Deep Discovery™ Inspector 6.0

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

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

P/N: APEM69304/210728_JP (2022/01)

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 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 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

第 5 章：Syslog コンテンツマッピング - TMEF

索引

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 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 Inspector を設定して管理する方法の詳細な手順、および Deep Discovery Inspector の概念や機能に関する説明が記載されています。
AWS 配信ガイド	AWS 配信ガイドには、Deep Discovery Inspector の AWS への導入の計画、実施、およびトラブルシューティングに関する要件および手順についての情報が含まれています。
インストールガイド	インストールガイドには、Deep Discovery 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。
VMware NSX-T ポートミラーリングガイド	VMware NSX-T ポートミラーリングガイドには、Deep Discovery Inspector 導入環境に VMware NSX-T でのミラーリングを設定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 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 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 Inspector のコンポーネントと機能、Deep Discovery Inspector を設定するために必要な手順が説明されています。

ドキュメント	説明
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 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
- データベース管理
- ウイルス対策とコンテンツのセキュリティ保護

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

表記規則	説明
 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

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 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 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、17 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 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、39 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 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、65 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 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。

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)
CCCA	Command and Control Contact Alert (コマンド&コントロールコンタクトアラート)

第 2 章

改訂

バージョン 6.0 の改訂はありません。

第 3 章

Syslog コンテンツマッピング - CEF

次の各表は、Deep Discovery 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。

CEF 形式の脅威ログ

表 3-1. CEF 形式の脅威ログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	イベント ID	例: 8
Header (eventName)	説明	例: Packed executable file copied to a network administrative share
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
act	イベントの処理	blocked または not blocked
app	プロトコル	例: HTTP
c6a1	注目すべき IPv6	例: 2001:0:0:1::21
c6a1Label	注目すべき IPv6	InterestedIPv6
c6a2	送信元 IPv6 アドレス	例: 2001:0:0:1::21
c6a2Label	送信元 IPv6 アドレス	送信元 IPv6 アドレス
c6a3	送信先 IPv6 アドレス	例: 2001:0:0:1::21
c6a3Label	送信先 IPv6 アドレス	送信先 IPv6 アドレス
c6a4	ピア IPv6 アドレス	例: 2001:0:0:1::21
c6a4Label	ピア IPv6 アドレス	PeerIPv6

CEF キー	説明	値
cat	イベントのカテゴリ	例: File
cnt	総数	例: 1
cn1	CCCA の検出	0 または 1
cn1Label	CCCA の検出 <cnx または csx>Label はラベルのキー名です。	CCCA_Detection
cn3	脅威の種類	• 0: 不正なコンテンツ • 1: 不正な動作 • 2: 不審動作 • 3: セキュリティホール悪用 • 4: グレーウェア
cn3Label	脅威の種類	ThreatType
cs1	メールの件名	例: hello
cs1Label	メールの件名	MailSubject
cs2	不正プログラム名	例: HEUR_NAMETRICK.A
cs2Label	不正プログラム名	DetectionName
cs3	ホスト名	例: CLIENT1
cs3Label	ホスト名	HostName_Ext
cs4	アーカイブ内のファイル名	例: mtxlegih.dll
cs4Label	アーカイブ内のファイル名	FileNameInArchive

CEF キー	説明	値
cs5	CCCA ログの検出元	例: GLOBAL_INTELLIGENCE または VIRTUAL_ANALYZER または USER_DEFINED
cs5Label	CCCA ログの検出元	CCCA_DetectionSource
cs6	攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
cs6Label	攻撃段階	pAttackPhase
destinationTranslatedAddress	ピア IP アドレス	例: 10.1.144.199
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
dhost	送信先ホスト名	例: dhost1

CEF キー	説明	値
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
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
duser	メール受信者	例: duser1
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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
filePath	ファイルパス	例: SHARE\\
fileType	実際のファイルタイプ	例: 1638400
flexNumber1	vLANId	例: 4095
flexNumber1Label	vLANId	vLANId
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
oldFileHash	メール添付ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
oldFileName	メール添付ファイル名	例: excel.rar
oldFileSize	メール添付ファイルのサイズ	例: 150000
oldFileType	メール添付ファイルのタイプ	例: 1638400

CEF キー	説明	値
requestClientApplication	ユーザエージェント	例: IE
request	URL	例: http://1.2.3.4/query?term=value
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
shost	送信元ホスト名	例: shost1
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	注目すべき IP	例: 10.1.144.199
src	送信元 IP アドレス	例: 10.1.144.199
spt	送信元ポート	0〜65535 の値
suid	ユーザ名	例: User1
suser	メール送信者	例: suser1

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|0|
Eicar_test_file
- HTTP (Response)|8|dvc=172.22.9.32
dvcmac=00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-
4738984C-A4BF-84A0-D603
rt=Jun 22 2017 09:42:47 GMT+08:00 app=HTTP
deviceDirection=1
dhost=172.22.9.5 dst=172.22.9.5 dpt=57908
dmac=00:50:56:82:e7:a9
shost=172.22.9.54 src=172.22.9.54 spt=80
smac=00:50:56:82:c6:ae
cs3Label=HostName_Ext cs3=172.22.9.54 cs2Label=
DetectionName
cs2=Eicar_test_file fname=eicarcom2.zip fileType=
262340608
fsize=308 requestClientApplication=Wget/1.12 (linux-gnu)
act=not blocked cn3Label=Threat Type cn3=0
destinationTranslatedAddress=172.22.9.5
fileHash=BEC1B52D350D721C7E22A6D4BB0A92909893A3AE
cs4Label=FileNameInArchive cs4=eicar.com
```

```
sourceTranslatedAddress=172.22.9.54
cnt=1 cat=Malware cs6Label=pAttackPhase cs6=Point
of Entry flexNumber1Label=vLANId flexNumber1=4095
request=http://172.22.9.54/eicarcom2.zip
devicePayloadId=0:143:P
```

CEF 形式の要注意アプリケーションログ

表 3-2. CEF 形式の要注意アプリケーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100120
Header (eventName)	説明	Deep Discovery Inspector detected this protocol in your monitored network.
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
app	プロトコル	例: HTTP
c6a1	注目すべき IPv6	例: 2001:0:0:1::21
c6a1Label	注目すべき IPv6	InterestedIPv6
c6a2	送信元 IPv6 アドレス	例: 2001:0:0:1::21
c6a2Label	送信元 IPv6 アドレス	送信元 IPv6 アドレス

CEF キー	説明	値
c6a3	送信先 IPv6 アドレス	例: 2001:0:0:1::21
c6a3Label	送信先 IPv6 アドレス	送信先 IPv6 アドレス
c6a4	ピア IPv6 アドレス	例: 2001:0:0:1::21
c6a4Label	ピア IPv6 アドレス	PeerIPv6
cnt	総数	例: 1
cn3	脅威の種類	6
cn3Label	脅威の種類	ThreatType
destinationTranslatedAddress	ピア IP アドレス	例: 10.1.144.199
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
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

CEF キー	説明	値
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
flexNumber1	vLANId	例: 4095
flexNumber1Label	vLANId	vLANId
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
shost	送信元ホスト名	例: shost1
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	注目すべき IP	例: 10.1.144.199
spt	送信元ポート	0〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100120|Deep
Discovery Inspector detected the protocol in your
monitored network.|2|dvc=172.22.9.32 dvcmac=
00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-
4738984C-A4BF-84A0-D603
rt=Jun 22 2017 10:06:24 GMT+08:00 app=eDonkey
deviceDirection=1 dhost=10.1.100.223 dst=10.1.100.223
dpt=4662 dmac=00:0c:29:a7:72:74 shost=10.1.117.231
src=10.1.117.231 spt=39933 smac=00:30:da:2d:47:32
cn3Label=Threat Type cn3=6 sourceTranslatedAddress=
10.1.117.231
destinationTranslatedAddress=10.1.100.223 cnt=1
flexNumber1Label=vLANId flexNumber1=4095
devicePayloadId=6:11:P
```

