



テキスト リソース

この章は、次の項で構成されています。

- [テキスト リソースの概要, 1 ページ](#)
- [コンテンツ ディクショナリ, 2 ページ](#)
- [コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法, 7 ページ](#)
- [テキスト リソースについて, 9 ページ](#)
- [テキスト リソース管理の概要, 10 ページ](#)
- [テキスト リソースの使用, 14 ページ](#)

テキスト リソースの概要

この章では、コンテンツ ディクショナリ、免責事項、およびテンプレートなどのさまざまなテキスト リソースの作成および管理について説明します。

コンテンツ ディクショナリ

コンテンツ ディクショナリは、アプライアンスの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツ フィルタ およびメッセージ フィルタ の両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージ ヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または隔離できます。

AsyncOS オペレーティング システムには、GUI ([メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)]) または CLI の `dictionaryconfig` コマンドを使用して、合計 100 個のコンテンツ ディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

コンテンツディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツフィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタルールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタアクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

効率的に処理するため、次のコンテンツディクショナリのエントリは単語として処理されることに注意してください。

- 英数字のみを含むエントリ
- 0～9、A～Z、a～z、ドット、アンダースコア、ハイフン、アットマークを含む電子メールアドレス
- 0～9、A～Z、a～z、ドット、アンダースコア、ハイフン、アットマークを含むドメイン名

このような単語を正規表現としてアプライアンスに処理させる場合は、たとえば(user@example.com)のように、その単語をカッコで囲みます。

テキストリソース

テキストリソースは、免責事項、通知テンプレート、アンチウイルステンプレートなどのテキストオブジェクトです。AsyncOS のさまざまなコンポーネントで使用できる新規オブジェクトを作成できます。テキストリソースをインポートおよびエクスポートできます。

メッセージの免責事項スタンプ

メッセージの免責事項スタンプを使用すると、免責事項のテキストリソースをメッセージに追加できます。たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

コンテンツディクショナリ

コンテンツディクショナリは、アプライアンスの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツフィルタおよびメッセージフィルタの両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリスト

を作成し、フィルタールールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または隔離できます。

AsyncOS オペレーティング システムには、GUI ([メール ポリシー (Mail Policies)]> [辞書 (Dictionaries)]) または CLI の `dictionaryconfig` コマンドを使用して、合計 100 個のコンテンツ ディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

コンテンツ ディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツ フィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタールールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタ アクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

効率的に処理するため、次のコンテンツ ディクショナリのエントリは単語として処理されることに注意してください。

- 英数字のみを含むエントリ
- 0～9、A～Z、a～z、ドット、アンダースコア、ハイフン、アットマークを含む電子メールアドレス
- 0～9、A～Z、a～z、ドット、アンダースコア、ハイフン、アットマークを含むドメイン名

このような単語を正規表現としてアプライアンスに処理させる場合は、たとえば (`user@example.com`) のように、その単語をカッコで囲みます。

ディクショナリの内容

ディクショナリの単語は 1 行につき 1 つのテキスト文字列で作成し、エントリはプレーン テキストまたは正規表現の形式で記載できます。ディクショナリには、非 ASCII 文字を含めることもできます。正規表現のディクショナリを定義すると、より柔軟に単語を照合させることができます。ただし、このためには適切に単語を区切る方法を理解する必要があります。Python スタイルの正規表現の詳細については、次の URL からアクセスできる「Python Regular Expression HOWTO」を参考にしてください。

<http://www.python.org/doc/howto/>



(注) ディクショナリのエントリの最初に特殊文字 # を使用すると、文字クラス [#] をコメントとして扱われることなく使用できます。

単語によってフィルタ条件をより簡単にトリガーできるように、各単語に「重み」を指定できます。AsyncOS では、コンテンツディクショナリの単語に対してメッセージをスキャンし、単語インスタンスの数に単語の重みを掛けることでメッセージのスコアを付けます。2つの単語インスタンスに3の重みが付いている場合、スコアは6になります。AsyncOS は、このスコアをコンテンツフィルタまたはメッセージフィルタに関連するしきい値と比較し、メッセージがフィルタアクションをトリガーするかどうかを決定します。

コンテンツディクショナリにスマートIDを追加することもできます。スマートIDは、社会保障番号やABAルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。これらのIDはポリシーの拡張に便利です。正規表現の詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Regular Expressions in Rules」を参照してください。スマートIDの詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Smart Identifiers」を参照してください。



(注) 端末のCLIに非ASCII文字を含むディクショナリが正しく表示される場合とされない場合があります。非ASCII文字を含むディクショナリを表示および変更する最適な方法は、ディクショナリをテキストファイルにエクスポートし、テキストファイルを編集して、新しいファイルを再びアプライアンスにインポートする方法です。詳細については、[テキストファイルとしてディクショナリをインポートおよびエクスポートする方法](#)、(4ページ)を参照してください。

単語境界と2バイト文字セット

一部の言語(2バイト文字セット)では、単語または単語の区切りに関する概念や、大文字/小文字がありません。単語を構成する文字(正規表現で「\w」と表される文字)の識別などが必要になる複雑な正規表現では、ロケールが不明な場合、またはエンコードが不明な場合、問題が発生します。この理由から、単語境界の拡張をディセーブルにできます。

