Deep Discovery™ Email Inspector 5.1

Syslog コンテンツマッピングガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/jp/solution/000207383

商標について

P/N: APEM59196/210115_JP (2021/06)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Deep Discovery Email Inspector により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Deep Discovery Email Inspector における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

本書について

次の項目を参照してください。

ドキュメント

Deep Discovery Email Inspector のドキュメントには次のものがあります。

表 1. 製品ドキュメント

ドキュメント	説明
管理者ガイド	管理者ガイドには、Deep Discovery Email Inspector を設定して管理する方法の詳細な手順、および Deep Discovery Email Inspector の概念や機能に関する説明が記載されています。
インストールガイド	インストールガイドには、Deep Discovery Email Inspector の導入計画とインストールの要件および手順、さらに事前設定コンソールを使用して初期設定とシステムタスクを実行する方法についての情報が含まれています。
Syslog コンテンツマッピングガイド	Syslog コンテンツマッピングガイドには、ログの管理基準や、Deep Discovery Email Inspector の Syslog イベントを実装するための構文に関する情報が記載されています。
クイックスタートガイド	クイックスタートガイドには、Deep Discovery Email Inspector をネットワークに接続して初期設定を実行するための手順がわかりやすく説明されています。
Readme	Readme には、オンラインヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれています。新機能、既知の問題、および製品リリースの履歴に関する情報を確認できます。
オンラインヘルプ	オンラインヘルプには、Deep Discovery Email Inspector のコンポーネントと機能、Deep Discovery Email Inspector を設定するために必要な手順が説明されています。
サポートポータル	サポートポータルは、問題の解決およびトラブルシューティングの情報を参照できるオンラインデータベースです。製品の既知の問題に関する最新の情報を得ることができます。サポートポータルにアクセスするには、以下の Web サイトをご覧ください。 https://success.trendmicro.com/jp/technical-support

対象読者

この Deep Discovery Email Inspector のドキュメントは、IT 管理者とセキュリティアナリストを対象としています。ここでは次のトピックを含め、読者にネットワークと情報セキュリティに関する十分な知識があることを前提としています。

- ネットワークトポロジ
- メールルーティング
- SMTP

ただし、サンドボックス環境や脅威イベントの相関分析については、読者がその知識を持っていないものとして説明します。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	必要な設定や初期設定、および製品の制限事項に関する情報
 警告!	重要な操作と設定オプション

トレンドマイクロについて

トレンドマイクロは、サイバーセキュリティにおける世界的企業として、安全にデジタル情報をやり取りできる環境の実現に向けて継続的に取り組んでいます。個人消費者、企業、および政府機関向けの革新的ソリューションである XGen セキュリティ戦略を巧みに利用することで、つながるセキュリティをデータセンター、クラウドワークロード、ネットワーク、およびエンドポイントにもたらします。

Amazon Web Services、Microsoft、および VMware などの主要な環境に合わせて最適化された階層化ソリューションにより、組織は、今日の脅威から重要な情報を自動的に保護することができます。トレンドマイクロの提供する Connected Threat Defense によって、脅威インテリジェンスのシームレスな共有が可能になるとともに、一元化された可視性と調査の提供によって、組織の柔軟性が最大限に高まります。

トレンドマイクロのお客さまには、自動車、銀行、医療、電気通信、および石油といった産業にわたる、Fortune Global 500 企業の上位 10 社のうち 9 社が含まれています。

世界 50 か国の 6,500 人を超える従業員と、最先端のグローバルな脅威調査および脅威インテリジェンスによって、トレンドマイクロは「つながる世界」のセキュリティを確保できるようお客さまを支援します。詳細については、次のサイトを参照してください。https://www.trendmicro.com

第 1 章

はじめに

Deep Discovery Email Inspector Syslog コンテンツマッピングガイドには、ログの管理基準や、Deep Discovery Email Inspector の Syslog イベントを実装するための構文に関する情報が記載されています。

サードパーティのログ管理システムとの柔軟な統合を実現するため、Deep Discovery Email Inspector では次の syslog 形式がサポートされます。

ログ管理システム	説明
CEF (Common Event Format) 詳細については、21 ページの Syslog コンテンツマッピング - CEF を参照してください。	HP ArcSight によって開発されたオープンなログ管理標準です。 Deep Discovery Email Inspector では CEF ディクショナリのサブセットを使用します。
LEEF (Log Event Extended Format) 詳細については、53 ページの Syslog コンテンツマッピング - LEEF を参照してください。	IBM Security QRadar 用に開発されたイベント形式です。 Deep Discovery Email Inspector では LEEF ディクショナリのサブセットを使用します。
TMEF (Trend Micro Event Format) 詳細については、87 ページの Syslog コンテンツマッピング - TMEF を参照してください。	ログフィールドのスーパーセットです。これにより、Deep Discovery Email Inspector から提供される検出イベントをサードパーティの Syslog 管理機能でより柔軟に制御できるようになります。

Syslog イベント

Deep Discovery Email Inspector では次のイベントがサポートされます。

表 1-1. Syslog イベント

イベント	説明
検出ログ: メール検出ログ	Deep Discovery Email Inspector のメール検出ログ。 送信者、受信者、件名、およびメッセージ ID など検出されたメールメッセージに関連する情報が含まれます。
検出ログ: 添付ファイル検出ログ	Deep Discovery Email Inspector の添付ファイル検出ログ。 ファイル名、ファイルサイズ、およびファイルタイプなど検出された添付ファイルに関連する情報が含まれます。
検出ログ: URL 検出ログ	Deep Discovery Email Inspector の URL 検出ログ。 検出された URL や脅威の可能性のある URL が含まれます。
アラートログ	Deep Discovery Email Inspector のアラートログ。 アラートの名前や通知の内容などアラートに関連する情報が含まれます。
仮想アナライザの分析ログ: ファイル分析イベント	仮想アナライザのファイル分析イベント。 ファイル名、ファイルサイズ、およびファイルタイプなど分析されたファイルに関連する情報が含まれます。
仮想アナライザの分析ログ: URL 分析イベント	仮想アナライザの URL 分析イベント。 分析された URL や脅威の可能性のある URL が含まれます。
仮想アナライザの分析ログ: 著しい特性イベント	仮想アナライザの著しい特性イベント。 分析したサンプルによって実行された著しい特性イベントに関する情報が含まれます。
仮想アナライザの分析ログ: 拒否リストトランザクションイベント	仮想アナライザの拒否リストトランザクションイベント。 特定の拒否リストに対して実行した処理と、SHA1 や URL など拒否リストのオブジェクトに関する情報が含まれます。

イベント	説明
メッセージ追跡ログ	Deep Discovery Email Inspector でメールメッセージが送受信されたかどうかを示し、メールメッセージの調査の証拠が含まれます。
送信者フィルタ/認証ログ	送信者の認証結果と実行された処理が含まれます。
システムログ	Deep Discovery Email Inspector の監査ログまたはアップデートログ。
MTA ログ	Deep Discovery Email Inspector 上での Postfix 接続と SMTP の活動に関する情報が含まれます。MTA ログは未加工のまま Syslog サーバに直接送信されます。
Time-of-Click プロテクションログ	ユーザのクリック時に検出された URL と実行された処理に関する情報が含まれます。

用語

用語	説明
CEF	Common Event Format (共通イベントフォーマット)
LEEF	Log Event Extended Format (ログイベント拡張フォーマット)
TMEF	Trend Micro Event Format (トレンドマイクロのイベント形式)

第 2 章

改訂履歴

次の表に本ドキュメントの改訂履歴を示します。

バージョン	説明
5.1	• メッセージ追跡ログに `recipient changed` イベントを追加 • メール検出ログに `recipient changed` 処理を追加 • Syslog イベントに Time-of-Click プロテクションログを追加

3.1	• DKIM 署名失敗のシステムアラートを追加
	• 次のイベントの新しいログを追加:
	  • メッセージ追跡
	  • 送信者フィルタ/認証
	  • MTA

バージョン	説明

3.0	• メール検出ログに以下を追加:
	  • 重大度の種類: 未評価
	  • 処理の種類: 削除、直接配信、および 駆除
	  • 脅威の種類: スパムメール/グレーメール、フィッシング、および コンテンツ違反
	• 添付ファイル検出ログの重大度の種類に未評価を追加
	• 新しいシステムアラートを追加:
	  • Account Locked (アカウントのロック)
	  • スパム隔離ディスク空き容量の低下
	  • メッセージ遅延キュー長の超過
	• 次のシステムアラートの名称を変更:
	  • 「隔離されたメッセージ」を「脅威の検出により隔離されたメッセージ」に
	  • 「検出の急増」を「脅威検出の急増」に
	  • 「隔離ディスク空き容量の低下」を「脅威隔離ディスク空き容量の低下」に

