

# 反スパム、アンチウイルス、Graymail および発生フィルタ用の最良の方法 ガイド

## 目次

### [概要](#)

#### [スパム対策](#)

[フィーチャーキーを確認して下さい](#)

[インテリジェントな複数のスキャン \(IMS\) をグローバルに有効にして下さい](#)

[中央集中型スパム検疫を有効にして下さい](#)

[ポリシーの反スパムを設定して下さい](#)

#### [ウイルス対策](#)

[フィーチャーキーを確認して下さい](#)

[アンチウイルス スキャンを有効にして下さい](#)

[メール ポリシーのアンチウイルスを設定して下さい](#)

#### [グレイメール](#)

[フィーチャーキーを確認して下さい](#)

[Graymail を有効にすればセーフはサービスの定期講読を解除します](#)

[設定 Graymail およびセーフはポリシーで定期講読を解除します](#)

#### [アウトブレイク フィルタ](#)

[フィーチャーキーを確認して下さい](#)

[発生フィルタ サービスを有効にして下さい](#)

[ポリシーの発生フィルタを設定して下さい](#)

### [結論](#)

## 概要

メールを通して組織によって直面される大部分の脅威、不正侵入および迷惑はスパム、malware および混ぜられた不正侵入の形になります。組織を入力する前に Cisco の E メール セキュリティ アプライアンス (ESA) はゲートウェイでこれらの脅威を断ち切るために複数の異なるテクノロジーおよび機能が含まれています。この資料は受信および送信 メール フローの反スパム、Graymail および発生フィルタをアンチウイルス、設定するために最良の方法アプローチを記述したものです。

## スパム対策

反スパム 保護によってはスパムを含む既知脅威の全域が、phishing およびゾンビ不正侵入、またハードに検出 少量、[「419」](#)のような短命のメール脅威 [詐欺](#) 当たります。さらに、反スパム 保護はダウンロード URL が実行可能モジュールによって悪意のあるコンテンツを配信するスパム不正侵入のような新しく、展開混ぜられた脅威を識別します。

Cisco E メール セキュリティは次の反スパム ソリューションを提供します:

- IronPort 反スパム フィルタリング (IPAS)
- Cisco インテリジェントな複数のスキャン フィルタリング (IMS)

ESA の両方のソリューションを認可し、有効にすることができまされたり特定のメール ポリシーでしか 1 つを使用できません。この最良の方法 資料が、私達 IMS 機能を使用する行っているの為。

## フィーチャーキーを確認して下さい

- ESA で、システム 管理 > フィーチャーキーにナビゲートして下さい
- インテリジェント な複数のスキャン ライセンスを探し、確かめて下さいアクティブであることを。

## インテリジェント な複数のスキャン ( IMS ) をグローバルに 有効に して下さい

- ESA で、セキュリティ サービス > IMS および Graymail にナビゲートして下さい
- IMS グローバルな設定の Enablebutton をクリックして下さい:

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
<a href="#">Edit IMS Settings</a>	

- よくあるグローバルな設定を探し、グローバルな設定を『Edit』 をクリックして下さい
- 複数の設定を行うことができます。推奨 設定は下記のようにイメージで示されています:

Edit Common Global Settings	
Message Scanning Thresholds:	Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment. Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i> Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- Submitand を保存します変更をクリックして下さい。

IMS ライセンス サブスクリプションを持たなければ:

- セキュリティ サービス > IronPort 反スパムへのナビゲート
- IronPort 反スパム 概要の Enablebutton をクリックして下さい
- [グローバル設定の編集 ( Edit Global Settings ) ] をクリックします
- 複数の設定を行うことができます。推奨 設定は下記のようにイメージで示されています:

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> Enable IronPort Anti-Spam Scanning	
Message Scanning Thresholds:	Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment. Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i> Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<input type="radio"/> Normal <input checked="" type="radio"/> Aggressive <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i> <input type="radio"/> Regional (China)

- Cisco はブロッキング スパムの強い重点を望む顧客向けに積極的なスキャン プロファイルを

選択することを推奨します。

- Submitand を保存します変更をクリックして下さい

## 中央集中型スパム検疫を有効に して下さい

反スパムに検疫するために送信される オプションがあるのでスパム検疫が設定されるようにすることは重要です:

- セキュリティ サービス > スパム検疫へのナビゲート
- Configurebutton をクリックして次のページに連れて行きます。
- enablebox のチェックによって検疫を有効にし、SMANAMEAND IP アドレスで byfilling SecurityManagement アプライアンス ( SMA ) で中心になるべき検疫を指すことができます。 推奨 設定は下記のように示されています:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	<input type="text" value="centralized_spam"/> <small>(e.g. spam_quarantine)</small>
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: <input type="button" value="Quarantine"/>

- Submitand を保存します変更をクリックして下さい

設定および中央集中型検疫に関する詳細については、最良の方法 資料を参照して下さい:

[ESA からの SMA への中央集中型ポリシーのための最良の方法、ウイルスおよび発生検疫セットアップおよび移行](#)

## ポリシーの設定反スパム

インテリジェント な複数のスキャンがグローバルに設定されたら、今ポリシーを郵送するためにインテリジェント な複数のスキャンを適用できます:

- ポリシー > 着信メール ポリシーを郵送するナビゲート
- 着信メール ポリシーは IronPort 反スパム設定をデフォルトで使用します。
- 反スパムの下のブルー リンクをクリックすることはその特定のポリシーがカスタマイズされた反スパム設定を使用することができるように可能にします。
- あなたの下でカスタマイズされた反スパム設定を使用してデフォルトポリシーを示す例を参照します:

Policies								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

カスタマイズしたいポリシーのための反スパムの下のブルー リンクのクリックによる着信メールポリシーのカスタマイズ反スパム設定。

このポリシーのために有効に したい反スパム スキャン オプションを選択できます。

- この最良の方法 資料の目的で、使用 IronPort インテリジェント な複数のスキャンの隣で

Radio ボタンをクリックして下さい:

Anti-Spam Settings	
<b>Policy:</b>	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan Spam scanning built on IronPort Anti-Spam. <input type="radio"/> Disabled

次の 2 つのセクションは肯定的識別されたスパム設定および疑われたスパム設定が含まれています:

- 推奨される最良の方法はサブジェクトに追加される付加されたテキスト[スパム]で肯定的識別スパム設定の検疫操作を設定することです;
- 付加されたテキスト[疑われたスパム]が付いている Suspected スパム設定のための操作がサブジェクトに追加したように渡すために適用して下さい:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ↓ <small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>
Add Text to Subject:	Prepend ↓ [SPAM]
▶ Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver ↓ Send to Alternate Host (optional):
Add Text to Subject:	Prepend ↓ [SUSPECTED SPAM]
▶ Advanced	Optional settings for custom header and message delivery.

- スパム しきい値設定は変更することができ推奨 設定は 90 へ肯定的識別されたスパム スコア および 43 へ疑われたスパム スコアをカスタマイズすることです:

Spam Thresholds	
<small>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</small>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > 90 (50 - 100) Suspected Spam: Score > 50 (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > 90 (50 - 100) Suspected Spam: Score > 43 (minimum 25, cannot exceed positive spam score)

- Submitand を保存します変更をクリックして下さい

## ウイルス対策

アンチウイルス 保護は 2 つのサードパーティ エンジンを通して- Sophos および McAfee 提供されます。これらのエンジンはすべての既知悪意のある脅威を、設定されるようにそれらをきれいにするか、または検疫する廃棄フィルタリングします。

フィーチャーキーを確認して下さい

フィーチャーキーが両方ともおよびアクティブ 有効になることを確認するため:

- システム 管理 > フィーチャーキーに行ってください
- Sophos がアンチウイルスおよび McAfee ライセンス アクティブであることを確かめて下さい。

## アンチウイルス スキャンを有効に して下さい

- セキュリティ サービスへのナビゲート > アンチウイルス- Sophos
- Enablebutton をクリックして下さい。
- 自動更新が有効になり、Sophos アンチウイルス ファイル アップデートがうまく働いていることを確かめて下さい。必要ならば、ファイル アップデートをすぐに始めるために『Update now』 をクリックして下さい:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled

[Edit Global Settings...](#)