CEF 形式の Web レピュテーションログ

表 3-3. CEF 形式の Web レピュテーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100101
Header (eventName)	説明	例: Dangerous URL in Web Reputation Services database - HTTP (Request)
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
app	プロトコル	例: HTTP
c6a1	注目すべき IPv6	例: 2001:0:0:1::21
c6a1Label	注目すべき IPv6	InterestedIPv6
c6a2	送信元 IPv6 アドレス	例: 2001:0:0:1::21
c6a2Label	送信元 IPv6 アドレス	送信元 IPv6 アドレス
c6a3	送信先 IPv6 アドレス	例: 2001:0:0:1::21
c6a3Label	送信先 IPv6 アドレス	送信先 IPv6 アドレス
c6a4	ピア IPv6 アドレス	例: 2001:0:0:1::21
c6a4Label	ピア IPv6 アドレス	PeerIPv6

CEF キー	説明	値
cn1	CCCA の検出	0 または 1
cn1Label	CCCA の検出	CCCA_Detection
cn2	スコア	例: 49
cn2Label	スコア	WRSScore
cn3	脅威の種類	例: 5
cn3Label	脅威の種類	ThreatType
cs1	メールの件名	例: hello
cs1Label	メールの件名	MailSubject
cs2	カテゴリ	例: Gambling
cs2Label	カテゴリ	URLCategory
cs3	ホスト名	例: CLIENT1
cs3Label	ホスト名	HostName_Ext
cs4	攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
cs4Label	攻撃段階	pAttackPhase
destinationTranslatedAddress	ピア IP アドレス	例: 10.1.144.199

CEF キー	説明	値
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
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
duser	メール受信者	例: duser1
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
flexNumber1	vLANId	例: 4095
flexNumber1Label	vLANId	vLANId
request	URL	例: http://1.2.3.4/query?term=value
requestClientApplication	ユーザエージェント	例: IE
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00

CEF キー	説明	値
shost	送信元ホスト名	例: shost1
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	注目すべき IP	例: 10.1.144.199
spt	送信元ポート	0〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: suser1

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector
|5.0.1329|100101|Ransomware
URL in Web Reputation Services database - HTTP
(Request)|8|dvc=172.22.9.32 dvcmac=00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-4738984
C-A4BF-84A0-D603
rt=Jun 22 2017 10:00:17 GMT+08:00 cs3Label=HostName_Ext
cs3=ca95-1.winshipway.com cn2Label=WRSScore cn2=49
cn3Label=Threat Type cn3=5 dmac=00:16:c8:65:98:d5
shost=172.22.9.5 src=172.22.9.5 spt=41757
smac=00:50:56:82:e7:a9
sourceTranslatedAddress=172.22.9.5
cn1Label=CCCA_Detection
cn1=1 request=http://ca95-1.winshipway.com/
requestClientApplication=Wget/1.12
(linux-gnu) app=HTTP deviceDirection=1
dhost=150.70.162.115
dst=150.70.162.115 dpt=80 cs2Label=URLCategory
cs2=Ransomware destinationTranslatedAddress=
150.70.162.115
cs4Label=pAttackPhase cs4=Command and Control
Communication flexNumber1Label=vLANId flexNumber1=4095
request=http://ca95-1.winshipway.com/
devicePayloadId=5:17:
```

CEF 形式のシステムログ

表 3-4. CEF 形式のシステムログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	• 300102 • 300999
Header (eventName)	説明	例: The system time setting has been changed.
Header (severity)	重大度	• 2: 情報 • 4: 警告 • 6: 重要 例: 2
c6a2	送信元 IPv6 アドレス	例: 2001:0:0:1::21
c6a2Label	送信元 IPv6 アドレス	送信元 IPv6 アドレス
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	アカウント	例: admin
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
outcome	結果	• Success • Failure 例: Success
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
src	ユーザの IP アドレス	例: 10.1.1.1

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1175|300999|T
he system time setting has been changed.|2|dvc=10.201.156.14
3 dvcmac=00:0C:29:A6:53:0C dvchost=ddi38-143 deviceExternalI
d=6B593E17AFB7-40FBBB28-A4CE-0462-A536 rt=Mar 09 2015 16:46:
08 GMT+08:00
```

CEF 形式の仮想アナライザログ:ファイル分析イベント

表 3-5. CEF 形式のファイル分析イベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	200119
Header (eventName)	説明	Sample file sandbox analysis is finished.
Header (severity)	重大度	3 (固定値)

CEF キー	説明	値
cn1	GRID が無害と知られている	• 0: 不正なファイル • -1: 不明なファイル • 1: 無害なファイル
cn1Label	GRID が無害と知られている	GRIDIsKnownGood
cn2	ROZ レーティング	• 0: リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高
cn2Label	ROZ レーティング	ROZRating
cn3	PcapReady	例: 0
cn3Label	PcapReady	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	ウイルス名	例: HEUR_NAMETRICK.A
cs2Label	ウイルス名	MalwareName
cs3	上位の SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
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

CEF キー	説明	値
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: WIN32 EXE
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+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200119|S
ample file sandbox analysis is finished|3| rt=Mar 11 2015 06
:51:46 GMT-04:00 dvc=10.201.156.143 dvchost=ddi38-143 dvcmac
=00:0C:29:A6:53:0C deviceExternalId=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E fname=Tomb Raider.rar fileHash=1E4677A1EF1FBAD1
1F8D06A9DAD8103C2CE861A9 fileType=RAR fsize=131372 cs1Label=
SandboxImageType cs1=MAK_win7sp1en_offices_noab_TL cn2Label=
ROZRating cn2=1 cn1Label=GRIDIsKnownGood cn1=-1 cs2Label=Mal
wareName cs2=HEUR_NAMETRICK.A cn3Label=PcapReady cn3=0
```

CEF 形式の仮想アナライザログ:著しい特性イベント

表 3-6. CEF 形式の著しい特性イベント

CEF キー	説明	値
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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	200127
Header (eventName)	説明	Notable Characteristics of the analyzed sample
Header (severity)	重大度	6 (固定値)
cs1	違反ポリシー名	例: Suspicious network or messaging activity
cs1Label	違反ポリシー名	PolicyCategory
cs2	違反イベントの分析	例: Uses spoofed version information
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: WIN32 EXE
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372

CEF キー	説明	値
msg	詳細	例: The file has no company information.
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200127|N
otable Characteristics of the analyzed sample|6|rt=Mar 11 20
15 05:00:26 GMT-04:00 dvc=10.201.156.143 dvchost=ddi38-143 d
vcmac=00:0C:29:A6:53:0C deviceExternalId=D2C1D6D20FF8-4FC98F
92-25EB-D7DA-AF0E fname=DTAS_WIN32_07 fileHash=672B1A8ADB412
C272CCA21A214732C447B650349 fileType=WIN32 EXE fsize=290304
cs1Label=PolicyCategory cs1=Deception, social engineering ms
g=The file has no company information. cs2Label=PolicyName c
s2=Uses spoofed version information
```

CEF 形式の仮想アナライザログ:拒否リストトランザクションイベント

表 3-7. CEF 形式の拒否リストトランザクションイベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	200120
Header (eventName)	説明	Deny List updated
Header (severity)	重大度	3 (固定値)

CEF キー	説明	値
act	イベントの処理	Add または Remove
cs1	種類	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	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: iplasticalsex.ru
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+08:00
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