2.6	「メモリ使用率の超過」システムアラートログを追加

2.5 SP1	• 次の LEEF ログの署名 ID (`eventid`) を削除
	  • メール検出ログ
	  • 添付ファイル検出ログ
	  • URL 検出ログ
	  • アラートログ
	• 「隔離メッセージ」セキュリティアラートログを追加

2.5	初リリース

第 3 章

Syslog コンテンツマッピング - CEF

次の各表は、Deep Discovery Email Inspector のログ出力と CEF 形式のシステム出力ログとのコンテンツマッピングを示しています。

- 51 ページの「MTA ログ」

CEF 形式の検出ログ:メール検出ログ

表 3-1. CEF 形式の検出ログ:メール検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100130
Header (eventName)	説明	EMAIL_DETECTION
Header (severity)	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高

CEF キー	説明	値
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
cn1	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント
cn1Label	脅威の種類 <cnx または csx>Label はラベルのキー名です。	threatType

CEF キー	説明	値
cn2	メールのサイズ	例: 30841
cn2Label	メールのサイズ	msgSize
cs1	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	メールで検出された脅威の名前	threats
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	社内メールの ID	msgUuid
cs3	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	メール ID	messageId
cs4	送信者のメールアドレス	例: user1@example.com
cs4Label	送信者のメールアドレスのラベル	senderMail
cs5	受信者のメールアドレス	例: user2@example.com
cs5Label	受信者のメールアドレスのラベル	rcptMail
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost

CEF キー	説明	値
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
msg	メールの件名	例: hello
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|100130|EMAIL_DETECTION|6|rt=Mar
23 2015 11:53:17 GMT+00:00 src=150.70.186.134 cs3Label=mess
ageId cs3=<20150323115314.BCA2C9168EA@internalbeta.bcc.ddei
> deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 act
=passed dvchost=internalbeta.bcc.ddei dvc=10.64.1.131 duser
=user1@domain1.com;user2@domain1.com;user3@domain1.com msg=
Virus_Report-20150323_02:00 cn2Label=msgSize cn2=83878 cn1L
abel=threatType cn1=3 suser=user@domain2.com dvcmac=C4:34:6
B:B8:09:BC cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB
5EC111FE7 cs1Label=threats cs1=PUA_Test_File|TROJ_GEN.R04AC
0PAH15|PAK_Generic.005|ADW_DOWNLOADER.WRS|LOW-REPUTATION-UR
L_BLOCKED-LIST.SCORE.WRS|LOW-REPUTATION-URL_BLOCKED-LIST.SC
ORE.WRS|TROJ_GEN.R02SC0OLH14|TROJ_GENERIC.WRS|TROJ_DOWNLOAD
ER.WRS
```

CEF 形式の検出ログ: 添付ファイル検出ログ

表 3-2. CEF 形式の検出ログ: 添付ファイル検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro

CEF キー	説明	値
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100131
Header (eventName)	説明	ATTACHMENT_DETECTION
Header (severity)	重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
cs1	脅威の名前	例:VAN_BOT.UMXX
cs1Label	脅威の名前	threats
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	社内メールの ID	msgUuid
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar

CEF キー	説明	値
fsize	ファイルサイズ	例: 131372
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|100131|ATTACHMENT_DETECTION|6|rt
=Mar 23 2015 14:04:46 GMT+00:00 fileHash=E49395FEACC12A5613
E7BA6C69AC5E42EDFDA42D fsize=17681 fileType=MIME Base64 dvc
host=internalbeta.bcc.ddei dvc=10.64.1.131 deviceExternalId
=c425624a-e9db-4f3f-8088-2726f15e6587 cs2Label=msgUuid cs2=
E89A23BE-11F5-2505-BCEE-21027D078154 fname=3C761B45-626D-4E
75-B4782FD0E5E8369C.eml dvcmac=C4:34:6B:B8:09:BC cs1Label=t
hreats cs1=TROJ_UP.258A1A7D
```

CEF 形式の検出ログ:URL 検出ログ

表 3-3. CEF 形式の検出ログ:URL 検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100132
Header (eventName)	説明	URL_DETECTION
Header (severity)	メールの重大度	• 4: 低 • 6: 中 • 8: 高

CEF キー	説明	値
cat	カテゴリ	例: 90:02
cs1	脅威の名前	例: LOW-REPUTATION-URL_MALWARE.WRS
cs1Label	脅威の名前	threats
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	社内メールの ID	msgUuid
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1139|100132|URL_DETECTION|6|rt=Mar 2
3 2015 11:57:46 GMT+00:00 cs2Label=msgUuid cs2=73A9FA6A-11F
3-4F05-BCEE-6BB5EC111FE7 dvcmac=C4:34:6B:B8:09:BC dvchost=i
nternalbeta.bcc.ddei request=http://www.alltobid.com/guopai
/upload/dan201401.zip dvc=10.64.1.131 deviceExternalId=c425
624a-e9db-4f3f-8088-2726f15e6587
```

CEF 形式のアラートログ

表 3-4. CEF 形式のアラートログ

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	300105
Header (eventName)	説明	ALERT_EVENT
Header (severity)	アラートの重大度	• 2: 情報 • 6: 重要 • 8: 重大
cs1	アラート名	例: Security: Suspicious Messages Identified
cs1Label	アラート名	ruleName
cs2	説明	例: 1 or more messages detected with threats
cs2Label	説明	ruleCriteria
cs3	実行値	例: 35
cs3Label	実行値	eventTriggeredValue

CEF キー	説明	値

cs4	通知のコンテンツ	例:
		`The following email messages contain threats:`
		
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <20150619032243.5923E650365@localhost.ddei-164>`
		`Recipients: fake@test.com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263`
		`Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		
		`Alert time: 2015-05-25 11:11:27 +0800`
		
		注意
		最大長は 1023 文字です。

cs4Label	通知のコンテンツ	ruleContent
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9

CEF キー	説明	値
externalId	アラートデータベースのログ ID	例: 1648
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1009|300105|ALERT_EVENT|6|rt=Jun 16 2
015 09:26:25 GMT+00:00 cs1Label=ruleName cs1=Security: Thre
at Messages cnt=1 cs2Label=ruleCriteria cs2=At least 1 thre
at message detected externalId=1299 cs3Label=ruleContent cs
3=The%20following%20email%20messages%20contain%20threats%3A
%0A%0A%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3
D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%
3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D
%3D%3D%3D%0ARisk%3A%20Medium%20%28Malware%29%0AAction%3A%20
%20Quarantined%0AMessage%20ID%3A%20%3C20150616092610.B56A66
503C6%40localhost.ddei-164%3E%0ARecipients%3A%20fake%40test
.com%3Btest%40test.com%0ASender%3A%20test%40fake.test%0ASub
ject%3A%20temail%20-%20Copyaaa... dvcmac=00:50:56:01:2C:BC
dvchost=localhost.ddei-164 deviceExternalId=361a091c-addd-
40cf-98e7-710e43500a66 dvc=10.204.253.164
```

CEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

表 3-5. CEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0

CEF キー	説明	値
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200119
Header (eventName)	説明	Sample file sandbox analysis is finished
Header (severity)	重大度	• 4:低 • 6:中 • 8:高
cn1	GRID/CSSS の結果	• 0: GRID が無害と知られていない • 1: GRID が無害と知られている
cn1Label	GRID/CSSS の結果	GRIDIsKnownGood
cn2	ROZ レーティング (仮想アナライザによる解析結果を示す内部コード)	例:3
cn2Label	ROZ レーティング	ROZRating
cn3	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
cn3Label	PCAP 使用可能	PcapReady
cs1	サンドボックスイメージの種類	例: win7
cs1Label	サンドボックスイメージの種類	SandboxImageType
cs2	不正プログラム名	例: HEUR_NAMETRICK.A

CEF キー	説明	値
cs2Label	不正プログラム名	MalwareName
cs3	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
cs3Label	上位の SHA-1	ParentFileSHA1
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200119|Sample file sandbox analy
sis is finished|3|rt=Mar 23 2015 14:48:24 GMT+00:00 dvc=10.
64.1.131 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6B:B8:0
9:BC deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587
fname=Wonga Express Loan Promtion 3.5% Offer.doc fileHash=A
46E1F56969DECC5FEAF120A2279946A2F42D619 fileType=MS Office
fsize=53760 cs1Label=SandboxImageType cs1=win81en cn1Label=
```

