

# 着信および発信コンテンツフィルタのベストプラクティスガイド

## 内容

### [概要](#)

### [手順の概要](#)

[ステップ 1：必要な辞書のインポート](#)

[ステップ 2：集中型隔離の作成](#)

[ステップ 3：着信コンテンツフィルタの作成](#)

[着信メールポリシーへの着信コンテンツフィルタの適用](#)

[ドメインのeBay & PaypalおよびSpooof Eメール保護のDKIM検証](#)

[ステップ 4：発信コンテンツフィルタの作成](#)

### [要約](#)

## 概要

コンテンツフィルタを使用すると、電子メールの複雑な詳細を調べ、電子メールに対してアクション（またはアクションなし）を実行できます。着信または発信コンテンツフィルタが作成されたら、着信または発信メールポリシーに適用します。いずれかの電子メールがコンテンツフィルタと一致すると、Cisco Eメールセキュリティアプライアンス(ESA)およびセキュリティ管理アプライアンス(SMA)の「コンテンツフィルタ」レポートに、コンテンツフィルタに一致するすべての電子メールが表示されます。したがって、何もアクションを実行しなくても、組織に出入りする電子メールの種類に関する有益な情報を取得する優れた方法であり、電子メールフローを「パターン化」できます。

コンテンツフィルタには「条件」と「アクション」が数多く存在するため、このドキュメントでは一般的で推奨される着信および発信コンテンツフィルタについて説明します。

## 手順の概要

### ステップ 1：必要な辞書のインポート

このドキュメントでは、着信および発信コンテンツフィルタのベストプラクティスを実装するために必要な手順について説明します。作成するコンテンツフィルタは、いくつかの辞書を参照します。したがって、まずそれらの辞書をインポートする必要があります。ESAには辞書が付属しており、作成するコンテンツフィルタで参照するために、それらを設定にインポートするだけで済みます。

### ステップ 2：集中型隔離の作成

ほとんどのコンテンツフィルタでは、「アクション」を作成し、指定されたカスタム（新）隔離に電子メール（または電子メールのコピー）を隔離するように設定します。したがって、SMA上で隔離を作成する必要があります esa および SMA。

### ステップ 3：着信および発信コンテンツフィルタの作成とポリシーへの適用

辞書をインポートして検疫を作成したら、着信コンテンツフィルタを作成し、着信メールポリシーに適用してから、発信コンテンツフィルタを作成し、発信メールポリシーに適用します。

## ステップ 1：必要な辞書のインポート

コンテンツフィルタで参照する辞書のインポート：

- ESAアプライアンスで、[Mail Policies] > [Dictionaries]に移動します。
- ページの右側にある「Import Dictionary」ボタンをクリックします。

収益性：

- 「IronPortアプライアンスの設定ディレクトリからインポート」を選択します。
- 「profanity.txt」を選択し、「次へ」をクリックします。
- 名前：Profity
- [Match whole words]をクリックします(非常に重要)。
- 用語を変更する (新しい用語を追加するか、不要な用語を削除する )
- [送信]をクリックします

性的なコンテンツ：


- 「IronPortアプライアンスの設定ディレクトリからインポート」を選択します。
- 「性内容.txt」を選択し、「次へ」をクリックします。
- 名前：性的内容
- [Match whole words]をクリックします(非常に重要)。
- 用語を変更する (新しい用語を追加するか、不要な用語を削除する )
- [送信]をクリックします

独自：

- 「IronPortアプライアンスの設定ディレクトリからインポート」を選択します。
- 「proprietary\_content.txt」を選択し、「次へ」をクリックします。
- 名前：プロプライテーター
- [Match whole words]をクリックします(非常に重要)。
- 用語を変更する (新しい用語を追加するか、不要な用語を削除する )
- [送信]をクリックします

## ステップ 2：集中型隔離の作成

- SMAで、[Email]タブ> [Message Quarantine] > [PVO Quarantines]に移動します
- これは、開始する前のQuarantinesテーブルの外観です。すべての隔離がデフォルトです。

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

- ・ポリシーの横の [レポート ( Report ) ] "ポリシー検疫の追加..." ボタン
- ・次の隔離を作成します。
- ・一部は着信コンテンツフィルタで使用され、一部は発信コンテンツフィルタで使用されます。同じ方法で作成します。

#### PVO隔離 – 着信コンテンツフィルタで使用

##### URL の悪意のあるインバウンド:

[Name] : URL の悪意のあるインバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### URLカテゴリ受信:

[Name] : URLカテゴリ受信  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### 銀行データインバウンド:

[Name] : 銀行データインバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### SSNインバウンド:

[Name] : SSNインバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### 不適切なインバウンド:

[Name] : 不適切なインバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### SPFハード障害:

[Name] : SPFハード障害  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### SPFソフト障害:

[Name] : SPFソフト障害  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### SpoofMail:

[Name] : SpoofMail  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### DKIMハード障害:

[Name] : DKIMハード障害  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### パスワード保護受信:

[Name] : Pwd Protected Inbound  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

#### PVO隔離 – 発信コンテンツフィルタで使用

##### 銀行データアウトバウンド:

[Name] : 銀行データ発信  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### SSNアウトバウンド:

[Name] : SSNアウトバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### 不適切なアウトバウンド:

[Name] : 不適切なアウトバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### 独自のアウトバウンド:

[Name] : 独自のアウトバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### URL の悪意のあるアウトバウンド:

[Name] : URL の悪意のあるアウトバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### URLカテゴリアウトバウンド:

[Name] : URLカテゴリアウトバウンド  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

##### Password Protected Outbound:

[Name] : Pwd Protected Outbound  
 保存期間 : 14 日  
 デフォルトのアクション : [削除 ( Delete ) ]  
 空き領域 : Enable

- ・すべてのPVO隔離を作成した後のPVOテーブルの外観を次に示します。

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Bank Data Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Bank Data Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
DKIM Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Inappropriate Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Inappropriate Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Proprietary Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Soft Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SpoofMail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
URL Category Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Category Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

*Available space for Policy, Virus & Outbreak quarantines is 33G.*

### ステップ 3 : 着信コンテンツフィルタの作成

辞書がインポートされ、PVO検査が作成されたら、着信コンテンツフィルタの作成を開始できます。

- [メールポリシー] > [受信コンテンツフィルタ]に移動します。
- 作成する必要がある着信コンテンツフィルタのテーブルを次に示します。たとえば、次の表は、最初の表の作成方法を示すスクリーンショットです。

#### これらの着信コンテンツフィルタの作成

[Name] : **Bank\_Data**

次の2つの条件を追加します。

メッセージ本文または添付ファイル :

スマートIDを含む : ABAルーティング番号

スマートIDを含む : クレジットカード番号

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「Bank Data Inbound ( 集中型 ) 」

重複メッセージ : 有効

( 適用ルールは「1つ以上の条件が一致する場合」である必要があります )

[Name] : **SSN**

条件を1つ追加 :

メッセージ本文または添付ファイル :

スマートIDを含む : 社会保障番号(SSN)

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「SSNインバウンド ( 集中型 ) 」

重複メッセージ：有効

[Name]：不適切

次の2つの条件を追加します。

メッセージ本文または添付ファイル：

辞書に用語が含まれています：下品

辞書に用語が含まれています：性的\_内容

アクションを1つ追加：

隔離：

メッセージを検査に送信：「不適切なインバウンド ( 集中型 )」

重複メッセージ：有効

[Name]：URL\_Category

条件を1つ追加：

URLカテゴリ：

カテゴリの選択：

大人、デート、フィルター回避、フリーウェアとシェアウェア、ギャンブル、ゲーム、ハッキング、ランジェリーと水着、性的でないヌード、パークされたドメイン、ピアファイル転送、ポルノ

アクションを1つ追加：

隔離：

メッセージを検査に送信：「URL Category Inbound ( 集中型 )」

重複メッセージ：有効

(注：このコンテンツフィルタでは、[セキュリティサービス]→[URLフィルタリング]を有効にする必要があります)

[Name]：URL\_Malicious

条件を1つ追加：

URLレピュテーション：

URLレピュテーション：悪意のある(-10.0 ~ -6.0)

アクションを1つ追加：

隔離：

メッセージを検査に送信：「URL Malicious Inbound ( 集中型 )」

重複メッセージ：無効(\*\*\*\*元の隔離\*\*\*\*)

[Name]：Password\_Protected

条件を1つ追加：

プロテクトされている添付ファイル:1つ以上の添付ファイルが保護されています

アクションを1つ追加：

隔離：

メッセージを検査に送信：「Pwd Protected Inbound ( 集中型 )」

重複メッセージ：有効

[Name]：サイズ\_10M

条件を1つ追加：

メッセージサイズ：

以上：1,000 万

アクションを1つ追加：

メッセージタグの追加：

[Term:NOOP

(注：何らかのアクションが必要なので、ここではメッセージを「タグ付け」して操作を行いません。コンテンツフィルタが「一致」していたという事実により、レポートに表示できません。レポートに表示する「アクション」は必要ありません)。

[Name] : SPF\_Hard\_Fail

条件を1つ追加 :