CEF キー	説明	値
request	URL	例: http://1.2.3.4/query?term=value
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200120|D
eny List updated|3|rt=Mar 11 2015 07:15:45 GMT-04:00 dvc=10.
201.156.143 dvchost=ddi38-143 dvcmac=00:0C:29:A6:53:0C devic
eExternalId=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E cs1Label=ty
pe cs1=Deny List Domain end=Apr 10 2015 07:15:35 GMT-04:00 a
ct=Add dhost=plasticalsex.ru cs2Label=RiskLevel cs2=Medium
```

第 4 章

Syslog コンテンツマッピング - LEEF

次の各表は、Deep Discovery 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。

注意

LEEF ログ構文では、イベント属性をタブ区切り記号「<009>」で区切ります。

LEEF 形式の脅威ログ

表 4-1. LEEF 形式の脅威ログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventName)	イベント名	• MALWARE_DETECTION • MALWARE_OUTBREAK_DETECTION • SECURITY_RISK_DETECTION
act	イベントの処理	blocked または not blocked
aggregatedCnt	集計数	例: 1
aptRelated	APT 関連イベントを示す	0 または 1
botCommand	BOT コマンド	例: COMMIT
botUrl	BOT URL	例: trend.com
cccaDestination	CCCA アドレス	例: 10.1.144.199
cccaDestinationFormat	CCCA の種類	• IP_DOMAIN • IP_DOMAIN_PORT • URL • EMAIL
cccaDetection	CCCA の検出	0 または 1

LEEF キー	説明	値
cccaDetectionSource	CCCA ログの検出元	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED
cccaRiskLevel	CCCA リスクレベル	• 0: 不明 • 1: 低 • 2: 中 • 3: 高
channelName	チャネル名	例: IRCChannel1
chatUserName	ニックネーム	例: IRCUser1
cnt	総数	例: 1
compressedFileName	アーカイブ内のファイル名	例: mtxlegih.dll
detectionType	検出の種類	• 0: 既知の検出 • 1: 未知の検出 • 2: OPS の検出
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
deviceRiskConfidenceLevel	判定の確実性	• 1: 高 • 2: 中 • 3: 低 • 0: 未定義

LEEF キー	説明	値
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
dhost	送信先ホスト名	例: dhost1
dOSName	送信先ホストの OS	例: Android
dst	送信先 IP アドレス	例: 10.1.144.199
dstGroup	送信先ホストに割り当てられているネットワークグループ	例: monitor1
dstMAC	送信先 MAC	例: 00:0C:29:6E:CB:F9
dstPort	送信先ポート	0〜65535 の値
dstZone	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
duser	メール受信者	例: duser1
dUser1	送信先ユーザ名 1	例: admin
dUser1LoginTime	送信先ユーザのログオン時刻 1	例: Mar 09 2015 17:05:21 GMT+08:00
dUser2	送信先ユーザ名 2	例: admin
dUser2LoginTime	送信先ユーザのログオン時刻 2	例: Mar 09 2015 17:05:21 GMT+08:00
dUser3	送信先ユーザ名 3	例: admin
dUser3LoginTime	送信先ユーザのログオン時刻 3	例: Mar 09 2015 17:05:21 GMT+08:00
dvc	アプライアンスの IP アドレス	例: 10.1.144.199

LEEF キー	説明	値
dvchost	アプライアンスのホスト名	例: localhost
evtCat	イベントのカテゴリ	例: Suspicious Traffic
evtSubCat	イベントのサブカテゴリ	例: Email
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
filePath	ファイルパス	例: SHARE\\
fileType	実際のファイルタイプ	例: 1638400
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
hackerGroup	ハッカーグループ	例: Comment Crew
hackingCampaign	ハッキング攻撃の名称	例: Aurora
hostName	ホスト名	例: CLIENT1
interestedIp	注目すべき IP	例: 10.1.144.199
mailMsgSubject	メールの件名	例: hello
malFamily	不正プログラムファミリ	例: Duqu
malName	不正プログラム名	例: HEUR_NAMETRICK.A
malType	不正プログラムの種類	例: MALWARE
mitigationTaskId	Mitigation のイベントタスク ID	例: dc036acb-9a2e-4939-8244-dedbda9ec4ba
msg	説明	例: HEUR_NAMETRICK.A - SMTP (Email)
oldFileHash	メール添付ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

LEEF キー	説明	値
oldFileName	メール添付ファイル名	例: excel.rar
oldFileSize	メール添付ファイルのサイズ	例: 150000
oldFileType	メール添付ファイルのタイプ	例: 1638400
pAttackPhase	一次攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
pComp	検出元	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199
proto	プロトコル	例: SMTP
protoGroup	プロトコルグループ	例: SMTP
ptype	アプリケーションの種類	IDS
requestClientApplication	ユーザエージェント	例: IE
riskType	潜在的なリスク	• 0: 既知のリスク • 1: 潜在的なリスク
ruleId	ルール ID	例: 52
sAttackPhase	二次攻撃段階	例: Point of Entry

LEEF キー	説明	値
sev	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
shost	送信元ホスト名	例: shost1
sOSName	送信元ホストの OS	例: Android
src	送信元 IP アドレス	例: 10.1.144.199
srcGroup	送信元ホストに割り当てられているネットワークグループ	例: monitor1
srcMAC	送信元 MAC	例: 00:0C:29:6E:CB:F9
srcPort	送信元ポート	0〜65535 の値
srcZone	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
suid	ユーザ名	例: User1
suser	メール送信者	例: suser1
sUser1	送信元ユーザ名 1	例: admin
sUser1LoginTime	送信元ユーザのログオン時刻 1	例: Mar 09 2015 17:05:21 GMT+08:00
sUser2	送信元ユーザ名 2	例: admin
sUser2LoginTime	送信元ユーザのログオン時刻 2	例: Mar 09 2015 17:05:21 GMT+08:00
sUser3	送信元ユーザ名 3	例: admin

LEEF キー	説明	値
sUser3LoginTime	送信元ユーザのログオン時刻 3	例: Mar 09 2015 17:05:21 GMT+08:00
threatType	脅威の種類	• 0: 不正なコンテンツ • 1: 不正な動作 • 2: 不審動作 • 3: セキュリティホール悪用 • 4: グレーウェア
url	URL	例: http://1.2.3.4/query?term=value
vLANId	VLAN ID	0〜4095 の値

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|SECUR
ITY_RISK_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss z<009>
ptype=IDS<009>dvc=10.201.156.143<009>deviceMacAddress=00:0C:
29:A6:53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB
7-40FBBB28-A4CE-0462-A536<009>devTime=Mar 09 2015 11:58:24 G
MT+08:00<009>sev=6<009>protoGroup=HTTP<009>proto=HTTP<009>vL
ANId=4095<009>deviceDirection=1<009>dhost=www.freewebs.com<0
09>dst=216.52.115.2<009>dstPort=80<009>dstMAC=00:1b:21:35:8b
:98<009>shost=172.16.1.197<009>src=172.16.1.197<009>srcPort=
12121<009>srcMAC=fe:ed:be:ef:5a:c6<009>malType=MALWARE<009>s
AttackPhase=Point of Entry<009>fname=setting.doc<009>fileTyp
e=0<009>fsize=0<009>ruleId=20<009>msg=HEUR_NAMETRIC
K.A - SMTP (Email)<009>deviceRiskConfidenceLevel=2
<009>url=http://www.freewebs.com/setting3/setting.doc
<009>pComp=CAV<009>riskType=1<009>
srcGroup=Default<009>srcZone=1<009>dstZone=0<009>dete
ctionType=1<009>act=not blocked<009>threatType=1<009>interes
tedIp=172.16.1.197<009>peerIp=216.52.115.2<009>hostName=www.
```

```
freewebs.com<009>cnt=1<009>aggregatedCnt=1<009>cccaDestinati
onFormat=URL<009>cccaDetectionSource=GLOBAL_INTELLIGENCE<009
>cccaRiskLevel=2<009>cccaDestination=http://www.freewebs.com
/setting3/setting.doc<009>cccaDetection=1<009>evtCat=Callbac
k evtSubCat=Bot<009>pAttackPhase=Command and Control Communi
cation
```

LEEF 形式の要注意アプリケーションログ

表 4-2. LEEF 形式の要注意アプリケーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventName)	イベント名	DISRUPTIVE_APPLICATION_DETECTION
aggregatedCnt	集計数	例: 1
cnt	総数	例: 1
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z