```
GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=1 cs2Label=Ma
lwareName cs2=VAN_MALWARE.UMXX cn3Label=PcapReady cn3=1
```

CEF 形式の仮想アナライザ分析ログ: URL 分析イベント

表 3-6. CEF 形式の仮想アナライザ分析ログ: URL 分析イベント

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200126
Header (eventName)	説明	URL sandbox analysis is finished
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
cn2	ROZ レーティング(仮想アナライザによる解析結果を示す内部コード)	例: 3
cn2Label	ROZ レーティング	ROZRating

CEF キー	説明	値
cn3	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
cn3Label	PCAP 使用可能	PcapReady
cs1	サンドボックスイメージの種類	例: win7
cs1Label	サンドボックスイメージの種類	SandboxImageType
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200126|URL sandbox analysis is
finished|3|rt=Mar 23 2015 16:32:15 GMT+00:00 dvc=10.64.1.1
31 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC
deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 requ
est=http://paypal-world.ga/home/? fileHash=5EA358C987D1FDE
```

```
34957B9A36AF38321C5F37D8B cs1Label=SandboxImageType cs1=wi
n81en cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

CEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

表 3-7. CEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200127
Header (eventName)	説明	Notable Characteristics of the analyzed sample
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
cs1	違反ポリシー名	例: Internet Explorer Setting Modification
cs1Label	違反ポリシー名	PolicyCategory

CEF キー	説明	値
cs2	違反イベントの分析	例: Modified important registry items
cs2Label	違反イベントの分析	PolicyName
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: Process ID:3020\n Image Path:%ProgramFiles%\\Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 / prefetch:2
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200127|Notable Characteristics o
f the analyzed sample|6|rt=Mar 23 2015 10:44:28 GMT+00:00 d
vc=10.64.1.131 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6
B:B8:09:BC deviceExternalId=c425624a-e9db-4f3f-8088-2726f15
e6587 fname=http://bsjv.tk/bbb/bbb/bbb fileHash=2D302EEEF70
3CBB8713B806B3C5B4B3A2A28E92A fileType=URL fsize=0 cs1Label
```

```
=PolicyCategory cs1=Process, service, or memory object chan
ge msg=Process ID: 3020\nImage Path: %ProgramFiles%\\Intern
et Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 /prefet
ch:2 cs2Label=PolicyName cs2=Creates process
```

CEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

表 3-8. CEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200120
Header (eventName)	説明	Deny List updated
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
act	イベントの処理	• Add • Remove

CEF キー	説明	値
cs1	拒否リストの種類	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	拒否リストの種類	type
cs2	リスクレベル	• Low • Medium • High • Confirmed Malware
cs2Label	リスクレベル	RiskLevel
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dhost	送信先ホスト名	例: dhost1
dpt	送信先ポート	0〜65535 の値
dst	送信先 IP アドレス	例: 10.1.144.199
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
end	レポート終了時刻	例: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

CEF キー	説明	値
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200120|Deny List updated|3|rt=Ma
r 24 2015 10:10:20 GMT+00:00 dvc=10.64.1.131 dvchost=intern
albeta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c
425624a-e9db-4f3f-8088-2726f15e6587 cs1Label=type cs1=Deny
List File SHA1 end=Apr 19 2015 16:03:13 GMT+00:00 act=Add
fileHash=41D188169D9B986818A437DD80814FA84B0522FB cs2Label=
RiskLevel cs2=High
```

CEF 形式のメッセージ追跡ログ

表 3-9. CEF 形式のメッセージ追跡ログ

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100136

CEF キー	説明	値
Header (eventName)	説明	MESSAGE_TRACKING
Header (severity)	メールの重大度	• 2: 使用不可 • 2: 未評価 • 2: 標準 • 4: 低 • 6: 中 • 8: 高
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
cs1Label	メール ID のラベル	messageId
cs1	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	社内メールの ID のラベル	msgUuid
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

CEF キー	説明	値
msg	メールの件名	例: hello
reason	ブロック処理の理由	例: Timeout period expired
cs3Label	最新のステータス	latestStatus
cs3	詳細	• Deleted • Delivered • Delivery unsuccessful • Processing completed • Quarantined • Recipient changed
src	送信元 IP アドレス	例: 10.1.144.199
cs4Label	送信者のメールアドレスのラベル	senderMail
cs4	送信者のメールアドレス	例: user1@example.com
cs5Label	受信者のメールアドレスのラベル	rcptMail
cs5	受信者のメールアドレス	例: user2@example.com
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146
cs6Label	処理履歴のラベル	procHistory
cs6	処理履歴	例: デバイスが実行した処理。形式: "タイムスタンプ 1 処理 1,タイムスタンプ 2 処理 2,..., タイムスタンプ n 処理 n"

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1106|100136|MESSAGE_TRACKING|2|rt=A
pr 27 2018 02:55:53 GMT+00:00 cs3Label=latestStatus cs3=De
```

```
livery unsuccessful dvchost=localhost.localdomain deviceEx
ternalId=9ceb7be2-3ec5-4b80-8697-6b4913eb044b dvc=10.204.6
3.177 duser=test@test.com dvcmac=00:50:56:A7:5F:AD reason=
host 10.204.253.179[10.204.253.179] said: 552 test@test.co
m mailbox full (in reply to end of DATA command) cs1Label=
messageId cs1=20180427025553.4D771D6135F@localhost.localdo
main cs4Label=senderMail cs4=marks@relay.ddei.comsuser=fak
e@test.testmsg=plain_text_upper_case.HTML/HTM cs2Label=msg
Uuid cs2=EB715918-6ACB-A405-BF46-56F53CE3FD86 cs6Label=pro
cHistory cs6=Apr 27 2018 02:55:53 GMT+00:00 Received,Apr 2
7 2018 02:55:53 GMT+00:00 Sent for analysis,Apr 27 2018 02
:56:48 GMT+00:00 Action set to 'pass',Apr 27 2018 02:56:48
 GMT+00:00 Delivery unsuccessful,Reason:host 10.204.253.17
9[10.204.253.179] said: 552 test@test.com mailbox full (in
 reply to end of DATA command)
```

CEF 形式の送信者フィルタ/認証ログ

表 3-10. CEF 形式の送信者フィルタ/認証ログ

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100137
Header (eventName)	説明	SENDER_FILTERING

CEF キー	説明	値
Header (severity)	メールの重大度	2
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com
cn1Label	イベントの種類のラベル	eventType

CEF キー	説明	値
cn1	イベントの種類	• 1: メールレピュテーション • 2: ディレクトリハーベスト攻撃 (DHA) からの保護 • 3: バウンスメール攻撃からの保護 • 4: SMTP トラフィックスロットリング (IP アドレス) • 5: SMTP トラフィックスロットリング (メールアドレス) • 6: SPF • 7: DKIM • 8: DMARC
act	イベントの処理	• 2: 一時的にブロック • 3: 常にブロック
cn2Label	送信者の認証結果のラベル	rfcResult
cn2	送信者の認証結果	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	ブロック処理の理由	例: No DNS txt record

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1133|100137|SENDER_FILTERING|2|rt=A
pr 27 2018 01:59:38 GMT+00:00 cn1Label=eventType cn1=7 cn2
```

```
Label=rfcResult cn2=5 dvchost=localhost.localdomain device
TranslatedAddress=10.206.155.122 deviceExternalId=15129231
-f1dc-4941-8014-1a1b9fbc9253 dvc=10.206.155.128 act=2 duse
r=user1@domain1.com;user2@domain1.com;user223@domain1.com;
user4@domain1.com reason=102 suser=user1@domain2.com dvcma
c=00:0C:29:8D:2E:74
```

CEF 形式のシステムログ

表 3-11. CEF 形式のシステムログ

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	説明	• PRODUCT_UPDATE (300102) • SYSTEM_EVENT (300999)
Header (severity)	重大度	• 4:低 • 6:中 • 8:高

CEF キー	説明	値
cn1	イベント ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
cn1Label	イベント ID	operationId
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
msg	イベントの詳細	例: Scheduled update - Unable to download Script Analyzer Pattern.
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|300999|SYSTEM_EVENT|3|rt=Mar 24
2015 08:43:35 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC cn3Label=
operationId cn3=30000 msg=Account 'admin' logged on from 1
0.64.50.147 deviceExternalId=c425624a-e9db-4f3f-8088-2726f
15e6587 dvchost=internalbeta.bcc.ddei dvc=10.64.1.131
```