SPF検証 : 「is」失敗

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「SPFハード障害 ( 集中型 ) 」

重複メッセージ : 有効

(注 : 「is Fail」はハードSPF障害であり、ドメインの所有者から、SPFレコードにリストされていない送信者から受信したすべての電子メールをドロップするように指示されたことを意味します。最初は、「重複メッセージ」を使用し、元のメッセージを隔離する前に1週間か2週間の障害を確認することをお勧めします ( 重複メッセージをオフにします ) 。

[Name] : SPF\_Soft\_Fail

条件を1つ追加 :

SPF検証 : 「is」ソフトフェイル

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「SPFソフト障害 ( 集中型 ) 」

重複メッセージ : 有効

[Name] : DKIM\_Hardfail\_Copy

条件を1つ追加 :

DKIM認証 : ハードフェイル

次の2つのアクションを追加します。

ヘッダーの追加/編集 :

ヘッダー名 : Subject

[Prepend to the Value of Existing Header]をクリックし、次のように入力します。[コピー - リリースしない]"

隔離 :

メッセージを検査に送信 : 「DKIMハード障害 ( 集中型 ) 」

重複メッセージ : 有効

(注 : メッセージのコピーを最初に検査します)。

[Name] : DKIM\_Hardfail\_Original

条件を1つ追加 :

DKIM認証 : ハードフェイル

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「DKIMハード障害 ( 集中型 ) 」

重複メッセージ : Disabled

(注 : PayPalドメインとeBayドメイン用に別の受信メールポリシー行を作成し、DKIM検証に合格する必要があることが分かっているドメインに対してこのコンテンツフィルタを使用します)。

[Name] : Spoof\_SPF\_Failures

[One Condition]を追加しますが、[SOFTFAIL]と[Hardfail]の両方がオンになっています。

SPF検証 : 「is」ソフトフェイルと「Fail」をクリック

(したがって、[Softfail]と[Fail]の2つのチェックボックスをクリックしました)。

アクションを1つ追加 :

隔離 :

メッセージを検査に送信 : 「SpoofMail ( 集中型 ) 」

重複メッセージ : Enable

(注 : このコンテンツフィルタを使用して、自分のドメイン ( スプーフィング ) から送信する電子メールの着信に対するアクションを実行します。コピーを検査するアクションセットから開始し、SpoofMail検査を数週間確認した後、SPF TXT DNSレコードを変更してすべての正当な送信者を追加できます。また、ある時点で、重複メッセージチェックボックスを無効にして元のコンテンツフィルタを検査できます)。

例として、送信する前にBank\_Dataコンテンツフィルタが次のようになります。

Content Filter Settings	
Name:	Bank_Data
Currently Used by Policies:	Default Policy
Description:	
Order:	1 (of 7)

Conditions			
Add Condition...			Apply rule: If one or more conditions match
Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("**aba", 1)	
2	Message Body or Attachment	body-contains("**credit", 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Bank Data Inbound")	

すべての着信コンテンツフィルタを作成した後、テーブルは次のようになります。

Filters					
Add Filter...					
Order	Filter Name	Description	Rules	Policies	
1	URLMalicious	Not in use			
2	URLCategory	Not in use			
3	SPFHardFail	Not in use			
4	Bank_Data	Not in use			
5	SSN	Not in use			
6	Inappropriate	Not in use			
7	URL_Category	Not in use			
8	URL_Malicious	Not in use			
9	Password_Protected	Not in use			
10	Size_10M	Not in use			
11	SPF_Hard_Fail	Not in use			
12	SPF_Soft_Fail	Not in use			
13	DKIM_Hardfail_Copy	Not in use			
14	DKIM_Hardfail_Original	Not in use			
15	Spoof_SPF_Failures	Not in use			

Edit Filter Order...

「ポリシー」機能が選択され（中央のポリシーハイパーテキストが表示されます）、中央の列には、コンテンツフィルタが適用された受信メールポリシーが表示されます。どの着信メールポリシーにも適用されていないため、「Not in use」と表示されます。

### 着信メールポリシーへの着信コンテンツフィルタの適用

- 次のとおりに移動します。"[Mail Policies] > [Incoming Mail Policies]
- [Default Policy]の[Content Filters]セルの[Disabled]テキストをクリックします。
- プルダウンメニューのボタンは、[コンテンツフィルタを無効にする]に設定されています。
- ボタンをクリックし、[コンテンツフィルタを有効にする]に設定すると、作成されたすべての

着信コンテンツフィルタがすぐに表示されます。

- DKIM\_Hardfail\_OriginalとSpooof\_SPF\_Failuresを除くすべてのフィルタを有効にします。
- 「Submit」と「Commit」です。

