

トレース機能でのフィルタ確認方法

株式会社ネットワークバリューコンポネンツ

エンジニアリング部 第二グループ

Ironport アプライアンスには、実際にメールを流さなくても設定したフィルタ類やAntiSPAM/AntiVirusの動作を確認する“トレース”機能が搭載されています。

トレース機能は GUI/CLIの両方で利用できますが、本解説書では GUIでの利用を次ページから説明致します。

※なお、現在の7.x台のOSではIncomingrelayの機能を利用した場合、このトレース機能では正しい結果が得られない事象を確認しておりますので Incomingrelayを使った環境の場合は実際にメールを流して確認する方法をお取りください。

モニター	メールポリシー	セキュリティサービス	ネットワーク	システム管理
------	---------	------------	--------	--------

システム管理 >> トレース

トレース

メッセージの定義	
送信者情報	
ソース IP:	<input type="text"/>
ソース IP の FQDN: ?	<input type="text"/>
トレースで確認するリスナー:	IncomingMail (172.16.11.34:25)
ネットワーク所有者 ID:	<input checked="" type="radio"/> ソース IP と関連するネットワーク所有者 ID を調べる <input type="radio"/> 指定したものを使用: <input type="text"/>
SenderBase レピュテーションスコア (SBRs):	<input checked="" type="radio"/> ソース IP に関連した SBRs を調べる <input type="radio"/> 指定したものを使用: <input type="text"/>
エンベロープ情報	
エンベロープ送信者:	<input type="text"/>
エンベロープ受信者 (カンマで区切る):	<input type="text"/>
メッセージボディ	
メッセージ本文をアップロード:	<input type="text"/> <input type="button" value="参照..."/>
メッセージ本文を貼り付け (アップロードするファイルがない場合)	<input type="text"/>

システム管理 >> トレースと辿ります

トレースに必要な情報の入力

NVC



モニター メールポリシー セキュリティサービス ネットワーク システム管理

トレース

メッセージの定義	
送信者情報	
ソース IP:	122.212.247.18
ソース IP の FQDN: ?	mail.technvc.com
トレースで確認するリスナー:	IncomingMail (172.16.11.34:25)
ネットワーク所有者 ID:	<input checked="" type="radio"/> ソース IP と関連するネットワーク所有者 ID を調べる <input type="radio"/> 指定したものを使用: []
SenderBase レピュテーションスコア (SBR):	<input type="radio"/> ソース IP に関連した SBR を調べる <input checked="" type="radio"/> 指定したものを使用: 10.0
エンベロープ情報	
エンベロープ送信者:	mkunimasa@technvc.com
エンベロープ受信者 (カンマで区切る):	test@hoge hoge.com
メッセージボディ	
メッセージ本文をアップロード:	<input type="text"/> 参照...
メッセージ本文を貼り付け (アップロードするファイルがない場合)	asfdkj: pasfd laisjpfdoi poiadsf qihhsadf p0oiguja sdaapfoii

ソースIPに送信元IPアドレスを入力します。
例えば、外部からの受信での動作確認であれば、事前にnslookupなどで調べておきます。

ソースIPのFQDN:空白でも可能です

確認するリスナーの選択を行います。

Senderbaseのレピュテーションスコア欄は指定したものを使用し、数値を入力します。例では-10.0を入力しています。

ここを任意の数字に入れ替えてご確認ください。

送信元アドレス、送信先アドレスを入力します

メール本文を入力します

最後に画面右下の”トレースを開始”を押下し
処理内容を確認します

トレースの結果例

NVC

結果をトレース			
Host Access Table 処理 (リスナー: IncomingMail)			
一致:	sbrs[-1.0:10.0]		
送信者グループ:	UNKNOWNLIST		
ポリシー名:	BLOCKED		
コネクション動作:	REJECT		
FQDN:			
ネットワーク所有者 ID:	714971		
SenderBase レピュテーション スコア(SBRS):	10.0		
ポリシーパラメータ:	各コネクションの最大のメッセージ数:	10	デフォルト
	各メッセージの最大受信者数:	50	デフォルト
	最大メッセージサイズ:	10M	デフォルト
	単一IPからの最大の同時コネクション:	10	デフォルト
	TLS:	いいえ	デフォルト
	許可されたタグなしバウンス:	いいえ	
	1 時間当たりの最大受信者数:	無制限	デフォルト
	SenderBase 使用:	はい	デフォルト
	スパム検知使用:	はい	デフォルト
	ウイルス検知使用:	はい	デフォルト