テキストファイルとしてディクショナリをインポートおよびエクスポートする方法

コンテンツディクショナリ機能には、デフォルトでアプライアンスのconfigurationディレクトリに配置されている次のテキストファイルが含まれます。

- config.dtd
- profanity.txt
- proprietary_content.txt
- sexual_content.txt

これらのテキストファイルは、コンテンツディクショナリ機能と組み合わせて使用することで、新規ディクショナリの作成をサポートすることを目的としています。これらのコンテンツディクショナリは重み付けされており、スマートIDを使用することでデータ内のパターンを高い精度で検出し、コンプライアンスの問題となるパターンの場合にはフィルタをトリガーします。



- (注) ディクショナリをインポートおよびエクスポートする場合は、完全に一致する単語の設定と大文字と小文字を区別する設定が保持されません。この設定は、設定ファイルにのみ保持されません。

configuration ディレクトリへのアクセスの詳細については、[FTP、SSH、およびSCP アクセス](#)を参照してください。

ユーザ独自のディクショナリ ファイルを作成して、アプライアンスにインポートすることもできます。非 ASCII 文字をディクショナリに追加する最適な方法は、アプライアンス以外の場所でテキストファイルのディクショナリに単語を追加し、アプライアンス上にファイルを移動してから新しいディクショナリとしてファイルをインポートする方法です。ディクショナリのインポートの詳細については、[ディクショナリのインポート、\(6 ページ\)](#)を参照してください。ディクショナリのエクスポートについては、[ディクショナリのエクスポート、\(7 ページ\)](#)を参照してください。

**注意**

これらのテキストファイルには、一部の人の間では卑猥、下品または不快に感じられる単語が含まれています。これらのファイルからコンテンツ ディクショナリに単語をインポートした場合、アプライアンスに設定したコンテンツ ディクショナリを後で閲覧する際にこれらの単語が表示されます。

ディクショナリの追加

ステップ 1 [メールポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。

ステップ 2 [辞書を追加 (Add Dictionary)] をクリックします。

ステップ 3 ディクショナリの名前を入力します。

ステップ 4 (任意) 高度なマッチングを設定します。

- (注) AsyncOS は、設定ファイルに保存する際に、[単語全体の一致 (Match Whole Words)] と [大文字小文字を区別 (Case Sensitive)] の設定を保持します。ディクショナリをインポートおよびエクスポートするときは、AsyncOS はこれらの設定は保持しません。

ステップ 5 (任意) ディクショナリにスマート ID を追加します。

スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。スマート ID の詳細については、「Using Message Filters to Enforce Email Policies」の章を参照してください。

ステップ 6 新規ディクショナリのエントリを単語のリストに入力します。

追加する複数の新しいエントリがあり、フィルタアクションを同じ様にトリガーにする場合は、1 行につき 1 つずつ新しい語を入力します。

(注) 正規表現「.*」をエントリの最初または最後に使用したコンテンツディクショナリのエントリがあると、その「単語」に一致する MIME パートが見つかった場合にシステムがロックされます。シスコは、「.*」をコンテンツディクショナリのエントリの先頭または末尾に使用しないことを推奨します。

ステップ7 単語に対する重みを指定します。
フィルタアクションを他の単語よりトリガーしやすくなるように、ディクショナリの単語に「重み」を付けられます。この重みがフィルタアクションの決定に使用される仕組みの詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Threshold Scoring for Content Dictionaries」を参照してください。

ステップ8 [追加 (Add)] をクリックします。

ステップ9 変更を送信し、保存します。

ディクショナリの削除

はじめる前に

AsyncOS は、削除されたディクショナリを参照しているすべてのメッセージフィルタを無効としてマークすることに注意してください。AsyncOS は削除されたディクショナリを参照しているすべてのコンテンツフィルタをイネーブルのままにしますが、今後無効と判断します。

ステップ1 [メールポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。

ステップ2 ディクショナリの横にあるゴミ箱アイコンをクリックして、ディクショナリのリストから削除します。確認メッセージには、ディクショナリを現在参照しているフィルタがすべて表示されます。

ステップ3 確認メッセージで [削除 (Delete)] をクリックします。

ステップ4 変更を保存します。

ディクショナリのインポート

はじめる前に

インポートするファイルが、アプライアンスの configuration ディレクトリに存在することを確認します。

-
- ステップ 1 [メールポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。
 - ステップ 2 [辞書をインポート (Import Dictionary)] をクリックします。
 - ステップ 3 インポート元の場所を選択します。
 - ステップ 4 インポートするファイルを選択します。
 - ステップ 5 ディクショナリの単語に使用するデフォルトの重みを選択します。
AsyncOS では、重みが指定されていない単語に対してデフォルトの重みを割り当てます。ファイルのインポート後に重みを編集できます。
 - ステップ 6 エンコード方式を選択します。
 - ステップ 7 [Next] をクリックします。
 - ステップ 8 ディクショナリの名前を指定し、編集します。
 - ステップ 9 変更を送信し、保存します。
-