CEF 形式の Time-of-Click プロテクションログ

表 3-12. CEF 形式の Time-of-Click プロテクションログ

CEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100139
Header (eventName)	説明	CTP_DETECTION
Header (severity)	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

CEF キー	説明	値
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
act	イベントの処理	例: • blocked • warned_and_stopped • warned_but_accessed
msg	メールの件名	例: hello
cs1	メールで検出された脅威の名前	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs1Label	メールで検出された脅威の名前	messageId
cs2	送信者のメールアドレス	例: user1@example.com
cs2Label	送信者のメールアドレスのラベル	senderMail
cs3	受信者のメールアドレス	例: user2@example.com
cs3Label	受信者のメールアドレスのラベル	rcptMail
cs4	URL クリックの時間	例: Mar 09 2015 17:05:21 GMT+00:00
cs4Label	URL クリックの時間のラベル	timeOfClick
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

ログの例:

```
Dec 16 06:32:36 ddei-172 CEF:0|Trend Micro|Deep Discovery
Email Inspector|5.1.0.1110|100139|CTP_DETECTION|8|rt=Dec
16 2020 06:30:08 GMT+00:00 cs2Label=senderMail cs2=tarek@
test.com request=http://g9yxzah7yu23n.com suser=tarek@tes
t.com dvchost=ddei-172 dvc=10.204.63.172 deviceExternalId
=2bcbcc98-3f99-40e3-864f-e5f102511631 duser=ddei_test1@de
mo.com msg=syslog - ctp cs3Label=rcptMail cs3=ddei_test1@
demo.com cs1Label=messageId cs1=20201216135712225943830@te
st.com act=blocked dvcmac=00:50:56:A7:D9:FD cs4Label=time
OfClick cs4=Dec 16 2020 06:30:36 GMT+00:00
```

MTA ログ

MTA ログの Syslog コンテンツマッピング情報はありません。Deep Discovery Email Inspector は未加工の MTA ログを Syslog サーバに直接送信します。

ログの例:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```

第 4 章

Syslog コンテンツマッピング - LEEF

次の各表は、Deep Discovery Email Inspector のログ出力と LEEF 形式のシステム出力ログとのコンテンツマッピングを示しています。

- 51 ページの「MTA ログ」

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

LEEF 形式の検出ログ: メール検出ログ

表 4-1. LEEF 形式の検出ログ: メール検出ログ

LEEF キー	説明	値
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	EMAIL_DETECTION
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00

LEEF キー	説明	値
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
mailMsgSubject	メールの件名	例: hello
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	メールのサイズ	例: 30841
msgUuid	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
rcptMail	受信者のメールアドレス	例: user2@example.com
senderMail	送信者のメールアドレス	例: user1@example.com
sev	重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

LEEF キー	説明	値
threatType	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|EMAIL_DETECTION|=8\0x09threatType=
4\0x09deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e0x09mess
ageId=<20150413072949.E8C0D1E9A363@internalbeta.bcc.ddei>\0x0
9msgUuid=6C4A91D7-1396-1405-94C5-D955018F938E\0x09mailMsgSubj
ect=Orcamento Total - 5636005\0x09src=69.162.64.30\0x09msgSiz
e=397113\0x09dvchost=internalbeta.bcc.ddei\0x09dvc=10.64.1.13
1\0x09act=passed\0x09duser=user1@domain1.com\0x09devTime=Apr
13 2015 07:29:50 GMT+00:00\0x09suser=www-data@contato30.danet
mail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09devTimeFormat=MMM d
d yyyy HH:mm:ss z\0x09threatName=VAN_BACKDOOR.UMXX
```

LEEF 形式の検出ログ: 添付ファイル検出ログ

表 4-2. LEEF 形式の検出ログ: 添付ファイル検出ログ

LEEF キー	説明	値
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	ATTACHMENT_DETECTION
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00

LEEF キー	説明	値
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
emailSeverity	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
emailThreats	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント

LEEF キー	説明	値
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
mailMsgSubject	メールの件名	例: hello
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	メールのサイズ	例: 30841
msgUuid	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|ATTACHMENT_DETECTION|sev=8\0x09msgU
```

```
uid=6C4A91D7-1396-1405-94C5-D955018F938E\0x09fileHash=2EF0B334
EFDE7F1BA16011158E25555C2B9D7BC5\0x09emailSeverity=8\0x09suser
=www-data@contato30.danetmail.net\0x09dvchost=internalbeta.bcc
.ddei\0x09emailThreatType=4\0x09duser=spam@support.trendmicro.
com\0x09messageId=<20150413072949.E8C0D1E9A363@internalbeta.bc
c.ddei>\0x09src=69.162.64.30\0x09deviceGUID=034eb532-9318-40d9
-b27b-d9feba7c269e\0x09mailMsgSubject=Orcamento Total - 563600
5\0x09msgSize=397113\0x09fileType=Directory\0x09dvc=10.64.1.13
1\0x09devTime=Apr 13 2015 15:45:58 GMT+00:00\0x09fname=Orcamen
to%20Total.zip\0x09act=passed\0x09dvcmac=C4:34:6B:B8:09:BC\0x0
9devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09threatName=VAN_BACKD
OOR.UMXX\0x09emailThreats=VAN_BACKDOOR.UMXX
```

LEEF 形式の検出ログ: URL 検出ログ

表 4-3. LEEF 形式の検出ログ: URL 検出ログ

LEEF キー	説明	値
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	URL_DETECTION

LEEF キー	説明	値
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost

LEEF キー	説明	値
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
eventTriggeredValue	実行値	例: 35
emailSeverity	メールの重大度	• 4: 低 • 6: 中 • 8: 高
emailThreats	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント
mailMsgSubject	メールの件名	例: hello
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	メールのサイズ	例: 30841
msgUuid	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03

LEEF キー	説明	値
sev	重大度	• 4: 低 • 6: 中 • 8: 高
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
url	URL	例: http://1.2.3.4/query?term=value
urlCat	カテゴリ	例: 90: 02

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|URL_DETECTION|sev=4\0x09deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e\0x09msgUuid=6C4A91D7-13
96-1405-94C5-D955018F938E\0x09mailMsgSubject=Orcamento Total
-5636005\0x09src=69.162.64.30\0x09emailSeverity=8\0x09msgSize
=397113\0x09dvchost=internalbeta.bcc.ddei0x09dvc=10.64.1.131\
0x09emailThreatType=4\0x09duser=user1@domain1.com\0x09url=htt
p://200.98.168.34/testam1/t3zs3.html\0x09act=passed\0x09devTi
me=Apr 13 2015 15:45:58 GMT+00:00\0x09suser=www-data@contato3
0.danetmail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09devTimeForma
t=MMM dd yyyy HH:mm:ss z\0x09messageId=<20150413072949.E8C0D1
E9A363@internalbeta.bcc.ddei>\0x09emailThreats=VAN_BACKDOOR.U
MXX
```

LEEF 形式のアラートログ

表 4-4. LEEF 形式のアラートログ

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	ALERT_EVENT
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
eventTriggeredValue	実行値	例: 35
externalId	アラートデータベースのログ ID	例: 1648

LEEF キー	説明	値

ruleContent	通知のコンテンツ	例:
		
		`The following email messages contain threats:`
		
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <20150619032243.5923E650365@localhost.ddei-164>`
		`Recipients: fake@test.com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263`
		`Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		
		`Alert time: 2015-05-25 11:11:27 +0800`
		`Generated by: localhost.localdomain (192.168.1.100)`
		`Management console: https://192.168.1.100/loginPage.ddei`
		
		注意
		最大長は 20000 文字です。

ruleCriteria	説明	例: 1 or more messages detected with threats

LEEF キー	説明	値
ruleEventType	アラートの種類	• 0: システムイベント • 1: セキュリティイベントおよびイベントの重大度が「高」、「中」、または「低」 • 2: セキュリティイベントおよびイベントの重大度が「高」または「中」 • 3: セキュリティイベントおよびイベントの重大度が「高」
ruleId	アラート ID	1〜15 の値
ruleName	アラート名	例: Security: Suspicious Messages Identified
sev	重大度	• 2: 情報 • 6: 重要 • 8: 重大

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1009|ALERT_EVENT|sev=2\0x09cnt=8\0x09rul
eEventType=0\0x09ruleId=10\0x09ruleCriteria=At least 1 message
s processed\0x09dvchost=localhost.ddei-164\0x09dvc=10.204.253.
164\0x09deviceGUID=361a091c-addd-40cf-98e7-710e43500a66\0x09ex
ternalId=1684\0x09devTime=Jun 19 2015 03:18:48 GMT+00:00\0x09r
uleName=System: Processing Surge\0x09dvcmac=00:50:56:01:2C:BC\
0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09ruleContent=The%2
0number%20of%20processed%20messages%20reached%20the%20specifie
d%20threshold%20%281%29.%0A%0AMessages%20processed%3A%208%0ACh
ecking%20interval%3A%200%20minutes%0A%0AAlert%20time%3A%202015
-06-19%2003%3A18%3A48%20%2B0000%0AGenerated%20by%3A%20localhos
```

```
t.ddei-164%20%2810.204.253.164%29%0AManagement%20console%3A%20
https%3A//10.204.253.164/loginPage.ddei
```

