■メッセージ追跡(msgtra.imss)

Column No.	Column Name	Value Example	Meaning
1	Message Log Type	QuarantineTransac HandoffTransac RcptChangedTransac ……	QuarantineTransac: 検索完了後、「隔離」処理が実行された HandoffTransac: 検索完了後、「中継」処理が実行された RcptChangedTransac: 検索完了後、「次の受信者に変更」処理が実行された DeleteTransac: 検索完了後、「メッセージ全体を削除」処理が実行された DeferredTransac: 検索完了後、なんらかの理由により配送が遅延されている NormalTransac: 検索完了後、宛先へ配送した場合 BouncedBackTransac: 検索完了後、なんらかの理由で宛先には配送されず、送信元へバウンスされた場合 Transac_ScanOut: 隔離メールをリリースして配送した等の場合等 ExpiredTransac_InScan: IMSVA のログモジュールが、内部的にExpire の処理を行った場合(内部的処理のためログクエリ等に影響はありません) ExpiredTransac_Scan: IMSVA のログモジュールが、内部的にExpire の処理を行った場合(内部的処理のためログクエリ等に影響はありません) Transac_In_NotSent: なんらかの理由で検索サービスにメールを渡すことができない(検索サービスの停止など)場合等 Transac_Redelivery: 遅延していたメールを再配送した場合 TransacToBeSplit: メールの宛先が複数だった場合やポリシーの適用に際してメールをスプリットして配送した場合 PostponeTransac ポリシー設定で配信を保留した場合
2	InTimeStamp	2014 Jan 17 03:01:57 +08:00	Postfix がメール受信した時刻
3	ScanTimeStamp	2014/01/17 03:01:57 +08:00	検索を実行した時刻
4	OutTimeStamp	2014 Jan 17 03:02:03 +08:00	Postfix がメールを検索サービスに渡した時刻
5	Message ID	20140116190156.0196E30035@imsva85-1.com	メールのMessage-IDヘッダの値
6	Internal Message ID	B98EA40A-3304-E605-96C3-03F170A4A04A	IMSVA内部でのメールのID
7	Postfix ID	689883003C	Postfix のメールの ID
8	Scanner ID	3	
9	sender	test_1@imsstest.com	
10	recipient	u_000_2@imsstest.com	
11	subject	test	
12	Client IP	10.64.48.151	IMSVAにメールを送信した SMTP クライアントの IP アドレス
13	Delivery IP	[10.64.73.155]:25	IMSVAがメールを配送した宛先 MTA の IP アドレス
14	DeliveryFeedback	250 Message accepted for delivery.	宛先 MTAからの応答
15	DeliveryStatus	sent	Sent Deferred Bounced #null# (メールが隔離された場合)
16	Action	00100000000000000	検索サービスによる実行された処理 0:アクションを実行しなかった 1:アクションを実施 1st – メッセージ全体を削除 2nd – 隔離 3rd – Deliver the message 4th – Archive the message 5th – 中継 6th – 受信者の変更 7th – 本文にスタンプを挿入 8th – 添付ファイルを削除 9th – 件名にタグを挿入 10th – 配信を保留 11th – ポリシー通知を送信 12th – ウイルスを駆除 13th – BCC 14th – X-header を挿入 15th – no special action. 16th – 暗号化 17th – no special action.
17	Split Flag	0	検索処理の際にメールがスプリットされたかどうか 0:スプリットなし 1:スプリットあり
18	Extra Item	“”	ほとんどのメッセージで 空白 になります。 データベース側で同一メッセージの情報をアップデートする必要がある場合に、数値(1~)が入ります。
19	ToDeliveryTimeStamp	2014 Jan 17 03:02:16 +08:00	
20	InDeliveryTimeStamp	2014 Jan 17 03:02:16 +08:00	
21	DKIMResult	DKIM-Signature field added (s=test, d=dkim.test	DKIM署名の処理結果が表示されます。DKIM署名が行われない場合は空白になります。 DKIM署名の設定は、管理画面の[管理] > [IMSVA設定] > [DKIM署名]で行います。
22	tls	0/1/2/3	0: 受信および送信トラフィックとも、TLS による暗号化なし 1: 受信トラフィックのみ、TLS による暗号化あり 2: 送信トラフィックのみ、TLS による暗号化あり 3: 受信および送信トラフィックとも、TLS による暗号化あり
23	original_attach_name	1.txt; june.zip	複数の添付ファイルがある場合には、セミコロンで区切られます