ディクショナリのエクスポート

-
- ステップ 1 [メールポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。
 - ステップ 2 [辞書をエクスポート (Export Dictionary)] をクリックします。
 - ステップ 3 エクスポートするディクショナリを選択します。
 - ステップ 4 エクスポートされたディクショナリのファイル名を入力します。
これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
 - ステップ 5 エクスポート先の場所を選択します。
 - ステップ 6 テキスト ファイルのエンコード方式を選択します。
 - ステップ 7 変更を送信し、保存します。
-

コンテンツ ディクショナリ フィルタ ルールの使用方法 およびテスト方法

ディクショナリは、さまざまな dictionary-match() メッセージ フィルタ ルールおよびコンテンツ フィルタに使用できます。

ディクショナリの照合フィルタ ルール

`dictionary-match(<dictionary_name>)` という名前のメッセージフィルタ ルール（および同様のルール）は、メッセージの本文にコンテンツ ディクショナリ (`dictionary_name`) に存在するいずれかの正規表現が含まれる場合に有効と判断されます。該当のディクショナリが存在しない場合は、ルールは無効と判断されます。

`dictionary-match()` ルールは、`body-contains()` 本文スキャンルールと同様にメッセージ本文と添付ファイルのみをスキャンし、ヘッダーをスキャンしないことに注意してください。

ヘッダーのスキャンには、適切な `*-dictionary-match()` タイプのルールを使用できます（`subject-dictionary-match()` や、より一般的なルールでカスタム ヘッダーを含むすべてのヘッダーを指定できる `header-dictionary-match()` など、特定のヘッダーに対するルールが存在します）。ディクショナリの照合の詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Dictionary Rules」を参照してください。

表 1: コンテンツ ディクショナリのメッセージフィルタ ルール

ルール (Rule)	構文	説明
ディクショナリ照合	<code>dictionary-match (<dictionary_name>)</code>	指定したディクショナリに存在するすべての正規表現に一致した単語がメッセージに含まれているか。

次の例では `dictionary-match()` ルールを使用して、アプライアンスが（前回の例で作成した）「secret_words」という名前のディクショナリ内の単語を含むメッセージをスキャンした際に、管理者にメッセージをブラインドカーボン コピーで送信する新規メッセージ フィルタが作成されます。設定値によっては、大文字/小文字も含めて「codename」と完全に一致する単語を含むメッセージのみが、このフィルタで有効と判断されることに注意してください。

```
bcc_codenames:
if (dictionary-match ('secret_words'))
{
bcc('administrator@example.com');
}
```

この例では、ポリシー隔離にメッセージを送信します。

```
quarantine_codenames:
if (dictionary-match ('secret_words'))
{
quarantine('Policy');
}
```


ディクショナリ エントリの例

表 2: ディクショナリ エントリの例

説明	例
ワイルドカード	
アンカー	末尾 : foo \$、先頭 : ^ foo
電子メールアドレス (ピリオドをエスケープしない)	foo@example.com, @example.com example.com\$ (次で終わる) @example.*
Subject	電子メールの件名 (電子メールの件名に ^アンカーを使用する際は、件名の先頭に「RE:」や「FW:」などが多く付いていることを覚えておいてください)

コンテンツ ディクショナリのテスト方法

trace 関数を使用すると、dictionary-match() ルールを使用しているメッセージフィルタに対して迅速なフィードバックが得られます。詳細については、[テストメッセージを使用したメールフローのデバッグ：トレース](#)を参照してください。上記の quarantine_codenames フィルタの例のように、quarantine() アクションを使用してフィルタをテストすることもできます。

テキストリソースについて

テキストリソースは、メッセージへの添付や、メッセージとしての送信が可能なテキストテンプレートです。テキストリソースは、次のいずれかの種類になります。

- **メッセージ免責事項**：メッセージに追加されるテキスト。詳細については、[免責事項テンプレート, \(14 ページ\)](#)を参照してください。
- **通知テンプレート**：通知として送信されるメッセージ (notify() および notify-bcc() アクションで使用されます)。詳細については、[通知テンプレート, \(20 ページ\)](#)を参照してください。
- **アンチウイルス通知テンプレート**：メッセージにウイルスが見つかったときに、通知として送信されるメッセージ。コンテナ用のテンプレート (元のメッセージに付加)、またはメッセージに付加せず通知として送信されるテンプレートを作成できます。詳細については、[アンチウイルス通知テンプレート, \(21 ページ\)](#)を参照してください。
- **バウンスおよび暗号化失敗通知テンプレート**：メッセージがバウンスされたときやメッセージの暗号化に失敗したときに通知として送信されるメッセージ。詳細については、[バウンス通知および暗号化失敗通知テンプレート, \(24 ページ\)](#)を参照してください。

- 暗号化通知テンプレート：発信電子メールを暗号化するようにアプライアンスを設定した場合に送信されるメッセージ。このメッセージは、受信者が暗号化されたメッセージを受信したことを受信者に通知し、メッセージを読む手順を示します。詳細については、[暗号化通知テンプレート](#)、(26 ページ) を参照してください。

CLI (`textconfig`) または GUI を使用して、テキストリソースの追加、削除、編集、インポート、およびエクスポートを含むテキストリソースの管理ができます。GUI を使用したテキストリソースの管理については、[テキストリソース管理の概要](#)、(10 ページ) を参照してください。