LEEF 形式の仮想アナライザ分析ログ: ファイル分析

表 4-5. LEEF 形式の仮想アナライザ分析ログ: ファイル分析

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Trend Micro
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	FILE_ANALYZED
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
deviceOSName	サンドボックスイメージの種類	例: win7
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00

LEEF キー	説明	値
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
gridIsKnownGood	GRID/CSSS の結果	• 0: GRID が無害と知られていない • 1: GRID が無害と知られている
malName	不正プログラム名	例: HEUR_NAMETRICK.A
pcapReady	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
pComp	検出エンジン/コンポーネント	Sandbox
rozRating	ROZ レーティング(仮想アナライザによる解析結果を示す内部コード)	例: 3
sev	重大度	3

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|FILE_ANALYZED|devTime=Apr 13 2015
07:45:54 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x
09sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=inte
rnalbeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09d
eviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fname=Or\x8
7amento Total.cpl\0x09fileHash=2EF0B334EFDE7F1BA16011158E25555
C2B9D7BC5\0x09deviceProcessHash=61DD815ABF2D1FFC58F261392DAFF4
F11B59D79C\0x09malName=VAN_BACKDOOR.UMXX\0x09fileType=Win32 DL
L\0x09fsize=482816\0x09deviceOSName=win81en\0x09gridIsKnownGoo
d=-1\0x09rozRating=3\0x09pcapReady=1
```

LEEF 形式の仮想アナライザ分析ログ: URL 分析

表 4-6. LEEF 形式の仮想アナライザ分析ログ: URL 分析

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	URL_ANALYZED
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

LEEF キー	説明	値
deviceOSName	サンドボックスイメージの種類	例: win7
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pcapReady	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
pComp	検出エンジン/コンポーネント	Sandbox
rozRating	ROZ レーティング(仮想アナライザによる解析結果を示す内部コード)	例: 3
sev	重大度	3
url	URL	例: http://1.2.3.4/query?term=value

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|URL_ANALYZED|devTime=Apr 13 2015 07
:34:41 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09
sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=intern
albeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09dev
iceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fileHash=BF68
52C834224BD2C26AC4BE20E7E08930B39FEF\0x09deviceOSName=win7sp1e
n\0x09url=http://climtorg.ru/bitrix/admin/1up\0x09rozRating=3\
0x09pcapReady=1
```

LEEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

表 4-7. LEEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	NOTABLE_CHARACTERISITICS
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57

LEEF キー	説明	値
deviceOSName	サンドボックスイメージの種類	例: win7
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: msg=Dropping Process ID: 2984\n File: %USERPROFILE% \AppData\Local\MICROSOFT \INTERNET EXPLORER\ Recovery \High\LAST ACTIVE\{D78424A0 E1AA-11E4-B7C5-7CC9C8DA4AD 2}.DAT\nType: VSDT_WINWORD\
pComp	検出エンジン/コンポーネント	Sandbox
ruleCategory	違反ポリシー名	例: Internet Explorer Setting Modification
ruleName	違反イベントの分析	例: Modified important registry items
sev	重大度	3

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|NOTABLE_CHARACTERISTICS|devTime=Ap
r 13 2015 07:01:13 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:
mm:ss z\0x09sev=6\0x09pComp=Sandbox\0x09dvc=10.64.1.132\0x09dv
chost=internalbeta.tapping.ddei\0x09deviceMacAddress=B0:83:FE:
DD:21:98\0x09deviceGUID=e57f0651-b197-42d4-a643-271c1277b5ff\0
x09fname=http://yt1nutj.wvp78.com/\0x09fileHash=8213271FD287C3
F27D6975FE0545AB77DC8EBF73\0x09fileType=URL\0x09fsize=0\0x09ru
leCategory=File drop, download, sharing, or replication\0x09ru
leName=Drops file that can be used to infect systems\0x09msg=D
ropping Process ID: 2984\nFile: %USERPROFILE%\AppData\Local\MI
CROSOFT\INTERNET EXPLORER\Recovery\High\LAST ACTIVE\{D78424A0-
E1AA-11E4-B7C5-7CC9C8DA4AD2}.DAT\nType: VSDT_WINWORD\0x09devic
eOSName=win7sp1en
```

LEEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

表 4-8. LEEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro

LEEF キー	説明	値
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	DENYLIST_CHANGE
act	イベントの処理	• Add • Remove
deviceExternalRiskType	リスクレベル	• Low • Medium • High • Confirmed Malware
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dhost	送信先ホスト名	例: dhost1
dpt	送信先ポート	0〜65535 の値
dst	送信先 IP アドレス	例: 10.1.144.199
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
end	レポート終了時刻	例: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

LEEF キー	説明	値
pComp	検出エンジン/コンポーネント	Sandbox
sev	重大度	3
type	拒否リストの種類	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
url	URL	例: http://1.2.3.4/query?term=value

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|DENYLIST_CHANGE|devTime=Apr 13 201
5 07:47:01 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\
0x09sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=in
ternalbeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x0
9deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09end=May 1
3 2015 07:44:37 GMT+00:00\0x09act=Add\0x09dst=200.98.168.34\0x
09dpt=80\0x09deviceExternalRiskType=Medium\0x09type=Deny List
IP/Port
```

LEEF 形式のメッセージ追跡ログ

表 4-9. LEEF 形式のメッセージ追跡ログ

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	MESSAGE_TRACKING
sev	メールの重大度	• 2: 使用不可 • 2: 未評価 • 2: 標準 • 4: 低 • 6: 中 • 8: 高
dvc	アプライアンスの IP アドレス	例: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost

LEEF キー	説明	値
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgUuid	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com
mailMsgSubject	メールの件名	例: hello
reason	ブロック処理の理由	例: Timeout period expired
latestStatus	最新のステータス	• Deleted • Delivered • Delivery unsuccessful • Processing completed • Quarantined • Recipient changed
src	送信元 IP アドレス	例: 10.1.144.199
senderMail	送信者のメールアドレス	例: user1@example.com
rcptMail	受信者のメールアドレス	例: user2@example.com
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146

LEEF キー	説明	値
procHistory	処理履歴	例: デバイスが実行した処理。形式: "タイムスタンプ 1 処理 1,タイムスタンプ 2 処理 2,..., タイムスタンプ n 処理 n"

ログの例:

```
May 15 16:00:4 7 internalbeta LEEF:1.0|Trend Micro|Deep Di
scovery Email Inspector|3.1.0.1154|MESSAGE_TRACKING|sev=2<
009>latestStatus=Processing completed<009>procHistory=May
15 2018 08:00:33 GMT+00:00 Received,May 15 2018 08:00:33 G
MT+00:00 Action set to 'pass',May 15 2018 08:00:33 GMT+00:
00 Processing completed<009>msgUuid=46252714-6C39-FF05-98F
4-5C63BCB20569<009>mailMsgSubject=Time is running out: New
 data privacy permissions<009>src=104.130.122.63<009>sende
rMail=sap@mailsap.com<009>suser=bounce+814a73.7ecda73-jeff
_lovelace=trendmicro.com@mailsap.com<009>dvchost=internalb
eta.bcc.ddei<009>dvc=10.64.1.131<009>duser=jeff_lovelace@t
rendmicro.com<009>deviceGUID=67067637-acbf-46de-a22d-be8d0
d976cd5<009>rcptMail=jeff_lovelace@trendmicro.com<009>devT
ime=May 15 2018 08:00:33 GMT+00:00<009>messageId=201805150
80033.0EE4B6834964@internalbeta.bcc.ddei<009>dvcmac=EC:F4:
BB:DE:E5:30<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>d
eviceTranslatedAddress=104.130.122.63
```