## ドメインのeBay & PaypalおよびSpooof Eメール保護のDKIM検証

これら2つのトピックには、DKIM検証とSPF検証を利用するコンテンツフィルタが含まれます。したがって、まず、DKIMとSPFの両方の検証が有効になっていることを確認する必要があります。

### 1.メールフローポリシー内でDKIMとSPFの検証を有効にする

- 次のとおりに移動します。[Mail Policies] > [Mail Flow Policies]
- [Accept]の[Connection Behavior]を持つすべてのメールフローポリシー内で、DKIMとSPFの検証を有効にします。
- 下のハイパーテキスト「Default Policy Parameters」をクリックして、「DKIM Verification」を「On」に設定し、「SFP/SIDF Verification」を「On」に設定します。
- 「送信」と「コミット」をクリックします。
- [Mail Flow Policies]テーブルが表示されます。「Behavior」という名前の列を見て、「Behavior」を「Relay」に設定したメールフローポリシーを編集します
- これらのメールフローポリシーのDKIMとSPFの両方の検証を「オフ」にします。
- 「送信」と「コミット」をクリックします。

ESAがExchangeメールサーバから送信を受け取った電子メールのDKIMまたはSPF検証を実行しないようにします。ほとんどの設定では、「RELAYED」メールフローポリシーは、リレーの動作を持つ唯一の行です。

### 2. eBayおよびPaypalの新しい着信メールフローポリシーを作成します

eBayおよびPaypalから受信したインバウンド電子メールは、常にDKIM検証に合格する必要があります。したがって、これらのドメインからの電子メールにDKIM\_Hardfail\_Original Incoming Content Filterを使用する別の着信メールポリシーを作成します。

- 次のとおりに移動します。"[Mail Policies] > [Incoming Mail Policies]
- [ポリシーの追加]ボタンをクリックします。
- [Name: 「DKIM Hardfail Original」
- ポリシーの横の [レポート ( Report ) ] 「ユーザの追加...」 をクリックして、クエリーを実行します。

次の設定パネルでは、この新しい着信メールポリシーに一致するメッセージを定義できます。ここでは、[Sender] ( 設定パネルの左側 ) の基準だけを定義します。

- クリック 「次の送信者」 オプションボタンをクリックし、[電子メールアドレス]テーブルに「@」と入力します。[ebay.com](http://ebay.com), [@paypal.com](http://paypal.com)"



- ポリシーの横の [レポート ( Report ) ] “OK” ボタンをクリックします。
- クリック」 Submit”.

### 3. ドメインの新しい受信メールフローポリシーの作成 (スプーフィング保護)

このセクションの手順では、自分のドメインの[From]電子メールアドレスを持ち、SPFの検証に失敗している受信メールに対してアクションを実行できます。もちろん、これはDNSでSPFテキストレコードをすでに公開している場合に依存します。ドメインのSPFテキストリソースレコードを作成または公開していない場合は、これらの手順をスキップします。

- 次のとおりに移動します。"[Mail Policies] > [Incoming Mail Policies]
- [ポリシーの追加]ボタンをクリックします。
- [Name: 「Spoof\_Protection」
- ポリシーの横の [レポート ( Report ) ] 「ユーザの追加…」 をクリックして、クエリーを実行します。

次の設定パネルでは、この新しい[受信メールポリシー(Incoming Mail Policy)]行に一致するメッセージを定義できます。[Sender] ( 設定パネルの左側 ) の条件だけを定義します。

- ポリシーの横の [レポート ( Report ) ] 「次の送信者」 オプションボタンをクリックし、[電子メールアドレス:]テキストボックスにドメインを入力します。私にとって、私のドメインは "@unc-hamiltons.com"です

- クリック」 Submit”.

[受信メールポリシー(Incoming Mail Policies)]テーブルが再度表示されますが、[デフォルトポリシー(Default Policy)]の上に2番目の新しい[メールポリシー(Mail Policy)]行があります。

- 新しい行の[コンテンツフィルタ]セルの ( デフォルトを使用 ) ハイパーテキストをクリックし

ます。

- プルダウンメニューを[コンテンツフィルタ ( カスタマイズ設定 ) を有効にする]に切り替えま
- す。
- 「Spoof\_SPF\_Failures」をチェックして、「DKIM\_Hardfail\_Copy」と「DKIM\_Hardfail\_Original」の両方がチェックされていないことを確認します。
- [Submit]と[Commit changes]をクリックします。

