするには、SPF をイネーブルにしたメール フロー ポリシーを使用して新しい送信者グループを定義する必要がある場合があります。 次に、前述のようにフィルタを作成します。

## SPF チェックをイネーブルにしてスパムの疑いを検出できますか。

Cisco Anti-Spam ではスパム スコアの計算時に多数の要因を考慮します。 検証可能な SPF レコードがあるとスパム スコアは低下することがある一方で、これらのメッセージをスパムの疑いとして検出する可能性は引き続きあります。

送信者 IP アドレスのホワイトリストを作成することや、複数の条件 ( リモート IP、メール送信元、クロススキップ スパム チェック ヘッダーなど ) によって、スパム チェックをスキップするメッセージ フィルタを作成することなどが最適な解決策として考えられます。 ヘッダーは送信サーバで追加して、あるタイプのメッセージを他のタイプのメッセージから識別できます。

## 関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems