電子メール認証

この章は、次の項で構成されています。

電子メール認証の概要

AsyncOS では、電子メールの偽造を防止するために、電子メール検証と署名をサポートします。着信メールを検証するために、AsyncOS は SPF（Sender Policy Framework）、SIDF（Sender ID Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting and Conformance）、および偽装電子メール検出をサポートします。送信メールを認証するために、AsyncOS は DomainKeys および DKIM 署名をサポートしています。

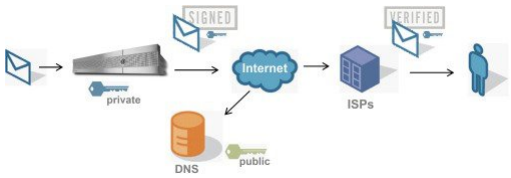
DomainKeys と DKIM 認証

DomainKeys または DKIM 電子メール認証では、送信側が公開キー暗号化を使用して、電子メールに署名します。これにより、検証済みのドメインを使用して、電子メールの From:（または Sender:）ヘッダーのドメインと比較して、偽造を検出できます。

DomainKeys と DKIM は、署名と検証の 2 つの主要部分から構成されます。AsyncOS では、DomainKeys の「署名」部分のプロセスをサポートし、DKIM の署名と検証の両方をサポートします。バウンスおよび遅延メッセージで DomainKeys および DKIM 署名を使用することもできます。

DomainKeys と DKIM 認証ワークフロー

図 *1*：認証ワーク フロー



1. 管理者（ドメイン所有者）が公開キーを DNS 名前空間にパブリッシュします。
2. 管理者は発信メール転送エージェント（MTA）に秘密キーをロードします。
3. そのドメインの権限のあるユーザによって送信される電子メールが、各秘密キーによってデジタル署名されます。署名は DomainKey または DKIM 署名ヘッダーとして電子メールに挿入され、電子メールが送信されます。
4. 受信側 MTA は、電子メールのヘッダーから DomainKeys または DKIM 署名と、要求された送信側ドメイン（Sender: または From: ヘッダーによって）を抽出します。DomainKeys または DKIM 署名ヘッダー フィールドから抽出された要求された署名ドメインから、公開キーが取得されます。
5. 公開キーは、DomainKeys または DKIM 署名が適切な秘密キーによって生成されているかどうかを確認するために使われます。

Yahoo! または Gmail アドレスを使用して、送信 DomainKeys 署名をテストできます。これらのサービスは無料で提供され、DomainKeys 署名されている着信メッセージを検証します。

AsyncOS の DomainKeys および DKIM 署名

AsyncOS の DomainKeys および DKIM 署名は、ドメイン プロファイルによって実装され、メール フロー ポリシー（一般に、発信「リレー」ポリシー）によってイネーブルにされます。詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。メッセージの署名は、メッセージ送信前にアプライアンスによって実行される最後の操作です。

ドメインプロファイルはドメインとドメインキー情報（署名キーと関連情報）を関連付けます。電子メールはアプライアンスのメールフローポリシーによって送信されるため、いずれかのドメイン プロファイルに一致する送信側電子メール アドレスは、ドメイン プロファイルに指定されている署名キーを使用して DomainKeys 署名されます。DKIM と DomainKeys の両方の署名をイネーブルにすると、DKIM 署名が使われます。DomainKeys および DKIM プロファイルは、domainkeysconfig CLI コマンドまたは GUI の [メールポリシー（Mail Policies）] > [ドメインプロファイル（Domain Profiles）] および [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページを使用して実装します。

DomainKeys および DKIM 署名は次のように機能します。ドメイン所有者はパブリック DNS（そのドメインに関連付けられた DNS TXT レコード）に格納される公開キーと、アプライアンスに格納され、そのドメインから送信されるメール（発信されるメール）の署名に使われる秘密キーの 2 つのキーを生成します。

メッセージがメッセージの送信（発信）に使われるリスナーで受信されると、アプライアンスはドメイン プロファイルが存在するかどうかを調べます。アプライアンスに作成された（およびメール フロー ポリシー用に実装された）ドメイン プロファイルが存在する場合、メッセージの有効な Sender: または From: アドレスがスキャンされます。両方が存在する場合、DomainKeys 署名および DKIM 署名には常に Sender: ヘッダーが使用され、From: ヘッダーも、DKIM 署名には使用されないものの、必要です。Sender: ヘッダーしか存在しない場合は、DomainKeys 署名または DKIM 署名のプロファイルが一致しません。From: ヘッダーは、次の場合のみ使用されます。

- Sender: ヘッダーがない。
- Web インターフェイスの [DKIMグローバル設定（DKIM Global Setting）] ページで [DKIM署名のFromヘッダーの使用（Use From Header for DKIM Signing）] オプションを選択している。

（注） AsyncOS 10.0 以降、Web インターフェイスの [DKIMグローバル設定（DKIM Global Setting）] ページで [DKIM署名へのFromヘッダーの使用（Use From Header for DKIM Signing）] オプションを選択できるようになっています。DKIM 署名に From ヘッダーを使用することが重要なのは、主に、適切な DMARC 検証のためです。

有効なアドレスが見つからない場合、メッセージは署名されず、イベントが mail_logs に記録されます。

（注） DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

有効な送信側アドレスが見つかった場合、送信側アドレスが既存のドメイン プロファイルに対して照合されます。一致しているものが見つかった場合、メッセージは署名されます。見つからない場合、メッセージは署名なしで送信されます。メッセージに既存の DomainKeys（「DomainKey-Signature:」ヘッダー）がある場合、メッセージは、元の署名の後に新しい送信側アドレスが追加されている場合にのみ、署名されます。メッセージに既存の DKIM 署名がある場合、新しい DKIM 署名がメッセージに追加されます。

AsyncOS はドメインに基づいて電子メールに署名するメカニズムに加えて、署名キーを管理する（新しいキーの作成または既存のキーの入力）方法を提供します。

このマニュアルのコンフィギュレーションの説明は、署名と検証の最も一般的な使用方法を示しています。着信電子メールのメール フロー ポリシーで DomainKeys および DKIM 署名をイネーブルにすることも、発信電子メールのメール フロー ポリシーで DKIM 検証をイネーブルにすることもできます。

（注） クラスタ環境にドメイン プロファイルと署名キーを設定する場合、[ドメイン キー プロファイル（Domain Key Profile）] 設定と [署名キー（Signing Key）] 設定がリンクしていることに注意します。そのため、署名キーをコピー、移動、または削除した場合、同じ操作が関連プロファイルに対して行われます。

DomainKeys および DKIM 署名の構成

署名キー

署名キーはアプライアンスに格納されている秘密キーです。署名キーの作成時に、キー サイズを指定します。キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性もあります。アプライアンスでは 512 ～ 2048 ビットのキーをサポートしています。768 ～ 1024 ビットのキーサイズは安全であると見なされ、現在ほとんどの送信側で使われています。大きなキーサイズに基づいたキーはパフォーマンスに影響する可能性があるため、2048 ビットを超えるキーはサポートされていません。署名キーの作成方法については、署名キーの作成または編集, （11 ページ）を参照してください。

既存のキーを入力する場合、それをフォームに貼り付けるだけです。既存の署名キーの別の使用方法は、キーをテキスト ファイルとしてインポートすることです。既存の署名キーの追加の詳細については、既存の署名キーのインポートまたは入力, （12 ページ）を参照してください。

キーを入力すると、ドメイン プロファイルで使用できるようになり、ドメイン プロファイルの [署名キー（Signing Key）] ドロップダウン リストに表示されます。

署名キーのエクスポートとインポート

署名キーをアプライアンス上のテキスト ファイルにエクスポートできます。キーをエクスポートすると、アプライアンスに現在存在するすべてのキーがテキスト ファイルに挿入されます。キーのエクスポートの詳細については、署名キーのエクスポート, （12 ページ）を参照してください。

エクスポートされたキーをインポートすることもできます。

（注） キーをインポートすると、アプライアンス上のすべての現在のキーが置き換えられます。

詳細については、既存の署名キーのインポートまたは入力, （12 ページ）を参照してください。

公開キー

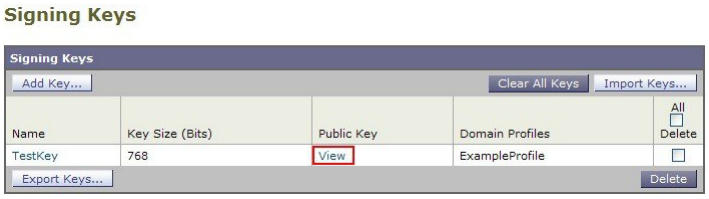
署名キーをドメイン プロファイルに関連付けると、公開キーが含まれる DNS テキスト レコードを作成できます。これは、ドメイン プロファイルのリストの [DNSテキストレコード（DNS Text

Record）] 列の [生成（Generate）] リンクから（または CLI の domainkeysconfig -> profiles -> dnstxt から）実行します。

DNS テキスト レコードの生成の詳細については、DNS テキスト レコードの生成, （14 ページ）を参照してください。

[署名キー（Signing Keys）] ページの [ビュー（View）] リンクから、公開キーを表示することもできます。

図 *2*：*[署名キー（Signing Keys）]* ページの公開キーの表示リンク



ドメイン プロファイル

ドメイン プロファイルは送信側ドメインを署名に必要なその他の情報と共に署名キーに関連付けます。

- ドメイン プロファイルの名前。
- ドメイン名（「d=」ヘッダーに含まれるドメイン）。
- セレクタ（セレクタは公開キーのクエリを形成するために使用されます。DNS クエリー タイプでは、この値が送信側ドメインの「_domainkey」名前空間の前に付けられます）。
- 正規化方法（署名アルゴリズムに提示するためにヘッダーと内容が準備される方法）。AsyncOS は DomainKeys に対して「simple」と「nofws」、DKIM に対して「relaxed」と「simple」をサポートしています。
- 署名キー（詳細については、署名キー, （4 ページ）を参照してください）。
- 署名するヘッダーのリストと本文の長さ（DKIM のみ）。
- 署名のヘッダー（DKIM のみ）に含めるタグのリスト。これらのタグは次の情報を保持します。
  - 署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。
  - 公開キーを取得するために使用されるクエリー方法のカンマ区切りリスト。
  - 署名が作成されたときのタイムスタンプ。
  - 秒による署名の有効期限。
  - 垂直バー（|）によって区切られているヘッダー フィールドのリストには、メッセージが署名された時が示されます。

- 署名（DKIM のみ）に含めるタグ。
- プロファイル ユーザのリスト（署名用にドメイン プロファイルの使用を許可されたアドレス）。

（注） プロファイル ユーザに指定されたアドレスのドメインは [ドメイン（Domain）] フィールドに指定されたドメインに一致している必要があります。

既存のすべてのドメイン プロファイルで、特定の用語を検索できます。詳細については、ドメイン プロファイルの検索，（16 ページ）を参照してください。

さらに、次のことを行うかどうか選択することができます。

- DKIM 署名を持つシステム生成メッセージへの署名
- DKIM 署名の From ヘッダーの使用

この説明については、DKIM グローバル設定の編集，（16 ページ） を参照してください。

ドメイン プロファイルのエクスポートとインポート

既存のドメインプロファイルをアプライアンス上のテキストファイルにエクスポートできます。ドメイン プロファイルをエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキスト ファイルに挿入されます。ドメイン プロファイルのエクスポート，（15 ページ）を参照してください。

以前にエクスポートしたドメインプロファイルをインポートできます。ドメインプロファイルをインポートすると、マシン上のすべての現在のドメイン プロファイルが置き換えられます。ドメイン プロファイルのインポート，（15 ページ）を参照してください。

送信メールの署名のイネーブル化

DomainKeys および DKIM 署名は発信メールのメール フロー ポリシーでイネーブルにします。詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

ステップ 1 [メール フロー ポリシー（Mail Flow Policies）] ページ（[メール ポリシー（Mail Policies）] メニューから）で、[リレー（RELAYED）] メール フロー ポリシー（送信）をクリックします。

ステップ 2 [セキュリティ サービス（Security Features）] セクションから、[オン（On）] を選択して、[DomainKeys/DKIM 署名（DomainKeys/DKIM Signing）] をイネーブルにします。

ステップ 3 変更を送信し、保存します。

バウンスおよび遅延メッセージの署名のイネーブル化

発信メッセージに署名するだけでなく、バウンスおよび遅延メッセージに署名したい場合があります。これにより、会社から受信するバウンスおよび遅延メッセージが正当なものであることを受信者に警告したい場合があります。バウンスおよび遅延メッセージのDomainKeysおよびDKIM署名をイネーブルにするには、公開リスナーに関連付けられたバウンス プロファイルのDomainKeys/DKIM 署名をイネーブルにします。

ステップ 1 署名された発信メッセージを送信する公開リスナーに関連付けられているバウンスプロファイルで、[ハード バウンスと遅延警告メッセージ（Hard Bounce and Delay Warning Messages）] に移動します。

ステップ 2 [バウンスおよび遅延メッセージに対してドメインキー署名を使用（Use Domain Key Signing for Bounce and Delay Messages）] をイネーブルにします。

（注） バウンスおよび遅延メッセージに署名するには、DomainKeys/DKIM 署名の設定（GUI），（8ページ）に示されたすべての手順を完了している必要があります。

ドメイン プロファイルの [差出人：（From:）] アドレスは、バウンス返信アドレスに使用されているアドレスと一致している必要があります。これらのアドレスを一致させるには、バウンス プロファイルの返信アドレスを設定し（[システム管理（System Administration）] > [返信先アドレス（Return Addresses）]）、ドメイン プロファイルの [ユーザのプロファイリング（Profile Users）] リストで同じ名前を使用します。たとえば、バウンス返信アドレスにMAILER-DAEMON@example.com の返信アドレスを設定し、ドメイン プロファイルにプロファイル ユーザとして MAILER-DAEMON@example.com を追加します。

DomainKeys/DKIM 署名の設定（GUI）

ステップ 1 新規の秘密キーを作成するか、既存の秘密キーをインポートします。署名キーの作成またはインポートについては、署名キー，（4 ページ）を参照してください。

ステップ 2 ドメイン プロファイルを作成し、キーをドメイン プロファイルに関連付けます。ドメイン プロファイルの作成については、ドメイン プロファイル，（5 ページ）を参照してください。

ステップ 3 DNS テキスト レコードを作成します。DNS テキスト レコードの作成については、DNS テキスト レコードの生成，（14 ページ）を参照してください。

ステップ 4 発信メールのメール フロー ポリシーで、DomainKeys/DKIM 署名をまだイネーブルにしていない場合は、イネーブルにします（送信メールの署名のイネーブル化，（6 ページ）を参照してください）。

ステップ 5 任意で、バウンスおよび遅延メッセージの DomainKeys/DKIM 署名をイネーブルにします。バウンスおよび遅延メッセージの署名のイネーブル化については、バウンスおよび遅延メッセージの署名のイネーブル化，（7 ページ）を参照してください。

ステップ 6 電子メールを送信します。ドメイン プロファイルに一致するドメインから送信されたメールは DomainKeys/DKIM 署名されます。さらに、バウンスおよび遅延メッセージの署名を設定した場合は、バウンスまたは遅延メッセージに署名されます。

（注） DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

DomainKeys 署名のドメイン プロファイルの作成

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profile）] セクションで、[プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します

ステップ 4 [ドメインキータイプ（Domain Key Type）] については、[ドメインキー（Domain Keys）] を選択します。新しいオプションがページに表示されます。

ステップ 5 ドメイン名を入力します。

ステップ 6 セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間

と電子メールヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 7 正規化（[no forwarding whitespaces] または [simple]）を選択します。

ステップ 8 すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。署名キーの作成または編集, （11 ページ）を参照してください。

ステップ 9 署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

ステップ 10 変更を送信し、保存します。

ステップ 11 この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化, （6 ページ）を参照してください）。

（注） DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

DKIM 署名の新しいドメイン プロファイルの作成

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profile）] セクションで、[プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します

ステップ 4 [ドメインキータイプ（Domain Key Type）] に対して、[DKIM] を選択します。
新しいオプションがページに表示されます。

ステップ 5 ドメイン名を入力します。

ステップ 6 セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メールヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 7 ヘッダーの正規化を選択します。次のオプションから選択します。

- [Relaxed]。 「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。ヘッダー名を小文字に変更し、ヘッダーを展開して、連続した空白を 1 つの空白に短縮し、先頭と末尾の空白を取り除きます。
- [Simple]。 ヘッダーは変更されません。

ステップ 8 本文の正規化を選択します。次のオプションから選択します。

- [Relaxed]。 「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。本文末尾の空の行を取り除き、行中の空白を 1 つの空白に短縮し、行の末尾の空白を取り除きます。
- [Simple]。本文末尾の空の行を取り除きます。

ステップ 9 すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。署名キーの作成または編集, （11 ページ）を参照してください。

ステップ 10 署名するヘッダーのリストを選択します。次のヘッダーから選択できます。

- [すべて（All）]。 AsyncOS は署名時に存在するすべてのヘッダーに署名します。送信中にヘッダーの追加や削除が予想されない場合は、すべてのヘッダーに署名することが考えられます。
- [標準（Standard）]。 送信中にヘッダーの追加や削除が予想される場合は、標準ヘッダーを選択することが考えられます。AsyncOS は次の標準ヘッダーにのみ署名します（メッセージにそのヘッダーが存在しない場合、DKIM 署名は、そのヘッダーにヌル値を示します）。
  - 送信元（From）
  - Sender、Reply To-
  - Subject
  - Date、Message-ID
  - To、Cc
  - MIME-Version
  - Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
  - Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
  - In-Reply-To、References
  - List-Id、List-Help、List-Unsubscribe、LIst-Subscribe、List-Post、List-Owner、List-Archive

（注） [標準（Standard）] を選択した場合、署名するヘッダーを追加できます。

ステップ 11 メッセージ本文に署名する方法を指定します。メッセージ本文に署名するか、署名するバイト数を選択できます。次のオプションのいずれかを選択します。

- [本文全体を含む（Whole Body Implied）]。本文の長さを判断するために「l=」タグを使用しないでください。メッセージ全体に署名し、変更を許可しません。
- [本文全体を自動判断（Whole Body Auto-determined）]。メッセージ本文全体に署名し、送信中に本文の末尾へのデータの追加を許可します。
- [最初に署名 _ バイト（Sign first _ bytes）]。指定したバイト数まで、メッセージ本文に署名します。

ステップ 12 メッセージ署名のヘッダーフィールドに含めるタグを選択します。これらのタグに格納されている情報はメッセージ署名の検証に使用されます。次のオプションから 1 つ以上を選択します。

- ["i" タグ]。署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。ドメイン @example.com など、@記号が付加されたドメイン名を入力します。

- ["q" タグ]。公開キーを取得するために使用されるクエリー方法のコロン区切りリスト。現在、唯一有効な値は dns/txt です。
- ["t" タグ]。署名が作成されたときのタイムスタンプを表示します。
- ["x" タグ]。署名が終了する絶対的な日時。署名の有効期限（秒単位）を指定します。デフォルトは 31536000 秒です。
- ["z" タグ]。垂直バー（|）によって区切られているヘッダー フィールドのリストには、メッセージが署名された時が示されます。これには、ヘッダー フィールドの名前と値が含まれます。次に例を示します。

z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700

ステップ 13 署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

（注） ドメイン プロファイルを作成する場合、特定のユーザに関連付けるプロファイルの決定において、階層を使用することに注意してください。たとえば、example.com のプロファイルと joe@example.com の別のプロファイルを作成するとします。joe@example.com からメールが送信される場合、joe@example.com のプロファイルが使われます。しかし、メールが adam@example.com から送信される場合は、example.com のプロファイルが使われます。

ステップ 14 変更を送信し、保存します。

ステップ 15 この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化, （6ページ）を参照してください）。

（注） DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

署名キーの作成または編集

新しい署名キーの作成

署名キーは DomainKeys および DKIM 署名のドメイン プロファイルに必要です。

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。

ステップ 2 [キーを追加（Add Key）] をクリックします。

ステップ 3 キーの名前を入力します。

ステップ 4 [生成（Generate）] をクリックし、キー サイズを選択します。

ステップ 5 変更を送信し、保存します。

（注） キーを割り当てるドメイン プロファイルを編集していない場合は、編集する必要がある場合があります。

既存の署名キーの編集

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。

ステップ 2 目的の署名キーをクリックします。

ステップ 3 新しい署名キーの作成，（11 ページ）の説明に従って、目的のフィールドを編集します。

（注） セキュリティ強化のため、FIPS モードでアプライアンス内での機密データの暗号化をイネーブルにすると、秘密キーを表示できなくなります。秘密キーを編集する場合は、秘密キーを貼り付けるか、または新しい秘密キーを作成します。

ステップ 4 変更を送信し、保存します。

署名キーのエクスポート

アプライアンスのすべてのキーは、1 つのテキスト ファイルとしてエクスポートされます。

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。

ステップ 2 [キーをエクスポート（Export Keys）] をクリックします。

（注） セキュリティ強化のため、FIPS モードでアプライアンス内での機密データの暗号化をイネーブルにすると、エクスポート中に署名キーが暗号化されます。

ステップ 3 ファイルの名前を入力し、[送信（Submit）] をクリックします。

既存の署名キーのインポートまたは入力

キーの貼り付け

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。

ステップ 2 [キーを追加（Add Key）] をクリックします。

ステップ 3 [貼り付けキー（Paste Key）] フィールドにキーを貼り付けます（PEM フォーマットされ、RSA キーのみである必要があります）。

ステップ 4 変更を送信し、保存します。

既存のエクスポート ファイルからのキーのインポート

（注） キーファイルを取得するには、署名キーのエクスポート，（12ページ）を参照してください。

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [キーをインポート（Import Keys）] をクリックします。
ステップ 3 エクスポートされた署名キーを含むファイルを選択します。
ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存の署名キーが置き換えられることが警告されます。テキスト ファイルのすべてのキーがインポートされます。
ステップ 5 [インポート（Import）] をクリックします。

署名キーの削除

選択した署名キーの削除

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 削除する各署名キーの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべての署名キーの削除

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [署名キー（Signing Keys）] ページの [すべてのキーを消去（Clear All Keys）] をクリックします。
ステップ 3 削除を確認します。

DNS テキスト レコードの生成

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profiles）] セクションの [DNSテキストレコード（DNS Text Record）] 列で、対応するドメイン プロファイルの [生成（Generate）] リンクをクリックします。

ステップ 3 DNS テキスト レコードに含める属性のチェックボックスをオンにします。

ステップ 4 [再生成（Generate Again）] をクリックして、変更を含めてキーを再生成します。

ステップ 5 DNS テキスト レコードがウィンドウの下部のテキスト フィールド（コピーできます）に表示されます。場合によっては、複数の文字列の DNS テキスト レコードが生成されます。複数の文字列の DNS テキスト レコード, （14 ページ）を参照してください。

ステップ 6 [完了（Done）] をクリックします。

複数の文字列の DNS テキスト レコード

DNS テキスト レコードの生成に使用される署名キーのサイズが 1024 ビットより大きい場合は、複数の文字列の DNS テキスト レコードが生成されることがあります。これは、DNS テキスト レコードの単一の文字列に含めることができるのは、255 文字以下であるためです。一部の DNS サーバでは複数の文字列の DNS テキスト レコードが受け入れられないか、実行されないため、DKIM 認証は失敗する可能性があります。

このシナリオを回避するために、二重引用符を使用して、複数の文字列の DNS テキスト レコードを、255 バイト未満の文字列に分割することを推奨します。次に、例を示します。

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVXlIXFT7OEl81amoZLbvwMX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoi"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74BVm+16Xq2mptWXEwpiwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTj1i4"
"mQg48yCD/HVNfsSRXaPinliEkypH9cSnvgvWuIYUQz0dHU;"
```

このようにして分割された DNS テキスト レコードが、DKIM 実装により、処理前に元の単一の文字列に再構築されます。

ドメイン プロファイルのテスト

署名キーを作成し、それをドメインプロファイルに関連付け、DNSテキストを生成して、権限のある DNS に挿入したら、ドメイン プロファイルをテストできます。

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profiles）] セクションの [テストプロファイル（Test Profile）] 列で、ドメイン プロファイルの [テスト（Test）] リンクをクリックします。

ステップ 3 成功または失敗を示すメッセージがページの上部に表示されます。テストが失敗した場合、エラーテキストを含む警告メッセージが表示されます。

ドメイン プロファイルのエクスポート

アプライアンスのすべてのドメインプロファイルは、単一のテキストファイルにエクスポートされます。

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメインプロファイルのエクスポート（Export Domain Profiles）] をクリックします。

ステップ 3 ファイルの名前を入力し、[送信（Submit）] をクリックします。

ドメイン プロファイルのインポート

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメインプロファイルのインポート（Import Domain Profiles）] をクリックします。

ステップ 3 エクスポートされたドメイン プロファイルを含むファイルを選択します。

ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存のドメインプロファイルが置き換えられることが警告されます。テキスト ファイルのすべてのドメイン プロファイルがインポートされます。

ステップ 5 [インポート（Import）] をクリックします。

ドメイン プロファイルの削除

ドメイン プロファイルの削除

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 削除する各ドメイン プロファイルの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべてのドメイン プロファイルの削除

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 [すべて消去（Clear All）] をクリックします。
ステップ 3 削除を確認します。

ドメイン プロファイルの検索

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 [ドメインプロファイルの検索（Find Domain Profiles）] セクションで、検索条件を指定します。
ステップ 3 [プロファイルの検索（Find Profiles）] をクリックします。
ステップ 4 検索では、各ドメイン プロファイルの email、domain、selector、signing key name のフィールドがスキャンされます。

（注） 検索語を入力しない場合、検索エンジンはすべてのドメイン プロファイルを返します。

DKIM グローバル設定の編集

DKIM のグローバル設定を使用して、次のことを行うかどうかを選択できます。

- DKIM 署名でシステムによって生成されたメッセージに署名します。アプライアンスは次のメッセージに署名します。
  - Cisco IronPort スパム隔離通知

- コンテンツ フィルタで生成された通知
- 設定メッセージ
- サポート リクエスト

- DKIM 署名の From ヘッダーの使用

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [DKIMグローバル設定（DKIM Global Settings）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 要件に応じて、次のフィールドを設定します。

- システム生成メッセージのDKIM署名（DKIM Signing of System Generated Messages）
- DKIM 署名の From ヘッダーの使用

（注） DKIM 署名に From ヘッダーを使用していない場合、または有効な From ヘッダーが存在しない場合は、Sender ヘッダーが使用されます。DKIM 署名済みメッセージの DMARC 検証の場合、DKIM 署名中は From ヘッダーを使用する必要があります。

ステップ 4 変更を送信し、保存します。

ドメイン キーとロギング

DomainKeys 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

DKIM 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

DKIM を使用した受信メッセージの検証方法

DKIM を使用した受信メッセージの検証方法

	操作内容	詳細（More Info）
ステップ 1	DKIM を使用してメッセージを検証するプロファイルを作成します。	DKIM 検証プロファイルの作成，（20 ページ）
ステップ 2	（任意）DKIM を使用した受信メッセージの検証に使用されるカスタムのメールフローポリシーを作成します。	メール フロー ポリシーを使用した着信メッセージのルールの定義
ステップ 3：	DKIM を使用して受信メッセージを検証するようにメールフローポリシーを設定します。	メール フロー ポリシーでの DKIM 検証の設定，（22 ページ）
ステップ 4：	E メール セキュリティ アプライアンスが確認されたメッセージで実行するアクションを定義します。	DKIM 検証済みメールのアクションの設定，（23 ページ）
ステップ 5：	特定の送信者または受信者のグループにアクションを関連付けます。	メール ポリシーの設定

AsyncOS による DKIM 検証チェック

DKIM 検証用に AsyncOS アプライアンスを設定すると、次のチェックが実行されます。

ステップ 1 AsyncOS は受信メールの [DKIMシグネチャ（DKIM-Signature）] フィールド、署名ヘッダーの構文、有効なタグ値、必須タグを調べます。署名がこれらのいずれかのチェックで失敗すると、AsyncOS は *permfail* を返します。

ステップ 2 署名チェックの実行後、公開 DNS レコードから公開キーが取得され、TXT レコードが検証されます。このプロセス中にエラーが検出されると、AsyncOS は *permfail* を返します。公開キーの DNS クエリーで応答を取得できない場合、*tempfail* が発生します。

ステップ 3 公開キーの取得後、AsyncOSはハッシュ値をチェックし、署名を検証します。この手順中にエラーが発生すると、AsyncOS は *permfail* を返します。

ステップ 4 チェックにすべて合格すると、AsyncOS は *pass* を返します。

（注） メッセージ本文が指定された長さより長い場合、AsyncOS は次の判定を返します。

```
dkim = pass (partially verified [x bytes])
```

ここで *X* は検証されたバイト数を表します。

最終検証結果は、*Authentication-Results* ヘッダーとして入力されます。たとえば、次のいずれかのようなヘッダーを受け取ることがあります。

```
Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (signature verified)
```

```
Authentication-Results: example1.com
header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])
Authentication-Results: example1.com
header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

（注） 現在の DKIM 検証は最初の有効な署名で停止します。最後に検出された署名を使用して、検証できません。この機能は、後のリリースで使用できるようになる可能性があります。

ドメインに DKIM テスト モードでその DNS TXT レコードがあるとき（t=y）、アプライアンスは DKIM 検証と操作を完全にスキップします。

DKIM 検証プロファイルの管理

DKIM 検証プロファイルは E メール セキュリティ アプライアンスのメール フロー ポリシーが DKIM 署名を保証するために使用されるパラメータのリストです。たとえば、クエリーがタイムアウトする前に 30 秒取る検証プロファイルと、クエリーがタイムアウトする前に 3 秒だけ取る検証プロファイルの、2 つの検証プロファイルを作成できます。THROTTLED メール フロー ポリシーに 2 つ目の検証プロファイルを割り当てて、DDoS の場合の接続スタベーションを防止できます。検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- 許容できる公開キーの最小、最大サイズ。デフォルトのキーのサイズは 512 および 2048 です。
- メッセージの中で検証できる署名の最大数。メッセージに定義した署名の最大数よりも多くの署名がある場合、アプライアンスは残りの署名の検証をスキップし、メッセージの処理を続行します。デフォルトは、5 つの署名です。
- 送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差（秒単位）。たとえば、メッセージ署名が 05:00:00 に期限切れとなり、検証者のシステム時刻が 05:00:30 である場合、時間の許容差が 60 秒であればメッセージ署名は有効なままですが、許容差が 10 秒であれば無効になります。デフォルトは 60 秒です。
- 本文の長さのパラメータを使用するかどうかを指定するオプション。
- 一時的な障害の場合に実行する SMTP アクション。
- 永続的な障害の場合に実行する SMTP アクション。

プロファイル名ですべての既存の検証プロファイルを検索できます。

アプライアンスのコンフィギュレーション ディレクトリに DKIM 検証プロファイルをテキスト ファイルとしてエクスポートできます。検証プロファイルをエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキスト ファイルに挿入されます。詳細については、DKIM 検証プロファイルのエクスポート，（21 ページ）を参照してください。

以前エクスポートした DKIM 検証プロファイルをインポートできます。DKIM 検証プロファイルをインポートすると、マシンの現在のすべての DKIM 検証プロファイルを置き換えることになります。詳細については、DKIM 検証プロファイルのインポート，（21 ページ）を参照してください。

DKIM 検証プロファイルの作成

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] をクリックします。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 アプライアンスが許可する署名キーの最小キー サイズを選択します。

ステップ 5 アプライアンスが許可する署名キーの最大キー サイズを選択します。

ステップ 6 1 つのメッセージで検証する署名の最大数を選択します。デフォルトは 5 つの署名です。

ステップ 7 キー クエリーがタイムアウトするまでの時間（秒）を選択します。デフォルトは 10 秒です。

ステップ 8 送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差（秒単位）を選択します。デフォルトは 60 秒です。

ステップ 9 メッセージの検証に、署名の本文の長さのパラメータを使用するかどうか選択します。

ステップ 10 署名を確認するときに一時的な障害がある場合、E メール セキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 11 署名を確認するときに永続的な障害がある場合は、E メール セキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 12 変更を送信します。
新しいプロファイルが DKIM 検証プロファイルのテーブルに表示されます。

ステップ 13 変更を保存します。

ステップ 14 この時点で着信メール フロー ポリシーで DKIM 検証をイネーブルにし、使用する検証プロファイルを選択する必要があります。

DKIM 検証プロファイルのエクスポート

アプライアンスのすべての DKIM 検証プロファイルは単一のテキスト ファイルとしてエクスポートされ、アプライアンスの configuration ディレクトリに保存されます。

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [プロファイルをエクスポート（Export Profiles）] をクリックします。
ステップ 3 ファイルの名前を入力し、[送信（Submit）] をクリックします。

DKIM 検証プロファイルのインポート

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [プロファイルをインポート（Import Profiles）] をクリックします。
ステップ 3 DKIM 検証プロファイルを含むファイルを選択します。
ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存の DKIM 検証プロファイルが置き換えられることが警告されます。
ステップ 5 [インポート（Import）] をクリックします。

DKIM 検証プロファイルの削除

選択した DKIM 検証プロファイルの削除

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 削除する各 DKIM 検証プロファイルの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべての DKIM 検証プロファイルの削除

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [すべて消去（Clear All）] をクリックします。
ステップ 3 削除を確認します。

DKIM 検証プロファイルの検索

すべての DKIM 検証プロファイルについてプロファイル名から特定の用語を検索します。

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [次のDKIM検証プロファイルを検索（Search DKIM Verification Profiles）] セクションで、検索条件を指定します。
ステップ 3 [プロファイルの検索（Find Profiles）] をクリックします。
検索では、各 DKIM 検証プロファイル名をスキャンします。

検索語を入力しない場合、検索エンジンはすべての DKIM 検証プロファイルを返します。

メール フロー ポリシーでの DKIM 検証の設定

DKIM 検証は、受信メールのメール フロー ポリシーでイネーブルにします。

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。
ステップ 2 検証を実行するリスナーの着信メール ポリシーをクリックします。
ステップ 3 メール フロー ポリシーの [セキュリティサービス（Security Features）] セクションで、[オン（On）] を選択して、[DKIM検証（DKIM Verification）] をイネーブルにします。
ステップ 4 ポリシーで使用する DKIM 検証プロファイルを選択します。
ステップ 5 変更を保存します。

DKIM 検証とロギング

DKIM 検証時には、次のような行がメール ログに追加されます。

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature

mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

DKIM 検証済みメールのアクションの設定

DKIM メールを検証すると、メールに Authentication-Results ヘッダーが追加されますが、認証結果に関係なく、メールは受け入れられます。これらの認証結果に基づいてアクションを設定するには、コンテンツ フィルタを作成して、DKIM 検証済みメールに対するアクションを実行します。たとえば、DKIM 検証が失敗した場合、メールを配信、バウンス、ドロップ、または隔離エリアに送るように設定することができます。これを実行するには、コンテンツ フィルタを使用して、アクションを設定する必要があります。

ステップ 1 [メールポリシー（Mail Policies）] > [着信フィルタ（Incoming Filters）] を選択します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 条件のリストから [DKIM認証（DKIM Authentication）] を選択します。

ステップ 5 DKIM 条件を選択します。次のオプションのいずれかを選択します。

- [Pass]。メッセージは認証テストに合格しました。
- [Neutral]。認証が実行されませんでした。
- [Temperror]。 修復可能なエラーが発生しました。
- [Permerror]。 修復不可能なエラーが発生しました。
- [Hardfail]。 認証テストが失敗しました。
- [None]。 メッセージは署名されていません。

ステップ 6 条件に関連付けるアクションを選択します。たとえば、DKIM 検証が失敗した場合、受信者に通知し、メッセージをバウンスさせることができます。または DKIM 検証に合格した場合、それ以上処理せずに、メッセージをすぐに配信することができます。

ステップ 7 新しいコンテンツ フィルタを送信します。

ステップ 8 適切な受信メール ポリシーでコンテンツ フィルタをイネーブルにします。

ステップ 9 変更を保存します。

SPF および SIDF 検証の概要

AsyncOS は、Sender Policy Framework（SPF）および Sender ID Framework（SIDF）検証をサポートしています。SPF と SIDF は DNS レコードに基づいて電子メールの信頼性を検証する方法です。SPF と SIDF により、インターネット ドメインの所有者は、特別な形式の DNS TXT レコードを使用して、そのドメインに電子メールを送信する権限のあるマシンを指定することができます。準拠したメール受信側は、パブリッシュされた SPF レコードを使用して、メール トランザクション中に、送信側のメール転送エージェントの ID の権限をテストします。

SPF/SIDF 認証を使用すると、送信側はそれらの名前の使用が許可されるホストを指定する SPF レコードをパブリッシュし、準拠するメール受信側はパブリッシュされた SPF レコードを使用して、メール トランザクション中に送信側のメール転送エージェントの ID の権限をテストします。

（注） SPF チェックでは、解析と評価が必要であるため、AsyncOS のパフォーマンスに影響する場合があります。さらに、SPF チェックによって、DNS インフラストラクチャの負荷が増えることに注意してください。

SPF と SIDF を操作する場合、SIDF は SPF に似ていますが、いくつかの違いがあります。SIDF と SPF の違いに関する詳しい説明については、RFC 4406 を参照してください。このマニュアルの目的のため、この 2 つの用語は、1 つのタイプの検証のみを適用する場合を除いて、まとめて説明しています。

（注） AsyncOS は着信リレーに対して SPF をサポートしていません。

有効な SPF レコードに関する注意

アプライアンスで SPF および SIDF を使用するには、RFC 4406、4408 および 7208 に従って、SPF レコードをパブリッシュします。PRA ID の決定方法の定義については、RFC 4407 を確認してください。さらに、SPF レコードと SIDF レコードを作成する場合に犯しやすい誤りについては、次の Web サイトを参照してください。

http://www.openspf.org/FAQ/Common_mistakes

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）「v=spf1 a –all」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 送信側が大量の None 判定を返した場合、これらの送信側は各送信側 MTA に「v=spf1 a –all」SPF レコードを含めていない可能性があります。

有効な SIDF レコード

SIDF フレームワークをサポートするには、「v=spf1」レコードと「spf2.0」レコードの両方をパブリッシュする必要があります。たとえば、DNS レコードは次の例のようになります。

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF は HELO ID を検証しないため、この場合、各送信側 MTA に SPF v2.0 レコードをパブリッシュする必要はありません。

（注） SIDF をサポートしない場合は、「spf2.0/pra ~all」レコードをパブリッシュします。

SPF レコードのテスト

RFC の確認に加えて、E メール セキュリティ アプライアンスに SPF 検証を実装する前に、SPF レコードをテストすることを推奨します。openspf.org Web サイトでは、いくつかのテスト ツールが提供されています。

http://www.openspf.org/Tools

次のツールを使用して、電子メールが SPF レコード チェックに失敗した理由を判断できます。

http://www.openspf.org/Why

さらに、テスト リスナーで SPF をイネーブルにし、シスコの trace CLI コマンドを使用して（または GUI からトレースを実行して）、SPF 結果を表示できます。トレースを使用すると、さまざまな送信側 IP を簡単にテストできます。

SPF/SDIF を使用した受信メッセージの検証方法

	操作内容	詳細（More Info）
ステップ 1	（任意）SPF/SDIF を使用した受信メッセージの検証に使用されるカスタムのメール フロー ポリシーを作成します。	メール フロー ポリシーを使用した着信メッセージのルールの定義
ステップ 2	SPF/SDIF を使用して受信メッセージを検証するようにメール フロー ポリシーを設定します。	SPF と SIDF のイネーブル化, （26 ページ）
ステップ 3：	E メール セキュリティ アプライアンスが確認されたメッセージで実行するアクションを定義します。	SPF/SIDF 検証済みメールに対して実行するアクションの決定, （30 ページ）

	操作内容	詳細（More Info）
ステップ 4：	特定の送信者または受信者のグループにアクションを関連付けます。	メール ポリシーの設定
ステップ 5：	（任意）メッセージの検証の結果をテストします。	SPF/SIDF 結果のテスト，（33 ページ）

注意 シスコでは、グローバルな電子メール認証を強く奨励していますが、業界での採用途上にある現時点では、SPF/SIDF 認証の失敗に対して慎重な処理を行うよう提案しています。さらに多くの組織で社内公認のメール送信インフラストラクチャの制御能力が向上するまでは、シスコは電子メールのバウンスを回避し、代わりに SPF/SIDF 検証に失敗した電子メールを隔離できます。

（注） AsyncOS コマンドライン インターフェイス（CLI）では、Web インターフェイスよりも詳細な SPF レベルの制御設定を提供しています。SPF 判定に基づいて、アプライアンスは、リスナー単位で SMTP カンバセーションにおいてメッセージを許可または拒否できます。SPF の設定は、listenerconfig コマンドを使用してリスナーのホスト アクセス テーブルのデフォルト設定を編集するときに変更できます。設定の詳細については、CLI を使用した SPF および SIDF のイネーブル化，（27 ページ）を参照してください。

SPF と SIDF のイネーブル化

SPF/SIDF を使用するには、受信リスナーでメール フロー ポリシーの SPF/SIDF をイネーブルにする必要があります。デフォルトのメール フロー ポリシーから、リスナーで SPF/SIDF をイネーブルにするか、特定の受信メール ポリシーについて SPF/SIDF をイネーブルにすることができます。

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policy）] を選択します。

ステップ 2 [デフォルトポリシーパラメータ（Default Policy Parameters）] をクリックします。

ステップ 3 デフォルトのポリシー パラメータで、[セキュリティサービス（Security Features）] セクションを表示します。

ステップ 4 [SPF/SIDF検証（SPF/SIDF Verification）] セクションで、[オン（On）] をクリックします。

ステップ 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 検証の規格を判断できます。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
SPF/SIDF 準拠レベル

準拠レベル	説明
SPF	SPF/SIDF 検証は RFC4408 および RFC7208 に従って動作します。 - PRA（Purported Responsible Address）ID 検証は行われません。 注：HELO ID に対してテストするには、この準拠オプションを選択します。
SIDF	SPF/SIDF 検証は RFC4406 に従って動作します。 - PRA ID は規格への完全準拠によって判断されます。 - SPF v1.0 レコードは spf2.0/mfrom,pra として扱われます。 - 存在しないドメインや形式が誤った ID については、Fail の判定が返されます。
SIDF 互換（SIDF Compatible）	SPF/SIDF 検証は、次の違いを除き、RFC4406 に従って動作します。 - SPF v1.0 レコードは spf2.0/mfrom として扱われます。 - 存在しないドメインや形式が誤った ID については、None の判定が返されます。 注：この準拠オプションは、OpenSPF コミュニティ（www.openspf.org）の要求に応じて導入されました。

（注） CLI からはさらに多くの設定を使用できます。詳細については、CLI を使用した SPF および SIDF のイネーブル化, （27 ページ）を参照してください。

ステップ 6 SIDF 互換の準拠レベルを選択した場合、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうかを設定します。このオプションをセキュリティ目的で選択できます。

ステップ 7 SPF の準拠レベルを選択した場合、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。

CLI を使用した SPF および SIDF のイネーブル化

AsyncOS CLI では各 SPF/SIDF 準拠レベルのより詳細な制御設定をサポートしています。リスナーのホストアクセステーブルのデフォルトの設定をする場合、リスナーの SPF/SIDF 準拠レベルと、アプライアンスが SPF/SIDF 検証結果に基づいて実行する SMTP アクション（ACCEPT または REJECT）を選択できます。アプライアンスがメッセージを拒否する場合に送信する SMTP 応答を定義することもできます。

準拠レベルに応じて、アプライアンスは HELO ID、MAIL FROM ID、または PRA ID に対してチェックを実行します。アプライアンスが、次の各 ID チェックの各 SPF/SIDF 検証結果に対し、セッションを続行する（ACCEPT）か、セッションを終了する（REJECT）かを指定できます。

- [None]。情報の不足のため、検証を実行できません。
- [Neutral]。ドメイン所有者は、クライアントに指定されたIDを使用する権限があるかどうかをアサートしません。
- [SoftFail]。ドメイン所有者は、ホストが指定されたIDを使用する権限がないと思うが、断言を避けたいと考えています。
- [失敗]：クライアントは、指定された ID でメールを送信する権限がありません。
- [TempError]。検証中に一時的なエラーが発生しました。
- [Permerror]。検証中に永続的なエラーが発生しました。

アプライアンスは、メッセージにResent-Sender:またはResent-From:ヘッダーが存在する場合に、PRA ID の Pass 結果を None にダウングレードするように SIDF 互換準拠レベルを設定していない限り、Pass 結果のメッセージを受け入れます。アプライアンスは PRA チェックで None が返された場合に指定された SMTP アクションを実行します。

IDチェックに対してSMTPアクションを定義していない場合、アプライアンスはFailを含むすべての検証結果を自動的に受け入れます。

イネーブルにされたいずれかのIDチェックのID検証結果がREJECTアクションに一致する場合、アプライアンスはセッションを終了します。たとえば、管理者は、すべてのHELO IDチェック結果に基づいてメッセージを受け入れるようにリスナーを設定しますが、MAIL FROM ID チェックからの Fail 結果に対してはメッセージを拒否するようにリスナーを設定するとします。メッセージがHELO IDチェックに失敗しても、アプライアンスはその結果を受け入れるため、セッションが続行します。次に、メッセージが MAIL FROM ID チェックで失敗した場合、リスナーはセッションを終了し、REJECT アクションの STMP 応答を返します。

SMTP応答は、アプライアンスがSPF/SIDF検証結果に基づいてメッセージを拒否する場合に返すコード番号とメッセージです。TempError結果は、他の検証結果と異なるSMTP応答を返します。TempErrorの場合、デフォルトの応答コードは451で、デフォルトのメッセージテキストは「`#4.4.3 Temporary error occurred during SPF verification`」です。他のすべての検証結果では、デフォルトの応答コードは550で、デフォルトのメッセージテキストは「`#5.7.1 SPF unauthorized mail is prohibited`」です。TempError や他の検証結果に独自の応答コードとメッセージ テキストを指定できます。

任意で、Neutral、SoftFail、または Fail 検証結果に対して REJECT アクションが実行された場合に、SPF パブリッシャ ドメインから、サードパーティの応答を返すように、アプライアンスを設定することができます。デフォルトで、アプライアンスは次の応答を返します。

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>
```

これらの SPF/SIDF 設定をイネーブルにするには、`listenerconfig -> edit` サブコマンドを使用し、リスナーを選択します。次に、`hostaccess -> default` サブコマンドを使用して、ホスト アクセス テーブルのデフォルトの設定を編集します。

ホスト アクセス テーブルでは、次の SPF 制御設定を使用できます。

CLI を使用した SPF 制御設定

準拠レベル	使用可能な SPF 制御設定
SPF のみ（SPF Only）	• HELO ID チェックを実行するかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション ◦ HELO ID（イネーブルの場合） ◦ MAIL FROM ID • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 互換（SIDF Compatible）	• HELO ID チェックを実行するかどうか • メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション ◦ HELO ID（イネーブルの場合） ◦ MAIL FROM ID ◦ PRA Identity • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 厳格（SIDF Strict）	• 次の ID チェックの結果に基づいて実行される SMTP アクション ◦ MAIL FROM ID ◦ PRA Identity • SPF REJECT アクションの場合に返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

アプライアンスは HELO ID チェックを実行し、None および Neutral 検証結果を受け入れ、その他の結果を拒否します。SMTP アクションの CLI プロンプトはすべての ID タイプで同じです。ユー

ザは MAIL FROM ID の SMTP アクションを定義しません。アプライアンスは、その ID のすべての検証結果を自動的に受け入れます。アプライアンスはすべての REJECT 結果に対して、デフォルトの拒否コードとテキストを使用します。

また、コマンドライン インターフェイスで `listenerconfig` コマンドを使用して、これを設定することもできます。

Received-SPF ヘッダー

AsyncOS で SPF/SIDF 検証を設定すると、電子メールに SPF/SIDF 検証ヘッダー（`Received-SPF`）が配置されます。さらに、Received-SPF ヘッダーには、次の情報が含まれます。

- 検証結果：SPF 検証結果（検証結果, （31 ページ）を参照してください）。
- ID：SPF 検証でチェックされた ID：HELO、MAIL FROM、PRA。
- レシーバ：検証するホスト名（チェックを実行する）。
- クライアント IP アドレス：SMTP クライアントの IP アドレス。
- ENVELOPE FROM：エンベロープ送信者メールボックス。（MAIL FROM ID は空にすることができないため、これは、MAIL FROM ID と異なることがあります）。
- x-sender：HELO、MAIL FROM、または PRA ID の値。
- x-conformance：準拠のレベル（表「SPF/SIDF 準拠レベル」を参照）と PRA チェックのダウングレードが実行されたかどうか。

次の例に、SPF/SIDF チェックに合格したメッセージに追加されるヘッダーを示します。

```
Received-SPF: Pass identity=pra; receiver=box.example.com;
client-ip=1.2.3.4; envelope-from="alice@fooo.com";
x-sender="alice@company.com"; x-conformance=sidf_compatible
```

（注） `spf-status` および `spf-passed` フィルタ ルールでは、received-SPF ヘッダーを使用して、SPF/SIDF 検証の状態が判断されます。

SPF/SIDF 検証済みメールに対して実行するアクションの決定

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。次のメッセージおよびコンテンツ フィルタ ルールを使用して、SPF/SIDF 検証済みメールの状態を判断し、検証結果に基づいてメッセージへのアクションを実行できます。

- `spf-status`。このフィルタ ルールは SPF/SIDF 状態に基づいてアクションを決定します。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。
- `spf-passed`。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。

（注） `spf-passed` フィルタ ルールはメッセージ フィルタでのみ使用できます。

より詳細な結果に対処する必要がある場合は、`spf-status` ルールを使用し、簡単なブール値を作成する必要がある場合は spf-passed ルールを使用できます。

検証結果

`spf-status` フィルタ ルールを使用する場合、次の構文を使用して、SPF/SIDF 検証結果に対してチェックできます。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

（注） `spf-status` メッセージ フィルタ ルールは、HELO、MAIL FROM、PRA ID に対して結果をチェックする場合にのみ使用できます。`spf-status` コンテンツ フィルタ ルールは、ID に対してチェックする場合に使用できません。`spf-status` コンテンツ フィルタは、PRA ID のみをチェックします。

次のいずれかの検証結果を受け取る可能性があります。

- None：情報の不足のため、検証を実行できません。
- Pass：クライアントは、指定された ID でメールを送信する権限がありません。
- Neutral：ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- SoftFail：ドメイン所有者は、指定された ID を使用する権限がホストにないと思うが、断言を避けたいと考えています。
- Fail：クライアントは、指定された ID でメールを送信する権限がありません。
- TempError：検証中に一時的なエラーが発生しました。
- PermError：検証中に永続的なエラーが発生しました。

CLI での spf-status フィルタ ルールの使用

次の例に、spf-status メッセージ フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"
or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
strip-header("Subject");
insert-header("Subject", "[POTENTIAL PHISHING] $Subject");
}
.
```

GUI での spf-status コンテンツ フィルタ ルール

GUI でコンテンツ フィルタから spf-status ルールをイネーブルにすることもできます。ただし、spf-status コンテンツ フィルタ ルールを使用した場合、HELO、MAIL FROM、PRA ID に対して結果をチェックできません。

GUI から spf-status コンテンツ フィルタ ルールを追加するには、[メール ポリシー（Mail Policies）] >[受信コンテンツ フィルタ（Incoming Content Filters）] をクリックします。次に [条件を追加（Add Condition）] ダイアログボックスから、[SPF検証（SPF Verification）] フィルタ ルールを追加します。条件に、1 つ以上の検証結果を指定します。

SPF 検証条件を追加したら、SPF 状態に基づいて実行するアクションを指定します。たとえば、SPF 状態が SoftFail の場合、メッセージを隔離します。

spf-passed フィルタ ルールの使用

`spf-passed` ルールは SPF 検証の結果をブール値として表示します。次の例に、`spf-passed` とマークされていない電子メールを隔離するための `spf-passed` ルールを示します。

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {


quarantine("Policy");

}
```

（注） `spf-status` ルールと異なり `spf-passed` ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、`spf-passed` ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、`spf-status` ルールを使用します。

SPF/SIDF 結果のテスト

組織によって SPF/SIDF の実装方法が異なるため、SPF/SIDF 検証の結果をテストし、これらの結果を使用して、SPF/SIDF の失敗の処理方法を決定します。コンテンツ フィルタ、メッセージ フィルタ、Email Security Monitor - Content Filters レポートを組み合わせて使用し、SPF/SIDF 検証の結果をテストします。

SPF/SIDF 検証の依存度によって、SPF/SIDF 結果をテストする詳細レベルが決まります。

SPF/SIDF 結果の基本の詳細度のテスト

受信メールの SPF/SIDF 検証結果の基本評価基準を取得するため、コンテンツ フィルタと [メール セキュリティモニタ-コンテンツフィルタ（Email Security Monitor - Content Filters）] ページを使用

できます。このテストでは、SPF/SIDF 検証結果のタイプごとに受信されたメッセージ数が表示されます。

ステップ 1 受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにし、コンテンツ フィルタを使用して、実行するアクションを設定します。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化, （26 ページ）を参照してください。

ステップ 2 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 での spf-status コンテンツ フィルタ ルール, （33 ページ）を参照してください。

ステップ 3 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（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。

SPF/SIDF 結果の高い詳細度のテスト

SPF/SIDF 検証結果のより包括的な情報を得るには、送信者の特定のグループの SPF/SIDF 検証をイネーブルにし、それらの特定の送信者の結果を確認するだけです。次に、その特定のグループのメール ポリシーを作成し、メール ポリシーで SPF/SIDF 検証をイネーブルにします。SPF/SIDF 結果の基本の詳細度のテスト, （33 ページ）で説明するように、コンテンツ フィルタを作成し、Content Filters レポートを確認します。検証が有効であることがわかったら、この指定した送信者のグループの電子メールをドロップするかバウンスするかの決断の基準として、SPF/SIDF 検証を使用できます。

ステップ 1 SPF/SIDF 検証のメール フロー ポリシーを作成します。受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにします。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化, （26 ページ）を参照してください。

ステップ 2 SPF/SIDF 検証の送信者グループを作成し、命名規則を使用して、SPF/SIDF 検証を示します。送信者グループの作成については、「Configuring the Gateway to Receive Mail」の章を参照してください。

ステップ 3 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 での spf-status コンテンツ フィルタ ルール, （33 ページ）を参照してください。

ステップ 4 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（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。

DMARC 検証

Domain-based Message Authentication, Reporting and Conformance（DMARC）は、電子メールベースの不正利用の可能性を減らすために作成された技術仕様です。DMARC では、電子メールの受信者が SPF および DKIM メカニズムを使用して電子メール認証を行う方法が標準化されています。DMARC 検証に合格するには、電子メールがこれらの認証メカニズムのうち少なくとも 1 つに合格し、認証 ID が RFC 5322 に準拠している必要があります。

E メール セキュリティ アプライアンスでは、以下を行うことができます。

- DMARC を使用して着信電子メールを検証する。
- ドメイン所有者のポリシーを上書き（受け入れ、隔離、または拒否）するプロファイルを定義する。
- ドメイン所有者に認証の導入環境の強化に役立つフィードバック レポートを送信する。
- DMARC 集計レポートのサイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合に、ドメイン所有者に配信エラー レポートを送信します。

AsyncOS では、2013 年 3 年 31 日に Internet Engineering Task Force（IETF）に提出された DMARC 仕様に準拠する電子メールを処理できます。詳細については、http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02 を参照してください。

（注） E メール セキュリティ アプライアンスでは、不正な形式の DMARC レコードを持つドメインからのメッセージの DMARC 検証は実行しません。ただし、こうしたメッセージを受信して処理することはできます。

DMARC 検証のワークフロー

次に、AsyncOS による DMARC 検証の実行方法について説明します。

1. AsyncOS に設定されたリスナーが SMTP 接続を受信します。
2. AsyncOS は、メッセージに対して SPF および DKIM 検証を実行します。
3. AsyncOS は、DNS から送信者のドメインの DMARC レコードを取得します。
   - レコードが見つからない場合、AsyncOS は DMARC 検証をスキップし、処理を続行します。
   - DNS ルックアップが失敗した場合、AsyncOS は指定された DMARC 検証プロファイルに基づいてアクションを実行します。
4. DKIM および SPF 検証の結果に応じて、AsyncOS はメッセージに対して DMARC 検証を実行します。

（注） DKIM および SPF 検証がイネーブルの場合は、DKIM および SPF 検証の結果が DMARC 検証で再利用されます。

5 DMARC 検証の結果と指定された DMARC 検証プロファイルに応じて、AsyncOS はメッセージを受け入れるか、隔離するか、または拒否します。DMARC 検証の失敗によってメッセージが拒否されなかった場合、AsyncOS は処理を続行します。
6 AsyncOS は適切な SMTP 応答を送信し、処理を続行します。
7 集計レポートの送信がイネーブルの場合、AsyncOS は DMARC 検証のデータを収集し、それをドメイン所有者に送信する日次レポートに追加します。DMARC 集計フィードバック レポートの詳細については、DMARC 集計レポート, （42 ページ）を参照してください。

（注） 集計レポートのサイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合、AsyncOS はドメイン所有者に配信エラー レポートを送信します。

DMARC を使用した受信メッセージの検証方法

DMARC を使用した受信メッセージの検証方法

	操作内容	追加情報
ステップ 1	新しい DMARC 検証プロファイルを作成するか、デフォルトの DMARC 検証プロファイルを要件に合わせて変更します。	DMARC 検証プロファイルの作成, （37 ページ） DMARC 検証プロファイルの編集, （38 ページ）
ステップ 2	（任意）DMARC のグローバル設定を要件に合わせて設定します。	DMARC のグローバル設定, （40 ページ）
ステップ 3：	DMARC を使用して受信メッセージを検証するようにメール フロー ポリシーを設定します。	メール フロー ポリシーでの DMARC 検証の設定, （41 ページ）
ステップ 4：	（任意）DMARC フィードバック レポートの返信アドレスを設定します。	DMARC フィードバック レポートの返信アドレスの設定, （42 ページ）
ステップ 5：	（任意）以下を確認します。 • DMARC 検証レポートと着信メール レポート • DMARC 検証に失敗したメッセージ（メッセージ トラッキングを使用）	• [DMARC検証（DMARC Verification）] ページ • [受信メール（Incoming Mail）] ページ • メッセージの検索

DMARC 検証プロファイルの管理

DMARC 検証プロファイルは、E メール セキュリティ アプライアンスのメール フロー ポリシーが DMARC を検証するために使用するパラメータのリストです。たとえば、特定のドメインからの非準拠メッセージをすべて拒否する厳格なプロファイルと、別のドメインからの非準拠メッセージをすべて隔離するあまり厳格でないプロファイルを作成できます。

DMARC 検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- DMARC レコード内のポリシーが拒否のときに実行するメッセージ アクション。
- DMARC レコード内のポリシーが隔離のときに実行するメッセージ アクション。
- 一時的な障害の場合に実行するメッセージ アクション。
- 永続的な障害の場合に実行するメッセージ アクション。

DMARC 検証プロファイルの作成

新しい DMARC 検証プロファイルを作成するには、次の手順を使用します。

（注） デフォルトでは、AsyncOS はデフォルトの DMARC 検証プロファイルを提供します。新しい DMARC 検証プロファイルを作成しない場合は、デフォルトの DMARC 検証プロファイルを使用できます。デフォルトの DMARC 検証プロファイルは、[メールポリシー（Mail Policies）] > [DMARC] ページで使用可能です。デフォルトの DMARC 検証プロファイルを編集する手順については、DMARC 検証プロファイルの編集, （38 ページ）を参照してください。

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 DMARC レコード内のポリシーが拒否のときに AsyncOS が実行するメッセージアクションを設定します。次のいずれかを実行します。

- [アクションなし（No Action）]。AsyncOS は、DMARC 検証に失敗したメッセージに対してアクションを実行しません。
- [隔離（Quarantine）]。AsyncOS は、DMARC 検証に失敗したメッセージを指定された隔離領域に隔離します。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証に失敗したすべてのメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `550` および「`#5.7.1 DMARC 未認証のメールは禁止されています（DMARC unauthenticated mail is prohibited）`」です。

ステップ 5 DMARC レコード内のポリシーが隔離のときに AsyncOS が実行するメッセージアクションを設定します。次のいずれかを実行します。

- [アクションなし（No Action）]。AsyncOS は、DMARC 検証に失敗したメッセージに対してアクションを実行しません。
- [隔離（Quarantine）]。AsyncOS は、DMARC 検証に失敗したメッセージを指定された隔離領域に隔離します。

ステップ 6 DMARC 検証中に一時的な障害が発生したメッセージに対して AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [承認（Accept）]。 AsyncOS は、DMARC 検証中に一時的な障害が発生したメッセージを受け入れます。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証中に一時的な障害が発生したメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `451` および「`#4.7.1 DMARC 検証を実行できません（Unable to perform DMARC verification）`」です。

ステップ 7 DMARC 検証中に永続的な障害が発生したメッセージに対して AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [承認（Accept）]。 AsyncOS は、DMARC 検証中に永続的な障害が発生したメッセージを受け入れます。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証中に永続的な障害が発生したメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `550` および「`#5.7.1 DMARC 検証に失敗しました（DMARC verification failed）`」です。

ステップ 8 変更を送信し、保存します。

DMARC 検証プロファイルの編集

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 目的の検証プロファイル名をクリックします。