テキストリソースには、非 ASCII 文字を含めることができます。



- (注) 非 ASCII 文字を含むテキストリソースは端末の CLI に正しく表示される場合とされない場合があります。非 ASCII 文字を含むテキストリソースを表示および変更するには、テキストリソースをテキストファイルにエクスポートし、テキストファイルを編集して、新しいファイルを再びアプライアンスにインポートします。詳細については、[テキストファイルとしてディクショナリをインポートおよびエクスポートする方法](#)、(4 ページ) を参照してください。

テキストファイルとしてのテキストリソースのインポートおよびエクスポート

アプライアンスの `configuration` ディレクトリに対するアクセス権を持っている必要があります。インポートするテキストファイルは、アプライアンス上の `configuration` ディレクトリに存在する必要があります。エクスポートされたテキストファイルは、`configuration` ディレクトリに配置されます。

`configuration` ディレクトリへのアクセスの詳細については、[FTP、SSH、およびSCPアクセス](#) を参照してください。

非 ASCII 文字をテキストリソースに追加するには、アプライアンス以外の場所でテキストファイルのテキストリソースに単語を追加し、アプライアンス上にファイルを移動し、新しいテキストリソースとしてファイルをインポートします。テキストリソースのインポートの詳細については、[テキストリソースのインポート](#)、(12 ページ) を参照してください。テキストリソースのエクスポートについては、[テキストリソースのエクスポート](#)、(12 ページ) を参照してください。

テキストリソース管理の概要

GUI または CLI を使用してテキストリソースを管理できます。この項では、GUI について説明します。

`textconfig` コマンドを使用して CLI からテキストリソースを管理します。

テキストリソース管理には、次のタスクが含まれます。

- 追加

- 編集および削除
- エクスポートおよびインポート
- すべてのテキストリソース タイプのプレーン テキスト メッセージの定義
- 一部のテキストリソース タイプの HTML ベースのメッセージの定義

テキストリソースの追加

-
- ステップ 1** [メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] に移動します。
- ステップ 2** [テキストリソースを追加 (Add Text Resource)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドにテキストリソースの名前を入力します。
- ステップ 4** [タイプ (Type)] フィールドからテキストリソースのタイプを選択します。
- ステップ 5** [テキスト (Text)] または [HTML およびプレーンテキスト (HTML and Plain Text)] のどちらかのフィールドに、メッセージテキストを入力します。
テキストリソースがプレーンテキストメッセージのみを許可する場合は、[テキスト (Text)] フィールドを使用します。テキストリソースが HTML およびプレーンテキストメッセージの両方を許可する場合は、[HTML およびプレーンテキスト (HTML and Plain Text)] フィールドを使用します。
- ステップ 6** 変更を送信し、保存します。
-

テキストリソースの削除

はじめる前に

テキストリソースの削除の影響に注意してください。

- 削除されたテキストリソースを参照しているすべてのメッセージフィルタは、無効としてマークされます。
- 削除されたテキストリソースを参照しているすべてのコンテンツ フィルタはイネーブルのままになりますが、今後無効と判断されます。

-
- ステップ 1** [メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] ページに移動し、削除するテキストリソースの [削除 (Delete)] 列にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。
- ステップ 2** [削除 (Delete)] をクリックして、テキストリソースを削除します。
- ステップ 3** 変更を保存します。
-

テキストリソースのインポート

はじめる前に

インポートするファイルが、アプライアンスの `configuration` ディレクトリに存在することを確認します。

-
- ステップ 1** [メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] ページに移動し、[テキストリソースのインポート (Import Text Resource)] をクリックします。
 - ステップ 2** インポートするファイルを選択します。
 - ステップ 3** エンコード方式を指定します。
 - ステップ 4** [Next] をクリックします。
 - ステップ 5** 名前を選択し、テキストリソース タイプを編集および選択します。
 - ステップ 6** 変更を送信し、保存します。
-

テキストリソースのエクスポート

はじめる前に

テキストリソースをエクスポートする場合は、テキストファイルがアプライアンスの `configuration` ディレクトリに作成されることに注意してください。

-
- ステップ 1** [メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] ページに移動し、[テキストリソースのエクスポート (Export Text Resource)] をクリックします。
 - ステップ 2** エクスポートするテキストリソースを選択します。
 - ステップ 3** テキストリソースのファイル名を入力します。
 - ステップ 4** テキストファイルのエンコード方式を選択します。
 - ステップ 5** [送信 (Submit)] をクリックしてテキストリソースを含むテキストファイルを `configuration` ディレクトリに作成します。
-

HTML ベースのテキストリソースの概要

免責事項などの一部のテキストリソースは、HTML ベースのメッセージおよびプレーンテキストメッセージの両方を使用して作成できます。HTML ベースのメッセージとプレーンテキストメッセージの両方を含むテキストリソースが電子メールメッセージに適用された場合、HTML ベースのテキストリソースメッセージは電子メールメッセージのテキストまたは HTML 部分に適用さ