LEEF キー	説明	値
dhost	送信先ホスト名	例: dhost1
dOSName	送信先ホストの OS	例: Android
dst	送信先 IP アドレス	例: 10.1.144.199
dstGroup	送信先ホストに割り当てられているネットワークグループ	例: monitor1
dstMAC	送信先 MAC	例: 00:0C:29:6E:CB:F9
dstPort	送信先ポート	0〜65535 の値
dstZone	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
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
interestedIp	注目すべき IP	例: 10.1.144.199
msg	説明	例: Deep Discovery Inspector detected the protocol in your monitored network.
pComp	検出元	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199
proto	プロトコル	例: SMTP
protoGroup	プロトコルグループ	例: SMTP
ptype	アプリケーションの種類	IDS

LEEF キー	説明	値
sev	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
shost	送信元ホスト名	例: shost1
sOSName	送信元ホストの OS	例: Android
src	送信元 IP アドレス	例: 10.1.144.199
srcGroup	送信元ホストに割り当てられているネットワークグループ	例: monitor1
srcMAC	送信元 MAC	例: 00:0C:29:6E:CB:F9
srcPort	送信元ポート	0〜65535 の値
srcZone	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
threatType	脅威の種類	6
vLANId	VLAN ID	0〜4095 の値

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|DISRU
PTIVE_APPLICATION_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:
ss z<009>dvc=10.201.156.143<009>deviceMacAddress=00:0C:29:A6
```

```
:53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40F
BBB28-A4CE-0462-A536<009>ptype=IDS<009>devTime=Mar 09 2015 1
4:20:38 GMT+08:00<009>sev=2<009>protoGroup=STREAMING<009>pro
to=WMSP<009>vLANId=4095<009>deviceDirection=1<009>dhost=12.1
90.48.13<009>dst=12.190.48.13<009>dstPort=80<009>dstMAC=00:1
7:9a:65:f3:05<009>shost=192.168.33.2<009>src=192.168.33.2<00
9>srcPort=35125<009>srcMAC=00:16:6f:a1:3d:7a<009>msg=Deep Di
scovery Inspector detected the protocol in your monitored ne
twork.<009>pComp=CAV<009>threatType=6<009>srcGroup=Default<0
09>srcZone=1<009>dstZone=0<009>interestedIp=192.168.33.2<009
>peerIp=12.190.48.13<009>cnt=1<009>aggregatedCnt=1
```

LEEF 形式の Web レピュテーションログ

表 4-3. LEEF 形式の Web レピュテーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventName)	イベント名	WEB_THREAT_DETECTION
cccaDetection	CCCA の検出	0 または 1
cccaDetectionSource	CCCA ログの検出元	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED
cccaRiskLevel	CCCA リスクレベル	• 0: 不明 • 1: 低 • 2: 中 • 3: 高

LEEF キー	説明	値
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
dhost	送信先ホスト名	例: dhost1
dOSName	送信先ホストの OS	例: Android
dst	送信先 IP アドレス	例: 10.1.144.199
dstGroup	送信先ホストに割り当てられているネットワークグループ	例: monitor1
dstMAC	送信先 MAC	例: 00:0C:29:6E:CB:F9
dstPort	送信先ポート	0〜65535 の値
dstZone	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
duser	メール受信者	例: duser1
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
hostName	ホスト名	例: CLIENT1
interestedIp	注目すべき IP	例: 10.1.144.199
mailMsgSubject	メールの件名	例: hello
msg	説明	例: Dangerous URL in Web Reputation Services database - HTTP (Request)
pComp	検出元	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199
proto	プロトコル	例: SMTP
protoGroup	プロトコルグループ	例: SMTP
ptype	アプリケーションの種類	IDS
requestClientApplication	ユーザエージェント	例: IE
riskScore	スコア	例: 49
sev	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
shost	送信元ホスト名	例: shost1
sOSName	送信元ホストの OS	例: Android
src	送信元 IP アドレス	例: 10.1.144.199
srcGroup	送信元ホストに割り当てられているネットワークグループ	例: monitor1
srcMAC	送信元 MAC	例: 00:0C:29:6E:CB:F9
srcPort	送信元ポート	0〜65535 の値

LEEF キー	説明	値
srcZone	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
suser	メール送信者	例: suser1
threatType	脅威の種類	5
url	URL	例: http://1.2.3.4/query?term=value
urlCat	カテゴリ	例: Gambling
vLANId	VLAN ID	0〜4095 の値

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|WEB_T
HREAT_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss z<009>dvc
=10.201.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>d
vchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40FBBB28-A4CE-0
462-A536<009>ptype=IDS<009>devTime=Mar 09 2015 14:06:36 GMT+
08:00<009>sev=6<009>protoGroup=HTTP<009>proto=HTTP<009>vLANI
d=4095<009>deviceDirection=1<009>dhost=www.freewebs.com<009>
dst=216.52.115.2<009>dstPort=80<009>dstMAC=00:1b:21:35:8b:98
<009>shost=172.16.1.197<009>src=172.16.1.197<009>srcPort=121
21<009>srcMAC=fe:ed:be:ef:5a:c6<009>hostName=www.freewebs.co
m<009>msg=Dangerous URL in Web Reputation Services
database - HTTP (Request)<009>url=http:
//www.freewebs.com/setting3/setting.doc<009>
pComp=TMUFE<009>srcGroup=Default<009>
srcZone=1<009>dstZone=0<009>urlCat=
Disease Vector<009>riskScore=49<009>threatTy
```

```
pe=5<009>interestedIp=172.16.1.197<009>
peerIp=216.52.115.2
```

LEEF 形式のシステムログ

表 4-4. LEEF 形式のシステムログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
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
deviceMacAddress	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: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy 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
msg	説明	例: The system time setting has been changed.
ptype	アプリケーションの種類	IDS

LEEF キー	説明	値
sev	重大度	• 2: 情報 • 4: 警告 • 6: 重要 例: 2

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|SYSTE
M_EVENT|dvc=10.201.156.143<009>deviceMacAddress=00:0C:29:A6:
53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40FB
BB28-A4CE-0462-A536<009>ptype=IDS<009>devTimeFormat=MMM dd y
yyy HH:mm:ss z<009>sev=2<009>msg=The system time setting has
 been changed.<009>devTime=Mar 09 2015 16:46:08 GMT+08:00
```

LEEF 形式の相関関係のあるインシデントログ

表 4-5. LEEF 形式の相関関係のあるインシデントログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventName)	イベント名	SUSPICIOUS_BEHAVIOUR_DETECTION

LEEF キー	説明	値
data0	相関関係データ 0	Additional attribute values
data1	相関関係データ 1	Additional attribute values
data2	相関関係データ 2	Additional attribute values
data3	相関関係データ 3	Additional attribute values
data4	相関関係データ 4	Additional attribute values
data5	相関関係データ 5	Additional attribute values
data6	相関関係データ 6	Additional attribute values
data7	相関関係データ 7	Additional attribute values
data8	相関関係データ 8	Additional attribute values
data9	相関関係データ 9	Additional attribute values
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
devTime	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy 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
interestedHost	関係するホスト名	例: trend.net
interestedIp	注目すべき IP	例: 10.1.144.199

LEEF キー	説明	値
interestedMacAddress	注目する MAC アドレス	例: 00:0C:29:6E:CB:F9
interestedUser	注目するユーザ名 1	例: user1
interestedUser2	注目するユーザ名 2	例: user2
interestedUser3	注目するユーザ名 3	例: user3
pComp	検出元	Correlation
proto	プロトコル	例: SMTP
ptype	アプリケーションの種類	IDS
ruleId	ルール ID	例: 52
ruleName	ルール名	例: This host has responded to DNS queries.
sev	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
threatName	脅威の名前	例: Malicious Bot
threatType	脅威の種類	例: Malware-related
userGroup	ユーザグループ	例: Default

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|SUSPI
CIOUS_BEHAVIOUR_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss
 z<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=ddi38-
143<009>pComp=Correlation<009>dvc=10.201.156.143<009>ptype=I
```

```
DS<009>deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E<009>d
evTime=Mar 11 2015 22:05:50 GMT-04:00<009>sev=2<009>interest
edIp=172.16.0.100<009>interestedHost=172.16.0.100<009>intere
stedMacAddress=00:0c:29:70:45:...36<009>ruleId=47<009>ruleNa
me=This host has responded to DNS queries.<009>threatType=Un
registered Service<009>threatName=Unregistered DNS Server<00
9>proto=DNS Response<009>userGroup=Default<009>deviceDirecti
on=1
```