ステップ 3 DMARC 検証プロファイルの作成, （37 ページ）の説明に従って、目的のフィールドを編集します。

ステップ 4 変更を送信し、保存します。

DMARC 検証プロファイルのエクスポート

アプライアンス上のすべての DMARC 検証プロファイルを configuration ディレクトリ内の単一のテキスト ファイルにエクスポートできます。

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 [プロファイルをエクスポート（Export Profiles）] をクリックします。
ステップ 3 ファイルの名前を入力します。
ステップ 4 [送信（Submit）] をクリックします。

DMARC 検証プロファイルのインポート

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 [プロファイルをインポート（Import Profiles）] をクリックします。
ステップ 3 DMARC 検証プロファイルを含むファイルを選択します。
ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存の DMARC 検証プロファイルが置き換えられることが警告されます。
ステップ 5 [インポート（Import）] をクリックします。
ステップ 6 変更を保存します。

DMARC 検証プロファイルの削除

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 削除する検証プロファイルを選択します。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

DMARC のグローバル設定

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 次の表に定義された設定を変更します。

DMARC のグローバル設定

グローバル設定	説明
特定の送信者はアドレスリストをバイパスします（Specific senders bypass address list）	特定の送信者から受信したメッセージの DMARC 検証をスキップします。ドロップダウン リストからアドレス一覧を選択します。 （注） [完全Eメールアドレスのみ許可（Allow only full Email Addresses）] オプションを選択して作成したアドレス リストのみを選択できます。詳細については、着信接続ルールへの送信者アドレス リストの使用を参照してください。
次のヘッダーのあるメッセージの場合、検証をバイパスする（Bypass verification for messages with headers）	特定のヘッダーを含むメッセージの DMARC 検証をスキップします。たとえば、メーリングリストや信頼できるフォワーダからのメッセージの DMARC 検証をスキップするには、このオプションを使用します。 ヘッダーを入力します。複数の場合はカンマで区切ります。
レポート生成のスケジュール（Schedule for report generation）	AsyncOS が DMARC 集計レポートを生成する時間。たとえば、集計レポートを生成する時間として非ピーク時間を選択することで、メールフローへの影響を回避できます。
レポートを生成するエンティティ（Entity generating reports）	DMARC 集計レポートを生成するエンティティ。これは、DMARC 集計レポートを受け取ったドメイン所有者がレポートを生成したエンティティを特定するのに役立ちます。 有効なドメイン名を入力します。
レポートの追加連絡先情報（Additional contact information for reports）	DMARC 集計レポートを受け取ったドメイン所有者がレポートを生成したエンティティと連絡を取る場合の、追加の連絡先情報（組織のカスタマー サポートの詳細など）。
すべての集計レポートのコピーの送信先（Send copy of all aggregate reports to）	すべての DMARC 集計レポートのコピーを特定のユーザ（集計レポートの分析を実行する内部ユーザなど）に送信します。 電子メール アドレスを入力します。複数の場合はカンマで区切ります。

グローバル設定	説明
エラーレポート（Error Reports）	DMARC 集計レポートのサイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合に、ドメイン所有者に配信エラー レポートを送信します。 チェックボックスをオンにします。

ステップ 4 変更を送信し、保存します。

メール フロー ポリシーでの DMARC 検証の設定

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。

ステップ 2 検証を実行するリスナーの着信メール ポリシーをクリックします。

ステップ 3 メール フロー ポリシーの [セキュリティサービス（Security Features）] セクションで、[オン（On）] を選択して、[DMARC検証（DMARC Verification）] をイネーブルにします。

ステップ 4 ポリシーで使用する DMARC 検証プロファイルを選択します。

ステップ 5 （任意）メッセージの送信元である DMARC 対応ドメインの RUA タグで指定された電子メール アドレスに対する DMARC 集計フィードバック レポートの送信をイネーブルにします。
集計フィードバック レポートは毎日生成されます。

ステップ 6 変更を送信し、保存します。

DMARC 検証ログ

DMARC 検証の次の段階で、メール ログにログ メッセージが追加されます。

- メッセージに対して DMARC 検証が試行されたとき
- DMARC 検証が完了したとき
- DKIM および SPF の調整結果を含む DMARC 検証の詳細が出力されるとき
- メッセージに対する DMARC 検証がスキップされたとき
- DMARC レコードが取得および解析されたとき、または DNS に障害が発生したとき
- ドメインに対する DMARC 集計レポートの配信が失敗したとき
- ドメインに対してエラー レポートが生成されたとき
- ドメインに対するエラー レポートの配信が成功したとき

- ドメインに対するエラー レポートの配信が失敗したとき

DMARC フィードバック レポートの返信アドレスの設定

ステップ 1 [システム管理（System Administration）] > [返信先アドレス（Return Addresses）] を選択します。
ステップ 2 [設定の編集（Edit Settings）] をクリックします。
ステップ 3 DMARC 集計フィードバック レポートの返信アドレスを入力します。
ステップ 4 変更を送信し、保存します。

DMARC 集計レポート

DMARC では、フィードバック メカニズムを利用して、ドメイン所有者のポリシーを安全かつスケーラブルな方法で適用します。このフィードバック メカニズムは、ドメイン所有者が認証の導入環境を強化するのに役立ちます。

メール フロー ポリシーで集計フィードバック レポートの送信をイネーブルにしてから、AsyncOS を使用して DMARC 検証を実行すると、AsyncOS は集計フィードバック レポートを毎日生成し、それをドメイン所有者に送信します。これらのレポートは、XML 形式で生成され、GZip ファイルにアーカイブされます。

（注） AsyncOS が生成するすべての DMARC 集計フィードバック レポートは、DMARC に準拠しています。

DMARC 集計フィードバック レポートには次のセクションが含まれています。

- レポート送信者のメタデータ（電子メール アドレスやレポート ID 番号など）。
- 公開済みの DMARC ポリシーの詳細。
- DMARC ポリシー処理の詳細（送信元 IP アドレスや処理のサマリーなど）。
- ドメイン ID
- DMARC 検証の結果と認証のサマリー。

DMARC 集計フィードバック レポートの例

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
    <org_name>cisco.com</org_name>
    <email>noreply-dmarc-support@cisco.com</email>
    <extra_contact_info>http://cisco.com/dmarc/support</extra_contact_info>
    <report_id>b1d925$4ecceab=0694614b826605cd@cisco.com</report_id>
    <date_range>
```

```
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>1.1.1.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
   <envelope_from>example.com</envelope_from>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
     <selector>ny</selector>
        <result>fail</result>
      </dkim>
      <dkim>
        <domain>example.net</domain>
<selector></selector>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
<scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

偽装メールの検出

電子メール偽造（スプーフィング、CEO詐欺、またはビジネス メール詐欺とも呼ばれる）とは、送信者の実際の身元を隠すためにメッセージ ヘッダーを変更し、それを既知の相手からの本物のメッセージのように見せかけるプロセスのことです。組織の幹部になりすましている詐欺師が、クライアントとその個人情報（PII）のリストを送信するように求める偽造メッセージを従業員に送信しているとしましょう。送信者の本当の身元に気づいていない従業員は、クライアントとその PII のリストを送信します。詐欺師はその PII を使用して個人情報の盗難を行います。

Cisco E メール セキュリティ アプライアンスは、偽装送信者のアドレス（送信元ヘッダ）がある詐欺メッセージを検出し、そのようなメッセージに対して指定されたアクションを実行することができます。たとえば、アプライアンスは偽装送信者のアドレスがあるメッセージを検出して、送信元ヘッダーをエンベロープ送信者に置き換えることができます。この場合、従業員には偽装電子メールアドレスではなく、実際の送信者（詐欺師）の電子メールアドレスが表示されます。

偽造メールの検出の設定

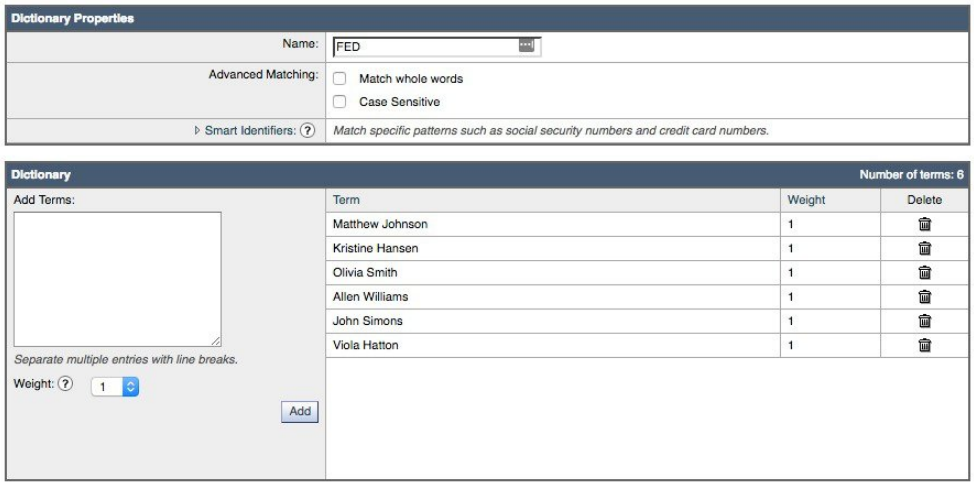
1. メッセージが偽造される可能性がある組織内のユーザ（幹部など）を特定します。新しいコンテンツ ディクショナリを作成し、特定したユーザの名前をそれに追加します。

   コンテンツ ディクショナリの作成時には、

   - ユーザの名前（電子メール アドレスではない）を入力します。たとえば、"olivia.smith@example.com" ではなく "Olivia Smith" を入力します。
   - 高度なマッチングとスマート ID は構成しないでください。
   - 使用する用語の重みは選択しないでください。
   - 正規表現は使用しないでください。

   次の図は、偽造メールの検出用に作成されたサンプル コンテンツ ディクショナリを示しています。

   図 *3*：偽造メールの検出用のコンテンツ ディクショナリ



   コンテンツディクショナリを構成する手順については、ディクショナリの追加を参照してください。

2. 偽造メールを検出するための受信コンテンツ フィルタまたはメッセージ フィルタと、そのようなメッセージに対してアプライアンスが取る必要があるアクションを作成します。次のように指定します。

   - [条件/ルール（Condition/Rule）]：偽造メールの検出（コンテンツ フィルタの条件およびメッセージ フィルタ ルールを参照）
   - [アクション（Action）]：偽造メールの検出またはユーザの要求に基づく他のアクション。（コンテンツ フィルタの条件 およびメッセージ フィルタ ルール を参照）。

3 新しく作成されたコンテンツ フィルタを受信メール ポリシーに追加します。メール ポリシーをユーザ単位で適用する方法を参照してください。

偽装メールの検出結果の監視

検出された偽装メッセージについてのデータを表示するには、[偽造メールの一致（Forged Email Matches）] レポートのページ（[モニタ（Monitor）]>[偽造メールの一致（Forged Email Matches）]）を参照してください。このレポート ページに表示されるレポートは、次のとおりです。

- 偽装メール一致の上位（Top Forged Email Matches）受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
- 偽装メールの一致：詳細（Forged Email Matches: Details）受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。メッセージ トラッキングのメッセージ一覧を表示するには、番号をクリックします。

メッセージ トラッキングでの偽装メールの詳細の表示

メッセージ トラッキングでアプライアンスによって検出された偽装メッセージの詳細を表示するには、次のことを確認します。

- メッセージ トラッキングが有効である。メッセージ トラッキングを参照してください。
- 偽装メッセージを検出するためのコンテンツまたはメッセージ フィルタが動作している。