[受信メールポリシー]テーブルは次のようになります。

Policies								
Add Policy...								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	DKIM Hardfail Original	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	
2	Spoof_Protection	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	
	Default Policy	IronPort Intelligent Multi-Scan Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	URLMalicious URLCategory SPFHardFail Bank_Data ...	Retention Time: Virus: 1 day	

## ステップ 4 : 発信コンテンツフィルタの作成

- [メールポリシー] > [送信コンテンツフィルタ]に移動します。
- 作成する必要がある発信コンテンツフィルタのテーブルを次に示します。

### これらの発信コンテンツフィルタの作成

[Name] : Bank\_Data

次の2つの条件を追加します。

メッセージ本文または添付ファイル :

スマートIDを含む : ABAルーティング番号

スマートIDを含む : クレジットカード番号

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「Bank Data Outbound ( 集中型 ) 」

重複メッセージ : 有効

( 適用ルールは「1つ以上の条件が一致する場合」である必要があります )

[Name] : SSN

条件を1つ追加 :

メッセージ本文または添付ファイル :

スマートIDを含む : 社会保障番号(SSN)

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「SSNアウトバウンド ( 集中型 ) 」

重複メッセージ : 有効

[Name] : 不適切

次の2つの条件を追加します。

メッセージ本文または添付ファイル :

辞書に用語が含まれています : 下品

辞書に用語が含まれています : 性的\_内容

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「不適切なアウトバウンド ( 集中型 ) 」

重複メッセージ : 有効

[Name] : URL\_Category

条件を1つ追加 :

URLカテゴリ :

カテゴリの選択 :

大人、デート、フィルター回避、フリーウェアとシェアウェア、ギャンブル、ゲーム、ハッキング、ランジェリーと水着、性的でないヌード、パークされたドメイン、ピアファイル転送、ポルノ

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「URL Category Outbound ( 集中型 ) 」

重複メッセージ : 有効

[Name] : URL\_Malicious

条件を1つ追加 :

URLレピュテーション :

URLレピュテーション : 悪意のある(-10.0 ~ -6.0)

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「URL Malicious Outbound ( 集中型 ) 」

重複メッセージ : 無効(\*\*\*\*元の隔離\*\*\*\*)

[Name] : Password\_Protected

条件を1つ追加 :

プロテクトされている添付ファイル:1つ以上の添付ファイルが保護されています

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「Pwd Protected Outbound ( 集中型 ) 」

重複メッセージ : 有効

[Name] : サイズ\_10M

条件を1つ追加 :

メッセージサイズ :

以上 : 1,000 万

アクションを1つ追加 :

メッセージタグの追加 :

[Term:NOOP

(注 : 何らかのアクションが必要なので、ここではメッセージを「タグ付け」して操作を行いません。コンテンツフィルタが「一致」していたという事実により、レポートに表示できます。レポートに表示する「アクション」は必要ありません)。

[Name] : 独自

条件を1つ追加 :

メッセージ本文または添付ファイル :

辞書に用語が含まれています : 独自

アクションを1つ追加 :

隔離 :

メッセージを検疫に送信 : 「独自 ( 中央集中型 ) 」

重複メッセージ : 有効

[Policies]機能が選択されている ( 中央の[Policies]ハイパーテキストが表示される ) ため、中央の列にコンテンツフィルタが適用されている発信メールポリシーが表示されます。送信メールポリシーに適用されていないため、[Not in use]が表示されます。

- 次のとおりに移動します。"[Mail Policies] > [Outgoing Mail Policies]
- デフォルトポリシーの[コンテンツフィルタ]セルの[無効]テキストをクリックします。
- プルダウンメニューのボタンは、[コンテンツフィルタを無効にする]に設定されます。
- ボタンをクリックし、[コンテンツフィルタを有効にする]に設定すると、作成されたすべての

発信コンテンツフィルタがすぐに表示されます。

- すべてのフィルタを「有効」にします。
- 「Submit」と「Commit」を選択します。

## 要約

これで、着信および発信コンテンツフィルタの初期ベストプラクティスが実装されました。ほとんどの（すべてではない）コンテンツフィルタは、検疫アクションを使用し、[重複メッセージ]オプションをチェック（有効）します。このオプションは、元の電子メールのコピーのみを配置し、電子メールの配信を妨げませんでした。これらのコンテンツフィルタの目的は、インバウンドとアウトバウンドを企業に流れる電子メールのタイプに関する情報を収集できるようにすることです。

ただし、コンテンツフィルタレポートを実行し、隔離に保存された電子メールコピーを調べた後、[重複メッセージ]チェックボックスをオフにして、コピー/複製ではなく元の電子メールを隔離に配置することを推奨します。