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available

No updates in progress. [Update Now](#)

- Submitand を保存します変更をクリックして下さい。

McAfee ライセンスが同様にアクティブである場合、> アンチウイルス- McAfee はセキュリティ サービスにナビゲート します

- Enablebutton をクリックして下さい。
- 自動更新が有効になり、McAfee アンチウイルス ファイル アップデートがうまく働いていることを確かめて下さい。必要ならば、ファイル アップデートをすぐに始めるために『Update now』 をクリックして下さい。
- Submitand を保存します変更をクリックして下さい

## メール ポリシーのアンチウイルスを設定して下さい

着信メール ポリシーで、以下は推奨されます:

- ポリシー > 着信メール ポリシーを郵送するナビゲート
- カスタマイズしたいポリシーのためのアンチウイルスの下のブルー リンクのクリックによる着信メール ポリシーのカスタマイズ アンチウイルス設定。
- このポリシーのために有効にしたいアンチウイルス スキャン オプションを選択できます。
- この最良の方法 資料の目的で、アンチウイルス McAfee および Sophos を両方選択して下さい:

Anti-Virus Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Anti-Virus Scanning for This Policy:</b>	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

- ファイルを修理するように試みません従ってメッセージ スキャンはウイルスのためのただスキャンに残ります:

Message Scanning	
	Scan for Viruses only ▾ <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS REMOVED]
▶ Advanced	Optional settings for custom header and message delivery.

- 暗号化されたおよび Unscannable メッセージのための推奨 処置は注意のための修正された件名との現状のまま渡すことです。
- ウイルス対策のための推奨されるポリシーは下記のようにイメージに示すようにドロップするすべてのウイルス感染した メッセージです:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- Submitand を保存します変更をクリックして下さい

同じようなポリシーは発信 メール ポリシーのためにが推奨されます、送信 メール の件名を修正することを推奨しません。

## グレイメール

Eメールセキュリティ アプライアンスの graymail マネジメントソリューションは 2 つのコンポーネントで構成します: 統合された graymail スキャン エンジンおよびクラウド ベースはサービスの定期講読を解除します。 graymail マネジメントソリューションは組織が統合された graymail エンジンを使用して graymail を識別するようにし、適切なポリシー制御を加え、不必要なメッセージのを使用して定期講読を解除するためにエンドユーザ用の容易なメカニズムを提供することはサービスの定期講読を解除します。

Graymail カテゴリはマーケティング メール、社会的ネットワーク メールおよびバルク メールが含まれています。 詳細オプションはカスタム ヘッダーを付加すること、代替ホストへの送信およびメッセージをアーカイブすることが含まれています。 この最良の方法に関しては、Graymail のセーフを定期講読を解除しますデフォルト メール ポリシーのための機能の有効に します。

## フィーチャーキーを確認して下さい

- ESA で、システム 管理 > フィーチャーキーにナビゲート して下さい
- Graymail 安全な Unsubscription を探し、確かめて下さいアクティブであることを。

## Graymail を有効に すればセーフはサービスの定期講読を解除します

- セキュリティ サービス > IMS への ESA、ナビゲート および Graymail
- Graymail グローバルな設定の編集 Graymail Settingsbutton をクリックして下さい
- 選択して下さいすべてのオプション- Graymail 検知を有効にして下さい、イネーブル セーフは自動更新の定期講読を解除し、有効に します:

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates (?)	Enabled

[Edit Graymail Settings](#)

- Submitand を保存します変更をクリックして下さい

## Graymail を設定すればセーフはポリシーで定期講読を解除します

Graymail およびセーフ Unsubscribe グローバルに設定されたら、今ポリシーを郵送するためにこれらのサービスを適用できます。

- ポリシー > 着信メール ポリシーを郵送するナビゲート
- Graymail の下のブルー リンクをクリックすることはその特定のポリシーが Graymail カスタマイズされた設定を使用することができるよう可能に します。
- このポリシーのために有効に したい Graymailoptions を選択 できます。
- この最良の方法 資料の目的で、Radio ボタンをこのポリシーのためのイネーブル Graymail 検出の隣でクリックし、このポリシーのために定期講読を解除する Graymail を有効に して下さい:

Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Perform this action for:	<input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

次の3つのセクションはマーケティングメール設定の処理、社会的ネットワークメール設定の処理およびバルクメール設定の処理が含まれています。

- 推奨される最良の方法はすべてを有効にし、付加されて下記に示されているようにカテゴリに関してサブジェクトに追加されるテキストとの操作のように渡します残ることです:

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
▶ Advanced	Optional settings for custom header and message delivery.