れ、プレーン テキスト メッセージは電子メール メッセージのテキストまたはプレーン部分に適用されます。

HTML ベースのテキストリソースを追加または編集する場合、GUI には、HTML コードを手動で記述せずにリッチ テキストの入力を可能にするリッチ テキスト編集が含まれます。

HTML ベースのテキストリソースを追加および編集する場合は、次の点に留意してください。

- HTML バージョンに基づいて、メッセージのプレーン テキスト バージョンを自動的に生成するよう選択できます。または、プレーン テキスト バージョンを個別に定義できます。
- [コードビュー (Code View)] ボタンをクリックすることにより、リッチ テキスト エディタと HTML コード間を切り替えることができます。
- リッチ テキスト エディタでサポートされない HTML コードを GUI で入力するには、コードビューに切り替え、HTML コードを手動で入力します。たとえば、これは、HTML タグを使用して外部サーバにあるイメージ ファイルへの参照を挿入する場合に行います。

HTML ベースのテキストリソースのインポートおよびエクスポート

HTML ベースのテキストリソースをテキスト ファイルにエクスポートしたり、テキスト ファイルから HTML ベースのテキストリソースをインポートしたりできます。HTML ベースのテキストリソースをファイルにエクスポートする場合、ファイルにはテキストリソースの各バージョンに対する次のセクションが含まれます。

- [html_version]
- [text_version]

これらのセクションの順序は重要ではありません。

たとえば、エクスポートされたファイルには、次のテキストが含まれることがあります。

```
[html_version]
<p>Sample <i>message.</i></p>
[text_version]
Sample message.
```

HTML ベースのテキストリソースをエクスポートおよびインポートする場合は、次のルールとガイドラインに留意してください。

- プレーン テキスト メッセージが HTML バージョンから自動的に生成される HTML ベースのテキストリソースをエクスポートする場合、エクスポートされたファイルには [text_version] セクションが含まれません。
- テキスト ファイルからインポートするとき、[html_version] セクション下のすべての HTML コードは作成されたテキストリソースの HTML メッセージに変換されます (テキストリソース タイプが HTML メッセージをサポートする場合)。同様に、[text_version] セクション下のすべてのテキストは、作成されたテキストリソースのプレーン テキスト メッセージに変換されます。
- HTML ベースのテキストリソースを作成するために、空の、または存在しない [html_version] セクションを含むファイルからインポートする場合、アプライアンスは [text_version] セク

ションのテキストを使用して HTML およびプレーンテキストメッセージの両方を作成します。

テキストリソースの使用

すべてのタイプのテキストリソースは、[テキストリソース (Text Resources)] ページまたは CLI の `textconfig` コマンドを使用して、同じ方法で作成されます。一度作成されると、各タイプで異なる使われ方をします。免責事項テンプレートおよび通知テンプレートは、フィルタおよびリスナーで使用されます。一方、アンチウイルス通知テンプレートは、メールポリシーおよびアンチウイルス設定値で使用されます。

免責事項テンプレート

アプライアンスは、リスナーが受信した一部またはすべてのメッセージのテキストの上または下（ヘッダーまたはフッター）にデフォルトの免責事項を追加できます。次の方法を使用して、アプライアンスでメッセージに免責事項を追加できます。

- リスナーから、GUI または `listenerconfig` コマンドを使用する方法（[リスナーからの免責事項テキストの追加](#)、[\(14 ページ\)](#) を参照）。
- コンテンツ フィルタ アクション `Add Disclaimer Text` を使用する方法（[コンテンツ フィルタのアクション](#)を参照）。
- メッセージ フィルタ アクション `add-footer()` を使用する方法（の「[Using Message Filters to Enforce Email Policies](#)」の章を参照）。
- データ消失防止プロファイルを使用する方法（[データ損失の防止](#)を参照）。
- メッセージの目的がフィッシングまたはマルウェアの配布である可能性があることをユーザに通知するようアウトブレイク フィルタに対してメッセージの修正を使用する方法（[メッセージの変更](#)を参照）。このタイプの通知に追加される免責事項は、テキストの上に追加されます。

たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

免責事項テキストを使用する前に、免責事項テンプレートを作成する必要があります。GUI で [テキストリソース (Text Resources)] ページを使用（[テキストリソースの追加](#)、[\(11 ページ\)](#) を参照）または `textconfig` コマンドを使用（『[CLI Reference Guide for AsyncOS for Cisco Email Security Appliances](#)』を参照）して、使用するテキスト文字列のセットを作成および管理します。

リスナーからの免責事項テキストの追加

免責事項テキストリソースを作成したら、リスナーで受信するメッセージに付加するテキスト文字列を選択します。免責事項テキストをメッセージの上部または下部に追加できます。この機能は、パブリック（インバウンド）リスナーとプライベート（アウトバウンド）リスナーの両方に使用できます。

テキストおよびHTMLから構成されるメッセージ（Microsoft Outlookでは、このタイプのメッセージを「multipart alternative」と呼びます）を送信する場合、アプライアンスは、メッセージの両方の部分に免責事項をスタンプします。ただし、メッセージが署名済みのコンテンツである場合、署名が無効になるためコンテンツは変更されません。代わりに、免責事項スタンプによって「Content-Disposition inline attachment」という新規パートが作成されます。マルチパートメッセージの詳細については、「Using Message Filters to Enforce Email Policies」の章の「Message Bodies vs. Message Attachments」を参照してください。

