データ損失防止：分類ミスおよびスキャン障害のトラブルシューティング

内容

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)のデータ損失防止(DLP)に関連する誤分類およびスキャン障害（ミス）のトラブルシューティングに関する一般的な方法について説明します。

前提条件

- AsyncOS 11.x以降を実行するESA。
- DLP機能キーがインストールされ、使用中です。

重要な情報

ESAのDLPは、有効にしてポリシーを作成し、機密データのスキャンを開始できるという意味でプラグアンドプレイに対応していることに注意することが重要です。ただし、最適な結果が得られるのは、会社固有の要件に合わせてDLPを調整した後だけであることにも注意してください。これには、DLPポリシーの種類、ポリシーのマッチングの詳細、重大度の調整、フィルタリング、追加のカスタマイズなどが含まれます。

違反と違反なしログの例

メールログやメッセージトラッキングに表示されるDLP違反の例をいくつか示します。ログラインには、タイムスタンプ、ログレベル、MID番号、違反または違反なし、重大度とリスク要因、および一致したポリシーが含まれます。

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP
```

```
policy match: 'US HIPAA and HITECH'.

Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy
match: 'US State Regulations (Indiana HB 1101)'.
```

違反が見つからない場合は、メールログまたはメッセージトラッキングが単にDLP違反を*記録します*。

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

トラブルシューティングチェックリスト

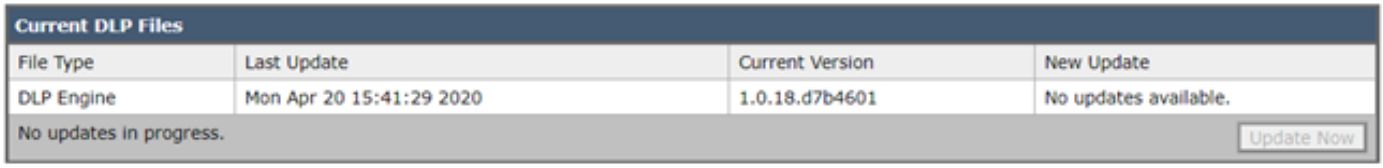
DLPの誤分類またはスキャンの失敗/ミスを処理する際に確認できる一般的な項目を次に示します。

> **注**：これはすべてを網羅したリストではありません。ご希望の内容がございましたら、Cisco TACまでお問い合わせください。

DLPエンジンのバージョンの確認