- Submitand を保存します変更をクリックして下さい

発信 Mail ポリシーは Graymail を無効状態に残ってもらうはずでずです。

## アウトブレイク フィルタ

発生フィルタは正しく本当スパム カテゴリ-たとえば、phishing メールおよび詐欺メールの外部で落ち、ユーザ通知か検疫とそれらを適切に処理する項目をタグ付けするために反スパム エンジンのトリガーを、URL スキャンおよび検出 テクノロジー等々結合します。

### フィーチャーキーを確認して下さい

- ESA で、システム 管理 > フィーチャーキーにナビゲートして下さい
- 発生フィルタを探し、それがアクティブであることを確かめて下さい。

### 発生フィルタ サービスを有効に して下さい

- ESA で、セキュリティ サービス > 発生フィルタにナビゲートして下さい
- 発生フィルタ 概要の Enablebutton をクリックして下さい
- 複数の設定を行うことができます。 推奨 設定は下記のようにイメージで示されています:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> <b>Enable Outbreak Filters</b>	
Adaptive Rules:	<input checked="" type="checkbox"/> <b>Enable Adaptive Rules</b>
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> <b>Receive Emailed Alerts</b>
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> <b>Enable Web Interaction Tracking</b>

• Submitand を保存します変更をクリックして下さい。  
ポリシーの発生フィルタを設定して下さい

発生 Filtershas がグローバルに設定されて、今この機能 tomail ポリシーを適用できれば。

- ポリシー > 着信メール ポリシーを郵送するナビゲート
- 発生フィルタの下のブルー リンクをクリックすることはその特定のポリシーがカスタマイズされた発生フィルタ設定を使用することができるようになります。
- この最良の方法 資料の目的で、デフォルト値を用いる発生フィルターの設定を保存します:

Outbreak Filter Settings	
Quarantine Threat Level: (?)	<input type="text" value="3"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="text" value="1"/> Days Other Threats: <input type="text" value="4"/> Hours <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- 発生フィルタは悪意のある、疑わしいですかまたは phish 考えられる場合 URL を書き換えることができます。URL によって基づく脅威を検出する、書き換えるためにメッセージ修正を『Enable』を選択して下さい。
- URL 書き換えオプションが示されている続くことようにすべてのメッセージのためのイネーブルあることを確かめて下さい:

Message Modification	
<input checked="" type="checkbox"/> <b>Enable message modification. Required for non-viral threat detection (excluding attachments)</b>	
Message Modification Threat Level: (?)	<input type="text" value="3"/>
Message Subject:	Prepend <input type="text" value="[[Possible \$threat_category Fraud]]"/> <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> <b>Disable</b>
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> <b>Disable</b>
Alternate Destination Mail Host (Other Threats only):	<input type="text"/>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> <b>Enable for all messages</b> <input type="radio"/> Disable
Bypass Domain Scanning (?)	<input type="text"/>
Threat Disclaimer:	<input type="text" value="System Generated"/> <a href="#">Preview Disclaimer</a> <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to <a href="#">Mail Policies &gt; Text Resources &gt; Disclaimers</a></small>

• Submitand を保存します変更をクリックして下さい  
発信 Mail ポリシーは発生フィルタを無効状態に残ってもらうはずで。

## 結論

この資料は E メール セキュリティ アプライアンス ( ESA ) で反スパム、アンチウイルスを、Graymail および発生フィルタ用のデフォルト、か最良の方法 コンフィギュレーション記述することを向けました。これらのフィルターすべては受信および送信 メール ポリシーで利用可能であり、設定およびフィルタリングは両方で推奨されます-保護のバルクが受信のためである間、送信フローをフィルタリングすることは中継で送られたメールが内部 悪意のある不正侵入に対して保護を提供します。