LEEF 形式の送信者フィルタ/認証ログ

表 4-10. LEEF 形式の送信者フィルタ/認証ログ

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	1.0

LEEF キー	説明	値
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	説明	SENDER_FILTERING
sev	メールの重大度	2
dvc	アプライアンスの IP アドレス	例: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

LEEF キー	説明	値
eventType	イベントの種類	• 1: メールレピュテーション • 2: ディレクトリハーベスト攻撃 (DHA) からの保護 • 3: バウンスメール攻撃からの保護 • 4: SMTP トラフィックスロットリング (IP アドレス) • 5: SMTP トラフィックスロットリング (メールアドレス) • 6: SPF • 7: DKIM • 8: DMARC
act	イベントの処理	• 2:一時的にブロック • 3:常にブロック
rfcResult	送信者の認証結果	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	ブロック処理の理由	例:No DNS txt record

ログの例:

```
May 15 16:00:4 7 internalbeta LEEF:1.0|Trend Micro|Deep Di
scovery Email Inspector|3.1.0.1147|SENDER_FILTERING|sev=2<
009>deviceGUID=15129231-f1dc-4941-8014-1a1b9fbc9253<009>rf
cResult=5<009>eventType=6<009>deviceTranslatedAddress=10.2
06.155.122<009>dvchost=localhost.localdomain<009>dvc=10.20
6.155.128<009>act=2<009>duser=user1@domain.com<009>reason=
```

```
56<009>devTime=May 15 2018 08:15:31 GMT+00:00<009>suser=us
er2@domain2.com<009>dvcmac=00:0C:29:8D:2E:74<009>devTimeFo
rmat=MMM dd yyyy HH:mm:ss z
```

LEEF 形式のシステムログ

表 4-11. LEEF 形式のシステムログ

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	イベント名	PRODUCT_UPDATE SYSTEM_EVENT
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost

LEEF キー	説明	値
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
msg	イベントの詳細	例: Scheduled update - Unable to download Script Analyzer Pattern.
operationId	イベント ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
sev	重大度	3

注意

LEEF ログ構文を使用する場合は、イベント属性をタブ区切り記号「\0x09」で区切ります。

ログの例:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|SYSTEM_EVENT|sev=3\0x09deviceGUID
=e57f0651-b197-42d4-a643-271c1277b5ff\0x09devTime=Apr 13 2015
 06:52:00 GMT+00:00\0x09msg=Logout: 'admin' logged off\0x09dv
cmac=B0:83:FE:DD:21:98\0x09devTimeFormat=MMM dd yyyy HH:mm:ss
 z\0x09dvchost=internalbeta.tapping.ddei\0x09dvc=10.204.253.1
63\0x09operationId=30000
```

LEEF 形式の Time-of-Click プロテクションログ

表 4-12. LEEF 形式の Time-of-Click プロテクションログ

LEEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45

LEEF キー	説明	値
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	LEEF 形式のバージョン	LEEF: 1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventName)	説明	CTP_DETECTION
Header (severity)	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	時刻の形式	yyyy MMM dd HH:mm:ss z
url	URL	例: http://1.2.3.4/query?term=value

LEEF キー	説明	値
act	イベントの処理	例: • blocked • warned_and_stopped • warned_but_accessed
mailMsgSubject	メールの件名	例: hello
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
senderMail	送信者のメールアドレス	例: user1@example.com
rcptMail	受信者のメールアドレス	例: user2@example.com
timeOfClick	URL クリックの時間	例: Mar 09 2015 17:05:21 GMT+00:00
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

ログの例:

```
Dec 16 06:38:57 ddei-172 LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|5.1.0.1110|CTP_DETECTION|deviceGUID=2bcbcc9
8-3f99-40e3-864f-e5f102511631<009>mailMsgSubject=syslog - ct
p<009>url=http://g9yxzah7yu23n.com<009>dvchost=ddei-172<009>
messageId=20201216135712225943830test.com<009>senderMail=tar
ek@test.com<009>dvc=10.204.63.172<009>act=blocked<009>duser=
ddei_test1@demo.com<009>rcptMail=ddei_test1@demo.com<009>dev
Time=Dec 16 2020 06:30:08 GMT+00:00<009>timeOfClick=Dec 16 2
020 06:36:56 GMT+00:00<009>dvcmac=00:50:56:A7:D9:FD<009>devT
imeFormat=MMM dd yyyy HH:mm:ss z<009>suser=tarek@test.com
```

MTA ログ

MTA ログの Syslog コンテンツマッピング情報はありません。Deep Discovery Email Inspector は未加工の MTA ログを Syslog サーバに直接送信します。

ログの例:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```

第 5 章

Syslog コンテンツマッピング - TMEF

次の各表は、Deep Discovery Email Inspector のログ出力と TMEF 形式のシステム出力ログとのコンテンツマッピングを示しています。

- 118 ページの「TMEF 形式の Time-of-Click プロテクションログ」
- 51 ページの「MTA ログ」

TMEF 形式の検出ログ:メール検出ログ

表 5-1. TMEF 形式の検出ログ:メール検出ログ

TMEF キー	説明	値
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100130
Header (eventName)	説明	EMAIL_DETECTION
Header (severity)	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高

TMEF キー	説明	値
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
cn1	メールのサイズ	例: 30841
cn1Label	メールのサイズ	msgSize
cs1	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs1Label	社内メールの ID	msgUuid
cs2	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	メール ID	messageId
cs3	送信者のメールアドレス	例: user1@example.com
cs3Label	送信者のメールアドレスのラベル	senderMail
cs4	受信者のメールアドレス	例: user2@example.com

TMEF キー	説明	値
cs4Label	受信者のメールアドレスのラベル	rcptMail
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
mailMsgSubject	メールの件名	例: hello
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

TMEF キー	説明	値
threatType	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|100130|EMAIL_DETECTION|8|rt=Apr 13 201
5 08:49:22 GMT+00:00 src=141.251.58.19 threatType=4 deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e mailMsgSubject=phishwatc
h Digest, Vol 2933, Issue 13 act=passed dvchost=internalbeta.b
cc.ddei cs2Label=messageId cs2=<20150413084922.2052D1E9A066@in
ternalbeta.bcc.ddei dvc=10.64.1.131 cs1Label=msgUuid cs1=ECBC7
B7E-1397-3005-94C5-0BA1DA0913D2 duser=user1@domain2.com suser=
user1@domain1.com dvcmac=C4:34:6B:B8:09:BC threatName=VAN_MALW
ARE.UMXX cn1Label=msgSize cn1=1204948
```

TMEF 形式の検出ログ: 添付ファイル検出ログ

表 5-2. TMEF 形式の検出ログ: 添付ファイル検出ログ

TMEF キー	説明	値
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro

TMEF キー	説明	値
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100131
Header (eventName)	説明	ATTACHMENT_DETECTION
Header (severity)	添付ファイルの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
cn1	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高

TMEF キー	説明	値
cn1Label	メールの重大度	emailSeverity
cn2	メールのサイズ	例: 30841
cn2Label	メールのサイズ	msgSize
cn3	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント
cn3Label	脅威の種類	emailThreatType
cs1	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	メールで検出された脅威の名前	emailThreats
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	社内メールの ID	msgUuid
cs3	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	メール ID	messageId
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

TMEF キー	説明	値
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
mailMsgSubject	メールの件名	例: hello
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Email Inspector|2.5.1.1161|100131|ATTACHMENT_DETECTION|8|rt=Apr 13 2015 16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3=<20150413084922.2052D1E9A066@internalbeta.bcc.ddei cn1Label=emailSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2933, Issue 13 fileHash=E07B349245FCDDB31CBF5A52012807E955D2EB7A fileType=Directory act=passed dvchost=internalbeta.bcc.ddei dvc=10.64.1.131 deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269
```