LEEF 形式の仮想アナライザログ:ファイル分析イベント

表 4-6. LEEF 形式のファイル分析イベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
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:29:6E:CB:F9
deviceOSName	サンドボックスイメージの種類	SandboxImageType
deviceProcessHash	上位の SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
devTime	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

LEEF キー	説明	値
devTimeFormat	時刻の形式	MMM dd yyyy 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	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: WIN32 EXE
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
gridIsKnownGood	GRID が無害と知られている	• 0: 不正なファイル • -1: 不明なファイル • 1: 無害なファイル
malName	ウイルス名	例: HEUR_NAMETRICK.A
pcapReady	PCAP 使用可能	例: 1
pComp	検出元	• Sandbox • UDSO (ユーザ指定の不審オブジェクト)
rozRating	ROZ レーティング	• 0: リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高
sev	重大度	3 (固定値)

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|FILE_
ANALYZED|devTime=Mar 11 2015 07:36:27 GMT-04:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009
>dvc=10.201.156.143<009>dvchost=ddi38-143<009>deviceMacAddre
ss=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E<009>fname=mwsoemon.exe<009>fileHash=89DE67C5220
91EE259533D9CBDDF37DDB8C8D636<009>malName=Possible_Virus<009
>fileType=WIN32 EXE<009>fsize=59392<009>deviceOSName=MAK_win
7sp1en_offices_noab_TL<009>gridIsKnownGood=-1<009>rozRating=
1<009>pcapReady=1
```

LEEF 形式の仮想アナライザログ:著しい特性イベント

表 4-7. LEEF 形式の著しい特性イベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventName)	イベント名	NOTABLE_CHARACTERISTICS
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:29:6E:CB:F9

LEEF キー	説明	値
deviceOSName	サンドボックスイメージの種類	例: win7
devTime	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy 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	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: WIN32 EXE
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: www.chapisteriadaniel.com
pComp	検出元	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	6 (固定値)

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|NOTAB
LE_CHARACTERISTICS|devTime=Mar 11 2015 05:00:26 GMT-04:00<00
```

```
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>pComp=S
andbox<009>dvc=10.201.156.143<009>dvchost=ddi38-143<009>devi
ceMacAddress=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4
FC98F92-25EB-D7DA-AF0E<009>fname=DTAS_WIN32_07<009>fileHash=
672B1A8ADB412C272CCA21A214732C447B650349<009>fileType=WIN32
EXE<009>fsize=290304<009>ruleCategory=Suspicious network or
messaging activity<009>ruleName=Queries DNS server<009>msg=0
12webpages.com<009>deviceOSName=MAK_win7sp1en_offices_noab_T
L
```

LEEF 形式の仮想アナライザログ:拒否リストトランザクションイベント

表 4-8. LEEF 形式の拒否リストトランザクションイベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
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

LEEF キー	説明	値
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
devTime	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
dhost	送信先ホスト名	例: insta-find.com
dpt	リモートポート	0〜65535 の値
dst	リモート 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+08:00
fileHash	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	検出元	Sandbox
sev	重大度	3 (固定値)
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/

ログの例:

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「<009>」で区切ります。

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|DENYL
IST_CHANGE|devTime=Mar 11 2015 05:00:42 GMT-04:00<009>devTim
eFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<0
09>dvc=10.201.156.143<009>dvchost=ddi38-143<009>deviceMacAdd
ress=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4FC98F92-
25EB-D7DA-AF0E<009>end=Apr 10 2015 05:00:26 GMT-04:00<009>ac
t=Add<009>dhost=ourdatatransfers.com<009>deviceExternalRiskT
ype=High<009>type=Deny List Domain
```

第 5 章

Syslog コンテンツマッピング - TMEF

次の各表は、Deep Discovery 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。

TMEF 形式の脅威ログ

表 5-1. TMEF 形式の脅威ログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	イベント ID	• 100100 • 100118 • 100119
Header (eventName)	イベント名	• MALWARE_DETECTION • MALWARE_OUTBREAK_DETECTION • SECURITY_RISK_DETECTION
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
act	イベントの処理	blocked または not blocked
app	プロトコル	例: HTTP
appGroup	プロトコルグループ	例: HTTP
compressedFileHash	圧縮ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
compressedFileName	アーカイブ内のファイル名	例: mtxlegih.dll

TMEF キー	説明	値
compressedFileType	実際のファイルタイプ	例: 0
cnt	総数	例: 1
cn1	CCCA の検出	0 または 1
cn1Label	CCCA の検出	CCCA_Detection
cn2	APT 関連イベントを示す	0 または 1
cn2Label	APT 関連イベントを示す	APT Related
cn3	潜在的なリスク	• 0: 既知のリスク • 1: 潜在的なリスク
cn3Label	潜在的なリスク	Deep Discovery_PotentialRisk
cn4	脅威の種類	• 0: 不正なコンテンツ • 1: 不正な動作 • 2: 不審動作 • 3: セキュリティホール悪用 • 4: グレーウェア
cn4Label	脅威の種類	Deep Discovery_ThreatType
cn5	集計数	例: 1
cn5Label	集計数	AggregatedCnt
cn6	CCCA リスクレベル	• 0: 不明 • 1: 低 • 2: 中 • 3: 高
cn6Label	CCCA リスクレベル	CCCA_RiskLevel
cn7	ヒューリスティックフラグ	• 0: 非ヒューリスティック検出 • 1: ヒューリスティック検出

TMEF キー	説明	値
cn7Label	ヒューリスティックフラグ	HeurFlag
cs1	チャネル名	例: IRCChannel1
cs1Label	チャネル名	IRCChannelName
cs2	ニックネーム	例: IRCUser1
cs2Label	ニックネーム	IRCUserName
cs3	ホスト名	例: CLIENT1
cs3Label	ホスト名	HostName_Ext
cs4	送信元ホストに割り当てられているネットワークグループ	例: monitor1
cs4Label	送信元ホストに割り当てられているネットワークグループ	Deep Discovery_SrcGroup
cs5	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs5Label	送信元ゾーン	Deep Discovery_SrcZone
cs6	検出の種類	• 0: 既知の検出 • 1: 未知の検出 • 2: OPS の検出
cs6Label	検出の種類	Deep Discovery_DetectionType
cs7	BOT コマンド	例: COMMIT
cs7Label	BOT コマンド	BOT_CMD
cs8	BOT URL	例: trend.com

TMEF キー	説明	値
cs8Label	BOT URL	BOT_URL
cs9	送信先ホストに割り当てられているネットワークグループ	例: monitor1
cs9Label	送信先ホストに割り当てられているネットワークグループ	Deep Discovery_DstGroup
cs10	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs10Label	送信先ゾーン	Deep Discovery_DstZone
cs11	CCCA ログの検出元	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED • RELEVANCE_RULE
cs11Label	CCCA ログの検出元	CCCA_DetectionSource
cs12	CCCA アドレス	例: 10.1.144.199
cs12Label	CCCA アドレス	CCCA_Destination
cs13	CCCA の種類	• IP_DOMAIN • IP_DOMAIN_PORT • URL • EMAIL
cs13Label	CCCA の種類	CCCA_DestinationFormat

TMEF キー	説明	値
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
deviceRiskConfidenceLevel	判定の確実性	• 1: 高 • 2: 中 • 3: 低 • 0: 未定義
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
dOSName	送信先ホストの OS	例: Android
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
duser	メール受信者	例: duser1
dUser1	送信先ユーザ名 1	例: admin
dUser1LoginTime	送信先ユーザのログオン時刻 1	例: Mar 09 2015 17:05:21 GMT+08:00
dUser2	送信先ユーザ名 2	例: admin

TMEF キー	説明	値
dUser2LoginTime	送信先ユーザのログオン時刻 2	例: Mar 09 2015 17:05:21 GMT+08:00
dUser3	送信先ユーザ名 3	例: admin
dUser3LoginTime	送信先ユーザのログオン時刻 3	例: Mar 09 2015 17:05:21 GMT+08:00
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
evtCat	イベントのカテゴリ	例: Suspicious Traffic
evtSubCat	イベントのサブカテゴリ	例: Email
externalId	ログ ID	例: 11
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
filePath	ファイルパス	例: SHARE\\
fileType	実際のファイルタイプ	例: 1638400
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
hackerGroup	ハッカーグループ	例: Comment Crew
hackingCampaign	ハッキング攻撃の名称	例: Aurora
hostSeverity	ホストの重大度	例: 4
interestedIp	注目すべき IP	例: 10.1.144.199
mailMsgSubject	メールの件名	例: hello
malFamily	不正プログラムファミリ	例: Duqu
malName	不正プログラム名	例: HEUR_NAMETRICK.A

TMEF キー	説明	値
malType	不正プログラムの種類	例: MALWARE
messageId	メッセージ ID	例: <20090130042416.7060505@jovencitasvirgenes.com.ar>
mitigationTaskId	Mitigation のイベントタスク ID	例: dc036acb-9a2e-4939-8244-dedbda9ec4ba
oldFileHash	メール添付ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
oldFileName	メール添付ファイル名	例: excel.rar
oldFileSize	メール添付ファイルのサイズ	例: 150000
oldFileType	メール添付ファイルのタイプ	例: 1638400
pAttackPhase	一次攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
pComp	検出元	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199
ptype	アプリケーションの種類	IDS
reason	理由	例: ["Protocol: 4"]
request	URL	例: http://1.2.3.4/query?term=value

TMEF キー	説明	値
requestClientApplication	ユーザエージェント	例: IE
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
ruleId	ルール ID	例: 52
ruleName	説明	例: Email message sent through an unregistered SMTP server
sAttackPhase	二次攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
shost	送信元ホスト名	例: shost1
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sOSName	送信元ホストの OS	例: Android
spt	送信元ポート	0〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199
suid	ユーザ名	例: User1
suser	メール送信者	例: suser1
sUser1	送信元ユーザ名 1	例: admin
sUser1LoginTime	送信元ユーザのログオン時刻 1	例: Mar 09 2015 17:05:21 GMT+08:00
sUser2	送信元ユーザ名 2	例: admin
sUser2LoginTime	送信元ユーザのログオン時刻 2	例: Mar 09 2015 17:05:21 GMT+08:00

TMEF キー	説明	値
sUser3	送信元ユーザ名 3	例: admin
sUser3LoginTime	送信元ユーザのログオン時刻 3	例: Mar 09 2015 17:05:21 GMT+08:00
vLANId	VLAN ID	0〜4095 の値

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|
5.0.1329|100100|
MALWARE_DETECTION|8| ptype=IDS dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
 deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
rt=Jun 22 2017 09:42:47  GMT+08:00 appGroup=HTTP
app=HTTP vLANId=4095 deviceDirection=1 dhost=172.22.9.5
 dst=172.22.9.5 dpt=57908 dmac=00:50:56:82:e7:a9
shost=172.22.9.54  src=172.22.9.54 spt=80
smac=00:50:56:82:c6:ae
cs3Label=HostName_Ext  cs3=172.22.9.54
malName=Eicar_test_file
malType=Virus fname=eicarcom2.zip  fileType=262340608
fsize=308 ruleId=0 ruleName=Eicar_test_file -
HTTP (Response) deviceRiskConfidenceLevel=0 cn3Label=Deep
Discovery_PotentialRisk cn3=0  cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone  cs5=1
cs9Label=Deep Discovery_DstGroup cs9=Default
cs10Label=Deep
 Discovery_DstZone cs10=1 cs6Label=Deep
 Discovery_DetectionType
cs6=0  request=http://172.22.9.54/eicarcom2.zip
requestClientApplication=Wget/1.12  (linux-gnu)
pComp=VSAPI act=not blocked cn4Label=Deep
Discovery_ThreatType
 cn4=0 peerIp=172.22.9.5
fileHash=BEC1B52D350D721C7E22A6D4BB0A92909893A3AE
 compressedFileName=eicar.com interestedIp=172.22.9.54
cnt=1 dOSName=Linux  cn5Label=AggregatedCount
cn5=1 evtCat=Malware evtSubCat=Trojan cn2Label=APT
 Related cn2=0 pAttackPhase=Point of Entry externalId=143
```

```
cn7Label=HeurFlag  cn7=0 compressedFileType=327680
compressedFileHash=3395856CE81F2B7382DEE72602F
798B642F14140 hostSeverity=8 reason=["Malware:
Eicar_test_file"]  devicePayloadId=0:143:P
```

TMEF 形式の要注意アプリケーションログ

表 5-2. TMEF 形式の要注意アプリケーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100120
Header (eventName)	イベント名	DISRUPTIVE_APPLICATION_DETECTION
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
app	プロトコル	例: HTTP
appGroup	プロトコルグループ	例: HTTP
cnt	総数	例: 1
cn4	脅威の種類	6
cn4Label	脅威の種類	Deep Discovery_ThreatType
cn5	集計数	例: 1

TMEF キー	説明	値
cn5Label	集計数	AggregatedCnt
cs4	送信元ホストに割り当てられているネットワークグループ	例: monitor1
cs4Label	送信元ホストに割り当てられているネットワークグループ	Deep Discovery_SrcGroup
cs5	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs5Label	送信元ゾーン	Deep Discovery_SrcZone
cs9	送信先ホストに割り当てられているネットワークグループ	例: monitor1
cs9Label	送信先ホストに割り当てられているネットワークグループ	Deep Discovery_DstGroup
cs10	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs10Label	送信先ゾーン	Deep Discovery_DstZone
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

TMEF キー	説明	値
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
dOSName	送信先ホストの OS	例: Android
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
externalId	ログ ID	例: 11
interestedIp	注目すべき IP	例: 10.1.144.199
msg	説明	例: Deep Discovery Inspector detected the protocol in your monitored network.
pComp	検出元	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199
ptype	アプリケーションの種類	IDS
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
shost	送信元ホスト名	例: shost1

TMEF キー	説明	値
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sOSName	送信元ホストの OS	例: Android
spt	送信元ポート	0〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199
vLANId	VLAN ID	0〜4095 の値