Sample:

QuarantineTransac 2016 May 17 15:43:44 +08:00 2016/05/17 15:43:45 +08:00 #null# 20160517074344.615DDD803E@imsva-17.com B98EA40A-3304-E605-96C3-03F170A4A04A 615DDD803E2 june_2@trend.com june_1@imsstest.com WTP testing 10.204.148.40 #null# #null# #null# 01000000000000000 0 #null# 2016 May 17 15:43:44 +08:00 0

NormalTransac 2016 May 18 15:49:10 +08:00 2016/05/18 15:49:10 +08:00 2016 May 18 15:49:12 +08:00201605180749 10.303FE10A040@imsva-16.com 3ED11D1C-3319-1705-AE29-2038E820770E 5004010A041 1june_2@trend.com june_2@trend.com 10.204.148.40 [10.204.168.99]:25
250 Message accepted for delivery. sent 00110000000000000 0 2016 May 18 15:49:10 +08:00 2016 May 18 15:49:10 +08:00 0

■ポリシーイベント(polevt.imss)

Column No.	Column Name	Value Example	Meaning
1	Insert Timestamp	2014/01/21 13:58:01 GMT+08:00	デーモンプロセスがローカルディスクに書き込んだ時間
2	Internal Message ID	133B8715-126D-B405-8DE2-978148EE81E1	検索サービスがメールを一意に特定するために利用する ID
3	Smtp sender	jing@imsstest.com	
4	Smtp recipient	imsstest1@imsstest.com	
5	Message subject	テストメール	
6	Message route	1	1: 受信メッセージ 2: 送信メッセージ 3: POP3
7	Trigger rule name	グローバルウイルス対策ルール	マッチしたルール名
8	Filter type	0100000000000000	1st – ウイルス 2nd – スパム 3rd – 添付ファイル 4th – コンテンツ 5th – サイズ 6th – その他 7th – Malformed 8th – 検索できないメッセージ 9th – フィッシング 10th – Web レピュテーション 11th – DKIM 12th – BATV (IMSVAでは使用していない) 13th – コンプライアンス 14th – C&C メール 15th – グレーメール 16th – ソーシャルエンジニアリング
9	Filter Description		
10	Message size	数値	
11	Action	0000000000000000	検索サービスにより実行された処理 0:アクションを実行しなかった 1:アクションを実施 1st – メッセージ全体を削除 2nd – 隔離 3rd – インターセプトしない 4th – アーカイブ 5th – 中継 6th – 受信者の変更 7th – 本文にスタンプを挿入 8th – 添付ファイルを削除 9th – 件名にタグを挿入 10th – 配信を保留 11th – ポリシー通知の送信 12th – ウイルスを駆除 13th – BCC 14th – X-header を挿入 15th – no special action. 16th – 暗号化 17th – no special action.
12	Spam score	数値	スパムスコア
13	Spam category	数値	スパムカテゴリ
14	Spam sensitive	数値	スパムの検出レベル: 0: スパムルールは無効 1: 高 2: 中 3: 低 4: 閾値を指定
15	Attachment name	Demo Sample.pdf	
16	Attachment type		
17	Virus name	HEUR_PDFEXP.C	
18	Virus type	2	
19	Quarantine id	1	
20	Quarantine TTL	15	隔離領域でメッセージを保存する期間(日)
21	Archive ID		
22	Archive TTL		アーカイブ領域でメッセージを保存する期間(日)
23	Original Message ID	20161025232500.2D34A5E034@imsva9.win.local	
24	Wrs threshold	65	
25	Wrs score	21	
26	reason	http://wrs21.winshipway.com	Web レピュテーション/コンプライアンスフィルタで検出した理由
27	Dkim author	gmail.com	DKIM 署名検証の際の送信者ドメイン
28	Dkim reason	DKIM 署名の検証に失敗しました。	DKIM 署名の検証に失敗した理由 DKIM 署名がありません。 DKIM 署名の検証に失敗しました。 DKIM 署名を検証できません。