```
e duser=user1@domain.com cn2Label=msgSize cn2=1204948 cn3Label
=emailThreatType cn3=4 fname=JNSA%20CSIRT-%E3%82%AA%E3%83%AA%E
3%83%91%E3%83%A9.pdf suser=user2@domain.com dvcmac=C4:34:6B:B8
:09:BC cs1Label=emailThreats cs1=VAN_MALWARE.UMXX threatName=V
AN_MALWARE.UMXX cs2Label=msgUuid cs2=ECBC7B7E-1397-3005-94C5-0
BA1DA0913D2
```

TMEF 形式の検出ログ: URL 検出ログ

表 5-3. TMEF 形式の検出ログ: URL 検出ログ

TMEF キー	説明	値
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100132
Header (eventName)	説明	URL_DETECTION
Header (severity)	URL の重大度	• 4: 低 • 6: 中 • 8: 高

TMEF キー	説明	値
act	イベントの処理	例: • analyzed • cleaned up • deleted • delivered directly • encrypted • file sanitized • passed • quarantined • recipient changed • stamped • stripped • subjectsTagged
cn1	メールの重大度	• 4: 低 • 6: 中 • 8: 高
cn1Label	メールの重大度	emailSeverity
cn2	メールのサイズ	例: 30841
cn2Label	メールのサイズ	msgSize

TMEF キー	説明	値
cn3	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント
cn3Label	脅威の種類	emailThreatType
cs1	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	メールで検出された脅威の名前	emailThreats
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	社内メールの ID	msgUuid
cs3	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	メール ID	messageId
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	メール受信者	例: user1@example2.com;test@163.com

TMEF キー	説明	値
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
mailMsgSubject	メールの件名	例: hello
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com
threatName	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
urlCat	カテゴリ	例: 90: 02

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|100132|URL_DETECTION|6|rt=Apr 13 2015
16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3=<2
0150413084922.2052D1E9A066@internalbeta.bcc.ddei cn1Label=emai
lSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2933, Is
sue 13 request=http://202.502.27.71:6610/ctldl.windowsupdate.c
om/msdownload/update/v3/static/trustedr/en/disallowedcertstl.c
ab?7f8b3bbc9534919b?7f8b3bbc9534919b act=passed dvchost=intern
albeta.bcc.ddei dvc=10.64.1.131 duser=user1@domain.com cn2Labe
l=msgSize cn2=1204948 cn3Label=emailThreatType cn3=4 suser=use
r2@domain.com dvcmac=C4:34:6B:B8:09:BC cs1Label=emailThreats c
s1=VAN_MALWARE.UMXX deviceGUID=034eb532-9318-40d9-b27b-d9feba7
c269e cs2Label=msgUuid cs2=ECBC7B7E-1397-3005-94C5-0BA1DA0913D
2
```

TMEF 形式のアラートログ

表 5-4. TMEF 形式のアラートログ

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	300105
Header (eventName)	説明	ALERT_EVENT
Header (severity)	アラートの重大度	• 2: 情報 • 6: 重要 • 8: 重大
cn1	アラートの種類	• 0: システムイベント • 1: セキュリティイベントおよびイベントの重大度が「高」、「中」、または「低」 • 2: セキュリティイベントおよびイベントの重大度が「高」または「中」 • 3: セキュリティイベントおよびイベントの重大度が「高」
cn1Label	アラートの種類	ruleEventType

TMEF キー	説明	値
cs1	説明	例: 1 or more messages detected with threats
cs1Label	説明	ruleCriteria
cs2	実行値	例: 35
cs2Label	実行値	eventTriggeredValue

cs3	通知のコンテンツ	例:
		`The following email messages contain threats:`
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <20150619032243.5923E650365@localhost.ddei-164>`
		`Recipients: fake@test.com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263`
		`Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		`Alert time: 2015-05-25 11:11:27 +0800`
		`Generated by: localhost.localdomain (192.168.1.100)`
		`Management console: https://192.168.1.100/loginPage.ddei`
		注意
		最大長は 20000 文字です。

TMEF キー	説明	値
cs3Label	通知のコンテンツ	ruleContent
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
externalId	アラートデータベースのログ ID	例: 1648
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
ruleId	アラート ID	1〜15 の値
ruleName	アラート名	例: Security: Suspicious Messages Identified

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1009|300105|ALERT_EVENT|2|rt=Jun 19 2015 03
:22:58 GMT+00:00 cnt=7 deviceGUID=361a091c-addd-40cf-98e7-710e
43500a66 ruleId=10 cs2Label=ruleContent cs2=The%20number%20of%
20processed%20messages%20reached%20the%20specified%20threshold
%20%281%29.%0A%0AMessages%20processed%3A%207%0AChecking%20inte
rval%3A%200%20minutes%0A%0AAlert%20time%3A%202015-06-19%2003%3
A22%3A58%20%2B0000%0AGenerated%20by%3A%20localhost.ddei-164%20
%2810.204.253.164%29%0AManagement%20console%3A%20https%3A//10.
204.253.164/loginPage.ddei cs1Label=ruleCriteria cs1=At least
1 messages processed dvchost=localhost.ddei-164 dvc=10.204.253
.164 externalId=1694 ruleName=System: Processing Surge dvcmac=
00:50:56:01:2C:BC cn1Label=ruleEventType cn1=0
```

TMEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

表 5-5. TMEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200119
Header (eventName)	説明	FILE_ANALYZED
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
cn1	GRID/CSSS の結果	• 0: GRID が無害と知られていない • 1: GRID が無害と知られている
cn1Label	GRID/CSSS の結果	GRIDIsKnownGood
cn2	ROZ レーティング(仮想アナライザによる解析結果を示す内部コード)	例: 3
cn2Label	ROZ レーティング	ROZRating

TMEF キー	説明	値
cn3	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
cn3Label	PCAP 使用可能	PcapReady
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
deviceOSName	サンドボックスイメージの種類	例: win7
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
malName	不正プログラム名	例: HEUR_NAMETRICK.A
pComp	検出エンジン/コンポーネント	Sandbox
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200119|FILE_ANALYZED|3|rt=Apr 13 2015
08:58:20 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=inter
nalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e fname=JNSA CSIRT-example
.pdf fileHash=E07B349245FCDDB31CBF5A52012807E955D2EB7A malName
=VAN_MALWARE.UMXX fileType=Adobe Portable Document Format(PDF)
 fsize=875029 deviceOSName=win81en cn1Label=GRIDIsKnownGood cn
1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

TMEF 形式の仮想アナライザ分析ログ: URL 分析イベント

表 5-6. TMEF 形式の仮想アナライザ分析ログ: URL 分析イベント

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200126
Header (eventName)	説明	URL_ANALYZED
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高

TMEF キー	説明	値
cn2	ROZ レーティング(仮想アナライザによる解析結果を示す内部コード)	例: 3
cn2Label	ROZ レーティング	ROZRating
cn3	PCAP 使用可能	• 0: PCAP が使用可能でない • 1: PCAP が使用可能
cn3Label	PCAP 使用可能	PcapReady
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
deviceOSName	サンドボックスイメージの種類	例: win7
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	検出エンジン/コンポーネント	Sandbox
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200126|URL_ANALYZED|3|rt=Apr 13 2015 0
8:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=intern
albeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID=
034eb532-9318-40d9-b27b-d9feba7c269e request=http://www.castel
ir.it/take/Small-9422.html fileHash=6389250B8468C46443FD775F6E
B744D6105B8DF3 deviceOSName=xpsp3en cn2Label=ROZRating cn2=3 c
n3Label=PcapReady cn3=1
```

TMEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

表 5-7. TMEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200127
Header (eventName)	説明	NOTABLE_CHARACTERISITICS
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高

TMEF キー	説明	値
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
deviceOSName	サンドボックスイメージの種類	例: win7
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: s1.bdstatic.com
pComp	検出エンジン/コンポーネント	Sandbox
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+00:00
ruleCategory	違反ポリシー名	例: Internet Explorer Setting Modification
ruleName	違反イベントの分析	例: Modified important registry items

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200127|NOTABLE_CHARACTERISTICS|6|rt=Ap
r 13 2015 08:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvc
host=internalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC
```

```
deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e fname=http://w
ww.castelir.it/take/Small-9422.html fileHash=6389250B8468C4644
3FD775F6EB744D6105B8DF3 fileType=URL fsize=0 ruleCategory=Susp
icious network or messaging activity ruleName=Queries DNS serv
er msg=s1.bdstatic.com deviceOSName=xpsp3en
```

TMEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

表 5-8. TMEF 形式の仮想アナライザ分析ログ: 拒否リストトランザクションイベント

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	200120
Header (eventName)	説明	DENYLIST_CHANGE
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
act	イベントの処理	• Add • Remove

TMEF キー	説明	値
cs1	拒否リストの種類	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	拒否リストの種類	type
deviceExternalRiskType	リスクレベル	• 1: 低 • 2: 中 • 3: 高 • 4: 確認された不正プログラム
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
dhost	送信先ホスト名	例: dhost1
dpt	送信先ポート	0〜65535 の値
dst	送信先 IP アドレス	例: 10.1.144.199
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
end	レポート終了時刻	例: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	検出エンジン/コンポーネント	Sandbox

TMEF キー	説明	値
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200120|DENYLIST_CHANGE|3|rt=Apr 14 201
5 10:25:24 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=int
ernalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGU
ID=034eb532-9318-40d9-b27b-d9feba7c269e cs1Label=type cs1=Deny
 List File SHA1 end=May 14 2015 09:59:20 GMT+00:00 act=Add fil
eHash=522A90D077884E880A454A4D8E1A315FCE36BB12 deviceExternalR
iskType=High
```

