

EメールセキュリティアプライアンスおよびクラウドEメールセキュリティでEメールをアーカイブする方法

内容

[概要](#)

[背景説明](#)

[ESAおよびCESで電子メールをアーカイブする方法](#)

[アンチスパムアーカイブの設定](#)

[アンチウイルスアーカイブの設定](#)

[高度なマルウェア防御アーカイブの設定](#)

[Graymailアーカイブの設定](#)

[メッセージフィルタアーカイブの設定](#)

[アーカイブ・メールボックス・ログの可用性の検証](#)

[Mboxログの取得](#)

[関連情報](#)

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)およびクラウドEメールセキュリティ(CES)で取得および確認のためにEメールをアーカイブする手順について説明します。

背景説明

ESAおよびCESで電子メールをアーカイブする場合、規制要件を満たすか、メールの診断とレビューを行うための追加のデータ手段を提供するために使用できます。電子メールのアーカイブは、管理者が取得および検証するために、メールボックスのログ形式で電子メールのセカンダリストレージとして機能します。

- 電子メールのアーカイブを有効にする場合は、設定をデフォルト値のままにすることを推奨します。デフォルト値は、ログごとに10 MBで、ログの最大保存数は10です。ログは、ログファイル自体のサイズに基づいて引き続き追加およびロールオーバーされます。アーカイブmboxログファイルは、アプライアンスを通過する電子メールトラフィックのレートに基づいて記録されます。より多くのログが作成されると、古いアーカイブ・メールボックス・ログが削除され、新しいログを作成するための空き領域が確保されます。
- アーカイブmboxログファイルのサイズと保持されるログファイルの最大数を増やす前に、デバイスに十分なディスク領域があることを確認してください。
- アーカイブmboxログの生成を停止するには、ポリシーごとにアーカイブ機能を無効にする必要があります。

注：ESAおよびCESアーカイブmboxログは、Security Management Appliance(SMA)では取得できず、機能が有効な状態で各ESAおよびCESごとにローカルに保存されます。


ESAおよびCESで電子メールをアーカイブする方法

電子メールのアーカイブは、アンチスパム、アンチウイルス、高度なマルウェア保護、グレイメールおよびメッセージフィルタで利用できます。アーカイブのアクションは、グラフィカルユーザーインターフェイス(GUI)またはコマンドラインインターフェイス(CLI)を使用してアンチスパム、アンチウイルス、高度なマルウェア保護、およびメールを設定できます。

メッセージフィルタの場合、アーカイブアクションはCLIのみを使用して設定できます。


アンチスパムアーカイブの設定

1. [GUI] > [Mail Policies] > [Incoming/Outgoing Mail Policies]に移動します。
2. 各ポリシーの[Anti-spam settings]をクリックして、電子メールアーカイブを設定します。
3. [Positively Identified Spam Settings]または[Suspected Spam]設定で使用可能な設定で[Advanced]をクリックします。
4. [Yes]の横にあるオプションボタンを押して、対応するアンチスパム判定を含む電子メールをアーカイブします。
5. 設定を送信し、図に示すように、これらの変更を確定します。

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ▼ <small>Note: If local and external quarantines are defined, mail will be</small>
Add Text to Subject:	Prepend ▼ [SPAM]
▼ Advanced	
Add Custom Header (optional):	Header: <input type="text"/> Value: <input type="text"/>
Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> <small>(e.g. employee@company.com)</small>
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

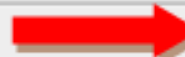
アンチウイルスアーカイブの設定

1. [GUI] > [Mail Policies] > [Incoming/Outgoing Mail Policies]に移動します。
2. それぞれのポリシーの[Anti-virus settings]をクリックして、電子メールアーカイブを設定します。
3. 元のメッセージをアーカイブする各スキャンバージョンで、[Yes]の横にあるオプションボタンを押してアーカイブします。
4. 設定を送信し、図に示すように、これらの変更を確定します。

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

高度なマルウェア防御アーカイブの設定

1. [GUI] > [Mail Policies] > [Incoming/Outgoing Mail Policies]に移動します。
2. それぞれのポリシーの[Advanced Malware Protection]設定をクリックして、電子メールアーカイブを設定します。
3. 元のメッセージをアーカイブするために必要な各スキャンバーデットで、[はい]の横にあるオプションボタンを押してアーカイブを行います。
4. 設定を送信し、図に示すように、これらの変更を確定します。

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
 Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<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: MALWARE DETECTED]

Graymailアーカイブの設定

1. [GUI] > [Mail Policies] > [Incoming/Outgoing Mail Policies]に移動します。
2. それぞれのポリシーの[Graymail settings]をクリックして、電子メールのアーカイブを設定します。
3. [マーケティング]、[ソーシャル]、[バルク]で使用可能な設定をクリックします。
4. [Yes]の横にあるオプションボタンを押して、対応するGraymail判定で電子メールをアーカイブします。
5. 設定を送信し、これらの変更を確定します。

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	Add Custom Header (optional): Header: <input type="text"/> Value: <input type="text"/>
	Send to an Alternate Envelope Recipient (optional): Email Address: <input type="text"/> (e.g. employee@)
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

メッセージフィルタアーカイブの設定

注:アーカイブされたログを表示するには、アーカイブアクションを含むメッセージフィルタが必要です。メッセージフィルタは、CLI内でのみ作成できます。

サンプルフィルタ：

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. CLIでデバイスにログインします。
2. 提供されているサンプルフィルタに示されているように、メッセージフィルタを作成します。
3. このフィルタを送信し、変更を確定します。

アーカイブ・メールボックス・ログの可用性の検証

アーカイブの設定が各サービスにコミットされると、アーカイブされた電子メールはmbox形式のログファイルに保存されます。アーカイブ・ログを取得できるかどうかを確認するには、[GUI] > [System Administration] > [Log Subscriptions]に移動します。

セキュリティサービスアーカイブは、図に示すように、アーカイブログタイプを持つ別のログを作成します。

Configured Log Subscriptions			
Add Log Subscription...			
Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/ ←	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/ ←	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/ ←	None

メッセージ・フィルタの場合、アーカイブ構成はCLIからのみ表示されます。

• Filters > Logconfig

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
-----
Log Name      Log Type      Retrieval      Interval
-----
1. Test       Filter Archive Logs  Manual Download  None
```

Mboxログの取得

スタンドアロンアプライアンスの場合、これらのmboxログはGUIから直接取得できます。[GUI] > [System Administration] > [Log Subscriptions]に移動し、取得する各アーカイブ・ログの[Log Files]をクリックします。

クラスタ化されたアプライアンスの場合、mboxログは、この記事で説明されているFTP/Secure Copy(SCP)を使用して取得**できます**。(https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)

関連情報

- [Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド](#)
- [UNIX mbox \(メールボックス\) 形式とは何ですか。](#)
- [Cisco Eメールセキュリティアプライアンス\(ESA\)のログの保存場所と、それらのログへのアクセス方法](#)
- [アーカイブ・メールボックス・ログからメールを抽出する方法](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)