DLPエンジンのアップデートはデフォルトでは自動的に行われないため、最新の拡張機能やバグ修正を含む最新バージョンを実行していることを確認することが重要です。

GUIの[Security Services] の[Data Loss Prevention] に移動して、現在のエンジンバージョンを確認し、更新プログラムが利用可能かどうかを確認できます。更新が可能な場合は、[今すぐ更新]をクリックして*更新*を実行できます。

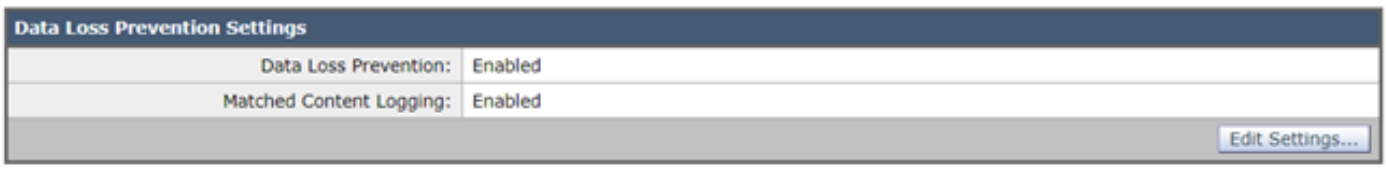


一致したコンテンツロギングの有効化

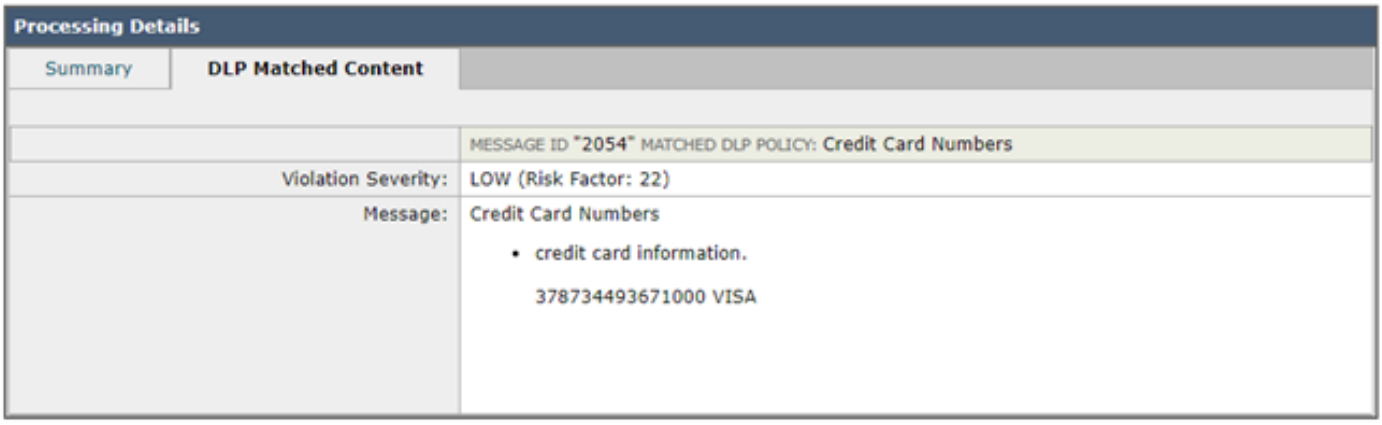
DLPには、DLPポリシーに違反するコンテンツを、周囲のコンテンツとともにログに記録するオプションがあります。このデータはメッセージの追跡で表示でき、特定の違反を引き起こしている可能性がある電子メール内のコンテンツを追跡できます。

> **注意**：有効にした場合、このコンテンツにはクレジットカード番号や社会保障番号などの機密データが含まれる可能性があることを知っておくことが重要です。

GUIの[Security Services]の下の[*Data Loss Prevention*]に移動して、*[Matched Content Logging]*が有効になっているかどうかを確認できます。



メッセージトラッキングに表示される一致したコンテンツロギングの例

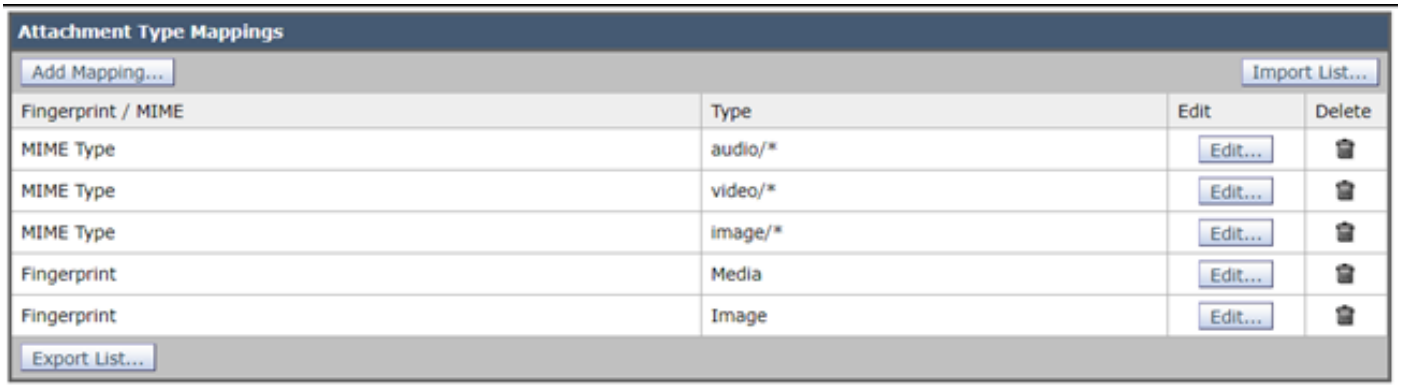


スキャン動作設定の確認

ESAのスキャン動作の設定は、DLPスキャンの背後にある機能にも影響します。次のスクリーンショットを例として見ると、添付ファイルの最大スキャンサイズが**5Mに設定されている場合**は、それ以上の場合はDLPスキャンが失われる可能性があります。また、MIMEタイ**プ設定を含む添付ファイル**に対するアクションも、確認する共通アイテムです。リストされているMIMEタイプがスキップされ、その他すべてがスキャンされるように、**Skip**のデフォルトに設定する必要があります。代わりにScanに設定されている場合は、テーブルにリストされている*MIMEタイプのみ*スキャンします。

同様に、ここに示した他の設定はDLPスキャンに影響を与える可能性があり、添付ファイルや電子メールの内容に応じて考慮する必要があります。

GUIの[Security Services] で[Scan Behavior]に移動するか、CLIで*scanconfigコマンドを実行*して移動できます。