29	dda process status	100	10: DDA(Deep Discovery Analyzer)での解析がユーザーによりキャンセルされました 11: DDAで例外が発生 100: DDA による解析のため、ポリシールールによる検索を中断 101: メールがルールをトリガしたため DDA での解析が必要 103: メールはルールをトリガしたが、同一ファイルが既に DDA に送信済みのため、メールサンプルは DDA に送られません 102: メールはルールをトリガしなかったが、DDA での解析が必要 (ファイルタイプによる指定など) 104: 103 と同じ。ただし実ファイルタイプフィルタ用
30	Ccca detection type	0	
31	Ccca detection address	news@chinabytecnc.com	
32	Wrs category list	93	Web レピュテーションのカテゴリの値
33	Graymail category	0	グレーメールのカテゴリ 1: MML(マーケティングメッセージ、ニュースレター) 2: SNL(ソーシャルネットワーク notification)
34	DLP detail Match Result Xml Path	/opt/trend/imss/log/DLPComplianceLog/20160927/F/2/F2EDF372-3D77-ED05-B783-FFF504D4DEA6.xml	
35		(空白)	常に 空白
36		(空白)	常に 空白
37	dda_rating	32766	32767:NULLを意味 32766:DDA (Deep Discovery Analyzer)での解析中にユーザーにメールが解除され、検索がキャンセルされました 32765:DDA での解析中にユーザーにメールが削除されました 32764:DDA で例外が発生 レーティング値:DDAからのレーティング値例) * 3(高リスク) * 2(中リスク) * 1(低リスク) * 0(リスクなし) * -1(サポートしないファイルタイプのためサンドボックスでフィルタした)
38	Suspicious APT Filters Map	0	
39	Analyzed APT Filters Map	0	
40	DLP Triggered keywords		
41	Message attachment name		
42	so file detection	数値	
43	so file sourcetype	数値	不審オブジェクトタイプ 0:サンドボックス 1:ユーザー定義
44	so file action	数値	不審オブジェクトの処理 1:ログのみ 3:隔離
45	so file value	文字列	File SHA1
46	so url detection	数値	不審オブジェクトでの URL 検知か否か 0:いいえ 1:はい
47	so url sourcetype	数値	不審オブジェクトタイプ 0:サンドボックス 1:ユーザー定義
48	so url action	数値	不審オブジェクトの処理 1:ログのみ 3:隔離
49	so url value	文字列	URL
50	is WRS triggered	数値	Webレピュテーション設定のセキュリティレベルに従って、Webレピュテーションがトリガーされたか 0: Webレピュテーションがトリガされなかった 1: Webレピュテーションがトリガされた
51	rewrite status	数値	メール処理時のTime-of-Clickプロテクションの設定状態 0: [Time-of-Clickプロテクsチョンを有効にする]が無効 1: [すべてのURLに適用]を選択 2: [トレンドマイクロでテストされていないURLに適用]を選択 3: [WebレピュテーションサービスによってマークされたURLに適用]を選択 -1: URLの書き換え時にエラーが発生
52	rewritten url num	数値	Time-of-Clickプロテクションによって書き換えられた URLの数
53	emergingThreatCategory	数値	スパムメール検出エンジンが検出した脅威カテゴリ: 0:UNKNOWN/UNCATEGORIZED 1:RANSOMEWARE 2:BANKING TROJAN ※スパムチェック未実施の場合も、0が表示されます。
54	ddaVirusName	検出脅威名	仮想アナライザ(Deep Discovery Analyzer)が検出した脅威名。 複数存在する場合は";"区切りで"A;B;C"のように表示されます。

Sample:

2016/09/27 11:24:04 GMT+08:00 9ABDB236-3D74-C605-8474-8AC4FC89FAD7 june_2@trend.com june_1@imsstest.com [HeaderEntity]MML.eml 1 graymail 0000000000000010 1.099609 01000000000000000 0.000000 0 0 1 15 0 0 <20160927032334.9534410A051@imsva-16.com> 0 0 0 0 1 32767 0 0 0 0 0 0 1 0 0

■ERSログ(ers.imss)