フィルタからの免責事項の追加

フィルタアクション `add-footer()` またはコンテンツ フィルタ アクション「免責条項文の追加」を使用して、メッセージの免責事項に特定の定義済みテキスト文字列を付加することができます。たとえば、次のメッセージフィルタールールは、LDAPグループ「Legal」に属するユーザから送信されるすべてのメッセージに、`legal.disclaimer` というテキスト文字列を付加します。

```
Add-Disclaimer-For-Legal-Team:
if (mail-from-group == 'Legal')
{
add-footer('legal.disclaimer');
}
```

免責事項およびフィルタ アクション変数

メッセージフィルタアクション変数を使用することもできます（詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照してください）。

免責事項テンプレートには、次の変数を使用できます。

表 3: アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます（エンベロープ受信者には置き換えられません）。
\$From	メッセージの From: ヘッダーに置き換えられます（エンベロープ送信者には置き換えられません）。
\$Subject	元のメッセージの件名に置き換えられます。
\$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
\$Time	現在の時刻（ローカル時間帯）に置き換えられます。
\$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。

変数	置き換える値
\$MID	メッセージを内部で識別するために使用するメッセージID (MID) に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase レピュテーションスコアに置き換えられます。レピュテーションスコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名のカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイルタイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルサイズのカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを E メールセキュリティ アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	E メールセキュリティ アプライアンスのホスト名に置き換えられます。
\$header[<i>'string'</i>]	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
\$envelope recipients	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
\$bodysize	メッセージのサイズ (バイト単位) に置き換えられます。
\$FilterName	処理中のフィルタの名前を返します。

変数	置き換える値
\$MatchedContent	スキャン フィルタ ルール (body-contains などのフィルタ ルールやコンテンツ デictionary を含む) をトリガーした内容を返します。
\$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
\$DLPSeverity	違反の重大度に置き換えられます。値は [低 (Low)]、[中 (Medium)]、[高 (High)]、または [重大 (Critical)] のいずれかです。
\$DLPRiskFactor	メッセージに含まれる機密性の高い情報のリスク係数 (0 ~ 100 のスコア) に置き換えられます。
\$threat_category	フィッシング、ウイルス、詐欺、マルウェアなどのアウトブレイク フィルタ 脅威のタイプに置き換えられます。
\$threat_type	アウトブレイク フィルタ 脅威カテゴリのサブカテゴリに置き換えられます。たとえば、チャリティ詐欺、金銭目的のフィッシング、偽の取引などがあります。
\$threat_description	アウトブレイク フィルタ 脅威の説明に置き換えられます。
\$threat_level	メッセージの脅威レベル (スコア 0 ~ 5) に置き換えられます。
\$threat_verdict	[メッセージの変更 - 脅威レベル (Message Modification Threat Level)] しきい値によって、「はい」または「いいえ」に置き換えられます。メッセージに含まれるウイルスまたは非ウイルスの脅威レベルが [メッセージの変更 - 脅威レベル (Message Modification Threat Level)] しきい値以上の場合、この変数の値は「はい」に設定されます。

メッセージ フィルタ アクション変数を免責事項で使用するには、(GUI の [テキストリソース (Text Resource)] ページまたは textconfig コマンドから) メッセージの免責事項を作成し、変数を参照します。

add-footer() アクションでは、フッターを inline attachment、UTF-8 coded attachment、quoted printable attachment として追加することで、非 ASCII テキストをサポートします。

免責事項スタンプと複数エンコード方式

AsyncOS には、異なる文字エンコード方式を含む免責事項スタンプの動作を変更するために使用される設定値が存在します。デフォルトでは、AsyncOS は電子メール メッセージの本文パート内に添付されるように、免責事項を配置します。localeconfig コマンド内で設定した設定値を使用して、本文パートと免責事項のエンコード方式が異なる場合の動作を設定できます。数個のパートから構成される電子メール メッセージを確認することで、この設定が理解しやすくなります。

To: joe@example.com From: mary@example.com Subject: Hi!	ヘッダー
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	最初の添付パート
Example.zip	2 番目の添付パート

最初の空白行に続くメッセージの本文には、多くの MIME パートが含まれている場合があります。多くの場合、最初のパートは「本文」または「テキスト」と呼ばれ、2 番目以降のパートは「アタッチメント」と呼ばれます。

免責事項は「アタッチメント」（上記の例）または本文の一部として、電子メールに含めることができます。

To: joe@example.com From: mary@example.com Subject: Hi!	ヘッダー
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	本文に含められた免責事項
Example.zip	最初の添付パート

一般的に、メッセージの本文と免責事項の間でエンコード方式の不一致が起こると、免責事項が本文に含まれ（インライン）個別のアタッチメントとして含まれないように、AsyncOS はメッセージ全体をメッセージの本文と同じエンコード方式でエンコードしようとします。つまり、免責事項と本文のエンコード方式が一致する場合、または免責事項のテキストに（本文の）インラインに表示できる文字が含まれている場合は、免責事項はインラインに含められます。たとえば、US-ASCII 文字のみを含む ISO-8859-1 エンコードされた免責事項が生成される可能性があります。結果的に、この免責事項は問題なく「インライン」に表示されます。

ただし、免責事項が本文と組み合わせられない場合、`localeconfig` コマンドを使用し、本文テキストを昇格または変換して免責事項のエンコード方式と一致させるように AsyncOS を設定することで、免責事項をメッセージの本文に含めることができます。

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body

Behavior for untagged non-ASCII headers: Impose encoding of message body

Behavior for mismatched footer or heading encoding: Only try encoding from
message body
```

```
Choose the operation you want to perform:

- SETUP - Configure multi-lingual settings.