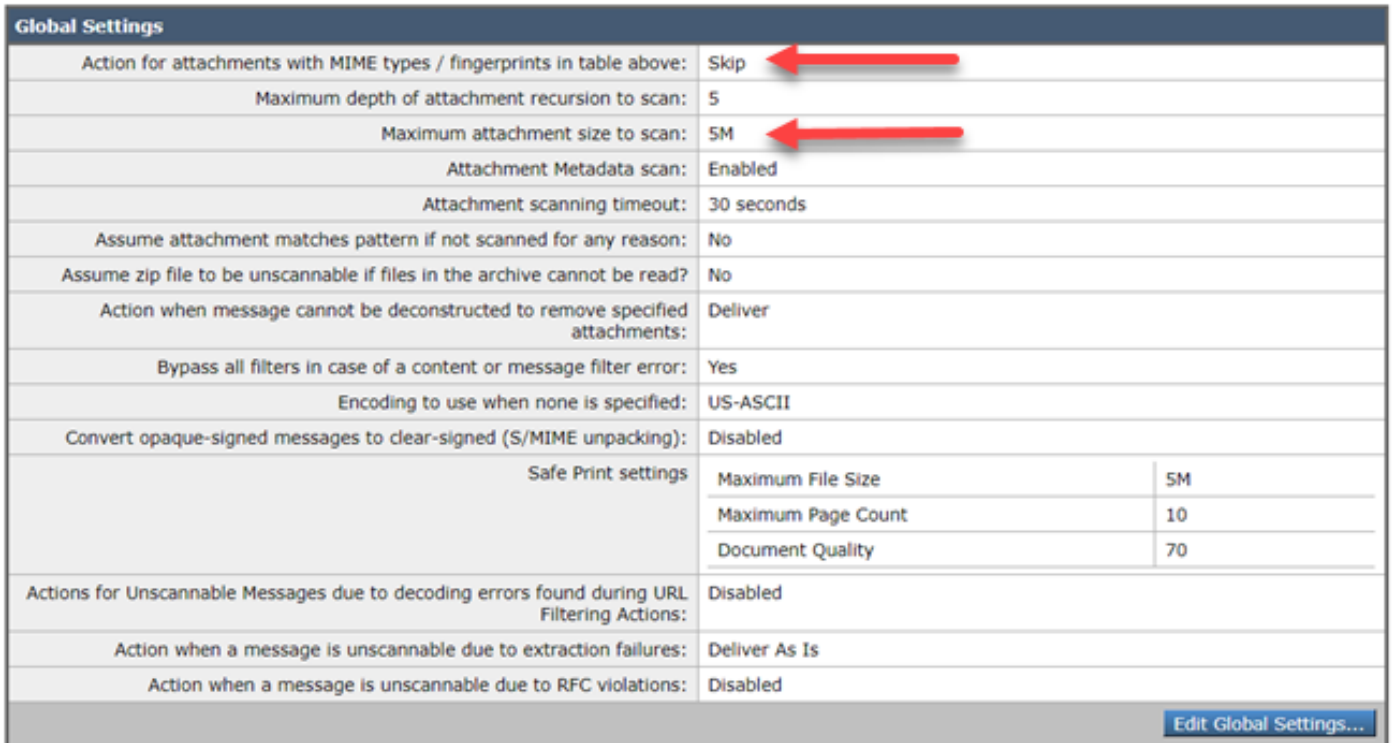


Attachment Type Mappings

Add Mapping... | Import List...

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Export List...



Global Settings

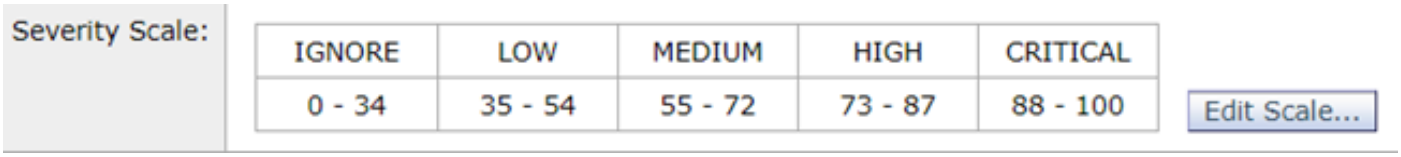
Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	Maximum File Size: 5M Maximum Page Count: 10 Document Quality: 70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

重大度スケール設定の確認

ほとんどの環境では、デフォルトの重大度スケールのしきい値で十分です。ただし、False Negative(FN)またはFalse Positive(FP)のマッチングをサポートするように修正する必要がある場合は、修正できます。また、新しいダミーポリシーを作成して比較することにより、推奨されるデフォルトのしきい値を使用していることを確認することもできます。

> **注**：事前定義されたポリシー（米国のHIPAAとPCI-DSSなど）によってスケールが異なります。



Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

[送信者と受信者のフィルタ]フィールドに追加された電子メールアドレスの確認

これらのフィールドに入力したエントリが、送信者または受信者の電子メールアドレスの正しい大文字と小文字に一致していることを確認します。[送信者と受信者のフィルタ]フィールドでは、大文字と小文字**が区別されます**。DLPポリシーは、電子メールアドレスがメールクライアントで「TestEmail@mail.com」のように表示され、これらのフィールドに「testemail@mail.com」と入力されている場合はトリガーされません。

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
- データ損失防止とは
- ESA で HIPAA ポリシーをテストするための DLP 違反のトリガー