# ESA で HIPAA ポリシーをテストするための DLP 違反のトリガー

## 目次



## 概要

Cisco E メール セキュリティ アプライアンス（ESA）の発信 メール ポリシーの DLP を有効にしたらこの資料に健康保険移植性および責任能力行為（HIPAA）データ損失防止（DLP）をテストする方法を記述されています。

## HIPAA ポリシーをテストするために DLP 違反を引き起こして下さい

この技術情報は ESA の DLP ポリシーに対してテストするために個人を保護するために修正された実質コンテンツを提供します。 この情報は経済的な、臨床健全性（HITECH） DLP ポリシーのための HIPAA およびヘルス情報 テクノロジーで引き起こすように設計され、また社会保障番号（SSN）のような他の DLP ポリシーを、CA AB-1298、CA SB-1386、等引き起こします。 ESA によってテスト電子メールを送信 するか、または**トレース** ツールを使用するとき情報を使用して下さい。

> **注:** 太字ところで出力で有効なか一般に誤用された SSN を使用して下さい。

> **注:** HIPAA および HITECH DLP ポリシーに関しては、お勧めのでカスタマイズされた識別番号を設定したようにして下さい。 忍耐強い識別番号（推奨されるカスタマイゼーション）または米国 National プロバイダ 識別子または米国社会保障番号およびヘルスケア辞書。きちんと引き起こすためにこれを設定してもらわなければなりません。

```
Procedure Notes
Progress Notes
Archie M Johnson Tue Jun 30, 2009 10:31 AM Pended
June 30, 2009
Patient Name: Gina, Lucas DOB: 01/23/1945
Telephone #: (559) 221-2345
SS#: [[[PLACE SSN HERE]]]
--------------------------------------------------------------------------------
Insurance: UHC
How was the patient referred to the office: *** ({:20})
Is a family member currently being seen by the requested physician? {YES/NO:63}
If yes, what is the family members name : ***
Previous PCP / Medical Group? ***
Physician Requested: Dr. ***
```

```
REASON:
1) Get established, no current problems: {YES/NO:63}
2) Chronic Issues: {YES/NO:63}
3) Specific Problems: {YES/NO:63}
Description of specific problem and/or chronic conditions:
{OPMED SYMPTOMS:11123} the problem started {1-10:5044} {Time Units:10300}.
Any Medications that may need a refill? {YES/NO:63}
Current medications: ***
--------------------------------------------------------------------------------
Archie M Johnson
Community Health Program Assistant Chief
Family Practice & Community Medicine
(559) 221-1234
Lucas Gina Wed Jul 8, 2009 10:37 AM Pended
ELECTIVE NEUROLOGICAL SURGERY
HISTORY & PHYSICAL
CHIEF COMPLAINT: No chief complaint on file.
HISTORY OF PRESENT ILLNESS: Mary A Xxtestfbonilla is a ***
Past Medical History
Diagnosis Date
• Other Deficiency of Cell-Mediated Immunity
Def of cell-med immunity
• Erythema Multiforme
• Allergic Rhinitis, Cause Unspecified
Allergic rhinitis
• Unspecified Osteoporosis 12/8/2005
DEXA scan - 2003
• Esophageal Reflux 12/8/2005
priolosec, protonix didn't work, lost weight
• Primary Hypercoagulable State
MUTATION FACTOR V LEIDEN
• Unspecified Glaucoma 1/06
• OPIOID PAIN MANAGEMENT 1/24/2007
Patient is on opioid contract - see letter 1/24/2007
• Chickenpox with Other Specified Complications 2002
```

# 確認

結果は DLP ポリシーのために設定 したメッセージ アクションに基づいて、変わります。 GUI からの確認が付いているアプライアンスのための操作を設定し、確認して下さい: **ポリシー > DLP ポリシー カスタマイズ > メッセージ アクションを郵送して下さい**。

この例では DLP 違反をポリシー検疫に検疫し、「付加のメッセージ 件名を修正する、**デフォルト アクションは**また[DLP 違反]」設定 されます。

**mail_logs は**テスト電子メールとして前のコンテンツを送信 するときこれに類似したのようである必要があります:

```
Wed Jul 30 11:07:14 2014 Info: New SMTP ICID 656 interface Management (172.16.6.165)
address 172.16.6.1 reverse dns host unknown verified no
Wed Jul 30 11:07:14 2014 Info: ICID 656 RELAY SG RELAY_SG match 172.16.6.1 SBRS
not enabled
Wed Jul 30 11:07:14 2014 Info: Start MID 212 ICID 656
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 From: <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 RID 0 To: <test_person@cisco.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 Message-ID
'<A85EA7D1-D02B-468D-9819-692D552A7571@gmail.com>'
Wed Jul 30 11:07:14 2014 Info: MID 212 Subject 'My DLP test'
Wed Jul 30 11:07:14 2014 Info: MID 212 ready 2398 bytes from <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 matched all recipients for per-recipient
policy DEFAULT in the outbound table
```

```
Wed Jul 30 11:07:16 2014 Info: MID 212 interim verdict using engine: CASE spam
negative
Wed Jul 30 11:07:16 2014 Info: MID 212 using engine: CASE spam negative
Wed Jul 30 11:07:16 2014 Info: MID 212 interim AV verdict using Sophos CLEAN
Wed Jul 30 11:07:16 2014 Info: MID 212 antivirus negative
Wed Jul 30 11:07:16 2014 Info: MID 212 Outbreak Filters: verdict negative
Wed Jul 30 11:07:16 2014 Info: MID 212 DLP violation
Wed Jul 30 11:07:16 2014 Info: MID 212 quarantined to "Policy" (DLP violation)
Wed Jul 30 11:08:16 2014 Info: ICID 656 close
```

**トレース** ツールから、メッセージ ボディで前のコンテンツを使用するときこのイメージのようにリストされている結果が表示されるはずです:

| Data Loss Prevention Processing | |
|---|---|
| Result: | Matches Policy: HIPAA and HITECH<br>Violation Severity: LOW (Risk Factor: 22) |
| Actions: | replace-header("Subject", "[DLP VIOLATION] $subject")<br>quarantine("Policy") |

# トラブルシューティング

**メール ポリシー >** GUI の **DLP Policy Manager > Add DLP ポリシー**から必要な DLP ポリシーを...選択したようにして下さい。

DLP ポリシーを追加されるように検討し、コンテンツ一致する分類子を規定 したこと、そして正規表現 パターンが有効であることを確認して下さい。 また**関連ワードまたは句**セクション**が設定されているおよび一致が**あることを確認して下さい。 分類子は DLP エンジンの検出コンポーネントです。 彼らは組み合せで使用されるか、またはそれぞれ敏感なコンテンツを識別できます。

> **注:** あらかじめ定義された分類子は uneditable です。

コンテンツに基づいて DLP トリガーを見ない場合また**メール ポリシーを > 発信 メール ポリシー > DLP** 検討し、必要な DLP ポリシーを有効に してもらうことを確認して下さい。

# 関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- ESA に関する FAQ： ESA によるメッセージの処理方法をデバッグするにはどうすればよいですか。
- SSA.gov: 誤用された社会保障番号
- オンライン regex テスト担当者
- テクニカルサポートとドキュメント - Cisco Systems