この場合、送信者グループ [UNKNOWNLIST] にマッチし、SBRS スコアが -10 であるため、BLOCKED のポリシーが適用され、メールは届きません。

トレースの結果例(フィルタ処理確認)

NVC

割り当てられた仮想ゲートウェイ:	なし
割り当てられたバウンスプロフィール:	なし
ドメインのマスカレード	
	変更なし
フィルタ処理	
test	ルール: header("recieved") == "10.156.120.11": False
duplicate_copy2	スキップ(休止)
SourceRoutedRelay_Prevention	ルール: rcpt-to == "{% @ !)(.*)@" : False
From_lie_NVC_Filter_test	スキップ(休止)
New_SBRS_Header	ルール: sendergroup != "RELAY": True ネストフィルタ評価: ルール: reputation <= 10.0: False ネストフィルタ評価: ルール: no-reputation: True アクション: insert-header("X-SBRS", "None")
StripHeader	ルール: sendergroup == "RELAY": False
AdressFilter_NVCfrom	ルール: mail-from == ".*@.*\\.nvc\\.co\\.jp\$": False ルール: mail-from == ".*@nvc\\.co\\.jp\$": False ルール: OR: False
AdressFilter_NVCrcpt	ルール: rcpt-to == ".*@.*\\.nvc\\.co\\.jp\$": False ルール: rcpt-to == ".*@nvc\\.co\\.jp\$": True ルール: OR: True アクション: archive ("nvcto.mbox") アクション: skip-filters()
メールポリシー処理: Inbound (ポリシーにマッチ DEFAULT)	
メッセージの宛先:	mkunimasa@nvc.co.jp
エンドユーザーフリスト/ブロックリスト処理	
結果:	評価されていない:
スパム対策処理	
評価:	サスペクトスパム
対処完了:	送信が完了したメッセージ 件名の前に"[SUSPECTSPAM]" を付加 ログされたメッセージ

別の設定でのトレース例ですが、メッセージフィルタの評価状況が確認できます。

トレースの結果例(フィルタ処理確認)

NVC

コンテンツフィルタ処理	
alt-mailhost-c10	スキップ(無効)
Alias_Non-User_Address_Policy	スキップ(無効)
SBRs	スキップ(無効)
Deny-ML	スキップ(無効)
willcom-ok	スキップ(無効)
FromNVC	スキップ(無効)
Virus Outbreak Filter 処理	
評価:	評価されていない:
データ漏洩防止 (DLP) 処理	
結果:	評価されていない:
免責事項が追加されました	
上記メッセージ:	変更なし
メッセージの最後:	変更なし
DomainKeys 署名	
DomainKeys 処理の結果:	Domainkeys 署名はこのリスナの HAT で有効になっていません
DKIM 署名	
DKIM 処理の結果:	Domainkeys 署名はこのリスナの HAT で有効になっていません
DKIM 認証	
DKIM 認証処理結果:	DKIM 認証はこのリスナの HAT で有効になっておりません。
SPF 認証	
SPF 認証処理結果:	SPF 認証はこのリスナの HAT で有効になっておりません。
メッセージ送信(ポリシーに適合 DEFAULT)	
最後のエンベロープ送信者:	mechy3@technvc.com
最終受信者	mkunimasa@nvc.co.jp
最終メッセージ	X-SBRs: None X-IronPort-Anti-Spam-Filtered: true X-IronPort-Anti-Spam-Result: At08ALc250t61Pe3/2dsb2JhbACB0JAoAYk8giABAQEDXXHAQgR Subject: [SUSPECTSPAM] Received: from 122x212x247x183.ap122.ftth.ucom.ne.jp ([122.212.247.183]) by mx1.nvc.co.jp with TEST; 10 May 2010 14:30:24 +0900

同じくコンテンツフィルタの有効/無効が確認できます

最終的にIronportでどう処理されたかが表示されます。