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100120|
DISRUPTIVE_APPLICATION_DETECTION|2|dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
ptype=IDS rt=Jun 22 2017 10:06:24 GMT+08:00 appGroup=P2P
app=eDonkey vLANId=4095 deviceDirection=1
dhost=10.1.100.223
dst=10.1.100.223 dpt=4662 dmac=00:0c:29:a7:72:74
shost=10.1.117.231 src=10.1.117.231 spt=39933
smac=00:30:da:2d:47:32 cn5Label=AggregatedCount
cn5=1 msg=Deep Discovery Inspector detected the
protocol in your monitored network. cn4Label=Deep
Discovery_ThreatType cn4=6 cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone cs5=1
cs9Label=Deep Discovery_DstGroup cs9=Default
cs10Label=Deep
Discovery_DstZone cs10=1 interestedIp=10.1.117.231
peerIp=10.1.100.223 pComp=CAV cnt=1 externalId=11
devicePayloadId=6:11:
```

TMEF 形式の Web レピュテーションログ

表 5-3. TMEF 形式の Web レピュテーションログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100101
Header (eventName)	イベント名	WEB_THREAT_DETECTION
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
app	プロトコル	例: HTTP
appGroup	プロトコルグループ	例: HTTP
cn1	CCCA の検出	0 または 1
cn1Label	CCCA の検出	CCCA_Detection
cn2	スコア	例: 49
cn2Label	スコア	Score
cn4	脅威の種類	5
cn4Label	脅威の種類	Deep Discovery_ThreatType

TMEF キー	説明	値
cn6	CCCA リスクレベル	• 0: 不明 • 1: 低 • 2: 中 • 3: 高
cn6Label	CCCA リスクレベル	CCCA_RiskLevel
cs3	ホスト名	例: CLIENT1
cs3Label	ホスト名	HostName_Ext
cs4	送信元ホストに割り当てられているネットワークグループ	例: monitor1
cs4Label	送信元ホストに割り当てられているネットワークグループ	Deep Discovery_SrcGroup
cs5	送信元ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs5Label	送信元ゾーン	Deep Discovery_SrcZone
cs9	送信先ホストに割り当てられているネットワークグループ	例: monitor1
cs9Label	送信先ホストに割り当てられているネットワークグループ	Deep Discovery_DstGroup

TMEF キー	説明	値
cs10	送信先ゾーン	• 0: 監視対象ネットワーク外 • 1: 監視対象ネットワーク内、信頼する • 2: 監視対象ネットワーク内、信頼しない
cs10Label	送信先ゾーン	Deep Discovery_DstZone
cs11	CCCA ログの検出元	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED • RELEVANCE_RULE
cs11Label	CCCA ログの検出元	CCCA_DetectionSource
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:29:6E:CB:F9
devicePayloadId	拡張可能なフィールド。 形式: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	例: • PCAP ファイルが取得される場合: 2:10245:P • PCAP ファイルが取得されない場合: 2:10245:
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
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
dhost	送信先ホスト名	例: dhost1

TMEF キー	説明	値
dmac	送信先 MAC	例: 00:0C:29:6E:CB:F9
dOSName	送信先ホストの OS	例: Android
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
duser	メール受信者	例: duser1
externalId	ログ ID	例: 11
hostSeverity	ホストの重大度	例: 4
interestedIp	注目すべき IP	例: 10.1.144.199
mailMsgSubject	メールの件名	例: hello
msg	説明	例: C&C Server URL in Web Reputation Services database - HTTP (Request)
pAttackPhase	一次攻撃段階	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (該当する攻撃段階なし)
pComp	検出元	例: VSAPI
peerIp	ピア IP アドレス	例: 10.1.144.199
ptype	アプリケーションの種類	IDS
reason	理由	例: ["Protocol: 4"]
request	URL	例: http://1.2.3.4/query?term=value

TMEF キー	説明	値
requestClientApplication	ユーザエージェント	例: IE
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
sAttackPhase	二次攻撃段階	例: Point of Entry
shost	送信元ホスト名	例: shost1
smac	送信元 MAC	例: 00:0C:29:6E:CB:F9
sOSName	送信元ホストの OS	例: Android
spt	送信元ポート	0〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: suser1
urlCat	URL カテゴリ	例: C&C Server
vLANId	VLAN ID	0〜4095 の値

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100101|WEB_THREAT_DETECTION|8|dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
ptype=IDS rt=Jun 22 2017 10:00:17 GMT+08:00
cs3Label=HostName_Ext
cs3=ca95-1.winshipway.com cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone cs5=1
cs10Label=Deep Discovery_DstZone cs10=0 cn2Label=Score
cn2=49 cn4Label=Deep Discovery_ThreatType cn4=5
dmac=00:16:c8:65:98:d5 shost=172.22.9.5 src=172.22.9.5
spt=41757 smac=00:50:56:82:e7:a9 interestedIp=172.22.9.5
cn1Label=CCCA_Detection cn1=1 msg=Ransomware URL
in Web Reputation Services database - HTTP (Request)
request=http://ca95-1.winshipway.com/
requestClientApplication=Wget/1.12
(linux-gnu) pComp=TMUFE appGroup=HTTP app=HTTP
vLANId=4095 deviceDirection=1 dhost=150.70.162.115
```

```
dst=150.70.162.115 dpt=80 urlCat=Ransomware
peerIp=150.70.162.115
sOSName=Linux cn6Label=CCCA_RiskLevel cn6=3
cs11Label=CCCA_DetectionSource
cs11=RELEVANCE_RULE externalId=17 hostSeverity=8
reason=["URL: http://ca95-1.winshipway.com/"]
pAttackPhase=Command and Control Communication
devicePayloadId=5:17:P
```

TMEF 形式のシステムログ

表 5-4. TMEF 形式のシステムログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	• 300102 • 300999
Header (eventName)	イベント名	• PRODUCT_UPDATE • SYSTEM_EVENT • PRODUCT_UPDATE
Header (severity)	重大度	• 2: 情報 • 4: 警告 • 6: 重要 例: 2
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

TMEF キー	説明	値
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
duser	アカウント	例: admin
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
engType	エンジン名	例: Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)
engVer	エンジンのバージョン	例: 10.300.1040
msg	説明	例: The web console timeout setting has been changed.
outcome	結果	• Success • Failure 例: Success
patType	パターン名	例: Deep Discovery Malware Pattern
patVer	パターンのバージョン	例: 14.271.92
ptype	アプリケーションの種類	IDS
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00
src	ユーザの IP アドレス	例: 10.1.1.1

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector
|3.85.1156|300999|SYSTEM_EVENT|2|ptype=IDS
dvc=172.22.9.12 deviceMacAddress=00:50:56:
AD:CC:EE dvchost=localhostdeviceGUID=
DBD38FFC70B4-41C792BE-D671-0040-8B1D
rt=Mar 10 2017 17:03:31 GMT+08:00
msg=The threat detection setting
```

```
has been changed. duser=admin
outcome=Success src=172.17.0.250
```

TMEF 形式の相関関係のあるインシデントログ

表 5-5. 相関関係のあるインシデントログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100127
Header (eventName)	イベント名	SUSPICIOUS_BEHAVIOUR_DETECTION
Header (severity)	重大度	• 2: 情報 • 4: 低 • 6: 中 • 8: 高
app	プロトコル	例: HTTP
cs1	注目するグループ	例: Default
cs1Label	注目するグループ	DD_InterestedGroup
cs2	不正プログラムのサーバのアドレス	例: 10.1.144.199
cs2Label	不正プログラムのサーバのアドレス	Malware_Server_IP_Address
cs3	ダウンロードされた不正プログラムファイル数	例: 1

TMEF キー	説明	値
cs3Label	ダウンロードされた不正プログラムファイル数	Number_of_Malware_Files_Downloaded
cs10	不正プログラム名	例: HEUR_NAMETRICK.A
cs10Label	不正プログラム名	Malware_Name
deviceDirection	パケットの方向	• 0: 送信元が外部 • 1: 送信元が内部 • 2: 不明
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:29:6E:CB:F9
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
interestedHost	注目すべきホスト	例: trend.net
interestedIp	注目すべき IP	例: 10.1.144.199
interestedMacAddress	注目する MAC	例: 00:0C:29:6E:CB:F9
interestedUser	注目するユーザ 1	例: user1
interestedUser2	注目するユーザ 2	例: user2
interestedUser3	注目するユーザ 3	例: user3
pComp	検出元	Correlation
peerHost	ピアホスト	例: 10.1.144.199
peerIp	ピア IP アドレス	例: 10.1.144.199
ptype	アプリケーションの種類	IDS
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00

TMEF キー	説明	値
ruleId	ルール ID	例: 52
ruleName	説明	例: Email message sent through an unregistered SMTP server
threatName	脅威の名前	例: Malware File Downloaded
threatType	脅威の種類	例: Malware-related

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|100127|S
USPICIOUS_BEHAVIOUR_DETECTION|2|dvc=10.201.156.143 deviceMac
Address=00:0C:29:A6:53:0C dvchost=ddi38-143 pComp=Correlatio
n ptype=IDS deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E
rt=Mar 11 2015 22:05:50 GMT-04:00 deviceDirection=1 interest
edIp=172.16.0.100 interestedHost=172.16.0.100 interestedMacA
ddress=00:0c:29:70:45:36 ruleId=47 ruleName=This host has re
sponded to DNS queries. threatType=Unregistered Service thre
atName=Unregistered DNS Server app=DNS Response cs1Label=DD_
InterestedGroup cs1=Default peerHost=172.16.1.141 peerIp=172
.16.1.141
```