TMEF 形式のメッセージ追跡ログ

表 5-9. TMEF 形式のメッセージ追跡ログ

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100136

TMEF キー	説明	値
Header (eventName)	説明	MESSAGE_TRACKING
Header (severity)	メールの重大度	• 2: 使用不可 • 2: 未評価 • 2: 標準 • 4: 低 • 6: 中 • 8: 高
dvc	アプライアンスの IP アドレス	例: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
cs1Label	メール ID のラベル	messageId
cs1	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	社内メールの ID のラベル	msgUuid
cs2	社内メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	メール送信者	例: user2@example.com

TMEF キー	説明	値
duser	メール受信者	例: user1@example2.com;test@163.com
mailMsgSubject	メールの件名	例: hello
reason	ブロック処理の理由	例: Timeout period expired
cs3Label	最新のステータス	latestStatus
cs3	詳細	• Deleted • Delivered • Delivery unsuccessful • Processing completed • Quarantined • Recipient changed
src	送信元 IP アドレス	例: 10.1.144.199
cs4Label	送信者のメールアドレスのラベル	senderMail
cs4	送信者のメールアドレス	例: user1@example.com
cs5Label	受信者のメールアドレスのラベル	rcptMail
cs5	受信者のメールアドレス	例: user2@example.com
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146
cs6Label	処理履歴のラベル	procHistory
cs6	処理履歴	例: デバイスが実行した処理。形式: "タイムスタンプ 1 処理 1,タイムスタンプ 2 処理 2,..., タイムスタンプ n 処理 n"

ログの例:

```
May 15 16:08:12 internalbeta CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1154|100136|MESSAGE_TRACKING|2|rt=May
15 2018 08:02:50 GMT+00:00 src=199.59.150.74 deviceGUID=67067
637-acbf-46de-a22d-be8d0d976cd5 cs6Label=procHistory cs6=May
15 2018 08:02:50 GMT+00:00 Received,May 15 2018 08:02:51 GMT+
00:00 Sent for analysis,May 15 2018 08:07:52 GMT+00:00 Action
 set to 'pass',May 15 2018 08:07:52 GMT+00:00 Processing comp
leted  mailMsgSubject=BBC News (World)"US to open controversi
al Jerusalem embassy" deviceTranslatedAddress=199.59.150.74 d
vchost=internalbeta.bcc.ddei dvc=10.64.1.131 duser=user1@doma
in.com cs1Label=messageId cs1=20180515080250.DEDC168349EC@int
ernalbeta.bcc.ddei cs4Label=senderMail cs4=info@twitter.com c
s5Label=rcptMail cs5=user2@domain2.com suser=n066660a6ef-3786
c6192ef34d49a9435fb49c655529-user2\=\=\=domain2.com@bounce.tw
itter.com dvcmac=EC:F4:BB:DE:E5:30 cs3Label=latestStatus cs3=
Processing completed cs2Label=msgUuid cs2=105D32B1-6C3A-0705-
954B-563DDB1B5714
```

TMEF 形式の送信者フィルタ/認証ログ

表 5-10. TMEF 形式の送信者フィルタ/認証ログ

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	CEF 形式のバージョン	1.0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100137

TMEF キー	説明	値
Header (eventName)	説明	SENDER_FILTERING
Header (severity)	メールの重大度	2
dvc	アプライアンスの IP アドレス	例: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
deviceTranslatedAddress	リレー MTA の IP アドレス	例: 204.92.31.146
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com
cn1Label	イベントの種類のラベル	eventType

TMEF キー	説明	値
cn1	イベントの種類	• 1: メールレピュテーション • 2: ディレクトリハーベスト攻撃 (DHA) からの保護 • 3: バウンスメール攻撃からの保護 • 4: SMTP トラフィックスロットリング (IP アドレス) • 5: SMTP トラフィックスロットリング (メールアドレス) • 6: SPF • 7: DKIM • 8: DMARC
act	イベントの処理	• 2: 一時的にブロック • 3: 常にブロック
cn2Label	送信者の認証結果のラベル	rfcResult
cn2	送信者の認証結果	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	ブロック処理の理由	例: No DNS txt record

ログの例:

```
May 15 16:08:12  internalbeta CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1147|100137|SENDER_FILTERING|2|rt=May 1
5 2018 08:20:01 GMT+00:00 cn1Label=eventType cn1=7 cn2Label=
```

```
rfcResult cn2=5 deviceTranslatedAddress=10.206.155.122 dvchost
=localhost.localdomain dvc=10.206.155.128 act=2 duser=user1@do
main.com reason=102 deviceGUID=15129231-f1dc-4941-8014-1a1b9fb
c9253 suser=user1@domain2.com dvcmac=00:0C:29:8D:2E:74
```

TMEF 形式のシステムログ

表 5-11. TMEF 形式のシステムログ

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	説明	• PRODUCT_UPDATE (300102) • SYSTEM_EVENT (300999)
Header (severity)	重大度	• 4: 低 • 6: 中 • 8: 高
cn1	イベント ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999

TMEF キー	説明	値
cn1Label	イベント ID	operationId
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
msg	イベントの詳細	例: Scheduled update - Unable to download Script Analyzer Pattern.
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|300999|SYSTEM_EVENT|3|rt=Apr 13 2015 0
9:31:08 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC deviceGUID=034eb532
-9318-40d9-b27b-d9feba7c269e cn1Label=operationId cn1=30000 ms
g=Login: 'admin' logged on from 10.204.253.21 dvchost=internal
beta.bcc.ddei dvc=10.204.253.163
```

TMEF 形式の Time-of-Click プロテクションログ

表 5-12. TMEF 形式の Time-of-Click プロテクションログ

TMEF キー	説明	値
Header (timestamp)	「Mmm dd hh:mm:ss」形式のローカル時間	例: Dec 5 05:26:45
Header (host)	ドメイン情報を含まないホスト名	例: internalAP1

TMEF キー	説明	値
Header (logVer)	TMEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダー	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Email Inspector
Header (pver)	アプライアンスのバージョン	例: 5.1.0.1110
Header (eventid)	署名 ID	100139
Header (eventName)	説明	CTP_DETECTION
Header (severity)	メールの重大度	• 2: 未評価 • 4: 低 • 6: 中 • 8: 高
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+00:00
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage

TMEF キー	説明	値
act	イベントの処理	例: • blocked • warned_and_stopped • warned_but_accessed
mailMsgSubject	メールの件名	例: hello
cs1	メールのメッセージ ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs1Label	メールのメッセージ ID のラベル	messageId
cs2	送信者のメールアドレス	例: user1@example.com
cs2Label	送信者のメールアドレスのラベル	senderMail
cs3	受信者のメールアドレス	例: user2@example.com
cs3Label	受信者のメールアドレスのラベル	rcptMail
cs4	URL クリックの時間	例: Mar 09 2015 17:05:21 GMT+00:00
cs4Label	URL クリックの時間のラベル	timeOfClick
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

ログの例:

```
Dec 16 06:42:06 ddei-172 CEF:0|Trend Micro|Deep Discovery
 Email Inspector|5.1.0.1110|100139|CTP_DETECTION|8|rt=Dec
 16 2020 06:30:08 GMT+00:00 cs2Label=senderMail cs2=tarek
@test.com deviceGUID=2bcbcc98-3f99-40e3-864f-e5f102511631
 mailMsgSubject=syslog - ctp request=http://g9yxzah7yu23n
```

```
.com suser=tarek@test.com dvchost=ddei-172 dvc=10.204.63.
172 duser=ddei_test1@demo.com cs3Label=rcptMail cs3=ddei_
test1@demo.com cs1Label=messageId cs1=2020121613571222594
383@test.com act=blocked dvcmac=00:50:56:A7:D9:FD cs4Labe
l=timeOfClick cs4=Dec 16 2020 06:40:11 GMT+00:00
```

MTA ログ

MTA ログの Syslog コンテンツマッピング情報はありません。Deep Discovery Email Inspector は未加工の MTA ログを Syslog サーバに直接送信します。

ログの例:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```