[]> setup
```

If a header is modified, encode the new header in the same encoding as the message body? (Some MUAs incorrectly handle headers encoded in a different encoding than the body. However, encoding a modified header in the same encoding as the message body may cause certain characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or modified, impose the encoding of the body on the header during processing and final representation of the message? (Many MUAs create non-RFC-compliant headers that are then handled in an undefined way. Some MUAs handle headers encoded in character sets that differ from that of the main body in an incorrect way. Imposing the encoding of the body on the header may encode the header more precisely. This will be used to interpret the content of headers for processing, it will not modify or rewrite the header unless that is done explicitly as part of the processing.) [Y]>

Footers or headings are added in-line with the message body whenever possible. However, if the footer or heading is encoded differently than the message body, and if imposing a single encoding will cause loss of characters, it will be added as an attachment. The system will always try to use the message body's encoding for the footer or heading. If that fails, and if the message body's encoding is USASCII, the system can try to edit the message body to use the footer's

```
or heading's encoding. Should the system try to impose the footer's
or headings's encoding on the message body? [N]> y
```

```
Behavior when modifying headers: Use encoding of message body
```

```
Behavior for untagged non-ASCII headers: Impose encoding of message
body. Behavior for mismatched footer or heading encoding: Try both
body and footer or heading encodings
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure multi-lingual settings.
```

localeconfig コマンドの詳細については、「[Configuring the Appliance to Receive Mail](#)」の章を参照してください。

通知テンプレート

通知テンプレートは、`notify()` および `notify-copy()` フィルタアクションで使用されます。通知テンプレートには、アンチウイルス通知により使用されるアンチウイルス関連の変数を含む非 ASCII テキストおよびアクション変数を含めることができます（「[Using Message Filters to Enforce Email Policies](#)」の章にある「[Action Variables](#)」を参照）。たとえば、`$Allheaders` アクション変数を使用して、元のメッセージのヘッダーを含めることができます。通知用の From: アドレスを設定できます。[アプライアンスに生成されるメッセージの返信アドレスの設定](#)を参照してください。

通知テンプレートを作成したら、コンテンツフィルタおよびメッセージフィルタから参照させることができます。次の図は、「grapewatchers@example.com」に「grape_text」通知が送信されるように notify-copy() フィルタ アクションを設定したコンテンツ フィルタを示しています。

図 1: コンテンツ フィルタによる通知の例

Edit Content Filter

Edit Filter	
Name:	grapecheck
Currently used by policies:	DEFAULT
Description:	Looking for grapes.
Order:	1
Apply filter:	<input checked="" type="radio"/> If one or more conditions match <input type="radio"/> Only if ALL conditions match
Conditions	
Select New Condition... Add Condition	
Condition	Delete
body-contains("grape")	
Actions	
Select New Action... Add Action	
Action	Delete
notify-copy ("grapewatchers@example.com", "Found one!", "", "grape_text")	
Cancel Submit	

アンチウイルス通知テンプレート

アンチウイルス通知テンプレートには、次の2つのタイプがあります。

- アンチウイルス通知テンプレート。アンチウイルス通知テンプレートは、元のメッセージがウイルス通知に添付されていない場合に使用されます。
- アンチウイルス コンテナ テンプレート。コンテナ テンプレートは、元のメッセージが添付ファイルとして送信される際に使用されます。

アンチウイルス通知テンプレートは、フィルタの代わりにアンチウイルス エンジンで使用される以外は、基本的に通知テンプレートと同様に使用されます。メール ポリシーの編集集中に送信するカスタム通知を指定できます。ウイルス対策通知用の From: アドレスを設定できます。詳細については、[アプライアンスに生成されるメッセージの返信アドレスの設定](#)を参照してください。

カスタム アンチウイルス通知テンプレート

次の図は、カスタム アンチウイルス通知が指定されたメール ポリシーを示しています。

図 2: メール ポリシーでのアンチウイルス コンテナ テンプレートの通知例

The screenshot shows the configuration for 'Virus Infected Messages' in a mail policy. The settings are as follows:

- Action Applied to Message:** Deliver as Attachment (RFC822) to New Message
- Archive Original Message:** Yes
- Modify Message Subject:** Prepend, with the value [WARNING : VIRUS DETECTED]
- Add Custom Header to Message:** No
- Container Notification:** anti_virus_container

アンチウイルス通知変数

ウイルス対策通知を作成する際に、次の表に記載されている通知変数を使用できます。

表 4: アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$AV_VIRUSES	メッセージで発見されたすべてのウイルスのリストに置き換えられます。 例: “Unix/Apache.Trojan”, “W32/Bagel-F”
\$AV_VIRUS_TABLE	パートごとに MIME-Part/Attachment 名とウイルスを示すテーブルに置き換えられます。 例: “HELLO.SCR”: “W32/Bagel-F” <unnamed part of the message>: “Unix/Apache.Trojan”
\$AV_VERDICT	アンチウイルスの判定に置き換えられます。

変数	置き換える値
\$AV_DROPPED_TABLE	ドロップされた添付ファイルのテーブルに置き換えられます。各行は、パートまたはファイル名とパートに付随するウイルスのリストにより構成されます。 例：“HELLO.SCR”：“W32/Bagel-f”, “W32/Bagel-d” “Love.SCR”：“Netsky-c”, “W32/Bagel-d”
\$AV_REPAIRED_VIRUSES	発見および修復されたすべてのウイルスのリストに置き換えられます。
\$AV_REPAIRED_TABLE	発見および修復されたすべてのパーツとウイルスのテーブルに置き換えられます。例：“HELLO.SCR”：“W32/Bagel-F”
\$AV_DROPPED_PARTS	ドロップされたファイル名のリストに置き換えられます。 例：“HELLO.SCR”, “CheckThisOut.exe”
\$AV_REPAIRED_PARTS	修復されたファイル名またはパートのリストに置き換えられます。
\$AV_ENCRYPTED_PARTS	暗号化されたファイル名またはパートのリストに置き換えられます。
\$AV_INFECTED_PARTS	ウイルスを含むファイルのファイル名のカンマ区切りリストに置き換えられます。
\$AV_UNSCANNABLE_PARTS	スキャンできなかったファイル名またはパートのリストに置き換えられます。
\$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
\$Time	現在の時刻（ローカル時間帯）に置き換えられます。
\$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを内部で識別するために使用するメッセージID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには \$Header を使用します）。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。

変数	置き換える値
\$Reputation	送信者の SenderBase レピュテーションスコアに置き換えられます。レピュテーションスコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名のカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイルタイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルサイズのカンマ区切りリストに置き換えられます。
\$remotehost	メッセージをEメールセキュリティアプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Eメールセキュリティアプライアンスのホスト名に置き換えられます。



(注) 変数名は大文字/小文字を区別しません。たとえば、テキストリソースで「\$to」と「\$To」は同等です。元のメッセージで「AV_」変数が空の場合、文字列 <None> で置き換えられます。

テキストリソースを定義した後、[メールポリシー (Mail Policies)] > [送受信メールポリシー (Incoming/Outgoing Mail Policies)] > [ウイルス対策設定を編集 (Edit Anti-Virus Settings)] ページまたは `policyconfig -> edit -> antivirus` コマンドを使用して、修復されたメッセージ、スキャンできなかったメッセージ、暗号化されたメッセージ、またはウイルスが陽性のメッセージに対して、元のメッセージがRFC 822のアタッチメントとして含まれるように指定します。詳細については、[カスタムアラート通知の送信](#)を参照してください。

バウンス通知および暗号化失敗通知テンプレート

バウンス通知および暗号化失敗通知テンプレートは、バウンス通知およびメッセージ暗号化失敗通知で使用される以外は、基本的に通知テンプレートと同様に使用されます。暗号化プロファイルを編集に、バウンスプロファイルおよびカスタムメッセージ暗号化失敗通知を編集していた場合に送信するカスタムバウンス通知を指定できます。

次の図は、バウンス プロファイルで指定されたバウンス通知テンプレートを示しています。

図 3: バウンス プロファイルのバウンス通知の例



(注) カスタム テンプレートを使用する場合は、RFC-1891 の DSN を使用してください。

次の図は、暗号化プロファイルで指定された暗号化失敗テンプレートを示しています。

図 4: 暗号化プロファイルの暗号化失敗通知の例

バウンス通知および暗号化失敗通知変数

バウンス通知または暗号化失敗通知を作成する際に、次の表に記載されている通知変数を使用できます。

表 5: バウンス通知変数

変数	置き換える値
\$Subject	元のメッセージの件名。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTTimeStamp	現在の時刻および日付 (GMT) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

変数	置き換える値
\$MID	メッセージを内部で識別するために使用するメッセージ ID (MID) に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには \$Header を使用します）。
\$BouncedRecipient	バウンスされた受信者のアドレス。
\$BounceReason	通知理由。
\$remotehost	メッセージを E メールセキュリティ アプライアンスに送信したシステムのホスト名に置き換えられます。

暗号化通知テンプレート

暗号化通知テンプレートは、アウトバウンド電子メールを暗号化するように Cisco 電子メール暗号化を設定した際に使用されます。この通知では、受信者が暗号化されたメッセージを受信したことを通知し、メッセージを読む手順を説明しています。暗号化メッセージと一緒に送信するカスタム暗号化通知を指定できます。暗号化プロファイルを作成する際は、HTML 形式およびテキスト形式の両方の暗号化通知を指定します。このため、カスタムプロファイルを作成する場合は、テキスト形式および HTML 形式の両方の通知を作成する必要があります。