TMEF 形式の仮想アナライザログ:ファイル分析イベント

表 5-6. TMEF 形式のファイル分析イベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181

TMEF キー	説明	値
Header (eventid)	署名 ID	200119
Header (eventName)	イベント名	FILE_ANALYZED
Header (severity)	重大度	3 (固定値)
cn1	GRID が無害と知られている	• 0: 不正なファイル • -1: 不明なファイル • 1: 無害なファイル
cn1Label	GRID が無害と知られている	GRIDIsKnownGood
cn2	ROZ レーティング	• 0: リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高
cn2Label	ROZ レーティング	ROZRating
cn3	PCAP 使用可能	0 または 1
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:29:6E:CB:F9
deviseOSName	サンドボックスイメージの種類	例: win7
deviceProcessHash	上位の SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
dvc	アプライアンスの IP アドレス	例: 10.1.144.199

TMEF キー	説明	値
dvchost	アプライアンスのホスト名	例: localhost
fileHash	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: 1638400
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: SWF_Lfm.926
pComp	検出元	• Sandbox • UDSO (ユーザ指定の不審オブジェクト)
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200119|F
ILE_ANALYZED|3|rt=Mar 11 2015 07:38:04 GMT-04:00 pComp=Sandb
ox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacAddress=00:
0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF
0E fname=multiple_mask.swf fileHash=643DBF968EF3BECD9A73CF1D
CF44006BC46E15F7 malName=SWF_Lfm.926 fileType=Macromedia Fla
sh fsize=9400 deviceOSName=MAK_win7sp1en_offices_noab_TL cn2
Label=ROZRating cn2=3 cn1Label=GRIDIsKnownGood cn1=-1 cn3Lab
el=PcapReady cn3=1
```

TMEF 形式の仮想アナライザログ:著しい特性イベント

表 5-7. TMEF 形式の著しい特性イベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	200127
Header (eventName)	イベント名	NOTABLE_CHARACTERISTICS
Header (severity)	重大度	6 (固定値)
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:29:6E:CB:F9
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	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: 1638400
fname	ファイル名	例: excel.rar

TMEF キー	説明	値
fsize	ファイルサイズ	例: 131372
msg	詳細	例: www.chapisteriadaniel.com
pComp	検出元	Sandbox
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00
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:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200127|N
OTABLE_CHARACTERISTICS|6|rt=Mar 11 2015 05:00:26 GMT-04:00 p
Comp=Sandbox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacA
ddress=00:0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E fname=DTAS_WIN32_07 fileHash=672B1A8ADB412C272C
CA21A214732C447B650349 fileType=WIN32 EXE fsize=290304 ruleC
ategory=Suspicious network or messaging activity ruleName=Qu
eries DNS server msg=012webpages.com deviceOSName=MAK_win7sp
1en_offices_noab_TL
```

TMEF 形式の仮想アナライザログ:拒否リストトランザクションイベント

表 5-8. TMEF 形式の拒否リストトランザクションイベント

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector

TMEF キー	説明	値
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	200120
Header (eventName)	イベント名	DENYLIST_CHANGE
Header (severity)	重大度	3 (固定値)
act	イベントの処理	Add または Remove
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	• 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:29:6E:CB:F9
dhost	送信先ホスト名	例: insta-find.com
dpt	リモートポート	0〜65535 の値
dst	リモート 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

TMEF キー	説明	値
end	レポート終了時刻	例: Mar 09 2015 17:05:21 GMT+08:00
fileHash	ファイルの SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	検出元	Sandbox
request	URL	例: _http://1.2.3.4/query?term=value
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200120|D
ENYLIST_CHANGE|3|rt=Mar 11 2015 07:15:45 GMT-04:00 pComp=San
dbox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacAddress=0
0:0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-
AF0E cs1Label=type cs1=Deny List URL end=Apr 10 2015 07:15:3
5 GMT-04:00 act=Add request=http://zalepivmordu.ru:80/ devic
eExternalRiskType=Medium
```

TMEF 形式の Retro Scan レポートログ

表 5-9. TMEF 形式の Retro Scan レポートログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100133

TMEF キー	説明	値
Header (eventName)	イベント名	RETROSCAN_REPORT
Header (severity)	重大度	8
callback_attempt_num	コールバック試行回数	例: 20
cnc_host_num	C&C ホストの数	例: 1
compromised_client_num	感染クライアントの数	例: 1
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
firstCallbackTime	最初のコールバック時刻	例: Mar 09 2015 17:05:21 GMT+08:00
lastCallbackTime	最後のコールバック時刻	例: Mar 09 2015 17:05:21 GMT+08:00
report_id	レポート ID	例: 74c15fe0-90c9-446b-abc4-379d6d7213e7
report_ts	レポート日時	例: Mar 09 2015 17:05:21 GMT+08:00
report_url	レポート URL	例: https://retroscan.trendmicro.com/retroscan/scanDetails.html?reportID\=1e84c77b-0452-4f00-b5b8-e41c0ea9ef1a &reportType\=standard

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1200|100133|R
ETROSCAN_REPORT|8|guid=906A61690458-4099A441-898C-BDD2-C7C1
report_ts=Mar 29 2015 03:14:27 GMT+02:00 report_id=ffa9474d-
6d72-44f7-a99c-c0d230fec1f3 report_url=https://retroscan.tre
ndmicro.com/retroscan/scanDetails.html?reportID\=1e84c77b-04
52-4f00-b5b8-e41c0ea9ef1a&reportType\=standard compromised_c
lient_num=1 cnc_host_num=1 callback_attempt_num=20 firstCall
backTime=Mar 29 2015 03:04:27 GMT+02:00 lastCallbackTime=Mar
 29 2015 03:09:27 GMT+02:00
```

TMEF 形式の Retro Scan 検出ログ

表 5-10. TMEF 形式の Retro Scan 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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Inspector
Header (pver)	アプライアンスのバージョン	例: 3.8.1181
Header (eventid)	署名 ID	100134
Header (eventName)	イベント名	RETROSCAN_DETECTION
Header (severity)	重大度	8
callback_address	コールバックアドレス	例: http://1.2.3.4/
callback_time	コールバック時刻	例: Mar 09 2015 17:05:21 GMT+08:00
category	カテゴリ	例: Reference
cnc_host	C&C ホストアドレス	例: 10.1.144.199
compromised_client	感染クライアントアドレス	例: 10.1.144.199
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
protocol	プロトコル	例: HTTP
rating	レーティング	例: Suspicious
related_attacker_group	関連する攻撃者グループ	例: Elise|Taidoor
related_malware	関連する不正プログラム	例: fosniw|ge|palevo
report_id	レポート ID	例: 74c15fe0-90c9-446b-abc4-379d6d7213e7

TMEF キー	説明	値
scan_category	検索カテゴリ	例: C&C Server
scan_rating	検索レーティング	例: Dangerous
scan_ts	検索時間	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1200|100134|R
ETROSCAN_DETECTION|8|guid=906A61690458-4099A441-898C-BDD2-C7
C1 report_id=0938508b-ec47-47a1-80ea-cd8e3b747822 scan_ts=Ma
r 29 2015 03:14:31 GMT+02:00 callback_time=Mar 29 2015 03:04
:31 GMT+02:00 callback_address=http://app2.winsoft98.com/app
.asp?prj\=4&pid\=haha1&logdata\=MacTryCnt:0&code\=&ver\=1.0.
0.45&appcheck\=1 compromised_client=59.125.99.235 cnc_host=
app2.winsoft98.com protocol=HTTP rating=Suspicious category
=Reference scan_rating=Dangerous scan_category=C&C Server r
elated_malware=fosniw|ge|mactrycnt|palevo related_attacker_
group=Elise|Taidoor
```

索引