Column No.	Column Name	Value Example	Meaning
1	Insert Timestamp	2016/10/09 14:19:00 GMT+08:00	NRSLogParserがログを書き込んだ時間
2	ERS query time	Oct 09 2016 14:18:57	IMSVAがEメールレピュテーションサービスにクエリした時刻
3	ip_address	10.204.168.99	チェック対象となったIPアドレス
4	Action	NULL値 or 1	NULL値：SMTPクライアントをブロックしない 1：SMTPクライアントをブロック
5	ActionNum	2	現在のインターバルで何回アクションを実施したか
6	connection_ip	10.204.168.99	IMSVAのSMTPクライアントのIPアドレス(接続元IPアドレス)
7	sender	文字列	メール送信者
8	recipient	文字列	メール受信者
9	type	NULL値 or 数値	NULL値: ERSによるブロックはなし 1: RBL+ Service (RBL, DUL) または ERS ポータルのブロック済みリストによってブロック 2: Network Anti-Spam Service (QIL)でブロック

Sample:

```
2016/07/21 23:51:48 GMT+09:00 Jul 21 2016 23:51:03 192.168.32.2 1 1 192.168.32.2 postmaster@test1.test.com 1
```

■送信者フィルタ(foxreport)

Column No.	Column Name	Value Example	Meaning
1	Insert Timestamp	2015/03/30 10:02:08 GMT+08:00	
2	IP Address	181184932	IMSVAのIPアドレス(ロングフォーマット)
3	time when the client was blocked	2015-03-30 10:02:08.573680	ブロックした時刻
4	Block type	5	ブロックの理由となった送信者フィルタの種類。取りうる値は以下。 (6, 7は実際には登場いたしません) 1: DHA攻撃 2: ウイルス 3: スパムメール 4: バウンスメール 5: ブロックリスト(ドメイン/IPアドレス) 8: ブロックリスト(グループ別の指定) ※SMTPトラフィックスロットリングによるブロックは次のページのログになります。
5	Count	数値	
6	Connection IP	10.204.169.164	接続元MTAのIPアドレス
7	Mail sender	imsstestsender@imsstest.com	送信者
8	Mail recipient	imsstestrcpt@imsstest.com	受信者

Sample:

2015/03/30 10:02:08 GMT+08:00 181184932 2015-03-30 10:02:08.573680 5 3 10.204.169.164 imsstestsender@imsstest.com imsstestrcpt@imsstest.com

■送信者フィルタ(connblockedimss)

Column No.	Column Name	Value Example	Meaning
1	Insert Timestamp	2016/10/09 16:12:28 GMT+08:00	
2	time when the client was blocked	Oct 09 2016 08:12:24 UTC	ブロックした時刻(UTC)
3	client ip address	10.204.148.40	接続元MTAのIPアドレス
4	sender address	imsstestrcpt@imsstest.com	5カラム目が"1"の場合は空になります。 送信者が<>の場合も空になります。
5	type	1 or 2	1: SMTPトラフィックスロットリングの「IPベースのスロットリング」によるブロック 2: SMTPトラフィックスロットリングの「送信者ベースのスロットリング」によるブロック
6	count	数値	

Sample:

```
2016/10/09 16:12:28 GMT+08:00 Oct 09 2016 08:12:24 UTC 10.204.148.40 1 1
```

■管理(euqerror.imss, euqretry.imss, euqsynch.imss)

Column No.	Column Name	Value Example	Meaning
1	Insert Timestamp	2014/01/21 13:58:01 GMT+08:00	
2	Internal message ID	BE86EA51-1283-9005-AE0A-	対象メールのIMSVA上の内部ID
3	Sender	jing@imsstest.com	送信者
4	Recipient	imsstest1@imsstest.com	受信者
5	Mail subject	文字列	メールのSubject
6	Scanner ID	1	
7	Message Size	3.447266	
8	Quarantine Area ID	1	
9	Quarantine Time stamp	1427731158	隔離された時刻
10	Action	1	1: EUQ DBに追加 2: EUQ DBから削除
11	Retry times	0	EUQの同期リトライが実行された回数(最大5回) ※初回の同期時は「0」と表示
12	Time to retry	0	EUQの同期リトライにかかった時間 ※初回の同期時は「0」と表示

Sample:

2015/03/31 00:00:13 GMT+08:00 BE86EA51-1283-9005-AE0A-A28F43BFC0B8 jing@imsstest.com imsstest1@imsstest.com plain text email test sample 1 3.447266 1 1427731158 1 0 0